HWL-3511-DS

取扱説明書

HYTEC INTER Co., Ltd.

第 1.3 版

管理番号:RFD-20MA0005-01.3

ご注意

- 本書の中に含まれる情報は、弊社（ハイテクインター株式会社）の所有するものであり、弊社の同意なしに、全体または一部を複写または転載することは禁止されています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容については万全を期して作成いたしましたが、万一、ご不審な点や誤り、記載漏れなどのお気づきの点がありましたらご連絡ください。

電波障害自主規制について

この装置は，クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

改版履歴

第 1 版	2020 年 11 月 2 日 新規作成
第 1.1 版	2020 年 11 月 09 日 改定（AC アダプター変更）
第 1.2 版	2020 年 11 月11 日 改定（誤記修正）
第 1.3 版	2021 年 11 月 05 日 改定（SMS 項目の追加）

ご使用上の注意事項

- 本製品及び付属品をご使用の際は、取扱説明書に従って正しい取り扱いをしてください。
- 本製品及び付属品を分解したり改造したりすることは絶対に行わないでください。
- 本製品及び付属品を直射日光の当たる場所や、温度の高い場所で使用しないでください。本体内部の温度が上がり、故障や火災の原因になることがあります。
- 本製品及び付属品を暖房器具などのそばに置かないでください。ケーブルの被覆が溶けて感電や故障、火災の原因になることがあります。
- 本製品及び付属品をほこりや湿気の多い場所、油煙や湯気のあたる場所で使用しないでください。故障や火災の原因になることがあります。
- 本製品及び付属品を重ねて使用しないでください。故障や火災の原因になることがあります。
- 通気口をふさがないでください。本体内部に熱がこもり、火災の原因になることがあります。
- 通気口の隙間などから液体、金属などの異物を入れないでください。感電や故障の原因になることがあります。
- 付属のACアダプタは本製品専用となります。他の機器には接続しないでください。
  また、付属品以外のACアダプタを本製品に接続しないでください。
- 本製品及び付属品の故障、誤動作、不具合、あるいは天災、停電等の外部要因によって、通信などの機会を逸したために生じた損害等の純粋経済損害につきましては、弊社は一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品及び付属品は、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。

目次

1. 製品概要

HWL-3511-DS は、-20～+60℃の広い動作温度に対応した産業用の LTE ルーターです。カテゴリー6のモジュールが使用されており、DL：300Mbps max, UL：50Mbps max となっています。

また、LTE2 回線を使用することにより、主回線が故障した場合に副回線に切り替えるフェールオーバー機能を搭載しています。

2. 梱包物一覧

ご使用いただく前に本体と付属品を確認してください。万一、不足の品がありましたら、お手数ですがお買い上げの販売店までご連絡ください。

名　称	数 量
本体	1 台
LTE アンテナ	2 本
WiFi アンテナ	1 本
AC アダプタ	1 個
ゴム製足	4 個
DIN レールブラケット	2 個

3. 設定および保守時の注意

3.1. 熱に関する注意事項

注意：**金属製ケースの表面温度は、非常に高くなる恐れがあります。**特に長時間動作させた後、空調のない閉じたキャビネットに設置した場合や周囲温度が高い空間に設置した場合は注意してください。

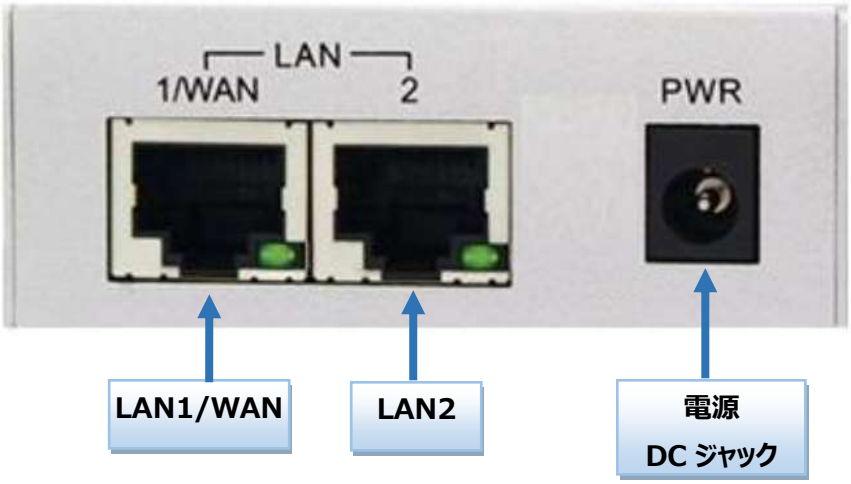
4. 製品外観

4.1. LED

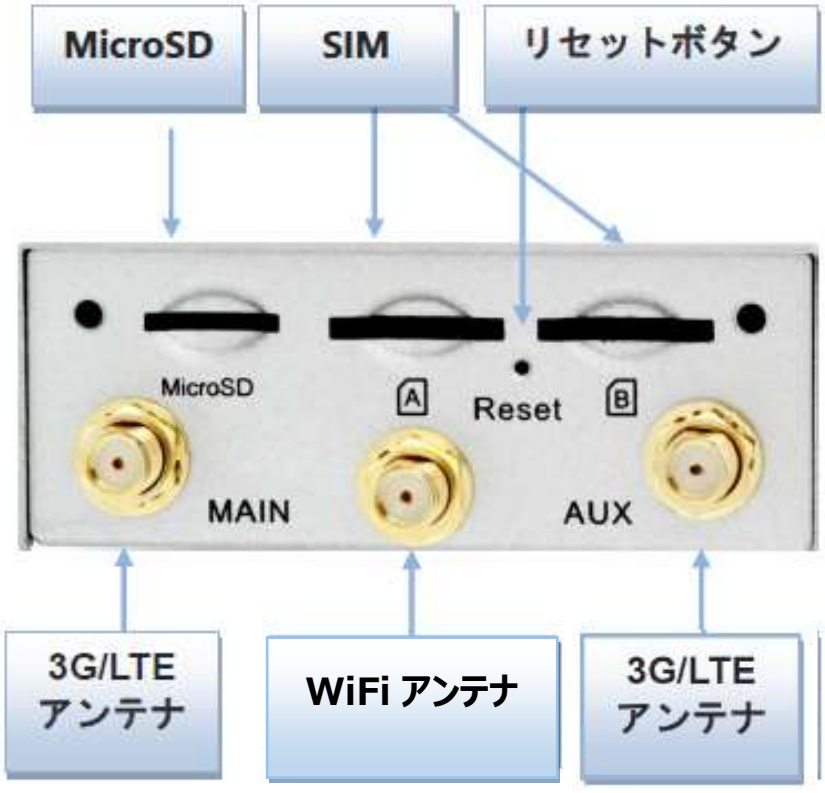
4.1.1. 各 LED

表示		説明
Signal	**点灯**	モバイル回線の接続状態を表します。 ● 青 :LTE で接続しています。 ● 紫 :HSPA/3G で接続しています。 ● 赤 :GSM/2G で接続しています。
	点滅	信号強度を表示します。 ● 高速 :0～30%です。 ● 低速 :31～60%です。 ● 点灯 :61～100%です。
WiFi	**点灯**	WiFi は有効になっています。
	点滅	WiFi で通信をしています。
	消灯	WiFi は無効になっています。
Status	**点滅**	デバイスの状態を表します。 ● 低速 :デバイスは正常に動作しています。 ● 高速 :デバイスはリカバリモードか異常状態です。

4.2. 前面



4.3. 背面



リセットボタン

◆ リセットボタンを 6 秒～8 秒間押し続けてから放すと、設定を初期化することが出来ます。

4.4. SIM カードの取り付け/取り外し方法

SIM カードの取り付け/取り外し方法について説明します。

◆SIM カバーを取り外します。

◆SIM カードを挿入します。

◆SIM カバーを取り付けます。

注意事項

SIM カードの取り付け/取り外しを行う際は、必ず機器の電源をオフにしてください。

5. WEB GUI での設定について

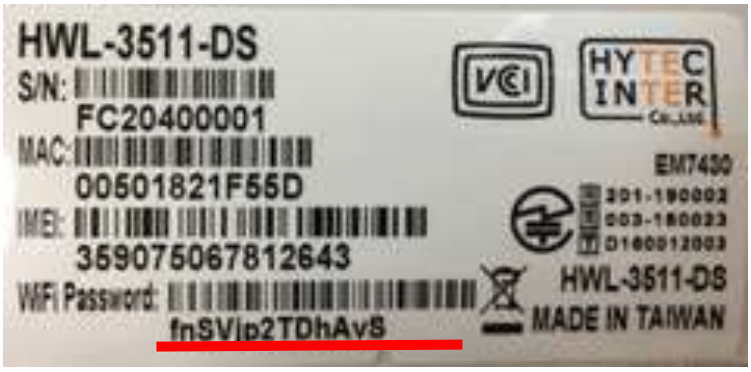
5.1. WEB GUI へのアクセス

5.1.1. PC システム要件

ネットワーク要件	PC にイーサネットアダプタが搭載されている
OS 要件	Windows®、Machintosh、Linux ベースの OS
Web ブラウザ要件	・Internet Explorer 6.0 以降 ・Microsoft Edge ・Chrome 2.0 以降 ・Firefox 3.0 以降 ・Safari 3.0 以降

5.1.2. ログイン初期設定

項目	初期値
IP アドレス	192.168.123.254
ユーザ名	admin
パスワード	admin
WiFi SSID	Staff_2.4G
WiFi Password	本体ラベルに表示(注 1)



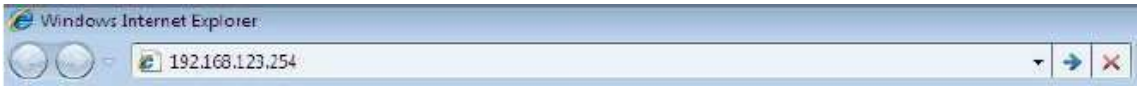
（注１） 装置ごとで WiFi Password（事前共有キー）は異なります。

5.1.3. ログイン手順

◆接続する PC の IP アドレスを 192.168.123.0/24 のネットワークの 192.168.123.254 以外のホストアドレスに設定します。

◆PC をデバイスの LAN ポートに接続します。

◆ブラウザのアドレスバーに http://192.168.123.254 と入力して接続します。



◆ログイン画面が表示されますので、ユーザ名とパスワード「admin」を入力して、ログイン ボタンをクリックします。

（注１） 本製品の工場出荷時 LAN IP アドレスは 192.168.123.254 です。変更した場合は、新しい IP アドレスを使用して、再度ログインをする必要があります。

（注２） ログインパスワードは工場出荷時設定より変更することを推奨します。

◆初期時には管理パスワードの変更を行います。<推奨> 新しいパスワードを入力して OK ボタンをクリックします。

◆再度ログイン画面が表示されますので、ユーザー名「admin」、設定した新しいパスワードを入力し、ログインボタンをクリックしてログインしてください。

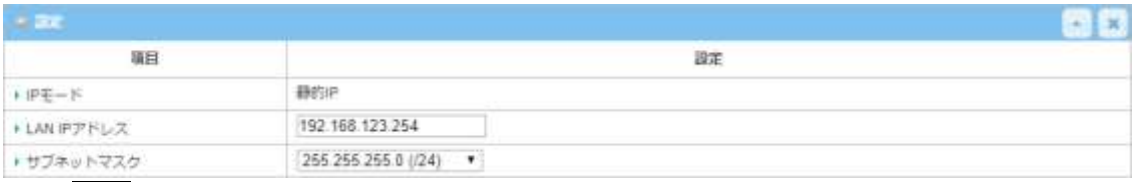
5.1.4. Web 表示言語の変更

◆工場出荷時点では WEB GUI は日本語表示です。ページ左上の Language（言語）を変更することで表記言語を変更できます。

5.2. LAN 側 IP アドレスの設定

◆画面左側のメニューから、基本ネットワーク ⇒ LAN および VLAN の順にクリックします。

◆LAN IP アドレスとサブネットマスクを設定します。



◆保存ボタンをクリックします。

◆保存後にには新しい IP アドレスでログインし直す必要があります。

5.3. 管理ユーザー名の変更

◆画面左側のメニューから、管理(Administration) ⇒ システム管理⇒ パスワード＆MMI の順にクリックします。

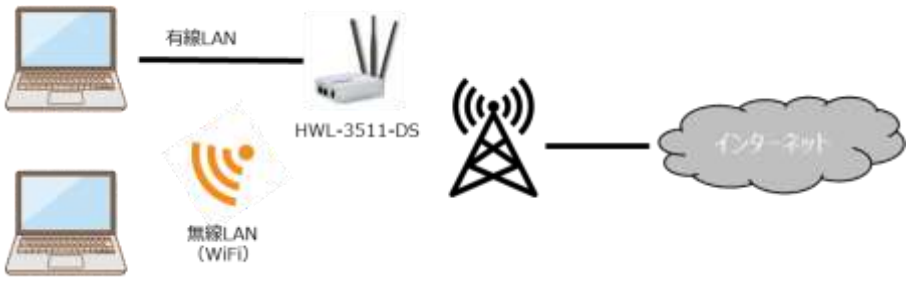
◆「ユーザー名」の変更ボタンを押し、管理用の新しいユーザー名と現在のパスワードを入力します。

◆保存ボタンをクリックします。

◆変更が成功するとログイン画面が表示されます。新しいユーザー名でログインしてください。

✧ 基本設定編

本章では、もっとも一般的な HWL-3511-DS を 3G/4G(LTE)回線でインターネットに接続するための設定について説明します。



6. LTE の設定

LTE 回線経由でインターネットに接続するための設定を行います。

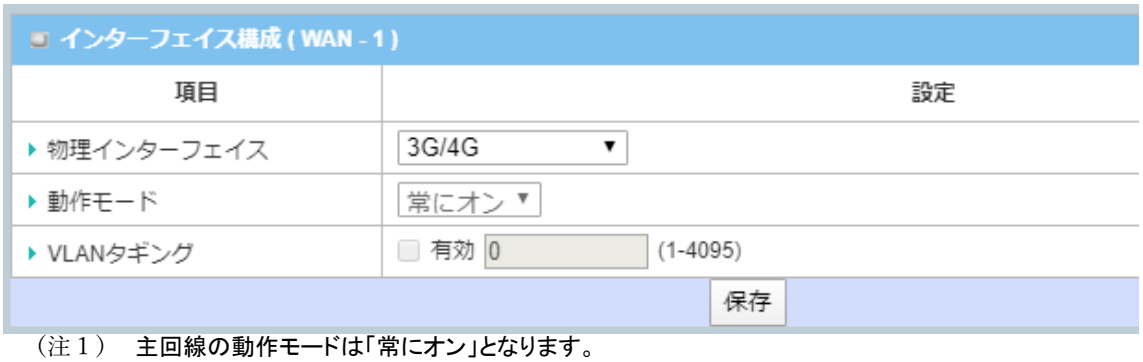
6.1. 物理インターフェイスの設定

注）本設定は工場出荷時のままで問題ありません。

◆画面左側のメニューから、基本ネットワーク ⇒ WAN&アップリンク ⇒ 物理インターフェイス の順にクリックします。

項目	説明
インターフェイス名	インターフェイス名を表示します。
物理インターフェイス	物理インターフェイスの種類を表示します。
動作モード	動作モードを表示します。
アクション	編集ボタンをクリックすると、設定変更を行うことができます。

◆WAN-1 の編集をクリックします。



（注１） 主回線の動作モードは「常にオン」となります。

◆物理インターフェイスを「3G/4G」、インターネットサービスプロバイダーにより VLAN タギングが指定されている場合は、有効をチェックして VLAN ID を入力します。

◆保存をクリックします。

6.2. LTE パラメータの設定

◆画面左側のメニューから、基本ネットワーク ⇒ WAN&アップリンク ⇒ 接続設定の順にクリックします。

◆WAN-1 の編集をクリックします。

◆[3G/4G WAN タイプ構成]を「SIM-A のみ」に設定します。

（注１） スロット A に SIM が挿入されていることを確認してください。
（注２） 自動機内モードは本機では使用できません。

◆[SIM-A カードとの接続]をご契約の回線の指定に合わせて設定します。

項目	説明
ネットワークタイプ	自動に設定します。
ダイアルアップ プロファイル	手動設定にします。
APN	APN を入力します。(ご契約に合わせて設定してください。)
IP タイプ	IP タイプを選択します。(ご契約に合わせて設定してください。)
PIN コード	PIN コードを入力します。(ご契約に合わせて設定してください。注1)
ダイヤルナンバー	ダイヤルナンバーを入力します。 (ご契約に合わせて設定してください。(注1)
アカウント	認証に使用するアカウントとパスワードを入力します。 (ご契約に合わせて設定してください注)
パスワード	
認証	認証方式を選択します。(ご契約に合わせて設定してください)
IP モード	動的 IP を選択します。
プライマリ DNS	特定の DNS サーバーを使用したいときのみ設定を入力します。
セカンダリ DNS	
ローミング	本機は国内使用専用機器であるためサポートしていません。

(注1) PIN コード、ダイヤルナンバー、アカウント、パスワードの指定が無い場合は、空欄にしてください。

◆[3G/4G 接続の共通設定]を設定します。

項目	説明
接続制御	自動再接続を選択します。
時間スケジュール	(0)常時固定です。
MTU 設定	☑をはずし無効にします。
IP パススルー	☑をはずし無効にします。
NAT	☑を入れ有効にします。
IGMP	無効を選択します。
WAN IP エイリアス	ご使用の機器ではこの機能はご使用になれません。

◆[ネットワークの監視構成]を設定します。

項目	説明
ネットワーク監視構成	☑をはずし無効にします。 本設定は、回線切り替えのフェールオーバー機能などで使用するものです。監視のためのデータ通信が行われるため、1 回線の場合は無効にしてください。
チェック方法	設定不要です。
読み込み確認	
クエリ間隔	
レイテンシーしきい値	設定不要です。
失敗しきい値	
ターゲット1	
ターゲット2	

◆ページ最後の保存ボタンをクリックして設定を保存してください。

7. WiFi（無線 LAN）の設定

スマートフォンなどをインターネットに接続する WiFi（無線 LAN）の設定を行います。

WiFi モジュール1は工場出荷時に有効に設定されています。初期電源投入時に WiFi 接続のための SSID は”Staff_2.4G”、WPA2-PSK の WiFi Password(事前共有キー)は、本体ラベルに表示されています。

7.1. WiFi モジュールの設定

◆画面左側のメニューから、基本ネットワーク ⇒ WiFi ⇒ WiFi モジュール１の順にクリックします。

◆[基本構成]の設定：本製品は IEEE802.11n/g/b 対応モジュールを搭載しているため、2.4GHz の周波数帯のみ対応しています。そのため、本設定は必要はありません。

◆[2.4GWiFi 構成]で WiFi モジュールの基本動作モードを設定します。

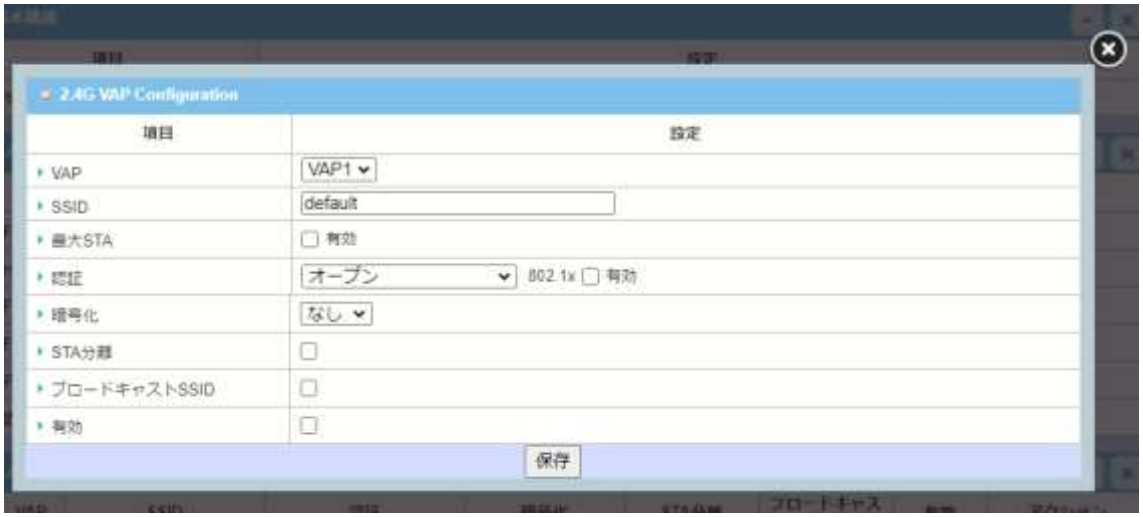
項目	説明
WiFi モジュール	無線 LAN を使用する場合は☑を入れ有効にします。 使用しない場合は☑を外して無効にしてください。無効の場合は以降の設定は不要です。
チャネル	自動を選択し、干渉が少ないを選択してください。
WiFi システム	[802.11b/g/n ミックス]を選択してください。
WiFi 動作モード	[AP ルーターモード]
VAP 分離	☑を外しバーチャルアクセスポイント(VAP)分離を無効にしてください。注

項目	説明
時間スケジュール	(0)常時を選択します。

（注１） VAP とはバーチャルアクセスポイントを指します。本製品は無線 LAN を最大 2 個の VAP を設定することで、ネットワークを分離することができます。

◆保存ボタンをクリックし保存してください。

◆[2.4GVAP リスト]で WiFi の SSID やパスワードなどを設定します。追加ボタンをクリックして各項目を入力してください。各項目入力完了後に保存ボタンをクリックして設定を保存してください。



項目	説明
VAP	VAP1 を選択してください。
SSID	アクセスポイントの SSID を入力してください。
最大 STA 数	接続できるデバイス数を制限する場合は、☑をして有効にするほか、最大デバイス数を入力してください。
認証	[WPA-PSK/WPA2-PSK]を選択してください。
暗号化	[AES]を選択してください。
プリシェアーキー	認証用のパスワード（プリシェアーキー）を入力してください。
STA 分離	☑をはずし無効にします。
ブロードキャスト SSID	☑を入れ有効にします。無効にすると接続デバイスのアクセスポイントリストに表示されなくなります。

◆PC，スマートフォンに、設定した SSID、パスワード（事前共有キー）を指定して、WiFi 接続してください。 **<PC，スマートフォンの設定はそれぞれの説明書を参照してください。>**

✧ 応用設定編

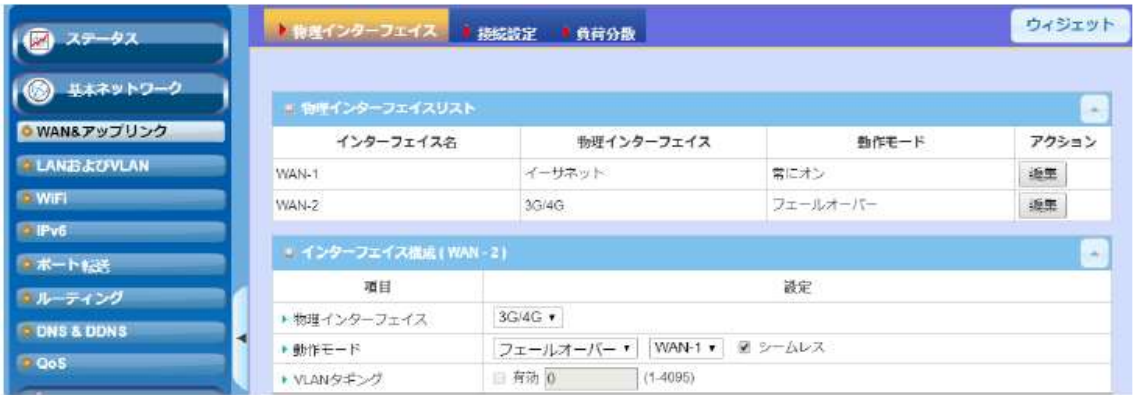
これ以降は詳細な設定について説明します。

8. 基本ネットワーク

本ページ以降詳細な設定について説明します。

8.1. WAN およびアップリンク

本機は、二つの WAN インターフェイスを搭載し、4G（LTE）/3G、イーサネット、WiFi モジュールの中から 2 つを選択することが可能です。WAN 接続により LAN/無線 LAN（WiFi）に接続された全ての PC、サーバー、スマートフォンがインターネットにアクセスできるようにします。WAN の物理インターフェイスおよびインターネットにアクセスするための様々な設定を行うことができます。各 WAN インターフェイスに対して、主インターフェイス(WAN-1)を選択し、その後、WAN 接続のための情報の設定をします。



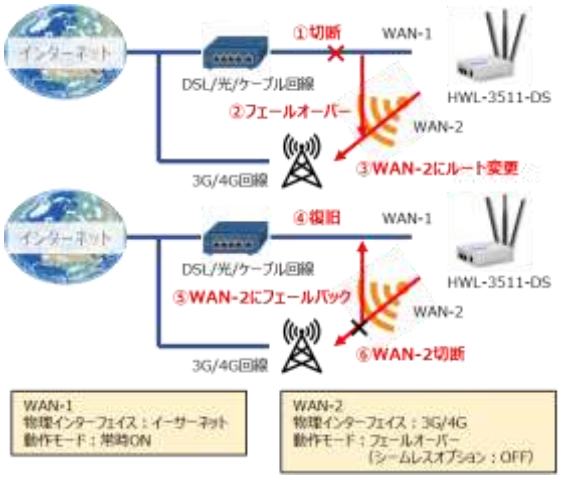
8.1.1. 物理インターフェイスリスト

項目	説明
インターフェイス名	インターフェイス名を表示します。
物理インターフェイス	物理インターフェイスの種類を表示します。
動作モード	動作モードを表示します。
アクション	編集ボタンをクリックすると、設定変更を行うことができます。

8.1.2. フェールオーバー機能

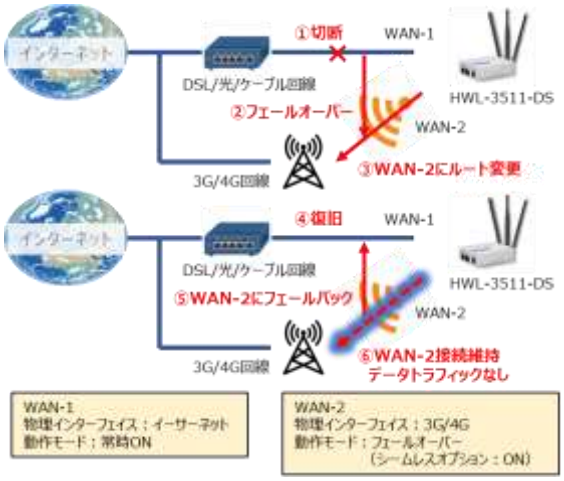
物理インターフェイス WAN-1(主インターフェイス)に回線の障害などが発生し通信が遮断した時に、WAN-2(副インターフェイス)に自動的に切り替える機能がフェールオーバー機能です。WAN-1 にイーサネットを WAN-2 に 3G/4G を割り当てたとすると、以下のような動作をします。

1) フェールオーバー(シームレスオプション:OFF)



フェールオーバーに設定した WAN-2 は WAN-1 のバックアップ接続です。これは主インターフェイスの WAN 接続が切断されたときのみ、切断していた WAN-2 によるバックアップ接続が行われ通信を継続します。次に、WAN-1 が復旧すると、WAN-2 から WAN-1 にフェールバックして WAN-2 を切断します。

2) フェールオーバー(シームレスオプション:ON)



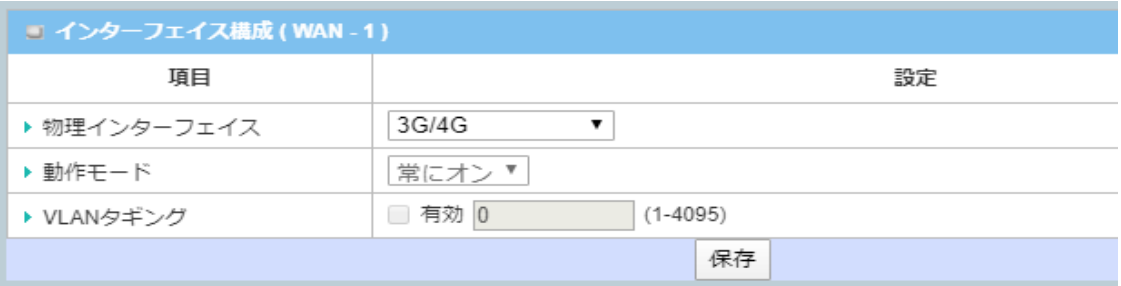
シームレスオプションを ON に設定すると、副回線である WAN-1 と同じく WAN-2 も同時に接続を開始します。この時に WAN-2 でデータの送受信は行われません。WAN-1 が切断されたときに、WAN-2 のデータ送受信を開始します。WAN-1 復旧時にはデータ送受信が WAN-1 側に移行しますが、WAN-2 は接続を維持します。このように、WAN-2 のバックアップ接続動作が無い分フェールオーバーにかかる切り替え時間が短縮できます。

(注1) ネットワークの監視は接続設定内の[ネットワーク監視構成]の設定により実行されます。切断検出時間は 4 秒以上となります。
(注2) シームレスオプション OFF の場合は LTE の接続を実行するため、WAN-2 のデータ送受信開始まで最低でも1分以上必要となります。
(注3) フェールオーバーはルート変更を伴うため、データ送受信を継続できないことがあります。この場合はデータ送受信のリスタートを実施してください。

8.1.3. 物理インターフェイスの設定

◆画面左側のメニューから、基本ネットワーク⇒WAN&アップリンク⇒物理インターフェイスの順にクリックします。

◆物理インターフェイスリスト内の WAN-1 または WAN-2 の編集ボタンをクリックします。



項目	説明
物理インターフェイス	WAN-1 または WNA-2 のインターフェイスを以下から選択します。 ・イーサネット ・3G/4G ・WiFi モジュール1
動作モード	動作モードを以下から選択します。(WAN-2 のみ) ◆無効 :WAN-2 のインターフェイスを無効にします。 ◆フェールオーバー :WAN-2 はバックアップの接続として動作します。WAN-1 の接続が切断された場合に有効になります。 さらに、"シームレス"にチェックをすると、WAN-2 はアクティブ状態でスタンバイし、WAN-1 接続が切断された場合に、より短時間で切り替わります。
VLAN タギング	ISP(インターネットプロバイダ)によって VLAN タギング設定が必要な時に、有効にして契約にある VLAN ID(1～4095)を入力します。

8.1.4. 接続設定

各々の物理インターフェイスを選択したのち、本装置がインターネットに接続するために必要な接続設定を行います。接続設定には、物理インターフェイスの種別によりISP 及びWAN ネットワークに適合した関連パラメータを設定する必要があります。

◆画面左側のメニューから、基本ネットワーク⇒WAN&アップリンク⇒接続設定の順にクリックします。

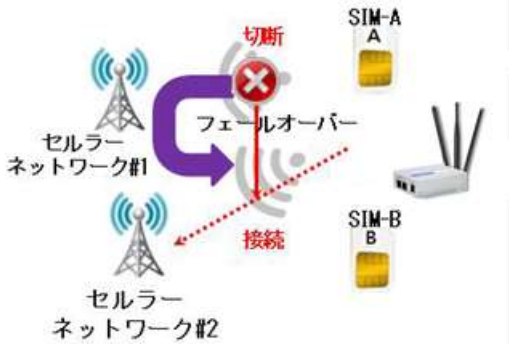
◆インターネット接続リスト内の WAN-1 または WAN-2 の編集ボタンをクリックします。

8.1.5. WAN タイプ：3G/4G の接続設定

8.1.5.1. デュアル SIM フェールオーバー機能について

デュアル SIM フェールオーバーは 2 枚の SIM カード に対応し、3G/4G を 2 回線使用したフェールオーバー機能を搭載しています。そのため、1 回線が不通に陥った時でも、もう 1 回線を利用し通信を継続することが可能です(*1)。また、フェールバック機能を組み合わせることにより様々な冗長性を確保することが可能となります。

1) SIM-A /SIM-B 優先あり、フェールバック無効



通常は優先された回線を使用します。回ネットワーク監視構成の条件を満たしたり、SIM 転換のポリシーで設定された条件を満たしたりしたときに、もう一回線へ切り替えます(*2)。このモードの場合 SIM-A/SIM-B の回線は交互に使用されますが、優先順位の高い SIM にスイッチバックすることはありません。

2) SIM-A /SIM-B 優先あり、フェールバック有効

フェールバックを有効にすると、優先順位の低いバックアップ回線に接続した後に、優先順位の高い回線が使用可能であるかどうかを一定間隔（設定値 5～1440 分）で確認し(*2)、回線の回復が確認できた場合は、優先順位の高い回線にスイッチバックします。

（注１） フェールオーバーが完了するまでには、各種設定にもよりますが最低でも 2 分以上の時間が必要です。フェールオーバーによる回線切り替え中の通信は保証されません。
（注２） フェールバック確認中にも 1 分以上の時間が必要です。フェールバックにより優先回線に接続できる前または非優先回線に戻る前の通信は保証されません。

8.1.5.2. インターネット接続構成および 3G/4G の WAN タイプ構成

項目	説明
WAN タイプ	3G/4G が工場出荷設定で選択されています。本設定は変更できません。
優先 SIM カード	[SIM-A は優先度が高い] 又は [SIM-B は優先度が高い]を選択 SIM カードスロットの優先順位を設定します。本設定の詳細はデュアル SIM フェールオーバー機能（7.5.1.1 項）を参照してください。 [SIM-A のみ] 又は [SIM-B のみ] を選択 選択した SIM 情報を使い接続をします。
自動機内モード	HWL-3511-DS ではサポートしておりません。チェックを外して無効にしてください。
SIM 転換のポリシー	SIM-A/B の切り替えのためのポリシーが設定できます。[SIM-A は優先度が高い]または[SIM-B は優先度が高い]を選択した場合に表示されます。

8.1.5.3. SIM 転換のポリシーの設定

◆SIM 転換ポリシー項目内のポリシー設定ボタンをクリックして設定項目画面を表示させます。

項目	説明
接続失敗	3G/4G の接続切替の回数を設定します。0 に設定すると、切替が実行されません。
RSSI 監視	有効☑にすると、接続中の 3G/4G の受信レベルが設定値(-90～-113dBm)より低くなると、 優先順位の高い SIM から低い SIM に転換し、接続を実行します。無効にすると、受信レベルを監視しません。
ネットワーク・サービス	有効☑にすると、3G/4G 信号が設定時間（1～30 分）内に受信できないときに、優先順位の高い SIM から低い SIM に転換し、接続を実行します。 無効にすると、即時切替えします。
ローミング・サービス	国内使用専用機であるため本機能は使用できません。無効にしてください。

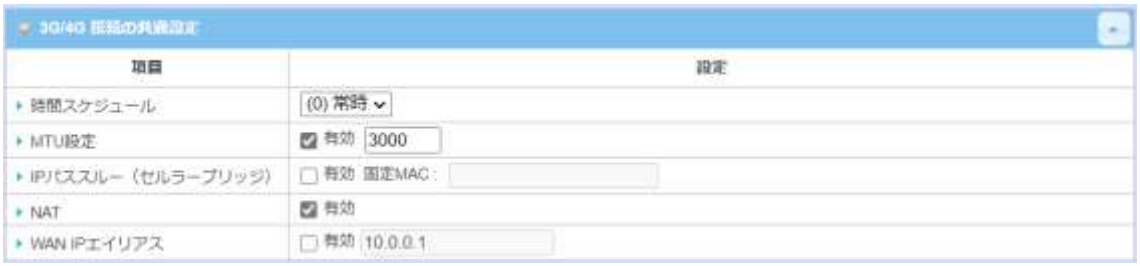
8.1.5.4. SIM-A カードとの接続/SIM-B カードとの接続

3G/4G 回線のご契約に合わせて、設定するパラメータです。

項目	説明
ネットワークタイプ	ネットワークタイプを[自動]、[3G のみ]、[LTE のみ] から選択します。[自動]を選択することを推奨しております。
ダイアルアッププロファイル	手動設定、自動検出から選択します。手動設定にすることを推奨しております。お使いの機器はプロファイルリストをサポートしていません。
APN	APN を入力します。(ご契約に合わせて設定します)
IP タイプ	IP タイプを選択します。(ご契約に合わせて設定します)
PIN コード(注 1)	PIN コードを入力します。(PIN コードを設定した SIM カードをお使いの場合、設定します)
ダイヤルナンバー(注 1)	接続先ダイヤルナンバーを入力します。(ご契約に合わせて設定します)
アカウント(注 1)	認証に使用するアカウントとパスワードを入力します。
パスワード(注 1)	
認証	認証方式を選択します。(ご契約に合わせて設定します)
IP モード	動的 IP、静的 IP から選択します。(ご契約に合わせて設定します) 静的 IP を選択すると、IP アドレス、IP サブネットマスク、IP ゲートウェイの欄が表示されますので、ご契約に合わせて設定してください。
プライマリ DNS(注 1)	DNS の設定を入力します。(ご契約に合わせて設定します)
セカンダリ DNS(注 1)	
ローミング	国内使用専用機器のため、本機能はサポートしておりません。

(*1)PIN コード、ダイヤルナンバー、アカウント、パスワード、プライマリ DNS、セカンダリ DNS はご契約の回線事業者からの指定が無い場合は空欄にしてください。

8.1.5.5. 3G/4G 接続の共有設定



項目	説明
時間スケジュール	お使いの機器では本機能をご使用になれません。（常時(0)のみ）
MTU 設定	MTU を 512～1500 の範囲で指定します。
IP パススルー	有効するとブリッジモードで動作し、LAN デバイスもしくは、指定した MAC アドレスを持つデバイスに対して直接 WAN IP を割り当てます。 接続できる端末は1台のみとなります。 （注１） WAN-1 に設定されているときのみ利用可能です。 （注２） ブリッジモードであるため NAT 機能は利用できません。
NAT	NAT（NAPT）の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。
WAN IP エイリアス	お使いの機器では本機能をご使用になれません。 無効に設定してください。

◆保存ボタンをクリックして設定を登録します。必要があれば［ネットワーク監視構成］に進みます。

8.1.6. WAN タイプ：イーサーネットの接続設定

イーサネットは、ネットワークルーターの汎用的な WAN およびアップリンクインターフェイスです。この WAN インターフェイスでは、インターネットプロバイダ(ISP)が提供する、光終端装置(メディアコンバータ)、xDSL またはケーブルモデムに接続します。インターネットプロバイダ(ISP)の接続要件により接続タイプを[静的IP]、[動的IP]、[PPPoE]、[PPTP]および[L2TP]から選択する必要があります。

8.1.6.1. イーサネット WAN 設定

◆インターネット接続リストのインターフェイス行のアクション欄にある編集ボタンをクリックすると[インターネット接続構成]画面が表示されます。

項目	説明
WAN タイプ	インターネットプロバイダ(ISP)の接続方式に合わせて WAN タイプを選択します。 ◆静的 IP：インターネットプロバイダ(ISP)から指定された固定グローバル IP アドレスを使用します。 ◆動的IP：DHCP サーバーから割り当てられるグローバル IP アドレスを使用します。本機の電源 ON の度にグルーバル IP アドレスが変わる可能性があります。 ◆PPPoE：PPP over Ethernet プロトコルで接続し、グローバルIPアドレスはプロトコル上で割り当てられます。 ◆PPTP：PPTP VPN プロトコルで接続し、グローバルIPアドレスはプロトコル上で割り当てられます。 ◆L2TP:L2TP VPN プロトコルで接続し、グローバルIPアドレスはプロトコル上で割り当てられます。

◆WAN タイプを選択後、タイプ毎に必要な設定を行います。

8.1.6.2. 静的IP WAN 設定

◆WAN タイプで[静的IP]を選択すると[静的IPWAN タイプ構成]欄が表示されます。

項目	説明
WAN IP アドレス	WAN ネットワークのグローバル IP アドレスを指定します。
WAN サブネットマスク	WAN ネットワークのサブネットマスクを指定します。
WAN ゲートウェイ	WAN ネットワークのゲートウェイIPアドレスを指定します。
プライマリーDNS	WAN ネットワークのプライマリ DNS の IP アドレスを指定します。
セカンダリーDNS	WAN ネットワークのセカンダリ DNS の IP アドレスを指定します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
NAT	NAT（NAPT）の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。
WAN IP エイリアス	お使いの機器では本機能をご使用になれません。 無効に設定してください。

◆保存ボタンをクリックして設定を登録します。必要があれば[ネットワーク監視構成]に進みます。

8.1.6.3. 動的IP WAN 設定

◆WAN タイプで[動的IP]を選択すると[動的IPWAN タイプ構成]欄が表示されます。

項目	説明
ホスト名	ホスト名を指定します。特に指定のない場合は空欄にします。
ISP 登録アドレス	インターネットプロバイダに登録した MAC アドレスを指定します。 本設定により、WAN 側の MAC アドレスが設定値に変更されます。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続:常時インターネットに接続します。(推奨) ◆オンデマンド接続:インターネットアクセスの要求があるときに接続します。 ◆手動接続:必要な時に接続します。
プライマリーDNS	WAN ネットワークのプライマリ DNS の IP アドレスを指定します。
セカンダリーDNS	WAN ネットワークのセカンダリ DNS の IP アドレスを指定します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
NAT	NAT(NAPT)の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。
WAN IP エイリアス	お使いの機器では本機能をご使用になれません。 無効に設定してください。

(注 1) 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示などに時間がかかることがあります。また、手動設定を選択した場合、WebGUI の[ステータス]→[基本ネットワーク]→[WAN&アップリング]の[WAN インタフェース IPv4 ネットワークステータス]表示内の[更新]ボタンをクリックして手動接続してください。

◆[保存]ボタンをクリックして設定を登録します。必要があれば[ネットワーク監視構成]に進みます。

8.1.6.4. PPPoE WAN 設定

◆WAN タイプで[PPPoE]を選択すると[PPPoE WAN タイプ構成]欄が表示されます。

項目	説明
IP タイプ	IP タイプを選択します。(ご契約に合わせて設定します)
PPPoE アカウント	インターネットプロバイダ(ISP)から付与されたアカウント名を指定します。
PPPoE パスワード	インターネットプロバイダ(ISP)から付与されたパスワードを指定します。
プライマリーDNS	WAN ネットワークのプライマリ DNS の IP アドレスを指定します。
セカンダリーDNS	WAN ネットワークのセカンダリ DNS の IP アドレスを指定します。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続:常時インターネットに接続します。(推奨) ◆オンデマンド接続:インターネットアクセスの要求があるときに接続します。 ◆手動接続:必要な時に接続します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
NAT	NAT(NAPT)の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。
WAN IP エイリアス	お使いの機器では本機能をご使用になれません。 無効に設定してください。

(注 1) 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示などに時間がかかることがあります。また、手動設定を選択した場合、WebGUI の[ステータス]→[基本ネットワーク]→[WAN&アップリング]の[WAN インタフェース IPv4 ネットワークステータス]表示内の[更新]ボタンをクリックして手動接続してください。

◆[保存]ボタンをクリックして設定を登録します。必要があれば[ネットワーク監視構成]に進みます。

8.1.6.5. PPTP WAN 設定

◆WAN タイプで[PPTP]を選択すると[PPTP WAN タイプ構成]欄が表示されます。

項目	説明
IP モード	IP モードを静的 IPアドレスまたは動的IPアドレスから選択します。(ご契約に合わせて設定します)
WAN IP アドレス(注 2)	静的 IP アドレス選択時にインターネットプロバイダ(ISP)から付与された WAN IP アドレスを指定します。
WAN サブネットマスク(注 2)	静的 IP アドレス選択時にインターネットプロバイダ(ISP)から付与された WAN サブネットマスクを選択します。
WAN ゲートウェイ(注 2)	静的 IP アドレス選択時にインターネットプロバイダ(ISP)から付与された WAN ゲートウェイを指定します。
サーバー IP アドレス/名	PPTP サーバーの名前または IP アドレスを入力します。
PPTP アカウント	インターネットプロバイダ(ISP)から付与されたアカウント名を指定します。
PPTP パスワード	インターネットプロバイダ(ISP)から付与されたパスワードを指定します。
接続 ID	PPTP 接続を識別する ID を入力します。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続:常時インターネットに接続します。 ◆オンデマンド接続:インターネットアクセスの要求があるときに接続します。 ◆手動接続:手動で必要な時に接続します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
MPPE	[有効]にチェックをすると、PPTP 接続用の MPPE(Microsoft Point-to-Point Encryption)セキュリティが有効になります。
NAT	NAT(NAPT)の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。
WAN IP エイリアス	お使いの機器では本機能をご使用になれません。

項目	説明
	無効に設定してください。

（注１） 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのためWeb ページ表示に時間がかかることがあります。また、手動設定を選択した場合、WebGUI の[ステータス]→[基本ネットワーク]→[WAN&アップリング]の［WAN インタフェース IPv4 ネットワークステータス］表示内の[更新]ボタンをクリックして手動接続してください。
（注２） IP モードで［静的 IP アドレス］を選択した時のみ表示されます。

◆[保存]ボタンをクリックして設定を登録します。必要があれば［ネットワーク監視構成］に進みます。

8.1.6.6. L2TP WAN 設定

◆WAN タイプで［L2TP］を選択すると［L2TPWAN タイプ構成］欄が表示されます。

項目	説明
IP モード	IP モードを静的 IPアドレスまたは動的IPアドレスから選択します。（ご契約に合わせて設定します）
WAN IP アドレス(注 2)	静的 IP アドレス選択時にインターネットプロバイダ(ISP)から付与された WAN IP アドレスを指定します。
WAN サブネットマスク(注 2)	静的 IP アドレス選択時にインターネットプロバイダ(ISP)から付与された WAN サブネットマスクを選択します。
WAN ゲートウェイ(注 2)	静的 IP アドレス選択時にインターネットプロバイダ(ISP)から付与された WAN ゲートウェイを指定します。
サーバー IP アドレス/名	PPTP サーバーの名前または IP アドレスを入力します。
L2TP アカウント	インターネットプロバイダ(ISP)から付与されたアカウント名を指定します。
L2TP パスワード	インターネットプロバイダ(ISP)から付与されたパスワードを指定します。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続：常時インターネットに接続します。（推奨）

項目	説明
	◆オンデマンド接続：インターネットアクセスの要求があるときに接続します。 ◆手動接続：必要な時に接続します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
サービスポート	インターネットサービスのサービスポートを入力します。 以下のオプションが選択できます。 ◆自動：ポートが自動的に割り当てられます。 ◆ 1701（Cisco の場合）：サービスポートをポート 1701 に設定し、CISCO サーバに接続します。 ◆ ユーザ定義：サービスプロバイダが提供するサービスポートを入力します。初期値としてポート 1702 が使用されます。
MPPE	[有効]にチェックをすると、PPTP 接続用の MPPE（Microsoft Point-to-Point Encryption）セキュリティが有効になります。
NAT	NAT（NAPT）の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。
WAN IP エイリアス	お使いの機器では本機能をご使用になれません。 無効に設定してください。

（注１） 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示に時間がかかることがあります。また、手動設定を選択した場合、WebGUI の ステータス → 基本ネットワーク → WAN&アップリング の［WAN インタフェース IPv4 ネットワークステータス］表示内の 更新 ボタンをクリックして手動接続してください。
（注２） IP モードで［静的 IP アドレス］を選択した時のみ表示されます。

◆ 保存 ボタンをクリックして設定を登録します。必要があれば［ネットワーク監視構成］に進みます。

8.1.7. WAN タイプ：WiFi アップリンクの接続設定

HWL-3511-DS は、ホットスポットのようなWiFi ネットワークを通してインターネットまたはイントラネットに接続することができます。WAN の物理インターフェイスで WiFi モジュール1を選択します。

（注１） WAN タイプはアップリンクのみ有効です。

8.1.7.1. WiFi アップリンク設定

項目	説明
AP に接続	スキャンボタンをクリックすると、近隣の WiFi アップリンクのアクセスポイント(AP)を選択できます。また、プロファイルを作成することで、アップリンクネットワークへの接続を容易にすることができます。（詳細は 8.3.6 項アップリンクプロファイルを参照してください。）
ネットワークタイプ	WiFi アップリンク接続のネットワークタイプを「NAT Mode」、「Bridge Mode」または「NAT Disable」から選択します。 ◆NAT Mode：WiFi アップリンク接続で NAT 機能が有効になります。 ◆Bridge Mode：ブリッジモードで動作し、アップリンクネットワークに全ての IP 機器が参加できます。

項目	説明
	◆NAT Disable：NAT 機能が無効になります。アップリンクネットワークには一台の機器のみが参加できます。
IP モード	IP モードを静的 IPアドレスまたは動的IPアドレスから選択します。（接続する WiFi アップリンクネットワークに合わせて設定します。）
IP アドレス(注 2)	WiFi アップリンクネットワークに合わせて IP アドレスを指定します。
IPサブネットマスク(注 2)	WiFi アップリンクネットワークに合わせてIPサブネットマスクを選択します。
IPゲートウェイ(注 2)	WiFi アップリンクネットワークに合わせてIPゲートウェイを指定します。
プライマリーDNS	PPTP サーバーの名前または IP アドレスを入力します。
セカンダリーDNS	インターネットプロバイダ(ISP)から付与されたアカウント名を指定します。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続：常時インターネットに接続します。 ◆オンデマンド接続：インターネットアクセスの要求があるときに接続します。 ◆手動接続：手動で必要な時に接続します。
高速ローミング	本機ではサポートしていません。無効に設定してください。
高速ローミングチャネル	本機ではサポートしていません。

（注１） 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示に時間がかかることがあります。また、手動設定を選択した場合、WebGUI の ステータス → 基本ネットワーク → WAN&アップリング の［WAN インタフェース IPv4 ネットワークステータス］表示内の 更新 ボタンをクリックして手動接続してください。
（注２） IP モードで［静的 IP アドレス］を選択した時のみ表示されます。

◆ 保存 ボタンをクリックして設定を登録します。必要があれば［ネットワーク監視構成］に進みます。

8.1.7.2. WiFi アップリンク スキャン画面

下図はスキャンボタンのクリックで表示される画面です。接続するアップリンクアクセスポイント(AP)のセキュリティキー（事前共有キー）を入力して適用ボタンをクリックすると、アップリンク先として登録されます。SSID が公開されていないアクセスポイントに接続する場合は、SSID も入力する必要があります。

8.1.8. ネットワーク監視構成の設定

フェールオーバー機能を使用して、主ネットワークに何らかの障害が発生しても、データ通信をできるだけ継続させるために、WAN の接続状態を監視する必要があります。本機には「ICMP 確認」と「DNS 問合せ」を使用してネットワークの正常性を監視します。ネットワーク監視設定の「レイテンシーしきい値」よりも応答が遅いとき、または応答が無いときに失敗回数がカウントされ、「失敗しきい値」より大きくなると、再接続やフェールオーバー動作を実行します。

項目	説明
ネットワーク監視構成	[有効]にチェックをすると、ネットワーク監視機能が動作します。
チェック方法	ネットワークの監視(チェック)方法を選択します。 ◆DNS クリエ:DNS Query を使用して、ターゲットの DNS サーバーに問合せパケットを送信します。 ◆ICMP チェック:ICMP を使用して、ターゲットのホストに要求パケットを送信します。
読み込み確認	[有効]にチェックすると、データ伝送によりネットワークが混雑しているときに、未応答の DNS クリエまたは ICMP 要求を無視することができます。この機能により、誤ったリンクダウン判断を防止することができます。
クエリ間隔(確認間隔)	DNS クリエまたは ICMP 要求の送信間隔を指定します。値の範囲は 2～30 秒です。
レイテンシーしきい値	DNS クリエまたは ICMP 要求の応答遅延しきい値を指定します。値の範囲は 1000～3000ms です。
失敗しきい値	DNS クリエまたは ICMP 要求の失敗限界回数を指定します。値の範囲は 1～10 回です。
ターゲット 1	DNS 問合せまたは ICMP 要求を送信する最初のターゲットホストを選択します。 ◆DNS1:WAN のプライマリーDNS を使用します。 ◆DNS2:WAN のセカンダリーDNS を使用します。 ◆ゲートウェイ:WAN のゲートウェイを使用します。(ICMP 確認のみ)

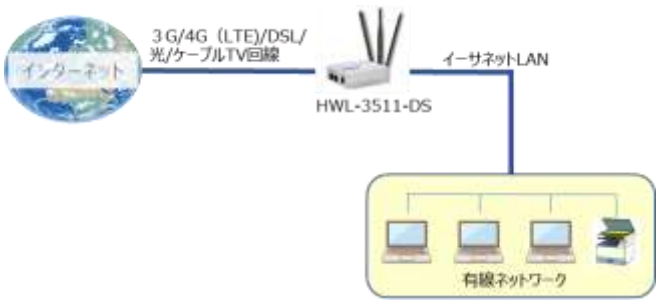
項目	説明
	◆他のホスト：ターゲットになるホストの IP アドレスを指定します。DNS クリエを使用する場合は、DNS サーバーである必要があります。
ターゲット 2	DNS 問合せまたは ICMP 確認を送信する 2 番目のターゲットホストを選択します。 ◆なし：ターゲット2を使用しません。 ◆DNS1：WAN のプライマリーDNS を使用します。 ◆DNS2:WAN のセカンダリーDNS を使用します。 ◆ゲートウェイ：WAN のゲートウェイを使用します。（ICMP 確認のみ） ◆他のホスト：ターゲットになるホストの IP アドレスを指定します。DNS クリエを使用する場合は、DNS サーバーである必要があります。

◆保存ボタンをクリックして設定を登録します。

8.2. LAN および VLAN

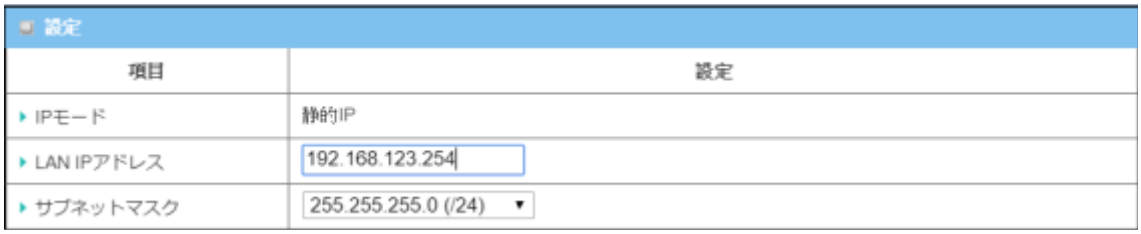
LAN(ローカルエリアネットワーク)関連の設定を行います。

8.2.1. イーサネット LAN



ローカルエリアネットワーク(LAN)を使って、ネットワークに接続されたコンピュータ間で、データまたはファイルを共有することができます。左の図は、コンピュータやプリンターをケーブルで接続するネットワークの代表例です。

◆画面左側のメニューから、基本ネットワーク⇒LAN および VLAN⇒イーサネット LAN の順にクリックします。



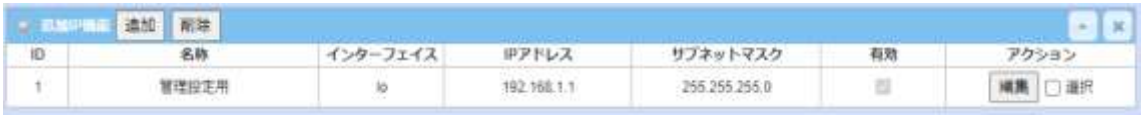
項目	説明
IP モード	本機の LAN IP モードは常に静的 IP(Static IP)です。
LAN IP アドレス	本デバイスのローカル IP アドレスを入力します。LAN ネットワークデバイスは本機のローカル IP アドレスをデフォルトゲートウェイとして使用する必要があります。
サブネットマスク	ドロップダウンリストから、このゲートウェイに対するサブネットマスクを選択します。サブネットマスクは、1 つのネットワークまたはサブネットで使用できるクライアントの数を定義します。デフォルトのサブネットマスクは 255.255.255.0 (/24)です。これは、このサブネットで最大 254 個の IP アドレスを使用できることを表します。実際には、そのうちの 1 つはこのゲートウェイの LAN IP アドレスとして使用されるため、LAN ネットワークで使用できるクライアント数は最大で 253 台です。 値の範囲: 255.0.0.0 (/8)～255.255.255.252 (/30)。

◆保存ボタンをクリックして設定を登録します。

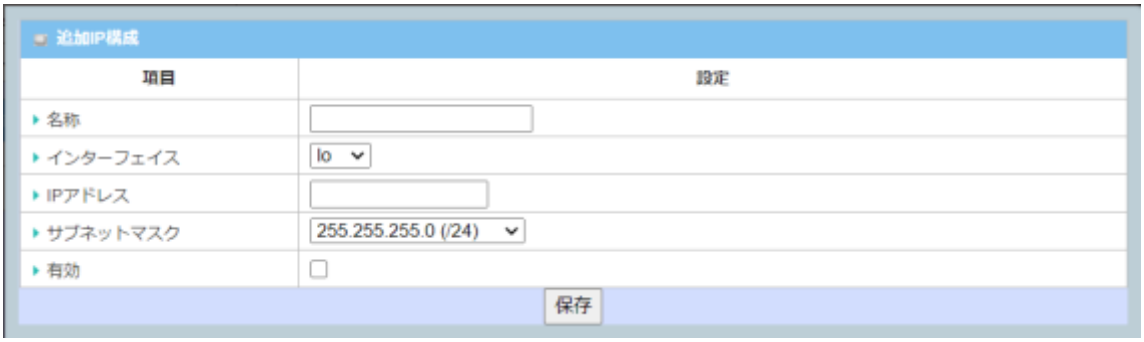
(注 1) この IP アドレスは Web UI アクセスにも使用しています。変更した場合、Web UI を表示するにはブラウザーに新しい IP アドレスを入力する必要があります。

8. 2. 2. 追加 IP（LAN IP エイリアス）機能

HWL-3511-DS は、特別な管理のために LAN IP エイリアス機能を搭載しています。本ゲートウェイに追加 LAN IP を追加し、その追加 IP を使って、HWL-3511-DS にアクセスすることができます。



◆追加ボタンをクリックすると[IP 追加構成]画面が表示されます。



項目	説明
名称	追加 IP アドレスの名称を入力します。（任意）
インターフェイス	インターフェイスタイプを指定します。 lo（Local Loopback）または br0（Bridge0）になります。
IP アドレス	追加 IP アドレスを入力します。
サブネットマスク	ドロップダウンリストから、追加 IP アドレスのサブネットマスクを選択します。
有効	追加 IP アドレスを有効にする場合に☑します。

◆保存ボタンをクリックして設定を登録します。

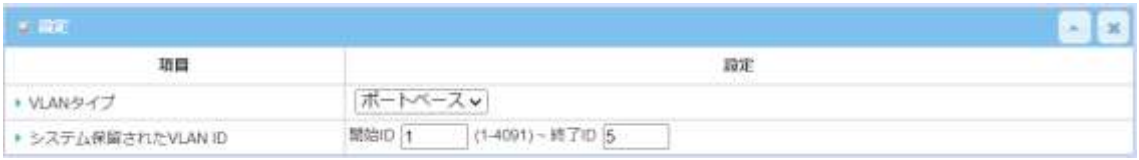
8. 2. 3. 仮想 LAN(VLAN)

仮想 LAN（VLAN）により、特定のスイッチまたはルーターデバイス下の論理ネットワークで、クライアントホストを特定の VLAN ID によりグループ化することができます。HWL-3511-DS では、ポートベースとタグベースの VLAN 両方を使用できます。

8. 2. 4. 仮想 LAN(VLAN)の設定

ポートベースの VLAN を使用することで、LAN ポート及び WiFi の仮想 AP(VAP-1/VAP-2)のグルーピングなどがポート単位で設定できます。

◆画面左側のメニューから、基本ネットワーク⇒LAN および VLAN⇒仮想 LAN の順にクリックします。



項目	説明
VLAN タイプ	VLAN タイプを選択します。 ポートベース：各 LAN ポート/Wi-Fi 仮想 AP に VLAN ID を指定します。 タグベース：選択すると[タッグベース VLAN リスト]テーブル画面に切り替わります。VLAN ID を追加し、この VLAN ID のメンバーと DHCP サーバーを指定します。
システム保留された VLAN ID	ネットワークで予約された VLANID 範囲を指定します。VLAN グルーピングのためには、この範囲外の ID を指定します。 値の範囲：1~4091

◆ポートベースまたはタグベース VLAN リストにルールを追加し、適用ボタンをクリックして設定を有効にします。

8.2.4.1. ポートベース VLAN ルールの設定

◆ポートベース VLAN リストにある追加ボタンをクリックしルールを入力します。

項目	説明
名称	このルールの名称を表示します。初期名称が定義され、変更することはできません。
VLAN !D	VLAN ID 番号を定義します。範囲は 1～4094 です。
VLAN タギング	[有効]を選択すると、ルールは[VLAN ID]および[ポートメンバー]の構成に従ってアクティブになります。 [無効]を選択すると、ルールは[ポートメンバー]の構成に従ってアクティブになります。
NAT/ブリッジ	ルールの[NAT]モードまたは[ブリッジ]モードを選択します。
ポートメンバー	ルールに追加する LAN ポートと VAP を選択します。 本機では VAP3~VAP8 は利用できません。
LAN to Join	[有効]をチェックしこの VLAN グループで使用する DHCP サーバーを選択します。[有効]を選択すると、これ以降の項目は入力できなくなります。
WAN＆WAN VID 結合	インターネットへのアクセスを許可する[WAN-1]、[WAN-2]または[すべての WAN]を選択します。 （注１） [Bridge(ブリッジ)]モードが選択されている場合は、WAN を選択して、VID を入力する必要があります。
LAN IP アドレス	このルールが使用する DHCP サーバーの[IP アドレス]を割り当てます。この IP アドレスは、本機の IP アドレスです。
サブネットマスク	DHCP サーバーの[サブネットマスク]を選択します。

項目	説明
DHCP サーバー/リレー	[DHCPサーバー]のタイプを定義します。 選択できるタイプは 3 つあります:[サーバー]、[リレー]、および[無効]です。 ・サーバー:VLAN グループに対して、DHCP サーバー機能を有効にします。DHCP サーバーで使用されるパラメータを指定する必要があります。 ・リレー:VLAN グループの DHCP リレー機能を有効にするには、[リレー]を選択し、リレーする DHCP サーバーのアドレスを[DHCP サーバーIP アドレス]フィールドに入力します。 ・無効:VLAN グループの DHCP サーバーが無効になります。
有効	有効ボックスにチェックをして、本ルールを有効します。

◆DHCP サーバー/リレーで[サーバー]を選択した場合は以下の項目を入力します。(選択的)と書かれた項目は DHCP で通知する内容を入力してください。

項目	説明
DHCP サーバー名	指定した VLAN グループの DHCP サーバーの名前を指定します。
IP プール	IP プールの範囲を定義します。 [開始アドレス]と[終了アドレス]フィールドがあります。クライアントが、この DHCP サーバーに IP アドレスを要求すると、IP プールの範囲内に IP アドレスが割り当てられます。
リース時間	DHCP サーバーが新しいデバイスにリースする IP アドレスの期間を指定します。
ドメイン名	DHCP サーバーのドメイン名を指定します。 値の範囲: 0～31 文字。
プライマリーDNS	DHCP サーバーが通知するプライマリーDNS IP アドレスです。
セカンダリーDNS	DHCP サーバーが通知するセカンダリーDNS IP アドレスです。
プライマリーWINS	DHCP サーバーが通知するプライマリーWINS IP アドレスです。
セカンダリーWINS	DHCP サーバーが通知するセカンダリーWINS IP アドレスです。

項目	説明
ゲートウェイ	DHCP サーバーが通知するゲートウェイ IP アドレスです。

3) DHCP サーバー/リレーで[リレー]を選択した場合は以下の項目を入力します。

項目	説明
DHCP サーバー IP アドレス	DHCP 要求をリレーする DHCP サーバーの IP アドレスを指定します。 DHCP サーバータイプを[リレー]にすると表示されます。
DHCP OPTION 82	リレーエージェント情報オプション（Option82）を有効にします。

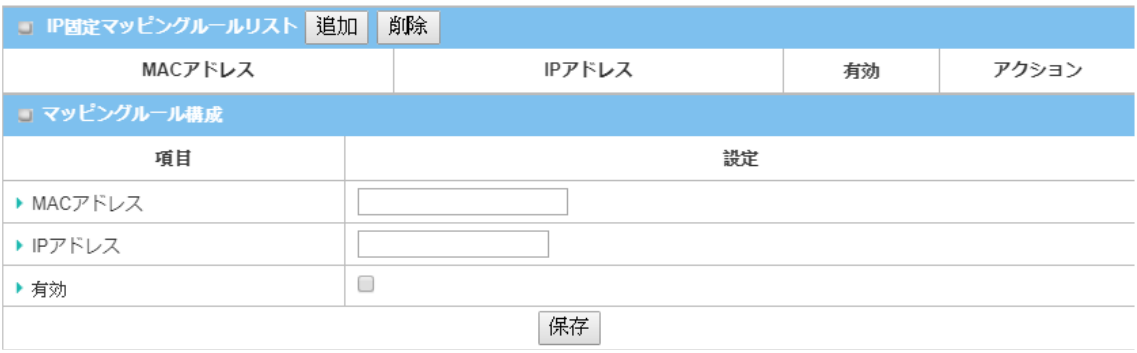
◆有効項目のチェックボックスをチェックし本ルールを有効にします。

◆保存ボタンをクリックしルールを登録します。登録されると〔ポートベース VLAN ルール〕にルールの内容が表示されます。

8.2.4.2. IP 固定マッピングルールの設定

MAC アドレスにより固定 IP アドレスを割り当てることができます。

◆IP 固定マッピングルールリストにある追加ボタンをクリックしルールを入力します



項目	説明
MAC アドレス	対象の機器の MAC アドレスを指定します。
IP アドレス	割り当てる IP アドレスを DHCP サーバーのサブネット内で指定します。
有効	ルールを有効にする場合に☑します。

◆保存ボタンをクリックしルールを登録します。登録されると IP 固定マッピングルールリストにルールの内容が表示されます。

8.2.4.3. ポートベース VLAN 間グループルーティング

◆VLAN 間グループルーティングボタンをクリックすると、[VLAN グループインターネットアクセス定義]画面と[VLAN 間グループルーティング]画面が表示されます。

◆各項目の編集ボタンをクリックしグループルーティング設定内容を編集します。

項目	説明
VLAN グループのインターネットアクセス定義	初期状態では、すべてのボックスがチェックされ、すべての VLAN ID メンバーが WAN インターフェイスにアクセスできることを示します。 特定の VLAN ID ボックスのチェックを外すと、VLAN ID メンバーがインターネットにアクセスできなくなります。 （注２） VLAN ID 1 は、常に使用できます。 LAN ルールのデフォルトの VLAN ID です。その他の VLAN ID は、有効になっている場合にのみ使用できます。
VLAN 間グループルーティング	使用する VLAN ID ボックスをクリックして、VLAN 間アクセス機能を有効にします。初期状態では、異なる VLAN ID のメンバーは互いにアクセスできません。ゲートウェイは、[VLAN 間グループルーティング]に対して、最大 4 つのルールをサポートします。例えば、ID_1 と ID_2 にチェックを入れると、VLAN ID_1 のメンバーは、VLAN ID_2 のメンバーにアクセスでき、その逆も可能です。

◆保存ボタンをクリックしルールを登録します。

8.2.4.4. タッグベース VLAN ルールの設定

タッグベースの VLAN を使用することで、LAN ポート及び WiFi の仮想 AP(VAP-1/VAP-2)のグルーピングなどが VLAN ID 単位で設定できます。

すべての LAN ポートおよび仮想 AP の構成を表示するデフォルトルールがあります。HWL-3511-DS は、最大 128 つのトラップイベントレシーバセットをサポートします。

◆仮想 LAN の設定画面にある[VLAN タイプ]をタッグベースに選択します。そうすると、タッグベース VLAN リストが表示されます。追加ボタンをクリックしてルールを追加します。

◆表示される[タグベースの VLAN 構成]にルールを設定します。

項目	説明
VLAN ID	VLAN ID 番号を指定します。範囲は 6～4094 です。
インタネットアクセス	[有効]ボックスをチェックすると、VLAN グループのメンバーがインターネットにアクセスできるようになります。
ポートメンバー	各ポートボックスにチェックを入れると、VLAN グループに参加することができます。本機では VAP3~VAP8 は利用できません。
ブリッジ インターフェース	事前に登録された DHCP サーバーを選択します。(DHCP サーバーの登録については 8.2.4 項を参照してください。) NEW を選択すると、VLAN グループのメンバーに対して新しい DHCP サーバーを作成し必要な項目の入力ができます。

◆保存ボタンをクリックしルールを登録します。登録されるとグベース VLAN リストにルールの内容が表示されます。

8. 2. 5. DHCP サーバー

HWL-3511-DS は DHCP サーバー機能を搭載しています。また、VLAN グループからの DHCP 要求に応答するために最大 4 つの DHCP サーバーを構築できます（詳細は 8.2.3 項仮想 LAN を参照してください）。また、工場出荷設定として本機の IP サブネットと同一であり、IP プール範囲が、「.100」から「.200」のゲートウェイの WEB UI の DHCP サーバーリストページに示されているよう、「.100」から「.200」）があらかじめ DHCP サーバーリストに登録されています。

8.2.5.1. DHCP サーバーリスト

◆画面左側のメニューから、基本ネットワーク⇒LAN および VLAN⇒DHCP サーバーの順にクリックします。

◆DHCP サーバーリストに DHCP ルールを追加/編集/登録することで、LAN ポートおよび WiFi に接続された PC/スマートフォンなど IP 機器に IP アドレス、サブネットマスクの割当とディフォルトゲートウェイや DNS サーバーアドレスの通知を行うとこができます。

8.2.5.2. DHCP サーバーの設定

◆DHCP サーバーリストにある追加または編集ボタンをクリックすると、DHCP サーバー構成画面が表示されます。

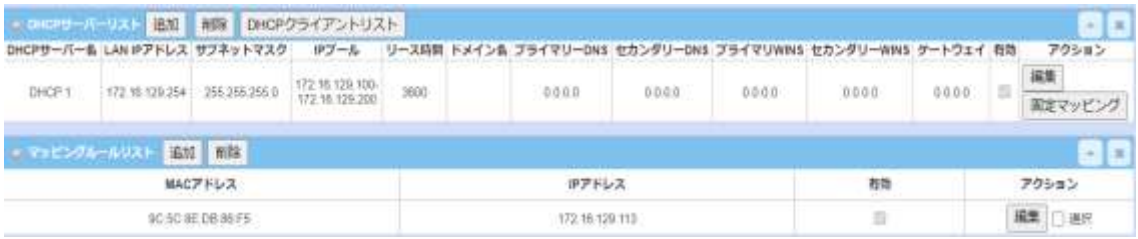
項目	説明
DHCP サーバー名	DHCPサーバー名を64文字以内で指定します。
LAN IP アドレス	DHCPサーバーのIPアドレスを指定します。
サブネットマスク	DHCPサーバーのサブネットマスクを指定します。
IP プール	DHCPサーバーが配布するIPアドレス範囲を指定します。 開始アドレスは終了アドレスよりも小さい値で設定します。
リース時間	DHCPサーバーのリース時間です。値の範囲は300～604800秒です。
ドメイン名	DHCPサーバーが通知するドメイン名です。
プライマリーDNS	DHCPサーバーが通知するプライマリーDNS名です。何も指定しないと本機のIPアドレスが通知されます。
セカンダリーDNS	DHCPサーバーが通知するセカンダリーDNSです。何も指定しないと本機のIPアドレスが通知されます。
プライマリ WINS	DHCPサーバーが通知するプライマリWINSです。何も指定しないと本機のIPアドレスが通知されます。
セカンダリーWINS	DHCPサーバーが通知するセカンダリーWINSです。何も指定しないと本機のIPアドレスが通知されます。
ゲートウェイ	DHCPサーバーが通知するデフォルトゲートウェイを指定します。何も指定しないと本機のIPアドレスが通知されます。
サーバー	有効ボックスをチェックするとDHCPサーバーが有効になります。

◆保存ボタンをクリックして設定を登録します。登録した内容が DHCP サーバーリストに表示されます。

8.2.5.3. IP 固定マッピングルールの設定

MAC アドレスにより固定 IP アドレスを割り当てることができます。

◆DHCP サーバーリストの各サーバー欄の右端にある固定マッピングボタンをクリックするとマッピングルールリストが表示されます。マッピングルールリスト上の追加ボタンをクリックし設定入力画面を表示させます。



保存ボタンをクリックしルールを登録します。登録した内容がマッピングルールリストに追加されます。

項目	説明
MAC アドレス	対象の機器の MAC アドレスを指定します。
IP アドレス	割り当てる IP アドレスを DHCP サーバーのサブネット内で指定します。
有効	ルールを有効にする場合に☑します。

8.2.5.4. DHCP クライアントリストの表示/マッピングルールへのコピー

DHCP サーバーが IP アドレスを割り当てた IP 機器の情報を表示します。また、リストにある IP 機器をマッピングリストにコピーすることができます。

◆DHCP サーバーリストにある DHCP クライアントリストボタンをクリックすると、DHCP クライアントリストが表示されます。

◆マッピングルールにコピーする場合は、登録する IP 機器のアクション欄にあるチェックボックスをチェックし、固定マッピングにコピーボタンをクリックすると、マッピングリストに登録されます。

8.2.5.5. DHCP サーバーオプションの有効/無効

DHCP サーバーオプション設定により、DHCP オプション 66、72 または 114 を設定することができます。DHCP サーバーは、DHCP パケット（DHCPOFFER DHCPACK）の送信において、適応するオプションを追加します。

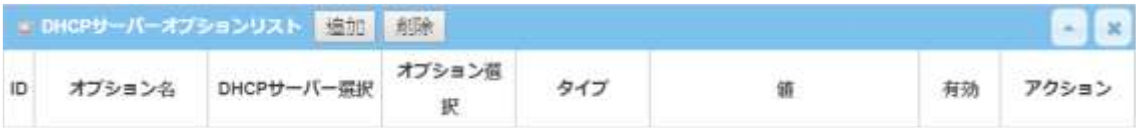
項目	説明
DHCP サーバーオプション	有効にする場合に☑します。

DHCP オプション番号

オプション番号	説明
42	NTP サーバー名[RFC 2132]
66	TFTP サーバー名[RFC 2132]
72	WWW サーバーIP アドレス[RFC 2132]
114	URL[RFC 3679]
150	TFTP サーバーのアドレス、イーサブート、GRUB 設定[RFC 5859]
160	URL[RFC 7710]

8.2.5.6. DHCP サーバーオプションリストの追加/編集

HWL-3511-DS は、最大 99 の DHCP サーバーオプション設定を登録できます。



◆DHCP サーバーオプションリストにある追加ボタンをクリックすると、DHCP サーバーオプションの構成画面が表示されます。

項目	説明
オプション名	DHCP サーバーオプション名を入力します。任意名称を入力します。
DHCP サーバー選択	このオプションが適用される DHCP サーバーを選択します。
オプション選択	ドロップダウンリストから適用するオプションを選択します。 選択できるオプション番号は、42/66/72/114/150/160 です。
タイプ	タイプは選択したオプション番号で異なります。 オプション番号 42:「,」により区切られた IP アドレスリスト オプション番号 66:単一 IP アドレス/単一完全ドメイン名(FQDN) オプション番号 72:「,」により区切られた IP アドレスリスト オプション番号 114:単一 URL オプション番号 150:「,」により区切られた IP アドレスリスト オプション番号 160:単一 IP アドレス/単一完全ドメイン名(FQDN)
値	以下のフォーマットで入力します。 IP アドレス:IPv4 形式 IP アドレスリスト:「,」により区切られた IPv4 形式 単一 URL:URL 形式 単一 FQDN:FQDN 形式
有効	ルールを有効にする場合に☑します。

◆保存ボタンをクリックしルールを登録します。登録した内容が DHCP サーバーオプションリストに追加されます。

8.2.5.7. DHCP リレー構成リストの追加/編集

HWL-3511-DS は、最大6の DHCP リレー構成を登録できます。

◆ DHCP リレー構成リストにある追加ボタンをクリックすると、DHCP リレー設定画面が表示されますので、各項目を入力しルールを作成します。

項目	説明
代理名	DHCP サーバーオプション名を入力します。任意名称を入力します。
LAN インターフェース	このオプションが適用される DHCP サーバーを選択します。
WAN インタフェース	ドロップダウンリストから適用するオプションを選択します。 選択できるオプション番号は、42/66/72/114/150/160 です。
サーバーIP	タイプは選択したオプション番号で異なります。 オプション番号 42:「,」により区切られた IP アドレスリスト オプション番号 66:単一 IP アドレス/単一完全ドメイン名（FQDN） オプション番号 72:「,」により区切られた IP アドレスリスト オプション番号 114:単一 URL オプション番号 150:「,」により区切られた IP アドレスリスト オプション番号 160:単一 IP アドレス/単一完全ドメイン名（FQDN）
DHCP オプション 82	以下のフォーマットで入力します。 IP アドレス:IPv4 形式 IP アドレスリスト:「,」により区切られた IPv4 形式 単一 URL:URL 形式 単一 FQDN:FQDN 形式
有効	ルールを有効にする場合に☑します。

◆保存ボタンをクリックしルールを登録します。登録した内容が DHCP リレー構成リストに追加されます。

8.3. WiFi

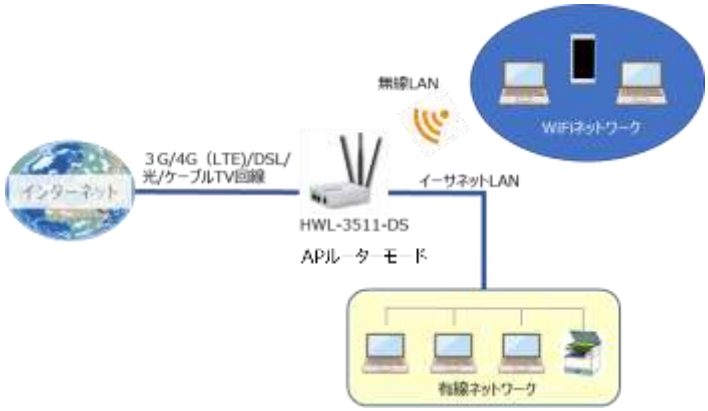
HWL-3511-DS は、WiFi に対応した PC、スマートフォン、タブレット端末やネットワークカメラをインターネット/イントラネットに接続できる WiFi インターフェイスを搭載しています。本機に搭載する WiFi システムは、2.4GHz シングルバンドの IEEE 802.11n/11g/11b 規格に準拠しています。また、「AP ルーターモード」、「WDS 専用モード」、および「WDS ハイブリッドモード」の 3 種類の動作モードを選択することにより、様々な WiFi ネットワーキングに対応できます。

（注１） WAN の物理インタフェーイスで WiFi モジュール1を選択した場合は、WiFi アップリンク（子機）動作モードとなり、WiFi の親機としての機能はお使いになれません。

8.3.1. WiFi 動作モードの説明

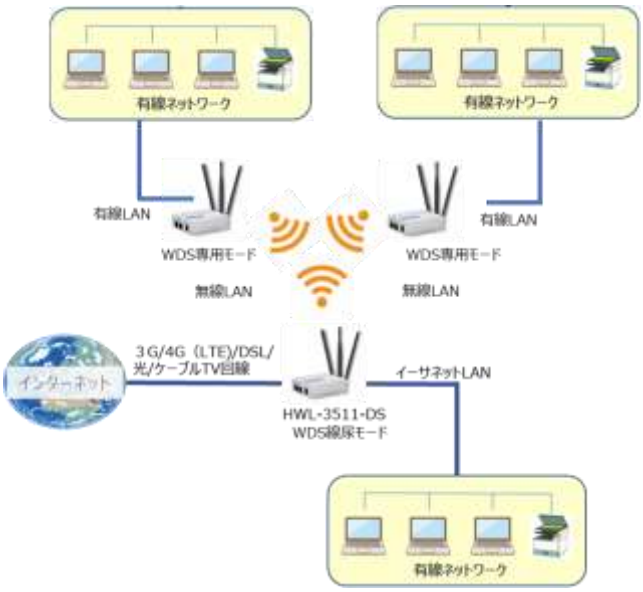
8.3.1.1. AP ルーターモード

有線デバイスおよびワイヤレスデバイスを接続してイントラネットを形成し、イントラネットは HWL-3511-DS の NAT メカニズムを使用してインターネットに接続します。このモードで本機は WiFi AP として機能するとともに WiFi インターネットアクセスを可能にします。アドレス変換（NAT）機能を有効にしておくと、無線 LAN 機器すべてがインターネットにアクセスできるようになります。

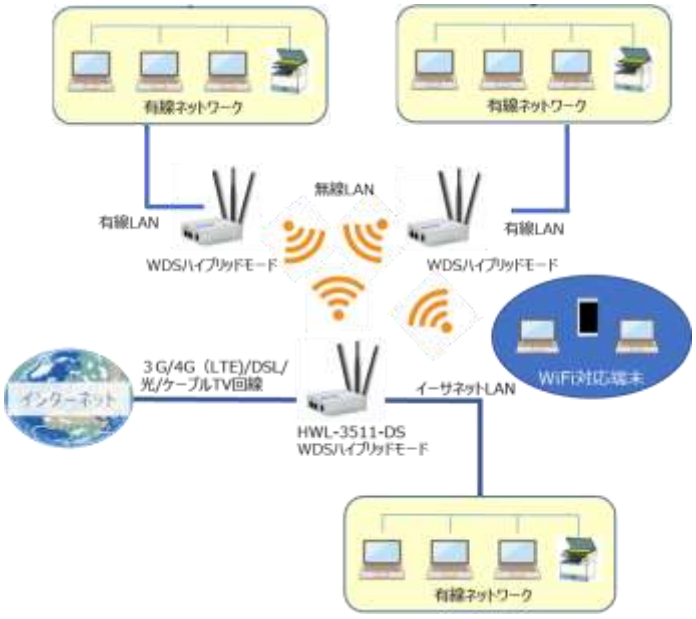


8.3.1.2. WDS 専用モード

WDS（Wireless Distributed System）専用モードでは、複数のゲートウェイ機器（HWL-3511-DS のような）が WiFi ネットワークで相互通信を行い、有線ネットワークの拡張を行うことが可能となります。WDS 専用モードで構築された WiFi ネットワークには、WiFi ステーション（WiFi 対応 PC/スマートフォン/タブレット/ネットワークカメラなど）を直接接続することができません。



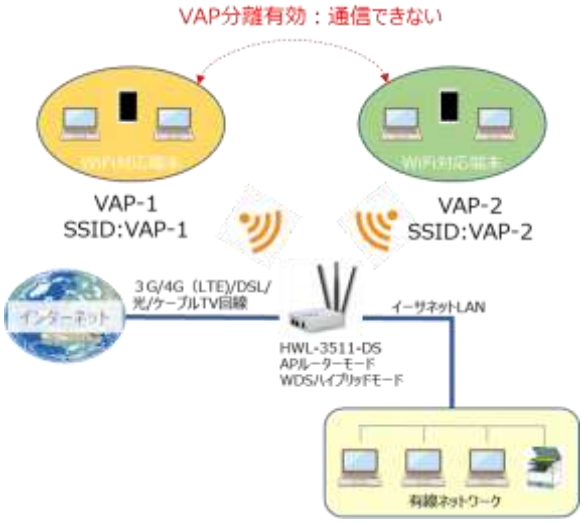
8.3.1.3. WDS ハイブリッドモード



WDS ハイブリッドモードではアクセスポイント間通信だけでなく WiFI 端末も同時に WiFi ネットワークに接続することが可能となります。それぞれのゲートウェイ機器（HWL-3511-DS のような）が同一 SSID を持つこともできれば、異なる SSID を持つこともできます。この機能により、WiFI ネットワークそのものを拡張することがかのうであり、商業施設などで展開するホットスポットなどに活用できます。

（注１） WDS ハイブリッドモードでは実質の通信速度が低下することがあります。

8.3.1.4. マルチ仮想 AP（Multiple Virtual Access Point）



仮想 AP（VAP: Virtual Access Point）は、ワイヤレスネットワークを複数のドメインに分割する機能です。1 つの物理 AP に 2 つの AP が動作しているようにネットワークを構築できます。各 VAP に対して、Wi-Fi クライアントアクセスを制御するために SSID、認証、暗号化を設定する必要があります。
また、VAP 間のアクセスを制限する VAP 分離オプションがあります。図に示すように、VAP-1 と VAP-2 のクライアントは、VAP 分離が無効になっているときのみ互いに通信できます。

8.3.1.5. WiFi セキュリティ – 認証および暗号化

HWL-3511-DS の WiFi 機能は、認証と暗号化メカニズムをサポートしていますので、データを無線でワイヤレスに転送するときに暗号化を実施してセキュリティを強化します。本機は、共有、WPA-PSK/WPA2-PSK および WPA/WPA2 認証をサポートします。ワイヤレス機器を検証するために、VAP 毎に 1 つの認証方式を選択できます。また、WEP、TKIP、および AES の暗号化アルゴリズムによりワイヤレス接続が確立されている間のデータセキュリティを確保します。

8.3.2. WiFi 構成の設定

WiFi 構成では、2.4GHz WiFi の各種パラメータを設定することができ、様々な WiFi ネットワーク構成を構築できます。

◆画面左側のメニューから、基本ネットワーク⇒WiFi⇒WiFi モジュール1の順にクリックします。

項目	説明
動作帯域	本機は、2.4GHz のみサポートしています。動作帯域の選択はできません。

◆[2.4GWiFi 構成]および[VAP リストの追加/編集]を終了したあと、保存ボタンで登録します。

◆新設定項目を動作に反映するために適用ボタンをクリックしてください。

8.3.2.1. 2.4GWiFi 構成の設定

各動作モード共通の WiFi ネットワーク構成を設定します。

項目	説明
WiFi モジュール	[有効]ボックスをチェックし、WiFi 機能を有効します。
チャネル	VAP の無線チャネルを選択します。各チャネルは異なる無線帯域に対応しています。CH1~CH13 の固定チャネルを選択することができます。 [自動]を選択すると、2 つのオプションが使用できます: ・AP 番号による AP 番号に応じてチャネルが選択されます(小さいほど良くなります)。 ・干渉の少なさによる 干渉に応じてチャネルが選択されます。(低いほど良くなります)。
WiFi システム	優先 WiFi システムを指定します。[WiFi システム]のドロップダウンリストは、IEEE 802.11 規格に基づいています。 2.4G WiFi は、b(11Mbps max)、g(54Mbps max)、n(150Mbps max)各規格のみを選択するか、各規格のミックスモードを選択できます。選択した規格に対応する無線子機の接続を受け付けます。

項目	説明
WiFi 動作モード	用途に応じて、[WiFi 動作モード]を指定します。 [AP ルーターモード]、[WDS 専用モード]、および、[WDS ハイブリッドモード]の動作については、8.1.3WiFi動作モードの説明を参照してください。
VAP 分離(注1)	有効にチェックをいれると、VAP-1 と VAP-2 のそれぞれ接続している WiFi 端末同士の通信を遮断します。(注1)
時間スケジュール(注1)	時間による動作制限を行う場合は、予め設定した時間スケジュールを選択します。それ以外は(0)常時を選択します。

(注1) [WDS 専用モード]を選択すると本設定項目は表示されません。

8.3.2.2. 2.4GWiFi 構成の設定(WDS 専用モードのみ)

項目	説明
リモート AP の MAC リストをスキャンする	スキャンボタンをクリックすると、近隣のアクセスポイントの情報が表示されます。その表示から WDS 接続するアクセスポイントの行の選択項目にあるエリア番号(1~4)を選択し Copy to ボタンをクリックすると、リモート AP MAC1~4 に MAC アドレスが登録されます。
リモート AP MAC 1～4	リモート AP の MAC アドレスを手動で入力するか、自動スキャン方式で入力します。正常に関連付けられると、本機はリモート AP にデータをブリッジします。

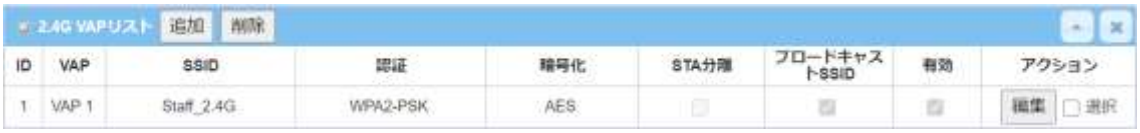
〇WirelessAP リスト表示例

8.3.2.3. 2.4GWiFi 構成の設定（WDS ハイブリッドモードのみ）

項目	説明
レイジーモード	[有効]をチェックすると、他のAPのMACアドレスを手動で入力せずに、WDSピアを自動学習できます。しかし、少なくとも1つのAPは、リモートAP MACアドレスを満たさなければなりません。 レイジーモードを無効にするとMACアドレス入力項目が表示されます。（詳細は2.4GWiFi構成の設定（WDS専用モードのみ参照）

8. 3. 3. 仮想 AP(VAP)構成の追加/編集

仮想AP(VAP)の SSID や暗号化のための設定を行います。HWL-3511-DS では仮想 AP を 2 個まで構成することができ、WiFi 機器の接続制限などのWiFiネットワークの構築ができます。



◆［VAP リスト］画面の追加/編集ボタンをクリックして、VAP の設定を作成または編集します。
［2.4G VAP Configuration］画面が表示されます。

（注１） WDS 専用モードでは使用できる仮想 AP(VAP)は 1 つとなります。

項目	説明
VAP	プルダウンリストから設定する仮想 AP(VAP)を選択します。
SSID	VAP の SSID を入力します。SSID は別の AP からの識別に使用され、クライアントステーションは、SSID に従って AP に関連付けられます。
最大 STA(注 1)	このボックスにチェックを入れ、クライアントステーションの制限する最大数（0-80）を入力します。初期状態では、STA最大数制限は無効になります。この時は最大数は80台です。
認証	セキュリティのための認証方法を選択することができます。本機にWiFi接続する場合は、クライアントステーションはキーを提供する必要があります。 ● オープン ［802.1x］をチェックして有効にすると、接続する WiFi 機器は外部のRADIUSサーバーにより認証されます。有効時にはRADIUSサーバーに関連する設定項目が表示されます。 ＊RADIUS サーバーIP：RADIUS サーバーの IP アドレスを指定します。 ＊RADIUS サーバーポート：RADIUS 認証で使用されるポート番号を指定します。（初期値 1812） ＊RADIUS 共有キー：RADIUS 認証で使用される共有キーを指定します。 ● 共有 WEP モードになります。認証に使用する共有 WEP キーを指定します。 ● 自動 自動的にクライアントの要求によって、［オープン］または［共有］を選択します。802.1x 有効時の RADIUS 設定は［オープン］と同様です。 ● WPA2-PSK、WPA-PSK / WPA2-PSK WPA または WPA2 と同じ暗号化システムを使用します。認証では、RADIUS サーバーの代わりに事前共有キー(PSK)が使用されます。事前共有キーは 8~40 文字の ASCII 文字を使用できます。 ● WPA2、WPA / WPA2 WPA またはWPA2 の認証方式を使用して、接続するWiFi 機器はRADIUSサーバーとの連携で認証されます。RADIUS 設定は［オープン］と同様です。
暗号化	暗号化方式を選択します。 ● なし WiFi ネットワークは暗号化されないオープンシステムとなります。 ● WEP 最大 4 つの WEP キーを設定することができ、その中から使用する 1 つを選択しなければなりません。HEX は 16 進数のキーとなり 5 桁の 16 進数(10 文字)を指定します。ASCII は ASCII 文字（アルファベットおよび数字、記号）

項目	説明
	13 文字を指定します。 ● AES Wi-Fi で最も使用される暗号化システムです。高速 802.11n 高速データ通信に適しています。8～63 文字の事前共有キーを指定します。 安全性向上のために AES 暗号化システムを使用することを推奨します。 ● TKIP/AES 接続する WiFi 機器に応じて TKIP または AES の暗号化を使用します。8～63 文字の事前共有キーを指定します。
STA 分離	[有効]ボックスをチェックすると、VAPに接続しているWiFi機器が相互で通信できなくなります。
ブロードキャスト SSID	[有効]ボックスをチェックすると、SSIDを公開しWiFi機器のスキャンで発見できるようになります。無効にするとSSIDが公開されなくなります。
有効	仮想AP(VAP)を有効にする場合に☑します。

（注１） HWL-3511-DS は最大接続数制限を 80 台までに設定できますが、安定動作のために接続台数を VAP-1/VAP-2 含めて 16 台以下にすることを推奨します。

◆保存ボタンをクリックして、VAP の設定をリストに登録します。

8.3.4. ワイヤレスクライアントリスト

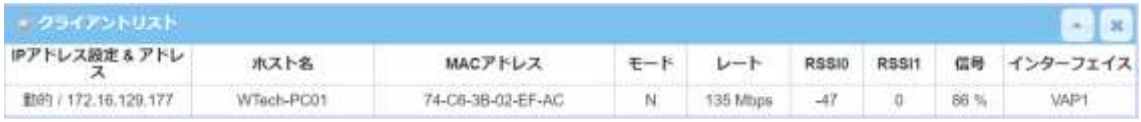
ワイヤレククライアントリストにより、本機WiFiネットワークに接続しているWiFi機器の情報を表示することができます。

◆画面左側のメニューから、基本ネットワーク⇒WiFi⇒ワイヤレスクライアントリストの順にクリックします。

項目	説明
動作帯域	本機は、2.4GHzのみサポートしています。動作帯域の選択はできません。
複数 VAP 名	クライアントリストに表示するVAPを指定します。全部を選択するとVAP-1/VAP-2両方のWiFi接続機器の情報を表示します。

8.3.4.1. クライアントリストの表示

クライアントリストには、選択した VAP に接続している WiFi 機器の情報が表示されます。



項目	説明
IP アドレス設定&アドレス	クライアントのIPアドレスとIPアドレス取得方法を表示します。 静的:IPアドレスが固定設定されています。 動的:IPアドレスがDHCPサーバーから取得しています。
ホスト名	WiFi機器のホスト名(Windows® PCだとPC名)が表示されます。
MAC アドレス	WiFi機器のMACアドレスが表示されます。
モード	通信しているWiFiモードを表示します。 B:IEEE802.11b、H:IEEE802.11h、N:IEEE802.11n
レート(注1)	WiFi機器とHWL-3511-DS間の想定物理データレートを表示します。
RSSI0、RSSI1	WiFi機器からの無線信号感度(RSSI)を表示します。本機ではRSSI1は常に0となります。
信号	WiFi機器との間の信号強度をパーセントで表示します。
インターフェイス	接続している仮想AP番号が表示されます。

(注1) 本レートは理想的な速度です。実際のレートはこれよりも低くなる場合があります。

◆更新ボタンをクリックすると最新の情報が表示されます。

8.3.5. 詳細構成

詳細パラメータを設定します。特定環境における WiFi 特性を最適化することができます。ほとんどの場合は初期値でのご使用を推奨します。また、詳細パラメータの不適切な設定により、接続性と性能が悪化することがありますので注意してください。

◆画面左側のメニューから、基本ネットワーク⇒WiFi⇒詳細構成の順にクリックします。

◆値を入力したのち、保存ボタンをクリックし、設定を保存します。

各パラメータの説明は以下の通りです。

項目	説明
動作帯域	本機は、2.4GHzのみサポートしています。動作帯域の選択はできません。
規制領域	日本国内使用限定のためCH1～13となります。設定の変更はできません。
ビーコン間隔	各仮想AP(VAP)のビーコンパケット間隔を設定します。
DTIM 間隔	DTIM（Delivery Traffic Indication Message）は、ブロードキャストメッセージを受信する次のタイミングをクライアントに知らせるカウント値です。
RTS しきい値	RTS（Request to send）しきい値は、受信パケットがオーバーフローした場合のフロー制御を実行するしきい値を設定します。小さい値を設定すると通信速度が極端に低下する可能性があります。
断片化	WiFi通信でのパケット断片化の最大サイズを指定します。小さなサイズで断片化するとノイズの多い環境で有利になります。通信環境が良い場合は、最大サイズを指定します。
WMM	WiFi接続を介してマルチメディアコンテンツを送信するときの遅延とジッタを

項目	説明
	制御する機能です。チェックボックスをチェックすると有効になります。
ショート GI	パケット間のガード時間を設定します。
TX レート	データ送信速度を指定します。[最高]を選択すると、本機は信号強度に応じて適切なデータレートを選択します。
RF 帯域幅	RF帯域幅を設定します。IEEE802.11n時に帯域幅40MHzが利用可能になります。
送信パワー	送信電力を制御します。100%,50%,25%,12%に制御が可能で小さい値を選択するとWiFiカバーエリアが狭くなります。
WIDS(注 1)	WIDS(Wireless Intrusion Detection System)はパケット分析を実行し統計データを作成します。WIDSステータスは、左側メニューから[ステータス] [基本ネットワーク] > [WiFi]をクリックし呼び出すことができます。

（注１） WIDS を有効にすると無線環境の統計情報は取得できますが、データ通信速度が低下する可能性があります。

8.3.6. アップリンクプロファイル

HWL-3511-DS は、イーサーネット WAN、3G/4GWAN と並んで、WiFi アクセスポイントを WAN として活用する WiFi アップリンク機能を搭載しています。この時 WiFi 機能は子機モードで動作し、その他は別の WAN インタフェースを選択した場合と同じゲートウェイ機能が活用できます。

（注１） HWL-3511-DS では、WiFi アップリンク機能を有効にすると、AP ルーターモードや WDS モードが利用できなくなります。

1) 画面左側のメニューから、基本ネットワーク⇒WiFi⇒アップリンクプロファイルの順にクリックします。

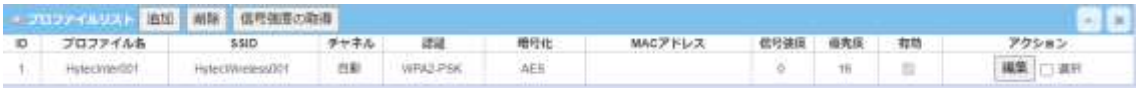
（注２） WAN&アップリンクで WiFi モジュール1が物理インターフェイスとして指定されていないと設定ができません。

8.3.6.1. アップリンクプロファイルの設定

項目	説明
プロファイル	[有効]にチェックを入れ、プロファイル機能を有効します。WiFiアップリンクモードで設定されている場合にのみ使用できます。
動作帯域	本機は、2.4GHzのみサポートしています。動作帯域の選択はできません。
優先度	ワイヤレスアップリンクネットワークに接続するための選択方法を指定します。[信号強度による]または[ユーザー定義による]の優先度を選択できます。 ・[信号強度による]:ワイヤレス信号強度が最も強いアップリンクネットワークに接続しようとします。 [ユーザー定義による]:優先度が最も高い利用可能なアップリンクネットワークに接続しようとします(1が最高優先度、16が最低優先度です)。
現在のプロフィール	プロファイルが有効で、接続が完了した後に、現在のプロファイル名が表示されます。

8.3.6.2. アップリンクプロファイルの追加/編集

[プロファイルリスト]には、作成されたアップリンクプロファイルの設定が表示されます。情報には、[プロファイル名]、[SSID]、[チャネル]、[認証]、[暗号化]、[MAC アドレス]、[信号強度]、[優先度]、[有効]が含まれます。



1) 追加ボタンをクリックすると[プロファイル構成]画面が表示されます。各々の項目を設定します。

項目	説明
プロファイル名	下に指定したアップリンクネットワークの判りやすいプロファイル名を入力します。入力文字数は64文字までです。
ネットワーク ID（SSID）	接続するWiFiアクセスポイントのSSIDを指定します。
チャネル	接続するWiFiアクセスポイントが使用する固定チャネルを指定します。固定チャネルを指定しない場合は[自動]を選択します。
認証	接続するWiFiアクセスポイントが使用する認証方法を選択します。[オープン]、[共有]、[WPA-PSK]または[WPA-PSK2]から選択します。 共有の場合はWEPキーを、WPA-PSKおよびWPA2-PSKの場合は[暗号化]を選択しと[プリシェアーキー]を指定する必要があります。
暗号化	接続するWiFiアクセスポイントが使用する暗号化方式を[なし]、[WEP]、[TKIP]または[AES]から選択します。
WEP キー	暗号化でWEPを選択すると表示されます。接続するWiFiアクセスポイントが使用するWEPキーを指定します。最大4つのWEPキーを設定することができ、その中から使用する1つを選択しなければなりません。HEXは16進数のキーとなり5桁の16進数(10文字)を指定します。ASCIIはASCII文字（アルファ

項目	説明
	ベットおよび数字、記号）13文字を指定します。
プリシェアキー	認証で[WPA-PSK]または[WPA2-PSK]を選択すると表示されます。8～63文字のプリシェアキー（事前共有鍵）を指定します。
MAC アドレス	接続先のWiFiアクセスポイントのMACアドレスを指定します。
優先度	本機では使用できません。
有効	本プロファイルを有効にする場合に☑します。

2) 保存ボタンをクリックして、アップリンクプロファイル設定をプロファイルリストに登録します。

8.3.6.3. アップリンクプロファイルの追加/編集（スキャン）

アップリンクネットワークの情報を手動で入力する代わりに、スキャンボタンをクリックして本機周辺で使用可能なワイヤレスネットワークパラメータを取得し、アップリンクネットワークとして選択することもできます。

Wireless APリスト

SSID	チャネル	Quality	認証	暗号化	MACアドレス	選択
Staff_2.4G	40	63%	WPA2-PSK	AES	00:50:18:77:22:67	
Staff_2.4G	40	65%	WPA2-PSK	AES	02:50:18:71:22:67	
HY-WIFI01	44	29%		なし	00:50:18:11:11:01	
HY-WIFI02	44	29%	WPA2-PSK	AES	02:50:18:16:11:01	
	44	47%	WPA2-PSK	AES	00:50:18:21:eb:08	
Staff_2.4G	48	26%	WPA2-PSK	AES	00:50:18:21:23:09	
Staff_2.4G	153	100%		WEP	00:50:18:21:e8:04	
	153	2%		WEP	00:50:18:21:e8:02	
	153	60%		WEP	00:50:18:21:e8:06	

[Wireless AP リスト]から登録したい AP の選択項目のラジオボタンをクリックすると、チャネル、SSID、認証、暗号化、および MAC アドレスが自動的にプロファイルに入力されます。必要に応じて、アップリンク接続の WEP キーやプロシェアキーを入力するだけで済みます。

8.4. IPv6

HWL-3511-DS は IPv6（インターネットプロトコルバージョン 6）をサポートします。IPv6は全てのネットワーク機器にグローバルIPv6 アドレスを割り当てるため、IPアドレス変換など IPv4 の煩わしい設定が要らなくなり、ネットワークの番号再設定、ルーター通知が簡単になります。また、データ転送速度の向上も期待できます。

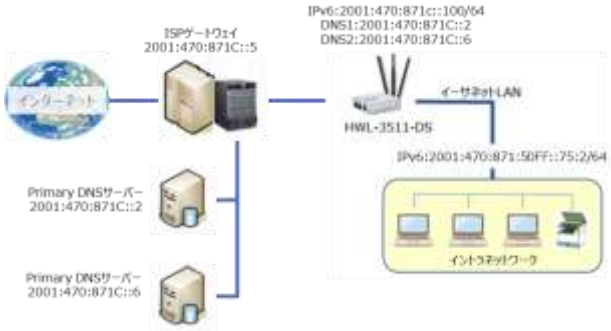
（注１） IPv6 を使用するためにはインターネットプロバイダ(ISP)が IPv6 に対応していなければなりません。
（注２） 3G/4G WAN インターフェイスを使用している場合は、IPv6 を IPv4 でカプセル化します。契約回線が IPv6 に対応しているかを確認してください。

8.4.1. IPv6 接続タイプ

IPv6 のネットワークに接続する方法として静的IPv6、DHCPv6 および PPPoEv6 があります。ご契約インターネットプロバイダ（ISP）の指定により選択します。

8.4.1.1. 静的 IPv6

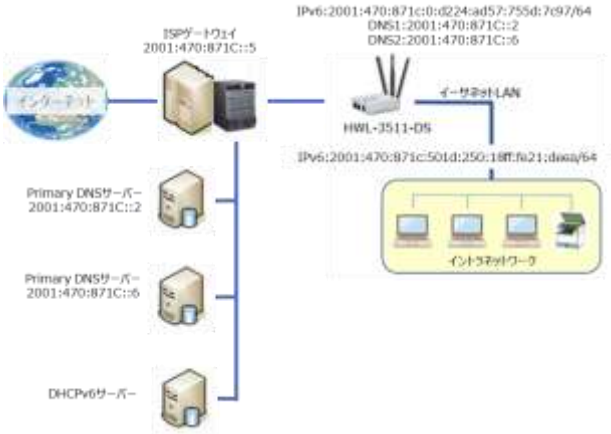
静的 IPv6 は、静的 IPv4 と同様な IP アドレッシングをします。静的 IPv6 動作には、IPv6 アドレス、IPv6 デフォルトゲートウェイアドレス、および、IPv6 DNS を手動で設定する必要があります。



左図は、IPv6 の IP アドレッシングを示しています。 IPv6 ネットワークを設定するために ISP から提供された情報を入力します。

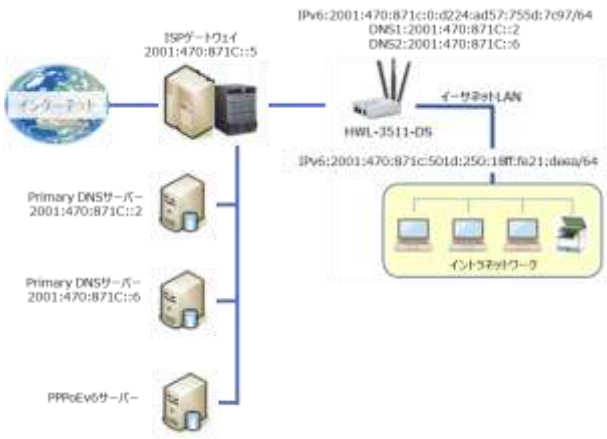
8.4.1.2. DHCPv6

IPv6 の DHCP サーバーは、IP アドレス、DNS サーバーアドレス、および、その他の可能なデータを DHCP クライアントに送信して自動的に設定します。また、サーバーは、アドレスのリース時間と IPv6 アドレスの更新のためにサーバーに再接続する時刻を送信します。クライアントは、IPv6 アドレスを更新する要求を再送信する必要があります。左図は、DHCPv6IP アドレッシングを示します。ISP の DHCPv6 サーバーが、IPv6 アドレス、IPv6 デフォルトゲートウェイアドレス、および、IPv6 DNS をクライアントホストに自動的に割り当てます。



8.4.1.3. PPPoEv6

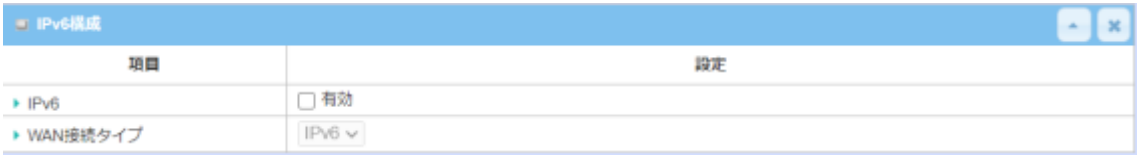
PPPoEv6 サーバーは、PPPoEv6 クライアントの要求に基づいて、構成パラメータを提供します。PPPoEv6 サーバーが、クライアントからの要求を取得し、正常に認証すると、サーバーは、IP アドレス、DNS サーバーアドレス、および、その他の必要なパラメータを送信し、クライアントを自動的に構成します。左図は、PPPoE による IPv6 アドレッシングを示しています。 ISP 側の PPPoEv6 サーバーは、PPPoEv6 クライアントからの要求を受信すると IPv6 構成を提供します。PPPoEv6 サーバーが、クライアントからの要求を取得し、正常に認証すると、サーバーは、IP アドレス、DNS サーバーアドレス、および、その他の必要なパラメータを送信し、クライアントを自動的に構成します。



8. 4. 2. IPv6 構成設定

IPv6 構成設定では、IPv6 ネットワークにアクセスするためのIPv6 接続タイプを設定します。

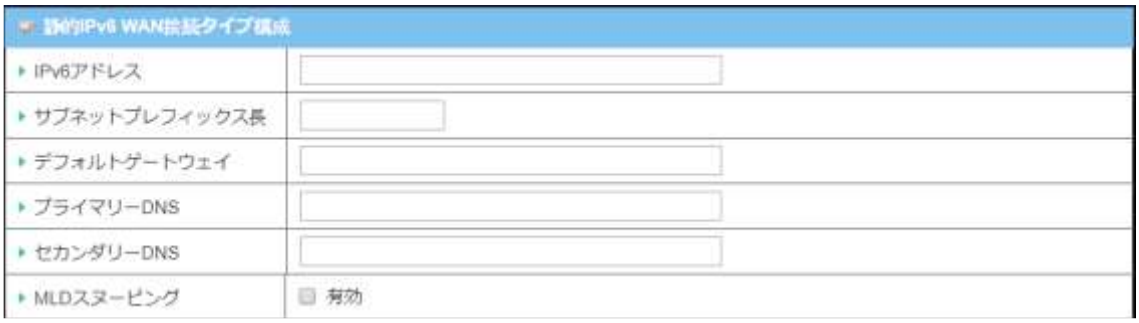
◆画面左側のメニューから、基本ネットワーク⇒IPv6⇒設定の順にクリックします。



項目	説明
IPv6	[有効]にチェックを入れると、IPv6機能が有効になります。
WAN 接続タイプ (注1)	IPv6接続を確立するIPv6 WAN接続タイプを指定します。 ご契約のインターネットプロバイダー（ISP）が静的IPv6接続であれば、[Static IPv6]を選択し、[スタティックIPv6 WANタイプ構成]に進みます。 DHCPv6サービス接続の場合は、[DHCPv6]を選択します。PPPoEv6アカウント接続の場合は、[PPPoEv6]を選択します。

（注１） 3G/4GWAN インタフェースの場合はIPv6のみの選択になります。

8.4.2.1. 静的 IPv6 WAN タイプ構成



項目	説明
IPv6 アドレス	WAN側のIPv6アドレスを入力します。
サブネットプレフィックス長	WAN側のサブネットプレフィックス長を入力します。
デフォルトゲートウェイ	WAN側のディフォルトゲートウェイIPv6アドレスを入力します。
プライマリーDNS	プライマリーDNSサーバーのIPv6アドレスを入力します。
セカンダリーDNS	セカンダリーDNSサーバーのIPv6アドレスを入力します。
MLD スヌーピング	[有効]をチェックするとMLDスヌーピングが有効になります。 VLAN環境でのIPv6マルチキャストフィルタリングが可能になります。

◆次に LAN 構成の設定を行います。

8.4.2.2. DHCPv6 WAN タイプ構成

項目	説明
DNS	IPv6 DNSサーバーアドレスの指定方法を選択します。 サーバーから：DHCPサーバーからDNSサーバーアドレスを取得します。 特定DNS：特定のDNSサーバーIPv6アドレスを手動設定します。
プライマリーDNS	特定のプライマリーDNSサーバーのIPv6アドレスを入力します。
セカンダリーDNS	特定のセカンダリーDNSサーバーのIPv6アドレスを入力します。
MLD スヌーピング	[有効]をチェックするとMLDスヌーピングが有効になります。 VLAN環境でのIPv6マルチキャストフィルタリングが可能になります。

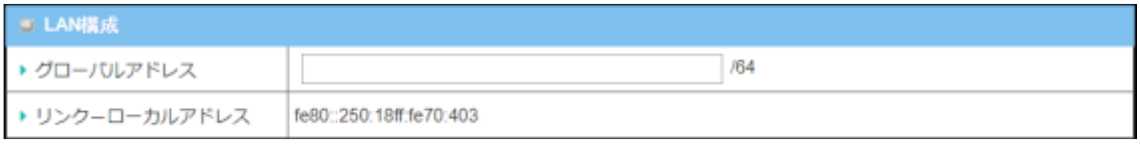
8.4.2.3. PPPoE WAN タイプ構成

項目	説明
アカウント(注 1)	PPPoEv6接続アカウント名（45文字以下）を入力します。
パスワード(注 1)	PPPoEv6接続パスワードを入力します
サービス名(注 1)	PPPoEv6接続サービス名（45文字以下）を入力します。
接続制御	自動再接続（常にオン）固定です。
MTU(注 1)	PPPoEv6接続時のMTUを入力します。値の範囲は1280～1492です。
MLD スヌーピング	[有効]をチェックするとMLDスヌーピングが有効になります。 VLAN環境でのIPv6マルチキャストフィルタリングが可能になります。

（注１） 詳しい情報が必要な場合は、ご利用のインターネットプロバイダ（IPS）にご確認ください。

◆次に LAN 構成に進みます。

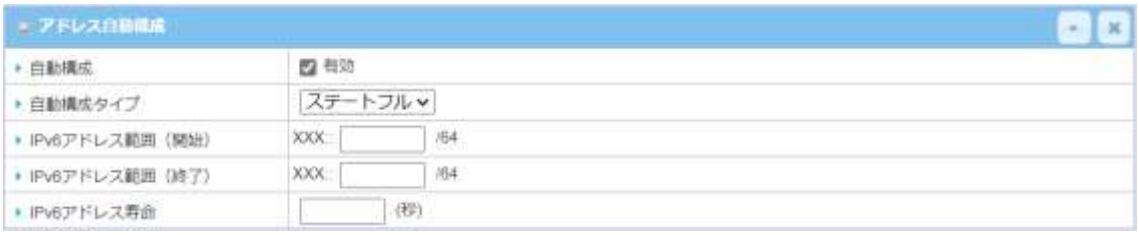
8.4.2.4. LAN 構成



項目	説明
グローバルアドレス	LANのIPv6アドレスを入力します。
リンクローカルアドレス	本機のLAN側リンクローカルアドレスが表示されます。

◆次にアドレス自動構成の設定に進みます。

8.4.2.5. アドレス自動構成



項目	説明
自動構成	[有効]チェックを入れて、自動構成機能を有効します。
自動構成タイプ	IPv6接続を確立する自動構成タイプを選択します。 ステートレス：ローカルエリアネットワークをSLAAC + RDNSSとなるように管理します。 ステートフル：ローカルエリアネットワークをステートフル（DHCPv6）となるように管理します。IPv6アドレス範囲（開始）とIPv6アドレス範囲（終了）を設定する必要があります。
IPv6 アドレス範囲（開始）	ローカルコンピュータに対するDHCPv6範囲の開始IPv6アドレスを入力します。値の範囲は0001～FFFFです。本項目は自動構成タイプにステートフルを選択した時のみ表示されます。
IPv6 アドレス範囲（終了）	ローカルコンピュータに対するDHCPv6範囲の終了IPv6アドレスを入力します。値の範囲は0001～FFFFです。本項目は自動構成タイプにステートフルを選択した時のみ表示されます。
IPv6 アドレス寿命	IPv6アドレスの有効時間（秒単位）を入力します。値の範囲は0～65535です。

◆ 設定終了後に保存ボタンをクリックして、設定を保存し、再起動ボタンをクリックして本機を再起動します。

8.5. ポート転送

IPv4 プロトコルで運用中のネットワークにおいて、一つのグローバル IP アドレスを複数のローカルネットワークの IP 機器で共用することを可能にするのが、ネットワークアドレス変換（NAT または NAPT）機能です。半面、この機能が動作していると、インターネットなど外部から、ローカルネットワークに接続された IP 機器に直接アクセスできない不都合が生じます。本機では、この不都合を解決するためにポート転送（ポートフォワーディング）機能を搭載し、外部から登録されたローカルネットワークのサーバーなどIP機器にアクセスできます。

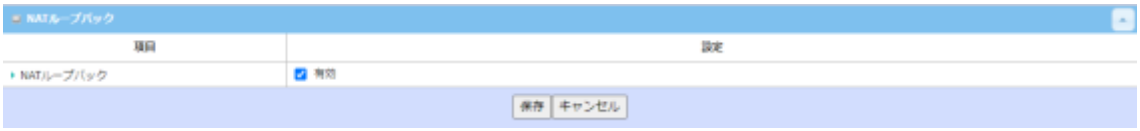
（注） NAT 機能の有効/無効は WAN ポートの接続設定内にあります。（詳細は 8.1 項 WAN およびアップリンクを参照してください。）

8.5.1. ポート転送設定

8.5.1.1. NAT ループバック

NAT ループバック機能を有効にすると、ローカルネットワーク機器から本機のグローバル IP アドレスにアクセスできます。 仮想サーバーの動作確認に使用できます。

◆画面左側のメニューから、基本ネットワーク⇒ポート転送⇒設定の順にクリックします。



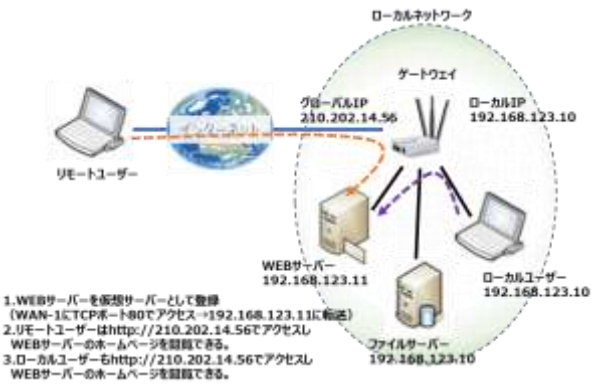
項目	説明
NTT ループバック	[有効]ボックスにチェックすると、NTT ループバック機能が有効になります。

◆設定終了後に保存ボタンをクリックして、設定を保存します。

8.5.2. 仮想サーバー＆仮想コンピュータ

仮想サーバーおよび仮想コンピュータはアドレス変換機能（NAT）有効のゲートウェイ（本機）ネットワーク構成において、ターネット経由など外部からローカルネットワーク内の各種サーバーなど IP 機器（ホスト）に対するアクセスを可能にする概念です。

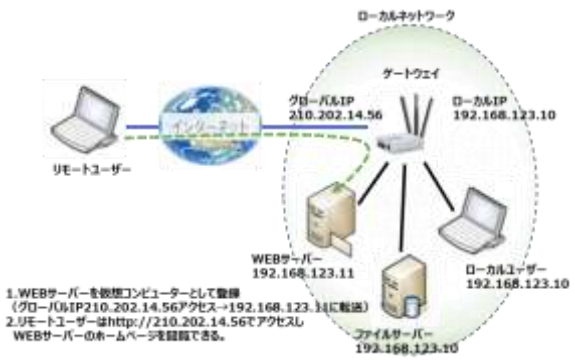
8.5.2.1. 仮想サーバー



仮想サーバーとは一般的なポートフォワーディング機能です。外部からWANポートへのアクセスに対して TCP/IP プロトコルのIP種別やポート番号で識別し、転送先（仮想サーバー）を決定します。この仮想サーバーには NAT ループバック機能を活用することで、外部からもイントラネットからも同一アドレス（WAN グローバル IP アドレス）でアクセスすることが可能になります。

8.5.2.2. 仮想コンピュータ

仮想コンピュータとは、TCP/IP プロトコルによる外部からのグローバル IP アドレスへのアクセスを全て特定のローカルネットワーク内のサーバーなどIP機器（仮想コンピュータ）1台のみに転送する機能です。本機能は固定グローバルIPアドレス契約などの環境で使用します。WAN ポートでなくグローバルIPアドレスが条件となる点が、後述の DMZ 機能との違いになります。



8.5.2.3. 仮想サーバーおよび仮想コンピュータの有効

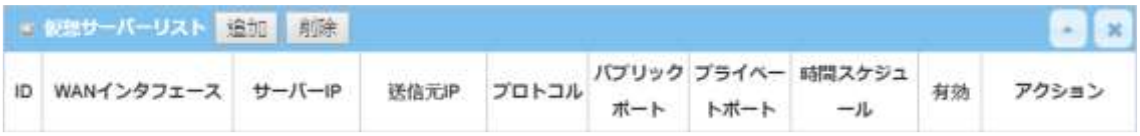
◆画面左側のメニューから、基本ネットワーク⇒ポート転送⇒仮想サーバーおよび仮想コンピュータの順にクリックします。

項目	説明
仮想サーバー	[有効]ボックスにチェックすると、仮想サーバー転送機能が有効になります。
仮想コンピュータ	[有効]ボックスにチェックすると、仮想コンピューター転送機能が有効になります。

◆保存ボタンをクリックして、設定を保存します。

8.5.2.4. 仮想サーバーの追加/編集

[仮想サーバーリスト]へ仮想サーバールールを登録します。最大20のルールが登録できます。



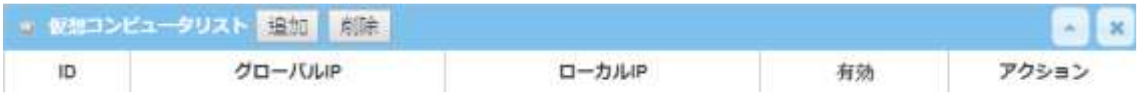
◆追加ボタンまたは編集ボタンをクリックすると、[仮想サーバールール設定]画面が表示されます。

項目	説明
WAN インターフェイス	仮想サーバーへのポート転送を許可するWANインターフェイスを選択します。全部、WAN-1 または WAN-2 が選択できます。
サーバーIP	仮想サーバーのローカルネットワーク IP アドレスを指定します。
送信元IP	外部アクセスを許可する送信元の IP アドレスを指定します。指定方法は以下の 3 種類があります。 ◆任意：全ての送信元の IP アドレスで仮想サーバーへの転送が許可されます。 ◆特定の IP アドレス：一つの送信元 IP アドレスのみが仮想サーバーへの転送が許可されます。 ◆IP 範囲：送信元の IP アドレスが指定した範囲であるときに仮想サーバーへの転送が許可されます。
プロトコル	仮想サーバーへの転送を許可するプロトコルを指定します。 ICMPv4、UDP、TCP、UDP&TCP、GRE、ESP、SCTP およびユーザー定義が選択できます。選択項目右の（）内の数字は IP プロトコル番号を表しています。ユーザー定義は任意の IP プロトコル番号を指定します。
パブリックポート	プロトコルで UDP、TCP および UDP&TCP を選択した時に、仮想サーバーへの転送を許可する TCP ポート（サービス）番号指定します。 ◆既知のサービス：よく使われるプロトコルから一つを選択します。 ◆単一ポート：任意の TCP ポート番号一つを指定します。 ◆ポート範囲：任意の TCP ポート番号を範囲で指定します。
プライベートポート	本機ではサポートしていません。空欄にしてください。
時間スケジュール	本仮想サーバールールが有効になる時間スケジュールを指定します。 常時(0)または「スケジュール設定」で定義されたスケジュールリストから選択できます。
ルール	[有効]にチェックを入れると、この仮想サーバールールが有効になります。

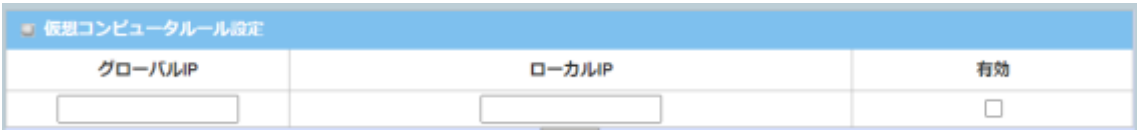
◆ 保存ボタンをクリックして、ルールを登録します。設定したルールが［仮想サーバーリスト］に表示されます。

8.5.2.5. 仮想コンピュータの追加/編集

[仮想コンピュータリスト]へ仮想コンピュータルールを登録します。最大 20 のルールが登録できます。



◆追加ボタンまたは編集ボタンをクリックすると、[仮想コンピュータルール設定]画面が表示されます。



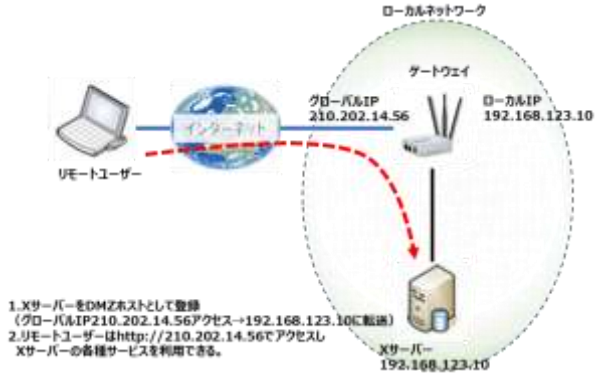
項目	説明
グローバル IP	仮想コンピュータへの転送を許可する、本機 WAN 側の IP アドレスを指定します。
ローカルIP	仮想コンピュータにローカル IP アドレスを指定します。
有効	[有効]にチェックを入れると、この仮想コンピュータルールが有効になります。

◆保存ボタンをクリックして、ルールを登録します。設定したルールが[仮想コンピュータリスト]に表示されます。

8.5.3. DMZ およびパススルー

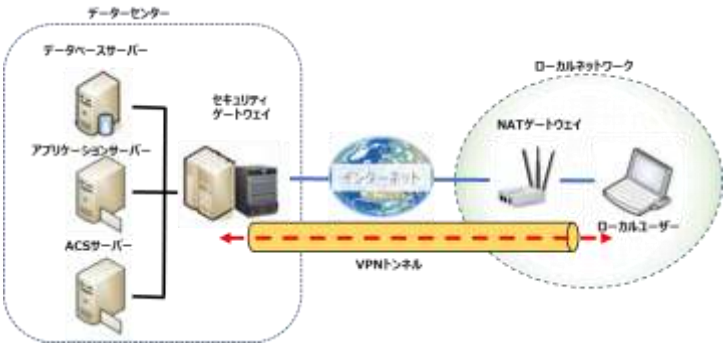
外部からの WAN ポートへのアクセスを全て特定のローカルネットワーク内のサーバーなど IP 機器（DMZ ホスト）1 台のみに転送する機能です。また、本機は NAT 配下の IP 機器が IPSec/PPTP/L2TP の VPN トネリングを外部の機器と構成できるようする VPN パススルー機能を搭載しています。

8.5.3.1. DMZ（De Militarized Zone）



X サーバーをローカルエリアネットワークに配置した場合、リモートユーザーがサーバーからのサービスを要求する場合には、このサーバーを DMZ ホストとなるように設定する必要があります。左図はリモートユーザーがグローバル IP210.202.14.56 のゲートウェイにアクセスすることで X サーバーからサービスを要求することができます。本機は、仮想サーバーの登録ルール以外の外部アクセスを直接 DMZ ホストに転送します。

8.5.3.2. VPN パススルー



アドレス変換機能(NAT)が動作している場合、ローカルエリアネットワークに接続されたローカルユーザーが、直接外部のセキュアネットワークにアクセスするための VPN トネリングを構成することはできません。本機は、VPN パススルー機能により、ローカルユーザーが任意のデータセンターなどのセキュアネットワークにアクセスできるよう設定できます。

8.5.3.3. DMZ の設定

◆画面左側のメニューから、基本ネットワーク⇒ポート転送⇒DMZ およびパススルーの順にクリックします。

項目	説明
有効	[有効]ボックスにチェックすると、DMZ 機能が有効になります。
ポート	DMZ を許可するインタフェースを全部、WAN-1 および WAN-2 から選択します。
DMZ ホスト	DMZ ホストにするローカルネットワーク内機器のローカル IP アドレスを指定します。

◆保存ボタンをクリックして、設定を登録します。

8.5.3.4. VPN パススルーの設定

◆画面左側のメニューから、基本ネットワーク⇒ポート転送⇒DMZ およびパススルーの順にクリックします。

項目	説明
パススルーの有効化	パススルー可能な VPN プロトコルは IPSec、PPTP、L2TP です。 パススルーを許可する VPN プロトコルにチェックを入れます。

◆保存ボタンをクリックして、設定を登録します。

8.6. ルーティング

複数のローカルネットワーク(サブネットネットワーク)間で通信ができるようにするには、データパケットが適切な経路を経由する必要があります。それぞれのローカルネットワークにはゲートウェイがルーティング(経路選択)を行うことで、実現しています。そのため、ゲートウェイ(ルーター)にはルーティングテーブルが作成され、サブネット情報を元にデータパケットの送信先を選択します。ルーティングテーブルを事前に手動入力する「静的ルーティング」とゲートウェイ(ルーター)間でルーティングテーブルを構築する「動的ルーティング」があります。本機では、静的ルーティング、RIP/RIP2 や OSPF のプロトコルを使用した動的ルーティングに対応しています。

8.6.1. 静的ルーティング

静的ルーティングを使用することにより、ルーティングテーブルに一部のホスト(IP 機器)/サーバーやサブネットへのルーティングパスを定義することができます。

8.6.1.1. 静的ルーティングの設定

◆画面左側のメニューから、基本ネットワーク⇒ルーティング⇒静的ルーティングの順にクリックします。

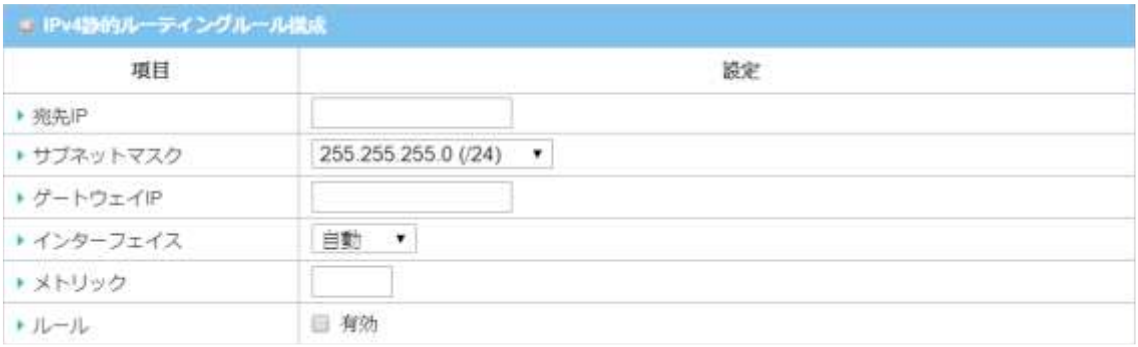
項目	説明
静的ルーティング	[有効]ボックスにチェックすると、静的ルーティング機能が有効になります。

◆保存ボタンをクリックして、設定を登録します。

8.6.1.2. IPv4 静的ルーティングルールの追加/編集

IPv4静的ルーティングルールリストには、全ての静的ルーティングルールのパラメータが表示されます。

◆追加ボタンまたは編集ボタンをクリックすると[IPv4 静的ルーティングルール構成]画面が表示されます。



項目	説明
宛先 IP	この静的ルーティングルールの宛先 IP を指定します。
サブネットマスク	この静的ルーティングルールのサブネットマスクを選択します。
ゲートウェイ IP	この静的ルーティングルールのゲートウェイ IP を指定します。
インターフェイス	この静的ルーティングルールのインターフェイスを選択します。「自動」、または、利用可能な「WAN/LAN」インターフェイスが選択できます。
メトリック	この静的ルーティングルールのメトリックです。値の範囲は 0~255 です。メトリックとは経路の距離を示し 0 が最短となります。
ルール	[有効]にチェックを入れると、この静的ルーティングルールが有効になります。

◆保存ボタンをクリックして、ルールを登録します。設定したルールが[IPv4静的ルーティングルールリスト]に表示されます。

8.6.2. 動的ルーティング

適応型ルーティングとも呼ばれる動的ルーティングは、近隣するゲートウェイ(ルーター)のルーティング情報(経路情報)を共有し、ネットワーク状態変化に適応しながら、ルーティングパス(経路)を選択します。そのため、ネットワークが多数のローカルネットワーク(サブネット)で構成される場合にネットワーク管理を簡易にします。本機に搭載する RIP(Routing Information Protocol)は小規模ネットワークに適しており、OSPF(Open Short Pass First)は中規模のネットワークに適しています。

8.6.2.1. RIPv1/RIPv2 ルーティング

RIP は、ルーティングメトリックにてホップ数を使用する距離ベクトルルーティングプロトコルです。RIP では最大ホップカウントが 15 に制限されているため、基本的にルーティングループを防止できますが、ネットワークサイズも比較的小さいものになります。本機の RIP には誤ったルーティング情報の伝搬を防止する機能(split horizon, route poisoning and hold-down mechanisms)を実装しています。

8.6.2.2. OSPF ルーティング

OSPF（Open Shortest Path First）とは、リンクステートルーティングアルゴリズムを使用するルーティングプロトコルです。大規模な企業ネットワークで広く使用されている動的ルーティングプロトコルの一つです。OSPF 対象ネットワーク（バックボーンネットワーク）上にあるゲートウェイ（ルーター）間で、IP アドレスに基づいたバックボーンネットワーク外のルーティング情報を共有します。

8.6.2.3. RIP 設定

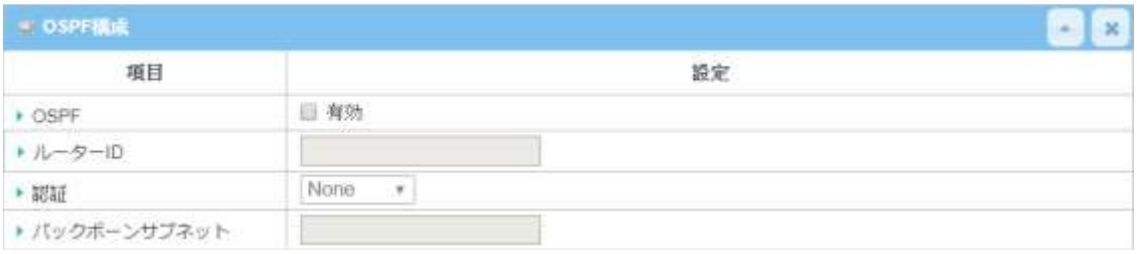
◆画面左側のメニューから、基本ネットワーク⇒ルーティング⇒動的ルーティングの順にクリックします。

項目	説明
RIP	RIP プロトコルの動作を選択します。 無効：RIP プロトコルが無効になります。 RIPv1：RIPv1 プロトコルが有効になります。 RIPv2：RIPv2 プロトコルが有効になります。

◆保存ボタンをクリックして、設定を登録します。

8.6.2.4. OSPF 設定

◆画面左側のメニューから、基本ネットワーク⇒ルーティング⇒動的ルーティングの順にクリックします。



項目	説明
OSPF	[有効]ボックスにチェックすると、OSPF プロトコルが有効になります。
ルーターID	OSPF プロトコル上の本機のルーターID（本機 IP アドレス）を指定します。
認証	OSPF プロトコルで使用する認証方法を選択します。 ◆None；、OSPF プロトコルの認証が無効です。 ◆テキスト； OSPF プロトコルでは、指定された「Key」によるテキスト認証が有効になります。 ◆MD5； OSPF プロトコル上では指定された「ID（範囲 1~255）」と「Key」に

	よる MD5 認証が有効になります。
バックボーンサブネット	OSPF プロトコルで使用するバックボーンサブネットを指定します。 サブネットアドレス/マスク長(10.24.0.0/16 など)形式です。

◆保存ボタンをクリックして、設定を登録します。

8.6.2.5. OSPF 領域リストの追加/編集

OSPF 領域リストには、全ての OSPF 領域のパラメータが表示されます。

◆追加ボタンまたは編集ボタンをクリックすると[IPv4 静的ルーティングルール構成]画面が表示されます。

項目	説明
領域サブネット	OSPF 領域リスト上の本機の領域サブネットを指定します。 サブネットアドレス/マスク長(10.24.0.0/16 など)形式です。
領域 ID	OSPF 領域リスト上の本機の領域 ID(IP アドレス)を指定します。
領域	[有効]にチェックを入れると、この OSPF 領域ルールが有効になります。

◆保存ボタンをクリックして、ルールを登録します。設定したルールが[OSPF 領域リスト]に表示されます。

8.6.3. ルーティング情報

静的ルーティングおよび動的ルーティングで構成された本機のルーティング情報を表示します。

◆画面左側のメニューから、基本ネットワーク⇒ルーティング⇒ルーティング情報の順にクリックします。

Routing Table

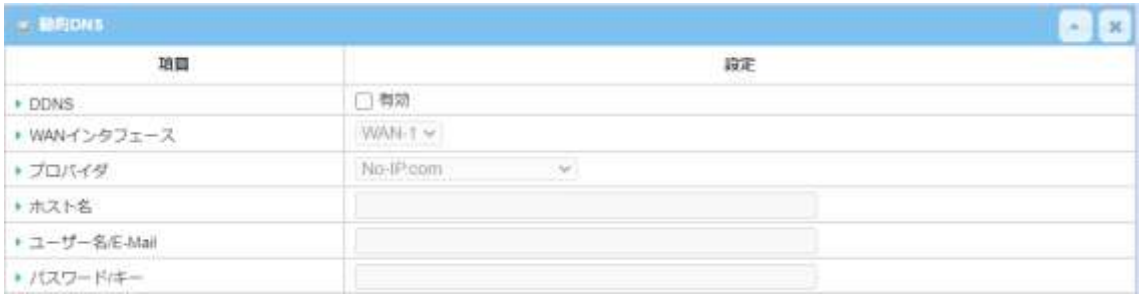
宛先IP	サブネットマスク	ゲートウェイIP	メトリック	インターフェイス
192.168.12.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

8.7. DNS & DDNS

3G/4G WAN インターフェイスのように WAN IP アドレスが動する場合、DDNS（ダイナミック・ドメインネーム・サーバー）サービスプロバイダのドメイン名を使用することで、外部より一つのドメイン名で本機および配下のローカルネットワークにアクセスすることができるようになります。DDNS サービスは、無料または有料となる場合があります。

◆画面左側のメニューから、基本ネットワーク⇒DNS & DDNS⇒設定の順にクリックします。

8.7.1. 動的 DNS の設定



項目	説明
DDNS	[有効]にチェックを入れ、DDNS機能を有効します。
WAN インタフェース	DDNSを適用するWANインターフェイスを選択します。
プロバイダ	使用するDDNSサービスプロバイダを選択します。 本機は以下のプロバイダをサポートしています。 DynDNS.org(Dynamic)/DynDNS.org(Custom)/No-IP.com/TZO.com/ DynamicDO!.jp(Free)/ DynamicDO!.jp(Charge) （注１） サービスは内容により有償/無償があります。詳細は各 DDNS サービスプロバイダのホームページで確認してください。
ホスト名	DDNSサービスプロバイダに登録した動的DNSのホスト名(63文字以下)を指定します。
ユーザー名/E-Mail	DDNSサービスのユーザー名またはEメールアドレスを指定します。
パスワード/キー	DDNSサービスのパスワードまたはキーを指定します。

◆保存ボタンをクリックして設定を保存します。

8.7.2. DNS リダイレクトの設定

DNS リダイレクトとは、あらかじめ設定した特定のデータを指定されたホスト(IP機器/サーバー)にリダイレクト(転送)する特別な機能です。管理者は、制限された DNS にアクセスしようとするインターネット/イントラネットのデータトラフィックを管理し、それらを指定されたホストにリダイレクトさせることができます。

項目	説明
DNS リダイレクト	[有効]にチェックを入れ、DNSリダイレクト機能を有効します。

DNS リダイレクト機能を有効にした場合、リダイレクトルールを作成する必要があります。このルールに従い、本機は特定のデータトラフィックを特定のホストにリダイレクトすることができます。

8.7.3. リダイレクトルールの定義

◆追加ボタンをクリックすると、[リダイレクトルール]画面が表示されます。

項目	説明
マッピングルール	ドメイン名:データをリダイレクト(転送)するドメイン名を指定します。 IP:リダイレクト(転送)先のIPアドレスを指定します。
条件	[常時]または登録したタイムスケジュールリスト内から選択します。
説明	このルールの説明を 63 文字以内に入力できます。
有効	[有効]にチェックを入れ、本ルールを有効します。
保存	保存ボタンをクリックして、本ルールを登録します。

9. オブジェクト定義

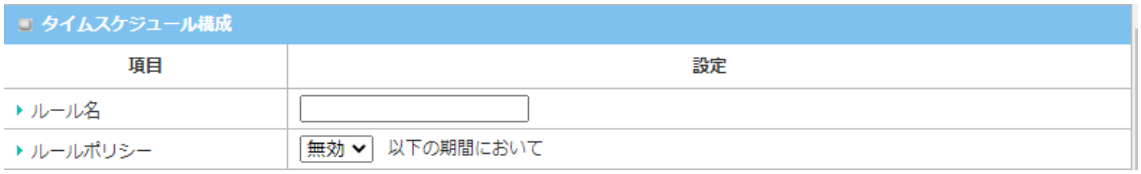
9.1. スケジューリング

スケジューリングは本機システム内で使用するタイムスケジュールリストを追加/編集し、必要な機能項目で選択できるようになります。

◆画面左側のメニューから、オブジェクト定義⇒スケジューリング⇒設定の順にクリックします。

9.1.1.1. タイムスケジュールリストの追加/編集

◆追加または編集ボタンをクリックすると、[タイムスケジュール構成]画面が表示されます。



項目	説明
ルール名	ルールを識別するためのルール名を指定します。
ルールポリシー	期間定義で設定した期間に機能の有効/無効を選択します。

9.1.1.2. 期間定義の設定

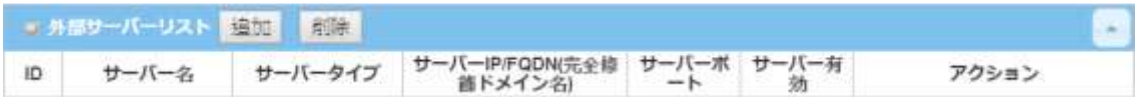
項目	説明
週日	毎日または曜日のいずれかを選択します
開始時間	選択した曜日の開始時間を指定します。
終時間	選択した曜日の終了時間を指定します。

9.2. 外部サーバー

いくつかの外部サーバーを定義することができます。

◆画面左側のメニューから、オブジェクト定義⇒外部サーバー⇒外部サーバーの順にクリックします。

9.2.1.1. 外部サーバーリストの追加/編集



◆追加または編集ボタンをクリックすると、[外部サーバー構成]画面が表示されます。

項目	説明
サーバー名	ルールを識別するためのサーバー名を指定します。
サーバータイプ	外部サーバーのサーバータイプを以下から選択し、サーバーにアクセスするために必要なパラメーターを指定します。 ◆Eメールサーバー:追加設定項目あり ユーザー名:文字列形式:任意のテキスト パスワード:文字列形式:任意のテキスト ◆Syslogサーバー:追加設定項目なし

項目	説明
	◆RADIUSサーバー：追加設定項目あり プライマリ： プリシェアキー（事前共有キー）：文字列形式<任意のテキスト> 認証プロトコル：CHAPまたはPAPから選択します。 セッションタイムアウト：値の範囲は1～60分。 アイドルタイムアウト：値の範囲は1～15分。 Sセカンダリ： プリシェアキー（事前共有キー）：文字列形式<任意のテキスト> 認証プロトコル：CHAPまたはPAPから選択します。 セッションタイムアウト：値の範囲は1～60分。 アイドルタイムアウト：値の範囲は1～15分。 ◆FTPサーバー追加設定項目あり ユーザー名：文字列形式＜任意のテキスト＞ パスワード：文字列形式＜任意のテキスト＞ プロトコル：FTPまたはSFTPを選択します。 暗号化：Plain、Explicit FTPSまたはImplicit FTPSを選択します。 転送モード：Passiveまたはアクティブを選択します。
サーバ IP/FQDN	外部サーバー用に使用するIPアドレスまたはFQDNを指定します。
サーバーポート または 認証ポート	外部サーバー用に使用するポートを指定します。特定のサーバータイプを選択した場合、初期サーバーポート番号が指定されてます。 ◆Eメールサーバー：25 ◆Syslogサーバー：514 ◆RADIUSサーバー：1812 ◆FTPサーバー:21
アカウンティングポート	外部RADIUSサーバーを選択する場合は、使用するアカウントポートを1～65535の範囲で指定します。
サーバー	[有効]にチェックを入れ、本ルールを有効します。

◆ 保存ボタンをクリックして、ルールを登録します。設定したルールが[外部サーバーリスト]に表示されます。

9.3. 証明書

証明書はトランスポート層セキュリティ(TLS、従来の SSL)の重要な要素で、攻撃者が安全な Web サイトやその他のサーバーを偽装することを防ぎます。また、電子メールの暗号化やコード署名などの重要な用途でも使用されます。ここでは、ユーザー認証用の IPSec トンネリングで使用できます。

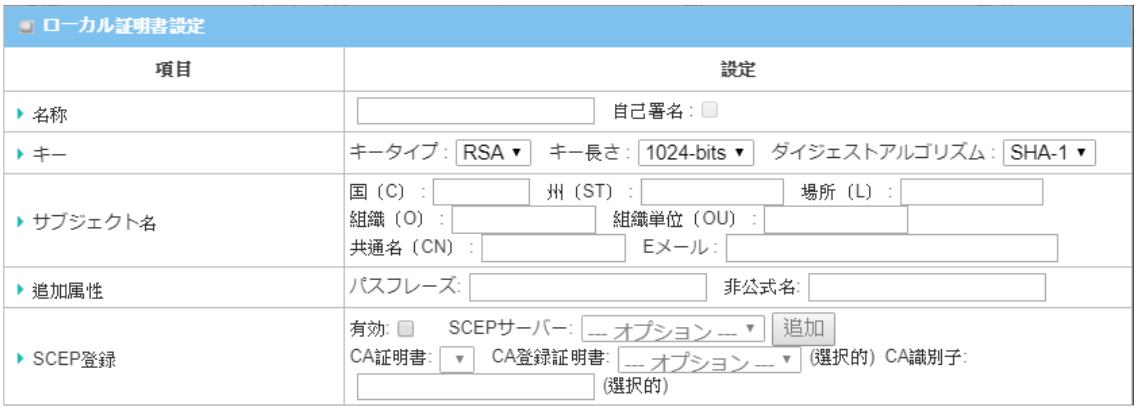
9.3.1. ローカル証明書

9.3.1.1. ローカル証明書の作成

◆画面左側のメニューから、オブジェクト定義⇒証明書⇒ローカル証明書の順にクリックします。

◆追加ボタンをクリックすると、[ローカル証明書作成構成]画面が表示されます。

証明書または CSR に記入するのに必要な情報には、名前、キーおよびサブジェクト名が含まれます。「自己署名」ボックスにチェックが入っている場合は証明書、それ以外の場合は CSR です。

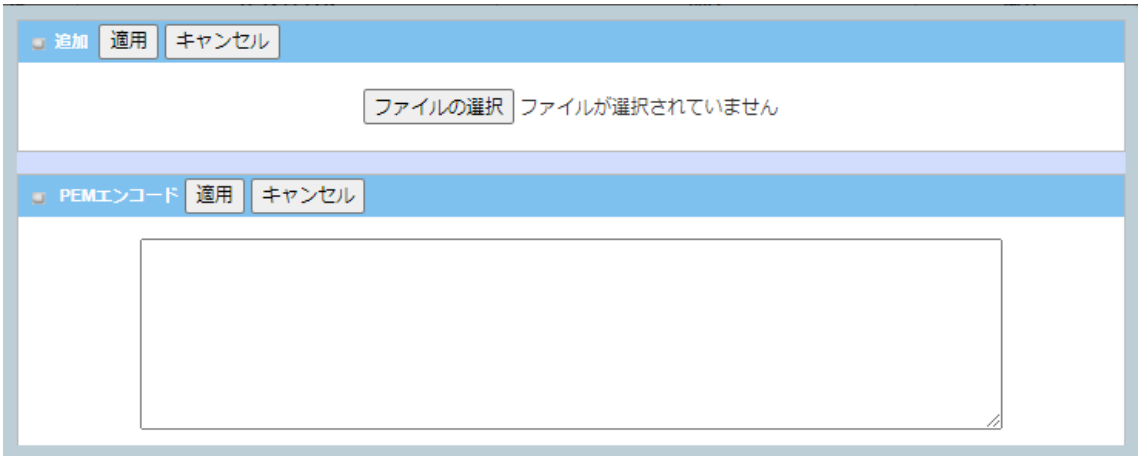


項目	説明
名称	証明書名を入力します。これが、証明書ファイル名になります ◆自己署名にチェックが入っている場合は、ルートCAにより署名されます。 ◆自己署名にチェックが入っていない場合、証明書署名要求(CSR)が生成されます。
キー	証明書のキー属性を指定します。 ◆公開鍵暗号システム:RSAのみがサポート ◆キービット長:「512」、「768」、「1024」、「1536」、「2048」から選択 ◆証明書の署名暗号化:「MD5」または「SHA-1」
サブジェクト名	証明書の情報を指定します。 ◆Country(C)(国(C))は、組織が所在する国の2文字のISOコードです。 ◆State(ST)(州(ST))は、組織が所在する州です。 ◆Location(L) (場所(L))は、組織が所在する場所です。

項目	説明
	◆Organization(O)（組織（O））は、組織の名称です。 ◆Organization Unit(OU)（組織単位（OU））は、組織単位の名称です。 ◆Common Name(CN)（共通名（CN））は、組織の名称です。 ◆Email（Eメール）は、組織のEメールです。これは、Eメールアドレス設定でなければなりません。
追加属性	証明書を生成するための追加情報を指定します。
SCEP 登録	SCEP.の情報を指定します。 証明書署名要求（CSR）を生成し、次に、SCEPサーバーにより、オンラインで署名する場合、[有効]にチェックを入れることができます。 SCEPサーバーを選択し、使用するSCEPサーバーを識別します。サーバーの詳細情報は、外部サーバー機能で登録します。 どの証明書が認証のためにSCEPサーバーにより、受け入れられるかを識別するために、CA証明書を選択します。これは、信頼できる証明書で生成されます。 必要に応じで、オプションのCA暗号化証明書選択して、どの証明書が、データ情報の暗号化のために、SCEPサーバーにより受け入れられるかを識別します。これは、信頼できる証明書で生成されます。 オプションのCA識別子を入力して、証明書に署名するために使用できるCAを識別します。

9.3.1.2. 証明書のインポート

Importボタンをクリックすると、[インポート]画面が表示されます。存在する証明書ファイルから証明書をインポートすること、または、証明書として PEM でエンコードされた文字列を直接貼り付けることができます。



項目	説明
インポート	ユーザーのコンピュータから証明書ファイルを選択し、適用ボタンをクリックして、指定した証明書ファイルをゲートウェイにインポートします。
PEM エンコード	EMエンコードされた証明書文字列を直接入力(コピーアンドペースト)することができます。また、適用ボタンをクリックして、指定した証明書をゲートウェイにインポートすることができます。
適用	適用ボタンをクリックして、証明書をインポートします。

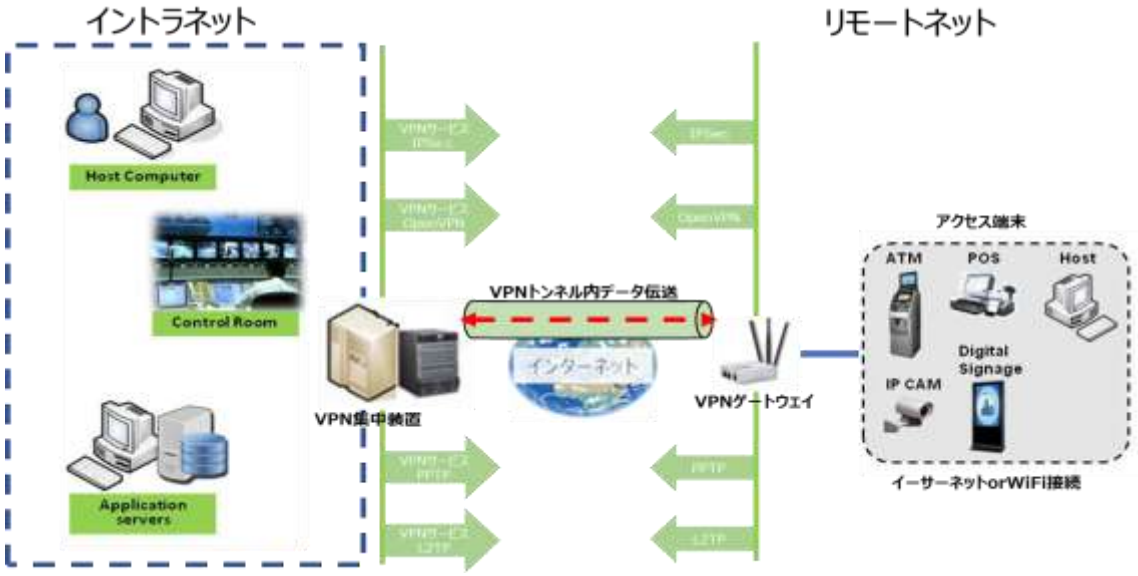
9.3.2. 信頼できる証明書

本機能はサポートしていません。

10. セキュリティ

10. 1. VPN

仮想プライベートネットワーク（VPN）は、インターネットなどのパブリックネットワーク全体にプライベートネットワークを拡張します。 これにより、ネットワーク機器は、プライベートネットワークの機能、セキュリティ、および管理ポリシーの配下の元、共有ネットワークまたはパブリックネットワークを介してプライベートネットワークに直接接続しデータを送受信できます。 これは、トンネル技術によるカプセル化プロトコル、暗号化アルゴリズム、およびハッシュアルゴリズムを利用することにより仮想ポイントツーポイント接続を確立することによって、ネットワーク情報のデータ機密性、データ発信元認証、およびデータ整合性を確保しながら実現しています。

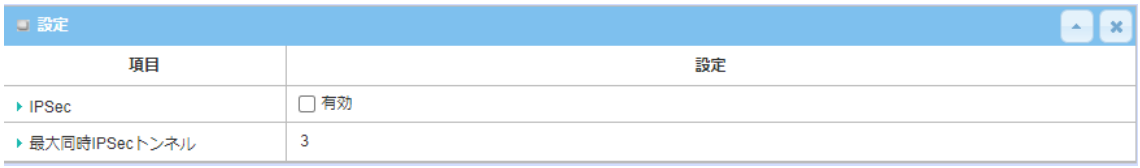


10. 1. 1. IPSec

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り、インターネットプロトコル(IP)通信を保護するためのプロトコルです。
IPSecVPN トンネルは IPSec クライアント(イニシエーター)とサーバー(レスポンダー)の間に確立されます。本機は、IPSec クライアントとしてもサーバーとしても動作できるのでさまざまなリモートデバイスとのトンネル確立できます。

10.1.1.1. IPSec の設定

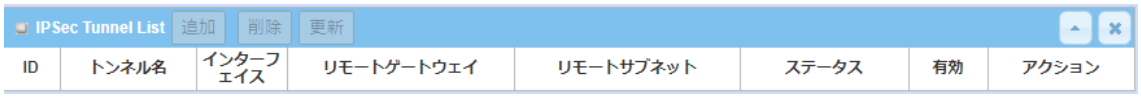
◆画面左側のメニューから、セキュリティ⇒VPN⇒IPSec の順にクリックします。



項目	説明
IPSec	[有効]にチェックを入れると、IPSecVPNが有効になります。
最大同時 IPSec トンネル	本機の場合、3です。

◆保存ボタンをクリックして、設定を登録します。

10.1.1.2. IPSec トンネルの追加/編集



◆追加または編集ボタンをクリックすると、[設定]画面が表示されます。「トンネル設定」、「ローカル＆リモート設定」、「認証」、「IKE フェーズ」、「IKE プロポーザル定義」、「IPSec フェーズ」および「IPSec プロポーザル定義」の項目を、ローカルとリモート両方の VPN デバイスにて、トンネルの詳細を設定する必要があります。

10.1.1.3. トンネル設定

項目	説明
IPSec	[有効]にチェックを入れると、トンネル有効になります。
トンネル名	識別のためのトンネル名(19文字以下)を指定します。
インターフェイス	IPSecトンネルを確立するインターフェイスを「WAN」および「LAN」から選択します。
トンネルシナリオ	アプリケーションのドロップダウンボックスから、IPSecトンネリングシナリオを選択します。 ◆Site to Site:サブネット間接続 ◆Site to Host: サブネット→ホスト間接続 ◆Host to Site:ホスト→サブネット接続 ◆Host to Host:ホスト→ホスト接続
トンネル TCP MSS	ドロップダウンボックスから選択して、Tunel TCPMSSのサイズを定義します。 自動:すべてのデバイスがこのパラメーターを自動的に調整します。 手動:Tunel TCPMSSの期待される値を指定します。値の範囲は64～1500バイトです。
ICMP Keep alive	[有効]にチェックを入れると、ICMP Keep aliveが有効になります。 キープアライブ機能が有効になっている場合: 失敗試行の数、チェック間隔、ICMPパケットの送信元/宛先IPアドレスを指定する必要があります。 値の範囲:失敗した試行と時間間隔は1～999。
カプセル化プロトコル	カプセル化プロトコルを「ESP」または「AH」から選択します。
IKE バージョン	IKEバージョンを「v1」または「v2」から選択します。 (注)カプセル化プロトコルに「AH」が選択されている場合、IKEバージョンは無効になります。

10.1.1.4. ローカル＆リモート設定

項目	説明
ローカルサブネットリスト	ローカルサブネットのIPアドレスとサブネットマスクを指定します。 ローカルサブネットが複数ある場合は追加ボタンで追加します。
リモートサブネットリスト	リモートサブネットのIPアドレスとサブネットマスクを指定します。 リモートサブネットが複数ある場合は追加ボタンで追加します。

項目	説明
リモートゲートウェイ	リモートゲートウェイのIPアドレスまたはFQDNを指定します。

10.1.1.5. 認証設定

項目	説明
キー管理	キー管理方法を選択します。 ◆IKE+事前共有キー：キー（8～32文字）を指定します。 ◆IKE+X.509：証明書を使用して認証します。証明書の詳細は証明書の項目を参照してください。
ローカル ID	IPSecトンネルのローカルIDを指定します。IDの形式は「ユーザー名」、「FQDN」、「User@FQDN」または「キーID」から選択し、それぞれに適合したフォーマットでIDを指定します。
リモート ID	IPSecトンネルのリモートIDを指定します。IDの形式は「ユーザー名」、「FQDN」、「User@FQDN」または「キーID」から選択し、それぞれに適合したフォーマットでIDを指定します。

10.1.1.6. IKE フェーズ設定

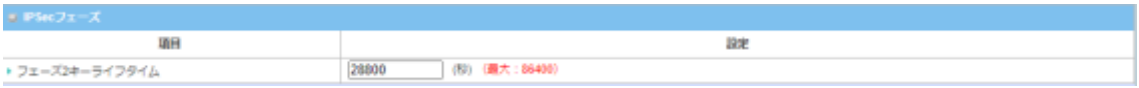
項目	説明
ネゴシエーションモード	IPSecトンネルのネゴシエーションモードを「メインモード」または「アグレッシブモード」から選択します。
X-Auth	IPSecトンネルのX-Authの役割を「サーバー」、「クライアント」または「なし」から選択します。 ◆サーバー：、X-Authサーバーになります。X-Authアカウントボタンをクリックして、リモートX-Authクライアントアカウントを作成します。 ◆クライアント；このゲートウェイは、X-Authクライアントになります。X-Authサーバーゲートウェイによって認証されるユーザー名とパスワードを指定します。 ◆なし：：X-Auth認証は無効です。
デッドピア検出（DPD）	［有効］にチェックを入れて、DPD機能を有効します。タイムアウトおよび

項目	説明
	遅延時間を0～999秒の範囲で指定します。
フェーズ 1 キーライフタイム	フェーズ1キーライフタイムを30～86400秒の範囲で指定します。

10.1.1.7. IKE プロポーザル定義

項目	説明
暗号化	IKE（フェーズ１）の暗号化方式を「DES」、「3DES」、「AES-auto」、「AES-128」、「AES-192」または「AES-256」から選択します。
認証	認証時の暗号化方法を「なし」、「MD5」、「SHA1」または「SHA2-256」から選択します。
DH グループ	DH（Diffie-Hellman）グループを選択します。
定義	［有効］にチェックを入れると、このIKEプロポーザルが有効になります。

10.1.1.8. IPSec フェーズ設定



項目	説明
フェーズ 2 キーライフタイム	フェーズ2キーライフタイムを86400秒以内で指定します。

10.1.1.9. IPSec プロポーザル定義

項目	説明
暗号化	IPSecデータ通信の暗号化方式を「なし」、「DES」、「3DES」、「AES-auto」、「AES-128」、「AES-192」または「AES-256」から選択します。「なし」はカプセル化プロトコルが「AH」の場合のみ使用できます。
認証	認証時の暗号化方法を「なし」、「MD5」、「SHA1」または「SHA2-256」から選択します。「なし」および「SHA2-256」はカプセル化プロトコルが「ESP」の場合のみ使用できます。

項目	説明
PFS グループ	PFS（Perfect Forward Security）グループを選択します。
定義	［有効］にチェックを入れると、このIPSecプロポーザルが有効になります。

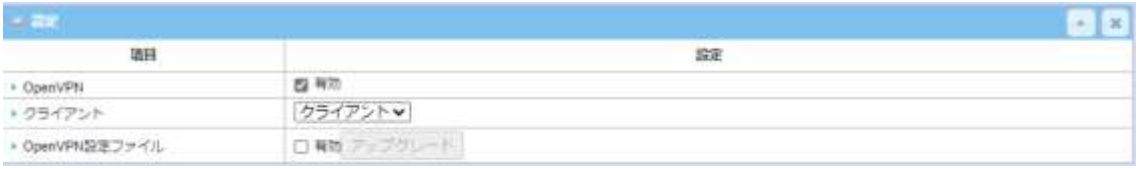
◆ 保存ボタンをクリックして、ルールを登録します。設定したルールが［IPSec トンネルリスト］に表示されます。

10. 1. 2. OpenVPN

OpenVPN は、事前共有キーまたは証明書を使って、お互いに認証しトネリングを構築します。また、サーバー＆クライアント形式のトネリング技術であり、本製品はクライアントのみサポートしています。加えて、OpenVPN は「TAP：レイヤ3レベル」と「TUN：レイヤ2レベル」の２つのトネリングモードに対応しています。

10.1.2.1. OpenVPN の設定

◆画面左側のメニューから、セキュリティ⇒VPN⇒OpenVPN の順にクリックします。



項目	説明
OpenVPN	[有効]にチェックを入れると、OpenVPNが有効になります。
クライアント	本製品はクライアントのみサポートしています。
OpenVPN 設定ファイル	[有効]にチェックを入れると、事前設定ファイルからのクライアント起動が有効になります。アップグレードボタンをクリックして、新規事前設定ファイルをアップロードすることができます。 （注）本機能を有効にすると、クライアントルールの設定ができなくなります。

◆保存ボタンをクリックして、設定を登録します。

10.1.2.2. OpenVPN クライアントリストの追加/編集

◆追加または編集ボタンをクリックすると、[OpenVPN クライアント構成]画面が表示されます。

項目	説明
OpenVPN クライアント名	識別のため32文字以下のクライアント名を指定します。
インターフェイス	OpenVPNクライアントトンネルを確立するインターフェイスを選択します。
プロトコル	OpenVPNクライアントの制御プロトコルを「UDP」または「TCP」から選択し、必要があればポート番号も指定します。 ◆TCP：OpenVPNはTCPプロトコル（ポート番号443自動設定）を使用します。 ◆UDP：OpenVPNはUDPプロトコル（ポート番号1194自動設定）を使用します。
トンネルシナリオ	OpenVPNが使用するトンネルシナリオを「TUN」または「TAP」から選択します。
リモート IP/FQDN	OpenVPNサーバーのIPアドレスまたはFQDNを指定します。
リモートサブネット	OpenVPAサーバーのサブネットとサブネットマスクを指定します。
リダイレクトインターネットトラフィック	[有効]にチェックを入れると、リダイレクトインターネットトラフィック機能が有効になります。
NAT	[有効]にチェックを入れると、NAT機能が有効になります。
認証モード	認証モードを「TLS」または「静的キー」から選択します。 ◆TLS：OpenVPNはTLS認証モードを使用し、CA証明書、クライアント証明書を使用します。 ◆静的キー：OpenVPNは静的キー認証モードを使用し、ローカルエンド

項目	説明
	ポイントIPアドレス、リモートエンドポイントIPアドレス、静的キーの項目が表示されます。
ローカルエンドポイント IP アドレス	OpenVPNゲートウェイのローカルエンドポイントIPアドレスを指定します。この項目は認証モードで「静的キー」を選択した時のみ利用可能です。
リモートエンドポイント IP アドレス	リモートOpenVPNゲートウェイのリモートエンドポイントIPアドレスを指定します。この項目は認証モードで「静的キー」を選択した時のみ利用可能です。
静的キー	静的キーを指定します。この項目は認証モードで「静的キー」を選択した時のみ利用可能です。
暗号化方法	暗号化方法を「Blowfish」、「AES-256」、「AES-192」、「AES-128」または「なし」から選択します。
ハッシュ・アルゴリズム	ハッシュ・アルゴリズム「SHA-1」、「MD5」、「MD4」、「SHA2-256」、「SHA2-512」、「なし」または「無効」から選択します。
LZO 圧縮	LZO圧縮方法を「適応」、「はい」、「いいえ」または「デフォルト」から選択します。
Persist キー	[有効]にチェックを入れると、Persistキー機能が有効になります。
Persist トンネル	[有効]にチェックを入れると、Persistトンネル機能が有効になります。
詳細構成	必要に応じて、編集をクリックすると詳細構成画面が表示されます。
トンネル	[有効]にチェックを入れると、本ルールが有効になります。

◆詳細構成を設定変更しない場合は、保存ボタンをクリックして、設定を登録します。登録されると[OpenVPN クライアントリスト]にルールが表示されます。詳細構成の設定変更する場合は、OpenVPN クライアント詳細構成に進みます。

10.1.2.3. OpenVPN クライアント詳細構成

項目	説明
TLS Cipher	TLS暗号方式を「なし」、「TLS-RSA-WITH-RC4-MD5」、「TLS-RSA-WITH-AES128-SHA」、「TLS-RSA-WITH-AES256-SHA」、「TLS-DHE-DSS-AES128-SHA」または「LS-DHE-DSS-AES256-SHA」から選択します。TLS暗号は、認証モードでTLSが選択されている場合のみ有効になります。
TLS Auth.キー（選択的）	OpenVPNサーバーTLS認証を要求している場合に、接続するためのキーを指定します。認証モードでTLSが選択されている場合のみ有効になります。
ユーザー名(選択的)	OpenVPNサーバー要求するユーザー名を指定します。認証モードでTLSが選択されている場合のみ有効になります。
パスワード（選択的）	OpenVPNサーバー要求するユーザー名を指定します。認証モードでTLSが選択されている場合のみ有効になります。
TAP のブリッジ先	TAPトンネルシナリオでTAPインターフェイスを選択します。この機能により、ローカルネットワーク側へブリッジ接続されます。トンネルシナリオでTAPが選択され、NATが無効のとき利用可能となります。
ファイアウォール保護	[有効]にチェックを入れると、ファイアウォール保護機能が有効になります。本機能はNATが有効の時のみ利用可能です。
クライアント IP アドレス	OpenVPNクライアントの仮想IPアドレスの付与方法を「動的IP」または「静的IP」から選択します。「静的IP」を選択した時は、仮想IPアドレスとそのサブネットマスクを指定します。
トンネル MTU	トンネルを通過させるパケットのMTUを100～1500の間で指定します。
トンネルの UDP 断片化	トンネルのUDP断片化（フラグメント）時のパケットサイズを0～1500の範囲で指定します。プロトコルで"UDP"が選択されているときのみ利用できます。
トンネル UDP MSS-Fix	[有効]にチェックを入れると、トンネルUDP MSS-Fix機能が有効になります。プロトコルで"UDP"が選択されているときのみ利用できます。
nsCerType 検証	[有効]にチェックを入れると、nsCerType検証が有効になります。認証モードでTLSが選択されている場合のみ有効になります。
TLS 再ネゴシエーション間隔	TLS再ネゴシエーションの時間間隔を1～86400（秒）の範囲で指定します。
接続再試行	接続再試行の時間間隔を1～86400（秒）の範囲で指定します。 1以下は接続再試行が必要ないことを意味します。

項目	説明
DNS	DNSの方法を「自動」または「手動」から選択します。「手動」選択した場合は、プライマリおよびセカンダリDNSを手動で指定します。
追加構成	オプションの設定文字列（最大256文字まで）をここに入力します。

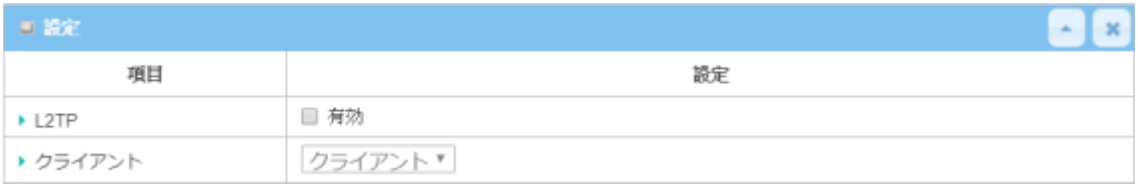
◆ 保存ボタンをクリックして、設定を登録します。登録されると[OpenVPN クライアントリスト]にルールが表示されます。

10.1.3. L2TP

Layer 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、または ISP によるサービスの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。 それ自体は暗号化や機密性を提供しません。 むしろ、プライバシーを提供するためにトンネル内を通過する暗号化プロトコルに依存しています。 本製品は、L2TPVPN トンネルの L2TP クライアントとしてのみ動作できます。

10.1.3.1. L2TP の設定

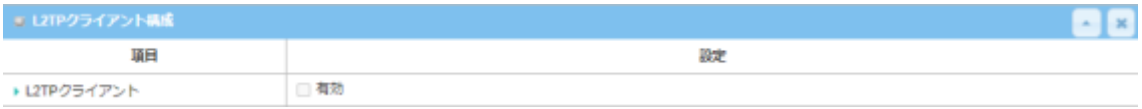
◆画面左側のメニューから、セキュリティ⇒VPN⇒L2TP の順にクリックします。



項目	説明
L2TP	[有効]にチェックを入れると、L2TPトネリングが有効になります。
クライアント	本製品はクライアントのみサポートしています。

◆保存ボタンをクリックして、設定を登録します。

10.1.3.2. L2TP クライアントの設定

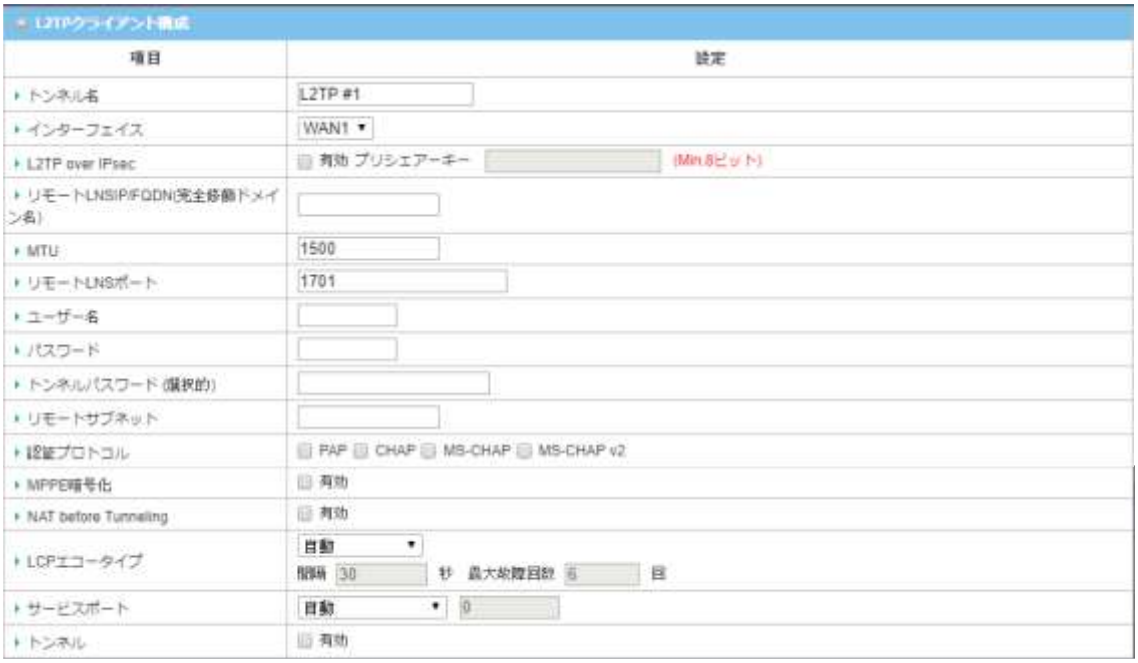


項目	説明
L2TP クライアント	[有効]にチェックを入れると、L2TPクライアント設定が有効になります。

◆保存ボタンをクリックして、設定を登録します。

10.1.3.3. L2TP クライアントリストの追加/編集

◆追加または編集ボタンをクリックすると、[L2TP クライアント構成]画面が表示されます。



項目	説明
トンネル名	識別のため32文字以下のトンネル名を指定します。
インターフェイス	L2TPトンネルを確立するインターフェイスを「WAN」または「LAN」から選択します。「WAN-1」しか選択できない場合があります。
MTU	L2TPトンネルを通過させるパケットのMTUを64～1500の間で指定します。
L2TP over IPSec	[有効]にチェックを入れると、L2TP over IPSecモード(IPSecによる暗号化)を有効にします。有効にした場合は文字長8～32のプレシェアキーを指定します。
リモート LNS IP/FQDN	L2TPサーバーのIPアドレスまたはFQDNを入力します。
リモート LNS ポート	L2TPトンネルのリモートLNSポートを1～65535の範囲で指定します。通常は“1701”を使用します。
ユーザー名	L2TPサーバーに接続するためのユーザー名(32文字以下)を指定します。
パスワード	L2TPサーバーに接続するためのパスワードを指定します。
トンネリングパスワード	L2TPサーバーの要求など必要があれば、L2TPトネリング用のトネリングパスワードを指定します。
リモートサブネット	リモートサブネットをIPアドレス/ネットマスク(例:192.168.123.100/24)のフォーマットで指定します。0.0.0.0/0を指定するとL2TPトンネルがデフォルトゲートウェイとして扱われ、全てのパケットはL2TPトンネルを通過するようになります。
認証プロトコル	L2TP接続に使用する認証プロトコルを「PAP」、「CHAP」、「MS-CHAP」および「MS-CHAR v2」から指定します。複数の認証プロトコルを指定すること

項目	説明
	ができます。
MPPE 暗号化	[有効]にチェックをすると、L2TP接続用のMPPE(Microsoft Point-to-Point Encryption)セキュリティが有効になります。L2TPサーバーが対応しているときのみ有効にしてください。MPPE暗号化が有効の場合、認証プロトコルPAP/CHAPは使用できません。
NAT before Tunneling	[有効]にチェックをすると、L2TPトンネルを通過する前にNAT機能によるアドレス変換が有効になります。
LCP エコータイプ	L2TPトンネルのLCPエコータイプを以下から選択します。 ◆自動:自動的に間隔および最大故障回数を指定します ◆ユーザー定義:間隔(1～99,999秒)および最大故障回数(1～999回)の範囲で指定します。 ◆無効:LCPエコーは無効です。
サービスポート	L2TPトネリングのサービスポートを以下から選択し、必要があればサービスポートを指定します。 ◆自動:自動的にサービスポートを割り振ります。 ◆1701 (for Cisco):CISCO L2TPサーバー接続時に選択します。 ◆ユーザー定義:1～65535の範囲の任意のポート番号を指定します。
トンネル	[有効]ボックスをチェックすると、本ルールが有効になります。

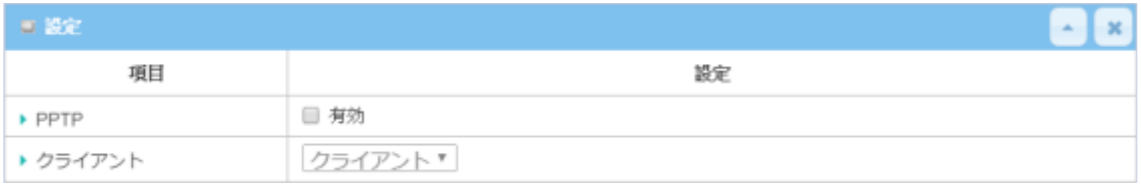
◆ 保存ボタンをクリックして、ルールを登録します。設定したルールが[L2TP クライアントリスト]に表示されます。

10.1.4. PPTP

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(VPN)を構築するトネリング技術です。 PPTP は、TCP を介した制御チャネルと、PPP パケットをカプセル化するために動作する GRE トンネルを使用します。 PPTP トンネリングにはさまざまなレベルの認証と暗号化があり、通常は WindowsPPTP スタックの標準機能としてネイティブに使用されます。本機は、PPTPVPN トンネルの PPTP クライアントとしてのみ動作します。PPTP トンネルプロセスは L2TP とほぼ同じです。

10.1.4.1. PPTP の設定

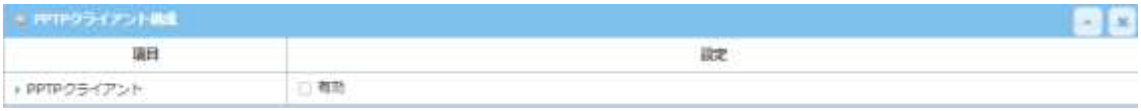
◆画面左側のメニューから、セキュリティ⇒VPN⇒PPTP の順にクリックします。



項目	説明
PPTP	[有効]にチェックを入れると、PPTPトネリングが有効になります。
クライアント	本製品はクライアントのみサポートしています。

◆保存ボタンをクリックして、設定を登録します。

10.1.4.2. PPTP クライアントの設定



項目	説明
PPTP クライアント	[有効]にチェックを入れると、PPTPクライアント設定が有効になります。

◆保存ボタンをクリックして、設定を登録します。

10.1.4.3. PPTP クライアントリストの追加/編集

◆追加または編集ボタンをクリックすると、[PPTP クライアント構成]画面が表示されます。

項目	説明
トンネル名	識別のため32文字以下のトンネル名を指定します。
インターフェイス	PPTPトンネルを確立するインターフェイスを「WAN」または「LAN」から選択します。「WAN-1」しか選択できない場合があります。
リモート IP/FQDN	PPTPサーバーのIPアドレスまたはFQDNを入力します。
MTU	PPTPトンネルを通過させるパケットのMTUを64～1500の間で指定します。
ユーザー名	PPTPサーバーに接続するためのユーザー名（32文字以下）を指定します。
パスワード	PPTPサーバーに接続するためのパスワードを指定します。
リモートサブネット	リモートサブネットをIPアドレス/ネットマスク（例：192.168.123.100/24）のフォーマットで指定します。0.0.0.0/0を指定するとL2TPトンネルがデフォルトゲートウェイとして扱われ、全てのパケットはPPTPトンネルを通過するようになります。
認証プロトコル	PPTP接続に使用する認証プロトコルを「PAP」、「CHAP」、「MS-CHAP」および「MS-CHAR v2」から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、PPTP接続用のMPPE（Microsoft Point-to-Point Encryption）セキュリティが有効になります。L2TPサーバーが対応していると

項目	説明
	きのみ有効にしてください。MPPE暗号化が有効の場合、認証プロトコルPAP/CHAPは使用できません。
NAT before Tunneling	[有効]にチェックをすると、PPTPトンネルを通過する前にNAT機能によるアドレス変換が有効になります。
LCP エコータイプ	PPTPトンネルのLCPエコータイプを以下から選択します。 ◆自動:自動的に間隔および最大故障回数を指定します ◆ユーザー定義:間隔(1～99,999秒)および最大故障回数(1～999回)の範囲で指定します。 ◆無効:LCPエコーは無効です。
トンネル	[有効]ボックスをチェックすると、本ルールが有効になります。

◆保存ボタンをクリックして、ルールを登録します。設定したルールが[PPTP クライアントリスト]に表示されます。

10.1.5. GRE

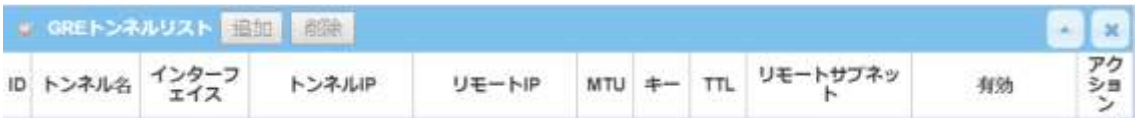
Generic Routing Encapsulation（GRE）は、シスコシステムズによって開発されたトンネリングプロトコルで、インターネットを介した仮想ポイントツーポイントリンク内に多種多様なネットワーク層プロトコルをカプセル化します。

10.1.5.1. GRE の設定

◆画面左側のメニューから、セキュリティ⇒VPN⇒GRE の順にクリックします。

項目	説明
GRE	[有効]にチェックを入れると、GREトネリングが有効になります。
最大同時 GRE トンネル	本機の場合、32です。

10.1.5.2. GRE トンネルの追加/編集



◆追加または編集ボタンをクリックすると、[GRE ルール構成]画面が表示されます。

項目	説明
トンネル名	識別のためのトンネル名（9文字以下）を指定します。
インターフェイス	GREトンネルを確立するインターフェイスを「WAN」または「LAN」から選択します。「WAN-1」しか選択できない場合があります。

項目	説明
トンネル IP	トンネルを通すIPアドレスサブネットを指定し、サブネットマスクを選択します。
リモート IP	リモートGREトンネルゲートウェイのIPアドレスを指定します。通常、リモートGREゲートウェイのグローバルIPアドレス（パブリックIPアドレス）と同一です。
MTU	GREトンネルを通過させるパケットのMTUを64～1500の間で指定します。
キー	GREの接続キーを0～999,999,999の範囲で指定します.。 キーは空欄のままでも構いません。
TTL	GREトンネルのTTLホップカウント値を1～255の範囲で指定します。
リモートサブネット	GREトンネル先のリモートサブネットをIPアドレス/ネットマスク（例：192.168.123.100/24）のフォーマットで指定します。
トンネル	[有効]ボックスをチェックすると、本ルールが有効になります。

◆ 保存ボタンをクリックして、ルールを登録します。設定したルールが[GRE トンネルリスト]に表示されます。

10.2. ファイヤーウォール

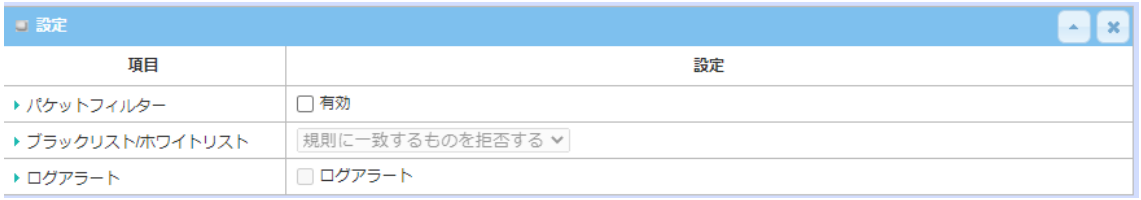
ファイアウォール機能には、パケットフィルタ、URL ブロッキング、コンテンツフィルタ、MAC 制御、アプリケーションフィルタ、IPS、およびいくつかのファイアウォールオプションが含まれます。

10.2.1. パケットフィルター

パケットフィルタ機能により、着信パケットと発信パケットの通過許可またはブロッキングによるフィルタリングを行うことができます。

◆画面左側のメニューから、セキュリティ⇒ファイヤーウォール⇒パケットフィルターの順にクリックします。

10.2.1.1. パケットフィルター設定



項目	説明
パケットフィルター	[有効]にチェックを入れると、パケットフィルター機能が有効になります。
ブラックリスト/ ホワイトリスト	フィルタリングのモードを以下から選択します。 ◆規則に一致するものを拒否する(ブラックリスト):フィルタリングルールと一致するものをブロックします。 ◆規則に一致するものを許可する(ホワイトリスト):フィルタリングルールと一致するもののみ許可します。
ログアラート	[有効]ボックスにチェックを入れると、イベントログが有効になります。

◆保存ボタンをクリックして設定を保存します。必要があれば、パケットフィルタルールの追加/編集に移行します。

10.2.1.2. パケットフィルタルールの追加/編集

パケットフィルタのルールを登録します。ルールは 20 ルールまで登録できます。

◆追加または編集ボタンをクリックすると、[パケットフィルタ規則構成]画面が表示されます。

項目	説明
ルール名	識別のためのパケットフィルタルール名（30 文字以内）を指定します。
入力インターフェース	パケットの入力インタフェイスを「任意」、「LAN」または「WAN」から選択します。全てのインタフェイスに対してもフィルタリングする場合は「任意」を選択します。
出力インターフェース	パケットの出力インタフェイスを「任意」、「LAN」または「WAN」から選択します。全てのインタフェイスに対してもフィルタリングする場合は「任意」を選択します。
送信元 IP アドレス	フィルタリングパケットを送信する IP アドレスを指定します。 ◆任意：全ての送信元 IP アドレスがフィルタされます。 ◆特定の IP アドレス：特定の IP アドレスからのパケットをフィルタします。 ◆IP 範囲：特定範囲の IP アドレスからのパケットをフィルタします。
宛先 IP アドレス	フィルタリングパケットの宛先 IP アドレスを指定します。 ◆任意：全ての宛先 IP アドレスがフィルタされます。 ◆特定の IP アドレス：特定の宛先 IP アドレスへのパケットをフィルタします。 ◆IP 範囲：特定範囲の宛先 IP アドレスへのパケットをフィルタします。

項目	説明
Source MAC	送信元の MAC アドレスを指定します。 ◆任意：全ての送信元 MAC アドレスがフィルタされます。 ◆Static MAC Address：特定の送信元MACアドレスのパケットをフィルタします。
プロトコル	フィルタリングを行うプロトコルを選択します。 ICMPv4、UDP、TCP、GRE、ESP、SCTP およびユーザー定義が選択できます。選択項目右の（）内の数字は IP プロトコル番号を表しています。ユーザー定義は任意の IP プロトコル番号を指定します。任意を選択すると全てのプロトコルでフィルタされます。
送信元ポート	プロトコルでTCP，UDP、任意を指定したときに送信元サービスポート番号を指定します。 ◆既知のサービス：よく使われるプロトコルから一つを選択します。 ◆ユーザー定義サービス：任意の TCP ポート番号を範囲で指定します。
宛先ポート	プロトコルでTCP，UDP、任意を指定したときに宛先サービスポート番号を指定します。 ◆既知のサービス：よく使われるプロトコルから一つを選択します。 ◆ユーザー定義サービス：任意の TCP ポート番号を範囲で指定します。
Protocol Number	プロトコルでユーザー定義を選択したときに特定の Protocol Number（ポート番号）を指定します。
時間スケジュール	本フィルタリングルールが有効になる時間スケジュールを指定します。 常時(0)または「スケジュール設定」で定義されたスケジュールリストから選択できます。
ルール	［有効］ボックスをチェックすると、本ルールが有効になります。

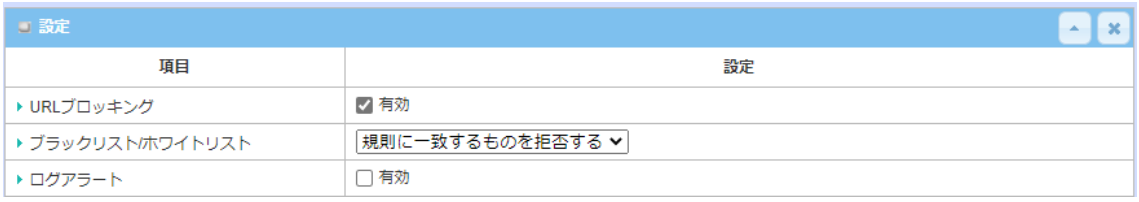
◆ 保存ボタンをクリックして、ルールを登録します。設定したルールが［パケットフィルタ］に表示されます。

10. 2. 2. URL ブロッキング

URL ブロッキング機能により、着信 Web 要求と発信 Web 要求パケットの通過許可またはブロッキングによるフィルタリングを行うことができます。完全な URL のみでなく、部分的なドメイン名やキーワードによるフィルタリングも可能です。

◆画面左側のメニューから、セキュリティ⇒ファイヤーウォール⇒URL ブロッキングの順にクリックします。

10.2.2.1. URL ブロッキング設定



項目	説明
URL ブロッキング	[有効]にチェックを入れると、URLブロッキング機能が有効になります。
ブラックリスト/ ホワイトリスト	URLブロッキングのモードを以下から選択します。 ◆規則に一致するものを拒否する(ブラックリスト):URLブロッキングルールと一致するものをブロックします。 ◆規則に一致するものを許可する(ホワイトリスト):URLブロッキングルールと一致するもののみ許可します。
ログアラート	[有効]ボックスにチェックを入れると、イベントログが有効になります。

◆保存ボタンをクリックして設定を保存します。必要があれば、URL ブロッキングルールの追加/編集に移行します。

10.2.2.2. URL ブロッキングルールの追加/編集

URL ブロッキングのルールを登録します。ルールは 20 ルールまで登録できます。

◆追加または編集ボタンをクリックすると、[URL ブロッキングルール構成]画面が表示されます。

項目	説明
ルール名	識別のための URL ブロッキングルール名（30 文字以内）を指定します。
送信元 IP アドレス	Web 要求を送信する IP アドレスを指定します。 ◆任意：全ての送信元 IP アドレスがフィルタされます。 ◆特定の IP アドレス：特定の IP アドレスからのパケットをフィルタします。 ◆IP 範囲：特定範囲の IP アドレスからのパケットをフィルタします。
Source MAC	送信元の MAC アドレスを指定します。 ◆任意：全ての送信元 MAC アドレスがフィルタされます。 ◆Static MAC Address：特定の送信元MACアドレスのパケットをフィルタします。
URL/ドメイン名/ キーワード	検査する「完全な URL」、「一部のドメイン名」または「一部のキーワード」を指定します。 条件一致した場合の通過許可かブロックかは、ブラックリスト/ホワイトリストの設定に依存します。
宛先ポート	宛先サービスポート番号を指定します。 ◆任意：全てのポート番号がブロッキングの対象になります。 ◆特定のサービスポート：ブロッキング対象の特定のサービスポート番号を指定します。 ◆ポート範囲：ブロッキング対象の特定のサービスポート番号を範囲で指定します。

項目	説明
時間スケジュール	本フィルタリングルールが有効になる時間スケジュールを指定します。 常時(0)または「スケジュール設定」で定義されたスケジュールリストから選択できます。
ルール	[有効]ボックスをチェックすると、本ルールが有効になります。

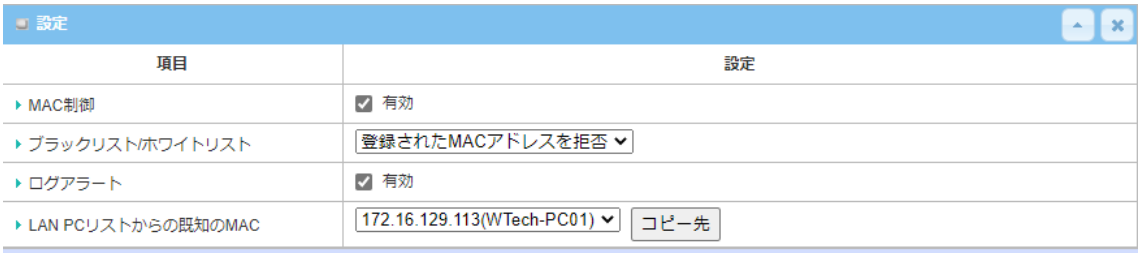
◆保存ボタンをクリックして、ルールを登録します。設定したルールが[URL ブロッキングルール]に表示されます。

10. 2. 3. MAC 制御

MAC 制御機能により、ネットワークにつながるユーザー毎でのパケットの通過許可またはブロッキングによるフィルタリングを行うことができます。管理者が特定の MAC アドレスのクライアントホストからの通信を拒否したい場合は、「MAC 制御」機能を使用してブラックリスト構成で拒否できます。

◆画面左側のメニューから、セキュリティ⇒ファイヤーウォール⇒MAC 制御の順にクリックします。

10.2.3.1. MAC 制御設定

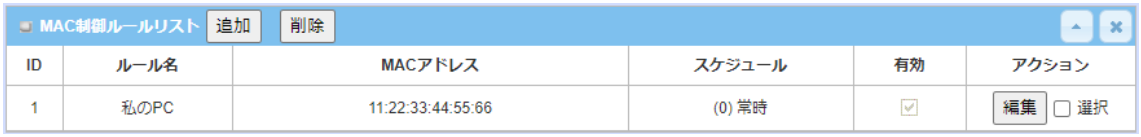


項目	説明
MAC 制御	[有効]にチェックを入れると、MAC制御機能が有効になります。
ブラックリスト/ ホワイトリスト	URLブロッキングのモードを以下から選択します。 ◆登録されたMACアドレスを拒否する(ブラックリスト):MAC制御ルールと一致するものをブロックします。 ◆登録されたMACアドレスを許可する(ホワイトリスト):MAC制御ルールと一致するもののみ許可します。
ログアラート	[有効]ボックスにチェックを入れると、イベントログが有効になります。
LAN PC リストからの既知の MAC	LAN クライアントリストから MAC アドレスを選択します。コピー先をクリックして、選択した MAC アドレスを MAC 制御ルールにコピーします。

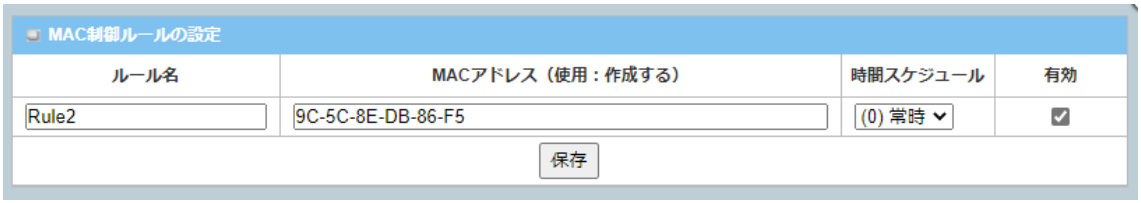
◆保存ボタンをクリックして設定を保存します。必要があれば、MAC 制御ルールリストの追加/編集に移行します。

10.2.3.2. MAC 制御ルールリストの追加/編集

MAC 制御ルールを登録します。ルールは 20 ルールまで登録できます。



◆追加または編集ボタンをクリックすると、[MAC 制御ルールの設定]画面が表示されます。



項目	説明
ルール名	識別のためのMAC制御ルール名（30 文字以内）を指定します。
MAC アドレス	ルールを適用する発信元 MAC アドレスを指定します。
時間スケジュール	本フィルタリングルールが有効になる時間スケジュールを指定します。 常時(0)または「スケジュール設定」で定義されたスケジュールリストから選択できます。
有効	[有効]ボックスをチェックすると、本ルールが有効になります。

◆保存ボタンをクリックして、ルールを登録します。設定したルールが[MAC 制御ルールリスト]に表示されます。

10. 2. 4. IPS

IPS(侵入防止システム)は、ネットワークやシステムで悪意のあるアクセスが実行されていないか監視するネットワークセキュリティ機能です。IPS の主な機能は、悪意のあるアクセスを特定すること、そのアクセスに関する情報を記録すること、およびそのアクセスをブロック/停止して報告することです。必要があれば、IPS 機能を有効にして、リストの侵入アクセスが存在しないか確認することができます。また、ログ警告を有効にすると、該当する侵入が検出された場合に侵入イベントが記録されます。

◆画面左側のメニューから、セキュリティ⇒ファイヤーウォール⇒IPS の順にクリックします。

10.2.4.1. IPS 設定

項目	説明
IPS	[有効]にチェックを入れると、IPS(侵入防止システム)機能が有効になります。
ログアラート	[有効]ボックスにチェックを入れると、イベントログが有効になります。

◆保存ボタンをクリックして設定を保存します。必要があれば、侵入防止機能設定に移行します。

10.2.4.2. 侵入防止機能設定

有効にする侵入防止システムを選択することができます。侵入防止機能はIPSが有効でなければ設定できません。

項目	説明
SYN フラッド防御	[有効]にチェックすると、SYN フラッド防御が有効になります。 トラフィックのしきい値を 10～10000（パケット/秒）の範囲で指定します。
UDP フラッド防御	[有効]にチェックすると、UDP フラッド防御が有効になります。 トラフィックのしきい値を 10～10000（パケット/秒）の範囲で指定します。
ICMP フラッド防御	[有効]にチェックすると、ICMP フラッド防御が有効になります。 トラフィックのしきい値を 10～10000（パケット/秒）の範囲で指定します。
ポートスキャン防御	[有効]にチェックすると、ポートスキャン防御が有効になります。 トラフィックのしきい値を 10～10000（パケット/秒）の範囲で指定します。
Land Attack のブロック	[有効]にチェックすると、各侵入防止ブロック機能が有効になります。
Ping of Death のブロック	
IP Spoof のブロック	
TCP Flag Scan のブロック	
Smurf のブロック	
Traceroute のブロック	
Fraggle Attack のブロック	
ARP スプーフィング防御	[有効]にチェックすると、ARP スプーフィング防御が有効になります。 トラフィックのしきい値を 10～10000（パケット/秒）の範囲で指定します。

◆保存ボタンをクリックして設定を保存します。

10.2.5. オプション

その他のオプション機能としてステルスモード、SPI などのファイアウォールオプションが使用できます。「ステルスモード」を使用すると、WAN からのポートスキャンに応答しないため、インターネットでの検出や攻撃の影響を受けにくくなります。「SPI」を使用すると、IP アドレス、ポートアドレス、ACK、SEQ 番号などのパケット情報がゲートウェイ（ルーター）を通過するときに記録し、ゲすべての受信パケットをチェックし、パケットの有効性を検査します。

◆画面左側のメニューから、セキュリティ⇒ファイアウォール⇒オプションの順にクリックします。

10.2.5.1. ファイアウォールオプション設定

項目	説明
ステルスモード	[有効]にチェックを入れると、ステルスモード機能が有効になります。
SPI	[有効]にチェックを入れると、SPI機能が有効になります。
WAN からの Ping パケットを破棄する	[有効]にチェックを入れると、WAN からの PING に応答しなくなります。

◆保存ボタンをクリックして設定を保存します。必要があれば、リモート管理者ホスト定義に移行します。

10.2.5.2. リモート管理者ホスト定義の編集

WAN から本機にアクセスできる管理者ホストを 5 つ設定できます。

◆編集ボタンをクリックするとモート管理者ホスト定義の該当 ID のホスト設定が編集できるようになります。

項目	説明
インターフェイス	常に「All WAN」です。
プロトコル	WebGUI アクセスプロトコルを「HTTP」または「HTTPS」より選択します。
IP	管理ホストのIPアドレスを指定します。 ◆任意の IP アドレス：管理ホストIPをチェックしません。 ◆特定の IP アドレス：管理ホスト IP をチェックします。
サブネットマスク	IP で「特定のIPアドレス」を選択した場合、管理ホストネットワークのサブネットを選択します。
サービスポート	HTTP または HTTPS のサービスポートを指定します。ユーザー任意のポートを割り振ることも可能です。
有効	[有効]にチェックを入れると、この管理者が WAN より本機にアクセスできるようになります。

◆保存ボタンをクリックして設定を保存します。

11. 管理(Administration)

11.1. 設定と管理 （本機ではサポートしておりません）

（注１） ハイテクインター株式会社のサポートで使用することがあります。コマンドなどの詳細資料の提供は致しておりません。

11.1.1. コマンドスクリプト

この機能はサポートしておりません。

11.1.2. TR-069

この機能はサポートしておりません。

11.1.3. SNMP

この機能はサポートしておりません。

11.1.4. Telnet & SSH

この機能はサポートしておりません。

11.2. システム管理

システム管理により、ネットワーク管理者は、Web ベースのユーティリティアクセスパスワードの変更、システム情報、システム時刻、システムログ、ファームウェア/設定のバックアップと復元、リセットおよび再起動などのシステム設定を管理することができます。

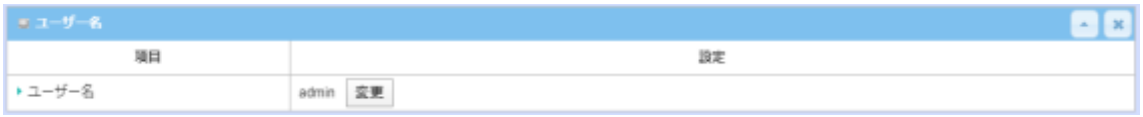
11.2.1. パスワード及び MMI

1) 画面左側のメニューから、管理(Administration)⇒システム管理⇒パスワード＆MMIの順にクリックします。

11.2.1.1. ホスト名の設定

項目	説明
ホスト名	本機のホスト名を設定します。保存ボタンをクリックして登録します。

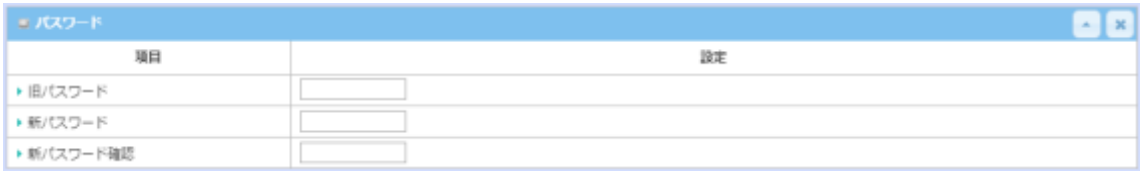
11.2.1.2. ユーザ名の変更



項目	説明
ユーザ名(注 1)	変更ボタンをクリックしてユーザ名の変更を行います。 [新しいユーザーネーム]を指定し、現在のパスワードを入力します。 保存ボタンで新しいユーザー名の変更登録をします。

（注 1） ユーザー名の変更を実施すると新ユーザー名による WebUI の認証が必要になります。

11.2.1.3. パスワードの変更



項目	説明
旧パスワード	現在のパスワードを入力します。

項目	説明
新パスワード	新しいパスワードを入力します。
新パスワード確認	確認のためもう一度新しいパスワードを入力します。
保存	保存ボタンをクリックして新パスワードを登録します。

11.2.1.4. MMI（マネージメントインターフェイス）の設定

本設定は管理者が HWL-3511-DS へ WebUI でアクセスするための管理情報を制御します。

項目	説明
ログイン	ログイン試行回数の上限を設定します。設定範囲は 3~10 回です。パスワードを間違えて、このカウントを超えたログイン試行を行った場合は、30 秒間はログイン試行がロックされます。
ログインタイムアウト	自動ログアウト機能の有効/無効と、自動ログアウトするまでの無操作監視秒数を設定します。設定範囲は 30~65535 秒です。
GUI アクセスプロトコル	GUI アクセスに使用するプロトコルを選択します。[http/https]、[http のみ]、[https のみ]の選択が可能です。
HTTPS 証明書のセットアップ	本機の WebUI 用証明書の詳細設定を行います。本設定は証明書リストを作成する必要があります。
HTTP 圧縮	http を圧縮したい場合に gzip および deflate にチェックをします。
HTTP バインディング	WebUI をバインドする DHCP サーバーを選択します。
システム起動モード	システム起動のモードを選択します。 [通常起動モード]:起動中にファームウエアイメージチェックを完全に実行します。起動時間は長くなります。 [早い起動モード]:起動中にファームウエアイメージチェックを実行しません。起動時間は約 5~10 秒程度短縮されます。
保存	保存ボタンをクリックして MMI 設定を登録します。

11.2.2. システム情報

システム情報画面では、ネットワーク管理者は HWL-3511-DS のデバイス情報をすばやく調べることができます。

1) 画面左側のメニューから、管理(Administration)⇒システム管理⇒システム情報の順にクリックします。

項目	説明
モデル名	本機のモデル名が表示されます。
デバイスのシリアル番号	ご使用製品のシリアル番号が表示されます。
カーネルバージョン	動作中の Linux カーネルバージョンが表示されます。
ファームウェアバージョン	動作中のファームウェアバージョンが表示されます。
システムタイム	この WebUI ページを閲覧したときのシステム時刻が表示されます。
デバイス稼働時間	起動(電源オンまたは再起動)からの稼働時間が表示されます。

2) 更新ボタンのクリックでシステムタイムが更新されます。

11.2.3. システムタイム

HWL-3511-DS はシステムが管理する時刻を合わせる方法を、[マニュアル]、[PC]、[タイムサーバー]および[セルラーモジュール]から選択することができます。

1) 画面左側のメニューから、管理（Administration）⇒システム管理⇒システムタイムの順にクリックします。

11.2.3.1. タイムサーバーと同期する

項目	説明
同期方法	[タイムサーバー]を選択します。
タイムゾーン	本機設置所在地のタイムゾーンを選択します。 所在地を直接選択するか、世界標準時間からのオフセット時間による指定も可能です。
オートシンクロ	利用可能な公開タイムサーバーをリストから選択します。独自タイムサーバーを利用する場合は、そのタイムサーバーの IP アドレスを指定します。
夏時間	日本国内では利用できません。チェックを外して[無効]に設定してください。
NTP サーバサービス	[有効]ボックスをチェックすると、本機に LAN や WiFi ネットワークでの NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
即時同期	アクティブボタンをクリックするとすぐに時刻同期を行います。
保存	保存ボタンをクリックして同期方式などの設定を保存します。

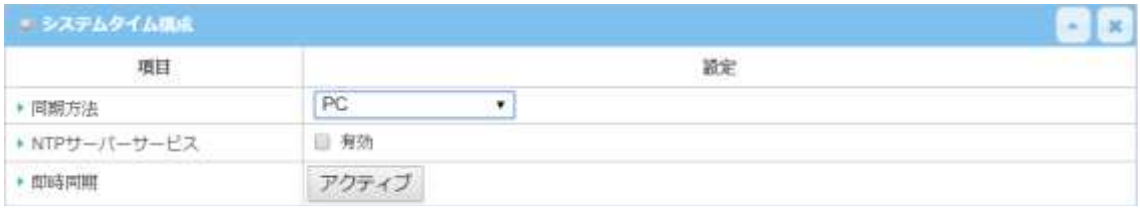
11.2.3.2. 手動でシステム時間を設定する

項目	説明
同期方法	[マニュアル]を選択します。
タイムゾーン	本機設置所在地のタイムゾーンを選択します。 所在地を直接選択するか、世界標準時間からのオフセット時間による指定も可能です。
夏時間	日本国内では利用できません。チェックを外して[無効]に設定してください。
日付と時刻を手動で設定する	現在の日付（年/月/日）と時刻を（時:分:秒）を入力します。
NTP サーバサービス	[有効]ボックスをチェックすると、本機に LAN や WiFi ネットワークでの NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
保存	保存ボタンをクリックして同期方式、時間設定を保存します。保存した時点から時計機能が動作します。

（注１） 内蔵の時計機能は日に数秒の誤差を持つことがあります。正確な時間が必要な場合は、時刻同期のある[タイムサーバー同期]をご利用ください。

11.2.3.3. PC と手動で同期をとる

WebUI で本機にアクセス中の PC と同期をとります。



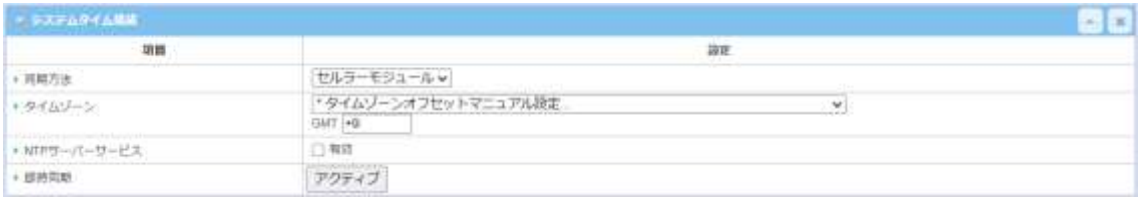
項目	説明
同期方法	[PC]を選択します。
NTP サーバサービス	[有効]ボックスをチェックすると、本機に LAN や WiFi ネットワークでの NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
即時同期	アクティブボタンをクリックすると、PC の時刻と即時に同期をとります。
保存	保存ボタンをクリックして時間設定を保存します。保存した時点から時計機能が動作します。

（注１） 内蔵の時計機能は日に数秒の誤差を持つことがあります。正確な時間が必要な場合は、時刻同期のある[タイムサーバー同期]をご利用ください。

11.2.3.4. 3G/4G 無線回線の時刻通知を利用して同期をとる

3G/4G 回線から時刻データを取得し同期することができます。

（注１） プライベート LTE や一部の回線事業者では正常に取得できないことがあります。



項目	説明
同期方法	[セルラーモジュール]を選択します。
タイムゾーン	本機設置所在地のタイムゾーンを選択します。 所在地を直接選択するか、世界標準時間からのオフセット時間による指定も可能です。
NTP サーバサービス	[有効]ボックスをチェックすると、本機に LAN や WiFi ネットワークでの NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
即時同期	アクティブボタンをクリックすると、PC の時刻と即時に同期をとります。

項目	説明
保存	保存ボタンをクリックして同期方式、時間設定を保存します。保存した時点から時計機能が動作します。

11.2.4. システムログ

システムログ画面には、ネットワーク管理者がローカルイベントロギングとリモートレポートを実行できるようにします。

（注１） 本機能はハイテクインター株式会社のサポート時のみに使用します。ログ内容などの詳細資料の提供は致しておりません。

1) 画面左側のメニューから、管理（Administration）⇒システム管理⇒システムログの順にクリックします。

11.2.4.1. 表示および E メールログ履歴

ネットワーク管理者が本機のログ履歴を WebUI 上に表示するためのビューボタンとインスタント E メールを分析用に送信する Email Now ボタンがあります。

項目	説明
ビュー	ビューボタンをクリックすると、[Web ログタイリスト]でログ履歴が表示されます。
Email Now(注 1)	Email Now ボタンをクリックすると、直ちに E メール経由でログ履歴を送信することができます。 ＜現在のところご使用できません。＞

（注１） E メールアラート項目で E メール送信に関する設定を行う必要があります。

Web ログリスト例

11.2.4.2. ログタイプカテゴリ

[システム]、[攻撃]、[ドロップ]、[ログインメッセージ]および[デバッグ]の項目をログ履歴として保管することができます。この項目は、Web ログ、Syslogd、ストレージそれぞれで有効/無効を設定できます

項目	説明
システム	システムイベントを記録します。
攻撃	攻撃イベントを記録します。
ドロップ	ドロップイベントを記録します。
ログインメッセージ	ログインイベントを記録します。
デバッグ	デバッグイベントを記録します。

11.2.4.3. E メールアラート

本機能はサポートしていません。

11.2.4.4. Syslogd

本機は選択したログイベントを Syslogd サーバーに送信することができます。

項目	説明
有効	[有効]ボックスにチェックを入れると Syslogd 機能が動作し、イベントログを Syslog サーバーに送信します。
サーバー	イベントログを送信する 1 台の syslog サーバーをサーバードロップダウンボックスから選択します。登録が無い場合は追加ボタンで追加します。
ログタイプカテゴリ	ログタイプカテゴリ項を参照してください。

11.2.4.5. ログの保管

本機は選択したログイベントを内部または外部のストレージに保存することができます。

項目	説明
有効	[有効]ボックスにチェックを入れると、ログ履歴のストレージへの保存を有効にします。
デバイスの選択	内部または外部ストレージを選択します。
ログファイル名	ストレージにログ履歴を保存するときのファイル名を指定します。
ファイル分割	[有効]ボックスにチェックを入れると、指定したファイルサイズに達する度にファイルを分割します。
間隔	[有効]ボックスにチェックを入れると、指定された時間間隔ごとにログをストレージに保存します。値の範囲は 1～10080 分です。
Max Records	保存できるイベント数を設定します。値の範囲は 5～10,000 イベントです。
ログファイルのダウンロード	ログファイルを PC にダウンロードします。ファイル形式は.tar です。
clear logs	一時保管中の Log 履歴をクリアします。
ログタイプカテゴリ	ログタイプカテゴリ項を参照してください。

11.2.5. バックアップ及び復元

新しいファームウェアが使用可能になったときにデバイスのファームウェアをアップグレードしたり、デバイス設定をバックアップ/復元したりすることができます。

1) 画面左側のメニューから、管理(Administration)⇒システム管理⇒バックアップおよび復元の順にクリックします。

項目	説明
FW アップグレード	ファイルを選択して、FW のアップグレードを行います。
バックアップ設定	バックアップファイルのダウンロード/アップロードを行います。
オートリストア設定	本機では、これらの機能はサポートしておりません。
ユーザ定義ロゴ	
ユーザ定義 CSS	

2) 保存ボタンをクリックして設定を登録します。

11.2.6. 再起動およびリセット

HWL-3511-DS を再起動したり、設定を工場出荷設定にリセットしたりすることができます。

◆画面左側のメニューから、管理（Administration）⇒システム管理⇒再起動およびリセットの順にクリックします。

項目	説明
再起動	タイミングを指定して、再起動ボタンをクリックして再起動を行います。[今すぐ]または[時間スケジュール]を設定できます。時間スケジュールはタイムスケジュールリストから選択できます。
デフォルト設定に戻す	設定リセットボタンをクリックして、設定を工場出荷設定に戻します。

（注１） 設定を初期設定に戻すと本機の LAN IP アドレスも初期化されるため、再度 WebGUI に初期時の IP アドレスでアクセスする必要があります。

11.3. 診断

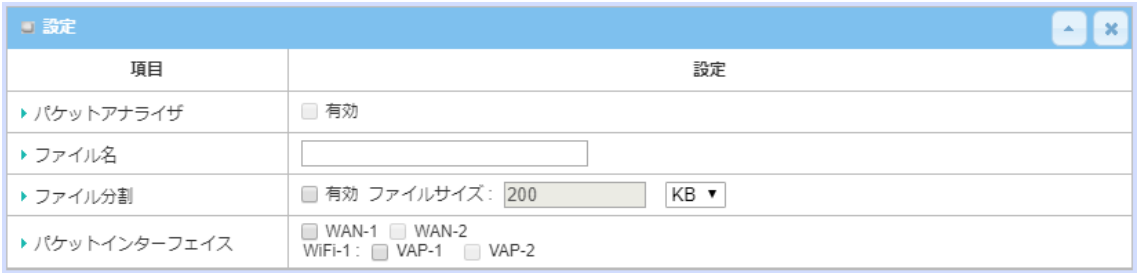
本機は、管理者が本機およびネットワークの異常原因のトラブルシューティングに利用できる簡単なネットワーク診断ツールを搭載しています。インターフェイスや特定の発信先/発信元ホスト（IP 機器）のデータパケットを記録する「パケットアナライザー」と、ネットワーク接続を PING やトレースルートで試験する「診断ツール」があります。

11.3.1. パケットアナライザ

パケットアナライザは、キャプチャやフィルタ条件ルールを設定することで、目的とするパケットをキャプチャすることができます。本機能はログストレージが使用可能でない場合動作しません。長時間にわたる場合は、SD カードメモリの利用を推奨します。

◆画面左側のメニューから、管理（Administration）⇒診断⇒パケットアナライザの順にクリックします。

11.3.1.1. 設定



項目	説明
パケットアナライザ	[有効]ボックスをクリックすると、パケットアナライザが有効になります。
ファイル名	ストレージに登録するファイル名を設定します。
ファイル分割	[有効]ボックスをクリックすると、ログファイル分割が有効になります。 分割ファイルサイズ：分割をするファイルサイズを指定します。値の範囲は 10～99,999 です。

項目	説明
	単位：“KB”または“MB”から選択します。
パケットインターフェイス	パケットアナライザが動作するインターフェイスを指定します。 WAN-1、WAN-2、VAP-1 および VAP-2 で有効にすることができます。

11.3.1.2. キャプチャとフィルタの条件

キャプチャとフィルタの条件を指定することにより、さらに細かいフィルタリングが可能になります。

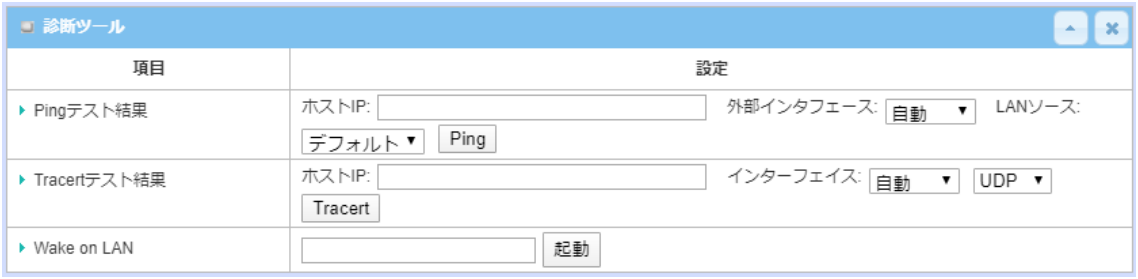
項目	説明
Filter	[有効]ボックスをクリックすると、フィルタ機能が有効になります。
ソース MAC	キャプチャするソース MAC アドレスを最大 10 個まで指定できます。 指定フォーマットは「11:22:33:44:55:66」です。 それぞれのソース MAC アドレスは「;」で区切ります。
ソース IP	キャプチャするソース IP アドレスを最大 10 個まで指定できます。 指定フォーマットは「192.168.123.254」の IPv4 形式です。 それぞれのソース IP アドレスは「;」で区切ります。
ソースポート	キャプチャするソースポート番号を最大 10 個まで指定できます。 値の範囲は 1～65535 です。 それぞれのポート番号は「;」で区切ります。
宛先 MAC	キャプチャする宛先 MAC アドレスを最大 10 個まで指定できます。 指定フォーマットは「11:22:33:44:55:66」です。 それぞれの宛先 MAC アドレスは「;」で区切ります。
宛先 IP	キャプチャする宛先 IP アドレスを最大 10 個まで指定できます。 指定フォーマットは「192.168.123.254」の IPv4 形式です。

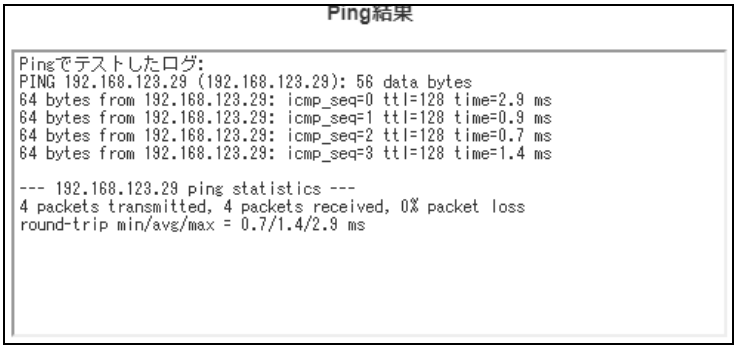
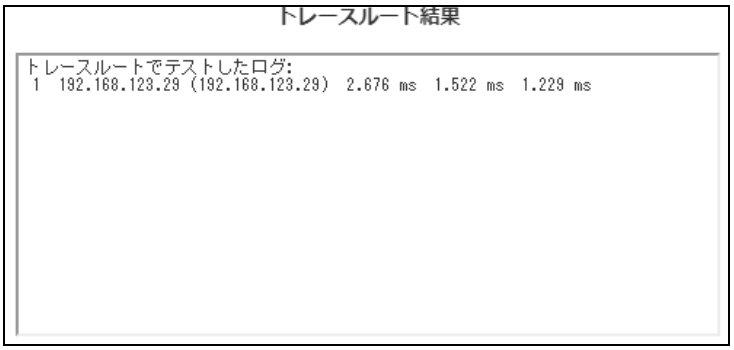
項目	説明
	それぞれの宛先 IP アドレスは「;」で区切ります。
宛先ポート	キャプチャする宛先ポート番号を最大 10 個まで指定できます。 値の範囲は 1～65535 です。 それぞれのポート番号は「;」で区切ります。

11.3.2. 診断ツール

管理者は診断ツールを使用することでネットワークの簡単な疎通確認のをすることができます。

◆画面左側のメニューから、管理(Administration)⇒診断⇒診断スールの順にクリックします。



項目	説明
Ping テスト結果	ホスト IP に宛先を入力し、Ping ボタンをクリックすることで、Ping テストを行うことが出来ます。 テスト結果は画面下部に下図のように表示されます。 
Tracert テスト結果	ホスト IP に宛先を入力し、Tracert ボタンをクリックすることで、トレースルートテストを行うことが出来ます。 テスト結果は画面下部に下図のように表示されます。 
Wake on LAN	この機能はサポートしておりません。

12. サービス

12. 1. セルラーツールキット

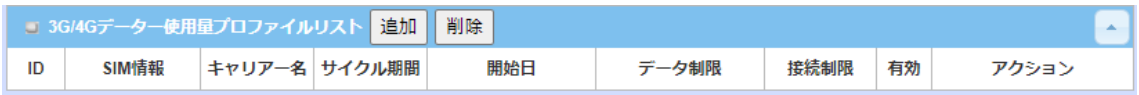
セルラーツールキットでは「データ使用量の監視」、「SMS（ショートメッセージ）」および「SIM PIN コード変更」など、3G/4G(LTE)の設定ができます。セルラーツールキットによる設定を行う前に、有効な SIM カードを本機に装着してください。

12. 1. 1. データ使用量（データ使用量の制限）

3G/4G（LTE）のデータープランでは、データ使用量が制限されている契約があります。この場合、データ使用量が制限を超えると、スループットの低下、請求金額が増えるなどが発生します。本機ではデータ使用量機能により、データ使用量を監視し、接続を切断したりSIM-B へ切り替えをしたりを自動的に行うことができます。データ容量制限による SIM 切り替え機能を使用する場合は、SIM-B へのフェールオーバー機能が有効でなければなりません。

SIM-Aの設定
サイクル期間：1月
開始日：2020/10/20
データ制限：1GB
制限：有効
SIM-Bへのフェールオーバー有効

◆ 画面左側のメニューから、サービス⇒セルラーキット⇒診断データ使用量の順にクリックします。



（注１） 本機の監視するデータ使用量は通信業者と異なる場合があります。制限の容量を契約より小さく設定することを推奨します。本機能の不動作による追加通信量などに関して一切責任を負いかねます。

12.1.1.1. 3G/4G データ使用量プロファイルリストの追加/編集

3G/4G データ使用量プロファイルは最大 4 ルールまで登録できます。

◆追加または編集ボタンをクリックすると、3G/4G データー使用量プロファイル設定画面が表示されます。

項目	説明
SIM 選択	SIM カードを「SIM-A」または「SIM-B」から選択します。通常は優先選択された SIM カードを選択します。 本機のインタフェースは 3G/4G 固定です。
キャリアー名	プロファイルの識別のために使用されるキャリア名を指定します。
サイクル期間	データ使用量をリセットする期間を「日単位」、「週単位」または「月単位」から選択します。日単位を選択した場合は、日数を 1～90 日までの範囲で指定します。
開始日	データ使用量監視を開始する日付を指定します。過去の日付の場合は、統計情報が正しく表示されない場合があります。
データ制限	選択したサイクル期間での制限容量を指定します。範囲は 1～999 で、「KB」、「MB」または「GB」の単位を選択できます。
接続制限	[有効]にチェックを入れると、データ使用量が容量制限を超えた場合に、強制的に 3G/4G 接続が切断されます。
制限有効化	[有効]にチェックを入れると、プロファイルが有効になります。

◆保存ボタンをクリックして、プロファイルを登録します。追加/編集したプロファイルが[3G/4G データ使用量プロファイルリスト]に表示されます。

12. 1. 2. SMS

本機では、WebGUI からモバイル NET の SMS（ショートメッセージ）機能が使用できます。この機能で、携帯電話やスマートフォンに短いメッセージを送信することができます。

（注２） 本機能を使用するためには SMS が使用できる回線契約が必要です。

◆画面左側のメニューから、サービス⇒セルラーキット⇒SMS の順にクリックします。

12.1.2.1. SMS の設定

SMS を送受信するための条件を設定します。

項目	説明
物理インターフェイス	本機で Cellular-1[モバイル NET-1]のみが使用できます。
SMS SIM ステータス	[有効]にチェックを入れると、SMS 機能が有効になります。 現在使用中の SIM を表示します。
SMS ストレージ	SMS メッセージの格納場所を [SIM カードのみ]、[セルラーモジュール]および[記憶装置]から選択します。本機では[SIM カードのみ]のみ対応しています。
SMS 容量	[有効]にチェックを入れると、記憶するメッセージの数を制限できます。SMS ストレージがいっぱいになると古いものから削除されます。

（注）新規 SMS ボタン、マネージングイベント設定ボタンおよび通知イベント設定ボタンについては、11.2 項の[SMS＆イベント]を参照してください。

12.1.2.2. SMS 要約（サマリー）

SMS の受信および送信の状況を表示します。

項目	説明
未読の SMS	SIM カードにある未読の SMS 数を表示します。
受信済 SMS	SIM カードにある SMS 数を表示します。
SMS を送信しました	本機から発信した SMS 数を表示します。
残り SMS	SMS の全容量から受信済み SMS 数を引いた値を表示します。

12.1.2.3. 新規 SMS

◆SMS 要約にある、新規 SMS ボタンをクリックすると、[新規 SMS]画面が表示されます。この画面から、SMS メッセージの作成・送信を行うことができます。

項目	説明
受取人	SMS メッセージの送信先（受信者）電話番号を指定します。セミコロン";"で区切ることで複数の送信先を指定することができます。
テキストメッセージ	SMS メッセージの本文を入力します。本機では最大 1023 文字まで入力できます。送信できる最大文字数は、回線契約によります。
Send ボタン	Send ボタンをクリックすると、SMS メッセージが送信されます。
結果	SMS メッセージの送信結果が[送信成功]または[送信失敗]のメッセージで表示されます。

12.1.2.4. SMS 受信トレイ

◆SMS 要約にある、SMS 受信トレイボタンをクリックすると、[SMS 受信トレイリスト]が表示され、受信 SMS メッセージの閲覧、削除、返信および転送などの操作ができます。。

項目	説明
ID	受信した SMS の番号です。
電話番号から	発信者の電話番号を表示します。
タイムスタンプ	SMS を受信した日時を表示します。
SMS テキストプレビュー	SMS メッセージ本文のプレビューを表示します。詳細ボタンをクリックすると全文が表示されます。
アクション	Reply ボタン：このメッセージに対して返信することができます。受取人がコピーされた[新規 SMS]画面が表示されます。 フォワードボタン：このメッセージを転送することができます。メッセージがコピーされた[新規 SMS]画面が表示されます。 チェックボックス：クリックすると選択され、削除ボタンでメッセージを削除することができます。

12.1.2.5. SMS 送信フォルダ

◆SMS 要約にある、SMS 送信フォルダボタンをクリックすると、[SMS 受信フォルダ]が表示され、送信 SMS メッセージの閲覧、削除などの操作ができます。。

項目	説明
ID	受信した SMS の番号です。
受取人	受信者の電話番号を表示します。
タイムスタンプ	SMS を送信した日時を表示します。
SMS テキストプレビュー	SMS メッセージ本文のプレビューを表示します。詳細ボタンをクリックすると全文が表示されます。
アクション	チェックボックス：クリックすると選択され、削除ボタンでメッセージを削除することができます。

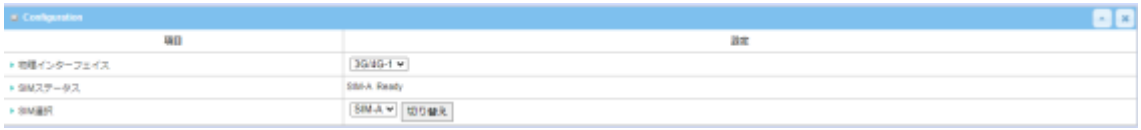
12. 1. 3. SIM PIN

3G/4G(LTE)のサービスを利用するためにSIMカードを本機に挿入する必要があります。SIMカードにはネットワーク所有者またはサービスプロバイダーが各加入者を識別するための情報が入力されており、不正アクセスを防ぐために SIM カードで PIN コードを有効にすることは、簡単で効果的な方法です。本機ではWebGUIを介してSIMカードのPINコードを有効化および管理できます。

◆画面左側のメニューから、サービス⇒セルラーキット⇒SIM PINの順にクリックします。

12.1.3.1. SIM カードの選択（Configuration）

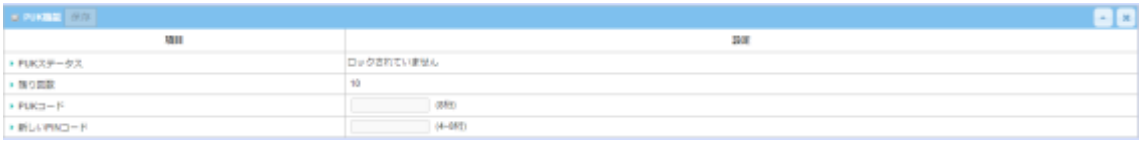
PIN コードを書き換える SIM カードを選択します。



項目	説明
物理インターフェイス	「3G/4G-1」固定です。
SIM ステータス	選択した SIM カードと SIM カードのステータスを示します。 ステータスは、Ready, Not Insert, or SIM PIN と表示されます。 ◆Ready: SIM カードが挿入され、使用できる状態です。 PIN 保護のない SIM カードであるか、正しい PIN コードで SIM カードのロックが解除されています。 ◆Not Insert: その SIM スロットに SIM カードが挿入されていません。 ◆SIM PIN: SIM カードは PIN コードで保護されており、正しい PIN コードでロック解除されていません。 その SIM カードはまだロックされた状態です。
SIM 選択	SIM PIN を設定する SIM カードを「SIM-A」または「SIM-B」から選択します。 切り替えボタンを押すと、SIM カードをもう一つカードに切り替えます。 その後、SIM カードを設定できます。

12.1.3.2. PUK 機能

PUK 機能による SIM ロック解除は、PIN コードの誤りを試行回数限界に達した時に、回線業者に SIM カードの PUK コードを聞き、ロックを解除する必要があります。PUK コードで SIM カードのロックを解除すると、SIM ロック機能が自動的に有効になります。



項目	説明
PUK ステータス	PUK の状態を表示します。 ◆PUKUnlock：PIN コードエラー限界以内で PUK でロックされていません。 ◆PUKLock：PIN コードエラー限界に達し PUK でロックされています。
残り回数	PUK ロック解除の残りの試行回数を表します。
PUK コード	PUK ロック解除ステータスで SIM カードのロックを解除できる PUK コード（8 桁）を指定します。
新しい PIN コード	SIM カードの新しい PIN コード（4～8 桁）を入力します。

◆保存ボタンをクリックし、PUK のロック解除と新しい PIN コードを SIM カードに登録します。

12.1.3.3. SIM 機能 （PIN コードの設定）

PIN コード（パスワード）機能を有効または無効にし、PIN コードを変更することもできます。

項目	説明
PIN ロック	[有効]ボックスをチェックし、SIM ロック機能を有効にします。 初めて SIM ロック機能を有効にする場合は、PIN コードも入力し、保存ボタンをクリックして設定を保存します。
残り回数	SIMPIN ロック解除の残りの試行回数を表します。

◆PIN コード変更ボタンをクリックすると、以下の画面が表示されます。

Item	Setting
Current PIN Code	(4~8 digits)
New PIN Code	(4~8 digits)
Vertified New PIN Code	(4~8 digits)

Apply Cancel

◆現在の PIN コードと新し PIN コード（確認含む）を入力して、Apply ボタンをクリックしてください。

12.1.4. 通信スキャン

本機能はサポートしていません。

12.2. SMS & イベント

本機は、ネットワーク管理者が個々のプロファイルであらかじめ定義したイベントまたは応答の動作を設定し、機器の各種ステータスや情報を取得できる機能を搭載します。イベントとしては「マネージングイベント」と「通知イベント」があります。

12.2.1. マネージングイベント

本機を管理するため、または、本機の特定の機能の設定/ステータスを変更するために使用されるイベントです。SMS 経由で管理イベントを受信すると、本機は機能を変更し、管理に必要なステータスを同時に収集します。

対応する動作は、ネットワークステータスの取得、LAN/VLAN の動作、NAT の動作、ファイアウォールの動作、VPN の動作、システム管理などの設定変更になります。

12.2.2. 通知イベント

本機が監視している内部イベントの発生が起因となるイベントで、イベントの発生時に対応した動作を実行します。SMS メッセージや電子メールなどで発生を管理者に通知します。

要因となるイベントは、接続変更（WAN、LAN および VLAN）、管理およびデータの使用です。

12.2.3. 設定

◆画面左側のメニューから、サービス⇒SMS＆イベント⇒設定の順にクリックします。

◆各項目の設定が完了したら、保存ボタンをクリックして、設定を保存します。

12.2.3.1. イベントマネージメントの設定

項目	説明
イベントマネージメント	[有効]にチェックを入れると、イベント管理機能が有効になります。

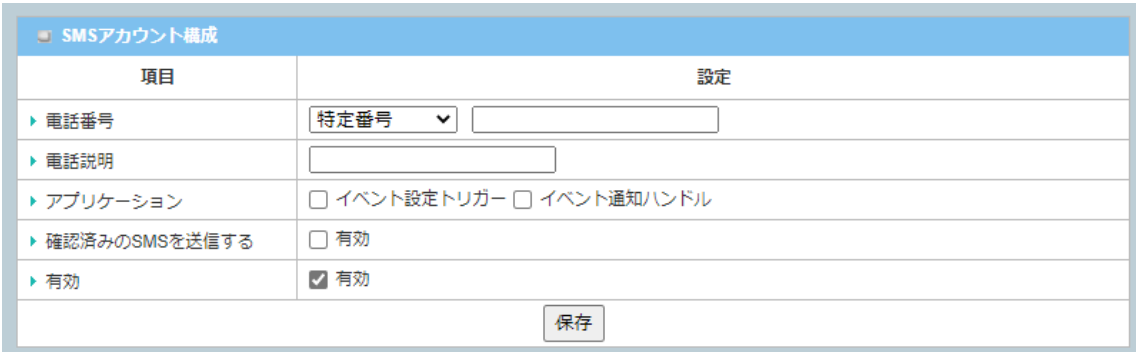
12.2.3.2. SMS コンフィグレーションの設定

項目	説明
メッセージ接頭辞	[有効]にチェックを入れると、受信 SMS の解析が有効になります。 また、マネージングイベントを識別するための接頭辞(プリフィックス文字列)を指定します。
物理インターフェイス	本機では 3G/4G 固定です。対象となる SIM が表示されます。
処理後の管理対象 SMS の削除	[有効]にチェックを入れると、受信したマネージングイベント SMS を処理した後に削除します。

12.2.3.3. SMS アカウントリスト追加/編集

SMS を経由して本機を管理するための SMS アカウントを最大5アカウントまで登録できます。

◆追加または編集ボタンをクリックすると、[SMS アカウント構成]画面が表示されます。

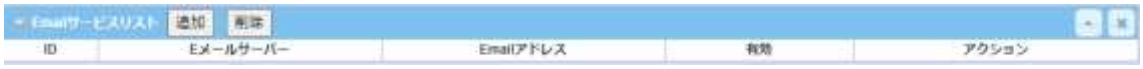


項目	説明
電話番号	マネージングイベントとして受信する SMS 送信者の電話番号を指定します。電話番号の桁数は 32 桁以内です。 「全てを許可」を選択すると電話番号による識別はしません。
電話説明	SMS の簡単なアカウント説明を指定します。
アプリケーション	アプリケーション(動作)タイプ「イベント設定トリガー」および「イベント通知ハンドル」にチェックを入れると、それぞれの動作が有効になります。
確認済みの SMS を送信する	[有効]にチェックを入れると、SMS 応答機能が有効になります。
有効	[有効]にチェックを入れると、このアカウントが有効になります。

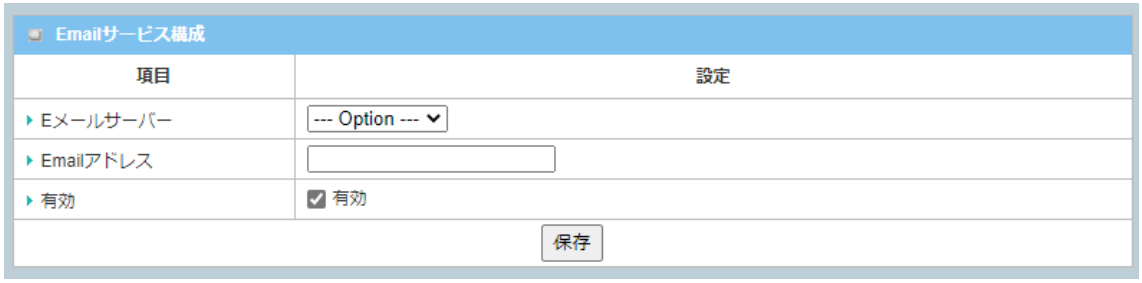
◆保存ボタンをクリックして、アカウントを登録します。追加/編集したアカウントが[SMS アカウントリスト]に表示されます。

12.2.3.4. Email サービスリストの追加/編集

イベント通知用の E メールサービスアカウントを設定します。 最大 5 つのアカウントをサポートします。



◆追加または編集ボタンをクリックすると、[Email サービス構成]画面が表示されます。



項目	説明
E メールサーバー	電子メールアカウント設定の外部サーバー設定から電子メールサーバープロファイルを選択します。
Email アドレス	宛先の電子メールアドレスを指定します。
有効	[有効]にチェックを入れると、この Email サービスが有効になります。

◆保存ボタンをクリックして、Email サービスを登録します。追加/編集した Email サービスが[SMS アカウントリスト]に表示されます。

12.2.3.5. リモートホストリストの追加/編集

リモートホストプロファイルを設定します。 最大 10 個のプロファイルをサポートします。

◆追加または編集ボタンをクリックすると、[リモートホスト設定]画面が表示されます。

項目	説明
ホスト名	リモートホストプロファイル名を指定します。名前の長さは 64 文字以下です。
ホスト IP	リモートホストの IPv4 フォーマットで IP アドレスを指定します。
プロトコルタイプ	リモートホストにアクセスするためのプロトコルを指定します。 TCP または UDP から選択します。
ポート番号	リモートホストにアクセスするためのポート番号を指定します。 値の範囲は 1～65535 です。
プレフィックスメッセージ	必要に応じて、リモートホストにアクセスするための事前に決められた ID としてプレフィックスメッセージ(64 文字以下)を指定します。
サフィックスメッセージ	必要に応じて、リモートホストにアクセスするための事前に決められた ID としてサフィックスメッセージ(64 文字以下)を指定します。
有効	[有効]にチェックを入れると、リモートホストが有効になります。

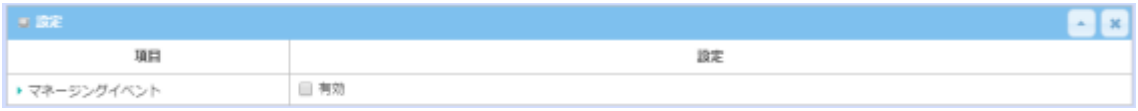
◆保存ボタンをクリックして、リモートホストプロフィルを登録します。追加/編集したリモートホストが[リモートホストリスト]に表示されます。

12.2.4. マネージングイベント

◆画面左側のメニューから、サービス⇒SMS＆イベント⇒マネージングイベントの順にクリックします。

◆設定、マネージングリストの追加が終了したら、保存ボタンをクリックして設定を登録します。

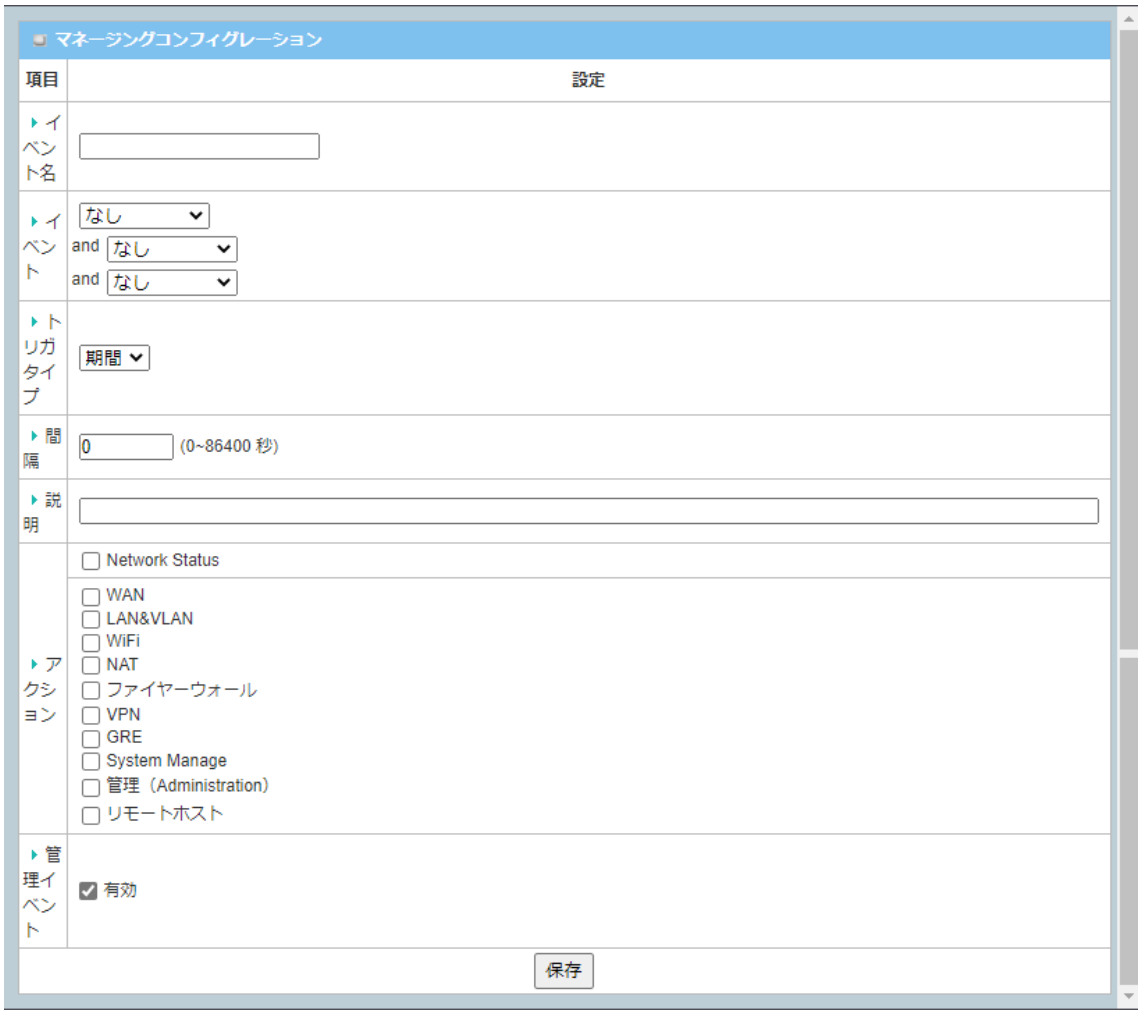
12.2.4.1. マネージングイベントの設定



項目	説明
マネージングイベント	[有効]にチェックを入れると、マネージングイベントが有効になります。

12.2.4.2. マネージングリストの追加/編集

◆追加または編集ボタンをクリックすると、[マネージメントコンフィグレーション]画面が表示されます。



項目	説明
イベント名	識別のためのイベント名を指定します。
イベント	イベントタイプを「SMS」または「SNMP トラップ」から選択し、イベント識別子/プロファイルを指定します。 イベントは最大 3 つのイベント条件を指定でき、すべての条件が同時に成立したときにイベントが発行されます。 SMS：テキストボックスに SMS メッセージを指定します。 SNMP：テキストボックスに SNMP トラップイベントメッセージを指定します。
トリガタイプ	イベントトリガーのタイプを「期間」または「1 回」を指定します。 期間：[期間]を選択し、時間間隔を指定します。指定したイベント条件が成立すると、イベントはすべての時間間隔で繰り返しトリガーされます。 1 回：[1 回]を選択すると、指定したイベント条件が成立したときに、イベントが 1 回だけトリガーされます。
間隔	繰り返しイベントトリガーの時間間隔を指定します。値の範囲は 0～86400 秒です。
説明	マネージングルールの説明を記述します。
アクション	ネットワークステータス、または定義したイベントが発生したときに実行する少なくとも 1 つの休止アクションを指定します。 ネットワークステータス：ネットワークステータスを取得します。 WAN:WAN の接続/切断、3G/4G のモード設定を変更します。 LAN＆VLAN：LAN1/WAN、LAN2 ポートリンクのオン/オフ設定を変更します。 WiFi：WiFi モジュール1のオン/オフ設定を変更します。 NAT：仮想サーバールールのオン/オフ、DMZ オン/オフ設定を変更します。 ファイアウォール：リモート管理者ホスト ID のオン/オフ設定を変更します。 VPN： IPSecトンネルのオン/オフ、PPTP クライアントのオン/オフ、L2TP クライアントのオン/オフ、OpenVPN クライアントのオン/オフ設定を変更します。 GRE：GRE トンネルのオン/オフ設定を変更します。 システム管理：本機ではサポートしていません。 管理：バックアップ構成、復元構成、再起動、現在の設定をデフォルトとして保存設定を変更します。 リモートホスト：リモートホストプロファイルを選択します。
管理イベント	[有効]にチェックを入れると、このマネージングイベントが有効になります。

◆保存ボタンをクリックして、マネージメントルールを登録します。追加/編集したマネージメントルールが[マネージングリスト]に表示されます。

12.2.5. 通知イベント

◆画面左側のメニューから、サービス⇒SMS＆イベント⇒通知イベントの順にクリックします。

◆設定、通知イベントリストの追加が終了したら、保存ボタンをクリックして設定を登録します。

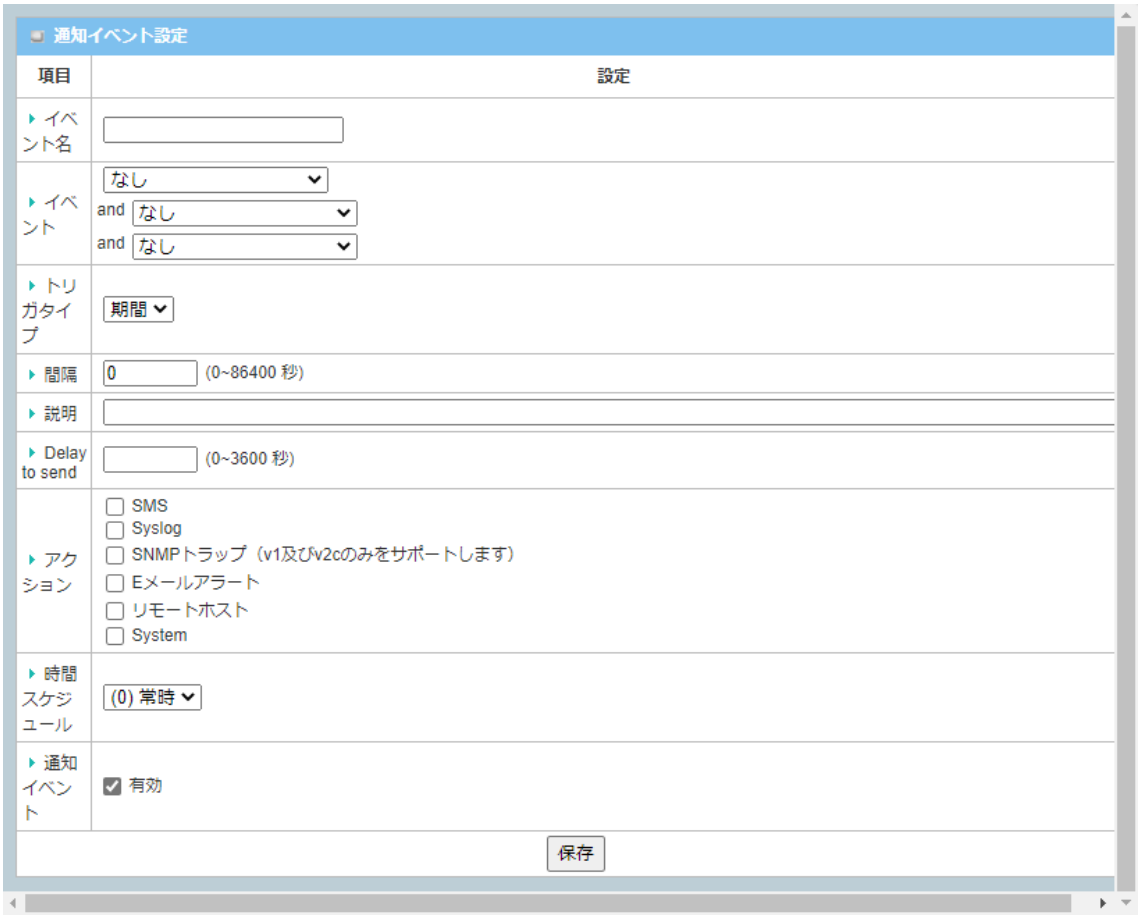
12.2.5.1. 通知イベントの設定

項目	説明
通知イベント	[有効]にチェックを入れると、通知イベントが有効になります。

12.2.5.2. 通知イベントリストの追加/編集

通知イベントルールは最大 128 ルールが登録できます。

◆追加または編集ボタンをクリックすると、[通知イベント設定]画面が表示されます。



項目	説明
イベント名	識別のためのイベント名を指定します。
イベント	イベントタイプを以下から選択し、「WAN」、「LAN&VLAN」、「WiFi」、「DDNS」、「管理(Administration)」、「データ使用量」および「System」から選択し、それぞれの通知要因を選択します。イベントは最大 3 つのイベント条件を指定でき、すべての条件が同時に成立したときにイベントが発行されます。
トリガタイプ	イベントトリガーのタイプを「期間」または「1 回」を指定します。 期間:[期間]を選択し、時間間隔を指定します。指定したイベント条件が成立すると、イベントはすべての時間間隔で繰り返しトリガーされます。 1 回:[1 回]を選択すると、指定したイベント条件が成立したときに、イベントが 1 回だけトリガーされます。
間隔	繰り返しイベントトリガーの時間間隔を指定します。値の範囲は 0～86400 秒です。
説明	通知イベントルールの説明を記述します。
Delay to send	必要に応じて、トリガーされた通知イベントを送信するための遅延時間を指定します。値の範囲は 0～3600 秒です。
アクション	登録したイベントが発生したときに実行するアクションを少なくとも 1 つ指定します。 SMS:登録されたすべての SMS アカウントに SMS を送信します。 Syslog:Syslog を選択し、イベントのアクションとして[チェックボックスを有効にする]を選択/選択解除します。 SNMP トラップ:登録された SNMP イベントレシーバーに SNMP トラップを送信します。 E メールアラート:登録された E メールアカウントに E メールを送信します。 リモートホスト:登録したリモートホストプロファイルを選択します。 システム:30 秒後に再起動を選択します。
時間スケジュール	本通知イベントルールが有効になる時間スケジュールを指定します。 常時(0)または「スケジュール設定」で定義されたスケジュールリストから選択できます。
通知イベント	[有効]にチェックを入れると、この通知イベントが有効になります。

◆ 保存ボタンをクリックして、通知イベントを登録します。追加/編集した通知イベントが[通知イベントリスト]に表示されます。

13. ステータス

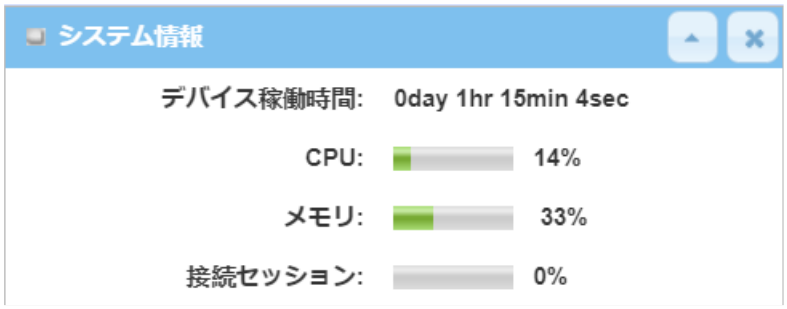
13. 1. ダッシュボード

[デバイスダッシュボード]ウィンドウには、ゲートウェイの動作ステータスをすばやく把握するためのグラフまたは表に現在の各種ステータスが表示されます。システム情報、システム情報履歴、および、ネットワークインターフェイスステータスが表示されます。表示は 1 秒ごとに更新されます。

◆画面左側のメニューから、ステータス⇒ダッシュボードの順にクリックします。

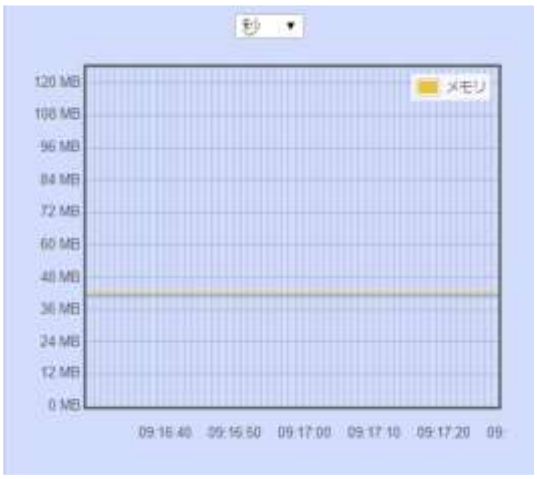
13. 1. 1. システム情報

[システム情報]画面には、デバイス稼働時間、CPU、メモリのリソース使用率、および接続セッションが表示されます。



13.1.2. システム情報履歴

[システム情報履歴]画面には、CPU とメモリの統計グラフが表示されます。



13.1.3. ネットワークインターフェイスステータス

ネットワークインターフェイスステータス

デバイス	タイプ	アップロードトラフィック	ダウンロードトラフィック	現在のアップロードトラフィック	現在のダウンロード トラフィック
eth2	Ethernet	85 (MB)	4 (MB)	701 (KB)	19 (KB)
br0	Ethernet	85 (MB)	4 (MB)	699 (KB)	16 (KB)
eth2.1	Ethernet	61 (MB)	2 (MB)	701 (KB)	17 (KB)

[ネットワークインターフェイスステータス]画面には、ゲートウェイの各ネットワークインターフェイスの統計情報が表示されます。統計情報には、インターフェイスタイプ、アップロードトラフィック、ダウンロードトラフィック、および、現在のアップロード/ダウンロードトラフィックが含まれます。

13.2. 基本ネットワーク

13.2.1. WAN & アップリンク

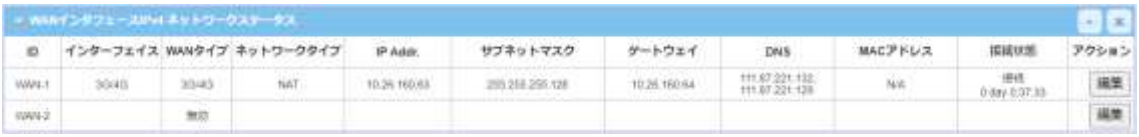
WAN & アップリンクステータスウィンドウには、ネットワーク構成、接続情報、モデムステータス、トラフィック統計など、さまざまなネットワークタイプの現在のステータスが表示されます。表示は 5 秒ごとに更新されます。

◆画面左側のメニューから、ステータス⇒基本ネットワーク⇒WAN & アップリンクの順にクリックします。

13.2.2. WAN インタフェース IPv4 ネットワークステータス

IPv4 ネットワークの各種ステータス情報が表示されます。

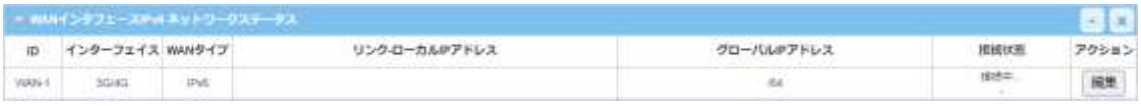
編集をクリックすると接続設定に移動します。



13.2.3. WAN インタフェース IPv6 ネットワークステータス

IPv6 ネットワークの各種ステータス情報が表示されます。

編集をクリックすると WAN インタフェースの IPv6 設定に移動します。



13.2.4. LAN インタフェースネットワークステータス

LAN ネットワークの各種ステータスが表示されます。

IPv4 を編集するボタンをクリックすると、LAN&VLAN の設定画面に移動します。

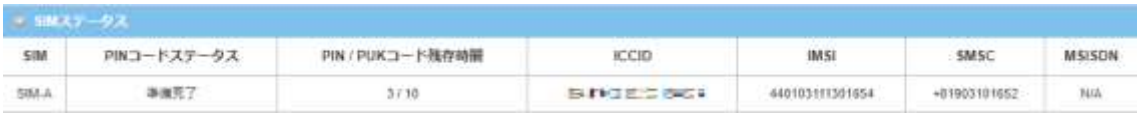
IPv6 を編集するボタンをクリックすると、IPv6 の設定画面に移動します。

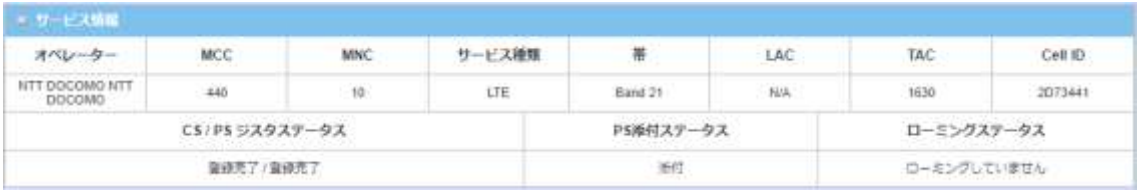
13.2.5. 3G/4G モデムステータスリスト

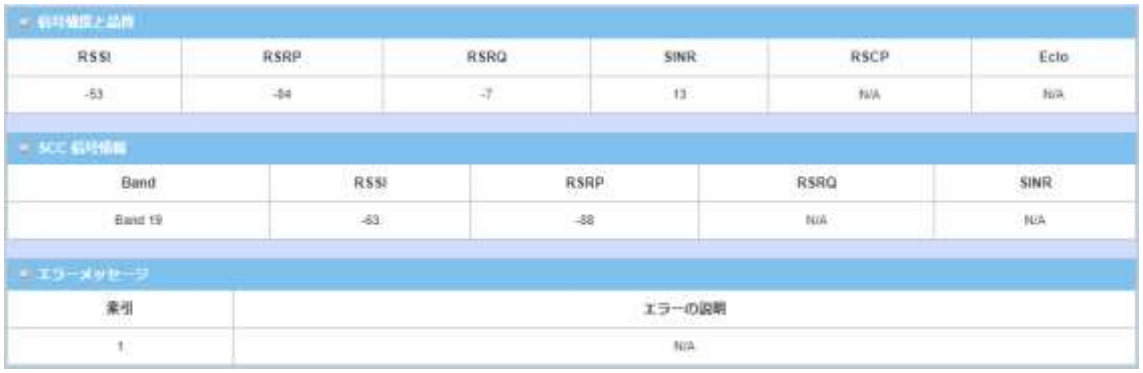
3G/4G(LTE)の無線通信の各種ステータスが表示されます。

詳細をクリックすると、「モデム情報」、「SIM ステータス」、「サービス情報」、「信号強度と品質」、「SCC 信号情報」および「エラーメッセージ」の詳細な状態情報が表示されます。

＜詳細情報例＞



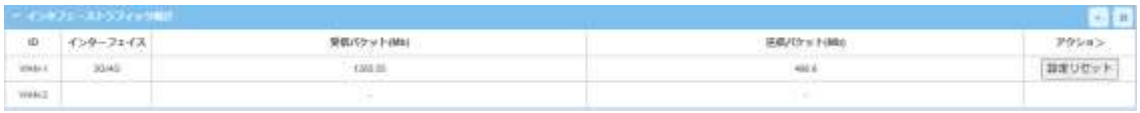




13.2.6. インタフェーストラフィック統計

WAN-1 および WAN-2 インターフェイスのトラフィック統計情報が表示されます。

設定リセットボタンでトラフィック情報をリセットできます。

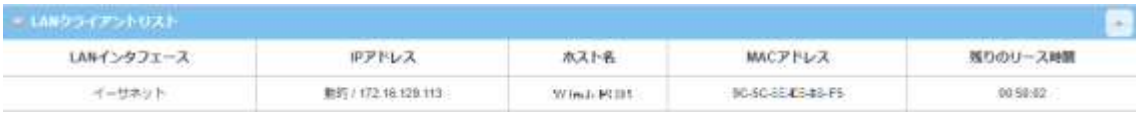


13.2.7. LAN および VLAN

◆画面左側のメニューから、ステータス⇒基本ネットワーク⇒LAN および VLAN の順にクリックします。

13.2.7.1. クライアントリスト

本機LANに接続されているデバイスの情報が表示されます。



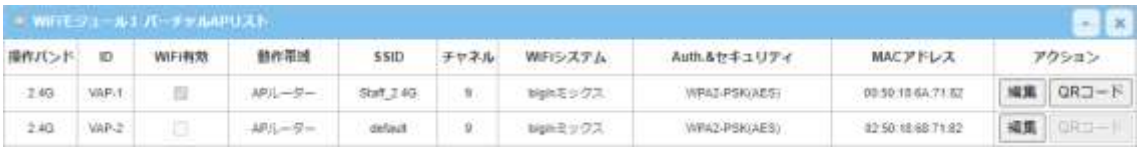
13. 2. 8. WiFi

◆画面左側のメニューから、ステータス⇒基本ネットワーク⇒WiFiの順にクリックします。

13.2.8.1. WiFi モジュール1バーチャル AP リスト

WiFi モジュール1で動作する仮想 AP のリストが表示されます。

編集ボタンで WiFi 設定に移動します。



13.2.8.2. WiFi モジュール 1WDS ステータス

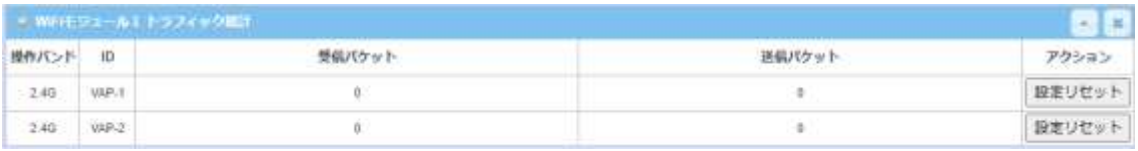
WiFi モジュール1が WDS モードで動作中のステータス情報が表示されます。

設定リセットボタンでリセットされます。

13.2.8.3. WiFi モジュール 1 トラフィック統計

仮想 AP 毎のトラフィック統計情報が表示されます。

設定リセットボタンでリセットされます。



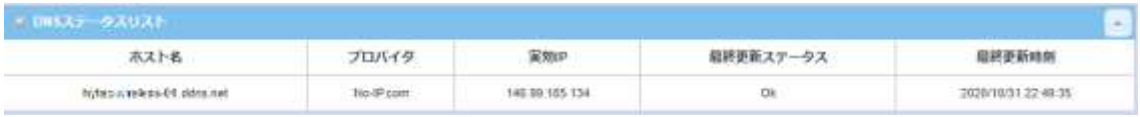
13. 2. 9. ダイナミック DNS

◆画面左側のメニューから、ステータス⇒基本ネットワーク⇒ダイナミック DNS の順にクリックします。

13.2.9.1. DNS ステータスリスト

ダイナミック DNS の状態が表示されます。

更新ボタンで最新の情報を表示します。



13.3. セキュリティ

VPN ステータスウィンドウには、VPN トンネルの全体的なステータスが表示されます。表示は 5 秒ごとに更新されます。

13.3.1. VPN

VPN ステータスウィンドウには、VPN トンネルの全体的なステータスが表示されます。表示は 5 秒ごとに更新されます。

◆画面左側のメニューから、ステータス⇒セキュリティ⇒VPN の順にクリックします。

13.3.1.1. IPSec トンネルステータス

IPSec VPN 接続設定と現在のステータスが表示されます。

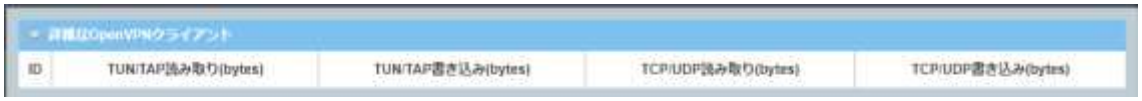
編集ボタンをクリックすると IPSec の設定画面に移動します。

13.3.1.2. OpenVPN クライアントステータス

OpenVPN による接続状態が表示されます。

編集ボタンをクリックすると、OpenVPN の設定画面に移動します。

詳細ボタンをクリックすると、クライアントのデータ通信ステータスが表示されます。



13.3.1.3. L2TP クライアントステータス

L2TP トンネリングの設定と現在のステータスが表示されます。

編集ボタンをクリックすると、L2TP の設定画面に移動します。

13.3.1.4. PPTP クライアントステータス

PPTPトンネリングの設定と現在のステータスが表示されます。

編集ボタンをクリックすると、PPTP の設定画面に移動します。

13.3.2. ファイヤーウォール

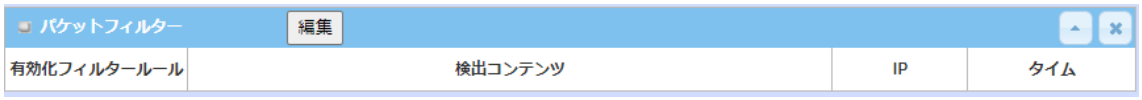
ファイヤーウォールステータスウィンドウには、ファイヤーウォールの全体的な設定とステータスが表示されます。表示は 5 秒ごとに更新されます。

◆画面左側のメニューから、ステータス⇒セキュリティ⇒ファイヤーウォールの順にクリックします。

13.3.2.1. パケットフィルターステータス

パケットフィルタリングのログ履歴が表示されます。

編集ボタンをクリックすると、パケットフィルター設定画面に移動します。



13.3.2.2. URL ブロッキングステータス

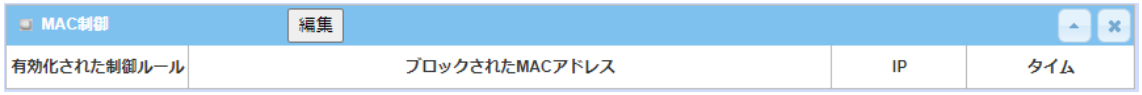
URL ブロッキングのログ履歴が表示されます。

編集ボタンをクリックすると、URL ブロッキング設定画面に移動します。

13.3.2.3. MAC 制御ステータス

MAC 制御のログ履歴が表示されます。

編集ボタンをクリックすると、MAC 制御設定画面に移動します。



13.3.2.4. IPS ステータス

IPS のログ履歴が表示されます。

編集ボタンをクリックすると、IPS 設定画面に移動します。

13.3.2.5. オプションステータス

オプションの設定とログ履歴が表示されます。

編集ボタンをクリックすると、オプション設定画面に移動します。

13.4. 管理(Administration)

13.4.1. 設定と管理

本機ではサポートしていません。

13.4.2. ログストレージ

◆画面左側のメニューから、ステータス⇒管理(Administration)⇒ログストレージの順にクリックします。

13.4.2.1. ストレージ情報ステータス

ログ保管メディアの現在の状態が表示されます。

更新ボタンで最新の情報が表示されます。

13.5. 統計とレポート

統計とレポートステータスでは「接続セッション」、「ログイン記録」、「セルラー使用状況」および「セルラー信号」の統計情報が表示されます。

13.5.1. 接続セッション

◆画面左側のメニューから、ステータス⇒統計とレポート⇒接続セッションの順にクリックします。

13.5.1.1. インターネットサーフィンリスト

本機で管理している接続トラフィック情報が表示されます。

インターネットサーフィンリスト (14 entries) 前 次に 最初 最後 Export(.xml) Export(.csv) 更新

ユーザー名	プロトコル	内部IP及びポート	MAC	外部IP及びポート	デュレーションタイム
	UDP	146.99.185.134:28676		220.159.212.200:53	2020/11/01 09:09~
	TCP	172.16.129.113:49672		5.188.71.27:80	2020/11/01 09:09~
	TCP	172.16.129.113:53263		20.191.46.211:443	2020/11/01 09:09~
	TCP	172.16.129.113:53249		20.191.46.211:443	2020/11/01 09:09~
	UDP	172.16.129.113:55047		172.16.129.254:53	2020/11/01 09:09~
	TCP	172.16.129.113:49691		52.139.250.253:443	2020/11/01 09:09~
	TCP	114.134.201.23:53727		146.99.185.134:80	2020/11/01 09:09~
	TCP	114.134.201.23:53723		146.99.185.134:80	2020/11/01 09:09~
	TCP	114.134.201.23:53720		146.99.185.134:80	2020/11/01 09:09~
	TCP	114.134.201.23:53719		146.99.185.134:80	2020/11/01 09:09~

前、次に、最初および最後ボタンをクリックして、表示ページを変更します。

更新ボタンをクリックすると、リストが最新の情報になります。

Export(.xml)および Export(.csv)ボタンをクリックすると、リストをPC内に選択したファイル形式で取り込むことができます。

13.5.2. ログイン統計

◆画面左側のメニューから、ステータス⇒統計とレポート⇒ログイン統計の順にクリックします。

13.5.2.1. デバイス管理者統計

本機へのログイン履歴が表示されます。

ユーザー名	プロトコルタイプ	IPアドレス	Info	デュレーションタイム
admin	HTTP	172.16.129.249	Login Fail	2018/01/01 09:00~
admin	HTTP	172.16.129.249	Admin	2018/01/01 09:00~
admin	HTTP	172.16.129.113	Admin	2020/10/30 19:33~
admin	HTTP	114.134.201.23	Admin	2020/10/31 12:04~

前、次に、最初および最後ボタンをクリックして、表示ページを変更します。

更新ボタンをクリックすると、リストが最新の情報になります。

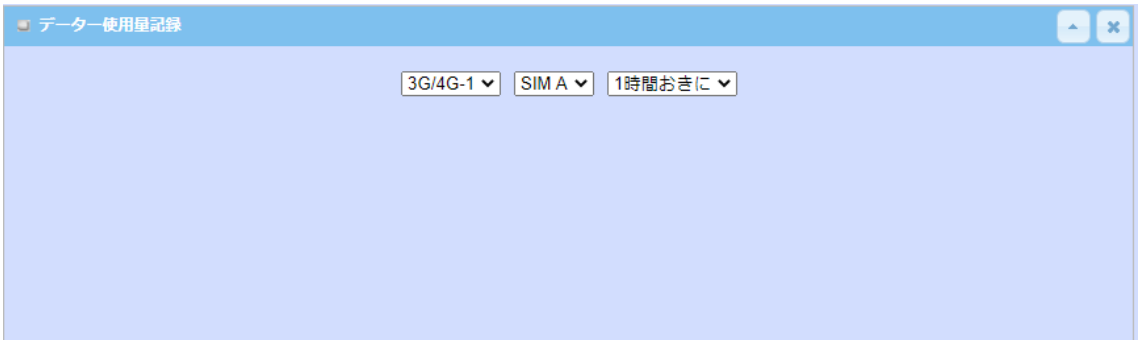
Export(.xml)および Export(.csv)ボタンをクリックすると、リストをPC内に選択したファイル形式で取り込むことができます。

13.5.2.2. セルラー使用状況

◆画面左側のメニューから、ステータス⇒統計とレポート⇒セルラー使用状況の順にクリックします。

13.5.2.3. データ使用量記録

「SIM-A」または「SIM-B」から選択した 3G/4G（セルラー）インターフェイスのデータ使用量記録が表示されます。使用量の記録頻度を「1 時間おき」または「毎日」から選択できます。

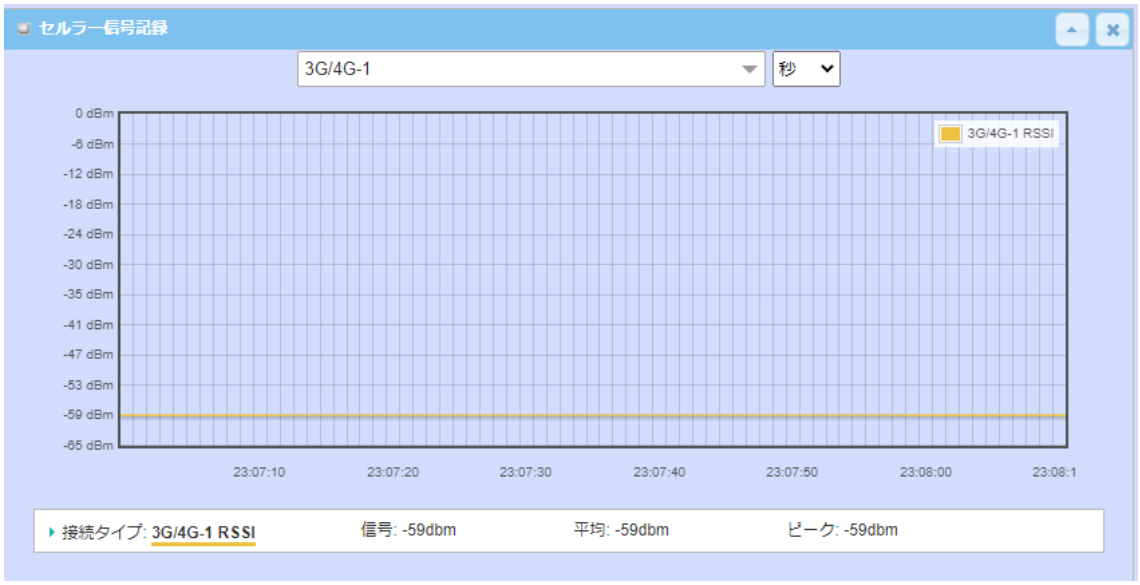


13.5.3. セルラー信号

◆画面左側のメニューから、ステータス⇒統計とレポート⇒セルラー信号の順にクリックします。

13.5.3.1. セルラー信号記録

3G/4G(LTE)の信号強度の履歴をグラフおよび現在値、平均値およびピーク値を表示します。
更新間隔を「秒」、「分」または「時間」より選択できます。



14. 製品仕様

製品型番		HWL-3511-DS
商品コード		189-HY-006
LTE	対応バンド	FDD LTE: B1/B3/B8/B18/B19/B26
		TDD LTE: B39/B41
		WCDMA: B1/B6/B8/B19
	対応キャリア	NTT DoCoMo、au、Softbank など
	LTE カテゴリー	LTE Cat.6 キャリアアグリゲーション対応
	対応 SIM カード/Slot	マイクロ SIM 2xSIM Card Slot
	アンテナ/インターフェイス	外部アンテナ<Main/AUX> / 2xSMA(F)コネクタ
Wi-Fi	対応規格	802.11b/g/n (2.4GHz)
	モード	AP(親機)モード/STA(子機)モード切替
	セキュリティ	WEP/WPA/WPA2/ WPA-PSK/ WPA2-PSK/802.1x
	クライアント数	最大 80 台 (推奨 16 台以下)
	アンテナ/インターフェイス	外部アンテナ/ 1xSMA(M)コネクタ
LAN	対応速度/規格	10Mbps(10Base-T)/100Mbps(100Base-TX)
	WAN ポート	1x イーサネット WAN/LAN 切替
	インターフェイス	2x RJ-45 コネクタ (状態表示 LED<緑>あり)
プロトコル	LAN	DHCP サーバー、Tag/ポートベース VLAN
	TCP/IP	IPv4/IPv6 Dual Stack
	ポート制御	NAT/Port Forwarding/DMZ/VPN パススルー
	ルーティング	Static/RIP1,2/OSPF
セキュリティ	VPN	IPsec/OpenVPN*1/ PPTP*1 /L2TP*1/ GRE
	ファイアウォール	SPI Firewall/IPS/MAC, Packet, URL 各種フィルター
推奨接続機器数		LAN/WiFi 含めて 16 台以下を推奨
LED 表示		Status, Signal, WiFi: 全て青
その他	SD メモリ	1x microSD Card Slot(システムログ格納用)
防水		なし
電源		AC100～240V/本体のみ:DC5V～18V(DC ジャック)
消費電力	AC100V 入力	最大 5W (AC アダプタ含む)
	本体消費電力	最大 4W (DC12V 入力時)
動作温度		-30 ～ +60℃
保存温度		-40 ～ +85℃
相対湿度		10 ～ 95% (結露なきこと)
本体寸法		(W)93mm x (D)90mm x (H)27mm (突起物含まず)
本体重量		270g 以下
認定		工事設計認証番号: 003-160023(LTE) TELEC 認定番号: 201-190002(WiFi) 技術基準適合認定番号: D160012003 VCCI Class A / PSE (AC アダプタ) 本体、添付品 RoHS 10 対応
製品保証期間		1 年間
付属品		LTE アンテナ x2、WiFi アンテナ x1、ゴム足 x4 DIN レールブラケット x2、AC アダプタ x1

15. 付属 AC アダプタ仕様

製品名	TRH25120-A-23E13 AC アダプタ	
商品コード	167-CN-011	
電源	入力	AC 100～240V
	出力	DC 12V (DC ジャック)
動作温度	-20～+60℃	
保存温度	-20～+85℃	
認定	RoHS、PSE ほか	

16. 製品保証

◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

1) 修理を依頼される前に今一度、この取扱説明書をご確認ください。
2) 本製品の保証期間内の自然故障につきましては無償修理させて頂きます。
3) 故障の内容により、修理ではなく同等品との交換にさせて頂く事があります。
4) 弊社への送料はお客様の負担とさせて頂きますのでご了承ください。

初期不良保証期間:

ご購入日より **3ヶ月間**（弊社での状態確認作業後、交換機器発送による対応）

製品保証期間:

《本体》ご購入日より **1年間**（お預かりによる修理、または交換対応）

◆ 保証期間内であっても、以下の場合は有償修理とさせて頂きます。
（修理できない場合もあります）

1) 使用上の誤り、お客様による修理や改造による故障、損傷
2) 自然災害、公害、異常電圧その他外部に起因する故障、損傷
3) 本製品に水漏れ・結露などによる腐食が発見された場合

◆ 保証期間を過ぎますと有償修理となりますのでご注意ください。

◆ 一部の機器は、設定を本体内に記録する機能を有しております。これらの機器は修理時に設定を初期化しますので、お客様が行った設定内容は失われます。恐れ入りますが、修理をご依頼頂く前に、設定内容をお客様にてお控えください。

◆ 本製品に起因する損害や機会の損失については補償致しません。

◆ 修理期間中における代替品の貸し出しは、基本的に行っておりません。別途、有償サポート契約にて対応させて頂いております。有償サポートにつきましてはお買い上げの販売店にご相談ください。

◆ 本製品の保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社
カスタマサポート
TEL 0570-060030
E-mail support@hytec.co.jp
受付時間 平日 9:00～17:00