



FREESPOT導入キット

FS-M1266

公衆Wi-Fi向け設定事例集 第3版

機器やソフトウェアのバージョンについて

本書で解説する設定には、下記のものを使用しています。お使いの機器やソフトウェアのバージョンによっては、本書に記載の画面や手順と一部変更となる場合があります。

- FS-M1266(Ver.4.01)
- BS-GS2008P(Ver.1.0.3.43)
- WAPM-1266R(Ver.1.14)
- WAPM-AX8R(Ver.1.01)
- BS-GSL2008P(Ver.1.10)
- ビジネススイッチ設定ツール(Ver.2.1.0)
- エアステーション設定ツール(Ver.2.0.19)

<https://www.buffalo.jp/>

35021654-03
2021.08

目次

第1章	はじめに	4
	本書に記載の設定事例について	4
	本製品の初期設定	4
	Step 1 設定画面を表示する	4
	Step 2 インターネットに接続する	6
	Step 3 設定画面のパスワードを変更する	9
	Step 4 FREESPOT管理者情報を登録する	10
	Step 5 FREESPOTマップ登録を行う	11
第2章	設定事例	12
	例1:個人経営の飲食店などの小規模施設に公衆Wi-Fiを新規導入したい	12
	Step 1 本製品を設置する	12
	Step 2 公衆Wi-Fiの設定を行う	12
	Step 3 オーナー端末を接続するためのSSIDを設定する	16
	例2:道の駅や商店街などの中規模施設に公衆Wi-Fiを新規導入したい(公衆Wi-Fi利用者端末とオーナー端末を接続する場合)	17
	Step 1 本製品を設置する	18
	Step 2 公衆Wi-FiのVLANの設定を行う	18
	Step 3 L2スイッチのIPアドレスを変更して設定画面を表示する	20
	Step 4 L2スイッチにVLANの設定をする	25
	Step 5 L2スイッチにACLルールを登録する	28
	Step 6 L2スイッチにACLポート設定をする	33
	Step 7 アクセスポイントをL2スイッチに接続する	34
	Step 8 アクセスポイントのIPアドレスを変更して設定画面を表示する	35

Step 9	アクセスポイントに公衆Wi-Fiの設定を行う	39
Step 10	アクセスポイントにオーナー端末を接続するためのSSIDを設定する	41
例3:道の駅や商店街などの中規模施設に公衆Wi-Fiを新規導入したい(公衆Wi-Fi利用者端末だけを接続する場合)		
Step 1	本製品を設置する	44
Step 2	設定に必要なツールをダウンロードする	44
Step 3	公衆Wi-FiのVLANの設定を行う	45
Step 4	本製品にオーナー用SSIDを設定し、VLAN設定を変更する	47
Step 5	L2スイッチのIPアドレスを変更して設定画面を表示する ..	49
Step 6	L2スイッチをインターネットマンションモードに設定する ..	53
Step 7	アクセスポイントをL2スイッチに接続する	54
Step 8	アクセスポイントのIPアドレスを変更して設定画面を表示する ..	54
Step 9	アクセスポイントに公衆Wi-Fiの設定を行う	59
例4:既設のネットワークに公衆Wi-Fiを追加したい		
Step 1	ルーターに公衆Wi-FiのWAN側用セグメントを追加する ..	64
Step 2	本製品のWAN設定を行い、公衆Wi-FiのVLANを有効にする ..	64
Step 3	既設のL2スイッチ(A)のVLAN設定を変更し、ACLルールを登録する ..	67
Step 4	既設のL2スイッチ(B)のVLAN設定を変更し、ACLルールを登録する ..	76
Step 5	アクセスポイントに公衆Wi-Fiの設定を行う	83
Step 6	本製品をL2スイッチ(A)に接続する	86
例5: L2スイッチのACL機能を使用せずにFREESPOTを導入したい		
Step 1	本製品を設置する	88
Step 2	公衆Wi-FiのVLANの設定を行う	88
Step 3	L2スイッチのIPアドレスを変更して設定画面を表示する ..	90

Step 4	L2スイッチにVLANの設定をする	95
Step 5	アクセスポイントをL2スイッチに接続する	98
Step 6	アクセスポイントのIPアドレスを変更して設定画面を表示する	98
Step 7	アクセスポイントに公衆Wi-Fiの設定を行う	103
Step 8	アクセスポイントにオーナー端末を接続するためのSSIDを設定する	106
例6:	災害などの発生に備えた設定をしたい	108
Step 1	「例1」の設定を行う	109
Step 2	緊急時用VLANを設定する	109
	災害が発生したときに公衆Wi-Fiを一般開放するには	112

第1章 はじめに

本書に記載の設定事例について

本書では、本製品を使った設定のうち、代表的な事例を実際の設定手順を交えて説明します。設定内容によっては、本製品以外にも別途機器が必要となる場合があります。また、インターネット回線契約の変更や既設のネットワーク設定の変更などが必要となる場合があります。あらかじめご了承ください。

メモ: 本書の内容は不定期に更新される場合があります。最新版は、当社ホームページ(https://www.buffalo.jp/support/download/list/?item_code=FS-M1266)でご確認ください。

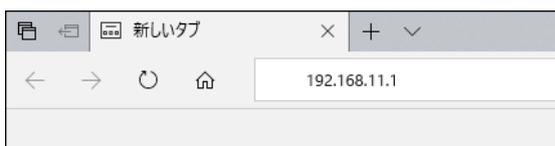
本製品の初期設定

本製品の初期設定として、次のStep 1～5までを行ってください。

Step 1 設定画面を表示する

本製品の設定画面は、以下の手順で表示できます。

- 1 本製品のLAN端子に設定用パソコンを接続します。
- 2 設定用パソコンのブラウザを起動します。
- 3 ブラウザーのアドレス欄に本製品のLAN側IPアドレスを入力します。



メモ: 本製品のLAN側IPアドレスの出荷時設定は、「192.168.11.1」です。

4 ユーザー名に本製品の管理ユーザー名、パスワードに本製品の管理パスワードを入力して[ログイン]をクリックします。

ユーザー名
admin

パスワード
●●●●●●●●

ログイン

メモ:

- 管理ユーザー名の出荷時設定は、「admin」です。
- 管理パスワードの出荷時設定は、「password」です。後述の「Step 3 設定画面のパスワードを変更する」を参照し、必ず変更を行ってください。

5 本製品の設定画面が表示されます。



以上で完了です。

Step 2 インターネットに接続する

本製品のインターネット接続設定は、以下の手順で行います。

メモ:

- 下記設定を行う前に、インターネットサービスの契約が完了し、サービスが開始されていることを確認してください。
- また、構内/社内LANに接続する場合は、ネットワーク管理者より必要な情報を取得してください。
- 設定の際に、インターネット回線の接続先ユーザー名や接続先パスワードが必要となる場合があります。プロバイダーから提供された書類を事前にご用意ください。

1 本製品の電源が入っている場合は、電源を切ります。

2 本製品のWAN端子とインターネット回線を接続します。

3 本製品の電源を入れます。

4 前述の「Step 1 設定画面を表示する」を参照して、本製品の設定画面を表示します。

5 [詳細設定]をクリックします。

6 [WAN/LAN] – [WAN設定]をクリックします。

7 WAN側の設定を行い、[設定]をクリックします。

本製品を設置する環境にあわせて設定してください。

メモ: 下記の例1～3のどれに該当するかが分からない場合は、ご契約のプロバイダーまたはネットワーク管理者にご確認ください。

例1: WAN側のIPアドレスを「手動設定」にしたい場合の例

VLAN名	WAN
VLAN ID	1000
IPアドレスの取得方法	手動設定
IPアドレス	お使いの環境にあわせて設定します
デフォルトゲートウェイ	
DNS	
MTU	1500
WAN側MACアドレス	デフォルトのMACアドレスを使用

WAN側インターフェース設定	
VLAN名	WAN
VLAN ID	1000
IP アドレスの取得方法	<input checked="" type="radio"/> 手動設定 <input type="radio"/> DHCP クライアント <input type="radio"/> PPPoE クライアント
IP アドレス	IP アドレス <input type="text"/> サブネットマスク <input type="text" value="255.255.255.0"/>
デフォルトゲートウェイ	<input type="text"/>
DNS	プライマリーサーバー: <input type="text"/> セカンダリーサーバー: <input type="text"/>
MTU	1500
WAN側MACアドレス	<input checked="" type="radio"/> デフォルトのMACアドレスを使用(XX:XX:XX:XX:XX:XX) <input type="radio"/> 手動設定 <input type="text"/>
<input type="button" value="設定"/>	

例2: WAN側のIPアドレスが「DHCPクライアント」の場合の例

VLAN名	WAN
VLAN ID	1000
IPアドレスの取得方法	DHCPクライアント
デフォルトゲートウェイ	お使いの環境にあわせて設定します
DNS	
MTU	1500
WAN側MACアドレス	デフォルトのMACアドレスを使用

WAN側インターフェース設定

VLAN名	WAN
VLAN ID	1000
IP アドレスの取得方法	<input type="radio"/> 手動設定 <input checked="" type="radio"/> DHCP クライアント <input type="radio"/> PPPoE クライアント
デフォルトゲートウェイ	<input style="width: 100%;" type="text"/>
DNS	プライマリーサーバー: <input style="width: 80%;" type="text"/> セカンダリーサーバー: <input style="width: 80%;" type="text"/>
MTU	1500
WAN側MACアドレス	<input checked="" type="radio"/> デフォルトのMACアドレスを使用(XX:XX:XX:XX:XX:XX) <input type="radio"/> 手動設定 <input style="width: 100%;" type="text"/>

例3: WAN側のIPアドレスが「PPPoEクライアント」の場合の例

VLAN名	WAN
VLAN ID	1000
IPアドレスの取得方法	PPPoEクライアント
PPPoE	プロバイダーから提供された書類を参照して設定します
PPPoE拡張設定	接続方法: 常時接続 自動切断条件: 送受信ともがない場合 自動切断待機時間: 5分 認証方法: 自動認証
DNS	お使いの環境にあわせて設定します
MTU	1454
MRU	1454
WAN側MACアドレス	デフォルトのMACアドレスを使用

WAN側インターフェース設定	
VLAN名	WAN
VLAN ID	1000
IP アドレスの取得方法	<input type="radio"/> 手動設定 <input type="radio"/> DHCP クライアント <input checked="" type="radio"/> PPPoE クライアント
PPPoE	接続先ユーザー名 <input type="text"/> 接続先パスワード <input type="text"/> (確認用) <input type="text"/> サービス名 <input type="text"/> キーブアライブ <input checked="" type="checkbox"/> 使用する
PPPoE拡張設定	接続方法 <input type="text" value="常時接続"/> 自動切断条件 <input type="text" value="送受信ともがない場合"/> 自動切断待機時間 <input type="text" value="5"/> 分 (0分では自動切断しません) 認証方法 <input type="text" value="自動認証"/>
DNS	プライマリサーバー: <input type="text"/> セカンダリサーバー: <input type="text"/>
MTU	1454
MRU	1454
WAN側MACアドレス	<input checked="" type="radio"/> デフォルトのMACアドレスを使用(XX:XX:XX:XX:XX:XX) <input type="radio"/> 手動設定 <input type="text"/>
<input type="button" value="設定"/>	

以上で完了です。

Step 3 設定画面のパスワードを変更する

設定画面にログインするには、ユーザー名とパスワードを入力する必要があります。管理ユーザー名で設定画面にログインすると、すべての設定パラメーターと統計情報の読み取りと書き換えを行う権限が与えられます。デフォルトの管理者ユーザー名は「admin」、管理パスワードは「password」が設定されています。第三者にログインされないよう、必ず管理パスワードおよび参照パスワードを変更してください。

- 1 前述の「Step 1 設定画面を表示する」を参照して、本製品の設定画面を表示します。
- 2 「詳細設定」をクリックします。
- 3 左側のメニューから「管理設定」-「本体/パスワード」をクリックします。
- 4 「管理パスワード」と「参照パスワード」に新しいパスワードを入力します。(確認用にも同じパスワードを入力してください)

本体/パスワード設定	
管理ユーザー名	admin
管理パスワード	●●●●●●●● (確認用)
参照ユーザー名	user
参照パスワード	●●●●●●●● (確認用)
<input type="button" value="設定"/>	
【拡張設定】	
エアステーション名	APXXXXXXXXXXXX
管理インターフェース	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input type="checkbox"/> SNMP
SNMP Version	SNMPv1/v2c
SNMP Getコミュニティ	public
SNMP Setコミュニティ	private
SNMP Trap	<input type="checkbox"/> 送信する
SNMP Trapコミュニティ	public
SNMP Trap送信先	
<input type="button" value="設定"/>	

メモ:

- 管理パスワードは、6～32文字までの半角英数字および記号を入力してください。
- 参照パスワードは、SNMP Versionが「SNMPv1/v2c」に設定されている場合は0～32文字までの半角英数字および記号を、SNMP Versionが「SNMPv3」に設定されている場合は6～32文字までの半角英数字および記号を入力してください。
- パスワードを設定する際は、管理パスワードおよび参照パスワードの両方を入力してください。片方が空欄の場合、パスワードを設定することができません。ただし、SNMP Versionに「SNMPv1/v2c」を選択している場合は参照パスワードを空欄に設定することができます。
- 管理ユーザー名/パスワードは、本製品の設定画面にログインして、設定変更するためのユーザー名/パスワードです。管理ユーザー名でログインすると、本製品のすべての設定項目が変更可能となります。
- 参照ユーザー名/パスワードは、本製品の設定画面にログインして、設定内容を確認するためのユーザー名とパスワードです。参照ユーザー名でログインすると、本製品の設定は変更できません。

- 5 パスワードを入力したら、「設定」をクリックします。

以上で設定は完了です。

Step 4 FREESPOT管理者情報を登録する

FREESPOTの管理者情報は、以下の手順で登録できます。

メモ: ここに入力した情報は、FREESPOT協議会が管理するサーバーに送信されます。送信を希望しない場合は、入力しないでください。

- 1 前述の「Step 1 設定画面を表示する」を参照して、本製品の設定画面を表示します。
- 2 [詳細設定]をクリックします。
- 3 [管理設定] – [FREESPOT管理者情報]をクリックします。
- 4 「管理者情報」と「設置場所情報」を入力して、[設定]をクリックします。

FREESPOTの管理情報	
管理者情報	
郵便番号	<input type="text"/>
住所	<input type="text"/>
会社名	<input type="text"/>
管理者名	<input type="text"/>
電話番号	<input type="text"/>
FAX	<input type="text"/>
E-mail	<input type="text"/>
設置場所情報	
郵便番号	<input type="text"/>
住所	<input type="text"/>
店舗名	<input type="text"/>
担当者名	<input type="text"/>
電話番号	<input type="text"/>
FAX	<input type="text"/>
E-mail	<input type="text"/>
<input type="button" value="設定"/>	

メモ:

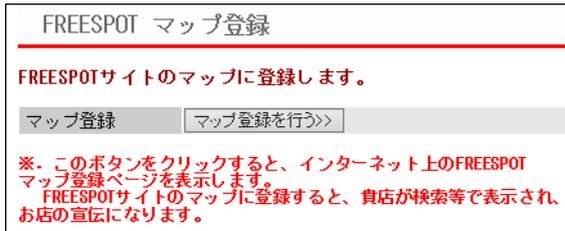
- 「管理者情報」や「設置場所情報」で入力できる文字列は、日本語と英語です。
- 郵便番号は、半角数字および「-」で8文字まで入力できます。
- 会社名、店舗名、管理者名、担当者名は、64文字まで入力できます。
- 電話番号・FAXは、半角数字および「-」で32文字まで入力できます。
- E-mailは、半角英数字と「<」、「>」、「(」、「)」、「[」、「]」、「¥」、「,」、「;」、「:」、「"」以外の記号で127文字まで入力できます。「@」、「.」、「-」で始まる、または終わるもの設定はできません。

以上で完了です。

Step 5 FREESPOTマップ登録を行う

FREESPOTサイトのマップに登録するには、以下の手順で設定します。

- 1 前述の「Step 1 設定画面を表示する」を参照して、本製品の設定画面を表示します。
- 2 [詳細設定]をクリックします。
- 3 [管理設定] – [FREESPOTマップ登録]をクリックします。
- 4 [マップ登録を行う]をクリックします。



- 5 マップ登録画面が表示されたら、画面に従って登録します。

メモ: マップ登録についての詳細は、フリースポットコールセンター(<http://www.freespot.com/about/access.html>)にお問い合わせください。

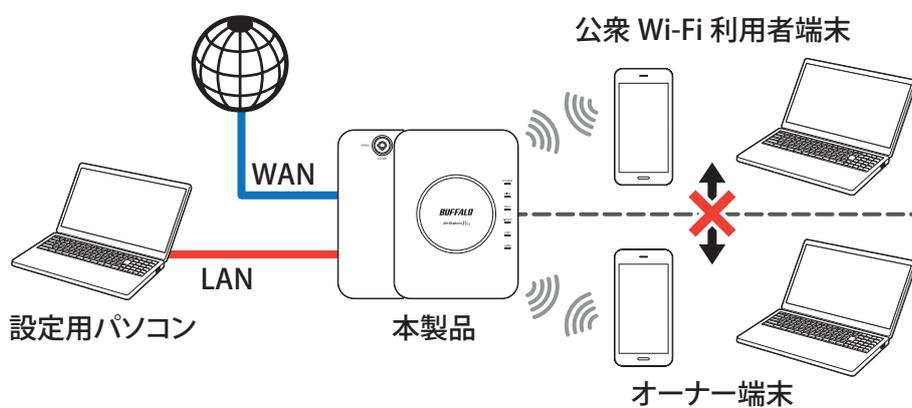
以上で完了です。

第2章 設定事例

例1:個人経営の飲食店などの小規模施設に公衆Wi-Fiを新規導入したい

本製品1台を使って、公衆Wi-Fiを新規導入する方法を説明します。

構成例



条件

- 本製品1台で公衆Wi-Fi(来訪者用ネットワーク)を構築する。
- 公衆Wi-Fi利用者向けに、店舗や自治体独自のSSIDを使用する。
- 公衆Wi-Fi利用者端末から、設定用パソコンやオーナー端末へのアクセスを禁止する。
- 公衆Wi-Fi利用者端末同士の通信を禁止する。

設定に使用する機器

- 本製品(FS-M1266)
- 設定用パソコン

メモ:

- オーナーが所有する有線端末が複数ある場合は、本製品のLAN端子に別売のスイッチ(BS-GU2008など)を接続して使用してください。
- 本製品をPoEによる給電しない場合は、別売のACアダプタ(WLE-OP-AC12C)をご用意ください。

Step 1 本製品を設置する

本製品の設置や初期設定(インターネットの接続設定、FREESPOT管理者登録情報の設定、FREESPOTマップの登録など)は、本書の第1章を参照して設定してください。
完了後、「Step 2 公衆Wi-Fiの設定を行う」へ進んでください。

Step 2 公衆Wi-Fiの設定を行う

カスタムVLANを有効にして、公衆Wi-Fi利用者用のSSIDを設定します。

1 本製品の設定画面を表示します。

設定画面の表示方法は、第1章の「Step 1 設定画面を表示する」を参照してください。

2 [詳細設定]をクリックします。**3 カスタムVLANの設定を行います。**

[WAN/LAN] – [LAN設定]画面にある「CUSTOM_0」(3行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN	有効
VLAN名	任意のVLAN名(例:Public_Wi-Fi)
VLAN ID	3
IPアドレス	IPアドレス: 192.168.13.1 サブネットマスク: 255.255.255.0
DHCPサーバー	割り当てIPアドレス: 192.168.13.2から128台 除外アドレス: 空欄 リース期間: 1時間
i-フィルター	使用しない
SPAMメール対策	使用する メール送信数制限: 20件/分
ポップアップテクノロジー	使用する 広告URL: 接続時に表示させたいポータル画面のURL 広告表示間隔: 0秒
接続時間制限	使用する 接続回数: 3回/日 接続許可時間: 30分/回
公衆無線LAN利用者認証	利用者認証: 使用する ゲスト方式認証: 使用しない SNSアカウント認証: 使用する Wi-Cert Web-API認証: 使用しない 認証画面バナーの汎用表記: 使用しない 認証前HTTPS通信制限: 使用する

VLAN情報の編集

VLAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
VLAN名	Public_Wi-Fi	
VLAN ID	3	
IP アドレス	IP アドレス	192.168.13.1
	サブネットマスク	255.255.255.0
DHCP サーバー	割り当て IP アドレス	192.168.13.2 から 128 台
	除外アドレス	
	リース期間	1 時間

公衆無線LAN関連設定

i-フィルター	<input type="checkbox"/> 使用する フィルターレベル 公衆
SPAMメール対策	<input checked="" type="checkbox"/> 使用する メール送信数制限 20 件/分
ポップアップテクノロジー	<input checked="" type="checkbox"/> 使用する 広告URL http://xxx.xxx.xxx/xxx/ 広告表示間隔 0 秒
接続時間制限	<input checked="" type="checkbox"/> 使用する 接続回数 3 回/日 接続許可時間 30 分/回
公衆無線LAN利用者認証	利用者認証 <input checked="" type="checkbox"/> 使用する
	利用者認証オプション
	ゲスト方式認証 <input type="checkbox"/> 使用する
	SNSアカウント認証 <input checked="" type="checkbox"/> 使用する
	Wi-Cert Web-API認証 <input type="checkbox"/> 使用する
認証画面バナーの汎用表記 <input type="checkbox"/> 使用する	
認証前HTTPS通信制限 <input checked="" type="checkbox"/> 使用する	

修正保存 編集を終了して前の画面へ戻る

メモ: 各内容の詳細は、ユーザーマニュアルを参照してください。

4 公衆Wi-Fi利用者用のSSIDを設定します。

[無線設定] - [SSID設定]画面で、[新規追加]をクリックします。

SSID設定 - SSIDの編集

Index	状態	SSID	VLAN	VLAN ID	2.4GHz	5GHz	認証	暗号化		
1	無効	FREESPOT	FREESPOT 2		<input type="radio"/>	<input type="radio"/>	認証を行わない	暗号化なし	編集	削除
2	無効	*freespot*+SecurityPassword(AES)	FREESPOT 2		<input type="radio"/>	<input type="radio"/>	WPA2/WPA(混在)-PSK TKIP/AES(混在)		編集	削除

新規追加

5 以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	任意のSSID(例:Public_Wi-Fi)
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN: Public_Wi-Fi(手順3で設定したVLAN名) VLAN ID: 3
ANY接続	許可する
プライバシーセパレーター	STAセパレーター
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	施設独自の設定
暗号化	
追加認証	

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SSID	Public_Wi-Fi
次の場合に有効にする	通常時と緊急時
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN: Public_Wi-Fi VLAN ID: 3
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	STAセパレーター
ロードバランス(同時接続台数制限)	2.4GHz: 128 / 128 5GHz: 128 / 128
無線の認証	認証を行わない
暗号化	暗号化なし <small>「暗号化なし」に設定すると、第三者から通信内容を読み取られる可能性があります。</small>
追加認証	追加認証を行わない
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>	

メモ:

- 本製品に接続している端末に対して公衆Wi-Fi利用者端末同士の通信を禁止するため、STAセパレーターを設定しています。
- 各内容の詳細は、ユーザーマニュアルを参照してください。

6 [設定]をクリックします。

Step 3 オーナー端末を接続するためのSSIDを設定する

店舗のオーナー(公衆Wi-Fiの提供者)が使用しているスマートフォンやパソコンなどを接続するためのSSID(オーナー用SSID)を設定します。

1 オーナー用SSIDの設定を行います。

[無線設定] - [SSID設定]画面にある[新規追加]をクリックし、以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	任意のSSID(例:Buffalo)
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
優先制御	優先
VLAN ID	VLANモード: Untagged VLAN: Management VLAN ID: 1
ANY接続	許可する
プライバシーセパレーター	使用しない
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	WPA2-PSK
暗号化	AES
キー更新間隔	60分
事前共有キー	任意の事前共有キー(例:buffalo12345678)
Management Frame Protection	無効
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SSID	Buffalo
次の場合に有効にする	通常時と緊急時
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
優先制御	優先
VLAN ID	VLANモード: Untagged VLAN: Management VLAN ID: 1
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	使用しない
ロードバランス(同時接続台数制限)	2.4GHz: 128 / 128 5GHz: 128 / 128
無線の認証	WPA2-PSK
暗号化方式	AES
キー更新間隔	60 分
事前共有キー	buffalo12345678
Management Frame Protection	無効
追加認証	追加認証を行わない
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>	

メモ: オーナー端末は、制限なく通信できるようにするため、プライバシーセパレーターは「使用しない」に設定します。

2 [設定]をクリックします。

以上で設定は完了です。

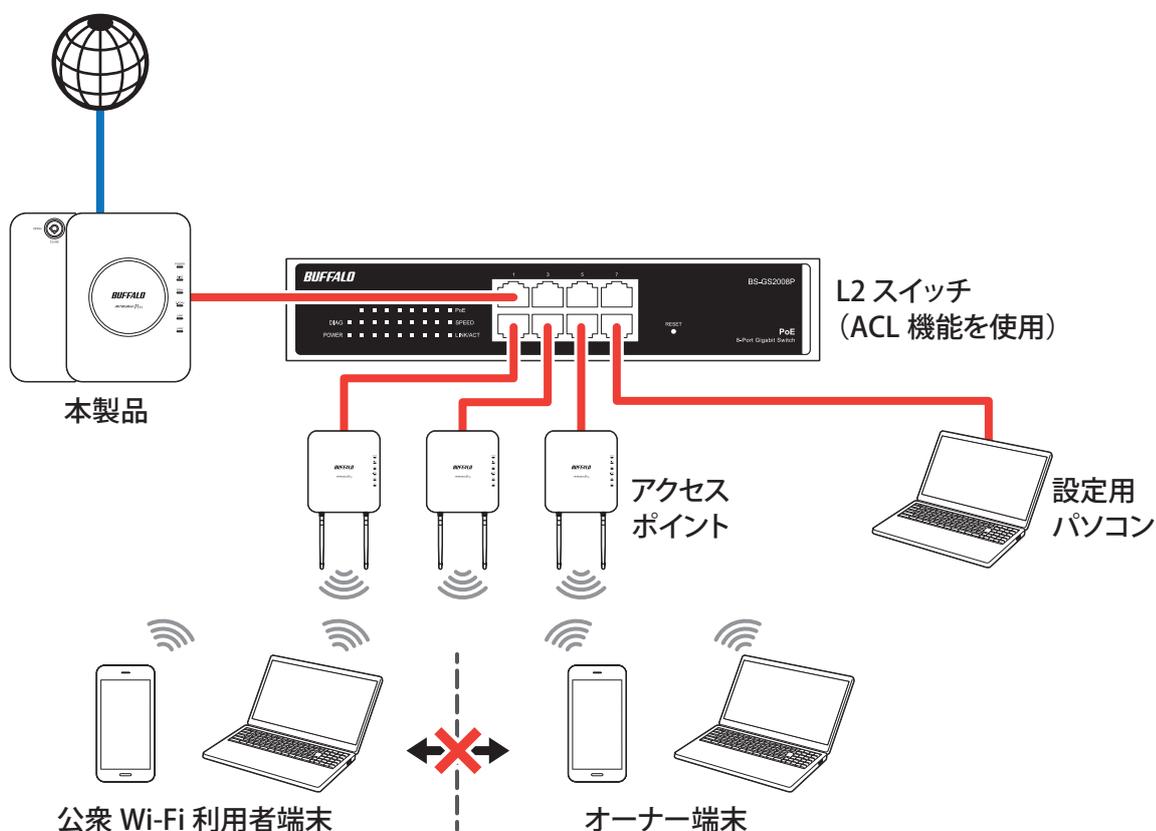
例2:道の駅や商店街などの中規模施設に公衆Wi-Fiを新規導入したい(公衆Wi-Fi利用者端末とオーナー端末を接続する場合)

本製品、スマートスイッチ、アクセスポイントなどを組み合わせて、中規模施設に公衆Wi-Fiを新規導入する方法を説明します。

後述の「例3」との違いは、L2スイッチの設定とオーナー端末をアクセスポイントに接続するかどうかです。本構成では、L2スイッチのACL(アクセスコントロールリスト)機能を使用し、以下の設定をする場合を想定しています。

- 各々のアクセスポイントに接続した、公衆Wi-Fi利用者端末同士の通信を防ぐ。
- どのアクセスポイントに接続していても、オーナー端末同士は通信を許可する。

構成例



条件

- 公衆Wi-Fi利用者は、本製品とは別のアクセスポイントに接続させる。
- 公衆Wi-Fi利用者端末から、設定用パソコンやオーナー端末へのアクセスを禁止する。
- 公衆Wi-Fi利用者端末同士の通信を禁止する。

設定に使用する機器

- 本製品 (FS-M1266)
- ACL機能に対応したL2スイッチ (BS-GS2008Pなど)
- アクセスポイント (WAPM-1266Rなど)
- 設定用パソコン

メモ:

- L2スイッチやアクセスポイントの推奨機器は、当社ホームページ (<https://www.buffalo.jp/product/detail/fs-m1266.html>) を参照してください。
- L2スイッチがPoEに対応していない場合は、別売のACアダプタ (WLE-OP-AC12C) をご用意ください。
- FREESPOT利用者が本製品とは別のアクセスポイントに接続するよう、本事例では本製品の無線機能はOFFで説明していますが、ONにすることもできます。

Step 1 本製品を設置する

本製品の設置や初期設定 (インターネットの接続設定、FREESPOT管理者登録情報の設定、FREESPOTマップの登録など) は、本書の第1章を参照して設定してください。

完了後、前述の「構成例」にあわせて配線し、「Step 2 公衆Wi-FiのVLANの設定を行う」へ進んでください。

メモ:

- 本製品のLAN端子は、L2スイッチのポート1に接続してください。
- 設定用パソコンは、L2スイッチのポート8に接続してください。

Step 2 公衆Wi-FiのVLANの設定を行う

公衆Wi-FiのVLANを有効にします。

1 本製品の設定画面を表示します。

設定画面の表示方法は、第1章の「Step 1 設定画面を表示する」を参照してください。

2 [詳細設定]をクリックします。

3 公衆Wi-FiのVLANの設定を行います。

[WAN/LAN] – [LAN設定]画面にある「CUSTOM_0」(3行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN	有効
VLAN名	任意のVLAN名(例:Public_Wi-Fi)
VLAN ID	3
IPアドレス	IPアドレス: 192.168.13.1 サブネットマスク: 255.255.255.0
DHCPサーバー	割り当てIPアドレス: 192.168.13.2から128台 除外アドレス: 空欄 リース期間: 1時間
i-フィルター	使用しない
SPAMメール対策	使用する メール送信数制限: 20件/分
ポップアップテクノロジー	使用する 広告URL: 接続時に表示させたいポータル画面のURL 広告表示間隔: 0秒
接続時間制限	使用する 接続回数: 3回/日 接続許可時間: 30分/回
公衆無線LAN利用者認証	利用者認証: 使用する ゲスト方式認証: 使用しない SNSアカウント認証: 使用する Wi-Cert Web-API認証: 使用しない 認証画面バナーの汎用表記: 使用しない 認証前HTTPS通信制限: 使用する

VLAN情報の編集	
VLAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
VLAN名	Public_Wi-Fi
VLAN ID	3
IP アドレス	IP アドレス 192.168.13.1
	サブネットマスク 255.255.255.0
DHCP サーバー	割り当て IP アドレス 192.168.13.2 から 128 台
	除外アドレス
	リース期間 1 時間
公衆無線LAN関連設定	
i-フィルター	<input type="checkbox"/> 使用する フィルターレベル 公衆
SPAMメール対策	<input checked="" type="checkbox"/> 使用する メール送信数制限 20 件/分
ポップアップテクノロジー	<input checked="" type="checkbox"/> 使用する 広告URL http://xxx.xxx.xxx.xxx/ 広告表示間隔 0 秒
接続時間制限	<input checked="" type="checkbox"/> 使用する 接続回数 3 回/日 接続許可時間 30 分/回
公衆無線LAN利用者認証	利用者認証 <input checked="" type="checkbox"/> 使用する
	利用者認証オプション
	ゲスト方式認証 <input type="checkbox"/> 使用する
	SNSアカウント認証 <input checked="" type="checkbox"/> 使用する
	Wi-Cert Web-API認証 <input type="checkbox"/> 使用する
認証画面/バナーの汎用表記 <input type="checkbox"/> 使用する	
認証前HTTPS通信制限 <input checked="" type="checkbox"/> 使用する	
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>	

メモ: 各内容の詳細は、ユーザーマニュアルを参照してください。

Step 3 L2スイッチのIPアドレスを変更して設定画面を表示する

「ビジネススイッチ設定ツール」を使ってL2スイッチのIPアドレスを変更し、設定画面を表示します。

- 1 当社ホームページ(https://www.buffalo.jp/support/download/detail/?dl_contents_id=60665)から「ビジネススイッチ設定ツール」をダウンロードして、設定用パソコンにインストールします。
- 2 「ビジネススイッチ設定ツール」を起動します。

3 [次へ]をクリックします。



4 L2スイッチを選択して、[次へ]をクリックします。



5 設定画面にアクセスするためには、セグメントを合わせる必要があります。

[このスイッチのIPアドレスを設定する]をクリックします。

← ビジネススイッチ設定ツール

操作の選択

次のスイッチが選択されました。おこないたい操作を選択してください。

スイッチ名	製品名	MAC アドレス	IP アドレス
BSXXXXXXXXXXXX	BS-GS2008P Ver. X.X.X.XX	XX:XX:XX:XX:XX:XX	192.168.1.254

設定画面を開く(W)
(通常はこちら)

このスイッチの IP アドレスを設定する(I)
(上級者・管理者向け)

6 L2スイッチのIPアドレスを変更します。

[次のIPアドレスを使う(上級者・管理者向け)]を選択し、IPアドレスを「192.168.11.254」、サブネットマスクを「255.255.255.0」に設定して[次へ]をクリックします。

← ビジネススイッチ設定ツール

スイッチの IP アドレス設定

スイッチの新しい IP アドレスを入力してください。

DHCP サーバーから IP アドレスを自動的に取得する(かんたん)(D)

次の IP アドレスを使う(上級者・管理者向け)(S)

IP アドレス(I) [設定方法](#)

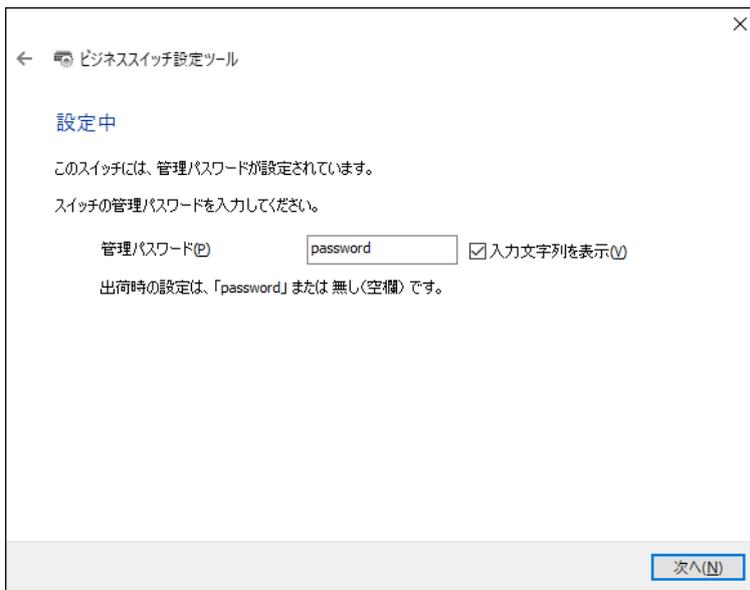
サブネットマスク(U)

* 参考情報 - このパソコンの IP アドレス:
68.11.2 / 255.255.255.0 : イーサネット (Intel(R) 82579V Gigabit Network Connection)

[次へ] をクリックすると、設定内容がスイッチに反映されます。

次へ(N)

- 7** パスワードの入力画面が表示されたら、L2スイッチに設定されている管理パスワードを入力して、[次へ]をクリックします。



← ビジネススイッチ設定ツール

設定中

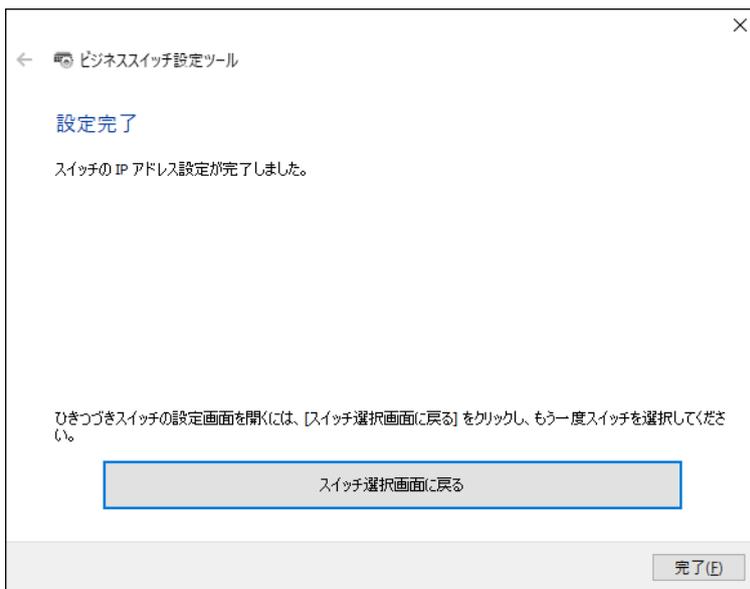
このスイッチには、管理パスワードが設定されています。
スイッチの管理パスワードを入力してください。

管理パスワード(P) 入力文字列を表示(V)

出荷時の設定は、「password」または「無し(空欄)」です。

次へ(N)

- 8** 以下の画面が表示されたら、[スイッチ選択画面に戻る]をクリックします。



← ビジネススイッチ設定ツール

設定完了

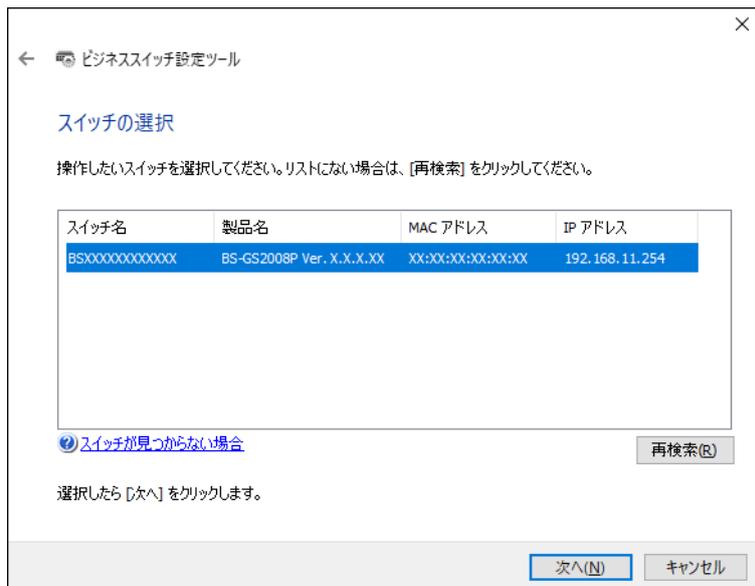
スイッチの IP アドレス設定が完了しました。

ひきつづきスイッチの設定画面を開くには、[スイッチ選択画面に戻る] をクリックし、もう一度スイッチを選択してください。

スイッチ選択画面に戻る

完了(F)

9 L2スイッチを選択して、「次へ」をクリックします。

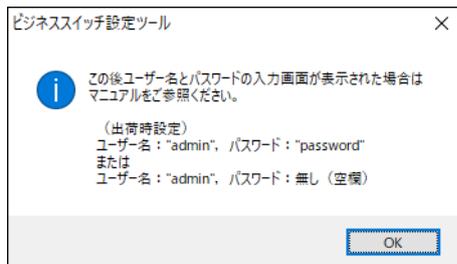


10 「設定画面を開く(通常はこちら)」をクリックします。



11 「OK」をクリックします。

ブラウザーが起動し、ログイン画面が表示されます。



12 L2スイッチの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

ユーザー名

パスワード

メモ: 設定画面のウィンドウが開くと、ビジネススイッチ設定ツールのウィンドウに「スイッチの設定画面を開きました」と表示されます。ビジネススイッチ設定ツールのウィンドウの[完了]をクリックしてください。ビジネススイッチ設定ツールが閉じます。

Step 4 L2スイッチにVLANの設定をする

L2スイッチの設定画面でVLAN設定を行います。

1 VLAN設定画面を表示します。

[基本設定] - [VLAN] - [VLAN設定]画面で、VLAN ID 1のチェックボックスにチェックマークをつけて、[編集]をクリックします。

VLANステータス												
<input checked="" type="checkbox"/>	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input checked="" type="checkbox"/>	1	192.168.11.254	U	U	U	U	U	U	U	U		Up
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
<input type="button" value="編集"/>			<input type="button" value="削除"/>									

2 Management VLANを以下のように設定して、[適用]をクリックします。

VLAN ID	1
VLAN名	Management
管理VLAN	チェックあり
接続方式	固定IPアドレス
IPv4アドレス	192.168.11.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.11.1
取得方式	手動設定
プライマリDNSサーバー	192.168.11.1
セカンダリDNSサーバー	0.0.0.0
IPv6	無効
Tagged	なし
Untagged	1、2、3、4、5、6、7、8
Not Member	なし

VLANの追加/編集

VLAN ID (2-4094)

VLAN名

管理VLAN

接続方式

接続方式 ▼

IPv4アドレス設定

IPv4アドレス

サブネットマスク

デフォルトゲートウェイ

DNSサーバー

取得方式 ▼

プライマリDNSサーバー

セカンダリDNSサーバー

IPv6アドレス設定

IPv6 有効

ポート	1	2	3	4	5	6	7	8
Tagged	<input type="radio"/>							
Untagged	<input checked="" type="radio"/>							
Not Member	<input type="radio"/>							

3 VLANステータスが以下のようになったことを確認します。

VLANステータス												
■	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.11.254	U	U	U	U	U	U	U	U	Management	Up
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
編集 削除												

4 公衆Wi-FiのVLANを作成します。

以下のように設定して、[適用]をクリックします。

VLAN ID	3
VLAN名	Public_Wi-Fi
管理VLAN	チェックなし
Tagged	1、2、3、4、5、6、7
Untagged	なし
Not Member	8

VLANの追加編集

VLAN ID (2-4094)

VLAN名

管理VLAN

ポート		1	2	3	4	5	6	7	8
Tagged	All	<input checked="" type="radio"/>	<input type="radio"/>						
Untagged	All	<input type="radio"/>							
Not Member	All	<input type="radio"/>	<input checked="" type="radio"/>						

適用 リセット キャンセル

5 VLANステータスが以下のようになったことを確認します。

VLANステータス												
■	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.11.254	U	U	U	U	U	U	U	U	Management	Up
<input type="checkbox"/>	3	-	T	T	T	T	T	T	T	-	Public_Wi-Fi	Down
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
編集 削除												

Step 5 L2スイッチにACLルールを登録する

L2スイッチの設定画面で、以下の2点に関するACLの設定を行います。

- 各々のアクセスポイントに接続した、公衆Wi-Fi利用者端末同士の通信を防ぐ。
- どのアクセスポイントに接続していても、オーナー端末同士は通信を許可する。

1 MAC ACL設定画面を表示します。

[詳細設定] - [ACL] - [MAC ACL]画面を表示します。

2 ACLグループ名に「Public_Wi-Fi_Downlink」と入力して、[適用]をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> Public_Wi-Fi_Downlink	

適用 名前の変更 削除

3 手順2で追加した「Public_Wi-Fi_Downlink」の[詳細]をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/>	
<input type="checkbox"/> Public_Wi-Fi_Downlink	0/10

適用 名前の変更 削除

4 本製品(FS-M1266)のMAC宛でのユニキャスト通信を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: 本製品(FS-M1266)の有線MACアドレス マスク: 00:00:00:00:00:00
送信元MACアドレス	すべて
イーサタイプ	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	手動 ▼ アドレス: XX:XX:XX:XX:XX:XX マスク: 00:00:00:00:00:00 (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて ▼ アドレス: マスク: (例: 00:11:22:33:44:55)
イーサタイプ	すべて ▼ (0600-FFFF Hex)
VLAN	すべて ▼
ACLの動作	
許可/拒否	許可 ▼
Egressキュー	なし ▼
リダイレクトポート	なし ▼
保存 戻る	

5 続けて、ブロードキャストMAC宛ての通信を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: FF:FF:FF:FF:FF:FF マスク: 00:00:00:00:00:00
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

6 続けて、マルチキャストMAC宛ての通信を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: 01:00:5E:00:00:00 マスク: 00:00:00:7F:FF:FF
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

7 続けて、管理用VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	1
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定

ACLグループ名 Public_Wi-Fi_Downlink

CoS

送信先MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

送信元MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

イーサータイプ (0600-FFFF Hex)

VLAN

ACLの動作

許可/拒否

Egressキュー

リダイレクトポート

8 続けて、手順4～7以外の通信をすべて禁止するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	拒否
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定

ACLグループ名 Public_Wi-Fi_Downlink

CoS

送信先MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

送信元MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

イーサータイプ (0600-FFFF Hex)

VLAN

ACLの動作

許可/拒否

Egressキュー

リダイレクトポート

- 9** ここまで登録したら、手順4～8の内容が正しく設定されているかを確認します。
正しく設定されている場合は、ACLルール一覧が以下のように表示されます。

MAC ACLルール設定

ACLルール一覧 (優先度順)

ルール番号	CoS	送信元MACアドレス	送信元マスク	送信元MACアドレス	送信元マスク	イーサタイプ	VLAN	許可/拒否	Egressキュー	リダイレクトポート
<input type="checkbox"/> 1	すべて	XXXXXXXXXXXX	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 2	すべて	FFFFFFFFFFFF	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 3	すべて	01:00:3E:00:00:00	00:00:00:7F:FF:FF	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 4	すべて	すべて	すべて	すべて	すべて	すべて	1	許可	なし	なし
<input type="checkbox"/> 5	すべて	すべて	すべて	すべて	すべて	すべて	すべて	拒否	なし	なし

ルールの移動
移動 ● 選択したルールの一つ上に移動 ○ 選択したルールの一つ下に移動 (ルール番号)

移動 編集 削除

- 10** 画面左のメニューで「MAC ACL」をクリックします。

- 11** ACLグループ名に「Public_Wi-Fi_Uplink」と入力して、「適用」をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> Public_Wi-Fi_Uplink	
<input type="checkbox"/> Public_Wi-Fi_Downlink	5/10 詳細

適用 名前の変更 削除

- 12** 手順11で追加した「Public_Wi-Fi_Uplink」の「詳細」をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> <input type="text"/>	
<input type="checkbox"/> Public_Wi-Fi_Downlink	5/10 詳細
<input type="checkbox"/> Public_Wi-Fi_Uplink	0/10 詳細

適用 名前の変更 削除

13 本製品(FS-M1266)のMACから送信されるパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	手動 アドレス: 本製品(FS-M1266)の有線MACアドレス マスク: 00:00:00:00:00:00
イーサertype	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Uplink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	手動 アドレス: XX:XX:XX:XX:XX:XX マスク: 00:00:00:00:00:00 (例: 00:11:22:33:44:55)
イーサertype	すべて (0600-FFFF Hex)
VLAN	すべて
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

14 続けて、管理用VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	1
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Uplink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
イーサertype	すべて (0600-FFFF Hex)
VLAN	1
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

15 続けて、手順13～14以外の通信をすべて禁止するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	拒否
Egressキュー	なし
リダイレクトポート	なし

16 ここまで登録したら、手順13～15の内容が正しく設定されているかを確認します。

正しく設定されている場合は、ACLルール一覧が以下のように表示されます。

Step 6 L2スイッチにACLポート設定をする

Step 5で登録したACLルールをL2スイッチに適用します。

1 ACLポート設定画面を表示します。

[詳細設定] - [ACL] - [ポート設定]画面を表示します。

2 ACLグループ名で、アクセスポイントを接続しているポートに対し、「Public_Wi-Fi_Downlink」のルールを適用します。

「Public_Wi-Fi_Downlink」を選択し、2～7にチェックをつけて[適用]をクリックします。

ポート設定

ポート設定	
有効なIPv4/MAC ACLルール数	0/126
有効なIPv6 ACLルール数	0/64
ACLグループ名	Public_Wi-Fi_Downlink
ポート選択	
1	2
3	4
5	6
7	8
<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>

適用

3 手順2と同様に、本製品(FS-M1266)を接続しているポートに対し、「Public_Wi-Fi_Uplink」のルールを適用します。

ACLグループ名で「Public_Wi-Fi_Uplink」を選択し、1にチェックをつけて[適用]をクリックします。

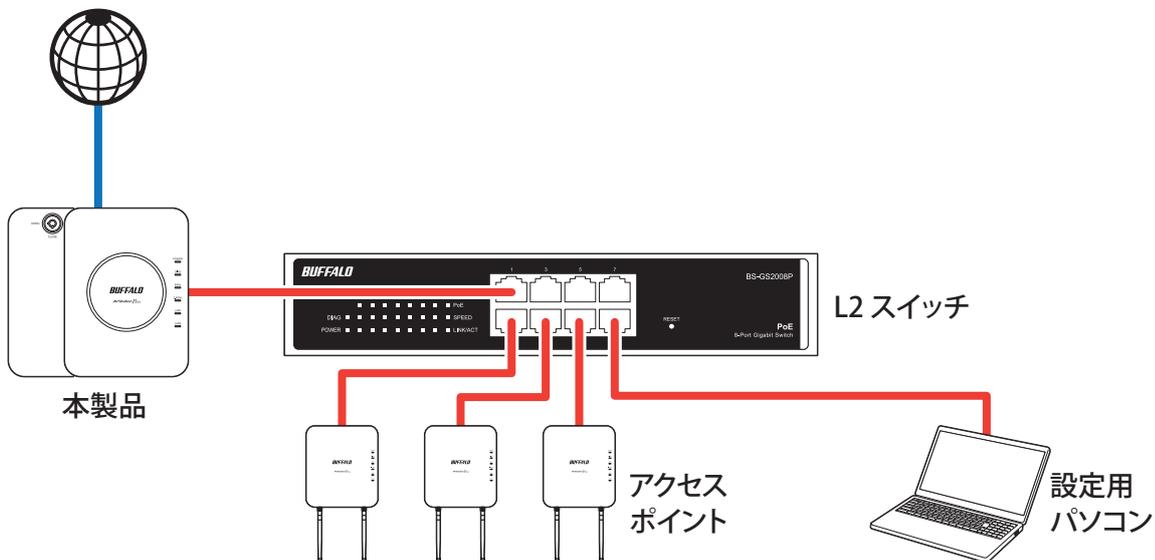
ポート設定

ポート設定	
有効なIPv4/MAC ACLルール数	5/126
有効なIPv6 ACLルール数	0/64
ACLグループ名	Public_Wi-Fi_Uplink
ポート選択	
1	2
3	4
5	6
7	8
<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

適用

Step 7 アクセスポイントをL2スイッチに接続する

L2スイッチのポート2～7に、アクセスポイントを接続します。



Step 8 アクセスポイントのIPアドレスを変更して設定画面を表示する

アクセスポイントすべてのIPアドレスを変更し、設定画面を表示します。

出荷時設定でお使いの場合、当社製アクセスポイントのIPアドレスは、DHCPサーバーから自動取得します。ここでは、アクセスポイントをより管理しやすくするために、「エアステーション設定ツール」を使って、アクセスポイントごとにIPアドレスを設定した後、設定画面を表示する方法を説明します。

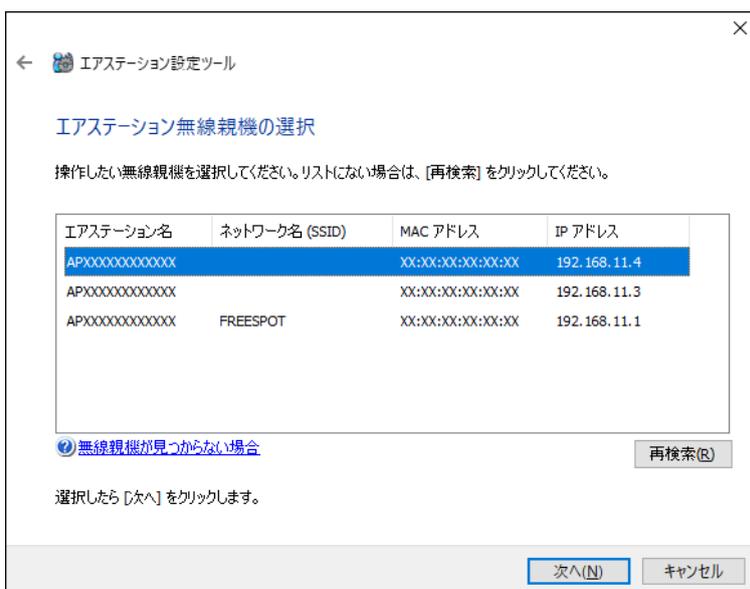
1 当社ホームページ(<https://86886.jp/airset/>)から「エアステーション設定ツール」をダウンロードして、設定用パソコンにインストールします。

2 「エアステーション設定ツール」を起動します。

3 「次へ」をクリックします。



4 アクセスポイントを選択して、「次へ」をクリックします。

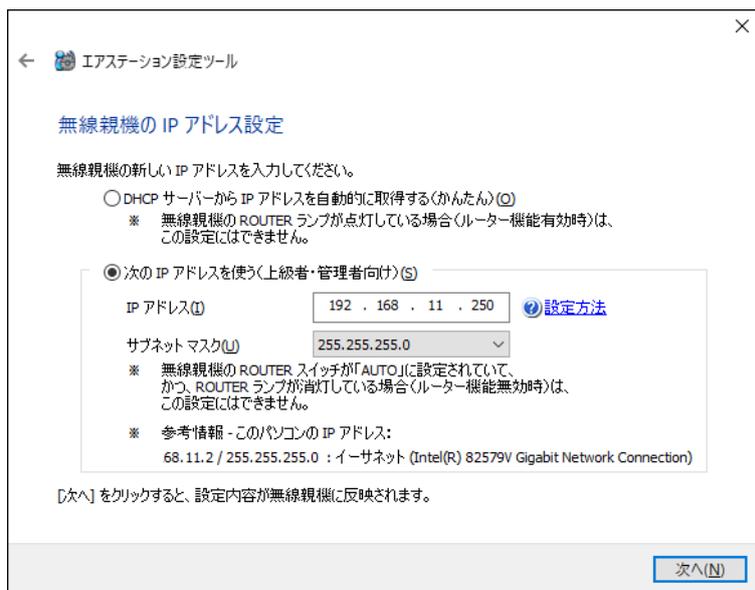


5 [この無線親機のIPアドレスを設定する]をクリックします。



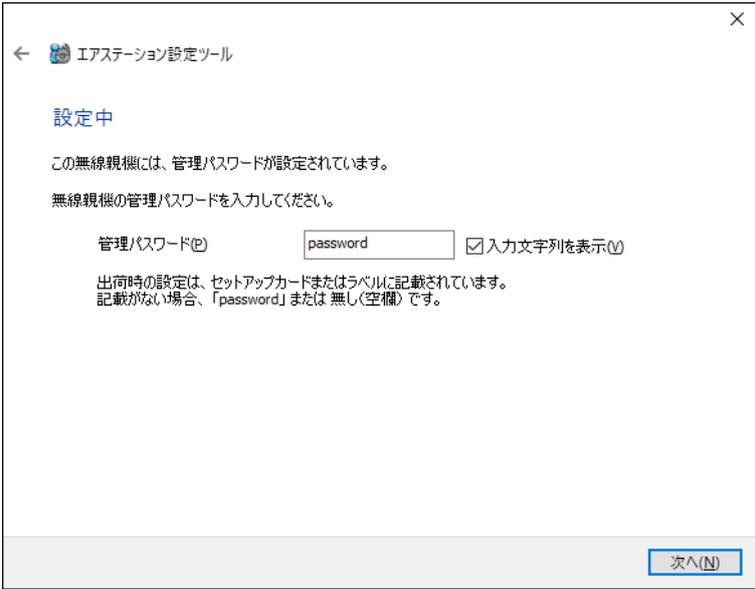
6 アクセスポイントのIPアドレスを変更します。

「次のIPアドレスを使う(上級者・管理者向け)」を選択し、IPアドレスを「192.168.11.250」など、サブネットマスクを「255.255.255.0」に設定して[次へ]をクリックします。



メモ: IPアドレスは、他のアクセスポイントと重複しない値を設定してください。

- 7** パスワードの入力画面が表示されたら、アクセスポイントに設定されている管理パスワードを入力して、[次へ]をクリックします。



← エアステーション設定ツール

設定中

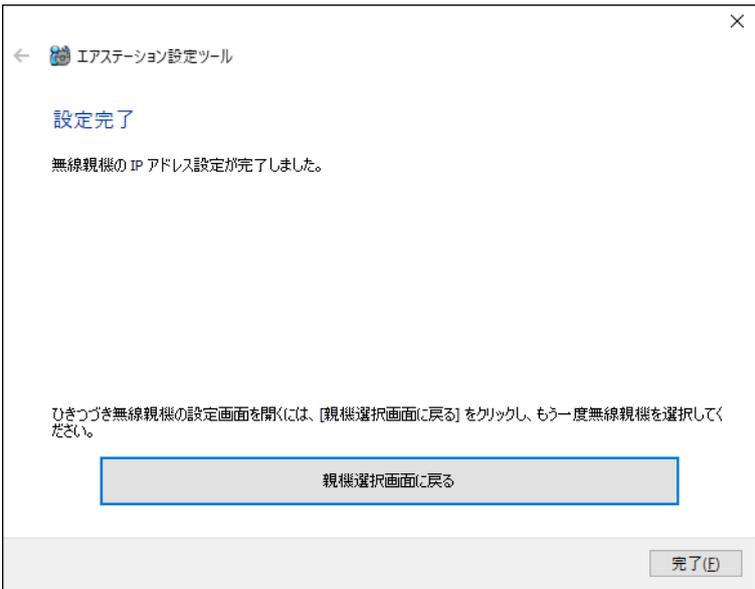
この無線親機には、管理パスワードが設定されています。
無線親機の管理パスワードを入力してください。

管理パスワード(P) 入力文字列を表示(V)

出荷時の設定は、セットアップカードまたはラベルに記載されています。
記載がない場合、「password」または「無し(空欄)」です。

次へ(N)

- 8** 以下の画面が表示されたら、[親機選択画面に戻る]をクリックします。



← エアステーション設定ツール

設定完了

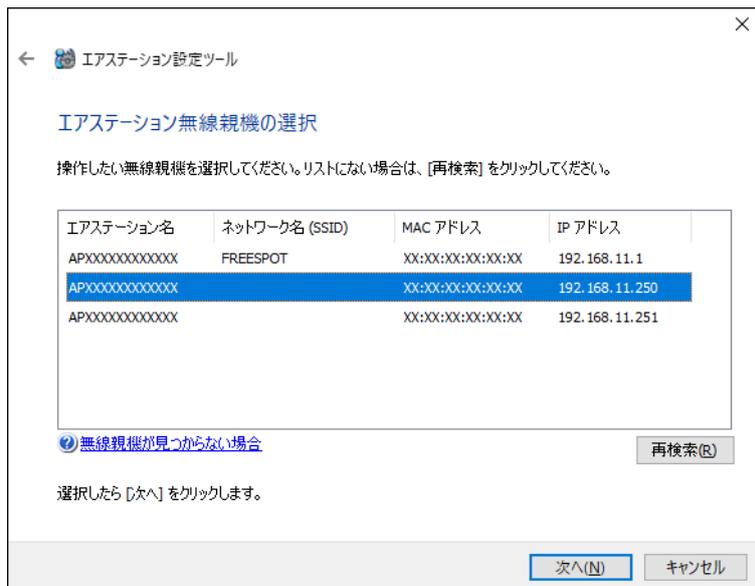
無線親機の IP アドレス設定が完了しました。

ひきつづき無線親機の設定画面を開くには、[親機選択画面に戻る] をクリックし、もう一度無線親機を選択してください。

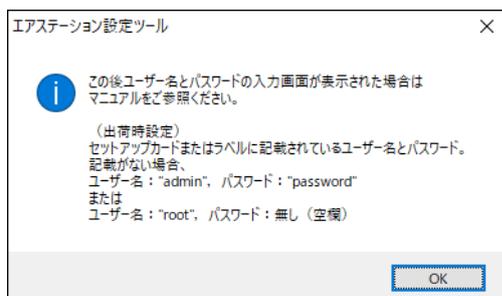
親機選択画面に戻る

完了(E)

- 9** 手順4～8の作業を、接続するアクセスポイントの台数分行います。

10 設定を行うアクセスポイントを選択して、[次へ]をクリックします。**11** [設定画面を開く(通常はこちら)]をクリックします。**12** [OK]をクリックします。

ブラウザが起動し、ログイン画面が表示されます。



13 アクセスポイントの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

メモ: 設定画面のウィンドウが開くと、エアステーション設定ツールのウィンドウに「無線LAN親機の設定画面を開きました」と表示されます。エアステーション設定ツールのウィンドウの[完了]をクリックしてください。エアステーション設定ツールが閉じます。

Step 9 アクセスポイントに公衆Wi-Fiの設定を行う

Step 7でL2スイッチに接続したアクセスポイントすべてに対して、公衆Wi-Fiの設定を行います。

1 [詳細設定]をクリックします。

2 SSID設定画面を表示します。

[無線設定] - [SSID設定]をクリックし、[新規追加]をクリックします。

SSID設定 - SSIDの編集								
ステアリング ポリシー設定								
ステアリング ポリシー <input type="text" value="無効"/>								
<input type="button" value="設定"/>								
SSID編集								
Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	無線の認証	暗号化
SSIDの設定は登録されていません								
<input type="button" value="新規追加"/>								

3 公衆Wi-Fi利用者用のSSID(Public_Wi-Fi)を設定します。

以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	Public_Wi-Fi
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
ステアリング	無効
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN ID: 3 追加VLAN ID: なし
ANY接続	許可する
プライバシーセパレーター	STAセパレーター
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	施設独自の設定
暗号化	
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
SSID	Public_Wi-Fi	
次の場合に有効にする	通常時と緊急時	
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz	
ステアリング	無効	
優先制御	通常	
VLAN ID	VLANモード	VLAN ID 追加VLAN ID
	Untagged Port	3
ANY接続	<input checked="" type="checkbox"/> 許可する	
プライバシーセパレーター	STAセパレーター	
ロードバランス(同時接続台数制限)	2.4GHz	5GHz
	128 /128	128 /128
無線の認証	認証を行わない	
暗号化	暗号化なし <small>「暗号化なし」に設定すると、第三者から通信内容を読み取られる可能性があります。</small>	
追加暗号化	追加暗号化を行わない	
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>		

メモ: アクセスポイントに接続している端末に対して公衆Wi-Fi利用者端末同士の通信を禁止するため、STAセパレーターを設定しています。

4 [設定]をクリックします。

Step 10 アクセスポイントにオーナー端末を接続するためのSSIDを設定する

Step 7でL2スイッチに接続したアクセスポイントすべてに対して、オーナー端末を接続するためのSSIDを設定します。

1 SSID設定画面を表示します。

[無線設定] - [SSID設定]をクリックし、[新規追加]をクリックします。

SSID設定 - SSIDの編集

ステアリング ポリシー設定

ステアリング ポリシー

SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	無線の認証	暗号化	
1	有効	Public_Wi-Fi3		<input type="radio"/>	<input type="radio"/>	無効	認証を行わない	暗号化なし	<input type="button" value="編集"/> <input type="button" value="削除"/>

2 オーナー用SSIDの設定を行います。

以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	任意のSSID(例:Buffalo)
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
ステアリング	無効
優先制御	優先
VLAN ID	VLANモード: Untagged VLAN ID: 1 追加VLAN ID: なし
ANY接続	許可する
プライバシーセパレーター	使用しない
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	WPA2 Personal
暗号化方式	AES
キー更新間隔	60分
事前共有キー	任意の事前共有キー(例:buffalo12345678)
Management Frame Protection	無効
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効						
SSID	Buffalo						
次の場合に有効にする	通常時と緊急時						
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz						
ステアリング	無効						
優先制御	優先						
VLAN ID	<table border="1"> <thead> <tr> <th>VLANモード</th> <th>VLAN ID</th> <th>追加VLAN ID</th> </tr> </thead> <tbody> <tr> <td>Untagged Port</td> <td>1</td> <td></td> </tr> </tbody> </table>	VLANモード	VLAN ID	追加VLAN ID	Untagged Port	1	
VLANモード	VLAN ID	追加VLAN ID					
Untagged Port	1						
ANY接続	<input checked="" type="checkbox"/> 許可する						
プライバシーセパレーター	使用しない						
ロードバランス(同時接続台数制限)	<table border="1"> <thead> <tr> <th>2.4GHz</th> <th>5GHz</th> </tr> </thead> <tbody> <tr> <td>128 / 128</td> <td>128 / 128</td> </tr> </tbody> </table>	2.4GHz	5GHz	128 / 128	128 / 128		
2.4GHz	5GHz						
128 / 128	128 / 128						
無線の認証	WPA2 Personal						
暗号化方式	AES						
キー更新間隔	60分						
事前共有キー	buffalo12345678						
Management Frame Protection	無効						
追加認証	追加認証を行わない						
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>							

メモ: オーナー端末は、制限なく通信できるようにするため、プライバシーセパレーターは「使用しない」に設定します。

3 [設定]をクリックします。

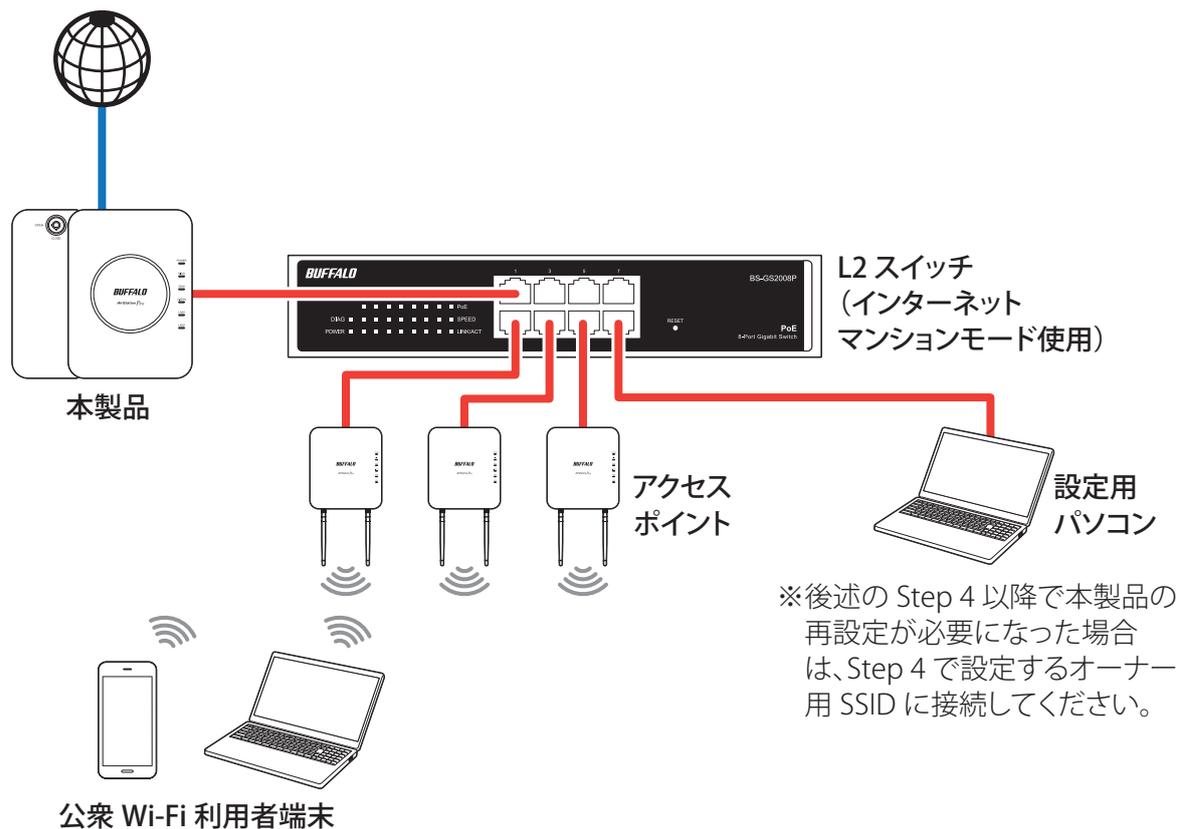
以上で設定は完了です。

例3:道の駅や商店街などの中規模施設に公衆Wi-Fiを新規導入したい(公衆Wi-Fi利用者端末だけを接続する場合)

本製品、L2スイッチ、アクセスポイントなどを組み合わせて、中規模施設に公衆Wi-Fiを新規導入する方法を説明します。

前述の「例2」との違いは、L2スイッチの設定とオーナー端末をアクセスポイントに接続するかどうかです。本構成では、L2スイッチのインターネットマンションモードを使用し、オーナー端末を接続しない簡易的な設定をする場合を想定しています。

構成例



条件

- 公衆Wi-Fi利用者は、本製品とは別のアクセスポイントに接続させる。
- 本製品は、ゲートウェイ機能のみ使用し、無線機能は必ずOFFにする。
(ONにした場合、ほかのアクセスポイントに接続した端末と本製品に接続した端末が通信可能になるなど、セキュリティーリスクになります)
- 上記のアクセスポイントには、公衆Wi-Fi利用者端末だけが接続し、オーナー端末は接続しない。
- 公衆Wi-Fi利用者端末同士の通信を禁止する。

制限事項

上記の構成例のように構築した後、本製品の設定画面を表示する場合は、後述の「Step 4 本製品にオーナー用SSIDを設定し、VLAN設定を変更する」で設定したオーナー用SSIDに接続する必要があります。

設定に使用する機器

- 本製品(FS-M1266)
- インターネットマンションモードに対応したL2スイッチ(BS-GS2008Pなど)
- アクセスポイント(WAPM-1266Rなど)
- 設定用パソコン

メモ:

- L2スイッチやアクセスポイントの推奨機器は、当社ホームページ(<https://www.buffalo.jp/product/detail/fs-m1266.html>)を参照してください。
- L2スイッチがPoEに対応していない場合は、別売のACアダプタ(WLE-OP-AC12C)をご用意ください。

Step 1 本製品を設置する

本製品の設置や初期設定(インターネットの接続設定、FREESPOT管理者登録情報の設定、FREESPOTマップの登録など)は、本書の第1章を参照して設定してください。

Step 2 設定に必要なツールをダウンロードする

本製品の設置が完了したら、L2スイッチやアクセスポイントの設定に必要なツールをダウンロードします。当社ホームページより、下記のツールをダウンロードしてください。

- ビジネススイッチ設定ツール(https://www.buffalo.jp/support/download/detail/?dl_contents_id=60665)
- エアステーション設定ツール(<https://86886.jp/airset/>)

ツールのダウンロードが完了したら、前述の「構成例」にあわせて配線し、「Step 3 公衆Wi-FiのVLANの設定を行う」へ進んでください。

メモ:

- 本製品のLAN端子は、L2スイッチのポート1に接続してください。
- 設定用パソコンは、L2スイッチのポート8に接続してください。

Step 3 公衆Wi-FiのVLANの設定を行う

公衆Wi-FiのVLANを有効にします。

1 本製品の設定画面を表示します。

設定画面の表示方法は、第1章の「Step 1 設定画面を表示する」を参照してください。

2 [詳細設定]をクリックします。

3 公衆Wi-FiのVLANの設定を行います。

[WAN/LAN] - [LAN設定]画面にある「CUSTOM_0」(3行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN	有効
VLAN名	任意のVLAN名(例:Public_Wi-Fi)
VLAN ID	3
IPアドレス	IPアドレス: 192.168.13.1 サブネットマスク: 255.255.255.0
DHCPサーバー	割り当てIPアドレス: 192.168.13.2から128台 除外アドレス: 空欄 リース期間: 1時間
i-フィルター	使用しない
SPAMメール対策	使用する メール送信数制限: 20件/分
ポップアップテクノロジー	使用する 広告URL: 接続時に表示させたいポータル画面のURL 広告表示間隔: 0秒
接続時間制限	使用する 接続回数: 3回/日 接続許可時間: 30分/回
公衆無線LAN利用者認証	利用者認証: 使用する ゲスト方式認証: 使用しない SNSアカウント認証: 使用する Wi-Cert Web-API認証: 使用しない 認証画面バナーの汎用表記: 使用しない 認証前HTTPS通信制限: 使用する

VLAN情報の編集

VLAN		<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
VLAN名		Public_Wi-Fi	
VLAN ID		3	
IP アドレス		IP アドレス	192.168.13.1
		サブネットマスク	255.255.255.0
DHCP サーバー		割り当て IP アドレス	192.168.13.2 から 128 台
		除外アドレス	
		リース期間	1 時間

公衆無線LAN関連設定

i-フィルター	<input type="checkbox"/> 使用する フィルターレベル 公衆
SPAMメール対策	<input checked="" type="checkbox"/> 使用する メール送信数制限 20 件/分
ポップアップテクノロジー	<input checked="" type="checkbox"/> 使用する 広告URL http://xxx.xxx.xxx.xxx/ 広告表示間隔 0 秒
接続時間制限	<input checked="" type="checkbox"/> 使用する 接続回数 3 回/日 接続許可時間 30 分/回
公衆無線LAN利用者認証	利用者認証 <input checked="" type="checkbox"/> 使用する 利用者認証オプション ゲスト方式認証 <input type="checkbox"/> 使用する SNSアカウント認証 <input checked="" type="checkbox"/> 使用する Wi-Cert Web-API認証 <input type="checkbox"/> 使用する 認証画面バナーの汎用表記 <input type="checkbox"/> 使用する 認証前HTTPS通信制限 <input checked="" type="checkbox"/> 使用する

メモ: 各内容の詳細は、ユーザーマニュアルを参照してください。

Step 4 本製品にオーナー用SSIDを設定し、VLAN設定を変更する

本製品にオーナー用SSIDを設定し、VLAN設定を変更します。

1 オーナー用SSIDの設定を行います。

[無線設定] - [SSID設定]画面にある[新規追加]をクリックし、以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	任意のSSID(例:Buffalo)
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
優先制御	優先
VLAN ID	VLANモード: Untagged VLAN: Management VLAN ID: 1
ANY接続	許可する
プライバシーセパレーター	使用しない
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	WPA2-PSK
暗号化方式	AES
キー更新間隔	60分
事前共有キー	任意の事前共有キー(例:buffalo12345678)
Management Frame Protection	無効
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効						
SSID	<input type="text" value="Buffalo"/>						
次の場合に有効にする	<input type="text" value="通常時と緊急時"/>						
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz						
優先制御	<input type="text" value="優先"/>						
VLAN ID	<table border="1"> <thead> <tr> <th>VLANモード</th> <th>VLAN</th> <th>VLAN ID</th> </tr> </thead> <tbody> <tr> <td><input type="text" value="Untagged"/></td> <td><input type="text" value="Management"/></td> <td><input type="text" value="1"/></td> </tr> </tbody> </table>	VLANモード	VLAN	VLAN ID	<input type="text" value="Untagged"/>	<input type="text" value="Management"/>	<input type="text" value="1"/>
VLANモード	VLAN	VLAN ID					
<input type="text" value="Untagged"/>	<input type="text" value="Management"/>	<input type="text" value="1"/>					
ANY接続	<input checked="" type="checkbox"/> 許可する						
プライバシーセパレーター	<input type="text" value="使用しない"/>						
ロードバランス(同時接続台数制限)	<table border="1"> <thead> <tr> <th>2.4GHz</th> <th>5GHz</th> </tr> </thead> <tbody> <tr> <td><input type="text" value="128"/> / <input type="text" value="128"/></td> <td><input type="text" value="128"/> / <input type="text" value="128"/></td> </tr> </tbody> </table>	2.4GHz	5GHz	<input type="text" value="128"/> / <input type="text" value="128"/>	<input type="text" value="128"/> / <input type="text" value="128"/>		
2.4GHz	5GHz						
<input type="text" value="128"/> / <input type="text" value="128"/>	<input type="text" value="128"/> / <input type="text" value="128"/>						
無線の認証	<input type="text" value="WPA2-PSK"/>						
暗号化方式	<input type="text" value="AES"/>						
キー更新間隔	<input type="text" value="60"/> 分						
事前共有キー	<input type="text" value="buffalo12345678"/>						
Management Frame Protection	<input type="text" value="無効"/>						
追加認証	<input type="text" value="追加認証を行わない"/>						
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>							

メモ: オーナー端末は、制限なく通信できるようにするため、プライバシーセパレーターは「使用しない」に設定します。

2 [設定]をクリックします。

3 VLAN設定を変更します。

[WAN/LAN] - [LAN設定]画面にあるインターフェース設定で、LANポートの設定を以下のように変更して[設定]をクリックします。

VLANモード	Untagged
VLAN	Public_Wi-Fi
VLAN ID	3

LAN側インターフェース設定

VLAN設定

No	状態	VLAN名	VLAN ID	IPアドレス	i-フィルター	SPAMメール対策	ポップアップ
1	有効	Management	1	192.168.11.1/24	無効	無効	無効
2	無効	FREESPOT	2	192.168.12.1/24	無効	有効	無効
3	有効	Public_Wi-Fi	3	192.168.13.1/24	無効	有効	無効
4	無効	CUSTOM_1	4	192.168.14.1/24	無効	有効	無効
5	無効	CUSTOM_2	5	192.168.15.1/24	無効	有効	無効

インターフェース設定

インターフェース	VLANモード	VLAN	VLAN ID
LANポート	Untagged	Public_Wi-Fi	3
SSID #1 [FREESPOT] 2.4GHz, 5GHz	Untagged	CUSTOM_1	2
SSID #2 [freespot'=SecurityPassword(AES)] 2.4GHz, 5GHz	Untagged	CUSTOM_2	2
SSID #3 [Buffalo] 2.4GHz, 5GHz	Untagged	Management	1

メモ: 手順3の設定を行うと、有線LANからは本製品の設定画面を表示できなくなります。もう一度本製品の設定画面を表示したい場合は、手順1で設定したオーナー用SSIDに接続してください。

4 設定用パソコンを再起動するなどして、設定用パソコンのIPアドレスを再取得します。

Step 5 L2スイッチのIPアドレスを変更して設定画面を表示する

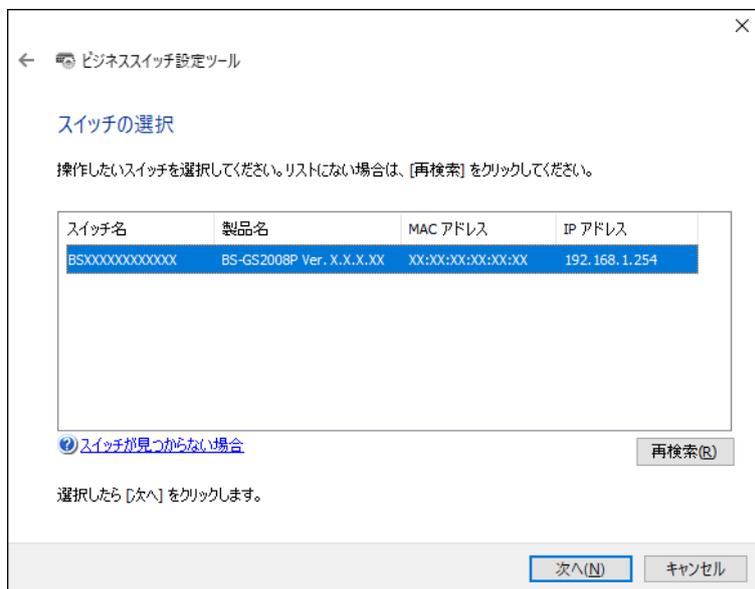
前述のStep 2でダウンロードした「ビジネススイッチ設定ツール」を使ってL2スイッチのIPアドレスを変更し、設定画面を表示します。

1 「ビジネススイッチ設定ツール」を起動します。

2 [次へ]をクリックします。



3 L2スイッチを選択して、[次へ]をクリックします。



4 設定画面にアクセスするためには、セグメントを合わせる必要があります。

[このスイッチのIPアドレスを設定する]をクリックします。

← ビジネススイッチ設定ツール

操作の選択

次のスイッチが選択されました。おこないたい操作を選択してください。

スイッチ名	製品名	MAC アドレス	IP アドレス
BSXXXXXXXXXXXX	BS-GS2008P Ver. X.X.X.XX	XX:XX:XX:XX:XX:XX	192.168.1.254

設定画面を開く(W)
(通常はこちら)

このスイッチの IP アドレスを設定する(U)
(上級者・管理者向け)

5 L2スイッチのIPアドレスを変更します。

[次のIPアドレスを使う(上級者・管理者向け)]を選択し、IPアドレスを「192.168.13.254」、サブネットマスクを「255.255.255.0」に設定して[次へ]をクリックします。

← ビジネススイッチ設定ツール

スイッチの IP アドレス設定

スイッチの新しい IP アドレスを入力してください。

DHCP サーバーから IP アドレスを自動的に取得する(かんたん)(D)

次の IP アドレスを使う(上級者・管理者向け)(S)

IP アドレス(U) [設定方法](#)

サブネットマスク(U)

※ 参考情報 - このパソコンの IP アドレス:
68.13.2 / 255.255.255.0 : イーサネット (Intel(R) 82579V Gigabit Network Connection)

[次へ] をクリックすると、設定内容がスイッチに反映されます。

次へ(N)

- 6 パスワードの入力画面が表示されたら、L2スイッチに設定されている管理パスワードを入力して、[次へ]をクリックします。



← ビジネススイッチ設定ツール

設定中

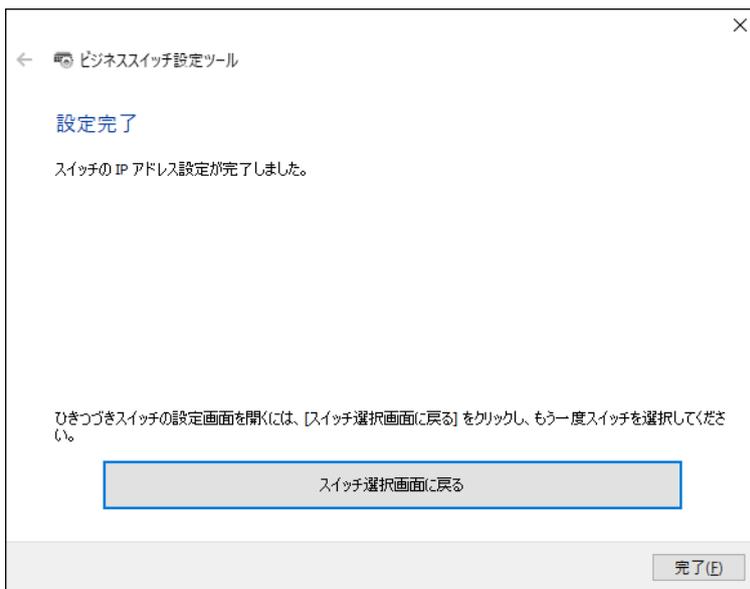
このスイッチには、管理パスワードが設定されています。
スイッチの管理パスワードを入力してください。

管理パスワード(P) 入力文字列を表示(V)

出荷時の設定は、「password」または「無し(空欄)」です。

次へ(N)

- 7 以下の画面が表示されたら、[スイッチ選択画面に戻る]をクリックします。



← ビジネススイッチ設定ツール

設定完了

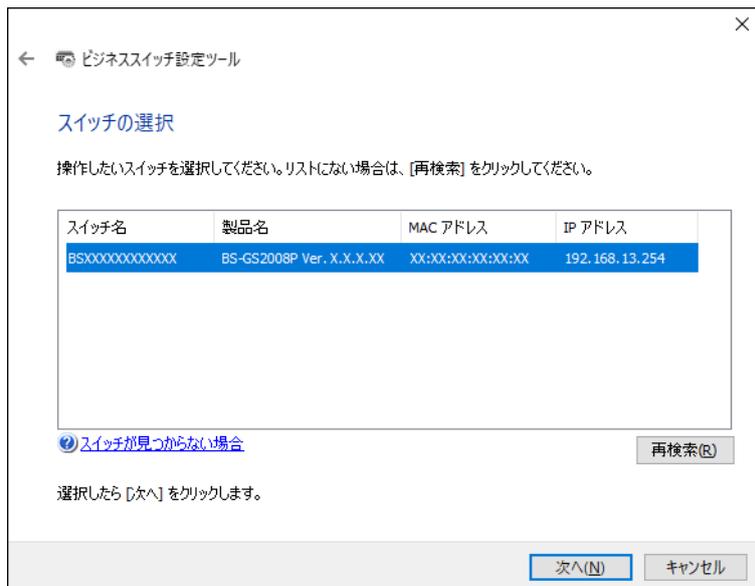
スイッチの IP アドレス設定が完了しました。

ひきつづきスイッチの設定画面を開くには、[スイッチ選択画面に戻る] をクリックし、もう一度スイッチを選択してください。

スイッチ選択画面に戻る

完了(F)

8 L2スイッチを選択して、「次へ」をクリックします。

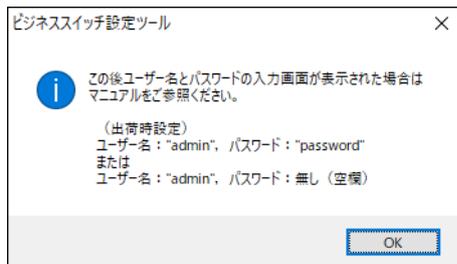


9 「設定画面を開く(通常はこちら)」をクリックします。



10 [OK]をクリックします。

ブラウザーが起動し、ログイン画面が表示されます。



11 L2スイッチの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

メモ: 設定画面のウィンドウが開くと、ビジネススイッチ設定ツールのウィンドウに「スイッチの設定画面を開きました」と表示されます。ビジネススイッチ設定ツールのウィンドウの[完了]をクリックしてください。ビジネススイッチ設定ツールが閉じます。

Step 6 L2スイッチをインターネットマンションモードに設定する

L2スイッチの設定画面でインターネットマンションモードの設定を行います。

1 [基本設定] - [VLAN] - [VLAN設定]画面を表示します。

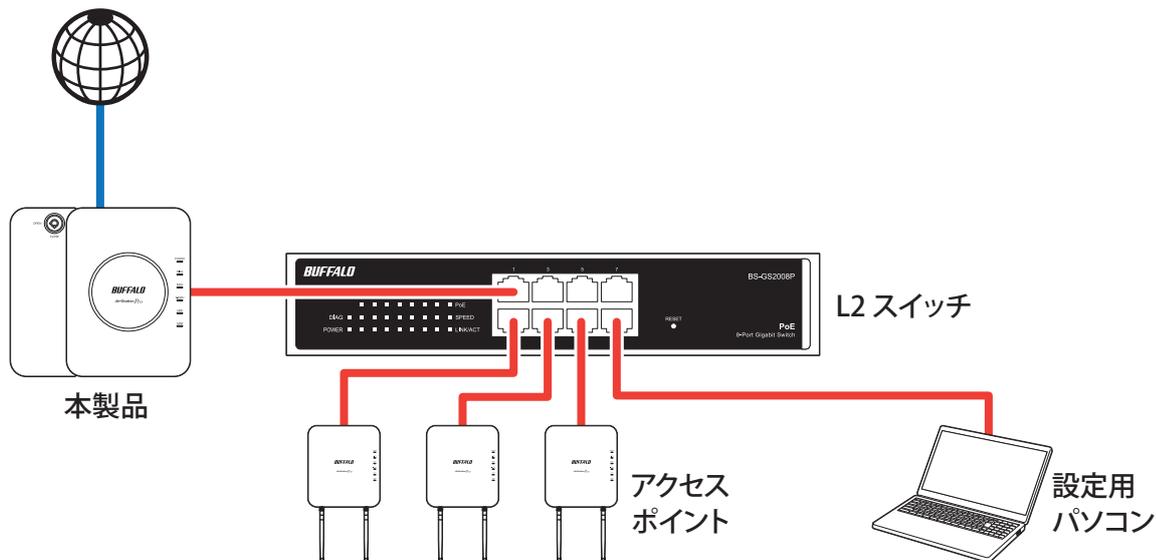
2 VLANモードに「インターネットマンション」を選択し、以下のように設定して[適用]をクリックします。

Uplink	1, 8
Downlink	2~7

メモ: インターネットマンションモードが選択できないときは、L2スイッチがレイヤー3モードに設定されている可能性があります。その場合は、[基本設定] - [ルーティング] - [レイヤー設定]から「レイヤー2モード」を選択してください。

Step 7 アクセスポイントをL2スイッチに接続する

L2スイッチのポート2～7に、アクセスポイントを接続します。



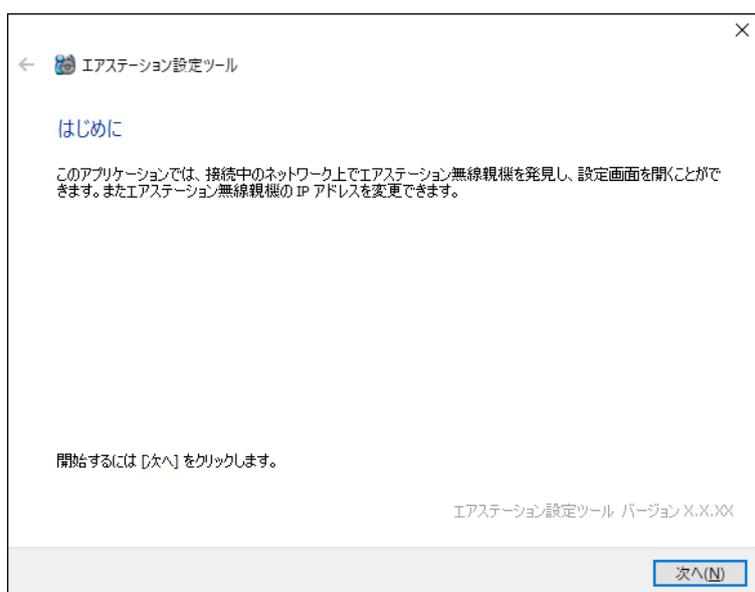
Step 8 アクセスポイントのIPアドレスを変更して設定画面を表示する

アクセスポイントすべてのIPアドレスを変更し、設定画面を表示します。

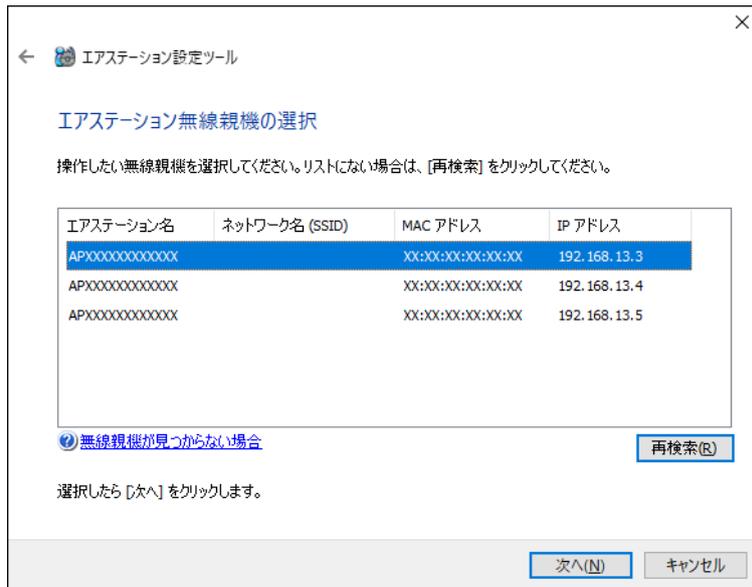
出荷時設定でお使いの場合、当社製アクセスポイントのIPアドレスは、DHCPサーバーから自動取得します。ここでは、アクセスポイントをより管理しやすくするために、前述のStep 2でダウンロードした「エアステーション設定ツール」を使って、アクセスポイントごとにIPアドレスを設定した後、設定画面を表示する方法を説明します。

1 「エアステーション設定ツール」を起動します。

2 [次へ]をクリックします。



3 アクセスポイントを選択して、[次へ]をクリックします。



4 [この無線親機のIPアドレスを設定する]をクリックします。



5 アクセスポイントのIPアドレスを変更します。

「次のIPアドレスを使う(上級者・管理者向け)」を選択し、IPアドレスを「192.168.13.250」など、サブネットマスクを「255.255.255.0」に設定して[次へ]をクリックします。

← エアステーション設定ツール

無線親機の IP アドレス設定

無線親機の新しい IP アドレスを入力してください。

DHCP サーバーから IP アドレスを自動的に取得する(かんたん) (D)

※ 無線親機の ROUTER ランプが点灯している場合(ルーター機能有効時)は、この設定にはできません。

次の IP アドレスを使う(上級者・管理者向け) (S)

IP アドレス (I) [設定方法](#)

サブネット マスク (M)

※ 無線親機の ROUTER スイッチが「ALTO」に設定されていて、かつ、ROUTER ランプが消灯している場合(ルーター機能無効時)は、この設定にはできません。

※ 参考情報 - このパソコンの IP アドレス:
68.13.2 / 255.255.255.0 : イーサネット (Intel(R) 82579V Gigabit Network Connection)

[次へ] をクリックすると、設定内容が無線親機に反映されます。

[次へ\(N\)](#)

メモ: IPアドレスは、他のアクセスポイントと重複しない値を設定してください。

6 パスワードの入力画面が表示されたら、アクセスポイントに設定されている管理パスワードを入力して、[次へ]をクリックします。

← エアステーション設定ツール

設定中

この無線親機には、管理パスワードが設定されています。

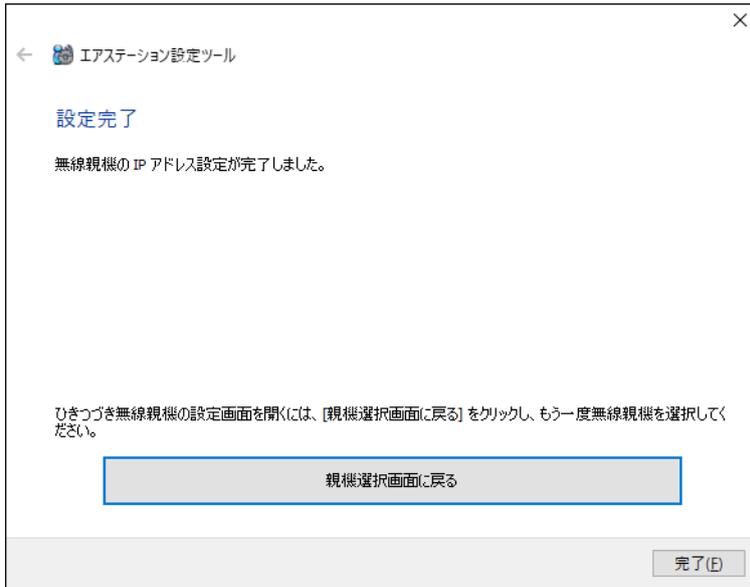
無線親機の管理パスワードを入力してください。

管理パスワード (P) 入力文字列を表示 (V)

出荷時の設定は、セットアップカードまたはラベルに記載されています。
記載がない場合、「password」または無し(空欄)です。

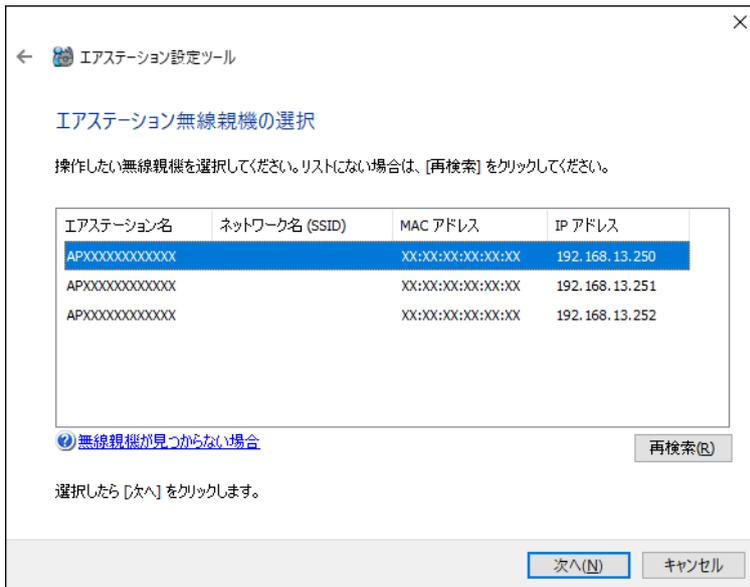
[次へ\(N\)](#)

7 以下の画面が表示されたら、[親機選択画面に戻る]をクリックします。



8 手順3～7の作業を、接続するアクセスポイントの台数分行います。

9 設定を行うアクセスポイントを選択して、[次へ]をクリックします。

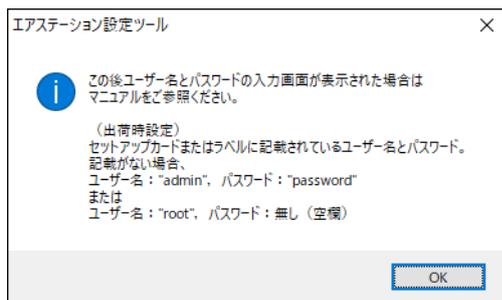


10 [設定画面を開く(通常はこちら)]をクリックします。



11 [OK]をクリックします。

ブラウザが起動し、ログイン画面が表示されます。



12 アクセスポイントの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。



メモ:

- 設定画面のウィンドウが開くと、エアステーション設定ツールのウィンドウに「無線LAN親機の設定画面を開きました」と表示されます。エアステーション設定ツールのウィンドウの[完了]をクリックしてください。エアステーション設定ツールが閉じます。
- 公衆Wi-Fi利用者は、次のStep9で設定するSSIDに接続します。公衆Wi-Fi利用者からアクセスポイントやL2スイッチの設定画面にアクセスされることを防ぐため、事前に管理ユーザー名や管理パスワードを任意のものに変更しておくことをおすすめします。

Step 9 アクセスポイントに公衆Wi-Fiの設定を行う

Step 8でL2スイッチに接続したアクセスポイントすべてに対して、公衆Wi-Fiの設定を行います。

1 [詳細設定]をクリックします。

2 SSID設定画面を表示します。

[無線設定] - [SSID設定]をクリックし、[新規追加]をクリックします。

SSID設定 - SSIDの編集

ステアリング ポリシー設定

ステアリング ポリシー

SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	無線の認証	暗号化
SSIDの設定は登録されていません								

3 公衆Wi-Fi利用者用のSSID(Public_Wi-Fi)を設定します。

以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	Public_Wi-Fi
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
ステアリング	無効
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN ID: 1 追加VLAN ID: なし
ANY接続	許可する
プライバシーセパレーター	STAセパレーター
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	施設独自の設定
暗号化	
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SSID	Public_Wi-Fi
次の場合に有効にする	通常時と緊急時
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
ステアリング	無効
優先制御	通常
VLAN ID	VLANモード: Untagged Port VLAN ID: 1 追加VLAN ID:
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	STAセパレーター
ロードバランス(同時接続台数制限)	2.4GHz: 128 /128 5GHz: 128 /128
無線の認証	認証を行わない
暗号化	暗号化なし <small>「暗号化なし」に設定すると、第三者から通信内容を読み取られる可能性があります。</small>
追加認証	追加認証を行わない
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>	

メモ: アクセスポイントに接続している端末に対して公衆Wi-Fi利用者端末同士の通信を禁止するため、STAセパレーターを設定しています。

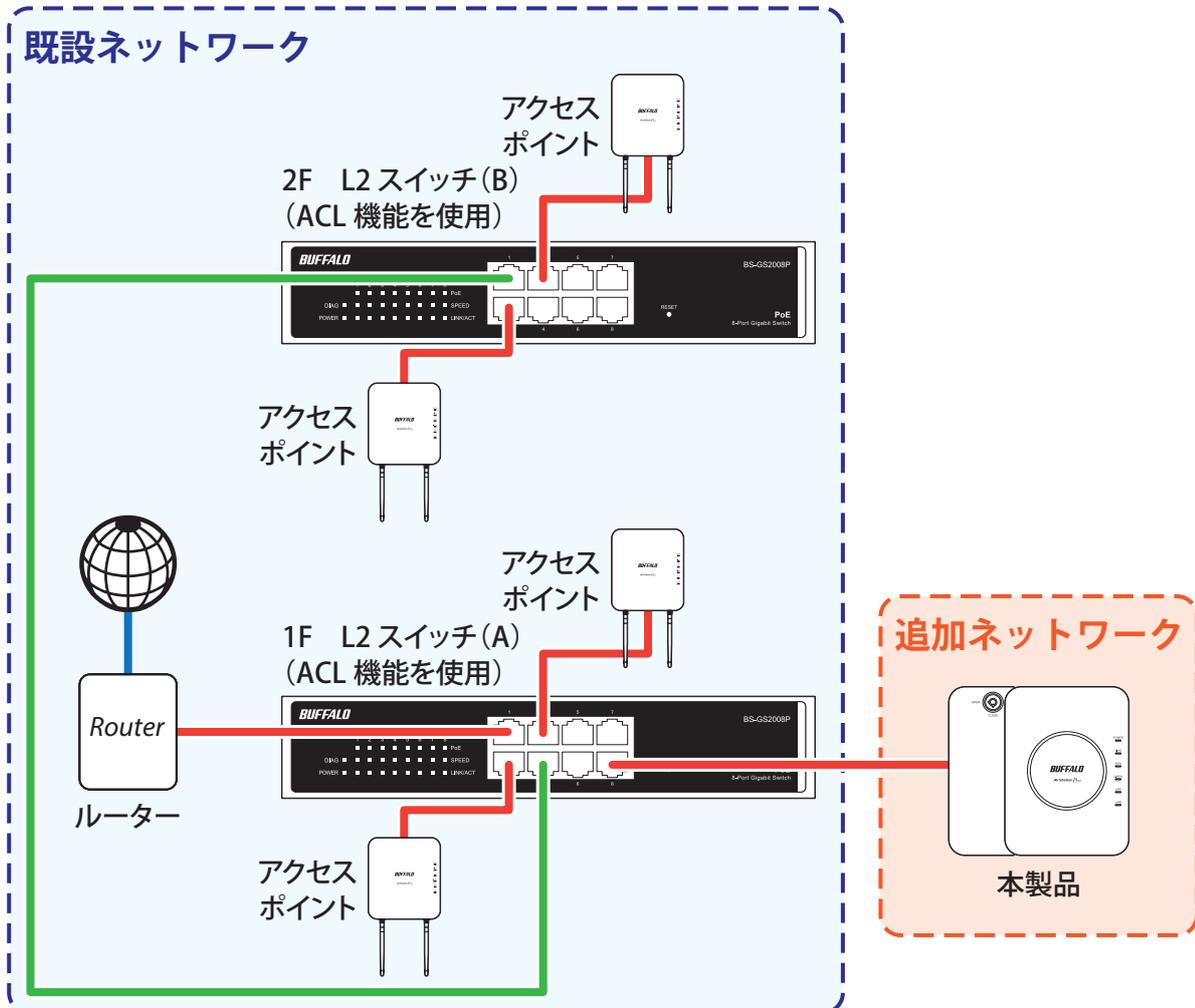
4 [設定]をクリックします。

以上で設定は完了です。

例4:既設のネットワークに公衆Wi-Fiを追加したい

ルーターやアクセスポイント、L2スイッチなどを使って構築された既設のネットワークに対して、公衆Wi-Fiを導入する方法を説明します。

構成例



既設セグメント情報

VLAN ID

Management VLAN(管理部): 1
 SOUMU VLAN(総務部): 2
 EIGYO VLAN(営業部): 3

各VLANの割り当てサブネット

Management VLAN(管理部): 192.168.1.0/24
 SOUMU VLAN(総務部): 192.168.2.0/24
 EIGYO VLAN(営業部): 192.168.3.0/24

各VLANのゲートウェイ

Management VLAN(管理部): なし
 SOUMU VLAN(総務部): 192.168.2.1

EIGYO VLAN(営業部): 192.168.3.1

Management VLAN所属のネットワーク機器とIPアドレス

ルーター: 192.168.1.1
 L2スイッチ(A): 192.168.1.101
 L2スイッチ(B): 192.168.1.102
 アクセスポイント: 192.168.1.201~192.168.1.204

既設ルーター情報

所属VLANとIPアドレス

Management(管理部): 192.168.1.1
 SOUMU(総務部): 192.168.2.1
 EIGYO(営業部): 192.168.3.1

既設L2スイッチ(A)情報

各ポートの用途

ポート1: ルーター接続用
 ポート2~3: アクセスポイント接続用
 ポート4: L2スイッチ(B)接続用
 ポート5~8: 未使用(管理用)

各ポートのVLAN設定

		ポート							
		1	2	3	4	5	6	7	8
VLAN ID	1	T	T	T	T	U	U	U	U
	2	T	T	T	T	-	-	-	-
	3	T	T	T	T	-	-	-	-
PVID		1	1	1	1	1	1	1	1

既設L2スイッチ(B)情報

各ポートの用途

- ポート1: L2スイッチ(A)接続用
- ポート2~3: アクセスポイント接続用
- ポート4~8: 未使用(管理用)

各ポートのVLAN設定

		ポート							
		1	2	3	4	5	6	7	8
VLAN ID	1	T	T	T	U	U	U	U	U
	2	T	T	T	-	-	-	-	-
	3	T	T	T	-	-	-	-	-
PVID		1	1	1	1	1	1	1	1

既設アクセスポイント情報

1Fに設置しているアクセスポイント2台

- SSID: SOUMU
- VLAN ID: 2
- プライバシーセパレーター: なし

2Fに設置しているアクセスポイント2台

- SSID: EIGYO
- VLAN ID: 3
- プライバシーセパレーター: なし

本事例で設定する内容

- 来訪者用にインターネット環境(公衆Wi-Fi)を提供できるように本製品を追加する。
- 本製品は、ゲートウェイ機能のみ使用し、無線機能はOFFにする。
- 公衆Wi-Fi利用者から、業務用ネットワーク(Management、SOUMU、EIGYO)にアクセスできないようにする。
- 公衆Wi-Fiに接続した来訪者同士で通信できないようにする。

設定に使用する機器

- TagVLANに対応したルーター(既設品)
- ACL機能に対応したL2スイッチ(BS-GS2008Pなどの既設品)
- アクセスポイント(WAPM-1266Rなどの既設品)
- 本製品(FS-M1266、新規導入)
- 設定用パソコン

メモ: L2スイッチがPoEに対応していない場合は、別売のACアダプタ(WLE-OP-AC12C)をご用意ください。

Step 1 ルーターに公衆Wi-FiのWAN側用セグメントを追加する

ルーターに公衆Wi-FiのWAN側用セグメント(VLAN ID: 4)を追加します。
ルーターの取扱説明書を参照して、以下の内容を設定してください。

VLAN名: FS_WAN_VLAN
VLAN ID: 4
IPアドレス: 192.168.4.1

上記に伴い、FS_WAN_VLANから既存のVLAN(SOUMU VLANやEIGYO VLAN)へのルーティングを禁止する設定もあわせて行ってください。

Step 2 本製品のWAN設定を行い、公衆Wi-FiのVLANを有効にする

本製品のWAN設定と公衆Wi-FiのVLANの設定を行います。

1 本製品のLAN端子に設定用パソコンを接続し、本製品の電源を入れます。

メモ: 本製品はまだ既設のネットワークには接続しないでください。

2 本製品の設定画面を表示します。

設定画面の表示方法は、第2章の「Step 1 設定画面を表示する」を参照してください。

3 [詳細設定]をクリックします。

4 WAN設定を行います。

[WAN/LAN] – [WAN設定]画面で、以下のように設定して[設定]をクリックします。

VLAN名	WAN
VLAN ID	4 前述のStep 1で設定したVLAN ID
IPアドレスの取得方法	手動設定
IPアドレス	IPアドレス: 192.168.4.2 サブネットマスク: 255.255.255.0
デフォルトゲートウェイ	192.168.4.1
DNS	任意のDNSサーバーのアドレス
MTU	1500
WAN側MACアドレス	デフォルトのMACアドレスを使用

WAN側インターフェース設定	
VLAN名	WAN
VLAN ID	4
IP アドレスの取得方法	<input checked="" type="radio"/> 手動設定 <input type="radio"/> DHCP クライアント <input type="radio"/> PPPoE クライアント
IP アドレス	IP アドレス <input type="text" value="192.168.4.2"/> サブネットマスク <input type="text" value="255.255.255.0"/>
デフォルトゲートウェイ	<input type="text" value="192.168.4.1"/>
DNS	プライマリーサーバー: <input type="text" value="192.168.4.1"/> セカンダリーサーバー: <input type="text"/>
MTU	<input type="text" value="1500"/>
WAN側MACアドレス	<input checked="" type="radio"/> デフォルトのMACアドレスを使用(XX:XX:XX:XX:XX:XX) <input type="radio"/> 手動設定 <input type="text"/>
<input type="button" value="設定"/>	

5 公衆Wi-FiのVLANの設定を行います。

[WAN/LAN] - [LAN設定]画面にある「CUSTOM_0」(3行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN	有効
VLAN名	任意のVLAN名(例:Public_Wi-Fi)
VLAN ID	5
IPアドレス	IPアドレス: 192.168.5.1 サブネットマスク: 255.255.255.0
DHCPサーバー	割り当てIPアドレス: 192.168.5.2から128台 除外アドレス: 空欄 リース期間: 1時間
i-フィルター	使用しない
SPAMメール対策	使用する メール送信数制限: 20件/分
ポップアップテクノロジー	使用する 広告URL: 接続時に表示させたいポータル画面のURL 広告表示間隔: 0秒
接続時間制限	使用する 接続回数: 3回/日 接続許可時間: 30分/回
公衆無線LAN利用者認証	利用者認証: 使用する ゲスト方式認証: 使用しない SNSアカウント認証: 使用する Wi-Cert Web-API認証: 使用しない 認証画面バナーの汎用表記: 使用しない 認証前HTTPS通信制限: 使用する

VLAN情報の編集

VLAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効		
VLAN名	Public_Wi-Fi		
VLAN ID	5		
IP アドレス	IP アドレス	192.168.5.1	
	サブネットマスク	255.255.255.0	
DHCP サーバー	割り当て IP アドレス	192.168.5.2	から 128 台
	除外アドレス		
	リース期間	1 時間	

公衆無線LAN関連設定

i-フィルター	<input type="checkbox"/> 使用する フィルターレベル 公衆
SPAMメール対策	<input checked="" type="checkbox"/> 使用する メール送信数制限 20 件/分
ポップアップテクノロジー	<input type="checkbox"/> 使用する 広告URL 広告表示間隔 0 秒
接続時間制限	<input checked="" type="checkbox"/> 使用する 接続回数 3 回/日 接続許可時間 30 分/回
公衆無線LAN利用者認証	利用者認証 <input checked="" type="checkbox"/> 使用する
	利用者認証オプション
	ゲスト方式認証 <input type="checkbox"/> 使用する
	SNSアカウント認証 <input checked="" type="checkbox"/> 使用する
	Wi-Cert Web-API認証 <input type="checkbox"/> 使用する
	認証画面バナーの汎用表記 <input type="checkbox"/> 使用する
	認証前HTTPS通信制限 <input checked="" type="checkbox"/> 使用する

修正保存 編集を終了して前の画面へ戻る

メモ: 各内容の詳細は、ユーザーマニュアルを参照してください。

6 管理VLANの設定を変更します。

[WAN/LAN] - [LAN設定]画面にある「Management」(1行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN名	Management
VLAN ID	1
IPアドレス	IPアドレス: 192.168.1.103 サブネットマスク: 255.255.255.0
ルーティング	ルーティングしない
DHCPサーバー	使用しない

VLAN情報の編集

VLAN名	Management		
VLAN ID	1		
IP アドレス	IP アドレス	192.168.1.103	
	サブネットマスク	255.255.255.0	
ルーティング	ルーティングしない		
DHCP サーバー	<input type="checkbox"/> 使用する		
	割り当て IP アドレス	192.168.1.1.2	から 32 台
	除外アドレス		
	リース期間	48 時間	
	デフォルトゲートウェイの通知	エアステーションのLAN側IPアドレス	
DNSサーバーの通知	エアステーションのLAN側IPアドレス		

修正保存 編集を終了して前の画面へ戻る

7 [設定]をクリックします。

Step 3 既設のL2スイッチ(A)のVLAN設定を変更し、ACLルールを登録する

1Fに設置されているL2スイッチ(A)のVLAN設定を変更し、以下の4点に関するACL(アクセスコントロールリスト)の設定を行います。

- 各々のアクセスポイントに接続した、公衆Wi-Fi利用者端末同士の通信を防ぐ。
- どのアクセスポイントに接続していても、営業部端末同士は通信を許可する。
- どのアクセスポイントに接続していても、総務部端末同士は通信を許可する。
- どのアクセスポイントに接続していても、管理部端末同士は通信を許可する。

1 前述のStep 2で使用した設定用パソコンを本製品から取り外して、L2スイッチ(A)のポート5~7のいずれかに接続します。

2 L2スイッチ(A)の設定画面を表示します。

設定用パソコンのWebブラウザを起動して、アドレス欄にL2スイッチ(A)のIPアドレス(192.168.1.101)を入力します。

3 L2スイッチ(A)の管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

4 続けて、公衆Wi-FiのWAN VLANを追加します。

以下のように設定して、[適用]をクリックします。

VLAN ID	4
VLAN名	Public_Wi-Fi_WAN
管理VLAN	チェックなし
Tagged	1、8
Untagged	なし
Not Member	2、3、4、5、6、7

ポート		1	2	3	4	5	6	7	8
Tagged	All	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Untagged	All	<input type="radio"/>							
Not Member	All	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

適用 リセット キャンセル

5 同様に、公衆Wi-FiのVLANを追加します。

以下のように設定して、[適用]をクリックします。

VLAN ID	5
VLAN名	Public_Wi-Fi
管理VLAN	チェックなし
Tagged	2、3、4、8
Untagged	なし
Not Member	1、5、6、7

VLANの追加/編集

VLAN ID (2-4094)

VLAN名

管理VLAN

ポート		1	2	3	4	5	6	7	8
Tagged	<input type="button" value="All"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Untagged	<input type="button" value="All"/>	<input type="radio"/>							
Not Member	<input type="button" value="All"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

6 VLANステータスが以下のようになったことを確認します。

VLANステータス

■	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.1.101	T	T	T	T	U	U	U	U	Management	Up
<input type="checkbox"/>	2	-	T	T	T	T	-	-	-	-	SOUMU	Down
<input type="checkbox"/>	3	-	T	T	T	T	-	-	-	-	EIGYO	Down
<input type="checkbox"/>	4	-	T	-	-	-	-	-	-	T	Public_Wi-Fi_WAN	Down
<input type="checkbox"/>	5	-	-	T	T	T	-	-	-	T	Public_Wi-Fi	Down
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		

T:Static Tagged U:Static Untagged -:Not Member X:有効

7 MAC ACL設定画面を表示します。

[詳細設定] - [ACL] - [MAC ACL]画面を表示します。

8 ACLグループ名に「Public_Wi-Fi_Downlink」と入力して、[適用]をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> Public_Wi-Fi_Downlink	

9 手順8で追加した「Public_Wi-Fi_Downlink」の「詳細」をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/>	
<input type="checkbox"/> Public_Wi-Fi_Downlink	0/10 詳細

[適用](#) [名前の変更](#) [削除](#)

10 本製品 (FS-M1266) のMAC宛でのユニキャスト通信を許可するルールを設定します。

以下のように設定して、「保存」をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: 本製品 (FS-M1266) の有線MACアドレス マスク: 00:00:00:00:00:00
送信元MACアドレス	すべて
イーサタイプ	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	手動 ▼ アドレス: XXXXX:XXX:XXX:XXX:XXX:XXX マスク: 00:00:00:00:00:00 (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて ▼ アドレス: マスク: (例: 00:11:22:33:44:55)
イーサタイプ	すべて ▼ (0600-FFFF Hex)
VLAN	すべて ▼
ACLの動作	
許可/拒否	許可 ▼
Egressキュー	なし ▼
リダイレクトポート	なし ▼
保存 戻る	

11 続けて、ブロードキャストMAC宛ての通信を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: FF:FF:FF:FF:FF:FF マスク: 00:00:00:00:00:00
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

12 続けて、マルチキャストMAC宛ての通信を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: 01:00:5E:00:00:00 マスク: 00:00:00:7F:FF:FF
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

13 続けて、管理用VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	1
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定

ACLグループ名 Public_Wi-Fi_Downlink

CoS

送信先MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

送信元MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

イーサertype (0600-FFFF Hex)

VLAN

ACLの動作

許可/拒否

Egressキュー

リダイレクトポート

14 続けて、総務VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	2
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定

ACLグループ名 Public_Wi-Fi_Downlink

CoS

送信先MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

送信元MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

イーサertype (0600-FFFF Hex)

VLAN

ACLの動作

許可/拒否

Egressキュー

リダイレクトポート

15 続けて、営業VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	3
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
イーサータイプ	すべて (0600-FFFF Hex)
VLAN	3
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

16 続けて、手順10～15以外の通信をすべて禁止するルールを設定します。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	拒否
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
イーサータイプ	すべて (0600-FFFF Hex)
VLAN	すべて
ACLの動作	
許可/拒否	拒否
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

17 ここまで登録したら、手順10～16の内容が正しく設定されているかを確認します。
正しく設定されている場合は、ACLルール一覧が以下のように表示されます。

ルール番号	CoS	送信元MACアドレス	送信元マスク	送信元MACアドレス	送信元マスク	イーサタイプ	VLAN	許可/拒否	Egressキュー	リダイレクトポート
<input type="checkbox"/> 1	すべて	XXXXXXXXXXXX	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 2	すべて	FFFFFFFFFFFF	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 3	すべて	01:00:5E:00:00:00	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 4	すべて	すべて	すべて	すべて	すべて	すべて	1	許可	なし	なし
<input type="checkbox"/> 5	すべて	すべて	すべて	すべて	すべて	すべて	2	許可	なし	なし
<input type="checkbox"/> 6	すべて	すべて	すべて	すべて	すべて	すべて	3	許可	なし	なし
<input type="checkbox"/> 7	すべて	すべて	すべて	すべて	すべて	すべて	すべて	拒否	なし	なし

ルールの移動
 移動 選択したルールの一つ上に移動 選択したルールの一つ下に移動 (ルール番号)
 移動 編集 削除

18 画面左のメニューで「MAC ACL」をクリックします。

19 ACLグループ名に「Public_Wi-Fi_Uplink」と入力して、「適用」をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> Public_Wi-Fi_Uplink	
<input type="checkbox"/> Public_Wi-Fi_Downlink	7/10 詳細

[適用](#) [名前の変更](#) [削除](#)

20 手順19で追加した「Public_Wi-Fi_Uplink」の「詳細」をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> <input type="text"/>	
<input type="checkbox"/> Public_Wi-Fi_Downlink	7/10 詳細
<input type="checkbox"/> Public_Wi-Fi_Uplink	0/10 詳細

[適用](#) [名前の変更](#) [削除](#)

21 本製品(FS-M1266)のMACから送信されるパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	手動 アドレス: 本製品(FS-M1266)の有線MACアドレス マスク: 00:00:00:00:00:00
イーサータイプ	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Uplink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	手動 アドレス: XX:XX:XX:XX:XX:XX マスク: 00:00:00:00:00:00 (例: 00:11:22:33:44:55)
イーサータイプ	すべて (0600-FFFF Hex)
VLAN	すべて
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

22 続けて、管理用VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	1
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Uplink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
イーサータイプ	すべて (0600-FFFF Hex)
VLAN	1
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

23 続けて、手順21～22以外の通信をすべて禁止するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	拒否
Egressキュー	なし
リダイレクトポート	なし

24 ここまで登録したら、手順21～23の内容が正しく設定されているかを確認します。

正しく設定されている場合は、ACLルール一覧が以下のように表示されます。

ルール番号	CoS	送信先MACアドレス	送信先マスク	送信元MACアドレス	送信元マスク	イーサータイプ	VLAN	許可/拒否	Egressキュー	リダイレクトポート
<input type="checkbox"/> 1	すべて	すべて	すべて	XX.XX.XX.XX.XX.XX	00:00:00:00:00:00	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 2	すべて	すべて	すべて	すべて	すべて	すべて	1	許可	なし	なし
<input type="checkbox"/> 3	すべて	すべて	すべて	すべて	すべて	すべて	すべて	拒否	なし	なし

25 ACLポート設定画面を表示します。

[詳細設定] - [ACL] - [ポート設定]画面を表示します。

26 ACLグループ名で、アクセスポイントを接続しているポートに対し、「Public_Wi-Fi_Downlink」のルールを適用します。

「Public_Wi-Fi_Downlink」を選択し、2～3にチェックをつけて[適用]をクリックします。

ポート設定

ポート設定

有効なIPv4 MAC ACLルール数 0/126

有効なIPv6 ACLルール数 0/64

ACLグループ名 Public_Wi-Fi_Downlink

ポート選択

1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				

適用

27 手順26と同様に、本製品(FS-M1266)を接続しているポートに対し、「Public_Wi-Fi_Uplink」のルールを適用します。

ACLグループ名で「Public_Wi-Fi_Uplink」を選択し、8にチェックをつけて[適用]をクリックします。

ポート設定

ポート設定

有効なIPv4 MAC ACLルール数 7/126

有効なIPv6 ACLルール数 0/64

ACLグループ名 Public_Wi-Fi_Uplink

ポート選択

1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input checked="" type="checkbox"/>						

適用

Step 4 既設のL2スイッチ(B)のVLAN設定を変更し、ACLルールを登録する

2Fに設置されているL2スイッチ(B)のVLAN設定を変更し、以下の4点に関するACL(アクセスコントロールリスト)の設定を行います。

- 各々のアクセスポイントに接続した、公衆Wi-Fi利用者端末同士の通信を防ぐ。
- どのアクセスポイントに接続していても、営業部端末同士は通信を許可する。
- どのアクセスポイントに接続していても、総務部端末同士は通信を許可する。
- どのアクセスポイントに接続していても、管理部端末同士は通信を許可する。

1 L2スイッチ(B)の設定画面を表示します。

設定用パソコンのWebブラウザを起動して、アドレス欄にL2スイッチ(B)のIPアドレス(192.168.1.102)を入力します。

2 L2スイッチ(B)の管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

ユーザー名 admin

パスワード

ログイン

3 公衆Wi-FiのVLANを追加します。

[基本設定] - [VLAN] - [VLAN設定]の画面で、以下のように設定して、[適用]をクリックします。

VLAN ID	5
VLAN名	Public_Wi-Fi
管理VLAN	チェックなし
Tagged	1、2、3
Untagged	なし
Not Member	4、5、6、7、8

VLANの追加 編集

VLAN ID (2-4094)

VLAN名

管理VLAN

ポート		1	2	3	4	5	6	7	8
Tagged	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	All	<input type="radio"/>							
Not Member	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

適用 リセット キャンセル

4 VLANステータスが以下のようになったことを確認します。

VLANステータス

■	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.1.102	T	T	T	T	U	U	U	U	Management	Up
<input type="checkbox"/>	2	-	T	T	T	-	-	-	-	-	SOUNU	Down
<input type="checkbox"/>	3	-	T	T	T	-	-	-	-	-	EIGYO	Down
<input type="checkbox"/>	5	-	T	T	T	-	-	-	-	-	Public_Wi-Fi	Down
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		

T:Static Tagged U:Static Untagged -:Not Member X:有効

編集 削除

5 MAC ACL設定画面を表示します。

[詳細設定] - [ACL] - [MAC ACL]画面を表示します。

6 ACLグループ名に「Public_Wi-Fi_Downlink」と入力して、[適用]をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/> Public_Wi-Fi_Downlink	

適用 名前の変更 削除

7 手順6で追加した「Public_Wi-Fi_Downlink」の「詳細」をクリックします。

ACLグループ名	ルール数
<input type="checkbox"/>	
<input type="checkbox"/> Public_Wi-Fi_Downlink	0/10 詳細

[適用](#) [名前の変更](#) [削除](#)

8 本製品 (FS-M1266) のMAC宛でのユニキャスト通信を許可するルールを設定します。

以下のように設定して、「保存」をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: 本製品 (FS-M1266) の有線MACアドレス マスク: 00:00:00:00:00:00
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定

ACLグループ名 Public_Wi-Fi_Downlink

CoS [すべて](#) ▾

送信先MACアドレス [手動](#) ▾ アドレス: マスク: (例: 00:11:22:33:44:55)

送信元MACアドレス [すべて](#) ▾ アドレス: マスク: (例: 00:11:22:33:44:55)

イーサータイプ [すべて](#) ▾ (0600-FFFF Hex)

VLAN [すべて](#) ▾

ACLの動作

許可/拒否 [許可](#) ▾

Egressキュー [なし](#) ▾

リダイレクトポート [なし](#) ▾

[保存](#) [戻る](#)

9 続けて、ブロードキャストMAC宛での通信を許可するルールを設定します。

以下のように設定して、「保存」をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: FF:FF:FF:FF:FF:FF マスク: 00:00:00:00:00:00
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし

リダイレクトポート	なし
-----------	----

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	手動 ▼ アドレス: FF:FF:FF:FF:FF:FF マスク: 00:00:00:00:00:00 (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて ▼ アドレス: マスク: (例: 00:11:22:33:44:55)
イーサertype	すべて ▼ (0600-FFFF Hex)
VLAN	すべて ▼
ACLの動作	
許可/拒否	許可 ▼
Egressキュー	なし ▼
リダイレクトポート	なし ▼
保存 戻る	

10 続けて、マルチキャストMAC宛ての通信を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	手動 アドレス: 01:00:5E:00:00:00 マスク: 00:00:00:7F:FF:FF
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	すべて
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	手動 ▼ アドレス: 01:00:5E:00:00:00 マスク: 00:00:00:7F:FF:FF (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて ▼ アドレス: マスク: (例: 00:11:22:33:44:55)
イーサertype	すべて ▼ (0600-FFFF Hex)
VLAN	すべて ▼
ACLの動作	
許可/拒否	許可 ▼
Egressキュー	なし ▼
リダイレクトポート	なし ▼
保存 戻る	

11 続けて、管理用VLANセグメントのパケットを許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	1
許可/拒否	許可
Egressキュー	なし

リダイレクトポート	なし
-----------	----

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて ▾
送信先MACアドレス	すべて ▾ アドレス: マスク: (例 : 00:11:22:33:44:55)
送信元MACアドレス	すべて ▾ アドレス: マスク: (例 : 00:11:22:33:44:55)
イーサertype	すべて ▾ (0600-FFFF Hex)
VLAN	1 ▾
ACLの動作	
許可拒否	許可 ▾
Egressキュー	なし ▾
リダイレクトポート	なし ▾
<input type="button" value="保存"/> <input type="button" value="戻る"/>	

12 続けて、総務VLANセグメントの packets を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	2
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
イーサertype	すべて (0600-FFFF Hex)
VLAN	2
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

13 続けて、営業VLANセグメントの packets を許可するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサertype	すべて
VLAN	3
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定	
ACLグループ名	Public_Wi-Fi_Downlink
CoS	すべて
送信先MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
送信元MACアドレス	すべて アドレス: マスク: (例: 00:11:22:33:44:55)
イーサertype	すべて (0600-FFFF Hex)
VLAN	3
ACLの動作	
許可/拒否	許可
Egressキュー	なし
リダイレクトポート	なし
保存 戻る	

14 続けて、手順8～13以外の通信をすべて禁止するルールを設定します。

以下のように設定して、[保存]をクリックします。

CoS	すべて
送信先MACアドレス	すべて
送信元MACアドレス	すべて
イーサータイプ	すべて
VLAN	すべて
許可/拒否	拒否
Egressキュー	なし
リダイレクトポート	なし

ACLルール設定

ACLグループ名 Public_Wi-Fi_Downlink

CoS

送信先MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

送信元MACアドレス アドレス: マスク: (例: 00:11:22:33:44:55)

イーサータイプ (0600-FFFF Hex)

VLAN

ACLの動作

許可/拒否

Egressキュー

リダイレクトポート

15 ここまで登録したら、手順8～14の内容が正しく設定されているかを確認します。

正しく設定されている場合は、ACLルール一覧が以下のように表示されます。

ACLルール一覧 (編集可能)

ルール番号	CoS	送信先MACアドレス	送信元MACアドレス	送信先マスク	送信元マスク	イーサータイプ	VLAN	許可/拒否	Egressキュー	リダイレクトポート
<input type="checkbox"/> 1	すべて	XXXXXXXXXXXX	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 2	すべて	FFFFFFFFFFFF	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 3	すべて	01:00:3E:00:00:00	00:00:00:00:00:00	すべて	すべて	すべて	すべて	許可	なし	なし
<input type="checkbox"/> 4	すべて	すべて	すべて	すべて	すべて	すべて	1	許可	なし	なし
<input type="checkbox"/> 5	すべて	すべて	すべて	すべて	すべて	すべて	2	許可	なし	なし
<input type="checkbox"/> 6	すべて	すべて	すべて	すべて	すべて	すべて	3	許可	なし	なし
<input checked="" type="checkbox"/> 7	すべて	すべて	すべて	すべて	すべて	すべて	すべて	拒否	なし	なし

ルールの移動

移動 ● 選択したルールの一つ上に移動 ○ 選択したルールの一つ下に移動 (ルール番号)

16 ACLポート設定画面を表示します。

[詳細設定] - [ACL] - [ポート設定]画面を表示します。

17 ACLグループ名で、アクセスポイントを接続しているポートに対し、「Public_Wi-Fi_Downlink」のルールを適用します。

「Public_Wi-Fi_Downlink」を選択し、2～3にチェックをつけて[適用]をクリックします。

ポート設定

ポート設定

有効なIPv4 MAC ACLルール数 0/126

有効なIPv6 ACLルール数 0/64

ACLグループ名 Public_Wi-Fi_Downlink ▾

ポート選択

1	2	3	4	5	6	7	8
<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>				

適用

Step 5 アクセスポイントに公衆Wi-Fiの設定を行う

L2スイッチに接続しているアクセスポイントすべてに対して、公衆Wi-Fiの設定を行います。

1 アクセスポイントの設定画面を表示します。

設定用パソコンのWebブラウザを起動して、アドレス欄にアクセスポイントのIPアドレス(192.168.1.201～192.168.1.204)を入力します。

2 アクセスポイントの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

ユーザー名

admin

パスワード

●●●●●●●●●●

ログイン

3 [詳細設定]をクリックします。

4 SSID設定画面を表示します。

[無線設定] - [SSID設定]をクリックし、[新規追加]をクリックします。

SSID設定 - SSIDの編集

ステアリング ポリシー設定

ステアリング ポリシー

SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	無線の認証	暗号化		
1	有効	Buffalo-Management	1	<input type="radio"/>	<input type="radio"/>	無効	WPA2 Personal AES		<input type="button" value="編集"/>	<input type="button" value="削除"/>
2	有効	SOMU	2	<input type="radio"/>	<input type="radio"/>	無効	WPA2 Personal AES		<input type="button" value="編集"/>	<input type="button" value="削除"/>
3	有効	EIGYO	3	<input type="radio"/>	<input type="radio"/>	無効	WPA2 Personal AES		<input type="button" value="編集"/>	<input type="button" value="削除"/>

5 公衆Wi-Fi利用者用のSSID(Public_Wi-Fi)を設定します。

以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	Public_Wi-Fi
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
ステアリング	無効
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN ID: 5 追加VLAN ID: なし
ANY接続	許可する
プライバシーセパレーター	STAセパレーター
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	施設独自の設定
暗号化	
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効			
SSID	Public_Wi-Fi			
次の場合に有効にする	通常時と緊急時			
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz	<input checked="" type="checkbox"/> 5GHz		
ステアリング	無効			
優先制御	通常			
VLAN ID	VLANモード	VLAN ID	追加VLAN ID	
	Untagged Port	5		
ANY接続	<input checked="" type="checkbox"/> 許可する			
プライバシーセパレーター	STAセパレーター			
ロードバランス(同時接続台数制限)	2.4GHz	5GHz		
	128 / 128	128 / 128		
無線の認証	認証を行わない			
暗号化	暗号化なし <small>「暗号化なし」に設定すると、第三者から通信内容を読み取られる可能性があります。</small>			
追加暗号化	追加暗号化を行わない			
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>				

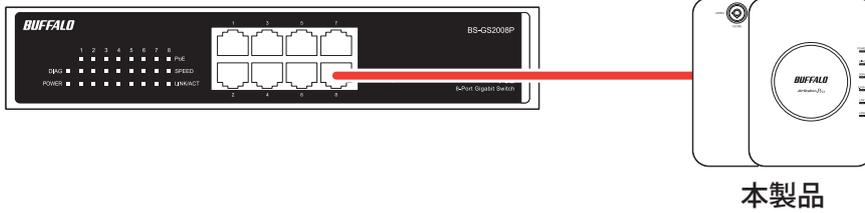
メモ: アクセスポイントに接続している端末に対して公衆Wi-Fi利用者端末同士の通信を禁止するため、STAセパレーターを設定しています。

6 [設定]をクリックします。

Step 6 本製品をL2スイッチ(A)に接続する

Step 5までの設定が完了したら、1FのL2スイッチ(A)のポート8に、本製品のLAN端子を接続します。

1F L2スイッチ(A)



メモ: 本製品のWAN端子は使用しません。

以上で設定は完了です。

例5: L2スイッチのACL機能を使用せずにFREESPOTを導入したい

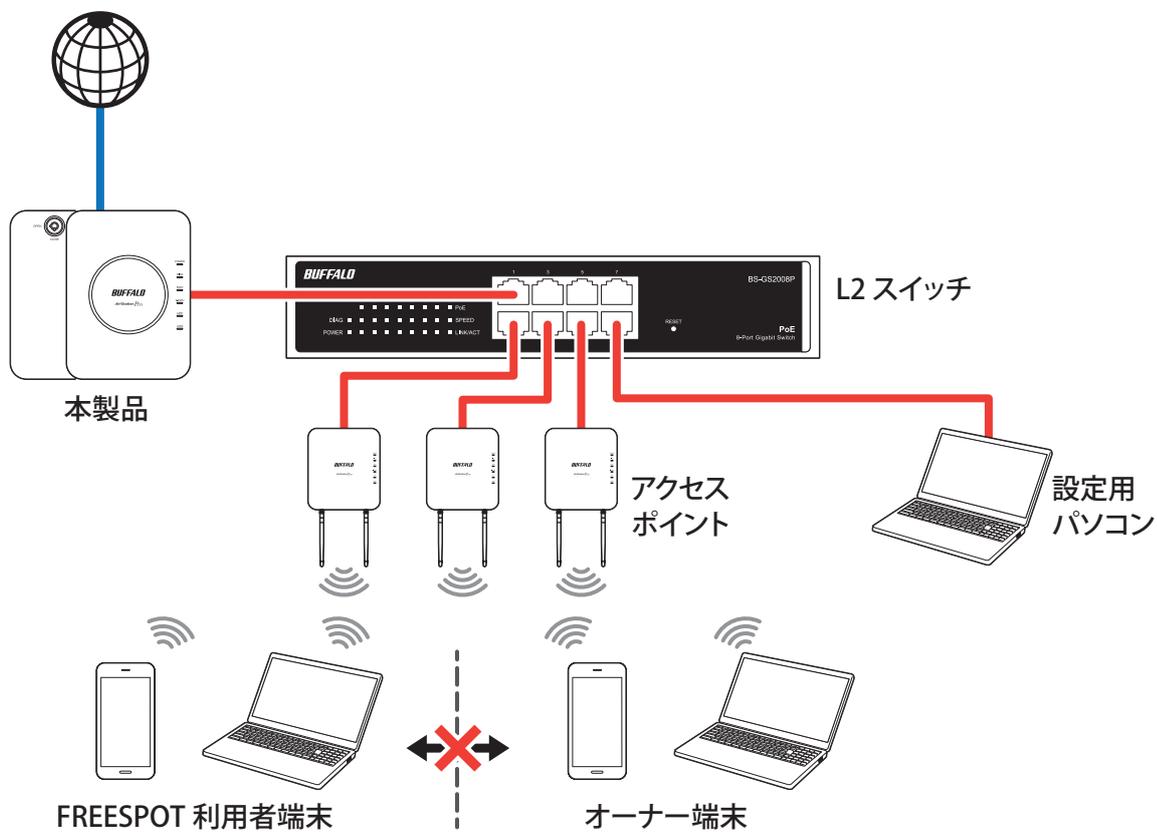
ゲストポート機能をもつアクセスポイントを使用することで、L2スイッチのACL(アクセスコントロールリスト)機能を使用せずに先述の例2~4と同等の構成を構築することができます。

先述の例との差分はL2スイッチのACLについての設定をしないこと、アクセスポイントをゲストポート用に設定することの2点です。

ここでは、前述の「例2」の設定例に対して、ACL機能を使わず設定する方法を説明します。

メモ: 用途によってはL2スイッチを使わずとも環境構成可能です。その際はFREESPOT、APのLAN側ポート同士をLANケーブルで直結してください。LAN側ポートの設定は必要なく、デフォルトのまま使用可能です。AP同士をつないで拡張することも可能です。

構成例



条件

- FREESPOT利用者は、本製品とは別のアクセスポイントに接続させる。
- FREESPOT利用者端末から、設定用パソコンやオーナー端末へのアクセスを禁止する。
- FREESPOT利用者端末同士の通信を禁止する。

設定に使用する機器

- 本製品(FS-M1266)
- VLAN対応のL2スイッチ(BS-GSL2008Pなど)
- ゲストポート機能対応のアクセスポイント(WAPM-AX8Rなど)
- 設定用パソコン

メモ:

- L2スイッチやアクセスポイントの推奨機器は、当社ホームページ(<https://www.buffalo.jp/product/detail/fs-m1266.html>)を参照してください。
- L2スイッチがPoEに対応していない場合は、別売のACアダプタ(WLE-OP-AC12C)をご用意ください。
- FREESPOT利用者が本製品とは別のアクセスポイントに接続するよう、本事例では本製品の無線機能はOFFで説明していますが、ONにすることもできます。
- 最新のゲストポート対応機種は当社ホームページ(https://www.buffalo.jp/r/compare_wireless_business.html)を参照してください。

Step 1 本製品を設置する

本製品の設置や初期設定(インターネットの接続設定、FREESPOT管理者登録情報の設定、FREESPOTマップの登録など)は、本書の第1章を参照して設定してください。

完了後、前述の「構成例」にあわせて配線し、「Step 2 FREESPOT VLANの設定を行う」へ進んでください。

メモ:

- 本製品のLAN端子は、L2スイッチのポート1に接続してください。
- 設定用パソコンは、L2スイッチのポート8に接続してください。

Step 2 公衆Wi-FiのVLANの設定を行う

公衆Wi-FiのVLANを有効にします。

1 本製品の設定画面を表示します。

設定画面の表示方法は、第1章の「Step 1 設定画面を表示する」を参照してください。

2 [詳細設定]をクリックします。

3 公衆Wi-FiのVLANの設定を行います。

[WAN/LAN] – [LAN設定]画面にある「CUSTOM_0」(3行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN	有効
VLAN名	任意のVLAN名(例:Public_Wi-Fi)
VLAN ID	3
IPアドレス	IPアドレス: 192.168.13.1 サブネットマスク: 255.255.255.0
DHCPサーバー	割り当てIPアドレス: 192.168.13.2から128台 除外アドレス: 空欄 リース期間: 1時間
i-フィルター	使用しない
SPAMメール対策	使用する メール送信数制限: 20件/分
ポップアップテクノロジー	使用する 広告URL: 接続時に表示させたいポータル画面のURL 広告表示間隔: 0秒
接続時間制限	使用する 接続回数: 3回/日 接続許可時間: 30分/回
公衆無線LAN利用者認証	利用者認証: 使用する ゲスト方式認証: 使用しない SNSアカウント認証: 使用する Wi-Cert Web-API認証: 使用しない 認証画面バナーの汎用表記: 使用しない 認証前HTTPS通信制限: 使用する

VLAN情報の編集	
VLAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
VLAN名	Public_Wi-Fi
VLAN ID	3
IP アドレス	IP アドレス 192.168.13.1
	サブネットマスク 255.255.255.0
DHCP サーバー	割り当て IP アドレス 192.168.13.2 から 128 台
	除外アドレス
	リース期間 1 時間
公衆無線LAN関連設定	
i-フィルター	<input type="checkbox"/> 使用する フィルターレベル 公衆
SPAMメール対策	<input checked="" type="checkbox"/> 使用する メール送信数制限 20 件/分
ポップアップテクノロジー	<input checked="" type="checkbox"/> 使用する 広告URL http://xxx.xxx.xxx.xxx/ 広告表示間隔 0 秒
接続時間制限	<input checked="" type="checkbox"/> 使用する 接続回数 3 回/日 接続許可時間 30 分/回
公衆無線LAN利用者認証	利用者認証 <input checked="" type="checkbox"/> 使用する
	利用者認証オプション
	ゲスト方式認証 <input type="checkbox"/> 使用する
	SNSアカウント認証 <input checked="" type="checkbox"/> 使用する
	Wi-Cert Web-API認証 <input type="checkbox"/> 使用する
認証画面/バナーの汎用表記 <input type="checkbox"/> 使用する	
認証前HTTPS通信制限 <input checked="" type="checkbox"/> 使用する	
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>	

メモ: 各内容の詳細は、ユーザーマニュアルを参照してください。

Step 3 L2スイッチのIPアドレスを変更して設定画面を表示する

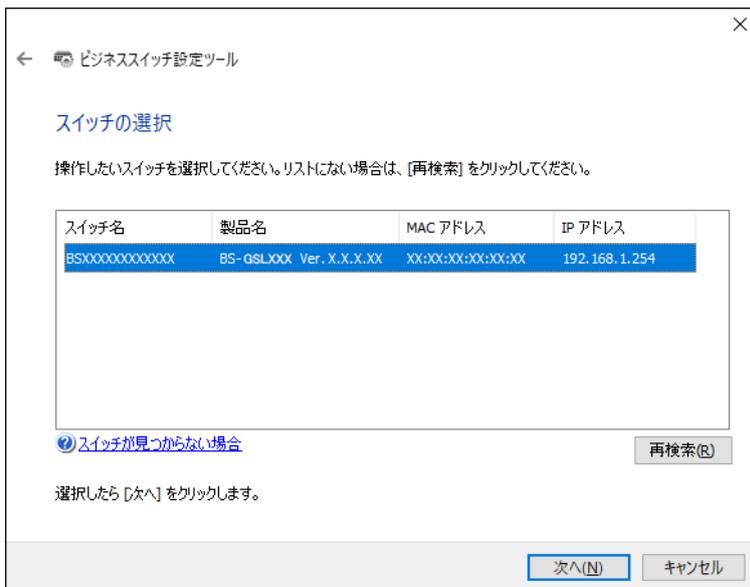
「ビジネススイッチ設定ツール」を使ってL2スイッチのIPアドレスを変更し、設定画面を表示します。

- 1 当社ホームページ(https://www.buffalo.jp/support/download/detail/?dl_contents_id=60665)から「ビジネススイッチ設定ツール」をダウンロードして、設定用パソコンにインストールします。
- 2 「ビジネススイッチ設定ツール」を起動します。

3 [次へ]をクリックします。



4 L2スイッチを選択して、[次へ]をクリックします。



5 設定画面にアクセスするためには、セグメントを合わせる必要があります。

[このスイッチのIPアドレスを設定する]をクリックします。

← ビジネススイッチ設定ツール

操作の選択

次のスイッチが選択されました。おこないたい操作を選択してください。

スイッチ名	製品名	MAC アドレス	IP アドレス
BSXXXXXXXXXXXX	BS-GSLXXX Ver. X.X.X.XX	XX:XX:XX:XX:XX:XX	192.168.1.254

設定画面を開く (W)
(通常はこちら)

このスイッチの IP アドレスを設定する (I)
(上級者・管理者向け)

6 L2スイッチのIPアドレスを変更します。

[次のIPアドレスを使う(上級者・管理者向け)]を選択し、IPアドレスを「192.168.11.254」、サブネットマスクを「255.255.255.0」に設定して[次へ]をクリックします。

← ビジネススイッチ設定ツール

スイッチの IP アドレス設定

スイッチの新しい IP アドレスを入力してください。

DHCP サーバーから IP アドレスを自動的に取得する(かんたん)(O)

次の IP アドレスを使う(上級者・管理者向け)(S)

IP アドレス(I) [設定方法](#)

サブネットマスク(U) ▼

* 参考情報 - このパソコンの IP アドレス:
68.11.2 / 255.255.255.0 : イーサネット (Intel(R) 82579V Gigabit Network Connection)

[次へ] をクリックすると、設定内容がスイッチに反映されます。

次へ(N)

- 7** パスワードの入力画面が表示されたら、L2スイッチに設定されている管理パスワードを入力して、[次へ]をクリックします。

← ビジネススイッチ設定ツール

設定中

このスイッチには、管理パスワードが設定されています。
スイッチの管理パスワードを入力してください。

管理パスワード(P) 入力文字列を表示(V)

出荷時の設定は、「password」または「無し(空欄)」です。

次へ(N)

- 8** 以下の画面が表示されたら、[スイッチ選択画面に戻る]をクリックします。

← ビジネススイッチ設定ツール

設定完了

スイッチの IP アドレス設定が完了しました。

ひきつづきスイッチの設定画面を開くには、[スイッチ選択画面に戻る] をクリックし、もう一度スイッチを選択してください。

スイッチ選択画面に戻る

完了(E)

9 L2スイッチを選択して、「次へ」をクリックします。

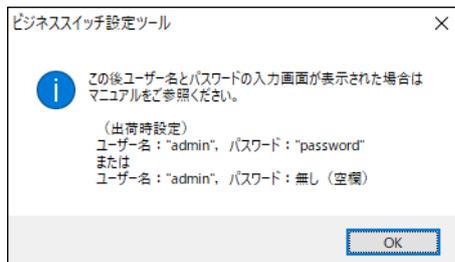


10 「設定画面を開く(通常はこちら)」をクリックします。



11 「OK」をクリックします。

ブラウザーが起動し、ログイン画面が表示されます。



12 L2スイッチの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

ユーザー名

パスワード

メモ: 設定画面のウィンドウが開くと、ビジネススイッチ設定ツールのウィンドウに「スイッチの設定画面を開きました」と表示されます。ビジネススイッチ設定ツールのウィンドウの[完了]をクリックしてください。ビジネススイッチ設定ツールが閉じます。

Step 4 L2スイッチにVLANの設定をする

L2スイッチの設定画面でVLAN設定を行います。

1 VLAN設定画面を表示します。

[基本設定] - [VLAN] - [VLAN設定]画面で、VLAN ID 1のチェックボックスにチェックマークをつけて、[編集]をクリックします。

VLANステータス												
<input checked="" type="checkbox"/>	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input checked="" type="checkbox"/>	1	192.168.11.254	U	U	U	U	U	U	U	U		Up
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
<input type="button" value="編集"/>			<input type="button" value="削除"/>									

2 Management VLANを以下のように設定して、[適用]をクリックします。

VLAN ID	1
VLAN名	Management
管理VLAN	チェックあり
接続方式	固定IPアドレス
IPv4アドレス	192.168.11.254
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.11.1
取得方式	手動設定
プライマリDNSサーバー	192.168.11.1
セカンダリDNSサーバー	0.0.0.0
IPv6	無効
Tagged	なし
Untagged	1、2、3、4、5、6、7、8
Not Member	なし

VLANの追加/編集

VLAN ID (2-4094)

VLAN名

管理VLAN

接続方式

接続方式 ▼

IPv4アドレス設定

IPv4アドレス

サブネットマスク

デフォルトゲートウェイ

DNSサーバー

取得方式 ▼

プライマリDNSサーバー

セカンダリDNSサーバー

IPv6アドレス設定

IPv6 有効

ポート	1	2	3	4	5	6	7	8
Tagged	<input type="radio"/>							
Untagged	<input checked="" type="radio"/>							
Not Member	<input type="radio"/>							

3 VLANステータスが以下のようになったことを確認します。

VLANステータス												
■	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.11.254	U	U	U	U	U	U	U	U	Management	Up
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
<input type="button" value="編集"/> <input type="button" value="削除"/>												

4 公衆Wi-FiのVLANを作成します。

以下のように設定して、[適用]をクリックします。

VLAN ID	3
VLAN名	Public_Wi-Fi
管理VLAN	チェックなし
Tagged	1、2、3、4、5、6、7
Untagged	なし
Not Member	8

VLANの追加編集

VLAN ID (2-4094)

VLAN名

管理VLAN

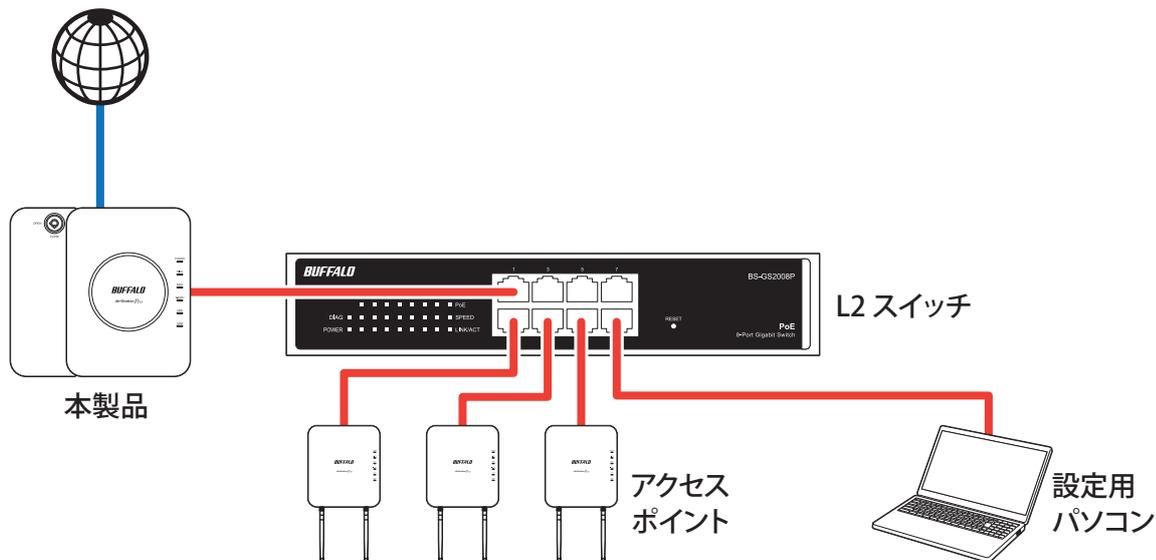
ポート		1	2	3	4	5	6	7	8
Tagged	<input type="button" value="All"/>	<input checked="" type="radio"/>	<input type="radio"/>						
Untagged	<input type="button" value="All"/>	<input type="radio"/>							
Not Member	<input type="button" value="All"/>	<input type="radio"/>	<input checked="" type="radio"/>						

5 VLANステータスが以下のようになったことを確認します。

VLANステータス												
■	VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	VLAN名	管理VLAN
<input type="checkbox"/>	1	192.168.11.254	U	U	U	U	U	U	U	U	Management	Up
<input type="checkbox"/>	3	-	T	T	T	T	T	T	T	-	Public_Wi-Fi	Down
PVID			1	1	1	1	1	1	1	1		
プロテクトポート			-	-	-	-	-	-	-	-		
T:Static Tagged U:Static Untagged -:Not Member X:有効												
<input type="button" value="編集"/> <input type="button" value="削除"/>												

Step 5 アクセスポイントをL2スイッチに接続する

L2スイッチのポート2～7に、アクセスポイントを接続します。

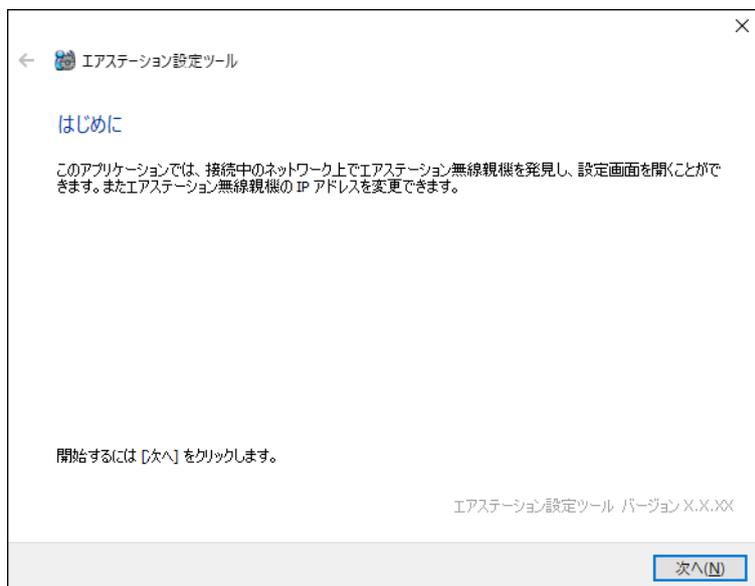


Step 6 アクセスポイントのIPアドレスを変更して設定画面を表示する

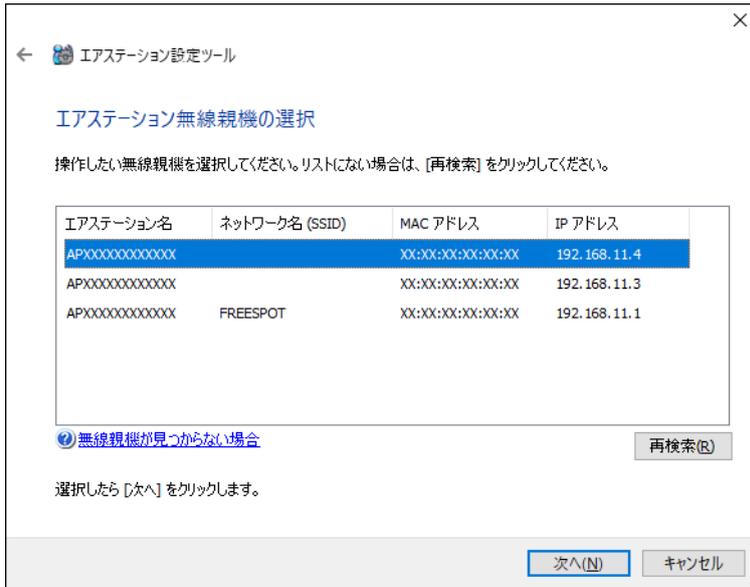
アクセスポイントすべてのIPアドレスを変更し、設定画面を表示します。

出荷時設定でお使いの場合、当社製アクセスポイントのIPアドレスは、DHCPサーバーから自動取得します。ここでは、アクセスポイントをより管理しやすくするために、「エアステーション設定ツール」を使って、アクセスポイントごとにIPアドレスを設定した後、設定画面を表示する方法を説明します。

- 1 当社ホームページ(<https://86886.jp/airset/>)から「エアステーション設定ツール」をダウンロードして、設定用パソコンにインストールします。
- 2 「エアステーション設定ツール」を起動します。
- 3 [次へ]をクリックします。



4 アクセスポイントを選択して、[次へ]をクリックします。



5 [この無線親機のIPアドレスを設定する]をクリックします。



6 アクセスポイントのIPアドレスを変更します。

「次のIPアドレスを使う(上級者・管理者向け)」を選択し、IPアドレスを「192.168.11.250」など、サブネットマスクを「255.255.255.0」に設定して[次へ]をクリックします。

← エアステーション設定ツール

無線親機の IP アドレス設定

無線親機の新しい IP アドレスを入力してください。

DHCP サーバーから IP アドレスを自動的に取得する(かんたん)(D)

※ 無線親機の ROUTER ランプが点灯している場合(ルーター機能有効時)は、この設定にはできません。

次の IP アドレスを使う(上級者・管理者向け)(S)

IP アドレス(I) [設定方法](#)

サブネットマスク(U)

※ 無線親機の ROUTER スイッチが「ALTO」に設定されていて、かつ、ROUTER ランプが消灯している場合(ルーター機能無効時)は、この設定にはできません。

※ 参考情報 - このパソコンの IP アドレス:
68.11.2 / 255.255.255.0 : イーサネット (Intel(R) 82579V Gigabit Network Connection)

[次へ] をクリックすると、設定内容が無線親機に反映されます。

次へ(N)

メモ: IPアドレスは、他のアクセスポイントと重複しない値を設定してください。

7 パスワードの入力画面が表示されたら、アクセスポイントに設定されている管理パスワードを入力して、[次へ]をクリックします。

← エアステーション設定ツール

設定中

この無線親機には、管理パスワードが設定されています。

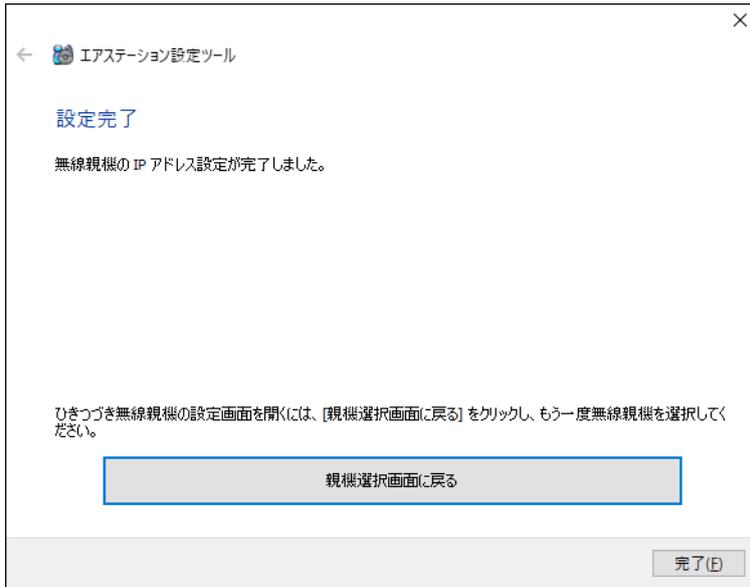
無線親機の管理パスワードを入力してください。

管理パスワード(P) 入力文字列を表示(V)

出荷時の設定は、セットアップカードまたはラベルに記載されています。
記載がない場合、「password」または無し(空欄)です。

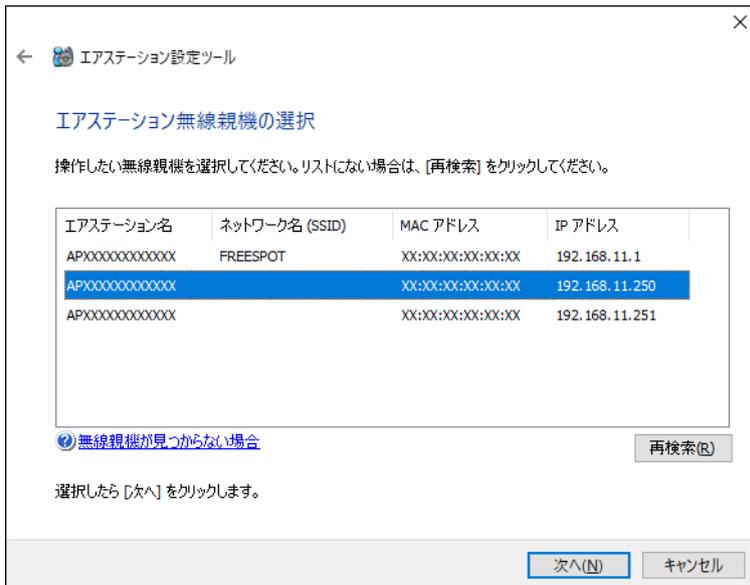
次へ(N)

8 以下の画面が表示されたら、[親機選択画面に戻る]をクリックします。



9 手順4～8の作業を、接続するアクセスポイントの台数分行います。

10 設定を行うアクセスポイントを選択して、[次へ]をクリックします。

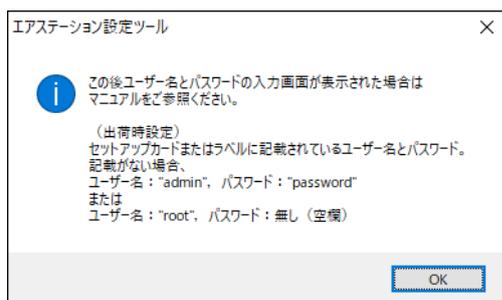


11 [設定画面を開く(通常はこちら)]をクリックします。



12 [OK]をクリックします。

ブラウザが起動し、ログイン画面が表示されます。



13 アクセスポイントの管理ユーザー名と管理パスワードを入力して、[ログイン]をクリックします。

メモ: 設定画面のウィンドウが開くと、エアステーション設定ツールのウィンドウに「無線LAN親機の設定画面を開きました」と表示されます。エアステーション設定ツールのウィンドウの[完了]をクリックしてください。エアステーション設定ツールが閉じます。

Step 7 アクセスポイントに公衆Wi-Fiの設定を行う

Step 5でL2スイッチに接続したアクセスポイントすべてに対して、公衆Wi-Fiの設定を行います。

1 [詳細設定]をクリックします。

2 SSID設定画面を表示します。

[無線設定] - [SSID設定]をクリックし、[新規追加]をクリックします。

SSID設定 - SSIDの編集

ステアリング ポリシー設定

ステアリング ポリシー

SSID編集

Index	状態	SSID	WLAN ID	2.4GHz	5GHz	ステアリング	無線の認証	暗号化
SSIDの設定は登録されていません								

3 公衆Wi-Fi利用者用のSSID(Public_Wi-Fi)を設定します。

以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	Public_Wi-Fi
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
ステアリング	無効
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN ID: 3 追加VLAN ID: なし
ANY接続	許可する
プライバシーセパレーター	ゲストポート (例外IPアドレス:設定なし)
ロードバランス	2.4GHz: 256/256 5GHz: 256/256
無線の認証	施設独自の設定
暗号化	

追加認証	追加認証を行わない		
無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効		
SSID	'frespot'=SecurityPassword(AES)		
次の場合に有効にする	通常時と緊急時		
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz		
ステアリング	無効		
優先制御	通常		
VLAN ID	VLANモード	VLAN ID	追加VLAN ID
	Untagged Port	2	
ANY接続	<input checked="" type="checkbox"/> 許可する		
プライバシーセパレーター	ゲストポート		
	<input checked="" type="checkbox"/> プライベートアドレスへの通信を禁止する 例外IPアドレス		
ロードバランス(同時接続台数制限)	2.4GHz	5GHz	
	256 /256	256 /256	
無線の認証	WPA/WPA2 Personal		
暗号化方式	TKIP/AES mixed mode		
キー更新間隔	60 分		
事前共有キー	frespot		
Fast Transition (802.11r)	無効		
	Mobility Domain ID		
追加認証	追加認証を行わない		

修正保存

編集を終了して前の画面へ戻る

4 [設定]をクリックします。

Step 8 アクセスポイントにオーナー端末を接続するためのSSIDを設定する

Step 7でL2スイッチに接続したアクセスポイントすべてに対して、オーナー端末を接続するためのSSIDを設定します。

1 SSID設定画面を表示します。

[無線設定] - [SSID設定]をクリックし、[新規追加]をクリックします。

SSID設定 - SSIDの編集

ステアリング ポリシー設定

ステアリング ポリシー

SSID編集

Index	状態	SSID	VLAN ID	2.4GHz	5GHz	ステアリング	無線の認証	暗号化	
1	有効	Public_Wi-Fi3		<input type="radio"/>	<input type="radio"/>	無効	認証を行わない	暗号化なし	<input type="button" value="編集"/> <input type="button" value="削除"/>

2 オーナー用SSIDの設定を行います。

以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	任意のSSID(例:Buffalo)
次の場合に有効にする	通常時と緊急時
使用デバイス	2.4GHz、5GHz
ステアリング	無効
優先制御	優先
VLAN ID	VLANモード: Untagged VLAN ID: 1 追加VLAN ID: なし
ANY接続	許可する
プライバシーセパレーター	使用しない
ロードバランス	2.4GHz: 256/256 5GHz: 256/256
無線の認証	WPA2 Personal
暗号化方式	AES
キー更新間隔	60分
事前共有キー	任意の事前共有キー(例:buffalo12345678)
Management Frame Protection	無効
追加認証	追加認証を行わない
Fast Transition (802.11r)	無効

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効						
SSID	Buffalo						
次の場合に有効にする	通常時と緊急時						
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz						
ステアリング	無効						
優先制御	優先						
VLAN ID	<table border="1"> <thead> <tr> <th>VLANモード</th> <th>VLAN ID</th> <th>追加VLAN ID</th> </tr> </thead> <tbody> <tr> <td>Untagged Port</td> <td>1</td> <td></td> </tr> </tbody> </table>	VLANモード	VLAN ID	追加VLAN ID	Untagged Port	1	
VLANモード	VLAN ID	追加VLAN ID					
Untagged Port	1						
ANY接続	<input checked="" type="checkbox"/> 許可する						
プライバシーセパレーター	使用しない						
ロードバランス(同時接続台数制限)	<table border="1"> <thead> <tr> <th>2.4GHz</th> <th>5GHz</th> </tr> </thead> <tbody> <tr> <td>256 / 256</td> <td>256 / 256</td> </tr> </tbody> </table>	2.4GHz	5GHz	256 / 256	256 / 256		
2.4GHz	5GHz						
256 / 256	256 / 256						
無線の認証	WPA2 Personal						
暗号化方式	AES						
キー更新間隔	60分						
事前共有キー	buffalo12345678						
Management Frame Protection	無効						
追加認証	追加認証を行わない						
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>							

メモ: オーナー端末は、制限なく通信できるようにするため、プライバシーセパレーターは「使用しない」に設定します。

3 [設定]をクリックします。

以上で設定は完了です。

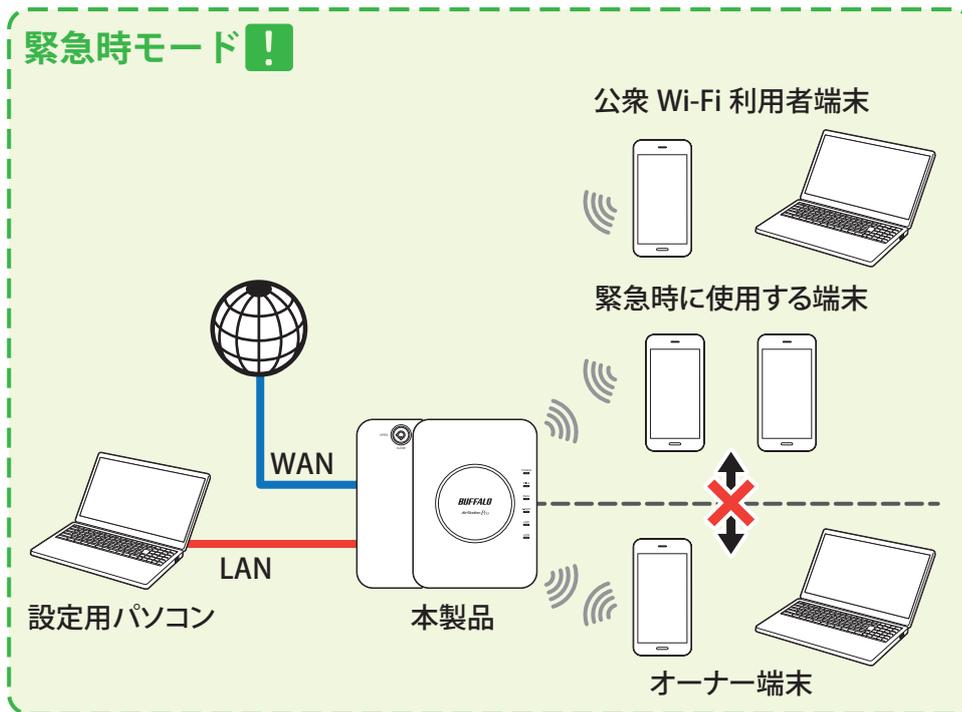
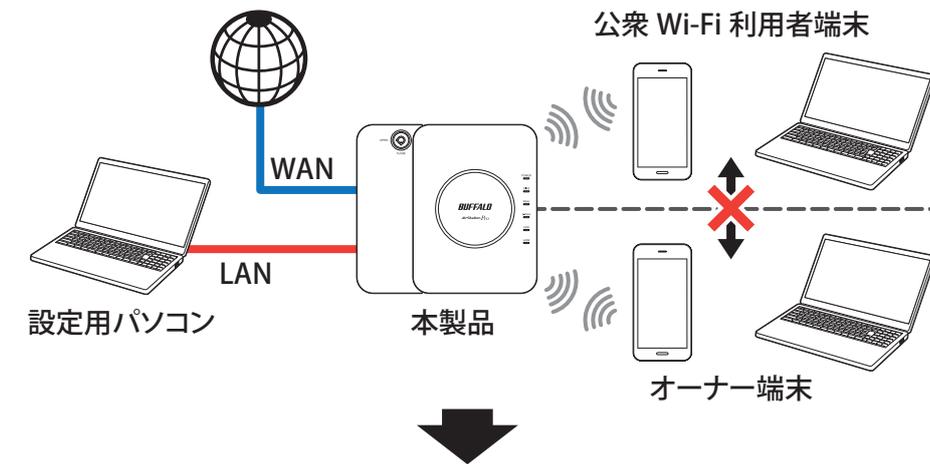
例6:災害などの発生に備えた設定をしたい

本製品は、緊急時モードに対応しており、通常動作(通常時モード)とは異なる動作モードを「緊急時モード」として設定できます。

たとえば、あらかじめ本製品に対して災害に備えた設定を行っておき、災害発生時に公衆Wi-Fiを一般開放(利用制限なく、誰でも使用できる状態に)するといった使い方ができます。

ここでは、前述の「例1」の設定例に対して、緊急時モードの設定を追加する方法を説明します。

構成例



条件

- 前述の「例1」の設定が完了している。
- 緊急時モードに切り替えた場合でも、設定用パソコンやオーナー端末に対しては、他の機器からアクセスできないようにする。
- 緊急時用のSSIDに接続した利用者の端末に、任意の災害用ポータル画面を表示させる。

設定に使用する機器

- ・ 本製品(FS-M1266)
- ・ 設定用パソコン

メモ:

- ・ オーナーが所有する有線端末が複数ある場合は、本製品のLAN端子に別売のスイッチ(BS-GU2008など)を接続して使用してください。
- ・ 本製品をPoEによる給電しない場合は、別売のACアダプタ(WLE-OP-AC12C)をご用意ください。

Step 1 「例1」の設定を行う

前述の「例1:個人経営の飲食店などの小規模施設に公衆Wi-Fiを新規導入したい」の設定を行います。設定が完了したら、「Step 2 緊急時用VLANを設定する」へ進んでください。

Step 2 緊急時用VLANを設定する

緊急時用のVLANを設定し、緊急時のネットワークから設定用パソコンやオーナー端末に対してアクセスできないようにします。

1 本製品の設定画面を表示します。

設定画面の表示方法は、第1章の「Step 1 設定画面を表示する」を参照してください。

2 [詳細設定]をクリックします。

3 緊急時用VLANの設定を行います。

[WAN/LAN] - [LAN設定]画面にある「CUSTOM_1」(4行目)の[編集]をクリックし、以下のように設定して[修正保存]をクリックします。

VLAN	有効
VLAN名	EMERGENCY
VLAN ID	4
IPアドレス	IPアドレス: 192.168.14.1 サブネットマスク: 255.255.255.0
DHCPサーバー	割り当てIPアドレス: 192.168.14.2から128台 除外アドレス: 空欄 リース期間: 1時間
i-フィルター	使用しない
SPAMメール対策	使用する メール送信数制限: 20件/分
ポップアップテクノロジー	使用する 広告URL: 緊急時用のSSIDに接続した端末に表示させたい 災害用ポータルURL 広告表示間隔: 0秒
接続時間制限	使用しない
公衆無線LAN利用者認証	使用しない

VLAN情報の編集

VLAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	
VLAN名	EMERGENCY	
VLAN ID	4	
IP アドレス	IP アドレス	192.168.14.1
	サブネットマスク	255.255.255.0
DHCP サーバー	割り当て IP アドレス	192.168.14.2 から 128 台
	除外アドレス	
	リース期間	1 時間

公衆無線LAN関連設定

i-フィルター	<input type="checkbox"/> 使用する フィルターレベル: 公衆
SPAMメール対策	<input checked="" type="checkbox"/> 使用する メール送信数制限: 20 件/分
ポップアップテクノロジー	<input checked="" type="checkbox"/> 使用する 広告URL: http://xxx.xxx.xxx.xxx/ 広告表示間隔: 0 秒
接続時間制限	<input type="checkbox"/> 使用する 接続回数: 3 回/日 接続許可時間: 30 分/回
公衆無線LAN利用者認証	利用者認証 <input type="checkbox"/> 使用する 利用者認証オプション ゲスト方式認証 <input type="checkbox"/> 使用する SNSアカウント認証 <input checked="" type="checkbox"/> 使用する Wi-Cert Web-API認証 <input type="checkbox"/> 使用する 認証画面バナーの汎用表記 <input type="checkbox"/> 使用する 認証前HTTPS通信制限 <input checked="" type="checkbox"/> 使用する

修正保存 編集を終了して前の画面へ戻る

4 緊急時用のSSIDを有効にします。

[無線設定] - [SSID設定]画面にある[新規追加]をクリックし、以下のように設定して[修正保存]をクリックします。

無線LAN	有効
SSID	Buffalo-EM
次の場合に有効にする	緊急時のみ
使用デバイス	2.4GHz、5GHz
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN: EMERGENCY VLAN ID: 4
ANY接続	許可する
プライバシーセパレーター	STAセパレーター
ロードバランス	2.4GHz: 128/128 5GHz: 128/128
無線の認証	認証を行わない
暗号化	暗号化なし
追加認証	追加認証を行わない

無線LAN	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SSID	Buffalo-EM
次の場合に有効にする	緊急時のみ
使用デバイス	<input checked="" type="checkbox"/> 2.4GHz <input checked="" type="checkbox"/> 5GHz
優先制御	通常
VLAN ID	VLANモード: Untagged VLAN: EMERGENCY VLAN ID: 4
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	STAセパレーター
ロードバランス(同時接続台数制限)	2.4GHz: 128 / 128 5GHz: 128 / 128
無線の認証	認証を行わない
暗号化	暗号化なし <small>「暗号化なし」に設定すると、第三者から通信内容を読み取られる可能性があります。</small>
追加認証	追加認証を行わない
<input type="button" value="修正保存"/> <input type="button" value="編集を終了して前の画面へ戻る"/>	

メモ: 本製品に接続している端末に対して緊急時に使用する端末同士、および公衆Wi-Fi利用者端末同士の通信を禁止するため、STAセパレーターを設定しています。

5 [設定]をクリックします。

以上で設定は完了です。

災害が発生したときに公衆Wi-Fiを一般開放するには

災害が発生したときは、緊急時モードに切り替えて、公衆Wi-Fiを一般開放します。以下の手順で設定してください。

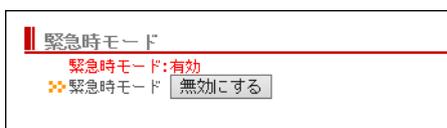
1 本製品の設定画面を表示します。

設定画面の表示方法は、第2章の「Step 1 設定画面を表示する」を参照してください。

2 緊急時モードの[有効にする]をクリックします。



3 しばらくして、緊急時モード欄に「有効」と表示されるのを確認します。



以上で設定は完了です。

災害が収束して、緊急時モードを解除する場合は、上記の手順3の画面で[無効にする]をクリックしてください。