Edgecore Network社 無線LANアクセスポイント

ECW5211-L

コンフィギュレーションガイド

APRESIA Systems株式会社

はじめに

本資料は、Edgecore　WiFiのAP単体で使用時の設定の手順をまとめたものです。

本資料に記載のない設定および詳細なパラメーターの説明はユーザーマニュアルをご参照ください。

使用機器

アクセスポイント 屋内用　ECW5211-L

APの初期設定準備

(1) 以下どちらかの方法でアクセスポイント(AP)へ給電します。

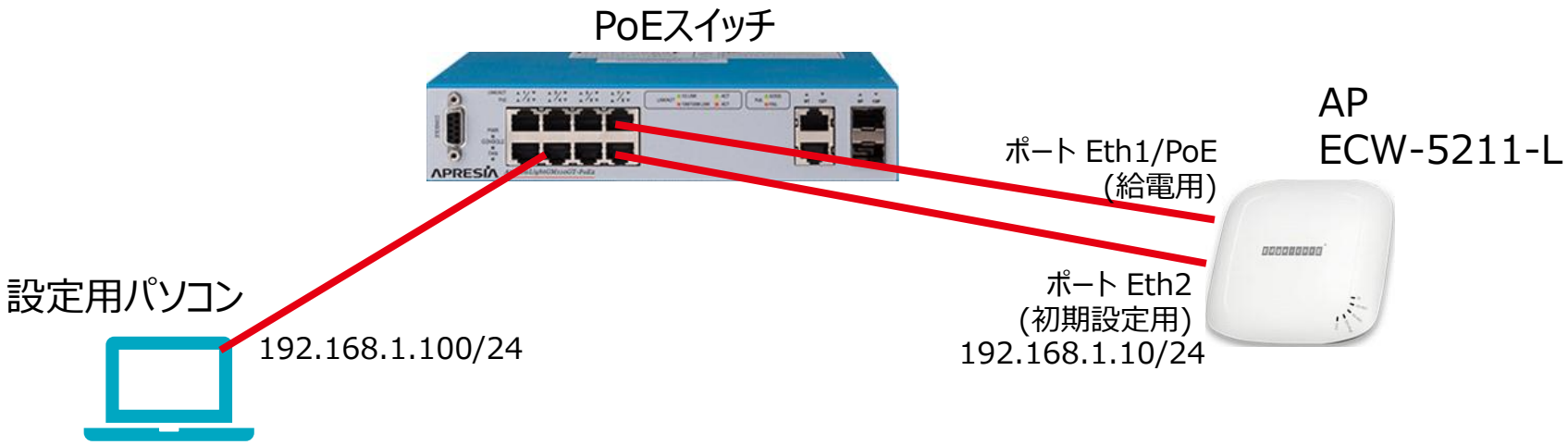
- ◇ 付属のACアダプターを使用して給電
- ◇ アクセスポイントのEth1/PoEポートからPoEで給電

(2) 設定用のパソコンのIPアドレスをAPのサブネットのIPアドレスに設定します。

- ◇ 下の接続図では192.168.1.100/24に設定しています。

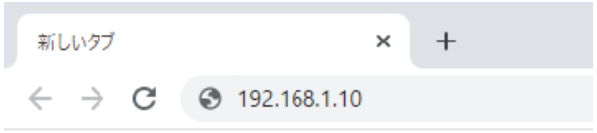
(3) APのポートEth2と設定用パソコンをLANケーブルで接続します。

- ◇ 以下の例ではアクセスポイントと設定用パソコンの間にPoEスイッチを入れています。
- ◇ APの初期設定用のEth2ポートのIPアドレスは 192.168.1.10/24 です。



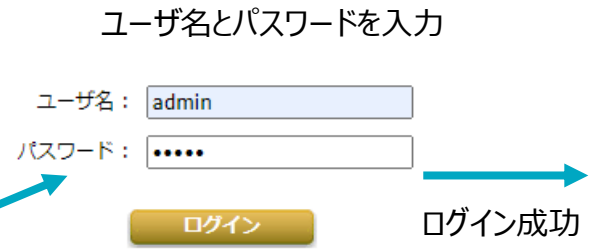
APへログイン

- 設定用PCでウェブブラウザを開き、アドレスバーにAPのIPアドレス 192.168.1.10を入力しAPのウェブ管理インターフェース(WMI)へアクセスします。



- AP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。
  - ログイン画面が表示されない場合：
    - APが起動中である(AP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APから応答があるか確認してください
- AP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APへログインします。
- ログインが成功するとシステム概要が表示されます。

ログイン画面



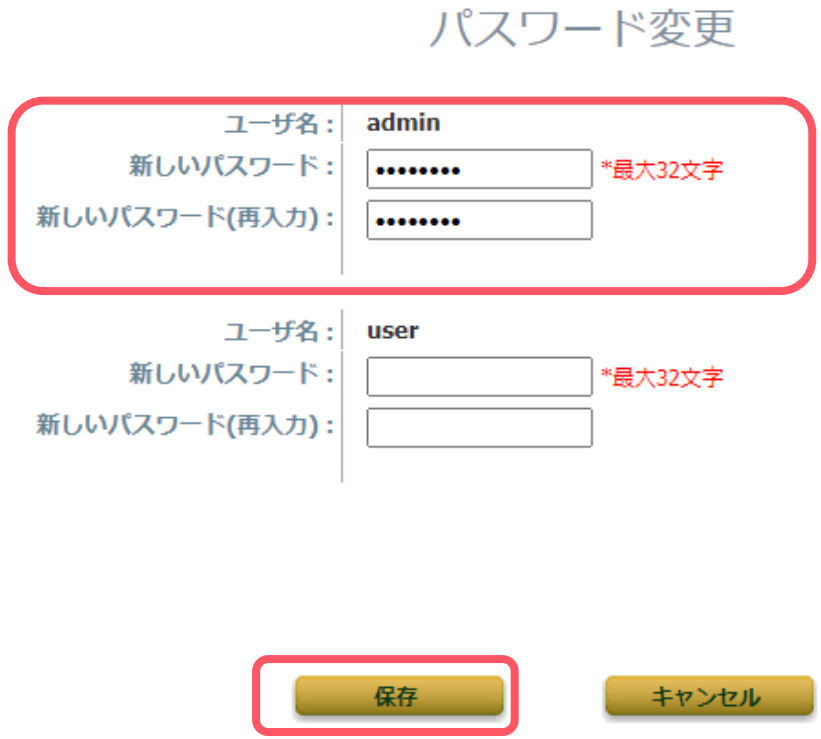
ログイン成功

システム概要画面

ログインパスワード変更

ホーム > ユーティリティー > パスワード変更

- admin(管理者)の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。
- user(ユーザー）のパスワードを変更します。
  - ✓ userはAP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。

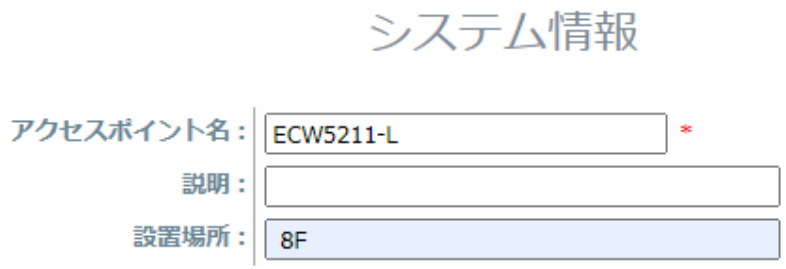


システム情報の設定

APを識別するための情報の設定をします。

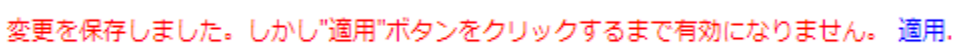
1. System→システム情報のタブを選択します。

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：APを識別できるようにAP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：APの詳細情報を入力します。
   - ◇ 場所：APの設置場所を入力します。この項目はSNMPのオブジェクトSysLocationに反映されます。



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。



時刻の設定

APの時刻の設定を行います。

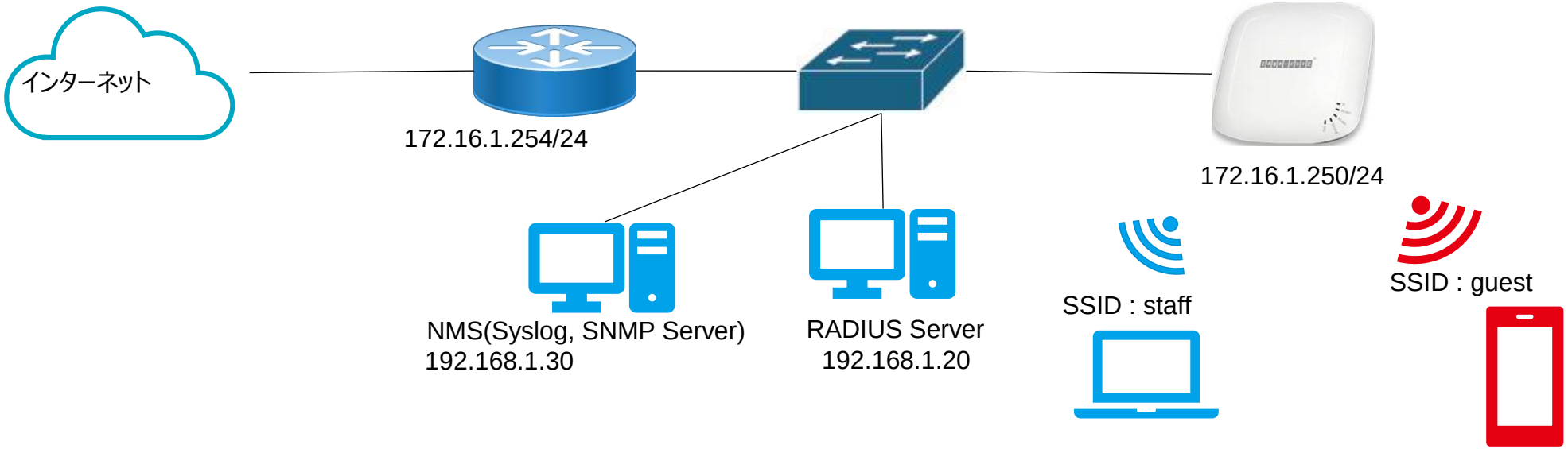
ホーム > システム > システム情報

1. System→システム情報のタブを選択します。
2. 時刻設定
   - ◇ 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。
   - ◇ 時刻設定　時刻の設定方法を選択します。
     - – NTPの有効化　システム時刻をNTPサーバと同期させます。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。
     - – 手動設定　システム時刻を手動で設定します。
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。

AP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。

ネットワーク構成

以下のネットワーク構成を例としてAPの設定方法を説明します。



APの無線設定

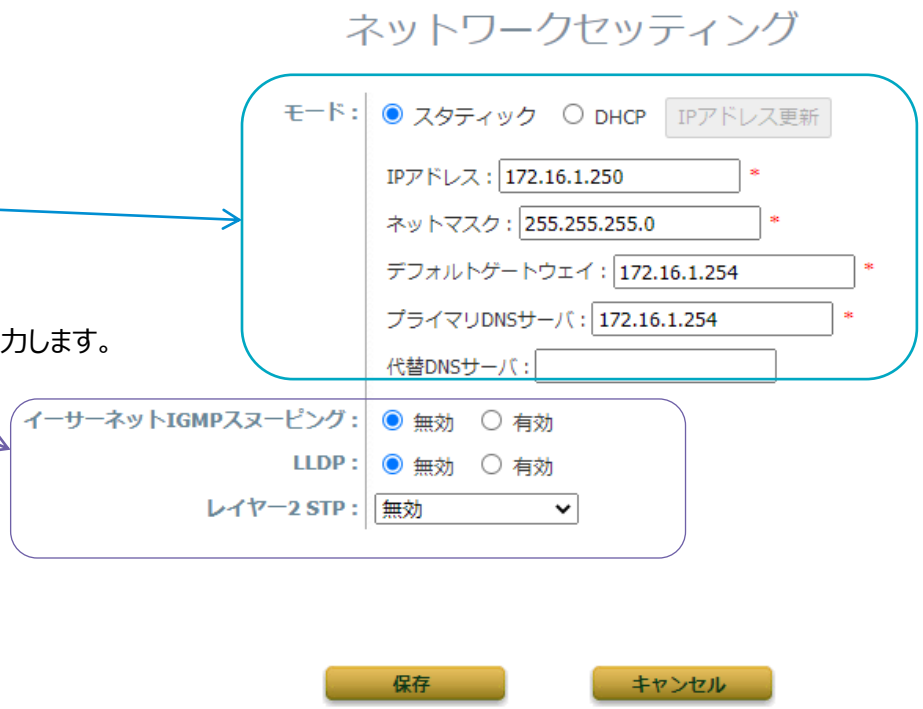
VAP	VAP-1	VAP-2
SSID	staff	guest
用途	従業員用	ゲスト用
VLAN ID	10	20
認証方式	WPA2 エンタープライズ （ID/パスワード）	WPA2 パーソナル (PSK)

APのネットワーク設定

APのLANインターフェースのネットワーク設定を行います。

1. 

2. ネットワークセッティングの欄の以下の項目を設定します。
   - ◇ モード：IPアドレスの設定方法をスタティックに選択します。
   - ◇ Staticを選択した場合、IPアドレス、ネットマスク、デフォルトゲートウェイ、DNSサーバ(プライマリ、代替)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。
4. 保存ボタンをクリックします。
5. 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。
6. APが再起動します。再起動後、設定したIPアドレスでAPのWMIにログインしてください。



SNMP/Syslog設定

SNMP Trap通知, Syslog送信先を設定します。（NMSでAPを監視する場合）

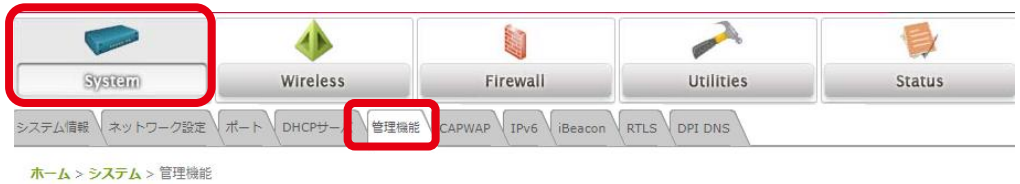
System→管理機能のタブを選択します。

- SNMP設定
  1. SNMP設定を有効にします。
  2. SNMP v1/v2cの場合コミュニティー名　Read, Writeを設定します。
  3. トラップの送信を有効にし、SNMPサーバ(Trap送信先)のIPアドレスを設定します。
- Syslog設定
  1. ログレベルをドロップダウンリストから選択します。
  2. 外部Syslogサーバを有効に設定にします。
  3. Syslogサーバ(Syslog送信先)のIPアドレスを設定します。
  4. 必要に応じて、ポート番号を変更します。
- 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。

管理端末のIPアドレス設定

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ので、設定を変更することを推奨します。

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します。

3. 管理端末のIPアドレスリストのページが表示されます。

4. 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。

5. 保存ボタンをクリックします。

無線設定　（無線カード、VAP）

- APには以下の２つの無線カード(RF Card)があります。各設定ページにRF Card A/Bでの表記がありますので、各カードの周波数帯に留意してください。

無線カード (RF Card)	周波数帯	無線LAN規格
RF Card A	2.4GHz帯	802.11b/g/n
RF Card B	5GHz帯	802.11a/n/ac

- VAP(仮想アクセスポイント,Virtual Access Point)
  - VAP機能を使用すると１つの物理AP上に以下の図のように複数の個別AP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。AP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。

VAP	SSID	セキュリティ	ネットワークモード	VLAN ID
VAP-1	staff	WPA2エンタープライズ	ブリッジ	10
VAP-2	guest	WPA2パーソナル	ブリッジ	20

VAP設定 – VAP-1 SSID : staff

RF Card A: VAP-1にSSID staff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：ドロップダウンリストから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します。
9. 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。

◆ 次に5GHz帯のプロファイル名：RF Card B：VAP-1に同様の設定をします。

VAP設定 – VAP-1 SSID : staff

RF Card B: VAP-1にSSID staff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：ドロップダウンリストから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。確認のダイアログが表示され、OKをクリックします。
8. 保存ボタンをクリックします。
9. 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。

セキュリティ設定 – SSID:staff

RF Card A：staff（VAP-1）に SSID：staff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：ドロップダウンリストからRF Card A: staff を選択します。
3. セキュリティタイプ：ドロップダウンリストからWPA-Enterpriseを選択します。
4. 暗号スイート：ドロップダウンリストからWPA2を選択します。
5. 管理フレーム保護：環境に応じて設定してください。

RADIUSサーバを設定します。

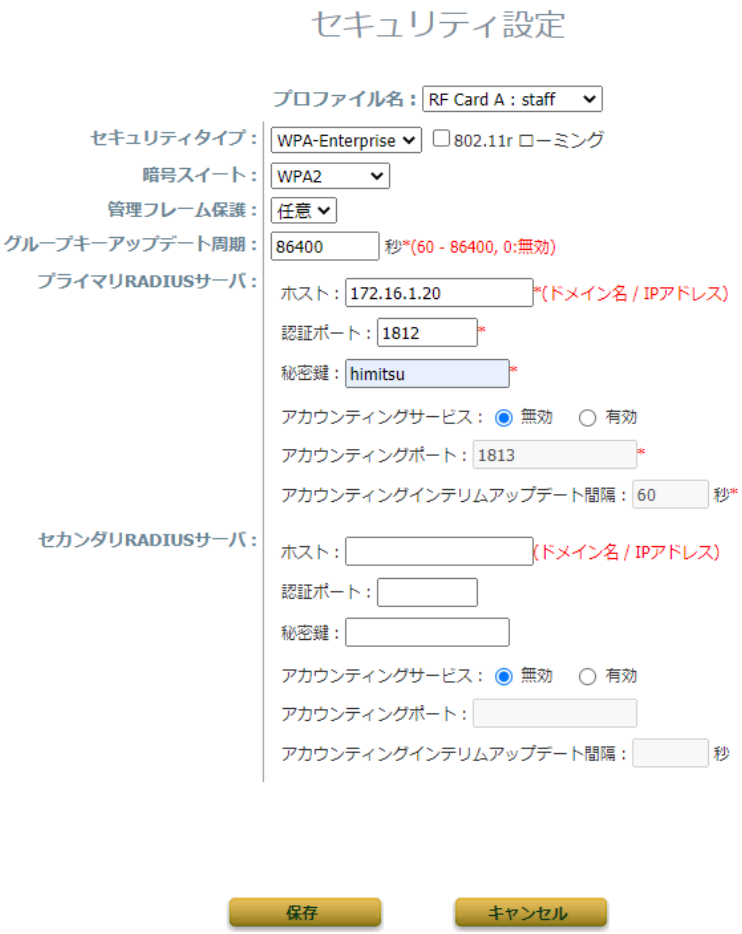
6. ホスト：RADIUSサーバのIPアドレスまたはホスト名を入力します
7. 認証ポート：必要に応じて変更します。
8. 秘密鍵：RADIUSサーバの秘密鍵を設定します。
9. 保存ボタンをクリックします。

◆ 同様に RF Card B：staff の設定も行います。

セキュリティ設定 – SSID:staff

RF Card B：staff（VAP-1）に SSID：staff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：ドロップダウンリストからRF Card B: staff を選択します。
3. セキュリティタイプ：ドロップダウンリストからWPA-Enterpriseを選択します。
4. 暗号スイート：ドロップダウンリストからWPA2を選択します。
5. 管理フレーム保護：環境に応じて設定してください。

RADIUSサーバを設定します。

6. 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
7. 認証ポート：必要に応じて変更します。
8. 秘密鍵：RADIUSサーバの秘密鍵を設定します。
9. 保存ボタンをクリックします。

VAP設定 – VAP-2 SSID : guest

RF Card A: VAP-2にSSID guest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-2　を選択します。
3. VAP：有効 を選択します。
4. プロファイル名 ：管理しやすい名称に変更します。
5. ESSID：SSID guestを設定します。
6. ネットワークモード：ドロップダウンリストから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：有効にし、VLAN ID：20を設定します。
9. 保存ボタンをクリックします。
10. 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。

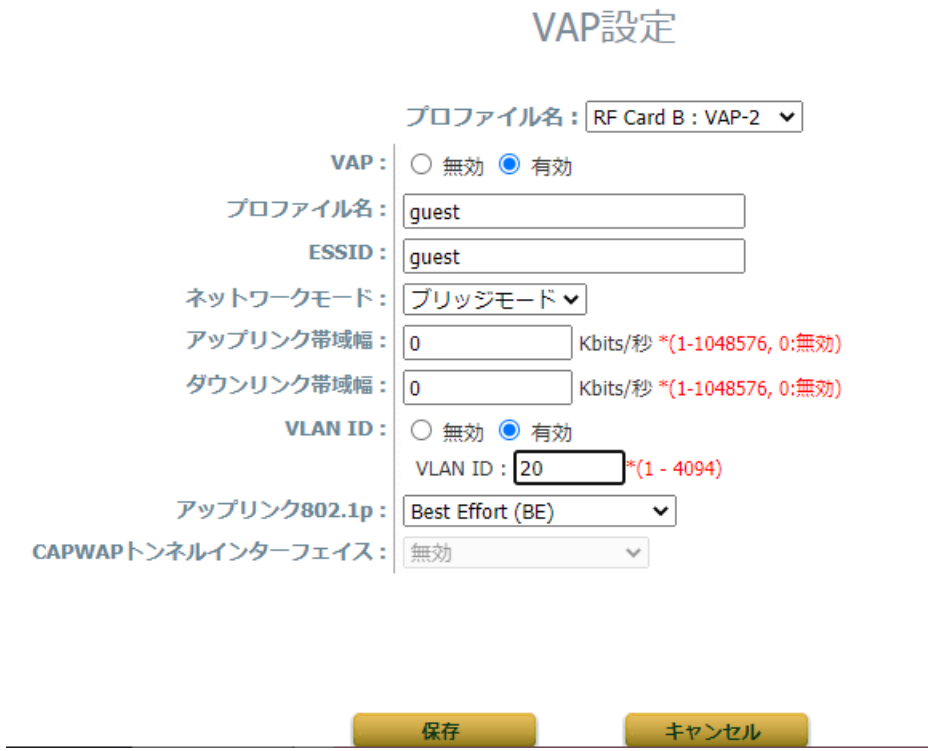
◆ 次に5GHz帯のプロファイル名：RF Card B：VAP-2に同様の設定をします。

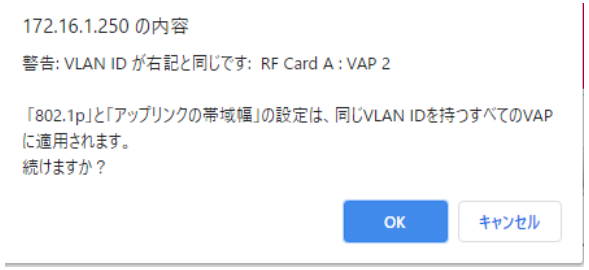
VAP設定 – VAP-2 SSID : guest

RF Card B: VAP-2にSSID guest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-2　を選択します。
3. VAP：有効 を選択します。
4. プロファイル名 ：管理しやすい名称に変更します。
5. ESSID：SSID guestを設定します。
6. ネットワークモード：ドロップダウンリストから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：有効にし、VLAN ID：20を設定します。確認のダイアログが表示され、OKをクリックします。
9. 保存ボタンをクリックします。
10. 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。





セキュリティ設定 – SSID:guest

RF Card A: guest(VAP-2)に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：ドロップダウンリストからWPA-Personalを選択します。
3. 暗号スイート：ドロップダウンリストからWPA2を選択します。
4. 管理フレーム保護：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：パスフレーズを選択します。
6. プリシェアードキー：事前共有鍵(PSK)を設定します。
7. 保存ボタンをクリックします。

◆ 同様に RF Card B：guest (VAP-2) に設定します。

セキュリティ設定 – SSID:guest

RF Card B: guest(VAP-2)に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：ドロップダウンリストからWPA-Personalを選択します。
3. 暗号スイート：ドロップダウンリストからWPA2を選択します。
4. 管理フレーム保護：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：パスフレーズを選択します。
6. プリシェアードキー：事前共有鍵(PSK)を設定します。
7. 保存ボタンをクリックします。

VAP一覧

APのVAPの一覧が表示され、各VAPの設定状態を確認できます。

- Wireless→VAP一覧のタブを選択します。

- 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
4	Virtual Access Point 3	ブリッジモード	無効	Open	無効	無効
5	Virtual Access Point 4	ブリッジモード	無効	Open	無効	無効
6	Virtual Access Point 5	ブリッジモード	無効	Open	無効	無効
7	Virtual Access Point 6	ブリッジモード	無効	Open	無効	無効
8	Virtual Access Point 7	ブリッジモード	無効	Open	無効	無効
9	Virtual Access Point 8	ブリッジモード	無効	Open	無効	無効
10	Virtual Access Point 9	ブリッジモード	無効	Open	無効	無効
11	Virtual Access Point 10	ブリッジモード	無効	Open	無効	無効
12	Virtual Access Point 11	ブリッジモード	無効	Open	無効	無効
13	Virtual Access Point 12	ブリッジモード	無効	Open	無効	無効
14	Virtual Access Point 13	ブリッジモード	無効	Open	無効	無効
15	Virtual Access Point 14	ブリッジモード	無効	Open	無効	無効
16	Virtual Access Point 15	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
4	Virtual Access Point 3	ブリッジモード	無効	Open	無効	無効
5	Virtual Access Point 4	ブリッジモード	無効	Open	無効	無効
6	Virtual Access Point 5	ブリッジモード	無効	Open	無効	無効
7	Virtual Access Point 6	ブリッジモード	無効	Open	無効	無効
8	Virtual Access Point 7	ブリッジモード	無効	Open	無効	無効
9	Virtual Access Point 8	ブリッジモード	無効	Open	無効	無効
10	Virtual Access Point 9	ブリッジモード	無効	Open	無効	無効
11	Virtual Access Point 10	ブリッジモード	無効	Open	無効	無効
12	Virtual Access Point 11	ブリッジモード	無効	Open	無効	無効
13	Virtual Access Point 12	ブリッジモード	無効	Open	無効	無効
14	Virtual Access Point 13	ブリッジモード	無効	Open	無効	無効
15	Virtual Access Point 14	ブリッジモード	無効	Open	無効	無効
16	Virtual Access Point 15	ブリッジモード	無効	Open	無効	無効

無線LAN基本設定 RF Card A

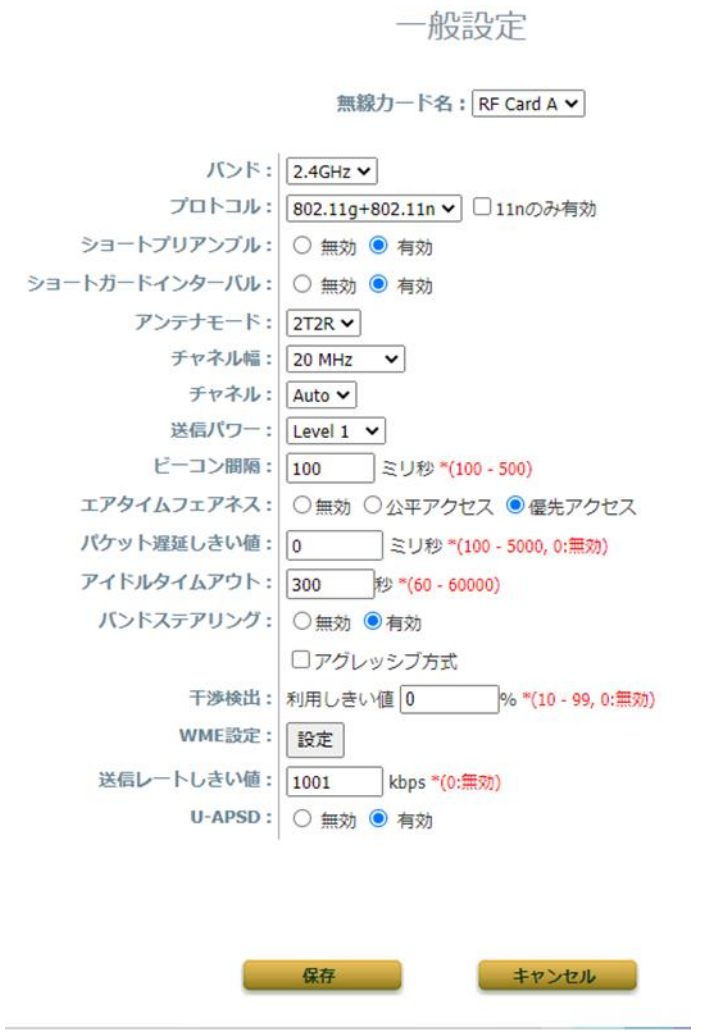
APの2.4GHz帯の無線設定を行います。

1. Wireless→基本設定のタブを選択します。

2. 各パラメータを設定します。

- 無線カード名：ドロップダウンリストから RF Card Aを選択します。
- バンド：使用しない場合、無効にできます。
- チャネル：チャンネルをドロップダウンリストから選択します。
- 送信パワー：送信される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。
- バンドステアリング：5GHz帯に接続できるクライアントを5GHz帯に誘導します。

3. 保存ボタンをクリックします。



無線LAN基本設定 RF Card B

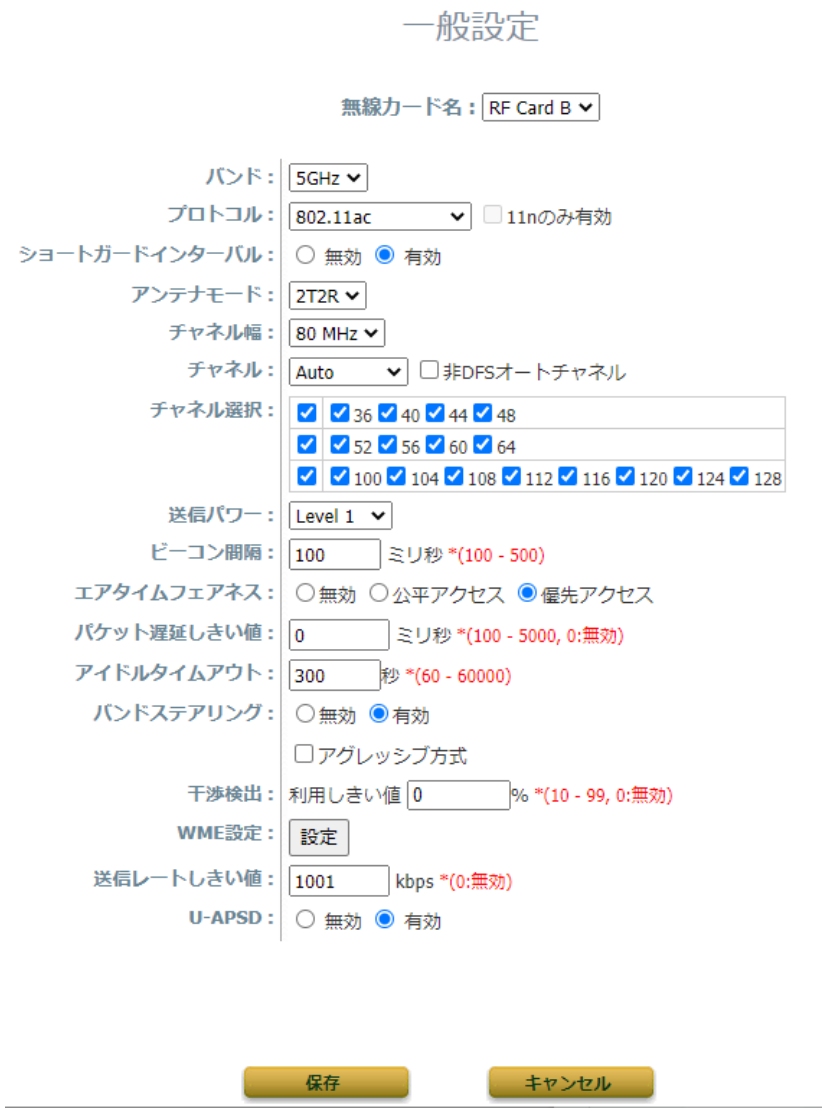
APの5GHz帯の無線設定を行います。

1. Wireless→基本設定のタブを選択します。

2. 各パラメータを設定します。

- 無線カード名：ドロップダウンリストからRF Card Bを選択します。
- バンド：使用しない場合、無効にできます。
- チャネル：チャネルをドロップダウンリストから選択します。
- チャネル選択：チャネルでAutoを選択した場合、APはチェックの入ったチャネルからチャネルを選択します。
- 送信パワー：送信される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。
- バンドステアリング：5GHz帯に接続できるクライアントを5GHz帯に誘導します。

3. 保存ボタンをクリックします。



無線LAN詳細設定

VAP毎にパラメーターが設定されます。

1. Wireless→詳細設定のタブを選択します。

2. プロファイル名：設定するVAPをドロップダウンリストから選択します。

3. 各パラメータの設定をします。

- SSIDブロードキャスト：SSIDを隠匿する場合、無効にしてください。
- 無線端末アイソレーション：有効にするとすべてのクライアントが分離され、クライアント間の通信を遮断します。
- 受信RSSIしきい値：クライアントのRSSIが閾値以下になると、APから切断されます。

4. 保存ボタンをクリックします。

アクセスコントロール設定

VAP毎にAPにアクセスできるクライアントの総数を制限することができ、MACアドレスによるアクセスコントロールが設定できます。

1. Wireless→アクセスコントロールのタブを選択します。

2. 設定項目

- プロファイル名：設定するVAPをドロップダウンボックスから選択します。
- 最大クライアント数：VAPに接続できる最大クライアント数を設定します。
- アクセスコントロール方式：ドロップダウンリストから選択します。
  - 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 (許可リスト)

アクセスコントロール方式でMACアドレス(許可リスト)を選択した場合、許可リストに登録されたMACアドレスのクライアントのみアクセスできます。

1. プロファイル名：ドロップダウンリストから設定するVAPを選択します。
2. アクセスコントロール方式：MACアドレス(許可リスト)を選択します。
3. 許可するMACアドレスリストが表示され、MACアドレスの欄にMACアドレスを登録します。
4. 状態の欄を有効をクリックします。
5. 登録が完了したら、保存ボタンをクリックします。
6. 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。
7. 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。

✓ 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拒否されます。

アクセスコントロール設定 (拒否リスト)

アクセスコントロール方式でMACアドレス(拒否リスト)を選択した場合、リストに登録されたMACアドレスのクライアントのアクセスを拒否できます。

1. プロファイル名：ドロップダウンリストから設定するVAPを選択します。
2. アクセスコントロール方式：MACアドレス(拒否リスト)を選択します。
3. 拒否するMACアドレスリストが表示され、MACアドレスの欄にMACアドレスを登録します。
4. 状態の欄を有効をクリックします。
5. 登録が完了したら、保存ボタンをクリックします。
6. 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。
7. 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。

✓ 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 (RADIUS ACL)

アクセスコントロール方式でRADIUS ACLを選択した場合、外部RADIUSでMACアドレス認証されます。

1. プロファイル名：ドロップダウンリストから設定するVAPを選択します。
2. アクセスコントロール方式：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。
5. 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。
6. 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。

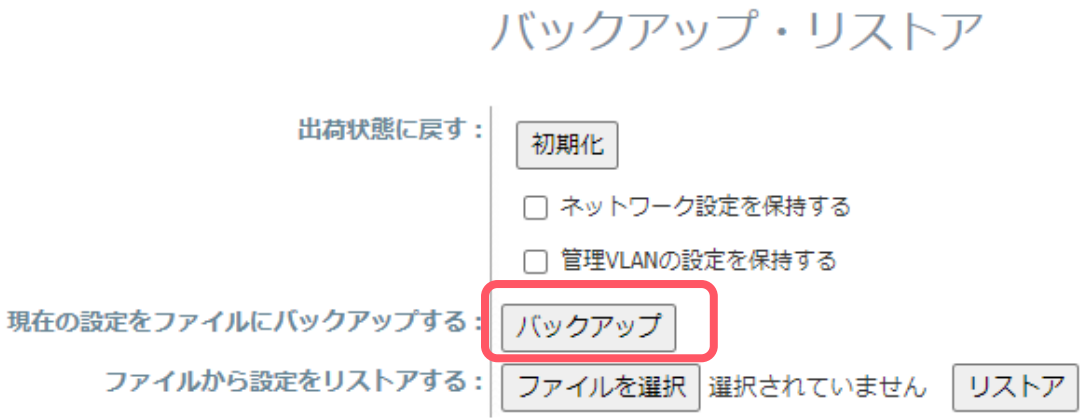
✓ RADIUSサーバの設定は、セキュリティーのRADIUSサーバの設定と共有されます。

設定のバックアップ

- AP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。

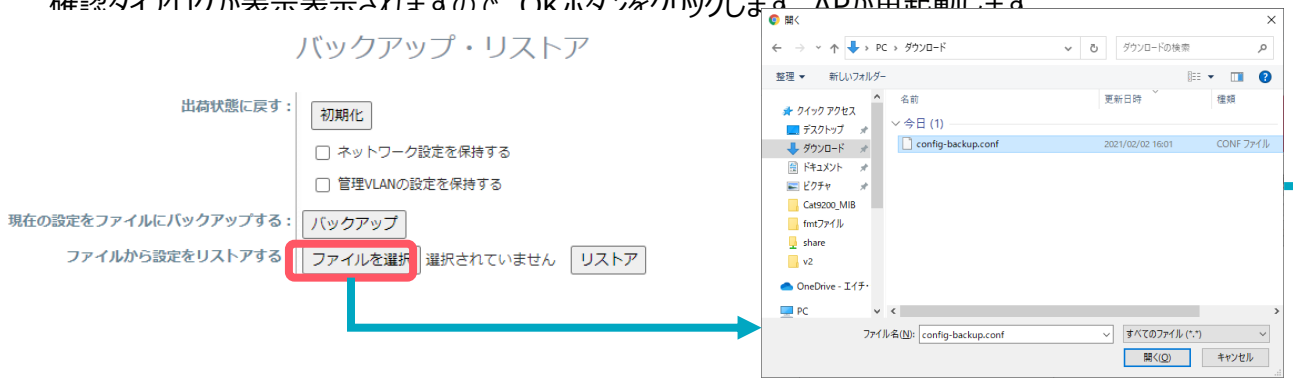


設定のリストア

◆ バックアップファイルからAP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。APが再起動します。



APの初期化 - WMI

APを工場出荷時の状態に初期化する方法について説明します。初期化する方法は、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。

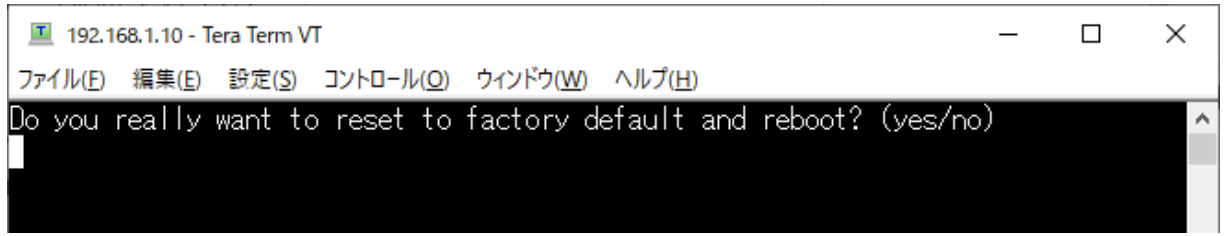
- WMIによる初期化

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. APが再起動し、工場出荷時の状態に初期化されます。

APの初期化 – SSH, Resetボタン

- SSHによる初期化
  1. Tera Term等のターミナルソフトでSSHでAPに接続します。
  2. ユーザ名：reset2def, パスワード：reset2defでAP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APは再起動し、初期化されます。



- AP本体のResetボタンによる初期化

  AP本体のResetボタンを5秒以上押し続け、Resetボタンを離すとAPは再起動し初期化されます。

APRESIA®