



Symantec Endpoint Protection インストールガイドおよび管理者ガイド

May 2021

Table of Contents

リリースノート.....	17
Symantec Endpoint Protection 14.3 RU2 の新機能.....	17
Symantec Endpoint Protection (SEP) の既知の問題と回避策.....	20
Symantec Endpoint Protection (SEP) 14.3 RU2 のシステム要件.....	26
国際化の必要条件.....	34
サポート対象の仮想インストールと仮想化製品.....	35
詳細情報の入手方法.....	36
Symantec Endpoint Protection とは.....	38
Symantec Endpoint Protection 技術でコンピュータが保護される仕組み.....	38
Symantec Endpoint Protection アーキテクチャコンポーネント.....	41
始めましょう.....	43
Symantec Endpoint Protection 14.x のクイックスタートガイド.....	47
つの Symantec Endpoint Protection Manager のインストール.....	52
インストール後の つの Symantec Endpoint Protection Manager の設定.....	53
カスタム設定を使った つの Symantec Endpoint Protection Manager のインストール.....	54
つの Symantec Endpoint Protection Manager コンソールへのログオン.....	56
Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート.....	58
Symantec Endpoint Protection ライセンスの購入.....	62
パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール.....	63
Symantec Endpoint Protection for Mac クライアントのインストール.....	64
Symantec Endpoint Protection for macOS 10.15 以降でのシステム拡張の認証について.....	65
Mac 用 Symantec Endpoint Protection クライアント配備時のカーネル拡張の承認管理.....	66
Symantec Agent for Linux または Symantec Endpoint Protection for Linux クライアントのインストール.....	66
Linux エージェントを始めましょう.....	68
Symantec Endpoint Protection client for Linux の自動コンパイルについて.....	70
Linux クライアントの GUI について.....	71
リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール.....	71
Web リンクと電子メールを使った Symantec Endpoint Protection クライアントのインストール.....	73
管理サーバーのインストール後に実行するタスク.....	75
Symantec Endpoint Protection の通信ポート.....	77
管理サーバーとクライアントのインストールおよびアンインストール.....	81
ネットワークアーキテクチャの注意事項.....	81
データベースの種類の選択について.....	82
基本管理サーバー設定について.....	82
SQL Server の設定について.....	83
SQL Server データベースの認証モードについて.....	87

つの Symantec Endpoint Protection Manager のアンインストール.....	88
Symantec Endpoint Protection クライアントのインストールの管理.....	88
リモート配備用 Windows と Mac コンピュータの準備.....	89
クライアントのインストールの種類を使用してクラウドベースまたはローカルベースの定義をダウンロードするかどうかを選択.....	92
クライアント配備ウィザードを使ったクライアントのインストール方法の選択.....	93
クライアントにインストールするセキュリティ機能の選択.....	94
つの Symantec Endpoint Protection Manager でのカスタムの Windows クライアントインストールパッケージの作成.....	95
Windows クライアントのインストール設定について.....	95
クライアントインストールの設定をカスタマイズする.....	96
既存のセキュリティソフトウェアのアンインストール.....	96
Symantec Endpoint Protection クライアントのアンインストールについて.....	98
Endpoint Protection 14 でのサードパーティ製セキュリティソフトウェアの削除.....	99
Symantec Endpoint Protection 14.3 RU1 以降のサードパーティ製セキュリティソフトウェアの削除.....	99
つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動.....	101
管理下クライアントと管理外クライアントについて.....	103
管理外のクライアントインストールパッケージの取得方法.....	103
管理外 Windows クライアントのインストール.....	104
Symantec Endpoint Protection for Windows クライアントのアンインストール.....	105
Mac 用の Symantec Endpoint Protection クライアントのアンインストール.....	106
Symantec Agent for Linux または Symantec Endpoint Protection for Linux クライアントのアンインストール....	107
クライアントインストールパッケージの管理.....	108
クライアントインストールパッケージのエクスポート.....	108
つの Symantec Endpoint Protection Manager へのクライアントインストールパッケージのインポート.....	109
Windows クライアントインストールパッケージとコンテンツ更新のサイズ.....	110
Symantec Endpoint Protection (SEP) の最新リリースへのアップグレードおよび移行.....	112
Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象およびサポート非対象アップグレードパス.....	113
アップグレード前に つの Symantec Endpoint Protection Manager のディスクの空き容量を増加する.....	116
管理サーバーのアップグレード.....	117
埋め込みデータベースから Microsoft SQL Server Express データベースへのアップグレードに関するベストプラクティス.....	118
Microsoft SQL Server Express へのアップグレード前にデータベースがいっぱいになった場合のデータベースサイズの削減.....	119
Microsoft SQL Server データベースの FILESTREAM の有効化.....	120
Microsoft SQL Server Express へのアップグレード前にデータベースのサイズを 10 GB 未満に削減する.....	121
デフォルトの Microsoft SQL Server Express データベースにアップグレードするためにより多くのディスク容量を使用できるようにする.....	123
Symantec Endpoint Protection Manager と Microsoft SQL Server の間の暗号化通信の設定.....	124
複数の埋め込みデータベースと管理サーバーを使う環境のアップグレード.....	133

管理サーバーサービスの停止と開始.....	133
アップグレード中の複製の防止.....	134
クライアントソフトウェアをアップグレードする方法の選択.....	135
自動更新によるクライアントソフトウェアのアップグレード.....	136
他のグループへの自動更新設定の適用.....	138
Symantec Agent for Linux のアップグレード.....	139
グループ更新プロバイダの更新.....	139
Symantec Endpoint Protection のアップグレードに関するリソース.....	140
Symantec Endpoint Protection のライセンス交付.....	141
つの Symantec Endpoint Protection Manager のライセンス状態の調査.....	142
ライセンスファイルのバックアップおよび回復 (slf).....	142
データベースから使われなくなったクライアントをパージして使用可能なライセンスを増やす.....	143
Symantec Endpoint Protection ライセンスに含まれるものは?.....	143
複数年ライセンスについて.....	144
Symantec Endpoint Protection 製品ライセンス用語.....	145
管理外 Windows クライアントのライセンス交付.....	145
クライアントとサーバー間の接続の管理.....	147
管理サーバーおよびサーバークライアント接続の設定.....	147
つの Symantec Endpoint Protection Manager とクライアント間の HTTPS 通信の設定.....	148
ポートの可用性の検証.....	148
クライアントの通信のための Apache の HTTPS ポートの変更.....	149
HTTPS クライアント/サーバー通信の有効化.....	149
クライアントとサーバーのパフォーマンスの向上.....	151
サーバー証明書について.....	153
サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス.....	154
クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート.....	155
サーバー証明書の更新または復元.....	157
コンピュータの IP アドレスとホスト名を変更した後の Symantec Endpoint Protection Manager の再設定.....	158
クライアントが管理サーバーに接続され、保護されているかどうかの確認.....	160
Symantec Endpoint Protection クライアントの状態アイコン.....	161
ポリシーのシリアル番号を使ったクライアント/サーバーの通信の確認.....	161
プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新.....	162
クライアントコンピュータと管理サーバーの通信方法.....	164
クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法.....	165
[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元.....	167
クライアントとサーバーの通信ファイル (Sylink.xml) の手動によるエクスポート.....	167
Windows クライアントへのクライアントとサーバーの通信設定のインポート.....	168
Linux クライアントへのクライアントとサーバーの通信設定のインポート.....	169
IPv6 ネットワークサポート.....	169

グループ、クライアント、管理者、およびドメインの管理	171
クライアントのグループの管理	171
グループを構成する方法	172
グループの追加	172
Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート	173
ディレクトリサーバーからの組織単位のインポートについて	174
ディレクトリサーバーへの 1 つの Symantec Endpoint Protection Manager の接続	174
複製されたサイトのディレクトリサーバーへの接続	175
ディレクトリサーバーからの組織単位のインポート	176
グループの継承の無効化	176
グループへのクライアントコンピュータ追加の遮断	177
別のグループへのクライアントコンピュータの移動	177
クライアントコンピュータの管理	178
クライアントコンピュータの保護状態の表示	179
クライアントコンピュータでの保護の有効化	180
クライアントソフトウェアをインストールしていないクライアントの検索	180
クライアントコンピュータについての情報の検索	181
クライアントコンピュータで実行できるコマンドについて	182
コンソールからクライアントコンピュータにコマンドを実行する	184
クライアントが再起動しないようにする設定	184
Windows クライアントのユーザーモードとコンピュータモードの切り替え	185
管理外デバイスを検出するためのクライアントの設定	186
Symantec Endpoint Protection クライアントのパスワード保護	187
ユーザーによるクライアントのユーザーインターフェースの変更を防止、許可	188
ユーザー情報の収集	189
リモートクライアントの管理	190
リモートクライアントの場所の管理	191
クライアントの場所認識の有効化	192
グループへの場所の追加	193
デフォルトの場所の変更	194
ネットワーク検出条件の設定シナリオ 1	194
ネットワーク検出条件の設定シナリオ 2	196
場所に対する通信の設定	197
リモートクライアントのセキュリティポリシーの強化について	198
リモートクライアントのファイアウォールポリシー設定のベストプラクティス	198
リモートクライアントの通知の有効化について	199
管理サーバーからのリモートクライアントの監視について	199
クラウドコンソールからのローミング Symantec Endpoint Protection クライアントの監視	200
管理者アカウントの管理	201
管理者アカウントとアクセス権について	202

管理者アカウントの追加とアクセス権の設定.....	204
管理者アカウントの認証方法の選択.....	204
つの Symantec Endpoint Protection Manager での RSA SecurID 認証の使用.....	205
Symantec VIP を使用した 2 要素認証の設定.....	207
スマートカードでログオンする管理者を認証するように つの Symantec Endpoint Protection Manager を設定する.....	208
管理者アカウントのディレクトリサーバー認証のテスト.....	210
管理者アカウントまたはデフォルトデータベースのパスワードの変更.....	212
忘れた つの Symantec Endpoint Protection Manager パスワードのリセット.....	213
[パスワードを忘れた場合] リンクを表示して、管理者が紛失したパスワードをリセットできるようにする.....	215
無期限の つの Symantec Endpoint Protection Manager ログオンパスワードの有効化.....	215
つの Symantec Endpoint Protection Manager 用の自己署名されたサーバー証明書の受け入れについて.....	216
つの Symantec Endpoint Protection Manager コンソールへのログオン前に管理者が見るメッセージの表示.....	216
ログオン画面への [ユーザー名を記憶する] と [パスワードを記憶する] のチェックボックスの表示.....	216
リモート つの Symantec Endpoint Protection Manager コンソールのアクセスの認可または遮断.....	217
ログオン失敗回数が多すぎる管理者のアカウントのロック解除.....	218
つの Symantec Endpoint Protection Manager コンソールへのログオン状態を維持するためのタイムアウト期間の変更.....	218
ドメインについて.....	219
ドメインの追加.....	221
現在のドメインへの切り替え.....	221
ポリシーを使ったセキュリティの管理.....	223
すべてのポリシーに共通なタスクの実行.....	223
セキュリティポリシーの種類.....	224
クライアントポリシーの更新.....	226
ポリシーの追加.....	226
ポリシーの編集.....	227
[ポリシー] ページでのポリシーのコピーと貼り付け.....	228
[クライアント] ページでのポリシーのコピーと貼り付け.....	228
グループまたは場所へのポリシーの割り当て.....	229
ポリシーの置換.....	230
個々の Endpoint Protection ポリシーのエクスポートとインポート.....	230
共有ポリシーと非共有ポリシーについて.....	231
共有ポリシーの非共有ポリシーへの変換.....	232
グループまたは場所からのポリシーの割り当て解除.....	233
クライアントコンピュータの保護をユーザーが無効にできない設定.....	234
クライアントコンピュータで動作するアプリケーションとサービスの監視.....	237
アプリケーション学習の有効化.....	237
コンピュータで実行される学習済みアプリケーションに関する情報の検索.....	238

ファイアウォール保護の管理.....	240
ファイアウォールのしくみ.....	240
Symantec Endpoint Protection ファイアウォールについて.....	241
Mac クライアントのファイアウォールの設定について.....	242
ファイアウォールポリシーの作成.....	242
ファイアウォールルールの管理.....	244
新しいファイアウォールルールの追加.....	245
ファイアウォールのサーバールールとクライアントルールについて.....	246
ファイアウォールルール、ファイアウォール設定、侵入防止の処理順について.....	247
継承したファイアウォールルールについて.....	248
ファイアウォールルールの順序の変更.....	249
ファイアウォールでのステートフルインスペクションの使い方.....	250
ファイアウォールルールのアプリケーショントリガについて.....	251
ファイアウォールルールのホストトリガについて.....	254
ホストグループの追加.....	255
ファイアウォールルールのネットワークサービストリガについて.....	255
ファイアウォールルールのネットワークアダプタトリガについて.....	256
ファイアウォールルールのインポートとエクスポート.....	258
クライアント上でのファイアウォールルールのインポートまたはエクスポート.....	258
ファイアウォールルールのカスタマイズ.....	259
混合制御のファイアウォール設定.....	267
ルールの追加ではなくネットワークサービスのための通信の有効化.....	268
攻撃側コンピュータへの接続の自動遮断.....	268
潜在的な攻撃と詐称の試行の検出.....	269
コンピュータに対する外部からのステルス攻撃の防止.....	270
Windows ファイアウォールの無効化.....	270
侵入防止の管理.....	271
侵入防止の動作.....	273
Symantec IPS シグネチャについて.....	274
カスタム IPS シグネチャについて.....	275
ネットワーク侵入防止とブラウザの侵入防止の有効化.....	275
IPS シグネチャの例外の作成.....	276
除外するコンピュータのリストの作成.....	277
侵入防止とメモリエクスプロイト緩和機能のクライアント通知の設定.....	278
カスタム侵入防止シグネチャの管理.....	278
カスタム IPS ライブラリの作成.....	279
カスタム IPS ライブラリへのシグネチャの追加.....	280
カスタム IPS シグネチャの順序の変更.....	281
カスタム IPS シグネチャの変数の定義.....	282
複数のカスタム IPS ライブラリのグループへの割り当て.....	282

カスタム IPS シグネチャのテスト.....	283
メモリエクспロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化.....	283
Symantec Endpoint Protection メモリエクспロイト緩和機能の技術.....	287
クライアントコンピュータに対するウイルスとスパイウェアの攻撃の防止と処理.....	289
ウイルスとセキュリティリスクの除去.....	290
感染コンピュータとリスクを伴うコンピュータの識別.....	292
スキャン処理の確認と識別されたコンピュータの再スキャン.....	293
Windows クライアントがクラウドから定義を受け取る方法.....	293
クライアントコンピュータでのスキャンの管理.....	295
スキャンの種類とリアルタイム保護について.....	297
Auto-Protect の種類について.....	299
ウイルスとセキュリティリスクについて.....	300
Symantec Endpoint Protection がウイルススキャンとスパイウェアスキャンから除外するファイルとフォルダについて.....	302
デフォルトのウイルスとスパイウェアの対策ポリシーのスキャン設定について.....	304
Symantec Endpoint Protection がウイルスとセキュリティリスクの検出を処理する方法.....	306
Windows 8 コンピュータでの検出に対する Symantec Endpoint Protection の処理方式.....	307
Windows コンピュータで実行される定時スキャンの設定.....	308
Mac コンピュータで実行される定時スキャンの設定.....	309
Linux コンピュータで実行する定時スキャンの設定.....	310
クライアントコンピュータでのオンデマンドスキャンの実行.....	311
スキャンの調整によるクライアントコンピュータパフォーマンスの改善.....	312
スキャンの調整によるクライアントコンピュータでの保護の強化.....	313
ダウンロードインサイト検出の管理.....	315
Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法.....	317
Symantec Endpoint Protection が高度な機械学習を使用する仕組み.....	318
Symantec Endpoint Protection のエミュレータがマルウェアを検出およびクリーニングする方法.....	320
Windows クライアント用の検疫の管理.....	321
クライアントコンピュータにある検疫ファイルのリスクログを使った削除.....	323
クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理.....	323
Windows 8 クライアントで表示されるポップアップ通知について.....	325
Windows 8 クライアントで表示される Symantec Endpoint Protection のポップアップ通知の有効化または無効化.....	325
早期起動マルウェア対策 (ELAM) の検出の管理.....	326
Symantec Endpoint Protection の早期起動マルウェア対策 (ELAM) のオプションの調整.....	327
クエリーの評価に専用インサイトサーバーを使うようにサイトを設定する.....	327
評価のクエリーおよび提出に専用サーバーを使うクライアントグループの設定.....	328
ウイルススキャンとスパイウェアスキャンのカスタマイズ.....	329
Mac コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ.....	331

Linux コンピュータで実行するウイルススキャンとスパイウェアスキャンのカスタマイズ.....	332
Windows クライアントの Auto-Protect のカスタマイズ.....	332
Mac クライアントの Auto-Protect のカスタマイズ.....	333
Linux クライアントの Auto-Protect のカスタマイズ.....	334
Windows コンピュータで実行する電子メールスキャンの Auto-Protect のカスタマイズ.....	335
Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ.....	336
Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ.....	337
Linux コンピュータで実行するクライアントに対する管理者定義のスキャンのカスタマイズ.....	338
スキャンのランダム化による Windows クライアントの仮想化環境でのコンピュータパフォーマンスの向上.....	339
Windows クライアントのグローバルなスキャン設定の修正.....	339
Windows コンピュータのログ処理と通知設定の修正.....	340
Linux コンピュータでのログ処理設定の修正.....	340
ダウンロードインサイトの設定のカスタマイズ.....	341
検出を行ったときに Symantec Endpoint Protection が実行する処理の変更.....	341
Windows コンピュータでのユーザーによるスキャンの進行状況の表示とスキャンの操作の許可.....	343
Symantec Endpoint Protection クライアントと連携する Windows セキュリティセンターの通知の設定.....	344
Symantec Endpoint Protection 遠隔測定データを提出してセキュリティを向上させる.....	345
サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について.....	354
クライアントがシマンテック社に送信する匿名または非匿名のデータの管理.....	356
Symantec Endpoint Protection で、クライアントの提出がネットワーク帯域幅に与える影響を最小化する方法.....	357
クライアントの提出と他の外部通信のためのプロキシサーバーの指定.....	357
SONAR の管理.....	358
SONAR について.....	359
SONAR の誤検知の検出の処理と防止.....	360
クライアントコンピュータでの SONAR 設定の調整.....	361
SONAR 検出結果の監視による誤認のチェック.....	362
改変対策の設定の変更.....	363
アプリケーション制御、システムロックダウン、デバイス制御について.....	363
アプリケーション制御の設定.....	364
デフォルトのアプリケーションルールの有効化とテスト.....	365
アプリケーション制御とデバイス制御ポリシーの構造.....	366
アプリケーション制御へのカスタムルールの追加.....	367
アプリケーション制御ルールの追加のベストプラクティス.....	369
ルールに使う条件を選択するためのベストプラクティス.....	371
アプリケーション制御ルールのテスト.....	372
システムロックダウンの設定.....	373
checksum.exe を使ったファイルフィンガープリントリストの作成.....	377
つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ.....	378

つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストの手動更新.....	379
システムロックダウンと Symantec EDR 拒否リスト (ブラックリスト) ルールとの対話.....	380
システムロックダウン設定にインポートするアプリケーション名リストの作成.....	381
システムロックダウン用に許可または遮断するファイルフィンガープリントリストの自動更新.....	382
システムロックダウンを有効化する前の、システムロックダウンの設定とテスト.....	384
許可モードでのシステムロックダウンの実行.....	386
拒否モードでのシステムロックダウンの実行.....	387
デバイス制御の管理.....	388
クライアントコンピュータのデバイスの許可または遮断.....	389
ハードウェアデバイスのリストについて.....	390
DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得.....	390
ハードウェアデバイスリストへのハードウェアデバイスの追加.....	392
Symantec Endpoint Protection の例外の管理.....	392
使用する Windows 例外と、適用するスキャンの種類について.....	393
ウイルスとスパイウェアのスキャンの例外作成.....	394
スキャンからのファイルまたはフォルダの除外.....	396
Windows クライアントのウイルススキャンとスパイウェアスキャンから既知のリスクを除外する.....	398
Windows クライアントと Linux クライアントのウイルススキャンとスパイウェアスキャンからファイル拡張子を除外する.....	398
Windows クライアントのアプリケーションの例外を作成するためのアプリケーションの監視.....	399
Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定する.....	399
Windows クライアントのスキャンからの信頼できる Web ドメインの除外.....	400
Windows クライアントの改変対策例外の作成.....	401
DNS またはホストファイルを変更するアプリケーションのための例外の作成.....	402
Windows クライアントのスキャンからの証明書の除外.....	402
クライアントコンピュータでユーザーが設定できる例外の種類の制限.....	403
ログイベントに基づく例外の作成.....	403
Web とクラウドのアクセス保護 の設定.....	405
Web とクラウドのアクセス保護 とは.....	407
クライアント上で Web とクラウドのアクセス保護 のトンネル方式が有効であり接続されていることの確認....	410
ブラウザでの Web とクラウドのアクセス保護 ポリシーのテスト.....	412
Web とクラウドのアクセス保護 for the Mac クライアントについて.....	414
Web とクラウドのアクセス保護 設定.....	414
つの Symantec Endpoint Protection Manager ポリシーのテスト.....	416
ウイルスとスパイウェアの対策ポリシーのテスト.....	417
クライアントコンピュータでの処理の開始の遮断.....	417
ユーザーがクライアントコンピュータのレジストリに書き込めないようにする.....	418
ユーザーが特定のファイルに書き込めないようにする.....	419
DLLを遮断するルールの追加とテスト.....	420

処理を終了するルールの追加とテスト.....	421
デフォルト IPS ポリシーのテスト.....	421
クライアント上のコンテンツと定義を更新する方法.....	423
クライアント上のコンテンツを更新するための配布方法の選択.....	424
プラットフォームに基づきクライアント上のコンテンツを更新するための配布方法の選択.....	427
LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード.....	428
つの Symantec Endpoint Protection Manager に最新のコンテンツが含まれていることの確認.....	431
LiveUpdate がダウンロードするコンテンツの種類について.....	432
社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定.....	437
外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定.....	439
インターネットにアクセスして Symantec LiveUpdate からコンテンツをダウンロードするためにプロキシサーバーに接続する つの Symantec Endpoint Protection Manager の設定.....	439
クライアントが Symantec LiveUpdate または社内 LiveUpdate サーバーへの通信に使うプロキシサーバーの指定.....	440
クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定.....	440
ユーザーが LiveUpdate に対して持つ制御権限の設定.....	442
クライアント更新要求のネットワーク過負荷の軽減.....	442
同時コンテンツダウンロードのランダム化について.....	443
デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化.....	444
LiveUpdate サーバーからのコンテンツダウンロードのランダム化.....	444
Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行する設定.....	445
定義が古いときや Windows コンピュータが切断されていたときに実行するクライアント更新の設定.....	446
つの Symantec Endpoint Protection Manager からコンテンツをダウンロードするためのクライアントの設定.....	446
Windows クライアントでリリースする前のエンジン更新のテスト.....	446
Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す.....	449
クライアントにコンテンツを配布するためのグループ更新プロバイダの使用.....	450
グループ更新プロバイダの種類について.....	451
GUP からコンテンツをダウンロードするためのクライアントの設定.....	452
グループ更新プロバイダとして機能するクライアントの検索.....	453
ネットワーク内に 2 種類以上のグループ更新プロバイダを設定した場合の影響について.....	454
Intelligent Updater ファイルを使用した Symantec Endpoint Protection クライアントのコンテンツの更新.....	455
サードパーティの配布ツールを使ったクライアントコンピュータの更新.....	456
管理下クライアントへのサードパーティのコンテンツ配布を許可する LiveUpdate 設定ポリシーの設定.....	457
サードパーティの配布ツールから更新を受信するための管理外クライアントの準備.....	458
サードパーティの配布ツールを使ったコンテンツの配布.....	459
Windows クライアントへの Endpoint Protection クライアント パッチのインストール.....	461
コンプライアンスの監視、レポート、エンフォース.....	463
ホストインテグリティの設定.....	463
ホストインテグリティの仕組み.....	464
ホストインテグリティ必要条件について.....	465

ホストインテグリティポリシーへの事前定義済み必要条件の追加.....	466
事前定義済みのホストインテグリティ必要条件の修復の設定.....	466
ユーザーによるホストインテグリティ修復の延期または中止の許可.....	467
ホストインテグリティ検査の頻度の設定.....	468
必要条件失敗時のホストインテグリティ検査の成功許可.....	468
ホストインテグリティ検査の通知の設定.....	469
失敗したホストインテグリティ検査のための検疫ポリシーの作成.....	469
ピアツーピア認証の設定によるリモートコンピュータの遮断.....	470
テンプレートのカスタム必要条件の追加.....	471
カスタマイズした必要条件スクリプトの記述.....	472
レジストリの条件について.....	473
クライアントでスクリプトを実行するカスタム必要条件の記述.....	473
ファイルのタイムスタンプを設定するカスタム必要条件の記述.....	474
レジストリ DWORD 値を増分するカスタム必要条件を記述する.....	475
カスタム必要条件スクリプトを使ったテスト用ホストインテグリティポリシーの作成.....	476
エンドポイント保護の監視.....	477
スキャンしていないコンピュータの検索.....	480
オフラインコンピュータの検索.....	480
ネットワーク内でインストールされている Symantec Endpoint Protection バージョンのリストの作成.....	480
クライアントの配備の状態についてのレポートの実行.....	481
リスクの表示.....	481
攻撃の標的と攻撃元の表示.....	482
日次または週次の状態レポートの表示.....	483
システム保護の表示.....	483
レポートの環境設定.....	483
スタンドアロン Web ブラウザからのレポートへのログオン.....	484
つの Symantec Endpoint Protection Manager のレポートの種類について.....	485
クイックレポートの実行とカスタマイズ.....	492
カスタムレポートの保存.....	494
定時レポートの実行方法.....	494
定時レポートに使うフィルタの編集.....	495
レポートの印刷と保存.....	496
ログの表示.....	496
つの Symantec Endpoint Protection Manager のログの種類について.....	497
フィルタを使ったカスタムログの保存と削除.....	499
別のサイトのログの表示.....	500
ログデータの Syslog サーバーへのエクスポート.....	501
ログデータのテキストファイルへのエクスポート.....	501
外部ログ記録用フェールオーバーサーバーの設定.....	503
通知の管理.....	503

通知のしくみ.....	504
通知の種類および通知が送信される場合.....	504
パートナー通知について.....	507
管理サーバーと電子メールサーバー間の通信の確立.....	508
通知の表示と対応.....	508
管理通知フィルタの保存と削除.....	509
管理者通知の設定.....	509
別のバージョンからのアップグレードが通知条件に与える影響.....	510
管理サーバー、サイト、およびデータベースの管理.....	512
Symantec Endpoint Protection サーバーの種類について.....	512
サーバーの設定のエクスポートとインポート.....	512
つの Symantec Endpoint Protection Manager サーバーとサードパーティサーバーの管理.....	513
データベースの保守.....	514
データベースの自動バックアップの実行.....	517
自動データベース保守タスクのスケジュール設定.....	517
Microsoft SQL Server データベースのファイルサイズの拡大.....	518
クライアントログサイズと管理サーバーにアップロードするログの指定.....	518
ログサイズとデータベース内でのログエントリの保存期間の指定.....	519
クライアントログデータ用にサーバーのディスク領域を拡大することについて.....	519
データベースからのログデータの手動の消去.....	520
フェールオーバーと負荷分散の設定.....	520
フェールオーバーと負荷分散について.....	521
負荷分散のための管理サーバーリストの設定.....	523
フェールオーバーまたは負荷分散に使う管理サーバーのインストール.....	523
グループと場所への管理サーバーリストの割り当て.....	524
サイトと複製の設定.....	525
サイトの概要と複製の仕組み.....	526
複製中に生じたサイト間のデータ競合を解決する方法.....	528
複数サイトと複製を設定するかどうか.....	529
必要なサイト数の決定.....	530
複製のための 2 番目のサイトのインストール方法.....	531
即座に実行されるデータの複製.....	532
サイトの削除.....	532
Endpoint Protection のディザスタリカバリのベストプラクティス.....	533
データベースとログのバックアップ.....	534
サーバー証明書のバックアップ.....	535
つの Symantec Endpoint Protection Manager の再インストールまたは再設定.....	536
新しいサーバー証明書の生成.....	537
データベースの復元.....	538

Symantec Endpoint Security クラウド コンソールからのクライアントおよびポリシーの管理.....	540
オンプレミス管理、ハイブリッド管理、またはクラウドのみ管理オプションの選択.....	540
クラウドコンソールへの Symantec Endpoint Protection Manager ドメインの登録.....	542
つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録した後の処理.....	545
ハイブリッド管理の つの Symantec Endpoint Protection Manager と Symantec Endpoint Security クラウドコンソールの連携方法.....	546
14.x つの Symantec Endpoint Protection Manager ドメインに登録されたクラウドコンソールの機能とオンプレミス 一つの Symantec Endpoint Protection Manager の比較.....	550
一つの Symantec Endpoint Protection Manager 例外ポリシーとクラウドコンソールの連携方法について.....	553
クラウドコンソールで複製パートナーとして設定するサイトの登録.....	556
低帯域幅環境でのクライアントのアップデート.....	558
クラウドコンソールから 一つの Symantec Endpoint Protection Manager ドメインを登録解除する.....	559
Symantec Endpoint Protection の仮想インフラストラクチャでの使用.....	561
共有インサイトキャッシュについて.....	561
仮想イメージ例外ツールについて.....	562
ネットワークベースの共有インサイトキャッシュを使用するために必要な準備.....	562
ネットワークベースの共有インサイトキャッシュを実装するためのシステム必要条件.....	563
ネットワークベースの共有インサイトキャッシュのインストールとアンインストール.....	563
ネットワークベースの共有インサイトキャッシュの使用の有効化.....	564
共有インサイトキャッシュ設定のカスタマイズ.....	565
ネットワークベースの共有インサイトキャッシュサービスの停止と開始について.....	568
ネットワークベースの共有インサイトキャッシュのログイベント.....	568
ネットワークベースの共有インサイトキャッシュパフォーマンスカウンタの監視.....	569
共有インサイトキャッシュのトラブルシューティング.....	570
基本イメージへの Virtual Image Exception ツールの使用.....	570
仮想イメージ例外ツールのシステム必要条件.....	571
仮想イメージ例外ツールの実行.....	571
基本イメージファイルのスキャンをバイパスするための Symantec Endpoint Protection の設定.....	572
非永続的な仮想デスクトップインフラストラクチャでの Symantec Endpoint Protection の使用.....	572
VDI で非永続的なゲスト仮想マシンの基本イメージの設定.....	572
ライセンスを開放するための使われなくなった非永続的 VDI クライアントのページ.....	573
非永続的 VDI クライアントのライセンス数の管理方法.....	574
viertools	574
viertools	574
Symantec Endpoint Protection のトラブルシューティング.....	576
SEP および SES がシマンテック社のサーバーへ接続するために許可する (ホワイトリストに登録する) URL	577
Symantec Diagnostic Tool (SymDiag) を使ったコンピュータの問題のトラブルシューティング.....	577
クライアントインストールに失敗した場所の識別.....	577

つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング	578
クライアントコンピュータの管理サーバーへの接続のチェック	579
トラブルシューティングファイルを使った保護の問題の調査	579
クライアントが管理サーバーに接続しているかどうかを確認するためのアクセスログの有効化と表示	579
Apache Web サーバーの停止と開始	580
ping コマンドを使用した管理サーバーへの接続性のテスト	580
ブラウザを使用した、つの Symantec Endpoint Protection Manager クライアントでの Symantec Endpoint Protection への接続テスト	581
クライアントコンピュータのデバッグログのチェック	581
管理サーバーの受信ボックスログのチェック	582
SylinkDrop ツールを使ったクライアントとサーバー間の通信設定の復元	582
Symantec Agent for Linux のトラブルシューティング	583
つの Symantec Endpoint Protection Manager とコンソールまたはデフォルトデータベースの間における通信の問題のトラブルシューティング	584
管理サーバーのデータベースとの接続の検証	585
クライアント/サーバーの通信のファイル	587
レポートに関する問題のトラブルシューティング	587
レポートとログを見直すためのタイムアウトパラメータの変更	588
ループバックアドレスの使用が無効になっている場合のレポートページへのアクセス	589
つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知るべきこと	590
つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク	592
つの Symantec Endpoint Protection Manager からの Power Eraser の分析の開始;	594
Power Eraser の検出の対処	595
付録	597
プラットフォームに基づく Symantec Endpoint Protection の機能	597
Windows クライアント用の Symantec Endpoint Protection 機能の依存関係	607
Symantec Endpoint Protection に含まれるツール	609
Symantec Endpoint Protection と Symantec Endpoint Security での Windows クライアントサービス smc のコマンド	615
smc.exe コマンドエラーコード	621
サードパーティツールを使った Windows クライアントソフトウェアのインストール	622
クライアントインストール機能とプロパティについて	623
MSI コマンド文字列の設定について	623
setaid.ini の設定について	623
Symantec Endpoint Protection クライアントのコマンドラインインストールプロパティ	624
コマンドラインを使った Symantec Endpoint Protection クライアント機能のインストール	625
Windows インストーラのパラメータ	626
Windows セキュリティセンターのプロパティ	627
Windows クライアントをインストールする場合のコマンドラインの例	628

Microsoft SCCM/SMS を使った Windows クライアントのインストール.....	629
Active Directory Group Policy Object (GPO) を使った Windows クライアントのインストール.....	630
組織単位にコンピュータを追加してソフトウェアをインストールする	630
Sylink.xml ファイルをコピーして管理下インストールパッケージにする	631
Active Directory Group Policy Object を使ったクライアントソフトウェアのアンインストール.....	632
著作権に関する声明.....	633

リリースノート

システム要件、サポートされているアップグレードパス、既知の問題、および詳細情報へのリンクが含まれます

Symantec Endpoint Protection をインストールまたはアップグレードする前に、あるいはテクニカルサポートに連絡する前に、リリースノートを確認してください。リリースノートには、インストールの変更、アップグレードの問題、既知の問題と回避策が掲載されています。

Symantec Endpoint Protection 14.3 RU2 の新機能

このセクションでは、このリリースの新機能を説明します。

保護機能

- マルウェア対策スキャンインターフェース (AMSI) との拡張された統合により Windows Management Instrumentation (WMI) を使用して、悪質な Excel マクロ (XLM) やペイロードなどのファイルレス脅威に対するランタイム保護が含まれています。
- 強化された動作の検出と防止は、Ryuk や Netwalker などのランサムウェア ファミリから保護し、動作の検出を改善し、悪質な変更やユーザ ファイルの削除を防止します。
- Symantec Endpoint Protection クライアントのエミュレータが機能拡張され、LemonDuck などの暗号通貨マイニング マルウェア ファミリの検出が増加しました。
- ブラウザ拡張機能は、Google Chrome Web ブラウザで送受信する HTTP トラフィックと HTTPS トラフィックの両方の保護を高めます。Symantec Endpoint Protection クライアントはユーザが悪質なサイトにアクセスするのをブロックし、ユーザをデフォルトのランディングページにリダイレクトします。ブラウザ拡張は IPS によって異なるため、IPS ポリシーを有効にしてグループに割り当てる必要があります。コンピュータが Active Directory ドメインに参加した場合、ブラウザ拡張はデフォルトで LiveUpdate からダウンロードされます。それ以外の場合、ブラウザ拡張機能は Google ウェブ ストアからダウンロードします。このコンテンツを有効または無効にするには、[管理] > [サーバ] > [サイト プロパティの編集] > [LiveUpdate] タブ > [ダウンロードするコンテンツの種類] > [ブラウザ機能拡張] をクリックします。

デフォルトで、Symantec Endpoint Protection インストーラは Google Chrome ブラウザ機能拡張をインストールします。ただし、Active Directory グループ ポリシー オブジェクトを使用して Chrome 拡張機能を管理する場合は、リストにブラウザ機能拡張を追加する必要があります。参照: [グループ ポリシー オブジェクトを使用した Endpoint Protection の Chrome ブラウザ拡張機能のインストール](#)

[LiveUpdate がダウンロードするコンテンツの種類について](#)

- 管理者が Symantec Endpoint Protection Manager コンソールからリモート SEP クライアントの検疫ファイルを取得できる機能。これらの悪質なファイルは、さらなる調査やサンドボックス処理に使用できます。検疫ファイルをアップロードするには、[管理] > [ドメイン] > [ドメイン プロパティの編集] > [全般] タブ > [クライアントから検疫ファイルをアップロードする] オプションにチェックを付けます。このオプションは、すべての検疫ファイルをクライアントから自動的にアップロードします。次に、[クライアントが検疫したファイルをダウンロード] コマンドを使用して、リスク ログから個別ファイルを選択して取り込みます。管理サーバは古いバージョンの中央検疫サーバをサポートしなくなったため、[ウイルスとスパイウェアの対策ポリシー] > [検疫] > [検疫項目] オプションは削除されました。

[Windows クライアント用の検疫の管理](#)

- 侵入防止 (IPS) コンテンツが大幅に最適化され、コンテンツサイズが削減し、ネットワークのスループットが向上しました。この改善は、サポートされるすべての Symantec Endpoint Protection バージョンで利用できます。
- Network Traffic Redirection は、Symantec Endpoint Protection Manager、Windows クライアント、Mac クライアントで、Web とクラウドのアクセス保護に名前が変更されました。クライアントで、ユーザは [Web とクラウドのアクセス保護] > [オプション] メニューで [再接続] ボタンをクリックできます。クライアント ユーザは、クライアントが Symantec WSS との接続が切断されたことを検出しない場合にこのオプションを使用する必要があります。

[Web とクラウドのアクセス保護の設定](#)

Symantec Endpoint Protection Manager

- 重要な修正とセキュリティ更新の自動 LiveUpdate が含まれます。SEP 14.3 RU2 から、重要なパッチとセキュリティ修正が LiveUpdate 経由でクライアントに自動的に配信され、エージェントの更新管理の負担が軽減されます。これらのパッチには重要な修正のみが含まれます。新機能は、リリース更新 (RU) 経由で個別に提供されます。クライアント パッチとクライアント製品の更新を LiveUpdate サーバから Symantec Endpoint Protection Manager にダウンロードされていることを確認するには、[サイトプロパティ] に移動して [クライアント パッチ] と [クライアント製品の更新] を選択します。このオプションはデフォルトで有効になっています。

LiveUpdate から Symantec Endpoint Protection Manager へのコンテンツのダウンロード

- Symantec Endpoint Protection Manager からクライアントにクライアント パッチをダウンロードするには、[LiveUpdate 設定ポリシー] で [拡張設定] > [クライアント パッチのダウンロード] をクリックします。LiveUpdate ポリシーは、他のコンテンツと同様にクライアントにクライアント パッチをダウンロードします。クライアント パッチは増分デルタ ファイルです。

Windows クライアントへの Endpoint Protection クライアント パッチのインストール

- 製品の更新をダウンロードするには、[利用可能な場合は LiveUpdate サーバからデルタ コンテンツをダウンロードする] を選択します。Symantec Endpoint Protection Manager に完全なコンテンツしかない場合、クライアントは LiveUpdate から少量のコンテンツを取得しようとします。クライアント パッチを有効にしない場合は、このオプションを使います。製品の更新オプションを使うと、パッチ ビルドが自動更新で確実に利用可能になります。LiveUpdate は完全なクライアント インストール パッケージを管理サーバにダウンロードします。パッケージは、[管理] > [インストール パッケージ] > [クライアント インストール パッケージ] テーブルと、自動更新ウィザードに表示されます。このオプションはデフォルトで有効になっています。クライアントのバージョンが変更することなく、ビルド番号のみ変更されます。このオプションを使うと、管理サーバに完全なコンテンツのみがある場合に、クライアントが LiveUpdate から小さいコンテンツを受信できます。

自動更新によるクライアントソフトウェアのアップグレード

- 以前のリリースでは、これらのオプションは、[クライアント セキュリティ パッチのダウンロード] と [利用可能な場合に LiveUpdate サーバからクライアント パッチの小さいコンテンツをダウンロードする] というものでした。[サイトプロパティ] > [LiveUpdate] タブ > [ダウンロードするコンテンツの種類] > [クライアント パッチ] オプションは、[クライアント セキュリティ パッチ] でした。
- 管理サーバ設定ウィザードで、SQL Server FILESTREAM が有効になっているかどうかを確認するための資格情報の入力を求められることがなくなりました。埋め込みデータベース (14.3 以前) からアップグレードすると、FILESTREAM が自動的に有効になります。14.3 RU1/RU1 MP1 からのアップグレードは、既存の FILESTREAM 設定が維持されます。SQL Server Express データベースで FILESTREAM が有効になっていない場合にのみ、ウィザードは資格情報の入力を求めます。

Microsoft SQL Server データベースの FILESTREAM の有効化

- Symantec Endpoint Protection クライアントと Symantec Endpoint Protection Manager の両方は、英語、フランス語、スペイン語、ポルトガル語、日本語の 5 つの言語にのみローカライズされています。サポート対象の 5 つの言語のいずれかを使用している場合は、操作は不要です。通常通りアップグレードできます。以前のクライアントの言語が利用できない場合、クライアントの言語を自動的に英語にアップグレードできます。英語を選択しない場合、サポート対象外の言語のクライアントはアップグレードされません。このオプションはデフォルトではオフになっています。このオプションを有効にするには、[クライアント] ページ > [インストール パッケージ] ページをクリックし、[クライアント インストール パッケージの追加] > [サポートされていない言語が利用できない場合は英語にアップグレードする] をクリックします。このオプションは Windows クライアントにのみ適用されます。

Symantec Endpoint Protection 14.3 RU2+ のサポート対象言語へのアップグレード

- 場所の認識には、コンピュータのホスト名、ユーザとグループ名、オペレーティング システム、クライアントで特定のファイルが実行されるかどうかという 4 つの新しい基準があります。

グループへの場所の追加

- SEPM REST API にアクセスするための権限レベルが追加されました。以前は、システム管理者のみがすべての POST 操作を実行することができました。現在、ドメイン管理者と限定管理者は API を使ってコンピュータの状態を監視できます。SOC アナリストは、サードパーティ ツールを使用して API と統合できます。
- [管理] ページ > [管理者] > [アクセス権] タブの、[共有ポリシーの編集を許可する] コマンドは、[共有ポリシーの編集を許可しない] から変更されました。[共有ポリシーの編集を許可しない] チェックボックスはデフォルト

トで選択されていなかったため、管理者が明示的に権限を拒否するのではなく、明示的に権限を付与するようになっていました。

- 次のサードパーティ コンポーネントがアップグレードまたは追加されました： Apache Commons FileUpload、jQuery、zip 拡張子が有効な PHP、Microsoft Drivers for PHP for Microsoft SQL Server、OpenSSL。

クライアントおよびプラットフォームの更新

Windows クライアント:

- Windows 用 Symantec Endpoint Protection クライアントは、Citrix Studio バージョン 2009.0.0 および Nutanix AOS 5.15 (LTS) をサポートしています。

Mac クライアント:

- Symantec Endpoint Protection Manager 14.3 RU2 には、Mac 用 Symantec Endpoint Protection クライアント 14.3 RU1 MP1 の最新リリースが付属しています。Mac クライアント 14.3 RU2 が利用可能になると、LiveUpdate は Mac クライアント インストール パッケージを Symantec Endpoint Protection Manager の [管理者] > [インストール パッケージ] > [クライアント インストール パッケージ] ページにダウンロードします。[監視] ページに [新しいソフトウェア パッケージ] の通知を追加した場合、インストール パッケージの準備が完了すると通知が送信されます。この機能により、すぐに最新の Symantec Endpoint Protection Manager にアップグレードできます。

NOTE

Mac 用 Symantec Endpoint Protection クライアントのリリースは、2021 年 6 月に予定されています。

- Mac クライアントが利用可能になると、以下の機能が含まれます。
 - Apple M1 チップを搭載したデバイスのサポート。
 - AppleScript と Mac クライアントの統合により、AppleScript スクリプトを作成して実行し、Mac クライアントのクエリまたは制御を行うことができます。
 - Mac クライアント インストール パッケージには、Mac デバイスから Mac クライアントの NLOK ビルド (バージョン 14.3 以前) を削除し、それ以降のバージョンの Mac クライアントにサイレントにアップグレードできるツールが含まれます。
 - Mac クライアントのパフォーマンスの改善には、Mac クライアント使用時のネットワーク スループットの向上、クライアント インストーラのサイズの削減、CPU とメモリ使用率の最適化が含まれます。
 - 侵入の痕跡検索と修復用検疫ファイルコマンドのサポート。これらの機能は、Symantec Endpoint Security クラウド コンソールまたはバージョン 4.6.5 以降の Symantec EDR で管理されているクライアントでサポートされます。

Linux クライアント

- Linux 用 Symantec Endpoint Protection クライアントは、Debian 9 および Debian 10 をサポートします。
- Linux 用 Symantec Endpoint Protection クライアントのコマンドライン ツール (sav) を使うと、Linux クライアントを制御および確認できます。

[Linux クライアントへのクライアントとサーバーの通信設定のインポート](#)

削除済みの機能

- 12.1.x の延長サポート期間は 2021 年 4 月 3 日に終了しました。
[Endpoint Protection 12.1 のサポート終了](#)
- 管理サーバは古いバージョンの中央検疫サーバをサポートしなくなりました。[ウィルスとスパイウェアの対策ポリシー] > [検疫] > [検疫項目] ページのオプションは削除されました。

マニュアル

- Windows クライアント ヘルプ ファイルは HTML5 ファイルに変換され、最新の形式と Broadcom カラーが表示されるようになりました。
- 以下のページで、各リリースのリリース ノートの PDF ファイルをダウンロードできます。

[関連ドキュメント](#)

データベーススキーマ

データベーススキーマには以下の変更があります。

テーブル	列の変更
HPP_APPLICATION	NONPE 列が追加されました。
新しいテーブル REQUESTED_FILES の追加	以下の列が追加されました。 • ID • APP_HASH • COMMAND_ID • BINARY_FILE_ID • TIME_STAMP • USN • RETRY_COUNT • DELETED

[Symantec Endpoint Protection のすべてのリリースの新機能](#)

Symantec Endpoint Protection (SEP) の既知の問題と回避策

このセクションの項目は、このリリースの Symantec Endpoint Protection に該当します。

Table 1: アップグレードの問題

問題	説明と解決策
「Symantec Endpoint Protection バージョン 14.3 RU2 for Win64bit は最新のパッケージです。削除できません。」というエラー メッセージが表示される。[14.3 RU2]	Symantec Endpoint Protection Manager に複数のビルドのパッケージが表示された場合、クライアント インストール パッケージを削除できません。14.3 RU2 以降、LiveUpdate はビルド番号が異なる複数のクライアント インストール パッケージをダウンロードできます。これは、[管理] ページ > [インストール パッケージ] > [クライアント インストール パッケージ] のテーブルに表示されます。[SEP-72531]
14.3 RU2 の [現在インストールされている言語がサポートされていない場合は英語にアップグレードする] オプションを使用して、サポート対象外の言語のクライアントを英語にアップグレードする場合、自動更新に失敗する。[14.3 RU2]	この状況は、14.3 RU1 MP1 以前で、サポート対象言語からサポート対象外言語に手動でアップグレードしたクライアント (チェコ語のクライアントを日本語のオペレーティングシステムで日本語にアップグレードする、など) で発生します。そして、[現在インストールされている言語がサポートされていない場合は英語にアップグレードする] オプションを使用して、14.3 RU2 でサポート対象外の言語を英語にアップグレードします。[SEP-72490] この問題は、クライアント言語がサポートされているオペレーティングシステムの言語 (この場合は日本語) を使っている場合に発生します。自動更新は英語ではなくサポート対象言語を使います。 この問題を回避するには、自動更新を再試行し、[現在インストールされている言語がサポートされていない場合は英語にアップグレードする] オプションをオフにします。
14.3 RU2 Symantec Endpoint Protection Manager (SEPM) からクライアント インストール パッケージをエクスポートするときに、「クライアント インストール パッケージにコンテンツが含まれていません。」という警告メッセージが表示される。	これは、パッケージのエクスポートに使用している Symantec Endpoint Protection Manager とコンソール間の通信が中断された場合に発生します。 Endpoint Protection Manager からインストール パッケージをエクスポートするときに、「クライアント インストール パッケージにコンテンツが含まれていません。」という警告メッセージが表示される。
最新のクライアント インストール パッケージを古いバージョンの Symantec Endpoint Protection Manager にインポートするとエラーが表示される。[14.3 RU2]	Symantec Endpoint Protection 14.3 RU2 クライアントは、14.3 RU1 MP1 以前の Symantec Endpoint Protection Manager では管理できません。[SEP-72292]

問題	説明と解決策
つの Symantec Endpoint Protection Manager のダーク ネットワークでは、LiveUpdate がアップグレード中に実行しないので、古いクライアント侵入検出システム (CIDS) コンテンツを新しいクライアントにダウンロードする [14.3 RU1]	14.3 RU1 Symantec Endpoint Protection Manager がインターネットまたは LiveUpdate Administrator (LUA) サーバにアクセスできない場合、古い互換性のないコンテンツをキャッシュに保持します。この古いコンテンツは通常、新しいクライアントに配信されます。管理サーバのキャッシュのコンテンツを更新するには、認証済みウイルス定義と CIDS .jdb ファイルを手動でダウンロードします。[SEP-69125] 新しいクライアントが古いコンテンツを取得しないようにするには、新しいクライアントをインストールする前、または古いクライアントをアップグレードする前に、CIDS .jdb ファイルを SEPM に手動でインストールします。 .jdb ファイルをダウンロードして Endpoint Protection Manager の定義を更新する
ネットワーク インターフェイス カードが無効な場合、Symantec Endpoint Protection Manager (SEPM) にログインできません [14.3 RU1]	Symantec Endpoint Protection Manager をインストールした後、コンソールにログインできず、次のエラー メッセージが表示されます。 ##### この問題は、SEPM をインストールしたときにコンピュータのネットワーク インターフェイス カードが無効になっている場合に発生する可能性があります。これによりサーバ証明書が生成されなくなります。[SEP-67040] SEPM が無効なネットワーク インターフェイス カードでインストールされたかどうかを調べるには、サーバ証明書を確認します。 NIC が有効になっていないサーバにインストールされた場合、SEPM ログイン時に予期しないサーバ エラーが発生する
SEPM をアンインストールし、オプションを使用してデフォルトのデータベースを削除して SQL Server Express インスタンスを残すと、「##### ##### # 」というエラーが表示される [14.3 RU1]	Symantec Endpoint Protection Manager をアンインストールし、[DB のみを削除して SEPM とインストールされた SQL Server Express インスタンスを残す] オプションを選択すると、「##### ##### # 」というエラーが表示される場合があります。この問題は、デフォルト ユーザ DBA の認証情報を追加した後に発生し、ユーザ権限に関連している可能性があります。[SEP-68670] この問題を回避するには、SEPM setup.exe ファイルを実行してアンインストールし、アンインストール中に [DB のみを削除して SEPM とインストールされた SQL Server Express インスタンスを残す] オプションをクリックします。
FIPS モードを有効にすると、SQL Server のバージョン 2017 からバージョン 2019 へのアップグレードに失敗する [14.3]	以下のエラーが表示される場合があります。「次のエラーが発生しました。拡張機能のインストール中にエラーが発生しました。エラーメッセージ: AppContainer の作成に失敗。エラーメッセージ「なし」状態。この実装は、Windows プラットフォームの FIPS で検証された暗号化アルゴリズムの一部ではありません。」これは、FIPS 対応の Symantec Endpoint Protection Manager 14.3 を使用し、Microsoft SQL Server 2017 から 2019 にアップグレードした場合に発生します。[SEP-61473] この問題を回避するには、オペレーティングシステムレベルで FIPS を無効にします。 1. C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools で、[ローカルセキュリティポリシー] > [ローカルポリシー] > [セキュリティオプション] をクリックし、[システム暗号化] を無効にし、暗号化、ハッシュ、およびサイニングに FIPS 準拠のアルゴリズムを使用します 2. SQL Server バージョン 2017 からバージョン 2019 にアップグレードします。 3. SQL Server を正常にアップグレードした後、FIPS を再度有効にします。 FIPS モードを有効にすると、2017 から 2019 への SQL アップグレードが失敗する
14.2 以降へのアップグレード時に、カスタム名が使用されているとファイアウォールポリシーを更新できない場合がある	Symantec Endpoint Protection 14.2 以降へのアップグレードでは、いくつかのデフォルト名を変更していた場合、ファイアウォールポリシーに IPv6 の変更が組み込まれません。このデフォルト名には、デフォルトポリシーの名前とデフォルトルールの名前が含まれます。アップグレード時にルールを更新できない場合、IPv6 のオプションは表示されません。アップグレード後に作成する新しいポリシーまたはルールには影響がありません。 可能な場合は、変更された名前をデフォルトに戻します。または、デフォルトポリシーに追加したカスタムルールが IPv6 通信を遮断しないことを確認します。追加するすべての新しいポリシーまたはルールについて、同じことを確認します。

Table 2: Symantec Endpoint Protection Manager の問題

問題	説明と解決策
一部の EDR イベントがクライアントに表示されない [14.3 RU1]	Symantec Endpoint Protection クライアントは、Symantec EDR の Windows 用 イベント追跡 (ETW) イベントを収集するために、Windows 10 ビルド 14393 以降を実行している必要があります。[SEP-67175]
ネットワークトラフィックリダイレクト機能にいくつかの制限事項がある [14.3 RU1]	- Symantec Web Security Service は、IPv6 ではなく IPv4 で提供されます。[SEP-68700] - トンネルリダイレクト方式 - Windows 10 x64 バージョン 1703 以降 (半期サービスチャネル) でのみ実行されます。この方法では、他の Windows オペレーティングシステムまたは Mac クライアントはサポートされていません。[SEP-67927] - HVCI 対応の Windows 10 64 ビットデバイスはサポートされていません。[SEP-67648] - Symantec Endpoint Protection クライアントからのアウトバウンドトラフィックは、クライアントのファイアウォールまたは URL 評価ルールのいずれかによって評価される前に、WSS にリダイレクトされます。代わりに、そのトラフィックは WSS ファイアウォールおよび URL に対して評価されます。たとえば、SEP クライアントファイアウォール ルールが google.com を遮断し、WSS のルールが google.com を許可する場合、クライアントは google.com へのアクセスをユーザに許可します。クライアントへのインバウンドローカルトラフィックは引き続き Symantec Endpoint Protection ファイアウォールによって処理されます。[SEP-67488] - WSS キャプティブ ポータルはトンネル方式では使用できません。クライアントはチャレンジ資格情報を無視します。今後のリリースでは、WSS エージェント内の SAML 認証はキャプティブ ポータルに置き換わり、Symantec Endpoint Protection クライアントで使用可能になります。 - クライアント コンピュータがトンネル方式を使用して WSS に接続して仮想マシンをホストする場合、各ゲスト ユーザは WSS ポータルで提供された SSL 証明書をインストールする必要があります。 - ホームディレクトリや Active Directory 認証のようなローカルネットワークへのトラフィックはリダイレクトされません。 - Microsoft DirectAccess VPN とは互換性がありません。 このトンネル方式は、現在のところ早期採用リリース機能です。
14.2.x から 14.3 MP1 以降へのアップグレード後のクライアント登録エントリの重複 [14.3 RU1]	Symantec endpoint Protection クライアントを 14.2.x から 14.3 MP1 以降にアップグレードすると、Symantec Endpoint Protection Manager の [クライアント] ページに、これらのクライアントのエージェント登録エントリが重複して作成されます。 機能上の影響はありません。また、14.3 RU1 クライアントの新しいエントリを使用し続けることもできます。Symantec Endpoint Protection Manager は古いエージェントエントリを削除します。
ハイブリッド管理オプション、プロキシ サーバ、境界ファイアウォールを使用する場合は、Symantec Endpoint Security URL を許可する [14.3]	Broadcom による Symantec Enterprise Security の買収にともない、14.2.2.1 でのクライアントからクラウドへの通信用 URL が変更されました。[CDM-42467] 以下の状況では、クライアントをバージョンビルド 14.2.5569.2100 以降にアップグレードする必要があります - オンプレミス Symantec Endpoint Protection Manager ドメインがクラウドコンソールに登録されているときに、Symantec Endpoint Security を使用してクライアントおよびポリシーを管理している - プロキシサーバーを使用している。 完全なクラウド管理エージェントまたはハイブリッド管理エージェントのいずれかの URL を許可し、プロキシサーバーまたは境界ファイアウォールを許可します。 「SEP および SES がシマンテックのサーバに接続するために許可する URL」を参照してください 「クラウド管理の Symantec Agents をバージョン 14.2 RU2 MP1 以降にアップグレードする」を参照してください。

問題	説明と解決策
Symantec Endpoint Protection Manager リモートコンソールは、32 ビット Windows プラットフォームをサポートしません [14.3]	14.3 以降、32 ビットバージョンの Windows を実行している場合、Symantec Endpoint Protection Manager リモート コンソールにログオンできません。Oracle Java SE Runtime Environment は、32 ビットバージョンの Microsoft Windows をサポートしなくなりました。[SEP-61106] 以下のメッセージが表示された場合は、ローカルで Symantec Endpoint Protection Manager にログオンします。 「このバージョンの C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe は、実行中の Windows のバージョンと互換性がありません。お使いのコンピュータのシステム情報を確認してから、ソフトウェア発行者にお問い合わせください。」
Symantec Endpoint Protection Manager をインストールするときに、「Microsoft Visual C++ ランタイムのインストールに失敗しました」というエラーが表示される [14.3]	Symantec Endpoint Protection Manager を Windows 2012 R2 にインストールしているときに、以下のエラーが表示される場合があります。「Microsoft Visual C++ ランタイムのインストールに失敗しました」[SEP-60396] この問題を回避するには、Windows をアクティブ化して、Windows 更新プログラムをインストールします。Windows 更新プログラムでは、Visual C++ 2017 再頒布可能パッケージをインストールします。これは、Windows 2012 R2 に Symantec Endpoint Protection Manager 14.3 をインストールするための前提条件です。
Windows の WinHTTP で、TLS 1.1 および TLS 1.2 をデフォルトのセキュアプロトコルとして有効にするための更新 [14.3]	クラウドコンソールに登録されている Symantec Endpoint Protection Manager バージョン 14.3 にアップグレードまたはインストールした後、管理サーバーは、クラウドにログを正常にアップロードしなくなります。アップローダーに、以下のエラーが表示される場合があります。 <SEVERE> WinHttpSendRequest: 12175: A security error occurred この問題は、TLS 1.1 および 1.2 のサポートを提供する Microsoft update がないことが原因で発生します。 この問題を解決するには、Microsoft update: KB3140245 をインストールします。詳細については、次を参照してください。 Windows の WinHTTP で、TLS 1.1 および TLS 1.2 をデフォルトのセキュアプロトコルとして有効にするための更新
クライアントが Endpoint Threat Defense for AD 用に更新されたポリシーを受信した後も、Symantec Endpoint Protection Manager に「配備が進行中」と引き続き表示される [14.2 RU1 MP1 以降]	これは正常な動作です。Endpoint Threat Defense for AD 3.3 ポリシーは、バージョン 14.2 RU1 MP1 以降のクライアントでのみサポートされます。 Symantec Endpoint Threat Defense for Active Directory 3.3 のポリシーをグループに適用します。このグループには、Symantec Endpoint Protection 14.2 RU1 以前のバージョンを実行するクライアントが含まれています。これらのクライアントはポリシーを予期したとおりに受信して適用しますが、Symantec Endpoint Protection Manager で状態に「配備が進行中」のメッセージが引き続き表示されます。

Table 3: Windows、Mac、Linux クライアントの問題

問題	説明と解決策
サポート対象外の言語のクライアントを英語に自動的にアップグレードした場合、クライアントは引き続き英語で定義の日付設定を表示する [14.3 RU1 以降]	この問題を回避するには、レガシ クライアントをアンインストールし、新しい英語のクライアント インストール パッケージを手動でインストールします。また、自動的にアップグレードされたクライアントに対する修正が予定されています。[SEP-72481]

問題	説明と解決策
スタンドアロン Symantec WSS Agent は、WSS エージェントと同じコンピュータに SEP をインストールする場合、Symantec Endpoint Protection クライアントのインストールをブロックする	Network Traffic Redirection (NTR) コンポーネントは、スタンドアロン Symantec WSS Agent (WSSA) と同じファイルを使用します。NTR は、デフォルトで Symantec Endpoint Protection と Symantec Endpoint Security クラウドコンソールの両方にインストールされます。NTR 機能がエンドポイントにインストールされている場合、WSSA はインストールできません。同様に、WSSA がインストールされている場合、NTR 機能はインストールできません。 以下のいずれかの方法を使って、クライアント全体をアンインストールすることなく、既存のエンドポイントから Network Traffic Redirection 機能を削除できます。 • Symantec Endpoint Protection Manager で、NTR を含まないクライアント インストール機能セットを作成してエンドポイントに適用します。 既存の Endpoint Protection クライアントに機能を追加または削除する • 次のコマンドライン オプションは、クライアントのインストール ファイルを使用して NTR を削除します: <code>setup.exe /s /v" REMOVE=NTR /qn"</code>
クリーン インストールに使用されるアップグレード インストール パッケージでデフォルト機能セットがインストールされる。[14.3 RU1 MP1 以前]	[更新時に既存のクライアント機能を維持する] オプションをオンにしてアップグレード インストール パッケージを作成し、このパッケージを使ってクリーン インストールを行うと、デフォルト機能セットがクライアント デバイスにインストールされます。カスタム機能セットをインストールする場合は、クリーン インストール用に個別のインストール パッケージを作成する必要があります。
サポート対象外のアップグレード パスを指定すると、クラウド コンソールに重複したデバイスが作成される。[14.3 RU1]	Symantec Agent for Mac を 14.2/14.3 から 14.3 RU1 にアップグレードする前に、macOS を 10.15 から 11.0 にアップグレードすると、クラウド コンソールに重複したデバイスが作成されます。 重複を回避するには、オペレーティング システムをアップグレードする前にクライアントをアップグレードする必要があります (例: Symantec Agent for Mac を 14.2/14.3 から 14.3 RU1 にアップグレードしてから macOS を 10.15 から 11.0 にアップグレードする)。
Linux 用 Symantec Agent のインストール ログに誤ったメッセージが記録される。[14.3 RU1]	エージェントインストーラによって、一致しないドライババージョンに関連する不正なメッセージや、再起動が必要であることを示すメッセージがログに記録される場合があります。 これらのメッセージは、エージェントの機能には影響しません。
SuSe Linux デバイス上で、zypper が「at」パッケージの削除時に SEP Linux クライアント パッケージを削除する。[14.3 RU1]	SuSe Linux デバイス上では、「at」パッケージが必須依存パッケージとして追加され、zypper コマンドが未使用の依存関係を持つパッケージとして SEP クライアント パッケージ「sdcss-kmod」および「sdcss-sepagent」を自動的に削除しようとするため、「zypper remove at」コマンドを実行すると SEP Linux クライアントパッケージが削除されます。 回避策: 「at」パッケージを削除する場合は、コマンド「rpm -e --nodeps at」を実行します。
macOS 10.15 以降でのアップグレードの問題 [14.3 MP1]	macOS 10.15 以降では、クライアント配備ウィザードの [リモートコンピュータに Symantec Endpoint Protection をインストール] 機能で、古いバージョンからバージョン 14.3 MP1 への Symantec Endpoint Protection クライアントのアップグレードが失敗します。 回避策: macOS 10.15 以降では、Symantec Endpoint Protection Manager の自動更新を使用して Symantec Endpoint Protection クライアントの更新を実行します。
最初に SHA-2 サポートをインストールしないと、Symantec Endpoint Protection 14.3 Windows クライアントのインストールに失敗することがある [14.3]	レガシーオペレーティングシステムのバージョン (Windows 7 RTM または SP1、Windows Server 2008 R2 または R2 SP1 または R2 SP2) を実行している場合、2019 年 7 月以降にリリースされた Windows アップデートをインストールするには、デバイスに SHA-2 コードサイニングサポートをインストールする必要があります。SHA-2 をサポートしていない場合、Windows クライアントのインストールに失敗することがあります。クライアントを初めてインストールする場合でも、以前のリリースから自動的にアップグレードする場合でも、インストールが失敗することがあります。[SEP-61175/61403] Microsoft が適用した SHA-2 コードサイニングサポートを取得するには、以下を参照してください。 Windows および WSUS の 2019 SHA-2 コードサイニングサポートの要件 SHA-2 サポートがインストールされていない場合、Symantec Endpoint Protection 14.3 Windows クライアントのインストールに失敗することがある

問題	説明と解決策
Windows 10 1803 で UWF が有効な場合、Symantec Endpoint Protection Windows クライアントが動作しない [14.3]	統合書き込みフィルタ (UWF) が有効で、Windows クライアントがインストールされているドライブを保護しているときに、Symantec Endpoint Protection クライアントを Windows 10 RS4 1803 32 ビットオペレーティングシステムで実行する場合、クライアントは正常に動作しません。この Windows オペレーティングシステムには、Windows クライアントを実行できない UWF 障害が含まれています。 この問題を回避する方法。 - 障害が含まれていない別のオペレーティングシステムバージョンにアップグレードする。 - UWF を無効にする。 UWF が有効な Windows 10 1803 にインストールすると、Endpoint Protection が誤動作を起こす を参照してください。
WSS トラフィックリダイレクトが有効な Mac クライアントで LiveUpdate にカスタムプロキシ設定を適用できない [14.2 RU1 MP1 以降]	Symantec Endpoint Protection 14.2 RU1 MP1 の管理対象 Mac クライアントで、外部通信設定を通じて LiveUpdate にカスタムプロキシ設定を使用するように設定しました。しかし、Symantec Endpoint Protection Manager ポリシーを使用して Mac クライアントの WSS トラフィックリダイレクト (WTR) を有効にすると、LiveUpdate トラフィックにカスタムプロキシ設定が適用されていないことに気がきました。代わりに、LiveUpdate は直接接続を試行しています。 この問題を回避するには、WSS トラフィックリダイレクトが無効になっているときにのみ、LiveUpdate でカスタムプロキシ設定を使用します。
強化が有効な状態で Microsoft Edge が PDF のダウンロードを予期せず許可する [14.2 RU1 MP1 以降]	Symantec Endpoint Protection クライアントでアプリケーション強化が有効な状態で Microsoft Edge ブラウザを使用すると、予期せず PDF ファイルをダウンロードできてしまいます。PDF ファイルのダウンロードの禁止は、他のブラウザでは想定どおりに機能します。 この問題は今後のリリースで修正される予定です。

Symantec Enterprise Protection が正式に Broadcom の一員になったという発表に伴い、シマンテックはマニュアルを Broadcom [Symantec Security Tech Docs Portal](#) に移行しました。

Endpoint Protection のマニュアルを見つけるには、[**Symantec Security Software**] タブをクリックし、[**Endpoint Security and Management**] > [**Endpoint Protection**] をクリックします。

Table 4: マニュアルの問題

問題	説明と解決策
操作方法の記事の有効期限が切れている。	Symantec Endpoint Protection Manager ヘルプのトピックと重複していた操作方法の記事は、Endpoint Protection サイトに再公開され、URL が変更しました。 記事を検索するには、[検索フィールド] を使用します。
PDF ファイル	Symantec は DOC 記事にすべての PDF ファイルを掲載していました。これらのページは有効期限が切れました。 PDF ファイルの最新バージョンのリリースを検索するには、「関連ドキュメント」ページに移動します。今後、Broadcom はレガシー PDF ファイルや翻訳した PDF ファイルを追加していく予定です。

解決済みの問題は、以下を参照してください

[Symantec Endpoint Protection 14.3 RU1 MP1 の新しい修正とコンポーネント](#)

[Symantec Endpoint Protection 14.3 RU1 の新しい修正とコンポーネント](#)

[Symantec Endpoint Protection 14.3 MP1 の新しい修正とコンポーネント](#)

[Symantec Endpoint Protection 14.3 の新しい修正とコンポーネント](#)

Symantec Endpoint Protection (SEP) 14.3 RU2 のシステム要件

一般に、次のシステム必要条件は、これらがサポートされるオペレーティングシステムのものと同じです。

NOTE

Symantec Endpoint Protection Manager の以前のバージョンでは、新しいバージョンのクライアントを正しく管理できない場合があります。コンテンツの更新やクライアント管理に問題が発生することがあります。たとえば、Symantec Endpoint Protection Manager 14.0.1 以前では、バージョン 14.2 クライアントをそのバージョン固有の名称で正しく指定することができません。Symantec Endpoint Protection Manager 14 MP2 以前のバージョンでは、14.0.1 以降のクライアントバージョンをバージョン固有の名称で正しく指定することができません。

以下の表に、Symantec Endpoint Protection のソフトウェア要件とハードウェア要件を示します。

Table 5: つの Symantec Endpoint Protection Manager (SEPM) ソフトウェアのシステム必要条件

コンポーネント	必要条件
オペレーティングシステム	- Windows Server 2008 R2 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2016 - Windows Server 2019 Note: デスクトップオペレーティングシステムはサポートされません。 Note: Windows Server Core エディションは、14.2x 以前ではサポートされていません。
Web ブラウザ	次のブラウザは、つの Symantec Endpoint Protection Manager に Web コンソールでアクセスする場合や、つの Symantec Endpoint Protection Manager のヘルプを表示する場合に使用できます。 - Microsoft Edge Chromium ベースのブラウザ (14.3 以降) - Microsoft Edge 注: 32 ビット版の Windows 10 は、Edge ブラウザ上での Web コンソールアクセスをサポートしません。 - Microsoft Internet Explorer 11 (14.2.x 以前) - Mozilla Firefox 5.x ~ 83 - Google Chrome 87

コンポーネント	必要条件
データベース	Symantec Endpoint Protection Manager には、デフォルトデータベースが含まれています。 - Microsoft SQL Server Express 2014 (Windows Server 2008 R2 用) - Microsoft SQL Server Express 2017 - Sybase 埋め込みデータベース (14.3 MP.x 以前のみ) 代わりに、Microsoft SQL Server の次のいずれかのバージョンのデータベースを使うこともできます。 - SQL Server 2008 SP4 - SQL Server 2008 R2、SP3 - SQL Server 2012 RTM - SP4 - SQL Server 2014 RTM - SP3 - SQL Server 2016 SP1、SP2 - SQL Server 2017 RTM - SQL Server 2019 RTM (14.3 以降) Note: Amazon RDS でホストされている SQL Server データベースがサポートされています (14.0.1 MP2 時点)。 Note: Symantec Endpoint Protection で SQL Server データベースを使用しており、環境で TLS 1.2 のみが使用されている場合は、その SQL Server で TLS 1.2 がサポートされることを確認してください。SQL Server にパッチを適用する必要がある場合があります。この推奨事項は SQL Server 2008、2012、2014 に適用されます。TLS 1.2 をサポートする SQL Server のパッチを適用しないと、Symantec Endpoint Protection 12.1 から 14 にアップグレードするときに問題が発生する可能性があります。 Note: Microsoft SQL Server 用の TLS 1.2 のサポート
その他の環境条件	IPv6 ネットワーク純粋に IPv4 スタックもをインストールし、無効になっています。IPv4 スタックがアンインストールされ、つの Symantec Endpoint Protection Manager は機能しません。;"

Table 6: つの Symantec Endpoint Protection Manager ハードウェアのシステム必要条件

コンポーネント	必要条件
プロセッサ	Intel Pentium デュアルコアまたは同等以上 (8 コア以上を推奨) Note: Intel Itanium IA-64 プロセッサはサポートされません。
物理 RAM	2 GB 以上の RAM 空き容量 (8 GB 以上を推奨)。 Note: つの Symantec Endpoint Protection Manager サーバーには、すでにインストールされている他のアプリケーションの RAM 要件によって RAM の追加が必要な場合があります。たとえば、つの Symantec Endpoint Protection Manager サーバーに Microsoft SQL Server がインストールされている場合、サーバーには少なくとも 8 GB が使用可能である必要があります。
表示	1024 x 768 以上
システムドライブにインストールする場合はハードディスクドライブ	ローカル SQL Server データベースを使用する場合: - 管理サーバーとデータベース用に最小 40 GB 利用可能であること (200 GB を推奨) リモート SQL Server データベースを使用する場合: - 管理サーバー用に最小 40 GB 利用可能であること (100 GB を推奨) - データベースのリモートサーバー用に追加のディスク容量が利用可能であること

コンポーネント	必要条件
代替ドライブにインストールする場合はハードディスクドライブ	ローカル SQL Server データベースを使用する場合: - システムドライブには 15 GB 以上の空き容量が必要 (100 GB を推奨) - インストールドライブには 25 GB 以上の空き容量が必要 (100 GB を推奨) リモート SQL Server データベースを使用する場合: - システムドライブには 15 GB 以上の空き容量が必要 (100 GB を推奨) - インストールドライブには 25 GB 以上の空き容量が必要 (100 GB を推奨) - データベースのリモートサーバー用に追加のディスク容量が利用可能であること
その他	有効なネットワーク インターフェース カード

SQL Server データベースを使う場合は、利用可能なディスク容量を追加しなければならないことがあります。追加容量のサイズと場所は、SQL Server で使うドライブ、データベース保守の必要条件、その他のデータベースの設定によって異なります。

Table 7: Symantec Endpoint Protection for Windows クライアントソフトウェアのシステム必要条件

コンポーネント	必要条件
オペレーティングシステム (デスクトップ)	- Windows 7 (32 ビット、64 ビット、RTM、SP1) - Windows Embedded 7 Standard、POSReady、Enterprise (32 ビット、64 ビット) - Windows 8 (32 ビット、64 ビット) - Windows Embedded 8 Standard (32 ビット、64 ビット) - Windows To Go を含む Windows 8.1 (32 ビット、64 ビット) - Windows 8.1 (2014 年 4 月更新) (32 ビット、64 ビット) - Windows 8.1 (2014 年 8 月更新) (32 ビット、64 ビット) - Windows Embedded 8.1 Pro、Industry Pro、Industry Enterprise (32 ビット、64 ビット) - Windows 10 (バージョン 1507) (32 ビット、64 ビット)、Windows 10 Enterprise 2015 LTSC を含む - Windows 10 November Update (バージョン 1511) (32 ビット、64 ビット) - Windows 10 Anniversary Update (バージョン 1607) (32 ビット、64 ビット)、Windows 10 Enterprise 2016 LTSC を含む - Windows 10 Creators Update (バージョン 1703) (32 ビット、64 ビット) - Windows 10 Fall Creators Update (バージョン 1709) (32 ビット、64 ビット) - Windows 10 April 2018 Update (バージョン 1803) (32 ビット、64 ビット) - Windows 10 October 2018 Update (バージョン 1809) (32 ビット、64 ビット)、Windows 10 Enterprise 2019 LTSC を含む - Windows 10 May 2019 Update (バージョン 1903) (32 ビット、64 ビット) - Windows 10 November 2019 Update (バージョン 1909) (32 ビット、64 ビット) (14.2 RU1 以降) - Windows 10 20H1 (Windows 10 バージョン 2004) (14.3 以降) - Windows 10 20H2 (Windows 10 バージョン 2009) (14.3 RU1 時点)
オペレーティングシステム (サーバー)	- Windows Server 2008 R2 - Windows Small Business Server 2011 - Windows Server 2012 - Windows Server 2012 R2 - Windows Server 2012 R2 (2014 年 4 月更新) - Windows Server 2012 R2 (2014 年 8 月更新) - Windows Server 2016 - Windows Server 2019 - Windows Server, version 1803 (サーバーコア) (14.2 以降) - Windows Server、バージョン 1809 (サーバーコア) - Windows Server, version 1903 (サーバーコア) (14.2 RU1 以降) - Windows Server, version 1909 (サーバーコア) (14.2 RU1 以降) - Windows Server、バージョン 2004 - Windows Server、バージョン 20H2 (14.3 RU1) 以前のリリースのサポート対象のオペレーティング システムのリストについては、次を参照してください。 Windows と Endpoint Protection クライアントの互換性 Windows 10 アップデートと Windows Server 2016/Server 2019 に対する Endpoint Protection のサポート
ブラウザの侵入防止	ブラウザ侵入防止のサポートは CIDS (Client Intrusion Detection System) エンジンのバージョンに基づきます。 「Endpoint Protection のブラウザ侵入防止がサポートするブラウザのバージョン」を参照してください。

Table 8: Symantec Endpoint Protection for Windows クライアントハードウェアのシステム必要条件

コンポーネント	必要条件
プロセッサ (物理コンピュータ用)	32 ビット CPU: 最低限 2 GHz Intel Pentium 4 または同等 (Intel Pentium 4 または同等を推奨) 64 ビット CPU: 最低限 2 GHz Pentium 4 with x86-64 サポートまたは同等 Note: Itanium CPU はサポートされません。
プロセッサ (仮想コンピュータ用)	1つの仮想ソケットと、ソケットごとに1つの1 GHz 以上のコア (1つの仮想ソケットと、ソケットごとに2つの2 GHz のコアを推奨) Note: ハイパーバイザリソースの予約を有効にする必要があります。
物理 RAM	1 GB (2 GB を推奨)、またはオペレーティングシステムの必要に応じてそれ以上
ディスプレイ	800 x 600 以上
ハードディスクドライブ	ディスク容量の必要条件は、インストールするクライアントの種類、インストール先のドライブ、プログラムデータファイルの保存先によって異なります。プログラムデータフォルダは通常、システムドライブのデフォルトの場所 (C:\ProgramData) に配置されています。 選択したインストールドライブに関係なく、システムドライブには利用可能なディスク容量が常に必要です。 Note: 必要なディスク空き領域は NTFS ファイルシステムに基づきます。コンテンツの更新とログ用の追加容量も必要です。

Table 9: システムドライブにインストールする場合に Symantec Endpoint Protection for Windows クライアントで利用可能なハードディスクドライブのシステム必要条件

クライアントの種類	必要条件
標準	システムドライブ上にプログラムデータフォルダが置かれている場合: 395 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合: - システムドライブ: 180 MB - 代替インストールドライブ: 350 MB
Embedded/VDI	システムドライブ上にプログラムデータフォルダが置かれている場合: 245 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合: - システムドライブ: 180 MB - 代替インストールドライブ: 200 MB
ダークネットワーク	システムドライブ上にプログラムデータフォルダが置かれている場合: 545 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合: - システムドライブ: 180 MB - 代替インストールドライブ: 500 MB

* インストール中は、さらに 135 MB が必要です。

Table 10: 代替ドライブにインストールする場合に Symantec Endpoint Protection for Windows クライアントで利用可能なハードディスクドライブのシステム必要条件

クライアントの種類	必要条件
標準	システムドライブ上にプログラムデータフォルダが置かれている場合: - システムドライブ: 380 MB - 代替インストールドライブ: 15 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合:** - システムドライブ: 30 MB - プログラムデータドライブ: 350 MB - 代替インストールドライブ: 150 MB
Embedded/VDI	システムドライブ上にプログラムデータフォルダが置かれている場合: - システムドライブ: 230 MB - 代替インストールドライブ: 15 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合:** - システムドライブ: 30 MB - プログラムデータドライブ: 200 MB - 代替インストールドライブ: 150 MB
ダークネットワーク	システムドライブ上にプログラムデータフォルダが置かれている場合: - システムドライブ: 530 MB - 代替インストールドライブ: 15 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合:** - システムドライブ: 30 MB - プログラムデータドライブ: 500 MB - 代替インストールドライブ: 150 MB

* インストール中は、さらに 135 MB が必要です。

** プログラムデータフォルダが代替インストールドライブと同じである場合は、プログラムデータドライブに 15 MB を加算して合計を算出します。ただし、インストール中は、完全に利用可能な 150 MB の容量が代替インストールドライブ上に必要になります。

Table 11: Windows Embedded の Symantec Endpoint Protection クライアントのシステム必要条件

コンポーネント	必要条件
プロセッサ	1 GHz Intel Pentium
物理 RAM	256 MB Note: この図は Symantec Endpoint Protection 埋め込みクライアントのインストール用です。EDR などの統合ソリューションから追加機能を実装する場合は、物理 RAM の追加が必要です。
ハードディスクドライブ	Symantec Endpoint Protection Embedded/VDI クライアントには、次のハードディスク空き容量が必要です。 - システムドライブにインストールした場合: 245 MB - 代替ドライブにインストールした場合: システムドライブ上に 230 MB、代替ドライブ上に 15 MB インストール中は、さらに 135 MB が必要です。 次の図では、プログラムデータフォルダがシステムドライブ上にあると想定しています。詳細または他のクライアントの種類の必要条件については、Symantec Endpoint Protection for Windows クライアントのシステム必要条件を参照してください。

コンポーネント	必要条件
組み込みオペレーティングシステム	- Windows Embedded Standard 7 (32 ビットおよび 64 ビット) - Windows Embedded POSReady 7 (32 ビットおよび 64 ビット) - Windows Embedded Enterprise 7 (32 ビットおよび 64 ビット) - Windows Embedded 8 Standard (32 ビット、64 ビット) - Windows Embedded 8.1 Industry Pro (32 ビットおよび 64 ビット) - Windows Embedded 8.1 Industry Enterprise (32 ビットおよび 64 ビット) - Windows Embedded 8.1 Pro (32 ビットおよび 64 ビット)
必要な最小コンポーネント	- フィルターマネージャ (FltMgr.sys) - パフォーマンスデータヘルパー (pdh.dll) - Windows インストーラサービス
テンプレート	- アプリケーション互換性 (デフォルト) - 電子看板 - Industrial Automation - IE、メディアプレーヤー、RDP - セフトップボックス - シンククライアント Minimum Configuration テンプレートはサポートされていません。 Enhanced Write Filter (EWF) と Unified Write Filter (UWF) はサポートされません。推奨される書き込みフィルタは、レジストリフィルタと共にインストールされる File Based Write Filter (FBWF) です。

Table 12: Symantec Endpoint Protection for Mac クライアントのシステム必要条件

コンポーネント	必要条件
プロセッサ	64 ビットの Intel Core 2 Duo 以降 Apple M1 chip (14.3 RU2 以降)
物理 RAM	2 GB の RAM
ハードディスクドライブ	: インストール時に 1 GB のハードディスク空き領域
ディスプレイ	800 x 600
オペレーティングシステム	- macOS 10.15 ~ 10.15.7 - macOS 11 (Big Sur) 以前のリリースのサポート対象のオペレーティングシステムのリストについては、「Mac と Endpoint Protection クライアントの互換性」を参照してください。

Table 13: Symantec Endpoint Protection for Linux クライアントのシステム必要条件

コンポーネント	必要条件
ハードウェア	- Intel Pentium 4 (2 GHz) 以上のプロセッサ 500 MB の空き RAM (4 GB の RAM を推奨) /var、/opt、および /tmp が同じファイルシステムまたはボリュームを共有する場合、2 GB のディスク空き容量 - 異なるボリュームにある場合、各 /var、/opt、および /tmp に 500 MB のディスク空き容量
オペレーティングシステム	バージョン 14.3 RU1 の時点でサポートされているオペレーティングシステム: - Amazon Linux 2 - CentOS 6、7、8 - Debian 9、10 (14.3 RU2 以降) - Oracle Enterprise Linux 6、7、8 - Red Hat Enterprise Linux 6、7、8 - SuSE Linux Enterprise Server 12.x、15.x - Ubuntu 14.04 LTS、16.04 LTS、18.04 LTS、20.04 LTS Symantec Linux Agent のサポート対象カーネル (サポート対象のマイナーな Linux OS のバージョンも表記) バージョン 14.3 MP1 以前でサポートされているオペレーティング システム : - Amazon Linux - CentOS 6U3 - 6U9, 7 - 7U7, 8 (32 ビットと 64 ビット) - Debian 6.0.5 Squeeze、Debian 8 Jessie (32 ビットおよび 64 ビット) - Fedora 16, 17 (32 ビットおよび 64 ビット) - Oracle Linux (OEL) 6U2、6U4、6U5、6U8、7、7U1、7U2、7U3、7U4 - Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 - SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4 (32 ビットと 64 ビット)、12 (64 ビット)、12 SP1 - 12 SP3 (64 ビット) - SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4 (32 ビットと 64 ビット)、12 SP3 (64 ビット) - Ubuntu 12.04, 14.04, 16.04, 18.04 (14.3 時点)、32 ビットと 64 ビット 以前のリリースでサポートされているオペレーティングシステムカーネルのリストについては、 「Symantec Endpoint Protection for Linux 14.x 用にプリコンパイルされた Auto-Protect ドライバ/モジュールを含む Linux ディストリビューションおよびカーネルのリスト」を参照してください。
グラフィカルデスクトップ環境	次のグラフィカルデスクトップ環境を使用して Symantec Endpoint Protection for Linux クライアントを表示できます。 - KDE - Gnome - Unity Symantec Agent for Linux 14.3 RU1 には、グラフィカルユーザーインターフェースがありません。

コンポーネント	必要条件
その他の環境要件 (14.3 MP1 以前)	- Glibc 2.6 より前の glibc を実行するオペレーティングシステムはサポートされません。 - net-tools または iproute2 Symantec Endpoint Protection は、コンピュータの既存のインストール内容に応じて、次の 2 つのツールのうちのいずれかを使います。 - OpenSSL 1.0.2k-fips 以降 - 開発者ツール Auto-Protect カーネルモジュールの自動コンパイルおよび手動コンパイルプロセスでは、特定の開発者ツールをインストールする必要があります。ここでの開発者ツールには、gcc、カーネルソース、ヘッダーファイルが含まれます。インストールするツール、および特定の Linux バージョンに対しツールをインストールする方法については、以下を参照してください。 Endpoint Protection for Linux の Auto-Protect カーネルモジュールの手動コンパイル 64 ビットコンピュータでの i686 ベース依存パッケージ Linux クライアントの実行可能ファイルの多くは 32 ビットプログラムです。64 ビットのコンピュータでは、Linux クライアントをインストールする前に i686 ベースの依存パッケージをインストールする必要があります。 i686 ベース依存パッケージをインストールしていない場合は、次のコマンドラインを使ってインストールできます。このインストールでは、sudo を使った次のコマンドが示すように、スーパーユーザ権限が必要です。 - Red Hat ベースの配布: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code> - Debian ベースの配布: <code>sudo apt-get install ia32-libs</code> - Ubuntu ベースの配布: <pre> sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386 </pre>

[Endpoint Security およびすべてのバージョンの Endpoint Protection のリリースバージョン、リリースノート、新しい修正、およびシステム要件](#)

国際化の必要条件

英語以外または複数言語が混在する環境に つの Symantec Endpoint Protection Manager をインストールするときには一定の制限があります。

Table 14: 国際化の必要条件

コンポーネント	必要条件
コンピュータ名、サーバー名、ワークグループ名	英語以外の文字は次の制限付きでサポートされています。 2 バイト文字セットまたは high-ASCII 文字セットを使うホストまたはユーザーには、ネットワーク監査は機能しません。 - つの Symantec Endpoint Protection Manager コンソールまたはクライアントユーザーインターフェースではダブルバイト文字セットまたは high-ASCII 文字セットの名前は正しく表示されないことがあります。 2 バイト文字セットまたは high-ASCII 文字セットのホスト名は、NetBIOS での上限の長さを越えることができません。ホスト名が NetBIOS での上限の長さを越えている場合、つの Symantec Endpoint Protection Manager コンソールで [ホーム]、[監視]、[レポート] のページが表示されません。
英語の文字	次の場合は英字である必要があります。 - リモートコンピュータにクライアントパッケージを配備する場合 - 管理サーバー設定ウィザードでサーバーデータフォルダを定義します。 - つの Symantec Endpoint Protection Manager のインストールパスを定義する場合 - リモートコンピュータにクライアントを配備するときに資格情報を定義する場合 - グループ名を変更する場合 英語以外の文字を含むグループ名用のクライアントパッケージを作成できます。ただし、グループ名に英語以外の文字が含まれている場合、プッシュ配備ウィザードを使ったクライアントパッケージの配備はできないことがあります。 - クライアントコンピュータに英語以外の文字をプッシュ配備する場合。 サーバー側で生成される英語以外の文字の一部がクライアントユーザーインターフェースで正しく表示されないことがあります。 たとえば、ダブルバイト文字セットを使ったロケーション名は、ダブルバイト文字以外の文字セットの名前を持つクライアントコンピュータでは正しく表示されません。
クライアントコンピュータの [ユーザー情報] ダイアログボックス	エクスポートしたパッケージをインストールした後で、[ユーザー情報] クライアントコンピュータダイアログボックスでフィードバックを提供するときには、2 バイトまたは high-ASCII 文字を使わないでください。 ユーザー情報の収集
ライセンスアクティブ化ウィザード	次のフィールドで 2 バイト文字を使わないでください。 - 名 [姓] [会社名] - 市区町村 [都道府県]

14.3 RU1 MP1 以前では、Symantec Endpoint Protection Manager と Symantec Endpoint Protection Windows クライアントは英語から 12 言語 (中国語、チェコ語、フランス語、ドイツ語、イタリア語、日本語、韓国語、ポーランド語、ポルトガル語 (ブラジル)、ロシア語、スペイン語) に翻訳されました。14.3 RU2 では、Symantec Endpoint Protection は、フランス語、日本語、ポルトガル語 (ブラジル)、スペイン語の 4 言語にのみ翻訳されました。

サポート対象の仮想インストールと仮想化製品

仮想環境で実行するサポート対象のオペレーティングシステムに Symantec Endpoint Protection をインストールできます。Symantec Endpoint Protection は、ホストではなくゲストオペレーティングシステムにインストールします。

以下の仮想化製品は、つの Symantec Endpoint Protection Manager、コンソール、および Windows と Linux 用の Symantec Endpoint Protection クライアントソフトウェアをサポートします。

- Microsoft Azure
- Amazon WorkSpaces
- Citrix Studio バージョン 2009.0.0
- Nutanix AOS 5.15 (LTS)
- VMware WS 5.0 (ワークステーション) 以降
- VMware GSX 3.2 (エンタープライズ) 以降
- VMware ESX 2.5 (ワークステーション) 以降
- VMware ESXi 4.1 - 5.5
- VMware ESXi 6.0
- VMware ESXi 6.0 Update 1
- VMware ESXi 6.0 Update 2
- VMware ESXi 6.0 Update 3 (14.0.1 現在)
- VMware ESXi 6.5 (14.0.1 現在)
- VMware ESXi 6.5U1 (14.2 現在)
- VMware ESXi 6.5U2 (14.2 現在)
- VMware ESXi 6.7 (14.2 現在)
- Microsoft Virtual Server 2005
- Windows Server 2008 Hyper-V
- Windows Server 2012 Hyper-V
- Windows Server 2012 R2 Hyper-V
- Windows Server 2016 Hyper-V (14.2 MP1 現在)
- Windows Server 2019 Hyper-V Core Edition (14.2 MP1 現在)
- Citrix XenServer 5.6 以降
- Oracle が提供する VirtualBox

Symantec Endpoint Protection には、仮想環境でのパフォーマンスを改善する多くの機能が含まれます。

[つの Symantec Endpoint Protection Manager の仮想インフラストラクチャでの使用](#)

[スキャンのランダム化による Windows クライアントの仮想化環境でのコンピュータパフォーマンスの向上](#)

最新のシステム必要条件について詳しくは、「[Symantec Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)」を参照してください。

詳細情報の入手方法

以下の表に、ベストプラクティス、トラブルシューティング情報、製品の使用に役立つその他のリソースを入手できる Web サイトを示します。

Table 15: Endpoint Protection Web サイトの情報

情報の種類	Web サイトリンク
体験版	アカウント担当者にお問い合わせください。
マニュアルとマニュアル更新	• 最新リリースの製品ガイド (英語) • 最新リリースの製品ガイド (その他の言語) • Symantec Endpoint Protection 14.x のすべてのバージョンの製品ガイド (英語)
テクニカルサポート	Endpoint Protection テクニカルサポート ナレッジベースの記事、製品リリースの詳細、更新、パッチ、サポートの問い合わせオプションが含まれます。
脅威の情報と更新	シマンテックセキュリティセンター

情報の種類	Web サイトリンク
トレーニング	教育サービス トレーニングコース、eLibrary、その他のコンテンツにアクセスできます。
Symantec Connect フォーラム (英語)	Endpoint Protection

Symantec Endpoint Protection とは

Symantec Endpoint Protection のアーキテクチャおよびコンポーネントについて

Symantec Endpoint Protection はネットワークのラップトップ、デスクトップ、サーバーをマルウェア、リスク、脆弱性から保護するクライアントサーバーソリューションです。Symantec Endpoint Protection はウイルス防止と高度な脅威防止を組み合わせ、コンピュータをウイルス、ウォーム、トロイの木馬、アドウェアなど既知と未知の脅威や未知の脅威からプロアクティブに守ります。また、Symantec Endpoint Protection は、ルートキット、ゼロデイ攻撃、変異するスパイウェアのような、従来のセキュリティ対策で対応できない最も高度な攻撃からも保護します。

Symantec Endpoint Protection は手間のかからない高い能力を備え、ネットワーク上で通信しながら物理システムと仮想システムの両方を攻撃から自動的に保護します。Symantec Endpoint Protection は、効率的かつ容易に配備でき使うことのできる管理ソリューションを提供します。

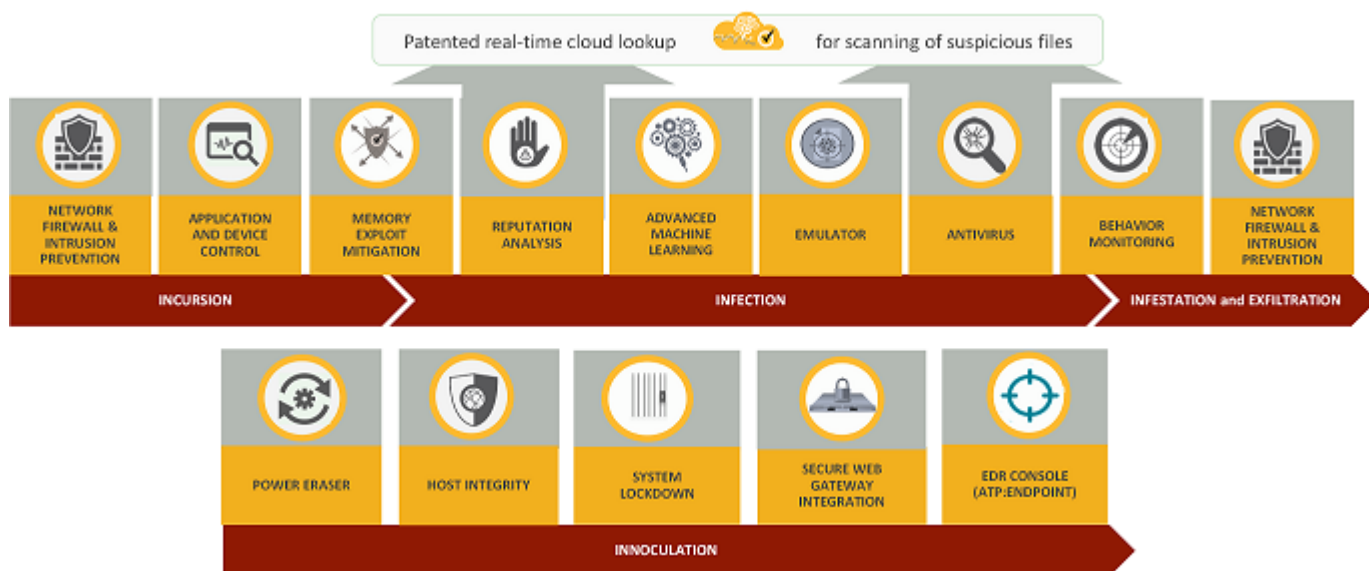
Symantec Endpoint Protection 技術でコンピュータが保護される仕組み

Symantec Endpoint Protection アーキテクチャコンポーネント

Symantec Endpoint Protection 技術でコンピュータが保護される仕組み

既知や未知の脅威に対する Symantec Endpoint Protection の中核的な保護では、防御のために階層化されたアプローチが使用されます。この包括的なアプローチによって、攻撃を受ける前、受けているとき、受けた後のネットワークを保護します。Symantec Endpoint Protection は、ツールを提供することで攻撃を受ける前にセキュリティ態勢を高め、攻撃にさらされるリスクを低減します。

ネットワーク内のコンピュータに対する完全な保護を実現するために、すべての保護を常時有効にします。



Symantec Endpoint Protection 技術が防止する攻撃の種類

Symantec Endpoint Protection は、次に説明する包括的なセキュリティアプローチを使用して、攻撃チェーン全体にわたって環境を保護します。このアプローチには、侵入、感染、汚染と漏洩、修復と予防接種の各ステージがあります。

フェーズ 1: 侵入

ハッカーは、一般的に、侵入のフェーズでソーシャルエンジニアリング、ゼロデイの脆弱性、SQL インジェクション、ターゲットマルウェアやその他の手段を使用して、組織のネットワークに侵入します。

Symantec Endpoint Protection は、次の技術を使用して、ハッカーがシステムに侵入する前に攻撃に対する防御を構築します。

- 侵入防止/ファイアウォール (ネットワーク脅威防止): 着信と発信のすべてのトラフィックを分析し、ブラウザ保護を提供して、前述のような脅威がコンピュータで実行される前にそれらを遮断します。ルールベースのファイアウォールとブラウザ保護が、Web ベースの攻撃から保護します。
[侵入防止の管理](#)
[ファイアウォール保護の管理](#)
- アプリケーション制御: ファイルアクセス、レジストリアccess、プロセスの実行を許可する方法を制御します。
[アプリケーション制御、システムロックダウン、デバイス制御について](#)
[アプリケーション制御の設定](#)
- デバイス制御: ハードウェアを選択するためのアクセスや、情報のアップロードやダウンロードを行えるデバイスの種類を制御するためのアクセスを制限します。
[デバイス制御の管理](#)
- メモリエクスプロイト緩和機能: よく使用されているソフトウェアのうち、ベンダーによってパッチが適用されていないものに対するヒープスプレー、SEHOP 上書き、Java エクスプロイトなどのゼロデイ攻撃を無効化します。
[メモリエクスプロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化](#)
- **Web** とクラウドのアクセス保護: 企業ユーザがどこにいるかにかかわらず、すべてのポートとプロトコルのネットワークトラフィックを制御します。
[Web とクラウドのアクセス保護 の設定](#)

フェーズ 2: 感染

ターゲット攻撃では、ハッカーは一般的にソーシャルエンジニアリング、ゼロデイの脆弱性、SQL インジェクション、ターゲットマルウェアやその他の手段を使用して、組織のネットワークに侵入します。

Symantec Endpoint Protection では、次の技術を使用して、システムが感染する前に、これらの攻撃を検出して予防します。

- メモリエクスプロイト緩和機能: マルウェアを検出します。
- ファイル評価の分析 (**Insight**): シマンテック社の Global Intelligence Network を使用した人工知能に基づいています。この高度な分析により、ユーザー、Web サイト、ファイル間の膨大な数の相関関係が検査され、急速に変異するマルウェアを識別し、それに対する防御を行います。主要な属性 (ファイルダウンロードの原点など) を分析することで、シマンテック社は、ファイルが良好か不良かを正確に識別し、ファイルがクライアントコンピュータに到達する前にすべてに評価スコアを割り当てることができます。
[ダウンロードインサイト検出の管理](#)
- 高度な機械学習: Global Intelligence Network 内にある良好ファイルと不良ファイルの何兆もの例を分析します。高度な機械学習はシグネチャレス型の技術で、マルウェアの新たなバリエーションを実行前の段階で遮断できます。
[Symantec Endpoint Protection が高度な機械学習を使用する仕組み](#)
- 高速エミュレーション: 多形態のカスタムパッカーを使用する、隠れたマルウェアを検出します。スキャナが、簡易的な仮想マシンで各ファイルをミリ秒単位で実行します。これにより脅威の状態が再現されるため、検出率とパフォーマンスの両方が向上します。
[Symantec Endpoint Protection のエミュレータがマルウェアを検出およびクリーニングする方法](#)
- ウイルス対策ファイル保護 (ウイルスとスパイウェアの対策): シグネチャベースのウイルス対策とファイルヒューリスティックを使用してシステム上のマルウェアを探して撲滅し、ウイルス、ワーム、トロイの木馬、スパイウェア、ボット、アドウェア、ルートキットから保護します。
[クライアントコンピュータでのスキャンの管理](#)
[スキャンの種類とリアルタイム保護について](#)
- 振る舞いの監視 (**SONAR**): 機械学習を活用することでゼロデイ防御を提供し、約 1,400 のファイルが実行される間にその振る舞いをリアルタイムで監視することで、ファイルのリスクを判断し、新たな未知の脅威を防止します。

SONAR の管理

フェーズ 3: 汚染と漏洩

データ漏洩とは、データがコンピュータから許可を得ずに転送されることです。侵入者がこれらの対象システムを制御できるようになると、知的財産やその他の機密データが盗まれる可能性があります。攻撃者は取得した情報を使用して分析を行い、その後の攻撃や詐欺に利用します。

- 侵入防止/ファイアウォール: ネットワークを通過する脅威を遮断します。
- 振る舞いの監視: 感染が広がらないようにします。

フェーズ 4: 修復と予防接種

Symantec Endpoint Protection には 1 つのコンソールと、オペレーティングシステム、プラットフォーム、あらゆる規模のビジネスにわたって保護を提供するエージェントが含まれます。

- **Power Eraser:** リモートからトリガできる拡張ツールで、APT (Advanced Persistent Threat) に対処し、執拗なマルウェアに対する修復を行います。

[この Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知るべきこと](#)

- **ホストインテグリティ:** ポリシーを強制適用し、権限のない変更を検出し、損害の評価を行うことで、エンドポイントを実際に保護し、コンプライアンスを維持します。その後、ホストインテグリティは、要件を満たさない管理下システムを隔離します。

[ホストインテグリティの仕組み](#)

- **システムロックダウン:** 良好であることが分かっているアプリケーションの実行を許可し、不良であることが分かっているアプリケーションの実行をブロックします。どちらのモードでも、システムロックダウンはチェックサムとファイルの場所のパラメータを使って、アプリケーションが承認済みであるか、未承認であるかを検証します。システムロックダウンは、単一のアプリケーションのみを実行するキオスクの場合に役に立ちます。

[システムロックダウンの設定](#)

- **Secure Web Gateway の統合:** プログラム可能な REST API を使用して Secure Web Gateway との統合を可能にし、クライアントコンピュータでの感染の広がりをすばやく止めることができますようにします。
- **EDR コンソール統合:** Symantec Endpoint Protection は、Symantec Endpoint Detection and Response と統合して、攻撃に優先順位を付けることで、ターゲット攻撃や APT (Advanced Persistent Threat) を迅速に検出、応答、遮断するように設計されています。EDR (エンドポイントにおける検出および対応) 機能は Symantec Endpoint Protection に組み込まれています。そのため、エージェントを追加で配備する必要がありません。

[システムロックダウンの設定](#)

Symantec Endpoint Protection 技術が防止する攻撃の種類

次の表に、攻撃の種類と、それぞれに対する保護を提供する Symantec Endpoint Protection 技術の種類を示します。

Table 16: 各 Symantec Endpoint Protection 技術が防止する攻撃の種類

攻撃	高度な機械学習	ヒューリスティック	侵入防止	ネットワーク保護	ポリシー ロックダウン
ゼロデイ	√	√	√		√
ソーシャルエンジニアリング	√	√	√	√	√
ランサムウェア	√	√		√	√
ターゲット攻撃	√	√	√		√
APT (Advanced Persistent Threat)	√	√	√		
ドライブバイダウンロード		√	√		

Symantec Endpoint Protection アーキテクチャコンポーネント

Symantec Endpoint Protection アーキテクチャでは、コンポーネントの 3 つの機能グループが使用されます。一部のコンポーネントには複数の機能があるため、それらのコンポーネントは複数のグループに所属します。



Table 17: 主要なコンポーネント

コンポーネント	説明
つの Symantec Endpoint Protection Manager	つの Symantec Endpoint Protection Manager は、会社のネットワークに接続するクライアントコンピュータに対するイベント、ポリシー、クライアント登録を管理する管理サーバーです。 つの Symantec Endpoint Protection Manager には次のサブコンポーネントが含まれます。 - 管理サーバーソフトウェアはクライアントコンピュータとコンソール間のセキュア通信を提供します。 - コンソールは管理サーバーへのインターフェースです。コンソールソフトウェアはセキュリティポリシー、クライアントコンピュータ、レポート、ログ、ロール、アクセス、管理機能、セキュリティを調整し、管理します。リモートコンソールをインストールし、ネットワーク接続を備えたコンピュータから管理サーバーにログオンするために使うこともできます。 - つの Symantec Endpoint Protection Manager と共にインストールされるデータベースにはセキュリティポリシーとイベントが格納されます。また、自動的にインストールされた Microsoft SQL Server Express (14.3 RU1 以降) または埋め込みデータベース (14.3 MP1 以前) の代わりに、Microsoft SQL Server データベースを使用するようにインストールすることもできます。SQL Server は、コンピュータ数が 5000 台を超える大規模な組織に推奨されます。Symantec Endpoint Protection Manager は、ローカルまたはリモートの Microsoft SQL Server データベースと通信します。 つの Symantec Endpoint Protection Manager のインストール
Symantec Endpoint Protection クライアント	Symantec Endpoint Protection クライアントはソリューションのセキュリティ保護の部分を提供します。クライアントは、つの Symantec Endpoint Protection Manager からポリシーや場合によってはコンテンツをダウンロードして、Windows、Mac、Linux で実行します。

Symantec Endpoint Protection は、管理サーバー、GUP、社内の LiveUpdate サーバー、インターネットからクライアントがコンテンツをダウンロードすることを可能にします。

Table 18: オプションのコンポーネントとその機能

コンポーネント	説明
LiveUpdate Administrator	LiveUpdate Administrator は定義、シグネチャ、その他のコンテンツを社内の LiveUpdate サーバーからダウンロードしてクライアントコンピュータに更新を配布します。非常に規模が大きいネットワークでは、社内 LiveUpdate サーバーを使って Symantec Endpoint Protection Manager の負荷を軽減できます。組織が複数のシマンテック製品を実行していて、それらもライブアップデートを使ってクライアントコンピュータを更新している場合にも社内ライブアップデートサーバーを使います。 LiveUpdate Administrator は、「Download LiveUpdate Administrator (LUA)」から入手できます。 クライアント上のコンテンツを更新するための配布方法の選択 社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定
グループ更新プロバイダ (GUP)	GUP は組織内でのコンテンツの配布に役立ちます。特に、最小限の帯域幅しかないリモートの場所のグループにとって有用です。多くのクライアントがある組織では、Windows クライアントに GUP を使うことを推奨します。GUP は管理サーバーの負荷を軽減し、その設定は社内 LiveUpdate サーバーよりも簡単です。 クライアントにコンテンツを配布するための GUP の使用
Symantec Endpoint Security クラウドコンソール	Symantec Endpoint Security は、クラウドからクライアントコンピュータを管理するために使用する管理コンソールです。Symantec Endpoint Security は、オンプレミス Symantec Endpoint Protection の完全なクラウド管理バージョンです。以下のいずれかのオプションを使用してコンピュータを管理できます。 • つの Symantec Endpoint Protection Manager (オンプレミスのみ) • つの Symantec Endpoint Protection Manager と Symantec Endpoint Security から (ハイブリッド: オンプレミスとクラウド) Symantec Endpoint Protection Manager コンソールからドメインをクラウドコンソールに登録する • Symantec Endpoint Security (クラウドのみ) Symantec Endpoint Protection から Symantec Endpoint Security へのアップグレード Symantec Endpoint Security は、クラウド製品とオンプレミス製品を 1 つの場所に統合するクラウドプラットフォームである Symantec ICDm (Integrated Cyber Defense Manager) 上で実行されます。

Symantec Endpoint Protection は、セキュリティの向上と製品の管理に役立つ複数のツールを備えています。

[Symantec Endpoint Protection に含まれるツール](#)

[Symantec Endpoint Protection 技術でコンピュータが保護される仕組み](#)

始めましょう

Symantec Endpoint Protection をすぐに起動して実行する

セキュリティの必要条件を評価し、デフォルト設定でパフォーマンスと必要なセキュリティとのバランスが得られるかどうかを判断します。パフォーマンス向上のためのいくつかの手順を つの Symantec Endpoint Protection Manager のインストール直後に実行できます。

ネットワークのコンピュータをすぐにインストールして保護するには、次のタスクを実行します。

- [ステップ 1: インストール構造の計画](#)
- [ステップ 2: つの Symantec Endpoint Protection Manager の準備とインストール](#)
- [ステップ 3: グループ、ポリシー、場所の追加](#)
- [ステップ 4: パフォーマンスを高めるための通信設定の変更](#)
- [ステップ 5: 製品のライセンスのアクティブ化](#)
- [ステップ 6: クライアントの配備方法の決定](#)
- [ステップ 7: クライアントのインストールの準備](#)
- [ステップ 8: クライアントソフトウェアの配備とインストール](#)
- [ステップ 9: 想定したグループにコンピュータが所属していることと、クライアントコンピュータが管理サーバーと通信していることの確認](#)

管理サーバーのインストール後に実行するタスク

ステップ 1: インストール構造の計画

製品をインストールする前に、ネットワークのサイズと地理的な配布を考慮してインストール構造を決定します。

ネットワークとデータベースの優れたパフォーマンスを実現するには、いくつかの要素を評価する必要があります。こうした要素には、保護が必要なコンピュータの数、それらのコンピュータが広域ネットワークで接続されているかどうか、コンテンツ更新のスケジュールの頻度が含まれます。

- 1箇所の地理的場所に存在する 500 クライアント未満の小規模なネットワークである場合、1 つの つの Symantec Endpoint Protection Manager のみをインストールする必要があります。
- ネットワークが非常に大規模な場合、追加のデータベースを含む追加サイトをインストールし、複製を利用してデータを共有するように設定できます。また、冗長性を強化するために、追加サイトをインストールしてフェールオーバーや負荷分散を可能にすることもできます。フェールオーバーおよび負荷分散は Microsoft SQL Server データベースでのみ使うことができます。
- ネットワークが地理的に分散している場合は、管理サーバーを追加インストールして、負荷や帯域幅を分散しなければならない可能性があります。

中規模から大規模のインストールを計画するために役立つ情報については、「[Symantec Endpoint Protection のサイジングおよび拡張性のベストプラクティスのホワイトペーパー](#)」を参照してください。

ネットワークアーキテクチャの注意事項

サイトと複製の設定

フェールオーバーと負荷分散の設定

ステップ 2: つの Symantec Endpoint Protection Manager の準備とインストール

1. 管理サーバーをインストールするコンピュータがシステムの最小必要条件を満たしていることを確認します。
「[Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)」を参照してください。
2. つの Symantec Endpoint Protection Manager をインストールするには、ローカルの管理者アクセスを許可されたアカウントを使用してログオンする必要があります。

-
3. デフォルトの Microsoft SQL Server Express データベースを使うか Microsoft SQL Server データベースを使うかを決定します。

Microsoft SQL Server データベースを使う場合は、追加の手順を実施する必要があります。これには、混合モードまたは Windows 認証モードを使用するように設定されているデータベースインスタンスの設定または作成が含まれます。このほかの手順が必要になる場合もあります。また、データベースやデータベースユーザーを作成するために、データベースサーバーの管理資格情報も必要になります。これらは管理サーバーで使用するためのものです。

[SQL Server の設定について](#)

[フェールオーバーと負荷分散の設定](#)

4. 最初に 1 つの Symantec Endpoint Protection Manager をインストールします。インストールした直後に、管理サーバー設定ウィザードを使ってインストールを設定します。

管理サーバーを設定するときに次の項目を決定します。

- 管理コンソールにログオンするためのパスワード
- 重要な通知やレポートを受け取る電子メールアドレス
- 暗号化パスワード (インストール時に選択するオプションに応じて必要になります)

[1 つの Symantec Endpoint Protection Manager のインストール](#)

[基本管理サーバー設定について](#)

[インストール後の 1 つの Symantec Endpoint Protection Manager の設定](#)

ステップ 3: グループ、ポリシー、場所の追加

1. グループを使ってクライアントコンピュータを組織化し、各グループに異なるレベルのセキュリティを適用します。デフォルトグループを使うか、ネットワークで Active Directory または LDAP サーバーを使う場合はデフォルトグループを使います。または新しいグループを追加します。

新しいグループを追加する場合は、次のグループ構造を基礎として使うことができます。

- デスクトップ
- ノートブック
- サーバー

[Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート](#)

[グループを構成する方法](#)

[グループの追加](#)

2. 場所を使うと、特定条件に基づいて異なるポリシーと設定をコンピュータに適用できます。たとえば、コンピュータが会社のネットワークの内側にあるか外側にあるかに基づいて、異なるセキュリティポリシーをコンピュータに適用できます。一般に、ファイアウォールの外側から会社のネットワークに接続するコンピュータには、ファイアウォールの内側にあるコンピュータよりも厳しいセキュリティが必要です。

場所により、オフィス内にないモバイルコンピュータがシマンテック社の LiveUpdate サーバーから自動的に定義を更新できるようにすることが可能です。

「[Symantec Endpoint Protection の場所の認識機能に関するベストプラクティス](#)」を参照してください。] の順にクリックします。

[グループへの場所の追加](#)

3. 別のポリシーまたは設定を使うグループまたは場所の継承を無効にします。

デフォルトでは、グループはデフォルトの親グループ [My Company] のポリシーと設定を継承します。子グループに別のポリシーを割り当てる場合または場所を追加する場合は、最初に継承を無効にする必要があります。次に、子グループのポリシーを変更するか、場所を追加できます。

NOTE

1 つの Symantec Endpoint Protection Manager ポリシーの継承は、クラウドから受信したポリシーには適用されません。クラウドポリシーは、クラウドで定義された継承に従います。

[グループの継承の無効化](#)

4. ポリシーの各タイプについては、デフォルトのポリシーを受け入れるか、新規ポリシーを作成し変更して、新しい各グループまたは場所に適用します。クライアントコンピュータに対して効果をもたらすようにするには、ホストインテグリティ検査のデフォルトのホストインテグリティポリシーに必要条件を追加する必要があります。

ステップ 4: パフォーマンスを高めるための通信設定の変更

各グループの次のクライアントサーバー通信の設定の修正によってネットワークパフォーマンスを改善できます。

- プッシュモードではなくプルモードを使って、クライアントがネットワークリソースを使っていつポリシーとコンテンツ更新をダウンロードするかを制御します。
- ハートビートの間隔を増やします。サーバーあたりのクライアント数が 100 よりも少ない場合、ハートビート間隔を 15 分から 30 分の間に延長します。クライアント数が 100 から 1,000 の場合は、ハートビート間隔を 30 分から 60 分の間に延長します。環境の規模が大きいほど、長いハートビート間隔が必要です。[すぐにクライアントに重要なイベントをアップロードさせる] にチェックマークを付けたままにすることを推奨します。
- ダウンロードのランダム化の間隔は、ハートビート間隔の 1 倍から 3 倍の間に延ばします。

[デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化](#)

[プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新](#)

ステップ 5: 製品のライセンスのアクティブ化

製品インストールから 60 日以内にライセンスを購入してアクティブ化します。

[Symantec Endpoint Protection のライセンス交付](#)

[Symantec Endpoint Protection 製品ライセンス用語](#)

[Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート](#)

ステップ 6: クライアントの配備方法の決定

お使いの環境のコンピュータにクライアントソフトウェアをインストールする上で最適なクライアント配備方法を判別します。

[クライアント配備ウィザードを使ったクライアントのインストール方法の選択](#)

- Linux クライアントの場合、パッケージの保存または **Web** リンクと電子メールを使うことができますが、リモートプッシュは使うことができません。
- Windows と Mac クライアントでは、[リモートプッシュ] を使う場合、次のタスクを実行しなければならない場合があります。
 - 管理者がリモートクライアントコンピュータにアクセスできることを確認します。つの Symantec Endpoint Protection Manager とクライアントコンピュータ間のリモート配備を許可するように、既存のファイアウォール設定 (ポートやプロトコルを含む) を修正します。
[Symantec Endpoint Protection の通信ポート](#)
 - ローカルの管理者アクセスを与えるアカウントを使用してログオンする必要があります。
クライアントコンピュータが Active Directory ドメインの一部である場合、クライアントコンピュータにローカル管理者アクセスを付与するアカウントを使って、つの Symantec Endpoint Protection Manager をホストするコンピュータにログオンする必要があります。Active Directory ドメインの一部でない各クライアントコンピュータについては、管理者のクレデンシャルを用意しておく必要があります。

[リモート配備用 Windows と Mac コンピュータの準備](#)

[クライアントインストールの準備](#)

ステップ 7: クライアントのインストールの準備

1. クライアントソフトウェアをインストールするコンピュータがシステムの最小必要条件を満たしていることを確認します。つの Symantec Endpoint Protection Manager のホストコンピュータにクライアントをインストールする必要があります。

「[Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)」を参照してください。

2. Symantec Endpoint Protection クライアントインストーラがアンインストールできないサードパーティソフトウェアプログラムを Windows コンピュータから手動でアンインストールします。

この機能が削除する製品の一覧については、「[SEP の他社製セキュリティソフトウェア削除のサポートについて](#)」を参照してください。

Linux コンピュータまたは Mac コンピュータから既存のセキュリティソフトウェアをアンインストールする必要があります。

一部のプログラムでは、特別なアンインストールルーチンがある場合や、自己防衛コンポーネントを無効にする必要がある場合があります。サードパーティソフトウェアのマニュアルを参照してください。

3. 14 では、標準の方法ではアンインストールされない Windows Symantec Endpoint Protection クライアントを削除するようインストールパッケージを設定できます。そのプロセスが完了すると、Symantec Endpoint Protection をインストールします。

[既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定](#)

ステップ 8: クライアントソフトウェアの配備とインストール

1. Windows クライアントの場合は、次のタスクを実行します。
 - クライアントコンピュータにインストールするコンポーネントを決定するカスタムクライアントインストール機能セットを作成します。デフォルトのクライアントインストール機能セットのいずれかを使うこともできます。

[Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート](#)

ワークステーションのクライアントインストールパッケージについては、環境内のメールサーバーに適用される電子メールスキャナの保護オプションを確認します。たとえば、Microsoft Exchange メールサーバーを使う場合は、[Microsoft **Outlook** スキャナ] を確認します。

- カスタムクライアントインストール設定を更新して、クライアントコンピュータのインストールオプションを決定します。これらのオプションには、対象インストールフォルダ、サードパーティセキュリティソフトウェアのアンインストール、インストール完了後の再起動の動作が含まれます。デフォルトのクライアントインストール設定を使うこともできます。

[クライアントにインストールするセキュリティ機能の選択](#)

2. クライアント配備ウィザードで、利用可能なオプションを選択してクライアントインストールパッケージを作成し、クライアントコンピュータに配備します。クライアント配備ウィザードでは、Mac または Windows のコンピュータに配備することのみが可能です。

- [Web リンクと電子メールを使った Symantec Endpoint Protection クライアントのインストール](#)
- [リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール](#)
- [パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール](#)
- [クライアントインストールパッケージのエクスポート](#)

Symantec Endpoint Protection のインストールと同時にサードパーティのインストールを実行することは推奨しません。ネットワークレベルまたはシステムレベルの変更を加えるサードパーティプログラムをインストールすると、Symantec Endpoint Protection をインストールするときに望ましくない結果を引き起こすことがあります。可能な場合は、Symantec Endpoint Protection をインストールする前にクライアントコンピュータを再起動します。

ステップ 9: 想定したグループにコンピュータが所属していることと、クライアントコンピュータが管理サーバーと通信していることの確認

管理コンソールの [クライアント] > [クライアント] ページで以下を行います。

1. 表示を [クライアントの状態] に変更し、各グループのクライアントコンピュータが管理サーバーと通信していることを確認します。

次の列の情報を参照します。

 - [名前] 列では、管理サーバーに接続されているクライアントには緑のドットが表示されます。
[クライアントが管理サーバーに接続され、保護されているかどうかの確認](#)
 - [前回の状態変更があった日時] 列には、各クライアントが最後に管理サーバーと通信した時刻が表示されます。
 - [再起動が必要] 列は、保護を有効にするためにクライアントコンピュータを再起動する必要があるかどうかを表示します。

つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動

- [ポリシーのシリアル番号] 列には、最新のポリシーシリアル番号が表示されます。1 つから 2 つのハートビートの間、ポリシーが更新されないことがあります。ポリシーがすぐに更新されない場合は、クライアント上で手動でポリシーを更新できます。

ポリシーのシリアル番号を使ったクライアントとサーバーの通信の確認

クライアントポリシーの更新

2. [保護技術] ビューに変更し、[ウイルス対策の状態] から [改変対策の状態] までの列に [オン] が設定されていることを確認します。

クライアントコンピュータの保護状態の表示

3. クライアントで、クライアントがサーバーに接続されていることを確認し、ポリシーのシリアル番号が最新であることを確認します。

クライアントコンピュータの管理サーバーへの接続のチェック

クライアントが管理サーバーに接続され、保護されているかどうかの確認

つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング

Symantec Endpoint Protection 14.x のクイックスタートガイド

このガイドは、デフォルトで 500 クライアント以下の初回管理下インストール向けに設計されている Symantec Endpoint Protection のダウンロード、インストール、設定を支援します。

アップグレードは、「[Symantec Endpoint Protection \(SEP\) の最新リリースへのアップグレードおよび移行](#)」を参照してください

- インストール前: システム要件を確認する
- ステップ 1: Symantec Endpoint Protection インストールファイルをダウンロードする
- ステップ 2: Symantec Endpoint Protection Manager をインストールする
- ステップ 3: ライセンスをアクティブ化しグループを追加する
- ステップ 4: Symantec Endpoint Protection のクライアントをインストールする
- ステップ 5: 最新の定義がインストールされているかを確認する
- ステップ 6: データベースバックアップ設定を確認する
- 付録 A: 追加のリソースとガイド
- インストール前: システム要件を確認する
- インストール前: システム要件を確認する

インストール前: システム要件を確認する

つの Symantec Endpoint Protection Manager または Symantec Endpoint Protection クライアントをインストールする前に、次のステップを実行してください:

1. [SymDiag](#) をダウンロードし、インストール前の点検を実行して、コンピュータがシステム要件を満たしていることを確認します。
2. 「[Symantec Endpoint Protection のリリースノートおよびシステム要件](#)」を確認します。

ステップ 1: Symantec Endpoint Protection インストールファイルをダウンロードする

最新バージョンの Symantec ソフトウェアおよびツールをダウンロードし、ライセンスキーを取得し、[Broadcom サポートポータル](#)から製品をアクティブ化します。次のサイトを参照してください。

- [Symantec スタートガイド](#)。それから、[オンプレミスセキュリティ製品] まで下にスクロールします。
- [シマンテックソフトウェアの最新バージョンをダウンロードする](#)

ステップ 2: Symantec Endpoint Protection Manager をインストールする

Broadcom サポートポータルから Symantec ソフトウェアを検索またはダウンロードできない場合は、[カスタマーケア](#)にお問い合わせください。

1. Symantec Endpoint Protection のインストールファイルをダウンロードしたフォルダで、ファイルをダブルクリックしてすべてのファイルを抽出します。[ファイルを開く - セキュリティの警告] のプロンプトが表示されたら、[実行] をクリックします。
2. インストールのバージョンに応じて、以下のいずれかの処理を実行します。
 - バージョン **14.2 MP1a (14.2.1023.0100)** 以降の場合、ファイルは C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX になります。この XXXXXXXXXX は、文字と数字のランダムな文字列を表します。Setup.exe が自動的に起動します。インストールが完了するまで、インストールメニューを開いたままにします。メニューを閉じると、一時ディレクトリ内のすべてのファイルが削除されます。
インストールファイルを保存するには、前述の一時フォルダに移動し、選択した場所にその内容をコピーします。インストールファイルには、[Tools] ディレクトリが含まれています。
 - バージョン **14.2 MP1a (14.2.1023.0100)** より前のバージョンでは、抽出する場所を入力するか、または参照して、[抽出] をクリックします。抽出が完了したら、Setup.exe を探してダブルクリックします。
3. [**Symantec Endpoint Protection** のインストール] をクリックします。
4. 使用許諾契約の条項に同意してインストールを続行し、すべてのプロンプトをデフォルト設定で受け入れて、[インストール] をクリックします。
5. [管理サーバー設定ウィザードによるこそ] パネルで、[デフォルト設定] をクリックし、[次へ] をクリックします。
SQL Server データベースを使うなど、インストールをカスタマイズする場合は、[カスタム設定] をクリックします。
6. システム管理者のアカウントを作成するのに必要なフィールドに入力し、つの Symantec Endpoint Protection Manager が通知を送信するのに使用する電子メールアドレスを入力したら、[次へ] をクリックします。
管理サーバーからの通知とパスワードのリセットの電子メールを受信するには、メールサーバーを設定する必要があります。また、指定されたメールサーバー情報を入力して、[テスト電子メールの送信] をクリックすることもできます。操作を続行する前に、テスト電子メールの受信を確認する必要があります。
7. 次のオプションから選択して、[次へ] をクリックします。
 - インストールが完了したら、LiveUpdate を実行するかどうか。インストール中に LiveUpdate を実行することをお勧めします。(14.3 MPx 以前)
 - シマンテック社がクライアントからのデータを収集するかどうか。
 - パートナー情報(ライセンスの状況に対して適用される場合)。このステップを完了するには、しばらく時間がかかります。
8. [設定が完了しました] パネルで [完了] をクリックして つの Symantec Endpoint Protection Manager を起動します。
9. つの Symantec Endpoint Protection Manager のログオン画面で、ステップ 6 で作成したユーザー名とパスワードを入力し、ログオンできることを確認します。
デフォルトのユーザー名は admin です。

クライアント数が 500 未満の環境では SQL Server データベースは不要ですが、次の記事で詳しく確認することができます。「[Symantec Endpoint Protection Manager をカスタム設定でインストールする](#)」

14.1 以降では、Symantec Endpoint Protection クラウドコンソールを使用して Symantec Endpoint Protection Manager を登録するオプションがあります。インストールが完了した後はいつでも Symantec Endpoint Protection Manager ドメインを登録できます。「[Symantec Endpoint Protection Manager コンソールからドメインをクラウドコンソールに登録する](#)」を参照してください。

ステップ 3: ライセンスをアクティブ化しグループを追加する

Symantec Endpoint Protection Manager にログオンすると、[始めましょう] 画面が表示され、共通タスクの複数のリンクが示されます。たとえば、ライセンスをアクティブ化したり、Symantec Endpoint Protection クライアントを配備したりできます。

この画面は、Symantec Endpoint Protection Manager の右上隅の [ヘルプ] > [始めましょうページ] をクリックして、いつでも開くことができます。Symantec Endpoint Protection Manager におけるその他の一般的なタスクのビデオツアーについては、[製品ツアー] をクリックしてください。

製品のライセンスをアクティブ化するには:

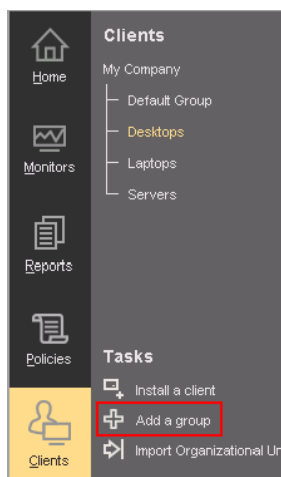
1. [始めましょう] 画面の [ライセンス状態] で、[製品をアクティブ化します] をクリックします。
2. シリアル番号または注文処理の電子メールに含まれる .SLF ライセンスファイルを使用し、プロンプトの指示に従ってライセンスをインストールします。

クライアントにグループを追加するには

シマンテック社はデスクトップ、ノートパソコン、サーバーの個別のグループを作成することを推奨します。

1. Symantec Endpoint Protection Manager の左ペインで、[クライアント] をクリックします。
2. [クライアント] の下にある [My Company] をクリックします。
3. [タスク] で、[グループを追加] をクリックします。
4. [My **Company** のグループを追加] ダイアログボックスで、グループ名と説明を入力し、[OK] をクリックします。

その後、ポリシー継承などのグループ設定をさらに設定できます。



ステップ 4: Symantec Endpoint Protection クライアントのインストール

Symantec Endpoint Protection Manager を使用してクライアントをインストールする前に、次の項目を確認します。

- ネットワーク経由でコンピュータにアクセスできることを確認します。
- 配備先のコンピュータに管理者の資格情報があることを確認します。

管理外クライアントのインストールに関しては、「[管理外 Windows クライアントのインストール](#)」を参照してください。

1. つの Symantec Endpoint Protection Manager の左ペインで、[クライアント] をクリックします。
2. [クライアント] で、前に作成したグループを選択します。
3. [タスク] で、[クライアントのインストール] をクリックします。
4. [クライアント配備ウィザードによる] パネルで [新しいパッケージ配備] をクリックし、[次へ] をクリックします。
5. [インストールパッケージ] ドロップダウンリストで、クライアントコンピュータのオペレーティングシステムに一致するオペレーティングシステムを選択します。
6. 前のステップで選択したオペレーティングシステムにより、以下のオプションを選択します。
 - **Windows** のインストールパッケージ:

- [インストール機能セット] ドロップダウンリストで、デフォルト設定の [クライアントの完全保護] を維持します。
- [インストールの設定] ドロップダウンリストで、デフォルト設定の [デフォルトの Windows 用標準クライアントインストール設定] を維持します。
これらのデフォルト設定には再起動が必要です。再起動の設定を変更するには、カスタムのクライアントパッケージを最初に追加する必要があります。クライアントパッケージを追加したら、[オプション] をクリックしてカスタムパッケージを選択します。「[Symantec Endpoint Protection Manager でカスタムクライアントインストールパッケージを作成する方法](#)」を参照してください。
- [コンテンツオプション] の横にあるチェックボックスでチェックマークを付けるか、またははずしてウイルス定義を含めるかどうかを選択し、[次へ] をクリックします。

– **Mac** のインストールパッケージ:

[アップグレードの設定] のデフォルト設定を維持し、[次へ] をクリックします。

– **Linux** のインストールパッケージ:

[次へ] をクリックします。Linux のパッケージでは、[Web リンクと電子メール] または [パッケージの保存] の配備方式のみに限定されます。

[Symantec Endpoint Protection for Linux クライアントのインストール \(14.3 MP1 以前\)](#)

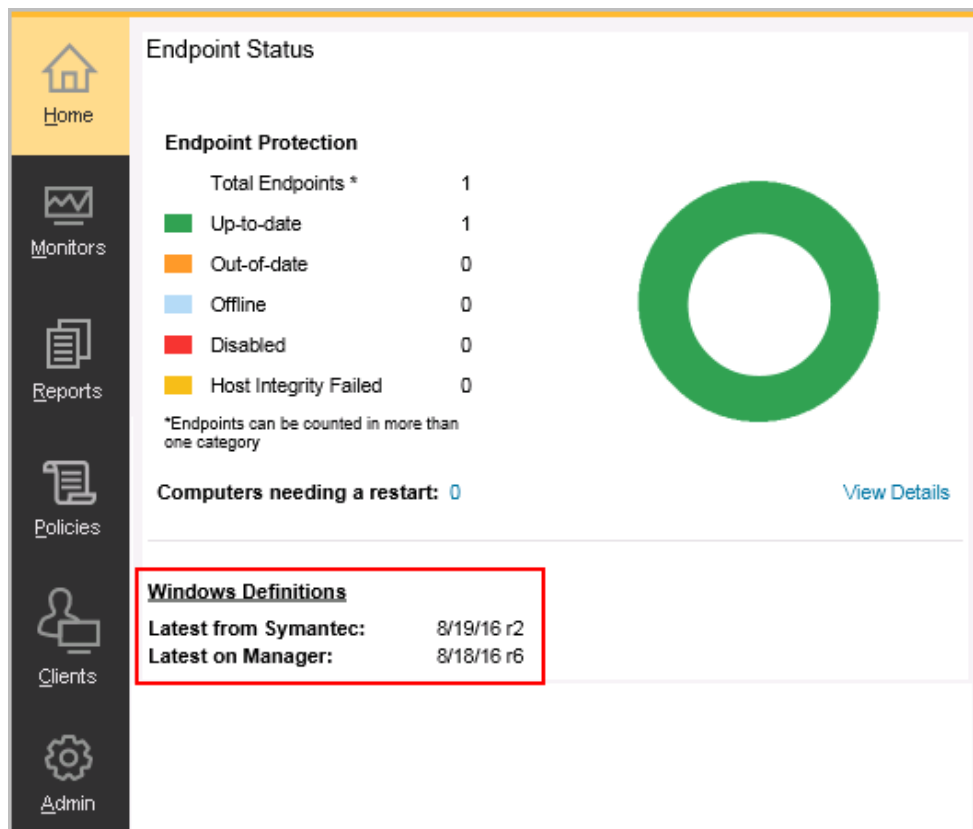
[Symantec Agent for Linux 14.3 RU1 のインストール](#)

7. [リモートプッシュ] をクリックし、[次へ] をクリックします。
8. [ネットワークの参照] タブで、ワークグループまたはドメインを参照し、Symantec Endpoint Protection クライアントをプッシュするターゲットのコンピュータを選択します。コンピュータを選択したら、[>>] オプションをクリックして右ウィンドウにそれらを追加します。
9. 目的のコンピュータを追加したら、[次へ] をクリックします。
10. [送信] をクリックして、処理を開始します。
プッシュインストールが完了すると、プッシュの結果を含む [配備の概略] ウィンドウが表示されます。
11. [次へ] をクリックし、[完了] をクリックして、ウィザードを終了します。
このウィンドウは、インストールファイルが正常にコピーされたことを示します。
12. クライアントが正常にインストールされたかを確認するには、先ほど [クライアント] ペインに追加したクライアントグループ内にそのクライアントが存在することを確認します。

[クライアントが管理サーバーに接続され、保護されているかどうかの確認](#)

ステップ 5: 最新の定義がインストールされているかを確認する

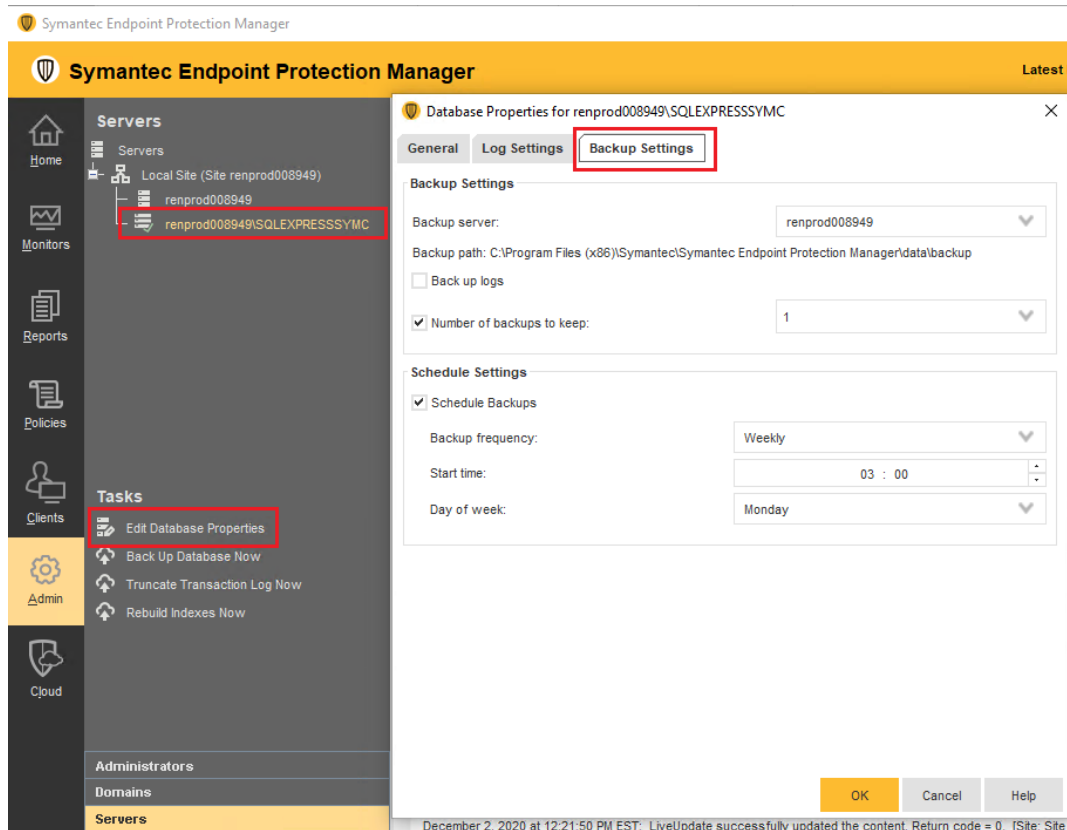
1. つの Symantec Endpoint Protection Manager の左ペインで、[ホーム] をクリックします。
2. [エンドポイントの状態] ボックスの [Windows 定義] で、[管理サーバー上の最新版] と [シマンテック社からの最新版] の日付を比較します。



3. 日付が一致しない場合は、[ヘルプ] > [「始めましょう」ページ] を選択し、[今すぐ LiveUpdate を実行します] をクリックしてから [ダウンロード] をクリックします。

ステップ 6: データベースバックアップ設定を確認する

1. つの Symantec Endpoint Protection Manager の左ペインで、[管理] > [サーバー] をクリックします。
2. [サーバー] で、[ローカルサイト (マイサイト)] > [SQLEXPRESSSYMC] をクリックします。
14.3 MPx 以前の場合は、[localhost] をクリックします。
3. [タスク] の下で、[データベースプロパティの編集] をクリックします。
4. [バックアップの設定] タブで、必要な調整を行い、[OK] をクリックします。
デフォルトでは、バックアップは週に 1 回保存されます。



付録 A: 追加のリソースとガイド

[Symantec Endpoint Protection の製品ガイドとマニュアル](#)

[Symantec Endpoint Protection のベストプラクティス](#)

[Symantec Endpoint Protection で使用する通信ポート](#)

インストール時または設定時に、ユーザー権利がない、またはユーザー権利を読み取れないというエラーが発生する

つの Symantec Endpoint Protection Manager のインストール

管理サーバーとコンソールをインストールする複数のタスクを実行します。インストールウィザードでは、完了した各タスクの横に緑色のチェックマークが表示されます。

最新のシステム必要条件について詳しくは、「[Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)」を参照してください。

一部の製品は 1 つの Symantec Endpoint Protection Manager と同じサーバーにインストールしたときに競合することがあります。これらの製品での必要な設定変更について詳しくは、「[Software compatibility with Symantec Endpoint Protection](#)」を参照してください。

また、1 つの Symantec Endpoint Protection Manager のインストールと設定は、仮想サービスアカウントを正しく実行するために必要な権限についてセキュリティポリシーを調べます。1 つの Symantec Endpoint Protection Manager は自動的にローカルセキュリティポリシーを変更して、ドメインセキュリティポリシーについて行う必要がある変更について警告します。インストール前にセキュリティポリシーを変更することもできます。「[Windows セキュリティポリシーを使い Symantec Endpoint Protection Manager のサービスに必要なユーザー権限を割り当てる](#)」を参照してください。

NOTE

つの Symantec Endpoint Protection Manager は、インストールと通常の操作でシステムレジストリへのフルアクセスを必要とします。つの Symantec Endpoint Protection Manager をリモートでインストールする Windows Server 2003 コンピュータを準備するには、最初にそのコンピュータでリモート制御を許可する必要があります。リモートデスクトップに接続するときに、コンソールセッションを使うか、リモートデスクトップでコンソールセッションをシャドウする必要もあります。

NOTE

IPv6 ネットワークで つの Symantec Endpoint Protection Manager 14.2 をインストールする場合、IPv4 が無効になっている場合でも Java が IPv4 スタックを使用できるようにする必要があります。IPv4 スタックがアンインストールされている場合、Java は動作せず、つの Symantec Endpoint Protection Manager のインストールが失敗します。

Symantec Endpoint Protection Manager をインストールするには

1. 製品をダウンロードした場合は、インストールファイル全体をハードディスクなどの物理ディスクに抽出します。物理ディスクから **Setup.exe** を実行します。

インストールは自動的に開始します。開始しない場合は、インストールファイルを開き、**Setup.exe** をダブルクリックします。

2. [**Symantec Endpoint Protection** インストールプログラム] ダイアログボックスで、[**Symantec Endpoint Protection** のインストール]、[つの **Symantec Endpoint Protection Manager** のインストール] の順に選択します。
3. インストールイベントのシーケンスを調べ、[次へ] をクリックして開始します。
4. [使用許諾契約] パネルで、[使用許諾契約の条項に同意します] をクリックし、[次へ] をクリックします。
5. [インストール先フォルダ] パネルで、デフォルトのインストール先フォルダを受け入れるか、または別のインストール先フォルダを指定して、[次へ] をクリックします。
6. [インストール] をクリックします。

つの Symantec Endpoint Protection Manager 管理サーバーとコンソールのインストール処理が開始します。インストールが完了したら、[次へ] をクリックします。

7. 初期インストールが完了した後、サーバーとデータベースを設定します。[次へ] をクリックします。

管理サーバー設定ウィザードが起動します。

[インストール後の つの Symantec Endpoint Protection Manager の設定](#)

[カスタム設定を使った つの Symantec Endpoint Protection Manager のインストール](#)

[つの Symantec Endpoint Protection Manager での初期作業](#)

インストール後の つの **Symantec Endpoint Protection Manager** の設定

管理サーバー設定ウィザードは、つの Symantec Endpoint Protection Manager のインストール後に自動的に開始します。必要条件に従って管理サーバーを設定します。

管理サーバー設定ウィザードは、インストール後いつでも、スタートメニューで [すべてのプログラム] > [Symantec Endpoint Protection Manager] > [Symantec Endpoint Protection Manager Tools] を選択して開始することもできます。

1. つの Symantec Endpoint Protection Manager のインストール

2. [新しいインストールのデフォルト設定] を選択した状態で、[次へ] をクリックします。

デフォルト設定では、デフォルトのデータベースである Microsoft SQL Server Express が自動的にインストールされます (14.3 RU1 以降)。バージョン 14.3 MPx では、埋め込みデータベースがデフォルトとしてインストールされています。

3. 会社名、デフォルト管理者 `admin` のパスワード、電子メールアドレスを入力します。

または、詳細を追加して指定したメールサーバーを使うことができます。

4. 必要に応じて、[テスト電子メールの送信] をクリックします。

つの Symantec Endpoint Protection Manager は、この電子メールアカウントにパスワード回復情報とその他の重要な通知を送信します。この電子メールを受信できない場合は、設定を続行するべきではありません。

5. テスト電子メールの受信を確認したら、[次へ] をクリックします。

14.3 MPx 以前では、インストールの一部として LiveUpdate を実行するかどうかを指定します。[次へ] をクリックします。14.3 RU1 以降、LiveUpdate は新規インストールの一部として自動的に実行されます。

6. パートナーがシマンテックライセンスを管理する場合は、省略可能な [パートナー情報] を追加し、[次へ] をクリックすることもできます。

7. シマンテック社に匿名データを送信するかどうかを指定し、[次へ] をクリックして、データベースの作成を開始します。

データベースの作成には数分かかる場合があります。

8. データベースの作成が完了したら、[完了] をクリックして つの Symantec Endpoint Protection Manager の設定を完了します。

つの Symantec Endpoint Protection Manager コンソールのログオン画面は、つの Symantec Endpoint Protection Manager を起動するオプションにチェックマークを付けたままにすると表示されます。ログオンしたら、クライアントの配備を開始できます。

つの Symantec Endpoint Protection Manager コンソールへのログオン

設定の概略は、つの Symantec Endpoint Protection Manager がインストールされているサーバー上の次の場所で確認できます。

ProgramFiles\Symantec\つの Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

カスタム設定を使った つの Symantec Endpoint Protection Manager のインストール

Microsoft SQL Server データベースを含む つの Symantec Endpoint Protection Manager をインストールする場合、または複数のサイトをインストールする場合は、管理サーバー設定ウィザードで [カスタム設定] を選択する必要があります。このオプションを選択すると、追加の設定が利用可能になります。

NOTE

データベースへの接続を提供するには、つの Symantec Endpoint Protection Manager を動作するサーバーで SQL Server クライアントツールをインストールする必要があります。

SQL Server の設定について

カスタム設定で つの Symantec Endpoint Protection Manager をインストールするには

1. つの Symantec Endpoint Protection Manager のインストール

2. [管理サーバー設定ウィザード] パネルで、[新しいインストールのカスタム設定] をクリックして [次へ] をクリックします。

コンピュータ数が 500 未満の場合は、[新しいインストールのカスタム設定] をクリックすることをお勧めします。

インストール後の つの Symantec Endpoint Protection Manager の設定

3. [1 つ目のサイトをインストールする] をクリックし、[次へ] をクリックします。

次のオプションは、拡張インストール用なので、つの Symantec Endpoint Protection Manager の初回のインストールには適用されません。

- [既存のサイトに追加の管理サーバーをインストールする] については、「[フェールオーバーと負荷分散の設定](#)」を参照してください。
- [追加サイトをインストールする] については、次を参照してください。

[サイトと複製の設定](#)

[複製のための 2 番目のサイトのインストール方法](#)

[複製のしくみ](#)

4. この画面では、次の設定をカスタマイズできます。その後に [次へ] をクリックします。

- サイト名
- サーバー名
- ポート番号

ただし、つの Symantec Endpoint Protection Manager のデフォルトのポート設定を変更する前に、ネットワーク管理者に連絡してください。

- つの Symantec Endpoint Protection Manager サーバーデータフォルダの場所
つの Symantec Endpoint Protection Manager をインストールしたドライブの空き容量が十分でない場合は、サーバーデータフォルダを代替ドライブに再配置します。

5. データベース選択画面で、[Microsoft **SQL Server** データベース] をクリックし、[次へ] をクリックします。

- クライアント数が 5,000 以下のカスタム設定でデフォルトの **Microsoft SQL Server Express** データベースを選択する場合は、ステップ 9 に移動します。ただし、残りの手順は、Microsoft SQL Server データベースを選択することを前提としています。
- 自動データベース保守タスクを有効にする必要があるかどうかを SQL データベースの管理者に確認してください。
- シマンテック社は、SQL Server と つの Symantec Endpoint Protection Manager を物理的に個別のサーバーでホストすることを推奨します。
- Microsoft SQL Server のサポートされているバージョンについては、「[Symantec Endpoint Protection のシステム要件](#)」を参照してください。

6. [新しいデータベースを作成する] をクリックし、[次へ] をクリックします。

NOTE

既存のデータベースの使用は拡張インストールのオプションと見なされ、通常は新しいインストールに適用されません。

7. [ステップ 1: データベースサーバー認証] 画面で、つの Symantec Endpoint Protection Manager の接続先の SQL Server の詳細を入力し、[データベースに接続] をクリックします。

データベースが正常に接続されたら、[ステップ 2: 新しいデータベースの作成] セクションが利用可能になります。

-
8. [ステップ 2: 新しいデータベースの作成] で、新しいデータベースを作成するための詳細を入力し、[次へ] をクリックします。
[データベースサーバー認証] または [データベースの作成] に関する質問がある場合は、SQL Server データベースの管理者に連絡してください。
 9. 会社名、デフォルト管理者 admin のパスワード、電子メールアドレスを入力します。
または、詳細を追加して指定したメールサーバーを使うことができます。
 10. [テスト電子メールの送信] をクリックします。テスト電子メールの受信を確認したら、[次へ] をクリックします。
この Symantec Endpoint Protection Manager は、この電子メールアカウントにパスワード回復情報とその他の重要な通知を送信します。この電子メールを受信できない場合は、設定を続行するべきではありません。
 11. 暗号化パスワードを作成するか、またはランダムパスワードを使うことを選択して [次へ] をクリックします。
このパスワードは、クライアントとこの Symantec Endpoint Protection Manager 間の通信を保護するために使われ、この Symantec Endpoint Protection Manager 回復ファイルに格納されます。
 12. インストールの一部として LiveUpdate を実行するかどうかを指定します。新規インストールの一部として LiveUpdate を実行すると、配備するクライアントが容易にコンテンツを入手できます。[次へ] をクリックします。
パートナーがシマンテックライセンスを管理する場合は、省略可能な [パートナー情報] を追加することもできます。
 13. シマンテック社に匿名データを送信するかどうかを指定し、[次へ] をクリックして、データベースの作成を開始します。
 14. データベースを作成、初期化したら (数分かかることがあります)、[完了] をクリックします。
この Symantec Endpoint Protection Manager コンソールのログオン画面は、この Symantec Endpoint Protection Manager を起動するオプションにチェックマークを付けたままにすると表示されます。ログオンしたら、クライアントの配備を開始できます。

[この Symantec Endpoint Protection Manager コンソールへのログオン](#)

設定の概略は、この Symantec Endpoint Protection Manager がインストールされているサーバー上の次の場所で確認できます。

ProgramFiles\Symantec\この Symantec Endpoint Protection Manager\tomcat\etc\SEPMConfigurationSummaryInfo.txt

[データベースの種類の選択について](#)

この Symantec Endpoint Protection Manager コンソールへのログオン

この Symantec Endpoint Protection Manager をインストールすると、この Symantec Endpoint Protection Manager コンソールにログオンすることになります。コンソールにログオンする方法は、2 つあります。

1. 管理サーバーをインストールしたコンピュータからローカルでログオンする。
[この Symantec Endpoint Protection Manager へのローカルでのログオン](#)
管理サーバーに接続したスタンドアロンの Web ブラウザからレポート機能にアクセスすることもできます。
[スタンドアロン Web ブラウザからのレポートへのログオン](#)
2. リモートコンソールのシステムの必要条件を満たし、管理サーバーへのネットワーク接続性のあるコンピュータからリモートにログオンする。リモート Web コンソールまたはリモート Java コンソールにログオンできます。
[リモートからのこの Symantec Endpoint Protection Manager へのログオン](#)

セキュリティを確保するため、コンソールは最大 1 時間後にユーザーをログアウトします。この時間は短くすることができます。

つの Symantec Endpoint Protection Manager コンソールへのログオン状態を維持するためのタイムアウト期間の変更

コンソールへのローカルでのログオン

コンソールにローカルでログオンするには

1. スタートメニューで [プログラム] > [つの Symantec Endpoint Protection Manager] > [つの Symantec Endpoint Protection Manager] に移動します。
2. **Symantec Endpoint Protection Manager** のログオンダイアログボックスで、インストール時に設定したユーザー名 (デフォルトは `admin`) とパスワードを入力します。
オプションで、利用できる場合は、[ユーザー名を記憶する] と [パスワードを記憶する] のいずれかまたはその両方にチェックマークを付けます。

[パスワードを忘れた場合] リンクを表示して、管理者が紛失したパスワードをリセットできるようにする

- PIV カードまたは CAC を使用してログオンするには、[オプション] をクリックして、[スマートカードにログオンする] にチェックマークをます (14.2 以降)。[ログインと PIN] メッセージに PIN 番号を入力します。

スマートカードでログオンする管理者を認証するように つの Symantec Endpoint Protection Manager を設定する

- 2 要素認証を使用してログオンするには、パスワードを入力して直後にトークンを入力します。トークンを省略すると、ログオンが失敗します。Symantec VIP スマートフォンアプリを使用する場合、パスワードを入力して、[ログオン] をクリックした後、アプリケーションで要求を承認します。2 分以内に要求を承認しない場合、ログオンが失敗します。

Symantec VIP を使用した 2 要素認証の設定

コンソールに複数のドメインがある場合は、[オプション] をクリックしてドメイン名を入力します。 [ドメインの追加](#)

3. [ログオン] をクリックします。

リモートからのコンソールへのログオン

リモートでログオンするには、管理サーバーがインストールされているコンピュータの IP アドレスまたはホスト名が必要です。また、Web ブラウザのインターネットオプションで、ログオンするサーバーの内容を表示できることと、Web ブラウザがサポートされていることも確認してください。サポート対象の Web ブラウザのリストは、以下を参照してください。

Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件

IP アドレスまたはホスト名を検索するには

1. ローカルでログオンします。
2. [ホーム] ページの [お気に入りレポート] で、[保護技術別のリスク分布] をクリックします。
3. [保護技術別のリスク分布] ダイアログボックスの下部で、次のテキストを探します。「Symantec Endpoint Protection Manager を <http://SEPMServer:9090/symantec.html> を使用して起動できます」。

リモートでログオンすると、ローカルでログオンした管理者と同じタスクを実行できます。コンソールから表示できる内容および実行できる項目は、管理者の種類によって異なります。小規模組織の管理者のほとんどは、システム管理者としてログオンします。Microsoft Windows Server 2008 および Windows 7 では、リモートコンソールにアクセスするコンピュータの管理者権限が必要で、管理者権限を使用して実行する必要があります。管理者権限を使用して起動するように、コンソールアイコンまたは [スタート] メニュー項目を設定できます。

管理者権限でリモートコンソールを起動するには

1. Windows デスクトップで [Symantec Endpoint Protection Manager コンソール] アイコン、または [スタート] メニューで [Symantec Endpoint Protection Manager コンソール] のエントリを右クリックします。
2. [プロパティ] > [詳細設定] > [管理者として実行] または [その他] > [管理者として実行] をクリックします。

Windows Server 2016 の場合、管理サーバーがインストールされているコンピュータのホスト名を使います。

NOTE

以前のバージョンの製品でリモート Java コンソールをインストールした場合は、新しいバージョンにアップグレードするときに再インストールする必要があります。14.3 以降では、32 ビットバージョンの Windows を実行している場合、Symantec Endpoint Protection Manager シックリモートコンソールにログインできません。Oracle Java SE Runtime Environment は、32 ビットバージョンの Microsoft Windows をサポートしなくなりました。14.3 以降、リモート Web コンソールは JRE バージョン 11 を使用します。

コンソールにリモートでログインするには

1. サポート対象の Web ブラウザを開き、アドレスボックスに次のアドレスを入力します。

`http://SEPMServer:9090/symantec.html`

ここで、SEPMServerは管理サーバーのホスト名または IP アドレスです。

IP アドレスには、IPv4 と IPv6 が含まれます (14.2 以降)。IPv6 アドレスは角カッコで囲む必要があります。例:

`http://[SEPMServer]:9090/symantec.html`

2. つの Symantec Endpoint Protection Manager コンソールの [Web アクセス] ページで、希望するコンソールの種類をクリックします。

[つの **Symantec Endpoint Protection Manager Web** コンソール] をクリックすると、安全な Web ページがロードされるので JRE (Java Runtime Environment) を使わずにリモートでログインできます。

[つの **Symantec Endpoint Protection Manager** コンソール] を選択する場合は、ログインするコンピュータに JRE をインストールして Java クライアントを実行する必要があります。インストールされていない場合は、ダウンロードしてインストールする必要があります。表示されるメッセージに従って JRE をインストールし、その他の指示にも従います。

他のオプションはリモート管理ソリューションではありません。[つの **Symantec Endpoint Protection Manager 証明書**] をクリックすると、管理コンソールの証明書ファイルのダウンロードを求めるメッセージが表示されます。必要に応じて、このファイルを Web ブラウザにインポートできます。

3. ホスト名メッセージが表示されたら、[はい] をクリックします。

このメッセージは、指定したリモートコンソールの URL が つの Symantec Endpoint Protection Manager の証明書名と一致していないことを示します。管理サーバーのコンピュータ名と異なる IP アドレスを指定してログインした場合にこの問題が生じます。

Web ページのセキュリティ証明書の警告が表示されたら [このサイトの閲覧を続行する (推奨されません)。] をクリックし、自己署名証明書を追加します。

4. 画面のメッセージに従ってログイン処理を完了します。

インストールの後で最初にログインするときは、アカウント名に `admin` を使います。

ログイン方法によっては、追加情報を指定する必要がある場合もあります。たとえば、コンソールに複数のドメインがある場合は、[オプション] をクリックし、ログインするドメインの名前を指定します。

5. Javaベースのコンソールを使う場合は、ユーザー名とパスワードを保存するオプションがある場合があります。[ログイン] をクリックします。

リモートコンソールの起動時に、1 つ、または複数のセキュリティ警告メッセージが表示される場合があります。表示された場合、[はい]、[実行]、[開始]などを、コンソールが表示されるまでクリックします。

つの Symantec Endpoint Protection Manager コンソールで必要な自己署名証明書を受け入れることが必要な場合もあります。

[リモート つの Symantec Endpoint Protection Manager コンソールのアクセスの認可または遮断](#)

[つの Symantec Endpoint Protection Manager コンソールへのログイン前に管理者が見るメッセージの表示](#)

[つの Symantec Endpoint Protection Manager 用の自己署名されたサーバー証明書の受け入れについて](#)

Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート

ライセンスアクティブ化ウィザードのワークフローを使って、次のタスクを実行できます。

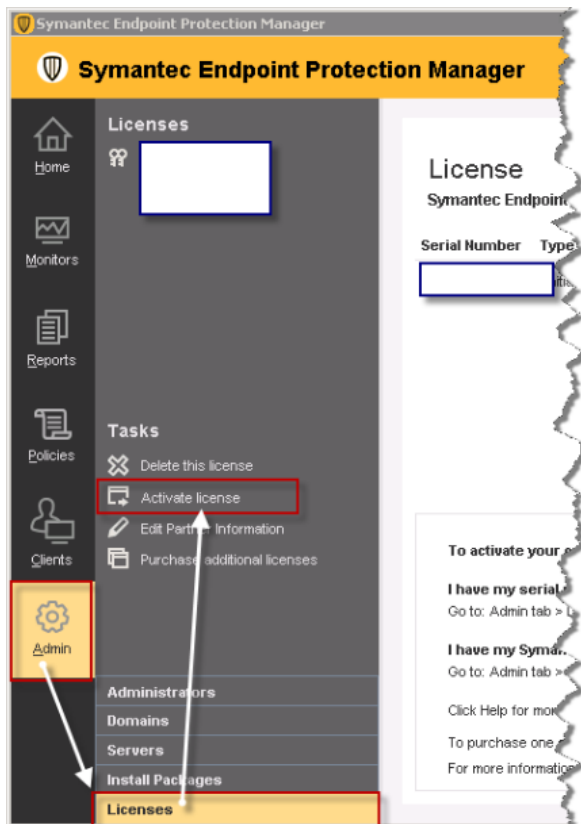
次の方法でライセンスアクティブ化ウィザードを起動できます。

- 製品のインストール後に表示される [始めましょう] 画面
[ヘルプ]、[始めましょう] ページの順に移動して [始めましょう] 画面にアクセスすることもできます。
- つの Symantec Endpoint Protection Manager コンソールの [管理] ページ

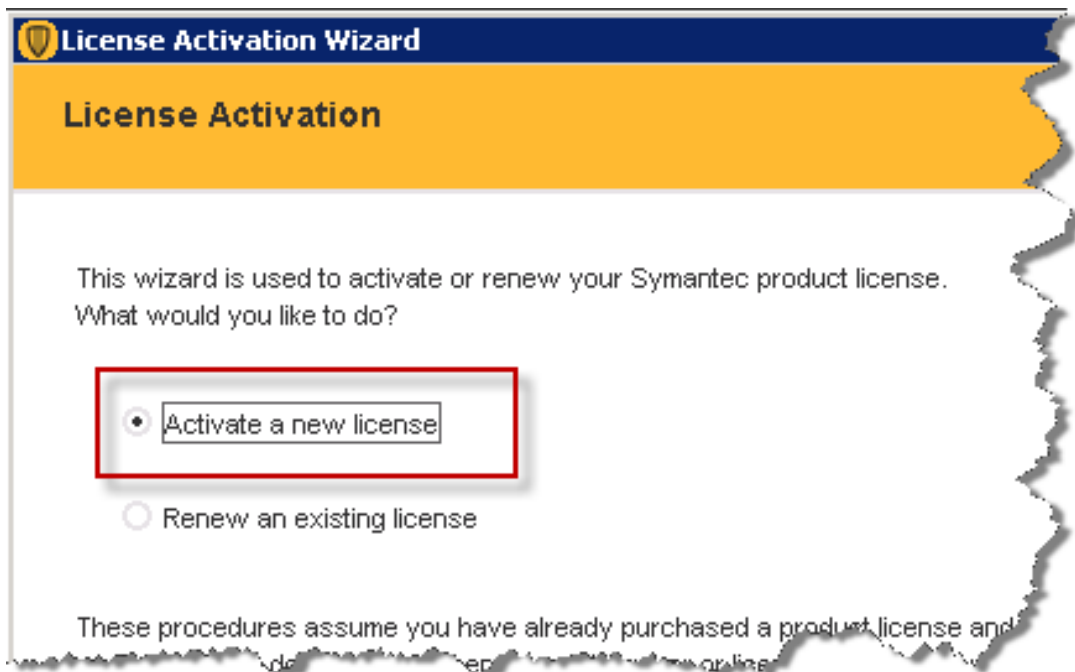
[始めましょう] 画面からライセンスをアクティブ化またはインポートする場合は、ステップ 3 にスキップできます。

Symantec Endpoint Protection 製品ライセンスをアクティブ化またはインポートするには :

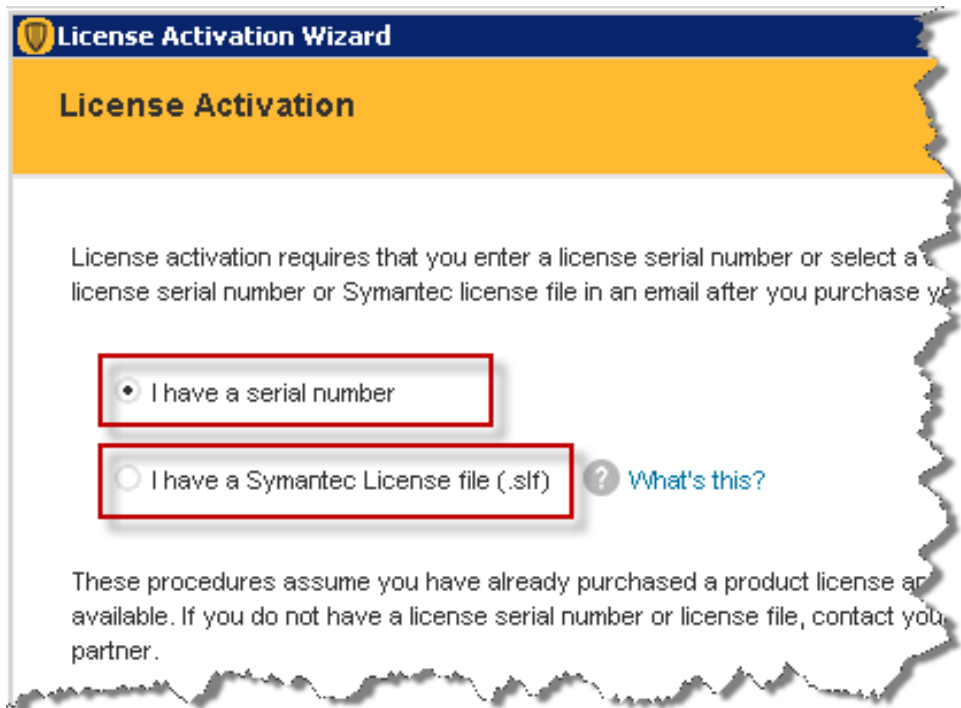
1. つの Symantec Endpoint Protection Manager で、[管理] > [ライセンス] をクリックします。
2. [タスク] で、[ライセンスをアクティブ化する] をクリックします。



3. [新しいライセンスをアクティブ化する]をクリックし、[次へ]をクリックします。このパネルが表示されない場合は、次の手順に進みます。



4. [ライセンスのアクティブ化] パネルで、状況に合致するオプションを選択して、[次へ] をクリックします。



次の表に各オプションの説明を示します。

オプション	説明
シリアル番号がある場合	ユーザーまたは正規代理店がライセンスを購入したときに、ライセンスシリアル番号を受け取る場合があります。ライセンスシリアル番号がある場合は、このオプションを選択します。 シリアル番号がある場合は、[シマンテックライセンスファイルがある場合] を選択します。

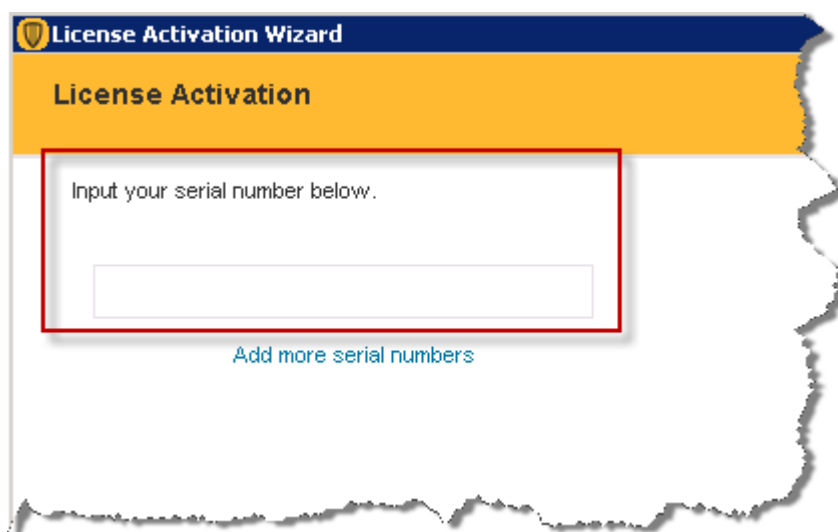
シマンテックライセンスファイル (.slf) がある場合	ほとんどの場合、シマンテックライセンスファイル (.slf ファイル) は、購入プロセスの完了後すぐに電子メールで Broadcom から送信されます。このファイルは通常、.zip ファイルとして通知電子メールに添付されます。.slf ファイルを受信した場合は、このオプションを選択します。 Note: 製品ライセンスをアクティブ化するために使う前に、.zip ファイルから .slf ファイルを抽出する必要があります。 Warning! .slf ファイルにはライセンスに一意の情報が含まれています。破損を避けるため、ライセンスファイルの内容は変更しないでください。記録のためにファイルをコピーできます。

5. 前の手順で行った選択に応じて、次のタスクのいずれかを行います。

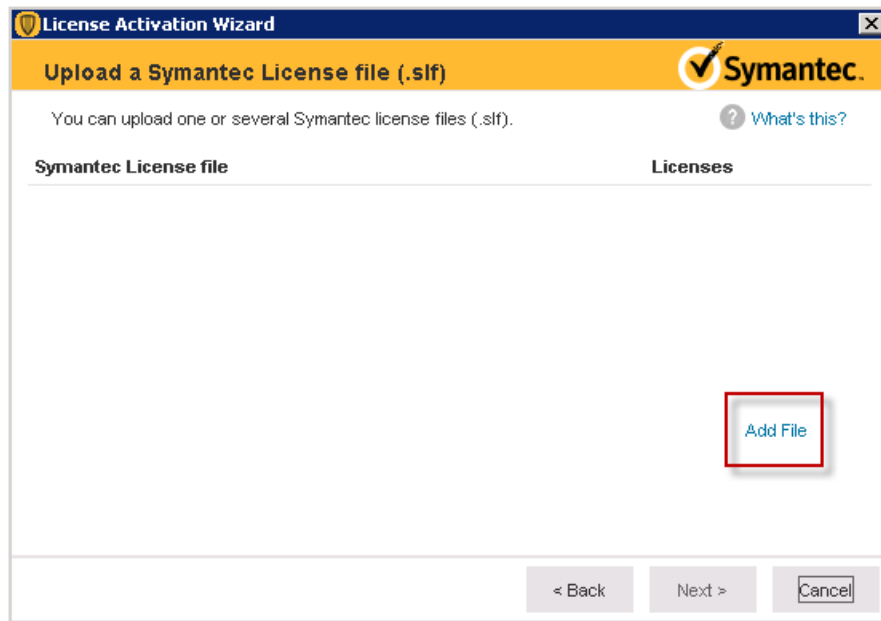
- [シリアル番号がある場合] を選択した場合は、シリアル番号を入力し、[提出] をクリックします。追加したライセンスについての情報を見直してから、[次へ] をクリックします。

NOTE

シリアル番号があるライセンスをアクティブ化するには、インターネット接続がアクティブで Symantec Licensing Server にアクセスできる必要があります。接続が成功すると、シマンテック社のホームページがロードされます。



- [シマンテックライセンスファイル (.slf) がある場合] を選択した場合は、[ファイルの追加] をクリックします。シマンテック社からの通知電子メールに添付されていた .zip ファイルから抽出した .slf ファイルを参照して選択します。[開く] をクリックし、[次へ] をクリックします。



6. 技術担当者、責任者、会社に関する情報を入力します。クリックして開示に関する声明を確認してから、[提出] をクリックします。

ライセンスを購入したときにこの情報を提供した場合、このパネルは表示されません。

7. [完了] をクリックします。

[Symantec Endpoint Protection ライセンスの購入](#)

[Symantec Endpoint Protection のライセンス交付](#)

Symantec Endpoint Protection ライセンスの購入

次の場合にライセンスを購入する必要があります。

- 試用ライセンスが期限切れになった場合。Symantec Endpoint Protection には、使用環境に製品をインストールし、評価できる試用ライセンスが付属しています。
- 現在のライセンスが期限切れになった場合。
- 現在のライセンスが過剰配備された場合。過剰配備とは、現在のライセンスで配備可能なクライアント数より多くのクライアントを配備していることを意味します。

ライセンスの購入方法に応じて、製品ライセンスのシリアル番号またはシマンテックライセンスファイルのどちらかを電子メールで受け取ります。ライセンスファイルは拡張子.sif を使います。電子メールでライセンスファイルを受信するときは、.zip ファイルとして電子メールに添付されます。.zip ファイルから .sif ファイルを抽出する必要があります。

ライセンスを購入または更新するには、以下のようにします。

- [正規代理店](#)にお問い合わせください。

つの Symantec Endpoint Protection Manager コンソールからアクセスできるコンピュータにライセンスファイルを保存します。多くのユーザーは、つの Symantec Endpoint Protection Manager をホストするコンピュータにライセンスを保存します。多くのユーザーはまた、ライセンスを安全に保管するために、ライセンスのコピーを別のコンピュータまたは取りはずし可能なストレージメディアに保存します。

WARNING

ライセンスファイルの破損を防ぐため、決してファイルの内容を開いたり、変更しないでください。ただし、必要に応じてライセンスをコピーして保管しておくことができます。

[Symantec Endpoint Protection 製品ライセンスの必要条件](#)

パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール

クライアントが少数の場合は、クライアントでインストールパッケージを配備、インストールする方法としてパッケージの保存を使います。

パッケージの保存では、サードパーティの配備ソフトウェアまたはログインスクリプトを使って手動でインストールできるインストールパッケージを作成します。

パッケージの保存は次のタスクで構成されます。

- 設定の選択を行い、クライアントインストールパッケージを作成します。
- つの Symantec Endpoint Protection Manager を実行するコンピュータのフォルダにインストールパッケージを保存します。

Windows の場合、インストールパッケージは 32 ビットまたは 64 ビットのオペレーションシステムに対応します。インストールパッケージは、1 つの setup.exe ファイル、または setup.exe ファイルを含むファイル群から構成されます。多くの場合、コンピュータユーザーは、1 つの setup.exe ファイルのほうが使いやすいと考える。

NOTE

Mac と Linux クライアントインストールパッケージは .zip アーカイブファイル形式で自動的にエクスポートされます。ファイル権限を正しく保持するには、Mac の #####などのネイティブアーカイブプログラムまたは ditto コマンドを使って、アーカイブファイルを展開する必要があります。Mac の unzip コマンド、サードパーティアプリケーション、Windows アプリケーションを使ってこれらのオペレーティングシステム用のファイルを展開できません。

パッケージの保存を使って Symantec Endpoint Protection クライアントをインストールするには

1. コンソールで、クライアント配備ウィザードを起動します。
[ヘルプ]、[始めましょう] ページをクリックして [必須タスク] で [コンピュータにクライアントソフトウェアをインストールします。] をクリックします。
2. クライアント配備ウィザードで、次のいずれかのタスクを実行します。
 - [新しいパッケージ配備] をクリックし、[次へ] をクリックします。パッケージの保存では、新しいインストールパッケージのみがインストールされます。
 - Symantec Endpoint Protection クライアントがすでにインストールされているコンピュータの Windows または Mac クライアント通信設定を更新する場合は、[通信の更新パッケージの配備] をクリックします。画面の指示に従い、ステップ 4 に進みます。
3. インストールパッケージのタイプによって異なる、利用可能なオプションから選択を行い、[次へ] をクリックします。

NOTE

既存のセキュリティソフトウェアを Windows クライアントからアンインストールするには、クライアントの配備ウィザードを開始する前に、カスタムのクライアントインストールの設定を行う必要があります。

[既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定](#)

[Windows クライアントのインストール設定について](#)

-
4. [パッケージの保存] をクリックし、[次へ] をクリックします。
 5. [参照] をクリックして、パッケージを受け取るフォルダを指定します。
通信の更新パッケージの配備、または Mac と Linux パッケージの場合は、「[[次へ](#)] をクリック」のステップに進みます。
新しい Windows パッケージの場合は、[単一の .exe ファイル (デフォルト)] または [個々のファイル (.MSI に必要)] にチェックマークを付けます。

NOTE

サードパーティの配備プログラムのために別のファイルが必要な場合を除き、[単一の .exe ファイル] を使います。

6. [次へ] をクリックします。
7. 設定の概略を確認して [次へ] をクリックし、[完了] をクリックします。
8. エクスポートしたパッケージコンピュータユーザーに提供します。
エクスポートされたパッケージを、電子メールで送信するか、安全な共有ネットワークの場所に保存するか、サードパーティプログラムを使うかのいずれかの方法で、ユーザーに提供します。
9. ユーザーがクライアントソフトウェアをダウンロードしてインストールしたことを確認します。また、クライアントのインストール状態も確認します。

新しい Symantec Endpoint Protection のインストールでは、クライアントコンピュータは自動的に再起動または管理者やユーザーが操作して再起動しないと つの Symantec Endpoint Protection Manager 内部に表示されないことがあります。インストールが完了すると、Mac クライアントは自動的に再起動を求めるメッセージを表示します。Linux クライアントでは再起動は不要です。

[Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動](#)

[クライアントの配備の状態についてのレポートの実行](#)

[クライアントにインストールするセキュリティ機能の選択](#)

[クライアント配備ウィザードを使ったクライアントのインストール方法の選択](#)

[クライアントインストールの準備](#)

Symantec Endpoint Protection for Mac クライアントのインストール

リモートプッシュを使えない場合や、使わない場合には、Symantec Endpoint Protection クライアントを Mac コンピュータに直接インストールできます。手順は、クライアントが対象外または対象下に関係なくほぼ同じです。

管理下クライアントをインストールする唯一の方法は、つの Symantec Endpoint Protection Manager で作成されるパッケージを使用することです。管理外クライアントは、クライアント/サーバーの通信設定を Mac クライアントにインポートすることでいつでも管理下クライアントに変換できます。

NOTE

サードパーティリモート配備ソフトウェアでの使用に向けた Symantec Endpoint Protection for Mac クライアントの準備については、「[Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper](#)」を参照してください。

Table 19: Mac クライアントをインストールする方法

インストールファイルをダウンロードした場合。	1. Mac コンピュータでその内容をフォルダに展開し、フォルダを開きます。 2. SEP_MAC を開きます。 3. Symantec Endpoint Protection.dmg を Mac コンピュータのデスクトップにコピーします。 4. Symantec Endpoint Protection.dmg をダブルクリックして、仮想ディスクとしてファイルをマウントします。Symantec Endpoint Protection for Mac クライアントをインストールします。
Broadcom サポートポータル からクライアントインストールパッケージの.zip をダウンロードした場合	1. ファイルを Mac コンピュータのデスクトップにコピーします。ファイルには、Symantec Endpoint Protection.zip または Symantec Endpoint Protection version Mac_Client.zip という名前が付いています。ここで、version は製品バージョンです。 2. [開く] > [アーカイブユーティリティ] の順に右クリックして、ファイルの内容を展開します。 3. 結果のフォルダを開きます。Symantec Endpoint Protection for Mac クライアントをインストールします。

展開した仮想ディスクイメージやフォルダは、アプリケーションインストーラと Additional Resources というフォルダを含んでいます。正常にインストールするには、これらの項目が両方とも同じ場所に存在する必要があります。別の場所にインストーラをコピーする場合は、Additional Resources もコピーする必要があります。

Mac 用 Symantec Endpoint Protection クライアントをインストールするには

1. #Symantec Endpoint Protection ##### をダブルクリックします。
2. インストールを開始するには、[インストール] をクリックします。
3. Symantec Endpoint Protection クライアントをインストールするのに必要なヘルパーツールをインストールするには、Mac の管理者ユーザー名およびパスワードを入力し、[ヘルパーのインストール] をクリックします。
4. インストール後、[続行] をクリックして、Symantec Endpoint Protection クライアントの設定を終了します。
5. Symantec Endpoint Protection クライアントを設定するには、以下の手順に従います。

Symantec Endpoint Protection システム拡張を許可します。	[セキュリティとプライバシー] ダイアログボックスの [全般] タブの「アプリケーション "Symantec Endpoint Protection" からのシステムソフトウェアのロードがブロックされました」で、[許可] をクリックします。 必要に応じて、ロックアイコンをクリックして変更を行います。 Symantec Endpoint Protection が完全に機能するためには、システム拡張を認証する必要があります。 Symantec Endpoint Protection for macOS 10.15 以降でのシステム拡張の認証について
ディスクへのフルアクセスを許可します。	[セキュリティとプライバシー] ダイアログボックスの [プライバシー] タブで、[Symantec System Extension (Symantec システム拡張)] が、Mac デバイスのすべてのユーザーのデータと管理設定にアクセスできることを確認します。 必要に応じて、ロックアイコンをクリックして変更を行います。
ネットワークプロファイルへの変更を許可します。	Symantec Endpoint Protection でネットワークコンテンツをフィルタするかどうかを確認するメッセージが表示されたら、[許可] をクリックします。

6. [完了] をクリックします。

Symantec Endpoint Protection for macOS 10.15 以降でのシステム拡張の認証について

macOS 10.15 以降のセキュリティ機能として、システム拡張の認証が必要になります。Symantec Endpoint Protection が完全に機能するためには、システム拡張を認証する必要があります。

Symantec Endpoint Protection のシステム拡張を認証するには、Symantec Endpoint Protection クライアントの設定中に、[セキュリティとプライバシー] ダイアログボックスの [全般] タブの「アプリケーション "Symantec Endpoint Protection" からのシステムソフトウェアのロードがブロックされました」で、[許可] をクリックします。

Mac 用 Symantec Endpoint Protection クライアントのインストール

Mac 用 Symantec Endpoint Protection クライアント配備時のカーネル拡張の承認管理

Mac 用 Symantec Endpoint Protection を大量配備する場合、追加の手順を実行して、カーネル拡張が承認されていることを確認しなければならない場合があります。この必要条件は macOS 10.13 (High Sierra) から適用されます。このオペレーティングシステムではローカルコンピュータで承認を行う必要があります。カーネル拡張はリモートアクセスを通じて承認できず、事前設定のディスクイメージを通じてカーネル承認を保存することもできません。

カーネル拡張が Mac で正しく承認されていることを確認するには、次のいずれかを実行します。

- Mac ユーザーに必要な拡張の承認を指示します。ユーザーは、管理者権限を持たない場合も、[セキュリティとプライバシー] の環境設定ペインを通してカーネル拡張を承認できます。

[Symantec Endpoint Protection for macOS 10.13 以降でのカーネル拡張の認証について](#)

- モバイルデバイス管理 (MDM) ソリューションに Mac を登録します。このソリューションを使用して積極的に Mac を管理するに関わらず、この登録により、カーネル拡張承認は macOS 10.13 より前の従来の実行方法に戻ります。
- macOS 10.13.2 以降では、チーム識別子を使用して、Mobile Device Management (MDM) からカーネル拡張を認証できます。macOS で Symantec Endpoint Protection のカーネル拡張を認証するには、チーム識別子 `9PTGMPNXZ2` を使用します。このチーム識別子を使用する方法については、MDM スイートのマニュアルを参照してください。

NOTE

Mac 14.3 用の Symantec Endpoint Protection クライアントから、チーム識別子は `Y2CCP3S9W7`、システム拡張名は `com.broadcom.mes.systemextension` になりました。

- **NetBoot**、**NetInstall**、または **NetRestore** を使用する場合は、次のコマンドを使用して、配備用にディスクイメージを準備します。

```
spctl kext-consent add 9PTGMPNXZ2
```

このコマンドは Symantec チーム識別子を使用し、Mac 上の Symantec カーネル拡張を事前承認します。

このコマンドによって設定されたチーム識別子は非揮発性ランダムアクセスメモリ (NVRAM) に保存され、Mac の電源がオフになっても維持されます。NVRAM をリセットすると、カーネル拡張は再承認を要求します。ユーザーが [セキュリティとプライバシー] ペインからカーネル拡張を承認した場合も、再承認は必要ありません。

カーネル拡張のロードについて詳しくは、次の Apple のマニュアルを参照してください。

[macOS High Sierra のカーネル機能拡張の変更点について準備を進める](#)

Symantec Agent for Linux または Symantec Endpoint Protection for Linux クライアントのインストール

(14.3 RU1 以降の場合)

Linux デバイスに Symantec Agent for Linux を直接インストールします。Linux エージェントを つの Symantec Endpoint Protection Manager からリモートで配備することはできません。

Symantec Agent for Linux をインストールするには、つの Symantec Endpoint Protection Manager でインストールパッケージを作成し、インストールパッケージを Linux デバイスに転送してから、インストーラを実行します。インストーラは、新しいエージェントを設定し、それを つの Symantec Endpoint Protection Manager に登録します。

NOTE

Symantec Agent for Linux 14.3 RU1 以降は、管理外クライアントとして実行できません。すべての管理タスクは、つの Symantec Endpoint Protection Manager またはクラウドコンソールで実行する必要があります。

(14.3 RU1 以降の場合) Symantec Management Agent for Linux をインストールするには

1. つの Symantec Endpoint Protection Manager で、インストールパッケージを作成してダウンロードします。
2. Linux デバイスに LinuxInstaller パッケージを移動します。
3. LinuxInstaller ファイルを実行可能にします。
`chmod u+x LinuxInstaller`
4. インストーラを実行します。
`./LinuxInstaller`
root としてコマンドを実行する必要があります。
インストールオプションのリストを表示するには、`./LinuxInstaller -h` を実行します。
5. インストールを検証するには、`/usr/lib/symantec` に移動し、`./status.sh` を実行して、モジュールがロード済みでデーモンが実行されていることを確認します。
`./status.sh`
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent running
sisamdagent running
sisidsagent running
sisipsagent running
Module status:
sisevt loaded
sisap loaded
communication status はクラウド管理のクライアントでのみ利用可能です。

(14.3 MP1 以前の場合)

管理外または管理下の Symantec Endpoint Protection クライアントを直接 Linux コンピュータにインストールします。Linux クライアントをつの Symantec Endpoint Protection Manager からリモートで配備することはできません。インストールの手順は、クライアントが対象外または対象下に関係なくほぼ同じです。

管理下クライアントは、つの Symantec Endpoint Protection Manager で作成するインストールパッケージを使ってのみインストールできます。管理外クライアントは、クライアント/サーバーの通信設定を Linux クライアントにインポートすることでいつでも管理下クライアントに変換できます。

Linux オペレーティングシステムのカーネルがコンパイル済み自動保護カーネルモジュールと互換性がない場合、インストーラは互換性のある自動保護カーネルモジュールのコンパイルを試みます。自動コンパイルプロセスは、必要に応じて自動的に起動します。ただし、インストーラは互換性のある自動保護カーネルモジュールをコンパイルできないことがあります。その場合、自動保護はインストールされますが、無効になります。詳細については、次を参照してください。

Symantec Endpoint Protection でサポートされる Linux のカーネル

NOTE

Linux コンピュータで Symantec Endpoint Protection クライアントをインストールするにはスーパーユーザーの権限が必要です。この手順では、`sudo` を使って権限の昇格を説明します。

(14.3 MP1 以前の場合) Symantec Endpoint Protection for Linux クライアントをインストールするには

1. 作成したインストールパッケージを Linux コンピュータにコピーします。パッケージは .zip ファイルです。
2. Linux コンピュータで、ターミナルアプリケーションウィンドウを開きます。
3. 次のコマンドを使ってインストールディレクトリに移動します。
`cd /directory/`
ここで、directory は .zip ファイルをコピーしたディレクトリの名前です。

-
4. 次のコマンドを使って、.zip ファイルの内容を tmp というディレクトリに抽出します。

```
unzip "InstallPackage" -d sepfiles
```

ここで、InstallPackage は .zip ファイルの完全名、sepfiles は抽出処理によりインストールファイルが配置されるデスティネーションフォルダを表します。

デスティネーションフォルダが存在しない場合は、抽出処理によって作成されます。

5. 次のコマンドを使って sepfiles に移動します。

```
cd sepfiles
```

6. install.sh の実行ファイルの権限を正しく設定するには、次のコマンドを使います。

```
chmod u+x install.sh
```

7. 次のコマンドで、組み込みスクリプトを使って Symantec Endpoint Protection をインストールします。

```
sudo ./install.sh -i
```

パスワードの入力を求めるメッセージが表示されたらパスワードを入力します。

このスクリプトは Symantec Endpoint Protection コンポーネントのインストールを開始します。デフォルトのインストールディレクトリは次のとおりです：

```
/opt/Symantec/symantec_antivirus
```

ライブアップデートのデフォルトの作業ディレクトリは次のとおりです。

```
/opt/Symantec/LiveUpdate/tmp
```

コマンドプロンプトが返されるとインストールの完了です。インストールを完了するためにコンピュータを再起動する必要はありません。

(14.3 MP1 以前の場合) クライアントインストールを検証するには、Symantec Endpoint Protection の黄色のシールドをクリックまたは右クリックし、[**Symantec Endpoint Protection** を開く] をクリックします。黄色のシールドの位置は Linux のバージョンによって異なります。クライアントユーザーインターフェースにプログラムバージョン、ウイルス定義、サーバー接続状態、管理に関する情報が表示されます。

[Symantec Endpoint Protection for Linux クライアントの自動コンパイルについて](#)

[Linux クライアントの GUI について](#)

[Linux クライアントへのクライアントとサーバーの通信設定のインポート](#)

[クライアントインストールの準備](#)

[Redhat ベースのディストリビューションの Symantec Endpoint Protection 14.x のインストール](#)

Linux エージェントを始めましょう

つの Symantec Endpoint Protection Manager 管理者によって Linux エージェントの設定が許可されていることがあります。

Table 20: Linux エージェントを開始する手順 (14.3 RU1 以降の場合)

手順	タスク	説明
1	Symantec Agent for Linux をインストールします。	管理者から管理下クライアント用のインストールパッケージが提供されるか、インストールパッケージをダウンロードするためのリンクが電子メールで送信されます。 Symantec Agent for Linux または Symantec Endpoint Protection for Linux クライアントのインストール
2	Linux エージェントが つの Symantec Endpoint Protection Manager またはクラウドコンソールと通信していることを確認します。	つの Symantec Endpoint Protection Manager またはクラウドコンソールとの接続を確認するには、以下のコマンドを実行します。 <code>/usr/lib/symantec/status.sh</code>
手順 3	Auto-Protect が動作していることを確認します。	Auto-Protect の状態を確認するには、次のコマンドを実行します。 <code>cat /proc/sisap/status</code>
手順 4	定義が最新であることを確認します。	LiveUpdate 定義は次の場所にあります。 <code>/opt/Symantec/sdcssagent/AMD/sef/definitions/</code>

Table 21: Linux クライアントを開始する手順 (14.3 MP1 以前)

手順	タスク	説明
1	Linux クライアントをインストールします。	つの Symantec Endpoint Protection Manager 管理者から管理下クライアント用のインストールパッケージが提供されるか、インストールパッケージをダウンロードするためのリンクが電子メールで送信されます。 つの Symantec Endpoint Protection Manager と通信しない管理外クライアントをアンインストールすることもできます。一次コンピュータのユーザーは、クライアントコンピュータの管理、ソフトウェアの更新、定義の更新を行う必要があります。管理外クライアントを管理下クライアントに変換できます。 Symantec Agent for Linux または Symantec Endpoint Protection for Linux クライアントのインストール
2	Linux クライアントが つの Symantec Endpoint Protection Manager と通信していることを確認します。	Symantec Endpoint Protection のシールドをダブルクリックします。クライアントが つの Symantec Endpoint Protection Manager と正常に通信している場合は、[管理] の [サーバー] の横にサーバー情報が表示されます。[オフライン] と表示される場合は、つの Symantec Endpoint Protection Manager 管理者に連絡してください。 [自己管理] と表示される場合は、クライアントが管理外です。 シールドアイコンは管理状態と通信状態を両方とも示します。
手順 3	Auto-Protect が動作していることを確認します。	Symantec Endpoint Protection のシールドをダブルクリックします。[状態] の [自動保護] の横に Auto-Protect の状態が表示されます。 次のコマンドラインインターフェースで Auto-Protect の状態を確認することもできます。 <code>sav info -a</code>
手順 4	定義が最新であることを確認します。	インストールが完了すると、LiveUpdate が自動的に起動します。Symantec Endpoint Protection シールドをダブルクリックしたときに、定義が更新されていることを確認できます。[定義] に定義日が表示されます。デフォルトでは、LiveUpdate for the Linux クライアントは 4 時間おきに実行されます。 定義が最新でない可能性がある場合は、[LiveUpdate] をクリックして LiveUpdate manually を手動で実行できます。次のコマンドラインインターフェースを使って LiveUpdate を実行することもできます。 <code>sav liveupdate -u</code>

手順	タスク	説明
手順 5	スキャンを実行します。	デフォルトでは、管理下の Linux クライアントは、毎日午前 12 時 30 分にすべてのファイルとフォルダをスキャンします。ただし、以下のコマンドラインインターフェースを使って手動スキャンを開始できます。 <pre>sav manualscan -s <パス名></pre> Note: 手動スキャンを開始するコマンドを実行するには、スーパーユーザーの権限が必要です。

[Symantec Endpoint Protection for Linux によく寄せられる質問 \(SEP for Linux FAQ \)](#)

Symantec Endpoint Protection client for Linux の自動コンパイルについて

(14.3 MP1 以前の場合)

オペレーティングシステムカーネルが事前コンパイルされた Auto-Protect カーネルモジュールと互換性がない場合、Symantec Endpoint Protection for Linux インストーラは Auto-Protect カーネルモジュールを自動コンパイルします。Symantec Endpoint Protection にはこの機能が 12.1.6 で導入されています。

インストールプロセスの終了間際にクライアントインストーラがアクティブな Auto-Protect モジュールを検出しない場合、自動コンパイラを起動し、互換性のあるモジュールをコンパイルします。

以前は、Linux コンピュータのオペレーティングシステムがサポート対象のカーネルを実行したときに Auto-Protect のみが機能しました。または、Auto-Protect カーネルモジュールを手動でコンパイルできます。

前提条件

自動コンパイルが機能するように、次の開発ツールが Linux クライアントコンピュータ上にある必要があります。

- kernel-devel
- kernel-source
- linux-headers
- build-essentials
- "開発ツール"

Symantec Endpoint Protection カーネルモジュールは、ソースが変更された Linux カーネル上で正常にコンパイルを行わない場合があります。そのような Linux カーネルはこの機能でサポートされません。

自動コンパイルの使用

自動コンパイルは必要に応じてインストール時に自動的に起動します。自動コンパイルを起動するための操作は不要です。

自動コンパイルプロセスが正常に完了すると、ターミナルウィンドウに以下が表示されます。

ソースコードからのビルド Auto-Protect カーネルモジュールが正常に実行されました

自動コンパイルプロセスで作成される symap および symev のカスタムドライバではファイル名に **custom** が含まれます。ファイル `sepfl-install.log` も自動コンパイルが正常に実行されたことを確認します。このファイルはデフォルトで `~/` に保存されます。

自動コンパイルプロセスが失敗すると、Auto-Protect はインストールしますが、無効のままになります。ターミナルウィンドウには次のようなメッセージが表示されます。

ソースコードからのビルド Auto-Protect カーネルモジュールが次のエラーで失敗しました: Number

Number はさまざまなエラーコードの番号を示します。受信するエラーコードについて詳細は、コンパイラのマニュアルを参照してください。

Linux クライアントの GUI について

(14.3 MP1 以前の場合)

NOTE

Symantec Agent for Linux 14.3 RU1 には、グラフィカルユーザーインターフェースがありません。

お使いの Linux コンピュータにグラフィカルユーザーインターフェース (GUI) が組み込まれている場合、Symantec Endpoint Protection for Linux クライアントの状態トレイには黄色のシールド通知領域アイコンが表示されます。このアイコンは、クライアントが管理サーバーに接続されているかどうか、および保護状態に関する情報を示します。

ほとんどの管理タスクはコマンドラインインターフェースを使って実行します。ただし、次のタスクを実行する場合は、Symantec Endpoint Protection クライアントの GUI を使うことができます。

- 製品のバージョンとウイルス定義に関する情報を確認する。
- Auto-Protect が有効かどうかや、定時スキャンまたは手動スキャンの状態など、クライアントの保護状態を確認する。
- LiveUpdate を実行して最新のウイルス定義と製品の更新を取得する。
- クライアントが管理外であるのか、それとも管理下であるのかに関する情報を取得し、つの Symantec Endpoint Protection Manager に接続して最新のポリシーを受信する。

これらのタスクはコマンドラインから実行することもできます。

Table 22: Symantec Endpoint Protection for Linux クライアントの状態アイコン

アイコン	説明
	クライアントは管理外で、正しく機能しています。アイコンは何も付いていない黄色のシールドです。
	クライアントは管理下で、正しく機能し、つの Symantec Endpoint Protection Manager と正常に通信します。アイコンは緑のドットが付いた黄色のシールドです。
	クライアントは管理下で、正しく機能していますが、つの Symantec Endpoint Protection Manager と正常に通信しません。アイコンは中に黒い感嘆符のある明るい黄色のドットが付いた黄色のシールドです。
	Auto-Protect、リアルタイムスキャンサービス (rtvscand)、クライアント管理サービス (smcd) などのコンポーネントが無効であるため、クライアントは正しく機能できません。アイコンは中央に赤い斜線のある赤く縁取られた白いドット付きの黄色のシールドです。

[Linux クライアントを始めましょう](#)

リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール

リモートプッシュは IP アドレスまたはコンピュータ名を使って、指定したコンピュータにクライアントソフトウェアをプッシュ型で転送します。パッケージが対象コンピュータにコピーされると、パッケージが自動的にインストールされます。コンピュータユーザーはインストールを開始する必要がありません。また、管理者権限も不要です。

リモートプッシュは次のタスクで構成されます。

- 既存のインストールパッケージを選択するか、新しいインストールパッケージを作成するか、または通信設定を更新するパッケージを作成します。
- 新しいインストールパッケージの場合は、インストールパッケージを設定し、作成します。
- ネットワークで 1 つの Symantec Endpoint Protection Manager からパッケージを受け取るコンピュータを指定します。リモートプッシュは、IP 番号または範囲を指定した特定のコンピュータ、またはネットワークを参照すると表示されるすべてのコンピュータを検索します。

NOTE

[ネットワークの参照] タブで Mac クライアントにクライアントインストールパッケージをプッシュ型転送するには、つの Symantec Endpoint Protection Manager サーバーで Bonjour サービスをインストールする必要があります。次の記事を参照してください。

[Bonjour サービスを つの Symantec Endpoint Protection Manager 12.1.5 にインストールする](#)

Bonjour サービスは IPv6 ネットワークをサポートしません。IPv6 ネットワークのみ有効になっている Mac は、[ネットワークの参照] に表示できません。

IPv6 ネットワークは 14.2 以降サポートされます。

- つの Symantec Endpoint Protection Manager は指定したコンピュータにクライアントソフトウェアをプッシュします。
パッケージが対象コンピュータに正常にコピーされるとインストールが自動的に開始します。

NOTE

リモートプッシュを使って Linux クライアントをインストールすることはできません。

リモートプッシュを使って Symantec Endpoint Protection クライアントをインストールするには

1. コンソールで、クライアント配備ウィザードを起動します。

[ヘルプ]、[始めましょう] ページをクリックして [必須タスク] で [コンピュータにクライアントソフトウェアをインストールします。] をクリックします。

バージョン 12.1.x の場合は、[共通のタスク] メニューで [クライアントのインストール] をクリックします。

2. クライアント配備ウィザードで、次のいずれかのタスクを実行します。

- [新しいパッケージ配備] をクリックして新しいインストールパッケージを作成し、[次へ] をクリックします。
- 前に作成されたパッケージを使う場合は [既存のパッケージ配備] をクリックし、[参照] をクリックしてインストールするパッケージを特定します。

クライアント配備ウィザードでパッケージをアップロードし、[コンピュータの選択] パネル (ステップ 5) に移動します。

- [通信の更新パッケージの配備] で、Symantec Endpoint Protection クライアントがすでにインストールされているコンピュータの Windows または Mac クライアント通信設定を更新するかどうかを選択します。画面の指示に従い、ステップ 4 に進みます。

管理外クライアントを管理下クライアントに変換するには、このオプションを使います。

[\[通信の更新パッケージの配備 \] を使ったクライアントサーバー通信の復元](#)

3. 新規パッケージの場合は、[グループとインストール機能セットの選択] パネルで利用可能なオプションから選択を行います。このオプションはインストールパッケージのタイプによって異なります。[次へ] をクリックします。

NOTE

既存のセキュリティソフトウェアを Windows クライアントからアンインストールするには、クライアント配備ウィザードを開始する前に、カスタムのクライアントインストールの設定を行う必要があります。また、この機能を有効にするように設定された既存のクライアントインストールパッケージを使うこともできます。

[既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定](#)

[Windows クライアントのインストール設定について](#)

-
4. [リモートプッシュ] をクリックし、[次へ] をクリックします。
 5. [コンピュータの選択] パネルで、次のいずれかの方法を使ってソフトウェアを受け取るコンピュータを特定します。
 - ネットワークでコンピュータを参照するには、[ネットワークの参照] をクリックします。
 - IP アドレスまたはコンピュータ名でコンピュータを検索するには、[ネットワークの検索] をクリックして、[コンピュータの検索] をクリックします。

タイムアウト値を設定して、サーバーが検索に費やす時間を制限できます。

6. [>>] をクリックしてコンピュータをリストに追加し、ウィザードで要求された場合にはドメインまたはワークグループで認証します。

リモートプッシュインストールには、システム特権が必要です。クライアントコンピュータが Active Directory ドメインの一部である場合は、ドメイン管理者アカウントを使ってください。

7. [次へ] をクリックしてから [送信] をクリックして、選択したコンピュータにクライアントソフトウェアをプッシュ型転送します。

[配備の概略] パネルに配備が成功したことが表示されると、インストールはクライアントコンピュータで自動的に開始します。

インストールが完了するまでに数分かかります。

8. [次へ] をクリックし、[完了] をクリックします。
9. [クライアント] ページで、インストールされたクライアントの状態を確認します。

新しい Symantec Endpoint Protection のインストールでは、クライアントコンピュータは自動的に再起動または管理者やユーザーが操作して再起動しないと つの Symantec Endpoint Protection Manager 内部に表示されないことがあります。

[つ の Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動](#)

[クライアントの配備の状態についてのレポートの実行](#)

NOTE

クライアントインストールパッケージをリモートで Mac クライアントにインストールしたら、クライアントコンピュータでカーネル拡張が認証されていることを確認する必要があります。カーネル拡張の認証は Symantec Endpoint Protection が完全に機能するために必要で、リモートプッシュでは認証が必要な場合でも確認画面が表示されません。Mac で、[セキュリティとプライバシー] システム環境設定を確認し、[許可する] をクリックします。

[クライアントインストールの準備](#)

[リモート配備用 Windows と Mac コンピュータの準備](#)

[クライアントにインストールするセキュリティ機能の選択](#)

[クライアント配備ウィザードを使ったクライアントのインストール方法の選択](#)

Web リンクと電子メールを使った Symantec Endpoint Protection クライアントのインストール

Web リンクと電子メールオプションではインストールパッケージとインストールパッケージの URL を作成します。ユーザーはパッケージをダウンロードして Symantec Endpoint Protection クライアントをインストールするための URL を電子メールで受け取ります。パッケージをインストールするには、管理者権限が必要です。

Web リンクと電子メールは次のタスクで構成されます。

- クライアントインストールパッケージの選択、設定、作成を行います。
Windows、Mac、Linux のクライアントインストールパッケージの設定に表示されるオプションから選択します。すべてのクライアントインストールパッケージは、つの Symantec Endpoint Protection Manager を動作するコンピュータ上に保管されます。
- つの Symantec Endpoint Protection Manager からの電子メールにより、クライアントインストールパッケージをダウンロードできることがコンピュータユーザーに通知されます。
インストールパッケージのダウンロードとインストールの手順が記載された電子メールメッセージを受信するユーザーの一覧を提供します。ユーザーは、クライアントソフトウェアをインストールする手順に従います。

NOTE

Mac と Linux クライアントインストールパッケージは .zip アーカイブファイル形式で自動的にエクスポートされます。ファイル権限を正しく保持するには、Mac の #####などのネイティブアーカイブプログラムまたは ditto コマンドを使って、アーカイブファイルを展開する必要があります。Mac の unzip コマンド、サードパーティアプリケーション、Windows アプリケーションを使ってこれらのオペレーティングシステム用のファイルを展開できません。

Web リンクと電子メールを使う前に、管理サーバーからメールサーバーへの接続を正しく設定する必要があります。

管理サーバーと電子メールサーバー間の通信の確立

Web リンクと電子メールを使って Symantec Endpoint Protection クライアントをインストールするには

1. コンソールで、クライアント配備ウィザードを起動します。
[ヘルプ]、[始めましょう] ページをクリックして [必須タスク] で [コンピュータにクライアントソフトウェアをインストールします。] をクリックします。
バージョン 12.1.x の場合は、[共通のタスク] メニューで [クライアントのインストール] をクリックします。
2. クライアント配備ウィザードで [新しいパッケージ配備] をクリックして [次へ] をクリックします。Web リンクと電子メールでは、新しいインストールパッケージのみが送信されます。
3. インストールパッケージのタイプによって異なる、利用可能なオプションから選択を行い、[次へ] をクリックします。

NOTE

既存のセキュリティソフトウェアを Windows クライアントからアンインストールするには、クライアントの配備ウィザードを開始する前に、カスタムのクライアントインストールの設定を行う必要があります。

既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定

Windows クライアントのインストール設定について

4. [Web リンクと電子メール] をクリックして、[次へ] をクリックします。
5. [電子メールの受信者とメッセージ] パネルで電子メールの受信者と件名を指定します。
複数の電子メールの受信者を指定するには、各電子メールアドレスの後にカンマを入力します。管理コンソールのシステム管理者は、自動的にメッセージのコピーを受け取ります。
電子メールのデフォルトの件名と本文を受け入れるか、またはテキストを編集します。URL をコピーして、イントラネットページなど、便利で安全なオンラインの場所にポストすることもできます。
6. パッケージを作成し、リンクを電子メールで配布するには、[次へ] をクリックし、[完了] をクリックします。
7. コンピュータユーザーが電子メールメッセージを受信し、クライアントソフトウェアをインストールしていることを確認します。
クライアントコンピュータは、自動的に再起動または管理者やユーザーが操作して再起動しないと 一つの Symantec Endpoint Protection Manager 内部に表示されないことがあります。インストールが完了すると、Mac クライアントは自動的に再起動を求めるメッセージを表示します。Linux クライアントでは再起動は不要です。

つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動
クライアントの配備の状態についてのレポートの実行

クライアントにインストールするセキュリティ機能の選択

クライアント配備ウィザードを使ったクライアントのインストール方法の選択

クライアントインストールの準備

管理サーバーのインストール後に実行するタスク

「インストール後に実行するタスク」では、製品をインストールして設定した後に、クライアントコンピュータの保護レベルが適切かどうかを評価するために実行するタスクを示します。これらのタスクを週単位ベースまたは月単位ベースで定期的に実行し続けます。

Table 23: インストール後に実行するタスク

処理	説明
ウイルスとスパイウェアの保護ポリシーを修正する	次のデフォルトスキャン設定を変更します。 • サーバーのグループを作成したら、定時スキャンの時間を、ほとんどのユーザーがオフラインである時刻に変更します。 Windows コンピュータで実行される定時スキャンの設定 • Auto-Protect でリスク追跡を有効にします。 詳しくは、記事「What is Risk Tracer?」を参照してください。 リスク追跡には次の前提条件があります。 – ネットワーク脅威防止が有効になっている。 – コンソールを使った、クライアントコンピュータでのコマンドの実行 – Windows のファイルとプリンタの共有が有効になっている。 Windows クライアントの Auto-Protect のカスタマイズ
リモートコンピュータグループとサーバーグループのファイアウォールポリシーを修正する	• オフサイトの場所に対して次のデフォルトのファイアウォールルールを有効にして、リモートコンピュータのセキュリティを向上させます。 – 外部コンピュータへのローカルファイル共有を遮断する – リモート管理の遮断 • ファイアウォールルール [ローカルコンピュータからのローカルファイル共有を許可する] を有効にすることで、サーバーグループのセキュリティを低下させます。このファイアウォールルールはローカルトラフィックのみを許可します。 ファイアウォールルールのカスタマイズ リモートクライアントの場所の管理

処理	説明
スキャンからアプリケーションとファイルを除外する	クライアントが特定のフォルダやファイルをスキャンしないように設定して、パフォーマンスを向上させることができます。 たとえば、クライアントは定時スキャンの実行のたびにメールサーバーディレクトリをスキャンします。メールサーバープログラムファイルとディレクトリを、スキャンから除外してください。 詳しくは、記事「About the automatic exclusion of files and folders for Microsoft Exchange server and Symantec products」というを参照してください。 スキャンした場合に問題が発生することがわかっているフォルダとファイルを除外することで、パフォーマンスを改善できます。たとえば、Symantec Endpoint Protection では Microsoft SQL Server 固有のファイルをスキャンしないようにする必要があります。SQL Server データベースファイルを格納するフォルダのスキャンを防ぐ例外を追加してください。これらの例外によってパフォーマンスが向上し、Microsoft SQL Server でファイルを使う必要があるときに破損したファイルやロックされているファイルを回避できます。 詳しくは、ナレッジベースの「How to exclude MS SQL files and folders using Centralized Exceptions」という記事を参照してください。 また、スキャンから誤検知を除外する必要があります。 拡張子で Windows コンピュータの Auto-Protect のスキャンからファイルを除外することもできます。 ウイルスとスパイウェアのスキャンの例外作成 Windows クライアントの Auto-Protect のカスタマイズ Mac クライアントの Auto-Protect のカスタマイズ
定時スキャンの後にクイックレポートと定時レポートを実行する	クイックレポートと定時レポートを実行し、クライアントコンピュータが適切なセキュリティレベルを備えているかどうかを確認します。 つの Symantec Endpoint Protection Manager のレポートの種類について クイックレポートの実行とカスタマイズ 定時レポートの実行方法
定時スキャンが正常に行われ、クライアントが予期したとおり動作していることを検査して確認する	クライアントコンピュータのモニタ、ログ、ステータスを調べて、各グループの保護レベルが適切であることを確認します。 エンドポイント保護の監視
コンテンツストレージの評価とクライアント通信の帯域幅の必要条件	12.1.5 以降では、つの Symantec Endpoint Protection Manager は複数の完全なコンテンツバージョンを格納しません。代わりに、最新の製品版と増分のみを格納します。この方法ではほとんどの場合にクライアントはパッケージ全体ではなく差分をダウンロードします。クライアントがかなり古い (3 か月を超える) まれな場合にのみ必要な最新コンテンツの完全版をダウンロードします。 環境でネットワーク帯域幅を正確に制御する必要がある場合はクライアント通信を調整することもできます。詳しくは、「SEP のクライアント通信の帯域制限について」という記事を参照してください。 クライアント上のコンテンツと定義を更新する方法 必要なストレージと帯域幅の計算について詳しくは、「Symantec Endpoint Protection サイジングとスケーラビリティに関するベストプラクティスホワイトペーパー」を参照してください。
新種のリスクが検出されたときの単一のリスクアウトブレイクについての通知を設定する	[単一リスクイベント] に対する通知を作成し、[リスクアウトブレイク] に対する通知を変更します。シマンテック社では、これらの通知のために、次の処理を推奨します。 1. [リスクの重大度] を [カテゴリ 1 (極低レベル) 以上] に変更し、Cookie による追跡に関する電子メールを受信しないようにします。 2. [ダンパー] の設定は [自動] のままにします。 通知は、セキュリティで保護された環境を維持するうえで重要であり、時間の節約も可能です。 管理者通知の設定 通知の管理

Symantec Endpoint Protection での初期作業

ナレッジベースの「[Symantec Endpoint Protection Recommended Best Practices for Securing an Enterprise Environment](#)」という記事を参照してください。

Symantec Endpoint Protection の通信ポート

つの Symantec Endpoint Protection Manager を実行するコンピュータと Symantec Endpoint Protection クライアントがサードパーティ製のファイアウォールソフトウェアやハードウェアも実行する場合は、特定のポートを開く必要があります。これらのポートは、リモート配備や、管理サーバーとクライアント間の通信で利用します。ポートを開く手順やアプリケーションでポートを使えるようにする手順については、ファイアウォールの製品マニュアルを参照してください。

デフォルトで、Symantec Endpoint Protection のファイアウォールコンポーネントはこれらのポートのトラフィックを許可します。

WARNING

Symantec Endpoint Protection クライアントのファイアウォールは、初期インストールではデフォルトでコンピュータが再起動するまで無効になっています。ファイアウォールによる保護を確実にするため、ソフトウェアがインストールされてクライアントが再起動されるまで、Windows ファイアウォールをクライアントで有効にしたままにします。Symantec Endpoint Protection クライアントのファイアウォールによって、コンピュータの再起動時に Windows ファイアウォールが自動的に無効化されます。

Table 24: クライアントとサーバーのインストールと通信に必要なポート

プロトコルとポート番号	用途	応答準備プロセス	説明	適用可能なバージョン
TCP 139、445 UDP 137、138	つの Symantec Endpoint Protection Manager から Windows コンピュータへのプッシュ配備	svchost.exe	• つの Symantec Endpoint Protection Manager によって開始 (clientremote.exe) • 設定不可 TCP エフェメラルポートも使います。	すべて
TCP 22	つの Symantec Endpoint Protection Manager から Mac コンピュータへのプッシュ配備	launchd	• つの Symantec Endpoint Protection Manager によって開始 (clientremote.exe) • 設定不可	すべて
TCP 2967	グループ更新プロバイダ (GUP) Web キャッシュプロキシ機能	ccSvcHst.exe (12.1.5 以降) Smc.exe (12.1.5 より前)	• Symantec Endpoint Protection クライアントによって開始 • 設定可能	すべて
TCP 2968	Web とクラウドのアクセス保護 クライアント認証	ccSvcHst.exe	• Symantec Endpoint Protection クライアントによって開始 • 設定可能	14.2 以降
TCP 2638	自動的にインストールされたデータベースと つの Symantec Endpoint Protection Manager との通信	• sqlserver.exe (SQL Server Express データベース、14.3 RU1 以降) • dbsrv16.exe (埋め込みデータベース、14.3 MP1 以前)	• つの Symantec Endpoint Protection Manager によって開始 • 設定可能	すべて
TCP 1433	リモート SQL Server データベースと つの Symantec Endpoint Protection Manager との通信	sqlserver.exe	• つの Symantec Endpoint Protection Manager によって開始 • 設定可能 つの Symantec Endpoint Protection Manager 管理サーバーは、TCP エフェメラルポートも使います。	すべて

プロトコル とポート番号	用途	応答準備プロセス	説明	適用可能な バージョン
TCP 8443	サーバー通信 (HTTPS)	SemSvc.exe	すべてのログオン情報と管理に関する通信は、このセキュアなポートを使って行われます。 - Java ベースのリモートコンソール、Web ベースのリモートコンソール、複製パートナーのいずれかによって開始 - 設定可能 この Symantec Endpoint Protection Manager はこのポートで応答準備します。	すべて
TCP 8444	SPC (Symantec Protection Center) 2.0 の Web サービス	SemSvc.exe	このポートは、Symantec Protection Center 2.0 の Web サービスのポートです。Symantec Protection Center 2.0 はデータフィードとワークフローをこの Symantec Endpoint Protection Manager に要求するときに、このポートを使います。 Symantec Protection Center 2.0 は、Symantec Endpoint Protection 14.x では使用できません。	12.1.x
TCP 9090	Web コンソール通信	SemSvc.exe	このポートは、リモート管理コンソールとこの Symantec Endpoint Protection Manager との初期 HTTP 通信のみで使われます。この初期通信はインストールを含んでいて、ログオン画面のみを表示します。 - リモート Web コンソールによって開始 - 設定可能 TCP エフェメラルポートも使います。	すべて
TCP 8014	この Symantec Endpoint Protection Manager (HTTP) と Symantec Endpoint Protection クライアントの間の通信	httpd.exe (Apache)	- Symantec Endpoint Protection クライアントによって開始 - 設定可能 クライアントは TCP エフェメラルポートも使います。	すべて
TCP 443	この Symantec Endpoint Protection Manager (HTTPS) と Symantec Endpoint Protection クライアントの間の通信	httpd.exe (Apache)	- Symantec Endpoint Protection クライアントによって開始 - 設定可能 12.1.x では省略可能ですが、14.x の新規インストールではデフォルトです。 クライアントは TCP エフェメラルポートも使います。	すべて
TCP 443	この Symantec Endpoint Protection Manager とクラウドコンソールの通信	prunsrv.exe	クラウドコンソールのプロキシバイパスリストに追加するドメインについて詳しくは、次のページを参照してください。 [Endpoint Protection Manager クラウド] タブ > [トラブルシューティング] にプロキシエラーメッセージが表示される	14.0.1 以降

プロトコル とポート番号	用途	応答準備プロセス	説明	適用可能な バージョン
HTTPS 443	Symantec Endpoint Protection ローミングクライアントとクラウドコンソールの通信	なし	つの Symantec Endpoint Protection Manager と断続的に通信している管理対象のクライアントが、重要なイベントをクラウドコンソールに直接アップロードします。つの Symantec Endpoint Protection Manager をクラウドコンソールに登録する必要があります。 クラウドコンソールからのローミング Symantec Endpoint Protection クライアントの監視	14.2 以降
HTTP 8081 HTTPS 8082	つの Symantec Endpoint Protection Manager と Content Analysis サーバーアプライアンスの通信	つの Symantec Endpoint Protection Manager	管理サーバーは、このポートを Content Analysis サーバーまたはマルウェア分析アプライアンスとの通信に使用します。	14.2.x バージョンのみ。14.3 で非推奨になりました。
TCP 8445	リモートレポートコンソールによって使用	httpd.exe (Apache)	- レポートコンソールによって開始 - 設定可能	すべて
TCP 8446	Web サービス	semapisrv.exe (14.x) SemSvc.exe (12.1.x)	リモート管理アプリケーションは、このポートを使用して、HTTPS を介して Web サービストラフィックを送信します。 - リモート監視および管理 (RMM) と EDR によって開始 - 設定可能 - Java リモートコンソール (バージョン 14.0.1 以降) で使用	すべて
TCP 8447	Process Launcher	semlaunchsrv.exe	この仮想サービスアカウントは、より高い権限を必要とする つの Symantec Endpoint Protection Manager プロセスを起動します。これにより、他のサービスでそれらのプロセスが不要になります。localhost からの要求を適用のみします。 - つの Symantec Endpoint Protection Manager によって開始 (SemSvc.exe) - 設定可能	12.1.5 以降
TCP 8765	サーバー制御	SemSvc.exe	つの Symantec Endpoint Protection Manager によって Tomcat Web サービスのシャットダウンのために使われます。 - つの Symantec Endpoint Protection Manager によって開始 - 設定可能	すべて
TCP 1100	リモートオブジェクトのレジストリ	SemSvc.exe	どのポートが RMI レジストリを実行するかを AjaxSwing に伝えます。 - AjaxSwing によって開始 - 設定不可	すべて

プロトコル とポート番号	用途	応答準備プロセス	説明	適用可能な バージョン
UDP 514	データを Syslog サーバーへフォワード (省略可能)	SemSvc.exe	- Syslog サーバーから 1 つの Symantec Endpoint Protection Manager へのアウトバウンドトラフィック - Syslog サーバーへのインバウンドトラフィック - 設定可能 1 つの Symantec Endpoint Protection Manager の送受信トラフィックは UDP エフェメラルポートを使用します。	

- Windows Vista 以降には、デフォルトで有効になっているファイアウォールがあります。ファイアウォールが有効になっていると、クライアントソフトウェアのリモートインストールやリモート配備を行えない場合があります。これらのオペレーティングシステムを実行するコンピュータへのクライアントの配備で問題が発生した場合、それらのファイアウォールで必要なトラフィックを許可するように設定します。
- 配備後、Windows ファイアウォールを使う場合、ファイルとプリンタの共有 (ポート 445) を許可するようにファイアウォールを設定する必要があります。

Windows ファイアウォールの設定について詳しくは、Windows のマニュアルを参照してください。

[基本管理サーバー設定について](#)

[リモート配備用 Windows と Mac コンピュータの準備](#)

[エンドポイント保護の監視](#)

[クライアントインストールの準備](#)

管理サーバーとクライアントのインストールおよびアンインストール

Symantec Endpoint Protection Manager とクライアントのインストールを計画します。

Symantec Endpoint Protection Manager をインストールする前に、以下の問題を検討する必要があります。

- ネットワーク内のクライアント数。
- 使用するデータベース (デフォルトの Microsoft SQL Server Express データベースまたは Microsoft SQL Server のいずれか)。
- 複数のサイトを設定するかどうか。
- フェールオーバーサーバーを設定するかどうか。

Symantec Endpoint Protection クライアントをインストールする前に、以下の点を検討する必要があります。

- インストールする機能
- 使用する配備方法

ネットワークアーキテクチャの注意事項

会社のネットワークアーキテクチャを考慮せず、テスト目的で Symantec Endpoint Protection をインストールできます。つの Symantec Endpoint Protection Manager を少数のクライアントとともにインストールして、機能に慣れることができます。

実働クライアントをインストールする準備ができたなら、組織構造とコンピューティングニーズに基づいて配備を計画してください。

配備を計画するときには、次の要素を考慮してください。

- つの Symantec Endpoint Protection Manager
管理者は つの Symantec Endpoint Protection Manager を使って、セキュリティポリシーとクライアントコンピュータを管理します。つの Symantec Endpoint Protection Manager がインストールされているコンピュータのセキュリティと可用性を考慮する必要があります。
- リモートコンソール
管理者は、コンソールソフトウェアを実行して つの Symantec Endpoint Protection Manager にアクセスするリモートコンピュータを使うことができます。管理者は、オフィスから離れているときにリモートコンピュータを使うことができます。リモートコンピュータがリモートコンソールの必要条件を満たしていることを確認してください。
- ローカルおよびリモートコンピュータ
リモートコンピュータのネットワーク接続は低速であることがあります。ローカルコンピュータのインストールに使った方法とは異なるインストール方法を使うことができます。
- ノートパソコンなどの持ち運び可能なコンピュータ
ノートパソコンは、定期的なスケジュールではネットワークに接続しないことがあります。ポータブルコンピュータに、LiveUpdate スケジュールを有効にする LiveUpdate のポリシーを設定すると便利です。定期的にチェックインしないポータブルコンピュータは、他のポリシー更新を取得しません。
- 安全な領域にあるコンピュータ
安全な領域内にあるコンピュータは、安全な領域内にはないコンピュータとは異なるセキュリティ設定を必要とする場合があります。

クライアントをインストールする予定のコンピュータを識別します。つの Symantec Endpoint Protection Manager を実行しているコンピュータを含め、すべての非保護コンピュータにクライアントソフトウェアをインストールすることを勧めます。

データベースの種類の選択について

つの Symantec Endpoint Protection Manager はデータベースを使ってクライアントと設定に関する情報を格納します。データベースは設定処理の一部として作成されます。管理サーバーをインストールする前にどのデータベースを使うかを決定する必要があります。データベースを使うように管理サーバーを設定するまでコンソールは使用できません。

Table 25: つの Symantec Endpoint Protection Manager が使うデータベース

データベースの種類	説明
Microsoft SQL Server Express (デフォルト)	SQL Server Express データベースは、デフォルトでは つの Symantec Endpoint Protection Manager と共に自動的にインストールされます。SQL Server Express データベースは設定する必要がなく、SQL Server よりも簡単にインストールできます。また、SQL Server Express を個別にインストールすることもできます。これにはいくつかの設定が必要です。SQL Server Express データベースは最大で 5,000 のクライアントをサポートします。 14.3 MP1 以前のバージョンでは、デフォルトのデータベースは埋め込みデータベースでした。 基本管理サーバー設定について
埋め込みデータベース	埋め込みデータベースは、デフォルトで つの Symantec Endpoint Protection Manager と共に自動的にインストールされます。埋め込みデータベースは設定する必要がありません。埋め込みデータベースは最大で 5,000 のクライアントをサポートします。
Microsoft SQL Server	このオプションを使う場合、つの Symantec Endpoint Protection Manager をインストールする前に、SQL Server と SQL Server Native Client をインストールする必要があります。互換性を最適化するには、SQL Server のバージョンと等しい SQL Server Native Client のバージョンをインストールします。 次のような場合は SQL Server を購入しインストールすることを検討してください。 5,000 以上のクライアントをサポートする必要がある。SQL Server を使えば、各管理サーバーは最大 18,000 クライアントをサポートできます (14.x の場合)。社内の部署にそれ以上のクライアントがある場合は、別の管理サーバーをインストールします。 - フェールオーバーと負荷分散をサポートする。 - 追加の管理サーバーをサイトパートナーとして設定する。 必要なサイト数の決定 SQL Server データベースを作成する場合は、最初にローカルサーバーかリモートサーバーのいずれかに SQL Server のインスタンスをインストールする必要があります。次に、管理サーバーとの通信用に設定する必要があります。 SQL Server の設定について

基本管理サーバー設定について

次の値は、つの Symantec Endpoint Protection Manager をインストールするときのデフォルト設定を示します。

カスタム設定を使って つの Symantec Endpoint Protection Manager をインストールするときのみ、次の値の一部を設定できます。

[つの Symantec Endpoint Protection Manager のインストール](#)

[Symantec Endpoint Protection の通信ポート](#)

Table 26: 基本サーバー設定

設定	デフォルト	説明
サイト名	マイサイト (デフォルト) サイト <ローカルホスト名> (カスタム)	つの Symantec Endpoint Protection Manager に表示されるサイトの名前。サイト名は、すべての機能を設定して実行する、つの Symantec Endpoint Protection Manager 内の最上位コンテナです。
サーバー名	<ローカルホスト名>	つの Symantec Endpoint Protection Manager を実行するコンピュータの名前。
サーバーデータフォルダ	SEPM_Install\data	つの Symantec Endpoint Protection Manager がバックアップ、レプリケーションログ、その他のファイルなどのデータファイルを格納するディレクトリ。このディレクトリが存在しない場合は、インストーラによって作成されます。 デフォルトの SEPM_Install のデフォルト値は C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。 32 ビットシステム (12.1.x のみ) の場合は、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。
暗号化パスワード	なし	このパスワードは、つの Symantec Endpoint Protection Manager とクライアント間の通信を暗号化します。 デフォルトの設定を選択した場合、システムは自動的に暗号化パスワードを生成します。概略画面から、この情報を印刷またはクリップボードにコピーできます。 カスタム設定を選択した場合は、システムがランダムなパスワードを自動的に生成するようにすることも、独自のパスワードを作成することもできます。パスワードには、6 から 32 文字の英数字を指定できます。 このパスワードは記録して安全な場所に保管してください。データベースの作成後にパスワードを変更または回復することはできません。また、復元するバックアップデータベースがない場合にディザスタリカバリの目的でもこのパスワードを入力する必要があります。 Endpoint Protection のディザスタリカバリのベストプラクティス
ユーザー名	管理	つの Symantec Endpoint Protection Manager コンソールに初めてログオンするときに使うデフォルトユーザー名。この値は設定できません。
Password	なし	サーバーの設定の間に管理アカウントのために指定したパスワード。 後に管理サーバーを再設定するには、元の admin パスワードが必要です。このパスワードは記録して安全な場所に保管してください。
[電子メールアドレス]	なし	指定した電子メールアドレスにシステム通知が送信されます。

SQL Server の設定について

つの Symantec Endpoint Protection Manager と SQL Server データベースをインストールする場合、SQL Server の設定に関する特定の必要条件があります。

シマンテック社では、データベースを作成する前に、シマンテックのインストールと設定の必要条件を満たす SQL Server の新しいインスタンスをインストールすることを推奨しています。データベースを既存のインスタンスにインストールすることもできますが、インスタンスを正しく設定する必要があります。正しく設定しないと、データベースのインストールが失敗します。たとえば、大文字と小文字を区別する SQL 照合を選択している場合も、インストールに失敗します。

WARNING

リモート SQL Server 通信のセキュリティを最大限に高めるには、両方のサーバーを安全に保護された同一のサブネットに配置します。

Table 27: 必要な SQL Server 設定

設定	インストールの必要条件
インスタンス名	デフォルトのインスタンス名は使わないでください。SEPM などの名前を作成します。 つの Symantec Endpoint Protection Manager をインストールするときに、SQL Server のインスタンスにデフォルトで Sem5 という名前のデータベースが作成されます。デフォルト名はサポートされていますが、複数のインスタンスを 1 台のコンピュータにインストールする場合には混乱を招く可能性があります。
認証設定	混合モードまたは Windows 認証モード SQL Server データベースの認証モードについて
sa パスワード	混合モード認証を設定するときは、このパスワードを設定します。
有効なプロトコル	TCP/IP
TCP/IP のための IP アドレス	IP1 と IP2 を有効にします。
IP1、IP2、IPALL の TCP/IP ポート番号	TCP ダイナミックポートを空白に設定し、TCP ポート番号を指定します。通常、デフォルトポートは 1433 です。データベースを作成するときに、このポート番号を指定します。 つの Symantec Endpoint Protection Manager データベースではダイナミックポートをサポートしません。
リモート接続	有効にする必要があります。TCP/IP プロトコルも指定する必要があります。

データベースをリモートサーバーに配置する場合、つの Symantec Endpoint Protection Manager を実行するコンピュータにも SQL Server クライアントコンポーネントをインストールする必要があります。SQL Server クライアントコンポーネントには BCP.EXE が含まれます。SQL Server クライアントコンポーネントのバージョン番号は、使用する SQL Server のバージョン番号と同じにする必要があります。インストール手順については SQL Server のマニュアルを参照してください。

インストールの つの Symantec Endpoint Protection Manager データベース設定フェーズで、各種のデータベース値を選択し、入力します。データベースを正しく設定するために、これらの決定を行う必要があることを理解してください。

以下の表に、インストール処理を始める前に理解しておくことが必要な場合がある設定を示します。

Table 28: SQL Server データベースの設定

設定	デフォルト	説明
サーバー名	<ローカルホスト名>	つの Symantec Endpoint Protection Manager を実行するコンピュータの名前。
サーバーデータフォルダ	SEPM_Install\data	つの Symantec Endpoint Protection Manager がバックアップ、レプリケーション、その他の つの Symantec Endpoint Protection Manager ファイルなどのデータファイルを格納するフォルダこのフォルダが存在しない場合は、インストーラによって作成されます。 デフォルトの SEPM_Installのデフォルト値は C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。 32 ビットシステム (12.1.x のみ) の場合は、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。

設定	デフォルト	説明
暗号化パスワード	なし	つの Symantec Endpoint Protection Manager とクライアントの間の通信を暗号化するパスワード。パスワードには、6 から 32 文字の英数字を指定できます (必須)。 このパスワードは記録して安全な場所に保管してください。データベースの作成後にパスワードを変更または回復することはできません。また、復元するバックアップデータベースがない場合にディザスタリカバリの目的でもこのパスワードを入力する必要があります。 Endpoint Protection のディザスタリカバリのベストプラクティス
[データベースサーバー]	<ローカルホスト名>	SQL Server がインストールされるコンピュータの名前と、省略可能なインスタンス名。データベースサーバーとデフォルトインスタンスをインストールした場合は、名前が付いていないので、ホスト名またはホストの IP address] の順にクリックします。データベースサーバーと名前付きインスタンスをインストールした場合は、ホスト名\インスタンス名または IP address\インスタンス名] の順にクリックします。入力した ホスト名は、DNS が適切に設定されている場合にのみ使うことができます。 リモートデータベースサーバーにインストールする場合は、最初に SQL Server クライアントコンポーネントを つの Symantec Endpoint Protection Manager を実行するコンピュータにインストールする必要があります。
SQL Server ポート	1433	SQL Server への送受信トラフィックに使うポート。ポート 0 は使用できません。ポート 0 は交渉された無作為のポートを指定します。
データベース名	sem5	作成するデータベースの名前。
データベースユーザー名	sem5	作成するデータベースユーザーアカウントの名前。ユーザーアカウントには読み込みと書き込みのアクセスが許可された標準の役割があります。名前は、英数字と特殊文字 を組み合わせることができます。~ # % _ + = : . 。特殊文字 ` ! @ ' \$ ^ & * () - { } [] " \ / < ; > , ? は使用できません。そのほかに使えない名前として、sysadmin、server admin、setupadmin、securityadmin、processadmin、dbcreator、
データベースのパスワード	なし	データベースユーザーアカウントと関連付けられるパスワードです。名前には、英数字と特殊文字 ~ # % _ + = : . / の組み合わせを指定できます。特殊文字 ! @ * () { } [] ; , ? は使用できません。

設定	デフォルト	説明
SQL Server ネイティブクライアントフォルダ	SQL Server 2005 (12.1.x) : ##### #\90\Tools\Binn SQL Server 2008: #####\100\Tools\Binn SQL Server 2012: #####\110\Tools\Binn SQL Server 2014 / 2016 / 2017 / 2019: ##### ##\Client SDK\ODBC\110\Tools\Binn	bcp.exe を含んだ SQL ネイティブクライアントのローカルディレクトリの場所。 表示されるインストールパスは、Microsoft SQL Server のデフォルトのパスを表します。 インストールディレクトリは、Microsoft SQL Server のインストールドライブとディレクトリを表します。 SQL Server ネイティブクライアントをインストールするには、お使いの SQL Server のバージョンに該当する Microsoft TechNet ページを参照してください。 SQL Server Native Client のインストール
サーバーユーザー名	なし	データベースサーバー管理者アカウントの名前で、通常は sa です。
サーバーパスワード	なし	データベースサーバーの管理者アカウントと関連付けられるパスワードです。一般的には「sa」です。

設定	デフォルト	説明
データベースのデータフォルダ	[デフォルト] をクリックすると自動的に検出されます。 SQL Server 2005 (12.1.x) : ##### # \MSSQL.1\MSSQL\Data SQL Server 2008: #####\ MSSQL10.MSSQLSERVER\MSSQL\Data SQL Server 2008 R2: #####\ MSSQL10_50.MSSQLSERVER\MSSQL\Data SQL Server 2012: #####\ MSSQL11.MSSQLSERVER\MSSQL\Data SQL Server 2014: #####\ MSSQL12.MSSQLSERVER\MSSQL\Data SQL Server 2016: #####\ MSSQL13.MSSQLSERVER\MSSQL\Data SQL Server 2017: ##### # \MSSQL14.MSSQLSERVER\MSSQL\Data SQL Server 2019: ##### # \MSSQL15.MSSQLSERVER\MSSQL\Data	SQL Server データフォルダの場所。リモートサーバーにインストールする場合、ボリューム ID がリモートサーバーの ID と一致する必要があります。 表示されるインストールパスは、Microsoft SQL Server のデフォルトのパスを表します。 - SQL Server 2005 の名前付きインスタンスにインストールする場合は、インスタンス名に、ドットと数値の ID が付いた MSSQL が付加されます。例: \MSSQL.n\MSSQL\Data - SQL Server 2008 の名前付きインスタンスにインストールする場合は、MSSQL10 にインスタンス名が付加されます。例: \MSSQL10.インスタンス名\MSSQL\Data - SQL Server 2008 R2 の名前付きインスタンスにインストールする場合は、MSSQL10_50 にインスタンス名が付加されます。例: \MSSQL10_50.インスタンス名\MSSQL\Data - SQL Server 2012 の名前付きインスタンスにインストールする場合は、MSSQL11 にインスタンス名が付加されます。例: \MSSQL11.インスタンス名\MSSQL\Data - SQL Server 2014 の名前付きインスタンスにインストールする場合は、MSSQL12 にインスタンス名が付加されます。例: \MSSQL12.インスタンス名\MSSQL\Data - SQL Server 2016 の名前付きインスタンスにインストールする場合は、MSSQL13 にインスタンス名が付加されます。例: \MSSQL13.インスタンス名\MSSQL\Data - SQL Server 2017 の名前付きインスタンスにインストールする場合は、MSSQL14 にインスタンス名が付加されます。例: \MSSQL14.インスタンス名\MSSQL\Data - SQL Server 2019 の名前付きインスタンスにインストールする場合は、MSSQL15 にインスタンス名が付加されます。例: \MSSQL15.インスタンス名\MSSQL\Data SQL Server のデフォルトおよび名前付きインスタンスのファイルの場所 Note: データベースサーバーとインスタンス名を正しく入力した場合は、[デフォルト] をクリックすると正しいインストールフォルダが表示されます。[デフォルト] をクリックしても正しいインストールフォルダが表示されない場合は、データベースの作成に失敗しています。

つの Symantec Endpoint Protection Manager のインストール

SQL Server データベースの認証モードについて

つの Symantec Endpoint Protection Manager は SQL Server データベース認証の 2 つのモードをサポートします。

- Windows 認証モード
- 混合モード

SQL Server は Windows 認証または混合モード認証のどちらかを使うように設定できます。混合認証モードでは Windows または SQL Server の資格情報を使用できます。SQL Server が混合モードを使うように設定されているとき、つの Symantec Endpoint Protection Manager は Windows 認証または混合モード認証のどちらを使うように設定してもかまいません。SQL Server が Windows 認証モードを使うように設定されているとき、つの Symantec Endpoint Protection Manager も Windows 認証モードを使うように設定する必要があります。

Windows 認証モードを使うリモートデータベース接続については、次の必要条件に注意してください。

- Active Directory 環境に配備する場合は、つの Symantec Endpoint Protection Manager と SQL Server を同じ Windows ドメインに配置する必要があります。
- ワークグループ環境に配備する場合は、Windows アカウントの資格情報がローカルコンピュータとリモートコンピュータで同じである必要があります。

SQL Server の設定について

つの Symantec Endpoint Protection Manager のアンインストール

つの Symantec Endpoint Protection Manager をアンインストールすると、サーバーとコンソールがアンインストールされます。必要に応じて、アンインストール時にデータベースとデータベースのバックアップファイルを削除できます。つの Symantec Endpoint Protection Manager をアンインストールするには、アプリケーションの削除、修復、変更を行うための Windows のコントロールパネルで、通常 [プログラムと機能] を使います。

つの Symantec Endpoint Protection Manager を再インストールする予定の場合は、アンインストールする前にデータベースをバックアップしてください。

場合によって、CleanWipe ユーティリティなど、他の方法を使って つの Symantec Endpoint Protection Manager をアンインストールする必要があります。次のサイトを参照してください。

Symantec Endpoint Protection のアンインストール

データベースとログのバックアップ

Symantec Endpoint Protection クライアントのインストールの管理

Symantec Endpoint Protection は、物理または仮想に関係なく、保護するあらゆるコンピュータのクライアントにインストールする必要があります。

Table 29: クライアントコンピュータのインストールタスク

処理	説明
ステップ 1: クライアントコンピュータの識別	クライアントソフトウェアをインストールするコンピュータを識別します。すべてのコンピュータで、サポート対象のオペレーティングシステムを実行していることを確認します。 Note: シマンテック社は つの Symantec Endpoint Protection Manager をホストするコンピュータでクライアントをインストールすることも推奨します。 最新のシステム必要条件について詳しくは、「 Endpoint Protection のすべてのバージョンのリリースノート 、 修正項目 、 システム要件 」を参照してください。
ステップ 2: コンピュータグループの識別 (オプション)	クライアントを追加するコンピュータグループを識別します。たとえば、クライアントを追加するグループは、コンピュータの種類に基づいて、会社組織に合わせて、または必要なセキュリティレベルに合わせて決定できます。クライアントソフトウェアをインストールする前か後にこれらのグループを作成できます。 Active Directory 構造のような既存のグループ構造をインポートすることもできます。 クライアントのグループの管理 Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート

処理	説明
ステップ 3: クライアント コンピュータの配備とインストールの準備	ユーザーがコンピュータの管理者権限を持たない場合は、リモートプッシュを使ってクライアントソフトウェアをリモートインストールします。リモートプッシュのインストールには、対象となるコンピュータのローカル管理者権限を持つクレデンシャルを入力する必要があります。 リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール インストール後、コンピュータのリモートクライアント配備を準備して、つの Symantec Endpoint Protection Manager との通信を準備します。 リモート配備用 Windows と Mac コンピュータの準備
ステップ 4: 機能の決定とクライアント ソフトウェアの配備	利用可能な方法のいずれかを使ってクライアントソフトウェアを配備します。カスタマイズされたクライアントパッケージをエクスポートし、後に配備したり、サードパーティ製ツールで配備したりできます。 Note: Symantec Endpoint Protection のインストールと同時にサードパーティのインストールを実行することは推奨しません。ネットワークレベルまたはシステムレベルの変更を加えるサードパーティプログラムをインストールすると、Symantec Endpoint Protection をインストールするときに望ましくない結果を引き起こすことがあります。可能な場合は、Symantec Endpoint Protection をインストールする前にクライアントコンピュータを再起動します。 クライアント配備ウィザードを使ったクライアントのインストール方法の選択 クライアントインストールパッケージのエクスポート サードパーティツールを使った Windows クライアントソフトウェアのインストール - クライアントコンピュータにインストールする機能を決定します。インストールパッケージをエクスポートまたは配備する前に、カスタムのクライアント機能セットとインストール設定を構成します。インストール設定にはインストールフォルダおよび再起動設定が含まれています。既定のクライアントインストール機能セットとインストール設定を使用することもできます。 クライアントにインストールするセキュリティ機能の選択 Windows クライアントのインストール設定について - Windows クライアントの場合、クライアントインストール設定を構成するとき、既存のサードパーティ製セキュリティソフトウェアを自動的にアンインストールするように選択できます。 既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定
ステップ 5: インストール状態の確認	クライアントのインストールが成功したとクライアントが つの Symantec Endpoint Protection Manager と通信することを確認します。管理下クライアントは、再起動後まで、コンソールに表示されないことがあります。 Symantec Endpoint Protection クライアントの状態アイコン つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動

インストール後、管理対象外コンピュータを保護し、Symantec Endpoint Protection インストールのパフォーマンスを最適化するための追加手順を実行できます。

リモート配備用 Windows と Mac コンピュータの準備

Symantec Endpoint Protection から つの Symantec Endpoint Protection Manager を配備する前に、コンピュータを準備するための手順を実行して、リモートインストールを確実に成功させる必要があります。これらの手順は、リモートインストールのみに関連します。これらの変更は後から戻すことができますが、別のリモートインストールを実行するためには、再度適用する必要があります。

NOTE

Symantec Endpoint Protection からリモートで Linux コンピュータに対して つの Symantec Endpoint Protection Manager クライアントを配備することはできません。

Table 30: リモート配備用にすべてのコンピュータを準備するためのタスク

タスク	詳細
クライアントコンピュータへの管理者権限の設定	クライアントコンピュータが Active Directory ドメインに含まれる場合、リモートプッシュインストールにドメイン管理者アカウントのクレデンシャルを使う必要があります。含まれない場合、配備する各コンピュータのために管理者のクレデンシャルを利用できるようにします。
ファイアウォール設定の修正	ファイアウォール設定を変更し、Symantec Endpoint Protection コンポーネント間の通信を許可します。 Symantec Endpoint Protection の通信ポート
既存のサードパーティ製セキュリティソフトウェアのアンインストール	現在使用中のサードパーティ製セキュリティソフトウェアをアンインストールします。Windows コンピュータの場合、Symantec Endpoint Protection バージョン 12.1 RU1 MP1 以降には、選択したサードパーティ製セキュリティソフトウェアを自動的にアンインストールするためのツールが含まれています。このツールによってアンインストールされないセキュリティソフトウェアは個別にアンインストールする必要があります。 Note: 一部のプログラムでは、特別なアンインストールルーチンがある場合や、自己防衛コンポーネントを無効にする必要がある場合があります。サードパーティソフトウェアのマニュアルを参照してください。 このツールは配備の前に設定します。Symantec Endpoint Protection のインストール前にアンインストールが実行されます。 既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定
正常にアンインストールされない Symantec Endpoint Protection クライアントのアンインストール	14 では、すでにインストールされている Symantec Endpoint Protection for Windows クライアントをアンインストールできます。このオプションは、既存の Symantec Endpoint Protection インストールが正常にアンインストールされない場合にのみ使用する必要があります。このオプションを標準的な配備の一部として使用しないでください。 このツールは配備の前に設定します。Symantec Endpoint Protection のインストール前にアンインストールが実行されます。 既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定
サポート外または個人向けシマンテック製セキュリティソフトウェアのアンインストール	Symantec AntiVirus や Symantec Client Security のようなサポート外のシマンテック製セキュリティソフトウェアがあれば、それをアンインストールします。これらの製品から直接移行することはできません。また、Norton Internet Security のような消費者向けのシマンテック製セキュリティ製品があれば、それをアンインストールします。 アンインストールについて詳しくはシマンテック製ソフトウェアのマニュアルを参照してください。 Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象アップグレードパス

Table 31: リモート配備用に Windows クライアントを準備するためのタスク

オペレーティングシステム	タスク
Windows Vista、Windows 7、Windows Server 2008 / 2008 R2 コンピュータの準備	Windows の User Account Control (UAC) は、ローカルの管理者アカウントが C\$ や Admin \$ などのリモート管理者共有にリモートでアクセスすることを防止します。レジストリキー LocalAccountTokenFilterPolicy を無効にする場合は、リモート配備時にクライアントコンピュータのユーザーアカウント制御を完全に無効にする必要はありません。 UAC のリモート制限を無効にするには、次を参照してください。 http://support.microsoft.com/kb/951016 次のタスクを実行します。 - 共有ウィザードを無効にする 共有ウィザードによって、リモートプッシュ中により高度な共有オプションの実行が防止されます。 - ネットワークと共有センターを使ってネットワーク探索を有効にします。 ネットワーク検出により、ネットワークの閲覧が可能になります。ネットワークを検索するためには必要ありません。 - 組み込みの管理者アカウントを有効にして、パスワードを割り当てる ローカルの管理者アカウントのパスワードが空白の場合、リモートプッシュは失敗します。 Windows クライアントコンピュータが Active Directory ドメインに含まれる場合は、リモートプッシュにローカル管理者権限を持つドメイン管理者アカウントの資格情報を使います。 - インストールをプッシュするアカウントに管理者権限があることを確認します。 - リモートレジストリサービスを有効にし、開始する - Windows Defender を無効にするか、削除します。 これらのタスクを正常に実行する方法については、オペレーティングシステムのドキュメントを参照してください。
Windows 8 / 8.1 以降または Windows Server 2012 / 2012 R2 以降のコンピュータの準備	配備する前に、次のタスクを実行します。 - レジストリキー LocalAccountTokenFilterPolicy を無効化します。 UAC のリモート制限を無効にするには、次を参照してください。 http://support.microsoft.com/kb/951016 - リモートレジストリサービスを有効にし、開始する - Windows Defender を無効にするか、削除します。

Table 32: リモート配備用に Mac クライアントを準備するためのタスク

オペレーティングシステム	タスク
サポートされているあらゆるオペレーティングシステムの Mac コンピュータの準備	配備する前に、Mac コンピュータで次のタスクを実行します。 [システム環境設定]、[共有]、[リモートログイン] の順にクリックし、すべてのユーザーのアクセスを許可するか、管理者など、特定のユーザーのみのアクセスを許可します。 - Mac ファイアウォールを使う場合、ステルスモードを無効にします。ステルスモードを有効にしている場合、リモートプッシュインストールは [ネットワークの検索] でクライアントを発見することができません。 Mac のステルスモードを無効にするには、次の記事を参照し、Mac オペレーティングシステムのお使いのバージョンを選択してください。 ステルスモードを使って Mac の安全性を確保する - セキュアシェル (SSH) が使うポートをファイアウォールが遮断しないことを確認します。デフォルトでは、このポートは TCP ポート 22 です。このポートはリモートログインに必要な通信を許可します。 - Bonjour サービスは IPv6 ネットワークをサポートしません。[ネットワークの参照] または [ネットワークの検索] にこれらの Mac を確実に表示するには、IPv4 ネットワークも有効になっていることを確認してください。 IPv6 ネットワークは 14.2 以降サポートされます。

クライアントのインストールの種類を使用してクラウドベースまたはローカルベースの定義をダウンロードするかどうかを選択

Windows クライアントのインストールパッケージを指定するときは、定義をクラウドからダウンロードするか、ローカルでダウンロードするかを選択する必要があります。クラウド対応オプションには、標準クライアントと埋め込み/VDI クライアントが含まれます。Symantec Endpoint Protection には、クラウドに接続していないクライアント用にダークネットワークインストールも含まれています。

NOTE

クライアントのインストール後に、Windows クライアントのインストールの種類を、[標準クライアント]、[埋め込みまたは VDI]、[ダークネットワーク] の間で変更する場合は、最初に既存のクライアントソフトウェアをアンインストールし、これらの設定を再度行ってから新しいクライアントパッケージを再インストールする必要があります。

標準クライアント (14 現在)	標準クライアント (12.1.x)
- クラウドにあるウイルスとスパイウェアの定義を使います。 - 最新のウイルスとスパイウェアの定義をディスクにインストールします。 標準クライアントは、レガシー標準またはダークネットワーク Windows クライアントよりもディスク上のサイズが約 80 から 90 パーセント小さくなります。 - 完全なインストールではなく、差分を使って自動更新を処理します。	- クラウドにあるウイルスとスパイウェアの定義を使うことができません。ただし、ダウンロードインサイトと SONAR で評価ルックアップを使うことができます。 - ウイルスとスパイウェアの完全な定義セットをインストールします。 - 完全なインストールではなく、差分を使って自動更新を処理します。

ダークネットワーククライアント (14 現在)	
- クラウドにある定義を使うことができません。 - クラウドに断続的にアクセスする、またはアクセスがないユーザーを対象としています。 - ウイルスとスパイウェアの完全な定義セットをインストールします。 - レガシーの標準サイズのクライアントと同様に、クラウドに接続している場合は、ダウンロードインサイトと SONAR で評価ルックアップを使います。 - 完全なインストールではなく、差分を使って自動更新を処理します。	

埋め込み/VDI クライアント (14 現在)	埋め込み/VDI クライアント (12.1.6)
- クラウドにあるウイルスとスパイウェアの定義を使います。 - 最新のウイルスとスパイウェアの定義のみをインストールします。 このクライアントは、ダークネットワーク Windows クライアントよりもディスク上のサイズが約 80 から 90 パーセント小さくなります。 - 埋め込み/VDI クライアントには標準クライアントよりも多くのサイズ最適化が提供されます。 - インストール完了後、インストーラのキャッシュは保存を実行しません。この変更は、最初にインストールパッケージをクライアントコンピュータにコピーしない限り、コントロールパネルを使ってインストールを削除または修正できないことを意味します。 - 埋め込みクライアントは、標準サイズのクライアントに比べ、より多くのフォルダで NTFS 圧縮を使います。 - 完全なインストールを使って自動更新を処理します。差分を使うことはできません。	- クラウドにあるウイルスとスパイウェアの定義を使うことができません。 - 最新のウイルスとスパイウェアの定義のみをインストールします。 レガシーのクライアントは、レガシーの標準 Windows クライアントよりもディスク上のサイズが約 80 から 90 パーセント小さくなります。 - このクライアントで提供される保護は、12.1.x 標準クライアントよりもわずかに低下します。シマンテック社は、ファイアウォール、ダウンロードインサイト、侵入防止、SONAR を含むすべての保護機能をインストールして有効にすることを推奨します。最高レベルのセキュリティを実現するには、システムロックダウン機能を使います。 - より新しい埋め込みクライアントと同じサイズ最適化が含まれています。 - 完全なインストールを使って自動更新を処理します。差分を使うことはできません。 12.1.6 で導入されました。

クライアント配備ウィザードを使ったクライアントのインストール方法の選択

クライアントインストールパッケージのエクスポート

クライアント配備ウィザードを使ったクライアントのインストール方法の選択

つの Symantec Endpoint Protection Manager をインストールしたら、クライアント配備ウィザードを使い、Symantec Endpoint Protection クライアントをインストールします。

Table 33: クライアントのインストール方法

オプション	説明
パッケージの保存	このインストールオプションにより、管理サーバーに保存し、その後、クライアントコンピュータに配布する実行可能なインストールパッケージが作成されます。次にユーザーはクライアントソフトウェアをインストールします。そのため、コンピュータに対してローカルの管理者権限が必要になります。 このオプションを使用し、Windows、Mac、Linux クライアントをインストールできます。 パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール
リモートプッシュ	リモートプッシュインストールは、指定したコンピュータにクライアントソフトウェアをプッシュします。クライアントコンピュータでインストールが自動的に開始します。リモートプッシュインストールでは、ユーザーはコンピュータに対するローカルの管理者権限を必要としません。 このオプションを使用し、Windows と Mac クライアントをインストールできます。 リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール リモート配備用 Windows と Mac コンピュータの準備

オプション	説明
Web リンクと電子メール	ユーザーは、クライアントソフトウェアをダウンロードおよびインストールするリンクを含んだ電子メールメッセージを受信します。次にユーザーはクライアントソフトウェアをインストールします。そのため、コンピュータに対してローカルの管理者権限が必要になります。 このオプションを使用し、Windows、Mac、Linux クライアントをインストールできます。 Web リンクと電子メールを使った Symantec Endpoint Protection クライアントのインストール

クライアント配備ウィザードを実行する前に、インストールオプションを見直し、必要に応じてカスタマイズし、インストール中にそれらのオプションを選択します。インストールオプションには、インストールする保護技術、インストール先のフォルダ、インストール後の再起動動作があります。

クライアントにインストールするセキュリティ機能の選択

Windows クライアントのインストール設定について

クライアントインストールの準備

クライアントにインストールするセキュリティ機能の選択

クライアント配備ウィザードを使用して、Windows クライアントインストールパッケージを配備する場合、機能セットを選択する必要があります。機能セットは、クライアントにインストールする保護機能を指定します。デフォルトの機能セットを選択するか、機能セットをカスタマイズできます。コンピュータの役割やコンピュータに必要なセキュリティまたはパフォーマンスのレベルに基づいて、インストールする機能セットを決定します。

インストール後、すべての機能を有効にしておく必要があります。

Table 34: クライアントインストール機能セット (Windows)

機能セット	説明
クライアントの完全保護	ワークステーション、デスクトップ、ノートパソコンに推奨されます。 すべての保護機能が含まれます。ラップトップ、ワークステーション、デスクトップに適しています。完全なダウンロード保護とメールプロトコル保護が含まれます。 可能な限り、最大のセキュリティのために完全保護を使用してください。
サーバーの完全保護	サーバーに推奨されます。 電子メールスキャナ保護を除くすべての保護機能が含まれます。つの Symantec Endpoint Protection Manager を含む、最大限のネットワークセキュリティを必要とするあらゆるサーバーに最適です。
サーバーの基本保護	高スループットサーバーに推薦されます。 ウイルスとスパイウェアの対策と基本ダウンロード保護が含まれます。侵入防止によりスループットが高いサーバでパフォーマンスの問題が起きることがあるので、このオプションはネットワークのパフォーマンスを最大にする必要があるサーバに適しています。

Mac クライアントのインストールパッケージは、ウイルスとスパイウェアの対策と侵入防止をインストールします。Mac クライアントのインストールパッケージのために機能をカスタマイズすることはできません。

Linux のクライアントインストールパッケージはウイルスとスパイウェアの対策のみをインストールします。

機能セットのカスタマイズ

保護機能のサブセットをインストールする場合は、カスタム機能セットを作成します。ただし、シマンテックではすべての機能をインストールすることを推奨しています。

Mac または Linux のクライアントインストールパッケージの機能はカスタマイズできません。

カスタム クライアント インストール機能セットを作成するには

1. コンソールで、[管理] > [インストールパッケージ] の順にクリックします。
2. [クライアントインストール機能セット] > [クライアントインストール機能セットの追加] を選択します。
3. [クライアントインストール機能セットの追加] ダイアログ ボックスで、名前と説明を入力し、クライアントにインストールする保護機能にチェックマークを付けます。
4. [OK] をクリックします。

[Symantec Endpoint Protection 技術でコンピュータが保護される仕組み](#)

つの Symantec Endpoint Protection Manager でのカスタムの Windows クライアントインストールパッケージの作成

クライアントインストール設定とクライアント機能セットの設定により、Windows 用の Symantec Endpoint Protection のクライアントインストールパッケージをカスタマイズできます。カスタマイズにより、インストールパス、インストール後の再起動の動作、インストールパッケージでサードパーティのセキュリティ製品などをアンインストールするかどうかを設定できます。

NOTE

クライアントインストール設定とクライアントインストール機能セットの設定は、Windows インストールパッケージにのみ適用されます。[管理] > [インストールパッケージ] > [クライアントインストールパッケージ] で Macintosh または Linux のインストールパッケージをエクスポートできますが、設定オプションは別のページで設定します。

Table 35: カスタムの Windows クライアントインストールパッケージを作成するタスク

タスク	詳細
新しいカスタムクライアントインストール設定を作成する	[クライアントインストールの設定] で、インストール方法を定義します。 クライアントコンピュータの既存のセキュリティソフトウェアをアンインストールする場合は、ここで設定します。 クライアントインストールの設定をカスタマイズする 既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定
新しいカスタム機能セットを作成する	[クライアントインストール機能セット] で、クライアントコンピュータにインストールする保護技術を定義します。 クライアントにインストールするセキュリティ機能の選択
新しいカスタムインストールパッケージを作成する	クライアントインストールパッケージをエクスポートするときに、作成したカスタマイズ済み設定ファイルから選択します。また、パッケージの保存場所と、パッケージが単一ファイル (.EXE) かファイルが含まれるフォルダかを選択します。 クライアント配備ウィザードで、カスタムインストール設定とカスタム機能セットを使用することもできます。 クライアントインストールパッケージのエクスポート リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール

クライアントインストールの準備

Windows クライアントのインストール設定について

クライアントの配備ウィザードを使うと、Windows クライアントのクライアントインストール設定を指定できます。クライアントインストール設定ではインストール処理自体のオプションを定義します。対象のインストールフォルダで、他のオプションでインストールログを無効にするかどうかやインストール後の再起動設定を定義します。

デフォルトのクライアントインストール設定を選択することも、[管理] > [インストールパッケージ] > [クライアントインストールの設定] でカスタムの [クライアントインストールの設定] を追加することもできます。コンテキストヘルプは、可能な設定に関する詳細を表示します。

ユーザーの中断を最小限にするには、サイレントインストールでリモート配備してください。サイレント配備を行う場合は、Microsoft Outlook などの Symantec Endpoint Protection にプラグインするアプリケーションを再起動する必要があります。

自動インストール ([進行バーのみを表示]) を使うと、Windows に 1 つ以上のポップアップウィンドウが表示されることがあります。ただし、それらのウィンドウに気づかなくてもインストールは失敗しません。

対話型インストールでリモート配備を行わないでください。この種類のインストールはユーザーが対話しないと失敗します。一部のオペレーティングシステムでは、セキュリティ機能 (Windows のセッション 0 分離など) により対話型インストールウィザードが表示されないことがあります。ローカルインストールにのみ対話型インストールを使ってください。これらの推奨事項は 32 ビットと 64 ビットのオペレーティングシステムの両方に適用されます。

[クライアントインストールの設定をカスタマイズする](#)

[クライアントにインストールするセキュリティ機能の選択](#)

クライアントインストールの設定をカスタマイズする

クライアントインストールパッケージや自動更新に適用するインストール設定を変更できます。

たとえば、クライアントをカスタムインストールフォルダにインストールする場合や、クライアント/サーバーの通信設定をリセットする場合は、カスタムクライアントインストール設定を作成します。その後で、パッケージのエクスポート時または配備時や、自動更新の設定時に、作成したカスタム設定を適用します。

クライアントインストールの設定をカスタマイズするには

1. コンソールで、[管理] > [インストールパッケージ] > [クライアントインストールの設定] を選択します。
2. [タスク] で、[クライアントインストール設定の追加] をクリックします。

デフォルトのクライアントインストール設定ファイルは修正できません。

3. 設定ファイルを適用するオペレーティングシステムを選択します。
4. 名前と説明を入力します。
5. 次の各タブで、利用可能なオプションから選択します。

- Windows: [基本設定] と [再起動の設定]
- Mac: [再起動の設定] と [アップグレードの設定]

Mac クライアントの再起動とアップグレードの設定は、自動更新にのみ適用されます (バージョン 14 以降)。

6. [OK] をクリックします。

クライアント配備ウィザードの実行時、または自動更新の設定時に、[インストールの設定] の横にあるドロップダウンメニューから、作成した設定を選択します。

[Windows クライアントのインストール設定について](#)

[既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定](#)

既存のセキュリティソフトウェアのアンインストール

Symantec Endpoint Protection クライアントのインストール前に、新しいインストールパッケージを設定、配備して、既存のセキュリティソフトウェアをアンインストールできます。既存のセキュリティソフトウェアをアンインストールすると、Symantec Endpoint Protection クライアントがより効率的に実行されるようになります。既存のサードパーティのセキュリティソフトウェアまたは既存の Symantec Endpoint Protection クライアントを削除できます。

カスタムのクライアントインストール設定を作成または修正して、セキュリティソフトウェアのアンインストール機能を有効にできます。作成したカスタム設定を、配備の際に選択します。

サードパーティのセキュリティソフトウェアをアンインストールするのにこの機能を使うことができます。クライアントパッケージがどのサードパーティソフトウェアを削除するか確認するには、[Endpoint Protection 14 でのサードパーティ製セキュリティソフトウェアの削除](#)を参照してください。一部のプログラムでは、特別なアンインストールルーチンがある場合や、自己防衛コンポーネントを無効にする必要がある場合があります。サードパーティソフトウェアのマニュアルを参照してください。

Mac または Linux クライアントパッケージでは、サードパーティのセキュリティソフトウェアを削除できません。Symantec Endpoint Protection クライアントパッケージを配備する前に、サードパーティのセキュリティソフトウェアをアンインストールする必要があります。

NOTE

バージョン 14.2 では、サードパーティ製セキュリティソフトウェアの削除機能が変更され、以前のバージョンのインストールパッケージに対しては有効にできなくなりました。たとえば、つの Symantec Endpoint Protection Manager のバージョン 14.2 で、バージョン 14.0.1 のクライアントパッケージを作成および配備した場合、そのパッケージに対してはサードパーティ製セキュリティソフトウェアの削除機能を有効にできません。

14 以降では、Windows のコントロールパネルなどの一般的な方法でアンインストールできない Symantec Endpoint Protection の既存のインストールを削除することもできます。この機能は、クライアントのインストール設定の別個のオプションとして表示されます。

次の手順で作成したパッケージのみが既存のセキュリティソフトウェアを削除できます。

1. 既存のセキュリティソフトウェアをアンインストールするためにクライアントパッケージを設定するには、コンソールの [管理] ページで、[インストールパッケージ] をクリックして [クライアントインストールの設定] をクリックします。
2. [タスク] で、[クライアントインストール設定の追加] をクリックします。

NOTE

カスタムのクライアントインストール設定を以前に作成している場合は、[タスク] で [クライアントインストールの設定の編集] をクリックして、設定を修正できます。既存のカスタム設定を修正しても、以前にエクスポートされたインストールパッケージは修正されません。

3. [基本設定] タブで、次のいずれかのオプションをクリックします。
 - 既存のサードパーティ製セキュリティソフトウェアを自動的にアンインストールする
 - Symantec Endpoint Protection クライアントの壊れたバージョンを削除するには、[アンインストールできない既存の **Symantec Endpoint Protection** クライアントソフトウェアを削除する] を使います (14)

[Symantec Endpoint Protection クライアントのアンインストールについて](#)

4. 選択したオプションについての情報を読んで、[OK] をクリックします。

この設定の他のオプションを修正することもできます。[ヘルプ] をクリックして、これらのオプションに関する情報を参照してください。

5. [OK] をクリックして、設定を保存します。

6. 既存のセキュリティソフトウェアをアンインストールするためにクライアントパッケージを配備するには、コンソールで [ホーム] ページから [クライアント配備ウィザード] を起動します。

[ヘルプ]、[始めましょう] ページをクリックして [必須タスク] で [コンピュータにクライアントソフトウェアをインストールします。] をクリックします。

-
7. クライアント配備ウィザードで [新しいパッケージ配備] をクリックして [次へ] をクリックします。

以前に作成したインストールパッケージを配備するのに [既存のパッケージ配備] を使うことができます。ただし、前の手順で説明されているようなカスタムのクライアントインストール設定を使って、これらのパッケージをエクスポートしておく必要があります。

8. [グループとインストール機能セットの選択] で、Windows のインストールパッケージを選択します。[インストールの設定] ドロップダウンリストで、前の手順で作成または修正したカスタムのクライアントインストール設定を選択します。[次へ] をクリックします。
9. 使う配備方法をクリックし、[次へ] をクリックして選択した配備方法を続行して完了します。

クライアント配備ウィザードを使ったクライアントのインストール方法の選択

Windows クライアントのインストール設定について

クライアントインストールの準備

Symantec Endpoint Protection クライアントのアンインストールについて

14 以降では、Symantec Endpoint Protection のインストールを開始する前にクライアントコンピュータ上の既存のクライアントインストールをアンインストールできます。この機能は CleanWipe ユーティリティに相当するため、すべての配備において有効にする必要はありません。Symantec Endpoint Protection クライアントの破損したインストールや正常に機能しないインストールを削除する場合にのみ、この機能を使う必要があります。

[アンインストールできない既存の **Symantec Endpoint Protection** クライアントソフトウェアを削除する] 機能を使用する前に、以下の重要な情報に注意してください。

- この機能は、作成したインストールパッケージのバージョン以下のすべての Symantec Endpoint Protection バージョンを削除します。
サポートされない製品である Symantec Endpoint Protection 11.x、Symantec AntiVirus 10.x、Symantec Client Security 3.x、Symantec Network Access Control を含む、すべてのバージョンも削除します。
- この機能は 14 より前のバージョンを削除しますが、以前のバージョンのインストールパッケージを作成するときはこの機能を有効にできません。たとえば、この機能を有効にするバージョン 12.1.6 MP4 のパッケージを作成することはできません。
- この機能が含まれるインストールパッケージよりも後の Symantec Endpoint Protection バージョンは、この機能でアンインストールできません。たとえば、計画ロールバック中にこの機能を使うことはできません。
- この機能を有効にした誤ったパッケージの種類を配備すると、この機能は削除を実行しません。たとえば、32 ビットのパッケージを 64 ビットのコンピュータに配備すると、この機能はインストールされません。したがって、既存の Symantec Endpoint Protection インストールを削除できません。
- GPO 配備を介する場合など、.MSI ファイルを直接使うインストールでは、この機能を使うことができません。
- この機能は手動更新と自動更新では正しく機能しません。この機能は新規インストールでのみ使用します。
- この機能は つの Symantec Endpoint Protection Manager を削除しません。
- このオプションは、他のシマンテック製品が Windows LiveUpdate を使っていない場合に、それのみを削除します。
- クライアントコンピュータでは、この機能はサイレントで実行して、状態画面またはユーザーインターフェースを表示しません。
- このオプションでは、インストールの種類が [サイレント] に強制されます。
- 削除が完了すると、コンピュータが自動的に再起動します。この再起動を延期または省略するように設定することはできません。

既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定

CleanWipe 駆除ツールをダウンロードして Endpoint Protection をアンインストール

Endpoint Protection 14 でのサードパーティ製セキュリティソフトウェアの削除

Endpoint Protection 14 でのサードパーティ製セキュリティソフトウェアの削除

以下の表に、Symantec Endpoint Protection クライアントのインストールパッケージによって削除できるサードパーティ製セキュリティ製品を示します。[クライアントインストールの設定] ダイアログボックスの [既存のサードパーティのセキュリティソフトウェアを自動的にアンインストール] オプションによって、これらの製品が削除されます。

サポート対象の製品リストに含まれていないセキュリティ製品は、[SEPprep ツール](#)を使用して削除できます。

Table 36: クライアントインストールウィザードによって削除されるサードパーティ製セキュリティ製品のリスト

[バージョン]	サードパーティ製品
14.3 RU1	Endpoint Protection 14.3 RU1 でのサードパーティ製セキュリティソフトウェアの削除
14.3 MP1	14.3 MP1 では、[既存のサードパーティのセキュリティソフトウェアを自動的にアンインストール] オプションが Symantec Endpoint Protection Manager から削除されました。代わりに、Symantec Endpoint Protection ダウンロードフォルダの Tools/TPAR フォルダにある TPAR ツールを使用します。 Readme は次の場所にあります: Symantec Endpoint Protection のサードパーティ製セキュリティソフトウェアの削除機能について 14.3 MP1 Symantec Endpoint Protection Manager を使用しており、14.0 ~ 14.3 クライアント用のインストールパッケージを作成する必要がある場合は、conf.properties ファイルに <code>scm.uninstall.thirdparty.security.software.enabled=true</code> を追加して管理サーバーサービスを再起動することで、[既存のサードパーティのセキュリティソフトウェアを自動的にアンインストール] オプションを表示して使用できます。
14.0 ~ 14.3	Endpoint Protection 14 でのサードパーティ製セキュリティソフトウェアの削除

[既存のセキュリティソフトウェアのアンインストール](#)

[Symantec Endpoint Protection クライアントのアンインストールについて](#)

Symantec Endpoint Protection 14.3 RU1 以降のサードパーティ製セキュリティソフトウェアの削除

以下の表は、クライアントインストールパッケージがインストールされる前に Symantec Endpoint Protection (SEP) が削除できるサードパーティ製品および製品バージョンを示しています。クライアントインストールパッケージによって、製品のすべてのバージョンが削除されます。

Table 37: 14.3 RU2 クライアント インストール ウィザードによって削除されるサードパーティ製セキュリティ製品のリスト

設定	説明
Avast	AntiVirus
AVG	AVG Internet Security Business Edition 2013
ESET	ESET Smart Security
Kaspersky	Kaspersky AntiVirus Kaspersky Endpoint Security Kaspersky Internet Security Kaspersky Security Center Network Agent
McAfee	McAfee Scan Enterprise

Table 38: 14.3 RU1 クライアント インストール ウィザードによって削除されるサードパーティ製セキュリティ製品のリスト

設定	説明
Avast	AntiVirus
AVG	AVG Protection
ESET	ESET Endpoint Antivirus / ESET Endpoint Security ESET Remote Administrator Agent
F-Secure	F-Secure Anti-Spyware F-Secure Anti-Spyware Scanner F-Secure Anti-Virus Client Security Installer F-Secure Automatic Update Agent F-Secure Backweb F-Secure Browsing Protection F-Secure CustomizationSetup F-Secure DAAS2 F-Secure Device Control F-Secure Diagnostics F-Secure E-mail Scanning F-Secure FWES F-Secure GateKeeper Interface F-Secure Gemini F-Secure GUI F-Secure Help F-Secure HIPS F-Secure Internet Shield F-Secure Localization API F-Secure Management Agent F-Secure Management Extensions F-Secure NAC Support F-Secure NAP Support F-Secure NIF F-Secure Offload Scanning Agent F-Secure ORSP Client F-Secure Policy Manager Support F-Secure Protocol Scanner F-Secure Safe Banking Popup F-Secure Sidegrade Support F-Secure Software Updater F-Secure System File Update F-Secure TNB F-Secure Uninstall F-Secure Anti-Virus

設定	説明
Kaspersky	Kaspersky Endpoint Security Kaspersky AES Encryption Module Kaspersky Anti-Virus for Windows Servers Kaspersky Security for Windows Servers Kaspersky Anti-Virus for Windows Workstations Kaspersky PURE Kaspersky Small Office Security Kaspersky AntiVirus / Kaspersky Internet Security Kaspersky Endpoint Security 8 for Windows Console Plug-in Kaspersky Anti-Virus SOS Kaspersky Security Center Network Agent
McAfee	McAfee Endpoint Security Web Control McAfee Endpoint Security Firewall McAfee Endpoint Security Threat Prevention McAfee Endpoint Security Platform McAfee Desktop Firewall McAfee VirusScan Enterprise McAfee Firewall Protection Service McAfee Virus and Spyware Protection Service McAfee Browser Protection Service McAfee SiteAdvisor Enterprise McAfee Agent McAfee Product Improvement Program McAfee Host Intrusion Prevention
Sophos	Sophos Endpoint Agent Sophos Patch Agent Sophos Network Threat Protection Sophos System Protection Sophos Client Firewall Sophos Anti-Virus Sophos Exploit Prevention Sophos Remote Management System Sophos AutoUpdate Sophos Endpoint Defense
Trend Micro	Trend Micro OfficeScan Agent

14.3 MP1 以降の Symantec Endpoint Protection Manager (SEPM) では、[クライアントインストールの設定] ダイアログボックスで [既存のサードパーティのセキュリティソフトウェアを自動的にアンインストール] オプションを使用してインストールパッケージを作成できなくなりました。代わりに TPAR を使用してください。ただし、14.3 MP1 SEPM を使用しており、14.3 MP1 よりも古い SEP クライアント用のインストールパッケージを作成するときは、この機能を使用できます。この場合、conf.properties に **scm.uninstall.thirdparty.security.software.enabled=true** を追加し、管理サーバーサービスを再起動する必要があります。この処理によってチェックボックスが表示されます。このオプションは、クライアント側の機能が含まれているバージョン 14.0 ~ 14.3 のクライアントでのみ有効です。

つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動

クライアントソフトウェアをインストールしたら、Windows クライアントコンピュータを再起動する必要があります。デフォルトでは、Windows クライアントのコンピュータはインストールの後で自動的に再起動します。ただし、事前にスケジュールした翌日の時間まで遅らせることができます。インストールパッケージをエクスポートするか、配備す

る前に、Windows クライアントのインストール設定を構成し、インストール後に再起動するようにカスタマイズできます。グループの再起動オプションを設定し、リスク修復または新しいクライアントダウンロードの後にクライアントコンピュータを再起動する方法を制御できます。

Mac クライアントのコンピュータはインストールの後で再起動の指示を要求します。クライアントパッケージをプッシュしたが、Mac コンピュータに誰もログオンしていない場合、インストールが完了したとき、自動的にハード要求が発生します。この設定はカスタマイズできません。

Linux クライアントコンピュータは再起動を必要とせず、インストール後、自動的に再起動しません。

また、管理サーバーから再起動コマンドを実行し、Mac または Windows クライアントコンピュータをいつでも再起動できます。管理サーバーからの再起動コマンドで Linux クライアントを再起動することはできません。ユーザーの都合のよい時間に再起動するように、Windows クライアントコンピュータをスケジュール設定することもできます。すぐに再起動するように強制することも、再起動を遅らせるオプションを有効にすることもできます。Mac クライアントのコンピュータに再起動コマンドを送ると、ハード要求が常に実行されます。

1. Windows クライアントのコンピュータでリスク修復と新しいクライアントダウンロードの再起動オプションを設定するには、コンソールで [クライアント] をクリックします。
2. [クライアント] ページでグループを選択し、[ポリシー] タブをクリックします。
3. [ポリシー] タブで、[全般の設定] をクリックします。
4. [全般の設定] ダイアログボックスの [再起動の設定] タブで、再起動の方法とスケジュールを選択します。
一部の再起動オプションは Windows クライアントにのみ適用されます。詳しくは、状況感知型ヘルプを参照してください。
再起動を行う前に、クライアントコンピュータに表示される通知を追加することもできます。デフォルトのメッセージでは、セキュリティリスク修復または新しいコンテンツダウンロードで再起動が必要となることが通知されます。
5. [OK] をクリックします。
6. 選択したクライアントコンピュータを再起動するには、コンソールで [クライアント] をクリックします。
7. [クライアント] ページの [クライアント] タブで、グループを選択します。
8. [クライアント] タブでクライアントを選択し、[コンピュータでコマンドを実行] を右クリックして、[クライアントコンピュータの再起動] を選択します。
9. [はい] をクリックして、必要な再起動オプションを指定し、[OK] をクリックします。
一部の再起動オプションは Windows クライアントにのみ適用されます。詳しくは、状況感知型ヘルプを参照してください。
10. 選択したグループのクライアントコンピュータを再起動するには、コンソールで [クライアント] をクリックします。
11. [クライアント] ページの [クライアント] タブでグループを選択し、[グループでコマンドを実行] をクリックして、[クライアントコンピュータの再起動] を選択します。
12. [はい] をクリックして、必要な再起動オプションを指定し、[OK] をクリックします。
一部の再起動オプションは Windows クライアントにのみ適用されます。詳しくは、状況感知型ヘルプを参照してください。

[Windows クライアントのインストール設定について](#)

[クライアントコンピュータで実行できるコマンドについて](#)

[コンソールを使った、クライアントコンピュータでのコマンドの実行](#)

[クライアントインストールの準備](#)

管理下クライアントと管理外クライアントについて

クライアントソフトウェアは、管理下クライアントまたは管理外クライアントとしてインストールできます。ほとんどの場合は、管理下クライアントとしてインストールしてください。テストコンピュータの場合や、コンピュータが主にオフサイトである場合などに、コンピュータに対するユーザーの制御性を高めるため、管理外クライアントをインストールします。管理外クライアントのユーザーが、デフォルト設定とは異なるセキュリティ設定を構成できるレベルの知識を持っていることを確認してください。

クライアントコンピュータでクライアントとサーバー間の通信ファイルを置換すると、後で管理外クライアントを管理下クライアントに変換できます。

Table 39: 管理下クライアントと管理外クライアントの違い

次のように入力します。	説明
管理下クライアント	管理下クライアントは、つの Symantec Endpoint Protection Manager に接続します。つの Symantec Endpoint Protection Manager コンソールからクライアントコンピュータを管理します。コンソールを使って、管理下クライアントコンピュータで、クライアントソフトウェア、セキュリティポリシー、およびウイルス定義を更新します。 管理下クライアントでは、つの Symantec Endpoint Protection Manager、GUP、インターネット、LiveUpdate からコンテンツのアップデートを取得できます。 ほとんどの場合、クライアントソフトウェアは管理下クライアントとしてインストールします。 管理下クライアントは次のいずれかの方法でインストールできます。 • 初期製品インストール中 • インストール後のコンソールから バージョン 14.0.1 以降のクラウド管理機能には、管理下クライアントが必要です。
管理外クライアント	一次コンピュータユーザーがクライアントコンピュータを管理する必要があります。管理外クライアントを、つの Symantec Endpoint Protection Manager に接続せずにコンソールで管理することはできません。ほとんどの場合、管理外クライアントは、ネットワークに断続的に接続するか、まったく接続しません。一次コンピュータユーザーが、管理外クライアントコンピュータ上でクライアントソフトウェア、セキュリティポリシー、ウイルス定義を更新する必要があります。 管理外クライアントでは、インターネットや LiveUpdate からコンテンツのアップデートを取得できます。各クライアント上のコンテンツを個別にアップデートする必要があります。 管理外のクライアントインストールパッケージの取得方法 管理外 Windows クライアントのインストール

[クライアントコンピュータと管理サーバーの通信方法](#)

[クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法](#)

[クライアントインストールの準備](#)

管理外のクライアントインストールパッケージの取得方法

管理外の Symantec Endpoint Protection クライアントインストールパッケージは次のいずれかの方法で取得できます。

- スタンドアロンクライアントインストーラを [Broadcom サポートポータル](#) からダウンロードします。
- [Broadcom サポートポータル](#) から、ダウンロードした完全インストールファイル内のフォルダをコピーします。
- デフォルトのポリシーと設定、またはカスタムのポリシーと設定とともに、つの Symantec Endpoint Protection Manager から管理外クライアントをエクスポートする

NOTE

ソフトウェアのダウンロードのガイダンスは、「[Symantec Endpoint Protection の最新バージョンのダウンロード](#)」を参照してください。

スタンドアロン クライアント インストーラをダウンロードするには

1. [Broadcom サポート ポータル](#)にサインインします。
2. 以下のファイルをダウンロードします。
Symantec_Endpoint_Protection_version_All_Clients_lang.zip
ここで、versionはバージョン番号です。langは言語で、英語の場合は EN などです。
3. ファイルの内容をハードディスクドライブに抽出します。
4. クライアントをインストールするオペレーティングシステムに応じて、以下のいずれかの操作を実行します。
 - Windows の場合: 32 ビットまたは 64 ビットの .exe ファイルをターゲットコンピュータにコピーします。
 - Mac の場合: Mac クライアントの .zip ファイルをターゲットコンピュータにコピーします。
 - Linux の場合: Linux クライアントの .zip ファイルをターゲットコンピュータにコピーします。

フル インストール ファイルからフォルダをコピーするには

1. [Broadcom サポート ポータル](#)にサインインします。
2. 以下のファイルをダウンロードします。
Symantec_Endpoint_Protection_version_Full_Installation_lang.exe
ここで、versionはバージョン番号です。langは言語です。
3. ファイルをダブルクリックして、その内容を抽出します。
4. 次のいずれかの操作をします。
 - バージョン 14.2 MP1a (14.2.1023.0100) 以降の場合、ファイルは C:\Users\username\AppData\Local\Temp\7zXXXXXXXXXX に抽出されます。ここで、XXXXXXXXXXは、文字と数字のランダムな文字列を表します。そのフォルダに移動します。インストールメニューは閉じないでください。
 - バージョン 14.2 MP1a (14.2.1023.0100) より前のバージョンでは、抽出する場所を入力するか、または参照して、[抽出] をクリックします。抽出が完了したら、そのフォルダに移動します。
5. クライアントをインストールするオペレーティングシステムに応じて、以下のいずれかの操作を実行します。
 - Windows の場合: フォルダ **SEP** (32 ビット) または **SEPx64** (64 ビット) をターゲットコンピュータにコピーします。
 - Mac の場合: フォルダ **SEP_MAC** をターゲットコンピュータにコピーします。
 - Linux の場合: フォルダ **SEP_LINUX** をターゲットコンピュータにコピーします。

つの Symantec Endpoint Protection Manager から管理外クライアントをエクスポートするには

1. 一つの Symantec Endpoint Protection Manager にログオンします。
2. 次のいずれかの操作をします。
 - デフォルトのポリシーと設定とともに、一つの Symantec Endpoint Protection Manager から管理外クライアントをエクスポートする
[クライアントインストールパッケージのエクスポート](#)
 - カスタムポリシーと設定とともに、一つの Symantec Endpoint Protection Manager から管理外クライアントをエクスポートする推奨事項については、次を参照してください。
[管理外クライアントのインストールパッケージの推奨ポリシーおよび設定](#)
グループポリシーとともに管理外の Mac クライアントをエクスポートすることはできません。
その後、Windows、Mac、または Linux 用の管理外クライアントをインストールできます。
ファイルが .zip ファイルの場合はインストールする前にすべての内容を解凍する必要があります。

[管理外 Windows クライアントのインストール](#)

[管理下クライアントと管理外クライアントについて](#)

管理外 Windows クライアントのインストール

管理外 (自己管理) クライアントを使用すると、通常、ユーザーはクライアントユーザーインターフェースを通じて、Symantec Endpoint Protection の設定をより詳細に制御できるようになります。通常、管理外 Symantec Endpoint

Protection クライアントは Windows コンピュータに直接インストールします。また、インストールを完了するためにはユーザー入力が必要です。

管理下クライアントと管理外クライアントについて

管理外のクライアントインストールパッケージの取得方法

NOTE

管理下 Windows クライアントのインストールパッケージは、同様の手順でクライアントコンピュータに直接インストールします。[対話型] インストールの場合のみ、ユーザーによる入力が必要です。クライアントインストール設定のオプション [進行バーのみを表示] または [サイレント] のインストールでは、ユーザー入力は不要です。

NOTE

カスタムポリシーを使用して設定された管理外クライアントパッケージが、説明にある一部のパネルに、インストール中に表示されない場合があります。手順内で説明されているインストールパネルが表示されない場合は、次の手順に進みます。

1. Setup.exe をダブルクリックして、[次へ] をクリックします。
2. [使用許諾契約] パネルで、[使用許諾契約の条項に同意します] をクリックし、[次へ] をクリックします。
3. [セットアップの種類] パネルで、次のいずれかのオプションをクリックします。
最も一般的なオプションの場合は [標準] をクリックし、[次へ] をクリックします。
インストールを設定するには [カスタム] をクリックし、[次へ] をクリックします。
 - [インストールの種類] パネルで、定義をクラウドからダウンロードするか、ローカル (ダーク ネットワーク) を選択します。
 - [カスタム セットアップ] パネルで、コンピュータにインストールする機能を選択します。機能の赤い「X」はインストールされません。

クライアントにインストールするセキュリティ機能の選択

クライアントにインストールするセキュリティ機能の選択

4. インストールウィザードに指示を求められたら、[Auto-Protect を有効にする] と [LiveUpdate を実行する] をクリックし、[次へ] をクリックします。
5. [ファイル評価データの提出] と [データ収集] パネルで、シマンテックに仮名データを提供しない場合はチェックマークを外し、[インストール] をクリックします。
管理外クライアントは、チェックボックスにチェックマークが付いていても有償ライセンスなしにデータを提出することはありません。
6. ウィザードの完了を示すパネルで [完了] をクリックします。

Windows クライアントのインストール設定について

クライアントインストールの準備

Symantec Endpoint Protection for Windows クライアントのアンインストール

Windows クライアントは次の方法でアンインストールできます。

- Windows コントロールパネルからアプリケーションを削除します。通常は [プログラムと機能] を使用します。
- Symantec Endpoint Protection クライアント (14 現在) を削除するカスタムクライアントインストールパッケージを設定および配備します。この方法は、Windows コントロールパネルを使用したアンインストールが機能しない場合にのみ使用してください。

Symantec Endpoint Protection クライアントに事前にインストールされた削除機能について

- つの Symantec Endpoint Protection Manager およびその他のコンポーネントをアンインストールする代替方法については、「[Symantec Endpoint Protection のアンインストール](#)」を参照してください。

Symantec Endpoint Protection クライアントソフトウェアがハードウェアデバイスを遮断するポリシーを使っている場合には、ポリシーはソフトウェアをアンインストールした後でデバイスを遮断します。アンインストールする前にポリシーによるデバイス制御を無効にしない場合、Windows のデバイスマネージャを使い、デバイスを遮断解除します。

Windows 用の Symantec Endpoint Protection クライアントをアンインストールするには

1. コンソールの [管理] ページで、[インストールパッケージ] をクリックして [クライアントインストールの設定] をクリックします。
2. [タスク] で、[クライアントインストール設定の追加] をクリックします。

NOTE

カスタムのクライアントインストール設定を以前に作成している場合は、[タスク] で [クライアントインストールの設定の編集] をクリックして、設定を修正できます。既存のカスタム設定を修正しても、以前にエクスポートされたインストールパッケージは修正されません。

3. [基本設定] タブで、[アンインストールできない既存の Symantec Endpoint Protection クライアントソフトウェアを削除します] にチェックマークを付けます。
4. メッセージを読み、[OK] をクリックします。
5. [OK] をクリックします。

[Mac 用の Symantec Endpoint Protection クライアントのアンインストール](#)

[Symantec Endpoint Protection for Linux クライアントのアンインストール](#)

Mac 用の Symantec Endpoint Protection クライアントのアンインストール

メニューバーのクライアントアイコンを使って、Symantec Endpoint Protection for Mac クライアントをアンインストールします。Symantec Endpoint Protection for Mac クライアントのアンインストールでは管理者ユーザーの資格情報が必要です。

NOTE

Symantec Endpoint Protection クライアントをアンインストールした後、アンインストールを完了するためにクライアントコンピュータを再起動するように求めるメッセージが表示されます。開始する前に、必ず未完了のすべての作業を保存して、すべての開いているアプリケーションを閉じます。

Mac 用の Symantec Endpoint Protection クライアントをアンインストールするには

1. Mac クライアントコンピュータで、Symantec Endpoint Protection クライアントを開き、[**Symantec Endpoint Protection**] > [**Symantec Endpoint Protection のアンインストール**] をクリックします。
2. [アンインストール] を再びクリックして、アンインストールを開始します。
3. Symantec Endpoint Protection クライアントをアンインストールするのに必要なヘルパーツールをインストールするには、Mac の管理者ユーザー名およびパスワードを入力し、[ヘルパーのインストール] をクリックします。
4. [**Symantec Endpoint Protection is trying to modify a System Extension** (Symantec Endpoint Protection はシステム拡張を変更しようとしています)] ダイアログボックスで、Mac の管理者ユーザー名とパスワードを入力し、[OK] をクリックします。

クライアントをアンインストールするためにパスワードの入力を求められる可能性もあります。このパスワードは、Mac の管理パスワードと別のパスワードである可能性があります。

5. アンインストールが完了したら、[今すぐに再起動] をクリックします。

アンインストールが失敗した場合は、別の方法を使用したアンインストールが必要になる場合があります。次のサイトを参照してください。

[Symantec Endpoint Protection のアンインストール](#)

Symantec Agent for Linux または Symantec Endpoint Protection for Linux クライアントのアンインストール

インストール時に取得したスクリプトとともに Symantec Endpoint Protection for Linux クライアントをアンインストールします。

NOTE

Linux コンピュータの Symantec Endpoint Protection クライアントをアンインストールするにはスーパーユーザー権限が必要です。この手順では、`sudo` を使って権限の昇格を説明します。

(14.3 RU1 以降の場合) Symantec Management Agent for Linux をアンインストールするには

1. Linux コンピュータで、ターミナルアプリケーションウィンドウを開きます。
2. 以下のディレクトリに移動します。
`/usr/lib/symantec/`
3. 以下の組み込みスクリプトを実行して、Symantec Agent for Linux をアンインストールします。
`./uninstall.sh`
4. アンインストールが完了して再起動プロンプトが表示されたら、コンピュータを再起動します。
`uninstall.sh` スクリプトを実行すると、Symantec Agent for Linux のすべてのコンポーネント (`sdcss-caf`、`sdcss-sepagent`、および `sdcss-kmod`) が削除されます。

```
[root@localhost symantec]# ./uninstall.sh
Running ./uninstall.sh (PWD /usr/lib/symantec; version 2.2.4.41)
Uninstalling Symantec Agent for Linux (SEPM) ...
Removing packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
Symantec Agent for Linux (SEPM) uninstalled successfully.
A reboot is required to complete uninstallation.
Please reboot your machine at the earliest convenience.
```

(14.3 MP1 以前の場合) Symantec Endpoint Protection for Linux クライアントをアンインストールするには

1. Linux コンピュータで、ターミナルアプリケーションウィンドウを開きます。
2. 次のコマンドを実行して Symantec Endpoint Protection インストールフォルダにナビゲートします。
`cd /opt/Symantec/symantec_antivirus`
このパスはデフォルトのインストールパスです。
3. 組み込みスクリプトで次のコマンドを実行して Symantec Endpoint Protection をアンインストールします。
`sudo ./uninstall.sh`
パスワードの入力を求めるメッセージが表示されたらパスワードを入力します。
このスクリプトは Symantec Endpoint Protection コンポーネントのアンインストールを開始します。
4. メッセージが表示されたら `Y` と入力して **Enter** キーを押します。
コマンドプロンプトが返るとアンインストールは完了します。

NOTE

一部のオペレーティングシステムでは、`/opt` フォルダの唯一の内容が Symantec Endpoint Protection クライアントファイルの場合にはアンインストーラスクリプトは `/opt` も削除します。このフォルダを作成し直すには、`sudo mkdir /opt` コマンドを入力します。

パッケージマネージャまたはソフトウェアマネージャを使ってアンインストールするには、ご使用の Linux 配布版に固有のマニュアルを参照してください。

クライアントインストールパッケージの管理

つの Symantec Endpoint Protection Manager をインストールしたクライアントを管理するには、管理下クライアントのインストールパッケージをエクスポートしてからクライアントコンピュータにパッケージのファイルをインストールする必要があります。つの Symantec Endpoint Protection Manager またはサードパーティ配備ツールでクライアントを配備できます。

通常、製品の新しいバージョンをリリースするときにシマンテック社がインストールファイルの更新済みパッケージを提供することもあります。自動更新機能を備えたグループのすべての管理下 Windows クライアントと Mac クライアントでクライアントソフトウェアを自動的に更新できます。インストール配備ツールでソフトウェアを再配備する必要はありません。

Table 40: クライアントインストールパッケージに関連するタスク

タスク	説明
クライアントインストールパッケージの設定	インストールする特定のクライアント保護技術を選択しインストールとエンドユーザーとの対話方法を指定できます。 クライアントにインストールするセキュリティ機能の選択 Windows クライアントのインストール設定について
クライアントインストールパッケージのエクスポート	管理下クライアントや管理外クライアントのパッケージをエクスポートできます。パッケージを単一の実行可能ファイルまたはディレクトリ内の一連のファイルとしてエクスポートすることができます。どちらの方法を選択するかは、配備の方法や、グループのクライアントソフトウェアをアップグレードするかどうかによって異なります。通常、Active Directory のグループポリシーオブジェクトを使う場合には、単一の実行可能ファイルへのエクスポートは選択しません。 クライアントインストールパッケージのエクスポート 管理外のクライアントインストールパッケージの取得方法 管理外 Windows クライアントのインストール
クライアントインストールパッケージ更新のインポート	更新済みのクライアントインストールパッケージをデータベースに追加して 1 つの Symantec Endpoint Protection Manager から配布できるようにします。省略可能なオプションとして、この手順を行うときにパッケージをエクスポートし、クライアントソフトウェアのないコンピュータにパッケージを配備できるようにすることもできます。 1 つの Symantec Endpoint Protection Manager へのクライアントインストールパッケージのインポート
1 つ以上のグループの Windows クライアントと Mac クライアントのアップグレード	エクスポートしたパッケージを一度に 1 台ずつコンピュータにインストールするか、エクスポートしたファイルを同時に複数のコンピュータに配備できます。 シマンテック社がクライアントインストールパッケージの更新を提供する場合は、まずそれをつの Symantec Endpoint Protection Manager に追加してエクスポートできるようにします。ただし、クライアント配備ツールで再インストールする必要はありません。Windows クライアントと Mac クライアントを最新のソフトウェアで更新する場合は、自動更新を使うのが最も簡単な方法です。最初に、少数のテストコンピュータを含むグループを更新してください。 自動更新によるクライアントソフトウェアのアップグレード クライアントによる LiveUpdate の実行を許可しており、LiveUpdate 設定ポリシーが更新を許可している場合には、LiveUpdate を使ってクライアントを更新することもできます。
クライアントインストールパッケージの削除	ディスク容量を節約するために古いクライアントインストールパッケージを削除できます。ただし、自動アップグレードは古い Windows クライアントインストールパッケージを使ってアップグレードパッケージを構築することがあります。アップグレードパッケージを使うとクライアントがダウンロードする回数が減ります。

クライアントインストールの準備

クライアントインストールパッケージのエクスポート

[クライアント配備ウィザード] の [パッケージの保存] を使った場合に利用できないオプションが必要な場合は、クライアントインストールパッケージをエクスポートすると便利です。たとえば、カスタムポリシーで管理外クライアントを

作成する必要がある場合もあります。また、Windows の 32 ビットまたは 64 ビットのインストールパッケージのみが必要な場合や、Linux の `DPKG` または `RPM` のインストールパッケージが必要な場合もあります。

クライアントインストールパッケージをエクスポートしたら配備します。クライアント配備ウィザードの [リモートプッシュ] で、エクスポートした Windows パッケージや Mac パッケージを配備できます。または、クライアントにエクスポートしたパッケージを直接インストールしたり、サードパーティプログラムを使って配備したりできます。

管理下クライアントや管理外クライアントのインストールパッケージを作成できます。両方の種類のパッケージに、割り当てられた機能、ポリシー、設定があります。管理下クライアント用に作成したパッケージは、つの Symantec Endpoint Protection Manager コンソールで管理することができます。管理外クライアント用に作成したパッケージは、コンソールでは管理できません。クライアント配備ウィザードで [通信の更新パッケージの配備] を使って、管理外の Windows クライアントや Mac クライアントを管理下クライアントにいつでも変換できます。

NOTE

リモートコンソールからクライアントインストールパッケージをエクスポートする場合、パッケージはリモートコンソールを実行しているコンピュータ上に作成されます。さらに、複数のドメインを使う場合は各ドメインにパッケージをエクスポートする必要があります。そうしないとクライアントが正しいドメイングループに表示されません。

クライアント インストール パッケージをエクスポートするには

1. コンソールで、[管理]、[インストールパッケージ] の順にクリックします。
2. [インストールパッケージ] で、[クライアントインストールパッケージ] をクリックします。
3. [クライアントインストールパッケージ] ペインの [パッケージ名] で、エクスポートするパッケージを右クリックして [エクスポート] をクリックします。
4. [参照] をクリックしてエクスポート済みパッケージが含まれるフォルダにナビゲートして選択し、[OK] をクリックします。

NOTE

パッケージのエクスポートは、2 バイト文字または Hi-ASCII 文字を含むディレクトリをサポートせず、その選択はブロックされます。

5. インストール目的に応じて他のオプションを設定します。オプションは、エクスポートするインストールパッケージの種類やプラットフォームに応じて異なります。

このダイアログボックスのエクスポートオプションについて詳しくは、[ヘルプ] をクリックしてください。

パッケージ設定のエクスポート

6. [OK] をクリックします。

つの Symantec Endpoint Protection Manager へのクライアントインストールパッケージのインポート

クライアントにインストールするセキュリティ機能の選択

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

つの Symantec Endpoint Protection Manager へのクライアントインストールパッケージのインポート

以前のバージョンから復元したデータベースを使用して新しいバージョンの つの Symantec Endpoint Protection Manager にアップグレードする場合、クライアントのインストール パッケージを つの Symantec Endpoint Protection Manager にインポートする必要があります。データベースには古いクライアントインストールパッケージが含まれていて、新しいパッケージをインポートする必要がある。

つの Symantec Endpoint Protection Manager のバージョンは必ずクライアントバージョンと同じか、それ以降にする必要があります。

NOTE

.exe や .zip ファイルパッケージなどの実行可能パッケージを直接インポートできますが、この方法は推奨しません。 .info ファイルにはパッケージ内容を説明する情報が含まれていて、デルタ更新を使って Symantec Endpoint Protection クライアントの将来のビルドへの適切な移行を確実に実行できます。一方、つの Symantec Endpoint Protection Manager Web コンソールは .info ファイル形式をインポートしません。Web コンソールでは、.zip または .exe ファイル形式など、単一ファイルのパッケージのインポートまたはエクスポートのみを実行できます。

クライアントインストールパッケージを つの Symantec Endpoint Protection Manager にインポートするには

1. インポートするインストールパッケージを、つの Symantec Endpoint Protection Manager が実行されているコンピュータ上のディレクトリにコピーします。

クライアントインストールパッケージは 2 つのファイルで構成されています。1 つが「製品名.dat」という名前のファイルで、もう 1 つが「製品名.info」という名前のファイルです。これらのファイルは つの Symantec Endpoint Protection Manager のインストールまたはアップグレード時に自動的にインポートされます。インストールファイルの SEPM/Packages フォルダからパッケージを取得することもできます。

2. コンソールで、[管理] > [インストールパッケージ] の順にクリックします。
3. [タスク] で、[クライアントインストールパッケージの追加] をクリックします。
4. [クライアントインストールパッケージの追加] ダイアログボックスで、パッケージの名前と説明を入力します。
5. [参照] をクリックします。
6. [フォルダの選択] ダイアログボックスで、新しいパッケージの [製品名] .info ファイル (ステップ 1 でコピーしたもの) を検索して選択し、[選択] をクリックします。
7. [正常に完了しました] というメッセージが表示されたら、[閉じる] をクリックします。

インストールファイルをエクスポートして配備に利用できるようにするには、[このパッケージをエクスポート] をクリックしてこの手順を完了します。

クライアントインストールパッケージのエクスポート

パッケージのインポートが正常に完了すると、[システム] の [管理ログ] に、パッケージの作成がイベントとして記録されます。イベントのログとして、「つの Symantec Endpoint Protection Manager によって SEP 12.1 RU5 32 ビットパッケージのインポートが正常に完了しました。このパッケージは配備可能になりました。」のような文が記載されているはずです。

Windows クライアントインストールパッケージとコンテンツ更新のサイズ

クライアントインストールパッケージ、製品パッチ、コンテンツ更新も Symantec Endpoint Protection データベースに格納され、ストレージの必要条件に影響を与えます。製品パッチには、クライアントパッケージの情報と各言語またはロケールの情報が含まれます。パッチによって新しい完全なクライアントビルドが作成される点に注意してください。

[#unique_166](#)以下のテーブルに、クライアントのログ記録と保護技術を最大レベルで有効にした場合のクライアントインストールパッケージのサイズを示します。

Table 41: Windows クライアントインストールパッケージのサイズ

クライアント/定義の種類	*ウイルス定義とともにインストールしたか	64 ビットのパッケージ (MB)	32 ビットのパッケージ (MB)
標準と埋め込み (14) CoreDefs-3**	はい	188	175
	【※No※】	93	81
ダークネットワーク (14) CoreDefs-1.5	はい	288	276
	【※No※】	93	80

クライアント/定義の種類	*ウイルス定義とともにインストールしたか	64 ビットのパッケージ (MB)	32 ビットのパッケージ (MB)
標準 (12.1.6) CoreDefs-1	はい	335	316
	【※No※】	86	70
縮小 (埋め込み/VDI) (12.1.6) CoreDefs-3	はい	182	165
	【※No※】	86	70

クライアントのインストールの種類を使用してクラウドベースまたはローカルベースの定義をダウンロードするかどうかを選択

これらのパッケージには、大きいサイズのハートビートを設定できます。このサイズにはパケットレベルのファイアウォールログは含まれません。パケットレベルのファイアウォールログは本番環境では推奨しません。クライアントのログ記録が無効にされており、管理サーバーからダウンロードする新しいポリシーやコンテンツがない場合にはクライアントインストールパッケージは小さくなります。この場合は小さいサイズのハートビートを設定できます。

*ネットワークの帯域幅が狭い場合は、ウイルス定義なしでクライアントパッケージをインストールします。クライアントは、管理サーバーに接続するとすぐにウイルス定義の完全なセットを受け取ります。

すべてのクライアントインストールパッケージに、ウイルスとスパイウェア、ファイアウォール、IPS、SONAR、システムロックダウン、アプリケーション制御、ホストインテグリティコンテンツなど、すべての機能が含まれています。クライアントの種類による相違点は、ウイルスとスパイウェアの定義のサイズです。

データベース内やファイルシステム上でコンテンツ更新に必要なストレージ領域がより少なくなりました。複数の完全なリビジョンを格納するのではなく、管理サーバーはコンテンツ全体のリビジョン 1 つのみと増分の差分を格納するようになりました。12.1.6 では、完全なコンテンツ更新に最大 470 MB が必要です。

NOTE

14 以降では、他のコンテンツと同じように LiveUpdate サーバー、管理サーバー、グループ更新プロバイダを使用してクライアントにセキュリティパッチをダウンロードできます。[Windows クライアントへの Endpoint Protection セキュリティパッチのダウンロード](#)

Symantec Endpoint Protection (SEP) の最新リリースへのアップグレードおよび移行

Symantec Endpoint Protection の最新リリースへの更新方法について

このトピックを使用して、SEP 14.x の最新リリースにアップグレードし、新機能を利用します。ここに記載された情報は、互換性のあるバージョンの製品がすでにインストールされている環境でソフトウェアをアップグレードするためのものです。

アップグレードする前に、以下の情報を確認します。

- [Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)
- [既知の問題と回避策](#)
- [Symantec Endpoint Protection 14.x のすべてのバージョンの新機能](#)
- [Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象およびサポート非対象アップグレードパス](#)
- [Symantec Endpoint Protection 14 の移行に関する考慮事項](#)

Table 42: Symantec Endpoint Protection をアップグレードする処理

タスク	説明
手順 1: Broadcom Download Center から最新バージョンをダウンロードする	シマンテックソフトウェアの最新バージョンをダウンロードする Symantec Endpoint Protection Manager (SEPM) と Symantec Endpoint Protection クライアントをアップグレードする前に、以下のベストプラクティスに従って、アップグレード時にネットワークの保護を最大限に高めるようにします。 • Symantec Endpoint Protection のアップグレードと同時にサードパーティ製品のインストールを実行することは推奨しません。ネットワークレベルまたはシステムレベルの変更を行うサードパーティソフトウェアをインストールすると、Symantec Endpoint Protection をアップグレードする際に、予期しない結果が生じる可能性があります。 • 可能な場合は、Symantec Endpoint Protection をインストールまたはアップグレードする前に、クライアントコンピュータを再起動します。 • Windows 10 への移行と同時に、バージョン 12.1.6 以前から Symantec Endpoint Protection をアップグレードする場合は、最初に Symantec Endpoint Protection を移行する必要があります。詳しくは、「Windows 10 での Endpoint Protection サポート」を参照してください。 • 複数のバージョンを管理するのではなく、ネットワーク全体を Symantec Endpoint Protection の現在のバージョンにアップグレードすることを推奨します。 Endpoint Protection 14.x のアップグレードのベストプラクティス
ステップ 2: データベースをバックアップしてディザスタリカバリに備える	クライアントデータの整合性を保証するために、次の Symantec Endpoint Protection Manager が使うデータベース、ログ、リカバリファイルのバックアップを作成します。これらのステップは、使用しているバージョンによって異なります。 Endpoint Protection のディザスタリカバリのベストプラクティス
ステップ 3: 複製関係を解消する	アップデートする管理サーバーを他の管理サーバーで複製する場合は、複製関係を解消します。アップグレード中に複製パートナーが複製を起動すると、予測不能な結果が生じる可能性があります。 Note: 管理サーバー間の関係を解消することは、複製パートナーを削除することと同じではありません。複製パートナーを完全に削除することがないようにします。 管理サーバー間で複製を使用しない場合は、この手順をスキップできます。

タスク	説明
手順 3: つの Symantec Endpoint Protection Manager サービスを停止する	新しいバージョンをインストールする前に、すべてのサイトの管理サーバーサービスを手動で停止する必要があります。管理サーバーサービスによって、SEPM 上で実行されている Syslog サービスまたは同様のサービスが停止します。これにより、SEPM ファイルまたはフォルダがロックし、アップグレードが失敗する可能性があります。アップグレード後、管理サーバーは自動的にサービスを開始します。 管理サーバーを他の管理サーバーに複製している場合、SEPM のアップグレード期間中に複製が行われないこと、また、管理サーバーサービスが停止していることを確認してください。 Note: アップグレード中の複製の防止
手順 4: つの Symantec Endpoint Protection Manager ソフトウェアをアップグレードする	ネットワーク内のすべてのサイトで既存のバージョンを上書きして つの Symantec Endpoint Protection Manager の新しいバージョンをインストールします。既存のバージョンが自動的に検出され、すべての設定はアップグレードの間に保存されます。 管理サーバーのアップグレード つの Symantec Endpoint Protection Manager のインストール アップグレード前に Symantec Endpoint Protection Manager ドメインを ICDm クラウドコンソールに登録している場合 (ハイブリッド管理)、ドメインはアップグレードプロセス中に登録されたままになります。アップグレード後に任意のドメインを登録することもできます。 Symantec Endpoint Protection Manager からドメインをクラウドコンソールに登録する
手順 5: アップグレード後に複製関係を復元する	アップグレードした管理サーバーを他の管理サーバーで複製する場合は、複製関係を復元します。 管理サーバ間で複製を使用しない場合は、この手順をスキップできます。 アップグレード前後での、複製の無効化と復元
手順 5: シマンテック製クライアントソフトウェアをアップグレードする	新しいバージョンをインストールする前に、以前のクライアントをアンインストールする必要はありません。インストール後のプロセスで、クライアント設定が保存され、クライアントが最新のバージョンにアップグレードされます。最初に少数のテストコンピュータを含むグループを更新してから、実働ネットワーク全体を更新してください。 クライアントをグループ更新プロバイダとして使用している場合、最初にこれらをアップグレードする必要があります。GUP の更新 「クライアントインストールの準備」と「リモート配備用 Windows と Mac コンピュータの準備」の該当する手順を確認します。その後、以下のいずれかの方法でクライアントをアップグレードします。 - 自動更新: 自動更新は、グループ内の Windows および Mac クライアントソフトウェアを更新する最も簡単な方法です。 手動または [クライアントをパッケージでアップグレード] ウィザードで、管理サーバーでクライアントパッケージをグループに割り当てます。アップグレードプロセスを完了するために、ユーザー側でその他の操作は必要ありません。 自動更新によるクライアントソフトウェアのアップグレード 自動更新では、Symantec Agent for Linux 14.3 RU1 はサポートされていません。 - インストールファイル: Broadcom Download Center からクライアントインストールファイルをダウンロードします。 シマンテックソフトウェアの最新バージョンをダウンロードする - クライアント配備ウィザード: 管理サーバーでクライアント配備ウィザードを実行します。このウィザードでクライアントパッケージを作成できます。このパッケージは、Web リンクや電子メール、リモートプッシュで配備したり、後でローカルにインストールするために保存したりできます。サードパーティツールを使用して配備することもできます。 クライアント配備ウィザードを使ったクライアントのインストール方法の選択

Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象およびサポート非対象アップグレードパス

通常、最新バージョンより前の Symantec Endpoint Protection バージョンでは、これより前のリストのすべてのバージョンがサポートされます。ただし、特定のバージョンのリリースノートを参照して確認してください。

Endpoint Security およびすべてのバージョンの Endpoint Protection のリリースバージョン、リリースノート、新しい修正、およびシステム要件

サポートされているアップグレードパス

- 埋め込みデータベースを使用する Symantec Endpoint Protection Manager バージョン 12.1.6 MP10 以降は、Microsoft SQL Server Express データベース、バージョン 14.3 RU1 MP1 にシームレスにアップグレードされます。12.1.6 MP9 以前から 14.3 RU1 MP1 へのアップグレードは遮断されます。
- Symantec Endpoint Protection Manager 14.x は、12.1.x をシームレスにアップグレードします。ただし、Windows Server 2003、デスクトップオペレーティングシステム、および 32 ビット版オペレーティングシステムのほか、一部のバージョンの SQL Server など、サポートが終了されたものは除きます。
- Symantec Endpoint Protection 14.x クライアントは、サポート対象のオペレーティングシステムにインストールされている以前のすべての 12.1 および 11 クライアントバージョンをシームレスにアップグレードします。例外は、12.1.4 より前の Mac クライアントです。これは、12.1.4 以降にアップグレードするか、アンインストールする必要があります。

Symantec Endpoint Protection 14 の移行に関する考慮事項

つの Symantec Endpoint Protection Manager および Windows クライアント

次のバージョンの 1 つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection の Windows クライアントは最新バージョンに直接アップグレードできます。

- 11.x と Small Business Edition 12.0 (Symantec Endpoint Protection クライアントのみ、サポート対象オペレーティングシステムの場合)
- 12.1.6 MP10 までの 12.1.x バージョン
- 14、14 MP1、14 MP2
- 14 RU1、14 RU1 MP1、14 RU1 MP2
- 14.2、14.2 MP1
- 14.2 RU1、14.2 RU1 MP1
- 14.2 RU2、14.2 RU2 MP1
- 14.3、14.3 MP1
- 14.3 RU1
- 14.3 RU1 MP1

Mac クライアント

次のバージョンの Symantec Endpoint Protection for Mac クライアントは最新バージョンに直接アップグレードできます。

- 12.1.4 から 12.1.6 MP9 までのバージョン
Mac クライアントはバージョン 12.1.6 MP10 では更新されませんでした。
- 14、14 MP1、14 MP2
- 14 RU1、14 RU1 MP1、14 RU1 MP2
Symantec Endpoint Protection for Mac クライアントでは 14.0.1 MP2 の更新は実施されていません。
- 14.2、14.2 MP1
- 14.2 RU1、14.2 RU1 MP1
- 14.2 RU2、14.2 RU2 MP1
- 14.3、14.3 MP1
- 14.3 RU1
- 14.3 RU1 MP1 (2021 年 6 月に利用可能)

Linux クライアント

NOTE

Symantec Agent for Linux 14.3 RU1 は、Linux 用の古い Symantec Endpoint Protection クライアントを検出してアンインストールし、新規インストールを実行します。古い設定は保持されません。

次のバージョンの Symantec Endpoint Protection for Linux クライアントは最新バージョンに直接アップグレードできます。

- 12.1.6 MP9 までの 12.1.x バージョン
Linux クライアントはバージョン 12.1.6 MP10.t では更新されませんでした。
- 14、14 MP1、14 MP2
- 14 RU1、14 RU1 MP1、14 RU1 MP2
- 14.2、14.2 MP1
- 14.2 RU1、14.2 RU1 MP1
- 14.2 RU2、14.2 RU2 MP1
- 14.3、14.3 MP1
- 14.3 RU1
- 14.3 RU1 MP1

Symantec AntiVirus for Linux 1.0.14 は、Symantec Endpoint Protection に直接移行できる唯一のバージョンです。Symantec AntiVirus for Linux の他のすべてのバージョンは、最初にアンインストールする必要があります。管理下クライアントは管理外クライアントに移行できません。

サポート対象外のアップグレードのパス

すべてのシマンテック製品から Symantec Endpoint Protection に移行できるわけではありません。Symantec Endpoint Protection クライアントをインストールする前に、以下の製品をアンインストールする必要があります。

- Symantec AntiVirus および Symantec Client Security (サポートされていません)。
- シマンテック社のすべての Norton 製品
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- 12.1.4 より前の Mac 用 Symantec Endpoint Protection クライアント。または、12.1.4 以降にアップグレードすることもできます。

注:

- 12.1.x より前のバージョンの Symantec Endpoint Protection クライアントの移行はサポートされていません。
- Symantec Endpoint Protection Manager 11.0.x または Symantec Endpoint Protection Manager Small Business Edition 12.0.x を Symantec Endpoint Protection Manager 14 の任意のバージョンに直接アップグレードすることはできません。最初にこれらのバージョンをアンインストールするか、12.1.x にアップグレードしてから 14.x の最新バージョンにアップグレードしてください。
- つの Symantec Endpoint Protection Manager 12.1.6 MP7 のデータベーススキーマのバージョンがバージョン 14 のデータベーススキーマより新しいため、12.1.6 MP7 を 14 にアップグレードできません。その代わり、12.1.6 MP7 を 14 MP1 以降にアップグレードする必要があります。
- 14.0.x では、Windows XP、Server 2003、および Windows XP に基づく Windows Embedded オペレーティングシステムのサポートを終了しました。Symantec Endpoint Protection Manager 14.2 RU1 では、これらのコンピュータをレガシー 12.1.x クライアントとして管理できます。ただし、12.1.x クライアントは EOL です。これらのクライアントについては、Data Center Security (DCS) など、これらのレガシーオペレーティングシステムを引き続きサポートする Symantec 製品を使用することができます。
- 14 MP1 (14.0.2332.0100) から 14 MP1 更新ビルド (14.0.2349.0100) へのアップグレードはサポートされません。
- ダウングレードパスはサポートされません。たとえば、Symantec Endpoint Protection 14.2.1.1 から 12.1.6 MP10 に移行する場合は、最初に Symantec Endpoint Protection 14.2.1 をアンインストールする必要があります。
- ビルド番号はあるが、リリースバージョンに変換する方法がわからない場合は、次を参照してください。

[Endpoint Protection のリリースタイプとバージョンについて](#)

アップグレード前に つの Symantec Endpoint Protection Manager の ディスクの空き容量を増加する

つの Symantec Endpoint Protection Manager のインストールには、利用可能な最低限のディスク容量を確保することが必要です。現在のサーバーまたは新しいハードウェアがハードウェアの最小必要条件を満たしていることを確認してください。アップグレードでは、一時ファイルを作成できるように、利用可能な追加のディスク領域が必要になることがあります。

設定の変更を行う前に、データベースのバックアップを作成してください。

データベースとログのバックアップ

Table 43: 管理サーバーのディスク容量を増やすためのタスク

タスク	説明
LiveUpdate の設定を変更して、必要な容量を削減する	1. [管理]、[サーバー] の順に移動し、[ローカルサイト] を右クリックします。[サイトプロパティの編集] を選択します。 2. [LiveUpdate] タブで、保持するコンテンツリビジョンの数を減らします。アップグレードのために、この設定を 10 まで減らすことができます。つの Symantec Endpoint Protection Manager が余分なリビジョンをパージするための時間を考慮します。ただし、12.1.5 以降のバージョンでは、リビジョンの数を減らすことにより、チェックインするクライアントからの完全な更新のダウンロードがトリガされる可能性があります。このような完全な更新の要求が増加することで、ネットワークパフォーマンスが低下する可能性があります。 Note: コンテンツストレージのデフォルト値と推奨値もバージョン 12.1.5 の時点で変更されています。ただし、アップグレードするバージョンに適切な値に設定する必要があります。 Note: アップグレードの完了後に、リビジョン設定を元の値に戻す必要はありません。つの Symantec Endpoint Protection Manager によるコンテンツの格納および管理方法が改善され、大量のレビジョンがディスクを占有する領域が以前のバージョンより少なくなりました。 クライアント上のコンテンツと定義を更新する方法 LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード
つの Symantec Endpoint Protection Manager データベースから未使用のウイルス定義が削除されていることを確認します。	1. [管理]、[サーバー] に移動し、データベースサーバーを右クリックし、[データベースプロパティの編集] を選択します。 データベース名は、SQLEXPRESSSYM (14.3 RU1 以降) または localhost (143 MPx 以前) です。Microsoft SQL Server データベースの場合、データベースサーバー名はデータベースの場所によって変わります。 2. [ログの設定] タブの [リスクログの設定] の下で、[未使用ウイルス定義を削除] にチェックマークを付けていることを確認します。
共存するプログラムとファイルを再配置するか削除する	• つの Symantec Endpoint Protection Manager と同じコンピュータに他のプログラムがインストールされている場合、それらを別のサーバーに再配置することを考慮します。未使用プログラムを削除できます。 • ストレージを集中的に利用するプログラムが つの Symantec Endpoint Protection Manager と同じコンピュータにインストールされている場合、つの Symantec Endpoint Protection Manager だけをサポートする専用コンピュータを用意することを検討します。 • つの Symantec Endpoint Protection Manager の一時ファイルを削除します。 削除可能な一時ファイルのリストについては、ナレッジベースの「Symantec Endpoint Protection Manager directories contain many .TMP folders consuming large amounts of disk space」を参照してください。 Note: プログラムとファイルの削除後、ハードドライブのデフラグを行います。
外部データベースを使用する	Symantec Endpoint Protection データベースが つの Symantec Endpoint Protection Manager と同じコンピュータにある場合、Microsoft SQL Server データベースを別のコンピュータにインストールすることを考慮します。大量のディスク容量を節約でき、ほとんどの場合、パフォーマンスが向上します。 データベースの種類の選択について

NOTE

アップグレードの前に、クライアントコンピュータにも十分なディスク容量があることを確認します。システムの必要条件を確認し、必要に応じて、不要なプログラムとファイルを削除してから、クライアントコンピュータハードドライブのデフラグを行います。

[Symantec Endpoint Protection Manager のディスク容量不足](#)

管理サーバーのアップグレード

アップグレードではすべての管理サーバーをまずアップグレードしてからクライアントをアップグレードする必要があります。

負荷分散、フェールオーバー、レプリケーションをサポートする環境の管理サーバーをアップグレードする場合は、決まった順番で管理サーバーを準備してアップグレードする必要があります。

WARNING

アップグレードに失敗しないためには、インストールの種類に該当するシナリオの手順に従う必要があります。

Table 44: アップグレードタスク

タスク	説明
管理サーバーのアップグレード	システムの必要条件とサポート対象のアップグレードパスを見直して、管理サーバーをアップグレードしてから、管理サーバー設定ウィザードで設定します。 14 では、つの Symantec Endpoint Protection Manager のアップグレードに次のことが適用されます。 - Windows Server 2003、すべてのデスクトップオペレーティングシステム、32 ビットオペレーティングシステムはサポート外です。 - SQL Server 2005 はデータベース用としてサポート外です。サポートは SP4 以前の SQL Server 2008、SP3 以前の SQL Server 2008 R2 に対しても対象外になりました。 - アップグレード時に SQL Server システム管理者の資格情報を入力することが必要になりました。 Note: Windows 7/Server 2008 R2 以降で仮想サービスアカウントを正しく実行するには、ドメインセキュリティポリシーの編集が必要になることがあります。 Note: インストール時または設定時に、ユーザー権利がない、またはユーザー権利を読み取れないというエラーが発生する つの Symantec Endpoint Protection Manager のインストール Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象アップグレードパス
管理サーバーへのログオン	つの Symantec Endpoint Protection Manager のログオンパネルが表示されたら、ログオンクレデンシャルを使ってコンソールにログオンできます。 つの Symantec Endpoint Protection Manager コンソールへのログオン

NOTE

アップグレード後のコンピュータの再起動は必須ではありませんが、再起動してログオンするとパフォーマンスが向上することがあります。

[フェールオーバーと負荷分散の設定](#)

[サイトと複製の設定](#)

埋め込みデータベースから Microsoft SQL Server Express データベースへのアップグレードに関するベストプラクティス

14.3 RU1 では、つの Symantec Endpoint Protection Manager (SEPM) と共にインストールされるデフォルトデータベースが、埋め込みデータベースから Microsoft SQL Server Express 2017 データベースに変更されました。管理サーバー設定ウィザードのデフォルト設定を使用して、管理サーバーを初めてアップグレードまたはインストールする場合、SQL Server Express データベースが自動的にインストールされ、埋め込みデータベースが置き換えられます。

バージョン 14.3 RU1 以降にアップグレードする場合、管理サーバーのコンピュータは特定の要件を満たす必要があります。そうでない場合、管理サーバーのアップグレードを続行できません。これらの問題が発生した場合、管理サーバー設定ウィザードによって通知されるので、問題を修正できます。

アップグレードする前に把握しておくこと

アップグレードする前に、インストール前に修正が必要になる可能性がある以下の問題を確認してください。

データベースサイズの不足	SQL Server Express データベースのデータファイルおよびログデータの最大容量は 10 GB です。Symantec Endpoint Protection Manager は、インストールが開始される前に埋め込みデータベースのバックアップを作成します。このバックアップが 10 GB を超える場合、アップグレードを続行できません。アップグレードの開始前、またはアップグレード中に、データの量を削減する必要があります。データベースのサイズが大きすぎると、管理サーバー設定ウィザードによって通知されます。インストールを開始する前に、データベースが 10 GB を超えている場合は、以下のタスクを実行します。 Microsoft SQL Server Express へのアップグレード前にデータベースがいっぱいになった場合のデータベースサイズの削減 Microsoft SQL Server Express データベースと Microsoft SQL Server データベースの両方で、FILESTREAM という機能を使用してデータベースサイズを削減します。アップグレード中にデータベースのサイズが大きすぎるか、またはサイズの上限に近づいていることが判明した場合は、以下のアクションを実行できます。 Microsoft SQL Server データベースの FILESTREAM の有効化 Note: SQL Server データベースを使用している場合は、データベースのサイズを定期的に調べて、データベースが最大サイズに達していないことを確認します。 Microsoft SQL Server データベースのファイルサイズの拡大
ディスク容量の不足	アップグレードを実行するために、管理サーバーコンピュータに少なくとも 10 GB の空きディスク容量があることを確認します。 デフォルトの Microsoft SQL Server Express データベースにアップグレードするためにより多くのディスク容量を使用できるようにする
Symantec Endpoint Protection Manager は、データベースと通信しません。	Symantec Endpoint Protection Manager は、証明書を使用して、Symantec Endpoint Protection (SEPM) と Microsoft SQL Server Express または SQL Server データベースの間の通信を認証します。SEPM がいずれかの SQL Server データベースに接続できるようにするには、証明書を生成して 1 つの Symantec Endpoint Protection Manager コンピュータにインポートする必要があります。証明書が存在しないか、期限切れになっているか、期限切れになりそうな場合、SEPM とデータベースの間の接続は失敗します。 Symantec Endpoint Protection Manager と Microsoft SQL Server の間の暗号化通信の設定 管理サーバーがデータベースに接続しているかどうかを確認するには、以下を参照してください。 管理サーバーのデータベースとの接続の検証

Microsoft SQL Server Express へのアップグレードに関する問題のトラブルシューティング	アップグレード時には、以下のいずれかの問題が発生する可能性があります。 - Windows Update が最新でないか、Windows Update サービスが実行されていません。この問題のトラブルシューティングを行うには、SEPM のインストールをキャンセルして、最新の更新を実行するか Windows Update サービスを再起動し、コンピュータを再起動してから、Symantec Endpoint Protection Manager のインストールを続行します。 - SQL Server Express データベースがインストールされません。トラブルシューティングを行うには、データベースログを確認します。 Endpoint Protection Manager のデフォルトの SQL Server Express データベースのインストールに関する問題のトラブルシューティング - Symantec Endpoint Protection Manager とデータベースの間の接続がありません。 管理サーバーのデータベースとの接続の検証 つの Symantec Endpoint Protection Manager とコンソールまたはデフォルトデータベースの間における通信の問題のトラブルシューティング - Symantec Endpoint Protection Manager が実行されているコンピュータの IP アドレスとホスト名を変更します。 コンピュータの IP アドレスとホスト名を変更した後の Symantec Endpoint Protection Manager の再設定

データベースとログのバックアップ

Microsoft SQL Server Express へのアップグレード前にデータベースがいっぱいになった場合のデータベースサイズの削減

デフォルトの Microsoft SQL Server Express データベースでは、データファイルとログデータに対してサイズ制限が 10 GB に設定されています。10 GB を超えるサイズの埋め込みデータベースからアップグレードする場合、Microsoft SQL Server Express へのアップグレード中にアップグレードプロセスを続行できません。

管理サーバーの設定ウィザードによって、データベースサイズが大きすぎることで検出されると、以下のメッセージが表示される場合があります。

```
SQL Server Express ##### 10 GB #####
#####
```

デフォルトのデータベースサイズが大きすぎる場合は、アップグレードを一時停止し、以下の手順を実行します。

ステップ 1: ログの収集日数を減らす

次のファイルで、日数を減らします: C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties

- scm.sqlexpress.migration.otherlog.days=7
- scm.sqlexpress.migration.learnedapps.days=0
- scm.sqlexpress.migration.clientserveractivity.days=3
- scm.sqlexpress.migration.traffic.days=7
- scm.sqlexpress.migration.packet.days=7
- scm.sqlexpress.migration.security.days=7

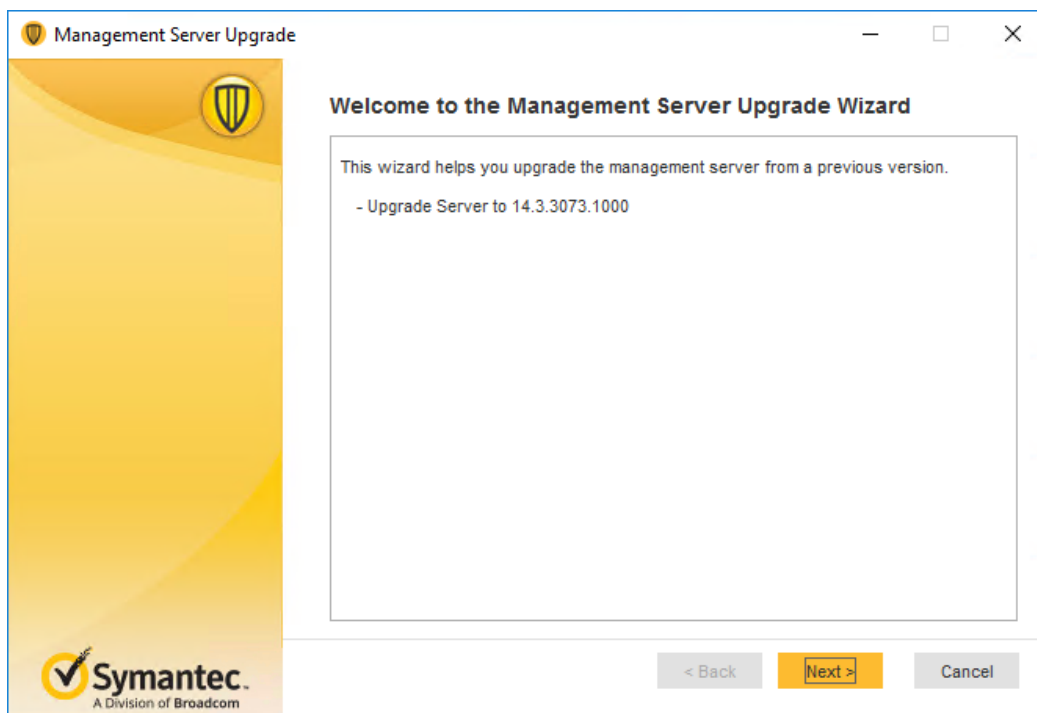
これにより、SQL Server Express データベースに移行されるデータの量が削減されます。

注: デフォルトでは、データベースサイズを小さくするため

に、scm.sqlexpress.migration.clientserveractivity.days がすでに 7 に設定されています。

ステップ 2: 管理サーバーアップグレードウィザードを再起動する

..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat をダブルクリックします。



NOTE

これらの変更を行う前に [データベースのバックアップと復元] ダイアログボックスを開いている場合、...
\\Symantec\\Symantec Endpoint Protection Manager\\bin\\dbtools.bat をダブルクリックして再起動します。

Microsoft SQL Server Express へのアップグレード前にデータベースのサイズを 10 GB 未満に削減する

Microsoft SQL Server データベースの FILESTREAM の有効化

このトピックでは、Microsoft SQL Server データベースの FILESTREAM を有効にする方法について説明します。

Microsoft SQL Server データベースは、FILESTREAM という機能を使用して、データベース サイズを削減し、データベースのパフォーマンスを向上させることができます。

- Microsoft SQL Server Express データベースの容量には 10 GB の制限があるので、FILESTREAM を有効にする必要があります。独自の SQL Server Express インスタンスをインストールする場合は、FILESTREAM を有効にする必要があります。
- 埋め込みデータベース (14.3 MP1 以前) から 14.3 RU1 以降にアップグレードする場合、FILESTREAM を有効にする必要はありません。アップグレード ウィザードまたは設定ウィザードで FILESTREAM が自動的に有効になります。
- Microsoft SQL Server データベースでは FILESTREAM の有効化は必須ではありませんが、パフォーマンスを向上させるために推奨されます。ローカルの SQL Server データベースの場合は、管理サーバーのアップグレードおよびインストールウィザードで FILESTREAM を有効にできます。リモートの Microsoft SQL Server データベースの場合、SQL Server データベースがインストールされているコンピュータ上で FILESTREAM を手動で有効にします。

アップグレードウィザードまたは設定ウィザードを実行して以下のメッセージが表示された場合、[はい] をクリックして FILESTREAM を有効にします。

FILESTREAM ##### Microsoft SQL Server #####

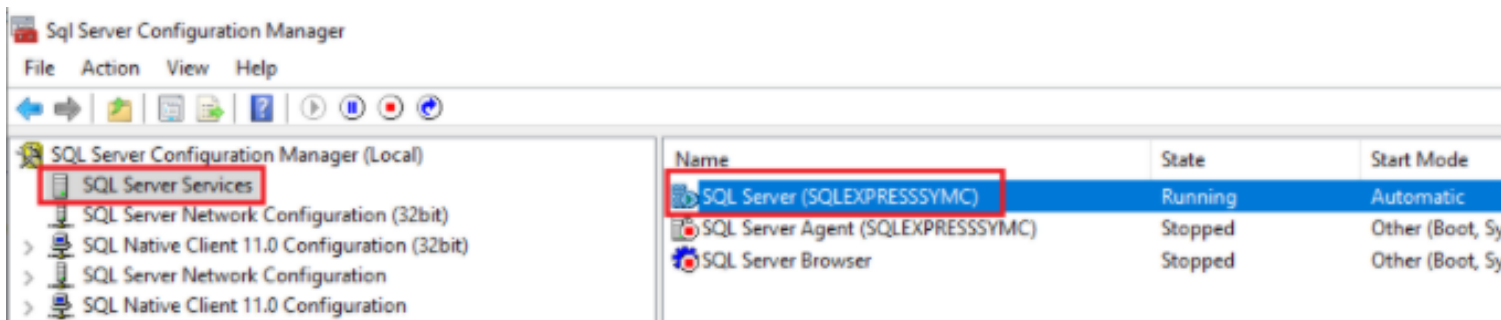
NOTE

アップグレードまたはインストールし、FILESTREAM 機能を現時点で有効にしない場合は、[いいえ] をクリックします。

アップグレードする場合は、管理サーバーアップグレードウィザードが閉じます。FILESTREAM を有効にした後、アップグレードウィザードを再起動して管理サーバーのアップグレードを続行する必要があります。Symantec Endpoint Protection Manager コンピュータで、..\Symantec\Symantec Endpoint Protection Manager\bin\upgrade.bat をクリックします。

FILESTREAM を手動で有効にするには

1. [スタート] メニューで、[Microsoft **SQL** Server] を展開し、[**SQL Server** 構成マネージャー] をクリックします。
2. サービスの [**SQL Server** 構成マネージャ] リストで、[**SQL Server** サービス] を選択し、FILESTREAM を有効化する SQL Server のインスタンスを見つけます。



3. インスタンスを右クリックして [プロパティ] をクリックします。
4. [SQL サーバプロパティ] ダイアログボックスで、[FILESTREAM] タブをクリックします。
5. [Transact-SQL アクセスに対して **FILESTREAM** を有効にする] を選択し、[ファイル I/O ストリーム アクセスに対して **FILESTREAM** を有効にする] ボックスにチェックマークを付けます。
6. [適用] > [OK] の順にクリックします。
7. SQL Server のインストールを選択し、[再起動] をクリックすることで、SQL Server データベースを再起動します。

FILESTREAM (SQL Server)

Microsoft SQL Server Express へのアップグレード前にデータベースのサイズを 10 GB 未満に削減する

デフォルトの Microsoft SQL Server Express データベースでは、データファイルとログデータに対してサイズ制限が 10 GB に設定されています。データファイルには、インストールパッケージ、ウイルス定義、ポリシー、アラート、および学習済みアプリケーションなどの項目が含まれます。サイズが 10 GB を超える埋め込みデータベース (14.3 MP1 以前) からアップグレードする場合、SQL Server Express へのアップグレード処理を続行できません。管理サーバー設定ウィザードによって、データベースサイズが大きすぎることが検出されると、以下のメッセージが表示される場合があります。

```
##### SQL Server Express # 10 GB #####
#####

##### Microsoft SQL Server Express # 10 GB #####
##### 10 GB #####
```

最初に、以下のいずれかのタスクを使用して、既存の埋め込みデータベースの容量を減らす必要があります。

- [続行] をクリックして、アップグレードプロセスの開始時に管理サーバー設定ウィザードによってデータベースのサイズが削減されるようにします。
- 管理サーバー設定ウィザードをキャンセルし、以下の手順に従ってデータベースのサイズを削減してからウィザードを再起動します。

使用可能なデータベースのサイズを手動で削減するには

- ステップ 1: つの **Symantec Endpoint Protection Manager** で使用しない複製パートナーを削除します。

[サイトの削除](#)

- ステップ 2: ログおよび学習済みアプリケーションのデータのサイズを削減します。

[ログサイズとデータベース内のログエントリの保存期間の指定](#)

Database Properties for karin-2012\SQLEXPRESS\SYMCM

General Log Settings Backup Settings

Specify the size of logs maintained in the database for the site.

Management Server Log Settings

System Administrative Log Limit:	10000	entries	Expires after:	60	days
System Client-Server Activity Log Limit:	10000	entries	Expires after:	60	days
Audit Log Limit:	10000	entries	Expires after:	60	days
System Server Activity Log Limit:	10000	entries	Expires after:	60	days

Client Log Settings

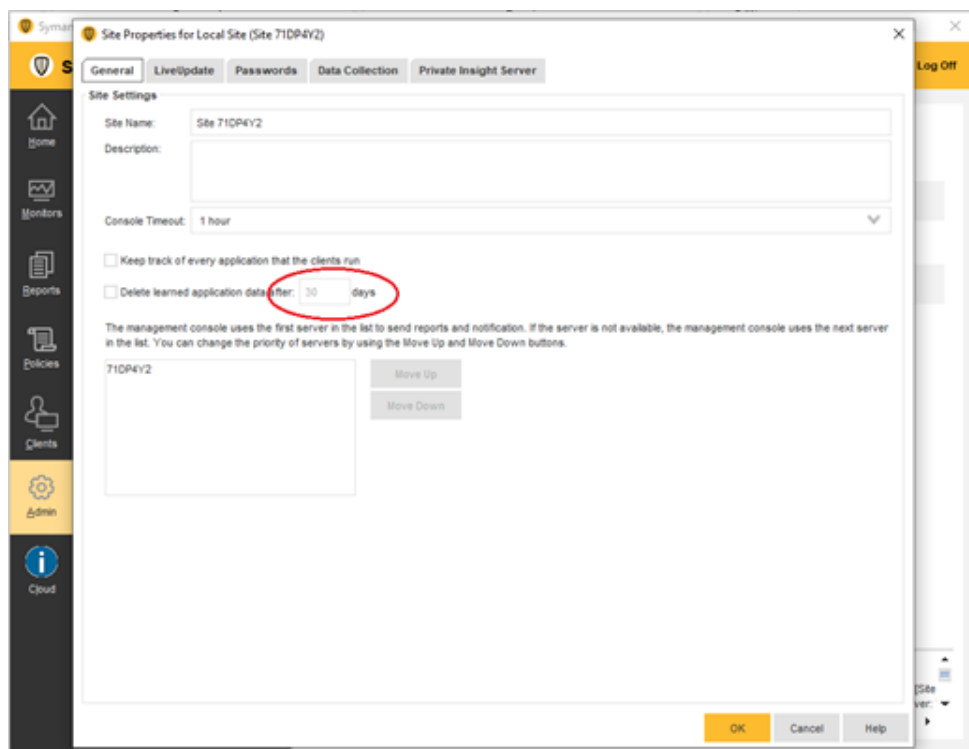
Client Activity Log Limit:	10000	entries	Expires after:	60	days
Security Log Limit:	10000	entries	Expires after:	60	days
Traffic Log Limit:	50000	entries	Expires after:	60	days
Packet Log Limit:	10000	entries	Expires after:	60	days
Control Log Limit:	20000	entries	Expires after:	60	days

Risk Log Settings

Delete risk events after:	60	days	Compress risk events after:	7	days
Delete acknowledged notifications after:	30	days	Delete unacknowledged notifications after:	30	days
Delete scan events after:	30	days	Delete commands after:	30	days

☒ Delete unused virus definitions ☒ Delete EICAR events

OK Cancel Help



アプリケーション学習の有効化

- ステップ 3: データベース保守スケジュールのデフォルト設定を変更します。
 - a. 管理サーバーを停止します。
 - b. ファイル `C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\etc\conf.properties` で、以下のエントリの秒数を減らします。


```
scm.timer.objectsweep=1800
scm.timer.objectsweep.delay=60
```

 注: これらのエントリがファイルに含まれていない場合は、追加します。このステップにより、データベースが不要なデータを削除としてマークする頻度が増加します。
Symantec Endpoint Protection Manager: データベース保守はどのようにスケジュールされていますか?
 - c. 管理サーバーを再起動し、数時間以上待機します。
- 管理サーバーサービスの停止と開始
- ステップ 4: すべてのパートナー間の複製を少なくとも 1 回実行するようにスケジュールします。より頻繁に複製することをお勧めします。
- 新しいサイトを複製パートナーとして既存のサイトにインストールする
- ステップ 5: スケジュールされた各複製の後に数時間待機してから、アップグレードを再起動します。
- ステップ 6: データベースバックアップを再実行して、復元を試みます。

デフォルトの Microsoft SQL Server Express データベースにアップグレードするためにより多くのディスク容量を使用できるようにする

Microsoft SQL Server Express データベースにアップグレードするために、つの Symantec Endpoint Protection Manager コンピュータに少なくとも 10 GB の空きディスク容量がない場合は、次のメッセージが表示される場合があります。

```
##### Microsoft SQL Server Express #####
#####10 ##### x #####
###
```

少なくとも 10 GB のディスク容量が使用可能でない限り、アップグレードプロセスを続行することはできません。ディスク容量を増やすには、以下の手順に従います。

ステップ 1: 未使用のファイルおよび一時ファイルの削除

Windows の一時ファイルは次の場所にあります。

- C:\Windows\Temp
- C:\Users\<username>\AppData\Local\Temp

Windows 10 でのディスククリーンアップ

ステップ 2: ごみ箱を空にする

ステップ 3: 追加の SEPM ファイルの削除

1. 前のステップで十分なディスク容量が削減されない場合は、追加の SEPM ファイルを削除します。

net stop semsrv コマンドを使用して、管理サーバーサービスを停止します。

管理サーバーサービスの停止と開始

2. 以下の SEPM ファイルを別のディスクドライブに移動します。

- ..\Symantec\Symantec Endpoint Protection Manager\Inetpub\ClientPackages
- ..\Symantec\Symantec Endpoint Protection Manager\Inetpub\content
- ..\Symantec\Symantec Endpoint Protection Manager\data\backup
- ..\Symantec\Symantec Endpoint Protection Manager\data\inbox

3. 管理サーバーサービスを再起動します。

ステップ 4: データベースのバックアップ設定の変更

- [保存するデータベースバックアップの世代数] オプションが 1 (デフォルト) に設定されていることを確認します。
- [ログのバックアップ] はオフのままにします。

データベースの自動バックアップの実行

ステップ 5: Symantec Endpoint Protection Manager によって使用されないファイルを別のディスクドライブに移動します。

証明書の期限が切れている場合は、[Symantec Endpoint Protection Manager と Microsoft SQL Server の間の暗号化通信の設定](#) を参照してください。

Symantec Endpoint Protection Manager と Microsoft SQL Server の間の暗号化通信の設定

Symantec Endpoint Protection Manager は、証明書を使用して、Symantec Endpoint Protection (SEPM) と Microsoft SQL Server Express または SQL Server データベースの間の通信を認証します。SEPM がいずれかの SQL Server データベースに接続できるようにするには、証明書を生成してその Symantec Endpoint Protection Manager コンピュータにインポートする必要があります。証明書が存在しないか、期限切れになっているか、期限切れになりそうな場合、SEPM とデータベースの間の接続は失敗します。

証明書をインポートしていない場合、管理サーバーといずれかの SQL Server データベースをインストールまたはアップグレードできます。ただし、管理サーバー設定ウィザードは、証明書がすでに期限切れになっているか、今後 30 日間に期限切れになるかを検出します。SEPM は、30 日が経過するたびに通知を送信して、管理者に証明書をインポートするよう通知します。以下のメッセージが表示される場合があります。

```
Symantec Endpoint Protection Manager #### 30 #####Microsoft SQL Server
#####
```

手順 1: 自己署名証明書の生成

組織に認証局 (CA) が署名した証明書がない場合は、それを生成する必要があります。この手順では、デフォルトの自己署名 つの Symantec Endpoint Protection Manager (SEPM) 証明書を生成して、CA が署名した証明書で置き換える方法について説明します。

「[Endpoint Protection Manager で署名された証明書の使用](#)」を参照してください。

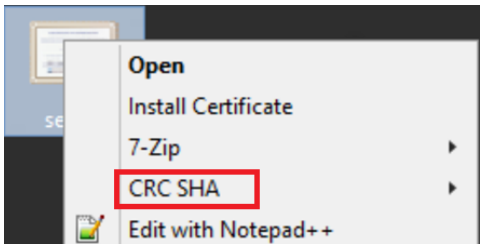
手順 2: SQL Server 用の永続証明書の設定

SQL Server データベースエンジンのインスタンスで暗号化された接続を有効にし、SQL Server 設定マネージャを使用して証明書を指定する必要があります。「[データベースエンジンへの暗号化された接続を有効にする](#)」の「SQL Server の設定」を参照してください。

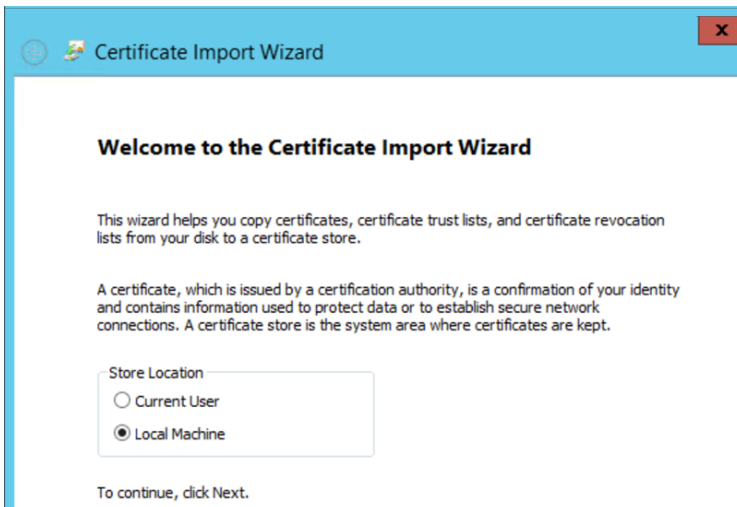
手順 3: つの Symantec Endpoint Protection Manager コンピュータ上の Windows への SQL Server 証明書のインポート

管理サーバーコンピュータでは、SQL Server の公開証明書がプロビジョニングされている必要があります。管理サーバーコンピュータ上で証明書をプロビジョニングするには、Windows に証明書をインポートします。サーバーコンピュータは、証明書のルート権限を信頼するように設定する必要があります。

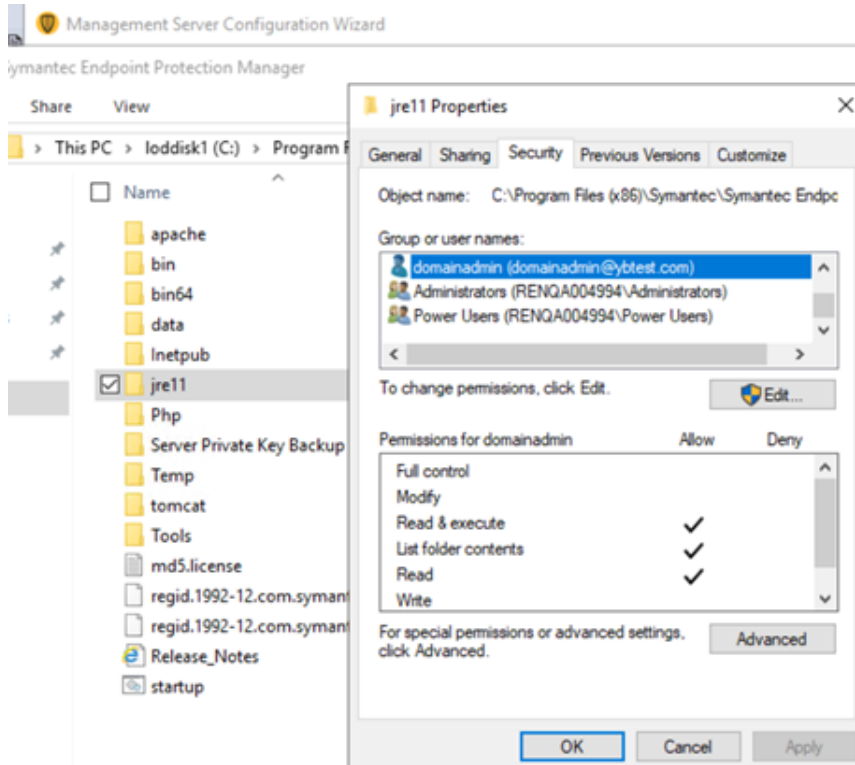
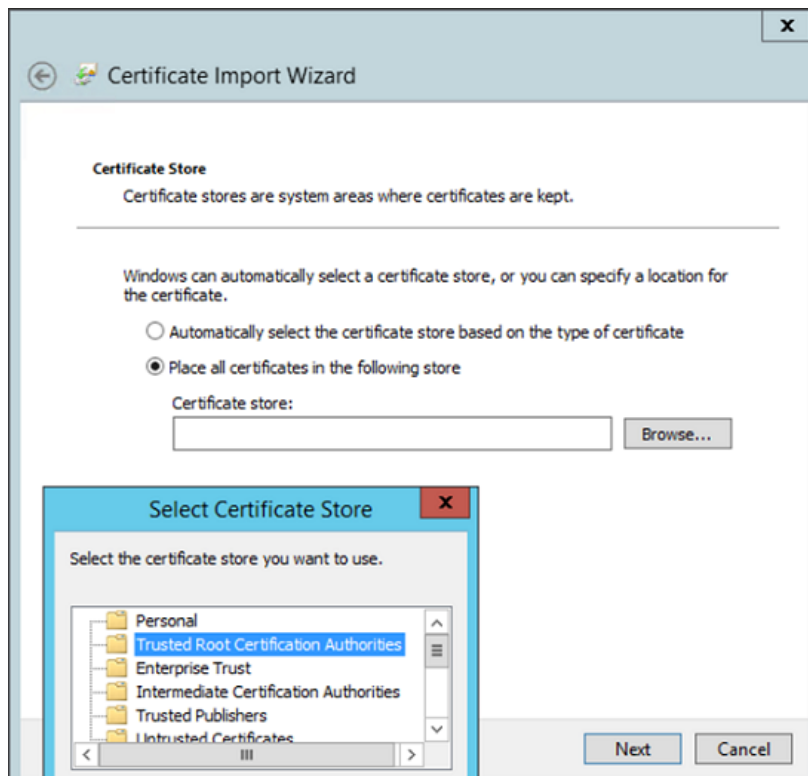
1. SEPM がインストールされている Windows サーバで、証明書を右クリックします。



2. 証明書のインポートウィザードで、証明書をインポートする手順に従います。
[保存場所] で、[ローカル コンピューター] を選択します。



[証明書をすべて次のストアに配置する] を選択して [参照] をクリックし、[証明書ストアの選択] ダイアログボックスで [信頼されたルート証明機関] をクリックします。



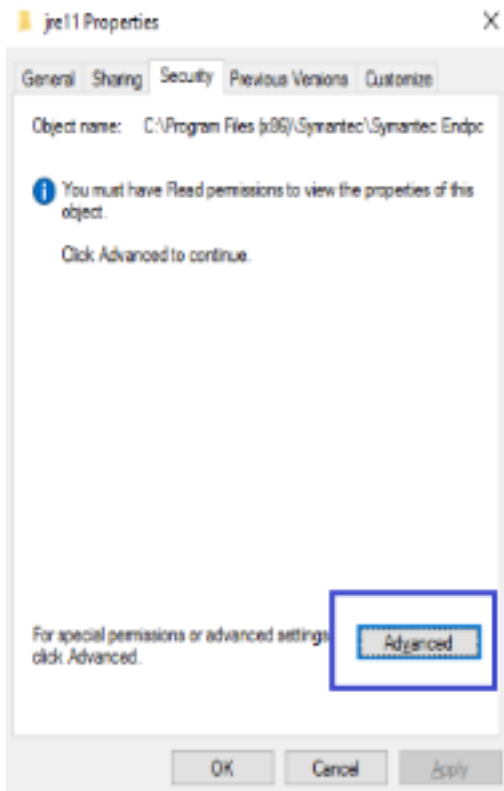
3. [OK] をクリックして [次へ] をクリックします。

手順 4: jre11 フォルダの権限の設定

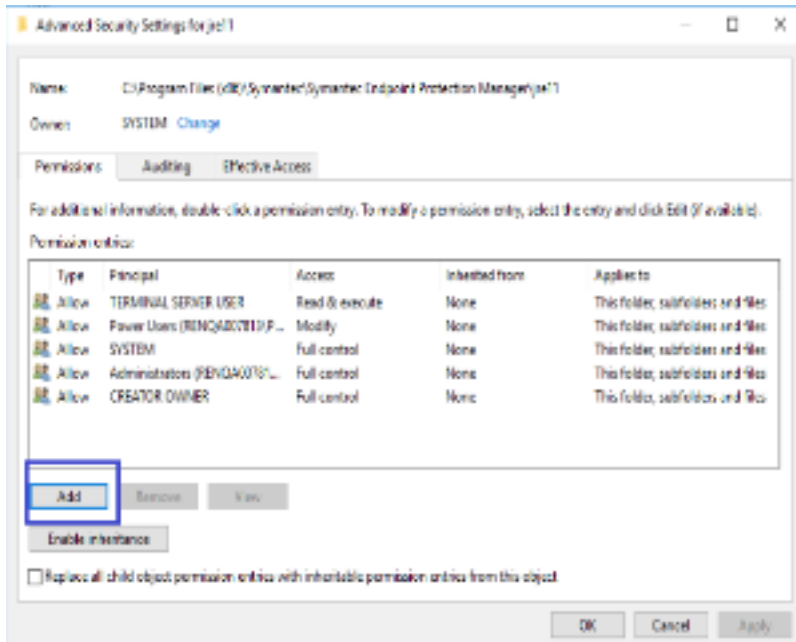
NOTE

SQL Server が Windows 認証でドメイン管理者を使って設定されている場合、そのドメイン管理者には、つの Symantec Endpoint Protection Manager サーバー上の jre11 フォルダの読み取りと実行、フォルダーの内容の一覧表示、および読み取りのアクセス許可が必要です。

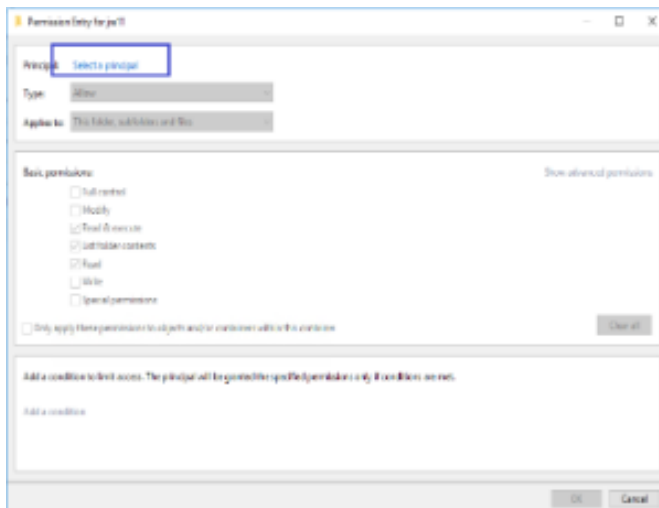
1. Symantec Endpoint Protection Manager サーバーで、\...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager フォルダに移動し、jre11 フォルダを右クリックして [プロパティ] をクリックします。
2. [ファイルのプロパティ] ウィンドウの [セキュリティ] タブで、[詳細設定] をクリックします。



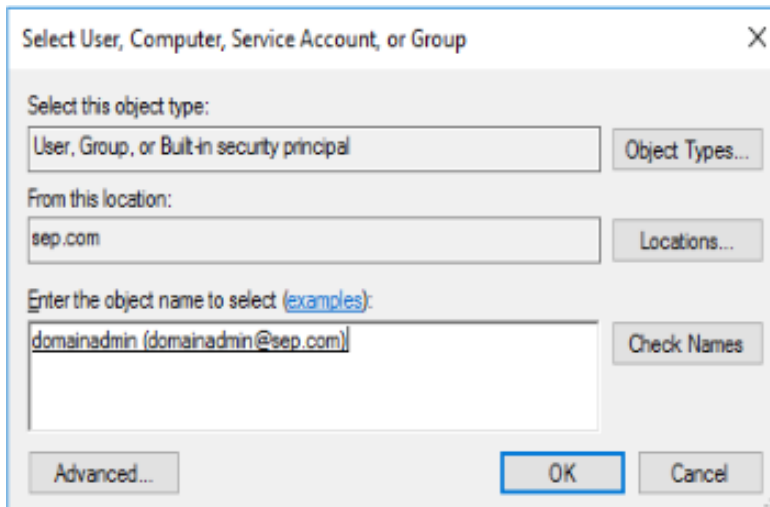
3. [セキュリティの詳細設定] ウィンドウの [アクセス許可] タブで、[追加] をクリックします。



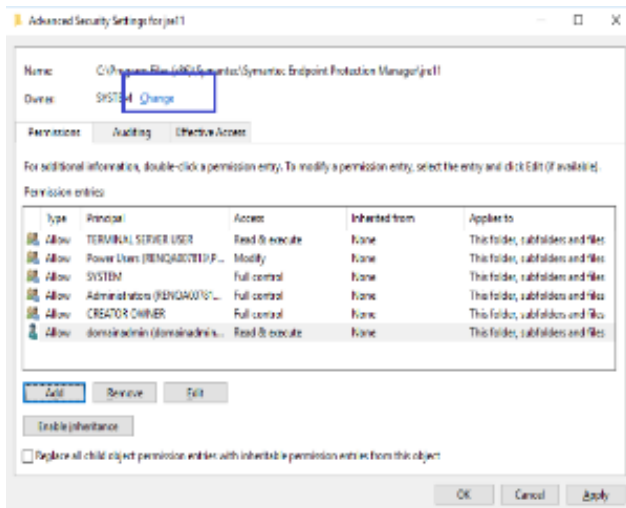
4. [アクセス許可エントリ] ウィンドウで、[プリンシパルの選択] をクリックします。



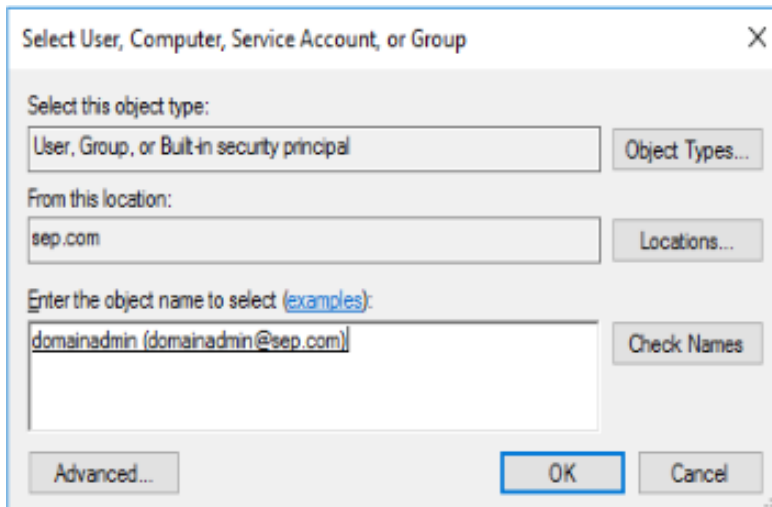
5. [ユーザー、コンピューター、サービス アカウントまたはグループの選択] ウィンドウで、**domainadmin** ユーザーを追加し、[OK] をクリックします。



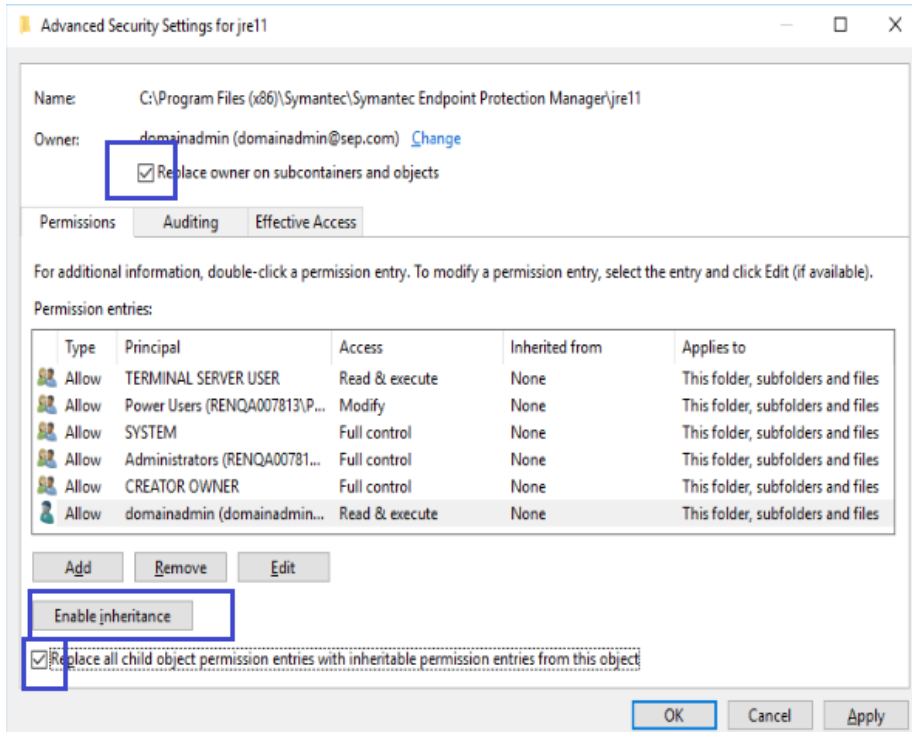
6. [アクセス許可エントリ] ウィンドウで、[OK] をクリックします。
7. [セキュリティの詳細設定] ウィンドウの [アクセス許可] タブで、「**domainadmin**」を選択して [変更] をクリックします。



8. [ユーザー、コンピューター、サービス アカウントまたはグループの選択] ウィンドウで、**domainadmin** ユーザーを再度追加し、[OK] をクリックします。



9. [セキュリティの詳細設定] ウィンドウで、[サブコンテナとオブジェクトの所有者を置き換える] と [子オブジェクトのアクセス許可エントリすべてを、このオブジェクトからの継承可能なアクセス許可エントリで置き換える] にチェックマークを付けた後、[継承の有効化] をクリックし、[適用] をクリックします。



10. [はい] をクリックし、[OK] をクリックして確定します。
11. [ファイルのプロパティ] ウィンドウで、**domainadmin** ユーザーが必要なすべてのアクセス許可を持っていることを確認し、[OK] をクリックします。

手順 5: 管理サーバーの設定ウィザードを開き、[Windows 認証] オプションでサーバーの設定を完了

ウィザードを開くには、\...\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\bin フォルダに移動し、sca.exe ファイルをダブルクリックします。

Management Server Configuration Wizard

Step One: Database Server Authentication
This step must be completed first.

Authentication type: Windows Authentication

Database server: renqa007813.sep.com

SQL server port: 1433

Windows user name: sepdomainadmin

Windows user password: *****

SQL Server client folder: C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\130\Tools\Binn\

Connect to database (required)

Step Two: New Database Creation

Database name: sem5

Database data folder: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\DATA

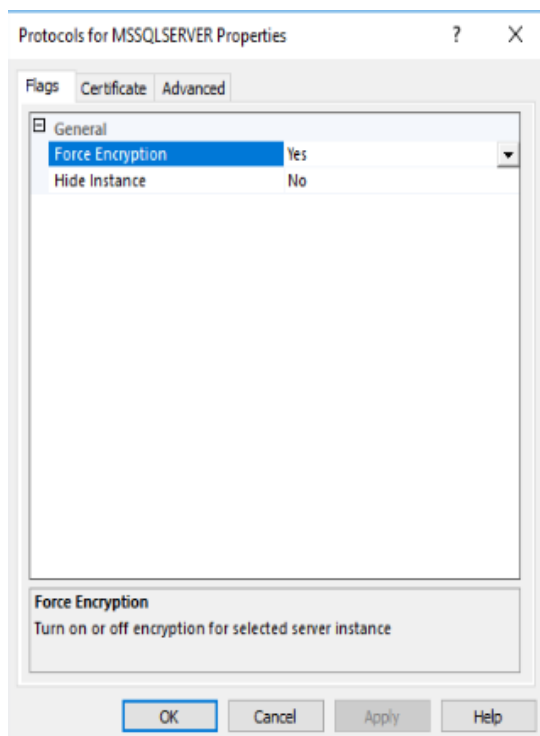
< Back Next > Cancel

手順 6: 通信が暗号化されており **SQL Server** 証明書が使用されていることを確認

1. 管理サーバーで、ファイル C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\tomcat\conf\Catalina\localhost\root.xml を開き、**encrypt=true** および **trustServerCertificate=false** であることを確認します。

```
<?xml version="1.0" encoding="UTF-8"?>
- <Context reloadable="false" privileged="true" crossContext="true" antiResourceLocking="false" antiJARLocking="false">
  <Resource validationQueryTimeout="60" validationQuery="SELECT count(*) FROM CONNECTION_TEST" username="domainadmin"
    url="jdbc:sqlserver://renqa007813.sep.com:1433;databaseName=sem5;integratedSecurity=true;encrypt=true;trustServerCertificate=false;domain=sep"
    type="javax.sql.DataSource" removeAbandonedOnBorrow="true" password="{V01}B7DAEBA1EF9473FAA7C9D103B5C3C712" name="jdbc/metadatabase"
    mssqlSocketReadTimeout="1800" maxWaitMillis="30000" maxTotal="150" maxIdle="50" logAbandoned="false" factory="com.sygate.scm.pool.ScmDataSourceFactory"
    driverClassName="com.microsoft.sqlserver.jdbc.SQLServerDriver" domain="sep" auth="Container"/>
</Context>
```

2. SQL Server で、[MSSQLSERVER のプロトコルのプロパティ] を開き、[強制的に暗号化] が [はい] になっていることを確認します。



3. SQL Server で以下のクエリーを実行し、つの Symantec Endpoint Protection Manager と SQL Server の間の接続が暗号化されていることを確認します。

```
SELECT session_id, connect_time, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

encrypt_option=TRUE であるかどうかを確認します。

SQLQuery1.sql - RE...Administrator (53))

```
SELECT session_id, net_transport, encrypt_option, auth_scheme, client_net_address FROM sys.dm_exec_connections
```

100 %

Results Messages

	session_id	net_transport	encrypt_option	auth_scheme	client_net_address
1	51	Shared memory	TRUE	NTLM	<local machine>
2	52	TCP	TRUE	SQL	10.32.168.100
3	53	Shared memory	TRUE	NTLM	<local machine>
4	54	Shared memory	TRUE	NTLM	<local machine>
5	55	TCP	TRUE	SQL	10.32.168.100
6	58	TCP	TRUE	SQL	10.32.168.100
7	57	TCP	TRUE	SQL	10.32.168.100
8	59	TCP	TRUE	SQL	10.32.168.100
9	60	TCP	TRUE	SQL	10.32.168.100

複数の埋め込みデータベースと管理サーバーを使う環境のアップグレード

複数の埋め込みデータベースと管理サーバーを使う環境では、以下の点が影響します。

- 組み込みデータベースがフェールオーバーまたは負荷分散されたサーバーをサポートしないため、管理サーバーは Symantec Endpoint Protection のフェールオーバーまたは負荷分散使いません。
- 管理サーバーは Symantec Endpoint Protection 複製パートナーです。

どのサイトにも、最初に管理サーバーをインストールしたコンピュータがあります。この管理サーバーは、暗号化キーまたは暗号化パスワードなどの重要なサイト情報を含むため、最初にアップグレードする必要があります。その後で、レプリケーション用にインストールしたその他の管理サーバーをアップグレードします。

NOTE

14.3 RU1 以降、埋め込みデータベースは Microsoft SQL Server Express データベースに置き換えられます。SQL Server Express では、フェールオーバーと負荷分散がサポートされています。

複数の埋め込みデータベースと管理サーバーを使う環境をアップグレードするには

1. 最初の つの Symantec Endpoint Protection Manager をインストールしたコンピュータの認証とログイン。
つの Symantec Endpoint Protection Manager にログインしないでください。複製を使う場合に、最初に無効にする必要はありません。Symantec Endpoint Protection は、製品バージョンが一致しない場合に複製を許可しません。
2. 管理サーバーのアップグレード。
3. その他のすべての管理サーバーを 1 つずつアップグレードします。

管理サーバーサービスの停止と開始

アップグレードする前に、サイトのすべての管理サーバーで つの Symantec Endpoint Protection Manager サービスを手動で停止する必要があります。アップグレード後、サービスは自動的に開始されます。

WARNING

サーバーをアップグレードする前に つの Symantec Endpoint Protection Manager サービスを停止しないと、既存の Symantec Endpoint Protection データベースが壊れる危険性があります。

NOTE

管理サーバーサービスを停止すると、クライアントはこのサービスに接続できなくなります。クライアントがネットワークに接続するために管理サーバーと通信する必要がある場合、このサービスが再起動されるまでクライアントのアクセスは拒否されます。

たとえば、クライアントはホストインテグリティ検査に成功するために管理サーバーと通信する必要があります。

新リリースへのアップグレード

1. つの Symantec Endpoint Protection Manager サービスを停止するには、[スタート] > [設定] > [コントロールパネル] > [管理ツール] > [サービス] をクリックします。
2. [サービス] ウィンドウの [名前] で、スクロールして [つの Symantec Endpoint Protection Manager] を右クリックします。
3. [停止] をクリックします。
4. [サービス] ウィンドウを閉じます。

WARNING

[サービス] ウィンドウを閉じないと、アップグレードに失敗する場合があります。

-
5. すべての つの Symantec Endpoint Protection Manager インストールに対して上記の手順を繰り返します。

NOTE

つの Symantec Endpoint Protection Manager サービスを開始するには、この手順を再び実行して、[中止] ではなく [開始] をクリックします。

6. コマンドラインを使用して つの Symantec Endpoint Protection Manager サービスを停止するには、コマンドプロンプトから以下のように入力します。

```
net stop semsrv
```

7. コマンドラインを使用して つの Symantec Endpoint Protection Manager サービスを開始するには、コマンドプロンプトから以下のように入力します。

```
net start semsrv
```

アップグレード中の複製の防止

アップグレードする管理サーバーの複製パートナーとして設定されている管理サーバーでは、複製が行われないようにする必要があります。アップグレード中に複製パートナーが複製を起動すると、予測不能な結果が生じる可能性があります。

アップグレード中の複製を防ぐには、以下のいずれかのタスクを実行します。

- アップグレード期間外に複製が発生するようにスケジュールを再設定します。手順が簡単なので、この方法が推奨されます。
- アップグレード前に複製を一時的に停止し、複製が完了した後に復元します。

複製のスケジュールの再設定

スケジュールを修正する方法の利点は、他のサイトは複製されないため、クライアントがアップグレードされるまで、それらのサイトがクライアントにサービスを提供し続けることです。アップグレードが完了した後、それらのサイトでは、強制的にワントタイム複製を実行することで複製をテストし、スケジュールを以前に設定したスケジュールと頻度に戻すことができます。

以下のベストプラクティスに従ってスケジュールを修正します。

- 既存のスケジュールと設定を記録します。
- アップグレード期間中に複製が発生しないように、複製のスケジュールを将来の日付や別の日付に再設定します。
- すべての複製パートナーやサイトがスケジュールを取得できるように複製を強制します。

複製の頻度とコンテンツの変更

複製の停止と復元

つの Symantec Endpoint Protection Manager にログオンし、少なくとも 2 つのサイトで複製を停止する必要があります。

WARNING

複製の停止とは、複製パートナーシップを永久に削除することではありません。関係を削除してから管理サーバーを再インストールすると、管理サーバーは、増分の複製ではなく完全な複製を実行します。 [サイトの削除](#)

1. 管理サーバーサービスを停止します。
2. コンソールで、[管理] > [サーバー] の順に選択します。
3. [ローカルサイト] > [サーバー] を選択し、[複製パートナー] を展開して、管理サーバーを選択します。
4. 管理サーバーを右クリックし、[複製パートナーの削除] をクリックします。
5. [はい] をクリックします。
6. データを複製するすべてのサイトで同じ手順を繰り返します。
7. 複製を復元し、管理サーバーサービスを再起動します。

クライアントソフトウェアをアップグレードする方法の選択

複数の方法からクライアントをアップグレードできます。使う必要のある方法は、環境や目的によって異なります。たとえば、多数のクライアント、グループまたはコンピュータがあり、異なるバージョンのクライアントを実行している場合があります。

方法によっては最大 30 分かかります。したがって、ほとんどのユーザーがコンピュータにログオンしていないときにクライアントソフトウェアをアップグレードする必要があります。

Table 45: クライアントソフトウェアをアップグレードする方法

方法	使うとき	使わないとき
自動更新（比較的の小規模な環境の場合に推奨）	- クライアントの数が（5,000 以下など）比較的に少ない場合。 - ユーザーの作業を中断しない時間に実行されるようにアップグレードをスケジュール設定する必要がある場合。 - サードパーティアプリケーションではなくつの Symantec Endpoint Protection Manager を使ってクライアントインストールパッケージを配備する場合。 - Linux クライアントではなく Windows または Mac クライアントをアップグレードする必要がある場合。 - 単純なアップグレード方法を使う必要がある場合。 自動更新によるクライアントソフトウェアのアップグレード	- クライアントの数が比較的に多い場合。この方法は十分な拡張性を提供しません。 - グループの数が多い場合。ウィザードで各グループを個別にクリックすると時間が掛かるため。 - アップグレードスケジュールが複雑で、多くの詳細度を必要とする場合。 - Linux クライアントをアップグレードする必要がある場合。 クローンドライブイメージの一部として Symantec Endpoint Protection Linux クライアントを配備する方法
クライアントインストールパッケージをエクスポートします（大規模な環境に推奨）	- つの Symantec Endpoint Protection Manager を使わずに手動でクライアントインストールパッケージを配備する場合。 - つの Symantec Endpoint Protection Manager を使わずに既存のサードパーティ配備アプリケーションを使ってクライアントインストールパッケージを配備する場合。この方法を使うには、このインフラストラクチャがすでに適切に用意されている必要があります。 - Windows クライアント、Mac クライアント、Linux クライアントをアップグレードする必要がある場合。 クライアントインストールパッケージのエクスポート サードパーティツールを使った Windows クライアントソフトウェアのインストール	通常は つの Symantec Endpoint Protection Manager を使ってクライアントを更新する場合。
クライアント配備ウィザード	- クライアントの数が（250 未満など）比較的少ない場合。 - サードパーティアプリケーションではなくつの Symantec Endpoint Protection Manager を使ってクライアントを配備する場合。 - より単純なアップグレード方法を使う必要がある場合。 [新しいパッケージ配備] を使います。 リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール	大規模なネットワーク環境の場合。この方法は十分な拡張性を提供しないため。

方法	使うとき	使わないとき
[Broadcom ダウンロード管理] ページからクライアントインストールファイルをダウンロードします	- 特定の事例において少数のクライアントを一度にアップグレードする場合。次に例を示します。 - 古いバージョンのクライアントを伴う少数のコンピュータで問題が発生した場合、新しいバージョンによって問題が修正されます。 - アップグレードするクライアントの数が比較的に少なく、管理サーバーをアップグレードしない場合。 - Windows、Mac、Linux クライアントをアップグレードする必要がある場合。 - つの Symantec Endpoint Protection Manager は使わずに、直接またはサードパーティ 配備アプリケーションを使ってクライアントをコンピュータに配備する必要がある場合。 スタンドアロンの [All Clients] インストールファイルを [ダウンロード管理] ページからダウンロードします。 Symantec スタートガイド で、[オンプレミスセキュリティ製品] までスクロールします。 管理外 Windows クライアントのインストール	コンピュータのクライアントを既存の管理下クライアントでアップグレードする場合、クライアントの管理は維持されます。ただし、既存のクライアントを使わずに新しいコンピュータに配備する場合、この方法によって管理外クライアントのみがインストールされます。管理サーバーに接続するには、後でクライアントを管理下クライアントに変換する必要があります。 クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法 クライアントとサーバーの通信ファイル (Sylink.xml) の手動によるエクスポート

新リリースへのアップグレード

自動更新によるクライアントソフトウェアのアップグレード

概要

自動更新によって、グループ内にあるすべての Windows または Mac クライアントの Symantec Endpoint Protection クライアントソフトウェアを自動的にアップグレードできます。

自動更新では、Windows 標準クライアントは 1 つの Symantec Endpoint Protection Manager が作成する差分のアップグレードパッケージを受け取ります。このパッケージは完全インストールのパッケージよりも小さいです。Windows の埋め込みクライアントまたは VDI クライアントは、常に完全インストールパッケージを受信します。これらのクライアントは、インストーラキャッシュ内にインストーラのコピーを保持しません。Mac クライアントは、常に完全インストールパッケージを受信します。

自動更新のベストプラクティス

自動アップグレードを使う場合は次のベストプラクティスを実行します。

- 実働ネットワーク内の多数のクライアントのアップグレードを試みる前に自動更新の処理をテストします。テストネットワークがない場合は、実働ネットワーク内にテストグループを作成できます。この種類のテストを行う場合、テストグループに少数の重要ではないクライアントを追加し、自動アップグレードを使ってそれらをアップグレードします。
- ピーク時間帯の帯域幅を削減するには、クライアントグループに縮小サイズのクライアントが含まれる場合は特に、[\[クライアントをパッケージでアップグレード \]](#) ウィザードで自動更新を時間外にスケジュール設定します。広域ネットワークでは、リモート Web サーバーからアップグレードパッケージを受信するようにリモートクライアントを設定してください。
- 14.3 RU2 以降、LiveUpdate はクライアント インストール パッケージをダウンロードします。これにはクライアントのバージョンを変更することなくインストールできる重要な修正やセキュリティ修正が含まれます。たとえば、14.3 RU2 ビルド 4870 をインストールしていて 14.3 RU2 ビルド 5200 が利用可能になった場合、自動更新ウィザードを使用してビルド 5200 をインストールします。管理サーバをアップグレードする必要はなく、クライアントをアップグレードするだけです。各アップグレードの後、クライアントを再起動する必要があります。
- 14.3 RU2 以降、クライアントの言語サポートは、英語、フランス語、日本語、ポルトガル語 (ブラジル)、スペイン語を除くすべての言語で廃止されました。サポート対象外の言語は、[\[クライアントの言語がサポート外の場合は 14.3+ クライアントを英語にアップグレードする \]](#) オプションにチェックを付けると自動的に英語にアップグレー

ドします。このオプションのチェックを外している場合、サポート対象外の言語のクライアントは自動的にアップグレードされません。このオプションは英語の Symantec Endpoint Protection Manager でのみ利用できます。このオプションは Windows クライアントにのみ適用されます。Mac クライアントは、サポート対象外の言語からサポート対象言語に手動でアップグレードする必要があります。Linux クライアントは引き続き日本語にのみ翻訳されます。

- 自動更新は Symantec Endpoint Protection 14 付属の Mac クライアントで初めて導入されたため、バージョン 14 より前のバージョンから自動更新によってアップグレードすることはできません。
- つの Symantec Endpoint Protection Manager をアップグレードした後、自動更新を使用してクライアントをアップグレードする前に、コンソールで LiveUpdate を少なくとも 1 回実行します。

つの Symantec Endpoint Protection Manager に最新のコンテンツが含まれていることの確認

- 自動更新は、以下の条件が満たされたときのみ、アプリケーション強化機能 (14.2 以降) をクライアント コンピュータにインストールできます。
 - [クライアントをパッケージでアップグレード] を実行するときは、[更新時に既存のクライアント機能を維持する] を有効にする必要があります。この設定はデフォルトで有効になっています。
 - クライアントコンピュータは、Symantec Data Center Security エージェントをインストールできません。
 - ウイルスとスパイウェアの対策機能は現在インストールされ、アップグレードのために選択されています。
- クライアントのインストール後に、Windows クライアントのインストールの種類を、[標準クライアント]、[埋め込みまたは VDI]、[ダークネットワーク] の間で変更する場合は、最初に既存のクライアントソフトウェアをアンインストールし、これらの設定を再度行ってから新しいクライアントパッケージを再インストールする必要があります。自動更新を使ってこの設定を変更することはできません。

自動更新ウィザードの設定

1. 自動更新でクライアントソフトウェアをアップグレードするには、コンソールで [管理] > [インストールパッケージ] をクリックします。
2. [タスク] で、[クライアントをパッケージでアップグレード] をクリックします。
3. [クライアントのアップグレードウィザード] パネルで、[次へ] をクリックして、適切なクライアントインストールパッケージを選択してから、[次へ] をクリックします。
4. アップグレードするクライアントコンピュータを含むグループ (複数可) を選択して [次へ] をクリックします。
5. クライアントによるパッケージのダウンロード元を、次のオプションから選択します。
 - つの Symantec Endpoint Protection Manager サーバーからダウンロードするには、[管理サーバーからダウンロード] をクリックします。
 - 更新が必要なコンピュータのローカルにある Web サーバーからダウンロードするには、[次の URL からダウンロード (http または https)] をクリックします。クライアントインストールパッケージの URL を指定されたフィールドに入力します。
6. [アップグレードの設定] をクリックして、アップグレードオプションを指定します。
7. [全般] タブの [クライアントの設定] の下で、クライアントのオペレーティングシステムに応じて次のオプションから選択します。
 - Windows の場合
 - [このパッケージのバージョンの選択] で、ビルドを選択します (14.3 RU2 以降)。
 - ドロップダウン メニューから [更新時に既存のクライアント機能を維持する] と [インストールの設定] のオプションを選択します。[更新時に既存のクライアント機能を維持する] を選択解除した場合、アップグレード時に必要に応じて機能を追加または削除できます。
 - Mac の場合は、ドロップダウンメニューから [インストールの設定] のオプションを選択します。
 - Windows の場合、[コンテンツの選択] によって、インストールパッケージにコンテンツを含めることができます。コンテンツを含めると、パッケージは大きくなりますが、クライアントはインストール後すぐに最新のコンテンツを取得します。コンテンツを含めないと、パッケージは小さくなりますが、クライアントはインストール後にコンテンツを更新する必要があります。

アップグレードスケジュールを追加することもできます (省略可能)。スケジュールが設定されていない場合、自動更新処理はウィザードの完了後に開始されます。

8. [通知] タブで、ユーザー通知の設定をカスタマイズします。

アップグレードの間にクライアントコンピュータに表示されるメッセージをカスタマイズできます。ユーザーがアップグレードを延期することを許可することもできます。

9. [OK] をクリックして [次へ] をクリックします。

10. [クライアントのアップグレードウィザードの完了] パネルで、[完了] をクリックします。

11. クライアントソフトウェアのバージョン番号を確認するには、アップグレードが完了した後に、次のいずれかの方法でバージョンを調べて正常にアップグレードされたことを確認できます。

- コンソールで、[クライアント]、[クライアント] の順にクリックして、適切なグループを選択し、表示を [クライアントの状態] に変更します。
- Windows クライアントの Symantec Endpoint Protection クライアントインターフェースで、[ヘルプ]、[バージョン情報] の順にクリックします。
- Mac クライアントで Symantec Endpoint Protection クライアントインターフェースを開きます。メニューバーで [**Symantec Endpoint Protection**]、[**Symantec Endpoint Protection** のバージョン情報] をクリックします。

追加情報

アップグレードしたら、クライアントコンピュータを再起動する必要があります。デフォルトでは、クライアントはインストール後に再起動します。グループの全般の設定で再起動オプションを設定してグループ内のクライアントが自動更新後にどのように再起動するかを制御できます。また、管理サーバーから再起動コマンドを実行して、いつでもクライアントを再起動できます。

[つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動](#)

[他のグループへのアップグレード設定の適用](#)

他のグループへの自動更新設定の適用

既存の自動更新クライアントインストールパッケージのアップグレード設定を 1 つのグループから別のグループにコピーできます。アップグレード設定をコピーする場合は、各グループに対して個別のパッケージ設定を作成する必要はありません。

このオプションでは、次のクライアントインストールパッケージ設定がコピーされます。

- クライアント機能セット
- [更新時に既存のクライアント機能を維持する] が有効であるか無効であるか
- クライアントインストール設定
- コンテンツの選択
- ダウンロード元
- アップグレードスケジュール
- [通知] タブの設定とメッセージテキスト

自動更新の実行中、Windows 設定は Windows クライアントに適用され、Mac 設定は Mac クライアントに適用されます。これらの設定は、グループの新たに加わったクライアントにも適用されます。

対象グループにすでに割り当てられているパッケージに、コピーした設定を適用すると、その設定により対象グループの既存の設定が上書きされます。対象グループに割り当て済みのパッケージがない場合、このオプションはコピーした設定でクライアントインストールパッケージを追加します。

アップグレード設定を他のグループに適用するには

1. コンソールで次のいずれかの操作をします。

- [クライアント] > [インストールパッケージ] の順にクリックし、グループを選択して、[タスク] で [現在の配備設定を他のグループに適用する] をクリックします。
- [クライアント] をクリックし、グループを右クリックして、[配備設定のコピー] をクリックします。

2. [配備設定のコピー] ダイアログボックスで、新しいグループをクリックし、[OK] をクリックして [はい] をクリックします。

自動更新によるクライアントソフトウェアのアップグレード

Symantec Agent for Linux のアップグレード

(14.3 RU1 以降の場合)

Symantec Agent for Linux は、Linux 用の古い Symantec Endpoint Protection クライアントを検出してアンインストールし、新規インストールを実行します。古い設定は保持されません。

Symantec Agent for Linux にアップグレードするには

1. つの Symantec Endpoint Protection Manager で、インストールパッケージを作成してダウンロードします。

[クライアントインストールパッケージのエクスポート](#)

2. Linux デバイスに LinuxInstaller パッケージを移動します。

3. LinuxInstaller ファイルを実行可能にします。

```
chmod u+x LinuxInstaller
```

4. 新しいエージェントのインストールを開始します。

```
./LinuxInstaller
```

root としてコマンドを実行します。

5. インストールを検証するには、`/usr/lib/symantec` に移動し、`./status.sh` スクリプトを実行して、モジュールがロード済みでデーモンが実行されていることを確認します。

```
./status.sh
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent running
sisamdagent running
sisidsagent running
sisipsagent running
Module status:
sisevt loaded
sisap loaded
```

グループ更新プロバイダの更新

グループ更新プロバイダであるクライアントを更新するには、次の手順を使います。

GUP のクライアントをアップグレードするには

1. つの Symantec Endpoint Protection Manager サーバーを新しいバージョンのソフトウェアにアップグレードします。
2. GUP であるクライアントを新しいバージョンのクライアントソフトウェアにアップグレードします。
3. 他のクライアントを新しいバージョンのクライアントソフトウェアに更新します。

[クライアントにコンテンツを配布するための GUP の使用](#)

[新リリースへのアップグレード](#)

Symantec Endpoint Protection のアップグレードに関するリソース

Table 46: アップグレードのリソース

項目	リソース
クライアントインストールパッケージの設定と機能	さまざまな設定と保護機能を使ってクライアントインストールパッケージを設定できます。 プラットフォームに基づく Symantec Endpoint Protection の機能 (12.1.x から 14.x) Windows クライアントのインストール設定について クライアントにインストールするセキュリティ機能の選択
機能とポリシーの説明	Symantec Endpoint Protection 技術でコンピュータが保護される仕組み セキュリティポリシーの種類
機能の依存関係	Windows クライアント用の Symantec Endpoint Protection 機能の依存関係 (12.1.x から 14.x)
製品ライセンスの管理	Symantec Endpoint Protection は、サイトでのコンピュータの保護に必要なクライアント数に応じて、ライセンスが交付されます。 Symantec Endpoint Protection 製品ライセンスの必要条件
追加リソース	次の記事を参照してください。 • Symantec Endpoint Protection の最新バージョンにアップグレードするためのベストプラクティス • シマンテックソフトウェアの最新バージョンをダウンロードする • Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件

[新リリースへのアップグレード](#)

Symantec Endpoint Protection のライセンス交付

Symantec Endpoint Protection (SEP) でセキュリティコンテンツの更新、製品の更新とバージョン、およびテクニカルサポートへのアクセスを受け取るには、有償ライセンスが必要です。この Symantec Endpoint Protection Manager をインストールした後、配備したクライアントすべてを扱うのに十分なライセンス枠の購入までに 60 日間の猶予が与えられます。

Symantec Endpoint Protection のメンテナンス権限の概要

Table 47: Symantec Endpoint Protection のライセンスを登録する方法

タスク	説明
ステップ 1: ライセンスの購入	新しいライセンスを購入するには、正規代理店にお問い合わせください。 「Symantec スタートガイド」を参照し、オンプレミスセキュリティ製品までスクロールします。まだ持っていない場合は、Broadcom サポートポータルアカウントを作成します。 以下の場合にライセンスを購入する必要があります。 • Symantec Endpoint Protection を購入する必要がある場合。 • 試用ライセンスが期限切れになった場合。 • 有償ライセンスが期限切れになった場合。 • ライセンスで許可されているよりも多くのクライアントを配備した場合 (過剰配備)。 サイトでのエンドポイントの保護に必要なクライアント数に応じて、ライセンスを交付します。 必要な Symantec Endpoint Protection ライセンス数
ステップ 2: 購入したライセンスのアクティブ化	ライセンスを購入すると、シマンテックライセンスファイル (.slf) またはライセンスのシリアル番号が .zip ファイルとして添付された電子メールを受信します。.zip ファイルから .slf ファイルを抽出する必要があります。 インストールをアクティブ化するには、シリアル番号が必要です。 • Symantec Endpoint Protection Manager には、デフォルトアカウント admin などのシステム管理者アカウントを使ってログオンする必要があります。 • SEP 製品ライセンスをインポートおよびアクティブ化するには、[管理者] > [ライセンス] ページに移動します。 Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート

以下のタスクを実行して、ライセンスを管理できます。

Table 48: ライセンスタスク

タスク	説明
シリアル番号の取得	シマンテックからの既存のライセンスがあり、シリアル番号を取得する必要がある場合は、「 シマンテックから Broadcom 社への移行ガイド - My Entitlements 」を参照してください。
ライセンスの更新	正規代理店へのお問い合わせ 「シマンテック更新 FAQ」を参照してください。
いつ期限切れになるかということと、過剰配備されているかどうかを確認します。	コンソールにインポートしたライセンスそれぞれの状態を調べて、ライセンスを更新する必要やライセンスを追加購入する必要があるかどうかを確認します。 既存のライセンスを製品アップグレードに適用できます。 この Symantec Endpoint Protection Manager のライセンス状態の調査
ライセンスファイルのバックアップ	ライセンスファイルのバックアップを作成すると、データベースやコンピュータのハードディスクが破損した場合に備えてライセンスファイルを保持できます。 ライセンスファイルのバックアップおよび回復

タスク	説明
ライセンスファイルの回復	ライセンスファイルを手違いで削除した場合は、そのファイルを回復できます。 ライセンスファイルのバックアップおよび回復
ライセンスが期限切れになったときに通知を送信する	デフォルトでは、Symantec Endpoint Protection は、期限切れのライセンスやその他のライセンスの問題について、事前に設定した通知を管理者に送信します。 通知の種類および通知が送信される場合
製品ライセンスの必要条件の確認	保護するコンピュータのライセンスの必要条件のについて確認します。ライセンスにより、Symantec Endpoint Protection クライアントを指定された台数のコンピュータにインストールできます。 製品ライセンスに含まれるものは？ Symantec Endpoint Protection 製品ライセンス用語 複数年ライセンスについて

つの Symantec Endpoint Protection Manager のライセンス状態の調査

管理サーバーが、試用ライセンスまたは有償ライセンスのどちらを使っているかを調べることができます。コンソールにインポートした各有償ライセンスの次のライセンス情報を取得することもできます。

- ライセンスのシリアル番号、ライセンス枠の合計数、合計の枠の件数、有効期限日
- 有効なライセンス枠数
- 配備済みのライセンス枠数
- 期限切れのライセンス枠数
- 過剰配備済みのクライアント数

試用ライセンスの状態は有効期限日と関連する限られた情報のみを示します。

1. 有償ライセンスと体験版ライセンスのどちらを持っているかを調べるには、コンソールで以下のいずれかのタスクを行います。
 - [管理]、[ライセンス] の順にクリックします。
 - [ホーム]、[ライセンスの詳細] の順にクリックします。
2. ライセンスの有効期限日を調べるには、コンソールで [管理] > [ライセンス] をクリックします。

[Symantec Endpoint Protection のライセンス交付](#)

[Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート](#)

ライセンスファイルのバックアップおよび回復 (.sif)

データベースまたはコンソールコンピュータのハードディスクが破損した場合に備えて、ライセンスファイルをバックアップする必要があります。

ライセンスファイルを受け取った後、つの Symantec Endpoint Protection Manager コンソールからアクセスできるコンピュータに保存します。多くのユーザーは、つの Symantec Endpoint Protection Manager をホストするコンピュータにライセンスを保存します。多くのユーザーはまた、ライセンスを安全に保管するために、ライセンスのコピーを別のコンピュータまたは取りはずし可能なストレージメディアに保存します。

ライセンスファイルをバックアップするには

1. ライセンスファイルを保存したディレクトリから、選択した別のコンピュータに .sif ライセンスファイルをコピーします。

ライセンスファイルを回復するには

- 次のいずれかのタスクを行います。
 - a. つの Symantec Endpoint Protection Manager コンソールの [管理] ページで、[ライセンス] をクリックし、[タスク] の下で [削除したライセンスを回復する] をクリックします。[ライセンス回復] パネルで、回復する削除済みライセンスの横にあるボックスにチェックマークを付けて、[提出] をクリックします。
 - b. 以下のデフォルトの場所からライセンスファイルを取得します。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\lnetpub\license ライセンスのアクティブ化ウィザードを使用してライセンスファイルをインポートする場合、Symantec Endpoint Protection Manager は、このフォルダにファイルのコピーを配置します。
 - c. [Symantec Endpoint Security](#) Web サイトに移動し、[My Entitlements] をクリックします。詳しくは、「[Symantec から Broadcom 社への移行ガイド - My Entitlements](#)」を参照してください。

Symantec Endpoint Protection のライセンス交付

データベースから使われなくなったクライアントをパージして使用可能なライセンスを増やす

つの Symantec Endpoint Protection Manager では、使われなくなったクライアントの存在により過剰配備のライセンスの状態が誤って表示されることがあります。これらは、保護された環境でつの Symantec Endpoint Protection Manager と通信しなくなったクライアントのデータベースエントリです。オペレーティングシステムのアップグレード、コンピュータの使用停止、ハードウェア構成の変更といったさまざまな理由により、クライアントが使われなくなることがあります。

ライセンスレポートで、配備していることを把握しているシートより多くのシートにライセンスが交付されていることがわかった場合は、使われなくなったクライアントのデータベースをパージしてください。使われなくなったクライアントは製品のライセンスを消費するので、使われなくなったクライアントが発生したときにはすぐにパージすることが重要です。デフォルトでは、パージは 30 日ごとに行われます。使われなくなったクライアントがすばやくパージされるように、パージサイクルの間隔を短くできます。パージサイクルが完了した後の長期的なニーズに合うように、必要に応じて間隔を設定し直します。

非永続的な仮想デスクトップインフラストラクチャ (VDI) では、非永続的なクライアントのパージ用に、個別の期間を設定できます。この設定は、設定した期間に接続を行わなかったオフラインのクライアントをパージします。非永続的なオフラインクライアントは、ライセンス数には影響を与えません。

1. コンソールの [管理] ページで、[ドメイン] をクリックし、ドメインを右クリックし、[ドメインプロパティの編集] をクリックします。
2. [全般] タブで、[一定期間にわたって接続しなかったクライアントを削除する] の設定をデフォルトの **30** から **1** に変更します。

ライセンス管理の目的で非永続的なクライアントをパージするオプションを設定する必要はありません。オフラインの非永続的なクライアントは、ライセンスの合計に加算されません。

3. [OK] をクリックします。
4. 24 時間待った後、設定を 30 日または要件に合う他の期間に戻します。

ライセンスを開放するための使われなくなった非永続的 VDI クライアントのパージ

Symantec Endpoint Protection のライセンス交付

Symantec Endpoint Protection ライセンスに含まれるものは?

Symantec Endpoint Protection ライセンス数は、次のルールに従ってエンフォースされます。

Table 49: ライセンスのエンフォースメントルール

適用される箇所	ルール
ライセンスの期間	ライセンス期間は、アクティブ化した日時からライセンス期間の最終日の午前 0 時までです。複数のサイトがある場合には、ライセンスは最も西の つの Symantec Endpoint Protection Manager データベースの有効期限の日時に期限切れになります。
Symantec Endpoint Protection コンポーネント	Symantec Endpoint Protection ライセンスは Symantec Endpoint Protection クライアントに適用されます。たとえば、コンピュータが 50 台あるネットワークでは、ライセンスは最低 50 の枠を提供する必要があります。つの Symantec Endpoint Protection Manager のインスタンスはライセンスを必要としません。 つの Symantec Endpoint Protection Manager では、管理サーバーにアクセスするためにクライアントでライセンスを所有する必要はありません。管理サーバーに接続するライセンスのないクライアントにライセンスが付与されます。各クライアントコンピュータのために十分なライセンス枠を購入する必要があります。
サイトとドメイン	Symantec Endpoint Protection 製品ライセンスは、インストールを構成する複製されたサイトまたはドメインの数に関係なく、インストール全体に適用されます。たとえば、100 の枠のライセンスは、それぞれのサイトに 50 の枠がある 2 つのサイトのインストールに対応します。 複製を実装していない場合は、複数の Symantec Endpoint Protection 管理サーバーに同じ .slf ファイルを配備できます。管理サーバーに対してレポートするクライアントの数は、ライセンス枠の総数を超えないようにする必要があります。
プラットフォーム	ライセンスの枠は、プラットフォームが Windows、Mac、Linux のいずれであるかにかかわらず、プラットフォームで実行しているクライアントに適用されます。
製品とバージョン	ライセンス枠は製品バージョンで均等に適用されます。

Microsoft SQL Server などのサードパーティのサーバーソフトウェアにアクセスするクライアントへのライセンス付与について詳しくは、ソフトウェアベンダーに問い合わせてください。

[Symantec Endpoint Protection のライセンス交付](#)

[ライセンスを開放するための使われなくなった非永続的 VDI クライアントのページ](#)

複数年ライセンスについて

複数年ライセンスを購入すると、ライセンスが有効な年数と等しい数の一連のライセンスファイルを受け取ります。たとえば、3 年のライセンスは、3 つの異なるライセンスファイルで構成されます。複数年ライセンスをアクティブ化するときは、同じアクティブ化セッションの間にすべてのライセンスファイルをインポートします。つの Symantec Endpoint Protection Manager によって異なるライセンスファイルがマージされ、購入期間のあいだ有効な単一のアクティブ化済みライセンスが作成されます。

推奨はできませんが、全期間より少ない数のライセンスファイルをアクティブ化することもできます。その場合、つの Symantec Endpoint Protection Manager はファイルをマージし、最後に期限が切れるライセンスファイルの期間を適用します。たとえば、3 年間のライセンスを最初の 2 つのファイルだけでアクティブ化すると、期間は 2 年だけになります。3 つ目のファイルを後にアクティブ化するとき、つの Symantec Endpoint Protection Manager はライセンスの完全期間を 3 年として正確に報告します。いずれの場合にも、枠の数は購入した枠の数と一致します。

つの Symantec Endpoint Protection Manager がファイルをマージするときは、最も短い期間のファイルが削除され、最も長い期間のファイルが内部のライセンス保持機能用に保持されます。つの Symantec Endpoint Protection Manager がライセンスを誤って削除したと考えられる場合は、削除されたライセンスを回復し、再度アクティブ化します。

アクティブなライセンスと関連付けられた短い期間のライセンスシリアル番号を確認できます。[管理] ページで [ライセンス] をクリックし、アクティブ化済みライセンスをクリックします。関連付けられたライセンスが [関連付けられたライセンス] 列に表示されます。

[Symantec Endpoint Protection のライセンス交付](#)

Symantec Endpoint Protection 製品ライセンス用語

配備された各クライアントに応じたライセンスを購入する必要があります。1つのライセンスは、プラットフォームとバージョンに関係なく、すべてのクライアントに対応します。

シマンテック製品のライセンスでは、次の用語が使われます。

シリアル番号	ライセンスには、ライセンスを一意に識別し、ライセンスを会社に関連付けるシリアル番号が含まれます。このシリアル番号を使って、Symantec Endpoint Protection ライセンスをアクティブ化できます。 Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート
配備済み	配備済みとは、Symantec Endpoint Protection クライアントソフトウェアの保護を受けているエンドポイントコンピュータを指します。たとえば、「50 の配備済みライセンス枠があります」とは、50 のエンドポイントでクライアントソフトウェアがインストールされていることを意味します。
アクティブ化	すべてのプログラム機能に制限なくアクセスできるようにするために、Symantec Endpoint Protection 製品ライセンスをアクティブ化します。アクティブ化プロセスを実行するには、ライセンスアクティブ化ウィザードを使います。 Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート
枠	シート枠とは、Symantec Endpoint Protection クライアントソフトウェアが保護する単一のエンドポイントコンピュータです。ライセンスは、特定数の枠に対して購入され、有効にされます。「有効な枠」とは、すべてのアクティブなライセンスで指定されている枠の合計数を示します。
試用ライセンス	試用ライセンスとは、無料の評価期間内で動作する Symantec Endpoint Protection の全機能インストール版を指します。評価期間以降も Symantec Endpoint Protection を使い続ける場合は、インストールに応じたライセンスを購入し、アクティブ化する必要があります。体験版からライセンス済みインストールに変換するときに、ソフトウェアをアンインストールする必要はありません。 体験版ライセンスは、セールスアカウント担当者から入手する必要があります。 評価期間は、つの Symantec Endpoint Protection Manager の初回インストールから 60 日です。
過剰配備	配備されたクライアント数がライセンス済みの枠の数を超えた場合、ライセンスは過剰配備されています。

ライセンスの必要条件を理解することは、Symantec Endpoint Protection インストール計画に必要であり、インストール後の製品ライセンスの管理に必要です。

[Symantec Endpoint Protection のライセンス交付](#)

[Symantec Endpoint Protection の製品ライセンスのアクティブ化またはインポート](#)

管理外 Windows クライアントのライセンス交付

管理外クライアントはライセンスファイルの手動インストールを必要としません。ただし、管理外 Windows クライアントからの評価データの提出を有効にするには、管理外クライアントに有償ライセンスをインストールする必要があります。管理外の Mac クライアントと Linux クライアントは評価データを提出しません。

1. 現在のシマンテックライセンスファイル (.slf) のコピーを見つけるか、または作成します。

つの Symantec Endpoint Protection Manager でライセンスをアクティブ化するために使ったファイルと同じものを使用します。

2. クライアントコンピュータで、コピーしたライセンスファイルを Symantec Endpoint Protection クライアント受信ボックス (デフォルトの場所) に置きます。

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox\

デフォルトでは、受信ボックスが表示されるフォルダは非表示です。そのため、フォルダオプションを利用し、非表示のファイルとフォルダを表示します。

ライセンスファイルが無効の場合、またはライセンスのインストールが失敗した場合、Invalid という名前の新しいフォルダにそのライセンスが表示されます。ファイルが有効の場合、処理後に受信ボックスから自動的に削除されます。

3. ライセンスを正しく適用したことを確認するには、inbox フォルダにファイルが表示されないことを確認します。
4. .slf ファイルが次のフォルダ (デフォルトの場所) にあることを確認します。

C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Config

サードパーティ製の配備パッケージの一部として .slf ファイルを含めることもできます。

クライアントとサーバー間の接続の管理

クライアントをインストールした後、管理サーバーはクライアントコンピュータに自動的に接続します。

Table 50: 管理サーバーとクライアント間の接続を管理するタスク

処理	説明
クライアントが管理サーバーに接続されているかどうかを確認する	クライアントと管理コンソールでクライアントの状態アイコンを確認できます。状態アイコンはクライアントとサーバーが通信しているかどうかを示します。 クライアントが管理サーバーに接続され、保護されているかどうかの確認 コンピュータにクライアントソフトウェアがインストールされている可能性があります、正しい通信ファイルを備えていません。 クライアントコンピュータと管理サーバーの通信方法 クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法
クライアントがポリシーの更新を取得することのチェック	クライアントと管理コンソールでポリシーのシリアル番号を調べることで、クライアントコンピュータが最新のポリシーの更新を取得していることを確認します。クライアントがサーバーと通信できており、定期的なポリシー更新を受信している場合、ポリシーのシリアル番号は一致する必要があります。 手動でポリシー更新を実行し、次にポリシーのシリアル番号をチェックして比べることができます。 ポリシーのシリアル番号を使ったクライアントとサーバーの通信の確認 クライアントポリシーの更新
クライアントにポリシーとコンテンツをダウンロードする方法の変更	ポリシーをクライアントにプッシュする管理サーバーまたはポリシーを管理サーバーからプルするクライアントを設定できます。 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新
デフォルトの管理サーバーリストを使うかどうかの決定	フェールオーバーと負荷分散用に管理サーバーの代替リストを使うことができます。管理サーバーリストはクライアントが接続できる複数の管理サーバーのリストを提供します。 負荷分散のための管理サーバーリストの設定
場所に対する通信の設定	場所およびグループに対する個別の通信を設定できます。 場所に対する通信の設定
管理サーバーの接続に関する問題のトラブルシューティング	管理サーバーとクライアントが接続していない場合、接続の問題をトラブルシューティングできます。 この Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング

詳しくは、次の記事を参照してください: [Symantec Endpoint Protection で使用される通信ポートについて](#)

管理サーバーおよびサーバークライアント接続の設定

このセクションを使用して、以下を行います。

- 管理サーバーとクライアント間の接続を設定する。
- クライアントとサーバーのパフォーマンスを向上させる。
- サーバー証明書を更新してクライアント/サーバー接続を維持する。
- Symantec Endpoint Protection Manager とサードパーティサーバーを統合する。

つの Symantec Endpoint Protection Manager とクライアント間の HTTPS 通信の設定

つの Symantec Endpoint Protection Manager は Apache Web サーバーを使ってクライアントと通信し、レポートサービスを提供します。Symantec Endpoint Protection 14 の新規インストールでは、HTTPS 通信がデフォルトで有効になります。HTTPS は証明書を使用して署名し、データを暗号化するセキュアなプロトコルであり、通信の機密性と整合性を実現します。

バージョン 12.1 の Web サーバーは、デフォルトで、すべての通信に非暗号化プロトコルの HTTP を使用します。バージョン 12.1 から Symantec Endpoint Protection 14 にアップグレードする場合、つの Symantec Endpoint Protection Manager はアップグレード中に設定を保持します。バージョン 12.1 で HTTPS を有効にしていなかった場合は、アップグレード後に HTTPS 通信を使用するように つの Symantec Endpoint Protection Manager Apache Web サーバーを構成できます。

Symantec Endpoint Protection 12.1 を使用する場合は、同じ手順に従って、HTTPS 接続を使用するように つの Symantec Endpoint Protection Manager Apache Web サーバーを構成できます。

Table 51: クライアントへの HTTPS 通信の設定

手順	説明
手順 1: デフォルトの HTTPS ポートが利用可能であることを確認する	デフォルトでは、HTTPS トラフィックは 443 ポートを使用します。ネットワークによっては、ポート 443 が別のアプリケーションまたはサービスにすでにバインドされている場合があります。HTTPS 通信を有効にする前に、デフォルトポートが利用可能かどうかを確認する必要があります。 ポートの可用性の検証
手順 2: 必要に応じてデフォルトの HTTPS ポートを変更する	ポート 443 が使えない場合は、大きいポート番号の範囲 (49152 ~ 65535) から使われていないポートを選択します。新しいポートを使うように管理サーバーを設定します。新しいポートを反映させるために管理サーバーリストを更新します。 クライアントの通信のための Apache の HTTPS ポートの変更 負荷分散のための管理サーバーリストの設定
手順 3: クライアントへの HTTPS 通信を有効にする	Apache の httpd.conf ファイルを編集して、クライアントへの HTTPS 通信を許可します。接続をテストし、次に HTTPS 通信にクライアントを切り替えます。 HTTPS クライアント/サーバー通信の有効化

クライアントとサーバー間の接続の管理

ポートの可用性の検証

つの Symantec Endpoint Protection Manager の一部の設定では、他のアプリケーションまたはサービスとの競合を防ぐために、ポートのデフォルトの割り当てを変更する必要があります。新しいポートを割り当てる前に、別のアプリケーションまたはサービスがその新しいポートを使わないことを確認する必要があります。

コマンドプロンプトを開き、次のコマンドを大文字と小文字を区別して入力します。

```
netstat -an | find ":<ポート>" | find "LISTENING"
```

ここで、ポート> は、可用性を確認するポートの番号です。たとえば、ポート 443 が使用可能であるかどうかを確認するには、次のように入力します。

```
netstat -an | find " :443" | find "LISTENING"
```

この netstat コマンドで結果が返された場合は、未使用のポートを見つける必要があります。同じコマンドを使用し、<ポート> には任意のポート番号を指定します。このコマンドで結果が返されなかった場合は、そのポートを使用できません。

クライアントの通信のための Apache の HTTPS ポートの変更

つの Symantec Endpoint Protection Manager とクライアント間の HTTPS 通信の設定

クライアント/サーバー間通信の保護

クライアントの通信のための Apache の HTTPS ポートの変更

Apache のデフォルトの HTTPS ポートは 443 です。つの Symantec Endpoint Protection Manager が別の HTTPS Web サイトをホストしている場合、ポート 443 がそれらの Web サイトのいずれかにすでに割り当てられている可能性があります。新しいインストールには別のポートを使用して、デフォルトのポート 443 をすでに使用しているアプリケーションとの競合を最小限に抑える必要があります。クライアントがデフォルトポートを使用してつの Symantec Endpoint Protection Manager と通信するようにする場合は、まずそのポートが使用可能であることを確認する必要があります。

NOTE

クライアントソフトウェアの配備後に HTTPS ポート番号をカスタマイズすると、クライアントは管理サーバーと通信できなくなります。これらのクライアントは、新しい接続情報が含まれるサーバーからの次のクライアント更新後に、通信を再確立します。また、通信の更新パッケージを使用することもできます。

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

この手順を完了した後で、HTTPS クライアント/サーバー通信を有効にします。

クライアントの通信のための Apache の HTTPS ポートを変更するには

1. テキストエディタで、次のファイルを開きます。

```
SEPM_Install\apache\conf\ssl\sslForClients.conf
```

SEPM_Installデフォルトでは、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

NOTE

ファイルの置かれているフォルダ SEPM_Install\apache\conf\ssl\ は読み取り専用である場合があります。その場合は、フォルダプロパティの [読み取り専用] のチェックマークをはずす必要があります。

2. 次の行を編集し、デフォルトの 443 を新しいポート番号に変更します。

```
Listen 443
```

```
<VirtualHost_default_: 443>
```

3. ファイルを保存し、テキストエディタを閉じます。

ポートの可用性の検証

HTTPS クライアント/サーバー通信の有効化

つの Symantec Endpoint Protection Manager とクライアント間の HTTPS 通信の設定

クライアント/サーバー間通信の保護

HTTPS クライアント/サーバー通信の有効化

httpd.conf ファイルを編集して、HTTPS プロトコルを使用する つの Symantec Endpoint Protection Manager サーバーとクライアント間のセキュア通信を有効にします。

セキュア通信に代替ポートを使う必要がある場合、つの Symantec Endpoint Protection Manager のポート割り当てを最初に変更する必要があります。

Symantec Endpoint Protection 14.x の新規インストールでは、HTTPS クライアント/サーバー通信がデフォルトで有効になります。バージョン 12.1 からバージョン 14.x にアップグレードする場合は、クライアント/サーバー通信の設定が引き継がれます。バージョン 12.1.x の場合、HTTPS クライアント/サーバー通信がデフォルトでは有効になりません。

1. Apache Web サーバーの HTTPS を有効にするには、テキストエディタで以下のファイルを開きます。

```
SEPM_Install\apache\conf\httpd.conf
```

SEPM_Installデフォルトでは、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

2. 次のテキスト文字列を見つけて、ハッシュマーク (#) を削除します。

```
#Include conf/ssl/sslForClients.conf
```

3. ファイルを保存して閉じます。

4. つの **Symantec Endpoint Protection Manager Webserver** サービスを再起動します。

つの Symantec Endpoint Protection Manager Webserver サービスを停止し、再起動すると、つの Symantec Endpoint Protection Manager サービスも停止および再起動されます。

[Apache Web サーバーの停止と開始](#)

5. HTTPS が正しく動作することを確認するには、Web ブラウザに以下の URL を入力します。

```
https://<SEPMServer>:<###>/secars/secars.dll?hello,secars
```

ここで、SEPMServerは つの Symantec Endpoint Protection Manager のサーバーホスト名であり、ポートは HTTPS ポート番号です。デフォルトでは、HTTPS トラフィックは 443 ポートを使用します。

6. ブラウザに「OK」という文字が表示されれば、HTTPS 接続は成功です。

ページエラーが表示される場合、前の手順を繰り返し、すべての文字列を正しく書式設定したことを確認します。また、URL を正しく入力したことを確認します。

証明局の署名入り証明書と秘密キーのペアを使用して管理サーバーを更新しなかった場合、Web ブラウザには証明書が信頼されないという警告が表示されます。管理サーバーの証明書の件名とは異なる URL から Web サイトにアクセスした場合にも、同じ警告が表示されます。

7. クライアントがつの Symantec Endpoint Protection Manager との通信に HTTPS を使用するように切り替えるには、つの Symantec Endpoint Protection Manager コンソールの [ポリシー] タブで、[ポリシーコンポーネント] > [管理サーバーリスト] をクリックします。

8. クライアントのグループと場所で使用される管理サーバーリストをダブルクリックします。デフォルトの管理サーバーリストだけがある場合、それを複製し、新しいリストをダブルクリックして編集します。

[タスク] で [管理サーバーリストの追加] をクリックすることもできます。[管理サーバー] で、[追加] > [新しいサーバー] を選択してサーバー情報を追加します。[新しいサーバー] エントリを、サーバー IP アドレス用に 1 つ、サーバー名用に 1 つ追加できます。

[\[ポリシー \] ページでのポリシーのコピーと貼り付け](#)

9. [HTTPS プロトコルを使う] をクリックします。

以前に証明機関の署名入り証明書と秘密キーのペアで管理サーバーを更新している場合、[HTTPS プロトコルを使うときに証明書を確認する] のみをクリックします。

[サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス](#)

NOTE

カスタム HTTPS ポート番号を `sslForClients.conf` ファイルで使用した場合は、管理サーバーのリストからサーバーを編集します。[HTTPS ポートをカスタマイズする] をクリックし、前に使用した番号と一致するようにポートを編集します。

[OK] をクリックしてカスタムポートを保存します。

10. [OK] をクリックして管理サーバーリストを保存します。

11. デフォルトの管理サーバーリストの複製を編集した場合は、それを右クリックし、[割り当て] をクリックし、それをすべてのグループと場所に割り当てます。

[グループと場所への管理サーバーリストの割り当て](#)

12. Symantec Endpoint Protection クライアントで、[ヘルプ] > [トラブルシューティング] > [サーバー接続の状態] を選択します。

13. [前回試みた接続] と [前回正常に完了した接続] で、HTTPS 通信のサーバーアドレスとポート番号の両方の表示を確認します。

14. 必要に応じて、[今すぐ接続] をクリックして強制的に即時接続します。

[クライアントの通信のための Apache の HTTPS ポートの変更](#)

[つの Symantec Endpoint Protection Manager とクライアント間の HTTPS 通信の設定](#)

[クライアント/サーバー間通信の保護](#)

クライアントとサーバーのパフォーマンスの向上

つの Symantec Endpoint Protection Manager は、高レベルのセキュリティを維持しながらクライアントとサーバーのパフォーマンスを向上させることができるさまざまな機能を備えています。

Table 52: サーバー上とクライアント上でパフォーマンスを向上させるタスク

タスク	説明
クライアントサーバー通信設定の変更	プッシュモードではなくプルモードを使って、管理サーバーがポリシーとコンテンツ更新をクライアントコンピュータにダウンロードする頻度を制御します。プルモードでは、管理サーバーは多くのクライアントをサポートできます。 クライアントとサーバーが通信する頻度が低下するようにハートビート間隔を延長します。サーバーあたりのクライアント数が 100 よりも少ない場合、ハートビート間隔を 15 分から 30 分の間に延長します。クライアント数が 100 から 1,000 の場合は、ハートビート間隔を 30 分から 60 分の間に延長します。ネットワークの規模が大きいほど、長いハートビート間隔が必要です。ダウンロードのランダム化の間隔は、ハートビート間隔の 1 倍から 3 倍の間に延ばします。 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新 ハートビート間隔の設定について詳しくは、ホワイトペーパー『Symantec Endpoint のサイジングと拡張性に関するベストプラクティスホワイトペーパー』を参照してください。
コンテンツ更新の数のランダム化と削減	コンテンツ更新は、コンテンツの種類と可用性に応じてサイズと頻度が変わります。次の方法を使って、コンテンツ更新一式のダウンロードとインポートの影響を軽減できます。 - 複数の管理サーバーにクライアント負荷を分散する。 負荷分散のための管理サーバーリストの設定 - 代替方法（グループ更新プロバイダ、サードパーティの配布ツールなど）を使ってコンテンツを配布する。 グループ更新プロバイダを使うと、サーバーからコンテンツをダウンロードするクライアントに処理能力をオフロードすることによって帯域幅を節約できます。 クライアントにコンテンツを配布するための GUP の使用 サードパーティの配布ツールを使ったクライアントコンピュータの更新 - LiveUpdate がクライアントコンピュータにコンテンツをダウンロードする時期をランダム化する。 LiveUpdate サーバーからのコンテンツダウンロードのランダム化 デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化 - ユーザーがクライアントコンピュータをアクティブに使っていないときにコンテンツ更新をダウンロードする。 Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行する設定
スキャンの調整によるコンピュータパフォーマンスの改善	一部のスキャン設定を変更して、保護レベルを低下させずにコンピュータのパフォーマンスを改善できます。 たとえば、信頼できるファイルを無視したり、コンピュータがアイドル状態のときに実行するようにスキャンを設定できます。 スキャンの調整によるクライアントコンピュータパフォーマンスの改善 Windows クライアントの Auto-Protect のカスタマイズ スキャンと監視の拡張設定

タスク	説明
データベースクライアントログの量の削減	ストレージの必要条件を最適化し、ログに記録されたデータの保持を制御する会社のポリシーに準拠するように、ログ記録オプションを設定できます。 データベースは、絶えずエントリのフローを受け取り、そのログファイルに記録します。データベースに格納されているデータが、利用可能なディスク領域を使い果たさないように、データを管理する必要があります。データが多すぎると、データベースを実行しているコンピュータがクラッシュする原因となります。 次のタスクを実行することによって、ログデータの量を減らすことができます。 - サーバーにクライアントログの一部のみをアップロードし、クライアントログをアップロードする頻度を変更する。 クライアントログサイズと管理サーバーにアップロードするログの指定 - クライアントコンピュータがデータベースに保持できるログエントリの数とそれらを保持する期間を指定する。 ログサイズとデータベース内のログエントリの保存期間の指定 - サーバーに転送されるデータ量が減るように、重要度の低いリスクイベントとシステムイベントをフィルタで除外する。 Windows コンピュータのログ処理と通知設定の修正 - 各管理サーバーが管理するクライアントの数を減らす。 負荷分散のための管理サーバーリストの設定 つの Symantec Endpoint Protection Manager のインストール - クライアントログをサーバーにアップロードする頻度をコントロールするハートビートの頻度を減らす。 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新 - ログデータがデータベースに書き込まれる前にログデータが格納されるディレクトリのハードディスク領域の量を増やす。 クライアントログデータ用にサーバーのディスク領域を拡大することについて
データベース保守タスクの実行	クライアントとサーバー間の通信速度を向上させるには、通常のデータベース保守タスクをスケジュール設定します。 自動データベース保守タスクのスケジュール設定

サーバー証明書について

証明書は、機密データを認証し暗号化するための業界標準です。情報がネットワーク内のルーターを通過するときその情報が読み取られるのを防ぐため、データを暗号化する必要があります。

クライアントと通信するために、管理サーバーはサーバー証明書を使います。管理サーバーがサーバー証明書を使ってそれ自体を識別し、認証するように、Symantec Endpoint Protection Manager はデータをデフォルトで暗号化します。ただし、サーバーとクライアント間の暗号化を無効にする必要がある場合があります。

[サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス](#)

[クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート](#)

証明書は念のためバックアップしておく安全です。管理サーバーが破損した場合や、キーストアパスワードを忘れた場合でも、簡単にパスワードを取得できます。

[サーバー証明書のバックアップ](#)

[サーバー証明書の更新または復元](#)

[新しいサーバー証明書の生成](#)

管理サーバーは次の種類の証明書をサポートしています。

- JKS キーストアファイル (.jks) (デフォルト)
キーストアファイルは、keytool.exe と呼ばれる Java ツールによって生成されます。Java Cryptography Extension (.jceks) 形式では、特定のバージョンの Java Runtime Environment (JRE) が必要です。管理サーバー

は、管理サーバー上の Java Development Kit と同じバージョンで生成された .jceks キーストアファイルのみをサポートします。

キーストアファイルには、証明書と専用キーの両方が格納されている必要があります。キーストアパスワードは、キーパスワードと同じである必要があります。次のファイルでパスワードを見つけることができます。

SEPM_Install\Server Private Key Backup\recovery_timestamp.zip

SEPM_Installデフォルトでは、C:\Program Files\Symantec\の Symantec Endpoint Protection Manager です。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files (x86)\Symantec\の Symantec Endpoint Protection Manager です。

パスワードは keystore.password= 行にあります。

- PKCS12 キーストアファイル (.pfx と .p12)

- 証明書と専用キーファイル (.der と .pem の形式)

シマンテックでは、.der 形式または .pem 形式の暗号化されていない証明書と専用キーがサポートされています。Pkcs8 で暗号化された専用キーはサポートされていません。

サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス

次のような場合、セキュリティ証明書の更新が必要になることがあります。

- クライアントがすでに使用している、以前のセキュリティ証明書を復元する場合。
- デフォルトの証明書 (.JKS) とは別のセキュリティ証明書を使用する場合。

クライアントがサーバーとの間でセキュア通信を行う場合、サーバー証明書はサーバーとクライアントの間で交換されます。この交換により、サーバーとクライアントの間に信頼関係が確立されます。サーバーで証明書を変更すると、信頼関係が壊れ、クライアントは通信できなくなります。この問題は孤立クライアントと呼ばれます。

NOTE

1 つの管理サーバーを更新する場合、または複数の管理サーバーを同時に更新する場合は、この処理を使います。

「[サーバー証明書を更新する手順](#)」では、サーバーが管理するクライアントを孤立させずに証明書を更新する手順を示します。

Table 53: サーバー証明書を更新する手順

手順	説明
ステップ 1: 複製関係を解消する	アップデートする管理サーバーを他の管理サーバーで複製する場合は、複製関係を解消します。 アップグレード前後での、複製の無効化と復元
ステップ 2: サーバー証明書の検証を無効にする	サーバーとクライアント間のセキュア通信を無効にします。検証を無効にすると、クライアントの接続は維持したまま、サーバーはサーバー証明書を更新します。 クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート
ステップ 3: すべてのクライアントで更新ポリシーを受信するまで待つ	更新されたポリシーを配備するプロセスには、次のような要因に応じて 1 週間以上かかることがあります。 • 管理サーバーに接続するクライアントの数。新しいポリシーを受け取るには管理下コンピュータがオンラインになる必要があるため、大規模なインストールでは処理が完了するまでに数日かかることがあります。 • ユーザーが休暇中でコンピュータがオフラインになっている、といった可能性があります。 ポリシーのシリアル番号を使ったクライアントとサーバーの通信の確認

手順	説明
ステップ 4: サーバー証明書を更新する	サーバーの証明書を更新する。管理サーバーをアップグレードする計画がある場合は、最初に証明書をアップグレードします。 管理サーバーのアップグレード サーバー証明書の更新または復元 新しい証明書を使うには次のサービスを再起動する必要があります。 • つの Symantec Endpoint Protection Manager サービス • つの Symantec Endpoint Protection Manager Webserver サービス • つの Symantec Endpoint Protection Manager API サービス (14 の時点)
ステップ 5: サーバー証明書の検証を再度有効にする	サーバーとクライアント間のセキュア通信を再度有効にします。 クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート
ステップ 6: すべてのクライアントで更新ポリシーを受信するまで待つ	クライアントコンピュータは前の手順で行ったポリシーの変更を受け取る必要があります。
ステップ 7: 複製関係を復元する*	アップデートした管理サーバーを他の管理サーバーで複製する場合は、複製関係を復元します。 アップグレード前後での、複製の無効化と復元

* これらのステップは、つの Symantec Endpoint Protection Manager 環境で複製を使用する場合にのみ実行する必要があります。

つの Symantec Endpoint Protection Manager のインストール

新しいサーバー証明書の生成

クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート

つの Symantec Endpoint Protection Manager は、Symantec Endpoint Protection クライアントとの通信を証明書を使用して認証します。証明書は、クライアントがダウンロードするポリシーファイルやインストールパッケージに対する電子署名も行います。クライアントは、証明書のキャッシュコピーを管理サーバーリストに保存します。証明書が壊れているか無効な場合、クライアントはサーバーと通信できません。セキュア通信を無効にしても、クライアントはサーバーと通信できますが、管理サーバーからの通信を認証しません。

次のような場合は、セキュア通信を無効にして証明書を更新します。

- 単一の 一つの Symantec Endpoint Protection Manager のサイト
- 複数の 一つの Symantec Endpoint Protection Manager, のサイトで、フェールオーバーや負荷分散を有効にできない場合

NOTE

証明書は壊れているがそれ以外は有効である場合は、ディザスタリカバリを実行するのがベストプラクティスです。

Endpoint Protection のディザスタリカバリのベストプラクティス

証明書の更新後、クライアントがチェックインしてそれを受け取ったら、セキュア通信を再び有効にします。

複数の管理サーバーがありフェールオーバーや負荷分散を使用するサイトで証明書をアップデートすると、証明書は管理サーバーリストでアップデートされます。フェールオーバーまたは負荷分散の処理中、クライアントはアップデート済みの管理サーバーリストと新しい証明書を受け取ります。

NOTE

手順 1 から 5 まではバージョン 14 以降にのみ適用されます。12.x を使用するには、手順 6 から開始します。

1. クライアントとの通信を切断せずに、単一管理サーバーサイト上でサーバー証明書をアップデートするには、コンソールで [ポリシー] > [ポリシーコンポーネント] > [管理サーバーリスト] をクリックします。
2. [タスク] で [リストをコピー] をクリックして、[リストの貼り付け] をクリックします。
3. リストのコピーをダブルクリックして編集し、次の変更を行います。
 - [HTTP プロトコルを使う] をクリックします。
 - 各サーバーアドレスについて、[管理サーバー] で [編集] をクリックし、[HTTP ポートをカスタマイズする] をクリックします。
デフォルトの 8014 のまま残します。カスタムポートを使用する場合は、ここで使用します。
4. [OK] をクリックし、もう一度 [OK] をクリックします。
5. リストのコピーを右クリックして、[割り当て] をクリックします。
6. コンソールで、[クライアント] > [ポリシー] > [全般] をクリックします。
7. [セキュリティの設定] タブで、[認証にデジタル認証を使うことによって管理サーバーとクライアントの間でセキュア通信を有効にする] のチェックマークをはずし、[OK] をクリックします。
8. すべてのグループに対してこの変更を行った後、少なくとも 3 ハートビートサイクル待機してから、手順 9 に進みます。

この設定は、親グループから継承しないグループにも設定してください。

9. サーバーの証明書を更新する。

[サーバー証明書の更新または復元](#)

10. [OK] をクリックします。

元の設定を再度有効にするには、少なくとも 3 回ハートビートサイクルを待機してから、[認証にデジタル認証を使うことによって管理サーバーとクライアントの間でセキュア通信を有効にする] に再度チェックマークを付け、自分のグループに元の管理サーバーリストを割り当て直します。

11. クライアントとの通信を切断せずに、複数管理サーバーサイト上でサーバー証明書をアップデートするには、コンソールで、1 つ以上の他の つの Symantec Endpoint Protection Manager に負荷分散またはフェールオーバーするようにクライアントが構成されていることを確認します。

[フェールオーバーと負荷分散の設定](#)

負荷分散またはフェールオーバーを有効にできない場合は、単一管理サーバーサイトの場合の手順に従って、セキュア通信を一度無効にしてから再び有効にします。

WARNING

通信モジュールの変更により、クライアントバージョン 14.2 では、この方法を使ってサーバー証明書を更新することはできません。これらのクライアントとの通信が切断されないようにするには、複数管理サーバーサイトの場合でも、これらのクライアントバージョンに対して単一管理サーバーサイトの手順を使います。

12. つの Symantec Endpoint Protection Manager 上のサーバー証明書をアップデートします。

[サーバー証明書の更新または復元](#)

-
13. 少なくとも 3 ハートビートサイクル待機してから、サイトの次の つの Symantec Endpoint Protection Manager 上のサーバー証明書を更新します。
 14. サイトの各 つの Symantec Endpoint Protection Manager に新しい証明書が置かれるまで、手順 2 と 3 を繰り返します。

NOTE

社外にいるユーザーや休暇中のユーザーのデバイスはオフライン状態であるため、これらの更新を受け取らない可能性があります。多くの組織では、こうした状態のクライアントをできるだけ多くキャッチするため、30 日間以上のフェールオーバー方法を採用しています。1 つの つの Symantec Endpoint Protection Manager を古い証明書で 90 日間実行し続けて、こうしたユーザーに対応することもできます。

サーバー証明書について

サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス

サーバー証明書の更新または復元

サーバー証明書は、サーバーとクライアント間のファイルを暗号化し、解読します。クライアントは暗号化キーを使ってサーバーに接続し、ファイルをダウンロードし、キーを解読してファイルの信頼性を確認します。手動でクライアントを更新せずに、サーバー上の証明書を変更した場合、サーバーとクライアント間の暗号化された接続が途絶えます。

次の場合はサーバー証明書を更新する必要があります。

- リカバリファイルを使わずに つの Symantec Endpoint Protection Manager を再インストールする場合。クライアントがすでに使っている前の証明書を復元するために証明書を更新します。

つの Symantec Endpoint Protection Manager のインストール

- 1 つの管理サーバーを別の管理サーバーに取り替え、同じ IP およびサーバー名を使う場合。
- ディザスタリカバリの後で間違ったサーバー証明書 (.JKS) を適用する場合。
- 別の証明書を購入し、デフォルトの .JKS 証明書の代わりにその証明書を使う場合。

サーバー証明書について

サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス

サーバー証明書を更新または復元するには

1. コンソールで、[管理] をクリックし、[サーバー] をクリックします。
2. [サーバー] の [ローカルサイト] で、サーバー証明書を更新する管理サーバーをクリックします。
3. [タスク] の下で [サーバー証明書の管理] をクリックし、[次へ] をクリックします。
4. [サーバー証明書の管理] パネルで [サーバー証明書を更新する] をクリックし、[次へ] をクリックしてから [はい] をクリックします。

サーバーとクライアントの接続を維持するため、セキュリティで保護された接続を無効にします。

クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート

5. [サーバー証明書の更新] パネルで更新後の証明書を選択し、[次へ] をクリックします。
6. 証明書の種類ごとにパネルの指示に従った後、[完了] をクリックします。

バックアップサーバー証明書は SEPM_Install\Server Private Key Backup\recovery_timestamp.zip にあります。キーストアファイル用のパスワードは、同じ .zip ファイル内の settings.properties ファイル内で見つけることができます。パスワードは keystore.password= 行にあります。

SEPM_Installデフォルトでは、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

7. 新しい証明書を使うには次のサービスを再起動する必要があります。

- つの Symantec Endpoint Protection Manager サービス
- つの Symantec Endpoint Protection Manager Webserver サービス
- つの Symantec Endpoint Protection Manager API サービス (14 現在)

[管理サーバーサービスの停止と開始](#)

[Apache Web サーバーの停止と開始](#)

コンピュータの IP アドレスとホスト名を変更した後の Symantec Endpoint Protection Manager の再設定

Symantec Endpoint Protection (SEP) クライアントは、Symantec Endpoint Protection Manager (SEPM) コンピュータのホスト名と IP アドレスを使用して、SEPM と通信します。コンピュータのホスト名と IP アドレスを変更すると、クライアントは自動的に通信を維持しません。また、データベースサーバーの名前が変更され、古いコンピュータ名と IP アドレスが含まれる以前の証明書が無効になるため、SEPM はデータベースに接続できません。

SEPM コンピュータの IP アドレスとホスト名が証明書の情報と異なるので、SEPM Web コンソールに証明書エラーが表示されます。

NOTE

SEPM と SEP クライアントが HTTP ではなく HTTPS のみを介して通信する場合に、これらのタスクを実行します。

Symantec Endpoint Protection Manager を再設定し、**SQL Server Express** または **SQL Server** データベースの証明書を作成するには

1. Symantec Endpoint Protection Manager で、現在の設定と新しいホスト名および IP アドレスの両方を使うように管理サーバーリストを更新し、そのリストがすべてのクライアントに割り当てられていることを確認します。
更新されたリストにより、ホスト名と IP アドレスが変更された後も、SEP クライアントは引き続き SEPM と通信できます。

[グループと場所への管理サーバーリストの割り当て](#)

2. [クライアント] > [ポリシー] タブで、[全般] > [セキュリティの設定] タブをクリックし、[認証にデジタル認証を使うことによって管理サーバーとクライアントの間でセキュア通信を有効にする] のチェックマークをはずします。セキュア通信を無効にすると、クライアントは SEPM との通信を認証せずに、引き続き SEPM と通信できます。

[クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート](#)

3. [クライアント] > [クライアント] タブで、クライアントが管理サーバーに接続されていることを確認します。
4. SEPM コンピュータの IP アドレスを変更します。
5. SEPM コンピュータのホスト名を変更してから、SEPM コンピュータを再起動します。

NOTE

コンピュータのホスト名のみを変更できます。必ずしも IP アドレスを変更する必要はありません。

6. 次のコマンドを実行して、SEPM サービスを停止します: `net stop semsrv`、`net stop semapisrv`、および `net stop semwebsrv`

[管理サーバーサービスの停止と開始](#)

7. 次のファイルについて、以下の手順を実行します。

```
<Symantec Endpoint Protection Manager #####>\tomcat\conf\Catalina\localhost\root.xml
```

```
<Symantec Endpoint Protection Manager #####>\tomcat\instances\sepm-api\conf\Catalina_WS\localhost\jdbc.properties
```

- a. `jdbc:sqlserver://SEPM_OLD_COMPUTER_NAME:2638` を `jdbc:sqlserver://SEPM_NEW_COMPUTER_NAME:2638` に変更します。2638 とは異なるポート番号を使用している場合は、引き続きその番号を使用します。

- b. `trustServerCertificate = false` を `trustServerCertificate = true` に変更します。
8. 次のコマンドを実行して、SEPM サービスを再起動します:`net start semsrv`、`net start semapisrv`、および `net start semwebsrv`
9. SEPM にログオンします。
「#####」というメッセージが表示されたら、[OK] をクリックして、そのままログオンします。
10. 新しい SEPM サーバー証明書を生成します。
この手順では、SEPM と SEP クライアント間の証明書の情報を、新しいコンピュータ名および IP アドレスに一致させます。
[新しいサーバー証明書の生成](#)
11. SEPM コンソールからログオフします。
12. 以下のいずれかの手順に従います。

Microsoft SQL Server Express データベース	1. SEPM を再設定します。 つの Symantec Endpoint Protection Manager の再インストールまたは再設定 2. SEPM にログオンします。
[Microsoft SQL Server データベース]	1. SEPM を再設定します。TLS メッセージが表示されます。 2. 新しい SQL TLS 証明書を生成してインポートします。設定を完了します。 3. SEPM にログオンします。 SQL Server データベースが SEPM と同じコンピュータ上にある場合は、「コンピュータのホスト名を変更した後に Microsoft SQL Server データベースをクライアントに再接続する」を参照してください。
埋め込みデータベース	SEPM にログオンします。

13. [認証にデジタル認証を使うことによって管理サーバーとクライアントの間でセキュア通信を有効にする] を有効にします。
14. クライアントが引き続き SEPM に接続されていることを確認します。

[サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス](#)

コンピュータのホスト名を変更した後に **Microsoft SQL Server** データベースをクライアントに再接続する

SEPM と同じコンピュータ上で Microsoft SQL Server をデータベースサーバーとして使う場合、コンピュータのホスト名を変更すると、ODBC 接続に使用されるサーバー名が変更されます。ODBC 接続に使用されるサーバー名を更新する必要があります。IP アドレスではなく、SEPM のコンピュータ名のみを変更します。

ODBC 接続で使用されるサーバー名を変更するには

1. Symantec Endpoint Protection Manager コンピュータで、[スタート] > [ファイル名を指定して実行] をクリックします。
2. [名前] フィールドに、「odbc32.exe」(32 ビットの場合) または「odbcad32.exe」(64 ビットの場合) を入力して、[OK] をクリックします。
3. [ODBC データ ソース アドミニストレーター] ダイアログボックスで、[システム DSN] タブをクリックします。
4. システム DSN として [SymantecEndpointSecurityDSN] を選択し、[構成] をクリックします。
5. サーバー名の正しい接続先 (I など) を入力し、[次へ] をクリックします。
6. Windows 認証を使う場合は、[統合 **Windows** 認証を使う] を選択します。SQL Server 認証を使う場合は、[ユーザーが入力する **SQL Server** 用のログイン ID とパスワードを使う] にチェックマークを付けて、ログイン ID とパスワードを入力し、[**SQL Server** に接続して追加の構成オプションの既定設定を取得する] にチェックマークを付けて、[次へ] をクリックします。
7. [既定のデータベースを以下に変更する:] を選択し、[sem5] を選択して [次へ] をクリックします。
8. [完了] をクリックします。
9. [ODBC Microsoft SQL Server] ダイアログボックスで、[データ ソースのテスト] をクリックします。
「#####」というメッセージが表示された場合、ODBC 接続テストは完了です。

クライアントが管理サーバーに接続され、保護されているかどうかの確認

クライアントをインストールした後、クライアントがオンラインで 2 つの Symantec Endpoint Protection Manager に接続しているかどうかを確認します。コンソールとクライアントの両方で接続状態を確認できます。

1. Symantec Endpoint Protection クライアントでクライアント管理サーバー接続を確認するには、クライアントコンピュータで、以下のいずれかのタスクを行います。

- コンピュータのタスクバーで、クライアントシールドには緑色のドットが表示されます。



- クライアントを開いて、[状態] 画面を確認します。この画面には、[このコンピュータは保護されています。] というメッセージと緑色のチェックマークが表示されま



- クライアントを開いて、[ヘルプ] > [トラブルシューティング] をクリックします。

Symantec Endpoint Protection クライアントの状態アイコン

2. 2 つの Symantec Endpoint Protection Manager でクライアント管理サーバーの接続を確認するには、コンソールで [クライアント] をクリックして、移動先グループを選択します。
3. [クライアント] タブでは、接続されているクライアントは [名前] 列に緑色のドット付きのアイコンが表示され、健全性状態が [オンライン] と表示されます。

NOTE

2 つの Symantec Endpoint Protection Manager から接続するクライアントの場合は、クラウドコンソールに正しいオンライン状態がすぐには表示されないことがあります。オンライン状態が変わってから 5 分から 10 分待ち、現在の状態が正確に反映されるかどうかを確認してください。

Table 54: [クライアント] > [クライアント] タブ > [名前] 列の管理コンソールのクライアントの状態アイコン

アイコン	説明
	クライアントソフトウェアのインストールが失敗した
	• クライアントは Symantec Endpoint Protection Manager と通信できる健全性の状態が [オンライン] である • クライアントはコンピュータモードを使用している
	• クライアントは Symantec Endpoint Protection Manager と通信できない健全性の状態が [オフライン] である • クライアントはコンピュータモードを使用している • クライアントがコンソールから追加され、シマンテック製クライアントソフトウェアがインストールされていない可能性がある
	• クライアントは Symantec Endpoint Protection Manager と通信できる • クライアントはコンピュータモードを使用している • クライアントは管理外検出になっている
	• クライアントは Symantec Endpoint Protection Manager と通信できない • クライアントはコンピュータモードを使用している • クライアントは管理外検出になっている
	• クライアントは Symantec Endpoint Protection Manager と通信できる • クライアントはユーザーモードを使っている

アイコン	説明
	- クライアントは Symantec Endpoint Protection Manager と通信できない - クライアントはユーザーモードを使っている - クライアントがコンソールから追加され、シマンテック製クライアントソフトウェアがインストールされていない可能性がある
	- クライアントは、別のサイトの Symantec Endpoint Protection Manager と通信できる - クライアントはコンピュータモードを使用している
	- クライアントは、別のサイトの Symantec Endpoint Protection Manager と通信できる - クライアントはコンピュータモードを使用している - クライアントは管理外検出になっている
	- クライアントは、別のサイトの Symantec Endpoint Protection Manager と通信できる - クライアントはユーザーモードを使っている

クライアントコンピュータの保護状態の表示

Symantec Endpoint Protection クライアントの状態アイコン

クライアントが管理サーバーに接続済みで、十分に保護されているかどうかを判断するには、クライアントの通知領域アイコンを確認します。通知領域アイコンはシステムトレイアイコンと呼ばれることもあります。

このアイコンは、クライアントコンピュータデスクトップの右下に表示されます。このアイコンを右クリックすると、使う頻度が高いコマンドが表示されます。

NOTE

管理下クライアントでは、管理者がこの機能を利用不能にしている場合、通知領域アイコンは表示されません。

Table 55: クライアントの状態アイコン

アイコン	説明
	クライアントは問題なく動作しています。オフラインになっているか管理外であるかのいずれかです。管理外クライアントは管理サーバーに接続されていません。
	クライアントは問題なく動作しています。管理サーバーに接続され、サーバーと通信しています。セキュリティポリシーのすべてのコンポーネントがコンピュータを保護しています。
	クライアントに軽度な問題があります。たとえば、ウイルス定義が最新ではないなどです。
	クライアントが実行されていないか、クライアントに重度の問題があるか、ライセンスの期限が切れているか、少なくとも 1 つの保護技術が無効になっています。

Symantec Endpoint Protection クライアントの通知領域アイコンの非表示と表示

ポリシーのシリアル番号を使ったクライアント/サーバーの通信の確認

サーバーとクライアントが通信しているかどうかを確認するには、コンソールとクライアントのポリシーのシリアル番号を確認します。クライアントが管理サーバーと通信しており、定期的なポリシー更新を受信している場合、シリアル番号は一致する必要があります。

ポリシーのシリアル番号が一致しない場合、手動でクライアントコンピュータのポリシーを更新し、トラブルシューティングのログを調べることができます。

クライアントポリシーの更新

プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新

1. オプション 1: コンソールでポリシーのシリアル番号を表示するには、コンソールで [クライアント] をクリックします。
2. [クライアント] の下で、関連したグループを選択します。

ポリシーのシリアル番号とポリシーの日付はプログラムウィンドウの右上に表示されます。

NOTE

ポリシーのシリアル番号とポリシーの日付は、[詳細] タブの詳細リストの下部にも表示されます。

3. オプション 2: クライアントコンピュータでポリシーのシリアル番号を表示するには、クライアントコンピュータのクライアントで、[ヘルプ] > [トラブルシューティング] をクリックします。

[管理] タブで、ポリシーのシリアル番号を確認します。

このシリアル番号は、クライアントコンピュータが属するグループのコンソールに表示されるシリアル番号と一致する必要があります。

すべてのポリシーに共通なタスクの実行

プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新

つの Symantec Endpoint Protection Manager とクライアントとの間の接続にプルモードまたはプッシュモードのどちらを使用するか の決定

グループに対してプッシュモードまたはプルモードを設定する

つの Symantec Endpoint Protection Manager とクライアントとの間の接続にプルモードまたはプッシュモードのどちらを使用するか の決定

管理サーバーのポリシーを設定するとき、更新されたポリシーをクライアントコンピュータにダウンロードする必要があります。コンソールでは、次の更新方法のどちらかを使うようにクライアントコンピュータを設定できます。

プルモード	クライアントコンピュータは、ハートビート設定の頻度に基づいて、管理サーバーに定期的に接続します。クライアントコンピュータは、クライアントの接続時に管理サーバーの状態を確認します。
プッシュモード	クライアントコンピュータは管理サーバーと常時 HTTP 接続を確立します。管理サーバーの状態に変更が発生すると、すぐにクライアントコンピュータに通知されます。

どちらのモードでも、クライアントコンピュータは管理サーバーの状態の変化に基づいて、対応する処理を行います。常時接続が必要であるため、プッシュモードでは大量のネットワーク帯域幅が必要です。プルモードを使うように設定されたクライアントコンピュータでは、必要な帯域幅は減少します。

ハートビートプロトコルは、クライアントコンピュータがログエントリなどのデータをアップロードして、ポリシーをダウンロードする頻度を定義します。最初のハートビートはクライアントの起動直後に発生します。次のハートビートは設定したハートビート頻度で発生します。

ハートビートの頻度は、各 1 つの Symantec Endpoint Protection Manager がサポート可能なクライアントの数を決める主要な要素です。ハートビートの頻度を 30 分以下に設定した場合、1 つの Symantec Endpoint Protection Manager がサポート可能なクライアントの合計数は制限されます。1,000 以上のクライアントが配備されている場合、ハートビート頻度をできる限り最大の時間長に設定することをお勧めします。会社のセキュリティ必要条件を満たす、最も長い間隔を使うことをお勧めします。たとえば、毎日ポリシーを更新してログを収集する場合、ハートビート頻度は 24 時間に設定できます。ご使用のネットワーク環境で必要とされる適切な設定、ハードウェア、ネットワークアーキテクチャを評価します。

NOTE

クライアントコンピュータで手動でポリシーを更新することもできます。

ポリシーのシリアル番号を使ったクライアントとサーバーの通信の確認

Symantec Endpoint Protection の通信ポート

グループに対してプッシュモードまたはプルモードを設定する

つの Symantec Endpoint Protection Manager がポリシーをクライアントにプッシュするか、クライアントが 1 つの Symantec Endpoint Protection Manager からポリシーをプルするかを指定できます。デフォルト設定はプッシュモードです。プルモードを選択した場合、デフォルトではクライアントは 5 分ごとに管理サーバーに接続しますが、このデフォルトハートビート間隔は変更できます。

すべてのポリシーに共通なタスクの実行

グループまたは場所に対してモードを設定できます。

NOTE

12.1.6.6 以前の場合、クライアント数が 100 を超え、1 つの Symantec Endpoint Protection Manager をデスクトップのオペレーティングシステムにインストールする場合はプルモードを使用します。デスクトップのオペレーティングシステムでは許可される同時接続に制限があるため、プッシュモードでは、それらの使用可能な接続がすぐになくなってしまう可能性があります。

1. グループに対してプッシュモードまたはプルモードを設定するには、コンソールで [クライアント] をクリックします。
2. [クライアント] で、ポリシーをプッシュ型またはプル型で転送するように指定するグループを選択します。
3. [ポリシー] をクリックします。
4. [ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。
5. [場所に依存しないポリシーと設定] ペインの [設定] で、[通信の設定] をクリックします。
6. [<グループ名> の通信設定] ダイアログボックスの [ダウンロード] で、[管理サーバーからポリシーやコンテンツをダウンロードする] にチェックマークを付けていることを確認します。
7. 次のいずれかのタスクを行います。
 - [プッシュモード] をクリックします。
 - [プルモード] をクリックし、[ハートビート間隔] で分または時間の数を設定します。
8. [OK] をクリックします。
9. 場所に対してプッシュモードまたはプルモードを指定するには、コンソールで [クライアント] をクリックします。
10. [クライアント] で、ポリシーをプッシュ型またはプル型で転送するように指定するグループを選択します。
11. [ポリシー] をクリックします。
12. [ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。
13. [場所固有のポリシーと設定] の修正する場所に対する [場所固有のポリシー] で、[場所固有の設定] を展開します。
14. [場所固有の設定] の [通信の設定] の右側で、[タスク] をクリックし、[グループ通信設定を使う] のチェックマークをはずします。
15. [通信の設定] の右側で、[ローカル - プッシュ型転送] (または [ローカル - プル型転送]) をクリックします。
16. 次のいずれかのタスクを行います。
 - [プッシュモード] をクリックします。
 - [プルモード] をクリックし、[ハートビート間隔] で分または時間の数を設定します。

17. [OK] をクリックします。

すべてのポリシーに共通なタスクの実行

クライアントコンピュータと管理サーバーの通信方法

つの Symantec Endpoint Protection Manager は、Sylink.xml と呼ばれる通信ファイルを使ってクライアントに接続します。Sylink.xml ファイルには、管理サーバーの IP アドレスやハートビート間隔などの通信設定が含まれています。クライアントコンピュータにクライアントインストールパッケージをインストールした後、クライアントとサーバーは自動的に通信します。

SyLink ファイルは、機能の多くをハートビートの間に実行します。ハートビートとは、クライアントコンピュータが管理サーバーにログをアップロードして、ポリシーとコマンドをダウンロードする頻度のことです。

SyLink ファイルには次の内容が含まれます。

- すべての管理サーバーの公開証明書
- KCS または暗号化キー
- 各クライアントが所属するドメイン ID

NOTE

SyLink ファイルは編集しないでください。設定を変更すると、クライアントが次に管理サーバーに接続したときに、管理サーバーがほとんどの設定を上書きします。

プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新

SyLink 通信のトラブルシューティング

バージョン 14.2 では通信モジュールがアップグレードされ、新しいログファイルが含まれています。ログファイルの情報を、つの Symantec Endpoint Protection Manager とクライアントの間の通信の問題をトラブルシューティングするために使用できます。

14.2 の通信モジュールは、Windows、Mac、Linux など、すべての種類のクライアントと連携します。また、IPv6 のサポートが改善されています。

NOTE

バージョン 14.2 以降、通信モジュールではシステムプロキシの情報だけが利用されます。

1. 通信モジュールのログファイルを表示するには、Windows クライアントの場合、次のフォルダを確認します。

`C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data`

次のファイルを表示できます。

- クライアント登録:
 - `RegistrationInfo.xml`
クライアントが 1 つの Symantec Endpoint Protection Manager に送信するクライアント登録のメタデータ。
 - `Registration.xml`
1 つの Symantec Endpoint Protection Manager がクライアントに返すクライアント登録のメタデータ。
 - `State.xml`
管理サーバーの IP アドレスなどの内部設定が含まれます。
- 通信モジュールのログ:
`\Logs\cve.log` と `\Logs\cve-actions.log`
これらのログは、1 つの Symantec Endpoint Protection Manager とクライアントの間の通信の問題をトラブルシューティングするために使用します。提供を求められた場合は、テクニカルサポートにこれらのログを送信します。
- 運用状態:

\Pending と \Sent フォルダのログに記載されます。

2. 通信モジュールのログを設定するには、Windows のレジストリエディタを開きます。それには、[スタート] > [ファイル名を指定して実行] をクリックし、「regedit」と入力して、[OK] をクリックします。
3. cve.log または cve-actions.log を有効にするには、次の Windows レジストリキーを開きます。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink  
REG_DWORD: CVELogLevel
```

次の値のいずれかを使用します。

- 1 = デバッグ
- 2 = 情報
- 3 = 警告
- 4 = エラー
- 5 = 致命的

レジストリキーが存在しないか有効な値がない場合、デフォルト設定は 4 になります。インストールでのデフォルト設定も 4 になります。

たとえば、次のように入力できます。

```
32 ビット: [HKLM\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink]  
"CVELogLevel"=dword:00000001
```

```
64 ビット: [HKLM\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SYLINK  
\SyLink] "CVELogLevel"=dword:00000001
```

4. これらのログのサイズを制御するには、次のレジストリ値を使用します。[HKEY_LOCAL_MACHINE\SOFTWARE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SYLINK\SyLink] REG_DWORD: CVELogSizeDB

デフォルトサイズは 250 MB です。

[Endpoint Protection 14.2 で通信モジュールのログを有効にする方法](#)

[Endpoint Protection クライアントの Sylink デバッグを有効にする方法 \(14.1 以前 \)](#)

クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法

クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える時期

通常は、Sylink.xml ファイルを取り替える必要はありません。ただし、次のような状況では、クライアントコンピュータの既存の Sylink.xml ファイルを取り替える必要がある場合もあります。

- クライアントとサーバーが通信しない。クライアントが管理サーバーとの通信を失った場合、古い Sylink.xml ファイルを新しいファイルで置き換える必要があります。

[クライアントコンピュータの管理サーバーへの接続のチェック](#)

- 管理外クライアントを管理下クライアントに変換する。ユーザーがインストールファイルからクライアントをインストールした場合、クライアントは管理外になり管理サーバーと通信しません。管理下コンピュータとして、コンピュータのクライアントソフトウェアを再インストールすることもできます。

[管理下クライアントと管理外クライアントについて](#)

- 前に孤立していたクライアントを管理する。たとえば、管理サーバーがインストールされていたハードドライブが損傷した場合は、管理サーバーを再インストールする必要があります。孤立していたクライアントの Sylink.xml ファイルをアップデートして、それらとの間の通信を再確立できます。

[クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート](#)

クライアントとサーバーの通信ファイル (Sylink.xml) の手動によるエクスポート

- 複数のグループから 1 つのグループに多数のクライアントを移動する。たとえば、リモートグループおよびラップトップグループのクライアントコンピュータをテストグループに移動する場合です。通常は、クライアントコンピュータを一度に 1 グループずつ移動する必要があります。

別のグループへのクライアントコンピュータの移動

クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

SEP for Macintosh 管理外クライアントを管理クライアントに変更する方法

クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法

クライアントコンピュータ上のクライアントとサーバーの通信ファイル (Sylink.xml) の置き換えが必要な場合は、次の方法を使えます。

- 新しいクライアントインストールパッケージを作成し、クライアントコンピュータに配備します。大規模な環境に手動で Sylink.xml をインポートすることが物理的に難しく、管理アクセスが必要な場合にこの方法を使います。

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

- SylinkDrop ツールを実行するスクリプトを記述します。このツールは、インストールファイルの \Tools フォルダにあります。この方法は、クライアント数が多い場合に推奨されます。また、SylinkDrop ツールは、ソフトウェア管理ツールを使ってコンピュータにクライアントソフトウェアをダウンロードする場合にも使います。ソフトウェア管理ツールの利点は、エンドユーザーがクライアントコンピュータを起動するとすぐに Sylink.xml ファイルをダウンロードすることです。それに対し、クライアントインストールパッケージでは、クライアントコンピュータが管理サーバーに接続した後にのみ、新しい Sylink.xml ファイルがダウンロードされます。

SylinkDrop ツールを使ったクライアントとサーバー間の通信設定の復元

- Sylink.xml ファイルをクライアントコンピュータにエクスポートし、クライアントコンピュータ上のファイルを手動でインポートします。ソフトウェア管理ツールを使用する場合は、この方法をお勧めします。ソフトウェア管理ツールでは、ジョブはキューに待機し、各ユーザーが自分のコンピュータを起動するときに完了されます。他の方法では、クライアントコンピュータはオンラインである必要があります。

「通信ファイルをエクスポートし、インポートする手順」は、クライアントコンピュータに Sylink.xml ファイルをエクスポートし、インポートする手順を示します。

Table 56: 通信ファイルをエクスポートし、インポートする手順

手順	説明
ステップ 1: クライアントを含めるグループのすべての通信設定を含むファイルをエクスポートする	デフォルトのファイル名は、グループ名_sylink.xml です。 クライアントとサーバーの通信ファイル (Sylink.xml) の手動によるエクスポート
ステップ 2: クライアントコンピュータにファイルを配備する	ネットワーク上の場所にファイルを保存するか、またはクライアントコンピュータの個々のユーザーに送信できます。
ステップ 3: クライアントコンピュータにファイルをインポートする	管理者またはユーザーがクライアントコンピュータでファイルをインポートできます。 Windows クライアントへのクライアントとサーバーの通信設定のインポート 管理外クライアントはパスワード保護されていないため、クライアントのパスワードは必要ありません。ただし、パスワード保護した管理下クライアントにファイルをインポートしようとする場合は、パスワードを入力する必要があります。パスワードはポリシーをインポートするか、またはエクスポートするために使われるものと同じです。 Symantec Endpoint Protection クライアントのパスワード保護 クライアントコンピュータを再起動する必要はありません。

手順	説明
ステップ 4: クライアント上でクライアントとサーバーの通信を確認する	クライアントは管理サーバーにただちに接続します。管理サーバーは通信ファイルで指定されているグループにクライアントを配置します。クライアントはグループのポリシーと設定によって更新されます。クライアントと管理サーバーが通信すると、緑のドットが付いた通知領域アイコンがクライアントコンピュータのタスクバーに表示されます。 クライアントが管理サーバーに接続され、保護されているかどうかの確認

クライアント/サーバーの通信のファイル

クライアントコンピュータと管理サーバーの通信方法

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

クライアントとサーバーの通信が切断された場合、クライアントコンピュータの Sylink.xml ファイルを置き換えることで通信をすばやく復元できます。通信の更新パッケージを配備することで、Sylink.xml ファイルを置き換えることができます。多数のコンピュータ、物理的に容易にはアクセスできないコンピュータ、管理アクセスを必要とするコンピュータに対して、この方法を使います。

クライアントコンピュータと管理サーバーの通信方法

クライアントコンピュータでクライアントとサーバーの通信ファイルを置き換える方法

1. コンソールで、クライアント配備ウィザードを起動します。
[ヘルプ]、[始めましょう] ページをクリックして [必須タスク] で [コンピュータにクライアントソフトウェアをインストールします。] をクリックします。
2. クライアント配備ウィザードの [通信の更新パッケージの配備] で Windows クライアント、Mac クライアントのどちらのパッケージが必要かを選択してから、[次へ] をクリックします。
3. ポリシーを適用するグループを選択してから、[次へ] をクリックします。
Windows クライアントに対してのみ、パスワード保護を設定できます。
[Symantec Endpoint Protection クライアントのパスワード保護](#)
4. 次の配備方法のいずれかを選択して [次へ] をクリックします。
 - [リモートプッシュ] をクリックして、次の手順の [コンピュータの選択] に進みます。
[リモートプッシュを使った Symantec Endpoint Protection クライアントのインストール](#)
 - [パッケージの保存] をクリックして、次の手順の [参照] に進みます。
[パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール](#)
5. 通信の更新パッケージが適用された後で、コンピュータが 2 つの Symantec Endpoint Protection Manager と正常に通信できることを確認します。

[クライアントが管理サーバーに接続され、保護されているかどうかの確認](#)

[クライアントの配備の状態についてのレポートの実行](#)

クライアントとサーバーの通信ファイル (Sylink.xml) の手動によるエクスポート

クライアントとサーバー間で通信が行われない場合は、通信を復元するために、クライアントコンピュータに Sylink.xml ファイルを置換する必要があることがあります。2 つの Symantec Endpoint Protection Manager からグループごとに Sylink.xml ファイルを手動でエクスポートできます。

クライアントで Sylink.xml を置き換える最も一般的な理由には次のものがあります。

-
- 管理外クライアントを管理下クライアントに変換するため。
 - 以前に孤立していたクライアントを管理サーバーに再接続するため。
クライアントとの通信を切断しない、管理サーバー上のサーバー証明書のアップデート

クライアントコンピュータと管理サーバーの通信方法

多数のクライアントを対象にクライアントとサーバーの通信を更新する必要がある場合は、この方法を使う代わりに通信の更新パッケージを配備します。

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、クライアントが含まれるグループを選択します。
3. グループを右クリックしてから、[通信設定のエクスポート] をクリックします。
4. [<グループ名> の通信設定のエクスポート] ダイアログボックスで、[参照] をクリックします。
5. [エクスポートファイルの選択] ダイアログボックスで .xml ファイルのエクスポート先のフォルダを検索してから、[OK] をクリックします。
6. [優先ポリシーモード] で、[コンピュータモード] にチェックマークが付いていることを確認します。
7. [エクスポート] をクリックします。

ファイル名がすでに存在する場合、上書きするには [OK]、新しいファイル名のファイルを保存するには [キャンセル] をクリックします。

変換を終えるためには、管理者またはユーザーはクライアントコンピュータに通信設定をインポートする必要があります。

Windows クライアントへのクライアントとサーバーの通信設定のインポート

Windows クライアントへのクライアントとサーバーの通信設定のインポート

Windows クライアントとサーバーの通信設定をエクスポートしたら、それらをクライアントにインポートできます。管理外クライアントを管理下クライアントに変換したり、以前に孤立していたクライアントを Symantec Endpoint Protection Manager に再接続するために、この設定を使用できます。

Windows クライアントとサーバーの通信設定をクライアントにインポートするには

1. 管理下クライアントに変換するコンピュータで Symantec Endpoint Protection を開きます。
2. 右上の [ヘルプ] をクリックして [トラブルシューティング] をクリックします。
3. [トラブルシューティング] ダイアログボックスの [管理] ペインで、[インポート] をクリックします。
4. [グループ登録設定のインポート] ダイアログボックスで、<グループ名_symlink>.xml ファイルを選択して [開く] をクリックします。
5. [閉じる] をクリックして [トラブルシューティング] ダイアログボックスを閉じます。

通信ファイルをインポートし、クライアントと管理サーバーが通信すると、通知領域アイコンが緑のドットと共にコンピュータのタスクバーに表示されます。緑のドットはクライアントと管理サーバーが相互に通信していることを示します。

クライアントとサーバーの通信ファイル (Symlink.xml) の手動によるエクスポート

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

Linux クライアントへのクライアントとサーバーの通信設定のインポート

(14.3 MP1 以前の場合)

管理外の Symantec Endpoint Protection for Linux クライアントをインストールした後で、管理下クライアントに変換して 1 つの Symantec Endpoint Protection Manager でクライアントのポリシーと状態を一元管理できます。管理下クライアントは 1 つの Symantec Endpoint Protection Manager と通信し、クライアントの状態やその他の情報を報告します。

以下の手順で、以前に孤立したクライアントを 1 つの Symantec Endpoint Protection Manager と再接続することもできます。

NOTE

この手順を実行するにはスーパーユーザーの権限が必要です。インポート手順で必要に応じて `sudo` を使ってこの権限に昇格します。

テキスト `path-to-sav` は、`sav` コマンドへのパスを表します。デフォルトのパスは `/opt/Symantec/symantec_antivirus/` です。

クライアントとサーバーの通信設定ファイルを **Linux** クライアントにインポートするには

1. ユーザーまたは 1 つの Symantec Endpoint Protection Manager 管理者は最初に 1 つの Symantec Endpoint Protection Manager から通信設定をエクスポートして Linux コンピュータにコピーする必要があります。ファイル名が `sylink.xml` であることを確認します。

[クライアントとサーバーの通信ファイル \(Sylink.xml \) の手動によるエクスポート](#)

2. Linux コンピュータでターミナルウィンドウを開いて次のコマンドを入力します。

```
sudo path-to-sav/sav manage -i path-to-sylink/sylink.xml
```

ここで、`path-to-sylink` は、`sylink.xml` をコピーしたパスを表します。

たとえば、ユーザープロファイルのデスクトップにコピーした場合は次のように入力します。

```
sudo path-to-sav/sav manage -i ~/Desktop/sylink.xml
```

3. 正常にインポートされると OK が返されます。さらに管理状態を確認する場合は次のコマンドを入力すると、正常にインポートされたポリシーのシリアル番号が表示されます。

```
path-to-sav/sav manage -p
```

[Symantec Endpoint Protection for Linux クライアントのインストール](#)

IPv6 ネットワークサポート

このサポートはバージョン 14.2 で追加されました。

IPv6 は IPv4 の後継となるインターネットプロトコルに対するリビジョンです。どちらのタイプのアドレスも、インターネット対応デバイスが通信するために必要な一意の IP アドレスを数値で提供します。IPv4 アドレスは 32 ビットで、IPv6 アドレスは 128 ビットです。このため、IPv6 では、ユーザーやデバイスがインターネットで通信に利用できるアドレスの数が増加します。

IPv6 アドレスは、慣例として 16 進文字列を使用する方式で表現されます。たとえ

ば、`fd32:32a4:d0cf:a0c4:0000:8a2e:0370:7334` などです。これは、`fd32:32a4:d0cf:a0c4::8a2e:0370:7334` のように表すこともできます。ポート番号で終了する IPv6 アドレスを入力するときは、IPv6 アドレスを角カッコで囲む必要があります。角カッコによって、ポート番号が IPv6 アドレスの一部として解釈されなくなります。例: `http://[fd32:32a4:d0cf:a0c4::8a2e:0370:7334]:9090`

Symantec Endpoint Protection 14.2 では、次のかたちで IPv6 をサポートしています。

-
- 管理サーバーと Windows、Mac、Linux クライアントの間の通信
 - つの Symantec Endpoint Protection Manager へのローカルまたはリモートでのログオンなど、コンソールと管理サーバーの間の通信
 - [つの Symantec Endpoint Protection Manager コンソールへのログオン](#)
 - 管理サーバーと LiveUpdate Administrator を実行する社内の LiveUpdate サーバーの間の通信
 - [社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定](#)
 - 管理サーバーへの Windows LiveUpdate
 - 管理サーバーまたはクライアントと LiveUpdate エンジン (LUE) や評価ルックアップなどのサービスまたは機能の間の通信
 - IPv6 ベースの基準によるネットワークの検出での場所の定義

さらに、その他の多くのポリシーによって、カスタム IPS シグネチャや明示的な GUP などの基準定義で IPv4 だけでなく IPv6 アドレスを入力できます。

次の項目では、IPv6 はサポートされません。

- Symantec VIP での 2 要素認証 (2 FA)
 - [Symantec VIP を使用した 2 要素認証の設定](#)
- クラウドコンソールへの登録と接続

グループ、クライアント、管理者、およびドメインの管理

グループ、クライアント、管理者、パスワード、およびドメインを追加および管理する方法について

このセクションでは、クライアントコンピュータ、クライアント、管理者、パスワード、およびドメインのグループを管理する方法を説明します。

クライアントのグループの管理

つの Symantec Endpoint Protection Manager では、グループはクライアントソフトウェアを実行するエンドポイントのコンテナとして機能します。これらのエンドポイントは、コンピュータかユーザーのどちらかになります。ネットワークセキュリティの管理を簡単にするため、類似したセキュリティニーズを持つクライアントをグループに編成します。

つの Symantec Endpoint Protection Manager は次のデフォルトグループを含んでいます。

- **My Company** グループは最上位、または親のグループです。子グループのフラットツリーを含んでいます。
- **Default Group** は **My Company** のサブグループです。クライアントは事前定義済みのグループに属さなければ、最初につの Symantec Endpoint Protection Manager に登録するとき **Default Group** に最初に割り当て済みです。**Default Group** の下にサブグループを作成することはできません。

NOTE

デフォルトグループは名前を変更または削除できません。

クラウドコンソールの [My Company] の名前を変更しても、つの Symantec Endpoint Protection Manager のグループ名は変更されません。

Table 57: グループ管理の処理

タスク	説明
グループの追加	グループを構成する方法 グループの追加
既存のグループのインポート	組織に既存のグループ構造がすでにある場合、組織単位としてグループをインポートできます。 Note: つの Symantec Endpoint Protection Manager で作成したグループを管理する方法では、インポートした組織単位を管理できません。 Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート
サブグループの継承の無効化	サブグループは親グループから同じセキュリティの設定をデフォルトで継承します。継承は無効にできません。 グループの継承の無効化
グループ内の場所の作成	クライアントの物理的な位置が変更された場合は異なるセキュリティポリシーに自動的に切り替えるようにクライアントを設定できます。 リモートクライアントの場所の管理 一部のセキュリティ設定はグループ別であり、一部の設定は場所固有のものです。場所固有の設定をカスタマイズできます。 場所に対する通信の設定
グループのセキュリティポリシーの管理	各グループのニーズに基づいてセキュリティポリシーを作成できます。さらに別々のポリシーを別々のグループまたは場所に割り当てられます。 ポリシーの追加 グループまたは場所へのポリシーの割り当て すべてのポリシーに共通なタスクの実行

タスク	説明
グループ保守の実行	管理を簡易化するためにグループを移動したり、グループ間でクライアントを移動できます。また、特定のグループにクライアントが追加されないようにすることもできます。 別のグループへのクライアントコンピュータの移動 グループへのクライアントコンピュータ追加の遮断

グループを構成する方法

会社の組織構造とセキュリティに合わせて複数のグループやサブグループを作成できます。機能、役割、地理、基準の組み合わせにグループ構造を基づかせることができます。

Table 58: グループを作成するための基準

基準	説明
関数	ノートパソコン、デスクトップ、サーバーなど、管理されるべきコンピュータのタイプに基づいてグループを作成できます。また、使用法の種類に基づいている複数のグループを作成できます。たとえば、外に持ち出すクライアントコンピュータのリモートグループや、オフィスに置いたままのクライアントコンピュータのローカルグループを作成できます。
役割	販売、エンジニアリング、財務、マーケティングなど、部門の役割のグループを作成できます。
地理	コンピュータがあるオフィス、都市、州、地域、国に基づいてグループを作成できます。
組み合わせ	基準の組み合わせに基づいてグループを作成できます。たとえば、機能と役割を使うことができます。次のシナリオのように、役割ごとに親グループを追加して機能ごとに子サブグループを追加できます。 - ノートパソコン、デスクトップ、サーバーのサブグループを含む販売。 - ノートパソコン、デスクトップ、サーバーのサブグループを含むエンジニアリング。

クライアントコンピュータをグループにまとめたら、そのグループに適切なセキュリティを適用できます。

たとえば、会社に通信販売部と経理部があるとします。会社のニューヨーク、ロンドン、フランクフルトオフィスにこれらの部門のスタッフがいます。両方の部門のすべてのコンピュータは同じ更新元からウイルス定義とセキュリティリスク定義の更新を受信するように同じグループに割り当てられています。ただし、IT レポートは通信販売部が経理部よりリスクに脆弱であることを示しています。その結果、システム管理者は通信販売グループと経理グループを別々に作成します。通信販売のクライアントは、ユーザーがウイルスとセキュリティリスク防止を操作する方法を厳しく限定する設定を共有します。

グループ構成するためのベストプラクティス

すべてのポリシーに共通なタスクの実行

クライアントのグループの管理

グループの追加

組織のグループ構造を定義した後で、グループを追加できます。

グループの説明の長さは最大 1024 文字です。グループ名には、次の文字を除く任意の文字を使うことができます。"/ \ * ? < > | : グループの説明には制限はありません。

NOTE

デフォルトグループにグループを追加することはできません。

グループを構成する方法

グループを追加するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、新しいサブグループを追加するグループを選択します。
3. [クライアント] タブの [タスク] で、[グループの追加] をクリックします。
4. [グループ名のグループを追加] ダイアログボックスで、グループ名と説明を入力します。
5. [OK] をクリックします。

Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート

会社で Active Directory または LDAP サーバーを使ってグループを管理している場合は、グループ構造を つの Symantec Endpoint Protection Manager にインポートできます。その後で、管理コンソールからグループとコンピュータを管理できます。

「[既存のグループとコンピュータのインポート](#)」は、グループ構造を管理する前に、グループ構造をインポートするのに必要なタスクについて説明しています。

Table 59: 既存のグループとコンピュータのインポート

手順	説明
ステップ 1: 会社のディレクトリサーバーに つの Symantec Endpoint Protection Manager を接続する	つの Symantec Endpoint Protection Manager は、Active Directory または LDAP 対応のサーバーに接続できます。サーバーを追加するときに、同期を有効化してください。 ディレクトリサーバーからの組織単位のインポートについて ディレクトリサーバーへの つの Symantec Endpoint Protection Manager の接続複製されたサイトのディレクトリサーバーへの接続
ステップ 2: 組織単位全体、またはコンテナをインポートする	Active Directory または LDAP の既存のグループ構造を つの Symantec Endpoint Protection Manager にインポートできます。また、インポートされたグループ構造の個別のアカウントを、既存の つの Symantec Endpoint Protection Manager グループ構造にコピーすることもできます。 ディレクトリサーバーからの組織単位のインポート Symantec Endpoint Protection 12.1.x の場合、つの Symantec Endpoint Protection Manager のグループ構造を使い、ディレクトリサーバーは使わない場合は、個々のアカウントをインポートします。 「ディレクトリサーバーからの特定のアカウントの検索とインポート」を参照してください。
ステップ 3: インポートされたコンピュータアカウントまたはユーザーアカウントをそれらのグループ内に維持するか、またはインポートされたアカウントを既存のグループにコピーする	組織単位をインポートした後で、次のいずれかの操作を実行できます。 • インポートされた組織単位またはアカウントをそのグループ内に維持します。組織単位または個々のアカウントをインポートした後で、組織単位またはグループにポリシーを割り当てます。 • インポートされたアカウントを既存の つの Symantec Endpoint Protection Manager グループにコピーします。コピーされたアカウントは、インポートされた組織単位ではなく、つの Symantec Endpoint Protection Manager グループのポリシーに従います。 グループの追加 グループまたは場所へのポリシーの割り当て セキュリティポリシーの種類
ステップ 4: 管理者アカウントの認証方法を変更する (任意)	つの Symantec Endpoint Protection Manager で追加した管理者アカウント用の認証方法を変更して、デフォルトの つの Symantec Endpoint Protection Manager 認証ではなく、ディレクトリサーバー認証を使うようにします。インポートしたアカウントを認証するのに、管理者アカウントを使用できます。管理者が つの Symantec Endpoint Protection Manager にログインするときに、管理サーバーは、ユーザー名をデータベースで、パスワードをディレクトリサーバーで検索します。 管理者アカウントの認証方法の選択 ディレクトリサーバーに対する認証の確認

ディレクトリサーバーからの組織単位のインポートについて

Microsoft Active Directory と LDAP サーバーでは、組織単位を使ってコンピュータとユーザーのアカウントを管理します。つの Symantec Endpoint Protection Manager に組織単位とそのアカウントデータをインポートし、管理コンソールでそのアカウントデータを管理できます。つの Symantec Endpoint Protection Manager は組織単位をグループとして扱うため、組織単位グループにセキュリティポリシーを割り当てることができます。

また、アカウントをコピーすることによって、組織単位から つの Symantec Endpoint Protection Manager にアカウントを移動することもできます。この場合、同じアカウントが つの Symantec Endpoint Protection Manager グループと組織単位の両方に存在することになります。つの Symantec Endpoint Protection Manager グループの方が組織単位より優先度が高いため、コピーされたアカウントは つの Symantec Endpoint Protection Manager グループのポリシーを採用します。

つの Symantec Endpoint Protection Manager グループにコピーしたアカウントをディレクトリサーバーから削除しても、そのアカウント名は つの Symantec Endpoint Protection Manager グループに維持されます。管理サーバーからアカウントを手動で削除する必要があります。

組織単位内のアカウントデータを修正する必要がある場合は、ディレクトリサーバー上でこの作業を実行します。つの Symantec Endpoint Protection Manager では実行しません。たとえば、管理サーバーから組織単位を削除しても、その組織単位がディレクトリサーバーから永久に削除されることはありません。つの Symantec Endpoint Protection Manager と Active Directory サーバーを同期して、これらの変更が つの Symantec Endpoint Protection Manager で自動的に更新されるようにする必要があります。ディレクトリサーバーへの接続を設定するときに、同期を有効にします。

NOTE

同期は Active Directory サーバーのみで可能です。Symantec Endpoint Protection は LDAP サーバーとの同期をサポートしません。

また、組織単位全体をインポートするのではなく、選択したユーザーを つの Symantec Endpoint Protection Manager グループにインポートすることもできます。

[ディレクトリサーバーへの つの Symantec Endpoint Protection Manager の接続](#)

[Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート](#)

[ディレクトリサーバーからの組織単位のインポート](#)

ディレクトリサーバーへの つの Symantec Endpoint Protection Manager の接続

コンピュータアカウントまたはユーザーアカウントが含まれる組織単位をインポートする前に、まず つの Symantec Endpoint Protection Manager を会社のディレクトリサーバーに接続する必要があります。

組織単位内のアカウントを管理サーバーで変更することはできません。ディレクトリサーバーでのみ変更できます。ただし、Active Directory サーバーと管理サーバー間でアカウントデータを同期できます。Active Directory サーバーで加えた変更は つの Symantec Endpoint Protection Manager で自動的に更新されます。Active Directory サーバー上で行った変更は管理サーバーにインポートされた組織単位にはすぐに反映されません。遅延時間は同期頻度によって異なります。接続を設定するときに、同期を有効化し、同期頻度を設定します。

つの Symantec Endpoint Protection Manager からディレクトリサーバー接続を削除する場合は、インポートした、その接続と関連付けられた組織単位をすべて削除する必要があります。その後でサーバー間でデータを同期できます。

NOTE

同期は Active Directory サーバーのみで可能です。Symantec Endpoint Protection は LDAP サーバーとの同期をサポートしません。

つの Symantec Endpoint Protection Manager をディレクトリサーバーに接続するには

-
1. コンソールで、[管理] > [サーバー] の順に選択します。
 2. [サーバー] と [ローカルサイト] で、管理サーバーを選択します。
 3. [タスク] の下で、[サーバーのプロパティを編集する] をクリックします。
 4. [サーバープロパティ] ダイアログボックスの [ディレクトリサーバー] タブで、[追加] をクリックします。
 5. [ディレクトリサーバーの追加] ダイアログボックスで、ディレクトリサーバーの名前を入力します。
 6. [Active Directory] または [LDAP] にチェックマークを付け、IP アドレス、ホスト名、またはドメイン名を入力します。
LDAP サーバーを追加する場合、デフォルト値と異なる LDAP サーバーのポート番号を使う場合は、ポート番号を変更します。
 7. 暗号化接続が必要な場合は、[信頼できる接続を使う] にチェックマークを付けます。
 8. [OK] をクリックします。
 9. [ディレクトリサーバー] タブで [ディレクトリサーバーと同期] にチェックマークを付け、[スケジュール] で同期スケジュールを設定します。
 10. [OK] をクリックします。

ディレクトリサーバーからの組織単位のインポート

複製されたサイトのディレクトリサーバーへの接続

複製された Active Directory または LDAP サーバーを使用するサイトでは、一次ディレクトリサーバーと複製されたサーバーのいずれにも つの Symantec Endpoint Protection Manager を接続できます。一次ディレクトリサーバーの接続が解除されても、管理サーバーと複製されたディレクトリサーバーとの接続は維持されます。

次に、つの Symantec Endpoint Protection Manager では、管理者アカウントを認証し、ローカルサイトと複製されたサイトのすべての Active Directory サーバーで組織単位を同期できます。

サイトと複製の設定

NOTE

同期は Active Directory サーバーのみで可能です。Symantec Endpoint Protection は LDAP サーバーとの同期をサポートしません。

複製されたサイトのディレクトリサーバーに接続するには

1. コンソールで、[管理] > [サーバー] の順に選択します。
2. [サーバー] の下で、管理サーバーを選択します。
3. [タスク] の下で、[サーバーのプロパティを編集する] をクリックします。
4. [サーバープロパティ] ダイアログボックスの [ディレクトリサーバー] タブで、[追加] をクリックします。
5. [ディレクトリサーバーの追加] ダイアログボックスの [複製サーバー] タブで、[追加] をクリックします。
6. [複製サーバーの追加] ダイアログボックスで、ディレクトリサーバーの IP アドレス、ホスト名、またはドメイン名を入力して、[OK] をクリックします。
7. [OK] をクリックします。
8. [OK] をクリックします。

ディレクトリサーバーへの つの Symantec Endpoint Protection Manager の接続

ディレクトリサーバーからの組織単位のインポート

Active Directory または LDAP サーバーからコンピュータアカウントまたはユーザーアカウントをインポートするときには、これらのアカウントを組織単位としてインポートします。その後で、組織単位にセキュリティポリシーを適用できます。また、既存の 1 つの Symantec Endpoint Protection Manager グループにこれらのアカウントをコピーすることもできます。

組織単位は [My Company] グループまたは作成したグループのサブグループとしてインポートできますが、[Default Group] としてはインポートできません。組織単位のサブグループとしてグループを作成することはできません。複数の 1 つの Symantec Endpoint Protection Manager グループに組織単位を配置することはできません。

1 つの組織単位またはコンテナ内のすべてのアカウントを 1 つの Symantec Endpoint Protection Manager に追加するのではない場合でも、インポートする必要があります。インポートが完了したら、管理対象のアカウントを既存のクライアントグループにコピーします。

ただし、Symantec Endpoint Protection 12.1.x の場合は、特定のアカウントを選択してインポートできます。

「[ディレクトリサーバーからの特定のアカウントの検索とインポート](#)」を参照してください。

NOTE

1 つの Symantec Endpoint Protection Manager に組織単位をインポートする前に、コンピュータ名またはユーザー名に先行する特殊文字のいくつかを変換する必要があります。このタスクはディレクトリサーバーで行います。特殊文字を変換しないと、管理サーバーはこれらのアカウントをインポートしません。

次の特殊文字を変換する必要があります。

- エントリの最初にある空白または番号記号 (#)。
- エントリの最後にある空白文字。
- カンマ (,)、プラス記号 (+)、二重引用符 (")、不等号 (< または >)、等号 (=)、セミコロン (;)、円記号 (\)。

これらの文字を含む名前をインポートできるようにするには、各文字の前に円記号 (\) を挿入します。

組織単位をディレクトリサーバーからインポートするには

1. 1 つの Symantec Endpoint Protection Manager をディレクトリサーバーに接続します。

[ディレクトリサーバーへの 1 つの Symantec Endpoint Protection Manager の接続](#)

2. コンソールで [クライアント] をクリックし、[クライアント] で、組織単位を追加するグループを選択します。
3. [タスク] で、[組織単位またはコンテナのインポート] をクリックします。
4. [ドメイン] ドロップダウンリストで、手順「[ディレクトリサーバーへの 1 つの Symantec Endpoint Protection Manager の接続](#)」で作成したディレクトリサーバー名を選択します。
5. ドメインまたはサブグループを選択します。
6. [OK] をクリックします。

[Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート](#)

[ディレクトリサーバーからの組織単位のインポートについて](#)

グループの継承の無効化

グループ構造において、サブグループは、その親グループから場所、ポリシー、設定を最初に自動的に継承します。デフォルトでは、すべてのグループに対して継承が有効になっています。サブグループに別のセキュリティのオプションを設定できるように継承を無効にできます。変更後に継承を有効にした場合は、サブグループの設定に加えた変更内容はすべて上書きされます。

クラウドから適用されるポリシーの場合は、つの Symantec Endpoint Protection Manager のポリシー継承設定に従いません。その代わりに、クラウドで設定されている継承ルールに従います。

クライアントのグループの管理

グループの継承を無効にするには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、継承を無効または有効にするグループを選択します。

最上位のグループ、My Company を除くグループを選択できます。

3. グループ名ペインの [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

グループへのクライアントコンピュータ追加の遮断

グループの所属がすでに定義されているクライアントインストールパッケージを設定できます。パッケージのグループを定義した場合、クライアントコンピュータは自動的に適切なグループに追加されます。クライアントは初めて管理サーバーに接続するときに、グループに追加されます。

クライアントインストールパッケージの管理

クライアントがネットワークに接続するときに、特定のグループに自動的に追加されることを望まない場合は、クライアントを遮断できます。新しいクライアントが、クライアントインストールパッケージで割り当てられているグループに追加されるのを防ぐことができます。この場合、クライアントはデフォルトグループに追加されます。コンピュータを、遮断されたグループに手動で移動できます。

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] でグループを右クリックし、[プロパティ] をクリックします。
3. [詳細] タブの [タスク] で、[グループプロパティの編集] をクリックします。
4. [グループ名のグループのプロパティ] ダイアログボックスで、[新しいクライアントの遮断] をクリックします。
5. [OK] をクリックします。

別のグループへのクライアントコンピュータの移動

別のグループへのクライアントコンピュータの移動

クライアントコンピュータが正しいグループにない場合、別のグループに移動できます。

複数のグループから 1 つのグループにクライアントを移動するには、クライアントインストールパッケージを再配備します。

[通信の更新パッケージの配備] を使ったクライアントサーバー通信の復元

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページで、グループを選択します。
3. [クライアント] タブの選択したグループで、コンピュータを選択し、[移動] を右クリックします。

複数のコンピュータを選択するには、Shift キーまたは Ctrl キーを使います。

4. [クライアントの移動] ダイアログボックスで、新しいグループを選択します。
5. [OK] をクリックします。

クライアントのグループの管理

クライアントコンピュータの管理

Table 60: クライアントコンピュータを管理するタスク

タスク	説明
クライアントソフトウェアがコンピュータにインストールされていることを確認する	- 各グループ内でクライアントソフトウェアがまだインストールされていないコンピュータを表示できます。 クライアントソフトウェアをインストールしていないクライアントの検索 - 他のデバイスにクライアントソフトウェアがインストールされていないことを検出するように、クライアントコンピュータを設定できます。このようなデバイスには、保護されていないコンピュータが含まれる場合があります。検出した後は、クライアントソフトウェアをそのコンピュータにインストールできます。 管理外デバイスを検出するためのクライアントの設定 - クライアントをグループに追加し、後でクライアントソフトウェアをインストールできます。 クライアント配備ウィザードを使ったクライアントのインストール方法の選択
クライアントが管理サーバーに接続されているかどうかを確認する	管理コンソールとクライアントでクライアントのステータスアイコンを確認できます。状態アイコンはクライアントとサーバーが通信しているかどうかを示します。 クライアントが管理サーバーに接続され、保護されているかどうかの確認 Symantec Endpoint Protection クライアントの状態アイコン コンピュータにクライアントがインストールされている場合がありますが、それは管理外クライアントです。管理外クライアントは管理できません。代わりに、管理外クライアントを管理下クライアントに変換できます。 クライアントコンピュータと管理サーバーの通信方法
クライアントとサーバー間の接続を設定する	クライアントソフトウェアをインストールした後、クライアントコンピュータは次のハートビートのときに管理サーバーに自動的に接続します。サーバーがクライアントコンピュータとどのように通信するかを変更できます。 クライアントとサーバー間の接続の管理 接続の問題がある場合は、トラブルシューティングできます。 Symantec Endpoint Protection Manager とコンソールまたはデータベースの間における通信の問題のトラブルシューティング
クライアントコンピュータの保護レベルが適切であることを確認する	- クライアントコンピュータでの各保護技術の状態を表示できます。 クライアントコンピュータの保護状態の表示 クライアントが管理サーバーに接続され、保護されているかどうかの確認 - レポートを実行するか、ログを表示して、保護の強化またはパフォーマンスの改善が必要かどうかを判断します。たとえば、スキャンで誤認が起きることがあります。保護の必要なクライアントコンピュータを識別することもできます。 エンドポイント保護の監視 - クライアントソフトウェアまたはクライアントコンピュータの特定の属性に基づいて、保護を修正できます。 クライアントコンピュータについての情報の検索
クライアントコンピュータでの保護を調整する	クライアントの保護レベルが適切でない場合は、保護設定を調節できます。 - レポートとログの結果に基づいて、各種類の保護を強化または緩和できます。 セキュリティポリシーの種類 Symantec Endpoint Protection 技術でコンピュータが保護される仕組み - クライアントでパスワードを要求することができます。 Symantec Endpoint Protection クライアントのパスワード保護

タスク	説明
グループ間でエンドポイントを移動し、保護を変更する（省略可能）	クライアントコンピュータの保護レベルを変更するには、より保護の厳しい、または緩いグループにコンピュータを移動できます。 別のグループへのクライアントコンピュータの移動 クライアントインストールパッケージを配備するときに、クライアントがどのグループに所属するかを指定します。別のグループにクライアントを移動できます。しかし、クライアントが削除または切断された後に再追加や再接続が行われると、クライアントは元のグループに戻ります。クライアントが最後に移動されたグループを維持する場合は、再接続の環境設定を設定してください。[クライアント] > [ポリシー] タブの [通信の設定] ダイアログボックスで、これらの設定を構成します。 <group_name> の通信設定
ユーザーがコンピュータの保護を制御できるかどうかを決定する（省略可能）	クライアントコンピュータでの保護についてユーザーが可能な制御の種類を指定できます。 • [ウィルスとスパイウェアの対策]、[プロアクティブ脅威防止]、[メモリエクスプロイト緩和機能] については、ポリシー内でチェックボックスのチェックマークを付けたりはずしたりして、ユーザーが個別の設定を変更できるかどうかを指定できます。 • ファイアウォールポリシー、IPS ポリシー、一部のクライアントユーザーインターフェースの設定については、ユーザー制御レベルをさらに一般的に変更できます。 クライアントコンピュータの保護をユーザーが無効にできない設定 • ユーザーがクライアントのフルコントロールを必要とする場合は、管理対象外クライアントをインストールできます。 クライアントコンピュータと管理サーバーの通信方法
Symantec Endpoint Protection クライアントソフトウェアを使わなくなったコンピュータから削除する（省略可能）	クライアントコンピュータを使用停止にし、そのライセンスを他のコンピュータのために使う場合は、Symantec Endpoint Protection クライアントソフトウェアをアンインストールします。接続しない管理下クライアントの場合、つの Symantec Endpoint Protection Manager はデフォルトで 30 日後にデータベースからクライアントを削除します。 つの Symantec Endpoint Protection Manager がデータベースからクライアントを削除するまでの期間は変更できます。クライアントを削除すると、データベースの領域を節約することもできます。 Windows 用の Symantec Endpoint Protection クライアントのアンインストール Mac 用の Symantec Endpoint Protection クライアントのアンインストール Symantec Endpoint Protection for Linux クライアントのアンインストール データベースから使われなくなったクライアントをバージして使用可能なライセンスを増やす

クライアントコンピュータの保護状態の表示

ネットワークのクライアントとコンピュータのリアルタイムな操作状態と保護状態についての情報を表示できます。

次のものを表示できます。

- クライアントがインストールされていない管理下クライアントコンピュータのリスト。
コンピュータ名、ドメイン名、ログオンしているユーザー名を表示できます。
- どの保護が有効で、どの保護が無効か。
- どのクライアントコンピュータが最新のポリシーと定義を備えているか。
- グループのポリシーシリアル番号とクライアントのバージョン番号。
- コンピュータが使うネットワークカードの MAC アドレスなど、クライアントコンピュータのネットワークコンポーネントについての情報。
- 利用可能なディスク容量やオペレーティングシステムのバージョン番号など、クライアントコンピュータについてのシステム情報。

特定のクライアントの状態を把握した後、クライアントコンピュータのセキュリティの問題を解決できます。グループに対してコマンドを実行することで、多くの問題を解決できます。たとえば、コンテンツを更新したり、Auto-Protect を有効にしたりできます。

NOTE

Symantec Endpoint Protection の旧バージョンを実行するクライアントを管理する場合、新しい保護技術の一部に [報告していません] と表示される場合があります。これは正常な動作です。これは、これらのクライアントに対して処理を行う必要があることを意味していません。

[クライアントが管理サーバーに接続され、保護されているかどうかの確認](#)

[コンソールを使った、クライアントコンピュータでのコマンドの実行](#)

[クライアントソフトウェアをインストールしていないクライアントの検索](#)

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、情報を取得する対象のクライアントを含むグループを検索します。
3. [クライアント] タブで、[表示] ドロップダウンリストをクリックします。次に、カテゴリを選択します。

右下にあるテキストボックスにページ番号を入力することにより特定のページに直接移動できます。

クライアントコンピュータでの保護の有効化

ご使用のコンピュータで Auto-Protect をはじめとするすべての種類の保護を常に有効にし続ける必要があります。

クライアントでいずれかの保護が無効にされていると、次のようになります。

- [状態] ページの先頭のステータスバーは赤くなります。
- クライアントのアイコンに一般的な禁止記号 (赤の円に斜線) が付きます。クライアントアイコンは、Windows デスクトップの右下のタスクバーに盾の形で表示されます。設定によってアイコンは表示されません。

[Symantec Endpoint Protection クライアントの状態アイコン](#)

管理下クライアントでは、管理者は保護技術をいつでも有効または無効にできます。ユーザーが無効化した保護を、管理者が後で再度有効にする場合があります。また、ユーザーが無効化できないように保護をロックする場合があります。

[状態] ページから保護技術を有効にするには

1. クライアントの [状態] ページの先頭で、[修復] または [すべてを修復] をクリックします。

タスクバーから保護技術を有効にするには

1. Windows デスクトップの通知領域でクライアントアイコンを右クリックして、[Symantec Endpoint Protection を有効にする] をクリックします。

クライアント内から保護技術を有効にするには

1. クライアントで、[状態] ページの [保護の種類] の隣で、[オプション] > [<保護の種類> を有効にする] をクリックします。

ファイアウォールを有効にするには

1. クライアントの [状態] ページの先頭の [ネットワークとホスト悪用防止の設定] の隣で、[オプション]、[設定の変更] の順にクリックします。
2. [ファイアウォール] タブで、[ファイアウォールを有効にする] のチェックマークを付けます。
3. [OK] をクリックします。

クライアントソフトウェアをインストールしていないクライアントの検索

次の基準に基づいてグループ内のクライアントを検索できます。

-
- クライアントソフトウェアはインストールされます。
 - Windows、Mac、Linux のどのコンピュータでクライアントを実行しているか。
 - Windows クライアントがコンピュータモードかまたはユーザーモードか。
 - 仮想デスクトップインフラストラクチャのクライアントは、非永続的でオフラインです。

クライアントコンピュータの保護状態の表示

クライアントが管理サーバーに接続され、保護されているかどうかの確認

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ペインで、検索するグループを選択します。
3. [クライアント] タブの [タスク] で、[表示フィルタの設定] をクリックします。
4. [表示フィルタの設定] ダイアログボックスで、[新しいユーザー、または、まだクライアントソフトウェアがインストールされていない作成済みのコンピュータ] にチェックマークを付けます。
5. [OK] をクリックします。

クライアントコンピュータについての情報の検索

ネットワークのセキュリティについて情報に基づく決定を行うためにクライアント、クライアントコンピュータ、ユーザーについての情報を検索できます。

たとえば、Sales グループのどのコンピュータが最新のオペレーティングシステムを実行しているかを見つけることができます。財務グループのどのクライアントコンピュータが最新のウイルス定義をインストールする必要があるかを調べることができます。

NOTE

ユーザーに関する情報を最大限に検索するには、クライアントソフトウェアのインストール時またはそれ以降にユーザー情報を収集する必要があります。このユーザー情報は、クライアントの [プロパティの編集] ダイアログボックスの [全般] タブと [ユーザー情報] タブにも表示されます。

ユーザー情報の収集

1. コンソールで、[クライアント] をクリックします。
2. [タスク] で、[クライアントの検索] をクリックします。
3. [クライアントの検索] ダイアログボックスの [検索] ドロップダウンリストで、[コンピュータ] または [ユーザー] をクリックします。
4. Default Group 以外のグループを選択するには [参照] をクリックします。クリックしてグループを選択してから [OK] をクリックします。
5. [検索基準] で [検索フィールド] をクリックしてドロップダウンリストを表示し、検索に使う基準を選択します。

埋め込みクライアントを見つけるには、使用中の書き込みフィルタの種類を検索します。[拡張書き込みフィルタ]、[ファイルベースの書き込みフィルタ]、[統一書き込みフィルタ] のいずれかをクリックしてフィルタをインストールしているか、フィルタが有効になっているか、またはその両方を調べます。縮小サイズのクライアントを検索することもできます。[縮小サイズ] の値を検索するには [インストールの種類] をクリックします。
6. [比較演算子] ドロップダウンリストをクリックしてから、比較演算子を選択します。

検索基準では、標準ブール演算子を使えます。これらのオプションに関する詳細が必要な場合、[ヘルプ] をクリックします。
7. [値] セルに検索文字列を入力します。
8. [検索] をクリックします。

テキストファイルに結果をエクスポートできます。

9. [閉じる] をクリックします。

テキストファイルにクエリーに含まれているデータをエクスポートできます。

クライアントコンピュータの保護状態の表示

クライアントコンピュータで実行できるコマンドについて

コンソールから、個々のクライアントまたはグループ全体に対して、コマンドをリモートで実行できます。

コマンドの結果を確認するには、[監視] ページ、[ログ]、[コマンドの状態] の順にクリックします。一部のコマンドを [種類] ドロップダウンリストから実行することもできます。

システム管理者とドメイン管理者は、これらのコマンドを自動的に実行できます。限定管理者に対しては、各コマンドへのアクセスを個別に有効または無効にします。

管理者アカウントの追加とアクセス権の設定

コンソールを使った、クライアントコンピュータでのコマンドの実行

Table 61: クライアントコンピュータで実行できるコマンド

コマンド	説明
分析 (14.3 で削除)	以前のリリースでは、分析コマンドによって、分析のためにクラウドコンソールから Content Analysis System (CAS) に送信したすべての要求の進行状況が表示されていました。
侵入の痕跡スキャンをキャンセル	サードパーティのリモート監視および管理で使用するスキャンを開始またはキャンセルします。
スキャン	クライアントコンピュータでオンデマンドスキャンを実行します。 スキャンコマンドを実行し、カスタムスキャンを選択すると、スキャンでは [管理者定義のスキャン] ページで管理者が設定したコマンドスキャン設定が使われます。このコマンドでは、選択したクライアントコンピュータに適用されるウイルスとスパイウェアの対策ポリシーの設定が使われます。 クライアントコンピュータでのオンデマンドスキャンの実行 Note: Mac クライアントコンピュータではカスタムスキャンのみ実行できます。
コンテンツの更新	クライアントコンピュータで LiveUpdate セッションを開始してクライアントのコンテンツを更新します。クライアントは Symantec LiveUpdate から最新のコンテンツを受信します。 LiveUpdate から 7 の Symantec Endpoint Protection Manager へのコンテンツのダウンロード
コンテンツの更新とスキャン	LiveUpdate セッションを開始してコンテンツを更新し、クライアントコンピュータでオンデマンドスキャンを実行します。
Power Eraser 分析の開始	選択したコンピュータで Power Eraser 分析を実行します。通常、Power Eraser は 1 台のコンピュータか、少数のコンピュータにのみ実行します。Power Eraser は、コンピュータが不安定か、問題が解消されないときにのみ実行します。他のスキャンとは異なり、Power Eraser の場合、潜在的な脅威が自動修復されることはありません。ログで検出を見直し、削除またはそのままにするリスクを指定する必要があります。 Note: Mac と Linux のクライアントコンピュータではこのコマンドは処理されません。 7 の Symantec Endpoint Protection Manager からの Power Eraser の分析の開始 ;

コマンド	説明
クライアントコンピュータの再起動	クライアントコンピュータを再起動します。 ユーザーがクライアントにログオンすると、管理者がそのクライアントに対して設定した再起動オプションに基づいて、警告が表示されます。[全般の設定] ページで、クライアントの再起動オプションを設定できます。 Note: 再起動オプションは Windows クライアントコンピュータのみに適用されます。Mac クライアントコンピュータは常にハード要求を実行します。Linux クライアントコンピュータはこのコマンドを無視します。 つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動 Note: Windows クライアントが再起動しないようにできます。管理者が再起動コマンドを発行しても再起動しないようにするレジストリキーをクライアントに追加できます。 Note: クライアントが再起動しないようにする設定
Auto-Protect を有効にする	クライアントコンピュータのファイルシステムに対して自動保護を有効にします。 デフォルトでは、ファイルシステムに対する自動保護は有効になっています。シマンテック社は Auto-Protect を常に有効のままにすることを推奨します。設定をロックしてクライアントコンピュータのユーザーが Auto-Protect を無効にできないようにすることができます。 Windows クライアントの Auto-Protect のカスタマイズ Mac クライアントの Auto-Protect のカスタマイズ 電子メールの Auto-Protect が無効になっている場合は、ウイルス対策とスパイウェア対策のポリシーで有効にします。
ネットワーク脅威防止を有効にするとネットワーク脅威防止を無効にする	クライアントコンピュータでファイアウォールを有効または無効にし、侵入防止を有効にします。 Note: Linux クライアントコンピュータではこのコマンドは処理されません。 ファイアウォール保護の管理
ダウンロードインサイトを有効にするとダウンロードインサイトを無効にする	クライアントコンピュータのダウンロードインサイトを有効または無効にします。 Note: Mac と Linux のクライアントコンピュータではこのコマンドは処理されません。 ダウンロードインサイト検出の管理
検疫から削除	検疫からすべてのファイルを削除します。このコマンドは、[リスク] ログ > [処理] ドロップダウンリストにのみ表示されます。 Symantec Endpoint Protection Manager から検疫項目を削除する方法
[ファイルフィンガープリントリストの収集]	選択されたクライアントから編集不可のファイルフィンガープリントリストを生成します。収集されたフィンガープリントリストは、[ポリシー] ページの [ポリシーコンポーネント] > [ファイルフィンガープリントリスト] に表示されます。通常、このコマンドは単一のコンピュータまたはコンピュータの小さなグループに対して実行します。複数のコンピュータを選択すると、コマンドは各コンピュータに対して個別のリストを収集します。 Note: Mac と Linux のクライアントコンピュータではこのコマンドは処理されません。
[クライアントを検疫に入れる] と [クライアントを検疫から削除]	クライアントを検疫に追加したり、検疫からクライアントを削除したりできます。これらのコマンドは、ディセプションを有効にしているときのみ使用できます。
シマンテック社にログを送信	予想外のクラッシュや動作が発生する Windows クライアントコンピュータについての情報を収集します。テクニカルサポートに連絡すると、クラッシュしたクライアントのイベント ID を求められるので、このコマンドを実行します。 イベント ID を見つけるには、[監視]、[コマンドの状態]、[詳細] の順にクリックします。 所属する会社に制限的なデータ保護ポリシーがある場合は、このコマンドを使わないようにします。 クラッシュしたクライアントに関する情報をシマンテック社に送信することを管理サーバーで有効にする

[プラットフォームに基づく Symantec Endpoint Protection の機能 \(12.1.x から 14.x \)](#)

コンソールからクライアントコンピュータにコマンドを実行する

スキャンの開始やキャンセルなどのコマンドを、クライアントコンピュータで任意のタイミングで手動により実行できます。管理下クライアントでは、管理サーバーから実行するコマンドがユーザーが実行するコマンドより優先されます。クライアントコンピュータ上でコマンドが処理される順序は、コマンドごとに異なります。コマンドが開始される場所に関係なく、コマンドは同じ方法で処理されます。

クライアントコンピュータで実行できるコマンドについて

以下のコマンドは、次の場所から実行します。

- [クライアント] ページ。
- [コンピュータ状態] ログ。[すべてのスキャンを中止] と [Power Eraser 分析の開始] のコマンドは、[コンピュータの状態] ログからのみ実行できます。
- [リスク] ログ。[検疫から削除する] コマンドは、[リスク] ログからのみ実行できます。

[Symantec Endpoint Protection Manager から検疫項目を削除する方法](#)

開始したスキャンは、即座にキャンセルすることもできます。

1. [クライアント] ページからクライアントコンピュータにコマンドを実行するには、コンソールで [クライアント] をクリックします。
2. グループまたはコンピュータに対して、次のいずれかの操作を実行します。
 - 左ペインでグループを右クリックして、[グループでコマンドを実行] > <コマンド> をクリックします。
 - [クライアント] タブでコンピュータを右クリックして、[コンピュータでコマンドを実行] > <コマンド> をクリックします。
3. メッセージが表示されたら、[はい] をクリックします。
4. コンピュータ状態ログからコマンドを実行するには、[監視] > [ログ] > [コンピュータの状態] ログの種類をクリックし、[ログの表示] をクリックします。
5. [コマンド] リストボックスからコマンドを選択し、コンピュータを選択し、[開始] をクリックします。

NOTE

進行中の定時スキャンや、自分で開始したスキャンを、コマンドリストから [すべてのスキャンを中止] をクリックしてキャンセルすることができます。

6. [監視] をクリックします。
7. [コマンドの状態] タブのリストでコマンドを選択し、[詳細] をクリックします。

NOTE

進行中のスキャンは、スキャンコマンドの [コマンド] 列の [スキャンの中止] アイコンをクリックして中止することもできます。

クライアントが再起動しないようにする設定

次の手順を使って、Symantec Endpoint Protection クライアントコンピュータが再起動しないようにすることができます。たとえば、Symantec Endpoint Protection クライアントを実行するサーバーでこの値を設定できます。このレジストリキーを設定すると、管理者がコンソールからグループに対して Restart コンピュータコマンドを発行した場合に、サーバーは再起動しません。

クライアントが再起動しないようにするには

1. クライアントコンピュータで、レジストリエディタを開きます。
2. HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC に移動します。
3. レジストリに次の行を追加します。

DisableRebootCommand REG_DWORD 1

Windows クライアントのユーザーモードとコンピュータモードの切り替え

グループに属するクライアントにポリシーを適用する方法に基づいて、ユーザーモードまたはコンピュータモードで Windows クライアントを追加します。ユーザーやコンピュータをグループに追加すると、グループに割り当てられているポリシーが使われます。

クライアントを追加するときは、ユーザーモードに優先するコンピュータモードにデフォルトで設定されます。シマンテック社はコンピュータモードを使うことを推奨します。Linux クライアントと Mac クライアントには、コンピュータモードのみがインストールされます。

モード	説明
コンピュータモード	クライアントコンピュータは、そのコンピュータがメンバーになっているグループからポリシーを取得します。コンピュータにログオンしているユーザーに関係なく、クライアントは同じポリシーを使ってコンピュータを保護します。ポリシーは、コンピュータが所属するグループに従います。コンピュータモードがデフォルトの設定です。多くの組織はクライアントの大半をコンピュータモードで設定します。ネットワーク環境に基づいて、特別な必要条件を持つ少数のクライアントをユーザーとして設定したいことがあります。 コンピュータ名が別のグループにすでに含まれている場合、ユーザーモードからコンピュータモードに切り替えることはできません。コンピュータモードへの切り替えにより、クライアントのユーザー名がグループから削除され、クライアントのコンピュータ名がグループに追加されます。 コンピュータモードで追加するクライアントは管理外検出として有効にでき、権限がないデバイスを検出するために使うことができます。 管理外デバイスを検出するためのクライアントの設定
ユーザーモード	クライアントコンピュータは、ユーザーがメンバーになっているグループからポリシーを取得します。クライアントにログオンしているユーザーに応じて、ポリシーが変更されます。ポリシーがユーザーに従います。 既存のグループ構造を Microsoft Active Directory または LDAP ディレクトリサーバーから 1 つの Symantec Endpoint Protection Manager にインポートして、ユーザー別にクライアントを組織化する場合は、ユーザーモードを使います。 ユーザーのログオン名とコンピュータ名がグループにすでに含まれている場合はコンピュータモードからユーザーモードに切り替えることはできません。ユーザーモードへの切り替えにより、クライアントのコンピュータ名がグループから削除されます。次に、クライアントのユーザー名がグループに追加されます。 Active Directory または LDAP サーバーからの既存のグループおよびコンピュータのインポート

クライアントインストールパッケージを配備するときに、クライアントがどのグループに所属するかを指定します。そのクライアントをユーザーモードとコンピュータモードのどちらにするかを、後で指定できます。後でクライアントが削除されるかまたは切断され、次に再追加されるかまたは再接続されると、クライアントは元のグループに戻ります。ただし、クライアントを、それがユーザーモードかコンピュータモードで最後に移動されたグループにとどまるように設定できます。たとえば、新しいユーザーが、ユーザーモードで設定されたクライアントにログオンする可能性があります。クライアントは前のユーザーのグループにとどまります。

[クライアント] > [ポリシー] > [通信の設定] の順にクリックし、これらの設定を行います。

<group_name> の通信設定

Windows クライアントのユーザーモードとコンピュータモードを切り替えるには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、ユーザーまたはコンピュータが含まれるグループを選択します。
3. [クライアント] タブで、表内のコンピュータ名またはユーザー名を右クリックし、[コンピュータモードに切り替え] または [ユーザーモードに切り替え] を選択します。

このモードはトグルで切り替わる設定なので、常にどちらかが表示されます。表に表示される情報は、新しい設定を反映して変わります。

管理外デバイスを検出するためのクライアントの設定

権限がないデバイスは会議室での物理アクセスや不正な無線アクセスポイントなどの多くの方法でネットワークに接続できます。すべてのエンドポイントにポリシーを強制するには、ネットワーク上での新しいデバイスの存在をすばやく検出する必要があります。デバイスが安全であるかどうかを判断する必要があります。不明なデバイスを検出するように管理外検出としてクライアントを有効にすることができます。不明なデバイスは、Symantec Endpoint Protection クライアントソフトウェアを実行しない、管理外デバイスです。管理外デバイスがコンピュータである場合は、Symantec Endpoint Protection クライアントソフトウェアをそれにインストールできます。

デバイスが開始するとき、オペレーティングシステムは他のコンピュータにデバイスの存在を知らせるように次のトラフィックをネットワークに送信します。

- アドレス解決プロトコル (ARP) トラフィック (ICMPv4)
 - Neighbor Discovery Protocol (NDP) トラフィック (ICMPv6)
- ICMPv6 はバージョン 14.2 以降でサポートされます。

管理外検出として有効になっているクライアントはこのパケットの情報を収集して管理サーバーに送信します。管理サーバーはデバイスの MAC アドレスと IP アドレスのためのパケットを検索します。サーバーはこれらのアドレスをサーバーのデータベースの既存の MAC アドレスと IP アドレスのリストと比較します。サーバーがアドレス一致を見つけることができなければサーバーはそのデバイスを新規として記録します。その後にデバイスが安全であるかどうかを決定できます。クライアントは情報のみを送信するので、追加リソースを使いません。

プリンタなどの特定のデバイスを無視するように、管理外検出を設定できます。管理外検出が不明なデバイスを検出したときに通知するように電子メール通知を設定することもできます。

管理外検出としてクライアントを設定するには、次の処理をする必要があります。

- ネットワーク脅威防止を有効にする
[コンソールを使った、クライアントコンピュータでのコマンドの実行](#)
- クライアントをコンピュータモードに切り替える
[Windows クライアントのユーザーモードとコンピュータモードの切り替え](#)
- 常時稼働のコンピュータにクライアントをインストールする

14.3 RU1 以降、Linux クライアントを管理外検出として有効化することは推奨されていません。

管理外検出の設定を行うには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、管理外検出として有効にするクライアントを含むグループを選択します。
3. [クライアント] タブで、管理外検出として有効にするクライアントを右クリックしてから [管理外検出として有効にする] をクリックします。
4. 1 つ以上のデバイスを管理外検出による検出から除外するように指定するには、[管理外検出の設定] をクリックします。
5. [<クライアント名> の管理外検出例外] ダイアログボックスで、[追加] をクリックします。
6. [管理外検出例外の追加] ダイアログボックスで、次のいずれかのオプションをクリックします。
 - [IP アドレス範囲の検出を除外する] をクリックしてから、複数のデバイスのための IP アドレス範囲を入力します。
 - [MAC アドレスの検出を除外する] をクリックしてから、デバイスの MAC アドレスを入力します。

-
7. [OK] > [OK] をクリックします。
 8. クライアントが検出する権限がないデバイスのリストを表示するには、コンソールで [ホーム] をクリックします。
 9. [ホーム] ページの [セキュリティの状態] セクションで、[詳細情報] をクリックします。
 10. [セキュリティ状態の詳細] ダイアログボックスで、[不明なデバイスのエラー] の表にスクロールします。
 11. ダイアログボックスを閉じます。

管理外クライアントが検出されているかどうかを確認するには

1. [ホーム] ページに移動して、[セキュリティの状態] 領域で [詳細を表示] をクリックします。
2. [セキュリティ状態の詳細] ウィンドウが表示されたら、[不明なデバイスのエラー] をクリックします。
[検出された不明なデバイスの合計数] に、管理外のデバイスの数が表示されます。これには、コンピュータに加えて、アクセスポイント、ルータ、スイッチ、およびその他のデバイスが含まれます。
3. 余分なデバイスをフィルタ処理するには、[クライアント] ページに移動して [管理外の検出] を右クリックします。
4. [管理外検出の設定] をクリックして、フィルタ処理するデバイスの IP アドレスまたは Mac アドレスを追加します。

Symantec Endpoint Protection クライアントのパスワード保護

ユーザーが特定のタスクを実行するときには常に、クライアントコンピュータでパスワード保護を要求することにより、企業のセキュリティを向上できます。

ユーザーが次の操作のいずれかを実行するとき、ユーザーにパスワード入力を要求できます。

- クライアントユーザーインターフェースを開く。
- クライアントサービスを停止します。
- クライアントをアンインストールする。

NOTE

このオプションは、Windows クライアントでのみ動作します。

- クライアント通信設定をインポート、エクスポートします。

ユーザーによるクライアントのユーザーインターフェースの変更を防止、許可

クライアントをパスワード保護するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、パスワード保護を設定するグループを選択します。
3. [ポリシー] タブの [場所に依存しないポリシーと設定] で、[パスワード] をクリックします。

Symantec Endpoint Protection の以前のバージョンでは、オプションの名前が異なる場合がありますが、[ポリシー] タブからクライアントをパスワードで保護できます。

4. [クライアントパスワード設定] ウィンドウで、チェックボックスのいずれかまたはすべてにチェックマークを付けます。

ボックスがグレー表示になっている場合は、このグループは親グループからポリシーを継承します。続行する前に、親グループのポリシーを編集するか、このグループでの継承を無効にする必要があります。

グループの継承の無効化

5. [パスワード] と [パスワードの確認] のテキストボックスに、同じパスワードを入力します。
6 文字から 256 文字までの長さのパスワードを作成できます。

パスワード強度が許容できないというメッセージが表示されたら、パスワードの強度を高めることを検討してください。ただし、パスワードを保存することはできません。

[設定が継承されないサブグループにパスワード設定を適用する] にチェックマークを付けると、親から設定を継承しないすべての子グループのために、パスワード保護の設定を修正できます。この設定は親グループにのみ表示されます。

6. [OK] をクリックします。

ユーザーによるクライアントのユーザーインターフェースの変更を防止、許可

ユーザーはクライアントユーザーインターフェースのどの部分を変更できるのでしょうか。

管理者はユーザー制御レベルを設定して、ユーザーがクライアントに変更を加えることを許可するかどうかを決定できます。たとえば、ユーザーがクライアントユーザーインターフェースや通知領域のアイコンを開けないようにすることができます。管理者がユーザーのために管理するユーザーインターフェース機能は、管理設定と呼ばれます。パスワード保護のように、クライアント機能の一部にはユーザーがアクセスできないものがあります。

Symantec Endpoint Protection クライアントのパスワード保護

ユーザーインターフェースはどのように設定できるのでしょうか。

次のいずれかのタスクを実行して、クライアントのユーザーインターフェースを設定できます。

- クライアントのユーザー制御レベルをサーバー制御に設定する。
- クライアントのユーザー制御レベルを混合制御に設定し、[クライアント/サーバー制御の設定] タブで親機能を [サーバー] に設定する。

たとえば、[通知領域アイコンの表示/非表示] オプションを [クライアント] に設定できます。通知領域アイコンがクライアントに表示され、ユーザーがそのアイコンの表示または非表示を選択できます。[通知領域アイコンの表示/非表示] オプションを [サーバー] に設定した場合は、クライアントに通知領域アイコンを表示するかどうかを選択できます。

NOTE

これらの設定の多くは、Windows クライアントにのみ適用されます。サーバー制御でのみ Mac クライアントのいくつかのオプションを設定できます。

1. 混合制御でユーザーインターフェースを設定するには、[クライアント] > [ポリシー] タブをクリックします。

クライアントコンピュータの保護をユーザーが無効にできない設定

2. [場所名 のクライアントユーザーインターフェース制御の設定] ダイアログボックスで、[混合制御] の横にある [カスタマイズ] をクリックします。
3. [クライアントユーザーインターフェース混合制御の設定] ダイアログボックスの [クライアント/サーバー制御の設定] タブで、次のいずれかの操作を行います。
 - サーバーからのみ設定するオプションをロックします。ロックするオプションについて、[サーバー] をクリックします。
ここで [サーバー] に設定したウイルス対策とスパイウェア対策の設定が、クライアントの設定よりも優先されます。
 - ユーザーがクライアントでオプションを設定できるように、ロックを解除します。クライアントでオプションを設定できるように、[クライアント] をクリックします。クライアントは、ウイルスとスパイウェアの設定を除くすべての設定で、デフォルトで選択されています。
4. [サーバー] に設定した一部のオプションは、[クライアントユーザーインターフェースの設定] タブをクリックして設定します。

[サーバー] に設定した他のオプションをコンソールのどの場所で設定するかについて詳しくは、[ヘルプ] をクリックしてください。たとえば、ファイアウォールの設定を有効にするには、ファイアウォールポリシーで設定します。

ルールの追加ではなくネットワークサービスのための通信の有効化

ネットワーク侵入防止とブラウザ侵入防止の有効化

5. [クライアントユーザーインターフェースの設定] タブで、クライアントで利用可能にするオプションのチェックボックスにチェックマークを付けます。
6. [OK] をクリックします。
7. [OK] をクリックします。
8. サーバー制御でユーザーインターフェースを設定するには、ユーザー制御レベルをサーバー制御に変更します。

クライアントコンピュータの保護をユーザーが無効にできない設定

9. [クライアントユーザーインターフェースの設定] ダイアログボックスで、クライアントに表示するオプションにチェックマークを付けます。
10. [OK] をクリックします。
11. [OK] をクリックします。

混合制御のファイアウォール設定

ユーザー情報の収集

クライアントソフトウェアのインストール処理中またはポリシーの更新中に、クライアントコンピュータのユーザーに自分自身の情報を入力するよう求めることができます。従業員の携帯電話番号、役職名、電子メールアドレスなどの情報を収集できます。収集した情報は、手動で保守と更新を行う必要があります。

NOTE

クライアントコンピュータでメッセージを表示するように初めて設定し、ユーザーが要求された情報を入力した後は、メッセージが再び表示されることはありません。フィールドを編集したり、メッセージを無効にしてから再び有効にした場合でも、クライアントで新しいメッセージは表示されません。ただし、ユーザーはいつでも情報を編集することができ、管理サーバーはその情報を取得します。

クライアントインストールパッケージの管理

ユーザー情報を収集するには

1. コンソールで、[管理]、[インストールパッケージ] の順にクリックします。
2. [インストールパッケージ] ペインで [クライアントインストールパッケージ] をクリックします。
3. [タスク] で、[ユーザー情報収集の設定] をクリックします。
4. [ユーザー情報収集の設定] ダイアログボックスで、[ユーザー情報の収集] にチェックマークを付けます。
5. [ポップアップメッセージ] テキストボックスに、情報を要求するときユーザーに対して表示するメッセージを入力します。
6. ユーザーがユーザー情報の収集を延期できるようにする場合は、[後で通知を有効にする] にチェックマークを付けて、時刻を分単位で設定します。
7. [ユーザーが入力できるように表示するフィールドを選択してください] で、収集する情報の種類を選択して [追加] をクリックします。

Shift キーまたは Ctrl キーを押すと、1つまたは複数のフィールドを同時に選択できます。

8. ユーザーの入力を省略可能にするフィールドの [省略可能] 列のチェックボックスに、チェックマークを付けます。
9. [OK] をクリックします。

リモートクライアントの管理

ネットワークには、異なる場所からネットワークに接続するクライアントが含まれることがあります。これらのクライアントは、ネットワーク内からのみ接続するクライアントとは異なる方法で管理することが必要な場合もあります。常にリモートから VPN に接続するクライアントや、従業員が出張するため複数の場所から接続するクライアントを管理する必要がある例もあります。また、管理者が制御する範囲外にあるコンピュータのセキュリティを管理しなければならない場合があります。たとえば、お客様、受託業者、製造元、ビジネスパートナーにネットワークへの限定的なアクセスを許可します。一部の従業員は自分のパーソナルコンピュータを使ってネットワークに接続することがあるため、これらのクライアントは異なる方法で管理する必要があるでしょう。

これらのどの場合にも、より高い危険度に対処する必要があります。接続やクライアントコンピュータの安全性がより低い場合があったり、制御できる範囲が狭いクライアントが存在する場合があります。ネットワークセキュリティ全体に対するこれらのリスクを最小限にするには、クライアントがネットワークへの接続で使うさまざまな種類のリモートアクセスを評価する必要があります。その後、評価に基づいてより厳しいセキュリティポリシーを適用できます。

ネットワークに接続するクライアントがセキュリティリスクをもたらすため、それらのクライアントを異なる方法で管理するには、Symantec Endpoint Protection の場所の認識を使うことができます。

クライアントの場所に基づいて、ネットワークにより大きいリスクをもたらすクライアントに異なるポリシーを適用します。Symantec Endpoint Protection における場所は、クライアントコンピュータがネットワークに接続するために使う接続の種類として定義されます。場所には、接続が企業ネットワークの内部と外部のどちらに配置されているかについての情報も含まれます。

場所はクライアントのグループに対して定義します。その後で、それぞれの場所に異なるポリシーを割り当てます。一部のセキュリティ設定は場所にかかわらずグループ全体に割り当てることができます。いくつかの設定は、場所に応じて異なります。

Table 62: リモートクライアントの管理

タスク	説明
セキュリティリスクの評価に基づいてグループを設定する	クライアントのグループの管理
リモートクライアントのグループの場所を設定する	リモートクライアントの場所の管理
場所の通信設定を指定する	場所に対する通信の設定
セキュリティポリシーを強化する	リモートクライアントのセキュリティポリシーの強化について
クライアントの通知をオンにする	リモートクライアントの通知の有効化について
クライアントのログ管理設定をカスタマイズする	特に、クライアントが数日間オフラインの場合に、リモートクライアントのログ設定をカスタマイズします。帯域幅と管理サーバーへの負荷を減らすには、次の変更を行ないます。 - クライアントが管理サーバーに自身のログをアップロードしないように設定する。 - クライアントがクライアントのセキュリティログのみをアップロードするように設定する。 - 指定したイベントのみをアップロードするようにログイベントのフィルタ処理を設定する。アップロードが推奨されるイベントには、定義更新や副作用修復エラーなどが含まれます。 - ログの保持時間を長めにする。 保持時間を長めにする、より多くのウイルスとスパイウェアのイベントデータを確認できるようになります。

タスク	説明
リモートクライアントを監視する	管理サーバーからのリモートクライアントの監視について クラウドコンソールからのローミング Symantec Endpoint Protection クライアントの監視

リモートクライアントの場所の管理

管理に必要なグループを設定した後で、場所を追加できます。セキュリティ戦略上必要であれば、グループごとに異なる場所を設定できます。つの Symantec Endpoint Protection Manager コンソールで、場所に基づいて自動ポリシー切り替えをトリガする条件を設定します。場所の認識は、クライアントが満たしている場所条件に基づいて、指定するセキュリティポリシーを自動的にクライアントに適用します。

場所条件にはさまざまな基準を利用できます。たとえば、IP アドレス、ネットワーク接続の種類、クライアントコンピュータが管理サーバーに接続できるかどうか、などを利用できます。クライアント接続は、指定する基準に基づいて許可したり遮断したりできます。

場所は、それを作成したグループと、そのグループを継承するサブグループに適用されます。ベストプラクティスは、どのクライアントでも My Company グループレベルで使うことができる場所を作成することです。その後、サブグループレベルで特定のグループの場所を作成します。

作成するグループと場所が少ないほうが、セキュリティポリシーと設定の管理が簡単になります。ただし、ネットワークの複雑さとセキュリティの必要条件によって、より多くのグループと場所が必要になることがあります。必要となるセキュリティ設定、ログ関連の設定、通信設定、ポリシーの数によって、作成するグループと場所の数が決まります。

一部の設定オプションはリモートクライアント用にカスタマイズできますが、これらは場所に依存しません。これらのオプションは、親グループから継承されるか、単独で設定されます。すべてのリモートクライアントが含まれる 1 つのグループを作成する場合、場所に依存しない設定はグループ内のクライアントの設定と同じになります。

次の設定は場所に依存しません。

- カスタム侵入防止シグネチャ
- システムロックダウンの設定
- ネットワークアプリケーション監視の設定
- LiveUpdate Content policy の設定
- クライアントログの設定
- クライアントサーバー通信の設定
- 場所の認識や改変対策などの、全般的なセキュリティ関連の設定

クライアントログの処理方法など、これらの場所に依存しない設定をカスタマイズするには、別々のグループを作成する必要があります。

一部の設定は場所に固有です。

ベストプラクティスとして、ユーザーが次の保護をオフにすることを許可しないでください。

- Auto-Protect
- SONAR
- 改変対策
- 作成済みのファイアウォールルール

Table 63: 実行できる場所の認識タスク

タスク	説明
場所の計画	使う場所を決定するために環境内で必要なセキュリティポリシーの種類を検討します。それから各場所の定義に使う基準を決定できます。ベストプラクティスは、グループと場所を同時に計画することです。 クライアントのグループの管理 次の情報を参照してください。 ネットワークの検出条件の設定シナリオ 1 ネットワークの検出条件の設定シナリオ 2
場所の認識を有効にする	クライアントの接続元の場所によってクライアントに割り当てられるポリシーを制御するには、場所の認識を有効にします。 クライアントの場所認識の有効化
場所の追加	グループに場所を追加できます。 グループへの場所の追加
デフォルトの場所の割り当て	すべてのグループにデフォルトの場所を設定する必要があります。コンソールをインストールするとき、Default と呼ばれるたった 1 つの場所があります。新しいグループを作成するとき、デフォルトの場所は常に Default です。他の場所を追加した後で、デフォルトの場所を変更できます。 デフォルトの場所は、以下の場合に使用します。 - 複数の場所の 1 つが場所の基準に適合するが、前回の場所が基準に適合していない場合 - 場所の認識を使っている、基準に適合する場所がない場合 - ポリシーで場所または場所の名前が変更され、新しいポリシーを受け取ったときにクライアントがデフォルトの場所に戻る場合 デフォルトの場所の変更
場所の通信オプションの設定	場所ごとに管理サーバーとクライアント間の通信設定を設定することもできます。 場所に対する通信の設定

「[Symantec Endpoint Protection の場所の認識機能に関するベストプラクティス](#)」を参照してください。

リモートクライアントの管理

クライアントの場所認識の有効化

クライアントの接続場所によってクライアントに割り当てられるポリシーを作成するには、クライアントの場所の認識を有効にします。

[前回の場所を記憶する] にチェックマークを付けた場合には、クライアントがネットワークに接続すると、前回使われた場所のポリシーが割り当てられます。場所の認識が有効な場合には、クライアントは数秒後に適切なポリシーに自動的に切り替わります。特定の場所に関連付けられているポリシーによってクライアントのネットワーク接続が決まります。場所の認識が無効な場合には、クライアントがサーバー制御であっても、クライアントは手動で任意の場所に切り替えることができます。検疫場所が有効な場合には、クライアントはしばらくして検疫ポリシーに切り替わる場合があります。

[前回の場所を記憶する] のチェックマークをはずした場合には、クライアントがネットワークに接続すると、デフォルトの場所のポリシーが割り当てられます。クライアントは、前回使った場所に接続できません。場所の認識が有効な場合には、クライアントは数秒後に適切なポリシーに自動的に切り替わります。特定の場所に関連付けられているポリシーによってクライアントのネットワーク接続が決まります。場所の認識が無効な場合には、クライアントがサーバー制御で

あっても、ユーザーは手動で任意の場所に切り替えることができます。検疫場所が有効な場合には、クライアントはしばらくして検疫ポリシーに切り替わる場合があります。

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、場所の自動切り替えを実装するグループを選択します。
3. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。
4. [場所に依存しないポリシーと設定] で、[全般の設定] をクリックします。
5. [全般の設定] ダイアログボックスの [全般の設定] タブの [場所の設定] で、[前回の場所を記憶する] にチェックマークを付けます。

デフォルトでは、このオプションは有効になっています。クライアントは、最初、クライアントがネットワークに前回接続した場所に関連付けられているポリシーに割り当てられます。

6. [場所の認識を有効にする] にチェックマークを付けます。
デフォルトでは場所の認識は有効です。クライアントはユーザーがネットワークに接続しようとしている場所に関連付けられているポリシーに自動的に割り当てられます。
7. [OK] をクリックします。

グループへの場所の追加

グループへの場所の追加

グループに場所を追加するときは、グループ内のクライアントをその場所に切り替える条件を指定します。場所の認識は、その場所に適切なポリシーと設定を適用する場合にのみ有効になります。

グループに場所を追加するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、1 つ以上の場所を追加するグループを選択します。
3. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

場所を追加できるのは、親グループからポリシーを継承していないグループのみです。

[場所の追加] をクリックして [場所の追加] ウィザードを実行することもできます。

4. [クライアント] ページの [タスク] で、[場所の管理] をクリックします。
5. [場所の管理] ダイアログボックスの [場所] で、[追加] をクリックします。
6. [場所の追加] ダイアログボックスで、新しい場所の名前と説明を入力し、[OK] をクリックします。
7. [この場所に切り替えるタイミング] ボックスの右側で、[追加] をクリックします。
8. [種類] リストで条件を選択し、条件の適切な定義を選択します。

クライアントコンピュータが指定された条件を満たしている場合、コンピュータはその条件の場所に切り替わります。

9. [OK] をクリックします。
10. さらに条件を追加するには、[追加] をクリックし、[AND 関係の基準] または [OR 関係の基準] を選択します。
11. [OK] をクリックします。

リモートクライアントのセキュリティポリシーの強化について

デフォルトの場所の変更

つの Symantec Endpoint Protection Manager が最初にインストールされる時には、「デフォルト」という 1 つの場所のみがあります。その時点で、すべてのグループのデフォルトの場所は「デフォルト」です。すべてのグループにデフォルトの場所を設定する必要があります。新しいグループを作成するとき、つの Symantec Endpoint Protection Manager コンソールは自動的にデフォルトの場所を「デフォルト」にします。

他の場所を追加した後にグループのデフォルトの場所にするために別の場所を指定できます。自宅や出張先のような場所をデフォルトの場所に指定することもできます。

グループのデフォルトの場所は、以下の場合に使います。

- 複数の場所の 1 つが場所の基準に適合するが、前回の場所が基準に適合していない場合
- 場所の認識を使っていて、基準に適合する場所がない場合
- ポリシーで場所または場所の名前が変更され、新しいポリシーを受け取ったときにクライアントがデフォルトの場所に戻る場合

デフォルトの場所を変更するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、別のデフォルトの場所を割り当てるグループをクリックします。
3. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。
4. [タスク] で、[場所の管理] をクリックします。
5. [場所の管理] ダイアログボックスの [場所] で、デフォルトの場所として指定する場所を選択します。
6. [説明] で、[競合に備えてこの場所をデフォルトの場所として設定します] にチェックマークを付けます。

グループに別の場所を割り当てるまで、常に「デフォルト」の場所がデフォルトの場所に設定されます。

7. [OK] をクリックします。

リモートクライアントの場所の管理

ネットワーク検出条件の設定シナリオ 1

リモートクライアントがある場合、最も単純なケースでは、My Company グループと 3 つの場所を使う方法が一般的です。これがシナリオ 1 です。

このシナリオでクライアントのセキュリティを管理するため、使う **My Company** グループの下で、次の場所を作成できます。

- オフィスでログオンするオフィスクライアント。
- VPN を介してリモートから企業ネットワークにログオンするリモートクライアント。
- VPN を介さずにリモートからインターネットにログオンするリモートクライアント。

VPN 接続を使っていないリモートの場所は安全性が最も低いため、最も安全なポリシーを設定します。常にこの場所をデフォルトの場所にすることがベストプラクティスです。

NOTE

My Company グループ継承をオフにしてグループを追加した場合、追加したグループは、My Company グループに対して設定した場所を継承しません。

次の提案は、シナリオ 1 のベストプラクティスを表します。

1. オフィス内に置かれたクライアントにオフィスの場所を設定するには、[クライアント] ページで、場所を追加するグループを選択します。
2. [ポリシー] タブの [タスク] で、[場所の追加] をクリックします。
3. [場所の追加ウィザード] で、[次へ] をクリックします。
4. 場所の名前を入力し、必要に応じてその説明を追加して、[次へ] をクリックします。
5. リストボックスで、リストから [クライアントは管理サーバーに接続できます] をクリックして、[次へ] をクリックします。
6. [完了] をクリックして、[OK] をクリックします。
7. [タスク] の下で [場所の管理] をクリックして、作成した場所を選択します。
8. [追加] をクリックして、[AND 関係の基準] をクリックします。
9. [場所の基準を指定します] ダイアログボックスの [種類] リストで、[ネットワーク接続の種類] をクリックします。
10. [下で指定するネットワーク接続の種類をクライアントコンピュータが使わない場合] をクリックします。
11. 下部のリストボックスで、組織で使う VPN クライアントの名前を選択して、[OK] をクリックします。
12. [OK] をクリックして、[場所の管理] ダイアログボックスを終了します。
13. VPN を介してログインしているクライアントのリモートの場所を設定するには、[クライアント] ページで、場所を追加するグループを選択します。
14. [ポリシー] タブの [タスク] で、[場所の追加] をクリックします。
15. [場所の追加ウィザード] で、[次へ] をクリックします。
16. 場所の名前を入力し、必要に応じてその説明を追加して、[次へ] をクリックします。
17. リストボックスで、[ネットワーク接続の種類] をクリックします。
18. [接続の種類] リストボックスで、組織で使う VPN クライアントの名前を選択して、[次へ] をクリックします。
19. [完了] をクリックします。
20. [OK] をクリックします。
21. VPN を介してログオンしていないクライアントにリモートの場所を設定するには、[クライアント] ページで、場所を追加するグループを選択します。
22. [ポリシー] タブの [タスク] で、[場所の追加] をクリックします。
23. [場所の追加ウィザード] で、[次へ] をクリックします。
24. 場所の名前を入力し、必要に応じてその説明を追加して、[次へ] をクリックします。
25. リストボックスで、[特定の条件がありません] のままにして、[次へ] をクリックします。
これらの設定を使うことにより、この場所のポリシー (最も厳密で最も安全なポリシー) がデフォルトの場所ポリシーとして使われます。
26. [完了] をクリックして、[OK] をクリックします。

ネットワークの検出条件の設定シナリオ 2

リモートクライアントの管理

ネットワーク検出条件の設定シナリオ 2

シナリオ 2 では、シナリオ 1 で指定したものと同一 2 つのリモート場所と、2 つのオフィスの場所の合計 4 つの場所を使います。

次のオフィスの場所を追加します。

- イーサネット接続を介してログオンするオフィス内のクライアント。
- 無線接続を介してログオンするオフィス内のクライアント。

この場合、管理は単純化され、すべてのクライアントはデフォルトのサーバー制御モードで管理されます。ユーザーが実行できる操作を細かく制御する場合、経験豊富な管理者は混合制御を使うことができます。混合制御設定では、エンドユーザーはセキュリティ設定をある程度制御できますが、管理者が必要に応じて、エンドユーザーの変更を上書きできます。クライアント制御は、実行できる操作について幅広い自由度をユーザーに提供するため、ネットワークセキュリティに大きいリスクを引き起こします。

シマンテック社は、次の状況でのみクライアント制御を使うことを推奨します。

- ユーザーがコンピュータセキュリティに詳しい場合。
- やむを得ない事情で使う場合。

NOTE

オフィス内で一部のクライアントがイーサネット接続を使い、他のクライアントが無線接続を使う場合があります。このため、オフィス内の無線クライアントの手順で最後の条件を設定します。この条件では、両方の接続が同時に使われているときに、すべての無線トラフィックを遮断するイーサネットの場所ファイアウォールポリシールールを作成できます。

イーサネットを介してログオンするクライアントにオフィスの場所を設定するには

1. [クライアント] ページで、場所を追加するグループを選択します。
2. [タスク] の下で、[場所の追加] をクリックします。
3. [場所の追加ウィザード] で、[次へ] をクリックします。
4. 場所の名前を入力し、必要に応じてその説明を追加して、[次へ] をクリックします。
5. リストボックスで、[クライアントは管理サーバーに接続できます] を選択して、[次へ] をクリックします。
6. [完了] をクリックします。
7. [OK] をクリックします。
8. [タスク] の下で [場所の管理] をクリックして、作成した場所を選択します。
9. [この場所に切り替えるタイミング] の横で、[追加] をクリックしてから、[AND 関係の基準] を選択します。
10. [場所の基準を指定します] ダイアログボックスの [種類] リストで、[ネットワーク接続の種類] をクリックします。
11. [下で指定するネットワーク接続の種類をクライアントコンピュータが使わない場合] をクリックします。
12. 下部のリストボックスで、組織で使う VPN クライアントの名前を選択して、[OK] をクリックします。
13. [追加] をクリックして、[AND 関係の基準] をクリックします。
14. [場所の基準を指定します] ダイアログボックスの [種類] リストで、[ネットワーク接続の種類] をクリックします。
15. [下で指定するネットワーク接続の種類をクライアントコンピュータが使う場合] をクリックします。
16. 下部のリストボックスで、[イーサネット] を選択して [OK] をクリックします。
17. [OK] をクリックして、[場所の管理] ダイアログボックスを終了します。

無線接続を介してログオンするクライアントにオフィスの場所を設定するには

1. [クライアント] ページで、場所を追加するグループを選択します。
2. [タスク] の下で、[場所の追加] をクリックします。
3. [場所の追加ウィザード] で、[次へ] をクリックします。
4. 場所の名前を入力し、必要に応じてその説明を追加して、[次へ] をクリックします。

-
5. リストボックスで、[クライアントは管理サーバーに接続できます] をクリックして、[次へ] をクリックします。
 6. [完了] をクリックします。
 7. [OK] をクリックします。
 8. [タスク] の下で [場所の管理] をクリックして、作成した場所を選択します。
 9. [この場所に切り替えるタイミング] の横で、[追加] をクリックしてから、[AND 関係の基準] をクリックします。
 10. [場所の基準を指定します] ダイアログボックスの [種類] リストで、[ネットワーク接続の種類] をクリックします。
 11. [下で指定するネットワーク接続の種類をクライアントコンピュータが使わない場合] をクリックします。
 12. 下部のリストボックスで、組織で使う VPN クライアントの名前を選択して、[OK] をクリックします。
 13. [追加] をクリックして、[AND 関係の基準] をクリックします。
 14. [場所の基準を指定します] ダイアログボックスの [種類] リストで、[ネットワーク接続の種類] をクリックします。
 15. [下で指定するネットワーク接続の種類をクライアントコンピュータが使わない場合] をクリックします。
 16. 下部のリストボックスで、[イーサネット] をクリックして [OK] をクリックします。
 17. [追加] をクリックして、[AND 関係の基準] をクリックします。
 18. [場所の基準を指定します] ダイアログボックスの [種類] リストで、[ネットワーク接続の種類] をクリックします。
 19. [下で指定するネットワーク接続の種類をクライアントコンピュータが使う場合] をクリックします。
 20. 下部のリストボックスで、[無線] をクリックして [OK] をクリックします。
 21. [OK] をクリックして、[場所の管理] ダイアログボックスを終了します。

ネットワークの検出条件の設定シナリオ 1

リモートクライアントの管理

場所に対する通信の設定

デフォルトでは、グループレベルで管理サーバーとクライアント間の通信設定を行います。ただし、グループ内の個々の場所に対してこれらの設定を行うこともできます。たとえば、クライアントコンピュータが VPN で接続する場所には別の管理サーバーを使うことができます。管理サーバーに同時に接続するクライアントの数を最小にするために、場所ごとに異なるハートビートを指定できます。

場所に対して次の通信設定を設定できます

- クライアントが実行する制御モード
- クライアントが使う管理サーバーリスト
- クライアントが動作するダウンロードモード
- クライアントで実行されるすべてのアプリケーションのリストを収集し、管理サーバーにそのリストを送信するかどうか
- クライアントがダウンロードのために使うハートビート間隔
- 管理サーバーでデフォルトの管理サーバーまたはグループ更新プロバイダからのコンテンツのダウンロードをランダム化するかどうか

NOTE

Mac クライアントの場合は、これらの設定の一部のみを設定できます。

場所に対する通信設定を設定するには

-
1. コンソールで、[クライアント] をクリックします。
 2. [クライアント] ページで、グループを選択します。
 3. [ポリシー] タブの [場所固有のポリシーと設定] で、場所の下の [場所固有の設定] を展開します。
 4. [通信の設定] の右側で、[タスク] をクリックし、[グループ通信設定を使う] のチェックマークをはずします。
 5. [タスク] を再びクリックし、[設定の編集] をクリックします。
 6. [場所名の通信設定] ダイアログボックスで、指定した場所専用の設定を変更します。
 7. [OK] をクリックします。

[プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新](#)

[リモートクライアントの場所の管理](#)

[クライアントのグループの管理](#)

リモートクライアントのセキュリティポリシーの強化について

リモートユーザーを管理する場合、基本的に次のどちらかの方針を採ります。

- リモートユーザーによるそれぞれのコンピュータの使用を妨げないように、デフォルトのポリシーをそのまま使う。
- リモートユーザーが行える操作を制限することになっても、デフォルトセキュリティポリシーを強化してネットワークの保護を高める。

ほとんどの状況で、リモートクライアントのセキュリティポリシーを強化する方法がベストプラクティスになります。

ポリシーは、共有としても非共有としても作成でき、グループに割り当てることも場所に割り当てることもできます。共有ポリシーは、すべてのグループおよび場所に適用され、継承できるポリシーです。非共有ポリシーは、グループ内の特定の場所にのみ適用されるポリシーです。通常、複数のグループおよび場所でポリシーを簡単に変更できるため、共有ポリシーを作成する方法がベストプラクティスであると考えられます。ただし、場所固有の特定のポリシーが必要な場合は、非共有ポリシーとして作成するか、または非共有ポリシーに変換する必要があります。

[リモートクライアントの管理](#)

リモートクライアントのファイアウォールポリシー設定のベストプラクティス

「[ファイアウォールポリシーのベストプラクティス](#)」で、シナリオとベストプラクティスの推奨事項について説明します。

Table 64: ファイアウォールポリシーのベストプラクティス

シナリオ	推奨事項
ユーザーが VPN を使わずにログオンするリモートの場所	- VPN を使わずにリモートでログオンするクライアントに最も厳格なセキュリティポリシーを割り当てます。 - NetBIOS の保護を有効にします。 Note: リモートクライアントが VPN 経由で企業ネットワークにログオンする場所については、NetBIOS の保護を有効にしないでください。このルールは、リモートクライアントが企業ネットワークではなくインターネットに接続される場合のみ適切です。 - セキュリティを向上させるため、NetBIOS ポート 135、139、445 で、ローカルの TCP トラフィックをすべて遮断します。
ユーザーが VPN 経由でログオンするリモートの場所	- すべてのアダプタでトラフィックを遮断するルールはすべてそのまま残します。それらのルールは変更しないでください。 - すべてのアダプタで VPN トラフィックを許可するルールはそのまま残します。そのルールは変更しないでください。 - 処理として [許可する] を使うすべてのルールで、[アダプタ] 列を [すべてのアダプタ] から、使っている VPN アダプタの名前に変更します。 - 他のトラフィックをすべて遮断するルールを有効にします。 Note: VPN によって分割トンネリングが起きる可能性を回避したければ、これらの変更をすべて作成する必要があります。
ユーザーがイーサネットまたは無線接続経由でログオンするオフィスの場所	デフォルトのファイアウォールポリシーを使います。無線接続の場合は、無線 EAPOL を許可するルールが有効になっていることを確認します。802.1x は接続の認証に EAPOL (Extensible Authentication Protocol over LAN) を使います。

ファイアウォールポリシーの作成

ルールの追加ではなくネットワークサービスのための通信の有効化

リモートクライアントの通知の有効化について

VPN を介してログオンしていないリモートクライアントの場合、次の状況でクライアント通知をオンにする方法がベストプラクティスです。

- 侵入検出
場所固有のサーバーを使うことによってこれらの通知をオンにすることも、[クライアントユーザーインターフェース制御の設定] で [混合制御] オプションを選択することもできます。[クライアントユーザーインターフェースの設定] タブで設定をカスタマイズできます。
- ウイルスとセキュリティリスク
ウイルスとスパイウェアの対策ポリシーで、これらの通知をオンにできます。

通知をオンにしておくと、セキュリティ上の問題が起きたときにリモートユーザーがこのことを確実に把握できます。

リモートクライアントの管理

管理サーバーからのリモートクライアントの監視について

通知とログは、安全な環境を保守するために不可欠です。一般に、他のクライアントの監視と同じ方法で、リモートクライアントを監視してください。保護が最新になっており、現在、ネットワークが攻撃されていないことを常に確認してください。ネットワークが攻撃されている場合は、背後で攻撃を行っている人物と、その攻撃方法を明らかにしよう考えます。

ホームページの優先設定は、Symantec Endpoint Protection Manager でデータを表示する期間を特定します。デフォルトでは、ホームページのデータは過去 12 時間に接続したクライアントのみを示します。高い頻度でオフラインになっている

るクライアントが多い場合は、ログとレポートを参照することが、監視のうえで最良の選択肢になります。ログとレポートでは、オフラインのクライアントを含めるようにデータをフィルタ処理できます。

モバイルクライアントがアップロードするクライアントログデータの一部を制限する場合でも、次の表示内容を調べることができます。

Table 65: リモートクライアントのセキュリティを監視する表示

ディスプレイ	説明
[ホーム] > [エンドポイントの状態]	内容が最新かどうか、または保護がオフになっていないかどうかを表示します。 次の状態を確認できます。 • コンテンツの日付とバージョン番号 • クライアント接続数 • 有効および無効な保護数 [詳細] をクリックすると、各クライアントの状態を確認できます。
[ホーム] > [セキュリティの状態]	システムセキュリティの概要を表示します。[ウイルスとリスクの活動の概略] を表示して、ネットワークが攻撃を受けているかどうかを確認します。 [詳細] をクリックすると、各セキュリティ保護技術の状態を確認できます。
[ホーム] > [ウイルスとリスクの活動の概略]	検出されたウイルスとリスクの活動や、クリーニング、遮断、検疫などの適用した処理を表示します。
[監視] > [概略の種類] > [ネットワーク脅威防止]	攻撃の種類と攻撃元についての情報を表示します。

リモートクライアントの管理

クラウドコンソールからのローミング Symantec Endpoint Protection クライアントの監視

クラウドコンソールからのローミング Symantec Endpoint Protection クライアントの監視

ローミング Symantec Endpoint Protection クライアントは、管理サーバーに断続的に接続するクライアントです。ローミングクライアントは、空港、ホテル、他の企業など、通常よりリスクの高いさまざまな場所でインターネットにアクセスします。つの Symantec Endpoint Protection Manager は、ネットワークの検出を使用して、これらのクライアントコンピュータにネットワーク上やネットワーク外の保護を提供します。

14.1 以前のローミングクライアントは、接続されたときのみ重要なイベントを管理サーバーに送信します。14.2 以降、ローミングクライアントは、管理サーバーに接続できないときは重要なイベントを自動的にクラウドコンソールに送信します。ローミングクライアントは、管理サーバーに再接続した後、新しい重要なイベントを管理サーバーに送信します。また、このクライアントはそれ以降ローミングとは見なされません。

重要なイベントのリストを つの Symantec Endpoint Protection Manager のセキュリティポリシーを強化する手段として使用します。たとえば、特定のホテルに「従業員 A」が存在しているときに、「従業員 A」のクライアントが大量のサービス拒否攻撃を受けているとします。これにより、そのホテルの場所を作成して、ファイアウォールポリシーでサービス拒否攻撃検出を有効にできます。

クラウドポータルが表示する重要なイベントとは

管理サーバーからのリモートクライアントの監視について

Endpoint Protection の場所の認識機能に関するベストプラクティス

ローミングクライアントと重要なイベントを見つける

ローミングしているクライアントを見つけるには、次の項目を探します。

-
- デバイスが管理サーバーではなくクラウドコンソールに直接接続されているかどうか
 - つの Symantec Endpoint Protection Manager のネットワークの検出ポリシーで定義される場所
 - クライアントの外部 IP アドレス

ローミングクライアントと重要なイベントを見つけるには

1. クラウドコンソールで [警告とイベント] に移動します。
2. [セキュリティイベント] タブの [接続の種類] で、[クラウド] をクリックしてクライアントがクラウドコンソールに送信するイベントを表示します。

管理サーバーが送信するイベントを表示するには、[Symantec **Endpoint Protection Manager**] をクリックします。

3. [重大度] で [致命的] をクリックします。

クラウドコンソールは、ローミングクライアントが検出した重要なセキュリティイベントのみフィルタ処理して表示します。

4. 場所と外部 IP アドレスを発見するには、デバイスを選択してデバイスの位置情報のエントリを探します。

クラウドコンソールが表示する重要なイベントとは

ローミングクライアントは、次のセキュリティイベントをクラウドコンソールにアップロードします。

- ポートスキャンイベント
- MAC 詐称
- サービス拒否
- カナリア
- IPS
- ディセプション
- メモリエクスプロイト緩和機能
- ホストインテグリティのコンプライアンス

ローミングクライアントは、次のセキュリティイベントをクラウドコンソールにアップロードします。

- ウイルス対策
- SONAR

管理者アカウントの管理

管理者アカウントを使って つの Symantec Endpoint Protection Manager データセンターを管理できます。管理者は つの Symantec Endpoint Protection Manager にログオンし、ポリシー設定の変更、グループの管理、レポートの実行、クライアントソフトウェアのインストール、その他の管理タスクを行います。

デフォルトのアカウントは、すべての機能にアクセスできるシステム管理者アカウントです。また、タスクのサブセットを行う必要がある管理者のために、より制限された管理者アカウントを追加できます。

規模の小さい会社では、単一の管理者とドメインのみを必要とする場合もあります。複数のサイトや Windows ドメインを持つ規模の大きい会社では、複数の管理者 (その一部は他の管理者よりも多くのアクセス権を持つ) が必要になることもあります。また、つの Symantec Endpoint Protection Manager 内に複数のドメインを追加する必要がある場合もあります。

ドメイン、管理者アカウント、管理者アカウントのパスワードは、[管理] ページで管理します。

Table 66: アカウントの管理

タスク	説明
複数のドメインを追加するかどうかを決定する	ドメインを追加するかどうかを決定します。 ドメインについて ドメインの追加 現在のドメインへの切り替え
管理者アカウントを追加する	つの Symantec Endpoint Protection Manager コンソールにアクセスする必要がある管理者用のアカウントを追加します。 1. 必要な管理者アカウントの種類とアクセス権のレベルを追加します。 管理者アカウントとアクセス権について 管理者アカウントの追加とアクセス権の設定 2. 一つの Symantec Endpoint Protection Manager にログインするときの管理者の認証方法を選択します (省略可能)。デフォルトでは、一つの Symantec Endpoint Protection Manager データベースは管理者のクレデンシャルを認証します。 管理者アカウントの認証方法の選択
管理者アカウントをロック解除またはロックする	デフォルトでは、一つの Symantec Endpoint Protection Manager は、ユーザーが管理者アカウントを使って一つの Symantec Endpoint Protection Manager へのログインを試みた回数が多すぎると、その管理者をロックします。この設定を、試行回数を増やすか、管理者をロックする時間を増やすように設定できます。管理者がアカウントからロックされた場合、指定された時間を待たなければ再度ログインできません。ロックアウト間隔の間はアカウントのロックを解除できません。 ログイン失敗回数が多すぎる管理者のアカウントのロック解除
紛失したパスワードの変更とリセット	- お使いのアカウントまたは別の管理者のアカウントのパスワードを変更します。 管理者アカウントまたはデフォルトデータベースのパスワードの変更 - 紛失したパスワードをリセットするには、管理サーバーのログイン画面に表示される [パスワードを忘れた場合] リンクを使います。管理者は、仮パスワードをアクティブ化するリンクを含む電子メールを受信します。 忘れた一つの Symantec Endpoint Protection Manager パスワードのリセット [パスワードを忘れた場合] リンクを表示して、管理者が紛失したパスワードをリセットできるようにする - 管理者が管理サーバーのログイン画面のユーザー名とパスワードを保存できるようにします。 ログイン画面への [ユーザー名を記憶する] と [パスワードを記憶する] のチェックボックスの表示 - 管理者のログインパスワードを特定の日数後に強制的に期限切れにします。 ログイン画面への [ユーザー名を記憶する] と [パスワードを記憶する] のチェックボックスの表示
一つの Symantec Endpoint Protection Manager のログインオプションの設定	各種の管理者用に、次のログインオプションを設定できます。 - ログイン前に読む管理者のためのメッセージを表示します。 一つの Symantec Endpoint Protection Manager コンソールへのログイン前に管理者が見るメッセージの表示 - 特定の管理者がリモートでログインできるように、またはログインできないように、管理コンソールへのログインアクセスを許可またはブロックします。 リモート一つの Symantec Endpoint Protection Manager コンソールのアクセスの認可または遮断 - 管理者が管理サーバーにログインし続けることのできる期間を変更します。 一つの Symantec Endpoint Protection Manager コンソールへのログイン状態を維持するためのタイムアウト期間の変更 一つの Symantec Endpoint Protection Manager コンソールへのログイン

管理者アカウントとアクセス権について

一つの Symantec Endpoint Protection Manager をインストールするときに、`admin` というデフォルトのシステム管理者アカウントが作成されます。システム管理者アカウントは一つの Symantec Endpoint Protection Manager のすべての機能に管理者アクセス権を与えます。

セキュリティの管理を容易にするために、システム管理者アカウント、ドメイン管理者アカウント、限定管理者アカウントを追加できます。ドメイン管理者と限定管理者は つの Symantec Endpoint Protection Manager 機能のサブセットにアクセスできます。

会社内で必要な役割の種類とアクセス権に基づいて、必要なアカウントを選択します。たとえば、大きい会社では次の種類の役割を使うことがあります。

- 管理サーバーとクライアントのインストールパッケージをインストールする管理者。製品がインストールされた後、操作を管理する管理者が引き継ぐ。これらの管理者のほとんどはシステム管理者です。
- 操作管理者はサーバー、データベースを保守し、パッチをインストールする。単一ドメインの場合は、操作管理者がサイトを全面的に管理する権限を持つドメイン管理者である場合もあります。
- クライアントのウイルス対策とスパイウェア対策のポリシーと LiveUpdate のポリシーを作成して保守するウイルス対策管理者。この管理者のほとんどは限定管理者です。
- セキュリティを担当し、クライアントのファイアウォールポリシーと侵入防止ポリシーを作成して保守するデスクトップ管理者。この管理者のほとんどはドメイン管理者です。
- レポートを作成し、ポリシーへの読み取り専用アクセスがあるヘルプデスク管理者。ウイルス対策管理者とデスクトップ管理者はヘルプデスク管理者が送信するレポートを確認する。ヘルプデスク管理者のほとんどは、レポート権とポリシー権が認可されている限定管理者です。

Table 67: 管理者の役割と職務

管理者の役割	職務
システム管理者	システム管理者は、すべての機能とタスクに対して制限のない完全なアクセス権で つの Symantec Endpoint Protection Manager コンソールにログインできます。 システム管理者は他のシステム管理者アカウント、ドメイン管理者アカウント、限定管理者アカウントを作成し、管理できます。 システム管理者は次のタスクを実行できます。 • すべてのドメインを管理する。 • ライセンスを管理する。 • すべてのコンソールの設定を表示して管理する。 • データベースと管理サーバーを管理する。
管理者	管理者は、単一ドメインを表示し、管理できるドメイン管理者です。ドメイン管理者は単一のドメインに対してのみシステム管理者と同じ権限を持ちます。 デフォルトでは、ドメイン管理者はドメインを管理する完全なシステム管理者権限を付与されますが、サイトに対しては付与されません。単一ドメイン内のサイト権限を明示的に付与する必要があります。ドメイン管理者は自分のサイト権限は修正できませんが、他の管理者と限定管理者のサイト権限を修正できます。 ドメイン管理者は次のタスクを実行できます。 • 単一ドメイン内の管理者アカウントと限定管理者アカウントを作成して管理する。 ドメイン管理者は自分のサイト権限を修正できません。システム管理者がこの機能を実行する必要があります。 • レポートの実行、サイトの管理、パスワードのリセット。 • ライセンスを管理できない。システム管理者のみがライセンスを管理できます。 ドメインについて
限定管理者	限定管理者は、制限付きアクセス権で つの Symantec Endpoint Protection Manager コンソールにログインできます。限定管理者はデフォルトではアクセス権を持ちません。システム管理者役割は、限定管理者にタスクの実行を許可するアクセス権を明示的に付与する必要があります。 アクセス権を制限すると、限定管理者は管理サーバーユーザーインターフェースの一部を利用できません。次に例を示します。 • レポート権のない限定管理者は、[ホーム]、[監視]、[レポート] の各ページを表示できません。 • ポリシー権のない限定管理者はポリシーを表示することも修正することもできません。さらに、ポリシーを適用することも、置換することも、撤回することもできない。

管理者アカウントの追加とアクセス権の設定

管理者アカウントの管理

管理者アカウントの追加とアクセス権の設定

システム管理者は、別のシステム管理者、管理者、または限定管理者を追加できます。ドメイン内の管理者は、アクセス権の制限が自分のアクセス権と同じかそれより緩い他の管理者を追加できます。管理者は限定管理者を追加して、アクセス権を設定できます。

管理者アカウントを追加するには

1. コンソールで、[管理] > [管理者] の順にクリックします。
2. [タスク] の下で、[管理者を追加する] をクリックします。
3. [管理者の追加] ダイアログボックスの [全般] タブで、ユーザー名と電子メールアドレスを入力します。
4. [アクセス権] タブで、管理者アカウントの種類を指定します。

限定管理者用のアカウントを追加する場合、管理者のアクセス権も指定する必要があります。無効状態では、アクセス権が一切与えられていない限定管理者のアカウントが作成され、限定管理者は管理サーバーにログオンできません。

管理者アカウントとアクセス権について

5. [認証] タブの [Symantec Endpoint Protection Manager 認証] に、管理者がログオンに使用するパスワードを入力します。

管理者が 1 つの Symantec Endpoint Protection Manager にログオンするときに、1 つの Symantec Endpoint Protection Manager はデータベースでユーザー名とパスワードが正しいかどうかを検証します。

管理者アカウントの認証方法の選択

6. [OK] をクリックします。

管理者アカウントの認証方法の選択

ログオンする前に管理者の資格情報を確認するために管理サーバーが使用する認証方法を、いくつかの方法から選択できます。

サードパーティ製品を使った認証方法では、1 つの Symantec Endpoint Protection Manager の管理者アカウントのデータベースにエントリがありますが、サードパーティ製サーバーがユーザー名とパスワードを検証します。

Table 68: 認証方法

次のように入力します。	使うとき
Symantec Endpoint Protection Manager 認証 (デフォルト)	1 つの Symantec Endpoint Protection Manager データベースに保存されている管理者のユーザー名とパスワードで管理者を認証します。管理者が管理サーバーにログオンするときに、管理サーバーはデータベースでユーザー名とパスワードが正しいかどうかを検証します。 [パスワードを無期限にする] オプションを表示することで、管理者アカウントの期限切れが発生しないようにすることができます。 無期限の 1 つの Symantec Endpoint Protection Manager ログオンパスワードの有効化
2 要素認証	スマートフォンでの Symantec VIP 認証によって管理者を認証します。管理者はログオンするときに、パスワードに加えて、固有のワンタイム認証コードを入力します。 このオプションを使用できるようにするには、まず、適切な PKCS キーストアファイルとキーストアのパスワードを追加する必要があります。 Symantec VIP を使用した 2 要素認証の設定

次のように入力します。	使うとき
RSA SecurID 認証	RSA SecurID トークン (ソフトウェア RSA トークンは除く)、RSA SecurID カード、RSA キーパッドカード (RSA スマートカードは除く) を使用して管理者を認証します。 RSA SecurID 機構を使う管理者を認証するには、RSA Authentication Manager サーバーを最初にインストールして RSA SecurID の暗号化された認証を有効にします。 つの Symantec Endpoint Protection Manager での RSA SecurID 認証の使用
ディレクトリサーバー認証	LDAP サーバーまたは Microsoft Active Directory サーバーで管理者を認証します。 Active Directory または LDAP ディレクトリサーバーを使って管理者を認証するには、ディレクトリサーバーでアカウントを設定する必要があります。ディレクトリサーバーと 一つの Symantec Endpoint Protection Manager 間の接続も確立する必要があります。接続を確立しないと、Active Directory サーバーからユーザーをインポートしたり、ユーザーをこのサーバーと同期したりできません。 Note: 同期は Active Directory サーバーのみで可能です。LDAP サーバーとの同期はサポートされていません。 ディレクトリサーバーへの 一つの Symantec Endpoint Protection Manager の接続 ディレクトリサーバーに対する認証の確認
スマートカード認証	米国連邦政府機関の文民または軍関係者で、PIV カードまたは CAC を使用してログオンする必要がある管理者を認証します。 スマートカードでログオンする管理者を認証するように 一つの Symantec Endpoint Protection Manager を設定する

管理者アカウントの認証方法を選択するには

1. 管理者アカウントを追加します。

[管理者アカウントの追加とアクセス権の設定](#)

2. **Symantec Endpoint Protection Manager** 認証 (デフォルト) を使用しない場合は、[認証] タブで認証方法を選択します。
3. [OK] をクリックします。
4. [変更の確認] ダイアログボックスで、一つの Symantec Endpoint Protection Manager にログオンするために使うパスワードを入力して [OK] をクリックします。

認証方法を切り替えるには、管理者アカウントのパスワードを入力する必要があります。

一つの Symantec Endpoint Protection Manager での RSA SecurID 認証の使用

NOTE

IPv6 環境で RSA SecurID 認証を使用するには、一つの Symantec Endpoint Protection Manager サーバーに IPv4 スタックをインストールして有効にする必要があります。

(IPv6 ネットワークはバージョン 14.2 以降でサポートされます。)

RSA SecurID を設定して 一つの Symantec Endpoint Protection Manager 管理者を認証します。

一つの Symantec Endpoint Protection Manager を使う管理者を RSA SecurID で認証するには、最初に RSA Authentication Manager サーバーへの接続を設定して、暗号化された認証を有効にする必要があります。

1. 必要に応じて、RSA Authentication Manager サーバーをインストールします。RSA Authentication Manager 8.1 を使用します。
2. Symantec Endpoint Protection Manager サーバーに RSA Authentication Agent をインストールし、正しく設定して、RSA サーバーに接続します。RSA Authentication Agent 7.x を使用します。
3. Symantec Endpoint Protection Manager サーバーが有効なホストとして RSA Authentication Manager サーバーに登録されることを確認します。

-
4. RSA Authentication Manager サーバー上の `sdconf.rec` ファイルにネットワークアクセスできることを確認します。
 5. 同期された SecurID カードまたはキー FOB を管理サーバーアカウントに割り当てます。RSA Authentication Manager サーバーでログオン名をアクティブ化します。
 6. 管理者が利用可能な RSA PIN またはパスワードを所有していることを確認します。
シマンテック社がサポートする RSA のログオンの種類は次のとおりです。
 - RSA SecurID トークン (ソフトウェア RSA トークンは除く)
 - RSA SecurID カード
 - RSA キーパッドカード (RSA スマートカードは除く)RSA SecurID を使って管理サーバーにログオンするには、管理者はログオン名、トークン (ハードウェア)、PIN 番号を所有している必要があります。

RSA Authentication Agent をインストールして、RSA SecurID 認証を使うように つの **Symantec Endpoint Protection Manager** サーバーを設定します。

つの Symantec Endpoint Protection Manager で RSA SecurID を使うには、RSA Authentication Agent を つの Symantec Endpoint Protection Manager サーバーにインストールして、SecurID Authentication クライアントとして設定します。

RSA Authentication Agent をインストールするには

1. RSA Authentication Agent のソフトウェアを Symantec Endpoint Protection Manager サーバーにインストールします。このソフトウェアをインストールするには、RSA Authentication Agent のインストールファイルから Windows .msi ファイルを実行します。
2. `sdconf.rec` ファイルを RSA Authentication サーバーから つの Symantec Endpoint Protection Manager サーバーにコピーします。
RSA Authentication Agent の以前のバージョンの場合は、`nodesecret.rec`、`sdconf.rec`、`agent_nsload.exe` をコピーします。

つの **Symantec Endpoint Protection Manager** サーバーを設定して、RSA SecurID 認証を使うには

1. つの Symantec Endpoint Protection Manager コンソールにログオンして、[管理]、[サーバー] の順にクリックします。
2. [サーバー] の [ローカルサイト] で、管理サーバーをクリックします。
3. [タスク] で、[SecurID 認証の設定] をクリックします。
4. [SecurID 認証の設定ウィザードによろこそ] パネルで、[次へ] をクリックします。
5. **SecurID** 認証の設定ウィザードの [必要条件] パネルで、前提条件を読んでそれらをすべて満たしていることを確認します。
6. [次へ] をクリックします。
7. **SecurID** 認証の設定ウィザードの [RSA ファイルのアップロード] パネルで、`sdconf.rec` ファイルがあるフォルダを参照します。
パス名を入力することもできます。
8. [次へ] をクリックし、[テスト] をクリックして設定をテストします。
9. [テストの設定] ダイアログボックスで、SecurID のユーザー名とパスワードを入力し、[テスト] をクリックします。
これで認証が正常に実行されました。

RSA SecurID 認証を使用する Symantec Endpoint Protection Manager 管理者の追加

1. 管理者アカウントを追加します。
[管理者アカウントの追加とアクセス権の設定](#)
2. [認証] タブで、RSA SecurID 認証をクリックします。
このオプションを利用できない場合は、設定ガイドラインを確認します。
[RSA SecurID を設定して認証する](#)
3. [OK] をクリックします。

RSA SecurID 認証を使うように既存の管理者アカウントを変更することもできますが、その方法は、特にデフォルトの管理者アカウント「admin」に対して、推奨されません。既存のユーザーを編集するときに無効な情報を指定すると、そのユーザーを復帰することはさらに困難です。

ただし、既存の管理者アカウントを変更する場合は、[変更の確認] ダイアログボックスで、つの Symantec Endpoint Protection Manager にログオンするために使うパスワードを入力して [OK] をクリックします。

認証方法を切り替えるには、管理者アカウントのパスワードを入力する必要があります。

[管理者アカウントの認証方法の選択](#)

Symantec VIP を使用した 2 要素認証の設定

環境内で Symantec VIP の 2 要素認証を使用する場合、つの Symantec Endpoint Protection Manager の管理者がこれを使用して承認するように設定できます。

2 要素認証により、セキュリティの追加レイヤーがログオンプロセスに追加されます。2 要素認証が有効になったら、ログオン時に、パスワードに加えて固有のワンタイム認証コードを入力する必要があります。コードは、音声、テキスト、無料の Symantec VIP Access アプリで受信できます。最も安全で使用しやすいため、アプリの使用が推奨されます。Symantec VIP の概要については、次を参照してください。

[Symantec VIP: エンタープライズクラスの認証を誰でも簡単に](#)

つの Symantec Endpoint Protection Manager 認証を使用する個別の管理者に対して、それぞれの 2 要素認証設定を管理します。RSA SecurID 認証またはディレクトリ認証を使用して認証する管理者は、2 要素認証は使用できません。

NOTE

2 要素認証は、IPv6 を使用する場合、または FIPS 対応環境ではサポートされていません。

Symantec VIP を使用して 2 要素認証の つの Symantec Endpoint Protection Manager を設定するには

1. コンソールで、[管理] > [サーバー] をクリックし、ローカルサーバー名をクリックします。
2. [タスク] で、[VIP 認証の設定] をクリックします。
3. PKCS キーストアファイルを参照して選択し、キーストアのパスワードを入力して、[OK] をクリックします。

証明書は、複製しなくても、同じサイトの他の つの Symantec Endpoint Protection Manager コンソールに自動的に伝播します。サイトの各 つの Symantec Endpoint Protection Manager サイトに証明書を手動で追加する必要はありません。

別のサイトの つの Symantec Endpoint Protection Manager に証明書を伝播するには、サイト同士が複製パートナーである必要があります。

Symantec VIP を使用して 2 要素認証の管理者を設定するには

4. つの Symantec Endpoint Protection Manager 管理者に、大文字と小文字の区別を含め正確に一致する Symantec VIP Manager 上での対応するユーザー名があることを確認します。2 つのユーザー名のパスワードは、一致する必要はありません。

ユーザー名を設定する方法については、Symantec VIP Manager のマニュアルを参照してください。

[Symantec VIP Access Manager 3.0 管理者ガイド](#)

5. コンソールで、[管理] > [サーバー] > [管理者] とクリックします。
6. 既存の管理者を選択し、[管理者の編集] をクリックします。

設定する新しい管理者を追加することもできます。

7. [認証] タブで [VIP を使用する 2 要素認証を有効にする] をクリックします。

スマートカードでログオンする管理者を認証するように つの Symantec Endpoint Protection Manager を設定する

バージョン 14.2 以降では、米国連邦政府機関で作業する管理者は、スマートカードを使用して つの Symantec Endpoint Protection Manager にログオンできます。

スマートカード認証を設定するには、管理者は次の手順を実行する必要があります。

[ステップ 1: スマートカード認証のための つの Symantec Endpoint Protection Manager の設定](#)

[ステップ 2: 失効確認を実行する管理サーバーの設定 \(ダークネットワークでは必須 \) \(省略可能 \)](#)

[ステップ 3: 管理者アカウントの追加とスマートカードの登録](#)

[ステップ 4: スマートカードを使用した つの Symantec Endpoint Protection Manager へのログオン](#)

スマートカードについて

米国連邦政府機関は、HSPD-12 必要条件のためにスマートカード認証対応のソフトウェアシステムを使用するようになりました。米国連邦政府のスマートカードには、カード保有者に連邦施設と情報システムへのアクセス権を付与するのに必要なデータが含まれています。このアクセスで、連邦の該当するすべてのアプリケーションに適切なレベルのセキュリティが保証されます。

一部の Windows クライアントコンピュータまたはワークステーションでは、すでに PIV または CAC リーダーがキーボードに組み込まれています。

つの Symantec Endpoint Protection Manager は、次の種類のスマートカードを使用する管理者を認証します。

- 個人識別検証 (PIV) カード (文民の場合)
- 一般アクセスカード (CAC) (軍関係者の場合)
- FIPS モード: つの Symantec Endpoint Protection Manager は、ECDSA と RSASSA-PSS を使用して署名されたスマートカードをサポートしません。
- 非 FIPS モード: つの Symantec Endpoint Protection Manager は、RSASSA-PSS を使用して署名されたスマートカードをサポートしません。

[HSPD-12](#) を参照してください。

[ステップ 1: スマートカード認証のための つの Symantec Endpoint Protection Manager の設定](#)

このステップでは、カード証明書が適切な機関によって発行されていることを検証します。そして、管理者がログオンした時点で、管理サーバーはスマートカードの証明書を読み取り、これを CA 証明書と照合して検証します。

証明書ファイルを検証するため、管理サーバーは、証明書ファイルがインターネット上の証明書失効リスト (CRL) に表示されていないことを確認します。

管理者のコンピュータにすべてのルートファイルと中間ファイルが存在していることを確認します。この条件を満たさない場合、ログオンできません。

スマートカード認証のために つの Symantec Endpoint Protection Manager を設定するには

1. コンソールで、[管理] > [サーバー] をクリックし、ローカル管理サーバー名を選択します。
2. [タスク] で [スマートカード認証を設定する] をクリックします。
3. [ルート証明書または中間証明書ファイルのパスを指定してください] テキストボックスで 1 つ以上の証明書ファイルを参照し、[OK] をクリックします。
失効を確認する必要があるすべての証明書ファイルを選択します。複数のファイルを選択するには、Ctrl キーを押します。
省略可能: 管理者がログオンする管理サーバーがインターネットにアクセスできない場合、[証明書失効リストのパスを指定してください] テキストボックスに .crl または .pem ファイルを追加します。また、これらの管理サーバー

で次のタスクを実行する必要があります。[ステップ 2: 失効確認を実行する管理サーバーの設定 \(ダークネットワークでは必須\)](#)

4. [OK] をクリックします。
5. 管理者が Web コンソールを利用してリモートで 1 つの Symantec Endpoint Protection Manager にログインする場合、1 つの Symantec Endpoint Protection Manager サービスと 1 つの Symantec Endpoint Protection Manager Web サービスを再起動する必要があります。

管理サーバーサービスの停止と開始

ステップ 2 (省略可能): 失効確認を実行する管理サーバーの設定 (ダークネットワークでは必須)

管理サーバーがインターネットにアクセスできない場合、代わりに管理サーバーコンピュータの CRL ファイルを確認するように管理サーバーを設定する必要があります。この確認がない場合、管理者は引き続きログインできますが、管理サーバーは CRL ファイルを確認できず、セキュリティ上の問題が発生する可能性があります。

失効確認を実行するように管理サーバーを設定するには (ダークネットワークのみ)

1. この管理サーバーで、次のファイルを開きます:<Symantec Endpoint Protection Manager #####>\tomcat\etc\conf.properties
2. conf.properties ファイルに smartcard.cert.revocation.ocsp.crl.dp.enabled=false を追加してファイルを保存します。
3. 管理サーバーサービスを再起動します。

管理サーバーサービスの停止と開始

ステップ 3 (オプション): 失効確認を実行する管理サーバーの設定 (ダークネットワークでは必須)

このステップでは、PIV 認証を設定して、管理者をスマートカードのユーザーとして認証します。PIV 認証には、証明書とキーのペアが必要です。これは、PIV 資格情報が権限のあるエンティティによって発行され、期限が切れておらず、失効していないことを確認するために使用されます。PIV 資格情報は、管理者が資格情報の発行対象と同じ個人であることも識別します。

また、このステップは、ユーザーがユーザー名を入力して、カードを挿入し、スマートカードの PIN を入力するだけで Symantec Endpoint Protection Manager にログインできるようにします。Symantec Endpoint Protection Manager のパスワードを入力する必要はありません。

IPv6 ではスマートカード認証はサポートされません。

1. コンソールで、[管理] > [サーバー] > [管理者] とクリックします。
2. 新しい管理者を追加するか、既存の管理者を編集します。

管理者アカウントの追加とアクセス権の設定

3. [認証] タブで [スマートカード認証を有効にする] をクリックします。
4. その管理者の PIV カードまたは CAC の認証証明書ファイルを参照し、[OK] をクリックします。
5. [変更の確認] ダイアログボックスに管理者のパスワードを入力して、[OK] をクリックします。
1 つの Symantec Endpoint Protection Manager へのログインでスマートカードを使用する管理者すべてに対してこのステップを繰り返します。

ステップ 4: スマートカードを使用した 1 つの Symantec Endpoint Protection Manager へのログイン

1 つの Symantec Endpoint Protection Manager にログインするには、管理者は、カードをスマートカードリーダーに挿入して、PIN 番号を入力します。スマートカードの管理者がログインして管理サーバーを使用している間、カードは常にスマートカードリーダーに挿入されている必要があります。管理者がスマートカードを取り除くと、1 つの Symantec Endpoint Protection Manager は 30 秒以内に管理者をログオフします。

Java コンソールと Web コンソールはスマートカード認証をサポートします。RMM コンソールと REST API はスマートカード認証をサポートしません。

1 つの Symantec Endpoint Protection Manager コンソールへのログイン

トラブルシューティングと複製

2つのサイトが互いを複製する場合、最も新しく設定された CA ファイルを持つサイトが他のすべてのサイトの CA ファイルを上書きします。

管理者アカウントのディレクトリサーバー認証のテスト

作成した管理者アカウントのユーザー名とパスワードが、Active Directory または LDAP サーバーによって認証されることを確認できます。確認するときに、ユーザー名とパスワードが正しく追加されたかどうか、およびディレクトリサーバー上にアカウント名が存在するかどうか評価されます。

ディレクトリサーバーで使うユーザー名とパスワードと同じものを、つの Symantec Endpoint Protection Manager の管理者アカウントで使います。管理者が管理サーバーにログオンするときに、ディレクトリサーバーは管理者のユーザー名とパスワードを認証します。管理サーバーは、ディレクトリサーバーのアカウントを検索するために追加したディレクトリサーバーの設定を使います。

また、ユーザー名とパスワードなしの管理者アカウントが、Active Directory または LDAP サーバーによって認証されるかどうか確認できます。ユーザー名またはパスワードのないアカウントによるアクセスは、匿名アクセスになります。ディレクトリサーバーでパスワードが変更されても管理者がロックアウトされないようにするには、匿名アクセスの管理者アカウントを作成してください。

NOTE

Windows 2003 Active Directory サーバーでは、匿名認証はデフォルトで無効になっています。このため、管理者アカウントにユーザー名のないディレクトリサーバーを追加して、[アカウントの確認] をクリックすると、「アカウント認証が失敗しました」というエラーメッセージが表示されます。この問題に対処するには、ディレクトリサーバーエントリを2つ作成し、1つをテスト用、もう1つを匿名アクセス用にします。このようにすると、管理者は、有効なユーザー名とパスワードを使って管理サーバーにログオンできます。

ステップ 1: 複数のディレクトリサーバーの接続を追加する

テストでの匿名アクセスの使用を容易にするには、少なくとも2つのディレクトリサーバーエントリを追加します。1つのエントリを認証のテストに使い、2つ目のエントリを匿名アクセスのテストに使います。これらのエントリでは、設定が異なる同じディレクトリサーバーを使用します。

デフォルトでは、別の組織単位に移動していない限り、ほとんどのユーザーは CN=Users に属しています。LDAP ディレクトリサーバーのユーザーは、CN=Users、DC=<サンプルドメイン>、DC=local の下に作成されます。ユーザーが LDAP 内のどこに所属しているかを調べるには、ADSIEdit を使います。

この例では、ディレクトリサーバーをセットアップするのに次の情報を使います。

- CN=John Smith
- OU=test
- DC=<サンプルドメイン>
- DC=local

この例では、デフォルトの Active Directory LDAP (389) を使いますが、セキュリティ保護された LDAP (636) も使用できます。

1. Active Directory と LDAP サーバーの認証を確認するためにディレクトリサーバーの接続を追加するには、コンソールで [管理] > [サーバー] をクリックし、デフォルトのサーバーを選択して [サーバーのプロパティを編集] をクリックします。
2. [ディレクトリサーバー] タブで、[追加] をクリックします。

3. [全般] タブで、次のディレクトリサーバーの設定を追加して [OK] をクリックします。

ディレクトリ 1	- 名前: <サンプルドメイン> Active Directory - サーバーの種類: Active Directory - サーバーの IP アドレスまたは名前: server01.<サンプルドメイン>.local - ユーザ名: <サンプルドメイン>\administrator - パスワード: <ディレクトリサーバーのパスワード>
ディレクトリ 2	- 名前: <サンプルドメイン> LDAP (ユーザー名あり) - サーバーの種類: LDAP - サーバーの IP アドレスまたは名前: server01.<サンプルドメイン>.local LDAP ポート: 389 LDAP BaseDN: DC=<サンプルドメイン>, DC=local - ユーザ名: <サンプルドメイン>\administrator - パスワード: <ディレクトリサーバーのパスワード>
ディレクトリ 3	- 名前: <サンプルドメイン> LDAP (ユーザー名なし) - サーバーの種類: LDAP - サーバーの IP アドレスまたは名前: server01.<サンプルドメイン>.local LDAP ポート: 389 LDAP BaseDN: <空白> 匿名アクセスを使うときは、このフィールドを空白のままにします。 - ユーザー名: <空白> - パスワード: <空白> [OK] をクリックすると、警告が表示されます。しかし、ディレクトリサーバーは有効です。 ユーザー名とパスワードを指定せずに BaseDN の追加を試みると、警告が表示されます。

ステップ 2: 複数の管理者アカウントを追加する

複数のシステム管理者アカウントを追加します。匿名アクセス用のアカウントでは、ユーザー名またはパスワードを使用しません。

1. ディレクトリサーバーエントリを使って管理者アカウントを追加するには、コンソールで [管理] > [管理者] をクリックし、[全般] タブで、前のステップの管理者アカウントを追加します。

[管理者アカウントの追加とアクセス権の設定](#)

[管理者アカウントの認証方法の選択](#)

2. 各管理者アカウントを追加して [アカウントの確認] オプションをクリックすると、メッセージが表示されます。アカウント情報を無効にするメッセージが表示される場合があります。しかし、管理者は つの Symantec Endpoint Protection Manager にログインできます。

3. [全般] タブで、次の情報を入力します。

管理者 1	- 名前: <サンプルドメイン> LDAP (ユーザー名なし) - サーバーの種類: LDAP - サーバーの IP アドレスまたは名前: server01.<サンプルドメイン>.local LDAP ポート: 389 LDAP BaseDN: <空白> 匿名アクセスを使うときは、このフィールドを空白のままにします。 - ユーザー名: <空白> - パスワード: <空白> [OK] をクリックすると、警告が表示されます。しかし、ディレクトリサーバーは有効です。ユーザー名とパスワードを指定せずに BaseDN の追加を試みると、警告が表示されます。
管理者 2	- ユーザー名: john - 氏名: John Smith - 電子メールアドレス: john@<サンプルドメイン>.local [アクセス権] タブで、[システム管理者] をクリックします。 [認証] タブで [ディレクトリ認証] をクリックします。 [ディレクトリサーバー] ドロップダウンリストで、[<サンプルドメイン> LDAP (ユーザー名あり)] を選択します。 [アカウント名] フィールドに john と入力します。 [アカウントの確認] をクリックします。 システム管理者の john は、ディレクトリの認証を使って つの Symantec Endpoint Protection Manager にログオンできません。
管理者 3	- ユーザー名: john - 氏名: John Smith - 電子メールアドレス: john@<サンプルドメイン>.local [アクセス権] タブで、[システム管理者] をクリックします。 [認証] タブで [ディレクトリ認証] をクリックします。 [ディレクトリサーバー] ドロップダウンリストで、[<サンプルドメイン> LDAP (ユーザー名あり)] を選択します。 [アカウント名] フィールドに John Smith と入力します。 [アカウントの確認] をクリックします。 システム管理者の john は、ディレクトリの認証を使って つの Symantec Endpoint Protection Manager にログオンできます。
管理者 4	- ユーザー名: john - 氏名: John Smith - 電子メールアドレス: john@<サンプルドメイン>.local [アクセス権] タブで、[システム管理者] をクリックします。 [認証] タブで [ディレクトリ認証] をクリックします。 [ディレクトリサーバー] ドロップダウンリストで、[<サンプルドメイン> LDAP (ユーザー名なし)] を選択します。 [アカウント名] フィールドに John Smith と入力します。 [アカウントの確認] をクリックします。 アカウントの認証は失敗しますが、システム管理者の John Smith は つの Symantec Endpoint Protection Manager にログオンできます。

[ディレクトリサーバーへの つの Symantec Endpoint Protection Manager の接続](#)

管理者アカウントまたはデフォルトデータベースのパスワードの変更

管理者アカウントのパスワードの変更

パスワードを忘れた、または紛失した場合や、パスワードが危殆化した場合は、お使いのアカウントまたは他の管理者アカウントのパスワードを変更する必要があります。

パスワードの変更には次のルールが適用されます。

- システム管理者はすべての管理者のパスワードを変更できる。
- ドメイン管理者は、同じドメイン内の他のドメイン管理者と限定管理者のパスワードを変更できる。
- 限定管理者は自分のパスワードのみを変更できる。

管理者アカウントロックアウトを解決するためにパスワードを変更する場合、管理者はロックアウト期間が過ぎるのを待つ必要があります。

NOTE

パスワードは 8 文字以上、16 文字未満とする必要があります。少なくとも 1 つの小文字 [a-z]、1 つの大文字 [A-Z]、1 つの数字 [0-9]、および 1 つの特殊文字 ["/\"[] ; : | = , + * ? < >] @ を含む必要があります。(14.2 以降)

ログオン失敗回数が多すぎる管理者のアカウントのロック解除

1. コンソールで、[管理] > [管理者] の順にクリックします。
2. [管理者] で管理者アカウントを選択して [パスワードの変更] をクリックします。
パスワードの制限を確認するには F1 を押します。
3. 自分のパスワードと管理者の新しいパスワードの両方を入力します。
4. [変更] をクリックします。

[忘れた つの Symantec Endpoint Protection Manager のリセット](#)

[\[パスワードを忘れた場合 \] リンクを表示して、管理者が紛失したパスワードをリセットできるようにする](#)

デフォルトの SQL Server Express データベースパスワードの変更

管理サーバーを設定してデフォルトデータベース (Microsoft SQL Server Express または埋め込みデータベース (14.3 MPx 以前)) を選択した場合は、デフォルトの管理者アカウント `admin` に入力するパスワードもデータベースのパスワードになります。デフォルトの管理者のパスワードを変更しても、データベースのパスワードは自動的に変更されません。データベースのパスワードを、管理サーバー設定ウィザードを再実行して つの Symantec Endpoint Protection Manager を再設定することによって変更することができます。

1. Windows のスタートメニューで、[Symantec **Endpoint Protection Manager**] > [管理サーバー設定ウィザード] を選択します。
2. [管理サーバーを再設定する] を選択してから、[次へ] > [次へ] を選択します。
[つの Symantec Endpoint Protection Manager の再インストールまたはパスワードの再設定](#)
3. [デフォルト **SQL Server Express** データベース] > [データベース管理者パスワードを変更する] を選択し、新しいパスワードを入力します。
4. 各パネルの指示に従って、設定を完了します。

忘れた つの Symantec Endpoint Protection Manager パスワードのリセット

システム管理者のアカウントがあれば、自身のパスワードをリセットしたり、ほかの管理者がそのパスワードをリセットすることを許可できます。

紛失したパスワードをリセットするには、次のことが有効になっていることを確認してください。

- 管理者は自分のパスワードをリセットできます。
[\[パスワードを忘れた場合 \] リンクを表示して、管理者が紛失したパスワードをリセットできるようにする](#)
- [パスワードを忘れた場合] リンクが管理サーバーのログオン画面に表示されるように設定されています。デフォルトでは、このリンクが表示されます。
[ログオン画面への \[ユーザー名を記憶する \] と \[パスワードを記憶する \] のチェックボックスの表示](#)
- 通知を送信するようにメールサーバーを設定する必要があります。

つの Symantec Endpoint Protection Manager の電子メールエラーのトラブルシューティングを行うには、「[Endpoint Protection Manager のテスト電子メールに対して「テスト電子メールを送信できませんでした」のエラーが発生する](#)」を参照してください。

管理サーバーと電子メールサーバー間の通信の確立

RSA SecurID 認証またはディレクトリ認証ではなく、Symantec Management Server 認証を使って認証する管理者アカウントにこの方法を使います。

NOTE

パスワードは 8 文字以上、16 文字未満とする必要があります。少なくとも 1 つの小文字 [a-z]、1 つの大文字 [A-Z]、1 つの数字 [0-9]、および 1 つの特殊文字 ["/\"[":;|=, + * ? < >] を含む必要があります。

(バージョン 14.2 以降)

管理者アカウントの認証方法の選択

忘れた つの Symantec Endpoint Protection Manager パスワードをリセットするには

1. 管理サーバーコンピュータのスタートメニューで、[すべてのプログラム] > [Symantec **Endpoint Protection Manager**] > [Symantec **Endpoint Protection Manager**] の順に選択します。

デフォルトでは、[パスワードを忘れた場合] リンクが管理サーバーのログオン画面に表示されることを確認します。

2. [ログオン] 画面で、[パスワードを忘れた場合] をクリックします。
3. [パスワードを忘れた場合] ダイアログボックスで、パスワードをリセットするアカウントのユーザー名を入力します。

ドメイン管理者と限定管理者の場合、アカウントのドメイン名を入力します。ドメインを設定していない場合は、ドメインのフィールドを空白のままにしておきます。

4. [仮パスワード] をクリックします。

管理者は、仮パスワードをアクティブ化するリンクを含む電子メールを受信します。管理者は、1 分間に 1 回のみ、管理コンソールから一時パスワードを要求できます。セキュリティ上の理由から、管理サーバーはエントリを検証しません。

5. 管理者はログオンした直後に仮パスワードを変更する必要があります。

管理者が正常にパスワードをリセットしたかどうかを確認するには、その管理者が電子メールメッセージを受け取ったことを確認します。

管理者アカウントまたはデフォルトデータベースのパスワードの変更

パスワードをリセットできない場合

管理者パスワードを [パスワードを忘れた場合] 機能を使って回復できない場合、シマンテック社はパスワードの回復をサポートできません。つの Symantec Endpoint Protection Manager とデータベースバックアップがない状態のデータベースを再設定する必要があります。この手順によって、以前の管理サーバーとデータベース設定が上書きされ、新しいパスワードを作成し直すことができるようになります。したがって、管理サーバーの設定時と管理者アカウント情報の監査時には、電子メール設定を正しく設定することが重要になります。

データベースの復元

「[Symantec Endpoint Protection Manager の再インストールまたは再設定](#)」。

[パスワードを忘れた場合] リンクを表示して、管理者が紛失したパスワードをリセットできるようにする

システム管理者のアカウントがあれば、ほかの管理者がパスワードを忘れた場合にリセットできるようにすることができません。[パスワードを忘れた場合] リンクを つの Symantec Endpoint Protection Manager ログオン画面で有効にして、管理者が仮パスワードを要求できるようにします。

忘れたパスワードのリセットを管理者に許可するには

1. コンソールで、[管理] をクリックします。
2. [管理] ページで、[サーバー] をクリックします。
3. [サーバー] で、ローカルサイトを選択します。

この設定で制御するのはローカルサイトのみです。

4. [サイトプロパティの編集] をクリックします。
5. [パスワード] タブで、[管理者によるパスワードのリセットを許可する] にチェックマークを付けます。
6. [OK] をクリックします。

[忘れた つの Symantec Endpoint Protection Manager パスワードのリセット](#)

[ログオン画面への \[ユーザー名を記憶する \] と \[パスワードを記憶する \] のチェックボックスの表示](#)

無期限の つの **Symantec Endpoint Protection Manager** ログオンパスワードの有効化

つの Symantec Endpoint Protection Manager 認証を使う場合、パスワードのデフォルトオプションではパスワードが 60 日後に期限切れになるように設定されます。

管理者が無期限のパスワードを使うためのオプションを表示できます。このオプションはセキュリティを向上させるためデフォルトで無効化されています。したがって、最初にこのオプションを有効にする必要があります。有効にすると、オプションが管理者アカウントの [認証] タブに表示されます。

無期限の つの Symantec Endpoint Protection Manager ログオンパスワードを有効化するには

1. コンソールで、[管理] をクリックします。
2. [管理] ページで、[ドメイン] をクリックします。
3. [ドメイン] の下で、ログオン資格情報を保存することを管理者に許可するドメインを選択します。
4. [ドメインプロパティの編集] をクリックします。
5. [パスワード] タブで、[管理者のパスワードを無期限にする] をクリックします。
6. [OK] をクリックします。
7. [管理]、[管理者] の順にクリックし、管理者アカウントを開きます。
8. [認証] タブで、[パスワードを無期限にする] をクリックし、[OK] をクリックします。

[忘れた つの Symantec Endpoint Protection Manager パスワードのリセット](#)

[ログオン失敗回数が多すぎる管理者のアカウントのロック解除](#)

つの Symantec Endpoint Protection Manager 用の自己署名されたサーバー証明書の受け入れについて

つの Symantec Endpoint Protection Manager をインストールするときに、ブラウザに表示されるページの自己署名証明書がインストールの一部として組み込まれます。これらのページにリモートコンソールから初めてアクセスするときに、表示するページの自己署名証明書を受け入れる必要があります。

証明書はユーザーごとに個別に保存されます。各管理者アカウントは、管理サーバーに接続する個々のリモートの場所用の証明書を受け入れる必要があります。

セキュリティ証明書を Web ブラウザに追加する方法について詳しくは、「[Internet Explorer に SPC や SEPM の自己署名証明書を追加する方法](#)」という記事を参照してください。

[つの Symantec Endpoint Protection Manager コンソールへのログオン](#)

つの Symantec Endpoint Protection Manager コンソールへのログオン前に管理者が見るメッセージの表示

コンソールにログオンする前に、すべての管理者に表示されるカスタマイズ可能なメッセージを作成し表示できます。主な目的は、所有権のあるコンピュータにログオンしようとしていることを管理者に伝える法的な通知を表示することです。

管理者がユーザー名とパスワードを入力し、[ログオン] をクリックした後、メッセージがコンソールに表示されます。メッセージを読んだ管理者は、通知の内容に同意し、[了解] をクリックし、ログオンできます。管理者が [取り消し] をクリックすると、ログオン処理は取り消され、管理者はログオンウィンドウに戻ります。

また、このメッセージは、管理者が管理サーバーに接続されたスタンドアロン Web ブラウザからレポート機能を実行するときにも表示されます。

つの Symantec Endpoint Protection Manager コンソールへのログオン前に管理者が見るメッセージを表示するには

1. コンソールで [管理]、[ドメイン] の順にクリックします。
2. ログオンバナーを追加するドメインを選択します。
3. [タスク] の下で、[ドメインプロパティの編集] をクリックします。
4. [ログオンバナー] タブで、[管理者が つの Symantec Endpoint Protection Manager マネージャにログオンするときに法的な通知について表示します。] にチェックマークを付けます。
5. バナーのタイトルとテキストを入力します。
詳しくは [ヘルプ] をクリックしてください。
6. [OK] をクリックします。

[管理者アカウントの追加とアクセス権の設定](#)

ログオン画面への [ユーザー名を記憶する] と [パスワードを記憶する] のチェックボックスの表示

システム管理者は、ほかの管理者アカウントの つの Symantec Endpoint Protection Manager ログオン画面に [ユーザー名を記憶する] と [パスワードを記憶する] チェックボックスを表示させることができます。管理者のユーザー名とパスワードがログオン画面に事前にポップアップされます。

[ユーザー名を記憶する] と [パスワードを記憶する] のチェックボックスをログオン画面に表示するには

-
1. コンソールで、[管理] をクリックします。
 2. [管理] ページで、[ドメイン] をクリックします。
 3. [ドメイン] の下で、ログオン資格情報を保存することを管理者に許可するドメインを選択します。
 4. [ドメインプロパティの編集] をクリックします。
 5. [パスワード] タブで、[ログオン時にユーザーによるクレデンシャルの保存を許可する] にチェックマークを付けます。
 6. [OK] をクリックします。

忘れた つの Symantec Endpoint Protection Manager パスワードのリセット

リモート つの Symantec Endpoint Protection Manager コンソールのアクセスの認可または遮断

デフォルトでは、すべてのコンソールのアクセスが認可されています。管理者はネットワーク上の任意のコンピュータからローカルまたはリモートでメインコンソールにログオンできます。

特定のコンピュータへのアクセスを拒否することで、管理コンソールをリモート接続から保護できます。

次の種類のユーザーまたはコンピュータによるアクセスを認可または拒否できます。

- インターネットからのアクセスはすべて拒否してください。拒否しない場合、コンソールはインターネット攻撃にさらされます。
- 管理対象以外のネットワークでコンソールを使っている限定管理者には、アクセスを拒否してください。
- システム管理者と IT 管理者にアクセス権を認可してください。
- テストに使われるコンピュータなど、ラボのコンピュータへのアクセスは認可してください。

グローバルにアクセスを許可または拒否できるのに加えて、IP アドレスによって例外を指定できます。すべてのリモートコンソールに対してアクセスを付与した場合、管理サーバーは例外に対してアクセスを拒否します。反対に、すべてのリモートコンソールに対してアクセスを拒否した場合、例外に対してアクセスは自動的に許可されます。例外を作成する場合は、指定したコンピュータに固定 IP アドレスが割り当てられている必要があります。サブネットマスクを指定することによってコンピュータのグループに対して例外を作成することもできます。たとえば、管理しているすべての領域のアクセスを認可すると便利な場合があります。ただし、パブリック領域にあるコンソールのアクセスは拒否できます。

リモートコンソールのアクセスを認可または拒否するには

1. コンソールで、[管理] をクリックし、[サーバー] をクリックします。
2. [サーバー] で、リモートコンソールのアクセス権を変更するサーバーを選択します。
3. [タスク] の下で、[サーバーのプロパティを編集する] をクリックします。
4. [全般] タブで、[アクセス認可] または [アクセス拒否] をクリックします。
5. このコンソールのアクセス許可から除外するコンピュータの IP アドレスを指定する場合は、[追加] をクリックします。

追加されたコンピュータは除外されます。[アクセス認可] をクリックすると、指定したコンピュータはアクセスが拒否されます。[アクセス拒否] をクリックすると、指定したコンピュータはアクセスが認可されます。単一コンピュータまたはコンピュータのグループの例外を作成できます。

6. [コンソールアクセスの拒否] ダイアログボックスで、次のいずれかのオプションをクリックします。
 - 単一コンピュータ
1 台のコンピュータに対する設定で、その IP アドレスを入力します。
 - コンピュータのグループ
数台のコンピュータに対する設定で、そのグループの IP アドレスとサブネットマスクを入力します。

7. [OK] をクリックします。

指定したコンピュータが例外リストに表示されます。IP アドレスやマスクごとに、許可の状態が表示されます。

[アクセス認可] から [アクセス拒否] に、またはその反対に変更すると、例外もすべて同様に変更されます。アクセス拒否の例外を作成した場合、例外はアクセスできるようになります。

8. 例外リストに表示されるコンピュータの IP アドレスまたはホスト名を変更する場合は [すべての編集] をクリックします。

IP アドレスエディタが表示されます。IP アドレスエディタは、IP アドレスとサブネットマスクを編集できるテキストエディタです。

9. [OK] をクリックします。

10. リストへの例外の追加またはリストの編集を完了したら、[OK] をクリックします。

管理者アカウントの追加とアクセス権の設定

つの Symantec Endpoint Protection Manager コンソールへのログオン

ログオン失敗回数が多すぎる管理者のアカウントのロック解除

つの Symantec Endpoint Protection Manager は、ログオンに何度も失敗すると特定の期間、管理者をロックアウトします。デフォルトでは、管理サーバーは、管理者が試行に 5 回失敗した後 15 分間、管理者をロックアウトします。

指定期間が過ぎるまで待たないと管理者アカウントをロック解除できません。ただし、この処理はアカウントをロック解除しませんが、管理者アカウントをロックしないようにできます。アカウントがロックされるまでに許可するログオン失敗回数や待機時間の変更もできます。パスワードを変更しても、ロックアウト間隔はリセットされず、その他の方法でロックアウト間隔に影響することはありません。

12.1.5 以降で強化されたセキュリティのために、最初のロックアウト後、ロックアウト間隔はロックアウトごとに倍増します。つの Symantec Endpoint Protection Manager は、正常なログオンの後、または最初のロックアウトの 24 時間後に、元のロックアウト間隔を復元します。たとえば、元のロックアウト間隔が 15 分の場合、2 回目のロックアウトでは、30 分のロックアウト間隔をトリガします。3 回目のロックアウトでは 60 分のロックアウト間隔をトリガします。最初のロックアウトが木曜日の午後 2 時に発生した場合、24 時間の期間は金曜日の午後 2 時に終了し、つの Symantec Endpoint Protection Manager によってロックアウト間隔が 15 分にリセットされます。

ログオン失敗回数が多すぎる管理者のアカウントをロック解除するには

1. コンソールで、[管理] > [管理者] の順にクリックします。
2. [管理者] で、ロックされている管理者アカウントを選択します。
3. [タスク] で、[管理者を編集する] をクリックします。
4. [全般] タブで、[指定する回数だけログオンが失敗したアカウントをロックする] のチェックをはずします。

忘れた つの Symantec Endpoint Protection Manager パスワードのリセット

管理者アカウントまたはデフォルトデータベースのパスワードの変更

無期限の つの Symantec Endpoint Protection Manager ログオンパスワードの有効化

つの Symantec Endpoint Protection Manager コンソールへのログオン状態を維持するためのタイムアウト期間の変更

つの Symantec Endpoint Protection Manager を保護できるようにするため、コンソールで 1 時間後にユーザー名とパスワードを再入力するように要求されます。セキュリティを高めるために、管理コンソールへのログオンを再度要求するまでのタイムアウト期間を短縮できます。

12.1.4 以前のバージョンでは、期間を [なし] に設定できます。

このログオンタイムアウト期間は、管理コンソールにローカルでログオンした場合や、リモートの Java コンソールからログオンした場合に適用されます。リモート Web コンソールのログオンタイムアウト期間は、定義された最短のタイムアウト値に基づきます。たとえば、[サイトプロパティ] の設定を 60 分、Apache の設定を 30 分、ブラウザの設定を 10 分に設定します。この場合、コンソールは 10 分後にタイムアウトします。

1. つの Symantec Endpoint Protection Manager のローカルまたはリモート Java コンソールへのログオン状態を維持するためのタイムアウト期間を変更するには、[管理] をクリックして、[サーバー] をクリックします。
2. [ローカルサイト] またはリモートサイトをクリックし、[サイトプロパティの編集] をクリックします。
3. [全般] タブで、[コンソールタイムアウト] ドロップダウンリストをクリックし、時間の選択肢の 1 つを選択します。
4. [OK] をクリックします。
5. つの Symantec Endpoint Protection Manager リモート Web コンソールへのログオン状態を維持するための Apache Tomcat のタイムアウト期間を変更するには、つの Symantec Endpoint Protection Manager を実行するサーバーで、次のファイルをテキストエディタで開きます。

```
<#####>\Symantec\## Symantec Endpoint Protection Manager\tomcat\etc\conf.properties
```

6. 次の行がない場合は追加します。

```
scm.web.timeout.minutes=timeout_value
```

値 timeout_value は、コンソールがログアウトするまでのアイドル状態の分数です。最大値は 60 です。値が 0 だと、この行が追加されていない場合と同じ効果になります。

この行がある場合は、タイムアウト値を変更できます。

7. ファイルを保存して閉じます。
8. 変更を有効にするには、Windows のサービス (services.msc) を開いて つの Symantec Endpoint Protection Manager サービスを再起動します。
9. つの Symantec Endpoint Protection Manager リモート Web コンソールへのログオン状態を維持するための Internet Explorer のタイムアウト期間を変更するには、Microsoft 社の記事「[Internet Explorer の既定の Keep-Alive タイムアウト値を変更する方法](#)」に従って、レジストリキー HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings を変更します。
10. つの Symantec Endpoint Protection Manager リモート Web コンソールへのログオン状態を維持するための Mozilla Firefox のタイムアウト期間を変更するには、アドレスバーに以下を入力します。

```
about:config
```

11. クリックして警告の内容を確認します。

12. 次の行を探します。

```
network.http.keep-alive.timeout
```

13. 必要に応じて値 (秒数) を変更します。デフォルトは 115 です。

NOTE

Google Chrome には、ネットワークタイムアウト期間の構成可能な設定はありません。

[つの Symantec Endpoint Protection Manager コンソールへのログオン](#)

ドメインについて

管理サーバーをインストールするとき、つの Symantec Endpoint Protection Manager コンソールには、Default という 1 つのドメインがあります。ドメインは、つの Symantec Endpoint Protection Manager インフラから切り離されたデータ

の論理的な分離です。ドメインはグループ、クライアント、コンピュータ、ポリシーの階層を編成するために使う、コンソールの構造コンテナです。ネットワークリソースを管理するために追加ドメインを設定します。

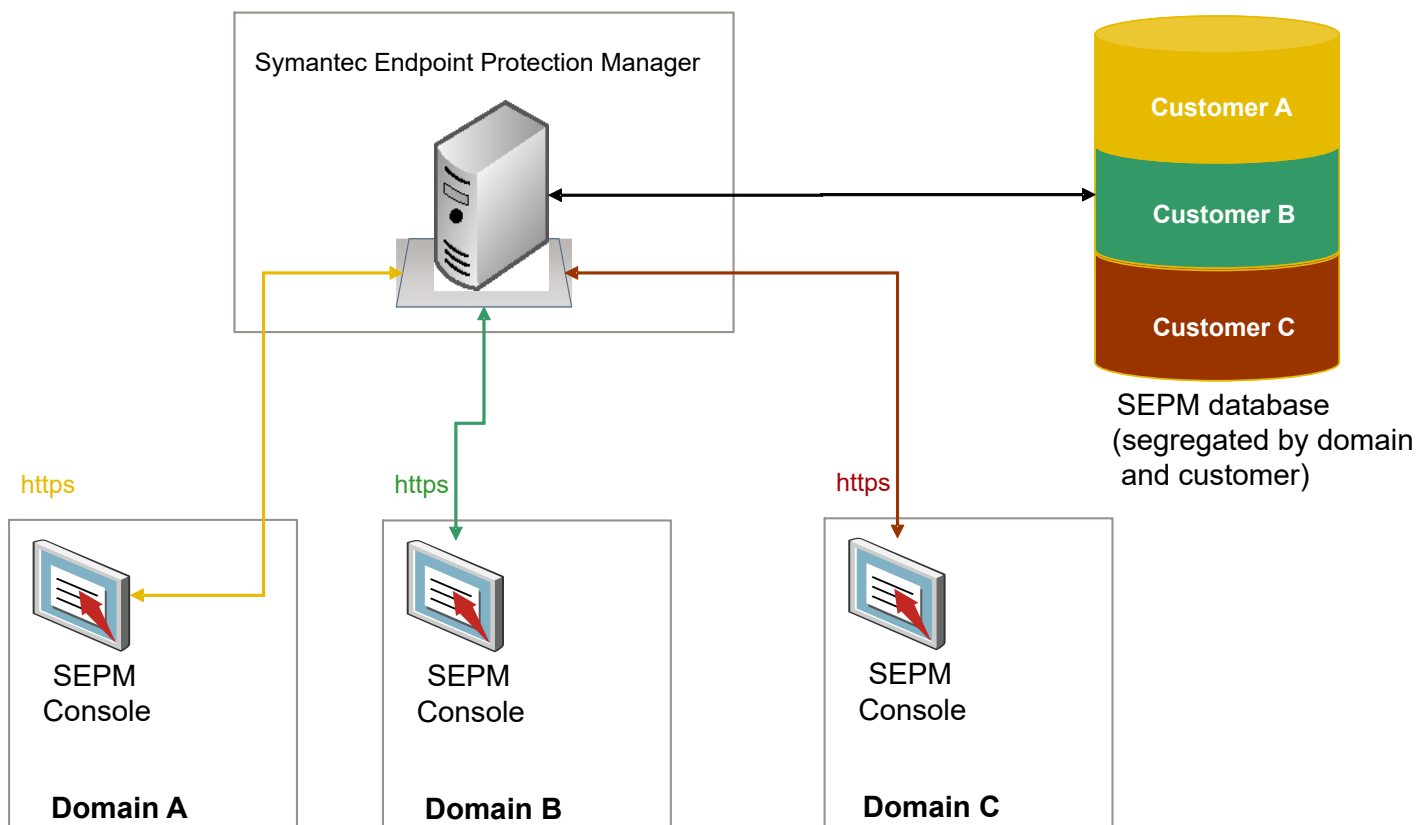
ドメインの主な目的は、マネージドサービスプロバイダが、複数の顧客にサービスを提供する 1 つの Symantec Endpoint Protection Manager インフラを構築できるようにすることです。

NOTE

つの Symantec Endpoint Protection Manager のドメインは Windows ドメインやその他のネットワークドメインと同等ではありません。

追加するそれぞれのドメインは、同じ管理サーバーとデータベースを共有し、コンソールの追加インスタンスを提供します。各ドメインのすべてのデータは完全に別です。このため、他のドメインの管理者がデータを表示することもできません。各ドメインに独自の管理者が存在するように管理者アカウントを追加できます。これらの管理者は、自身のドメインのコンテンツのみを表示および管理できます。

会社が大規模で複数の地域にサイトがある場合、管理情報の単一のビューが必要になることもあります。管理権限を委任したり、セキュリティデータを物理的に分けたり、ユーザー、コンピュータとポリシーがどのように編成されるかについて柔軟性を高めたりすることができます。MSP (Managed Service Provider の略でマネージドサービスプロバイダの意味) である場合、インターネットサービスプロバイダと同様、複数の独立した会社を運営する必要があることもあります。これらのニーズを満たすためには、複数のドメインを作成できます。たとえば、それぞれの国、地域、会社のための別のドメインを作成できます。



ドメインを追加すると、そのドメインは空です。現在のドメインになるようにそのドメインを設定する必要があります。その後このドメインに管理者、グループ、クライアント、コンピュータとポリシーを追加します。

ドメインから別のドメインにポリシーをコピーできます。ドメイン間でポリシーをコピーするには、コピー元ドメインからポリシーをエクスポートしてコピー先ドメインにポリシーをインポートします。

ドメインから別のドメインにポリシーを移動することもできます。ドメイン間でクライアントを移動する場合には、古いドメインの管理者はクライアントグループからクライアントを削除する必要があります。クライアントの通信設定ファイルを新しいドメインの通信設定ファイルに置換します。

不要になったら、ドメインを無効にできます。無効にしようとするときに、このドメインが現在のドメインとして設定されていないことを確認してください。

ドメインの追加

管理者アカウントの管理

現在のドメインへの切り替え

SylinkDrop ツールを使ったクライアントとサーバー間の通信設定の復元

ドメインの追加

組織内のグループ、ユーザー、クライアント、ポリシーを階層化するときは、ドメインを作成します。たとえば、部署ごとにユーザーを編成するためにドメインを追加できます。

NOTE

ディザスタリカバリ用にドメイン ID を使用できます。組織内のすべての管理サーバーに障害が発生した場合は、古いサーバーと同じ ID を使って管理サーバーを再構築する必要があります。古いドメイン ID は、任意のクライアントの sylink.xml ファイルから入手できます。

ドメインを追加するには

1. コンソールで、[管理] をクリックします。
2. [管理] ページで、[ドメイン] をクリックします。
3. [タスク] で、[ドメインの追加] をクリックします。
4. [ドメインの追加] ダイアログボックスで、ドメイン名、省略可能な会社名、省略可能な連絡先情報を入力します。
5. ドメイン ID を追加する場合は、[拡張] をクリックしてからテキストボックスに値を入力します。
6. [OK] をクリックします。

ドメインについて

現在のドメインへの切り替え

デフォルトのドメイン名は、**Default** であり、これが現在のドメインとして設定されます。つの Symantec Endpoint Protection Manager コンソールで新しいドメインを追加したときには、ドメインは空です。新しいドメインにグループ、クライアント、ポリシー、管理者を追加するには、最初にこのドメインを現在のドメインに指定する必要があります。ドメインを現在のドメインに指定すると、現在のドメインというテキストがタイトルのドメイン名に続きます。多くのドメインがある場合は、[ドメイン] リストをスクロールして現在のドメインを表示する必要があります。

システム管理者としてコンソールにログオンした場合は、現在のドメインに関係なくすべてのドメインが表示されます。ただし、現在のドメインで作成された管理者と限定管理者のみが表示されます。管理者または限定管理者としてコンソールにログオンした場合は、アクセスできるドメインのみが表示されます。

現在のドメインを削除する場合は、管理サーバーはログアウトします。現在のドメインではなく唯一のドメインでもない場合のみ、そのドメインを削除できます。

現在のドメインに切り替えるには

-
1. コンソールで、[管理] をクリックします。
 2. [管理] ページで、[ドメイン] をクリックします。
 3. [ドメイン] の下で、現在のドメインにするドメインをクリックします。
 4. [タスク] の下で、[ドメインの管理] をクリックします。
 5. [ドメインの管理] ダイアログボックスで、[はい] をクリックして確認します。
 6. [OK] をクリックします。

[ドメインについて](#)

[ドメインの追加](#)

ポリシーを使ったセキュリティの管理

ポリシーを使用してクライアントコンピュータのセキュリティを管理する

ネットワークセキュリティを管理するため、さまざまな種類のセキュリティポリシーを使います。デフォルトポリシーはインストール時に自動的に作成されます。デフォルトポリシーを使うことも、特定の環境に合わせてポリシーをカスタマイズすることもできます。

すべてのポリシーに共通なタスクの実行

セキュリティポリシーでは、保護技術によって、既知の脅威と未知の脅威からコンピュータを保護する方法を定義します。

多くの方法で、Symantec Endpoint Protection セキュリティポリシーを管理できます。たとえば、セキュリティポリシーの複製を作成してから、特定のニーズに合った複製をカスタマイズできます。ユーザーがクライアントコンピュータ上で変更できるように、特定の設定をロックおよびロック解除できます。

Table 69: すべてのポリシーに共通するタスク

タスク	説明
ポリシーの追加	デフォルトポリシーのいずれも使わない場合は、新しいポリシーを追加できます。 共有ポリシーまたは非共有ポリシーを追加できます。 Note: 共有ポリシーを [ポリシー] ページで追加または編集した場合は、そのポリシーをグループまたは場所にも割り当てる必要があります。そうしないとポリシーは有効になりません。 セキュリティポリシーの種類 共有ポリシーと非共有ポリシーについて ポリシーの追加
ポリシー設定のロックおよびロック解除	一部のポリシー設定やクライアントユーザーインターフェースの設定を、ユーザーが構成することを許可または防止できます。 クライアントコンピュータの保護をユーザーが無効にできない設定
ポリシーの編集	既存のポリシーの設定を変更する場合は、その設定を編集できます。セキュリティポリシーを修正して、コンピュータの保護レベルを上げるか、または下げることができます。グループの割り当てを変更しない限り、修正したポリシーを再割り当てする必要はありません。 ポリシーの編集
ポリシーの割り当て	ポリシーを使うには、1 つ以上のグループや場所にそのポリシーを割り当てなければなりません。 グループまたは場所へのポリシーの割り当て
ポリシーのテスト	実働環境で使う前に、必ず新しいポリシーをテストすることをお勧めします。
クライアントのポリシーの更新	利用可能な帯域幅に基づいて、ポリシー更新方法としてプッシュモードまたはプルモードを使うようにクライアントを設定できます。 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新
ポリシーの置換	共有ポリシーを別の共有ポリシーに置換できます。すべての場所、1 つの場所のいずれでも、共有ポリシーを置換できます。 ポリシーの置換

タスク	説明
ポリシーのコピーと貼り付け	新しいポリシーを追加する代わりに、新しいポリシーのベースとして使うために既存のポリシーをコピーすると便利です。 [ポリシー] ページで、または [クライアント] ページの [ポリシー] タブで、ポリシーをコピーして貼り付けることができます。 Note: また、[クライアント] ページの [ポリシー] タブから、グループ内のすべてのポリシーをコピーして、別のグループに貼り付けることができます。 [クライアント] ページでのポリシーのコピーと貼り付け [ポリシー] ページでのポリシーのコピーと貼り付け
共有ポリシーの非共有ポリシーへの変換	共有ポリシーのコンテンツをコピーして、そのコンテンツから非共有ポリシーを作成できます。 共有ポリシーと非共有ポリシーについて コピーを使うと、1 つの場所で共有ポリシーのコンテンツを変更できますが、その他のすべての場所では変更できません。コピーは既存の非共有ポリシーを上書きします。 共有ポリシーがすべてのグループまたはすべての場所に適用されなくなった場合は共有ポリシーを非共有ポリシーへ変換できます。変換が完了すると、変換済みの新しい名前のポリシーが、[場所固有のポリシーと設定] に表示されます。 共有ポリシーの非共有ポリシーへの変換
ポリシーのエクスポートおよびインポート	別のサイトや管理サーバーで使う場合には既存のポリシーをエクスポートできます。その後、ポリシーをインポートし、グループまたは特定の場所に適用できます。 個々の Endpoint Protection ポリシーのエクスポートとインポート
ポリシーの撤回	ポリシーを削除すると、つの Symantec Endpoint Protection Manager はデータベースからポリシーを削除します。ポリシーを削除する必要はないが不要になった場合は、削除する代わりにポリシーを撤回できます。 [ウイルスとスパイウェアの対策ポリシー] と [LiveUpdate 設定ポリシー] を除き、あらゆる種類のポリシーを撤回できます。 グループまたは場所からのポリシーの割り当て解除
ポリシーの削除	ポリシーが 1 つ以上のグループと場所に割り当てられている場合には、すべてのグループと場所からそのポリシーの割り当てを解除するまでポリシーを削除できません。ポリシーは別のポリシーと置き換えることもできます。
クライアントに最新のポリシーが適用されていることの確認	クライアントに最新のポリシーが適用されているかどうかを確認できます。そうでない場合は、手動でクライアントのポリシーを更新できます。 ポリシーのシリアル番号を使ったクライアントとサーバーの通信の確認 クライアントポリシーの更新

セキュリティポリシーの種類

ネットワークセキュリティを管理するため、いくつかの種類のセキュリティポリシーを使います。ほとんどの種類のポリシーはインストール時に自動的に作成されます。デフォルトポリシーを使うことも、特定の環境に合わせてポリシーをカスタマイズすることもできます。

[すべてのポリシーに共通なタスクの実行](#)

Table 70: セキュリティポリシーの種類

ポリシーの種類	説明
ウイルスとスパイウェアの対策ポリシー	[ウイルスとスパイウェアの対策ポリシー] は次の保護を提供します。 - シグネチャを使って、ウイルスとセキュリティのリスクの副作用を検出し、削除し、修復します。 - ダウンロードインサイトからの評価データを使って、ユーザーがダウンロードを試みるファイルに含まれる脅威を検出します。 - SONAR のヒューリスティックと評価データを使って、疑わしい動作を示すアプリケーションを検出します。 [ウイルスとスパイウェアの対策ポリシー] は SONAR 技術によって動作の異常を見つけます。 Note: ダウンロードインサイトと SONAR 技術は Windows クライアントでのみ利用可能です。 クライアントコンピュータでのスキャンの管理
ファイアウォールポリシー	[ファイアウォールポリシー] は以下の保護を提供します。 - 権限がないユーザーがインターネットに接続するコンピュータとネットワークにアクセスすることを遮断します。 - ハッカーによる攻撃を検出します。 - 迷惑な送信元からのネットワークトラフィックを除去します。 Note: ファイアウォールポリシーは Windows クライアントにのみ適用できます。 ファイアウォール保護の管理
侵入防止ポリシー	[侵入防止ポリシー] は、脆弱性からアプリケーションを保護しながら、ネットワーク攻撃とブラウザに対する攻撃を自動的に検出して遮断します。 侵入防止の管理
アプリケーションとデバイス制御	[アプリケーションとデバイス制御ポリシー] は、アプリケーションからシステムのリソースを保護し、コンピュータに接続可能な周辺機器を管理します。 アプリケーション制御の設定 アプリケーション制御ポリシーは Windows クライアントにのみ適用できます。デバイス制御ポリシーは Windows と Mac コンピュータに適用します。
ホストインテグリティ	[ホストインテグリティポリシー] は、企業のネットワークとデータを安全に維持するためにクライアントコンピュータのセキュリティの定義、実施、復元を行う機能を提供します。このポリシーを使って、ネットワークにアクセスするクライアントが、管理者が定義したウイルス対策ソフトウェア、パッチ、その他のアプリケーション基準を実行していることを確認します。 ホストインテグリティの設定
LiveUpdate のポリシー	[LiveUpdate Content policy] と [LiveUpdate 設定ポリシー] には、クライアントコンピュータが LiveUpdate からコンテンツ更新をダウンロードする方法と時間を指定する設定が含まれます。クライアントが更新の有無をチェックするために交信するコンピュータと、クライアントコンピュータが更新をチェックする頻度を指定できます。 クライアント上のコンテンツと定義を更新する方法
メモリエクспロイト緩和機能	[メモリエクспロイト緩和機能ポリシー] は、DLL ハイジャック、ヒープスプレイの緩和、Java エクспロイトの防止などの緩和機能を使用して、ソフトウェアに対する脆弱性攻撃を防止します。 メモリエクспロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化 このポリシーの種類は 14.0.1 用に追加されました。バージョン 14 では、この機能は [汎用エクспロイト緩和機能] という名前で侵入防止ポリシーに追加されています。

ポリシーの種類	説明
Web とクラウドのアクセス保護	Web とクラウドのアクセス保護 は、Symantec Web Security Service (WSS) にネットワークトラフィックを送信します。WSS ソリューションでは、アプリケーションおよび Web サイトを分類し、ポリシーに基づいてそれらへのアクセスを許可または拒否することによって、ユーザーと組織を保護します。 14.3 RU2 で、Web とクラウドのアクセス保護 は Network Traffic Redirection から名前が変更されました。Web とクラウドのアクセス保護 Web とクラウドのアクセス保護 の設定
例外	[例外ポリシー] は、ウイルスとスパイウェアのスキャンや SONAR によってアプリケーションとプロセスを検出から除外する機能を提供します。 アプリケーションをアプリケーション制御から除外することもできます。 Symantec Endpoint Protection の例外の管理

クライアントポリシーの更新

Symantec Endpoint Protection クライアントコンピュータのポリシーが最新でないと考えられる場合は、ポリシーを更新できます。クライアントが更新を受信していない場合、通信の問題が存在する可能性があります。

ポリシーのシリアル番号を確認して、管理下クライアントコンピュータが管理サーバーと通信できるかどうかを確認します。

クライアントコンピュータのポリシーは、手動でのみ更新できます。ポリシー設定が原因で、ユーザーインターフェースまたは通知領域アイコンを開けない場合、ポリシーを手動で更新できないことがあります。

つの Symantec Endpoint Protection Manager には、クライアントにポリシーを更新するように手動でメッセージを出すコマンドは存在しません。クライアントは、プルモードまたはプッシュモードの更新方法に基づくポリシー更新のためにチェックインします。

Windows タスクバーからクライアント上のクライアントポリシーを更新するには

1. Windows タスクバーの通知領域で、Symantec Endpoint Protection のアイコンを右クリックします。
2. [ポリシーの更新] をクリックします。

クライアントのユーザーインターフェースからクライアントポリシーを更新するには

1. クライアントで、[ヘルプ] > [トラブルシューティング] の順にクリックします。
2. [トラブルシューティング] ダイアログボックスの左の列で、[管理] をクリックします。
3. [管理] パネルの [ポリシープロファイル] で、次のいずれかをクリックします。
4. 管理コンソールから直接ポリシーを更新するには、[更新] をクリックします。
5. 管理コンソールからエクスポートされたポリシーをインポートするには、[インポート] をクリックします。メッセージに従って、インポートするポリシーファイルを選択します。

ポリシーの追加

つの Symantec Endpoint Protection Manager には、保護の種類ごとにデフォルトポリシーが用意されています。ポリシーをカスタマイズする必要がある場合は、ポリシーを 1 つ追加し、それを編集します。各種ポリシーの複数のバージョンを作成できます。

新しいポリシーはすべて、実働環境で使う前にテストすることをお勧めします。

新しいポリシーを追加するには

-
1. コンソールで、[ポリシー] をクリックします。
 2. [ポリシー] ページで、ポリシーの種類を選択して、新しいポリシーを追加するリンクをクリックします。
 3. 保護を強めるか弱めるようにポリシー設定を修正します。
 4. [OK] をクリックしてポリシーを保存します。
 5. 必要に応じて、新しいポリシーをグループに割り当てます。

ポリシーの作成中でも作成後でも、新しいポリシーをグループに割り当てることができます。新しいポリシーは、現在割り当てられている、保護の種類が同じポリシーに置き換わります。

[グループまたは場所へのポリシーの割り当て](#)

[すべてのポリシーに共通なタスクの実行](#)

ポリシーの編集

共有ポリシーと非共有ポリシーは、[ポリシー] ページでも、[クライアント] ページの [ポリシー] タブでも編集できます。

グループだけでなく場所も同じポリシーを共有できます。共有ポリシーを編集したら、それを割り当てする必要があります。

[グループまたは場所へのポリシーの割り当て](#)

1. オプション 1: [ポリシー] ページでポリシーを編集するには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] ページの [ポリシー] で、ポリシーの種類をクリックします。
3. [ポリシーの種類 ポリシー] ペインで、編集する特定のポリシーをクリックします。
4. [タスク] の下で、[ポリシーの編集] をクリックします。
5. <ポリシーの種類> ポリシーの概要ペインで、必要に応じて、ポリシーの名前と説明を編集します。
6. ポリシーを編集するには、ポリシーに対するポリシーの種類の [ポリシー] ページのいずれかをクリックします。
7. オプション 2: [クライアント] ページでポリシーを編集するには、コンソールで [クライアント] をクリックします。
8. [クライアント] ページの [クライアント] で、編集するポリシーのグループを選択します。
9. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

ポリシーを削除するグループの継承を無効にする必要があります。継承のチェックマークをはずさないと、ポリシーを編集できません。

10. [場所固有のポリシーと設定] でスクロールして、編集するポリシーのある場所の名前を検索します。
11. 編集する場所固有のポリシーを検索します。
12. 選択したポリシーの右側で [タスク] をクリックして、[ポリシーの編集] をクリックします。
13. 次のいずれかのタスクを行います。
 - 非共有ポリシーを編集するには、次のステップに進みます。
 - 共有ポリシーを編集するには、[ポリシーの編集] ダイアログボックスで、[共有の編集] をクリックし、すべての場所のポリシーを編集します。

14. 編集するポリシーの種類のリンクをクリックできます。

[ポリシー] ページでのポリシーのコピーと貼り付け

[ポリシー] ページではポリシーのコピーと貼り付けが可能です。たとえば、ポリシー設定を少し編集して別のグループに適用すると便利な場合があります。

1. [ポリシー] ページでポリシーをコピーするには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] ページの [ポリシー] で、コピーするポリシーの種類をクリックします。
3. ポリシーの種類の [ポリシー] ペインで、コピーする特定のポリシーをクリックします。
4. [ポリシー] ページの [タスク] で、[ポリシーのコピー] をクリックします。
5. この処理に関する通知が今後表示されないようにする場合は、[ポリシーのコピー] ダイアログボックスで、[今後このメッセージを表示しない] にチェックマークを付けます。
[今後このメッセージを表示しない] チェックボックスを再度表示するには、[管理]、[管理者] の順にクリックし、管理者アカウントを選択し、[ポリシーのコピー通知のリセット] をクリックします。
6. [OK] をクリックします。
7. [ポリシー] ページでポリシーを貼り付けるには、コンソールで [ポリシー] をクリックします。
8. [ポリシー] ページの [ポリシー] で、貼り付けるポリシーの種類をクリックします。
9. ポリシーの種類の [ポリシー] ペインで、貼り付ける特定のポリシーをクリックします。
10. [ポリシー] ページの [タスク] で、[ポリシーの貼り付け] をクリックします。

[クライアント] ページでのポリシーのコピーと貼り付け

[クライアント] ページでのポリシーのコピーと貼り付け

新しいポリシーを追加する代わりに、ポリシーをコピーして貼り付けることができます。[クライアント] ページでは、共有ポリシーや非共有ポリシーをコピーできます。

すべてのポリシーに共通なタスクの実行

1. [クライアント] ページでポリシーをコピーするには、コンソールで [クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、ポリシーのコピー先のグループを選択します。
3. [ポリシー] タブの [場所固有のポリシーと設定] でスクロールして、ポリシーのコピー元の場所の名前を検索します。
4. コピーする場所固有のポリシーを検索します。
5. ポリシーの右側で、[タスク] をクリックしてから、[コピー] をクリックします。
6. [OK] をクリックします。
7. [クライアント] ページでポリシーを貼り付けるには、コンソールで [クライアント] をクリックします。
8. [クライアント] ページの [クライアント] で、ポリシーの貼り付け先のグループを選択します。
9. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

ポリシーを削除するグループの継承を無効にする必要があります。継承のチェックマークをはずさないと、ポリシーを貼り付けることはできません。

10. [場所固有のポリシーと設定] でスクロールして、貼り付けるポリシーのある場所の名前を検索します。

11. 貼り付ける場所固有のポリシーを検索します。

12. ポリシーの右側で、[タスク] をクリックしてから、[貼り付け] をクリックします。

13. 既存のポリシーを上書きするかどうかの確認を求められたら、[はい] をクリックします。

グループまたは場所へのポリシーの割り当て

グループを通じてクライアントコンピュータにポリシーを割り当てます。すべてのグループには、常にグループに割り当てられている保護の種類ごとに、正確に 1 つずつポリシーが含まれます。通常は、プラットフォームを実行するクライアントごとに個別のグループを作成します。異なるプラットフォームを実行するクライアントを同じグループに入れると、各クライアントプラットフォームは自身に適用されない設定を無視します。

割り当てられていないポリシーは、グループと場所にあるクライアントコンピュータにダウンロードされません。ポリシーを追加するときにポリシーを割り当てない場合は、後でグループと場所に割り当てることができます。別のグループまたは場所にポリシーを再割り当てすることもできます。

ポリシーは、次のようにコンピュータグループに割り当てられます。

- 初期インストール時に、シマンテック社のデフォルトのセキュリティポリシーは、**My Company** 親グループに割り当てられます。
- **My Company** 親グループのセキュリティポリシーは、新しく作成された各子グループに自動的に割り当てられます。デフォルトでは、新しく作成する子グループは [My Company] から継承します。
新しいグループは常に、直接の親グループからポリシーを継承します。子グループの階層を作成すると、各階層は最上位の親ではなく直接の親からポリシーを継承します。
- 同じ種類の別のポリシーを割り当てることによって、グループ内のポリシーを置き換えます。**My Company** 親グループまたは任意の子グループに割り当てられたポリシーを置き換えられます。

アイコンには次の情報が表示されます。

Table 71: ポリシーのアイコン

アイコン	説明
	ポリシーが割り当てられていないグループ。
	ポリシーが割り当てられているグループ。テキストは太字です。
	ポリシーが割り当てられていない場所。
	ポリシーが割り当てられている場所。テキストは太字です。
	親グループから継承されていて、ポリシーが割り当てられていない場所。
	親グループから継承されていて、ポリシーが割り当てられている場所。

グループまたは場所にポリシーを割り当てるには

-
1. コンソールで、[クライアント]、[ポリシーの種類] の順にクリックします。
 2. [ポリシー] ページで、ポリシーを選択して [ポリシーの割り当て] をクリックします。
 3. [ポリシーの割り当て] ダイアログボックスで、グループまたは場所を選択して [割り当て] をクリックします。
 4. [OK] をクリックして確定します。

グループまたは場所からのポリシーの割り当て解除

ポリシーの置換

ある共有ポリシーを別の共有ポリシーと置換すると便利な場合があります。すべての場所、個々の場所のいずれでも、共有ポリシーを置換できます。

すべての場所でポリシーを置換すると、管理サーバーによってそのポリシーを持つ場所のポリシーのみが置換されます。たとえば、Sales グループで 4 カ所のうち 3 カ所の場所で Sales ポリシーを使用しているとします。Sales ポリシーを Marketing ポリシーに変更すると、その 3 カ所の場所だけが Marketing ポリシーを受け取ります。

クライアントの配置場所に関係なく、クライアントのグループで同じ設定を使うと効率的です。この場合、非共有ポリシーを共有ポリシーに置換できます。非共有ポリシーと共有ポリシーとの置換は、各場所で個別に行います。

すべてのポリシーに共通なタスクの実行

1. すべての場所の共有ポリシーを置換するには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] ページの [ポリシー] で、置換するポリシーの種類をクリックします。
3. [ポリシーの種類 ポリシー] ペインで、ポリシーをクリックします。
4. [ポリシー] ページの [タスク] で、[ポリシーの置換] をクリックします。
5. [ポリシーの種類 ポリシーの置換] ダイアログボックスの [新しい ポリシーの種類 ポリシー] リストボックスで、古いポリシーを置換する共有ポリシーを選択します。
6. 既存のポリシーを置換するグループと場所を選択します。
7. [置換] をクリックします。
8. グループと場所のポリシーを置換することの確認を求めるメッセージが表示されたら、[はい] をクリックします。
9. 1 つの場所で共有ポリシーまたは非共有ポリシーを置換するには、コンソールで [クライアント] をクリックします。
10. [クライアント] ページの [クライアント] で、置換するポリシーのグループを選択します。
11. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

ポリシーを削除するグループの継承を無効にする必要があります。継承のチェックマークをはずさないと、ポリシーを置換することはできません。

12. [場所固有のポリシーと設定] でスクロールして、ポリシーを含む場所を見つけます。
13. 置換するポリシーの横で、[タスク] をクリックし、[ポリシーの置換] をクリックします。
14. [ポリシーの置換] ダイアログボックスの [新しいポリシー] リストボックスで、置換ポリシーを選択します。
15. [OK] をクリックします。

個々の Endpoint Protection ポリシーのエクスポートとインポート

ポリシーは、作り直さずに、エクスポートしたりインポートしたりできます。ポリシーに関連付けられているすべての設定が自動的にエクスポートされます。

次の理由でポリシーのエクスポートが必要になる場合があります。

-
- 管理サーバーを以前のリリースから新しいリリースに更新する場合。新しい管理サーバーを、以前にカスタマイズしたポリシーで更新することがあります。
 - 別の場所で使うためにポリシーをエクスポートする場合。

それぞれのポリシーを一度に1つずつエクスポートし、インポートします。ファイルをエクスポートしたら、そのファイルをインポートしてグループを対象にして、または場所のみを対象にして適用します。[クライアント] ページでは、特定の場所の共有ポリシーまたは非共有ポリシーをエクスポートできます。

すべてのポリシーに共通なタスクの実行

1. [ポリシー] ページで単一のポリシーをエクスポートするには、コンソールで[ポリシー] をクリックします。
2. [ポリシー] ページの[ポリシー] で、エクスポートするポリシーの種類をクリックします。
3. [ポリシーの種類 ポリシー] ペインで、エクスポートする特定のポリシーをクリックします。
4. [ポリシー] ページの[タスク] で、[ポリシーのエクスポート] をクリックします。
5. [ポリシーのエクスポート] ダイアログボックスでポリシーファイルのエクスポート先のフォルダを検索し、[エクスポート] をクリックします。
6. [クライアント] ページから共有ポリシーまたは非共有ポリシーをエクスポートするには、コンソールで[クライアント] をクリックします。
7. [クライアント] で、ポリシーのエクスポート先となるグループを選択します。
8. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。
ポリシーを削除するグループの継承を無効にする必要があります。継承のチェックマークをはずさないと、ポリシーをエクスポートすることはできません。
9. [場所固有のポリシーと設定] でスクロールして、エクスポートするポリシーのある場所の名前を検索します。
10. エクスポートする場所固有のポリシーを検索します。
11. ポリシーの右側で、[タスク] をクリックしてから、[ポリシーのエクスポート] をクリックします。
12. [ポリシーのエクスポート] ダイアログボックスで、ポリシーのエクスポート先となるフォルダを参照します。
13. [ポリシーのエクスポート] ダイアログボックスで、[エクスポート] をクリックします。
14. 単一のポリシーをインポートするには、コンソールで[ポリシー] をクリックします。
15. [ポリシー] ページの[ポリシー] で、インポートするポリシーの種類をクリックします。
16. [ポリシーの種類 ポリシー] ペインで、インポートするポリシーをクリックします。
17. [ポリシー] ページの[タスク] で、[Import aポリシーの種類 Policy] をクリックします。
18. [ポリシーのインポート] ダイアログボックスで、インポートするポリシーファイルを参照して、[インポート] をクリックします。

共有ポリシーと非共有ポリシーについて

ポリシーは共有または非共有のいずれかです。ポリシーを複数のグループまたは場所に適用する場合、ポリシーは共有されます。共有ポリシーを作成する場合、そのポリシーを使うすべてのグループと場所で簡単にポリシーを編集や置換することができます。My Company グループレベルまたはより低いグループレベルで共有ポリシーを適用でき、サブグループはポリシーを継承できます。複数の共有ポリシーを作成できます。

特定のグループまたは場所のために特別なポリシーが必要な場合は、固有のポリシーを作成します。作成した固有の非共有ポリシーを、1つの特定のグループまたは場所に割り当てます。1つの場所に割り当て可能なポリシーは、1種類のポリシーにつき1つだけです。

例として、考えられるいくつかのシナリオを以下に示します。

- 経理部のユーザーのグループは、在社時と在宅時には異なる場所の設定を使って企業ネットワークに接続する必要があります。その場合、この1つのグループのために、独自のルールセットと設定を持つ異なるファイアウォールポリシーを、それぞれの場所に適用する必要があります。
- 会社には通常は DSL や ISDN を使うリモートユーザーがいて、これらのユーザーには VPN 接続が必要な場合があります。他のリモートユーザーは、社内ネットワークに接続するときにはダイヤルアップすることを望んでいます。しかし、営業やマーケティングのグループではワイヤレス接続を使うこともあります。これらの各グループでは、社内ネットワークへの接続元の場所に固有のファイアウォールポリシーが必要です。
- 社内ネットワークを攻撃から保護するために、認定されていないアプリケーションのインストールを制限するポリシーをほとんどの社員のワークステーションに実装することを推奨します。IT グループは、追加のアプリケーションへのアクセスが必要な場合があります。そのため、IT グループに対しては一般の社員よりも制限の緩いセキュリティポリシーが必要です。この場合、IT グループ向けに異なるファイアウォールポリシーを作成できます。

一般に、[ポリシー] ページの [ポリシー] タブでグループと場所が共有するポリシーを追加します。ただし、グループ間では共有されず、特定の場所にのみ適用されるポリシーは、[クライアント] ページで追加します。[クライアント] ページでポリシーを追加する場合、次のいずれかの方法を使って新しいポリシーを追加できます。

- 新しいポリシーを追加します。
[ポリシーの追加](#)
- 新しいポリシーの基になる既存のポリシーをコピーします。
[ポリシー] ページでのポリシーのコピーと貼り付け
[クライアント] ページでのポリシーのコピーと貼り付け
- 別のサイトから以前エクスポートされたポリシーをインポートします。
[個々の Endpoint Protection ポリシーのエクスポートとインポート](#)

[すべてのポリシーに共通なタスクの実行](#)

[共有ポリシーの非共有ポリシーへの変換](#)

共有ポリシーの非共有ポリシーへの変換

共有ポリシーのコンテンツをコピーして、そのコンテンツから非共有ポリシーを作成できます。コピーを使うと、1つの場所で共有ポリシーのコンテンツを変更できますが、その他のすべての場所では変更できません。コピーは既存の共有ポリシーを上書きします。

変換が完了すると、変換済みの新しい名前のポリシーが、[場所固有のポリシーと設定] に表示されます。ただし、非共有ポリシーは [クライアント] ページ > [ポリシー] タブから [ポリシー] ページにコピーしない限り、ポリシータイプについて [ポリシー] ページには表示されません。

[共有ポリシーと非共有ポリシーについて](#)

[\[クライアント \] ページでのポリシーのコピーと貼り付け](#)

[\[ポリシー \] ページでのポリシーのコピーと貼り付け](#)

共有ポリシーを非共有ポリシーに変換するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] ページの [クライアント] で、変換するポリシーのグループを選択します。
3. 前の手順で選択したグループに関連付けられたペインで、[ポリシー] タブをクリックします。
4. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

ポリシーを削除するグループの継承を無効にする必要があります。継承のチェックマークをはずさないと、ポリシーを置換することはできません。

-
5. [場所固有のポリシーと設定] で、変換する特定のポリシーとそのポリシーのある場所の名前をスクロールして探します。
 6. 固有のポリシーの隣にある [タスク] をクリックしてから、[非共有ポリシーに変換] をクリックします。
 7. [概要] ダイアログボックスで、ポリシーの名前と説明を編集します。
 8. 必要に応じて他のポリシーの設定を修正します。
 9. [OK] をクリックします。

すべてのポリシーに共通なタスクの実行

グループまたは場所からのポリシーの割り当て解除

ポリシーを完全に削除するか、または後で使うためにポリシーを保存する場合は、グループまたは場所からポリシーの割り当てを解除できます。

たとえば、新しいポリシーを導入した後に特定のグループに問題が生じることがあります。データベースにポリシーを残したい場合は、削除する代わりにポリシーを撤回できます。ポリシーを撤回すると、ポリシーを割り当てたグループと場所から自動的に撤回されます。ポリシーが使われている場所の番号は [ポリシー] ページの [ポリシーの種類 ポリシー] ペインに表示されます。

NOTE

ポリシーを削除する前に、すべてのグループと場所からポリシーを撤回するか、置き換える必要があります。

[ポリシー] ページでは、次のポリシーを除き、場所やグループからすべてのポリシーを撤回できます。:

- ウイルス対策とスパイウェア対策
- **LiveUpdate** 設定

これらのポリシーは別の [ウイルスとスパイウェアの対策ポリシー] または [LiveUpdate ポリシー] との置換のみが可能です。

ポリシーの置換

グループまたは場所へのポリシーの割り当て

1. [ポリシー] ページで共有ポリシーの割り当てを解除するには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] ページの [ポリシー] で、撤回するポリシーの種類をクリックします。
3. [ポリシーの種類 ポリシー] ペインで、撤回する特定のポリシーをクリックします。
4. [ポリシー] ページの [タスク] で、[ポリシーの撤回] をクリックします。
5. [ポリシーの撤回] ダイアログボックスで、ポリシーを撤回するグループと場所にチェックマークを付けます。
6. [撤回] をクリックします。
7. グループと場所のポリシーを撤回することの確認を求めるメッセージが表示されたら、[はい] をクリックします。
8. [クライアント] ページで共有ポリシーまたは非共有ポリシーの割り当てを解除するには、コンソールで [クライアント] をクリックします。
9. [クライアント] ページの [クライアント] で、ポリシーを撤回する対象のグループを選択します。
10. [ポリシー] タブで、[ポリシーと設定を親グループ「グループ名」から継承する] のチェックマークをはずします。

ポリシーを削除するグループの継承を無効にする必要があります。継承のチェックマークをはずさないと、ポリシーを撤回することはできません。

11. [場所固有のポリシーと設定] でスクロールして、ポリシーを撤回する場所の名前を検索します。
12. 撤回する場所のポリシーを検索します。
13. [タスク] をクリックし、[ポリシーの撤回] をクリックします。
14. [ポリシーの撤回] ダイアログボックスで、[はい] をクリックします。

すべてのポリシーに共通なタスクの実行

クライアントコンピュータの保護をユーザーが無効にできない設定

つの Symantec Endpoint Protection Manager 管理者としてユーザー制御レベルを設定する、またはポリシーオプションをロックして、ユーザーがクライアントコンピュータの保護を無効にできないようにすることができます。たとえば、ファイアウォールポリシーでは制御レベルを使用し、ウイルスとスパイウェアの対策ポリシーではロックを使用します。

シマンテック社では、ユーザーによる保護の無効化を常に許可しないようにすることを推奨します。

- [ユーザー制御レベルについて](#)
- [ユーザー制御レベルの変更](#)
- [ポリシー設定のロックおよびロック解除](#)
- [特定の保護技術をユーザーが無効にできない設定](#)
- [つの Symantec Endpoint Protection Manager からのクライアントポリシーのアップデート](#)

ユーザー制御レベルについて

ユーザー制御レベルは、特定の機能の制御をクライアントユーザーに付与するために使用します。また、ユーザー制御レベルによって、クライアントユーザーインターフェースを完全に不可視にするか、一部の機能セットを表示するか、すべてを表示するかも決定されます。

Table 72: ユーザー制御レベル

ユーザー制御レベル	説明
サーバー制御	ユーザーは最小レベルでクライアントを制御できます。サーバー制御では、ユーザーはロック解除された設定を変更することはできませんが、これらの設定は次のハートビート時に上書きされます。
クライアント制御	ユーザーは最大レベルでクライアントを制御できます。クライアント制御では、ユーザーによる設定が許可されます。クライアントで修正された設定がサーバー設定に優先します。それらの設定は、新しいポリシーでロックされている場合を除き、新しいポリシーが適用されても上書きされません。 クライアント制御はリモートまたは在宅で作業する従業員に役立ちます。 Note: ユーザーがクライアント制御モードまたは混合制御モードの設定を変更するためには、Windows の管理者グループに入っている必要があります。
混合制御	ユーザーは混合レベルでクライアントを制御できます。オプションを [サーバー制御] または [クライアント制御] に設定することで、ユーザーがどのオプションを設定できるようにするかを決定します。クライアント制御のアイテムについては、ユーザーが設定を制御します。サーバー制御のアイテムについては、管理者が設定を制御します。

Windows クライアントの場合、すべてのオプションを設定できます。Mac クライアントの場合、サーバー制御とクライアント制御において通知領域アイコンと一部の IPS オプションを利用できます。

サーバーによって検疫ポリシーが適用されると、[クライアント制御] または [混合制御] 下で実行しているクライアントは [サーバー制御] に切り替えられます。

[ユーザーによるクライアントのユーザーインターフェースの変更を防止、許可](#)

ユーザー制御レベルの変更

一部の管理設定には、依存関係があります。たとえば、ユーザーがファイアウォールルールを設定する権限を有していても、クライアントユーザーインターフェースにアクセスできないことがあります。ユーザーは [ファイアウォールルールの設定] ダイアログボックスにアクセスできないので、ルールを作成できません。

1. コンソールで、[クライアント] をクリックします。
2. [クライアントの表示] でグループを選択して [ポリシー] タブをクリックします。
3. [場所固有のポリシーと設定] で、修正する場所の下の [場所固有の設定] を展開します。
4. [クライアントユーザーインターフェース制御の設定] の隣で、[タスク] > [設定の編集] をクリックします。
5. [クライアントユーザーインターフェース制御の設定] ダイアログボックスで、次のいずれかの操作を行います。
 - [サーバー制御]、[カスタマイズ] の順にクリックします。
必要な設定を行った後、[OK] をクリックします。
 - [クライアント制御] をクリックします。
 - [混合制御]、[カスタマイズ] の順にクリックします。
必要な設定を行った後、[OK] をクリックします。
6. [OK] をクリックします。

混合制御のファイアウォール設定

ポリシー設定のロックおよびロック解除

一部のポリシー設定はロックおよびロック解除できます。ユーザーは、ロックされた設定を変更できません。錠前アイコンが、ロック可能な設定の横に表示されます。ウイルスとスパイウェアの対策の設定、改変対策の設定、提出の設定、侵入防止の設定のロックとロック解除もできます。

特定の保護技術をユーザーが無効にできない設定

クライアントを [混合制御] または [サーバー制御] に設定していても、オプションをロックしなければユーザーは設定を変更できます。これらの変更は、つの Symantec Endpoint Protection Manager での次のハートビートまではそのまま保持されます。さまざまなポリシーのポリシーオプションをロックすることで、設定が [クライアント制御] でも、ユーザーが設定を変更できないようになります。

NOTE

管理者グループに属していない Windows ユーザーは、[場所固有の設定] の構成に関係なく、Symantec Endpoint Protection クライアントユーザーインターフェースで設定を変更できません。Windows 10 の管理者は、これらのオプションを設定した後でも、通知領域のアイコンから製品を無効にできます。ただし、個々の保護技術をクライアントユーザーインターフェースから無効にすることはできません。

NOTE

グループすべてに対するポリシーを変更する必要がある場合は、変更を加える対象となるグループのポリシー継承を無効にします。共有ポリシーを編集する場合、ポリシー継承が無効化されていても、そのポリシーが適用されている各グループに編集後のポリシーが適用されます。

ユーザーがファイアウォールまたはアプリケーションとデバイス制御を無効化しないようにするには

1. コンソールで、[クライアント] をクリックします。
2. 制限するクライアントグループをクリックし、[ポリシー] タブをクリックします。
3. [場所固有の設定] を展開します。
4. [クライアントユーザーインターフェース制御の設定] の隣で、[タスク] > [設定の編集] をクリックします。
5. [サーバー制御] または [混合制御] をクリックし、次に [カスタマイズ] をクリックします。
6. [クライアントユーザーインターフェースの設定] ダイアログボックス (サーバー制御) またはペイン (混合制御) で、[次のユーザーによるファイアウォールの有効と無効の切り替えを許可する] と [ユーザーによるアプリケーションデバイス制御の有効と無効の切り替えを許可する] のチェックマークをはずします。
7. [OK] をクリックし、もう一度 [OK] をクリックします。

ユーザーが侵入防止を無効化しないようにするには

1. コンソールで、[クライアント] をクリックします。
2. 制限するクライアントグループをクリックし、ポリシーの [ポリシー] タブをクリックします。
3. [場所固有のポリシー] を展開します。
4. [侵入防止ポリシー] の隣で、[タスク] > [ポリシーの編集] をクリックします。
5. [侵入防止] をクリックして、[ネットワーク侵入防止を有効にする] および [ブラウザ侵入防止を有効にする] の隣にあるロックをクリックして、これらの機能をロックします。
6. [OK] をクリックします。

ユーザーがウイルスとスパイウェアの対策を無効にできないようにするには

1. コンソールで、[クライアント] をクリックします。
2. 制限するクライアントグループをクリックし、[ポリシー] タブをクリックします。
3. [場所固有のポリシー] を展開します。
4. [ウイルスとスパイウェアの対策ポリシー] の隣で、[タスク] > [ポリシーの編集] をクリックします。
5. [Windows の設定] で、次の機能をロックします。
 - [Auto-Protect] をクリックして、次に [Auto-Protect を有効にする] の隣のロックをクリックします。
 - [ダウンロード保護] をクリックして、[ダウンロードインサイトを有効にし、ファイル評価に基づいてダウンロード済みファイルの潜在的なリスクを検出する] の隣のロックをクリックします。
 - [SONAR] をクリックして、次に [SONAR を有効にする] の隣のロックをクリックします。
 - [早期起動マルウェア対策ドライバ] をクリックして、[Symantec 早期起動マルウェア対策を有効にする] の隣のロックをクリックします。
 - [Microsoft Outlook Auto-Protect] をクリックして、次に [Microsoft Outlook Auto-Protect を有効にする] の隣のロックをクリックします。
 - 14.2 RU1 より前のバージョンでは、[インターネット電子メール Auto-Protect] をクリックして、次に [インターネット電子メール Auto-Protect を有効にする] の隣のロックをクリックします。
 - 14.2 RU1 より前のバージョンでは、[Lotus Notes Auto-Protect] をクリックして、次に [Lotus Notes Auto-Protect を有効にする] の隣のロックをクリックします。
 - [グローバルスキャンオプション] をクリックして、[有効にするインサイト] と [Bloodhound ヒューリスティックウイルス検出の有効化] の隣のロックをクリックします。
6. [OK] をクリックします。

ユーザーがメモリエクスプロイト緩和機能を無効化しないようにするには (14.1 以降)

バージョン 14 では、侵入防止ポリシーに [メモリエクスプロイト緩和機能] が表示されて、[汎用エクスプロイト緩和機能] と呼ばれていました。

1. コンソールで、[クライアント] をクリックします。
2. 制限するクライアントグループをクリックし、ポリシーの [ポリシー] タブをクリックします。
3. [場所固有の設定] を展開します。
4. [メモリエクスプロイト緩和機能] の隣で、[タスク] > [ポリシーの編集] をクリックします。
5. [メモリエクスプロイト緩和機能] をクリックして、次に [メモリエクスプロイト緩和機能を有効にする] の隣のロックをクリックします。
6. [OK] をクリックします。

つの Symantec Endpoint Protection Manager からのクライアントポリシーのアップデート

これらの変更を加えた後、グループに属するクライアントは、グループの通信設定に応じて、アップデート済みポリシーを受信します。グループがプッシュモードの場合、つの Symantec Endpoint Protection Manager は数秒以内にクライアントにチェックインを求めるメッセージを表示します。グループがプルモードの場合は、クライアントは、次の定時ハートビートでチェックインします。

次のハートビートよりも早くポリシーを受け取るには、クライアントにチェックインしてポリシーをアップデートするように求めるメッセージを表示できます。また、Symantec Endpoint Protection クライアントからポリシーをアップデートすることもできます。

クライアントポリシーの更新

クライアントでポリシーがアップデートされると、Symantec Endpoint Protection の通知領域のアイコンを右クリックしたときに、[**Symantec Endpoint Protection** を無効にする] がグレー表示されます。

クライアントコンピュータで動作するアプリケーションとサービスの監視

Windows クライアントは、各コンピュータで実行されているアプリケーションとサービスの情報を監視して収集します。情報をリストに収集し、リストを管理サーバーに送信するように、クライアントを設定できます。アプリケーションのリストとそれらの特性は、学習済みアプリケーションと呼ばれます。

この情報を使うと、ユーザーが実行しているアプリケーションを調べることができます。次の領域のアプリケーションに関する情報を必要とする場合に、この情報を使うこともできます。

- ファイアウォールポリシー
- アプリケーションとデバイス制御ポリシー
- SONAR 技術
- ホストインテグリティポリシー
- ネットワークアプリケーション監視
- ファイルフィンガープリントリスト

NOTE

Mac と Linux クライアントはそのコンピュータで実行されるアプリケーションとサービスを監視しません。

いくつかのタスクを実行して学習済みアプリケーションを設定し使用できます。

Table 73: アプリケーションを監視する手順

手順	説明
学習済みアプリケーションの有効化	クライアントコンピュータで実行されるアプリケーションに関する情報を収集するために管理サーバーを設定します。 クライアントコンピュータで実行するアプリケーションに関する情報の収集
アプリケーションの検索	クエリーツールを使用してクライアントコンピュータで実行されるアプリケーションのリストを検索できます。アプリケーションベースの基準またはコンピュータベースの基準を指定して検索できます。たとえば、クライアントコンピュータが使っている Internet Explorer のバージョンを調べることができます。 コンピュータで実行されるアプリケーションに関する情報の検索 アプリケーションの検索結果は確認のために保存できます。

NOTE

一部の国では、社員が会社のノートパソコンで自宅からオフィスのネットワークにログオンしノートパソコンからアプリケーション使用情報を取得する、といった特定の状況で学習済みアプリケーションツールを使うことが法律で許可されていない場合もあります。このツールを使う前に、使用目的が自国の法律で許可されていることを確認してください。許可されていない場合は、ツールを無効にする手順に従ってください。

アプリケーション学習の有効化

グループまたは場所に対して、学習済みアプリケーションを有効にできます。これにより、クライアントコンピュータで実行するアプリケーションに関する情報が収集されます。その後クライアントは、実行されるすべてのアプリケーションを追跡し、そのデータを管理サーバーに送信します。

学習済みアプリケーションデータは個々の Symantec Endpoint Protection クライアントから管理サーバーに転送されるため、この Symantec Endpoint Protection Manager は、このデータが処理され、SQL Server データベースに格納されるようにするための処理の大半を担っています。学習済みアプリケーションデータを転送するシステムの数や、環境内で実行される大規模なアプリケーションの数が多いほど、この Symantec Endpoint Protection Manager がより多くの情報を一時的に保存して処理する必要があります。これにより、動作状態データやセキュリティログデータなど、その他の SEP クライアントデータについて、待機時間が長くなる可能性があります。非常にビジーな環境では、これにより、すでにリソースが不足している SEPM で CPU またはメモリの問題が発生する可能性があります。

NOTE

Mac および Linux クライアントでは、学習済みアプリケーションをサポートされていません。

グループに対してアプリケーション学習を有効にするには

1. コンソールで、[クライアント] をクリックし、グループを選択して、[ポリシー] をクリックします。
2. [ポリシー] タブで、[通信の設定] をクリックします。
3. [通信設定] ダイアログボックスで、[クライアントコンピュータ上で実行するアプリケーションを学習する] にチェックマークを付けて、[OK] をクリックします。

場所に対してアプリケーション学習を有効にするには

1. コンソールで、[クライアント] をクリックし、グループを選択して、[ポリシー] をクリックします。
2. [ポリシー] タブで、場所を選択し、[場所固有の設定] を展開します。
3. [通信の設定] の右側で、[タスク] をクリックし、[グループ通信設定を使う] のチェックマークを外して、[設定の編集] をクリックします。
4. [<場所名> の通信設定] ダイアログボックスで、[クライアントコンピュータ上で動作するアプリケーションを学習する] にチェックマークを付けて、[OK] をクリックします。

サイトに対してアプリケーション学習を有効にするには

1. コンソールで、[管理者]、[サーバー]、[サイトプロパティの編集] の順にクリックします。
2. [全般] タブで、[クライアントが実行するすべてのアプリケーションを追跡する] にチェックマークを付けます。
3. デフォルトデータベースのサイズを減らすには、[Delete learned application data after x days (x 日後に学習済みアプリケーションデータを削除)] にチェックマークを付けます。管理サーバーデータベースの更新に関して問題が発生した場合は、「7」と入力することをお勧めします。
4. [OK] をクリックします。

グループまたは場所の各クライアントでアプリケーションが実行されている場合、管理者の電子メールアドレスに通知を送信するように設定できます。

管理者通知の設定

クライアントコンピュータで動作するアプリケーションとサービスの監視

すべてのポリシーに共通なタスクの実行

コンピュータで実行される学習済みアプリケーションに関する情報の検索

管理サーバーがクライアントから学習済みアプリケーションのリストを受信したら、クエリーを実行してアプリケーションの詳細を調べることができます。たとえば、権限のないアプリケーションを使っているすべてのクライアントコンピュータを調べることができます。その後、ファイアウォールルールを作成して、クライアントコンピュータ上のアプリケーションを遮断できます。または、クライアントコンピュータをアップグレードして、最新バージョンの Microsoft Word を使うようにすることもできます。どの種類のポリシーからも [アプリケーションの検索] タスクを使うことができます。

NOTE

Mac クライアントは Mac コンピュータで実行されるアプリケーションとサービスを監視しません。

アプリケーションは次の方法で検索できます。

- アプリケーションごと

検索対象を、特定のアプリケーションやアプリケーションの詳細（名前、ファイルフィンガープリント、パス、サイズ、バージョン、前回の修正日時など）に制限できます。

- クライアントまたはクライアントコンピュータごと

特定のユーザーまたは特定のコンピュータが実行しているアプリケーションを検索できます。たとえば、コンピュータの IP アドレスを基準として検索できます。

ファイアウォールルールに追加するアプリケーション名について、ファイアウォールポリシーで直接検索することもできます。

アプリケーションについての情報の定義

NOTE

[検索] フィールドの情報はクライアントが実行するすべてのアプリケーションを追跡する機能を有効にするまで収集されません。各グループまたは場所の [通信の設定] ダイアログボックスにある [クライアント] ページに移動すると、この機能を有効にできます。

コンピュータで実行されるアプリケーションに関する情報を検索するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシー] ページの [タスク] で、[アプリケーションの検索] をクリックします。
3. [アプリケーションの検索] ダイアログボックスの [アプリケーションを検索する場所] フィールドの右側で、[参照] をクリックします。
4. [グループまたは場所の選択] ダイアログボックスで、表示するアプリケーションが存在するクライアントのグループを選択し、[OK] をクリックします。
一度に指定できるグループは 1 つだけです。
5. [サブグループを検索する] にチェックマークを付けていることを確認します。
6. 次のいずれかの処理を実行します。
 - ユーザーまたはコンピュータの情報に基づいて検索するには、[クライアント/コンピュータ情報に基づく] をクリックする
 - アプリケーションに基づいて検索するには、[アプリケーションに基づく] をクリックする
7. [検索フィールド] の下の空のセルをクリックし、リストから検索基準を選択します。
[検索フィールド] セルに、選択したオプションに対する基準が表示されます。これらの基準について詳しくは [ヘルプ] を参照してください。
8. [比較演算子] の下の空のセルをクリックし、演算子を 1 つ選択します。
9. [値] の下の空のセルをクリックし、値を選択または入力します。
[値] セルでは、[検索フィールド] セルで選択した基準に応じて、入力形式が指定されるか、ドロップダウンリストから値を選択できます。
10. 検索基準を追加するには、2 つ目の行をクリックし、[検索フィールド]、[比較演算子]、[値] の各セルに情報を入力します。
検索基準の複数の行に入力した場合、すべての条件に一致するクエリーを実行します。
11. [検索] をクリックします。
12. [クエリー結果] の表で、次のいずれかのタスクを行います。
 - スクロール矢印をクリックして、行や列をさらに表示する
 - [前へ] や [次へ] をクリックし、情報の画面をさらに表示する
 - 行を選択して [詳細の表示] をクリックし、アプリケーションの追加情報を表示する

結果はファイルにエクスポートしないと保存されません。

13. クエリー結果を削除するには、[すべてを消去] をクリックします。

14. [閉じる] をクリックします。

クライアントコンピュータで動作するアプリケーションとサービスの監視

すべてのポリシーに共通なタスクの実行

ファイアウォール保護の管理

ファイアウォールは、ファイアウォールポリシーで指定した着信ネットワークトラフィックおよび発信ネットワークトラフィックを許可します。Symantec Endpoint Protection ファイアウォールポリシーにはルールおよび保護設定が含まれ、そのほとんどは有効と無効を切り替えられ、設定できます。

Table 74: ファイアウォール保護を管理する省略可能なタスク

タスク	説明
ファイアウォール保護の理解	ファイアウォール保護を設定する前に、ファイアウォールに精通しておく必要があります。 ファイアウォールのしくみ Symantec Endpoint Protection ファイアウォールについて
ファイアウォールポリシーの作成	Symantec Endpoint Protection は、デフォルトのファイアウォールポリシーをインストールします。デフォルトのポリシーを修正することも、新しいポリシーを作成することもできます。 ポリシーのファイアウォールルールとファイアウォール保護設定を設定する前に、ポリシーを作成しておく必要があります。 ファイアウォールポリシーの作成
ファイアウォールルールの作成およびカスタマイズ	ファイアウォールルールとは、ファイアウォールで、悪質な攻撃からクライアントコンピュータを保護する方法を制御するポリシーコンポーネントです。 デフォルトのファイアウォールポリシーには、デフォルトのファイアウォールルールが含まれます。 また、新しいポリシーを作成すると、Symantec Endpoint Protection によりデフォルトのファイアウォールルールが与えられます。ただし、デフォルトのルールを修正することも、新しいルールを作成することもできます。 新しいファイアウォールルールの追加 ファイアウォールルールのカスタマイズ
ファイアウォール保護設定の有効化	ファイアウォールがある特定の操作を完了した後、制御はいくつかのコンポーネントに渡されます。各コンポーネントは異なる種類のパケット分析を実行するように設計されています。 ルールの追加ではなくネットワークサービスのための通信の有効化 攻撃側コンピュータへの接続の自動遮断 コンピュータに対する外部からのステルス攻撃の防止 Windows ファイアウォールの無効化 ピアツーピア認証の設定によるリモートコンピュータの遮断
ファイアウォール保護の監視	定期的に、コンピュータのファイアウォール保護の状態を監視してください。 エンドポイント保護の監視

コンソールを使った、クライアントコンピュータでのコマンドの実行

混合制御のファイアウォール設定

ファイアウォールのしくみ

ファイアウォールは、以下のタスクをすべて行います。

-
- 権限がないユーザーが、インターネットに接続した組織内のコンピュータおよびネットワークにアクセスできないようにする
 - 使用中のコンピュータとインターネット上の他のコンピュータ間の通信を監視する
 - コンピュータ上の情報へのアクセス試行を許可または遮断するシールドを作成する
 - 他のコンピュータから接続の試みがあることを警告する
 - 他のコンピュータに接続するコンピュータのアプリケーションによって接続の試みがあったことを警告する

ファイアウォールは、インターネット上で送受信されるデータの packets を調べます。Packet は 2 つのコンピュータ間の情報の流れの一部である個別のデータ単位です。Packet は送信先で組み立てられ連続したデータストリームとして表示されます。

Packet はデータについての次の情報を含んでいます。

- 発生元のコンピュータ
- 意図される受信者または複数の受信者
- Packet データの処理方法
- Packet を受信するポート

ポートはインターネットから受信するデータのストリームを分割するチャネルです。コンピュータで動作するアプリケーションはポートで応答準備を行います。アプリケーションはポートに送られるデータを受け入れます。

ネットワーク攻撃は脆弱なアプリケーションの弱点を利用します。攻撃者はこうした弱点を利用して悪質なプログラムコードが含まれた Packet をポートに送信します。脆弱なアプリケーションがポートで応答準備を行うとき、攻撃者は悪質なコードによってコンピュータへアクセスできるようになります。

Symantec Endpoint Protection ファイアウォールについて

Symantec Endpoint Protection ファイアウォールはファイアウォールポリシーとルールを使って、ネットワークトラフィックを許可または遮断します。Symantec Endpoint Protection にはオフィス環境向けのデフォルトのファイアウォールルールとファイアウォールの設定を含んだデフォルトのファイアウォールポリシーが用意されています。オフィス環境は通常は企業ファイアウォール、境界パケットフィルタ、ウイルス対策サーバーの保護下にあります。そのため、限定的な境界保護しか利用できないほとんどのホーム環境よりも通常は安全です。

ファイアウォールルールは悪質なインバウンドトラフィックとアウトバウンドトラフィックからクライアントコンピュータを保護する方法を制御します。ファイアウォールはすべてのインバウンドとアウトバウンドの Packet をこれらのルールと照合して自動的に検査します。次にファイアウォールはルールで指定した情報に基づく Packet を許可または遮断します。コンピュータが別のコンピュータへ接続を試みると、ファイアウォールは接続の種類とファイアウォールルールのリストを比較します。ファイアウォールはすべてのネットワークトラフィックのステートフルインスペクションも使います。

コンソールの初回のインストール時に、各グループに対してデフォルトのファイアウォールポリシーが自動的に追加されます。

新しい場所を追加するたびに、コンソールによってファイアウォールポリシーがデフォルトの場所に自動的にコピーされます。

管理者はユーザーによるファイアウォールルールとファイアウォール設定の変更を許可するか禁止するかによって、ユーザーが行うクライアントの管理操作のレベルを決定します。ユーザーがクライアントを操作できるのは、クライアントが新しいネットワーク接続と問題の可能性について通知するときだけです。または、ユーザーインターフェースをすべて利用することもできます。

デフォルトのファイアウォール設定を使ってクライアントをインストールできます。ほとんどの場合その設定を変更する必要はありません。ただし、ネットワークを詳しく理解しているユーザーは、クライアントのファイアウォールをさまざまに変更してクライアントコンピュータの保護を微調整できます。

バージョン 14.2 以降、Mac クライアントは管理下クライアントに対してのみファイアウォールを提供します。ユーザーは、管理者がクライアント制御を許可している場合にのみ、ファイアウォールを有効または無効にできます。これは

Mac のオペレーティングシステムファイアウォールとは異なるネットワーク層で動作するため、両方を有効にして並列で実行できます。

Mac クライアントのファイアウォールの設定について

ファイアウォール保護の管理

ファイアウォールのしくみ

ファイアウォールでのステートフルインスペクションの使い方

セキュリティポリシーの種類

Mac クライアントのファイアウォールの設定について

Mac 用の Symantec Endpoint Protection クライアントに含まれているファイアウォールの設定は、次のとおりです。

- ファイアウォールのスマートルール
- カスタムファイアウォールルール

これらの設定は、つの Symantec Endpoint Protection Manager 管理者のみが構成できます。ファイアウォールは、管理下クライアントでのみ利用できます。

ファイアウォールは、バージョン 14.2 以降の Mac 用 Symantec Endpoint Protection クライアントに含まれています。

Table 75: ファイアウォールの設定

設定の種類	説明
ファイアウォールのスマートルール	ファイアウォールのスマートルールは、一般的な種類の攻撃を防ぐための保護を提供します。これにより、特定のプロトコルに基づく初期要求を Mac が行うときに、そのプロトコルに基づくトラフィックが許可されます。 保護設定には、次のものが含まれます。 • ポートスキャン検出 • サービス拒否検出 • MAC 詐称対策 • 自動的に攻撃者の IP アドレスを遮断する トラフィックプロトコルには次のものが含まれます。 • スマート DHCP • スマート DNS Mac 用 Symantec Endpoint Protection ファイアウォールは、オペレーティングシステムの組み込みファイアウォールとは統合しません。そうではなく、並列で実行されます。オペレーティングシステムファイアウォールはアプリケーション層で検査しますが、Symantec Endpoint Protection ファイアウォールは下位レベル (ネットワークと伝送) で検査します。 Mac 用 Symantec Endpoint Protection ファイアウォールは、ピアツーピア遮断ルールは提供しませんが、カスタムファイアウォールルールによってこれらを部分的に作成することはできます。
カスタムファイアウォールルール	カスタムファイアウォールルールにより、管理者はネットワークトラフィックの多様な属性に関わるルールを作成できます。

ファイアウォール保護の管理

ファイアウォールポリシーの作成

Symantec Endpoint Protection にはオフィス環境向けのデフォルトのファイアウォールのルールと設定を含むデフォルトのファイアウォールポリシーが用意されています。オフィス環境は通常は企業ファイアウォール、境界パケットフィルタ、ウイルス対策サーバーの保護下にあります。そのため、限定的な境界保護しか利用できないほとんどのホーム環境よりも通常は安全です。

コンソールの初回のインストール時に、各グループに対してデフォルトのファイアウォールポリシーが自動的に追加されます。

NOTE

デフォルトのファイアウォールポリシーの名前を変更すると、アップグレードでポリシーが更新されない場合があります。デフォルトのファイアウォールポリシー内のデフォルトのルールの名前を変更した場合も同様の問題が生じる可能性があります。

新しい場所を追加するたびに、コンソールによってファイアウォールポリシーがデフォルトの場所に自動的にコピーされます。デフォルトの保護が適切でない場合は、ホームページやカスタマーサイトなどの場所ごとにファイアウォールポリシーをカスタマイズできます。デフォルトのファイアウォールポリシーが必要ない場合は、それを編集することも別の共有ポリシーに置換することもできます。

「[ファイアウォールポリシーを作成する方法](#)」で、新しいファイアウォールポリシーを設定する場合に実行できるタスクについて説明します。最初にファイアウォールポリシーを追加する必要があります。その後の残りのタスクは省略可能で、任意の順序で完了できます。

Table 76: ファイアウォールポリシーを作成する方法

タスク	説明
新しいファイアウォールルールを追加する	ファイアウォールルールは、ファイアウォールが悪質な着信トラフィックとアプリケーションからクライアントコンピュータをどのように保護するかを制御するポリシーコンポーネントです。ファイアウォールはこれらのルールを基準にして、すべての着信パケットと発信パケットを自動的に検査します。ファイアウォールはルールで指定された情報に基づいてパケットを許可または遮断します。デフォルトルールを修正すること、新しいルールを作成すること、デフォルトルールを無効にすることが可能です。 新しいファイアウォールポリシーを作成すると、Symantec Endpoint Protection によってデフォルトのファイアウォールルールが提供されます。このルールは、デフォルトで有効になります。 新しいファイアウォールルールの追加
アプリケーションへのアクセスが遮断されたことをユーザーに伝える通知を有効にしてカスタマイズする	アクセスしようとしているアプリケーションが遮断されていることを知らせる通知を、ユーザーに送信できます。 これらの設定はデフォルトで無効になっています。 アプリケーションへのアクセスが遮断されていることに関するユーザーへの通知
自動ファイアウォールルールを有効にする	特定のネットワークサービス間の通信を自動的に許可するオプションを有効にできます。これらのオプションを使うと、それらのサービスを明示的に許可するルールを作成する必要がなくなります。トラフィックの設定を有効にすることで NetBIOS とトークンリングを使って通信するトラフィックの検出と遮断も実行できます。 トラフィックのプロトコルのみがデフォルトで有効になります。 ルールの追加ではなくネットワークサービスのための通信の有効化 Symantec Endpoint Protection クライアントがネットワーク攻撃を検出すると、接続を自動的に遮断してクライアントコンピュータの安全を確保できます。クライアントはアクティブレスポンスをアクティブ化して、クライアントと攻撃側コンピュータの間のすべての通信を一定期間自動的に遮断します。攻撃側コンピュータの IP アドレスは単一の場所で遮断されます。 このオプションはデフォルトでは無効になっています。 攻撃側コンピュータへの接続の自動遮断
保護とステルスの設定を指定する	クライアントに対する潜在的な攻撃を検出してログに記録し、詐称の試みを遮断する設定を有効にできます。外部からの攻撃によってクライアントに関する情報が検出されないようにする設定を有効にできます。 コンピュータに対する外部からのステルス攻撃の防止 保護オプションとステルスオプションすべて、デフォルトでは無効になります。

タスク	説明
Symantec Endpoint Protection ファイアウォールを Windows ファイアウォールと統合する	Symantec Endpoint Protection が Windows ファイアウォールを無効にする条件を指定できます。Symantec Endpoint Protection をアンインストールするとき、Symantec Endpoint Protection は Windows ファイアウォールの設定を、Symantec Endpoint Protection がインストールされる前の状態に復元します。 デフォルト設定では、Windows ファイアウォールは一度だけ無効にされ、Windows ファイアウォール無効のメッセージが無効にされます。 Windows ファイアウォールの無効化
ピアツーピア認証を設定する	ピアツーピア認証を使って、リモートクライアントコンピュータ（ピア）が、同じ企業ネットワーク内の別のクライアントコンピュータ（認証子）に接続するのを許可することができます。認証子は、リモートコンピュータがホストインテグリティ検査に合格するまで、一時的にリモートコンピュータからの TCP および UDP のインバウンドトラフィックを遮断します。 このオプションはデフォルトでは無効になっています。 ピアツーピア認証の設定によるリモートコンピュータの遮断

ファイアウォール保護を有効にすると、ポリシーは IP ベースのインバウンドとアウトバウンドのネットワークトラフィックをすべて許可しますが、次の例外があります。

- デフォルトのファイアウォール保護は、すべてのリモートシステムとのインバウンドとアウトバウンドの IPv6 トラフィックを遮断します。

NOTE

IPv6 はインターネットで使われるネットワーク層プロトコルです。Microsoft Vista が動作するコンピュータにクライアントをインストールすると、イーサネットプロトコルの種類が IPv6 のトラフィックを遮断する複数のデフォルトルールが [ルール] リストに含まれます。デフォルトのルールを削除する場合は、IPv6 を遮断するルールを作成する必要があります。

- デフォルトのファイアウォール保護は、攻撃でよく使われるいくつかのプロトコルのインバウンド接続を制限します（たとえば、Windows ファイル共有）。
内部ネットワーク接続は許可され、外部ネットワークは遮断されます。

ファイアウォール保護の管理

リモートクライアントのファイアウォールポリシー設定のベストプラクティス

ファイアウォールルールの管理

ファイアウォールルールは、ファイアウォールが悪質な着信トラフィックとアプリケーションからコンピュータをどのように保護するかを制御します。ファイアウォールは有効にしたルールを基準にして、すべての着信パケットと発信パケットを検査します。ファイアウォールはファイアウォールルールで指定する条件に基づいてパケットを許可または遮断します。

Symantec Endpoint Protection クライアントには、コンピュータを保護するデフォルトのファイアウォールルールが含まれています。ただし、管理者が許可する場合、またはクライアントが管理外である場合は、追加の保護のためファイアウォールルールを修正できます。

Symantec Endpoint Protection はデフォルトのルールを含むデフォルトのファイアウォールポリシーとともにインストールされます。新しいファイアウォールポリシーを作成するときには、Symantec Endpoint Protection によってデフォルトのファイアウォールルールが提供されます。管理者が許可する場合、またはクライアントが管理外である場合は、デフォルトのルールを修正したり、新しいファイアウォールルールを作成したりできます。

ポリシーには少なくとも 1 つのルールを含める必要があります。しかし、必要な数のルールを利用できます。ルールは必要に応じて有効と無効を切り替えることができます。たとえば、ルールを無効にしてトラブルシューティングを実行し、終了したら有効にできます。

「[ファイアウォールルールの管理](#)」では、ファイアウォールルールを管理するために知っておく必要がある事柄を説明します。

Table 77: ファイアウォールルールの管理

タスク	説明
ファイアウォールルールがどのように機能し、どのようなもので構成されているかについて理解する	ファイアウォールルールを修正する前に、ファイアウォールルールがどのように機能するかについての次の情報を理解してください。 - ルールの順序を指定して、最も制限の厳しいルールが最初に評価され、最も制限の緩いルールが最後に評価されるようにする方法 ファイアウォールルール、ファイアウォール設定、侵入防止の処理順について - クライアントは、ネットワーク接続の状態を追跡するステートフルインスペクションを使うこと ファイアウォールでのステートフルインスペクションの使い方 - ファイアウォールルールを構成するファイアウォールのコンポーネント これらのトリガと、トリガの最適な使用方法について理解すれば、ファイアウォールルールをカスタマイズしてクライアントとサーバーを保護できます。 クライアント上のファイアウォールルールの要素
新しいファイアウォールルールを追加する	次のタスクを実行して、ファイアウォールルールを管理できます。 - コンソールからいくつかの方法を使って、新しいファイアウォールルールを追加します。 1つの方法では、デフォルト設定を適用した空白のルールを追加できます。その他の方法では、新しいルールの作成手順をガイドするウィザードが表示されます。 Symantec Endpoint Protection がデフォルトでインストールするルールに、自分のルールを追加します。 クライアント上のファイアウォールルールの追加 - ファイアウォールルール基準のいずれかを変更して、ルールをカスタマイズします。 - 別のファイアウォールポリシーのファイアウォールルールをエクスポートおよびインポートします。 クライアント上でのファイアウォールルールのエクスポートまたはインポート - ファイアウォールルールをコピーして貼り付けます。 作成するルールに似ている既存のルールをコピーすると、新しいファイアウォールルールを作成する時間を節約できます。その後、コピーしたルールを修正して、必要を満たせます。
ファイアウォールルールをカスタマイズする	新しいルールを作成した後、またはデフォルトのルールをカスタマイズする場合は、ファイアウォールルールの任意の基準を修正できます。

新しいファイアウォールルールの追加

新しいファイアウォールルールは、次のいずれかの方法で作成できます。

空白ルール	空白ルールはすべてのトラフィックを許可します。 新しい空白のファイアウォールルールを追加するには
ファイアウォールルールの追加ウィザード	ファイアウォールルールの追加ウィザードでルールを追加する場合は、必ずルールを設定してください。このウィザードでは、複数の基準を持つ新しいルールは設定しません。 ウィザードを使用してファイアウォールルールを追加するには

可能な限りインバウンドとアウトバウンドの両方のトラフィックをルールで指定してください。HTTP などのトラフィックにはインバウンドルールを作成する必要はありません。Symantec Endpoint Protection クライアントは TCP トラフィックにステートフルインスペクションを使います。そのため、クライアントが開始するリターントラフィックをフィルタ処理するルールを必要としません。

新しいファイアウォールルールを作成すると、自動的に有効になります。コンピュータまたはアプリケーションに対する特定のアクセスを許可する必要がある場合はファイアウォールルールを無効にできます。ルールは継承したすべてのポリシーについて無効になります。

ルールが共有ポリシーの場合、ルールはすべての場所について無効になり、場所固有のポリシーの場合は 1 つの場所についてのみ無効になります。

NOTE

ファイアウォールがルールを処理するにはルールを有効にする必要があります。

1. 新しい空白のファイアウォールルールを追加するには、コンソールで [ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。
バージョン 14.2 より前には、[Mac の設定] のオプションはありません。
3. [ルール] タブの [ルール] リストで、[空白ルールの追加] をクリックします。
4. オプションで、必要に応じてファイアウォールルール基準を変更できます。
5. ルールの設定を完了したら、[OK] をクリックします。
6. ウィザードを使用してファイアウォールルールを追加するには、コンソールで [ファイアウォールポリシー] を開きます。
7. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。
[ルール] タブの [ルール] リストで、[ルールの追加] をクリックします。
8. 各画面のオプションを入力して [次へ] をクリックします。
9. [完了] をクリックします。
オプションで、必要に応じてファイアウォールルール基準を変更できます。

ファイアウォールルールのカスタマイズ

ファイアウォールでのステートフルインスペクションの使い方

ファイアウォールのサーバールールとクライアントルールについて

ルールはサーバールールとクライアントルールのいずれかに分類されます。サーバールールは、Symantec Endpoint Protection Manager で作成して Symantec Endpoint Protection クライアントにダウンロードしたルールです。クライアントルールはユーザーがクライアントで作成したルールです。

Mac クライアントでのすべてのルールは、サーバールールです。Mac ユーザーには、Mac クライアントのクライアントルールを作成するためのオプションはありません。

ファイアウォールは、バージョン 14.2 以降の Mac クライアントに導入されました。

クライアントのユーザー制御レベルとユーザーによるファイアウォールルールに対する介入の関係を「[ユーザー制御レベルとルールの状態](#)」に示します。

Table 78: ユーザー制御レベルとルールの状態

ユーザー制御レベル	ユーザーの介入
サーバー制御	Windows クライアントはサーバールールを受信しますがユーザーはそれらのルールを表示できません。ユーザーはクライアントルールを作成できない Mac クライアントでは、ユーザーはファイアウォールを有効または無効にできません。
混合制御	Windows クライアントはサーバールールを受信します。ユーザーはクライアントルールを作成できる。作成したルールはサーバールールやクライアントのセキュリティの設定とマージされる Mac クライアントは、ユーザーがファイアウォールを有効または無効にすることを許可または禁止します。詳細設定がサーバー制御またはクライアント制御に設定されるかどうかによって異なります。

ユーザー制御レベル	ユーザーの介入
クライアント制御	クライアントはサーバールールを受信しない。ユーザーはクライアントルールを作成できる。つの Symantec Endpoint Protection Manager 管理者はクライアントルールを表示できません。 Mac クライアントではユーザーはファイアウォールを有効または無効にできます。

クライアントコンピュータの保護をユーザーが無効にできない設定

ファイアウォールがサーバールール、クライアントルール、クライアント設定を処理する順序を「[サーバールールとクライアントルールの処理の優先度](#)」に示します。

Table 79: サーバールールとクライアントルールの処理の優先度

優先度	ルールの種類または設定
1 番目	優先度レベルが高いサーバールール ([ルール] リストで青色の線の上に表示されるルール)
2 番目	クライアントルール
3 番目	優先度レベルが低いサーバールール ([ルール] リストで青色の線の下に表示されるルール) クライアントでは、青色の線の下に表示されるサーバールールはクライアントルールの後に処理される
4 番目	クライアントのセキュリティの設定
5 番目	クライアントのアプリケーション固有の設定

クライアントでは、ユーザーはクライアントルールやセキュリティの設定を修正できますが、サーバールールは修正できません。

WARNING

クライアントが混合制御の場合、ユーザーはすべてのトラフィックを許可するクライアントルールを作成できます。このルールは青色の線の下に表示されるすべてのサーバールールに優先します。

ファイアウォールルールの管理

ファイアウォールルールの順序の変更

クライアントコンピュータの保護をユーザーが無効にできない設定

ファイアウォールルール、ファイアウォール設定、侵入防止の処理順について

ファイアウォールルールには、ルールリストの優先度の最も高いものから最も低いものまでの連続した順序が付けられます。1 つ目のルールでパケットの処理方法が指定されていない場合は、2 つ目のルールで検査されます。この処理はファイアウォールが一致するものを検出するまで続きます。一致するルールが見つかったら、ファイアウォールではそのルールによって指定された処理が行われます。それよりも優先度の低いルールは検査されません。たとえば、最初のルールがすべてのトラフィックを遮断し、次のルールがすべてのトラフィックを許可する場合、クライアントはすべてのトラフィックを遮断します。

排他的にルールの順序を変更できます。最も制限の厳しいルールが最初に評価され、最も制限の緩いルールが最後に評価されます。たとえば、トラフィックを遮断するルールはルールリストの先頭の近くに配置します。リストの後ろにあるルールではトラフィックを許可します。

ルールリストには青色の分割線が含まれます。この分割線は次の状況においてルールの優先度を設定します。

- サブグループがルールを親グループから継承する場合
- Windows クライアントを混合制御に設定する場合。ファイアウォールはサーバールールとクライアントルールの両方を処理する

ルールベースを作成するためのベストプラクティスは以下の順序でルールを含んでいます。

1 番目	すべてのトラフィックを遮断するルール。
2 番目	すべてのトラフィックを許可するルール。
3 番目	特定のコンピュータを許可または遮断するルール。
4 番目	特定のアプリケーション、ネットワークサービス、ポートを許可または遮断するルール。

「[処理順](#)」に、ルール、ファイアウォール設定、侵入防止設定がファイアウォールで処理される順序を示します。

Table 80: 処理順

優先度	設定
1 番目	カスタム IPS シグネチャ
2 番目	侵入防止の設定、トラフィックの設定、ステルス設定
3 番目	組み込みルール
4 番目	ファイアウォールルール
5 番目	ポートスキャンチェック
6 番目	LiveUpdate でダウンロードした IPS シグネチャ

継承したファイアウォールルールについて

サブグループのポリシーは親グループで有効なファイアウォールルールのみ継承できます。ルールを継承した場合、それらのルールを無効にできますが修正はできません。新しいルールは親グループのポリシーに追加されるため、継承先のポリシーに自動的に追加されます。

継承したルールが [ルール] リストに表示される場合は、バージョン 14.x では斜体、バージョン 12.1.x では紫色で網掛けされます。継承したルールは、つの Symantec Endpoint Protection Manager 管理者として作成したルールの上 (青色の線の上) に追加されます。青色の線の下側では、継承したルールは作成したルールの下に追加されます。

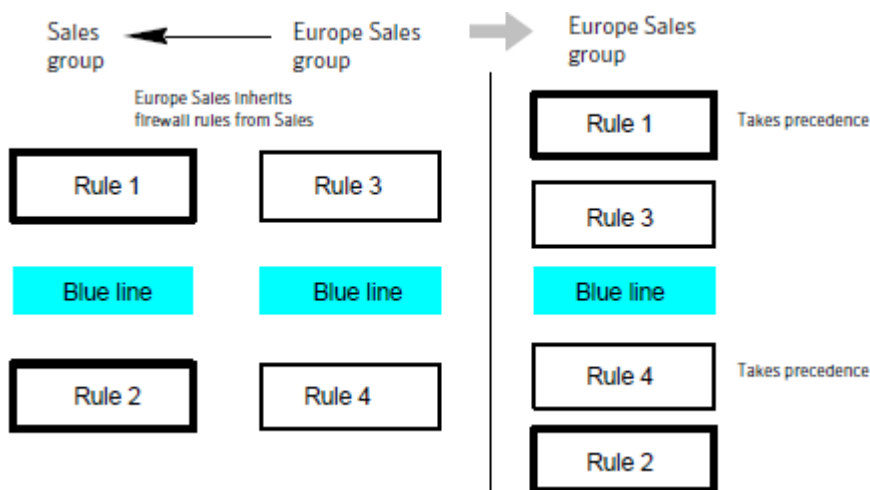
ファイアウォールポリシーはデフォルトルールも継承するため、サブグループのファイアウォールポリシーは 2 つのデフォルトルールを持つことがあります。一方のデフォルトルールを削除すると便利です。

継承したルールを取り除く場合は、ルールを削除するのではなく継承を除去します。選択したルールではなく継承したすべてのルールを除去する必要があります。

ファイアウォールは、継承したファイアウォールルールを [ルール] リストで次のように処理します。

青色の分割線の上側	管理者が作成したルールよりもポリシーが継承したルールが優先されます。
青色の分割線の下側	ポリシーが継承したルールよりも管理者が作成したルールが優先されます。

以下の図は、サブグループが親グループからルールを継承した場合に、[ルール] リストでルールがどのように順序付けられるかを示しています。この例では、Sales グループが親グループです。Europe Sales グループは Sales グループから継承します。



ファイアウォールルールの管理

親グループから継承したファイアウォールルールの追加

親グループから継承したファイアウォールルールの追加

親グループからルールを継承することで、ファイアウォールポリシーにファイアウォールルールを追加できます。親グループからルールを継承するには、サブグループのポリシーが非共有ポリシーである必要があります。

NOTE

グループがすべてのポリシーを親グループから継承する場合、このオプションは使用できません。

親グループから継承したファイアウォールルールを追加するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。

バージョン 14.2 より前には、[Mac の設定] のオプションはありません。

3. [ルール] タブで、[親グループからファイアウォールルールを継承する] にチェックマークを付けます。

継承したルールを除去するには、[親グループからファイアウォールルールを継承する] のチェックマークをはずします。

4. [OK] をクリックします。

ポリシーの編集

継承したファイアウォールルールについて

ファイアウォールルールの管理

ファイアウォールルールの順序の変更

ファイアウォールはファイアウォールルールのリストを上から順に処理します。ファイアウォールがファイアウォールルールを処理する方法を決めるにはルールの順序を変更します。

Symantec Endpoint Protection クライアントで場所の切り替えが使用されている場合にファイアウォールルールの順序を変更すると、この変更は現在の場所の順序にのみ影響します。

NOTE

保護を改善するには、最も制限の厳しいルールを最初に、最も制限の緩いルールを最後に配置します。

ファイアウォールルール、ファイアウォール設定、侵入防止の処理順について

ファイアウォールルールの順序を変更するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページで、[ルール] をクリックして、移動するルールを選択します。
3. 次のいずれかのタスクを行います。

- このルールを上のルールよりも前に処理するには、[上に移動] をクリックする
- このルールを下のルールよりも後に処理するには、[下に移動] をクリックする

4. [OK] をクリックします。

ファイアウォールルールの順序を変更するには

5. クライアントのサイドバーで、[状態] をクリックします。
6. [ネットワークとホスト悪用防止] の横で、[オプション]、[ファイアウォールルールの設定] の順にクリックします。
7. [ファイアウォールルールの設定] ダイアログボックスで、移動するルールを選択します。
8. 次のいずれかの処理を実行します。
 - 選択しているルールを、上のルールよりも前にファイアウォールに処理させる場合は、上向きの矢印をクリックします。
 - 選択しているルールを、下のルールよりも後にファイアウォールに処理させる場合は、下向きの矢印をクリックします。
9. ルールの移動が終わったら、[OK] をクリックします。

ファイアウォールルールの管理

ファイアウォールでのステートフルインスペクションの使い方

ファイアウォール保護は、現在の接続の追跡にステートフルインスペクションを使います。ステートフルインスペクションは、送信元と送信先の IP アドレス、ポート、アプリケーション、およびその他の接続情報を追跡します。クライアントは、ファイアウォールルールを検査する前に、接続情報に基づいてトラフィックフローを決定します。

たとえば、ファイアウォールルールでコンピュータが Web サーバーに接続することが許可されている場合、ファイアウォールは接続情報をログに記録します。サーバーが応答すると、ファイアウォールは、Web サーバーからコンピュータに応答が送信されるものと判断します。ルールベースを検査することなく、接続を開始したコンピュータに Web サーバーのトラフィックが送信されることを許可します。ファイアウォールが接続をログに記録する前に、ルールが最初のアウトバウンドトラフィックを許可する必要があります。

ステートフルインスペクションにより、新しいルールを作成する必要性がなくなります。1 方向で開始されるトラフィックについては、両方向のトラフィックを許可するルールを作成する必要はありません。一方向に開始されるクライアントのトラフィックには、Telnet (ポート 23)、HTTP (ポート 80)、HTTPS (ポート 443) があります。クライアントコンピュータは、このアウトバウンドトラフィックを開始します。これらのプロトコルに対してアウトバウンドトラフィックを許可するルールを作成します。ステートフルインスペクションは、自動的にアウトバウンドトラフィックに応答するリターントラフィックを可能にします。ファイアウォールは事実上ステートフルであるため、特定のパケットの性質ではなく、接続を開始するルールを作成すれば済みます。許可した接続に属するすべてのパケットはそれと同じ接続の一部として暗黙に許可されます。

ステートフルインスペクションは TCP トラフィックを方向付けるすべてのルールをサポートします。

ステートフルインスペクションは、ICMP トラフィックをフィルタ処理するルールをサポートしません。ICMP トラフィックの場合は、両方向のトラフィックを許可するルールを作成する必要があります。たとえば、クライアントが ping コマンドを使い応答を受信するには、両方向の ICMP トラフィックを許可するルールを作成する必要があります。

接続情報を保守する状態テーブルは定期的に消去されることがあります。たとえば、ファイアウォールポリシーの更新を処理するときや Symantec Endpoint Protection サービスを再起動するときに消去されます。

ファイアウォールルールのアプリケーショントリガについて

アプリケーションがトラフィックを許可するルールで定義した唯一のトリガである場合には、ファイアウォールはそのアプリケーションが任意のネットワーク操作を実行することを許可します。重要なのはアプリケーション自体でありアプリケーションが実行するネットワーク操作ではありません。たとえば、Internet Explorer を許可してその他のトリガを定義しないとします。ユーザーは HTTP、HTTPS、FTP、Gopher、Web ブラウザがサポートするその他の任意のプロトコルを使うリモートサイトにアクセスできます。管理者は追加のトリガを定義して通信を許可する特定のネットワークプロトコルとホストを記述できます。

アプリケーションが複数のプロトコルを使えるためアプリケーションベースのルールはトラブルシューティングが困難な場合があります。たとえば、ファイアウォールが FTP を遮断するルールより前に Internet Explorer を許可するルールを処理した場合には、ユーザーは FTP と通信できます。ユーザーはブラウザに FTP ベースの URL (たとえば ftp://ftp.symantec.com) を入力できます。

たとえば、Internet Explorer を許可し、その他のトリガを定義しない場合を考えます。コンピュータユーザーは HTTP、HTTPS、FTP、Gopher、Web ブラウザがサポートするその他の任意のプロトコルを使うリモートサイトにアクセスできます。管理者は追加のトリガを定義して通信を許可するネットワークプロトコルとホストを記述できます。

アプリケーションルールはトラフィックをネットワークレベルで制御するためには使わないでください。たとえば、Internet Explorer の使用を遮断または制限するルールはユーザーが別の Web ブラウザを使っている場合には効果がありません。その他の Web ブラウザが生成するトラフィックは Internet Explorer ルールを除くその他すべてのルールと比較されます。アプリケーションベースのルールはトラフィックを送受信するアプリケーションを遮断するようにルールを設定した場合に、より効果的です。

アプリケーションについての情報の定義

アプリケーションへのアクセスが遮断されていることに関するユーザーへの通知

ファイアウォールルールの管理

攻撃を受けている可能性のあるネットワークアプリケーションの遮断

アプリケーションについての情報の定義

クライアントで動作するアプリケーションに関する情報を定義し、この情報をファイアウォールルールに含めることができます。

次の方法でアプリケーションの特性を定義できます。

- 手動で情報を入力する。
[アプリケーションについての情報を手動で定義するには](#)
 - 学習済みアプリケーションのリストでアプリケーションを検索する。
学習済みアプリケーションリストのアプリケーションはネットワーク上のクライアントコンピュータで動作しているアプリケーションです。
[学習済みアプリケーションリストからアプリケーションを検索するには](#)
1. アプリケーションについての情報を手動で定義するには、コンソールで [ファイアウォールポリシー] を開きます。
 2. [ファイアウォールポリシー] ページの [Windows の設定] で、[ルール] をクリックします。
14.2 より前のバージョンでは、[ファイアウォールポリシー] ページで、[ルール] をクリックします。

-
3. [ルール] タブのルールリストで、変更するルールの [アプリケーション] フィールドを右クリックして、[編集] をクリックします。
 4. [アプリケーションリスト] ダイアログボックスで、[追加] をクリックします。
 5. [アプリケーションの追加] ダイアログボックスで、次の 1 つまたは複数のフィールドに入力します。
 - ファイル名。ファイルパスを含めることができます。
 - ファイルの説明
このフィールドは表示のみの目的で使います。一致条件としては機能しません。
 - ファイルサイズ (バイト数)
 - 前回の修正
 - ファイルフィンガープリント

NOTE

ファイルサイズ、最終変更日、ファイルフィンガープリントでファイアウォールルールを定義するには、ネットワークアプリケーション監視を有効にする必要があります。ネットワークアプリケーション監視が無効になっていると、ルールの処理は [ファイル名] 以外のすべてのフィールドを無視します。

6. [OK] をクリックしてアプリケーション条件を追加します。
7. [OK] をクリックしてアプリケーションリストを保存します。
8. 学習済みアプリケーションリストからアプリケーションを検索するには、[ファイアウォールポリシー] ページで [ルール] をクリックします。
9. [ルール] タブでルールを選択し、[アプリケーション] フィールドを右クリックし、[編集] をクリックします。
10. [アプリケーションリスト] ダイアログボックスで、[追加元] をクリックします。
11. [アプリケーションの検索] ダイアログボックスで、アプリケーションを検索します。
12. [クエリー結果] 表で [アプリケーション] リストにアプリケーションを追加するには、アプリケーションを選択し、[追加]、[OK] の順にクリックします。
13. [閉じる] をクリックします。
14. [OK] をクリックします。

ファイアウォールルールの管理

ポリシーの編集

ファイアウォールルールのアプリケーショントリガについて

攻撃を受けている可能性のあるネットワークアプリケーションの遮断

ネットワークアプリケーション監視はアプリケーションの動作をセキュリティログ内で追跡します。アプリケーションのコンテンツが頻繁に修正される場合は、トロイの木馬によってアプリケーションが攻撃されてクライアントコンピュータが安全でないと考えられます。コンテンツの修正頻度が低い場合にはパッチがインストールされてクライアントコンピュータが安全であると考えられます。この情報を使ってアプリケーションを許可または遮断するファイアウォールルールを作成できます。

クライアントコンピュータ上で動作しネットワークに接続する任意のアプリケーションを検出して監視するようにクライアントを設定できます。ネットワークアプリケーションはトラフィックを送受信します。クライアントはアプリケーションの内容が変更されているかどうかを検出します。

トロイの木馬によってアプリケーションが攻撃された疑いがある場合は、ネットワークアプリケーション監視を使ってアプリケーションを遮断するようにクライアントを設定できます。また、アプリケーションを許可するか遮断するかをユーザーに確認するようにクライアントを設定することもできます。

アプリケーションのコンテンツは次の理由で変化します。

- トロイの木馬がアプリケーションを攻撃した
- アプリケーションが新しいバージョンまたは更新プログラムで更新された

クライアントがアプリケーションを監視しないようにアプリケーションをリストに追加できます。アプリケーションのうち、トロイの木馬攻撃の危険はないと考えられ、パッチが頻繁かつ自動的に更新されるものは除外すると便利です。

また、ネットワークアプリケーションを許可するか遮断するかをユーザーに確認する通知の数を減らすこともできます。

攻撃を受けている可能性のあるネットワークアプリケーションを遮断するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] でグループを選択し、[ポリシー] タブをクリックします。
3. [ポリシー] タブの [場所に依存しないポリシーと設定] で、[ネットワークアプリケーション監視] をクリックします。
4. [グループ名 のネットワークアプリケーション監視] ダイアログボックスで、[ネットワークアプリケーション監視 を有効にする] をクリックします。
5. [アプリケーション変更を検出したとき] ドロップダウンリストで、次のように、クライアント上で動作するアプリケーションに対してファイアウォールが行う処理を選択します。

確認	アプリケーションを許可するか遮断するかをユーザーに確認します。
トラフィックを遮断する	アプリケーションの実行を遮断します。
許可とログ	アプリケーションの実行を許可してセキュリティログに情報を記録します。 ファイアウォールは修正されたアプリケーションに対してのみこの処理を行います。

6. [確認] を選択した場合は、[追加テキスト] をクリックします。
7. [追加テキスト] ダイアログボックスで、標準メッセージの下に表示するテキストを入力し、[OK] をクリックします。
8. アプリケーションを監視対象から除外するには、[監視外アプリケーションリスト] で、次のいずれかのタスクを行います。

アプリケーションを手動で定義するには	[追加] をクリックし、1 つ以上のフィールドに入力して、[OK] をクリックします。
学習済みアプリケーションリストからアプリケーションを定義するには	[追加元] をクリックします。 学習済みアプリケーションリストではネットワークに接続するアプリケーションと接続しないアプリケーションの両方が監視されます。そのため、学習済みアプリケーションリストからはネットワークに接続するアプリケーションだけを選択する必要があります。[監視外アプリケーションリスト] にアプリケーションを追加した後で、アプリケーションを有効または無効にしたり、編集、削除を行うことができます。

9. 有効にするアプリケーションの横にあるボックスにチェックマークを付けます。無効にするにはチェックマークをはずします。
10. [OK] をクリックします。

ファイアウォールルールの管理

アプリケーションへのアクセスが遮断されていることに関するユーザーへの通知

ファイアウォールルールのアプリケーショントリガについて

コンピュータで実行されるアプリケーションに関する情報の検索

クライアントコンピュータで実行するアプリケーションに関する情報の収集

アプリケーションへのアクセスが遮断されていることに関するユーザーへの通知

アクセスしようとしているアプリケーションが遮断されていることを知らせる通知を、ユーザーに送信できます。この通知はユーザーのコンピュータで表示されます。

NOTE

非常に多くの通知を有効にすると、ユーザーを困らせるだけでなく、不安にさせてしまう可能性があります。通知を有効にするときには慎重にしてください。

アプリケーションへのアクセスが遮断されていることについてユーザーに通知するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページで、[ルール] をクリックします。
3. [通知] タブで、[クライアントがアプリケーションを遮断したときにコンピュータの画面に通知を表示する] にチェックマークを付け、必要に応じてカスタムメッセージを追加します。
4. [OK] をクリックします。

ファイアウォールルールの管理

侵入防止とメモリエクスポloit緩和機能のクライアント通知の設定

管理者通知の設定

ファイアウォールルールのホストトリガについて

ホストトリガを定義する場合は、記述するネットワーク接続の両端のホストを指定します。

ホスト間の関係は、従来からネットワーク接続の送信元または送信先と呼ばれます。

ホストの関係は次のいずれかの方法で定義できます。

送信元と送信先	送信元ホストと送信先ホストはトラフィックの方向によって決まります。ある場合にはローカルのクライアントコンピュータが送信元になり、別の場合にはリモートのコンピュータが送信元になります。送信元と送信先の関係はネットワークベースのファイアウォールでより一般的に使われます。
ローカルとリモート	ローカルホストは常にローカルのクライアントコンピュータであり、リモートホストは常にネットワークの別の場所にあるリモートのコンピュータです。このホストの関係の記述は、トラフィックの方向と無関係です。ローカルとリモートの関係はホストベースのファイアウォールでより一般的に使われ、トラフィックも簡単に観察できます。

管理者は複数の送信元ホストと送信先ホストを定義できます。

トラフィックの方向を基準とした送信元の関係と送信先の関係を「[送信元と送信先のホスト間の関係](#)」に示します。



トラフィックの方向を基準としたローカルホストとリモートホストの関係を「[ローカルとリモートのホスト間の関係](#)」に示します。



関係は、文の次の種類によって評価されます。

接続の両端で定義するホスト (送信元と送信先との間)	OR 文
選択したホスト	AND 文

たとえば、単一のローカルホストと複数のリモートホストを定義するルールを考えます。ファイアウォールがパケットを診断するときに、ローカルホストは該当する IP アドレスに一致する必要があります。逆に、そのアドレスの反対側は任意のリモートホストと一致する場合があります。たとえば、ローカルホストと Yahoo.com、Google.com のいずれかとの HTTP 通信を許可するルールを定義できます。単一のルールとして定義しても、2 つのルールとして定義しても同じです。

ホストグループの追加

特定のサーバーとの間で送受信されるトラフィックの遮断

ファイアウォールルールの管理

ホストグループの追加

ホストグループは DNS ドメイン名、DNS ホスト名、IP アドレス、IP アドレス範囲、MAC アドレス、サブネットを 1 つの名前にグループ化したものです。ホストグループの目的はホストのアドレスと名前を再入力しなくても済むようにすることです。たとえば、複数の IP アドレスをファイアウォールルールに 1 つずつ追加することは可能です。しかし、複数の IP アドレスをホストグループに追加することで、グループをファイアウォールルールに追加できるようになります。

ホストグループを使う場合には、グループを使う場所を記述する必要があります。後でホストグループを削除することにした場合は、まずそのホストグループを参照しているすべてのファイアウォールルールからグループを削除する必要があります。

ホストグループを追加すると、[ホスト] リストの末尾にそのグループが表示されます。[ホスト] リストにアクセスするにはファイアウォールルールの [ホスト] フィールドからアクセスします。

ホストグループを追加するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシーコンポーネント] を展開し、[ホストグループ] をクリックします。
3. [タスク] で、[ホストグループの追加] をクリックします。
4. [ホストグループ] ダイアログボックスで、名前を入力し、[追加] をクリックします。
5. [ホスト] ダイアログボックスの [種類] ドロップダウンリストで、ホストを選択します。
6. それぞれのホストの種類に対して適切な情報を入力します。
7. [OK] をクリックします。
8. 必要に応じて、さらにホストを追加します。
9. [OK] をクリックします。

ファイアウォールルールのホストトリガについて

ファイアウォールルールのネットワークサービストリガについて

ネットワークサービスを利用することで、ネットワークに接続するコンピュータはメッセージの送受信、ファイルの共有、印刷を行うことができます。ネットワークサービスは 1 つ以上のプロトコルやポートを使って特定の種類のトラフィックを受け渡します。たとえば、HTTP サービスは TCP プロトコルのポート 80 と 443 を使います。管理者はネットワークサービスを許可または遮断するファイアウォールルールを作成できます。ネットワークサービストリガは記述するネットワークトラフィックに関して重要な 1 つ以上のネットワークプロトコルを識別します。

TCP ベースまたは UDP ベースのサービストリガを定義するときには、示されているネットワーク接続の両側でポートを識別します。通常、ポートはネットワーク接続の送信元または送信先と見なされています。

デフォルトのネットワークサービスリストへのネットワークサービスの追加

ネットワーク内のファイルおよびプリンタを参照できるようにするクライアントの許可 ファイアウォールルールの管理

デフォルトのネットワークサービスリストへのネットワークサービスの追加

ネットワークサービスを利用することで、ネットワークに接続するコンピュータはメッセージの送受信、ファイルの共有、印刷を行うことができます。管理者はネットワークサービスを許可または遮断するファイアウォールルールを作成できます。

ネットワークサービスリストにより、ネットワークサービスを遮断または許可するために作成するファイアウォールルールの、プロトコルとポートを再入力する必要がなくなります。ファイアウォールルールを作成するときは、よく使うネットワークサービスのデフォルトリストからネットワークサービスを選択できます。また、ネットワークサービスをデフォルトリストに追加できます。ただし、管理者はプロトコルの種類やそれが使われるポートに精通している必要があります。

NOTE

IPv4 と IPv6 はインターネットで使われる 2 つのネットワーク層プロトコルです。Windows Vista を実行しているコンピュータにクライアントをインストールすると、イーサネットプロトコルの種類が IPv6 のトラフィックを遮断する複数のデフォルトルールが [ルール] リストに含まれます。デフォルトのルールを削除する場合は、IPv6 を遮断するルールを作成する必要があります。

NOTE

カスタムネットワークサービスはファイアウォールルールを通して追加できます。しかし、そのネットワークサービスはデフォルトリストには追加されません。また、カスタムのネットワークサービスには他のルールからはアクセスできません。

デフォルトのネットワークサービスリストにネットワークサービスを追加するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシーコンポーネント] を展開し、[ネットワークサービス] をクリックします。
3. [タスク] で、[ネットワークサービスの追加] をクリックします。
4. [ネットワークサービス] ダイアログボックスで、サービスの名前を入力し、[追加] をクリックします。
5. [プロトコル] ドロップダウンリストからプロトコルを選択します。

選択したプロトコルに基づいて、オプションが変化します。

6. 適切なフィールドに情報を入力し、[OK] をクリックします。
7. 必要に応じて、1 つ以上のプロトコルを追加します。
8. [OK] をクリックします。

ファイアウォールルールの管理

ファイアウォールルールのネットワークサービストリガについて

ネットワークコンピュータがメッセージ、ファイル、印刷を共有できるかどうかの制御

ネットワーク内のファイルおよびプリンタを参照できるようにするクライアントの許可

ファイアウォールルールのネットワークアダプタトリガについて

ネットワークアダプタを通過する (送信または受信される) トラフィックを遮断または許可するファイアウォールルールを定義できます。

特定の種類のアダプタを定義する場合には、そのアダプタをどう使うか考慮してください。たとえば、ルールがイーサネットアダプタから送信されるアウトバウンド HTTP トラフィックを許可する場合には、同じ種類のすべてのインストール済みアダプタを経由する HTTP を許可します。唯一の例外はローカルホストアドレスも指定した場合です。クライアントコンピュータは複数の NIC を装備したサーバーと複数のネットワークセグメントをブリッジするワークステーションを使う場合があります。特定のアダプタに関連するトラフィックを制御するには、アダプタ自体ではなく各セグメントのアドレス方式を使う必要があります。

ネットワークアダプタリストにより、ファイアウォールルールのアダプタの種類を再入力する必要がなくなります。その代わりに、ファイアウォールルールを作成するときに、一般に使われるネットワークアダプタのデフォルトリストからネットワークアダプタを選択できます。また、ネットワークアダプタをデフォルトリストに追加できます。

ファイアウォールポリシーとルール全体で共有されるデフォルトリストからネットワークアダプタを選択できます。[ポリシーコンポーネント] リスト内のデフォルトリストには最も一般的なアダプタが含まれています。

NOTE

カスタムネットワークアダプタはファイアウォールルールから追加できます。しかし、そのネットワークアダプタはデフォルトリストには追加されません。また、カスタムネットワークアダプタには他のルールからはアクセスできません。

ファイアウォールルールの管理

ネットワークアダプタリストへのカスタムネットワークアダプタの追加

ネットワークアダプタを通過するトラフィックの制御

ネットワークアダプタリストへのカスタムネットワークアダプタの追加

ネットワークアダプタごとに個別のファイアウォールルールを適用できます。たとえば、VPN 経由のトラフィックをオフィスでは遮断し、ホームでは遮断したくない場合に便利です。

ファイアウォールポリシーとルール全体で共有されるデフォルトリストからネットワークアダプタを選択できます。[ポリシーコンポーネント] リスト内のデフォルトリストには最も一般的なアダプタが含まれています。デフォルトリストを使うと、作成するすべてのルールで各ネットワークアダプタを再入力する必要がありません。

ネットワークアダプタリストにより、ファイアウォールルールのアダプタを再入力する必要がなくなります。ファイアウォールルールを作成するときは、よく使うネットワークアダプタのデフォルトリストからネットワークアダプタを選択できます。また、ネットワークアダプタをデフォルトリストに追加できます。

NOTE

カスタムネットワークアダプタはファイアウォールルールから追加できます。しかし、そのネットワークアダプタはデフォルトリストには追加されません。また、カスタムネットワークアダプタには他のルールからはアクセスできません。

ネットワークアダプタリストにカスタムのネットワークアダプタを追加するには

1. コンソールで、[ポリシー]、[ポリシーコンポーネント]、[ネットワークアダプタ] の順に選択します。
2. [タスク] で、[ネットワークアダプタの追加] をクリックします。
3. [ネットワークアダプタ] ダイアログボックスの [アダプタの種類] ドロップダウンリストで、アダプタを選択します。
4. [アダプタ名] フィールドに、省略可能なオプションとして説明を入力します。
5. [アダプタ ID] テキストボックスに、アダプタのブランド名を入力します (大文字と小文字は区別されます)。

アダプタのブランド名を知るには、クライアント上でコマンドラインを開き、次のコマンドを入力します。

```
ipconfig/all
```

-
6. [OK] をクリックします。

[ファイアウォールルールの管理](#)

[ファイアウォールルールのネットワークアダプタトリガについて](#)

[ネットワークアダプタを通過するトラフィックの制御](#)

ファイアウォールルールのインポートとエクスポート

ファイアウォールルールと設定は別のファイアウォールポリシーからエクスポートしてインポートできるため、ルールや設定を再作成する必要はありません。たとえば、1つのポリシーから別のポリシーにルールセットの一部をインポートできます。ルールをインポートするには、まずルールを .dat ファイルにエクスポートしてそのファイルにアクセスできるようにする必要があります。

ルールは親ポリシーに青色の線を基準にして表示される順序と同じ順序で追加されます。その後でルールの処理順を変更できます。

1. ファイアウォールルールをエクスポートするには、コンソールで [ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。

バージョン 14.2 より前には、[Mac の設定] のオプションはありません。

3. [ルール] リストで、エクスポートするルールを選択して右クリックし、[エクスポート] をクリックします。
4. [ポリシーのエクスポート] ダイアログボックスで、.dat ファイルを保存するディレクトリを検索してファイル名を入力し、[エクスポート] をクリックします。
5. ファイアウォールルールをインポートするには、コンソールで [ファイアウォールポリシー] を開きます。
6. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。

バージョン 14.2 より前には、[Mac の設定] のオプションはありません。

7. ルールリストを右クリックして、[インポート] をクリックします。
8. [ポリシーのインポート] ダイアログボックスで、インポートするファイアウォールルールを含む .dat ファイルを検索し、[インポート] をクリックします。
9. [入力] ダイアログボックスで、ポリシーの新しい名前を入力して [OK] をクリックします。
10. [OK] をクリックします。

[新しいファイアウォールルールの追加](#)

[ファイアウォールルールのカスタマイズ](#)

[ファイアウォールルール、ファイアウォール設定、侵入防止の処理順について](#)

クライアント上でのファイアウォールルールのインポートまたはエクスポート

他の Symantec Endpoint Protection クライアントとルールを共有することで、ルールを作成し直す必要がなくなります。別のコンピュータとの間でルールをエクスポートしたりインポートしたりできます。インポートしたルールは、ファイアウォールルールリストの一番下に追加されます。インポートしたルールが既存のルールと同一である場合でも、インポートしたルールは既存のルールを上書きしません。

エクスポートしたルールとインポートしたルールは、.sar ファイルに保存されます。

クライアント上でファイアウォールルールをエクスポートするには

1. クライアントのサイドバーで、[状態] をクリックします。
2. [ネットワークとホストのエクスプロイト緩和機能] の隣で、[オプション] > [ファイアウォールルールの設定] を選択します。
3. [ファイアウォールルールの設定] ダイアログボックスで、エクスポートするルールを選択します。
4. ルールを右クリックし、[選択したルールのエクスポート] をクリックします。
5. [エクスポート] ダイアログボックスでファイル名を入力し、[保存] をクリックします。
6. [OK] をクリックします。

クライアント上でファイアウォールルールをインポートするには

1. クライアントのサイドバーで、[状態] をクリックします。
2. [ネットワークとホストのエクスプロイト緩和機能] の隣で、[オプション] > [ファイアウォールルールの設定] を選択します。
3. [ファイアウォールルールの設定] ダイアログボックスで、ファイアウォールルールリストを右クリックし、[ルールのインポート] をクリックします。
4. [インポート] ダイアログボックスで、インポートするルールを含む .sar 形式のファイルを検索します。
5. [開く] をクリックします。
6. [OK] をクリックします。

ファイアウォールルールのカスタマイズ

新しいファイアウォールポリシーを作成すると、そのポリシーにはいくつかのデフォルトルールが含まれます。必要に応じて、1 つまたは複数のルールコンポーネントを修正できます。

ファイアウォールルールコンポーネントは次のとおりです:

処理	処理パラメータはファイアウォールが正常にルールと一致した場合に行う処理を指定します。ルールが一致して受信したパケットに対する応答としてそのルールを選択した場合には、ファイアウォールはすべての処理を実行します。ファイアウォールがパケットを許可するか遮断するか、またログに記録するかしないかを指定します。ファイアウォールがトラフィックを許可すると、ルールが指定したトラフィックはネットワークにアクセスできます。ファイアウォールがトラフィックを遮断する場合には、ルールが指定したトラフィックがネットワークにアクセスしないようにそのトラフィックを遮断します。 処理は次のとおりです: - 許可する ファイアウォールはネットワーク接続を許可します。 - 遮断 ファイアウォールはネットワーク接続を遮断します。 Note: Mac クライアントのファイアウォールはパケットを監視しますが、それらをログに記録することはありません。 Note: この注記は 14.2 以降にのみ適用されます。
トリガ	ファイアウォールがルールを評価するとき、ルールを適用するためにはすべてのトリガが true である必要があります。現在のパケットに関していずれかのトリガが true でない場合、ファイアウォールはルールを適用できません。複数のトリガ定義を組み合わせてより複雑なルール (たとえば特定の送信先アドレスに関して特定のプロトコルを識別するルール) を作成できます。 トリガは次のとおりです: - アプリケーション トラフィックを許可するルールで、アプリケーションのみをトリガに定義した場合、ファイアウォールはアプリケーションにネットワーク操作の実行を許可します。重要なのはアプリケーション自体でありアプリケーションが実行するネットワーク操作ではありません。管理者は追加のトリガを定義して通信を許可する特定のネットワークプロトコルとホストを記述できます。 ファイアウォールルールのアプリケーショントリガについて - ホスト ホストトリガを定義する場合は、記述するネットワーク接続の両端のホストを指定します。ホスト間の関係は、従来からネットワーク接続の送信元または送信先と呼ばれます。 ファイアウォールルールのホストトリガについて - ネットワークサービス ネットワークサービストリガは記述するトラフィックに関して重要な 1 つ以上のネットワークプロトコルを識別します。ローカルホストコンピュータには常にローカルポートがあり、リモートコンピュータには常にリモートポートがあります。このポートの関係の記述は、トラフィックの方向と無関係です。 ファイアウォールルールのネットワークサービストリガについて - ネットワークアダプタ ネットワークアダプタトリガを定義すると、ルールは指定した種類のアダプタを使用して送受信されたトラフィックのみに適用されます。任意のアダプタ、または現在クライアントコンピュータに関連付けられているアダプタを指定できます。 ファイアウォールルールのネットワークアダプタトリガについて
条件	ルール条件は、ルールのスケジュールとスクリーンセーバーの状態から構成されます。条件パラメータはネットワーク接続に関するパラメータではありません。条件パラメータは、ルールがアクティブな状態を決定します。管理者はスケジュールを定義したりルールをアクティブとするか非アクティブとするかを決定するスクリーンセーバーの状態を識別できます。条件パラメータは省略可能で、定義しなくてもかまいません。ファイアウォールは非アクティブなルールを評価しません。
通知	ログ設定では、ルールに対して設定した基準にトラフィックイベントが一致したときに、サーバーがログエントリを作成するか、電子メールメッセージを送信するかを指定できます。 重大度の設定では、ルール違反の重大度を指定できます。

ファイアウォールルールをカスタマイズするには

-
1. コンソールで、[ファイアウォールポリシー] を開きます。
 2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。
バージョン 14.2 より前には、[Mac の設定] のオプションはありません。
 3. [ルール] タブの [ルール] リストにある [有効] フィールドで、ルールを有効にする場合は、ボックスにチェックマークが付いていることを確認します。ルールを無効にする場合は、ボックスのチェックマークをはずします。
Symantec Endpoint Protection は、有効にしたルールのみを処理します。デフォルトでは、すべてのルールが有効になっています。
 4. [名前] フィールドをダブルクリックし、ファイアウォールルールの重複しない名前を入力します。
 5. [処理] フィールドを右クリックし、トラフィックがトリガされた場合に Symantec Endpoint Protection が行う処理を選択します。
 6. [アプリケーション] フィールドで、アプリケーションを定義します。
[アプリケーションについての情報の定義](#)
 7. [ホスト] フィールドで、ホストトリガを指定します。
[特定のサーバーとの間で送受信されるトラフィックの遮断](#)
 8. ホストトリガの指定以外に、ローカルサブネットへのアクセスを許可するトラフィックも指定できます。
[ローカルサブネットへの特定トラフィックのみの許可](#)
 9. [サービス] フィールドで、ネットワークサービストリガを指定します。
[ネットワークコンピュータがメッセージ、ファイル、印刷を共有できるかどうかの制御](#)
 10. [ログ] フィールドで、このファイアウォールルールに違反したときに、Symantec Endpoint Protection に電子メールメッセージを送信させるタイミングを指定します。
[ファイアウォールルール違反の通知の設定](#)
 11. [重大度] フィールドを右クリックして、ルール違反の重大度を選択します。
 12. [アダプタ] 列で、ルールのアダプタトリガを指定します。
[ネットワークアダプタを通過するトラフィックの制御](#)
 13. [時間] 列で、このルールがアクティブである期間を指定します。
 14. [スクリーンセーバー] フィールドを右クリックし、ルールがアクティブになるために必要なクライアントコンピュータのスクリーンセーバーの状態を指定します。
[次の場所に作成しました] フィールドは編集できません。ポリシーが共有される場合、「共有」という文字が表示されます。ポリシーが共有されていない場合、フィールドには非共有ポリシーが割り当てられているグループの名前が表示されます。
 15. [説明] フィールドを右クリックし、[編集] をクリックし、ルールの説明を入力して (省略可能)、[OK] をクリックします。
 16. ルールの設定を完了したら、[OK] をクリックします。

[新しいファイアウォールルールの追加](#)

[ファイアウォールルールの管理](#)

特定のサーバーとの間で送受信されるトラフィックの遮断

特定のサーバーとの間で送受信されるトラフィックの遮断では、ドメイン名やホスト名ではなく IP アドレスでトラフィックを遮断できます。そうしないと、ユーザーがホスト名に対応する IP アドレスでアクセスできる場合があります。

特定のサーバーとの間で送受信されるトラフィックを遮断するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページで、[ルール] をクリックします。
3. [ルール] タブの [ルール] リストで、編集するルールを選択し、[ホスト] フィールドを右クリックして、[編集] をクリックします。
4. [ホストリスト] ダイアログボックスで、次のいずれかの処理を行います。
 - [送信元/送信先] をクリックする
 - [ローカル/リモート] をクリックする
5. 次のいずれかのタスクを行います。

ホストの種類を選択するには、[種類] ドロップダウンリストから入力します。	次のすべてのタスクを実行します。 • [送信元と送信先] または [ローカルとリモート] テーブルで、[追加] をクリックします。 • [ホスト] ダイアログボックスの [種類] ドロップダウンリストからホストの種類を選択し、各ホストの種類に適切な情報を入力します。 • [OK] をクリックします。 作成したホストは自動的に有効になります。
ホストグループを選択するには	[ホストリスト] ダイアログボックスで、次のいずれかの処理を行います。 • [送信元/送信先] をクリックする • [ローカル/リモート] をクリックする [ホストリスト] ダイアログボックスで、ルールに追加するホストグループすべての [有効] 列のフィールドにチェックマークを付けます。

6. 必要に応じて、さらにホストを追加します。
7. [OK] をクリックして、[ルール] リストに戻ります。

新しいファイアウォールルールの追加

ファイアウォールルールのカスタマイズ

ホストグループの追加

ローカルサブネットへの特定トラフィックのみの許可

ローカルサブネットに向かう特定のトラフィックのみを許可するファイアウォールルールを作成できます。このファイアウォールルールは、実際のアドレスとは無関係に、常にローカルサブネットの IP アドレスに適用されます。このため、ローカルサブネットの IP アドレスを変更しても、新しいアドレスのためにこのルールを修正する必要はありません。

たとえば、ローカルサブネットの IP アドレスとは無関係に、ローカルサブネットのポート 80 に向かうトラフィックのみを許可するようにこのルールを作成できます。

ローカルサブネットへの特定のトラフィックのみを許可するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。

バージョン 14.2 より前には、[Mac の設定] のオプションはありません。

-
3. [ルール] タブの [ファイアウォールルール] リストで、編集するルールを見つけます。
 4. ローカルサブネットのトラフィック条件を作成するルールの [ホスト] 列をダブルクリックします。
 5. このルールを適用するホストの種類の下で ([ローカル] または [リモート])、[追加] をクリックします。
 6. [アドレスの種類] ドロップダウンリストをクリックして、次のいずれかを選択します。
 - Windows: [ローカルサブネット]
 - Mac: [サブネット]
 7. [OK] をクリックし、もう一度 [OK] をクリックして [ホストリスト] ダイアログボックスを閉じます。

ファイアウォールルールのカスタマイズ

ネットワークコンピュータがメッセージ、ファイル、印刷を共有できるかどうかの制御

ネットワークサービスを利用することで、ネットワークに接続するコンピュータはメッセージの送受信、ファイルの共有、印刷を行うことができます。管理者はネットワークサービスを許可または遮断するファイアウォールルールを作成できます。

カスタムネットワークサービスはファイアウォールルールを通して追加できます。しかし、そのネットワークサービスはデフォルトリストには追加されません。また、カスタムサービスには他のルールからはアクセスできません。

ネットワークコンピュータがメッセージ、ファイル、印刷を共有できるかどうかを制御するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。

バージョン 14.2 より前には、[Mac の設定] のオプションはありません。

3. [ルール] タブの [ルール] リストで、編集するルールを選択し、[サービス] フィールドを右クリックして、[編集] をクリックします。
4. [サービスリスト] ダイアログボックスで、ルールをトリガする各サービスの横のチェックボックスにチェックマークを付けます。
5. 選択したルールに対してのみサービスを追加するには、[追加] をクリックします。
6. [プロトコル] ダイアログボックスで、[プロトコル] ドロップダウンリストからプロトコルを選択します。
7. 適切なフィールドに入力します。
8. [OK] をクリックします。
9. [OK] をクリックします。
10. [OK] をクリックします。

新しいファイアウォールルールの追加

ファイアウォールルールのカスタマイズ

ファイアウォールルールのネットワークサービストリガについて

デフォルトのネットワークサービスリストへのネットワークサービスの追加

ネットワーク内のファイルおよびプリンタを参照できるようにするクライアントの許可

管理者は、クライアントがローカルネットワークでファイルを共有したり、共有しているファイルやプリンタを参照したりできるようにすることができます。ネットワークベースの攻撃を防止するために、ネットワークファイルとプリンタの共有を有効にしない場合があります。

ファイアウォールルールを追加することで、ネットワークでのファイルとプリンタの共有を有効にできます。ファイアウォールルールにより、ポートにアクセスしてファイルとプリンタを参照したり共有したりすることができます。クライアントがファイルを共有できるように、1 つめのファイアウォールルールを作成します。2 つめのファイアウォールルールは、クライアントがその他のファイルとプリンタを参照できるように作成します。

設定は、次のように、クライアントに対して指定する制御の種類に基づいて、別々に機能します。

クライアント制御または混合制御	Windows クライアントのユーザーはこれらの設定を、ネットワークとホストのエクスプロイト緩和機能で設定して、自動的に有効にできます。 Mac クライアントのユーザーのみがファイアウォールを有効または無効にできます。
混合制御	Windows 上では、この種のトラフィックを指定するサーバーのファイアウォールルールで、これらの設定を上書きできます。 Mac 上では、すべてのファイアウォールルールはサーバーのファイアウォールルールです。
サーバー制御	これらの設定はクライアントでは利用できません。

- オプション 1: ネットワーク内のファイルとプリンタを参照できるように Windows クライアントを許可するには、コントロールで [ファイアウォールポリシー] を開きます。
- [ファイアウォールポリシー] ページの [Windows の設定] で、[ルール] をクリックします。
- [ルール] タブの [ルール] リストで、編集するルールを選択し、[サービス] フィールドを右クリックして、[編集] をクリックします。
- [サービスリスト] ダイアログボックスで、[追加] をクリックします。
- [プロトコル] ダイアログボックスの [プロトコル] ドロップダウンリストで [TCP] をクリックして、[ローカル/リモート] をクリックします。
- 次のいずれかのタスクを行います。

ネットワーク内のファイルおよびプリンタを参照できるようにクライアントを許可するには	[リモートポート] ドロップダウンリストで、88, 135, 139, 445 と入力します。
その他のコンピュータによるクライアントのファイルの参照を有効にするには	[ローカルポート] ドロップダウンリストで、88, 135, 139, 445 と入力します。

- [OK] をクリックします。
- [サービスリスト] ダイアログボックスで、[追加] をクリックします。
- [プロトコル] ダイアログボックスの [プロトコル] ドロップダウンリストで、[UDP] をクリックします。
- 次のいずれかのタスクを行います。

ネットワーク内のファイルおよびプリンタを参照できるようにクライアントを許可するには	[ローカルポート] ドロップダウンリストで、137, 138 と入力します。 [リモートポート] ドロップダウンリストで、88 と入力します。
その他のコンピュータによるクライアントのファイルの参照を有効にするには	[ローカルポート] ドロップダウンリストで、88, 137, 138 と入力します。

-
11. [OK] をクリックします。
 12. [サービスリスト] ダイアログボックスでこの 2 つのサービスが有効になっていることを確認して、[OK] をクリックします。
 13. [ルール] タブで、[処理] フィールドが [許可する] に設定されていることを確認します。
 14. ポリシーの設定を完了したら、[OK] をクリックします。
 15. オプション 2: ネットワーク内のファイルとプリンタを参照できるように Mac クライアントを許可するには、コンソールで [ファイアウォールポリシー] を開きます。

NOTE

Mac ファイアウォールはバージョン 14.2 以降で利用できます。

16. [ファイアウォールポリシー] ページの [Mac の設定] で、[ルール] をクリックします。
17. [ルール] タブの [ルール] リストで、編集するルールを選択し、[サービス] フィールドを右クリックして、[編集] をクリックします。
18. [サービスリスト] ダイアログボックスで、[追加] をクリックします。
19. [プロトコル] ダイアログボックスの [プロトコル] ドロップダウンリストで [TCP] をクリックして、[ローカル/リモート] をクリックします。
20. 他のコンピュータがクライアントのファイル参照できるようにするには、[ローカルポート] ドロップダウンリストで 139 と 445 を入力します。
デフォルトでは、Mac からネットワークを参照する発信要求は有効になっています。
21. [OK] をクリックします。
22. [サービスリスト] ダイアログボックスで新しいサービスが有効になっていることを確認して、[OK] をクリックします。
23. [ルール] タブで、[処理] フィールドが [許可する] に設定されていることを確認します。
24. ポリシーの設定を完了したら、[OK] をクリックします。

Mac でのプリンタ検出は Bonjour サービスを通じて行われ、デフォルトでオープンになっています。Bonjour サービスのカスタムルールを設定する必要はありません。

新しいファイアウォールルールの追加

ファイアウォールルールのカスタマイズ

ファイアウォールルール違反の通知の設定

ファイアウォールがルール違反、攻撃、イベントを検出するたびに Symantec Endpoint Protection が電子メールメッセージを送信するように設定できます。たとえば、クライアントが特定の IP アドレスから送信されるトラフィックを遮断したことがわかると便利です。

ファイアウォールルール違反の通知を設定するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[ルール] をクリックします。

バージョン 14.2 より前には、[Mac の設定] のオプションはありません。

3. [ルール] タブでルールを選択し、[ログ] フィールドを右クリックし、次のタスクを実行します。

ファイアウォールルールがトリガされたときに電子メールメッセージを送信するには	[電子メール警告の送信] にチェックマークを付けます。
ファイアウォールルールがトリガされたときにログイベントを生成するには	Windows ルールの場合、[トラフィックログに書き込み] と [パケットログに書き込み] の両方にチェックマークを付けます。 Mac ルール場合、[トラフィックログに書き込み] にチェックマークを付けます。

4. このポリシーの設定を完了したら、[OK] をクリックします。

5. セキュリティ警告を設定します。

6. メールサーバーを設定します。

7. [OK] をクリックします。

新しいファイアウォールルールの追加

ファイアウォールルールのカスタマイズ

管理者通知の設定

ネットワークアダプタを通過するトラフィックの制御

ネットワークアダプタトリガを定義するとき、ルールは、指定されたアダプタが送受信するトラフィックにのみ適用されます。

カスタムネットワークアダプタはファイアウォールルールから追加できます。しかし、そのアダプタは共有リストには追加されません。また、カスタムアダプタには他のルールからはアクセスできません。

ネットワークアダプタを通過するトラフィックを制御するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] で、[ルール] をクリックします。
3. [ルール] タブの [ルール] リストで、編集するルールを選択し、[アダプタ] フィールドを右クリックして、[その他のアダプタ] をクリックします。
4. [ネットワークアダプタ] ダイアログボックスで、次のいずれかの処理を行います。

任意のアダプタ (リストにない場合も含む) に対してルールをトリガするには	[ルールをすべてのアダプタに適用する] をクリックし、続いて ステップ 7 に進みます。
選択したアダプタに対してルールをトリガするには	[ルールを以下のアダプタに適用する] をクリックします。 続いて、ルールをトリガする各アダプタの横にあるボックスにチェックマークを付けます。

5. 選択したルールに対してのみカスタムアダプタを追加するには、次のタスクを実行します。

- [追加] をクリックします。
- [ネットワークアダプタ] ダイアログボックスで、アダプタの種類を選択して [アダプタ ID] テキストフィールドにアダプタのブランド名を入力します。

6. [OK] をクリックします。
7. [OK] をクリックします。
8. [OK] をクリックします。

[新しいファイアウォールルールの追加](#)

[ファイアウォールルールのカスタマイズ](#)

[ファイアウォールルールのネットワークアダプタトリガについて](#)

混合制御のファイアウォール設定

ファイアウォール設定においてユーザーが制御不能、フルコントロール可能、限定された制御が可能なようにクライアントを設定できます。

Mac ファイアウォールの場合、ユーザーはファイアウォールルールを作成したり、クライアントユーザーインターフェースの設定に関係なく設定を変更したりすることはできません。オプションは、クライアントユーザーインターフェースには表示されません。

サーバー制御	Windows の場合、ユーザーがファイアウォールルールを作成したりファイアウォール設定を有効にしたりすることはできません。 Mac の場合、ユーザーはファイアウォールを有効または無効にできません。
クライアント制御	Windows の場合、ユーザーはファイアウォールルールを作成したりすべてのファイアウォール設定を有効にしたりできます。 Mac の場合、ユーザーはファイアウォールを有効または無効にできます。
混合制御	Windows の場合、ユーザーはファイアウォールルールを作成できます。ユーザーがどのファイアウォール設定を有効にできるかを決定します。 Mac の場合、ユーザーはファイアウォールを有効または無効にできるかどうかを決定します。

NOTE

ファイアウォールは Mac クライアントのバージョン 14.2 以降でのみ利用できます。

混合制御のファイアウォール設定を行うには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、修正するユーザー制御レベルを持つグループを選択します。
3. [ポリシー] タブの [場所固有のポリシーと設定] で、場所の下に [場所固有の設定] を展開します。
4. [クライアントユーザーインターフェース制御の設定] の右側で、[タスク]、[設定の編集] の順にクリックします。
5. [制御モード設定] ダイアログボックスで、[混合制御] をクリックし、[カスタマイズ] をクリックします。
6. [クライアント/サーバー制御の設定] タブの [ファイアウォールポリシー] カテゴリで、次のいずれかのタスクを実行します。
 - クライアント設定をユーザーが設定できるようにするには、[クライアント] をクリックする
 - クライアント設定を行うには、[サーバー] をクリックする
7. [OK] をクリックします。
8. [OK] をクリックします。
9. [サーバー] に設定したファイアウォール設定ごとに、ファイアウォールポリシーの設定を有効または無効にします。

[ファイアウォール保護の管理](#)

ルールの追加ではなくネットワークサービスのための通信の有効化

ルールの追加ではなくネットワークサービスのための通信の有効化

特定のネットワークサービス間の通信を自動的に許可するオプションを有効にして、それらのサービスを明示的に許可するルールを定義する必要がなくなります。トラフィックの設定を有効にすることで NetBIOS とトークンリングを使って通信するトラフィックの検出と遮断も実行できます。

DHCP、DNS、WINS トラフィックを使うように設定されたネットワーク接続のアウトバウンド要求とインバウンド応答を許可できます。

フィルタは DHCP、DNS、WINS クライアントがサーバーから IP アドレスを受信することを許可します。また、次の条件でネットワークからの攻撃に対してクライアントを保護します。

クライアントがサーバーに要求を送信する場合	クライアントはインバウンド応答の許可を 5 秒間待ちます。
クライアントがサーバーに要求を送信しない場合	各フィルタはパケットを許可しません。

これらのオプションを有効にすると、Symantec Endpoint Protection は要求が行われた場合にパケットが許可され、パケットは遮断されません。パケットを遮断するにはファイアウォールルールを作成する必要があります。

NOTE

これらのオプションを混合制御で設定するには、これらのオプションを [クライアントユーザーインターフェース混合制御の設定] ダイアログボックスでも有効にする必要があります。

ルールを追加するのではなくネットワークサービスのための通信を有効にするには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページの [Windows の設定] または [Mac の設定] で、[組み込みルール] をクリックします。

14.2 より前のバージョンでは、これらの設定は Windows のみが対象です。

3. 有効にするオプションにチェックマークを付けます。
4. [OK] をクリックします。
5. メッセージが表示されたら、ポリシーを場所に割り当てます。

ファイアウォールポリシーの作成

ポリシーの編集

クライアントコンピュータの保護をユーザーが無効にできない設定

攻撃側コンピュータへの接続の自動遮断

Symantec Endpoint Protection クライアントがネットワーク攻撃を検出すると、接続を自動的に遮断してクライアントコンピュータの安全を確保できます。クライアントはアクティブレスポンスをアクティブ化して、クライアントと攻撃側コンピュータの間のすべての通信を一定期間自動的に遮断します。攻撃側コンピュータの IP アドレスは単一の場所で遮断されます。

攻撃者の IP アドレスはセキュリティログに記録されます。特定の IP アドレスを取り消すか、すべてのアクティブレスポンスを取り消すことによって攻撃を遮断解除できます。

クライアントを混合制御に設定している場合は、ユーザーがクライアントで有効にできる設定を表示するかどうかを指定できます。設定が表示されていない場合は、[クライアントユーザーインターフェース混合制御の設定] ダイアログボックスで有効にする必要があります。

更新された IPS シグネチャ、更新されたサービス拒否シグネチャ、ポートスキャン、MAC 詐称によってもアクティブレスポンスがトリガされます。

攻撃側コンピュータへの接続を自動遮断するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. 左ペインの [ファイアウォールポリシー] ページで、次のオプションのいずれかをクリックします。
 - [Windows の設定] : [保護とステルス]
 - [Mac の設定] : [保護]Mac の設定はバージョン 14.2 以降でのみ利用できます。
3. [保護設定] の下で、[自動的に攻撃者の IP アドレスを遮断する] にチェックマークを付けます。
4. [IP アドレスを遮断する秒数: **XX** 秒] テキストボックスに、潜在的な攻撃者を遮断する秒数を指定します。
1 から 999,999 までの値を入力できます。
5. [OK] をクリックします。

ファイアウォールポリシーの作成

混合制御のファイアウォール設定

ポリシーの編集

潜在的な攻撃と詐称の試行の検出

Symantec Endpoint Protection でクライアントに対する潜在的な攻撃を検出してログに記録したり、詐称の試行を遮断したりするための、さまざまな設定を有効にできます。これらのオプションはすべて、デフォルトでは無効になっています。

有効にできる設定は次のとおりです。

ポートスキャン検出を有効にする	この設定を有効にすると、Symantec Endpoint Protection はセキュリティルールによって遮断されるすべての着信パケットを監視します。ルールによって短時間に異なるポートで複数の異なるパケットが遮断される場合、Symantec Endpoint Protection はセキュリティログエントリを作成します。 ポートスキャン検出ではパケットは遮断されません。ポートスキャンの実行時にトラフィックを遮断するには、セキュリティポリシーを作成する必要があります。
サービス拒否検出を有効にする	サービス拒否検出は侵入検知の一種です。これが有効になっている場合は、ポート番号やインターネットプロトコルの種類に関係なく、クライアントは既知のシグネチャからパターンを検出するとトラフィックを遮断します。
MAC 詐称対策を有効にする	この設定を有効にすると、Symantec Endpoint Protection は、特定のホストに要求が行われたときに、次の着信と発信のトラフィックを許可します。 • アドレス解決プロトコル (ARP) (IPv4) • Neighbor Discovery Protocol (NDP) (IPv6) バージョン 14.2 以降でサポートされます。 その他の予期されていないトラフィックはすべて遮断され、セキュリティログにエントリが生成されます。

NOTE

これらのオプションを混合制御で設定するには、これらのオプションを [クライアントユーザーインターフェース混合制御の設定] ダイアログボックスでも有効にする必要があります。

潜在的な攻撃と詐称の試行を検出するには

-
1. コンソールで、[ファイアウォールポリシー] を開きます。
 2. [ファイアウォールポリシー] ページで、次のいずれかをクリックします。
 - [Windows の設定]: [保護とステルス]
 - [Mac の設定]: [保護]Mac の設定はバージョン 14.2 以降でのみ利用できます。
 3. [保護の設定] の下で、有効にしたいオプションにチェックマークを付けます。
 4. [OK] をクリックします。
 5. メッセージが表示されたら、ポリシーを場所に割り当てます。

ファイアウォールポリシーの作成

クライアントコンピュータの保護をユーザーが無効にできない設定

ポリシーの編集

コンピュータに対する外部からのステルス攻撃の防止

外部からの攻撃によってクライアントに関する情報が検出されないようにする設定を有効にできます。これらの設定はデフォルトで無効になっています。

NOTE

これらのオプションを混合制御で設定するには、これらのオプションを [クライアントユーザーインターフェース混合制御の設定] ダイアログボックスでも有効にする必要があります。

NOTE

これらのステルス設定は、Mac ファイアウォールには利用できません。
ファイアウォールは 14.2 以降の Mac クライアントに含まれています。

コンピュータに対する外部からのステルス攻撃を防止するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページで、[保護とステルス] をクリックします。
3. [ステルスの設定] の下で、有効にするオプションにチェックマークを付けます。
4. [OK] をクリックします。
5. メッセージが表示されたら、ポリシーを場所に割り当てます。

ファイアウォールポリシーの作成

クライアントコンピュータの保護をユーザーが無効にできない設定

ポリシーの編集

Windows ファイアウォールの無効化

Symantec Endpoint Protection が Windows ファイアウォールを無効にする条件を指定できます。次が発生するときに、Symantec Endpoint Protection は Windows ファイアウォールの設定を、Symantec Endpoint Protection がインストールされる前の状態に復元します。

- Symantec Endpoint Protection がアンインストールされる。
- Symantec Endpoint Protection ファイアウォールが無効である。

NOTE

Symantec Endpoint Protection は既存の Windows ファイアウォールポリシーのルールや除外は変更しません。

通常、Windows ユーザーは Windows ファイアウォールが無効になっている場合、コンピュータが再起動するときに通知を受信します。Symantec Endpoint Protection は Windows ファイアウォールが無効になっているときにユーザーが警告されないように、デフォルトでこの通知を無効にします。ただし、必要な場合は通知を有効にできます。

Windows ファイアウォールを無効にするには

1. コンソールで、[ポリシー] をクリックします。
2. [Policies] で [Firewall] をクリックします。
3. 次のいずれかのタスクを行います。
 - 新しいファイアウォールポリシーを作成します。
 - [ファイアウォールポリシー] リストで、修正するファイアウォールポリシーをダブルクリックします。
4. [ファイアウォールポリシー] で [Windows 統合] をクリックします。
5. [Windows ファイアウォールを無効にする] ドロップダウンリストで、Windows ファイアウォールをいつ無効にするかを指定します。

デフォルト設定は [1 回のみ無効にする] です。

これらのオプションに関する詳細が必要な場合、[ヘルプ] をクリックします。

Windows 統合

6. [Windows ファイアウォール無効のメッセージ] ドロップダウンリストで、ファイアウォールが無効になっていることを示す起動時の Windows メッセージを無効にするかどうかを指定します。

デフォルトの設定は [無効] です。これは、ユーザーはコンピュータの起動時に、Windows ファイアウォールが無効になっているというメッセージを受信しないことを意味します。

7. [OK] をクリックします。

ファイアウォールポリシーの作成

セキュリティポリシーの種類

侵入防止の管理

デフォルトの侵入防止設定はクライアントコンピュータをさまざまな脅威から保護します。デフォルトの設定はネットワークに合わせて変更できます。

サーバーで Symantec Endpoint Protection を実行すると、侵入防止はサーバーのリソースや応答時間に影響を与えることがあります。詳細については、次を参照してください。

Windows Server 上の Endpoint Protection のベストプラクティス

NOTE

Linux クライアントは侵入防止をサポートしません。

Table 81: 侵入防止の管理

タスク	説明
侵入防止について学習する	侵入防止がネットワーク攻撃とブラウザ攻撃を検出して遮断する方法を学習します。 侵入防止の動作 Symantec IPS シグネチャについて
侵入防止を有効にする	クライアントコンピュータを安全に保つために、侵入防止を有効にする必要があります。 - ネットワーク侵入防止 - ブラウザの侵入防止 (Windows コンピュータのみ) 検出項目をログに記録して遮断しないようにブラウザの侵入防止を設定することもできます。クライアントのセキュリティプロファイルのレベルが低下するのでこの設定の使用は一時的にしてください。たとえば、クライアントで遮断されたトラフィックの問題を解決する間のみログのみのモードを設定します。攻撃ログを確認し、トラフィックを遮断するシグネチャを識別して除外したら、ログのみのモードを無効にします。 ネットワーク侵入防止とブラウザ侵入防止の有効化 IPS シグネチャの例外の作成 グループまたはクライアントで [ネットワーク脅威防止を有効にする] コマンドを実行するときには、両方の種類の侵入防止に加えて、ファイアウォールも有効にすることができます。 コンソールを使った、クライアントコンピュータでのコマンドの実行
例外を作成して、シマンテック社のネットワーク侵入防止シグネチャのデフォルトの動作を変更する	シマンテック社のデフォルトのネットワーク侵入防止シグネチャのデフォルトの動作を変更するには、例外を作成すると便利です。一部のシグネチャはデフォルトでトラフィックを遮断し、他のシグネチャはデフォルトでトラフィックを許可します。 Note: ブラウザの侵入防止シグネチャの動作を変更することはできません。 次の理由から、いくつかのネットワークシグネチャのデフォルトの動作を変更すると効率的な場合があります。 - クライアントコンピュータでの消費量を減らす。 たとえば、トラフィックを遮断するシグネチャの数を減らしたい場合があります。ただし、攻撃シグネチャが脅威を示していないことを確認してから、攻撃シグネチャを遮断から除外してください。 - シマンテック社がデフォルトでは遮断する一部のネットワークシグネチャを許可する。 たとえば、無害なネットワーク活動が攻撃シグネチャと一致する誤認を減らすため、例外を作成したい場合があります。ネットワーク活動が安全であることがわかっている場合には、例外を作成できます。 - シマンテック社が許可する一部のシグネチャを遮断する。 たとえば、シマンテック社はピアツーピアアプリケーション用のシグネチャを含めて、デフォルトではトラフィックを許可しています。そうする代わりに、トラフィックを遮断する例外を作成できます。 - 監査シグネチャを使い、特定の種類のトラフィックを監視する (Windows のみ) 監査シグネチャでは、インスタントメッセージアプリケーションからのトラフィックなど、特定の種類のトラフィックを [ログに記録しない] ことがデフォルトの動作になっています。ログを表示し、ネットワークのこのトラフィックを監視できるように、トラフィックをログに記録する例外を作成できます。その後、その例外を使ってトラフィックを遮断したり、トラフィックを遮断するファイアウォールルールを作成したり、トラフィックをそのままにしたりできます。 トラフィックのアプリケーションルールを作成することもできます。 IPS シグネチャの例外の作成 アプリケーション制御を使って、ユーザーが各自のコンピュータでピアツーピアアプリケーションを実行しないようにできます。 アプリケーション制御へのカスタムルールの追加 ピアツーピアのトラフィックを送受信するポートを遮断する場合は、ファイアウォールポリシーを使います。 ファイアウォールポリシーの作成

タスク	説明
クライアントコンピュータでブラウザシグネチャを無視する例外を作成する (Windows のみ)	Windows コンピュータのブラウザの侵入防止からブラウザシグネチャを除外する例外を作成できます。 ネットワーク内のブラウザでブラウザの侵入防止が原因の問題が起きている場合は、ブラウザシグネチャを無視したいことがあります。 IPS シグネチャの例外の作成
ネットワーク侵入防止スキャンから特定のコンピュータを除外する	ネットワーク侵入防止から特定のコンピュータを除外すると便利な場合があります。たとえば、社内ネットワークの一部のコンピュータはテスト目的でセットアップされている可能性があります。それらのコンピュータとの間で送受信されるトラフィックは、Symantec Endpoint Protection では無視したい場合があります。 コンピュータを除外するときには、ファイアウォールが提供するサービス拒否の保護とポートスキャンの保護からも、それらのコンピュータを除外します。 除外するコンピュータのリストの作成
侵入防止の通知を設定する	デフォルトでは、クライアントコンピュータに侵入の試みについてのメッセージが表示されます。メッセージをカスタマイズすることもできます。 侵入防止とメモリエクспロイト緩和機能のクライアント通知の設定
カスタム侵入防止シグネチャを作成する (Windows のみ)	独自の侵入防止シグネチャを記述し、特定の脅威を識別することができます。独自のシグネチャを記述するときには、シグネチャによって誤認が発生する可能性を減らすことができます。 たとえば、Web サイトを遮断してログに記録するためにカスタム侵入防止シグネチャを利用できます。 カスタム侵入防止シグネチャの管理 カスタム IPS シグネチャを使うには、ファイアウォールをインストールして有効にする必要があります。 クライアントにインストールするセキュリティ機能の選択
侵入防止を監視する	ネットワーク内のクライアントコンピュータで侵入防止が有効になっていることを定期的に確認してください。 エンドポイント保護の監視

侵入防止の動作

侵入防止とファイアウォールはネットワーク脅威防止の一部です。バージョン 14 では、ネットワーク脅威防止とメモリエクспロイト緩和機能が、ネットワークとホストのエクспロイト緩和機能を構成します。

侵入防止は、ネットワーク攻撃とブラウザに対する攻撃を自動的に検出して遮断します。侵入防止はクライアントコンピュータを保護するための、ファイアウォールの次にある第 2 の防衛層です。侵入防止は侵入防止システム (IPS) と呼ばれる場合もあります。

侵入防止はネットワーク攻撃を自動的に検出して遮断します。Windows コンピュータでは、侵入防止はサポート対象のブラウザでブラウザ攻撃も検出して遮断します。侵入防止はクライアントコンピュータを保護するための、ファイアウォールの次にある第 2 の防衛層です。侵入防止は侵入防止システム (IPS) と呼ばれる場合もあります。

侵入防止はネットワーク層でデータを傍受します。侵入防止はシグネチャを使い、パケットまたはパケットのストリームをスキャンします。ネットワーク攻撃またはブラウザ攻撃に対応するパターンを検索することで、各パケットを個別にスキャンします。侵入防止は、オペレーティングシステムコンポーネントとアプリケーション層に対する攻撃を検出します。

Table 82: 侵入防止の種類

次のように入力します。	説明
ネットワーク侵入防止	ネットワーク侵入防止は、シグネチャを使ってクライアントコンピュータに対する攻撃を識別します。既知の攻撃の場合、侵入防止はシグネチャと一致するパケットを自動的に破棄します。 この Symantec Endpoint Protection Manager で独自のカスタムネットワークシグネチャを作成することもできます。クライアントでカスタムシグネチャを直接作成することはできませんが、クライアントでカスタムシグネチャをインポートできます。カスタムシグネチャは Windows コンピュータでのみサポートされます。 Symantec IPS シグネチャについて
ブラウザの侵入防止 (Windows のみ) ブラウザの侵入防止	ブラウザの侵入防止は Internet Explorer と Firefox に対する攻撃を監視します。ブラウザの侵入防止は、それら以外のブラウザではサポートされません。 Firefox では Symantec Endpoint Protection プラグインが無効になることがありますが、再び有効にできます。 この種類の侵入防止は、攻撃シグネチャに加えてヒューリスティックを使い、ブラウザに対する攻撃を識別します。 ブラウザを終了するよう侵入防止からクライアントに要求が行われるブラウザ攻撃もあります。クライアントコンピュータに通知が表示されます。 ブラウザの侵入防止で保護されるブラウザの最新情報については、「ブラウザ侵入防止がサポートするブラウザのバージョン」を参照してください。

侵入防止の管理

侵入防止の設定

Symantec IPS シグネチャについて

シマンテック製侵入防止のシグネチャはデフォルトでクライアントにインストールされます。

侵入防止はシマンテック社のシグネチャを使って、個々のパケットまたはパケットのストリームを監視します。パケットのストリームの場合、侵入防止は以前のパケットのパターンまたは部分パターンのリストを記憶できます。その後で、この情報を以降のパケット検査に適用できます。

シマンテックシグネチャには、LiveUpdate コンテンツの一部としてクライアントにダウンロードされるネットワーク侵入防止のためのシグネチャが含まれています。Mac コンピュータの場合、追加のネットワーク侵入防止シグネチャがいくつかソフトウェアに組み込まれています。

Windows コンピュータでは、LiveUpdate コンテンツにブラウザの侵入防止のためのシグネチャも含まれています。

ネットワーク侵入防止シグネチャ	ネットワークシグネチャは、クライアントコンピュータでアプリケーションをクラッシュさせたりオペレーティングシステムを悪用したりする可能性がある攻撃のパターンと一致します。 シマンテック製ネットワークシグネチャによってトラフィックを遮断するか許可するかは変更できません。Symantec Endpoint Protection で、シグネチャによる検出をセキュリティログに記録するかどうかを変更できます。
ブラウザの侵入防止シグネチャ (Windows のみ)	ブラウザシグネチャは、ブラウザをクラッシュさせる可能性があるスクリプトファイルなど、サポート対象のブラウザに対する攻撃のパターンと一致します。 ブラウザシグネチャの処理やログの設定はカスタマイズできませんが、ブラウザシグネチャを除外することはできます。 ブラウザの検出をログに記録して検出した項目を遮断しないようにブラウザの侵入防止を設定できます。この処理は除外する必要があるブラウザシグネチャの識別に役立ちます。シグネチャ除外項目を作成したら、ログのみのモードを無効にします。

シマンテックセキュリティレスポンスのグループが攻撃のシグネチャを供給します。デフォルトでは、侵入防止エンジンと、対応するシグネチャのセットがクライアントにインストールされます。シグネチャはクライアントで更新を行うコンテンツの一部です。

IPS シグネチャに関する情報は、シマンテック社 Web サイトの次のページで参照できます。

[攻撃シグネチャ](#)

Mac クライアントの組み込み IPS シグネチャに関する情報については、次の記事を参照してください。

[Symantec Endpoint Protection IPS for Mac の組み込みシグネチャ](#)

[IPS シグネチャの例外の作成](#)

[侵入防止の管理](#)

カスタム IPS シグネチャについて

固有の IPS ネットワークシグネチャを作成できます。これらのシグネチャはパケットベースです。

シマンテック社のシグネチャとは異なり、カスタムシグネチャは単一のパケットペイロードのみをスキャンします。ただし、カスタムシグネチャは TCP/IP スタックで、シマンテック社のシグネチャよりも早期に攻撃を検出できます。

パケットベースのシグネチャはルールに一致する単一のパケットを診断します。ルールはポート、プロトコル、送信元または送信先の IP アドレス、TCP フラグ番号、アプリケーションなどさまざまな基準に基づいています。たとえば、カスタムシグネチャは受信したパケットの、CGI プログラム攻撃を示す GET / cgi-bin/phf? 内の文字列「phf」を監視します。各パケットに対してこの特定のパターンが評価されます。トラフィックのパケットがルールと一致する場合に、クライアントはパケットを許可または遮断します。

Symantec Endpoint Protection でカスタムシグネチャによる検出をパケットログに記録するかどうかを指定できます。

NOTE

カスタム IPS シグネチャを使うには、ファイアウォールをインストールして有効にする必要があります。

[クライアントにインストールするセキュリティ機能の選択](#)

カスタムシグネチャは Windows コンピュータでのみサポートされます。

[カスタム侵入防止シグネチャの管理](#)

ネットワーク侵入防止とブラウザの侵入防止の有効化

侵入防止はデフォルトで有効です。通常はどちらの種類の侵入防止も無効にしないでください。

ブラウザ侵入防止のログのみのモードを有効にしてクライアントユーザーに影響を与えずに遮断するトラフィックを記録できます。つの Symantec Endpoint Protection Manager のネットワークとホスト悪用防止の攻撃ログを使って特定のブラウザシグネチャを無視する侵入防止ポリシーの例外を作成できます。ログのみのモードは無効にします。

NOTE

これらのオプションを混合制御で設定するには、これらのオプションを [クライアントユーザーインターフェース混合制御の設定] ダイアログボックスでも有効にする必要があります。

ネットワーク侵入防止とブラウザの侵入防止を有効にするには

1. コンソールで、[侵入防止] ポリシーを開きます。
2. ポリシーページで、[侵入防止] をクリックします。
3. 次のオプションにチェックマークが付いていることを確認します。
 - ネットワーク侵入防止を有効にする
ネットワーク侵入防止から特定のコンピュータを除外することもできます。
[除外するコンピュータのリストの作成](#)
 - Windows のブラウザの侵入防止を有効にする

-
4. [OK] をクリックします。

IPS シグネチャの例外の作成

侵入防止の管理

混合制御のファイアウォール設定

IPS シグネチャの例外の作成

例外を使い、Symantec IPS シグネチャの動作を変更できます。

Windows と Mac コンピュータの場合、IPS がネットワークシグネチャを認識したときにクライアントが行う処理を変更できます。また、クライアントがイベントをセキュリティログに記録するかどうかを変更できます。

Windows コンピュータの場合、シマンテック社のブラウザシグネチャの動作は変更できません。ネットワークシグネチャとは異なり、ブラウザシグネチャについてはカスタム処理やログ記録の設定は許されていません。ただし、クライアントがシグネチャを無視するように、ブラウザシグネチャの例外を作成できます。

NOTE

ブラウザシグネチャの例外を追加すると、つの Symantec Endpoint Protection Manager は例外リストにシグネチャを含めて自動的に処理を [許可] に、ログの設定を [ログに記録しない] に設定します。処理やログの設定はカスタマイズできません。

侵入防止の管理

NOTE

作成またはインポートするカスタム IPS シグネチャの動作を変更するには、直接シグネチャを編集します。カスタムシグネチャは Windows コンピュータでのみサポートされます。

IPS シグネチャの例外を作成するには

1. コンソールで、[侵入防止] ポリシーを開きます。
2. [Windows 設定] または [Mac 設定] の下で、[例外] をクリックし、[追加] をクリックします。

NOTE

シグネチャの一覧には、管理コンソールにダウンロードされた最新の LiveUpdate コンテンツがポピュレートされます。Windows コンピュータの場合、管理サーバーがコンテンツをダウンロードしていなければ一覧は空の状態が表示されます。Mac コンピュータの場合、この一覧には少なくとも組み込みのシグネチャが常に入っています。これは Mac クライアントに自動的にインストールされるものです。

3. [侵入防止例外の追加] ダイアログボックスで、次のいずれかの処理を行ってシグネチャをフィルタ処理します。
 - (Windows のみ) 特定のカテゴリのシグネチャを表示するには、[カテゴリを表示] ドロップダウンリストからオプションを選択します。[ブラウザ保護] を選択すると、シグネチャの処理オプションは [許可] と [ログに記録しない] に自動的に変わります。
 - (Windows と Mac) 特定の重大度で分類されるシグネチャを表示するには、[重大度を表示] ドロップダウンリストからオプションを選択します。
4. 1 つ以上のシグネチャを選択します。

すべてのシグネチャの動作を同じにするには、[すべてを選択] をクリックします。
5. [次へ] をクリックします。
6. [シグネチャ処理] ダイアログボックスで、次のオプションを設定して [OK] をクリックします。
 - [処理] を [遮断] または [許可] に設定
 - [ログ] を [トラフィックをログ記録する] または [トラフィックをログに記録しない] に設定

NOTE

これらのオプションはネットワークシグネチャにのみ適用されます。ブラウザシグネチャの場合は、[OK] をクリックします。

シグネチャの動作を元の動作に戻す場合は、[例外] 一覧でシグネチャを選択して [削除] をクリックします。

7. [OK] をクリックしてポリシーの変更を保存します。

Symantec Endpoint Protection の例外の管理

除外するコンピュータのリストの作成

除外ホストはネットワーク侵入防止のみでサポートされます。

クライアントが攻撃シグネチャの照合、ポートスキャンやサービス拒否攻撃の確認をしないコンピュータのリストを作成できます。ネットワーク侵入防止やピアツーピア認証は、除外済みホストのリストにあるホストから流れ込む送信元トラフィックを許可します。ただし、ネットワーク侵入防止とピアツーピア認証は、リストにあるホストに流れ込む送信元トラフィックを評価し続けます。リストはインバウンドとアウトバウンドの両方のトラフィックに適用されますが、トラフィックの送信元のみ適用されます。また、リストはリモート IP アドレスのみにも適用されます。

たとえば、インターネットサービスプロバイダがネットワークのポートをスキャンすることを許可し、利用規約に準拠するようにコンピュータを除外することもできます。また、内部ネットワークにある一部のコンピュータをテスト用に設定する場合があります。

NOTE

また、IPS シグネチャによって攻撃が検出されない限り、すべてのインバウンドトラフィックとアウトバウンドトラフィックを許可するコンピュータのリストを作成することもできます。この場合、すべてのホストを許可するファイアウォールルールを作成します。

除外するコンピュータのリストを設定するには

1. コンソールで、[侵入防止] ポリシーを開きます。
2. ポリシーページで、[侵入防止] をクリックします。
3. チェックマークが付いていない場合は、[除外ホストを有効にする] にチェックマークを付け、[除外ホスト] をクリックします。
4. [除外ホスト] ダイアログボックスで、ネットワーク侵入防止から除外したいホストグループの横にある [有効] にチェックマークを付けます。

特定のサーバーとの間で送受信されるトラフィックの遮断

5. 除外したいホストを追加するには、[追加] をクリックします。
6. [ホスト] ダイアログボックスのドロップダウンリストで、次のいずれかのホストの種類を選択します。
 - IP address
 - IP アドレス範囲
 - サブネット
7. 選択したホストの種類に関連する適切な情報を入力します。

これらのオプションについて詳しくは [ヘルプ] を参照してください。

-
8. [OK] をクリックします。
 9. 「[除外したいホストを追加するには、\[追加 \] をクリックします。](#)」と「[\[OK \] をクリックします。](#)」を繰り返し、除外するコンピュータのリストにデバイスとコンピュータを追加します。
 10. 除外ホストを編集または削除するには、行を選択し、[編集] または [削除] をクリックします。
 11. [OK] をクリックします。
 12. ポリシーの設定を完了したら、[OK] をクリックします。

侵入防止とメモリエクスプロイト緩和機能のクライアント通知の設定

クライアントが侵入防止イベントやメモリエクスプロイト緩和機能を検出すると、デフォルトでクライアントコンピュータ上に通知が表示されます。これらの通知が有効になっていると、通知によって標準のメッセージが表示されます。IPS 通知の場合は、標準のメッセージにカスタマイズしたテキストを追加することもできます。

侵入防止とメモリエクスプロイト緩和機能のクライアント通知を設定するには

1. コンソールで、[クライアント] をクリックし、[クライアント] の下でグループを選択します。
2. [ポリシー] タブの [場所固有のポリシーと設定] で、場所の下の [場所固有の設定] を展開します。
3. [クライアントユーザーインターフェース制御の設定] の右側で、[タスク]、[設定の編集] の順にクリックします。
4. [<グループ名> のクライアントユーザーインターフェース制御の設定] ダイアログボックスで、[サーバー制御] または [混合制御] をクリックします。
5. [混合制御] または [サーバー制御] の横で、[カスタマイズ] をクリックします。
[混合制御] をクリックした場合、[クライアント/サーバー制御の設定] タブで、[侵入防止通知の表示/非表示] の横の [サーバー] をクリックし、[クライアントユーザーインターフェースの設定] タブをクリックします。
6. [クライアントユーザーインターフェースの設定] ダイアログボックスまたはタブで、[侵入防止とメモリエクスプロイト緩和機能の通知の表示] をクリックします。
7. 通知が表示されたときの音を有効にするには、[ユーザーに通知するときにサウンドを使う] をクリックします。
8. [OK] をクリックします。
9. [OK] をクリックします。

侵入防止の管理

[メモリエクスプロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化](#)

管理者通知の設定

カスタム侵入防止シグネチャの管理

特定の侵入を識別してシグネチャが誤認の原因となる可能性を減らすために、独自のネットワーク侵入防止シグネチャを作成できます。カスタムシグネチャに詳しい情報を追加するほど、より効果的なシグネチャになります。

WARNING

侵入防止シグネチャを作成するには、TCP、UDP、ICMP の各プロトコルに精通する必要があります。シグネチャを正しく作成しないと、カスタムシグネチャライブラリが壊れてクライアントの整合性が損なわれる可能性があります。

NOTE

カスタム IPS シグネチャを使うには、ファイアウォールをインストールして有効にする必要があります。[クライアントにインストールするセキュリティ機能の選択](#)

Table 83: カスタム侵入防止シグネチャの管理

タスク	説明
シグネチャグループを含むカスタムライブラリを作成する	カスタムシグネチャを格納するため、カスタムライブラリを作成する必要があります。カスタムライブラリを作成するときには、シグネチャグループを使うとシグネチャを管理しやすくなります。シグネチャを追加する前に少なくとも 1 つのシグネチャグループをカスタムシグネチャライブラリに追加する必要があります。 カスタム IPS シグネチャについて カスタム IPS ライブラリの作成
カスタムライブラリにカスタム IPS シグネチャを追加する	カスタム IPS シグネチャは、カスタムライブラリ内のシグネチャグループに追加します。 カスタム IPS ライブラリへのシグネチャの追加
クライアントグループにライブラリを割り当てる	カスタムライブラリは、場所ではなくクライアントグループに割り当てます。 複数のカスタム IPS ライブラリのグループへの割り当て
シグネチャの順序を変更する	侵入防止では、最初に一致したルールが使われます。Symantec Endpoint Protection はシグネチャリストに記載されている順序でシグネチャを調べます。 たとえば、送信先ポート 80 で両方の方向の TCP トラフィックを遮断するシグネチャグループを追加する場合、次のシグネチャを追加できます。 - ポート 80 のすべてのトラフィックを遮断 - ポート 80 のすべてのトラフィックを許可 すべてのトラフィックを遮断するシグネチャを最初に置くと、すべてのトラフィックを許可するシグネチャが実行されることはありません。すべてのトラフィックを許可するシグネチャを最初に置くと、すべてのトラフィックを遮断するシグネチャが実行されることはなく、HTTP トラフィックは常に許可されます。 Note: ファイアウォールルールは侵入防止シグネチャよりも優先されます。 カスタム IPS シグネチャの順序の変更
シグネチャをコピーして貼り付ける	グループ間やライブラリ間でシグネチャをコピー、貼り付けできます。
シグネチャの変数を定義する	カスタムシグネチャを追加するときには、変数を使ってシグネチャ内の可変データを表すことができます。データが変更された場合には、ライブラリ全体でシグネチャを編集する代わりに変数を編集できます。 カスタム IPS シグネチャの変数の定義
カスタムシグネチャをテストする	カスタム侵入防止シグネチャをテストして、シグネチャが機能することを確認する必要があります。 カスタム IPS シグネチャのテスト

カスタム IPS ライブラリの作成

カスタム IPS シグネチャを格納するにはカスタム IPS ライブラリを作成します。

カスタム侵入防止シグネチャの管理

カスタム IPS ライブラリを作成するには

1. コンソールの [ポリシー] ページの [ポリシー] の下で、[侵入防止] をクリックします。
2. [カスタム侵入防止] タブをクリックします。
3. [タスク] で、[カスタム侵入防止シグネチャの追加] をクリックします。
4. [カスタム侵入防止シグネチャ] ダイアログボックスで、ライブラリの名前と省略可能な説明を入力します。

[NetBIOS グループ] はサンプルのシグネチャグループであり、1 つのサンプルシグネチャが含まれています。既存のグループを編集することも新しいグループを追加することもできます。

5. 新しいグループを追加するには、[シグネチャ] タブの [シグネチャグループ] リストで [追加] をクリックします。
6. [侵入防止シグネチャグループ] ダイアログボックスで、グループ名と省略可能な説明を入力し、[OK] をクリックします。

デフォルトでグループは有効です。シグネチャグループが有効であればグループ内部のすべてのシグネチャが自動的に有効になります。参照用にグループを維持するが設定は無効にする場合には [このグループを有効にする] のチェックマークをはずします。

7. カスタムシグネチャを追加します。

カスタム IPS ライブラリへのシグネチャの追加

カスタム IPS ライブラリへのシグネチャの追加

カスタム侵入防止シグネチャは、新規または既存のカスタム IPS ライブラリに追加します。

カスタム侵入防止シグネチャの管理

カスタムシグネチャを追加するには

1. カスタム IPS ライブラリを作成する

カスタム IPS ライブラリの作成

2. [シグネチャ] タブの [このグループのシグネチャ] で、[追加] をクリックします。
3. [シグネチャの追加] ダイアログボックスで、シグネチャの名前と省略可能な説明を入力します。
4. [重大度] ドロップダウンリストで、重大度を選択します。

シグネチャ条件に一致するイベントはこの重大度を使ってログに記録されます。

5. [方向] ドロップダウンリストで、シグネチャで検査するトラフィックの方向を指定します。
6. [コンテンツ] フィールドに、シグネチャの構文を入力します。

たとえば、いくつかの一般的なプロトコル用のシグネチャでは、次の構文を使います。

HTTP	<pre>rule tcp, dest=(80,443), saddr=\$LOCALHOST, msg="MP3 GET in HTTP detected", regexpcntent="[Gg][Ee][Tt] .*[Mm][Pp]3 ."</pre>
FTP	<pre>rule tcp, dest=(21), tcp_flag&ack, saddr=\$LOCALHOST, msg="MP3 GET in FTP detected", regexpcntent="[Rr][Ee][Tt][Rr] .*[Mm][Pp]3\x0d\x0a"</pre>

構文について詳しくは [ヘルプ] を参照してください。

カスタム侵入防止シグネチャの構文

7. アプリケーションでシグネチャをトリガする場合は、[追加] をクリックします。
8. [アプリケーションの追加] ダイアログボックスで、アプリケーションのファイル名と省略可能な説明を入力します。

たとえば、Internet Explorer アプリケーションを追加するには、ファイル名として `iexplore` または `iexplore.exe` と入力します。ファイル名を指定しないと、すべてのアプリケーションでシグネチャがトリガされます。

9. [OK] をクリックします。

追加したアプリケーションはデフォルトで有効です。当面アプリケーションを無効にする場合は、[有効] 列にあるチェックボックスのチェックマークをはずします。

10. [処理] グループボックスで、シグネチャがイベントを検出したときにクライアントが実行する処理を選択します。

遮断	イベントや攻撃を識別して遮断してセキュリティログに記録します。
許可する	イベントや攻撃を識別して許可してセキュリティログに記録します。

11. イベントや攻撃をパケットログに記録するには、[パケットログに書き込み] にチェックマークを付けます。

12. [OK] をクリックします。

追加したシグネチャはデフォルトで有効です。当面シグネチャを無効にする場合は、[有効] 列にあるチェックボックスのチェックマークをはずします。

13. その他のシグネチャを追加できます。確認が終わったら、[OK] をクリックします。

14. メッセージが表示されたら、カスタム IPS シグネチャをグループに割り当てます。

複数のカスタム IPS ライブラリをグループに割り当てることもできます。

[複数のカスタム IPS ライブラリのグループへの割り当て](#)

カスタム IPS シグネチャの順序の変更

カスタムシグネチャ用の IPS エンジンがシグネチャをシグネチャリストの順に検査します。パケットごとにトリガされるシグネチャは 1 つだけです。シグネチャがインバウンドトラフィックパケットまたはアウトバウンドトラフィックパケットに一致する場合、IPS エンジンが他のシグネチャの検査を停止します。IPS エンジンがシグネチャを正しい順序で検査するように、シグネチャリストでシグネチャの順序を変更できます。複数のシグネチャが一致する場合は、優先度の高いシグネチャを上に移動します。

たとえば、送信先ポート 80 で両方の方向の TCP トラフィックを遮断するシグネチャグループを追加する場合、次のシグネチャを追加できます。

- ポート 80 のすべてのトラフィックを遮断
- ポート 80 のすべてのトラフィックを許可

すべてのトラフィックを遮断するシグネチャを最初に置くと、すべてのトラフィックを許可するシグネチャが実行されることはありません。すべてのトラフィックを許可するシグネチャを最初に置くと、すべてのトラフィックを遮断するシグネチャが実行されることはなく、HTTP トラフィックは常に許可されます。

NOTE

ファイアウォールルールは侵入防止シグネチャよりも優先されます。

カスタム侵入防止シグネチャの管理

カスタム IPS シグネチャの順序を変更するには

1. カスタム IPS ライブラリを開きます。
2. [シグネチャ] タブの [このグループのシグネチャ] 表で、移動するシグネチャを選択して次のいずれかの処理を行います。
 - このシグネチャを上シグネチャよりも前に処理するには、[上に移動] をクリックする
 - このシグネチャを下シグネチャよりも後に処理するには、[下に移動] をクリックする

-
3. このライブラリの設定を完了したら、[OK] をクリックします。

カスタム IPS シグネチャの変数の定義

カスタム IPS シグネチャを追加するとき、変化の多いデータは変数を使って表すことができます。データが変更された場合には、ライブラリ全体でシグネチャを編集する代わりに変数を編集できます。

カスタム侵入防止シグネチャの管理

シグネチャで変数を使う前に、変数を定義する必要があります。カスタムシグネチャライブラリで定義した変数は、そのライブラリのどのシグネチャでも使えます。

既存のサンプル変数からコンテンツをコピーして貼り付けて、コンテンツを作成するベースにできます。

1. カスタム IPS シグネチャの変数を定義するには、カスタム IPS ライブラリを作成します。
2. [カスタム侵入防止シグネチャ] ダイアログボックスで、[変数] タブをクリックします。
3. [追加] をクリックします。
4. [変数の追加] ダイアログボックスで、変数の名前と省略可能な説明を入力します。
5. 変数の値を示す 255 文字以内のコンテンツ文字列を追加します。

変数のコンテンツ文字列を入力するときは、シグネチャのコンテンツに値を入力するときと同じ構文ガイドラインに従ってください。

カスタム侵入防止シグネチャの構文

6. [OK] をクリックします。
変数が表に追加されると、カスタムライブラリのすべてのシグネチャでこの変数を使用できるようになります。
7. カスタム IPS シグネチャで変数を使うには、[シグネチャ] タブで、シグネチャを追加または編集します。
8. [シグネチャの追加] または [シグネチャの編集] ダイアログボックスの [コンテンツ] フィールドに、変数名の前にドル記号 (\$) を付けて入力します。

たとえば、HTTP ポートを指定するための HTTP という名前の変数を作成する場合は、次のように入力します。

\$HTTP

9. [OK] をクリックします。
10. このライブラリの設定を完了したら、[OK] をクリックします。

複数のカスタム IPS ライブラリのグループへの割り当て

カスタム IPS ライブラリを作成したら、個々の場所ではなくグループに割り当てます。そのグループには後でカスタム IPS ライブラリを追加割り当てできます。

カスタム侵入防止シグネチャの管理

複数のカスタム IPS ライブラリをグループに割り当てるには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、カスタムシグネチャを割り当てるグループを選択します。
3. [ポリシー] タブの [場所に依存しないポリシーと設定] で、[カスタム侵入防止] をクリックします。
4. [グループ名 のカスタム侵入防止] ダイアログボックスで、そのグループに割り当てる各カスタム IPS ライブラリの [有効] 列にあるチェックボックスにチェックマークを付けます。
5. [OK] をクリックします。

カスタム IPS シグネチャのテスト

カスタム IPS シグネチャを作成したら、それらをテストして正しく機能することを確認してください。

Table 84: カスタム IPS シグネチャのテスト

手順	説明
ステップ 1: クライアントが現在のポリシーを使っていることを確認する	クライアントは次回のポリシー受信時に、新しいカスタムシグネチャを適用します。 クライアントポリシーの更新
ステップ 2: クライアントでシグネチャのコンテンツをテストする	遮断したいトラフィックをクライアントコンピュータでテストする必要があります。 たとえば、カスタム IPS シグネチャによって MP3 ファイルを遮断する必要がある場合は、クライアントコンピュータにいくつかの MP3 ファイルをダウンロードしてみます。ダウンロードが発生しない場合や多くの試行後にダウンロードがタイムアウトする場合は、カスタム IPS シグネチャが正しく作成されています。 カスタム IPS シグネチャで使うことができる構文について詳しくは、[ヘルプ] をクリックしてください。 カスタム侵入防止シグネチャの構文
ステップ 3: 遮断されたイベントをつの Symantec Endpoint Protection Manager で表示する	ネットワークとホスト悪用防止の攻撃ログのイベントを表示できます。カスタム IPS シグネチャで指定したメッセージはこのログ内に現れます エンドポイント保護の監視

カスタム侵入防止シグネチャの管理

メモリエクスプロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化

- [メモリエクスプロイト緩和機能がアプリケーションを保護する仕組み](#)
- [エクスプロイト防止の種類](#)
- [メモリエクスプロイト緩和機能の要件](#)
- [誤検知の修正と防止](#)
- [メモリエクスプロイト緩和機能イベントのログとレポートの検索](#)
- [アプリケーションを終了させる緩和技術に対する保護の監査](#)
- [メモリエクスプロイト緩和機能の無効化](#)
- [セキュリティレスポンスに誤検知を報告](#)

メモリエクスプロイト緩和機能がアプリケーションを保護する仕組み

バージョン 14 以降の Symantec Endpoint Protection には、メモリエクスプロイト緩和機能が導入されました。この機能では、複数の緩和機能を使用してソフトウェアの脆弱性に対する攻撃を停止させます。たとえば、クライアントユーザーが Internet Explorer などのアプリケーションを実行するときに、代わりに、悪質なコードが含まれた別のアプリケーションが起動される恐れがあります。

エクスプロイトを止めるために、メモリエクスプロイト緩和機能は保護対象のアプリケーションに DLL を挿入します。エクスプロイトの試みを検出すると、メモリエクスプロイト緩和機能はエクスプロイトを遮断するか、エクスプロイトの脅威にさらされたアプリケーションを終了します。Symantec Endpoint Protection は、クライアントコンピュータのユーザーに検出について通知し、クライアントのセキュリティログにイベントを記録します。

たとえば、クライアントユーザーに、次の通知が表示される場合があります。

Symantec Endpoint Protection: 攻撃: 構造化された例外ハンドラの上書きが検出されました。Symantec Endpoint Protection は <アプリケーション名>アプリケーション

クライアントコンピュータで脆弱性が修正されたバージョンのソフトウェアが実行されるまで、メモリエクスプロイト緩和機能はエクスプロイトを遮断し続けるか、アプリケーションを終了します。

NOTE

14 MPx では、メモリエクスプロイト緩和機能は汎用エクスプロイト緩和機能と呼ばれました。

エクスプロイト防止の種類

メモリエクスプロイト緩和機能では、アプリケーションの種類にどの技術が最も適しているかに基づいて、複数の種類の緩和機能を使用してエクスプロイトに対処します。たとえば、StackPvt と RopHeap の両方の技術によって、Internet Explorer を攻撃するエクスプロイトが遮断されます。

Symantec Endpoint Protection メモリエクスプロイト緩和機能の技術

NOTE

機能をコンピュータで有効にしている場合、メモリエクスプロイト緩和機能は、App-V で保護されている Microsoft Office プロセスを保護しません。

メモリエクスプロイト緩和機能の要件

メモリエクスプロイト緩和機能は、侵入防止をインストールしている場合にのみ利用できます。メモリエクスプロイト緩和機能には、侵入防止定義とともにダウンロードされるそれ独自の個別シグネチャがあります。ただし、侵入防止とメモリエクスプロイト緩和機能は、個別に有効または無効にすることができます。

NOTE

14.0.1 以降のメモリエクスプロイト緩和機能には、独自のポリシーが用意されています。14 MPx リリースでは、このポリシーは侵入防止ポリシーの一部になっています。[概要] タブで侵入防止ポリシーを無効にした場合は、メモリエクスプロイト緩和機能が無効になります。

また、メモリエクスプロイト緩和機能ポリシーにアプリケーションリストを表示するには、少なくとも 1 回 LiveUpdate を実行する必要があります。デフォルトで、ポリシーに表示されるすべてのアプリケーションに対して保護が有効化されます。

つの Symantec Endpoint Protection Manager に最新のコンテンツが含まれていることの確認

誤検知の修正と防止

メモリエクスプロイト緩和機能によって、クライアントコンピュータ上のアプリケーションが意図せずに終了されることがあります。そのアプリケーションの動作が正当であり、エクスプロイトされていなかったことが判明した場合、その検出は誤検知になります。シマンテックセキュリティレスポンスでメモリエクスプロイト緩和機能の動作が変更されるまでは、このような誤検知に対する保護を無効にしてください。

以下の表に、誤検知の検出を処理する手順を示します。

Table 85: 誤検知を見つけて修復する手順

タスク	
ステップ 1: クライアントコンピュータで予期せずに終了したアプリケーションを見つける	次の方法で、クライアントコンピュータで予期せずに終了したアプリケーションを見つけることができます。 - クライアントコンピュータのユーザーによって、アプリケーションが実行されていないことが通知されます。 - どの緩和機能によってクライアントコンピュータのアプリケーションが終了されたかを示す、メモリエクспロイト緩和機能のログまたはレポートを開きます。 Note: エクспロイトの性質上、緩和機能でログが生成されない場合もあります。 メモリエクспロイト緩和機能イベントのログとレポートの検索
ステップ 2: 保護を無効化し、アプリケーションを終了した機能を監査する	他のプロセスの保護が維持されるようにするため、まず、必要最低限のレベルで保護を無効化します。他のすべての方法を試し終わるまでアプリケーションを実行できるようにするために、メモリエクспロイト緩和機能はオフにしないようにします。 次の各サブタスクが終了したら、ステップ 3 に進みます。 - まず、緩和機能によって終了された特定のアプリケーションに対する保護を監査します。 たとえば、Mozilla Firefox が終了した場合は、SEHOP 機能または HeapSpray 機能のいずれかを無効にします。エクспロイトの性質上、緩和機能でログイベントが生成されない場合があります。このために、どの緩和技術がアプリケーションを終了したかを明確にできないことがあります。このような場合は、アプリケーションを保護している各機能を 1 つずつ無効にして、終了の原因となっている技術を見つけます。 1 つの緩和機能が保護するすべてのアプリケーションに対する保護を監査します。 - 機能に関係なく、すべてのアプリケーションに対する保護を監査します。この方法はメモリエクспロイト緩和機能の無効化と似ていますが、管理サーバーで検出のためのログイベントが収集される点が異なります。この方法は、14 MPx のレガシークライアントでの誤検知を調べるために使用します。 アプリケーションを終了させる緩和技術に対する保護の監査
ステップ 3: クライアントコンピュータのポリシーをアップデートして、アプリケーションを再実行する	- アプリケーションが正しく実行された場合、その緩和機能に対する検出は誤検知です。 - アプリケーションが期待したようには実行されなかった場合、その検出は真陽性です。 - アプリケーションが引き続き終了する場合は、より高い制限レベルで監査します。たとえば、別の緩和機能を監査したり、その機能で保護されるすべてのアプリケーションを対象に監査を行います。 クライアントポリシーの更新
ステップ 4: 誤検知をレポートし、真陽性に対する保護を再度有効にする	誤検知の場合: - シマンテック社のチームに、検出が誤検知であったことを通知します。「シマンテックインサイダーヒント: ファイルの提出方法」を参照してください。 - 各機能の処理を [いいえ] に設定して、終了したアプリケーションに対する保護が無効なままになるようにします。 - セキュリティレスポンスで問題が解決されたら、機能の処理を [はい] に変更して保護を再度有効にします。 真陽性の場合: - 該当する緩和機能に対するルールを [はい] に戻して、保護を再度有効にします。 - 現在の脆弱性が修正された、感染したアプリケーションのパッチ適用バージョンや新規リリースがあるかどうかを確認します。パッチが適用されたアプリケーションをインストールしたら、クライアントコンピュータで再実行して、メモリエクспロイト緩和機能によってそのアプリケーションが引き続き終了されるかどうかを確認します。

メモリエクспロイト緩和機能イベントのログとレポートの検索

メモリエクスプロイト緩和機能によって終了したアプリケーションを見つけるために、ログを表示してクイックレポートを実行する必要があります。

1. コンソールで次のいずれかの処理を実行します。

- ログの場合は、[監視] > [ログ] > [ネットワークとホストのエクスプロイト緩和機能] ログの種類 > [メモリエクスプロイト緩和機能] ログコンテンツ > [ログの表示] をクリックします。
[メモリエクスプロイト緩和機能によって遮断されたイベント] のイベントの種類を検索します。[イベントの種類] 列には緩和機能のリストが表示され、[処理] 列には [アプリケーション名] 列のアプリケーションが遮断されたかどうかが表示されます。たとえば、次のログイベントは、スタックピボット攻撃を示します。

```
##: Return Oriented Programming #####
```

- クイックレポートの場合は、[レポート] > [クイックレポート] > [ネットワークとホストのエクスプロイト緩和機能] レポートの種類 > [メモリエクスプロイト緩和機能検出] レポート > [レポートの作成] をクリックします。

遮断されたメモリエクスプロイト緩和機能の検出を探します。

終了したアプリケーションに対する保護の監査

誤検知をテストする際に、アプリケーションが実行されたまま検出が監査されるように、メモリエクスプロイト緩和機能の動作を変更します。ただし、メモリエクスプロイト緩和機能はアプリケーションを保護しません。

終了したアプリケーションに対する保護を監査するには

2. コンソールで [ポリシー] > [メモリエクスプロイト緩和機能] > [メモリエクスプロイト緩和機能] をクリックします。

3. [緩和機能] タブの [緩和機能を選択] の隣で、アプリケーションを終了した機能を選択します ([StackPvt] など)。

4. [保護されています] 列で終了したアプリケーションを選択して、[デフォルト (はい)] を [ログのみ] に変更します。

検出が本当に誤検知であることを確認したら、処理を [いいえ] に変更します。[ログのみ] と [いいえ] の両方で、可能性があるエクスプロイトが許可されますが、アプリケーションの実行は継続されます。

一部のアプリケーションには、エクスプロイトを遮断するための複数の緩和機能があります。その場合は、各機能で個別にこのステップに従います。

5. (省略可能) 次のステップのいずれかを行い、[OK] をクリックします。

- どの機能によってアプリケーションが終了されたかが分からない場合は、[このリストにあるすべてのアプリケーションの保護処理を選択] をクリックします。このオプションによって、各機能の設定が上書きされます。
- 14.0.1 クライアントと 14 MPx のレガシークライアントが混在していて、14.0.1 クライアントのみをテストする場合は、[すべての技術の保護処理を「ログのみ」に設定] をクリックします。

6. (省略可能) 機能に関係なくアプリケーションをテストする場合は、[アプリケーションルール] タブの [保護されています] 列で、終了したアプリケーションのチェックマークをはずして [OK] をクリックします。

14 MPx のレガシークライアントの場合は、このオプションのみを使用できます。14.0.1 クライアントにアップグレードした後で保護を再度有効にし、詳細な設定を調整します。[コンピュータの状態] ログを開いて、どのクライアントでどの製品バージョンが実行されているかを確認します。

7. コンソールで、[ポリシー] > [メモリエクスプロイト緩和機能] の順にクリックします。

8. [メモリエクスプロイト緩和機能を有効にする] のチェックマークをはずします。

9. [OK] をクリックします。

10. つの Symantec Endpoint Protection Manager, で Symantec Insight が有効になっていることを確認します。Insight はデフォルトで有効になっています。

[ダウンロードインサイトの設定のカスタマイズ](#)

-
11. クライアントコンピュータで SymDiag ツールをダウンロードして実行します。「[製品の問題を検出するために SymDiag をダウンロードする](#)」を参照してください。
 12. SymDiag ツールの [ホーム] で [サポート用のデータを収集] をクリックし、[デバッグログ] > [拡張] オプションで、[WPP のデバッグ] > [トレースレベル] を [詳細] に設定します。
[Endpoint Protection クライアント用の SymDiag の詳細デバッグログオプション](#)
 13. 誤検知の検出を再現します。
 14. ログの収集が完了した後に、.sdbz ファイルを <https://mysymantec.force.com/customer/s/> に提出します（新しいケースを開くか、既存のケースに新しい情報を更新して）。
 15. 検出されたアプリケーションを [SymSubmit サイト](#) に提出し、以下のタスクを実行します。
 - 検出が発生したタイミングを選択し、[B2 Symantec Endpoint Protection 14.x] 製品を選択し、[C5 - IPS] イベントをクリックします。
 - 送信メモには、前のステップのテクニカルサポートのケース番号、MEM 検出がトリガされたアプリケーション、アプリケーションのバージョン番号に関する詳細を入力します。
たとえば、次のような情報を追加できます: "Blocked Attack: Return Oriented Programming API Invocation attack against C:\Program Files\VideoLAN\VLC\vlc.exe", vlc.exe のバージョンは 2.2.0-git-20131212-0038 です。これは最新の利用可能なバージョンではありませんが、組織で使用する必要があるバージョンです。
[シマンテックインサイダーヒント: ファイルの提出方法](#)
 16. クライアントコンピュータで、次の場所にある提出フォルダのコピーを圧縮します: %PROGRAMDATA%\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\CmnClnt\ccSubSDK。

このフォルダをテクニカルサポートに提出し、以前のステップで開いた誤検知の提出の追跡番号を通知します。テクニカルサポートがすべての必要なログと資料に変更が加えられておらず、誤検知の調査と関連付けられていることを確認します。

Symantec Endpoint Protection メモリエクスプロイト緩和機能の技術

バージョン 14 以降では、メモリエクスプロイト緩和機能 (MEM) が Windows クライアントコンピュータでソフトウェアに対する脆弱性攻撃を防止します。MEM は以下の種類の緩和技術を使用して脆弱性攻撃を防止します。

- **SEHOP** (構造化例外処理の上書き保護) (14)
メモリエクスプロイト緩和機能は、RealPlayer メディアプレーヤーなどのアプリケーションを構造化例外処理の上書きから保護します。悪用攻撃は、例外処理を上書きする関数を使ってソフトウェアの実行フローを制御して攻撃者のシェルコードに導きます。例外処理関数のアドレスは、スタックメモリに格納され、スタックバッファオーバーフローが存在するときに容易に上書きされてしまいます。Windows オペレーティングシステムは SEHOP を備えていますが、一部の Windows Vista オペレーティングシステムではデフォルトでこの保護が無効化されています。Windows で SEHOP が無効でもメモリエクスプロイト緩和機能で保護します。SEHOP の攻撃は、32 ビットクライアントでのみ発生します。
- **Java Security Manager** (14)
メモリエクスプロイト緩和機能は、Windows Security Manager を無効化しようとする Java アプレットを遮断します。一部の悪用攻撃では、Security Manager をオフにして、特権的な処理を実行する Java コードを許可するために Java アプレットが使われます。
- **StackPvt** (スタックピボット) (14.0.1)
スタックピボット技術は、コールスタックアドレスが変更されたかどうかを検出します。変更されている場合は、ESP (exploit changed the stack pointer の略で攻略により変更されたスタックポインタの意味) レジスタが攻略による偽装や攻略により作成されたコールスタックメモリを参照していることを示します。偽装メモリには、ROP 攻撃チェーンが含まれます。
- **ForceDEP** (Force Data Execution Prevention の略でデータ実行防止の強制的意味) (14.0.1)

通常、エクスプロイト攻撃は悪質な実行可能ファイルコード(シェルコードと呼ばれる)をバッファオーバーフローを使用してスタックメモリに挿入するか、ヒープスプレーを使用してヒープメモリに挿入します。次に、これらの場所に対する実行フローを乗っ取ります。この攻撃を緩和するために、Windows XP SP2 以降には、これらのメモリの場所を実行不可としてマーク付けするシステムレベルの保護であるデータ実行防止 (DEP) が備えられています。ただし、この機能には `SetProcessDEPPolicy()` API 呼び出しを使用してオフにできるという問題があります。さらに、DEP でプロセスを保護するには、/NXCOMPAT スイッチを使用してコンパイルする必要があります。ForceDEP 技術は、このスイッチでコンパイルされていないプログラムでも DEP がオフになるのを防止します。

- **ForceASLR** (Force address space layout randomization の略でアドレス空間レイアウトのランダム化の強制の意味) (14.0.1)

オペレーティングシステムを変更または破損させるには、`URLDownloadToFile` や `CreateProcess` などのシステム API を呼び出す必要があります。初期の Windows XP 以前では、`Kernel32.dll` などのシステム DLL は常に固定化された予測可能なメモリの場所にロードされていました。そのため、ハードコードアドレスで簡単に API を呼び出すことができました。さらに、DEP の導入後は ROP (Return-Oriented Programming) というコードを実行する別の方法が考案されて攻略されるようになりました。スタックメモリまたはヒープメモリにシェルコードを書き込んで実行するのではなく、プロセスでロードされたさまざまな DLL の既存の実行可能コードバイトを組み合わせでシェルコードを作成します。このプロセスを防ぐために、Windows Vista 以降のバージョンで ASLR が導入されました。この機能は、メモリ内の DLL のロードアドレスをランダム化して、ハードコードアドレスの使用を無効にします。ただし、DLL をランダムメモリにロードする場合は /DYNAMICBASE スイッチを使用してコンパイルされている必要があります。一部の古い DLL はこのスイッチを使用せずにコンパイルされているため、攻略される可能性があります。このような DLL で、ForceASLR が ASLR を必須にします。

- **HeapSpray** (14)

ヒープスプレー攻撃は、攻撃者が攻撃コードをあらかじめ定められたメモリの場所に配置しようとしたときに発生します。HeapSpray 技術は、通常使用するメモリの場所を予約して攻撃者が使用できないようにします。ヒープスプレー攻撃は、古い Web ブラウザやアプリケーションで見られるバッファ攻撃の一種です。

- **EnhASLR** (Enhance Address space layout randomization の略でアドレス空間レイアウトのランダム化強化の意味) (14.0.1)

EnhASLR 技術は、プロセスでランダムメモリ領域を割り当てます。メモリの割り当てが予測しにくくなると、ヒープスプレーの緩和に役立ちます。EnhASLR は ASLR と DLL の再配置のエントロピーも増やします。

- **NullProt** (Null Page Protection の略で Null ページの保護の意味) (14.0.1)

NULL (0x00000000) は、攻略時に利用できる有効なメモリアドレスです。NullProt 技術は、このメモリの場所を事前に割り当てて攻略されるのを防止します。

- **DllLoad** (14.0.1)

プロセスで、共有フォルダから DLL をロードしないようにします。この技術を逆手にとって悪質なサーバーから \malicious.com\malware.dll のような DLL を直接実行して攻略されることもあります。DllLoad 技術は、ローカルホストアドレス、リンクローカルアドレス、プライベート IP アドレスなど、ローカルネットワーク経由での DLL のリモートロードを防止するものではありません。ロードパスを調べてから実際にロードするまでに、ホスト名を使用して DNS サーバーにリモートパスを問い合わせた結果は異なる場合があります。

以下の緩和技術によって、ROP (Return Oriented Programming) 攻撃から保護します。

- **StackNX** (14.0.1)

StackNX 技術は、`VirtualProtect` などのメモリ保護 API を呼び出してスタックに属するメモリアドレスを実行可能とマーク付けすることを防止します。

- **RopCall** (14.0.1)

システムの重要な API が既存の RET 命令やジャンプ命令ではなく呼び出し命令で呼び出されるようにします。

- **RopHeap** (14.0.1)

ヒープへのメモリ保護 API の呼び出しを拒否し、リターン命令を使用して実行します。

- **RopFlow**

RopFlow 技術は、システムの重要な API を呼び出すときにコールスタックでリターンアドレスの実行をシミュレーションします。RopFlow は RET 命令が別の重要な API を参照しているか、実行可能と適切にマーク付けされていないメモリを参照しているかを調べます。どちらの状況も、ROP 攻撃が発生していることを示します。RopFlow は、最大許容数の命令をシミュレーションしてパフォーマンスに影響が及ばないようにします。

メモリエクスプロイト緩和機能のイベントは、クライアントのセキュリティログと つの Symantec Endpoint Protection Manager のメモリエクスプロイト緩和機能のログに記録されます。これらのイベントは IPS イベントに似ていますが、イベント ID に 61000 から 61999 の範囲のシグネチャ ID を使用する点が異なります。

NOTE

クライアントコンピュータで以下のアプリケーションをインストールまたは有効化している場合、MEM はこれらのアプリケーションが保護するプロセスを保護しません。

Windows EMET (Enhanced Mitigation Experience Toolkit)

Microsoft App-V (Application Virtualization) 機能

[メモリエクスプロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化](#)

クライアントコンピュータに対するウイルスとスパイウェアの攻撃の防止と処理

いくつかの重要なガイドラインに従うことで、クライアントコンピュータに対するウイルスやスパイウェアの攻撃を防止し、処理できます。

Table 86: ウイルスとスパイウェアの攻撃からのコンピュータの保護

タスク	説明
コンピュータに Symantec Endpoint Protection がインストールされていることを確認する	ネットワーク内のすべてのコンピュータとすべてのサーバーに Symantec Endpoint Protection がインストールされている必要があります。Symantec Endpoint Protection が正しく機能していることを確認します。 クライアントコンピュータの保護状態の表示
定義を最新の状態に維持する	最新の定義がクライアントコンピュータにインストールされていることを確認します。定義の日付は [クライアント] タブで確認できます。最新ではない定義はコマンドを実行して更新できます。 コンピュータの状態レポートを実行して、最新の定義の日付を調べることもできます。 クライアント上のコンテンツと定義を更新する方法
定期スキャンを実行する	デフォルトでは、Auto-Protect と SONAR はクライアントコンピュータで実行されます。デフォルトの定時アクティブスキャンもクライアントコンピュータで実行されます。 スキャンはオンデマンドで実行できます。スキャンの設定をカスタマイズできます。 クライアントコンピュータでのオンデマンドスキャンの実行 定時スキャンを作成し、カスタマイズすると便利です。 通常は、1 週間に一度実行する完全な定時スキャン、1 日に一度実行するアクティブスキャンを作成すると便利です。デフォルトでは、Symantec Endpoint Protection は午後 12 時 30 分に行うアクティブスキャンを生成します。管理外コンピュータでは、Symantec Endpoint Protection に無効にされたデフォルトの起動時スキャンも含まれます。 ネットワーク内のコンピュータで毎日アクティブスキャンを実行していることを確認する必要があります。ネットワークに非アクティブな脅威があると疑われる場合は、週または月に 1 回、完全スキャンを実行するようにスケジュール設定することをお勧めします。完全スキャンではコンピュータのリソースがより多く消費され、コンピュータのパフォーマンスに影響することがあります。 Windows コンピュータで実行される定時スキャンの設定 Mac コンピュータで実行される定時スキャンの設定 Linux コンピュータで実行される定時スキャンの設定

タスク	説明
重要なイベントはクライアントにすぐにアップロードさせる	クライアント (Windows のみ) がハートビート間隔をバイパスし、管理サーバーに重要なイベントをすぐに送信できるようにします。重要なイベントには、検出されたすべてのリスク (Cookie を除く) とすべての侵入イベントが含まれます。このオプションは [クライアント]、[ポリシー]、[通信の設定] にあります。このオプションはデフォルトで有効になっています。 関連通知のダンパー期間がなしに設定されるときは、管理者通知からすぐに警告が届きます。 管理者通知の設定 Note: 重要なイベントをすぐに送信できるのは 12.1.4 以降のクライアントだけです。それ以前のクライアントはハートビート間隔だけでイベントを送信します。
保護を強化するためにスキャンの設定を調査または修正する	デフォルトでは、ウイルススキャンとスパイウェアスキャンはウイルスとセキュリティリスクの副作用を検出、除去、修復します。 デフォルトのスキャン設定では、高レベルの保護を提供すると同時にクライアントコンピュータのパフォーマンスが最適化されます。しかし、保護のレベルを高めることができます。 たとえば、Bloodhound のヒューリスティック保護のレベルを高めることもできます。 また、ネットワークドライブのスキャンを有効にできます。 スキャンの調整によるクライアントコンピュータでの保護の強化
クライアントが検出についての情報をシマンテック社に提出することを許可する	クライアントは検出についての情報をシマンテック社に提出できます。この提出された情報は、シマンテック社が脅威に対応する助けになります。 サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について
侵入防止を実行する	シマンテック社はクライアントコンピュータで、ウイルス対策とスパイウェア対策はもとより、侵入防止を実行することを推奨します。 侵入防止の管理
必要な場合は感染を修復する	スキャンの実行後、クライアントコンピュータがまだ感染している場合があります。たとえば、新種の脅威にはシグネチャがなかったり、Symantec Endpoint Protection が完全に脅威を削除できなかったりする場合があります。場合によっては、Symantec Endpoint Protection がクリーニング処理を完了できるようにクライアントコンピュータの再起動が必要になります。 ウイルスとセキュリティリスクの除去

ウイルスとセキュリティリスクの除去

コンピュータに対するウイルスやスパイウェアの攻撃を処理することの一部として、リスクを修復します。

どのコンピュータが感染したかを特定し、修復の結果を表示するには、コンソールのレポート機能と監視機能を使います。

Table 87: ウイルスとセキュリティリスクの除去

手順	説明
ステップ 1: 感染したコンピュータとリスクを伴うコンピュータを識別する	感染したコンピュータとリスクを伴うコンピュータについての情報を 1 つの Symantec Endpoint Protection Manager から入手できます。[ホーム] ページの [ウイルスとリスクの活動の概略] で、[新しく感染した項目] と [まだ感染しています] の数を調べます。[◎新しく感染した項目◎] の数は [◎まだ感染しています◎] のサブセットです。[◎新しく感染した項目◎] の数は、概略で指定した時間間隔の間に感染したコンピュータとリスクを伴うコンピュータの数を示します。 Note: 未修復の SONAR 検出は [未解決感染] としては数えられません。これらは概略では、[◎疑いあり◎] の数に含まれています。 その後のスキャンで感染として検出されたコンピュータは、まだ感染していると見なされます。たとえば定時スキャンでは、部分的にファイルがクリーニングされることがあります。その後の Auto-Protect では、このファイルはリスクとして検出されます。 「まだ感染している」と見なされたファイルは、新しい定義が到着したとき、またはクライアントコンピュータがアイドル状態になるとすぐに再スキャンされます。 感染コンピュータとリスクを伴うコンピュータの識別
ステップ 2: 定義を更新して再スキャンする	クライアントが最新の定義を使っていることを確認してください。 Windows コンピュータで実行されるレガシークライアントの場合は、定時スキャンとオンデマンドスキャンがインサイトルックアップ機能を使っていることも確認する必要があります。14 では、定時スキャンとオンデマンドスキャンは常にインサイトルックアップを使います。 定義の日付は、[感染コンピュータとリスクを伴うコンピュータ] レポートで調べることができます。リスクログから [コンテンツの更新とスキャン] コマンドを実行できます。 [ホーム] ページの [ウイルスとリスクの活動の概略] で、[まだ感染しています] の数と [新しく感染した項目] の数が 0 と表示されていれば、すべてのリスクが除去されています。 クライアント上のコンテンツと定義を更新する方法
ステップ 3: スキャン処理を確認して再スキャンする	スキャンは、リスクを放置するように設定されている場合があります。ウイルスとスパイウェアの対策ポリシーを編集し、リスクカテゴリの処理を変更することができます。次回スキャンが実行されると、Symantec Endpoint Protection は新しい処理を適用します。 処理の設定は、特定のスキャンの種類 (管理者定義やオンデマンドスキャン、または Auto-Protect) の [処理] タブで行います。ダウンロードインサイトと SONAR の検出処理も変更できます。 スキャン処理の確認と識別されたコンピュータの再スキャン
ステップ 4: 必要な場合はコンピュータを再起動して修復を完了する	ウイルスやセキュリティリスクの修復を完了するために再起動が必要な場合には、コンピュータがまだリスク状態にある、または感染している可能性があります。 リスクログを表示すると、いずれかのコンピュータで再起動が必要かどうかを判断できます。コンピュータ状態ログからコマンドを実行してコンピュータを再起動できます。 コンソールを使った、クライアントコンピュータでのコマンドの実行

手順	説明
ステップ 5: 残ったリスクを調査してクリーニングする	リスクが残った場合には、さらに調査する必要があります。 シマンテックセキュリティレスポンス Web ページでウイルスとセキュリティリスクに関する最新情報を確認することができます。 http://www.symantec.com/region/jp/sarcj クライアントコンピュータでは、スキャン結果のダイアログボックスからも、セキュリティレスポンスの Web サイトにアクセスできます。 つの Symantec Endpoint Protection Manager からパワーイレイサーを実行し、面倒で執拗な脅威を分析し、修復できます。Power Eraser は、1 台のコンピュータまたは少数のコンピュータが不安定になったか、深刻に感染したときにのみ、それらのコンピュータで実行する強力な分析機能です。 つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知るべきこと Symantec Technical Support では、脅威の詳細解析を迅速に提供する Threat Expert ツールも提供されています。また、問題のトラブルシューティングに役立つロードポイント分析ツールを実行できます。これらのツールはクライアントコンピュータで直接実行します。 Symantec Diagnostic Tool (SymDiag) を使ったコンピュータの問題のトラブルシューティング
ステップ 6: コンピュータ状態ログを調べる	コンピュータ状態ログを表示し、リスクが修復されるかクライアントコンピュータから削除されたことを確認します。 ログの表示

詳しくは、「[ネットワーク上のウイルス駆除とトラブルシューティング](#)」を参照してください。

[クライアントコンピュータに対するウイルスとスパイウェアの攻撃の防止と処理](#)

[エンドポイント保護の監視](#)

感染コンピュータとリスクを伴うコンピュータの識別

つの Symantec Endpoint Protection Manager の [ホーム] ページとリスクレポートを使って、感染コンピュータとリスクを伴うコンピュータを識別できます。

感染コンピュータを識別するには

1. コンソールで、[ホーム] をクリックし、[ウイルスとリスクの活動の概略] を表示します。

システム管理者には、サイトのコンピュータのうち [新しく感染した項目] と [まだ感染しています] の数が表示されます。ドメイン管理者には、ドメイン内部のコンピュータのうち [新しく感染した項目] と [まだ感染しています] の数が表示されます。

[まだ感染しています] は [新しく感染した項目] のサブセットであり、[まだ感染しています] の数はネットワークからリスクを除去すると減少します。その後のスキャンで感染していると報告されたコンピュータは、まだ感染しています。たとえば、Symantec Endpoint Protection はコンピュータのリスクを部分的にしかクリーニングできていない場合があるので、Auto-Protect は引き続きリスクを検出します。

2. コンソールで、[レポート] をクリックします。
3. [レポートの種類] リストボックスで、[リスク] をクリックします。
4. [レポートの選択] リストボックスで、[感染コンピュータとリスクを伴うコンピュータ] をクリックします。
5. [レポートの作成] をクリックして、表示される感染コンピュータとリスクを伴うコンピュータのリストを書き留めます。

[ウイルスとセキュリティリスクの除去](#)

スキャン処理の確認と識別されたコンピュータの再スキャン

感染コンピュータとリスクを伴うコンピュータがある場合は、コンピュータがまだそれらの状態にある理由を識別する必要があります。感染コンピュータやリスクを伴うコンピュータ上の各リスクに対して適用した処理をチェックします。設定され適用された処理が [放置] だった可能性があります。処理が [放置] だった場合は、コンピュータからリスクをクリーニングするか、ネットワークからコンピュータを削除するか、リスクを受け入れるかいずれかを行う必要があります。Windows クライアントの場合は、ウイルスとスパイウェアの対策ポリシーを編集し、スキャン処理を変更できます。

ウイルスとセキュリティリスクの除去

変更が必要な処理を識別し、識別されたコンピュータを再スキャンするには

1. コンソールで、[監視] をクリックします。
2. [ログ] タブで [リスク] ログを選択して、[ログの表示] をクリックします。

リスクログの [イベント] 列に、どのような状態でどの処理が適用されたかが表示されます。[リスク名] 列には、まだアクティブなリスクの名前が表示されます。[ドメイン] 列には、コンピュータが属しているグループが表示されます。

スキャンで [放置] の処置が適用されたためにクライアントがリスク状態にある場合は、そのグループのウイルスとスパイウェアの対策ポリシーを変更する必要があります。[コンピュータ] 列に、まだアクティブなリスクがあるコンピュータの名前が表示されます。

検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

プッシュモードを使用するようにポリシーが設定されている場合は、次のハートビートのときにそのポリシーがグループのクライアントにプッシュされます。

プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新

3. [戻る] をクリックします。
4. [ログ] タブで [コンピュータの状態] ログを選択して、[ログの表示] をクリックします。
5. 処理を変更して新しいポリシーをプッシュした場合には、新しい設定を使って再スキャンする必要があるコンピュータを選択します。
6. [コマンド] リストボックスで [スキャン] を選択し、[開始] をクリックしてコンピュータを再度スキャンします。

スキャンコマンドの状態は、[コマンドの状態] タブで監視できます。

Windows クライアントがクラウドから定義を受け取る方法

14 以降では、Symantec Endpoint Protection の標準クライアントと埋め込み/VDI クライアントは、クラウド内の定義を使ってリアルタイム保護を提供します。以前のバージョンでは、ダウンロードインサイトなど、さまざまな機能を使って一部のクラウド保護が提供されていました。現在では、すべてのウイルスとスパイウェアの機能はクラウドを使ってファイルを評価します。クラウドコンテンツには、ウイルスとスパイウェアの定義セット、ファイルと潜在的な脅威に関してシマンテック社が保有する最新情報が含まれます。

NOTE

Intelligent Threat Cloud Service は Windows クライアントでのみサポートされます。

クライアントはクラウド対応のコンテンツをサポートします。

クラウド対応コンテンツには、強力な保護を提供する定義の縮小セットが含まれています。クライアントで新しい定義が必要な場合、クライアントは定義をダウンロードするか、クラウド内で定義を検索して、パフォーマンスと速度を改善します。

お使いのクライアントの種類がクラウド対応コンテンツをサポートする必要があります。

お使いのクライアントの種類は、[ヘルプ] > [トラブルシューティング] > [インストール設定] で確認できます。

14 以降では、標準クライアントと埋め込み/VDI クライアントはクラウド対応コンテンツをサポートします。

すべてのスキャンは自動的にクラウドルックアップを使います。

クラウドルックアップには、クラウド内のファイル評価情報と定義確認についての **Symantec Insight** へのクエリーが含まれます。

- 定時スキャンとオンデマンドスキャンでは、クラウドルックアップが自動的に実行されます。
- 自動保護もクラウドルックアップを自動的に実行します。現在では、自動保護はカーネルモードではなくユーザーモードで動作するため、メモリ使用量が削減され、パフォーマンスが向上します。

Intelligent Threat Cloud Service は、ディスク上で定義に使う占有域を削減するだけでなく、スキャン時間を 15%短縮します。

NOTE

12.1.x のインサイトルックアップ機能は、レガシークライアント上のポータルファイルの定時スキャンとオンデマンドスキャンに対してファイル評価ルックアップを提供します。このオプションには個別の感度が使われます。バージョン 14.0.x では、12.1.x クライアントがダウンロードインサイト用に設定されている感度を使用し、インサイトルックアップの有効化または無効化のみが可能です。

クライアントはファイル評価ルックアップの情報をシマンテック社に自動的に送信します。

ネットワークにおけるクラウドルックアップの動作

Symantec Endpoint Protection はクラウドルックアップをクラウドに直接送信します。

プロキシサーバーを使う場合は、クライアントのブラウザのインターネットオプションで HTTPS プロキシを指定できます。または、つの Symantec Endpoint Protection Manager コンソールを使って、[ポリシー] > [外部通信] でクライアントの HTTPS プロキシを指定することもできます。

Intelligent Threat Cloud Service クライアントが使う帯域幅の量は、ダウンロードインサイトなどの特定の機能でのみ評価ルックアップを使用する 14 以前のクライアントの場合とほとんど同じです。

つの **Symantec Endpoint Protection Manager** がユーザーにクラウドルックアップエラーを通知する方法

クライアントがクラウドルックアップの試行に 3 日間成功しない場合、デフォルトで 一つの Symantec Endpoint Protection Manager は電子メール通知をシステム管理者に送信します。この警告は、[監視] > [ログ] > [システムログ] > [クライアント活動] でも確認できます。通知条件の種類は、ファイル評価の検出です。

ポータルファイルとは

ダウンロードインサイトは、サポート対象のポータルからユーザーがダウンロードしたファイルを検査するときに、そのファイルをポータルファイルとしてマークを付けます。定時スキャンとオンデマンドスキャン、Auto-Protect、ダウンロードインサイトは、ダウンロードインサイトに設定された感度レベルを使ってポータルファイルの評価を調査します。

NOTE

ファイルをポータルファイルとしてマークするには、ダウンロードインサイトを有効にする必要があります。

サポート対象のポータルには、Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Google Chrome、Windows Live Messenger、Yahoo! Messenger が含まれます。ポータルリスト (または自動保護ポータルリスト) は、LiveUpdate によって管理サーバーまたはクライアントにダウンロードされるウイルスとスパイウェアの対策のコンテンツの一部です。

スキャンとダウンロードインサイトは、シマンテック社が設定するデフォルトの内部感度レベルを使って非ポータルファイルを常に評価します。この内部デフォルトは、最も悪質なファイルのみを検出します。

実際に使われるクラウドルックアップの例

Intelligent Threat Cloud Service がクライアントを保護する方法の例

- クライアントユーザーが Internet Explorer を実行し、ファイルをダウンロードする。ダウンロードインサイトは、その感度レベルとクラウドにある Symantec Insight からの評価情報を使って、そのファイルが有害でないことを確認します。

Internet Explorer を使ってファイルをダウンロードする。ダウンロードインサイトは、その感度レベルとクラウドにある Symantec Insight からの評価情報を使って、そのファイルが有害でないことを確認します。

- ダウンロードインサイトは、ファイルの評価が受け入れ可能であることを判断し、ダウンロードするファイルを許可して、そのファイルをポータルファイルとしてマークを付けます。
- その後、シマンテック社はその広範な Global Intelligence Network からそのファイルに関する詳しい情報を取得します。シマンテック社は、そのファイルが有害である可能性があることを判断し、インサイト評価データベースを更新します。シマンテック社は、そのファイルの最新のシグネチャをクラウドでの定義で提供する場合があります。
- ユーザーがファイルを開くか、スキャンを実行するときに、自動保護またはスキャンでそのファイルに関する最新の情報をクラウドから取得する。現在では、自動保護またはスキャンは、最新のファイル評価とダウンロードインサイトの感度レベルを使うか、最新のファイルシグネチャを使って、潜在的に悪質なものとしてファイルを検出します。ファイルを開く、またはスキャンを実行するときに、自動保護またはスキャンでそのファイルに関する最新の情報をクラウドから取得する。現在では、自動保護またはスキャンは、最新のファイル評価とダウンロードインサイトの感度レベルを使うか、最新のファイルシグネチャを使って、潜在的に悪質なものとしてファイルを検出します。

必須設定と推奨設定

デフォルトで、**Symantec Endpoint Protection** はクラウドを使います。次のオプションのいずれかを無効にすると、クラウド保護が制限されるか、無効になります。

- Auto-Protect
Auto-Protect が有効になっている必要があります。Auto-Protect はデフォルトで有効になっています。
- ダウンロードインサイト
ダウンロードインサイトを有効にして、それがファイルダウンロードを検査し、今後のスキャンのためにファイルダウンロードをポータルファイルとしてマークを付けることができるようにする必要があります。ダウンロードインサイトを無効にすると、すべてのファイルダウンロードが非ポータルとして扱われます。スキャンは、最も悪質な非ポータルファイルのみを検出します。
- インサイトルックアップ
Insight ルックアップが有効になっている必要があります。インサイトルックアップオプションでは、評価ルックアップとクラウド定義ルックアップを制御します。このオプションはデフォルトで有効になっています。

WARNING

インサイトルックアップを無効にすると、クラウド保護が完全に無効になります。

- 提出
シマンテック社は、情報をシマンテック社と共有することを推奨します。シマンテック社と共有するデータは、検出機能のパフォーマンスを向上するために役立ちます。コンピュータを攻撃する可能性のある潜在的なマルウェアに関する情報は、セキュリティランドスケープを向上して、より迅速に脅威に対応するために役立ちます。シマンテック社は、個人の身元を特定する情報の移動を防ぐため、すべての手段を実施してデータの匿名性を確保します。

[コンピュータの保護を向上するシマンテック社への提出について](#)

クライアントコンピュータでのスキャンの管理

一部のスキャンはデフォルトで実行されますが、設定を変更したり、独自の定時スキャンを設定したいことがあります。スキャンをカスタマイズし、クライアントコンピュータでどれだけの保護を提供するかを変更することもできます。

14 以降では、スキャンはクラウドの完全な定義セットにアクセスします。

[Windows クライアントがクラウドから定義を受け取る方法](#)

Table 88: クライアントコンピュータのスキンの変更

タスク	説明
スキンの種類と標準設定を確認する	スキンの設定を確認します。デフォルトを確認して、変更を加えるかどうかを判断できます。 スキンの種類とリアルタイム保護について デフォルトのウイルスとスパイウェアの対策ポリシーのスキン設定について
定時スキンを作成してオンデマンドスキンを実行する	定時スキンとオンデマンドスキンを使って、Auto-Protect が提供する保護を補うことができます。Auto-Protect は、ファイルを読み書きするときの保護を提供します。定時スキンとオンデマンドスキンは、クライアントコンピュータに存在する任意のファイルをスキンできます。また、メモリ、ロードポイント、クライアントコンピュータの他の重要な場所を保護することもできます。 定時スキンの設定はテンプレートとして保存できます。スキンテンプレートを使うと、複数のポリシーを設定するときに時間を節約できます。テンプレートとして保存した任意のスキンを、異なるポリシーの新しいスキンのベースとして利用できます。 Note: 管理下クライアントに対し、Symantec Endpoint Protection は、クライアントコンピュータ上のすべてのファイル、フォルダ、場所をスキンするデフォルト定時スキンを提供します。 Windows コンピュータで実行される定時スキンの設定 Mac コンピュータで実行される定時スキンの設定 Linux コンピュータで実行する定時スキンの設定 クライアントコンピュータでのオンデマンドスキンの実行
環境のスキン設定をカスタマイズする	管理者定義のスキンのオプションに加えて、Auto-Protect の設定をカスタマイズできます。誤検出の処理、コンピュータやスキンパフォーマンスの最適化、スキン処理や通知の変更を行うために、スキンの設定を変更したいことがあります。 定時スキンについては、未実行のスキン、ランダム化されたスキン、ネットワークドライブをスキンするかどうかのオプションも設定できます。 Windows コンピュータで実行されるウイルススキンとスパイウェアスキンのカスタマイズ Mac コンピュータで実行されるウイルススキンとスパイウェアスキンのカスタマイズ Linux コンピュータで実行するウイルススキンとスパイウェアスキンのカスタマイズ
スキンを調整してクライアントコンピュータのパフォーマンスを改善する	デフォルトでは、Symantec Endpoint Protection はクライアントコンピュータのパフォーマンスへの影響を最小限にするのと同時に、高レベルのセキュリティを提供します。しかし、いくつかの設定を変更するとコンピュータのパフォーマンスをさらに最適化できます。最適化は仮想化された環境で重要です。 Note: クライアントコンピュータのパフォーマンスを最適化するために設定を調整するときには、クライアントコンピュータで一部のセキュリティを低下させる場合があります。 スキンの調整によるクライアントコンピュータパフォーマンスの改善
スキンを調整してクライアントコンピュータでの保護レベルを高める	デフォルトのスキン設定では、高レベルの保護を提供するのと同時にクライアントコンピュータのパフォーマンスが最適化されます。しかし、保護のレベルを高めることができます。 スキンの調整によるクライアントコンピュータでの保護の強化
ダウンロードインサイト検出を管理する	ダウンロードインサイトは、ユーザーが Web ブラウザ、テキストメッセージクライアント、その他のポータルを通してダウンロードを試みるファイルを検査します。ダウンロードインサイトは Symantec Insight からの評価情報を使って、ファイルに関する決定を下します。 ダウンロードインサイト検出の管理
SONAR を管理する	SONAR はクライアントコンピュータに対するプロアクティブ脅威防止の一部です。ただし、SONAR の設定はウイルスとスパイウェアの対策ポリシーの一部です。 SONAR の管理
スキンの例外を設定する	安全だとわかっているファイルとアプリケーションの例外を作成できます。 いくつかのファイルとフォルダも、Symantec Endpoint Protection によって自動的に除外されます。 Symantec Endpoint Protection の例外の管理 Symantec Endpoint Protection がウイルススキンとスパイウェアスキンから除外するファイルとフォルダについて

タスク	説明
検疫にあるファイルを管理する	クライアントコンピュータで検疫されたファイルを監視し、削除できます。 検疫についての設定も指定できます。 Windows クライアント用の検疫の管理
クライアントが検出についての情報をシマンテック社に提出することを許可する	デフォルトでは、クライアントは検出についての情報をシマンテック社に送信します。提出をオフにすることも、クライアントが提出する情報の種類を選択することもできます。 シマンテック社は提出の送信を常にクライアントに許可することを推奨します。この情報はシマンテック社が脅威に対処するために役立ちます。 サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について
クライアントコンピュータに表示されるウイルスとスパイウェアの通知を管理する	クライアントコンピュータにウイルスとスパイウェアのイベントについての通知を表示するかどうかを指定できます。 クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理

スキャンの種類とリアルタイム保護について

Symantec Endpoint Protection には、さまざまな種類のウイルス、脅威、リスクを検出するために、さまざまな種類のスキャンとリアルタイム保護が用意されています。

NOTE

14 以降では、スキャンはクラウドの完全な定義セットにアクセスします。

[Windows クライアントがクラウドから定義を受け取る方法](#)

デフォルトでは、Symantec Endpoint Protection はアクティブスキャンを毎日午後 12 時 30 分に実行します。また、Symantec Endpoint Protection は新しい定義がクライアントコンピュータに届いたときにもアクティブスキャンを実行します。管理外コンピュータでは、Symantec Endpoint Protection に無効にされたデフォルトの起動時スキャンも含まれます。

NOTE

クライアントコンピュータがオフ、休止状態、スリープモードの場合には、コンピュータは定時スキャンを実行していない可能性があります。コンピュータが起動またはスリープ解除すると、デフォルトでは指定された間隔内でスキャンが再試行されます。再試行間隔がすでに期限切れの場合には、Symantec Endpoint Protection はスキャンを実行せず、次の定時スキャンまで待機します。未実行の定時スキャンの設定は修正できます。

ネットワーク内のコンピュータで毎日アクティブスキャンを実行していることを確認する必要があります。ネットワークに非アクティブな脅威があると疑われる場合は、週または月に 1 回、完全スキャンを実行するようにスケジュール設定することをお勧めします。完全スキャンではコンピュータのリソースがより多く消費され、コンピュータのパフォーマンスに影響することがあります。

[クライアントコンピュータでのスキャンの管理](#)

Table 89: スキャンの種類

スキャンの種類	説明
Auto-Protect	Auto-Protect はファイルや電子メールデータがコンピュータに対して読み書きされるときに、それらを連続的に検査します。Auto-Protect は検出されたウイルスとセキュリティリスクを自動的に中和または除去します。Mac クライアントと Linux クライアントではファイルシステムについてのみ Auto-Protect がサポートされます。 14 以降、クラウドに接続されている標準クライアントと埋め込み/VDI クライアントでは、Auto-Protect がクラウドで自動的に最新の定義を検索します。 Linux クライアントの Auto-Protect のカスタマイズ
ダウンロードインサイト (Windows のみ)	ダウンロードインサイトは、ユーザーがブラウザや他のポータルからファイルのダウンロードを試みたときにファイルを検査することで、Auto-Protect スキャンのセキュリティを向上させます。Symantec Insight の評価情報を使って、ダウンロードの試行を許可したり遮断したりします。 ダウンロードインサイトは Auto-Protect の一部として機能するので、Auto-Protect が有効になっている必要があります。 Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法
管理者定義のスキャン	管理者定義のスキャンはクライアントコンピュータ上のすべてのファイルとプロセスを調べて、ウイルスとセキュリティリスクを検出します。管理者定義のスキャンはメモリとロードポイントも検査できます。 次の種類の管理者定義のスキャンを利用できます。 定時スキャン 定時スキャンは指定した時刻にクライアントコンピュータで実行されます。同じ時刻に設定された定時スキャンがあれば順次実行されます。定時スキャンの間にコンピュータがオフ、休止状態、スリープモードになった場合には、未実行のスキャンを再試行するように設定されていなければスキャンは実行されません。コンピュータが起動またはスリープ解除すると、Symantec Endpoint Protection は、スキャンが開始するまで、または再試行間隔が経過するまでスキャンを再試行します。 Windows クライアントのアクティブスキャン、完全スキャン、カスタムスキャンをスケジュール設定できます。Mac クライアントと Linux クライアントの場合、カスタムスキャンだけをスケジュールできます。 定時スキャンの設定はテンプレートとして保存できます。テンプレートとして保存した任意のスキャンを、異なるスキャンのベースとして使うことができます。スキャンテンプレートを使うと、複数のポリシーを設定するときに時間を節約できます。定時スキャンテンプレートは、デフォルトでポリシーに含まれています。デフォルト定時スキャンでは、すべてのファイルとディレクトリがスキャンされます。 起動時スキャンとトリガのスキャン 起動時スキャンはユーザーがコンピュータにログオンするときに実行されます。トリガのスキャンは新しいウイルス定義がコンピュータにダウンロードされたときに実行されます。 Note: 起動時スキャンとトリガのスキャンは Windows クライアントでのみ利用可能です。 オンデマンドスキャン オンデマンドスキャンは つの Symantec Endpoint Protection Manager でスキャンコマンドを選択するとすぐに実行されるスキャンです。 このコマンドは [クライアント] ページまたはログから選択できます。 Windows 用 Symantec Endpoint Protection クライアントが多数のウイルス、スパイウェア、危険度が高い脅威を検出すると、拡張スキャンモードになります。スキャンはインサイトルックアップを再起動してを使います。 このスキャンの期間に対してポリシーで定義されているレベルよりも高い感度で、スキャンによる検出が記録される場合があります。 Windows コンピュータで実行される定時スキャンの設定 Mac コンピュータで実行される定時スキャンの設定
SONAR (Windows のみ)	SONAR はゼロデイ攻撃に対するリアルタイム保護を提供します。SONAR は従来のシグネチャベースの定義が脅威を検出する前であっても攻撃を止めることができます。SONAR は、ヒューリスティックとファイル評価データを使って、アプリケーションまたはファイルについての決定を行います。 SONAR はプロアクティブ脅威スキャンのように、キーロガー、スパイウェア、悪質または潜在的に悪質な可能性がある他のすべてのアプリケーションを検出します。 SONAR について

スキャンの種類	説明
早期起動マルウェア対策 (ELAM) (Windows のみ)	Windows の早期起動マルウェア対策ドライバと連携して働きます。Windows 8 および Windows Server 2012 以降でのみサポートされます。 早期起動マルウェア対策は、ネットワーク上のコンピュータを起動するときやサードパーティドライバを初期化する前にネットワーク上のコンピュータを保護します。 早期起動マルウェア対策 (ELAM) の検出の管理

Auto-Protect の種類について

Auto-Protect は、ファイルのほか、特定の種類の電子メールと電子メールの添付ファイルをスキャンします。

デフォルトでは、すべての種類の Auto-Protect が有効です。Symantec Mail Security などのサーバーベースの電子メールスキャンソリューションを使う場合、電子メール用の Auto-Protect を有効にする必要はありません。

Mac クライアントと Linux クライアントでは電子メールの Auto-Protect スキャンはサポートされません。

Table 90: Auto-Protect の種類

Auto-Protect の種類	説明
Auto-Protect	ファイルがクライアントコンピュータに対して読み書きされるときに、それらを連続的にスキャンします。 Auto-Protect はデフォルトで、ファイルシステムに対して有効になります。自動保護はコンピュータの起動時にロードされます。自動保護はウイルスやセキュリティリスクがないかすべてのファイルを検査し、インストールされないようにセキュリティリスクを遮断します。オプションで、拡張子によるファイルのスキャン、リモートコンピュータでのファイルのスキャン、ブートウイルスを探すフロッピーディスクのスキャンが可能です。また、オプションで、ファイルの修復を試みる前のバックアップ、プロセスの終了、サービスの停止サービスが可能です。 選択した拡張子のファイルだけをスキャンするように Auto-Protect を設定できます。自動保護は選択した拡張子のファイルのスキャンするとき、ウイルスによってファイルの拡張子を変更された場合でもファイルの種類を判定することができます。 電子メール Auto-Protect を実行しないこれらのクライアントでは、Auto-Protect が有効になれば、クライアントコンピュータは保護されています。ほとんどの電子メールアプリケーションは、ユーザーが電子メールの添付ファイルを開くと、それを一時フォルダに保存します。Auto-Protect は一時フォルダに書き込まれときにファイルのスキャンし、ウイルスやセキュリティリスクを検出します。Auto-Protect では、感染した添付ファイルをユーザーがローカルドライブまたはネットワークドライブに保存しようとした場合にもウイルスが検出されます。
Microsoft Outlook Auto-Protect (Windows のみ)	Microsoft Outlook の入力電子メールの添付をダウンロードし、ユーザーがメッセージを閲覧し、添付を開くときにウイルスとセキュリティリスクについてスキャンします。 Microsoft Outlook Auto-Protect は、MAPI またはインターネットプロトコル向けに、Microsoft Outlook 98 から Outlook 2013 をサポートします。Microsoft Outlook Auto-Protect は、32 ビットシステムと 64 ビットシステムをサポートします。 Microsoft Outlook Auto-Protect をパッケージに含め、Microsoft Outlook をコンピュータにすでにインストールしている場合、インストール時に Symantec Endpoint Protection によって Microsoft Outlook Auto-Protect がインストールされます。 ユーザーが低速な接続でサイズの大きな添付ファイルをダウンロードすると、メールのパフォーマンスに影響があります。ドキュメントが安全であることがわかっている場合には、例外を作成できます。 スキャンからのファイルまたはフォルダの除外 Note: Microsoft Exchange Server には Microsoft Outlook Auto-Protect をインストールしないでください。その代わりに、Symantec Mail Security for Microsoft Exchange をインストールする必要があります。

Auto-Protect の種類	説明
インターネット電子メール Auto-Protect (Windows のみ) この機能は 14.2 RU1 より前のクライアントバージョンでのみ利用できます。	インバウンドのインターネット電子メールの本文と添付ファイルをスキャンして、ウイルスとセキュリティリスクをチェックします。アウトバウンド電子メールのヒューリスティックスキャンも実行します。 デフォルトでは、インターネット電子メールの自動保護で、POP3 と SMTP 接続による暗号化パスワードと電子メールがサポートされています。インターネット電子メールの自動保護は、32 ビットシステムまたは 64 ビットシステムをサポートします。SSL (Secure Sockets Layer) を利用する POP3 または SMTP を使う場合に、クライアントはセキュリティで保護された接続を検出しますが、暗号化メッセージはスキャンしません。 Note: パフォーマンス上の理由により、POP3 のインターネット電子メール Auto-Protect は、サーバーオペレーティングシステムではサポートされていません。 電子メールスキャンは Hotmail または Yahoo のような IMAP、AOL、または HTTP ベースの電子メールをサポートしません電子メール。
Lotus Notes Auto-Protect (Windows のみ) この機能は 14.2 RU1 より前のクライアントバージョンでのみ利用できます。	着信する Lotus Notes 電子メールの添付ファイルをスキャンして、ウイルスとセキュリティリスクをチェックします。 Lotus Notes Auto-Protect は Lotus Notes 7.x 以降をサポートします。 Lotus Notes Auto-Protect をパッケージに含め、Lotus Notes をコンピュータにすでにインストールしている場合、インストール時に Symantec Endpoint Protection によって Lotus Notes Auto-Protect がインストールされます。

スキャンの種類とリアルタイム保護について

Windows コンピュータで実行する電子メールスキャンの Auto-Protect のカスタマイズ

ウイルスとセキュリティリスクについて

Symantec Endpoint Protection はウイルスとセキュリティリスクの両方をスキャンします。ウイルスとセキュリティリスクは、電子メールメッセージやインスタントメッセージングプログラムを通して到着する可能性があります。ソフトウェアプログラムのエンドユーザー使用許諾契約を受け入れることで、気付かずにリスクをダウンロードしてしまうこともあります。

多くのウイルスとセキュリティリスクはドライブバイダウンロードとしてインストールされます。これらのダウンロードは通常、ユーザーが悪質な Web サイトや感染した Web サイトにアクセスしたときに発生し、アプリケーションのダウンロードが本物の脆弱性を通してコンピュータにインストールされます。

Symantec Endpoint Protection がウイルスまたはセキュリティリスクを検出したときに実行する処理を変更できます。Windows クライアントの場合、セキュリティリスクのカテゴリは動的であり、シマンテック社がリスクに関する情報を収集するため、時間とともに変化します。

検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

特定のウイルスおよびセキュリティリスクについての情報は、シマンテックセキュリティレスポンスの Web サイトで参照できます。

Table 91: ウイルスとセキュリティリスク

リスク	説明
ウイルス	実行時に自身のコピーを別のコンピュータプログラムまたはファイルに添付するプログラムまたはコード。感染したプログラムを実行すると、添付されたウイルスプログラムがアクティブになり、自身を他のプログラムやファイルに添付します。 ウイルスのカテゴリには、次の種類の脅威が含まれます。 • 悪意のあるインターネットボット インターネット介して自動化されたタスクを実行するプログラム。ボットは、コンピュータへの攻撃を自動化したり、Web サイトから情報を収集したりする目的で使用できます。 • ワーム 他のプログラムに影響を与えることなく複製されるプログラム。ワームには、ディスク間で自身をコピーすることで広がるものや、メモリ内で自己複製してコンピュータのパフォーマンスを低下させるものがあります。 • トロイの木馬 ゲームやユーティリティなどの良性なものの中に隠れたプログラム。 • 複合型脅威 ウイルス、ワーム、トロイの木馬、サーバーの特性と、インターネットの脆弱性を利用して攻撃を開始、伝搬、拡散させるコードが複合された脅威。複合型脅威は複数の方法や技法を使って急速に広がり、広範な損傷を引き起こします。 • ルートキット コンピュータのオペレーティングシステムから自身を隠ぺいするプログラム。
アドウェア	何らかの広告コンテンツを配信するプログラム。
cookie	コンピュータまたはユーザーを識別する目的で Web サーバーが Web ブラウザに送るメッセージ。
ダイヤラー	ユーザーの許可なく、またはユーザーが気付かないうちに、コンピュータを使ってインターネット経由でダイヤル Q2 や FTP サイトにダイヤルするプログラム。一般に、課金により利益を得るためにこれらの番号にダイヤルします。
ハッキングツール	コンピュータへの権限のないアクセスを可能にするためにハッカーが使うプログラムです。ハッキングツールの例としては、キーストロークを追跡して記録し、この情報をハッカーに送信するキーロガーがあります。ハッカーはこの情報を使って、ポートスキャンまたは脆弱性スキャンを実行できます。ハッキングツールは、ウイルスの作成にも使うことができます。
ジョークプログラム	ユーモラスであったり、怖がらせるように、コンピュータの操作を改変したり妨害したりするプログラム。たとえば、ジョークプログラムでは、ユーザーが項目を削除しようすると、ごみ箱がマウスから逃げたりすることがあります。
紛らわしいアプリケーション	コンピュータのセキュリティの状態を意図して不正に表現するアプリケーション。これらのアプリケーションは通常、削除する必要がある偽の感染に関するセキュリティの通知を偽装します。
保護者機能プログラム	コンピュータの使用を監視または制限するプログラム。これらのプログラムは検出されことなく動作する可能性があり、通常は監視情報を別のコンピュータに伝送します。
リモートアクセスプログラム	インターネット経由で別のコンピュータからのアクセスを可能にし、情報収集、攻撃、ユーザーのコンピュータを改変できるようにするプログラム。
セキュリティ評価ツール	コンピュータへの権限のないアクセスを目的とした情報の収集に使われるプログラム。
スパイウェア	密かにシステムの動作を監視し、パスワードやその他の機密情報を検出して別のコンピュータに中継するスタンドアロンプログラム。
トラックウェア	インターネット上でのユーザーのパスを追跡して、管理者やハッカーのシステムに情報を送信するスタンドアロンアプリケーションまたは追加されたアプリケーション。

Symantec Endpoint Protection がウイルススキャンとスパイウェアスキャンから除外するファイルとフォルダについて

Symantec Endpoint Protection は特定のサードパーティのアプリケーションや一部のシマンテック製品が存在することを検出すると、これらのファイルとフォルダのために自動的に除外を作成します。クライアントでは、これらのファイルとフォルダをすべてのスキャンから除外します。

NOTE

コンピュータ上のセキュリティの脆弱性が大幅に高まる可能性があるため、クライアントがシステムの一時フォルダをスキャンから除外することはありません。

スキャンパフォーマンスを改善したり、誤認検出を減らしたりするために、例外ポリシーにファイルまたはフォルダの例外を追加することで、ファイルを除外できます。特定のスキャンに含める拡張子やフォルダも指定できます。

WARNING

スキャンから除外するファイルやフォルダは、ウイルスとセキュリティリスクから保護されません。

クライアントが自動的に作成した除外を表示できます。

Windows レジストリの次の場所を調べます。

- 32 ビットコンピュータでは、HKEY_LOCAL_MACHINE\Software\Symantec\Symantec Endpoint Protection\AV\Exclusions を参照します。
- 64 ビットコンピュータでは、HKEY_LOCAL_MACHINE\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Exclusions を参照します。

WARNING

このレジストリを直接編集しないでください。

Table 92: ファイルとフォルダの除外

ファイル	説明
Microsoft Exchange	クライアントソフトウェアは、Microsoft Exchange Server の次のバージョンに対するファイルとフォルダのスキャンの除外項目を自動的に作成します。 • Exchange 5.5 • Exchange 6.0 • Exchange 2000 • Exchange 2003 • Exchange 2007 • Exchange 2007 SP1 • Exchange 2010 • Exchange 2013 • Exchange 2016 Exchange 2007 のウイルス対策ソフトウェアとの互換性について詳しくは、ユーザーマニュアルを参照してください。環境によっては、Exchange 2007 のフォルダについて、スキャン除外項目を手動で作成する必要がある場合があります。たとえば、クラスタ化されたサーバー環境では、除外項目をいくつか作成する必要があります。 クライアントソフトウェアは、一定の間隔で Microsoft Exchange サーバーのファイルとフォルダの場所の変更をチェックします。クライアントソフトウェアがすでにインストールされているコンピュータに Microsoft Exchange サーバーをインストールした場合、クライアントは変更をチェックしたときに除外項目を作成します。クライアントは、ファイルとフォルダの両方を除外します。除外したフォルダからファイルを移動しても、そのファイルは除外されたままになります。 詳しくは、「SEP が Microsoft Exchange 2007/2010 ディレクトリ構造をスキャンしないように設定する方法」を参照してください。
Microsoft Forefront	クライアントは次の Microsoft Forefront 製品のためにファイルとフォルダの除外を自動的に作成します。 • Forefront Server Security for Exchange • Forefront Server Security for SharePoint • Forefront Threat Management Gateway 推奨される除外のリストについては、Microsoft 社の Web サイトを確認してください。 「Microsoft Forefront 向けに Symantec Endpoint Protection の例外を設定する」という記事も参照してください。
Active Directory ドメインコントローラ	クライアントは、Active Directory ドメインコントローラのデータベース、ログ、作業ファイルに関するファイルとフォルダの除外項目を自動的に作成します。クライアントは、クライアントコンピュータにインストールされているアプリケーションを監視します。このソフトウェアがクライアントコンピュータ上で Active Directory を検出した場合は、自動的に例外項目が作成されます。
シマンテック製品	クライアントは、特定のシマンテック製品が検出されると、それらに対する適切なファイルとフォルダのスキャンの除外項目を自動的に作成します。 クライアントソフトウェアでは、次のシマンテック製品について除外項目を自動的に作成します。 • Symantec Mail Security 4.0、4.5、4.6、5.0、6.0 for Microsoft Exchange • Symantec AVF 3.0 for Microsoft Exchange • ノートン アンチウイルス 2.x Microsoft Exchange 版 • つの Symantec Endpoint Protection Manager デフォルトデータベース (Microsoft SQL Server Express または埋め込みデータベース) およびログ
ベリタス製品	クライアントは、特定のベリタス製品が検出されると、それらに対する適切なファイルとフォルダのスキャンの除外項目を自動的に作成します。 この機能は、12.1.6 MP4 で利用可能です。 • Veritas Backup Exec • Veritas NetBackup • Veritas System Recovery Veritas Netbackup の自動除外のサポートは 8.x で終了しました。

ファイル	説明
選択した拡張子と Microsoft 社関係のフォルダ	各種の管理者定義のスキャンや Auto-Protect では、対象に含めるファイルを拡張子によって選択できます。管理者定義のスキャンの場合は、対象に含めるファイルをフォルダによって選択することもできます。たとえば、定時スキャンでは特定の拡張子のみをスキャンし、Auto-Protect ではすべての拡張子を選択するように指定できます。 実行可能ファイルと Microsoft Office ファイルの場合には、ウイルスによって拡張子を変更されていても Auto-Protect がファイルの種類を特定できます。 デフォルトでは、Symantec Endpoint Protection はすべての拡張子のファイルとフォルダをスキャンします。選択解除した拡張子やフォルダはそのスキャンから除外されます。 どの拡張子についても、それらをスキャンから除外することは推奨されません。しかし、拡張子や Microsoft 社関係のフォルダによってファイルを除外する場合は、ネットワークに必要な保護のレベルを考慮してください。クライアントコンピュータがスキャンを完了するために必要とする時間とリソースも考慮する必要があります。 Note: ファイルシステムの Auto-Protect スキャンから除外した拡張子はすべて、ダウンロードインサイトからも除外されます。ダウンロードインサイトを実行する場合、スキャンする拡張子のリストに、一般的なプログラムとデータファイルの拡張子を含める必要があります。 .msi ファイルをスキャンすることを確認する必要があります。
ファイルとフォルダの例外	Symantec Endpoint Protection 例外ポリシーを使って、すべてのウイルススキャンとスパイウェアスキャンから除外するファイルまたはフォルダの例外を作成します。 Note: デフォルトでは、クライアントコンピュータのユーザーはファイルとフォルダの例外も作成できます。 たとえば、電子メールアプリケーションの受信ボックス用にファイルの除外を作成できます。クライアントがオンデマンドスキャンまたは定時スキャン中に受信ボックスのファイル内でウイルスを検出した場合、クライアントは受信ボックス全体を検疫します。そうする代わりに、受信ボックスのファイルを除外する例外を作成できます。ただし、ユーザーが電子メールメッセージを開いたときにクライアントがウイルスを検出した場合は、クライアントは今までどおりメッセージを検疫または削除します。
信頼ファイル	ウイルススキャンとスパイウェアスキャンでは Insight が使用されます。これにより、信頼できるファイルがスキャンでスキップされます。スキップするファイルの信頼のレベルを選択することも、オプションを無効にすることもできます。オプションを無効にすると、スキャン時間が増加することがあります。 Auto-Protect では、Windows Search などの信頼できるプロセスがアクセスするファイルをスキップすることもできます。

スキャンからのファイルまたはフォルダの除外

デフォルトのウイルスとスパイウェアの対策ポリシーのスキャン設定について

つの **Symantec Endpoint Protection Manager** には 3 つのデフォルトのポリシーが用意されています。

- ウイルスとスパイウェアのバランス型対策ポリシー
- ウイルスとスパイウェアの対策のセキュリティ重視ポリシー
セキュリティ重視のポリシーは、すべての事前設定済みのポリシーでもっとも厳格なものです。これによって、その他のアプリケーションのパフォーマンスに影響する可能性があることに留意してください。
- ウイルスとスパイウェアの対策のパフォーマンス重視ポリシー
パフォーマンス重視のポリシーでは、セキュリティ重視のポリシーよりもパフォーマンスは向上しますが、同じ保全是得られません。この場合、ポリシーは主に Auto-Protect を使って、選択した拡張子を持つファイルをスキャンし、脅威を検出します。

基本のウイルスとスパイウェアの対策ポリシーは、セキュリティとパフォーマンスをほどよくバランスさせたものです。

Table 93: ウイルスとスパイウェアのバランス型対策ポリシーのスキャン設定

設定	説明
ファイルシステムに対する Auto-Protect	有効 ダウンロードインサイトの悪質なファイルの感度はレベル 5 に設定されます。ダウンロードインサイトでの未確認ファイルの処理は [無視] です。 Auto-Protect には次の設定が含まれています。 • ウイルスとセキュリティリスクがないかすべてのファイルをスキャンします。 • セキュリティリスクのインストールを遮断します。 • ウイルスに感染したファイルをクリーニングします。修復する前にファイルをバックアップします。クリーニングできないファイルを検疫します。 • セキュリティリスクがあるファイルを検疫します。検疫できないファイルをログに記録します。 • ブートウイルスがないかすべてのフロッピーディスクを調べます。ブートウイルスをログに記録します。 • ウイルスとセキュリティリスクについてコンピュータのユーザーに通知します。
電子メールに対する Auto-Protect	有効 他の種類の Auto-Protect には次の設定が含まれています。 • 圧縮ファイルの内部にあるファイルを含め、すべてのファイルをスキャンします。 • ウイルスに感染したファイルをクリーニングします。クリーニングできないファイルを検疫します。 • セキュリティリスクがあるファイルを検疫します。検疫できないファイルをログに記録します。 • 検出されたウイルスとセキュリティリスクについてのメッセージをコンピュータのユーザーに送信します。
SONAR	有効 • 高危険度のヒューリスティック検出は検疫されます。 • 低危険度のヒューリスティック検出はログに記録します。 • 拡張モードは無効にされます。 • [検出時に警告を表示する] は有効になります。 • システム変更検出の処理は [無視] に設定されます。 • 疑わしい動作の検出では、高危険度の脅威が遮断され、低危険度の脅威は無視されます。
管理者定義のスキャン	定時スキャンには次のデフォルトの設定が含まれています。 • アクティブスキャンを毎日午後 12 時 30 分に実行します。スキャンはランダム化されます。 • 圧縮ファイルに含まれるファイルを含め、すべてのファイルとフォルダをスキャンします。 • メモリ、一般的な感染場所、既知のウイルスやセキュリティリスクの場所をスキャンします。 • ウイルスに感染したファイルをクリーニングします。修復する前にファイルをバックアップします。クリーニングできないファイルを検疫します。 • セキュリティリスクがあるファイルを検疫します。検疫できないファイルをログに記録します。 • 3 日以内の未実行のスキャンを再試行します。 オンデマンドスキャンは次の保護を提供します。 • 圧縮ファイルに含まれるファイルを含め、すべてのファイルとフォルダをスキャンします。 • メモリと一般的な感染場所をスキャンします。 • ウイルスに感染したファイルをクリーニングします。修復する前にファイルをバックアップします。クリーニングできないファイルを検疫します。 • セキュリティリスクがあるファイルを検疫します。検疫できないファイルをログに記録します。

デフォルトのウイルスとスパイウェアのセキュリティ重視ポリシーは、高レベルのセキュリティを提供し、ウイルスとスパイウェアの対策ポリシーに含まれる設定の多くを含んでいます。このポリシーでは強化されたスキャンが提供されます。

Table 94: ウイルスとスパイウェアの対策のセキュリティ重視ポリシーの設定

設定	説明
ファイルシステムと電子メールに対する Auto-Protect	ウイルスとスパイウェアのバランス型対策ポリシーと同様です。 Auto-Protect はリモートコンピュータ上のファイルも検査します。
SONAR	ウイルスとスパイウェアのバランス型対策ポリシーと同様ですが、次の点が違います。 システム変更イベントを遮断します。
グローバル設定	Bloodhound は [拡張] に設定されます。 Note: [拡張] オプションでは、おそらくより多くの誤検知が生成されます。このオプションは詳しい知識のあるユーザーにのみお勧めします。

デフォルトのウイルスとスパイウェアの対策のパフォーマンス重視ポリシーは、高レベルのパフォーマンスを提供します。このポリシーには、ウイルスとスパイウェアの対策ポリシーにある設定の多くが含まれます。このポリシーではセキュリティは低下します。

Table 95: ウイルスとスパイウェアの対策のパフォーマンス重視ポリシーの設定

設定	説明
ファイルシステムに対する Auto-Protect	ウイルスとスパイウェアのバランス型対策ポリシーと同様ですが、次の点が違います。 ダウンロードインサイトの悪質なファイルの感度はレベル 1 に設定されます。
Microsoft Outlook Auto-Protect インターネット電子メール Auto-Protect* Lotus Notes Auto-Protect* * 14.2 RU1 より前のクライアントバージョンでのみ利用可能	無効
SONAR	ウイルスとスパイウェアのバランス型対策ポリシーと同様ですが、次の点が違います。 - システム変更イベントは無視します。 - 動作ポリシーエンフォースメントのイベントは無視します。
管理者定義のスキャン	ウイルスとスパイウェアのバランス型対策ポリシーと同様です。

Symantec Endpoint Protection がウイルスとセキュリティリスクの検出を処理する方法

Symantec Endpoint Protection はデフォルトの処理を使ってウイルスとセキュリティリスクの検出を処理します。デフォルトの一部は変更できます。

Table 96: Symantec Endpoint Protection がウイルスとセキュリティリスクの検出を処理する方法

検出	説明
ウイルス	デフォルトでは、Symantec Endpoint Protection クライアントはまずウイルスに感染したファイルをクリーニングしようと試みます。 クライアントソフトウェアがファイルをクリーニングできない場合は次の処理を実行します。 • ファイルを感染コンピュータ上の [検疫] に移動する • ファイルへのアクセスを拒否する • イベントをログに記録する
セキュリティリスク	デフォルトでは、クライアントはセキュリティリスクに感染したすべてのファイルを感染コンピュータの [検疫] に移動します。また、リスクの副作用の削除または修復も試みます。 セキュリティリスクの検疫と修復ができない場合、第 2 の処理はリスクをログに記録することです。 デフォルトでは、[検疫] にはクライアントが実行したすべての処理の記録が格納されます。クライアントが削除と修復を試みる前の状態にクライアントコンピュータを戻すことができます。

SONAR による検出は、疑わしいイベントと見なされます。これらの検出の処理は SONAR 設定の一部として設定します。

SONAR の管理

Windows クライアントと Linux クライアントの場合、リスクを見つけたときに Symantec Endpoint Protection が実行する第 1 と第 2 の処理を割り当てることができます。ウイルスとセキュリティリスクには異なる処理を設定できます。定時スキャン、オンデマンドスキャン、Auto-Protect スキャンのそれぞれに異なる処理を適用できます。

14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。

NOTE

cookie をログに記録することを指定しない限り、危険な cookie は常に削除されます。cookie に対しては [削除]、[放置する (ログのみ)] のいずれかの 1 つの処理のみを指定できます。

NOTE

Windows クライアントでは、セキュリティリスクの検出の種類のリストは動的であり、シマンテック社が新しいカテゴリを発見すると変更されます。新しいカテゴリは、新しい定義の受信時にコンソールまたはクライアントコンピュータにダウンロードされます。

Mac クライアントの場合、見つけた感染ファイルを Symantec Endpoint Protection で修復するかどうかを指定できます。Symantec Endpoint Protection で修復できない感染ファイルを検疫に移動するかどうかも指定できます。定時スキャン、オンデマンドスキャン、Auto-Protect スキャンのそれぞれに異なる処理を適用できます。

Windows クライアント用の検疫の管理

Windows 8 コンピュータでの検出に対する Symantec Endpoint Protection の処理方式

Symantec Endpoint Protection は、Windows 8 形式のユーザーインターフェースと、Windows 8 デスクトップの両方を保護します。ただし、Windows 8 形式のアプリケーションやファイルに関連した検出に対する処理は、他の検出に対する処理とは異なる方式で機能します。

Windows 8 形式のユーザーインターフェース上にホストされるアプリケーションは、オペレーティングシステムの他のプロセスから検疫されたコンテナ内で実装されます。Symantec Endpoint Protection は、Windows 8 形式アプリケーションまたはファイルに影響する検出に対し、クリーニングや検疫を行いません。これらのアプリケーションとファイルに関連する検出に対しては、Symantec Endpoint Protection は削除するか、ログに記録するのみです。

Windows 8 形式のアプリケーションとファイルに関連しない検出に対しては、Symantec Endpoint Protection は他の Windows オペレーティングシステムで通常行われるように、検疫して修復することが可能です。

ウイルスとスパイウェアの対策ポリシーの処理を設定したり、レポートを実行する場合には、この違いを考慮してください。

[Windows 8 クライアントで表示されるポップアップ通知について](#)

[Symantec Endpoint Protection がウイルスとセキュリティリスクの検出を処理する方法](#)

Windows コンピュータで実行される定時スキャンの設定

定時スキャンは、ウイルスとスパイウェアの対策ポリシーの一部として設定します。

ネットワークセキュリティの Windows コンピュータに定時スキャンを設定するときは次の重要な点を考慮してください。

複数の同時スキャンが順次実行される	複数のスキャンを同じコンピュータ上で実行するようにスケジュール設定し、スキャンが同時に始まる場合には、スキャンは順次実行されます。1つのスキャンが終わってから次のスキャンが始まります。たとえば、同じコンピュータ上で3つの別々のスキャンが午後1時に実行されるように設定するとします。それぞれのスキャンで別のドライブをスキャンします。1つのスキャンがドライブ C、2つ目のスキャンがドライブ D、3つ目のスキャンがドライブ E をスキャンします。この例では、ドライブ C、D、E をスキャンする1つの定時スキャンを作成するほうがよいでしょう。
未実行の定時スキャンが実行されない可能性がある	定時スキャンが何らかの理由で実行されなかった場合、デフォルトでは、Symantec Endpoint Protection は、そのスキャンを開始するまで、または指定された時間間隔が経過するまで、スキャンを実行しようとはします。Symantec Endpoint Protection が未実行のスキャンを試行期間内に開始できない場合、そのスキャンは実行されません。
定時スキャンの時間が変わる可能性がある	スキャン期間または未実行の定時スキャン設定が原因で、前回のスキャンが別の時刻に実行された場合、Symantec Endpoint Protection は設定された時刻を使わないことがあります。たとえば、週ごとのスキャンを毎週日曜日の深夜に実行し、再試行間隔を1日に設定したとします。スキャンが実行されず、コンピュータを月曜日の午前6時に起動した場合は午前6時にスキャンが実行されます。次のスキャンは、次の日曜日の深夜ではなく、月曜日から1週間後の午前6時に実行されます。コンピュータが火曜日の午前6時まで再起動されなかった場合は、再試行間隔が2日を超えるため、Symantec Endpoint Protection はスキャンを再試行しません。次の日曜日の深夜までスキャンの実行を待機します。どちらの場合も、スキャン開始時刻をランダム化した場合は、スキャンの前回の実行時刻が変わることがあります。

NOTE

Windows 設定には、他のオペレーティングシステムで実行されるクライアントでは利用できないオプションが含まれています。

この手順で使うオプションについて詳しくは [ヘルプ] を参照してください。

Windows コンピュータで実行される定時スキャンを設定するには

-
1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
 2. [Windows の設定] で、[管理者定義のスキャン] をクリックします。
 3. [スキャン] タブの [定時スキャン] で、[追加] をクリックします。
 4. [定時スキャンの追加] ダイアログボックスで、[新しい定時スキャンを作成する] をクリックします。
 5. [OK] をクリックします。
 6. [定時スキャンの追加] ダイアログボックスの [スキャンの詳細] タブで、追加する定時スキャンの名前と説明を入力します。
 7. [アクティブスキャン]、[完全スキャン]、[カスタムスキャン] のいずれかをクリックします。
 8. [カスタム] を選択した場合、[スキャン] で、スキャンするフォルダを指定できます。
 9. [ファイルの種類] で、[すべてのファイルをスキャンする] または [選択した拡張子のみをスキャンする] をクリックします。

NOTE

定時スキャンでは、[スキャンの拡張オプション] で [圧縮ファイル内部のファイルをスキャンする] オプションを無効にしない限り、またはコンテナファイル拡張子用の特定の例外を作成しない限り、コンテナファイルが常にスキャンされます。

10. [次の項目を調べることによってスキャンを拡張] で、[メモリ]、[感染しやすい場所]、[既知のウイルスやセキュリティリスクの場所] にチェックマークを付けるかは必ずしもありません。
11. [スケジュール] タブの [スキャンスケジュール] で、スキャンを実行する頻度と時刻を設定します。
[未実行の定時スキャン] の再試行の設定は、[日単位]、[週単位]、[月単位] のどれを選択したかに応じて自動的に変化します。
12. [未実行の定時スキャン] では、未実行のスキャンを実行するオプションを無効にするか、再試行間隔を変更できます。
スキャンが一時停止するまでの、最長のスキャン期間も指定できます。また、スキャンの開始時間をランダム化できます。
13. このスキャンをテンプレートとして保存する場合は、[複製を定時スキャンテンプレートとして保存する] にチェックマークを付けます。
14. [OK] をクリックします。

クライアントコンピュータでのスキャンの管理

Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

Windows クライアントと Linux クライアントのウイルススキャンとスパイウェアスキャンからファイル拡張子を除外する

Mac コンピュータで実行される定時スキャンの設定

定時スキャンは、ウイルスとスパイウェアの対策ポリシーの一部として設定します。

クライアントコンピュータでのスキャンの管理

Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

NOTE

Mac 設定には、Windows で実行されるクライアントで利用できるオプションの一部が含まれていません。

Mac コンピュータで実行される定時スキャンを設定するには

-
1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
 2. [Mac の設定] で、[管理者定義のスキャン] をクリックします。
 3. [スキャン] タブの [定時スキャン] で、[追加] をクリックします。
 4. [定時スキャンの追加] ダイアログボックスで、[新しい定時スキャンを作成する] をクリックしてから [OK] をクリックします。
 5. [定時スキャンの追加] ダイアログボックスの [スキャンの詳細] タブで、スキャンの名前と説明を入力します。
 6. [ドライブとフォルダをスキャン] で、スキャンする項目を指定します。
 7. [スケジュール] タブの [スキャンスケジュール] で、スキャンを実行する頻度と時刻を設定します。
 8. このスキャンをテンプレートとして保存する場合は、[複製を定時スキャンテンプレートとして保存する] にチェックマークを付けます。
 9. [OK] をクリックします。

Linux コンピュータで実行する定時スキャンの設定

定時スキャンは、ウイルスとスパイウェアの対策ポリシーの一部として設定します。

Linux コンピュータで実行する定時スキャンを設定するには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Linux の設定] で、[管理者定義のスキャン] をクリックします。
3. [スキャン] タブの [定時スキャン] で、[追加] をクリックします。
4. [定時スキャンの追加] ダイアログボックスで、[定時スキャンの追加] をクリックします。
5. [定時スキャンの追加] ダイアログボックスの [スキャンの詳細] タブで、追加する定時スキャンの名前と説明を入力します。
6. [フォルダの種類] で、[すべてのフォルダをスキャン] をクリックするかまたはスキャンするフォルダを指定します。
7. [ファイルの種類] で、[すべてのファイルをスキャンする] または [選択した拡張子のみをスキャンする] をクリックします。

14.3 RU1 以降、[選択した拡張子のみをスキャンする] オプションは利用できません。

NOTE

[圧縮ファイル内部のファイルをスキャンする] オプションを無効にするか、またはコンテナファイル拡張子に特定の例外を作成しないと、定時スキャンはコンテナファイルを常にスキャンします。

8. [追加オプション] で、[セキュリティリスクをスキャンする] にチェックマークを付けるか、またはチェックマークをはずします。
9. [スケジュール] タブの [スキャンスケジュール] で、スキャンを実行する頻度と時刻を設定します。
[未実行の定時スキャン] の再試行の設定は、[日単位]、[週単位]、[月単位] のどれを選択したかに応じて自動的に変化します。

-
10. [未実行の定時スキャン] では、未実行のスキャンを実行するオプションを無効にするか、再試行間隔を変更できます。
 11. このスキャンをテンプレートとして保存する場合は、[複製を定時スキャンテンプレートとして保存する] にチェックマークを付けます。
 12. [OK] をクリックします。

クライアントコンピュータでのスキャンの管理

クライアントコンピュータでのオンデマンドスキャンの実行

リモートの管理コンソールから、クライアントコンピュータで手動でのスキャン、つまりオンデマンドスキャンを実行できます。クライアントコンピュータに対するウイルス攻撃とスパイウェア攻撃を防止して処理する戦略の一部として、オンデマンドスキャンを実行することを推奨します。

デフォルトでは、アクティブスキャンは定義の更新後、自動的に実行されます。完全スキャンまたはカスタムスキャンとしてオンデマンドスキャンを設定し、その後、より広範なスキャンのオンデマンドスキャンを実行できます。

オンデマンドスキャンの設定は、定時スキャンの設定に類似しています。

Windows クライアントコンピュータの場合は、オンデマンドでアクティブスキャン、完全スキャン、カスタムスキャンを実行できます。Mac クライアントコンピュータと Linux クライアントコンピュータの場合は、カスタムオンデマンドスキャンのみ実行できます。

カスタムスキャンでは、ウイルスとスパイウェアの対策ポリシーでオンデマンドスキャン用に設定した設定が使われます。

NOTE

オンデマンドスキャンを実行しているクライアントコンピュータで再起動コマンドを発行した場合、スキャンは停止し、クライアントコンピュータが再起動します。スキャンは再開されません。

オンデマンドスキャンは、コンピュータ状態ログまたはコンソールの [クライアント] タブから実行できます。

コンピュータ状態ログからは、選択されたクライアントに対して進行中のスキャンとキューに入っているスキャンをすべてキャンセルできます。コマンドを確認すると、テーブルが更新され、コマンド状態テーブルにキャンセルコマンドが追加されます。

クライアントコンピュータでオンデマンドスキャンを実行するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、スキャンするグループまたはクライアントを右クリックします。
3. 次のいずれかの処理を実行します。
 - [グループでコマンドを実行] > [スキャン] を選択します。
 - [コンピュータでコマンドを実行] > [スキャン] を選択します。
- [コンテンツの更新とスキャン] をクリックして 1 つの手順で定義を更新してスキャンを実行します。
4. Windows クライアントの場合、[アクティブスキャン]、[完全スキャン]、[カスタムスキャン] のいずれかを選択し、[OK] をクリックします。

クライアントコンピュータでのスキャンの管理

クライアントコンピュータに対するウイルスとスパイウェアの攻撃の防止と処理

コンソールを使った、クライアントコンピュータでのコマンドの実行

クライアントコンピュータで実行できるコマンドについて

スキヤンの調整によるクライアントコンピュータパフォーマンスの改善

デフォルトでは、クライアントコンピュータのリソースに対する影響が最小限になるようにウイルスとスパイウェアのスキヤンが行われます。いくつかのスキヤン設定を変更するとパフォーマンスをさらに最適化できます。ここで推奨するタスクの多くは、仮想コンピュータ (VM) のゲストオペレーティングシステムで Symantec Endpoint Protection を実行する環境で有効です。

Table 97: スキヤンを調整し、Windows コンピュータでのパフォーマンスを改善するには

タスク	説明
定時スキヤンとオンデマンドスキヤンの調整オプションと圧縮ファイルオプションを修正する	定時スキヤンとオンデマンドスキヤンについて、次のオプションを調整できます。 - 調整オプションの変更 スキヤン調整を [アプリケーションに最適なパフォーマンス] に変更できます。この設定でスキヤンを設定すると、スキヤンを開始することはできますが、クライアントコンピュータがアイドルのときだけ実行されます。新しい定義を受信したときにアクティブスキヤンが実行されるように設定しても、ユーザーがコンピュータを使っている場合、スキヤンは最大 15 分間実行されないことがあります。 - 圧縮ファイルをスキヤンするレベル数の変更 デフォルトのレベルは 3 です。スキヤン時間を減らすためにレベルを 1 や 2 に変更したいことがあります。 Windows コンピュータで実行されるクライアントに対する管理者定義のスキヤンのカスタマイズ
再開可能スキヤンの使用	大容量のボリュームを持つネットワーク内のコンピュータの場合、定時スキヤンは再開可能スキヤンとして設定できます。 スキヤン期間オプションにより、スキヤンを実行する期間を指定できます。スキヤンが指定した期間の終りまでに完了しない場合、次の定時スキヤン期間になったときにスキヤンが再開されます。ボリューム全体がスキヤンされるまで、スキヤンは停止した場所で再開されます。通常、スキヤン期間のオプションはサーバーで使います。 Note: コンピュータが感染したことが疑われる場合は、再開可能スキヤンを使わないでください。コンピュータ全体をスキヤンするまで実行される完全スキヤンを実行してください。指定した期間より前にスキヤンが完了できる場合も再開可能スキヤンを使わないでください。 Windows コンピュータで実行される定時スキヤンの設定
Auto-Protect 設定を調整する	ファイルシステムの自動保護スキヤンの一部の設定を調整できます。それらの設定により、クライアントコンピュータのパフォーマンスが改善されることがあります。 次のオプションを設定できます。 - ファイルキャッシュ ファイルキャッシュが有効になっていることを確認してください (デフォルトは有効)。ファイルキャッシュを有効にすると、Auto-Protect はスキヤンした未感染のファイルを記憶し、それらのファイルを再スキヤンしません。 - ネットワークの設定 リモートコンピュータの自動保護スキヤンが有効になっている場合は、[ファイルの実行時のみ] を有効になっていることを確認してください。 Windows クライアントの Auto-Protect のカスタマイズ
すべてのスキヤンで信頼ファイルのスキップを許可する	ウイルススキヤンとスパイウェアスキヤンには、信頼できるファイルをスキップするインサイトと呼ばれるオプションがあります。デフォルトでは、インサイトは有効にされます。スキヤンでスキップするファイルの種類の信頼レベルを変更できます。 - シマンテック信頼とコミュニティ信頼 このレベルでは、シマンテック社とシマンテック製品コミュニティが信頼するファイルをスキップします。 - シマンテック信頼 このレベルでは、シマンテック社が信頼するファイルのみスキップします。 Windows クライアントのグローバルなスキヤン設定の修正

タスク	説明
定時スキャンをランダム化する	複数の仮想マシン (VM) が配備される仮想化された環境では、同時スキャンによってリソースの問題が発生します。たとえば、単一サーバーで 100 以上の VM を実行することがあります。それらの VM に対して同時スキャンが発生するとサーバーのリソースが使い果たされます。 スキャンをランダム化すれば、サーバーへの影響を限定できます。 スキャンのランダム化による Windows クライアントの仮想化環境でのコンピュータパフォーマンスの向上
仮想化された環境で Shared Insight Cache を使う	共有インサイトキャッシュにより、Symantec Endpoint Protection がクリーンであると判断したファイルを再スキャンする必要がなくなります。共有インサイトキャッシュをクライアントコンピュータで定時スキャンと手動スキャンに使用できます。共有インサイトキャッシュは、サーバーまたは仮想化環境にインストールする独立したアプリケーションです。 ネットワークベースの共有インサイトキャッシュの使用の有効化
早期起動マルウェア対策 (ELAM) の検出を無効化する	Symantec Endpoint Protection ELAM は、Windows の ELAM と連携して、悪意のある起動時のドライバからの保護を提供します。 早期起動マルウェア対策 (ELAM) の検出の管理

Table 98: スキャンを調整し、Mac コンピュータでのパフォーマンスを改善するには

タスク	説明
アイドルタイムスキャンを有効にする	Mac コンピュータで実行されるクライアントでの定時スキャンに適用されます。 このオプションは、コンピュータがアイドル状態の間だけ定時スキャンを実行するように設定します。 Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ
圧縮ファイルの設定を修正する	Auto-Protect スキャンとオンデマンドスキャンに適用されます。 オプションの有効と無効は切り替え可能ですが、スキャンする圧縮ファイルのレベルは指定できません。 Mac クライアントの Auto-Protect のカスタマイズ

Table 99: スキャンを調整し、Linux コンピュータでのパフォーマンスを改善するには

タスク	説明
フォルダの種類別スキャン	デフォルトでは全種類のフォルダをスキャンします。Root、Home、Bin、Usr、Etc、 Opt を指定できます。フォルダが安全であることがわかっている場合、リストのチェックマークを外すことができます。
ファイルの種類別スキャン	デフォルトでは全ファイルをスキャンします。特定の拡張子が安全であることがわかっている場合、リストからそれを削除できます。
圧縮ファイル内部のファイルをスキャンする	圧縮ファイル内のスキャンを最大 3 つのレベルまで拡大できます。スキャン時間を減らすためにレベルを 1 や 2 に変更したいことがあります。
セキュリティリスクをスキャンする	セキュリティリスクをスキャンするかどうかを選択できます。セキュリティリスクは LiveUpdate 経由で更新されます。セキュリティリスクのスキャンを行うと、スキャンの速度が低下しますが、セキュリティが向上します。デフォルトでは、セキュリティリスクのスキャンが実行されます。コンピュータのパフォーマンスを改善するには、このオプションのチェックマークをはずします。

クライアントコンピュータでのスキャンの管理

スキャンの調整によるクライアントコンピュータでの保護の強化

Symantec Endpoint Protection はデフォルトで、高レベルのセキュリティを提供します。保護をさらに強化することができます。

設定は、Windows コンピュータで実行されるクライアントと Mac および Linux コンピュータで実行されるクライアントでは異なります。

NOTE

クライアントコンピュータで保護を強化すると、コンピュータのパフォーマンスに影響することがあります。

Table 100: スキャンの調整による Windows コンピュータでの保護の強化

タスク	説明
スキャン設定をロックする	一部の設定はデフォルトでロックされています。ユーザーがコンピュータでの保護を変更できないように、その他の設定をロックできます。
管理者定義のスキャンの設定を修正する	次のオプションを調査または修正する必要があります。 - スキャンパフォーマンス スキャン調整を [スキャンに最適なパフォーマンス] に設定します。ただし、この設定はクライアントコンピュータのパフォーマンスに影響することがあります。スキャンはコンピュータがアイドル状態でなくても実行されます。 - 定時スキャンの期間 デフォルトでは、定時スキャンは指定された期間の終りまで実行され、その後、クライアントコンピュータがアイドル状態になったときに再開されます。このスキャン期間を [完了するまでスキャン] に設定することができます。 12.1.6.x 以前のクライアントのインサイトルックアップの使用 インサイトルックアップは、クラウドと Insight 評価データベースにある情報から取得した最新のウイルス定義セットを使ってスキャンを行い、サポート対象のポータルからダウンロードしたファイルについての決定を下します。 12.1.6.x 以前のバージョンでは、インサイトルックアップを有効、無効に切り替えることに加えて、インサイトルックアップの感度を設定することができました。バージョン 14 では、12.1.6.x クライアントのインサイトルックアップを有効、無効にすることのみが可能です。 Warning! インサイトルックアップが有効になっていることを確認してください。インサイトルックアップを無効にすると、クラウド保護が完全に無効になります。14 では、定時スキャンとオンデマンドスキャンは常にクラウドを使ってポータルファイルを評価します。Auto-Protect もポータルファイルを評価するのにクラウドを使います。 Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ Windows クライアントがクラウドから定義を受け取る方法
より厳しいスキャン検出の処理を指定する	検出のために [検疫]、[削除]、[終了] の処理を指定します。 Note: セキュリティリスクの検出に対して [削除] や [終了] を使うときは注意してください。この処理によって、一部の正当なアプリケーションが機能を失うことがあります。 検出を行ったときに Symantec Endpoint Protection が実行する処理の変更
Bloodhound による保護のレベルを上げる	Bloodhound は、ウイルスのような動作を検出するため、ファイルの論理的な領域を見つけて隔離します。検出レベルを [自動] から [拡張] に変更すると、コンピュータでの保護を強化できます。ただし [拡張] 設定では、おそらくより多くの誤認が生成されます。 Windows クライアントのグローバルなスキャン設定の修正
Auto-Protect 設定を調整する	変更できるオプションは次のとおりです。 - ファイルキャッシュ Auto-Protect が適切なファイルを再スキャンするようにファイルキャッシュを無効にできます。 - ネットワークの設定 デフォルトでは、ネットワークドライブ上のファイルは実行時にのみスキャンされます。 Windows クライアントの Auto-Protect のカスタマイズ

Table 101: スキャンの調整による Mac および Linux コンピュータでの保護の強化

タスク	説明
スキャンのための圧縮ファイルオプションの変更	デフォルトでは、圧縮ファイルを 3 つのレベルの深さでスキャンします。防御力を上げるには 3 つのレベルのままにするか、それより低いレベルであれば 3 つに変更します。 Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ Linux コンピュータで実行するクライアントに対する管理者定義のスキャンのカスタマイズ
Auto-Protect の設定をロックする	一部の設定はデフォルトでロックされています。ユーザーがコンピュータでの保護を変更できないように、その他の設定をロックできます。Mac クライアントおよび Linux クライアントで、[Auto-Protect を有効にする] をクリックし、ロックアイコンをクリックして設定をロックします。 Mac クライアントの Auto-Protect のカスタマイズ Linux クライアントの Auto-Protect のカスタマイズ
より厳しいスキャン検出の処理を指定する	検出に対して [検疫] または [削除] (Linux のみ) 処理を指定します。 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 Note: セキュリティリスクの検出に [削除] を使うときは注意してください。この処理によって、一部の正当なアプリケーションが機能を失うことがあります。 検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

ダウンロードインサイト検出の管理

Auto-Protect には、ユーザーが Web ブラウザ、テキストメッセージクライアント、その他のポータルを通してダウンロードを試みたファイルを検査する、ダウンロードインサイトと呼ばれる機能が含まれています。

サポート対象のポータルには、Internet Explorer、Firefox、Microsoft Outlook、Outlook Express、Google Chrome、Windows Live Messenger、Yahoo! Messenger が含まれます。

ダウンロードインサイトは、ファイルの評価についての証拠に基づいて、ダウンロードされたファイルがリスクである可能性があることを判断します。ダウンロードインサイトは Windows コンピュータで実行されるクライアントでのみサポートされます。

NOTE

電子メールの Auto-Protect をクライアントコンピュータにインストールした場合、Auto-Protect はユーザーが電子メールの添付ファイルとして受信したファイルもスキャンします。

[クライアントコンピュータでのスキャンの管理](#)

Table 102: ダウンロードインサイト検出の管理

タスク	説明
ダウンロードインサイトがどのように評価情報を使ってファイルに関する決定を下すかを学習する	ダウンロードインサイトは、ダウンロードされたファイルについて決定を下すときに評価情報のみを使います。決定を下すためにシグネチャやヒューリスティックを使いません。ダウンロードインサイトは、ユーザーがファイルを開いたとき、または実行するときに、ファイルスキャン、Auto-Protect、SONAR にファイルのスキャンを許可します。 Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法
ダウンロードリスク分布のレポートを表示して、ダウンロードインサイト検出を表示する	ダウンロードリスク分布のレポートを使って、ダウンロードインサイトがクライアントコンピュータで検出したファイルを表示できます。レポートは URL、Web ドメイン、アプリケーションのいずれかでソートできます。検出されたファイルをユーザーが許可したかどうか確認できます。 Note: ダウンロードインサイトによる検出のリスクの詳細には、ダウンロードを試みた最初のポータルアプリケーションのみが表示されます。たとえば、ユーザーが Internet Explorer を使って、ダウンロードインサイトが検出したファイルのダウンロードを試みたとき、次にユーザーが Firefox を使ってこのファイルのダウンロードを試みると、リスクの詳細には、ポータルとして Internet Explorer が表示されます。 レポートに表示されるユーザー許可ファイルは、誤認検出を示している場合があります。新しいユーザー許可ダウンロードに関する電子メール通知を受信するように指定することもできます。 管理者通知の設定 ユーザーは、検出に対する通知に応答することによりファイルを許可できます。 管理者は、Symantec Endpoint Protection Manager が生成し、電子メールで送信する週次レポートの一部としてレポートを受信します。電子メールアドレスは、インストール時に管理者用に指定済みであるか、管理者のプロパティの一部として設定済みであるはずで、レポートはコンソールの [レポート] タブから生成することもできます。 クイックレポートの実行とカスタマイズ
特定のファイルまたは Web ドメインの例外を作成する	ユーザーがダウンロードするアプリケーションの例外を作成できます。信頼に値すると信じる特定の Web ドメインの例外も作成できます。 Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定する Windows クライアントのスキャンからの信頼できる Web ドメインの除外 Note: クライアントコンピュータで、認証が必要なプロキシを使用する場合、シマンテック URL に信頼できる Web ドメイン例外を指定する必要があります。例外により、クライアントコンピュータは Symantec Insight と他の重要なシマンテック社のサイトと通信できます。 推奨される例外については、次の記事を参照してください。 • ライセンスサーバーやダウンロードインサイトサーバーへの接続をテストする方法 • SEP で Symantec のレピュテーションサーバーおよびライセンスサーバーと通信するために推奨されるプロキシサーバーの Web ドメイン除外指定について デフォルトでは、ダウンロードインサイトは、ユーザーが信頼できるインターネットサイトまたはイントラネットサイトからダウンロードするファイルを検査しません。Windows の [コントロールパネル]、[インターネットオプション]、[セキュリティ] タブで、信頼済みサイトと信頼済みローカルイントラネットサイトを設定します。[イントラネット Web サイトからダウンロードしたファイルを自動的に信頼する] オプションが有効になっている場合、Symantec Endpoint Protection はリストに含まれる任意のサイトからユーザーがダウンロードするファイルを許可します。 Symantec Endpoint Protection は、ユーザーがログオンするときに、4 時間ごとに、インターネットオプションの信頼できるサイトのリストの更新を確認します。 Note: ダウンロードインサイトは明示的に設定された信頼できるサイトのみを認識します。ワイルドカードは許可されますが、ルーティング不可能な IP アドレス範囲はサポートされません。たとえば、ダウンロードインサイトは 10.*.* を信頼済みサイトとして認識しません。また、ダウンロードインサイトは、[インターネットオプション]、[セキュリティ]、[イントラネットのネットワークを自動的に検出する] オプションによって発見されるサイトをサポートしません。

タスク	説明
Insight ルックアップが有効になっていることを確認する	ダウンロードインサイトでは、ファイルに関する決定を下すために Symantec Insight からの評価データが必要です。Insight ルックアップを無効にすると、ダウンロードインサイトは実行されますが、評価が最悪のファイルのみが検出されます。Insight ルックアップはデフォルトでは有効になっています。 ダウンロードインサイトの設定のカスタマイズ
ダウンロードインサイトの設定のカスタマイズ	次の理由でダウンロードインサイトの設定をカスタマイズしたい場合があります。 - ダウンロードインサイト検出の数を増加または減少させます。 悪質なファイルの感度スライダーを調整し、検出数を増加または減少させることができます。ダウンロードインサイトは低い感度レベルでは、より少ない数のファイルを悪質だと検出し、より多くのファイルを未確認として検出します。検出が少ないと誤認検出となります。 ダウンロードインサイトは高い感度レベルでは、より多くのファイルを悪質だと検出し、より少ないファイルを未確認として検出します。検出が多いと誤認検出となります。 - 悪質なファイルや未確認ファイルの検出の処理を変更します。 ダウンロードインサイトが悪質なファイルや未確認ファイルを処理する方法を変更できます。指定した処理は、検出だけでなく、ユーザーが検出を操作できるかどうかにも影響を与えます。 たとえば、未確認ファイルの処理を [無視] に変更できます。その後ダウンロードインサイトは未確認ファイルを常に許可し、ユーザーに警告しません。 - ダウンロードインサイト検出についてユーザーに警告します。 通知が有効になっている場合、悪質なファイルの感度設定が、ユーザーが受信する通知の数に影響します。感度を高めると、検出の合計数が増加するためユーザーへの通知の数が増加します。 ダウンロードインサイトが検出したときにユーザーに選択肢がないように、通知をオフにできます。通知を有効のままにしておく場合、これらの検出が常に許可され、ユーザーへの通知が行われないように、未確認ファイルの処理を [無視] に設定できます。 通知の設定にかかわらず、ダウンロードインサイトが未確認ファイルを検出し、この処理が [確認する] の場合、ユーザーはファイルを許可または遮断できます。ユーザーがファイルを許可すると、ファイルは自動的に実行されます。 通知が有効になっていて、ダウンロードインサイトがファイルを検疫する場合、ユーザーは検疫処理を元に戻し、ファイルを許可できます。 Note: ユーザーが検疫ファイルを許可した場合、ファイルは自動的に実行されません。ユーザーは Temporary Internet Files フォルダからファイルを実行できます。通常、このフォルダの場所は次のいずれかです。 - Windows 8 以降: <ドライブ>:\Users\username\AppData\Local\Microsoft\Windows\INetCache - Windows Vista/7: <ドライブ>:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files - Windows XP (レガシー 12.1.x クライアント用) : <ドライブ>:\Documents and Settings\username\Local Settings\Temporary Internet Files ダウンロードインサイトの設定のカスタマイズ
評価検出についての情報をシマンテック社に提出することをクライアントを許可する	デフォルトでは、クライアントは評価検出についての情報をシマンテック社に送信します。評価検出の提出は、有効にすることを推奨します。この情報はシマンテック社が脅威に対処するために役立ちます。 クライアントがシマンテック社に送信する匿名または非匿名のデータの管理

Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法

シマンテック社は、数百万ユーザーのグローバルなコミュニティと、Symantec Global Intelligence Network からファイルについての情報を収集しています。収集された情報は、Symantec Insight を介したクラウドのシマンテック製品で利用可能です。Symantec Insight はファイル評価データベースと、最新のウイルス定義とスパイウェア定義を提供します。

シマンテック製品は Insight を活用して、新しい脅威、対象となる脅威、変異する脅威からクライアントコンピュータを保護します。データはクライアントコンピュータ上には存在しないため、クラウド内に存在していると表現される場合も

あります。Symantec Endpoint Protection はインサイトに情報を要求またはクエリーする必要があります。クエリーは評価ルックアップ、クラウドルックアップ、インサイトルックアップと呼ばれます。

インサイト評価の方法

Symantec Insight は、各ファイルの危険度またはセキュリティの評価のレベルを判断します。この評価は、ファイルの評価とも見なされます。

Insight はファイルとそのコンテキストについて次の特性を調べ、ファイルのセキュリティ評価を決定します。

- ファイルのソース
- ファイルのどの程度新しいものか
- ファイルがコミュニティでどれだけ一般的であるか
- ファイルがマルウェアとどのように関係している可能性があるかなど、その他のセキュリティ基準

インサイトルックアップ

Symantec Endpoint Protection のスキャン機能は Insight を活用して、ファイルとアプリケーションについての決定を下します。ウイルスとスパイウェアの対策には、ダウンロードインサイトと呼ばれる機能が含まれます。ダウンロードインサイトは、検出を行うために評価情報が必要です。SONAR も、検出を行うために評価情報を使います。

インサイトルックアップの設定を [クライアント] タブで変更できます。[ポリシー] > [設定] > [外部通信の設定] > [クライアント提出] に移動します。

インサイトルックアップの設定を変更できます。[設定の変更]、[クライアント管理]、[提出] の順に移動します。

14 以降では、標準クライアントと埋め込み/VDI クライアント上でインサイトルックアップオプションを使用することにより、Auto-Protect と、定時スキャンおよび手動スキャン時に、クラウドでファイル評価情報と定義を検索できます。シマンテック社はこのオプションを有効のままにしておくことを推奨します。

WARNING

ダウンロードインサイト、SONAR、ウイルスとスパイウェアのスキャンは脅威の検出にインサイトルックアップを使います。シマンテック社は常にインサイトルックアップを許可することを推奨します。ルックアップを無効にするとダウンロードインサイトが無効になり、SONAR ヒューリスティックとウイルスとスパイウェアのスキャンが損なわれます。

ファイル評価提出

デフォルトでは、クライアントコンピュータは分析のため、シマンテックセキュリティレスポンスに評価検出についての情報を送信します。この情報は、インサイトの評価データベースとクラウドの最新の定義を調整するのに役立ちます。情報を提出するクライアントが多いほど、評価データベースは有用になります。

評価検出のクライアント提出は、有効なままにすることを推奨します。

Symantec Endpoint Protection が高度な機械学習を使用する仕組み

- [高度な機械学習の機能](#)
- [AML がクラウドと連携する仕組み](#)
- [AML の設定方法](#)
- [高度な機械学習のトラブルシューティング](#)

高度な機械学習の機能

高度な機械学習 (AML) エンジン、学習プロセスを通じて、ファイルが良好であるか問題があるかを判断します。シマンテックセキュリティレスポンスは、このエンジンが悪質な属性を認識するようにトレーニングし、AML エンジンが検出に使用するルールを定義します。シマンテック社は、ラボ環境で次のプロセスを使用して、AML エンジンのトレーニングとテストを実行します。

- LiveUpdate が AML モデルをクライアントにダウンロードし、数日間実行します。
- AML エンジン、クライアントの遠隔測定データを使用して、クライアント上で稼働するどのアプリケーションがエクスプロイトされたかを学習します。各クライアントコンピュータは、モデルに関する情報をシマンテック社に返す Global Intelligence Network に属します。
- シマンテック社は、クライアントの遠隔測定データから得た情報に基づいて AML モデルを調整します。
- シマンテック社は、攻撃でエクスプロイトされたアプリケーションを遮断するように、AML モデルを修正します。

AML は静的データスキャナ (SDS) エンジンの一部です。SDS エンジンには、エミュレータ、ITCS (Intelligent Threat Cloud Services)、CoreDef-3 定義エンジンが含まれます。

Symantec Endpoint Protection は、ダウンロードインサイト、SONAR、ウイルスとスパイウェアのスキャンで高度な機械学習を使用し、これらすべてがインサイトルックアップを使用して脅威を検出します。

AML がクラウドと連携する仕組み

シマンテック社は ITCS (Intelligent Threat Cloud Services) を活用して、AML がクライアントコンピュータ上で行った検出が正しいかどうかを確認します。ITCS でチェックされた後に、AML が判断を変える場合もあります。AML エンジンには Symantec Insight を必要としませんが、このフィードバックによって、シマンテック社が AML アルゴリズムをトレーニングし、誤検知を減らし、正しい検出を増やすことができます。コンピュータがオンラインの場合、Symantec Endpoint Protection は平均で 99% の脅威を防止できます。

Windows クライアントがクラウドから定義を受け取る方法

Symantec Endpoint Protection のエミュレータがマルウェアを検出およびクリーニングする方法

AML の設定方法

高度な機械学習をユーザーが設定することはできません。LiveUpdate はデフォルトで AML 定義をダウンロードします。ただし、次の技術が有効になっていることを確認する必要があります。

Table 103: AML がクライアントコンピュータを保護することを確認する手順

タスク	説明
ステップ 1: クラウドルックアップが有効であることの確認	AML が Symantec Insight に対して実行するクエリーは、評価ルックアップ、クラウドルックアップ、またはインサイトルックアップと呼ばれます。インサイトルックアップが有効な場合、AML が SONAR やウイルスとスパイウェアのスキャンで行う検出で誤検知が少なくなります。 インサイトルックアップが有効になっていることを確認するには、次の場所を参照してください。 Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法 また、クライアント提出が有効になっていることを確認します。この情報は、シマンテック社が検出技術の有効性を測定し、向上を図るのに役立ちます。 サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について
ステップ 2: Bloodhound 検出が有効であることの確認	Bloodhound 検出のレベルを、自動または拡張に設定します。 Windows クライアントのグローバルなスキャン設定の修正 AML エンジンが特定の高リスクファイルを検出すると、クライアントはよりアグレッシブなスキャンを自動的に実行します。 拡張スキャンモードでは、次の処理が実行されます。 • スキャンが再起動します。 • 次の通知がクライアントに表示されます。 ##### 拡張モードでは、誤検知をより細かく管理する必要があります。

タスク	説明
ステップ 3: LiveUpdate が高集中定義をダウンロードすることの確認 (14.0.1) (省略可能)	LiveUpdate は常に AML コンテンツをダウンロードします。 14.0.1 では、LiveUpdate がよりアグレッシブな定義セットをダウンロードします。この定義は、クラウドから取得する低帯域幅ポリシーと連携します。AML コンテンツが LiveUpdate でダウンロードされないようにすることができます。 LiveUpdate から つの Symantec Endpoint Protection Manager: LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード つの Symantec Endpoint Protection Manager から Windows クライアント: Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻る LiveUpdate がダウンロードするコンテンツの種類について
ステップ 4: 誤検知の処理	誤検知は、例外ポリシーを使用して管理します。 ウイルスとスパイウェアのスキャンの例外作成 SONAR の誤検知の検出の処理と防止 Symantec Endpoint Protection が安全と見られるファイルを検出した場合のベストプラクティス

高度な機械学習のトラブルシューティング

高度な機械学習による検出のログとレポートは、他の SDS エンジンの場合と同じです。最新の脅威を示すレポートを確認するには、[ネットワークで検出された新種のリスク] のリスクレポートを実行します。

14.0.1 では、AML 検出の定時レポートを実行できます。[レポート] ページで、[定時レポート] > [追加] > [コンピュータの状態] > [高度な機械学習 (静的) コンテンツ配布] を選択します。レポートを表示するには、クラウドコンソールで つの Symantec Endpoint Protection Manager ドメインを登録する必要があります。

定時レポートの実行方法

ログの表示

Symantec Endpoint Protection のエミュレータがマルウェアを検出およびクリーニングする方法

Symantec Endpoint Protection 14 に導入された強力な新しいエミュレータは、カスタムパッカー攻撃によるマルウェアから保護します。Auto-Protect スキャンとウイルススキャンの場合、この新しいエミュレータにより、スキャンのパフォーマンスと効果が以前のリリースに比べて少なくとも 10% 向上します。この回避対策技術はバックされたマルウェアの難読化技術に対応し、カスタムパッカー内に隠れているマルウェアが検出されます。

カスタムパッカーとは

多くのマルウェアプログラムは「パッカー」を利用します。パッカーは、ファイルを圧縮し、暗号化して送信するのに使用する、ソフトウェアプログラムです。これらのファイルは、ユーザーのコンピュータに到着するとすぐに、メモリ内で実行されます。

パッカー自体はマルウェアではありませんが、攻撃者はパッカーを使用してマルウェアを隠し、コードの真の意図を分かりにくくします。マルウェアのパッキングが解除されると、ファイアウォール、ゲートウェイ、マルウェア対策を避けて、その悪質なペイロードが起動します。攻撃者は、商用のパッカー (UPX、PECompact、ASProtect、Themida など) の使用を避け、カスタムパッカーを作成するようになりました。カスタムパッカーは、独自のアルゴリズムを使用して標準的な検出技術を回避します。

新しいカスタムパッカーの多くは、多様な形態を持ちます。検出を回避するためにコード自体を頻繁に変えますが、マルウェアの目的と機能は変わりません。また、カスタムパッカーは、巧みな方法でコードをターゲットプロセスに挿入し、その実行フローを変更し、アンパッカールーチンを頻繁に混乱させます。一部のカスタムパッカーはコンピューティング集中型で、パッキング解除を困難にする特殊な API を呼び出します。

カスタムパッカーはますます洗練され、手遅れになるまでその攻撃を隠します。

Symantec Endpoint Protection のエミュレータがカスタムパッカー攻撃から保護する方法

Symantec Endpoint Protection の高速エミュレータは、通常のコンピュータ上で実行されているとマルウェアに思い込ませます。実際には、エミュレータがカスタムパッカーのファイルをクライアントコンピュータ上の軽量仮想サンドボックスにパッキング解除します。マルウェアはそのペイロードを完全に開始するため、隔離された環境内で脅威が明らかにされます。ウイルス対策エンジンとヒューリスティックエンジンが含まれる静的データスキャナが、そのペイロードに対して実行されます。このサンドボックスは一時的なもので、脅威が処理された後で消えます。

エミュレータは、オペレーティングシステム、API、プロセッサの命令を装う、洗練された技術を必要とします。エミュレータは同時に仮想メモリを管理し、さまざまなヒューリスティックおよび検出技術を実行して、ペイロードを検査します。平均で、ファイルのクリーニングに 3.5 ミリ秒、マルウェアのクリーニングに 300 ミリ秒かかります。これは、クライアントユーザーがデスクトップ上の 1 ファイルをクリックするのと同程度の時間です。このエミュレータは、パフォーマンスと生産性に与える影響を最小限に抑えて迅速に脅威を検出します。そのため、クライアントユーザーの操作が妨害されることはありません。また、このエミュレータが使用するのは最小限のディスク容量と、仮想環境で最大 16 MB のメモリのみです。

このエミュレータは、高度な機械学習、メモリエクスポイト緩和機能、動作監視、評価分析など、他の保護技術とも連携します。場合によっては複数のエンジンが作動し、連携して、攻撃を防止、検出、修復します。

このエミュレータはインターネットを使用しません。しかし、エミュレータがカスタムパッカーから抽出したマルウェアによっては、静的データスキャナ内のエンジンがインターネットを必要とする場合があります。

[Symantec Endpoint Protection が高度な機械学習を使用する仕組み](#)

エミュレータの設定方法

このエミュレータは Symantec Endpoint Protection ソフトウェアに組み込まれているため、設定は不要です。シマンテック社は、新種の脅威に対応するためエミュレータのコンテンツを定期的に追加または変更し、エミュレータエンジンのコンテンツ更新も年に 4 回リリースします。デフォルトでは、LiveUpdate がウイルス定義とスパイウェア定義を含むコンテンツを自動的にダウンロードします。

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

つの Symantec Endpoint Protection Manager には、エミュレータが行った検出に関する個別のログはありません。検出結果については、リスクログとスキャンログで確認できます。

[ログの表示](#)

Windows クライアント用の検疫の管理

ウイルス アウトブレイク戦略の重要な部分として検疫設定を管理します。

ウイルス スキャンとスパイウェア スキャン、または SONAR が脅威を検出すると、Symantec Endpoint Protection は疑わしいファイルを感染したコンピュータのローカル検疫に移動します。クライアントはファイルを修復、修復して復元、または削除します。

クライアントがリスクを検出し、ファイルを検疫すると、クライアントは管理サーバに通知します。管理サーバが検疫ファイルを自動的に要求して取り込むようにできます。管理サーバはリスク サンプルをデータベースにアップロードして格納してそのイベントの詳細を表示し、それらをさらに分析するためにダウンロードできるようにします。ファイルを社内のマルウェアまたはセキュリティチームに送信してリバースエンジニアリングを行ったり、分析用の別のサンドボックスに送信したりすることもできます。これが誤検知である可能性がある場合、シマンテック サポートに連絡してケースを記録してください。

NOTE

バージョン 14 以降には中央検疫サーバは含まれません。

14.3 RU2 以降、中央検疫サーバは使用できません。代わりに、クライアントは Symantec Endpoint Protection Manager に検疫ファイルを提出します。

管理サーバに検疫ファイルをアップロードする

デフォルトでは、管理サーバはクライアントから検疫ファイルを取り込みません。この設定を有効にする必要があります。

1. コンソールで、[管理] > [ドメイン] > [ドメイン プロパティの編集] をクリックします。
2. [全般] タブで [クライアントから検疫済みファイルをアップロードする] をクリックし、[OK] をクリックします。

クライアントが検疫して管理サーバにアップロードしたファイルをダウンロードするには

1. コンソールで、[監視] > [ログ] をクリックし、[リスク] ログの種類を選択します。
2. ログを開いて検疫ファイルを選択し、[処理] ドロップダウン リストで、[クライアントが検疫したファイルをダウンロード] をクリックします。

検疫の設定

検疫がクライアントのファイルを処理する方法は、以下のオプションを修正できます。

- クライアントに新しい定義が到着した場合
デフォルトでは、新しい定義が到着すると、クライアントは検疫内のアイテムを再スキャンし、自動的にアイテムを修復してサイレントに復元します。検疫にあるファイルまたはアプリケーションの例外を作成した場合、Symantec Endpoint Protection は新しい定義の到着後にファイルを復元します。
 - 検疫アイテムを格納する場所
デフォルトでは、検疫はデフォルトのフォルダにバックアップファイル、修復したファイル、検疫ファイルを格納します。検疫のクリーンアップ機能は、ファイルが指定された時間を超えた場合、または格納されるディレクトリが一定のサイズに達した場合に、検疫内のファイルを自動的に削除します。ファイルは 30 日後に自動的に削除されます。
デフォルトの検疫ディレクトリ (%ProgramData%\Symantec\Symantec Endpoint Protection \CurrentVersion\Data\Quarantine) を使って検疫ファイルをクライアント コンピュータに格納したくない場合、異なるローカル ディレクトリを指定できます。パスを入力するときにパーセント記号を使うことでパス展開を使用できます。たとえば、%COMMON_APPDATA% と入力します。相対パスは指定できません。
1. ウィルスとスパイウェアの対策ポリシーで、[Windows の設定] > [検疫] をクリックします。
 2. [全般] タブの、[新しいウィルス定義の到着時] と [ローカル検疫オプション] を設定します。
検疫アイテムの処理方法と検疫ファイルを格納するローカル フォルダを指定します。

検疫: 全般

3. [OK] をクリックします。

検疫にあるファイルを削除する

検疫では、指定した日数後、修復したファイル、バックアップ ファイル、検疫ファイルが自動的に削除されます。ファイルを格納するフォルダが指定したサイズに達したときに、または指定の日数後にファイルを削除するように検疫を設定できます。

多数のファイルが蓄積されないように、定期的にクライアント コンピュータの検疫を調べる必要があります。ネットワークで新しいウィルスアウトブレイクが現れたときには検疫ファイルを調べます。

不明な感染のあるファイルは検疫に残します。クライアントが新しい定義を受信すると、検疫内にあるアイテムを再スキャンして、ファイルを削除または修復することがあります。

バックアップが存在する場合や、信頼に値するソースから入手したファイルのコピーがある場合は検疫ファイルを削除できます。検疫ファイルは感染したコンピュータで直接、または Symantec Endpoint Protection コンソールのリスクログを使って削除できます。

NOTE

Symantec Endpoint Protection が圧縮ファイル内でリスクを検出した場合、圧縮ファイルがまとめて検疫されます。ただし、リスクログには圧縮ファイル内の各ファイルのエントリが別々に含まれています。圧縮ファイル内のすべてのリスクを正しく削除するには、圧縮ファイル内のすべてのファイルを選択する必要があります。

ファイルを自動的に削除するようにクライアントを設定するには

1. ウィルスとスパイウェアの対策ポリシーで、[Windows の設定] > [検疫] をクリックします。
2. [クリーンアップ] タブでオプションのチェックマークを付けるかはずして有効または無効にして、間隔とサイズの最大値を設定します。

検疫: クリーンアップ

3. [OK] をクリックします。

リスク ログからファイルを削除するには

1. コンソールで、[監視] をクリックします。
2. [ログ] タブの [ログの種類] リストボックスで、[リスク] ログを選択して [ログの表示] をクリックします。
3. 次のいずれかの処理を実行します。
 - 検疫されたファイルが含まれているログでエントリを選択します。
 - 圧縮ファイル内のファイルのすべてのエントリを選択します。
圧縮ファイルのすべてのエントリがログ表示に含まれている必要があります。[追加設定] の [限度] オプションを使うと、表示されるエントリを増やすことができます。
4. [処理] リスト ボックスで、[検疫から削除] を選択します。
5. [開始] をクリックします。
6. ダイアログ ボックスが表示されたら、[削除] をクリックしてから [OK] をクリックします。

クライアントコンピュータにある検疫ファイルのリスクログを使った削除

つの Symantec Endpoint Protection Manager コンソールでリスクログを使って、クライアントコンピュータにある検疫ファイルを削除できます。削除する任意の検疫ファイルについて、ログから [検疫から削除] コマンドを実行します。

クライアントコンピュータでのスキャンの管理

Symantec Endpoint Protection が圧縮ファイル内でリスクを検出した場合、圧縮ファイルがまとめて検疫されます。ただし、リスクログには圧縮ファイル内の各ファイルのエントリが別々に含まれています。圧縮ファイル内のすべてのリスクを正しく削除するには、圧縮ファイル内のすべてのファイルを選択する必要があります。

リスクログを使って、クライアントコンピュータの検疫からファイルを削除するには

1. [監視] をクリックします。
2. [ログ] タブの [ログの種類] リストボックスで、[リスク] ログを選択して [ログの表示] をクリックします。
3. 次のいずれかの処理を実行します。
 - 検疫されたファイルが含まれているログでエントリを選択します。
 - 圧縮ファイル内のファイルのすべてのエントリを選択します。
圧縮ファイルのすべてのエントリがログ表示に含まれている必要があります。[追加設定] の [限度] オプションを使うと、表示されるエントリを増やすことができます。
12.1.xでは、[追加設定] ではなく [拡張設定] です。
4. [処理] リストボックスで、[検疫から削除] を選択します。
5. [開始] をクリックします。
6. ダイアログボックスが表示されたら、[削除] をクリックします。
7. 確認のダイアログボックスが表示されたら、[OK] をクリックします。

クライアントコンピュータに表示されるウィルスとスパイウェアの通知の管理

クライアントコンピュータにウィルスとスパイウェアのイベントについての通知を表示するかどうかを指定できます。検出についてのメッセージはカスタマイズできます。

クライアントコンピュータでのスキャンの管理

Table 104: クライアントコンピュータに表示されるウイルスとスパイウェアの通知を管理するためのタスク

タスク	説明
スキャン検出メッセージをカスタマイズする	Windows および Linux クライアントコンピュータの場合、次の種類のスキャンについて、検出メッセージを設定できます。 - Auto-Protect の全種類 - 定時スキャンとオンデマンドスキャン 定時スキャンの場合、各スキャンに別個のメッセージを設定できます。 Note: プロセスがクライアントコンピュータに同じセキュリティリスクを絶えずダウンロードする場合、Auto-Protect は 3 回の検出後、自動的に通知の送信を停止します。Auto-Protect はイベントのログ記録も停止します。ただし状況によっては、Auto-Protect は通知の送信とイベントのログ記録を停止しません。検出の処理が [放置する (ログのみ)] のときには、Auto-Protect は通知の送信とイベントのログ記録を続けます。 Mac クライアントコンピュータの場合、すべての定時スキャン、オンデマンドスキャン、Auto-Protect 検出に適用される検出メッセージを設定できます。これらの通知メッセージは、macOS の通知センターに表示されます。Mac 用のメッセージをカスタマイズすることはできません。 Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ Linux コンピュータで実行するクライアントに対する管理者定義のスキャンのカスタマイズ
ダウンロードインサイト検出に関するユーザー通知の設定を変更する	該当するのは Windows クライアントコンピュータのみです。 ユーザーがダウンロードインサイト検出について受信する通知を変更できます。 ダウンロードインサイト検出の管理
SONAR 検出に関するユーザー通知の設定を変更する	該当するのは Windows クライアントコンピュータのみです。 ユーザーが SONAR 検出について受信する通知を変更できます。 SONAR の管理
Auto-Protect 結果ダイアログボックスを表示するかどうかを選択する	該当するのは Windows クライアントコンピュータのみです。 該当するのはファイルシステムの Auto-Protect のみです。 Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ
Auto-Protect の電子メール通知を設定する	該当するのは Windows クライアントコンピュータのみです。 Auto-Protect の電子メールスキャンでリスクが見つかった場合、Auto-Protect は指定した電子メール送信者とその他任意の電子メールアドレスに警告するため、電子メール通知を送信できます。電子メールメッセージに警告を挿入することもできます。 インターネット電子メール Auto-Protect については、Auto-Protect が電子メールをスキャンするときに、スキャンの進行状況に関する通知が表示されるように指定できます。インターネット電子メール Auto-Protect は 14.2 RU1 より前のクライアントバージョンでのみ利用できます。 Windows コンピュータで実行する電子メールスキャンの Auto-Protect のカスタマイズ
ユーザーがスキャンの進行状況とスキャンの開始または停止を参照できるようにする	該当するのは Windows クライアントコンピュータのみです。 スキャンの進行状況のダイアログボックスを表示するかどうかを設定できます。スキャンを一時停止すること、または遅らせることをユーザーに許可するかどうかを設定できます。 ユーザーがスキャンの進行状況を参照できるようにすると、スキャンの進行状況のダイアログボックスへのリンクがクライアントユーザーインターフェースのメインページに表示されます。次の定時スキャンのスケジュールを再設定するリンクも表示されます。 Windows コンピュータでのユーザーによるスキャンの進行状況の表示とスキャンの操作の許可
警告、エラー、確認を設定する	該当するのは Windows クライアントコンピュータのみです。 クライアントコンピュータに表示される、ウイルスとスパイウェアの対策イベントに関するいくつかの種類警告を有効または無効にできます。 Windows コンピュータのログ処理と通知設定の修正

タスク	説明
Windows 8 形式のユーザーインターフェースのポップアップ通知を有効化または無効化する	該当するのは Windows 8 で実行されるクライアントです。 検出および他の重要なイベントのために Windows 8 形式のユーザーインターフェースで表示されるポップアップ通知を有効化または無効化できます。 Windows 8 クライアントで表示される Symantec Endpoint Protection のポップアップ通知の有効化または無効化

Windows 8 クライアントで表示されるポップアップ通知について

Windows 8 のコンピュータでは、マルウェア検出とその他の重要な Symantec Endpoint Protection イベントのポップアップ通知が Windows 8 形式のユーザーインターフェースや Windows 8 デスクトップに表示されます。通知は、ユーザーが現在表示しているインターフェースに関係なく、Windows 8 形式のユーザーインターフェースまたは Windows 8 デスクトップで発生したイベントについてユーザーに警告します。

クライアントコンピュータのポップアップ通知を有効または無効にすることができます。

NOTE

Windows 8 の設定には、通知の表示と非表示に関する設定も含まれます。Symantec Endpoint Protection のポップアップ通知は、Windows 8 でそれらを表示するよう設定した場合にのみ表示されます。Windows 8 形式のユーザーインターフェースでは、[設定] ペインまたは [PC 設定の変更] オプションで、アプリケーションの通知の表示と非表示を切り替えられます。詳しくは、Windows 8 のユーザーマニュアルを参照してください。

Windows 8 形式のユーザーインターフェースで通知をクリックすると、Windows 8 デスクトップが表示されます。Windows 8 デスクトップで通知をクリックすると、その通知は消えます。マルウェアやセキュリティリスクの検出について、Windows 8 デスクトップの [検出結果] ダイアログボックスで検出結果の情報を確認できます。

Symantec Endpoint Protection が、Windows 8 形式のアプリケーションに影響するマルウェアまたはセキュリティリスクを検出したことを Windows 8 に通知すると、アプリケーションのタイル上に警告アイコンが表示されます。ユーザーがタイルをクリックすると、Windows App Store が表示され、そのアプリケーションを再ダウンロードできるようになります。

[Windows 8 クライアントで表示される Symantec Endpoint Protection のポップアップ通知の有効化または無効化](#)

[Windows 8 コンピュータでの検出に対する Symantec Endpoint Protection の処理方式](#)

Windows 8 クライアントで表示される Symantec Endpoint Protection のポップアップ通知の有効化または無効化

デフォルトでは、マルウェア検出とその他の重要な Symantec Endpoint Protection イベントに関するポップアップ通知が Windows 8 形式のユーザーインターフェースや Windows 8 デスクトップに表示されます。

ユーザーは通知を生成したイベントの詳細を参照するために Windows のデスクトップを表示できます。ユーザーはアプリケーションの再ダウンロードなどの処理を行うことが必要になる場合があります。ただし、状況によって、これらのポップアップ通知をユーザーに表示しないようにすることもできます。Symantec Endpoint Protection の設定で、この種類の通知を有効にしたり、無効にしたりすることができます。

NOTE

Windows 8 の設定には、通知の表示と非表示に関する設定も含まれます。Symantec Endpoint Protection の通知は、Windows 8 でそれらを表示するよう設定した場合にのみ表示されます。Windows 8 形式のユーザーインターフェースでは、[設定] ペインまたは [PC 設定の変更] オプションで、アプリケーションの通知の表示と非表示を切り替えられます。詳しくは、Windows 8 のユーザーマニュアルを参照してください。

Windows 8 クライアントで表示される Symantec Endpoint Protection のポップアップ通知を有効または無効にするには

1. コンソールで、[クライアント] タブの [ポリシー] タブの [場所固有の設定] で、[クライアントユーザーインターフェイス制御の設定] の隣の [サーバー制御] をクリックします。
2. [サーバー制御] の隣で、[カスタマイズ] をクリックします。
3. [クライアントユーザーインターフェイスの設定] ダイアログボックスの [全般] で、[Windows トースト通知を有効にする] にチェックマークを付けるか、またははずします。
4. [OK] をクリックします。

Windows 8 クライアントで表示されるポップアップ通知について

早期起動マルウェア対策 (ELAM) の検出の管理

早期起動マルウェア対策 (ELAM) は、ネットワーク内のコンピュータの起動時に、他社製のドライバが初期化される前にコンピュータに保護を提供します。ドライバまたはルートキットとしてロードされる悪質なソフトウェアは、オペレーティングシステムが完全にロードし、Symantec Endpoint Protection が起動する前に攻撃を行う可能性があります。ルートキットはウイルススキャンやスパイウェアスキャンから、自分自身を隠すことができます。早期起動マルウェア対策は、これらのルートキットと危険なドライバを起動時に検出します。

NOTE

ELAM は Microsoft Windows 8 以降と Windows Server 2012 以降のみでサポートされます。

Symantec Endpoint Protection は、早期起動マルウェア対策 (ELAM) ドライバを用意しており、Windows ELAM ドライバと連携して保護を提供します。保護を有効にするには、Windows ELAM ドライバをシマンテック社の早期起動マルウェア対策ドライバに対して機能するようにする必要があります。

Windows グループポリシーエディタを使い、Windows ELAM の設定の表示と修正を行います。詳しくは、Windows のマニュアルを参照してください。

Table 105: ELAM の検出の管理

タスク	説明
クライアントコンピュータの ELAM の状態を表示する	Symantec Endpoint Protection ELAM が有効になっているかどうかをコンピュータの状態ログで確認できます。 ログの表示
ELAM の検出を表示する	早期起動マルウェア対策の検出をリスクログで確認できます。 Symantec Endpoint Protection の早期起動マルウェア対策が、悪いまたは非常に悪いドライバを検出した場合に不明のドライバとして Windows に報告するよう設定されているとき、Symantec Endpoint Protection は [ログのみ] として検出結果をログに記録します。デフォルトでは、Windows ELAM は不明なドライバのロードを可能にしています。
ELAM を有効または無効にする	Symantec Endpoint Protection ELAM を無効にして、コンピュータのパフォーマンス向上に役立てる場合があります。 Symantec Endpoint Protection の早期起動マルウェア対策 (ELAM) のオプションの調整 スキャンの調整によるクライアントコンピュータパフォーマンスの改善
誤認が発生した場合に ELAM の検出設定を調節する	Symantec Endpoint Protection ELAM の設定には、危険なドライバまたは危険で重大なドライバを不明ドライバとして扱うためのオプションがあります。危険で重大なドライバとは、マルウェアとして識別されるがコンピュータの起動に必要なドライバを指します。この優先オプションは、誤認検出によって重要なドライバが遮断される場合に選択することができます。重要なドライバを遮断すると、クライアントコンピュータを起動できなくなる可能性があります。 Note: ELAM では、個々のドライバに固有の例外はサポートされません。優先オプションは、ELAM の検出全体に適用されます。 Symantec Endpoint Protection の早期起動マルウェア対策 (ELAM) のオプションの調整

タスク	説明
Symantec Endpoint Protection で修復できない ELAM の検出に Power Eraser ツールを実行する	場合によって、ELAM の検出に Power Eraser が必要になります。そのような場合、Power Eraser を実行することを推奨するメッセージがログに表示されます。コンソールから Power Eraser を実行できます。Power Eraser もシマンテックヘルプツールの一部です。Power Eraser はルートキットモードで実行してください。 この Symantec Endpoint Protection Manager からの Power Eraser の分析の開始 Symantec Diagnostic Tool (SymDiag) を使ったコンピュータの問題のトラブルシューティング

Symantec Endpoint Protection の早期起動マルウェア対策 (ELAM) のオプションの調整

Symantec Endpoint Protection は、Microsoft 社の ELAM ドライバと連携して機能して、ネットワークのコンピュータの起動時にコンピュータを保護する、早期起動マルウェア対策 (ELAM) ドライバを提供します。この設定は Microsoft Windows 8 および Windows Server 2012 以降でサポートされます。

Symantec Endpoint Protection の早期起動マルウェア対策ドライバは特別な種類のドライバで、他の起動時のドライバをまず初期化してから、それらに悪質なコードがないかどうかを調べます。このドライバが起動時のドライバを検出すると、そのドライバが安全か、危険か、不明かを判断します。Symantec Endpoint Protection ドライバはその情報を Windows に渡し、検出されたドライバを許可するか、遮断するかを決定します。

個別の ELAM の検出のために例外を作成することはできませんが、すべての危険なドライバを不明ドライバとして記録する、グローバルな例外を作成できます。デフォルトでは、不明なドライバのロードが許可されています。

ELAM の検出の一部では、修復処理が要求された場合に、Power Eraser の実行が必要になることがあります。Power Eraser はシマンテックヘルプツールの一部です。

NOTE

Auto-Protect はロードされるドライバをスキャンします。

Symantec Endpoint Protection の ELAM オプションを調整するには

1. この Symantec Endpoint Protection Manager のコンソールの [ポリシー] タブで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [保護技術] で、[早期起動マルウェア対策ドライバの状態] を選択します。
3. [Symantec **Early Launch Anti-Malware** を有効にする] を選択または選択解除します。
このオプションを有効にするには、Windows の早期起動マルウェア対策ドライバを有効にする必要があります。Windows グループポリシーエディタまたはレジストリエディタを使い、Windows ELAM の設定の表示と修正を行います。詳しくは、Windows のマニュアルを参照してください。
4. 検出のログを記録のみを行う場合は、[検出設定] で [検出結果を不明としてログ記録して、Windows にドライバのロードを許可する] を選択します。
5. [OK] をクリックします。

早期起動マルウェア対策 (ELAM) の検出の管理

Symantec Diagnostic Tool (SymDiag) を使ったコンピュータの問題のトラブルシューティング

クエリーの評価に専用インサイトサーバーを使うようにサイトを設定する

Symantec Insight for Private Clouds を購入してインストールしている場合は、専用インサイトサーバーを設定するとクライアントの評価クエリーをイントラネットサーバーに直接送信できます。Symantec Insight for Private Clouds は通常インターネットに接続していないネットワークにインストールされます。専用インサイトサーバーに Symantec Insight の評価データベースの複製を保存します。Symantec Endpoint Protection の評価クエリーはシマンテック社のインサイトサーバーではなく専用インサイトサーバーで処理します。

専用サーバーは、信頼できて暗号化された接続で Symantec Insight のデータをダウンロードします。手動でインサイトデータを更新するかまたはサードパーティツールを使って自動的にデータの更新やダウンロードを調べることができます。更新方法は Symantec Insight for Private Clouds を実行しているネットワークやサーバーの種類によって異なります。

専用インサイトサーバーを使うと、シマンテック社はクエリーやファイル評価の提出を受信できません。

クエリー評価に専用のインサイトサーバーを使うようにサイトを設定するには

1. コンソールの [管理] ページで [サーバー] を選択します。
2. サイトを選択し、[タスク] で [サイトプロパティの編集] を選択します。
3. [専用インサイトサーバー] タブで、[専用インサイトサーバーを有効にします] にチェックすることを確認します。

名前、サーバー URL、ポート番号も入力する必要があります。

NOTE

既存のサーバー URL を無効な URL に変更すると、クライアントは専用インサイトサーバーに以前の有効な URL を使います。サーバー URL が設定されていない場合に無効な URL を入力すると、クライアントはデフォルトの Symantec インサイトサーバーを使います。

クライアントは、次のハートビートで評価クエリーに指定した専用サーバーの使用を開始します。

[Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法](#)

[評価のクエリーおよび提出に専用サーバーを使うクライアントグループの設定](#)

評価のクエリーおよび提出に専用サーバーを使うクライアントグループの設定

グループから専用イントラネットサーバーにクライアント評価クエリー(インサイトルックアップ)を指示できます。専用サーバーは別途購入してネットワークにインストールする Symantec Endpoint Detection and Response アプライアンスまたは Symantec Insight for Private Clouds サーバー場合があります。

グループの専用サーバーオプションは次のとおりです。

- Symantec Endpoint Detection and Response
Symantec EDR サーバーは、クライアント検出に関するデータを収集し、犯跡分析を提供します。Symantec EDR サーバーを使う場合は、Symantec Endpoint Protection によってすべての評価クエリー (ルックアップ) とほとんどの種類のクライアント提出が Symantec EDR に送信されます。Symantec EDR は次にシマンテック社にクエリーまたは提出を送信します。Symantec EDR はウイルス対策、SONAR、IPS 提出を受信しますが、ファイル評価提出は受信しません。Symantec Endpoint Protection は常にシマンテック社にファイル評価提出を直接送信します。
- Symantec Insight for Private Clouds
このオプションでは、グループ内のクライアントから専用 Insight サーバーに評価クエリーがリダイレクトされます。専用インサイトサーバーには、Symantec の Insight の評価データベースの複製が保存されます。専用 Insight サーバーはシマンテックの Insight サーバーよりも評価クエリーを処理します。専用 Insight サーバーを使う場合、クライアントは引き続きシマンテック社に検出についての提出を送信します。通常、専用 Insight サーバーは、インターネットから切断されているダークネットワークで使います。その場合、シマンテック社ではクライアント提出を受け取ることができません。

[サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について](#)

専用のサーバーの構成を他のクライアントグループにコピーすることもできます。

複数の専用サーバーを指定して、ネットワークトラフィックを負荷分散することができます。また複数のサーバーグループを指定して、フェールオーバーを管理することができます。

EDR サーバーを有効にする選択を行うと、クライアントのユーザーインターフェース、管理コンソールログ、レポートに EDR 接続の状態が表示されます。] の順にクリックします。EDR サーバーと通信するには、Symantec Endpoint Protection クライアントで少なくともウイルスとスパイウェアの対策を実行する必要があります。

NOTE

グループ用の専用サーバーを有効にする場合、指定された専用サーバーを利用できなければ、それらのグループ内の 12.1.5 以前のクライアントではシマンテックサーバーを使用できません。12.1.5 以前のクライアントでは優先度リストを使用できないため、単一サーバーを使用するように設定する必要があります。

専用サーバーを使うようにクライアントグループを設定するには

1. コンソールで、[クライアント] に移動し、専用サーバーリストを使用してください。
2. [ポリシー] タブで、[外部通信の設定] をクリックします。
3. [専用クラウド] タブで、[自分のデータを管理する専用サーバーを有効にします] をクリックします。
4. 使用するサーバーの種類に応じて、[インサイトルックアップと提出に **Advanced Threat Protection** サーバーを使用する] または [インサイトルックアップに専用 **Insight** サーバーを使用する] をクリックします。

優先度リスト内のサーバーの種類を混合しないでください。

5. クライアントで評価クエリーおよびクライアントのウイルス対策と SONAR 提出にシマンテックサーバーを使用する場合は、[専用サーバーが利用可能でないときは、シマンテック社のサーバーを使用します] をクリックします。

クライアントはシマンテック社に常にファイル評価の提出を送信します。

6. [専用サーバー] の下で、[追加] > [新しいサーバー] をクリックします。
7. [専用サーバーの追加] ダイアログボックスで、プロトコルを選択し、次に URL のホスト名を入力します。
8. サーバーのポート番号を指定します。
9. 12.1.5 以前のクライアントが使う単一サーバーとしてこのサーバーを指定するには、[12.1.5 以前のクライアントでは、このサーバーを専用 **Insight** サーバーとして使用します] をクリックします。12.1.5 以前のクライアントは、サーバーリストを使うことができないため、これらのレガシークライアントが使うべきサーバーを指定する必要があります。
10. 優先度グループを追加するには、[追加] > [新しいグループ] をクリックします。
11. 設定を追加のクライアントグループに適用するには [設定のコピー] をクリックします。グループと場所を選択し、[OK] をクリックします。

ウイルススキャンとスパイウェアスキャンのカスタマイズ

Windows コンピュータで実行される管理者定義のスキャン (定時スキャンとオンデマンドスキャン) のオプションをカスタマイズできます。Auto-Protect のオプションもカスタマイズできます。

Table 106: Windows コンピュータでのウイルススキャンとスパイウェアスキャンのカスタマイズ

タスク	説明
Auto-Protect 設定をカスタマイズする	次の設定を含め、多くの方法で Auto-Protect をカスタマイズできます。 - Auto-Protect でスキャンするファイルの種類 - 検出を行うときに Auto-Protect が実行する処理 - 自動保護検出のユーザー通知 ファイルシステムの Auto-Protect スキャンについて、[スキャン結果] ダイアログボックスを有効にすることもできます。 Windows クライアントの Auto-Protect のカスタマイズ Windows コンピュータで実行する電子メールスキャンの Auto-Protect のカスタマイズ
管理者定義のスキャンをカスタマイズする	定時スキャンとオンデマンドスキャンについて、次の種類のオプションをカスタマイズできます。 - 圧縮ファイル - 調整オプション - 拡張スケジュールオプション - 検出についてのユーザーへの通知 Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ スキャン処理もカスタマイズできます。
ELAM の設定を調節する	Symantec Endpoint Protection の早期起動マルウェア対策 (ELAM) がコンピュータのパフォーマンスに影響を与えていると思われる場合は、ELAM の検出を有効または無効にします。また、ELAM での誤検知が多い場合は、デフォルトの検出設定を上書きできます。 早期起動マルウェア対策 (ELAM) の検出の管理
ダウンロードインサイトの設定を調整する	検出の数を増加または減少させるために、悪質なファイルの感度を調整したいことがあります。検出の処理と、検出についてのユーザーへの通知についても設定できます。 ダウンロードインサイトの設定のカスタマイズ
スキャン処理をカスタマイズする	検出を行ったときに Symantec Endpoint Protection が実行する処理を変更できます。 検出を行ったときに Symantec Endpoint Protection が実行する処理の変更
グローバルスキャン設定をカスタマイズする	グローバルスキャン設定をカスタマイズして、クライアントコンピュータでの保護レベルを上げる、または下げることができます。 Windows クライアントのグローバルなスキャン設定の修正
ウイルス対策とスパイウェア対策のその他のオプションをカスタマイズする	クライアントが 1 つの Symantec Endpoint Protection Manager に送信するリスクイベントの種類を指定できます。 Windows コンピュータのログ処理と通知設定の修正

Table 107: Mac コンピュータでのウイルススキャンとスパイウェアスキャンのカスタマイズ

タスク	説明
Auto-Protect をカスタマイズする	Mac コンピュータで実行されるクライアントの Auto-Protect 設定をカスタマイズできます。 Mac クライアントの Auto-Protect のカスタマイズ
管理者定義のスキャンをカスタマイズする	スキャン優先度はもちろん、一般的な設定と通知もカスタマイズできます。 また、警告を有効にして、定義が最新ではないときにユーザーに警告できます。 Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

Table 108: Linux コンピュータでのウイルススキャンとスパイウェアスキャンのカスタマイズ

タスク	説明
Auto-Protect 設定をカスタマイズする	次の設定を含め、多くの方法で Auto-Protect をカスタマイズできます。 - Auto-Protect でスキャンするファイルの種類 - 検出を行うときに Auto-Protect が実行する処理 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 - 自動保護検出のユーザー通知 ファイルシステムの Auto-Protect スキャンについて、[スキャン結果] ダイアログボックスの有効と無効を切り替えることもできます。 Linux クライアントの Auto-Protect のカスタマイズ
管理者定義のスキャンをカスタマイズする	定時スキャンとオンデマンドスキャンについて、次の種類のオプションをカスタマイズできます。 - ファイルとフォルダの種類 - 圧縮ファイル - セキュリティリスク - スケジュールのオプション - 検出の処理 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 - ユーザーに送信する通知
スキャン処理をカスタマイズする	検出を行ったときに Symantec Endpoint Protection が実行する処理を変更できます。 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 検出を行ったときに Symantec Endpoint Protection が実行する処理の変更
ウイルス対策とスパイウェア対策のその他のオプションをカスタマイズする	クライアントが 1 つの Symantec Endpoint Protection Manager に送信するリスクイベントの種類を指定できます。 14.3 RU1 以降、Linux クライアントではウイルスとスパイウェアの対策に関するその他のオプションのカスタマイズが非推奨になりました。 Linux コンピュータでのログ処理設定の修正

クライアントコンピュータでのスキャンの管理

Mac コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ

Mac コンピュータで実行される管理者定義のスキャン (定時スキャンとオンデマンドスキャン) のオプションをカスタマイズできます。Auto-Protect のオプションもカスタマイズできます。

Table 109: Mac コンピュータでのウイルススキャンとスパイウェアスキャンのカスタマイズ

タスク	説明
Auto-Protect をカスタマイズする	Mac コンピュータで実行されるクライアントの Auto-Protect 設定をカスタマイズできます。 Mac クライアントの Auto-Protect のカスタマイズ
管理者定義のスキャンをカスタマイズする	スキャン優先度はもちろん、一般的な設定と通知もカスタマイズできます。 また、警告を有効にして、定義が最新ではないときにユーザーに警告できます。 Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

Linux コンピュータで実行するウイルススキャンとスパイウェアスキャンのカスタマイズ

Linux コンピュータで実行する管理者定義のスキャン（定時スキャンとオンデマンドスキャン）のオプションをカスタマイズできます。Auto-Protect のオプションもカスタマイズできます。

Table 110: Linux コンピュータでのウイルススキャンとスパイウェアスキャンのカスタマイズ

タスク	説明
Auto-Protect 設定をカスタマイズする	次の設定を含め、多くの方法で Auto-Protect をカスタマイズできます。 - Auto-Protect でスキャンするファイルの種類 - 検出を行うときに Auto-Protect が実行する処理 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 - 自動保護検出のユーザー通知 ファイルシステムの Auto-Protect スキャンについて、[スキャン結果] ダイアログボックスの有効と無効を切り替えることもできます。 Linux クライアントの Auto-Protect のカスタマイズ
管理者定義のスキャンをカスタマイズする	定時スキャンとオンデマンドスキャンについて、次の種類のオプションをカスタマイズできます。 - ファイルとフォルダの種類 - 圧縮ファイル - セキュリティリスク - スケジュールのオプション - 検出の処理 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 - ユーザーに送信する通知
スキャン処理をカスタマイズする	検出を行ったときに Symantec Endpoint Protection が実行する処理を変更できます。 14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。 検出を行ったときに Symantec Endpoint Protection が実行する処理の変更
ウイルス対策とスパイウェア対策のその他のオプションをカスタマイズする	クライアントが 1 つの Symantec Endpoint Protection Manager に送信するリスクイベントの種類を指定できます。 14.3 RU1 以降、Linux クライアントではウイルスとスパイウェアの対策に関するその他のオプションのカスタマイズが非推奨になりました。 Linux コンピュータでのログ処理設定の修正

Windows クライアントの Auto-Protect のカスタマイズ

Windows クライアントの Auto-Protect の設定をカスタマイズできます。

Windows クライアントの Auto-Protect をカスタマイズするには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] の下の [保護技術] で、[Auto-Protect] をクリックします。
3. [スキャンの詳細] タブで、[Auto-Protect を有効にする] にチェックマークが付いていることを確認します。

WARNING

Auto-Protect を無効にしている場合、ダウンロードインサイトが有効になっていてもダウンロードインサイトは機能できません。

4. [スキャン] の [ファイルの種類] で、次のいずれかのオプションを選択します。
 - すべてのファイルをスキャンする

このオプションがデフォルトで、最も安全なオプションです。

- 選択した拡張子のみをスキャンする

このオプションを選択するとスキャンパフォーマンスを高められますが、コンピュータでの保護レベルは下がる可能性があります。

5. [追加オプション] で、[セキュリティリスクをスキャンする] にチェックマークを付けるか、またはチェックマークをはずします。
6. [スキャンと監視の拡張設定] をクリックし、Auto-Protect スキャンをトリガする処理のオプションと、Auto-Protect がフロッピーディスクのスキャンを処理する方法を変更します。
7. [OK] をクリックします。
8. [ネットワークの設定] で、[リモートコンピュータ上でファイルをスキャンする] にチェックマークを付けるか、チェックマークをはずしてネットワークファイルの Auto-Protect スキャンを有効または無効にします。

デフォルトでは、Auto-Protect はファイルが実行されるときのみリモートコンピュータでファイルをスキャンします。

スキャンとコンピュータのパフォーマンスを高めるためにネットワークのスキャンを無効にしたいことがあります。

9. リモートコンピュータでのファイルスキャンが有効になっている場合は、[ネットワークの設定] をクリックして、ネットワークのスキャンオプションを修正します。
10. [ネットワークの設定] ダイアログボックスで、次のいずれかの処理を行います。
 - Auto-Protect を実行するリモートコンピュータのファイルを信頼するために Auto-Protect を有効または無効にする
 - Auto-Protect スキャンのネットワークキャッシュオプションを設定する

11. [OK] をクリックします。

12. [処理] タブで、いずれかのオプションを設定します。

[検出を行ったときに Symantec Endpoint Protection が実行する処理の変更](#)

Auto-Protect の修復オプションも設定できます。

13. [通知] タブで、いずれかの通知オプションを設定します。

[クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理](#)

14. [拡張] タブで、次のいずれかのオプションを設定します。

- 起動と終了
- **Auto-Protect** の再ロードと有効化

15. [追加オプション] で、[ファイルキャッシュ] または [リスク追跡] をクリックします。

16. ファイルキャッシュまたはリスク追跡を設定し、[OK] をクリックします。

17. このポリシーの設定を完了したら、[OK] をクリックします。

[Windows コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ](#)

[クライアントコンピュータでのスキャンの管理](#)

Mac クライアントの **Auto-Protect** のカスタマイズ

Mac コンピュータで実行されるクライアントの Auto-Protect 設定をカスタマイズできます。

Mac クライアントの Auto-Protect をカスタマイズするには

-
1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
 2. [Mac の設定] の下の [保護技術] で、[Auto-Protect と SONAR] をクリックします。
 3. [スキャンの詳細] タブの一番上にあるロックアイコンをクリックし、すべての設定をロックまたはロック解除します。
 4. 次のいずれかのオプションのチェックマークを付けるかはずします。
 - **Auto-Protect** を有効にする
 - 感染ファイルを自動的に修復する
 - 修復できないファイルを検疫する
 - 圧縮ファイルをスキャン
 5. [一般スキャンの詳細] で、Auto-Protect がスキャンするファイルを指定します。

NOTE

スキャンからファイルを除外するには、[指定したフォルダを除くすべての場所をスキャンする] を選択してから例外ポリシーを追加し、除外するファイルを指定します。

スキャンからのファイルまたはフォルダの除外

6. [マウント済みディスクのスキャンの詳細] で、利用可能なオプションのチェックマークを付けるかはずします。
7. [疑わしい動作の検出] で、[疑わしい動作の検出を有効にする] のチェックマークをつけるか外します。
このオプションは、バージョン 14.3 RU1 以降で利用可能です。
8. [通知] タブで、いずれかの通知オプションを設定してから [OK] をクリックします。

Mac コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ

検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理

Linux クライアントの Auto-Protect のカスタマイズ

Linux コンピュータで実行するクライアントの Auto-Protect 設定をカスタマイズすると便利です。

NOTE

14.3 RU1 以降、Linux クライアントでは、[処理] タブ、[通知] タブ、[拡張] タブ (ステップ 9、10、11) のオプションの設定は非推奨になりました。

Linux クライアントの Auto-Protect をカスタマイズするには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Linux の設定] の [保護技術] で、[Auto-Protect] をクリックします。
3. [スキャンの詳細] タブで、[Auto-Protect を有効にする] にチェックマークを付けるか、チェックマークをはずします。
4. [スキャン] の [ファイルの種類] で、次のいずれかのオプションをクリックします。
 - すべてのファイルをスキャンする
このオプションがデフォルトで、最も安全なオプションです。
 - 選択した拡張子のみをスキャンする
このオプションを選択するとスキャンパフォーマンスを高められますが、コンピュータでの保護レベルは下がる可能性があります。
(14.3 RU1 以降使用できません)

-
5. [追加オプション] で、[セキュリティリスクをスキャンする] にチェックマークを付けるか、またはチェックマークをはずします。
 6. [スキャンと監視の拡張設定] をクリックし、Auto-Protect スキャンをトリガする処理のオプションと、Auto-Protect が圧縮ファイルのスキャンを扱う方法を変更します。
 7. [OK] をクリックします。
 8. [ネットワークの設定] で、[リモートコンピュータ上でファイルのスキャンする] にチェックマークを付けるか、チェックマークをはずしてネットワークファイルの Auto-Protect スキャンを有効または無効にします。
デフォルトでは、Auto-Protect はファイルが実行されるときのみリモートコンピュータでファイルのスキャンします。
スキャンとコンピュータのパフォーマンスを高めるためにネットワークのスキャンを無効にしたいことがあります。
 9. [処理] タブで、いずれかのオプションを設定します。
[検出を行ったときに Symantec Endpoint Protection が実行する処理の変更](#)
Auto-Protect の修復オプションも設定できます。
 10. [通知] タブで、いずれかの通知オプションを設定します。
[クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理](#)
 11. [拡張] ページで、[キャッシュを有効にする] にチェックマークを付けるかまたははずします。
キャッシュサイズを設定するか、またはデフォルトの設定を使います。
 12. [OK] をクリックします。

[Linux コンピュータで実行するウイルススキャンとスパイウェアスキャンのカスタマイズ](#)

[検出を行ったときに Symantec Endpoint Protection が実行する処理の変更](#)

[クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理](#)

Windows コンピュータで実行する電子メールスキャンの Auto-Protect のカスタマイズ

Windows コンピュータでは、電子メールスキャンの Auto-Protect をカスタマイズできます。

Windows コンピュータで実行する電子メールスキャンの Auto-Protect をカスタマイズするには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] で、次のいずれかのオプションを選択します。
 - **Microsoft Outlook Auto-Protect**
 - **インターネット電子メール Auto-Protect***
 - **Lotus Notes Auto-Protect***

* 14.2 RU1 より前のクライアントバージョンでのみ利用可能。
3. [スキャンの詳細] タブで、[インターネット電子メール **Auto-Protect** を有効にする] にチェックマークを付けるか、チェックマークをはずします。
4. [スキャン] の [ファイルの種類] で、次のいずれかのオプションを選択します。
 - **すべてのファイルをスキャンする**
このオプションがデフォルトで、最も安全なオプションです。
 - **選択した拡張子のみをスキャンする**

このオプションを選択するとスキャンパフォーマンスを高められますが、コンピュータでの保護レベルは下がる可能性があります。

5. [圧縮ファイル内部のファイルをスキャンする] をチェックするかチェックマークをはずします。
6. [処理] タブで、いずれかのオプションを設定します。

検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

7. [通知] タブの [通知] で、[感染コンピュータに通知メッセージを表示する] をチェックするかチェックマークをはずします。メッセージはカスタマイズすることもできます。
8. [電子メール通知] で、次のいずれかのオプションをチェックするかチェックマークをはずします。
 - 電子メールメッセージに警告を挿入する
 - 送信者に電子メールを送信する
 - 他のユーザーに電子メールを送信

メッセージテキストをカスタマイズし、警告を含めることができます。インターネット電子メール Auto-Protect の場合は、電子メールサーバーも指定する必要があります。

9. インターネット電子メール Auto-Protect の場合のみ、[拡張] タブの [暗号化接続] で、暗号化 POP3 または SMTP 接続を有効または無効にします。
10. [大量メール送信型ワームヒューリスティック] で [アウトバウンドワームヒューリスティック] をチェックするかチェックマークをはずします。
11. このポリシーの設定を完了したら、[OK] をクリックします。

Windows コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ

クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理

Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

Windows コンピュータで実行されるクライアントに対する定時スキャンまたはオンデマンドスキャンをカスタマイズすることができます。圧縮ファイルのスキャンのオプションを設定し、コンピュータのスキャンやスキャンパフォーマンスを最適化できます。

Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンをカスタマイズするには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] で、[管理者定義のスキャン] をクリックします。
3. 次のいずれかの処理を実行します。
 - [定時スキャン] で、カスタマイズする定時スキャンを選択するか、新しい定時スキャンを作成します。
 - [管理者オンデマンドスキャン] で、[編集] をクリックします。
4. [スキャンの詳細] タブで、[スキャンの拡張オプション] を選択します。
 - [圧縮ファイル] タブで、圧縮ファイルをスキャンするレベルの数を減らすことができます。レベルの数を減らすと、クライアントコンピュータのパフォーマンスが向上することがあります。
 - [調整] タブで、クライアントコンピュータまたはスキャンにとって最適なパフォーマンスが得られるように調整のレベルを変更します。

[OK] をクリックして変更を保存します。

-
5. [スキャンの詳細] タブで、レガシーの 12.1.x クライアントのみについて、インサイトルックアップを有効、無効にできます。

14 以前のバージョンの Symantec Endpoint Protection Manager では、[インサイトルックアップ] タブで、任意の設定を変更して、インサイトルックアップが評価検出をどのように処理するかを調整します。

6. 定時スキャンの場合のみ、[スケジュール] タブで、次のいずれかのオプションを設定します。
- スキャン期間
スキャンが一時停止し、クライアントコンピュータがアイドル状態になるまで待機するまで、どれだけの期間スキャンを実行するかを設定できます。また、スキャンの開始時間をランダム化できます。
 - 未実行の定時スキャン
未実行のスキャンのために再試行の間隔を指定できます。
7. [処理] タブで、任意の検出処理を変更します。
- [検出を行ったときに Symantec Endpoint Protection が実行する処理の変更](#)
8. [通知] タブで、スキャンが検出を行ったときにクライアントコンピュータに表示される通知を有効または無効にします。
- [クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理](#)
9. [OK] をクリックします。

[Windows コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ](#)

[Windows コンピュータで実行される定時スキャンの設定](#)

Mac コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

定時スキャンとオンデマンドスキャンは別個にカスタマイズします。オプションの一部は異なります。

1. Mac コンピュータで実行する定時スキャンをカスタマイズするには、コンソールで [ウィルスとスパイウェアの対策ポリシー] を開きます。
2. [Mac の設定] で、[管理者定義のスキャン] を選択します。
3. [定時スキャン] で、カスタマイズする定時スキャンを選択するか、新しい定時スキャンを作成します。
新しいスキャンでは、新しいスキャンを手動で作成するか、またはテンプレートで定時スキャンを作成することができます。
4. [スキャンの詳細] タブの [ドライブとフォルダをスキャン] で、スキャンする項目を選択します。
5. アイドルタイムスキャンの有効と無効を切り替えることもできます。オプションを有効にすると、コンピュータの性能が良くなります。オプションを無効にすると、スキャンの性能が良くなります。
6. [OK] をクリックします。
このポリシーに含まれている他のすべてのスキャンについて、スキャンの詳細を編集します。
7. [通知] タブで、スキャン検出についての通知メッセージを有効または無効にします。設定は、このポリシーに含めるすべての定時スキャンに適用されます。
8. [共通の設定] タブで、次のいずれかのオプションを設定します。
 - スキャンオプション
 - 処理
 - 警告

これらの設定は、このポリシーに含めるすべての定時スキャンに適用されます。

9. [OK] をクリックします。
10. Mac コンピュータで実行するオンデマンドスキャンをカスタマイズするには、[ウィルスとスパイウェアの対策ポリシー] ページの [**Mac** の設定] で、[管理者定義のスキャン] を選択します。
11. [管理者オンデマンドスキャン] で、[編集] をクリックします。
12. [スキャンの詳細] タブの [ドライブとフォルダをスキャン] で、スキャンする項目を選択します。
また、スキャン検出の処理を指定したり、圧縮ファイルのスキャンを有効または無効にしたりできます。
13. [通知] タブで、検出についての通知を有効または無効にします。
クライアントに表示されるメッセージも指定できます。
14. [OK] をクリックします。

Mac コンピュータで実行されるウィルススキャンとスパイウェアスキャンのカスタマイズ

Mac コンピュータで実行される定時スキャンの設定

検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

クライアントコンピュータに表示されるウィルスとスパイウェアの通知の管理

Linux コンピュータで実行するクライアントに対する管理者定義のスキャンのカスタマイズ

Linux コンピュータで実行するクライアントに対する定時スキャンやオンデマンドスキャンをカスタマイズすると便利です。圧縮ファイルのスキャンのオプションを設定し、コンピュータのスキャンやスキャンパフォーマンスを最適化できます。

Linux コンピュータで実行するクライアントに対する管理者定義のスキャンをカスタマイズするには

1. コンソールで、ウィルスとスパイウェアの対策ポリシーを開きます。
2. [Linux の設定] で、[管理者定義のスキャン] をクリックします。
3. 次のいずれかの処理を実行します。
 - [定時スキャン] で、カスタマイズする定時スキャンを選択するか、新しい定時スキャンを作成します。
 - [管理者オンデマンドスキャン] で、[編集] をクリックします。
4. [スキャンの詳細] ページで、[すべてのフォルダをスキャン] にチェックマークを付けるか、またはスキャンする特定のフォルダを指定します。
5. [すべてのファイルをスキャンする] または [選択した拡張子のみをスキャンする] をクリックしてスキャンしたい拡張子を指定します。
14.3 RU1 以降、[選択した拡張子のみをスキャンする] オプションは利用できません。
6. [圧縮ファイル内部のファイルをスキャンする] を選択して圧縮ファイルをスキャンするレベル数を減らすことができます。レベルの数を減らすと、クライアントコンピュータのパフォーマンスが向上することがあります。
7. [セキュリティリスクをスキャンする] にチェックマークを付けるか、チェックマークをはずします。
8. 定時スキャンの場合のみ、[スケジュール] タブで、次のいずれかのオプションを設定します。
 - スキャンスケジュール
スキャンを実行する頻度 (日単位、週単位、月単位) を設定できます。
 - 未実行の定時スキャン
未実行のスキャンのために再試行の間隔を指定できます。

-
9. [処理] タブで、任意の検出処理を変更します。

[検出を行ったときに Symantec Endpoint Protection が実行する処理の変更](#)

14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。

10. [通知] タブで、スキャンが検出を行ったときにクライアントコンピュータに表示される通知を有効または無効にします。

[クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理](#)

11. [OK] をクリックします。

[Linux コンピュータで実行するウイルススキャンとスパイウェアスキャンのカスタマイズ](#)

[Linux コンピュータで実行する定時スキャンの設定](#)

[検出を行ったときに Symantec Endpoint Protection が実行する処理の変更](#)

[クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理](#)

スキャンのランダム化による Windows クライアントの仮想化環境でのコンピュータパフォーマンスの向上

定時スキャンをランダム化して、Windows クライアントコンピュータでのパフォーマンスを向上させることができます。ランダム化は仮想化された環境で重要です。

たとえば、午後 8 時にスキャンを実行するようにスケジュールしたとします。間隔に 4 時間を選択すると、午後 8 時から午前 12 時の間のランダム化された時刻に、クライアントコンピュータでスキャンが開始されます。

仮想化された環境でスキャンのランダム化によってコンピュータパフォーマンスを向上させるには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] で、[管理者定義のスキャン] をクリックします。
3. 新しい定時スキャンを作成するか、既存の定時スキャンを選択して編集します。
4. [定時スキャンの追加] または [定時スキャンの編集] ダイアログボックスで、[スケジュール] タブをクリックします。
5. [スキャンスケジュール] で、スキャンを実行する頻度を選択します。
6. [スキャン期間] で、[最長で] にチェックマークを付け、時間数を選択します。この時間数は、その間にスキャンがランダム化される時間間隔を制御します。
7. [この期間内でスキャン開始日時をランダム化する (VM で推奨)] は必ず有効にします。
8. [OK] をクリックします。
9. 仮想コンピュータを実行するコンピュータを含むグループにポリシーを適用するようにします。

[スキャンの調整によるクライアントコンピュータパフォーマンスの改善](#)

[Windows コンピュータで実行される定時スキャンの設定](#)

Windows クライアントのグローバルなスキャン設定の修正

Windows クライアントコンピュータで実行されるスキャンのグローバルな設定をカスタマイズできます。これらのオプションを修正すると、クライアントコンピュータのセキュリティを向上させることができます。

NOTE

これらのオプションを修正してクライアントコンピュータでの保護を強化すると、クライアントコンピュータのパフォーマンスに影響することがあります。

クライアントコンピュータでのスキャンの管理

Windows コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ

Windows クライアントのグローバルなスキャン設定を修正するには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] で、[グローバルスキャンオプション] をクリックします。
3. 次のいずれかのオプションを設定します。

Insight	インサイトを使うと、スキャンでシマンテック社が良好だと信頼するファイル（安全性は高）や、コミュニティが良好だと信頼するファイル（安全性は低）をスキップできます。
Bloodhound	Bloodhound は、ファイルの論理部分を分離して確認し、未知のウイルスである見込みの高いものを検出します。続いて、Bloodhound はウイルスのように動作するプログラム論理を分析します。検出の感度のレベルを指定できます。
マップしたネットワークドライブのパスワード	クライアントがネットワークドライブをスキャンするときにユーザーにパスワードを要求するかどうかを指定します。

4. [OK] をクリックします。

Windows コンピュータのログ処理と通知設定の修正

それぞれのウイルスとスパイウェアの対策ポリシーには、Windows クライアントコンピュータで実行されるすべてのウイルススキャンとスパイウェアスキャンに適用されるオプションが含まれています。

次のオプションを設定できます。

- ブラウザのホームページを変更したセキュリティリスクを修復するときに Symantec Endpoint Protection が使うデフォルトの URL を指定します。
- リスクログの処理オプションを指定します。
- 定義が最新でないときや見つからないときにユーザーに警告します。
- 自動保護または管理者定義のスキャンから仮想イメージを除外します。

Windows コンピュータのログ処理と通知設定を修正するには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] の下で、[その他] をクリックします。
[インターネットブラウザ保護] のオプションを指定します。
3. [ログの処理] タブで、イベントフィルタ、ログの保有、ログの集計のオプションを設定します。
4. [通知] タブで、グローバルな通知を設定します。

Windows コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ

5. [OK] をクリックします。

クライアントコンピュータに表示されるウイルスとスパイウェアの通知の管理

Linux コンピュータでのログ処理設定の修正

それぞれのウイルスとスパイウェアの対策ポリシーには、Linux クライアントコンピュータで実行するすべてのウイルススキャンとスパイウェアスキャンに適用されるログ処理設定が含まれています。

14.3 RU1 以降では、Linux クライアントでログ処理の設定を変更することは推奨されていません。

Linux コンピュータのログ処理設定を修正するには

-
1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
 2. [Linux の設定] で、[その他] をクリックします。
 3. [ログの処理] タブで、イベントフィルタ、ログの保有、ログの集計のオプションを設定します。

ログの表示

ダウンロードインサイトの設定のカスタマイズ

クライアントコンピュータでの誤認検出を減らすため、ダウンロードインサイトの設定をカスタマイズしたいことがあります。悪質なファイルの特徴付けるために使われるファイル評価データに対するダウンロードインサイトの感度を変更できます。ダウンロードインサイトが検出を行った場合にクライアントコンピュータに表示する通知も変更できます。

Windows コンピュータで実行されるウイルススキャンとスパイウェアスキャンのカスタマイズ

ダウンロードインサイト検出の管理

ダウンロードインサイトの設定をカスタマイズするには

1. コンソールで、[ウィルスとスパイウェアの対策ポリシー] を開き、[ダウンロード保護] を選択します。
2. [ダウンロードインサイト] タブで、[ダウンロードインサイトのファイル評価に基づく潜在的リスク検出を有効にする] にチェックマークが付いていることを確認します。

Auto-Protect が無効になっている場合、ダウンロードインサイトが有効になっていてもダウンロードインサイトは動作できません。

3. 悪質なファイルの感度スライダーを適切なレベルまで移動します。
レベルを高く設定すると、より多くのファイルを悪質だと検出し、より少ないファイルを未確認として検出します。しかし、高い設定であるほど、より多くの誤認が返されます。
4. 選択 次のオプションにチェックマークを付けると、未確認ファイルを調べるための追加条件として使います。
 - [x 人以下のユーザーによるファイル]
 - [ユーザーにレポートされてから x 日以内のファイル]

未確認ファイルがこれらの基準を満たすと、ダウンロードインサイトはファイルが悪質であると検出します。

5. [信頼できるインターネットサイトまたはイントラネットサイトからダウンロードしたファイルを自動的に信頼する] にチェックマークが付いていることを確認します。
6. [処理] タブの [悪質なファイル] で、第 1 の処理と第 2 の処理を指定します。
7. [未確認ファイル] で処理を指定します。
8. [通知] タブで、ダウンロードインサイトが検出を行ったときにクライアントコンピュータにメッセージを表示するかどうかを指定します。
ダウンロードインサイトが検出したファイルをユーザーが許可すると表示される警告メッセージのテキストをカスタマイズすることもできます。
9. [OK] をクリックします。

検出を行ったときに Symantec Endpoint Protection が実行する処理の変更

スキャンで検出を行ったときに実行する必要がある 1 つ以上の処理を設定できます。各スキャンには、[クリーニング]、[検疫]、[削除]、[放置する (ログのみ)] などの独自の処理のセットがあります。

Windows クライアントと Linux クライアントでは、検出の各カテゴリは、第 1 の処理と、第 1 の処理が可能でない場合の第 2 の処理を指定して設定できます。

14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。

デフォルトでは、**Symantec Endpoint Protection** はウイルスに感染したファイルのクリーニングを試みます。**Symantec Endpoint Protection** はファイルをクリーニングできなければ、次の処理を実行します。

- ファイルを感染コンピュータの検疫に移動し、ファイルへのアクセスをすべて拒否します。
- イベントをログに記録します。

デフォルトでは、Symantec Endpoint Protection はセキュリティリスクに感染したすべてのファイルを検疫に移動します。

処理をログのみに設定した場合、デフォルトでは、ユーザーが感染ファイルを作成または保存すると、Symantec Endpoint Protection はそれらのファイルを削除します。

Windows コンピュータでは、管理者によるスキャン、オンデマンドスキャン、ファイルシステムの Auto-Protect スキャンについて、修復処理を設定することもできます。

ユーザーがこのポリシーを使うクライアントコンピュータ上で処理を変更できないように、処理をロックできます。

WARNING

セキュリティリスクの削除処理は慎重に使ってください。場合によっては、アプリケーションが機能しなくなることがあります。セキュリティリスクによる影響があるファイルを削除するようにクライアントを設定すると、ファイルを復元できなくなります。

セキュリティリスクによる影響があるファイルをバックアップするには、代わりに検疫の処理を使います。

1. オプション 1: Windows クライアントまたは Linux クライアントでの検出時に Symantec Endpoint Protection が実行する処理を変更するには、[ウイルスとスパイウェアの対策のポリシー] で、[Windows の設定] または [Linux 設定] で、スキャン (Auto-Protect スキャン、管理者スキャン、オンデマンドスキャン) を選択します。

14.3 RU1 以降、Linux クライアントの検出用の処理の設定は非推奨になりました。

2. [処理] タブの [検出] で、マルウェアまたはセキュリティリスクの種類を選択します。

デフォルトでは、各サブカテゴリは自動的に、カテゴリ全体に設定されている処理を使うように設定されます。

NOTE

Windows クライアントでは、これらのカテゴリはシマンテック社がリスクに関する新しい情報を入手するにつれて動的に変化します。

3. サブカテゴリに対する処理のみを設定するには、次のいずれかを実行します。

- [マルウェアに対して設定した処理を上書きする] にチェックマークを付け、そのサブカテゴリ専用の処理を設定します。

NOTE

シマンテック社がリスクを分類する方法に応じて、1 つのカテゴリの下に 1 つのサブカテゴリだけが存在する場合があります。たとえば、[マルウェア] にウイルスという名前のサブカテゴリが 1 つ存在することもあります。

- [セキュリティリスクに設定した処理を上書きする] にチェックマークを付け、そのサブカテゴリ専用の処理を設定します。

4. [処理対象] で、クライアントソフトウェアがそのカテゴリのウイルスまたはセキュリティリスクを検出したときに実行する第 1 と第 2 の処理を選択します。

セキュリティリスクの削除処理は慎重に使ってください。場合によっては、アプリケーションが機能しなくなることがあります。

5. 処理を設定するカテゴリ (ウイルスとセキュリティリスク) ごとにこれらの手順を繰り返します。
6. このポリシーの設定を完了したら、[OK] をクリックします。
7. オプション 2: Mac クライアントでの検出時に Symantec Endpoint Protection が実行する処理を変更するには、[ウイルスとスパイウェアの対策ポリシー] の [Mac の設定] で、[管理者定義のスキャン] を選択します。
8. 次のいずれかの処理を実行します。
 - 定時スキャンの場合は、[共通の設定] タブを選択します。
 - オンデマンドスキャンの場合は、[スキャン] タブの [管理者オンデマンドスキャン] で、[編集] をクリックします。
9. [処理] で、次のオプションのどちらかにチェックマークを付けます。
 - 感染ファイルを自動的に修復する
 - 修復できないファイルを検疫する
10. オンデマンドスキャンの場合は [OK] をクリックします。
11. このポリシーの設定を完了したら、[OK] をクリックします。

スキャン処理の確認と識別されたコンピュータの再スキャン

ウイルスとセキュリティリスクの除去

Windows コンピュータでのユーザーによるスキャンの進行状況の表示とスキャンの操作の許可

スキャンの進行状況のダイアログボックスを Windows クライアントコンピュータに表示するかどうかを設定できます。このダイアログボックスをクライアントコンピュータに表示するようにした場合、ユーザーはいつでも管理者定義のスキャンを一時停止または延期することができます。

ユーザーがスキャンの進行状況を表示することを許可すると、クライアント UI のメインページに現在実行中のスキャンのスキャン進行状況を表示するためのリンクが表示されます。次の定時スキャンのスケジュールを再設定するリンクも表示されます。

ユーザーがスキャンの進行状況を表示することを許可すると、クライアント UI のメインページに次のオプションが表示されます。

- スキャンの実行時に、メッセージリンク [スキャン実行中] が表示されます。
ユーザーはこのリンクをクリックしてスキャンの進行状況を表示できます。
- 次の定時スキャンのスケジュールを再設定するリンクも表示されます。

ユーザーがスキャンを確実に停止できるように設定できます。ユーザーによるスキャンの一時停止または延期のオプションを設定することもできます。

ユーザーによる次のスキャン処理の実行を許可できます。

一時停止	ユーザーがスキャンを一時停止すると、スキャン結果のダイアログボックスは開いたままで、ユーザーがスキャンを続行するか中止するまで待機します。コンピュータの電源を切った場合、一時停止されたスキャンは継続されません。
休止	ユーザーが定時スキャンを休止する場合、1 時間休止または 3 時間休止のどちらかを選択できます。また、休止する回数も設定できます。スキャンが休止されると、スキャン結果のダイアログボックスは一度閉じ、休止期間が終了してスキャンが再開された時点で再表示されます。
中止	ユーザーがスキャンを停止した場合、通常スキャンはすぐに停止します。クライアントソフトウェアが圧縮ファイルをスキャン中にユーザーがスキャンを停止した場合、スキャンはすぐには停止しません。この場合、スキャンは、圧縮ファイルのスキャンが完了するとすぐに停止します。停止されたスキャンは再開されません。

一時停止されたスキャンは、指定した時間間隔が経過すると自動的に再開されます。

NOTE

ユーザーは Power Eraser 分析を停止できますが、一時停止または休止することはできません。

この手順で使うオプションについて詳しくは [ヘルプ] を参照してください。

Windows コンピュータでのユーザーによるスキャンの進行状況の表示とスキャンの操作を許可するには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] で、[管理者定義のスキャン] をクリックします。
3. [拡張] タブの [スキャン進行状況オプション] で、[スキャンの進行状況を表示する] または [リスクを検出した場合にスキャンの進行状況を表示する] をクリックします。
4. スキャンが完了したら自動的にスキャンの進行状況インジケータを閉じるには、[完了したらスキャン進行状況ウィンドウを閉じる] にチェックマークを付けます。
5. [ユーザーによるスキャンの停止を許可する] にチェックマークを付けます。
6. [一時停止オプション] をクリックします。
7. [スキャン一時停止オプション] ダイアログボックスで、次のいずれかの処理を行います。
 - ユーザーがスキャンを一時停止できる時間を制限するには、[スキャンを一時停止できる時間を限定する] にチェックマークを付け、時間を分単位で入力します。範囲は 3 から 180 です。
 - ユーザーがスキャンを延期 (または休止) できる回数を制限するには、[休止の最大回数] ボックスに 1 から 8 の数値を入力します。
 - デフォルトでは、ユーザーがスキャンを延期できる時間は 1 時間です。この制限を 3 時間に変更するには、[ユーザーがスキャンを 3 時間休止するのを許可する] にチェックマークを付けます。
8. [OK] をクリックします。

クライアントコンピュータでのスキャンの管理

Symantec Endpoint Protection クライアントと連携する Windows セキュリティセンターの通知の設定

ウイルスとスパイウェアの対策ポリシーを使って、Windows XP Service Pack 3 を実行するクライアントコンピュータの Windows セキュリティセンターを設定できます。

Windows コンピュータで実行されるクライアントに対する管理者定義のスキャンのカスタマイズ

NOTE

Windows XP SP3 のみを実行するクライアントコンピュータでは、Windows セキュリティセンターのすべてのオプションを設定できます。Windows Vista と Windows 7 以降では、[定義が最新でないときに Windows セキュリティセンターメッセージを表示する] オプションのみ設定できます。

Table 111: Windows セキュリティセンターとクライアントの連携方法を設定するオプション

オプション	説明	使うとき
Windows セキュリティセンターを無効にする	クライアントコンピュータの Windows セキュリティセンターを永続的または一時的に無効にします。 利用可能なオプション: • しない。Windows セキュリティセンターはクライアントコンピュータで常に有効になります。 • 1 回。Windows セキュリティセンターを 1 回だけ無効にします。ユーザーが有効にした場合は、再び無効になりません。 • 常時。Windows セキュリティセンターはクライアントコンピュータで永続的に無効になります。ユーザーが有効にしても、すぐに無効になります。 • 復元。Windows セキュリティセンターはウイルスとスパイウェアの対策ポリシーが以前に無効にした場合に有効になります。	セキュリティ警告をクライアントユーザーに表示しない場合は Windows セキュリティセンターを永続的に無効にしてください。クライアントユーザーは Symantec Endpoint Protection の警告を受信できません。 セキュリティ警告をクライアントユーザーに表示する場合は Windows セキュリティセンターを永続的に有効にしてください。Symantec Endpoint Protection の警告を表示するために Windows セキュリティセンターを設定できます。
Windows セキュリティセンターでウイルス対策警告を表示する	Symantec Endpoint Protection クライアントからのウイルス対策の警告が Windows の通知領域に表示されるように設定します。	コンピュータの Windows の通知領域で他のセキュリティ警告とともに Symantec Endpoint Protection の警告をユーザーに表示する場合はこの設定を有効にしてください。
定義が最新でないときに Windows セキュリティセンターメッセージを表示する	Windows セキュリティセンターで定義が最新ではないと見なされるまでの日数を設定します。デフォルトでは、Windows セキュリティセンターは 30 日後にこのメッセージを送信します。	Windows セキュリティセンターで最新ではない定義についてクライアントユーザーにデフォルトの時間 (30 日) よりも高頻度で通知する場合はこのオプションを設定してください。 Note: クライアントコンピュータでは、Symantec Endpoint Protection は 15 分ごとに有効期限、定義の日付、現在の日付を比較します。通常、定義は自動的に更新されるため、最新でない状態が Windows セキュリティセンターに報告されることはありません。定義を手動で更新する場合、Windows セキュリティセンターで正確な状態を表示するには最大 15 分待つ必要があります。

Symantec Endpoint Protection クライアントと連携するように Windows セキュリティセンターを設定するには

1. コンソールで、ウイルスとスパイウェアの対策ポリシーを開きます。
2. [Windows の設定] の下で、[その他] をクリックします。
3. [その他] タブで、Windows セキュリティセンターのオプションを指定します。
4. [OK] をクリックします。

Symantec Endpoint Protection 遠隔測定データを提出してセキュリティを向上させる

[概要](#)

[目的](#)

[遠隔測定データ収集の有効化](#)

[よく寄せられる質問 - 遠隔測定データで解決できる問題は？](#)

パフォーマンス、サイジング、および配備

概要

遠隔測定（データ提出、データ収集ともいわれる）ではネットワークのセキュリティ態勢を強化し、製品の使用感を向上するために情報を収集します。遠隔測定は次の種類の情報を幅広く収集します。

- ハードウェアとソフトウェアの詳細を含むシステム環境
- 製品のエラーと関連イベント
- 製品構成の有効性

収集したデータはシマンテック社に送信されます。

NOTE

シマンテック社が遠隔測定によって収集したデータには、直接的には識別できない匿名要素が含まれている場合があります。シマンテック社は個人ユーザーを特定するために遠隔測定データの使用を必要としたり求めたりすることはありません。

目的

シマンテック社は、これらの情報を使ってユーザーの製品使用感を分析し、改良します。

- シマンテック社のサポートで遠隔測定を使用します。
- シマンテック社は、脅威の状況を明らかにするために、Risk Insight プログラムに含まれる遠隔測定を使用します。

遠隔測定データ収集の有効化

シマンテック社は、管理サーバーと Symantec Endpoint Protection クライアントの両方から遠隔測定データを収集します。

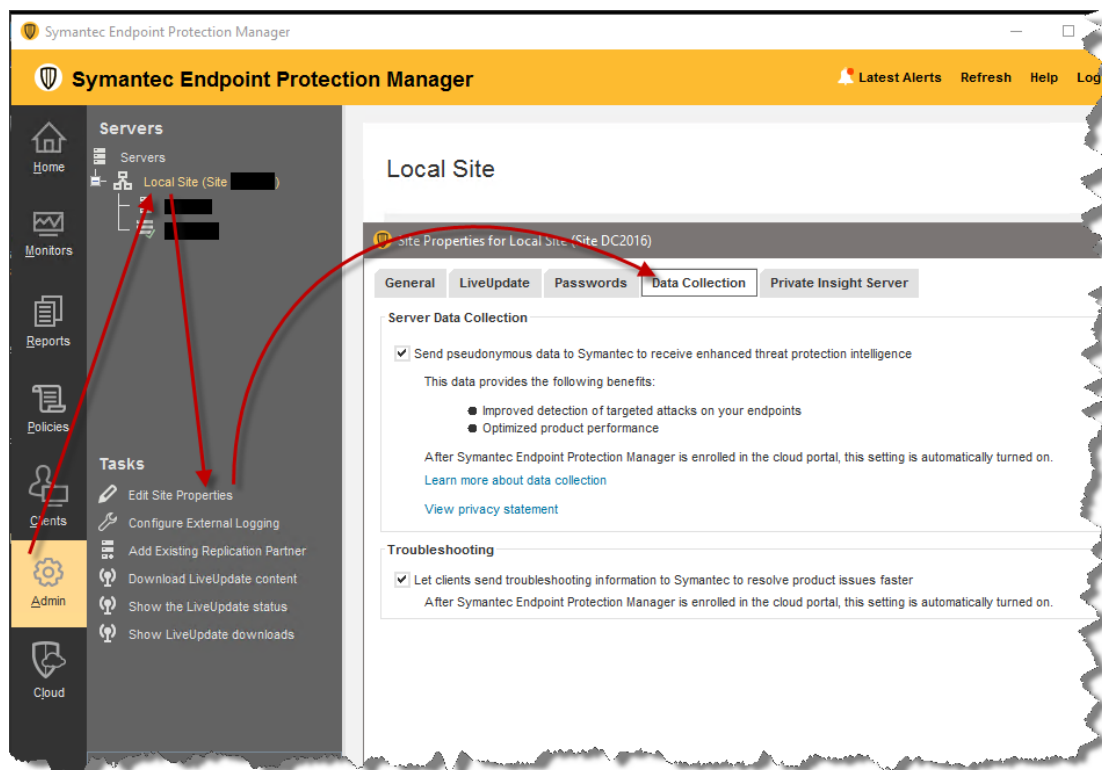
ただし、ネットワーク帯域幅の問題やクライアントから送信するデータの制限によっては、遠隔測定データの提出の無効化が必要な場合もあります。クライアント活動ログを調べると、提出活動を確認し、帯域幅の使用状況を監視できます。

管理サーバーの遠隔測定データの収集を有効または無効にするには

1. サーバーのデータ収集の [匿名のデータをシマンテック社に送信して詳細な脅威防止インテリジェンスを受け取る] オプションを有効または無効にします。
 - 管理コンソールで、[管理] > [サーバー] > [ローカルサイト] > [サイトのプロパティ] > [データ収集] に移動してオプションを変更します。

NOTE

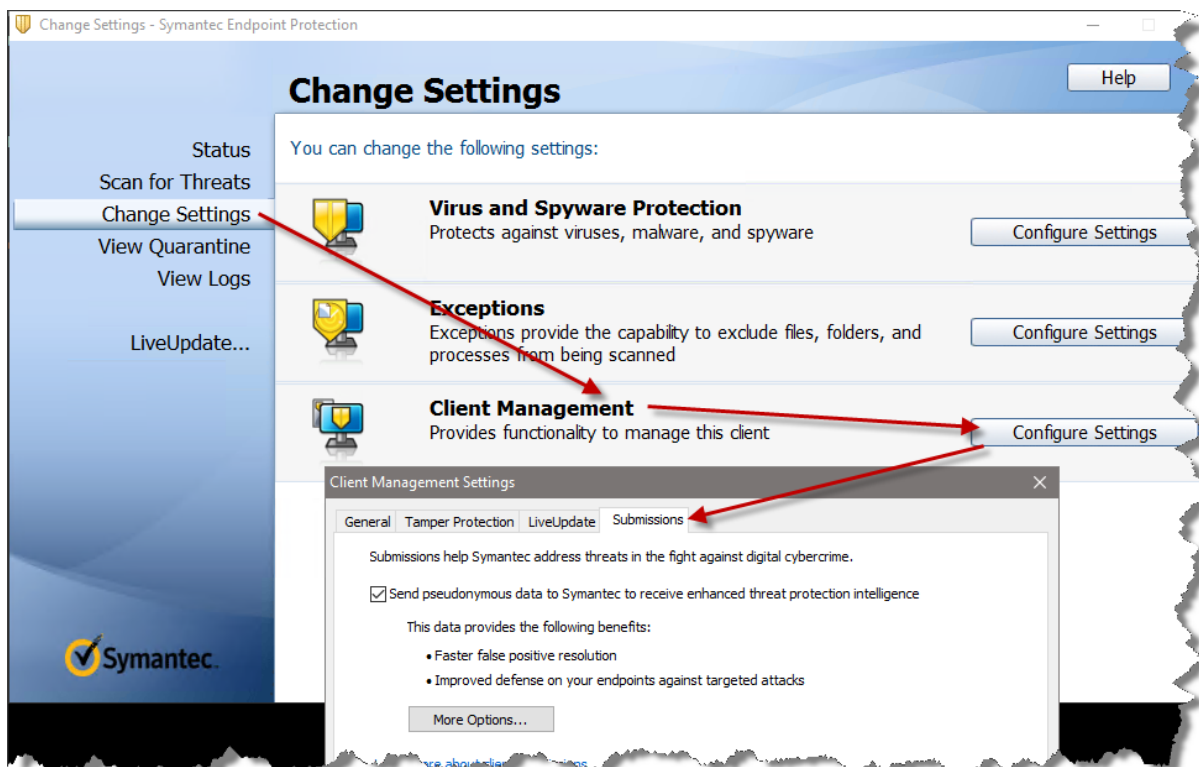
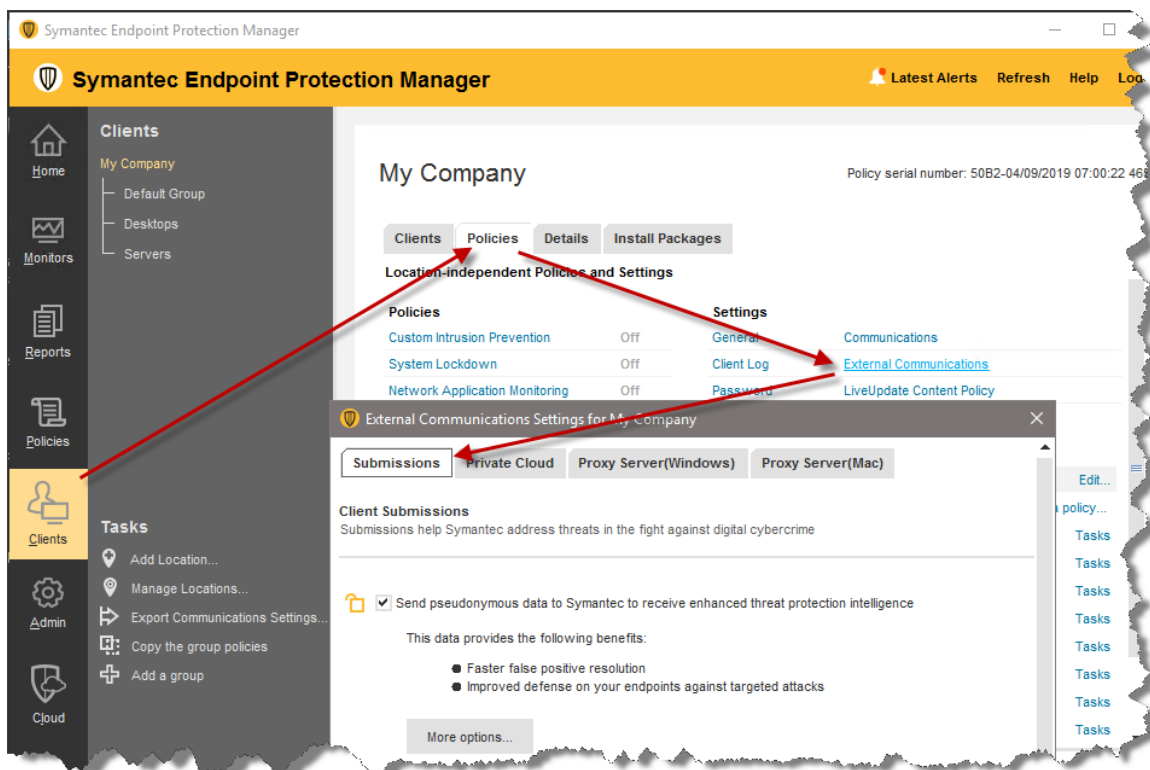
つの Symantec Endpoint Protection Manager のインストール時に、サーバーのデータ収集オプションを変更することもできます。



クライアントの遠隔測定データの提出を有効または無効にするには

2. クライアントのデータ提出の [匿名のデータをシマンテック社に送信して詳細な脅威防止インテリジェンスを受け取る] オプションを有効または無効にします。管理コンソールでグループレベルでオプションを変更したり、クライアントユーザーインターフェースで単一クライアントのオプションのみを変更することができます。

 - 管理コンソールで、[クライアント] > [ポリシー] タブに移動します。[設定] ペインで [外部通信の設定] > [クライアント提出] を選択します。
 - クライアントユーザーインターフェースで、[設定の変更] > [クライアント管理] > [オプションの設定] > [クライアント提出] に移動します。



企業の各クライアントは1つのグループに属します。グループには独自のポリシーが設定されています。親グループからポリシーを継承するようにグループを設定することもあります。クライアントによるデータ提出をグループ全体に設定した場合は、必要に応じてすべてのグループに設定が適用されていることを確認します。

NOTE

提出を無効にして設定をロックすると、ユーザーは提出データを送信するようにグループ内のクライアントを設定できません。オプションを有効にして提出タイプを選択し、設定をロックすると、ユーザーは提出を無効にできません。設定をロックしなければ、[詳細] の提出タイプなどの設定を変更できます。

シマンテック社が最良の脅威防止を提供できるように、脅威の情報の提出をお願いします。

よく寄せられる質問

Symantec Endpoint Protection ではどのような種類の情報が収集されますか？

[プライバシーとデータ保護](#)

Symantec Endpoint Protection が収集する情報の種類について詳しくは、以下の表に示します。

Table 112: Symantec Endpoint Protection が収集する情報の種類の詳細

次のように入力します。	詳細
ソフトウェアの設定、製品の詳細、インストールの状態	ウイルスとスパイウェアの対策ポリシーに関する情報には次のものが含まれます。 • Bloodhound の設定 Bloodhound が有効または無効のどちらか。レベルが自動またはアグレッシブのどちらか。 ([ウイルスとスパイウェアの対策ポリシー] > [グローバルスキャンオプション]) • ダウンロードインサイトの設定 ダウンロードインサイトが有効または無効のどちらか。感度や普及率のしきい値など、ダウンロードインサイトの設定。([ウイルスとスパイウェアの対策ポリシー] > [ダウンロード保護]) • 自動保護の設定 マルウェアやセキュリティリスクに設定している上書き ([ウイルスとスパイウェアの対策ポリシー] > [自動保護]) クライアントの台数が多い上位 20 位のグループに関する情報を含みます。各グループの 1 番目の場所 (通常はデフォルトの場所) を選択して情報を送信します。 通常、この情報には次のものが含まれます。 • クライアントモード: クライアントでサーバー制御、クライアント制御、混合モードを使用しているか。データが見つからないか。 • プッシュ型/プル型転送モード: クライアントがサーバーからポリシーを取得しているか。サーバーにポリシーを要求しているか。 • アプリケーション学習のオン/オフ。 • ハートビート間隔 (分)。 • 重要なイベントのアップロードのオン/オフ。 • ダウンロードのランダム化のオン/オフ。ランダム化の時間帯 (分)。 • クライアントで前回使用したグループ設定やグループモードを使用しているか。 • クライアントが検出の提出データを送信しているか。ウイルス対策の検出、ファイル評価、SONAR など、提出データの種類。 • クライアントでホストインテグリティを有効にしているか。 • ドメインの数。 • ドメインすべてのグループの合計数は、<1500 のように近似値で表示されます。3,000 以上の場合、>= 3000 と送信される • すべてのドメインにおけるグループの最大深度 • クライアントの合計数 • コンピュータモードのクライアントの台数 • ユーザーモードのクライアントの台数 • 組織単位 (OU) グループのクライアントの台数
ライセンスの状態、ライセンスの資格情報、ライセンス ID、ライセンスの使用状況	なし
デバイス名、種類、OS バージョン、言語、場所、ブラウザの種類とバージョン、IP アドレス、ID	なし
デバイスのハードウェア、ソフトウェア、アプリケーションインベントリ	サーバーデータベースからは、クライアントのハードウェアに関する集計情報を送信します。情報には、CPU、RAM、Symantec Endpoint Protection インストールディスクのディスク空き容量が含まれます。

次のように入力します。	詳細
アプリケーションとデータベースのアクセス設定、ポリシーの必要条件、ポリシーコンプライアンスの状態、アプリケーション例外、ワークフローのエラーログ	システム管理ログのエントリのルール数を含みます。次のデータベースログのログエントリ数、ログエントリが期限切れになるまでの日数も送信します。 - システム管理ログ - クライアント/サーバー活動ログ - 監査ログ - システムサーバー活動ログ 複製エラーやデータベースバージョンの不一致など、サーバーの複製エラーイベントを含みます。
クライアントのセキュリティイベント情報、IP アドレス、ユーザー ID、パス、デバイス名やデバイスの状態などのデバイス情報、ダウンロードしたファイル、ファイルの処理など、潜在的な脅威に関連付けられた情報	なし
ファイルのダウンロード、処理や実行アプリケーションの情報、マルウェアの送信など、ファイルやアプリケーションの評価情報	ファイル評価データとは、評価に基づいて検出したファイルに関する情報です。 これらの情報を提出すると Symantec Insight 評価データベースに反映され、コンピュータを新たなリスクから保護するための役に立ちます。 情報には、ファイルハッシュ、クライアントの IP ハッシュ、ファイルのダウンロード元の IP アドレス、ファイルサイズ、ファイルの評価スコアが含まれます。
アプリケーション例外のログとワークフローのエラーログ	なし
サービスの設定時に入力した個人情報や、設定後の他のサービス呼び出し	なし
名前、バージョン、言語、ライセンスの資格データなどのライセンス情報	なし
SEP に装備されている保護技術の使用状況	クライアントの台数が多い上位 20 位のグループに関する情報を含みます。各グループの 1 番目の場所（通常はデフォルトの場所）を選択して情報を送信します。 この情報には、次のものが含まれます。 - 特定の保護技術が有効または無効になっているクライアントの台数。 - 有効になっている保護技術を使った 1 番目の検出処理と 2 番目の検出処理の数と種類（検疫、ログのみ、クリーン、など）。 つの Symantec Endpoint Protection Manager はデータベースにおける各種の共有ポリシーの数を送信します。この数は、デフォルトのポリシーとカスタムのポリシーの数を足したものです。この情報には、次のものが含まれます。 - ドメインの数 - 次の共有ポリシーそれぞれの数 - ウイルスとスパイウェアの対策ポリシー - ファイアウォールポリシー - 侵入防止ポリシー - アプリケーションとデバイス制御ポリシー - LiveUpdate のポリシー - ホストインテグリティポリシー - カスタム侵入防止シグネチャの数

次のように入力します。	詳細
オペレーティングシステム情報、サーバーハードウェアとソフトウェアの設定の詳細、CPU 名、メモリサイズ、インストール済みパッケージのソフトウェアバージョンと機能など、SEP の設定を記述した情報	以下のサーバー情報を含みます。 - 複製パートナーの数 - ログデータの複製の有無 - コンテンツデータの複製の有無 Linux オペレーティングシステムの種類、カーネルバージョン、この設定を適用しているクライアントの台数を含みます。 次のクライアントの台数など、つの Symantec Endpoint Protection Manager クライアントの稼働状態に関する Symantec Endpoint Protection データベースの集計情報を含みます。 - クライアントの合計数 - 縮小サイズのクライアント - 標準サイズのクライアント - EFW 対応クライアント - FBWF 対応クライアント - UFW 対応クライアント - Microsoft 社のハイパーバイザクライアント - VMware 社のハイパーバイザクライアント - Citrix 社のハイパーバイザクライアント - 不明なハイパーバイザクライアント LiveUpdate のリビジョンの概数 (<30 など) を送信します。
潜在的なセキュリティリスク、移植可能な実行可能ファイルや実行可能コンテンツを含むファイル (インストール時にこのようなファイルが実行する処理に関する情報など、個人情報を含む可能性があり、マルウェアとして識別される) の情報	- ウイルス対策の検出 (Windows と Mac のみ) ウイルスとスパイウェアスキャンの検出についての情報。クライアントが提出する情報には、ファイルハッシュ、クライアント IP のハッシュ、ウイルス対策シグネチャ、攻撃者の URL などが含まれます。 - ウイルス対策の拡張ヒューリスティック検出 (Windows のみ) Bloodhound やその他のウイルスとスパイウェアのスキャンでヒューリスティックに検出された潜在的な脅威に関する情報。これらの検出は、リスクログに表示されないサイレントな検出です。これらの検出についての情報は統計分析のために使われます。 - SONAR 検出 (Windows のみ) 危険度が高い検出や危険度が低い検出、システム変更イベント、信頼できるアプリケーションによる疑わしい動作などの、SONAR が検出する脅威についての情報。 次のような処理データも含みます。 - SONAR のヒューリスティック検出 (Windows のみ) は、リスクログに表示されないサイレントな検出です。この情報は統計分析のために使われます。クライアントが通常提出する情報の種類には、次のような検出の属性が含まれます - 非表示の処理 - 占有域が少ない処理 - キー入力のログ記録や画面のキャプチャ動作 - セキュリティ製品の動作の無効化 - 検出の日付とタイムスタンプ

次のように入力します。	詳細
アクセスした URL を含むネットワーク活動に関する情報、ネットワーク接続に関する集計情報（ネットワーク接続に使用したホスト名、IP アドレス、統計情報など）	次の情報を含みます。 - ネットワーク検出イベント（Windows と Mac のみ） IPS エンジンによる検出（侵入防止）に関する情報。クライアントが提出する情報には、クライアント IP のハッシュ、攻撃者の URL、検出のタイムスタンプ、攻撃者の IP アドレス、IPS シグネチャなどが含まれます。 - ブラウザ検出イベント（Windows のみ） ブラウザのアドレスバーに入力したすべての URL とダウンロードするためにクリックまたは接続したすべての URL。 クライアントは、以下に関するメタデータも送信します。 - IP アドレス、ポート番号、ホスト名、接続を初期化するアプリケーション、プロトコル、接続時間、接続ごとのバイト数など、各ネットワーク接続 - デバイス ID、転送時間、プロトコル、ファイル属性（種類、名前、パス、サイズ）、コンテンツの SHA-256 など、デバイス間のすべてのファイル転送活動
SEP のインストールと動作に関する状態情報（インストール時またはエラー発生時に SEP が検出したファイルまたはフォルダの名前に個人情報が含まれている場合にのみ、状態情報に個人情報が含まれることがあります。状態情報には、SEP のインストールが正常に完了したかどうかや、SEP でエラーが発生したかどうかを示されます）	なし
匿名の一般的な統計情報と状態情報	なし

自分の **Symantec Endpoint Protection** クライアントが送信している遠隔測定 of 提出データはどのようにしたらわかりますか？

提出イベントを確認するには、クライアント活動ログを調べます。ログに最新の提出イベントが記録されていない場合は、次のことを調べます。

- クライアントによるデータ提出が有効であることを確認する
- プロキシサーバーを使用している場合は、プロキシ例外を調べる「[クライアントがデータを提出する場合に使用するプロキシサーバーは指定できますか？](#)」を参照してください。
- シマンテック社のサーバーの接続を調べる次のナレッジベースの記事 https://support.symantec.com/en_US/article.TECH163042.html を参照してください。
- クライアントに最新の LiveUpdate コンテンツをダウンロードしていることを確認する
Symantec Endpoint Protection で SCD (Submission Control Data) ファイルを使用しています。シマンテック社では SCD ファイルを発行し、それを LiveUpdate パッケージの一部として含めます。各シマンテック製品には独自の SCD ファイルが含まれます。このファイルは次の設定を制御します。
 - クライアントが 1 日に提出できる回数
 - クライアントソフトウェアが提出を再試行するまでの待機時間の長さ
 - 失敗した提出を再試行する回数
 - 提出データを受信するシマンテックセキュリティレスポンスサーバーの IP アドレス

SCD ファイルが期限切れになった場合には、クライアントは提出データの送信を停止します。シマンテック社は、クライアントコンピュータが 7 日間 LiveUpdate コンテンツを取得しなければ SCD ファイルが期限切れになったと見なします。クライアントは 14 日後に提出の送信を停止します。

クライアントが提出を停止した場合は、クライアントソフトウェアは提出情報を収集せずに後で送信します。クライアントが提出を再び開始するときは、再開された後に発生したイベントに関する情報のみが送信されます。

遠隔測定 of データ提出を断ることはできますか？

はい。断ることができます。クライアントとサーバーのユーザーインターフェースでサーバーデータの収集オプションやクライアントのデータ提出オプションを修正できます。ただし、シマンテック社はネットワークのセキュリティ向上を可能にする程度の遠隔測定を有効にすることを推奨します。

パフォーマンス、サイジング、および配備

遠隔測定では帯域幅をどれくらい使用しますか？

Symantec Endpoint Protection は、クライアントコンピュータによるデータ提出を調整してネットワークへの影響を最小限に抑えます。Symantec Endpoint Protection は、次の方法で提出を調整します

- クライアントコンピュータはコンピュータがアイドル状態のときだけサンプルを送信します。アイドル状態の提出は、ネットワーク上の提出トラフィックをランダム化するのに役立ちます。
- クライアントコンピュータは、一意のファイルについてのみサンプルを送信します。シマンテック社ですでにファイルを認識している場合、クライアントコンピュータは情報を送信しません。

NOTE

これらの提出データは非常に小さいサイズです。たとえば、ウイルス対策の提出データは通常 4 KB を超えません。同様の IPS の提出データは約 32 KB です。

クライアントがデータを提出する場合に使用するプロキシサーバーは指定できますか？

Windows クライアントが提出とその他の外部通信にプロキシサーバーを使うように、つの Symantec Endpoint Protection Manager を設定できます。クライアントコンピュータで認証にプロキシを使う場合、プロキシサーバーの設定でシマンテック社の URL を例外として指定することが必要になる場合があります。例外により、クライアントコンピュータは Symantec Insight と他の重要なシマンテック社のサイトと通信できます。

プロキシについて詳しくは、以下を参照してください。

[クライアントの提出と他の外部通信のためのプロキシサーバーの指定](#)

シマンテック社の URL の例外について詳しくは、次のサイトを参照してください。

https://support.symantec.com/en_US/article.TECH162286.html

サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について

デフォルトで、Symantec Endpoint Protection クライアントと 一つの Symantec Endpoint Protection Manager では一部の種類の匿名情報がシマンテック社に送信されます。クライアントは、非匿名データをシマンテック社に送信して、カスタマイズされた分析を得ることができます。クライアントまたは 一つの Symantec Endpoint Protection Manager が情報を提出するかどうかを制御できます。

サーバーデータとクライアント提出はいずれもネットワークのセキュリティの向上において重要な意味を持ちます。

[サーバーデータ収集とは](#)

[匿名のクライアント提出とは](#)

[非匿名のクライアント提出とは \(Windows のみ \)](#)

[プライバシーに関する考慮事項](#)

[帯域幅の使用状況に関する考慮事項](#)

[サーバーデータ収集とは](#)

サーバーデータは、シマンテック社が検出技術の対策とその効率向上を実現するのに役立ちます。

つの **Symantec Endpoint Protection Manager** は、次の種類の匿名情報をシマンテック社に送信します。

- 名前、バージョン、言語、ライセンス資格データを含むライセンス情報
- Symantec Endpoint Protection 保護機能の使用状況
- Symantec Endpoint Protection 設定に関する情報この情報には、オペレーティングシステム情報、サーバーハードウェアとソフトウェアの設定、CPU サイズ、メモリサイズ、インストール済みパッケージのソフトウェアバージョンと機能が含まれます。

インストール時にサーバー提出設定を変更する、またはコンソールでサーバーの [サイトプロパティ]、[データ収集] タブで設定を変更できます。

NOTE

シマンテック社は、サーバーデータ収集を有効のままにしておくことを常に推奨します。

匿名のクライアント提出とは

Symantec Endpoint Protection クライアントは検出、ネットワーク、設定についての匿名情報をシマンテックセキュリティレスポンスに自動的に提出します。シマンテック社は、この匿名情報を使って新しい脅威と変化する脅威に対応すると同時に製品のパフォーマンスの向上に役立てます。匿名データが特定のユーザーに直接識別されることはありません。

クライアントが送信する検出情報には、ウイルス対策検出、侵入防止、SONAR、ファイル評価検出に関する情報が含まれます。

NOTE

Mac クライアント提出には SONAR またはファイル評価の提出が含まれません。Linux クライアントはいかなるクライアント提出もサポートしません。

クライアントがシマンテック社に送信する匿名情報により、ユーザーは次の恩恵を受けることができます。

- ネットワークのセキュリティの向上
- 製品パフォーマンスの最適化

ただし、場合によっては、クライアントが一部の情報を提出することを防止する必要があります。たとえば、企業のポリシーで、クライアントコンピュータが社外のエンティティにいかなるネットワーク情報も送信できないようにする場合があります。すべての種類のクライアント提出を無効にするのではなく、ネットワーク情報などの 1 つの種類の提出を無効にすることができます。

NOTE

シマンテック社はこのオプションを常に有効のままにしておくことを推奨します。提出を無効にすることにより、お客様の組織で排他的に使われているアプリケーションの誤認検出をすばやく解決できなくなる場合があります。組織で発生したマルウェアに関する情報がないと、脅威に対する製品の対応とシマンテック社による対応に長い時間がかかる場合があります。

[クライアントがシマンテック社に送信する匿名または非匿名のデータの管理](#)

[Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法](#)

非匿名のクライアント提出とは

シマンテック社に非匿名のクライアント情報を提出することを選択できます。この種類の情報は、セキュリティの課題に対する洞察を提供し、シマンテック社がカスタマイズしたソリューションを推奨する上で役に立ちます。

- カスタム分析を提供できるシマンテック社出資のプログラムに参加している場合にのみこのオプションを使います。
- このオプションはデフォルトで無効です。

[クライアントがシマンテック社に送信する匿名または非匿名のデータの管理](#)

プライバシーに関する考慮事項

シマンテック社は、クライアント提出データを匿名化するためのすべての手段を実施しています。

- 疑わしい実行可能ファイルのみが提出されます。
- ユーザー名はパス名から削除されます。
- コンピュータとエンタープライズは固有かつ匿名の値で識別されます。
- IP アドレスは、地理的場所のために使われ、使用後に破棄されます。

プライバシーについて詳しくは、次のドキュメントを参照してください。

[プライバシーに関する声明](#)

帯域幅の使用状況に関する考慮事項

Symantec Endpoint Protection は、ネットワーク帯域幅に対するクライアント提出の影響を最小限に抑えます。

クライアント活動ログを調べてクライアントコンピュータが送信する提出の種類を確認したり、帯域幅の使用状況を監視することができます。

[Symantec Endpoint Protection で、クライアントの提出がネットワーク帯域幅に与える影響を最小化する方法 ログの表示](#)

クライアントがシマンテック社に送信する匿名または非匿名のデータの管理

Symantec Endpoint Protection は、検出についての匿名情報をシマンテック社に提出することで、コンピュータを保護できます。シマンテック社は、この情報を使って新しい脅威や変化する脅威に対応します。提出されるデータは、シマンテック社がコンピュータに対する脅威に対処して対策をカスタマイズするために役立ちます。シマンテック社では、可能な限り多くの検出情報を提出することを推奨しています。

[サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について](#)

クライアントコンピュータは検出についての情報を匿名で提出します。どの検出タイプに対してクライアントから情報を提出するかを指定できます。シマンテック社が遠隔測定によって収集したデータには、直接的には識別できない匿名要素が含まれている場合があります。シマンテック社は個人ユーザーを特定するために遠隔測定データの使用を必要としたり求めたりすることはありません。

NOTE

Mac クライアント提出には SONAR またはファイル評価の提出が含まれません。Linux クライアントはいかなるクライアント提出もサポートしません。

クライアント提出の設定を変更するには

1. コンソールで、[クライアント] を選択し、[ポリシー] タブをクリックします。
2. [設定] ペインで、[外部通信の設定] をクリックします。
3. [クライアント提出] タブをクリックします。
4. [匿名のデータをシマンテック社に送信して詳細な脅威防止インテリジェンスを受け取る] オプションを有効または無効にします。
5. ファイル評価などの特定の提出の種類を有効または無効にするには、[詳細] を選択します。
6. シマンテック社出資のカスタム分析プログラムに参加している場合は、[カスタム分析のために、クライアントが特定できるデータをシマンテック社に送信する] を選択します。

WARNING

このオプションは非匿名の情報をシマンテック社に送信します。シマンテック社出資のプログラムに参加しており、クライアントの識別が可能なデータをシマンテック社と共有する場合にのみ、このオプションを使います。

7. [OK] を選択します。

NOTE

Mac クライアントでは IPS ping 送信を無効にすることもできます。次の記事を参照してください。

[Symantec Endpoint Protectionでの Mac クライアント用 IPS データ提出を無効にする方法](#)

Symantec Endpoint Protection で、クライアントの提出がネットワーク帯域幅に与える影響を最小化する方法

Symantec Endpoint Protection は、クライアントコンピュータの提出を調整することで、ネットワークへの影響を最小限に抑えます。Symantec Endpoint Protection は、次のように提出を調整します。

- クライアントコンピュータはコンピュータがアイドル状態のときだけサンプルを送信します。アイドル状態の提出は、ネットワーク上の提出トラフィックをランダム化するのに役立ちます。
- クライアントコンピュータは、一意のファイルについてのみサンプルを送信します。シマンテック社ですでにファイルを認識している場合、クライアントコンピュータは情報を送信しません。
- Symantec Endpoint Protection は、SCD (提出制御データ) ファイルを使います。シマンテック社では SCD ファイルを発行し、それを LiveUpdate パッケージの一部として含めます。各シマンテック製品には独自の SCD ファイルが含まれます。

このファイルは次の設定を制御します。

- クライアントが 1 日に提出できる回数
- クライアントソフトウェアが提出を再試行するまでの待機時間の長さ
- 失敗した提出を再試行する回数
- 提出を受信するシマンテックセキュリティレスポンスサーバーの IP アドレス

SCD ファイルが期限切れになった場合は、クライアントは提出の送信を停止します。シマンテック社ではクライアントコンピュータが 7 日間 LiveUpdate コンテンツを取得しなければ SCD ファイルが期限切れになったと見なします。クライアントは 14 日後に提出の送信を停止します。

クライアントが提出を停止した場合は、クライアントソフトウェアは提出情報を収集せずに後で送信します。クライアントが提出を再び開始するときは、再開された後に発生したイベントに関する情報のみが送信されます。

[サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について](#)

クライアントの提出と他の外部通信のためのプロキシサーバーの指定

Windows クライアントが提出と他の外部通信のためにプロキシサーバーを使うように、つの Symantec Endpoint Protection Manager を設定できます。

NOTE

クライアントコンピュータで認証にプロキシを使う場合、プロキシサーバーの設定でシマンテック社の URL を例外として指定することが必要になる場合があります。例外により、クライアントコンピュータは Symantec Insight と他の重要なシマンテック社のサイトと通信できます。

次のプロキシ設定オプションを使用する場合、プロキシサーバーの設定にシマンテック URL の例外を含める必要があります。

- 認証にプロキシサーバーを使用します。
- 一つの Symantec Endpoint Protection Manager の [外部通信 (External Communication)] ダイアログで [クライアントブラウザで指定されたプロキシサーバーを使う (Use a proxy server specified by my client browser)] オプションを選択します。
- ブラウザのインターネットオプションで自動検出または自動設定を使用します。

自動検出または自動設定を使用しない場合、プロキシサーバーの設定でシマンテック社の URL を例外として指定する必要があります。[外部通信 (External Communication)] ダイアログで [カスタムプロキシ設定を使う] を選択してから、認証設定を指定する必要があります。

クライアントの提出と他の外部通信のためのプロキシサーバーを指定するには

1. コンソールの [クライアント] ページで、グループを選択し、[ポリシー] をクリックします。
2. [設定] または [場所固有の設定] で、[外部通信] をクリックします。
3. [プロキシサーバー (Windows)] タブの [HTTPS プロキシの設定] で、[カスタムプロキシ設定を使う] を選択します。
4. クライアントが使うプロキシサーバーについての情報を入力します。オプションについて詳しくは、オンラインヘルプを参照してください。
5. [OK] をクリックします。

推奨される例外については、次の記事を参照してください。

- [ライセンスサーバーやダウンロードインサイトサーバーへの接続をテストする方法](#)
- [SEP で Symantec のレピュテーションサーバーおよびライセンシングサーバーと通信するために推奨されるプロキシサーバーの Web ドメイン除外指定について](#)

[サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について](#)

[ウイルスとスパイウェアのスキンの例外作成](#)

SONAR の管理

SONAR はクライアントコンピュータに対するプロアクティブ脅威防止と、つの Symantec Endpoint Protection Manager のウイルスとスパイウェアの対策ポリシーの一部です。

Table 113: SONAR の管理

タスク	説明
SONAR の動作について学習する	SONAR が不明な脅威をどのように検出するかについて学習します。SONAR の動作方法についての情報は、セキュリティネットワークでの SONAR の使用法について決定を下す助けになります。 SONAR について
SONAR が有効になっていることを確認する	クライアントコンピュータに最大限の保護を提供するには、SONAR を有効にする必要があります。SONAR は、その他いくつかの Symantec Endpoint Protection の機能と相互動作します。SONAR には Auto-Protect が必要です。 [◎クライアント◎] タブを使って、クライアントコンピュータでプロアクティブ脅威防止が有効になっているかどうかを確認できます。 クライアントコンピュータでの SONAR 設定の調整
SONAR のデフォルト設定を確認する	SONAR の設定は、ウイルスとスパイウェアの対策ポリシーの一部です。 デフォルトのウイルスとスパイウェアの対策ポリシーのスキニング設定について
Insight ルックアップが有効になっていることを確認する	SONAR はヒューリスティックに加えて評価データを使って検出を行います。Insight ルックアップを無効にすると、SONAR はヒューリスティックのみを使って検出を行います。誤認の比率が増える可能性があり、SONAR が提供する保護は限られたものになります。 [提出] ダイアログボックスで、Insight ルックアップを有効または無効にできます。 サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について

タスク	説明
誤認検出をチェックするために SONAR イベントを監視する	SONAR ログを使ってイベントを監視できます。 [リスクレポート] で SONAR の検出結果レポートを表示して、検出の情報を参照することもできます。 SONAR 検出結果の監視による誤認のチェック エンドポイント保護の監視
SONAR の設定を調整する	SONAR が検出する一部の種類の脅威については、検出処理を変更できます。誤認検出を減らすために、検出処理を変更したい場合があります。 また、ヒューリスティック検出の危険度の高低に応じて通知の有効と無効を切り替えたいことがあります。 クライアントコンピュータでの SONAR 設定の調整 SONAR の誤検知の検出の処理と防止
安全だとわかっているアプリケーションを SONAR が検出しないようにする	クライアントコンピュータで実行したいアプリケーションやファイルが SONAR によって検出されることがあります。例外ポリシーを使って、許可したい特定のファイル、フォルダ、またはアプリケーションのために例外を指定できます。SONAR が検疫した項目の場合は、SONAR ログから検疫項目の例外を作成できます。 検出をログに記録して許可するように、SONAR の処理を設定したい場合もあります。アプリケーション学習を利用すれば、Symantec Endpoint Protection がクライアントコンピュータの正当なアプリケーションを学習するようにできます。ネットワークで使うアプリケーションを Symantec Endpoint Protection が学習した後で、検疫する SONAR の処理を変更できます。 Note: 危険度が高い検出の処理をログに記録するだけに設定すると、クライアントコンピュータで潜在的な脅威を許容することになります。 SONAR の誤検知の検出の処理と防止
一部のアプリケーションを SONAR が検出しないようにする	検査のために SONAR がアプリケーションにコードを挿入するときに、アプリケーションが不安定になったり実行できなくなる場合があります。アプリケーション用にファイル、フォルダ、またはアプリケーションの例外を作成できます。 ウイルスとスパイウェアのスキャンの例外作成
DNS またはホストファイルを変更するアプリケーションを SONAR が検出する方法を管理する	SONAR のポリシー設定を使って、SONAR が検出した DNS またはホストファイルの変更を処理する方法をグローバルに調整できます。例外ポリシーを使って、特定のアプリケーションのための例外を設定できます。 クライアントコンピュータでの SONAR 設定の調整 DNS またはホストファイルを変更するアプリケーションのための例外の作成
SONAR 検出についての情報をシマンテック社に提出することをクライアントが許可する	シマンテック社はクライアントコンピュータで提出を有効にすることを推奨します。クライアントが検出について提出する情報は、シマンテック社が脅威に対応する助けになります。この情報によってシマンテック社はより優れたヒューリスティックを作成でき、誤認検出が減ることになります。 サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について

SONAR について

SONAR は、潜在的に悪質なアプリケーションがコンピュータで実行されたときにそれらを検出するリアルタイム保護です。SONAR は、脅威に対応するために従来のウイルスやスパイウェアの検出定義が作成される前に脅威を検出するため、「ゼロデイ」対策となります。

SONAR はヒューリスティックに加えて評価データを使って、広がりつつある未知の脅威を検出します。SONAR はクライアントコンピュータで保護のレベルを追加し、既存のウイルスとスパイウェアの対策、侵入防止、メモリエクスプロイト緩和機能、ファイアウォール保護を補います。

SONAR は、クライアントコンピュータでローカルに行うプロアクティブな監視とともに、シマンテック社のオンラインインテリジェンスネットワークを利用するヒューリスティックシステムを使って、広がりつつある脅威を検出します。SONAR は監視する必要があるクライアントコンピュータで変更や動作も検出します。

NOTE

Auto-Protect も、Bloodhound と呼ばれるヒューリスティックの 1 種類を使ってファイル内の疑わしい動作を検出します。

SONAR は、Windows のユーザーモードで実行されるアプリケーションにコードを挿入して、それらのアプリケーションの疑わしい活動を監視します。場合によっては、挿入がアプリケーションのパフォーマンスに影響したり、アプリケーションの実行に問題を起こすことがあります。ファイル、フォルダ、またはアプリケーションをこの種類の監視から除外するための例外を作成できます。

SONAR は、アプリケーションの種類に対してではなく、処理の動作方法について検出を行います。SONAR はアプリケーションが悪質な動作を行う場合にのみ、アプリケーションの種類とは無関係に、そのアプリケーションに対してのみ作用します。たとえば、トロイの木馬やキーロガーが悪質な動作を行わない場合、SONAR では検出されません。

SONAR は以下の項目を検出します。

ヒューリスティック脅威	SONAR はヒューリスティックを使って、不明なファイルが不審な動作をしているかどうかと、ファイルの危険度が高いか低いかを判断します。また、評価データを使って、脅威の危険度が高いか低いかを判断します。
システムの変更	SONAR はクライアントコンピュータで DNS 設定やホストファイルの修正を試みるアプリケーションやファイルを検出します。
不適切な動作を示している信頼できるアプリケーション	適切で信頼できるファイルの一部が、疑わしい動作と関連付けられることがあります。SONAR はこれらのファイルを、疑わしい動作のイベントとして検出します。たとえば、よく知られた文書共有アプリケーションが実行可能ファイルを作成することがあります。

Auto-Protect を無効にすれば、高く、危険度が低いファイルの検出をする SONAR の能力を限定します。Insight ルックアップ (評価クエリー) を無効にすると、SONAR の検出機能も制限することになります。

SONAR の管理

Symantec Endpoint Protection の例外の管理

コンピュータでの SONAR の管理

スキャンからの項目の除外

SONAR の誤検知の検出の処理と防止

SONAR は特定の社内カスタムアプリケーションについて誤認検出を行う場合があります。また、Insight ルックアップを無効にすると、SONAR からの誤認数が増加します。

サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について

誤認検出全般を減らすために SONAR 設定を変更できます。SONAR で誤認検出される特定のファイルまたはアプリケーションの例外を作成することもできます。

WARNING

危険度が高い検出の処理をログに記録するだけに設定すると、クライアントコンピュータで潜在的な脅威を許容することになります。

Table 114: SONAR の誤認の処理

タスク	説明
SONAR の高危険度のヒューリスティック検出をログに記録し、アプリケーション学習を使う	高危険度のヒューリスティック検出の検出処理を、短い期間 [ログ] に設定することを推奨します。同じ期間にアプリケーション学習が実行されるようにします。Symantec Endpoint Protection はネットワーク内で実行されている正当なプロセスを学習します。ただし、一部の本当の検出が検疫されない可能性があります。 クライアントコンピュータで実行するアプリケーションに関する情報の収集 この期間後は、検出の処理を [検疫] に設定し直す必要があります。 Note: 低危険度のヒューリスティック検出に拡張モードを使っている場合、誤認検出の確率が高くなっています。拡張モードはデフォルトでは無効になっています。 クライアントコンピュータでの SONAR 設定の調整
SONAR の例外を作成して安全なアプリケーションを許可する	SONAR の例外は次の方法で作成できます。 - SONAR ログを使って、検出と検疫が行われたアプリケーションの例外を作成します。SONAR ログから誤認検出の例外を作成できます。項目が検疫された場合、Symantec Endpoint Protection は検疫内で項目を再スキャンした後にその項目を復元します。検疫にある項目は、更新された定義をクライアントが受信した後に再スキャンされます。 ログイベントに基づく例外の作成 コンピュータでの検疫ファイルの管理 - 例外ポリシーを使って、特定のファイル名、フォルダ名、またはアプリケーションの例外を指定します。 SONAR 検出からフォルダ全体を除外できます。カスタムアプリケーションが存在するフォルダは除外することを推奨します。 ウイルスとスパイウェアのスキャンの例外作成

クライアントコンピュータでの SONAR 設定の調整

誤検知の比率を下げるために、SONAR の処理を変更したい場合があります。クライアントコンピュータに表示される検出通知の数を変えるため、SONAR の処理を変更したい場合もあります。

NOTE

このドメインがクラウドコンソールに登録されると、クラウドアイコンが一部のオプションの横に表示されます。集中保護ポリシーが有効になっている場合、ポリシーによりこれらのオプションが 14.0.1 クライアントに対してのみ上書きされます。

クライアントコンピュータで SONAR 設定を調整するには

1. ウイルスとスパイウェアの対策ポリシーで、[SONAR] を選択します。
2. [SONAR を有効にする] にチェックマークを付けていることを確認します。

NOTE

SONAR が有効になると、[疑わしい動作の検出] が自動的にオンになります。SONAR が有効である場合、[疑わしい動作の検出] をオフにすることはできません。

3. [スキャンの詳細] で、高危険度または低危険度のヒューリスティック脅威の処理を変更します。

低危険度検出の拡張モードを有効にできます。この設定では、低危険度検出に対する SONAR の感度を高めます。誤認検出が増加する可能性があります。

- オプションで、クライアントコンピュータに表示される通知の設定を変更します。
- [システム変更イベント] で、[DNS 変更の検出] または [ホストファイル変更の検出] の処理を変更します。

NOTE

[確認する] の処理により、クライアントコンピュータに多数の通知が表示される可能性があります。[無視] 以外のどの処理でも、コンソールに多数のログイベントが表示され、管理者に電子メール通知が送信される可能性があります。

WARNING

処理を [遮断] に設定した場合、クライアントコンピュータ上の重要なアプリケーションを遮断できます。

たとえば、[DNS 変更の検出] の処理を [遮断] に設定すると、VPN クライアントが遮断される可能性があります。[ホストファイル変更の検出] の処理を [遮断] に設定すると、ホストファイルにアクセスする必要があるアプリケーションが遮断される可能性があります。DNS またはホストファイルの変更の例外を使うと、特定のアプリケーションに DNS またはホストファイルの変更を許可できます。

DNS またはホストファイルを変更するアプリケーションのための例外の作成

- [疑わしい動作の検出] で、高リスクまたは低リスクの検出の処理を変更できます。
SONAR が無効の場合、[疑わしい動作の検出] の有効と無効を切り替えることもできます。
- [OK] をクリックします。

SONAR の管理

ウイルスとスパイウェアのスキンの例外作成

SONAR 検出結果の監視による誤認のチェック

クライアントは、SONAR 検出結果を収集し、管理サーバーにアップロードします。結果は SONAR ログに保存されます。

どの処理が正当であるか、どれがセキュリティリスクであるかを判断するには、ログ内の次の列を調べます。

イベント	イベントの種類と、クリーニングしたりログ記録するなどクライアントがプロセスで行う処理。次のイベントの種類を調べます。 - 考えられる正当なプロセスは、[潜在的なリスクが見つかりました] イベントとしてリストされています。 - 推定されるセキュリティリスクは、[セキュリティリスクが見つかりました] イベントとしてリストされています。
アプリケーション	プロセス名。
アプリケーションの種類	SONAR スキャンが検出したマルウェアの種類。
ファイル/パス	プロセスが開始された場所からのパス名。

[イベント] 列を見ると、検出されたプロセスがセキュリティリスクか、可能性のある正当なプロセスであるかが、すぐにわかります。ただし、検出された潜在的なリスクが正当なプロセスである場合もない場合もあります。また、検出されたセキュリティリスクが悪意のあるプロセスである場合もない場合もあります。したがって、詳細については、[アプリケーションの種類] 列と [ファイル/パス] 列を調べる必要があります。たとえば、サードパーティ企業が開発した正当なアプリケーションのアプリケーション名を認識できます。

誤認を確認するために SONAR 検出結果を監視するには

-
1. コンソールで、[監視]、[ログ] の順にクリックします。
 2. [ログ] タブの [ログの種類] ドロップダウンリストで、[SONAR] をクリックします。
 3. [時間範囲] リストボックスから、スキャン設定を最後に変更した時点に最も近い時間を選択します。
 4. [追加設定] をクリックします。
12.1.xでは、[追加設定] ではなく [拡張設定] です。
 5. [イベントの種類] ドロップダウンリストで、次のログイベントのいずれかを選択します。
 - 検出されたすべてのプロセスを表示するには、必ず [すべて] を選択します。
 - セキュリティリスクとして評価されているプロセスを表示するには、[セキュリティリスクが見つかりました] をクリックします。
 - 潜在的なリスクとして評価され、ログ記録されているプロセスを表示するには、[潜在的なリスクが見つかりました] をクリックします。
 6. [ログの表示] をクリックします。
 7. 正当なアプリケーションとセキュリティリスクを識別した後、例外ポリシーでそれらの例外を作成します。
直接、[SONAR ログ] ペインから例外を作成できます。

ログイベントに基づく例外の作成

改変対策の設定の変更

改変対策は、サーバーとクライアントで実行されるシマンテック製アプリケーションにリアルタイム保護を提供します。ワーム、トロイの木馬、ウイルスなどのシマンテック製品以外のプロセスが、シマンテック製品のリソースに影響を与えることがないようにします。クライアントを設定して、シマンテック製品のリソースを変更しようとする試みを遮断するか、またはログに記録することができます。改変対策が検出するアプリケーションの例外を作成できます。

改変対策の設定は、選択したグループに対してグローバルに設定されます。

改変対策の設定を変更するには

1. コンソールで、[クライアント] をクリックします。
2. [ポリシー] タブの [設定] で、[全般の設定] をクリックします。
3. [改変対策] タブで、[シマンテック製セキュリティソフトウェアを改変または終了から保護する] にチェックマークを付けるかはずします。
4. [アプリケーションがシマンテック製セキュリティソフトウェアを改変または終了しようとした場合に適用する処理] のリストボックスで、いずれかのログ処理を選択します。
5. [OK] をクリックします。

Windows クライアントの改変対策例外の作成

アプリケーション制御、システムロックダウン、デバイス制御について

クライアントコンピュータ上のアプリケーションの動作を監視、制御するには、アプリケーション制御とシステムロックダウンを使います。アプリケーション制御は、クライアントコンピュータのシステムリソースにアクセスを試みる定義済みのアプリケーションを許可または遮断します。システムロックダウンは、クライアントコンピュータの承認済みアプリケーションのみを許可します。クライアントコンピュータにアクセスするハードウェアデバイスを管理するには、Device Control を使います。

WARNING

アプリケーション制御とシステムロックダウンは高度なセキュリティ機能であるため、経験のある管理者だけが設定してください。

次のタスクでアプリケーション制御、システムロックダウン、デバイス制御を使います。

アプリケーション制御	- マルウェアがアプリケーションを占有できないようにする - 実行できるアプリケーションを制限する - ユーザーが設定ファイルを変更できないようにする - 特定のレジストリキーを保護する \\WINDOWS\system のような特定のフォルダを保護する アプリケーションとデバイス制御ポリシーを使って、アプリケーション制御とデバイス制御を設定します。 アプリケーション制御の設定
システムロックダウン	- クライアントコンピュータのアプリケーションを制御する。 - ほとんどすべてのトロイの木馬、スパイウェア、または既存のアプリケーションに自己を実行またはロードしようと試みるマルウェアを遮断する。 システムロックダウンはシステムを信頼できる既知の状態に保ちます。 Note: システムロックダウンの実装を慎重に行わないと、ネットワークで深刻な問題が生じることがあります。特定の段階でシステムロックダウンを実装することをお勧めします。 [クライアント] ページの [ポリシー] ページで、システムロックダウンを設定します。 システムロックダウンの設定
デバイス制御	- USB、赤外線、FireWire デバイスなど、クライアントコンピュータに接続するさまざまな種類のデバイスを遮断または許可する。 - シリアルポートとパラレルポートを遮断または許可する。 デバイス制御の管理

アプリケーション制御とデバイス制御の両方は、32 ビットコンピュータと 64 ビットの Windows コンピュータでサポートされます。

14 では、Mac コンピュータはデバイス制御をサポートします。

アプリケーション制御の設定

アプリケーション制御は、クライアントコンピュータのシステムリソースにアクセスを試みる定義済みのアプリケーションを許可または遮断します。特定のレジストリキー、ファイル、フォルダへのアクセスを許可または遮断できます。また、実行を許可するアプリケーション、通常とは異なるプロセスで終了できないアプリケーション、DLL を呼び出せるアプリケーションを定義することもできます。

クライアントコンピュータのグループにアプリケーション制御を設定するには、次の手順を使います。

Table 115: アプリケーション制御の設定

手順	説明
ポリシーを開き、デフォルトのアプリケーション制御ルールセットを有効にします。	アプリケーション制御ポリシーは、デフォルトで無効の事前定義済みのルールセットを含んでいます。必要なセットを有効にして、ポリシーをグループに適用できます。事前定義済みのルールセットは、テストモードではなく実働モードで設定されます。ただし、設定をテストモードに変更してテストネットワークでルールをテストしてから、実働ネットワークに適用する必要があります。 デフォルトのアプリケーションルールの有効化とテスト
追加のアプリケーション制御ルールを追加する (省略可能)	デフォルトルールセットが必要条件を満たしていない場合は、新しいルールセットとルールを追加します。通常は、詳しい知識のある管理者のみが、このタスクを実行してください。 アプリケーション制御へのカスタムルールの追加

手順	説明
アプリケーションの例外を追加する	アプリケーション制御は、一部のアプリケーションに検査のためのコードを挿入します。これにより、コンピュータで実行するアプリケーションが遅くなる可能性があります。必要に応じて、アプリケーション制御から一部のアプリケーションを除外できます。アプリケーション制御のファイル例外またはフォルダ例外を追加するには、例外ポリシーを使います。 スキャンからのファイルまたはフォルダの除外
アプリケーション制御ログを表示する	新しいポリシーをテストするか、または問題をトラブルシューティングする場合は、ログのアプリケーション制御イベントを監視する必要があります。 テストモードと実動モードの両方で、アプリケーション制御イベントは 1 つの Symantec Endpoint Protection Manager のアプリケーション制御ログにあります。クライアントコンピュータでは、アプリケーション制御およびデバイス制御イベントは制御ログに表示されます。 単一のアプリケーション制御処理に対して、重複または複数のログエントリを確認できます。たとえば、explorer.exe はファイルをコピーしようすると、ファイルのアクセスマスクの書き込みおよび削除ビットを設定します。Symantec Endpoint Protection はイベントをログに記録します。アプリケーション制御ルールが処理を遮断したためにコピー処理が失敗した場合、explorer.exe は、アクセスマスクの削除ビットのみを使ってファイルのコピーを試みます。Symantec Endpoint Protection は、コピー試行の別のイベントをログに記録します。 ログの表示
アプリケーション制御の有効と無効の切り替えをユーザーに禁止または許可する (省略可能)	まれに、アプリケーション制御が、クライアントコンピュータで実行される安全なアプリケーションに干渉することがあります。トラブルシューティングのために、ユーザーがこのオプションを無効にできるようにすることをお勧めします。混合モードまたはクライアントモードで、[クライアントユーザーインターフェースの設定] ダイアログの [ユーザーによるアプリケーションデバイス制御の有効と無効の切り替えを許可する] 設定を使います。 クライアントコンピュータの保護をユーザーが無効にできない設定

システムロックダウンを使って、クライアントコンピュータで承認済みアプリケーションを許可したり、未承認のアプリケーションを遮断したりすることができます。

システムロックダウンの設定

デフォルトのアプリケーションルールの有効化とテスト

アプリケーション制御には、1 つ以上のルールからなるデフォルトルールセットが含まれています。デフォルトのアプリケーション制御ルールセットは、1 つの Symantec Endpoint Protection Manager とともにインストールされます。デフォルトのルールセットは、インストール時は無効になっています。アプリケーション制御ポリシー内でデフォルトのルールセットを使うには、これらを有効にして、ポリシーをクライアントグループに適用する必要があります。

共通の事前定義済みのルールの説明については、「[Hardening Symantec Endpoint Protection \(SEP\) with an Application and Device Control Policy to increase security](#)」を参照してください。

次のタスクで [USB ドライブの書き込みを遮断する] ルールセットを有効にして、テストします。

1. デフォルトのアプリケーションルールセットを有効にするには、コンソールで [ポリシー] > [アプリケーションとデバイス制御] をクリックし、[タスク] で [アプリケーション制御ポリシーを追加] をクリックします。
2. [概要] ペインで、ポリシーの名前と説明を入力します。
3. [アプリケーション制御] をクリックします。
4. [アプリケーション制御] ペインで、実装する各ルールセットの横にある [有効] チェックボックスにチェックマークを付けます。
たとえば、[USB ドライブの書き込みを遮断する] ルールセットの横にある [有効] 列のチェックボックスにチェックマークを付けます。
5. ルールセットのルールを確認するには、[編集] をクリックしてから、[OK] をクリックします。

アプリケーション制御へのカスタムルールの追加

-
6. [実働] を [テスト (ログのみ)] に変更します。
 7. グループにポリシーを割り当てて、[OK] をクリックします。
 8. ルールセット [USB ドライブの書き込みを遮断する] をテストするには、クライアントコンピュータで、USB ドライブを接続します。
 9. Windows エクスプローラを開き、USB ドライブをダブルクリックします。
 10. ウィンドウを右クリックし、[新規]、[フォルダ] の順に選択します。
アプリケーション制御が有効な場合、[フォルダを作成できません] というエラーメッセージが表示されます。

アプリケーション制御、システムロックダウン、デバイス制御について

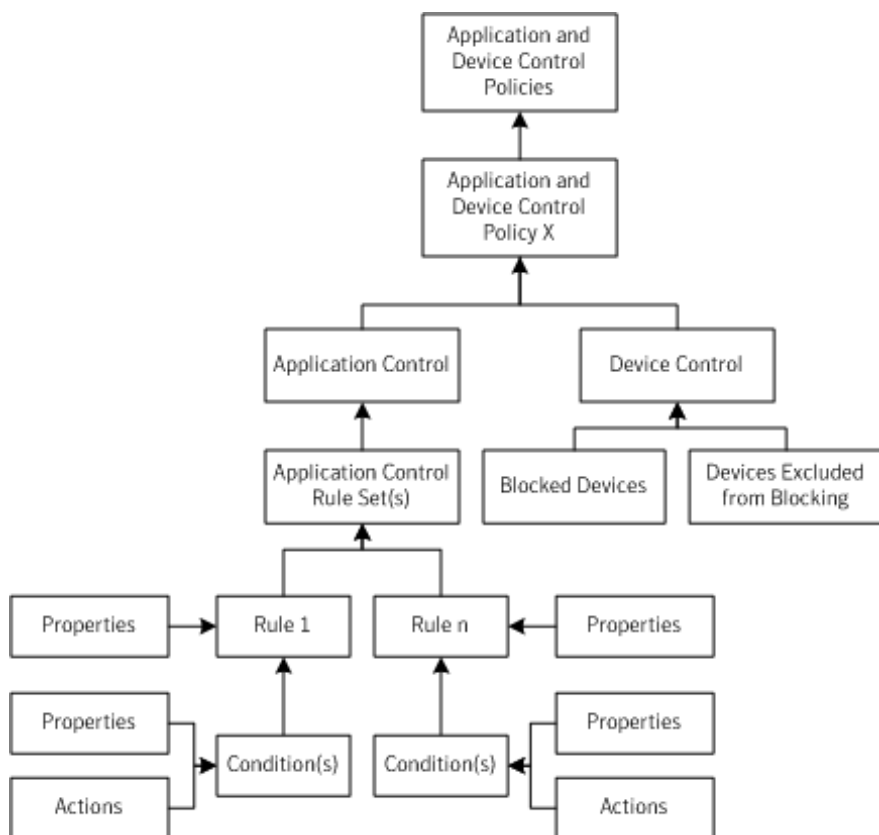
アプリケーション制御とデバイス制御ポリシーの構造について

アプリケーション制御とデバイス制御ポリシーの構造

[アプリケーションとデバイス制御ポリシー] には次の 2 つの要素があります。

- アプリケーション制御は 1 つ以上のルールセットを含みます。各ルールセットは、1 つ以上のルールを含みます。各ルールについて、プロパティ、条件、処理を設定します。
 - [ルール] には、監視するアプリケーションを定義します。
 - [条件] には、ルールで定義したアプリケーションに指定した操作の監視を設定します。条件には、指定した運用を監視するときに実行する処理も含めます。
 - ルールと条件を追加するときは、条件の特定のプロパティと、条件が満たされた場合に実行する処理を指定する必要があります。条件の種類によってプロパティは異なります。
- デバイス制御は、遮断されるデバイスのリストと、遮断対象から除外するデバイスのリストで構成されます。これら 2 つのリストに追加でき、その内容を管理できます。

「[アプリケーションとデバイス制御ポリシーの構造](#)」に、アプリケーション制御、デバイス制御のコンポーネントと、それぞれの関連を示します。



アプリケーション制御、システムロックダウン、デバイス制御について

アプリケーション制御の設定

アプリケーション制御へのカスタムルールの追加

デバイス制御の管理

アプリケーション制御へのカスタムルールの追加

デフォルトルールセットが必要条件を満たしていない場合は、新しいルールセットとルールを追加します。ポリシーと一緒にインストールされた事前定義済みのルールセットを変更することもできます。

- ルールセットは、処理を許可またはブロックする 1 つ以上のルールを保持するコンテナです。
- ルールセットのルールは 1 つ以上のプロセスまたはアプリケーションを定義します。監視からプロセスを除外することもできます。
- 各ルールには、指定の 1 つのプロセスまたは複数のプロセスに適用される条件と処理が含まれます。各条件に対し、条件が満たされたときに実行する処理を設定できます。特定のアプリケーションにだけ適用されるようにルールを設定し、他のアプリケーションを処理の適用対象から除外することもできます。

アプリケーション制御とデバイス制御ポリシーの構造について

独自のアプリケーションルールを追加するには、次の手順を実行します。

- ステップ 1: アプリケーション制御ポリシーにカスタムルールセットとルールを追加する (オプション)
- ステップ 2: ルールのアプリケーションまたはプロセスを定義する (オプション)
- ステップ 3: ルールに条件と処理を追加する (オプション)
- ステップ 4: 実働ネットワークに適用する前に、ルールをテストする

アプリケーション制御ルールのテスト

ステップ 1: カスタムルールセットとルールを追加する

ベストプラクティスは、1つのルールセットを作成し、その中に指定したタスクを許可、遮断、監視するすべての処理を含めることです。一方、複数のタスクがある場合は、複数のルールセットを作成する必要があります。たとえば、すべてのリムーバブルドライブへの書き込みを遮断し、アプリケーションが特定のアプリケーションを改変することも遮断する場合は、2つのルールセットを作成する必要があります。ルールセットとルールは必要な数だけ追加し、有効にできます。

たとえば、BitTorrent はピアツーピアのファイル共有に使用される通信プロトコルで、安全ではありません。BitTorrent は、ムービー、ゲーム、ミュージックなどのファイルを配布します。BitTorrent は脅威を拡散させる非常に単純な方法の 1 つです。マルウェアはピアツーピアネットワークで共有されるファイルに隠されています。アプリケーション制御を使うと、BitTorrent プロトコルへのアクセスを遮断できます。ピアツーピア認証と侵入防止を使うこともできます。[ピアツーピア認証の設定によるリモートコンピュータの遮断](#)

ルールを設定する場合には、予期しない結果にならないようにルールとその条件の順序を考慮してください。通常は、詳しい知識のある管理者のみが、このタスクを実行してください。

アプリケーション制御ルールの追加のベストプラクティス

カスタムルールセットとルールを追加するには

1. アプリケーション制御ポリシーを開きます。
[デフォルトのアプリケーションルールの有効化とテスト](#)
2. [アプリケーション制御] パネルのデフォルトルールセットのリストで、[追加] をクリックします。
事前定義済みのルールセットを修正するには、ルールセットを選択して [編集] をクリックします。たとえば、BitTorrent プロトコルにアクセスするアプリケーションを監視するには、[リムーバブルドライブからのプログラムの実行を遮断する [AC2]] を選択します。
3. [アプリケーション制御ルールセットの追加] ダイアログボックスにルールセットの名前と説明を入力します。
4. [ルール] で [ルール 1] を選択して [プロパティ] ページでルールのわかりやすい名前と説明を入力します。
その他のルールを追加するには、[追加]、[ルールの追加] の順にクリックします。

ステップ 2: ルールのアプリケーションまたはプロセスを定義する

各ルールには、クライアントコンピュータ上で監視する少なくとも 1 つのアプリケーションまたはプロセスが含まれている必要があります。また、ルールから特定のアプリケーションを除外できます。

ルールのアプリケーションまたはプロセスを定義するには

1. ルールを選択した状態で、[プロパティ] ページの [このルールを次のプロセスに適用する] の横にある [追加] をクリックします。
2. [プロセス定義の追加] ダイアログボックスで、アプリケーション名またはプロセス名を `textpad.exe` のように入力します。
指定されたアプリケーションのセットを除いてすべてのアプリケーションにルールを適用する場合は、この手順ですべてを意味するワイルドカード (*) を定義します。例外とする必要のあるアプリケーションを、[このルールを次のプロセスに適用しない] の横に一覧表示します。
3. [OK] をクリックします。
[このルールを有効にする] チェックボックスは、デフォルトで有効になっています。このオプションのチェックマークをはずすと、ルールは適用されません。

ステップ 3: ルールに条件と処理を追加する

条件は、クライアントコンピュータ上で実行が試行されるアプリケーションまたはプロセスの動作を制御します。各条件の種類には、条件の検索対象を指定する独自のプロパティがあります。

各条件には独自の処理が含まれ、条件に該当する場合にプロセスが実行されます。プロセス終了処理を除いて、処理は常に条件ではなくルールに対して定義されたプロセスに適用されます。

警告: プロセスの終了処理によって、呼び出し側プロセス、または要求を行ったアプリケーションが終了します。呼び出し側プロセスとは、条件ではなくルールで定義するプロセスのことです。その他の処理は、条件内で定義された対象プロセスに作用します。

条件	説明
レジストリアクセスの試み	クライアントコンピュータのレジストリ設定へのアクセスを許可または遮断します。
ファイルやフォルダのアクセスの試み	クライアントコンピュータ上の定義されたファイルやフォルダに対するアクセスを許可または遮断します。
プロセス起動の試み	クライアントコンピュータ上でのプロセスの起動機能を許可または遮断します。
プロセス終了の試み	クライアントコンピュータ上でのプロセスの終了機能を許可または遮断します。たとえば、特定のアプリケーションを停止する動作を遮断しようとする場合があります。 警告: プロセス終了の試みの条件は、ターゲットプロセスを示します。Symantec Endpoint Protection または別の重要なプロセスで [プロセス終了の試み] 条件を使う場合は、[プロセスを終了] 処理を使って Symantec Endpoint Protection を強制終了しようとするプロセスを強制終了します。
DLL ロードの試み	クライアントコンピュータ上での DLL のロード動作を許可または遮断します。

- [ルール] 下で、追加したルールを選択し、[追加] > [条件の追加] の順にクリックして条件を選択します。
ルールに使う条件を選択するためのベストプラクティス
たとえば、[プロセス起動の試み] をクリックすると、クライアントコンピュータが BitTorrent プロトコルにアクセスするタイミングに関する条件を追加できます。
- [プロパティ] タブで、起動する必要があるプロセスと起動しないプロセスを選択します。
 - 起動するプロセスを指定するには
[次のエンティティに適用する] の横にある [追加] をクリックします。
 - プロセスを起動対象から除外するには
[次のプロセスに適用しない] の横にある [追加] をクリックします。
- [エンティティ定義の追加] ダイアログボックスで、プロセス名、DLL、またはレジストリキーを入力します。
たとえば、BitTorrent を追加するには、ファイルパスと実行可能ファイルを次のように入力します。C:\Users\UserName\AppData\Roaming\BitTorrent
条件を特定のフォルダ内のすべてのエンティティに適用するには、ベストプラクティスとして、folder_name* または folder_name** を使います。1 つのアスタリスクには、名前付きフォルダ内のすべてのファイルとフォルダが含まれます。名前付きフォルダ内のすべてのファイルとフォルダに加え、すべてのサブフォルダ内のファイルとフォルダを含めるには、folder_name** を使います。
- [OK] をクリックします。
- 条件の [処理] タブで、実行する処理を選択します。
たとえば、Textpad が Firefox を起動する試みを遮断するには、[アクセスを遮断する] をクリックします。
- [ログ記録を有効にする] と [ユーザーに通知] にチェックマークを付けて、クライアントコンピュータがユーザーに対して表示するメッセージを入力します。
たとえば、「Textpad # Firefox #####」と入力します。
- [OK] をクリックします。
新しいルールセットが表示され、テストモードに設定されます。クライアントコンピュータに適用する前に、新しいルールセットをテストしてください。

アプリケーション制御ルールの追加のベストプラクティス

カスタムアプリケーション制御ルールは、慎重に計画する必要があります。アプリケーション制御ルールを追加するときは、次のベストプラクティスに留意してください。

Table 116: アプリケーション制御ルールのベストプラクティス

ベストプラクティス	説明	例
ルールの順序を考慮する	アプリケーション制御ルールは、最初に一致したルールが適用されるという点で、ほとんどのネットワークベースファイアウォールルールと同様に動作します。複数の条件が該当する場合、最初のルールだけが適用されます。ただし、そのルールに設定されている処理が「他のルールの処理を続ける」である場合を除きます。	すべてのユーザーが、USB ドライブ上のファイルを移動、コピー、作成できないようにします。 Test.doc という名前のファイルへの書き込みアクセスを許可する条件が含まれた既存のルールがあります。この既存のルールセットに対して 2 つ目の条件を追加し、すべての USB ドライブを遮断します。このシナリオでは、ユーザーは引き続き USB ドライブ上の Test.doc ファイルを作成、変更できます。Test.doc への「アクセスを許可する」という条件は、ルールセットにおいて、USB ドライブへの「アクセスを遮断する」という条件の前に現れます。USB ドライブへの「アクセスを遮断する」という条件は、リストでこの条件よりも前に現れる条件が該当するときには処理されません。
正しい処理を使う	「プロセス終了の試み」条件は、クライアントコンピュータ上でのアプリケーションによる呼び出しプロセスの終了を許可または遮断します。 この条件は、ユーザーが「ファイル」メニューから「中止する」をクリックするなどの通常の方法でアプリケーションを停止することを許可または防止しません。	Process Explorer は、開かれているまたはロードされている DLL プロセスと、そのプロセスが使っているリソースを表示するツールです。 Process Explorer が特定のアプリケーションを終了しようとしているとき、Process Explorer を終了することができます。 「プロセス終了の試み」条件と「プロセスを終了する」処理を使って、この種類のルールを作成します。Process Explorer アプリケーションに条件を適用します。Process Explorer で終了しない、1 つまたは複数のアプリケーションにルールを適用します。
目的ごとに 1 つのルールセットを使う	指定したタスクを許可、遮断、監視するすべての処理を含んだ 1 つのルールセットを作成します。	すべてのリムーバブルドライブへの書き込みを遮断し、アプリケーションが特定のアプリケーションを変更することを遮断できます。 これらの目的を実現するため、1 つのルールセットではなく、2 つの異なるルールセットを作成します。
「プロセスを終了する」処理を控えめに使う	「プロセスを終了する」処理は、呼び出しプロセスが設定された条件を満たした場合に、プロセスを強制終了します。 「プロセスを終了する」処理を使うのは、詳しい知識のある管理者のみにしてください。通常は、代わりに「アクセスを遮断する」処理を使ってください。	プロセスが Winword.exe を起動したときはいつでも、Winword.exe を終了したいと考えているとします。 これは、ルールを作成し、「プロセス起動の試み」条件と「プロセスを終了する」処理を使って設定します。条件を Winword.exe に適用し、ルールをすべてのプロセスに適用します。 このルールが Winword.exe を終了すると思うかもしれませんが、これはこのルールが行う処理ではありません。Windows エクスプローラから Winword.exe を開始しようとすると、この設定を含むルールによって Winword.exe ではなく Explorer.exe が終了します。ユーザーが直接 Winword.exe を起動する場合は、Winword.exe は実行可能な状態のままです。代わりに、対象プロセスまたは Winword.exe を遮断する、「アクセスを遮断する」処理を使います。

ベストプラクティス	説明	例
ルールを実働状態にする前にテストする	ルールセットの [テスト (ログのみ)] オプションを設定すると処理がログに記録されます。クライアントコンピュータに処理を適用することはありません。実働モードに切り替える前に、許容できる一定期間ルールをテストモードで実行します。この期間中に、アプリケーション制御ログを見直して、ルールが予定どおりに機能することを検証します。	テストのオプションにより、ルールを適用すると発生する可能性がある結果をすべて検討できなかった場合でも潜在的なエラーが減少します。 アプリケーション制御ルールのテスト

アプリケーション制御へのカスタムルールの追加

ルールに使う条件を選択するためのベストプラクティス

ルールに使う条件を選択するためのベストプラクティス

ユーザーがアプリケーションを開いたり、ファイルに書き込んだり、ファイルを共有したりできないようにするために、カスタムアプリケーション制御ルールと条件を追加します。デフォルトのルールセットを見れば、ルールを設定する方法を決定する場合に役立ちます。たとえば、[アプリケーションの実行を遮断する] ルールセットを編集して、[プロセス起動の試み] 条件の使い方を確認できます。

アプリケーション制御へのカスタムルールの追加

Table 117: ルールに使う一般的な条件

ルール	条件
ユーザーがアプリケーションを開けないようにする	これらの条件のいずれかを満たす場合に、アプリケーションを遮断できます。 - プロセス起動の試み たとえば、ユーザーが FTP ファイルを転送できないようにするには、ユーザーに FTP クライアントを起動させないルールをコマンドプロンプトから追加できます。 - DLL ロードの試み たとえば、クライアントコンピュータの Msvcr7.dll を遮断するルールを追加した場合、ユーザーは Microsoft WordPad を開くことができません。ルールはまた、DLL を使うその他のアプリケーションもすべて遮断します。
ユーザーが特定のファイルに書き込めないようにする	ユーザーがファイルを開くことができても、ファイルを修正できないようにすることができます。たとえば、ファイルには、従業員が確認する必要があるが編集できない財務データが含まれる場合があります。 ユーザーにファイルへの読み取り専用アクセスを与えるルールを作成できます。たとえば、メモ帳でテキストファイルを開くことはできるが、編集はできないルールを追加できます。 この種類のルールには、[ファイルやフォルダのアクセスの試み] 条件を使います。

ルール	条件
Windows コンピュータでファイル共有を遮断する	Windows コンピュータでローカルファイルとプリンタの共有を無効にできます。次の条件を含めます。 - レジストリアクセスの試み 適切な Windows セキュリティおよび共有するレジストリキーをすべて追加します。 - プロセス起動の試み サーバーサービス処理 (svchost.exe) を指定します。 - DLL ロードの試み [セキュリティ] および [共有] タブで DLL を指定します (rshx32.dll、ntshrui.dll)。 - DLL ロードの試み サーバーサービス DLL (srvsvc.dll) を指定します。 各条件の処理を [アクセスを遮断する] に設定します。 また、ファイアウォールルールを使って、クライアントコンピュータに対してファイルの共有を禁止するか共有するかを指定できます。 ネットワーク内のファイルおよびプリンタを参照できるようにするクライアントの許可
ユーザーがピアツーピアアプリケーションを実行できないようにする	ユーザーが各自のコンピュータでピアツーピアアプリケーションを実行しないようにできます。[プロセス起動の試み] 条件で、カスタムルールを作成できます。条件では、LimeWire.exe や *.torrent など、遮断するすべてのピアツーピアアプリケーションを指定する必要があります。各条件の処理を [アクセスを遮断する] に設定します。] の順にクリックします。 侵入防止ポリシーを使って、ピアツーピアアプリケーションからのネットワークトラフィックを遮断します。ファイアウォールポリシーを使って、ピアツーピアアプリケーショントラフィックを送受信するポートを遮断します。 侵入防止の管理 ファイアウォールポリシーの作成
DVD ドライブへの書き込み試行を遮断する	現在、アプリケーション制御には CD/DVD の書き込みを直接遮断するデフォルトルールがありません。代わりに、[条件の追加] と [ファイルやフォルダのアクセスの試み] 条件を使って、CD または DVD ドライブに書き込む特定の DLL を遮断するルールを作成します。 DVD ドライブに書き込む試行を遮断するには Windows のレジストリキーを設定するホストインテグリティポリシーも作成してください。 ホストインテグリティの設定 「How to block CD/DVD Writing in Windows 7」を参照してください。

アプリケーション制御ルールのテスト

アプリケーション制御ルールを追加した後は、ネットワークでそれらをテストする必要があります。アプリケーション制御ポリシーで使われているルールセット内に設定エラーがあると、コンピュータまたはサーバーが使用できなくなることがあります。また、クライアントコンピュータが障害になったり、つの Symantec Endpoint Protection Manager との通信が遮断されることもあります。テストした後、ルールを実働ネットワークに適用します。

ステップ 1: ルールセットをテストモードに設定する

モードをテストモードに設定してルールセットをテストします。テストモードでは、実際にはルールを適用しないで、ルールセットのルールがいつ適用されるかを示すログエントリが作成されます。

デフォルトルールは、デフォルトで実働モードを使います。カスタムルールは、デフォルトでテストモードを使います。デフォルトルールセットとカスタムルールセットを両方テストしてください。

セット内のルールを個別にテストしたい場合もあります。ルールセットの各ルールの有効と無効を切り替えることで、個々のルールをテストできます。

ルールセットのテストモードへの変更

-
1. コンソールで、アプリケーションとデバイス制御ポリシーを開きます。
 2. [アプリケーション制御ポリシー] で [アプリケーション制御] をクリックします。
 3. [アプリケーション制御ルールの設定] リストで、ルールセットの [テスト/実働] 列のドロップダウン矢印をクリックし、[テスト (ログのみ)] をクリックします。

アプリケーション制御の設定

ステップ 2: テストネットワーク内にあるコンピュータにアプリケーションとデバイス制御ポリシーを適用する

新しいアプリケーションとデバイス制御ポリシーを作成したら、テストネットワーク内のクライアントにポリシーを適用します。

グループまたは場所へのポリシーの割り当て

ステップ 3: アプリケーション制御ログを監視する

ルールセットをテストモードでしばらく実行したら、ログでエラーを調べます。テストモードと実働モードの両方で、アプリケーション制御イベントは 1 つの Symantec Endpoint Protection Manager のアプリケーション制御ログにあります。クライアントコンピュータでは、アプリケーション制御およびデバイス制御イベントは制御ログに表示されます。

単一のアプリケーション制御処理に対して、重複または複数のログエントリを確認できます。たとえば、explorer.exe はファイルをコピーしようとする、ファイルのアクセスマスクの書き込みおよび削除ビットを設定します。Symantec Endpoint Protection はイベントをログに記録します。アプリケーション制御ルールが処理を遮断したためにコピー処理が失敗した場合、explorer.exe は、アクセスマスクの削除ビットのみを使ってファイルのコピーを試みます。Symantec Endpoint Protection は、コピー試行の別のイベントをログに記録します。

ログの表示

ステップ 4: ルールセットを実働モードに戻す

ルールが予期したとおり機能している場合は、ルールセットを実働モードに戻します。

システムロックダウンの設定

システムロックダウンは、許可されていないアプリケーションを遮断することによって、クライアントコンピュータのグループのアプリケーションを制御します。指定されたリストのアプリケーションだけを許可するように、システムロックダウンを設定できます。許可リスト (ホワイトリスト) はすべての承認済みアプリケーションで構成されます。他のアプリケーションはクライアントコンピュータで遮断されます。また、指定されたリストのアプリケーションだけを遮断するように、システムロックダウンを設定することもできます。拒否リスト (ブラックリスト) は、すべての許可されていないアプリケーションで構成されます。他のアプリケーションはすべて、クライアントコンピュータで許可されます。

NOTE

システムロックダウンで許可されるアプリケーションはすべて、Symantec Endpoint Protection の他の保護機能の対象となります。

許可リストまたは拒否リストには、ファイルフィンガープリントリストおよび特定のアプリケーション名を含めることができます。ファイルフィンガープリントリストは、ファイルチェックサムとコンピュータのパスの場所のリストです。

システムロックダウンの代りに、またはシステムロックダウンに加えて、アプリケーションとデバイス制御ポリシーを使って特定のアプリケーションを制御できます。

ネットワークの各グループまたは場所に、システムロックダウンを設定します。

Table 118: システムロックダウンの手順

処理	説明
手順 1: ファイルフィンガープリントリストの作成	クライアントコンピュータで実行することを許可されている、または許可されていないアプリケーションが含まれる、ファイルフィンガープリントリストを作成できます。システムロックダウンの許可リストと拒否リストにファイルフィンガープリントリストを追加します。 システムロックダウンを実行するときは、許可リストまたは拒否リストに含めるすべてのクライアントのアプリケーションを含むファイルフィンガープリントリストが必要です。たとえば、ネットワークに Windows 8.1 32 ビットおよび 64 ビット、Windows 10 64 ビットのクライアントが含まれる場合があります。各クライアントイメージのファイルフィンガープリントリストを作成できます。 ファイルフィンガープリントのリストは、次の方法で作成できます。 • Symantec Endpoint Protection には、ファイルフィンガープリントリストを作成するためのチェックサムユーティリティが用意されています。このユーティリティは、クライアントコンピュータに Symantec Endpoint Protection とともにインストールされています。 このユーティリティは、指定されたパスの特定のアプリケーションまたはすべてのアプリケーション用にチェックサムを作成するのに使います。システムロックダウンを拒否モードで実行する場合に使うファイルフィンガープリントを生成するには、この方法を使います。 checksum.exe を使ったファイルフィンガープリントリストの作成 • [ファイルフィンガープリントリストの収集] コマンドを使って、単一のコンピュータまたはコンピュータの小グループのファイルフィンガープリントのリストを作成します。 コンソールから [ファイルフィンガープリントリストの収集] コマンドを実行できます。このコマンドは、ターゲットコンピュータのすべてのアプリケーションを含むファイルフィンガープリントリストを収集します。たとえば、ゴールドイメージを実行するコンピュータでこのコマンドを実行します。この方法は、システムロックダウンを許可モードで実行するときに使うことができます。コマンドを使って生成したファイルフィンガープリントリストは修正できません。コマンドを再実行すると、ファイルフィンガープリントリストは自動的に更新されます。 コンソールを使った、クライアントコンピュータでのコマンドの実行 • 任意のサードパーティ製チェックサムユーティリティを使って、ファイルフィンガープリントリストを作成します。 Note: Symantec EDR を実行すると、ネットワークで Symantec EDR からファイルフィンガープリントリストが表示されることがあります。 Note: システムロックダウンと Symantec EDR 拒否リスト (ブラックリスト) ルールとの対話
手順 2: つの Symantec Endpoint Protection Manager へのファイルフィンガープリントリストのインポート	システムロックダウン設定でファイルフィンガープリントリストを使うには、事前に つの Symantec Endpoint Protection Manager でリストを利用可能にしておく必要があります。 チェックサムツールを使ってファイルフィンガープリントリストを作成する場合は、つの Symantec Endpoint Protection Manager にリストを手動でインポートする必要があります。 つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ [ファイルフィンガープリントリストの収集] コマンドを使ってファイルフィンガープリントリストを作成すると、結果のリストは自動的に つの Symantec Endpoint Protection Manager コンソールで利用可能になります。 つの Symantec Endpoint Protection Manager から既存のファイルフィンガープリントリストをエクスポートすることもできます。

処理	説明
手順 3: 許可されているアプリケーションまたは許可されていないアプリケーションのための、アプリケーション名リストの作成	任意のテキストエディタを使って、許可リストまたは拒否リストに含めるアプリケーションのファイル名を記載したテキストファイルを作成できます。ファイルフィンガープリントリストの場合とは異なり、これらのファイルはシステムロックダウン設定に直接インポートします。ファイルをインポートした後、アプリケーションはシステムロックダウン設定の個々のエントリとして表示されます。 また、システムロックダウン設定で個々のアプリケーション名を手動で入力することもできます。 Note: 指定されたアプリケーションが多いと、システムロックダウンが拒否リストモードで有効化された場合に、クライアントコンピュータのパフォーマンスに影響を与える可能性があります。 システムロックダウン設定にインポートするアプリケーション名リストの作成
手順 4: システムロックダウンの設定とテスト	テストモードではシステムロックダウンが無効となり、アプリケーションを遮断しません。許可されていないアプリケーションはすべてログに記録されますが、遮断はされません。[システムロックダウン] ダイアログボックスで [許可しないアプリケーションだけをログする] オプションを使って、システムロックダウン設定全体をテストします。 テストを設定し、実行するには、次の手順を実行します。 - システムロックダウン設定にファイルフィンガープリントリストを追加します。 許可モードでは、ファイルフィンガープリントは許可されるアプリケーションです。拒否モードでは、ファイルフィンガープリントは許可されないアプリケーションです。 - システムロックダウン設定に個々のアプリケーション名を追加するか、アプリケーション名のリストをインポートします。 システムロックダウン設定で、アプリケーション名を 1 つずつ入力するのではなく、アプリケーション名のリストをインポートできます。許可モードでは、許可されるアプリケーションを指定します。拒否モードでは、許可されないアプリケーションを指定します。 - 一定の期間、テストを実行します。 クライアントが通常のアプリケーションを実行できるだけ十分な時間、システムロックダウンをテストモードで実行します。通常の時間枠は 1 週間です。 システムロックダウンを有効化する前の、システムロックダウンの設定とテスト
手順 5: 許可されないアプリケーションの表示と、システムロックダウン設定の修正 (必要な場合)	一定の期間テストを実行した後、許可されないアプリケーションのリストをチェックできます。[システムロックダウン] ダイアログボックスで状態を調べることによって、未承認アプリケーションのリストを表示できます。 記録されたイベントはアプリケーション制御ログにも表示されます。 ここで、ファイルフィンガープリントまたはアプリケーションリストにアプリケーションを追加するかどうかを決定できます。システムロックダウンを有効にする前に、必要に応じて、ファイルフィンガープリントリストまたはアプリケーションを追加または削除できます。 システムロックダウンを有効化する前の、システムロックダウンの設定とテスト
手順 6: システムロックダウンを有効にする	デフォルトでは、システムロックダウンは許可モードで実行されます。代わりに、システムロックダウンを拒否モードで実行するように設定できます。 許可モードでシステムロックダウンを有効にすると、許可されるアプリケーションのリストに含まれていないアプリケーションはすべて遮断されます。拒否モードでシステムロックダウンを有効にすると、許可されていないアプリケーションのリストにあるアプリケーションが遮断されます。 Note: システムロックダウンを有効にする前に、必ず設定をテストしてください。必要なアプリケーションを遮断した場合、クライアントコンピュータが再起動できなくなる場合があります。 許可モードでのシステムロックダウンの実行 拒否モードでのシステムロックダウンの実行

処理	説明
手順 7: システムロックダウン用のファイルフィンガープリントリストの更新	時間の経過とともに、ネットワークで実行するアプリケーションを変更する場合があります。ファイルフィンガープリントリストを更新するか、または必要に応じてリストを削除できます。ファイルフィンガープリントリストは次の方法で更新できます。 • インポートしたフィンガープリントリストを手動で追加、置換、マージする。 [ファイルフィンガープリントリストの収集] コマンドを使って生成したフィンガープリントリストにファイルフィンガープリントリストを追加することはできません。コマンドで生成したリストを含むインポート済みリストは追加できます。その場合は、フィンガープリントコマンドを再実行するときに追加リストを再び作成する必要があります。 つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストの手動更新 つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ • インポートした既存のファイルフィンガープリントリストを自動的に更新する。 インポートするアプリケーションまたはアプリケーション名リストを自動的に更新することもできます。 システムロックダウン用に許可または遮断するファイルフィンガープリントリストの自動更新 システムロックダウン設定にインポートするアプリケーション名リストの作成 • [ファイルフィンガープリントリストの収集] コマンドを再実行するとコマンドで生成したフィンガープリントリストが自動的に更新される。 コマンドを再実行すると、既存のリストは自動的に新しいリストに置換されます。 Note: ネットワークにクライアントコンピュータを追加する場合、システムロックダウン設定全体の再テストが必要になることがあります。別のグループに新しいクライアントを移動したり、ネットワークをテストしてシステムロックダウンを無効にしたりできます。または、システムロックダウンを有効にしたままログのみのモードで設定を実行できます。次の手順で説明するようにファイルフィンガープリントやアプリケーションを個別にテストすることもできます。
手順 8: システムロックダウンが有効な状態での、選択した項目の追加前テストまたは削除前テスト	システムロックダウンが有効化された後、個々のファイルフィンガープリント、アプリケーション名リスト、または特定のアプリケーションをテストしてから、それらをシステムロックダウン設定に追加するか、またはシステムロックダウン設定から削除できます。リストの数が多く、その一部は使用しない場合に、ファイルフィンガープリントリストの削除が必要になることがあります。 Note: システムロックダウンからファイルフィンガープリントリストまたは特定のアプリケーションを追加または削除するときは、注意してください。システムロックダウンの項目を追加または削除すると危険な場合があります。クライアントコンピュータ上の重要なアプリケーションが遮断される可能性があります。 • 選択した項目をテストします。 特定のファイルフィンガープリントリストまたは特定のアプリケーションを未承認としてログに記録するには、[削除前にテスト] を使います。 このテストを実行するとき、システムロックダウンは有効になりますが、選択したアプリケーション、または選択したファイルフィンガープリントリスト内のアプリケーションは遮断されません。その代わりに、システムロックダウンは、許可されていないアプリケーションとしてこれらのアプリケーションをログに記録します。 • アプリケーション制御ログを調べます。 ログエントリは、アプリケーション制御ログに表示されます。テストされたアプリケーションのエントリがログにない場合は、クライアントでこれらのアプリケーションが使われていないことがわかります。

アプリケーション制御の設定

checksum.exe を使ったファイルフィンガープリントリストの作成

checksum.exe ユーティリティを使って、ファイルフィンガープリントリストを作成できます。リストには、コンピュータ上の指定されたパスに存在する実行可能ファイルまたは DLL ごとに次の内容が含まれます。

- パス
- ファイル名
- 対応するチェックサム

ファイルフィンガープリントリストをつの Symantec Endpoint Protection Manager にインポートしてシステムロックダウン設定に使用します。

このユーティリティは、クライアントコンピュータに Symantec Endpoint Protection とともにインストールされています。

つ Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ システムロックダウンの設定

サードパーティユーティリティまたは [ファイルフィンガープリントリストの収集] コマンドを使ってファイルフィンガープリントリストを作成することもできます。

コンソールを使った、クライアントコンピュータでのコマンドの実行

checksum.exe を使ってファイルフィンガープリントリストを作成するには

1. ファイルフィンガープリントリストを作成するイメージがあるコンピュータでコマンドプロンプトウィンドウを開きます。

このコンピュータには Symantec Endpoint Protection クライアントソフトウェアがインストールされている必要があります。

2. checksum.exe ファイルを含むクライアントインストールフォルダに移動します。通常、ファイルは次のフォルダで見つかります。

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\

3. 次のコマンドを入力します。

checksum.exe outputfile.txt path

前述の引数について説明します。

- outputfile.txtは、指定ドライブに存在するすべてのアプリケーションのチェックサムを持つ出力テキストファイルの名前です。
- pathは、チェックサム情報を収集するコンピュータ上のファイルパスです。

NOTE

C ドライブのすべてのファイルに対しチェックサムを実行するには、path] の順にクリックします。そうしないと、このコマンドは checksum.exe が配置されているフォルダでのみ実行されます。

出力ファイルの各行の形式は次のとおりです。

checksum_of_the_file full_pathname_of_the_exe_or_DLL

チェックサム値と絶対パス名はスペースで区切られます。

checksum.exe の出力の例を次に示します。

```
0bb018fad1b244b6020a40d7c4eb58b7 c:\dell\openmanage\remind.exe
35162d98c2b445199fef95e838feae4b c:\dell\pnp\m\co\HSFCI008.dll
2f276c59243d3c051547888727d8cc78 c:\Nokia Video Manager\QtCore4.dll
```

構文の例

以下に、C ドライブ上のすべてのファイルのフィンガープリントリストを作成するために使用できる構文の例を示します。

```
checksum.exe cdrive.txt c:/
```

このコマンドでは、cdrive.txt という名前のファイルが生成されます。実行されるコンピュータの C ドライブで見つかったすべての実行可能ファイルと DLL のチェックサムとファイルパスが含まれます。

NOTE

パスにスペースが含まれている場合や、バッチファイルを使用する場合は、パスを引用符 (") で囲みます。たとえば、"C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" cdrive.txt c:/ と指定します。

以下に、クライアントコンピュータのフォルダにフィンガープリントを作成する際に使用できる構文の例を示します。

```
checksum.exe blocklist.txt c:\Files
```

このコマンドは blocklist.txt と呼ばれるファイルを作成します。[ファイル] フォルダで見つかった実行可能ファイルと DLL のチェックサムとファイルパスが含まれます。

NOTE

パスにスペースが含まれている場合や、バッチファイルを使用する場合は、パスを引用符 (") で囲みます。たとえば、スペースが含まれる場合は、"C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Checksum.exe" blocklist.txt "c:\Files" と指定します。

つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ

ファイルフィンガープリントリストは、システムロックダウン設定に追加できるように、つの Symantec Endpoint Protection Manager コンソールで利用可能になっている必要があります。checksum.exe ユーティリティまたはサードパーティのチェックサムツールを使ってファイルフィンガープリントリストを作成する場合は、手動でリストをインポートする必要があります。また、ファイルフィンガープリントリストをマージすることもできます。

[ファイルフィンガープリントリストの収集] コマンドを使って作成するファイルフィンガープリントリストは、コンソールで自動的に利用可能になります。ファイルフィンガープリントリストをインポートする必要はありません。[ファイルフィンガープリントリストの収集] コマンドを使って作成したファイルフィンガープリントリストは修正できません。ただし、コマンドで生成したファイルフィンガープリントリストと別のファイルフィンガープリントリストをマージできます。再度コマンドを実行してリストを再生成する場合は、手動でリストを再びマージする必要があります。

システムロックダウンの設定

checksum.exe を使ったファイルフィンガープリントリストの作成

ファイルフィンガープリントリストのインポートまたはマージ

-
1. コンソールで、[ポリシー] をクリックします。
 2. [ポリシー] で、[ポリシーコンポーネント] を展開し、[ファイルフィンガープリントリスト] をクリックします。
 3. [タスク] で、[ファイルフィンガープリントリストの追加] をクリックします。
 4. [ファイルフィンガープリントの追加ウィザードによろこそ] で、[次へ] をクリックします。
 5. [新しいファイルフィンガープリントについての情報] パネルで、新しいリストの名前と説明を入力します。
 6. [次へ] をクリックします。
 7. [ファイルフィンガープリントの作成] パネルで、次のいずれかのオプションを選択します。
 - ファイルフィンガープリントファイルをインポートすることによってファイルフィンガープリントを作成します
 - 複数の既存のファイルフィンガープリントを組み合わせるファイルフィンガープリントを作成するこのオプションは複数のファイルフィンガープリントリストをすでにインポートした場合にのみ利用可能です。
 8. [次へ] をクリックします。
 9. 次のいずれかの処理を実行します。
 - 作成したファイルフィンガープリントへのパスを指定します。参照してファイルを見つけることができます。
 - マージするフィンガープリントリストを選択します。
 10. [次へ] をクリックします。
 11. [閉じる] をクリックします。
 12. [完了] をクリックします。

インポートまたはマージされたフィンガープリントリストは、[ポリシー] タブの [ポリシー] > [ポリシーコンポーネント] > [ファイルフィンガープリントリスト] に表示されます。

つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストの手動更新

しばらくの間システムロックダウンを実行したら、ファイルフィンガープリントリストを更新すると便利です。インポートした既存のファイルフィンガープリントリストでエントリを追加、置換、削除できます。つの Symantec Endpoint Protection Manager で既存のファイルフィンガープリントリストを直接編集することはできません。

新しいリストにフィンガープリントリストをマージして異なる名前を付ける場合は、ファイルフィンガープリントの追加ウィザードを使います。

[ファイルフィンガープリントリストの収集] コマンドを使ってフィンガープリントリストを作成した場合は、エントリを追加、置換、削除できません。ただし、インポート済みリストにコマンドで生成したリストを追加できます。コマンドを再実行する場合は、手動でフィンガープリントのリストを再度更新する必要があります。

Symantec EDR が つの Symantec Endpoint Protection Manager に送信するファイルフィンガープリントリストは変更できません。

つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ システムロックダウンの設定

つの Symantec Endpoint Protection Manager でファイルフィンガープリントリストを更新するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシー] で、[ポリシーコンポーネント] を展開し、[ファイルフィンガープリントリスト] をクリックします。
3. [ファイルフィンガープリントリスト] ペインで、編集するファイルフィンガープリントリストを選択します。
4. [編集] をクリックします。
5. ファイルフィンガープリントの編集ウィザードで、[次へ] をクリックします。
6. 次のいずれかの操作をします。
 - 新規ファイルを既存のファイルに追加するには、[このファイルフィンガープリントにフィンガープリントを追加する] をクリックします。
 - すでにインポート済みのファイルフィンガープリントリストをマージするには、[このファイルフィンガープリントに別のファイルフィンガープリントを追記する] をクリックします。
 - [既存のリストを新しいもので置き換える] をクリックします。
 - [新しいリストにも表示されるフィンガープリントを削除する] をクリックします。
7. 次のいずれかの操作をします。
 - [参照] をクリックしてファイルを指定するか、または追加、置換、削除するファイルフィンガープリントリストの絶対パスを入力します。
 - マージするファイルフィンガープリントを選択します。
8. [次へ]、[閉じる]、[完了] の順にクリックします。

システムロックダウンと Symantec EDR 拒否リスト (ブラックリスト) ルールとの対話

ネットワークに Symantec EDR が含まれる場合、Symantec EDR からのシステムロックダウン設定の遮断アプリケーションが表示されることがあります。

Symantec EDR 拒否リスト (ブラックリスト) は、次のようにシステムロックダウン設定と対話します。

- つの Symantec Endpoint Protection Manager が Symantec EDR から拒否ルールを受信すると、つの Symantec Endpoint Protection Manager はすべてのドメインとグループのシステムロックダウンを拒否モードで有効にします。
- 拒否ルールは、システムロックダウン設定の つの Symantec Endpoint Protection Manager ファイルフィンガープリントリストに記載されます。Symantec EDR からファイルフィンガープリントリストを変更することはできません。
- 許可モードでシステムロックダウンを有効にしてクライアントグループを設定すると、その設定が保持され、つの Symantec Endpoint Protection Manager は Symantec EDR の拒否ルールを使用しません。
- システムロックダウンを無効にし、Symantec EDR の拒否リストを削除すると、つの Symantec Endpoint Protection Manager は自動的にシステムロックダウンを再度有効にして拒否リストを適用します。
- システムロックダウンを無効にし、Symantec EDR の拒否リストを削除しなければ、システムロックダウンは再度有効になるまで無効のままになります。

NOTE

Symantec EDR は、Symantec Endpoint Protection クライアントに許可ルールを直接送信します。Symantec EDR は、許可リストのファイルフィンガープリントを つの Symantec Endpoint Protection Manager に送信しません。

[許可モードでのシステムロックダウンの実行](#)

[拒否モードでのシステムロックダウンの実行](#)

[評価のクエリーおよび提出に専用サーバーを使うクライアントグループの設定](#)

システムロックダウン設定にインポートするアプリケーション名リストの作成

アプリケーション名のリストをシステムロックダウンの設定にインポートできます。アプリケーション名をシステムロックダウン設定に個々に追加するよりも、アプリケーション名リストをインポートすると効率的です。

アプリケーション名リストをすべてまとめると、デフォルトでは最大 512 個のアプリケーションを含めることができます。conf.properties ファイルで最大数を変更できます。

任意のテキストエディタを使ってアプリケーション名リストファイルを作成できます。

ファイルの各行には、次の項目をスペースで区切って入力できます：

- ファイル名
パス名を使用する場合は、引用符で囲む必要があります。
- テストモード
有効にする場合は 1 または Y の値、無効にする場合は 0 または N の値にしてください。フィールドを空のままにすると、テストモードは無効になります。照合モードを指定するには値を設定する必要があります。
- 照合モード (ワイルドカードまたは正規表現)
正規表現の一致を使う場合は 1 または Y の値、ワイルドカードの一致を使う場合は 0 または N の値にしてください。フィールドを空のままにすると、ワイルドカードの一致は使われません。

NOTE

テストモードフィールドでは、リストのそれぞれのアプリケーションに対して [追加前のテスト] オプションまたは [削除前にテスト] オプションを有効または無効にします。[ログアプリケーションのみ] オプションを使ってシステムロックダウン設定全体をテストする場合は、テストモードフィールドは無視されます。

各行では次のような構文を使用してください。

```
filename test_mode matching_mode
```

次に例を示します。

```
aa.exe
bb.exe 0 1
cc.exe 1
dd.exe 1 0
"c:\program files\ee.exe" 0 0
```

システムロックダウンにこのリストをインポートすると、個々のアプリケーションが次の設定とともにシステムロックダウン設定に表示されます。

Table 119: 照合モードの設定の例

アプリケーション名	[追加前のテスト] または [削除前にテスト]	照合モード
aa.exe	無効	ワイルドカード
bb.exe	無効	正規表現
cc.exe	有効	ワイルドカード
dd.exe	有効	ワイルドカード
c:\program files\ee.exe	無効	ワイルドカード

システムロックダウンの設定

システムロックダウン用に許可または遮断するファイルフィンガープリントリストの自動更新

つの Symantec Endpoint Protection Manager はインポート済み、マージ済み、追加済みの既存のファイルフィンガープリントリストとアプリケーション名リストを自動的に更新します。

[ファイルフィンガープリントリストの収集] コマンドで生成したファイルフィンガープリントリストは、同じコンピュータでこのコマンドを再実行すると自動的に更新されます。

既存のファイルフィンガープリントを手動で更新することもできます。

Table 120: システムロックダウンの許可リスト (ホワイトリスト) および拒否リスト (ブラックリスト) の更新

手順	説明
ステップ 1: 更新されたファイルフィンガープリントリストまたはアプリケーション名リストを作成し、ファイルを圧縮する	checksum.exe ユーティリティまたは任意のサードパーティユーティリティを使って、更新されたファイルフィンガープリントリストを作成できます。任意のテキストエディタを使って、アプリケーション名リストを更新できます。リストには、つの Symantec Endpoint Protection Manager にすでに存在する名前と同じものが含まれる必要があります。 checksum.exe を使ったファイルフィンガープリントリストの作成 [ファイルフィンガープリントリストの収集] コマンドで生成したフィンガープリントリストは直接更新できません。コマンドで生成したリストを別のリストとマージしたり、コマンドで生成したリストとともにインポート済みリストを追加したりできます。 自動更新機能には、ファイルフィンガープリントリストとアプリケーション名リストの圧縮ファイル (zip ファイル) が必要です。Windows のファイル圧縮機能または任意の圧縮ユーティリティを使って、ファイルを圧縮できます。
ステップ 2: index.ini ファイルを作成する	index.ini ファイルでは、つの Symantec Endpoint Protection Manager がどのファイルフィンガープリントリストとアプリケーション名リストを更新する必要があるかを指定します。 また、任意のテキストエディタを使って index.ini ファイルを作成し、そのファイルを指定の URL にコピーできます。 システムロックダウンで使用される許可リストと拒否リストの自動更新のための index.ini ファイルの作成
ステップ 3: 圧縮ファイルと index.ini を つの Symantec Endpoint Protection Manager で利用可能にする	つの Symantec Endpoint Protection Manager は UNC、FTP、または HTTP/HTTPS を使って、指定の URL で index.ini ファイルと zip ファイルを取得します。つの Symantec Endpoint Protection Manager は、index.ini ファイルの指示を使って、指定されたファイルを更新します。自動更新を有効にすると、つの Symantec Endpoint Protection Manager は設定されたスケジュールに基づいて、更新されたファイルがある URL を定期的に確認します。 UNC の場合は JCFIS 共有のみがサポートされます。DFS 共有はサポートされません。 Note: UNC、FTP、HTTP/HTTPS を使用できない場合は、index.ini ファイル、更新されたファイルフィンガープリント、アプリケーション名のファイルを直接次のフォルダにコピーできます。C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager\data\inbox\WhitelistBlacklist\content ファイルは圧縮解除してください。つの Symantec Endpoint Protection Manager は、ファイルを更新するために UNC、FTP、または HTTP/HTTPS を使えない場合は、このフォルダを確認します。
ステップ 4: 管理コンソールで許可リストと拒否リストの自動更新を有効にする	つの Symantec Endpoint Protection Manager コンソールで、既存の許可リストまたは拒否リストの自動更新を有効にする必要があります。 つの Symantec Endpoint Protection Manager の [ファイルフィンガープリントの更新] ダイアログを使って更新機能を有効にし、スケジュールと URL 情報を指定します。 システムロックダウンの許可リストと拒否リストの自動更新の有効化

手順	説明
ステップ 5: 許可リストまたは拒否リストの自動更新の状態を確認する	コンソールで状態を確認することにより、つの Symantec Endpoint Protection Manager が更新を完了したことを確認できます。 コンソールで次のいずれかの処理を実行します。 • [管理] タブで、サイトを選択します。「リビジョン「20200528 R016 説明」の許可リストおよび拒否リストの更新が正常に完了しました」のようなメッセージが表示されます。 • [監視] タブで、[システムログ: サーバー活動] を表示します。通常、イベントの種類は [ファイルフィンガープリントの更新] のように表示されます。 • [ポリシー] タブの [ポリシーコンポーネント] で、ファイルフィンガープリントリストの説明を確認します。説明は、「リビジョン: 20200528 R016 説明」のように表示されます。

つの Symantec Endpoint Protection Manager でのファイルフィンガープリントリストの手動更新 システムロックダウンの設定

システムロックダウンで使用される許可リストと拒否リストの自動更新のための index.ini ファイルの作成

自動更新機能には index.ini ファイルが必要です。このファイルは、任意のテキストエディタで作成できます。

NOTE

このテキストファイルにアルファベット以外の文字を使う場合は、バイトオーダーマーク (BOM) なしの UTF-8 文字を使ってファイルを編集して保存してください。

index.ini ファイルでは、次の項目が指定されます。

- 更新されたファイルフィンガープリントリストとアプリケーション名リストが含まれる圧縮ファイルのリビジョンと名前。
- 更新するファイルフィンガープリントリストとアプリケーション名リストの名前。
- アプリケーション名リストを使うクライアントグループの名前。

既存のファイルフィンガープリントリストまたはグループが現在 Symantec Endpoint Protection Manager に存在している必要があります。グループでシステムロックダウンが有効になっている必要があります。ファイルフィンガープリントリストやアプリケーション名リストが、指定した圧縮ファイルで利用できる必要があります。

index.ini を次の構文で構成する必要があります。

```
[Revision]
Revision=YYYYMMDD RXXX
SourceFile=zip file name
Description=optional description
```

```
[FingerprintList - domain name or Default]
existing fingerprint list="updated list" REPLACE/APPEND/REMOVE
```

```
[ApplicationNameList - domain name or Default]existing group path="updated list" REPLACE/APPEND/REMOVE
```

たとえば、次のように index.ini ファイルの行を使用できます。

```
[Revision]
Revision=20111014 R001
SourceFile=20110901 R001.zip
```

```
Description=NewUpdates

[FingerprintList - Default]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - Default]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE

[FingerprintList - DomainABC]
FingerprintListName 1="FingerprintList1.txt" REPLACE
FingerprintListName 2="FingerprintList2.txt" REPLACE

[ApplicationNameList - DomainABC]
My Company\Group AA\Group AA 1="ApplicationNameList1.txt" REPLACE
My Company\Group AA\Group AA 2="ApplicationNameList2.txt" REPLACE
```

システムロックダウン用に許可または遮断するファイルフィンガープリントリストの自動更新 システムロックダウン設定にインポートするアプリケーション名リストの作成

システムロックダウンの許可リストと拒否リストの自動更新の有効化

システムロックダウンに使う許可リスト (ホワイトリスト) と拒否リスト (ブラックリスト) を自動的に更新するように つの Symantec Endpoint Protection Manager を設定できます。

[ファイルフィンガープリントリストの収集] コマンドで生成したファイルフィンガープリントリストを自動的に更新するには、まずこのコマンドを実行します。

1. コンソールの [管理] タブで、[サーバー] をクリックします。
2. 関連するサーバーを右クリックして、[サーバーのプロパティを編集] を選択します。
3. [サーバープロパティ] ダイアログボックスで、[ファイルフィンガープリントの更新] タブを選択します。
4. [ファイルフィンガープリントの更新] タブで、[許可リストまたは拒否リストの自動更新] にチェックマークを付けます。
5. index.ini と圧縮ファイルの場所を示す URL を入力します。
UNC または FTP を使う場合、index.ini とコンテンツの両方のユーザー名とパスワードを指定する必要があります。
6. [スケジュール] で、つの Symantec Endpoint Protection Manager による許可リストまたは拒否リストの更新頻度を指定できます。
7. [OK] をクリックします。

システムロックダウン用に許可または遮断するファイルフィンガープリントリストの自動更新

システムロックダウンを有効化する前の、システムロックダウンの設定とテスト

通常は、1 週間、またはクライアントが典型的なアプリケーションを実行するのに十分な時間、テストモードでシステムロックダウンを実行します。システムロックダウン設定は、それによってユーザーに問題が生じないと判断した後で、有効にできます。

テストモードでシステムロックダウンを実行するときには、システムロックダウンが無効になります。システムロックダウンはアプリケーションを遮断しません。許可されないアプリケーションは遮断されずにログに記録されるため、リストを確認してからシステムロックダウンを有効化できます。制御ログでログエントリを見ることができます。また、[システムロックダウン] ダイアログボックスで、許可されないアプリケーションを確認することもできます。

NOTE

また、承認済みアプリケーションをクライアントで許可するファイアウォールルールを作成することもできます。

システムロックダウンを有効化する前にシステムロックダウンを設定およびテストするには

1. コンソールで [クライアント] をクリックし、システムロックダウンを設定するグループを [クライアント] で特定します。
2. [ポリシー] タブで、[システムロックダウン] をクリックします。
3. [許可しないアプリケーションだけをログする] をクリックしてシステムロックダウンをテストモードで実行します。
このオプションを使うと、クライアントが現在実行している未承認のアプリケーションに関するログが記録されます。
4. [許可モード] または [拒否モード] を選択します。
これらのオプションは、14.3 RU1 の [ホワイトリストモード] または [ブラックリストモード] から変更されました。
5. [アプリケーションファイルのリスト] の [ファイルフィンガープリントリスト] でファイルフィンガープリントリストを追加または削除します。
リストを追加するには、リストが 1 つの Symantec Endpoint Protection Manager で利用できる必要があります。
[この Symantec Endpoint Protection Manager でのファイルフィンガープリントリストのインポートまたはマージ](#)
6. アプリケーション名リストを追加するには、[アプリケーションファイルのリスト] の [ファイル名] で [インポート] をクリックします。
インポートするアプリケーション名リストを指定し、[インポート] をクリックします。リスト内のアプリケーションが、システムロックダウン設定に個々のエントリとして表示されます。
アプリケーション名のリストは、ファイル名、テストモード、照合モードを指定するテキストファイルである必要があります。
[システムロックダウン設定にインポートするアプリケーション名リストの作成](#)
7. 個々のアプリケーションを追加するには、[アプリケーションファイルのリスト] の [ファイル名] で [追加] をクリックします。
8. [ファイル定義の追加] ダイアログボックスで、ファイル (拡張子が .exe または .dll のファイル) の絶対パス名を指定します。
この名前は、標準文字列または正規表現構文を使って指定できます。ワイルドカード文字として、任意の文字を表すアスタリスク (*)、1 文字を表す疑問符 (?) も使用できます。また、Program Files ディレクトリの場所を表す %ProgramFiles% または Windows インストールディレクトリを表す %windir% などの環境変数も使用できます。
9. デフォルトでは [ワイルドカード一致を使う (* と ? をサポートします)] が選択されています。これをそのまま使うか、ファイル名に正規表現を使った場合は [正規表現の一致を使う] をクリックします。
10. ファイルを特定の種類のドライブで実行する場合にのみ許可するには、[次の種類のドライブ上のファイルのみを照合する] をクリックします。
対象から除外するドライブの種類を選択解除します。デフォルトでは、すべての種類のドライブが選択されています。
11. デバイス ID の種類で照合する場合は、[次の ID で識別される種類のデバイス上にあるファイルのみを照合する] にチェックマークを付け、[選択] をクリックします。
12. リスト中で目的のデバイスをクリックし、[OK] をクリックします。
13. [OK] をクリックしてテストを開始します。

しばらくすると、承認されていないアプリケーションのリストを見ることができます。[<グループ名> のシステムロックダウン] ダイアログボックスを再度開くと、テストが実行されていた時間を確認できます。

テストでログに記録されたが遮断はされていない未承認のアプリケーションを確認するには

1. [<グループ名> のシステムロックダウン] ダイアログボックスで、[未承認アプリケーションの表示] をクリックします。

-
2. [未承認のアプリケーション] ダイアログボックスで、アプリケーションを確認します。
このリストには、アプリケーションの実行時刻、コンピュータホスト名、クライアントユーザー名、実行ファイル名の情報が含まれます。
 3. この未承認アプリケーションをどのように処理するかを決定します。
許可モードの場合は、許可するアプリケーションの名前を承認済みアプリケーションのリストに追加できます。拒否モードの場合は、許可するアプリケーションの名前を削除できます。
 4. ファイルフィンガープリントリストまたは個々のアプリケーションを変更した場合にテストを再度実行するには、[未承認のアプリケーション] ダイアログボックスで [テストのリセット] をクリックします。そうでない場合は、[閉じる] をクリックします。
 5. テストが終了したら、システムロックダウンを有効にできます。

システムロックダウンの設定

許可モードでのシステムロックダウンの実行

システムロックダウンを設定して、承認されたアプリケーションのみをクライアントコンピュータで許可できます。承認済みリストにあるアプリケーションのみが、実行を許可されます。他のアプリケーションはすべて遮断されます。承認済みリストは許可リスト (ホワイトリスト) と呼ばれます。承認済みアプリケーションは、Symantec Endpoint Protection の他の保護機能の対象になります。

NOTE

デフォルトでは、許可モードを有効化すると、システムロックダウンはそのモードで実行されます。

以下の条件を満たす場合にのみ、許可モードで実行されるようにシステムロックダウンを設定する必要があります。

- [許可しないアプリケーションだけをログする] オプションを使ってシステムロックダウン設定をテストした。
- クライアントコンピュータで実行する必要があるアプリケーションがすべて、承認済みアプリケーションリストに記されていることが確実である。

WARNING

システムロックダウンからファイルフィンガープリントリストまたは特定のアプリケーションを追加または削除するときは、注意してください。システムロックダウンの項目を追加または削除すると危険な場合があります。クライアントコンピュータ上の重要なアプリケーションが遮断される可能性があります。

システムロックダウンを有効化する前の、システムロックダウンの設定とテスト

NOTE

許可モードでシステムロックダウンを有効にして実行する場合、つの Symantec Endpoint Protection Manager は Symantec EDR から遮断したアプリケーションを適用しません。

システムロックダウンと Symantec EDR 拒否リスト (ブラックリスト) ルールとの対話

許可モードでシステムロックダウンを実行するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、システムロックダウンを設定するグループを選択します。
サブグループを選択する場合は、親グループで継承が無効になっている必要があります。

-
3. [ポリシー] タブで、[システムロックダウン] をクリックします。
 4. [システムロックダウン] で、[システムロックダウンを有効にする] を選択してクライアントが実行しようとしている未承認のアプリケーションを遮断します。
 5. [アプリケーションファイルのリスト] で、[許可モード] (14.3 MP1 以前では [ホワイトリストモード]) を選択します。
 6. [承認済みアプリケーション] で、クライアントコンピュータで実行するすべてのアプリケーションが含まれていることを確認します。

WARNING

クライアントコンピュータで実行するすべてのアプリケーションを承認済みアプリケーションリストに含める必要があります。含めていない場合、一部のクライアントコンピュータが再起動できなくなったり、ユーザーが重要なアプリケーションを実行できなくなる可能性があります。

7. クライアントがアプリケーションを遮断したときに、クライアントコンピュータにメッセージを表示するには、[アプリケーションを遮断した場合にユーザーに通知する] にチェックマークを付けます。
8. [OK] をクリックします。

システムロックダウンの設定

グループの継承の無効化

拒否モードでのシステムロックダウンの実行

システムロックダウンを有効にして、リストに含まれる未承認アプリケーションをクライアントコンピュータで遮断できます。未承認リストに含まれるすべてのアプリケーションが遮断されます。未承認リストは拒否リスト (ブラックリスト) と呼ばれます。他のアプリケーションはすべて許可されます。許可されたアプリケーションは、Symantec Endpoint Protection の他の保護機能の対象になります。

NOTE

ネットワークで Symantec EDR を実行する場合、Symantec EDR の設定はシステムロックダウンの許可リストの設定に影響します。

システムロックダウンと Symantec EDR ブラックリストルールとの対話

次の条件に該当した後でのみ、システムロックダウンが未承認アプリケーションを遮断するように設定してください。

- [許可しないアプリケーションだけをログする] オプションを使ってシステムロックダウン設定をテストした。
- クライアントコンピュータで遮断する必要のあるすべてのアプリケーションが、未承認アプリケーションリストに含まれていることを確認した。

システムロックダウンを有効化する前の、システムロックダウンの設定とテスト

WARNING

システムロックダウンからファイルフィンガープリントリストまたは特定のアプリケーションを追加または削除するときは、注意してください。システムロックダウンの項目を追加または削除すると危険な場合があります。クライアントコンピュータ上の重要なアプリケーションが遮断される可能性があります。

ブラックリストモードでのシステムロックダウンの実行

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] で、システムロックダウンを設定するグループを選択します。
サブグループを選択する場合は、親グループで継承が無効になっている必要があります。

グループの継承の無効化

3. [ポリシー] タブで、[システムロックダウン] を選択します。
4. [システムロックダウン] ダイアログボックスで、[システムロックダウンを有効にする] を選択します。
5. [アプリケーションファイルのリスト] で、[拒否モード] を選択します。このオプションは、14.3 MP1 以前の [ブラックリストモード] です。
6. [未承認のアプリケーション] で、クライアントコンピュータで遮断する必要があるすべてのアプリケーションが含まれていることを確認します。

NOTE

多数のアプリケーションを指定すると、クライアントコンピュータのパフォーマンスが低下する可能性があります。

7. クライアントがアプリケーションを遮断したときに、クライアントコンピュータにメッセージを表示するには、[アプリケーションを遮断した場合にユーザーに通知する] にチェックマークを付けます。
8. [OK] をクリックします。

システムロックダウンを有効化する前の、システムロックダウンの設定とテスト

システムロックダウンの設定

デバイス制御の管理

デバイス制御は、クライアントコンピュータでどのハードウェアデバイスを許可し、遮断するかを指定します。デフォルトのハードウェアデバイスのリストと、デバイス制御ポリシーを使ってデバイス制御を管理します。独自に追加することもできます。

Table 121: デバイス制御の管理

手順	説明
つの Symantec Endpoint Protection Manager のデフォルトのハードウェアデバイスのリストを確認する	デフォルトでは、つの Symantec Endpoint Protection Manager にはハードウェアデバイスのリストが含まれています。リストは つの Symantec Endpoint Protection Manager で、[ポリシーコンポーネント] の [ポリシー] タブに表示されます。このリストを使って、クライアントコンピュータ上で制御するデバイスを選択します。 リストに含まれていないデバイスを制御したい場合は、最初にデバイスを追加する必要があります。 ハードウェアデバイスのリストについて
ハードウェアデバイスのリストにデバイスを追加する (必要な場合)	デバイスリストにデバイスを追加するときには、デバイスのクラス ID またはデバイス ID が必要です。 Mac 用にカスタマイズしたデバイスを追加することはできません。使用できるのは提供されているデバイスの種類のみです。 ハードウェアデバイスリストへのハードウェアデバイスの追加 DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得
デバイス制御ポリシーのデバイスの許可または遮断	クライアントでアクセスされることを許可または遮断するデバイスを指定します。 クライアントコンピュータのデバイスの許可または遮断

Mac クライアントの場合には、デバイス制御は SymDaemon サービスに含まれます。デバイス制御を機能させるために、Windows クライアントまたは Mac クライアントを再起動する必要はありません。

アプリケーション制御、システムロックダウン、デバイス制御について

クライアントコンピュータのデバイスの許可または遮断

デバイス制御を設定するには、アプリケーションとデバイス制御ポリシーを使います。開始する前に、必要なデバイスをハードウェアデバイスリストに追加します。

ハードウェアデバイスリストへのハードウェアデバイスの追加

14 では、Windows と Mac の両方のデバイス制御を設定できます。

1. オプション 1: Windows クライアントのデバイス制御を設定するには、コンソールで [アプリケーションとデバイス制御] ポリシーを開きます。
2. [デバイス制御] をクリックします。
3. [遮断するデバイス] で [追加] をクリックします。
4. [デバイス選択] ウィンドウで、1 つ以上のデバイスを選択します。必要に応じて、特定のポートを遮断してデバイスを除外しているかどうかを確認します。

NOTE

通常は、キーボードを遮断しないでください。

5. [OK] をクリックします。
6. [遮断から除外するデバイス] で [追加] をクリックします。
7. [デバイス選択] ウィンドウで、1 つ以上のデバイスを選択します。
8. ユーザーに通知する場合は、[デバイスを遮断したときにユーザーに通知する] にチェックマークを付けます。
9. [OK] をクリックします。
10. オプション 2: Mac クライアントのデバイス制御を設定するには (14 現在)、コンソールで [アプリケーションとデバイス制御] ポリシーを開きます。
11. [Mac の設定] で、[デバイス制御] をクリックします。
12. [遮断するデバイス] で [追加] をクリックします。
13. [デバイス選択] ウィンドウで、リストからデバイスを選択します。一度に追加できるデバイスは 1 つだけです。

ウィンドウの下部のフィールドが利用可能な場合は、それに記入します。フィールドを空白のままにすると、この種類のすべてのデバイスが遮断されます。

デバイスの製造元、デバイスモデル、またはシリアル番号を定義するために正規表現を使うこともできます。詳しくは、[Mac のデバイス制御] ウィンドウのヘルプを参照してください。

Mac に接続したデバイスのシリアル番号、モデル番号、製造元の名前を入手するには、インストールファイルから DeviceInfo ツールを使います。このツールとその操作手順は `Tools/DeviceInfo` にあります。

14. [OK] をクリックします。
15. [遮断から除外するデバイス] で [追加] をクリックします。
16. [デバイス選択] ウィンドウで、リストからのデバイスを選択し、除外されたデバイスを定義し、[OK] をクリックします。
17. ユーザーに通知する場合は、[デバイスを遮断したときにユーザーに通知する] にチェックマークを付けます。
18. [OK] をクリックします。

Mac デバイス制御

デバイス制御の管理

アプリケーション制御、システムロックダウン、デバイス制御について

ハードウェアデバイスのリストについて

つの Symantec Endpoint Protection Manager には、ハードウェアデバイスのリストが含まれています。いくつかのデバイスはデフォルトでリストに含まれています。デバイス制御を設定するときにはデバイスを使います。

デバイス制御の管理

リストにデバイスを追加できます。デフォルトのデバイスの編集や削除はできません。

Mac 用にカスタマイズしたハードウェアデバイスを追加することはできません。

デバイスはデバイス ID またはクラス ID によって識別されます。これらの値のどちらかを使って、リストにデバイスを追加します。デバイス ID またはクラス ID の判別ツールを使うことができます。Windows の場合は、Tools\DevViewer に移動します。Mac の場合は、Tools\DeviceInfo に移動します。

DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得

クラス ID	クラス ID は、Windows GUID を表します。デバイスの各種類には、Class と ClassGuid の両方が関連付けられています。ClassGuid は、以下の形式の 16 進数値です。 {00000000-0000-0000-0000-000000000000}
デバイス ID	デバイス ID は、デバイスに最も固有の ID です。デバイス ID の構文にはクラス ID よりも読み取りを容易にする説明的な文字列が含まれます。 デバイス ID を追加する場合は、デバイスの固有の ID を使うことができます。また、デバイス ID 文字列内でワイルドカード文字を使って指定するデバイスグループの範囲を広げることができます。ゼロ文字以上の任意の値を示すにはアスタリスク (*) を、1 文字の任意の値を示すには疑問符 (?) を使用できます。 特定の USB SanDisk デバイスのデバイス ID を次に示します。 USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0 任意の USB SanDisk デバイスを示すワイルドカードを含んだデバイス ID を次に示します。 USBSTOR\DISK&VEN_SANDISK* 任意の USB ディスクデバイスを示すワイルドカードを含んだデバイス ID を次に示します。 USBSTOR\DISK* 任意の USB ストレージデバイスを示すワイルドカードを含んだデバイス ID を次に示します。 USBSTOR*

DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得

クラス ID (GUID) またはデバイス ID を取得するためにシマンテック社の DevViewer ツールを使うことができます。デバイス ID を取得するために Windows のデバイスマネージャを使うことができます。

デバイス ID を取得したら、ワイルドカード文字を使ってデバイスの特定のグループを示すように修正できます。

1. クラス ID またはデバイス ID を DevViewer ツールを使って取得するには、[Broadcom ダウンロードセンター](#)から入手した完全な製品インストールファイルで Tools\DevViewer フォルダを検索して、クライアントコンピュータに DevViewer.exe ツールをコピーします。
2. クライアントコンピュータで、DevViewer.exe を実行します。
3. [Device Tree] を展開し、デバイス ID か GUID を取得するデバイスを検索します。
たとえば、[ディスクドライブ] を展開し、そのカテゴリ内のデバイスを選択します。

-
4. 右側のペインで、デバイス ID ([device ID] で始まる) を右クリックし、[デバイス ID をコピー] を選択します。
 5. [Exit] をクリックします。
 6. 管理サーバーで、ハードウェアデバイスのリストにデバイス ID を貼り付けます。
 7. コントロールパネルからデバイス ID を取得するには、コントロールパネルからデバイスマネージャを開きます。
デバイスマネージャへのパスは Windows オペレーティングシステムによって決まります。たとえば、Windows 7 ではスタートメニューで [コントロールパネル]、[システム]、[デバイスマネージャ] の順に選択します。
 8. [デバイスマネージャ] ダイアログボックスでデバイスを右クリックし、[プロパティ] をクリックします。
 9. そのデバイスの [プロパティ] ダイアログボックスの [詳細] タブで、[デバイス ID] を選択します。
デフォルトでは、最初に表示される値がそのデバイスのデバイス ID になります。
 10. ID 文字列をコピーします。
 11. [OK] をクリックします。

ハードウェアデバイスリストへのハードウェアデバイスの追加

クラス ID について

デバイス ID について

クラス ID について

クラス ID は、Windows GUID を表します。デバイスの各種類には、Class と ClassGuid の両方が関連付けられています。ClassGuid は、以下の形式の 16 進数値です。

```
{00000000-0000-0000-0000-000000000000}
```

DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得

デバイス ID について

デバイス ID は、デバイスに最も固有の ID です。デバイス ID の構文にはクラス ID よりも読み取りを容易にする説明的な文字列が含まれます。

デバイス ID を追加する場合は、デバイスの固有の ID を使うことができます。また、デバイス ID 文字列内でワイルドカード文字を使って指定するデバイスグループの範囲を広げることができます。ゼロ文字以上の任意の値を示すにはアスタリスク (*) を、1 文字の任意の値を示すには疑問符 (?) を使用できます。

特定の USB SanDisk デバイスのデバイス ID を次に示します。

```
USBSTOR\DISK&VEN_SANDISK&PROD_CRUZER_MICRO&REV_2033\0002071406&0
```

任意の USB SanDisk デバイスを示すワイルドカードを含んだデバイス ID を次に示します。

```
USBSTOR\DISK&VEN_SANDISK*
```

任意の USB ディスクデバイスを示すワイルドカードを含んだデバイス ID を次に示します。

```
USBSTOR\DISK*
```

任意の USB ストレージデバイスを示すワイルドカードを含んだデバイス ID を次に示します。

```
USBSTOR*
```

DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得

ハードウェアデバイスリストへのハードウェアデバイスの追加

ハードウェアデバイスのクラス ID またはデバイス ID を取得したら、デフォルトのハードウェアデバイスリストにハードウェアデバイスを追加できます。これによってアプリケーションとデバイス制御ポリシーのデバイス制御部分からこのデフォルトリストにアクセスできます。

ハードウェアデバイスのリストについて

ハードウェアデバイスリストにハードウェアデバイスを追加するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシー] で、[ポリシーコンポーネント] を展開し、[ハードウェアデバイス] をクリックします。
3. [タスク] で、[ハードウェアデバイスの追加] をクリックします。
4. 追加するデバイスの名前を入力します。

クラス ID とデバイス ID はいずれも規約に従い波カッコ ({ }) で囲みます。場合によっては、波カッコをワイルドカード文字 (?) に置き換える必要があります。

5. [クラス ID] または [デバイス ID] を選択し、Windows のデバイスマネージャまたは DevViewer ツールからコピーした ID を貼り付けます。
6. ワイルドカード文字を使ってデバイス ID セットを定義できます。たとえば、文字列 *IDE\DVDROM* を使うことができます。

[DevViewer がインストールされた Windows コンピュータのデバイス製造元またはモデルの取得](#)

7. [OK] をクリックします。

Symantec Endpoint Protection の例外の管理

Symantec Endpoint Protection コンソールで、つの Symantec Endpoint Protection Manager の例外を管理できます。

Table 122: 例外の管理

タスク	説明
例外について学習する	クライアントコンピュータのスキャンから項目を除外するには、例外を使います。
Symantec Endpoint Protection がスキャンから自動的に除外するファイルとフォルダの種類を確認する	Symantec Endpoint Protection は一部のサードパーティアプリケーションとシマンテック製品について、例外（除外）を自動的に作成します。 特定の拡張子のみをスキャンし、他の拡張子はすべてスキップするように個々のスキャンを設定することもできます。 Symantec Endpoint Protection がウイルススキャンとスパイウェアスキャンから除外するファイルとフォルダについて
スキャンの例外を作成する	例外は、例外ポリシーに直接追加します。または [監視] ページで、ロギイベントから例外を追加できます。 ウイルスとスパイウェアのスキャンの例外作成 ロギイベントに基づく例外の作成
クライアントコンピュータでユーザーが設定できる例外の種類の制限（Windows のみ）	デフォルトでは、クライアントコンピュータ上のユーザーが例外に対して持つ設定権限には限度があります。ユーザーがウイルスとスパイウェアのスキャンの例外、または SONAR の例外を作成できないように制限できます。 ユーザーは、アプリケーション検出を強制することはできず、改変対策例外を作成する権限を持つこともありません。 ユーザーはまた、アプリケーション制御のためのファイル例外を作成できません。 クライアントコンピュータでユーザーが設定できる例外の種類の制限

タスク	説明
例外を作成する可能性がある検出のログを確認する	Symantec Endpoint Protection によって検出が行われたら、ログイベントから検出の例外を作成できます。 たとえば、スキャンで検出されるがユーザーがダウンロードを要求しているファイルの例外を作成したい場合があります。 ログイベントに基づく例外の作成
侵入防止シグネチャの例外を作成する	侵入防止について例外を指定できます。 侵入防止で除外されるホストのリストも設定できます。 侵入防止例外は、侵入防止ポリシーで設定します。 IPS シグネチャの例外の作成

使用する Windows 例外と、適用するスキャンの種類について

「[例外名](#)」に、バージョン 14 MPx 以前を対象として、例外ポリシーで使用される例外の種類と、適用するスキャンの種類を示します。

Table 123: 例外名

つの Symantec Endpoint Protection Manager	クライアント制限 (つの Symantec Endpoint Protection Manager 上)*	Windows クライアント	例外の使用対象
アプリケーション	アプリケーション例外	アプリケーション例外	- Auto-Protect - 手動スキャン - 定時スキャン - ダウンロードインサイト - SONAR
監視するアプリケーション	利用不能	利用不能	アプリケーション制御
証明書	利用不能	利用不能	- Auto-Protect - 手動スキャン - 定時スキャン - ダウンロードインサイト - SONAR
DNS またはホストファイルの変更	DNS またはホストファイルの変更例外	[DNS またはホストファイルの変更例外] > [アプリケーション]	SONAR
拡張子	拡張子例外	[セキュリティリスク例外] > [拡張子]	- Auto-Protect - 手動スキャン - 定時スキャン
ファイル	ファイル例外	[セキュリティリスク例外] > [ファイル]	- Auto-Protect - 手動スキャン - 定時スキャン - SONAR - アプリケーション制御
ファイルアクセス	ファイルアクセス		アプリケーション制御
フォルダ	フォルダ例外: - セキュリティリスク例外 - SONAR 例外	[セキュリティリスク例外] > [フォルダ SONAR 例外]	- Auto-Protect - 手動スキャン - 定時スキャン - SONAR - アプリケーション制御

つの Symantec Endpoint Protection Manager	クライアント制限 (つの Symantec Endpoint Protection Manager 上)*	Windows クライアント	例外の使用対象
既知のリスク	既知のリスク例外	[セキュリティリスク例外] > [既知のリスク]	- Auto-Protect - 手動スキャン - 定時スキャン - SONAR
信頼できる Web ドメイン	信頼できる Web ドメイン例外	[セキュリティリスク例外] > [Web ドメイン]	ダウンロードインサイト
改変対策例外	利用不能	利用不能	改変対策で保護されるアプリケーション

*クライアント制限については、クライアントユーザーによる例外の追加対象としてクライアントで表示するか非表示にするかを切り替えることができます。クラウドコンソールに追加する例外は、クライアントでの有効化と無効化を つの Symantec Endpoint Protection Manager で制御することはできません。

[クライアントコンピュータでユーザーが設定できる例外の種類の制限](#)

[つの Symantec Endpoint Protection Manager 例外ポリシーとクラウドコンソールの連携方法について](#)

ウイルスとスパイウェアのスキャンの例外作成

Symantec Endpoint Protection には異なる種類の例外を作成できます。

管理者が作成するどの例外も、ユーザーが定義することがある例外よりも優先されます。クライアントコンピュータで、ユーザーは管理者が作成する例外を表示できません。ユーザーは自分が作成した例外のみを表示できます。

ウイルスとスパイウェアのスキャンの例外もダウンロードインサイトに適用されます。

Table 124: Symantec Endpoint Protection の例外の作成

タスク	説明
ウイルススキャンとスパイウェアスキャンからファイルを除外する	Windows クライアントと Mac クライアントでサポートされます。 ファイル名を指定して、Windows クライアントのウイルスとスパイウェアのスキャン、SONAR、またはアプリケーション制御からファイルを除外します。 スキャンからのファイルまたはフォルダの除外
ウイルススキャンとスパイウェアスキャンからフォルダを除外する	Windows、Mac、Linux クライアントでサポートされます。 Windows クライアントでは、ウイルススキャンとスパイウェアスキャン、SONAR、すべてのスキャンからフォルダを除外します。 Windows クライアントと Linux クライアントでは、ウイルススキャンとスパイウェアスキャンの例外を Auto-Protect スキャン、定時スキャン、オンデマンドスキャンに限定できます。数多くの一時ファイルをフォルダに書き込むアプリケーションを実行する場合は、そのフォルダを Auto-Protect から除外できます。Auto-Protect はファイルの書き込み時にファイルをスキャンするため、例外を定時スキャンとオンデマンドスキャンに制限することでコンピュータパフォーマンスを向上できます。 頻繁に使われないフォルダ、アーカイブまたはバックされたファイルを定時スキャンとオンデマンドスキャンから除外できます。たとえば、頻繁に使われない深くアーカイブされたファイルの定時スキャンまたはオンデマンドスキャンは、コンピュータのパフォーマンスを低下させる場合があります。ただし、Auto-Protect はフォルダのファイルがアクセスされたり、フォルダに書き込まれた場合のみスキャンを行うことでフォルダを保護できます。 スキャンからのファイルまたはフォルダの除外

タスク	説明
ウイルススキャンとスパイウェアスキャンから既知のリスクを除外する	Windows クライアントでサポートされます。 ウイルススキャンとスパイウェアスキャンから既知のリスクを除外します。スキャンはリスクを無視しますが、スキャンによる検出がログに記録されるように例外を設定できます。どちらの場合も、クライアントソフトウェアは指定したリスクの検出時にユーザーに通知しません。 無視するように設定した既知のリスクに対してユーザーがカスタム処理を設定している場合、Symantec Endpoint Protection はカスタム処理を無視します。 セキュリティリスク例外は SONAR には適用されません。 Windows クライアントのウイルススキャンとスパイウェアスキャンから既知のリスクを除外する
ウイルススキャンとスパイウェアスキャンから拡張子を除外する	Windows クライアントと Mac クライアントでサポートされます。 ウイルススキャンとスパイウェアスキャンから、指定した拡張子が付いているファイルを除外します。 拡張子の例外は SONAR と Power Eraser に適用されません。 Windows クライアントと Linux クライアントのウイルススキャンとスパイウェアスキャンからファイル拡張子を除外する
アプリケーションの例外を作成するためにアプリケーションを監視する	Windows クライアントでサポートされます。 特定のアプリケーションを監視するには、[監視するアプリケーション] の例外を使います。Symantec Endpoint Protection がアプリケーションを学習したら、Symantec Endpoint Protection でアプリケーションを処理する方法を指定するための例外を作成できます。 アプリケーションの学習を無効にした場合、[監視するアプリケーション] の例外は、指定するアプリケーションのアプリケーション学習を強制します。 Windows クライアントのアプリケーションの例外を作成するためのアプリケーションの監視
ウイルススキャンとスパイウェアスキャンで監視対象アプリケーションを処理する方法を指定する	Windows クライアントでサポートされます。 Symantec Endpoint Protection が監視対象アプリケーションに適用する処理を指定するには、アプリケーション例外を使います。Symantec Endpoint Protection は、アプリケーションの検出時、またはアプリケーションの実行時に、処理の種類によってその処理を適用するかどうかを判断します。Symantec Endpoint Protection は、アプリケーションの起動時や実行時に、アプリケーションに終了、検疫、削除の処理を適用します。[ログのみ] と [無視] 処理は、アプリケーションの検出時に適用します。 ファイル名の例外とは違って、アプリケーション例外はハッシュベースの例外です。異なるファイルに同じ名前が付いている場合がありますが、ファイルハッシュはアプリケーションを一意に識別します。 アプリケーション例外は SHA-2 ハッシュベースの例外です。 例外を作成できるアプリケーションは、Symantec Endpoint Protection でのアプリケーションの学習の後で、[例外] ダイアログに表示されます。Symantec Endpoint Protection が学習する特定のアプリケーションを監視するように要求できます。 Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定する クライアントコンピュータで実行するアプリケーションに関する情報の収集
ウイルススキャンとスパイウェアスキャンから Web ドメインを除外する	Windows クライアントでサポートされます。 ダウンロードインサイトは、ユーザーが Web サイトやその他のポータルからのダウンロードを試みるファイルをスキャンします。ダウンロードインサイトはウイルススキャンとスパイウェアスキャンの一部として実行されます。安全だとわかっている特定の Web ドメインの例外を設定できます。 例外を有効にするには、ダウンロードインサイトが有効になっている必要があります。 Note: クライアントコンピュータで、認証が必要なプロキシを使用する場合、シマンテック URL に信頼できる Web ドメイン例外を指定する必要があります。例外により、クライアントコンピュータは Symantec Insight と他の重要なシマンテック社のサイトと通信できます。 次の記事を参照してください。 • ライセンスサーバーやダウンロードインサイトサーバーへの接続をテストする方法 • SEP で Symantec のレピュテーションサーバおよびライセンスサーバと通信するために推奨されるプロキシサーバの Web ドメイン除外指定について Windows クライアントのスキャンからの信頼できる Web ドメインの除外

タスク	説明
改変対策のファイル例外を作成する	Windows クライアントでサポートされます。 改変対策はシマンテックのプロセスと内部オブジェクトを改変するプロセスからクライアントコンピュータを保護します。改変対策はシマンテックの設定や Windows のレジストリ値を修正する可能性のあるプロセスを検出すると、そのプロセスを遮断します。 サードパーティアプリケーションが、何らかの理由でシマンテックのプロセスや設定を修正を試みる場合があります。場合によっては、アプリケーションがシマンテックの設定を修正できるようにする必要があります。クライアントコンピュータ上のレジストリの一定の領域または一定のファイルについて改変対策を停止すると便利です。 場合によっては、改変対策がスクリーンリーダーなどの支援技術アプリケーションを遮断することがあります。このようなアプリケーションをクライアントコンピュータで実行できるようにするには、ファイル例外を作成します。フォルダ例外は、改変対策ではサポートされません。 Windows クライアントの改変対策例外の作成
DNS またはホストファイルの変更をアプリケーションに許可する	Windows クライアントでサポートされます。 アプリケーションが DNS またはホストファイルを変更するための例外を作成できます。通常、SONAR では DNS やホストファイルの変更のようなシステム変更は防止されます。たとえば、VPN アプリケーションのための例外を作成することが必要な場合があります。 DNS またはホストファイルを変更するアプリケーションのための例外の作成
証明書を除外する	Windows クライアントでサポートされます (14.0.1 以降)。 証明書をスキャンから除外できます。証明書を除外することで、疑わしいファイルとしてフラグが付けられないようにできます。たとえば、ダウンロードインサイトのスキャンによって、内部ツールの自己署名証明書が疑わしいファイルとしてフラグが付けられる可能性があります。 Windows クライアントのスキャンからの証明書の除外

Symantec Endpoint Protection の例外の管理

ログイベントに基づく例外の作成

スキャンからのファイルまたはフォルダの除外

ファイルやフォルダの例外は個別に追加します。複数のファイルに対して例外を作成する場合は、手順を繰り返します。

Windows クライアントと Mac クライアントの両方に、ファイルまたはフォルダの例外を設定できます。Windows クライアントでは、ファイル例外をウイルスとスパイウェアスキャン、SONAR、アプリケーション制御に適用できます。フォルダ例外はウイルスとスパイウェアのスキャンと SONAR に適用されます。

- オプション 1: Windows クライアントでスキャンからファイルを除外するには、[例外ポリシー] ページで、[例外] をクリックします。
- [例外] で、[追加]、[Windows の例外]、[ファイル] の順にクリックします。
- [プレフィックス変数] ドロップダウンボックスで、共通のフォルダを選択します。
絶対パスとファイル名を入力する場合には [なし] を選択します。
プレフィックスを選択するときは、例外を異なる Windows オペレーティングシステムで使うことができます。
- [ファイル] テキストボックスに、ファイル名を入力します。
プレフィックス変数を選択する場合、パス名はプレフィックスに関連したものにします。[なし] を選択した場合は、絶対パス名を入力します。

NOTE

パスは円記号を使って示す必要があります。

-
5. [このファイルを除外するスキャンの種類を指定します] で、スキャンの種類 ([セキュリティリスク]、[SONAR]、または [アプリケーション制御]) を選択します。
少なくとも 1 つの種類を選択する必要があります。
 6. セキュリティリスクスキャンの場合は、[セキュリティリスクスキャンの種類を選択してください] で、[Auto-Protect]、[定時とオンデマンド]、または [すべてのスキャン] を選択します。
例外を特定の種類のセキュリティリスクスキャンに限定する理由についてはヘルプを参照してください。
 7. [OK] をクリックします。
 8. オプション 2: Windows クライアントでスキャンからフォルダを除外するには、[例外ポリシー] ページで、[例外] をクリックします。
 9. [例外] で、[追加]、[Windows の例外]、[フォルダ] の順にクリックします。
 10. [プレフィックス変数] ドロップダウンボックスで、共通のフォルダを選択します。
絶対パスとファイル名を入力する場合には [なし] を選択します。
プレフィックスを選択するときは、例外を異なる Windows オペレーティングシステムで使うことができます。
 11. [フォルダ] テキストボックスに、フォルダ名を入力します。
プレフィックス変数を選択する場合、パス名はプレフィックスに関連したものにします。[なし] を選択した場合は、絶対パス名を入力します。

NOTE

パスは円記号を使って示す必要があります。

12. [このフォルダを除外するスキャンの種類を指定してください] で、スキャンの種類 ([セキュリティリスク]、[SONAR]、[アプリケーション制御]、[すべてのスキャン] のいずれか) を選択します。
少なくとも 1 つの種類を選択する必要があります。
13. セキュリティリスクスキャンの場合は、[セキュリティリスクスキャンの種類を選択してください] で、[Auto-Protect]、[定時とオンデマンド]、または [すべてのスキャン] を選択します。
例外を特定の種類のセキュリティリスクスキャンに限定する理由についてはヘルプを参照してください。
14. [OK] をクリックします。
15. オプション 3: Mac クライアントでスキャンからファイルまたはフォルダを除外するには、[例外ポリシー] ページで、[例外] をクリックします。
16. [例外] で、[追加] > [Mac の例外] > [ファイルまたはフォルダのセキュリティリスク例外] の順にクリックします。
17. [セキュリティリスクのファイルまたはフォルダの例外] の [プレフィックス変数] ドロップダウンボックスで、共通のフォルダを選択します。
絶対パスとファイル名を入力する場合には [なし] を選択します。
18. [ファイル] または [フォルダ] テキストボックスに、ファイルまたはフォルダの名前を入力します。
プレフィックス変数を選択する場合、パス名はプレフィックスに関連したものにします。[なし] を選択した場合は、絶対パス名を入力します。

NOTE

フォルダのパスはスラッシュを使って示す必要があります。

-
19. [OK] をクリックします。
 20. オプション 4: Linux クライアントでスキャンからフォルダを除外するには、[例外ポリシー] ページで、[例外] をクリックします。
 21. [例外] で、[追加]、[Linux の例外] の順にクリックします。
 22. [フォルダ] をクリックします。
 23. [フォルダ例外の追加] のダイアログボックスで、プレフィックス変数を選択し、フォルダ名を入力し、サブフォルダを必要に応じて追加できます。

14.3 RU1 以降、オプションの [サブフォルダも除外] は Symantec Agent for Linux ではサポートされません。また、すべてのサブディレクトリは常にスキャンから除外されます。

プレフィックス変数を選択する場合、パス名はプレフィックスに関連したものにします。[なし] を選択した場合は、絶対パス名を入力します。

NOTE

フォルダのパスはスラッシュを使って示す必要があります。

24. セキュリティリスクスキャンの種類を選択してください (Specify the type of security risk scan) [Auto-Protect]、[定時とオンデマンド]、[すべてのスキャン] を選択し、[OK] をクリックします。

ウイルスとスパイウェアのスキャンの例外作成

Windows クライアントと Linux クライアントのウイルススキャンとスパイウェアスキャンからファイル拡張子を除外する

Windows クライアントのウイルススキャンとスパイウェアスキャンから既知のリスクを除外する

クライアントソフトウェアが検出したセキュリティリスクは [既知のセキュリティリスク例外] ダイアログボックスに表示されます。

既知のセキュリティリスクリストにはリスクの重大度に関する情報が含まれています。

Windows クライアントのウイルススキャンとスパイウェアスキャンから既知のリスクを除外するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [例外] で、[追加]、[Windows の例外]、[既知のリスク] の順にクリックします。
3. [既知のセキュリティリスク例外の追加] ダイアログボックスで、ウイルススキャンとスパイウェアスキャンから除外する 1 つ以上のセキュリティリスクを選択します。
4. 検出をログに記録する場合は [セキュリティリスクの検出時にログに記録する] にチェックマークを付けます。
このオプションをチェックしない場合、クライアントは選択したリスクを検出しても無視します。そのためクライアントは検出をログに記録しません。
5. [OK] をクリックします。
6. このポリシーの設定を完了したら、[OK] をクリックします。

ウイルスとスパイウェアのスキャンの例外作成

Windows クライアントと Linux クライアントのウイルススキャンとスパイウェアスキャンからファイル拡張子を除外する

1 つの例外に複数の拡張子を追加できます。例外を作成した後で、同じポリシーに対して別の拡張子の例外は作成できません。既存の例外を編集する必要があります。

一度に追加できる拡張子は 1 つだけです。[追加] テキストボックスに複数の拡張子を入力すると、ポリシーは入力内容を 1 つの拡張子として処理します。

ウイルスとスパイウェアのスキンの例外作成

Windows クライアントと Linux クライアントのウイルススキャンとスパイウェアスキャンからファイル拡張子を除外するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [例外] で、[追加]、[Windows の例外]、[拡張子] または [追加]、[Linux の例外]、[拡張子] の順にクリックします。
3. 除外する拡張子をテキストボックスに入力し、[追加] をクリックします。
4. [セキュリティリスクスキャンの種類を選択してください] で、[Auto-Protect]、[定時とオンデマンド]、[すべてのスキャン] を選択します。
5. 例外にその他任意の拡張子を追加します。
6. [OK] をクリックします。

スキャンからのファイルまたはフォルダの除外

Windows クライアントのアプリケーションの例外を作成するためのアプリケーションの監視

Symantec Endpoint Protection で監視対象アプリケーションが学習されると、そのアプリケーションは [アプリケーション例外] ダイアログに表示されます。例外ポリシーで、アプリケーション用の例外処理を作成できます。アプリケーションは、関連するログにも表示され、ログから例外を作成できます。

アプリケーションの学習を無効にした場合、[監視するアプリケーション] の例外は、指定したアプリケーションのアプリケーション学習を強制します。

Windows クライアントのアプリケーションの例外を作成するためにアプリケーションを監視するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [追加]、[Windows の例外]、[監視するアプリケーション] の順にクリックします。
3. ダイアログボックスで、アプリケーション名を入力します。
たとえば、実行可能ファイルの名前を次のように入力します。
`foo.exe`
4. [追加] をクリックします。
5. [OK] をクリックします。

クライアントコンピュータで動作するアプリケーションとサービスの監視

ウイルスとスパイウェアのスキンの例外作成

Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定する

ログイベントに基づく例外の作成

Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定する

特定のアプリケーションを監視して、Symantec Endpoint Protection でアプリケーションがどのように処理されるかを指定するための例外を作成できます。Symantec Endpoint Protection がアプリケーションを学習し、管理コンソールがイベントを受信すると、[アプリケーション例外] ダイアログボックスのアプリケーションリストにそのアプリケーションが

表示されます。ネットワーク内のクライアントコンピュータがまだアプリケーションを学習していない場合は空のアプリケーションリストが表示されます。

アプリケーションリストには、監視対象のアプリケーションとユーザーがダウンロードするファイルが含まれています。Symantec Endpoint Protection は、Symantec Endpoint Protection がアプリケーションを検出した場合、またはアプリケーションが実行されている場合に、処理を適用します。

アプリケーションは、[DNS またはホストファイルの変更例外] のリストにも表示されます。

Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [追加]、[Windows の例外]、[アプリケーション] の順にクリックします。
3. [表示] ドロップダウンボックスで、[すべて]、[監視したアプリケーション]、[ユーザー許可アプリケーション] のいずれかを選択します。
4. 例外を作成するアプリケーションを選択します。
5. [処理] ドロップダウンボックスで、[無視]、[ログのみ]、[検疫]、[終了]、[削除] のいずれかを選択します。

[無視] と [ログのみ] の処理は、スキャンでアプリケーションが不良または悪質として検出されたときに適用されます。[終了]、[検疫]、[削除] の処理は、アプリケーションが起動したときに適用されます。

6. [OK] をクリックします。

Windows クライアントのアプリケーションの例外を作成するためのアプリケーションの監視

ウイルスとスパイウェアのスキャンの例外作成

クライアントコンピュータで動作するアプリケーションとサービスの監視

DNS またはホストファイルを変更するアプリケーションのための例外の作成

Windows クライアントのスキャンからの信頼できる Web ドメインの除外

ウイルススキャンとスパイウェアスキャン、SONAR から Web ドメインを除外できます。信頼できる Web ドメインを除外すると、そのドメインの任意の場所からユーザーがダウンロードしたファイルは常に許可されます。ただし、Auto-Protect やその他の定義済みスキャンはそのファイルを引き続きスキャンします。

デフォルトでは、ダウンロードインサイトは、**Internet Explorer** の [ツール] > [インターネットオプション] > [セキュリティ] の [信頼済みサイト] のリストに表示される Web サイトを除外します。この設定は、ダウンロードインサイトの [ウィルスとスパイウェアの対策] ポリシーの設定から構成できます。

ダウンロードインサイトまたは Auto-Protect が無効になっている場合、信頼できる Web ドメインの例外も無効になります。

NOTE

例外を設定するときには注意が必要です。例外を作成するたびに、コンピュータのセキュリティプロファイルは低下します。恒久的なスキャンの例外を設ける代わりに、疑わしい誤検知があった場合は検査のために送信することを検討してください。Symantec Endpoint Protection が提供する複数の保護レイヤーを常に使用します。

誤認検出 (偽陽性) の疑いのレポート

サポートされる Web ドメインの例外

Web ドメインの例外を作成する際には、次のガイドラインに従います。

-
- 信頼できる Web ドメインの例外を指定する場合は、単一のドメインを URL または IP アドレスとして入力する必要があります。一度に指定できる ドメインは 1 つだけです。
 - ポート番号はサポートされません。
 - URL を指定する場合、例外では URL のドメイン名部分のみを使います。URL の先頭に HTTP または HTTPS (大文字と小文字の区別なし) を追加できますが、例外は両方のプロトコルに適用されます。
 - IP アドレスを指定する場合、例外は指定した IP アドレスとそれに対応するホスト名の両方に適用されます。その URL を利用してある場所に移動する場合、Symantec Endpoint Protection はホスト名を IP アドレスに解決し、例外を適用します。IP アドレスの先頭には HTTP (大文字と小文字の区別なし) のみを追加できます。
 - ダウンロードインサイトと SONAR の両方で、ユーザーが HTTP と HTTPS のどちらを使用してドメインに移動した場合でも、ドメインが除外されます。
 - FTP ロケーションの場合は、IP アドレスを指定する必要があります。FTP の URL はサポートされません。
 - 信頼できる Web ドメインの例外では、ワイルドカード * がサポートされています。
 - 侵入防止ポリシー内の URL 評価は、信頼できる Web ドメイン例外として指定するすべての Web サイトが許可されます。

Windows クライアントのスキャンから信頼できる Web ドメインを除外するには

1. [例外ポリシー] ページで、[追加] > [Windows の例外] > [信頼できる **Web** ドメイン] の順にクリックします。
2. [信頼できる **Web** ドメイン例外の追加] ダイアログボックスで、除外するドメイン名または IP アドレスを入力します。

Web ドメイン例外のガイドライン

3. [OK] をクリックします。
4. Web ドメインの例外をさらに追加するには、手順を繰り返します。

ウイルスとスパイウェアのスキャンの例外作成

Windows クライアントの改変対策例外の作成

改変対策のファイル例外を作成できます。クライアントコンピュータで改変対策が既知の安全なアプリケーションと干渉する場合は、改変対策例外を作成すると便利です。たとえば、改変対策がスクリーンリーダーなどの支援技術アプリケーションを遮断することがあります。

この支援技術アプリケーションに関連付けられているファイル名がわかっている場合は、アプリケーションに実行を許可する例外を作成することができます。

NOTE

改変対策はフォルダの例外をサポートしません。

14.2 RU1 以降では、[User Profile] および [System] プレフィックス変数がサポートされています。

Windows クライアントの改変対策例外を作成するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [追加]、[Windows の例外]、[改変対策例外] の順にクリックします。
3. [改変対策例外の追加] ダイアログボックスの [プレフィックス変数] ドロップダウンボックスで、共通のフォルダを選択します。

プレフィックスを選択するときは、例外を異なる Windows オペレーティングシステムで使うことができます。

絶対パスとファイル名を入力する場合には [NONE] を選択します。

-
4. [ファイル] テキストボックスに、ファイル名を入力します。

プレフィックスを選択した場合は、パス名はプレフィックスに関連したものにしてください。プレフィックスに [NONE] を選択した場合は、絶対パス名を入力します。

ファイル名を指定する必要があります。改変対策はフォルダの例外をサポートしません。フォルダ名を入力すると、改変対策はその名前のフォルダにあるすべてのファイルを除外しません。指定した名前のファイルのみを除外します。

5. [OK] をクリックします。

「[How to collect the Tamper Protection log from Symantec Endpoint Protection Manager in Symantec Endpoint Protection 12.1](#)」を参照してください。

ウイルスとスパイウェアのスキンの例外作成

DNS またはホストファイルを変更するアプリケーションのための例外の作成

DNS またはホストファイルを変更する特定のアプリケーションのために例外を作成できます。SONAR により、DNS またはホストファイルの変更などのシステム変更が防止されていることがあります。たとえば、VPN アプリケーションのための例外を作成することが必要な場合があります。

特定のアプリケーションを監視して、DNS またはホストファイルの変更の例外を作成できます。Symantec Endpoint Protection がアプリケーションを学習し、管理コンソールがイベントを受信した後、アプリケーションリストにそのアプリケーションが表示されます。ネットワーク内のクライアントコンピュータがまだアプリケーションを学習していない場合は空のアプリケーションリストが表示されます。

SONAR 設定を使って、SONAR が DNS またはホストファイルの変更をどのようにグローバルに検出するかを制御します。

DNS またはホストファイルを変更するアプリケーションのための例外を作成するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [追加] > [Windows の例外] > [DNS またはホストファイルの変更例外] の順にクリックします。
3. 例外を作成するアプリケーションを選択します。
4. [処理] ドロップダウンボックスで、[無視]、[ログのみ]、[確認]、または [遮断] を選択します。

選択した処理は、スキャンで DNS またはホストファイルの変更を行っているアプリケーションが検出されたときに適用されます。

5. [OK] をクリックします。

ウイルスとスパイウェアのスキンの例外作成

[Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定するクライアントコンピュータでの SONAR 設定の調整](#)

Windows クライアントのスキャンからの証明書の除外

14.0.1 以降、証明書の例外を個別に追加して、証明書によって署名されたファイルがスキャンされて疑わしいファイルとして検出されることがないように設定できます。たとえば、社内で開発されたツールに自己署名証明書が使用されている場合があります。この証明書をスキャン対象から除外すると、署名されたファイルが Auto-Protect、ダウンロードインサイト、SONAR、またはその他のスキャンによって疑わしいファイルとして検出されることがなくなります。

証明書の除外は、X.509 と base64 証明書のタイプのみをサポートします。証明書の例外を追加するときには、DER または base64 エンコードファイルのパブリック証明書 (.cer) のコピーが必要です。

証明書の例外は、次のアイテムではサポートされません。

-
- メモリエクスプロイト緩和機能
 - プロアクティブ脅威防止のシステム変更イベント
 - 改変対策
 - 圧縮ファイル内の証明書署名済みファイル

除外を有効にするために、クライアントコンピュータの証明書ストアにその除外した証明書をインストールする必要はありません。証明書の例外と拒否リストルールが競合する場合は、拒否リストルールが優先されます。

証明書の例外は、つの Symantec Endpoint Protection Manager クライアントインターフェースの設定からではなく、Symantec Endpoint Protection ポリシーからのみ追加できます。

NOTE

クラウドコンソールから登録解除されている場合にのみ、つの Symantec Endpoint Protection Manager に証明書の例外を追加できます。つの Symantec Endpoint Protection Manager が登録されている場合は、クラウドコンソールを使用して証明書の例外を追加または管理します。

Windows クライアントでスキャンから証明書を除外するには

1. [例外ポリシー] ページで、[例外] をクリックします。
2. [例外] で、[追加] > [Windows の例外] > [証明書] をクリックします。

つの Symantec Endpoint Protection Manager がクラウドコンソールに登録されている場合には、このオプションは表示されません。代わりに、クラウドコンソールで証明書の例外を追加します。

3. [証明書ファイル] の [参照] をクリックして、除外する証明書を参照して [OK] をクリックします。
4. [証明書情報] の値が、除外する証明書として正しいことを確認して、[OK] をクリックします。

複数の証明書に対して例外を作成する場合は、手順を繰り返します。

ウイルスとスパイウェアのスキャンの例外作成

クライアントコンピュータでユーザーが設定できる例外の種類の制限

クライアントコンピュータでユーザーがウイルスとスパイウェアのスキャンの例外や、SONAR の例外を作成できないように制限を設定できます。デフォルトでは、ユーザーは例外を設定できます。

クライアントコンピュータ上のユーザーは制限の設定に関係なく、改変対策の例外を作成できません。

ユーザーはまた、アプリケーション制御のためのファイル例外を作成できません。

クライアントコンピュータでユーザーが設定できる例外の種類を制限するには

1. [例外ポリシー] ページで、[クライアント制限] をクリックします。
2. [クライアント制限] で、クライアントコンピュータのユーザーに設定させない例外のチェックマークをすべてはずします。
3. このポリシーの設定を完了したら、[OK] をクリックします。

Symantec Endpoint Protection の例外の管理

ログイベントに基づく例外の作成

ウイルススキャンとスパイウェアスキャン、SONAR、アプリケーション制御、改変対策のログイベントに基づいて例外を作成できます。

NOTE

早期起動マルウェア対策検出のためのログイベントからは例外を作成できません。

Table 125: 例外とログの種類

例外の種類	ログの種類
ファイル	リスクログ
フォルダ	リスクログ SONAR ログ
既知のリスク	リスクログ
拡張子	リスクログ
アプリケーション	リスクログ SONAR ログ
信頼できる Web ドメイン	リスクログ SONAR ログ
改変対策	アプリケーション制御ログ
DNS またはホストファイルの変更	SONAR ログ

例外を作成する項目は、Symantec Endpoint Protection によってすでに検出されている必要があります。ログイベントを使って例外を作成するときには、その例外を含む必要がある例外ポリシーを指定します。

ログイベントに基づく例外を作成するには

1. [監視] タブで、[ログ] タブをクリックします。
2. [ログの種類] ドロップダウンリストで、[リスク]、[SONAR]、[アプリケーションとデバイス制御] のいずれかのログを選択します。
3. [アプリケーションとデバイス制御] を選択した場合は、[ログの内容] リストから [アプリケーション制御] を選択します。
4. [ログの表示] をクリックします。
5. [時間範囲] の横で、ログをフィルタ処理するための期間を選択します。
6. 例外を作成するエントリを 1 つ以上選択します。
7. [処理] の横で、作成する例外の種類を選択します。

選択する例外の種類は、選択したアイテムに対して有効である必要があります。

8. [適用] または [開始] をクリックします。
9. ダイアログボックスで、例外に含めない項目をすべて削除します。
10. セキュリティリスクの場合は、Symantec Endpoint Protection で検出をログに記録させるには、[セキュリティリスクの検出時にログに記録する] にチェックマークを付けます。
11. この例外を使う必要のあるすべての例外ポリシーを選択します。
12. [OK] をクリックします。

エンドポイント保護の監視

Symantec Endpoint Protection の例外の管理

ウイルスとスパイウェアのスキャンの例外作成

Web とクラウドのアクセス保護 の設定

Web とクラウドのアクセス保護 ポリシーは、Symantec Web Security Service (WSS) の機能を Symantec Endpoint Protection に統合します。Web とクラウドのアクセス保護 は、クライアント上のすべてのインターネット トラフィックまたは Web トラフィックのみを Symantec WSS にリダイレクトします。ここでは、WSS ポリシーに基づいてトラフィックが許可または遮断されます。

Web とクラウドのアクセス保護 とは

この Symantec Endpoint Protection Manager (SEPM) 内でこの機能を使用するには、Symantec Web Security Service の有効なサブスクリプションが必要です。サブスクリプションについてはアカウント担当者にお問い合わせください。

注: 14.3 RU1 では、WSS トラフィックリダイレクトは、ネットワークトラフィックリダイレクトに名前が変更されました。統合ポリシーは、ネットワークトラフィックリダイレクトポリシーに名前が変更されました。

NOTE

14.3 RU2 で、Network Traffic Redirection は Web とクラウドのアクセス保護に名前が変更されました

技術的な要件と制限

必要条件	説明
サポートされるブラウザ	Windows: - Microsoft Internet Explorer 9 から 11 - Mozilla Firefox - Google Chrome - Microsoft Edge Mac: - Mac では、Apple Safari、Google Chrome、Mozilla Firefox がサポートされます。 - Firefox バージョン 65 以降は、14.2 RU1 以降でサポートされます。
制限事項	- Web Security Service は、IPv6 ではなく IPv4 で提供されます。 - Network Traffic Redirection 機能がエンドポイントにインストールされている場合、スタンドアロンの Symantec WSS Agent (WSSA) はインストールできません。同様に、WSSA がインストールされている場合、NTR 機能はインストールできません。ただし、以下のいずれかの方法を使って、クライアント全体をアンインストールする必要なく、既存のエンドポイントから NTR 機能を削除できます。 - Symantec Endpoint Protection Manager で、Network Traffic Redirection を含まないクライアント インストール機能セットを作成してエンドポイントに適用します。 既存の Endpoint Protection クライアントに機能を追加または削除する - 次のコマンドライン オプションは、クライアントのインストール ファイルを使用して NTR を削除します： <pre>setup.exe /s /v" REMOVE=NTR /qn"</pre> トンネル方式には以下の制限があります。 64 ビット版 Windows 10 バージョン 1703 以降 (半期サービスチャネル) でのみ実行されます。この方法では、他の Windows オペレーティングシステムまたは Mac クライアントはサポートされていません。 - 長期サービス チャネル (LTSC) はサポートされていません。Microsoft は、LTSC を特殊なシステムにのみ使用することを対象としています。 - HVCI 対応の Windows 10 64 ビット デバイスはサポートされません。 - クライアントコンピュータはインストール中に ctc.symantec.com と通信し、統合トークンを CustomerID に変換します。その通信ができない場合、インストールは失敗します。すべてのクライアントでこの問題の可能性を回避するには、変換が必要ないように、統合トークンの代わりに CustomerID を使用できます。 - Symantec Endpoint Protection クライアントからのアウトバウンドトラフィックは、クライアントのファイアウォールまたは URL 評価ルールのいずれかによって評価される前に、WSS にリダイレクトされます。代わりに、そのトラフィックは WSS ファイアウォールおよび URL に対して評価されます。たとえば、SEP クライアント ファイアウォール ルールが google.com を遮断し、WSS のルールが google.com を許可する場合、クライアントは google.com へのアクセスをユーザに許可します。クライアントへのインバウンド ローカル トラフィックは引き続き Symantec Endpoint Protection ファイアウォールによって処理されます。 - WSS キャプティブ ポータルはトンネル方式では使用できません。クライアントはチャレンジ資格情報を無視します。今後のリリースでは、WSS エージェント内の SAML 認証はキャプティブ ポータルに置き換わり、Symantec Endpoint Protection クライアントで使用可能になります。 - クライアント コンピュータがトンネル方式を使用して WSS に接続して仮想マシンをホストする場合、各ゲスト ユーザは WSS ポータルで提供された SSL 証明書をインストールする必要があります。 - ホームディレクトリや Active Directory 認証のようなローカルネットワークへのトラフィックはリダイレクトされません。 - Microsoft DirectAccess VPN とは互換性がありません。

PAC ファイル方式による Web とクラウドのアクセス保護 ポリシーの設定

WSS 管理者は、プロキシの自動構成 (PAC) ファイル URL または WSS ポータルからの統合トークンを提供します。PAC ファイルまたは統合トークンで Web とクラウドのアクセス保護 ポリシーを更新し、NTR ポリシーをグループに割り当てます。

[接続: シームレス ID による WSS-SEP-WTR](#)

[Endpoint Protection と Web Security Services の統合のベストプラクティス](#)

トンネル方式による Web とクラウドのアクセス保護 の設定

このトンネル方式は、早期採用リリース機能です。WSS ポリシーに対してアプリケーションの徹底的なテストを実行する必要があります。

Table 126: トンネル方式の設定

手順	説明
ステップ 1: WSS ポータルからの統合トークンの取得	1. 新しいまたはデフォルトの Web とクラウドのアクセス保護 ポリシーに統合トークンを追加します。 接続: シームレス ID による WSS-SEP-NTR 2. ポリシーのロックは解除しないでください。 3. NTR ポリシーをテストグループに割り当てます。
ステップ 2: クライアントで Web とクラウドのアクセス保護 ポリシーが有効であることの確認	クライアントをテストしている間、Web とクラウドのアクセス保護 が有効で、WSS に接続されていることを確認します。また、誤って設定された WSS ポリシーによりユーザがリソースにアクセスできないままである場合にクライアントユーザが Web とクラウドのアクセス保護 を無効化できることも確認してください。 クライアントで Web とクラウドのアクセス保護 ポリシーが有効であることの検証
ステップ 3: WSS ポリシーを設定およびテストします。	Web とクラウドのアクセス保護 をテストするには、まず、ラボ環境で WSS ポリシーを設定または編集します。WSS ポリシーに対してさまざまなテストシナリオを実行します。これは多くの場合、WSS ポリシーに対するデバイスのコンプライアンスの比較が含まれます。 Symantec Endpoint Protection クライアントでの NTR ポリシーのテスト
ステップ 4: Web とクラウドのアクセス保護 ポリシーをロックする	WSS ポリシーが Symantec Endpoint Protection クライアントで期待どおりに動作することを確認したら、クライアントコンピュータが保護され、ユーザーが WSS からクライアントを切断できないように、ポリシーをロックします。 NTR をロックするには、SEPM Web とクラウドのアクセス保護 ポリシーの南京錠をロックします。

レポート

- Web とクラウドのアクセス保護 ポリシーに対する設定の変更は、Symantec Endpoint Protection Manager 監査ログに表示されます。
- トンネル方式のイベントは、クライアントのネットワーク脅威リダイレクトログに表示されます。これらのイベントは、Symantec Endpoint Protection Manager システムログにアップロードされます。

クライアントの NTR ログを表示するには

1. クライアント コンピュータの [状態] ページで、[**Web とクラウドのアクセス保護**] の隣の [オプション] > [ログの表示] をクリックします。

バージョン変更

- バージョン 14.0.1 MP1 ~ 14.2 RU1 では、WSS トラフィックリダイレクトは Windows コンピュータにのみ適用されます。
- 14.2 RU2 では、Mac コンピュータのサポートが追加されました。
- 14.2 では、WSS によってクライアント認証を拡張し、送信ユーザーに基づいて、Web トラフィックをより詳細に制御するためのサポートが追加されました。
- 14.3 RU1 では、WSS トラフィック リダイレクトは、Network Traffic Redirection Web とクラウドのアクセス保護 に名前が変更されました。
- 14.3 RU1 では、トンネル方式という新しい接続手法が追加されました。

Web とクラウドのアクセス保護 とは

Web とクラウドのアクセス保護 は、ネットワークトラフィックを Symantec Web Security Service (WSS) にリダイレクトし、Symantec Endpoint Protection (SEP) クライアントのトラフィックを WSS ポリシーで許可または遮断するこ

とで、安全でない URL からクライアント コンピュータを保護します。Symantec WSS との統合により、従業員は悪質な Web サイトにアクセスできなくなり、定義済みの Web 使用ポリシーを順守することができます。

Web とクラウドのアクセス保護 の仕組み

WSS 管理者は、Symantec WSS ポータルで PAC ファイルまたは統合トークンのいずれかを生成します。PAC ファイルまたは統合トークンをつの Symantec Endpoint Protection Manager Web とクラウドのアクセス保護 ポリシーに追加します。これにより、SEP クライアントに統合がプッシュされます。クライアントコンピュータは ctc.symantec.com に接続して、統合トークンを CustomerID に変換します。これには、ログインユーザーの ID とデバイス情報が含まれます。カスタマー ID を持つユーザーは、インターネットにアクセスするたびにログオンする必要はありません。クライアントユーザーがコンピュータにログオンすると、SEP クライアントは、セッションキーと事前共有キー (PSK) を使用して WSS へのセキュア接続を開始します。その後、SEP クライアントは WSS に#####を提供します。アサーションには、ユーザー ID と、コンピュータに関するその他の情報 (OS のバージョンなど) が含まれています。この#####によって、ユーザーは、キャプティブポータルまたはローミングキャプティブポータル (PAC ファイル方式のみ) を介してインターネットにアクセスする際に、再度ログオンする必要がなくなります。このプロセスでは、ユーザーごとのポリシーがトラフィックに適用され、ログ記録およびレポート用に、WSS に対して危険なクライアントコンテキストが提供されます。

サポートされているすべてのブラウザのトラフィックは、以下のいずれかの方法で処理されます。

- WSS サーバーへリダイレクトされる
- 遮断される
- 宛先への転送が許可される

リダイレクト方法

ネットワーク脅威リダイレクトポリシーでは、クライアントと Symantec WSS の間で 2 つのリダイレクト方法が提供されます。以下の表で、各方法の利点とその仕組みについて説明します。

Table 127: リダイレクト方法

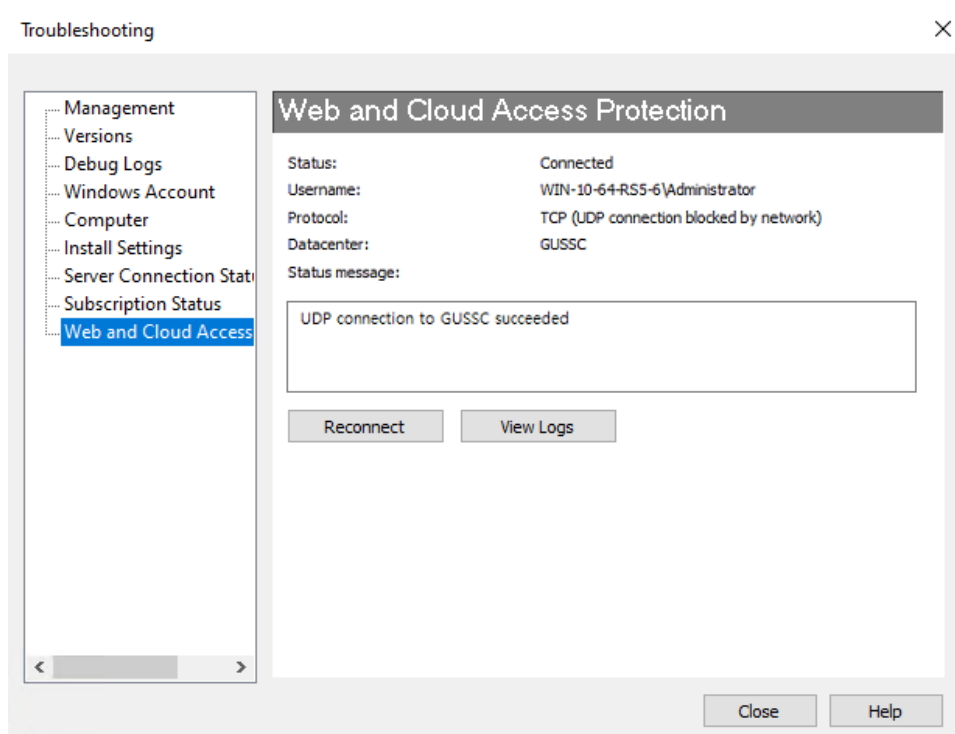
方法	使用すべきケース	仕組み
トンネル	トンネル方式では、WSS Agent 技術を Symantec Endpoint Protection に埋め込んで配備し、非プロキシアプリケーションをキャプチャします。この方式の特徴を以下に示します。 80 および 443 のみではなく、任意のポートにリダイレクトします。 - Web ブラウザだけでなく、すべてのアプリケーションをリダイレクトします。Web トラフィックのみをリダイレクトするように選択することもできます。 - ネットワークを頻繁に変更するローミングユーザーにとって、より堅牢です。 - トラフィックを暗号化することにより、クライアントコンピュータとデータセンターの間のセキュリティを向上させることができます。PAC ファイル方式では、トラフィックは暗号化されません。 - 今後の WSS への主な接続方法と見なされています。 64 ビット版 Windows 10 バージョン 1703 以降でのみ実行されます。 - Windows 10 長期サービス チャネル (LTSC) はサポートされていません。Microsoft は、LTSC を特殊なシステムにのみ使用することを対象としています。	WSS 管理者は、WSS ポータルでランダム化された統合トークンを生成し、そのトークンを Web とクラウドのアクセス保護 ポリシーに追加します。この方式では、非プロキシ対応アプリケーションからのトラフィックをキャプチャし、PAC ファイルでリダイレクトするよりも詳細なレベルのセキュリティ管理が可能です。WSS 統合トークンでは、トラフィックを開始したユーザーを特定するために追加のヘッダーデータを転送して、ユーザーごとのトラフィックルールの適用を実現します。 トンネル方式によってリダイレクトされるトラフィックは、WSS ポリシーの設定によって異なります。たとえば、ポリシールールでは、Web トラフィックのみ、またはすべてのポートおよびプロトコルを指定できます。トンネル方式は、WSS のライセンスにも依存します。 トンネル方式は暗号化されたトンネルであるため、デフォルトで証明書がインストールされます。
PAC ファイル	PAC ファイル方式の特徴を以下に示します。 - トンネル方式よりも高速です。 - サポートされているすべての Windows オペレーティングシステムで動作します。 - Mac コンピュータで動作します。 - Web トラフィックのみをリダイレクトします。	WSS 管理者は、PAC ファイルの URL を取得するために、WSS ポータルで PAC ファイルを設定します。PAC ファイルは、WSS への Web トラフィックリダイレクトを自動化し、Web ブラウザに安全なプロキシ設定を提供します。PAC ファイル方式では、ポート 80 および 443 のトラフィック (Web トラフィック) を検査用にリダイレクトできます。ただし、80/443 以外のトラフィックはリダイレクトできません。また、プロキシに対応しないアプリケーションからのトラフィックもリダイレクトできません。WSS にリダイレクトされるのは Web トラフィックのみです。 ユーザーが Web ブラウザを使用して Web サイトにアクセスするたびに、ブラウザは、PAC ファイルの定義に従い、最も近いクラウドでホストされた Web Security Service を介してすべての Web ブラウザトラフィックを送信します。PAC ファイルが定義するルールに基づいて、すべてのサポート対象のブラウザトラフィックが、次の方法のいずれかで処理されます。 - WSS 統合トークンがない場合、Web ブラウザのすべてのトラフィックは、WSS の PAC ファイルの URL を参照します。すべてのユーザーが WSS の同じトラフィックルールに従います。 - WSS 統合トークンがある場合、Web ブラウザのすべてのトラフィックは、ローカルのキャッシュに保存された WSS の PAC ファイルを参照します。WSS は、トラフィックの起点となるユーザーを判断し、それに従って Web トラフィックの送信先を決定できます。 409 PAC ファイル方式は、14.3 MP1 以前では Web トラフィックリダイレクト (WTR) と呼ばれていました。

クライアント上で **Web** とクラウドのアクセス保護 のトンネル方式が有効であり接続されていることの確認

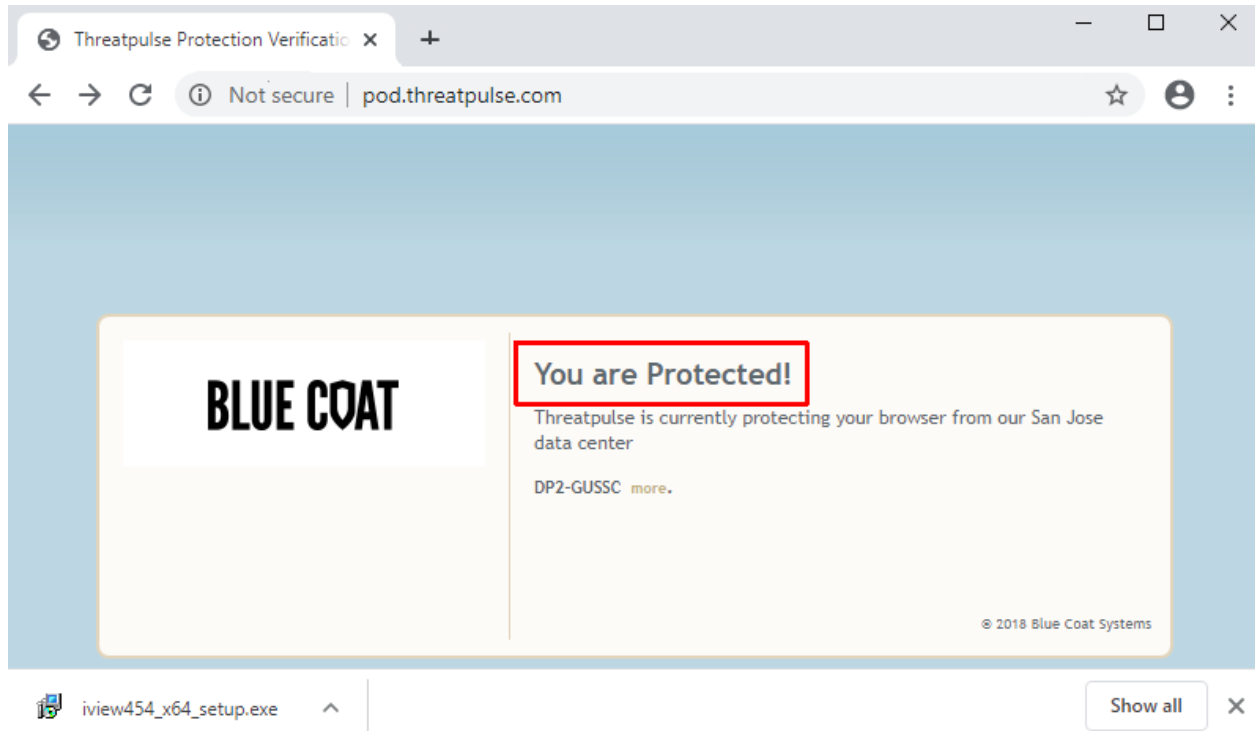
1. Symantec Endpoint Protection (SEP) クライアントで、[ヘルプ] > [トラブルシューティング] > [**Web とクラウドのアクセス保護**] をクリックします。

Web とクラウドのアクセス保護 パネルが表示された場合。パネルが表示されない場合、このトンネル方式はクライアント上で有効になっていません。

[状態] フィールドに「接続済み」と表示されている場合は、Web とクラウドのアクセス保護 が接続されています。



2. クライアントで、次のテスト URL にアクセスします: pod.threatpulse.com。
Web とクラウドのアクセス保護 が有効になっている場合、クライアント ユーザーに以下のメッセージが表示されます。



WSS への再接続

Web とクラウドのアクセス保護 は、WSS に常時接続されている必要があります。ただし、接続が中断される場合があります。Wi-Fi がダウンしたり、インターネット接続が無効になったり、データセンターに障害が発生したりすることがあります。停止の原因に関係なく、サービスが復帰すると、クライアントユーザーは WSS に再接続する必要があります。

以下の状況に基づいてクライアントに再接続します。

方法	説明
接続が切断されたことがクライアントによって検出された場合	1. SEP クライアントで、[状態] ページをクリックします。 2. Web とクラウドのアクセス保護 が有効で、接続されており、正常に動作している 3. WSS に再接続するには、クライアントユーザーは [修復] ボタンをクリックする 
接続が切断されたことがクライアントによって検出されない場合	1. クライアントで、[状態] ページをクリックします。 2. [Web とクラウドのアクセス保護] の隣にある [オプション] > [詳細なステータス] をクリックします。 3. [状態] フィールドに「接続済み」と表示されているはずです。そうでない場合は、[修復] ボタンをクリックします。

ブラウザでの Web とクラウドのアクセス保護 ポリシーのテスト

テスト用 Web サイトへのアクセス

WSS ソリューションでは、アプリケーションおよび Web サイトを分類し、WSS ポリシーに基づいてクライアントユーザーを許可または拒否することによって組織を保護します。多くの場合、これらのポリシーのテストは簡単ではありません。クライアントユーザーは、既知のマルウェアが含まれていると分類されたサイトなど、危険かもしれないサイトにアクセスする必要があるためです。テストを安全に実施できるように、シマンテック社はカテゴリごとに個々のリンクがある Web サイトを構築しています。クライアントユーザーはリンクをクリックして、リスクなしでそのカテゴリへのアクセスをシミュレートできます。

1. クライアントコンピュータで、ブラウザのウィンドウを開き、<http://sitereview.symantec.com> にアクセスします。
2. [カテゴリ] をクリックし、[テストページ] を選択します。
3. WSS ポリシーで許可および拒否されるサイトに対応する、個別のリンクをクリックします。エージェントが WSS カテゴリのポリシーに準拠していることを検証します。たとえば、許可されたサイトは以下のように表示されます。

Test Rating

This is a Symantec WebFilter test rating page categorized as

Charitable/Non-Profit

Sites that foster volunteerism for charitable causes. Also encompasses non-profit associations that cultivate philanthropic or relief efforts. Does not include organizations that attempt to influence legislation as a significant portion of their activities or organizations that campaign for, contribute to or affiliate with political organizations or candidates.

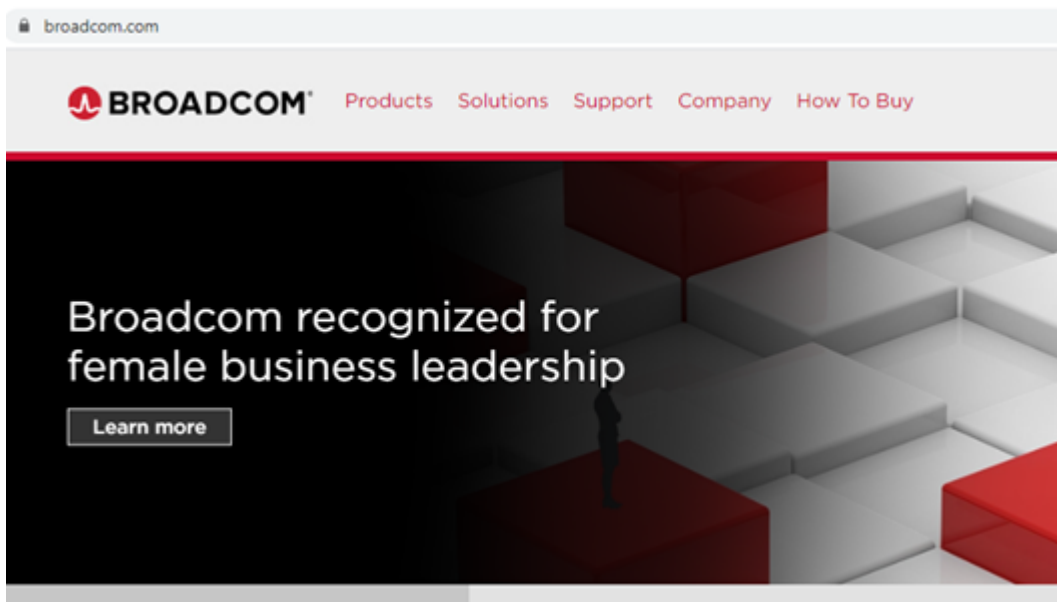
Examples: scouting.org 4-h.org ymca.net lionsclubs.org redcross.org
unicef.org pewtrusts.org cityharvest.org soles4souls.org

4. [脅威リスク] をクリックし、[テストページ] を選択します。
リンクは、シミュレートされたリスクの昇順で 1 ~ 10 にソートされて表示されます。
5. 各リンクをクリックして、クライアントが WSS リスクのポリシーに準拠していることを検証します。

ポリシーによって許可されたサイトへのアクセス

ここでは、クライアントユーザーが WSS ポリシーで許可されている Web サイトにアクセスする例を示します。トラフィックは WSS にリダイレクトされ、検査され、Web サイトに渡されます。

1. <http://www.broadcom.com> にアクセスします。
2. クライアントコンピュータでサイトを開けることを検証します。



WSS ポリシーを使用したトンネル手法のテスト

WSS 管理者が WSS コンソールで設定したポリシーを使用する統合 Web とクラウドのアクセス保護 ソリューションをテストできます。各組織のポリシーは異なっているので、各シナリオをテストするために使える Web サイトのリストを取得するには、WSS 管理者の協力が必要な場合があります。

Web とクラウドのアクセス保護 for the Mac クライアントについて

Web とクラウドのアクセス保護 は Symantec Web Security Service への Web トラフィックリダイレクトを自動化し、Symantec Endpoint Protection を使用する各コンピュータ上で Web トラフィックを保護します。

管理者は Web とクラウドのアクセス保護 が使用する設定を制御します。これにはプロキシの設定 URL と、オプションで Symantec Web Security Service ルート証明書が含まれます。つの Symantec Endpoint Protection Manager 管理者のみがこれらの設定を構成できます。これらの設定は Symantec Endpoint Protection クライアント UI には表示されません。Mac のプロキシ構成ファイルの URL は、[プロキシ] の下の [システム環境設定] > [ネットワーク] で表示できます。クラウドサービス証明書は、[キーチェーン] に表示されます。

Web とクラウドのアクセス保護 をサポートする Web ブラウザは、Safari、Chrome、Firefox バージョン 65 以降です。14.2 RU1 以前の Symantec Endpoint Protection バージョンでは、Safari と Chrome のみがサポートされます。

NOTE

トンネル方式は、Mac クライアント上では実行されません。

Web とクラウドのアクセス保護 設定

Web とクラウドのアクセス保護 は、ネットワーク トラフィックを Symantec Web Security Service (WSS) にリダイレクトし、WSS でトラフィックを許可または遮断することで、ネットワーク トラフィックから Windows および Mac クライアント コンピュータを保護します。WSS は、WSS 管理者が WSS で設定したポリシーに基づいて、トラフィックを許可または遮断します。

注: つの Symantec Endpoint Protection Manager 内でこの機能を使用するには、Web Security Service の有効なサブスクリプションが必要です。サブスクリプションについてはアカウント担当者にお問い合わせください。

Table 128: Web とクラウドのアクセス保護 設定

オプション	説明
有効にする Web とクラウドのアクセス保護	Symantec Endpoint Protection クライアントで Web とクラウドのアクセス保護 機能を有効または無効にします。クライアントでこの機能を有効にするには、このオプションにチェックマークを付ける必要があります。 PAC ファイル方式でこのオプションを無効にした場合でも、[Symantec Web Security Service ルート証明書をクライアントにインストールし、暗号化されたトラフィックによる保護を促進できます] オプションを有効にすることができます。 このオプションは、14.3 RU1 で [WSS トラフィックリダイレクトの有効化] から名前が変更されました。
リダイレクト方法	- トンネル方式では、すべてのインターネットトラフィックを自動的に WSS にリダイレクトします。WSS ポリシーに対してアプリケーションの徹底的なテストを実行する必要があります。 - PAC ファイル方式では、Web のみのトラフィック (ポート 80 および 443) をリダイレクトします。 リダイレクト方法の違いについては、以下を参照してください。 Web とクラウドのアクセス保護 とは

Table 129: トンネル方式のオプション

オプション	説明
ネットワーク統合トークン	WSS 管理者は、WSS ポータルからランダム化された統合トークンを生成します。Symantec Endpoint Protection クライアントがトークンを受信すると、ctc.symantec.com が検索され、トークンが CustomerID に変換されます。カスタマー ID は、クライアントが WSS に接続した後に、ユーザー ID およびクライアントコンテキスト情報を WSS に安全に転送します。 注: インストール中にクライアントコンピュータがインターネットに接続できない場合は、トークンの代わりに CustomerID を使用できます。

Table 130: PAC ファイル方式のオプション

オプション	説明
PAC (プロキシの自動構成) ファイル URL	WSS 管理者によって定義される PAC (プロキシの自動構成) ファイルへの URL を示します。 この URL は、つの Symantec Endpoint Protection Manager でのみ設定したり編集したりできます。
トラフィック傍受ポート	ローカルプロキシサービスによって使用中のポートを示します。 14.2 RU1 より前のバージョンでは、このオプションは Windows コンピュータにのみ適用されます。
ネットワーク統合トークン	Symantec Endpoint Protection クライアントは、このトークンを使用して、ユーザー ID およびクライアントコンテキスト情報を WSS に安全に転送します。ローカルプロキシサービスは、ユーザーごとのルールに基づいてヘッダー情報を解析して Web トラフィックを許可または遮断するために、このトークンが必要です。 このオプションによって PAC ファイルのローカルキャッシュが可能になります。 14.2 RU1 より前のバージョンでは、このオプションは Windows コンピュータにのみ適用されます。
ネットワーク保護が利用できない場合に直接トラフィックを許可する	このオプションを使用すると、WSS クラウドプロキシ (proxySG) を使用したユーザー認証が失敗した場合に、ユーザーに Web へのアクセスを許可できます。管理者が PAC ファイルを設定したにもかかわらず、WSS ローミングユーザーではない場合に、この状況が発生します。 - このオプションにチェックマークが付いていて、クライアントユーザーが認証に失敗した場合、クライアントはフェイルオープン状態になります。 - このオプションのチェックマークがはずれており、クライアントユーザーが認証に失敗した場合、クライアントはフェイルクローズ状態になります。 ユーザが認証されるまで、Web とクラウドのアクセス保護では保護されません。WSS は、5 分ごとにバックグラウンドでユーザの認証を試行します。WSS は、WSS ローミングキャプティブポータルでの手動認証をユーザーに要求します。 有効な認証の試行が行われるまで、この設定は無視されます。 このオプションは、クライアント 14.2 RU2 MP1 以降に適用されます。

オプション	説明
LPS カスタム PAC ファイルの有効化	クライアント上の LPS サーバがホストしているデフォルトの PAC ファイルを、カスタム PAC ファイルと置き換えます。カスタム PAC ファイルは、ルーブバックアダプタを応答準備しているローカルプロキシサーバーで動作しないサードパーティアプリケーションとの互換性の問題を解決します。WSS ポータルを使用して、バイパスおよびフィルタリングの他のすべての設定を行うことをお勧めします。 このオプションは、クライアント 14.3 以降に適用されます。 警告: カスタム PAC ファイルオプションを誤って設定した場合、クライアントユーザーとアプリケーションがインターネットにアクセスできなくなる可能性があります。 注: カスタム PAC ファイルの効果はすぐに有効にならない場合があります。クライアントの再起動が必要になる場合があります。
Symantec Web Security Service ルート証明書をクライアントにインストールし、暗号化されたトラフィックによる保護を促進できます。	暗号化されたトラフィックを保護するため、Symantec Endpoint Protection クラウドに適切なルート証明書をインストールします。 [Web とクラウドのアクセス保護 を有効にする] オプションが無効になっている場合、このオプションを有効にできます。これにより、PAC ファイルオプションが選択されていない場合でも、ルート証明書をインストールできます。

つの Symantec Endpoint Protection Manager ポリシーのテスト

Symantec Endpoint Protection を評価したり、クライアントコンピュータにダウンロードする前にポリシーをテストしたりする必要がある場合があります。製品がクライアントコンピュータで正しく動作することを確認するため、つの Symantec Endpoint Protection Manager ポリシーを使用して次の機能をテストできます。

Table 131: テストできる機能

機能	参照トピック
ウイルス対策とスパイウェア対策	デフォルトのウイルスとスパイウェアの対策のポリシーをテストするには、EICAR テストウイルスを次の場所からダウンロードします。 http://www.eicar.org/86-0-Intended-use.html ウイルスとスパイウェアの対策ポリシーのテスト ウイルスとスパイウェアの対策ポリシーのテスト
SONAR	Download the Socar.exe test file to verify that SONAR works correctly
Insight	ライセンスサーバーやダウンロードインサイトサーバーへの接続をテストする方法
侵入防止	デフォルト IPS ポリシーのテスト
アプリケーション制御	クライアントコンピュータでの処理の開始の遮断 ユーザーがクライアントコンピュータのレジストリに書き込めないようにする ユーザーが特定のファイルに書き込めないようにする DLL を遮断するルールの追加とテスト 処理を終了するルールの追加とテスト クライアントコンピュータでの処理の開始の遮断 ユーザーがクライアントコンピュータのレジストリに書き込めないようにする ユーザーが特定のファイルに書き込めないようにする DLL を遮断するルールの追加とテスト 処理を終了するルールの追加とテスト

ウイルスとスパイウェアの対策ポリシーのテスト

ウイルスとスパイウェアの対策ポリシーが正常に機能することをテストするには、テスト用ウイルスファイル eicar.com を使うことができます。EICAR テストウイルスは、EICAR (European Institute for Computer Antivirus Research) によって開発されたテキストファイルです。ほとんどのウイルス対策ソフトウェアをテストするための容易かつ安全な方法を提供します。このファイルを使って、クライアントのウイルス対策機能が機能していることを確認できます。

ウイルスとスパイウェアの対策ポリシーをテストするには

1. クライアントコンピュータで、次の場所にある EICAR Web サイトからウイルス対策テストファイルをダウンロードします。

<http://2016.eicar.org/86-0-Intended-use.html>

2. EICAR テストファイルを実行します。

リスクが検出されたことを伝える通知が表示されます。

3. つの Symantec Endpoint Protection Manager の [監視] ページで [ログ] をクリックします。
4. [ログ] タブの [ログの種類] ドロップダウンリストで [リスク] をクリックし、[ログの表示] をクリックします。
5. [リスクログ] ページにウイルス検出イベントが表示されます。

クライアントコンピュータでの処理の開始の遮断

サーバーからクライアントコンピュータへのファイル転送の一般的な方法として FTP クライアントがあります。ユーザーがファイルを転送できないようにするには、ユーザーに FTP クライアントを起動させないルールをコマンドプロンプトから追加できます。

1. クライアントコンピュータで処理の開始を遮断するルールを追加するには、アプリケーション制御ポリシーを開き、[アプリケーション制御] ペインで [追加] をクリックします。
 2. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストでルールを選択し、[プロパティ] タブの [ルール名] テキストボックスに ftp_ blocked_from_cmd と入力します。
 3. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
 4. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] で cmd.exe と入力し、[OK] をクリックします。
 5. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[条件の追加] > [条件の追加] > [プロセス起動の試み] の順にクリックします。
 6. [プロパティ] タブの [説明] テキストボックスに no ftp from cmd と入力します。
 7. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
 8. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] で ftp.exe と入力し、[OK] をクリックします。
 9. [アプリケーション制御ルールセット] ダイアログボックスの [処理] タブで、[アクセスを遮断する]、[ログ記録を有効にする]、[ユーザーに通知] をクリックします。
 10. [ユーザーに通知] に ftp is blocked if launched from the cmd と入力します。
 11. [OK] を 2 回クリックし、ポリシーをグループに割り当てます。
- ルールをテストします。

12. クライアントコンピュータで処理の開始を遮断するルールをテストするには、クライアントコンピュータで、コマンドプロンプトを開きます。

13. コマンドプロンプトウィンドウで `ftp` と入力し、**Enter** キーを押します。

ルールが指定されているため、FTP クライアントが開きません。

ユーザーがクライアントコンピュータのレジストリに書き込めないようにする

特定のレジストリキーを保護して、ユーザーがレジストリ内のレジストリキーまたは値にアクセスしたり修正できないようにすることができます。レジストリキーの表示をユーザーに許可する一方で、レジストリキーの名前変更または修正できないようにすることができます。

機能をテストするには

- テスト用のレジストリキーを追加します。
 - レジストリキーの読み取りを許可し、書き込みを拒否するルールを追加します。
 - レジストリキーに新しい値を追加します。
1. テスト用のレジストリキーを追加するには、クライアントコンピュータでコマンドラインを開き、「`regedit`」と入力してレジストリエディタを開きます。
 2. レジストリエディタで `HKEY_LOCAL_MACHINE\Software` を展開し、新しいレジストリキーを作成し、`test` と命名します。
 3. ユーザーがクライアントコンピュータのレジストリに書き込みできないようにするには、アプリケーション制御ポリシーを開き、[アプリケーション制御] ペインで [追加] をクリックします。
 4. [アプリケーション制御ルールセット] の [ルール] リストで [追加] > [ルールの追加] をクリックします。
 5. [プロパティ] タブの [ルール名] テキストボックスに `HKLM_write_not_allowed_from_regedit` と入力します。
 6. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
 7. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] に `regedit.exe` と入力し、[OK] をクリックします。
 8. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[追加] > [条件の追加] > [レジストリアクセスの試み] の順にクリックします。
 9. [プロパティ] タブの [説明] テキストボックスに `registry access` と入力します。
 10. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
 11. [レジストリキー定義の追加] ダイアログボックスの [レジストリキー] テキストボックスに `HKEY_LOCAL_MACHINE\software\test` と入力し、[OK] をクリックします。
 12. [アプリケーション制御ルールセット] ダイアログボックスの [処理] タブにある [読み込みの試み] グループボックスで、[アクセスを許可する]、[ログ記録を有効にする]、[ユーザーに通知] をクリックします。
 13. [ユーザーに通知] で `reading is allowed` と入力します。
 14. [作成、削除、書き込みの試み] グループボックスで [アクセスを遮断する]、[ログ記録を有効にする]、[ユーザーに通知] をクリックします。
 15. [ユーザーに通知] に `writing is blocked` と入力します。
 16. [OK] を 2 回クリックし、ポリシーをグループに割り当てます。
- ルールをテストします。

17. レジストリへの書き込みを遮断するルールをテストするには、ポリシーを適用した後に、クライアントコンピュータのレジストリエディタで HKEY_LOCAL_MACHINE\Software を展開します。

18. 上記で作成した「test」という名前のレジストリキーをクリックします。

19. テストキーを右クリックし、[新規作成] をクリックして、[文字列値] をクリックします。

これでテスト用のレジストリキーに新しい値を追加できないようになります。

ユーザーが特定のファイルに書き込めないようにする

ユーザーがファイルを表示することはできても、修正できないようにすることができます。たとえば、ファイルには、従業員が確認する必要があっても編集できない財務データが含まれる場合があります。

アプリケーションとデバイス制御ルールを作成し、ファイルへの読み取り専用アクセス権をユーザーに付与します。たとえば、メモ帳でテキストファイルを開くことはできるが、編集はできないルールを追加できます。

1. ユーザーが特定のファイルに書き込めないようにするルールを追加するには、アプリケーション制御ポリシーを開き、[アプリケーション制御] ペインで [追加] をクリックします。

2. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[ルール] > [ルールの追加] をクリックします。

3. [プロパティ] タブの [ルール名] テキストボックスに `1.txt in c read allowed write terminate` と入力します。

4. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。

5. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] に `notepad.exe` と入力し、[OK] をクリックします。

6. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[追加] > [条件の追加] > [ファイルやフォルダのアクセスの試み] の順にクリックします。

7. [プロパティ] タブの [説明] テキストボックスに `file access launched` と入力します。

8. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。

9. [ファイルまたはフォルダの定義を追加] ダイアログボックスの [一致するファイルまたはフォルダの名前] グループボックスのテキストボックスに `c:\1.txt` と入力し、[OK] をクリックします。

10. [アプリケーション制御ルールセット] ダイアログボックスの [処理] タブにある [読み込みの試み] グループボックスで、[アクセスを許可する] を選択し、[ログ記録を有効にする] と [ユーザーに通知] にチェックマークを付けます。

11. [ユーザーに通知] で `reading is allowed` と入力します。

12. [作成、削除、書き込みの試み] グループボックスで [アクセスを遮断する]、[ログ記録を有効にする]、[ユーザーに通知] をクリックします。

13. [ユーザーに通知] に `writing to block Notepad` と入力します。

14. [OK] を 2 回クリックし、ポリシーをクライアントコンピュータグループに割り当てます。

ルールをテストします。

15. ユーザーが特定のファイルに書き込めないようにするルールをテストするには、クライアントコンピュータでファイルエクスプローラを開き、`c:\` ドライブを検索して [ファイル] > [新規作成] > [テキストファイル] をクリックします。

Notepad を使ってファイルを作成する場合、読み取り専用ファイルになります。

16. ファイルの名前を `1.txt` に変更します。

ファイルを `c:\` フォルダに保存します。

17. Notepad で c:\1.txt ファイルを開きます。

これでファイルを開くことはできますが、編集できなくなります。

DLLを遮断するルールの追加とテスト

ユーザーが特定のアプリケーションを開くことができないようにすることができます。ユーザーがアプリケーションを開くことができないようにする 1 つの方法として、アプリケーションがその実行に使う DLL を遮断する方法があります。DLL を遮断するには、DLL がロードされるのを遮断するルールを作成できます。ユーザーがアプリケーションを開こうとしても開くことはできません。

たとえば、Msvcr7.dll ファイルには Microsoft WordPad などさまざまな Windows アプリケーションを実行するために使われるプログラムコードが含まれています。クライアントコンピュータで Msvcr7.dll を遮断するルールを追加すると、Microsoft WordPad を開くことができません。

NOTE

「セキュリティを意識する」ように作成された一部のアプリケーションは DLL の挿入を悪意ある行為としてみなす場合があります。DLL の挿入を遮断したり、DLL を削除する対策を講じる必要があります。

1. DLL を遮断するルールを追加するには、アプリケーション制御ポリシーを開き、[アプリケーション制御] ペインで [追加] をクリックします。
2. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[ルール] > [ルールの追加] をクリックします。
3. [プロパティ] タブの [ルール名] テキストボックスに Block user from opening Microsoft Wordpad と入力します。
4. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
5. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] に C:\Program Files\Windows NT\Accessories\wordpad.exe と入力し、[OK] をクリックします。
6. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[追加] > [条件の追加] > [DLL ロードの試み] の順にクリックします。
7. [プロパティ] タブの [説明] テキストボックスに dll blocked と入力します。
8. [次の DLL に適用する] の右側で [追加] をクリックします。
9. [DLL 定義の追加] ダイアログボックスの [一致する DLL 名] グループボックスのテキストボックスに MSVCRT.dll と入力し、[OK] をクリックします。
10. [アプリケーション制御ルールセット] ダイアログボックスの [処理] タブで、[アクセスを遮断する]、[ログ記録を有効にする]、[ユーザーに通知] をクリックします。
11. [ユーザーに通知] に Should not be able to load WordPad と入力します。
12. [OK] を 2 回クリックし、ポリシーをクライアントコンピュータグループに割り当てます。
ルールをテストします。

-
13. DLL を遮断するルールをテストするには、クライアントコンピュータで Microsoft WordPad を開くことができないことを確認します。

処理を終了するルールの追加とテスト

Process Explorer は、開かれているまたはロードされている DLL プロセスと、そのプロセスが使っているリソースを表示するツールです。Process Explorer を使って処理を終了することもできます。ユーザーが Process Explorer を使って電卓アプリケーションを終了する場合、Process Explorer を終了するルールを追加できます。

1. 処理を終了するルールを追加するには、アプリケーション制御ポリシーを開き、[アプリケーション制御] ペインで [追加] をクリックします。
2. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[ルール] > [ルールの追加] をクリックします。
3. [プロパティ] タブの [ルール名] テキストボックスに `Terminates Process Explorer if Process Explorer tries to terminate calc.exe` と入力します。
4. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
5. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] に `procexp.exe` と入力し、[OK] をクリックします。
6. [アプリケーション制御ルールセット] ダイアログボックスの [ルール] リストで、[追加] > [条件の追加] > [プロセス終了の試み] の順にクリックします。
7. [プロパティ] タブの [説明] テキストボックスに `dll stopped` と入力します。
8. [このルールを次のプロセスに適用する] の右側にある [追加] をクリックします。
9. [プロセス定義の追加] ダイアログボックスの [照合するプロセス名] グループボックスのテキストボックスに `calc.exe` と入力し、[OK] をクリックします。
10. [アプリケーション制御ルールセット] ダイアログボックスの [処理] タブで、[プロセスを終了]、[ログ記録を有効にする]、[ユーザーに通知] をクリックします。
11. [ユーザーに通知] に `If you try to terminate the calc from procexp, procexp terminates` と入力します。
12. [OK] を 2 回クリックし、ポリシーをグループに割り当てます。
ルールをテストします。
13. 処理を終了するルールをテストするには、クライアントコンピュータで、以下の URL から Process Explorer の無償バージョンをダウンロードして実行します。

<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

14. Windows で電卓を開きます。
15. Process Explorer を開きます。
16. [Process Explorer] ウィンドウで `calc.exe` プロセスを右クリックし、[プロセスの強制終了] をクリックします。

Process Explorer が終了します。

デフォルト IPS ポリシーのテスト

デフォルト IPS ポリシーをテストするには、最初にクライアントコンピュータでイベントをトリガする必要があります。

デフォルト IPS ポリシーをテストするには

-
1. 実行可能ファイル (.exe) の名前を jpeg (.jpg) に変更します。
 2. .jpg ファイルを Web サーバー/サイトにアップロードします。
 3. クライアントコンピュータで Web ブラウザを使って、名前を変更した実行可能ファイルを開きます。

NOTE

名前を変更した実行可能ファイルを開くには、IP アドレスを使って Web サーバー/サイトにアクセスする必要があります。たとえば、次のように入力します。http://<Web ##### IP #####>/<#####
##>.jpg

4. クライアントで IPS ポリシーが正しく機能する場合は、次のイベントが発生します。
 - .jpg ファイルは開くことができません。
 - 通知領域アイコンのメッセージで、クライアントが .jpg ファイルを遮断したことが示されます。
 - セキュリティログを開いて、クライアントが .jpg ファイルを遮断したことを示すログエントリを見ることができます。

クライアント上のコンテンツと定義を更新する方法

デフォルトでは、つの Symantec Endpoint Protection Manager は公開 Symantec LiveUpdate サーバーからコンテンツ更新をダウンロードします。Symantec Endpoint Protection クライアントは次にこれらの更新を つの Symantec Endpoint Protection Manager からダウンロードします。コンテンツには、ウイルス定義、侵入防止シグネチャ、ホストインテグリティテンプレートなどが含まれています。

Table 132: Symantec Endpoint Protection クライアント上のコンテンツを更新する手順

タスク	説明
管理サーバーに LiveUpdate からの最新のコンテンツがあることを確認する (推奨)	デフォルトでは、つの Symantec Endpoint Protection Manager のインストールの一環として LiveUpdate を実行します。次の場合には、LiveUpdate の手動実行が必要なこともあります。 - インストール時に LiveUpdate をスキップした。 - LiveUpdate を実行してホストインテグリティテンプレートと侵入防止シグネチャをダウンロードする必要があります。 - 次の回の定時更新の前に LiveUpdate を実行したい。 つの Symantec Endpoint Protection Manager に最新のコンテンツが含まれていることの確認 つの Symantec Endpoint Protection Manager のコンテンツを .jdb ファイルを使用してアップデートすることもできます。 .jdb ファイルをダウンロードして Endpoint Protection Manager の定義を更新する また、複製を使用する場合は、ローカルサイトとパートナーサイト間でコンテンツとポリシーを複製できます。 複製のための 2 番目のサイトのインストール方法
クライアントコンピュータが更新を取得する方法を変更する (任意)	デフォルトでは、Windows クライアントコンピュータが管理サーバーからコンテンツ更新を取得します。他の配信方法には、GUP、社内の LiveUpdate サーバー、サードパーティツールによる配布があります。異なるクライアントプラットフォーム、多数のクライアント、ネットワーク制限事項をサポートするように配信方法を変更する必要があることもあります。 クライアント上のコンテンツを更新するための配布方法の選択 プラットフォームに基づきクライアント上のコンテンツを更新するための配布方法の選択
管理サーバーの LiveUpdate 設定を変更する (任意)	LiveUpdate セッションの頻度、ダウンロードした保護コンポーネントなどをカスタマイズできます。 LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード
ネットワーク過負荷を削減する (推奨)	管理サーバーがクライアントから完全な定義パッケージに対する大量の同時要求を受信すると、ネットワークが過負荷の状態になる場合があります。クライアントが完全定義をダウンロードしないようにするとネットワークの過負荷リスクを軽減できます。 クライアント更新要求のネットワーク過負荷の軽減
パフォーマンスの向上 (推奨)	ネットワーク帯域幅に対するダウンロードの影響を軽減するため、すべてのクライアントが更新を同時に取得しないようにコンテンツをランダムにダウンロードします。 同時コンテンツダウンロードのランダム化について デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化 LiveUpdate サーバーからのコンテンツダウンロードのランダム化 クライアントコンピュータのパフォーマンスに対するダウンロードの影響を軽減するため、クライアントコンピュータがアイドルのときに、クライアントコンピュータにコンテンツ更新をダウンロードさせることができます。 Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行する設定

タスク	説明
エンドポイントユーザーに自身の更新を管理させる (任意)	デフォルトでは、クライアントコンピュータのユーザーは、いつでも LiveUpdate を実行できます。コンテンツ更新についてどれだけの制御をユーザーに付与するかを指定できます。 ユーザーが LiveUpdate に対して持つ制御権限の設定 また、Intelligent Updater ファイルをクライアントコンピュータで使用して定義をアップデートできます。 Intelligent Updater ファイルを使用した Symantec Endpoint Protection クライアントのコンテンツの更新
シマンテック社がリリースする前にエンジンの更新をテストする (省略可能)	シマンテック社では四半期単位でエンジンの更新をリリースします。特定の Symantec LiveUpdate サーバーを使用して、リリース前にエンジンの更新をダウンロードできます。実働環境にコンテンツをロールアウトする前に、エンジンコンテンツをテストできます。 Windows クライアントでリリースする前のエンジン更新のテスト

クライアント上のコンテンツを更新するための配布方法の選択

クライアントプラットフォーム、ネットワーク構成、クライアント数、会社のセキュリティポリシーとアクセスポリシーによっては、クライアントに対するデフォルトの更新方法を変更しなければならない場合があります。

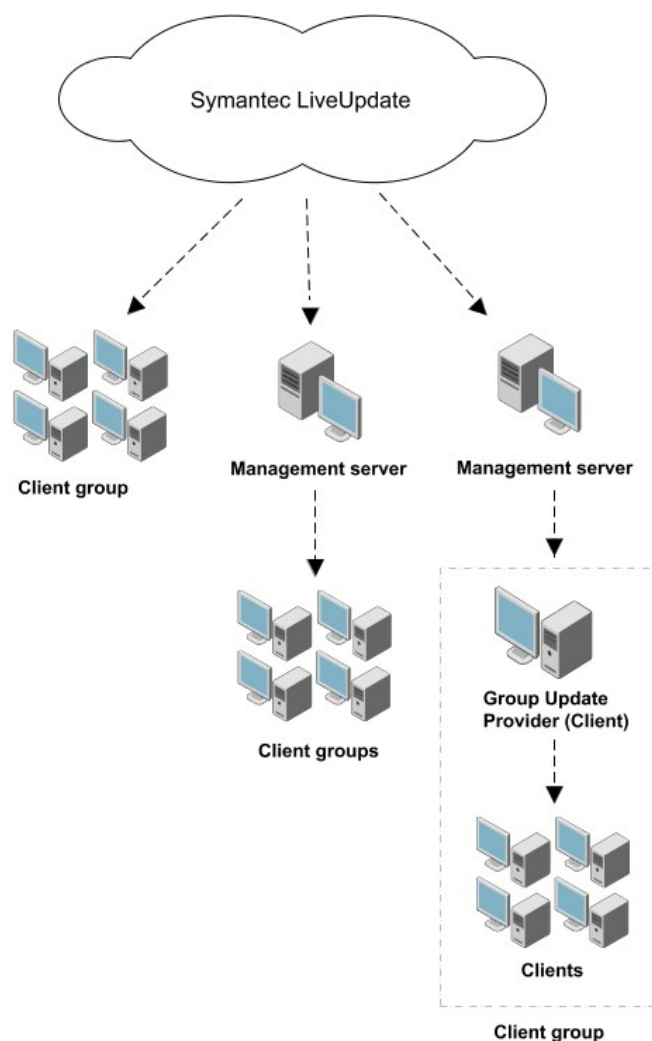
Table 133: コンテンツ配布方法とそれを使うケース

方法	説明	使用すべきケース
つの Symantec Endpoint Protection Manager からクライアントコンピュータ (デフォルト) (Windows、Mac、Linux)	デフォルトの管理サーバーは管理するクライアントコンピュータを自動的に更新します。 管理サーバーからクライアントに対する更新のスケジュールを定義しないでください。クライアントは、通信モードとハートビート頻度に基づき管理サーバーからコンテンツをダウンロードします。 つの Symantec Endpoint Protection Manager からコンテンツをダウンロードするためのクライアントの設定 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新	ネットワーク制約や会社のポリシーの代わりに他の方法を使う必要がなければこの方法を使うことを推奨します。 多数のクライアントまたは帯域幅の問題が存在する場合は、グループ更新プロバイダとともに、この方法を使うことができます。 Mac または Linux コンピュータが管理サーバーからコンテンツ更新を受け取るには、Apache Web Server を設定する必要があります。 Mac および Linux クライアントがリバースプロキシとして Apache Web サーバーを使用して、LiveUpdate 内容をダウンロードすることを有効にすること
GUP からクライアントコンピュータ (Windows のみ)	GUP は管理サーバーから更新を受信するクライアントコンピュータです。次に、グループ更新プロバイダによって更新がグループ内のほかのクライアントコンピュータに転送されます。1 つの GUP で複数のグループを更新できます。 グループ更新プロバイダはクライアントソフトウェアの更新を除くすべての種類の LiveUpdate コンテンツを配布できます。また、グループ更新プロバイダを使ってポリシーを更新することはできません。	グループ更新プロバイダは管理サーバーの負荷を軽減し、社内 LiveUpdate サーバーより設定が簡単です。GUP は最小の帯域幅が割り当てられたリモートの場所のグループに使います。 クライアントにコンテンツを配布するための GUP の使用 複数サイトと複製を設定するかどうか

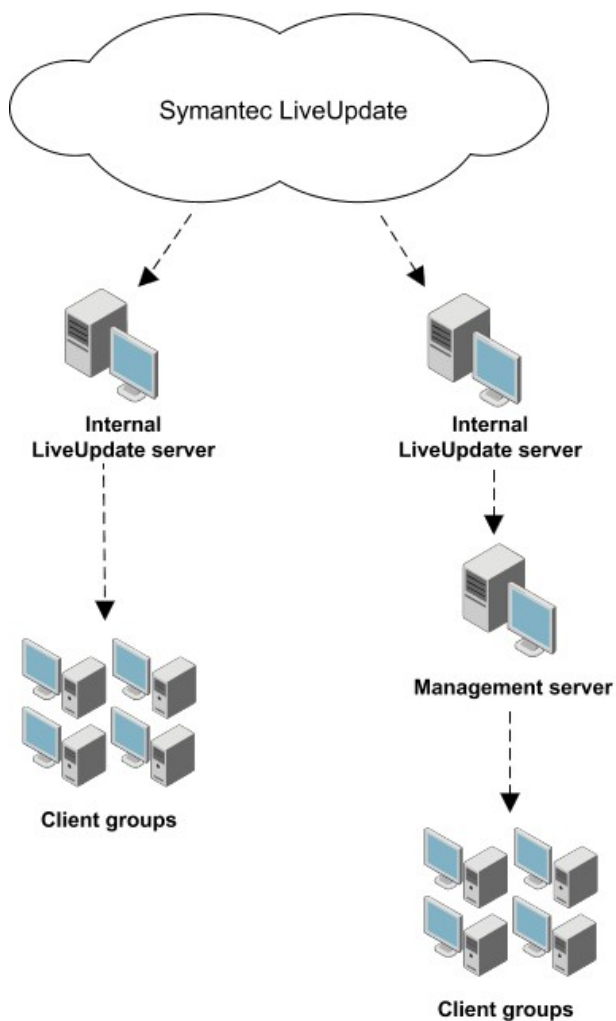
方法	説明	使用すべきケース
社内 LiveUpdate サーバーからクライアントコンピュータ (Windows、Mac、Linux)	クライアントコンピュータは Symantec LiveUpdate サーバーから更新を受信した社内 LiveUpdate サーバーから更新を直接ダウンロードできます。 必要に応じて、社内 LiveUpdate サーバーを複数セットアップし、クライアントコンピュータにリストを配布できます。 ダウンロードスケジュールを LiveUpdate サーバーから管理サーバーに変更できます。 クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定 社内 LiveUpdate サーバーの設定について詳しくは、次のナレッジベースから『<i>LiveUpdate Administrator #####</i>』を参照してください。 LiveUpdate Administrator のダウンロード	社内 LiveUpdate サーバーは非常に大規模なネットワークの管理サーバーの負荷を削減できます。小規模のネットワークでは、グループ更新プロバイダが組織のニーズを満たすかどうかを検討してください。 次の場合は、内部 LiveUpdate サーバーを使うことを考慮してください。 - 大規模なネットワーク（10,000 台以上のクライアント）を管理する場合 - 外部 LiveUpdate サーバーに接続すべきでない Mac または Linux クライアントを管理する場合 - 組織がコンテンツをクライアントコンピュータに配布するために LiveUpdate も使う複数のシマンテック製品を配備している場合 Note: 管理サーバーと社内 LiveUpdate サーバーは、同一の物理ハードウェアや仮想マシンにインストールしないでください。同じコンピュータにインストールすると、重大なサーバーパフォーマンスの問題が生じる可能性があります。 詳細については、次を参照してください。 LiveUpdate Administrator 2.x と SEPM の共存に関して 社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定
インターネット経由で外部 Symantec LiveUpdate サーバーからクライアントコンピュータに配布 (Windows、Mac、Linux)	クライアントコンピュータは Symantec LiveUpdate サーバーから更新を直接受信できます。	クライアントによるコンテンツの更新をスケジュール設定する必要がある場合や Symantec Endpoint Protection Manager とクライアント間の利用可能な帯域幅が制限されている場合、外部 Symantec LiveUpdate server を使います。 つの Symantec Endpoint Protection Manager と定時更新はデフォルトで有効になっています。デフォルト設定では、クライアントは管理サーバーから長期間応答がない場合を除いて常に管理サーバーから更新を取得します。 Note: ネットワーク上の多数の管理下クライアントを外部の Symantec LiveUpdate server から更新をプル型で転送するように設定しないでください。この設定では帯域幅が無駄に消費されます。 外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定
サードパーティツールの配布 (Windows のみ)	Microsoft SMS などのサードパーティツールでは、特定の更新ファイルをクライアントに配布できます。	この方法を使うと更新ファイルを配布する前にテストできます。サードパーティツールの配布インフラが整っている場合はこれを利用することもできます。 サードパーティの配布ツールを使ったコンテンツの配布

方法	説明	使用すべきケース
Intelligent Updater (Windows のみ)	Intelligent Updater ファイルには、ウイルスとセキュリティリスクのコンテンツと侵入防止のコンテンツが含まれています。手動でクライアントを更新する際に利用できます。 シマンテック社の Web サイトから Intelligent Updater の自己解凍ファイルをダウンロードできます。	LiveUpdate が利用できない場合は Intelligent Updater ファイルを使うことができます。 Intelligent Updater ファイルを使用した Symantec Endpoint Protection クライアントのコンテンツの更新 他の種類のコンテンツを更新するには、更新ファイルをダウンロードしてステージングするように、管理サーバーを設定する必要があります。 サードパーティの配布ツールを使ったクライアントコンピュータの更新

以下の図に、より小さいネットワークのための配布アーキテクチャの例を示します。



以下の図に、より大きいネットワークのための配布アーキテクチャの例を示します。



[プラットフォームに基づきクライアント上のコンテンツを更新するための配布方法の選択](#)

[クライアント上のコンテンツと定義を更新する方法](#)

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

プラットフォームに基づきクライアント上のコンテンツを更新するための配布方法の選択

ウイルス定義やその他のコンテンツをクライアントコンピュータに配布するために使うことのできる方法は、クライアントプラットフォームによって異なります。

Table 134: Windows、Mac、Linux クライアントに基づくコンテンツ配布方法

プラットフォーム	方法
Windows	デフォルトでは、Windows クライアントは管理サーバーからコンテンツを取得します。 Windows クライアントは次のソースから更新を取得することもできます。 - LiveUpdate サーバー (外部または内部) 社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定 外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定 - 外部 LiveUpdate サーバー (テストのみ) Windows クライアントでリリースする前のエンジン更新のテスト - グループ更新プロバイダ クライアントにコンテンツを配布するための GUP の使用 - サードパーティの配布ツール サードパーティの配布ツールを使ったコンテンツの配布 - Intelligent Updater Intelligent Updater ファイルを使用した Symantec Endpoint Protection クライアントのコンテンツの更新 クライアント上のコンテンツを更新するための配布方法の選択 Windows クライアントの場合、また次の設定をカスタマイズすることもできます。 - クライアントが受信するコンテンツの種類 - クライアントが複数のソースから定義を取得できるかどうか - 管理サーバーが完全な定義パッケージだけを提供できる場合、クライアントが LiveUpdate から小さいパッケージ (差分) を取得できるかどうか 完全定義パッケージは非常に大きくなります。完全パッケージのダウンロードが多すぎる場合、ネットワークに負荷がかかる可能性があります。差分は通常はるかに小さく、ネットワーク帯域幅への影響はるかに少なくまります。 クライアント更新要求のネットワーク過負荷の軽減
Mac または Linux	- LiveUpdate サーバー (外部または内部) - リバースプロキシとして設定した Apache Web サーバー Mac または Linux クライアントがリバースプロキシとして Apache Web サーバーを使用して、LiveUpdate 内容をダウンロードすることを有効にすること

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

[LiveUpdate がダウンロードするコンテンツの種類について](#)

[クライアント上のコンテンツと定義を更新する方法](#)

LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード

LiveUpdate コンテンツをダウンロードするように管理サーバーを設定する時は、多くの決定を行う必要があります。つの Symantec Endpoint Protection Manager にコンテンツをダウンロードする時は、サイトのすべての管理サーバーのコンテンツをダウンロードします。

コンテンツのダウンロードに関する決定

Table 135: コンテンツのダウンロードに関する決定

決定	説明
サイトにコンテンツを渡す LiveUpdate サーバーの種類。	外部の Symantec LiveUpdate サーバー（推奨）、またはすでにインストールと設定が行われている 1 台以上の社内 LiveUpdate サーバーのいずれかを指定できます。 つの Symantec Endpoint Protection Manager と社内 LiveUpdate サーバーは、同一の物理ハードウェアや仮想マシンにインストールしないでください。同じコンピュータにインストールすると、重大なサーバーパフォーマンスの問題が生じる可能性があります。 社内 LiveUpdate サーバーを 1 つ以上の使う予定の場合は、シマンテック社の公開 LiveUpdate サーバーを最後のエントリとして追加することを推奨します。クライアントがリストのどのサーバーにも到達できない場合でも、Symantec LiveUpdate サーバーから更新できます。 社内 LiveUpdate サーバーを使い続ける場合は、最新版の LiveUpdate Administrator にアップグレードしてください。 LiveUpdate Administrator のダウンロード 外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定 社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定 クライアント上のコンテンツを更新するための配布方法の選択
サイトはコンテンツリビジョンをいくつ格納する必要がありますか。	12.1.6 以降では、管理サーバーは最近の完全コンテンツパッケージとここで指定する数のリビジョンの増分のみを格納します。この手法では、複数のコンテンツリビジョンをサーバーに格納するために必要なディスク領域が減ります。 つの Symantec Endpoint Protection Manager のインストール中に選択するクライアントの数により、サーバーが格納するリビジョンの数が決まります。 LiveUpdate コンテンツの種類別のデフォルト値は次のようになります。 14 の場合: ・ [管理サーバーは 500 未満のクライアントを管理します] にチェックマークを付けない場合、つの Symantec Endpoint Protection Manager は 21 のリビジョンを格納します。 ・ [管理サーバーは 500 未満のクライアントを管理します] にチェックマークを付けると、つの Symantec Endpoint Protection Manager は 90 のリビジョンを格納します。 12.1.6 の場合、または 14 へのアップグレードの場合: ・ 100 以下のクライアントを選択した場合、つの Symantec Endpoint Protection Manager は 12 のリビジョンを格納します。 ・ 手動で 100 から 500 のクライアントを選択した場合、つの Symantec Endpoint Protection Manager は 21 のリビジョンを格納します。 ・ 500 から 1,000 のクライアントを選択した場合、つの Symantec Endpoint Protection Manager は 42 のリビジョンを格納します。 ・ 1,000 を超えるクライアントを選択した場合、つの Symantec Endpoint Protection Manager は 90 のリビジョンを格納します。 アップグレード中のほとんどのインスタンスで、インストールにより、これらの新しいデフォルトに合わせてリビジョンの数が増えます。この増加は、上記の条件に基づき、アップグレード前のリビジョンの数が新しい最小デフォルトよりも少ない場合に発生します。 Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す
サイトが LiveUpdate コンテンツの更新を確認する頻度。	つの Symantec Endpoint Protection Manager のデフォルトは、ベストプラクティスとして 4 時間ごとに LiveUpdate を実行するようにスケジュールされています。
コンテンツをダウンロードするオペレーティングシステム。	LiveUpdate は指定したオペレーティングシステムの内容のみをダウンロードします。
サイトとクライアントにダウンロードする必要があるコンテンツの種類。	サイトに、クライアントの LiveUpdate Content policy で指定されているすべてのコンテンツがダウンロードされていることを確認します。 LiveUpdate がダウンロードするコンテンツの種類について Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す
ダウンロードして製品の更新で使用する言語。	この設定は製品の更新にのみ適用されます。コンテンツ更新はすべての言語で自動的にダウンロードされます。

決定	説明
ダウンロードする定義のコンテンツサイズ。	バージョン 14 の標準クライアントと埋め込み/VDI クライアントは、クラウド対応の縮小サイズの (最新のもの) 定義セットを使います。これらのクライアントに対するスキャンは、クラウドの拡張定義セットを使います。 14 は、完全な定義セットをダウンロードするダークネットワーククライアントも含んでいます。 12.1.6.x 埋め込み/VDI クライアントは、レガシーの縮小サイズのコンテンツを必要とします。 Warning! 管理サーバーは、ネットワークのクライアントの種類に応じて、正しいコンテンツをダウンロードする必要があります。インストールされたクライアントが必要とするコンテンツを管理サーバーがダウンロードしない場合、クライアントは管理サーバーから更新を取得できません。
リリース前にエンジンの更新をテストする必要があるか。	大規模な組織では、すべてのクライアントコンピュータにロールアウトする前に、新しいエンジンの更新と定義をテストする必要があります。中断や停止時間を最小にして、新しいエンジンの更新をテストします。 Windows クライアントでリリースする前のエンジン更新のテスト

LiveUpdate サーバーから つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード

管理サーバーにコンテンツをダウンロードする時は、サイト内のすべての管理サーバーのコンテンツをダウンロードします。

サイトでコンテンツをダウンロードするように設定するには

1. コンソールで、[管理] > [サーバー] の順に選択します。
2. [サーバー] で、[ローカルサイト] を右クリックして [サイトプロパティを編集] をクリックします。
3. [LiveUpdate] ページで、次の利用可能なオプションから選択します。
4. [LiveUpdate 更新元サーバー] で、[ダウンロード元サーバーの編集] をクリックし、管理サーバーの更新に使われている現在の LiveUpdate サーバーを調べます。このサーバーは、デフォルトで Symantec LiveUpdate サーバーです。次のいずれかの処理を行います。
 - 既存の LiveUpdate 更新元サーバーを使うには、[OK] をクリックします。
 - 社内 LiveUpdate サーバーを使うには、[指定した社内 LiveUpdate サーバーを使う] をクリックし、[追加] をクリックします。

[指定した社内 LiveUpdate サーバーを使う] を選択した場合は、[LiveUpdate サーバーの追加] ダイアログボックスで、その LiveUpdate サーバーを識別する情報をボックスに入力し、[OK] をクリックします。

フェールオーバーの目的で複数のサーバーを追加できます。1 台のサーバーがオフラインになっても、他のサーバーがサポートを提供します。シマンテック社の公開 LiveUpdate サーバーも、リストの最後のサーバーとして追加できます。公開サーバーを追加する場合は、URL として <http://liveupdate.symantecliveupdate.com> を使います。

NOTE

UNC サーバーを使う場合、LiveUpdate のためには、ユーザー名の一部としてドメインまたはワークグループを使う必要があります。

コンピュータがドメイン内にある場合は、ドメイン名\ユーザー名] の順にクリックします。

コンピュータがワークグループ内にある場合は、コンピュータ名\ユーザー名] の順にクリックします。

[LiveUpdate サーバー] ダイアログボックスで [OK] をクリックします。

-
5. [ダウンロードのディスク容量管理] で、保持する LiveUpdate コンテンツリビジョンの数を入力します。
 6. [ダウンロードスケジュール] グループボックスで、[スケジュールの編集] をクリックしてサーバーが更新を確認する必要がある頻度についてのオプションを設定します。[OK] をクリックします。
 7. [ダウンロードするプラットフォーム] で、[プラットフォームの変更] をクリックし、プラットフォームのリストを調べます。コンテンツをダウンロードしないプラットフォームのチェックマークをはずします。
 8. [ダウンロードするコンテンツの種類] で、ダウンロードする更新の種類のリストを調べます。

更新の種類を追加または削除するには、[選択項目の変更] をクリックし、リストを変更してから [OK] をクリックします。

リストはクライアントコンピュータ LiveUpdate Content policy に含めるコンテンツの種類のリストと一致します。

9. [クライアントの種類に対してダウンロードするコンテンツ] の下で、標準クライアントと埋め込み/VDI クライアント、またはダークネットワーククライアントのコンテンツをダウンロードして格納するかどうかを決めます。ネットワークの 12.1.x クライアントを実行する場合は、縮小サイズのコンテンツまたは標準サイズのコンテンツをダウンロードして格納する必要があります。

WARNING

ネットワークのクライアントの種類に応じて、コンテンツをダウンロードする必要があります。インストールしたクライアントが必要とするコンテンツをダウンロードしないと、そのクライアントは管理サーバーから更新を取得できません。

設定を修正する場合は、[選択項目の変更] をクリックして選択項目を修正し、[OK] をクリックします。

10. [ダウンロードする言語] で、ダウンロードする更新の種類の言語リストを調べます。

言語を追加または削除するには、[選択項目の変更] をクリックし、リストを変更してから [OK] をクリックします。

11. [OK] をクリックし、選択項目を保存してウィンドウを閉じます。

クライアント上のコンテンツと定義を更新する方法

つの Symantec Endpoint Protection Manager に最新のコンテンツが含まれていることの確認

LiveUpdate はスケジュールに従って 1 つの Symantec Endpoint Protection Manager に定義などのコンテンツをダウンロードします。ただし、1 つの Symantec Endpoint Protection Manager に最新のバージョンが含まれない場合は、いつでもコンテンツをダウンロードできます。その後、1 つの Symantec Endpoint Protection Manager はデフォルトの LiveUpdate ポリシーを使用して、このコンテンツをクライアントコンピュータに提供します。

1 つの Symantec Endpoint Protection Manager に最新のコンテンツが含まれていることを確認するには

1. コンソールで [ホーム] をクリックします。
2. [エンドポイントの状態] グループボックスの [Windows 定義] で、[管理サーバー上の最新版] と [シマンテック社からの最新版] の日付を比較します。
3. 日付が一致しない場合は、[管理]、[サーバー]、[ローカルサイト (マイサイト)] の順にクリックします。
4. [タスク] で、[LiveUpdate コンテンツのダウンロード]、[ダウンロード] の順にクリックします。

1 つの Symantec Endpoint Protection Manager でコンテンツを LiveUpdate を通じてアップデートできない場合は、シマンテックセキュリティレスポンスから .jdb ファイルをダウンロードできます。1 つの Symantec Endpoint Protection Manager は、これらのファイルのコンテンツを処理して、クライアントからダウンロードできるようにします。

[.jdb ファイルをダウンロードして Endpoint Protection Manager の定義を更新する](#)

コンテンツが **LiveUpdate** から つの **Symantec Endpoint Protection Manager** にダウンロードされた日時の確認
つの Symantec Endpoint Protection Manager でコンテンツが最後に LiveUpdate から更新された日時を判断できま
す。

どのコンテンツが LiveUpdate から つの Symantec Endpoint Protection Manager にダウンロードされたかを確認す
るには

5. コンソールで、[管理] をクリックします。
6. [管理] ページの [タスク] で、[サーバー] をクリックし、サイトを選択します。
7. 次のいずれかのタスクを行います。
 - ダウンロードの状態を確認するには、[LiveUpdate の状態を表示] をクリックします。
 - つの Symantec Endpoint Protection Manager が使用している現在のコンテンツバージョンを確認するに
は、[LiveUpdate の状態を表示] をクリックします。
8. [閉じる] をクリックします。

[Endpoint Protection Manager の LiveUpdate とコンテンツのトラブルシューティング](#)

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

LiveUpdate がダウンロードするコンテンツの種類について

デフォルトで、つの Symantec Endpoint Protection Manager は公開 Symantec LiveUpdate サーバーからすべての種類の
コンテンツをダウンロードします。その後、LiveUpdate Content Policy は つの Symantec Endpoint Protection Manager
からすべての種類のコンテンツを Windows クライアントと Mac クライアントにダウンロードします。

サイトからコンテンツの種類を除外して、LiveUpdate コンテンツポリシーのコンテンツを削除すると、そのコンテンツ
はクライアントに配布されません。通常、つの Symantec Endpoint Protection Manager がダウンロードするコンテンツ
を除外する必要はありません。必要でないことが確実な場合を除いて、コンテンツの種類を除外しないでください。

[Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す](#)

LiveUpdate は更新されたポリシーをダウンロードしません。グループに新しいポリシーを割り当てるか、または既存
のポリシーを編集すると、つの Symantec Endpoint Protection Manager によってクライアントのポリシーが更新されま
す。

Table 136: LiveUpdate から つの Symantec Endpoint Protection Manager にダウンロードできるコンテンツの種類

コンテンツの種類	説明
クライアント製品の更新	Windows クライアントのセキュリティの脆弱性に対するソフトウェアの改善と重要な修正が含まれています。たとえば、攻撃者は Symantec Endpoint Protection の保護機能をバイパスする可能性があります。 LiveUpdate は RUx リリース間で製品の更新を完全なクライアント インストール パッケージとしてダウンロードします。各パッケージは同じバージョン番号ですが、ビルド番号が更新されています。たとえば、最初のクライアント インストール パッケージは 14.3.4555.2000、2 番目のクライアント インストール パッケージは 14.3.5228.1000 とラベル付けされます。このオプションが有効な場合、最新の中間パッケージは [バージョン選択] ドロップダウン リスト内の以下の場所に表示されます。 - 自動更新ウィザード: [管理] ページ > [インストール パッケージ] ページ > [クライアント インストール パッケージ] > [クライアントをパッケージでアップグレード] > [アップグレードの設定] オプション > [全般] タブに表示されます。自動更新ウィザードには、最新のビルドのみ表示されます。 - 新しいパッケージ: [クライアント] ページ > [インストール パッケージ] タブ > [クライアント インストール パッケージの追加] > [全般] タブに表示されます。 このオプションは、14.3 RU2 から 14.3 RU3 のような、新しいリリースで主要な機能を持つクライアントのインストール パッケージをアップグレードするものではありません。自動更新を使用して更新するか、Broadcom [ダウンロード管理] ページからフル クライアント インストール パッケージを手動でダウンロードしてインストールする必要があります。 Mac クライアントと Linux クライアントを更新するには、[クライアント配備ウィザード] の [Web リンクと電子メール] と [パッケージの保存] オプションを使う必要があります。 14.3 RU1 MP1 以前では、このオプションは使用できないため、この設定のチェックマークは外したままにします。 新リリースへのアップグレード 自動更新によるクライアントソフトウェアのアップグレード
クライアント パッチ	製品の更新と同じクライアント ソフトウェアの改善とセキュリティ修正が含まれますが、パッチは完全なクライアント インストール パッケージの代わりに増分デルタ ファイル (.dax) としてダウンロードされます。 クライアントにコンテンツをダウンロードするには、[LiveUpdate 設定] ポリシー > [追加設定] タブに移動し、[クライアント パッチのダウンロード] にチェックを入れます。このオプションを使って、LiveUpdate、管理サーバ、グループ更新プロバイダからクライアント パッチをアップデートできます。 このオプションは、14.3 RU2 でクライアント セキュリティ パッチから名前が変更されました。
ウイルスとスパイウェアの定義	ウイルス定義パッケージは、x86 プラットフォームと x64 プラットフォーム向けに別々に用意されています。このコンテンツの種類には Auto-Protect ポータルリストと Power Eraser 定義も含まれています。
SONAR ヒューリスティックシグネチャ	ゼロデイ攻撃の脅威から保護します。
侵入防止シグネチャ	ネットワークの脅威とホストの脆弱性から保護します。侵入防止と検出エンジン、メモリエクスプロイト緩和機能をサポートします。
ホストインテグリティコンテンツ	更新されたパッチやセキュリティ対策をクライアントコンピュータに強制する、事前定義済みの必要条件のテンプレートが含まれます。LiveUpdate は、Windows オペレーティングシステムと Mac オペレーティングシステムを実行するコンピュータのためのテンプレートをダウンロードします。 テンプレートのカスタム必要条件の追加
提出制御シグネチャ	シマンテックセキュリティレスポンスへの提出のフローを制御します。
評価設定	保護で使われる評価データに対する更新が含まれます。
拡張ファイル属性とシグネチャ	更新証明書とダウンロードインサイトのデータ駆動性を高めるために使います。シマンテック社ではこれらのデータ駆動型ダウンロードを利用して、定義スタイルを更新することにより信頼できるシグネチャのリストを更新します。
エンドポイントの検出とレスポンス	Endpoint Detection and Response (EDR) コンポーネントの更新により、ホストとエンドポイントでの疑わしい活動と問題を検出して調査します。EDR は、提出や EDR サーバーを含むさまざまな製品コンポーネントに犯跡情報を提供します。バージョン 14 で追加されました。 14 RU1 と新しいクライアントに対する Endpoint Detection and Response エンジンの更新

コンテンツの種類	説明
一般的なネットワーク転送のライブラリと設定	ネットワーク転送と遠隔測定を実現するために製品全体で使う定義です。これらの定義は、評価クエリーや、EDR による提出と通信に必要です。このカテゴリの定義には、つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントのそれぞれ用に SEPM STIC と SEPC STIC があります。
高度な機械学習	低帯域幅ポリシーを使用するクライアント用にウイルスとスパイウェアスキャンに使用される定義です (14.0.1 で追加)。インターネット接続が低速なネットワーク内の標準クライアントと埋め込みクライアントで低帯域幅モードを使用します。低帯域幅モードでは、LiveUpdate は週に 1 回またはそれより少ない頻度で定義をダウンロードします。低帯域幅モードを使用するためには、クラウドに登録して低帯域幅ポリシーを有効にする必要があります。低帯域幅モードは、ダークネットワーククライアントでは機能しません。 管理サーバーをクラウドコンソールに登録しない場合や、低帯域幅ポリシーを使用しない場合には、このオプションを無効にして、つの Symantec Endpoint Protection Manager の帯域幅やディスク容量を節約します。 低帯域幅環境でのクライアントのアップデート
WSS トラフィックリダイレクト	Web Security Services (WSS) トラフィックリダイレクト機能が使用する定義です。WSS トラフィックリダイレクトは、WSS サーバーを使用して、Web ブラウザに安全なプロキシ設定を提供します。(14.1 MP1 で追加)
SymPlatform 定義	Symantec Endpoint Foundation (SEF) は、LiveUpdate を通じて今後の保護技術をコンテンツとして提供するフレームワークです。SEF を使用すると、クライアントをアップグレードすることなく、新しい機能をダウンロードできます。 14.3 RU1 以降のクライアントで実行される URL 評価の定義が含まれます。
アプリケーション制御のコンテンツ	アプリケーション制御ポリシーにアプリケーション制御エンジンが使用する定義。このオプションは常に有効にしておく必要があります。 このコンテンツは、バージョン 14.2 以降のクライアントでのみで実行します。古い Windows クライアントは、まず 14.2 にアップグレードする必要があります。
ポリシー コマンド ハンドラ	ポリシーコマンドハンドラーエンジンによって使用されるコンテンツ。
AD データのエンドポイント脅威対策	Active Directory Defense エンジンによって使用されるコンテンツ。14.2 RU1 で追加されました。
ブラウザ拡張機能	Google Chrome で悪質な Web サイトを遮断するためにクライアントが使用するエンジンのコンテンツをダウンロードします。14.3 RU2 で追加されました。

Endpoint Protection 14 用の LiveUpdate Administrator コンテンツのオプション

LiveUpdate コンテンツポリシーでは、[拡張ファイル属性とシグネチャ]、[エンドポイント検出およびレスポンス]、[一般的なネットワーク転送のライブラリと設定] などの種類のコンテンツを無効にできません。

Table 137: 機能と更新が必要なコンテンツ

管理外クライアントをインストールする場合	更新時に、ダウンロードする必要があるコンテンツの種類
ウイルス対策とスパイウェア対策	• ウイルス定義とスパイウェア定義 • SONAR 定義 [サイトのプロパティ] でダウンロードするコンテンツの種類を設定する場合、これらは [SONAR ヒューリスティックシグネチャ] という名称です。 • 集中型評価の設定 [サイトのプロパティ] でダウンロードするコンテンツの種類を設定する場合、このコンテンツの種類は [評価設定] という名称です。 • 失効データ (デフォルトでダウンロードされる、つの Symantec Endpoint Protection Manager では設定不可) • Symantec 許可リスト (Symantec ホワイトリスト) • 提出制御シグネチャ • Auto-Protect ポータルリスト • Power Eraser の定義 • 拡張ファイル属性とシグネチャ (14 以降) • Endpoint Detection and Response (14 以降) • 一般的なネットワーク転送のライブラリと設定 • 高度な機械学習 (14.1 以降)
ウイルス対策とスパイウェア対策の設定 > ダウンロード保護	• ウイルス定義とスパイウェア定義 • SONAR 定義 [サイトのプロパティ] でダウンロードするコンテンツの種類を設定する場合、これらは [SONAR ヒューリスティックシグネチャ] という名称です。 • 集中型評価の設定 • 失効データ • Symantec 許可リスト (Symantec ホワイトリスト) • 侵入防止シグネチャ このオプションを選択してダウンロードすると、侵入防止シグネチャと侵入防止エンジンの両方の更新が含まれます。 • 提出制御シグネチャ • Auto-Protect ポータルリスト • Power Eraser の定義 • 拡張ファイル属性とシグネチャ (14 以降) • Endpoint Detection and Response (14 以降) • 一般的なネットワーク転送のライブラリと設定 • 高度な機械学習 (14.1 以降)

管理外クライアントをインストールする場合	更新時に、ダウンロードする必要があるコンテンツの種類
ウイルスとスパイウェアの対策 > Outlook スキャナ	• ウイルス定義とスパイウェア定義 • SONAR 定義 [サイトのプロパティ] でダウンロードするコンテンツの種類を設定する場合、これらは [SONAR ヒューリスティックシグネチャ] という名称です。 • 集中型評価の設定 • 失効データ • Symantec 許可リスト (Symantec ホワイトリスト) • 提出制御シグネチャ • Auto-Protect のポータルリスト • Power Eraser の定義 • 拡張ファイル属性とシグネチャ • Endpoint Detection and Response (14 以降) • 一般的なネットワーク転送のライブラリと設定 • 高度な機械学習 (14.1 以降)
ウイルスとスパイウェアの対策 > Notes スキャナ	• ウイルス定義とスパイウェア定義 • SONAR 定義 [サイトのプロパティ] でダウンロードするコンテンツの種類を設定する場合、これらは [SONAR ヒューリスティックシグネチャ] という名称です。 • 集中型評価の設定 • 失効データ • Symantec 許可リスト (Symantec ホワイトリスト) • 提出制御シグネチャ • Auto-Protect のポータルリスト • Power Eraser の定義 • 拡張ファイル属性とシグネチャ • Endpoint Detection and Response (14 以降) • 一般的なネットワーク転送のライブラリと設定 • 高度な機械学習 (14.1 以降)
プロアクティブ脅威防止 > SONAR	SONAR 定義 提出制御シグネチャ 拡張ファイル属性とシグネチャ 高度な機械学習
プロアクティブ脅威防止 > アプリケーション制御	提出制御シグネチャ 拡張ファイル属性とシグネチャ アプリケーション制御のコンテンツ (14.2 以降)
Network Traffic Redirection ポリシー	WSS トラフィックリダイレクト (14.1 MP1 以降)
ネットワークとホスト悪用防止 > 侵入防止	• 侵入防止シグネチャ このオプションを選択してダウンロードすると、侵入防止シグネチャと侵入防止エンジンの両方の更新が含まれます。 • 提出制御シグネチャ • 拡張ファイル属性およびシグネチャ • ブラウザ拡張機能 (14.3 RU2 以降)
ネットワークとホストのエクспロイト緩和機能 > ファイアウォール	提出制御シグネチャ 拡張ファイル属性とシグネチャ

管理外クライアントをインストールする場合	更新時に、ダウンロードする必要があるコンテンツの種類
ホストインテグリティ	ホストインテグリティコンテンツ 提出制御シグネチャ 拡張ファイル属性とシグネチャ

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

[クライアント上のコンテンツと定義を更新する方法](#)

[クライアント上のコンテンツを更新するための配布方法の選択](#)

社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

デフォルトでは、Windows、Mac、および Linux のクライアントが管理サーバーから更新を取得します。

多くのクライアントを管理する場合、Windows クライアントにグループ更新プロバイダ (GUP) を使うことを推奨します。GUP は管理サーバーの負荷を軽減し、その設定は社内 LiveUpdate サーバーよりも簡単です。

[クライアントにコンテンツを配布するための GUP の使用](#)

クライアントの更新にデフォルトの管理サーバーまたは GUP を使わない場合は、以下が可能です。

- 社内 LiveUpdate サーバーを設定します。
- 会社のネットワークの外側にある Symantec LiveUpdate サーバーを使います。

社内の LiveUpdate サーバーを使うには、次のタスクを実行する必要があります。

- 社内 LiveUpdate サーバーをインストールします。
社内 LiveUpdate サーバーの使用について詳しくは、『LiveUpdate #####』を参照してください。

NOTE

つの Symantec Endpoint Protection Manager は LiveUpdate Administrator 1.x のレガシーサポートに対応していません。社内 LiveUpdate サーバーを使い続ける場合は、最新版の LiveUpdate Administrator にアップグレードしてください。LiveUpdate Administrator 2.x 以降のサポートは常に有効です。

- その社内 LiveUpdate サーバーを使うようにクライアントを設定するには、LiveUpdate 設定ポリシーを使います。

NOTE

更新のために社内 LiveUpdate サーバーに接続するクライアントのプロキシ設定を指定できます。プロキシ設定は更新のためにのみ指定します。クライアントが使うその他の種類の外部通信には適用されません。その他の種類のクライアント外部通信用のプロキシは別に設定します。

[クライアントが Symantec LiveUpdate または社内 LiveUpdate サーバーへの通信に使うプロキシサーバーの指定](#)

社内の LiveUpdate サーバーを使うように Windows クライアントを設定するには

1. [ポリシー] で、[LiveUpdate] をクリックします。
2. [LiveUpdate の設定] タブで、編集するポリシーを開きます。
3. [Windows の設定] の下で、[サーバーの設定] をクリックします。
4. [サーバーの設定] ペインで、[LiveUpdate サーバーを使う] にチェックマークを付けます。
5. [指定した社内 LiveUpdate サーバーを使う] をクリックし、[追加] をクリックします。
6. [LiveUpdate サーバーの追加] ダイアログボックスで、使うサーバーを識別して通信するために必要な情報を入力します。

URL の場合:

-
- HTTP または HTTPS 方式を使う場合、サーバーの URL を入力します。例: ドメイン名: `http://myliveupdateserver.com`
 - IPv4 アドレス: `http://192.168.133.11:7070/clu-prod`
 - IPv6 アドレス: `http://[fd00:fe32::b008]:7070/clu-prod`
 - FTP 方式を使う場合、サーバーの FTP アドレスを入力します。たとえば、`ftp://myliveupdateserver.com` など。
 - LAN 方式を使う場合、サーバー UNC パス名を入力します。たとえば、`\\myliveupdateserver\LUDepot` など。
7. 必要に応じて、サーバーのユーザー名とパスワードを入力し、[OK] をクリックします。

NOTE

UNC サーバーを使う場合、LiveUpdate のためには、ユーザー名に加えてドメインまたはワークグループを使う必要があります。コンピュータがドメインの一部の場合は、ドメイン名\ユーザー名] の順にクリックします。コンピュータがワークグループの一部の場合は、コンピュータ名\ユーザー名] の順にクリックします。

8. [LiveUpdate ポリシー] の下で、[スケジュール] をクリックし、LiveUpdate による更新のスケジュールを設定して [OK] をクリックします。

クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定

9. 必要に応じて、[拡張設定] をクリックします。
- デフォルトのユーザー設定、製品更新の設定、非標準ヘッダーの設定をそのままにしておくか、変更するかを決定します。通常、ユーザーには更新の設定を変更できないようにします。ただし、サポートしているクライアントが少ない場合は、ユーザーが手動で LiveUpdate セッションを起動するようにもできます。

ユーザーが LiveUpdate に対して持つ制御権限の設定

10. [OK] をクリックします。

社内の **LiveUpdate** サーバーを使うように **Mac** クライアントまたは **Linux** クライアントを設定するには

1. [ポリシー] ページで、[LiveUpdate] をクリックします。
2. [LiveUpdate の設定] タブで、ポリシーを開きます。
3. [Mac の設定] または [Linux の設定] で、[サーバーの設定] をクリックします。
4. [指定した社内 **LiveUpdate** サーバーを使う] をクリックし、[追加] をクリックします。
5. [LiveUpdate サーバーの追加] ダイアログボックスで、使うサーバーを識別して通信するために必要な情報を入力します。

URL の場合:

- HTTP または HTTPS 方式を使う場合、サーバーの URL を入力します。例: ドメイン名: `http://myliveupdateserver.com`
 - IPv4 アドレス: `http://192.168.133.11:7070/clu-prod`
 - IPv6 アドレス: `http://[fd00:fe32::b008]:7070/clu-prod`
 - FTP 方式を使う場合、サーバーの FTP アドレスを入力します。たとえば、`ftp://myliveupdateserver.com` など。
 - LAN 方式を使う場合、サーバー UNC パス名を入力します。たとえば、`\\myliveupdateserver\LUDepot` など。
6. 必要に応じてサーバーのユーザー名とパスワードを入力し、[OK] をクリックします。
 7. サーバーで FTP を使用する場合、[サーバーの拡張設定] をクリックし、サーバーで使う FTP のモード ([アクティブ] または [パッシブ] のいずれか) をクリックし、[OK] をクリックします。
 8. スケジュールを修正するには、[スケジュール] をクリックします。
 9. [OK] をクリックします。

LiveUpdate サーバーからのコンテンツダウンロードのランダム化

Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行する設定

クライアント上のコンテンツを更新するための配布方法の選択

外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

デフォルトでは、つの Symantec Endpoint Protection Manager は Windows クライアントに更新を提供します。Windows クライアントの更新のネットワーク負荷を軽減するには、クライアントが LiveUpdate サーバーから更新を取得できるようにする必要があります。Linux および Mac クライアントは LiveUpdate サーバーから更新を取得する必要があります。あるいは、Apache Web サーバーをリバースプロキシとして設定し、管理サーバーから更新をダウンロードできます。

クライアント上のコンテンツを更新するための配布方法の選択

Mac および Linux クライアントがリバースプロキシとして Apache Web サーバーを使用して、LiveUpdate 内容をダウンロードすることを有効にすること

NOTE

プロキシサーバーがシマンテック製品の更新サービスと接続できるように、プロキシサーバーと つの Symantec Endpoint Protection Manager 間の通信を確立することもできます。プロキシサーバーはサイトと外部 Symantec LiveUpdate サーバーとの間に、保護のレベルを追加提供できます。

インターネットにアクセスして Symantec LiveUpdate からコンテンツをダウンロードするためにプロキシサーバーに接続する つの Symantec Endpoint Protection Manager の設定

外部 LiveUpdate サーバーからコンテンツをダウンロードするようにクライアントを設定するには

1. コンソールで LiveUpdate ポリシーを開き、[編集] をクリックします。
2. [Windows 設定]、[Mac 設定]、[Linux 設定] の下で、[サーバーの設定] をクリックします。
3. [デフォルト **Symantec LiveUpdate server** を使う] をクリックするか、別の LiveUpdate サーバーを指定します。必要に応じて、プロキシ設定を指定します。
4. [OK] をクリックします。

クライアント上のコンテンツと定義を更新する方法

インターネットにアクセスして Symantec LiveUpdate からコンテンツをダウンロードするためにプロキシサーバーに接続する つの Symantec Endpoint Protection Manager の設定

つの Symantec Endpoint Protection Manager は、プロキシサーバーを経由してインターネットに接続するように設定できます。インターネットに直接接続されるのはプロキシサーバーのみなので、プロキシサーバーを使えばセキュリティ層を追加できます。

インターネットにアクセスして Symantec LiveUpdate からコンテンツをダウンロードするためにプロキシサーバーに接続する つの Symantec Endpoint Protection Manager を設定するには

1. コンソールで、[管理] をクリックし、[サーバー] をクリックします。
2. [サーバー] で、プロキシサーバーの接続先の管理サーバーを選択します。
3. [タスク] の下で、[サーバーのプロパティを編集する] をクリックします。
4. [プロキシサーバー] タブの [HTTP プロキシの設定] または [FTP プロキシの設定] のいずれかで、[プロキシの使用状況] について [カスタムプロキシ設定を使う] を選択します。
5. プロキシの設定を入力します。
これらの設定について詳しくは [ヘルプ] をクリックしてください。
6. [OK] をクリックします。

クライアントが Symantec LiveUpdate または社内 LiveUpdate サーバーへの通信に使うプロキシサーバーの指定

クライアントが Symantec LiveUpdate または社内 LiveUpdate サーバーへの通信に使うプロキシサーバーの指定

クライアントが社内 LiveUpdate サーバーとの通信に使うプロキシサーバーを指定できます。プロキシの設定はグループ更新プロバイダの設定に影響しません。

NOTE

他のクライアント通信に対するプロキシは別に設定します。

1. オプション 1: Windows コンピュータまたは Linux コンピュータのクライアントが Symantec LiveUpdate または社内の LiveUpdate サーバーへの通信に使うプロキシサーバーを指定するには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] で [LiveUpdate] をクリックし、[LiveUpdate の設定] タブをクリックします。
3. 目的のポリシーを右クリックして、[編集] を選択します。
4. [Windows 設定] または [Linux 設定] で、[サーバーの設定] をクリックします。
5. [LiveUpdate プロキシの設定] で、[プロキシオプションの設定] をクリックします。
6. 次のいずれかの操作をします。
 - Windows クライアントの場合、[HTTP または HTTPS] タブで任意のオプションを選択します。FTP のプロキシ設定を指定することもできます。
 - Linux クライアントの場合、[HTTP] タブで任意のオプションを選択します。オプションについて詳しくは、オンラインヘルプを参照してください。
7. ダイアログボックスで [OK] をクリックします。
8. [OK] をクリックします。
9. オプション 2: Mac コンピュータ上のクライアントが Symantec LiveUpdate または社内の LiveUpdate サーバーへの通信に使うプロキシサーバーを指定するには、コンソールで [クライアント] > [ポリシー] をクリックします。
10. [場所に依存しないポリシーと設定] の [設定] で、[外部通信の設定] をクリックします。
11. [プロキシサーバー (Mac)] タブで、必要なオプションを選択します。
オプションについて詳しくは、オンラインヘルプを参照してください。
12. [OK] をクリックします。

クライアント上のコンテンツと定義を更新する方法

クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定

LiveUpdate クライアントのスケジュール設定は、LiveUpdate 設定ポリシーで定義されます。これらの設定は Symantec LiveUpdate server または社内の LiveUpdate サーバーから最新の更新を取得する LiveUpdate セッションに適用されます。

外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

帯域幅を節約するために、次の条件のいずれかを満たす場合にのみクライアントで定時 LiveUpdate セッションを実行するようにできます。

-
- クライアントコンピュータのウイルス定義とスパイウェア定義の経過日数が 2 日を越えている
 - クライアントコンピュータが 7 日の Symantec Endpoint Protection Manager から 8 時間以上接続解除されている

NOTE

ネットワークにあまり接続しないクライアントコンピュータで確実に最新の更新を取得するには、これらのコンピュータが Symantec LiveUpdate server から更新を取得するようにします。これらのサーバーは公開サーバーです。そのため、クライアントがネットワークに接続しているかどうかにかかわらず更新を取得します。

1. オプション 1: Windows クライアントコンピュータへの LiveUpdate ダウンロードのスケジュールを設定するには、[ポリシー] をクリックしてから、[LiveUpdate] をクリックします。
2. [LiveUpdate の設定] タブで、目的のポリシーを右クリックして、[編集] をクリックします。
3. [Windows の設定] の下で、[スケジュール] をクリックします。
4. [LiveUpdate スケジュールを有効にする] にチェックマークを付けていることを確認します。このオプションはデフォルトで有効になっています。
5. 頻度を指定します。
[毎日] を選択した場合は、実行する時刻も設定します。[毎週] を選択した場合は、実行する時刻と曜日も設定します。
6. [連続的] 以外の頻度を選択した場合は、[再試行ウィンドウ] を指定します。
[再試行ウィンドウ] は、定時 LiveUpdate が何らかの理由で失敗した場合に、クライアントコンピュータが LiveUpdate を実行しようとする時間数または日数です。
7. 必要に応じてその他のオプションを設定します。定義が最新でない場合や最近クライアントが管理サーバーに接続していない場合はデフォルト値のままにして LiveUpdate を実行することを推奨します。

8. [OK] をクリックします。

LiveUpdate サーバーからのコンテンツダウンロードのランダム化

9. オプション 2: Mac クライアントコンピュータへの LiveUpdate ダウンロードのスケジュールを設定するには、[ポリシー] をクリックしてから、[LiveUpdate] をクリックします。
10. [LiveUpdate 設定ポリシー] ページで、目的のポリシーを右クリックして [編集] をクリックします。
11. [Mac の設定] の下で、[スケジュール] をクリックします。
12. 頻度を指定します。
[毎日] を選択した場合は、実行する時刻も設定します。[毎週] を選択した場合は、実行する時刻と曜日も設定します。
13. 終了したら [OK] をクリックします。
14. オプション 3: Linux クライアントコンピュータへの LiveUpdate ダウンロードのスケジュールを設定するには、[LiveUpdate 設定ポリシー] タブで、目的のポリシーを右クリックして、[編集] をクリックします。
15. [Linux の設定] の下で、[スケジュール] をクリックします。
16. [LiveUpdate スケジュールを有効にする] にチェックマークを付けます。このオプションはデフォルトで有効になっています。

NOTE

このボックスのチェックマークをはずすべきではありません。[LiveUpdate スケジュール] を無効にすると、Linux クライアントが最新の更新を受信しなくなります。

17. 頻度を指定します。

[毎日] を選択した場合は、実行する時刻も設定します。[毎週] を選択した場合は、実行する時刻と曜日も設定します。

18. [連続的] 以外の頻度を選択した場合は、[再試行ウィンドウ] を指定します。

[再試行ウィンドウ] は、定時 LiveUpdate が失敗した場合にクライアントコンピュータが LiveUpdate を試行するまでの時間数または日数です。

コンテンツダウンロードをランダム化することもできます。

19. [OK] をクリックします。

クライアント上のコンテンツと定義を更新する方法

ユーザーが LiveUpdate に対して持つ制御権限の設定

出張するユーザーに、インターネット接続を使って Symantec LiveUpdate server から更新を直接取得することを許可したい場合があります。また、コンテンツダウンロードについて設定した LiveUpdate スケジュールの修正をユーザーに許可できます。

NOTE

インストールパッケージが作成されたときに、管理外クライアントに LiveUpdate の設定ポリシーが割り当てられていた場合、ユーザーによるコンピュータの再起動後に、そのポリシーの設定はユーザーの変更よりも常に優先されます。コンピュータを再起動した後にユーザーが変更した LiveUpdate の設定を保つ管理外クライアントをインストールするには、インストールファイルからクライアントをインストールします。つの Symantec Endpoint Protection Manager からエクスポートされたクライアントインストールパッケージは使わないでください。

ユーザーが LiveUpdate に対して持つ制御権限を設定するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシー] で、[LiveUpdate] をクリックします。
3. [LiveUpdate の設定] タブで、目的のポリシーを右クリックして、[編集] をクリックします。
4. [Windows の設定] の下で、[拡張設定] をクリックします。
5. [ユーザー設定] ペインで、[ユーザーが手動で LiveUpdate を起動するのを許可する] にチェックマークを付けます。
6. オプションで、[ユーザーに LiveUpdate スケジュールを修正を許可する] にチェックマークを付けます。
7. [OK] をクリックします。

Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す

クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定

クライアント更新要求のネットワーク過負荷の軽減

管理サーバーまたは GUP から同時にウイルスとスパイウェアの完全な定義セットのダウンロードを要求するクライアントの数が多すぎるという、発生頻度は低いものの重大な状況では、ネットワークの管理が必要になります。この状況は、管理サーバーにエラーが発生したり、ディスク容量を使い果たしたりした場合に発生します。そのためクライアントでの定義のダウンロードと更新が失敗します。この状況は、管理サーバーが定義パッケージをダウンロードせず、クライアントがこの特定の差分を要求する場合にも発生することがあります。いずれにしても、クライアントは管理サーバーまたは GUP から完全な定義のセットを含むパッケージを要求する必要があります。

ネットワークでの過負荷を防ぐため、管理サーバーは次の機能を提供します。

-
- 指定した時間内に、指定した数の完全な定義セットの要求を管理サーバーが受け取ったときの通知。
この通知の条件は、環境における過負荷の原因に応じて設定します。通知を設定するには、[ネットワークロード: ウィルスとスパイウェアの完全定義の要求] という通知の定義を追加します。

管理者通知の設定

- 管理サーバーが完全セットのみを提供する場合に、クライアントがウィルスとスパイウェアの定義の差分を LiveUpdate サーバーから取得できるようにする機能。LiveUpdate 設定ポリシーで、[拡張設定]、[LiveUpdate サーバーから小さなクライアントインストールパッケージをダウンロードします] の順にクリックします。
- クライアントが管理サーバーからウィルスとスパイウェアの完全な定義セットをダウンロードできないようにする機能。
ネットワークの過負荷の通知を受け取ると、その後管理サーバーからの完全なパッケージのダウンロードを遮断できます。ただし、すでに進行中のダウンロードは停止できません。このオプションは、[管理] > [サーバー] > サーバー名 > [サーバーのプロパティを編集] > [完全定義のダウンロード] > [クライアントが完全定義パッケージをダウンロードできないようにする] の順にクリックして構成します。

完全定義のダウンロード

同時コンテンツダウンロードのランダム化について

この Symantec Endpoint Protection Manager はデフォルト管理サーバーまたは GUP (Group Update Provider) からクライアントへの同時コンテンツダウンロードのランダム化をサポートします。LiveUpdate サーバーからクライアントへのコンテンツダウンロードのランダム化もサポートします。ランダム化はピーク時のネットワークトラフィックを減らしデフォルトで有効になっています。

ランダム化機能は有効または無効にできます。デフォルト設定は有効です。ランダム化ウィンドウを設定することもできます。管理サーバーはランダム化ウィンドウを使ってコンテンツダウンロードのタイミングをずらしします。通常は、デフォルトのランダム化設定を変更する必要はありません。

ただし、場合によっては、ランダム化ウィンドウの値を増やす必要があります。たとえば、管理サーバーを実行する同じ物理コンピュータ上の複数の仮想コンピュータで Symantec Endpoint Protection クライアントを実行することがあります。ランダム化の値を大きくするとサーバーのパフォーマンスは向上しますが、仮想マシンへのコンテンツ更新は遅くなります。

管理サーバーを実行する単一のサーバーに多くの物理クライアントコンピュータが接続しているときにもランダム化ウィンドウを大きくすることが必要になる場合があります。一般に、クライアントとサーバーの比率が大きいほど、ランダム化ウィンドウに設定する値を高くする必要があります。ランダム化の値を大きくするとサーバーのピーク負荷は小さくなりますが、クライアントコンピュータへのコンテンツ更新は遅くなります。

クライアントの数が非常に少なくコンテンツの配信を急ぐ場合は、ランダム化ウィンドウに設定する値を小さくします。ランダム化の値が小さいほどサーバーのピーク負荷は大きくなりますが、クライアントへのコンテンツ配信は速くなります。

デフォルト管理サーバーまたは GUP からのダウンロードの場合は、選択したグループの [通信の設定] ダイアログボックスでランダム化を設定します。この設定は LiveUpdate 設定ポリシーには含まれません。

LiveUpdate サーバーからクライアントへのダウンロードの場合は、LiveUpdate 設定ポリシーの一部としてランダム化の設定を行います。

デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化

LiveUpdate サーバーからのコンテンツダウンロードのランダム化

社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化

複数のクライアントコンピュータが同時にデフォルトの管理サーバーまたは GUP からのコンテンツのダウンロードを試みると、それらのサーバーや GUP ではパフォーマンスの低下が発生することがあります。クライアントコンピュータの所属先グループの通信設定でランダム化ウィンドウを設定できます。各クライアントコンピュータは、そのウィンドウ内のランダムな時刻にコンテンツのダウンロードを試みます。

NOTE

この通信設定では、LiveUpdate サーバーからコンテンツをダウンロードするクライアントコンピュータのランダム化の設定は制御されません。それらのコンピュータのランダム化の設定は LiveUpdate 設定ポリシーで変更できます。

LiveUpdate サーバーからのコンテンツダウンロードのランダム化

デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードをランダム化するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] の下で、目的のグループをクリックします。
3. [ポリシー] タブの [場所に依存しないポリシーと設定] の [設定] で、[通信の設定] をクリックします。
4. [通信の設定] ダイアログボックスの [ダウンロードランダム化] で、[ランダム化を有効にする] にチェックマークを付けます。
5. オプションで、ランダム化ウィンドウの期間を変更します。
6. [OK] をクリックします。

同時コンテンツダウンロードのランダム化について

社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

LiveUpdate サーバーからのコンテンツダウンロードのランダム化

複数のクライアントコンピュータが LiveUpdate サーバーからのコンテンツのダウンロードを試みると、ネットワークでトラフィックの混雑が発生することがあります。Windows または Linux クライアントのランダム化ウィンドウを含めるように更新スケジュールを設定できます。各クライアントコンピュータは、そのウィンドウ内のランダムな時刻にコンテンツのダウンロードを試みます。

NOTE

LiveUpdate 設定ポリシー内のスケジュール設定では、デフォルトの管理サーバーまたは GUP からコンテンツをダウンロードするクライアントコンピュータのために、ランダム化は制御されません。それらのコンピュータのランダム化の設定は、コンピュータが属するグループの [通信の設定] ダイアログボックスで変更できます。

デフォルトの管理サーバーまたは GUP からのコンテンツダウンロードのランダム化

LiveUpdate サーバーからのコンテンツダウンロードをランダム化するには

-
1. [ポリシー] をクリックします。
 2. [ポリシー] で、[LiveUpdate] をクリックします。
 3. [LiveUpdate の設定] タブで、編集するポリシーを右クリックし、次に [編集] をクリックします。
 4. [Windows 設定]、[Mac 設定]、[Linux 設定] の下で、[スケジュール] をクリックします。
 5. [ダウンロードランダム化オプション] の下で、[開始日時を時間単位の±でランダム化する] にチェックマークを付けます。

NOTE

この設定は、[週単位] の更新を選択する場合は日単位です。

6. オプションで、ランダム化された開始日時の期間を変更します。
7. [OK] をクリックします。

同時コンテンツダウンロードのランダム化について

社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行する設定

Windows クライアントコンピュータのパフォーマンスの問題を軽減するため、クライアントコンピュータがアイドル状態のときにコンテンツのダウンロードが実行されるように設定できます。この設定はデフォルトでオンになります。コンピュータがいつアイドル状態になっているかを特定するためには、ユーザー、CPU、ディスクの動作など、いくつかの基準が使われます。

[アイドル検出] が有効になっている場合、いったん更新の期日になると、次の条件によってセッションの遅延が起きることがあります。

- ユーザーがアイドル状態でない。
- コンピュータがバッテリー電源で動作中。
- CPU がビジー状態。
- ディスク I/O がビジー状態。
- ネットワーク接続が存在しない。

1 時間後、実行を妨げる条件は CPU がビジー状態、ディスク I/O がビジー状態、ネットワーク接続が存在しない、に少なくなります。定時更新が 2 時間遅滞すると、ネットワーク接続が存在すればアイドルの状態を無視して定時 LiveUpdate が実行されます。

Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行するように設定するには

1. [ポリシー] をクリックします。
2. [ポリシー] で、[LiveUpdate] をクリックします。
3. [LiveUpdate の設定] タブで、編集するポリシーを右クリックし、次に [編集] をクリックします。
4. [Windows の設定] の下で、[スケジュール] をクリックします。
5. **Delay scheduled LiveUpdate until the computer is idle.** を調べてください遅滞のセッションは無条件で動作します。
6. [OK] をクリックします。

クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定

定義が古いときや Windows コンピュータが切断されていたときに実行するクライアント更新の設定

定義が古いときや Windows コンピュータが切断されていたときに実行するクライアント更新の設定

定義が古いとき、または指定された期間コンピュータがネットワークから切断されていたときに、Windows クライアントが更新されるようにできます。

NOTE

両方の利用可能なオプションにチェックマークを付けた場合、クライアントコンピュータは両方の条件を満たす必要があります。

定義が古いときに、またはコンピュータがマネージャから切断されているときに Windows クライアント更新を設定するには

1. [ポリシー] をクリックします。
2. [ポリシー] で、[LiveUpdate] をクリックします。
3. [LiveUpdate の設定] タブで、編集するポリシーを右クリックし、次に [編集] をクリックします。
4. [Windows の設定] の下で、[スケジュール] をクリックします。
5. [LiveUpdate が動作するのはウイルス定義やスパイウェア定義の経過日数が次の日数を超えた場合のみです:] にチェックマークを付けてから、時間数または日数を指定します。
6. [LiveUpdate が動作するのはクライアントが つの **Symantec Endpoint Protection Manager** から切断されてからの経過日数が次の日数を超えた場合のみです:] にチェックマークを付けてから、分数または時間数を指定します。
7. [OK] をクリックします。

[クライアントコンピュータへの LiveUpdate ダウンロードスケジュールの設定](#)

[Windows クライアントコンピュータがアイドル状態のときにクライアント更新を実行する設定](#)

つの Symantec Endpoint Protection Manager からコンテンツをダウンロードするためのクライアントの設定

クライアントにコンテンツをダウンロードするためのデフォルトの方法は、管理サーバーを使うことです。

管理サーバーからクライアントに対する更新のスケジュールを定義しないでください。クライアントは、通信モードとハートビート頻度に基づき管理サーバーからコンテンツをダウンロードします。

つの Symantec Endpoint Protection Manager からコンテンツをダウンロードするようにクライアントを設定するには

1. コンソールで LiveUpdate ポリシーを開き、[編集] をクリックします。
2. [Windows の設定] の下で、[サーバーの設定] をクリックします。
3. [デフォルト管理サーバーを使う] にチェックマークを付けていることを確認します。
4. [OK] をクリックします。

[プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新](#)

Windows クライアントでリリースする前のエンジン更新のテスト

Symantec Endpoint Protection には、その機能の一部を実行するエンジンがいくつか含まれています。これらのエンジンは、バイナリファイル (.dll または .exe) であり、セキュリティ定義と共に提供されます。シマンテック社は、これらのエンジンの機能を更新して、Symantec Endpoint Protection の機能を強化し、新しい脅威に対応します。

シマンテック社は 1 日に数回ウイルス定義を更新しますが、エンジンコンテンツの更新は四半期単位です。エンジンは LiveUpdate を使用して更新されます。

バージョン 14.0.1 MP1 以降では、シマンテック社は、実働環境にエンジンコンテンツをロールアウトする前にコンテンツをダウンロードしてテストできる特別なサーバーを提供します。これらの更新は早期採用サーバー (EAS) でリリースされます。一般リリースで LiveUpdate 公開サーバーからエンジンが入手できるようになる数週間前に、エンジンの更新がリリースされます。

EAS を使用してエンジンの更新をダウンロードして、ラボ環境で試し、シマンテック社まで、発生した競合をお知らせください。このプロセスにより、シマンテック社は、一般リリース前にこの競合を修正できます。

エンジンの更新をテストするには、次の手順を使用します。

ステップ 1: コンテンツを受信するテストコンピュータのグループを作成する

ステップ 2: 早期採用サーバーからプレリリースコンテンツを受信するテストコンピュータを設定する

ステップ 3: 特定のエンジンバージョンに対してテストコンピュータと非テストコンピュータを設定する

ステップ 4: 新しいエンジンのリリースに関する通知を設定する (省略可能)

ステップ 5: エンジンコンテンツがリリースされた後、テストコンピュータを監視する

ステップ 1: コンテンツを受信するテストコンピュータのグループを作成する

エンジンの互換性の最も正確なテストには、実際の作業を行う実働システムを利用します。次の基準を使用して EAS コンテンツを受信するクライアントコンピュータのセットを選択して、永続的なテストグループを作成します。

- 環境内の重要なシステムのさまざまな種類を識別します。これらのシステムは、ハードウェア、ソフトウェア、機能によって、互いに異なる場合があります。たとえば、デスクトップのゴールデンイメージ (マスターイメージ)、POS システム、Web サーバーなどの小売りシステムを、テストする他の重要なシステムから識別する可能性があります。
- 一部のソフトウェアの競合は断続的にのみ現れるため、各種類に対して複数のシステムを使用します。通常使用して、代表的な作業負荷を実行するソフトウェアがインストールされている実働システムを選択します。
- 早期リリースコンテンツを受信するテストクライアントコンピュータを、テストしない実働コンピュータに似せて設定します。テストクライアントと非テストクライアントの両方が、同じ Symantec Endpoint Protection 機能をインストールして、同じポリシーを使用する必要があります。

EAS によるテストに実働コンピュータを使用したくない場合、ラボベースのシステムを使用できます。この場合、テストでシステムの機能を実行して負荷をシミュレーションする自動化のコーディングを行うと便利です。

クライアントコンピュータが少数の場合、必要なのは 1 つの Symantec Endpoint Protection Manager 1 つと Windows クライアント用の Symantec Endpoint Protection 1 つです。

ステップ 2: 早期採用サーバーからプレリリースコンテンツを受信するテストコンピュータを設定する

テストグループについては、次の手順を実行して、シマンテック社の早期採用サーバーからコンテンツをダウンロードするように LiveUpdate を設定します。

シマンテック社の早期採用 **LiveUpdate** サーバーからコンテンツをダウンロードするサイトを設定するには

1. コンソールで、[管理] > [サーバー] の順に選択します。
2. [サーバー] で、[ローカルサイト] を右クリックして [サイトプロパティを編集] をクリックします。
3. [LiveUpdate 更新元サーバー] で、[ダウンロード元サーバーの編集] をクリックします。
4. [LiveUpdate サーバー] ダイアログボックスで、[プレリリースのコンテンツに **Symantec LiveUpdate** サーバーを使用] をクリックして、[OK] > [OK] とクリックします。

シマンテック社の早期採用 **LiveUpdate** サーバーでプレリリースを使用する管理下クライアントを設定するには

1. コンソールで、新しい LiveUpdate 設定ポリシーを開いて、[ポリシー] > [LiveUpdate] とクリックします。
2. [Windows の設定] で、[サーバーの設定] > [LiveUpdate サーバーを使う] > [プレリリースのコンテンツに **Symantec LiveUpdate** サーバーを使用] とクリックします。

3. [OK] をクリックして、ポリシーをテストグループに割り当てます。

LiveUpdate 設定ポリシーが EAS からコンテンツを取得するがぎり、テストクライアントはコンテンツのプレリリースバージョンを受信し続けます。

NOTE

テストしないグループについては、LiveUpdate 設定ポリシーを通常使用している LiveUpdate サーバーに設定します。一般リリースのエンジンが入手できるようになったら、クライアントコンピュータの受信設定に応じて、すべてのクライアントコンピュータが LiveUpdate コンテンツを受信します。

[社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定](#)

[外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定](#)

ステップ 3: 特定のエンジンバージョンに対してテストコンピュータと非テストコンピュータを設定する

次のように複数の LiveUpdate コンテンツポリシーを設定します。

- テストグループは、セキュリティ定義とエンジンの最新バージョンを受信します。このグループは、プレリリースのエンジンバージョンを含む今後すべてのコンテンツリビジョンをダウンロードします。
- 非テストグループは、エンジンの既存の安全なバージョンを受信します。
14.0.1 MP1 以降、エンジンバージョンをロックすることもできます。このオプションでは、クライアントは特定のエンジンに関連付けられている最新のセキュリティ定義を受信し続けますが、エンジンの最新のバージョンは受信しません。

[Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す](#)

テストグループがプレリリースコンテンツで普通に機能することを確認したら、非テストグループで次に使用するエンジンバージョンを手動で選択します。

ステップ 4: 新しいエンジンのリリースに関する通知を設定する (省略可能)

LiveUpdate が つの Symantec Endpoint Protection Manager にダウンロードする予定のエンジンリリースの通知を取得するには、次のいずれかを実行します。

- 新しいコンテンツが つの Symantec Endpoint Protection Manager にダウンロードされたとき用の通知を追加します。14.0.1 MP1 以降では、新しいコンテンツの通知には新しいエンジンリリースとセキュリティ定義の情報が含まれます。エンジンのバージョンによってコンテンツリビジョンを指定する 1 つ以上の LiveUpdate コンテンツポリシーが入手可能なエンジンの更新によりロックされている場合にのみ、通知を受信します。
通知を表示するには、[ホーム] ページの [セキュリティの状態] ペインで、[通知の表示] をクリックします。

NOTE

EAS での更新の頻度は正規の LiveUpdate サーバーと同じです。これらの通知の受信頻度が高すぎると感じる場合、通知が表示されないように設定します。

[管理者通知の設定](#)

- 以前のリリースでは、お客様向けのサブスクリプションポータルにログインします。

[PCS のお客様が警告と通知を登録する方法](#)

ステップ 5: エンジンコンテンツがリリースされた後、テストコンピュータを監視する

シマンテック社がエンジンの更新を EAS に公開した後、このコンテンツを受信するように設定したコンピュータの監視を開始します。次の項目を監視します。

- テストコンピュータがエンジンの更新のプレリリースバージョンを実行することを確認します。
[クライアントコンピュータで動作するエンジンと定義の確認](#)
- Microsoft System Center Operations Manager などのツールを使用するサーバーとその他の重要なインフラ上での稼働時間と利用可能なリソース。
- クライアントコンピュータで動作するアプリケーションが、想定通り動作し続けることを確認します。
- Symantec Endpoint Protection クライアントの状態が、管理サーバーに接続されたまま保護されていることを確認します。

クライアントが管理サーバーに接続され、保護されているかどうかの確認

さらに、ポリシーを変更した後にクライアントを実行するか、スキャンを実行して、想定通りコンピュータが機能することを確認します。

予想外の動作に気付くか、エンジンの更新とのソフトウェアの競合が存在すると感じる場合、サポートに連絡してください。通常、段階的ロールアウトの開始前にソフトウェアの競合があることを確認した場合、シマンテック社は、公開のスケジュールを再設定して、お客様と共に問題を修正します。その後、シマンテック社は、更新されたエンジンを EAS に再公開します。

Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す

デフォルトでは、LiveUpdate サーバーから管理サーバーにダウンロードされるコンテンツの最新バージョンは、Windows クライアントに自動的にダウンロードされます。LiveUpdate コンテンツポリシーは、クライアントが調べてインストールできるコンテンツの種類を指定します。

ただし、次の場合、古いバージョンのコンテンツをダウンロードする必要があります。

- 定義またはエンジンの最新のセットによって、クライアントコンピュータでソフトウェアの競合が発生している。
- コンテンツを実働環境にリリースする前に、制御グループで新しいエンジンをテストする時間が必要である。

NOTE

この機能は特に注意して使ってください。コンテンツの種類のチェックマークをはずすことは、クライアントでその機能が最新の状態に維持されないことを意味します。この結果、クライアントを潜在的により大きいリスクにさらす可能性があります。

コンテンツの種類を [リビジョンを選択する] に設定してから、Symantec Endpoint Protection クライアントをクラウド管理下クライアントに変換する場合、コンテンツはクライアントで更新されません。この問題を回避するには、クライアントを変換する前にコンテンツ オプションを [利用可能な最新のものを使う] に設定します。

Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻すには

1. コンソールで、[ポリシー] > [LiveUpdate] とクリックして、LiveUpdate コンテンツポリシーを開きます。
2. [Windows の設定] の下で、[セキュリティ定義] をクリックします。

Mac クライアントまたは Linux クライアントのコンテンツはロールバックできません。

3. 特定のバージョンにコンテンツをロールバックするには、次のオプションのいずれかをクリックします。
 - [リビジョンを選択する] > [編集] をクリックし、リビジョン番号を選択します。
このオプションは、1 つの特定のセキュリティ定義セットにクライアントをロックします。クライアントは新しいセキュリティ定義を受信しません。
 - [エンジンのバージョンを選択してください] > [編集] をクリックし、エンジンのバージョンを選択します。
14.0.1 MP1 以降、このオプションは、1 つの特定のエンジンのバージョンにクライアントをロックしますが、そのエンジンに関連付けられている最新のセキュリティ定義を配布し続けます。環境で現在のエンジンが動作することが判明していて、新しいエンジンのリリース前に異なるグループでテストする必要がある場合、エンジンのバージョンを選択します。または、クライアントがそのコンテンツの種類の最新のエンジンバージョンと定義を受信し続けられるように、[利用可能な最新を使う] をクリックします。14.0.1 以前のクライアントはこの設定を無視します。
4. [OK] をクリックします。

コンテンツの更新で、クライアントコンピュータを再起動する必要はありません。

5. トラブルシューティングの問題を解決した後、[Windows の設定] で、コンテンツの各種類に対して [セキュリティ定義] > [利用可能な最新を使う] をクリックします。

Windows クライアントでリリースする前のエンジン更新のテスト

LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード

クライアントにコンテンツを配布するためのグループ更新プロバイダの使用

グループ更新プロバイダ (GUP) は、コンテンツ更新を他のクライアントに直接配布するクライアントコンピュータです。

GUP の利点は次のとおりです。

- GUP に処理能力をオフロードすることによって帯域幅と管理サーバーのリソースを節約します。
- ネットワーク接続が低速かつ制限された状態で、更新を効果的に配信します。
- 社内の LiveUpdate サーバーよりも設定が容易です。

Table 138: グループ更新プロバイダを使うためのタスク

手順	説明
ステップ 1: 設定できる GUP の種類の違いを理解する	単一、複数、クロスサブネットの GUP を設定できます。設定する GUP の種類は、ネットワークやそのネットワーク上のクライアントによって決まります。グループ更新プロバイダのそれぞれの種類は、相互に排他的ではありません。ポリシーごとに 1 つ以上の種類のグループ更新プロバイダを設定できます。 グループ更新プロバイダの種類について ネットワークに 2 種類以上の GUP を設定した場合の影響について
ステップ 2: クライアント通信を確認する	GUP を設定する前に、クライアントコンピュータがサーバーからコンテンツ更新を受信できることを確認します。クライアント/サーバーの通信の問題を解決します。 クライアントとサーバーの活動は、[監視] ページの [ログ] タブのシステムログで表示できます。 つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング
ステップ 3: 1 つ以上の LiveUpdate 設定ポリシーで GUP を設定する	GUP は LiveUpdate 設定ポリシーで設定します。 GUP からコンテンツをダウンロードするためのクライアントの設定
ステップ 4: グループに LiveUpdate 設定ポリシーを割り当てる	GUP を使うグループに LiveUpdate 設定ポリシーを割り当てます。GUP が存在するグループにもポリシーを割り当てます。 単一のグループ更新プロバイダについては、各サイトの各グループに 1 つの LiveUpdate 設定ポリシーを割り当てます。 複数の GUP と GUP の明示的リストについては、複数のサブネットにわたる複数のグループに 1 つの LiveUpdate 設定ポリシーを割り当てます。 グループまたは場所へのポリシーの割り当て
ステップ 5: クライアントが GUP として指定されることを確認する	GUP として指定されるクライアントコンピュータを表示するには、次のタスクのいずれかを実行します。 • [クライアント]、[クライアント] タブの順にクリックして目的のクライアントを右クリックし、[プロパティの編集] をクリックします。GUP のフィールドは True または False です。 • グループ更新プロバイダとして機能するクライアントの検索

グループ更新プロバイダの種類について

複数種類の GUP を LiveUpdate 設定ポリシーで設定できます。使用する GUP の種類は、ネットワークの設定によって決まります。ポリシーごとに 1 つ以上の種類の GUP を設定できます。これらは相互に排他的ではありません。

Table 139: 特定の種類のグループ更新プロバイダを使う状況

グループ更新プロバイダの種類	使うとき
単一	単一のグループ更新プロバイダは、クライアントの 1 つ以上のグループにコンテンツを提供する専用のクライアントコンピュータです。単一のグループ更新プロバイダを設定すると、単一のクライアントがグループ更新プロバイダになります。単一のグループ更新プロバイダはあらゆるグループのクライアントコンピュータになることができます。 すべてのクライアントコンピュータに対して同一のグループ更新プロバイダを使う場合は、単一のグループ更新プロバイダを使います。 単一の GUP に固定 IP アドレスまたはホスト名を指定するには、単一の LiveUpdate 設定ポリシーを使います。ただし、単一の GUP として機能するクライアントの場所を変更する場合は、ポリシーの IP アドレスを変更する必要があります。 異なるグループの異なる単一のグループ更新プロバイダを使う場合には、各グループに個別の LiveUpdate 設定ポリシーを作成する必要があります。
複数	複数のグループ更新プロバイダは、1 組のルール（基準）を使って、それ自体を、それが属するサブネット内のクライアントのグループで使用するよう選択します。すべてのクライアントコンピュータは同一のサブネット上に存在します。 クライアントコンピュータが GUP としての役割を担うために必要な基準を指定します。クライアントコンピュータが基準を満たす場合、管理サーバーは GUP のグローバルリストにそのクライアントを追加します。その後で、管理サーバーはグローバルリストをネットワーク内のすべてのクライアントで使えるようにします。クライアントはリストを調べ、それ自体のサブネットにある GUP を選択します。 複数の GUP を設定すると、複数のクライアントが GUP になります。 次のいずれかのシナリオでは、複数の GUP を使います。 - 複数のグループがあり、各グループに異なる GUP を使います。 複数のグループ更新プロバイダの選択のためのルールを指定する 1 つのポリシーを使うことができます。クライアントが場所を変更する場合は、LiveUpdate 設定ポリシーを更新する必要があります。つの Symantec Endpoint Protection Manager はサイトとドメイン全体で複数のグループ更新プロバイダを結合します。リストをネットワークのすべてのグループのすべてのクライアントで使えるようにします。 - 複数の GUP はフェールオーバー機構として機能できます。複数のグループ更新プロバイダを使うと、各サブネットで少なくとも 1 つのグループ更新プロバイダが利用できる確率が上がります。
明示的リスト	クライアントがそのクライアントのサブネット以外のサブネット上にある GUP に接続できるようにする場合は、明示的な GUP リストを使います。場所が変わるクライアントは、リスト内のグループ更新プロバイダのうち最も近いものにローミングできます。 明示的な GUP リストでは、クライアントは GUP になりません。 明示的なリストを設定すると、特定のサブネットの IP アドレスが設定されたクライアントで特定の GUP を使うように指定できます。クライアントに複数の IP アドレスが設定されていることがあるため、管理サーバーは、使用するグループ更新プロバイダと一致するときにクライアントのすべての IP アドレスを検討します。したがって、ポリシーが一致する IP アドレスは、クライアントがグループ更新プロバイダと通信するために使うインターフェースにバインドする必要はありません。 たとえば、クライアントに IP アドレス A が設定されていて、この IP アドレスを管理サーバーとの通信と GUP との通信に使うとします。このクライアントには IP アドレス B も設定されており、この IP アドレスがクライアントの LiveUpdate 設定ポリシーに設定した明示的 GUP と一致します。クライアントは、アドレス B がグループ更新プロバイダとの通信に使うアドレスでない場合でも、使うグループ更新プロバイダをアドレス B に基づいて選択することがあります。

LiveUpdate の設定のポリシーで単一または複数のグループ更新プロバイダを設定した場合は、以下の処理が実行されます。

-
- このポリシーでどのクライアントがグループ更新プロバイダとして機能するかを指定します。
 - クライアントがこのポリシーでどの GUP をコンテンツ更新に使用するかを指定します。

明示的な GUP リストを設定した場合は、1 つの処理のみが実行されます。

- クライアントがこのポリシーでどの GUP をコンテンツ更新に使用するかを指定します。
クライアントは GUP になりませんが、明示的なプロバイダリストのみが含まれているポリシーを設定、適用することはできます。ただし、つの Symantec Endpoint Protection Manager の別のポリシーで、単一のグループ更新プロバイダまたは複数のグループ更新プロバイダが設定されている必要があります。または、他のポリシーで両方の種類を設定することもできます。

クライアントがどのグループ更新プロバイダからも更新を取得できない場合は、オプションで 1 つの Symantec Endpoint Protection Manager からの更新を試行できます。

[ネットワークに 2 種類以上の GUP を設定した場合の影響について](#)

[クライアントにコンテンツを配布するための GUP の使用](#)

[GUP からコンテンツをダウンロードするためのクライアントの設定](#)

[LiveUpdate から 1 つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

GUP からコンテンツをダウンロードするためのクライアントの設定

LiveUpdate 設定ポリシーを使って、クライアントが GUP のみから更新を取得して管理サーバーからは受け取らないようにします。単一、複数、クロスサブネットの GUP を設定できます。設定する GUP の種類は、ネットワークやそのネットワーク上のクライアントによって決まります。

[グループ更新プロバイダの種類について](#)

1. GUP からコンテンツをダウンロードするようにクライアントを設定するには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] で、[LiveUpdate] をクリックします。
3. [LiveUpdate の設定] タブで、目的のポリシーを右クリックし、次に [編集] をクリックします。
4. [LiveUpdate 設定ポリシー] ウィンドウで、[サーバーの設定] をクリックします。
5. [社内または社外の LiveUpdate サーバー] の下で、[デフォルト管理サーバーを使う] にチェックマークを付けます。
6. [グループ更新プロバイダ] で、[GUP を使います] にチェックマークを付けます。
7. [GUP (Group Update Provider)] をクリックします。
8. 次のいずれかのタスクを行います。
 - 「[単一の GUP を設定するには](#)」の手順に従います。
 - 「[複数の GUP を設定するには](#)」の手順に従います。
 - 「[GUP の明示的リストを設定するには](#)」の手順に従います。
9. [GUP の設定] で、コンテンツを GUP コンピュータにダウンロードして格納する方法を制御するオプションを設定します。

コンテンツダウンロードについて詳しくは [ヘルプ] を参照してください。

-
10. [OK] をクリックします。
 11. 単一のグループ更新プロバイダを設定するには、[グループ更新プロバイダ] ダイアログボックスで、[単一 GUP の IP アドレスまたはホスト名] にチェックマークを付けて、単一のグループ更新プロバイダとして機能するクライアントコンピュータの IP アドレスまたはホスト名を入力します。
IP アドレスまたはホスト名について詳しくは [ヘルプ] を参照してください。
 12. グループ更新プロバイダを設定する手順に戻ります。
 13. 複数のグループ更新プロバイダを設定するには、[グループ更新プロバイダ] ダイアログボックスで、[複数グループ更新プロバイダ] にチェックマークを付けて [グループ更新プロバイダリストの設定] をクリックします。
 14. [GUP リスト] ダイアログボックスで、ツリーノード [グループ更新プロバイダ] を選択して [追加] をクリックしてルールセットを追加します。
 15. [GUP ルール基準を指定してください] ダイアログボックスの [選択] ドロップダウンリストで、次のいずれかのオプションを選択します。
 - コンピュータ IP アドレス / ホスト名
 - レジストリキー
 - オペレーティングシステム
 16. [コンピュータ IP アドレス / ホスト名] または [レジストリキー] を選択した場合は、[追加] をクリックします。
 17. IP アドレス、ホスト名、Windows レジストリキー、オペレーティングシステムの情報を入力または選択します。
ルールの設定について詳しくは [ヘルプ] を参照してください。
 18. [GUP (Group Update Provider) リスト] ダイアログボックスに戻るまで [OK] をクリックします。このダイアログボックスでは任意に、より多くのルールセットを追加できます。
 19. [OK] をクリックします。
 20. グループ更新プロバイダを設定する手順に戻ります。
 21. グループ更新プロバイダの明示的リストを設定するには、[グループ更新プロバイダ] ダイアログボックスで、[ローミングクライアントの明示的グループ更新プロバイダ] にチェックマークを付けて [明示的グループ更新プロバイダリストを設定する] をクリックします。
 22. [追加] をクリックします。
 23. [明示的グループ更新プロバイダを追加する] ダイアログボックスで、これらの GUP をマップするクライアントのサブネットを入力します。
[クライアントサブネットマスクの指定] をクリックして複数のクライアントのサブネットを一度に追加します。
[明示的なグループ更新プロバイダの追加](#)
 24. IP アドレス、ホスト名、GUP のネットワークアドレスに基づいて、設定するマッピングの [種類] を選択します。
選択したマッピングの種類に必要な設定を入力します。
 25. [OK] をクリックします。

[クライアント上のコンテンツを更新するための配布方法の選択](#)

[クライアントにコンテンツを配布するための GUP の使用](#)

グループ更新プロバイダとして機能するクライアントの検索

クライアントが GUP として利用可能であることを検証できます。[クライアント] タブで検索することによって GUP のリストを表示できます。

NOTE

クライアントのプロパティも調べることができます。プロパティはクライアントがグループ更新プロバイダであるかどうかを示すフィールドを含んでいます。

グループ更新プロバイダとして機能するクライアントを検索するには

1. コンソールで、[クライアント] をクリックします。
2. [クライアント] タブの [表示] ボックスで、[クライアントの状態] を選択します。
3. [タスク] ペインで [クライアントの検索] をクリックします。
4. [検索] ドロップダウンリストで、[コンピュータ] を選択します。
5. [グループ] フィールドで、グループ名を指定します。
6. [検索基準] で、[検索フィールド] 列をクリックし、[グループ更新プロバイダ] を選択します。
7. [検索基準] で、[比較演算子] 列をクリックし、[=] を選択します。
8. [検索基準] で、[値] 列をクリックし、[True] を選択します。

検索基準については [ヘルプ] をクリックしてください。

9. [検索] をクリックします。

クライアントにコンテンツを配布するための GUP の使用

ネットワーク内に 2 種類以上のグループ更新プロバイダを設定した場合の影響について

ポリシーに単一または複数のグループ更新プロバイダを設定すると、つの Symantec Endpoint Protection Manager は、チェックインしたすべてのプロバイダのグローバルリストを作成します。デフォルトでは、このファイルは次のようになります。

64 ビットオペレーティングシステム: C:\Program Files (x86)\Symantec\## Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml

32 ビットオペレーティングシステム: C:\Program Files \Symantec\## Symantec Endpoint Protection Manager\data\outbox\agent\gup\globallist.xml

つの Symantec Endpoint Protection Manager は、グローバルリストを要求するすべてのクライアントにこのリストを提供します。クライアントはこのリストにより、使用するグループ更新プロバイダを決定できます。この処理により、複数のまたは明示的グループ更新プロバイダのみが設定されたポリシーを持つクライアントは、単一のプロバイダが明示的なマッピング基準を満たせば、単一のグループ更新プロバイダも使用できます。これが可能になるのは、単一のプロバイダが、つの Symantec Endpoint Protection Manager からクライアントに提供されるプロバイダのグローバルリストの一部であるためです。

したがって、クライアントは、つの Symantec Endpoint Protection Manager 上のいずれかのポリシーで設定されているどのグローバル更新プロバイダでも使用できます。明示的グループ更新プロバイダリストのみを含んだポリシーをグループ内のクライアントに適用すると、グループ内のすべてのクライアントは、明示的なマッピング基準を満たす、つの Symantec Endpoint Protection Manager グローバルグループ更新プロバイダリスト内のグループ更新プロバイダを使用しようとしています。

NOTE

Symantec Endpoint Protection クライアントには、複数の IP アドレスが設定されていることがあります。Symantec Endpoint Protection では、グループ更新プロバイダとの一致においてすべての IP アドレスが考慮されます。したがって、ポリシーが照合する IP アドレスは、クライアントが 1 つの Symantec Endpoint Protection Manager やグループ更新プロバイダとの通信で使うインターフェースにバインドされているとは限りません。

全種類の GUP が つの Symantec Endpoint Protection Manager 上のポリシーで設定されている場合、クライアントは次の順番で、グローバルリスト内の GUP に接続を試みます。

- 複数のグループ更新プロバイダのリストにあるプロバイダに対して順番に試行
- 明示的グループ更新プロバイダのリストにあるプロバイダに対して順番に試行
- 単一 GUP として設定されているプロバイダ

次の種類の明示的なマッピング基準を設定できます。

- IP アドレス: サブネット A 内のクライアントは、IP アドレスが x.x.x.x の GUP を使う。
- ホスト名: サブネット A 内のクライアントは、ホスト名が xxxxx の GUP を使う。
- サブネットネットワークアドレス: サブネット A 内のクライアントは、##### B に存在する GUP を使う。

単一のポリシーの明示的グループ更新プロバイダリスト内で、複数のマッピング基準を使用できます。複数のマッピング基準を設定する場合、意図しない結果を回避するために慎重に設定することを推奨します。たとえば、明示的なマッピングを誤って設定すると、更新を取得するための手段がクライアントから失われることがあります。

次の複数の明示的な基準を単一のポリシーに設定した場合を考えてみてください。

- クライアントがサブネット 10.1.2.0 内にある場合、IP アドレスが 10.2.2.24 の GUP を使う
- クライアントがサブネット 10.1.2.0 内にある場合、IP アドレスが 10.2.2.25 の GUP を使う
- クライアントがサブネット 10.1.2.0 内にある場合、ホスト名が SomeMachine のグループ更新プロバイダを使う
- クライアントがサブネット 10.1.2.0 内にある場合、サブネット 10.5.12.0 上の任意のグループ更新プロバイダを使う
- クライアントがサブネット 10.6.1.0 内にある場合、サブネット 10.10.10.0 上の任意の GUP を使う

この明示的グループ更新プロバイダポリシーを使うと、クライアントがサブネット 10.1.2.0 上にある場合、最初の 4 つのルールが適用され、5 番目のルールは適用されません。10.15.1.0 など、マッピングが指定されていないサブネットにクライアントが存在する場合、そのクライアントにはどのルールも適用されません。そのクライアントのポリシーでは、明示的 GUP リストを使うように設定されていますが、クライアントがこれらのルールに基づいて使えるマッピングはありません。つの Symantec Endpoint Protection Manager と Symantec LiveUpdate server から更新をダウンロードする機能も無効にすると、そのクライアントには利用可能な更新手段がなくなります。

グループ更新プロバイダの種類について

GUP からコンテンツをダウンロードするためのクライアントの設定

Intelligent Updater ファイルを使用した Symantec Endpoint Protection クライアントのコンテンツの更新

シマンテック社は、Symantec Endpoint Protection クライアントのコンテンツを更新するときにクライアントコンピュータで LiveUpdate を使うことを推奨します。ただし、LiveUpdate の使用を望まない場合や LiveUpdate を利用できない場合は、Intelligent Updater ファイルを使ってクライアントを更新できます。Windows 用の Intelligent Updater の .exe ファイルは、クライアントのみを更新するように設計されています。Intelligent Updater ファイルには、つの Symantec Endpoint Protection Manager がその管理下クライアントを更新するために必要とする情報は含まれていません。

Windows 用の Intelligent Updater ファイルは、ウイルスとスパイウェアの定義が含まれる自己実行型のファイルです。SONAR 定義用と、侵入防止シグネチャ用に追加の Intelligent Updater ファイルを使用できます。Mac と Linux 用に、ウイルスとスパイウェアの定義をダウンロードできます。

ファイルをダウンロードした後、クライアントに更新を配布するために選択した配布方法を使うことができます。

NOTE

Intelligent Updater ファイルは、他の種類のコンテンツの更新は提供しません。たとえば、Intelligent Updater では、拡張ファイル属性とシグネチャ、Auto-Protect ポータルリスト、Power Eraser 定義、縮小サイズの定義はサポートされません。

1. Intelligent Updater ファイルをダウンロードするには、Web ブラウザを利用して次のページに進みます。
https://www.symantec.com/security_response/definitions.jsp
2. ドロップダウンリストから、次の使用可能な Symantec Endpoint Protection オプションのいずれかを選択します。

- Symantec Endpoint Protection 12.1
(Windows および Linux)
- Symantec Endpoint Protection 12.1.2
(Windows および Linux)
- Symantec Endpoint Protection 12.1.3 (またはそれ以降)
(Windows および Linux)
- Symantec Endpoint Protection 14
(Windows および Linux)
- Symantec Endpoint Protection for Macintosh 12.x
- Symantec Endpoint Protection for Macintosh 14.x

ページが更新されて、そのバージョンで利用できるコンテンツが表示されます。

3. [ファイルベースの保護 (従来のウイルス対策)]、[ネットワークベースの保護 (IPS)] (Windows のみ)、または [ビヘイビアベースの保護] (Windows のみ) の [ダウンロード] の隣にある [定義ファイル] をクリックします。
4. 更新するクライアントのバージョンに該当するファイル名をクリックします。

NOTE

Linux のウイルス定義の場合は、[Unix プラットフォーム] タブをクリックします。

5. ファイルを保存する場所を確認するメッセージが表示されたら、ハードディスクドライブ上のフォルダを選択します。
6. 選択した配布方法を使って、クライアントコンピュータにファイルを配布します。
追加のファイルが必要な場合は、手順を繰り返して実行できます。
7. ウイルス定義とセキュリティ更新ファイルをクライアントコンピュータにインストールするには、クライアントコンピュータで、クライアントに配布された Intelligent Updater ファイルを検索します。
8. 次のいずれかの操作をします。
 - Windows の場合: .exe ファイルをダブルクリックし、画面の指示に従います。
 - Mac の場合: .zip ファイルをダブルクリックし、.pkg ファイルをダブルクリックし、画面の指示に従います。
 - Linux の場合: ファイルの実行権限があることと、uudecode と uncompress がインストールされていることを確認したら、スーパーユーザーの権限を使用して .sh ファイルを実行します。詳しくは次を参照してください。

[Intelligent Updater を使用して Linux ベースのコンピュータのウイルス定義ファイルを更新する方法について](#)

[クライアント上のコンテンツを更新するための配布方法の選択](#)

サードパーティの配布ツールを使ったクライアントコンピュータの更新

一部の企業は IBM Tivoli や Microsoft SMS などのサードパーティの配布ツールを利用して、クライアントコンピュータにコンテンツ更新を配布しています。Symantec Endpoint Protection では、サードパーティの配布ツールを使って Windows オペレーティングシステムが実行されている管理下クライアントと管理外クライアントを更新することができ

ます。Mac クライアントと Linux クライアントは社内または外部 LiveUpdate サーバーからのみコンテンツ更新を受信できます。

サードパーティの配布ツールの使用を設定する前に、つの Symantec Endpoint Protection Manager と、更新するクライアントコンピュータをインストール済みである必要があります。

Table 140: 更新用のサードパーティの配布ツールの使用を設定するタスク

タスク	説明
コンテンツ更新を受信するように 1 つの Symantec Endpoint Protection Manager を設定する	コンテンツ更新を自動または手動で受信するように管理サーバーを設定できます。 LiveUpdate から 1 つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード クライアント上のコンテンツと定義を更新する方法
サードパーティのコンテンツ更新の配布を許可するためにグループの LiveUpdate の設定のポリシーを設定してください。	管理下クライアントを更新するためにサードパーティの配布のツールを使いたい場合にはそれを可能にするためにグループの LiveUpdate の設定のポリシーを設定してください。 管理下クライアントへのサードパーティのコンテンツ配布を許可する LiveUpdate 設定ポリシーの設定
サードパーティの配布ツールから更新を受信するように管理外クライアントを準備する	サードパーティの配布ツールを使って管理外クライアントを更新する場合は、最初に、各管理外クライアントでレジストリキーを作成する必要があります。 サードパーティの配布ツールから更新を受信するための管理外クライアントの準備
コンテンツを検索し、コピーし、配布する	それぞれの 1 つの Symantec Endpoint Protection Manager クライアントグループには、1 つの Symantec Endpoint Protection Manager を実行するコンピュータに配置された index2.dax ファイルがあります。これらのファイルは、デフォルトで SEPM_Install\data\outbox\agent フォルダの下の子フォルダにあります。クライアントを更新するには、この index2.dax ファイルを使う必要があります。 デフォルトの場所の SEPM_Install のデフォルト値は C:\Program Files (x86)\Symantec\1 つの Symantec Endpoint Protection Manager です。 32 ビットシステム (12.1.x) の場合は、C:\Program Files\Symantec\1 つの Symantec Endpoint Protection Manager です。 LiveUpdate から 1 つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード サードパーティの配布ツールを使ったコンテンツの配布

管理下クライアントへのサードパーティのコンテンツ配布を許可する LiveUpdate 設定ポリシーの設定

管理下クライアントを更新するためにサードパーティの配布のツールを使いたい場合にはそれを可能にするためにクライアントグループの LiveUpdate の設定のポリシーを設定してください。手動で LiveUpdate を実行するクライアントユーザーの機能を無効にするかどうかを選択できます。

この手順を終えると、グループのクライアントコンピュータでは次の場所にフォルダが表示されます。

- Vista 以降のオペレーティングシステム
C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox
- Vista 以前のオペレーティングシステム (12.1.x レガシークライアント)
C:\Documents and Settings\All Users\Application Data\Symantec\CurrentVersion\inbox

LiveUpdate のポリシーによる管理下クライアントへのサードパーティのコンテンツ配布を有効にするには

-
1. コンソールで、[ポリシー] をクリックします。
 2. [ポリシー] で、[LiveUpdate] をクリックします。
 3. [LiveUpdate の設定] タブの [タスク] で、[LiveUpdate 設定ポリシーの追加] をクリックします。
 4. [LiveUpdate ポリシー] ウィンドウの [ポリシー名] と [説明] テキストボックスに、名前と説明を入力します。
 5. [Windows の設定] の下で、[サーバーの設定] をクリックします。
 6. [サードパーティ管理] で、[サードパーティコンテンツ管理を有効にする] にチェックマークを付けます。
 7. その他の LiveUpdate 更新元オプションはすべて解除します。
 8. [OK] をクリックします。
 9. [ポリシーの割り当て] ダイアログボックスで、[はい] をクリックします。
この手順を取り消し、後からポリシーを割り当てることもできます。
 10. [LiveUpdate ポリシーの割り当て] ダイアログボックスで、このポリシーを割り当てる 1 つ以上のグループにチェックマークを付け、[割り当て] をクリックします。

社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

サードパーティの配布ツールから更新を受信するための管理外クライアントの準備

インストールファイルから管理外クライアントをインストールする場合は、すぐにサードパーティの配布ツールを使って、それらのクライアントに LiveUpdate コンテンツやポリシーの更新を配布することはできません。セキュリティ対策として、これらのクライアントコンピュータはデフォルトではサードパーティの配布ツールが提供するコンテンツを信頼したり、処理したりしません。

サードパーティの配布ツールを使って更新を正しく配信するには、最初に各管理外クライアントで Windows レジストリキーを作成する必要があります。このキーは、管理外クライアントで受信ボックスのフォルダを使って LiveUpdate コンテンツとポリシーの更新を配布することを可能にします。

受信ボックスのフォルダは管理外クライアントでは次の場所にあります。

- Vista 以降のオペレーティングシステム
C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\inbox
- Vista 以前のオペレーティングシステム (12.1.x レガシークライアント)
C:\Documents and Settings\All Users\Application Data\Symantec\CurrentVersion\inbox

レジストリキーを作成したら、サードパーティの配布ツールを使って、コンテンツまたはポリシーの更新をこのフォルダにコピーできます。Symantec Endpoint Protection クライアントソフトウェアは、更新を信頼して処理します。

サードパーティの配布ツールから更新を受信するために管理外クライアントを準備するには

1. 各クライアントコンピュータで、regedit.exe または別の Windows レジストリ編集ツールを使って次の Windows レジストリキーのいずれかを追加します。
 - 64 ビットコンピュータ上の 12.1.5 以降のクライアントの場合、HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState を追加します。
 - 32 ビットコンピュータ上の 12.1.5 以降のクライアントの場合と、その他すべての 12.1 クライアントの場合、HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\SPE\TPMState を追加します。
2. レジストリキーの値型を DWORD (32 ビット版) または QWORD (64 ビット版) に設定してこの値を次のように 16 進数の 80 に設定します。

0x00000080 (128)

3. レジストリキーを保存し、レジストリ編集ツールを終了します。

サードパーティの配布ツールを使ったクライアントコンピュータの更新

サードパーティの配布ツールを使ったコンテンツの配布

サードパーティの配布ツールを使ったコンテンツの配布

サードパーティの配布ツールを使ってクライアントコンピュータにコンテンツを配布するには、index2.dax ファイルを使う必要があります。index2 ファイルの LiveUpdate に関連するコンテンツには、コンテンツモニカと呼ばれる 1 組の GUID とそれらに関連付けられたシーケンス番号が含まれています。各コンテンツモニカは特定のコンテンツの種類に対応します。index2 ファイルの各シーケンス番号は特定のコンテンツの種類のリビジョンに対応します。インストールした保護機能に応じて、必要なコンテンツの種類を決定する必要があります。

LiveUpdate がダウンロードするコンテンツの種類について

NOTE

コンテンツモニカは通常、メジャーリリースごとに変わります。まれにマイナーリリースで変わる場合もあります。シマンテック社は通常、リリース更新や保守パッチのモニカは変更しません。

ContentInfo.txt ファイルを開くことによってコンテンツの種類へのモニカのマップを参照できます。デフォルトで、ContentInfo.txt ファイルは C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager\lnetpub\content\にあります。

たとえば、次のエントリを参照できます。

```
{535CB6A4-441F-4e8a-A897-804CD859100E}: SEPC Virus Definitions  
Win32 12.1 RU6 - MicroDefsB.CurDefs - SymAllLanguages
```

つの Symantec Endpoint Protection Manager のクライアントグループにはそれぞれ固有の index2 ファイルがあります。各クライアントグループの index2 ファイルはそのグループのフォルダ内にあります。デフォルトで、クライアントグループのフォルダは C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager\data\outbox\agent\にあります。クライアントグループのフォルダ名はグループポリシーのシリアル番号に対応しています。シリアル番号は、[グループのプロパティ] ダイアログボックス、または [クライアント] ページの [詳細] タブで見つかります。各グループポリシーのシリアル番号の最初の 4 つの 16 進値は、そのグループのフォルダの最初の 4 つの 16 進値と一致します。

管理下クライアントが使う index2.dax ファイルは暗号化されます。ファイルの内容を参照するには、同じフォルダで利用可能な index2.xml ファイルを開きます。index2.xml ファイルには、コンテンツモニカと連続 (リビジョン) 番号のリストがあります。たとえば、次のエントリを参照できます。

```
<File Checksum="D5ED508E8CF7A8A4450B0DBA39BCCB25" DeltaFlag="1"  
FullSize="625203112" LastModifiedTime="1425983765211" Moniker=  
"{535CB6A4-441F-4e8a-A897-804CD859100E}" Seq="150309034"/>
```

グループの LiveUpdate Content policy では、特定リビジョンのコンテンツまたは最新コンテンツのいずれかを指定します。index2 ファイル内のシーケンス番号は、グループの LiveUpdate Content policy のコンテンツの指定に対応するシーケンス番号と一致している必要があります。たとえば、ポリシーがすべてのコンテンツの種類について [利用可能な最新を使う] に設定されている場合は、各種類のシーケンス番号が、利用可能な最新のコンテンツとなっています。この例では、index2 ファイルが最新のコンテンツリビジョンに対応するシーケンス番号 (リビジョン) を呼び出す場合にのみ配布が機能します。シーケンス番号が他のリビジョンにも対応する場合は配布は失敗します。

NOTE

クライアントの \inbox フォルダにファイルを配置するには、Copy コマンドを使う必要があります。Move コマンドを使用しても更新処理はトリガされず、更新は失敗します。コンテンツを配布用の単一アーカイブに圧縮する場合は、直接 \inbox フォルダに圧縮解除しないでください。

サードパーティの配布ツールを使ってクライアントにコンテンツを配布するには

-
1. つの Symantec Endpoint Protection Manager を実行するコンピュータで、\\Work_Dir などの作業フォルダを作成します。
 2. 次のいずれかの処理を実行します。
 - 管理下クライアントの場合は、コンソールの [クライアント] タブで、更新するグループを右クリックして [プロパティ] をクリックします。
 - 管理外クライアントの場合は、コンソールの [クライアント] タブで、 [My Company] を右クリックして [プロパティ] をクリックします。
 3. [ポリシーのシリアル番号] の最初の 4 つの 16 進値 (たとえば 7B86) を書き留めます。
 4. 次のフォルダに移動します。

SEPM_Install\data\outbox\agent

ここで、SEPM_Installは、つの Symantec Endpoint Protection Manager のインストールフォルダを表します。デフォルトのインストールフォルダは、C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。

5. 最初の 4 つの 16 進数値が [ポリシーのシリアル番号] の値と一致するフォルダを探します。
6. そのフォルダを開き、index2.dax ファイルを作業フォルダにコピーします。
7. 次のフォルダに移動します。

SEPM_Install\inetpub\content

ここで、SEPM_Installは、つの Symantec Endpoint Protection Manager のインストールフォルダを表します。デフォルトのインストールフォルダは、C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files\Symantec\つの Symantec Endpoint Protection Manager です。

8. ContentInfo.txt を開いて読み、各 target monikerフォルダに含まれるコンテンツを探します。
各ディレクトリのコンテンツの形式は target moniker\シーケンス番号\full.zip|full です。
9. 各 \target monikerフォルダのコンテンツを \\Work_Dir などの作業フォルダにコピーします。
10. 各 \target monikerからすべてのファイルとフォルダを削除し、次のフォルダ構造とファイルのみが作業フォルダに残るようにします。

\\Work_Dir\target moniker\latest sequence number\full.zip

これで、作業フォルダは、クライアントに配布するフォルダ構造とファイルが含まれている状態になりました。

11. サードパーティの配布ツールを使って、作業フォルダのコンテンツを各クライアントの \\Symantec Endpoint Protection\inbox\ フォルダに配布します。

最終結果は次のようになります。

\\Symantec Endpoint Protection\inbox\index2.dax

\\Symantec Endpoint Protection\inbox\target moniker\latest sequence number\full.zip

正常に処理されたファイルは処理後に削除されます。正常に処理されていないファイルは Invalid という名前のサブフォルダに移動されます。inbox フォルダの下に Invalid フォルダ内にファイルがある場合は、それらのファイルを使って再試行する必要があります。

サードパーティの配布ツールを使ったクライアントコンピュータの更新

Windows クライアントへの Endpoint Protection クライアント パッチのインストール

クライアント パッチとその仕組み

クライアント パッチまたはセキュリティ修正は、Symantec Endpoint Protection Windows クライアントのソフトウェアパッチで、コード内に存在するセキュリティの脆弱性または機能問題を解決します。新しい脆弱性や問題が判明すると、シマンテックはこの問題を修正するクライアント パッチを提供し、LiveUpdate サーバにアップロードします (14.3 RU2 以降)。クライアント パッチは、IPS シグネチャやウイルスとスパイウェアの定義など、他の種類のコンテンツに類似します。クライアント パッチを LiveUpdate サーバから管理サーバに増分差分 (.dax) ファイルとしてダウンロードします。他のコンテンツと同じように、LiveUpdate サーバ、管理サーバ、または、グループ更新プロバイダ (GUP) を使ってクライアントにパッチをダウンロードします。

クライアント上のコンテンツを更新するための配布方法の選択

NOTE

クライアント パッチは、メンテナンス パッチ (MP) またはリリース更新 (RU) とは異なります。クライアント パッチは潜在的なセキュリティの問題またはクライアントの障害のみを解決し、LiveUpdate を通じて配信されます。メンテナンス パッチは新しいオペレーティングシステムに対するサポートの提供など、その他の更新や機能を提供し、Broadcom [ダウンロード管理](#) ページからフル インストールダウンロードとして配信されます。14.3 RU2 以降では、クライアント パッチには製品の更新と同じコンテンツが含まれます。ただし、製品の更新はフル クライアント インストール パッケージに含まれますが、クライアント パッチにはデルタ ファイルのみが含まれます。

Endpoint Protection のリリースタイプとバージョンについて

クライアントと管理サーバのバージョンが一致する場合、クライアントは LiveUpdate サーバ、管理サーバ、GUP からクライアント パッチを取得できます。クライアントと管理サーバのバージョンが一致しない場合、管理サーバで複数のバージョンをインストールしたクライアントを管理する場合と同じように、クライアントは LiveUpdate サーバからのみクライアント パッチを取得します。管理サーバまたは GUP を使ってパッチをダウンロードする場合は、クライアントまたは管理サーバのバージョンを更新して両方を同じバージョンにする必要があります。

以下の表に、つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントのバージョン番号に基づいて、クライアントが管理サーバからクライアント パッチを受信できるかどうかの例を示します。

Table 141: クライアント バージョンとバージョンに応じてダウンロードできるクライアント パッチの例

管理サーバのバージョン	クライアントのバージョン	クライアントが管理サーバからパッチをダウンロードするか
14.2	14.2	はい
14.2	14.0.1 MP2	【※No※】
14.0.1 MP2	14.0.1 MP2	はい
14.0.1 MP2	14.0.1 MP1	【※No※】
14.0.1 MP2	14.2	いいえ

14.3 RU2 では、LiveUpdate はクライアント パッチだけでなく機能の更新もダウンロードします。この場合、クライアント ビルドは管理サーバと一致する必要はありません。古い、同じ、または新しいビルドを使用できます。

自動更新によるクライアントソフトウェアのアップグレード

クライアント パッチをダウンロードするには、クライアントの言語と管理サーバの言語が一致する必要があります。たとえば、フランス語、ドイツ語、簡体字中国語のクライアントを管理するフランス語の管理サーバは、フランス語のク

クライアントにのみクライアント パッチを提供します。ただし、自動更新を使って、クライアント パッチを含むフランス語、ドイツ語、中国語のクライアント インストール パッケージをインストールできます。LiveUpdate をインポートまたは使用して、他言語のクライアント インストール パッケージやクライアント パッチを含めることもできます。

WINDOWS コンピュータへのクライアント パッチのインストール

デフォルトで、LiveUpdate から つの Symantec Endpoint Protection Manager にクライアント パッチがダウンロードされ、そこで他のコンテンツの種類用に設定した配布方法に基づいてクライアントにパッチがインストールされます。

クライアント パッチをダウンロードしてインストールした後、クライアントは引き続き以前のパッチが適用されていないバージョンのクライアントを実行して、クライアントを再起動します。クライアントのエンドユーザーがコンピュータを再起動するか、または管理サーバーから再起動コマンドを自分で実行する必要があります。管理サーバーから再起動が必要なクライアントを示す通知が送信されます。

Windows クライアントにクライアント パッチをインストールするには

1. コンソールで、管理サーバにクライアント パッチをダウンロードするように LiveUpdate を設定していることを確認します。

[ダウンロードするコンテンツの種類] ダイアログ ボックスで、[クライアント パッチ] にチェックが付いていることを確認します。

14.3 RU1 以前では、このオプションはクライアントセキュリティパッチと呼ばれていました。

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

2. クライアントコンピュータにインストールされているリリースを特定するレポートを実行するには、[保護コンテンツのバージョン] レポートを実行します。

[ネットワーク内でインストールされている Symantec Endpoint Protection バージョンのリストの作成](#)

3. クライアントにパッチをダウンロードするように LiveUpdate の設定ポリシーを設定していることを確認します。LiveUpdate 設定ポリシーで、[Windows の設定] の [拡張設定] をクリックします。[クライアント パッチのダウンロード] にチェックが付いていることを確認します。

NOTE

[利用可能な場合は LiveUpdate サーバからデルタ コンテンツをダウンロードする] にチェックが付いていることを確認します。このオプションは現在のリリースのクライアント パッチを新しいパッチのコンテンツとマージし、その差分 (デルタ) のみをダウンロードします。クライアントの帯域幅が低い場合は、このオプションを使います。

4. クライアント コンピュータを再起動します。

[つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動](#)

コンプライアンスの監視、レポート、エンフォース

レポートとログの実行および読み取り、ホストインテグリティの設定を行う方法について

このセクションでは、以下の方法について説明します。

- ホストインテグリティを設定して、クライアントコンピュータが保護され、会社のセキュリティポリシーに準拠するようにする。
- ログおよびレポートを使用して、環境内のセキュリティを監視する。
- 通知を管理する。

ホストインテグリティの設定

ネットワーク内のクライアントコンピュータに組織のセキュリティポリシーを順守させるには、ホストインテグリティポリシーを使います。

「[ホストインテグリティポリシーを設定するためのタスク](#)」は、ホストインテグリティポリシーを使用してセキュリティコンプライアンスを設定するために必要な手順の一覧です。

Table 142: ホストインテグリティポリシーを設定するためのタスク

手順	説明
ステップ 1: クライアントコンピュータの必要条件を調べ、ポリシーに従わないコンピュータに修復処理を実施するホストインテグリティポリシーを追加する	新しいポリシーを追加するとき、次のタスクを実行します。 1. クライアントコンピュータに検査させる必要条件の種類を選択します。ソフトウェアの種類別に必要条件を作成します (アプリケーション、ファイル、パッチなど)。 ホストインテグリティ必要条件について ホストインテグリティポリシーへの事前定義済み必要条件の追加 2. ポリシーに従わないクライアントコンピュータの修復処理を設定します。 修復では、クライアントコンピュータが必要なソフトウェアをインストールするか、クライアントユーザーにインストールを要求する必要があります。 事前定義済みのホストインテグリティ必要条件の修復の設定 3. 必要条件を検査し、修復を試す順序を設定します。たとえば、更新は特定の順序で完了する必要があります。そうすることで、クライアントコンピュータの再起動が必要になる前にすべての更新が適用されます。
ステップ 2: ホストインテグリティの検査と通知のオプションを設定する	• ホストインテグリティ検査の実行頻度を設定します。 ホストインテグリティ検査の頻度の設定 • ユーザーによる修復取り消しを可能にするかどうかを設定します。 ユーザーによるホストインテグリティ修復の延期または中止の許可 • ホストインテグリティ検査で合格または失格が判断されたときにクライアントコンピュータに表示する通知を設定します。通知を使い、エンドユーザーに次の指示を与えます。たとえば、場合によっては、エンドユーザーはクライアントコンピュータに新しいパッチをダウンロードし、インストールすることを許可する必要があります。 ホストインテグリティ検査の通知の設定
ステップ 3: ピアツーピアエンフォースメントを設定する	ホストインテグリティコンプライアンスが試験されているクライアントコンピュータがすでにポリシーに従っているクライアントコンピュータと同じネットワークにある場合、ピアツーピアエンフォースメントを設定できます。主に、ファイル共有のためのピアツーピアエンフォースメントを使います。 ピアツーピア認証の設定によるリモートコンピュータの遮断

手順	説明
ステップ 4: ポリシーに従わないコンピュータと未修復のコンピュータの検疫ポリシーを設定する (省略可能)	クライアントコンピュータがホストインテグリティ検査を失敗し、修復を実行しない場合、検疫ポリシーを使用してコンピュータを隔離できます。 失敗したホストインテグリティ検査のための検疫ポリシーの作成

ホストインテグリティの仕組み

ホストインテグリティは、クライアントコンピュータが保護され、会社のセキュリティポリシーに準拠するようにします。ホストインテグリティポリシーを使用して、企業のネットワークとデータを保護するためにクライアントのセキュリティを定義、強制、復元します。

Table 143: クライアントコンピュータのセキュリティコンプライアンスを強制するためのプロセス

手順	説明
手順 1: クライアントコンピュータが、クライアントコンピュータ上でホストインテグリティ検査を実行する	管理サーバーは割り当てグループのクライアントコンピュータにホストインテグリティポリシーをダウンロードします。クライアントコンピュータはホストインテグリティ検査を実行し、ホストインテグリティポリシーに追加した要件と各コンピュータの設定を比較します。 ホストインテグリティポリシーはウイルス対策ソフトウェア、パッチ、ホットフィックス、その他のセキュリティ要件の存在を確認します。たとえば、ポリシーは、最新のパッチがオペレーティングシステムに適用されたかどうかを確認できます。 ホストインテグリティの設定
手順 2: ホストインテグリティ検査が成功するか、または失敗するか	- コンピュータがすべてのポリシー要件を満たしている場合、ホストインテグリティ検査は成功します。 - コンピュータがポリシー要件を満たしていない場合、ホストインテグリティ検査は失敗します。検査を成功させるために、失敗した要件を無視するようにポリシーを設定することもできます。 必要条件失敗時のホストインテグリティ検査の成功許可 また、クライアントがインストールされているリモートコンピュータへのインバウンドアクセスを許可または遮断できる、ファイアウォールポリシーのピアツーピア認証を設定できます。 ピアツーピア認証の設定によるリモートコンピュータの遮断
手順 3: ホストインテグリティ検査に失敗した準拠しないコンピュータを修復する (省略可能)	- ホストインテグリティ検査が失敗した場合、クライアントを修復するように設定できます。修復するためには、クライアントは見つからないソフトウェアをダウンロードしてインストールします。事前定義済みの必要条件またはカスタム必要条件で、クライアントを修復するように、またはエンドユーザーを修復するように設定できます。修復後に、ホストインテグリティは、クライアントコンピュータがソフトウェアをインストールしたこと再確認します。 事前定義済みのホストインテグリティ必要条件の修復の設定 - 修復を検証するホストインテグリティ検査が引き続き失敗する場合、クライアントは検疫のポリシーを適用します。検疫ポリシーを使って、失敗したコンピュータにより厳密な制限を適用できます。 失敗したホストインテグリティ検査のための検疫ポリシーの作成 - クライアントが検疫の場所にある間、ホストインテグリティ検査は実行し、修復を試行し続けます。検査と修復の頻度の設定は、ホストインテグリティポリシーをどのように設定するかに基づいています。クライアントが修復され、ホストインテグリティ検査に成功したら、クライアントは検疫の場所から自動的に移動します。 場合によっては、クライアントコンピュータを手動で修復する必要がある場合もあります。

手順	説明
手順 4: クライアントでコンプライアンスの監視を続行する	ホストインテグリティ検査は、各クライアントのコンプライアンス状態をアクティブに監視します。クライアントのコンプライアンス状態が変化する場合はいつでも、コンピュータの権限も変化します。 - ホストインテグリティポリシーを変更すると、次のハートビート時にクライアントにダウンロードされます。その後にクライアントはホストインテグリティ検査を実行します。 - ホストインテグリティ検査の進行中に異なるホストインテグリティポリシーを持つ場所にクライアントが切り替える場合、そのクライアントは検査を停止します。この停止の間、すべての修復の試みが停止されます。新しい場所で修復サーバー接続が利用できない場合は、タイムアウトメッセージが表示されることがあります。検査が完了するとクライアントは結果を破棄します。次にクライアントはその場所の新しいポリシーに基づいて新しいホストインテグリティ検査をすぐに実行します。 ホストインテグリティ検査の結果はコンプライアンスログで確認できます。 ログの表示

ホストインテグリティ必要条件について

新しいホストインテグリティポリシーを作成するときに、追加する必要条件の種類を決めます。

各必要条件では次の項目を指定します。

- 検査の条件
たとえば、1つの必要条件としてウイルス定義の最新セットがクライアントコンピュータにインストールされているかどうかを調べます。
- クライアントが条件の必要条件を満たしていない場合に実行する修復処理
たとえば、見つからないウイルス定義をインストールするためにクライアントがこの定義をダウンロードできる URL を修復処理に入れることができます。

「[ホストインテグリティポリシーの必要条件の種類](#)」に、使用可能な必要条件の種類を示します。

Table 144: ホストインテグリティポリシーの必要条件の種類

次のように入力します。	説明
事前定義済み必要条件	特定のアプリケーションまたはファイルをインストールし、クライアントで実行していることを調べる事前定義済み必要条件を使います。事前定義済み必要条件は、アプリケーション（ウイルス対策ソフトウェア、スパイウェア対策ソフトウェア、ファイアウォール、パッチ、Service Pack のいずれか）の状態を調べます。たとえば、パッチ必要条件はクライアントコンピュータが特定のオペレーティングシステムのパッチを実行しているかを調べます。 事前定義済み必要条件の詳細が十分でない場合は、カスタム必要条件を追加してスクリプトを書き込みます。 ホストインテグリティポリシーへの事前定義済み必要条件の追加
テンプレートのカスタム必要条件	テンプレートは、シマンテック社が通常の実行タスクを書き込んだ事前定義済みカスタム必要条件です。たとえば、クライアントはパスワードが過去 42 日間に変更されたかを調べることができます。カスタム必要条件のスクリプトを書き込む土台としてテンプレートを使うこともできます。 テンプレート必要条件は、ホストインテグリティポリシー LiveUpdate サービスを介して使えます。最初に LiveUpdate を設定して管理サーバーにホストインテグリティのテンプレートをダウンロードする必要があります。 テンプレートのカスタム必要条件の追加 LiveUpdate から 1 つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード

次のように入力します。	説明
カスタム必要条件	事前定義済み必要条件にもテンプレートにも必要な種類の検査が含まれていない場合はカスタム必要条件を使います。カスタム必要条件のフィールドは事前定義済み必要条件と同じですが、より柔軟性に富んでいます。たとえば、スパイウェア対策アプリケーションの事前定義済みリストに含まれていないスパイウェア対策アプリケーションを指定できます。 同様のアプリケーションを1つのカスタム必要条件にまとめることで、必要なアプリケーションの管理が簡単になります。たとえば、Internet Explorer や Firefox などのインターネットブラウザを1つの必要条件にまとめることができます。 カスタマイズした必要条件スクリプトの記述

ホストインテグリティの設定

ホストインテグリティポリシーへの事前定義済み必要条件の追加

ホストインテグリティポリシーの事前定義済み必要条件は、クライアントコンピュータがウイルス対策、スパイウェア対策、ファイアウォールなどの複数種類のアプリケーションを実行していることを調べます。

Windows 7 オペレーティングシステムの特定のパッチなど、アプリケーションを特定します。クライアントコンピュータが取得する必要があるパッチのパスを指定します。

事前定義済み必要条件をホストインテグリティポリシーに追加するには

1. コンソールで、[ホストインテグリティポリシー] を開きます。
2. [ホストインテグリティポリシー] ページで、[必要条件] > [追加] をクリックします。
3. [必要条件の追加] ダイアログボックスで [必要条件を選択してください] ドロップダウンリストをクリックして事前定義済み必要条件を選択し、[OK] をクリックします。

バージョン 12.1.x では、Mac クライアントに オンデマンドクライアントがインストールされている場合にのみ、[Mac] をクリックします。は使用できなくなり、Symantec Endpoint Protection 14.x での使用はサポートされていません。

4. 必要条件の設定と修復のオプションを設定し、[OK] をクリックします。

事前定義済みのホストインテグリティ必要条件の修復の設定

詳しくは [ヘルプ] を参照してください。

5. [OK] をクリックします。
6. グループまたは場所にポリシーに割り当てます。
7. [OK] をクリックします。

テンプレートのカスタム必要条件の追加

カスタマイズした必要条件スクリプトの記述

事前定義済みのホストインテグリティ必要条件の修復の設定

クライアントのホストインテグリティ検査で必要条件を満たしていないと示された場合は、ポリシーを設定して必要なファイルを復元します。クライアントは必要なアプリケーションをダウンロード、インストール、実行してファイルを復元し、必要条件を満たします。そうすることで、クライアントコンピュータはホストインテグリティ検査に成功します。

事前定義済みの必要条件を追加するダイアログボックスと同じダイアログボックスで修復を設定します。クライアントが修復ファイルをダウンロードするパスと修復処理の実行方法の両方を指定します。

ユーザーがコンピュータを修復するタイミングを制御できるようにすることも可能です。たとえば、再起動するとユーザーの操作が消失する可能性がある場合に就業時間が終わるまで修復を延期すると安全です。

必要条件を復元するコマンドをダウンロード、インストール、実行した後はクライアントは常に必要条件を再テストします。クライアントは `pass` または `fail` の結果をログに記録します。

事前定義済みのホストインテグリティ必要条件の修復を設定するには

1. コンソールでホストインテグリティポリシーを開き、事前定義された必要条件を追加します。

ホストインテグリティポリシーへの事前定義済み必要条件の追加

2. [必要条件の追加] ダイアログボックスで、[<必要条件の種類> がクライアントにインストール済みでなければインストールする] をクリックします。
3. [インストールパッケージをダウンロード] をクリックする。
4. [ダウンロード URL] テキストボックスに、クライアントコンピュータにダウンロードするインストールファイルの URL を入力します。

ファイルの場所の指定と修復用のコマンド実行について

5. [コマンドを実行する] テキストボックスで、次のタスクのいずれかを実行します。
 - クライアントユーザーがインストールを実行できるようにするには、テキストボックスを空白のままにします。
 - インストールを自動的に実行するには、`%F%` と入力します。
`%F%` 変数は、最後にダウンロードしたファイルを表します。スタートメニューの [ファイル名を指定して実行] で実行できる任意のコマンドを使います。たとえば、Vista 用のパッチをインストールするにはコマンド `%Systemroot%\system32\wusa.exe /quiet /norestart %F%` を入力します。
6. 省略可能なオプションとして、修復の延期または中止を設定して [OK] をクリックします。

ユーザーによるホストインテグリティ修復の延期または中止の許可

7. [OK] をクリックします。

必要条件失敗時のホストインテグリティ検査の成功許可

ユーザーによるホストインテグリティ修復の延期または中止の許可

ユーザーが修復を都合のいい時間まで延期することを許可できます。必要条件のソフトウェアをインストールした後でユーザーがコンピュータを再起動する必要がある場合は、後でコンピュータを再起動できると便利です。

ユーザーが修復を延期すると次のイベントのいずれかが起きる場合があります。

- クライアントがイベントをログに記録する。必要条件を満たしていないのでホストインテグリティの状態に失敗であることが示されます。ユーザーは、クライアントからいつでも手動で新しいホストインテグリティ検査を実行できます。
- クライアントが別のホストインテグリティ検査を実行するまで、ホストインテグリティ検査の修復メッセージウィンドウが表示されない。ユーザーが 5 分後の再通知を選択しても、ホストインテグリティ検査を 30 分ごとに実行する場合にはメッセージウィンドウは 30 分後まで表示されません。ユーザーの混乱を避けるために、最小時間設定をホストインテグリティ検査の頻度設定に合わせることをお勧めします。
- ユーザーが次のホストインテグリティ検査の前に修復を延期すると、ユーザーの選択が強制変更される。
- ユーザーが修復処理を延期し、クライアントが更新済みポリシーを受け取った場合に修復までの猶予期間が新しい最大期間にリセットされる。

ユーザーによるホストインテグリティ修復の延期または中止を許可するには

1. コンソールでホストインテグリティポリシーを開いて必要条件を追加します。

ホストインテグリティポリシーへの事前定義済み必要条件の追加

2. [必要条件の追加] ダイアログボックスで修復を設定します。

事前定義済みのホストインテグリティ必要条件の修復の設定

3. 必要条件のダイアログボックスで次のいずれかのタスクを実行して [OK] をクリックします。

- クライアントユーザーがファイルのダウンロードを延期できるようにする場合は、[ダウンロードが失敗した場合に再びダウンロードを試みる前の待ち時間を指定する] にチェックマークを付ける
- クライアントユーザーが修復を中止できるようにする場合は、[ユーザーがホストインテグリティ修復のダウンロードを中止できる] にチェックマークを付ける

4. [OK] をクリックします。

5. [拡張設定] をクリックします。

6. [拡張設定] ページの [修復ダイアログボックスオプション] で、修復を中止するオプションを設定します。

7. クライアントコンピュータでカスタムメッセージを追加するには、[追加テキストの設定] をクリックします。

入力したメッセージは、ユーザーが [詳細] オプションをクリックするとクライアント修復ウィンドウに表示されます。

8. [OK] をクリックします。

ホストインテグリティ検査の頻度の設定

ホストインテグリティ検査の実行方法や結果の処理方法を設定できます。

ホストインテグリティポリシーを追加または更新すると、ポリシーは次のハートビートでクライアントにダウンロードされます。クライアントはホストインテグリティ検査を実行します。

ホストインテグリティ検査の進行中にユーザーが異なるポリシーの場所に切り替えると、クライアントは検査を停止します。ポリシーが要求する場合は修復の試みも停止します。新しい場所で修復サーバー接続が利用できない場合はタイムアウトメッセージが表示されることがあります。検査が完了するとクライアントは結果を破棄します。次にクライアントはその場所の新しいポリシーに基づいて新しいホストインテグリティ検査をすぐに実行します。

新しい場所でもポリシーが同じである場合はクライアントはホストインテグリティタイムの設定を維持します。クライアントは新しいホストインテグリティ検査をポリシー設定が要求する場合にのみ実行します。

ホストインテグリティ検査の頻度を設定するには

1. コンソールでホストインテグリティポリシーを開いて [拡張設定] をクリックします。
2. [拡張設定] ページの [ホストインテグリティ検査オプション] で、ホストインテグリティ検査の頻度を設定します。
3. [OK] をクリックします。

ホストインテグリティポリシーへの事前定義済み必要条件の追加

必要条件失敗時のホストインテグリティ検査の成功許可

必要条件失敗時のホストインテグリティ検査の成功許可

コンピュータがホストインテグリティ検査に失敗しても操作の続行が必要な場合があります。特定の必要条件を満たしていなくても、ホストインテグリティ検査を合格にすることができます。クライアントは結果をログに記録しますが、結果を無視します。

特定の必要条件にこの設定を適用します。この設定をすべての必要条件に適用する場合は、各必要条件について個別に有効にする必要があります。この設定は、デフォルトでは無効です。

必要条件が失敗してもホストインテグリティ検査の合格を許可するには

1. コンソールで、[ホストインテグリティポリシー] を開きます。
2. 事前定義済み必要条件またはカスタム必要条件を追加して [OK] をクリックします。

ホストインテグリティポリシーへの事前定義済み必要条件の追加

カスタマイズした必要条件スクリプトの記述

3. 必要条件のダイアログボックスで [この必要条件が失敗してもホストインテグリティ検査の合格を許可する] にチェックマークを付け、 [OK] をクリックします。
4. [OK] をクリックします。

ホストインテグリティ検査の通知の設定

クライアントがホストインテグリティ検査を実行するとき、次の条件に該当する場合に表示される通知を設定できます。

- ホストインテグリティ検査が失敗する
- ホストインテグリティ検査が失敗した後に成功する

ホストインテグリティ検査の結果はクライアントのセキュリティログに表示されます。それらは管理サーバーの [監視] ページのコンプライアンスログにアップロードされます。

クライアントのセキュリティログには複数のペインがあります。ホストインテグリティ検査のイベントの種類を選択した場合、左下のペインには個々の必要条件が満たされているか、または満たされていないかの一覧が表示されます。右下のペインには必要条件の条件の一覧が表示されます。右下のペインの情報が表示されないようにクライアントを設定できます。トラブルシューティングするときにこの情報を必要とする場合もありますが、ユーザーに情報を表示することが望ましくない場合もあります。たとえば、レジストリ値がファイル名を指定するカスタム必要条件を書き込む場合があります。詳細は引き続きセキュリティログに記録されます。

ソフトウェアをただちにダウンロードするか、または修復を延期するかを選択をユーザーに与える通知を有効にすることもできます。

ユーザーによるホストインテグリティ修復の延期または中止の許可

ホストインテグリティ検査の通知を設定するには

1. コンソールで、 [ホストインテグリティポリシー] を開きます。
2. [ホストインテグリティ] ページで、 [拡張設定] をクリックします。
3. [拡張設定] ページの [通知] で、必要条件の詳細情報を表示するには、 [ホストインテグリティログの詳細を表示] にチェックマークを付けます。

クライアントのセキュリティログの右下のペインに、ホストインテグリティの必要条件についての詳しい情報が表示されます。

4. 次のいずれかのオプションを選択します。
 - ホストインテグリティ検査が失敗したときに通知メッセージを表示する
 - 以前に失敗したホストインテグリティ検査が成功したときに通知メッセージを表示する
5. カスタムメッセージを追加するには、 [追加テキストの設定] をクリックし、最大 512 文字の追加テキストを入力してから、 [OK] をクリックします。
6. このポリシーの設定を完了したら、 [OK] をクリックします。

失敗したホストインテグリティ検査のための検疫ポリシーの作成

ホストインテグリティ検査に失敗したクライアントコンピュータに検疫ポリシーを使って修復しようとしても、再度失敗します。クライアントコンピュータの修復に失敗すると、クライアントは自動的に検疫場所に切り替わります。この場所は、コンピュータに検疫ポリシーが適用される場所です。検疫ポリシーを使って、より厳密な制限を失敗したコンピュータに対して適用できます。検疫ポリシーには、あらゆる種類の保護ポリシーを使うことができます。たとえば、インターネットへのコンピュータのアクセスを遮断するファイアウォール検疫ポリシーを適用できます。

クライアントコンピュータが検疫場所にある間、コンピュータを実行し続けて修復を試みるために、ホストインテグリティ検査を設定できます。また、コンピュータを手動で修復する必要がある場合もあります。

失敗したホストインテグリティ検査のための検疫ポリシーを作成するには

-
1. コンソールで、[クライアント] をクリックし、[ポリシー] タブをクリックします。
 2. [ホストインテグリティが失敗したときの検疫ポリシー] の隣の [ポリシー] タブで、[ポリシーの追加] をクリックします。
 3. [検疫ポリシーの追加] ダイアログボックスでポリシーの種類を選択し、[次へ] をクリックします。
 4. 既存のポリシーの使用、新しいポリシーの作成、ポリシーファイルのインポートのいずれかを選択し、[次へ] をクリックします。
 5. 次のいずれかのタスクを行います。
 - [ポリシーの追加] ダイアログボックスでポリシーを選択し、[OK] をクリックします。
 - [ポリシーの種類] ダイアログボックスでポリシーを設定し、[OK] をクリックします。
 - [ポリシーのインポート] ダイアログボックスで .dat ファイルを見つけて [インポート] をクリックします。

事前定義済みのホストインテグリティ必要条件の修復の設定

ホストインテグリティ必要条件について

ピアツーピア認証の設定によるリモートコンピュータの遮断

ピアツーピア認証を使って、リモートクライアントコンピュータ (ピア) が、同じ企業ネットワーク内の別のクライアントコンピュータ (認証子) に接続するのを許可することができます。認証子は、リモートコンピュータがホストインテグリティ検査に合格するまで、一時的にリモートコンピュータからの TCP および UDP のインバウンドトラフィックを遮断します。リモートコンピュータが物理的なリモートの場合はこのエンフォースメント技法を使うことができます。この技法は、Symantec Endpoint Protection ファイアウォールの拡張機能を利用して共有ファイルに対するアクセスを拡張します。

ホストインテグリティ検査では、リモートコンピュータの以下の特性を確認します。

- リモートコンピュータに Symantec Endpoint Protection をインストールしていること。
- リモートコンピュータがホストインテグリティ検査に合格していること。

リモートコンピュータがホストインテグリティ検査に合格すると、認証子はリモートコンピュータから入ってくるインバウンド接続を許可します。

リモートコンピュータがホストインテグリティ検査に失敗すると、認証子はリモートコンピュータの遮断を継続します。リモートコンピュータが認証子への接続を再度試みることができるようになるまで遮断を継続する時間を指定することができます。ホストインテグリティ検査に合格しなくても常に許可する特定のリモートコンピュータを指定することもできます。リモートコンピュータに対するホストインテグリティポリシーを有効にしない場合、リモートコンピュータはホストインテグリティ検査に合格します。

ピアツーピア認証情報は、ネットワークとホストのエクスポloit緩和機能トラフィックログに表示されます。

NOTE

ピアツーピア認証は、サーバー制御でも混合制御でも機能しますが、クライアント制御では機能しません。

ピアツーピア認証の設定によってリモートコンピュータを遮断するには

1. コンソールで、[ファイアウォールポリシー] を開きます。
2. [ファイアウォールポリシー] ページで、[ピアツーピア認証の設定] をクリックします。
3. [ピアツーピア認証の設定] ページで、[ピアツーピア認証を有効にする] にチェックマークを付けます。
4. このページに表示される各値を設定します。

これらのオプションについて詳しくは [ヘルプ] を参照してください。

-
5. リモートコンピュータが認証なしでクライアントコンピュータに接続するのを許可するには、[ホストを認証から除外する] にチェックマークを付け、[除外ホスト] をクリックします。

クライアントコンピュータは、[ホスト] リストに表示されているコンピュータに対してトラフィックを許可します。

6. [除外ホスト] ダイアログボックスで、[追加] をクリックして認証の必要がないリモートコンピュータを追加します。
7. [ホスト] ダイアログボックスで、IP アドレス、IP 範囲、サブネットのいずれかを使ってホストを定義し、[OK] をクリックします。
8. [除外ホスト] ダイアログボックスで [OK] をクリックします。
9. [OK] をクリックします。
10. メッセージが表示されたら、ポリシーをグループに割り当てます。

[ファイアウォールポリシーの作成](#)

[ホストインテグリティの設定](#)

[クライアントコンピュータの保護をユーザーが無効にできない設定](#)

テンプレートのカスタム必要条件の追加

カスタム必要条件をゼロから書き込む代わりに、シマンテック社が作成した一般的なカスタム必要条件を追加できます。LiveUpdate を使って管理サーバーにホストインテグリティコンテンツをダウンロードします。ホストインテグリティコンテンツはテンプレートを含みます。テンプレートからホストインテグリティポリシーにカスタム必要条件を追加します。

最新のホストインテグリティテンプレートを取得するには、ホストインテグリティコンテンツのダウンロードを LiveUpdate Content policy で設定する必要があります。

同名のものが存在する必要条件を 2 回目にインポートする場合、インポートした必要条件は既存の必要条件を上書きしません。代わりに、インポートした必要条件は [必要条件] の表で名前の横に数字の 2 が表示されます。

テンプレートからカスタム必要条件を追加するには

1. コンソールで、[ホストインテグリティポリシー] を開きます。
2. [ホストインテグリティポリシー] ページで、[必要条件] > [追加] をクリックします。
3. [必要条件の追加] ダイアログボックスで [必要条件を選択してください] ドロップダウンリストをクリックして事前定義済み必要条件を選択し、[OK] をクリックします。

バージョン 12.1.x では、Mac クライアントに オンデマンドクライアントがインストールされている場合にのみ、[Mac] をクリックします。

4. [ホストインテグリティオンライン更新] ダイアログボックスで [テンプレート] を展開し、テンプレートカテゴリを選択します。
5. 追加する各テンプレートの横にある [追加] をクリックします。
6. [インポート] をクリックします。
7. [OK] をクリックします。

[ホストインテグリティ必要条件について](#)

[LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード](#)

[Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す](#)

カスタマイズした必要条件スクリプトの記述

カスタム必要条件を使うと、事前定義済みの必要条件よりも柔軟性が増します。たとえば、アプリケーションの事前定義済みリストに含まれていないアプリケーションを追加できます。

カスタム必要条件を構築するには、1 つ以上の関数または **IF..THEN** 文をスクリプトに追加します。スクリプトを実行すると、ホストインテグリティ検査は **IF** ノードのリストにある条件を検索します。条件に応じて **THEN** ノードのリストに示された処理を実行すると、結果 (pass または fail) が返ります。

1 つのスクリプトに多くの異なる検査条件を追加する場合は、この設定がカスタム必要条件スクリプト全体に適用されます。この設定が、簡単なカスタム必要条件をいくつか作成するか、または複数の手順を含む長いカスタム必要条件を 1 つ作成するかを決めるときに影響する場合があります。

カスタマイズした必要条件のスクリプトを記述するには

1. コンソールで、[ホストインテグリティポリシー] を開きます。
2. [ホストインテグリティポリシー] ページで、[必要条件] > [追加] をクリックします。
3. [必要条件の追加] ダイアログボックスで [必要条件を選択してください] ドロップダウンリストをクリックして事前定義済み必要条件を選択し、[OK] をクリックします。

バージョン 12.1.x では、Mac クライアントに オンデマンドクライアントがインストールされている場合にのみ、[Mac] をクリックします。

4. [カスタム必要条件] ダイアログボックスで、必要条件の名前を入力します。

必要条件名は、クライアントコンピュータに表示されます。名前により、必要条件が成功したか失敗したかをユーザーに通知したり、ソフトウェアをダウンロードするようにユーザーに要求するメッセージを表示したりします。

5. 条件を追加するには、[カスタム必要条件スクリプト] で [追加]、[IF..THEN] の順にクリックします。

NOTE

最初に関数または **IF..THEN** 文をフィールドに書き込まずに追加すると、エラーが表示されます。文を追加しない場合は文を右クリックし、[削除] をクリックします。

6. **IF** ノードで空の条件をハイライトして、右ペインで条件を選択します。

ホストインテグリティ検査により、クライアントコンピュータの条件が検索されます。

7. [条件を選択してください] ドロップダウンリストで、必要な追加情報を指定します。
8. [カスタム必要条件スクリプト] で、[THEN]、[追加] の順にクリックします。

THEN 文には、条件に該当する場合に実行する処理を指定します。

9. 次のいずれかのオプションをクリックします。

- **IF..THEN**

入れ子の **IF..THEN** 文を使って検査する条件を定義し、条件に該当すると評価された場合に実行する処理を定義します。

- 関数

関数を使ってファイルのダウンロードなどの修復処理を定義します。

- 戻り値

return 文を使って、条件の評価結果が成功または失敗のどちらであるかを指定します。すべてのカスタム必要条件は、成功または失敗の文で終わる必要があります。

- コメント (省略可能なオプション)

コメントを使って、追加する条件、関数、文の機能を説明します。

10. 右側のペインで、追加した基準を定義します。

これらのオプションについて詳しくは [ヘルプ] を参照してください。

11. さらに入れ子になった文、条件、関数を追加するには、[カスタム必要条件スクリプト] でノードを右クリックして、[追加] をクリックします。
12. 必要に応じて、手順 9 から 11 を繰り返します。
13. 結果にかかわらずホストインテグリティ検査の合格を許可するには、[この必要条件が失敗してもホストインテグリティ検査の合格を許可する] にチェックマークを付けます。
14. [OK] をクリックします。

カスタム必要条件スクリプトを使ったテスト用ホストインテグリティポリシーの作成

ホストインテグリティポリシーへの事前定義済み必要条件の追加

レジストリの条件について

検査する Windows のレジストリ設定を指定できます。この設定は、**IF.THEN** 条件文の一部として、カスタム必要条件に対して指定します。また、レジストリ値を変更する方法も指定できます。サポート対象のレジストリ設定は、`HKEY_CLASSES_ROOT#HKEY_CURRENT_USER#HKEY_LOCAL_MACHINE#HKEY_USERS`、`HKEY_CURRENT_CONFIG` のみです。

レジストリキーを指定する場合には以下の点に注意してください。

- キー名は 255 文字に制限される
- レジストリキーの最後にバックスラッシュ (\) がある場合は、レジストリキーとして解釈される。例:
`HKEY_LOCAL_MACHINE\SOFTWARE\`
- レジストリキーの最後に円記号がない場合、レジストリ名として解釈される。例: `HKEY_LOCAL_MACHINE\SOFTWARE\ActiveTouch`

レジストリ値を指定する場合には以下の点に注意してください。

- 値名は 255 文字に制限される。
- 値を DWORD (10 進)、バイナリ (16 進)、文字列のいずれかとして検査できる。
- DWORD 値では、値が指定した値より小さいか、等しいか、等しくないか、より大きいかを検査できる。
- 文字列値では、値データが指定した文字列に等しいか、指定した文字列が含まれているかどうかを検査できる。文字列の比較で大文字と小文字を区別する場合は、[一致のケース] チェックボックスにチェックマークを付ける。
- バイナリ値では、値データが指定したバイナリデータに等しいか、指定したバイナリデータが含まれているかどうかを検査できる。データは 16 進のバイトで表される。値が含まれているかどうかを検査する場合は、このデータのオフセットも指定できる。オフセットを空のままにすると、値の中に指定したバイナリデータが含まれているかどうかを検索される。16 進値の編集フィールドには、0 から 9 までと a から f までの値を指定できる。

レジストリ値の例を次に示します。

DWORD	12345 (10 進値)
バイナリ	31 AF BF 69 74 A3 69 (16 進値)
文字列	ef4adf4a9d933b747361157b8ce7a22f

クライアントでスクリプトを実行するカスタム必要条件の記述

カスタムホストインテグリティ必要条件では、クライアントでスクリプトを実行する関数を指定できます。Microsoft Windows Script Host で実行できる、JScript や VBScript などのスクリプト言語を使えます。

クライアントでスクリプトを実行するカスタム必要条件を記述するには

-
1. コンソールで、[ホストインテグリティポリシー] を開きます。
 2. [ホストインテグリティポリシー] ページで、[必要条件] > [追加] をクリックします。
 3. [必要条件の追加] ダイアログボックスで [必要条件を選択してください] ドロップダウンリストをクリックして事前定義済み必要条件を選択し、[OK] をクリックします。

バージョン 12.1.x では、Mac クライアントに オンデマンドクライアントがインストールされている場合にのみ、[Mac] をクリックします。

カスタマイズした必要条件スクリプトの記述

4. [カスタム必要条件] ダイアログボックスの [カスタム必要条件スクリプト] で、関数を追加するノードを選択します。
5. [追加]、[関数] の順にクリックします。
6. [ユーティリティ: スクリプトを実行] をクリックします。
7. `myscript.js` のように、スクリプトのファイル名を入力します。
8. スクリプトの内容を入力します。
9. [コマンドを実行する] テキストフィールドに、スクリプトの実行に使うコマンドを入力します。
スクリプトのファイル名を指定するには `%F` を使います。スクリプトはシステムコンテキストで実行されます。
10. **Execute** コマンドの実行が完了するまで許容する時間を指定するには、次のいずれかのオプションを選択します。
 - 待たない
実行に成功すると処理は `True` を返しますが、実行が完了するのを待ちません。
 - 実行が完了するまで待つ
 - 最大時間を入力してください
時間を秒単位で入力します。指定した時間内に `Execute` コマンドが完了しない場合は、ファイルの実行を終了します。
11. 省略可能なオプションとして、不要になった場合は [実行の完了後または終了後に一時ファイルを削除する] のチェックマークをはずします。
このオプションは、[待たない] を選択すると無効になり利用できません。
12. 省略可能なオプションとして、スクリプトを実行する必要条件を示すウィンドウを表示しない場合は、[新しいプロセスウィンドウを表示する] のチェックマークをはずします。

ファイルのタイムスタンプを設定するカスタム必要条件の記述

カスタムホストインテグリティ必要条件では、現在の日付と時刻を保存する Windows レジストリ設定を作成する **Set Timestamp** 関数を指定できます。**Check Timestamp** 条件を使うと、タイムスタンプを作成してから指定した時間が経過したかがわかります。

たとえば、ホストインテグリティ検査が 2 分ごとに実行する場合、日などのより長い間隔で実行する処理を指定できます。この場合、保存された時間の値は削除されます。次のように実行するように、スクリプトを設定できます。

-
- クライアントが新しいプロファイルを受信した時間
 - ユーザーが手動でホストインテグリティ検査を実行した時間

1. ファイルのタイムスタンプを設定するカスタム必要条件を記述するには、コンソールで [ホストインテグリティポリシー] をます。
2. [ホストインテグリティポリシー] ページで、[必要条件] > [追加] をクリックします。
3. [必要条件の追加] ダイアログボックスで [必要条件を選択してください] ドロップダウンリストをクリックして事前定義済み必要条件を選択し、[OK] をクリックします。

バージョン 12.1.x では、Mac クライアントに オンデマンドクライアントがインストールされている場合にのみ、[Mac] をクリックします。

カスタマイズした必要条件スクリプトの記述

4. [カスタム必要条件] ダイアログボックスの [カスタム必要条件スクリプト] で、関数を追加するノードを選択します。
5. [追加]、[関数] の順にクリックします。
6. [ユーティリティ: タイムスタンプの設定] をクリックします。
7. 日付と時刻の情報を格納するレジストリ設定の名前を、最大 255 文字で入力します。
たとえば、#####: と入力します。
8. 現在の時刻を保存されている時刻の値と比較するには、カスタム必要条件スクリプトを記述します。

カスタマイズした必要条件スクリプトの記述

9. [カスタム必要条件] ダイアログボックスの [カスタム必要条件スクリプト] で、条件を追加するノードを選択します。
10. [追加]、[IF..THEN] の順にクリックします。
11. [ユーティリティ: タイムスタンプの確認] をクリックします。
12. 時間を格納するためのレジストリ設定の名前を入力します。
13. 分、時間、日、週単位で期間を指定します。

指定した期間が経過したかまたはレジストリ設定の値が空の場合には、**Set Timestamp** 関数は True の値を返します。

レジストリ **DWORD** 値を増分するカスタム必要条件を記述する

カスタム必要条件は、Windows のレジストリ **DWORD** 値を増分できます。レジストリの **DWORD** 値の増分関数では、キーが存在しない場合にはキーが作成されます。

レジストリ **DWORD** 値を増分するカスタム必要条件を記述するには

1. コンソールで、カスタム必要条件のスクリプトとともにホストインテグリティポリシーを追加します。

カスタマイズした必要条件スクリプトの記述

-
2. [カスタム必要条件] ダイアログボックスの [カスタム必要条件スクリプト] で、関数を追加するノードを選択します。
 3. [追加]、[関数] の順にクリックします。
 4. [レジストリ: レジストリの **DWORD** 値の増分] をクリックします。
 5. [レジストリキー] フィールドに調べるレジストリキーを入力します。
 6. [値名] フィールドに調べる値名を入力します。
 7. [OK] をクリックします。

カスタム必要条件スクリプトを使ったテスト用ホストインテグリティポリシーの作成

このテスト用に作成するポリシーは、デモンストレーション専用です。ポリシーは、オペレーティングシステムの存在を検出し、検出した時点で##イベントを生成します。通常、##イベントは他の理由で生成します。

次のタスクを完了します。

- クライアントコンピュータのオペレーティングシステムを検査するカスタム必要条件スクリプトを含むホストインテグリティポリシーを追加します。
[カスタム必要条件スクリプトを使ってテスト用ホストインテグリティポリシーを作成するには](#)
 - 作成したホストインテグリティポリシーをテストします。
[クライアントコンピュータでホストインテグリティポリシーをテストするには](#)
1. カスタム必要条件スクリプトを使ってテスト用ホストインテグリティポリシーを作成するには、コンソールで [ホストインテグリティ] ポリシーをます。
 2. [ホストインテグリティポリシー] ページで、[必要条件] > [追加] をクリックします。
 3. [必要条件の追加] ダイアログボックスで [必要条件を選択してください] ドロップダウンリストをクリックして事前定義済み必要条件を選択し、[OK] をクリックします。

バージョン 12.1.x では、Mac クライアントに オンデマンドクライアントがインストールされている場合にのみ、[Mac] をクリックします。

-
4. [名前] ボックスにカスタム必要条件の名前を入力します。
 5. [カスタム必要条件] ダイアログボックスの [カスタム必要条件スクリプト] で、 [下に文を挿入してください:] を右クリックして [追加] > [IF..THEN] の順にクリックします。
 6. 右ペインの [条件を選択してください] ドロップダウンリストで、 [ユーティリティ: オペレーティングシステム は] をクリックします。
 7. [オペレーティングシステム] で、クライアントコンピュータで実行され、テストできる 1 つまたは複数のオペレーティングシステムにチェックマークを付けます。
 8. [カスタム必要条件スクリプト] で [THEN //ここに文を挿入してください] を右クリックし、 [追加]、 [関数]、 [ユーティリティ: メッセージダイアログボックスを表示] をクリックします。
 9. [メッセージウィンドウのキャプション] フィールドに、メッセージのタイトルとして表示する名前を入力します。
 10. [メッセージウィンドウのテキスト] フィールドに、表示するメッセージの本文を入力します。
 11. 左ペインの [カスタム必要条件スクリプト] で [パス] をクリックします。
 12. 右ペインの [必要条件の結果、戻り値] で、 [失敗] にチェックマークを付け、 [OK] をクリックします。
 13. [OK] をクリックします。
 14. [ホストインテグリティポリシー] ダイアログボックスの左パネルで [ポリシーの割り当て] をクリックします。
 15. [ホストインテグリティポリシーの割り当て] ダイアログボックスで、ポリシーを割り当てるグループを選択し、 [割り当て] をクリックします。
[ホストインテグリティポリシーの割り当て] ダイアログボックスで [はい] をクリックして、ホストインテグリティポリシーの変更を割り当てます。

NOTE

複数のグループに 1 つのホストインテグリティポリシーを割り当てることができますが、1 つのグループが持つことができるのは 1 つのホストインテグリティポリシーのみです。既存のポリシーを別のポリシーに置換できます。

16. クライアントコンピュータでホストインテグリティポリシーをテストするには、コンソールで [クライアント] > [クライアント] をクリックします。
17. [クライアント] で、ホストインテグリティポリシーを適用したクライアントコンピュータを含むグループをクリックしてハイライトします。
18. [タスク] で、 [グループでコマンドを実行する] > [コンテンツの更新] の順に選択して [OK] をクリックします。
19. クライアントを実行するコンピュータにログオンし、表示されるメッセージボックスに注意します。
このメッセージフィールドは、ルールにより##テストがトリガされたため表示されます。テスト後、テストポリシーを無効にするか削除してください。

[カスタマイズした必要条件スクリプトの記述](#)

[レジストリ DWORD 値を増分するカスタム必要条件を記述する](#)

[クライアントでスクリプトを実行するカスタム必要条件の記述](#)

エンドポイント保護の監視

Symantec Endpoint Protection はネットワークのセキュリティイベントについての情報を収集します。これらのイベントを表示するためにログとレポートを使うことができ、イベント発生時のイベントについての情報を常に取得するために通知を使うことができます。

レポートとログを使って、コンピュータに関する次のような疑問に対する答えを見つけることができます。

- どのコンピュータが感染しているか。
- どのコンピュータをスキャンする必要があるか。
- どのようなリスクがネットワークで検出されたか。

Table 145: エンドポイント保護を監視するためのタスク

タスク	説明
ネットワークのセキュリティの状態の確認	次のリストに、クライアントコンピュータのセキュリティの状態を監視するために実行できるタスクをいくつか示します。 • インストールされなかったクライアントの数を表示します。 クライアントの配備の状態についてのレポートの実行 • オフラインのコンピュータの台数を表示します。 オフラインコンピュータの検索 • 検出されたウイルスとその他のセキュリティリスクの件数を取得して各ウイルスとセキュリティリスクの詳細を表示します。 リスクの表示 • ネットワークの保護されていないコンピュータの件数を取得してそれぞれのコンピュータの詳細を表示します。 システム保護の表示 • 最新のウイルス定義とスパイウェア定義を含んだコンピュータの台数を表示します。 システム保護の表示 • クライアントコンピュータのリアルタイムの稼働状態を表示します。 クライアントコンピュータの保護状態の表示 • ネットワーク内で実行されているプロセスを確認します。 SONAR 検出結果の監視による誤認のチェック • どのコンピュータがどのグループに割り当てられているかを検索します。 • ネットワーク内のクライアントと Symantec Endpoint Protection サーバーにインストールされている、つの Symantec Endpoint Protection Manager ソフトウェアバージョンのリストを表示します。 ネットワーク内でインストールされている Symantec Endpoint Protection バージョンのリストの作成 • 有効なライセンス枠数、過剰配備されたライセンス枠数、期限切れのライセンス枠数、有効期限日など、クライアントコンピュータのライセンス情報を表示します。 つの Symantec Endpoint Protection Manager のライセンス状態の調査 日次または週次の状態レポートの表示 ホームページ
保護が必要なクライアントコンピュータの検索	どのコンピュータで付加的な保護が必要であるかを表示または検索するために次のタスクを実行できます。 • Symantec Endpoint Protection が無効なコンピュータの台数を表示します。 システム保護の表示 • 最新ではないウイルス定義とスパイウェア定義を含んだコンピュータの台数を表示します。 システム保護の表示 • 最近スキャンが行われなかったコンピュータを検索する。 スキャンしていないコンピュータの検索 • 攻撃の標的と攻撃元を表示します。 攻撃の標的と攻撃元の表示 • イベントログを表示します。 ログの表示
クライアントコンピュータの保護	クライアントコンピュータを保護するためにコンソールからコマンドを実行できます。 コンソールを使った、クライアントコンピュータでのコマンドの実行 たとえば、クライアントコンピュータのセキュリティリスクを除去できます。 スキャン処理の確認と識別されたコンピュータの再スキャン

タスク	説明
セキュリティイベントが発生したときに警告するための通知の設定	通知を作成して、特定のセキュリティ関連イベントが発生したときにトリガされるように設定できます。たとえば、侵入の試みがクライアントコンピュータで発生したときに受け取る通知を設定できます。 管理者通知の設定
進行中の監視用のカスタムクイックレポートと定時レポートの作成	カスタマイズされたクイックレポートを作成、生成したり、必要な情報が含まれるカスタムレポートをスケジュール設定して定期的に行ったりできます。 クイックレポートの実行とカスタマイズ 定時レポートの実行方法 カスタムレポートの保存 レポートの環境設定
クライアントログが占める空き容量の最小化	セキュリティのため、ログ記録を長期間維持することが必要な場合があります。ただし、多数のクライアントがある場合は、クライアントログデータの量も多くなることがあります。 管理サーバーを低容量で実行している場合は、ログサイズとデータベースがログを保持する期間を短縮する必要があります。 次のタスクを実行することによって、ログデータの量を減らすことができます。 - サーバーにクライアントログの一部のみをアップロードし、クライアントログをアップロードする頻度を変更する。 クライアントログサイズと管理サーバーにアップロードするログの指定 - クライアントコンピュータがデータベースに保持できるログエントリの数とそれらを保持する期間を指定する。 ログサイズとデータベース内でのログエントリの保存期間の指定 - サーバーに転送されるデータ量が減るように、重要度の低いリスクイベントとシステムイベントをフィルタで除外する。 Windows コンピュータのログ処理と通知設定の修正 - 各管理サーバーが管理するクライアントの数を減らす。 - クライアントログをサーバーにアップロードする頻度をコントロールするハートビートの頻度を減らす。 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新 - ログデータがデータベースに挿入される前にログデータが格納されるディレクトリ領域の量を減らす。 クライアントログデータ用にサーバーのディスク領域を拡大することについて
集中管理する場所へのログデータのエクスポート	ログデータのエクスポートは、ネットワーク全体のすべてのログを 1 つの場所に集中して蓄積する場合に便利です。ログデータのエクスポートは、表計算などの他社製プログラムを使ってデータを整理または操作する場合にも便利です。ログレコードを削除する前にログのデータをエクスポートすることもできます。 ログのデータをカンマ区切りテキストファイルにエクスポートできる場合があります。ログのデータを、ダンプファイルと呼ばれるタブ区切りテキストファイルや Syslog サーバーにエクスポートできる場合もあります。 ログデータのテキストファイルへのエクスポート ログデータの Syslog サーバーへのエクスポート 別のサイトのログの表示
レポートとログの問題のトラブルシューティング	レポートの問題のいくつかをトラブルシューティングできます。 レポートに関する問題のトラブルシューティング

NOTE

Symantec Endpoint Protection は、レポートに表示するイベントを管理サーバーのイベントログから抽出します。イベントログには、クライアントコンピュータのタイムゾーンにおけるタイムスタンプがあります。管理サーバーがイベントを受信すると、イベントのタイムスタンプをグリニッジ標準時 (GMT) に変換してデータベースに挿入します。レポートの作成時には、レポートを表示するコンピュータのローカル時刻で、イベントの情報がレポートソフトウェアにより表示されます。

スキャンしていないコンピュータの検索

スキャンする必要があるコンピュータをリストできます。

エンドポイント保護の監視

スキャンしていないコンピュータを検索するには

1. コンソールで、[レポート] をクリックします。
2. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	[スキャン] を選択します。
選択したレポート	[スキャンしていないコンピュータ] を選択します。

3. [レポートの作成] をクリックします。

オフラインコンピュータの検索

オフラインになっているコンピュータをリストできます。

クライアントは多くの理由でオフラインになります。オフラインになっているコンピュータを識別してその問題を修復する方法もさまざまです。

つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング

1. オフラインのコンピュータを検索するには、コンソールで [ホーム] をクリックします。
2. [ホーム] ページの [エンドポイントの状態] ペインで、オフラインコンピュータの数を表すリンクをクリックします。
3. オフラインコンピュータについて詳しくは、[詳細を表示] リンクをクリックしてください。
4. コンピュータの状態ログでオフラインのクライアントコンピュータを表示するには、コンソールで [監視] をクリックします。
5. [ログ] タブの [ログの種類] リストボックスで、[コンピュータの状態] をクリックします。
6. [追加設定] をクリックします。
12.1.x では、[追加設定] ではなく [拡張設定] です。
7. [オンライン状態] リストボックスで、[オフライン] をクリックします。
8. [ログの表示] をクリックします。

デフォルトでは、過去 24 時間オフラインだったコンピュータのリストが表示されます。リストには各コンピュータの名前、IP アドレス、前回サーバーにチェックインした時刻が含まれます。時間範囲を調整して、任意の時間のオフラインコンピュータを表示することができます。

ネットワーク内でインストールされている Symantec Endpoint Protection バージョンのリストの作成

ネットワーク内でインストールされている 1 つの Symantec Endpoint Protection Manager ソフトウェアのバージョンを一覧表示するレポートを Symantec Endpoint Protection からすばやく作成できます。このリストは、ソフトウェアを、前のバージョンの Symantec Endpoint Protection からアップグレードまたは移行するときに便利です。リストには、ローカルコンピュータとリモートコンピュータも表示されます。

レポートは、MHTML Web ページのアーカイブ形式を使って保存できます。

レポートの印刷と保存

1. Symantec Endpoint Protection ソフトウェアのバージョンを一覧表示するレポートを作成するには、コンソールで [レポート] をクリックします。
2. [レポートの種類] に [コンピュータの状態] を選択します。
3. [レポートの選択] に [**Symantec Endpoint Protection** 製品バージョン] を選択します。
4. [レポートの作成] をクリックします。
5. Symantec Endpoint Protection ソフトウェアのバージョンを含む、クライアントコンピュータの詳細なリストを作成するには、コンソールで [監視] をクリックし、[ログ] タブをクリックします。
6. [ログの種類] として [コンピュータの状態] を選択します。
7. 必要に応じて [時間範囲] を調整し、[ログの表示] をクリックします。
8. スクロールして [バージョン] 列を見つけます。ヘッダーをクリックして、バージョン番号でソートします。
[適用したフィルタを表示] をクリックして、ログフィルタを調整します。[エクスポート] をクリックして、リストをエクスポートします。クライアントコンピュータをクリックし、[詳細] をクリックして詳細を表示します。

ログの表示

クライアントソフトウェアをアップグレードする方法の選択

Symantec Endpoint Protection のアップグレードに関するリソース

クライアントの配備の状態についてのレポートの実行

クライアントの配備の状態についての複数のレポートを実行できます。たとえば、インストールに成功したクライアントと失敗したクライアントの数を表示できます。また、どのクライアントにどの保護技術がインストールされているのかを、クライアントコンピュータについてのシステム情報とともに表示できます。

エンドポイント保護の監視

配備されたクライアントの状態を表示するには

1. コンソールで、[レポート] をクリックします。
2. [クイックレポート] タブで、[コンピュータの状態] レポートの種類をクリックし、次のレポートのいずれかをクリックします。
 - クライアントの配備の状態については [配備レポート] をクリックします。
 - クライアントの保護の状態については [クライアントインベントリの詳細] をクリックします。
3. [レポートの作成] をクリックします。

リスクの表示

ネットワークのリスクに関する情報を入手できます。

エンドポイント保護の監視

1. 感染コンピュータとリスクを伴うコンピュータを表示するには、コンソールで [レポート] をクリックします。
2. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	リスク
選択したレポート	感染コンピュータとリスクを伴うコンピュータ

-
3. [レポートの作成] をクリックします。
 4. 特定の機能を有効にしない利点と危険性を理解するために、保護技術別のリスク分布レポートを実行できます。このレポートは次の情報を提供します。
 - ウイルスおよびスパイウェアのシグネチャベースの検出
 - SONAR 検出
 - ダウンロードインサイト検出
 - 侵入防止およびブラウザ保護の検出保護技術の種類別に検出されるリスクを表示するには、コンソールで [レポート] をクリックします。
 5. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	リスク
選択したレポート	保護技術別のリスク分布

6. [レポートの作成] をクリックします。
7. 新しく検出されたリスクを表示するには、コンソールで [レポート] をクリックします。
8. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	リスク
選択したレポート	ネットワークで検出された新種のリスク

9. [レポートの作成] をクリックします。
10. 総合リスクレポートを表示するには、コンソールで [レポート] をクリックします。
11. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	リスク
レポートの選択	総合リスクレポート

12. [レポートの作成] をクリックします。

攻撃の標的と攻撃元の表示

攻撃の標的と攻撃元を表示できます。

エンドポイント保護の監視

1. 上位を占める攻撃された標的を表示するには、コンソールで [レポート] をクリックします。
2. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	[ネットワークとホスト悪用防止] を選択します。
レポートの選択	[上位を占める攻撃の標的] を選択します。

3. [レポートの作成] をクリックします。
4. 上位を占める攻撃元を表示するには、コンソールで [レポート] をクリックします。
5. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	[ネットワークとホスト悪用防止] を選択します。
レポートの選択	[上位を占める攻撃元] を選択します。

6. [レポートの作成] をクリックします。
7. コンソールで、[レポート] をクリックします。
8. [クイックレポート] タブで、次の情報を指定します。

レポートの種類	[ネットワークとホスト悪用防止] を選択します。
レポートの選択	[詳細レポート] を選択します。
[設定] オプション	必要に応じて、詳細レポートに含めるレポートを選択できます。

9. [レポートの作成] をクリックします。

日次または週次の状態レポートの表示

日次状態レポートには、次の情報が表示されます。

- クリーニング、疑いあり、遮断、検疫、削除、新しく感染した項目、未解決感染処理のウイルス検出数
- ウイルス定義配布タイムライン
- 上位 10 のリスクと感染

週次状態レポートには、次の情報が表示されます。

- コンピュータの状態
- ウイルス検出
- 保護の状態のスナップショット
- ウイルス定義配布タイムライン
- 日単位のリスク分布
- 上位 10 のリスクと感染

エンドポイント保護の監視

日次状態レポートを表示するには

1. コンソールで [ホーム] をクリックします。
2. [ホーム] ページの [お気に入りレポート] ペインで、[**Symantec Endpoint Protection** の日次状態] または [**Symantec Endpoint Protection** の週次状態] をクリックします。

システム保護の表示

システム保護は、次の情報から構成されます。

- 最新のウイルス定義を含んだコンピュータの台数。
- 最新ではないウイルス定義を含んだコンピュータの台数。
- オフラインのコンピュータの台数。
- 無効になっているコンピュータの台数。

エンドポイント保護の監視

システム保護を表示するには

1. コンソールで [ホーム] をクリックします。
システム保護は [エンドポイントの状態] ペインに表示されます。
2. [エンドポイントの状態] ペインで [詳細を表示] をクリックすると、より多くのシステム保護情報が表示されます。

レポートの環境設定

次のレポートの環境設定ができます。

-
- [ホーム] ページと [監視] ページの表示オプション
 - セキュリティ状態しきい値
 - ログとレポート、さらにレガシーログファイルのアップロードに使われる表示オプション

設定するセキュリティ状態しきい値は、つの Symantec Endpoint Protection Manager の [ホーム] ページのセキュリティの状態メッセージが「不良」になる時期を決定します。しきい値は割合で表され、使用するネットワークがセキュリティポリシーを順守していないと見なされる時期を示します。

たとえば、不良のセキュリティ状態をトリガする、ウイルス定義が古いコンピュータ台数の割合を設定できます。また、定義が「古い」と見なされる経過日数も設定できます。Symantec Endpoint Protection はシグネチャや定義が古いかどうかを計算するときに、「最新」のものを次のように決定します。コンソールが実行される管理サーバーで利用可能な最新のウイルス定義と IPS シグネチャを「最新」の基準にします。

設定できる環境設定オプションについて詳しくは、[環境設定] ダイアログボックスの各タブの [ヘルプ] をクリックしてください。

レポートの環境設定を行うには

1. コンソールの [ホーム] ページで、[環境設定] をクリックします。
2. 設定する環境設定に合わせて、次のいずれかのタブをクリックします。
 - ホームと監視
優先設定: [\[ホーム \] ページと \[監視 \] ページ](#)
 - セキュリティの状態
環境設定: [セキュリティの状態](#)
 - ログとレポート
環境設定: [ログとレポート](#)
3. 変更するオプションの値を設定します。
4. [OK] をクリックします。

スタンドアロン Web ブラウザからのレポートへのログオン

管理サーバーに接続されたスタンドアロン Web ブラウザから、[ホーム] ページ、[監視] ページ、[レポート] ページにアクセスできます。ただし、スタンドアロンブラウザを使うときには、それ以外のコンソールの機能は使用できません。

レポートのページとログのページは、常に管理サーバーのインストールに使った言語で表示されます。リモートコンソールまたはブラウザを使ってこれらのページを表示する場合は、使っているコンピュータに適切なフォントがインストールされている必要があります。

Web ブラウザからレポートにアクセスするには、次の情報が必要です。

- 管理サーバーのホスト名。
- 管理サーバーのユーザー名とパスワード。

NOTE

使用する Symantec Endpoint Protection バージョンでサポートされる最小ブラウザバージョンのシステム必要条件を確認します。古いバージョンの Web ブラウザはサポートされません。

[Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)

スタンドアロン Web ブラウザからレポートにログオンするには

1. Web ブラウザを開きます。
2. [アドレス] テキストボックスに、次の形式でデフォルトのレポート URL を入力します。

`https://<SEPMServer>:8445/reporting`

ここで、SEPMServerは管理サーバーのホスト名または IP アドレスです。サポート対象の Web ブラウザのリストについては、「[Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)」を参照してください。

IP アドレスには IPv4 と IPv6 があります。IPv6 アドレスは角カッコで囲む必要があります。例: `https://[SEPMServer]:8445`

IPv6 はバージョン 14.2 以降でサポートされます。

NOTE

HTTPS スタンドアロンレポート URL をブラウザに入力すると、警告が表示されることがあります。警告が表示されるのは、管理サーバーが使う証明書が自己署名であるからです。この問題を回避するには、ブラウザの信頼できる証明書ストアに証明書をインストールします。証明書はホスト名のみをサポートするので、URL にホスト名を使用します。localhost、IP アドレス、または完全修飾ドメイン名を使うと、警告が引き続き表示されます。

3. ログオンのダイアログボックスが表示されたら、ユーザー名とパスワードを入力して [ログオン] をクリックします。

複数のドメインがある場合は、[ドメイン] テキストボックスにドメイン名を入力します。

つの Symantec Endpoint Protection Manager のレポートの種類について

次のカテゴリのレポートが利用可能です。

- クイックレポート。必要に応じて実行できます。
- 定時レポート。設定したスケジュールに基づいて自動的に実行されます。

レポートには、管理サーバーおよび管理サーバーと通信するクライアントコンピュータから収集されたイベントデータが含まれます。確認する必要がある情報が提供されるようにレポートをカスタマイズできます。

クイックレポートは前もって定義されていますが、カスタマイズすることができ、カスタマイズされたレポートの作成に使うフィルタを保存できます。カスタムフィルタを使って、カスタム定時レポートを作成できます。レポートの実行スケジュールを設定するときは、任意の数の受信者に電子メールで送信されるように設定できます。

デフォルトでは、定時レポートは常に実行されます。未実行の定時レポートについて、設定を変更できます。単一の定時レポート、またはすべての定時レポートを削除することもできます。

Table 146: クイックレポートと定時レポートとして利用可能なレポートの種類

レポートの種類	説明
監査	クライアントと場所が現在使っているポリシーに関する情報が表示されます。イベントの日時と種類、ポリシー修正、ドメイン、サイト、管理者、説明など、ポリシーを修正する活動に関する情報が含まれます。 監査ログとクイックレポート
アプリケーションとデバイス制御	ある種類の動作が遮断されたイベントに関する情報が表示されます。これらのレポートには、アプリケーションのセキュリティ警告、遮断したターゲット、遮断したデバイスに関する情報が含まれます。遮断したターゲットとして、Windows のレジストリキー、DLL、ファイル、プロセスがあります。 アプリケーションとデバイス制御のログとクイックレポート
コンプライアンス	ホストインテグリティ検査に成功したクライアントと失敗したクライアントの数についての情報を表示します。
コンピュータの状態	どのコンピュータのセキュリティ機能がオフになったかなど、ネットワーク内のコンピュータの稼働状態に関する情報が表示されます。これらのレポートには、バージョン、サーバーにチェックインしていないクライアント、クライアントイベントリ、オンライン状態に関する情報が含まれます。 コンピュータ状態ログとレポート

レポートの種類	説明
ディセプション	ディセプション活動を報告する件数が上位のコンピュータまたはユーザー、トリガされた件数が上位のディセプタなど、ディセプション活動に関する情報を表示します。 ディセプションのログとレポート
ネットワークとホスト悪用防止	侵入防止、ファイアウォールへの攻撃、ファイアウォールのトラフィックとパケット、メモリエクスプロイト緩和機能に関する情報を表示します。 ネットワークとホストのエクスプロイト緩和機能レポートでは、コンピュータの活動と、他のコンピュータやネットワークとのやり取りを追跡できます。ネットワーク接続を通してコンピュータに出入りしようとするトラフィックに関する情報が記録されます。メモリエクスプロイト緩和機能のイベントは、どの緩和機能がアプリケーションを終了したり、エクスプロイトによるアプリケーションへの攻撃を遮断したりしたかを一覧で表示します。 ネットワークとホストのエクスプロイト緩和機能のログとクイックレポート
リスク	管理サーバーとそのクライアントのリスクイベントに関する情報が表示されます。SONAR スキャンに関する情報が含まれます。 リスクログとクイックレポート SONAR ログ
スキャン	ウイルスとスパイウェアのスキャンアクティビティに関する情報が表示されます。 スキャンログとクイックレポート
システム	イベント時間、イベントの種類、サイト、ドメイン、サーバー、重大度に関する情報が表示されます。システムレポートには、クライアントの問題をトラブルシューティングするときに役立つ情報が含まれます。 システムログとクイックレポート

ネットワークに複数のドメインがある場合は、多くのレポートですべてのドメイン、1つのサイト、一部のサイトのいずれかのデータを表示できます。すべてのクイックレポートのデフォルトでは、作成するレポートに応じてすべてのドメイン、グループ、サーバーが表示されます。

[クイックレポートの実行とカスタマイズ](#)

[定時レポートの実行方法](#)

次のセクションでは、名前とその全般的な内容別にレポートを示します。すべてのレポートで、基本設定と拡張設定を変更して表示するデータを調整できます。カスタムフィルタに名前を付けて保存し、同じカスタムレポートを後で実行することもできます。

Table 147: 監査レポート

レポート名	説明
使われるポリシー	このレポートには、クライアントおよび場所で現在使用されているポリシーが表示されます。情報には、ドメイン名、グループ名、および各グループに適用されるポリシーのシリアル番号が含まれます。

Table 148: アプリケーションとデバイス制御レポート

レポート名	説明
警告最多アプリケーション制御ログの上位グループ	このレポートは、円グラフと相対値の棒グラフで構成されます。最も多くのセキュリティ警告を生成したグループとそのアプリケーション制御ログを示します。
上位を占める遮断した対象	このレポートは、円グラフと以下の対象 (該当する場合) で構成されます。 • 上位のファイル • 上位のレジストリキー • 上位のプロセス • 上位のモジュール (dll)
上位を占める遮断したデバイス	このレポートは、ネットワークへのアクセスが最も頻繁に遮断されたデバイスを示す円グラフで構成されます。

Table 149: コンプライアンスレポート

レポート名	説明
ホストインテグリティの状態	このレポートには、クライアントのコンピュータで実行されるホストインテグリティ検査に成功または失敗したクライアントが表示されます。
コンプライアンスエラーの概略別クライアント	このレポートは、次の内容を示す棒グラフで構成されます。 • ウイルス対策、ファイアウォール、VPN などの制御エラーイベントの種類別の個別ワークステーションの数 • グループ内のクライアントの合計数
コンプライアンスエラーの詳細	このレポートは、制御エラーによる重複のないコンピュータを示す表で構成されます。各エラーに関連する基準とルール、および配備されるクライアントの割合と失敗した割合を示します。
場所別の準拠しないクライアント	このレポートは、コンプライアンスエラーのイベントを示す表で構成されます。これらのイベントは、場所に基づくグループごとに表示されます。情報には、失敗した重複のないコンピュータ、合計エラーと場所エラーの割合が含まれます。

Table 150: コンピュータ状態レポート

レポート名	説明
ウイルス定義分布	このレポートには、ネットワーク全体で使われている重複のないウイルス定義ファイルのバージョンと、それぞれのバージョンを使っているコンピュータの数と割合が表示されます。
最近更新していないコンピュータ	このレポートには、最近更新していないすべてのコンピュータのリストが表示されます。また、コンピュータのオペレーティングシステム、IP アドレス、ユーザー名、および最後にコンピュータの状態が変更された時刻も表示されます。
Symantec Endpoint Protection 製品バージョン	このレポートには、ネットワーク内のすべての Symantec Endpoint Protection 製品バージョンのバージョン番号のリストが表示されます。また、それぞれのドメインとサーバー、コンピュータの数と割合も含まれます。
侵入防止シグネチャの分布	このレポートには、ネットワーク全体で使用される IPS シグネチャファイルのバージョンが表示されます。また、それぞれのドメインとサーバー、コンピュータの数と割合も含まれます。
ダウンロード保護シグネチャ分布	このレポートには、ネットワーク全体で使用されるダウンロード保護シグネチャファイルのバージョンが表示されます。また、それぞれのドメインとサーバー、コンピュータの数と割合も含まれます。
SONAR シグネチャの分布	このレポートには、ネットワーク全体で使用される SONAR シグネチャファイルのバージョンが表示されます。また、それぞれのドメインとサーバー、コンピュータの数と割合も含まれます。

レポート名	説明
クライアントインベントリ	このレポートは、コンピュータの合計数と次の項目の割合を示す棒グラフで構成されます。 - オペレーティングシステム - メモリの合計 - 空きメモリ - ディスク容量の合計 - 空きディスク容量 - CPU の種類
コンプライアンス状態分布	このレポートは、グループまたはサブネットごとにコンプライアンスの成功と失敗を表示する円グラフと相対値の棒グラフで構成されます。コンプライアンスを満たしているコンピュータの数と割合を示します。
クライアントオンライン状態	このレポートは、グループまたはサブネットごとの円グラフと相対値の棒グラフで構成されます。オンラインのコンピュータの割合を示します。 オンラインとは次の状態を表します。 - プッシュモードのクライアントの場合、クライアントが現在サーバーに接続されていることを表します。 - プルモードのクライアントの場合、直前の 2 つのクライアントハートビートの間に、クライアントがサーバーに接続していることを表します。 - リモートサイトのクライアントの場合、直前の複製時にクライアントがオンラインであったことを表します。
最新ポリシーを備えたクライアント	このレポートは、グループまたはサブネットごとの円グラフで構成されます。コンピュータの数と最新のポリシーが適用されたコンピュータの割合を示します。
グループ別のクライアント数	このレポートは、グループ別のホスト情報を示す表で構成されます。クライアントとユーザーの数を示します。複数のドメインを使う場合、この情報はドメインごとに表示されます。
セキュリティ状態の概略	このレポートには、ネットワークの全般的なセキュリティの状態が反映され、以下の状態のコンピュータの数と割合が表示されます。 - ウイルス対策 (英語) がオフ - Auto-Protect がオフ - 改変対策がオフ - 再起動が必要である - ホストインテグリティ検査が失敗した - ネットワーク脅威防止がオフ
保護コンテンツのバージョン	このレポートには、ネットワーク全体で使用されるすべてのプロアクティブ防止コンテンツのバージョンが表示されます。以下の種類の保護ごとに 1 つの円グラフが表示されます。 - 分解エンジンのバージョン - 消去エンジンのバージョン - SONAR コンテンツのバージョン - SONAR エンジンのバージョン - 商用アプリケーションリストのバージョン - コンテンツハンドラエンジンのバージョン - 許可アプリケーションリストのバージョン - シマンテックセキュリティレスポンスによって追加された新しいコンテンツの種類
Symantec Endpoint Protection ライセンスの状態	このレポートは、体験版ライセンスの有効期限までの残り日数と新しいライセンスを追加する手順を示します。
クライアントインベントリの詳細	このレポートは、コンピュータの仕様とシグネチャなどのクライアントインベントリの詳細を示します。

レポート名	説明
クライアントソフトウェアロールアウト (スナップショット) 定時レポートのみ	このレポートは、クライアントパッケージ配備の進行状況を追跡する表で構成されます。スナップショット情報により、ロールアウトの進行状況や、配備が完全に完了していないクライアントの数を確認できます。
一定期間にわたってオンライン/オフラインのクライアント (スナップショット) 定時レポートのみ	このレポートは、オンラインまたはオフラインのクライアントの数を示す折れ線グラフと表で構成されます。上位を占める対象ごとに 1 つのグラフが表示されます。対象はグループまたはオペレーティングシステムです。
一定期間にわたって最新ポリシーを備えたクライアント (スナップショット) 定時レポートのみ	このレポートは、最新のポリシーが適用されたクライアントを示す折れ線グラフで構成されます。上位クライアントごとに 1 つのグラフが表示されます。
一定期間にわたって準拠しないクライアント (スナップショット) 定時レポートのみ	このレポートは、一定期間にわたってホストインテグリティ検査に失敗したクライアントの割合を示す折れ線グラフで構成されます。上位クライアントごとに 1 つのグラフが表示されます。
ウイルス定義ロールアウトレポート (スナップショット) 定時レポートのみ	このレポートは、クライアントにロールアウトされたウイルス定義パッケージのバージョンを示します。この情報は、新しいウイルス定義の配備の進行状況をコンソールから追跡する場合に役立ちます。
配備レポート	このレポートは、クライアントのインストールと配備の状態の概略を示します。

Table 151: ネットワークとホストのエクスポloit緩和機能のレポート

レポート名	説明
上位を占める攻撃の標的	攻撃の数と割合、攻撃の種類と重大度、攻撃の分布などの情報が表示されます。グループ、サブネット、クライアント、またはポートを対象として使用して情報を表示できます。
上位を占める攻撃元	ネットワークに対する攻撃を開始した上位ホストが表示されます。攻撃の数と割合、攻撃の種類と重大度、攻撃の分布などの情報が表示されます。
上位を占める攻撃の種類	イベントの数と割合、グループと重大度、グループごとのイベントの種類と数などの情報が表示されます。
上位を占める遮断したアプリケーション	ネットワークへのアクセスが遮断された上位アプリケーションが表示されます。攻撃の数と割合、グループと重大度、グループごとのイベントの種類と数などの情報が表示されます。
一定期間にわたる攻撃	選択された期間の攻撃が表示されます。たとえば、時間範囲が過去 1 カ月の場合、レポートには過去 1 カ月間の 1 日ごとの攻撃の合計数が表示されます。レポートには、攻撃の数と割合が含まれます。すべてのコンピュータに対する攻撃を表示したり、上位のオペレーティングシステム、ユーザー、IP アドレス、グループ、攻撃の種類ごとの情報を表示できます。
重大度別セキュリティイベント	重大度に従って順位付けされた、ネットワーク内のセキュリティイベントの合計数と割合が表示されます。
一定期間に遮断したアプリケーション	選択した期間にネットワークへのアクセスが遮断されたアプリケーションの合計数が表示されます。レポートには、イベントの時間、攻撃の数、割合が含まれます。すべてのコンピュータの情報を表示したり、グループ、IP アドレス、オペレーティングシステム、ユーザーごとの情報を表示できます。
一定期間にわたるトラフィック通知	一定期間にわたるファイアウォールルール違反に基づく通知の数が表示されます。カウントされるルールは、[ファイアウォールルール] リストの [ログ記録] 列で [電子メール警告の送信] オプションにチェックマークを付けたルールです。このレポートにはすべてのコンピュータの情報を表示したり、グループ、IP アドレス、オペレーティングシステム、ユーザーごとの情報を表示したりできます。

レポート名	説明
上位を占めるトラフィック通知	グループまたはサブネットと、通知の数と割合が一覧表示されます。通知を行うように設定したファイアウォールルール違反に基づいて、通知の数が示されます。カウントされるルールは、[ファイアウォールルール] リストの [ログ記録] 列で [電子メール警告の送信] オプションにチェックマークを付けたルールです。情報は、すべてのログ、トラフィックログ、パケットログのいずれかについて、上位のグループまたはサブネットごとにグループ化して表示できます。
メモリエクスプロイト緩和機能検出	遮断または許可されたメモリエクスプロイト緩和機能の種類が表示されます。
上位を占める URL 検出	URL 評価によってブロックされる URL が一覧表示されます。
詳細レポート	上位のネットワーク脅威防止アイテムが 1 つのレポート内に一覧表示されます。

Table 152: リスクレポート

レポート名	説明
感染コンピュータとリスクを伴うコンピュータ	このレポートは 2 つの表で構成されます。1 つの表にはウイルスに感染したコンピュータが示され、もう 1 つの表にはまだ解決されていないセキュリティリスクのあるコンピュータが示されます。
処理リスト	このレポートは、リスクが検出されたときに実行可能なすべての処理の数を示す表で構成されます。実行可能な処理は、[クリーニング]、[疑いあり]、[遮断]、[検疫]、[削除]、[修復の保留]、[強制または商用の検出をログに記録しました]、[新規感染]、および [未解決感染] です。この情報は、Symantec Endpoint Protection のホームページにも表示されます。
リスクの検出数	このレポートは、円グラフ、リスクの表、関連する相対値の棒グラフで構成されます。リスク検出の数をドメイン、サーバー、コンピュータごとに示します。レガシー Symantec AntiVirus クライアントがある場合、レポートではドメインの代わりにサーバーグループが使われます。
ネットワークで検出された新種のリスク	このレポートは、表と分布円グラフで構成されます。新しいリスクのそれぞれについて、次の情報が表示されます。 - リスク名 - リスクのカテゴリまたは種類 - 最初に検出されたデータ - 組織で最初の発生 - 最初に検出したスキンの種類 - リスクが発見されたドメイン (レガシーコンピュータでは、サーバーグループ) - リスクが発見されたサーバー (レガシーコンピュータでは、親サーバー) - リスクが発見されたグループ (レガシーコンピュータでは、親サーバー) - リスクが発見されたコンピュータと、発見されたときにログオンしていたユーザーの名前 円グラフは、選択した対象の種類 (ドメイン (レガシーコンピュータでは、サーバーグループ)、グループ、サーバー (レガシーコンピュータでは、親サーバー)、コンピュータ、またはユーザー名) 別の新しいリスク分布を示します。
上位のリスク検出相関関係	このレポートは、2 つの変数を使ってウイルス検出とセキュリティリスク検出の相関を示す 3 次元棒グラフで構成されます。x 軸と y 軸の変数として、それぞれコンピュータ、ユーザー名、ドメイン、グループ、サーバー、リスク名のいずれかを選択できます。このレポートは、各軸の変数に対して上位 5 つのインスタンスを示します。変数の 1 つとしてコンピュータを選択し、感染コンピュータが 4 台以下の場合には、感染していないコンピュータがグラフに表示されます。 Note: レガシー版の Symantec AntiVirus を実行しているコンピュータでは、ドメインとサーバーの代わりにサーバーグループと親サーバーが使われます。
ダウンロードリスク分布	このレポートには、ダウンロードインサイトで検出されたファイルの数が表示されます。ファイルは感度によってグループ化されます。検出されたファイルの詳細なレポートが表示されます。レポートを実行する前に、URL、Web ドメイン、アプリケーション、およびユーザー許可別にファイルをグループ化することもできます。

レポート名	説明
リスク分布の概略	このレポートは、選択した対象の種類について各項目の相対的な割合を示す、円グラフと関連する棒グラフで構成されます。たとえば、選択した対象がリスク名の場合、円グラフは重複のないリスクそれぞれの割合を示します。リスク名ごとに棒グラフが表示され、そこには検出数と検出の合計に対する割合が含まれます。
一定期間にわたるリスク分布	このレポートは、単位時間あたりのウイルスとセキュリティリスクの検出数を示す表と、相対値の棒グラフで構成されます。
保護技術別のリスク分布	このレポートには、保護技術ごとのウイルスとセキュリティリスク検出の数が表示されます。
SONAR 検出結果	このレポートは、以下の情報を示す円グラフと棒グラフで構成されます。 - リスクとしてラベルが付けられ、ネットワークで許容可能として例外に追加したアプリケーションのリスト - 検出され、リスクとして確認されたアプリケーションのリスト - 検出されたがリスクとしての状態が未確認であるアプリケーションのリスト 各リストについて、このレポートには会社名、アプリケーションハッシュとバージョン、および関係するコンピュータが表示されます。許可アプリケーションについては、許可のソースも表示されます。
SONAR 脅威分布	検出された上位アプリケーションの名前が、相対値の棒グラフおよび概略の表と一緒に表示されます。検出には、商用アプリケーションリストと強制検出リストのアプリケーションが含まれます。最初の概略の表には、アプリケーション名および検出の数と割合が含まれます。
一定時間にわたる SONAR 脅威検出	このレポートは、選択した期間のプロアクティブ脅威検出の数を示す折れ線グラフで構成されます。一定期間にわたって検出された脅威の合計数を示す表と相対値の棒グラフも表示されます。
上位リスクの処理概略	このレポートは、ネットワークで発見された上位リスクを示します。リスクごとに、検出されたときに実行された処理の割合を示す、処理の概略の棒グラフが表示されます。処理には、検疫、クリーニング、削除などがあります。このレポートには、それぞれの処理が設定された第1の処理であった場合、設定された第2の処理であった場合、いずれでもない場合、不明の場合の割合も示されます。
通知の数	このレポートは、円グラフと関連する相対値の棒グラフで構成されます。グラフは、通知を行うように設定したファイアウォールルール違反でトリガされた通知の数を示します。通知の種類と、それぞれの数も示されます。
一定期間にわたる通知の数	このレポートは、選択した期間に送信されたネットワーク内の通知の数を示す折れ線グラフで構成されます。一定期間の通知の数と割合を示す表も表示されます。フィルタ処理により、通知の種類、応答の状態、作成者、通知名ごとにデータを表示できます。
週次アウトブレイク	このレポートには、週あたりのウイルスとセキュリティリスクの検出数と相対値の棒グラフが、指定した時間範囲で表示されます。範囲が1日の場合は、過去1週間のデータが表示されます。
総合リスクレポート	デフォルトでは、このレポートには分布レポートや新しいリスクのレポートがすべて含まれます。レポートを設定することで、特定のレポートだけを含めることができます。このレポートには、すべてのドメインの情報が含まれます。
Symantec Endpoint Protection の日次状態	このレポートは、過去24時間にわたるウイルス検出、ネットワークイベントの介入と定義の状態を示します。
Symantec Endpoint Protection の週次状態	このレポートは、前週のエンドポイントコンピュータのライセンス状態とウイルス検出統計を示します。データは特に断りがない限り累積値を反映します。

Table 153: スキャンレポート

レポート名	説明
スキャン統計ヒストグラム	このレポートは、ヒストグラムで構成されます。スキャンにおける以下の情報を分布する方法をヒストグラムで選択できます。 - スキャン時間 (秒単位) - 検出したリスクの数 - 検出したファイルの数 - スキャンしたファイルの数 - スキャンを省略したファイルの数 ヒストグラムに使うビンの範囲とビンの数も設定できます。ビンの範囲は、選択したグループごとに使うデータの区間です。ビンの数は、ヒストグラムでデータ区間を繰り返す回数を指定します。 表示される情報には、エントリ数、最大値と最小値、平均値と標準偏差が含まれます。 レポートの値を変更して、レポートのヒストグラムに生成される情報を最大化できます。たとえば、ネットワークのサイズや表示する情報の量を検討します。
前回のスキャン時間別のコンピュータ	このレポートは、セキュリティネットワーク内のコンピュータのリストを前回のスキャン時間別に示します。また、スキャン時にログインしていたユーザーの IP アドレスと名前も含まれます。
スキャンしていないコンピュータ	このレポートは、セキュリティネットワーク内でスキャンしていないコンピュータのリストを示します。また、以下の情報が提供されます。 - IP アドレス - 前回のスキャンの時間 - 現在のユーザーまたは前回のスキャン時にログインしていたユーザーの名前

Table 154: システムレポート

レポート名	説明
エラーを生成する上位クライアント	このレポートは、警告の条件とエラーの条件ごとの円グラフで構成されます。グラフは、相対的なエラー数と警告数および割合をクライアント別に示します。
エラーを生成する上位サーバー	このレポートは、警告の条件とエラーの条件ごとの円グラフで構成されます。グラフは、相対的なエラー数と警告数および割合をサーバー別に示します。
一定期間にわたるデータベース複製エラー	このレポートは、選択した時間範囲の複製エラーを示す折れ線グラフと関連する表で構成されます。
サイト状態レポート	このレポートは、すべてのサイトの健全性状態およびローカルサイトのすべてのサーバーに関する情報のリアルタイム概略を示します。
WSS 統合トークンの使用状況	このレポートは、Web とクラウドのアクセス保護 を使用するクライアント認証の統合トークンの使用状況に関する概略を示します。

クイックレポートの実行とカスタマイズ

クイックレポートは事前定義済みのカスタマイズ可能なレポートです。これらのレポートは管理サーバーと通信するクライアントコンピュータと管理サーバーから収集されるイベントデータを含んでいます。クイックレポートはレポートのために設定するオプションに特定のイベントの情報を提供します。レポート設定を保存して同じレポートを後で実行したり、レポートを印刷または保存できます。

クイックレポートは静的で、レポートのために指定する時間枠に特定の情報を提供します。また、ログを使ってリアルタイムのイベントを監視できます。

1. オプション 1: クイックレポートを実行するには、コンソールで [レポート] をクリックします。
2. [クイックレポート] タブの [レポートの種類] リストボックスで、実行するレポートの種類を選択します。
3. [レポートの選択] リストボックスでは、実行するレポートの名前を選択します。
4. [レポートの作成] をクリックします。
5. オプション 2: クイックレポートをカスタマイズするには、コンソールで [レポート] をクリックします。
6. [クイックレポート] タブの [レポートの種類] リストボックスで、カスタマイズするレポートの種類を選択します。
7. [レポートの選択] リストボックスでは、カスタマイズするレポートの名前を選択します。

[ネットワークコンプライアンス状態] レポートと [コンプライアンス状態] レポートについては、[ステータス] リストボックスで、使いたい保存されたフィルタ設定を選択するか、デフォルトのフィルタのままにします。

[上位のリスク検出相関関係] レポートについては、[X 軸] と [Y 軸] のリストボックスの値を選択してレポートの表示方法を指定できます。

[スキャン統計ヒストグラム] レポートについては、[ビンの範囲] と [ビンの数] の値を選択できます。

一部のレポートについては、[グループ] リストボックスでレポート結果を分ける方法を指定できます。他のレポートについては、[対象] フィールドでレポート結果をフィルタ処理する対象を選択できます。
8. [保存したフィルタを使う] リストボックスで、保存したフィルタ設定を選択するか、デフォルトのフィルタのままにします。
9. [適用したいフィルタ設定は?] の [時間範囲] リストボックスで、レポートの時間範囲を選択します。
10. [特定日を設定する] を選択する場合は、[開始日] と [終了日] のリストボックスを使います。これらのオプションは、情報を表示する時間間隔を設定します。

コンピュータの状態レポートを生成して [特定日を設定する] を選択するとき、日時のフィールドで指定する時間以降にサーバーでチェックインされなかったコンピュータが関係するすべてのエントリを表示するように指定します。
11. レポートの追加設定をする場合は、[追加設定] をクリックして、必要なオプションを設定します。

12.1.xでは、[追加設定] ではなく [拡張設定] です。

[詳しい説明を表示] をクリックすると状況感知型ヘルプでフィルタオプションの説明を参照できます。

NOTE

フィルタオプションのテキストボックスは、ワイルドカード文字を使って一致するものを検索でき、大文字小文字は区別しません。ワイルドカード文字として使用できるのは、ASCII のアスタリスク文字だけです。

このレポートを後で再実行する場合は、レポート設定を保存できます。

12. [レポートの作成] をクリックします。

[カスタムレポートの保存](#)

[レポートの印刷と保存](#)

[定時レポートの実行方法](#)

カスタムレポートの保存

カスタムレポートの設定をフィルタに保存して、後で再度レポートを生成できます。設定を保存するときに、これらはデータベースに保存されます。フィルタに付けた名前は、関連するログとレポートの [保存したフィルタを使う] リストボックスに表示されます。

NOTE

ユーザーが保存したフィルタ設定は、本人のユーザーログオンアカウントでのみ利用できます。レポート作成の権限を持つユーザーは、他のユーザーが保存した設定にアクセスできません。

定時レポートに使うフィルタの編集

作成したレポート設定は削除できます。設定を削除すると、そのレポートを利用できなくなります。デフォルトのレポート設定の名前が [保存したフィルタを使う] リストボックスに表示され、画面はデフォルトの設定で更新されます。

NOTE

管理サーバーから管理者を削除する場合、削除する管理者によって作成されたレポートを保存できます。レポートの所有権と名前は変更されます。新しいレポート名の形式は、「####('####')」です。たとえば、管理者 JSmith によって作成された Monday_risk_reports という名前のレポートは、Monday_risk_reports(JSmith) という名前に変更されます。

管理者アカウントとアクセス権について

カスタムレポートを保存するには

1. コンソールで、[レポート] をクリックします。
2. [クイックレポート] タブで、リストボックスからレポートの種類を選択します。
3. レポートの基本設定と追加設定を変更します。
12.1.xでは、[追加設定] ではなく [拡張設定] です。
4. [フィルタの保存] をクリックします。
5. [フィルタ名] テキストボックスに、レポートフィルタの詳しい名前を入力します。フィルタが [保存したフィルタを使う] リストに追加されるときに、入力した名前の最初の 32 文字だけが表示されます。
6. [OK] をクリックします。
7. 確認のダイアログボックスが表示されたら、[OK] をクリックします。

保存したフィルタは、関連するレポートとログの [保存したフィルタを使う] リストボックスに表示されます。

定時レポートの実行方法

定時レポートは、設定したスケジュールに基づいて自動的に実行されるレポートです。定時レポートは受信者に電子メールで送信されるため、少なくとも 1 人の受信者の電子メールアドレスを指定する必要があります。レポートの実行後、レポートは .mht 添付ファイルとして、設定した受信者に電子メールで送信されます。

定時レポートに表示されるデータは、データベースで 1 時間ごとに更新されます。レポートのデータは、管理サーバーによって定時レポートが電子メールで送信される日時から 1 時間以内のものです。

一定期間のデータを含むその他のレポートは、クライアントログに対して設定したアップロード間隔に基づいて、データベースで更新されます。

クライアントログサイズと管理サーバーにアップロードするログの指定

NOTE

サイト内にデータベースを共有する複数のサーバーがある場合は、最初にインストールされたサーバーがサイトの定時レポートを実行します。このデフォルトの動作により、サイトのすべてのサーバーが同じ定時スキャ

ンを同時に実行することはありません。別のサーバーで定時レポートを実行する場合は、ローカルサイトのプロパティでこのオプションを設定できます。

定時レポートを実行するには

1. コンソールで、[レポート] をクリックします。
2. [定時レポート] タブで、[追加] をクリックします。
3. [レポート名] テキストボックスに詳しい名前を入力し、さらに詳しい説明を入力します (省略可能)。
説明のテキストボックスには 255 文字を超える文字を貼り付けることができますが、説明として保存されるのは 255 文字だけです。
4. しばらくこのレポートを実行しない場合は、[この定時レポートを有効にする] チェックボックスのチェックマークをはずします。
5. リストボックスから、スケジュールを設定するレポートの種類を選択します。
6. リストボックスから、スケジュールを設定するレポートの名前を選択します。
7. リストボックスから、利用する保存済みフィルタの名前を選択します。
8. [実行間隔] テキストボックスで、レポートを電子メールで受信者に送信する間隔を選択します (時間、日、週、月)。続いて、選択した間隔の値を入力します。たとえば、1 日おきにレポートを送信する場合は、[日] を選択して 2 を入力します。
9. [開始まで] テキストボックスに、レポートを開始する日付を入力するか、カレンダーアイコンをクリックして日付を選択します。続いて、リストボックスから時間と分を選択します。
10. [レポート受信者] に、1 つ以上の電子メールアドレスをカンマ区切りで入力します。

電子メール通知が機能するようにメールサーバーのプロパティが設定済みである必要があります。

11. [OK] をクリックします。

定時レポートに使うフィルタの編集

スケジュールを設定したレポートの設定を変更できます。次にレポートが実行されるときに、新しいフィルタ設定が使われます。保存済みのレポートフィルタを基にして、追加の定時レポートを作成することもできます。

フィルタの保存は作成者ごとに行われるため、2 人のユーザーが同じ名前のフィルタを作成しても問題は発生しません。ただし、デフォルトの管理アカウントにログオンする 1 人または 2 人のユーザーが、同じ名前のフィルタを作成しないようにしてください。

ユーザーが同じ名前のフィルタを作成する場合、次の 2 つの状況で競合が発生する場合があります。

- 2 人のユーザーがデフォルトの管理アカウントに別のサイトでログオンし、それぞれが同じ名前でフィルタを作成する場合
- 1 人のユーザーがフィルタを作成し、別のサイトにログオンして、すぐに同じ名前のフィルタを作成する場合

サイトの複製が実行される前にいずれかの状況が発生すると、フィルタリストに同じ名前の 2 つのフィルタが表示されるようになります。使えるのは一方のフィルタだけです。最も実践的な習慣として、この問題が発生した場合は使えるフィルタを削除し、別の名前で作成し直します。使えるフィルタを削除するときに、使えないフィルタも削除します。

カスタムレポートの保存

NOTE

保存したフィルタを定時レポートに関連付けるときには、フィルタにカスタム日付が含まれていないことを確認します。フィルタでカスタム日付が指定されていると、レポートが実行されるたびに同じレポートを受け取ります。

定時レポートの実行方法

定時レポートに使うフィルタを編集するには

1. コンソールで、[レポート] をクリックします。
2. [定時レポート] をクリックします。
3. レポートのリストで、編集する定時レポートをクリックします。
4. [フィルタの編集] をクリックします。
5. フィルタに必要な変更を行います。
6. [フィルタの保存] をクリックします。

元のレポートフィルタを維持する場合は、編集したフィルタに新しい名前を付けます。

7. [OK] をクリックします。
8. 確認のダイアログボックスが表示されたら、[OK] をクリックします。

レポートの印刷と保存

レポートを印刷したり、クイックレポートのコピーを保存したりできます。定時レポートを印刷することはできません。保存したファイルや印刷したレポートはレポートデータベースの現在のデータを示すスナップショットであるため、履歴を保持できます。

NOTE

Internet Explorer のデフォルト設定では、背景の色と画像が印刷されません。この印刷オプションが無効の場合、作成したレポートと印刷されたレポートの見た目が異なる場合があります。ブラウザの設定を変更して、背景の色と画像を印刷できます。

クイックレポートの実行とカスタマイズ

レポートを保存するときに、レポート用データベースの現在のデータに基づいてセキュリティ環境のスナップショットが保存されます。後で同じフィルタ設定に基づいて同じレポートを実行した場合、新しいレポートには異なるデータが表示されます。

1. レポートを印刷するには、レポートウィンドウで [印刷] をクリックします。
2. [印刷] ダイアログボックスで、必要に応じてプリンタを選択し [印刷] をクリックします。
3. レポートを保存するには、レポートウィンドウで [保存] をクリックします。
4. [ファイルのダウンロード] ダイアログボックスで、[保存] をクリックします。
5. [名前を付けて保存] ダイアログボックスの [保存する場所] ダイアログボックスで、ファイルを保存する場所を参照します。
6. [ファイル名] リストボックスで、必要に応じてデフォルトのファイル名を変更します。
7. [保存] をクリックします。

レポートが、MHTML Web ページアーカイブ形式で選択した場所に保存されます。

8. [ダウンロードの完了] ダイアログボックスで、[閉じる] をクリックします。

ログの表示

選択したフィルタ設定集に基づくログから、表示するイベントのリストを生成できます。

NOTE

大量のデータを含むログを表示したときにデータベースエラーが発生した場合、データベースのタイムアウトパラメータを変更すると安全です。

CGI エラーまたはプロセス終了エラーが発生する場合、その他のタイムアウトパラメータを変更すると安全です。

レポートとログを見直すためのタイムアウトパラメータの変更

レポートとログは、常に管理サーバーのインストールに使った言語で表示されます。リモートの Symantec Endpoint Protection Manager コンソールまたはブラウザを使ってこれらを表示する場合は、使っているコンピュータに適切なフォントがインストールされている必要があります。

つの Symantec Endpoint Protection Manager のログの種類について

フィルタを使ったカスタムログの保存と削除

ログを表示するには

1. コンソールで、[監視] をクリックします。
2. [ログ] タブの [ログの種類] リストボックスで、表示するログの種類を選択します。
3. ログの種類によっては、[ログの内容] リストボックスが表示されます。このリストボックスが表示された場合、表示するログの内容を選択します。
4. [保存したフィルタを使う] リストボックスで、保存したフィルタを選択するか、値をデフォルトのままにします。
5. [時間範囲] リストボックスで、時間を選択するか、デフォルト値のままにします。[特定日を設定する] を選択した場合、表示するエントリの日時を設定します。
6. [追加設定] をクリックして、表示するエントリの数を制限します。

選択した種類のログに、その他の利用可能な [追加設定] を設定することもできます。

12.1.xでは、[追加設定] ではなく [拡張設定] です。

NOTE

フィルタオプションフィールドは、ワイルドカード文字を使って一致するものを検索できますが、大文字小文字は区別しません。ワイルドカード文字として使用できるのは、ASCII のアスタリスク文字だけです。

7. [ログの表示] をクリックします。

[フィルタの保存] をクリックしてフィルタ構成を保存し、後で同じログ表示を生成することもできます。

つの Symantec Endpoint Protection Manager のログの種類について

ログにはクライアント設定の変更、セキュリティに関する活動、エラーについての記録が含まれています。これらの記録はイベントと呼ばれます。ログには、これらのイベントと追加の関連情報が表示されます。セキュリティに関する活動にはウイルス検出、コンピュータ状態、クライアントコンピュータから送受信されるトラフィックについての情報が含まれています。

ログは、各クライアントコンピュータの活動や、他のコンピュータやネットワークとの通信を追跡するための重要な手段です。このデータを使って、ネットワーク全体のセキュリティ状態を分析し、クライアントコンピュータでの保護を変更できます。ウイルス、セキュリティリスク、攻撃に関する傾向を追跡できます。複数のユーザーが同じコンピュータを使用する場合、誰がリスクを持ち込んだかを識別し、そのユーザーに予防措置を取らせることができます。

[監視] ページの [ログ] タブでログデータを表示できます。

管理サーバーはクライアントからログの情報を定期的にアップロードします。ログまたはレポートでこの情報を表示できます。レポートは固定であり、ログほどの詳しい情報が含まれないため、ログを使ってネットワークを監視することが好まれる場合もあります。

ログを使ってネットワークを監視するのに加えて、さまざまなログから次の操作を行うことができます。

- クライアントコンピュータでコマンドを実行する。

コンソールを使った、クライアントコンピュータでのコマンドの実行

- さまざまな種類の例外を追加する。
[ログイベントに基づく例外の作成](#)
- 検疫からファイルを削除する。
[コンピュータでの検疫ファイルの管理](#)

「[ログの種類](#)」では、表示できるコンテンツの種類と各ログから実行できる処理について説明します。

Table 155: ログの種類

ログの種類	コンテンツと処理
監査	監査ログには、ポリシー修正活動に関する情報が記載されます。 利用可能な情報には、イベントの日時と種類、修正されたポリシー、関係したドメイン、サイト、ユーザー名、説明が含まれます。 このログに関連付けされた処理はありません。 監査ログとクイックレポート
アプリケーションとデバイス制御	アプリケーション制御とデバイス制御のログには、ある種の動作が遮断されたイベントに関する情報が記載されます。 利用可能なアプリケーションとデバイス制御のログは次のとおりです。 - アプリケーション制御（改変対策に関する情報を含む） - デバイス制御 利用可能な情報には、イベントが発生した時刻、講じられた処置、関与したコンピュータ、ドメインなどがあります。また、関与したユーザー、重大度、関与したルール、呼び出し元プロセス、ターゲットも含まれています。 アプリケーション制御ログから、アプリケーション制御例外または改変対策例外を作成できます。 Symantec Endpoint Protection が Windows クライアントの監視対象アプリケーションを処理する方法を指定する アプリケーションとデバイス制御のログとクイックレポート
コンプライアンス	コンプライアンスログにはクライアントのホストインTEGRITYに関する情報が記録されます。 このログに関連付けされた処理はありません。 コンプライアンスログとクイックレポート
コンピュータの状態	コンピュータの状態ログには、ネットワーク内のクライアントコンピュータのリアルタイム稼働状態に関する情報が含まれます。 利用可能な情報には、コンピュータ名、IP アドレス、感染の状態、保護技術、Auto-Protect の状態、バージョン、定義日などがあります。また、ユーザー、前回のチェックイン日時、ポリシー、グループ、ドメイン、再起動が必要かどうかが含まれます。 また、このログからコンピュータの感染状態を消去することもできます。 Note: このログには、Windows クライアントと Mac クライアントの両方から収集された情報が含まれています。 コンピュータ状態ログとレポート
ディセプション	ディセプションのログには、ディセプタの活動の結果 つの Symantec Endpoint Protection Manager にクライアントが送信するあらゆる活動に関する情報が記録されます。 ディセプションは、望ましいデータと攻撃ベクトルに見える内容を攻撃者に示すために使用するツールのセットです。これらのツールを使用すると、侵入の試みをすばやく検出して停止できます。ディセプションツールとヘルプファイルは、インストールファイルの /Tools/Deception フォルダにあります。 [監視]: [概略] タブ

ログの種類	コンテンツと処理
ネットワークとホスト悪用防止	ネットワークとホストの 익스프로이트緩和機能のログには、侵入防止、ファイアウォール、メモリ 익스프로이트緩和機能に関する情報が含まれます。 ログには、ファイアウォールに対する攻撃に関する情報や、侵入防止に関する情報が含まれます。サービス拒否攻撃、ポートスキャン、実行可能ファイルに行われた変更に関する情報を利用できます。この中には、ファイアウォールを介して行われる接続（トラフィック）や、通過するデータバケットに関する情報も含まれます。このログには、ネットワークアプリケーションの検出やソフトウェアの設定など、コンピュータに対して行われる動作上の変更情報も一部含まれます。 ネットワークとホストの 익스프로이트緩和機能のログとクイックレポート
SONAR	SONAR ログには、SONAR 脅威スキャン中に検出された脅威に関する情報が含まれています。悪質である可能性のあるアプリケーションがクライアントコンピュータで実行されたときに、それらをリアルタイムに検出するスキャンです。 情報には、発生日時、イベントの実際の処理、ユーザー名、Web ドメイン、アプリケーション、アプリケーションの種類、ファイル、パスなどの項目があります。 SONAR ログ SONAR について
リスク	リスクログには、リスクイベントに関する情報が含まれます。利用可能な情報には、イベントの日時、イベントの実際の処理、ユーザー名、コンピュータ、ドメイン、リスク名、送信元、件数、ファイル、パスなどがあります。 リスクログとクイックレポート
スキャン	スキャンログには、Windows クライアントと Mac クライアントの両方から得た、ウイルスとスパイウェアのスキャンアクティビティについての情報が含まれています。 利用可能な情報には、スキャン開始、コンピュータ、IP アドレス、状態、期間、検出、スキャンされた項目、省略された項目、ドメインなどの項目があります。 このログに関連付けされた処理はありません。 スキャンログとクイックレポート
システム	システムログには、サービスの開始日時や停止日時などのイベントに関する情報が含まれます。 このログに関連付けされた処理はありません。 システムログとクイックレポート

フィルタを使ったカスタムログの保存と削除

[基本設定] と [追加設定] を使ってカスタムフィルタを作成すると、表示される情報を変更できます。フィルタ設定をデータベースに保存すると、後で同じ表示を再び作成できます。設定を保存するときに、これらはデータベースに保存されます。フィルタに付けた名前は、関連するログとレポートの [保存したフィルタを使う] リストボックスに表示されます。

12.1.xでは、[追加設定] ではなく [拡張設定] です。

NOTE

ログフィルタの時間範囲として [過去 24 時間] を選択した場合、最初にフィルタを選択した時点が 24 時間の起点になります。ページを更新する場合、24 時間の時間範囲の開始時点はリセットされません。フィルタを選択して、ログの表示を待っていると、フィルタを選択したときに時間範囲の計時が始まります。ログを表示した時点で始まるものではありません。

過去 24 時間の時間範囲を確実に今すぐ開始するには、別の時間範囲を選択してから [過去 24 時間] を再び選択します。

1. フィルタを使ってカスタムログを保存するには、メインウィンドウで [監視] をクリックします。
2. [ログ] タブの [ログの種類] リストボックスで、フィルタを設定するログ表示の種類を選択します。
3. ログの種類によっては、[ログの内容] リストボックスが表示されます。このリストボックスが表示された場合、フィルタを設定するログの内容を選択します。
4. [保存したフィルタを使う] リストボックスで、最初に使うフィルタを選択します。たとえば、デフォルトのフィルタを選択します。
5. [適用したいフィルタ設定は?] で、[追加設定] をクリックします。
12.1.x では、[追加設定] ではなく [拡張設定] です。
6. 設定を変更します。
7. [フィルタの保存] をクリックします。
8. 表示されるダイアログボックスの [フィルタ名] ボックスに、このログフィルタ設定に使う名前を入力します。保存したフィルタがフィルタリストに追加されると、名前の最初の 32 文字のみが表示されます。
9. [OK] をクリックします。新しいフィルタ名が [保存したフィルタを使う] リストボックスに追加されます。
10. 確認のダイアログボックスが表示されたら、[OK] をクリックします。
11. 保存したフィルタを削除するには、[保存したフィルタを使う] リストボックスで、削除するログフィルタの名前を選択します。
12. [保存したフィルタを使う] リストボックスの横にある [削除] アイコンをクリックします。
13. フィルタを削除するかどうかの確認を求められたら、[はい] をクリックします。

別のサイトのログの表示

別のサイトのログを表示する場合、つの Symantec Endpoint Protection Manager コンソールからリモートサイトのサーバーにログオンする必要があります。リモートサイトのサーバーにアカウントを持っている場合、リモートでログオンして、そのサイトのログを表示できます。

複製パートナーを設定した場合、複製パートナーのすべてのログをローカルパートナーにコピーしたり、その逆を行ったりすることを選択できます。ログの複製を選択した場合、デフォルトでは、ログを表示したときに管理者のサイトと複製されたサイトの両方の情報が表示されます。1 つのサイトのみを確認する場合、データをフィルタ処理して、表示する場所を限定する必要があります。ログの複製を選択する場合は、すべての複製パートナーに追加ログ用の十分なディスク容量があることを確認してください。

複製のための 2 番目のサイトのインストール方法

別のサイトのログを表示するには

1. Web ブラウザを開きます。
2. アドレスのテキストボックスに、次のように入力します。

`http://<SEPMServer>:9090`

ここで、SEPMServer はサーバー名または IP アドレスです。

IP アドレスには IPv4 と IPv6 があります。IPv6 アドレスの場合は、次のように角カッコで囲む必要があります。`http://[<SEPMServer>]:9090`

コンソールがダウンロードを開始します。ログオンに使うコンピュータには、JRE (Java Runtime Environment) がインストールされている必要があります。インストールされていない場合、ダウンロードしてインストールするように促すメッセージが表示されます。メッセージに従って JRE をインストールします。

-
3. コンソールのログオンダイアログボックスで、ユーザー名とパスワードを入力します。
 4. 自動的に入力されない場合、[サーバー] テキストボックスにサーバー名または IP アドレスとポート番号 8443 を次のように入力します。

`http://<SEPMServer>:8443`

5. [ログオン] をクリックします。

ログデータの Syslog サーバーへのエクスポート

データベースの領域を増やすには、管理サーバーでログデータを Syslog サーバーに送信するように設定できます。

ログデータを Syslog サーバーにエクスポートする場合、ログを受信するように Syslog サーバーを設定する必要があります。

ログデータのテキストファイルへのエクスポート

ログデータを Syslog サーバーにエクスポートするには

1. コンソールで、[管理] をクリックします。
2. [サーバー] をクリックします。
3. ログデータのエクスポート元となるローカルサイトまたはリモートサイトをクリックします。
4. [外部ログ記録の設定] をクリックします。
5. [全般] タブの [更新頻度] リストボックスで、ログデータをファイルに送信する頻度を選択します。
6. [マスターログ記録サーバー] リストボックスで、ログを送信する管理サーバーを選択します。

SQL Server を使い、複数の管理サーバーをデータベースに接続する場合は、1 台のサーバーのみをマスターログ記録サーバーとして指定します。

7. [Syslog サーバーへのログの送信を有効にする] にチェックマークを付けます。
8. 次の情報が表示されます。

- **Syslog サーバー**
ログデータを受信する Syslog サーバーの IP アドレスまたはドメイン名を入力します。
- **送信先ポート**
使うプロトコルを選択し、Syslog サーバーが Syslog メッセージの応答準備に使う送信先ポートを指定します。
- **ログ機能**
Syslog 設定ファイルで使うログ機能の数を入力するか、デフォルトを使います。有効な値は 0 から 23 です。

9. [ログフィルタ] タブで、エクスポートするログにチェックマークを付けます。

10. [OK] をクリックします。

ログデータのテキストファイルへのエクスポート

ログからテキストファイルにデータをエクスポートするとき、デフォルトではファイルはフォルダに配置されます。デフォルトのフォルダパスは、C:\Program Files (x86)\Symantec\の Symantec Endpoint Protection Manager\data\dump です。レコードがテキストファイルに転送されるまで、エントリは .tmp ファイルに配置されます。

12.1.x を実行する 32 ビットシステムの場合は、C:\Program Files (x86)\Symantec\の Symantec Endpoint Protection Manager\data\dump です。

NOTE

エクスポートしたログデータを使ってデータベースを復元することはできません。

「Symantec Endpoint Protection のログテキストファイル名」は、ログデータの種類とエクスポートされたログデータファイルの名前を対応させて示しています。ログ名は、[監視] ページの [ログ] タブで使われているログ名と 1 対 1 で対応するものではありません。

Table 156: Symantec Endpoint Protection のログテキストファイル名

ログデータ	テキストファイル名
サーバー管理	scm_admin.log
アプリケーションとデバイス制御	agt_behavior.log
サーバークライアント	scm_agent_act.log
サーバーポリシー	scm_policy.log
サーバーシステム	scm_system.log
クライアントパケット	agt_packet.log
クライアントプロアクティブ脅威	agt_proactive.log
クライアントリスク	agt_risk.log
クライアントスキャン	agt_scan.log
クライアントセキュリティ	agt_security.log
クライアントシステム	agt_system.log
クライアントトラフィック	agt_traffic.log

NOTE

テキストファイルにエクスポートした場合、エクスポートされたレコードの数が [外部ログ記録] のダイアログボックスで設定した数と異なることがあります。この状況は管理サーバーを再起動したときに発生します。管理サーバーを再起動すると、ログエントリカウンタはゼロにリセットされますが、すでにエントリが一時ログファイルに存在する場合があります。この場合、再起動後に生成された各種類の最初の *.log ファイルには、指定した値よりも多くのエントリが含まれます。それ以降にエクスポートされたログファイルには、正しい数のエントリが含まれます。

ログデータをテキストファイルにエクスポートするには

1. コンソールで、[管理] をクリックします。
2. [サーバー] をクリックします。
3. 外部ログ記録を設定するローカルサイトまたはリモートサイトをクリックします。
4. [外部ログ記録の設定] をクリックします。
5. [全般] タブで、ログデータをファイルに送信する頻度を選択します。
6. [マスターログ記録サーバー] リストボックスで、ログを送信するサーバーを選択します。

複数の管理サーバーをデータベースに接続して Microsoft SQL を使う場合、1 台のサーバーのみをマスターログ記録サーバーにする必要があります。

7. [ログをダンプファイルにエクスポート] にチェックマークを付けます。
8. 必要に応じて、[ダンプファイルレコードを制限する] にチェックマークを付けて、一度にテキストファイルに送信するエントリの数を入力します。
9. [ログフィルタ] タブで、テキストファイルに送信するログのすべてを選択します。

ログの種類を選択したときに重大度を選択できる場合、エクスポートする重大度にチェックマークを付ける必要があります。

10. [OK] をクリックします。

外部ログ記録用フェールオーバーサーバーの設定

Symantec Endpoint Protection Manager は、syslog サーバーにログを転送するマスターログ記録サーバーとして機能します。14.3 以降、2 番目の管理サーバーを設定して、プライマリサーバーのフェールオーバーサーバーとして動作させることができます。プライマリ管理サーバーがオフラインになった場合、2 番目の管理サーバーが引き継ぎ、ログを syslog サーバーに転送します。プライマリ管理サーバーがオンラインに復帰すると、ログの転送を再開します。

外部ログ記録用フェールオーバーサーバーの設定方法

1. コンソールで、[管理] > [サーバー] をクリックして、サイトを選択し、[外部ログ記録の設定] をクリックします。
2. [全般] タブの、[マスターログ記録サーバー] ドロップダウンリストで、ログを送信するプライマリ管理サーバーを選択します。
プライマリサーバーがダウンした場合、リスト内の次の管理サーバーが引き継ぎます。管理サーバーは、[管理] > [サーバー] > [サイトプロパティの編集] > [全般] タブのレポート記録用サーバー優先度リストに表示されます。
3. [OK] をクリックします。

フェールオーバーまたは負荷分散に使う管理サーバーのインストール

通知の管理

通知は、潜在的なセキュリティ上の問題について管理者とコンピュータユーザーに警告します。

通知の種類によっては、設定するときのデフォルト値が含まれていることがあります。このガイドラインは、環境の規模に応じて、起点となる妥当な値を提供しますが、調整が必要な場合もあります。環境に適した通知の数を特定するには、試行錯誤が必要です。まず 1 つしきい値を設定して数日様子を見ます。数日後、通知の設定を調整できます。

ウイルス、セキュリティリスク、ファイアウォールイベントの検出に関して、1 つのネットワーク内に 100 台未満のコンピュータがあると仮定します。このネットワークでの開始値としては、1 分以内に 2 つのリスクイベントが検出されたときに通知を送信するように設定することが妥当です。コンピュータの数が 100 台から 1000 台の場合、1 分以内に 5 つのリスクイベントを検出する方が開始値としては有効です。

[監視] ページで通知を管理します。[ホーム] ページを使って、注意を必要とする未対応の通知の数を判断できます。

「[通知管理](#)」に、通知の管理で実行できるタスクを示します。

Table 157: 通知管理

タスク	説明
通知について学習する	通知のしくみを学習します。 通知のしくみ
電子メール通知を有効にするように電子メールサーバーが設定されていることを確認する	通知を電子メールで送信する場合は、つの Symantec Endpoint Protection Manager と電子メールサーバーを正しく設定している必要があります。 管理サーバーと電子メールサーバー間の通信の確立
事前設定された通知を確認する	Symantec Endpoint Protection に用意されている事前設定された通知を確認します。 通知の種類および通知が送信される場合
未対応の通知を表示する	未対応の通知を表示し、これに応答します。 通知の表示と対応

タスク	説明
新しい通知を設定する	必要に応じて、重要な問題について自身と自身以外の管理者に注意を促す通知を作成します。 管理者通知の設定 リモートクライアントの通知の有効化について
通知フィルタを作成する	必要に応じて、トリガされたすべての通知の表示を拡張または限定するフィルタを作成します。 管理通知フィルタの保存と削除

通知のしくみ

通知は、潜在的なセキュリティ上の問題について管理者とユーザーに警告します。たとえば、通知は、期限切れのライセンスまたはウイルスの感染について管理者に警告できます。

イベントは通知をトリガします。新しいセキュリティリスク、クライアントコンピュータでのハードウェアの変更、または試用ライセンスの期限切れで、通知をトリガできます。通知がトリガされたときに、システムによって処理が行われるように設定できます。処理には、ログへの通知の記録、バッチファイルまたは実行可能ファイルの実行、電子メールの送信などがあります。

NOTE

電子メール通知には、つの Symantec Endpoint Protection Manager と電子メールサーバーとの間の通信が正しく設定されている必要があります。

通知のダンパー期間:を設定できます。ダンパー期間は、新しいデータの通知条件を調べるまでに経過する必要がある時間を指定します。通知条件にダンパー期間がある場合、通知はこの期間内でトリガ条件が最初に起きたときにのみ発行されます。たとえば、大規模なウイルス攻撃が起き、ネットワーク上の 5 台のコンピュータにウイルスが感染するごとに電子メールを送信するように、通知条件が設定されているとします。その通知条件に対して 1 時間のダンパー期間を設定した場合、サーバーは、攻撃中、1 時間ごとに通知電子メールを 1 つずつ送信します。

NOTE

重要なイベントの通知について、[ダンパー] 期間を [なし] に設定した場合は、クライアントが重要なイベントを即座にアップロードすることを確認します。[重要なイベントをすぐにクライアントにアップロードさせる] オプションはデフォルトで有効で、[通知の設定] ダイアログボックスで設定されています。

通知の管理

管理サーバーと電子メールサーバー間の通信の確立

通知の種類および通知が送信される場合

管理者通知の設定

通知の表示と対応

通知の種類および通知が送信される場合

つの Symantec Endpoint Protection Manager は、管理者に通知を提供します。特定のニーズを満たすように、これらの通知の大部分はカスタマイズできます。たとえば、フィルタを追加して、トリガ条件を特定のコンピュータのみに限定できます。または、トリガされたときに特定の処理を行うように通知を設定できます。

デフォルトでは、これらの通知の一部が、つの Symantec Endpoint Protection Manager をインストールしたときに有効になります。デフォルトで有効になっている通知は、サーバーにログ記録し、システム管理者に電子メールを送信するように設定されています。

通知の管理

別のバージョンからのアップグレードが通知条件に与える影響

Table 158: 事前設定された通知

通知	説明
認証エラー	定義された期間内に、設定された回数ログオンに失敗すると、認証エラーの通知がトリガされます。通知をトリガするために必要なログオンエラーの数とログオンエラーが発生する期間を設定できます。
クライアントリストを変更しました	この通知は、既存のクライアントリストに変更があったときにトリガします。この通知条件はデフォルトで有効になっています。 クライアントリストの変更には次のものが含まれます。 - クライアントの追加 - クライアントの名前の変更 - クライアントの削除 - クライアントハードウェアでの変更 - クライアントの管理外検出状態での変更 - クライアントモードの変更
クライアントセキュリティ警告	この通知は、次のセキュリティイベントのいずれかが起きたときにトリガします。 - コンプライアンスイベント - ネットワークとホストのエクスポイト緩和機能のイベント - トラフィックイベント - パケットイベント - デバイス制御イベント - アプリケーション制御イベント これらの通知を変更して、これらの通知がいつトリガされるかを定める、イベントの種類、重大度、頻度を指定できます。 これらの発生の種類の中には、関連するポリシーでログ記録を有効にする必要があるものがあります。 Note: 通知のダンパー期間を [なし] に設定した場合、クライアントが重要なイベントをすぐにアップロードできることを確認する必要があります。[重要なイベントをすぐにクライアントにアップロードさせる] オプションはデフォルトで有効で、[通知の設定] ダイアログボックスで設定されています。
ディセプション検出	攻撃者がディセプタに接触したり修正しようとしたりすると、ディセプションツールがイベントをログに記録します。通知は以下のときにトリガされます。 - 攻撃者がクライアントの防御を突破する。 - 攻撃者がクライアントコンピュータについての情報を取得する。 - 攻撃者が企業ネットワーク内でのさらなる攻撃にクライアントコンピュータを使用しようとする。
最新でないダウンロード保護コンテンツ	最新ではないダウンロード保護コンテンツについて管理者に警告します。定義が通知をトリガする経過時間を指定できます。
ファイル評価ルックアップの警告	評価検査のためにファイルをシマンテック社に送信する際に管理者に警告が表示されます。SONARとダウンロードインサイトは、ファイル評価ルックアップを使用してファイルをシマンテック社に自動的に送信します。 [ファイル評価の検出] の通知は、デフォルトで有効になります。
強制アプリケーション検出	商用アプリケーションリストのアプリケーションが検出されたり、管理者によって監視されるアプリケーションリストのアプリケーションが検出されたときに、この通知がトリガされます。
IPS シグネチャが最新ではありません	最新ではない IPS シグネチャについて管理者に警告します。定義が通知をトリガする経過時間を指定できます。

通知	説明
Licensing issue	有償ライセンス期限 この通知は、管理者や、必要に応じてパートナーに、期限切れになった、または期限切れ間近の有償ライセンスについて警告します。 この通知はデフォルトで有効になっています。 過剰配備 この通知は、管理者や、必要に応じてパートナーに、過剰配備の有償ライセンスについて警告します。 この通知はデフォルトで有効になっています。 試用ライセンス期限 この通知は、期限切れになった試用ライセンスについて、および 60 日、30 日、7 日以内に期限切れになる試用ライセンスについて、管理者に警告します。 この通知は、試用ライセンスがあるとデフォルトで有効になります。ライセンスがアップグレードの対象になっているか、すでに支払われている場合、この通知はデフォルトで有効になりません。
メモリエクスポloit緩和機能検出	Windows の脆弱性攻撃が検出されると、この通知がトリガします。
ネットワークロードアラート: ウイルスとスパイウェアの完全定義の要求	完全定義セットを要求するクライアントが多すぎてネットワーク帯域幅の問題が発生する可能性がある場合は管理者に警告します。 この通知はデフォルトで有効になっています。
新しい学習済みアプリケーション	アプリケーション学習で新しいアプリケーションが検出されたときに、この通知がトリガします。
新種のリスクを検出しました	この通知は、ウイルススキャンおよびスパイウェアスキャンが新種のリスクを検出するとトリガされます。 Note: 通知のダンパー期間を [なし] に設定した場合、クライアントが重要なイベントをすぐにアップロードできることを確認する必要があります。[重要なイベントをすぐにクライアントにアップロードさせる] オプションはデフォルトで有効で、[通知の設定] ダイアログボックスで設定されています。
新しいソフトウェアパッケージ	新しいソフトウェアパッケージをダウンロードするか、または次の状況が起きた場合にこの通知がトリガします。 • LiveUpdate でクライアントパッケージがダウンロードされる。 • 管理サーバーがアップグレードされる。 • コンソールで手動でクライアントパッケージをインポートする。 • LiveUpdate に新しいセキュリティ定義やエンジンコンテンツがある。 新しいセキュリティ定義によってのみ、新しいクライアントパッケージによってのみ、またはその両方によってのみ通知がトリガされるかを指定できます。 この通知はデフォルトで有効になっています。
新しいユーザー許可ダウンロード	ダウンロードインサイトによって検出されたアプリケーションをクライアントコンピュータが許可するときに、この通知がトリガされます。管理者はこの情報を使って、アプリケーションを遮断したり許可したりするための評価に役立てます。
パワーイレイサーを推奨	通常のスキャンで感染を修復できない場合に管理者がパワーイレイサーを使用できるように管理者に警告します。 この通知はデフォルトで有効になっています。

通知	説明
リスクアウトブレイク	この通知は、セキュリティリスクアウトブレイクについて管理者に警告します。通知をトリガするために必要な新しいリスクの発生数および種類とリスクが発生する期間を設定します。発生の種類には、任意のコンピュータでの発生、単一コンピュータでの発生、個別のコンピュータでの発生などがあります。 この通知条件はデフォルトで有効になっています。 Note: 通知のダンパー期間を [なし] に設定した場合、クライアントが重要なイベントをすぐにアップロードできることを確認する必要があります。[重要なイベントをすぐにクライアントにアップロードさせる] オプションはデフォルトで有効で、[通知の設定] ダイアログボックスで設定されています。
サーバーの健全性	サーバー健全性問題は通知をトリガします。通知には、サーバー名、健全性状態、理由、最新のオンラインまたはオフライン状態が示されます。 この通知はデフォルトで有効になっています。
単一リスクイベント	この通知は、単一のリスクイベントの検出時にトリガし、リスクに関する詳細を示します。詳細には、関与するユーザーおよびコンピュータと、管理サーバーにより行われる処理が含まれます。 Note: 通知のダンパー期間を [なし] に設定した場合、クライアントが重要なイベントをすぐにアップロードできることを確認する必要があります。[重要なイベントをすぐにクライアントにアップロードさせる] オプションはデフォルトで有効で、[通知の設定] ダイアログボックスで設定されています。
SONAR 定義が最新ではありません	最新ではない SONAR 定義について管理者に警告します。定義が通知をトリガする経過時間を指定できます。
システムイベント	この通知は、特定のシステムイベントが発生したときにトリガし、このようなイベントが検出された数を示します。システムイベントは、管理サーバーの活動、複製エラー、バックアップ、システムエラーを含んでいます。
管理外コンピュータ	この通知は、管理サーバーがネットワークで管理外コンピュータを検出したときにトリガします。通知には、各管理外コンピュータの IP アドレス、MAC アドレス、オペレーティングシステムを含む詳細が示されます。
アップグレードライセンス期限	以前のバージョンの Symantec Endpoint Protection Manager から現在のバージョンへのアップグレードでは、アップグレードライセンスが与えられます。この通知は、アップグレードライセンスが期限切れ間近になったときにトリガされます。 この通知はアップグレード後のみに表示されます。
ウイルス定義が最新ではありません	最新ではないウイルス定義について管理者に警告します。定義が通知をトリガする経過時間を指定できます。 この通知はデフォルトで有効になっています。

パートナー通知について

管理サーバーは、期限切れ間近、または期限切れになった有償ライセンスがクライアントにあることを検出すると、システム管理者に通知を送信できます。同様に、管理サーバーは、ライセンスが過剰配備されていることを検出したときに、管理者に通知を送信できます。

ただし、どちらの場合でも、問題を解決するには新しいライセンスまたは更新ライセンスの購入が必要になることがあります。多くのインストールでは、サーバー管理者にはそのような購入を行う権限がない場合がありますが、代わりに、シマンテック社のパートナーに依頼してこのタスクを実行してください。

管理サーバーには、パートナーの連絡先情報を保持する機能が用意されています。この情報は、サーバーがインストールされているときに入力できます。システム管理者はまた、インストール後はいつでも、コンソールの [ライセンス] ペインで、パートナー情報を入力または編集できます。

パートナーの連絡先情報が管理サーバーで利用可能なとき、有償ライセンス関連の通知と過剰配備ライセンスの通知が管理者とパートナーの両方に自動的に送信されます。

管理サーバーと電子メールサーバー間の通信の確立

管理サーバーが自動的に電子メール通知を送信するには、管理サーバーと電子メールサーバー間の接続を設定する必要があります。

通知の管理

管理サーバーと電子メールサーバー間の通信を確立するには

1. コンソールで、[管理] をクリックし、[サーバー] をクリックします。
2. [サーバー] で、電子メールサーバーと接続を確立する管理サーバーを選択します。
3. [タスク] の下で、[サーバーのプロパティを編集する] をクリックします。
4. [サーバープロパティ] ダイアログボックスで、[電子メールサーバー] タブをクリックします。
5. 電子メールサーバー設定を入力します。

このダイアログボックスのオプション設定について詳しくは [ヘルプ] を参照してください。

6. [OK] をクリックします。

「[Endpoint Protection Manager のテスト電子メールに対して「テスト電子メールを送信できませんでした」のエラーが発生する](#)」を参照してください。

通知の表示と対応

未対応の通知を表示することも、すべての通知を表示することもできます。未対応の通知に対応できます。コンソールで現在設定されているすべての通知条件を表示できます。

[ホーム] ページの [セキュリティの状態] ペインには、過去 24 時間に起きた未対応の通知の数が表示されます。

通知の管理

1. 最近の未対応の通知を表示するには、コンソールで [ホーム] をクリックします。
2. [ホーム] ページの [セキュリティの状態] ペインで、[通知の表示] をクリックします。
最近の未対応の通知のリストが、[通知] タブに表示されます。
3. 必要に応じて、通知のリストの [レポート] 列に文書アイコンがある場合は、これをクリックします。

通知レポートが別のブラウザウィンドウに表示されます。文書アイコンがない場合は、通知のリストの [メッセージ] 列にすべての通知情報が表示されます。

4. すべての通知を表示するには、コンソールで、[監視] をクリックし、[通知] タブをクリックします。
5. 必要に応じて、[通知] タブの [保存したフィルタを使う] メニューから、保存したフィルタを選択します。

[管理通知フィルタの保存と削除](#)

-
6. 必要に応じて、[通知] タブの [時間範囲] メニューから、時間範囲を選択します。
 7. [通知] タブで、[通知の表示] をクリックします。
 8. 通知に対応するには、通知を表示します。
 9. [通知] タブの通知のリストにある [対応] 列で、赤色のアイコンをクリックして通知に対応します。
 10. 設定した通知条件をすべて表示するには、コンソールで [監視] をクリックします。
 11. [監視] ページの [通知] タブで、[通知条件] をクリックします。

コンソールで設定されたすべての通知条件が表示されます。[通知の種類を表示する] メニューから通知の種類を選択して、リストをフィルタ処理できます。

管理通知フィルタの保存と削除

フィルタを使って、コンソールでの管理通知の表示を拡張または限定できます。新しいフィルタを保存でき、以前に保存したフィルタを削除できます。

通知の表示と対応

通知の管理

次の基準を組み合わせて使う、保存済みのフィルタを作成できます。

- 時間範囲
- 対応済みの状態
- 通知の種類
- 作成者
- 通知名

たとえば、過去 24 時間に送信された未対応のリスクアウトブレイク通知のみを表示するフィルタを作成できます。

1. 通知フィルタを追加するには、コンソールで [監視] をクリックします。
2. [監視] ページの [通知] タブで、[追加設定] をクリックします。
12.1.xでは、[追加設定] ではなく [拡張設定] です。
3. [適用したいフィルタ設定は?] の見出しの下で、フィルタの基準を設定します。
4. [フィルタの保存] をクリックします。
5. [通知] タブの [フィルタ名] ボックスにフィルタ名を入力して、[OK] をクリックします。
6. 保存した通知フィルタを削除するには、コンソールで [監視] をクリックします。
7. [監視] ページの [通知] タブの [保存したフィルタを使う] メニューで、フィルタを選択します。
8. [保存したフィルタを使う] メニューの右側で、X アイコンをクリックします。
9. [フィルタの削除] ダイアログボックスで、[はい] をクリックします。

管理者通知の設定

特定の種類のイベントが行われるときに、自身および他の管理者に警告するように通知を設定できます。また、重要なタスクを実行するように注意を促すための通知をトリガする条件も追加できます。たとえば、ライセンスが期限切れになったり、セキュリティリスクが検出されたときに知らせる通知条件を追加できます。

トリガされた通知は、次のような特定の処理を実行できます。

-
- データベースに通知をログ記録する
 - 1人以上の個人に電子メールを送信する
 - バッチファイルを実行する

NOTE

電子メール通知を送信するには、管理サーバーと通信するようにメールサーバーを設定する必要があります。

管理サーバーと電子メールサーバー間の通信の確立

利用可能な通知の種類のリストから通知条件を選択します。

通知の種類を選択した後、次のように設定します。

- フィルタを指定します。
すべての種類の通知でフィルタが用意されているわけではありません。フィルタが用意されている場合は、そのフィルタを使って通知をトリガする条件を限定できます。たとえば、特定のグループのコンピュータが影響される場合にのみトリガするように、通知を制限できます。
- 設定を指定します。
すべての種類の通知で設定が用意されていますが、具体的な設定は種類ごとに異なります。たとえば、リスクの通知では、通知をトリガするスキャンの種類を指定できます。
- 処理を指定します。
すべての種類の通知で、指定できる処理が用意されています。

NOTE

重要なイベントの通知について、[ダンパー] 期間を [なし] に設定した場合は、クライアントが重要なイベントを即座にアップロードすることを確認します。関連通知には、クライアントセキュリティ警告、単一リスクイベント、新しいリスクを検出しました、リスクアウトブレイクが含まれます。[重要なイベントをすぐにクライアントにアップロードさせる] オプションはデフォルトで有効で、[通知の設定] ダイアログボックスで設定されています。

管理者通知を設定するには

1. コンソールで、[監視] をクリックします。
2. [監視] ページの [通知] タブで、[通知条件] をクリックします。
3. [通知] タブで、[追加] をクリックして、通知の種類をクリックします。
4. [通知条件の追加] ダイアログボックスで、次の情報を入力します。
 - [通知名] テキストボックスで、通知条件に付ける名前を入力します。
 - [適用したいフィルタ設定は?] が表示されている場合、この下で通知条件のフィルタ設定を指定します。
 - [この通知に適用したい設定は?] の下で、通知をトリガする条件を指定します。
 - [この通知がトリガされたときに実行したい処理は?] の下で、通知がトリガされるときに行われる処理を指定します。
5. [OK] をクリックします。

通知の管理

通知の表示と対応

別のバージョンからのアップグレードが通知条件に与える影響

Symantec Endpoint Protection が新しいサーバーにインストールされるときには、事前設定済みの通知条件の多くがデフォルトで有効になります。しかし以前のバージョンから Symantec Endpoint Protection へのアップグレードは、デフォルトでどの通知条件が有効になるかに影響を与える場合があります。また、デフォルトの設定に影響することがあります。

Symantec Endpoint Protection の新規インストールでは、次の通知条件がデフォルトで有効になります。

- クライアントリストを変更しました
- 新しいクライアントソフトウェア
- 配備過剰の問題
- 有償ライセンスの問題
- リスクアウトブレイク
- サーバーの健全性
- 体験版ライセンス期限
- ウイルス定義が最新ではありません

管理者が以前のバージョンからソフトウェアをアップグレードするときには、以前のバージョンで使われていた既存の通知条件はすべて保持されます。ただし、[新しいソフトウェアパッケージ]通知条件は[新しいクライアントソフトウェア]通知条件になります。[新しいクライアントソフトウェア]の条件には、[新しいソフトウェアパッケージ]の条件には存在しない設定が2つあります。[クライアントパッケージ]と[セキュリティ定義]です。ソフトウェアがアップグレードされると、アップグレードを経ても保存されるこの種類の通知条件では、これらの設定はどちらも有効になります。ただし、アップグレード後に作成される条件の[新しいクライアントソフトウェア]通知では、デフォルトで[クライアントパッケージ]設定が有効になり、[セキュリティ定義]設定が無効になります。

NOTE

[新しいクライアントソフトウェア]通知条件で[セキュリティ定義]設定が有効になっている場合、多量の通知が送信される可能性があります。この状況は、多くのクライアントが存在する場合や、セキュリティ定義の更新が高頻度でスケジュール設定されている場合に起きることがあります。セキュリティ定義の更新についての通知を頻繁に受信したくない場合は、通知条件を編集して[セキュリティ定義]設定を無効にできます。

いくつかの通知条件には、以前のバージョンにはなかった[システム管理者に電子メールを送信]という新しい設定が付与されることがあります。通知条件にこの設定が新しく付与される場合、その種類の既存の条件すべてについて、アップグレード後の設定はデフォルトでは無効になります。

以前のインストールでデフォルトの種類の通知条件が追加されていない場合、その通知条件は、アップグレードされるインストールで追加されます。ただし、管理者によって以前のインストール時に意図的に削除されたデフォルトの通知条件を、アップグレード処理で特定することはできません。そのため1つの例外を除いて、[システム管理者に電子メールを送信]、[通知をログに記録する]、[バッチファイルを実行]、[電子メールの送信先]の処理の設定はすべて、アップグレードされたインストールのデフォルトの各通知条件で無効にされます。これらの4つの処理がすべて無効になっている場合、条件自体は存在していますが通知条件は処理されません。管理者は通知条件を編集し、これらの設定の一部またはすべてを有効にできます。

[新しいクライアントソフトウェア]通知条件は例外で、アップグレード処理中に追加された場合はデフォルトで通知を生成できることに注意してください。他のデフォルトの通知条件とは異なり、[通知をログに記録する]と[システム管理者に電子メールを送信]の処理設定はどちらも、この条件では有効にされます。

以前のバージョンのソフトウェアがライセンスをサポートしていない場合、[アップグレードライセンス期限]通知条件は有効にされます。

いくつかの種類の通知条件は、以前のバージョンのソフトウェアでは利用できません。それらの通知条件は、ソフトウェアがアップグレードされるときにデフォルトで有効にされます。

[通知の種類および通知が送信される場合](#)

管理サーバー、サイト、およびデータベースの管理

クライアント/サーバー通信、ディザスタリカバリの実行、および複製、サイト、フェールオーバーについてこのセクションを使用して、以下を行います。

- 管理サーバーとクライアント間の接続を設定する。
- 管理サーバーと証明書を設定する。
- データベースを管理する。
- フェールオーバーと負荷分散を設定する。
- サイトと複製を管理する。
- ディザスタリカバリを実行する。

Symantec Endpoint Protection サーバーの種類について

サーバーを管理するときには、次の定義を理解しておく役立ちます。

- **サイト**
サイトは、通常は同じ事業場所に一緒に配置される 1 つ以上の管理サーバーと 1 つのデータベースから成ります。ログオン先のサイトはローカルサイトです。ローカルサイトは直接修正できます。ローカルサイト以外のすべてのサイトはリモートサイトと呼ばれます。レプリケーションを使ってサイトに接続します。
[サイトと複製の設定](#)
- **管理サーバー**
つの Symantec Endpoint Protection Manager ソフトウェアがインストールされているコンピュータ。管理サーバーで、ポリシーを作成して異なる組織グループに割り当てることができます。クライアントを監視し、レポート、ログ、警告を表示し、サーバーと管理者アカウントを設定できます。単一サイトで管理サーバーを複数使い、フェールオーバーと負荷分散の機能を提供します。
[フェールオーバーと負荷分散の設定](#)
- **[データベースサーバー]**
つの Symantec Endpoint Protection Manager によって使われるデータベース。1 つのサイトあたり 1 つのデータベース (Microsoft SQL Server Express または Microsoft SQL Server のいずれか) があります。データベースは管理サーバーと同じコンピュータに配置できます。SQL Server データベースを使う場合は、異なるコンピュータに配置できません。14.3 RU1 で、埋め込みデータベースが SQL Server Express に置き換えられました。
[データベースの保守](#)
- **複製パートナー**
サイトの間のデータ複製を可能にするため、2 つのサイト間に作成される関係。
[サイトと複製の設定](#)

サーバーの設定のエクスポートとインポート

サーバープロパティファイルには、つの Symantec Endpoint Protection Manager 用のサーバー設定が含まれています。次の場合に、サーバープロパティファイルのエクスポートとインポートを行う必要があります。

- つの Symantec Endpoint Protection Manager を再インストールするためディザスタリカバリファイルを使います。ディザスタリカバリファイルには、サーバー設定が含まれていません。つの Symantec Endpoint Protection Manager を再インストールすると、前に変更したデフォルトのサーバー設定はすべて失われます。エクスポートされたサーバープロパティファイルを使って、変更後のサーバー設定を再度インポートできます。
- つの Symantec Endpoint Protection Manager をテスト環境でインストールし、後で管理サーバーを実働環境でインストールします。エクスポートされたサーバープロパティファイルを実働環境にインポートできます。

つの Symantec Endpoint Protection Manager サーバーとサードパーティサーバーの管理

1. サーバー設定をエクスポートするには、コンソールで [管理] をクリックし、[サーバー] をクリックします。
2. [サーバー] で、[ローカルサイト (サイト **site_name**)] を展開してエクスポートする管理サーバーを選択します。
3. [サーバードプロパティのエクスポート] をクリックします。
4. ファイルを保存する場所を選択し、ファイル名を指定します。
5. [エクスポート] をクリックします。
6. サーバー設定をインポートするには、コンソールで [管理] をクリックし、[サーバー] をクリックします。
7. [サーバー] で、[ローカルサイト (サイト **site_name**)] を展開して設定をインポートする管理サーバーを選択します。
8. [サーバードプロパティのインポート] をクリックします。
9. インポートするファイルを選択して、[インポート] をクリックします。
10. [はい] をクリックします。

つの Symantec Endpoint Protection Manager サーバーとサードパーティサーバーの管理

ネットワーク環境で多くの異なる種類のサーバーを統合するように つの Symantec Endpoint Protection Manager を設定できます。

Table 159: サーバー管理

タスク	説明
サーバーについて学習する	設定が必要なサーバーの種類を決定します。 Symantec Endpoint Protection サーバーの種類について
サーバー通信パーミッションを設定する	リモートコンソールへのアクセスを許可または拒否できます。アクセスを管理するには、単一コンピュータまたはコンピュータグループの IP アドレスに基づく例外を追加します。 リモート つの Symantec Endpoint Protection Manager コンソールのアクセスの認可または遮断
サーバー設定を修正する	データベース設定を修正したり、別のコンピュータ上にデータベースを復元したりするために、サーバー設定を修正できます。 つの Symantec Endpoint Protection Manager の再インストールまたは再設定
メールサーバーを設定する	ネットワーク内の特定のメールサーバーを操作するには、メールサーバーを設定する必要があります。 管理サーバーと電子メールサーバー間の通信の確立
ディレクトリサーバーを管理する	管理者アカウントを管理したり、組織単位を作成したりするために、Symantec Endpoint Protection をディレクトリサーバーと統合できます。 ディレクトリサーバーへの つの Symantec Endpoint Protection Manager の接続
プロキシサーバーを使って Symantec LiveUpdate server に接続する場合はプロキシの設定を指定する	プロキシサーバー経由でインターネットに接続するために つの Symantec Endpoint Protection Manager を設定するには、プロキシサーバー接続を設定する必要があります。 インターネットにアクセスして Symantec LiveUpdate からコンテンツをダウンロードするためにプロキシサーバーに接続する つの Symantec Endpoint Protection Manager の設定
サーバーのプロパティをインポートまたはエクスポートする	サーバーの設定を xml ファイルにエクスポートし、同じ設定を再インポートできます。 サーバーの設定のエクスポートとインポート

タスク	説明
サーバー証明書を管理する	つの Symantec Endpoint Protection Manager サーバーでは、ネットワーク上のすべてのサーバーとクライアントの間の通信のデータを暗号化するために、サーバー証明書を使います。サーバーはサーバー証明書を使って自身の識別と認証を行います。新しいサーバー証明書をバックアップ、更新、または生成する必要がある場合もあります。 サーバー証明書について サーバー証明書の更新または復元 サーバー証明書のバックアップ 新しいサーバー証明書の生成
サーバーの SecuriID 認証を設定する	RSA SecuriID を使用して管理者アカウントを認証するように選択する場合、管理サーバーを RSA サーバーと通信するように設定する必要もあります。 つの Symantec Endpoint Protection Manager での RSA SecuriID 認証の使用
Symantec VIP を使用して つの Symantec Endpoint Protection Manager の 2 要素認証を設定します。	2 要素認証の環境内で Symantec VIP を使用する場合は、それをつの Symantec Endpoint Protection Manager 認証で認証する管理者に対して有効にできます。 このサポートはバージョン 14.2 で追加されます。 Symantec VIP を使用した 2 要素認証の設定
別のコンピュータにサーバーを移動する	次の理由で、あるコンピュータから別のコンピュータに管理サーバーソフトウェアを移動することが必要になる場合があります。 - テスト環境から実働環境に管理サーバーを移動する必要がある。 - 管理サーバーが動作するコンピュータにハードウェア障害がある。 次の方法で管理サーバーソフトウェアを移動できます。 - 別のコンピュータに管理サーバーをインストールし、レプリケーションを実行する。 複製のための 2 番目のサイトのインストール方法 - リカバリファイルを使って別のコンピュータに管理サーバーをインストールする。 つの Symantec Endpoint Protection Manager の再インストールまたは再設定
管理サーバーを開始または終了する	管理サーバーは自動サービスとして実行されます。アップグレードしたり、ディザスタリカバリを実行したりする場合は、管理サーバーサービスを停止する必要があります。 管理サーバーサービスの停止と開始

データベースの保守

Symantec Endpoint Protection (SEPM) では、Microsoft SQL Server Express データベースと Microsoft SQL Server データベースの両方をサポートしています。5,000 台を超えるクライアントがある場合は、Microsoft SQL Server データベースを使用してください。

つの Symantec Endpoint Protection Manager では、Microsoft SQL Server Express データベースが自動的にインストールされます。また、SQL Server Express を個別にインストールすることもできます。データベースには、セキュリティポリシー、設定、攻撃データ、ログ、レポートの情報が含まれています。14.3 RU1 で、埋め込みデータベースが SQL Server Express に置き換えられました。

つの Symantec Endpoint Protection Manager をインストールした後、数週間または数カ月経過すると管理サーバーの速度が低下し始めることがあります。管理サーバーのパフォーマンスを改善するには、データベースのストレージ領域を減らし、各種データベース保守タスクをスケジュール設定する必要があります。

Table 160: データベース管理タスク

タスク	説明
通常のデータベースバックアップのスケジュール設定	データベースが破損した場合に備えて、通常のデータベースバックアップをスケジュール設定する必要があります。 データベースとログのバックアップ データベースの自動バックアップのスケジュール設定 Endpoint Protection のディザスタリカバリのベストプラクティス 省略可能なオプションとして、バックアップが行われるまでデータベースの自動スナップショットが行われないようにするために、手動でデータベースからデータをスナップショットできます。 データベースからのログデータの手動の消去
データベース保守タスクのスケジュール設定	データベース保守タスクをスケジュール設定することにより、管理サーバーとデータベースの間でやり取りする時間を高速化できます。次の保守タスクをすぐに実行したり、ユーザーがクライアントコンピュータを使っていないときに実行したりするために管理サーバーをスケジュール設定できます。 - トランザクションログから未使用のデータを削除する。 - データベーステーブルインデックスを再構築して、データベースのソートと検索の機能を改善する。 自動データベース保守タスクのスケジュール設定
データベースファイルサイズの定期調査	データベースが最大ファイルサイズに達していないことを確認します。Microsoft SQL Server Express データベースには、10 GB のサイズ制限があります。SEPM をインストールするときに SQL Server Express をインストールする場合、この制限に近いと SEPM によって警告が表示されます。 Microsoft SQL Server データベースのファイルサイズの拡大
必要なデータベースのストレージ領域の計算	ストレージ領域を減らす方法を決定する前に、必要な総ディスク容量を計算します。データベースのストレージは次の要因に基づいて決まります。 - ログサイズと有効期限 - クライアントコンピュータの台数 - 月あたり平均ウイルス数 - 各ログに保持する必要があるイベント数 - コンテンツ更新の数。 コンテンツ更新ごとに約 300 MB が必要になります。 LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す - 各言語に保持する必要があるクライアントバージョンの数 たとえば、32 ビットクライアントと 64 ビットのクライアントの両方がある場合、言語バージョンの数の 2 倍の数が必要になります。 - 保存する必要があるバックアップ数 バックアップサイズはデータベースの約 75 パーセントです。保存するバックアップコピー数を乗じて算出します。 必要なハードディスク容量を計算する方法について詳しくは、シマンテック社のホワイトペーパー「Symantec Endpoint Protection のサイジングおよび拡張性のベストプラクティスのホワイトペーパー」を参照してください。

タスク	説明
ログデータの量の削減	データベースは、絶えずエントリのフローを受け取り、そのログファイルに記録します。データベースに格納されているデータが、利用可能なディスク領域を使い果たさないように、データを管理する必要があります。データが多すぎると、データベースを実行しているコンピュータがクラッシュする原因となります。 次のタスクを実行することによって、ログデータの量を減らすことができます。 - サーバーにクライアントログの一部のみをアップロードし、クライアントログをアップロードする頻度を変更する。 クライアントログサイズと管理サーバーにアップロードするログの指定 - クライアントコンピュータがデータベースに保持できるログエントリの数とそれらを保持する期間を指定する。 ログサイズとデータベース内のログエントリの保存期間の指定 - サーバーに転送されるデータ量が減るように、重要度の低いリスクイベントとシステムイベントをフィルタで除外する。 Windows コンピュータのログ処理と通知設定の修正 - ログデータがデータベースに挿入される前にログデータが格納されるディレクトリ領域の量を減らす。 クライアントログデータ用にサーバーのディスク領域を拡大することについて - 各管理サーバーが管理するクライアントの数を減らす。 負荷分散のための管理サーバーリストの設定 - クライアントログをサーバーにアップロードする頻度をコントロールするハートビートの頻度を減らす。 プッシュモードまたはプルモードを使用した、クライアントのポリシーとコンテンツの更新
別のサーバーへのログデータのエクスポート	セキュリティのため、ログ記録の数を長期間維持することが必要な場合があります。クライアントログデータの量を少なく維持するために、ログデータを別のサーバーにエクスポートできます。1 台のサーバーがダウンした場合にログデータを受信するように、複数の管理サーバーを設定できます。 ログデータの Syslog サーバーへのエクスポート ログデータのテキストファイルへのエクスポート
必要な保護のみを備えるクライアントインストールパッケージの作成	クライアントにインストールする保護機能を多くするほど、データベース内でクライアント情報が占める領域が増加します。クライアントコンピュータで必要となる適切な保護レベルのみを備えるクライアントインストールパッケージを作成します。追加するグループを多くするほど、データベース内でクライアント情報が占める領域が増加します。 クライアントにインストールするセキュリティ機能の選択
GUP を使ったコンテンツのダウンロード	狭帯域幅の場合、または 100 以上のクライアントコンピュータがある場合は、グループ更新プロバイダを使ってコンテンツをダウンロードします。たとえば、2,000 クライアントで GUP を使うと、4 台から 5 台の管理サーバーを使ってコンテンツをダウンロードするのと同等になります。 クライアントにコンテンツを配布するための GUP の使用 ディスク容量とデータベースサイズを減らすため、サーバーで保存されるコンテンツのリビジョン数を減らすことができます。 LiveUpdate から つの Symantec Endpoint Protection Manager へのコンテンツのダウンロード
データベースの復元	壊れたデータベースを復元するには、そのデータベースがインストールされていた元のコンピュータにデータベースを復元します。また、そのデータベースを別のコンピュータにインストールできます。 データベースの復元

データベースとの接続の検証

データベースの情報は、テーブル (データベーススキーマとも呼ばれる) に格納されます。カスタマイズレポートのクエリを記述するためのスキーマが必要になる場合があります。詳しくは、次を参照してください。

Symantec Endpoint Protection Manager データベーススキーマリファレンス

データベースの自動バックアップの実行

ネットワークにログオンするユーザーが少ない時間に、データベースのバックアップが行われるようにスケジュール設定できます。

さらに、いつでもデータベースをバックアップできます。

データベースとログのバックアップ

1. コンソールで、[管理] > [サーバー] の順に選択します。
2. [サーバー] で、[ローカルサイト (マイサイト)] > [SQLEXPRESSSYMC] をクリックします。
3. [タスク] の下で、[データベースプロパティの編集] をクリックします。
4. [データベースのプロパティ] ダイアログボックスの [バックアップの設定] タブで、次のタスクを実行します。
 - [バックアップサーバー] ドロップダウンリストで、バックアップを保存する管理サーバーを指定します。
 - セキュリティ目的や会社のポリシーのために、ログのコピーを保存する必要がある場合は、[ログのバックアップ] にチェックマークを付けます。
必要がなければ、ログは大量のディスク領域を使用するため、このオプションを無効のままにしておいてください。
 - 会社のポリシーで必要な場合、[保存するバックアップの世代数] を設定します。デフォルトデータベースを使用しており、データベースのサイズが大きすぎる場合は、この値を小さくしておきます。
5. [バックアップのスケジュール] にチェックマークが付けられていることを確認し、スケジュールを設定します。
6. [OK] をクリックします。

自動データベース保守タスクのスケジュール設定

管理サーバーをインストール後、データベース内の領域は増加し続けます。数週間または数カ月経過すると管理サーバーの速度が低下します。データベースのサイズを減らし、データベースの応答時間を改善するために、管理サーバーは次のデータベース保守タスクを実行します。

- トランザクションログを切り捨てる
データベース内で変更が行われるたびに、トランザクションログが記録されます。管理サーバーは、トランザクションログから未使用のデータを削除します。
- インデックスを再構築する
管理サーバーは、データベースのソートと検索にかかる時間を改善するためにデータベーステーブルのインデックスの断片化を解消します。

デフォルトで、管理サーバーはこれらのタスクをスケジュールに従って実行します。保守タスクをすぐに実行したり、ユーザーがコンピュータを使っていないときに実行するようスケジュールを調整したりできます。

NOTE

Microsoft SQL Server Management Studio でデータベース保守タスクを実行することもできます。ただし、これらのタスクは つの Symantec Endpoint Protection Manager または Management Studio のいずれかで実行し、両方では実行しないでください。

1. データベース保守タスクをオンデマンドで実行するには、コンソールで [管理] > [サーバー] をクリックします。
2. [サーバー] で、データベースを表すアイコンをクリックします。
3. [タスク] で、次のオプションのいずれかを選択します。
 - [今すぐにトランザクションログを切り捨てる]
 - [今すぐにインデックスを再構築]

-
4. [実行] をクリックします。
 5. タスクが完了したら、[OK] をクリックします。
 6. データベース保守タスクを自動的に実行するようにスケジュール設定するには、コンソールで [管理] > [サーバー] をクリックします。
 7. [サーバー] で、データベースを表すアイコンをクリックします。
 8. [タスク] の下で、[データベースプロパティの編集] をクリックします。
 9. [全般] タブで、次のオプションのいずれかまたは両方にチェックマークを付けて、[タスクのスケジュール] をクリックし、各タスクのスケジュールを指定します。
 - [データベーストランザクションログを切り捨てる]。このタスクのデフォルトのスケジュールは 4 時間ごとです。
 - [インデックスの再構築]。このタスクのデフォルトのスケジュールは毎週日曜日の午前 2 時です。

WARNING

これらのタスクを SQL Server Management Studio で実行する場合は、これらのオプションのチェックマークをはずしてください。

データベースの自動バックアップのスケジュール設定

Microsoft SQL Server データベースのファイルサイズの拡大

SQL Server データベースを使用している場合は、データベースのサイズを定期的に調べて、データベースが最大サイズに達していないことを確認します。可能な場合は、SQL Server データベースが保持する最大サイズを増やします。

自動データベース保守タスクのスケジュール設定

Microsoft SQL Server データベースのファイルサイズを拡大するには

1. Microsoft SQL サーバーコンピュータで、SQL Server Management Studio を開きます。
2. オブジェクトエクスプローラで、「Databases」フォルダを展開し、**sem5** を右クリックして [プロパティ] をクリックします。
3. [データベースのプロパティ] ダイアログボックスで、[ファイル] を選択します。
4. [データベースファイル] で **sem5_log1** を選択し、右にスクロールして [自動拡張] 列を表示します。
5. [自動拡張] 列で、[...] ボタンをクリックします。
6. [**sem5_log1** の自動拡張を変更] ダイアログボックスで、[ファイルを無制限に拡張] をクリックし、[OK] をクリックします。
7. [OK] をクリックします。

クライアントログサイズと管理サーバーにアップロードするログの指定

企業ポリシーでは、データベースで保存するログイベントの時間と種類を増やす必要がある場合があります。維持されるログエントリの数と、各エントリがクライアント上で維持される日数を指定できます。

各種類のクライアントログをサーバーにアップロードするかどうかを設定できます。最大アップロードサイズを設定することもできます。クライアントログをアップロードしないように選択した場合は次のタスクを実行できません。

- [監視] ページの [ログ] タブを使って、つの Symantec Endpoint Protection Manager コンソールからクライアントログデータを表示できない
- データベースをバックアップするときにクライアントログをバックアップできない
- クライアントログデータをファイルや集中ログサーバーにエクスポートできない

NOTE

クライアントログ設定にはグループ固有のものやウイルス対策とスパイウェア対策ポリシーで設定するものがあり、これらは場所に適用できます。すべてのリモートクライアントログとオフィスのクライアントログ設定を変える必要がある場合、リモートクライアントを管理するために、場所ではなく、グループを使う必要があります。

ログサイズとデータベース内でのログエントリの保存期間の指定

クライアントログサイズと管理サーバーにアップロードするログを指定するには

1. コンソールで、[クライアント] をクリックし、グループを選択します。
2. [ポリシー] タブで、[クライアントログ] をクリックします。
3. [グループ名のクライアントログの設定] ダイアログボックスで、最大ファイルサイズと、ログエントリを維持する日数を設定します。
4. クライアントからサーバーに転送するすべてのログに対して [管理サーバーにアップロードする] にチェックマークを付けます。
5. セキュリティログとトラフィックログについては、ダンパー期間とダンパーアイドル期間を設定します。
6. [OK] をクリックします。

ログサイズとデータベース内でのログエントリの保存期間の指定

ハードディスク容量の制御のため、データベースで保存するログエントリ数を減らすことができます。また、エントリが保持される日数も設定できます。

NOTE

つの Symantec Endpoint Protection Manager コンソールの [監視] ページの [ログ] タブには、論理的なグループ単位でログ情報が表示されます。サイトのプロパティの [ログの設定] タブは、[監視] ページの [ログ] タブのログの種類ではなく、ログの内容に対応します。

クライアントログサイズと管理サーバーにアップロードするログの指定

ログサイズとデータベース内でのログエントリの保存期間を指定するには

1. コンソールで、[管理] をクリックします。
2. [サーバー] で、[ローカルサイト] を展開してデータベースをクリックします。
3. [タスク] の下で、[データベースプロパティの編集] をクリックします。
4. [ログの設定] タブで、エントリの数と、それぞれの種類のログエントリを保持する日数を設定します。
5. [OK] をクリックします。

クライアントログデータ用にサーバーのディスク領域を拡大することについて

大量のクライアントログデータをサーバーに頻繁にアップロードする設定では、サーバー上でディスク領域の問題が発生するおそれがあります。大量のクライアントログデータをアップロードする必要がある場合は、デフォルト値を調整して、これらの領域上の問題を避けることが必要になります。クライアントを配備するとき、サーバー上のログ格納ディレクトリの領域を監視し、必要に応じてこれらの値を調整する必要があります。

ログが .dat ファイルに変換され、データベースに書き込まれるデフォルトのディレクトリは次のデフォルトの場所にあります。

C:\Program Files (x86)\Symantec\## Symantec Endpoint Protection Manager\data\inbox\log。

サーバー上で使用可能な領域をコントロールする値を調整するには、Windows レジストリ内でこれらの値を変更する必要があります。変更が必要な Windows レジストリキーは、サーバーの HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM にあります。

「[ログアップロード設定が含まれる Windows レジストリキー](#)」に、Windows レジストリキーとそのデフォルト値、説明を示します。

Table 161: ログアップロード設定が含まれる Windows レジストリキー

値名	説明
MaxInboxSpace	ログファイルがデータベースに格納される前に .dat ファイルに変換されるディレクトリに割り当てられた領域を指定します。 デフォルト値は 8 GB です。
MinDataFreeSpace	このディレクトリ内で必要な空き領域の最低量を指定します。このキーは、同じディレクトリを使う他のアプリケーションに対して、パフォーマンスに悪影響をおよぼさずに動作するのに十分な領域を保証するのに便利です。 デフォルト値は 200 MB です。
IntervalOfInboxSpaceChecking	ログデータ用に使用可能な受信ボックス内の領域の量を確認するときの管理サーバーの待ち時間を指定します。 デフォルト値は 30 秒です。

データベースの保守

データベースからのログデータの手動の消去

この方法を定期的なデータベース保守の一部として使う場合は、データベースのバックアップ後に手動のログスイープを実行できます。

自動的なスイープの実行を許可する場合、データベースのバックアップを頻繁に行わないと、一部のデータが失われる可能性があります。データベースのバックアップを実行した後で手動ログスイープを定期的に行うと、すべてのログデータが確実に保持されます。この手順は、1 年など、比較的長い期間ログを保持する必要がある場合に非常に便利です。ログは手動で消去できますが、この手順はオプションであり実行する必要はありません。

データベースとログのバックアップ

ログサイズとデータベース内でのログエントリの保存期間の指定

データベースからログデータを手動で消去するには

1. バックアップを行うまでデータベースの自動スイープを禁止するには、サイトのログサイズを最大値に増やします。
2. 必要に応じてバックアップを実行します。
3. マネージャがインストールされているコンピュータで、Web ブラウザを開き、次の URL を入力します。

`https://localhost:8443/servlet/ConsoleServlet?ActionType=ConfigServer&action=SweepLogs`

このタスクを実行した後、すべての種類のログのログエントリが、代替データベーステーブルに格納されます。元のテーブルは、次のスイープを開始するまで保持されます。

4. 最新のエントリ以外のすべてのエントリを空にするには、再度スイープを実行します。元のテーブルがクリアされ、エントリが再度そのテーブルに格納され始めます。
5. [サイトのプロパティ] ダイアログボックスの [ログの設定] タブの設定を目的の設定に戻します。

フェールオーバーと負荷分散の設定

クライアントコンピュータは、セキュリティポリシーをダウンロードしたり、ログイベントを受信したりするために、常に管理サーバーに接続可能である必要があります。管理サーバーが利用不能になったときに Symantec Endpoint Protection Manager との通信を維持するには、フェールオーバーを設定する必要があります。管理サーバーリストを使用してクライアント管理を複数の管理サーバー間で分散するには、負荷分散を使用します。

以下の表に、フェールオーバーと負荷分散を設定するために実行する必要があるタスクの一覧を示します。

Table 162: フェールオーバーと負荷分散を設定するための処理

タスク	説明
フェールオーバーと負荷分散のしくみを理解します。	フェールオーバーと負荷分散用に管理サーバーを設定する必要があるかどうか、また、必要があるのはいつかを理解する必要があります。 フェールオーバーと負荷分散について
追加の管理サーバーをインストールします。	フェールオーバーまたは負荷分散に使う管理サーバーのインストール 各管理サーバーのクライアントの数はログサイズなどのいくつかの要因によって異なります。 必要な管理サーバーの数を計算するには、以下を参照してください。 Symantec Endpoint Protection のサイジングおよび拡張性のベストプラクティスのホワイトペーパー
管理サーバーリストに管理サーバーを追加します。	負荷分散を設定するには、複数の管理サーバーを管理サーバーリストに追加します。デフォルトの管理サーバーリストを使うか、または管理サーバーを新しい管理サーバーリストに追加することができます。管理サーバーリストには、クライアントが接続できる管理サーバーの IP アドレスまたはホスト名が含まれています。 負荷分散のための管理サーバーリストの設定
グループにカスタム管理サーバーリストを割り当てます。	カスタム管理サーバーリストを作成した後、グループに管理サーバーリストを割り当てる必要があります。 グループと場所への管理サーバーリストの割り当て

サイトと複製の設定

管理サーバーがオフラインになる場合や、クライアントと管理サーバーが通信を行わない場合は、その問題を解決する必要があります。

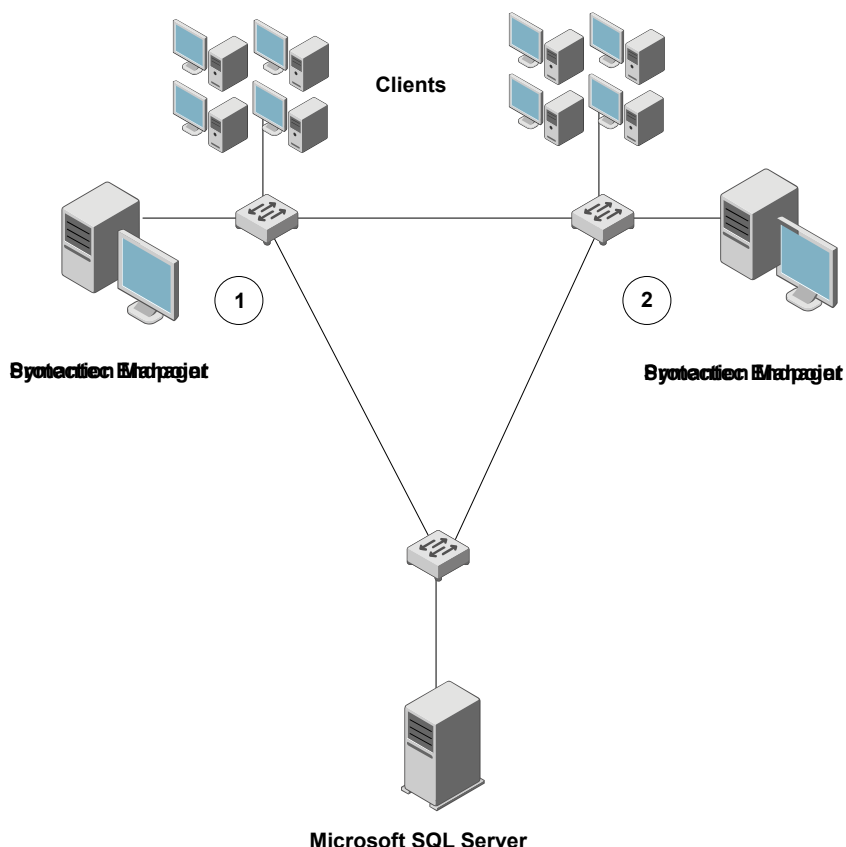
[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

フェールオーバーと負荷分散について

1 つのデータベースと通信する 2 つ以上の管理サーバーをインストールして、フェールオーバーまたは負荷分散用に設定できます。

負荷分散はグループに割り当てられている管理サーバーの優先度順のリストに基づいて発生します。サイトに少なくとも 2 つの管理サーバーを追加して、それらの間の負荷を自動的に分散することをお勧めします。インストールする管理サーバーの数は、個々の管理サーバーの障害からクライアントを保護するために必要な数より多くてもかまいません。カスタム管理サーバーリストでは、すべてのサーバーが特定の優先度レベルに割り当てられています。ネットワークに接続するクライアントは、ランダムに接続するために優先度 1 のサーバーを選択します。最初に試みたサーバーが利用不能であり、リストにその他の優先度 1 のサーバーがある場合は、ランダムに別のサーバーへの接続が試みられます。優先度 1 のサーバーが利用可能でない場合、クライアントはリストの優先度 2 のサーバーのいずれかへの接続を試みます。このようなクライアント接続をランダムに分散することによって、管理サーバー間にクライアントの負荷が分散されます。

以下の図に、異なるサブネットのコンポーネントを示します。管理サーバーとデータベースサーバーは同じサブネット上にある場合もあります。サーバーを番号 1 と 2 で識別しており、フェールオーバー構成であることを示しています。



フェールオーバー設定では、すべてのクライアントはサーバー 1 に対してトラフィックを送受信します。サーバー 1 がオフラインになった場合は、サーバー 1 がオンラインに戻るまで、すべてのクライアントはサーバー 2 に対してトラフィックを送受信します。図のデータベースはリモートインストールになっていますが、この Symantec Endpoint Protection Manager を実行するコンピュータにインストールしてもかまいません。

ローカルサーバーを使う予定の場合は、コンテンツ更新のフェールオーバーも検討することができます。LiveUpdate を実行するすべてのコンポーネントは、更新元の優先度付けされたリストも使えます。管理サーバーは、ローカル LiveUpdate サーバーを使い、他の物理的な場所の LiveUpdate サーバーにフェールオーバーできます。

NOTE

社内 LiveUpdate サーバー、GUP (Group Update Provider)、サイトの複製を使っても、負荷分散機能は得られません。負荷分散を目的として複数のサイトを設定しないでください。

NOTE

14.3 MPx 以前では、Microsoft SQL Server データベースのみを使用している場合、フェールオーバーと負荷分散を設定できます。複製を使うときだけ埋め込みデータベースとのフェールオーバーを設定できます。埋め込みデータベースを使って複製を行うとデータの不整合や欠如が起きることがあるため、負荷分散を設定しないことを推奨します。

フェールオーバーと負荷分散の設定

負荷分散のための管理サーバーリストの設定

必要なサイト数の決定

サイトと複製の設定

負荷分散のための管理サーバーリストの設定

デフォルトでは、管理サーバーにはフェールオーバーと負荷分散に対して設定されたときと同じ優先度が割り当てられます。インストールの後にデフォルトプライオリティを変更する場合は、つの Symantec Endpoint Protection Manager コンソールを使って行うことができます。サイトが複数の管理サーバーを含んでいるときのみ負荷分散を設定できます。

負荷分散は、管理サーバーリストで優先度 1 に割り当てられているサーバー間で発生します。複数のサーバーが優先度 1 に割り当てられている場合、クライアントはいずれかのサーバーをランダムに選択して通信を確立します。優先度 1 のすべてのサーバーで障害が発生した場合、クライアントは優先度 2 に割り当てられているサーバーと通信します。

負荷分散とローミングの両方を提供するには

- DNS を有効にし、カスタム管理サーバーリストに唯一のエントリとしてドメイン名を入力します。
- Symantec Endpoint Protection ネットワーク検出機能を有効にし、各場所のカスタム管理サーバーリストを使います。それぞれのサイトに対して少なくとも 1 つの場所を作成します。
- フェールオーバーまたは負荷分散を備えたハードウェアデバイスを使います。これらのデバイスの多くは、ローミングのセットアップも用意しています。

フェールオーバーと負荷分散について

負荷分散のために管理サーバーリストを設定するには

1. コンソールで、[ポリシー] をクリックします。
2. [ポリシーコンポーネント] を展開し、[管理サーバーリスト] をクリックします。
3. [タスク] で、[管理サーバーリストの追加] をクリックします。
4. [管理サーバーリスト] ダイアログボックスで、[追加]、[新しいサーバー] の順にクリックします。
5. [管理サーバーの追加] ダイアログボックスの [サーバーアドレス] フィールドに、管理サーバーの完全修飾ドメイン名または IP アドレスを入力します。
IP アドレスを入力する場合は、それが静的であることと、すべてのクライアントがそれを解決できることを確認します。
6. [OK] をクリックします。
7. 他のサーバーをすべて追加します。
8. 別の管理サーバーとの負荷分散を設定する場合は、[追加]、[新しい優先度] の順にクリックします。
9. 負荷分散に対するサーバーの優先度を変更するには、サーバーを選択し、[上に移動] または [下に移動] をクリックします。
10. [OK] をクリックします。

その後、グループに管理サーバーリストを適用する必要があります。

グループと場所への管理サーバーリストの割り当て

フェールオーバーまたは負荷分散に使う管理サーバーのインストール

クライアントが Symantec Endpoint Protection Manager と通信できない場合に通信を維持するには、フェールオーバー設定を使います。クライアント管理を複数の管理サーバー間で分散するには、負荷分散を使います。フェールオーバーと負荷分散を設定するには、管理サーバーのリストで管理サーバーに優先度を割り当てます。

フェールオーバーと負荷分散のインストールがサポートされるのは元の 1 つの Symantec Endpoint Protection Manager で Microsoft SQL Server データベースが使用されるときだけです。SQL Server Native Client ファイルはフェールオーバーまたは負荷分散に使用するコンピュータにもインストールする必要があります。

フェールオーバーまたは負荷分散に使う管理サーバーをインストールするには

-
1. Symantec Endpoint Protection Manager をインストールします。

つの Symantec Endpoint Protection Manager のインストール

2. [管理サーバー設定ウィザード] パネルで、[カスタム設定] にチェックマークを付け、[次へ] をクリックします。

インストール後の つの Symantec Endpoint Protection Manager の設定

3. このサーバーで管理するクライアント数を選択し、[次へ] をクリックします。
4. [既存のサイトに追加の管理サーバーをインストールする] にチェックマークを付け、[次へ] をクリックします。
5. [サーバー情報] パネルで、デフォルト値を受け入れるか変更してから、[次へ] をクリックします。
6. [Microsoft **SQL Server** 情報] ダイアログボックスに表示される SQL Server クライアントツールのインストールに関するメッセージで [OK] をクリックします。
7. 次のテキストボックスにリモートサーバーの値を入力します。

[ステップ 1] では、ホスト名、インスタンス名、ポートなど、ネットワーク上で SQL Server を見つける場所を つの Symantec Endpoint Protection Manager に示します。

Windows 認証や SQL 認証などの認証の種類も選択します。

- データベースサーバー\インスタンス名

SQL Server ポート

データベース名

SQL Client フォルダ (ローカルコンピュータ上)

このテキストボックスに自動的に正しいパスが表示されない場合は、Microsoft SQL Client ユーティリティをインストールしていないか正しくインストールしていません。

8. [ステップ 2] では、つの Symantec Endpoint Protection Manager に SQL Server の認証方法を示し、データベース名、データベースユーザー、データベースユーザーのパスワードなどを入力します。

該当のサイトに初めて管理サーバーをインストールしたときにこの情報をすでに利用できたはずです。

9. [次へ] をクリックします。

10. Symantec Endpoint Protection Manager の admin アカウントのパスワードを指定して確定します。

オプションで、管理者の電子メールアドレスを入力します。

11. [次へ] をクリックします。

12. 警告のメッセージを読んで [OK] をクリックします。

13. [管理サーバーの完了] パネルで、[完了] をクリックします。

外部ログ記録用フェールオーバーサーバーの設定

グループと場所への管理サーバーリストの割り当て

ポリシーを追加した後はそのポリシーをグループまたは場所 (またはその両方) に割り当てる必要があります。ある管理サーバーから別の管理サーバーにクライアントのグループを移動するために管理サーバーリストを使うこともできます。

リストを割り当てる前に、管理サーバーリストの追加または編集を完了しておく必要があります。

負荷分散のための管理サーバーリストの設定

1. グループと場所に管理サーバーリストを割り当てるには、コンソールで [ポリシー] をクリックします。
2. [ポリシー] ページで、[ポリシーコンポーネント] を展開し、[管理サーバーリスト] をクリックします。
3. [管理サーバーリスト] ペインで、割り当てる管理サーバーリストを選択します。
4. [タスク] で、[リストの割り当て] をクリックします。
5. [管理サーバーリストの適用] ダイアログボックスで、管理サーバーリストを適用するグループと場所にチェックマークを付けます。
6. [割り当て] をクリックします。
7. [はい] をクリックします。
8. [クライアント] ページでグループまたは場所に管理サーバーリストを割り当てるには、コンソールで [クライアント] > [ポリシー] をクリックします。
9. [ポリシー] タブでグループを選択したら、[ポリシーと設定を親グループから継承する] のチェックマークをはずします。
親のグループからポリシーと設定を継承していないグループ以外は、通信を設定することはできません。
10. [場所に依存しないポリシーと設定] で、[通信の設定] をクリックします。
11. [グループ名の通信設定] ダイアログボックスの [管理サーバーリスト] で、管理サーバーリストを選択します。
選択したグループで管理サーバーと通信するときに、ここで選択する管理サーバーリストが使用されます。
12. [OK] をクリックします。

サイトと複製の設定

サイトは 1 つのデータベース、1 つ以上の管理サーバーとクライアントで構成されます。デフォルトでは、単一のサイトとして Symantec Endpoint Protection を配備します。複数のデータセンターや物理的な場所を持つ組織は、一般的に複数のサイトを使います。

冗長性を持たせるために、複製を設定します。一方のデータベースのデータがもう一方のデータベースに複製またはレプリケートされます。一方のデータベースが失敗した場合でも、もう一方のデータベースにクライアント情報が含まれているのですべてのクライアントの管理を続行できます。

サイトの概要と複製の仕組み

Table 163: サイトと複製を設定するための処理

タスク	説明
ステップ 1: 別のサイトを追加する必要があるかどうかを判断する	複数のサイトと複製を設定する前に、それが必要であることを確認してください。シマンテック社は、特別な場合のみに複数のサイトを設定することと、サイトファームでのサイト追加数を最大 5 つまでにすることを推奨します。別のサイトを追加する場合は、組織にはどのサイト設計が機能するかを決定します。 複数サイトと複製を設定するかどうか 必要なサイト数の決定
ステップ 2: 1 番目のサイトにつの Symantec Endpoint Protection Manager をインストールする	Symantec Endpoint Protection を初めてインストールする場合、デフォルトでは最初のサイト、つまりローカルサイトがインストールされています。 つの Symantec Endpoint Protection Manager のインストール

タスク	説明
ステップ 3: 2 番目のサイトに つの Symantec Endpoint Protection Manager をインストールする	2 番目の管理サーバーをインストールして、2 番目のサイトを作成します。2 番目のサイトは、リモートサイトに分類され、管理サーバーは複製パートナーと呼ばれます。複製は、管理サーバーの初回インストール時に、2 番目のサイト追加のデフォルトスケジュールに従って行われます。複製パートナーを追加したら、複製スケジュールや複製されるデータを変更できます。 複製のための 2 番目のサイトのインストール方法 2 つのサイト間のデータベースの複製を初めて行う場合は、複製を完全に完了させてください。複製では、データベース全体が複製されるため時間がかかる場合があります。データベース複製の予定時間まで待機するのではなく、データを即座に複製することもできます。複製スケジュールを変更して、予定時間の前または後に実行することもできます。 1 つのサイトで管理サーバーをアップグレードする場合は、すべてのサイトで管理サーバーのバージョンをアップグレードする必要があります。 即座に実行されるデータの複製
ステップ 4: 複製イベントの履歴を確認する (省略可能)	発生した複製を確認したり、複製イベントをトラブルシューティングしたりする必要がある場合は、システムログを参照します。 2 番目の管理サーバーでシステムログを表示します。[管理] > [複製イベント] イベントタイプをフィルタします。 ログの表示

また、管理サーバーを再設定して、ネットワーク内の現在の既存のサイトでデータを複製することができます。または、2 つの非複製のサイトがある場合は、サイトの 1 つを 2 番目のサイトでデータを複製するサイトに変換します。

つの Symantec Endpoint Protection Manager の再インストールまたは再設定

- Symantec Endpoint Protection を設定した後、すべての設定変更が含まれているデータベースのバックアップを作成する必要があります。
- [データベースとログのバックアップ](#)
- 管理サーバーの最新バージョンにアップグレードするために複製パートナーを無効にした場合は、その複製パートナーを再度追加する必要があります。
- [アップグレード前後での、複製の無効化と復元](#)
- [新リリースへのアップグレード](#)

複製されたサイトのディレクトリサーバーへの接続

サイトの概要と複製の仕組み

サイトと複製パートナー

複製の機能について

複製サーバーのサイズの決定

サイトと複製パートナー

サイトは 1 つの Symantec Endpoint Protection Manager データベースで、そのデータベースには 1 つ以上の 1 つの Symantec Endpoint Protection Manager が接続されています。複製により、異なるサイト上のデータベース間で、両方のデータベースに同じ情報が含まれるようにデータを複製することができます。一方のデータベースが失敗した場合でも、もう一方のサイトにあるデータベースの情報を使うことで、各サイトを管理できます。

複製パートナーは 2 番目のサイトまたはリモートサイトの独立した管理サーバーです。サイトには、必要な数の複製パートナーを指定できます。各パートナーはメインサイトまたはローカルサイトに接続し、ユーザーはこのサイトにログオンすることになります。パートナーとして設定されたすべてのサイトが、同じサイトファームにあると見なされます。

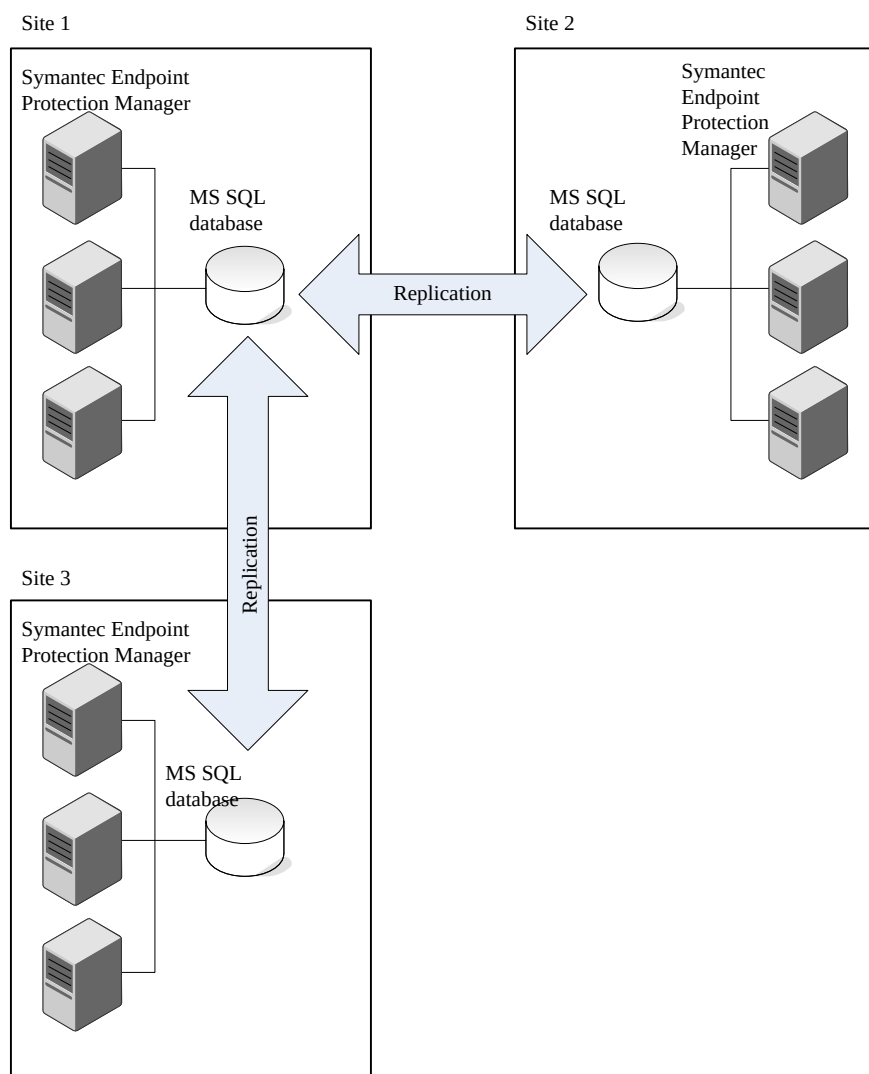
データを複製する各サイトは、複製パートナーとサイトパートナーのいずれかです。複製パートナーもサイトパートナーも複数の管理サーバーを使いますが、使うデータベースと通信方法が異なります。

- 複製パートナーは、デフォルトデータベース (14.3 RU1 では Microsoft SQL Server Express) または Microsoft SQL Server データベースを使用できます。管理サーバーはデータベースを共有しません。すべての複製パートナーが、共通のライセンスキーを共有します。Microsoft SQL Server データベースを使う場合は、1 つのデータベースを共有する複数の管理サーバーに接続できます。複製パートナーとして設定する必要があるのは、それらの管理サーバーのいずれか 1 つだけです。
- サイトパートナーは 1 つの Microsoft SQL Server データベースを共有します。

複製の機能について

パートナーに加えた変更は、他のすべてのパートナーに複製されます。たとえば、本社 (サイト 1) および 2 番目のサイト (サイト 2) で 1 つのサイトを設定できます。サイト 2 はサイト 1 のパートナーです。サイト 1 とサイト 2 のデータベースは、複製スケジュールを使って一致が保たれます。サイト 1 に変更が加えられた場合、複製によってサイト 2 にも自動的に変更が加えられます。サイト 2 に変更が加えられた場合、複製によってサイト 1 にも自動的に変更が加えられます。3 番目のサイト (サイト 3) をインストールして、そこにサイト 1 またはサイト 2 のデータを複製することもできます。

複製を行うと、サイト 1 のデータベースとサイト 2 のデータベースが同じになります。サーバーのコンピュータ識別情報だけが異なります。



複製の頻度について詳しくは、ナレッジベースの記事「[The Philosophy of SEPM Replication Setup](#)」を参照してください。

複数サイトと複製を設定するかどうか

必要なサイト数の決定

複製中に生じたサイト間のデータ競合を解決する方法

複製サーバーのサイズの決定

複製パートナーには、単一の管理サーバーのインストールよりも大きいデータベースが必要です。複製サーバーでより大きなサイズが必要なのは、次の要因によります。

- 管理下クライアントの数
- データベースに保持されるクライアントインストールパッケージのサイズ
- 保持されるログファイルの数
- データベースの保守設定
- ログのサイズと有効期限
- 定義の更新のサイズ
- データベースバックアップ情報の必要条件

最初に複製を作成する際、複製サーバーのハードディスクの必要条件は、一般に元の Symantec Endpoint Protection Manager で使われているハードディスク容量の 3 倍以上でなければなりません。

複製のための 2 番目のサイトのインストール方法

複製の考慮事項とベストプラクティス

Symantec Endpoint Protection のサイジングおよび拡張性のベストプラクティスのホワイトペーパー

複製中に生じたサイト間のデータ競合を解決する方法

複製により、データが別の管理サーバーに移送、転送されます。サイトは複数の複製パートナーを持つことが可能で、1 つのパートナーに対して行なわれた変更はすべてのサイトに複製されます。

複製されるデータ

どの複製サイトも他の複製サイトに対して優先されることはありません。各サイトの内容が比較され、あるサイトに他のサイトにはないパッケージまたはコンテンツの一部がある場合、それらは共有されます。すべての LiveUpdate コンテンツとクライアントパッケージが一致する場合は、何も交換されません。

複製パートナーは次のデータを複製します。

- ポリシーとグループ (双方向が必須)
- LiveUpdate コンテンツとクライアントインストールパッケージ (これらのオプションを指定した場合。双方向は任意)
- ログ (双方向か単方向は任意)

1 つのサイトで管理サーバーをアップグレードする場合は、すべてのサイトで管理サーバーのバージョンをアップグレードする必要があります。データベーススキーマバージョンが一致しない場合、複製は行われません。

以下の表では、管理者がサイトファームにあるサイトの設定を変更した場合に、管理サーバーがどのように競合を解決するかを説明します。

Table 164: 管理サーバーがサイト間の競合を解決するしくみ

競合の種類	例	解決策
2 つの変更は同時に存在できない。	サイト 1 とサイト 2 の管理者が、同じファイアウォールポリシー設定を設定する。サイト 1 では、設定は有効になります。サイト 2 では、設定は無効になります。	管理サーバーは最後に行われた変更のみを保持します。 たとえば、最初にサイト 1 を、次にサイト 2 を変更した場合は、サイト 2 の変更が保持されます。
同じ変数が両方のサイトに作成される。	サイト 1 とサイト 2 の管理者が、同じ名前のグループを追加する。	管理サーバーは両方の変更を保持します。最後に作成された変数の後に、波形符号と数字の 1 (~1) が追加されます。 たとえば、2 つのグループに Sales という名前を付けると、最後に名前が付けられた Sales グループは Sales ~1 になります。
データは競合なしでマージできる。	サイト 1 の管理者が 2 つのファイアウォールポリシーを追加し、サイト 2 の管理者が 5 つのファイアウォールポリシーを追加する。	管理サーバーは変更をマージします。 たとえば、管理サーバーは両方のサイトの 7 つのファイアウォールポリシーをすべて表示します。

複数サイトと複製を設定するかどうか

2 番目のサイトをインストールする前に、複数サイトと複製が現状のネットワークにおいてよい選択であるか判断する必要があります。複数サイトを設定することによって、無用な複雑さが生じます。複数サイトは、クライアントのログ表示やレポート表示などのタスクがより難しくなる要因になります。通常、インストールするサイトは 1 つのみにしてください。

複数サイトと複製を設定する主な目的は次のとおりです。

- ネットワークに遅い WAN リンクがある場合。
複数サイトによって、複数の地理上の領域内にあるクライアントがローカルで接続可能な、第 2 管理サーバーが提供されます。たとえば、ある会社がドイツと米国に複数の大規模なオフィスを持っているという状況を想定します。ドイツと米国間の接続が遅い場合、会社はドイツで 1 つのサイト、米国で 1 つのサイトをそれぞれ作成する必要があります。ドイツのクライアントはドイツのサイトに接続、米国のクライアントは米国のサイトに接続できます。この分散により、遅い WAN リンクで通信しなければならないクライアントの数は少なくなります。
- データベースの冗長性のため。
複製によって、1 つのデータセンターが壊れたり失われたりした場合に、別のデータセンターにバックアップ済みのデータベースが存在することになります。

状況によっては、複数サイトと複製の代わりに GUP (グループ更新プロバイダ) を使う必要があります。多数のクライアントがある、または複数の地理上の場所に分散しているクライアントがある場合に、GUP を使用します。

NOTE

設定する複製されたサイトは、5 つを超えないようにしてください。

Table 165: 複製がある複数のサイトを使うか、GUP を使うか、どちらも使わないかを決めます。

質問	回答	複製がある複数のサイトを使うか、GUP を使う
45,000 を超えるクライアントがありますか。	はい。 複数の場所、または 1,000 を超えるクライアントがある場所に接続する遅い WAN リンクが存在しますか。	はい。 - 遅い WAN リンクの場合は、複製の使用を検討します。 - 複数の場所の場合は、GUP の使用を検討します。
		いいえ。複製や GUP を必要としません。

質問	回答	複製がある複数のサイトを使うか、GUP を使う
	No. 1,000 を超えるクライアントがある場所に接続する、遅い WAN リンクが存在しますか。	はい。複製の使用を検討します。 いいえ。複製や GUP を必要としません。
遅い WAN リンクが存在しますか。	はい。 場所ごとに 1,000 を超えるクライアントを持つ複数の場所が存在しますか。	はい。複製の使用を検討します。 いいえ。GUP の使用を検討します。
	No. 場所ごとに 1,000 を超えるクライアントを持つ複数の場所が存在しますか。	はい。複製の使用を検討します。 いいえ。複製や GUP を必要としません。
場所ごとに 1,000 を超えるクライアントを持つ複数の場所が存在しますか。	はい。 1,000 を超えるクライアントがある場所に接続する、遅い WAN リンクが存在しますか。	はい。GUP の使用を検討します。 いいえ。複製や GUP を必要としません。
	【※No※】 1,000 を超えるクライアントがある場所に接続する、遅い WAN リンクが存在しますか。	はい。GUP の使用を検討します。 いいえ。複製や GUP を必要としません。

Symantec Endpoint Protection Manager で複製を使用する場合

クライアントにコンテンツを配布するための GUP の使用

サイトと複製の設定

必要なサイト数の決定

必要なサイト数の決定

大半の中小規模の組織では、ネットワークセキュリティを集中的に管理するには 1 つのサイトのみで十分です。各サイトからアクセスするのは 1 つのデータベースだけなので、すべてのデータが中央に置かれます。

1 つの場所にある大規模組織でも、一般的には 1 つのサイトのみを必要とします。しかし、集中的に管理するには複雑すぎる組織の場合は、複数のサイトがある分散型の管理アーキテクチャを使う必要があります。

複数のサイトの場合は、次の要因について検討することをお勧めします。

- 多数のクライアント。
- 地理的な場所の数とそれらの間の通信リンクの種類。
- 機能区分または管理グループの数。
- データセンターの数。ベストプラクティスは、データセンターごとに 1 つの Symantec Endpoint Protection サイトを設定することです。
- コンテンツを更新したい頻度。
- 保持する必要があるクライアントログデータの量、それらを保持する必要がある期間、それらを格納する場所。
- 数千台のクライアントを持つ複数の物理的場所の間での低速 WAN リンク。専用の管理サーバーを持つ 2 番目のサイトを設定すると、その低速リンク上のクライアントサーバートラフィックを最小化できます。クライアントの台数が少ない場合は、グループ更新プロバイダを使ってください。

クライアントにコンテンツを配布するための GUP の使用

- 固有のさまざまな企業管理および IT セキュリティ管理に関する考慮事項。

インストールするサイトの数を決定する際は、サイズに関する次のガイドラインを参考にしてください。

- インストールするサイトはできるだけ少なくし、最大 20 までにする。複製されたサイトの数を常に 5 より少なくする。
- データベースに接続する管理サーバーは 10 までにする。
- 最大で 18,000 台までのクライアント (14.x) または 50,000 台までのクライアント (12.1.x) を管理サーバーに接続します。

サイトを追加した後、複製によって複数のサイト全体でサイト情報を複製する必要があります。複製は、データベース間で情報を共有して、内容の一貫性を確保する処理です。

Table 166: 複数サイトの設計

サイト設計	説明
配布済み	各サイトがグループとポリシーの複製を双方向で行いますが、ログとコンテンツの複製は行いません。サイトのレポートを表示するには、コンソールを使ってリモートサイトの管理サーバーに接続します。リモートサイトのデータに直接アクセスする必要がないときは、この設計を使います。
集中型のログ記録	すべてのログは他のサイトから中央のサイトに転送されます。集中型のレポートが必要なときは、この設計を使います。
高可用性	すべてのサイトで、複数の管理サーバーがインストールされ、データベースがクラスタ化されます。追加のクライアントを処理するには、複数のサイトを追加するのではなく、複数の管理サーバーを追加します。次に管理サーバーリストを使用して、プライマリ管理サーバーが利用不能になった場合に自動的に代替の管理サーバーに切り替えるように、クライアントコンピュータを設定できます。冗長性、フェールオーバー、ディザスタリカバリを提供するには、この設計を使います。 Note: 埋め込みデータベース (14.3 MPx 以前) でレプリケーションを使う場合は、データの不整合や損失が生じる可能性があるため、負荷分散を追加しないことを推奨します。 フェールオーバーと負荷分散の設定

複製を設定するかどうかについて詳しくは、ナレッジベースの記事「[Symantec Endpoint Protection Manager で複製を使用する場合](#)」を参照してください。

[サイトの概要と複製の仕組み](#)

[サイトと複製の設定](#)

[複数サイトと複製を設定するかどうか](#)

複製のための 2 番目のサイトのインストール方法

複製のために 2 番目のサイトをインストールするプロセスは 2 つの手順で構成されます。

- 2 番目の 1 つの Symantec Endpoint Protection Manager とデータベースをインストールして、これらは、すでにインストールされている 1 つの Symantec Endpoint Protection Manager とデータベースを使って複製されます。
- 2 番目の 1 つの Symantec Endpoint Protection Manager にログオンして、複製するスケジュールとアイテムを変更します (省略可能)。

[複製の頻度とコンテンツの変更](#)

複製のための 2 番目のサイトのインストール

1. 2 番目の 1 つの Symantec Endpoint Protection Manager をインストールします。
[1 つの Symantec Endpoint Protection Manager のインストール](#)
管理サーバー設定ウィザードは、管理サーバーのインストール後に自動的に開始します。
2. [管理サーバー設定ウィザード] で、新しいインストールのカスタム設定 (クライアント数が **500** 以上またはカスタム設定) をクリックして [次へ] をクリックします。
3. [追加サイトをインストールする] をクリックして、[次へ] をクリックします。

-
4. 表示されたパネルで次の情報を入力してから、[次へ] をクリックします。
 - 複製サーバー
すでにインストールされ、この管理サーバーが複製する、管理サーバーの名前または IP アドレス。
 - システム管理者名とパスワード。
システム管理者のデフォルトのユーザー名は `admin` です。限定管理者アカウントやドメイン管理者アカウントではなく、システム管理者アカウントを使用する必要があります。
 - [ローカルサイトとこのパートナーサイトの間でクライアントパッケージと **LiveUpdate** コンテンツを複製する] にチェックマークを付けます (省略可能)。
このオプションに今すぐにチェックマークを付けない場合、後でチェックマークを付けることができます。
 5. 証明書の受け入れに関する警告メッセージが表示されたら、[はい] をクリックします。
 6. サイト情報ペインで、デフォルト値を受け入れるか変更してから、[次へ] をクリックします。
 7. データベース選択ペインで、[デフォルトの **SQL Server Express** データベース] または [**Microsoft SQL Server** データベース] をクリックして、[次へ] をクリックします。
複製するサイトで同じ種類のデータベースを使用することをお勧めしますが、必須ではありません。14.3 MPx 以前では、デフォルトのデータベースは [デフォルト埋め込みデータベース] です。
選択したデータベースに基づいてインストールを完了してください。
 8. [LiveUpdate の実行] ペインで、[次へ] をクリックします。
パートナー情報を追加することもできます。
 9. 必要に応じてデータ収集機能を受け入れ、[次へ] をクリックします。
データベースが作成されます。このステップは時間がかかります。
つの Symantec Endpoint Protection Manager が起動します。

必要に応じてスケジュールを変更します。 [複製の頻度とコンテンツの変更](#)

[サイトと複製の設定](#)

[サイトの概要と複製の仕組み](#)

[複数サイトと複製を設定するかどうか](#)

[アップグレード中の複製の防止](#)

即座に実行されるデータの複製

複製は通常、追加のサイトを設定するときにデフォルトのスケジュールに従って行われます。すぐに複製を開始することもできます。ID 番号が小さいサイトにより、スケジュール設定された複製が開始されます。

複数のサーバーで Microsoft SQL Server データベースを使っている場合、サイトの最初のサーバーからのみ複製を開始できます。

1. コンソールで、[管理] > [サーバー] の順に選択します。
2. [サーバー]、[ローカルサイト] の下で、[複製パートナー] を展開して、サイトを選択します。
3. [タスク] の下で、[今すぐに複製] をクリックします。
4. [はい] をクリックして [OK] をクリックします。

[複製の頻度とコンテンツの変更](#)

[サイトと複製の設定](#)

サイトの削除

複製パートナーを削除すると、つの Symantec Endpoint Protection Manager のパートナーシップを解除しますが、管理サーバーソフトウェアのアンインストールや 2 番目のサイトの削除は行いません。

リモートサイトで管理サーバーを削除する場合は、すべてのサイトから手動で削除する必要があります。1つの管理サーバーコンソールからソフトウェアをアンインストールしても、そのアイコンは他のコンソールの [サーバー] ペインから削除されません。

アップグレード前後での、複製の無効化と復元

サイトを削除するには

1. コンソールで [管理] > [サーバー] > [ローカルサイト] を選択し、[複製パートナー] を展開して複製パートナーを右クリックし、[複製パートナーの削除] をクリックします。
2. [リモートサイト] の下でサイトを右クリックし、[リモートサイトの削除] をクリックします。
3. [はい] をクリックします。

サイトと複製の設定

Endpoint Protection のディザスタリカバリのベストプラクティス

ハードウェアの故障やデータベースの破損に備えるには、つの Symantec Endpoint Protection Manager をインストールした後に収集する情報のバックアップを作成する必要があります。

ディザスタリカバリの準備

ディザスタリカバリの実行

ディザスタリカバリの準備

Table 167: ディザスタリカバリに備えるための高レベルの手順

手順	説明
手順 1: データベースのバックアップを作成する	定期的に (できれば週 1 回) データベースのバックアップを作成します。 デフォルトでは、データベースバックアップフォルダは次のデフォルトの場所に保存されます。 C:\Program Files (x86)\Symantec\## Symantec Endpoint Protection Manager\data/backup バックアップファイルの名前は、日付_timestamp.zip になります。 データベースとログのバックアップ
ステップ 2: ディザスタリカバリファイルのバックアップを作成する	回復ファイルには、暗号化パスワード、キーストアファイルのドメイン ID、証明書ファイル、ライセンスファイル、ポート番号が含まれています。このファイルは、デフォルトでは次のディレクトリにあります。 C:\Program Files (x86)\Symantec\## Symantec Endpoint Protection Manager\Server Private Key Backup\recovery_#####.zip リカバリファイルはデフォルトのドメイン ID のみを格納しています。複数のドメインがある場合、その情報は回復ファイルに格納されていません。ディザスタリカバリを実行する必要がある場合は、ドメインを再度追加する必要があります。 ドメインの追加
ステップ 3: サーバー証明書を更新またはサーバー証明書のバックアップを作成する (省略可能)	自己署名証明書を異なる種類の証明書に更新すると、管理サーバーで新しい回復ファイルが作成されます。回復ファイルにはタイムスタンプがあるため、どれが最新のファイルであるかがわかります。 サーバー証明書の更新または復元 サーバー証明書のバックアップ
ステップ 4: 管理サーバーの IP アドレスとホスト名をテキストファイルに保存する (省略可能)	壊滅的なハードウェア障害が発生した場合は、元の管理サーバーの IP アドレスとホスト名を使って管理サーバーを再インストールする必要があります。 IP アドレスとホスト名を Backup.txt などの名前のテキストファイルに追加します。

手順	説明
ステップ 5: オフサイトの安全な場所にバックアップデータを保存する	前の手順でバックアップしたファイルの別のコンピュータへのコピー

ディザスタリカバリの実行

「[ディザスタリカバリを実行するための処理](#)」に、ハードウェアの故障やデータベースの破損が発生した場合に Symantec Endpoint Protection 環境を回復する手順を示します。

これらの手順を実行する前に、バックアップと回復のファイルを作成済みであることを確認します。

Table 168: ディザスタリカバリを実行するための処理

手順	処理
ステップ 1: ディザスタリカバリファイルを使って Symantec Endpoint Protection Manager を再インストールする	管理サーバーを再インストールすることで、初期インストール後に保存されたファイルを回復できます。 この Symantec Endpoint Protection Manager の再インストールまたは再設定 ディザスタリカバリファイルを使わずにこの Symantec Endpoint Protection Manager を別のコンピュータに再インストールする場合は、新しいサーバー証明書を生成する必要があります。 新しいサーバー証明書の生成
ステップ 2: データベースを復元する	データベースバックアップの有無にかかわらず、データベースを復元できます。 データベースの復元
ステップ 3: 連邦情報処理標準 (FIPS) 140-2 コンプライアンスを再び有効にする (省略可能)	Symantec Endpoint Protection の FIPS 対応バージョンを使い、FIPS コンプライアンスを有効にした場合は、この Symantec Endpoint Protection Manager を回復した後に、FIPS コンプライアンスを再び有効にする必要があります。 この設定は、ディザスタリカバリファイルに格納されません。

ライセンスファイルのバックアップ

サーバーの設定のエクスポートとインポート

「[Endpoint Protection のディザスタリカバリのベストプラクティス](#)」を参照してください。

データベースとログのバックアップ

データベースを少なくとも週単位でバックアップすることをお勧めします。バックアップファイルは、別のコンピュータに格納してください。

デフォルトでは、バックアップファイルは C:\Program Files (x86)\Symantec\## Symantec Endpoint Protection Manager\data\backup フォルダに保存されます。

バックアップは .zip ファイルで保存されています。デフォルトでは、バックアップデータベースファイルの名前は、date_timestamp.zip です。

NOTE

製品のインストールディレクトリにバックアップファイルを保存することは避けてください。そうしないと、バックアップファイルは製品がアンインストールされるときに削除されます。

この Symantec Endpoint Protection Manager でバックアップの設定を行わないかぎりログデータはバックアップされません。ログをバックアップしないと、ログ設定オプションのみがバックアップ中に保存されます。バックアップを使ってデータベースを復元できますが、データベース内のログは復元時に空のデータになります。

サイトのバックアップは 10 バージョンまで保持できます。複数のバージョンを保持する場合には、すべてのデータを保持するのに十分なディスク容量を確保する必要があります。

バックアップ中にもバックアップ後にもシステムログとバックアップフォルダの状態を確認できます。

データベースをすぐにバックアップしたり、自動的に実行されるようにバックアップをスケジュール設定したりできます。

NOTE

Microsoft SQL Server Express データベースには 10 GB の制限があります。データベースをバックアップする場合、データベースは 10 GB を超えることはできません。また、少なくとも 10 GB の空きディスク容量が必要です。 [埋め込みデータベースから Microsoft SQL Server Express データベースへのアップグレードに関するベストプラクティス](#)

データベースの自動バックアップのスケジュール設定

Endpoint Protection のディザスタリカバリのベストプラクティス

1. Symantec Endpoint Protection Manager を実行しているコンピュータでデータベースとログをバックアップするには、[スタート] メニューで、[すべてのプログラム] > [Symantec **Endpoint Protection Manager**] > [Symantec **Endpoint Protection Manager** ツール (Symantec **Endpoint Protection Manager Tools**)] > [データベースのバックアップと復元] の順に選択します。
2. [データベースのバックアップと復元] ダイアログボックスで、[バックアップ] をクリックします。
3. [データベースのバックアップ] ダイアログボックスで、省略可能なオプションとして、[バックアップログ] にチェックマークを付け、[はい] をクリックします。
4. [OK] をクリックします。
5. データベースバックアップが完了したら、[終了] をクリックします。
6. バックアップデータベースファイルを別のコンピュータにコピーします。
7. データベースとログのバックアップをコンソール内から作成するには、コンソールで [管理] > [サーバー] をクリックします。
8. [サーバー] で、[ローカルサイト (マイサイト)] > [SQLEXPRESSSYMC] (14.3 RU1 以降) または [ローカルホスト] をクリックします。
9. [タスク] で、[今すぐにデータベースのバックアップを作成] をクリックします。
10. [データベースのバックアップ] ダイアログボックスで、省略可能なオプションとして、[バックアップログ] にチェックマークを付け、[はい] をクリックします。
11. [OK] をクリックします。
12. [閉じる] をクリックします。

サーバー証明書のバックアップ

管理サーバーがインストールされたコンピュータが壊れた場合に備え、専用キーと証明書をバックアップしてください。

JKS キーストアファイルは、初回のインストール時にバックアップされます。server_timestamp.xml という名前のファイルもバックアップされます。JKS キーストアファイルには、サーバーの専用キーと公開キーのペアおよび自己署名の証明書が格納されています。

サーバー証明書をバックアップするには

-
1. コンソールで、[管理] をクリックし、[サーバー] をクリックします。
 2. [サーバー] の下で、サーバー証明書のバックアップを作成する管理サーバーをクリックします。
 3. [タスク] の下で [サーバー証明書の管理] をクリックし、[次へ] をクリックします。
 4. [サーバー証明書の管理] パネルで、[サーバー証明書のバックアップを作成する] をクリックしてから [次へ] をクリックします。
 5. [サーバー証明書のバックアップを作成] パネルで、[参照] をクリックしてバックアップフォルダを指定してから [次へ] をクリックします。
管理サーバーの証明書は同じフォルダにバックアップされます。
 6. [サーバー証明書のバックアップを作成] パネルで、[次へ] をクリックします。
 7. [完了] をクリックします。

サーバー証明書について

新しいサーバー証明書の生成

サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス

つの Symantec Endpoint Protection Manager の再インストールまたは再設定

管理サーバーを再インストールまたは再設定する必要がある場合、ディザスタリカバリファイルを使ってすべての設定をインポートできます。続いて、同じコンピュータの同じインストールディレクトリにソフトウェアを再インストールできます。つの Symantec Endpoint Protection Manager はインストール中にリカバリファイルを作成します。この手順を使って、既存のサイトを再設定することも、レプリケーション用に追加サイトをインストールすることもできます。

Endpoint Protection のディザスタリカバリのベストプラクティス

1. 管理サーバーを再インストールするには、既存の管理サーバーをアンインストールします。
2. インストールファイルからサーバーをインストールします。

つの Symantec Endpoint Protection Manager のインストール

3. [ようこそ] パネルで、[回復ファイルを使用して、以前に配備したクライアントとの通信を復元する] オプションにチェックマークが付いていることを確認し、[次へ] をクリックします。

デフォルトで、リカバリファイルは C:\Program Files (x86)\Symantec\## Symantec Endpoint Protection Manager\Server Private Key Backup にあります。リカバリファイルによって、クライアントが 1 つの Symantec Endpoint Protection Manager に再接続されます。

4. 各パネルの指示に従います。ほとんどの場合、デフォルト設定が機能します。再インストールしたサーバーが既存のデータベースに接続されている場合、データベースの設定を既存のデータベースの設定に変更します。

必要に応じて、データベースを復元することもできます。ただし、つの Symantec Endpoint Protection Manager データベースが別のコンピュータにあるか、影響を受けない場合は、データベースを復元する必要はありません。

データベースの復元

5. 管理サーバーを再設定するには、[スタート]、[すべてのプログラム]、[Symantec Endpoint Protection Manager]、[Symantec Endpoint Protection Manager ツール]、[管理サーバー設定ウィザード] の順にクリックします。
6. 次のオプションのいずれかを選択します。
 - 既存のサイトで管理サーバーを再設定するには、[管理サーバーを再設定する] をクリックします。
 - 管理サーバーを再設定して既存のサイトでデータを複製するには、[管理サーバーを再設定して別のサイトで複製する] をクリックします。

このオプションはローカルにインストールされた管理サーバーを再設定し、新しいサイトを作成してネットワークの別の既存のサイトでデータを複製します。また 2 つの非複製のサイトがある場合は、このオプションを使って、サイトの 1 つを 2 番目のサイトでデータを複製するサイトに変換します。

NOTE

[回復ファイルを使用して、以前に配備したクライアントとの通信を復元する] にチェックマークを付けておいた場合、インストールが続行します。ただし、リカバリファイルの既定のドメイン ID が無視され、複製パートナーのドメイン ID が使われます。再設定が完了した後、ドメイン ID の変更が原因で既存のクライアントが接続に失敗する可能性があります。

7. 各パネルの指示に従います。

つの Symantec Endpoint Protection Manager の再インストールまたは再設定

新しいサーバー証明書の生成

サーバーの IP アドレスまたはホスト名が変更された場合や、秘密鍵が危殆化した場合は、つの Symantec Endpoint Protection Manager の新しいサーバー証明書を生成します。

デフォルトでは、クライアント/サーバー通信にはサーバー証明書の検証が必要です。新しいサーバー証明書を生成した場合、この検証に失敗し、通信が中断します。この手順を開始する前に、証明書のアップデートのベストプラクティスを確認してください。

サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス

新しいサーバー証明書を生成するには

1. コンソールで、[管理] をクリックし、[サーバー] をクリックします。
2. [サーバー] の下で、管理サーバーをクリックします。
3. [タスク] の下で [サーバー証明書の管理] をクリックし、[次へ] をクリックします。
4. [サーバー証明書の管理] パネルで、[新しいサーバー証明書を生成する] をクリックします。[新しいキーの生成] にチェックマークが付けられていることを確認してから、[次へ] をクリックします。

[新しいキーの生成] では、新しいキーペア（公開キーと秘密鍵）を使用して証明書を新規作成します。このオプションのチェックマークをはずすと、新しい証明書で以前と同じキーペアが使用されます。その場合、キーペアが危殆化したときに、つの Symantec Endpoint Protection Manager サーバーのセキュリティプロファイルが低下します。

5. [はい] をクリックし、[次へ] をクリックします。
6. 新しい証明書を使うには次のサービスを再起動する必要があります。

- つの Symantec Endpoint Protection Manager サービス
 - つの Symantec Endpoint Protection Manager Webserver サービス
 - つの Symantec Endpoint Protection Manager API サービス
- (14 の時点)

管理サーバーサービスの停止と開始

Apache Web サーバーの停止と開始

つの Symantec Endpoint Protection Manager に次回ログオンしたときに、新しい証明書を信頼するように求められます。

つの Symantec Endpoint Protection Manager 用の自己署名されたサーバー証明書の受け入れについて

つの Symantec Endpoint Protection Manager コンソールへのログオン

データベースの復元

データベースが壊れている場合またはディザスタリカバリを実行する必要がある場合、データベースを復元できます。データベースを復元するには、最初にデータベースのバックアップを作成しておく必要があります。

データベースとログのバックアップ

NOTE

データベースの復元には、データベースのバックアップ時と同じバージョンの Symantec Endpoint Protection Manager を使う必要があります。データベースは、元々インストールされていた同じコンピュータで復元することも、別のコンピュータで復元することもできます。

データベースの復元が完了するまで数分かかる場合があります。

データベースバックアップでデータベースを復元するには

1. 管理サーバーサービスを停止します。
[管理サーバーサービスの停止と開始](#)
2. [スタート] メニューで、[すべてのプログラム]、[Symantec Endpoint Protection Manager]、[Symantec Endpoint Protection Manager Tools]、[データベースのバックアップと復元] の順にクリックします。
3. [データベースのバックアップと復元] ダイアログボックスで、[復元] をクリックします。
4. [はい] をクリックしてデータベースの復元を確認します。
5. [サイトの復元] ダイアログボックスで、バックアップデータベースファイルを選択し、[OK] をクリックします。
6. データベースをバックアップするときに作成したバックアップデータベースファイルのコピーを検索します。デフォルトでは、バックアップデータベースファイルの名前は、date_timestamp.zip になります。
7. [OK] をクリックします。
8. [Exit] をクリックします。
9. 管理サーバーサービスを再起動します。

データベースバックアップを使用せずにデータベースを復元するには

次のような場合、データベースバックアップを使用しないデータベースの復元が必要になることがあります。

- 管理者パスワードのリセットを試行したが、できない場合。
[忘れた つの Symantec Endpoint Protection Manager パスワードのリセット](#)
 - データベースバックアップは実行していなかったが、データベースが壊れた場合。
1. ポリシーファイルをバックアップします。
エクスポートしたポリシーファイルは、データベースの再インストール後にインポートします。
 2. 複数のドメインがある場合、SEPBackup.txt という名前のテキストファイルを作成して、任意のドメイン ID を追加します。(省略可能)
管理サーバーの情報を保存するには、管理サーバーの IP アドレスとホスト名をファイルに追加します。
 3. 管理サーバーサービスを停止します。
[管理サーバーサービスの停止と開始](#)
 4. 管理サーバー設定ウィザードとリカバリファイルを使って、管理サーバーを再設定します。
[つの Symantec Endpoint Protection Manager の再インストールまたは再設定](#)
 5. 再設定された つの Symantec Endpoint Protection Manager で、次のファイルを見つけてます。
SEPM_Install/tomcat/etc/conf.properties
デフォルトの SEPM_Install のデフォルト値は C:/Program files (x86)/Symantec/つの Symantec Endpoint Protection Manager です。
次のように変更します。
scm.agent.groupcreation=false を scm.agent.groupcreation=true に変更

このように編集することで、クライアントグループが自動的に作成されます。このように設定しないと、チェックインしたクライアントはデフォルトグループに再度表示されます。

クライアントは 1 つの Symantec Endpoint Protection Manager と通信できますが、次回のチェックイン後にのみコンソールに再表示されます。

Symantec Endpoint Security クラウド コンソールからのクライアントおよびポリシーの管理

ICDm クラウドコンソールと Symantec Endpoint Protection Manager の両方からクライアントおよびポリシーを管理する方法について説明します。

クラウドの一部のポリシー機能を活用するために、環境内でハイブリッド管理を設定できます。ハイブリッド管理を使用して、ICDm コンソールに Symantec Endpoint Protection Manager (SEPM) ドメインを登録します。その後、ICDm クラウドコンソールおよび Symantec Endpoint Security からクライアントコンピュータと一部のポリシーを管理できます。

オンプレミス管理、ハイブリッド管理、またはクラウドのみ管理オプションの選択

Symantec Endpoint Protection 14.0.1 (14.1) 以降のエージェントは、Symantec Endpoint Security (Endpoint Security) が管理するバージョンです。これらのエージェントはクラウド対応で、つの Symantec Endpoint Protection Manager (SEPM) または Integrated Cyber Defense Manager クラウドコンソールのいずれかから管理できます。

エージェントは、クラウドのみ、オンプレミスのみ、または両方の組み合わせ (ハイブリッド管理) で管理できます。

- クラウド管理の場合のみ、統合クラウドコンソールの Symantec Integrated Cyber Defense Manager (ICDm) を使用します。Symantec Endpoint Security Enterprise または Symantec Endpoint Security Complete のいずれかを購入する必要があります。
- オンプレミス管理の場合、Symantec Endpoint Protection の管理コンソールである つの Symantec Endpoint Protection Manager をインストールします。Symantec Endpoint Protection、Symantec Endpoint Security Enterprise、または Symantec Endpoint Security Complete を購入できます。
- ハイブリッド管理の場合、オンプレミス管理下デバイス用に つの Symantec Endpoint Protection Manager を使い、クラウド管理下デバイスを管理するために ICDm コンソールを使います。ICDm クラウドコンソールの各 つの Symantec Endpoint Protection Manager ドメインを登録します。登録すると、ICDm 内のすべてのデバイスおよびアラートを 1 つのビューで表示できます。さらに、ハイブリッド展開全体について、ICDm からデバイスと一部のポリシーを管理できます。ただし、オンプレミスデバイスの残りの保護については、Symantec Endpoint Protection Manager から管理できます。Symantec Endpoint Security Enterprise または Symantec Endpoint Security Complete を購入する必要があります。

Table 169: オンプレミス Symantec Endpoint Protection か、クラウド管理の Symantec Endpoint Security のどちらを使用するかを決定する

以下を使う場合	この製品を使用
クラウドコンソールを使用してクライアントを完全に管理する	Symantec Endpoint Security (Enterprise または Complete) クラウドのみの管理コンソールは、Integrated Cyber Defense Manager (ICDm) で、デバイスは Symantec Agents バージョン 14.2 RU1 以降を使います。Symantec Endpoint Security からエージェントインストールパッケージを作成および配備します。以前と同様に、デバイスにオンプレミスクライアントソフトウェアをインストールします。 クラウドからエージェントを完全に管理し、オンプレミス管理コンソールである 1 つの Symantec Endpoint Protection Manager との通信をバイパスします。 この方法は以下のシナリオで使います。 - 管理サーバーおよびデータベースのインストールと管理のコストやオーバーヘッドを望まない場合。 - 複数の Symantec enterprise 製品があり、1 つの管理コンソールで管理機能を共有したい場合。 - 複数のシマンテック製品からの脅威、ポリシー、インシデントを統合して可視化し、インシデント対応時間を数日から数分に短縮したい場合。 - Symantec Endpoint Security に、Symantec Endpoint Protection オンプレミスにはない追加機能がある場合。 ICDm での Symantec Endpoint Protection 管理と Symantec Endpoint Security 管理機能のクリックリフレッシュ クラウドからエージェントを管理するには、Symantec Security Cloud アカウントに直接ログオンします。1 つの Symantec Endpoint Protection Manager をインストールした場合、ドメインはクラウドに登録しません。 Symantec Endpoint Security にアップグレードすると、クラウド内の同等の設定は 1 つの Symantec Endpoint Protection Manager 設定よりも優先されます。相当する設定がない場合は、以前の 1 つの Symantec Endpoint Protection Manager 設定が優先されます。 1 つの Symantec Endpoint Protection Manager からクラウドにアップグレードした場合、後から 1 つの Symantec Endpoint Protection Manager での管理に戻すことができます。ただし、管理サーバーをアンインストールした場合は、再インストールする必要があります。後でディザスタリカバリを実行する必要がある場合に備えて、アップグレードする前にデータベースのバックアップを作成してください。smc コマンドを使用して、Windows デバイスを 1 つの Symantec Endpoint Protection Manager による管理に戻すことができます。 Symantec Endpoint Protection から Symantec Endpoint Security へのアップグレード Endpoint Security スタートガイド Endpoint Protection のディザスタリカバリのベストプラクティス
オンプレミス 1 つの Symantec Endpoint Protection Manager を使用してクライアントを完全に管理する	Symantec Endpoint Protection または Symantec Endpoint Security (Enterprise または Complete) クラウドに SEPM ドメインを登録しません。1 つの Symantec Endpoint Protection Manager からクライアントインストールパッケージを作成および配備します。 この方法は以下のシナリオで使います。 - ネットワークに、石油掘削装置やオフショア環境などのリモートの場所が含まれている場合 - ネットワークが非常に制限されている政府環境で作業する場合。 - ダークネットワークに多数のクライアントがある場合。 - オンプレミス管理サーバーと同じ機能が必要な場合。ただし、Symantec Endpoint Protection は機能の追加を継続します。

以下を使う場合	この製品を使用
レガシークライアントとクラウドのみの管理下エージェント (ハイブリッド) の両方を管理する	Symantec Endpoint Protection または Symantec Endpoint Security (Enterprise または Complete) ハイブリッド展開を正常に実行するには、SEPM とエージェントがバージョン 14.1 以降である必要があります。Symantec Endpoint Security のエージェントおよび一部のポリシーを管理します。つの Symantec Endpoint Protection Manager から 14.1 より前のクライアントを管理します。 注: Symantec Endpoint Protection クライアントは Symantec Agent と同じです。 この方法は以下のシナリオで使います。 14.1 以降から Symantec Endpoint Security にアップグレードするけれども、クラウド管理型コンソールに徐々に移動する場合。 - Symantec Endpoint Security がサポートしていないオペレーティングシステムを使用するデバイスにクライアントがある場合。 - つの Symantec Endpoint Protection Manager のアプリケーション制御ポリシーを置き換えるアプリケーション制御を使用する場合。アプリケーション制御には、14.2 MP1 以降のクライアントが必要です。アプリケーション分離 (新規) には、14.2 RU1 (クラウドのみ) または 14.2 RU1 クライアント以降が必要で、Symantec Endpoint Security クラウドコンソールを使用します。 アプリケーション制御とアプリケーション分離には、Symantec Endpoint Security Complete サブスクリプションを購入する必要があります。 ハイブリッドモデルにアップグレードし、後で つの Symantec Endpoint Protection Manager のみに戻す場合は、つの Symantec Endpoint Protection Manager ドメインを登録解除するだけです。このオプションを使用すると柔軟性が向上し、後からクラウドに完全に移行できます。 クラウドコンソールへの Symantec Endpoint Protection Manager ドメインの登録 クラウドコンソールから つの Symantec Endpoint Protection Manager ドメインを登録解除する

NOTE

14.0.1 以降のクライアントの機能は、Symantec Endpoint Security ではなく、つの Symantec Endpoint Protection Manager が管理する場合、わずかに異なります。つの Symantec Endpoint Protection Manager は、クライアントでより多くのオプションを制御しますが、Symantec Endpoint Security が制御するオプションの数は少なくなります。つの Symantec Endpoint Protection Manager には、ユーザーが設定するオプションが追加されています。クラウド管理下クライアントでは、用意されているオプションの数は少なくなります。ただし、シマンテックは、月単位の更新で Symantec Endpoint Security に新機能を追加しています。

[オンプレミス Symantec Endpoint Protection 14. x と Symantec Endpoint Security Complete の比較](#)

クラウドコンソールへの Symantec Endpoint Protection Manager ドメインの登録

クラウドコンソールでドメインを表示または管理する前に、まず つの Symantec Endpoint Protection Manager ドメインを登録する必要があります。

NOTE

最大 50 個の Symantec Endpoint Protection Manager ドメインを登録できます。

登録を開始する前に

クラウドコンソールで登録すると、.MSI ファイルを使用して、つの Symantec Endpoint Protection Manager ブリッジサービス、またはコネクタがインストールされます。

ICDm クラウドコンソールへのドメインの登録をサポートするには、環境が以下の要件を満たす必要があります。

- Symantec Endpoint Security の有償ライセンス
- [Symantec Security Cloud のアカウント](#)

つの Symantec Endpoint Protection Manager からドメインの登録を開始する際に、このログインアカウントを設定できます。ログインに使用するアカウントをすでにお持ちの場合は、既存のアカウントを利用できます。

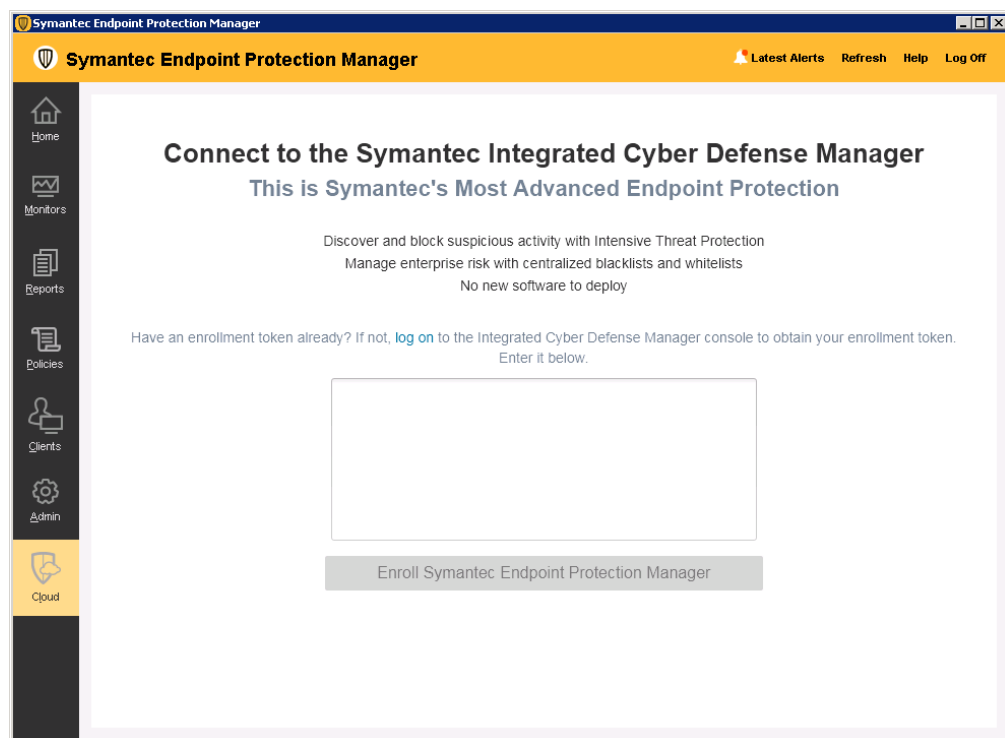
- つの Symantec Endpoint Protection Manager の管理者アクセス
- つの Symantec Endpoint Protection Manager 14.0.1 以降のクライアント

以前のクライアントを使用して つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録できますが、以前のクライアントでは、クラウドのみの集中保護ポリシーを活用できません。

- アプリケーションとデバイス制御をテスト (ログのみ) モードに、システムロックダウンをログのみのモードにします。この状況は、つの Symantec Endpoint Protection Manager を実行中のサーバーにそのようなポリシーが適用され、ポリシーが .MSI インストールを遮断する場合にのみ該当します。

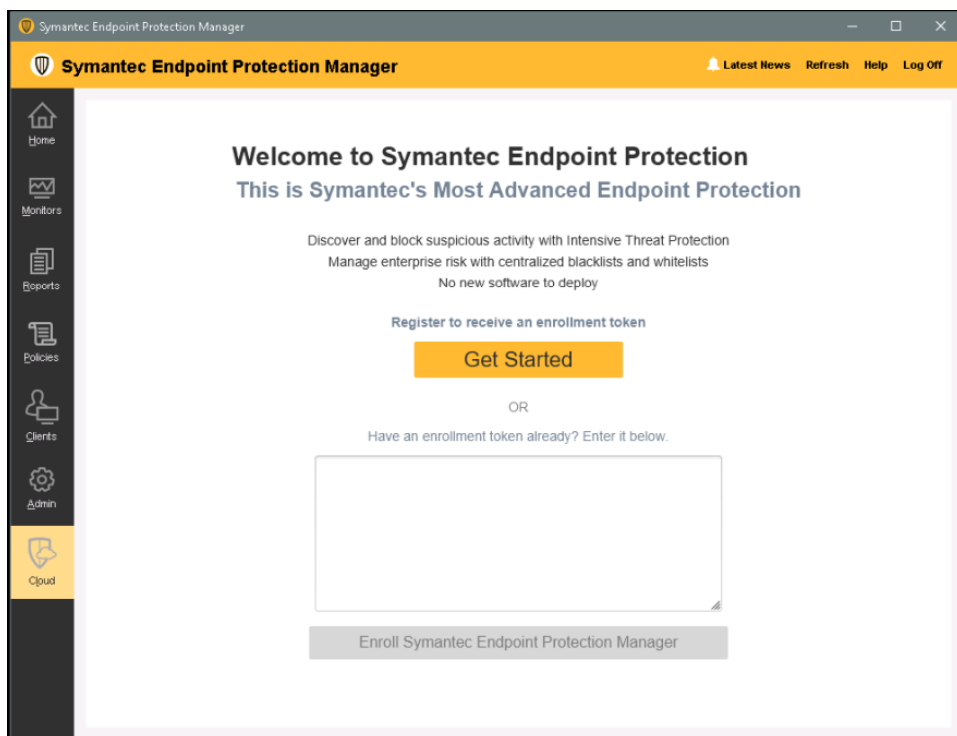
ステップ 1: 登録を開始する

Symantec Endpoint Protection Manager 14.3 から登録を開始するには、[クラウド] タブを選択します。



Symantec Endpoint Protection Manager 14.2 より前から登録を開始するには

つの Symantec Endpoint Protection Manager の [ホーム] ページで、[今すぐ登録] を選択するか、[クラウド] タブに移動します。[開始] ボタンをクリックすると、クラウドコンソールのサインインページに移動します。サインインの資格情報を持っていない場合は、アカウントチーム管理者にお問い合わせください。



クラウドコンソールからの登録プロセスは、[登録] ページで開始することもできます。

ステップ 2: クラウドコンソールから登録トークンを取得する

クラウドコンソールで、[エンドポイント] > [統合] > [登録] に移動します。このページから登録トークンを生成およびコピーできます。

ステップ 3: 登録を完了する

1. つの Symantec Endpoint Protection Manager で、[クラウド] ページの指定領域に登録トークンを貼り付けます。
2. [Enroll **Symantec Endpoint Protection Manager**] を選択します。
確認メッセージが表示されます。
3. つの Symantec Endpoint Protection Manager [ホーム] ページのバナーの [起動] を押すと、クラウドコンソールにログインできます。
4. 登録後、すべてのデバイスがクラウドコンソールに表示されます。デバイスとは、クライアントを実行するクライアントコンピュータのことです。デフォルトでは、つの Symantec Endpoint Protection Manager でトポロジが管理されます。
5. クラウドコンソールからグループおよびデバイスを管理するには、ログオンしているドメインにのみ、[クラウドからデバイスを管理] をオンにします。クラウドベースのポリシーを管理するには、[クラウドからポリシーを管理する] をオンにします。これらのオプションは、クラウドコンソールの [エンドポイント] > [統合] > [登録] で有効にします。

Active Directory またはサードパーティの API を使用してデバイスを管理する場合は、[クラウドからデバイスを管理] を無効にしたままにする必要があります。

WARNING

デバイスグループの構造を変更すると、その変更は常に 10 分遅れてから つの Symantec Endpoint Protection Manager に表示されます。逆の場合も同様です。これは、つの Symantec Endpoint Protection Manager の複製機能の動作に似ています。遅延が発生している間は、それ以上トポロジを変更しないようにします。その変更が有効にならない場合があります。

つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録した後の処理

つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録した後の処理

Symantec Endpoint Security (SES) クラウドコンソールにおけるユーザーの作業環境は、つの Symantec Endpoint Protection Manager とは異なります。

ステップ 1: Symantec Security Cloud アカウントにサインオンする

クラウドコンソールにサインオンします。

[Symantec Security Cloud アカウントにサインイン](#)

「[Endpoint Security スタートガイド](#)」を参照してください。

登録後、つの Symantec Endpoint Protection Manager データはクラウドコンソールに同期されます。データには、クラウドコンソールがサポートするクライアント階層とポリシーが含まれています。同期は即時には行われません。クラウドコンソールでデバイスを参照するまでに一定期間待たなければならない場合があります。

ステップ 2: クライアントをクラウドのみで管理するか、つの Symantec Endpoint Protection Manager のみで管理するかを選択する

つの Symantec Endpoint Protection Manager クライアントコンピュータとクライアントグループは、[デバイス] ページでデバイスとしてクラウドコンソールに自動的に表示されます。デフォルトでは、デバイスはフラットリストに表示され、[デバイス] ページのグループには表示されません。

つの Symantec Endpoint Protection Manager クライアントは、クラウドコンソールで Symantec Agents と呼ばれます。

Symantec Endpoint Protection Manager が管理するデバイスを表示するには

1. クラウドで、[エンドポイント] > [デバイス] に移動します。
2. [デバイス] タブの [管理者] ドロップダウンメニューで、[Endpoint Protection Manager] を選択します。

デフォルトでは、つの Symantec Endpoint Protection Manager でデバイスの編成を管理します。クラウドコンソールまたは つの Symantec Endpoint Protection Manager でのみデバイスを管理できますが、両方で同時に管理することはできません。

クラウドコンソールからデバイスおよびグループを管理するには

1. [エンドポイント] > [統合] に移動します。
2. [登録] タブで、[クラウドからデバイスを管理] がオンになっていることを確認します。

NOTE

Active Directory またはその他のサードパーティのディレクトリツールでデバイスの編成を管理する場合は、この設定を無効のままにしてください。

NOTE

デバイスグループの構造を変更すると、その変更は常に 10 分遅れてから つの Symantec Endpoint Protection Manager に表示されます。逆の場合も同様です。これは、つの Symantec Endpoint Protection Manager の複製機能の動作に似ています。遅延が発生している間は、それ以上トポロジを変更しないようにします。その変更が有効にならない場合があります。

ステップ 3: ポリシーをクラウドのみで管理するか、つの Symantec Endpoint Protection Manager のみで管理するかを選択する

ポリシーは、クラウドコンソールの [エンドポイント] > [ポリシー] ページに自動的に表示されます。ICDm から環境を完全に管理する場合を除き、Symantec Endpoint Protection Manager からポリシーをエクスポートしてクラウドにインポートする必要はありません。

ドメイン登録後、クラウドコンソールは常に、ICDm から管理するサポートされているポリシーを制御します。

その他のポリシー (ホストインテグリティポリシーなど) を管理するには、引き続き つの Symantec Endpoint Protection Manager を使用します。ポリシーは つの Symantec Endpoint Protection Manager にプッシュされて、各クライアントに配布されます。

クラウドコンソールからデバイスを管理するには

- [エンドポイント] タブ > [統合] ページ > [登録] タブで、[クラウドからポリシーを管理] をオンにします。

ステップ 4: クラウドコンソールが検出した脅威を探す

クラウドコンソールの [ダッシュボード] リストと [検出された項目] リストには、環境内の検出に関するより包括的な情報が表示されます。ダッシュボードを使用して、ポリシー設定の結果を確認し、必要に応じてポリシー設定を調整します。

- [エンドポイント] > [ダッシュボード] > [SEP 14.2] に移動します。

[14.x Symantec Endpoint Protection Manager ドメイン登録済みクラウドコンソールの機能とオンプレミス Symantec Endpoint Protection Manager との比較](#)

ハイブリッド管理の つの Symantec Endpoint Protection Manager と Symantec Endpoint Security クラウドコンソールの連携方法

このセクションでは、つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録する際に発生する可能性がある動作をいくつか示します。

- [クラウドポータルと つの Symantec Endpoint Protection Manager 間の通信と登録](#)
- [ライセンス、インストール、アップグレード、データベース](#)
- [ドメインの登録と登録解除](#)
- [サイト、複製](#)
- [グループ、クライアント、場所](#)
- [ポリシーと継承](#)

クラウドコンソールと つの Symantec Endpoint Protection Manager 間の通信と登録

- つの Symantec Endpoint Protection Manager コネクタでクラウドコンソールへのアクセストークンを取得できない場合は、毎時間再試行されます。
- つの Symantec Endpoint Protection Manager から接続するクライアントの場合は、クラウドコンソールに正しいオンライン状態がすぐには表示されないことがあります。オンライン状態が変わってから 5 分から 10 分待ち、現在の状態が正確に反映されるかどうかを確認してください。

[クライアントが管理サーバーに接続され、保護されているかどうかの確認](#)

- 管理サーバーと Amazon Web Services (AWS) サーバーのシステム時間の差は 10 分以内である必要があります。その他の場合、登録は失敗し、次のエラーメッセージが表示されます。

```
Symantec Endpoint Protection Manager #####  
#### #####
```

時間の不一致を解決するには、つの Symantec Endpoint Protection Manager サーバーと NTP (Network Time Protocol) を同期してください。詳しくは、「[NTP: ネットワークタイムプロトコル](#)」を参照してください。

- 失敗した登録のトラブルシューティングを行うには、次のログを使用できます:

BRIDGE_INSTALL.log、catalinaWs.out、Cloud-0.log、scm-server-0.log、および semapisrv_access_log.date.log。これらのファイルはすべて つの Symantec Endpoint Protection Manager インストールフォルダ内の \tomcat\logs にあります。

つの Symantec Endpoint Protection Manager ドメイン (14.1 以降) をクラウドコンソールに登録する

負荷分散のための管理サーバーリストの設定

ライセンス、インストール、アップグレード、データベース

- Symantec Endpoint Security をクラウドコンソールで使用または登録するには、ライセンスを購入する必要があります。
- クラウドコンソールから管理サーバーをアップグレードすることはできません。
- クラウドからデータベースまたは 1 つの Symantec Endpoint Protection Manager 設定をバックアップまたは復元することはできません。
- ライセンスを解放するため、1 つの Symantec Endpoint Protection Manager データベースではドメインに接続していないクライアントが指定する日数に基づいて削除されます。クラウドコンソールで、これらの未接続のクライアントは 30 日を過ぎると自動的に削除されます。この間隔を設定することはできません。まず 1 つの Symantec Endpoint Protection Manager データベースのクライアントが削除され、次にクラウドコンソールのクライアントが削除されます。[データベースから使われなくなったクライアントをパージして使用可能なライセンスを増やす](#)

ドメインの登録と登録解除

ドメインを登録すると、以下のようになります。

- イベント、ポリシー、クライアント、およびクライアントグループが同期されます。
- クラウドでサポート対象のポリシー機能は、1 つの Symantec Endpoint Protection Manager の設定には使用できません。
- クラウドポリシー設定が優先します。

必要に応じて、デフォルトドメインを登録解除できます。たとえば、接続の問題が発生した場合や、クラウドコンソールでポリシーを管理する必要がない場合などです。1 つの Symantec Endpoint Protection Manager の登録ページ、またはクラウドコンソールの [エンドポイント] > [統合] > [登録] で登録解除できます。

登録解除処理により、クラウドの登録解除されたドメインのクライアントグループとクライアントが削除されます。関連するすべてのポリシーは、クラウドコンソールおよび関連するイベントに残ります。

Symantec Endpoint Protection Manager ドメインの登録解除

サイト、複製

- 各サイトに、クラウドコンソールのサイトあたり 1 つの 1 つの Symantec Endpoint Protection Manager ドメインを登録します。ドメインが別々のサイトに存在する場合でも、複数のドメインを登録することはできません。同じクラウドコンソールアカウントを使用している別々の 1 つの Symantec Endpoint Protection Manager ドメインを登録することもできません。
- SQL Server データベースを共有し、フェールオーバーが設定されている 2 台の 1 つの Symantec Endpoint Protection Manager が存在するサイトの場合は、いずれかの管理サーバーの 1 つのドメインを登録します。各管理サーバーとクラウドコンソール間で通信するブリッジサービスは、一度に 1 台の管理サーバーで実行されます。サービスは、まずサーバー優先度が高い管理サーバーで実行されます。最初のブリッジサービスがダウンすると、代わりに 2 台目の管理サーバーでサービスが実行されます。クラウドコンソールでは一度に 1 つのみのドメインを管理できます。クラウドコンソールと各管理サーバー間で同時に同期が行われます。

「[クラウドコンソールがサポートするサイト設定](#)」に、1 つの Symantec Endpoint Protection Manager ドメインを登録するときにクラウドコンソールがサポートするサイト設定を示します。

Table 170: クラウドコンソールがサポートするサイト設定

サイト設定	クラウドコンソールでのサポートの有無
1つのサイト、1台のコンピュータに1つの Symantec Endpoint Protection Manager、同じコンピュータ上のデータベースのみ	はい
1つのサイト、1台目のコンピュータに1つの Symantec Endpoint Protection Manager、2台目のコンピュータに Microsoft SQL Server データベース	はい
1つのサイト、複数の Symantec Endpoint Protection Manager	はい
複数のサイト、各サイトに1つの Symantec Endpoint Protection Manager、複製を利用*	はい (14.2 以降)
複数のサイト、各サイトに複数の Symantec Endpoint Protection Manager、複製を利用*	はい (14.2 以降)

* クラウドへの登録の際にサポートされる 1 つの Symantec Endpoint Protection Manager は、複製パートナーシップのいずれかのサイトで 1 つのみです。

クラウドコンソールで複製パートナーとして設定するサイトの登録

グループ、クライアント、場所

- クラウドコンソールの [My Company] の名前を変更しても、1 つの Symantec Endpoint Protection Manager のグループ名は変更されません。
- クラウド管理機能には、管理下クライアントが必要です。管理外クライアントを管理することも、クラウド機能を使用するポリシーを管理外クライアントに適用することもできません。クラウド機能を使用するポリシーを管理外クライアントに適用する場合、ポリシーは対応するレガシー Symantec Endpoint Protection オプションにデフォルト設定されます。
- バージョン 14、14 MP1、14 MP2、12.1.x レガシークライアントコンピュータがクラウドコンソールに表示されますが、新しいクラウドベースの機能はサポートされません。
- [クラウドからデバイスを管理] オプションがクラウドコンソールでオンになっている場合、クラウドコンソールでデバイスが管理されます。オフになっている場合、1 つの Symantec Endpoint Protection Manager でデバイスが管理されます。

Active Directory を 1 つの Symantec Endpoint Protection Manager で使用してグループとクライアントを管理する場合、自動的に 1 つの Symantec Endpoint Protection Manager でデバイスが管理されます。この場合、[クラウドからデバイスを管理] をクラウドコンソールに切り替えることはできません。この設定は、デバイス編成の制御を 1 つの Symantec Endpoint Protection Manager のみに戻します。どのグループのポリシー保護にも影響しません。高度なポリシー機能は引き続きクラウドコンソールから管理します。

- デバイスグループの構造を変更すると、その変更は常に 10 分遅れてから 1 つの Symantec Endpoint Protection Manager に表示されます。逆の場合も同様です。これは、1 つの Symantec Endpoint Protection Manager の複製機能の動作に似ています。遅延が発生している間は、それ以上トポロジを変更しないようにします。
- 特殊文字: \ * ? < > | : " を含むグループまたはポリシーをクラウドコンソールに追加する場合、これらの文字は 1 つの Symantec Endpoint Protection Manager でハイフン (-) に変換されます。たとえば、グループに「Europe***」という名前を付けると、このグループは 1 つの Symantec Endpoint Protection Manager で「Europe---」とラベル付けされます。
- クラウドコンソールは、14.3 以降のエージェントのロケーション認識をサポートします。以前のエージェントバージョンでは、1 つの Symantec Endpoint Protection Manager グループに場所が複数存在して、各場所のポリシー (共有または非共有) が異なる場合、デフォルトの場所のポリシーのみが同期され、クラウドコンソールの同等のグループに適用されます。続いて、クラウドコンソールから 1 つの Symantec Endpoint Protection Manager への逆方向の同期が完了すると、クラウドコンソールのそのグループのポリシーが、1 つの Symantec Endpoint Protection Manager の同等のグループのすべての場所に共有ポリシーとして適用されます。このプロセスは、1 つの Symantec Endpoint Protection Manager のメモリエクスプロイト緩和機能ポリシーと例外ポリシーの両方に適用されます。
- クラウドコンソールでは、IPv6 での接続をサポートしません。次のエラー結果 1 つの Symantec Endpoint Protection Manager の IPv6 ネットワーク経由の登録。:

#####

Symantec Endpoint Protection Manager #####

ポリシー

- クラウドからは、14.0.1 以降のクライアントのポリシー設定を管理できます。
14.0.1 より前のクライアントのポリシー設定は、引き続き つの Symantec Endpoint Protection Manager から直接管理する必要があります。ただし、例外があります。クラウドから例外ポリシーを適用し、クライアントで例外の種類がサポートされている場合、例外がバージョンに関係なくクライアントに適用されます。メモリエクスプロイト緩和機能ポリシーは、すべてのバージョン 14 以降のクライアントに適用されます。
- クラウドに由来するポリシーは、つの Symantec Endpoint Protection Manager のポリシー継承設定には従いません。その代りに、クラウドで設定されている継承ルールに従います。
- ウイルスとスパイウェアの対策ポリシーでは、ドメインがクラウドコンソールに登録される際にクラウドアイコンが一部のオプションの横に表示されます。集中保護ポリシーが有効になっている場合、ポリシーは 14.0.1 以降のクライアントでこれらのオプションを上書きします。
- クラウドコンソールで作成し割り当てる最初のデフォルトのクラウドポリシーには、Default MEM Policy v1 のように つの Symantec Endpoint Protection Manager で v と番号 (#) が付けられます。つの Symantec Endpoint Protection Manager ドメインに登録解除してから再登録すると、さらに v# がポリシー名に付けられます。たとえば、Default MEM Policy v1 は Default MEM Policy v1 v1 または Default MEM Policy v1 v3 のようになります。つの Symantec Endpoint Protection Manager 例外ポリシーとクラウドコンソールの拒否リストと許可リストポリシーの違いについては、次の項目を参照してください。
[Symantec Endpoint Protection Manager 例外ポリシーとクラウドコンソールの連携方法について](#)
- つの Symantec Endpoint Protection Manager では、一部のクラウドポリシーが [クライアント] > [ポリシー] タブのリストに表示されます。クラウドアイコンは、ポリシーがクラウドで生成されたことを示します。

Table 171: クラウドアイコン

アイコン	説明
	グループのポリシーは、クラウドコンソールの親から継承されていません。ポリシーはグループに直接適用されています。
	グループのポリシーは、クラウドコンソールの親から継承されています。

クラウドコンソールのポリシーは、新しいものもあれば、既存のポリシーのクラウドバージョンであるものもあります。クライアントがサポートするポリシーはクライアントのバージョンで決まります。ポリシーをサポートしていないクライアントにポリシーを適用すると、クライアントはポリシーを無視します。この動作は、ポリシーを生成した場所がクラウドコンソールでも つの Symantec Endpoint Protection Manager でも同様です。つの Symantec Endpoint Protection Manager のユーザーインターフェースでは、クラウドコンソールが制御するオプションまたはポリシー全体が示されます。

- ハイブリッド管理のクラウドコンソールでは、Windows クライアントの つの Symantec Endpoint Protection Manager ポリシーのみが現在サポートされていますが、Mac または Linux クライアントはサポートされていません。Mac および Linux クライアントは、クラウドから完全に管理するか、つの Symantec Endpoint Protection Manager から完全に管理する必要があります。

[14.x つの Symantec Endpoint Protection Manager ドメインに登録されたクラウドコンソールの機能とオンプレミス つの Symantec Endpoint Protection Manager の比較](#)

ポリシー継承

クラウドコンソールでは、子デバイスグループがその親デバイスグループからポリシーを継承します。ただし、子グループまたは子デバイスにはポリシーを直接適用できます。継承を無効にする必要はありません。

[14.x Symantec Endpoint Protection Manager ドメイン登録済みクラウドコンソールの機能とオンプレミス Symantec Endpoint Security との比較](#)

14.x での Symantec Endpoint Protection Manager ドメインに登録されたクラウドコンソールの機能とオンプレミスでの Symantec Endpoint Protection Manager の比較

での Symantec Endpoint Protection Manager ドメインの登録後は、クラウドコンソールとでの Symantec Endpoint Protection Manager (SEPM) の両方でポリシーを管理します。

Table 172: 機能リファレンス

での Symantec Endpoint Protection Manager	Symantec Endpoint Security
ようこそページ	ホームページ クラウドコンソールでは、クラウドコンソールの機能を理解できるように、初めてのユーザーエクスペリエンスをガイド付きで提供します
ホームページ	ダッシュボードページ コンソールダッシュボードには、疑わしいファイルの検出に関する詳細情報が表示されます。 このダッシュボードには、重要業績評価指標 (KPI) バーと、ドリルダウンの詳細を表示する対話型ウィジェット (グラフ) が含まれます。
クライアント、クライアントグループ ドメインのデバイスマスターオプション ([クラウドからデバイスを管理]) が有効な場合は、クラウドコンソールを使用してクライアントとクライアントグループを組織化する必要があります。 での Symantec Endpoint Protection Manager、Active Directory、またはサードパーティの API を使用してデバイスを管理する場合は、このオプションを無効にします。	デバイス、デバイスグループ デフォルトでは、での Symantec Endpoint Protection Manager によって管理されます。 クラウドからこれらのポリシーを管理するには、[エンドポイント] > [統合] > [登録] > [クラウドからデバイスを管理] オプションを選択します。このオプションは、グループの作成または削除、およびデバイスの移動または削除のみに影響します。この機能は、Active Directory がでの Symantec Endpoint Protection Manager と連携する方法と同様に機能します。 クラウドコンソールでデバイスおよびデバイスグループを表示できます。ドメインがクラウドに登録されていて、デバイスマスターオプションが有効になっている場合、での Symantec Endpoint Protection Manager でグループを作成することはできません。デバイスマスターオプションが有効になっている場合、グループ構造はクラウドで管理されます。
対応する設定はありません。	ポリシーグループ
ポリシー継承 での Symantec Endpoint Protection Manager で、子グループにポリシーを直接適用する場合、ポリシーの継承を無効にする必要があります。 注: ドメインの登録を解除する場合、での Symantec Endpoint Protection Manager 継承設定に関わらず、クラウドコンソールから直接子グループに適用した MEM ポリシーが子グループとその場所に適用されます。	ポリシー継承 クラウドコンソールで、ポリシー継承は常に有効です。ただし、ポリシーは、常に直接子ポリシーグループに適用して親ポリシーを上書きできます。

つの Symantec Endpoint Protection Manager	Symantec Endpoint Security
監視およびレポートページ	警告と調査ページ 警告とイベントのビューをフィルタ処理できます。両方のビューで、詳細情報を含むドリルダウンを利用できます。 デフォルトの警告ルールは、特定の警告をトリガすると管理者に通知します。ルール管理は、関連するイベントに関するアラートを受信する管理者を定義する方法を提供します。 [警告] > [警告ルール] で、事前定義済みの警告ルールを表示および編集できます。 イベントビューは、イベントをすばやく分析して、環境内のポリシーを調整する方法を決定するために役立ちます。調査ページでイベントを表示できます。
管理者ロール - システム管理者 - 管理者 (ドメインベース) - 限定管理者 (ポリシーベース) クラウドコンソール管理者と つの Symantec Endpoint Protection Manager 管理者はまったくリンクされていません。	管理者ロール - スーパー管理者 - ドメイン管理者 - 限定管理者 - ビューア
コンソールタイムアウト デフォルトは 1 時間です。このタイムアウトは変更できます。	コンソールタイムアウト このタイムアウト期間は変更できません。タイムアウトは 2 時間です。
[ハートビート] オプション	利用できません。 ポリシーの変更はすべてリアルタイムで行われます。

以下の表に、クラウドに登録されている つの Symantec Endpoint Protection Manager でポリシーと、各ポリシーをサポートする最低クライアントバージョンで利用可能なポリシーを示します。

注: バージョン 14.0.1 と 14.1 は同じバージョンです。14.01 Windows クライアントは 14.1 つの Symantec Endpoint Protection Manager と共にリリースされました。

Table 173: ポリシー機能リファレンス

つの Symantec Endpoint Protection Manager	Symantec Endpoint Security
すぐに使えるポリシー 以下のポリシーは つの Symantec Endpoint Protection Manager で引き続き管理されます。 - ファイアウォールポリシー - デバイス制御 - 侵入防止ポリシー - LiveUpdate のポリシー - ホストインテグリティポリシー - Bloodhound、SONAR ヒューリスティック、ダウンロードインサイト、およびスキャンアクション以外のウイルスとスパイウェアの対策ポリシー - アプリケーションとデバイス制御 - システムロックダウン	デフォルトでは つの Symantec Endpoint Protection Manager によって管理されます。 クラウドから以下のポリシーを管理するには、[エンドポイント] > [統合] > [登録] > [クラウドからポリシーを管理] を選択します。 - 集中保護ポリシー - システムポリシー (低帯域幅オプションのみ) - 許可リストポリシー - 拒否リストポリシー - MEM ポリシー 完全なクラウド管理型 Symantec Endpoint Security は、Symantec Endpoint Protection が管理しない追加のポリシーを管理します。 ICDm での Symantec Endpoint Protection 管理と Symantec Endpoint Security 管理機能のクイックリファレンス
ウイルスとスパイウェアの対策ポリシーのダウンロードインサイト、Bloodhound、SONAR の設定 ドメインがクラウドコンソールに登録されている場合、以下の設定は Symantec Endpoint Protection 14.1 以降のクライアントには適用できません。 - ウイルスとスパイウェアの対策ポリシーの検出処理 - Bloodhound の設定 - ダウンロードインサイトの重大度スライダー - ダウンロードインサイトの普及率、初回、イントラネットのオプション - SONAR のヒューリスティック検出、SONAR のアグレッシブモード、SONAR の疑わしい動作の設定 これらの設定は引き続きレガシークライアントに使用され、ドメインを登録解除した場合は 14.1 以降のクライアントにも使用されます。 注: デフォルトの集中保護の遮断レベルは、ウイルスとスパイウェアの対策ポリシーの Bloodhound 設定で最も積極的なものと比較すると、その積極性は低くなります。現在のポリシーで Bloodhound が最高レベルとして指定されている場合は、集中保護のレベルを増やす必要がある場合があります。	集中保護ポリシー (14.0.1 以降) ドメイン登録後に Windows クライアントに自動的に適用されます Windows クライアントに対するウイルスとスパイウェアの対策ポリシーの一部の設定を置き換えます。 これらのクライアントでは、集中保護ポリシーを使用して、ウイルスとスパイウェアの対策ポリシーの既存の特定の設定を置き換えます。 - Bloodhound - SONAR ヒューリスティック - ダウンロードインサイトオプション - スキャン処理 ただしクライアントは、他のオプションではウイルスとスパイウェアの対策ポリシーを引き続き使用します。
例外ポリシー つの Symantec Endpoint Protection Manager には、1 つの例外ポリシーがあります。このポリシーには、さまざまな項目の除外、およびアプリケーションの除外が含まれます。クラウドコンソールの許可リストポリシーと拒否リストポリシーは、つの Symantec Endpoint Protection Manager の個別ポリシーとして表示されます。 クラウドコンソールからのアイテムは、[例外ポリシー] > [例外] リストに表示されます。 ドメインが登録されている場合は、クラウドコンソールでサポートされていない種類に対する例外のみを作成できます。 Symantec Endpoint Protection Manager 例外ポリシーとクラウドコンソールの連携方法について	許可リストポリシー (14.0.1 以降) クラウドで作成する許可リストポリシーは、ドメインを登録解除していても つの Symantec Endpoint Protection Manager に表示されます。 クラウドコンソールには、許可リストまたは拒否リストに登録された項目の中央リストが含まれているため、これらのすべての項目をすべて 1 か所で表示できます。 14.3 RU1 で、ホワイトリストポリシーは許可リストポリシーに名前が変更されました。

つの Symantec Endpoint Protection Manager	Symantec Endpoint Security
例外ポリシー クラウドコンソールの拒否リストポリシーは、スキャンの例外ではありません。ただし、クラウドコンソールの拒否リストアイテムは、[例外] リストに表示されます。	拒否リストポリシー (14.0.1 以降) クラウドで作成する拒否リストポリシーは、ドメインを登録解除していても つの Symantec Endpoint Protection Manager に表示されます。 つの Symantec Endpoint Protection Manager またはクラウドコンソールで例外を設定できます。現在、クラウドコンソールではすべての範囲の例外がサポートされているわけではありません。 Note: 拒否リストポリシーは、つの Symantec Endpoint Protection Manager で SONAR 技術を使用してそのルールを強制適用する、アプリケーション制御の種類です。このポリシーは、つの Symantec Endpoint Protection Manager でアプリケーション制御ドライバを使用しません。 14.3 RU1 で、ブラックリストポリシーは拒否リストポリシーに名前が変更されました。
対応するオプションはありません。 つの Symantec Endpoint Protection Manager によって低帯域幅の状態が表示されます。低帯域幅オプションが有効になっているかどうかは、[外部通信] > [クラウド設定] で確認できます。 つの Symantec Endpoint Protection Manager は、低帯域幅が機能するのに必要な LiveUpdate AML コンテンツも管理します。	システムポリシー (低帯域幅オプション) (14.0.1 以降) システムポリシーは、つの Symantec Endpoint Protection Manager に対応する設定が存在しないクラウドの新しいポリシーです。ただし、このポリシーで低帯域幅オプションを機能させるには、低帯域幅の高度な機械学習 (AML) LiveUpdate コンテンツを つの Symantec Endpoint Protection Manager で利用できる必要があります。 デフォルトはオフです。
メモリエクスプロイト緩和機能 (MEM) ポリシー ドメインが登録されたら、クラウドコンソールを使用してこのポリシーを設定する必要があります。	エクスプロイト緩和機能ポリシー (MEM) ポリシー 14.0 以降 (全体的なポリシー機能の場合)。 14.0.1 以降 (各機能の設定の場合)。 14.2 RU1 (カスタムアプリケーションの場合)。アプリケーション分離を有効にする必要があります。クライアントにアプリケーション強化がインストールされている必要があります。 ポリシーオプションは つの Symantec Endpoint Protection Manager のオプションに相応します。

つの Symantec Endpoint Protection Manager 例外ポリシーとクラウドコンソールの連携方法について

例外ポリシーのクラウドコンソールでの動作について

クラウドコンソールでは、Symantec Endpoint Protection Manager でサポートされているすべての例外がサポートされているわけではありません。つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録した後、元の つの Symantec Endpoint Protection Manager 例外ポリシーは例外の種類に基づいてクラウドコンソールで 2 つのポリシーの種類に分けられます。これらのクラウドベースのポリシーはそれぞれ拒否リストポリシー、許可リストポリシーと呼ばれます。クラウドポリシーでサポートされていない例外は、Symantec Endpoint Protection Manager 例外ポリシーに残ります。クラウドコンソールと つの Symantec Endpoint Protection Manager が同期されると、クラウドベースのポリシーが つの Symantec Endpoint Protection Manager にインポートされます。

たとえば、つの Symantec Endpoint Protection Manager で SEPM Exceptions Policy] の順にクリックします。このポリシーには、アプリケーション例外、信頼できる Web ドメイン例外、および監視するアプリケーション例外が含まれます。クラウドコンソールに登録すると、SEPM Exceptions Policyのクラウドベースの例外が 2 つのポリシーに分けられます。これらのポリシーはそれぞれ Imported SEPM Exceptions Policy (BL) と Imported SEPM Exceptions Policy (WL)] の順にクリックします。拒否リストポリシーはアプリケーション例外でのみ作成され、許可リストポリシーはアプリケーション例外とドメイン例外で作成されます。元の つの Symantec Endpoint Protection Manager の SEPM Exceptions Policyは監視するアプリケーション例外を保持します。クラウドコンソールを つの Symantec Endpoint Protection Manager と同期すると、つの Symantec Endpoint Protection Manager には同じグループに割り当てられている 3 つのポリシー (SEPM Exceptions Policy, Imported SEPM Exceptions Policy (DL) v1、Imported SEPM Exceptions Policy (AL) v1

クラウドコンソールで、ブラックリストポリシーは許可リストポリシーに名前が変更されました。ホワイトリストポリシーは許可リストポリシーに名前が変更されました。

ウイルスとスパイウェアのスキンの例外作成

また、クラウドコンソールの許可リストポリシーと拒否リストポリシーでは、つの Symantec Endpoint Protection Manager 例外ポリシーでサポートされているすべての処理がサポートされているわけではありません。クラウドコンソールの許可リストポリシーのアプリケーション例外では、[無視] 処理のみがサポートされています。クラウドコンソールの拒否リストポリシーのアプリケーション例外では、[検疫] 処理のみがサポートされています。アプリケーション例外を つの Symantec Endpoint Protection Manager 例外ポリシーに追加してから、つの Symantec Endpoint Protection Manager をクラウドコンソールに登録すると、処理がクラウドコンソールのポリシーで自動的に変更されます。[ログのみ] 処理は、許可リストポリシーの [無視] 処理に変換されます。[終了] 処理と [削除] 処理は、[検疫] 処理に変換されます。これらのポリシーが つの Symantec Endpoint Protection Manager にインポートされると、管理サーバーではクラウドコンソールのポリシーからの処理が維持されます。

Windows クライアントのアプリケーションの例外を作成するためのアプリケーションの監視

クラウドコンソール上のサポート対象の例外とサポート対象外の例外について

クラウドコンソールでは、Windows クライアント上の次の例外がサポートされています。

拒否リストポリシー:

- ハッシュ (SHA-256)

許可リストポリシー:

- 証明書
- ファイル名
- ドメイン
- ハッシュ
- ファイルパス
- 拡張子
- IPS ホスト

つの Symantec Endpoint Protection Manager をクラウドコンソールに登録すると、つの Symantec Endpoint Protection Manager 例外ポリシーの Windows 例外が次のポリシータイプと例外タイプに変換されます。

Table 174: Windows 例外と、クラウドコンソール例外への変換処理

つの Symantec Endpoint Protection Manager 例外ポリシー	拒否リストポリシー	許可リストポリシー
アプリケーション	ハッシュ (SHA-256 のみ)	ハッシュ (SHA-256 のみ)
証明書	なし	証明書
[ファイル] > [セキュリティリスク/SONAR]	なし	ファイル名
[フォルダ] > [セキュリティリスク/SONAR]	なし	パス
信頼できる Web ドメイン	なし	ドメイン

次の Windows 例外は つの Symantec Endpoint Protection Manager 例外ポリシーに残り、クラウドコンソールでサポートされません。

-
- 監視するアプリケーション
 - 拡張子
 - ファイル - アプリケーション制御
 - フォルダ - アプリケーション制御
 - 既知のリスク
 - 改変対策例外
 - DNS またはホストファイルの変更例外

クラウドコンソールでは、Linux クライアント例外も Mac クライアント例外もサポートされていません。Linux 例外アイテムと Mac 例外アイテムはすべて つの Symantec Endpoint Protection Manager 例外ポリシーに残ります。

NOTE

例外をクラウドコンソールに直接追加するには、つの Symantec Endpoint Protection Manager からエクスポートするチェックサムのある .csv ファイルを使用します。ファイルフィンガープリントリストには、コンピュータ上の指定されたパスに存在する各実行可能ファイルまたは DLL のパス、ファイル名、対応するチェックサムが含まれます。「[checksum.exe を使ったファイルフィンガープリントリストの作成](#)」を参照してください。

使用する Windows 例外と、適用するスキャンの種類について

ユーザーが **Windows** クライアントで追加できる例外

つの Symantec Endpoint Protection Manager 例外ポリシーにより、Windows クライアント上のユーザーはクライアント制限と呼ばれる例外を追加することができます。

つの Symantec Endpoint Protection Manager がクラウドコンソールに登録されている場合、つの Symantec Endpoint Protection Manager には次のクライアント制限は表示されません。

- アプリケーション例外
- ファイル例外
- [フォルダ例外] > [セキュリティリスク例外/SONAR 例外]
- 信頼できる Web ドメインの例外
- 証明書例外

NOTE

また、クラウドベースの例外ポリシーで制御される Windows クライアントで、これらの例外はクライアントユーザーインターフェースに表示されません。

つの Symantec Endpoint Protection Manager には、つの Symantec Endpoint Protection Manager が登録されているかどうかに関係なく、次のクライアント制限は表示されません。

- DNS またはホストファイルの変更例外
- 拡張子例外
- 既知のリスク例外

クライアントコンピュータでユーザーが設定できる例外の種類の制限

例外ポリシーのクラウドコンソールへの登録と、クラウドコンソールとの同期の問題

- 拒否リストポリシーまたは許可リストポリシーがクラウドコンソールで自動的に作成されるのは、元の つの Symantec Endpoint Protection Manager 例外ポリシーに、拒否リストポリシーと許可リストポリシーでサポートされている例外が含まれている場合のみです。その他の場合、クラウドコンソールでは例外ポリシーが無視されます。
- 登録後、割り当て済みの つの Symantec Endpoint Protection Manager 例外ポリシーのみがクラウドコンソールと同期され、その後 つの Symantec Endpoint Protection Manager にインポートされます。未割り当てのポリシーは、非クラウドベースの例外ポリシーとして つの Symantec Endpoint Protection Manager に残ります。また、割り当て済みの つの Symantec Endpoint Protection Manager 例外ポリシーに拒否リストの例外または許可リストの例外が存在しない

場合は、対応する空の拒否リストポリシーや空の許可リストポリシーがそのグループのクラウドコンソールで作成されます。

- 登録後、つの Symantec Endpoint Protection Manager で非クラウドベースの例外ポリシーを作成し、割り当てることができます。ただし、これらのポリシーにはクラウドベースの例外ではなく、つの Symantec Endpoint Protection Manager ベースの例外のみを含める必要があります。クラウドベースの拒否リストポリシーまたは許可リストポリシーを作成して割り当てると、これらのポリシーは同期され、つの Symantec Endpoint Protection Manager にインポートされます。
- クラウドコンソールで作成した例外ポリシーは、ドメインを登録解除した後は つの Symantec Endpoint Protection Manager に残ります。ただし、クラウドベースのポリシーは つの Symantec Endpoint Protection Manager のグループから割り当て解除されます。必要がなくなったら、各ポリシーをマージ、再割り当て、または削除できます。
- クラウドコンソールにインポートした つの Symantec Endpoint Protection Manager 例外ポリシーにアプリケーションの例外がある場合、インポート後に例外が失われます。アプリケーションの例外をクラウドコンソールの拒否リストポリシーや許可リストポリシーに手動で再び追加する必要があります。クラウドコンソールでは、証明書の例外など、他の種類の例外も保守します。

クラウドコンソールで複製パートナーとして設定するサイトの登録

- [クラウドポータルでサイトを登録するには](#)
- [クラウドポータルで登録されたサイト間での複製の削除と復元](#)
- [クラウドポータルでのサイト複製のトラブルシューティング](#)

クラウドコンソールでサイトを登録するには

バージョン 14.2 以降、クラウドコンソールに登録されている 1 つのサイトと登録されていない追加サイトの間の複製を設定できます。1 つのサイトをマスターサイトとして登録します。その他すべてのサイトは、マスターサイトを直接複製したり互いに複製したりできます。たとえば、サイト A がマスターサイトである場合、サイト A をクラウドコンソールに登録します。サイト A を複製するようにサイト B とサイト C を設定します。または、サイト A を複製するようにサイト B を設定し、サイト B を複製するようにサイト C を設定できます。

Table 175: 複製するサイトを複数登録するプロセス

タスク	説明
ステップ 1: クラウドコンソールに登録する前に、2 つのサイトを複製します。	データベースの競合を回避するため、マスターサイトを登録する前に、すべてのポリシー、グループ、ログイベントを複製します。 クラウドにマスターサイトを登録した後も、複製パートナーを追加できます。 マスターサイトは複数のパートナーサイトを持つことができます。 即座に実行されるデータの複製 サイトの概要と複製の仕組み
ステップ 2: マスターサイトを登録します。	登録やポリシーの作成などの処理を実行するために、1 つのサイトをマスターサイトとして選択して登録します。 複数の管理サーバーがあるサイトでは、管理サーバーのいずれか 1 台のみ登録する必要があります。追加の管理サーバーは自動的に登録されます。 2 番目のサイトまたはパートナーサイトはクラウドコンソールに登録しません。

タスク	説明
ステップ 3: 同期の完了を待機します。	登録済みのマスターサイトとクラウドコンソールが同期した後、以下のイベントがマスターサイトで発生します。 - ブリッジサービスが、すべての管理サーバーに自動的にインストールされます。ただし、ブリッジサービスは、クラウドコンソールで登録するのに使用した管理サーバーでのみアクティブになります。 - マスターサイトは、レポートイベントをクラウドコンソールと同期します。 - マスターサイトは、このサイトに接続されないすべてのクライアントのグループ、デバイス、ポリシー、ログイベント、クライアントパッケージ、定義をアップロードします。 - マスターサイトは、クラウドコンソールからポリシー、ログ、コマンドを受信し、すぐにこのサイトと通信するクライアントにデータを渡します。 つの Symantec Endpoint Protection Manager ドメインをクラウドコンソールに登録した後の処理
ステップ 4: マスターサイトとパートナーサイトを複製します。	両方のサイトが同じ登録データを持つように複製のスケジュールを設定します。複製後、パートナーサイトで以下のイベントが発生します。 - パートナーサイトは、マスターサイトとの複製のスケジュールに基づいて、クラウドコンソールからコンテンツを受信します。パートナーサイトに接続されるクライアントが、このデータを受信します。 - パートナーサイトはマスターサイトから登録の詳細を取得します。これらの詳細は、[クラウド] ページ > [トラブルシューティング] ページに表示されます。 - パートナーサイトの管理サーバーはブリッジサービスをインストールしません。このため、パートナーサイトは直接クラウドコンソールと同期しません。 複製のための 2 番目のサイトのインストール方法
ステップ 5: (省略可能) グループとデバイスの制御をクラウドコンソールに切り替えます。	デフォルトでは、複製されない 1 つの Symantec Endpoint Protection Manager ドメインに登録するときは、クラウドコンソールがクライアントのグループ構造を管理します。デフォルトでは、複製されるサイトを登録するときは、1 つの Symantec Endpoint Protection Manager がグループ構造を管理します。 1 つの Symantec Endpoint Protection Manager がマスターの場合、グループとポリシーをマスターサイトに追加できます。これがパートナーサイトで複製されます。 - クラウドコンソールをマスターにする場合、最初にパートナーサイトとの複製を実行します。この複製で、パートナーサイトに追加したグループとポリシーを確実にクラウドコンソールと同期できます。 クラウドコンソールに制御を切り替えるには、登録完了後にクラウドコンソールの [設定] > [1 つの Symantec Endpoint Protection Manager の登録] で [デバイスの管理] オプションを有効にします。

複製されるパートナーのフェールオーバーや負荷分散は実行できません。

フェールオーバーと負荷分散の設定

クラウドコンソールで登録されたサイト間での複製の削除と復元

マスターサイトとパートナーサイトの間のパートナーシップを削除する場合、クラウドコンソールとの関係も削除します。

マスターサイトとのパートナーシップを復元するには、[既存の複製パートナーを追加] ウィザードを使用します。

パートナーサイトを個別のサイトとして直接クラウドコンソールに登録することもできます。この場合、別の Symantec Cyber Defense Manager アカウントを作成する必要があります。マスターサイトとのパートナーシップを復元するには、パートナーサイトの登録を解除する必要があります。そして、マスターサイトで、管理サーバー設定ウィザードを使用してパートナーシップを再設定します。

NOTE

ベストプラクティスとしては、パートナーサイトは個別のサイトとして維持し、マスターサイトとの複製を復元しようとししないでください。

アップグレード前後での、複製の無効化と復元

1 つの Symantec Endpoint Protection Manager の再インストールまたは再設定

クラウドコンソールでのサイト複製のトラブルシューティング

マスターサイト登録と複製に関する情報を確認するには

-
- 複製イベントを検索します。
マスターサイトで [システムログ] からログの種類が [管理] のログを開き、イベントの種類が [複製イベント] のイベントを検索します。
[ログの表示](#)
 - パートナーサイトの登録の状態を確認します。
パートナーサイトでは、[登録の状態] は [登録済み] と表示されます。
[接続の状態] などの他のフィールドには [なし] と表示されます。
登録情報を表示するには、[クラウド] ページ > [トラブルシューティング] をクリックします。

低帯域幅環境でのクライアントのアップデート

低帯域幅モードとは

14.1 以降で、低帯域幅モードは、次の条件を少なくとも 1 つ満たす環境用に新しく導入されたオプションです。

- ウイルスとスパイウェア、SONAR、IPS のコンテンツで必要なアップデートの頻度が少ない
- クラウドへの接続性が低い

低帯域幅クライアントは、アップデートを受け取る頻度が少なくなります。シマンテック社による低帯域幅コンテンツのアップデートは、週に 1 度行われます。低帯域幅モードでは、アグレッシブモードポリシーを使用して、エンドポイントのセキュリティをさらに調整することができます。

[Symantec Endpoint Protection が高度な機械学習を使用する仕組み](#)

低帯域幅オプションを使用するためには、クラウドコンソールに登録する必要があります。低帯域幅モードはデフォルトではオフになっています。

- クラウドコンソールのデフォルトシステムポリシー (14) で、低帯域幅モードを有効にします。
- LiveUpdate で低帯域幅コンテンツがダウンロードされることを確認します。

[低帯域幅コンテンツのダウンロード](#)

- 低帯域幅コンテンツを受け取るクライアントグループを作成します。

[低帯域幅クライアント用グループの作成](#)

低帯域幅モードを有効にすると、[デフォルト] ビューと [保護技術] ビューの [クライアント] タブにその状態が表示されます。また、低帯域幅コンテンツ配布に基づいてレポートを生成することもできます。

[低帯域幅モードで実行されるクライアントに関するレポートの実行](#)

クラウドからの低帯域幅モードの有効化

クラウドコンソールのシステムポリシーで低帯域幅モードを有効または無効にします。

- Symantec Endpoint Security コンソールで、[エンドポイント] > [ポリシー] > [デフォルトシステムポリシー (14)] に移動します。製品の体験版または購入バージョンが必要です。
- [低帯域幅モードで実行] をオンにします。
- [ポリシーの保存] をクリックします。

低帯域幅コンテンツを つの **Symantec Endpoint Protection Manager** にダウンロードします

デフォルトでは、高度な機械学習コンテンツがダウンロードされて有効化されます。次の手順を使用して、それらのコンテンツが有効かどうかを確認できます。

低帯域幅コンテンツを つの **Symantec Endpoint Protection Manager** にダウンロードするには

- つの Symantec Endpoint Protection Manager コンソールで、[管理] > [ローカルサイト] > [サイトプロパティを編集] の順にクリックします。
- [LiveUpdate] タブをクリックして選択し、次に [ダウンロードするコンテンツの種類] の隣の [選択項目の変更] をクリックします。
- [高度な機械学習] の隣のボックスのチェックマークが付いていることを確認します。

-
4. [OK] > [OK] をクリックして変更を保存します。

LiveUpdate コンテンツポリシーに低帯域幅コンテンツを含めるには

つの Symantec Endpoint Protection Manager コンソールで、[ポリシー] > [LiveUpdate] と移動して、低帯域幅が有効なクライアントが含まれるグループに割り当てられているポリシーを編集します。

1. [LiveUpdate コンテンツ] をクリックして、[LiveUpdate コンテンツポリシー] をダブルクリックします。
2. [Windows の設定] の下で、[セキュリティ定義] をクリックします。
3. クラウドコンソールで、[デバイス] をクリックし、子グループを [My Company] の下に追加します。
4. [高度な機械学習] ボックスのチェックマークが付いていることを確認します。
5. [OK] をクリックして、変更を保存します。

低帯域幅クライアント用グループの作成

1. クラウドコンソールで、[デバイス] をクリックし、子グループを [My Company] の下に追加します。
子グループを追加できない場合は、クラウドコンソールで [デバイスの管理] を有効にします ([設定] > [つの Symantec Endpoint Protection Manager の登録])。それ以外の場合は、つの Symantec Endpoint Protection Manager でグループを追加します。Active Directory の同期を使用する場合は、Active Directory からグループを追加します。
2. 低帯域幅用に以前設定したグループにシステムポリシーを適用します。デバイスグループで [ポリシーの適用] をクリックし、システムポリシーを追加して [送信] をクリックします。
3. つの Symantec Endpoint Protection Manager コンソールで、以前に設定した LiveUpdate Content Policy が作成済みグループに適用されていることを確認します。つの Symantec Endpoint Protection Manager で有効または無効にしたポリシー継承は、クラウドコンソールのデバイスポリシーではなく、つの Symantec Endpoint Protection Manager ポリシーにのみ適用されます。

クラウドコンソールからのグループの同期が完了するまで、時間がかかる場合があります。

低帯域幅モードで実行されるクライアントに関するレポートの実行

レポートを実行して、低帯域幅コンテンツを受け取るクライアントを一覧表示できます。

1. つの Symantec Endpoint Protection Manager コンソールで [レポート] > [クイックレポート] をクリックして、次のように選択します。
 - レポートの種類: コンピュータの状態
 - レポートの選択: 低帯域幅コンテンツ配布
2. 時間範囲の選択: その他のオプションの追加設定。
3. [レポートの作成] をクリックします。

クラウドコンソールから つの Symantec Endpoint Protection Manager ドメインを登録解除する

登録解除処理により、クラウドの登録解除されたドメインのクライアントグループとクライアントが削除されます。関連するすべてのポリシーは、クラウドコンソールおよび関連するイベントに残ります。

ICDm クラウドコンソールから つの Symantec Endpoint Protection Manager ドメインの登録を解除すると、以下の作業ができなくなります。

- クラウドコンソールからデバイスを管理する。
- デバイス上のファイルとアプリケーションを参照する。
- デバイスおよびデバイスグループにクラウドに固有のポリシーを適用して保護する。

登録解除プロセス中は、クラウドコンソールに通知が表示され、次の作業ができなくなります。

- デバイス管理に関連する機能 (グループの作成、グループの削除、グループ間でのデバイスの移動など) を実行する。
- ポリシー管理に関連する機能 (デバイスまたはデバイスグループへのポリシーの適用など) を実行する。
- 現在のドメインが登録解除されるまで新しいドメインを登録する。

NOTE

ドメインを登録解除するにはエンドポイントコンソールのスーパー管理者ロールが必要です。

管理者アカウントの作成

登録の解除後も、警告、イベント、およびポリシーをクラウドコンソールで引き続き参照できます。

つの Symantec Endpoint Protection Manager ドメインを登録解除するには

1. Endpoint Security クラウドコンソールで、[エンドポイント] > [統合] に移動します。
2. [登録] タブで、[ドメイン登録の状態] > [登録済み] チェックボックスを選択し、[登録解除] を選択します。
3. 適切なオプションを選択します。
 - 登録解除 - このオプションは、クラウドコンソールから 1 つの Symantec Endpoint Protection Manager の登録解除のみを行う場合に選択します。
 - 登録解除して削除 - このオプションは、クラウドコンソールから 1 つの Symantec Endpoint Protection Manager を登録解除して、検出されたデバイスとファイルの情報をすべて削除する場合に選択します。
4. テキストボックスに「登録解除」と入力して確定します。
5. [ドメインの登録解除] を選択します。

NOTE

通常、登録解除の完了には 2 時間かかります。

[1 つの Symantec Endpoint Protection Manager ドメイン \(14.1 以降\) をクラウドコンソールに登録する](#)

Symantec Endpoint Protection の仮想インフラストラクチャでの使用

Symantec Endpoint Protection では、仮想インフラストラクチャ向けに共有インサイトキャッシュと仮想イメージ例外の機能が提供されています。これらの機能を有効にすると、パフォーマンスが向上します。これらの機能を有効にするために、いくつかのインストールタスクと設定タスクを追加で実施する必要があります。

Table 176: 仮想インフラストラクチャ機能とその使用

機能と使用	説明
共有インサイトキャッシュを使って、クリーンであることが確認されているファイルのスキャンをスキップできます。	共有インサイトキャッシュは、クリーンであると認識されているファイルを記録します。共有インサイトキャッシュは、それらのファイルを再スキャンの対象からはずすことで、スキャンの負荷を減らすことができます。 次の種類の共有インサイトキャッシュを設定できます。 ネットワークベースの共有インサイトキャッシュ 任意の種類の仮想インフラを使う仮想クライアントは、ネットワークベースの共有インサイトキャッシュを使ってスキャン負荷を低減できます。 Note: 14.0 では、vShield 対応の共有インサイトキャッシュはサポートされなくなりました。 共有インサイトキャッシュについて ネットワークベースの共有インサイトキャッシュを使用するために必要な準備
仮想イメージ例外ツールを使って、クライアントは基本イメージファイルのスキャンをスキップできます。	仮想イメージ例外ツールでは、基本イメージファイルを安全であるとマーキングし、スキャンの負荷を減らすためにそれらのファイルをスキャン中にスキップできます。 仮想イメージ例外ツールは仮想環境でのみ動作します。 仮想イメージ例外ツールについて
非永続的な仮想デスクトップインフラストラクチャ機能を設定します。	Symantec Endpoint Protection クライアントには、非永続的な仮想クライアントであることを示すための設定があります。非永続的な仮想デスクトップインフラストラクチャに含まれるオフラインの GVM 用に、個別の期間を設定できます。つの Symantec Endpoint Protection Manager は、指定された期間よりも長い間オフラインであった非永続的な GVM クライアントを削除します。 非永続的な仮想デスクトップインフラストラクチャでの Symantec Endpoint Protection の使用ライセンスを開放するための使われなくなった非永続的 VDI クライアントのパージ

仮想インフラストラクチャでの つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection の保護技術は、通常、物理環境と同じように機能します。仮想インフラストラクチャでの つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection のクライアントのインストール、設定、使用は、物理環境と同じように行えます。

共有インサイトキャッシュについて

共有インサイトキャッシュを使うと、仮想インフラストラクチャのパフォーマンスが向上します。Symantec Endpoint Protection クライアントによってクリーンであると判断されたファイルは、キャッシュに追加されます。同じウイルス定義バージョンを使ったその後のスキャンでは、共有インサイトキャッシュにあるファイルのスキャンをスキップできます。共有インサイトキャッシュは、定時スキャンと手動スキャンでのみ使用されます。

ネットワークベースの共有インサイトキャッシュは、Symantec Endpoint Protection クライアントに依存しない Web サービスとして実行されます。共有インサイトキャッシュは投票システムを使います。最新のコンテンツを使ってファイルをスキャンし、そのファイルがクリーンであると判断されたら、クライアントはキャッシュに投票を送ります。ファイルがクリーンでない場合、クライアントは投票を送りません。ファイルの投票数が投票数のしきい値以上になったときに、共有インサイトキャッシュはファイルをクリーンであると判断します。他のクライアントが続いて同じファイルを送

キャンする必要がある場合、そのクライアントはまず共有インサイトキャッシュに問い合わせます。現在のコンテンツに対してファイルがクリーンであるとマークされた場合、クライアントはそのファイルをスキャンしません。

クライアントが共有インサイトキャッシュに投票を送るときに、キャッシュはファイルをスキャンするのにクライアントが使ったコンテンツのバージョンを確認します。クライアントに最新のコンテンツがない場合、共有インサイトキャッシュは投票を無視します。より新しいコンテンツが利用可能な場合、新しいコンテンツが既知の最新コンテンツとなり、Shared Insight は投票数を 1 に戻します。

キャッシュサイズを管理可能なサイズに維持するため、Shared Insight Cache はプルーニングアルゴリズムを使います。このアルゴリズムでは、最も古いタイムスタンプが付いた、最も古いキャッシュエントリから先に削除されます。このアルゴリズムにより、キャッシュサイズがメモリ使用量のしきい値を超えないことが保証されます。

ネットワークベースの共有インサイトキャッシュを使用するために必要な準備

共有インサイトキャッシュ設定のカスタマイズ

Symantec Endpoint Protection の仮想インフラストラクチャでの使用

仮想イメージ例外ツールについて

仮想イメージ例外ツールを使うと、クライアントによる基本イメージファイルの脅威のスキャンを省略できます。この機能は、ディスク I/O と CPU のリソースの負荷を減らします。

Symantec Endpoint Protection は、管理下クライアントと管理外クライアントの両方に対する仮想イメージ例外ツールの使用をサポートしています。

NOTE

物理環境での仮想イメージ例外ツールの使用はサポートされません。

基本イメージへの仮想イメージ例外ツールの使用

Symantec Endpoint Protection の仮想インフラストラクチャでの使用

ネットワークベースの共有インサイトキャッシュを使用するために必要な準備

ネットワークベースの共有インサイトキャッシュを使用して、スキャンパフォーマンスを高めることができます。

Table 177: ネットワークベースの共有インサイトキャッシュをインストールして使用するためのタスク

手順	タスク
手順 1: 共有インサイトキャッシュをインストールします。	ネットワークベースの共有インサイトキャッシュを実装するためのシステム必要条件 ネットワークベースの共有インサイトキャッシュのインストールとアンインストール
手順 2: つの Symantec Endpoint Protection Manager のウイルスとスパイウェアのポリシーで、仮想クライアントでの共有インサイトキャッシュの使用を有効にします。	ネットワークベースの共有インサイトキャッシュの使用の有効化

共有インサイトキャッシュをインストールすると、省略可能なオプションとして次のタスクを実行できます。

- 共有インサイトキャッシュのサービス、キャッシュ、ログ設定をカスタマイズします。
共有インサイトキャッシュ設定のカスタマイズ
- ログで、関連するイベントを参照します。

ネットワークベースの共有インサイトキャッシュのログイベント

- Windows Performance Manager を使用してパフォーマンスを監視します。

ネットワークベースの共有インサイトキャッシュパフォーマンスカウンタの監視

ネットワークベースの共有インサイトキャッシュを実装するためのシステム必要条件

ネットワークベースの共有インサイトキャッシュサーバーは、スタンドアロンの物理または仮想マシンで実行する設計になっています。つの Symantec Endpoint Protection Manager または Microsoft SQL Server のような他のデータベースアプリケーションまたは高可用性サーバーアプリケーションを実行するシステムへの共有インサイトキャッシュのインストールは推奨されません。

以下の表に、仮想インフラストラクチャで共有インサイトキャッシュを実行するために必要なシステムの最小必要条件を示します。

Table 178: ネットワークベースの共有インサイトキャッシュのシステム必要条件

必要条件	説明
ソフトウェア	- Windows Server 2003 (12.1 から 12.1.4 のみ) - Windows Server 2008 以降 - Windows Server 2012 と Windows Server 2012 R2 (12.1.5 以降) - Windows Server 2016 (14.2 MP1 現在) - Windows Server 2019 (14.2 MP1 現在) .NET Framework 4
CPU	共有インサイトキャッシュは、専用サーバーまたは仮想マシンにインストールする必要があります。
メモリ	最低 2 GB
使用できるディスク領域	最低 100 MB

共有インサイトキャッシュについて

ネットワークベースの共有インサイトキャッシュのインストールとアンインストール

ネットワークベースの共有インサイトキャッシュのインストールとアンインストール

ネットワークベースの共有インサイトキャッシュをインストールする前に、すべてのシステム必要条件を満たしていること、Windows の管理者としてログオンしていることを確認してください。共有インサイトキャッシュをスタンドアロンの物理または仮想マシンにインストールして実行します。

NOTE

共有インサイトキャッシュをインストールするサーバーのホスト名には、DBCS 文字または high-ASCII 文字を使わないでください。また、サーバーにアクセスするのに使うユーザー名に DBCS 文字または high-ASCII 文字を使うことも避けてください。これらの文字を使用すると、共有インサイトキャッシュが起動に失敗します。

ネットワークベースの共有インサイトキャッシュを実装するためのシステム必要条件

ネットワークベースの共有インサイトキャッシュをインストールするには

1. Symantec Endpoint Protection インストールファイルで、Tools/Virtualization/SharedInsightCache フォルダに移動します。
2. 次のファイルをダブルクリックして、インストールプログラムを起動します。

SharedInsightCacheInstallation.msi

NOTE

代わりに、次のコマンドを入力して、同じインストールプログラムを起動できます。

```
msiexec /i SharedInsightCacheInstallation.msi
```

3. [共有インサイトキャッシュの設定] ウィザードのパネルで、[次へ] をクリックします。
4. シマンテックソフトウェア使用許諾契約を読み、[使用許諾契約の条項に同意します] にチェックマークを付け、[次へ] をクリックします。
5. [インストール先フォルダ] パネルで、次のいずれかのタスクを実行します。
 - [次へ] をクリックして、共有インサイトキャッシュのデフォルトの場所を受け入れます。
 - [変更] をクリックし、別のインストール先フォルダに移動してそのフォルダを選択し、[OK] をクリックして [次へ] をクリックします。
6. [共有インサイトキャッシュの設定] ペインで、次の共有インサイトキャッシュ設定を指定します。

キャッシュの使用量 (物理メモリの割合)	キャッシュの最大サイズ。 キャッシュがこのしきい値を超えると、共有インサイトキャッシュはキャッシュサイズをプルーニングします。
応答準備ポート	サーバーが応答準備するポートです。
状態応答準備ポート	サーバーがサーバーの状態を伝えるために使うポートです。

7. [インストール] をクリックします。
8. インストールが完了したら、[完了] をクリックします。

共有インサイトキャッシュ設定のカスタマイズ

共有インサイトキャッシュのアンインストールには共有インサイトキャッシュサービスの停止と同じ効果があります。共有インサイトキャッシュを完全にアンインストールしてよいかどうか確かでない場合は、代わりにこのサービスを停止することができます。

ネットワークベースの共有インサイトキャッシュサービスの停止と開始について

NOTE

共有インサイトキャッシュをアンインストールするには、[プログラムの追加と削除] などの適切な Windows コントロールパネルを使います。共有インサイトキャッシュをアンインストールするには、Windows の管理者権限が必要です。

共有インサイトキャッシュをアンインストールする場合は、つの Symantec Endpoint Protection Manager の共有インサイトキャッシュを無効にすることもできます。共有インサイトキャッシュを無効にすると、クライアントがキャッシュとのやり取りに失敗しても、Windows のイベントログは通知を受信できません。

ネットワークベースの共有インサイトキャッシュの使用の有効化

ネットワーク上の Symantec Endpoint Protection クライアントとの通信では、共有インサイトキャッシュはデフォルトでは認証と SSL を使いません。共有インサイトキャッシュの設定を SSL を使用する基本認証または SSL を使用しない基本認証に変更する場合は、共有インサイトキャッシュにアクセスできるユーザー名とパスワードを指定する必要があります。

共有インサイトキャッシュ設定のカスタマイズ

ネットワークベースの共有インサイトキャッシュの使用を有効にするには

1. つの Symantec Endpoint Protection Manager コンソールで、適切なウイルスとスパイウェアの対策ポリシーを開き、[その他] をクリックします。
2. [共有インサイトキャッシュ] タブで、[ネットワークを使用する共有インサイトキャッシュ] にチェックマークを付けます。
3. 設定ファイルの SSL 認証を有効にした場合は [SSL が必要] をクリックします。
4. [ホスト名] フィールドに、共有インサイトキャッシュをインストールしたホストの名前を入力します。
5. [ポート] フィールドに、共有インサイトキャッシュのポート番号を入力します。
6. 共有インサイトキャッシュの認証を設定した場合 (省略可能):
 - [ユーザー名] フィールドにユーザー名を入力します。
 - [パスワードの変更] をクリックして、デフォルトのパスワード (null) を認証のために作成したパスワードに変更できます (省略可能)。パスワードを使わない場合は、これらのフィールドを空のままにします。
7. [OK] をクリックします。

ネットワークベースの共有インサイトキャッシュを使用するために必要な準備

共有インサイトキャッシュ設定のカスタマイズ

共有インサイトキャッシュをインストールした後、設定ファイルでその設定をカスタマイズすることができます。

設定ファイルは .NET フレームワークアプリケーション設定標準に従った XML ファイルです。無効な XML、不正な値の種類、必要な値の不足などの無効な設定がある場合、共有インサイトキャッシュは起動しません。

詳細については、次を参照してください。

構成エディタツール (SvcConfigEditor.exe)

以下の表で、設定できるオプションについて説明します。

Table 179: Shared Insight Cache 設定のオプション

オプションとデフォルト値	説明とコメント
Cache Service Listening Port デフォルト値は 9005 です。	サービスが応答準備するポート。応答準備ポートは、ファイルのスキャン結果を提出したり、クライアントがファイルのスキャンする必要があるかどうかを判断するための要求を行ったりするために、クライアントによって使われます。 ポートの範囲が 0 から 65535 まででない場合、サービスは開始しません。 指定したポートで応答準備できない場合、サービスは開始しません。 <pre><endpoint address="http://localhost:9005/1"</pre> デフォルトで共有インサイトキャッシュサーバーはすべての IP アドレスで応答準備します。HTTP サービスまたは HTTPS サービスを応答準備する IP アドレスを設定するには、Netsh.exe を使う必要があります。共有インサイトキャッシュサーバーは、それらのツールで変更され、IP の応答準備リストに指定された IP アドレスで応答準備します。 Netsh.exe は Windows Server 2008 に含まれています。 詳細については、次を参照してください。 HTTP および HTTPS の設定
Status Service Listening Port デフォルト値は 9006.	サーバーがサーバーの状態を伝えるために使うポートです。状態応答準備ポートでは、設定セクションで指定されたポートで、SOAP ベースのインターフェースが使われます。このインターフェースにより、管理者が Cache Server に関する情報と状態を問い合わせることができる手段が提供されます。 範囲が 0 から 65535 までではない場合、サービスは開始しません。 指定したポートで応答準備できない場合、サービスは開始しません。
投票件数 デフォルト値は 1 です。	共有インサイトキャッシュが結果を使う前にファイルがクリーンであることを検証する必要があるクライアントの数です。 値は 15 以下である必要があります。値が 15 より大きい場合、サーバーはデフォルト値を使います。 <pre><cache.configuration vote.count="1" /></pre>
Prune Size デフォルト値は 10 です。	キャッシュがメモリ使用量の限界に達したときにキャッシュから削除するメモリ使用量の割合です。 値は 10 と 100 の間にする必要があります。値が 10 から 100 までの間でない場合、サーバーはデフォルト値を使います。 Note: デフォルトのブルーニングサイズを保つことを推奨します。 <pre><prune.size="10" /></pre>
メモリの使用状況 デフォルト値は 50 です。	共有インサイトキャッシュがキャッシュのブルーニングを開始する前のキャッシュのサイズの割合です。 10 以上である必要があります。 <pre><mem.usage="50" /></pre>
Log File デフォルト値は <#####>/CacheServer.log です。	共有インサイトキャッシュログのファイルです。 <pre><filevalue="CacheServer.log" /></pre>

オプションと デフォルト値	説明とコメント
ログレベル デフォルト値は ERROR です。	ALL DEBUG 情報 WARN ERROR FATAL OFF 値 OFF は、共有インサイトキャッシュがメッセージをログに記録しないことを示します。 <code><level value="ERROR" /></code> ネットワークベースの共有インサイトキャッシュのログイベント
Log Size デフォルト値は 10000 です。	共有インサイトキャッシュがログをロールオーバーするまでのログのサイズ (バイト単位) です。 <code><maximumFileSizevalue="10000" /></code>
Log Backups デフォルト値は 1 で す。	ロールオーバーされるログの数。最も古いログが削除されるまで保持されます。 値 0 は Shared Insight Cache がバックアップを保持しないことを示します。負の値は共有インサイトキャッシュが無限の数のバックアップを保持することを示します。 <code><maxSizeRollBackupsvalue="1" /></code>
SSL を有効にする 認証を有効にする	共有インサイトキャッシュは、デフォルトで、認証も SSL も使用しないように設定されます。SSL を使用した基本認証、SSL を使用した認証なし、SSL を使用しない基本認証に変更できます。 <code><webHttpBinding></code> <code><bindingname="CacheServerBinding"></code> <code><!--</code> Uncomment the appropriate section to get the desired security. If enabling ssl modify the uri to use https. A cert will also have to be installed and registered for the ip/port. <code>--></code> <code><!-- Basic authentication with SSL.--></code> <code><security mode="Transport"></code> <code><transport clientCredentialType="Basic"/></code> <code></security--></code> <code><!-- No authentication with SSL.--></code> <code><security mode="Transport"></code> <code><transport clientCredentialType="None"/></code> <code></security--></code> <code><!-- Basic authentication with no SSL.--></code> <code><security mode="TransportCredentialOnly"></code> <code><transport clientCredentialType="Basic"/></code> <code></security--></code> <code><!-- No authentication with no SSL. DEFAULT --></code> <code><securitymode="None"></code> <code><transportclientCredentialType="Basic"/></code> <code></security></code> <code></binding></code> <code></webHttpBinding></code> ネットワークベースの共有インサイトキャッシュの使用の有効化

共有インサイトキャッシュ設定をカスタマイズするには

1. 次のファイルに移動して開きます。

```
C:\Program Files (x86)\Symantec\Shared Insight Cache  
\SharedInsightCacheInstallation.exe.config
```

レガシーインストールでは、このファイルパスは異なる場合があります。

2. 必要に応じて修正を加えます。
3. 変更内容を保存してファイルを閉じます。
4. 共有インサイトキャッシュサービスを再起動します。

ログレベルを除くすべての構成設定への変更を有効にするために、共有インサイトキャッシュサービスを再起動する必要があります。

[ネットワークベースの共有インサイトキャッシュサービスの停止と開始について](#)

[ネットワークベースの共有インサイトキャッシュを使用するために必要な準備](#)

ネットワークベースの共有インサイトキャッシュサービスの停止と開始について

トラブルシューティングするには、共有インサイトキャッシュサービスを一時的に停止する必要がある場合もあります。問題を解決した後、サービスを再起動できます。コントロールパネルのサービスアプレットからサービスを開始し、停止できます。

共有インサイトキャッシュのアンインストールには共有インサイトキャッシュサービスの停止と同じ効果があります。共有インサイトキャッシュを完全にアンインストールしてよいかどうか確かでない場合は、代わりにこのサービスを停止することができます。

共有インサイトキャッシュサービスを停止したり開始するには、Windows の管理者権限が必要です。

[共有インサイトキャッシュのトラブルシューティング](#)

ネットワークベースの共有インサイトキャッシュのログイベント

共有インサイトキャッシュログファイルを表示して、共有インサイトキャッシュによって作成されたすべてのイベントを表示できます。ログファイルはインストールフォルダにあり、名前は `CacheServer.log` です。

共有インサイトキャッシュはログを次の形式で出力します。

```
[ ] %thread | %d{MM/dd/yyyyHH:mm:ss} | %level | %logger{2} | %message [-]%newline
```

次に例を示します。

```
[ ] 4 | 12/15/2010 10:51:37 | INFO | CacheServerService.Service | Started service [-]
```

ネットワークベースの共有インサイトキャッシュで使いたいログレベルを指定するには、設定ファイルを修正します。

「[ネットワークベースの共有インサイトキャッシュのログレベル](#)」で、設定できるレベルについて説明します。

Table 180: ネットワークベースの共有インサイトキャッシュのログレベル

ログレベル	説明
OFF	OFF は、インシデントをログに記録しないことを示します。
FATAL	FATAL メッセージは対応を必要とします。これらのメッセージは、Shared Insight Cache を停止させるエラーです。たとえば、FATAL メッセージはサーバー IP アドレスが利用可能でないことを示す場合があります、それは共有インサイトキャッシュを実行できないことを意味します。

ログレベル	説明
ERROR	ERROR メッセージは対応を必要としますが、処理は引き続き実行されます。これは、共有インサイトキャッシュの機能を失敗させたり失わせたりする、システムでのエラーです。 FATAL メッセージのすべてのログエントリも受信します。 このレベルはデフォルトのログレベルです。
WARN	WARN メッセージは、望ましくはないがエラーを引き起こすわけではない共有インサイトキャッシュの動作を示します。 FATAL メッセージと ERROR メッセージのすべてのログエントリも受信します。
情報	INFO メッセージは、共有インサイトキャッシュの一般的な処理を記述したり、共有インサイトキャッシュに関する情報を提供します。システムの状態を示し、動作を検証したり問題を突き止めたりするのに役立つことがあります。ただし、それだけで、実施可能なアイテムを報告することを意図するものではありません。 たとえば、キャッシュのプルーニングが完了したことを示すのが情報メッセージです。問題について詳しく説明するものではありません。動作をログに記録するだけです。 FATAL メッセージ、ERROR メッセージ、WARN メッセージのすべてのログエントリも受信します。
DEBUG ALL	DEBUG と ALL のログレベルのメッセージは同じ結果を生成します。これらのログレベルは、共有インサイトキャッシュのトラブルシューティングを支援することを意図するものです。 また、他のすべてのログレベルのすべてのログエントリも受信します。

ログレベルを高くするのは、共有インサイトキャッシュのトラブルシューティングが必要な場合にのみしてください。ログレベルを高くするときは、まずログファイルのサイズをかなり大きくしてください。問題を解決したら、デフォルトの ERROR のログレベルに戻してください。

次の場所に移動します。

<#####>/CacheServer.log

共有インサイトキャッシュ設定のカスタマイズ

ネットワークベースの共有インサイトキャッシュパフォーマンスカウンタの監視

Windows パフォーマンスモニタで、ネットワークベースの共有インサイトキャッシュの統計を確認できます。パフォーマンスカウンタを確認するには、対象となる共有インサイトキャッシュサービスが実行中である必要があります。

Table 181: 共有インサイトキャッシュの統計

統計情報	説明
キャッシュ内の項目の数	この数はキャッシュ内の項目の現在の数を表します。
キャッシュ内のクリーンと投票された項目の数	この数は、キャッシュ内のクリーンと投票されたアイテムの現在の数を表します。
キャッシュ要求の数	共有インサイトキャッシュサービスに行われたキャッシュ要求の数。 この数には、200 件のレスポンスを受信した有効な要求の数のみが含まれます。このカウンタはサービスが再開されると持続されません。
更新要求の数	サービスに対して行われた更新要求の数。 この数は、200 件の応答を受信した有効な要求のみの数です。このカウンタはサービスが再開されると持続されません。

ネットワークベースの共有インサイトキャッシュパフォーマンスカウンタを監視するには

1. コマンドプロンプトに次のコマンドを入力します。

```
perfmon
```

2. [パフォーマンス] ウィンドウで、グラフを右クリックします。
3. [Add Counters] を選択します。
4. [Performance object] ドロップダウンリストで、[共有インサイトキャッシュ] を選択します。
5. 確認したいカウンタを選択し、[追加] をクリックします。
6. [閉じる] をクリックします。

選択した共有インサイトキャッシュカウンタがパフォーマンスグラフに表示されます。

Windows パフォーマンスモニタの使用について詳しくは、Windows のマニュアルを参照してください。

共有インサイトキャッシュのトラブルシューティング

ネットワークベースの共有インサイトキャッシュを使用するために必要な準備

共有インサイトキャッシュのトラブルシューティング

「[共有インサイトキャッシュのトラブルシューティング](#)」で、共有インサイトキャッシュのトラブルシューティングする方法を示します。

Table 182: Shared Insight Cache のトラブルシューティング

問題	説明/対策
キャッシュ結果の問題の発生	サービスを再起動します。 ネットワークベースの共有インサイトキャッシュサービスの停止と開始について
共有インサイトキャッシュが「結果なし」という応答を返す	共有インサイトキャッシュは、キャッシュのルックアップが正常に実行されないと、結果なしの応答を返します。クライアントがキャッシュのルックアップを要求する場合、「結果なし」はファイルのスキャンする必要があることを意味します。 Note: 共有インサイトキャッシュは、キャッシュの更新が正常に実行されないときでも、正常に完了の応答を返します。これは、エラーが発生したときに、クライアントが別の処理を実行する必要がないためです。
HTTP トラフィックの疑いのある問題	HTTP トラフィックのエラーログを確認してください。HTTP トラフィックのエラーは次の場所にあるログに記録されます。 %Windir%\System32\Logfiles\HTTPERR

ネットワークベースの共有インサイトキャッシュのログイベント

ネットワークベースの共有インサイトキャッシュパフォーマンスカウンタの監視

基本イメージへの Virtual Image Exception ツールの使用

仮想マシンを構築する前に、基本イメージに仮想イメージ例外ツールを使えます。仮想イメージ例外ツールを使用して、クライアントで基本イメージファイルの脅威のスキャンをバイパスできるため、ディスク I/O のリソース負荷を軽減できます。さらに、仮想デスクトップインフラストラクチャの CPU スキャンプロセスのパフォーマンスも向上します。

Symantec Endpoint Protection は、管理下クライアントと管理外クライアントに対する仮想イメージ例外ツールの使用をサポートしています。

NOTE

非仮想環境では仮想イメージ例外ツールを使えません。

Table 183: 基本イメージへの仮想イメージ例外ツールの使用のプロセス

手順	処理
1	基本イメージに対して、すべてのファイルの完全スキャンを実行し、ファイルがクリーンであることを確認します。 Symantec Endpoint Protection クライアントが感染ファイルを検疫した場合、検疫ファイルを修復するか削除して、それらを
2	クライアントの検疫が空であることを確認します。
手順 3	コマンドラインから Virtual Image Exception ツールを実行して、基本イメージファイルをマークします。 仮想イメージ例外ツールの実行 vietool
手順 4	クライアントがスキャンの実行時にマークされたファイルを見つけてバイパスすることを認識するように、つの Symantec 基本イメージファイルのスキャンをバイパスするための Symantec Endpoint Protection の設定
手順 5	基本イメージから仮想イメージ例外ツールを削除します。

仮想イメージ例外ツールは固定のローカルドライブをサポートしています。このツールは、NTFS (New Technology File System) 規格に準拠するファイルで機能します。

仮想イメージ例外ツールのシステム必要条件

仮想イメージ例外ツールのシステム必要条件

仮想イメージ例外ツールは、VMware ESX、Microsoft Hyper-V、Citrix XenDesktop プラットフォームでの使用がサポートされます。

クライアントは次のすべての必要条件を満たしている必要があります。

- クライアントは、サポート対象の仮想環境のいずれかにインストールする必要があります。
- クライアントでは、Symantec Endpoint Protection クライアントソフトウェアのバージョン 12.1 以降を実行する必要があります。

WARNING

クライアントは Virtual Image Exception ツールと同じバージョンである必要があります。

必要条件とサポート対象プラットフォームについての最新情報は、次の Web ページを参照してください。

[Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件](#)

基本イメージへの仮想イメージ例外ツールの使用

仮想イメージ例外ツールの実行

仮想イメージ例外ツールを実行する前に、すべてのシステムの必要条件を満たしていることを確認します。

WARNING

クライアントは Virtual Image Exception ツールと同じバージョンである必要があります。

仮想イメージ例外ツールのシステム必要条件

仮想イメージ例外ツールを実行するには

1. Symantec Endpoint Protection ツールフォルダのインストールファイルから、次のファイルを基本イメージにダウンロードします。

`/Virtualization/VirtualImageException/vietool.exe`

2. 管理者権限でコマンドプロンプトを開きます。
3. 正しい引数を使用して Virtual Image Exception ツールを実行します。
たとえば、`vietool c: --generate` と入力します。

[vietool](#)

基本イメージファイルのスキャンをバイパスするための Symantec Endpoint Protection の設定

基本イメージファイルに仮想イメージ例外ツールを実行したら、つの Symantec Endpoint Protection Manager で仮想イメージ例外の使用を有効にできます。この機能を有効にすると、仮想クライアントはツールが挿入した属性を探します。次に、Symantec Endpoint Protection はその属性を含んでいる基本イメージファイルのスキャンをスキップします。

Auto-Protect スキャンまたは管理者定義のスキャン（手動スキャンや定時スキャンなど）で、未変更の基本イメージファイルのスキャンをバイパスできます。

Symantec Endpoint Protection で仮想イメージ例外を使うように設定して、基本イメージファイルのスキャンをバイパスするには

1. コンソールで、適切なウイルスおよびスパイウェアの対策ポリシーを開きます。
2. [拡張オプション] で [その他] をクリックします。
3. [Virtual Images] タブで、有効にするオプションにチェックマークを付けます。
4. [OK] をクリックします。

[基本イメージへの仮想イメージ例外ツールの使用](#)

非永続的な仮想デスクトップインフラストラクチャでの Symantec Endpoint Protection の使用

仮想環境での Symantec Endpoint Protection の設定

Table 184: 非永続的な仮想デスクトップインフラストラクチャで Symantec Endpoint Protection を使用するためのタスク

手順	説明
手順 1: 基本イメージを設定します。	基本イメージで Symantec Endpoint Protection クライアントを設定して、非永続的な仮想クライアントであると示します。 VDI での非永続的なゲスト仮想マシンの基本イメージの設定
手順 2: つの Symantec Endpoint Protection Manager で、オフラインの非永続的 VDI クライアントに個別のページ間隔を設定します。	つの Symantec Endpoint Protection Manager では、指定した期間を超えてオフラインになっている非永続的な GVM クライアントは削除されます。この機能により、つの Symantec Endpoint Protection Manager での GVM の管理が容易になります。 ライセンスを開放するための使われなくなった非永続的 VDI クライアントのページ

VDI で非永続的なゲスト仮想マシンの基本イメージの設定

つの Symantec Endpoint Protection Manager を使って非永続的な仮想デスクトップインフラでゲスト仮想マシン（GVM）を簡単に管理できるように基本イメージを設定できます。

Table 185: 非永続的なゲスト仮想マシン (GVM) の基本イメージを設定するタスク

手順	説明
手順 1: Symantec Endpoint Protection を基本イメージにインストールします。	クライアント配備ウィザードを使ったクライアントのインストール方法の選択
手順 2: レジストリを修正できるように、管理サーバーで改変対策を無効にします。	改変対策の設定の変更
手順 3: つの Symantec Endpoint Protection Manager が非永続的な仮想クライアントのライセンス数を正確に算出することを確認します。	非永続的なクライアントの長所は、配備済みライセンス数にオフラインの非永続的なクライアントを加算しないことです。オンラインクライアントの数のみを加算します。仮想クライアントを非永続的なクライアントとしてマーク付けするには、基本イメージでレジストリキーを作成する必要があります。 非永続的 VDI クライアントのライセンス数の管理方法
手順 4: つの Symantec Endpoint Protection Manager で、改変対策を再び有効にします。	改変対策の設定の変更

基本イメージの設定が終了した後、つの Symantec Endpoint Protection Manager で非永続的なクライアントに対する個別のページ間隔を設定できます。

[ライセンスを開放するための使われなくなった非永続的 VDI クライアントのページ](#)

ライセンスを開放するための使われなくなった非永続的 VDI クライアントのページ

使われなくなったクライアントは、時間の経過とともに つの Symantec Endpoint Protection Manager データベースに蓄積されることがあります。使われなくなったクライアントとは、つの Symantec Endpoint Protection Manager に 30 日間接続しなかったクライアントです。つの Symantec Endpoint Protection Manager は、デフォルトで 30 日ごとに、使われなくなったクライアントをページします。

使われなくなった非永続的なクライアントがページされるまで同じ日数を待機しないようにする場合は、これらのクライアント用に個別の間隔を設定できます。個別の間隔を設定しないと、オフラインの非永続的な仮想クライアントは、使われなくなった物理クライアントと同じ間隔でページされます。

オンラインの非永続的なクライアントは、配備済みライセンス数に加算されますが、オフラインの非永続的なクライアントは加算されません。

[非永続的 VDI クライアントのライセンス数の管理方法](#)

また、オフラインの非永続的なクライアントをフィルタ処理して、[クライアント] ページに表示されないようにできます。

ライセンスを開放するために使われなくなった非永続的 VDI クライアントをページするには

1. つの Symantec Endpoint Protection Manager コンソールの [管理] ページで、[ドメイン] をクリックします。
2. [ドメイン] ツリーで目的のドメインをクリックします。
3. [タスク] の下で、[ドメインプロパティの編集] をクリックします。
4. [ドメインプロパティの編集] > [全般] タブで、[一定期間にわたって接続しなかった非永続的な VDI クライアントを削除します] チェックボックスにチェックマークを付けて、[日] の値を必要な数に変更します。

オフラインの非永続的な VDI クライアント用のオプションにアクセスするには、[一定期間にわたって接続しなかったクライアントを削除する] オプションにチェックマークを付ける必要があります。

-
5. [OK] をクリックします。

非永続的な仮想デスクトップインフラストラクチャでの Symantec Endpoint Protection の使用

非永続的 VDI クライアントのライセンス数の管理方法

管理サーバーはコンピュータがオンラインかオフラインかにかかわらず、物理コンピュータの各クライアントのライセンスを数えます。仮想クライアントの場合には、管理サーバーはオンラインの非永続的なクライアントのみのライセンスを数えます。オフラインの非永続的なクライアントは数えません。クライアントよりユーザーが多い場合は仮想クライアントを非永続的なクライアントにします。

仮想クライアントを非永続的なクライアントとしてマーク付けするには、基本イメージでレジストリキーを作成する必要があります。

非永続的 VDI クライアントのライセンス数を管理するには

1. Symantec Endpoint Protection クライアントをインストールし、改変対策を無効にした後、基本イメージでレジストリエディタを開きます。

[改変対策の設定の変更](#)

2. 次のレジストリキーの 1 つに移動します:

- 32 ビットシステムの場合: HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\
- 64 ビットシステムの場合: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Symantec\Symantec Endpoint Protection\SMC\

3. Virtualization という名前の新しいサブキーを作成します。

4. **Virtualization** サブキーの下に、IsNPVDIClient という名前の DWORD 型のキーを作成し、それに値 1 を割り当てます。

[ライセンスを開放するための使われなくなった非永続的 VDI クライアントのページ](#)

[VDI での非永続的なゲスト仮想マシンの基本イメージの設定](#)

vietool

vietool

vietool - 仮想イメージ例外ツールを実行します。

概要

```
vietool.exe volume: --generate|clear|verify|hash [options ...]
```

説明

vietool コマンドは、属性を追加して、指定したボリューム上の基本イメージファイルをマークします。

オプション

--generate

指定したボリューム上のすべてのファイルに対して Virtual Image Exception ツールを実行します。このオプションは --clear オプションと一緒に使用できません。

例: vietool c: --generate

--verify

指定したボリューム上のすべてのファイルに対して Virtual Image Exception が設定されていることを確認します。このオプションは --clear オプションと一緒に使用できません。

例: `viertools c: --verify`

--clear

指定したボリューム上のすべてのファイルの Virtual Image Exception を削除します。

例: `viertools.exe c: --clear`

特定のファイルを削除するには: `viertools.exe c:\Users\Administrator\target.file --clear`

ボリューム識別子の代わりに、完全修飾パスを使用して、単一のファイルまたはフォルダの内容の Virtual Image Exception on を消去できます。コマンドラインあたり、1 つのファイル名、フォルダ名、またはボリューム識別子のみを使用できます。このコマンドは `--generate`、`--verify`、または `--hash` と一緒に使用できません。

`--clear` コマンドを実行したら、クライアントを再起動する必要があります。

--hash

指定したボリューム上のすべてのファイルのハッシュ値を生成します。

Virtual Image Exception ツールはハッシュを利用して将来のスキャンからローカルファイルを除外します。クライアントはハッシュを個別に計算し、スキャン結果を格納する Shared Insight Cache に送信します。このオプションは `--clear` オプションと一緒に使用できません。

例: `viertools.exe c: --generate --hash`

--volume arg

ツールがスキャンするボリュームを指定します。

`--clear` オプションを使用する場合、このオプションにファイルを指定できます。ボリュームを指定する必要がありますが、ボリュームフラグまたは単独で指定できます。たとえば、フラグの場合 `viertools.exe --volume c: --generate`、または単独の場合 `viertools.exe c: --generate` となります。

--verbose

最大量のプログラム実行情報をコンソールに出力します。

--stop

ツールが最初に検出したエラーで停止します。このオプションを使用しない場合、ツールはエラー情報をコンソールに書き込み、続行します。

--help

このヘルプメッセージを表示します。

Symantec Endpoint Protection のトラブルシューティング

Symantec Endpoint Protection の問題をトラブルシューティングする方法

「[トラブルシューティング可能な一般的な問題](#)」では、Symantec Endpoint Protection をインストールしたり使っているときに起きる可能性のある一般的な問題を示します。

Table 186: トラブルシューティング可能な一般的な問題

タスク	説明
インストールの問題の解決	Symantec Diagnostic Tool (SymDiag) をダウンロードして実行すると、インストールの準備ができていないかコンピュータに確認できます。このツールはシマンテック社のサポート Web サイトから、管理サーバーとクライアントのヘルプを通じて提供されます。 Symantec Diagnostic Tool (SymDiag) を使ったコンピュータの問題のトラブルシューティング インストールに失敗した場所の識別
ウイルスアウトブレイクの処理	脅威によってネットワーク上のコンピュータが攻撃されるのを防ぐことができます。 クライアントコンピュータに対するウイルスとスパイウェアの攻撃の防止と処理 ウイルスとセキュリティリスクの除去 クライアントコンピュータが脅威に攻撃された場合は、その脅威を識別して対処することができます。 ネットワーク上のウイルス駆除とトラブルシューティング
コンテンツ更新の問題のトラブルシューティング	つの Symantec Endpoint Protection Manager またはクライアントで最新のウイルス定義が正しく更新されない場合は、次の記事を参照してください。 Endpoint Protection Manager の LiveUpdate とコンテンツのトラブルシューティング Symantec Endpoint Protection: LiveUpdate トラブルシューティングのフローチャート
通信問題の修正	Symantec Endpoint Protection のすべてのコンポーネント間の通信チャンネルが開いている必要があります。これらのチャンネルには、サーバーからクライアントへのチャンネル、サーバーからデータベースへのチャンネル、サーバーとクライアントから LiveUpdate などのコンテンツ配信コンポーネントへのチャンネルが含まれます。 つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング つの Symantec Endpoint Protection Manager とコンソールまたはデータベース間における通信の問題のトラブルシューティング グループ更新プロバイダのベストプラクティスとトラブルシューティング
ディザスタリカバリの実行	データベースが破損したりハードウェア障害が発生した場合でも、データベースのバックアップファイルがあれば、データベースの最新のスナップショットを復元できます。 Endpoint Protection のディザスタリカバリのベストプラクティス
データベースの領域の縮小	データベースのサイズが大きくなりすぎた場合は、データベースで利用可能な領域を増やすことができます。 データベースの保守
レポートに関する問題のトラブルシューティング	レポートとログに関するさまざまな問題を解決できます。 レポートに関する問題のトラブルシューティング
複製に関する問題のトラブルシューティング	Symantec Endpoint Protection の複製のトラブルシューティングのフローチャート

[Symantec Endpoint Protection に含まれるツール](#)

SEP および SES がシマンテック社のサーバーへ接続するために許可する (ホワイトリストに登録する) URL

Symantec Endpoint Protection (SEP) およびクライアント (Symantec エージェント) は、特定の URL と通信して、ライセンスの検証、不審なファイルのサンプルの提出、オンプレミスの Symantec Endpoint Protection Manager やクラウドコンソールとの通信など、複数の機能を実行します。お客様の環境で 1 つ以上のプロキシを使用しており、必要なトラフィックをシマンテック社のサーバーにリダイレクトする場合は、これらの URL を許可する必要があります。

[SEP および SES がシマンテック社のサーバーへ接続するために許可する URL](#)

Symantec Diagnostic Tool (SymDiag) を使ったコンピュータの問題のトラブルシューティング

つの Symantec Endpoint Protection Manager または Symantec Endpoint Protection クライアントのインストール時や使用時に起きる一般的な問題を診断するためのユーティリティをダウンロードできます。

Symantec Endpoint Protection クライアントのインストール時や使用時に起きる一般的な問題を診断するためのユーティリティをダウンロードできます。

サポートツールは次の問題を解決するのに役立ちます。

- 既知の問題を素早く正確に識別できます。
 - ツールが問題を認識すると、ツールはユーザーがその問題を自分で解決できるように、リソースを示します。
 - 問題が解決しない場合、このツールは、サポートにデータを簡単に送信してさらに診断できるようにします。
1. 次のいずれかのタスクを行います。
 - 「[シマンテック製品の問題を検出する Symantec Diagnostic Tool \(SymDiag \) 診断ツールをダウンロードする](#)」を参照してください。
 - つの Symantec Endpoint Protection Manager またはクライアントで、[ヘルプ]、[Symantec Diagnostic Tool のダウンロード] の順にクリックします。
 2. 画面の指示に従います。

クライアントインストールに失敗した場所の識別

Windows インストーラとプッシュ配備ウィザードは、インストールが正常に完了したかどうかを確認できるログファイルを作成します。ログファイルには、正常にインストールされたコンポーネントが一覧されているほか、インストールパッケージに関連するさまざまな詳細情報が記載されています。ログファイルを使えば、インストールの失敗原因となったコンポーネントや処理を識別できます。インストールに失敗した理由を判断できない場合は、ログファイルを保存しておいてください。Symantec Technical Support からログファイルの提出を指示されることがあります。

NOTE

インストールパッケージが実行されるたびに、ログファイルは上書きされます。

1. テキストエディタで、インストールで作成されたログファイルを開きます。
2. 障害を探すには、次のエントリを検索します。

Value 3

このエントリが含まれる行の前に実行した処理が、失敗原因の可能性が高いと思われます。このエントリの後の行は、インストールに問題があったためにロールバックされたインストールコンポーネントです。

[クライアント配備ウィザードを使ったクライアントのインストール方法の選択](#)

つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング

クライアントとサーバー間の通信に問題がある場合は、ネットワークに問題がないことを最初に確認してください。また、Symantec Technical Support に問い合わせる前に、ネットワークの接続性もチェックしてください。

クライアントと管理サーバー間の通信を、複数の方法でテストできます。

Table 187: 管理サーバーとクライアント間の接続のチェック

チェック項目	解決策
クライアントを調べて、クライアントが管理サーバーに接続しているかどうか確認します。	通信設定を検証するためにクライアントでトラブルシューティングファイルをダウンロードして表示できます。 Symantec Endpoint Protection クライアントの状態アイコン クライアントコンピュータの管理サーバーへの接続のチェック トラブルシューティングファイルを使った保護の問題の調査
クライアントと管理サーバー間の接続性をテストする	いくつかのタスクを実行して、クライアントと管理サーバーの間の接続性を確認できます。 - クライアントが管理サーバーに接続しているかどうかを調べるためのアクセスログの有効化と表示 - クライアントコンピュータから管理サーバーに ping を実行する ping コマンドを使用した管理サーバーへの接続性のテスト - クライアントコンピュータの Web ブラウザを使って管理サーバーに接続する ブラウザを使用した、つの Symantec Endpoint Protection Manager クライアントでの Symantec Endpoint Protection への接続テスト
管理サーバーが正しいサーバー証明書を使っていることを確認する	つの Symantec Endpoint Protection Manager を再インストールした場合は、正しいサーバー証明書を適用しているかを調べます。管理サーバーで異なるサーバー証明書を使っていると、サーバーはコンテンツをダウンロードしますがクライアントはコンテンツを読み込めません。管理サーバーが間違ったサーバー証明書を使っている場合は、証明書を更新する必要があります。 サーバー証明書の更新または復元 サーバー証明書を更新してクライアント/サーバー接続を維持するためのベストプラクティス 次のことを調べると、管理サーバーが間違ったサーバー証明書を使っているかを確認できます。 - クライアントのタスクバーに緑色のドットが表示されていない。これは、クライアントが管理サーバーと通信していないことを示します。 クライアントが管理サーバーに接続され、保護されているかどうかの確認 - クライアントがポリシーの更新を管理サーバーから受信しない。 - 管理サーバーがクライアントと接続していないことを示している。 Symantec Endpoint Protection クライアントの状態アイコン
ネットワークに問題があるかどうかをチェックする	次の項目をチェックすることによって、ネットワークに問題がないことを確認します。 - 最初に、クライアントと管理サーバー間の接続性をテストする。クライアントコンピュータが管理サーバーに ping または Telnet を実行できない場合、クライアントの DNS サービスを確認してください。 - クライアントのルーティングパスを調べる - 管理サーバーにネットワークの問題がないことを確認する - Symantec Endpoint Protection ファイアウォール (またはサードパーティのファイアウォール) がネットワークの問題を引き起こしていないことをチェックする
クライアントのデバッグログをチェックする	クライアントのデバッグログを使って、クライアントに通信の問題があるかどうかを判断できます。 クライアントコンピュータのデバッグログのチェック 管理サーバーの受信ボックスログのチェック

チェック項目	解決策
失われたクライアント通信を回復する	クライアントが管理サーバーとの通信を失った場合、通信ファイルを回復するためにツールを使うことができます。 SylinkDrop ツールを使ったクライアントとサーバー間の通信設定の復元

つの Symantec Endpoint Protection Manager にログエラーまたは HTTP エラーコードが表示された場合は、「[つの Symantec Endpoint Protection Manager の通信のトラブルシューティング](#)」という記事を参照してください。

クライアントコンピュータの管理サーバーへの接続のチェック

管理下クライアントがある場合は、管理サーバーとの接続を確認できます。管理サーバーに接続されていない場合は、クライアントが接続するよう要求できます。

Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアント間の接続の問題のトラブルシューティング

クライアントコンピュータの管理サーバーへの接続のチェック

1. [状態] ページで、[ヘルプ]、[トラブルシューティング] の順にクリックします。
2. [トラブルシューティング] ダイアログボックスで [接続の状態] をクリックします。
3. [接続の状態] ペインで、最後に試行した接続と最後に成功した接続を確認できます。
4. 管理サーバーとの接続を再確立するには、[Connect Now] をクリックします。

トラブルシューティングファイルを使った保護の問題の調査

クライアントの問題を調査するには、クライアントコンピュータの Troubleshooting.txt ファイルを調べます。Troubleshooting.txt ファイルにはポリシー、ウイルス定義、他のクライアント関連データについての情報が含まれています。

シマンテックテクニカルサポートは Troubleshooting.txt ファイルを電子メールで送るように要求することがあります。

つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング

クライアントからトラブルシューティングファイルをエクスポートするには

1. クライアントコンピュータで、クライアントを開きます。
2. クライアントで、[ヘルプ] > [トラブルシューティング] の順にクリックします。
3. [管理] ペインの [トラブルシューティングデータ] で、[エクスポート] をクリックします。
4. [名前を付けて保存] ダイアログボックスで、デフォルトのトラブルシューティングファイル名を受け入れるか、または新しいファイル名を入力し、[保存] をクリックします。

デスクトップまたは選択したフォルダにファイルを保存できます。

5. テキストエディタを使って Troubleshooting.txt を開き、内容を調べます。

クライアントが管理サーバーに接続しているかどうかを確認するためのアクセスログの有効化と表示

管理サーバーで Apache HTTP サーバーのアクセスログを表示し、クライアントが管理サーバーに接続しているかどうかを確認できます。クライアントが接続している場合、クライアントの接続の問題は、おそらくネットワークの問題ではありません。ネットワークの問題には、ファイアウォールによるアクセスの遮断や、相互に接続していないネットワークの問題が含まれます。

ログを表示する前に、まず Apache HTTP サーバーのアクセスログを有効にする必要があります。

NOTE

ログは不必要な CPU リソースとハードディスク容量を消費するため、参照後はログを無効にします。

[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

NOTE

デフォルトの SEPM_Install のデフォルト値は C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

1. Apache HTTP サーバーのアクセスログを有効にするには、テキストエディタで、ファイル SEPM_Install\apache\conf\httpd.conf を開きます。
2. httpd.conf ファイルで、次の文字列から番号記号 (#) を削除し、ファイルを保存します。

```
#CustomLog "logs/access.log" combined
```

3. つの Symantec Endpoint Protection Manager サービスと Apache HTTP サーバーを停止し、再開します。

[管理サーバーサービスの停止と開始](#)

[Apache Web サーバーの停止と開始](#)

4. Apache HTTP サーバーのアクセスログを表示するには、管理サーバーで、ファイル SEPM_Install\apache\logs\access.log を開きます。
5. クライアントコンピュータの IP アドレスまたはホスト名を探します。それらがあれば、クライアントが Apache HTTP サーバーに接続していることを示しています。
6. Apache HTTP サーバーのアクセスログを無効にします。

Apache Web サーバーの停止と開始

Symantec Endpoint Protection Manager をインストールすると、Apache Web サーバーがインストールされます。Apache Web サーバーは自動サービスとして実行されます。Apache HTTP サーバーアクセスログを有効にするには、Web サーバーを停止して開始することが必要な場合があります。

[クライアントが管理サーバーに接続しているかどうかを調べるためのアクセスログの有効化と表示](#)

1. Apache Web サーバーを停止するには、コマンドプロンプトから以下のように入力します。

```
net stop semwebsrv
```

2. Apache Web サーバーを開始するには、コマンドプロンプトから以下のように入力します。

```
net start semwebsrv
```

ping コマンドを使用した管理サーバーへの接続性のテスト

接続性をテストするために、クライアントコンピュータから管理サーバーに ping の実行を試みることができます。

[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

ping コマンドを使用して管理サーバーへの接続性をテストする手順

1. クライアントで、コマンドプロンプトを開きます。
2. ping コマンドを入力します。次に例を示します。

```
ping name
```

ここで、name は管理サーバーのコンピュータ名です。コンピュータ名の代わりにサーバーの IP アドレスを使うことができます。どちらの場合も、コマンドはサーバーの正しい IP アドレスを返します。

ping コマンドが正しいアドレスを返さない場合は、クライアントの DNS サービスを確認し、ルーティングパスをチェックします。

ブラウザを使用した、つの Symantec Endpoint Protection Manager クライアントでの Symantec Endpoint Protection への接続テスト

クライアントコンピュータで Web ブラウザを使って、管理サーバーとクライアントの間の接続性をテストできます。この方法は、接続、ネットワーク、クライアント自体のいずれかに問題があるかどうかを判断する場合に役立ちます。

次の方法を使って管理サーバーとクライアントコンピュータ間の接続を調べることもできます。

- Symantec Endpoint Protection クライアントの状態アイコンに緑のドットが表示されているかどうかのチェック。
[Symantec Endpoint Protection クライアントの状態アイコン](#)
- Symantec Endpoint Protection クライアントでの接続の状態のチェック。
[クライアントコンピュータの管理サーバーへの接続のチェック](#)

ブラウザを使用して、つの Symantec Endpoint Protection Manager クライアントで Symantec Endpoint Protection への接続をテストするには

1. クライアントコンピュータで Internet Explorer などの Web ブラウザを開きます。
2. ブラウザのコマンドラインに次のコマンドを入力します。

```
http://<SEPMServer>:8014/secars/secars.dll?hello,secars
```

ここで、SEPMServerは管理サーバーの DNS 名、NetBIOS 名、または IP アドレスです。

IP アドレスには IPv4 と IPv6 があります。IPv6 アドレスは次のように角カッコで囲む必要があります: `http://[<SEPMServer>]:<#####>`

3. Web ページが表示されたら、次のどちらの結果であるかを確認します。
 - **OK** という単語が表示されている場合、クライアントコンピュータは管理サーバーに接続しています。クライアントで問題をチェックしてください。
 - **OK** という単語が表示されていない場合、クライアントコンピュータは管理サーバーに接続していません。クライアントのネットワーク接続をチェックし、クライアントコンピュータでネットワークサービスが実行されていることを確認します。クライアントのための DNS サービスを確認し、ルーティングパスをチェックします。
[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

クライアントコンピュータのデバッグログのチェック

クライアントのデバッグログをチェックできます。クライアントで管理サーバーとの通信に問題があれば、接続の問題についての状態メッセージがログに示されます。

[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

次の方法を使って、デバッグログをチェックできます。

- クライアントの [ヘルプとサポート] メニューの [トラブルシューティング] ダイアログボックスで、[デバッグログ設定の編集] をクリックし、ログの名前を入力します。次に、[ログの表示] をクリックします。
- Windows レジストリを使ってクライアントのデバッグをオンにできます。
Windows レジストリキーは次の場所にあります。
HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC\smc_debuglog_on

管理サーバーの受信ボックスログのチェック

Windows レジストリキーを使って、管理サーバー受信ボックスの活動についてのログを生成できます。Windows レジストリキーを修正するときに、管理サーバーはログ (ersecreg.log と exsecars.log) を生成します。クライアントとサーバー間の通信の問題を解決するために、これらのログを表示できます。

[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

クライアントコンピュータのデバッグログのチェック

管理サーバーの受信ボックスログをチェックする手順

1. 管理サーバーの HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM の下で、DebugLevel 値を 3 に設定します。

受信ボックスは管理サーバーコンピュータ上の次に示すデフォルトの場所に置かれています: SEPM_Install\data\inbox\log

デフォルトの SEPM_Install のデフォルト値は C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

2. メモ帳を使ってログを開きます。

SylinkDrop ツールを使ったクライアントとサーバー間の通信設定の復元

Sylink.xml ファイルはクライアントと Symantec Endpoint Protection Manager サーバー間の通信設定を含んでいます。クライアントが管理サーバーとの通信を失った場合、古い Sylink.xml ファイルを新しい Sylink.xml ファイルで置き換える必要があります。SylinkDrop ツールは新しい Sylink.xml ファイルによって自動的にクライアントコンピュータの Sylink.xml ファイルを置き換えます。

NOTE

クライアントインストールパッケージを再配備して、Sylink.xml ファイルを置き換えることもできます。多数のコンピュータ、物理的に容易にはアクセスできないコンピュータ、管理アクセスを必要とするコンピュータに対して、この方法を使います。

[\[通信の更新パッケージの配備 \] を使ったクライアントサーバー通信の復元](#)

SylinkDrop ツールを実行するとき、次のタスクも実行できます。

- 新しいドメインが管理サーバーにクライアントを移行するか、または移動する
- 管理サーバーで修正できないクライアントに対する通信の破損を復元する
- 1つのサーバーから複製パートナーではない別のサーバーにクライアントを移動する
- 1つのドメインから別のものにクライアントを移動する
- 管理下クライアントに管理外クライアントを変換する

ツールを使ってスクリプトを記述すると多くのクライアントの通信設定を修正できます。

管理下クライアントと管理外クライアントについて

[つの Symantec Endpoint Protection Manager と Symantec Endpoint Protection クライアントの間の接続に関する問題のトラブルシューティング](#)

Windows 用 SylinkDrop ツールを使ってクライアントとサーバー間の通信設定を復元するには

1. コンソールで、クライアントコンピュータを接続する管理サーバーに接続するグループから通信ファイルをエクスポートします。通信ファイルは Sylink.xml ファイルです。

[クライアントとサーバーの通信ファイル \(Sylink.xml \) の手動によるエクスポート](#)

2. クライアントコンピュータに通信ファイルをコピーします。

ネットワーク上の場所にファイルを保存するか、クライアントコンピュータのユーザーに電子メールで送信するか、またはリムーバブルメディアにコピーできます。

3. 次のいずれかのタスクを行います。

- [Broadcom ダウンロードセンター](#)の完全な製品のインストールファイルで、Tools\SylinkDrop\SylinkDrop.exe を検索します。
- 管理サーバーを実行するコンピュータで、C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\Version.Number\Bin\SylinkDrop.exe を検索します。

ツールをリモートで実行するか、またはクライアントコンピュータで保存してから実行することができます。コマンドラインオプションについて詳しくは、\Tools\SylinkDrop フォルダ内の readme ファイルをクリックして参照してください。

4. [Sylink Drop] ダイアログボックスで、[参照] をクリックし、ステップ 2 でクライアントコンピュータに配備した .xml ファイルを検索します。

5. [Update Sylink] をクリックします。

6. 確認のダイアログボックスが表示されたら、[OK] をクリックします。

7. [Sylink Drop] ダイアログボックスで、[終了] をクリックします。

Symantec Agent for Linux のトラブルシューティング

以下の表に、Symantec Agent for Linux のトラブルシューティングに関するリソースを示します (14.3 RU1 現在)。

処理	説明
エージェントの状態の確認。	エージェントのバージョンおよび接続状態をチェックし、モジュールがロード済みでデーモンが実行されていることを確認するには、/usr/lib/symantec に移動し、以下のコマンドを実行します。 ./status.sh
エージェントパッケージのバージョンの確認。	/usr/lib/symantec に移動し、以下のコマンドを実行します。 ./version.sh
ログの表示。	Symantec Agent for Linux のログは、以下の場所で確認できます。 • AMD ログ - スキャンに関連する情報を提供します。 /var/log/sdcssllog/amdlog • CAF ログ - サーバーとの通信、登録、コマンド、イベントなど、エージェントの活動に関連する情報を提供します。 /var/log/sdcssl-caflog/ • エージェントログ - エージェントの活動に関連する情報を提供します。 /var/log/sdcssllog/SISIDSEvents*.csv • CVE ログ - つの Symantec Endpoint Protection Manager とエージェントの間の通信に関連する情報を提供します。 /var/log/sdcssl-caflog/cve.log
ログを zip ファイルに収集。	GetAgentInfo スクリプトを使用して、すべてのログファイルを ZIP ファイルに収集し、カスタマサポートに送信できます。 1. Symantec Agent for Linux 14.3 RU1 システムにログインします。 2. /opt/Symantec/sdcsslagent/IPS/tools/ に移動します。 3. root として ./getagentinfo.sh を実行します。 4. /tmp/ ディレクトリに ZIP ファイルが作成されます。 ファイル名は 20201208_184935_0001_CU_mihsan-rhel8.zip のようになります。 -out <directory> を指定して、生成される ZIP ファイルの場所と名前を変更できます。

処理	説明
CVE ログレベルの変更。	デフォルトでは、CVE のログレベルは info です。 /opt/Symantec/cafagent/bin/log4j.properties ファイルで、ログ記録レベルを debug に変更できます。 ファイルを変更した後に、cafagent サービスを再起動する必要があります。
AMD ログレベルの変更。	デフォルトでは、AMD のログレベルは info です。 /opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini ファイルで、ログレベルを trace、warning、または error に変更できます。 ファイルを変更した後に、サービスを再起動する必要があります。

つの Symantec Endpoint Protection Manager とコンソールまたはデフォルトデータベースの間における通信の問題のトラブルシューティング

つの Symantec Endpoint Protection Manager コンソールまたはデフォルトデータベースとの接続に問題がある場合、以下のいずれかの症状が見られる可能性があります。

- 管理サーバーサービス (semsrv) が停止する。
- 管理サーバーサービスが、開始した状態のままにならない。
- [ホーム]、[監視]、[レポート] のページに HTTP エラーが表示される
- [ホーム]、[監視]、[レポート] のページが空白である
- [ホーム]、[監視]、[レポート] のページには、コンテンツが表示されず、進行バーが連続的に読み込まれて表示される

これらの問題が生じると、Windows イベントログに Java -1 エラーが示されます。Java -1 エラーの原因を特定するには、scm-server ログを調べます。scm-server ログはデフォルトで次の場所にあります。

SEPM_Install\tomcat\logs\scm-server-0.log

デフォルトの SEPM_Install のデフォルト値は C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager です。

Table 188: コンソールまたはデータベースとの通信の確認

チェック項目	説明
データベースと管理サーバー間の接続性をテストする。	管理サーバーとデータベースが正しく通信していることを検証できます。 データベースとの接続の検証
管理サーバーのヒープサイズが正しいことを調べる。	管理サーバーのリモートコンソールにログインできない場合、Java のヒープサイズを増加することが必要になる可能性があります。また scm-server ログにメモリ不足メッセージが表示される場合があります。 デフォルトのヒープサイズについて詳しくは「 Symantec Endpoint Protection Manager のインストール時に選択するネットワークサイズのデフォルト設定の決定 」を参照してください。
管理サーバーで複数のバージョンの PHP が実行していないことを調べる。	管理サーバーで、異なるバージョンの PHP を使っている複数のソフトウェアパッケージが実行しているかどうかを確認できます。PHP は、グローバル設定ファイル (php.ini) を確認します。複数の設定ファイルがある場合は、各製品がそれぞれのインタープリタを使うように強制する必要があります。各製品が、それぞれに関連付けられている正しいバージョンの PHP を使うと、管理サーバーは正しく動作します。
システムの必要条件の確認。	クライアントと管理サーバーの両方で、最小のシステム必要条件を実行しているか、または推奨のシステム必要条件を実行しているかを確認できます。 最新のシステム必要条件について詳しくは、「 Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件 」を参照してください。

管理サーバーのデータベースとの接続の検証

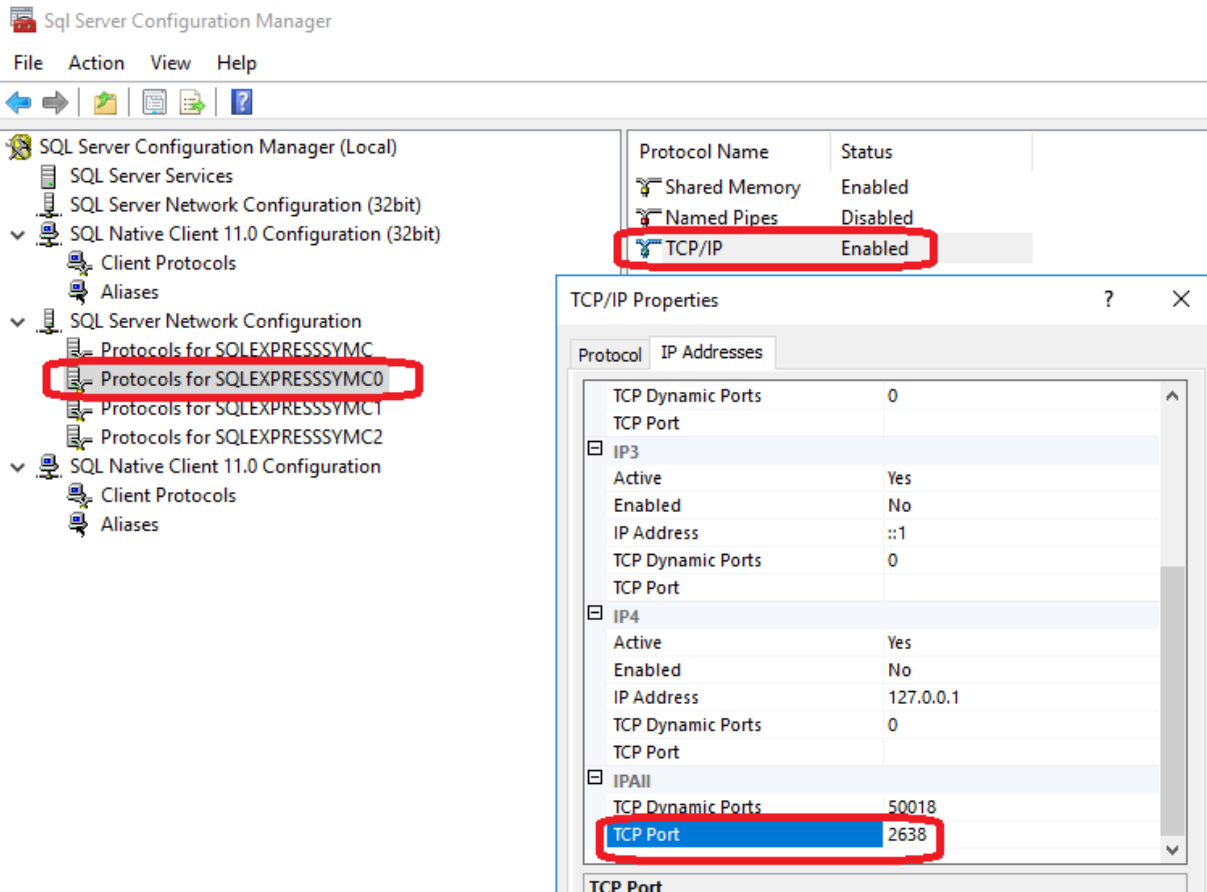
管理サーバーとデータベースが正しく通信していない場合があります。データベースが動作していることを確認してから、サーバーとデータベース間の接続をテストしてください。

Table 189: データベース接続の検証

データベースの種類	以下の手順を実行します
Microsoft SQL Server Express データベース (14.3 RU1 以降)	• SQL Server Express サービスが実行されており、sqlserver.exe プロセスが TCP ポート 2638 をリスニングしていることを確認します。 • ODBC 接続をテストします。
埋め込み Sybase データベース (14.3 MP1 以前)	• Symantec Embedded Database サービスが動作しており、dbsrv9.exe プロセスが TCP ポート 2638 を応答準備していることを確認します。 • ODBC 接続をテストします。
リモート Microsoft SQL Server データベース	• Symantec Endpoint Protection Manager をインストールし設定したときに、名前付きインスタンスを指定したことを確認します。 • SQL Server が動作し、正しく設定されていることを確認します。 • 管理サーバーと SQL データベースとの間のネットワーク接続が正しいことを確認します。 • ODBC 接続をテストします。

Microsoft SQL Server Express データベースとの通信を検証するには

1. [スタート] メニューで、[Microsoft **SQL Server 2017**] を展開し、[**SQL Server 2017** 構成マネージャー] をクリックします。
2. [**SQL Server** 構成マネージャー] ダイアログボックスで、[**SQL Server** ネットワークの構成] を展開し、[SQLEXPRESS のプロトコル] インスタンスを選択します。
[TCP/IP] フィールドを [有効] に設定する必要があります。
3. [TCP/IP] を右クリックして [プロパティ] をクリックします。
4. [IP アドレス] タブで、[IPAll] カテゴリまで下にスクロールします。[TCP ポート] フィールドには、デフォルトでポート番号 2638 が表示されます。



埋め込みデータベースとの通信を検証するには

1. 管理サーバーのコンピュータで、[スタート] > [コントロールパネル] > [管理ツール] を選択します。
2. [管理ツール] ダイアログボックスで、[データソース (ODBC)] をダブルクリックします。
3. [データソース (ODBC) アドミニストレータ] ダイアログボックスで、[システム DSN] をクリックします。
4. [システム DSN] タブで、[SymantecEndpointSecurityDSN] をダブルクリックします。
5. [ODBC] タブで、データソースの [名前] ドロップダウンリストが #SymantecEndpointSecurityDSN# になっていることを確認し、説明を入力します (省略可能)。
6. [ログイン] をクリックします。
7. [ログイン] タブの [ユーザーID] ボックスで、dba と入力します。
8. [パスワード] テキストボックスに、データベースのパスワードを入力します。
このパスワードは、管理サーバーをインストールしたときにデータベース用に入力したものです。
9. [データベース] をクリックします。
10. [データベース] タブの [サーバー名] テキストボックスで、次のように入力します。
\\servername\instancename
英語バージョンの つの Symantec Endpoint Protection Manager を使用する場合、デフォルトの sem5 を入力します。
それ以外の場合は、[サーバー名] テキストボックスを空白のままにします。
11. [ODBC] タブで、[テスト接続] をクリックして、成功するかどうかを確認します。
12. [OK] をクリックします。
13. [OK] をクリックします。

Microsoft SQL Server データベースとの通信を検証するには

1. 管理サーバーのコンピュータで、[スタート] > [コントロールパネル] > [管理ツール] を選択します。
2. [管理ツール] ダイアログボックスで、[データソース (ODBC)] をダブルクリックします。
3. [データ ソース (ODBC) アドミニストレータ] ダイアログボックスで、[システム DSN] をクリックします。
4. [システム DSN] タブで、[SymantecEndpointSecurityDSN] をダブルクリックします。
5. [サーバー] ドロップダウンリストで、正しいサーバーとインスタンスが選択されていることを確認します。
6. [次へ] をクリックします。
7. [ログイン ID] に、sa と入力します。
8. [パスワード] テキストボックスに、データベースのパスワードを入力します。
このパスワードは、管理サーバーをインストールしたときにデータベース用に入力したものです。
9. [次へ] をクリックして、デフォルトのデータベースに sem5 が選択されていることを確認します。
10. [次へ] をクリックします。
11. [完了] をクリックします。
12. [データソースのテスト] をクリックして、次のような結果を探します。

TESTS COMPLETED SUCCESSFULLY!

クライアント/サーバーの通信のファイル

クライアントとサーバー間の通信設定と他のクライアントの設定は、クライアントコンピュータのファイルに保存されます。

Table 190: クライアントのファイル

ファイル名	説明
SerDef.dat	場所ごとの通信設定を保存する暗号化ファイル。ユーザーが場所を変更するたびに、SerDef.dat ファイルを読み込んで新しい場所の適切な通信設定をクライアントに適用します。
sylink.xml	グローバルな通信設定を保存します。このファイルは内部的にのみ使われるので、編集しないでください。ファイルには Symantec Endpoint Protection Manager の設定が含まれています。このファイルを編集しても、次にクライアントが管理サーバーに接続するときに、ほとんどの設定は管理サーバーの設定で上書きされます。
SerState.dat	クライアントの画面サイズや、クライアントのネットワークとホスト悪用防止用コンソールが表示されるかどうか、Windows のサービスが表示されるかどうかなどの、ユーザーインターフェースについての情報を保存する暗号化ファイルです。クライアントは起動時にこのファイルを読み込み、ユーザーインターフェースを前回停止したときと同じ状態に戻します。

レポートに関する問題のトラブルシューティング

レポートを使うときは次の情報に注意してください。

- レポートとログのタイムスタンプ (クライアントスキャン時間を含む) はユーザーの現地時間で表されます。レポート用データベースに含まれるイベントの時刻は、グリニッジ標準時 (GMT) です。レポートを作成するときに、GMT の値がレポートを表示するコンピュータのローカル時刻に変換されます。
- 管理下クライアントのタイムゾーンが管理サーバーとは異なる場合に、[特定日を設定する] フィルタオプションを使用すると、予想外の結果が起きることがあります。クライアントと管理サーバー両方のデータと時間の精度が影響を受けることがあります。
- サーバーのタイムゾーンを変更する場合は、コンソールからログオフして再びログオンし、ログとレポートの時間が正確であることを確認してください。
- レポートデータは、セキュリティ製品に表示される内容と 1 対 1 で対応していない場合があります。この対応の不足は、レポートソフトウェアがセキュリティイベントを集計しているために発生します。
- セキュリティ向上の目的で、レポート機能で SSL を使うことができます。SSL により、機密性とデータのインテグリティが得られ、クライアントとサーバーとの間の認証が行われます。

「[SEPM と SEP クライアント間で SSL を有効にする方法](#)」を参照してください。

- レポートのリスクカテゴリの情報は、シマンテックセキュリティレスポンスの Web サイトから取得されます。つの Symantec Endpoint Protection Manager コンソールがこの情報を取得できるまで、生成するレポートのリスクカテゴリのフィールドには [不明] が表示されます。
- 生成するレポートでは、ネットワーク内のセキュリティが低下したコンピュータが正確に示されます。レポートは Windows のレジストリデータではなく、ログデータに基づきます。
- 大量のデータを含むレポートを実行するときにデータベースエラーが発生する場合は、データベースのタイムアウトパラメータを変更します。

レポートとログを見直すためのタイムアウトパラメータの変更

- CGI エラーまたはプロセス終了エラーが発生する場合、その他のタイムアウトパラメータを変更すると安全です。詳しくは、「[SEPM Reporting does not respond or shows a timeout error message when querying large amounts of data](#)」という記事のマニュアルを参照してください。
- コンピュータでループバックアドレスの使用を無効にした場合、レポートページは表示されません。[ループバックアドレスの使用が無効になっている場合のレポートページへのアクセス](#)

レポートとログを見直すためのタイムアウトパラメータの変更

大量のデータが含まれるレポートまたはログを表示しているときにデータベースエラーが発生する場合は、次の変更を行うことができます。

- データベース接続のタイムアウトの変更
- データベースコマンドのタイムアウトの変更

これらの値のレポートのデフォルトは次のとおりです。

- 接続タイムアウトは 300 秒 (5 分)
- コマンドタイムアウトは 300 秒 (5 分)

1. Reporter.php のデータベースのタイムアウト値を変更するには、つの Symantec Endpoint Protection Manager サーバーで次のデフォルトのフォルダを参照します。

C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager\Php\Include\Resources

2. メモ帳のようなテキスト形式エディタで、Reporter.php ファイルを開きます。

3. **\$CommandTimeout** という行と **\$ConnectionTimeout** という行を探し、値を増やします (単位は秒)。行が存在しない場合は作成します。たとえば、タイムアウト期間を 10 分に延ばすには、この行を次の値に変更します。

```
$CommandTimeout = 600;
```

```
$ConnectionTimeout = 600;
```

これらの新しい行を ?> の前に追加します。

4. Reporter.php ファイルを保存して閉じます。

NOTE

ゼロを指定するか、フィールドを空白のままにすると、デフォルトの設定が使われます。

CGI エラーまたはプロセス終了エラーが起きる場合は、次のパラメータを変更すると効率的です。

- Php.ini ファイルの max_execution_time パラメータ
 - httpd.conf ファイルの Apache タイムアウトパラメータ FcgidIOTimeout、FcgidBusyTimeout、FcgidIdleTimeout
5. Php.ini の max_execution_time パラメータを変更するには、つの Symantec Endpoint Protection Manager サーバーで次のデフォルトのフォルダを参照します。

C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager\Php

-
6. Php.ini ファイルを右クリックして [プロパティ] をクリックします。
 7. [全般] タブで、[読み取り専用] のチェックマークをはずします。
 8. [OK] をクリックします。
 9. メモ帳のようなテキスト形式エディタで、Php.ini ファイルを開きます。
 10. **max_execution_time** というエントリを探し、値を増やします (単位は秒)。たとえば、タイムアウトを 10 分に延ばすには、この行を次の値に変更します。
`max_execution_time=600`
 11. Php.ini ファイルを保存して閉じます。
 12. Php.ini ファイルを右クリックして [プロパティ] をクリックします。
 13. [全般] タブで、[読み取り専用] にチェックマークを付けます。
 14. [OK] をクリックします。
 15. httpd.conf の Apache タイムアウトパラメータを変更するには、つの Symantec Endpoint Protection Manager サーバーで次のデフォルトのフォルダを参照します。
`C:\Program Files (x86)\Symantec\つの Symantec Endpoint Protection Manager\apache\conf`
 16. メモ帳のようなテキスト形式エディタで、httpd.conf ファイルを開きます。
 17. 次の行を探し、値を増やします (単位は秒)。
 - `FcgidIOTimeout 1800`
 - `FcgidBusyTimeout 1800`
 - `FcgidIdleTimeout 1800`
 18. httpd.conf ファイルを保存して閉じます。

ループバックアドレスの使用が無効になっている場合のレポートページへのアクセス

コンピュータでループバックアドレスの使用を無効にした場合、レポートページは表示されません。つの Symantec Endpoint Protection Manager コンソールにログオンしようとしたり、レポート機能にアクセスしようとすると、次のエラーメッセージが表示されます。

レポートコンポーネントと通信できません

[ホーム] ページ、[監視] ページ、[レポート] ページは空白です。[ポリシー] ページ、[クライアント] ページ、[管理] ページは通常どおり表示され、機能します。

ループバックアドレスを無効にしているときに、[レポート] のコンポーネントを表示するには、localhost という語をコンピュータの IP アドレスに関連付ける必要があります。Windows の hosts ファイルを編集して、localhost を IP アドレスに関連付けることができます。

スタンドアロン Web ブラウザからのレポートへのログオン

Windows を実行しているコンピュータ上で localhost を IP アドレスに関連付けるには

1. ディレクトリを hosts ファイルの場所に変更します。
デフォルトでは、hosts ファイルは %SystemRoot%\system32\drivers\etc
2. エディタで hosts ファイルを開きます。
3. hosts ファイルに次の行を追加します。
`IPAddress localhost #レポート機能にログオンするため`

ここで、IPAddressは自分のコンピュータの IP アドレスで置き換えます。シャープ記号 (#) の後には任意のコメントを追加できます。たとえば、次の行を入力できます。

192.168.1.100 localhost # このエントリは、コンソールコンピュータ用の IPv4 です

2001:db8:85a3::8a2e:370:7334 localhost # このエントリは、コンソールコンピュータ用の IPv6 アドレスです
IPv6 はバージョン 14.2 以降でサポートされます。

4. ファイルを保存して閉じます。

つの Symantec Endpoint Protection Manager コンソールから Power Eraserを実行する前に知るべきこと

Power Eraser は、積極的なスキャンと分析を提供し、重度に感染した Windows コンピュータにおける問題の解決を支援します。Power Eraser の分析は積極的なため、場合によっては必要とする重要なファイルに対してフラグを付けることがあります。Power Eraser はウイルススキャンやスパイウェアスキャンよりも誤認が生じる可能性があります。

WARNING

コンピュータが不安定性を示していたり、持続的な問題があるときなど、緊急の状況においてのみ Power Eraser を実行することになります。通常、単一のコンピュータまたは小さいグループのコンピュータで Power Eraser を実行します。他のアプリケーションと同時に実行しないでください。場合によって、通常のスキャンイベントでも Power Eraser の分析を実行するよう警告が出されます。

Power Eraser を 1 つの Symantec Endpoint Protection Manager から使うことと SymDiag ツールでローカルで使うことの違い

Windows クライアントの管理コンソールから **Power Eraser** をリモートで実行できます。**Symantec Endpoint Protection** にはクライアントから **Power Eraser** を直接起動するオプションは含まれません。ただし、クライアントコンピュータのユーザーは **SymDiag** ツールをダウンロードしてツールから **Power Eraser** を実行することができます。

- SymDiag ツールを使うと、Power Eraser の検出は 1 つの Symantec Endpoint Protection Manager ログに表示されません。
- コンソールから Power Eraser を実行する場合、Power Eraser は SymDiag ツールが検査するユーザー固有のロードポイント、登録、およびフォルダは検査しません。

NOTE

Power Eraser を、コンソールからとローカルで SymDiag ツールを使って同時に実行しないようにしてください。同時に実行すると、コンピュータのパフォーマンスが低下する可能性があります。

Power Eraser は多量のコンピューターリソースを消費します。コンピュータで Power Eraser を複数回実行すると、Power Eraser ファイルがコンピュータ上の容量を大量に消費します。各分析の実行時に、Power Eraser は Symantec Endpoint Protection のアプリケーションフォルダに格納されるファイルに検出情報を保存します。これらのファイルは、クライアントがログをパージするときにパージされます。

Power Eraser がウイルススキャンやスパイウェアスキャンとどう異なるか

Power Eraser は通常のスキャンと次の点で異なります:

- 完全スキャンと違い、Power Eraser はコンピュータ上の各ファイルをすべてスキャンすることはありません。Power Eraser はロードポイントとロードポイントのディスクの場所、また実行中のプロセスとインストールされたサービスを検査します。
- Power Eraser の検出は検疫に表示されません。
- Power Eraser はウイルススキャンとスパイウェアスキャンよりも優先します。Power Eraser を実行すると、Symantec Endpoint Protection は進行中のウイルススキャンとスパイウェアスキャンをキャンセルします。
- Power Eraser は検出を自動修復しません。スキャンログまたはリスクログの検出のリストを見直し、ログから処理を選択してください。検出を除去するか、検出を安全としてマーク付け（放置）するか選択できます。除去された検出を復元する（元に戻す）こともできます。

Power Eraser は通常モードまたはルートキットモードで実行可能です。ルートキットモードはスキャンを開始する前に再起動する必要があります。また、Power Eraser の検出を除去することを選択した場合、修復を完了するためにコンピュータを再起動する必要があります。

Power Eraser を実行する必要があるときに実行する高レベルの手順の概略

コンソールから **Power Eraser** を実行するときに次の 2 つの高レベルの手順を実行します。

- 単一コンピュータまたは複数コンピュータの小さいグループで Power Eraser の分析を開始します。Power Eraser は、誤認の可能性を考慮して、検出を自動的に修復しません。
- リスクログまたはスキャンログを使って Power Eraser の検出を見直し、脅威と判断した検出をすべて Power Eraser が削除するよう手動で指示してください。また、検出を無視して放置するものとして対応することもできます。

コンソールから Power Eraser を実行する方法と、コンソール設定を正しく設定したことを確かめる方法について詳しくは、ワークフローを確認してください。

[つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク](#)

Power Eraser に影響する 一つの Symantec Endpoint Protection Manager ポリシー設定の概要

次に **Power Eraser** に影響するポリシーの設定を示します。

- ユーザー介入のためのスキャン設定
ユーザーによるウイルススキャンとスパイウェアスキャンのキャンセルを許可すると、Power Eraser の分析もキャンセル可能になります。ただし、ユーザーは Power Eraser を一時停止したり休止することはできません。
[Windows コンピュータでのユーザーによるスキャンの進行状況の表示とスキャンの操作の許可](#)
- 例外ポリシー
Power Eraser は次のウイルスとスパイウェアの例外を適用します: ファイル、フォルダ、既知のリスク、アプリケーション、および信頼できる Web ドメイン。Power Eraser は拡張子の例外を適用しません。
[ウイルスとスパイウェアのスキャンの例外作成](#)
- ログの保持設定
検出がログに表示される限り Power Eraser の検出に対して処理を適用することができます。ログはウイルス対策とスパイウェア対策のポリシーで指定された一定期間後にページされます。デフォルトでは、ログイベントは 14 日間利用可能です。ログの保持設定は修正可能で、イベントの期限後に、別のスキャンを実行してログを再ポピュレートすることができます。
[Windows コンピュータのログ処理と通知設定の修正](#)
- 再起動オプション
ルートキット検出モードで Power Eraser を実行する選択をする場合、再起動の設定をルートキットの分析に特化して行えます。管理者には再起動する権限が必要です。Power Eraser の検出の削除を選択した後、コンピュータはグループの再起動の設定を使います。Power Eraser は再起動と修復を完了するのにルートキットの再起動の設定を使いません。
[一つの Symantec Endpoint Protection Manager からのクライアントコンピュータの再起動](#)
- 評価のクエリー
Power Eraser は、ファイルについてスキャンを実行し決定を行う場合に、クラウドで Symantec Insight サーバーを使います。評価のクエリーを無効にしたり、クライアントコンピュータが Insight サーバーに接続できない場合、Power

Eraser では Symantec Insight を使うことができません。Symantec Insight がないと、Power Eraser は検出数が少なくなり、誤認を生じる検出結果を出す可能性が高くなります。評価のクエリーは [脅威検出のインサイトルックアップを許可する] オプションが有効になると有効になります。このオプションはデフォルトで有効になっています。

[Symantec Endpoint Protection が Symantec Insight を使ってファイルに関する決定を下す方法](#)

- 提出

Symantec Endpoint Protection は [ウイルス対策の検出] オプションが有効の場合に、シマンテック社に Power Eraser の検出についての情報を送ります。このオプションはデフォルトで有効になっています。

[サーバーデータ収集とクライアント提出、ネットワークのセキュリティにおけるそれらの重要性について](#)

[Symantec Diagnostic Tool \(SymDiag\) を使ったコンピュータの問題のトラブルシューティング](#)

つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク

通常、[リスク] ログが修復の失敗を示し、Power Eraser の実行を推奨するときに、Power Eraser の分析を実行する必要があります。コンピュータが不安定になり、削除することができないマルウェアまたはウイルスがあるような状態のときにも、Power Eraser を実行することになります。

WARNING

Power Eraser は注意して使用してください。この分析は強力で、誤認を導く傾向があります。

[つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知べきこと](#)

Windows クライアントコンピュータのみで つの Symantec Endpoint Protection Manager から Power Eraser を実行できます。

NOTE

Power Eraser はルートキットの検出なし、ルートキットの検出ありの 2 つのモードのいずれか 1 つで動作します。ルートキットの検出の分析では再起動が必要になります。管理者はルートキットの検出を用いて Power Eraser を実行するために、再起動する権限がなければなりません。

Table 191: つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク

タスク	説明
Power Eraser を実行するための管理者権限を設定する	Power Eraser をクライアントコンピュータ上で実行するには、管理者は次のコマンドアクセス権が必要です: Power Eraser 分析の開始 - クライアントコンピュータの再起動 (ルートキットの検出を用いて Power Eraser を実行するために必要) 管理者アカウントの追加とアクセス権の設定
ログの保持ポリシーを設定します	ログの保持設定は、Power Eraser の修復と復元の処理を実行する際にイベントが利用可能になる時間の長さに影響します。これらの処理を考慮してより多くの時間が必要な場合はログの保持設定を修正できます。また、ログを再ポピュレートするために Power Eraser を実行できます。ログの保持設定はウイルス対策とスパイウェア対策ポリシーのその他のオプションの一部です。 Windows コンピュータのログ処理と通知設定の修正
クライアントにインターネット接続があることを確認する	クライアントコンピュータは、Power Eraser が潜在的な脅威について決定するために Symantec Insight 評価データを使えるように、インターネットアクセスが必要です。インターネットアクセスが断続的または存在しない場合、Power Eraser は Symantec Insight を使うことができないことになります。Symantec Insight がないと、Power Eraser は検出数が少なくなり、誤認を生じる検出結果を出す可能性が高くなります。

タスク	説明
つの Symantec Endpoint Protection Manager からクライアントコンピュータ上で Power Eraser 分析を開始する;	Power Eraser を通常モードまたはルートキットモードのどちらで実行するか選択します。つの Symantec Endpoint Protection Manager の複数の場所から Power Eraser コマンドを発行できます。 • [クライアント] ページ • コンピュータ状態ログ • リスクログ Note: クライアントコンピュータのユーザーは Power Eraser をクライアントユーザーインターフェースから直接実行できません。Power Eraser は SymDiag ツールの一部として利用可能です。ただし、クライアントユーザーがツールを実行すると、Power Eraser の検出を含んでいる結果ログは つの Symantec Endpoint Protection Manager に送信されません。 つの Symantec Endpoint Protection Manager からの Power Eraser の分析の開始 コンピュータの状態ログのコマンドの状態を表示できます。見やすくするため Power Eraser コマンドだけを表示するようにログをフィルタ処理することができます。 Power Eraser の実行後、スキャンログまたはリスクログに結果を表示します。スキャンログはスキャン結果が保留中であるかどうかを示します。
クライアントコンピュータ上の Power Eraser コマンドまたは処理をキャンセルする	Power Eraser コマンドをキャンセルするには、コマンド状態のログを使います。 Note: 再起動を求めるプロンプトがクライアントコンピュータに表示された後は、ルートキットモードで実行中の Power Eraser の実行を取り消すことはできません。再起動後、ウイルス対策とスパイウェア対策ポリシーによってユーザーによるスキャンのキャンセルが許可されると、コンピュータのユーザーだけが Power Eraser をキャンセルできます。 Power Eraser コマンドをキャンセルすると、修復や取り消しの処理も含めた、すべての Power Eraser 分析に関連付けされているあらゆる保留状態の処理もキャンセルされます。 コンソールを使った、クライアントコンピュータでのコマンドの実行
ログから Power Eraser の検出を表示する	Power Eraser の検出を つの Symantec Endpoint Protection Manager の次のログから表示できます。 • スキャンログ スキャンログには Power Eraser の結果だけ表示する [スキャンの種類] フィルタがあります。この表示でスキャン結果が保留中であるかどうか示されます。フィルタ処理された表示で [検出] を選択して [Power Eraser の検出] を表示することができます。 • リスクログ リスクログにも Power Eraser の検出用の同じようなフィルタがあります。ただし、リスクログではスキャン結果が保留状態であるかどうか示されません。 • コンピュータ状態ログ コンピュータの状態ログでは [感染] 列にレポートのアイコンが含まれる場合があります。イベントの詳細のアイコンは修復できない現存するすべての脅威を示すレポートにリンクします。レポートにはログ記録のみの検出と未解決の検出が含まれています。レポートがいくつかのコンピュータ上で Power Eraser を実行することを推奨する場合があります。 Power Eraser アイコンは、管理者の処理を必要とするコンピュータ上のすべての Power Eraser の検出を示すレポートにリンクします。 これらのアイコンは [クライアント] ページの [健全性状態] の列にも表示されます。 ログの表示
クライアントコンピュータで Power Eraser を実行するよう推奨する通知を確認する	デフォルトでは、管理者は通常のスキャンで感染を修復できない場合で、Power Eraser が推奨されるときに通知を受信します。[監視] > [通知] ページで [Power Eraser を推奨] の通知を確認できます。 通知の表示と対応

タスク	説明
[コマンドの状態] ページで Power Eraser の検出を表示する	[コマンドの状態] ページで Power Eraser の検出についてのレポートにアクセスできます。イベントの詳細のアイコンは [完了状態] 列に表示されます。アイコンは [Power Eraser の分析の開始] コマンドおよび他のスキャンコマンドによってなされた検出の情報を示すレポートにリンクします。 コマンドの状態の詳細オプションは、特定のスキャンについての情報を提示します。イベントの詳細のアイコンをクリックして、特定のクライアントコンピュータについての情報を入手できます。 コンソールを使った、クライアントコンピュータでのコマンドの実行
[クライアント] タブから Power Eraser の検出を表示する	[クライアント] ページの [クライアント] タブから Power Eraser の検出についてのレポートにアクセスできます。 レポートのアイコンは利用可能な情報がある場合に [健全性状態] 列に表示されます。イベントの詳細のアイコンは修復できない現存するすべての脅威を示すレポートにリンクします。レポートには Power Eraser 検出が含まれます。 Power Eraser アイコンは、管理者の処理を必要とするコンピュータ上のすべての Power Eraser の検出を示すレポートにリンクします。 アイコンはコンピュータの状態ログにも表示されます。 クライアントコンピュータの保護状態の表示
つの Symantec Endpoint Protection Manager のスキャンログやリスクログから Power Eraser の検出を修復または復元する	他の Symantec Endpoint Protection スキャンとは異なり、Power Eraser は検出された脅威を自動的に修復しません。Power Eraser の分析は強力で、多くの誤認検出をする可能性があります。検出に修復が必要だと判断した後に、手動で修復を開始してください。 修復した Power Eraser の検出を元に戻す (復元する) こともできます。 Power Eraser の検出の対処

つの Symantec Endpoint Protection Manager からの Power Eraser の分析の開始;

単一コンピュータまたはコンピュータのグループ上の永続的な脅威を分析して検出するために Power Eraser を実行できます。

つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知ること

Power Eraser が潜在的なリスクを検出した後、リスクを表示し、どのリスクが脅威であるか判断します。Power Eraser はリスクを自動修復しません。脅威と判断したリスクを修復するには手動で Power Eraser を実行する必要があります。また他の保護機能が検出する特定の脅威に対しても Power Eraser を実行できます。Power Eraser は検出と関連付けされているコンピュータで実行します。

つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク

Power Eraser の検出の対処

NOTE

Power Eraser をルートキットモードで実行して、再起動オプションのメッセージがクライアントコンピュータ上で表示されると、管理者またはユーザーが Power Eraser をキャンセルすることはできません。再起動後、ウイルス対策とスパイウェア対策ポリシーによってユーザーによるスキャンのキャンセルが許可されると、ユーザーは Power Eraser をキャンセルできます。

1. つの Symantec Endpoint Protection Manager の [クライアント] ページから Power Eraser の分析を開始するには、[クライアント] ページで、[クライアント] タブで、分析するコンピュータを選択します。
- 多数のコンピュータを選択すると、ネットワークのパフォーマンスが低下する可能性があります。

-
2. [タスク] で、[コンピュータでコマンドを実行する] をクリックし、次に [Power Eraser 分析の開始] をクリックします。
 3. [Power Eraser スキャンの種類の選択] ダイアログで、Power Eraser をルートキットモードで実行するかしないかを選択します。ルートキットモードの場合は、再起動オプションを設定できます。再起動オプションを設定し、ルートキットスキャンを実行するには管理者権限が必要です。
 4. [OK] をクリックします。

Power Eraser が選択したコンピュータで実行します。[監視] ページの [コマンドの状態] タブでコマンドをキャンセルすることができます。
 5. つの Symantec Endpoint Protection Manager の [コンピュータの状態] ログから Power Eraser の分析を開始するには、コンソールのサイドバーで、[監視] をクリックし、[ログ] タブを選択します。
 6. [ログの種類] リストボックスで [コンピュータ状態] ログを選択して、[ログの表示] をクリックします。
 7. Power Eraser を実行するコンピュータを選択し、[コマンド] ドロップダウンリストから [Power Eraser の分析の開始] を選択します。

多数のコンピュータを選択すると、ネットワークのパフォーマンスが低下する可能性があります。
 8. [開始] をクリックします。
 9. [Power Eraser スキャンの種類の選択] ダイアログで、Power Eraser をルートキットモードで実行するかしないかを選択します。ルートキットモードの場合は、再起動オプションを設定できます。再起動オプションを設定し、ルートキットスキャンを実行するには管理者権限が必要です。
 10. [OK] をクリックします。

Power Eraser が選択したコンピュータで実行します。[コマンドの状態] タブでコマンドをキャンセルすることができます。
 11. つの Symantec Endpoint Protection Manager の [リスク] ログから Power Eraser の分析を開始するには、コンソールのサイドバーで、[監視] をクリックし、[ログ] タブを選択します。
 12. [ログの種類] リストボックスで [リスク] ログを選択して、[ログの表示] をクリックします。
 13. Power Eraser を実行する対象のリスクを選択します。[イベント処理] 列に、Power Eraser を実行するよう求める警告が表示される場合があります。

ログのすべてのリスクに対して Power Eraser を実行できます。
 14. [処理] ドロップダウンまたは [処理] 列から [Power Eraser の分析の開始] を選択します。
 15. [開始] をクリックします。
 16. [Power Eraser スキャンの種類の選択] ダイアログで、Power Eraser をルートキットモードで実行するかしないかを選択します。ルートキットモードの場合は、再起動オプションを設定できます。再起動オプションを設定し、ルートキットスキャンを実行するには管理者権限が必要です。
 17. [OK] をクリックします。

Power Eraser は選択したリスクで感染しているコンピュータ上で実行します。[コマンドの状態] タブでコマンドをキャンセルすることができます。

Power Eraser の検出の対処

Power Eraser は、その積極的な検出機能により誤認が発生するため、スキャン中に検出内容を修復しません。検出内容を確認し、修復するかまたはそのままにしておくかを決定した上で、ログから検出イベントの修復を要求する必要があります。修復を選択すると、Power Eraser は検出に関連するファイルを削除します。ただし、削除したファイルはログがページされるまで復元可能です。

Power Eraser イベントの利用可能期間はログの保持ポリシーにより決定します。デフォルトでは、イベントの利用可能期間は 14 日間です。

つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク

つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知るべきこと

Power Eraser の検出に対処するには

1. Power Eraser の分析が完了したことを確認します。

- コンピュータの状態ログには、スキャンが完了したことを示すアイコンがあります。
- スキャンログは Power Eraser が分析を終了したかどうかを示します。

2. リスクログまたは [スキャンログ] > [検出の表示] ページで、1 つの検出または複数の検出を選択して処理を適用します。

- [処理] 列で、[潜在的なリスクが見つかりました (管理の処理の保留)] というラベルが付いている特定のリスクの横にあるプラスアイコンをクリックします。
- [潜在的なリスクが見つかりました (管理の処理の保留)] というラベルが付いているリスクを複数選択し、[処理] ドロップダウンメニューから処理を選択します。

3. 次の処理のいずれかを選択します。

- **Power Eraser** が検出したリスクを削除する
リスクをコンピュータから削除することでリスクの修復を行います。Power Eraser は、復元可能な安全なバックアップファイルを作成します。
- **Power Eraser** が検出したリスクを無視する
検出内容を確認した上でリスクを修復しないことを肯定します。

NOTE

この処理は管理コンソールのログのみでイベント処理を「管理者による放置」に変更します。この指定では、クライアント上の対応のイベント処理が更新されません。クライアントログの表示では、イベント処理が継続的に「分析保留」として表示されます。

4. [処理] ドロップダウンメニューから処理を選択した場合は、[適用] をクリックします。

[**Power Eraser** が検出したリスクを無視する] を選択した場合、検出が [潜在的なリスクが見つかりました (放置)] として表示されます。

[潜在的なリスクが見つかりました (削除)] というラベルの付いた削除済みの検出は、[**Power Eraser** が削除したリスクを復元する] 処理を選択することで復元できます。

Table 192: Power Eraser の検出状態の概略

検出の状態	説明
管理の処理の保留	Power Eraser が潜在的な脅威としてリスクを検出しました。リスクを確認して、Power Eraser にそのリスクを修復させるか、そのまま放置するかを決定します。
復元	管理者が Power Eraser にリスクの修復を要求したときに、移動したすべてのファイルを修復した状態です。
削除	管理者がリスクの修復と削除を Power Eraser に要求した状態です。Power Eraser は、リスクを削除するときにリスクに関連するファイルを削除しますが、復元可能な安全なバックアップコピーを作成します。後で削除済みのリスクが実際にはリスクではないと判別したときに、削除済みのリスクを復元できます。ファイルは、ログイベントがパージされるまで復元可能です。
管理者による放置	管理者が Power Eraser にリスクの放置を要求した状態です。

付録

クライアント機能の比較、ツール、コマンドラインオプション、サードパーティインストールツールに関するリファレンス情報の取得

このセクションでは、クライアントの機能比較、Symantec Endpoint Protection に含まれるツール、クライアントのコマンドラインオプション、サードパーティツールを使った Windows インストールなどを説明します。

プラットフォームに基づく Symantec Endpoint Protection の機能

- プラットフォームに基づくクライアントの保護機能
- プラットフォームに基づく管理サーバー機能
- プラットフォームに基づく自動更新機能
- プラットフォームに基づくウイルスとスパイウェアの対策ポリシーの設定
- プラットフォームに基づく侵入防止ポリシーとメモリエクスプロイト緩和機能ポリシーの設定
- プラットフォームに基づく LiveUpdate ポリシー設定
- プラットフォームに基づく Web とクラウドのアクセス保護 ポリシー設定 (統合から Network Traffic Redirection に変更)
- プラットフォームに基づくポリシー設定
- プラットフォーム別 Device Control の差異

クライアントのインストールの種類を選択する方法

Windows クライアント用の Symantec Endpoint Protection 機能の依存関係 (12.1.x から 14.x)

プラットフォームに基づくクライアントの保護機能

Table 193: プラットフォームに基づくクライアントの保護機能

クライアント機能	Windows	Mac	Linux
ウイルス対策とスパイウェア対策	はい	はい	はい
ネットワークとホスト悪用防止 - ネットワーク脅威防止 (侵入防止とファイアウォール) - メモリエクスプロイト緩和機能 (14 では汎用エクスプロイト緩和機能として導入)	はい	- ファイアウォール (14.2 以降) - 侵入防止 (12.1.4 以降) Mac の侵入防止はカスタムシグネチャをサポートしません。	【※No※】
プロアクティブ脅威防止 - アプリケーションとデバイス制御 - SONAR	はい	Device Control のみ (14 現在)	【※No※】
ホストインテグリティ	はい	【※No※】	【※No※】
他の保護 - システムロックダウン - 改変対策	はい	【※No※】	【※No※】

アプリケーション制御、システムロックダウン、デバイス制御について

ホストインテグリティの仕組み

プラットフォームに基づく管理機能

Table 194: プラットフォームに基づく管理機能

管理機能	Windows	Mac	Linux
つの Symantec Endpoint Protection Manager からのクライアントのリモート配備 • Web リンクと電子メール • リモートプッシュ • パッケージの保存	はい	はい	はい ([Web リンクと電子メール]、[パッケージの保存] のみ)
管理サーバーからクライアントのコマンド実行	• スキャン • コンテンツの更新 • コンテンツの更新とスキャン • Power Eraser 分析の開始 (12.1.5 現在) • クライアントコンピュータの再起動 • Auto-Protect を有効にする • ネットワーク脅威防止を有効にする • ネットワーク脅威防止を無効にする • ダウンロードインサイトを有効にする • ダウンロードインサイトを無効にする • ファイルフィンガープリントリストを収集する (12.1.6 現在) • 検疫から削除** • すべてのスキャンを中止**	• スキャン • コンテンツの更新 • コンテンツの更新とスキャン • クライアントコンピュータの再起動 (ハード再起動のみ) • Auto-Protect を有効にする • ネットワーク脅威防止を有効にする (12.1.4 現在) • ネットワーク脅威防止を無効にする (12.1.4 現在)	• スキャン • コンテンツの更新 • コンテンツの更新とスキャン • Auto-Protect を有効にする
学習済みアプリケーションとネットワークアプリケーション監視を有効にする	はい	【※No※】	【※No※】
場所を作成して場所別に適用するセキュリティポリシーを設定する	はい	はい	【※No※】 コマンドラインを使ってクライアントの場所を表示できますが、クライアントは特定の基準に基づいて場所を自動的に切り替えません。
クライアントの再起動オプションを設定する	はい	【※No※】	【※No※】

管理機能	Windows	Mac	Linux
クイックレポートと定時レポート	- 監査 - アプリケーションとデバイス制御 - コンプライアンス - コンピュータの状態 - ディセプション (14.0.1) - ネットワークとホスト悪用防止 - リスク - スキャン - システム	- コンピュータの状態 - ネットワークとホスト悪用防止 - リスク - スキャン	- 監査 - コンピュータの状態 - リスク - スキャン - システム
クライアントコンピュータで保守管理されるログのサイズと保存期間を設定する	- システム - セキュリティとリスク - セキュリティ - トラフィック - パケット - 制御	- システム - セキュリティとリスク - セキュリティ	- システム - セキュリティとリスク
クライアントを保護するパスワード	はい	クライアントをアンインストールする (14.0.1)	【※No※】
SylinkDrop ツールを実行し、異なる管理サーバーにクライアントを移動する	はい	はい	【※No※】
「通信の更新パッケージの配備」オプションでクライアントパッケージを再配備し、異なる管理サーバーにクライアントを移動する	はい	はい	【※No※】
シマンテック社に匿名セキュリティ情報のクライアント提出を設定する	はい	(12.1.4 以降) 提出の設定はウイルス対策の検出情報のみを制御します。 クライアントで侵入防止提出の有効と無効を手動で切り替えることができます。 Symantec Endpoint Protectionでの Mac クライアント用 IPS データ提出を無効にする方法	【※No※】
匿名システムと使用状況の情報を安全に送信するためのクライアントの設定	はい	【※No※】	【※No※】
管理サーバーとクライアントの間の外部通信を管理する	はい	LiveUpdate のみ	【※No※】

管理機能	Windows	Mac	Linux
クライアント通信設定を管理する	- 管理サーバーリスト - 通信モード（プッシュ型転送またはプル型転送） - ハートビート間隔を設定する - 学習済みアプリケーションをアップロードする - 重要なイベントをすぐにアップロードする - ダウンロードのランダム化を設定する - 再接続の環境を設定する	- 管理サーバーリスト - 通信モード（プッシュ型転送またはプル型転送） - ハートビート間隔を設定する - ダウンロードのランダム化を設定する - 再接続の環境を設定する	- 管理サーバーリスト - 通信モード（プッシュ型転送またはプル型転送） - ハートビート間隔を設定する
専用サーバー (12.1.6) を使うようにクライアントを設定する - Insight ルックアップおよび提出用のエンドポイントの検出とレスポンスサーバー - Insight ルックアップ用の専用インサイトサーバー	はい	【※No※】	【※No※】
自動更新によって Symantec Endpoint Protection クライアントを自動的にアップグレードする	はい	はい (14)	【※No※】
既存のサードパーティ製セキュリティソフトウェアを自動的にアンインストールする	はい	【※No※】	【※No※】
問題のある Symantec Endpoint Protection クライアントを自動的にアンインストールする	はい (14)	【※No※】	【※No※】
つの Symantec Endpoint Protection Manager のログオンの認証	- Symantec Endpoint Protection Manager 認証 2 要素認証 (14.2) - RSA SecurID 認証 - ディレクトリ認証 - スマートカード (PIV/CAC) 認証 (14.2)	なし	なし

** つの Symantec Endpoint Protection Manager でログを表示するには、これらのコマンドを実行するしかありません。

[クライアントコンピュータで実行できるコマンドについて](#)

[つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する必要があるときに実行するタスク](#)

[クライアントコンピュータで動作するアプリケーションとサービスの監視](#)

[クライアントとサーバー間の接続の管理](#)

[\[通信の更新パッケージの配備 \] を使ったクライアントサーバー通信の復元](#)

[プラットフォームに基づく自動更新の差異](#)

Table 195: プラットフォームに基づく自動更新の差異

機能	Windows	Mac
デルタパッケージ	標準およびダークネットワーククライアントは、つの Symantec Endpoint Protection Manager が生成する差分のアップグレードパッケージを受信します。埋め込みクライアントは、アップグレードの完全なインストールパッケージを受信します。	Mac クライアントは、常にアップグレードの完全なインストールパッケージを受信します。
設定オプション	カスタムインストールフォルダや、既存のセキュリティソフトウェアをアンインストールするオプションが用意されています。	再起動とアップグレード用のみ。インストールフォルダはカスタマイズできません。インストールのログ記録は常に /tmp/sepinstall.log に書き込まれます。
[クライアントインストールの設定] でのアップグレードの完了後の再起動オプション	Windows クライアントコンピュータを再起動しないためのオプションが用意されています。	再起動しないようにするオプションは用意されていません。Mac クライアントコンピュータは、アップグレードが完了すると常に再起動します。
[クライアントをパッケージでアップグレード] ウィザード	Windows クライアントでは機能セットを変更できます。	Mac クライアントで設定する機能は修正できません。
以前のバージョンからのアップグレード	サポート対象のアップグレードパスに基づいて以前のバージョンから最新版に Symantec Endpoint Protection をアップグレードできます。	バージョン 12.1.6.x 以前からのアップグレードではサポートされません。たとえば、自動更新を使って 12.1.6.4 から 14 にアップグレードすることはできません。

[自動更新によるクライアントソフトウェアのアップグレード](#)

[Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象アップグレードパス](#)

[クライアントのインストールの種類を選択する方法](#)

[プラットフォームに基づくウイルスとスパイウェアの対策ポリシーの設定](#)

Table 196: プラットフォームに基づくウイルスとスパイウェアの対策ポリシーの設定

ポリシー設定	Windows	Mac	Linux
管理者定義のスキャン	- 定時スキャン (アクティブ、完全、カスタム) - オンデマンドスキャン - トリガのスキャン - 起動時スキャン - 未実行提示スキャンの再試行 - ランダム化された定時スキャン	- 定時スキャン (カスタム) - オンデマンドスキャン - 未実行提示スキャンの再試行	- 定時スキャン (カスタム) - オンデマンドスキャン - 未実行提示スキャンの再試行
Auto-Protect	- Auto-Protect を有効にする - すべてのファイルをスキャンする - 選択した拡張子のみをスキャンする - ファイルの内容を調べることによって種類を判断する - セキュリティリスクをスキャンする - リモートコンピュータ上でファイルをスキャンする (14) - ファイルにアクセス、修正、バックアップが発生した場合にスキャンする - ブートウイルスを削除するか、単にログに記録することにとどめるオプションを指定した上でフロッピーディスクをスキャンし、ブートウイルスを検出する - 感染ファイルまたはセキュリティリスクが新たに発生した場合、常に削除する - ファイルの時刻を保持する - スキャン速度またはアプリケーション速度のスキャンパフォーマンスを調整する - バックされたマルウェアのエミュレータ (14)	- Auto-Protect を有効にする - 感染ファイルを自動的に修復する - 修復できないファイルを検疫する - 圧縮ファイルをスキャン - すべてのファイルをスキャンする - 選択したフォルダのみをスキャンする - 選択したフォルダを除くすべての場所をスキャンする - セキュリティリスクをスキャンする 現在のクライアントのマウントをスキャンする - データディスク - 他のすべてのディスクとデバイス レガシークライアントのマウントのスキャンする (12.1.3 以前) : - 音楽ディスクまたはビデオディスク - iPod プレーヤー - スキャン中に進行状況を表示する	- Auto-Protect を有効にする - すべてのファイルをスキャンする - 選択した拡張子のみをスキャンする (14.3 RU1 で削除) - リムーバブルメディアをスキャンする - セキュリティリスクをスキャンする - リモートコンピュータ上でファイルをスキャンする - ファイルがアクセスされたか、修正されたときにスキャンする - 圧縮ファイルの内部をスキャンする
電子メールスキャン	- Microsoft Outlook Auto-Protect - インターネット電子メール Auto-Protect (14.2 RU1 で削除) - Lotus Notes Auto-Protect (14.2 RU1 で削除)	【※No※】	【※No※】

ポリシー設定	Windows	Mac	Linux
スキャン対象	- 追加の場所 - メモリ - 選択したフォルダ - 選択した拡張子 - ストレージ移行場所 - 圧縮ファイル内のファイル - セキュリティリスク	- すべてのフォルダまたは選択したフォルダ - ハードディスクドライブとリムーバブルドライブ - 圧縮ファイル内のファイル	- すべてのファイル - すべてのフォルダまたは選択したフォルダ - 選択した拡張子 - 圧縮ファイル内のファイル - セキュリティリスク
ユーザー定義のスキャン (クライアント)	- アクティブスキャン - 完全スキャン - 個々のフォルダ、ファイル、拡張子のカスタムスキャン	- 完全スキャン - 個々のフォルダとファイルのカスタムスキャン	- 完全スキャン - 個々のフォルダとファイルのカスタムスキャン
検出の修復処理を定義する	- 消去 (マルウェアにのみ適用する) - 検疫 - 削除 - 放置する (ログのみ) この処理は、シマンテック社が定期的に更新するカテゴリのマルウェアとセキュリティリスクに適用されます。	- 感染ファイルを修復する - 修復できないファイルを検疫する	(14.3 MP1 以前) - 消去 (マルウェアにのみ適用する) - 検疫 - 削除 - 放置する (ログのみ)
スキャンの実行中に行う処理を設定する	- スキャンを停止する - スキャンを一時停止する - スキャンを休止する - コンピュータがアイドル状態のときだけスキャンする	(12.1.4) - スキャンを停止する - スキャンを一時停止する - 開始前にスキャンを休止する - 進行中のスキャンを休止する (12.1.6x のみ) - コンピュータがアイドル状態のときだけスキャンする	【※No※】
ダウンロードインサイト	はい	【※No※】	【※No※】
脅威検出のインサイト ルックアップ	はい	【※No※】	【※No※】
Bloodhound	はい	【※No※】	【※No※】
SONAR	はい リモートコンピュータのスキャン (14) 疑わしい動作の検出 (14)	【※No※】	【※No※】
早期起動マルウェア対策 ドライバ	Windows 8 以降、Windows Server 2012 以降	【※No※】	【※No※】
Power Eraser	はい (12.1.5)	【※No※】	【※No※】
エンドポイントの検出と レスポンスの有効化	はい (12.1.6)	【※No※】	【※No※】
Shared Insight Cache	はい vShield 対応 (12.1.6 以降)	【※No※】	【※No※】
仮想イメージの例外	はい	【※No※】	【※No※】

クライアントコンピュータに対するウイルスとスパイウェアの攻撃の防止と処理

Symantec Endpoint Protection の仮想インフラストラクチャでの使用

プラットフォームに基づくファイアウォール、侵入防止、メモリエクスプロイト緩和機能の設定

Table 197: プラットフォームに基づく侵入防止ポリシーの設定

ポリシー設定	Windows	Mac (12.1.4)
侵入防止シグネチャの例外	はい Note: カスタム例外はブラウザ保護シグネチャではサポートされません。	はい
ユーザー通知の表示/非表示	はい	はい
除外ホストの有効と無効を切り替える	はい	はい
カスタム IPS シグネチャ	はい	【※No※】
ネットワーク侵入防止の有効と無効を切り替える	はい	はい
LiveUpdate が IPS コンテンツを更新する	はい	はい
管理サーバーが IPS コンテンツを更新する	はい	いいえ **
クライアントパッケージは IPS を含みます	はい	はい
ネットワーク侵入防止	はい	はい
ブラウザの侵入防止	はい • ログのみのモード (12.1.6)	【※No※】
除外ホスト (ネットワーク侵入防止)	はい	はい

** LiveUpdate コンテンツのリバースプロキシとして つの Symantec Endpoint Protection Manager とともにインストールする Apache Web サーバーを設定できます。次のサイトを参照してください。

Mac および Linux クライアントがリバースプロキシとして Apache Web サーバーを使用して、LiveUpdate 内容をダウンロードすることを有効にすること

侵入防止の管理

Table 198: プラットフォームに基づくメモリエクスプロイト緩和機能ポリシーの設定

ポリシー設定	Windows	Mac (12.1.4)
メモリエクスプロイト緩和機能 汎用エクスプロイト緩和機能 (14 MPx)	はい (14) • 誤検知の微調整 (14.0.1) • カスタムアプリケーション (14.1、クラウドのみ)	【※No※】

メモリエクスプロイト緩和機能ポリシーを使用した、メモリ改ざんの試みに対する Windows クライアントの強化
プラットフォームに基づく LiveUpdate ポリシー設定

Table 199: プラットフォームに基づく LiveUpdate ポリシー設定

ポリシー設定	Windows	Mac	Linux
デフォルト管理サーバーを使う	はい	いいえ **	いいえ **
LiveUpdate サーバーを使う (内部または外部)	はい	はい	はい
GUP (Group Update Provider) を使います	はい	【※No※】	【※No※】
サードパーティコンテンツ管理を有効にする	はい	【※No※】	【※No※】
定義の有効化/無効化	はい	はい	【※No※】
縮小サイズの定義 (12.1.6)	はい	【※No※】	【※No※】
Intelligent Updater を実行して内容を更新	- ウイルス定義とスパイウェア定義 - SONAR (12.1.3 以降) - IPS 定義 (12.1.3 以降)	ウイルス定義とスパイウェア定義	ウイルス定義とスパイウェア定義
LiveUpdate プロキシの設定	はい	ただし、LiveUpdate のポリシーで設定されません。この設定を行うには、[クライアント] > [ポリシー] > [外部通信の設定] の順に選択します。	はい
LiveUpdate のスケジュール設定	- 頻度 - 再試行時間帯 - ダウンロードランダム化 - コンピュータがアイドル状態のときに実行 - LiveUpdate をスキップするオプション	- 頻度 - ダウンロードランダム化	- 頻度 - 再試行時間帯 - ダウンロードランダム化
標準 HTTP ヘッダーを使用 (12.1.6 以前)	デフォルトで可能	デフォルトで可能	デフォルトで可能
クライアントのセキュリティパッチ	はい (14)	【※No※】	【※No※】
アプリケーション制御のコンテンツ	サポート対象 (14.2)	【※No※】	【※No※】

** LiveUpdate コンテンツのリバースプロキシとして 2 つの Symantec Endpoint Protection Manager とともにインストールする Apache Web サーバーを設定できます。次のサイトを参照してください。

[Mac および Linux クライアントがリバースプロキシとして Apache Web サーバーを使用して、LiveUpdate 内容をダウンロードすることを有効にすること](#)

[クライアントのインストールの種類を選択する方法](#)

[クライアント上のコンテンツと定義を更新する方法](#)

[Intelligent Updater ファイルを使用した Symantec Endpoint Protection クライアントのコンテンツの更新](#)

プラットフォームに基づく **Web** とクラウドのアクセス保護 ポリシー設定

統合ポリシーは、バージョン 14.0.1 MP1 以降で利用できます。統合ポリシーは、14.3 RU1 で Network Traffic Redirection ポリシーに、14.3 RU2 で Web とクラウドのアクセス保護 に名前が変更されました。

ポリシー設定	Windows	Mac	Linux
PAC ファイル方式 • ローカルプロキシサービス	はい	はい • 14.2 RU2 以降でサポートされています。	いいえ
トンネル方式 (14.3 RU1)	はい、64 ビット版 Windows 10 のみ	いいえ	

Web とクラウドのアクセス保護 の設定

プラットフォームに基づくポリシー設定

Table 200: プラットフォームに基づくポリシー設定

ポリシー設定	Windows	Mac	Linux
サーバーベースの例外	- アプリケーション - 監視するアプリケーション - 拡張子 - ファイル - フォルダ - 既知のリスク - 信頼できる Web ドメイン - 改変対策例外 - DNS またはホストファイルの変更例外 - 証明書 (14.0.1)	ファイルまたはフォルダのセキュリティリスクの例外	- フォルダ - 拡張子
クライアントの制限 (エンドユーザーがクライアントコンピュータに追加できる制限事項を制御)	はい	【※No※】	【※No※】

Symantec Endpoint Protection の例外の管理

プラットフォーム別 **Device Control** の差異

アプリケーション制御は Windows コンピュータのみで実行されます。

Table 201: プラットフォーム別 Device Control の差異

Windows	Mac
Device Control はクラス ID (GUID) とデバイス ID にのみ基づいて働きます。	Device Control はファイルシステムレベルで働きます。ボリュームレベルタスク (コマンドラインやディスクユーティリティを使って実行できるボリュームレベルタスクなど) は影響を受けません。
Device Control は、星印 (アスタリスク (*)) が付いたクラス ID やデバイス ID でワイルドカードの照合を実行します。	Device Control は、正規表現 (regexp) の照合を実行し、次の特定の操作に限定されます。 • . (ドット) • \ (バックスラッシュ) • [set], [^Set] (セット) • * (星印 (アスタリスク)) • + (プラス)
ハードウェアデバイスのリストには、デフォルトで多くの種類の共通デバイスが記載されています。	次の 5 種類のデバイスから選択できます。 • Thunderbolt • CD/DVD • USB • FireWire • SD カード ハードウェアデバイスのリストは使いません。
クラス ID またはデバイス ID 別のハードウェアデバイスのリストにカスタムデバイスを追加できます。	カスタムデバイスは追加できません。
遮断する (または遮断から除外する) デバイスは、ハードウェアデバイスのリストからのみ派生します。リストには、追加したカスタムデバイスとそれらのデフォルトの共通デバイスの種類が記載されています。	遮断する (または遮断から除外する) デバイスは、前述のデバイスの種類から選択します。製造元、モデル、シリアル番号は空白にすることも、正規表現 (regexp) のクエリーで定義することもできます。製造元、モデル、シリアル番号の範囲などが異なる似たようなデバイスの範囲を定義する場合に正規表現を使うことができます。
一度に複数の種類のデバイスを追加できます。	一度に追加できるデバイスの種類は 1 つのみです。
遮断、または遮断から除外する (遮断からの除外を許可する) 処理を実行します。	遮断、またはマウント権限で遮断から除外する (遮断からの除外を許可する) 処理を実行します。 次のマウント権限がサポートされます。 • 読み込み専用 • 読み込みと書き込み • 読み込みと実行 • 読み込み、書き込み、実行
デバイス制御のクライアント通知をカスタマイズできます。	デバイス制御のクライアント通知をカスタマイズできません。

デバイス制御の管理

Windows クライアント用の Symantec Endpoint Protection 機能の依存関係

一部のポリシー機能は、互いに Windows クライアントコンピュータで完全な保護を提供するように要求します。

WARNING

シマンテック社では、Insight ルックアップを無効にしないことを推奨しています。

Table 202: 保護機能の依存関係

機能	相互運用性に関するメモ
ダウンロード保護	ダウンロード保護は Auto-Protect の一部で、URL を追跡する機能を Symantec Endpoint Protection に付与します。URL 追跡はいくつかのポリシー機能のために必要です。 ダウンロード保護なしで Symantec Endpoint Protection をインストールすると、ダウンロードインサイトの機能は限定されたものになります。ブラウザの侵入防止と SONAR にはダウンロード保護が必要です。 [イン트라ネット Web サイトからダウンロードしたファイルを自動的に信頼する] オプションにもダウンロード保護が必要です。
ダウンロードインサイト	ダウンロードインサイトには次の依存関係があります。 - Auto-Protect の有効化が必要 自動保護を無効にしている場合、ダウンロードインサイトが有効になっていてもダウンロードインサイトは機能できません。 - Insight ルックアップの有効化が必要 シマンテック社では、インサイトルックアップオプションを有効のままにしておくことを推奨しています。このオプションを無効にすると、ダウンロードインサイトは完全に無効になります。 Note: 基本的なダウンロード保護がインストールされていない場合、クライアントのダウンロードインサイトはレベル 1 で動作します。ポリシーで設定したどのレベルも適用されません。また、ユーザーは感度を調整できません。 ダウンロードインサイトを無効にしても、[イン트라ネット Web サイトからダウンロードしたファイルを自動的に信頼する] オプションは引き続き機能します。 ダウンロードインサイトを無効にすると、ポータル検出も無効になります。これにより、自動保護スキャンと定時スキャンとオンデマンドスキャンはすべてのファイルをポータル以外のファイルとして評価し、シマンテック社が設定した感度レベルを使うことになります。 ダウンロードインサイト検出の管理
インサイトルックアップ (12.1.x クライアント) とクラウド保護	インサイトルックアップは、クラウドの Symantec Insight 評価データベースを使ってサポート対象のポータルからダウンロードしたファイルについて判断をします。 14 以降: - インサイトルックアップの機能は、標準クライアントと埋め込み/VDI クライアントで自動保護スキャン、定時スキャン、オンデマンドスキャンの一部として自動的に動作します。標準クライアントと埋め込み/VDI クライアントはクラウド対応コンテンツをサポートします。 12.1.x クライアントのスキャン設定でインサイトルックアップを有効または無効にすることができますが、インサイトルックアップに対して特定の感度レベルを設定することはできません。レガシーのインサイトルックアップは、ダウンロードインサイトポリシーで設定される感度レベルを使います。 Windows クライアントがクラウドから定義を受け取る方法 クラウドスキャンと 12.1.x インサイトルックアップには次の機能依存関係があります。 - Insight ルックアップが有効になっている必要があります。そうでない場合、クラウドスキャンとインサイトルックアップは機能できません。 - ファイルをポータルファイルとしてマーク付けできるように、ダウンロードインサイトを有効にする必要があります。 - ダウンロードインサイトが無効の場合、クラウドスキャンとインサイトルックアップは引き続き機能します。最も悪意のあるファイルのみを検出するシマンテック社が自動的に設定する感度レベルを使用します。 Note: (12.1.x クライアントのみ) クラウドルックアップは、クライアントコンピュータのフォルダまたはドライブを右クリックして実行するスキャンに適用されません。ただし、クラウドルックアップは、選択したポータルファイルを右クリックして実行するスキャンに適用されます。

機能	相互運用性に関するメモ
SONAR	SONAR には次の依存関係があります。 - ダウンロード保護がインストールされている必要があります。 - Auto-Protect が有効になっている必要があります。 Auto-Protect が無効な場合、SONAR はいくつの検出機能を使用できず、クライアントで誤動作しているかのように見受けられます。ただし、SONAR は Auto-Protect が無効な場合でもヒューリスティック脅威を検出できます。 - Insight ルックアップが有効になっている必要があります。 Insight ルックアップを使わない場合、SONAR は実行されますが検出を行うことができません。まれに、SONAR はインサイトルックアップを使わずに検出することができる場合があります。Symantec Endpoint Protection が特定のファイルに関する評価情報を以前にキャッシュに保存している場合、SONAR はキャッシュに保存された情報を使う場合があります。 SONAR の管理
ブラウザの侵入防止	ダウンロード保護がインストールされている必要があります。ダウンロードインサイトは有効と無効のどちらにもできます。
信頼できる Web ドメインの例外	例外は、ダウンロード保護がインストールされている場合にのみ適用されます。
カスタム IPS シグネチャ	ファイアウォールを使用します。 カスタム侵入防止シグネチャの管理
Power Eraser	インサイトルックアップを使用します。 Power Eraser は評価情報を使い、ファイルを検査します。Power Eraser にはデフォルトの評価感度設定があります。これは変更できません。オプションの [脅威検出のインサイトルックアップを許可する] を無効にした場合、Power Eraser は Symantec Insight からの評価情報を利用できません。インサイトなしでは、Power Eraser はわずかししか検出できず、検出した場合も誤認である可能性が高くなります。 Note: Power Eraser は つの Symantec Endpoint Protection Manager では設定できない独自の評価しきい値を使用します。Power Eraser はダウンロードインサイト設定を使用しません。 つの Symantec Endpoint Protection Manager コンソールから Power Eraser を実行する前に知るべきこと
メモリエクスプロイト緩和機能 (バージョン 14 では汎用エクスプロイト緩和機能)	侵入防止がインストールされている必要があります。侵入防止は有効と無効のどちらにもできます。

[クライアントにインストールするセキュリティ機能の選択](#)

Symantec Endpoint Protection に含まれるツール

この記事では、Symantec Endpoint Protection に含まれるツールとその使用方法について説明します。

[FileConnect のインストールファイルに含まれているツール](#)

[Symantec Endpoint Protection Manager と一緒にインストールされるツール](#)

インストールファイルに含まれているツール

次のツールとマニュアルは、 [Broadcom [ダウンロード管理](#)] ページからダウンロードする Symantec Endpoint Protection インストールファイルの \Tools フォルダにあります。

-
- [ApacheReverseProxy](#) (12.1.4 以降)
 - [CentralQ](#) (12.1.6 以前)
 - [CleanWipe](#)
 - [ContentDistributionMonitor](#) ([SEPMMonitor](#))
 - [ディセプション](#) (14.0.1)
 - [DeviceInfo](#) (14)、[DevViewer](#)
 - [統合](#) ([WebServicesDocumentation](#))
 - [IT Analytics](#)
 - [JAWS](#)
 - [LiveUpdate Administrator](#) (12.1.4 以前)
 - サポート外 > [MoveClient](#)
 - サポート外 > [Qextract](#)
 - サポート外 > [SEPprep](#) (12.1.6 以前)
 - [OfflineImageScanner](#) (12.1.6 以前)
 - [PushDeploymentWizard](#)
 - [SylinkDrop](#)
 - [SymDiag](#) ([SymHelp](#))
 - [仮想化](#)
 - [WebServicesDocumentation](#) ([統合](#))

[Symantec Endpoint Protection のすべてのバージョンの製品ガイド](#)

ApacheReverseProxy (12.1.4 以降)

このツールを使って、Symantec Endpoint Protection Manager で Apache Web サーバーを設定して、Mac クライアントと Linux クライアントが Web サーバーを介して LiveUpdate コンテンツをダウンロードできるようにします。新しいコンテンツが公開されるたびに、Apache Web サーバーが つの Symantec Endpoint Protection Manager と連動して、Mac と Linux クライアント用の LiveUpdate コンテンツをローカルにダウンロードしてキャッシュに保存します。

このツールは、クライアント数が少ないネットワークに適しています。

CentralQ (12.1.6 以前)

Symantec Endpoint Protection では、感染ファイルとそれらの関連する副作用が格納されたパッケージをローカル検疫から中央検疫に自動的に転送できます。中央検疫を使うと、より簡単に犯跡情報を収集できます。このツールを使うと、感染したコンピュータに直接にアクセスせずに、そのコンピュータからサンプルを取得できます。

次の場合に、Symantec Endpoint Protection 環境で検疫サーバーを使います。

- Symantec Endpoint Protection から疑わしい脅威サンプルを取得する。
- これらのサンプルをセキュリティレスポンスに自動的に提出する。
- 検疫サーバーにのみ提出された疑わしい脅威に固有のラピッドリリース定義をダウンロードする。これらの定義は、脅威の発生元である Symantec Endpoint Protection クライアントにプッシュされません。

[ラピッドリリースウイルス定義](#)

詳しくは、「[中央検疫サーバーを SEP と組み合わせて利用する方法について](#)」を参照してください。

CleanWipe

CleanWipe は Symantec Endpoint Protection 製品をアンインストールします。CleanWipe は、Windows のコントロールパネルなどその他のアンインストール方法が失敗した後の最終手段としてのみ使ってください。

[Symantec Endpoint Protection のアンインストール](#)

このツールは次の場所 (64 ビット) にあります。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

ContentDistributionMonitor (SEPMMonitor)

ContentDistributionMonitor ツールを使うと、お使いの環境で複数のグループ更新プロバイダ (GUP) を管理、監視できます。このツールは、GUP の健全性とコンテンツの配布状態をグラフィックで表示します。

12.1.6 以前では、ContentDistributionMonitor は SEPMMonitor と呼ばれていました。12.1.5 以前では、ContentDistributionMonitor は NoSupport フォルダ内にありました。

「[Symantec Endpoint Protection コンテンツ配布監視ツール](#)」を参照してください。

ディセプション (14.0.1)

「ディセプタ」を使用しているエンドポイントで、ディセプションを使用して敵対者の活動を検出します。このアプローチは、攻撃者がネットワークの基本的な防御をすでに突破し、環境で偵察を行っているということを根底で仮定しています。攻撃者は、ドメインコントローラやデータベースの資格情報のような重要な資産を見つけようとします。

DeviceInfo (14)、DevViewer

DeviceInfo (Mac 用、バージョン 14 現在) と DevViewer (Windows 用) を使って、特定のデバイスのデバイス製造元、モデルまたはシリアル番号を取得します。この情報をハードウェアデバイスリストに追加します。次にデバイス ID をデバイス制御ポリシーに追加して、クライアントコンピュータのデバイスを許可または遮断します。

[ハードウェアデバイスリストへのハードウェアデバイスの追加](#)

[Endpoint Protection におけるデバイスのブロックまたは許可](#)

統合 (WebServicesDocumentation)

バージョン 14 で、Integration フォルダの名前が `WebServicesDocumentation` に変更されました。

[ハードウェアデバイスリストへのハードウェアデバイスの追加](#)

IT Analytics

IT Analytics ソフトウェアは、カスタムレポートとカスタムクエリーの作成を可能にすることで、Symantec Endpoint Protection の組み込みレポートを拡張します。つの Symantec Endpoint Protection Manager データベースに含まれるデータに基づいた多次元分析とグラフィカルレポート作成機能を提供します。この機能により、データベースやサードパーティレポート作成ツールに関する高度な知識なしで、独自にデータを攻略できます。

JAWS

JAWS スクリーンリーダープログラムとスクリプトセットにより、Symantec Endpoint Protection のメニューとダイアログの閲覧が容易になります。JAWS は第 508 条の製品アクセシビリティに準拠する補助技術です。

LiveUpdate Administrator (12.1.4 以前)

Symantec LiveUpdate Administrator は Symantec Endpoint Protection と別途のスタンドアロン Web アプリケーションです。LiveUpdate Administrator は LiveUpdate 公開サーバーのコンテンツをミラー化し、そのコンテンツを内蔵 Web サーバーを介してシマンテック製品に内部的に提供します。

LiveUpdate Administrator は Symantec Endpoint Protection のオプションコンポーネントです。Symantec Endpoint Protection クライアントの更新には必要ありません。デフォルトで、つの Symantec Endpoint Protection Manager は LiveUpdate Administrator ではなく LiveUpdate 技術を使って、シマンテック社の LiveUpdate 公開サーバーからコンテンツを直接にダウンロードします。

LiveUpdate Administrator は一部の状況で使うことができます。たとえば、多数の非 Windows クライアントにコンテンツをダウンロードしたり、つの Symantec Endpoint Protection Manager がコンテンツをダウンロードできない場合にクライアントにコンテンツをダウンロードしなければならない場合があります。したがって、LiveUpdate Administrator サーバーをインストールしてから、コンテンツをダウンロードするように つの Symantec Endpoint Protection Manager を設定することができます。

[LiveUpdate Administrator を使う場合](#)

LiveUpdate Administrator とそのマニュアルをダウンロードするには、「[Download LiveUpdate Administrator \(LUA \)](#)」を参照してください。

LiveUpdate Administrator 2.3.x リリースノート

サポート外 > MoveClient

MoveClient は、クライアントのホスト名、ユーザー名、IP アドレス、またはオペレーティングシステムに基づいてつの Symantec Endpoint Protection Manager グループ間でクライアントを移動する Visual Basic スクリプトです。クライアントのユーザーモードとコンピュータモードを切り替えます。

Windows クライアントのユーザーモードとコンピュータモードの切り替え

サポート外 > Qextract

Qextract は、クライアントのローカル検疫からファイルを抽出して復元します。このツールが必要になるのは、クライアントで検疫されたファイルが誤認であるとわかった場合です。

サポート外 > SEPprep (12.1.6 以前)

SEPprep は、競合他社のウイルス対策製品を自動的にアンインストールするサポート対象外のツールです。ノートンから Symantec Endpoint Protection に移行する場合、SEPprep はシマンテック社の Norton ™ 製品もアンインストールします。

競合他社の製品をアンインストールするスクリプトに SEPprep をパッケージ化して、Symantec Endpoint Protection インストーラを自動的にかつサイレントに起動できます。

競合他社の製品をアンインストールするには、SEPprep ではなく、クライアント配備ウィザードを使います。ウィザードの [クライアントインストールの設定] タブで [既存のサードパーティのセキュリティソフトウェアを自動的にアンインストール] をクリックします。

既存のセキュリティソフトウェアをアンインストールするためのクライアントパッケージの設定

SEPprep を使用したサードパーティ製セキュリティソフトウェアのアンインストール

クライアント配備ウィザードでアンインストールされる製品のリストについては、以下を参照してください。

SEP 12.1 の他社製セキュリティソフトウェア削除のサポートについて

SEPprep はシマンテック製品をアンインストールしません。ただし、バージョン 14 以降では、CleanWipe がクライアント配備ウィザードに組み込まれて、Symantec Endpoint Protection クライアントを含むその他のシマンテック製品を削除できるようになりました。

OfflineImageScanner (12.1.6 以前)

このツールは、オフラインの VMware 仮想ディスク (.vmdk ファイル) をスキャンして、脅威を検出します。

Symantec Offline Image Scanner ツールについて

PushDeploymentWizard

プッシュ配備ウィザードを使って、Symantec Endpoint Protection クライアントインストールパッケージを対象コンピュータに配備します。プッシュ配備ウィザードは、つの Symantec Endpoint Protection Manager のクライアント配備ウィザードに相当します。通常、このウィザードはコンピュータまたはリモートコンピュータの小規模なグループに配備するときに使います。

詳しくは、「[Overview of the Push Deployment Wizard in Symantec Endpoint Protection](#)」を参照してください。

SEPICIntegrationComponent (12.1.5 以前)

SEPIC (Symantec Endpoint Integration Component) は、単一の Web ベース Symantec Management Console を使用して Symantec Endpoint Protection と他の Symantec Management Platform ソリューションを組み合わせます。SEPIC を使うとコンピュータのインベントリ処理、パッチの更新、ソフトウェアの配信、新しいコンピュータの配備を行うことがで

きます。また、システムとデータのバックアップと復元、DLP エージェントの管理、Symantec Endpoint Protection クライアントの管理を行うこともできます。

SylinkDrop

Sylink.xml ファイルには Windows クライアントまたは Mac クライアントと Symantec Endpoint Protection Manager 間の通信設定が含まれています。クライアントと 1 つの Symantec Endpoint Protection Manager との通信が切断された場合は、SylinkDrop ツールを使って、クライアントコンピュータの既存の Sylink.xml ファイルを新しい Sylink.xml ファイルで置き換えます。

Sylink.xml ファイルの置換では次のタスクが実行されます。

- 管理下クライアントに管理外クライアントを変換する
- 新しいドメインが管理サーバーにクライアントを移行するか、または移動する
- 管理サーバーで修正できないクライアントに対する通信の破損を復元する
- 1 つのサーバーから複製パートナーではない別のサーバーにクライアントを移動する
- 1 つのドメインから別のものにクライアントを移動する

このツールは Windows クライアント専用として使うこともできます。このツールは次の場所に配置されています (64 ビット版)。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

SylinkDrop ツールを使ったクライアントとサーバー間の通信設定の復元

SymDiag (SymHelp)

バージョン 14 で、SymHelp ツールの名前が Symantec Diagnostic (SymDiag) に変更されました。

SymDiag は、よくある問題を特定して、サポートが支援するトラブルシューティングのためのデータを収集し、他のお客様の自力での解決やサポートリソースへのリンクを提供するマルチ製品診断ツールです。SymDiag では、シマンテック製品や潜在的なマルウェアの発見に役立つ脅威分析スキャンのライセンスとメンテナンスの状態も提供します。

仮想化

この仮想ツールは、仮想デスクトップインフラストラクチャ (VDI) 環境にインストールされているクライアントのスキャンパフォーマンスを向上します。

- **SecurityVirtualAppliance (12.1.6 以前)**
シマンテック社のセキュリティ仮想アプライアンスには、VMware vShield インフラストラクチャで使う vShield 対応の共有インサイトキャッシュが含まれます。
[セキュリティ仮想アプライアンスのインストールに必要なタスク](#)
[Symantec Endpoint Protection のセキュリティ仮想アプライアンスのインストール](#)
- **SharedInsightCache**
共有インサイトキャッシュツールは、Symantec Endpoint Protection クライアントがクリーンであると判断したファイルをスキャンしないことによって、仮想化された環境のスキャンパフォーマンスを向上します。クライアントがファイルの脅威をスキャンし、それがクリーンであると判断すると、クライアントはファイルについての情報を共有インサイトキャッシュに提出します。
その後で別のクライアントが同じファイルのスキャンを試みたときは、そのクライアントが共有インサイトキャッシュに照会して、ファイルがクリーンかどうかを確認できます。ファイルがクリーンな場合、クライアントはその特定ファイルをスキャンしません。ファイルがクリーンでない場合、クライアントはファイルのウイルスをスキャンして、その結果を共有インサイトキャッシュに提出します。
共有インサイトキャッシュはクライアントとは独立して実行する Web サービスです。ただし、クライアントが共有インサイトキャッシュと通信できるように、Symantec Endpoint Protection を設定して共有インサイトキャッシュの場所を指定する必要があります。Shared Insight Cache は HTTP または HTTPS によってクライアントと通信します。クライアントの HTTP 接続は、スキャンが終了するまで維持されます。
[SEP 共有インサイトキャッシュのインストールと設定](#)
- 仮想イメージの例外

VDI 環境のパフォーマンスとセキュリティを向上するための一般的な手段では、必要に応じて基本イメージを使って仮想マシンセッションを構築します。シマンテック社の仮想イメージ例外ツールを使うと、Symantec Endpoint Protection クライアントで基本イメージファイルの脅威のスキャンをバイパスできるため、ディスク I/O のリソース負荷を軽減できます。さらに、VDI 環境の CPU スキャンプロセスのパフォーマンスも向上します。

[Symantec 仮想イメージ例外ツールについて](#)

WebServicesDocumentation (統合)

12.1.6 以前の場合、このツールは \Tools\Integration フォルダにあります。

Symantec Endpoint Protection には、リモート監視および管理 (RMM) アプリケーションのサポートを提供するため、Web サービスの形式で公開 API のセットが含まれています。これらの Web サービスはクライアントと管理サーバー上で機能を提供します。Symantec Endpoint Protection Web サービスに対するすべての呼び出しは OAuth を使って認証され、認証済みの Symantec Endpoint Protection 管理者のアクセスのみを許可します。開発者は、これらの API を使って、所属する会社のサードパーティネットワークセキュリティソリューションを Symantec Endpoint Protection 管理サーバーとクライアントと統合します。

リモート管理とリモート監視のサポートを提供します。リモート管理は、サードパーティのソリューションまたはカスタムコンソールに基本的なクライアントと管理サーバーの機能を統合できる、Web サービス形式の公開 API を使って提供されます。リモート監視は公式にサポートされているレジストリキーと Windows イベントログ記録を使って提供されます。

リモート管理用の **Web** サービスは次のタスクを実行できます。

- Windows イベントログへのライセンス状態の報告に加えて、Web サービス呼び出し別に管理サーバーのライセンス状態とコンテンツ状態を報告する。
- 更新、更新とスキャン、再起動などのコマンドをクライアントに送信する。
- クライアントに配布されるポリシーを管理する。ポリシーは別の管理サーバーからインポートしたり、別の管理サーバーのグループまたは場所に割り当てたりできます。

Symantec Endpoint Protection Manager と一緒にインストールされるツール

次のツールは つの Symantec Endpoint Protection Manager と一緒に次の場所にインストールされます。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

- [CleanWipe](#)
- [CollectLog](#)
- [データベース検証](#)
- [SetSQLServerTLSEncryption](#)
- [SylinkDrop](#)
- [つの Symantec Endpoint Protection Manager API リファレンス](#)

CollectLog

CollectLog.cmd は つの Symantec Endpoint Protection Manager ログを圧縮 .zip ファイルにアーカイブします。この .zip ファイルは、トラブルシューティングの目的でシマンテック社のサポートまたは別の管理者に送信します。

このツールは次の場所 (64 ビット) にあります。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

データベース検証

dbvalidator.bat を使って、つの Symantec Endpoint Protection Manager を実行するデータベースの問題に対するサポートの診断を支援します。

このツールは次の場所 (64 ビット) にあります。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

SetSQLServerTLSEncryption (14)

つの Symantec Endpoint Protection Manager は、デフォルトで暗号化されたチャネル上で Microsoft SQL Server と通信します。このツールを使うと、管理サーバーと Microsoft SQL Server 間の通信で TLS 暗号化を無効または有効にできます。バージョン 14 では、このツールは Microsoft SQL Server データベースを使うように設定した管理サーバーインストールで使うことができます。

このツールは、Symantec Endpoint Protection Manager と共に次の場所 (64 ビット) にインストールされます。C:\Program Files (x86)\Symantec\Symantec Endpoint Protection Manager\Tools

つの Symantec Endpoint Protection Manager API リファレンス (14)

つの Symantec Endpoint Protection Manager には、Endpoint Detection and Response (EDR) から つの Symantec Endpoint Protection Manager に接続して操作する一連の REST API が含まれています。つの Symantec Endpoint Protection Manager にアクセスできない場合は、これらの API を使います。マニュアルは次の場所にあります。

- つの Symantec Endpoint Protection Manager サーバー上の次のアドレス (URL 内の SEPM-IP は つの Symantec Endpoint Protection Manager サーバーの IP アドレスです)
https://SEPM-IP:8446/sepm/restapidocs.html
IP アドレスには IPv4 と IPv6 があります。IPv6 アドレスは次のように角カッコで囲む必要があります: http://[<SEPM-Server>]:<#####>
- [Symantec Endpoint Protection のすべてのバージョンの製品ガイド](#)

Symantec Endpoint Protection と Symantec Endpoint Security での Windows クライアントサービス smc のコマンド

smc (または smc.exe) コマンドラインインターフェースを使って Windows クライアントサービスを実行できます。smc コマンドは、クライアントをリモートで実行するスクリプトで使うことができます。たとえば、1 つのアプリケーションを複数のクライアントにインストールするためにクライアントを停止する必要があります。スクリプトを使って一度にすべてのクライアントを停止または再起動できます。

クライアントサービスは smc -start パラメータを除いてコマンドラインパラメータを使って実行する必要があります。コマンドラインパラメータは、大文字と小文字を区別しません。一部のパラメータでは、パスワードが必要になることがあります。クライアントは、UNC パスをサポートしません。

smc コマンドラインインターフェースを使って Windows コマンドを実行するには

1. クライアントコンピュータで、[開始] > [実行] をクリックし、cmd と入力します。
2. [コマンド プロンプト] ウィンドウで、以下のいずれかのタスクを実行します。

- パラメータでパスワードが必要ない場合は、以下を入力します。

```
smc -parameter
```

ここで、parameter はパラメータです。

- パラメータでパスワードが必要な場合は、以下を入力します。

- smc -p password -parameter

例: smc -p password-exportconfig c:\profile.xml

NOTE

コマンドの前に smc サービスのインストールパスを入力する必要があります。たとえば、Symantec Endpoint Protection がデフォルトの場所にインストールされている 64 ビット Windows システムでは、以下を入力します。

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe

Table 203: smc のパラメータ

パラメータ	説明	適用先
<code>smc -start *</code>	クライアントサービスを開始します。 0 または -1 が返されます。	すべてのサポート対象バージョン
<code>smc -stop *†</code>	クライアントサービスを停止し、メモリからアンロードします。 このコマンドがパスワードで保護されている場合、エンドユーザーが正しいパスワードを入力してから 1 分以内にクライアントが無効になります。 0 または -1 が返されます。	すべてのサポート対象バージョン
<code>smc -cloudmanaged path\to \Symantec_Agent_Setup.exe</code>	クラウド管理のデバイスを別のクラウドドメインまたはテナントに移動します。 クライアントコンピュータを 1 つの Symantec Endpoint Protection Manager 管理からクラウドコンソール管理に移動します。 移動先のクラウドドメインまたはテナントに、Symantec Agent Setup.exe インストールファイルが必要です。このファイルはクラウドコンソールからダウンロードします。 smc を使用したデバイスのテナントまたはドメインの変更	14.2 RU1 現在
<code>smc -enable -ntp</code> <code>smc -disable -ntp †</code>	Symantec Endpoint Protection ファイアウォールと侵入防止システムを有効/無効にします。	すべてのサポート対象バージョン 14.2 RU1 以降、 <code>-disable</code> ではパスワードが必要
<code>smc -enable -mem *</code> <code>smc -disable -mem *</code>	Symantec Endpoint Protection メモリエクスプロイト緩和機能システムを有効/無効にします。	バージョン 14 MP1 現在
バージョン 14: <code>smc -enable -gem *</code> バージョン 14: <code>smc -disable -gem *</code>	Symantec Endpoint Protection 汎用メモリエクスプロイト緩和機能システムを有効/無効にします。 この機能は、以降のバージョンではメモリエクスプロイト緩和機能と呼ばれます。	バージョン 14 のみ
<code>smc -dismissgui</code>	クライアントユーザーインターフェースを閉じます。 クライアントは引き続き動作し、クライアントコンピュータを保護します。 0 が返されます。	すべてのサポート対象バージョン
<code>smc -exportconfig *†</code>	クライアントの設定ファイルを .xml ファイルにエクスポートします。設定ファイルには、次の管理サーバー設定が含まれています。 - ポリシー - グループ - セキュリティの設定 - ユーザーインターフェースの設定 パス名とファイル名を指定する必要があります。たとえば、以下のコマンドを入力できます。 <code>smc -exportconfig C:\My Documents\MyCompanyprofile.xml</code> 0、-1、-5、-6 のいずれかが返されます。	すべてのサポート対象バージョン

パラメータ	説明	適用先
smc -exportlog	ログのコンテンツ全体を .txt ファイルにエクスポートします。ログをエクスポートするには、次の構文を使います。 <pre>smc -exportlog log_type 0 -1 output_file</pre> 前述の引数について説明します。 log_typeは次のとおりです。 • 0 = システムログ • 1 = セキュリティログ • 2 = トラフィックログ • 3 = パケットログ • 4 = 制御ログ たとえば、以下のような構文を入力できます。 <pre>smc -exportlog 2 0 -1 c:\temp\TrafficLog</pre> ここで、0 はファイルの先頭を意味し、-1 はファイルの末尾を意味します。 エクスポートできるのは、制御ログ、パケットログ、セキュリティログ、システムログ、トラフィックログのみです。 名前 output_fileは、エクスポート先のファイルに割り当てるパス名とファイル名です。 0、-2、-5 のいずれかが返されます。	すべてのサポート対象バージョン
smc -exportadvrule *†	クライアントのファイアウォールルールを .xml ファイルにエクスポートします。エクスポートされたルールは管理対象外クライアントまたはクライアント制御モードと混合モードの管理下クライアントにのみインポートできます。サーバー制御モードの管理下クライアントでは、これらのルールは無視されます。 パス名とファイル名を指定する必要があります。たとえば、以下のコマンドを入力できます。 <pre>smc -exportadvrule C:\myrules.xml</pre> 0、-1、-5、-6 のいずれかが返されます。 設定ファイルとファイアウォールルールをインポートするときには、次のルールが適用される点に注意してください。 • 設定ファイルまたはファイアウォールルールファイルは、マップしたネットワークドライブから直接インポートすることはできません。	すべてのサポート対象バージョン

パラメータ	説明	適用先
smc -importadvrule *†	ファイアウォールルールをクライアントにインポートします。インポートしたルールは、既存のルールを上書きします。次のルールをインポートできます。 • <code>smc -exportadvrule</code> を通じてエクスポートした .xml 形式のルール • クライアントユーザーインターフェースからエクスポートした .sar 形式のルール クライアントが管理対象外である場合、または管理下クライアントがクライアント制御モードあるいは混合モードである場合にのみ、ファイアウォールルールをインポートできます。サーバー制御モードの管理下クライアントでは、これらのルールは無視されます。 ファイアウォールルールをインポートするには、.xml または .sar ファイルをインポートします。たとえば、以下のコマンドを入力できます。 <pre>smc -importadvrule C:\myrules.xml</pre> ルールをインポートすると、システムログにエントリが追加されます。0、-1、-5、-6 のいずれかが返されます。 ルールを上書きするのではなく追加するには、クライアントユーザーインターフェース内から「ルールのインポート」を使用します。 ユーザーによるクライアントのユーザーインターフェースの変更を防止、許可 クライアント上でのファイアウォールルールのエクスポートまたはインポート	すべてのサポート対象バージョン
smc -importconfig *†	インポートされた設定ファイルでクライアントの現在の設定ファイルのコンテンツを置換し、クライアントのポリシーを更新します。設定ファイルのコンテンツをインポートするには、クライアントが実行中である必要があります。 パス名とファイル名を指定する必要があります。たとえば、以下のコマンドを入力できます。 <pre>smc -importconfig C:\My Documents\MyCompanyprofile.xml</pre> 0、3、-1、-5、-6 のいずれかが返されます。	すべてのサポート対象バージョン
smc -importsylink path \to\sylink.xml †	クライアント通信ファイル (symlink.xml) をインポートします。 -sepmmanaged と同等です。	すべてのサポート対象バージョン
smc -enable -wss smc -disable -wss	Web とクラウドのアクセス保護 を有効化または無効化します。	バージョン 14.0.1 MP1 現在
smc -p password †	パスワードを必要とするコマンドとともに使用され、password は必須パスワードです。次に例を示します。 <pre>smc -p password -importconfig</pre>	すべてのサポート対象バージョン
smc -report	クライアントで発生したクラッシュや論理エラーを含んでいるダンプファイル (.dmp) を作成します。ファイルは Symantec Technical Support に自動的に送信されます。エラーの診断でサポートを受けるには、テクニカルサポートに連絡します。 ダンプファイルは、次の場所にあります。 <pre><SEP_Install>\Data\LocalDumps</pre> ここで、SEP_Install はインストールフォルダです。デフォルトでは、このパスは C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\version] の順にクリックします。	バージョン 14 以降
smc -runhi	ホストインテグリティ検査を実行します。 0 が返されます。	すべてのサポート対象バージョン
smc -sepmmanaged	クライアント管理をクラウドコンソールから、以前管理していた つの Symantec Endpoint Protection Manager に戻します。	14.2 RU1 現在

パラメータ	説明	適用先
<code>smc -sepmmanaged path \to\sylink.xml</code>	クライアント管理を SyLink.xml ファイルで指定された つの Symantec Endpoint Protection Manager に更新します。 -importsylink と同等です。	14.2 RU1 現在
<code>smc -showgui</code>	クライアントユーザーインターフェースを表示します。 0 が返されます。	すべてのサポート対象バージョン
<code>smc -updateconfig</code>	クライアントとサーバーの通信を開始して、クライアントの設定ファイルが最新であることを確認します。 クライアントの設定ファイルが古い場合は、updateconfig は最新の設定ファイルをダウンロードして、これと既存の設定ファイル (serdef.dat) を置換します。 0 が返されます。	すべてのサポート対象バージョン
<code>smc -image</code>	Symantec Agent (Symantec Endpoint Protection クライアント) の登録を解除し、未登録の状態を維持します。 通常の登録解除との違いは、ハードウェアキーと永続化ハードウェアキー情報が削除される点です。	14.3 RU1 以降 (Symantec Endpoint Security のみ)
<code>smc -configure -customer-id <id> -domain-id <id> -customer-secret-key <cc #####> -server-address <##### URL></code>	デバイスを登録し、そのデバイスの既存のプロキシオプションを使用します。 すべての登録パラメータは必須です。	14.3 RU1 現在
<code>smc -configure -proxy-mode <###></code>	登録パラメータと共に使用され、クライアントが必要なプロキシ設定を使用して登録できるようにします。無効なプロキシオプションを修正するためにも使用できます。 有効なモードは、 system 、 manual 、 none です。 プロキシアドレスを指定すると、自動的に manual モードに切り替わります。 manual を指定しても、プロキシホストを指定しない場合、このモードは無視されます。 つの Symantec Endpoint Protection Manager で管理されているクライアントではサポートされません。 プロキシ設定の組み合わせ	14.3 RU1 現在
<code>smc -configure -proxy-address <##### IP></code>	プロキシホストまたはプロキシアドレスを手動で指定できます。 プロキシモードが manual に設定されている場合は必須です。	14.3 RU1 現在
<code>smc -configure -proxy-port <#####></code>	プロキシポートを手動で指定できます。 HTTP および HTTPS 接続の両方に同じポートが使用されます。 ポートが指定されていない場合、HTTP の場合は 80、HTTPS の場合は 443 に自動的に設定されます。	14.3 RU1 現在
<code>smc -configure -proxy-port-http <#####></code>	HTTP 接続のプロキシポートを手動で指定できます。 デフォルトの HTTP ポートまたは <code>smc -configure -proxy-port</code> で指定されたポートを上書きします。	14.3 RU1 現在
<code>smc -configure -proxy-port-https <#####></code>	HTTPS 接続のプロキシポートを手動で指定できます。 デフォルトの HTTPS ポートまたは <code>smc -configure -proxy-port</code> で指定されたポートを上書きします。	14.3 RU1 現在
<code>smc -configure -proxy-auth-mode basic</code>	有効な認証モードは basic 、 ntlm です。 デフォルトの認証モードは basic です。	14.3 RU1 現在
<code>smc.exe -configure -proxy-user-name <##></code>	プロキシユーザーを手動で指定できます。 ntlm の場合、ドメイン/ユーザーを指定する必要があります。	14.3 RU1 現在

パラメータ	説明	適用先
<code>smc -configure -proxy-password <#####></code>	プロキシパスワードを手動で指定できます。 最大長は NULL なしで 255 文字です。パスワードの大文字と小文字は区別されます。	14.3 RU1 現在
<code>smc -reset-state -configure -customer-id <epmp id> -domain-id <epmp id> -server-address <##### URL></code>	クライアントを登録解除し、新しいデバイスとして再登録します。 必須の -configure 登録オプションはすべて指定する必要があります。	14.3 RU1 現在
<code>smc -tags "<csv #####>"</code>	登録タグを手動で指定できます。 最大長は NULL なしで 1024 文字です。 登録パラメータと共に指定する必要があります。	14.3 RU1 現在

`smc -checkinstallation` と `smc -checkrunning` はサポートされなくなりました。

* 次の条件が満たされた場合に管理者グループのメンバーのみが使うことのできるパラメータ

- Windows /Vista または Windows Server 2008 が実行されているクライアントで、ユーザーが Windows Administrators グループのメンバーである場合
Windows Vista が実行されているクライアントで User Account Control が有効になっている場合は、ユーザーは自動的にグループ Administrators と Users のメンバーになります。

† パスワードが必要なパラメータ。つの Symantec Endpoint Protection Manager クライアントをパスワードで保護します。

Table 204: コマンドプロンプトで入力されるプロキシ設定の組み合わせ

プロキシ設定の組み合わせ					処理
proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	
system	no	no	no	no	システムプロキシの使用
system	yes	no	no	no	ERROR_INVALID_COMMAND_LINE (パスワードが指定されていません)
system	no	yes	no	no	ERROR_INVALID_COMMAND_LINE (ユーザーが指定されていません)
system	no	no	yes	no	システムプロキシの使用 (サーバーを無視)
system	yes	yes	no	no	認証にシステムプロキシを使用
system	yes	yes	yes	no	認証にシステムプロキシを使用 (サーバーを無視)
system	yes	yes	yes	yes	認証にシステムプロキシを使用 (サーバーおよびポートを無視)
manual	no	no	no	no	ERROR_INVALID_COMMAND_LINE
manual	yes	no	no	no	ERROR_INVALID_COMMAND_LINE
manual	no	yes	no	no	ERROR_INVALID_COMMAND_LINE
manual	no	no	yes	no	デフォルトポートで「manual」(カスタム) プロキシが有効
manual	yes	yes	no	no	ERROR_INVALID_COMMAND_LINE

プロキシ設定の組み合わせ					処理
proxy-mode	proxy-user-name	proxy-password	proxy-address	proxy-port	
manual	yes	yes	yes	no	デフォルトポートで「manual」(カスタム)プロキシが有効
manual	yes	yes	yes	yes	「manual」(カスタム)プロキシが有効
manual	yes	no	yes	yes または no	ERROR_INVALID_COMMAND_LINE (パスワードなし)
manual	no	yes	yes	yes または no	ERROR_INVALID_COMMAND_LINE (ユーザーなし)
なし	no	no	no	no	「none」プロキシが有効
なし	yes	no	no	no	「none」プロキシが有効
なし	no	yes	no	no	「none」プロキシが有効
なし	no	no	yes	no	「none」プロキシが有効
なし	yes	yes	no	no	「none」プロキシが有効
なし	yes	yes	yes	no	「none」プロキシが有効
なし	yes	yes	yes	yes	「none」プロキシが有効
no	no	no	no	no	プロキシ設定なし
no	yes	no	no	no	プロキシ設定なし (ユーザーを無視)
no	no	yes	no	no	プロキシ設定なし (パスワードを無視)
no	no	no	yes	no	デフォルトポートで「manual」(カスタム)プロキシが有効
no	yes	yes	no	no	プロキシ設定なし (追加オプションを無視)
no	yes	yes	yes	no	デフォルトポートで「manual」(カスタム)プロキシが有効
no	yes	yes	yes	yes	「manual」(カスタム)プロキシが有効

コマンドエラーコード

smc.exe コマンドエラーコード

「[コマンドエラーコード](#)」では、必須パラメータが無効であるか見つからない場合に `smc.exe` コマンドによって返されるエラーコードについて説明します。

Table 205: `smc.exe` コマンドエラーコード

エラーコード	説明
0	コマンドは正常に実行されました。
-1	ユーザーが Windows Administrators グループまたは Windows Power Users グループに属していません。Windows Vista が実行されているクライアントの場合は、ユーザーが Windows Administrators グループのメンバーではありません。
-2	無効なパラメータです。 パラメータを正しく入力しなかったか、またはパラメータの後に間違ったスイッチを追加した可能性があります。
-3	<code>smc</code> クライアントサービスがインストールされていません。

エラーコード	説明
-4	smc クライアントサービスが実行されていません。
-5	入力ファイルが無効です。 たとえば、importconfig、exportconfig、updateconfig、importadv、exportadvrule、exportlog の各パラメータでパス名とファイル名を正しく指定する必要がある場合があります。
-6	入力ファイルが存在しません。 たとえば、importconfig、updateconfig、importadvrule の各パラメータでパス名、設定ファイル名 (.xml)、ファイアウォールルールファイル名 (.sar) を正しく指定する必要がある場合があります。

Endpoint Protection クライアントサービスの Windows のコマンド

サードパーティツールを使った Windows クライアントソフトウェアのインストール

管理サーバーにインストールされているツール以外のサードパーティツールを使って、クライアントをインストールできます。大規模なネットワークがある場合は、シマンテック製クライアントソフトウェアをインストールするために、これらのオプションを使うことにより、大きいメリットが見込まれます。

さまざまな種類のサードパーティ製品を使って、クライアントをインストールできます。これらの製品には、Microsoft Active Directory、Tivoli、Microsoft Systems Management Server (SMS)、Novell ZENworks が含まれます。Symantec Endpoint Protection は Novell ZENworks、Microsoft Active Directory、Microsoft SMS をサポートします。

Symantec Software Management Solution powered by Altiris で管理する環境で、Symantec Endpoint Protection を配備することもできます。次のポリシーの 1 つを使って、Software Management Solution サイトの 1 つから Symantec Endpoint Protection を配備できます。

- 管理下ソフトウェア配布のポリシー
- クイック配信のポリシー

詳しくは、Software Management Solution サイトの製品のヘルプを参照するか、または次を参照してください。

[Symantec Software Management Solution の製品のランディングページ](#)

Table 206: クライアントをインストールするサードパーティツール

ツール	説明
Windows インストーラのコマンドラインツール	シマンテック製クライアントソフトウェアのインストールパッケージは Windows インストーラ (MSI) ファイルであり、標準の Windows インストーラオプションを使って設定できます。Active Directory や Tivoli など、MSI の配備をサポートする環境管理ツールを使って、ネットワークにクライアントをインストールできます。Windows セキュリティセンターと管理外クライアントが連携する方法を設定できます。 クライアントインストール機能とプロパティについて MSI コマンド文字列の設定について setaid.ini の設定について Symantec Endpoint Protection クライアントのコマンドライン機能 Symantec Endpoint Protection クライアントのコマンドラインインストールプロパティ Windows インストーラのパラメータ Windows クライアントをインストールする場合のコマンドラインの例 Windows セキュリティセンターのプロパティ
Microsoft SMS 2003	Microsoft SMS を使ってクライアントをインストールできます。 Microsoft SCCM/SMS を使った Windows クライアントのインストール

ツール	説明
Windows Active Directory	クライアントコンピュータが Windows Active Directory ドメインのメンバーの場合は、Windows Active Directory Group Policy Object を使うことができます。また、クライアントコンピュータは、サポートされる Windows オペレーティングシステムを使う必要があります。 Active Directory Group Policy Object (GPO) を使った Windows クライアントのインストール Active Directory Group Policy Object を使ったクライアントソフトウェアのアンインストール
仮想化ソフトウェア	仮想環境でクライアントをインストールできます。 サポート対象の仮想インストールと仮想化製品

クライアントインストールパッケージのエクスポート

クライアントインストール機能とプロパティについて

インストール機能とプロパティは、テキストファイルやコマンドラインに文字列として表示されます。テキストファイルとコマンドラインはすべてのクライアントソフトウェアのインストールの間に処理されます。インストール機能はどのコンポーネントをインストールするかを制御します。インストールプロパティはインストール後に有効または無効にするサブコンポーネントを制御します。インストール機能とプロパティは、Symantec Endpoint Protection ライアントソフトウェアのみで利用できます。また、Windows オペレーティングシステムでも利用できます。インストール機能とプロパティは つの Symantec Endpoint Protection Manager のインストールでは利用できません。

インストール機能とプロパティは、Setaid.ini ファイルの行と Windows インストーラ (MSI) コマンドの値の方法で指定します。MSI コマンドは、Windows インストーラの文字列とカスタム配備の Setaid.ini で指定できます。Windows インストーラコマンドと setaid.ini は、必ずすべての管理下クライアントソフトウェアのインストールで処理されます。異なる値が指定された場合、Setaid.ini の値が常に優先されます。

MSI コマンド文字列の設定について

Symantec Endpoint Protection インストールソフトウェアは Windows インストーラ (MSI) 3.1 以降のパッケージを使ってインストールと配備を行います。コマンドラインを使ってパッケージを配備する場合は、インストールをカスタマイズできます。Windows の標準インストーラパラメータおよび Symantec 固有の機能とプロパティを使うことができます。

Windows インストーラを使うには、システム特権が必要です。システム特権がないままインストールしようとすると、インストールは通知なく失敗します。

シマンテック製品のインストールコマンドとパラメータの最新リストについては、「[MSI command line reference for Symantec Endpoint Protection](#)」という記事を参照してください。

NOTE

Windows インストーラのアダプタイズ機能はサポートされていません。setaid.ini で指定されている機能やプロパティは、MSI で指定された機能やプロパティよりも優先されます。MSI コマンドの機能名とプロパティ名は大文字と小文字を区別します。

[setaid.ini の設定について](#)

setaid.ini の設定について

Setaid.ini はすべてのインストールパッケージに含まれ、どの機能がインストールされるかなどの、インストールに関するさまざまな側面を制御します。Setaid.ini は、インストールの開始に使われる MSI コマンド文字列に表示されるすべての設定よりも必ず優先されます。Setaid.ini は setup.exe と同じディレクトリ内にあります。単一の .exe ファイルにエクスポートする場合は、Setaid.ini を設定できません。ただし、コンソールから Symantec Endpoint Protection クライアントインストールファイルをエクスポートする場合は、このファイルが自動的に設定されます。

次の行は、setaid.ini で設定できるオプションをいくつか示しています。

```
[CUSTOM_SMC_CONFIG]
```

```
InstallationLogDir=  
DestinationDirectory=  
[FEATURE_SELECTION]  
Core=1  
  
SAVMain=1  
Download=1  
OutlookSnapin=1  
Pop3Smtplib=0  
NotesSnapin=0  
  
PTPMain=1  
DCMain=1  
TruScan=1
```

NOTE

機能は階層を示すためにインデントされています。setaid.ini ファイル内ではインデントされません。setaid.ini の機能名は大文字と小文字を区別します。

値が 1 に設定されている機能はインストールされます。値が 0 に設定されている機能はインストールされません。クライアント機能を正しくインストールするには、親機能を指定してインストールする必要があります。

また、Symantec **Endpoint Protection** クライアントインストールで **MSI** プロパティにマップされる、以下の **setaid.ini** の設定についても注意してください。

- PRODUCTINSTALLDIR にマップされる DestinationDirectory
- MIGRATESETTINGS にマップされる KeepPreviousSetting
- ADDSTARTMENUICON にマップされる AddProgramIntoStartMenu

[Symantec Endpoint Protection クライアントのコマンドライン機能](#)

[Symantec Endpoint Protection クライアントのコマンドラインインストールプロパティ](#)

[Windows インストーラのパラメータ](#)

Symantec Endpoint Protection クライアントのコマンドラインインストールプロパティ

これらのインストールプロパティは、MSI コマンドラインインストールで使用します。

Table 207: Symantec Endpoint Protection クライアントのインストールプロパティ

プロパティ	説明
RUNLIVEUPDATE=val	LiveUpdate をインストールの一部として実行するかどうかを決定します。ここで、val は次のいずれかの値です。 1: インストール中に LiveUpdate を実行します (デフォルト)。 0: インストール中に LiveUpdate を実行しません。 デフォルトでは、グループのすべての Symantec Endpoint Protection クライアントはすべてのコンテンツとすべての製品の更新の最新版を受け取ります。管理サーバーから更新を取得するように設定したクライアントは、サーバーがダウンロードした更新だけを受け取ります。LiveUpdate Content policy ですべての更新の受け取りが許可されていても、管理サーバーがすべての更新をダウンロードしない場合には、クライアントはサーバーがダウンロードする更新のみを受け取ります。
ENABLEAUTOPROTECT=val	インストールの完了後に、ファイルシステム Auto-Protect を有効にするかどうかを決定します。ここで、val は次のいずれかの値です。 1: インストール後に Auto-Protect を有効にします (デフォルト)。 0: インストール後に Auto-Protect を無効にします。
CACHE_INSTALLER=val	インストールファイルをクライアントのキャッシュに保存するかどうかを決めます。val は次のいずれかの値です。 1: インストールファイルをキャッシュに保存する (デフォルト)。 0: インストールファイルをキャッシュに保存しない。
MIGRATESETTINGS=val	アップグレードシナリオに設定を保存する状態を決めます。val は次のいずれかの値です。 0: 設定やログを保存しない。 1: すべての設定とログを保存する。 2: Sylink.xml とログのみを保存する。
ADDSTARTMENUICON=val	スタートメニューのフォルダにプログラムを追加するかどうかを決めます。val は次のいずれかの値です。 0: スタートメニューのフォルダにプログラムを追加しない。 1: スタートメニューのフォルダにプログラムを追加する (デフォルト)。

コマンドラインを使った Symantec Endpoint Protection クライアント機能のインストール

保護機能を Setaid.ini ファイルと MSI コマンドで指定してインストールできます。ほとんどの機能には親子の関係があります。親機能を持つ子機能をインストールしたい場合は、親機能もインストールする必要があります。たとえば、ファイアウォール機能のインストールを指定して NTPMain のインストールを指定しない場合、ファイアウォールはインストールされません。

Table 208: Symantec Endpoint Protection クライアントの機能

機能	説明	必要な親機能
Core	クライアントと つの Symantec Endpoint Protection Manager 間の通信に使うファイルをインストールします。この機能は必須です。	なし
ADDefense	Endpoint Threat Defense for Active Directory コンポーネントをインストールします。	Core
DCMain	アプリケーション制御とデバイス制御機能をインストールします。	PTPMain

機能	説明	必要な親機能
ダウンロード	ダウンロードされるファイルに対する完全な保護をインストールします。ダウンロードインサイトによる完全に機能する評価スキャンが含まれます。	SAVMain
ファイアウォール	ファイアウォール機能をインストールします。	NTPMain
ITPMain	ネットワークの侵入防止とブラウザ侵入防止の機能をインストールします。	NTPMain
LANG1033	英語のリソースをインストールします。	Core
NotesSnapin	Lotus Notes Auto-Protect 電子メール機能をインストールします。 14.2 RU1 より前のバージョンにのみ適用されます。	SAVMain
NTPMain	ネットワークとホスト悪用防止コンポーネントをインストールします。	Core
NTR	ネットワークトラフィックリダイレクトのコンポーネントをインストールします。	Core
OutlookSnapin	Microsoft Exchange Auto-Protect 電子メール機能をインストールします。	SAVMain
Pop3Smtpt	POP3 と SMTP のメールに対する保護をインストールします。32 ビットシステムでのみ利用可能です。 14.2 RU1 より前のバージョンにのみ適用されます。	SAVMain
PTPMain	プロアクティブ脅威防止コンポーネントをインストールします。	Core
SAVMain	ウイルス、スパイウェア、基本的なダウンロードの保護をインストールします。サブ機能で追加の保護がインストールされます。	Core
TruScan	動作分析 (SONAR) 機能をインストールします。	PTPMain

Windows インストーラのパラメータ

Symantec Endpoint Protection クライアントインストールパッケージは、標準の Windows インストーラパラメータに加え、コマンドラインによるインストールや配備では拡張セットも使います。

標準の Windows インストーラパラメータの使い方の詳細については、Windows インストーラのマニュアルを参照してください。また、コマンドラインから msixec.exe を実行すれば、すべてのパラメータの一覧を表示できます。

Table 209: Windows インストーラのパラメータ

パラメータ	説明
Sep.msi (32 ビット) Sep64.msi (64 ビット)	Symantec Endpoint Protection クライアントのインストールファイル。ファイル名にスペースが含まれている場合に /I や /x で使うにはファイル名を引用符で囲みます。 必要なディスク容量
Msiexec	Windows インストーラの実行可能ファイル。 必要なディスク容量
/I ".msi file name"	指定したファイルをインストールします。ファイル名にスペースが含まれている場合は、ファイル名を引用符で囲みます。ファイルが Msiexec を実行するディレクトリと同じディレクトリにない場合はパス名を指定します。パス名にスペースが含まれている場合は、パス名を引用符で囲みます。たとえば、msiexec.exe /I "C:\path to\Sep.msi" のようにします。 必要なディスク容量

パラメータ	説明
/qn	サイレントでインストールします。 Note: サイレント配備を使う場合には、Symantec Endpoint Protection にプラグインする Microsoft Outlook などのアプリケーションをインストール後に再起動する必要があります。
/x ".msi file name"	指定したコンポーネントをアンインストールします。 省略可能
/qb	インストールの進捗状況を示す基本のユーザーインターフェースでインストールします。 省略可能
/!v logfilename	詳細なログファイルを作成します。logfilenameは、作成するログファイルの名前です。 省略可能
PRODUCTINSTALLDIR=path	対象コンピュータのカスタムパスを指定します。ここで、pathは指定された対象ディレクトリです。パスにスペースが含まれる場合は、パスを引用符で囲んでください。 Note: 32 ビットコンピュータのデフォルトのディレクトリは、C:\Program Files\Symantec\Symantec Endpoint Protection です。64 ビットコンピュータのデフォルトのディレクトリは、C:\Program Files (x86)\Symantec\Symantec Endpoint Protection です。 省略可能
SYMREBOOT=value	インストール後のコンピュータの再起動を制御します。ここで、valueは有効な引数です。有効な引数は次のとおりです。 • Force: コンピュータを再起動する必要があります。アンインストールの場合も必要です。 • Suppress: ほとんどの再起動を実行しません。 • ReallySuppress: インストールプロセスのすべての再起動を実行しません。サイレントインストールの場合も実行しません。 省略可能 Note: Symantec Endpoint Protection クライアントのアンインストールをサイレントで実行する場合に再起動を抑制するには、ReallySuppress を使います。
ADDLOCAL= feature	インストールするカスタム機能を選択します。ここで、featureは指定されたコンポーネントまたはコンポーネントのリストです。このプロパティを使用しない場合、適用できるすべての機能がデフォルトでインストールされます。また、Auto-Protect 電子メールクライアントは電子メールプログラムが検出された場合のみインストールされます。クライアントインストールに適切なすべての機能を追加するには、ADDLOCAL=ALL のように ALL コマンドを使います。 Symantec Endpoint Protection クライアントのコマンドライン機能 Note: インストールする新しい機能を指定するとき、インストール済みでそのまま使いたい機能はそれらの名前も含める必要があります。使用したい機能を指定しない場合、Windows インストーラはそれらを削除します。既存の機能を指定しても、インストール済みの機能が上書きされることはありません。既存の機能をアンインストールするには、REMOVE コマンドを使います。 省略可能
REMOVE=feature	以前にインストールしているプログラムやインストール済みのプログラムから特定の機能をアンインストールします。ここで、feature は次のいずれかです。 • 機能対象コンピュータから機能または一連の機能をアンインストールします。 • ALL: プログラムおよびインストール済みのすべての機能をアンインストールします。機能が指定されていない場合、ALL がデフォルトです。 省略可能

Windows セキュリティセンターのプロパティ

Windows セキュリティセンター (WSC) のプロパティは、Symantec Endpoint Protection クライアントのインストール時にカスタマイズできます。これらのプロパティは管理外のクライアントにのみ適用されます。つの Symantec Endpoint Protection Manager は、管理下クライアントではこれらのプロパティを制御します。

NOTE

これらのプロパティは Windows XP Service Pack 3 にのみ適用されます。WSCAVUPTODATE プロパティを除いて、Windows Vista または Windows 7 以降を実行するクライアントには適用されません。

Windows セキュリティセンターは、Windows 7/8 では「アクション センター」に、Windows 10 では「セキュリティとメンテナンス」に名前が変更されました。

Table 210: Windows セキュリティセンターのプロパティ

プロパティ	説明
WSCCONTROL=val	WSC を制御します。ここで、 val は次のいずれかの値です。 0: 制御しない (デフォルト) 1: 最初の検出時にいったん無効にする 2: 常に無効にする 3: 無効な場合に復元する
WSCAVALERT=val	WSC のウイルス対策警告を設定します。ここで、 val は次のいずれかの値です。 0: 有効にする 1: 無効にする (デフォルト) 2: 制御しない
WSCFWALERT=val	WSC のファイアウォール警告を設定します。ここで、 val は次のいずれかの値です。 0: 有効にする 1: 無効にする (デフォルト) 2: 制御しない
WSCAVUPTODATE=val	WSC にウイルス対策定義の期限を設定します。ここで、val は次のいずれかの値です。 1 から 90: 日数 (デフォルトは 30)
DISABLEDEFENDER=val	インストール中に Windows Defender を無効にするかどうかを判断します。ここで、 val は次のいずれかの値です。 1: Windows Defender を無効にする (デフォルト) 0: Windows Defender を無効にしない

Windows クライアントをインストールする場合のコマンドラインの例

Table 211: コマンドラインの例

タスク	コマンドライン
Symantec Endpoint Protection クライアントコンポーネントのすべてをデフォルト設定で C:\SFN ディレクトリにサイレントでインストールします。 コンピュータの再起動を抑止し、詳細なログファイルを作成します。	<code>msiexec /I SEP.msi PRODUCTINSTALLDIR=C:\SFN SYMREBOOT=ReallySuppress /qn /l*v c:\temp\msi.log</code>
ウイルス対策とスパイウェア対策、侵入防止とファイアウォールが有効な Symantec Endpoint Protection クライアントをサイレントでインストールします。 コンピュータを強制的に再起動し、詳細なログファイルを作成します。	<code>msiexec /I SEP.msi ADDLOCAL=Core,SAVMMain,OutlookSnapin, Pop3Smtplib,ITPMain,Firewall SYMREBOOT=Force /qn / l*v c:\temp\msi.log</code>

Microsoft SCCM/SMS を使った Windows クライアントのインストール

Microsoft System Center Configuration Manager (SCCM) を使ってシマンテック製クライアントソフトウェアをインストールできます。SCCM を使うシステム管理者は、これまでに SCCM を使ってソフトウェアをインストールしたことがあると想定されます。そのため、ここでは SCCM を使ったシマンテック製クライアントソフトウェアのインストールに関する詳しい説明は不要であると見なします。

NOTE

このトピックは、Microsoft Systems Management Server (SMS) にも適用されます。

NOTE

この注意は SMS バージョン 2.0 以前にも適用されます。SMS を使う場合、[SMS プログラムモニタ] でクライアントに対する [システムアクティビティすべてのステータスアイコンをタスクバー上に表示する] 機能をオフにします。状況によっては、[SMS プログラムモニタ] で使用中の共有ファイルを Setup.exe で更新する必要がある場合もあります。ファイルが使用中の場合は、インストールが失敗します。

SCCM/SMS パッケージでは、MSI を直接起動するのではなく、Setup.exe を起動することをお勧めします。この方法ではインストーラのログ記録が有効になります。パッケージウィザード機能の代わりに、SCCM/SMS のカスタムパッケージ作成機能を使用して、カスタムパッケージを作成します。

WARNING

つの Symantec Endpoint Protection Manager からエクスポートした管理下クライアントインストールパッケージを使います。製品ダウンロードまたはインストールファイルのクライアントインストールパッケージを使う場合は、管理外クライアントを配備することになります。管理外クライアントは、デフォルト設定でインストールされ、管理サーバーとの通信を行いません。

[パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール](#)

Table 212: Microsoft System Center Configuration Manager/Systems Management Server を使ったクライアントのインストールの処理

手順	説明
1	クライアントコンピュータにインストールするソフトウェアとポリシーが含まれる つの Symantec Endpoint Protection Manager から管理下クライアントインストールパッケージをエクスポートする。デフォルトにより、管理下クライアントインストールパッケージには、クライアントを管理するサーバーを識別する Sylink.xml という名前のファイルが含まれます。
2	ソースディレクトリを作成し、シマンテック製クライアントインストールパッケージをこのソースディレクトリにコピーする。たとえば、ソースディレクトリを作成し、つの Symantec Endpoint Protection Manager からエクスポートした Setup.exe ファイルをそこにコピーします。
手順 3	SCCM/SMS で、パッケージを作成し、パッケージに名前を付け、ソースディレクトリをこのパッケージの一部として識別する。
手順 4	パッケージのプログラムのダイアログボックスで、インストールプロセスを開始する実行可能ファイルを指定し、状況に応じて MSI のパラメータを指定する。
手順 5	アドバタイズで特定のコレクションにソフトウェアを配布する。

SCCM/SMS の使用について詳しくは、お使いのバージョンに該当する Microsoft のマニュアルを参照してください。

Active Directory Group Policy Object (GPO) を使った Windows クライアントのインストール

Windows Active Directory Group Policy Object を使って Windows クライアントをインストールできます。手順では、このソフトウェアがインストールされ、Active Directory Group Policy Object を使ったクライアントソフトウェアのインストールに Windows Active Directory を使うことを前提にしています。

シマンテック製クライアントのインストールでは、標準の Windows インストーラ (MSI) ファイルを使います。その結果、MSI のプロパティを持つクライアントインストールをカスタマイズできます。

MSI コマンド文字列の設定について

配備する前に DNS サーバーが正しく設定されていることを確認してください。Active Directory では、コンピュータ通信を DNS サーバーに依存しているため、正しく設定されている必要があります。設定をテストするには、Windows Active Directory コンピュータに ping を実行し、次に逆方向に ping を実行する方法があります。完全修飾ドメイン名を使用してください。コンピュータ名のみを使用すると、新しい DNS ルックアップが呼び出されません。次の形式を使います。

ping computername] の順にクリックします。fullyqualifieddomainname.com

WARNING

つの Symantec Endpoint Protection Manager からエクスポートした管理下クライアントインストールパッケージを使います。製品ダウンロードまたはインストールファイルのクライアントインストールパッケージを使う場合は、管理外クライアントを配備することになります。管理外クライアントは、デフォルト設定でインストールされ、管理サーバーとの通信を行いません。

パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール

Table 213: Active Directory Group Policy Object を使ったクライアントソフトウェアのインストール手順

手順	処理
1	[個々のファイル (.MSI に必要)] オプションを使って管理下クライアントインストールパッケージをエクスポートします。 パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール
2	インストールファイルのフォルダのステージングを行います。たとえば、アクセスを許可するための正しい権限を設定している共有フォルダに管理下クライアントインストールパッケージをコピーします。
手順 3	GPO ソフトウェア配布の作成 実働配備の前に、少ない数のコンピュータで GPO によるインストールをテストすることも必要です。DNS を正しく設定しないと、GPO によるインストールが 1 時間以上かかる可能性があります。 GPO ソフトウェア配布の作成
手順 4	コンピュータの組織単位への追加 組織単位にコンピュータを追加してソフトウェアをインストールする

Active Directory Group Policy Object を使ったクライアントソフトウェアのアンインストール

組織単位にコンピュータを追加してソフトウェアをインストールする

GPO によって Symantec Endpoint Protection がインストールされる組織単位にコンピュータを追加できます。コンピュータを再起動すると、クライアントソフトウェアのインストールプロセスが開始します。ユーザーがコンピュータにログオンすると、クライアントソフトウェアのインストールプロセスが完了します。ただし、グループポリシーの更新は瞬時には終わらず、このポリシーが伝播するのに時間がかかる場合があります。次の処理には、ポリシーをオンデマンドで更新するためにクライアントコンピュータで実行できるコマンドがあります。

Active Directory Group Policy Object (GPO) を使った Windows クライアントのインストール

1. 組織単位にコンピュータを追加してソフトウェアをインストールするには、Windows のタスクバーで、[スタート] > [すべてのプログラム] > [管理ツール] > [Active Directory ユーザーとコンピュータ] をクリックします。
2. [Active Directory ユーザーとコンピュータ] ウィンドウのコンソールツリーで、GPO によるインストールのために選択した組織単位に追加する 1 つ以上のコンピュータを見つけます。
コンピュータは、初めに [コンピュータ] 組織単位に表示されます。
3. インストールのために選択または作成した組織単位にコンピュータをドラッグアンドドロップします。
4. [Active Directory ユーザーとコンピュータ] ウィンドウを閉じます。
5. クライアントコンピュータでオンデマンドで GPO を更新するには、クライアントコンピュータでコマンドプロンプトを開きます。
6. gpupdate と入力して **Enter** キーを押します。
完了すると、コマンドプロンプトウィンドウにポリシーの更新が正常に完了したことを伝えるメッセージが表示されます。エラーメッセージが表示された場合は、画面上の指示に従って詳細を確認してください。
7. コマンドプロンプトウィンドウを閉じます。

Sylink.xml ファイルをコピーして管理下インストールパッケージにする

つの Symantec Endpoint Protection Manager をインストールすると、各クライアントグループ用の Sylink.xml ファイルが作成されます。Symantec Endpoint Protection クライアントは、このファイルの内容を読み取って、どの管理サーバーがクライアントを管理するかを確認します。シマンテック社から入手したインストールファイルからクライアントをインストールする場合、管理外クライアントをインストールすることになります。ただし、インストール前にこのフォルダに Sylink.xml ファイルをコピーすると管理下クライアントをインストールできます。

NOTE

つの Symantec Endpoint Protection Manager コンソールでエクスポートしたパッケージは管理対象であり、Sylink.xml ファイルを含んでいます。Group Policy Object で配備できる新しい管理下パッケージをエクスポートするには、クライアント配備ウィザードを使います。メッセージが表示されたら [パッケージの保存] をクリックし、[個々のファイル (.MSI に必要)] にチェックマークを付けます。

パッケージの保存を使った Symantec Endpoint Protection クライアントのインストール

Sylink.xml ファイルを製品インストールファイルにコピーして管理下インストールパッケージにするには

1. 一つの Symantec Endpoint Protection Manager から正しいクライアントグループの Sylink.xml ファイルをエクスポートしてコンピュータにコピーします。

NOTE

Sylink.xml ファイルをエクスポートする前に、管理コンソールで新しいグループを少なくとも 1 つ作成してください。これを行わないとデフォルトのグループにクライアントが表示されます。

グループの追加

クライアントとサーバーの通信ファイル (Sylink.xml) の手動によるエクスポート

2. ダウンロードしたインストールファイルにあるインストールフォルダを、コンピュータ上の任意のフォルダにコピーします。フォルダ SEP は 32 ビットのクライアントを含み、フォルダ SEPx64 は 64 ビットのクライアントを含んでいます。

個別のファイルとして以前にエクスポートした管理外クライアントパッケージのインストールフォルダを使うこともできます。

-
3. Sylink.xml をインストールフォルダにコピーします。メッセージが表示されたら既存の Sylink.xml ファイルを置換します。

Active Directory Group Policy Object を使ったクライアントソフトウェアのアンインストール

Active Directory を使ってインストールしたクライアントソフトウェアをアンインストールできます。

Symantec Endpoint Protection for Windows クライアントのアンインストール

Active Directory Group Policy Object を使ってクライアントソフトウェアをアンインストールするには

1. Windows のスタートメニューで [すべてのプログラム]、[管理ツール]、[グループ ポリシーの管理] の順に選択します。
お使いの Windows のバージョンによってはスタートメニューで [すべてのプログラム] の代わりに [プログラム] を表示することがあります。
2. [グループポリシーの管理] ウィンドウのコンソールツリーでドメインを展開し、[コンピュータの構成]、[ソフトウェアの設定] の順に展開し、[ソフトウェアインストール] を右クリックしてから [プロパティ] をクリックします。
3. [詳細設定] タブで、[管理の対象でなくなったときは、このアプリケーションをアンインストールする] にチェックマークを付けてから [OK] をクリックします。
4. 右ペインで、ソフトウェアパッケージを右クリックしてから [削除] をクリックします。
5. [ソフトウェアの削除] ダイアログボックスで、[直ちに、ソフトウェアをユーザーとコンピュータからアンインストールする] にチェックマークを付けてから [OK] をクリックします。
6. [グループポリシーオブジェクトエディタ] ウィンドウを閉じてから、[グループポリシーの管理] ウィンドウを閉じます。

クライアントコンピュータを再起動すると、ソフトウェアがアンインストールされます。

著作権に関する声明

Broadcom、パルスロゴ、Connecting everything、および Symantec は、Broadcom の商標です。

「Broadcom」または「ブロードコム」という用語は、Broadcom Inc. またはその関連会社を示します。詳しくは、www.broadcom.com を参照してください。

Broadcom は、品質、機能、設計を改善するため、ここに記載された製品やデータを予告なく変更する権利を留保します。Broadcom は、提供する情報の正確さと信頼性に細心の注意を払っています。ただし、Broadcom はこの情報の適用または使用、もしくはここに記載された製品や回路の適用または使用から生じる一切の責任を負わないものとし、また特許権やその他の権利に対するライセンスを付与しません。

