

Cisco UCS C-シリーズ ソフトウェア、リリース 3.0(4) リリース ノート

初版 : 2018 年 3 月 21 日

最終更新 : 2020 年 6 月 4 日

Cisco UCS C-シリーズ ソフトウェア リリース ノート

Cisco UCS C シリーズ サーバ

Cisco UCS C シリーズサーバは、業界標準のラック筐体でユニファイドコンピューティングの機能を提供できるため、総所有コストの軽減と俊敏性の向上に役立ちます。このシリーズの各モデルは、処理、メモリ、I/O、内蔵ストレージリソースのバランスを取ることで、処理負荷にまつわるさまざまな課題に対応しています。

リリース ノートについて

このマニュアルでは、Cisco Integrated Management Controller ソフトウェアおよび関連する BIOS、ファームウェア、ドライバを含む C シリーズのソフトウェア リリース 3.0(4) の新機能、システム要件、未解決の問題、および既知の動作について説明します。このドキュメントは、[関連資料](#)の項に示されているマニュアルと併せてご利用ください。



(注) 元のドキュメントの発行後に、ドキュメントを更新することがあります。したがって、マニュアルのアップデートについては、Cisco.com で確認してください。

マニュアルの変更履歴

改定	日付	説明
M0	2020 年 6 月 4 日	次の点に変更されました。 • 「解決済みの問題告」の項を更新しました。 • 「既知の動作」セクションが更新されました。 • HUU のバージョンが 3.0(4q) に更新されました。個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C-シリーズ統合管理コントローラファームウェアファイル、リリース 3.0
L0	2020 年 4 月 20 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • 「未解決の問題」の項を更新。 • HUU のバージョンが 3.0(4p) に更新されました。個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C-シリーズ統合管理コントローラファームウェアファイル、リリース 3.0

改定	日付	説明
K0	2019 年 12 月 9 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • 「セキュリティ修正」の項を更新。 • HUU のバージョンが 3.0(4o) に更新されました。個々のリリースに対する Cisco ホスト アップグレードユーティリティのファームウェア ファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0
J0	2019 年 9 月 17 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • 「セキュリティ修正」の項を更新。 • HUU のバージョンが 3.0(4n) に更新されました。個々のリリースに対する Cisco ホスト アップグレードユーティリティのファームウェア ファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0

改定	日付	説明
I0	2019 年 8 月 13 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • HUU のバージョンが 3.0(4m) に更新されました。個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C-シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0
H0	2019 年 5 月 15 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • HUU のバージョンが 3.0(4l) に更新されました。個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C-シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0

改定	日付	説明
G0	2019 年 4 月 8 日	次の点に変更されました。 • このリリースでは、セキュリティ修正が適用されました。 • 「解決済みの問題」の項を更新。 • 「サポートされているソフトウェア機能」の項を更新しました。 • HUU のバージョンが 3.0(4k) に更新されました。個々のリリースに対する Cisco ホスト アップグレードユーティリティのファームウェア ファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0

改定	日付	説明
F0	2018 年 9 月 10 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • 「未解決の問題」の項を更新。 • バージョンが 4.0(1b)に変更されました。次のハードウェアのファームウェアが更新されました。 • Intel® SSD DC S4500 および DC S4600 シリーズ SATA • Micron 5100 SATA SSD (M.2 および U.2) • Intel® SSD DC P4500 および P4600 シリーズ NVMe 個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェア ファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0
E0	2018 年 8 月 29 日	リリース 3.0(4e) およびリリース 3.0(4i) のセキュリティ修正が更新されました。

改定	日付	説明
D0	2018 年 7 月 20 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • 「セキュリティ修正」の項を更新。 • HUU のバージョンが 3.0(4i) に更新されました。個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0
C0	2018 年 6 月 25 日	次の点に変更されました。 • 「解決済みの警告」の項を更新。 • 「セキュリティ修正」の項を更新。 • 「サポートされているソフトウェア機能」の項を更新しました。 • HUU のバージョンが 3.0(4e) に更新されました。個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0

改定	日付	説明
B0	2018年5月10日	次の点が変更されました。 • このリリースでは、製造上の問題に対処しました。 • 「サポートされているハードウェア」の項を更新しました。 • 「解決済みの問題」の項を更新しました。 • HUU のバージョンが 3.0(4d) に更新されました。個々のリリースに対する Cisco ホスト アップグレードユーティリティのファームウェア ファイルは、次から入手可能です。Cisco UCS C シリーズ 統合管理コントローラ ファームウェア ファイル、リリース 3.0
A0	2018年3月21日	リリース 3.0(4a) のリリースノートを作成しました。

サポートされているプラットフォームとリリース互換性マトリクス

このリリースでサポートされているプラットフォーム

このリリースでは、次のサーバがサポートされています。

- UCS-C22 M3
- UCS-C24 M3
- UCS-C220 M3
- UCS-C240 M3
- UCS-C3160 M3
- UCS-S3260 M3
- UCS-S3260 M4
- UCS-C220 M4

- UCS-C240 M4
- UCS-C460 M4

Cisco IMC および Cisco UCS Manager リリース互換性マトリクス

Cisco UCS C シリーズ ラックマウント サーバは、内蔵スタンドアロンソフトウェア (Cisco IMC) によって管理されます。しかし、C シリーズ ラックマウント サーバを Cisco UCS Manager と統合すると、Cisco IMC ではサーバを管理しません。

次の表には、C シリーズ ラックマウント サーバのサポートプラットフォーム、C シリーズ ソフトウェア スタンドアロンおよび Cisco UCS Manager リリースを示します。



(注) この表には、一部のマイナー リリースの UCS Manager および C シリーズ バージョンの互換性は含まれていません。主に、C シリーズ サーバがメジャー リリースの UCS Manager と最初に統合されたときの情報が含まれています。

表 1: CC シリーズ サーバ向けの Cisco C シリーズと UCS Manager Ss ソフトウェア リリース

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
3.0(4q)	サポートなし	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4p)	3.2(3o)	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4o)	サポートなし	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4n)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3
3.0(4m)	サポートしない	Cisco UCS C220 M4、C240 M4、C460 M4、S3260 M4、C22 M3、C24 M3、C220 M3、C240 M3、C3160 M3、S3260 M3

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
3.0(4l)	サポートしない	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(4k)	サポートしない	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(4j)	3.1(3k)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(4i)	3.1(3j)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(4e)	サポートなし	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(4d)	3.1(3h)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(4a)	3.1(3f)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
3.0(3a)	3.1(3a)	Cisco UCS C220 M4 および C240 M4
3.0(2b)	サポートなし (注) Cisco UCS Manager で検出とアップグ レードまたはダウ ングレード機能をサ ポートしています。	Cisco UCS C220 M4 および C240 M4

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
3.0(1d)	サポートなし (注) Cisco UCS Manager で検出とアップグ レードまたはダウ ングレード機能をサ ポートしています。	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C3160 M3、 S3260 M3
2.0(13e)	3.1(2b)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C3160 M3、 S3260 M3
2.0(10b)	3.1(1g)	Cisco UCS C220 M4 および C240 M4
2.0 (9c)	3.1(1e)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
2.0(9f)	2.2 (7b)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
2.0(10b)	2.2 (7b)	Cisco UCS C220 M4 および C240 M4
1.5(9d)	2.2 (7b)	Cisco UCS C420 M3、C260 M2、 および C460 M2
1.5(9d)	2.2(8f)	C420-M3、C260-M2、C460-M2 のみ
2.0 (9c)	2.2 (8f)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
2.0(10b)	2.2(8f)	Cisco UCS C220 M4 および C240 M4
2.0 (12b)	2.2(8f)	Cisco UCS C460 M4

C シリーズ スタンドアロン リリース	Cisco UCS Manager リリース	C シリーズ サーバ
1.5(8a)	2.2(6g)	Cisco UCS C420 M3、C260 M2、 および C460 M2
2.0 (8d)	2.2(6c)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
1.5(7f)	2.2(5b)	Cisco UCS C420 M3、C260 M2、 および C460 M2
2.0(6d)	2.2(5a)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
1.5(7a)2	2.2 (4b)	Cisco UCS C420 M3、C260 M2、 および C460 M2
2.0 (4c)	2.2 (4b)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3
1.5(7c)1	2.2 (3b)	Cisco UCS C420 M3、C260 M2、 および C460 M2
2.0 (3d) 1	2.2(3a)	Cisco UCS C220 M4、C240 M4、 C460 M4、S3260 M4、C22 M3、 C24 M3、C220 M3、C240 M3、 C3160 M3、S3260 M3

システム要件

管理クライアントは、次の最小システム要件を満たしているか、これを超過している必要があります。

- Sun JRE 1.8.0_92 以降 (1.8.0_121 まで)
- HTML ベースのインターフェイスは次でサポートされています。
 - Microsoft Internet Explorer 10.0 または 11
 - Mozilla Firefox 30 以降
 - Google Chrome 38 以降

- Safari 7 以降



(注) 管理クライアントがサポートされていないブラウザを使用して開始されている場合、サポートされているブラウザバージョンのログインウィンドウで入手可能な「サポートされたブラウザの最も良い結果のために」のオプションからのヘルプ情報を確認してください。

- クラシック表示の場合：すべてのブラウザで Adobe Flash Player 11 プラグイン以降が必要です。サポート対象のブラウザは次のとおりです。
 - Microsoft Internet Explorer 11 以降
 - Mozilla Firefox 54 以降
 - Google Chrome 61 以降
 - Safari 11 以降
- Microsoft Windows 7、Microsoft Windows XP、Microsoft Windows Vista、Microsoft Windows 10、Apple Mac OS X v10.6、Red Hat Enterprise Linux 5.0 またはそれ以上のオペレーティング システム
- Transport Layer Security (TLS) バージョン 1.2

ハードウェアおよびソフトウェアの相互運用性

ストレージ スイッチ、オペレーティング システム、アダプタに関する詳細については、以下の URL にあるお使いのリリースの『ハードウェアおよびソフトウェア相互運用性マトリクス』を参照してください。

http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html



(注) 接続は、サーバと最初に接続されたデバイス間でテストされます。スイッチの後のストレージ アレイなどのその他の接続は、Cisco UCS ハードウェア互換性リストには表示されませんが、これらのデバイスのベンダー サポート マトリクスでは強調表示される場合があります。

VIC カードでサポートされているトランシーバーとケーブルの詳細は、「[トランシーバー モジュールの互換性マトリクス](#)」を参照してください。

その他の互換性に関する情報については、VIC データ シートも参照できます。[Cisco UCS 仮想インターフェイス カード データ シート](#)

リリース 3.0 へのアップグレードパス

このセクションではリリース 3.0 へのアップグレードパスについて説明します。さまざまな Cisco UCS C シリーズ IMC バージョンのアップグレードパスの表を参照してください。

表 2: リリース 3.0 へのアップグレードパス

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
2.0(4c) よりも低いリリースの C460 M4 の場合	3.0	

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
		2.0(4c) よりも前のリリースから 3.0 にアップグレードするには、これらのステップに従ってください。 2.0(4c) より小さいものから 2.0(4c) バージョンへのアップグレード - サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 - 非インタラクティブ HUU (NIHHU) ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 - クライアント側で OpenSSL 1.0.0e-fips を使用します (NIHHU python スクリプトが実行中) ここ から HUU iso をダウンロードします。 ここ から NIHHU スクリプトをダウンロードします。 2.0(4c) から 3.0 へのアップグレード - サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 - 非インタラクティブ HUU (NIHHU) ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 - クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHHU python スクリプトが実行中) - Cimc Boot をセキュアにする場合、フラグ use_cimc_secure を python multiserver_config ファイルで yes にセットします。 ここ から HUU iso をダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
		• ここ から NIHUU スクリプトをダウンロードします。
2.0(4c) より後のリリースの C460 M4 の場合 2.0 からのその他のすべての M4 サーバ	3.0	以下のアップグレードパスに従ってください: • サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 • 非インタラクティブ HUU (NIHUU) ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 • クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中) • Cmc Boot をセキュアにする場合、フラグ use_cmc_secure を <code>python multiserver_config</code> ファイルで yes にセットします。 • ここ から HUU iso をダウンロードします。 • ここ から NIHUU スクリプトをダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
C220 M4 および C240 M4 で 2.0 からの場合	3.0(4a) および 3.0(4d)	以下のアップグレードパスに従ってください: • サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 • 非インタラクティブ HUU (NIHUU) ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 • クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中) • Cmc Boot をセキュアにする場合、フラグ use_cmc_secure を python multiserver_config ファイルで yes にセットします。 • Cisco IMC (BMC) ファームウェアは 2 回更新する必要があります。Cisco Intersight で使用するデバイスコネクタを有効にするには、この 2 つのファームウェア更新を実行する必要があります。 • インタラクティブな HUU は自動的に処理を行いますが、同じようにアクティベートするには、KVM を起動し、2 回目の更新後に [HUU を終了 (HUU EXIT)] を押す必要があります。つまり、HUU はまず CIMC を更新し、アクティベートし、その後 KVM が切断されます。2 番目の更新では、CIMC > KVM を再度起動 > HUU の終了を含む、コンポーネントのすべての更新が処理されます。 • ここ から HUU iso をダウンロードします。 • ここ から NIHUU スクリプトをダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
M3 サーバで、1.4 および 1.5(5) 以前のリリースから	3.0	

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
		更新前に、bmc を再起動します。 1.4 から 1.5 (4) へのアップグレード - インタラクティブ HUU を使用します。非インタラクティブ HUU (NIHUU) スクリプトはリリース 1.4 ではサポートされていません。 - Cisco.com から HUU iso をダウンロードします。 1.5(4) から 2.0(4c) へのアップグレード - サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 - 非インタラクティブ HUU (NIHUU) スクリプトを使用してファームウェアを更新する際には、バージョン 3.0(3a) でリリースされた Python スクリプトを使用します。 - クライアント側で OpenSSL 1.0.0e-fips を使用します (NIHUU python スクリプトが実行中) ここ から HUU iso をダウンロードします。 ここ から NIHUU スクリプトをダウンロードします。 2.0(4c) から 3.0 へのアップグレード - サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 - 非インタラクティブ HUU (NIHUU) ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 - クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中)

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
		• Cime Boot をセキュアにする場合、python スクリプトに付属する multiserver_config ファイルのフラグ use_cime_secure を yes にセットします。 • ここ から HUU iso をダウンロードします。 • ここ から NIHUU スクリプトをダウンロードします。

リリースからアップグレード	リリースにアップグレード	推奨されるアップグレードパス
1.5(4) より後のリリースのすべての M3 サーバの場合	3.0	1.5 から 2.0(4c) へのアップグレード - サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 - 非インタラクティブ HUU (NIHUU) スクリプトを使用してファームウェアを更新する際には、バージョン 3.0(3a) でリリースされた Python スクリプトを使用します。 - クライアント側で OpenSSL 1.0.0e-fips を使用します (NIHUU python スクリプトが実行中) ここ から HUU iso をダウンロードします。 ここ から NIHUU スクリプトをダウンロードします。 2.0(4c) から 3.0 へのアップグレード - サーバをアップグレードするには、インタラクティブ HUU または非インタラクティブ HUU (NIHHU) スクリプトを使用できます。 - 非インタラクティブ HUU (NIHUU) ツールを使用して、ファームウェアを更新する間、バージョン 3.0(3a) でリリースされる Python スクリプトを使用します。 - クライアント側で OpenSSL 1.0.1e-fips を使用します (NIHUU python スクリプトが実行中) - Cimc Boot をセキュアにする場合、python スクリプトに付属する multiserver_config ファイルのフラグ use_cimc_secure を yes にセットします。 ここ から HUU iso をダウンロードします。 ここ から NIHUU スクリプトをダウンロードします。

ファームウェア アップグレードの詳細

ファームウェア ファイル

C シリーズのソフトウェア リリース 3.0(4) には、次のソフトウェア ファイルが含まれます。

CCO ソフトウェア タイプ	ファイル名	備考
Unified Computing System (UCS) サーバ ファームウェア	ucs-s3260-huu-3.0.4.iso ucs-c3160-huu-3.0.4.iso ucs-c240m4-huu-3.0.4.iso ucs-c220m4-huu-3.0.4.iso ucs-c460m4-huu-3.0.4.iso ucs-c220-huu-3.0.4.iso ucs-c240-huu-3.0.4.iso ucs-c2x-huu-3.0.4.iso リリース特有の ISO バージョンについては、 Cisco UCS C シリーズ統合管理コントローラファームウェア ファイル、リリース 3.0 を参照してください。	ホスト アップグレードユーティリティ
Unified Computing System (UCS) ドライバ	ucs-cxxx-drivers.3.0.4.iso	ドライバ
Unified Computing System (UCS) ユーティリティ	ucs-cxxx-utils-efi.3.0.4.iso ucs-cxxx-utils-linux.3.0.4.iso ucs-cxxx-utils-vmware.3.0.4.iso ucs-cxxx-utils-windows.3.0.4.iso	ユーティリティ



- (注) 必ず BIOS、Cisco IMC および CMC を HUU ISO からアップグレードしてください。予期しない動作の原因となる場合があるため、コンポーネント（BIOS のみ、または Cisco IMC または CMC のみ）を個別にアップグレードしないでください。BIOS をアップグレードし、HUU ISO からではなく、Cisco IMC と CMC を個別にアップグレードすることを選択した場合は、Cisco IMC と BIOS の両方を同じコンテナリリースにアップグレードしてください。BIOS、CMC と Cisco IMC のバージョンが異なるコンテナリリースからのものである場合、予期しない動作が発生する可能性があります。Cisco IMC、BIOS、CMC、およびその他すべてのサーバコンポーネント（VIC、RAID コントローラ、PCI デバイス、および LOM）のファームウェアバージョンを更新するには、Host Upgrade Utility から [すべて更新 (Update All)] オプションを使用することを推奨します。

ホストアップグレードユーティリティ

Cisco Host Upgrade Utility (HUU) は、Cisco UCS C シリーズファームウェアをアップグレードするツールです。

ファームウェアのイメージファイルは、ISO に埋め込まれています。ユーティリティにメニューが表示され、これを使用してアップグレードするファームウェアコンポーネントを選択することができます。このユーティリティに関する詳細については、以下を参照してください。

http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

個々のリリースに対する Cisco ホストアップグレードユーティリティのファームウェアファイルは、[Cisco UCS C シリーズ統合管理コントローラ ファームウェア ファイル、リリース 3.1](#) を参照してください。

ファームウェアの更新

Host Upgrade Utility を使用して、C シリーズのファームウェアを更新します。Host Upgrade Utility は、次のソフトウェア コンポーネントをアップグレードできます。

- BIOS
- Cisco IMC
- CMC
- SIOC
- Cisco VIC アダプタ
- LSI アダプタ
- LAN On Motherboard の設定
- PCIe アダプタ ファームウェア
- HDD ファームウェア
- SAS エクспанダ ファームウェア

すべてのファームウェアは、サーバが正常に動作するようにまとめてアップグレードする必要があります。



- (注)
- Cisco IMC バージョン 3.0(x) から 2.0(x) にサーバをダウングレードすると、ローカル管理者パスワードが工場出荷時のデフォルトパスワードにリセットされます。ダウングレードが完了したら、手動でパスワードを以前に設定したものに変更する必要があります。
 - Cisco IMC、BIOS、およびその他のすべてのサーバコンポーネント (VIC、RAID コントローラ、PCI デバイス、および LOM) のファームウェアバージョンを更新するには、Host Upgrade Utility から **[すべて更新 (Update All)]** オプションを使用することをお勧めします。ファームウェアを導入したら、**[終了 (Exit)]** をクリックします。

ユーティリティを使用してファームウェアをアップグレードする方法の詳細については、次を参照してください。

<http://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-c-series-rack-servers/products-user-guide-list.html>

Supported Features

サポート対象ハードウェア

リリース 3.0(4d)

次の新しいハードウェアがリリース 3.0(4d) で追加されました。

- C3160 M3 および S3260 M3 サーバの Artesyn 1050W 電源装置のサポートが追加されました。
- Intel® SSD DC S4500 シリーズ 480GB (UCS SD480GBIS6-EV)
- Intel® SSD DC S4500 シリーズ 960GB (UCS SD960GBIS6-EV)
- Intel® SSD DC S4500 シリーズ 3.8 TB (CS-SD38TBIS6-EV)

サポート対象ソフトウェア機能

リリース 3.0(4k)

リリース 3.0(4k) では、次の新しいソフトウェア機能が追加されました。

- 証明書署名リクエスト (CSR) の生成の際の **チャレンジパスワード** を有効または無効にするオプション。

リリース 3.0(4a)

次の新しいソフトウェア機能がリリース 3.0(4a) でサポートされています。

- **デバイス コネクタ**: Cisco Intersight 管理を有効にすると、クラウドベースの管理プラットフォームと Cisco IMC 間の双方向通信が確立されます。この機能を使用すると、C220 M4、C240 M4、および C460 M4 システムを Cisco Intersight からモニタし、インベントリで管理することができます。これはオプトアウト機能です。Intersight 管理が必要ない場合は、オフにすることができます。



(注) 以前のバージョンから 3.0(4a) - 3.0(4d) バージョンにアップグレードする場合、Cisco Intersight で使用するデバイス コネクタを有効にするには、Cisco IMC (BMC) ファームウェアの二重アップデートを実行する必要があります。それ以外の場合にアクセスしようとする、ブランクの Intersight デバイス コネクタの画面が表示されることがあります。

重要: リリース 3.0(4e) では、Cisco Intersight デバイス コネクタにアクセスするためにはアップグレードを 2 回実行する必要があるという問題が解決されています。1 つのアップデートを使用すると、Cisco Intersight 機能にアクセスできるようになります。

ソフトウェア ユーティリティ

次の標準ユーティリティを使用できます。

- Host Update Utility (HUU)
- BIOS および Cisco IMC ファームウェアのアップデート ユーティリティ
- サーバ設定ユーティリティ (SCU)
- サーバ診断ユーティリティ (SDU)

ユーティリティ機能は次のとおりです。

- USB 上の HUU、SCU のブート可能なイメージとしての可用性。USB にはドライバ ISO も含まれており、ホストのオペレーティングシステムからアクセスできます。

SNMP

このリリース以降のリリースでサポートされている MIB 定義については、次のリンクを参照してください。

<ftp://ftp.cisco.com/pub/mibs/supportlists/ucs/ucs-C-supportlist.html>



(注) 上記のリンクは、IE 9.0 と互換性がありません。

セキュリティ修正

リリース 3.0(4o) のセキュリティ修正

リリース 3.0(4o) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
3.0(4o)	CSCvr54416	• CVE-2019-0151 • CVE-2019-11137	

リリース	不具合 ID	CVE	症状
			Intel® プロセッサに基づく Cisco UCS C シリーズおよび S シリーズ M4 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。 • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) は、特定の Intel® 第 4 世代 Intel® Core™ プロセッサ、第 5 世代 Intel® Core™ プロセッサ、第 6 世代 Intel® Core プロセッサ、第 7 世代 Intel® Core™ プロセッサ、第 8 世代 Intel® コア™ プロセッサ、Intel® Xeon® プロセッサ E3 v2/v3/v4/v5/v6 ファミリー、Intel® Xeon® プロセッサ E5 v3/v4 ファミリー、Intel® Xeon® プロセッサ E7 v3/v4 ファミリー、Intel® Xeon® スケーラブル プロセッサ 第 2 世代、Intel® Xeon® スケーラブル プロセッサ、Intel® Xeon® プロセッサ D-1500/D-2100)、Intel® Xeon® プロセッサ E-2100/E3100、および Intel® Xeon® プロセッサ W-2100/W-310 に影響を与えます (Intel® TXT の十分なメモリ保護によって、権限を持つユーザーがローカル アクセスによる権限の昇格を有効にした場合)。これにより、Intel® TXT 保護をバイパスする可能性があります。 • システム ファームウェアでの入力検証が不十分なことによって、権限の昇格、サービス拒否、またはローカル アクセスによる情報漏えいが可能になる可能性がある場合、CVE-2019-11137 (BIOS 2019.2 IPU Advisory) は、第 2 世代 Intel® Xeon® スケーラブル プロセッサ、Intel® Xeon® スケーラブル プロセッサ、Intel® Xeon® プロセッサ D ファミリー、Intel® Xeon® プロセッサ E5 v4 ファミリー、Intel® Xeon® プロセッサ E7 v4 ファミリー、Intel® Atom® プロセッサ C シリーズに影響を与えます。システム ファームウェアでの入力検証が不十分な場合、特権ユーザーが潜在的に有効にできる可能性があります。特権のエスカレーション、サービス拒否、またはローカル アクセスによる情報漏えい。 このリリースには、Cisco UCS M4 世代サーバ

リリース	不具合 ID	CVE	症状
			の BIOS 改定が含まれています。これらの BIOS リビジョンには、Cisco UCS M4 サーバ向けのこれらの脆弱性への対策に必要な、更新されたマイクロコードおよび Secure Initialization (SINIT) Authenticated Code Modules (ACM) が含まれています。
3.0(4o)	CSCvr54416	• CVE-2019-0151	Intel® プロセッサに基づく Cisco UCS C シリーズおよび S シリーズ M3 サーバは、次の一般的な脆弱性およびエクスポージャ (CVE) ID によって特定された脆弱性の影響を受けます。 • CVE-2019-0151 (CPU Local Privilege Escalation Advisory) は、特定の Intel® 第 4 世代 Intel® Core™ プロセッサ、第 5 世代 Intel® Core™ プロセッサ、第 6 世代 Intel® Core プロセッサ、第 7 世代 Intel® Core™ プロセッサ、第 8 世代 Intel® コア™ プロセッサ、Intel® Xeon® プロセッサ E3 v2/v3/v4/v5/v6 ファミリ、Intel® Xeon® プロセッサ E5 v3/v4 ファミリ、Intel® Xeon® プロセッサ E7 v3/v4 ファミリ、Intel® Xeon® スケーラブルプロセッサ 第 2 世代、Intel® Xeon® スケーラブルプロセッサ、Intel® Xeon® プロセッサ D-1500/D-2100)、Intel® Xeon® プロセッサ E-2100/E3100、および Intel® Xeon® プロセッサ W-2100/W-310 に影響を与えます (Intel® TXT の十分なメモリ保護によって、権限を持つユーザーがローカルアクセスによる権限の昇格を有効にした場合)。これにより、Intel® TXT 保護をバイパスする可能性があります。 このリリースには、Cisco UCS M3 世代サーバの BIOS 改定が含まれています。これらの BIOS リビジョンには、Cisco UCS M3 サーバ向けのこれらの脆弱性への対策に必要な、更新された Secure Initialization (SINIT) Authenticated Code Modules (ACM) が含まれています。

リリース 3.0(4n) のセキュリティ修正

リリース 3.0(4n) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
3.0(4n)	CSCvp34795	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	

リリース	不具合 ID	CVE	症状
			Cisco UCS C シリーズおよび S シリーズ M3 サーバは、Intel® Xeon® プロセッサ E5 v2 製品ファミリ プロセッサに基づいており、Microarchitectural Data Sampling (MDS) を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクспロイトの亜種に対して脆弱です。 • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストアバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 • 17 CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) は、CPU の到達不能なメモリに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 このリリースには、Cisco UCS M3 世代サーバの BIOS 改定が含まれています。これらの

リリース	不具合 ID	CVE	症状
			BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。

リリース 3.0(4I) のセキュリティ修正

リリース 3.0(4I) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
3.0(4l)	CSCvp34790 CSCvp34799	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	

リリース	不具合 ID	CVE	症状
			Cisco UCS C シリーズおよび S シリーズ M4 サーバは、Intel® Xeon®プロセッサ E7 v2、V3、および v4 製品ファミリ プロセッサに基づいており、Microarchitectural Data Sampling (MDS)を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクスプロイトの亜種に対して脆弱です。 • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストアバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • 17 CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) は、CPU の到達不能なメモリに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 このリリースには、Cisco UCS M4 世代サー

リリース	不具合 ID	CVE	症状
			バの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。

リリース	不具合 ID	CVE	症状
3.0(4I)	CSCvp34786	• CVE-2018-12126 • CVE-2018-12127 • CVE-2018-12130 • CVE-2019-11091	

リリース	不具合 ID	CVE	症状
			Cisco UCS C シリーズおよび S シリーズ M4 サーバは、Intel® Xeon® プロセッサ E5 V3、および v4 製品ファミリ プロセッサに基づいており、Microarchitectural Data Sampling (MDS) を使用して、他のアプリケーションによって CPU で処理されるデータへのアクセスを取得するエクスプロイトの亜種に対して脆弱です。 • CVE-2018-12126 (Microarchitectural Store Buffer Data Sampling) は、CPU のストアバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12127 (Microarchitectural Load Port Data Sampling) は、CPU のロードバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2018-12130 (Microarchitectural Fill Buffer Data Sampling) は、CPU のラインフィルバッファに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 • 17 CVE-2019-11091 (Microarchitectural Uncacheable Data Sampling) は、CPU の到達不能なメモリに影響を及ぼし、UCS Cisco IMC リリースに含まれる更新されたマイクロコードと、適切なベンダーから関連するオペレーティング システムおよびハイパーバイザパッチを適用することによって対処されます。 このリリースには、Cisco UCS M4 世代サー

リリース	不具合 ID	CVE	症状
			バの BIOS 改定が含まれています。これらの BIOS 改定には、これらの脆弱性の緩和に必要な更新されたマイクロコードが含まれています。

リリース 3.0(4i) のセキュリティ修正

リリース 3.0(4i) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
3.0(4i)	CSCvm03357	• CVE-2018-3615 • CVE-2018-3620 • CVE-2018-3646	Cisco UCS C シリーズ M3 サーバは、CPU の投機処理とデータキャッシュのタイミングを使用して権限情報を識別するエクスプロイトに対して脆弱な、Intel® プロセッサに基づいています。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。 • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel® SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシン モニタに影響) は、Intel® による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel® から更新されたプロセッサ マイクロ コードを適用することによって軽減されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 このリリースには、Cisco UCS M3 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサ マイクロ コードが含まれています。これらの脆弱性を軽減するために、適切なベンダーからのオペレーティングシステムおよびハイパーバイザパッチも必要になる場合があります。 詳細については、Cisco セキュリティ アドバイザリ: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 を参照してください。

リリース	不具合 ID	CVE	症状
3.0(4i)	CSCvj59326	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS C シリーズ M4 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して情報を効率的に漏洩する、Spectre と呼ばれるエクスプロイトの変種に対して脆弱な、Intel® プロセッサに基づいています。 CVE-2018-3639 (Spectre/Variant #4) および CVE-2018-3640 (Spectre/Variant #3a) は、サーバファームウェア バンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって対応されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 このリリースには、Cisco UCS M4 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサ マイクロコードが含まれています。
3.0(4i)	CSCvj59312	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS C シリーズ M3 サーバは、CPU の投機処理とデータ キャッシュのタイミングを使用して情報を効率的に漏洩する、Spectre と呼ばれるエクスプロイトの変種に対して脆弱な、Intel® プロセッサに基づいています。 CVE-2018-3639 (Spectre/Variant #4) および CVE-2018-3640 (Spectre/Variant #3a) は、サーバファームウェア バンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって対応されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 このリリースには、Cisco UCS M3 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサ マイクロコードが含まれています。

リリース 3.0(4e) のセキュリティ修正

リリース 3.0(4e) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
3.0(4e)	CSCvm03353	• CVE-2018-3615 • CVE-2018-3620 • CVE-2018-3646	Cisco UCS C シリーズ M4 サーバ (C460 M4 を除く) は、CPU の投機処理とデータ キャッシュのタイミングを使用して権限情報を識別する可能性のあるエクスプロイトに対して脆弱な、Intel® プロセッサに基づいています。これらのエクスプロイトは、総称して L1 Terminal Fault (L1TF) と呼ばれています。 • CVE-2018-3615 (SGX に影響) は Foreshadow と呼ばれ、既存の Cisco UCS サーバに影響を与えます。これは、Cisco UCS M5 および旧世代サーバと、HyperFlex M5 および旧世代サーバは Intel® SGX テクノロジーを使用しないためです。 • CVE-2018-3620 (OS/システム管理モードに影響) および CVE-2018-3646 (仮想マシンモニタに影響) は、Intel® による L1 Terminal Fault 攻撃とも呼ばれます。これらの脆弱性は、サーバファームウェアバンドルに含まれている Intel® から更新されたプロセッサ マイクロ コードを適用することによって軽減されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 このリリースには、Cisco UCS M4 世代サーバ (460 M4 を除く) の BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサ マイクロ コードが含まれています。これらの脆弱性を軽減するために、適切なベンダーからのオペレーティングシステムおよびハイパーバイザパッチも必要になる場合があります。 詳細については、Cisco セキュリティ アドバイザリ: CPU Side-Channel Information Disclosure Vulnerabilities: August 2018 を参照してください。

リリース	不具合 ID	CVE	症状
3.0(4e)	CSCvj59318	• CVE-2018-3639 • CVE-2018-3640	Cisco UCS C シリーズ M4 サーバは、CPU の投機処理とデータキャッシュのタイミングを使用して情報を効率的に漏洩する、Spectre と呼ばれるエクスプロイトの変種に対して脆弱な、Intel®プロセッサに基づいています。 CVE-2018-3639 (Spectre/Variant #4) および CVE-2018-3640 (Spectre/Variant #3a) は、サーバファームウェア バンドルに含まれている Intel から更新されたプロセッサマイクロコードを適用することによって対応されます。また、該当するベンダーからのオペレーティングシステムとハイパーバイザのパッチも適用されます。 このリリースには、Cisco UCS M4 世代サーバの BIOS 改定が含まれています。これらの BIOS 改定には、CVE-2018-3620 (OS/SMM) および CVE-2018-3646 (VMM) の緩和に必要な、更新されたプロセッサ マイクロ コードが含まれています。

リリース 3.0(4a) のセキュリティ修正

リリース 3.0(4a) では、次のセキュリティ修正が追加されました。

リリース	不具合 ID	CVE	症状
3.0(4a)	CSCvh07357	CVE ID はこの修正では使用できません	Clickjacking またはフィッシング攻撃に関連する Cisco UCS C シリーズ ラック サーバの Web インターフェイスの脆弱性に対処します。

リリース	不具合 ID	CVE	症状
3.0(4a)	CSCvg97965, CSCvg97979, CSCvg98015	• CVE-2017-5715 • CVE-2017-5753 • CVE-2017-5754	Cisco UCS C シリーズ サーバは、CPU の投機処理とデータキャッシュのタイミングを使用して権限情報を識別する可能性のあるエクスプロイトに対して脆弱な、Intel プロセッサに基づいています。これらのエクスプロイトは総称して Spectre および Meltdown と呼ばれています。 • CVE-2017-5753 Spectre/バリエント 1—適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2017-5715 Spectre/バリエント 2—USC C シリーズのリリースに含まれる更新されたマイクロコードを適用することによって、また、適切なベンダーから関連するオペレーティングシステムおよびハイパーバイザパッチを適用することによって対処されます。 • CVE-2017-5754 Meltdown—適切なベンダーからの、関連するオペレーティングシステムパッチを適用することによって対処されます。 この UCS C シリーズリリースには、CVE-2017-5715 (Spectre/バリエント 2) への対策の一環として必要な更新されたマイクロコードを含む、Cisco UCS M4 および M3 世代サーバの BIOS リビジョンが含まれています。 詳細については、次の Cisco セキュリティアドバイザリを参照してください: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel

解決済みの不具合

次の項では、解決済みの警告をリストします。

リリース 3.0(4) で解決済みの問題

リリース 3.0(4q)

リリース 3.0(4q) では、次の問題が解決されました。

表 3: VIC ファームウェア

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvm59040	Cisco UCS C220 サーバの稼働時間が180日を超えており、Cisco UCS VIC 1225 が搭載されている場合は、ホストからの接続が失われたと報告されることがあります。 この問題は、最新のファームウェアバージョンで解決されました。	2.0(13f)	3.0(4q)

リリース 3.0(4p)

リリース 3.0(4p) では、次の問題が解決されました。

表 4: 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvt63509	以下の LT0400MO および LT1600MO SSD モデルでは、電源投入時間が 40,000 時間に達すると、正常な動作条件でも、利用可能な残リストレージスペースが 0GB になったと報告されます。 • UCS-SD400G1KHY-EP • UCS-SD400G12S4-EP • UCS-C3X60-12G240 • UCS-SD16TG1KHY-EP • UCS-SD16TB12S4-EP • UCS-C3X60-12G2160 ドライブは電源サイクルを実行すると、オフラインになり、使用できなくなります。 この問題は、最新のファームウェアバージョンで解決されました。	3.0(4p)	3.0(4p)

リリース 3.0(4o)

リリース 3.0(4o) では、次の問題が解決されました。

表 5: 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvr67027	Cisco UCS S3260 M4 サーバは、RHEL 7.6 から 7.7 バージョンにアップグレードした後、ブートドライバを認識しなくなりました、 この問題は解決されました。	3.0(1d)	3.0(4o)

リリース 3.0(4n)

リリース 3.0(4n) では、次の問題が解決されました。

表 6: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq57969	脆弱性スキャナは、X-XSS 保護ヘッダーが存在していても、存在しないと報告します。	3.0(4a)	3.0(4n)

表 7: 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj91628	LSI9271 では、致命的なファームウェア (FW) エラーが発生します。RAID コントローラ上のすべてのファイルシステムがオフラインになるか、または切断されます。	3.0(4a)	3.0(4n)

リリース 3.0(4m)

リリース 3.0(4m) では、次の問題が解決されました。

表 8: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvq83392	アダプタ BU に関する新しいアップグレードまたはダウングレードルールのサポートが追加されました。	3.0(4l)	3.0(4m)

リリース 3.0(4l)

リリース 3.0(4l) では、次の問題が解決されました。

表 9: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvp41543	SSH クライアントが Cisco IMC への接続を確立できません。このことは、SSH クライアントが diffie-hellman-group14-sha1 をデフォルトの KEX アルゴリズムとして使用するときが発生します。この KEX アルゴリズムが Cisco IMC から削除されているためです。 SSH セッションを確立するために、より厳格な KEX アルゴリズムを使用する最新バージョンに SSH クライアントを更新します。	3.0(4j)	3.0(4l)

リリース 3.0(4k)

リリース 3.0(4k) では、次の問題が解決されました。

表 10: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvm37559	次の HTTP ヘッダーが TCP ポート 80 および TCP ポート 443 の HTTP 応答で欠落しています。 • X-Content-Type-Options • X-XSS-Protection	3.0(2f)	3.0(4k)

リリース 3.0(4j)

リリース 4.0(4) では、次の問題が解決されました。

表 11: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCve60056	C シリーズサーバを 3.0 (x) ファームウェアバージョンにアップグレードした後、SNMP は正しいローカルディスクステータスを返さなくなります。	3.0(1d)	3.0(4j)
CSCvk52168	S3260 サーバでは、SLAAC を使用して KVM または Cisco IMC web UI を起動すると、BMC SLAAC IP が ping に応答しなくなります。	3.0 (4i)	3.0(4j)

リリース 3.0 (4i)

リリース 3.0(4i) では、次の問題が解決されました。

表 12: ホスト ファームウェア アップグレード

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvk17568	IPv6 NFS 共有を使用しているときに、非インタラクティブな HUU を起動できません。次のエラーが表示されます。: 「エラー: リモート共有の指定が間違っているか、サーバに到達できません (Error: Bad remote share specification or Server not reachable)」	3.0(4a)	3.0(4i)

表 13: ハードウェア

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj83780	特定の低書き込みおよび長時間のアイドル時間のワークロードで、次の SATA SSD では読み取りエラーが表示されなくなりました。 • UCS-M2-240GB • HX-M2-240GB	3.0(4a)	3.0(4i)

リリース 3.0(4e)

リリース 3.0(4e) では、次の問題が解決されました。

表 14: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj66524	S3260 サーバの Cisco IMC では、サーバが起動し、問題なく実行されている場合でも、 BIOS POST タイムアウト (BIOS POST Timeout) エラーが表示されることがあります。	3.0(1c)	3.0(4e)

表 15: Web 管理

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj42923	IPv6 アドレスを使用していて、IPv4 アドレスが設定されていないか 0.0.0.0 に設定されている場合、KVM ウィンドウを起動できません。	3.0(3a)	3.0(4e)

表 16: XML API

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj75669	S3260 サーバでは、1つのコンピューティング ノードだけが存在する場合、XML API を使用して BMC2 インターフェイスを設定することはできません。	3.0(4a)	3.0(4e)

リリース 3.0(4d)

リリース 3.0(4d) では、次の問題が解決されました。

表 17: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvj54481	Redfish スキーマでは、システム下のリセットアクションの名前が誤って「 System.Reset 」となっており (正しくは「 ComputerSystem.Reset 」)、「 Target 」も間違っています (正しくは「 target 」)。これらの 2 つは、Redfish スキーマに準拠していません。	3.0(4a)	3.0(4d)
CSCvi06813	ファンが断続的に回転し、短時間後に通常の速度に戻ります。これは、タイムアウト値以内に raid コントローラのセンサーを読み取ることができなかったために発生します。	3.0 (3b)	3.0(4d)
CSCvi92466	ユーザパスワードに「\$」 (ドル記号) が付いている場合、 export-vnic コマンドは ftp プロトコルを使用して vNIC 設定をエクスポートできません。	3.0(3a)	3.0(4d)

リリース 3.0(4a)

リリース 3.0(4a) では、次の問題が解決されました。

表 18: BMC

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvh61997	C240 M4 SD ブート (Raid 1) サーバでは、バージョン 3.0(3e) へのアップグレード後に、obfl とメッセージログが次のメッセージでいっぱいになります (これにより syslog がいっぱいになります)。 4:2018 Jan 3 18:03:05 CET:BMC:kernel:-:<4>CYWB FWLOG (usbapp): USB VendorAck event, data=04:2018 Jan 3 18:04:10 CET:BMC:kernel:-:最後のメッセージは 5 回繰り返されます.....	3.0(3a)	3.0(4a)
CSCvh66273	Cisco IMC の再起動は、ドライブの予測的な障害に対するフォールトを発生させるために必要です。	3.0(3f)	3.0(4a)

表 19: 外部コントローラ

不具合 ID	症状	最初に影響を受けるリリース	リリースで解決済み
CSCvg25428	Call Home Alert メッセージは、定期的に (1 週間に 1 回) 生成されます。	3.0(3f)	3.0(4a)

未解決の不具合

次の項では、未解決の警告をリストしています。

リリース 3.0(4) で未解決の問題

リリース 3.0(4p) で未解決の問題

リリース 3.0(4p) には、次の未解決の問題があります。

表 20: ホスト ファームウェア アップグレード

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvt79547	Cisco UCS C220 M3 サーバでは、更新が完了すると、ユーザが [終了 (EXIT)] を押すのを待たずに、インタラクティブな HUU によって自動的にアクティベーションがトリガーされます。	これは、機能上の影響はありません。 すべてのコンポーネントが更新され、正常にアクティブ化されます。	3.0(4o)

リリース 3.0(4i) で未解決の問題

リリース 3.0(4i) には、次の未解決の問題があります。

表 21: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvo77732	Intel® Xeon® プロセッサ v2 から 4.0 (1a) バージョンに C460 M4 サーバをアップグレードした後、サーバが CATERR 障害を検出し、サーバが応答しなくなります。	3.0 (x) バージョンにダウングレードします。	3.0(4a)

リリース 3.0(4j) で未解決の問題

リリース 3.0(4j) には、次の未解決の問題があります。

表 22: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvm41493	Intel X7104 または XL710 アダプタを搭載した C460M4 サーバでは、Cisco IMC web UI が、Intel 710 PCIe アダプタのファームウェアバージョンとして 0 を表示します。	なし。	3.0(4j)

リリース 3.0(4a) で未解決の問題

リリース 3.0(4a) には、次の未解決の問題があります。

表 23: Web 管理

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvj37231	Cisco IMC が 3.0(4a) バージョンにアップグレードされた後、SMTP はメールアラートの送信を停止します。	Cisco IMC を 3.0(4d) にアップグレードし、CLI を使用して設定してください。 <pre>Server # scope smtp Server /smtp # set from-addr Server@cisco.com Server /smtp *# commit</pre> (注) アドレスが明確に区別されるように、[差出人アドレス (From address)] フィールドに一意のホスト名を追加することを推奨します。 たとえば、送信されるすべてのメールの送信元アドレスを 「C240M4-FXX1836J72S@cisco.com」のようにします。	3.0(4a)

リリース 3.0(3) で未解決の問題

リリース 3.0(3e) で未解決の問題

リリース 3.0(3e) では、次の問題が未解決です。

表 24: PID

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvg05613	次のドライブの PID 情報が正しく報告されません。 • UCS-S3260-NVM48 • UCS-S3260-NVM416 • UCS-S3260-NVM464 • UCS-S3260-NVM432	ホストの電源をオフにして、最新の S3260 PID カタログで CMC を更新します。	3.0(3e)

リリース 3.0(a3) で未解決の問題

リリース 3.0(3a) では、次の問題が未解決です。

表 25: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb11910	M3 サーバが、システムの BIOS POST 中に、「プラットフォームハードウェアの設定」段階で応答しなくなることがあります。システムイベントログには CATERR エラー記録されます。	自動回復の耐障害ブート (FRB) タイムアウトを有効にします。	3.0(3a)

表 26: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd84866	デュアル コントローラを搭載した S3260 サーバでは、すべての物理ドライブ (56) を AC サイクルなしでホットスワップするか、ホストを再起動すると、Web UI および PMCLI には引き続き古い物理ドライブデータが残ります。これは、すべての 56 ドライブが存在し、複数の仮想ドライブが設定されているシステムでのみ発生します。	サーバのブレードの電源を切り替えます。	3.0(3a)
CSCvb89330	C460 M4 サーバでは、NI-HUU を使用してファームウェアを任意の 2.x リリースファームウェアにダウングレードすると、複数のファンセンサー障害イベントが瞬間的に観測されます。これは、更新後に手動でサーバの電源を再投入した後に発生する可能性があります。	なし。	3.0(3a)

表 27: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd54828	RAID コントローラでエラーが発生し、リセットされます。これは、SAS SSD ではなく、外部 SATA ソリッドステートドライブ (SSD) を使用する場合に発生します。	なし。	3.0(3a)
CSCuv67943	C3160 サーバでは、MSM アプリケーションが、問題のあるスロットをレポートするポップアップメッセージを表示します。ただし、エラーは、1 つ小さいスロット番号に対して表示されます。たとえば、スロット番号 31 が不良スロットの場合、エラーはスロット 30 を不良スロットとして表示します。	正しいスロット番号は、エラーメッセージの番号より 1 つ大きいものです。	3.0(3a)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCva90939	S3260 サーバでは、MegaRAID ストレージ マネージャ (MSM) の物理ドライブの物理および論理セクターが誤って表示されることがあります。これは、S3260 サーバのノード構成で、ドライブがあるサーバからゾーン解除され、別のサーバに再ゾーン設定された場合に生じます。	MegaRAID ストレージ マネージャの画面を更新します。これにより、物理ドライブの情報が正しく表示されます。 または、[Cisco IMC ストレージ (Cisco IMC storage)] ページを使用して、物理ドライブの物理情報と論理情報を表示することもできます。	3.0(3a)
CSCvd25263	まれに、Cisco 12G SAS モジュール型 RAID コントローラは、高負荷の I/O ロードが発生している間にマルチビット ECC エラーが発生させる可能性があります。	コントローラを新しいものに交換し、古いコントローラは返却してください。	3.0(3a)
CSCvd07355	S3260 サーバでは、接続管理を有効または無効にすると、予測不可能な I/O パフォーマンスが得られます。これは、ホストがオンラインになったときに発生します。	接続管理を有効化または無効化する前に、ホストをオフラインにします。	3.0(3a)
CSCvd18495	C460 M4 サーバでは、10GE LOM ポート (X540 ベース) のファームウェアを、リリース 3.0(3) からそれ以前のリリースにダウングレードすると失敗し、次のエラー メッセージが表示されます: <i>ERROR LOM</i> ファームウェアの <i>EEupdation</i> に失敗しました (エラーコード: 2705) (<i>ERROR LOM Firmware EEupdation failed (Error Code: 2705)</i>)	なし。	3.0(3a)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd10359	Intel X540 PCIe アダプタのファームウェア バージョンを 3.0 (3) バージョンから以前のバージョンにダウングレードすると失敗し、次のエラーメッセージが表示されます。 <i>Intel X540 PCI</i> アダプタの更新に失敗しました (エラーコード: 3115) (<i>Intel X540 PCI adapter update failed (Error Code: 3115)</i>)	なし	3.0(3a)

表 28: ハードウェア

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvc17387	一部の C220 M4 サーバでは、770 ワット電源装置 (PSU) に接続されている場合、ファームウェアをリリース 2.0(13e) にアップグレードすると PSU エラーが表示されます。このエラーは、UPS が出しているノイズの結果として発生している可能性があります。	なし。	3.0(3a)

表 29: ユーティリティ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd78351	UCSCFG ユーティリティを使用して Cisco IMC 設定のインポートを実行しようとすると、Cisco IMC データのインポートが失敗し、インポートエラーメッセージが表示されます。これは、電力特性評価ステータスが「実行中」の場合、または実行が必要な場合に発生します。	Cisco IMC 設定をインポートまたはエクスポートする前に、電力特性評価を手動で実行します。	3.0(3a)

リリース 3.0(2b) で未解決の問題

リリース 3.0(2b) では、次の問題が未解決です。

表 30: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvc31545	Cisco IMC のインポートまたはエクスポート オプションを使用して KMIP 設定を構成することはできません。	XML API、web UI、CLI を使用して、サーバごとに KMIP 設定を手動で設定します。	3.0(2b)

リリース 3.0(1c) で未解決の問題

リリース 3.0(1c) では、次の問題が未解決です。

表 31: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb49288	Web UI では、[パーセンテージ残量 (Percentage Life left)] フィールドが 35% 未満になると、ステータスバーは赤色で表示されますが、障害エンジンのエントリは生成されません。	なし。UI の [パーセンテージ残量 (Percentage Life left)] フィールドは、アドバイザーの警告だけを表示します。	3.0(1c)

表 32: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb96598	サーバをリリース 3.0 (1x) にアップグレードした後、SAS HBA コントローラで「CTRL+C」ユーティリティを使用してブートデバイスを再挿入しようとする、デフォルトの追加キー「+」は期待どおりに機能しません。[ブート順 (Boot Order)] フィールドは、複数のコントローラが存在することを示す値または 0 または 1 を受け入れます。ただし、現在、フィールドの値を変更したり、入力したりすることはできません。 これは、リリース 2.0 (10) または 2.0 (13) などの以前のリリースからアップグレードする場合に発生します。	CTRL + C ユーティリティでは、ブートデバイスを再挿入するのに j 「INS」キーを使用します。デフォルトの「+」キーは使用しません。	3.0(1c)

表 33: ユーティリティ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvc25435	HDD ファームウェアは、ホスト更新ユーティリティを使用してアップグレードした後も、古いバージョン表示します。 これは、高度な BIOS 設定でファームウェアを AHCI モードに変更した場合に発生します。その結果、ファームウェアのアクティベーションが失敗します。	LSI SW RAID モードでファームウェアをアップグレードします。	3.0(1c)

リリース 2.0(13h) で未解決の問題

リリース 2.0(13h) には、次の未解決の問題があります。

表 34: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCva96401	1227、1387、または 1385 VIC アダプタが搭載された C220 M4 および C240 M4 サーバでは、サーバのリブートの際、時折、VIC アダプタのマッピングが解除されます。 (注) VIC アダプタは、次のホストのリブート時に検出されます。	なし。	2.0(13h)

リリース 2.0(13e) で未解決の問題

リリース 2.0(13e) では、次の問題が未解決です。

表 35: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCva38014	C220 M4 および C240 M4 サーバでは、BIOS の post 中にシステムが応答なくなり、「設定およびメモリ (Configuring and Memory)」ステージで、次の警告がログに記録されます。 警告がログに記録されました (A warning has been logged!) Warning Code = 0x30, Minor Warning Code = 0x13, Data = 0x10100	1. サーバの AC 電源をオフにします 2. ケーブルを抜きます 3. CPU を交換します 4. Dimm を再度装着してから、サーバの電源を入れ直します。	2.0(13e)

CSCuz94596	再起動プロセスのテスト中に、DIMMがマッピングされます。この問題は、Intel Xeon v4 プロセッサと Montage DIMM を使用している場合にのみ発生します。DIMM のラウンドトリップ時間が DIMM に対して予想されているよりも長いからです。	なし。	2.0(13e)
------------	---	-----	----------

表 36: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCva82566	Intel X520 ネットワーク アダプタでは、サービスプロファイルの関連付け後に、Web UI またはコマンドライン インターフェイスで vNIC のパスが表示されない場合があります。	なし。	2.0(13e)
CSCuy16602	進行中の I/O 操作中にストレージコントローラをリセットすると、BSOD になります。	なし。	2.0(13e)
CSCuy37152	C220 M4 サーバでは、検出が失敗した後も、OMB ドライブは Cisco UCSC-P-12Gbps SAS HBA コントローラによって不良としてマークされません。	なし。	2.0(13e)
CSCuz21377	C240 M4 サーバの場合、Web UI とコマンドライン インターフェイスでは、エキスパンダで接続されたケースに1つのコネクタ表示ビュー (CN0) しか表示されません。	ストレージ ログを参照し、次の文字列を確認してください。 •BBBBBBBB0000 00000000000000 •BBBB00000000 00000000000000	2.0(13e)

CSCva59776	C240 M4 サーバでは、別のドライブが Locate LED コマンドを発行した場合でも、直前に挿入されたドライブの LED が点滅します。 これは、ドライブが挿入された後の、連続した Locate LED コマンドを伴う任意の操作で発生します。	ドライブの取り外し操作を実行する前に、ドライブの物理スロットを書き留めておきます。	2.0(13e)
CSCvb00471	大量の I/O が発生すると、Windows OS が「死のブルー スクリーン」を表示してクラッシュします。ログにマルチビットの ECC エラーが記録されます。	なし。	2.0(13e)

リリース 2.0(9c) で未解決の問題

リリース 2.0(9c) では、次の問題が未解決です。

表 37: VIC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuw17399	Cisco UCS VIC 1387 から Nexus 3016Q スイッチに 7 メートルのアクティブな光ケーブルを接続した後で、トランシーバの詳細を確認すると、QSFP のタイプの検出に失敗します。トランシーバの詳細を確認しても、コネクタの QSFP タイプは検出されません。	なし。	2.0(9c)

リリース 2.0(4c) で未解決の問題

リリース 2.0(4c) では、次の問題が未解決です。

表 38: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCut37666	JBOD モードでは、Cisco 12G モジュール型 SAS パススルーコントローラに接続された HDD の高精度ブート順序を作成した後、HDD は作成された順序で表示されません。この問題は、JBOD 機能を備えた LSI コントローラに当てはまります。	システムのブート順序を制御するには、F6/Setup のブート順序制御機能を使用します。	2.0(4c)

表 39: HUU

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCus94537	HDD を使用する HDD ファームウェアの更新は、HDD ファームウェアが順番に更新されるため、時間がかかります。これにより、多くの HDD を搭載したサーバのアップグレードにかかる時間が長くなります。	なし	2.0(3d)

リリース 2.0(3d) で未解決の問題

リリース 2.0(3d) では、次の問題が未解決です。

表 40: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース

リリース 1.4(7) で未解決の問題

CSCup56423	実際のブート順序には、どの LUN が LSI sSATA、LSI SATA、および AHCI モードのさまざまな HDD に割り当てられているかを識別するための情報がありません。	[ROM モード (ROM mode)] オプションを [UEFI のみ (UEFI only)] に設定します。	2.0(3d)
CSCun24358	C220 M4 および C240 M4 サーバは、BIOS セットアップから HII インターフェイスを使用してアダプタ設定を変更すると、F10 を押しても再起動しません。サーバは起動動作を繰り返し、新しい設定は有効になりません。	手動でサーバをリブートします。	2.0(3d)

リリース 1.4(7) で未解決の問題

リリース 1.4(7) では、次の問題が未解決です。

表 41: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCud18756	外部ポートを搭載した LSI ストレージコントローラ (-8e カード) は、CIMC ローカルストレージ管理には表示されません。	なし。	1.4(7)

既知の動作

次の項では、既知の動作を示します。

リリース 3.0(4) の既知の動作

リリース 3.0(4q) の既知の動作

リリース 3.0(4q) の既知の動作は次のとおりです。

表 42: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvu41958	Emulex カード LPe16002、OCe14102、および OCe11102 カードのファームウェアを、2.0(13q) より前のリリースから最新のリリースにアップデートしようとする、失敗することがあります。	アップグレードパス: 1. リリース 2.0(13q) にアップグレードします。 2. 最新のリリースにアップグレードします。	3.0(4p)
CSCvu42509	ユーザは、LPe16002 および OCe11102 カードを搭載した Cisco UCS C シリーズ M3 サーバ上では、FC および FCoE LUN を設定できません。カード BIOS でのサーバ側のマッピング LUN のターゲットの詳細は、入力されません。	この問題の既知の回避策はありません。 FC および FCoE LUN を設定するには、同じサーバで LPe16002 カードまたは OCe11102 カードのいずれかを使用する必要があります。	3.0(4p)

リリース 3.0(3) の既知の動作

リリース 3.0(3e) の既知の動作

リリース 3.0(3e) の既知の動作は次のとおりです。

表 43: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvf96879	HTML ベースの vMedia のアクティブ化が失敗します。これは、Google Chrome ブラウザバージョン61または62を使用すると発生します。	IE またはその他のブラウザを使用します。	3.0(3a)

リリース 3.0(3a) の既知の動作

リリース 3.0 (3a) の既知の動作は次のとおりです。

表 44: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuq15528	レガシー ブート モードでは、いくつかのブート オプションがメニューまたはブート オーバーライド ページに表示されません。これは断続的に発生する問題であり、SATA/RAID が接続された複数のブート オプションがあり、[ブート (boot)] オプションで UEFI ブート オプションが無効になっている場合に発生します。	メニューまたはオーバーライド オプションに表示されない特定のオプションからブートする場合は、Cisco IMC からポリシーを実行するか、F2 キーを押してデバイスを最初のブートデバイスとして設定します。ブートオプションページには、すべてのデバイスが正しく表示されます。	3.0(3a)

CSCva57433	Intel イーサネット コンバージド ネットワーク アダプタ X710-DA2 PCI カードは、ポート 2 のレガシー iSCSI オプション ROM を起動できません。これを表示するには、SEL log で警告メッセージを検索します。 DXE ブート サービスのドライバに、レガシー プシオン ROM をシャドウイングするだけのメモリがありません。 これは、システムがレガシーブート用に設定されており、Intel イーサネット コンバージド ネットワーク アダプタ X710-DA2 PCI カードが iSCSI ブートに設定されている場合に発生します。カードは余分なランタイム オプション ROM メモリ領域を消費するので、ポート 1 にのみオプション ROM をロードできます。ポート 1 のオプション ROM をロードすると、残りの使用可能なオプション ROM のメモリ領域が不足して、ポート 2 のオプション ROM をロードできません。	X710-DA2 PCI カードでレガシー iSCSI ブートを行う場合にはポート 1 を使用し、残りのスロットと LOM ではオプション ROM を無効にしてください。	2.0(13e)
------------	---	---	----------

表 45: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCux43338	Mozilla Firefox Web ブラウザで、[サーバ証明書 の貼り付け (Paste Server Certificate)] オプションを Web UI でクリックすると、ポップアップ ダイアログ ボックスのため [証明書の保存 (Save Certificate)] および [キャンセル (Cancel)] ボタンが隠れます。	ダイアログ ボックスを移動して [証明書の保存 (Save Certificate)] ボタンと [キャンセル (Cancel)] ボタンが表示されるようにするか、Google Chrome や Microsoft Internet Explorer など、別の Web ブラウザを使用してください。	2.0(9c)

CSCuw76431	UCS C シリーズ サーバに Red Hat Enterprise Linux 7.1 オペレーティングシステムをインストールすると、次のような重要な SEL エントリが作成されます。 <i>The 2015-10-12 10:35:07 critical "System Software event: OS Event sensor, unknown event".</i> (システム ソフトウェア イベント: OS イベントセンサー、不明なイベント)	なし。	2.0(9c)
CSCvd04304	KMIP 証明書および KMIP サーバの詳細を設定した後に工場出荷時の初期状態にリセットしても、既存の Cisco IMC および KMIP サーバの証明書は期待どおりに削除されません。	コマンドライン インターフェイスで任意の kmip モードを範囲として、restore または delete コマンドを使用してください。または、Web UI にログインし、[セキュア キー管理 (Secure Key Management)] タブの [削除 (Delete)] ボタンを使用します。	3.0(3a)

表 46: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvc51343	Broadcom 5709 イーサネット PCIe アダプタを搭載した C220 M4 および C240 M4 サーバは、ネットワーク使用率が高くなるとクラッシュする可能性があります。	BIOS で PCI デバイスのアクティブ状態電源管理 (ASPM) を無効にしてください。	3.0(3a)

CSCuy05774	S3260 サーバで、RedHat Linux OS 7.2 でサーバをシャットダウンしようとする、デフォルトで OS が Web UI モード (Ctrl + Alt + F7) で起動し、BMC からの power shutdown コマンドはシステムをスリープ状態にします。 キーボードまたはマウスでアクションを実行すると、システムが正常状態に戻ります。 ユーザが root としてログインしても、同じ動作が観察されます。	シェルプロンプトインターフェイス (Ctrl + Alt + F2) を使用し、root としてログインします。	3.0(3a)
CSCvc81096	サーバをプルアウトすると、M3 または M4 サーバを検出するのが困難になります。M3 サーバは複数のコントローラをサポートできないため、下位互換性のための「S1」ディスプレイが必要です。M4 サーバは複数のコントローラをサポートしているため、「S1-MZ1」のディスプレイが必要です。 これは、サーバ上でゾーン分割を設定してから、サーバをプルアウトしたときに発生します。	なし。	3.0(3a)
CSCux20272	C240 M4 サーバでは、インストール後に Redhat Enterprise Linux OS バージョン 6.5 が起動しなくなります。これは、PXE または DVD イメージを使用して OS をインストールすると発生します。	OS のインストール中に、[デスクトップパッケージ (Desktop Packages)] オプションを選択しないでください。	2.0(10b)
CSCva44733	PCI スロット設定でオプション ROM が無効になっている場合、storelib ライブラリはディスクのインベントリ操作を行うことができません。	オプション ROM を有効にしたままにしてください。	2.0(13e)

CSCvb34628	まれに、ストレージコントローラのファームウェアを更新する際に、「Flash Programming error」(Flash プログラミングエラー)が発生し、障害が発生したコントローラの返品許可 (RMA) が必要となる場合があります。 これは、バッテリー スーパー コンデンサの再学習が進行中にファームウェアのアップデートが発行され、フラッシュの書き込みが完了する前に再学習が完了した場合にのみ発生します。	この問題が発生した場合は、次の手順を実行します。 1. バッテリー/スーパーコンデンサの学習サイクルのステータスを確認し、完了するまで待ちます。 2. 「次の学習時間」が、ファームウェア アップデート発行前の1時間以内に予定されていないことを確認します。	2.0(13e)
CSCva55926	Redhat Enterprise Linux OS バージョン7.2 を、Qlogic 8442T iSCSI LUN にインストールしようとする、「Unknown error occurred」(不明なエラーが発生しました)というメッセージが表示されて失敗します。	なし。	2.0(13e)

表 47: 外部 OS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd65151	RedHat Enterprise Linux オペレーティング システム バージョン6.8 のインストールでデスクトップ パッケージを選択した場合、iSCSI LUN 経由で起動しません。 これは、OSがローカルストレージまたはSANターゲットではなく、iSCSIターゲットにインストールされている場合にのみ発生します。	インストールにデスクトップパッケージが必須の場合は、RedHat Enterprise Linux オペレーティング システムバージョン6.9 を使用してください。	3.0(3a)
CSCuz28948	C460 M4 サーバでは、SSD LSI ドライバの ESXi vFlash の問題が原因で、RedHat Enterprise Linux 仮想マシンがクラッシュします。これは、複数の IO がバックアップソフトウェアで実行されている場合に発生します。	vFlash を無効にしてください。	3.0(3a)

表 48: ユーティリティ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd34692	UCS Configuration Utility を使用して遅延ファームウェアの更新を開始しようとしているときに、NIHUU は更新をトリガーできません。これは、KVM または Web UI を使用してワンタイム ブートの順序を設定した場合に発生します。	リクエストをキャンセルし、CLI を使用して、ワンタイム ブートの順序を設定してください。	3.0(3a)
CSCvc78162	ブート順序を設定するときに、Cisco IMC トークンをテキストファイルにエクスポートする前に (Windows の UCS CFG ツールを使用して) IPv6 を有効にすると、Cisco IMC で IPv6 が有効として表示されている場合でも、[V6有効 (V6 Enabled)] トークンが [無効 (Disabled)] と表示されます。	コマンドライン インターフェイス、または XML API インターフェイスを使用して、[V6 有効 (V6-Enabled)] トークンのステータスを [有効 (Enabled)] に戻してください。	3.0(3a)
CSCvc78173	Web UI からブート順序を設定するときに、set コマンドを使用してブート順序を設定すると、「class name tag missing」(クラス名タグがありません) というエラーメッセージが表示されます。 これは、UEFI シェルを使用してブート順序をテキスト (入力) ファイルにインポートしたとき、ブート順序のヘルプ コンテンツが入力ファイルの一部となっている場合に発生します。	ヘルプコンテンツを削除し、入力ファイルに設定パラメータ データを残してください。	3.0(3a)
CSCvc56345	S3260 サーバでは、HUU を使用してリリース 3.0(3) を以前のバージョンにダウングレードすると、CMC1 および CMC2 がアクティブになりません。 これは、シングル サーバデュアル SIOC 機能が有効になっている場合に発生します。	サーバをダウングレードする前に、[シングル サーバデュアル SIOC (single server dual SIOC)] オプションを無効にしてください。	3.0(3a)

表 49: VIC ファームウェア

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuu59408	Nexus 7018 スイッチバージョン 7.2.0 (ファブリックエクステンダ N2232PP のアップリンクが 1 つの F2 モジュールポートにのみ接続されており、物理ホスト UCS に接続されているホストインターフェイスがストレージ仮想デバイスと共有されている) では、モジュールのアップリンク後に F2 モジュールをホストインターフェイスにリロードすると、DCBX PDU の確認応答が失われます。	Nexus 7018 スイッチのオーナー仮想デバイスで、ファブリックエクステンダのホストインターフェイス (HIF) ポートをフラッピングして、DCBX 交換が初期化されるようにしてください。	2.0(6d)

表 50: Web 管理

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvd58182	C220 M3、C240 M3、C22 M3、および C24 M3 サーバでは、Java ベースの KVM の起動に失敗します。これは Java バージョン 1.8 (アップデート 121) で Microsoft Internet Explorer ブラウザを使用すると発生します。	起動中に画面上にセキュリティ警告がポップアップ表示されたら、 [キャンセル (Cancel)] をクリックしてください。その後、KVM コンソールが正常に起動します。	3.0(3a)

リリース 3.0(1c) の既知の動作

リリース 3.0(1c) の既知の動作は次のとおりです。

表 51: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCva99738	ユーザ権限でログインしている場合は、BIOS のオプション、「Save and Exit」を使用して BIOS 設定の変更を保存することはできません。これは、ユーザモードで BIOS 設定領域にログインした場合にのみ発生します。	F10 キーを押し、保存して終了します。	3.0(1c)
CSCvc14144	セットアップ中に Enhanced Intel Speedstep テクノロジー (EIST) が無効になっている BIOS を更新すると、電力特性評価が行われず、ステータスが「Not Run」と表示されます。	なし。	3.0(1c)
CSCva67765	C460 M4 サーバでは、Cisco IMC F8 設定メニューを使用して VLAN 設定を変更すると、VLAN 設定は正しく適用されますが、[設定 (configuration)] メニューには完全に表示されません。	F5 ボタンを押して画面を更新する前に、2 分以上待機します。	2.0(13e)

表 52: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb77846	証明書を適切にインストールせずに Safari ブラウザで HTML ベースの KVM を起動すると、HTML ベースの KVM の起動が失敗します。	証明書をインストールするには、次の手順を実行します。 「Safari が Web サイトの ID を確認できない」というメッセージが表示されたら、[証明書の表示 (Show Certificate)] ボタンをクリックします。 - 証明書のドロップダウンメニューから、[常に信頼 (Always Trust)] を選択します。 [続行 (Continue)] をクリックします。ローカルパスワードを入力して証明書を更新するように求められます。 [設定の更新 (Update Settings)] をクリックします。 証明書がインストールされます。この証明書は、サーバとのすべての通信に使用できます。	3.0(1c)
CSCva43470	Mozilla Firefox ブラウザバージョン 32.0 では、HTML ベースの KVM コンソールでの仮想メディアのアクティブ化が失敗します。	Mozilla Firefox ブラウザバージョン 38.0 以降を使用するか、Google Chrome や Microsoft Internet Explorer などの別のブラウザを使用します。	3.0(1c)
CSCva05249	HTML ベースの KVM コンソールでの仮想メディア データ転送には、かなりの時間がかかります。	暗号化を無効にした状態で Java ベースの仮想メディアを使用します。	3.0(1c)
CSCuy92283	Cisco IMC に CA チェーン証明書をダウンロードし、証明書バインディングが有効になっている場合、LDAP ユーザ認証は失敗します。	Cisco IMC にダウンロードする前に、CA チェーン証明書 (.p7b 形式) を PEM 形式に変換します。	2.0(13e)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuz82915	Redhat Linux が UI モードの場合、スクロールキーを有効にすると、HTML KVM ウィンドウには表示されません。	なし。スクロールロックは、UI モードの Redhat ではサポートされていません。	2.0(13e)

表 53: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvc08224	PMCSSACLI ユーティリティを使用する場合でも、次のコマンドでは、VMware オペレーティングシステムの HDD ファームウェアを更新できません。 <pre>pmcssaccli ctrl slot=1 pd CN0:1:1 flash file=firmware.bin mode=7 immediate=enable。</pre> ファームウェアの更新は、コマンドで強制フラグを使用した場合にのみ成功します。 これは、サーバまたはクライアントの SSACLI 間のリモート接続環境が VMware のコマンドプロンプトをサポートしていないために発生します。	次の例に示すように、force flag オプションを使用します。 <pre>pmcssaccli ctrl slot=1 pd CN0:1:1 flash file=firmware.bin mode=7 immediate=enable forced。</pre>	3.0(1c)

表 54: ユーティリティ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvc06814	最新の非インタラクティブな HUU Python スクリプトは、リリース 3.0(1) での cookie の取得とファームウェア コンポーネントの更新に失敗します。		3.0(1c)

不具合 ID	症状	回避策	最初に影響を受けるリリース
		問題を解決するには、次のガイドラインに従ってください。 - リリース 2.0(3) よりも古いリリースからアップグレードする場合は、次のようにします。 - クライアントで Open SSL バージョン 1.0.0-fips を使用し、リリース 2.0(4) で利用可能な Python スクリプトを使用して、リリース 2.0(4) にアップグレードします。 - 次に、クライアントで Open SSL 1.0.1e-fips を使用し、リリース 3.0(1) で利用可能な Python スクリプトを使用して、リリース 3.0(1) にアップグレードします。 - ファームウェアをリリース 2.0(2) 以降からリリース 3.0(1) にアップグレードする場合は、Open SSL 1.0.1e-fips を使用し、リリース 3.0(1) で使用可能な NIHUU Python スクリプトを使用して、リリース 3.0(1) に更新します。 3.0(1) から 2.0 リリースに 2.0(1) へダウングレードする場合は、クライアントで Open SSL 1.0.1e-fips を使用して、必要なバージョンに	

不具合 ID	症状	回避策	最初に影響を受けるリリース
		ダウングレードします。	
CSCvc38739	非インタラクティブな HUU スクリプトを使用してファームウェアを更新した後、ファームウェア出力のサマリに、次のようなタイムアウトエラーが表示されることがあります。 CIMC-< IP > のファームウェアの更新に失敗しました。エラー-ファームウェアの更新がタイムアウトしたため失敗しました (Firmware update failed for CIMC - <IP>, Error - Firmware update failed because it timed out)。詳細については、ホストを確認してください (Check host for details)。 エラーメッセージが表示されても、ファームウェアの更新に成功している場合があります。	すべてのファームウェアコンポーネントが正常に更新されたかどうかを確認してください。	3.0(1c)

表 55: VMware

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCux87650	VMware ESXi 5.5.0 以降を使用しているサーバでは、storecli はアダプタを識別できますが、ストレージコントローラと通信できません。	影響を受けるモジュールを ESXi コマンドラインから無効にし、次のコマンドを使用してコントローラと通信します。 1. <code>esxcli system module set --enabled=false --module=lsi_mr3</code> 2. <code>~# esxcli system module set --enabled=false --module=lsi_mr3</code> 3. <code>~# reboot</code>	2.0(10b)
------------	--	--	----------

表 56: Web 管理

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb78527	Microsoft Internet Explorer を使用して Cisco IMC にログインし、 [ヘルプ (Help)] ボタンをクリックすると、ポップアップウィンドウを有効にするようにページが表示されます。ポップアップウィンドウを有効にして Internet Explorer リロードしても、ページ上のアイコンは表示されず、 [ヘルプ (Help)] ウィンドウは開くことができません。	Google Chrome または Mozilla Firefox ブラウザを使用します。	3.0(1c)
CSCuz83739	HTML ベースの KVM コンソールで、ドロップアンドダウン方式を使用して仮想メディア内のイメージをマッピングしようとする、仮想メディアが応答を停止することがあります。	仮想メディアイメージをマッピングするには、 [参照 (Browse)] オプションを使用します。	3.0(1c)

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb43134	ファームウェアを以前のバージョンから 3.0(1) にアップグレードした後、初めてログインすると、新しい HTML5 ベースの UI ではなく古い web UI がページに表示されます。	Web ブラウザを更新します。	3.0(1c)
CSCvb67922	複数の (既存の) Java バージョンを使用して KVM コンソールを起動すると、ネイティブライブラリエラーが表示されます。	マシン上で複数の Java バージョンを無効にするには、次の手順を実行します 1. [スタート (Start)] パネルで [Java の設定 (Configure Java)] を選択します。 2. [Java] タブをクリックします。 3. [表示 (View)] をクリックします。 4. Java バージョンのリストから、必要のない Java バージョンのチェックボックスをオフにし、適切なバージョンをオンにします。	3.0(1c)
CSCvb66685	HTML ベースの KVM コンソールでは、「CTRL」キーと「ALT」キーは機能しません。	[マクロ (Macro)] > [管理 (Manage)] オプションを使用してユーザ定義マクロを作成するか、Java ベースの KVM を使用します。	3.0(1c)
CSCuz68208	Microsoft Internet Explorer では、HTML ベースの KVM コンソールをフルスクリーンモードに最大化することはできません。	Google Chrome または Mozilla Firefox ブラウザを使用します。	3.0(1c)
CSCuz39581	Java 8 Update 77 を搭載したブラウザで Java ベースの KVM を起動することはできません。	使用可能な最新の Java バージョンを使用します。これは、Java8 Update 92 または 91 です。または Java 8 Update 45 以下を使用します。	2.0(13e)

表 57: XML API

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCvb17203	Web ブラウザでコマンド CURL または POST を使用した XML API の操作は、リリース 3.0 の場合、Transport Layer Security (TLS) バージョン 1.0 および 1.1 では動作しません。	TLS バージョン 1.2 にアップグレードします。	3.0(1c)

リリース 2.0(13e) の既知の動作

リリース 2.0(13e) では、次の問題が既知の動作です。

表 58: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCux72847	2番目の 10 GE LOM ポートからの PXE ブートは機能しません。この問題は、PXE ブートが2番目の 10GE LOM ポートからブートするように設定されており、SAS コントローラのオプション ROM も有効になっており、ロードされている場合に発生することがあります。	SAS または LOM0 (1GE) オプション ROM を無効にして、両方の 10GE オプション ROM をロードするのに十分なスペースを確保します。	2.0(13e)
CSCuy15543	Cisco IMC Web UI および CLI では、Cisco IMC から IpmiBootOrder を設定するのに、高精度ブート順序ポリシーの設定に使用される Configpolicy.xml ファイルを使用すると、実際のブート順序が正しく表示されません。	なし。正しくないブート順序は無視する必要があります。この機能は期待どおりに動作し、BIOS セットアップで実際のブート順序が正しく表示されます。	2.0(9e)

表 59: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCux92616	Java バージョン1.8 および update 66 を実行しているクライアントシステムでは、vMedia をアクティブ化しようとし、暗号化されていない vMedia セッションのポップアッププロンプトを受け入れると、KVM がクラッシュします。	このポップアップを回避するには、Cisco IMC Web UI を使用して仮想メディア暗号化を有効にします。	2.0(13e)
------------	--	---	----------

表 60: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuy62185	ポートが iSCSI で設定されている場合は、 Fast Utility オプションにアクセスするのに Ctrl+Q キーを使うことができません。	BIOS の USB 設定でポート60/64 エミュレーションを有効にします。	2.0(10b)
CSCuz55512	SLES11 SP3 OS レガシー インストールは、C220 M4 サーバと C240 M4 サーバで UCSC UCSC-PSAS12GHBA の inbox ドライバを使用すると、応答なくなります。	なし。非同期ドライバを使用します。	2.0(13e)
CSCuy12854	Windows 上の UCSC UCSC-PSAS12GHBA では、ブートドライブを除くすべてのドライブがオフラインとしてマークされます。	なし。	2.0(13e)
CSCuv51716	複数の Tesla (k40/K80) カードを搭載した Magma シャーシ GPU エクспанダに接続され、RedHat Enterprise Linux 6.x オペレーティングシステムを実行している C240 M4 サーバは、再起動中に応答なくなる場合があります。	サーバをハードリブートします。	2.0(9c)

CSCuw86750	すべての仮想ドライブを含む物理ドライブが取り外される、または交換されると、システムは、「設定が失われた (configuration lost)」という障害を表示します。これは、仮想ドライブが作成されるか、または WebBIOS または Ctrl + R 機能を使用して設定がクリアされるまで、変わりません。	再起動して、エラーがクリアされたかどうかを確認します。ほとんどの場合、これはクリアできます。 エラーがクリアされない場合は、仮想ドライブを作成するか、または Web BIOS または Ctrl + R 機能を使用して設定をクリアします。	1.5(1)
CSCux44506	ブート仮想ドライブが、別の仮想ドライブをブート ドライブとして設定した後に非表示とマークされ、システムが以前に設定されたブート仮想ドライブから実行されている場合は、オペレーティング システムによりシステムがシャットダウンされることがあります。	なし。	2.0(9c)
CSCuz61344	CLI または GUI を使用してスタンダロンの Cisco IMC バージョン 2.0.9 にログインしようとする、インターフェイスが応答しなくなります。エラーが表示されることがありますが、ほとんどの場合、応答しません。これは、Cisco IMC での LDAP グループ認証が原因で発生します。	影響を受けている LDAP グループをグループ認証オプションから削除するか、または AD データベースの循環ループを解決します。 検索グループの深さを 1 ～ 3 の間の値に変更します。	2.0(9d)
CSCuz93611	仮想ドライブまたはドライブ グループがトランスポート レディに設定して、メンバーの物理ドライブを取り外すと、仮想ドライブまたはドライブ グループがブロックされて削除できなくなり、トランスポート レディ状態もクリアできなくなります。トランスポート レディの設定は、最適な仮想ドライブまたはドライブ グループに対してのみ行えるものだからです。	仮想ドライブまたはドライブ グループのすべてのメンバを削除し、再挿入してから、次の手順に進みます。	2.0(13e)

CSCva17225	すべての物理ドライブに Powersave コマンドを送信した後でも、 Samsung および SanDisk SAS SSD はアクティブのままです。これは、 Start Stop Unit (SSU) コマンドをサポートしていないためです。	なし。	2.0(13e)
CSCuw55009	3260 サーバでは、240 VD ファームウェアをサポートする SAS ファームウェアのアップグレードまたはダウングレードを行う際、次のような問題が発生します。 アップグレード中は、 <i>auto-rebuild</i> は開始されません。ダウングレード中は、整合性チェックとセキュア イレースの操作は再開されません。	なし。	2.0(9)

表 61: ファームウェアのアップグレード

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuz48865	ホスト ファームウェアを 2.0(13x) バージョンから 2.0(2x) バージョンにダウングレードすることはできません。	最初にファームウェアを 2.0(13x) から 2.0(6f) にダウングレードし、その後 2.0 (2x) バージョンにダウングレードします。	2.0(13e)

表 62: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCun50408	StorCli および WebBIOS から VD を作成すると、作成後に表示されるデフォルトのディスクポリシーが UI ごとに異なり、矛盾しているように見えます。MegaRAID Storage Manager では「変更なし (Unchanged)」であるのに対し、StorCli では「ディスクのデフォルト (Disk's default)」となります。	なし。この場合は、「変更なし」と「ディスクのデフォルト」は同じ意味です。Cisco は disk cache policy = Disabled のドライブをサポートしているので、この場合については、「ディスクのデフォルト」と「変更なし」は同じで、ディスクのキャッシュが無効であることを示しています。	2.0(4c)
------------	--	---	---------

CSCuq35761	StorCli、MSM、CIMC ストレージ管理などの LSI アプリケーションを使用すると、オペレーティングシステムまたはファイルシステムの JBOD が「未設定の良好なドライブ」に変換することができますが、このような場合にデータ損失が発生する可能性があることを示す、意味のあるエラーメッセージは表示されません。	OS またはファイルシステムを含んでいた JBOD が「未設定の良好」に変換されると、データが失われることに注意してください。MSM および StorCli のような LSI アプリケーションは、ユーザに対し「確認してください」というメッセージを表示します。OS またはファイルシステムが含まれていた JBOD を「未設定の良好」なドライブに変換するように選択した場合は、データが失われることを理解しておく必要があります。CIMC ストレージ管理では、警告ポップアップメッセージなしで JBOD を「未設定の良好」に変換できます。ここでも、JBOD を「未設定の良好」なドライブに変換することを選択した場合は、OS またはファイルシステムが含まれていないことを確認する必要があります。	2.0(4c)
CSCus82741	RHEL の LSI SWRAID ドライバは、RAID INIT 操作が実行されると、「バッファ IO エラー (Buffer IO Error)」をメッセージファイルに出力します。	なし。	2.0(4c)

表 63: XML API

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCva77821	非インタラクティブな HUU を使用して 2.0(7e) から 2.0(13e) にアップグレードする際に、BIOS、BMC、CMC などの一部のコンポーネントがアクティブになりません。	2.0(7e) から 2.0(9l) にアップグレードし、その後 2.0(13e) にアップグレードします。	2.0(13e)

リリース 2.0(12b) の既知の動作

次に、リリース 2.0(12b) の既知の動作を示します。

表 64: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuz30387	C460 M4 サーバでは、ホストの電源がオフになっている場合、ホストのシリアルポート (PMCLI) は機能しません。	ホストの電源をオンにします。	2.0 (12b)

リリース 2.0(10e) の既知の動作

次に、リリース 2.0(10e) の既知の動作を示します。

表 65: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCuy42320	ファームウェアがレガシーファームウェアにダウングレードされている場合、または新しいファームウェアで Transport Ready が無効になっている場合は、[Transport Ready] が NVRAM でクリアされます。ただし、ファームウェアがレガシーファームウェアではない場合、または Transport Ready の実装がない場合、トランスポート対応はクリアされません。この場合、Transport Ready 対応のファームウェアが再度フラッシュされると、Transport Ready の DG が再度表示されます。その後、Transport Ready を手動でクリアする必要があります。	なし。	2.0(10b)
CSCux62038	セットアップ時に Qlogic QLE8362 カードが装着すると、サーバは BIOS (F2 メニュー) を起動できなくなります。	すべての BIOS 関連の設定は、Cisco IMC を使用して構成します。	2.0(10b)

表 66: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuy46516	シャーシに K80 が装着された Magma シャーシに接続すると、BIOS POST 中にサーバが断続的に応答しなくなります。	なし。	2.0(10b)

リリース 2.0(9d) の既知の動作

次に、リリース 2.0(9d) の既知の動作を示します。

表 67: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuu56166	C3260 サーバで、拡張または raid レベルの移行操作を実行すると、仮想ドライブ (VD) には更新されたサイズが表示されません。	次の手順を実行します。 1. 次のコマンドを実行する前に、すべての仮想マシンの電源をオフにすることによって、ディスクの使用を禁止します: ~ <code>esxcli storage core claiming unclaim ?t device ?d naa.xxx</code> 2. ファイル naa.xxx ディスクが <code>/vmfs/devices/disks</code> の下に配置されていないことを確認します。 3. 次のコマンドを使用して、ディスクを再度使用します: ~ <code>esxcli storage core adapter rescan ?A vmhbaX</code> 4. ディスクが新しいサイズで再び追加されたかどうかを確認します。	2.0(7d)

リリース 2.0(9c) の既知の動作

次に、リリース 2.0(9c) の既知の動作を示します。

表 68: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCun99348	仮想 KVM を無効にすると、[録画の再生 (Play Recording)] アクション ([トラブルシューティング (Troubleshooting)] 画面) が失敗します。	[仮想 KVM (Virtual KVM)] を [リモート プレゼンス (Remote Presence)] タブで有効にします。	2.0(1)
CSCuv08978	ハードウェアの制限により、管理ポートの MTU を設定することはできません。	なし。	1.5(4)
CSCuj36245	工場出荷時の初期状態に復元した後で、ターゲット マシンに BIOS トークンをインポートしても、値は変更されません。	BIOS post が完了してから、ターゲットマシンの電源をオンにして、インポート操作を試行します。	2.0(1)

表 69: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCun99297	ブートオプションの優先順位で、特定の USB サムドライブを選択することはできません。	特定の USB ドライブを選択するには、[ブートの選択 (boot selection)] メニューから F6 を使用します。	2.0(1)
CSCuo08591	ホストの電源がオンのときに SD カードを取り外すと、システムが POST で応答しなくなります。	- SD カードを取り外した後で、システムの電源を再投入します。 - SD カードを再度挿入します。	2.0(4c)
CSCun91835	オプション ROM の有効と無効を切り替えると、ブート順序が変わります。	なし。	2.0(1)

CSCur61234	セキュア ブート モードでは、セキュリティ違反エラーがトリガーされます。この問題は、電力特性評価が UEFI セキュア モードで有効になっている場合に、AC 電源の再投入を試行したときにも発生することがあります。	なし。	2.0(4)
------------	--	-----	--------

表 70: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCum87051	boot @ BIOS POST 画面で約 2 分間、システムのランダムなフリーズが発生し、Ctrl + R を押すと、LSI BIOS でさらに 2 分間、「バッテリ パック待機中 (Waiting for Battery Pack)」メッセージが表示されます。これは、スーパーキャパシタの学習サイクルが保留中であり、ホストが再起動された (AC/DC/再起動のいずれか) 場合にのみ発生します。これは、他のすべてのリブート/電源再投入では発生しません。	現時点では回避策はありません。	2.0(4c)

CSCuu86314	M4 サーバでは、iMR (ゼロメモリ) RAID コントローラは、最大32の仮想ドライブをサポートしますが、単一のドライブグループに仮想ドライブを作成するコマンドは、16の仮想ドライブのみを許可します。	なし。RAID コントローラは、ドライブグループ全体で 32 の仮想ドライブをサポートし、単一のドライブグループでは 16 台のドライブのみをサポートします。	2.0(6)
CSCum87232	Cisco IMC ストレージ BBU 情報は、設計容量より少ないバックエネルギー値を示します。これは、 storcli /cX /cv show all コマンドでも同じです。スーパーキャパシタが搭載された、現在出荷されている 6G SAS RAID コントローラでは、バックエネルギーは常に設計容量を上回っています。この動作のためにユーザが混乱し、スーパーキャパシタが劣化した、またはしつとすると判断して、データの整合性に懸念を抱く場合があります。	現時点では回避策はありません。これは単なる表示の問題であり、実際の機能やデータの整合性には影響しません。	2.0(4c)

CSCuw69844	2008M-8i を搭載したサーバでは、VMware ESXi 5.5 Update 1 のインストールが、インストーラのロード中に失敗します。	1. システム BIOS に移動します (F2 を押します)。 2. [PCI 構成 (PCI configuration)] > [MMCFG] を選択します。 3. 値を [自動 (Auto)] から [2 GB] に変更します。 4. 4G より上のメモリマップ IO の値を有効に変更します。 5. ファイルを保存して、システムをリブートします。	2.0(7)
------------	--	--	--------

表 71: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuw42070	MegaRAID Storage Manager は、新しい 6TB HGST ドライブを検出できず、黄色の LED が点灯します。これは、ドライブで問題が発生し、SAS リンク障害が表示された場合に発生します。	なし。	2.0(8)

CSCuw55045	ネットワーク仮想化 (NV) のデータバージョンが変更された場合、SAS Flash および MSM ユーティリティは IT ファームウェアをダウングレードできません。NV データバージョンをダウングレードするには、Host Upgrade Utility (HOU) にバンドルされている FlashOEM ツールを使用します。	SAS Flash および MSM ユーティリティを使用して、IT ファームウェアをダウングレードしないでください。これらは、HUU のみを使用する場合に使用してください。	2.0(9c)
CSCuw09414	仮想グラフィックプロセッサユニット (vGPU) を使用している仮想マシン (VM) の電源をオフにすると、VMware ESXi 6.0 では 90 ~ 120 秒かかります。	少数の VM の電源を順にオフにします。	2.0(4c)

表 72: 外部 OS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuw80507	https://access.cisco.com/solutions/21322 のナレッジベースによれば、Red Hat Enterprise Linux で IPMI コマンドを使用すると、CPU リソースが過剰に使用されます。	/etc/grub.conf: ipmi_si のカーネル行の末尾に、 ipmi_skip_bios_us= <i>ipmi_skip_bios_us=<time in microseconds></i> コマンドを追加します。	1.5(2)

リリース 2.0(8d) の既知の動作

次に、リリース 2.0(8d) の既知の動作を示します。

表 73: BMC

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCul16923	障害コード F0181 は、ラック サーバの使用中にローカルディスクが削除されたとき、CIMC によって発生します。この障害は、CIMC WebUI、CLI、および SNMP インターフェイスを介して表示されます。ただし、XML API インターフェイスを使用して同じ障害を取得することはできません。	なし。	1.5(4)
CSCuj40520	ホストアップグレードユーティリティ (HUU) を使用してファームウェアをアップグレードすると、アップグレードの進行中に一時的なストレージ障害が発生することがあります。これらの障害は無害であり、アップグレードが完了するとクリアされます。	なし。	1.5(4)

表 74: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuq23984	Cisco IMC は、flex flash 上のユーティリティ仮想ドライブ (SCU/HUU/ドライバ) の OOB 更新時に、応答しなくなります。	flex flash でユーティリティ仮想ドライブの OOB 更新を実行している間は、ホストの再起動アクションを実行しないことを推奨します。	2.0(3d)

表 75: Web 管理

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCuv63101	Cisco IMC ファームウェアを 2.0(6) から 2.0(8) にアップグレードすると、Web UI からユーザがログアウトされることがあります。これは、ブラウザの cookie がクリアされない場合に発生します。	ブラウザの cookie をクリアします。	2.0(7)
------------	---	-----------------------	--------

表 76: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCun00121	SD カードのパーティションのブートオプションを作成できません。	なし。	2.0(1)
CSCul84767	memtest.org からの memtest86 を実行している間、システムはロックアップします。この問題は、memtest.org からの memtest86 を使用した場合にのみ表示されます。	C460 M4 では、memtest.org からの memtest86 は使用しないでください。代わりに、IvyBridge EX プラットフォームをサポートしている、Pass Mark またはその他のメモリテストツールを使用してください。	2.0(4c)
CSCun02543	FC および FCOE カードの実際のブート順序にポート番号属性がありません。	なし。	2.0(1)

表 77: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCut92393	C240 M4 サーバでは、仮想ドライブを削除しようとする、まれに Cisco 12 ギガバイト SAS モジュール型 RAID コントローラでエラーが表示されることがあります。	なし。	2.0(6)
CSCuv34371	任意の RAID タイプの新しい仮想ドライブを作成する場合、書き込みキャッシュポリシーは、完全に機能している BBU またはスーパーキャパシタバッテリーであっても、デフォルトで「write through」になります。BBU が存在する場合、デフォルトの書き込みキャッシュポリシーは「良好な BBU ではライトバック (write back with good BBU)」にする必要があります。これは、12 ギガバイト SAS メザニン RAID コントローラを搭載した C240 M4 および C220 M4 サーバで発生します。	スタンドアロンモードでは、Web UI の [Ciso IMC ストレージ (Ciso IMC storage)] タブで、仮想ドライブを編集して、書き込みキャッシングポリシーを「良好な BBU ではライトバック (write back with good BBU)」に設定します。また、LSI コマンドラインオプション rom config utility を使用して設定を変更することもできます。	2.0(3d)
CSCuv36714	MegaRAID ストレージマネージャは、Windows の RAID 1 ボリュームの整合性チェックエラーを表示します。これは、整合性検査 (正常と思われる) の 20~30 分後に、ドライブにデータを書き込むと発生します。	これは既知の Microsoft による制限です。詳細については、 https://support.microsoft.com/help/2713398 を参照してください。	2.0(4c)

表 78: 外部 GPU エクスパンダ

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCuv04922	C240 M4 サーバでは、最大64Kをサポートする CPU I/O スペースの制限により、Magma シャーシ GPU エクスパンダ設定で「PCI リソース エラー(PCI Resource Error)」というメッセージが表示されます。これは、PCI スロットのすべてまたは一部が、別のサードパーティ製アダプタによって占有されている場合に発生します。		2.0(4c)
------------	---	--	---------

Nvidia Grid K1 の設定:
(1 つの Nvidia Grid K1 が C240 M4 で内部的に接続されており、2 つの Nvidia Grid K1 アダプタが Magma シャーシを介して外部で接続されている場合)

- ローカルブート:
Cisco 12 ギガバイト SAS モジュール型 RAID コントローラ (HBA スロット)、Intel I350 LOM (L スロット)、Nvidia Grid K1 (slot2)、Magma エクスパンダ HBA (スロット 5)、Teradici APEX2800 (スロット 6)、フュージョン IO ドライブ (スロット 4)
- iSCSI ブート: Intel i350 LOM (L スロット)、Nvidia Grid K1 (slot2)、Magma エクスパンダ HBA (スロット 5)、Teradici APEX2800 (スロット 6)、Fusion IO drive (スロット 4)
- SAN ブート:
CISCO VIC1227 (MLOM)、Nvidia GRID K1 (slot2)、Magma エクスパンダ HBA (スロット 5)、Teradici APEX2800 (スロット 6)、Fusion IO drive (スロット 4)

		Nvidia Grid K2 の設定: (1 つの Nvidia GridK2 が C240 M4 で内部的に 接続されており、4 つ の Nvidia Grid K2 アダ プタが Magma シャー シを介して外部に接続 されている場合) - ローカルブート: CISCO 12G SAS モジュール型 RAID コントロー ラ (HBA スロッ ト)、Intel I350 LOM (L スロッ ト)、Nvidia GRID K2 (slot2)、Magma エクспанダー HBA (スロット 5)、Teradici APEX2800 (スロッ ト 6)、Fusion IO drive (スロット 4) - iSCSI ブート: Intel i350 LOM (L ス ロット)、Nvidia Grid K2 (slot2)、 Magma エクスパ ンダー HBA (スロッ ト 5)、Teradici APEX2800 (スロッ ト 6)、Fusion IO drive (スロット 4) - SAN ブート: CISCO 1227 SAN (MLOM)、Nvidia Grid K2 (slot2)、 Magma エクスパ ンダー HBA (スロッ ト 5)、Teradici APEX2800 (スロッ ト 6)、Fusion IO drive (スロット 4)	
--	--	---	--

リリース 2.0(7d) の既知の動作

次に、リリース 2.0(7d) の既知の動作を示します。

表 79: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuv34476	3260 サーバでは、KVM の起動に失敗し、「アプリケーションを起動できません (Unable to Launch the application)」というメッセージが表示されます。これは、CMC を交換または変更して、それをアクティブまたはマスターにすることで発生します。	Web UI または CLI を使用して証明書を再生成し、CMC を再起動します。	2.0(7d)
CSCuv28734	3260サーバでは、ダウンロードで Chrome 43 バージョンのブラウザを使用すると、ネットワークエラーでブートまたはダウンロードファイルの破損による失敗が起きます。	他のブラウザを使用するか、Chrome バージョン 42 を使用します。	2.0(7d)
CSCuu50850	3260 サーバでは、BMC を工場出荷時のデフォルトにリセットすると、BMC へ IPMI セッションを確立することができなくなります。	アクティブな CMC を使用してユーザを再設定します。	2.0(7d)

CSCur77980	3260サーバでは、CMCを工場出荷時のデフォルトにリセットすると、ユーザを設定することができなくなります。この問題は、リセット後に別のインデックス番号を使用してユーザを設定しようとした場合に発生します。	ユーザを設定するには、リセット前に使用したのと同じインデックス番号を使用します。	2.0(7d)
CSCuu43406	3260サーバでは、GUIを数分間アイドル状態にすると、サーバが応答しなくなり、エラーメッセージが表示されます。これは、Chromeバージョン41を使用すると発生します。	他のブラウザを使用するか、Chromeバージョン 42 を使用します。	2.0(7d)
CSCuu43330	3260サーバでは、ログイン画面が数分間アイドル状態になると、Web UI にログインできなくなります。これは、Chromeバージョン41を使用すると発生します。	他のブラウザを使用するか、Chromeバージョン 42 を使用します。	2.0(7d)

CSCur60690	3260サーバでは、CLI または Web UI を使用してユーザを設定すると、次のメッセージが表示されることがあります。「エラー: 同じ名前 <ユーザ名> のユーザが既に存在します (Error: user with same name <username> exists)」BMC のローカルユーザで IPMI を使用してユーザを設定した場合、データベースがアクティブ CMC と同期しないことがあります。したがって、同じユーザがアクティブ CMC 上で別のインデックスで設定されている場合、このエラーが発生します。	IPMI を使用して BMC のローカルユーザデータベースのユーザインデックス番号を確認し、同じインデックス番号を使用して、アクティブ CMC の CLI または Web UI を使用してユーザを設定します。	2.0(7d)
------------	--	--	---------

表 80: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCuu36101	3260 サーバで、MegaRAID カードに最大許容数の仮想ドライブが作成されている場合、カードはRAID レベルの移行をサポートしません。 (注) 注: これは、RLM 操作を実行するために一時またはゴースト VD が必要な、MegaRAID ソフトウェア スタックの制限です。	仮想ドライブを許容される最大数まで作成することは避けてください。	2.0(7d)
------------	---	----------------------------------	---------

リリース 2.0(6d) の既知の動作

次に、リリース 2.0(6d) の既知の動作を示します。

表 81: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCui64842	Broadcom 57810 アダプタのハードウェア構成設定は、ファームウェアの更新後にリセットされます。この問題は、すべての57810アダプタで発生します。次の設定がリセットされます。 • DCB プロトコル • SRIOV • PF あたりの VF 数	BIOS 設定を再設定します。	1.5(3)

CSCuu35160	LSI ファームウェアをダウングレードまたはアップグレードする際、Cisco IMC ログはいくつかの CMD over OOB エラーを報告します。これは予期された動作であり、ファームウェアの更新中に、コントローラがアウトオブバンドで短時間応答しないことが原因でエラーメッセージが発生します。	なし。	2.0(3e)
CSCuu36101	MegaRAID カードは、カードに最大許容数の仮想ドライブが作成されている場合、RAID レベルの移行をサポートしません。 (注) これは、RLM 操作を実行するために一時またはゴースト VD が必要な MegaRAID ソフトウェア スタックの制限です。	仮想ドライブを許容される最大数までは作成しないでください。	2.0(6d)

表 82: VIC

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCuu56903	VIC 1225 で同じアップリンクを持つ VNIC では VM 間のデータトラフィックをアップストリームに切り替えることができませんでした。	vnic0、vnic1 をピン状態で Uplink-1 に、vnic6、vnic7 を Uplink-2 に割り当てます。 1. これは、物理的なアップリンクの冗長性に影響を与える可能性があることに注意してください。	2.0(3e)
------------	---	---	---------

リリース 2.0(4c) の既知の動作

次に、リリース 2.0(4c) の既知の動作を示します。

表 83: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCut76388	C220 M4 および C240 M4 サーバの場合、電力制限が有効になっており、電力制限値が許容範囲内の低い値に設定されている場合、1400W PSU の電力消費が変動します。	より高い電力上限値を設定します。たとえば、許容された電力制限の範囲が 350W ~ 650 W の場合は、500W より大きい値を設定します。	2.0(4c)
CSCuq39610	SD カードの設定中に、次のエラーが表示されます: ERROR_METADATA_EXISTS	SD カードを取り外して挿入し、再設定します。エラーが解決しない場合は、カードを交換します。	2.0(3d)

表 84: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCur74413	2.0(3d) と 2.0(3f) バージョンの間で BIOS ファームウェアのアップグレードまたはダウングレードを行うと、ウォッチドッグ タイマー ポリシーの値が変更されます。	BIOS ファームウェアのアップグレードまたはダウングレード後に値をリセットします。	2.0(3d)
CSCut05524	何回かリブートを行うと、TxT が無効になります。	BIOS で TPM Clear コマンドを使用してカウンタをリセットしてからやり直します。	2.0(3e)

表 85: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCus54600	LSI9271-8i では、UCSM でストレージコントローラ非動作? (Storage Controller Inoperable?) の障害が報告されます (イベントログには PMU 障害が存在 (PMU Fault present) と記録されます)。	LSI9271-8i アダプタを交換します。	2.0(3i)
CSCus68862	Ubuntu (現在使用可能なすべてのバージョン) には、IT ベースのアダプタのインボックスドライバがありません。	なし	2.0(3d)

表 86: VIC

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCut78400	CLI コマンドの <code>adapter-reset-defaults</code> を使用して VIC アダプタをデフォルト設定にリセットすると、デフォルトの MAC アドレスが変わる場合があります。それで、デフォルトの MAC アドレスの変更を補正するために DHCP と OS の設定が必要になる場合があります。これは、リリース 2.0(4)以降で、VIC に関連した特定の問題に対応するため、デフォルトの MAC アドレス範囲を移動したことによります。	なし。	2.0(4c)
------------	---	-----	---------

表 87: 外部 OS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuq75761	Red Hat Enterprise Linux 7 のインストール時に、マッピングされた SAN LUN が表示されません。Red Hat Enterprise Linux 7 OS がローカルストレージにインストールされ、SAN LUN がマッピングされている場合、サーバではカーネルパニックが発生します。	回避策はありません。この問題に対処するためにのドライバ更新ディスクが後ほど使用可能になるかもしれません。	2.0.2c

表 88: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース

CSCuq43129	OL 5.9 および OL 5.10 オペレーティングシステムは、インストール中に QLE2672 SAN LUN を認識しません。	なし。	2.0(3d)
------------	--	-----	---------

CSCuq60947	Citrix XenCenter 6.2 が設定された VM インスタンスは、ドライバが渡されて、vGPU の関連付けが解除されると起動できません。	次の手順に従って、VM インスタンスから vGPU の関連付けを解除します。 1. VM コンソールから、[スタート (Start)] > [コントロール パネル (Control Panel)] > [ハードウェアとサウンド (Hardware and Sound)] > [デバイス マネージャ (Device Manager)] > [ディスプレイ アダプタ (Display Adapters)] > [Nvidia K1 または K2 (Nvidia K1 or K2)] を選択します。 2. 右クリックして、[アンインストール (Uninstall)] を選択します。 3. XenCenter コンソールで VM をオフにします。 4. eXenCenter console で、VM のプロパティを開きます。 5. 左側の列で GPU を右クリックし、[GPU タイプ: (GPU type:)] > [なし (None)] を選択します。 6. VM を起動します。	2.0(3d)
------------	--	--	---------

リリース 2.0(3d) の既知の動作

次に、リリース 2.0(3d) の既知の動作を示します。

表 89: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCuq99268	ESXi 5.5 以降のアップデートでは、ネイティブのインボックス ドライバ (lsi-msgpt3) を使用して、Cisco 9300 HBA の背後にあるディスクに OS をインストールできます。ただし、lsi_msgpt3 は完全にはサポートされていません。そのため、これを無効にして、非同期ドライバをインストールする必要があります。		2.0(3d)
------------	--	--	---------

		OS をインストールした後、次の手順を実行して mpt3sas ドライバをインストールします。 1. #esxcli software vib install -v <code>{FULL_PATH_TO_YOUR_VIB(.xxx.vib)}</code> 2. 次のコマンドを使用して、lsi-msgpt3 (ネイティブ ドライバ) を無効にします: #esxcli module ?d lsi-msgpt3 3. システムが再起動されると、通常、mpt3sas ドライバが引き継ぐはずですが、次のコマンドを使用して、この点を確認します。 ~# esxcli storage core adapter list: HBA Name Driver Link State UID Description ----- ----- ----- vmhba0 ahci link-n/a sata.vmhba0 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba1 mpt3sas link-n/a sas.xxxxxxxx LSI / Symbios Logic SAS3008 PCI-Express .. vmhba32 ahci link-n/a sata.vmhba32 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba33 ahci link-n/a sata.vmhba33 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba34 ahci link-n/a sata.vmhba34 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba35 ahci link-n/a sata.vmhba35 Intel Corporation Patsburg 6 Port SATA AHCI .. vmhba36 ahci link-n/a sata.vmhba36 Intel Corporation Patsburg 6 Port SATA AHCI .. 4. 上記のコマンドの結果、ドライバ
--	--	---

		名としてまだ lsi-msgpt3 と表示された場合は、次のコマンドを使用して (無効化する代わりに) lsi msgpt3 を削除してください: <pre>#esxcli software vib remove ?n lsi-msgpt3</pre> 5. システムを再起動する。	
CSCup89033	[パワー モニタリング (Power Monitoring)] ページの読み込み中に他のページに移動すると、すべてのページの上部に [パワー モニタリング (Power Monitoring)] グラフが表示されます。	[Power Monitoring] ページに戻って、ページの読み込みが終わってから、他のページに移動してください。	2.0(3d)
CSCuq00837	C220 M4 および C240 M4 サーバでは、ESXi 5.1 U2 パッチ05をインストールし、TPM と TXT を有効にしてアクティブにすると、TPM の初期化が失敗します。	回避策はありません。	2.0(3d)
CSCuq04009	ESXi インストーラは、xHCI モードの SD カードを検出しません。	BIOS で USB xHCI モードを無効にしてください。	2.0(3d)
CSCuo28585	エクспанダが2つのポートを介してコントローラに接続されている場合、[HII ドライブ管理 (HII Drive Management)] および [エンクロージャ管理 (Enclosure Management)] メニューには、1つのポート/接続 (0 ~ 3) のみが表示され、他方 (4 ~ 7) は表示されません。	回避策はありません。	2.0(3d)

CSCuq14862	SLES 11 SP3 のインボックス IGB ドライバを使用すると、2.0(3d) のドライバ ISO(5.2.5) から Intel i350 LOM をインストールした後、ethtool は、Intel i350 LOM に対して間違ったファームウェアバージョンを表示します。	igb バージョンを 5.2.5 にアップデートします。Igb をアンロードしてロードしてください。	2.0(3d)
CSCuq24196	Windows Server 2012 を iSCSILUN にインストールすると、いくつかのネットワーク アダプタで、次のような説明とともに、デバイス マネージャに黄色の感嘆符が表示されます (コード 10)。「このデバイスは、このデバイスに必要なドライバを読み込めないため正常に作動していません」。このことは、iSCSI ブートに使用される NIC でのみ生じます。	次のいずれかを実行します。Windows 8 および Windows Server 2012 ではホットフィックスを使用できます。Windows OS イメージでこの修正プログラムを実行してから、iSCSI インストールを実行します。修正の詳細については、 http://support.microsoft.com/kb/2822241 を参照するか、次の手順を実行してください。 : 1. デバイスは削除せず、黄色の感嘆符が表示されているデバイスのドライバをアンインストールします。 2. ドライバを再インストールします。 3. サーバを再起動します。	2.0(3d)
CSCup82749	インボックス ドライバを使用してインストールした場合、Intel i350 および Pinecrest アダプタを使用して Windows 2K12 R2 iSCSI ブートを行うと、BSOD が表示されます。	W2K12 R2 iSCSI のインストール時に、ドライバ ISO での Intel ドライバのインストールをスキップします。インストールが完了したら、サーバを再起動します。	2.0(3d)
CSCuq92331	nvqual のような総合的ベンチマークの実行中に、帯域幅テストが失敗します。これは、プロセッサの電源管理が有効になっている場合に発生します。	BIOS セットアップを使用して、プロセッサの電源管理オプションを無効にします。	2.0(3e)

CSCuo05774	ブートモードをUEFIまたはレガシーに設定するには、変更を反映するために2回リブートする必要があります。	サーバを2回リブートします。	2.0(3e)
CSCul04884	サービス プロファイルに設定されているブートデバイスが見つからない場合、サーバはBIOSセッアップメニューに入ります。これは、CシリーズサーバがCisco UCS Managerによって管理されている場合にのみ、影響します。	なし。	2.0(3e)
CSCuj28644	ブートモードがUEFIに設定されている場合、UEFI PXE ブートまたはUEFI iSCSI ブートは機能しません。	PXE または iSCSI ブートを使用する場合は、レガシーブートモードを使用します。	2.0(3e)

表 90: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuo26946	リリース 1.5(x) から 2.0(x) にアップグレードするか、または 2.0(x) から 1.5(x) にダウングレードする場合、またはレガシーから高精度ブート順序に移行する場合、さらにSDカードに4つのパーティションがある場合、SDカードのBIOSブート順序の不一致が発生します。	回避策はありません。ブート順序を再設定する必要があります。	2.0(3d)

リリース 2.0(1b) の既知の動作

CSCuq32910	サーバが 2.0.3d リリースファームウェアを使用して起動すると、HUU ファームウェアバージョンのアップデートに失敗し、Emulex OCe14102/Oce11102 の現在のバージョンを Not と表示します。	サーバをリブートします。	2.0(3d)
------------	--	--------------	---------

表 91: 外部コントローラ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCup87719	工場出荷時のデフォルト設定の i350 アダプタは、最初のポートに対してのみブートプロトコル オプション ROM をディスパッチします。i350 カードの残りの 3 つのポートのオプション ROM はディスパッチされません。	Boot Util を使用して、必要なポートのブートオプションを有効にします。	2.0(3d)

リリース 2.0(1b) の既知の動作

次に、リリース 2.0(1b) の既知の動作を示します。

表 92: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCup49368	バージョン1.5.7 から 2.x にアップグレードする場合、 Cisco Host Upgrade Utility を使用して [すべて更新 (Update All)] をクリックしても、シャーシファームウェアは更新されません。		2.0 (1b)
------------	---	--	----------

		Web UI を使用して シャーシファームウェアをアップグレードするには、次の手順を実行します。 1. [Navigation] ペインの [Server] タブをクリックします。 2. [Server] タブの [Summary] をクリックします。 3. [Actions] 領域で、[Power Off Server] をクリックします。 4. [OK] をクリックすると、サーバの電源が切れ、システムファームウェアが更新されます。 CLI を使用してシャーシファームウェアをアップグレードするには、次の手順を実行します。 1. Server# scope chassis 2. Server /chassis # scope firmware 3. Server /chassis/firmware # show detail: Firmware update required on some components, please run update-all (under chassis/firmware scope) .
--	--	--

		4. Server /chassis/firmware # update-all	
CSCup58906	2.0(1a)にダウングレードすると、Cisco IMC Web UI に警告メッセージとクリティカルイベントが表示されます。	サーバに A/C 電源を再投入します。	2.0 (1b)

リリース 2.0(1) の既知の動作

次に、リリース 2.0(1) の既知の動作を示します。

表 93: Cisco IMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCth84883	LED 状態がオフに設定されていても、LED センサーの色が赤、オレンジ、青（またはサポートされている色）になります。	LED 状態をオフに設定した場合は、LED の色を無視してください。	2.0(1)
CSCtt08424	Cisco IMC の電力制限は VMware ESXi 5.0 ではサポートされていません。	Cisco IMC を 1.4(2) にアップグレードすると、Cisco IMC は自動的に電力制限を無効にします。電力制限を使用するには、手動で再度有効にする必要があります。	2.0(1)
CSCun97225	リリース 2.0(1a) から 1.5(x) リリースにダウングレードすると、12 のフィルタではなく、7つのプラットフォーム イベント フィルタのみが表示されます。	工場出荷時のデフォルト設定を復元するか、 <code>ipmitool raw 0x36 0X03 0xAA</code> で Cisco OEM ファンクションコマンドを実行します。	2.0(1)

CSCuo40835	リリース 2.0(1a) から 1.5(x) リリースにダウングレードする際、SNMP ポート値をデフォルト値 (161) 以外に設定していると、この数値はリセットできません。	ダウングレードする前に、SNMP ポートを 161 に設定するか、工場出荷時のデフォルトに戻すようにします。	2.0(1)
CSCun10320	Cisco IMC ファームウェアのバージョンを、FTP を使用して 1.5(3d) から 2.0(1a) にアップグレードすることはできません。	ブラウザまたは SCP クライアントによるアップグレードを使用してください。	2.0(1)
CSCum70086	Windows OS で、ダウンロードした DVR プレーヤーは、Java バージョン 6 以前ではオフライン再生ができません。	正しい Java バージョンで script_win bat ファイルを編集して更新します。	2.0(1)
CSCun66062	CLI を使用して高精度ブート順序を定義しているときに、複数のデバイスの順序を個々のデバイスのスコープによって変更した場合、デバイスの最終順序が変更されたとおりに表示されないことがあります。	複数のデバイスのブート順序を設定するには、 rearrange-boot-device コマンドを使用します。または、Cisco IMC Web UI を使用します。	2.0(1)
CSCum26002	DDNS 更新がトリガーされる前に、DNS サーバへの接続を確認するための ping を実行すると、遅延が発生します。	このリリースで使用可能な ping オプションを使用すれば、IPv4 と IPv6 の両方のアドレスについて、優先 DNS サーバと代替 DNS サーバへの接続を手動で確認できます。	2.0(1)
CSCun11979	Cisco IMC Web UI を使用してレガシーブート順序を設定することはできません。	CLI または XML API を使用します。	2.0(1)

CSCuo71634	Cisco IMC ファームウェアをアップグレードしてセキュアブートモードを有効化した後、すぐに Cisco IMC をリブートしようとしても、応答しません。	アップグレード後、約 10 分後に Cisco IMC を再起動します。	2.0(1)
------------	---	--------------------------------------	--------

リリース 1.5.7 の既知の動作

次に、リリース 1.5(7) の既知の動作を示します。

表 94: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCul62033	SD カードで大量の I/O トランザクションがあると、CIMC に読み取りエラーが表示されることがあります。	Cisco FlexFlash 3.0 カードの使用	1.5(7)
CSCua94308	クローズドループサーマルスロットリング (CLTT) の CIMC 通知は発生しません。CLTT は、DIMM の温度が UC (高温側重大) 温度を超えたときに自動的に発生します。	なし。	1.5(7)
CSCuo18891	UCScfg_X64、入力ファイルが Unicode 形式の場合は、「エラー: 引数の数が不正 (Error: Invalid Number of Arguments)」というエラーメッセージが表示されます。	ANSI 形式の入力ファイルを使用します。(	1.5(7)

CSCud84978	SELにはメモリエントリがありますが、障害ページにはエントリが表示されません。Cisco UCSM障害コードは、これらのSELでは使用できません。	なし。SELは、メモリ関連のイベントをデコードするために使用する必要があります。	1.5(1)
------------	---	--	--------

表 95: OS

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCun77988	ESXi を UEFI モードでインストールすると、OS の起動に失敗します。インストールは完了しますが、その後のリブートでは、サーバは ESXi OS を起動しません。		1.5(7)
------------	---	--	--------

この問題を解決するには、次の手順を実行します。

1. シェルを起動します。
2. Fsxx を特定します (xx は ESX がインストールされている場所で、通常は 0、つまり fs0: になります)。これは、fsxx:\EFIBoot\BOOTX64.EFI コマンドを実行して、確認できます。
3. 現在の EFI ブートオプションのリストを取得するには、**bcfg boot dump** コマンドを使用します。

(注) 後ほど使用するために、最後のブート番号を保存します。

4. LAST_BOOT_NO + 1 の位置に新しいブートオプションを追加するには、次のコマンドを使用します。引用符で囲まれた最後のパラメータには、この新しいブートオプションの説明を指定でき

		ます。この説明は、BIOS F6 メニューで表示されるものです。 - <pre>bcfg boot add LAST_BOOT_NO + 1 bcfg boot add LAST_BOOT_NO + 1 "UEFI: ESXi"</pre> 5. bcfg boot mv LAST_BOOT_NO + 41 コマンドを使用して、ESX用に新しく作成したブートオプションが先頭に来るようにします。 シェルで reset コマンドを発行して、プラットフォームをリセットします。BIOS が起動しているときに F6 を押して、BIOS ブート選択メニューを表示します。新しく作成されたブートオプションが表示されていることを確認します。これを選択して、ESX を起動します。	
--	--	--	--

表 96: NVIDIA

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuo39368	1 TB 以上のメモリを超えるシステムでは、NVIDIA の GPU カードが機能しないか、動作が不安定になります。	これは、GPU での 40 ビットアドレッシングが原因で生じる、NVIDIA の GPU の制限です。GPU を機能させるには、メモリを 1 TB 以下にする必要があります。	1.5(7)

表 97: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCue88244	ハードドライブの取り外しの準備をすると、実際には取り外す準備ができますが、HDDのLEDがオレンジ色に点滅しないため、ドライブの交換準備ができていないことがわかりません。これは、直接接続のC260 M3設定でのみ発生します。	なし。	1.5(4)

CSCui29979	BBU 充電ステータスには、常に充電中または放電中のいずれかが表示されます。充電中または放電中であると示されるために、バッテリーが最適な状態ではないとの誤解を招く可能性があります。	バッテリーが最適な状態であるかどうかを判断するには、BBU ステータスフィールドを使用する必要があります。BBU のステータスが最適な場合は、バッテリーが良好であることを示します。BBU の状態によってバッテリーの交換が必要であることが示されている場合は、BBU が不良であるため、交換する必要があります。充電ステータスは設計どおりに動作しており、常に充電中または放電中と示します。これは、ファームウェアがバッテリーの充電をチェックし、充電が帯域のギャップを下回っていないことを保証するためです。この場合、バッテリーは下限に達したときに充電され、帯域の上限に達すると充電が停止します。リーク電流があると、バッテリーが放電し、下限しきい値に戻ることがあります。この場合、ファームウェアは充電を開始します。	1.5(2)
------------	--	---	--------

リリース 1.5(4) での既知の動作

次に、リリース 1.5 (4) での既知の動作を示します。

表 98: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCul36732	Cisco UCS Manager によって管理される C シリーズ サーバでは、Emulex アダプタを使用した SAN ブートは失敗する可能性があります。この動作は、Cisco UCS Manager によって管理されているサーバでのみ発生します。	BIOS post 中に、ホットキーを押して Emulex オプション ROM 設定画面に入り、「EDD」を有効にし、保存して終了します。	1.5(4)
CSCub21433	UEFIOS のインストールは、ソフトウェア RAID (オンボード SCU コントローラ) ではサポートされていません。	なし。ソフトウェア RAID を使用する場合は、レガシーモード OS インストールを使用してください。	1.5(4)
CSCtz11862	システムをオンにしたときに、連続的な BEEP 音が鳴ります。	CIMC とホストを同時にオンにしないでください。電源装置をオンにした 3 分後に、ホストをオンにします。	1.5(4)

表 99: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuj89681	SD カードをシングルパーティションモードに移行した後、1.5(4x) より前のリリースにダウングレードすると、4 つのパーティションすべてが WebUI/CLI に表示されます。	なし。	1.5(4)

CSCuj84718	SD カードのパーティションのサイズは、ダウングレード中に SCU、HUU、およびドライバのごみ箱の値として表示されます。	リリース 1.5(4x) にアップグレードし、単一のパーティションを作成してから、以前のリリースにダウングレードしてください。パーティションのサイズは 2097151 MB として表示されます。	1.5(4)
CSCuj67995	ポートパラメータを使用して複数の設定を変更しても、CIMC 設定のみからだ失敗します。	次の手順を実行します。 1. モードを[専用 (Dedicated)]に設定し、冗長性を[なし (None)]に設定します。 2. 変更をシステムに保存します。 3. 自動ネゴシエーションフィールドを[[はい (Yes)]]に設定します。	1.5(4)
CSCuj52943	4 パーティション設定から単一パーティションへの移行では、設定の詳細のみが変更されます。SD のデータはそのまま残ります。したがって、単一パーティション (HV) に移行すると、設定の移行中に SCU に有効なファイルシステムがある場合に限り、HV パーティションは SCU データを保持します。	単一パーティション (HV) 設定に移行した後、HV パーティションをフォーマットして必要な OS をインストールします。	1.5(4)

CSCul50285	<pre>ucs-c220-m3# scope bios/advanced ucs-c220-m3 /bios/advanced # ucs-c220-m3 /bios/advanced # set ConsoleRedir COM_0 ucs-c220-m3 /bios/advanced *# set BaudRate 115200 ucs-c220-m3 /bios/advanced *# set FlowCtrl None ucs-c220-m3 /bios/advanced *# set TerminalType VT100+ ucs-c220-m3 /bios/advanced *# commit ucs-c220-m3 /bios/advanced #</pre>	次のプロセスを使用します。 <pre>ucs-c220-m3# scope bios ucs-c220-m3 /bios #scope advanced ucs-c220-m3 /bios/advanced # set ConsoleRedir COM_0 ucs-c220-m3 /bios/advanced # commit</pre> BIOS セットアップのパラメータを変更すると、再起動が必要になります。 Do you want to reboot the system?[y N] (システムをリブートしますか)	1.5(4)
CSCue10121	PWRGD センサーの通常のイベントは、CIMC ブートおよびホスト ブート時に SEL に記録されます。	これらは予想されるイベントであり、無視することができます。	1.5(4)
CSCuj41445	いくつかのフィールドでは自動補完が行われます。	1.5(x) ビルドにアップグレードします。	1.5(4)

CSCud17092	CIMC のアップグレード後の最初のログイン時に、メインページの Web UI にエラー ダイアログボックス 「Error: 予期しないエラー」が表示されることがあります。ストレージデータも空白または無効になることがあります。CIMC のアップグレードの直後、ログインしただけで発生することがあります。これは、1.4x から 1.5 へのアップグレードに関連している可能性があります。	ログアウトしてから再度ログインすると修正されますが、おそらく時間がかかります。それで、数分待ってから WebUI を更新してください。問題が解決される場合があります。	1.5(4)
------------	--	--	--------

表 100: Cisco usNIC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCul56178	CIMC は、設定可能な vNIC と usNIC を 229 に制限します。	なし。残りの vNIC は、内部アダプタの使用のために予約されています。これらの残りの vNIC のうち 4 つは必須で、そのうちの 2 つが eNIC、2 つが fNIC です。16 の vNIC (2 つの必須 eNIC を含む) を設定すると、残りは $229 - 2 (\text{fNIC}) - 16 (\text{eNIC}) = 211$ usNIC になります。	1.5(4)

表 101: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCuj83316	バッテリーには、手動 (ユーザが開始する) 再学習サイクルが必要で、性能は徐々に低下します。1 年以上使用したバッテリーでは、残っているキャパシティを正確に測定する必要があります。	手動 (ディープ サイクル) 再学習は、ユーザが開始する必要があります。これは、MegaCLI ユーティリティまたはサーバ CIMC の [ストレージ (Storage)] タブで実行できます。再学習は完了するまでに数時間、最大で 1 日かかる場合があります。バッテリーは再学習の完了後も十分なキャパシティを備えていますが、再学習の前に設定しておけば、最適な状態になり、VD は書き戻しモードになります。	1.5(4)
------------	--	--	--------

表 102: Web 管理

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCtx16030	WebUI の DIMM のメモリ インベントリの [動作 (Operability)] フィールドに、障害が発生した DIMM が正しく表示されません。	この問題は、WebUI によって報告されたメモリ インベントリでのみ発生します。BIOS セットアップでは、DIMM のステータスは正しく報告されます。したがって、WebUI に DIMM が動作不能であると示された場合は、BIOS セットアップの [Advanced] > [Memory Configuration] ページで、メモリアイザーのすべての DIMM のステータスをチェックしてください。	1.5(4)

リリース 1.5(3) の既知の動作

次に、リリース 1.5(3) の既知の動作を示します。

表 103: ファームウェアのアップグレード

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCui82263	リリースバージョン 1.5(3) から 1.5(1) リリースバージョンにダウングレードしても、ホストアップグレードユーティリティではエラーはスローされません。	これは問題ではありません。エラーは報告されませんが、更新は続行されません。	1.5(3)

リリース 1.5(2) の既知の動作

次に、リリース 1.5(2) の既知の動作を示します。

表 104: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuf52723	ファームウェアを 1.5 (1B) にアップグレードした後、C240M3 の電源が入らなくなります。HUU を使用してファームウェア 1.4(6c) から 1.5(1b) へのアップグレードを試みた場合、正常に完了したとして報告されても、実際にはこの CIMC は 1.5(1b) にアップグレードされていません。	CIMC および BIOS 更新を手動で強制して修正します。	1.5(2)
CSCug78887	ベース識別名 (base-dn) パラメータの構文は、新しい LDAP の実装では変わっています。	次の構文を使用します: /ldap # set base-dn DC=Scom, DC=msdn, DC=com 次は古い構文です: /ldap # set base-dn Scom.msdn.com	1.5(2)

CSCuh71550	Windows Active Directory で簡略化されたドメイン名を使用すると、子ドメインのユーザ ログインに失敗します。	完全修飾ログイン名を入力します。	1.5(2)
CSCuh39061	Intel VTD および ATS では、usNIC の BIOS 設定が必要です。ただし、usNIC を設定していて、これらのパラメータが有効になっていない場合でも、CIMC に警告メッセージは表示されません。	usNIC を設定する場合は、Intel VTD と ATS が BIOS 設定で有効になっていることを確認してください。	1.5(2)
CSCuf08450	C24 M3 を 1.4.7.a から 1.4.7.f へ HUU を使用してアップグレードすると (すべてアップグレードのオプション)、サーバのファンが 1.4.7.a での 2 倍の速度で動作します。	なし	1.5(2)
CSCug65160	場合によっては、VIC の再起動または CIMC の再起動後に、SFP + 銅ケーブルの VIC リンクがダウンすることがあります。シリアル番号が MOC1238 ~ MOC1309 で始まるケーブルは影響を受ける可能性があります。	シャーシの AC 電源を再投入して、回復します。	1.5(2)
CSCtx43305	PSU ファームウェアのリビジョンは、PSU に AC 電力が供給されていない場合、一部しか取得できません。	PSU に AC 電源を接続します。完全なファームウェア リビジョンが使用可能になります。	1.5(2)

表 105: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCue10144	Cisco C22x または C24x サーバを起動すると、LSI オプション ROM をロードするときに RAID レベルが表示されます。ただし、サポートされているすべての RAID レベルが表示されるわけではありません。	これは、複数の 9240 コントローラを区別するための動作です。これらの一部は RAID5 をサポートしていますが、一部はサポートしていません。同じ 9240 名の 2 つの製品があります。ただし、[名前 (name)] フィールドには、サポートされるすべての RAID レベルを一覧表示するだけの十分なスペースがありません。そのため、RAID レベルは部分的なリストのみ表示されます。	1.5(2)
CSCug95648	BBU の充電ステータスは常に充電中として表示され、充電の割合は 100% に到達しません。常に 67% と表示されます。	これは、ファームウェアの新しい変更です。バッテリーの再学習サイクルが正常に完了すると、バッテリーは 67% まで再度充電されます。これはバンドギャップ内にあり、LSI ファームウェアによる充電は停止し、バッテリーの状態は最適であると宣言されます。これは、データを最大 48 時間保持するために必要な充電レベルです。いくらかの漏れ電流があり、その分をゆっくりと充電するので、バッテリーは常に充電状態で、充電ステータスには「充電」と表示されます。	1.5(2)

CSCuh82265	BBUステータスが放電中として表示され、充電率は 64% で停止します。サーバはバッテリー交換アラートを出します。サーバでバッテリーが放電中であると表示されます。また、「ステータス: 学習サイクルが必要ですか (Status: Learning Cycle Needed?)」という重要度中のアラートが発生します。	なし	1.5(2)
CSCud13257	64ビットの MSM 12.08.03.03 を使用すると、ハングが発生します。	MSM の 32 ビットバージョンを使用します。	1.5(2)

表 106: ホストアップグレードユーティリティ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCui09482	特定のサーバの HUU から Emulex LPe16002 のファームウェア更新を行うと、失敗します。	Emulex LPe16002 のファームウェアレベルは、すでに、HUU がターゲットとしているのと同じレベルになっています。したがって、実質的に更新は必要ありません。または、カードを別のサーバに移動してから、更新を試してください。	1.5(2)

表 107: SNMP

不具合 ID	症状	回避策	最初に影響を受けるリリース
--------	----	-----	---------------

CSCug37639		なし。	1.5(2)
------------	--	-----	--------

複数の MIB で MIB ウォークを実行すると、最後に「この MIB ビューには残りの変数はありません(MIB ツリーの最後を超えています)(No more variables left in this MIB View (It is past the end of the MIB tree))」というエラーが表示されます。失敗した MIB は、snmpVacmMIB です。

正常な出力の例:

```
[root@pebbles-iptv mibs]#
snmpwalk -v2c -c public
localhost
notificationLogMIB
NOTIFICATION-LOG-
MIB::nlmConfigGlobalAgeOut.0
= Gauge32: 1440 minutes
NOTIFICATION-LOG-
MIB::nlmStatsGlobalNotificationsLogged.0
= Counter32: 33
notifications
NOTIFICATION-LOG-
MIB::nlmStatsGlobalNotificationsBumped.0
= Counter32: 33
notifications
[root@pebbles-iptv mibs]#
**
```

MIB は正常に終了しており、エラーがないことに注意してください。

** 問題のある出力の例:

```
[snmp@sv-repo ~]$ snmpwalk
-t 120 -v3 -u glasco -l
AuthPriv -a MD5 -A
enuf4me2do -x DES -X
tqbFjotlCow 14.17.2.45
.1.3.6.1.6.3.16.1.5.2.1.6
SNMP-VIEW-BASED-ACM-MIB::varViewTreeFamilyStatus."all".1.1
= INTEGER: active(1)
SNMP-VIEW-BASED-
ACM-MIB::varViewTreeFamilyStatus."all".1.0
= INTEGER: active(1)
SNMP-VIEW-BASED-ACM-
MIB::varViewTreeFamilyStatus."all".1.1
= INTEGER: active(1)
```

	<pre> SNMP-VIEW-BASED-ACM- MIB::vacViewTreeFamilyStatus."_all_".1.2 = INTEGER: active(1) SNMP-VIEW-BASED-ACM- MIB::vacViewTreeFamilyStatus."_none_".1.0 = INTEGER: active(1) SNMP-VIEW-BASED-ACM- MIB::vacViewTreeFamilyStatus."_none_".1.1 = INTEGER: active(1) SNMP-VIEW-BASED-ACM- MIB::vacViewTreeFamilyStatus."_none_".1.2 = INTEGER: active(1) SNMP-VIEW-BASED-ACM- MIB::vacViewTreeFamilyStatus."_none_".1.2 = No more variables left in this MIB View (It is past the end of the MIB tree) [snmp@sv-repo ~]\$ </pre> まだウォークの対象である mib が残っているのに、「この MIB ビューにはこれ以上変数は残っていません (No more variables left in this MIB View)」と出力されます。確認された最後の oid は 1.3.6.1.6.3.16.1.5.2.1.6 であり、get-response パケットの error-status 内で noSuchName(2) が出ています。これは noError(0) となるはずのものです。		
--	--	--	--

表 108: Web 管理

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuc19323	Windows 2008 および IE 8.0 CIMC WEB UI で、ログインプロンプトが表示されないことがあります。	IE 8.0 の信頼済みサイトのリストに CIMC の IP を追加します。 Internet Explorer のブラウザ ウィンドウで、 [ツール] -> [インターネット オプション] -> [セキュリティ] -> [信頼済みサイト] -> [サイト] -> [追加] を選択します。	1.4(7)

CSCuh76949	[例外を追加 (Add Exception)] をクリックすると、[証明書は有効です (certificate is valid)] というウィンドウが表示されますが、[セキュリティ例外の確認 (Confirm Security Exception)] ボタンはグレー表示されます。	キャッシュをクリアするか、問題が解決されるまで複数回更新します。	1.5(2)
------------	---	----------------------------------	--------

リリース 1.5(1f) の既知の動作

次に、リリース 1.5(1f) の既知の動作を示します。

表 109: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuf53059	FlexFlash の動作プロファイルは 1.5 (1x) からダウングレードすると保持されないため、すべての FlexFlash パーティションがオペレーティングシステムに表示されます。	ダウングレード後に、動作プロファイルを再設定します。	1.5(1f)

表 110: Intel RSTe

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuf02487	Intel RSTe のソフトウェア RAID オプション ROM (Ctrl-I) から RAID ボリュームを作成することはサポートされていません。	LSI ソフトウェア RAID、LSI ハードウェア RAID、または OS SW RAID を使用します。	1.5(1f)

CSCue72256	Intel RSTe の使用時にサーバをブートアップすると、ハードドライブのクリティカルイベントが SEL に報告されます。	実際にハードドライブに障害が発生しているわけではありません。報告された HDD のクリティカルイベントは、システムの起動後には正常になるものなので、無視できます。実際の HDD 障害の場合、HDD で生成された重大なイベントは永続化され、サーバが起動した後でも正常にはなりません。この場合、その HDD の交換処置が必要になります。	1.5(1f)
------------	--	--	---------

リリース 1.5(1) の既知の動作

次に、リリース 1.5(1) の既知の動作を示します。

表 111: BIOS

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuc75369	LSI Web BIOS は、Ctrl + H を押しても起動しないことがあります。	BIOS post 中に、F6 を押してブートオーバーライドリストを表示し、適切なエントリを選択して Web BIOS を起動します。	1.5(1)
CSCuc60934	BIOS ブート順が、仮想メディアデバイスが CIMC WebUI vKVM コンソールまたは CIMC CLI を介してマウントされ、マウント解除されると、変更されます。	仮想メディア デバイスをマウント解除した後、BIOS セットアップまたは CIMC のいずれかを使用してブート順序を再設定し、ブート順序を復元します。	1.5(1)

CSCtf54851	シリアルポート B は、BIOS セットアップの [サーバ管理 (Server Management)] > [コンソールリダイレクション (Console Redirection)] ページでコンソールリダイレクションを設定しても、有効にすることはできません。	シリアルポート B は、主に SOL 機能で使われます。SOL が有効になっている場合、BIOS はコンソールメッセージをシリアルポート B へリダイレクトします。シリアルポート B を介してコンソールリダイレクションメッセージを取得するには、BMC から SOL を有効にする必要があります。	1.5(1)
CSCth71350	現在の CIMC ネットワーキングモードが出荷モードの場合、BIOS F8 の CIMC 設定ユーティリティでは、新しいネットワーキングモードと IP アドレスを同時に設定することはできません。	新しいネットワークモードを設定し、保存してから、新しい IP アドレスを設定して、再度保存します。	1.5(1)
CSCtq84425	BIOS コンソールリダイレクションが有効になっている場合、Broadcom PCIe オプション ROM で特定のボーレートに設定すると、キーボードが動作を停止することがあります。	コンソールリダイレクションを無効にします。	1.5(1)
CSCtx27907	BIOS を起動すると、次のメッセージが表示されることがあります: Cisco IMC IP/MAC アドレスの取得エラー (Error on Getting Cisco IMC IP/MAC Address)。	このメッセージは無視できます。	1.5(1)

CSCtx92042	Broadcom 5709 ギガビットイーサネットアダプタをいずれかの PCIE スロットに差し込んだ場合、サーバが起動プロセス中の BIOS POST 画面で停止します。	Broadcom 5709 ギガビットイーサネットアダプタのファームウェアをバージョン 5.2.7 以降にアップグレードします。	1.5(1)
CSCtr93601	iFlash32 ユーティリティを使用した BIOS ダウングレード (1.4. x から古いバージョンの 1.2. x へ) は失敗します。	ダウングレードするには、1.2. x コンテナで使用可能な startup.nsh スクリプトを使用します。このスクリプトは BIOS のダウングレードを正常に実行します。	1.5(1)

表 112: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuf05110	Intel RSTe を使用している場合、CIMC CLI は HDD の PID を報告しません。	なし	1.5(1)

CSCue54670	Virident カード (または特定のファン制御を行う任意のカード) を搭載したサーバの場合、ホストがオンのときに CIMC を工場出荷時の初期状態にリセットすると、ファン制御がカード固有ではない設定に戻ります。これによりファンが遅くなり、ファンが高速で動作することを必要とするカード (Virident FlashMaxII カードなど) が存在する場合、カードが過熱する可能性があります。これは、カードに関する情報を CIMC がホストから得ているためであり、工場出荷時のデフォルト設定に戻すと、この情報は消去されるからです。	CIMC がカード固有の情報を取得し、必要に応じてファンの速度を上げることができるように、ホストをリブートします。	1.5(1)
CSCtg92856	一部の PS 電源ケーブルが取り外された状態でも、シャーシの電源をオンにすると、前面パネルのシステムヘルス LED が緑色に点灯します。しかし、一部の電源装置には電圧がかかりません。	APC 電源から電源装置へのすべてのケーブルをしっかりと接続します。	1.5(1)

CSCtz52715	Macに挿入されたUSBキーは、強制的に読み取り専用にされることがあります。		1.5(1)
------------	--	--	--------

		Mac ユーザは、マッピングの前にリムーバブルドライブのマウントを解除する必要があります。 1. コマンドラインインターフェイスから次のコマンドを実行します: <code>diskutil unmount /Volumes/<Volume name></code> 2. KVM/vMedia クライアントで、[読み取り専用 (Read Only)] チェックボックスをオフにします。この時点で、ユーザにドライブの自動マウントを停止するかどうかを尋ねるプロンプトが表示されることがあります。[はい (Yes)] をクリックします。 3. ドライブのマッピングを続行します。 mac OS はマウント解除されたドライブを積極的に再マウントしようとするため、タイミングによってはこれらの手順がうまくいかない場合があります。手順を完了する前にドライブが OS によって再マウントされた場合は、この手順を繰り返してください。または、USB スティックの
--	--	---

		マッピングを解除するため、Finder を使用してデバイスを取り出し、デバイスが vMedia クライアントビューから消えるのを待ち、vMedia セッションの実行中に物理的に取り外して再挿入することもできます。前述のように、ドライブの自動マウントを停止するか尋ねられた場合は、[はい (Yes)] をクリックします。	
CSCua63839	Spaces が有効になっている Mac では、セッションが終了したことを示す vKVM ポップアップ通知を閉じることができません。このボタンをクリックしようとする、フォーカスがポップアップがある Space から移動するからです。	vKVM のメインウィンドウを、ポップアップ通知と同じ Space に移動します。こうすると、ボタンをクリックしてポップアップを閉じることができます。	1.5(1)
CSCtr37876	SNMPv2 および SNMPv3 トラップがイネーブルになっている場合に、SNMPv1 トラップが送信されます。	なし。	1.5(1)

CSCtx00839	[KVM]画面にブランク画面が表示されます。	物理モニタを使用して、画面の解像度を変更します。次の解像度がサポートされています。 • 640x480 (8bpp) • 800x600 (8bpp) • 1024x768 (8bpp) • 1280x1024 (8bpp) • 1600x1200 (8bpp) • 1920x1080 (8bpp) • 1920x1200 (8bpp) • 640x480 (16bpp) • 800x600 (16bpp) • 1024x768 (16bpp) • 1280x1024 (16bpp) • 1600x1200 (16bpp) • 1920x1080 (16bpp) • 1920x1200 (16bpp) • 640x480 (24bpp) • 800x600 (24bpp) • 1024x768 (24bpp) • 1280x1024 (24bpp) • 640x480 (32bpp) • 800x600 (32bpp) • 1024x768 (32bpp) • 1280x1024 (32bpp)	1.5(1)
------------	------------------------	--	--------

CSCtx88183	ファームウェアの更新後、CIMC Web GUI と CLI は [仮想ドライブ (Virtual Drive)] ドライブタブの下に仮想ドライブの情報を表示しない場合があります。仮想ドライブタブには、システムに存在する仮想ドライブのリストが表示されるはずですが、仮想ドライブの数がゼロと表示されます。	Cisco IMC を再起動します。	1.5(1)
CSCty58229	SNMP ハードディスクインベントリは 0 から番号を付けるのに対し、CIMC HDD センサーは 1 から番号を付けます。	なし。この現象は、SNMP ハードディスクインベントリがストレージインベントリと一致しており、両方ともインデックス 0 で始まるために発生します。ハードディスクセンサーの番号は、SKU のラベルと一致するため、1 から始まりません。センサーとストレージインベントリ全体で特定の HDD の詳細を参照しながら、違いを認識し、それに応じてマッピングする必要があります。	1.5(1)
CSCty60975	HDD が存在することが、SNMP では確認できません。	代替インターフェイスを使用するか、アクション後に HDD インベントリに対して snmp クエリーをもう一度実行します。	1.5(1)
CSCual1831	Cisco C22 にファン 2、4、および 5 を挿入すると、SNMP トラップが重複して取得されます。	なし。	1.5(1)

CSCuc87936	CIMC をバージョン 1.4 にダウングレードした後に、「FlexFlash と通信できません (Unable to communicate with FlexFlash)」というエラーメッセージが表示されます。	SD カードのタイプが SD253 の場合、ユーザは [Flexcontroller のリセット (Reset Flex Controller)] ボタンを 2 回選択する必要があります。それ以外の場合は、ボタンを 1 回だけ選択します。	1.5(1)
------------	---	---	--------

表 113: Intel アダプタ

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCuc52172	複数の Intel ネットワークアダプタが存在する場合、1 つのカードから iSCSI 設定を入力して、すべての Intel カードの設定が変更できます。変更後、いずれかのカードが取り外されると、残りのカードのオプション ROM が、取り外されたカードによって上書きされているように見えます。	変更する必要があるカードの iSCSI 設定を入力します。他のカードが表示されている場合は変更しないでください。この問題は、PXE 設定ではなく、iSCSI 設定でのみ発生します。	1.5(1)

表 114: LSI

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCtg25373	LSI MegaRAID コントローラで作成された仮想ドライブの数が 50 以上の場合、システムはこれらの仮想ドライブから起動しません。	なし。仮想ドライブの数が 49 以下の場合のみ、システムは MegaRAID 仮想ドライブから起動します。	1.5(1)

CSCua03604	C220/C240 M3 サーバで 2008 MEZZ カードのオプション ROM が無効になっている場合、iSCSI ターゲットに RHEL 6.2 をインストールしようとする、ハングします。	2008 LSI OPROM がサーバに存在する場合は、常にシステム BIOS で有効にする必要があります。ユーザがこれを無効にした場合、OS によっては、インストール中にシステムがハングしないように、2008 MEZZ カードの LSI MegaRAID ドライバをブラックリストに登録する必要があります。	1.5(1)
CSCts37240	[Cisco IMC] > [インベントリ (Inventory)] > [ストレージ (Storage)] > [バッテリーバックアップユニット (Battery Backup Unit)] に移動すると、一部の LSI RAID コントローラに次のエラーメッセージが表示されます。エラー: 必要な HW が欠落しています (アラームまたは BBU) (Error: required HW is missing (i.e Alarm or BBU))。サーバに BBU が搭載されておらず、ユニットが存在しないことを確認する必要があります。	なし。この問題については、現在調査中です。	1.5(1)

表 115: Web UI

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCtc22985	Web UI からの印刷はサポートされていません。	Web UI では、スクリーンショットを撮って、印刷してください。	1.5(1)

リリース 1.4(3) の既知の動作

次に、リリース 1.4 (3) の既知の動作を示します。

表 116: CIMC

不具合 ID	症状	回避策	最初に影響を受けるリリース
CSCun24570	WebUIからは、すべての数字 CN が設定できません。	CLI から CN を更新してください。	1.4(3)

推奨されるベストプラクティス

VMware インストールのためのベスト プラクティス

第 1 世代 (Gen 1) SD カードに VMware をインストールするためのエキスパート モードによる回避策

インストーラアプリケーションを起動したら、VMware をインストールするパーティションを見つけます。次の例では、パーティションは **vmhba33: c0: T0: L0** です。

1. Alt+F1 を押して、VMware リカバリ コンソールに入ります。
2. ディスクに GUID パーティション テーブル (GPT) を作成します。

```
/dev/disks # partedUtil mklabel mpx.vmhba33:C0:T0:L0 gpt
```

3. 次のように、GPT を確認します。

```
/dev/disks # partedUtil get mpx.vmhba33:C0:T0:L0
3785 255 63 60817408
```

4. VMware のインストールに戻ります。

BIOS および Cisco IMC ファームウェアのアップグレード

Cisco は、Cisco Host Upgrade Utility を提供しています。これは、BIOS、Cisco IMC、CMC LOM、LSI ストレージコントローラ、および Cisco UCS 仮想インターフェイス カードのファームウェアを互換性のあるレベルへアップグレードするために役立ちます。C220 M3、C240 M3、C22 M3、および C24 M3 サーバでは、Cisco IMC および BIOS ファームウェアのアップデートを実行する前に、Cisco IMC を再起動することを推奨します。これには、MIHUU、HUU、Web UI、CLI、または XML API を使用します。



- (注) UCS C シリーズプラットフォームの Cisco IMC ファームウェアをアップグレードする場合は、更新に完全なイメージを使用していることを確認してください(たとえば `upd-pkg-cXXX-mx-Cisco IMC.full.*.bin`)。

サーバ モデルに対して、互換性のある正しいファームウェア レベルが、ユーティリティ ISO に埋め込まれています。

このユーティリティを使用するには、ISO ユーティリティをダウンロードして使用するための指示を含む『Cisco Host Upgrade Utility User Guide』を使用します。次の URL からガイドを選択します。

http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html

関連資料

関連資料

このリリースの設定については、次を参照してください。

- 『Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide』
- 『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』
- Cisco UCS ラックマウント サーバ Cisco IMC API プログラマ ガイド

C シリーズサーバのインストールの詳細については、次を参照してください。

- Cisco UCS C シリーズラックサーバのインストールおよびアップグレードガイド

次の関連資料は、Cisco Unified Computing System (UCS) で入手できます。

- 『Cisco UCS C-Series Servers Documentation Roadmap』
- 『Cisco UCS Site Preparation Guide』
- 『Regulatory Compliance and Safety Information for Cisco UCS』
- 管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、「[Release Bundle Contents for Cisco UCS Software](#)」を参照してください。

次の場所にある『Cisco UCS Manager ソフトウェアのリリースノート』および『Cisco UCS C シリーズの Cisco UCS Manager との統合に関するガイド』を参照してください。

- 『Cisco UCS Manager Release Notes』
- Cisco UCS C シリーズ サーバと Cisco UCS Manager との統合に関するガイド

