

Edgecore Networks社製無線LANアクセスポイント
ECW5211-L 設定例

開梱～社内ネットワークで使用開始までのシンプル設定例

2023.7.31



■設定したいこと

ECW5211-Lを新たに設置し、クライアント端末が無線で社内ネットワークにアクセスできるようにしたい

■対応型式、ファームウェアバージョン

- ECW5211-L: 3.45.0000 以降

■設定方法

- 次ページ以降をご参照ください。

■設定後の動作*1

- クライアント端末が無線で社内ネットワークにアクセス可能になります。
- 管理者がブラウザGUI経由でアクセスポイントにアクセス可能になり、アクセスポイント設定を変更可能です。
- GUIを使って最新のファームウェアへ更新が可能になります。

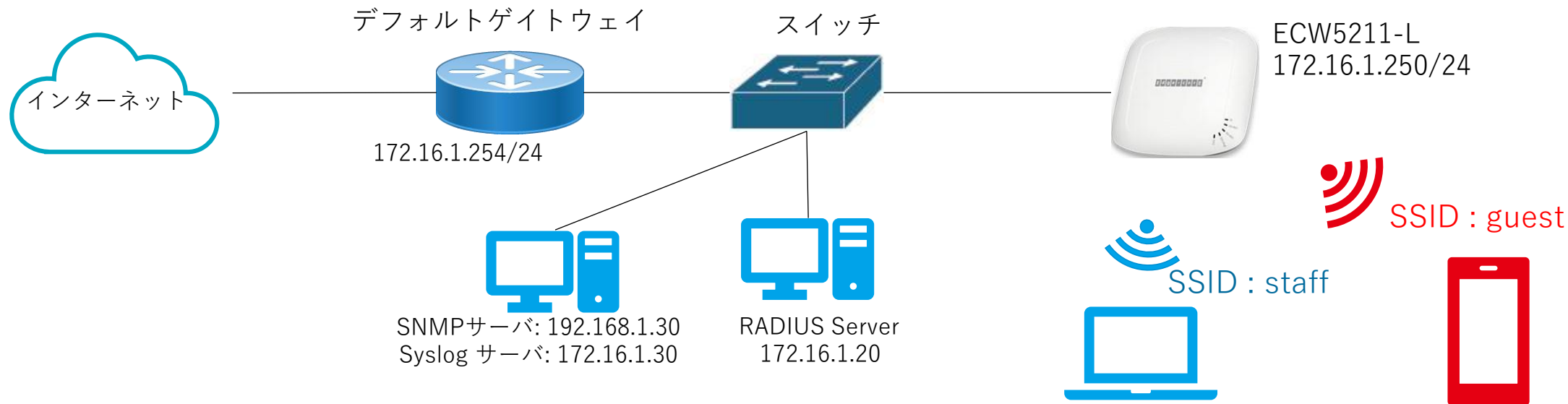
*1

- 記載の動作内容は事前に通知なく変更されることがあります。
- 最新の情報は、Edgecore Networks社発行のユーザーマニュアルをご参照ください。ユーザーマニュアルは以下URLよりダウンロード可能です
- URL: <https://www.apresia.jp/products/wireless/support/download.html>

ECW5211-L

開梱～社内ネットワークで使用開始までのシンプル設定例

本ドキュメントでは、以下のネットワーク構成における設定例を説明します。



アクセスポイントの無線設定

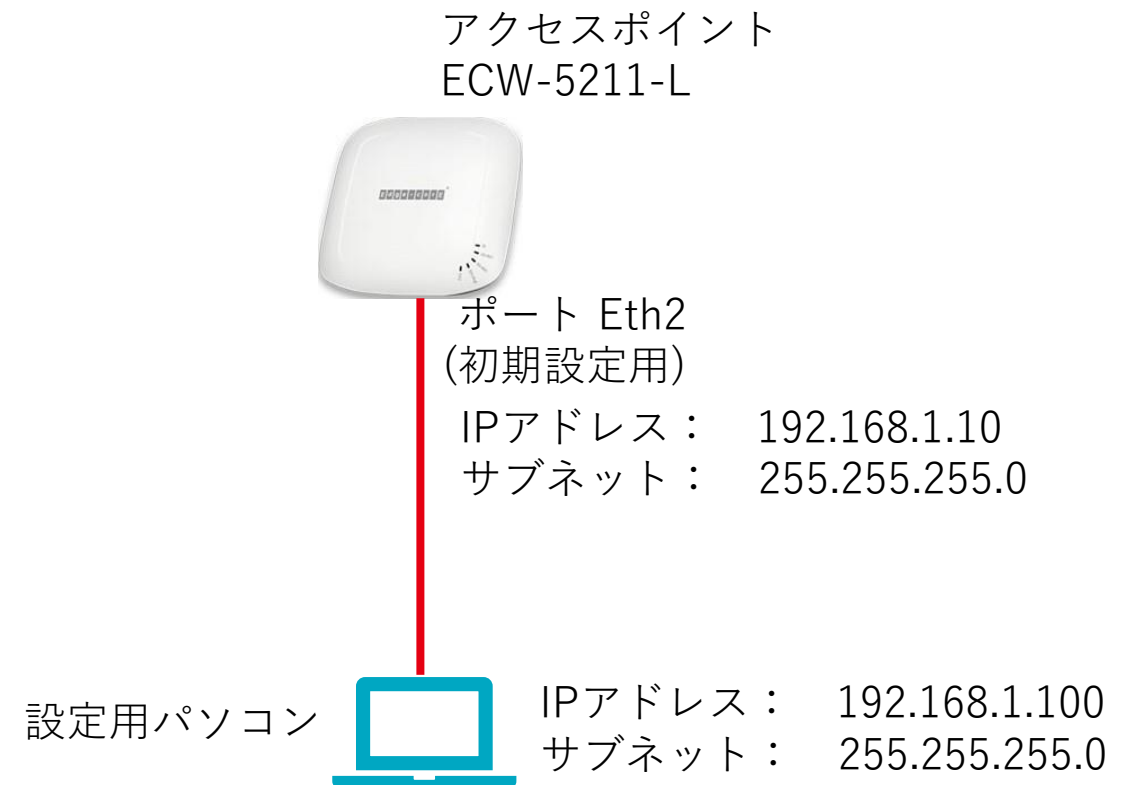
VAP	VAP-1	VAP-2
SSID	staff	guest
用途	従業員用	ゲスト用
VLAN ID	10	20
認証方式	WPA2 エンタープライズ (ID/パスワード)	WPA2 パーソナル (PSK)

備考

1. アクセスポイントECW5211-Lには2.4GHzと、5GHz用の2つの無線カード(RF Card A/B)があります。この設定例では、RF Card A/B両方で同じSSIDを出力します。
2. VAP(Virtual Access Point = 仮想アクセスポイント)機能を使用することで、1つの物理アクセスポイント上に複数の仮想アクセスポイントを表示できます。各VAPは個別の設定(SSID, ネットワークモード, VLAN ID, セキュリティ)を使用して個別に有効・無効にできます。アクセスポイントは複数のSSIDを通して異なるクライアントをサポートできます。VAPは各無線カードごとに最大8個設定できます。

(1)
アクセスポイント初期設定用の準備を行います。

- ① 付属のACアダプターを使用してアクセスポイントへ給電します。
- ② 設定用のパソコンのIPアドレスをアクセスポイントのサブネットのIPアドレスに設定します。右の接続図ではIPアドレスを192.168.1.100、サブネットマスクを255.255.255.0に設定しています。
- ③ アクセスポイントのポートEth2と設定用パソコンをLANケーブルで接続します。アクセスポイントの初期設定用のEth2ポートのIPアドレスは192.168.1.10、サブネットマスクは255.255.255.0です。



(2)

アクセスポイントへログインします。

- ① 設定用PCでウェブブラウザを開き、アドレスバーにアクセスポイントのIPアドレス 192.168.1.10を入力しアクセスポイントのウェブ管理インターフェース(WMI)へアクセスします。
- ② アクセスポイントのWMIへアクセスができると、ログイン画面が表示されます。
- ③ アクセスポイントの初期設定のユーザ名:admin、パスワード:adminを入力し、ログインボタンをクリックしアクセスポイントへログインします。ログインが成功するとシステム概要画面が表示されます。

注) ログイン画面が表示されない場合：

- アクセスポイントが起動中である(アクセスポイントの電源LEDが点滅中) → 電源LEDが点灯してからアクセスしてください。
- 設定用のPCでPingコマンドでアクセスポイントから応答があるか確認してください。



ログイン画面



システム概要画面

(3)
ログインパスワードを変更します。

- ① Utilities->パスワード変更のタブを選択し、パスワード変更の画面へ移動します。
- ② パスワード変更の画面で、admin(管理者)の新しいパスワードと新しいパスワード（再入力）の欄にパスワードを入力します。パスワードに使用できる文字は英数字のみです。パスワード長は最大32文字です。
- ③ 保存ボタンをクリックすると、ログイン画面へ遷移します。
- ④ 必要に応じてuser(ユーザー) のパスワードを変更します。userはアクセスポイントの再起動、設定変更はできませんが、全てのWMIの画面を閲覧できます。

System Wireless Firewall Utilities Status

パスワード変更 バックアップ・リストア ファームウェア更新 再起動 証明書のアップロード バックグラウンドスキャン 発見ツール ネットワークツール

ホーム > ユーティリティ > パスワード変更

パスワード変更

ユーザ名: admin
新しいパスワード: *最大32文字
新しいパスワード(再入力):

ユーザ名: user
新しいパスワード: *最大32文字
新しいパスワード(再入力):

パスワード変更

ユーザ名: admin
新しいパスワード: *最大32文字
新しいパスワード(再入力):

ユーザ名: user
新しいパスワード: *最大32文字
新しいパスワード(再入力):

保存 キャンセル

(4)
システム情報を設定します。

① System→システム情報のタブを選択します。

② システム情報が表示され、以下の項目を登録します。
アクセスポイント名のみ登録必須です。

- アクセスポイント名：アクセスポイントを識別できるようにアクセスポイント名を入力します。この項目はSNMPのオブジェクトSysNameに反映されます。
- 説明：アクセスポイント詳細情報を入力します。
- 設置場所：アクセスポイント設置場所を入力します。この項目はSNMPのオブジェクトSysNameに反映されません

③ 保存ボタンをクリックします。

④ アラームメッセージが表示されますので、適用をクリックし、確認ダイアログのウィンドウでOKボタンをクリックします。



システム情報

アクセスポイント名: *

説明:

設置場所:



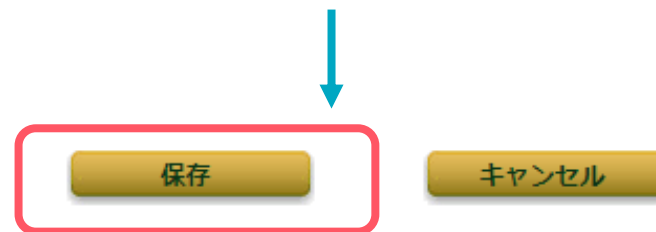
変更を保存しました。しかし"適用"ボタンをクリックするまで有効になりません。 **適用**

(5)
時刻設定を行います。

- ① System→システム情報のタブを選択します。
- ② タイムゾーン ドロップダウンリストから
(GMT+9:00) Osaka,Sapporo,Tokyoを選択します
- ③ 時刻の設定方法を選択します。ここではNTPを使用するを選びます。
- ④ NTPサーバ1, NTPサーバ2 の欄にNTPサーバのIPアドレスまたはFQDNを入力して保存をクリックします。
- ⑤ 保存ボタンをクリックします。アラームメッセージが表示されますので、適用をクリックし、確認ダイアログのウィンドウでOKボタンをクリックします。

時刻設定

現在の時刻 :	2000/01/01 01:10:49
タイムゾーン :	(GMT+09:00)Osaka,Sapporo,Tokyo ▼
時刻設定 :	<input checked="" type="radio"/> NTPを使用する <input type="radio"/> 手動設定
NTP サーバ 1 :	172.16.1.30 *
NTP サーバ 2 :	ntp.nict.jp



注)アクセスポイントはシステム時刻を保持しませんので、再起動時にシステム時刻がリセットされます。システム時刻はNTPサーバから取得することを推奨します。

(5) アクセスポイントのネットワーク設定を行います。

- ① System→ネットワーク設定のタブを選択します。
- ② ネットワークセッティングのモード選択でスタティックを選び、IPアドレス、ネットマスク、デフォルトゲートウェイ、プライマリDNSサーバ、必要に応じて代替DNSサーバ情報を入力します。
- ③ イーサーネットIGMPスヌーピング、LLDP、レイヤー2STPは導入環境に合わせて設定してください。ここでは全て無効を選択しています。
- ④ 保存ボタンをクリックします。アラームメッセージが表示されますので適用をクリックし、確認ダイアログウィンドウでOKボタンをクリックします。
- ⑤ アクセスポイントが再起動します。再起動後、設定したIPアドレスでアクセスポイントのWMIにログインしてください。

ホーム > システム > ネットワークセッティング

ネットワークセッティング

モード: スタティック DHCP

IPアドレス: *

ネットマスク: *

デフォルトゲートウェイ: *

プライマリDNSサーバ: *

代替DNSサーバ:

イーサーネットIGMPスヌーピング: 無効 有効

LLDP: 無効 有効

レイヤー2 STP:

(6)
SNMP Trap通知、Syslog送信設定を行います。

- ① System→管理機能のタブを選択します。
- ② SNMP設定を行います。
 - SNMP v1/v2cの場合コミュニティー名 Read, Writeを設定
 - トラップの送信を有効にし、SNMPサーバ(Trap送信先)のIPアドレスを設定
- ③ Syslog設定を行います。
 - ログレベルをドロップダウンリストから選択
 - 外部Syslogサーバを有効に設定
 - Syslogサーバ(Syslog送信先)のIPアドレスを設定
 - 必要に応じて、ポート番号を変更
- ④ 保存ボタンをクリックします。アラームメッセージが表示されますので適用をクリックし、確認ダイアログウィンドウでOKボタンをクリックします。

The screenshot shows the configuration interface of the device. The 'System' tab is selected, and the 'Management Function' sub-tab is highlighted. A blue arrow points from the 'Management Function' sub-tab to the configuration page below.

SNMP設定:

- 無効 有効
- コミュニティー名:
 - Read:
 - Write:
-
- トラップの送信: 無効 有効
- SNMPサーバのIPアドレス:

ログレベル:

外部Syslogサーバ:

- 無効 有効
- SNMPサーバのIPアドレス:
- ポート番号:

(7)
管理端末のIPアドレスを設定します。

WMIにアクセスできる管理端末のIPアドレスを設定することにより、WMIにアクセスできる端末を制限することができます。デフォルトの設定では0.0.0.0/0.0.0.0が設定されてすべてのIPアドレスからWMIにアクセスできる設定になっています。

- ① System→管理機能のタブを選択します。
- ② 管理可能な端末のIPアドレス欄のIPアドレスリストの編集ボタンをクリックすると、管理端末のIPアドレスリストのページが表示されます。
- ③ WMIにアクセスできるIPアドレス(またはネットワークアドレス)/サブネットマスクを設定します。
- ④ 保存ボタンをクリックします。



ホーム > システム > 管理機能 > 管理端末のIPアドレスリスト

管理端末のIPアドレスリスト

管理端末のIPアドレスリスト			
No.	IPアドレス/サブネットマスク	No.	IPアドレス/サブネットマスク
1	0.0.0.0/0.0.0.0	2	
3		4	
5		6	
7		8	
9		10	



(8)
スタッフ用にRF Card A(2.4GHz)VAP-1の設定を行います。

- ① Wireless→VAP設定のタブを選択します。
- ② プロファイル名：ドロップダウンリストから RF Card A : VAP-1 を選択します。
- ③ VAP : 有効 を選択します。
- ④ プロファイル名：管理しやすい名称を設定します。
- ⑤ ESSID : SSID staff を設定します。
- ⑥ ネットワークモードでブリッジモードを選択します。
- ⑦ VLAN ID : 有効にし、VLAN ID : 10を設定します。
- ⑧ 保存ボタンをクリックすると、アラームメッセージが表示されますので、適用をクリックし、ダイアログのウィンドウでOKをクリックします。

The screenshot shows the configuration interface for the wireless network. The 'Wireless' tab is selected, and the 'VAP設定' sub-tab is active. The configuration page is titled 'VAP設定' and includes the following settings:

- プロファイル名: RF Card A : VAP-1 (dropdown menu)
- VAP: 無効 有効
- プロファイル名: staff (text input)
- ESSID: staff (text input)
- ネットワークモード: ブリッジモード (dropdown menu)
- アップリンク帯域幅: 0 Kbits/秒 *(1-1048576, 0:無効)
- ダウンリンク帯域幅: 0 Kbits/秒 *(1-1048576, 0:無効)
- VLAN ID: 無効 有効
- VLAN ID: 10 *(1 - 4094)
- アップリンク802.1p: Best Effort (BE) (dropdown menu)
- CAPWAPトンネルインターフェイス: 無効 (dropdown menu)

At the bottom of the page, there are two buttons: '保存' (Save) and 'キャンセル' (Cancel).

(9) スタッフ用にRF Card B(5GHz) VAP-1の設定を行います。

- ① Wireless→VAP設定のタブを選択します。
- ② プロファイル名：ドロップダウンリストから RF Card B : VAP-1 を選択します。
- ③ VAP : 有効 を選択します。
- ④ プロファイル名：管理しやすい名称を設定します。
- ⑤ ESSID : staff SSIDを設定します。
- ⑥ ネットワークモードでブリッジモードを選択します。
- ⑦ VLAN ID : 有効にし、VLAN ID : 10を設定します。
- ⑧ 保存ボタンをクリックするとアラームメッセージが表示されますので、適用をクリックし、ダイアログの表示でOKをクリックします。



VAP設定

プロファイル名: RF Card B : staff ▼
RF Card B : staff

VAP: 無効 有効

プロファイル名: staff

ESSID: staff

ネットワークモード: ブリッジモード ▼

アップリンク帯域幅: 0 Kbits/秒 *(1-1048576, 0:無効)

ダウンリンク帯域幅: 0 Kbits/秒 *(1-1048576, 0:無効)

VLAN ID: 無効 有効
VLAN ID: 10 *(1 - 4094)

アップリンク802.1p: Best Effort (BE) ▼

CAPWAPトンネルインターフェイス: 無効 ▼

172.16.1.250 の内容

「802.1p」と「アップリンクの帯域幅」の設定は、同じVLAN IDを持つすべてのVAPに適用されます。
続けますか？

OK

キャンセル

(10)
スタッフ用にRF Card A(2.4GHz) VAP-1のセキュリティ設定を行います。

- ① Wireless→セキュリティ設定のタブを選択します。
- ② プロファイル名でRF Card A: staff を選択します。
- ③ セキュリティタイプでWPA-Enterpriseを選択します。
- ④ 暗号スイートでWPA2を選択します。
- ⑤ 管理フレーム保護は環境に応じて設定してください。
- ⑥ RADIUSサーバを設定します。
 - ホスト：RADIUSサーバのIPアドレスまたはホスト名を入力します。
 - 認証ポート：必要に応じて変更します。
 - 秘密鍵：RADIUSサーバの秘密鍵を設定します。
- ⑦ 保存ボタンをクリックします。

ホーム > 無線LAN設定 > セキュリティ設定

セキュリティ設定

プロファイル名: RF Card A: staff

セキュリティタイプ: WPA-Enterprise 802.11r ローミング

暗号スイート: WPA2

管理フレーム保護: 任意

グループキーアップデート周期: 86400 秒*(60 - 86400, 0:無効)

プライマリRADIUSサーバ:

ホスト: 172.16.1.20 *(ドメイン名 / IPアドレス)

認証ポート: 1812 *

秘密鍵: himitsu *

アカウントサービス: 無効 有効

アカウントポート: 1813 *

アカウントインテリムアップデート間隔: 60 秒*

セカンダリRADIUSサーバ:

ホスト: (ドメイン名 / IPアドレス)

認証ポート:

秘密鍵:

アカウントサービス: 無効 有効

アカウントポート:

アカウントインテリムアップデート間隔: 秒

保存 キャンセル

(11)
スタッフ用にRF Card B(5GHz) VAP-1のセキュリティ設定を行います。

- ① Wireless→セキュリティ設定のタブを選択します。
- ② プロファイル名でRF Card B: staff を選択します。
- ③ セキュリティタイプでWPA-Enterpriseを選択します。
- ④ 暗号スイートでWPA2を選択します。
- ⑤ 管理フレーム保護 は環境に応じて設定してください。
- ⑥ RADIUSサーバを設定します。
 - ホスト：RADIUSサーバのIPアドレスまたはホスト名を入力します
 - 認証ポート：必要に応じて変更します。
 - 秘密鍵：RADIUSサーバの秘密鍵を設定します。
- ⑦ 保存ボタンをクリックします。

ホーム > 無線LAN設定 > セキュリティ設定

セキュリティ設定

プロファイル名: RF Card B: staff

セキュリティタイプ: WPA-Enterprise 802.11r ローミング

暗号スイート: WPA2

管理フレーム保護: 任意

グループキーアップデート周期: 86400 秒*(60 - 86400, 0:無効)

プライマリRADIUSサーバ:

ホスト: 172.16.1.20 *(ドメイン名 / IPアドレス)

認証ポート: 1812 *

秘密鍵: himitsu *

アカウントサービス: 無効 有効

アカウントポート: 1813 *

アカウントインテリムアップデート間隔: 60 秒*

セカンダリRADIUSサーバ:

ホスト: (ドメイン名 / IPアドレス)

認証ポート:

秘密鍵:

アカウントサービス: 無効 有効

アカウントポート:

アカウントインテリムアップデート間隔: 秒

保存 キャンセル

(12)
ゲスト用にRF Card A(2.4GHz) VAP-2の設定を行います。

- ① Wireless→VAP設定のタブを選択します。
- ② プロファイル名でRF Card A : VAP-2を選択します。
- ③ VAP で 有効 を選択します
- ④ プロファイル名 で管理しやすい名称に変更します。
- ⑤ ESSID で、SSID guestを設定します。
- ⑥ ネットワークモードでブリッジモードを選択します。
- ⑦ アップリンク帯域幅、ダウンリンク帯域幅：帯域幅を制限する場合は設定します。
- ⑧ VLAN ID を有効にし、VLAN ID：20を設定します。
- ⑨ 保存ボタンをクリックするとアラームメッセージが表示されますので、適用をクリックし、ダイアログの表示でOKをクリックします。

ホーム > 無線LAN設定 > VAP設定

VAP設定

プロファイル名: RF Card A : guest ▼

VAP: 無効 有効

プロファイル名:

ESSID:

ネットワークモード: ▼

アップリンク帯域幅: Kbits/秒 *(1-1048576, 0:無効)

ダウンリンク帯域幅: Kbits/秒 *(1-1048576, 0:無効)

VLAN ID: 無効 有効

VLAN ID: *(1 - 4094)

アップリンク802.1p: ▼

CAPWAPトンネルインターフェイス: ▼

(13)
ゲスト用にRF Card B(5GHz) VAP-2の設定を行います。

- ① Wireless→VAP設定のタブを選択します。
- ② プロファイル名でRF Card B : VAP-2を選択します。
- ③ VAP で 有効 を選択します
- ④ プロファイル名 で管理しやすい名称に変更します。
- ⑤ ESSID で、SSID guestを設定します。
- ⑥ ネットワークモードでブリッジモードを選択します。
- ⑦ アップリンク帯域幅、ダウンリンク帯域幅：帯域幅を制限する場合は設定します。
- ⑧ VLAN ID を有効にし、VLAN ID：20を設定します。
- ⑨ 保存ボタンをクリックするとアラームメッセージが表示されますので、適用をクリックし、ダイアログの表示でOKをクリックします。



VAP設定

プロファイル名: RF Card B : VAP-2

VAP: 無効 有効

プロファイル名:

ESSID:

ネットワークモード:

アップリンク帯域幅: Kbits/秒 *(1-1048576, 0:無効)

ダウンリンク帯域幅: Kbits/秒 *(1-1048576, 0:無効)

VLAN ID: 無効 有効

VLAN ID: *(1 - 4094)

アップリンク802.1p:

CAPWAPトンネルインターフェイス:

保存

172.16.1.250 の内容

警告: VLAN ID が右記と同じです: RF Card A : VAP 2

「802.1p」と「アップリンクの帯域幅」の設定は、同じVLAN IDを持つすべてのVAPに適用されます。
続けますか？

(14)
ゲスト用にRF Card A(2.4GHz) VAP-2のセキュリティ設定を行います。

- ① Wireless→セキュリティ設定のタブを選択します。
- ② セキュリティタイプでWPA-Personalを選択します。
- ③ 暗号スイートでWPA2を選択します。
- ④ 管理フレーム保護は環境に応じて設定して下さい
- ⑤ プリシェアードキータイプでパスフレーズを選択します。
- ⑥ プリシェアードキーでパスワードを設定します。
- ⑦ 保存ボタンをクリックします。



セキュリティ設定

プロフィール名: RF Card A : guest ▼

セキュリティタイプ: WPA-Personal ▼ 802.11r ローミング

暗号スイート: WPA2 ▼

管理フレーム保護: 任意 ▼

プリシェアードキータイプ: PSK(Hex)*(64文字) パスフレーズ*(8 - 63文字)

プリシェアードキー: password

グループキーアップデート周期: 86400 秒*(60 - 86400, 0:無効)

(15)
ゲスト用にRF Card B(5GHz) VAP-2のセキュリティ設定を行います。

- ① Wireless→セキュリティ設定のタブを選択します。
- ② セキュリティタイプでWPA-Personalを選択します。
- ③ 暗号スイートでWPA2を選択します。
- ④ 管理フレーム保護は環境に応じて設定して下さい
- ⑤ プリシェアードキータイプでパスフレーズを選択します。
- ⑥ プリシェアードキーでパスワードを設定します。
- ⑦ 保存ボタンをクリックします。



セキュリティ設定

プロフィール名: RF Card B : guest ▼

セキュリティタイプ: WPA-Personal ▼ 802.11r ローミング

暗号スイート: WPA2 ▼

管理フレーム保護: 任意 ▼

プリシェアードキータイプ: PSK(Hex)*(64文字) パスフレーズ*(8 - 63文字)

プリシェアードキー: password

グループキーアップデート周期: 86400 秒*(60 - 86400, 0:無効)

(16)
アクセスポイントのVAPの一覧を表示し、各VAPの設定状態を確認します。

- ① Wireless→VAP一覧のタブを選択します。
- ② VAP一覧の各VAPのステータス、セキュリティ、MACフィルタリング、Hotspot2.0のリンクをクリックすると、設定ページへ移動できます。



VAP一覧

RF Card A

VAP No.	ESSID	ネットワークモード	ステータス	セキュリティ	MACフィルタリング	Hotspot 2.0
1	staff	ブリッジモード	有効	WPA-Enterprise	無効	無効
2	guest	ブリッジモード	有効	WPA-Personal	無効	無効
3	Virtual Access Point 2	ブリッジモード	無効	Open	無効	無効

RF Card B

VAP No.	ESSID	ネットワークモード	ステータス	セキュリティ	MACフィルタリング	Hotspot 2.0
1	staff	ブリッジモード	有効	WPA-Enterprise	無効	無効
2	guest	ブリッジモード	有効	WPA-Personal	無効	無効
3	Virtual Access Point 2	ブリッジモード	無効	Open	無効	無効

(17)
アクセスポイントの2.4GHz帯の無線設定を行います。

- ① Wireless→基本設定のタブを選択します。
- ② 無線カード名でRF Card Aを選択します。
- ③ 2.4GHz帯を使わない場合は、バンドで無効を選びます。
- ④ チャンネルで固定チャンネルかAutoを選びます。Autoを選択した場合、アクセスポイントは電源投入時チェックの入ったチャンネルからチャンネルを選択します。
- ⑤ 送信パワーで信号強度を設定します。Level 1が最大電力でLevelが1下がるごとに1dBmずつ出力電力が下がります。
- ⑥ バンドステアリングを有効にすると、5GHz帯に接続できるクライアントを5GHz帯に誘導します。
- ⑦ 保存ボタンをクリックします。

System Wireless Firewall Utilities Status

VAP基本設定 VAP設定 セキュリティ リピーター設定 詳細設定 アクセスコントロール Hotspot 2.0

ホーム > 無線LAN設定 > 一般設定

一般設定

無線カード名: RF Card A

バンド: 2.4GHz

プロトコル: 802.11g+802.11n 11nのみ有効

ショートプリアンプル: 無効 有効

ショートガードインターバル: 無効 有効

アンテナモード: 2T2R

チャンネル幅: 20 MHz

チャンネル: Auto

送信パワー: Level 1

ビーコン間隔: 100 ミリ秒 *(100 - 500)

エアタイムフェアネス: 無効 公平アクセス 優先アクセス

パケット遅延しきい値: 0 ミリ秒 *(100 - 5000, 0:無効)

アイドルタイムアウト: 300 秒 *(60 - 60000)

バンドステアリング: 無効 有効

アグレッシブ方式

干渉検出: 利用しきい値 0 % *(10 - 99, 0:無効)

WME設定: 設定

送信レートしきい値: 1001 kbps *(0:無効)

U-APSD: 無効 有効

保存 キャンセル

(18)
アクセスポイントの5GHz帯の無線設定を行います。

- ① Wireless→基本設定のタブを選択します。
- ② 無線カード名でRF Card Bを選択します。
- ③ 5GHz帯を使わない場合は、バンドで無効を選びます。
- ④ チャンネルで固定チャンネルかAutoを選びます。Autoを選択した場合、アクセスポイントは電源投入時チェックの入ったチャンネルからチャンネルを選択します。
- ⑤ 送信パワーで信号強度を設定します。Level 1が最大電力でLevelが1下がるごとに1dBmずつ出力電力が下がります。
- ⑥ バンドステアリングを有効にすると、5GHz帯に接続できるクライアントを5GHz帯に誘導します。
- ⑦ 保存ボタンをクリックします。

System Wireless Firewall Utilities Status

VAP-基本設定 VAP-セキュリティ リピーター設定 詳細設定 アクセスコントロール Hotspot 2.0

ホーム > 無線LAN設定 > 一般設定

一般設定

無線カード名: RF Card B

バンド: 5GHz

プロトコル: 802.11ac 11nのみ有効

ショートガードインターバル: 無効 有効

アンテナモード: 2T2R

チャンネル幅: 80 MHz

チャンネル: Auto 非DFSオートチャンネル

チャンネル選択:	<input checked="" type="checkbox"/> 36	<input checked="" type="checkbox"/> 40	<input checked="" type="checkbox"/> 44	<input checked="" type="checkbox"/> 48
	<input checked="" type="checkbox"/> 52	<input checked="" type="checkbox"/> 56	<input checked="" type="checkbox"/> 60	<input checked="" type="checkbox"/> 64
	<input checked="" type="checkbox"/> 100	<input checked="" type="checkbox"/> 104	<input checked="" type="checkbox"/> 108	<input checked="" type="checkbox"/> 112
	<input checked="" type="checkbox"/> 116	<input checked="" type="checkbox"/> 120	<input checked="" type="checkbox"/> 124	<input checked="" type="checkbox"/> 128

送信パワー: Level 1

ビーコン間隔: 100 ミリ秒 *(100 - 500)

エアタイムフェアネス: 無効 公平アクセス 優先アクセス

パケット遅延しきい値: 0 ミリ秒 *(100 - 5000, 0:無効)

アイドルタイムアウト: 300 秒 *(60 - 60000)

バンドステアリング: 無効 有効

アグレッシブ方式

干渉検出: 利用しきい値 0 % *(10 - 99, 0:無効)

WME設定: 設定

送信レートしきい値: 1001 kbps *(0:無効)

U-APSD: 無効 有効

保存 キャンセル

(19)
VAP毎に詳細設定を行います。

- ① Wireless→詳細設定のタブを選択します。
- ② プロファイル名で設定するVAPを選択します。
- ③ SSIDがクライアント端末に表示されなくしたい場合は、SSIDブロードキャストで無効を選びます。
- ④ クライアント間の通信を遮断したい場合、無線端末アイソレーションで有効を選択します。
- ⑤ 受信RSSIしきい値を設定すると、クライアントのRSSIが閾値以下になると、そのクライアントはアクセスポイントから切断されます。
- ⑥ 最後に保存ボタンをクリックします。



プロファイル名: RF Card A : staff ▼

DTIM間隔: 1 *(1 - 15)

連続リトライしきい値: 0 *(2 - 50, 0:無効)

SSIDブロードキャスト: 無効 有効

無線端末アイソレーション: 無効 有効

IAPP: 無効 有効

マルチキャスト・ユニキャスト変換: 無効 有効

送信側STBC: 無効 有効

チキャスト/ブロードキャスト速度: 5.5M ▼

管理フレーム速度: 5.5M ▼

受信RSSIしきい値: -85 dBm *クライアントのRSSIがしきい値以下になった場合、APから切断されます(-95 ~ 0, 0:無効)

保存 キャンセル

(20)
VAP毎にアクセスポイントにアクセスできる最大クライアント数と、MACアドレスによるアクセスコントロール設定を行います。

① Wireless→アクセスコントロールのタブを選択します。

② プロファイル名でVAPを択します。

③ 最大クライアント数で、VAPに接続できる最大クライアント数を設定します。

④ アクセスコントロール方式を選択します。

- 無効：クライアントのアクセスは制限されません。
- MACアドレス(許可リスト)：リストに登録されているMACアドレスのクライアントのみアクセスできます。
- MACアドレス(拒否リスト)：リストに登録されているMACアドレスのクライアントはアクセスを拒否されます。
- RADIUS ACL：RADIUSでMACアドレスを認証します。



アクセスコントロール設定

プロファイル名:

最大クライアント数: *(1 ~ 128)

アクセスコントロール方式:

保存

キャンセル

(21)

アクセスコントロール方式でMACアドレス(許可リスト)を選択する場合、許可リストにクライアントのMACアドレスを登録します。

- ① プロファイル名で設定するVAPを選択します。
- ② アクセスコントロール方式でMACアドレス(許可リスト)を選択します。
- ③ MACアドレスの欄にMACアドレスを登録し、状態の欄で有効を選びます。
- ④ 登録が完了したら、保存ボタンをクリックします。アラームメッセージが表示されますので、適用をクリックします。確認のダイアログが表示されますので、OKボタンをクリックします。

注)

- ① MACアドレスは最大100個登録できます。
- ② 状態の設定が無効の場合、そのMACアドレスのクライアントはアクセスを拒否されます。

アクセスコントロール設定

プロファイル名: RF Card A : VAP-1 ▼

最大クライアント数: 128 *(1 ~ 128)

アクセスコントロール方式: MACアドレス(許可リスト) ▼

No.	MACアドレス	状態
1	34:EF:B6:A8:5E:C0	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
2		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
3		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
4		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
5		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
6		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
7		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
8		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
9		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
10		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

最初へ 前へ 次へ 最後へ (合計: 100)

保存

キャンセル

(22)

アクセスコントロール方式でMACアドレス(拒否リスト)を選択する場合、拒否リストにクライアントのMACアドレスを登録します。

- ① プロファイル名で設定するVAPを選択します。
- ② アクセスコントロール方式でMACアドレス(拒否リスト)を選択します。
- ③ MACアドレスの欄にMACアドレスを登録し、状態の欄で有効を選びます。
- ④ 登録が完了したら、保存ボタンをクリックします。アラームメッセージが表示されますので、適用をクリックします。確認のダイアログが表示されますので、OKボタンをクリックします。

注)

- MACアドレスは最大100個登録できます。
- 状態の設定が無効の場合、そのMACアドレスのクライアントはアクセスを許可されます

アクセスコントロール設定

プロファイル名: RF Card A : VAP-1 ▼

最大クライアント数: 128 *(1 ~ 128)

アクセスコントロール方式: MACアドレス(拒否リスト) ▼

No.	MACアドレス	状態
1	34:EF:B6:A8:5E:C0	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
2		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
3		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
4		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
5		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
6		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
7		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
8		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
9		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
10		<input checked="" type="radio"/> 無効 <input type="radio"/> 有効

最初へ 前へ 次へ 最後へ (合計: 100)

保存

キャンセル

(23)
アクセスコントロール方式でRADIUS ACLを選択する場合
RADIUSサーバの各種設定を入力します。

- ① プロファイル名で設定するVAPを選択します。
- ② アクセスコントロール方式でRADIUS ACLを選択します。
- ③ RADIUSサーバのIPアドレス、認証ポート、秘密鍵を設定します。
- ④ 保存ボタンをクリックします。アラームメッセージが表示されますので、適用をクリックします。確認のダイアログが表示されますので、OKボタンをクリックします。
- ⑤ RADIUSサーバの設定は、セキュリティーのRADIUSサーバの設定と共有されます。

ホーム > 無線LAN設定 > アクセスコントロール設定

アクセスコントロール設定

プロフィール名: RF Card A : staff ▼

最大クライアント数: *(1 ~ 128)

アクセスコントロール方式: RADIUS ACL ▼

プライマリRADIUSサーバ: この設定はこのVAPと同じRADIUSサーバを使っているセキュリティー設定にも運用されます

ホスト: *(ドメイン名またはIPアドレス)

認証ポート番号: *(1 - 65535)

秘密鍵: *

セカンダリRADIUSサーバ:

ホスト:

認証ポート番号:

秘密鍵:

(24)
アクセスポイントの現在の設定をPC上のローカルディスクのバックアップファイルに保存します。

- ① Utilities->バックアップ・リストアのタブを選択し、バックアップ・リストアの画面を表示します。
- ② バックアップのボタンをクリックします。PCに設定のバックアップ config-backup.conf がダウンロードされます。



バックアップ・リストア

出荷状態に戻す:

ネットワーク設定を保持する

管理VLANの設定を保持する

現在の設定をファイルにバックアップする:

ファイルから設定をリストアする: 選択されていません

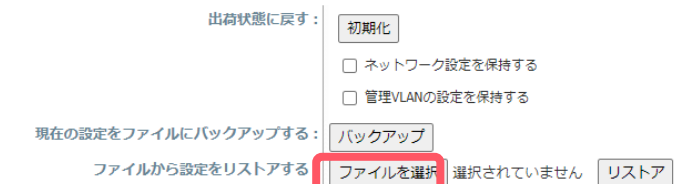
(25)

アクセスポイント故障時などハードウェアを交換した場合バックアップファイルからアクセスポイントの設定をリストアします。

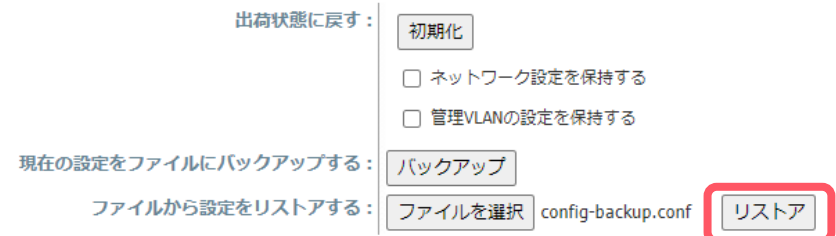
- ① Utilities->バックアップ・リストアのタブを選択し、バックアップ・リストアの画面を表示します。
- ② ファイルを選択をクリックし、PCにあるバックアップファイルを選択し、開くボタンをクリックします。
- ③ リストアボタンをクリックします。
- ④ 確認ダイアログが表示表示されますので、OKボタンをクリックします。アクセスポイントが再起動します。



バックアップ・リストア



バックアップ・リストア



192.168.1.10 の内容

このアクションはAPの再起動を伴います。続けますか?

OK

キャンセル

(26)-1

アクセスポイントを工場出荷時の状態に初期化する場合、WMI, SSHによる初期化と本体のResetボタンによる初期化の3つがあります。

1) WMIによる初期化

- ① Utilities→バックアップ・リストアのタブを選択し、バックアップ・リストアの画面を表示します。
- ② 初期化ボタンをクリックします。
- ③ 確認のダイアログが表示されますので、OKボタンをクリックします。
- ④ アクセスポイントが再起動し、工場出荷時の状態に初期化されます。



バックアップ・リストア



192.168.1.10 の内容

このアクションはAPの再起動を伴います。続けますか？

OK

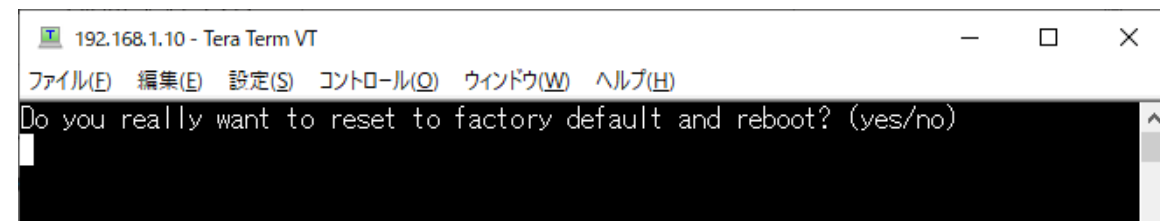
キャンセル

(26)-2

アクセスポイントを工場出荷時の状態に初期化する場合、WMI, SSHによる初期化と本体のResetボタンによる初期化の3つがあります。

2) SSHによる初期化

- ① Tera Term等のターミナルソフトでSSHでアクセスポイントに接続します。
- ② ユーザ名：reset2def, パスワード：reset2defでアクセスポイントにログインします。
- ③ ログイン後、初期化の確認ダイアログが表示されます。yesを入力し、enterを入力するとアクセスポイントは再起動し、初期化されます。



3) アクセスポイント本体のResetボタンによる初期化

- ① アクセスポイント本体のResetボタンを5秒以上押し続け、Resetボタンを離すとアクセスポイントは再起動し初期化されます。

- ✓ アクセスポイント開封から社内ネットワークで使用開始までのシンプル設定例は以上になります。
- ✓ 引き続き、お客様のネットワーク環境に合わせ必要な認証設定等を行ってください。

