EAP101
EAP102

ユーザーマニュアル

ソフトウェアリリース 11.2.0

www.edge-core.com

ユーザーマニュアル

EAP101
EAP102

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

E092021-CS-R02

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。

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。45 ページ「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。45 ページ「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。42 ページ「電波設定」参照。
- オープンメッシュのサポート。51 ページ「無線ネットワーク — Open Mesh Settings」を参照 。
- SNMP v2 のサポート。63 ページ「SNMP」を参照。
- リモートシスログのサポート。64 ページ「Remote System Log Setup」を参照。
- LLDP のサポート。64 ページ「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、56 ページ「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

本ガイドの使い方 3

目次 5

図の一覧 8

表 10

セクション I 操作を開始する 11

1 はじめに 12

設定項目 13

ウェブインターフェースへの接続 13

LAN ポート接続 14

AP セットアップウィザード 15

QR コードからデバイスを登録する 20

メインメニュー 22

ダッシュボード 23

ウェブインターフェース上でよく見られるボタン 23

セクション II ウェブ設定 25

2 ステータス情報 26

一般ステータス 27

ネットワークステータス 28

無線ステータス 30

3 ネットワーク設定 33

インターネット設定 34

イーサネット設定 37

LAN 設定 39

4 無線設定 41
無線設定 42
電波設定 42
無線ネットワーク — 一般設定 44
無線ネットワーク — セキュリティ設定 45
無線ネットワーク — ネットワーク設定 50
無線ネットワーク — Open Mesh Settings 51
無線ネットワーク — 無線詳細設定 52
VLAN 設定 52

5 システム設定 55
システム設定 56
メンテナンス 57
システムログの表示 58
診断ログのダウンロード 58
AP の再起動 58
AP のリセット 59
設定内容のバックアップ 59
設定内容の復元 60
ファームウェアアップグレード 60
ユーザーアカウント 61
サービス 61
SSH 61
NTP 62
SNMP 63
Remote System Log Setup 64
LLDP 64
iBeacon 65
診断 66

セクション III 付録 67

A トラブルシューティング 68
管理インターフェースにアクセスできない場合 68

システムログを使う 68

図の一覧

図 1: ウェブ管理インターフェースへのログイン 14
図 2: パスワードの変更 15
図 3: 国の選択 16
図 4: クラウドによる管理もしくはスタンドアロンの選択 17
図 5: 無線ネットワークの設定 18
図 6: 詳細設定 19
図 7: AP の QR コードを読み取る 20
図 8: ecCLOUD　ログインページ 21
図 9: ecCLOUD　デバイス登録 22
図 10: ダッシュボード 23
図 11: 設定の変更を保存する 24
図 12: 一般ステータス情報 27
図 13: ローカルネットワーク 28
図 14: アクティブな DHCP リースと ARP テーブル 29
図 15: 無線ステータス 30
図 16: インターネット設定 34
図 17: IP アドレスモード – 固定 IP 35
図 18: IP アドレスモード – PPPoE 36
図 19: イーサネット設定 – インターネットソース 37
図 20: イーサネット設定 – ネットワークモード 37
図 21: ブリッジモード 38
図 22: ルーターモード 39
図 23: ネットワーク – LAN 設定 39
図 24: 無線設定（Radio 5 GHz） 42
図 25: 無線設定（Radio 2.4 GHz） 43
図 26: 無線設定 （一般設定） 44
図 27: セキュリティ設定 45
図 28: 無線ネットワーク設定 50
図 29: Open Mesh 設定 51

図 30: 無線詳細設定 52
図 31: 無線 VLAN 設定 53
図 32: システム設定 56
図 33: メンテナンス 57
図 34: システムログ 58
図 35: AP の再起動 58
図 36: 初期状態へのリセット 59
図 37: 設定内容の復元 60
図 38: ファームウェアアップグレード 60
図 39: ユーザーアカウント 61
図 40: SSH 設定 62
図 41: NTP 設定 62
図 42: SNMP 設定 63
図 43: リモートシステムログ設定 64
図 44: LLDP 設定 64
図 45: iBeacon 設定 65
図 46: ネットワークユーティリティ 66

表

表 1: トラブルシューティングチャート 68

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。

■ 12 ページ「はじめに」

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。

- 13 ページ「設定項目」
- 13 ページ「ウェブインターフェースへの接続」
- 15 ページ「AP セットアップウィザード」
- 20 ページ「QR コードからデバイスを登録する」
- 22 ページ「メインメニュー」

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 および 5GHz 無線の設定
- 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

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、15 ページ「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、20 ページ「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)。

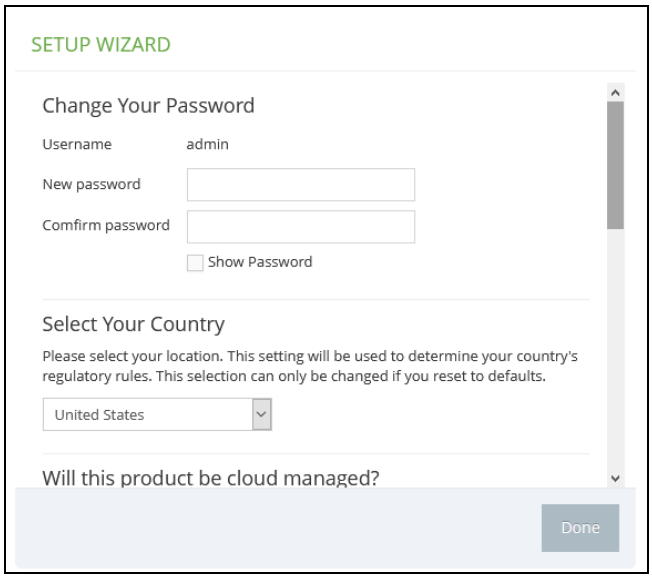
注意：Uplink （PoE）ポートを使用してウェブインターフェースに接続する場合、初期設定では、IP アドレスは DHCP によって自動的に割り当てられます。DHCP サーバーに到達できない場合、Uplink （PoE）ポートは 192.168.1.10 という予備の IP アドレスに戻ります。

AP のウェブ管理インターフェースにアクセスするには、以下の手順に従ってください。

1. ウェブブラウザから、初期設定の IP アドレス 192.168.2.1 を使用して管理インターフェースに接続します。

   初めてアクセスする場合は、セットアップウィザードが自動的に起動します。

図 1: ウェブ管理インターフェースへのログイン



2. 管理アクセス用の新しいパスワードを設定してから、15 ページ「AP セットアップウィザード」に記載されているその他の手順に従ってください。

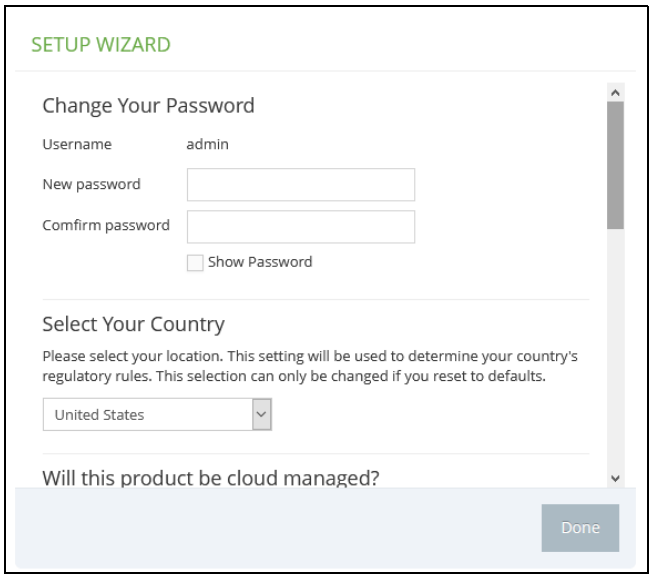
注意：お使いのネットワークに適合する別の管理用 IP アドレスで AP を設定するには、39 ページ「LAN 設定」を参照してください。

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。

Step 1 パスワードの変更 — AP への管理アクセスのための新しいパスワードを設定します（初期値ではユーザー名・パスワード共に「admin」）。パスワードは 6 ～ 20 文字の ASCII 文字で、大文字と小文字を区別し、特殊文字は使用しないでください。

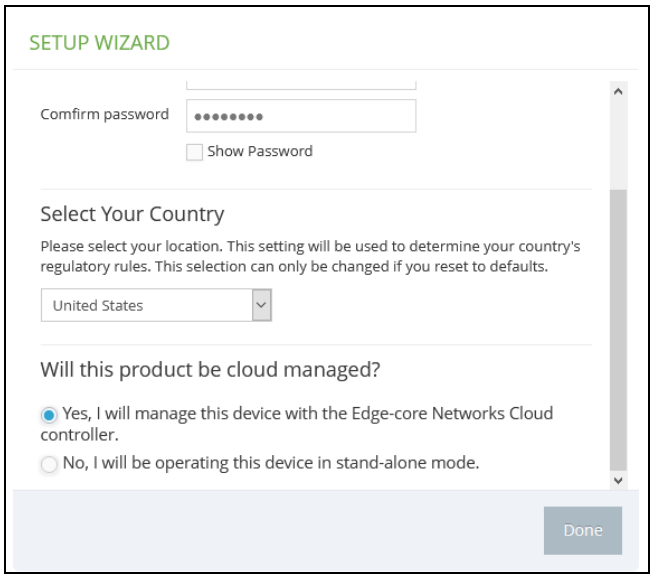
図 2: パスワードの変更



注意：ユーザー名やパスワードの変更については、61 ページ「ユーザーアカウント」をご参照ください。

Step 2 国の選択 — ドロップダウンメニューから、AP を動作させる国を選択します。AP の国コードを設定することで、無線機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必要があります。すなわち、国コードを設定すると、AP の動作が、指定された国の無線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制限されます。

図 3: 国の選択

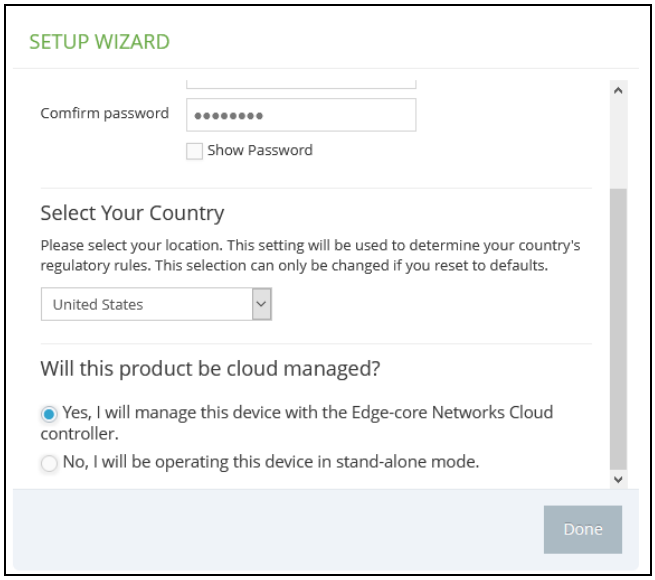


警告：使用する国を設定する必要があります。これにより、無線ネットワークに規定されている地域の規制の範囲内で無線機が動作するようになります

注意：国の選択は、米国以外のモデルにのみ適用され、米国のモデルには一切適用されません。FCC の規制により、米国で販売されるすべての Wi-Fi 製品は、米国の操作チャネルにのみ固定されなければなりません。

Step 3 クラウドによる管理もしくはスタンドアロンの選択 — Edgecore ecCLOUD コントローラーを使用して AP を管理する場合は、「Yes, I will manage this device with the Edge-core Networks Cloud controller」を選択して、「Done」をクリックします。それ以外の場合は、「No, I will be operating this device in stand-alone mode」を選択し、ステップ 4 に進みます。

図 4: クラウドによる管理もしくはスタンドアロンの選択

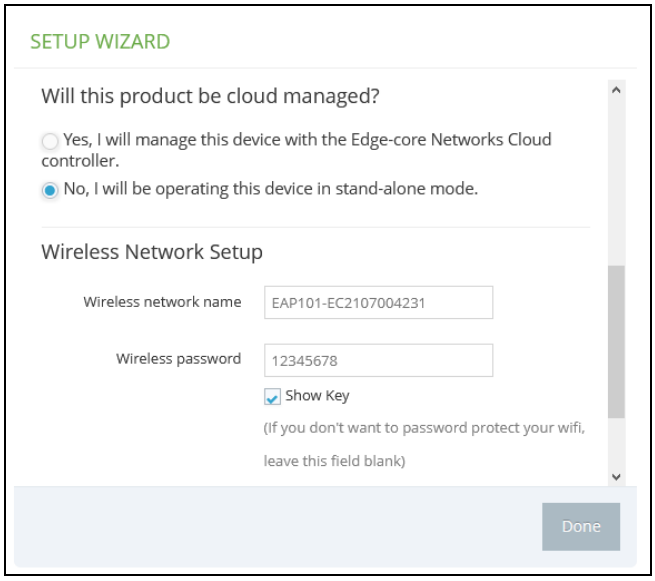


Edgecore ecCLOUD コントローラーを使用して AP を管理することを選択した場合は、cloud.ignitenet.com にアクセスして AP を登録します。ログイン後、メニューから「デバイス」を選択してください。「デバイスを追加する」をクリックし、AP のシリアル番号と MAC アドレスを入力して、AP をクラウドネットワークに登録します。シリアル番号と MAC アドレスは、製品パッケージまたはラベルに記載されています。

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ースについて説明します。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。

Step 4 無線ネットワークの設定 — 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は、そのまま無線ネットワークの設定が続きます。

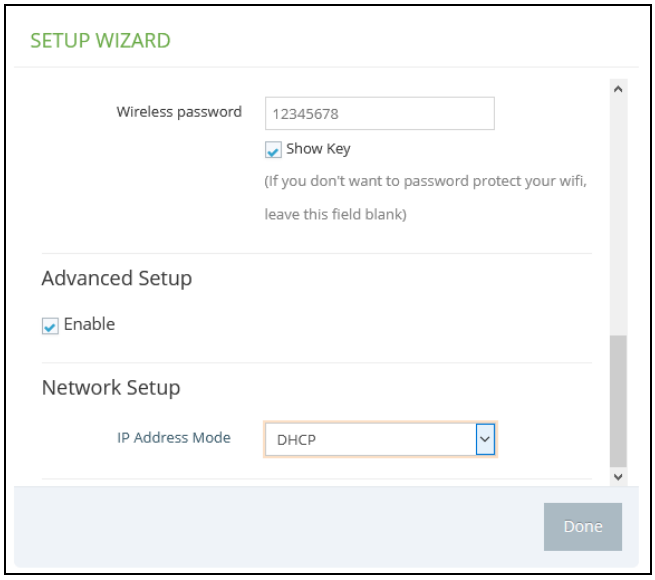
図 5: 無線ネットワークの設定



初期設定の無線ネットワーク名は、AP のモデルとシリアル番号で構成されています。また、パスワードの初期値が表示されます。これらは変更が可能です。無線ネットワーク名は 1 ～ 32 文字の ASCII 文字、パスワードは 8 ～ 63 文字の ASCII 文字で、特殊文字は使用しないでください。

Step 5 詳細設定 — スタンドアロンモードでは、詳細設定オプションを有効にすることができます。ここでは、IP アドレスモードを選択することで、インターネットアクセスポートへの IP アドレスの割り当て方法を設定することができます。

図 6: 詳細設定



初期値の IP アドレスモードは DHCP で、その他に固定 IP と PPPoE が選択できます。詳しくは、34 ページ「インターネット設定」をご覧ください。

Step 6 セットアップウィザードの完了後、「Done」をクリックしてウェブ管理インターフェースのメインメニューに進みます。

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（iPhone の場合）または携帯電話のバーコードアプリ（Android の場合）を使って、AP の QR コードをスキャンします。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 7: AP の QR コードを読み取る

4. メッセージが表示されたら、「接続」をタップして Wi-Fi ネットワークに参加します（iPhone では、「設定」→「Wi-Fi」でメッセージが表示されます）。

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

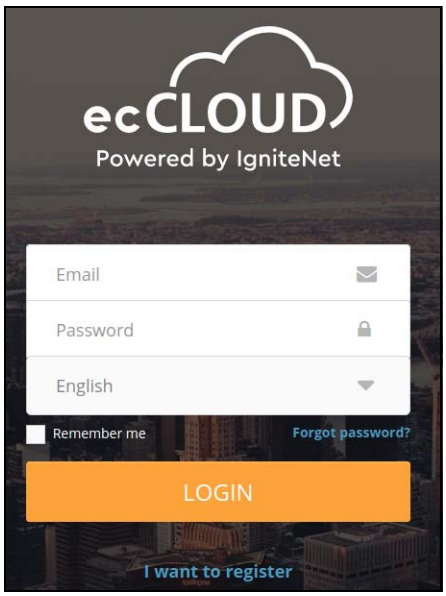
   a. スタンドアロンモードの場合：無線ネットワークの初期設定を使用する、もしくは、ネットワーク名とパスワードをカスタマイズするこ

とができます。「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 分間待ってから、セットアップウィザードで設定した無線ネットワーク名に接続します。その後、ブラウザは AP のログインページにリダイレクトされます
(14 ページ図 1 を参照)。

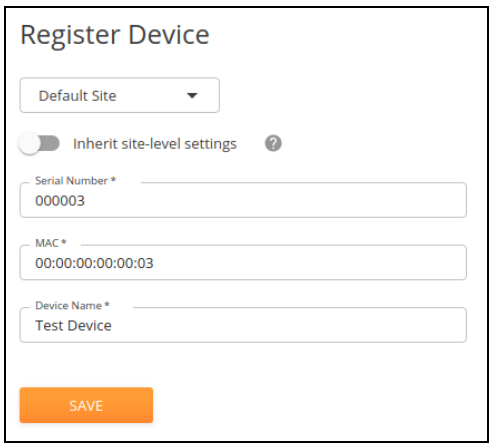
b. クラウド管理モードの場合：「Done」をタップすると、セットアップウィザードが終了し、ブラウザが ecCLOUD のログインページにリダイレクトされます。

図 8: ecCLOUD　ログインページ



すでに ecCLOUD のアカウントを持っている場合は、
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に登録されます。「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 2 分間待ちます。

図 9: 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 2 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。26 ページ「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。33 ページ「ネットワーク設定」をご参照ください。
- 無線 — 5 GHz / 2.4 GHz 無線及び VLAN の設定を行います。41 ページ「無線設定」をご参照ください。

- 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 10: 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 11: 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。

- 26 ページ「ステータス情報」
- 33 ページ「ネットワーク設定」
- 41 ページ「無線設定」
- 55 ページ「システム設定」

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、無線電波の状態など、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。

- 27 ページ「一般ステータス」
- 28 ページ「ネットワークステータス」
- 30 ページ「無線ステータス」

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 12: 一般ステータス情報

「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。
- 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。

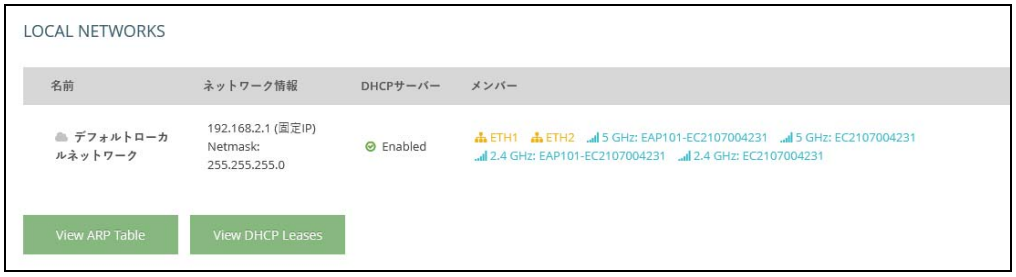
- ファームウェア — ファームウェアのバージョン。

- 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。

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。

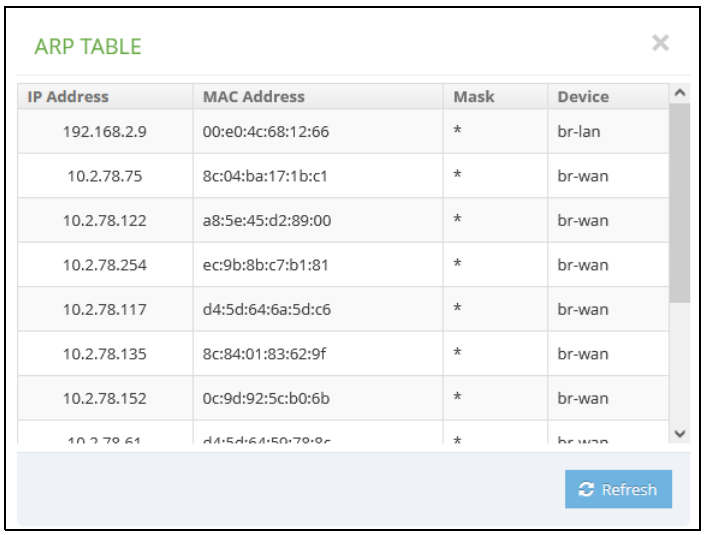
図 13: ローカルネットワーク

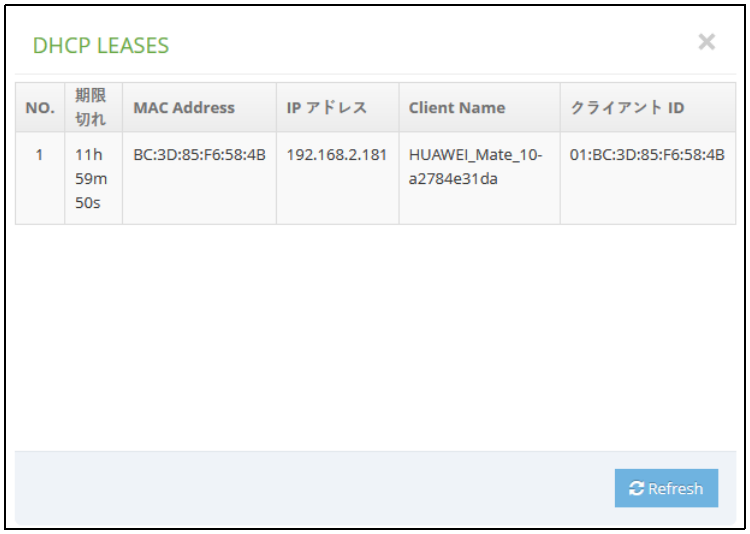


このセクションでは以下の項目が表示されます。

- 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 — ARP キャッシュを表示します。

図 14: アクティブな DHCP リースと ARP テーブル

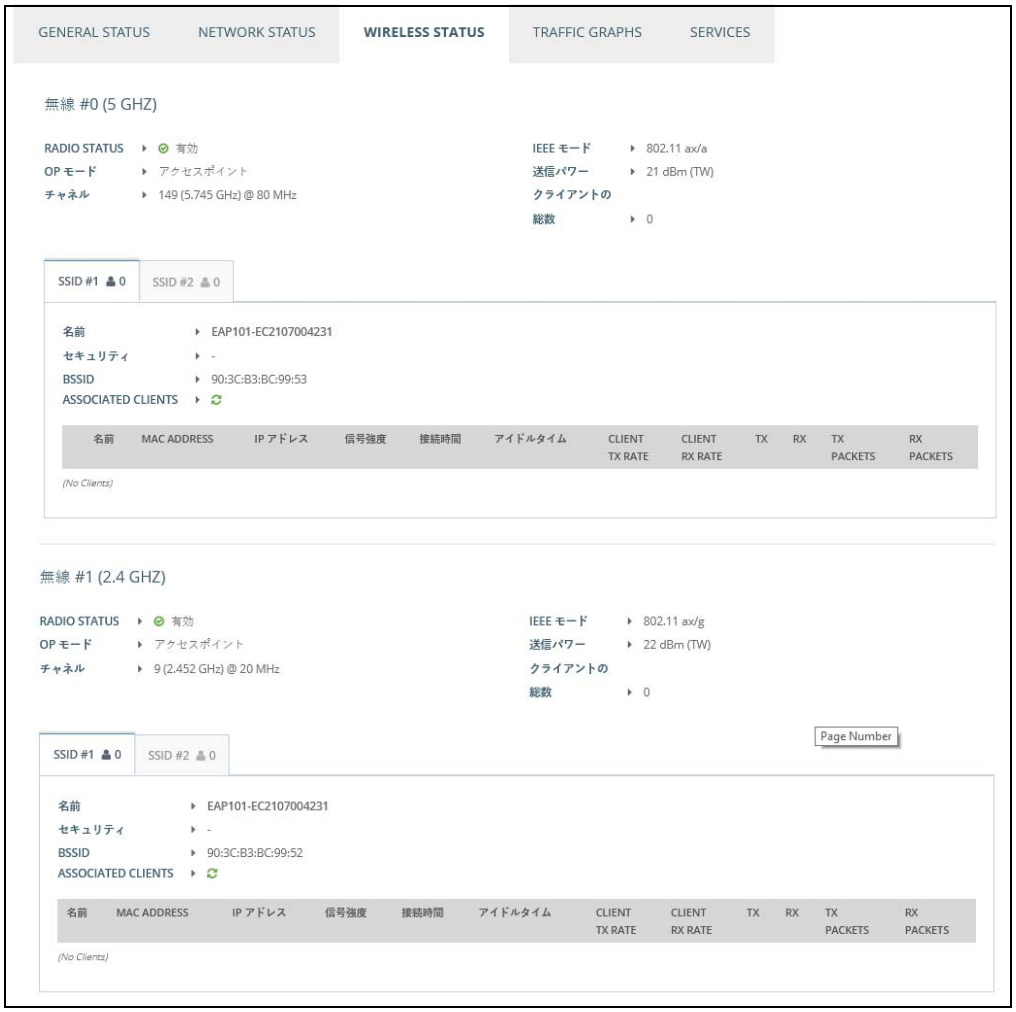




無線ステータス

「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 15: 無線ステータス



このセクションでは、以下の項目が表示されます。

- Wireless Radio 5 GHz/2.4 GHz —2.4GHz または 5GHz の無線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。
- 関連クライアント — SSID に接続されている無線クライアントの数です。

■ 接続済み端末 — 接続された無線クライアントの詳細情報を表示します。

- ネットワーク — SSID 名。
- 無線 — 接続されている無線（5GHz または 2.4GHz）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。
- 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。

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。

- 34 ページ「インターネット設定」
- 37 ページ「イーサネット設定」
- 39 ページ「LAN 設定」

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 16: 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。

- 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図 16 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 17: 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 18: 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。

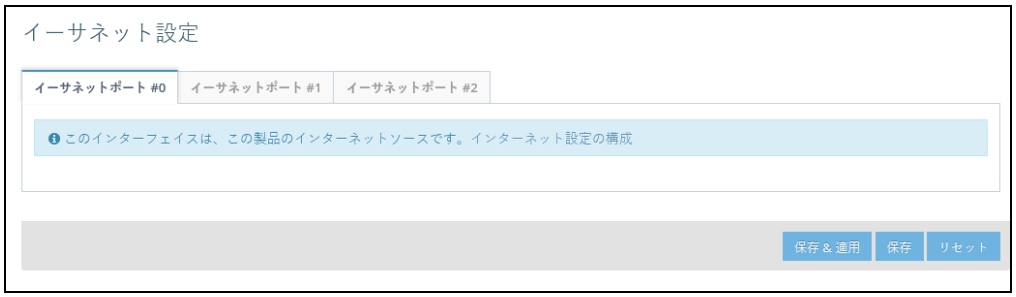
イーサネット設定

「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 19: 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。

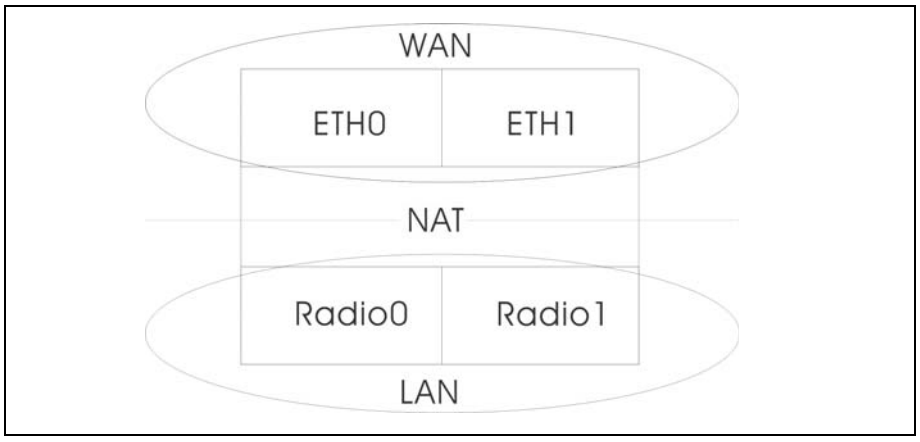
図 20: イーサネット設定 – ネットワークモード

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。

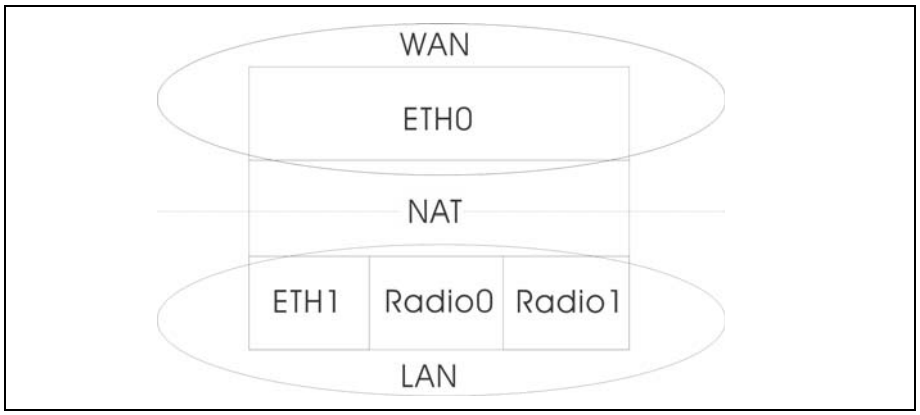
    次の図では、イーサネットポート 0 (ETH0) とイーサネットポート 1 (ETH1) の両方が WAN に接続されています。

    図 21: 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 22: ルーターモード



- 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。

- 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。

LAN 設定

「LAN 設定」ページでは、IP インターフェースの設定、DHCP サーバーの設定、STP の管理状態など、ローカルネットワークの LAN 設定を行います。

図 23: 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）。

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。

- 42 ページ「無線設定」
- 52 ページ「VLAN 設定」

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。

AP は、802.11b+g+n/ax（2.4GHz）または 802.11a/a+n/ac+a+n/ax（5GHz）の複数の無線モードで動作可能です。なお、デュアルバンドの AP は、2.4GHz と 5GHz で同時に動作することができます。ウェブ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ています。

- Radio 5 GHz — 5GHz 802.11a/n/ac/ax 無線インターフェース
- Radio 2.4 GHz — 2.4 GHz 802.11b/g/n/ax 無線インターフェース

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 24: 無線設定（Radio 5 GHz）

図 25: 無線設定 （Radio 2.4 GHz）

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。
- 802.11 モード — 無線動作モードを定義します。
  - Radio 5 GHz — 初期値：11ax
    オプション：11a、11a+n、11ac+a+n、11ax
  - Radio 2.4 GHz — 初期値：11ax
    オプション：11b+g+n/ax
- チャネル帯域幅 — AP のチャネル帯域幅のオプションには、20、40、80 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 (初期値：2.4GHz 帯無線の場合は 20MHz、5GHz 帯無線の場合は 80MHz、オプション：20MHz、40MHz、80MHz)。
  - 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）

- 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）。

- 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）。

- Minimum signal allowed — クライアントの信号強度（SNR）が指定した値以上の場合にのみ、無線インターフェースへの接続を許可します。値をゼロに設定すると、この機能は無効になります（範囲：0 ～ 99、初期値：0、無効）。

無線ネットワーク — 一般設定

図 26: 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）。

- 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）。

- 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）。
- 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）。
- 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）。

無線ネットワーク — セキュリティ設定

図 27: 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：セキュリティなし）。
  - 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。
- 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。

- 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）。
- 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。

- 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）。

- 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。

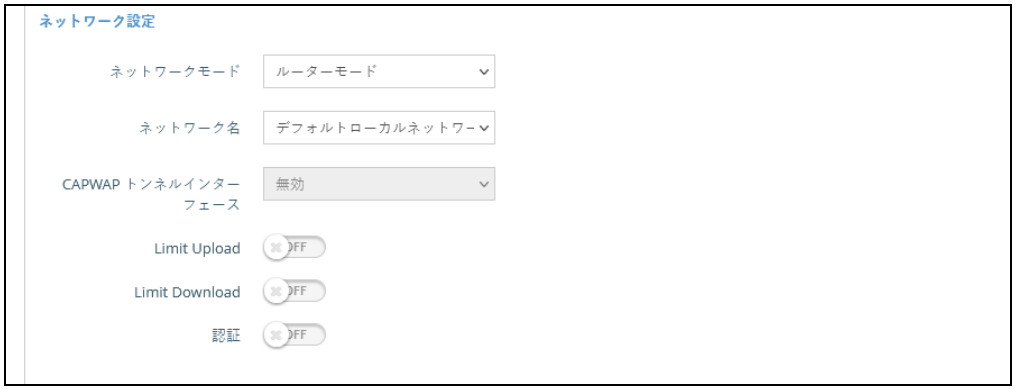
- アクセスコントロールリスト — 無線クライアントの MAC アドレスを、AP に設定されたローカルデータベースと照合して、ネットワーク接続の認証を行うことができます（初期値：OFF）。

  - 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。

無線ネットワーク — ネットワーク設定

図 28: 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（38 ページ図 21「ブリッジモード」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（39 ページ図 22「ルーターモード」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。
  - 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、52 ページ「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。

- 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（ 56 ページ「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）。

- サービスゾーン — AP が動作し、EWS-Series コントローラーによって管理されるサービスゾーンを選択します。

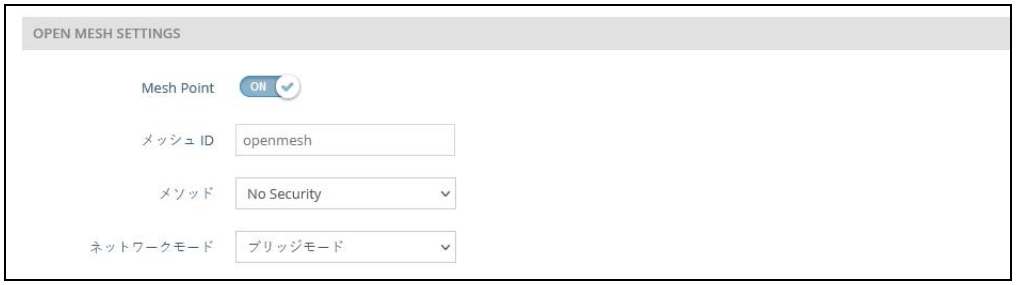
- 認証 — AP のシステム管理が ecCLOUD モードに設定されている場合（56 ページ「システム設定」を参照）、このオプションは ecCLOUD コントローラーとの AP 通信を認証します（初期値：OFF）。

無線ネットワーク — 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（2.4GHz または 5GHz）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 29: 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。

無線ネットワーク — 無線詳細設定

図 30: 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）。

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 31: 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。

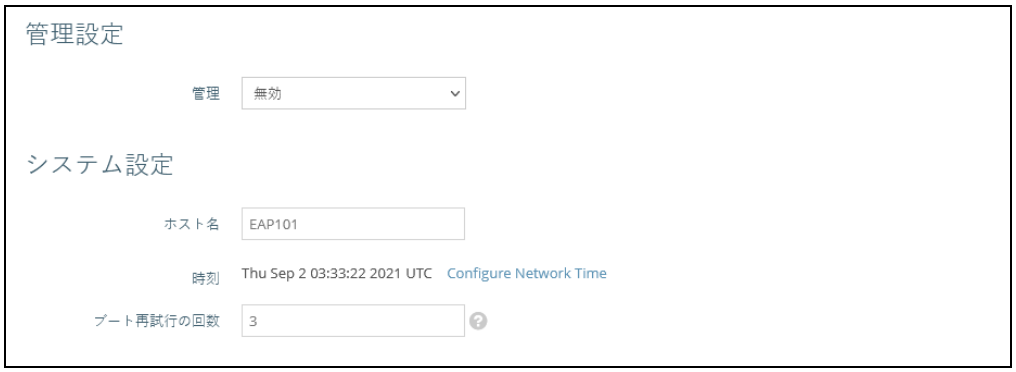
以下の内容が含まれています。

- 56 ページ「システム設定」
- 57 ページ「メンテナンス」
- 61 ページ「ユーザーアカウント」
- 61 ページ「サービス」
- 66 ページ「診断」

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 32: 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。
  - EWS-Series Controller — 選択すると、以下のパラメータが表示されます。
    - 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。
    - 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。

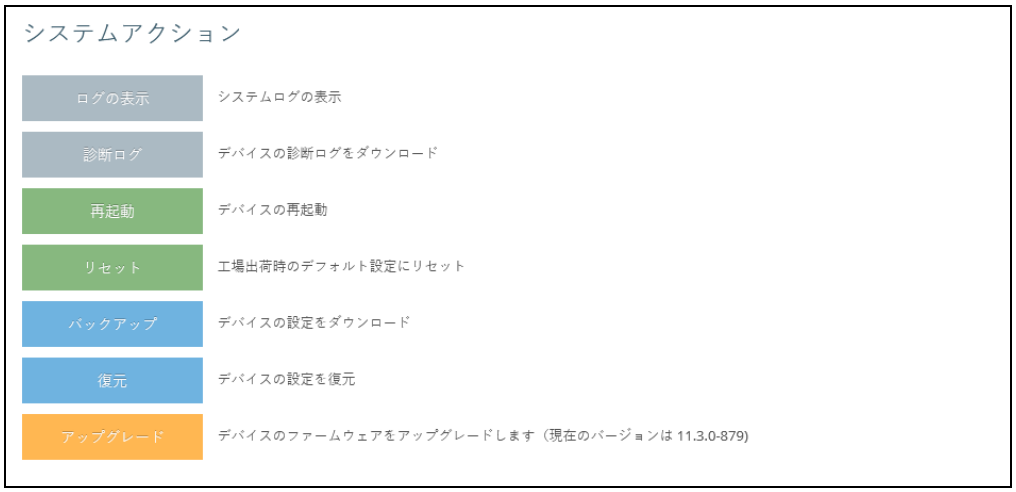
- ブロードキャストによる探索 — AP はブロードキャストリクエストを送信し、同じサブネット内の EWS コントローラーを検出します。
- マルチキャストによる探索 — AP は、EWS コントローラーを見つけるために、ネットワーク上でマルチキャストディスカバリーパケットを送信します。このオプションは、ネットワークにルーティングパスが適切に設定されている必要があります。
- 手動設定による探索 — AP が CAPWAP ジョインリクエストを送信する際に使用する IP アドレスを入力することで、EWS コントローラーに手動で到達する方法を提供します。

- 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：0 ～ 50 文字）。
- 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）。

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 33: 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 34: システムログ

診断ログのダウンロード

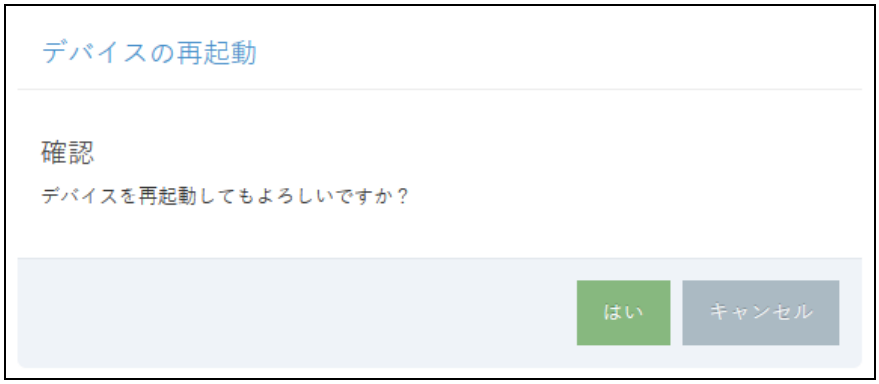
「診断ログ」をクリックすると、ログファイルが管理ワークステーションにダウンロードされます。Windows では、GNU Zip （*.tar.gz）ファイルがダウンロードフォルダーに保存されます。

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。

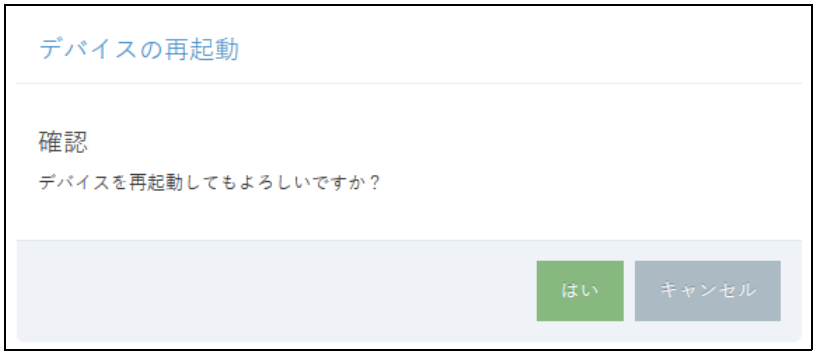
図 35: AP の再起動



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 36: 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

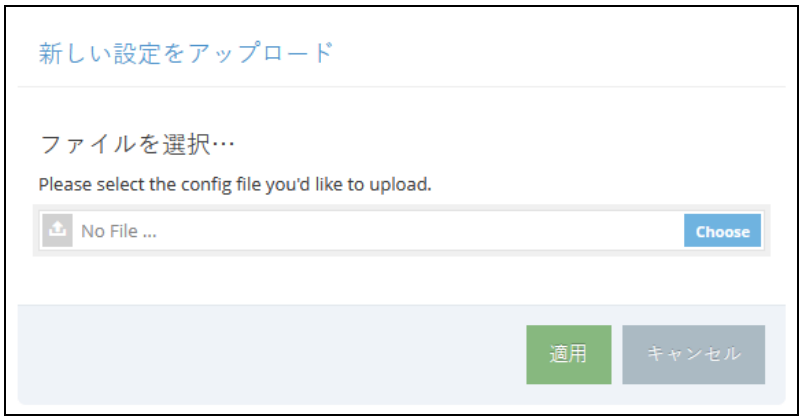
バックアップ機能を使うと、AP の設定を管理用のワークステーションにバックアップすることができます。Windows では、ダウンロードフォルダーに GNU Zip （*.tar.gz）ファイルが格納されます。ファイル名は次のようになります。

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 37: 設定内容の復元

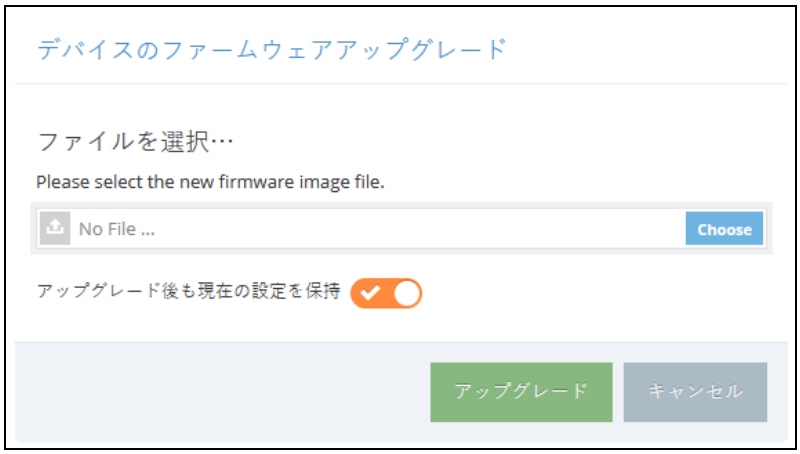


ファームウェアアップグレード

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。

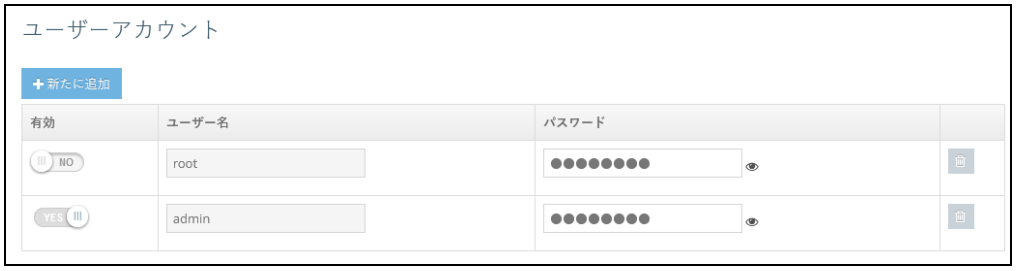
図 38: ファームウェアアップグレード



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 39: 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 (1 ～ 32 文字の ASCII 文字で、特殊文字は使用しないでください)。
- 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

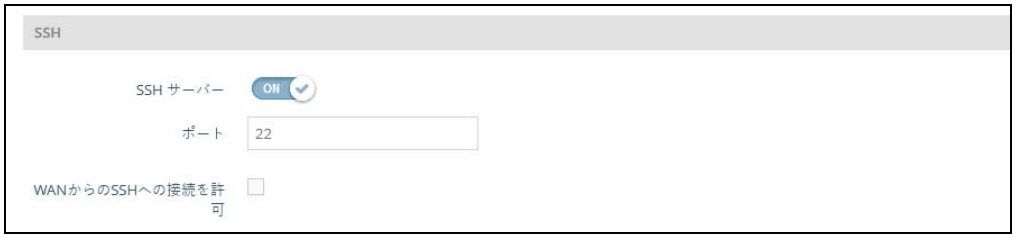
「サービス」ページでは、AP への SSH 接続の制御、NTP タイムサーバーの設定、iBeacon の設定を行うことができます。

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 40: SSH 設定



このページには以下の項目が表示されます。

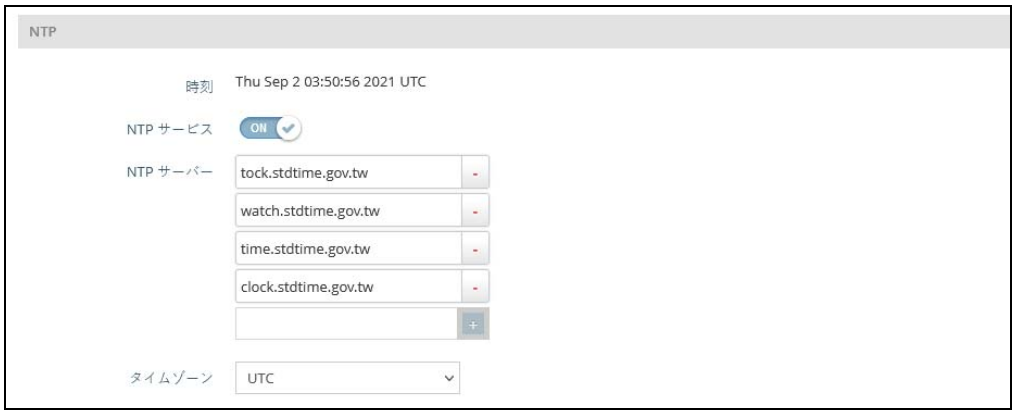
- SSH サーバー — AP への SSH 接続を有効または無効にします (初期値：ON)。
- ポート — AP の SSH サーバーの TCP ポート番号を設定します (範囲：1 ～ 65535、初期値：22)。
- WAN から SSH への接続を許可 — WAN からの SSH 管理接続を許可します。

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 41: NTP 設定



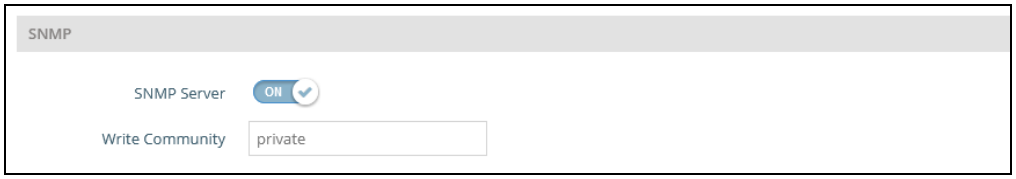
このページには以下の項目が表示されます。

- 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 42: SNMP 設定



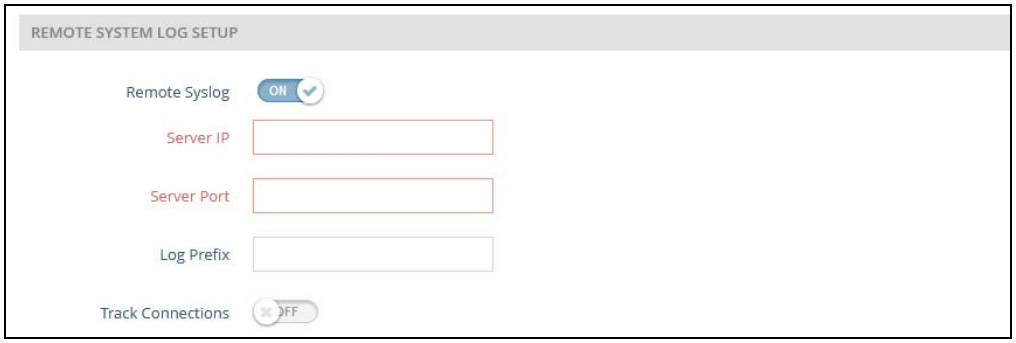
このページには以下の項目が表示されます

- SNMP Server — AP の SNMP を有効または無効にします（初期値：ON)。
- 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)

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 43: リモートシステムログ設定



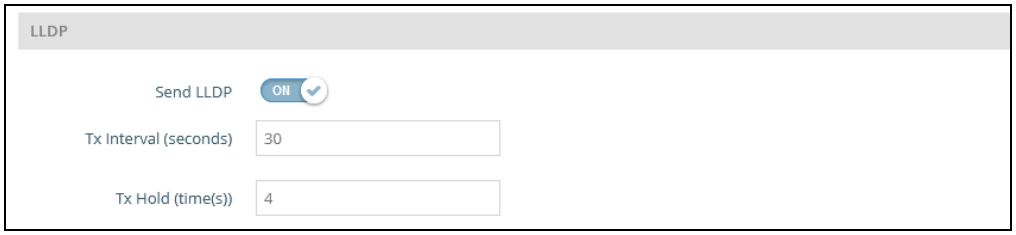
このページには以下の項目が表示されます。

- 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。

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 44: 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）。

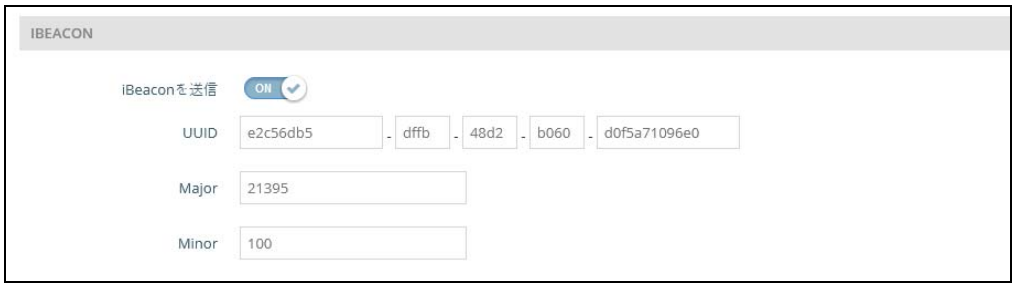
  TTL は、受信側の LLDP エージェントに、送信側のデバイスがタイムリーにアップデートを送信しなかった場合に、そのデバイスに関連するすべての情報をどのくらいの期間保持するかを伝えます。

  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。

iBeacon

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 45: iBeacon 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）。

診断

「診断」ページには、接続問題のトラブルシューティングのための Ping、Traceroute、および Nslookup ツールが用意されています。

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

図 46: ネットワークユーティリティ

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。

■ 68 ページ「トラブルシューティング」

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。