Edge-corE®

Wi-Fi 6 アクセスポイント

ソフトウェアリリース 12.5.3

ユーザーマニュアル

www.edge-core.com

ユーザーマニュアル

Wi-Fi 6 アクセスポイント

クラウド管理可能なエンタープライズ向けアクセスポイント
EAP101
EAP102
EAP104
EAP104 (WL)
EAP111
EAP112
OAP101

E062024-CS-R09

本ガイドの使い方

本ガイドには、Edgecore 社のアクセスポイント（AP）ソフトウェアについて、AP の操作方法や管理機能の利用方法などの詳細情報が記載されています。AP を効果的に導入し、トラブルなく運用するためには、まず本ガイドの 関連セクションを読み、すべてのソフトウェア機能に精通しておく必要があります。

対象読者

本ガイドは、ネットワーク機器の運用・保守を担当するネットワーク管理者にお読みいただくことを想定しています。LAN（ローカルエリアネットワーク）と IP（インターネットプロトコル）に関する基本的な知識を前提としています。

本ガイドの構成

本ガイドの構成は、AP のウェブ管理インターフェースに基づいています。また、初期設定に関する情報も記載されています。

本ガイドは、以下のセクションを設けています。

- セクション I 「操作を開始する」— AP の導入方法と初期設定について記載されています。
- セクション II 「ウェブ設定」— ウェブインターフェースで利用可能なすべての管理オプションについて記載されています。
- セクション III 「付録」— AP の管理・接続に関するトラブルシュー ティング。

関連文書

本ガイドは、AP ソフトウェアの設定を中心に説明しており、ハードウェアの設置方法については説明していません。AP の設置方法についての具体的な情報は、以下のガイドを参照してください。

クイックスタートガイド

すべての安全情報および規制に関する記述については、以下の文書を参照してください。

クイックスタートガイド

注意喚起

このガイドでは、注意喚起のために次のような表記を使用します。

注意：重要な情報を強調する、または関連する機能や説明を知らせるものです。

警告：データの損失、システムや機器の損傷を引き起こす可能性があります。

改訂履歴

このセクションでは、本ガイドの各改訂版における変更点をまとめています。

2024 年 6 月改訂版

これは本ガイドの 15 回目の改訂版です。ソフトウェアリリース v12.5.3 に対して有効であり、以下の変更が含まれています：

- EAP112 のサポートを追加
- EAP112 の HaLow および LTE 機能を追加
- 40 ページの「インターネット設定」に 3G/LTE を追加
- 99 ページの「BLE」に MQTT を追加

2024 年 3 月改訂版

これは本ガイドの 14 回目の改訂版です。ソフトウェアリリース v12.5.3 に対して有効であり、以下の変更が含まれています：

- 各 SSID の最小許容信号設定「69 ページの「無線ネットワーク — 一般設定」をご参照ください
- デバイス OS ブラックリストの追加「69 ページの「無線ネットワーク — 一般設定」をご参照ください

2024 年 1 月改訂版

これは本ガイドの 13 回目の改訂版です。ソフトウェアリリース v12.5.0 に対して有効であり、以下の変更が含まれています：

- EAP111 のサポートを追加
- RADIUS NAS ID を追加（71 ページの「無線ネットワーク — セキュリティ設定」をご参照ください。）
- 追加したデフォルトの最小許容信号の変更については、65 ページの「電波設定」をご参照ください。

- OpenRoaming キャプティブポータルを追加（56 ページの「OpenRoaming」をご参照ください。）
- OpenRoaming NAI Realm List Method/Authentication を追加（56 ページの「OpenRoaming」をご参照ください）
- Syslog Level を追加（84 ページの「システム設定」をご参照ください。）

2023 年 9 月改訂版
本ガイドは 12 回目の改訂版です。ソフトウェアリリース v12.4.3 に対して有効であり、以下の変更が含まれています：

- OAP101 のサポートを追加
- SSID 分離の追加（65 ページの「電波設定」を参照）
- マルチプル PSK 機能の強化（76 ページの「無線ネットワーク — ネットワーク設定」を参照）

2023 年 7 月改訂版
これは本ガイドの 11 回目の改訂版です。ソフトウェアリリース v12.4.1 に対して有効であり、以下の変更が含まれています：

- OpenRoaming を追加。56 ページの「OpenRoaming」および 78 ページの「無線ネットワーク — OpenRoaming」を参照。
- 変更されたブロードキャスト・レート（65 ページの「電波設定」を参照）
- アクセス制御リストの強化 (71 ページの「無線ネットワーク — セキュリティ設定」を参照)
- ホスト名の拡張 (84 ページの「システム設定」を参照)
- 言語設定をシステムページ (84 ページの「システム設定」を参照)
- ファームウェアのアップグレード機能 (89 ページの「ファームウェアアップグレード」を参照)
- アカウントのユーザー名強化 (91 ページの「ユーザーアカウント」を参照)

2023 年 5 月改訂
本書は、本ガイドの第 10 回目の改訂版です。ソフトウェアリリース v12.4.0 に有効で、以下の変更点が含まれています：

- QRコードオンボーディングにWANポートの自動検出機能を追加しました (23 ページの「QR コードからデバイスを登録する」を参照)。

- メッシュ AP の自動設定機能を追加しました（26 ページの「メッシュ AP 構成」を参照）。
- ファイアウォールルールから Mark と No track を削除しました（49 ページの「ファイアウォールのルール」を参照）。
- 最小許容信号の変更（65 ページの「電波設定」を参照）。
- RF アイソレーションの追加（65 ページの「電波設定」を参照）。
- Dynamic VLAN の変更、76 ページの「無線ネットワーク — ネットワーク設定」を参照。
- HotSpot 2.0 設定の変更、76 ページの「無線ネットワーク — ネットワーク設定」を参照。
- ログレベルの追加、84 ページの「システム設定」を参照。
- SNMPv3 User を追加、96 ページの「SNMP」を参照。
- Diagnostics を変更し、Speed Test を追加、101 ページの「診断」を参照。

2023 年 3 月改訂
第 3 版。本版はソフトウェア v12.3.0 に対応しており、以下の変更点が含まれています。

- 追加済み
  17 ページの「Zero-Touch Provisioning」
  37 ページの「トラフィックグラフ」
  38 ページの「サービス」
  43 ページの「IPv6 設定」
  49 ページの「ファイアウォールのルール」
  50 ページの「ポートフォワーディング」
  51 ページの「ホットスポット設定」
  59 ページの「DHCP スヌーピング」
  60 ページの「ARP インスペクション」
  61 ページの「DHCP リレー」
  90 ページの「証明書をアップロードする」
  92 ページの「Telnet」
  93 ページの「Edgecore Networks ディスカバリーツール」
  93 ページの「ウェブサーバー」
  97 ページの「マルチキャスト DNS」
  102 ページの「デバイス・ディスカバリー」
- アップデート済み
  18 ページの「ウェブインターフェースへの接続」
  19 ページの「AP セットアップウィザード」

23 ページの「QR コードからデバイスを登録する」
31 ページの「一般ステータス」
33 ページの「ネットワークステータス」
35 ページの「無線ステータス」
44 ページの「イーサネット設定」
47 ページの「LAN 設定」
65 ページの「電波設定」
69 ページの「無線ネットワーク — 一般設定」
71 ページの「無線ネットワーク — セキュリティ設定」
76 ページの「無線ネットワーク — ネットワーク設定」
79 ページの「無線ネットワーク — Open Mesh Settings」
80 ページの「無線ネットワーク — 無線詳細設定」
84 ページの「システム設定」
96 ページの「SNMP」
99 ページの「BLE」

2021 年 7 月改訂
第 2 版。本版はソフトウェア v11.2.0 に対応しており、以下の変更点が含まれています。

- WPA3 パーソナルトランジション、WPA3 エンタープライズ、および WPA3 エンタープライズトランジションを追加しました。71 ページの「無線ネットワーク — セキュリティ設定」を参照。
- IEEE 802.11 k/r のサポート。71 ページの「無線ネットワーク — セキュリティ設定」を参照。
- Minimum signal allowed（RSSI Threshold）の追加。65 ページの「電波設定」参照。
- オープンメッシュのサポート。79 ページの「無線ネットワーク — Open Mesh Settings」を参照 。
- SNMP v2 のサポート。96 ページの「SNMP」を参照。
- リモートシスログのサポート。94 ページの「Remote System Log Setup」を参照。
- LLDP のサポート。98 ページの「LLDP」を参照。
- EWS シリーズコントローラーによる管理のサポート、84 ページの「システム設定」を参照。

2021 年 4 月改訂版
これは、このガイドの最初の改訂版です。ソフトウェアリリース v11.1.1 に対応しています。

目次

図の一覧

表

セクション I

操作を開始する

このセクションでは、AP の概要を説明し、無線ネットワークの基本的な概念を紹介します。また、管理インターフェースにアクセスするために必要な基本設定についても説明します。

このセクションには、以下の章が含まれています。

1 はじめに

アクセスポイント（AP）には、ネットワーク管理エージェントを含むソフトウェアが搭載されています。このエージェントには、ウェブベースのインターフェースを含むさまざまな管理オプションが用意されています。また、セキュアシェル（SSH）を使って AP に接続し、コマンドラインインターフェース（CLI）を使って設定を行うこともできます。

注意：本マニュアルでは、スタンドアロンモードの設定インターフェースについて説明しています。クラウドインターフェースによる AP の設定について は、Edgecore ecCLOUD コントローラーユーザーマニュアルを参照してくだ さい。

本章には、以下の内容が含まれています。

設定項目

AP のウェブエージェント上では、標準的なウェブブラウザを使用し、AP のパラメータの設定、無線接続の監視、統計情報の表示を行うことができます。このウェブ管理インターフェースは、ネットワークに接続されたどのコンピュータからでもアクセスできます。

CLI プログラムは、ネットワーク上のセキュアシェル（SSH）接続によってリモートでアクセスできます。CLI は主に技術的なサポートに使用されます。

AP のウェブインターフェースでは、以下のような管理機能を実行できます。

- 管理者のユーザー名とパスワードの設定
- IP の設定
- 2.4GHz, 5GHz 無線の設定
- HaLow 無線の設定（EAP112 のみ）
- 無線セキュリティ設定によるアクセス制御
- アクセスコントロールリスト（ACL）によるパケットのフィルタリング
- システムファームウェアのダウンロード
- 設定ファイルのダウンロード及びアップロード
- システム情報の表示

Zero-Touch Provisioning

AP は Edgecore ecCLOUD コントローラーか EWS-Series コントローラーで自動管理することができます。AP が ecCLOUD コントローラに登録済みの場合、AP の WAN ポートがインターネットに接続されると、自動的に管理されます。

AP が EWS-Series コントローラとローカル LAN に接続されている場合、AP は DHCP Option 138 によりコントローラ IP アドレスを設定し、コントローラにより自動的に管理されます。

ゼロタッチプロビジョニングの代わりに、ウェブインターフェイスから優先管理方法を手動で設定できます（「システム設定」（79 ページ）を参照 .

ウェブインターフェースへの接続

AP のウェブ管理インターフェースに初めてアクセスする場合は、PC を AP の LAN ポートに直接接続するか、クイックセットアップ用 QR コード（AP のポートの横にあるラベルに印刷されています）を使用します。初めてウェブインターフェースにアクセスしたときには、AP の初期設定のためにセットアップウィザードが自動的に実行されます。

セットアップウィザードの詳細については、19 ページの「AP セットアップウィザード」を参照してください。

QR コードの使用については、23 ページの「QR コードからデバイスを登録する」を参照してください。

LAN ポート接続

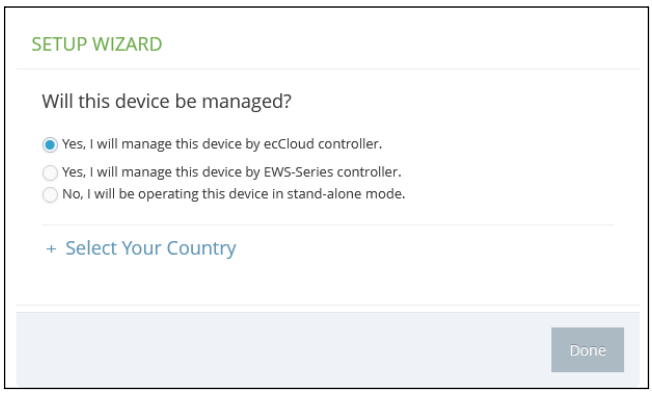
AP の LAN ポートを介してウェブ管理インターフェースに接続する場合、AP の初期値の管理 IP アドレスは 192.168.2.1 で、サブネットマスクは 255.255.255.0 となっています。そのため、PC の IP アドレスを AP と同じサブネット上に設定する必要があります（すなわち、PC と AP のアドレスは両方とも 192.168.2.x で始まる必要があります）。

注意：Uplink（PoE）ポートを使用してウェブインターフェースに接続する場合、初期設定では、IP アドレスは DHCP によって自動的に割り当てられま す。DHCP サーバーに到達できない場合、Uplink（PoE）ポートは 192.168.1.10 という予備の IP アドレスに戻ります。

AP の Web 管理インターフェースにアクセスするには、Web ブラウザーを使用して、次の場所に接続します。管理インターフェイスにデフォルトの IP アドレス 192.168.2.1 を入力してください。

初回アクセスの場合、ユーザーログインはなく、セットアップウィザードが自動的に起動します。19 ページの「AP セットアップウィザード」に記載されている手順に従ってください。

図 1: ウェブ管理インターフェースへのログイン



注意：お使いのネットワークに適合する別の管理用 IP アドレスで AP を設定するには、47 ページの「LAN 設定」を参照してください。

AP セットアップウィザード

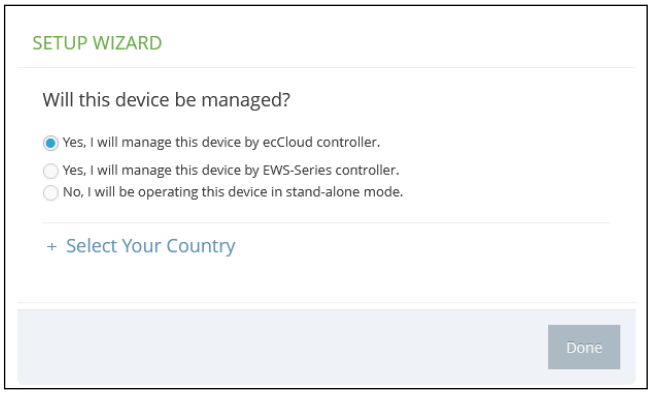
セットアップウィザードでは、AP の起動に必要な基本設定を行います。

ステップ 1 Edgecore の ecCLOUD コントローラを使用して AP を管理する場合は、「Yes, I will manage this device by ecCloud controller」を選択し、ステップ 6 へ進みます。

Edgecore EWS シリーズコントローラを使用して AP を管理するには、「Yes, I will manage this device by EWS-Series controller」を選択し、ステップ 2 に進みます。

そうでない場合は、「No, I will be operating this device in stand-alone mode」を選択し、ステップ 3 に進みます。

図 2: ecCloud、EWS コントローラー、スタンドアローンの選択



Edgecore ecCLOUD コントローラを使用して AP を管理することを選択した場合、cloud.ignitenet.com にアクセスして AP を登録します。ログインし、メニューから「Devices」を選択します。Add Device をクリックし、AP のシリアル番号と MAC アドレスを入力し、AP をクラウドネットワークに登録します。シリアル番号と MAC アドレスは、製品のパッケージやラベルに記載されています。

注意：本マニュアルでは、スタンドアロンモードの設定インターフェイスについて説明しています。クラウドインターフェースによる AP の設定については *Edgecore ecCLOUD Controller ユーザーマニュアル*を、EWS コントローラによる AP の管理については *EWS-Series Controller ユーザーマニュアル*を参照してください。

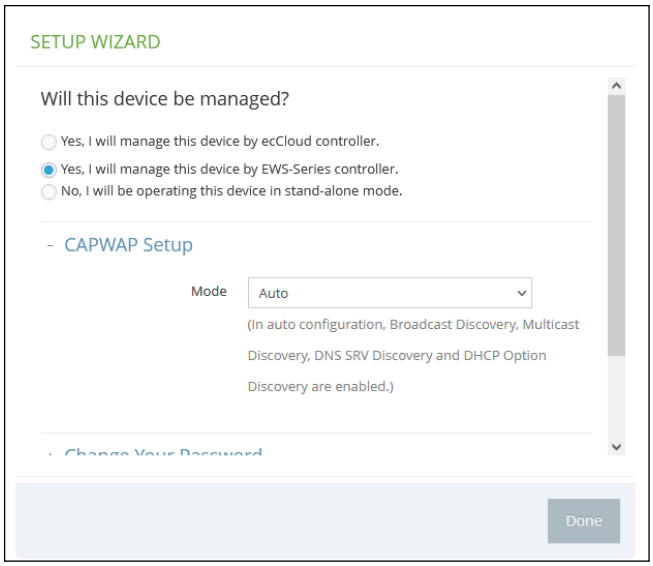
ステップ 2 CAPWAP セットアップ - EWS シリーズコントローラ管理を選択した場合、コントローラを検出するモードを設定できます。AP がネットワーク上のコントローラを検出すると、CAPWAP（Control And Provisioning of Wireless Access Points）参加要求を送信できます。

自動モードでは、AP は 4 つの方法を使用してコントローラを検出します。これらの方法は、これ以上設定する必要はありません。

マニュアルモードでは、2 つのオプションが利用可能です。AP が DNS サーバーレコードを使用して EWS コントローラーを検出できるように、Domain Name Suffix を指定します。または、コントローラーの静的 IP アドレスを指定するだけです。

CAPWAP のセットアップの詳細については、84 ページの「システム設定」を参照してください。

図 3: CAPWAP のセットアップ

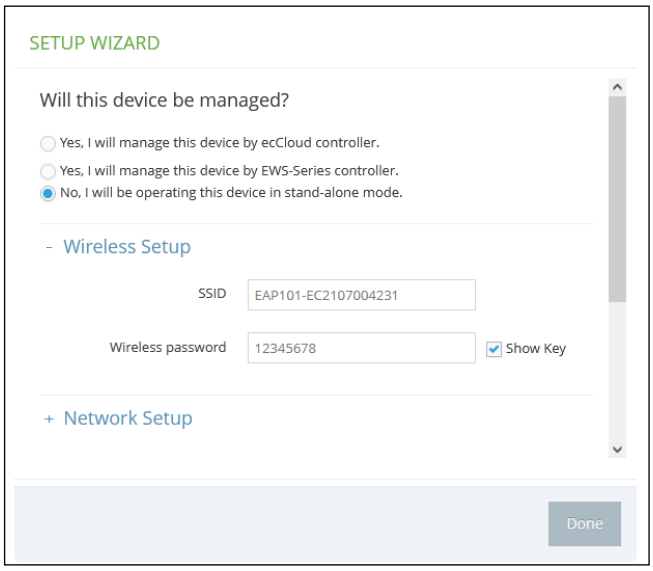


CAPWAP の設定が完了したら、ステップ 5 へ進みます。

ステップ 3 無線設定 - スタンドアロンモードで AP を管理することを選択した場合、デフォルトのワイヤレスネットワークを設定します。

デフォルトのワイヤレスネットワーク名（SSID）は、AP モデルとそのシリアル番号で構成され、デフォルトのワイヤレスパスワードが存在します。ワイヤレスネットワーク名とパスワードは、お好みの設定に変更することができます。ワイヤレス名は 1 ～ 32 の ASCII 文字、パスワードは 8 ～ 63 の ASCII 文字（特殊文字は不可）である必要があります。

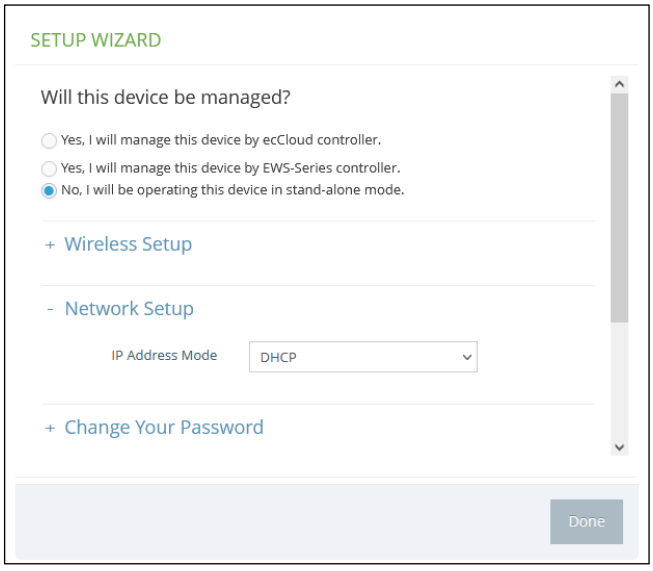
図 4: 無線のセットアップ



ステップ 4 ネットワーク設定 - AP スタンドアローンモードの場合、以下の設定も可能です。インターネットアクセスポートに IP アドレスを提供するために使用される IP アドレスモードです。

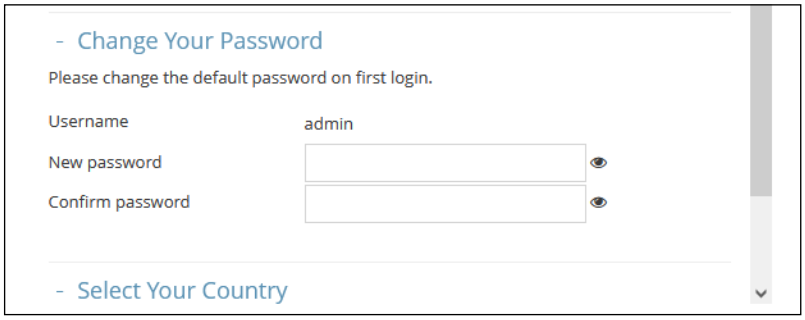
デフォルトの IP アドレスモードは DHCP で、その他のオプションには Static IP と PPPoE があります。詳細については、40 ページの「インターネット設定」を参照してください。

図 5: ネットワーク設定



ステップ 5 パスワードの変更 - AP の管理アクセス用に新しいパスワードを設定します（デフォルトのユーザー名は「admin」、パスワードは「admin」です）。パスワードは、6 ～ 20 文字の ASCII 文字（大文字と小文字を区別し、特殊文字は使用しない）でなければなりません。

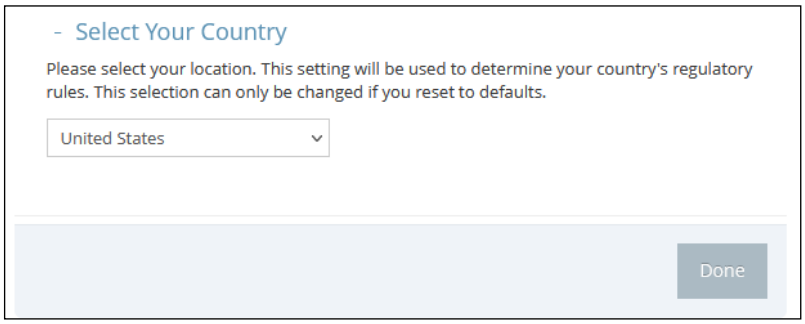
図 6: パスワードの変更



注意：ユーザー名とパスワードの変更については、91 ページの「ユーザーアカウント」を参照してください。

ステップ 6 Select Your Country - ドロップダウンメニューから、アクセスポイントの動作国を選択します。無線が許可された地域の規制に従って動作することを確認するために、AP の国コードを設定する必要があります。つまり、国コードを設定すると、指定された国のワイヤレスネットワークで許可された無線チャネルと送信電力レベルに AP の動作が制限されます。

図 7: 国の選択



警告：国番号は、運用する国に設定する必要があります。国コードを設定することで、無線機がワイヤレスネットワークに指定された地域の規制の中で動作するようになります。

注意：国番号の選択は非米国モデルのみで、米国モデルにはありません。FCC 規制により、米国で販売されるすべての Wi-Fi 製品は、米国の動作チャンネルにのみ固定する必要があります。

ステップ 7　セットアップウィザードが完了したら、" 完了 " をクリックします。

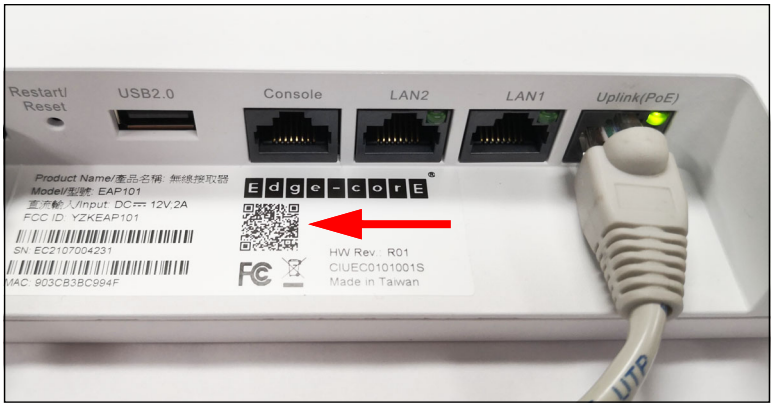
QR コードからデバイスを登録する

AP と ecCLOUD コントローラーを素早く登録するために、AP の QR コードを 携帯電話で読み取ることができます。

以下の手順で行います。

1. AP の電源を入れます。
2. AP をインターネットに接続します。ネットワークまたはインターネットアクセスデバイスを AP の RJ-45 Uplink ポートに接続します。
3. カメラまたはスマホのバーコードアプリで、AP の QR コードを読み取る。QR コードは、AP のポートの横にあるラベルに印刷されています。

図 8: AP の QR コードを読み取る



4. メッセージが表示されたら、「はい」をタップして Wi-Fi ネットワークに参加します。(iPhone の場合 を表示させるには、「設定」→「Wi-Fi」を選択するか、ブラウザを開く必要があります。)

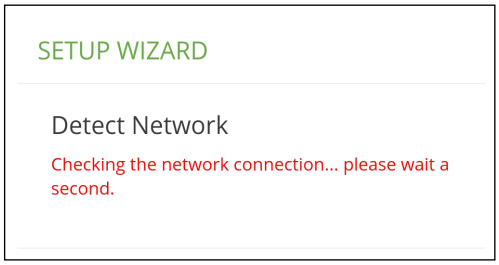
   ウェブブラウザが開き、セットアップウィザードのページに移動します。

注意：本機が Wi-Fi ネットワークに接続できない場合は、SSID（ネットワー ク名）とパスワードを手動で入力してください。SSID には AP のシリアル番号（例：EC0123456789)、パスワードには AP の MAC アドレス（例：903CB3BC1234）を入力します。

5. WAN ポートの設定（DHCP、Static IP、PPPoE）の自動検出を待ちます。

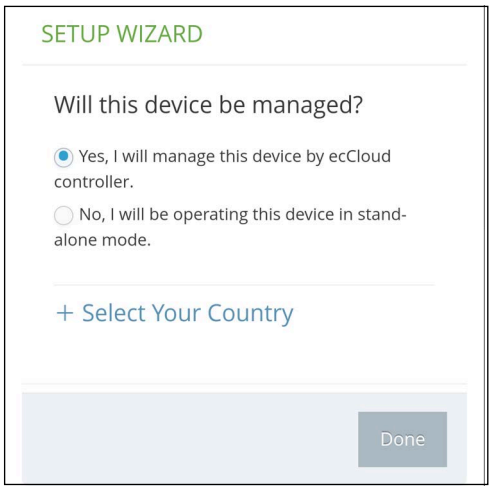
DHCP が検出されると、AP は自動的にセットアップウィザードを続行します。

図 9: Wizard のセットアップ - ネットワークの検出



6. ecCLOUD コントローラーを使用して AP を管理するか、スタンドアローンモードで AP を管理するかを選択します。

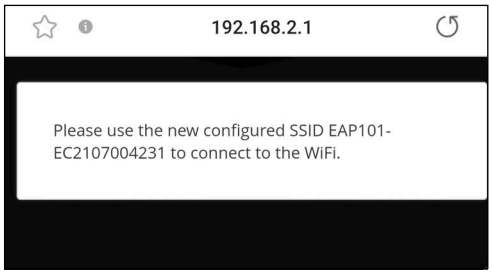
図 10: セットアップウィザード - デバイス管理



a. スタンドアローンモード。デフォルトのワイヤレスネットワーク設定を使用するか、ネットワーク名とパスワードをカスタマイズします。ログインパスワードを変更し、動作国を設定します。完了をタップして、セットアップウィザードを終了します。

AP の設定が更新されるまで約 2 分待ち、セットアップウィザードで設定したワイヤレスネットワーク名に接続します。

図 11: 新しい SSID に接続する

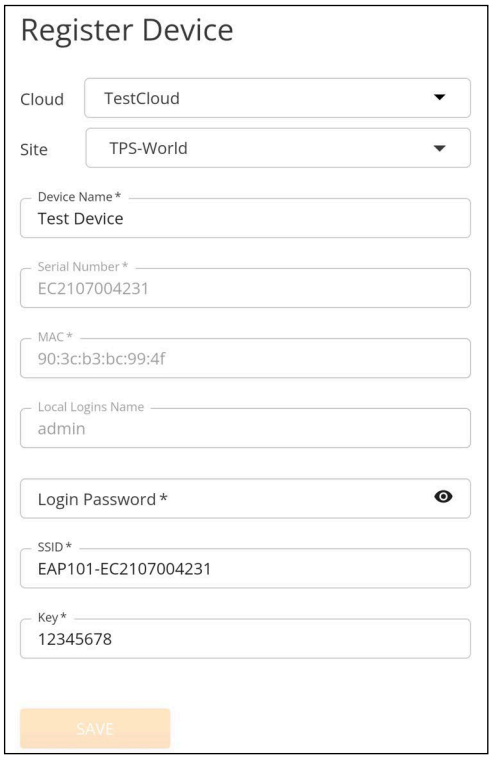


b. クラウドマネージドモードです。国を設定し、「完了」をタップしてセットアップウィザードを終了します。ブラウザは ecCLOUD のログインページにリダイレクトされます。

図 12: ecCLOUD　ログインページ

すでに ecCLOUD のアカウントをお持ちの場合は、ログインして AP のサイトを選択します。AP は自動的にクラウド管理用に登録されます。デバイス名、ログインパスワード、SSID、セキュリティキーを変更します。保存をタップした後、クラウドコントローラーが AP を設定するまで約 5 分待ちます。

図 13: ecCLOUD　デバイス登録



ecCLOUD のアカウントをお持ちでない場合は、「新規登録」をタップしてアカウントを設定してください。お使いの国を登録する前に、クラウドとサイトを作成してください。「次へ」をタップすると、AP が自動的にクラウドに登録されます。

“ 保存 ” をクリックした後、クラウドコントローラーが AP を設定するまで約 5 分待ちます。

注意：ecCLOUD を利用した AP の設定や構成の詳細については、Edgecore ecCLOUD コントローラーユーザーマニュアルを参照してください。

メッシュ AP 構成

最初の AP は、ecCLOUD またはスタンドアローンモードのいずれかで管理することができます。2 台目の AP が 1 台目の AP とのメッシュ接続を確立する必要がある場合は、以下の手順で行います：

1. 1 台目の AP（メッシュポータルポイント）の LAN ポートと 2 台目の AP（メッシュアクセスポイント）の LAN ポートを接続し、2 台目の AP が 1 台目の AP と設定を同期するようにします。
2. LAN ポートのプラグを抜いた後、自動的にメッシュ接続が確立されます。

メインメニュー

ウェブインターフェースのメインメニューでは、AP で利用可能なすべての設定にアクセスできます。

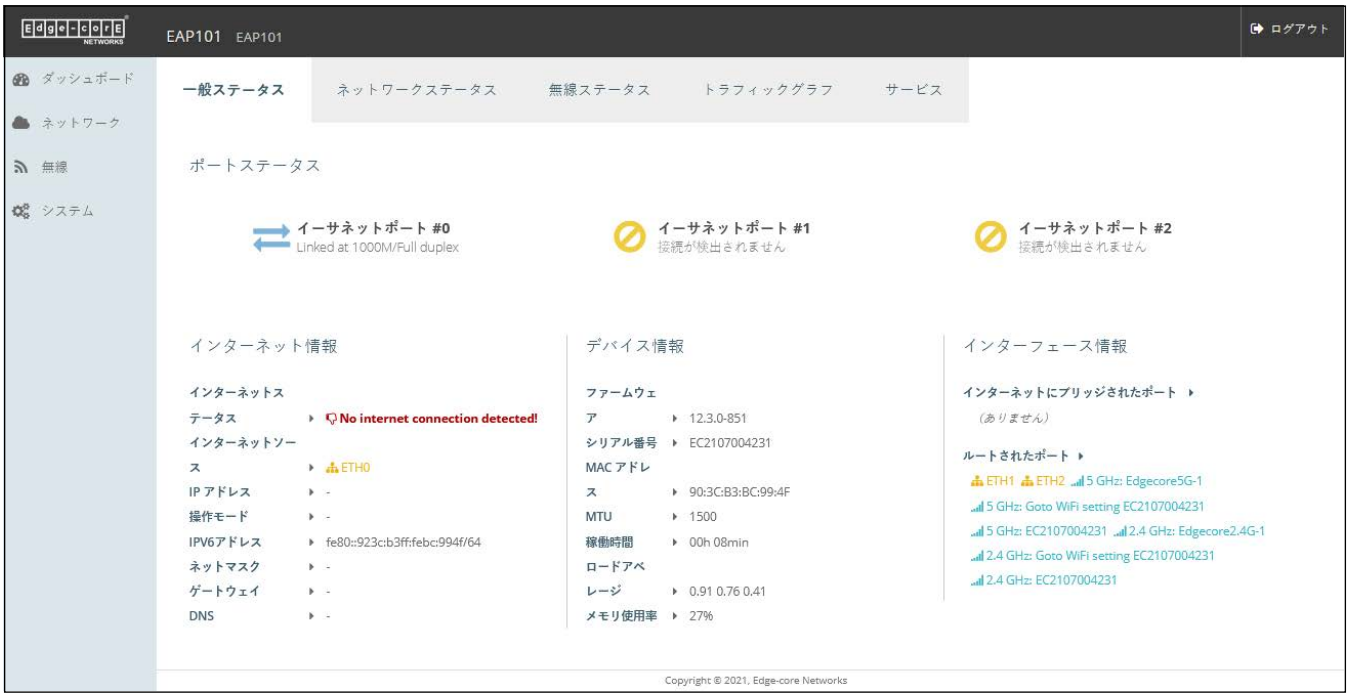
設定を行うには、メインメニューから関連する項目をクリックします。各メインメニュー項目の概要は以下のとおりです。各ページへのリンクをク リックすると、設定パラメータの詳細を確認することができます。

- ダッシュボード — ダッシュボードには、一般ステータス、ローカルネットワークの設定、無線 LAN のステータスなど、AP の基本的な設定が表示されます。30 ページの「ステータス情報」をご参照ください。
- ネットワーク — インターネット、イーサネット、LAN の設定を行います。39 ページの「ネットワーク設定」をご参照ください。
- 無線 - 2.4 GHz、5 GHz 無線および VLAN 設定を行います。63 ページの「無線設定」を参照してください。
- システム — システム（クラウドエージェントや各種システム設定など）、メンテナンス（ログの表示、再起動、リセット、バックアップ、復元、ファームウェアのアップグレードなど）、ユーザーアカウント、サービス（NTP など）、診断（ping、traceroute など）の設定を行います。

ダッシュボード

ウェブインターフェースにログインすると、ダッシュボードが表示されます。ダッシュボードには、インターネットの状態、ローカルネットワークの設定、無線 LAN のステータスなど、AP の基本的な設定が表示されます。

図 14: ダッシュボード



ウェブインターフェース上でよく見られるボタン

以下では、ウェブ管理インターフェース上で共通して使われているボタンについて説明しています。

- 保存 – 新しいパラメータを適用し、一時的に RAM メモリーに保存します。また、変更内容がまだフラッシュメモリに保存されていない ことを知らせるメッセージが画面上部に表示されます。「保存 & 適用」ボタンをクリックしないと、再起動時に現在の設定は保存されません。

図 15: 設定の変更を保存する

- 保存 & 適用 – ページで行った変更を保存してから適用することで、再起動後も設定が保持されます。
- リセット – 新たに入力した設定を取り消し、元の設定に戻します。
- ログアウト – ウェブ管理セッションを終了します。

セクション II

ウェブ設定

このセクションでは、ウェブブラウザのインターフェースを使って AP を設定するための詳細を説明します。

このセクションには、以下の章が含まれています。

2 ステータス情報

ダッシュボードには、インターネットの状態、ローカルネットワークの設定、無線 LAN の状態、トラフィックグラフ、サービスなど、現在のシステム構成に関する情報が表示されます。

本章には、以下の内容が含まれています。

一般ステータス

「一般ステータス」セクションには、AP に関する情報が表示されます。

図 16: 一般ステータス情報

ポートステータスには、次の項目が表示されます。

- Ethernet Port #0 — WAN イーサネットポートのステータスを表示します（リンクアップ状態、速度、およびデュプレックスモード）
- Ethernet Port #1 — LAN イーサネットポート 1 の以下のステータスを表示します。（リンクアップ状態、速度、デュプレックスモード）
- Ethernet Port #2 — LAN イーサネットポート 2 の以下のステータスを表示します。（リンクアップ状態、速度、デュプレックスモード）
- 3G/LTE — 3G/LTE 接続のステータスが表示されます（EAP112 のみ）

「インターネット情報」には、以下の項目が表示されます。

- インターネットステータス — インターネット接続が確立しているかどうかを表示します。
- インターネットソース — インターネットに接続されているイーサネットポートです。初期値では ETH0 に設定されています。

- IP アドレス — インターネット接続の IP アドレスです。
- モード — IP アドレスが固定もしくはDHCPで設定されているかを示します。
- IPv6 アドレス — インターネット接続の IPv6 アドレス
- ネットマスク — IP アドレスのサブネットマスクです。
- ゲートウェイ — 宛先アドレスがローカルサブネット上にない場合に使用されるゲートウェイルーターの IP アドレス。
- DNS — ネットワーク上のドメインネームサーバーの IP アドレス。DNS は、数値化された IP アドレスをドメイン名に対応させるもので、IP アドレスの代わりに親しみのある名前でネットワークホストを識別するのに使用できます。

「デバイス情報」には以下の項目が表示されます。

- ファームウェア — ファームウェアのバージョン。
- シリアル番号 — AP 本体のシリアル番号。
- MAC アドレス — AP のシステム MAC アドレス。
- MTU — ネットワーク上で送信されるパケットの最大送信単位。
- 稼働時間 — マネジメントエージェントの稼働時間の長さ。
- ロードアベレージ — 直近の 1 分間 / 5 分間 / 15 分間の CPU 負荷の平均値。
- メモリ使用率 — 使用されているメモリの割合。

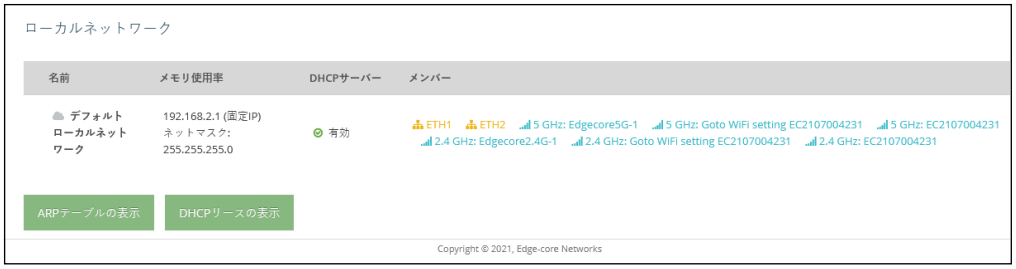
インターフェース情報には、次の項目が表示されます :

- インターネットに接続されたポート - WAN(インターネット) に直接接続された追加のインターフェイスを表示します。
- ルーティングされたポート - デフォルトでは、すべてのインタフェースが LAN のメンバーとして構成されています。これらのインターフェイスからのトラフィックは、イーサネットポート 0 を通して、アクセスポイント全体でインターネットにルーティングされます。(これは、インターネットへのルートとも呼ばれます)。

ネットワークステータス

「ネットワークステータス」セクションでは、ローカルネットワークの接続に関する情報が表示されます。

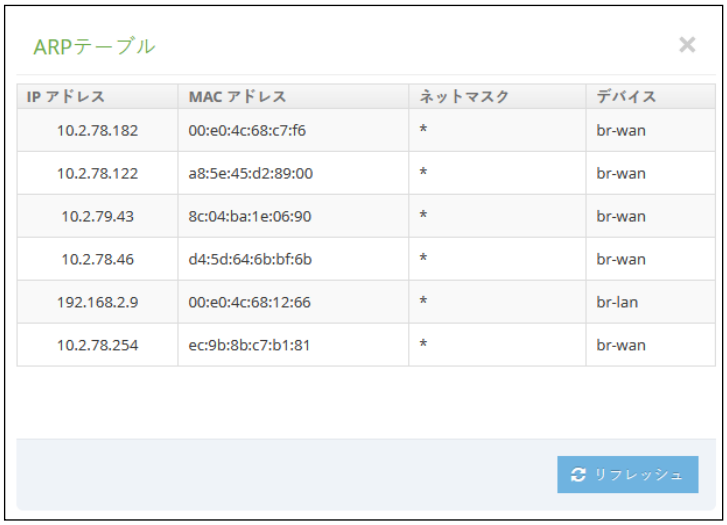
図 17: ローカルネットワーク



このセクションでは以下の項目が表示されます。

- 名前 — ローカルネットワークの名前に関する情報を表示します。
- ネットワーク情報 — ローカルネットワークの構成（スタティック／ダイナミック）、及びネットワークマスクが表示されます。
- DHCP サーバー — このネットワークで DHCP サービスが有効になっているかどうかを表示します。
- メンバー — このネットワークに接続されているポートと無線LANが表示されます。
- アクティブな DHCP リース — DHCP リースを表示します。
- ARP テーブルを閲覧する — ARP キャッシュを表示する。

図 18: ARP テーブル



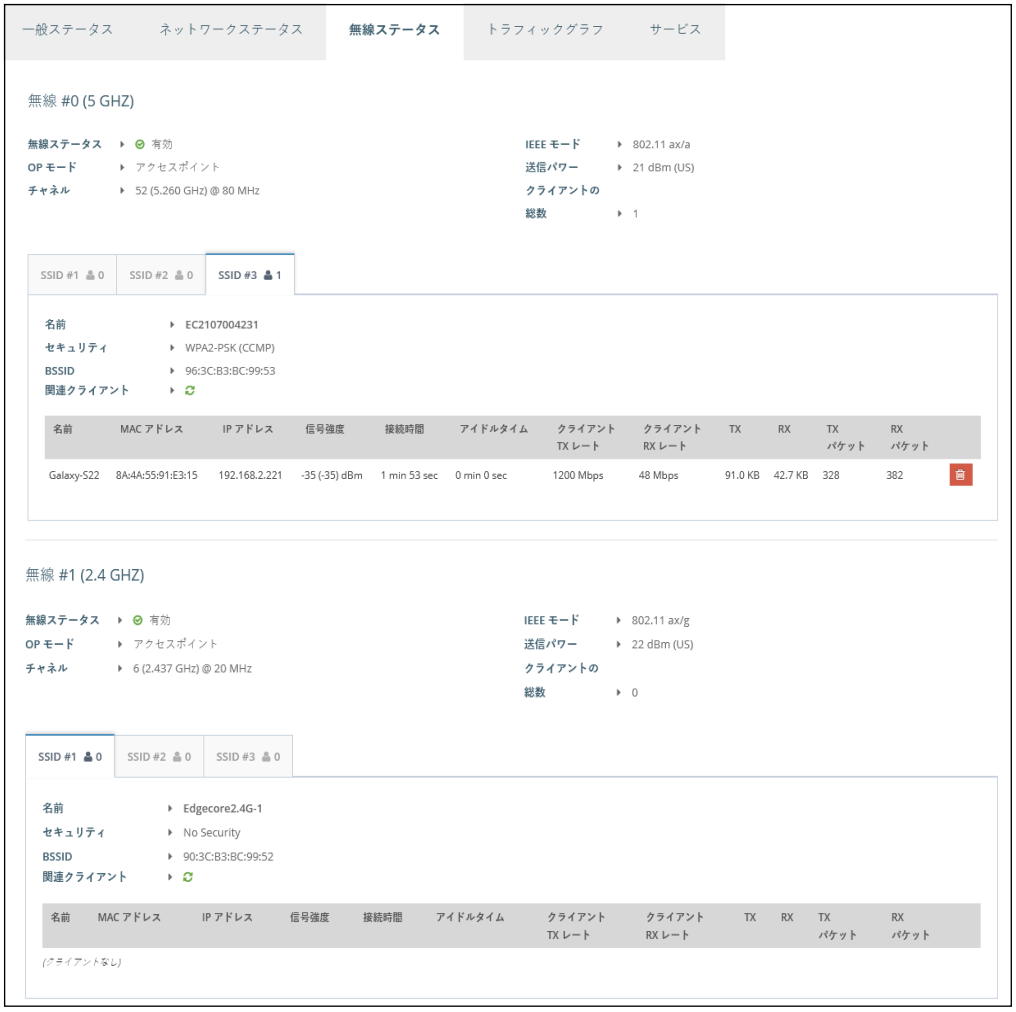
- DHCP リースを閲覧する —DHCP リースを表示する

図 19: DHCP リース

無線ステータス

「無線ステータス」セクションには、無線設定と関連するクライアントに関する情報が表示されます。

図 20: 無線ステータス



また、関連するクライアントの横にある赤いボタンをクリックすると、強制的に接続を解除することができます。

このセクションでは、以下の項目が表示されます。

- 無線 5 GHz/2.4 GHz/HaLow — 2.4 GHz、5 GHz、HaLow（EAP112）ワイヤレスインターフェースを示します。
  - 無線ステータス — 無線インターフェースの有効／無効を示します。
  - IEEE モード — AP がサポートする 802.11 無線 LAN 規格を示します。

- OP モード — 無線インターフェースが、AP モードまたはクライアントモードで動作するように設定されているかどうかを示します。
- 送信パワー — AP から送信される無線信号のパワーです。
- チャネル — AP が無線クライアントとの通信に使用する無線チャネル。利用可能なチャネルは、「802.11 モード」、「チャネル帯域幅」、「国コード」の設定によって異なります。
- クライアントの総数 — このインターフェースに接続されているクライアントの合計数。

- SSID # — サービスセット識別子。AP を経由して無線ネットワークに接続したいクライアントは、SSID を AP のものと同じに設定する必要があります。
  - 名前 — ローカル無線ネットワークの固有の識別子です。
  - セキュリティ — セキュリティが有効になっているかどうかを示します。
  - BSSID — 基本サービスセット識別子。これは、24 ビットの OUI（Organization Unique Identifier、製造者識別子）と、AP の無線チップセットに割り当てられた製造者の 24 ビットの識別子を組み合わせて生成された AP の MAC アドレスです。
- 接続済み端末 — 無線クライアントの詳細を表示します。
  - 名前 — クライアント名。
  - MAC アドレス — クライアントの MAC アドレス。
  - IP アドレス — クライアントに割り当てられている IP アドレス。
  - 信号 — 信号強度（TX/RX）を dBm で表示します。
  - 接続時間 — 無線クライアントが接続されている時間。
  - アイドリング時間 — ワイヤレスクライアントが非アクティブになっている時間です。
  - クライアント TX レート — 無線クライアントへのデータ送信レート。
  - クライアント RX レート — 無線クライアントからのデータ受信レート。
  - TX — 無線クライアントに送信されたバイト数。
  - RX — 無線クライアントから受信したバイト数。

- TX パケット — 無線クライアントに送信されたパケット数。
- RX パケット — 無線クライアントから受信したパケット数。

トラフィックグラフ

Traffic Graphs セクションには、イーサネットポート、ワイヤレスインターフェイス、メッシュインターフェイスのデータレートが表示されます。

図 21: トラフィックグラフ

サービス

サービスセクションには、Edgecore クラウド管理エージェントのステータスが表示されます。

図 22: サービス

- Edge-core Networks Cloud Agent Status - クラウドコントローラーのためのエージェントの有無が表示されます。
- ホットスポット（チリ）- ホットスポットサービスが有効かどうかが表示されます。クリックすると、「ホットスポット設定」メニューが表示されます。
- Edge-core Networks EWS-Series Controller - CAPWAP があるかどうかを表示します。サービスは、EWS-Series コントローラーを介した AP の管理のために有効です

3 ネットワーク設定

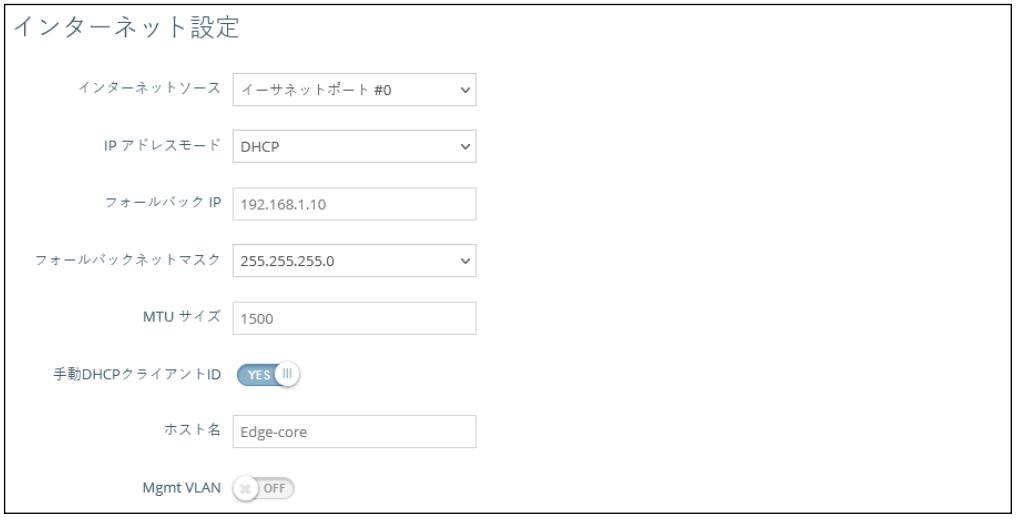
本章では、AP の基本的なネットワーク設定について説明します。

以下の内容が含まれています。

インターネット設定

「インターネット設定」ページでは、ソースポートや IP エイリアス、さらにホスト名や最大 MTU サイズなど、AP の基本的なインターネット設定を行います。

図 23: インターネット設定



このページには以下の項目が表示されます。

- インターネット・ソース — インターネットへのアクセスに使用されるインターフェース。
  - 3G/LTE — インターネットソースとしてLTEインターフェースを選択します (EAP112 のみ)。
    - モデムデバイス — システムに接続されている 3G/LTE モデムデバイスを選択します。
    - APN — LTEネットワークに接続する際にこのデバイスを識別するために使用されるアクセスポイント名（APN)。
    - PIN — デバイスに取り付けられている SIM カードの個人識別番号（PIN)。PIN は、LTE ネットワークにアクセスするための SIM カードの使用を認証します。
    - ユーザー名 — LTE アクセスに使用される名前。
    - パスワード — LTE アクセスに使用されるパスワード。

- IP アドレスモード — インターネットアクセスポートに IP アドレスを提供する際に使用する方法です。初期設定では DHCP になっていて、その他に固定 IP、PPPoE から選択することができます。
  - DHCP— DHCP に表示される設定オプションを Figure 23 に示します。
    - フォールバック IP — DHCP サービスが利用できない、または失敗した場合に使用される IP アドレスです（初期値：192.168.1.10）。
    - フォールバックネットマスク — フォールバック IP アドレスに関連するネットワークマスクです（初期値：255.255.255.0）。
    - Manual DHCP Client Id — DHCP クライアントのホスト名を手動で入力するオプションです。

図 24: IP アドレスモード – 固定 IP

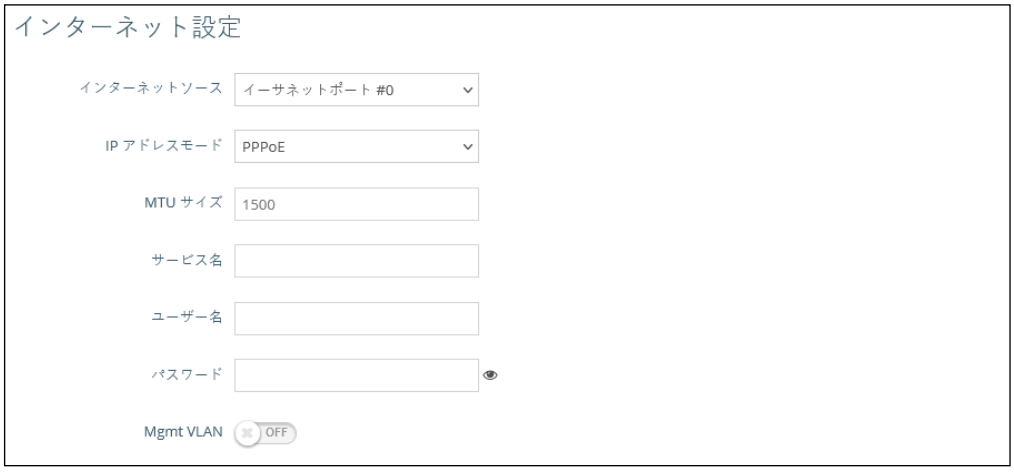
  - 固定 IP — 特定のイーサネットインターフェースに固定 IP アドレスを設定するには、以下の項目を指定する必要があります。
    - IP アドレス — AP の IP アドレスを指定します。有効な IP アドレスは、ピリオドで区切られた 0 ～ 255 の 4 つの 10 進数で構成されています（初期値：192.168.1.1）。
    - サブネットマスク — ローカルのサブネットマスクを示します（初期値：255.255.255.0）。
    - デフォルトゲートウェイ— 要求された宛先アドレスがローカルサブネット上にない場合に使用される、デフォルトゲートウェイ の IP アドレスです。

      管理ステーション、DNS、RADIUS などのネットワークサーバーが別のサブネットにある場合は、デフォルトゲートウェイルーターの IP アドレスをテキストフィールドに入力してください。

- DNS サーバー — ネットワーク上のドメインネームサーバーの IP アドレスです。DNS は、数値化された IP アドレスをドメイン名にマッピングするもので、IP アドレスの代わりに親しみのある名前でネットワークホストを識別するのに使用されます。

  ローカルネットワーク上に DNS サーバーがある場合は、提供されたテキストフィールドに IP アドレスを入力してください。

図 25: IP アドレスモード – PPPoE



- PPPoE — 選択したイーサネットインターフェースの IP アドレスを PPPoE で取得するには、以下の項目を指定する必要があります。
  - サービス名 — PPPoE 接続に割り当てられたサービス名です。通常、サービス名は任意ですが、サービスプロバイダによっては必要な場合があります（範囲：1 ～ 32 文字の英数字）
  - ユーザー名 — サービスプロバイダが指定するユーザー名（範囲：1 ～ 32 文字）
  - パスワード — サービスプロバイダが指定するパスワード（範囲：1 ～ 32 文字）。

- MTU サイズ — このインターフェースで送信されるパケットの最大転送単位（MTU）。のサイズを設定します（範囲：1400 ～ 1500 バイト、初期値：1500 バイト）。

- VLAN タグ — このポートのタグ付けを有効にして、タグ ID を 2 ～ 4094 の間で選択します。

- Mgmt VLAN — このデバイスでマネジメント VLAN を有効にするには、このオプションを選択します。このオプションを有効にすると、内蔵されているローカルネットワーク（192.168.2.1 など）から本機に接続することができなくなります。指定した VLAN ネットワークからのみ、このデバイスに接続できるようになります。このデバイスの IP モードが DHCP

に設定されている場合は、VLAN ネットワークに割り当てられた サブネット範囲内の新しい IP アドレスも要求されます。

IPv6 設定

インターネットアクセスポートに IPv6 アドレスを提供するための方法を設定できます。

図 26: IPv6 設定

この部分には、次の項目が表示されます。

- IPアドレスモード—IPv6アドレスを提供するために使用される方法です。インターネットアクセスポート。(デフォルト：DHCP、オプション：DHCP、スタティック IP)
  - DHCP — DHCP を設定する場合は、Client Id を指定する必要があります。
    - クライアントID — DHCPクライアントのクライアントIDを手動で入力する。
  - スタティック IP - インターネットアクセスポートに静的 IPv6 アドレスを設定します。以下の項目を指定する必要があります。
    - IP アドレス — アクセスポイントの IPv6 アドレスを指定します。IPv6 アドレスは、RFC2373 に従って、コロンで区切られた 16 ビットの 16 進数値 8 個を使用して構成する必要があります。未定義のフィールドを埋めるために必要な適切な数のゼロを示すために、アドレス内で 1 つのダブルコロンを使用することができます。
    - デフォルトゲートウェイ— デフォルトゲートウェイのIPv6アドレスです。要求された宛先アドレスがローカルサブネット上にない場合に使用されます。
    - DNS — ネットワーク上のドメインネームサーバーの IPv6 アドレスです。DNS は、数値の IPv6 アドレスをドメイン名にマッピングし、IPv6 アドレスの代わりに馴染みのある名前でネットワークホストを識別するために使用することができます。ローカルネットワーク上に DNS サーバーがある場合は、IPv6 アドレスをテキストフィールドに入力してください。

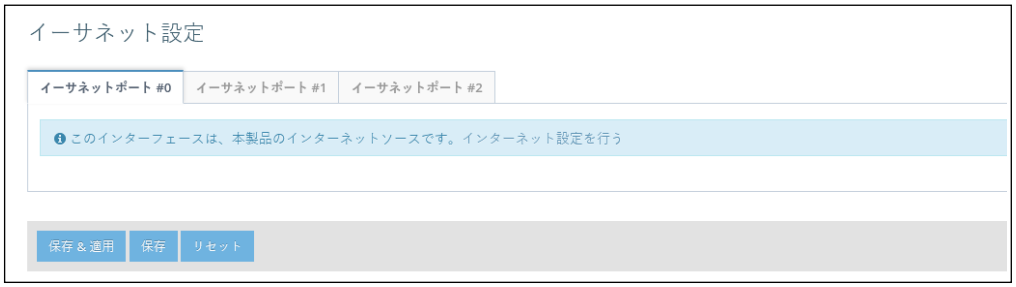
イーサネット設定

「イーサネット設定」のページでは、イーサネットポートのネットワーク動作を設定し、ポートがローカルネットワークに接続された無線クライアントにインターネット接続を提供する（インターネットにルーティングされる）か、インターネットに直接ブリッジされるかを示します。

以下の項目は、「イーサネット設定」の全ページに共通しています。

- イーサネットポート #0 — WAN イーサネットポートの状態を表示します。
- イーサネットポート #1 — LAN イーサネットポート 1 の状態を表示します。
- イーサネットポート #2 — LAN イーサネットポート 2 の状態を表示します。

図 27: イーサネット設定 – インターネットソース

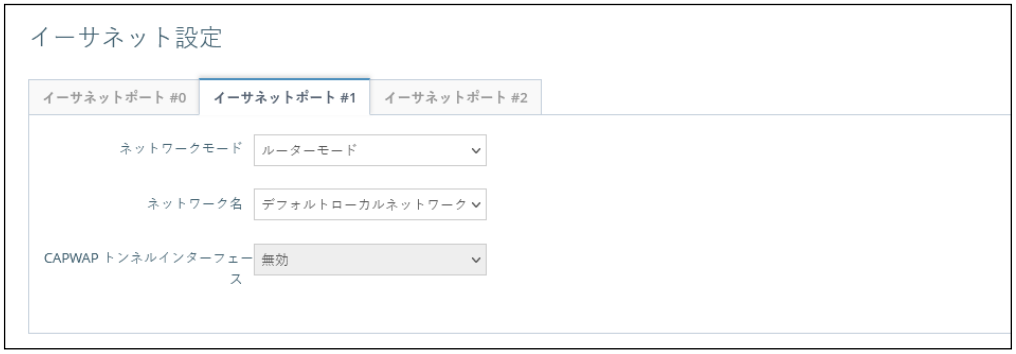


インターネットのソースにインターフェースが設定されている場合、次のようなステータスメッセージが表示されます。

- 「このインターフェースは本製品のインターネットソースです。インターネット設定を行う」

  複数のインターフェースがインターネットに接続されている場合は、最後に設定されたインターフェースのみが使用されます。

図 28: イーサネット設定 – ネットワークモード



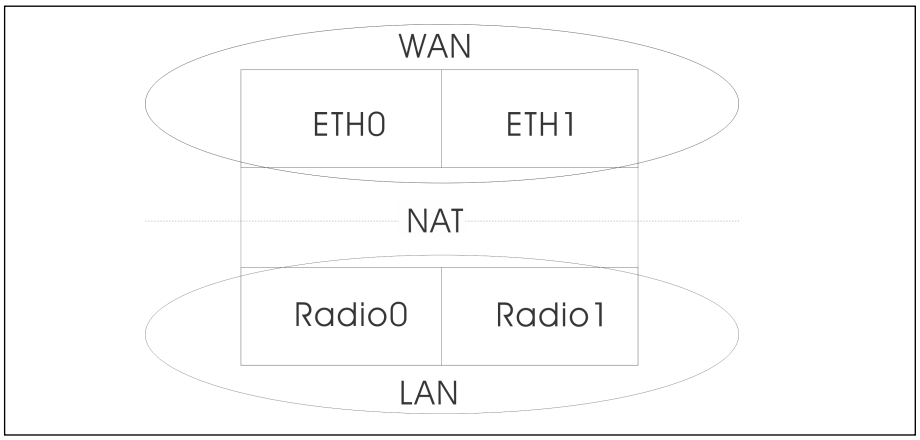
このページには以下の項目が表示されます。

- ネットワークモード — インターネットに接続していないイーサネットポートについては、以下のいずれかの接続方法を指定する必要があります（初期値：ルーターモード）。

  - ブリッジモード— WANに接続されるインターフェースを設定します。このインターフェースからのトラフィックは、インターネットに直接ブリッジされます。イーサネットポートがインターネットにブリッジされている場合、このポートに直接接続して管理アクセスを行うことはできません。しかし、別のイーサネットポートや無線インターフェースが LAN 内にある場合（インターネットにルーティングされている場合）、同じサブネット内の IP アドレスが設定されている PC から、このインターフェースを介して AP を管理することができます。

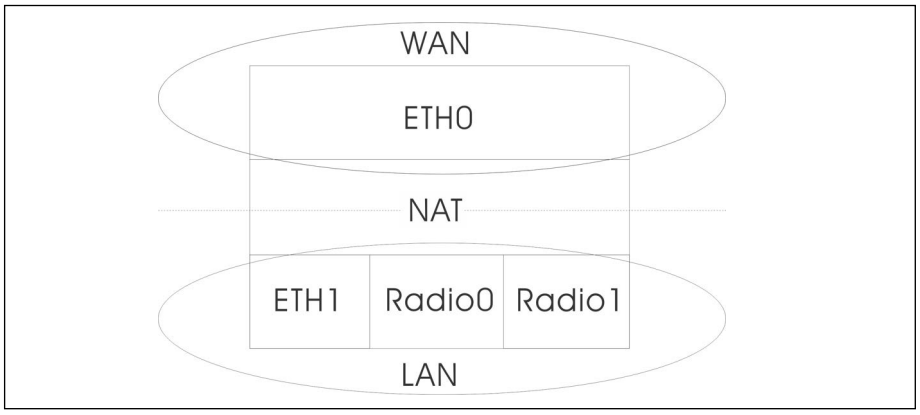
    次の図では、イーサネットポート 0（ETH0）とイーサネットポート 1（ETH1）の両方が WAN に接続されています。

図 29: ブリッジモード



  - ルーターモード — LAN のメンバーとなるインターフェースを設定します。このインターフェースからのトラフィックは、AP を経由して、インターネットに直接ブリッジされているインターフェースを 経由してルーティングされます。初期値では、イーサネットポート 1 はインターネットにルーティングされ、同じサブネット内のアドレス で構成された PC に直接接続して管理アクセスを可能にします。

図 30: ルーターモード



- ネットワーク名 — ルーティングするネットワークです。初期値は、「LAN 設定」-「ローカルネットワーク」で表示されるネットワークです。

- ゲストネットワークを追加 — このポートはゲストネットワークにのみ対応可能です .

- Hotspot Controlled - このポートは、ホットスポットサービスにのみアクセスできます。リンクをクリックすると、「Hotspot Settings」ページが表示されます。51 ページの「ホットスポット設定」を参照してください。

- VLAN タグトラフィック — 指定した VLAN からのタグ付きトラフィ ックを送信するポートです。設定されたリストから VLAN ID を選択するか、リンクをクリックして「ワイヤレス VLAN 設定」ページを開き、VLAN ID を作成します。76 ページの「VLAN 設定」を参照してください。

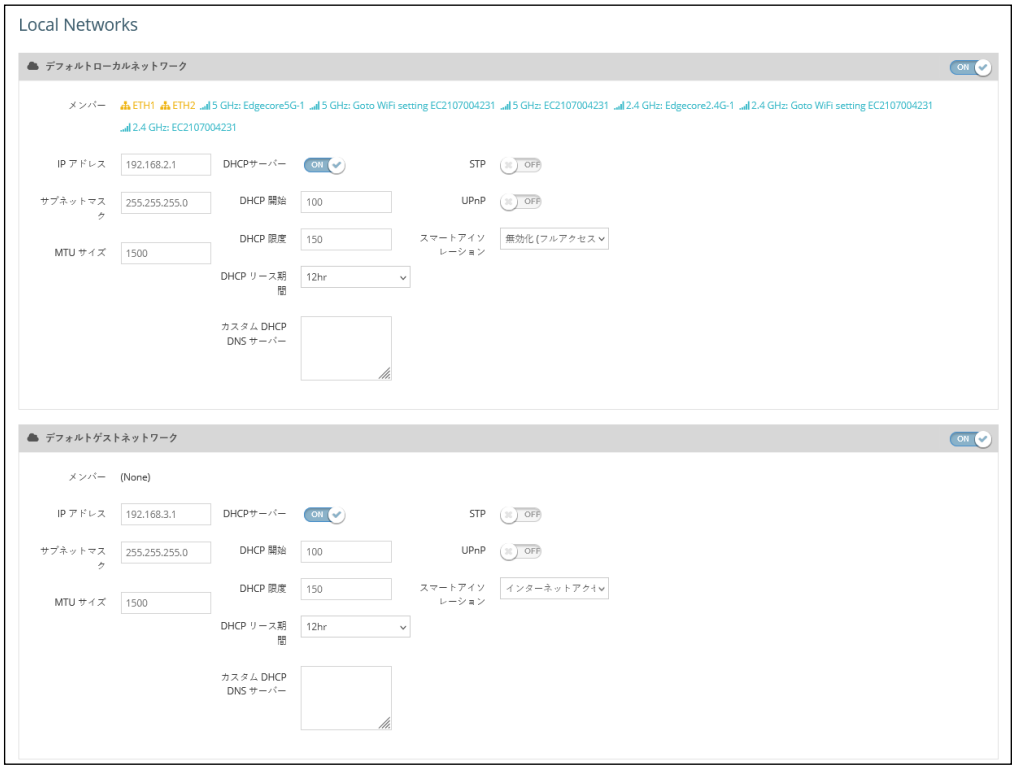
- PoE Out — (EAP104 のみ) PoE ソースが 802.3at として検出された場合、PoE Out 機能を有効にし、それ以外の場合は PoE Out 機能を無効にします。Off に設定すると、PoE Out は常に無効となります。(デフォルト：オン)

- CAPWAP トンネルインターフェース - AP システム管理が EWS-Series Controller モードに設定されている場合（84 ページの「システム設定」を参照)、CAPWAP（Control And Provisioning of Wireless Access Points）プロトコルトンネルモードをコントローラテンプレートからイーサネットポートに設定することができます。オプションは、"Disable " または "Complete " です。Complete トンネルは、AP からのすべての管理、認証、およびデータトラフィックをコントローラに送り返します。(デフォルト：無効)

LAN 設定

LAN 設定」ページでは、IP インターフェース設定、DHCP サーバー設定、STP 管理状態など、ローカルネットワークとゲストネットワークの LAN 設定を行います。

図 31: ネットワーク – LAN 設定



このページには以下の項目が表示されます。

- IPアドレス — ローカルネットワークまたはゲストネットワークのIPアドレスを指定します。有効な IP アドレスは、ピリオドで区切られた 0 ～ 255 の 4 つの 10 進数で構成されています（初期値：192.168.2.1）。
- サブネットマスク — ローカルのサブネットマスクを示します（初期値：255.255.255.0）。
- MTU サイズ — このネットワークで送信されるパケットの最大送信単位（MTU）のサイズを設定します（範囲：1400 ～ 1500 バイト、初期値：1500 バイト）。
- DHCPサーバー — このネットワークでのDHCPの有効/無効を設定します（初期値：有効）。
  - DHCP 開始 — アドレスプールの最初のアドレス（範囲：1 ～ 256、初期値：x.x.x.100）。

- DHCP 限度 — アドレスプール内の最大アドレス数（範囲：1 ～ 254、初期値：150）。
- DHCP リース時間 — DHCP クライアントに IP アドレスが割り当てられる期間です。
- カスタム DHCP DNS サーバー — 使用するカスタム DNS サーバーのア ドレスまたはホスト名を指定します。

- STP — スパニングツリープロトコルメッセージの処理を有効または無効にします（初期値：無効）。
- UPnP — Universal Plug-and-Play ブロードキャストメッセージの有効／無効を設定します。(デフォルト：無効)
- スマートアイソレーション — ネットワークトラフィックを指定された範囲に制限できるようにします。ネットワークに接続します。
  - 無効（フルアクセス）- トラフィックの分離はありません。クライアントはインターネットやローカル LAN 上の他のデバイスにアクセスすることができます。
  - インターネットアクセスのみーこのネットワークからのトラフィックは、インターネット間でのみルーティングできます。
  - LAN アクセスのみ — このネットワークからのトラフィックは、ローカル LAN 機器にのみ制限されます。
  - インターネットアクセス厳禁 - このネットワークからのトラフィックは、インターネットとの間でしかルーティングできませんが、ユーザーはプライベートネットワーク上のリソースやデバイスにアクセスできないという追加制限があります（192.168.0.0, 172.16.0.0, 10.0.0.0 など).
- カスタム LAN を追加 - このボタンをクリックすると、独自のカスタム設定を持つ追加のネットワークを作成することができます。最大 5 つのカスタム LAN を作成することができます。

ファイアウォールのルール

ファイアウォール・フィルタリングは、接続パラメータを制限して、侵入のリスクを抑制します。ファイアウォール設定では、送信元および送信先の IP アドレスとポートに基づいてトラフィックをフィルタリングするルールの逐次リストを定義することができます。入力パケットは、フィルタールールに 1 つずつ照合されます。パケットがルールにマッチするとすぐに、設定されたターゲットアクションが実行されます。

Allow-Ping というルールは、インターネットからの Ping パケットを許可するようにあらかじめ設定されています。このルールは有効・無効を切り替えることができますが、変更・削除はできません。新規追加ボタンをクリックすると、新しいファイアウォールルールを追加することができます。

図 32: ファイアウォールのルール

このページでは、次の項目が表示されます。

- 有効 - ルールの有効・無効を設定します。
- 名前 - フィルタリング・ルールのユーザー定義の名前です。(範囲：1 ～ 30 文字)
- ターゲット - パケットがマッチしたときに取るべきアクションです。(オプション : Accept, Reject, Drop, Mark, Notrack; デフォルト : Accept)
  - Accept — 一致するパケットを受け付けます。
  - Reject — 一致するパケットをドロップし、応答としてエラーパケットを返します。
  - Drop — マッチングパケットをドロップします。
- IP アドレスファミリー — IP アドレスファミリーを指定します。(オプション：Any、IPv4、デフォルト：Any)
- ソース — 送信元インターフェースです。(オプション ゲストネットワーク、ホットスポットネットワーク、デフォルトのローカルネットワーク、インターネット)
- ソース IP — CIDR 表記の送信元 IPv4 アドレスです。IPv4 アドレスの後にスラッシュ（/）とネットワークマスクを定義するための 10 進数を含む。

- ソースポート — 送信元プロトコルポートです。(範囲 : 0-65535)
- プロトコル — プロトコルタイプ (オプション : Any, TCP+UDP, TCP, UDP, ICMP; Default: TCP+UDP)
- 宛先 — 宛先インターフェイスを指定します。(オプション ゲストネットワーク、ホットスポットネットワーク、デフォルトのローカルネットワーク、インターネット、任意)
- 宛先 IP — 宛先 IP address.
- 宛先ポート - 宛先プロトコルポートです。(範囲 : 0-65535)

ポートフォワーディング

ポートフォワーディングは、インバウンドのプロトコルタイプ（TCP/UDP）とポートを「内部」IP アドレスとポートにマッピングするために使用できます。内部（ローカル）IP アドレスは、ネットワークの端にあるローカルデバイスに割り当てられた IP アドレスで、外部 IP アドレスは、AP インターフェースに割り当てられた IP アドレスです。これにより、リモートユーザーは、単一のパブリック IP アドレスを使用して、ローカルネットワーク上の異なるサーバーにアクセスすることができます。

パブリック IP アドレスを通じてローカルサイトの Web や FTP などのサービスにアクセスするリモートユーザーは、他のローカルサーバーの IP アドレスと TCP/UDP ポート番号にリダイレクト（マッピング）されます。例えば、タイプ / パブリックポートを TCP/80（HTTP または Web)、プライベート IP/ ポートを 192.168.3.9/80 に設定すると、外部のユーザーからのすべての HTTP リクエストはポート 80 の 192.168.3.9 に転送されます。したがって、ISP から提供される外部 IP アドレスを使用するだけで、インターネットユーザーは、リダイレクト先のローカルアドレスで必要なサービスにアクセスすることができます。

図 33: ポートフォワーディング

以下がこのページに表示されます。

- 有効 — ポートフォワーディングを有効にする
- 名前 — ユーザー名 (範囲 : 1-30 文字)

- プロトコル — ポートフォワーディングを適用するプロトコルを設定します。(オプション：TCP、UDP、TCP+UDP)
- 外部 Port - TCP/UDP ポート番号です。(範囲 : 1-65535)

  一般的な TCP サービスのポート番号には、以下のようなものがあります。HTTP: 80、FTP: 21、Telnet: 23、POP3: 110 などです。
- 内部 IP アドレス — 内部宛先 IP アドレスです。
- 内部ポート — 内部宛先プロトコルポートです。(範囲：1 ～ 65535)

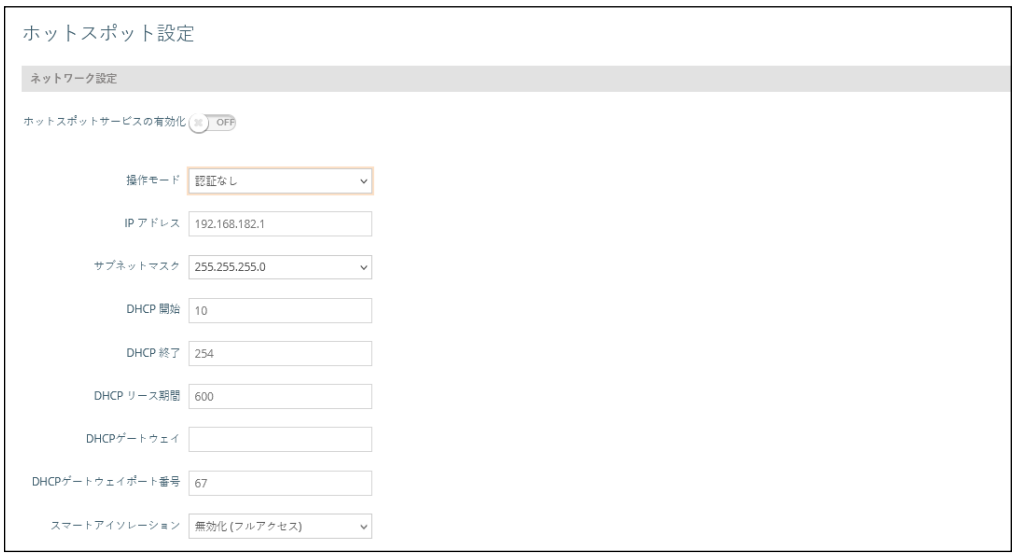
ホットスポット設定

ホットスポット設定ページでは、喫茶店、図書館、病院などの場所で、一般の人がインターネットにアクセスできるように設定することができます。また、RADIUS サーバーを介して特定のアクセス権を定義することもできます。

ネットワーク設定

このセクションには、ホットスポットサービスを有効または無効にするオプション、ホットスポットモードオプション、およびネットワーク設定が含まれています。

図 34: ホットスポット設定 (ネットワーク設定)



このページには以下の項目が含まれています :

- ホットスポットサービスを有効にする — ホットスポットのサービスを有効または無効にします。ホットスポットは、インターネットサービスプロバイダに接続されたルーターを使用して、無線ローカルエリアネット

ワークを介して、一般的に Wi-Fi 技術を使用して、人々がインターネットアクセスを得ることができる場所です。

- モード — ホットスポットサービスには以下のオプションが含まれています：
  - 外部キャプティブポータルサービス - このオプションは、ホットスポットのゲストに外部でホストされているキャプティブポータルのスプラッシュページを表示し、サービス設定の方法によっては、ログインを促すことができます。Cloud4Wi や HotSpotSystem など、サードパーティのキャプティブポータルサービスプロバイダと契約している場合は、このオプションを選択してください。
  - 認証なし - このオプションは、カスタマイズされたローカルホストキャプティブポータルスプラッシュページをホットスポットゲストに表示し、インターネットにアクセスする前にゲストがログインする必要はありません。(オプションの) 利用規約テキストを記入すると、ゲストはインターネットにアクセスする前にこれを承諾する必要があります。
  - シンプルなパスワードのみのスプラッシュページ - このオプションは、ホットスポットのゲストに、カスタマイズされたローカルにホストされたキャプティブポータルスプラッシュページを表示し、ログインしてインターネットにアクセスするためにシンプルなパスワードを入力するよう要求します。(オプションの) 利用規約テキストを記入すると、ゲストはインターネットにアクセスする前にこれを承諾する必要があります。
  - 外部 RADIUS 付きローカルスプラッシュページ - このオプションは、カスタマイズされたローカルにホストされたキャプティブポータルスプラッシュページをホットスポットゲストに表示し、ログインしてインターネットにアクセスするために有効な RADIUS ユーザー名とパスワードを入力するよう要求します。オプションの）利用規約テキストを記入した場合、ゲストはインターネットにアクセスする前に、これを承諾する必要があります。
- ネットワーク IP - ホットスポットの IP アドレスを指定します。有効な IP アドレスは、ピリオドで区切られた 4 つの 10 進数（0 ～ 255）で構成されています。(デフォルト : 192.168.182.1)

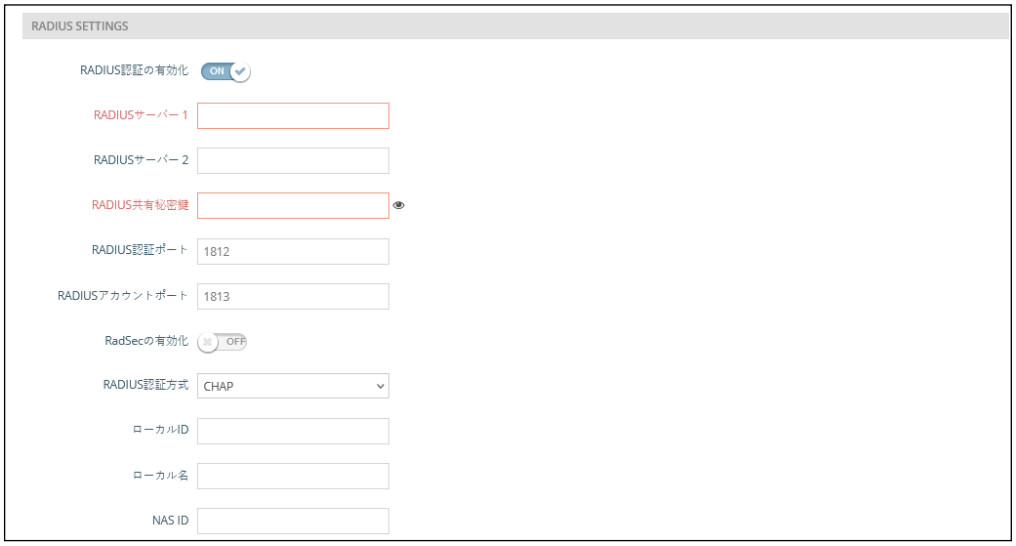
  WAN サブネットがローカルネットワーク（作成したカスタムネットワークも含む）と競合する場合、AP はローカルネットワークのサブネットを自動的に変更します。
- Network Mask - 関連する IP サブネットのネットワークマスクです。このマスクは、特定のサブネットへのルーティングに使用されるホストアドレスビットを特定します。

- DHCP Start - アドレスプールの（最後の数字フィールド）の開始番号です。(範囲 : 1-254; デフォルト : 10)
- DHCP End - アドレスプールの（最後の数値フィールド）の終了番号です。(範囲 : 1-254; デフォルト : 254)
- DHCPリース時間 - IPアドレスがDHCPクライアントに割り当てられる期間です。(範囲：600 ～ 43200 秒、初期値：600 秒)
- DHCP ゲートウェイ - DHCP ゲート IP アドレスを使用する場合は、設定します。内部 DHCP サーバーの代わりに外部 DHCP サーバーを使用します。
- DHCP ゲートウェイポート - DHCP ゲートウェイが使用するリスニングポートです。
- スマートアイソレーション – ホットスポットユーザーが WAN リソースにアクセスできないようにするために有効化します。

RADIUS サーバー

外部キャプティブポータルサービスまたは外部 RADIUS を使用したローカルスプラッシュページにモードを設定するをクリックすると次の項目が表示されます。

図 35: ホットスポット設定 (RADIUS 設定)



本ページには以下の項目が含まれています :

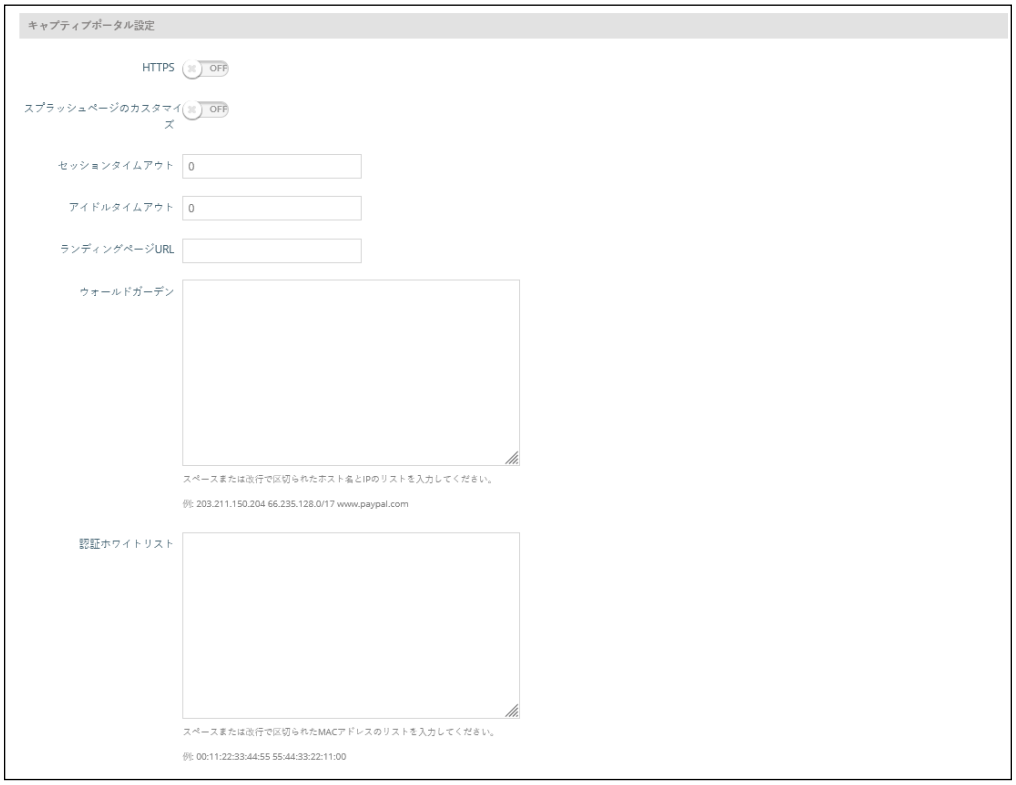
- RADIUS Auth を有効にする - RADIUS サーバーを介したクライアント認証の有効 / 無効を設定します。
- RADIUS サーバー 1 - プライマリ RADIUS サーバーの IP アドレスまたはホスト名です。

- RADIUS サーバー 2 — セカンダリーRADIUS サーバーの IP アドレスまたはホスト名です。
- RADIUS Shared Secret - アクセスポイントと RADIUS サーバー間のメッセージを暗号化するために使用される共有テキスト文字列です。同じ文字列が RADIUS サーバーで指定されていることを確認してください。文字列には空白を使用しないでください。(範囲 : 1-255 文字)。
- RADIUS Auth ポート - 認証メッセージに使用する RADIUS サーバーの UDP ポートです。(範囲：1 ～ 65535、デフォルト：1812)。
- RADIUS Acct Port - アカウンティングメッセージに使用される RADIUS サーバーの UDP ポートです。(範囲 : 1-65535、デフォルト : 1813)
- Enabl RadSec を有効にする - RADIUS データグラムを TCP および TLS で転送するための認証および認可プロトコルです。RADSec は、RADIUS の初期設計で使用されていた UDP を置き換え、信頼性の高いトランスポートプロトコルとパケットペイロードのより広範なセキュリティを提供します。
- RADIUS Auth メソッド - AP と RADIUS サーバー間のメッセージに使用する暗号化方法（CHAP、PAP、MSCHAPv2）を選択します。暗号化方式は、RADIUS サーバーが使用するものと一致する必要があります。
- ローカル ID — ローカル RADIUS サーバーの識別子です。
- ローカル名 — ローカル RADIUS サーバー名です。
- NAS ID - ローカル RADIUS サーバーの操作識別子です。

キャプティブポータル設定

すべてのホットスポットモードのオプションについて、次のセクションが表示されます。

図 36: ホットスポット設定 (キャプティブポータル設定)



本ページには以下の項目が含まれています :

- HTTPS — キャプティブポータルの HTTPS を有効にします。(初期値 : 無効)

注意 : HTTPS キャプティブポータル用に信頼できる認証機関から固有のセキュリティ証明書をアップロードするには、90 ページの「証明書をアップロードする」を参照してください。

- HTTPS ドメイン — HTTPS キャプティブポータルのドメイン名です。
- キャプティブポータル URL — ホットスポットのインターネットサービスポータルのホスト名です。

  キャプティブポータルは、ホットスポットクライアントがインターネットにアクセスする前に、ウェルカムウェブページ（通常は認証のために使用される）にアクセスすることを強制します。ウェルカムページは、認証や支払いを要求する場合があります。
- キャプティブポータル Secret - ホットスポットにログインする際に使用するパスワードです。
- スプラッシュページのカスタマイズ - このオプションは、外部キャプティブポータルサービス以外のすべてのホットスポットサービスオプ

ションに表示されます。有効な場合、タイトル、背景色、ロゴ画像ファイル、およびオプションの利用規約の情報を入力します。

- セッションタイムアウト - クライアントがホットスポットに接続された状態を維持できる最大時間。(範囲：0 ～ 86400 秒)
- アイドルタイムアウト - 接続が非アクティブな状態を維持できる最大値です。(範囲：0 ～ 86400 秒)
- Landing URL - キャプティブポータルにログインした後にユーザーが誘導される URL を示します。
- Swap Octets - 報告された "入力オクテット" と "出力オクテット" の値を入れ替えます。このオプションは、「外部キャプティブポータルサービス」の下にのみ表示されます。
- Walled Garden - 認証されていないユーザーがナビゲートすることを許可されているウェブサイトのリストです。
- Auth ホワイトリスト - キャプティブポータルを迂回してインターネットにアクセスすることが許可されている MAC アドレスのリストです。

OpenRoaming

OpenRoaming は、無線ネットワーク間のシームレスなローミングをサポートするための公衆アクセス Wi-Fi ネットワークの標準を提供します。OpenRoaming ネットワークは、クライアントがネットワークに接続するかどうかを決定できるように、その公衆 Wi-Fi 機能とサービスをアドバタイズします。

最大 32 の OpenRoaming プロファイルを設定し、特定のワイヤレスネットワークに適用することができます（76 ページの「無線ネットワーク — ネットワーク設定」73 ページの「ワイヤレスネットワーク - ネットワーク設定」の「OpenRoaming」を参照）。プロファイルを設定するには、「新規追加」をクリックします。

図 37: OpenRoaming プロファイル

このページには以下の項目が表示されます：

- プロファイル名 — プロファイルを識別する名前。
- インターネットアクセス — このネットワークがインターネットへのアクセスを提供する場合に有効にします。
- アクセス・ネットワーク・タイプ — 定義済みのリストから 1 つを選択します。
  - プライベート・ネットワーク - 無許可のユーザーがアクセスできないホーム・ネットワークおよび企業ネットワーク。
  - ゲストアクセス付きプライベートネットワーク — ゲストアクセスを提供するプライベートネットワーク。典型的な例は、ゲストアクセスを提供する企業ネットワーク。
  - 有料公衆ネットワーク - すべてのユーザーが有料で利用できるネットワーク。
  - 無料公衆ネットワーク - すべてのユーザーが無料で利用できるネットワーク。
  - パーソナル・デバイス・ネットワーク - アドホック・モードで周辺機器を接続するためのネットワーク。例えば、プリンターに接続するカメラなど。
  - 緊急サービス専用ネットワーク - 緊急時用のサービス専用ネットワーク。

- テストネットワーク - テストまたは実験作業用のネットワーク。
- ワイルドカード - これを選択すると、AP はクライアントのクエリで要求されたネットワークの種類に関係なく、クライアントに返信します。

- HESSID — OpenRoaming ネットワークの HESSID（Homogenous Extended Service Set Identifier）。設定されると、HESSID (MAC アドレス) は同じネットワークに属するすべての AP を一意に識別します。
- Venue Group — Venue の一般グループを示します。以下の定義リストから選択します。
- Venue Type — 各グループ内の特定の Venue タイプを特定します。
- ネットワーク Auth タイプ — ネットワークに必要な認証を指定します。定義済みのリストからオプションを選択します。(デフォルト：「利用規約の承認）
- Type4 Availability — ネットワークから利用可能なIPv4アドレスの種類を指定します。
- Type6 Availability — ネットワークから利用可能なIPv6アドレスの種類を指定します。
- Operating Class —IEEE Std 802.11-2012 Annex E に基づく AP がサポートする動作チャネルを指定する標準インデックス。
- キャプティブポータル — Captive Portal 機能を有効にします。(デフォルト：無効）
  - ?キャプティブポータルURL — インターネットサービスポータルのホスト名（HTTP または HTTPS)。

    キャプティブ・ポータルは、インターネットへのさらなるアクセスを得る前に、クライアントにウェルカム・ウェブ・ページ（通常は認証に使用）へのアクセスを強制します。ウェルカムページは、認証やお支払いを要求する場合があります。
  - Wall Garden — 認証されていないユーザにナビゲーションを許可する Web サイトのリストです。スペースまたは改行で区切られたホスト名と IP アドレスのリストを入力します。
- Venue 名情報 — 最大 10 の Venue 名のリストを設定します。
  - 言語コード — リストから言語を選択します。(デフォルト：英語）
  - Venue 名 — ネットワーク Venue の名前。複数の名前をリストに追加できます。

  - Venue URL — Venue の追加情報を提供する URL を指定します。

- セルラーネットワーク情報リスト（PLMN）— （オプション）AP を通じて利用可能な 3GPP セルラーネットワークを識別します。具体的には、このフィールドは、移動体通信事業者の移動国コード（MCC）と移動体ネットワークコード（MNC）で構成される公衆陸上移動体ネットワーク（PLMN）ID を識別します。最大 10 個の PLMN ID を設定できます。
  MCC、MNC のペアを入力します。
  例 : 400, 00
  MCC: 小数点以下 3 桁 (000-999)
  MNC: 小数点以下 2 桁（00 ～ 99）または 3 桁 (000-999)

- オペレーター・フレンドリー・ネーム — ネットワーク・オペレーターの名前。最大 10 個の名前を設定できます。

- ローミング・コンソーシアム・リスト — （オプション）ローミング・コンソーシアムとは、ユーザのクレデンシャルを認証に使用できるサービス・プロバイダ（SP）のグループです。各ローミング・コンソーシ アムは、IEEE が割り当てる組織識別子（OI）によって識別されます。OI の長さは 24 ビットであることが多いですが、36 ビットにすることもできます。最大 10 個の識別子を設定できます。

- ドメイン名リスト — AP を操作するエンティティについて、1 つまたは最大 10 のドメイン名をリストします。これは OpenRoaming ネットワーク選択ポリシーにとって重要です。モバイルデバイスがホームホットスポットにいるのか、訪問先のホットスポットにいるのかを示します。

- NAI Realm リスト — （オプション）ネットワーク・アクセス識別子（NAI）レルム・リストは、AP を介してアクセス可能なサービス・プロバイダまたはその他のネットワークを識別します。ネットワークでサポートされている認証レルムを検出することで、モバイルデバイスは優先するネットワークに選択的に認証できます。最大 10 の識別子を設定できます。

  - Method/Authentication — NAI レルムリストに追加された各サービスプロバイダの EAP メソッドと認証を指定します。

DHCP スヌーピング

DHCP snooping は、AP が受信した DHCP メッセージの検証およびフィルタリングに使用されます。DHCP snooping が有効な場合、DHCP snooping テーブルにリストされていないデバイスから受信した DHCP メッセージは、ドロップされます。

MAC アドレスと IP アドレスを指定することで、既知の信頼できる DHCP サーバーをテーブルに追加することができます。

図 38: DHCP スヌーピング

本ページには以下の項目が含まれています：

- DHCP スヌーピングを有効にする—AP 上で DHCP スヌーピングを有効にします。
- Trust DHCP サーバー MAC - 既知の信頼できる DHCP サーバーの MAC アドレスです。
- Trust DHCP サーバー IP - 既知で信頼できる DHCP サーバーの IP アドレスです。
- Remark - 設定された DHCP サーバーに関連するコメントです。

ARP インスペクション

ARP Inspection は、Address Resolution Protocol パケットの MAC アドレスバインディングを検証するセキュリティ機能です。これは、特定の「中間者」攻撃の基礎となる、無効な MAC-IP アドレスバインディングを持つ ARP トラフィックに対する保護を提供します。これは、すべての ARP リクエストとレスポンスを傍受し、ローカル ARP キャッシュが更新されるか、パケットが適切な宛先に転送される前に、これらのパケットのそれぞれを検証することによって達成される。無効な ARP パケットはドロップされます。

図 39: ARP インスペクション

本ページには以下の項目が含まれています：

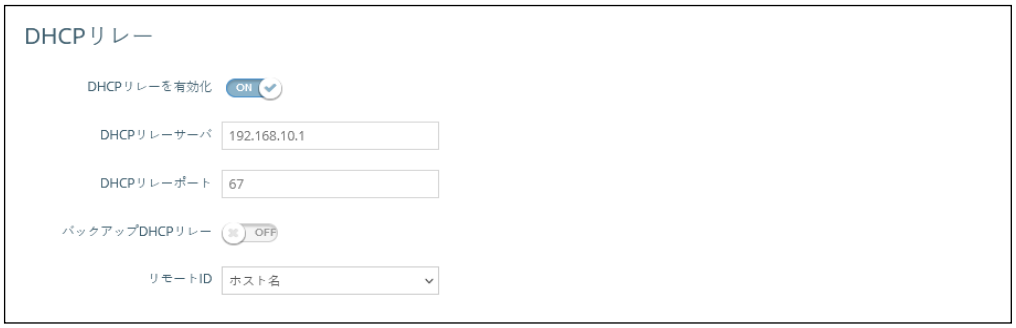
- ARP インスペクション - 有効にすると、ARP パケットは ARP スプーフィングに対して検証されます。
- Force DHCP - APがDHCPパケットを通じてMAC/IPペア情報のみを学習することを許可します。静的 IP アドレスで構成されたデバイスは DHCP トラフィックを送信しないため、静的 IP アドレスを持つクライアントは、その MAC/IP ペアが「静的信頼リスト」にリストされて有効になっていない限り、AP によってブロックされます。
- Trust List ブロードキャスト - 他の AP に ARP 要求を発行するための信頼できる MAC/IP ペアを学習させます。
- 静的信頼リスト - ARP 要求を発行するために信頼されているデバイスの MAC または MAC/IP ペアを追加します。他のネットワークノードは ARP 要求を送信できますが、その IP が静的リストに異なる MAC で表示されている場合、その ARP 要求はドロップされます。

DHCP リレー

DHCP リレーが有効な場合、AP はすべてのクライアントのエージェントとして、すべてのブロードキャスト DHCP 要求を指定した DHCP サーバーに直接送信します。DHCP サーバーの IP アドレスとポートが設定されている必要があり、オプションでバックアップサーバーも設定できます。

DHCP リレーを有効にすると、VLAN 設定または LAN 設定ページで回線 ID を設定することができます。その後、クライアントの IP アドレスは DHCP リレーサーバーによって取得され、IP 範囲はリモート ID と回路 ID によって決定されます。

図 40: DHCP リレー



本ページは以下の項目が含まれています：

- DHCP リレーを有効にする — AP の DHCP リレー機能を有効にします。
- DHCP リレーサーバー — DHCP サーバーの IP アドレスを指定します。
- DHCP リレーポート — DHCP サーバーのポートを指定します。

- バックアップ DHCP リレー - オプションで、プライマリーサーバーからの応答がない場合に使用するバックアップ DHCP サーバーの IP アドレスとポートを指定します。
- リモート ID - ホスト名をリモート ID として使用するか、テキスト文字列をリモート ID として手動で設定します。

4 無線設定

この章では、AP の無線設定について説明します。

以下の内容が含まれています。

無線設定

IEEE 802.11 無線インターフェースには、無線信号の特性や無線セキュリテ ィ機能の設定オプションが含まれています。

アクセスポイントは、802.11b+g+n/ax（2.4GHz）、802.11a/a+n/ac+a+n/ax（5GHz）の複数の無線モードで動作できます。デュアルバンド・アクセスポイントは 2.4GHz と 5GHz で同時に動作し。Web インターフェースでは、無線設定ページを次のように識別します：

- Radio 2.4 GHz — 2.4 GHz 802.11b/g/n/ax 無線インターフェース
- Radio 5 GHz — 5GHz 802.11a/n/ac/ax 無線インターフェース
- HaLow — HaLow（863 ～ 928MHz）無線インターフェース（EAP112 のみ）

各無線機は、SSID1 ～ SSID16 と呼ばれる SSID に基づいて、16 個の VAP（バーチャル AP）インターフェースをサポートします。各 VAP は個別の AP として機能し、独自の SSID（Service Set Identification）とセキュリテ ィ設定を行うことができます。ただし、ほとんどの無線信号パラメータはす べての VAP インターフェースに適用されます。特定の VAP へのトラフィッ クは、ユーザーグループやアプリケーションのトラフィックに基づいて分離することができます。クライアントは、別々の物理的な AP と同じように、各 VAP と関連付けることができます。

電波設定

図 41: 無線 5 GHz のフィジカル設定

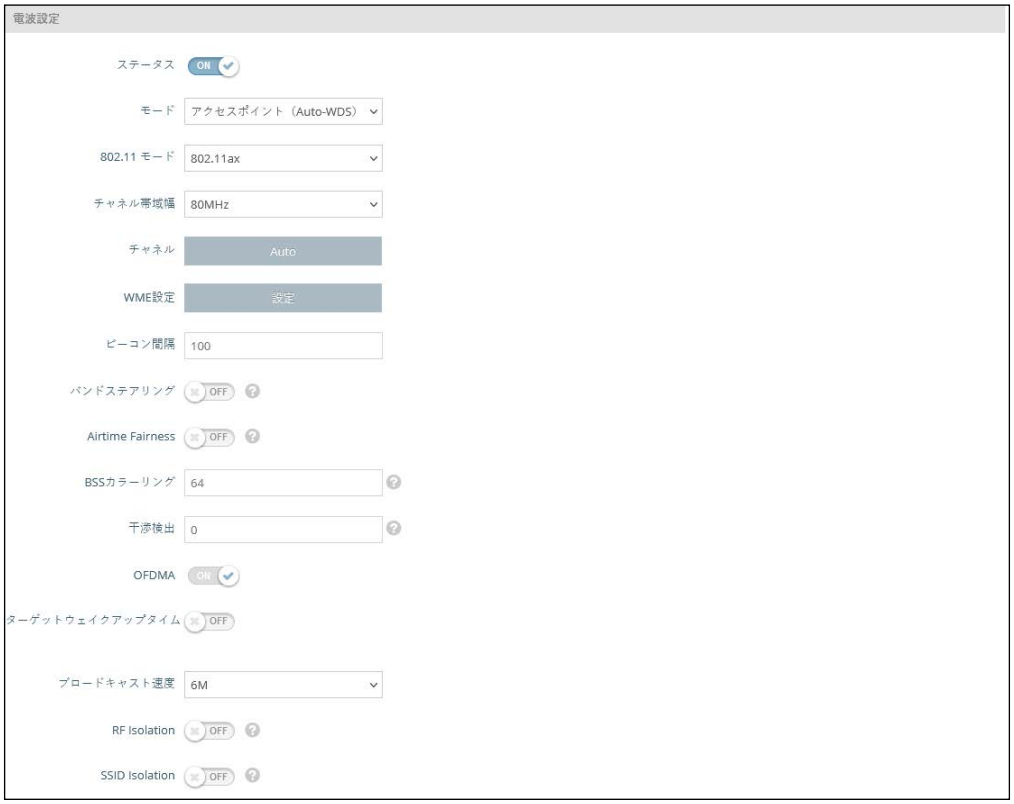


図 42: 無線設定（Radio 2.4 GHz）

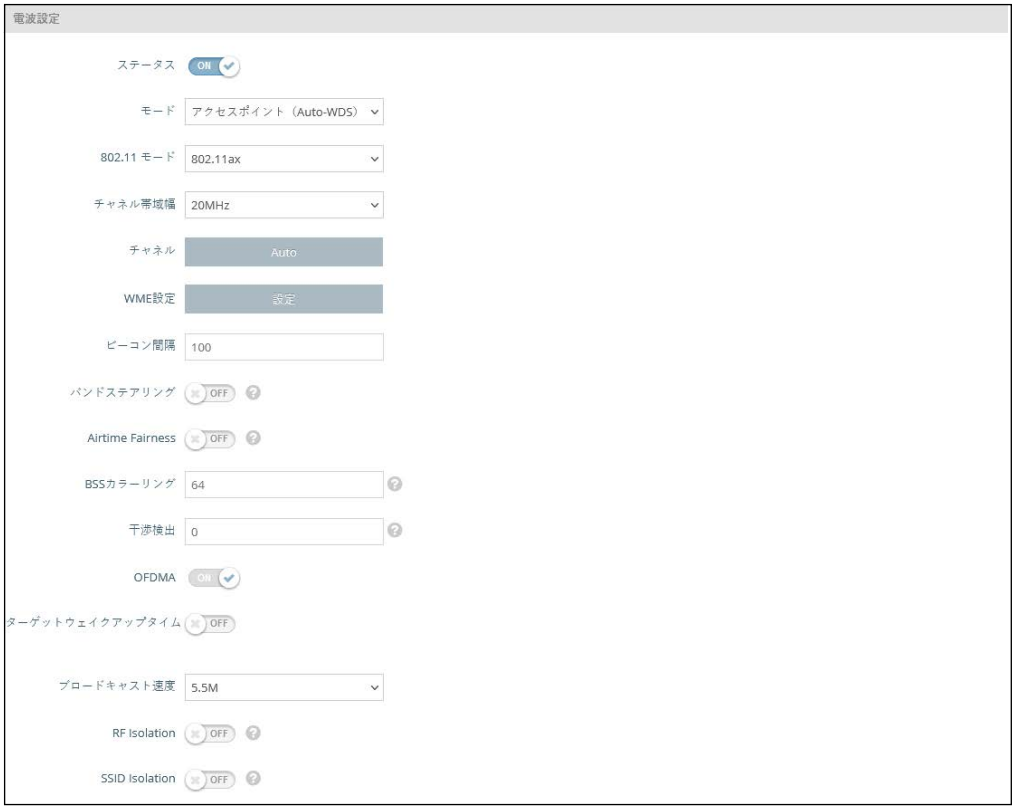
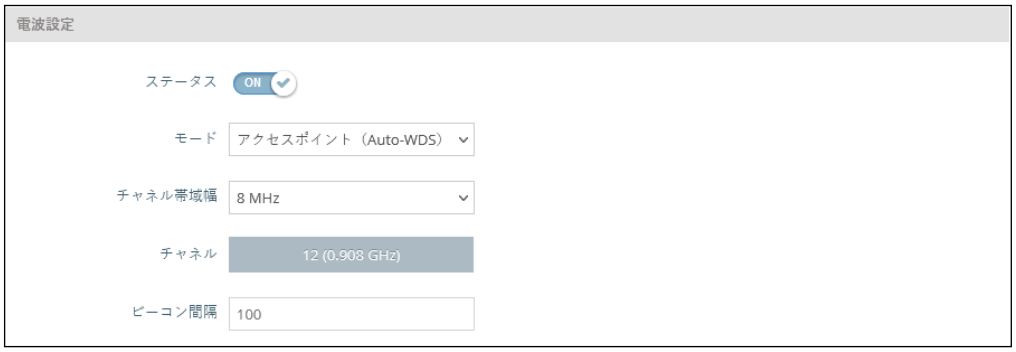


図 43: HaLow のフィジカル設定 (EAP112)



このページには以下の項目が表示されます。

- ステータス — このインターフェースでの無線サービスの有効 / 無効を選択します。
- モード — AP が機能するモードを選択します。
  - アクセスポイント (Auto-WDS) — AP は、WDS モードの AP として動作し、クライアント WDS モードの AP からの接続を受け入れます（初期設定はこの設定です。）

    このモードでは、AP は通常の AP としてクライアントにサービスを提供します。WDS は、同じ SSID とセキュリティ設定を使用する他の AP を自動的に検索して接続するために使用されます。
  - クライアント — AP は、他の AP にワイヤレス接続を提供するだけでなく、ローカルな有線ホストや無線クライアントとの間で情報を受け渡しできます。
- 802.11 モード — 無線機の動作モードです。
  - 無線 2.4 GHz — 初期値：11ax; オプション：11b+g+n/ax
  - 無線 5 GHz — 初期値：11ax; オプション：11a、11a+n、11ac+a+n、11ax
- チャネル帯域幅 — チャネル帯域幅の AP オプションには、20、40、80、160 MHz があります。利用可能なチャネル帯域幅は、802.11 モードに依存します。(デフォルト：2.4 GHz 無線では 20 MHz、5 GHz 無線では 80 MHz、オプション：オプション：20 MHz、40 MHz、80 MHz、160 MHz)
  - 1–8 MHz — 802.11ah HaLow 用（EAP112 のみ）
  - 20MHz — 対応モード：802.11a、802.11a+n、802.11ac+a+n、802.11b+g+n、802.11ax

- 40MHz — 対応モード：802.11b+g+n、802.11a+n、802.11ac+a+n、802.11ax
- 80MHz — 対応モード：802.11ac+a+n、802.11ax（Radio 5GHz のみ）
- 160MHz — (EAP104、EAP111、EAP112、OAP101 5GHz 無線機でのみサポート) 802.11ac+a+n および 802.11ax 用

- チャネル — AP が無線クライアントとの通信に使用する無線チャネル。同一エリアに複数の AP を配置する場合は、以下のように設定します。隣接する AP のチャネルは、お互いに干渉しないように、少なくとも 5 つの チャネルを離して設定してください。例えば、11g/n の 20MHz モード では、チャネル 1、6、11 を使用して、同じエリアに最大 3 台の AP を配置することができます。なお、無線クライアントは、リンクしている AP が使用しているチャネルと同じチャネルを自動的に設定します (利用可能なチャネルは、「802.11 モード」、「チャネル帯域幅」、「国コード」の設定によって異なります)。

  「自動」を選択すると、AP は自動的に空いている無線チャネルを選択します（初期値：自動)。

- WME 設定 - Wi-Fi Multimedia（WMM）としても知られる Wireless Multimedia Extensions（WME）は、IEEE 802.11e 規格に基づく Wi-Fi Alliance の相互運用性認定です。IEEE 802.11 ネットワークに基本的な QoS（Quality of Service）機能を提供します。アクセスプライオリティは、以下のパラメータを使用して 4 つの「アクセスカテゴリー」(AC) タイプに設定することができます。

  - CW Min (Minimum Contention Window) - 無線媒体アクセスが試みられるまでのランダムバックオフ待ち時間の初期上限値である。初期待ち時間は、ゼロと CWMin 値の間のランダムな値です。CWMin 値は、0 ～ 15 マイクロ秒の範囲で指定する。なお、CWMin 値は CWMax 値と同じかそれ以下である必要があります。
  - CW Max (Maximum Contention Window) - 無線媒体アクセスが試みられるまでのランダムバックオフ待ち時間の最大上限値です。衝突が検出されるたびに、CWMax 値までコンテンションウィンドウが 2 倍になります。CWMax 値は、0 ～ 15 マイクロ秒の範囲で指定します。なお、CWMax 値は CWMin 値以上である必要があります。
  - AIFS（Arbitration Inter-Frame Space）- 次のデータ送信を試みるまでの最小の待ち時間です。AIFS の値は、0 ～ 15 マイクロ秒の範囲で指定する。
  - TXOP Limit (Transmit Opportunity Limit) - AC 送信キューが無線媒体にアクセスできる最大時間です。AC キューが送信機会を与えられると、TXOP Limit までの時間、データを送信することができます。このデータバーストにより、高データレートのトラフィックに対する効

率が大幅に改善されます。0 ～ 8192 マイクロ秒の範囲で値を指定します。

- ビーコン間隔 — AP からビーコン信号を送信する速度を設定します。ビーコン信号は、無線クライアントが AP との連絡を維持するためのもの です。ビーコン信号には、電源管理などの情報も含まれています（範囲：100 ～ 1024TU、初期値：100TU)。

- バンドステアリング - 有効にすると、2.4GHz と 5GHz をサポートするクライアントは、最初に 5GHz 無線に接続されます。この機能により、2 つの無線帯域でクライアントの負荷のバランスをとることができます。この機能を完全に動作させるには、両方の無線機で SSID とセキュリティ設定が一致している必要があることに注意してください。(初期値：オフ）

- Airtime Fairness — この機能を有効にすると、ワイヤレスネットワーク全体のパフォーマンスが向上します。(デフォルト : 無効)

- BSS カラーリング - 802.11ax（Wi-Fi 6）モードでは、BSS カラーリングにより、同じ周波数で動作する近隣の AP が、自身の基本サービスセット（BSS）に属するトラフィックを識別することができます。BSS カラーリングにより、近隣の AP とクライアントの送信が重なる高密度環境において、Wi-Fi 6 ネットワークがより効率的に動作するようになります。無線 BSS を識別するためのカラー値（1 ～ 63 の数値）を割り当てるか、AP がカラー値をランダムに選択するようにするために値 64 を入力します。(範囲：1 ～ 63、64 ランダム、デフォルト：64)

- 干渉検出 - 現在のチャンネルの利用率が設定された閾値（パーセンテージ）に達すると、AP は別のチャンネルに切り替わります。(範囲：0 ～ 100%、デフォルト：0、無効)。

- OFDMA — 802.11ax（Wi-Fi 6）モードは直交周波数分割多重アクセス（OFDMA）をサポートしており、これを無効にすることはできません。

- Target Wake Time - 802.11ax（Wi-Fi 6）モードでは、AP は、クライアントが定期的なビーコンに頼らず、フレームを送信または受信するために特定の Target-Wakeup Time（TWT）を要求できるようにします。この機能により、クライアント端末のスリープ時間を大幅に延長することができ、大幅な省電力化を実現します。また、AP はクライアントの TWT を制御してスケジュールすることで、ネットワーク内の競合を管理し、遅延に敏感なトラフィックに対応することができます。(デフォルト：無効)

- ブロードキャストレート — ブロードキャストパケットによって消費されるワイヤレス帯域幅を制限できます。

  - 無線 2.4 Ghz — オプション : 5.5M, 6M, 9M, 11M, 12M, 18M, 24M, 36M, 48M, 54M; デフォルト : 5.5M

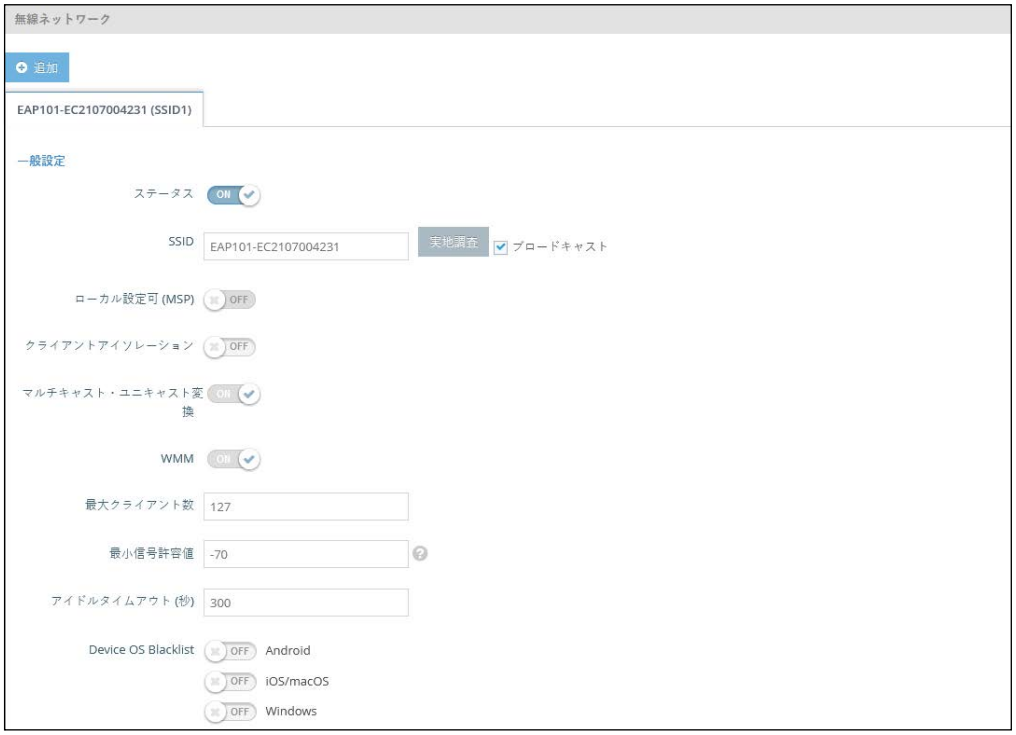
- 無線 5 Ghz — オプション : 6M, 9M, 12M, 18M, 24M, 36M, 48M, 54M; デフォルト : 6M

- RF Isolation — 有効にすると、クライアントは異なる無線カード間で隔離されます。

- SSID アイソレーション - 有効にすると、クライアントは同じ無線カード上の異なる SSID 間で隔離されます。

無線ネットワーク — 一般設定

図 44: 無線設定 （一般設定）



「無線設定」ページのこのセクションには、以下の項目が表示されます。

- ステータス — この VAP の無線サービスを有効または無効にします。

- SSID — バーチャル AP（VAP）インターフェースが提供する基本サービスセットの名前。AP を介してネットワークに接続したいクライア ントは、SSID を AP の VAP インターフェースのものと同じに設定する必要があります（初期値：5GHz の場合は Edgecore5G-#（# は 1 ～ 16)、2.4GHz の場合は Edgecore2.4G-# (# は 1 ～ 16)。1 ～ 32 文字で設定してください)。

- サイトサーベイ - SSID をブロードキャストしているすべてのワイヤレスネットワークをスキャンします。

- ブロードキャスト — SSID を一定の間隔でブロードキャストして、ネットワーク接続を探している無線ステーションが発見できるようにし ま

す。これにより、無線クライアントは WLAN を動的に発見し、WLAN 間をローミングすることができます。また、この機能は、ハッカーがホームネットワークに侵入することを容易にします。SSID は暗号化されていないので、AP からの SSID ブロードキャストメッセージを探して WLAN をスヌーピングすれば、簡単に SSID を取得することができます（初期値：有効）。

- Local Configurable - システムが MSP モードで動作しているときに、SSID をユーザー設定できるようにします（84 ページの「システム設定」を参照）。(デフォルト : 無効)
- クライアントアイソレーション — 有効にすると、無線クライアントは LAN と通信でき、インターネット接続が可能な場合はインターネットにも接続できますが、クライアント同士は通信できません（初期値：OFF）。
- マルチキャストからユニキャストへの変換 — 有効にすると、AP はマルチキャストトラフィックをユニキャストトラフィックに変換し、各関連クライアントに送信します。この機能は、AP がマルチキャストトラフィックを低い基本レートで送信するのに対し、ユニキャストトラフィックは HT、VHT、または HE レートで送信できるため、ネットワークのスループットを向上させることができます。
- 最大クライアント数 — この SSID に同時に接続することができるクライアントの最大数です（範囲：1 ～ 256、初期値：127）。
- 最小信号許容値 — クライアントの信号強度（RSSI）が指定した値を超えると無線インターフェースへの接続を許可します。値を -100 に設定すると本機能は無効になります。既に接続されているクライアントは定期的にチェックされます。(範囲：-1 ～ -100、デフォルト：-100)

  これにより、クライアントはより良い信号強度を持つ AP と関連付けるようになります（アシストローミングとも呼ばれます）。アクセスポイントの密度とカバレッジに応じて、推奨値は -70 ～ -80 です。

- アイドルタイムアウト（秒）— 設定された時間内にアクティビティがない場合、AP はクライアントとの接続を切断します（範囲：60 ～ 60000 秒、初期値：300 秒）。
- Device OS Blacklist — Android, iOS/macOS, Windows のいずれかの OS を搭載したクライアントデバイスからの SSID へのアクセスを拒否します。クライアント OS が SSID に接続できないようにするには ON に設定し、接続を許可するには OFF に設定してください。

無線ネットワーク — セキュリティ設定

図 45: セキュリティ設定

「無線設定」ページのこのセクションには、以下の項目が表示されます。

- メソッド — 各 VAP の無線セキュリティ方式（接続モード、暗号化、認証など）を設定します（初期値：WPA2-PSK）。
  - セキュリティなし — VAP は、設定された SSID を含むビーコン信号をブロードキャストします。SSID の設定が「任意」の無線クライアントは、ビーコンから SSID を読み取り、自動的に SSID を設定してすぐに接続できるようにします。
  - WPA-PSK — 企業が WPA を導入する際には、有線ネットワーク上に RADIUS 認証サーバーを設定する必要があります。一方、RADIUS サーバーを設定・維持するためのリソースを持たない小規模オフィスのようなネットワークでは、WPA は、ネットワークへの接続に事前共有のパスワードだけを使用するシンプルな操作方式を提供します。PSK（Pre-Shared Key、事前共有鍵）モードでは、AP とす べての無線クライアントに手動で入力されるユーザー認証用の共通パスワードを使用します。また、企業における WPA と同じ TKIP パケ ット暗号化と鍵管理を使用し、小規模なネットワークに堅牢で管理しやすい選択肢を提供することが可能です。
    - 暗号化 — データの暗号化には、以下のいずれかの方法が用いられます。
      - CCMP （AES）— マルチキャストの暗号化暗号として AES-CCMP を使用します。AES-CCMP は、WPA2 で必要とされる標準的な暗号化暗号です（初期設定ではこの設定になっています）。
      - Auto: TKIP + CCMP （AES）— クライアントが使用する暗号化方式は、AP によって検出されます。
    - Key Method — 以下の PSK 方式のいずれかを使用します。
      - Single PSK — 単一の PSK キーの入力を可能にします。
        - キー — WPA は、無線クライアントと VAP の間で送信されるデー タを暗号化するために使用されます。ネットワークを使用したい すべてのクライアントに手動で配布され

る静的な共有キー（固定長の 16 進数または英数字の文字列）を使用します。

これは 8 ～ 63 文字の ASCII 文字（アルファベットと数字）で設定される必要があり、特殊文字は使用できません。

- Multiple PSK — 複数の PSK キーの入力を可能にします。最大 128 キーまで設定可能です。

  - Multiple Keys — 1 行に 1 つずつ、複数のキーを入力します。特定の MAC アドレスを持つキーを入力すると、そのキーは 1 つのクライアントで使用できるように制限されます。MAC アドレスを指定しないキーを入力すると、すべてのクライアントでキーが使用できるようになります。

    WPA-PSK、WPA2-PSK、WPA3 Personal Transition のセキュリティでは、複数のキーに対応しています。

- Dynamic PSK — RADIUS 認証サーバーによって定期的に生成・更新される動的 PSK キーの使用を可能にします。RADIUS サーバーの IP アドレス、UDP ポート、シークレットテキスト文字列を指定する必要があります。(詳細は、後述の「RADIUS 設定」を参照してください)。

  ダイナミックキーは、WPA2-PSK セキュリティにのみ対応しています。

- WPA2-PSK — 事前共有暗号鍵を持つ WPA2 を使用しているクライアントの認証を受け付けます。

  WPA は、IEEE 802.11i 無線セキュリティ規格の批准を待つ間、WEP の脆弱性に対する暫定的な解決策として導入されました。WPA のセキュリティ機能は、802.11i 規格のサブセットとなっています。WPA2 は、現在批准されている 802.11i 規格を含んでいますが、WPA との下位互換性も備えています。そのため、WPA2 には 802.1X と PSK の動作モードが同じで、TKIP 暗号化もサポートされています。

  暗号化方式とキーについては、「WPA-PSK」を参照してください。

- WPA-EAP — WPA は、複数の技術を組み合わせて、802.11 無線ネットワークのセキュリティソリューションを強化します。認証には RADIUS サーバーが使用され、アカウンティングにも使用されます。

  暗号化方式については、「WPA-PSK」を参照してください。

- RADIUS Settings — IEEE 802.1Xネットワークアクセスコントロールと Wi-Fi Protected Access（WPA）無線セキュリティを実装するには、AP に RADIUS サーバーを指定する必要があります。

また、RADIUS アカウンティングサーバーを設定して、AP からユーザーセッションアカウンティング情報を受信することができます。RADIUS アカウンティングは、ネットワーク上のユーザー活動に関する有用な情報を提供します。

注意：このガイドは、AP をサポートする RADIUS サーバーがすでに設定されていることを前提としています。RADIUS サーバーの設定については、RADIUS サーバーソフトウェアに付属のマニュアルを参照してください。

- RADIUS 認証サーバー—RADIUS 認証サーバーの IP アドレスまたはホスト名を指定します。
- Radius 認証ポート — RADIUS サーバーが認証メッセージに使用する UDP ポート番号（範囲：1024 ～ 65535、初期値：1812）。
- Radius 認証秘密鍵 — AP と RADIUS サーバー間のメッセージの暗号化に使用する共有テキスト文字列です。同じ文字列が RADIUS 認証サーバーで指定されていることを確認してください。文字列には空白を使用しないでください（最大長：255 文字）。
- NAS ID — SSID インタフェースの RADIUS NAS 識別子 この値は 1 ～ 48 文字の長さでなければなりません。
- バックアップRadius認証 — バックアップRADIUS認証サーバーのサポートを有効にします。
  - バックアップ Radius 認証サーバー — バックアップ RADIUS 認証サーバーの IP アドレスまたはホスト名を指定します。
  - バックアップ Radius 認証ポート — バックアップ RADIUS サーバーが認証メッセージに使用する UDP ポート番号（範囲：1024 ～ 65535、初期値：1812）。
  - バックアップ Radius 認証秘密鍵— AP と RADIUS サーバー間のメッセージの暗号化に使用する共有テキスト文字列です。バックアップの RADIUS 認証サーバーでも同じ文字列が指定されていることを確認してください。文字列には空白を使用しないでください（最大長：200 文字）。
- Radiusアカウンティングを使用— RADIUSアカウンティングサ ーバーのサポートを有効にします。
  - Radius アカウンティングサーバー— RADIUS アカウンティングサーバーの IP アドレスまたはホスト名を指定します。
  - Radius アカウンティングポート— RADIUS サーバーがアカウンティングメッセージに使用する UDP ポート番号です（範囲：1024 ～ 65535、初期値：1813）。

- Radius アカウンティング秘密鍵 — AP と RADIUS サーバー間のメッセージの暗号化に使用する共有テキスト文字列です。同じテキスト文字列が RADIUS アカウンティングサーバーで指定されていることを確認してください。文字列には空白を使用しないでください（最大長：200 文字）。

- Acct Interim Interval — サーバーに送信される各アカウンティング更新の間の時間 [秒] です（範囲：60 ～ 600 秒）。

- WPA2-EAP — WPA は、IEEE 802.11i 無線セキュリティ規格の批准を待つ間、WEP の脆弱性に対する暫定的な解決策として導入されました。実際、WPA のセキュリティ機能は、802.11i 規格のサブセットとなっています。WPA2 は、現在批准されている 802.11i 規格を含んでいますが、WPA との下位互換性も備えています。そのため、WPA2 には、802.1X および PSK の動作モードと、TKIP 暗号化のサポートが含まれています。

  認証には RADIUS サーバーを使用しますが、アカウンティングにも使用できます。

  暗号化方式については、「WPA-PSK」を参照してください。

  RADIUS サーバーの設定方法については、「WPA-EAP」を参照してください。

- WPA3 Personal — SAE（Simultaneous Authentication of Equals）を用いた WPA3 を使用しているクライアントは、認証を受けることができます。

  WPA3 は、WPA2-Personal の PSK（Pre-Share Key）に代わり、SAE（Simultaneous Authentication of Equals）と呼ばれる、より強固なパスワードベースの認証を提供しています。この技術により、オフラインでの辞書攻撃を防ぐことができ、データトラフィックを安全に送信することができます。

- WPA3 Personal Transition— SAE を使用した WPA3 を使用しているクライアント、または PSK を使用した WPA2 を使用しているクライアントの認証を受け付けます。AP は、ネットワークへの接続を許可する前に、サポートされている認証と暗号化を各クライアントとやり取りします。

- WPA3 Enterprise — WPA2-EAP セキュリティの強化版で、より強固な暗号化を使用します。クライアントがネットワークに接続するためには、より強力な WPA3 暗号化オプションのいずれかをサポートし、PMF（Protected Management Frames）を使用する必要があります。IEEE 802.1X ネットワークアクセスコントロールと RADIUS サーバーの使用が必要です。

  RADIUS の設定については、上記の「RADIUS の設定」を参照してください。

- WPA3 Enterprise Transition— WPA3 および WPA2 クライアントのネ ットワークへの接続を許可します。暗号化オプションや PMF（Protected Management Frames）の使用については、ネットワークへの接続を許可する前に各クライアントと交渉します。

  RADIUS の設定については、上記の「RADIUS の設定」を参照してください。

- WPA3 Enterprise 192-bit — WPA3 Enterprise のセキュリティは、標準的な 128 ビット暗号化を使用しています。より機密性の高いデータを扱うネットワークでは、さらに保護するために 192 ビット暗号化を使用するオプションがあります。

  RADIUS の設定については、上記の「RADIUS 設定」を参照してください。

- OWE — Opportunistic Wireless Encryption（OWE）は、WPA3 のオープンネットワークセキュリティで、公衆 Wi-Fi ネットワークのユーザーがパスワードを使用せずに安全なアクセスを得ることができます。OWE は、AP と各クライアント間のデータ通信を個別に暗号化しますが、ユーザー ID の認証は行いません。

- PMF — Protected Management Frames（PMF）は、AP とクライアント間のユニキャストおよびマルチキャストの管理フレームに WPA2/WPA3 のセキュリティを提供します。「Optional」の設定では、PMF をサ ポートしていないクライアントがネットワークに接続できます。「Mandatory」の設定では、PMF をサポートするクライアントのみがネ ットワークに接続できます（初期値：Optional）。

- 802.11k — ローミング時にクライアントに近隣 AP の情報を提供します。クライアントは、ある AP からローミングしようとすると、利用可能な AP のリストと関連情報を含む「ネイバーレポート」のリクエストを送信します。これにより、クライアントは、すべてのチャネルをスキャンすることなく、ローミング先の最適な AP をすばやく特定することができます（初期値：OFF）。

- 802.11r — AP 間のローミングを高速に遷移させる方法を提供します。クライアントが新しい AP にローミングする前に、最初のハンドシェイ クと暗号化の計算が事前に行われるため これにより、再認証を必要としない高速なハンドオフが可能になります（初期値：OFF）。

- 802.11v — 関連するクライアントに、ワイヤレスネットワーク全体の改善を促進する情報を提供します。また、アイドル時間を設定することで、クライアントのバッテリー寿命の向上にも貢献します。(初期値：無効)

- Radius MAC 認証 — アソシエイトステーションの MAC アドレスを、設定した RADIUS サーバーに送信して認証を行います（初期値：OFF）。

- ダイナミック認証 — RADIUS の Dynamic Authorization Extensions（DAE）は、ネットワークにすでに接続されているクライアントの認証をサーバーが切断または変更できるようにするものです（初期値：OFF）。
  - DAE ポート — DAE メッセージに使用する UDP ポート番号です（初期値：3799）。
  - DAE クライアント — RADIUS サーバーの IPv4 アドレスを指定します。
  - DAE シークレット — AP と RADIUS サーバー間の DAE メッセージの暗号化に使用される共有テキスト文字列。
- アクセスコントロールリスト — 無線クライアントの MAC アドレスを、AP に設定されたローカルデータベースと照合して、ネットワーク接続の認証を行うことができます（初期値：OFF）。
  - ポリシー — MAC リストは、指定したクライアントのネットワーク接続を許可するか拒否するかを設定できます（初期値：リスト上の全ての MAC を許可）。
  - Filtered MACs — クライアントの MAC アドレスの一覧。MAC アドレスは最大 512 個まで設定可能。

無線ネットワーク — ネットワーク設定

図 46: 無線ネットワーク設定

「無線設定」ページこのセクションには、以下の項目が表示されます。

- ネットワークモード — 以下のいずれかの接続方法を指定する必要があります（初期値：ルーターモード）。
  - ブリッジモード — WAN に接続されたインターフェースを設定します。このインターフェースからのトラフィックは、インターネットに直接ブリッジされます（Figure 29, “ ブリッジモード ", on page 45 参照）。
  - ルーターモード — LAN のメンバーとしてインターフェースを設定します。このインターフェースからのトラフィックは、AP を経由して、インターネットにブリッジされているインターフェースを経由して

ルーティングされます（ Figure 30, “ ルーターモード ", on page 46 参照）。

- ネットワーク名 — ルーティングするネットワークです。初期値は、「LAN 設定」—「ローカルネットワーク」で表示される「デフォルトローカルネットワーク」です。

- Add to Guest Network — このインターフェイスは、ゲストネットワークにのみ対応できます。

- Hotspot Controlled — このインターフェースは、ホットスポット・サービスのみをサポートすることができます。

  - Configure Hotspot - Hotspot Settings ページを開きます。

  - Walled Garden — ホットスポット設定」ページの「Walled Garden」リストを設定します。

- VLAN タグトラフィック — この VAP（仮想 AP）から関連するイーサネットポートに通過するすべてのパケットに、81 ページの「VLAN 設定」で設定した VLAN Id をタグ付けします。

  - VLAN Id — VAP にトラフィックをタグ付けするために設定された VLAN Id を選択します。

  - VLAN 設定 — VLAN の設定ページを開きます。

- Dynamic VLAN — RADIUS サーバーは、AP にユーザー VLAN 情報を提供します。AP は、関連するユーザーを関連する VLAN に割り当 てます。

  - Default VLAN Behavior — クライアントの VLAN ID が RADIUS サーバーで定義されていない場合の動作（Accept または Reject）を指定します。デフォルトの設定は Reject です。

    - Reject — クライアントの VLAN ID が RADIUS サーバーで定義されていない場合、クライアントは SSID に接続することができません。

    - Accept — クライアントの VLAN ID が RADIUS サーバーで定義されていない場合、クライアントは割り当てられたまたはタグなし VLAN ID で SSID に接続することができます。

- CAPWAP トンネルインターフェース — AP のシステム管理が EWS-Series Controller モードに設定されている場合（ 84 ページの「システム設定」を参照）、CAPWAP （Control And Provisioning of Wireless Access Points）プロトコルのトンネルモードを設定することができます。オプションは、"Disable"、"Complete"、"Split " のいずれかです。Complete トンネルは、AP からのすべての管理、認証、およびデータトラフィックをコントローラーに送り返します。スプリットトンネルは、

管理と認証のトラフィックのみをコントローラーに送信します（初期値：無効）。

- Proxy ARP — Proxy ARP が有効な場合、AP は独自の ARP ルックアップテーブルを維持し、下流局の代わりに ARP リクエストに返信するため、ネットワークの非効率性を回避することができます。この機能は、クライアント分離が無効の場合は自動的に有効になり、クライアント分離が有効の場合は無効になります。この機能は、手動で設定することはできません。Proxy ARP は、ネットワーク動作が "Bridge to Internet " または "VLAN Tag Traffic " の場合にサポートされます。

- Limit Upload — VAP インターフェースから有線ネットワークに渡されるトラフィックのレート制限を有効にします。最大レートは Kbytes per second で設定できます。(範囲：256 ～ 10048576K バイト / 秒、初期値：OFF)。

- Limit Download — 有線ネットワークからVAPインターフェースに渡されるトラフィックのレート制限を有効にします。最大レートは kbyte/sec で設定可能です。(範囲：256 ～ 10048576K バイト / 秒、初期値：OFF)。

- 認証 — AP のシステム管理が ecCLOUD モードに設定されている場合（84 ページの「システム設定」を参照)、このオプションは ecCLOUD コントローラーとの AP 通信を認証します（初期値：OFF)。

無線ネットワーク — OpenRoaming

WPA2-EAP セキュリティが選択されている場合に利用可能な OpenRoaming (Hotspot 2.0) は、無線ネットワーク間のシームレスなローミングをサポートする公衆アクセス Wi-Fi ネットワークの標準を提供します。OpenRoaming AP は、クライアントがネットワークに接続するかどうかを決定できるように、そのパブリック Wi-Fi 機能とサービスをアドバタイズします。

図 47: OpenRoaming 設定

無線設定ページのこのセクションには、以下の項目が表示されます：

- OpenRoaming — WPA2-EAPセキュリティ選択時にOpenRoamingを有効化。

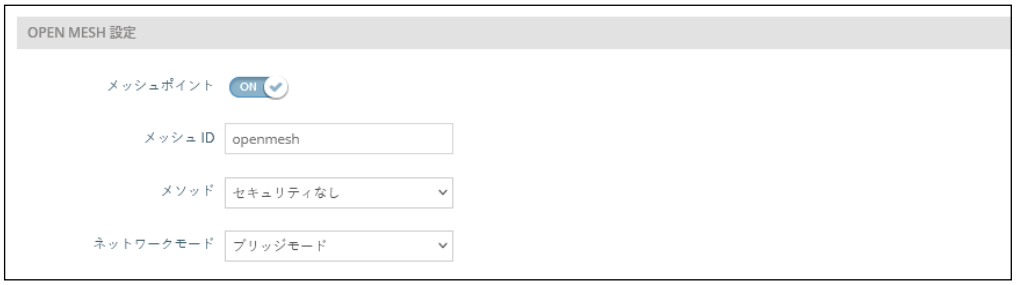
- OpenRoaming プロファイル — ワイヤレスネットワークに適用するプロファイルを選択します。プロファイルの設定については、56 ページの「OpenRoaming」を参照してください。
- OpenRoaming 設定 — OpenRoaming プロファイル設定ページにアクセスします。プロファイルの設定については、56 ページの「OpenRoaming」を参照してください。

無線ネットワーク — Open Mesh Settings

オープンメッシュは、相互に接続されたノード AP のネットワークで、そのうち 1 台だけがネットワーク（およびインターネット）に有線で接続されています。他のノード AP は、相互に無線リンクを提供し、一部は無線クライアントへの接続をサポートします。メッシュネットワークは、無線接続をより遠くまで拡張するだけでなく、ネットワーク内の 1 つのノードが故障した場合にバックアップリンクを提供します。

メッシュネットワークのノードとなる AP を設定する場合は、1 つの無線インターフェース（2.4 GHz, 5 GHz）を選択し、特定のチャネルで動作するように設定します（「自動」は選択しないでください）。他の AP ノードが同じ無線インターフェース、チャネル、同じ SSID で動作するように設定します。

図 48: Open Mesh 設定



無線設定ページのこのセクションには、以下の項目が表示されます。

- Mesh Point— SSID インターフェースの Open Mesh サポートを有効にします。
- メッシュ ID — メッシュネットワークの名前。
- 方式 — Open Mesh リンクに適用されるセキュリティ。
  - No Securiy— セキュリティなし
  - WPA3 Personal— 他の AP とのメッシュリンクでは、WPA3 と SAE（Simultaneous Authentication of Equals）を使用。
- ネットワーク動作 - 以下の接続方法のいずれかを指定する必要があります。(初期値：インターネットへのルート)。

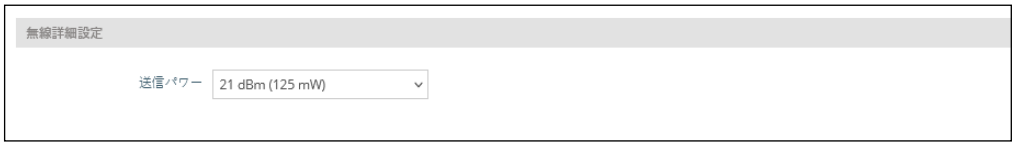
- Bridge to Internet - WAN に接続されているインターフェイスを構成します。このインターフェイスからのトラフィックは、インターネットに直接ブリッジされます。(45 ページの図 29「Bridge to Internet」を参照)。

- Route to Internet — LAN のメンバーとしてインターフェイスを設定します。このインターフェイスからのトラフィックは、アクセスポイントを横切って、インターネットにブリッジされたインターフェイスを経由して外に出るようにルーティングされます。(46 ページの図 30「インターネットへのルート」を参照してください)。

  - ネットワーク名 — ルーティングの対象となるネットワークです。デフォルトは、「LAN 設定」-「ローカルネットワーク」で表示される「デフォルトのローカルネットワーク」です。

無線ネットワーク — 無線詳細設定

図 49: 無線詳細設定



無線設定ページこのセクションには、以下の項目が表示されます。

- 送信パワー — AP から送信される無線信号のパワーを調整します。送信パワーが大きいほど、送信範囲が広くなります。パワーの選択は、単にカバーエリアとサポートする最大クライアント数のトレードオフだけではありません。高出力の信号がサービスエリア内の他の無線機器の動作を妨害しないようにする必要もあります（電力設定の範囲と初期値は、AP のモデルと国の設定によって異なります)。

- SGI — 次の 802.11 モードでショートガード間隔（SGI）を有効にします：5 GHz 無線、802.11a、802.11a+ n、802.11ac+a+n。
  2.4 GHz ラジオ：802.11 b g+ n。

  802.11n ドラフトでは、2 つのガードインターバルが規定されています。400ns (short) と 800ns (long) です。400ns の短いガードインターバルのサポートは、送信と受信のためにオプションです。ガードインターバルの目的は、デジタルデータが通常非常に敏感である伝搬遅延、エコー、反射に対する耐性を導入することです。SGI を有効にすると、400ns に設定されます。(デフォルト：無効)

VLAN 設定

VLAN（仮想ローカルエリアネットワーク）は、初期設定ではオフになっています。VLAN をオンにすると、該当する VAP（仮想 AP）から LAN ポートに渡されるパケットに自動的にタグが付けられます。

AP は、VLAN タグを使用してネットワークリソースへのアクセスを制御し、セキュリティを高めることができます。VLAN は、AP、関連するクライアント、および有線ネットワークの間を通過するトラフィックを分離します。最大 16 の VLAN タグ付きネットワークを作成できます。

AP の VLAN 対応については、以下の点に注意してください。

- AP のイーサネット LAN ポートに VLAN ID が割り当てられている場合、そのポートに入るトラフィックは同じ VLAN ID でタグ付けされている必要があります。

- AP に接続されている無線クライアントは、VLAN に割り当てられます。無線クライアントは、自分が関連付けられている VAP インターフェースの VLAN に割り当てられます。AP は、正しい VLAN ID でタグ付けされたトラフィックのみを、各 VAP インターフェースの関連クライアントに転送することができます。

- AP で VLAN サポートが有効になっている場合、有線ネットワークに渡されるトラフィックには、適切な VLAN ID がタグ付けされます。AP のイーサネットポートが VLAN メンバーとして設定されている場合、有線ネットワークから受信するトラフィックも同じ VLAN ID でタグ付けされている必要があります。不明な VLAN ID や VLAN タグを持たない受信トラフィックは破棄されます。

- VLAN サポートが無効の場合、AP は有線ネットワークに渡すトラフィックにタグを付けず、受信フレームの VLAN タグを無視します。

- ネットワーク IP 範囲の衝突の検出および解決 — AP には、「メイン」ネットワークと、より安全な「ゲスト」ネットワークの 2 つがローカルネットワークとして組み込まれています。初期設定では、これらのネットワークのサブネット範囲は、それぞれ 192.168.2.1 と 192.168.3.1 に設定されています。

  ネットワークがすでにこれらのサブネットのいずれかを使用するように設定されている場合、ネットワークケーブルを AP の WAN ポートに接続すると、通常はローカル AP のネットワークと上流のネットワークで IP の競合が発生します。

  しかし、WAN サブネットがいずれかのローカルネットワーク（あなたが作成したカスタムネットワークも含む）と衝突した場合、AP は自動的にローカルネットワークのサブネットを変更します。

注意：AP で VLAN タグを有効にする前に、接続しているネットワークスイッ チのポートを、AP で設定した VLAN ID のタグ付き VLAN フレームをサポ ートするように設定してください。そうしないと、VLAN 機能を有効にした ときに、AP への接続性が失われてしまいます。

図 50: 無線 VLAN 設定

このページには以下の項目が表示されます。

- VLAN ID — 割り当てる VLAN 識別子（範囲：2 ～ 4094）。（VLAN1 は内部用に予約されています。）
- ポート — 指定の VLAN に割り当てられるイーサネットポート。
- メンバー — 指定された VLAN のメンバーとして構成された VAP の SSID。このオプションは、「無線設定」-「ネットワーク設定」-「ネットワー クモード」で設定します。

5 システム設定

本章では、AP のメンテナンス設定について説明します。

以下の内容が含まれています。

システム設定

「システム設定」ページは、Edgecore ecCLOUD コントローラーや EWS-Series コントローラーから AP を管理できるようにしたり、AP に関する一般的な記述情報を設定するために使用できます。

図 51: システム設定

このページには以下の項目が表示されます。

- 管理 — Edgecore ecCLOUD コントローラーからこの AP を管理するには、「ecCLOUD」に設定します。また、「EWS-Series Controller」に設定すると、ローカルネットワークの Edgecore EWS-Series コントローラーからこの AP を管理することができます。スタンドアロンモードでウェブインターフェースを介して AP を管理するには、「無効」に設定します。
  - ecCLOUD — 選択すると、以下のパラメータが表示されます。
    - コントローラー URL — Edgecore ecCLOUD コントローラー管理サイトへの URL リンクを提供します。
    - Enable agent — ecCLOUD コントローラーから AP を管理できるようにします。
      - 登録 URL — デバイス登録用の URL を指定します。
    - Log Level — ecCLOUD デーモン（mgmtd）のシステムログレベルを調整します。デフォルト値は Info です。ログレベルの標準的

な順位は、次のとおりです：Trace < Debug < Info < Warn < Error.

- EWS-Series Controller — 選択すると、以下のパラメータが表示されます。
  - CAPWAP — CAPWAP（Control And Provisioning of Wireless Access Points）プロトコルトンネルモードを有効にします。
  - DNS サーバーによる探索 — AP は、DNS サーバーレコードを使用して、CAPWAP ジョインリクエストを送ることができる EWS コントローラーを発見します。
    - Domain Name Suffix - コントローラのドメインサフィックスを指定します。
  - DHCP オプションによる探索 — AP は DHCP サーバーを使用して EWS コントローラーと同じサブネット内の IP アドレスを取得し、CAPWAP ジョインリクエストを送信することができます。
  - ブロードキャストによる探索 — AP はブロードキャストリクエストを送信し、同じサブネット内の EWS コントローラーを検出します。
  - マルチキャストによる探索 — AP は、EWS コントローラーを見つけるために、ネットワーク上でマルチキャストディスカバリー パケットを送信します。このオプションは、ネットワークにルーティングパスが適切に設定されている必要があります。
  - 手動設定による探索 — AP が CAPWAP ジョインリクエストを送信する際に使用する IP アドレスを入力することで、EWS コントロー ラーに手動で到達する方法を提供します。
- Syslog Level — 重大度に基づいてシステムログメッセージを制限します。ログレベルの標準的な順位は以下の通りです：Debug < Info < Notice < Warning < Error < Critical < Alert < Emergency. (デフォルト : Info)
- ホスト名 — AP のエイリアスで、ネットワーク上でデバイスを一意に識別できるようにします（初期値：EAP101、範囲：1-63 ASCII 文字。A-Z、a-z、0-9、ダッシュ "-" のみ使用可能)。
- Enable Reset Button - AP のハードウェアリセットボタンを有効にします。(デフォルト : Enabled)
- 時刻 — 曜日、月、日、時間、年を指定します。
- ブート再試行の回数 — 次のブートバンクに切り替えるまでのブートアップ再試行の最大回数（初期値：3、範囲：1 〜 254)。

- MSP モード — エンドユーザーがユーザー定義のユーザーアカウントからほとんどのデバイス設定にアクセスし、変更することを防止するマネージドサービスプロバイダー（MSP）モードを有効にすることができます。root と admin アカウントからの管理アクセスは、すべてのデバイス設定へのフルアクセスを提供します。(初期値：無効)

  MSP モードを有効にすると、サービスプロバイダーは、「ローカル設定可能」設定を有効にすることで、特定の無線 SSID 設定をユーザー設定に利用できるようにするオプションがあります。の「ワイヤレスネットワーク - 一般設定」を参照してください。69 ページの「無線ネットワーク — 一般設定」を参照。

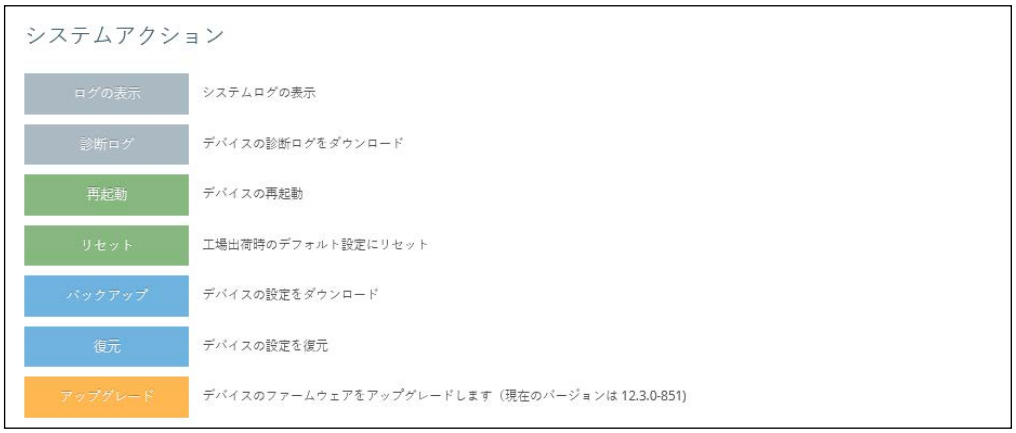
- LED を有効にする - AP の LED インジケータを有効にします。(デフォルト : Enabled)

- 言語 — Web インターフェイスの言語を選択します。(オプション：英語と日本語・デフォルト：英語)

メンテナンス

「メンテナンス」ページでは、システムログの表示、診断ログのダウンロード、デバイスの再起動、工場出荷時の設定にリセット、構成設定のバックア ップまたは復元、ファームウェアのアップグレードなど、一般的なメンテナ ンス作業を行うことができます。

図 52: メンテナンス



システムログの表示

AP は、イベントやエラーのメッセージをローカルのシステムログデータベースに保存しています。ログメッセージには、日付と時刻、デバイス名、メッセージタイプ、メッセージの詳細が含まれます。

図 53: システムログ

診断ログのダウンロード

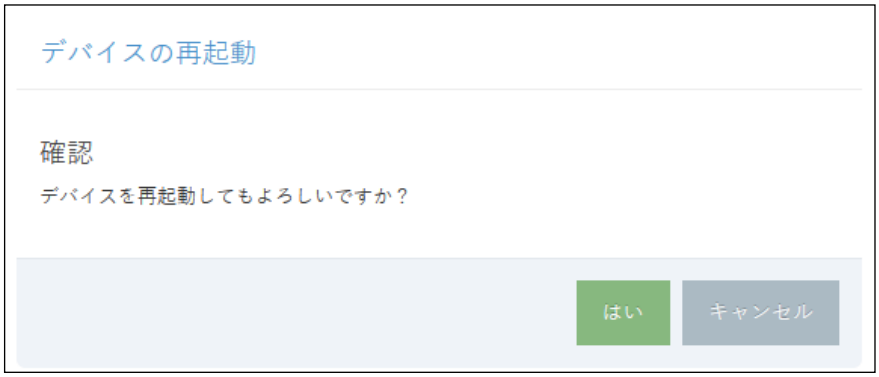
「診断ログ」をクリックすると、ログファイルが管理ワークステーションにダウンロードされます。Windows では、GNU Zip （*.tar.gz）ファイルがダウンロードフォルダーに保存されます。

診断ログファイルには、Edgecore 社が AP の技術的問題を解決するのに役立つ情報が含まれています。

AP の再起動

「再起動」ページでは、AP を再起動することができます。

図 54: AP の再起動



APのリセット

「リセット」ページでは、APを工場出荷時の設定にリセットすることができます。ただし、ユーザーが設定した情報はすべて失われます。このデバイスへの管理アクセスを再開するには、初期設定のユーザー名とパスワードを再度入力する必要があります。

図 55: 初期状態へのリセット

注意：APのコネクターパネルにある「Restart / Reset」と書かれたピンホールにピンを差し込んで、APを再起動またはリセットすることも可能です。

- 素早く押すと、APが再起動します。
- 5秒間押し続けると、APを工場出荷時の状態にリセットすることができます。

設定内容のバックアップ

バックアップ機能を使うと、APの設定を管理用のワークステーションにバックアップすることができます。Windowsでは、ダウンロードフォルダーにGNU Zip（*.tar.gz）ファイルが格納されます。ファイル名は次のようになります。
backup-EAP101-2021-02-09.tar.gz

設定内容の復元

「復元」ページでは、管理ワークステーションから設定ファイルをアップロードすることができます。指定するファイルは、以前に AP からバックアップされたものでなければなりません。

図 56: 設定内容の復元

ファームウェアアップグレード

新しい AP のソフトウェアは、管理ワークステーションのローカルファイルからアップグレードすることができます。新しいソフトウェアは、Edgecore 社から定期的に提供されます。

新しいソフトウェアをアップグレードした後は、新しいコードを実装するために AP を再起動する必要があります。再起動が行われるまでは、AP はアップグレード開始前に使用していたソフトウェアを実行し続けます。AP はデュアルソフトウェアイメージをサポートしているため、新しくロードされたソフトウェアが破損した場合は、次回の再起動時に代替イメージが使用されます。設定内容はソフトウェアとは別に保存されるため、新しいソフトウェアでは常に現在の設定内容が適用されます。ただし、現在の設定が破損している場合は、システムの初期設定が適用されますのでご注意ください。

注意：アップロードされたファームウェアが現在のバージョンより古い場合、デバイスは「アップグレード後も現在の設定を維持する」オプションのチェックを強制的に外します。

図 57: ファームウェアアップグレード

証明書をアップロードする

証明書のアップロード」ページでは、設定された HTTPS キャプティブポータルへのセキュアなアクセス（暗号化された接続）のために、信頼できる認証局から固有のセキュリティ証明書をアップロードすることができます。または、リセットしてデフォルトの証明書を使用することもできます。

図 58: 証明書をアップロードする

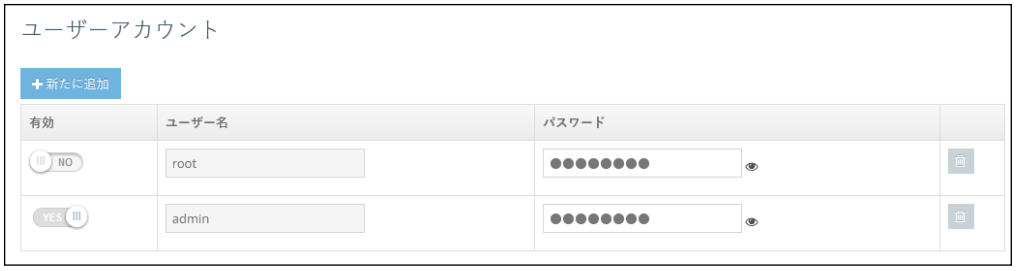
本ページでは、次の項目が表示されます。

- 証明書のアップロード - クリックすると、信頼できる認証局からセキュリティ証明書と秘密鍵をアップロードします。
- Use Default Certificate - クリックすると、AP のデフォルト証明書を使用するようにリセットされます。

ユーザーアカウント

「ユーザーアカウント」のページでは、手動で設定したユーザー名とパスワードに基づいて、AP への管理アクセスを制御することができます。

図 59: ユーザーアカウント



このページには以下の項目が表示されます。

- 有効 — クリックすると、ユーザーアカウントの有効 / 無効を切り替えます。
- ユーザー名 — ユーザーの名前です（範囲：1-32 ASCII 文字。A-Z、a-z、0-9、ピリオド "."、アンダースコア "_"、ハイフン "-" のみ使用可能。ユーザー名はハイフン "-" またはピリオド ". " で始まることはできません）。
- パスワード — ユーザーのパスワードです(範囲:6 ～ 20 文字の ASCII 文字で、大文字と小文字は区別し、特殊文字は使用しないでください)。

サービス

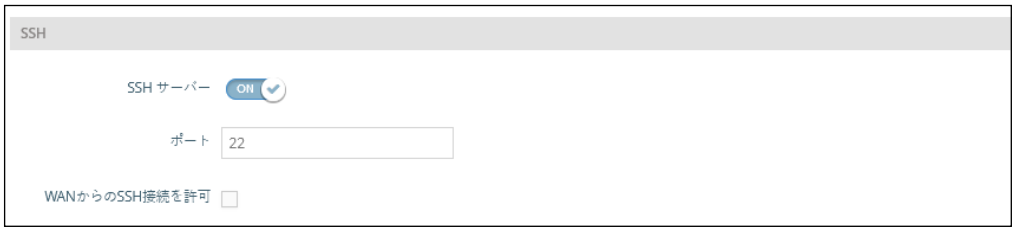
「サービス」ページでは、AP への SSH 接続の制御、NTP タイムサーバーの設定、iBeacon の設定を行うことができます。

SSH

セキュアシェル（SSH）は、Telnet に代わる安全な手段として機能します。SSH プロトコルは、生成された公開鍵を使用して、AP と SSH 対応の管理ステーションクライアントとの間で行われるすべてのデータ転送を暗号化し、ネットワーク上を移動するデータが改ざんされずに届くことを保証します。クライアントは、ローカルのユーザー名とパスワードを使って安全に接続認証を行うことができます。

なお、SSH プロトコルで AP を管理するためには、管理ステーションに SSH クライアントソフトウェアをインストールする必要があります。

図 60: SSH 設定



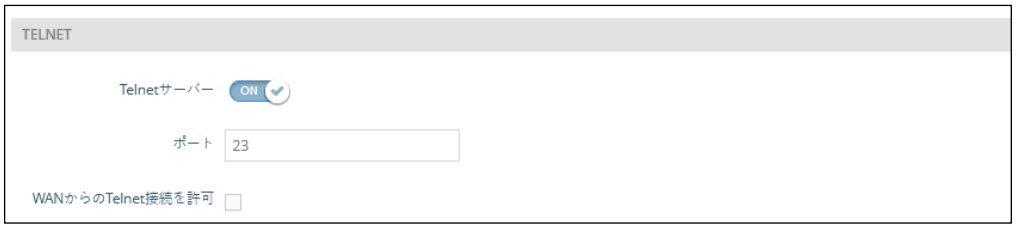
このページには以下の項目が表示されます。

- SSH サーバー — AP への SSH 接続を有効または無効にします（初期値：ON）。
- ポート — AP の SSH サーバーの TCP ポート番号を設定します（範囲：1 ～ 65535、初期値：22）。
- WAN から SSH への接続を許可 — WAN からの SSH 管理接続を許可します。

Telnet

Telnet は、ネットワーク上のどこからでもアクセスポイントの設定を行うことができるリモート管理ツールです。ただし、Telnet は敵対的な攻撃から安全でないことに注意してください。

図 61: Telnet サーバー設定



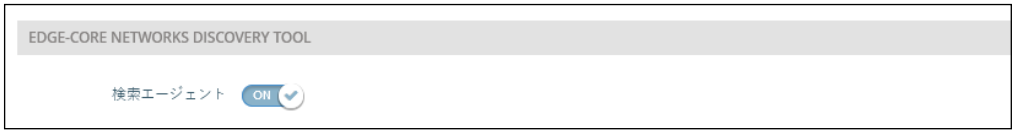
本ページでは、次の項目が表示されます。

- Telnet サーバー — アクセスポイントへの Telnet アクセスの有効／無効を設定します。（初期値：有効）
- ポート — アクセスポイントの Telnet サーバーの TCP ポート番号を設定します。（範囲：1 ～ 65535、初期値：23）
- Allow Telnet from WAN — WAN からの Telnet による管理アクセスを許可します。

Edgecore Networks ディスカバリーツール

Discovery Tool エージェントは、AP が同じレイヤー 2 ネットワーク内の他の Edgecore デバイスを見つけることができるようにします。ネットワークをスキャンしてデバイスを探すには、102 ページの「デバイス・ディスカバリー」を参照してください。

図 62: ディスカバリーエージェント設定



本ページは以下の項目を表示します：

- ディスカバリーエージェント — ディスカバリーエージェントを有効にします。(初期値 : 有効)
- Allow over WAN — インターネットソースに接続されたポート上でディスカバリーエージェントを動作させることを有効にします。(デフォルト : 有効)

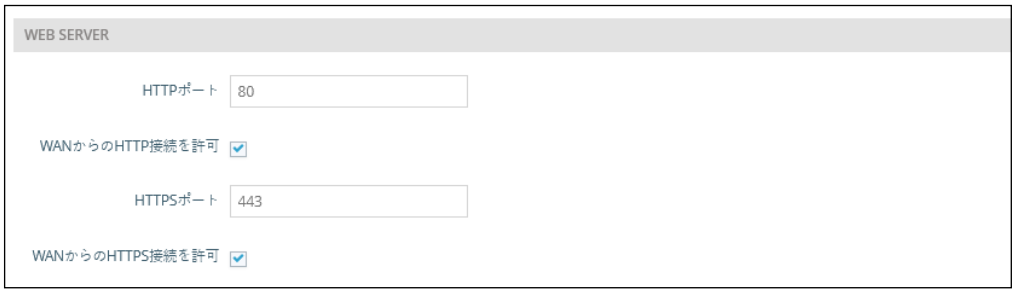
ウェブサーバー

Web ブラウザは、アクセスポイントを管理する主要な方法を提供します。HTTP と HTTPS の両方のサービスに独立してアクセスすることができます。HTTPS を有効にする場合は、URL でその旨を示す必要があります：https://device:port_number]。

HTTPS を起動すると、このように接続が確立されます。

- クライアントは、サーバーのデジタル証明書を使用してサーバーを認証する。
- クライアントとサーバーは、接続に使用する一連のセキュリティプロトコルをネゴシエートします。
- クライアントとサーバーは、データを暗号化・復号化するためのセッションキーを生成します。
- クライアントとサーバーは、安全な暗号化された接続を確立します。
- ほとんどのブラウザのステータスバーに南京錠のアイコンが表示されるはずです。

図 63: ウェブサーバー設定



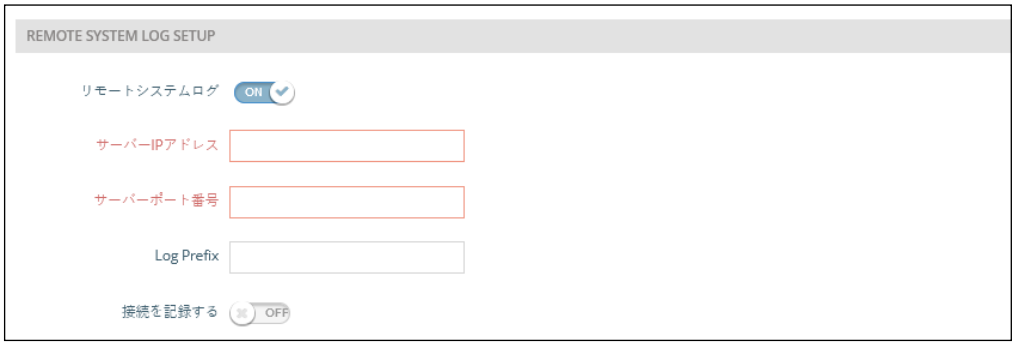
本ページは以下の項目を表示します：

- HTTP ポート — HTTP Web ブラウザーのインターフェイスで使用する TCP ポートです。(範囲：1 ～ 65535、デフォルト：80)
- Allow HTTP from WAN — WAN からの HTTP 管理アクセスを可能にします。
- HTTPS ポート — HTTPS Web ブラウザーのインターフェースで使用される TCP ポートです。(範囲：1 ～ 65535、デフォルト：443)。
- Allow HTTPS from WAN — WAN からの HTTPS 管理アクセスを許可します。

Remote System Log Setup

この機能を使って、シスログサーバーにログメッセージを送信します。

図 64: リモートシステムログ設定



このページには以下の項目が表示されます。

- Remote Syslog — デバッグメッセージやエラーメッセージをリモート ロギングプロセスに記録することを有効にします（初期値：OFF)。
- Server IP — ログメッセージを送信するリモートシスログサーバーの IP アドレスを指定します。

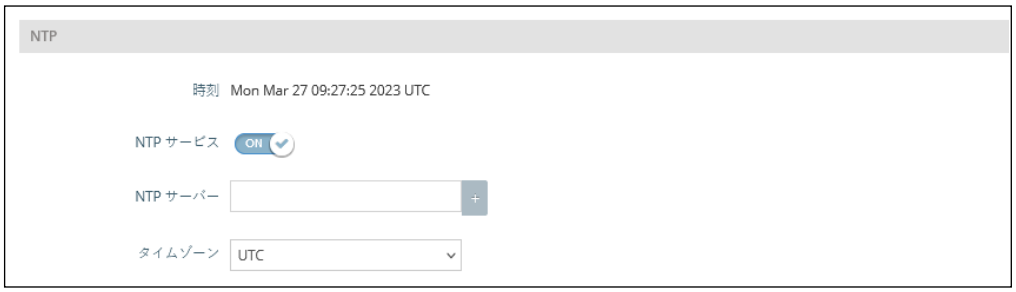
- Server Port — リモートシスログサーバーが使用する UDP ポート番号を指定します（範囲：1 ～ 65535）。
- Log Prefix — 指定されたサーバーに送信されるログメッセージのプレフィックス文字列を設定します。プレフィックスは、サーバー上でのメッセージの並び替えに役立ちます。
- Track Connections — ログメッセージに、送信元 IP とポート、送信先 IP とポートなどの接続情報を含めることを可能にします。

NTP

ネットワークタイムプロトコル（NTP）は、タイムサーバー（SNTP または NTP）からの定期的な更新に基づいて、AP が内部時計を設定することを可能にします。AP の正確な時刻を維持することで、システムログにイベントエントリの意味のある日付と時刻を記録することができます。時計が設定されていない場合、AP は前回の起動時に設定された工場出荷時の時間のみを記録します。

AP は、NTP クライアントとして動作し、指定されたタイムサーバーに定期的に時刻同期要求を送信します。AP は、設定された順序で各サーバーをポーリングして、時刻の更新を受信しようとします。

図 65: NTP 設定



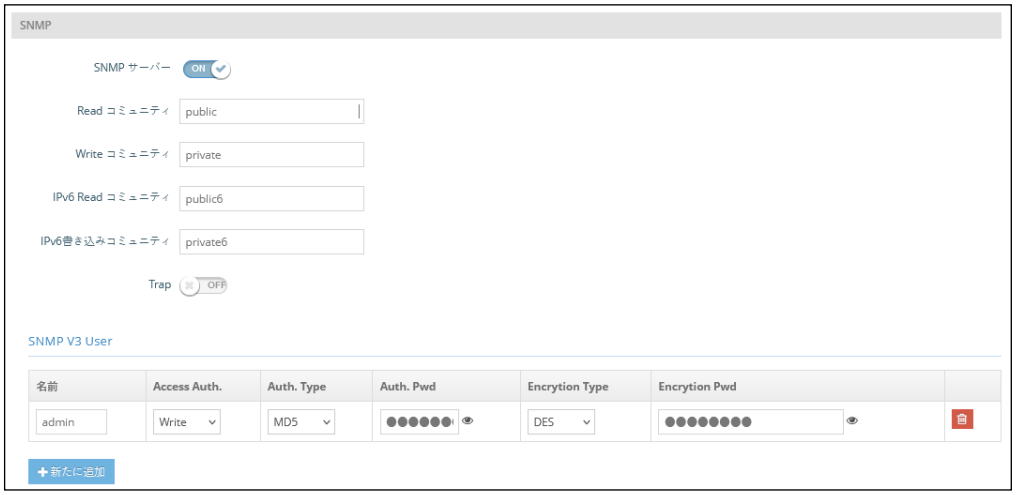
このページには以下の項目が表示されます。

- 時刻 — 世界標準時を基準とした、曜日、月、日、時：分：秒、年の現地時間を表示します
- NTP サービス — 時刻の更新要求の送信を有効または無効にします（初期値：有効）。
- NTP サーバー — タイムサーバーのホスト名を設定します。スイッチは最初のサーバーから時刻の更新を試み、失敗した場合は順番に次のサーバーから更新を試みます。追加のサーバーを設定するには、「+」ボタンを クリックして新しい編集フィールドを開きます。
- タイムゾーン — 現地時間に対応した時間を表示するには、スクロールダウンリストから定義済みのタイムゾーンを選択します。

SNMP

SNMP（Simple Network Management Protocol）は、ネットワーク上の機器を管理するために開発された通信プロトコルです。一般的には、ネットワーク環境で適切に動作するように機器を設定したり、性能評価や潜在的な問題を検出するために機器を監視したりするのに使用されます。

図 66: SNMP 設定



このページには以下の項目が表示されます

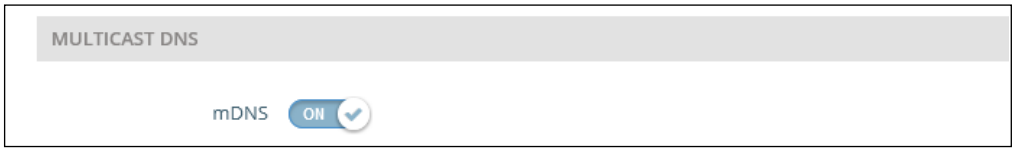
- SNMP Server — AP の SNMP を有効または無効にします（初期値：ON）。
- Read Community — パスワードのように動作し、アクセスポイントの管理情報ベース（MIB）への読み取りアクセスを許可するコミュニティ文字列です。（範囲：1 ～ 32 文字、大文字と小文字を区別する、デフォルト：パブリック）
- Write Community — AP の MIB（Management Information Base）への書き込みアクセスを許可する、パスワードのような役割を持つコミュニティ文字列（範囲：1 ～ 32 文字、大文字小文字の区別あり、初期値：private）
- IPv6 Read Community — アクセスポイントの管理情報（MIB）データベースへの IPv6 読み取りアクセス用のコミュニティ文字列です。（範囲：1 ～ 32 文字、大文字と小文字を区別する、デフォルト：public6）。
- IPv6 Write Community — アクセスポイントの管理情報（MIB）データベースへの IPv6 書き込みアクセス用のコミュニティ文字列です。（範囲：1 ～ 32 文字、大文字と小文字を区別する。デフォルト：private6）

- Trap — 指定したサーバーへの SNMP トラップメッセージの送信を有効にします。アクセスポイントでは、コールドスタート、ウォームスタート、リンクアップ、リンクダウンのトラップメッセージを送信します。(初期値：無効)
  - サーバー IP — トラップメッセージを送信する SNMP トラップサーバーの IP アドレスを指定します。
- SNMPv3 ユーザー — SNMP プロトコルバージョン 3 は、アカウント認証とデータ暗号化によって安全なアクセスを提供します。SNMP v3 ユーザーは、「新規追加」ボタンをクリックすることで定義することができます。
  - 名前 — SNMP サービスにアクセスするために使用されるユーザー名。
  - Access Auth — アクセス許可を "Read" または "Write" として選択します。
  - Auth Type — 認証のためのハッシュアルゴリズムを選択します。
  - Auth Pwd — 認証用のパスワードを設定します。
  - Encryption Type — データパケットの暗号化アルゴリズムを選択します。
  - Encryption Pwd — データ暗号化用のパスワードを設定します。

マルチキャスト DNS

マルチキャスト DNS（mDNS）プロトコルは、ローカルネットワーク内の接続を容易にするためのゼロコンフィギュレーションサービスです。

図 67: マルチキャスト DNS 設定



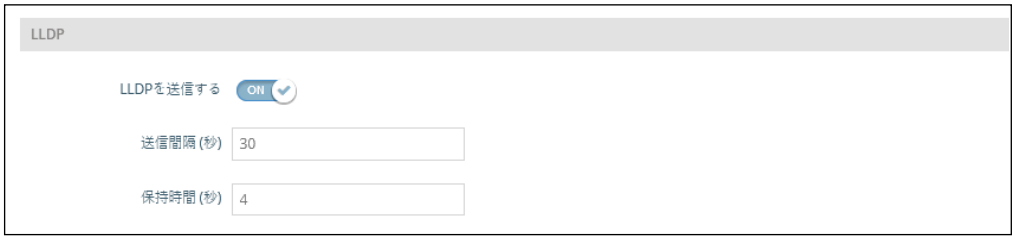
本ページは以下の項目を表示します：

- mDNS — アクセスポイントでのマルチキャスト DNS の有効／無効を設定します。(初期値：Enabled)

LLDP

LLDP（Link Layer Discovery Protocol）は、ネットワーク上で隣接する機器の基本情報を発見するためのプロトコルです。LLDP は、定期的なブロードキ ャストを用いて、送信側の機器の情報を発信するレイヤ 2 プロトコルです。

図 68: LLDP 設定



このページには以下の項目が表示されます。

- Send LLDP — ネットワーク内の近隣の機器にAPに関するLLDP広告を送信することを有効にします（初期値 :OFF）。
- Tx Interval （seconds）— LLDP アドバタイズメントの定期的な送信間隔を設定します（範囲：5 ～ 32768 秒、初期値：30 秒）。
- Tx Hold （time(s)）— LLDP アドバタイズメントで送信される TTL（time-to-live）値を以下の式のように設定します（範囲：2 ～ 10、初期値：4）。

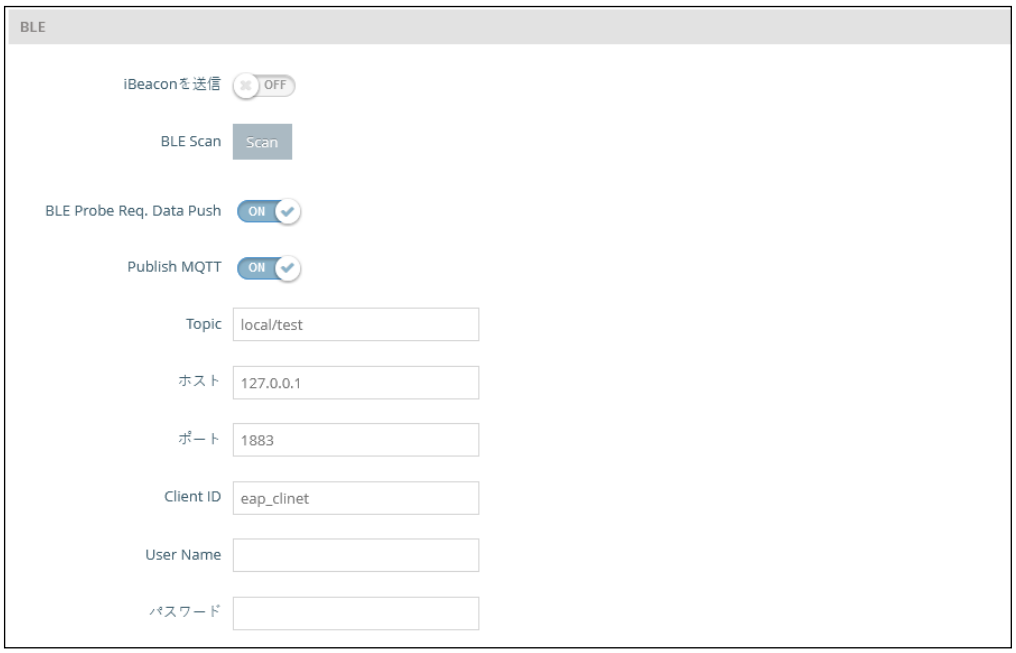
  TTL は、受信側の LLDP エージェントに、送信側のデバイスがタイムリー にアップデートを送信しなかった場合に、そのデバイスに関連するすべ ての情報をどのくらいの期間保持するかを伝えます。

  TTL[秒] は、以下のルールに基づいて設定されます。
  最小値 （(Tx Interval * Tx Hold)、または 65535）したがって、初期値の TTL は 4*30 = 120 秒となります。

BLE

AP は、Bluetooth Low Energy（BLE）をベースにした iBeacon 規格に対応しています。BLE ビーコンを搭載した機器は、ビーコン信号を認識し、提供された情報を抽出します。その内容に基づいて、対応機器（電話など）の BLE クライアントに、位置情報サービスを提供することができます。

図 69: BLE 設定



このページには以下の項目が表示されます。

- iBeacon を送信 — AP の iBeacon サポートを有効にします（初期値：ON）。
- UUID — ビーコンサービスを発信する iBeacon の Universally Unique Identifier。UUID は、ハイフンで区切られた 5 つのグループの 16 進数 32 桁で構成されています。
- Major — ビーコングループの識別に使用される iBeacon の値（範囲：0 ～ 65535）。
- Minor — グループ内の個々のビーコンを識別するために使用される iBeacon の値（範囲：0 ～ 65535）。
- Tx Power — BLE 無線送信電力を設定します（EAP101、EAP104 のみ対応）。(範囲：5dBm ～ -20dBm、初期値：5dBm)。
- BLE Scan — (EAP101 および EAP104 のみ) 以下の 4 つのタイプを含む、すべての BLE デバイスをスキャンします : EddyStone-UID、EddyStone-URL、EddyStone-TLM、ibeacon。

図 70: BLE Scan

- BLE Probe Req. Data Push — デバイスの BLE プローブ要求データプッシュを有効にします。(EAP112 のみ)
- Publish MQTT — プッシュされたデータを MQTT（Message Queuing Telemetry Transport）メッセージとして発行します。(EAP112 のみ)
  - トピック — MQTT メッセージ・トピック名
  - ホスト — MQTT サーバー / ブローカーの IP アドレス
  - ポート — TCP ポートナンバー
  - クライアント ID — このクライアント・デバイスの識別子
  - ユーザー名 — クライアントのユーザー名
  - パスワード — クライアントのパスワード

診断

Diagnostics ページには、接続の問題をトラブルシューティングするための Ping、Traceroute、Nslookup、および Speed Test ツールが用意されています。

Ping ホスト名または IP アドレスを入力し、クリックすると Ping ツールが実行されます。

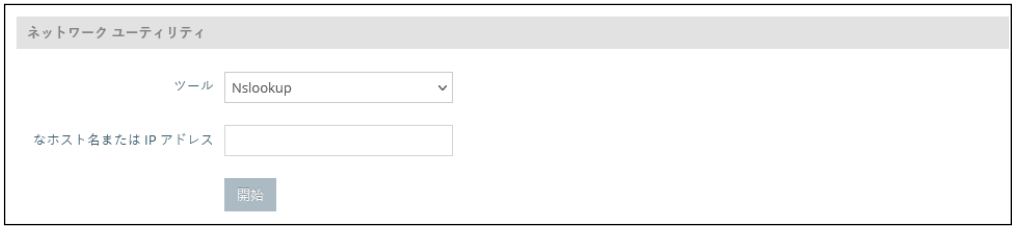
図 71: ネットワークユーティリティ — Ping

Traceroute ホスト名または IP アドレスを入力し、クリックするとトレースアウトツールが実行されます。

図 72: ネットワークユーティリティ — Traceroute

Nslookup ホスト名または IP アドレスを入力し、クリックすると Nslookup ツールが実行されます。

図 73: ネットワークユーティリティ — Nslookup



Speed Test AP とサーバー間の速度をテストするための Netperf サーバーのホスト名またはIP アドレスを入力します。

図 74: ネットワークユーティリティ — Speed Test

デバイス・ディスカバリー

デバイス検索ツールは、同じレイヤー 2 ネットワーク内にある他の Edgecore AP を見つけるための方法を提供します。機能するには、Discovery Agent を有効にする必要があります（86 ページの「Edgecore Networks Discovery Tool」を参照。

「Scan Network」ボタンをクリックし、デバイスをスキャンします。

図 75: デバイス・ディスカバリーツール

セクション III

付録

このセクションでは、追加情報を提供します。

以下の内容が含まれています。

A トラブルシューティング

管理インターフェースにアクセスできない場合

表 1: トラブルシューティングチャート

症状	解決策
ウェブブラウザで接続できない	■ AP の電源が入っていることを確認してください。 ■ 管理ステーションと AP の間のネットワークケーブルを確認します。 ■ AP に有効なネットワーク接続があること、および中間スイッチポートが無効になっていないことを確認します。 ■ AP に有効な IP アドレス、サブネットマスク、デフォルトゲートウェイが設定されていることを確認します。 ■ 管理ステーションの IP アドレスが AP の IP と同じサブネットにあることを確認してください。 ■ タグ付き VLAN グループを使用して AP に接続しようとしている場合は、管理ステーションおよびネットワーク内の中間スイッチに接続するポートに適切なタグが設定されている必要があります。 ■ SSH での接続ができない場合は、許可されている最大同時 SSH セッション数を超えている可能性があります。時間をおいて再度接続してください。
パスワードが分からない	■ リセットボタンで AP を工場出荷時の状態に戻します。

システムログを使う

問題が発生した場合は、クイックスタートガイドを参照して、発生した問題が実際に AP に起因するものであるかどうかを確認してください。問題が AP に起因していると思われる場合は、以下の手順を実行してください。

1. エラーが発生するまでの一連のコマンドやその他の操作を繰り返します。
2. エラーの原因となったコマンドや状況をリストアップします。また、表示されたエラーメッセージのリストを作成します。
3. 関連するすべてのシステム設定を記録する。
4. 「システム」>「メンテナンス」ページでログファイルを表示し、ログファイルから情報をコピーする。
5. 「システム」>「メンテナンス」ページから診断ログをファイルにダウンロードする。