TD61-8133

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



©APRESIA Systems, Ltd. All Rights Reserved.





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。





- 🗆 🗙

* 0



◆ 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。



@ ECW5211-L

× +

← → C ▲ 保護されていない通信 | 192.168.1.10/status/overview.asp

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<u>英数字のみ</u>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。

Wireless Firewall Uninties System Status 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 スワード変更 ホーム > ユーティリティー > 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



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。

ネットワーク設定 \ ポート \ DHCPサーバ \ 管理機能 \ CAPWAP \ IPv6 \ iBeacon \ RTLS \ DPI DNS

◇ 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。

Utilities

Status

- ◇ 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。

Firewall

3. 保存ボタンをクリックします。

System

ホーム > システム > システム情報

√ステム情報 \

保存 キャンセル

Wireless

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。

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.

アクセスポイント名: ECW5211-L * 説明: 設置場所: 8F



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。

時刻設定

現たの時期, 2000/01/01 01:10:40

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。

切口の可刻・	2000/01/01 01.10.49		
タイムゾーン:	(GMT+09:00)Osak	ka,Sapporo,Tokyo	~
時刻設定:	 NTPを使用する 	○手動設定	
NTP サーバ 1 :	172.16.1.30	*	
NTP サーバ 2:	ntp.nict.jp		



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.	システム情報 ネットワーク設定 ボート DHCPサーバ 管理職能 CAPWAP IPv6 iBeacon RTLS DPI DNS ホーム > ジステム > ネットワークセッティング ビークジェーング ビークジェークジェーング ビークジェーング ビークジェーング ビークジェーング ビークジェーング ビークジェーング ビークジェークジェーング ビークジェークジェークジェーング ビークジェークジェークジェークジェークジェークジェークジェークジェークジェークジェ	マットワークセッティング ● スタティック ○ DHCP IPアドレス更新
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。	ネットマスク: 255.255.255.0 *
	◇ 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。	デフォルトゲートウェイ: 172.16.1.254 *
	◇ 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。	プライマリDNSサーバ: 172.16.1.254 *
		代替DNSサーバ:
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。	● 無効 ○ 有効
4		● 無効 ○ 有効
4.	保存ホタンをクリックしま9。 レイヤー2 STP:	無効 ~
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。	保存 キャンセル
		117200



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。

- システム情報
 ポットワーク設定
 ポート
 DHCPサーノ
 管理機能
 IPv6
 iBeacon
 RTLS
 DPI DNS

 ホーム > >ステム > 営理機能
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
- 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。

SIMPERAL :	○ 無効 ◎ 有効
	コミュニティー名:
	Read : public
	Write : private
	SNMPv3 ユーザリストの編集
	トラップの送信: 🔿 無効 💿 有効
	SNMPサーバのIPアドレス: 192.168.1.30



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。



- 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。

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

保存

キャンセル

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	2	
3		4	
5		6	
7		8	
9		10	





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)	周波数带	無線LAN規格
RF Card A	2.4GHz帯	802.11b/g/n
RF Card B	5GHz带	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
000088000°	VAP-2	guest	WPA2パーソナル	ブリッジ	20
N.					



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。





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?



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
------	------

	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 V
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 *
	アカウンティングサービス: 💿 無効 🛛 有効
	アカウンティングポート: 1813 *
	アカウンティング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:
	アカウンティングサービス: 💿 無効 🛛 有効
	アカウンティングポート:
	アカウンティングインテリムアップデート間隔: 秒



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。

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 □-ミング
暗号スイート:	WPA2 V
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 *
	アカウンティングサービス: 💿 無効 🛛 有効
	アカウンティングポート: 1813 *
	アカウンティング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:
	アカウンティングサービス: 💿 無効 🛛 有効
	アカウンティングポート:
	アカウンティングインテリムアップデート間隔: 秒



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。

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:	guest
ESSID :	guest
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 : 20 *(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 ~
ダウンリンク帯域幅: VLAN ID: アップリンク802.1p: CAPWAPトンネルインターフェイス:	0 Kbits/秒 *(1-1048576, 0:無効) ○ 無効 ● 有効 VLAN ID : 20 *(1 - 4094) Best Effort (BE) ▼ 無効 ▼







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

	プロファイル名:RF Card A : guest \vee
セキュリティタイプ:	WPA-Personal □ 802.11r □-ミング
暗号スイート:	WPA2 V
管理フレーム保護:	任意
プリシェアードキー タイ プ:	〇 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)





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。





セキュリティ設定





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。

1	л≘лф	
力	又可以上	



保存 キャンセル

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。

System	Wireless	Firewall	Utilities	Status
VAP一覧 基本設定 VAP設定	(セキュリティ) リピーター 設定)	洋細設定 アク・スコントロール	Hotspot 2.0	
ホーム > <u>無線</u>LAN設定 > 無線	LAN詳細設定			

- 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。

System WirdCross Firewall Utilities Status VAP-覧 基本設定 VAP競定 セキュリティ リピーター設定 詳細語で、アクセスコントロール Hotsi et 2.0 ホーム > 無線LAN設定 > アクセスコントロール設定

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





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

プロファイル名: RF Card A: VAP-1 V

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	○ 無効 ● 有効
2		● 無効 ○ 有効
3		● 無効 ○ 有効
4		● 無効 ○ 有効
5		● 無効 ○ 有効
6		● 無効 ○ 有効
7		● 無効 ○ 有効
8		● 無効 ○ 有効
9		● 無効 ○ 有効
10		● 無効 ○ 有効

最初へ 前へ 次へ 最後へ (合計:100)



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

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	○ 無効 ● 有効
2		● 無効 ○ 有効
3		● 無効 ○ 有効
4		● 無効 ○ 有効
5		● 無効 ○ 有効
6		● 無効 ○ 有効
7		● 無効 ○ 有効
8		● 無効 ○ 有効
9		● 無効 ○ 有効
10		● 無効 ○ 有効

最初へ 前へ 次へ 最後へ (合計:100)



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。

保存

ホーム > 無線LAN設定 > アクセスコントロール設定

	プロファイル名: RF Card A : staff 🛛 🗸
最大クライアント数:	128 *(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: 172.16.1.20 「(トメイン名またはIPアトレス) 認証ボート番号: 1812 *(1 - 65535)
	秘密鍵:himitsu *
セカンダリRADIUSサーバ:	ホスト:
	認証ポート番号:
	秘密鍵:

キャンセル

アクセスコントロール設定



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。
- 確認ダイアログが表示表示されますので へんボタンをクリックします ムロが再起動します 4 バックアップ・リストア ← → ~ ↑ ↓ > PC > ダウンロード ✓ ひ ダウンロードの検索 バックアップ・リストア 整理 ▼ 新しいフォルダー)= • 🔟 🕐 名前 更新日時 種類 出荷状態に戻す: 📌 クイック アクセス 初期化 ~今日 (1) 🔜 デスクトップ 🛛 🖈 出荷状態に戻す: config-backup.conf CONF ファイル 初期化 2021/02/02 16:01 □ ネットワーク設定を保持する 👆 ダウンロード 🛛 🖈 F#1X7 管理VLANの設定を保持する 📰 ピクチャ □ ネットワーク設定を保持する Cat9200_MIB 現在の設定をファイルにバックアップする: バックアップ fmtファイル 管理VLANの設定を保持する 📮 share ファイルから設定をリストアする ファイルを選択 選択されていません リストア v2 現在の設定をファイルにバックアップする: バックアップ 📥 OneDrive - エイチ・ PC ファイルから設定をリストアする: ファイルを選択 config-backup.conf リストア ファイル名(N): config-backup.conf マ すべてのファイル (*.*) 開<(Q) キャンセル 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? キャンセル



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。





TD61-8133

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®