FUJITSU Desktop ESPRIMO

B6FY-4781-01 Z0

アクセスポイント操作ガイド

ESPRIMO Edge Computing Edition

FUJITSU

目次

本書をお読みになる前に

安全にお使いいただくために

本製品を安全に正しくお使いいただくための重要な情報が『取扱説明書』に記載されています。
特に、「安全上のご注意」をよくお読みになり、理解されたうえで本製品をお使いください。

本書の表記

■本書の記号

本書に記載されている記号には、次のような意味があります。

重要	お使いになるときの注意点や、してはいけないことを記述しています。 必ずお読みください。
POINT	操作に関連することを記述しています。必要に応じてお読みください。

■連続する操作の表記方法

本書中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：ナビゲーションパネルから「基本設定」をクリックし、「マイルーター」をクリックする操作

↓

「基本設定」→「マイルーター」の順にクリックします。

■画面例およびイラストについて

本文中の画面およびイラストは一例です。お使いの機種やモデルによって、実際に表示される画面やイラスト、およびファイル名などが異なることがあります。また、イラストは説明の都合上、本来接続されているケーブル類を省略したり形状を簡略化したりしていることがあります。

商標および著作権

1 通常ユーザの設定

無線ルータには、Webに基づく直感的なグラフィカルユーザインターフェイス（GUI）が含まれています。これを使用すると、管理者はその機能をWebブラウザー経由で容易に構成できます。

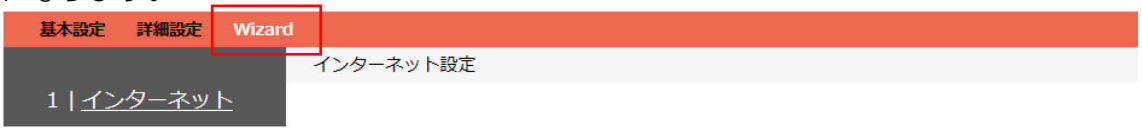
1.1 ログイン

1. エッジコンピューティングデバイス上でInternet Explorerを起動し、アクセスポイント部分のIPアドレス（初期値「192.168.1.1」）に接続します。
   ログイン画面が表示されます。
2. ユーザ名とパスワードを入力し、「ログイン」をクリックします。
   ユーザ名の初期値は「admin」、パスワードの初期値は「admin」です。

左上に「パスワード変更」、「日本語」、「ログアウト」の3つのコマンドボタンがあります。
「パスワード変更」をクリックすると、パスワードを変更する画面に移動します。
「日本語」をクリックすると、Webページの言語（日本語または英語）を選択できます。
「ログアウト」をクリックすると、アクセスポイントの設定画面から抜け、ログイン画面に戻ります。各種設定が終わったら、「ログアウト」をクリックしてログアウトしてください。

1.2 ウィザード設定

管理者は、無線ルータの基本設定の構成に移動できます。これにより、ルータの設定が非常に簡単になります。

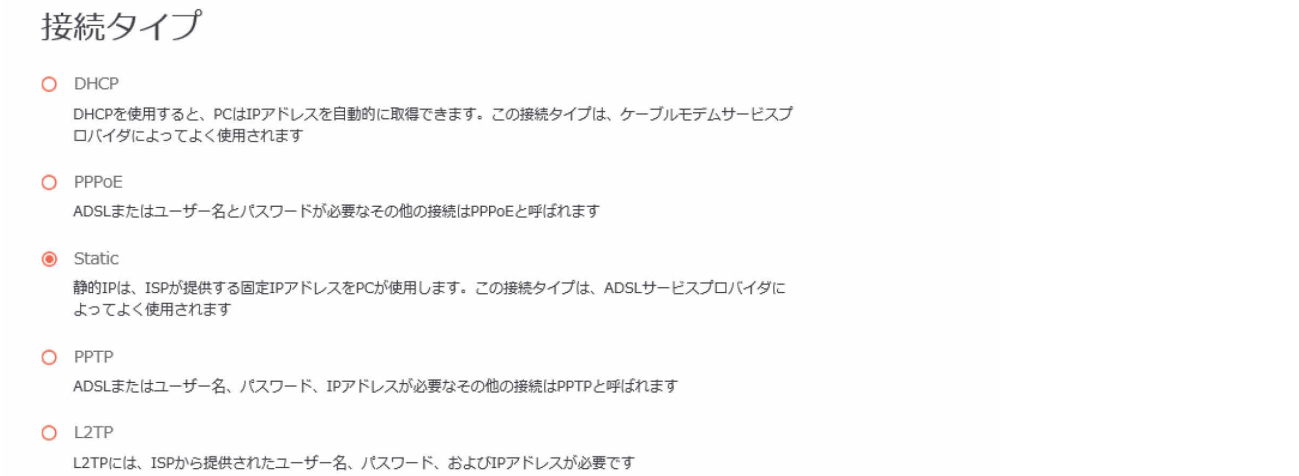


■インターネット設定

「Wizard」をクリックすると、**インターネット設定**ページが表示されます。

接続タイプ

接続タイプには、DHCP、PPPoE、Static（静的IPアドレス）、PPTP、L2TPの5種類があります。



どの種類のWAN接続タイプを選択したらよいかわからない場合は、インターネットサービスプロバイダ（以下ISP）に問い合わせてください。

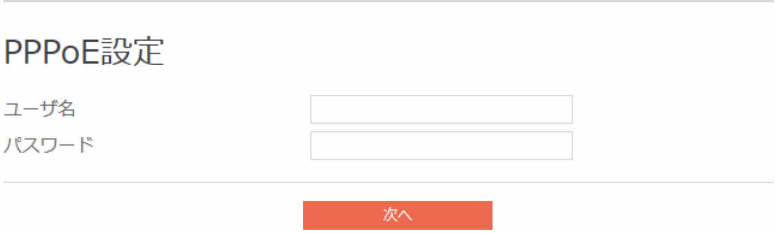
以下に各接続タイプの設定方法について説明します

1. DHCP：ルータがIPアドレスを自動的に取得できるようにします。このタイプは通常、ケーブルモデムのサービスプロバイダーが使用します。

- WAN MAC：WANポートのMACアドレス。一部のISPは、自身のサービスに接続しているデバイスのMACアドレスを監視し、無効なMACアドレスのインターネット接続を禁止します。この問題を解決するために、次のいずれかを実行してください。
  *ISPに連絡して、ISPサブスクリプションに関連付けられたMACアドレスを更新するよう要求します。
  *新しいデバイスのMACアドレスを元のデバイスのMACアドレスに一致するように複製または変更します。
- ホスト名：ルータの名前を指定します。通常、ホスト名はISPから提供されます。

- **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
- 「**次へ**」をクリックします。

2. **PPPoE**：ユーザ名とパスワードが必要な、ISPから提供されるインターネットプロトコルです。ユーザ名とパスワードがわからない場合は、ISPに問い合わせてください。



- **ユーザ名**：ISPから入手したアカウントを入力します。
- **パスワード**：ISPから入手したパスワードを入力します。
- 「**次へ**」をクリックします。

3. **静的IPアドレス**：ルータがISPから提供された固定IPアドレスを使用するようにします。

- **IPアドレス**：ISPから入手したIPアドレスを入力します。
- **サブネットマスク**：ISPから入手したIPアドレスを入力します。
- **ゲートウェイアドレス**：ISPから入手したゲートウェイのIPアドレスを入力します。
- **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
- **WAN MAC**： WANポートのMACアドレス。一部のISPは、自身のサービスに接続しているデバイスのMACアドレスを監視し、無効なMACアドレスのインターネット接続を禁止します。この問題を解決するために、次のいずれかを実行してください。
  *ISPに連絡して、ISPサブスクリプションに関連付けられたMACアドレスを更新するよう要求します。
  *新しいデバイスのMACアドレスを元のデバイスのMACアドレスに一致するように複製または変更します。
- 「**次へ**」をクリックします。

POINT

「静的IPアドレス」のすべてのパラメーターは、ISPから提供されます。各パラメーターがわからない場合は、ISPにご確認ください。

4. **PPTP**：ユーザ名とパスワード、または静的IPアドレスの設定が必要なISPから提供されるサービスです。

- **ユーザ名**：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- **パスワード**：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- **WANのIPアドレスを自動取得**：WANのIPアドレスを自動的に取得する場合は**「はい」**を、静的IPアドレスを使用する場合は**「いいえ」**を選択します。
- **IPアドレス**：WAN接続に静的IPアドレスを使用する場合は、IPアドレスを入力します。
- **サブネットマスク**：WAN接続に静的IPアドレスを使用する場合は、サブネットマスクを入力します。
- **ゲートウェイアドレス**：WAN接続に静的IPアドレスを使用する場合は、ゲートウェイアドレスを入力します。
- **DNSサーバへ接続**：デバイスが自動的にDNSサーバに接続できるようにする場合は**「はい」**を、接続するDNSサーバを手動で設定する場合は**「いいえ」**を選択します。
- **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
- **VPNサービス**：VPNサーバのIPアドレスまたはDNS名を入力します。
- **「次へ」**をクリックします。

5. **L2TP**：ユーザ名とパスワード、またはISPから提供された静的IPアドレスの設定が必要です。

- **ユーザ名**：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- **パスワード**：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- **WANのIPアドレスを自動取得**：WANのIPアドレスを自動的に取得する場合は**「はい」**を、静的IPアドレスを使用する場合は**「いいえ」**を選択します。
- **IPアドレス**：WAN接続に静的IPアドレスを使用する場合は、IPアドレスを入力します。
- **サブネットマスク**：WAN接続に静的IPアドレスを使用する場合は、サブネットマスクを入力します。
- **ゲートウェイアドレス**：WAN接続に静的IPアドレスを使用する場合は、ゲートウェイIPアドレスを入力します。
- **DNSサーバへ接続**：デバイスが自動的にDNSサーバに接続できるようにする場合は**「はい」**を、接続するDNSサーバを手動で設定する場合は**「いいえ」**を選択します。
- **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
- **VPNサービス**：VPNサーバのIPアドレスまたはDNS名を入力します。
- **「次へ」**をクリックします。

■ネットワーク設定

「インターネット設定」ページで「次へ」をクリックすると、ここに移動します。

1. SSID：無線ネットワークの名前で、無線ネットワークを識別するために使用されます。
2. 事前共有キー(PSK)：無線接続を認証するためにルータによって使用されるパスワードのことです。事前共有キーは、SSID名、アクセスポイントごとに変更することをお勧めします。
3. 完了したら、「次へ」をクリックします。

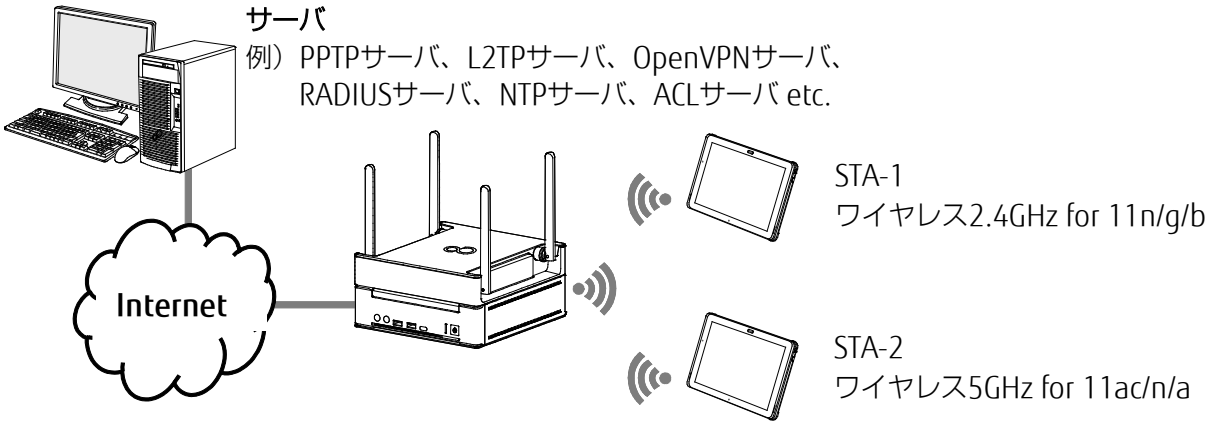
■設定情報

「ネットワーク設定」ページで「次へ」をクリックすると、ここに移動します。
ここには構成情報の要約が表示されます。設定がすべて正しい場合、「適用」をクリックします。

1.3 基本設定

1.3.1 ネットワークビュー

デバイスに関する基本的な情報はここで指定します



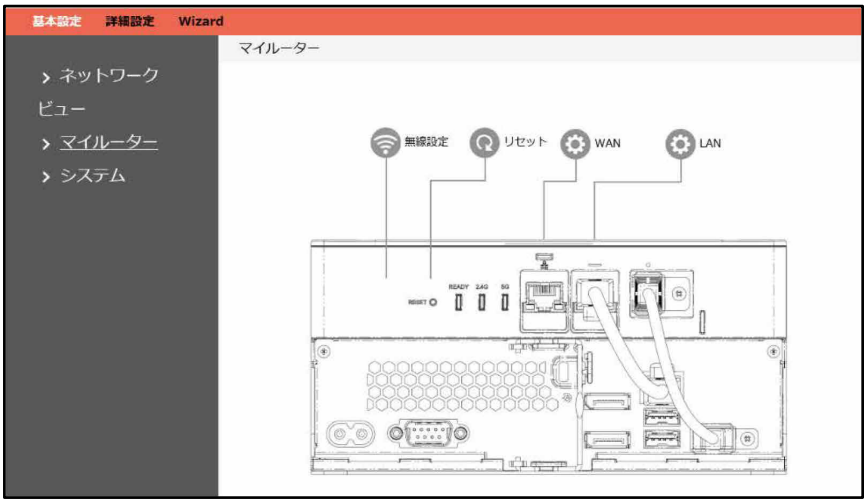
図は、ネットワークトポロジの例を示しています。

「ネットワークビュー」には、Internet、ルータ、およびユーザが表示されます。

1. ナビゲーションパネルから、**「基本設定」→「ネットワークビュー」**の順にクリックします。
2. **Internet**：接続状態、接続タイプ、接続時刻、およびトラフィックのアップロード/ダウンロードを示します。
3. **ルータ**：システム、LAN、およびWLAN情報を示します。
4. **ユーザ**：クライアントユーザおよびアクセスポイントがブロックしたユーザ情報を示します。

1.3.2 マイルーター

ナビゲーションパネルから、「**基本設定**」→「**マイルーター**」の順にクリックします。
ボタンを使用して、ルータを迅速かつ容易に設定します。



1.3.2.1 無線設定

ルータの無線接続に関する一部の基本設定を構成するために実装されています。

1. **SSID**：無線デバイスは、その通信範囲内のすべてのネットワークを自動的に検出できます。SSIDの最大長は32文字です。
2. **事前共有キー(PSK)**：長さは、0～63文字（文字、数字、またはその組み合わせ）あるいは16進数8～64桁です。
3. 「**適用**」をクリックします。

1.3.2.2 リセット

図の「リセット」は、ルータを手動で再起動するために使用します。

1.3.2.3 LAN設定

エッジコンピューティングデバイス背面のRESETボタンを押したときの、デフォルトのIPアドレスを変更できます。通常は変更の必要はありません。

POINT

- リセット時のIPアドレスが変わってしまいますので、設定したIPアドレスを忘れないようにご注意ください。

LAN IP設定を変更するための手順：

1. ナビゲーションパネルから、「基本設定」→「マイルーター」の順にクリックします。
2. LAN IP：無線ルータのLAN IPアドレス。そのデフォルト値は192.168.1.1です。IPベースのネットワークでは、パケットはネットワークデバイスの固有のIPアドレスに送信されます。
3. サブネットマスク：無線ルータのサブネットマスク。そのデフォルト値は255.255.255.0です。
4. DHCPサーバ：DHCPはほとんどの場合、LAN側のデバイスにIPアドレスを割り当てるために使用されます。さらに、DHCPサーバは、LAN側のデバイスにDNSサーバのアドレスやデフォルトゲートウェイのIPなどを通知できます。この無線ルータは、最大253のIPアドレスを割り当てることができます。

POINT

管理者はLAN IP設定として「DHCPサーバ」を選択することをお勧めします。選択しない場合、管理者はLAN側のデバイスにIPアドレスを手動で割り当てる必要があります。

5. 「適用」をクリックします。

1.3.2.4 WAN設定

WAN接続の設定を構成するには、「WAN」をクリックします。

1. **接続タイプ**：インターネットサービスのタイプを選択します。
   DHCP、PPPoE、Static（静的IPアドレス）、PPTP、L2TPの5つのオプションがあります。どの種類のWAN接続タイプを選択したらよいかわからない場合は、ISPに問い合わせてください。
2. **DHCPを選択した場合**

- **WAN MAC**： WANポートのMACアドレス。一部のISPは、自身のサービスに接続するデバイスのMACアドレスを監視し、新しいMACアドレスのインターネット接続を禁止します。
  この問題を解決するために、次のいずれかを実行してください。
  *ISPに連絡して、ISPサブスクリプションに関連付けられたMACアドレスを更新するよう要求します。
  *新しいデバイスのMACアドレスを元のデバイスのMACアドレスに一致するように複製または変更します。
- **ホスト名**：無線ルータのホスト名を指定できます。通常、ホスト名はISPから提供されます。
- **WANのDNSサーバを使用**：DNSサーバを使用する場合はチェックを付けます。
- **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
- 「**適用**」をクリックします。

3. PPPoEを選択した場合

- **ユーザ名：** ISPから入手したアカウントを入力します。
- **パスワード**：ISPから入手したパスワードを入力します。
- **Connect to DNS Server**：デバイスが自動的にDNSサーバに接続できるようにする場合は「Yes」を、接続するDNSサーバを手動で設定する場合は「No」を選択します。
- **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
- **「適用」**をクリックします。

POINT

「PPPoE」のすべてのパラメーターは、ISPから提供されます。パラメーターがわからない場合は、ISPに問い合わせてください。

4. Static（静的IPアドレス）を選択した場合

- IP：WAN接続に静的IPアドレスを使用する場合は、IPアドレスを入力します。
- サブネットマスク：WAN接続に静的IPアドレスを使用する場合は、サブネットマスクを入力します。
- Gateway：WAN接続に静的IPアドレスを使用する場合は、ゲートウェイのIPアドレスを入力します。
- DNSサーバ1：優先DNSサーバのIPアドレスを入力します。
- DNSサーバ2：代替DNSサーバのIPアドレスを入力します。
- WAN MAC：WANポートのMACアドレス。一部のISPは、自身のサービスに接続するデバイスのMACアドレスを監視し、新しいMACアドレスのインターネット接続を禁止します。この問題を解決するために、次のいずれかを実行してください。
  *ISPに連絡して、ISPサブスクリプションに関連付けられたMACアドレスを更新するよう要求します。
  *新しいデバイスのMACアドレスを元のデバイスのMACアドレスに一致するように複製または変更します。
- 「適用」をクリックします。

5. PPTPを選択した場合

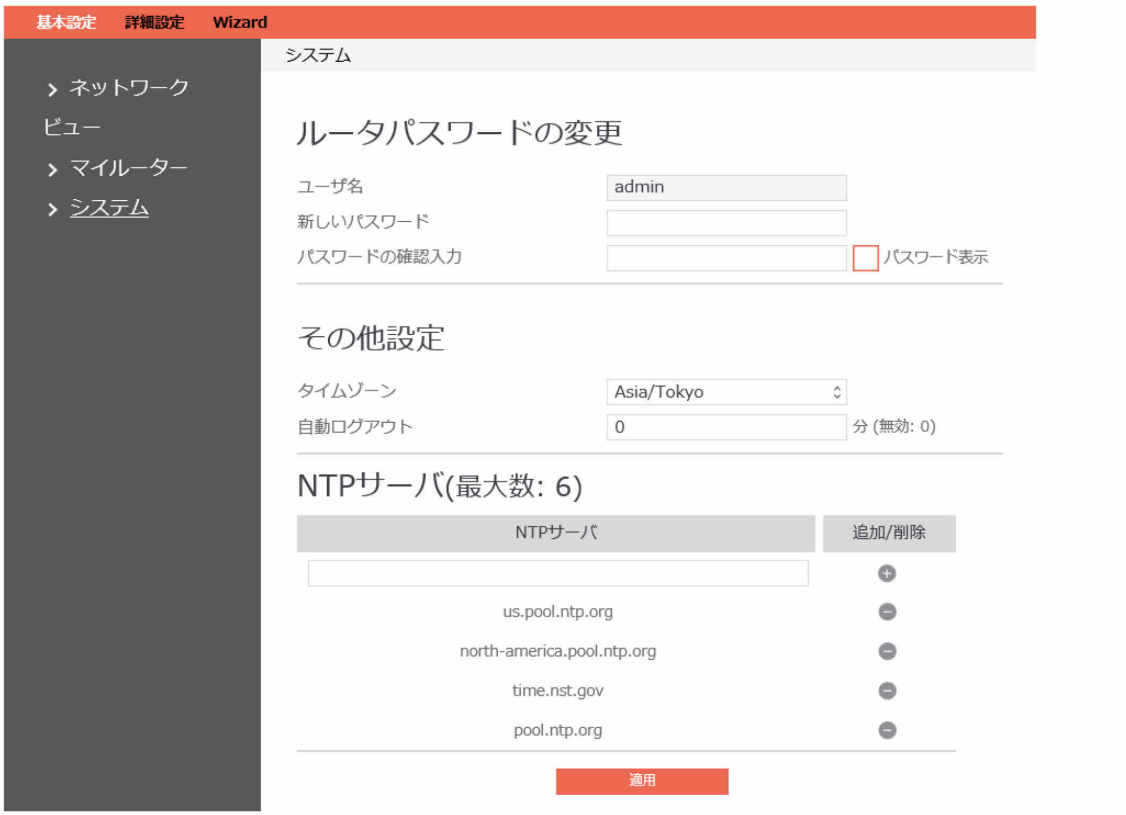
- Username：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- Password：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- Get WAN IP Automatically：WANのIPアドレスを自動的に取得する場合は「Yes」を、静的IPアドレスを使用する場合は「No」を選択します。
- IPアドレス：WAN接続に静的IPアドレスを使用する場合は、IPアドレスを入力します。
- サブネットマスク：WAN接続に静的IPアドレスを使用する場合は、サブネットマスクを入力します。
- Gateway：WAN接続に静的IPアドレスを使用する場合は、ゲートウェイのIPアドレスを入力します。
- 「適用」をクリックします。

6. L2TPを選択した場合

- Username：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- Password：ISPから提供される値を入力します。設定値としては自由に入力可能です。
- Get WAN IP Automatically：WANのIPアドレスを自動的に取得する場合は「Yes」を、静的IPアドレスを使用する場合は「No」を選択します。
- IPアドレス：WAN接続に静的IPアドレスを使用する場合は、IPアドレスを入力します。
- サブネットマスク：WAN接続に静的IPアドレスを使用する場合は、サブネットマスクを入力します。
- Gateway：WAN接続に静的IPアドレスを使用する場合は、ゲートウェイIPアドレスを入力します。
- Connect to DNS Server：デバイスが自動的にDNSサーバに接続できるようにする場合は「Yes」を、接続するDNSサーバを手動で設定する場合は「No」を選択します。
- DNSサーバ1：優先DNSサーバのIPアドレスを入力します。
- DNSサーバ2：代替DNSサーバのIPアドレスを入力します。
- VPN Server Address：VPNサーバのIPアドレスまたはDNS名を入力します。
- 「適用」をクリックします。

1.3.3 システム

システムを使用すると、ルータを構成できます。ルータのGUIにログインするために使用されるユーザ名とパスワードや、タイムゾーン、自動ログアウト、NTPサーバなどのその他のさまざまな設定を変更できます。



システム設定を設定するための手順：

1. ナビゲーションパネルから、**「基本設定」→「システム」**の順にクリックします。
2. **ユーザ名**：ルータにログインするために使用される名前が表示されます。
3. **新しいパスワード**：ルータの新しいログインパスワードを入力します。4～16文字以内で英数字!#$%&@+*の特殊記号が設定可能です。
4. **パスワードの確認入力**：ルータの新しいログインパスワードを再入力します。
5. **タイムゾーン**：デフォルトで使用されるタイムゾーンを指定します。
6. **自動ログアウト**：指定された期間が経過すると自動ログアウトします。
7. **NTPサーバ**：NTP（ネットワークタイムプロトコル）サーバのDNS名を入力します。
8. **「適用」**をクリックします。

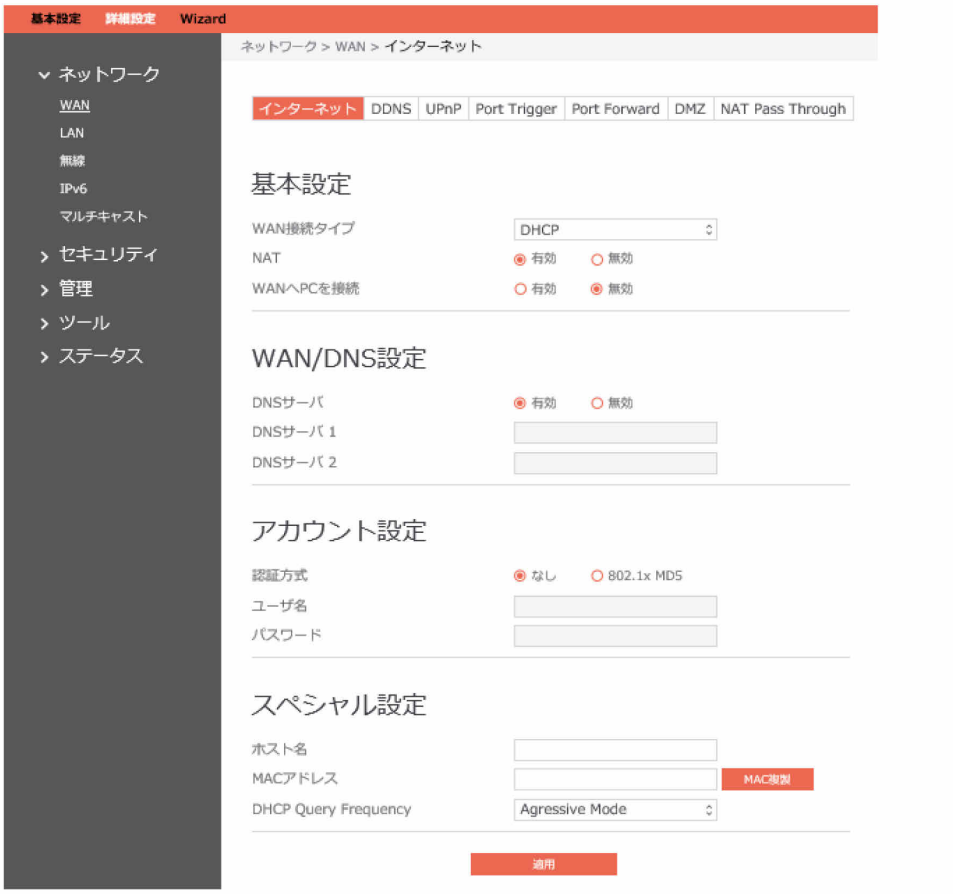
1.4 詳細設定

1.4.1 ネットワーク

1.4.1.1 WAN設定

1.4.1.1.1 インターネット設定

ルータは、いくつかのWAN接続タイプをサポートしています。
「WAN接続タイプ」ドロップダウンメニューからタイプを選択します。



WAN接続の設定を構成するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「WAN」→「インターネット」**の順にクリックします。
   WAN接続タイプ：インターネットサービスプロバイダーのタイプを選択します。**DHCP、PPPoE、Static IP（静的IPアドレス）、PPTP、L2TP**の5つのオプションがあります。どのタイプを選択したらよいかわからない場合は、ISPに問い合わせてください。
2. **NAT**：NAT（ネットワークアドレス変換）は、1つのパブリックIP（WAN IP）アドレスを使用して、LAN内のプライベートIPアドレスを持つネットワーククライアントにインターネットアクセスを提供するシステムです。各ネットワーククライアントのプライベートIPアドレスはNATテーブル内に保存され、受信データパケットをルーティングするために使用されます。
3. **WANへPCを接続**：PCをWANまたはLANのどちらにブリッジするかを切り替えます。
4. **DNSサーバ**：ルータがIPアドレスをDNSサーバから自動的に取得できるようにします。DNSサーバは、インターネット名を数値のIPアドレスに変換する、インターネット上のホストです。

5. **DNSサーバ1**：優先DNSサーバのIPアドレス。
   DNSサーバ2：代替DNSサーバのIPアドレス。
6. **認証方式**：802.1x MD5認証を使用するかどうか選択します（IEEE 802.1xは、ポートベースのネットワークアクセスコントロールのIEEE標準です）。
7. **ユーザ名**：802.1x MD5認証のユーザ名。
8. **パスワード**：802.1x MD5認証のパスワード。802.1x MD5認証のユーザ名。
9. **ホスト名**：ルータのホスト名を指定できます。通常、ホスト名はISPから提供されます。
10. **MACアドレス**：WANポートのMACアドレス。一部のISPは、自身のサービスに接続するデバイスのMACアドレスを監視し、新しいMACアドレスのインターネット接続を禁止します。
    この問題を解決するために、次のいずれかを実行してください。
    *ISPに連絡して、ISPサブスクリプションに関連付けられたMACアドレスを更新するよう要求します。
    *新しいデバイスのMACアドレスを元のデバイスのMACアドレスに一致するように複製または変更します。
11. **DHCP Query Frequency**：一部のISPは、デバイスのDHCPクエリの実行頻度が高すぎるとMACアドレスをブロックします。これを防ぐには、「DHCP Query Frequency」を変更します。
    デフォルトのアグレッシブモードでは、無線ルータがISPから応答を受信しない場合、20秒後に別のクエリを送信し、その後さらに3回再試行します。通常モードでは、無線ルータがISPから応答を受信しない場合、120秒後に2つ目のクエリを実行し、その後さらに2回再試行します。
12. **「適用」**をクリックします。

1.4.1.1.2 DDNS

DDNS（動的DNS）を設定すると、提供されている無線ルータDDNSサービスまたは別のDDNSサービス経由で、外部からルータへのアクセスを取得できるようになります。

DDNSを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「WAN」→「DDNS」**の順にクリックします。
2. **DDNSクライアント**：「有効」はDDNS機能を有効にし、「無効」はDDNS機能を無効にします。
3. **サーバ**：リストからサポートされているDDNSプロバイダーのURLを選択します。
4. **ホスト名**：更新されるホスト名を指定します。
5. **ユーザ名/E-mailアドレス**：DDNSプロバイダーでアカウント登録されているユーザ名またはEmailアドレスを入力します。
6. **パスワード/DDNSキー**：アカウント登録されているパスワードを入力します。
7. **「適用」**をクリックします。

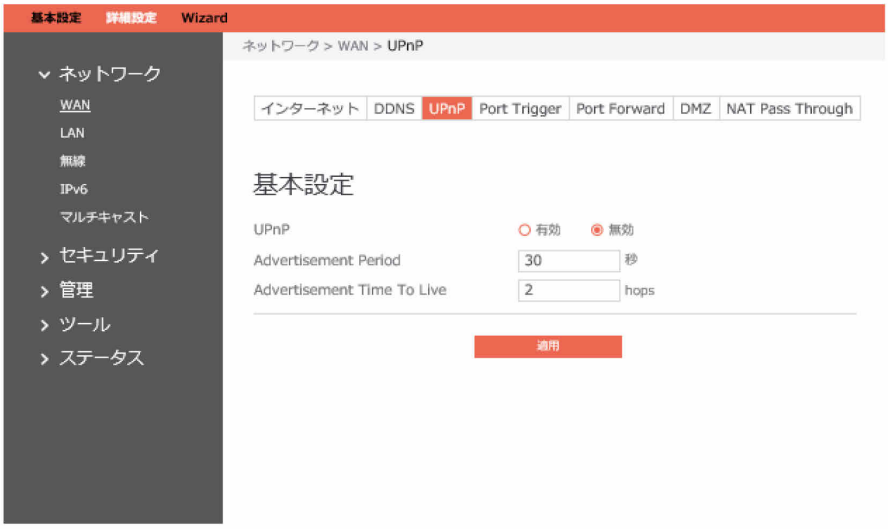
POINT

DDNSサービスは、次の条件のもとでは正しく機能しません。

- 黄色のテキストで示すように、無線ルータがプライベートWAN IPアドレス（192.168.x.x、10.x.x.x、または172.16.x.x）を使用している場合。
- ルータが複数のNATテーブルを使用するネットワーク上で動作している場合。

1.4.1.1.3 UPnP

UPnP（ユニバーサルプラグアンドプレイ）は、中央制御装置の有無にかかわらず、IPベースのネットワーク経由でデバイス（ルータ、テレビ、ステレオシステムなど）を制御できるようにします。UPnPのサポートにより、ネットワークに接続されたデバイスを検出した後、そのデバイスをP2Pアプリケーション、対話型のゲーム、ビデオ会議、Webまたはプロキシサーバなどをサポートするようにリモートで構成できます。ポートフォワーディングとは異なり、UPnPは受信接続を許可するようにルータを自動的に構成し、要求をローカルネットワーク上の特定のPCに転送します。

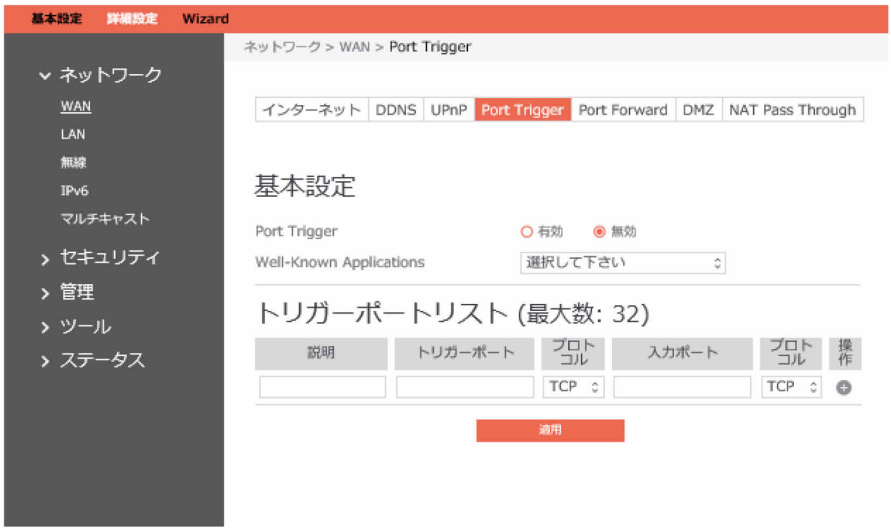


UPnPを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「WAN」→「UPnP」の順にクリックします。**
2. **UPnP**：「有効」はUPnPを有効にし、「無効」は無効にします。
3. **Advertisement Period**：UPnP情報をすべてのデバイスにブロードキャストするアドバタイズ期間（秒単位）を入力します。
4. **Advertisement Time To Live**：アドバタイズが転送されるホップ数を入力します。
5. **「適用」**をクリックします。

1.4.1.1.4 ポートトリガー（Port Trigger）

ポートトリガーメカニズムでは、最初にポート（**トリガーポート**）を定義します。LAN側のデバイスがこの定義されたポートにデータを書き込むと、**入力ポート**からの受信データは、このメカニズムをアクティブ化したデバイスの同じポートにフォワーディングされます。



ポートトリガーを設定するための手順：

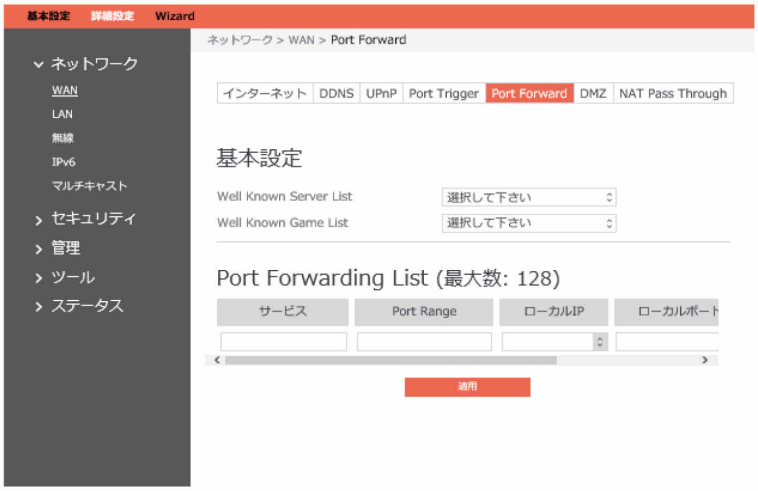
1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「WAN」→「ポートトリガー」**の順にクリックします。
2. **Port Trigger**：クリックしてポートトリガーを「有効」または「無効」にします。
3. **Well-Known Applications**：ポートトリガーリストに追加する一般的なゲームやWebサービスを選択します。
4. **説明**：アプリケーションの簡単な説明を入力します。
5. **トリガーポート**：LAN側のアプリケーションからこのポートへの受信データが存在する場合は、ポートトリガーメカニズムがアクティブ化されます。
6. **プロトコル：アプリケーションが使用するプロトコルのタイプを選択します。**
7. **入力ポート**：ポートの範囲を定義します。ポートトリガーメカニズムがアクティブ化されると、この範囲内のポートからのデータは、ポートトリガーメカニズムをアクティブ化したアプリケーションの対応するポートにフォワーディングされます。
8. **操作**：この項目に対する追加、編集、または削除操作を行います。
9. **「適用」**をクリックします。

POINT

リスト内の「トリガーポート」要素はトリガーと見なされます。つまり、このポートにデータが到着するとポートトリガーメカニズムがアクティブ化されます。

1.4.1.1.5 Port Forward

ポートフォワーディングは、ネットワークトラフィックをインターネットから指定されたポートに転送するために使用される方法です。ポートフォワーディングを設定すると、外部からのトラフィックが、LAN側のデバイスによって提供される指定のサービスへのアクセスを取得できるようになります。



POINT

ポートフォワードが有効になっている場合、ルータはインターネットからの未承認の受信トラフィックをブロックし、LANからの送信要求の応答のみを許可します。
ネットワーククライアントは直接インターネットにアクセスできず、その逆も同様です。

ポートフォワーディングを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「WAN」→「Port Forward」**の順にクリックします。
2. **Well Known Server List**：ドロップダウンメニューから定義済みのサーバリストを選択すると、「ポートフォワーディングリスト（Port Forwarding List）」に自動的に入力されます。
3. **Well Known Game List**：サーバリストからゲームを選択すると、「ポートフォワーディングリスト（Port Forwarding List）」に自動的に入力されます。
4. **サービス**：このサービスに関する短い説明を入力します。
5. **Port Range**：WAN側のポートの範囲を定義します。

POINT

- ネットワークはデータを交換するためにポートを使用し、各ポートにはポート番号と特定のタスクが割り当てられます。例えば、ポート80はHTTPに使用されます。特定のポートで同時に使用できるアプリケーションまたはサービスは1つのみです。そのため、2台のPCが同じポート経由で同時にデータにアクセスしようとすると失敗します。例えば、ポート100のポートフォワーディングを2台のPCで同時に設定することはできません。
- ネットワークのファイアウォールが無効になっているとき、WAN設定のためのHTTPサーバのポート範囲として80を設定した場合、HTTPサーバまたはWebサーバはルータのWebユーザインターフェイスと競合します。

6. **ローカルIP**：クライアントのLAN IPアドレスを入力します。
7. **ローカルポート**：フォワーディングされたパケットを受信する特定のポートを入力します。指定されたポート範囲に受信パケットをリダイレクトする場合は、このフィールドを空白のままにします。
8. **プロトコル**：必要なプロトコル。ホストしているサービスのドキュメントをご覧ください。

9. **操作**：この項目に対する追加、編集、または削除操作を行います。
10. **「適用」**をクリックします。

ポートフォワーディングモジュールが正常にアクティブ化されたかどうかを確認するための手順

- サーバまたはアプリケーションが設定され、動作していることを確認します。
- インターネットにアクセスできるLAN外部のクライアント（「インターネットクライアント」と呼ばれます）が必要になります。このクライアントは無線ルータに接続できません。
- インターネットクライアントでは、ルータのWAN IPアドレスを使用してサーバにアクセスします。ポートフォワーディングが成功した場合は、使用可能な、または指定されたファイルやアプリケーションにアクセスできるはずです。

ポートトリガーとポートフォワードの違い：

- ポートトリガーは、特定のLAN IPアドレスを設定しなくても機能します。静的LAN IPアドレスが必要なポートフォワーディングとは異なり、ポートトリガーでは、ルータを使用した動的ポートフォワーディングが可能です。受信接続を一定期間だけ許可するために、事前に定義されたポート範囲が構成されます。ポートトリガーでは、アプリケーションを複数のコンピューターが実行できます。通常は、ネットワーク上の各PCに同じポートを手動でフォワーディングする必要があります。
- ポートトリガーは、入力ポートが常に開いているわけではないため、ポートフォワーディングより安全です。これらのポートは、アプリケーションがトリガーポート経由で送信接続を行っている場合にのみ開かれます。

1.4.1.1.6 DMZ

仮想DMZモジュールは、1つのクライアントをインターネットに公開して、このクライアントがローカルエリアネットワーク宛てのすべての受信パケットを受信できるようにします。通常、インターネットからの受信トラフィックは破棄され、ネットワーク上でポートフォワーディングまたはポートトリガーが構成されている場合にのみ特定のクライアントにルーティングされます。DMZ構成では、1つのネットワーククライアントがすべての受信パケットを受信します。
ネットワーク上でのDMZの設定は、入力ポートを開いておく必要がある場合や、ドメイン、Web、またはE-mailサーバをホストする場合に役立ちます。

重要

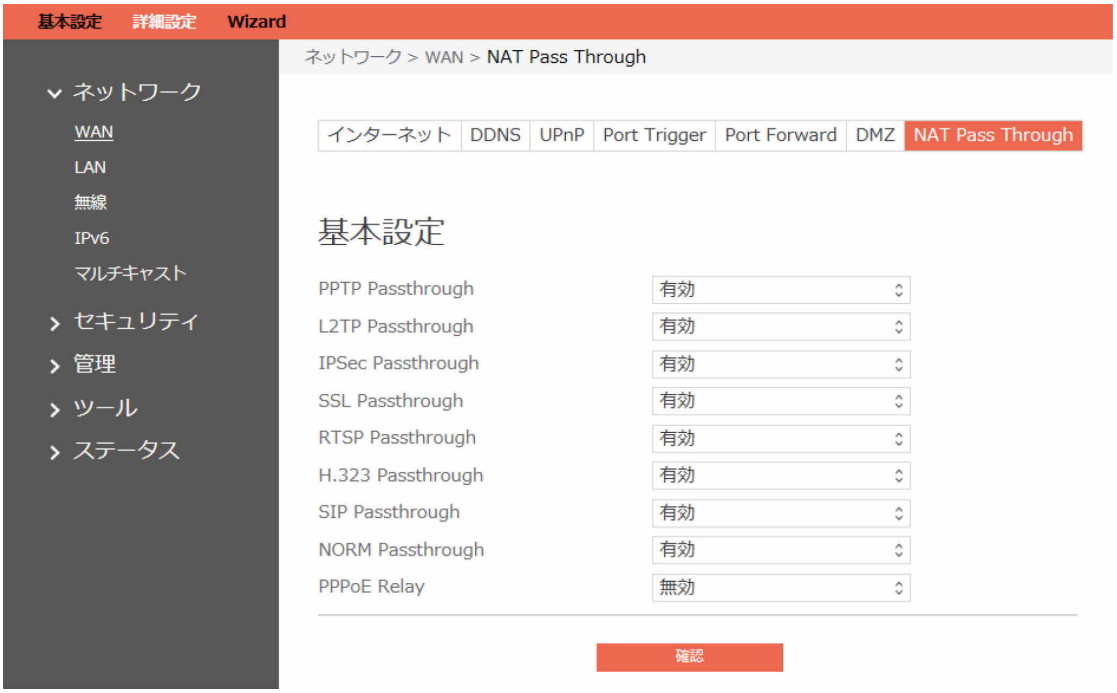
クライアントのすべてのポートをインターネットに開くと、そのネットワークが外部の攻撃に対して脆弱になります。DMZの使用に関連したセキュリティ上のリスクに注意してください。

DMZを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「WAN」→「DMZ」**の順にクリックします。
2. **DMZ**：クリックしてDMZを有効または無効にします。
3. **IP Address of Exposed Station**：DMZサービスを提供できるクライアントのLAN IPアドレス。これにより、このIPアドレスを持つデバイスがインターネットに公開されます。サーバクライアントに静的IPアドレスがあることを確認してください。
4. **「適用」**をクリックします。

1.4.1.1.7 NAT Pass Through

NATパススルーは、仮想プライベートネットワーク（VPN）接続でルータをネットワークサーバにパススルーできるようにします。



NATパススルーを設定するための手順：

1. NATパススルーの設定を構成するには、**「詳細設定」→「ネットワーク」→「WAN」→「NAT Pass Through」**の順にクリックします。
2. **PPTP Passthrough**：有効または無効にします。ポイントツーポイントトンネリングプロトコル（PPTP）は、仮想プライベートネットワークを実装するための方法です。
3. **L2TP Passthrough**：有効または無効にします。コンピューターネットワークでは、レイヤ2トンネリングプロトコル（L2TP）は、仮想プライベートネットワーク（VPN）をサポートするために、またはISPによるサービス提供の一部として使用されるトンネリングプロトコルです。これ自体では、暗号化や機密性は提供されません。
4. **IPSec Passthrough**：有効または無効にします。インターネットプロトコルセキュリティ（IPsec）は、通信セッションの各IPパケットを認証および暗号化することによってインターネットプロトコル（IP）通信をセキュリティ保護するためのプロトコルスイートです。
5. **SSL Passthrough**：有効または無効にします。Secure Sockets Layer（SSL）プロトコルは、セキュリティで保護されていないネットワーク経由でネットワークアプリケーションクライアントとサーバの間の接続をセキュリティ保護するためのコンピューターネットワークプロトコルです。
6. **RTSP Passthrough**：有効または無効にします。リアルタイムストリーミングプロトコル（RTSP）は、エンターテイメントおよび通信システムでストリーミングメディアサーバを制御するために設計されたネットワークコントロールプロトコルです。
7. **H.323 Passthrough**：有効または無効にします。H.323は、任意のパケットネットワーク上でオーディオビジュアル通信セッションを提供するプロトコルを定義するための、ITU電気通信標準化部門（ITU-T）からの推奨プロトコルです。

8. SIP Passthrough：有効または無効にします。セッション開始プロトコル（SIP）は、マルチメディア通信セッションを信号伝送および制御するための通信プロトコルです。SIPの最も一般的なアプリケーションは、音声およびビデオ通話のためのインターネットテレフォニーや、インターネットプロトコル（IP）ネットワーク全体にわたるインスタントメッセージングで使用されています。
9. NORM Passthrough：有効または無効にします。NACK-Oriented Reliable Multicast（NORM）トランスポートプロトコル。これは、汎用のIPマルチキャストルーティングおよびフォワーディングサービスにおける一括データオブジェクトまたはストリームの、信頼性に優れたエンドツーエンドでのトランスポートを提供できます。
10. PPPoE Relay：PPPoEリレーは、LAN内のデバイスでNATをパススルーする個別のPPPoE接続を確立できるようにします。
11. 完了したら、「次へ」をクリックします。

1.4.1.2 LAN設定

1.4.1.2.1 LAN

LAN IPモジュールを使用すると、管理者はルータのLAN側のIPアドレスを変更できます。

LAN IP設定を変更するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「LAN」→「LAN IP」**の順にクリックします。
2. **IPアドレス**：無線ルータのLAN IPアドレス。デフォルト値は192.168.1.1です。IPベースのネットワークでは、データパケットはネットワークデバイス固有のIPアドレスに送信されます。
3. **サブネットマスク**：無線ルータのLANサブネットマスク。そのデフォルト値は255.255.255.0です。
4. **「適用」**をクリックします。

POINT

LAN IPモジュールへの変更はすべて、ルータのDHCP設定に影響を与えます。

1.4.1.2.2 DHCPサーバ

DHCPサーバは各クライアントにIPアドレスを割り当てることができ、そのクライアントにDNSサーバのIPやデフォルトゲートウェイのIPなどを通知します。この無線ルータは、LAN側のデバイスに最大253のIPアドレスを割り当てることができます。

DHCPサーバを構成するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「LAN」→「DHCPサーバ」**の順にクリックします。
2. **DHCPサーバ**：DHCPサーバ機能を有効にし、ルータがDHCPサーバとして機能してネットワーククライアントにIPアドレスを自動的に割り当てられるようにします。この機能が無効になっている場合、管理者はLANデバイスを手動で設定する必要があります。
3. **ドメイン名**：DHCPサーバにIPアドレスを要求するクライアントのドメイン名を入力します。このフィールドには、英数字とダッシュ記号のみが含まれます。
4. **IP開始アドレス**：LAN側のデバイスに割り当てることができる開始アドレスを入力します。
5. **IP終了アドレス**：LAN側のデバイスに割り当てることができる終了アドレスを入力します。
6. **使用可能時間**：LAN側のデバイスが割り当てられたIPアドレスを使用できる時間を定義します。この使用可能時間が経過すると、ネットワーククライアントはDHCPサーバに更新または再バインドのメッセージを送信します。
7. **デフォルトゲートウェイ**：LANのゲートウェイのIPアドレスを入力します。。
8. **DNSサーバ**：DNSサーバのIPアドレスを入力します。DNSサーバは、DNSを数値のIPアドレスに解決するために使用されます。デフォルトでは、ルータがDNSサーバとして機能します。
9. **WINSサーバ**：Windowsインターネットネームサービスは、各PCのインターネットとの相互通信を管理します。WINSサーバを使用する場合は、ここでサーバのIPアドレスを入力します。

POINT

IP開始アドレス、IP終了アドレスはプライベートIPアドレスのみ指定可能で、グローバルIPアドレスには対応していません。グローバルIPアドレスに関してはP.107のPOINTを参照してください。

静的IP割り当て

1. **手動設定**：クライアントに固定IPアドレスを割り当てます。
2. **MACアドレス**：LAN側のデバイスのMACアドレス。
3. **IPアドレス**：LAN側のデバイスのDHCP IPプール内のIPアドレス。
4. **追加/削除**：静的IPアドレスを追加または削除します。
5. **「適用」**をクリックします。

POINT

- 管理者はIPアドレス範囲を指定する場合、192.168.1.xxx（ここで、xxxは2～254の任意の数値）のIPアドレス形式を使用することをお勧めします。
- 「IP開始アドレス」は、「IP終了アドレス」より大きくする必要があります。

1.4.1.3 無線設定

1.4.1.3.1 基本設定

基本設定では、基本的な無線設定を設定できます。

POINT

ルータは緊急モードを含む16個のSSIDをサポートしています。

基本的な無線設定を設定するための手順：

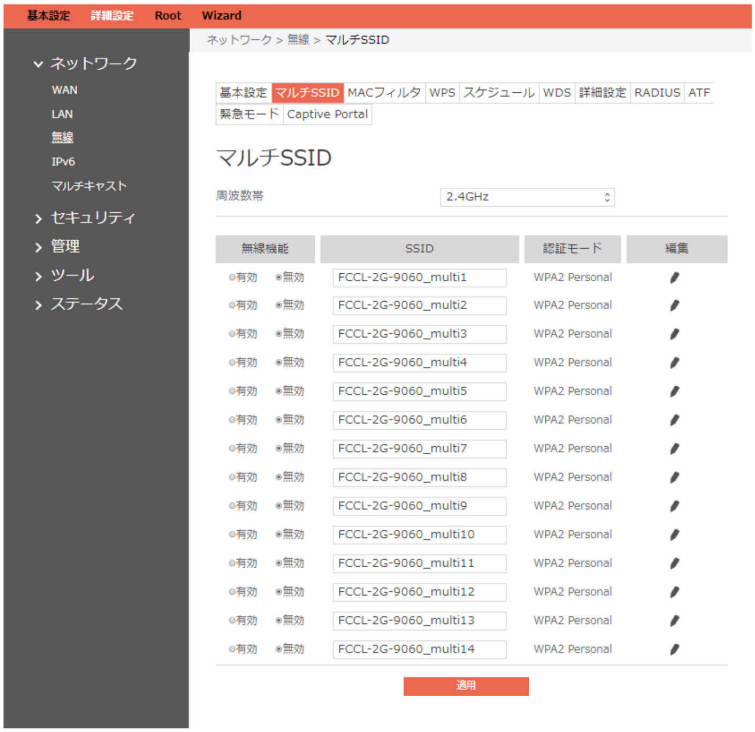
1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「基本設定」**の順にクリックします。
2. **周波数帯**：構成する周波数帯を選択します。
3. **無線機能**：SSIDのオン/オフ（有効/無効）を切り替えます。
4. **SSID**：無線ネットワークを識別するために、32文字未満の長さの名前が使用されます。Wi-Fiデバイスは、その通信範囲内のすべてのネットワークを自動的に検出します。
5. **ステルス(隠蔽)SSID**：「有効」が選択されている場合は、無線モバイルクライアントによるサイトの検索でSSIDが表示されず、SSIDを手動で入力することによってのみ無線ルータに接続されます。
6. **通信モード**：本製品では、次の無線規格に対応しています。接続する端末に応じて設定してください。
   - 2.4GHz : IEEE802.11b/IEEE802.11g/IEEE802.11n
   - 5GHz: IEEE802.11a/IEEE802.11n/IEEE802.11ac
7. **b/gプロテクション**：b/gプロテクション機能にチェックを付けると、IEEE802.11bとIEEE802.11gの通信が混在する環境で、IEEE802.11gのスループットが著しく落ちるのを防ぎます。ただし、IEEE802.11g単体通信の環境では、IEEE802.11bを抑制する信号を出すため、スループットが低下します。
8. **チャネルボンディング**：チャンネルボンディングは、複数の無線チャンネルを結合することで、通信速度を高めます。本機能を利用する場合は、接続する端末もチャネルボンディングに対応している必要があります。

9. **チャネル**：各無線通信モードで使用できる通信チャネルは、決まっています。無線LAN機器どうしでデータを送受信するためには、同じチャネルを使用する必要があります。同じチャネルに複数のSSIDが存在する場合は、アクセスポイントのチャネルを変更してください。
10. **セカンダリチャネルオフセット**：2.4GHzでチャネルボンディングを利用かつチャネルを固定する場合、まとめるチャネルを上にするか下にするかを決める必要があります。
11. **認証モード**：このフィールドは、無線クライアントの認証方法を有効にします。
12. **暗号化モード**：データを暗号化するための暗号化モードを有効にします。
13. **事前共有キー(PSK)**：暗号化プロセスを開始するには、8～63文字（文字、数字、またはその組み合わせ）あるいは16進数8～64桁のパスワードが必要です。
14. Protected Management Frames：管理フレーム保護は、承認解除、関連付け解除、アクションフレームなどの一部のタイプの管理フレームを保護する機能です。
15. **最大端末数**：許可されるクライアントの最大数を指定します。
16. **キー更新間隔**：このフィールドは、WPAグループキーが変更されるまでの間隔（秒単位）を指定します。キーの定期的な変更が必要ないことを示すには、0（ゼロ）を入力します。600～86400の値（秒単位）を入力してください。
17. **「適用」**をクリックします。

1.4.1.3.2 マルチSSID

マルチSSID設定では、複数のSSID設定を設定できます。

マルチSSIDモジュールを設定するための手順：



1. **周波数帯**：構成する周波数帯を選択します。
2. **無線機能**：SSIDのオン/オフ（有効/無効）を切り替えます。
3. **SSID**：ネットワーク名またはSSIDは、無線ネットワークを識別する一意の名前です。Wi-Fiデバイスは、範囲内のすべてのネットワークを自動的に検出します。無線接続の最大32文字の識別文字列を割り当てます。
4. **編集**：編集アイコン（ ）をクリックすると、マルチSSIDモジュールの詳細を設定できます。
   - 4-1. **ステルス(隠蔽)SSID**：「有効」が選択されている場合は、無線モバイルクライアントによるサイトの検索でSSIDが表示されず、SSIDを手動で入力することによってのみ無線ルータに接続されます。
   - 4-2. **認証モード**：無線クライアントの認証方法を有効にします。
   - 4-3. **暗号化モード**：データを暗号化するための暗号化モードを有効にします。
   - 4-4. **事前共有キー(PSK)**：暗号化プロセスを開始するには、8～63文字（文字、数字、または その組み合わせ）あるいは16進数64桁のパスワードが必要です。
   - 4-5. **Protected Management Frames**：管理フレーム保護は、承認解除、関連付け解除、アクションフレームなどの一部のタイプの管理フレームを保護する機能です。
   - 4-6. **キー更新間隔**：このフィールドは、WPAグループキーが変更されるまでの間隔（秒単位）を指定します。キーの定期的な変更が必要ないことを示すには、0（ゼロ）を入力します。1～2592000の値（秒単位）を入力してください。
   - 4-7. **最大端末数**：許可されるクライアントの最大数を入力します。
   - 4-8.**「確認」**をクリックします。
5. 完了したら、**「適用」**をクリックします。

1.4.1.3.3 MACフィルタ

ネットワーク上で無線のMACフィルタを使用すると、ブラックリストとホワイトリストを使用して、特定のデバイスへの無線ネットワークアクセスが許可または拒否されます。

POINT

MACフィルタは、WPSが無効になっている場合にのみ有効になります。

無線のMACフィルタを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「MACフィルタ」**の順にクリックします。
2. **周波数帯**：構成する周波数帯を選択します。
3. **SSID**：SSIDグループを選択します。
4. **MACフィルタ**：MACフィルタのオン/オフ（有効/無効）を切り替えます。
5. **MACフィルタモード**：フィルタモードには、「許可」と「拒否」の2種類があります。「許可」は、ルータがリストで定義されている指定されたサービスを処理でき、「拒否」は、ルータが指定されたサービスの処理を拒否します。
6. **MACアドレスリストをインポート**：MACアドレスリストのcsvファイルをインポートします。

MACアドレスリストの手動での追加/削除：

1. **MACフィルタリスト**：無線クライアントのMACアドレスを入力します。
2. MACアドレスを追加するには、**「追加」**をクリックします。
3. MACアドレスを削除するには、**「削除」**をクリックします。

1.4.1.3.4 WPS

WPS（Wi-Fi Protected Setup）は、デバイスを無線ネットワークに容易に接続できる無線のセキュリティ標準です。WPS機能は、PINコードまたはWPSボタンを使用して構成できます。WPSは、オープンシステム、WPAパーソナル、およびWPA2パーソナルの認証をサポートしています。共有キー、WPAエンタープライズ、WPA2エンタープライズ、およびRADIUSはサポートされていません。

WPSを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「WPS」**の順にクリックします。
2. **周波数帯**：WPSの動作帯域（2.4GHzまたは5GHz）を選択します。動作帯域を変更するには、最初にWPS機能を無効にしてください。
3. **WPS機能**：WPSを有効にするには「有効」を選択します。これにより、デバイスを無線ネットワークに接続するプロセスを簡略化できます。

   POINT

   WPSは、オープンシステム、WPAパーソナル、およびWPA2パーソナルを使用した認証をサポートしています。WPSでは、共有キー、WPAエンタープライズ、WPA2エンタープライズ、およびRADIUSの暗号化方式を使用する無線ネットワークをサポートしていません。

4. **接続状態**：WPSの接続状態が表示されます。
5. **WPSステータス**：WPSの構成された状態が表示されます。
6. **APピンコード**：これは、ルータのWPS PINコードです。接続を行うには、これをクライアントのWPSユーティリティで入力します。
7. **WPS方式**：PIN（個人情報番号）方式では、無線接続を確立するためにPIN番号を入力する必要があります。PBC（プッシュボタン構成）方式では、無線接続を確立するためにボタン（このページの「開始」または物理的なWPSボタン）を押す必要があります。

8. ルータのWPSボタンを使用してWPSを設定するには：
   a) 「開始」をクリックするか、または無線ルータの背面にあるWPSボタンを押します。
   b) 無線デバイスのWPSボタンを押します。これは通常、WPSロゴによって識別できます。

   POINT

   WPSボタンの場所については、無線デバイスまたはそのユーザマニュアルを確認してください。

9. クライアントのPINコードを使用してWPSを設定するには：
   a) 無線デバイスのユーザマニュアルまたはデバイス自体にあるWPS PINコードをみつけます。
   b) テキストボックスにクライアントのPINコードを入力します。
   c) **「開始」**をクリックして、無線ルータをWPS検索モードにします。WPS設定が完了するまで、ルータのLEDインジケーターが3回すばやく点滅します。
10. **PINコード**：PIN方式を使用して接続するクライアントのWPS PINコード。
11. 完了したら、**「開始」**をクリックします。

1.4.1.3.5 スケジュール

スケジュールでは、指定された時間にWi-Fiが有効になるように管理できます。

スケジュールを設定するための手順：

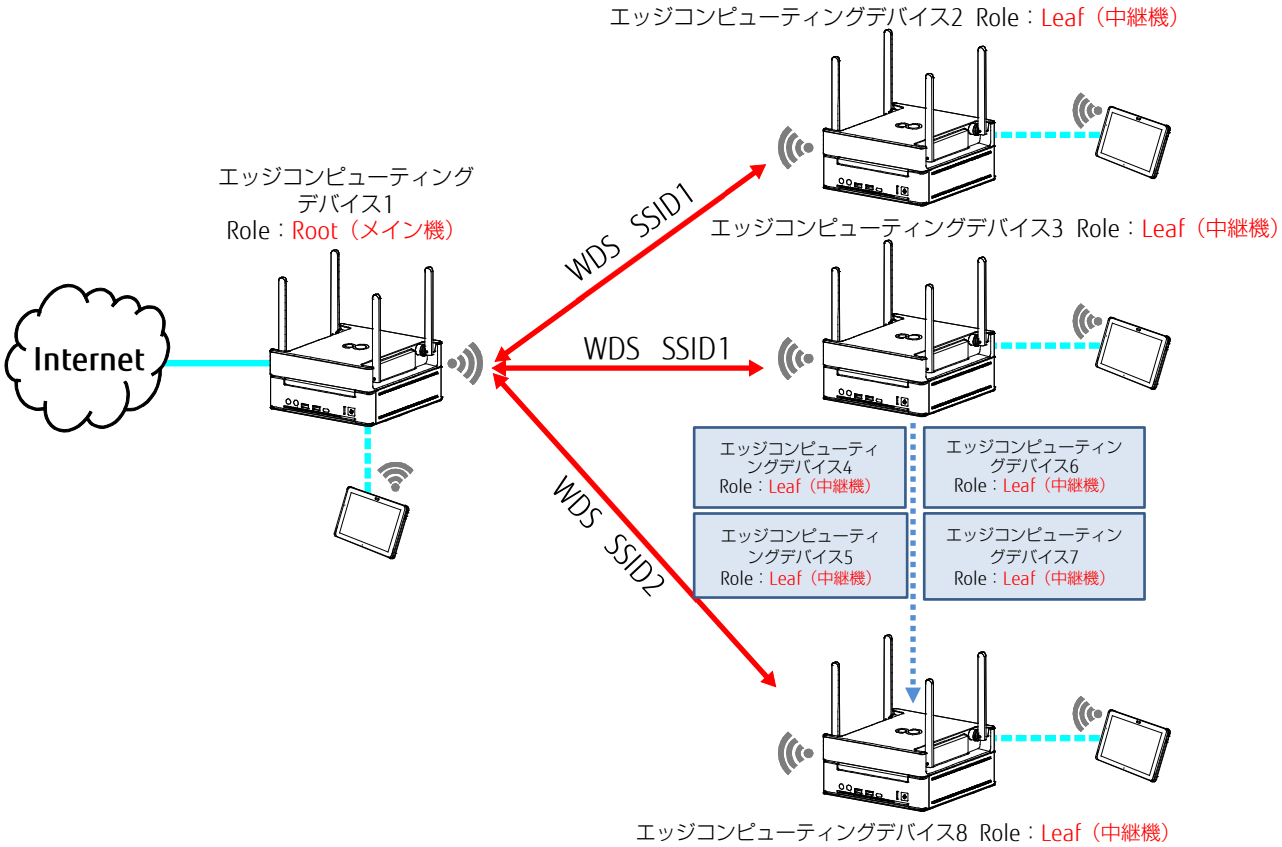
1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「スケジュール」**の順にクリックします。
2. **無線スケジューラ**：無線のスケジュールのオン/オフを切り替えます。
3. **有効にする曜日（平日）**：Wi-Fiを有効にする平日を選択します。
4. **有効にする時間**：Wi-Fiを有効にする平日の時間を設定します。
5. **有効にする曜日（週末）**：Wi-Fiを有効にする休日を選択します。
6. **有効にする時間**：Wi-Fiを有効にする週末の時間を設定します。
7. 完了したら、**「適用」**をクリックします。

1.4.1.3.6 WDS

Wireless Distribution System（WDS）は、IEEE 802.11ネットワーク内にあるアクセスポイント（AP）の無線の相互接続を有効にするシステムです。
従来の要件であったリンクのための有線バックボーンも必要なく、複数のアクセスポイントを使用して無線ネットワークを拡張できます。
WDSには、次の2つの役割があります。
メイン機APは、無線ネットワークのルートノードです。
中継機APは無線ネットワークのリーフノードであり、中継機APはメイン機APに接続します。

POINT

- WDSセキュリティは、「なし（None）」、「WPAパーソナル」、「WPA2パーソナル」、「WPA/WPA2パーソナルの混在（Mixed WAP / WPA2 Personal）」をサポートしています。
- WDS機能は、2つのレイヤに制限されます。
- WDS機能は、他社製品との組み合わせでは動作しません。



図は、WDSトポロジの例を示しています。

WDSの基本設定のための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「WDS」**の順にクリックします。
2. **WDS**：WDS機能を有効または無効に切り替えます。
3. **周波数帯**：WDSの動作帯域（2.4GHzまたは5GHz）を選択します。
4. **メイン機/中継機**：WDSには、メイン機モードと中継機モードがあります。メイン機APは、無線ネットワークのルートノードです。中継機APは無線ネットワークのリーフノードであり、中継機APはメイン機APに接続します。

WDSの中継機設定のための手順：

1. **SSID**：メイン機APのSSID名を設定します。
2. **認証モード**：このフィールドは、無線クライアントの認証方法を有効にします。
3. **事前共有キー(PSK)**：暗号化プロセスを開始するには、8～63文字（文字、数字、またはその組み合わせ）あるいは16進数8～64桁のパスワードが必要です。

1.4.1.3.7 詳細設定

詳細設定モジュールは、詳細な構成オプションを提供します。

無線機能設定のための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「詳細設定」**の順にクリックします。
2. **周波数帯**：ルータが動作している周波数帯を選択します。
3. **無線機能**：無線機能（無線ネットワーク）を有効にするには「有効」を選択します。無線機能（無線ネットワーク）を無効にするには「無効」を選択します。
4. TX Bursting：TXバーストは、ルータと802.11gデバイスの間の転送速度を向上させます。
5. Tx Power Adjustment：伝送電力の性能を設定します。最大値は100%です。無線を最大範囲まで必要としない場合は、電力を節約し、セキュリティを強化することができます。ローミング環境を構築する際には、本機能で電波強度の調整を行うことができます。

   POINT

   伝送電力の調整値を大きくすると、無線ネットワークの安定性に影響を与える可能性があります。

6. OBSS RSSI：OBSS RSSIのしきい値を構成します。OBSS RSSIが構成された値を超えた場合は、20 MHzに移動します。
7. RTS Threshold：ネットワークトラフィックが多く、無線デバイスが多すぎるようなビジー状態やノイジー状態の無線ネットワークで無線通信を改善するには、RTS（送信要求）のしきい値として小さい値を選択します。
8. Fragmentation Threshold：フラグメントのしきい値を設定します。これはフラグメントの最大サイズです。
9. Beacon送信間隔：ビーコン送信間隔は、あるビーコンと次のビーコンの間の期間を示します。デフォルト値は100です（単位はミリ秒、つまり1/1000秒です）。ビーコン送信間隔を短くすると、不安定な環境での転送パフォーマンスやクライアントをローミングするための転送パフォーマンスが向上しますが、電力消費が大きくなります。
10. AMPDU Aggregation：インターフェイス全体のTx AMPDUアグリゲーションを有効または無効にします。これが無効になっていると、アグリゲーションフレームの受信は引き続き実行されますが、アグリゲーションフレームは転送されません。

11. DCS：CW干渉を検出して回避する機能であるDCS機能を有効または無効にします。
12. 完了したら、「適用」をクリックします。

AP設定のための手順：

1. TX STBC：送信（TX）方向のSpace Time Coding Block（STBC）機能（802.11n仕様に記述されています）を有効または無効にします。
2. RX STBC：受信（RX）方向のSpace Time Coding Block（STBC）機能（802.11n仕様に記述されています）を有効または無効にします。
3. プライバシー保護：無線デバイスが互いに通信しないようにします。この機能は、多数のゲストが頻繁にネットワークに参加したり、ネットワークから離れたりする場合に役立ちます。この機能を有効にするには「有効」を、無効にするには「無効」を選択します。

   POINT

   本製品のアクセスポイント部を通して接続している端末同士は、この設定が無効になっている場合は通信できません。
   そのためPINGにも応答しません。
4. Multicast Transmission Mode：マルチキャスト転送モードを選択します。
5. Multicast Rate (Mbps)：マルチキャストの転送レートを選択します。
6. Short Guard Interval：ルータがCRC（巡回冗長検査）に費やす時間の長さを定義します。CRCは、データ転送中にエラーを検出するための方法です。ネットワークトラフィックが多い、ビジー状態の無線ネットワークでは「有効」を選択します。
7. DTIM Priod：DTIM（Delivery Traffic Indication Message）間隔またはデータビーコンレートは、スリープモードの無線デバイスに、データパケットが配信を待機中であるという信号が送信されるまでの時間間隔です。 デフォルト値は3ミリ秒です。

8. WMM：無線通信時に、特定の通信にのみ優先順位を付ける場合に有効にします。WMMをオフに切り替えるには「無効」を選択します。
9. WMM APSD：無線デバイス間の電源管理を向上させるためにWMM APSD（Wi-Fi Multimedia Automatic Power Save Delivery）を有効にします。WMM APSDをオフに切り替えるには「無効」を選択します。
10. Turbo QAM：256-QAM（MCS 8/9）のサポート。無線モードが自動に設定されている必要があります。
11. Universal Beamforming：ビームフォーミングをサポートしていない従来の無線ネットワークアダプタの場合、ルータがチャネルを予測し、ダウンリンク速度を向上させるためのステアリング方向を決定します。（暗黙的ビームフォーミングとも呼ばれます。）
12. Radio Resource Management：802.11kを有効または無効にします。
13. WMM-Admission Control：WMMアドミッションコントロールを有効または無効にします。
14. 完了したら、**「適用」**をクリックします。

1.4.1.3.8 RADIUS

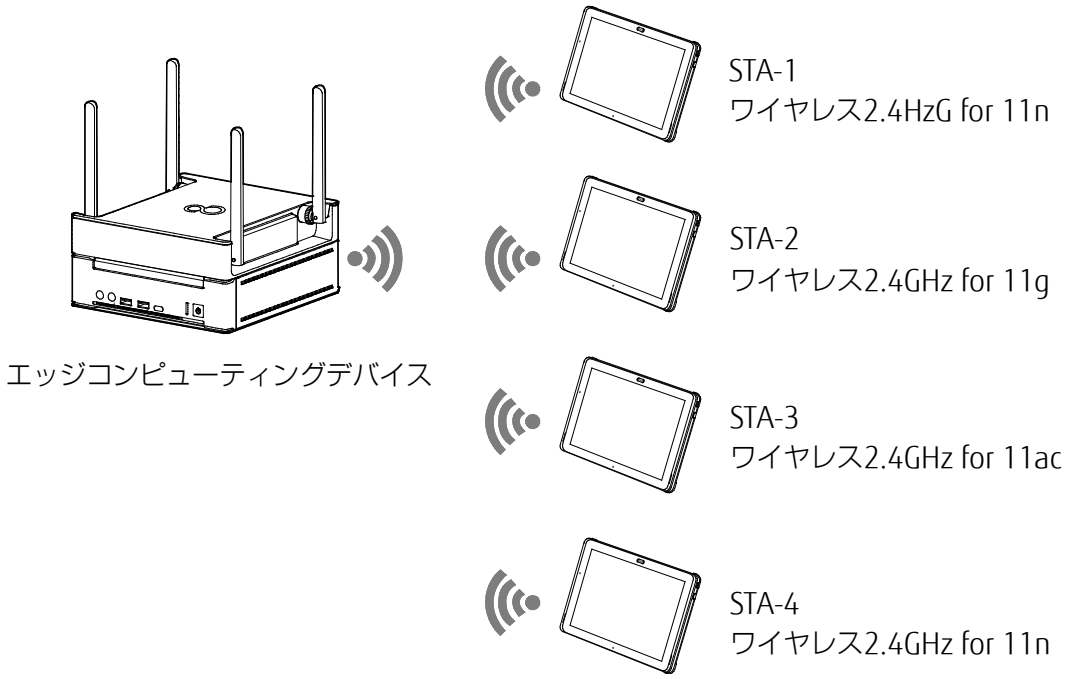
RADIUS（Remote Authentication Dial In User Service）設定は、認証モードとして802.1xでWPAエンタープライズ、WPA2エンタープライズ、またはRADIUSが選択された場合に、セキュリティの追加のレイヤを提供できます。

RADIUSを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「RADIUS」**の順にクリックします。
2. **周波数帯**：「周波数帯」フィールドで、RADIUS設定に使用する周波数帯を選択します。
3. **サーバIP**：無線認証および動的WEPキー派生のためのRADIUSサーバのIPアドレスを入力します。
4. **サーバポート**：RADIUSサーバへの接続のためのUDPポート番号を入力します。
5. **サーバシークレット**：RADIUSサーバに接続するためのパスワード。
6. 完了したら、**「適用」**をクリックします。

1.4.1.3.9 ATF

ATF（エアタイムフェアネス）モジュールは、ビジー状態または使用頻度の高い環境でより優れたパフォーマンスを実現するために、Wi-Fiデバイスの混合レートをサポートしています。



図は、ATFトポロジの例を示しています。

ATFを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「ATF」**の順にクリックします。
2. **ATF機能**：有効または無効にします。ATFでは、アクセスポイント（AP）からのトラフィックの転送や、Wi-Fi帯域幅の効率的な使用のために、主にスケジューリングの公平性に重点を置くことが必要になります。
3. **周波数帯**：「周波数帯」フィールドで、ATF設定に使用する周波数帯を選択します。

4. **ATFモード**：エアタイムフェアネスでは、strict-queueアルゴリズム（厳密キューアルゴリズム）とfari-queueアルゴリズム（公平キューアルゴリズム）という、互いに排他的な2つのスケジューリングアルゴリズムを実装します。strict-queueアルゴリズムは、ユーザによって構成された厳密なエアタイム割り当てに従い、未使用の帯域幅の利用を試行することはしません。fari-queueアルゴリズムは、輻輳した環境でも構成されたエアタイムを保証し、未使用の帯域幅も利用します。
5. **SSID**：ATFによって制御されるSSIDを設定します。
6. **Air時間(%)**：ATFコントロールに使用されるSSIDの割合（%）を設定します。

   POINT

   エアタイムの割合（%）のデフォルト値は、0（ゼロ）です。これは、SSIDへのエアタイムの平均の割り当てを示します。

7. **「適用」**をクリックします。

1.4.1.3.10 緊急モード

緊急モードでだれでもアクセスポイントを使用できるように、アクセスポイントのパブリック無線LANモードへの設定を有効にします。

緊急モードのSSID設定のための手順：

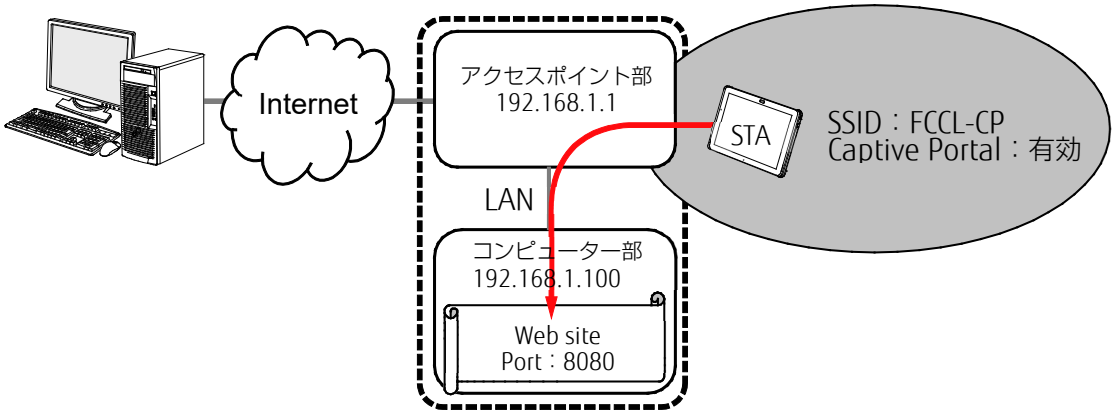
1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「緊急モード」**の順にクリックします。
2. **緊急モード**：緊急モード機能の有効または無効を切り替えます。
3. **周波数帯**：「周波数帯」フィールドで、緊急モードのSSID設定に使用する周波数帯を選択します。

SSID設定を設定するための手順：

1. **SSID**：無線ネットワークを識別するために、32文字未満の長さの名前が使用されます。Wi-Fiデバイスは、その通信範囲内のすべてのネットワークを自動的に検出します。
2. **ステルス(隠蔽)SSID**：「有効」が選択されている場合は、無線モバイルクライアントによるサイトの検索でSSIDが表示されず、SSIDを手動で入力することによってのみ無線ルータに接続されます。
3. **認証モード**：このフィールドは、無線クライアントの認証方法を有効にします。
4. **最大端末数**：許可されるクライアントの最大数を指定します。
5. **MACフィルタ**：MACフィルタのオン/オフ（有効/無効）を切り替えます。
6. 完了したら、**「適用」**をクリックします。

1.4.1.3.11 Captive Portal設定

Captive PortalはSTAがインターネットを利用する前に、ネットワーク上の特定のWeb siteの参照（通常は認証目的で）を強制する機能です。



図は、Captive Portal設定の例を示しています。

Captive Portalの設定手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「無線」→「Captive Portal」**の順にクリックします。
2. **Captive Portal有効：** Capative Portalを使用する場合は、「有効」を選択します。「有効」を選択すると、各種設定項目と設定済みSSIDリストが表示されます。
3. **Forward IP：**インターネット接続前に転送したいWeb siteのIPアドレスを入力します。（図の場合、コンピューター部のIPアドレス：192.168.1.100）
4. **Forward Port：**転送時のポート番号を入力します。（図の場合、Web siteのポート：8080）
5. **Captive Portal有効（SSIDリスト）：**Captive Portal設定対象のSSIDについて、「有効」を選択します（図の場合、FCCL-CP）。

1.4.1.4 IPv6

このモジュールは、IPv6に関連したいくつかの基本的な機能を設定するために使用されます。IPv6サービスはまだ広く普及していないため、ISPに連絡してIPv6サービスが提供されているかどうかを確認してください。

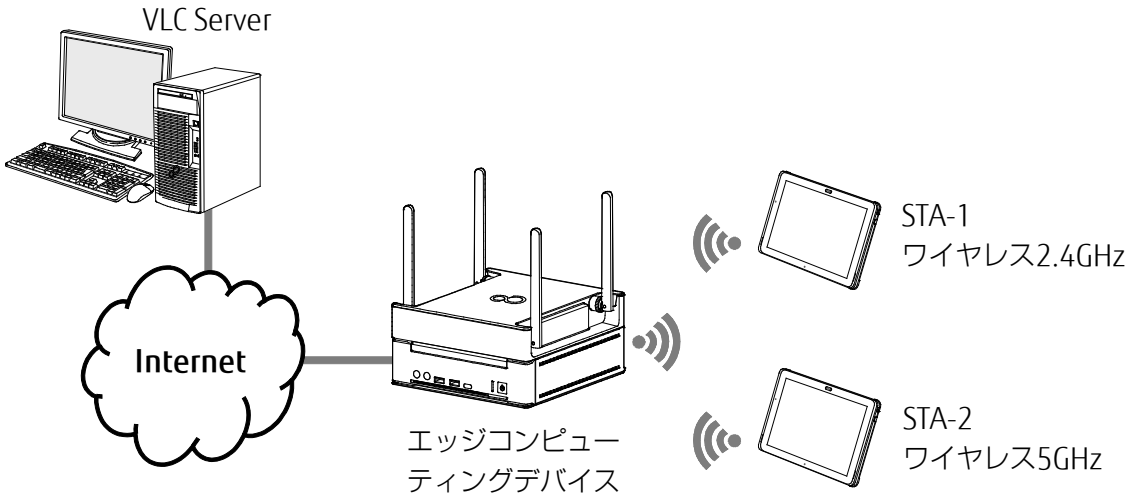
IPv6を設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「IPv6」**の順にクリックします。
2. **通信タイプ**：IPv6の通信タイプを選択して「無効」、「Native」、「Static IPv6」を構成します。
3. **WAN IPv6 MTU**：WANインターフェイスのIPv6 MTU（最大転送ユニット）を設定します。
4. **ユーザクラスオプション**：DHCPv6クライアントが請求メッセージでDHCPv6サーバに送信するORO のユーザクラスオプション（15）を指定します。
5. **LAN**：ルータのLAN側のデバイスへのIPv6アドレスの割り当てを有効または無効にします。
6. **Simultaneous**：LANインターフェイスに接続されているホストがIPv6アドレスを取得できるモード。有効になっている場合、ホストは同時ステートレスまたはステートフルでIPv6アドレスを取得します（DHCPプールスタートおよびエンド値が必要です）。無効になっている場合、ホストはステートレスまたはステートフルで同時にIPv6アドレスを取得せず、代わりにモードが選択されている必要があります。

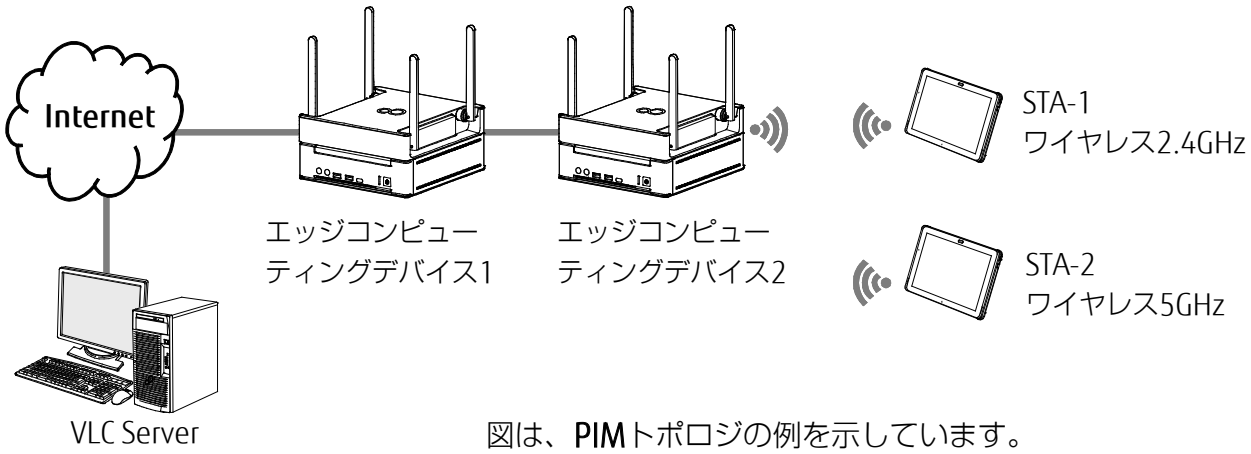
7. **LAN IPv6アドレス**：LANインターフェイスのIPv6アドレスを設定します。
8. **LANプレフィクス長**：LANインターフェイスのIPv6プレフィクス長を設定します。
9. **LAN IPv6プレフィクス**：LANインターフェイスのプレフィクスを設定します。
10. **Pool Setting For Lan Host**：LAN側のデバイスへの範囲内のIPv6アドレスの割り当てを有効または無効にします。
11. **DHCPプールスタート**：プール開始アドレスを設定するDHCPv6アドレス。
12. **DHCPプールエンド**：プール終了アドレスを設定するDHCPv6アドレス。
13. **LAN IPv6 MTU**：LAN側のデバイスのMTUを設定します。
14. **DNSサーバへ自動接続**：アップリンクから手動でDNSを取得する場合に選択します。
15. **IPv6 DNS サーバ 1**：優先DNSサーバ1のIPv6アドレス。
16. **IPv6 DNS サーバ 2**：代替DNSサーバ2のIPv6アドレス。
17. **IPv6 DNS サーバ 3**：DNSサーバ2以外の代替DNSサーバのIPv6アドレス。
18. **「適用」**をクリックします。

1.4.1.5 マルチキャスト

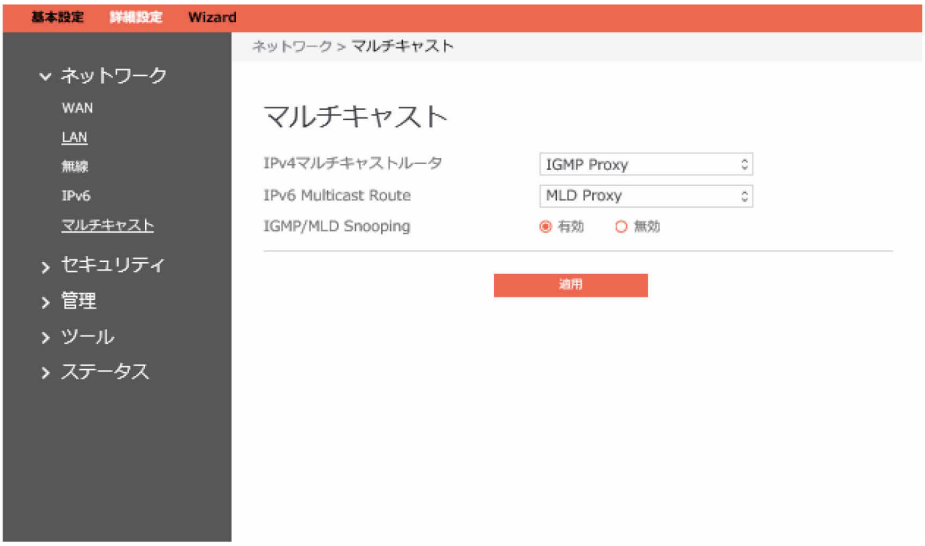
マルチキャストを有効にします。送信者と受信者は、ポイントツーマルチポイント接続を実現します。



図は、**マルチキャスト**（プロキシ/スヌーピング）トポロジの例を示しています。



図は、**PIM**トポロジの例を示しています。



マルチキャストを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ネットワーク」→「マルチキャスト」**の順にクリックします。
2. **IPv4マルチキャストルータ**：IPv4マルチキャストルータを選択します。
   IGMPプロキシ：IGMPプロキシは、ダウンストリームルータに直接接続されていない単方向リンクルーティング（UDLR）環境内のホストが、アップストリームネットワークをソースとするマルチキャストグループに参加できるようにします。
   PIM：PIM Source Specific Multicast（SSM）はIPv4/IPv6で使用される、マルチキャストパケットを配信するための方法です。この場合、受信者に配信されるパケットは、その受信者が要求した特定のソースアドレスから発信されたパケットだけになります。ソースを制限することによって、SSMはネットワークに対する要求を軽減し、セキュリティを強化します。
3. **IPv6 Multicast Route**：IPv6マルチキャストルータを選択します。
   MLDプロキシ：MLDプロキシは、IPv6環境で使用されます。この機能を使用すると、デバイスはプロキシグループのメンバーシップ情報を学習し、その情報に基づいてマルチキャストパケットを転送できます。デバイスがルートプロキシエントリのRPとして機能している場合は、これらのエントリのMLDメンバーシップレポートを、ユーザが指定したプロキシインターフェイス上で生成できます。
4. **Enable IGMP/MLD Snooping**：スヌーピングを有効にするには「有効」を、スヌーピングを無効にするには「無効」をクリックします。IGMP/MLDスヌーピングは、Internet Group Management Protocol（IGMP）/Multicast Listener Discovery（MLD）ネットワークトラフィックを待機するプロセスです。この機能を使用すると、ネットワークスイッチはホストとルータの間のIGMP/MLD対話を待機できます。これらの対話を待機することによって、スイッチは、どのリンクにどのIPマルチキャストストリームが必要かを示すマップを保持します。マルチキャストは、それを必要としないリンクからフィルタリングされる可能性があるため、特定のマルチキャストトラフィックをどのポートが受信するかを制御します。
5. 完了したら、**「適用」**をクリックします。

1.4.2 セキュリティ

1.4.2.1 VPN

VPN（仮想プライベートネットワーク）は、インターネットなどのパブリックネットワークを使用して、リモートコンピューターまたはリモートネットワークに安全な通信を提供します。

1.4.2.1.1 PPTP VPNサーバ

VPNサーバを使用すると、管理者はいつでも、どこでもホームネットワークへのアクセスを取得できます。

POINT

VPN接続を設定する前に、アクセスしようとしているVPNサーバのIPアドレスまたはドメイン名が必要です。

PPTP VPNサーバへのアクセスを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「VPN」→「PPTP VPNサーバ」**の順にクリックします。
   - **VPNサーバ**：PPTP VPNサーバを有効または無効にします。
   - **VPN詳細**：PPTP VPNサーバの詳細。「基本設定」または「詳細設定」を選択します。
   - **ユーザ名とパスワード**：PPTP VPNサーバのユーザ情報。VPNサーバのユーザ名とパスワードを入力し、⊕ボタンをクリックします。
2. 次のように、VPNサーバの詳細を設定します。

- **ブロードキャストサポート**：ルータからクライアントへのブロードキャストリレーをオンにします。
- **Authorization Mode**：承認モードを選択します。
- **MPPE Encryption**：MPPE暗号化のタイプを選択します。
- **DNSサーバへ自動接続**：PPTPクライアントのDNSサーバへの自動接続を指定します。
- **WINSサーバへ自動接続**：PPTPクライアントのWINSへの自動接続を指定します。。
- **MRU/MTU**：最大受信ユニット（MRU）または最大転送ユニット（MTU）サイズは、PPTPセッション中に使用するPPTPパラメーターの一部としてクライアントに送信されます。変更によってPPTPセッションに関する既知の問題が修正されることが確かでない限り、MTUまたはMRU値を変更しないことをお勧めします。MTUまたはMRU値が正しくないと、PPTP VPN経由のトラフィックが失敗します。
- **Client IP Address**：PPTPクライアントのIPアドレス範囲を指定します。
- **「適用」**をクリックします。

1.4.2.1.2 OpenVPNサーバ

VPNサーバを使用すると、いつでも、どこでもホームネットワークにアクセスできます。

OpenVPNサーバを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「VPN」→「OpenVPNサーバ」**の順にクリックします。
   - **VPNサーバ**：OpenVPNサーバ機能を有効または無効にします。
   - **VPN詳細**：VPNサーバの詳細を入力します。「基本設定」または「詳細設定」を選択します。
   - **ユーザ名とパスワード**：OpenVPNサーバのユーザ情報。VPNサーバのユーザ名とパスワードを入力し、⊕ ボタンをクリックします。

2. VPNサーバの詳細設定：

- **インターフェイスタイプ**：「TUN」はルーティングされたIPトンネルを作成し、「TAP」はイーサネットトンネルを作成します。
- **プロトコル**：TCPまたはUDPサーバ。
- **サーバポート**：OpenVPNサーバが待機するTCP/UDPポート。

- ファイアウォール：VPNサーバのファイアウォール構成。「Auto」は完全なファイアウォール構成を作成し、「External only」は基本的なファイアウォール構成を作成し、「Custom」はファイアウォール構成を作成しません。
- Authorization Mode：承認モードを選択します。
- Username / Password auth. Only：「はい」では認証にユーザ名とパスワードのみが必要であり、「いいえ」では認証証明書も必要になります。
- Extra HMAC Authorization：有効になっている場合は、サーバでtls_authキーが使用されます。どのクライアントにもこのキーが必要です。
- VPN Subnet / Subnet Mask：VPNサブネットとサブネットマスクの設定。
- Poll Interval：VPNサーバ起動のcrontabの時間間隔。
- Push LAN to Clients：クライアントにルートをプッシュして、そのクライアントがサーバの背後にある他のプライベートサブネットに到達できるようにします。
- All traffic through VPN：有効になっている場合、このディレクティブはすべてのクライアントで、デフォルトネットワークゲートウェイがVPNを経由してリダイレクトするように構成して、Web閲覧やDNS参照などのIPトラフィックがすべてVPNを経由するようにします。
- Respond to DNS：クライアントにDNSをプッシュします。
- Encryption Cipher：暗号化方式を選択します。この構成項目は、クライアントの構成ファイルにもコピーする必要があります。
- Compression：VPNリンク上の圧縮を有効にします。ここでこの機能を有効にした場合、管理者はこれをクライアント構成でも有効にする必要があります。
- TLS Renegotiation Time：一定の時間が経過すると、再び認証が必要になります。
- Manage Client-Specific Options：特定のクライアントに固有のIPアドレスを割り当てる場合、または接続しているクライアントの背後に同様にVPNにアクセスできるプライベートサブネットが存在する場合は、このオプションを有効にします。
- 「適用」をクリックします。

1.4.2.1.3 VPNクライアント

VPNサーバリストを表示し、プロファイルを追加します。VPNには、PPTP、L2TP、OpenVPNの3つのタイプがあります。

VPNクライアントを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「VPN」→「VPNクライアント」**の順にクリックします。
2. VPNサーバリストが表示されます。VPNクライアントを設定するには、**「プロファイルの追加」**をクリックします。

3. **VPNサーバリスト**：構成されている現在のVPNサービスが表示されます。
4. **VPNタイプ**：PPTP、L2TP、OpenVPNなどの、VPNサーバアクセスのタイプを指定します。
5. **ディフォルトルータ**：VPNサーバからのデフォルトルータの取得を使用するには「有効」をクリックします。一般的なデフォルトルータを使用するには「無効」をクリックします。
6. **詳細**：参考のための説明を入力します。
7. **VPNサーバ**：VPNサーバのIPアドレスまたはURLを入力します。
8. **ユーザ名**：VPN認証のユーザ名を入力します。

9. **パスワード**：VPN認証のパスワードを入力します。
10. **PPTPオプション**：PPTPの暗号化方式。自動Microsoft Point-to-Point Encryption（MPPE）を使用するには「Auto」を、MPPEを無効にするには「No Encryption」を選択します。PPTPサーバで40ビットのMPPEを使用するには「MPPE 40」を、PPTPサーバで128ビットのMPPEを使用するには「MPPE 128」を選択します。
11. 完了したら、**「確認」**をクリックします。

1.4.2.2 IPv4ファイアウォール

ファイアウォールが外部からの攻撃からローカルエリアネットワークを保護できるようにします。ファイアウォールは、受信および送信パケットをルールに基づいてフィルタリングします。

POINT

ファイアウォールは、デフォルトで有効になっています。

1.4.2.2.1 共通

ファイアウォールがハッカーからの攻撃からローカルエリアネットワークを保護できるようにします。ファイアウォールは、受信および送信パケットをフィルタルールに基づいてフィルタリングします。

基本的なファイアウォール設定を設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「IPv4ファイアウォール」→「共通」**の順にクリックします。
2. **ファイアウォール**：ファイアウォールを無効にすると、関連するすべての機能が非アクティブ化されます。
3. **DoS Protection**：「サービス拒否」攻撃は、正当なユーザのサービスまたはコンピューターリソースの使用を拒否しようとする明示的な攻撃です。この機能を有効にすると、DoS攻撃からルータを保護できますが、ルータのワークロードも増加します。
4. **Respond to Ping Request from WAN**：この機能は、ルータがWANからのping要求に応答できるようにします。
5. **IGMP**：IGMPパッケージのルータへの転送を許可するには「有効」をクリックします。IGMPパッケージを拒否するには「無効」をクリックします。
6. **「適用」**をクリックします。

1.4.2.2.2 URLフィルタ

URL（Uniform Resource Locator - 例えば、http://www.abcde.comまたは http://www.example.comの形式のアドレス）フィルタルールを使用すると、ネットワーク上のユーザに特定のWebサイトのURLにアクセスさせないようにできます。定義済みのURLフィルタルールは存在しないため、個別の要件を満たすフィルタルールを追加できます。

URLフィルタを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「IPv4ファイアウォール」→「URLフィルタ」**の順にクリックします。
2. **URLフィルタ**：URLフィルタを有効にするには「有効」を、URLフィルタを無効にするには「無効」を選択します。
3. **有効にする曜日（平日）**：URLフィルタを有効にする平日を選択します。
4. **有効にする時間**：URLフィルタを有効にする平日の時間を設定します。
5. **有効にする曜日（週末）**：URLフィルタを有効にする週末の日を選択します。
6. **有効にする時間**：URLフィルタを有効にする週末の時間を設定します。
7. **URLフィルタリスト**：ルータは、LAN側のデバイスがリスト内のURLにアクセスしないようにします。
8. **追加/削除**：プロファイルを追加または削除するには、⊕または⊖をクリックします。
9. **「適用」**をクリックします。

1.4.2.2.3 キーワードフィルタ

完全なURLを指定しなくても、個々のURL内の特定のキーワードに対してブロックできるようにします（例えば、「advertisement.gif」という名前のすべての画像をブロックするなど）。有効になっている場合は、指定されたキーワードリストをチェックし、アクセスされたURL内にいずれかのキーワードが存在するかどうかを確認して、その接続試行をブロックすべきかどうかを判定します。URLフィルタは、ポート80のみを使用してWebブラウザー（HTTP）の接続試行をブロックすることに注意してください。

キーワードフィルタを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「IPv4ファイアウォール」→「キーワードフィルタ」**の順にクリックします。
2. **キーワードフィルタ**：キーワードフィルタを有効にするには「有効」を、キーワードフィルタを無効にするには「無効」を選択します。
3. **有効にする曜日（平日）**：キーワードフィルタを有効にする平日を選択します。
4. **有効にする曜日（週末）**：キーワードフィルタを有効にする週末の日を選択します。
5. **有効にする曜日（週末）**：キーワードフィルタを有効にする週末の日を選択します。
6. **有効にする時間**：キーワードフィルタを有効にする週末の時間を設定します。
7. **キーワードフィルタリスト**：ルータは、LAN側のデバイスがリスト内のキーワードを含むWebページにアクセスしないようにします。
8. **「追加/削除」**：プロファイルを追加または削除するには、 または をクリックします。
9. **「適用」**をクリックします。

1.4.2.2.4 ネットサービスフィルタ

このモジュールのサポートにより、管理者は特定のサービスをブロックするためにブラックリストを設定したり、一部のサービスがルータをパススルーできるようにホワイトリストを設定したりできます。

ネットサービスフィルタを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「IPv4ファイアウォール」→「ネットサービスフィルタ」**の順にクリックします。
2. **ネットワークサービスフィルタ**：このモジュールを有効または無効にします。
3. **フィルタテーブルリスト**：フィルタリストには、「ホワイトリスト」と「ブラックリスト」の2種類があります。ホワイトリストは、ルータがリストで定義されている指定されたサービスを処理でき、ブラックリストは、ルータが指定されたサービスの処理を拒否します。
4. **有効にする曜日（平日）**：ネットサービスフィルタを有効にする平日を選択します。
5. **有効にする時間**：ネットサービスフィルタを有効にする平日の時間を設定します。
6. **有効にする曜日（週末）**：ネットサービスフィルタを有効にする週末の日を選択します。
7. **有効にする時間**：ネットサービスフィルタを有効にする週末の時間を設定します。
8. **Filtered ICMP packet types**：このフィールドは、フィルタリングされるLANからWANへのICMPパケットタイプのリストを定義します。例えば、エコー（タイプ8）とエコー応答（タイプ0）のICMPパケットをフィルタリングする場合は、数字を空白で区切った文字列（［0 8］など）を入力する必要があります。
9. **ソースIP**：ソースまたはデスティネーションのIPアドレスには、（a）固有のIPアドレス（「192.168.122.1」など）を入力するか、（b）1つのサブネット内または同じIPプール内のIPアドレス（「192.168.123.*」や「192.168.*.*」など）を入力するか、または（c）「*.*.*.*」としてすべてのIPアドレスを入力できます。
10. **Port Range**：ソースまたはデスティネーションのポート範囲には、a）特定のポート（「95」など）を入力するか、またはb）ある範囲内のポート（「103:315」、「>100」、「<65535」など）を入力できます。

11. **デスティネーションIP**：ソースまたはデスティネーションのIPアドレスには、（a）固有のIPアドレス（「192.168.122.1」など）を入力するか、（b）1つのサブネット内または同じIPプール内のIPアドレス（「192.168.123.*」や「192.168.*.*」など）を入力するか、または（c）「*.*.*.*」としてすべてのIPアドレスを入力できます。
12. **Port Range**：ソースまたはデスティネーションのポート範囲には、a）特定のポート（「95」など）を入力するか、またはb）ある範囲内のポート（「103:315」、「>100」、「<65535」など）を入力できます。
13. **プロトコル**：パッケージを転送するために使用されるサービスのプロトコル（UDP、TCP）を選択します。
14. **追加/削除**：プロファイルを追加または削除するには、 または をクリックします。
15. 完了したら、**「適用」**をクリックします。

1.4.2.3 IPv6ファイアウォール

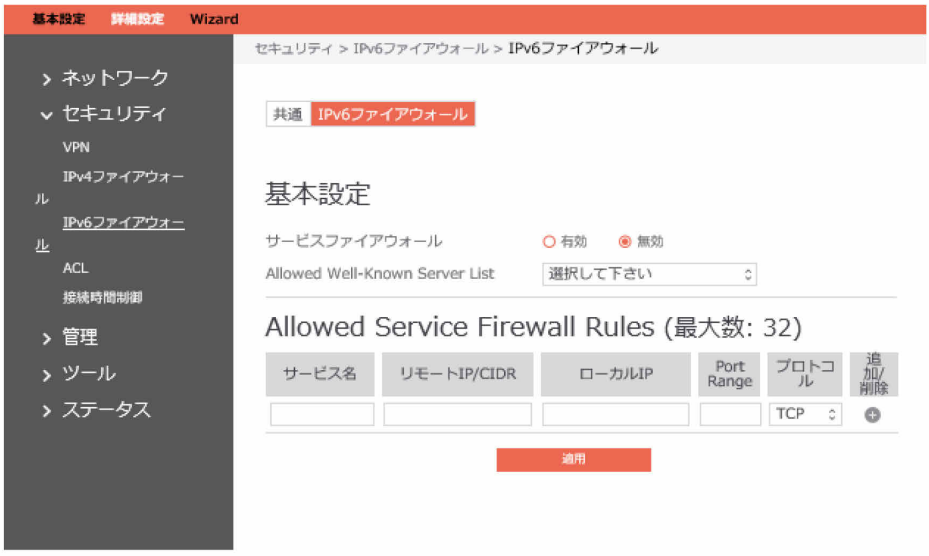
1.4.2.3.1 共通

一般的なIPv6ファイアウォールを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「IPv6ファイアウォール」→「共通」**の順にクリックします。
2. **ファイアウォール**：ファイアウォールを無効にすると、関連するすべての機能が非アクティブ化されます。
3. **Respond to Ping Request from WAN**：この機能は、ルータがWANからのping要求に応答できるようにします。
4. **MLD**：MLDパッケージのルータへの転送を許可するには「有効」をクリックします。MLDパッケージを拒否するには「無効」をクリックします。
5. **「適用」**をクリックします。

1.4.2.3.2 IPv6ファイアウォール

LAN側のIPv6ホストから来る送信トラフィック、および関連する受信トラフィックはすべて許可されます。その他の受信トラフィックはすべて、ここで明確に許可する必要があります。リモートIPを空のままにすると、任意のリモートホストからのトラフィックを許可することができます。また、サブネットも指定できます。



IPv6ファイアウォールを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「IPv6ファイアウォール」→「IPv6ファイアウォール」**の順にクリックします。
2. **サービスファイアウォール**：IPv6ファイアウォールを有効または無効にします。無効になっている場合は、すべてのIPv6パッケージのルータへの入力、ルータからの出力、および制限なしでの転送が可能です。
3. **Allowed Well-Known Server List**：許可される既知のサーバリスト。例えば、ftpやsambaなどです。
4. **サービス名**：IPv6ファイアウォールルールを追加するサービスの名前を入力します。
5. **リモートIP/CIDR**：リモートサーバのIPv6アドレスを入力します。
6. **ローカルIP**：LAN側のクライアントのIPv6アドレスを入力します。
7. **Port Range**：ポート範囲では、ポートの範囲（300:350）、個々のポート（566,789）またはその混在（1015:1024、3021）などのさまざまな形式が許可されます。
8. **プロトコル**：サービスがパッケージを転送するために使用するプロトコル（UDP、TCPなど）を選択します。
9. **追加/削除**：プロファイルを追加または削除するには、 または をクリックします。
10. 完了したら、**「適用」**をクリックします。

1.4.2.4 ACL

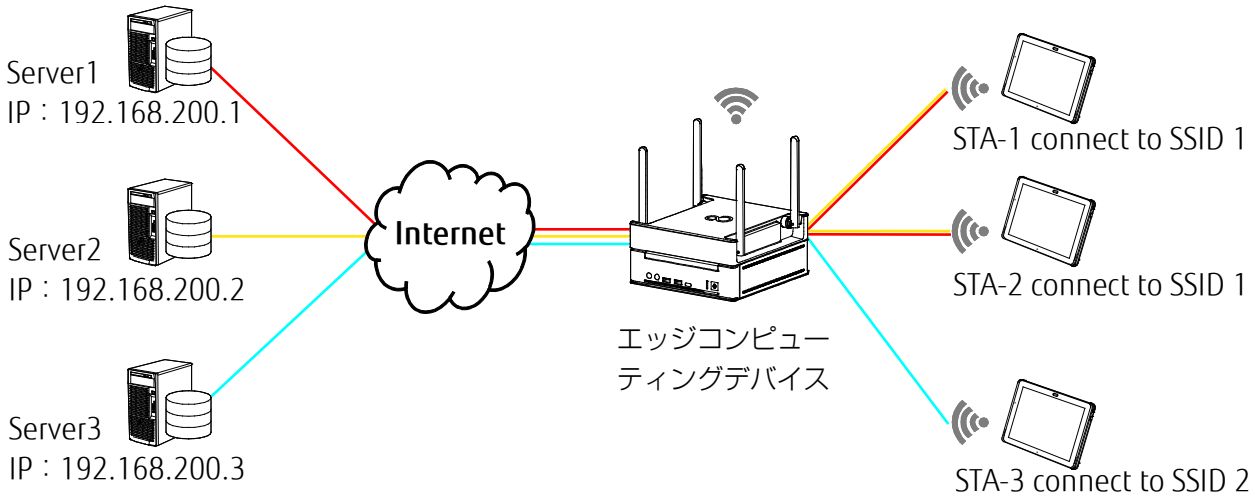
サーバへのユーザアクセスが正しいかどうか、およびネットワークを制御します。

Server DB	IP address/HostName
Server 1	192.168.200.1
Server 2	192.168.200.2
Server 3	192.168.200.3

Access Rule DB	IP address/HostName
Rule 1	Server 1
Rule 1	Server 2
Rule 2	Server 3

User DB Rule	User Mac Address	Access path
User DB 1	74:C6:3B:C3:28:73	
User DB 1	74:C6:3B:C3:28:74	
User DB 2	74:C6:3B:C3:28:75	

SSID DB	User	Action mode	Access path
SSID 1	User DB 1	1	
SSDI 2	User DB 2	1	

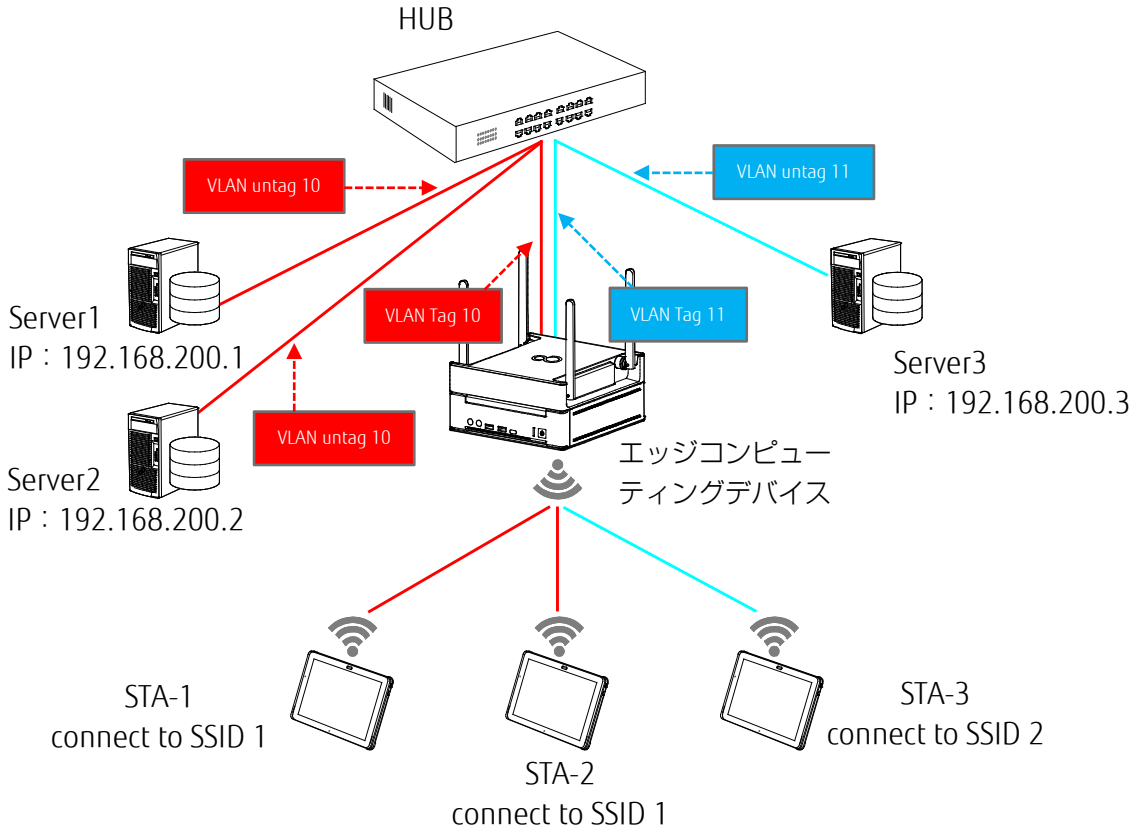


図は、**ACLモード1**トポロジの例を示しています。

Access Rule DB	VLAN ID	IP address/HostName
Rule 1	10	Server 1& 2
Rule 2	11	Server 3

User DB Rule	User Mac Address	Access path
User DB 1	74:C6:3B:C3:28:73	
User DB 1	74:C6:3B:C3:28:74	
User DB 2	74:C6:3B:C3:28:75	

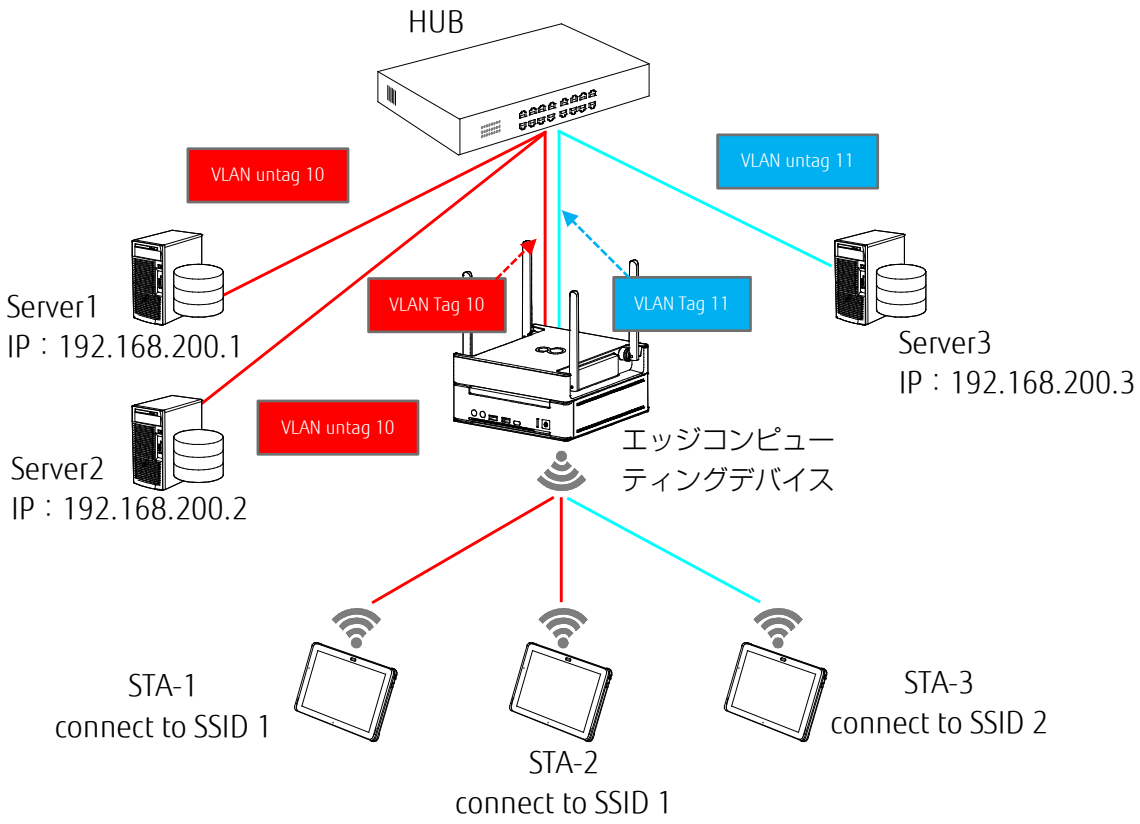
SSID DB	User	Action mode	VLAN ID	Access path
SSID 1	User DB 1	2	10	
SSID 2	User DB 2	2	11	



図は、**ACL**モード**2**トポロジの例を示しています。

User DB Rule	User Mac Address	Access path
User DB 1	74:C6:3B:C3:28:73	
User DB 1	74:C6:3B:C3:28:74	
User DB 2	74:C6:3B:C3:28:75	

SSID DB	User	Action mode	VLAN ID	Access path
SSID 1	User DB 1	3	10	
SSID 2	User DB 2	3	11	



図は、**ACLモード3**トポロジの例を示しています。

1.4.2.4.1 基本設定

基本設定では、ACLのオン/オフを切り替えることができます。

ACLの基本設定ページを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「ACL」→「基本設定」**の順にクリックします。
2. **アクセスコントロール**：ACL機能のオン/オフを切り替えます。
3. **すべてのデータベースをエクスポート**：すべてのACLデータベースをtgzファイルとしてエクスポートします。
4. **すべてのデータベースをインポート**：すべてのACLデータベースのtgzファイルをインポートします。

プライバシープロテクション：

1. **同一SSID内の通信禁止**：同一SSIDのもとにあるクライアントを分離します。
2. **異なるSSID間の通信禁止**：異なるSSIDのもとにあるクライアントを分離します。

1.4.2.4.2 サーバDB

サーバDB設定では、サーバDBの内容を設定できます。

サーバDBを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「ACL」→「サーバDB」**の順にクリックします。
2. **サーバDBの削除**：このボタンは、すべてのサーバDBデータを削除します。
3. **サーバDBのエクスポート**：サーバDBをファイルにエクスポートできます。
4. **サーバDBのインポート**：サーバDBをcsv形式でインポートできます。

サーバDBの追加：

1. **「追加」**をクリックします。
2. **サーバ名**：サーバの名前を入力します。
3. **IPアドレス/ホスト名**：IPアドレスまたはホスト名を入力します。
4. **「確認」**をクリックします。

1.4.2.4.3 アクセスルールDB

アクセスルールDB設定では、アクセスルールDBのルールを設定できます。

アクセスルールDBを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「ACL」→「アクセスルールDB」**の順にクリックします。
2. **アクセスルールの削除**：アクセスルールDBのすべてのルールを削除します。
3. **アクセスルールDBのエクスポート**：ルールファイル：アクセスルールDBをファイルにエクスポートします。
4. **アクセスルールDBのインポート**：アクセスルールDBをcsvファイルで追加します。

アクセスルールの追加：

1. **「追加」**をクリックします。
2. **アクセスルール名**：アクセスルールDB名。最大バイト数は32です。
3. **VLAN ID**：VLAN IDは数値である必要があり、範囲は0～4096です。0（ゼロ）は、VLAN IDを無効にすることを示します。
4. **選択したサーバ名**：右側のサーバリストから項目を選択して左側のサーバリストに移動します。左側のリストは、アクセスルールDBとして選択されています。
5. **「確認」**をクリックします。

1.4.2.4.4 ユーザDB

ユーザDBでは、ユーザルールおよびDB全体を追加/編集/削除/インポートできます。

ユーザDBを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「ACL」→「ユーザDB」**の順にクリックします。

ユーザDBのエクスポート：

1. **すべてのユーザDBをエクスポート**：すべてのユーザDBのtgzファイルをエクスポートします。
2. **ひとつのユーザDBをエクスポート**：ファイルにエクスポートするユーザDBを選択します。

ユーザDBのインポート：

1. **すべてのユーザDBをインポート**：すべてのユーザDBのtgzファイルをインポートします。
2. **ひとつのDBのインポート**：
    - 選択または新しいDB：新しいDB名を入力するか、インポートするか選択します。
    - 新しいDB名：新しいユーザDB名を入力します。
    - ユーザDBのインポート：ユーザDBをインポートするファイルを選択します。

ユーザDBの削除：

1. **ひとつのユーザDBを削除**：削除するユーザDBを選択します。

ユーザDB設定：

1. **ユーザDBを選択して下さい**：新しいユーザを追加する場合は、［新しいユーザを追加する］選択します。既存のDBを編集する場合は、ユーザDBを選択します。

ユーザDBの追加：

1. **「追加」**をクリックします。
2. **ユーザDB名**：［新しいユーザを追加する］選択した場合は、ユーザDB名を入力します。
3. **ユーザ名**：ユーザ名を入力します。
4. **MAC address**：MACアドレスを入力します。
5. **Access Class**：アクセスクラス値を選択します。
6. **アクセスルール**：アクセスルールを選択します。
7. **「確認」**をクリックします。

1.4.2.4.5 SSID DB

SSID DBでは、SSIDルールおよびDB全体を追加/編集/削除/インポートできます。

SSID DBを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「ACL」→「SSID DB」**の順にクリックします。
2. **SSID DBの削除**：DB全体を削除します。
3. **SSID DBのエクスポート**：DBをファイルにエクスポートします。
4. **SSID DBのインポート**：DBをインポートします。

SSID DBの追加：

1. **「追加」**をクリックします
2. **SSID名**：SSID名を選択します。
3. **ACLモード**：ACLモードを選択します。
4. **VLAN ID**：VLAN IDを入力します。その値の範囲は0～4095です。
5. **ユーザDB**：ユーザDBを選択します。
6. **「確認」**をクリックします。

1.4.2.5 接続時間制御

接続時間制御を使用すると、インターネットアクセス時間を制御できます。ユーザは、クライアントのネットワーク使用の時間制限を設定できます。

接続時間制御機能を設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「セキュリティ」→「接続時間制御」**の順にクリックします。
2. **接続時間制御**：接続時間制御を有効にするには「有効」を、接続時間制御を無効にするには「無効」を選択します。
3. **クライアント名**：リストからクライアントを選択します。リスト内の名前は、ルータと通信しているクライアントを表します。
4. **MACアドレス**：選択されたクライアントのMACアドレス。

   POINT

   「クライアント名」は、管理者がLAN側のデバイスを簡単に区別できるようにするだけです。実際にどのデバイスが接続時間制御の対象になるかを指定するのは**「MACアドレス」**です。

5. **時間管理**： をクリックしてから、クライアントのインターネットアクセスを許可または拒否するようにクライアントのスケジュール予定表を設定します。
6. **追加/削除**：プロファイルを追加または削除するには、 または をクリックします。
7. **「適用」**をクリックします。

1.4.3 管理

1.4.3.1 システム

「システム」ページでは、無線ルータ設定を構成できます。

システムを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「管理」→「システム」**の順にクリックします。
2. **ユーザ名**：ルータのログイン名。
3. **新しいパスワード**：新しいパスワード。
4. **パスワードの確認入力**：新しいパスワードを再入力します。

POINT

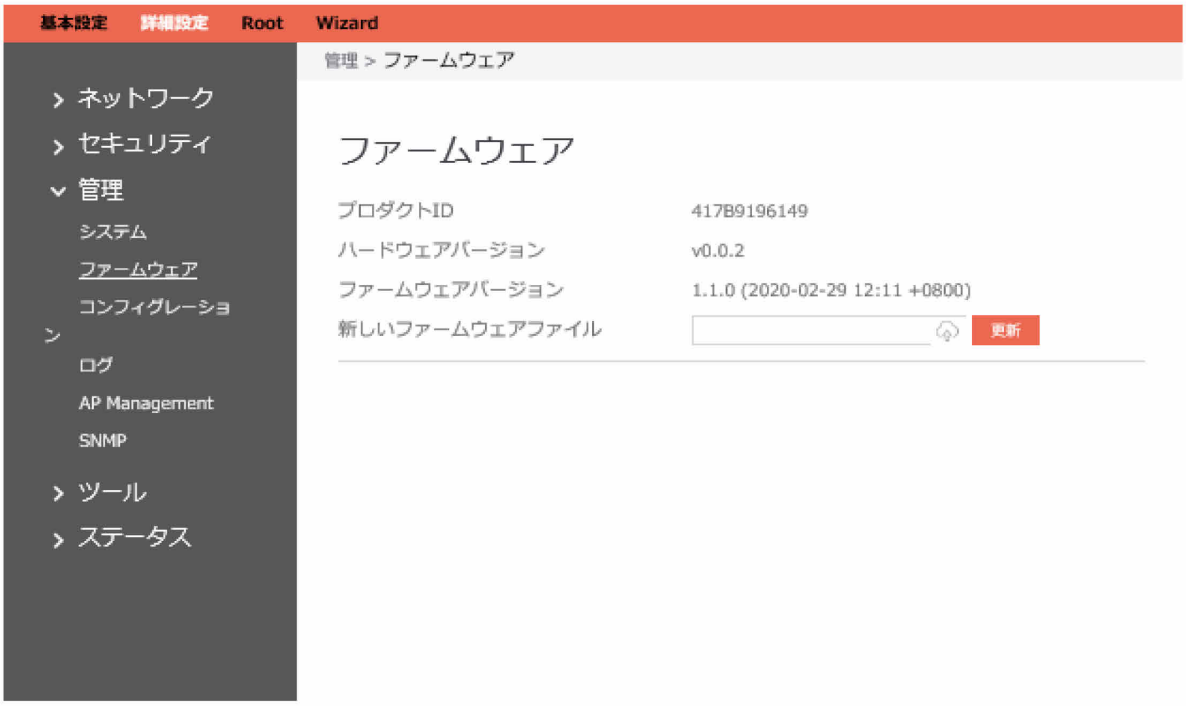
・ルータへのログインには、2つのSSHアカウントを使用できます。
- **管理：ユーザ名は「admin」、パスワードの初期値は「admin」です。**
- **ルート：ユーザ名は「root」、パスワードの初期値は「root」です。**

・運用管理ツールを利用して運用する際は、エッジコンピューティングデバイスに運用管理ツールクライアント機能をインストール後、必ず「運用管理ツール/AP部 連携用パスワード設定ツール」を実行してください。上記ツールではadminのパスワードを入力する必要があります。

5. **WANからSSHでのアクセス可否**：WANポートからのSSH接続を有効または無効にします。
6. **LANからSSHでのアクセス可否**：LANポートからのSSH接続を有効または無効にします。
7. **リモートログサーバ**：ローカルの送信先のほか、ログメッセージが送信される先のsyslogサーバのIPアドレス。
8. **タイムゾーン**：デフォルトのタイムゾーンは「アジア/東京（Asia/Tokyo）」です。
9. **手動時間設定**：「取得」と「時刻設定」の2つのボタンがあります。
   「取得」ボタン：「取得」ボタンをクリックすると、WebページにPCの時間が表示されます。
   「時刻設定」：時間が手動でアクセスポイントに設定されます。
10. **WANからのWebアクセス**：WANポート経由のリモートアクセスを有効または無効にします。
11. **WANからSNMPアクセス**：WANポート経由のSNMPアクセスを有効または無効にします。
12. **自動ログアウト**：指定された時間が経過すると自動ログアウトします。
13. **WANダウン通知**：インターネットアクセスが存在しない場合は、接続端末に対してブラウザー経由で通知されます。
14. **NTPサーバ**：ルータは、NTP（ネットワークタイムプロトコル）サーバにアクセスして、時間を自動的に同期できます。本アクセスポイント部には、バックアップ用の電池を搭載していません。電源OFFごとに時刻が初期値に戻ります。そのため、NTPサーバの設定をお勧めします。
15. **「適用」**をクリックします。

1.4.3.2 ファームウェア

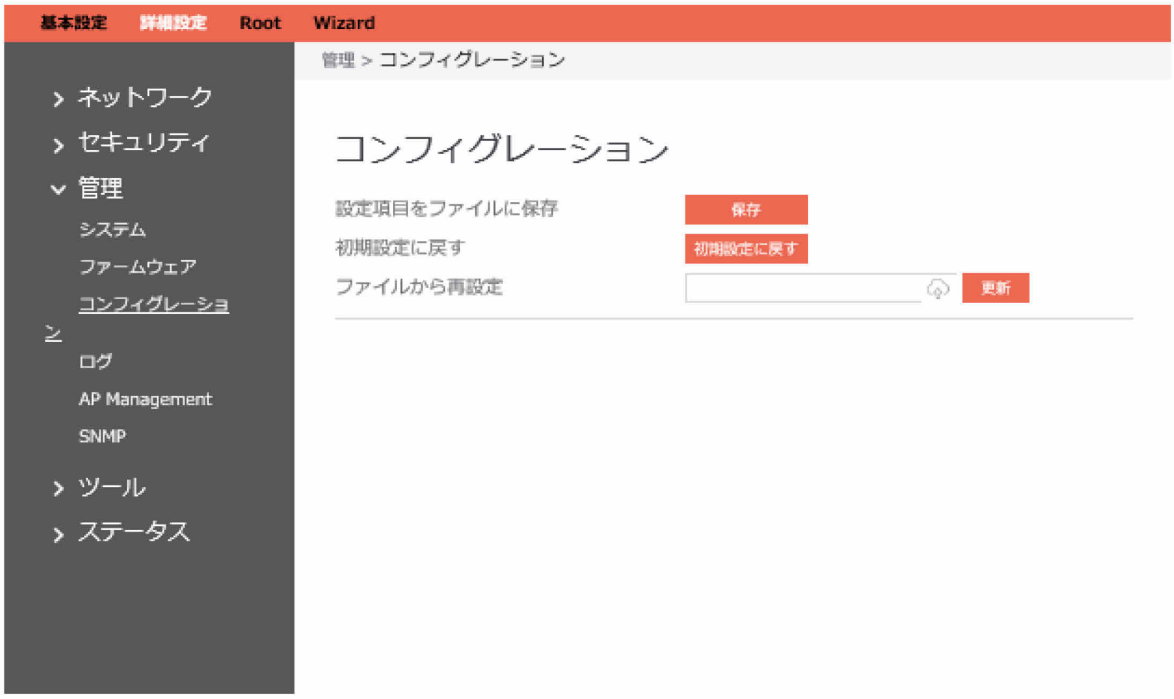
このモジュールでは、管理者はWeb経由でファームウェアをアップグレードできます。



ファームウェアをアップグレードするための手順：

1. ナビゲーションパネルから、**「詳細設定」→「管理」→「ファームウェア」**の順にクリックします。
2. **新しいファームウェアファイル：**をクリックして、ファームウェアファイルを指定します。
3. **「更新」**をクリックします。

1.4.3.3 コンフィグレーション



ルータの構成を保存/リセット/復元するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「管理」→「コンフィグレーション」**の順にクリックします。
2. **「保存」**をクリックすると、アクセスポイントの設定を指定の場所に保存することができます。
3. **「初期設定に戻す」**をクリックすると、すべての設定が工場出荷のデフォルト設定にリセットされます。
4. をクリックして設定ファイルを選択してから、**「更新」**をクリックすると、ルータが設定されます。

1.4.3.4 ログ

システムログには、ルータ内のネットワーク操作に関するログが含まれています。

ルータのログを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「管理」→「ログ」**の順にクリックします。
2. **削除**：ログファイルの内容をクリアします。
3. **保存**：ルータからログファイルをダウンロードします。
4. **更新**：最新のログを表示するようにログウィンドウを更新します。

1.4.3.5 AP Manegement

AP Management内の項目を設定するための手順：
（通常は変更する必要はありません。）

1. ナビゲーションパネルから、**「詳細設定」→「管理」→「AP Management」**の順にクリックします。
2. 「ログファイルパス」に「/tmp/syslog/messages」を設定します。
3. **AP Name**：APの名前を設定します。
4. **AP情報通知有効**：APからServerへ情報を通知する機能の有効/無効を設定します。
5. **通知先サーバアドレス**：APから通知を行うサーバのIPアドレスを記載します。
6. **通知先ポート番号**：APから通知を行うサーバのポート番号を記載します。
7. **通知周期(秒)**：APからServerへの情報通知の周期(秒)を記載します。
8. **ログファイルパス**：AP集中管理機能などで遠隔取得するログファイルを絶対パスで指定します。複数のファイルを指定する場合はカンマ区切りで複数指定します。
   デフォルトは /tmp/prpl_log,/tmp/messages です。

   POINT

   - エッジコンピューティングデバイス背面のRESETボタンを5秒以上押して設定をご購入時の状態に戻すと、デフォルトの /tmp/prpl_log,/tmp/messages に戻ります。
   - AP Management内の項目を変更するときは、必ず /tmp/syslog/messages に変更してください。

9. **「適用」**をクリックします。

AP情報通知の項目について

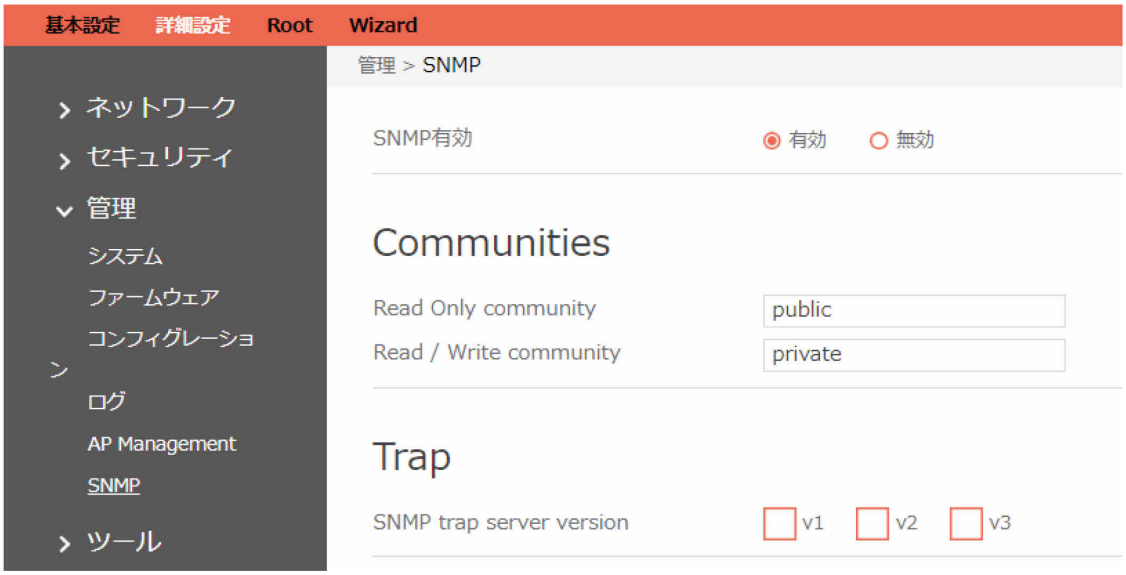
AP情報通知有効、通知先サーバアドレス、通知先ポート番号、通知周期（秒）の4つの設定項目があります。
この機能をご利用いただくには、お客様でサーバーのアプリを作成していただく必要があります。
「AP情報通知」では、次のような情報を取得できます。

・APのエラー情報
・DFSでレーダー関知したときのステータス変化情報等

APIの応答例は次のようになります。


```
Header": { "Name": "OK" },
"Body": { "WIFISTATUS": [
                        {
                                "SSID": "MIB6-5G",
                                "Enabled": true,
                                "IsHideSsid": false,
                                "Mode": "Master",
                                "Wireless Mode": "11ac",
                                "Frequency": "5G",
                                "Channel": "56",
                                "BSSID": "B0:EA:BC:E2:A9:DB",
                                "Authentication Method": "WPA2 Personal",
                                "WPA Encryption": "AES"
                        }
                ]
        }
```

1.4.3.6 SNMP

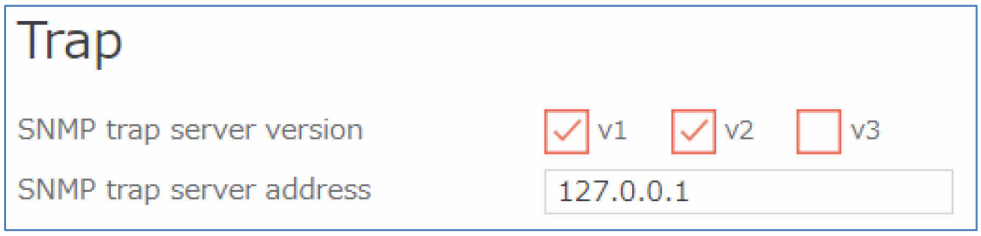


SNMPを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ツール」→「SNMP」**の順にクリックします。
2. **SNMP有効**：SNMPの有効/無効を設定します。
3. **Read Only community**：読み出し専用のcommunityを設定します。
4. **Read/Write community**：読み出し・書き込み可能のcommunityを設定します。

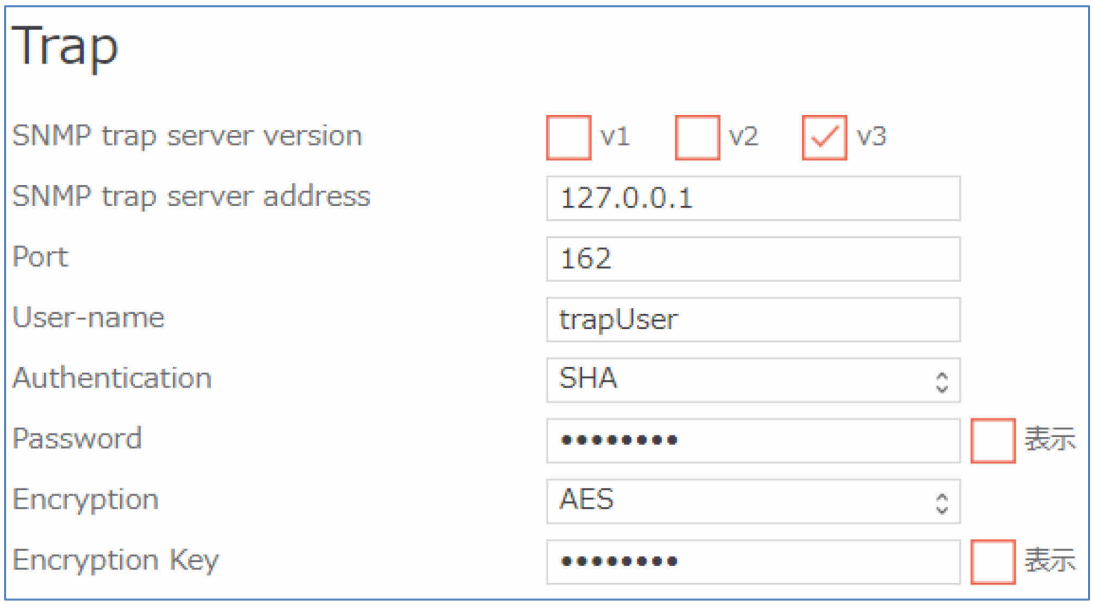
5. **SNMP trap server version**：SNMP trap serverのバージョンを選択します。v1/v2とv3では以降の入力項目が異なります。

●v1/v2



SNMP trap server address：SNMP trap serverのアドレスを指定します。

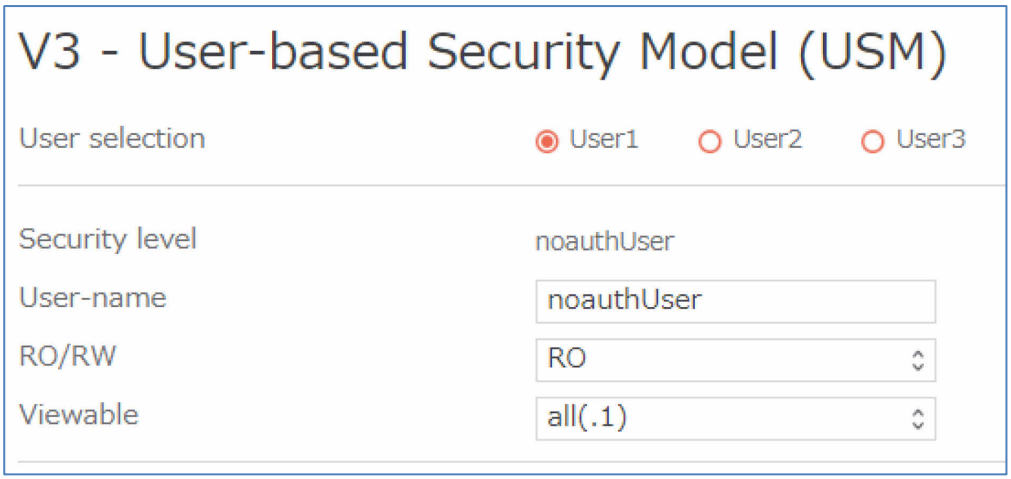
●v3



SNMP trap server address：SNMP trap server のアドレスを指定します。
Port：ポート番号を入力します。
User-name：ユーザ名を設定します。
Authentication：認証方式を選択します。
Password：パスワードを入力します。
Encryption：暗号化方式を選択します。
Encryption Key：暗号キーを入力します。

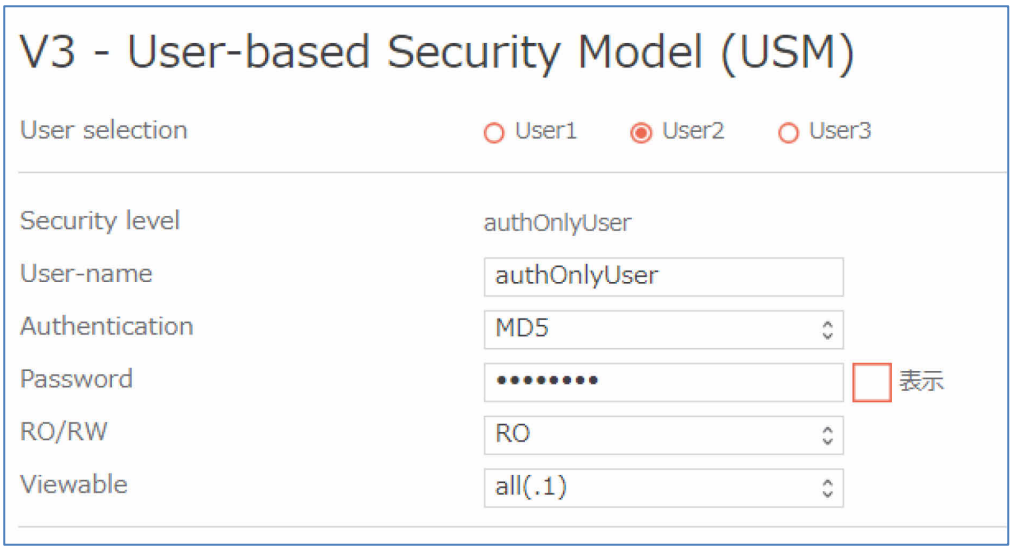
6. User selection：User1, User2, User3をボタンで選択します。選択したUserによって、以降の入力項目が異なります。

●User1



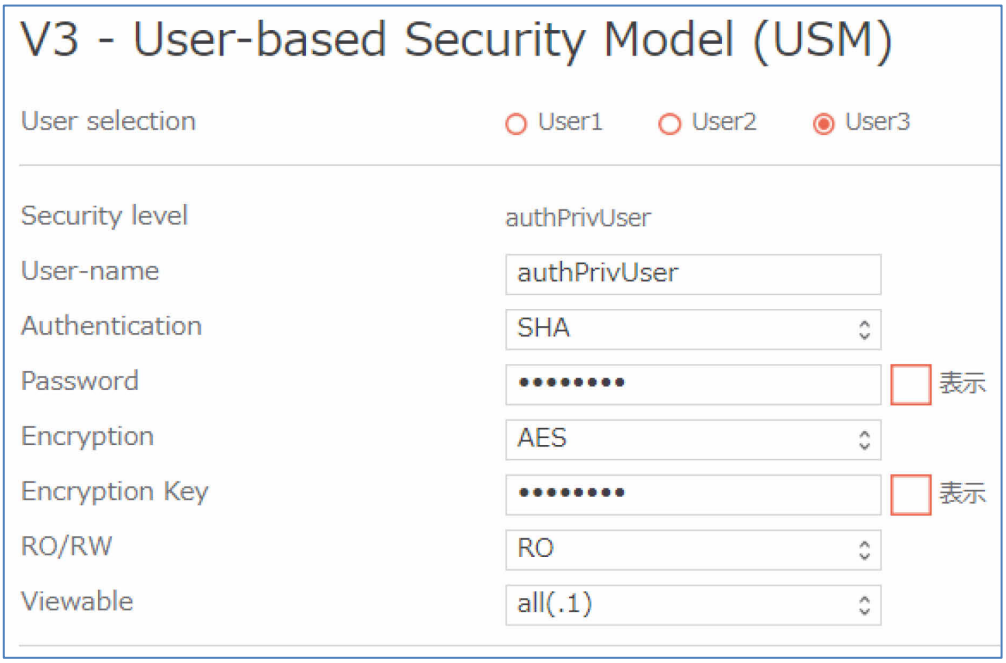
Security level：セキュリティレベルを表示します。
User-name：ユーザ名を設定します。
RO/RW：読み出し専用(RO)か読み出し・書き込み可能(RW)かを選択します。
Viewable：表示許可範囲を設定します。

●User2



Security level：セキュリティレベルを表示します。
User-name：ユーザ名を設定します。
Authentication：認証方式を選択します。
Password：パスワードを入力します。
RO/RW：読み出し専用(RO)か読み出し・書き込み可能(RW)かを選択します。
Viewable：表示許可範囲を設定します。

●User3

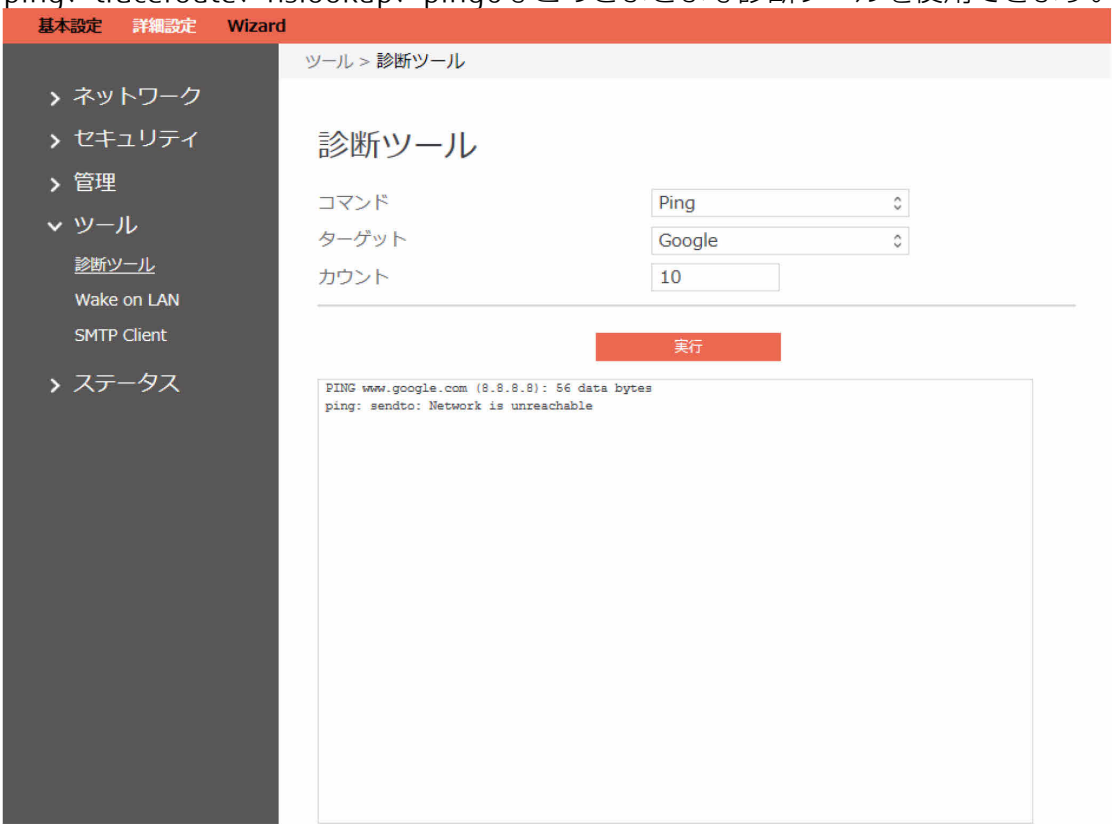


Security level：セキュリティレベルを表示します。
User-name：ユーザ名を設定します。
Authentication：認証方式を選択します。
Password：パスワードを入力します。
Encryption：暗号化方式を選択します。
Encryption key：暗号キーを入力します。
RO/RW：読み出し専用(RO)か読み出し・書き込み可能(RW)かを選択します。
Viewable：表示許可範囲を設定します。

1.4.4 ツール

1.4.4.1 診断ツール

ping、traceroute、nslookup、ping6などのさまざまな診断ツールを使用できます。



診断ツールを使用するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ツール」→「診断ツール」**の順にクリックします。
2. **コマンド**：ネットワークをテストする指定の方法を選択します。
3. **ターゲット**：テストのターゲットを選択します。
4. **カウント**：テストする回数。
5. **「実行」**をクリックします。

1.4.4.2 Wake on LAN

Wake on LANは、電源管理機能です。これにより、ネットワーク管理者は、LAN側のデバイスをスタンバイまたは休止モードからウェイクアップできます。この機能では、LAN側のデバイスにマザーボードのサポートが必要です。

Wake on LANを設定するための手順：

1. ナビゲーションパネルから、**「詳細設定」→「ツール」→「Wake on LAN」**の順にクリックします。
2. **ターゲット**：ウェイクアップされるデバイスのMACアドレスを入力するか、またはリストからデバイス名を選択します。
3. **デバイス名**：デバイスの名前。
4. **MACアドレス**：MACアドレスの形式は、転送の順に「: 」（コロン）で区切られた16進数2桁の6つのグループ（12:34:56:aa:bc:efなど）です。
5. 完了したら、**「適用」**をクリックします。

1.4.4.3 SMTPクライアント

SMTPクライアント機能を使用すると、ログインまたは無線チャネルの変更があったときに、指定されたEmailアドレスに対して自動的にメールを送信することができます。

SMTPクライアントを設定するための手順：

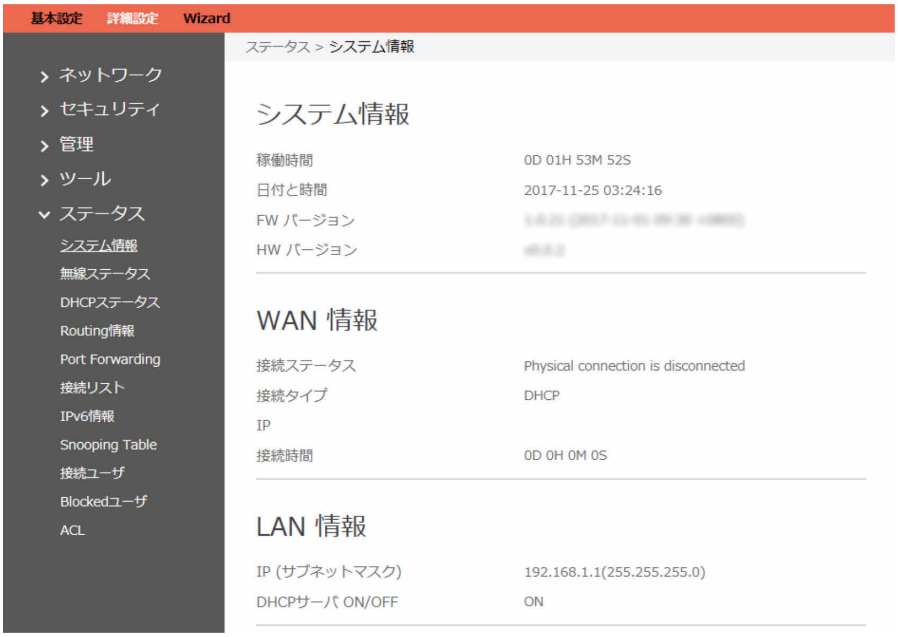
1. ナビゲーションパネルから、**「詳細設定」→「ツール」→「SMTP Client」**の順にクリックします。
2. **基本設定**
   - **SMTP クライアント：** SMTPクライアント機能を有効または無効にします。

3. **イベント通知**
   - **ログイン**：ログインの通知を有効または無効にします。
   - **チャンネル変化**：無線チャネルの変更の通知を有効または無効にします。
4. **サーバ情報**
   - **SMTPサーバ**：Email SMTPサーバ（163.smtp.comなど）を入力します。
   - **TLS/SSL**：TLS/SSL機能を有効または無効にします。
   - **ポート**：TLS/SSLのポート。
5. **Mailアカウント情報**
   - **Emailアドレス**：SMTPクライアントのEmailアドレス（送信者）を入力します（abc@163.comなど）。
   - **ユーザ名**：SMTPクライアントのユーザ名。
   - **パスワード**：SMTPクライアントのパスワード。
6. **構成**
   - **宛先**：Emailの受信者。
   - **件名**：Emailの件名。
   - **内容**：Mailの内容。
7. 完了したら、**「適用」**をクリックします。

1.4.5 ステータス

1.4.5.1 システム情報

「システム情報」には、基本的なシステム、WAN、およびLAN情報が表示されます。
ナビゲーションパネルから、**「詳細設定」→「ステータス」→「システム情報」**の順にクリックします。



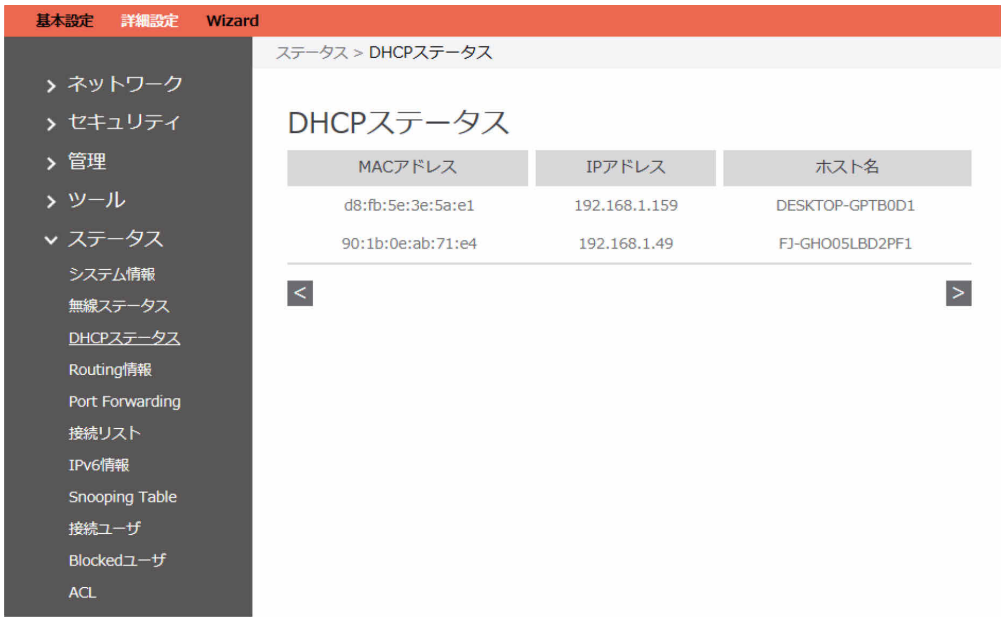
1.4.5.2 無線ステータス

「無線ステータス」には、無線クライアントの状態情報が表示されます。
ナビゲーションパネルから、**「詳細設定」→「ステータス」→「無線ステータス」**の順にクリックします。

1.4.5.3 DHCPステータス

DHCPステータス状態情報を表示します。これには、MAC、IP、およびホスト名情報が含まれます。

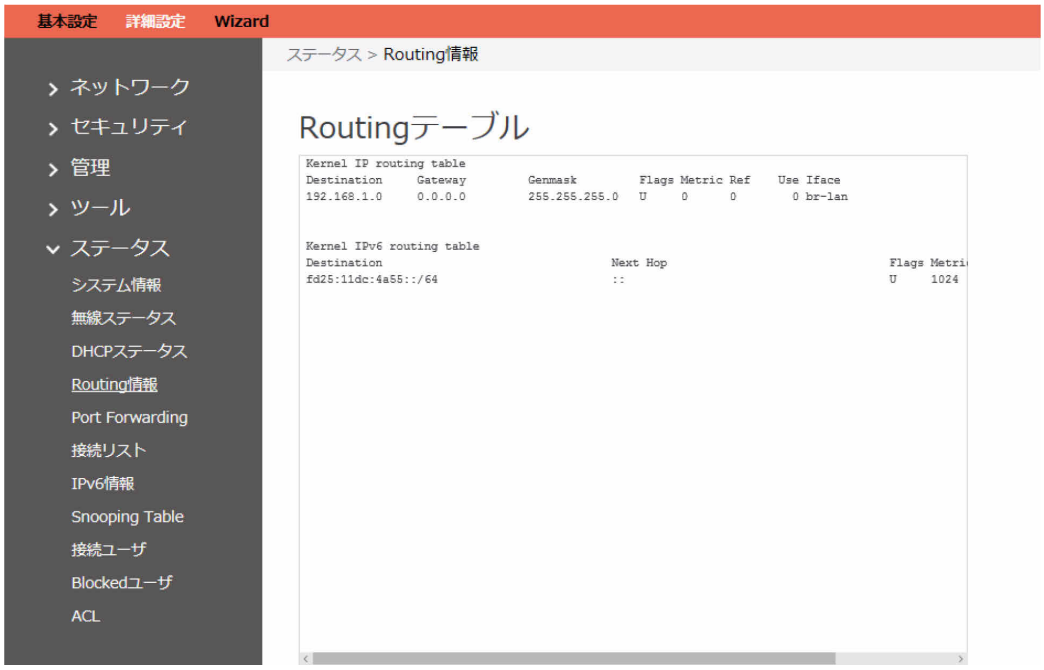
ナビゲーションパネルから、**「詳細設定」→「ステータス」→「DHCPステータス」**の順にクリックします。



1.4.5.4 Routing情報

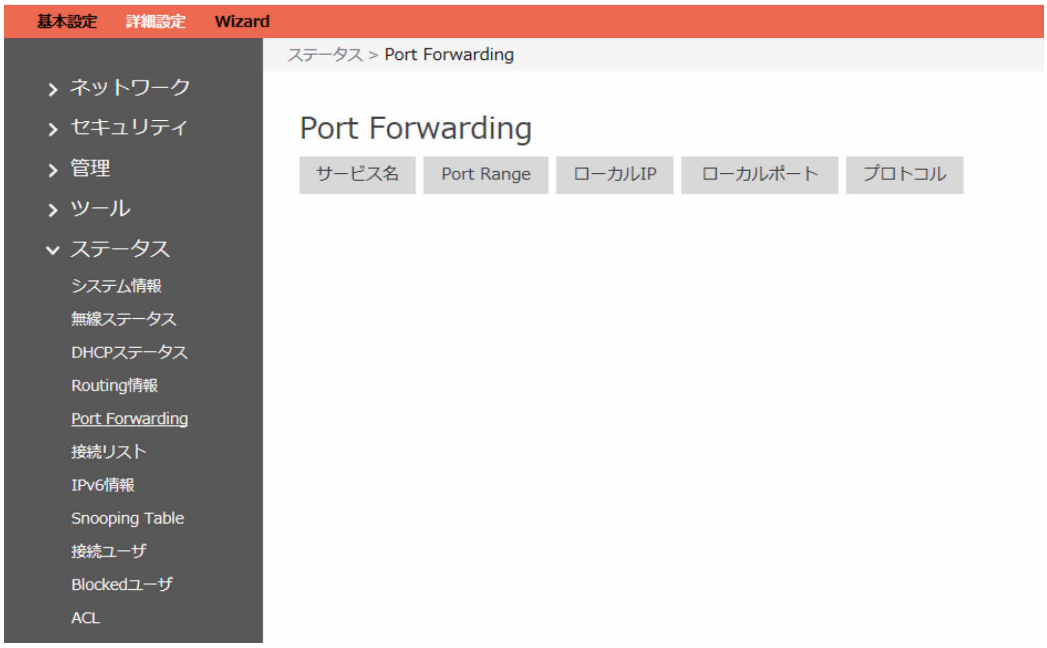
IPv4とIPv6のルーティング情報および状態情報を示します。

ナビゲーションパネルから、**「詳細設定」→「ステータス」→「Routing情報」**の順にクリックします。



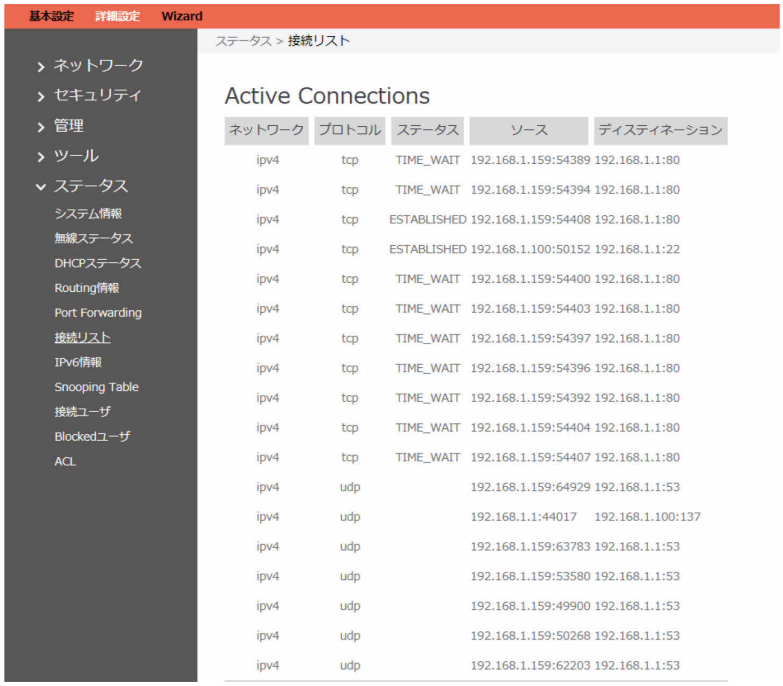
1.4.5.5 Port Forwarding

このモジュールは、ポートフォワーディング状態情報を表示するために使用されます。
ナビゲーションパネルから、「詳細設定」→「ステータス」→「Port Forwarding」の順にクリックします。



1.4.5.6 接続リスト

アクティブな接続の状態情報を表示します。
ナビゲーションパネルから、「詳細設定」→「ステータス」→「接続リスト」の順にクリックします。

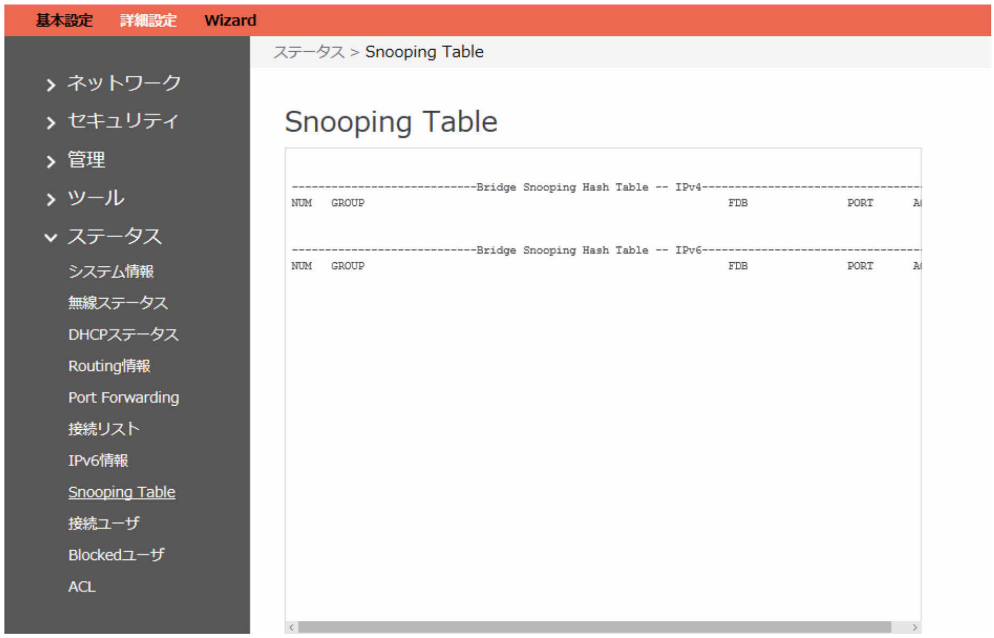


1.4.5.7 IPv6情報

WANおよびLAN IPv6情報に関する詳細を表示します。
ナビゲーションパネルから、**「詳細設定」→「ステータス」→「IPv6情報」**の順にクリックします。

1.4.5.8 Snooping Table

有線と無線の両方のクライアントストリームで、クライアントの参加または退出するためのスヌーピングテーブルを表示します。
ナビゲーションパネルから、**「詳細設定」→「ステータス」→「Snooping Table」**の順にクリックします。

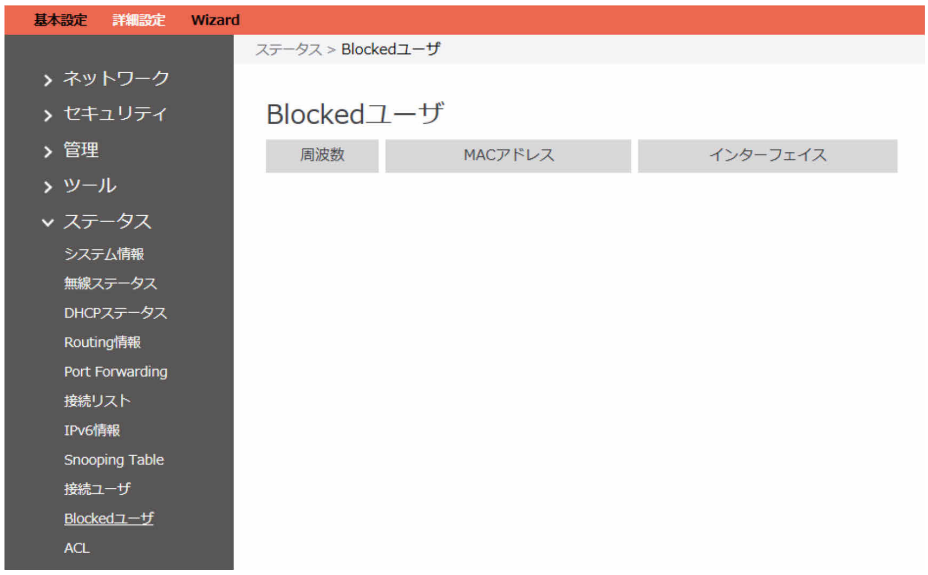


1.4.5.9 接続ユーザ

ルータを経由したインターネットアクセスを許可されている現在のユーザを表示します。
ナビゲーションパネルから、「詳細設定」→「ステータス」→「接続ユーザ」の順にクリックします。

1.4.5.10 Blockedユーザ

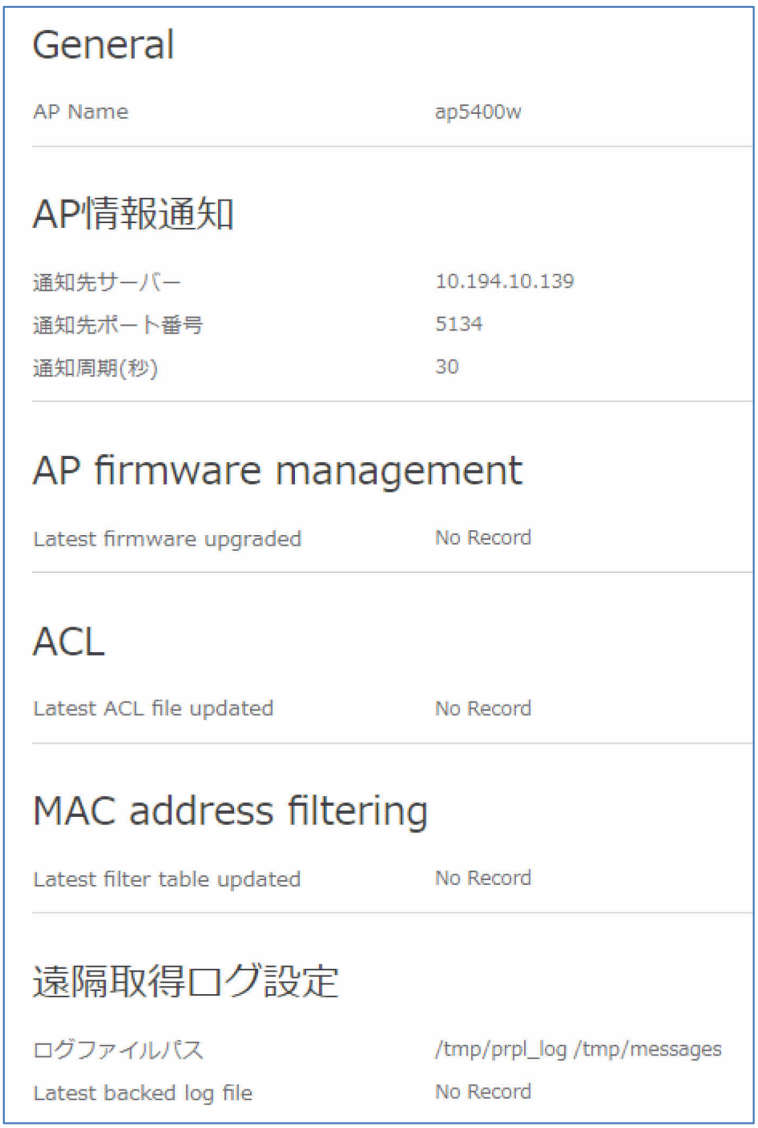
ルータを経由したインターネットアクセスを許可されていない現在のユーザを表示します。
ナビゲーションパネルから、「詳細設定」→「ステータス」→「Blockedユーザ」の順にクリックします。



1.4.5.11 ACL

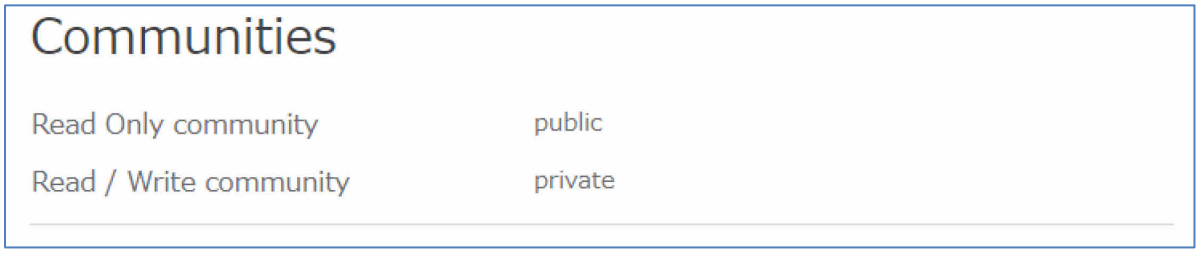
ACL情報を表示します。これには、MAC、SSID、IP、ホスト名、モード、クラス、VLAN、グループ名、ユーザ名、ルール名が含まれます。
ナビゲーションパネルから、「詳細設定」→「ステータス」→「ACL」の順にクリックします。

1.4.5.12 AP Manegement

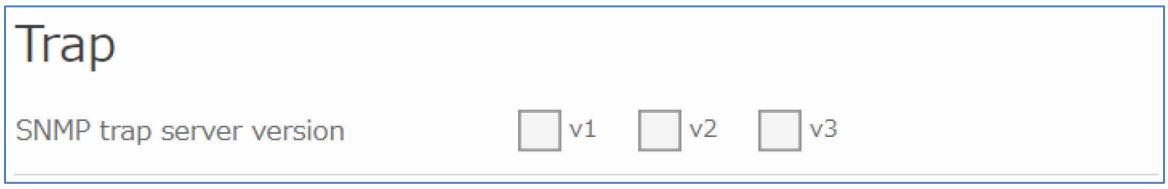


AP Name： APの名前が表示されます。
通知先サーバアドレス：AP情報を通知するサーバのIPアドレスが表示されます。
通知先ポート番号：APから通知を行うサーバのポート番号が表示されます。
通知周期(秒)：APからサーバへの情報通知の周期(秒) が表示されます。
Latest firmware updated：ファイルをアップロードした時間が表示されます。
Latest ACL file updated：ファイルをアップロードした時間が表示されます。
Latest filter table updated：ファイルをアップロードした時間が表示されます。
ログファイルパス：設定しているログファイルパスが表示されます。

1.4.5.13 SNMP



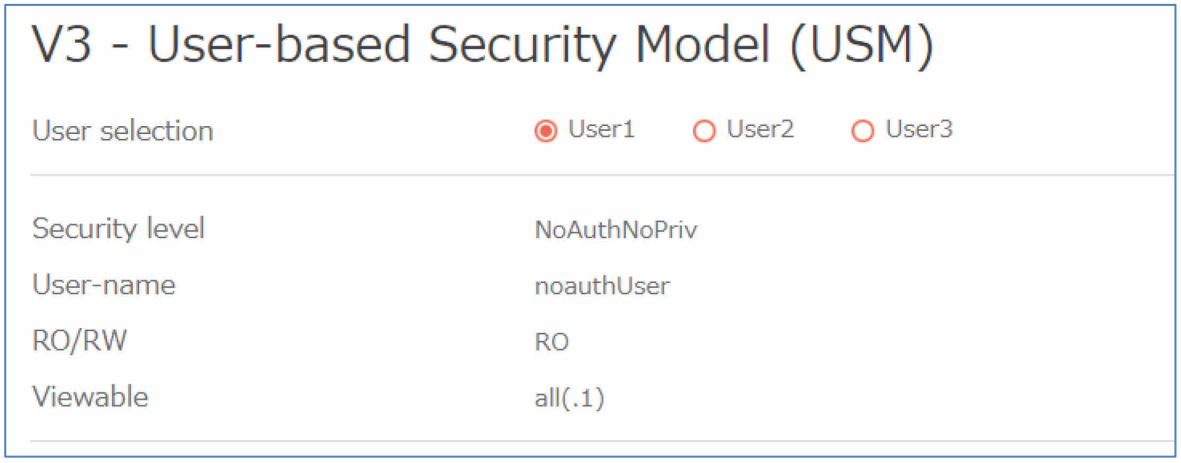
Read Only community：読み出し専用のcommunityが表示されます。
Read/Write community：読み出し・書き込み可能のcommunityが表示されます。



SNMP trap server address：SNMP trap server versionごとの、SNMP trap serverのアドレスが表示されます。

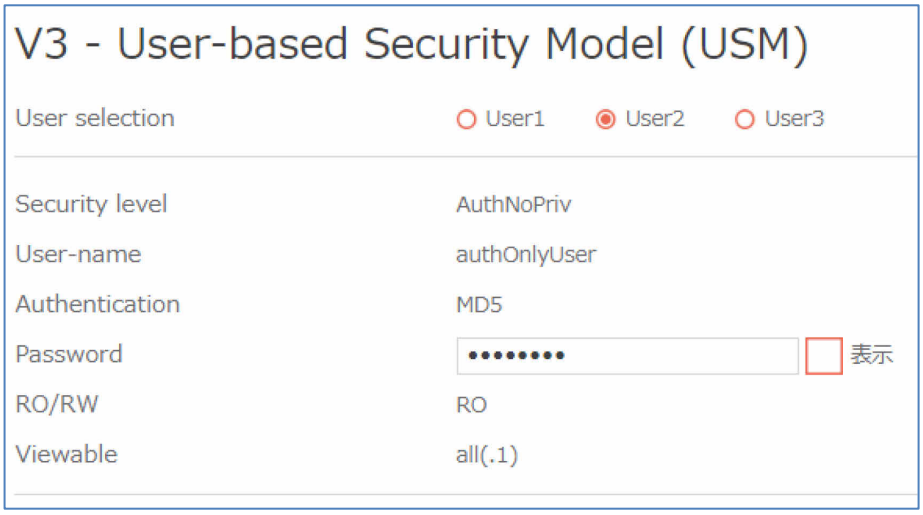
User selection：User1, User2, User3をボタンで選択します。選択したUserによって、以降の表示内容が変わります。

●User1



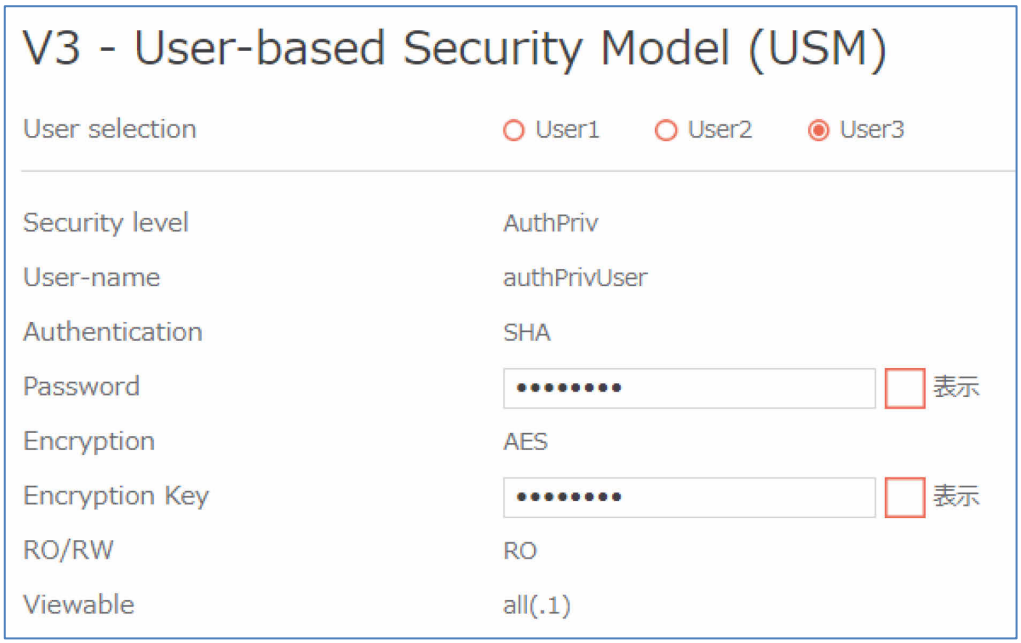
Security level：セキュリティレベルが表示されます。
User-name：ユーザ名が表示されます。
RO/RW：読み出し専用(RO)か読み出し・書き込み可能(RW)かが表示されます。
Viewable：表示許可範囲が表示されます。

●User2



Security level：セキュリティレベルが表示されます。
User-name：ユーザ名が表示されます。
Authentication：認証方式が表示されます。
Password：パスワードが表示されます。
RO/RW：読み出し専用(RO)か読み出し・書き込み可能(RW)かが表示されます。
Viewable：表示許可範囲が表示されます。

●User3



Security level：セキュリティレベルが表示されます。
User-name：ユーザ名が表示されます。
Authentication：認証方式が表示されます。
Password：パスワードが表示されます。
Encryption：暗号化方式が表示されます。
Encryption key：暗号キーが表示されます。
RO/RW：読み出し専用(RO)か読み出し・書き込み可能(RW)かが表示されます。
Viewable：表示許可範囲が表示されます。

2 ルートユーザの設定

より多くの構成オプションを使用するために、ルートユーザとしてGUIにログインできます。ルートユーザの設定は非表示になっており、通常ユーザでは構成できません。

2.1 ログイン

ルータのルートユーザは、通常ユーザより多くの特権を所有しています。ルートユーザのGUIにログインするための手順は次のとおりです。

1. エッジコンピューティングデバイス上でInternet Explorerを起動し、アクセスポイント部分のIPアドレス（初期値「192.168.1.1」）に接続します。
   ログイン画面が表示されます。
2. ユーザ名とパスワードを入力し、「ログイン」をクリックします。
   ユーザ名は「root」、パスワードの初期値は「root」です。

2.2 ウィザード（Wizard）

ウィザード機能の概要は、「1.2　ウィザード設定」の項目と同じです。

2.3 基本設定

基本設定機能の概要は、「1.3　基本設定」の項目と同じです。

2.4 詳細設定

詳細設定機能の概要は、「1.4　詳細設定」の項目と同じです。

2.5 ルータ

2.5.1 静的ルーティング

このモジュールを使用すると、管理者はルータのルーティングルールを追加できます。この機能は、ルータと接続しているデバイスが複数存在する場合に役立つことがあります。

静的ルーティングを設定するための手順：

1. ナビゲーションパネルから、**「Root」→「ルータ」→「静的ルーティング」**の順にクリックします。
2. **静的ルーティング機能**：静的ルーティングを有効にするには「有効」を選択します。
3. **ネットワーク/ホストIP**：ルートルールのデスティネーションネットワークまたはホスト。ホストアドレス（「192.168.123.11」など）またはネットワークアドレス（「192.168.0.0」など）を指定できます。
4. **サブネットマスク**：ネットワークIDとサブネットIDのためのビット数を示します。例えば、ドット区切り10進数のサブネットマスクが255.255.255.0である場合、そのサブネットマスクのビット数は24です。デスティネーションがホストである場合、そのサブネットマスクのビット数は32になります。
5. **ゲートウェイ**：これは、パケットがルーティングされる先のゲートウェイのIPアドレスです。指定されたゲートウェイが設定されており、最初に到達可能である必要があります。
6. **メトリック**：メトリックは、ネットワークの距離の値です。
7. **インターフェイス**：ルートルールが適用されるネットワークインターフェイス。

8. **追加/削除**：プロファイルを追加または削除するには、⊕または⊖をクリックします。
9. 完了したら、**「確認」**をクリックします。

2.5.2 動的ルーティング

動的ルーティングは、ルータがルーティング情報を自動的に維持できることを示します。動的ルーティングには、ルーティング情報の維持と、他のルータとのルーティング情報の交換という2つの基本的な機能があります。

動的ルーティングを設定するための手順：

1. ナビゲーションパネルから、**「Root」→「ルータ」→「動的ルーティング」**の順にクリックします。
2. **RIP**：RIPを有効または無効にします。
3. **RIPキー認証**：他のルータとRIPを切り替える場合は認証方法を選択し、認証を無効にするには「None」を選択します。
4. **RIP Key Chain**：RIPキー名を入力します。
5. **RIP Key 0/1**：RIPキー0/1のRIPキー値を入力します。
6. 完了したら、**「確認」**をクリックします。

2.6 動作モード

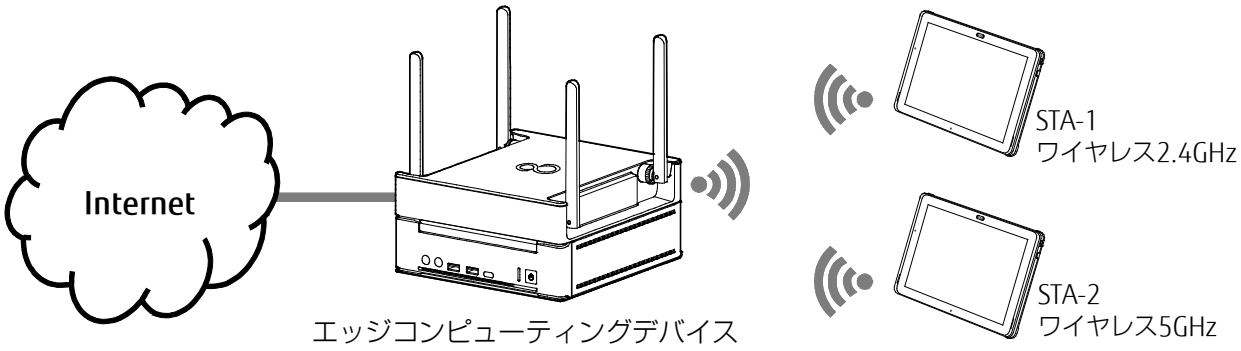
「動作モード」ページでは、ネットワークに適切なモードを選択できます。モードを無線ルータ、アクセスポイント、またはメディアブリッジから選択します。
セキュリティの関係上、アクセスポイントはpingには応答しません。

動作モードを設定するための手順：

1. ナビゲーションパネルから、**「Root」→「動作モード」**の順にクリックします。
2. ルータで実行するモードを選択します。
3. **「適用」**をクリックします。

2.6.1 Wireless Router（ルータ）

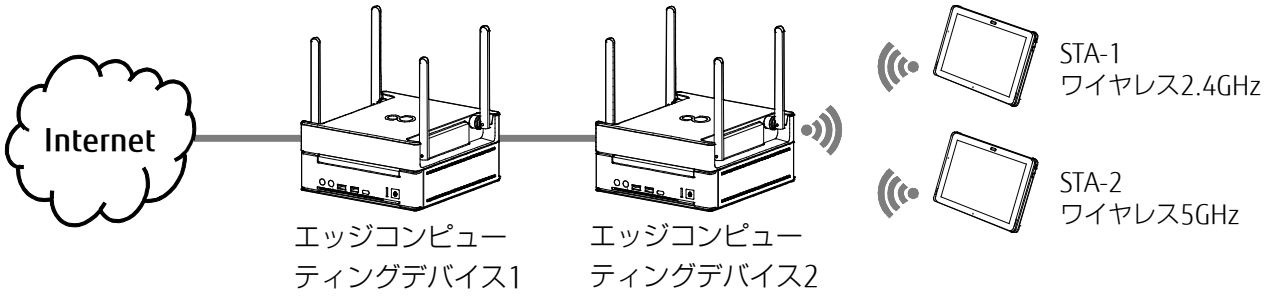
ルータでは、PPPoE、DHCP、PPTP、L2TP、または静的IPアドレス経由でインターネットに接続し、LANクライアントまたはデバイスと無線ネットワークを共有します。このモードでは、NAT、ファイアウォール、およびDHCPサーバがデフォルトで有効になっています。SOHOやホームユーザのために、UPnPおよび動的DNSがサポートされています。新規ユーザである場合や、現在どの有線または無線ルータも使用していない場合は、このモードを選択してください。無線ルータモードを選択し、「適用」をクリックしてウィザードページに移動してから、通常ユーザの設定について**「1.2 ウィザード設定」**をご覧ください。



図は、無線ルータモードトポロジの例を示しています。

2.6.2 Access Point（ブリッジ）

ブリッジでは、他のネットワーククライアントへの無線信号のカバレッジを拡張するために、デバイスがイーサネットケーブル経由で無線ルータに接続します。このモードでは、ファイアウォール、IP共有、およびNAT機能はデフォルトで無効になっています。



図は、アクセスポイントモードトポロジの例を示しています。

ブリッジを設定するための手順：

1. 「動作モード」選択画面で**「Access Point(ブリッジ)」**を選択し、**「適用」**をクリックします。
   - **IPアドレス**：無線ルータのLAN IPアドレス。デフォルト値は192.168.1.1です。IPベースのネットワークでは、データパケットはネットワークデバイス固有のIPアドレスに送信されます。
   - **サブネットマスク**：無線ルータのLANサブネットマスク。デフォルト値は255.255.255.0です。
   - **デフォルトゲートウェイ**：無線ルータのLANのゲートウェイのIPアドレス。
   - **DNSサーバ1**：優先DNSサーバのIPアドレスを入力します。
   - **DNSサーバ2**：代替DNSサーバのIPアドレスを入力します。
   - **「次へ」**をクリックします。

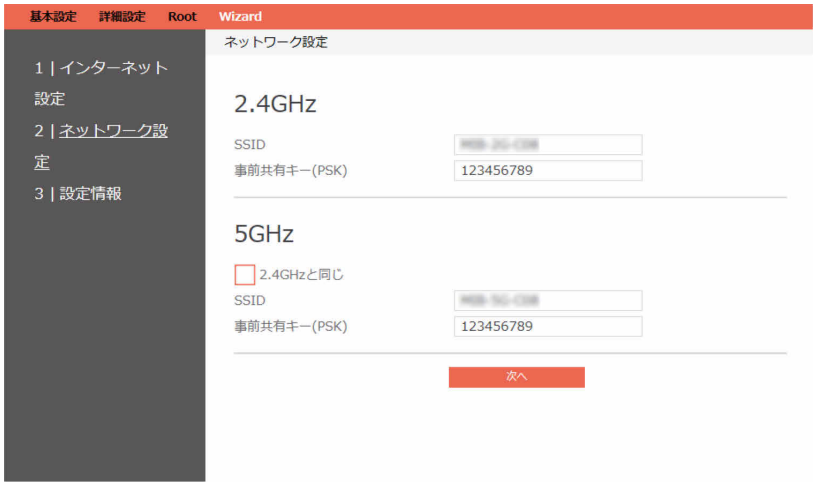
POINT

・グローバルIPアドレスには対応していません。入力すると「マスクエラー」が表示されます。IPアドレスには、プライベートIPアドレスを入力してください。
プライベートIPアドレスとは、組織内のネットワーク（プライベートネットワーク）でのみ使用できるIPアドレスです。プライベートIPアドレスの範囲は次のとおりです。

クラス	範囲	サブネットマスク	アドレス数
クラスA	10.0.0.0~10.255.255.255	255.0.0.0	16,777,216 (16,777,216×1サブネット)
クラスB×16	172.16.0.0~172.31.255.255	255.240.0.0	1,048,576 (65,536×16サブネット)
クラスC×256	192.168.0.0~192.168.255.255	255.255.0.0	65,536 (256×256サブネット)

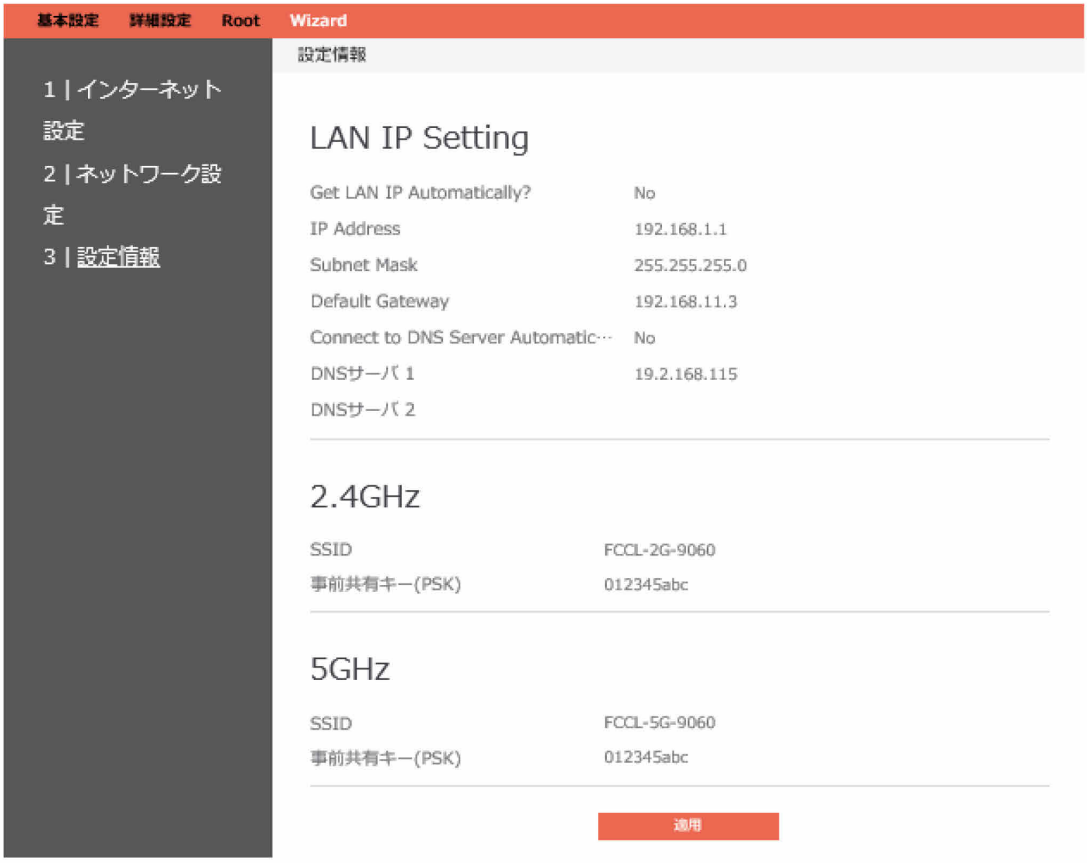
・DNSサーバ1、DNSサーバ2のうち、DNSサーバ1の値は必ず入力する必要があります。
DNSサーバが存在しない場合は、アクセスポイントのIPアドレスを入力してください。

2. 「2.4GHz」および「5GHz」無線接続の無線ネットワーク名（SSID）とセキュリティキーを割り当てます。



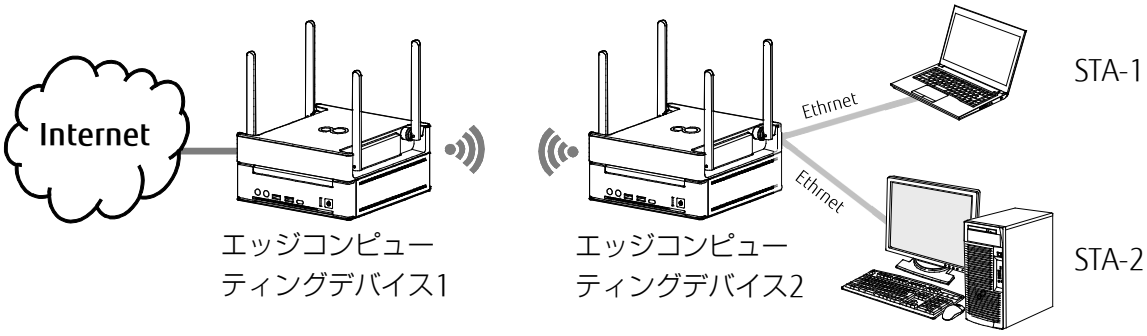
- **SSID**：ネットワーク名またはSSIDは、無線ネットワークを識別する一意の名前です。Wi-Fiデバイスは、範囲内のすべてのネットワークを自動的に検出します。
- **事前共有キー(PSK)**：セキュリティキーは、無線ネットワークを不正なアクセスから保護するために割り当てられたパスワードです。セキュリティで保護されたネットワークにアクセスする場合、ユーザはセキュリティキーを入力するよう求められます。
- 完了したら、「次へ」をクリックします。

3. 新しい構成情報が表示されたら内容を確認して、「適用」をクリックします。



2.6.3 Media Bridge（メディアブリッジモード）

メディアブリッジは、コンピューター、スマートテレビ、ゲームコンソール、DVR、メディアプレーヤーなどの複数のメディアデバイスを高速な802.11ac Wi-Fi接続をイーサネットケーブル経由で同時に提供します。メディアブリッジモードを設定するには、メディアブリッジとして構成されたデバイスとルータとして構成されたデバイスの、2つのデバイスが必要です。



図は、メディアブリッジモードトポロジの例を示しています。

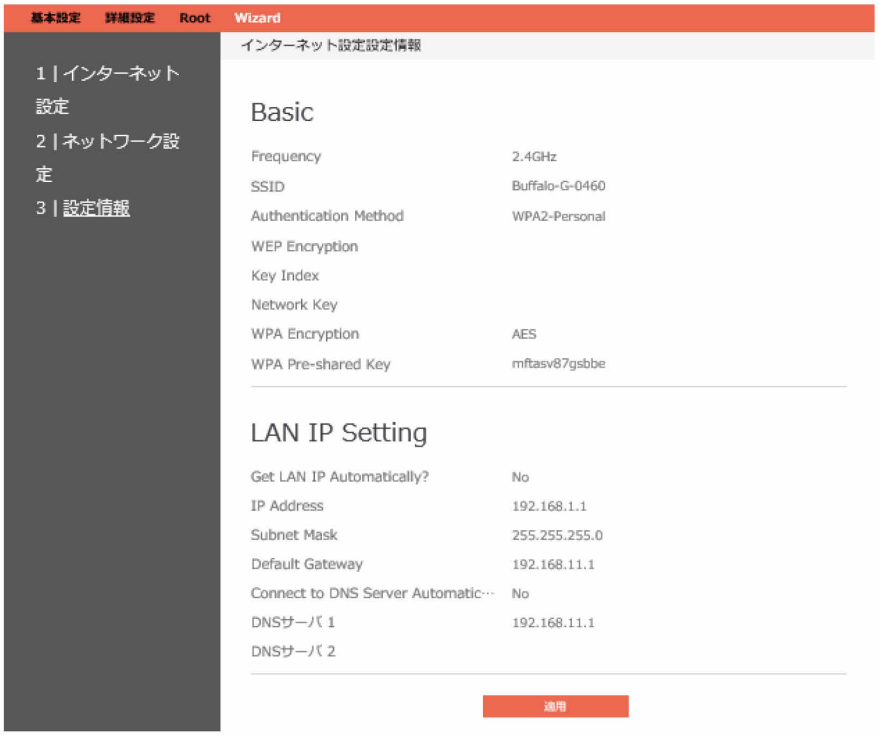
メディアブリッジを設定するには：

1. 「動作モード」選択画面で「Media Bridge（メディアブリッジモード）」を選択し、**「適用」**をクリックします。
   - メディアブリッジの接続先の無線ネットワークを選択し、パスワードを入力します。
   - 完了したら、**「Connect」**をクリックします。

2. LAN IP情報を入力し、「適用」をクリックします。

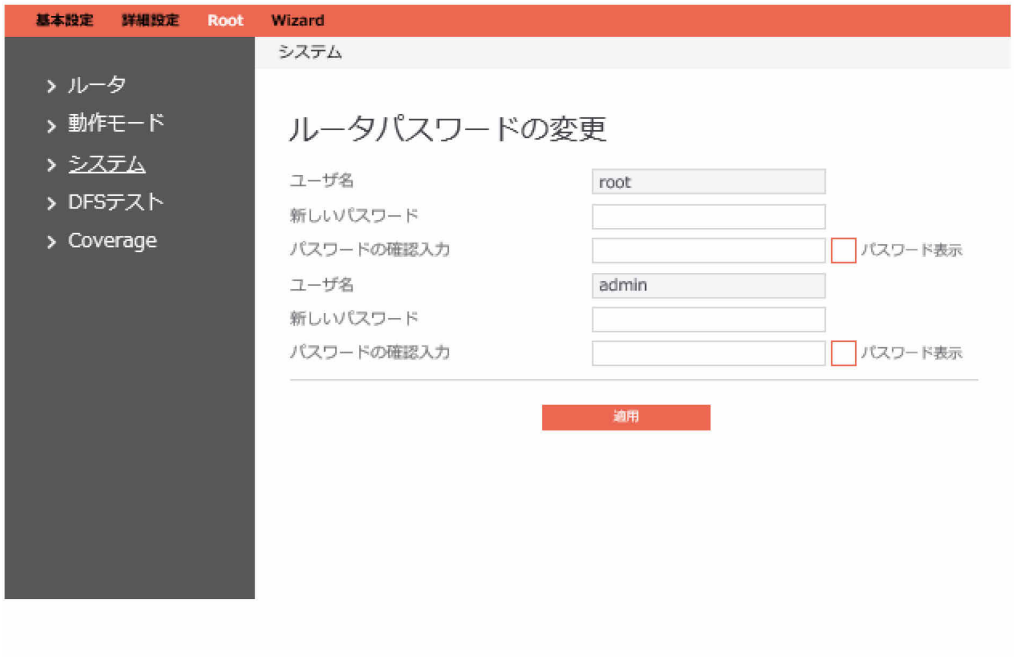
- **IP アドレス**：無線ルータのLAN IPアドレス。デフォルト値は192.168.1.1です。IPベースのネットワークでは、データパケットはネットワークデバイスの固有のIPアドレスに送信されます。
- **サブネットマスク**：無線ルータのLANサブネットマスク。デフォルト値は255.255.255.0です。
- **DNS サーバ1**：優先DNSサーバのIPアドレスを入力します。
- **DNS サーバ2**：代替DNSサーバのIPアドレスを入力します。

3. 新しい構成情報が表示されたら内容を確認して、「適用」をクリックします。



2.7 システム

ここでは、ルートユーザは、「root」のパスワードと「admin」のパスワードを変更できます。



ルータのログインパスワードを変更するための手順：

1. ナビゲーションパネルから、**「Root」→「システム」**の順にクリックします。
2. **新しいパスワード**：使用する新しいパスワードを入力します。4～16文字以内で英数字!#$%&@+*の特殊記号が設定可能です。
3. **パスワードの確認入力**：確認のために新しいパスワードを再入力します。
4. 完了したら、**「適用」**をクリックします。

POINT

・運用管理ツールを利用して運用する際は、エッジコンピューティングデバイスに運用管理ツールクライアント機能をインストール後、必ず「運用管理ツール/AP部 連携用パスワード設定ツール」を実行してください。上記ツールではadminのパスワードを入力する必要があります。

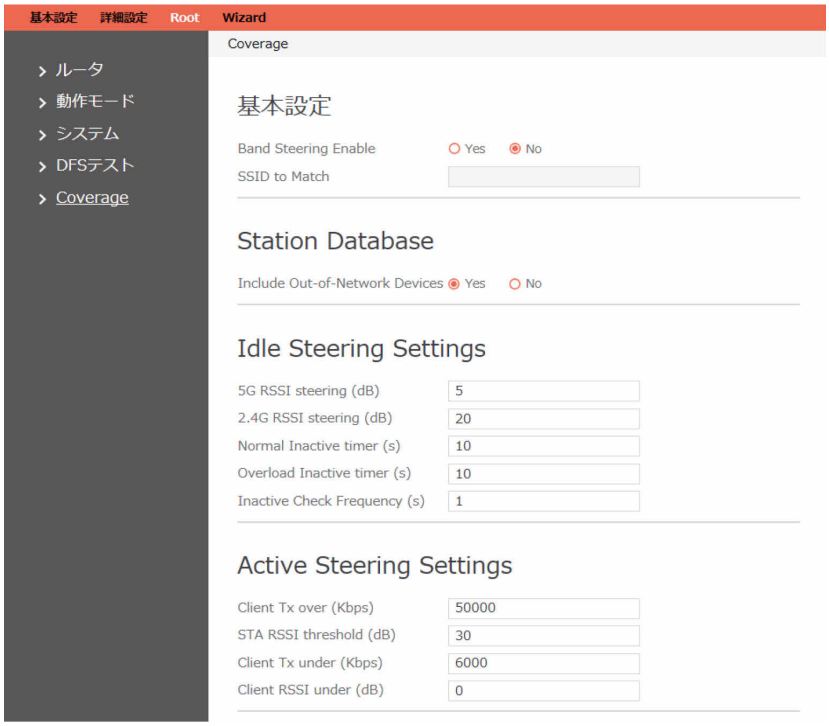
2.8 DFSテストモード

このモジュールは、無線スイッチをテストするために使用されます。

1. ナビゲーションパネルから、「Root」→「DFSテスト」の順にクリックします。
2. **テストモード**：DFSテストモードを有効または無効にします。

2.9 COVERAGE

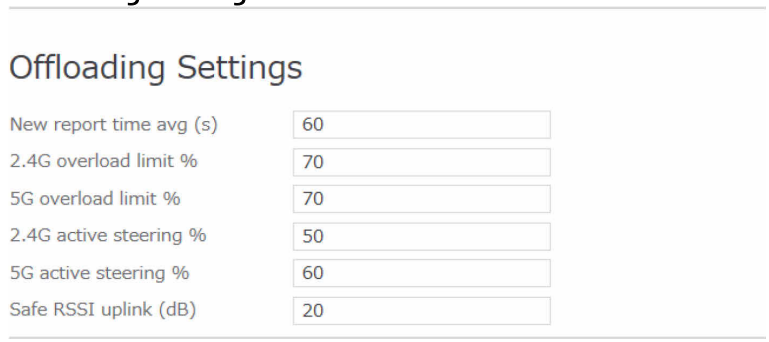
Coverageは、最適な信号条件を維持するために、信号（2.4GHzまたは5GHz）の強度に応じた自動ネットワーク切り替えを可能にします。



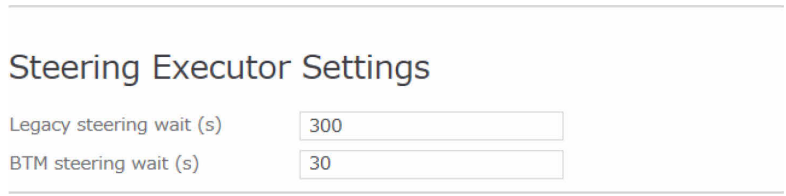
Coverageを設定するための手順：

1. ナビゲーションパネルから、「Root」→「Coverage」の順にクリックします。
2. **基本設定：**
   - Band Steering Enable：負荷分散ロジックを有効または無効にします。家庭内全体のカバレッジは、負荷分散デーモン（lbd）でいくつかの新しいステアリングメカニズムおよびアルゴリズムを提供し、より多くのシナリオを処理し、最新のWi-Fiデバイスでサポートされている機能を活用します。
   - SSID to Match：バンドステアリングを1つのSSIDのみに制限するときに照合するSSIDを入力します。
3. Station Database：
   - ネットワーク外デバイスを含める（Include Out-of-Network Devices）：データベースにネットワーク外デバイスを含めるかどうか指定します。
4. Idle Steering Settings：
   - 5G RSSI steering (dB)：5GHzで関連付けられたノードが2.4GHzにステアリングされることを示すRSSI値（dB）を入力します。
   - 2.4G RSSI steering (dB)：2.4GHzで関連付けられたノードが5GHzにステアリングされることを示すRSSI値（dB）を入力します。。
   - Normal Inactive timer(s)：両方の帯域に過負荷状態が存在しないときの非アクティブ値（秒）を入力します。。
   - Overload Inactive timer(s)：処理中の帯域が過負荷になっているときの非アクティブ値（秒）を入力します。。
   - Inactive Check Frequency(s)：両方の帯域で関連する非アクティブのSTAを確認する頻度（秒単位）を入力します。。

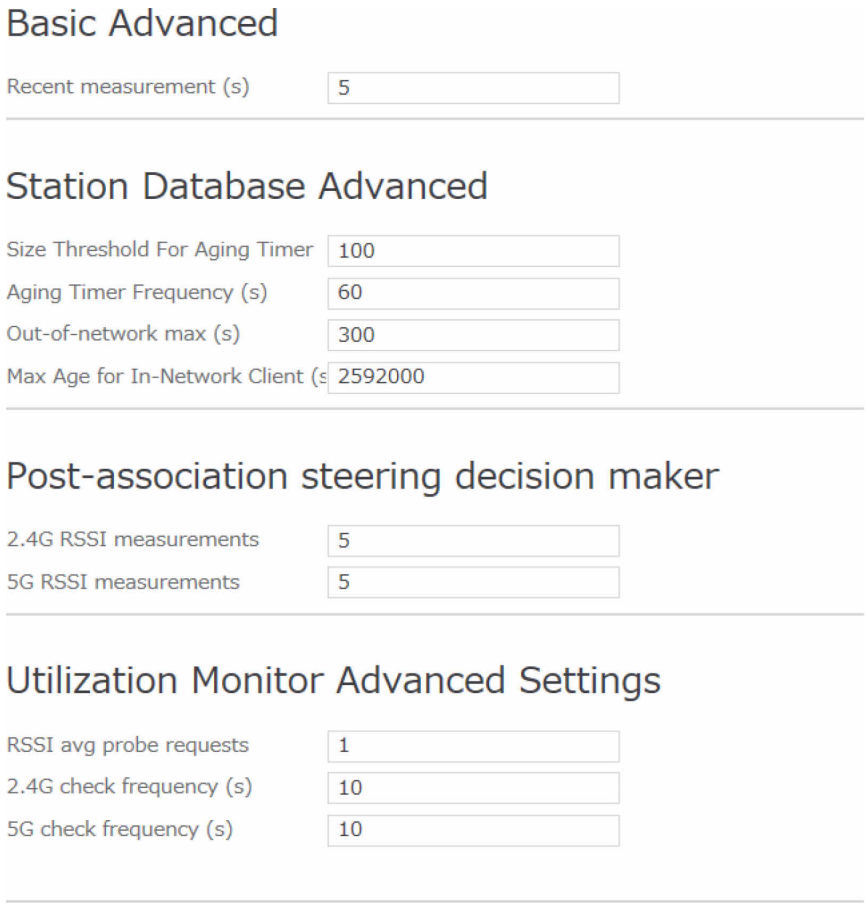
5. Active Steering Settings：
   - Client Tx over(Kbps)：クライアントTxレートがこのしきい値を超えた場合は、通知を生成します（Kbps）。
   - STA RSSI threshold(dB)：STAをレートベースのアップグレードステアリングで評価する場合は、RSSIもこのしきい値を上回っている必要があります（dB）。
   - Client Tx under(Kbps)：クライアントTxレートがこのしきい値を下回った場合は、通知を生成します（Kbps）。
   - Client RSSI under(dB)：クライアントRSSIがこのしきい値を下回った場合は、通知を生成します（dB）。
6. Offloading Settings：



   - New report time avg (s)：新しい使用レポートを生成するまでの平均時間（秒）を入力します。
   - 2.4G overload limit %：2.4GHzでの過負荷状態のメディア使用のしきい値（%）を入力します。
   - 5G overload limit %：5GHzでの過負荷状態のメディア使用のしきい値（%）を入力します。
   - 2.4G active steering %：2.4GHzへのアクティブステアリングでのメディア使用の安全性のしきい値（%）を入力します。
   - 5G active steering %：5GHzへのアクティブステアリングでのメディア使用の安全性のしきい値（%）を入力します。
   - Safe RSSI uplink (dB)：その値を上回ると関連付けが安全と見なされるアップリンクRSSI（dB）を入力します。
7. Steering Executor Settings：



   - Legacy steering wait (s)：ステアリングの完了後にレガシークライアントを再度ステアリングするまでに待機する時間（秒）を入力します。
   - BTM steering wait (s)：認証拒否を送信することなく、ステアリングの完了後にBTM経由でクライアントを再度ステアリングするまでに待機する時間（秒）を入力します。



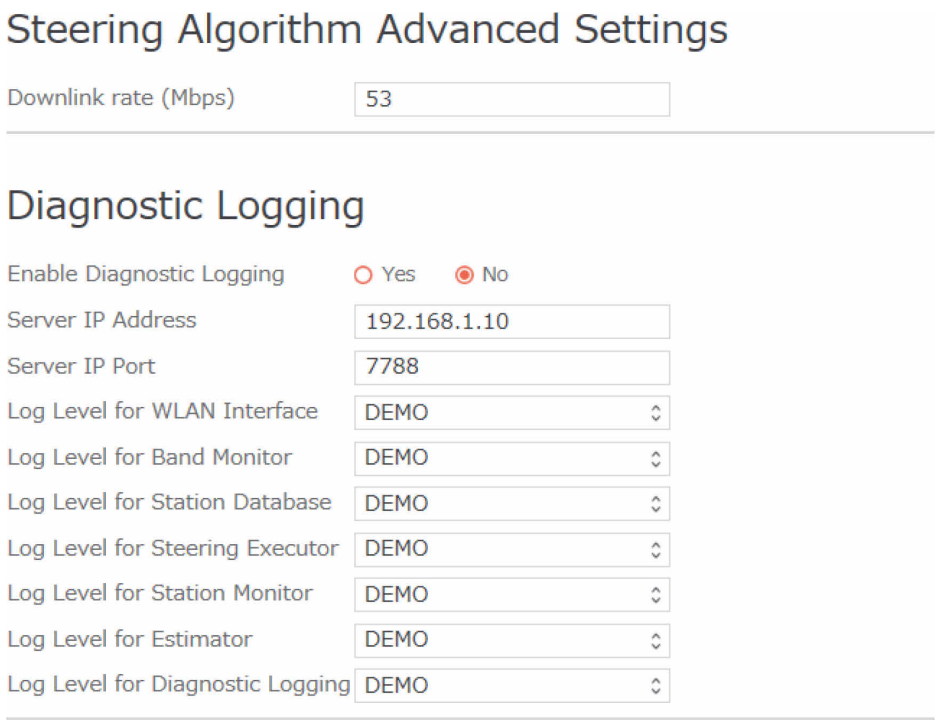
8. Basic Advanced：
   - Recent measurement (s)：最新の測定に対して許可されている最大経過秒数を入力します。
9. Station Database Advanced：
   - Size Threshold For Aging Timer：定期的なエージングがトリガーされるまでステーションデータベースで許可されるエントリの数を入力します。
   - Aging Timer Frequency (s)：エージングがトリガーされた後、ステーションデータベースのエージングを実行する頻度（秒）を入力します。
   - Out-of-network max (s)：ネットワーク外クライアントの最大有効期間（秒）を入力します。
   - Max Age for In-Network Clients(s)： ネットワーク内のエントリの最後の更新から、古すぎると見なされ、データベースから削除されるまでの経過秒数を入力します。削除対象と見なされるのは、関連付けが解除されているエントリだけです。
10. Post-association steering decision maker：
    - 2.4G RSSI measurements：2.4GHz帯域でのRSSI測定の数を入力します。
    - 5G RSSI measurements：5GHz帯域でのRSSI測定の数を入力します。
11. Utilization Monitor Advanced Settings：
    - RSSI avg probe requests：RSSIの平均に必要なプローブ要求の数を入力します。
    - 2.4G check frequency(s)：2.4GHzでのメディア使用を確認する頻度を入力します。
    - 5G check frequency(s)：5GHzでのメディア使用を確認する頻度を入力します。

12. Rate estimation：

- 5G RSSI difference：2.4GHzで測定された値と5GHz RSSI値を予測したときの差異を入力します。
- 2.4G RSSI difference：5GHzで測定された値と2.4GHz RSSI値を予測したときの差異を入力します。
- RSSI avg probe requests：RSSIの平均に必要なプローブ要求の数を入力します。
- Data rate estimate (s)：データレートを予測するための連続した統計サンプル間の秒数を入力します。
- PHY scaling factor (%)：エアタイム計算のためにPHYレートを上位レイヤのレートに変換するためのスケールファクタ（%）を入力します。
- Continuous measure demo：スループットを連続して測定する際に「Yes」にします（デモ目的のみ）。
- 11k active scan (s)：802.11kビーコンレポートで使用されるアクティブスキャンの有効期間（秒）を入力します。
- 11k passive scan (s)：802.11kビーコンレポート要求で使用されるパッシブスキャンの有効期間（秒）を入力します。

13. Steering Executor Advanced Settings：
    - Abort steering time (s)：クライアントがターゲット帯域に関連付ける、アクセスポイントがステアリングを中止するまでの最長時間（秒）を入力します。
    - Coalesce reject time (s)：複数の認証拒否を1つに合体するための時間（秒）を入力します。
    - Max auth. Rejects）：デバイスがステアリング未対応としてマークされるまでの連続した最大認証拒否数を入力します。

- Unfriendly time (s)：デバイスがステアリング未対応と見なされる、再試行までの基準時間（秒）を入力します。
- Max unfriendly STAs (s)：ステアリング未対応のSTAに対するバックオフに使用される最長時間を入力します。バックオフの総量は、min（MaxSteeringUnfriendly, SteeringUnfriendlyTime * 2 ^ CountConsecutiveFailures）として計算されます（秒）
- 2.4G RSSI assoc. (dB) ：2.4GHz帯域が関連付け用には充分ではないことを示すRSSIのしきい値（dB）を入力します。
- 5G RSSI assoc. (dB) ：5GHz帯域が関連付け用には充分ではないことを示すRSSIのしきい値（dB）を入力します。
- Autoremove blacklist (s)：ブラックリストの自動削除までの時間（秒）を入力します。
- BTM response wait (s)： BTM応答を待機する時間（秒）を入力します。
- Association wait (s)：BTM応答受信後の正しい帯域での関連付けを待機する時間（秒）を入力します。
- If set to 1, will also setup blacklist：実際のBTMメッセージングに加えて、ベストエフォートではないステアリングがブラックリストを使用すべきかどうか指定します。
- BTM unfriendly (s)：デバイスがBTMステアリング未対応と見なされる、BTM経由でステアリングを再試行するまでの基準時間（秒）を入力します。。
- Unfriendly BTM STAs (s)：BTM未対応のSTAに対するバックオフに使用される最長時間を入力します。バックオフの総量は、min（MaxBTMUnfriendly, BTMUnfriendlyTime * 2 ^ CountConsecutiveFailures）として計算されます（秒）。
- BTM STA backoff (s)：アクティブステアリングを失敗したBTM STAに対するバックオフに使用される最長時間を入力します。。バックオフの総量は、min（MaxBTMActiveUnfriendly, BTMUnfriendlyTime * 2 ^ CountConsecutiveFailures）として計算されます（秒）。
- Min best effort RSSI dB：その値を下回るとlbdがベストエフォートでしかクライアントをステアリングしなくなる最小のRSSI（ブラックリストなし、失敗しても未対応としてマークされない）（dB）を入力します。
- RSSI indication (dB) ：クライアントがその値に達したら通知を生成するRSSIのしきい値（dB）を入力します。



14.Steering Algorithm Advanced Settings：
- Downlink rate (Mbps)：過負荷のために2.4GHzから5GHzにステアリングする場合、ダウンリンクレート（Mbps）は少なくともLow TxRateXingThresholdにこの値を加算した値を超える必要があります。

15.Diagnostic Logging：
- Enable Diagnostic Logging：処理されたすべてのトラフィックパケットに関する情報を取得するか指定します。
- Server IP Address：診断ログサーバのIPアドレスを入力します。
- Server IP Port：診断ログサーバに接続するためのポート番号を入力します。
- Log Level for WLAN Interface：WLANインターフェイスの診断ログレベルを決定します。
- Log Level for Band Monitor：バンドモニターの診断ログレベルを決定します。
- Log Level for Station Database：ステーションデータベースの診断ログレベルを決定します。
- Log Level for Steering Executor：ステアリングエグゼキューターの診断ログレベルを決定します。
- Log Level for Station Monitor：ステーションモニターの診断ログレベルを決定します。
- Log Level for Estimator：エスティメーターの診断ログレベルを決定します。
- Log Level for Diagnostic Logging：診断ログの診断ログレベルを決定します。

ESPRIMO Edge Computing Edition
アクセスポイント操作ガイド
B6FY-4781-01 Z0-02
発行日：2020 年 4 月
発行責任：富士通株式会社
〒105-7123 東京都港区東新橋 1-5-2 汐留シティセンター