SIM Router

IDG500V-0T501

取扱説明書

株式会社バルテック

第 1.0 版

本書には本装置を正しくご利用いただく為の、接続・設置方法、注意・警告事項が記載されている為、お使いになる前に必ずお読みになり、方法や注意事項を十分ご理解いただいた上でご利用ください。
本書は紛失しないように、大切に保管してください。

目次

第1章. はじめに

1-1. はじめに

本製品は、M2M（マシンツーマシン）での使用に最適です。世界クラスのLTEモジュールが搭載されているため、モバイルキャリアのSIMカードを差し込むだけでインターネットに接続できます。冗長SIM設計により、重要な用途でのWAN接続の信頼性がさらに高くなります。世界クラスの3G HSPA+または4G LTEモジュールが搭載されているため、モバイルキャリアのSIMカードを差し込むだけでインターネットに接続できます。冗長SIM設計により、重要な用途でのWAN接続の信頼性がさらに高くなります。VPNトンネリングテクノロジーにより、リモートサイトを簡単にイントラネットの一部に組み込むことができます。また、すべてのデータはセキュリティ保護（256ビットAES暗号化）されたリンクで送受信されます。M2M用途のさまざまな要件に対応できるよう、モジュラー設計により製作されています。

■主な機能：

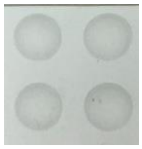
- 3G/4G WAN接続ができます。
- 包括的なLAN接続のためのイーサネットポートを提供し、LAN-1ポートは別のWANインターフェイスとして構成することができます。
- NATファイアウォールにより高度なセキュリティを実現します。
- 高度なリモート管理やローカル管理によりネットワークを監視できます。
- 本体は頑丈で取り付けがしやすい金属製で、ビジネス環境やM2M環境でのさまざまなM2M（マシンツーマシン）用途に対応しています。
- 推奨利用は、楽天SIMです。

本製品を設置して使用する前に、本書をよくお読みになって、本製品の機能を十分に理解してください。

1-2. 内容品リスト

1.2.1　梱包の内容

■標準パッケージ

		説明	数量
1		SIMルータ 本体 （型番：IDG500V-0T501）	1個
2		セルラーアンテナ	2個
3		ネジ端子ブロックアダプターに対する オスDCジャック	1個
4		DINレールブラケット	2個
5		RJ45 ケーブル	1個
6		ゴム製足	4個
7		電源アダプタ ● PSE認証	1個

1-3. 製品仕様

デバイスインタフェース
•モジュール内蔵: 1*LTE-Cat.4、2*SIM
•LANポート: 1(2)*RJ45 GE
•ログストレージ: 1*Micro-SDスロット
•拡張機能: 1*Micro USB
•GNSS : 1*GPSの組み込み受信機(Active)
•入力電源: DC 5~18V、消費電力: max. 6.5W
•アンテナコネクタ: 2*SMA (F)-LTE、1* SMA(F)-GPS

WAN機能
•WAN機能: セルラー、デュアルSIMフェールオーバー
•セルラー: 3GPP、LTE、セルラーブリッジ
•ネットワーク監視: ICMP/DNSチェッキング

プロトコル
•DHCPサーバー
•ポート転送: NAT、DMZ、仮想サーバー&コンピュータ、VPNパススルー
•ルーティング: 静的ルーティング

ステータス
•ダッシュボード:システム情報
•ネットワークステータス:ワイヤレスWAN＆LAN接続情報、詳細ワイヤレス信号品質
•セルラーモバイル通信情報：電波品質、IMEI/MEID、使用周波数取得
•セキュリティ: VPNステータスと概要、ファイアーウォールリスト

セキュリティ
•VPN：IPSec、L2TP
•ファイアウォール:ステルスモード、IPS
•フィルタリング機能:パケットフィルタ、 MAC制御

管理
•設定装置: Web GUI、コマンドプロンプト
•管理ツール: SNMPv3 Std. & AMIT MIB
•システム:設定保存/復元、FWアップグレード
•診断機能:診断ツール

サービス
•セルラーツールキット: SMS、セルラーデータ使用量管理、通信スキャン
•イベント制御機能: 設定/通知/モニターイベントSMS、ログ、SNMPトラップ、Eメール通知
•ネットワークサービス: ダイナミックDNS、時刻設定
•スケジューリング: システムの再起動、機能のオン/オフ

環境条件
•動作/保存温度:-30° C ~ 70° C、-40° C ~ 85° C
•湿度:10%~95%（結露なきこと）
•外形寸法:93x90x27mm

認証
•認証取得:TELEC、JATE

付属品
•1 *デバイス、2*アンテナ(3dBi)
•1 * RJ45ケーブル(1.5M)

他の項目
•DC電源ジャックピン仕様：2.0（DS-210-20）
•適切なDCコネクタ:外径5.5mm / 内径2.1mm
•DINレールキット

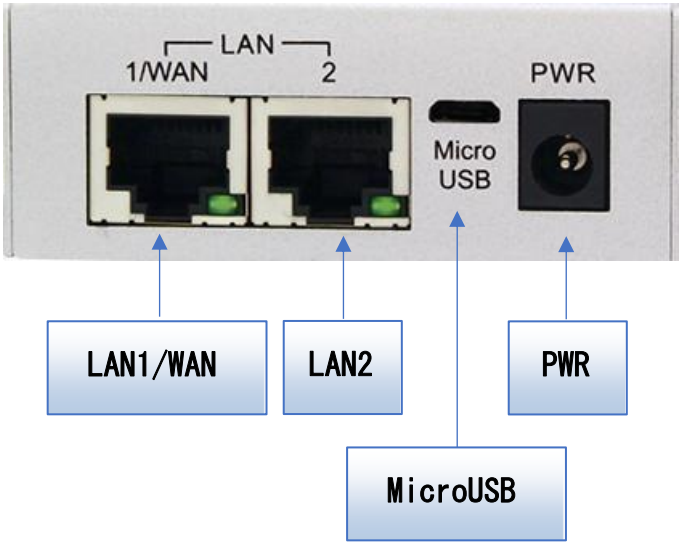
yy	Sku	Band	モジュール認証
JO	Japan	B1/B3/B8/18/19/41	docomo/SoftBank/au/楽天

※固定IP付きプランは楽天のみ

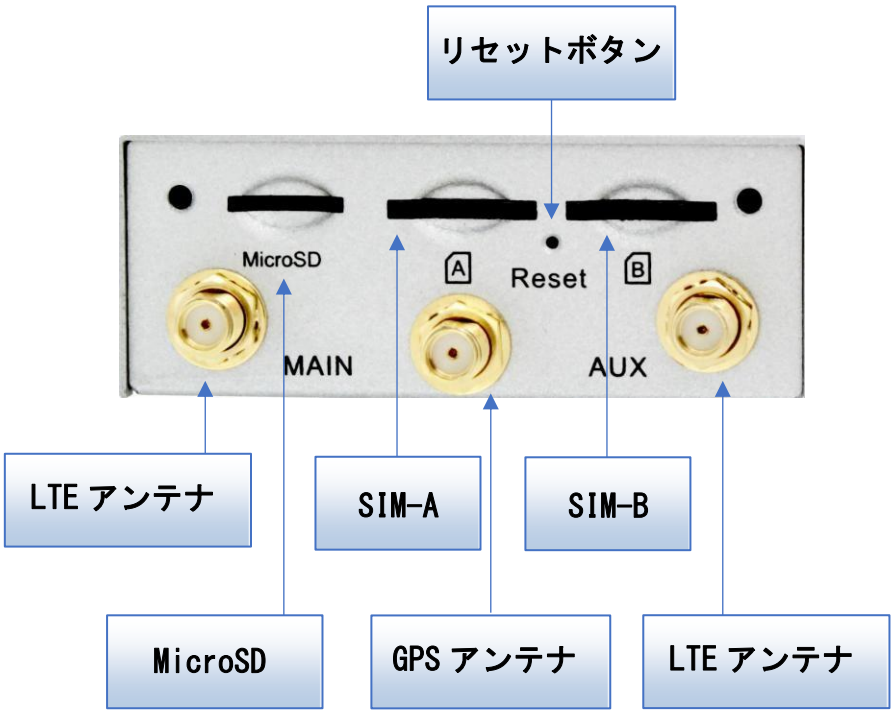
※固定 IP 付きプランの SIM については、楽天 SIM のみ動作検証済みです。
他キャリアの動的 IP プランの SIM については、インターネット接続のみ確認済みです。
SIM の契約プランによっては、外部公開サーバなどの利用はできません。
従量制プランでの SIM 利用は通信料金が高額になる可能性があるため推奨いたしません。

1-4. ハードウェア構成

➢ 左側



➢ 右側



※リセットボタン
リセットボタンを 6～8 秒間押し続けてから放すと（長押しすると）、デバイスが工場出荷時のデフォルトの設定に戻ります。

1-5. LED 表示

表示	LEDの色	説明
WAN Uplink Status	青色 赤色	LED の色が以下のように表示されるとき • **青色**： Cellular モジュールは、LTE モードです。 • **赤**： Cellular モジュールは、HSPA/3G モードです。 LED の動作が以下のようであるとき： • **点滅（高速）**： 信号強度は、0～30%です。 • **点滅（低速、1.5～2 秒に 1 回）**： 信号強度は、31～60%です。 • **常時点灯**： 信号強度は、61～100%です。
System Status	青色 赤色	**青色ー点滅（1 秒ごと）**：ゲートウェイは、正常に動作しています。 **赤色ー点滅（高速）**：ゲートウェイは、リカバリモードまたは異常状態にあります。
LAN1 LAN2 (RJ45)	緑色	**OFF**：イーサネットケーブルが接続されていないか、デバイスがリンクされていません。 **緑色**：イーサネット接続が確立されています。 **緑色のフラッシュ**：イーサネット経由で転送されるデータパケット。

1-6. 設置および保守に関する注意事項

1.5.1　システム要件

ネットワークの要件	·イーサネット RJ45 ケーブル ·3G/4G セルラーサービスに加入契約している ·PC にイーサネットアダプターが搭載されている
Web ベースの 構成ユーティリティの 要件	**次のものを搭載しているコンピュータ** ·Windows®、Macintosh、Linux ベースのオペレーティングシステム ·インストール済みのイーサネットアダプター **ブラウザーの要件**: ·Internet Explorer 6.0 以降 ·Chrome 2.0 以降 ·Firefox 3.0 以降 ·Safari 3.0 以降

1.5.2　警告・注意事項

注意

- 電源アダプタはパッケージに付属のもののみを使用してください。
  電圧定格が異なる電源アダプタの使用は危険を伴い、本製品に損傷が発生する場合がございます。
- ケースを開けて、修理や分解、改造をしないでください。
  火災、やけど、感電などの原因となります。
  本製品が非常に高温になっている場合は、ただちに電源を切断し、所定のサービスセンターに修理を依頼してください。
- 本製品は安定した場所に設置してください。
  傾き、ぐらつきのある台などに設置すると、落下の原因となります。
  本製品と付属品は屋外で使用しないでください。
- ほこりや湿気が多い場所、または高温になる場所での使用、保管は行わないでください。
- 従量制プランでの SIM 利用は通信料金が高額になる可能性があるため推奨いたしません。

1.5.3　表面温度に関する注意事項

- **金属製エンクロージャーの表面温度は、非常に高くなる恐れがあります。**
  ※特に、以下の場合に表面温度が高くなります。
  ・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
  ・高い周囲温度の空間に設置した場合

- **保守点検中に指で熱い表面に触れないようにしてください。**

1-7. ハードウェアの設置

本章では、ハードウェアの設置および構成方法について説明します。

1.6.1　設置方法

本装置は、デスクトップ上、または、壁に取り付けることができます。

1.6.2　SIM カードを挿入する

警告：SIM カードを挿入または交換する前に、必ずデバイスの電源を切断してください。

SIM カードスロットは、ハウジングの右側にあり、SIM カードを保護する役割があります。SIM カードの取り付けや取り外しを行う前に、外部 SIM カードを取り外す必要があります。
SIM カードを挿入または取り出しを行うには、次の手順に従ってください。
SIM カードを正しく取り付けてから、外部 SIM カードカバーを取り付けます。

ステップ 1： 以下の通り、ネジを緩め、SIM カバーを取り外します。	ステップ 2： SIM カードをスロット 1（SIM-A）またはスロット 2（SIM-B）に押し込みます。	ステップ 3: 挿入した SIM カードを再度押して、SIM スロットから取り出します。
		

1.6.3　電源の接続

パッケージには、DC5V/2A 電源アダプタ(最大消費電力は 5～6W)と 2 ピン端子ブロックがあり、DC 電源をこのゲートウェイに簡単に接続することができます。
ゲートウェイに他の DC 電源を使って給電する場合は、DC 電源の電圧が、5V～18V に従っており、電極がその割り当て（「+」は DC 電源用、「-」は GND 線用）に従って、正しく接続されていることを確認してください。

警告：この業務用電源アダプタは、主にこのデバイスを初期構成で使用する場合の電源に使用します。温度の幅が大きい環境での使用を目的としたものではありません。このデバイスに対応した他の業務用電源を用意または購入してください。

1.6.4　DIN レールを取り付ける

以下、取り付けイメージです。

1.6.5　ネットワーク、またはホストへの接続

本装置には、RJ45 ポート×1 があり、イーサネットに接続できます。また、ネットワークの伝送速度を自動検出し、自動構成を実行します。デバイスの RJ45 ポート（LAN）にイーサネットケーブルを接続し、イーサネットケーブルのもう一方の端部をコンピュータのネットワークポートに接続します。これにより、RJ45 イーサネットケーブルを使用して、デバイスをホスト PC のイーサネットポートに接続し、デバイスの構成を行うことができるようになります。

1.6.6　Web UI の構成・設定

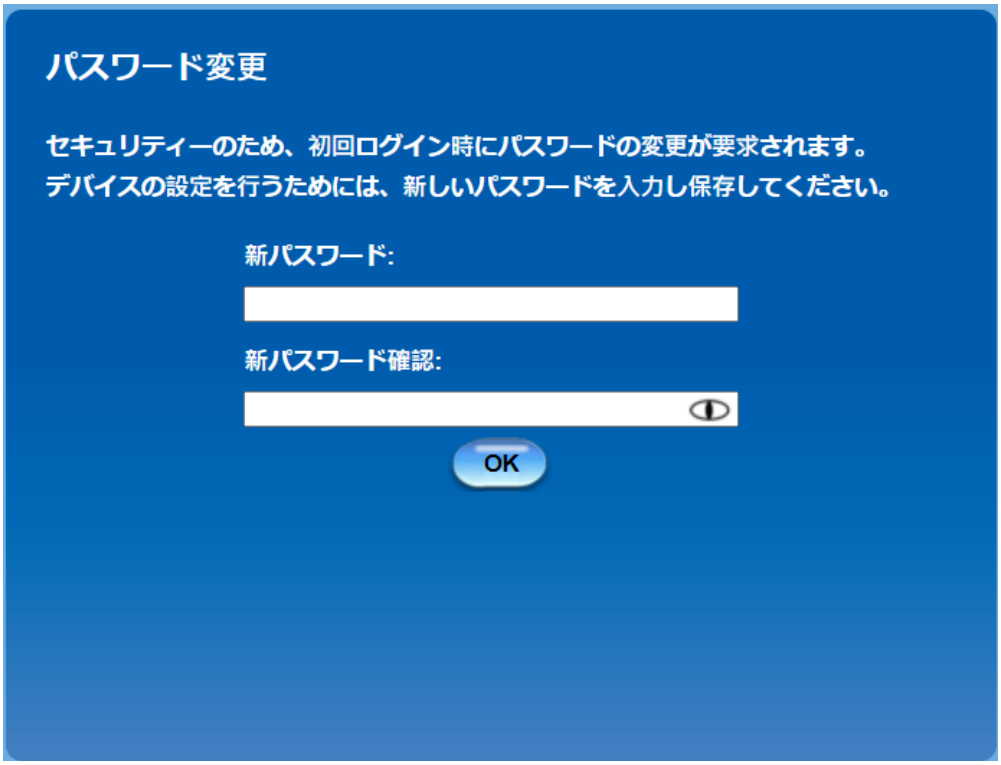
デバイスの構成は Web UI から行うことができます。
IP アドレス（http://192.168.123.254）*1 を入力します。

ログインページが表示されたら、ユーザー名とパスワード「admin」*2 を入力し、［ログイン)］ボタンをクリックします。
※［ログイン］ボタンをクリック後、リロードする必要がございます。

セキュリティのため、初回ログイン時にパスワードの変更を要求されます。
新しいパスワードを設定してください。
注:パスワードは 10 文字以上で、少なくとも 1 つの英字と 1 つの数字を含む必要があります。パスワードはログイン アカウントと同じにすることはできません。

*1：このゲートウェイのデフォルトの LAN IP アドレスは 192.168.123.254 です。
　　変更する場合は、新しい IP アドレスを使用して、ログインする必要があります。
*2：ログインパスワードは必ずデフォルト値から変更するようにしてください。

新しいパスワードを入力して再度ログインしてください



第2章. 基本ネットワーク

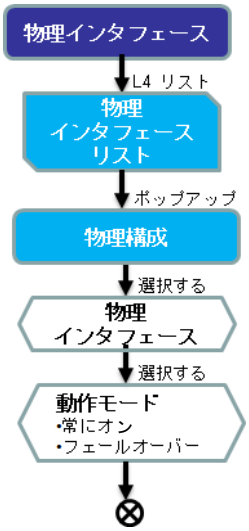
2-1. WAN＆アップリンク

基本ネットワーク ＞ [WAN＆アップリンク]

ゲートウェイは、二つの WAN インターフェイスを提供し、ゲートウェイのイントラネット内の全クライアントホストが ISP を介してインターネットにアクセスできるようにします。しかし、世界中の ISP は、様々な接続プロトコルを適用し、ゲートウェイまたはユーザーのデバイスを ISP にダイアルインさせ、その後、異なる種類の伝送媒体を介して、インターネットにリンクさせます。
したがって、WAN 接続により、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イントラネット用のインターネット設定を指定することができます。各 WAN インターフェイスに対して、最初に、物理インターフェイスを指定し、その後、ISP に接続するためのインターネットに設定を指定しなければなりません。

2.1.1　物理インターフェイス

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] タブ



物理インターフェイスリスト

インターフェイス名	物理インターフェイス	動作モード	アクション
WAN-1	モバイル NET(5G/LTE)	常にオン	編集
WAN-2	イーサネット	常にオン	編集

1 つの WAN インターフェイスを構成するための最初のステップは、「物理インターフェイス」ページに表示される通り、WAN 接続に対して、どの種類の接続媒体を使用するかを指定することです。
「物理インターフェイス」ページには、2 つの構成ウィンドウ（「物理インターフェイスリスト」および「インターフェイス構成)」）があります。
「物理インターフェイスリスト」ウィンドウには、利用可能なすべての物理インターフェイスが表示されます。
「物理インターフェイスリスト」ウィンドウで、インターフェイスに対する［編集］ボタンをクリックすると、「インターフェイス構成」ウィンドウが表示され、ここで、WAN インターフェイスを構成することができます。

物理インターフェイスの設定

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] タブに進みます。

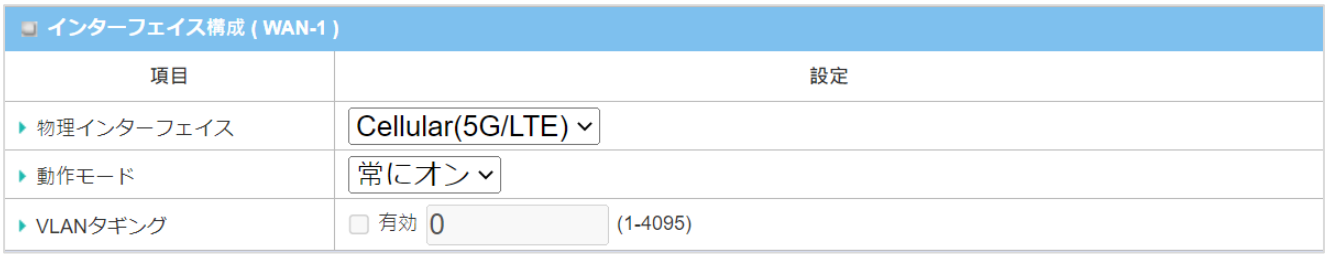
物理インターフェイスにより、物理 WAN インターフェイスを設定し、WAN の挙動を調整することができます。
注：利用可能な WAN インターフェイスの数は、購入したゲートウェイにより異なる場合があります。

［編集］ボタンが適用されると、インターフェイス構成画面が表示されます。
この例では、WAN-1 インターフェイスが使用されています。

物理インターフェイスリスト

インターフェイス名	物理インターフェイス	動作モード	アクション
WAN-1	モバイル NET(5G/LTE)	常にオン	編集

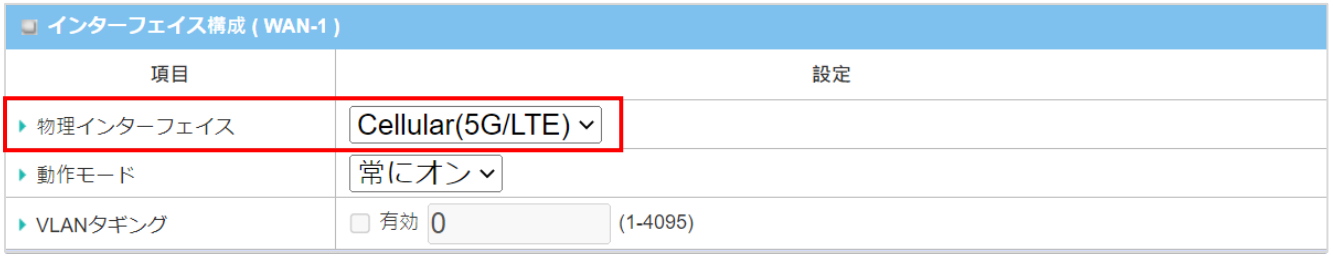
インターフェイス構成：



インターフェイス構成		
項目	**設定値**	**説明**
物理 インターフェイス	入力必須	ドロップダウンリストから、希望するインターフェイスを選択します。
動作モード	1. 入力必須 2. WAN-1は、一次インターフェースであり、デフォルトは、「常にオン」です	インターフェイスの動作モードを定義します。 このWANを常に有効にするには、「常にオン」を選択します。 注）「常にオン」は 、WAN-1の場合のみ利用可能です。
VLANタギング	任意の設定	「有効」ボックスにチェックを入れて、ISPにより提供されるタグ値を入力します。 入力値の範囲：1～4095です。 入力しない場合は、ボックスからチェックを外します。 注：この機能は、このゲートウェイに対して利用できません。

■物理インターフェイス：

- **イーサネット WAN**：ゲートウェイには、WAN 接続として構成できる 1 つ以上の RJ45 WAN ポートがあります。ファイアウォールデバイスの背後にある外部 DSL モデム、またはセットアップに直接接続できます。
- **モバイル NET WAN**：ゲートウェイには、WAN 接続として、1 つの内蔵 3G/4G セルラーがあります。各セルラーWAN に対して、特殊フェールオーバー機能用に挿入する 1 つ、または 2 つの SIM カードがあります。



注意

- SIM カードの挿入や取り外しを行う前に必ずゲートウェイの電源を切断してください。
- ゲートウェイの稼働中に SIM カードの挿入や取り外しを行うと、SIM カードが破損する恐れがあります。

■動作モード:

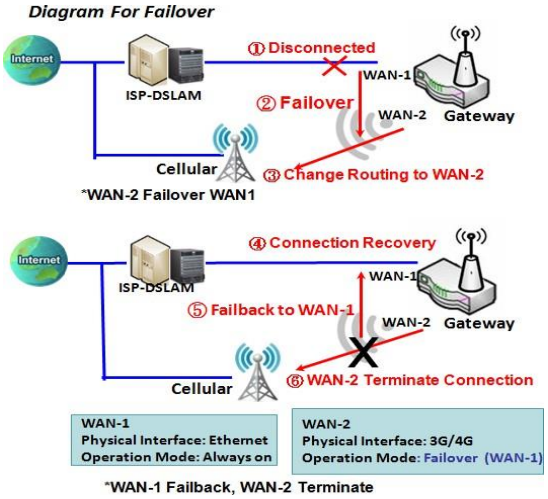
動作モード設定には、3 つの項目（「常にオン」、「フェールオーバー」、「無効」）があります。※シングル WAN デバイスの場合、「常にオン」のみが利用可能です。

インターフェイス構成 (WAN-1)

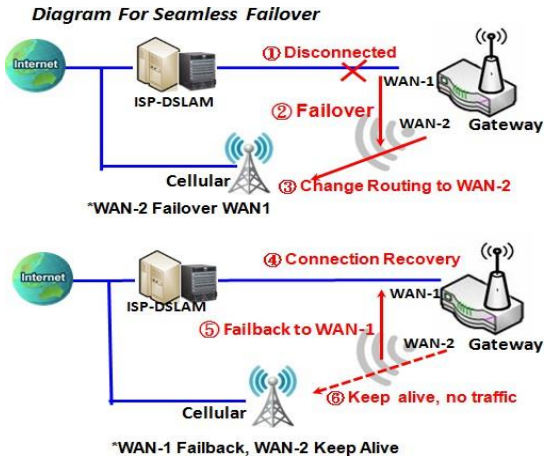
項目	設定
物理インターフェイス	Cellular(5G/LTE)
動作モード	常にオン
VLANタギング	有効 0 (1-4095)

- **常にオン**　　：この WAN インターフェイスを常に有効に設定します。

- **フェールオーバー**：フェールオーバーインターフェイスは、プライマリへのバックアップ接続です。これは、プライマリ WAN 接続が切断された場合にのみ、バックアップ接続が起動されてプライマリ接続の代わりになることを意味します。



図に示すように、WAN-2 は、WAN-1 のバックアップ WAN です。WAN-1 は、動作モード「常時オン」のプライマリ接続として機能します。WAN-1 が切断されるまで、WAN-2 はアクティブ化されません。WAN-1 接続が接続で復元されると、データトラフィックが再び引き継がれます。このとき、WAN-2 接続は終了します。



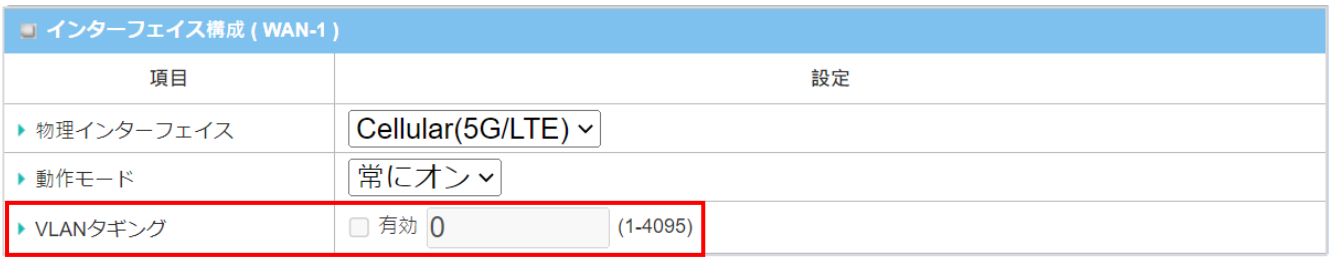
シームレスフェールオーバー、さらにフェールオーバー操作モードには、「シームレス」オプションがあります。構成ウィンドウで「シームレス」チェックボックスをオンにしてシームレスオプションを有効にすると、システムの再起動後にプライマリ接続とフェールオーバー接続の両方が起動されます。しかし、プライマリ接続だけがデータ転送を実行しますが、フェールオーバーは接続ラインを維持します。プライマリ接続が切断されると、システムはフェールオーバー接続のルーティングパスをフェールオーバー接続に切り替えることで、フェールオーバー接続がアクティブになってからダイヤルアップ時間を節約します。

「シームレス」有効チェックボックスがアクティブになると、システムの起動時にフェールオーバーインターフェイスを連続して接続できるようになります。フェールオーバーWAN インタ

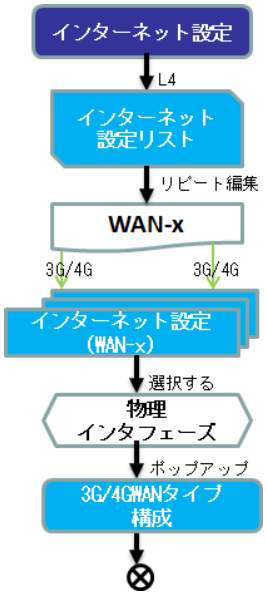
ーフェイスは、データトラフィックなしで接続を維持します。フェールオーバー処理中の切り替え時間を短縮することを目的としています。したがって、プライマリ接続が切断されると、フェールオーバーインターフェイスは、フェールオーバーインターフェイスへのルーティングパスを変更するだけで、即座にデータ転送ミッションを引き継ぎます。フェールオーバー接続のダイヤルアップ時間は、あらかじめ接続されているため保存されます。

■VLAN タギング:

一部の ISP は、特定のサービスに対してゲートウェイから VLAN タグを WAN パケットに挿入することを要求する場合があります。WAN 物理インターフェイスで、VLAN タギングを有効にし、タグを指定してください。イーサネットおよび ADSL 物理インターフェイスのみがこの機能をサポートすることに注意してください。VLAN タギングは、ゲートウェイに対しては、利用できません。



2.1.2　インターネット設定



基本ネットワーク ＞［WAN&アップリンク］＞［接続設定］タブ　に進みます。

各WAN接続に対する物理インターフェイスを指定した後、管理者は、ISPのダイアルインプロセスを満たすため、接続プロファイルを構成しなければなりません。これにより、ゲートウェイのイントラネット内の全クライアントホストが、インターネットにアクセスできるようになります。

「インターネット設定」ページには、いくつかの構成ウィンドウ（「インターネット接続リスト」、「インターネット接続構成」、「WANタイプ構成」および各WANタイプに対する関連構成ウィンドウ）があります。各WANインターフェイスのインターネット設定の場合、最初に物理インターフェイスの WANタイプを指定し、次に、そのWANタイプに対する関連パラメータ構成を指定しなければなりません。

「インターネット設定リスト」ウィンドウで、物理インターフェイスの[編集]ボタンをクリックすると、「インターネット接続構成」ウィンドウが表示されます。ここで、インターネット接続を行うための物理インターフェイスに対するWANタイプの種類を指定します。選択した WANタイプに基づき、対応する各構成ウィンドウにおいて、必要なパラメータを構成することができます。

・ インターネット接続リスト － イーサネット WAN

WAN-1、WAN-2 の［編集］から、各設定画面を表示します。

■イーサネットインターフェイスの WAN タイプ:

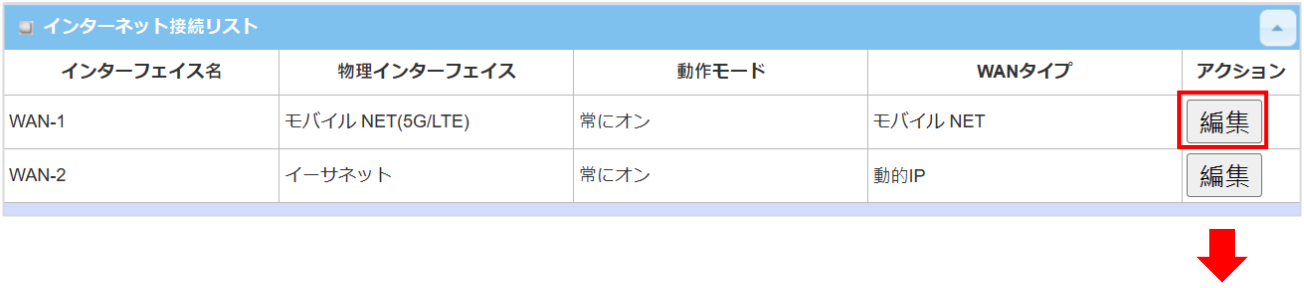
イーサネットは、M2M ゲートウェイ用の最も一般的な WAN＆アップリンクインターフェイスです。
通常、WAN 接続をセットアップするために、xDSL またはケーブルモデムに接続されています。ISP に接続するには、さまざまな WAN タイプがあります。

WAN タイプ	説明
静的 IP	ISP が固定 IP を提供する場合に、選択します。
動的 IP	DHCP サーバーにより WAN の割り当てられる IP アドレスは毎回異なります。
PPPoE	この WAN タイプは、ADSL 接続に広く使用されています。 通常、ダイヤルアップごとに IP が異なります。
PPTP	この WAN タイプは、ロシアなど一部の国で一般的です。
L2TP	この WAN タイプは、イスラエルなど一部の国で一般的です。

※PPTP、L2TP はサポートされていない機能です。

イーサネット WAN 設定の構成

［編集］ボタンが適用されると、「インターフェイス接続構成」画面が表示されます。
この例では、WAN-1 インターフェイスが使用されています。



・WAN タイプ = 動的 IP

選択すると、「動的 IP WAN タイプ構成」が表示されます。
項目、および設定に関する説明は、以下です。

動的 IP WAN タイプ		
項目	**設定値**	**説明**
ホスト名	任意の設定	サービスプロバイダから提供されたホスト名を入力します。
ISP 登録アドレス	任意の設定	サービスプロバイダに登録した MAC アドレスを入力します。 または、［複製］ボタンをクリックして、PC の MAC をこのフィールドに複製します。 通常、インターネットに接続するために割り当てられた PC の MAC アドレスです。

・WAN タイプ = 静的 IP

選択すると、「静的 IP WAN タイプ構成」が表示されます。

項目、および設定に関する説明は、以下です。

インターネット接続構成 (WAN - 1)

項目	設定
WANタイプ	静的IP

静的IPWANタイプ構成

項目	設定
WAN IPアドレス	
WANサブネットマスク	255.255.255.0 (/24)
WANゲートウェイ	
プライマリーDNS	
セカンダリーDNS	(選択的)

・WAN タイプ = PPPoE

選択すると、「PPPoE WAN タイプ構成」が表示されます。

項目、および設定に関する説明は、以下です。

インターネット接続構成 (WAN - 1)

項目	設定
WANタイプ	PPPoE

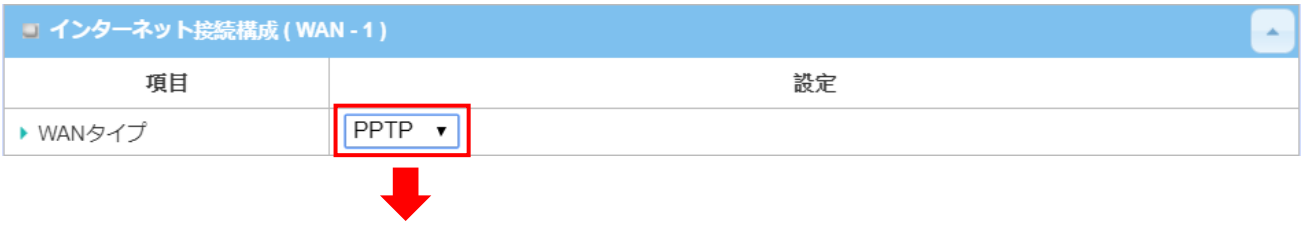
PPPoE WANタイプ構成

項目	設定
IP Type	IPv4
PPPoEアカウント	
PPPoEパスワード	
プライマリーDNS	(選択的)
セカンダリーDNS	(選択的)
サービス名	(選択的)
割り当てられたIPアドレス	(選択的)

・WAN タイプ = PPTP　　※PPTP はサポートされていない機能です。

選択すると、「PPTP WAN タイプ構成」が表示されます。

項目、および設定に関する説明は、以下です。

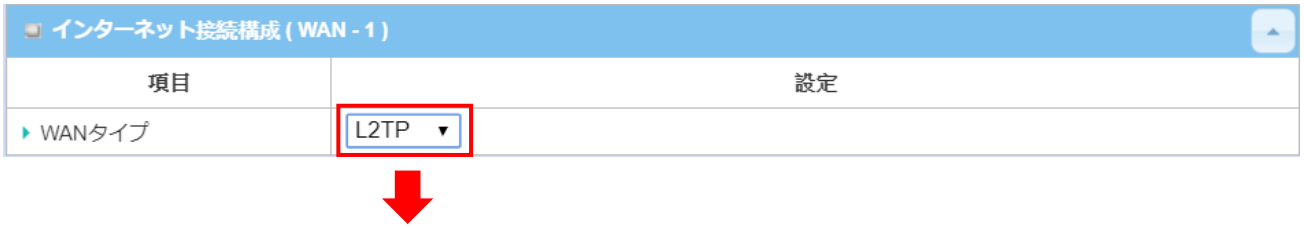


PPTP WAN タイプ		
項目	**設定値**	**説明**
IP モード	入力必須	PPTP インターネット接続の場合は、静的または動的 IP アドレスを選択します。 ■**静的 IP アドレス**を選択した場合、[WAN IP アドレス]、[WAN サブネットマスク]、および [WAN ゲートウェイ] を入力する必要があります。 ・WAN IP アドレス（入力必須）：サービスプロバイダから提供された WAN IP アドレスを入力します。 ・WAN サブネットマスク（入力必須）：サービスプロバイダから提供された WAN サブネットマスクを入力します。 ・WAN ゲートウェイ（入力必須）：サービスプロバイダから提供された WAN ゲートウェイの IP アドレスを入力します。 ■**動的 IP アドレス**を選択した場合、上記の設定は必要ありません。
サーバーIP アドレス/名	入力必須	PPTP サーバー名または IP アドレスを入力します。
PPTP アカウント	入力必須	サービスプロバイダから PPTP ユーザー名を入力します。
PPTP パスワード	入力必須	サービスプロバイダから提供された PPTP パスワードを入力します。
接続 ID	任意の設定	PPTP 接続を識別する名前を入力します。
MPPE	任意の設定	「有効」にチェックを入れると、PPTP 接続用の MPPE（MicrosoftPoint-to-Point Encryption）セキュリティが有効になります。

・WAN タイプ = L2TP　　※L2TP はサポートされていない機能です。

選択すると、「L2TP WAN タイプ構成」が表示されます。

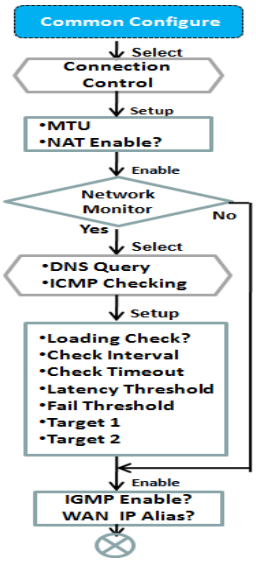
項目、および設定に関する説明は、以下です。



L2TP WAN タイプ		
項目	**設定値**	**説明**
IP モード	入力必須	L2TP インターネット接続の場合は、静的または動的 IP アドレスを選択します。 ■静的 IP アドレスが選択を選択した場合、[WAN IP アドレス]、[WAN サブネットマスク]、および [WAN ゲートウェイ] を入力する必要があります。 ・WAN IP アドレス（入力必須）： サービスプロバイダから提供された WAN IP アドレスを入力します。 ・WAN サブネットマスク（設定を入力しなければなりません）：サービスプロバイダから提供された WAN サブネットマスクを入力します。 ・WAN ゲートウェイ（入力必須）：サービスプロバイダから提供された WAN ゲートウェイの IP アドレスを入力します。 ■動的 IP を選択した場合、上記の設定は必要ありません。
サーバーIP アドレス/名	入力必須	L2TP サーバー名または IP アドレスを入力します。
L2TP アカウント	入力必須	サービスプロバイダから L2TP ユーザー名を入力します。
L2TP パスワード	入力必須	サービスプロバイダから提供された L2TP パスワードを入力します。
サービスポート	入力必須	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。選択できる項目は 3 つあります。 ・**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。

		・ユーザー定義：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。
MPPE	任意の設定	「有効」にチェックを入れると、PPTP 接続用の MPPE（MicrosoftPoint-to-Point Encryption）セキュリティが有効になります。

イーサネット接続の共通構成



ネットワーク監視構成

項目	設定
ネットワーク監視構成	☑ 有効
チェック方法	DNSクエリ
読み込み確認	☑ 有効
クエリ間隔	5 (秒)
レイテンシーしきい値	3000 (ms)
失敗しきい値	5 (回)
ターゲット1	DNS1
ターゲット2	なし

どの WAN タイプを設定した場合でも、重要なパラメータがいくつか設定されます。
構成するルールに従ってください。

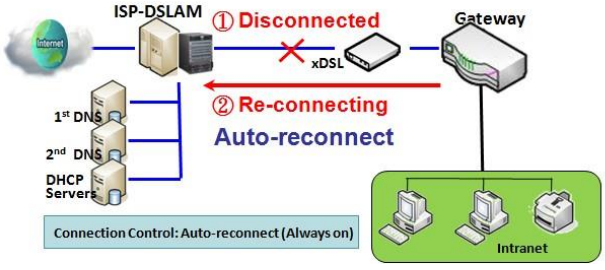
接続制御	自動再接続

NAT	☑ 有効
IGMP	無効
WAN IPエイリアス	☐ 有効

■接続制御

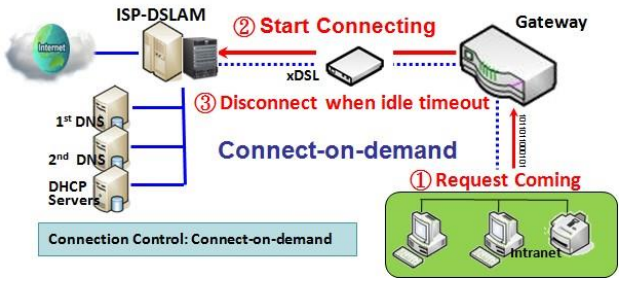
接続制御	自動再接続

・**自動再接続**：
このゲートウェイは、起動後に自動的にインターネット接続を確立し、接続が切断されると再接続を試みます。重要な用途で使用する場合は、このオプションを選択して、常時インターネット接続を確保することをお勧めします。



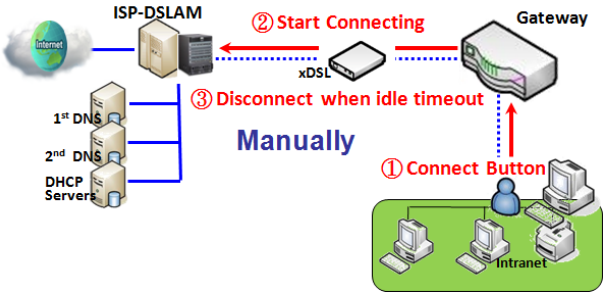
・**オンデマンド接続**：

このゲートウェイは、ローカルデータを WAN 側に送信する時点までインターネット接続の確立を開始しません。LAN と WAN の間で通常のデータ転送が行われた後、アイドル時間が［最大アイドル時間］の値に達すると、このゲートウェイは WAN 接続を切断します。



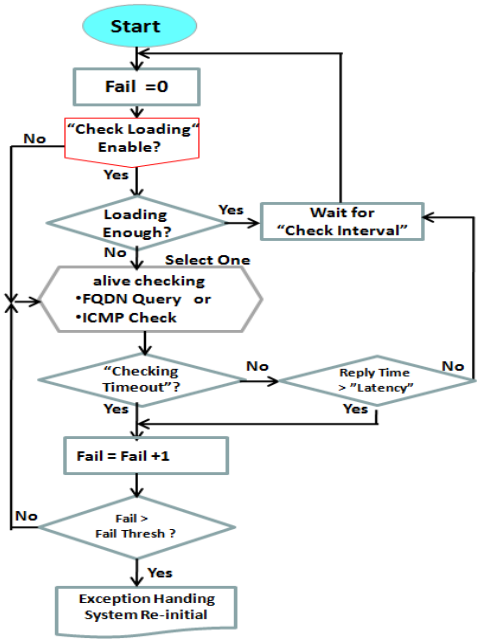
・**手動**：

このゲートウェイは、Web UI で、[接続]ボタンを押すまで、WAN 接続の確立を開始しません。 LAN と WAN の間で通常のデータ転送が行われた後、アイドル時間が［最大アイドル時間］の値に達すると、このゲートウェイは WAN 接続を切断します。



WAN インターフェイスが、フェールオーバーロールの別の WAN インターフェイスのプライマリインターフェイスとして機能する場合、システムが「(自動再接続（常にオン)」に設定する必要があるため、[接続制御］パラメータを構成できません。

ネットワーク監視



継続的に接続状態を監視する必要があります。これを行うには、「ICMP 確認」と「FQDN クエリ」を使用して確認します。接続トラフィックがある場合、パケットの確認は帯域幅を浪費します。応答されるパケットの応答時間も増加する可能性があります。「ネットワーク監視」が異常に動作しないようにするには、「負荷の確認」を有効にすると、トラフィックがあるときに接続確認を停止します。別の「確認間隔」を待機してから、もう一度、読み込みを確認します。

「ネットワーク監視」を行うとき、「待ち時間」よりも応答時間が長い場合、または「タイムアウトの確認」よりも応答がない場合、「失敗」カウントが増加します。継続し、「失敗」カウントが、「失敗しきい値」より大きい場合、ゲートウェイは、例外ハンド

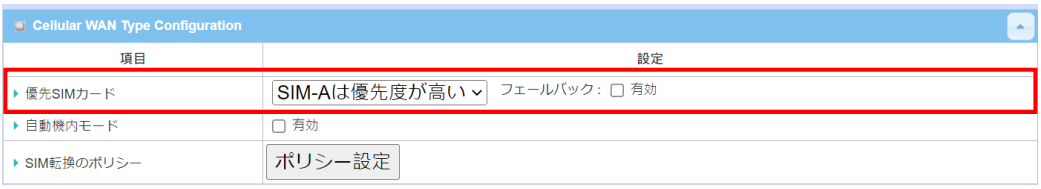
リングプロセスを実行し、この接続を再度初期化します。そうしなければ、ネットワーク監視プロセスが再び開始されます。

イーサネット接続の共通構成を設定する

イーサネットWANの共通構成		
項目	**設定値**	**説明**
接続制御	入力必須	・**自動再接続**が選択されている場合： 常に、インターネット接続を維持することを意味します。 ・**オンデマンド接続**が選択されている場合： データトラフィックが検出されたときのみ、インターネット接続が確立されることを意味します。 ・**手動接続**が選択されている場合： 手動で接続をダイアルアップするために、[接続]ボタンをクリックする必要があることを意味します。 詳細は、ステータス > 基本ネットワーク > 「WAN&アップリンク」タブに進んでください。 注_1：このフィールドは、基本ネットワーク > 物理インターフェイス > 「動作モード」が、「常にオン」に選択されている場合のみ利用可能です。 注_2：自動接続が選択されているとき、自動再接続が正常に動作していることを確認するため、別なネットワーク監視機能を有効化しなければなりません。
最大アイドル時間	1. 任意の設定 2. デフォルトは、「600秒」です	接続アイドルタイムアウト時にインターネット接続を切断する最大アイドル時間を指定します。 値の範囲：300～86400 注：このフィールドは、接続制御スキームとして、「オンデマンド接続」、または「手動接続」が選択されている場合のみ利用可能です。
MTU設定	1. 入力必須 2. デフォルトは、「0」です 3. 文字列形式：整数	MTU（最大伝送単位）を指定します。 値の範囲：512～1500（自動の場合は、0 を設定します）
NAT	デフォルトは、チェックありです	ボックスのチェックを外して、NAT 機能を無効化します。
ネットワーク監視構成	1. 任意の設定 2. デフォルトは、有効です	ネットワーク監視機能が有効化されているとき、ゲートウェイは、DNS クエリまたは ICMP を使って、インターネット接続（接続中または切断中）を定期的に確認します。 ・**DNS クエリ**、または **ICPM チェッキング**を選択して、WAN リンクを検出します。DNS クエリを使って、システムは、DNS クエリパケットをターゲット 1、およびターゲット 2 で指定される宛先に送信することにより、接続を確認します。

		ICMP チェッキングを使って、システムは、ICMP 要求パケットを指定された宛先に送信することにより、接続を確認します。 ・**読み込み確認**を有効化することにより、帯域幅が完全に占有去れている場合、ルーターに未応答の DNS クエリまたは ICMP 要求を無視することを許可します。これにより、偽リンクダウンステータスを防ぐことになります。 ・**クエリ/確認間隔**は、2 つの DNS クエリまたは ICMP チェッキングパケット間の伝送間隔を定義します。 値の範囲：2～30 秒 ・**確認タイムアウト**は、各 DNS クエリ/ICMP のタイムアウトを定義します。 値の範囲：2～5 秒 ・**レイテンシーしきい値**は、応答時間のしきい値を定義します。 値の範囲：2000（1000 回分の確認タイムアウト）ミリ秒以上 ・**失敗しきい値**は、ルーターが、WAN リンクダウンステータスを認識する前の検出される切断を指定します。切断を確認する前にしきい値に対する切断検出時間を入力します。 値の範囲：2～10 秒 ・**ターゲット 1**（デフォルトでは、DNS1 が設定）は、DNS クエリ/ICMP 要求を送信する最初のターゲットを指定します。 ■DNS1：ターゲットにあるプライマリ DNS を設定します。 ■DNS2：ターゲットであるセカンダリ DNS を設定します。 ■Other Host（他のホスト）：ターゲットである IP アドレスを入力します。 ・**ターゲット 2**（デフォルトでは、None（なし）が設定）は、DNS クエリ/ICMP 要求を送信する 2 番目のターゲットを指定します。 ■None（なし）：ターゲット 2 を無効化します。 ■DNS1：ターゲットにあるプライマリ DNS を設定します。 ■DNS2：ターゲットであるセカンダリ DNS を設定します。 ■Other Host（他のホスト）：ターゲットである IP アドレスを入力します。 注：自動再接続を接続制御スキームとして選択した場合、デフォルトで、ネットワーク監視機能は有効化されます。オンデマンド接続または手動接続の場合、それを無効化しても、自動再接続に変更すると、有効化チェックボックスに自動的にチェックが入ります。
IGMP	デフォルトは、無効です	自動を選択し、IGMP 機能を有効化します。 有効化ボックスにチェックを入れて、IGMP ゲートウェイを有効化します。
WAN IP エイリアス	1. デフォルトは、チェックなしです 2. 文字列形式：IP アドレス（IPv4タイプ）	ボックスにチェックを入れて、WAN IP エイリアスを有効化し、割り当てる IP アドレスを入力します。
保存	該当なし	[保存]ボタンをクリックし、構成を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックし、構成した内容を元の設定に復元します。

・ インターネット接続 － モバイル NET



優先の SIM カード － デュアル SIM フェールオーバー

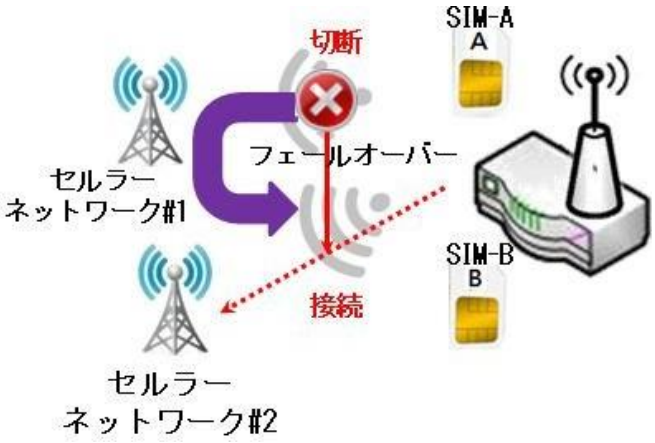
モバイル NET 組み込みデバイスの場合、1 つの組み込みセルラーモジュールは、1 つの WAN インターフェイスのみを作成することができます。このデバイスは、1 つのモジュールに対して、デュアル SIM カードを用いることにより、特殊フェールオーバーメカニズムを備えています。これは、デュアル SIM フェールオーバーと呼ばれます。この機能は、地理的位置が変更されたとき、ISP 切り替えを行う場合に有用です。

「デュアル SIM フェールオーバー」には、「フェールバック」を有効、または無効した状態での「SIM-A は優先度が高い」、「SIM-B は優先度が高い」、「SIM-A のみ」および「SIM-B のみ」を含む様々な利用シナリオがあります。

・SIM-A/SIM-B のみ：

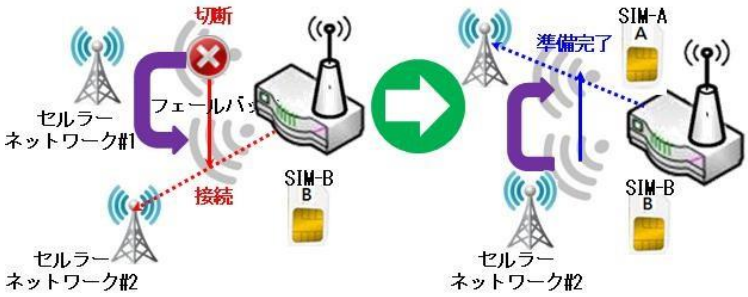
「SIM-A のみ」または「SIM-B のみ」を使用する場合、ゲートウェイデバイスとセルラー ISP の間のネゴシエーションパラメータとして、指定した SIM カードスロットしか使用されません。

・SIM-A / SIM-B は優先度が高い（フェールバック有効無し）：



デフォルトでは、セルラーISP に対するデータ転送に「SIM-A は優先度が高い」が使用されます。
「SIM-A は優先度が高い」または「SIM-B は優先度が高い」状態の場合、ゲートウェイは、最初に、SIM-A または SIM-B カードを使用することにより、インターネットへの接続を試みます。接続が切断されたとき、ゲートウェイは、自動的に代替用の他の SIM カードを使用するように切り替わります。そして、現在の SIM 接続がされるという例外を除き、元の SIM カードを使用しようするよう、スイッチバックすることはありません。つまり、SIM-A と SIM-B は交互に使用されますが、どちらが使用されている場合でも、現在の接続が継続されている間は引き続きデータ転送に使用されます。

・SIM-A / SIM-B は優先度が高い（フェールバック有効有り）：



フェールバックを有効にした「SIM-A は優先度が高い」シナリオは、接続が切断され、ゲートウェイシステムは、SIM-B を使用するように切り替わるときに使用されます。そして、SIM-A 接続が回復すると、元の SIM-A カードを使用するよう、スイッチバックします。

Cellular（4G/LTE） 設定の構成

インターネット接続リストに Cellular(4G/LTE) WAN 設定の構成が表示されます。
［編集］ボタンをクリックして、構成します。
詳細設定については、以下のページに従います。

インターネット接続リスト

インターフェイス名	物理インターフェイス	動作モード	WANタイプ	アクション
WAN-1	Cellular(5G/LTE)	常にオン	モバイル NET	編集
WAN-2	-	無効	-	編集

Cellular WAN 接続構成		
項目	**設定値**	**説明**
WANタイプ	1. 入力必須 2. デフォルトは、「モバイルNET」です	ドロップダウンボックスから、Cellular WAN 接続に対するインターネット接続方法を選択します。 モバイル NET のみが利用可能です。
優先SIMカード	1. 入力必須 2. デフォルトは、「SIM-Aは優先度が高い」です 3. デフォルトは、「フェールバック」のチェックはなしです	接続用にどの SIM カードを使用するかを選択します。 「SIM-A は優先度が高い」または「SIM-B は優先度が高い」が選択されている場合、SIM A/SIM B を使って接続が確立されることを意味します。 そして、接続に失敗した場合、他の SIM カードに切り替わり、接続が確立するまで、再度ダイアルを試みます。 「SIM-A のみ」 または「SIM-B のみ」が選択されている場合、選択した SIM カードのみを使って、ダイアルアップを試みます。 フェールバックにチェックが入っていると、接続が選択されたメイン SIM を用いるダイアルアップではない場合、メイン SIM にフェールバックし、定期的に接続の確立を試みることを意味します。 注_1：シングル SIM 設計の製品の場合、「SIM-A のみ」が利用可能です。 注_2：フェールバックは、「SIM-A は優先度が高い」または「SIM-B は優先度が高い」が選択されているときのみ利用可能です。
自動機内モード	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、機能を有効にします。 デフォルトでは、オートフライトモードを無効にすると、セルラーモジュールは常に携帯電話タワーで物理チャネルを占有します。 それは即座にデータ接続を得ることができ、管理 SMS は常に必要な時に受信できます。 自動機内モードを有効にすると、ゲートウェイは「フライトモードでデータセッションがオフラインになると携帯機能が誤動作する」というメッセージを表示し、携帯電話モジュールを自動機内モードにします。さらに、セルラーモジュールが故障したプライマリ接続をバックアップするためのデータ接続に使用されるときはいつでも、セルラーモジュールはアクティブになり、セルラータワーに接続し、データ接続を取得します。 注：セルラーISP が接続されているゲートウェイに自動機内モードを有効にするように、要求されない限り、チェックしないでください。

SIM転換の ポリシー		※本項目は対応しておりません。

ポリシー設定を構成する　※本項目は対応しておりません。

ポリシー設定

項目	設定
接続失敗	0 (1-10) 回
RSSI監視	有効 しきい値: - 0 (-90~-113 dBm)
ネットワーク・サービス	有効 LTE信号なし: 0 (1~30 分)
ローミング・サービス	有効 タイムアウト: 0 (1~30 分)

SIM-A/SIM-B カードを構成する

ここでは、状況または要件に応じて、セルラー接続に対する構成を設定することができます。

SIM-Aカードとの接続

項目	設定
ネットワークタイプ	自動
ダイアルアッププロファイル	手動設定
APN	
IPタイプ	IPv4
PINコード	(選択的)
ダイヤルナンバー	(選択的)
アカウント	(選択的)
パスワード	(選択的)
認証	CHAP
IPモード	動的IP
プライマリーDNS	1.1.1.1 (選択的)
セカンダリーDNS	4.4.4.4 (選択的)
ローミング	有効

注_1：SIM-B カードの構成は、SIM-A カードの構成と同じ規則に従います。
ここでは、例として、 SIM-A を一覧表示します。
注_2：「SIM-A または SIM-B は優先度が高い」 が選択されている場合のみ、SIM-A カードによる接続、および SIM-B カードによる接続の両方がポップアップ表示されます。
そうでない場合は、それらの一方のみがポップアップ表示されます。

SIM-A/SIM-B APN プロファイルの設定		
項目	**設定値**	**説明**
ネットワークタイプ	1. 入力必須 2. デフォルトは、「自動」です	**「自動」**を選択すると、ネットワークタイプにかかわらず、自動的にネットワークが登録されます。 LTE ネットワークのみを登録するには、**「LTE のみ」**を選択します。 注：選択肢は、モデルの仕様により、異なる場合があります。
ダイアルアッププロファイル	1. 入力必須 2. デフォルトは、「手動構成」です	ご利用のモバイル NET ネットワークに対するダイアルアッププロファイルのタイプを指定します。 「手動構成」、「APN プロファイルリスト」、「自動」のいずれかになります。 ・**「手動構成」**を選択し、「アクセスポイント名」、「ダイアル番号」、「アカウント」、および「パスワード」をご利用のキャリアが提供した内容で設定します。 ・**「APN プロファイルリスト」**を選択し、接続が確立されるまで、順番にダイアルアップする複数のプロファイルを設定します。新しいフィールドがポップアップ表示されます。詳細については、基本 ネットワーク ＞ WAN およびアップリック ＞ インターネット設定 ＞ SIM-A APN プロファイルリストに進んでください。 ・SIM カードの IMSI をメーカーのデータベース内に一覧表示される記録と比較することにより、ダイアルアップ中に必要なすべての構成を自動的に取得するには、**「自動検出」**を選択します。 注_1：加入契約に対するネットワークを指定するために、「手動」または 「APN プロファイルリスト」を選択することを強く推奨します。 ISP は、加入者に対して、このようなネットワーク設定を必ず提供します。 注_2：Auto-detection（自動検出）を選択した場合、不適切なネットワークに接続、またはご利用の ISP に対する有効な APN を検索できない可能性があります。
APN	1. 入力必須 2. 文字列形式：任意のテキスト	接続を確立するために使用する APN を入力します。 ダイアルアッププロファイルスキームとして、**「手動構成」**を選択した場合、必須入力です。
IP タイプ	1. 入力必須 2. 文字列形式：IP アドレス（IPv4）	Cellular ネットワークが提供するネットワークサービスの IP タイプを指定します。IPv4、IPv6、または IPv4/6 から選択が可能です。 ※IPv6 は、本製品では対応しておりません。
PIN コード	文字列形式：整数	ご利用の SIM カードをロック解除するために必要な場合は、PIN を入力します。

ダイヤルナンバー	文字列形式：任意のテキスト	接続を確立するために使用する APN を入力します。 ※ダイアルアッププロファイルスキームとして、**「手動設定」**を選択した場合、表示する項目です。
アカウント	文字列形式：任意のテキスト	認証に使用するアカウントを入力します。 値の範囲：0～53 文字 ※ダイアルアッププロファイルスキームとして、**「手動設定」**を選択した場合、表示する項目です。
パスワード	文字列形式：任意のテキスト	認証に使用する パスワードを入力します。 ※ダイアルアッププロファイルスキームとして、**「手動設定」**を選択した場合、表示する項目です。
認証	1.入力必須 2 デフォルトは、「自動」です	**・PAP**（パスワード認証プロトコル）を選択し、そのプロトコルを使ってキャリアのサーバーにより認証します。 **・CHAP**（チャレンジハンドシェイク認証プロトコル）を選択し、そのプロトコルを使って、キャリアのサーバーにより認証します。 **・自動**が選択されているとき、PAP または CHAP いずれかのサーバーにより認証します。 ※ダイアルアッププロファイルスキームとして、**「手動設定」**を選択した場合、表示する項目です。
IP モード	1.入力必須 2 デフォルトは、「動的 IP」です	**「動的 IP」**が選択されているとき、キャリアのサーバーから、すべての IP 構成を取得し、デバイスを直接設定します。 キャリアにより提供された固有のアプリケーションを有している場合、または、独自の IP 構成を設定する場合は、「スタティック IP」モードに切り替え、IP アドレス、サブネットマスクおよびゲートウェイなどの必要なすべてのパラメータを入力します。 注：「IP サブネットマスク」は入力必須です。 正しく構成されていることを確認してください。
プライマリーDNS	文字列形式：IP アドレス（IPv4 タイプ）	IP アドレスを入力し、プライマリーDNS 設定を変更します。 入力されていない場合、ダイアルアップ中に、キャリアによりサーバーアドレスが与えられます。

SIM-A/SIM-B APN プロファイルリストの作成/編集

接続用に新しい APN プロファイルを追加したり、追加した APN プロファイルの内容を編集したりすることができます。
これは「ダイアルアッププロファイル」で「APN プロファイルリスト」を選択しているときのみ利用可能です。
確認および変更しやすいよう、作成したすべての APN プロファイルが一覧表示されます。
［追加］ボタンが適用されると、「APN プロファイルの設定」画面を表示します。

SIM-A/SIM-B APN プロファイルの設定		
項目	**設定値**	**説明**
プロファイル名	1. デフォルトは、「Profile-x」です 2. 文字列形式：任意のテキスト	プロファイルに対して記述するプロファイル名を入力します。
APN	文字列形式：任意のテキスト	接続を確立するために使用する APN を入力します。
IP Type	1. 入力必須 2. デフォルトは、「IPv4」です	IPv4 ネットワークを利用するには、IPv4 を選択します。 IPv6 ネットワークを利用するには、IPv6 を選択します。 IPv4 と IPv6 ネットワークを利用するには、IPv4/6 を選択します。 ※IPv6 は、本製品では対応しておりません。

アカウント	文字列形式：任意のテキスト	認証に使用するアカウントを入力します。 値の範囲： 0～53 文字
パスワード	文字列形式：任意のテキスト	認証に使用するパスワードを入力します。
認証	1. 入力必須 2. デフォルトは、「自動」です	モバイル NET 接続に対する認証方法を選択します。 自動、PAP、CHAP、または、None（なし）を選択することができます。
優先度	1. 入力必須 2. 文字列：整数	ダイアルアップ順序に対する値を入力します。有効な値は、1～16 です。最も小さい番号が割り当てられたプロファイルを使って、ダイアルアップを開始します。 値の範囲： 1～16
プロファイル	デフォルトは、チェックありです	ボックスにチェックを入れて、このプロファイルを有効します。 ダイアルアップ操作において、このプロファイルを無効するには、ボックスのチェックを外します。
保存	該当なし	「保存」ボタンをクリックして、構成を保存します。
キャンセル	該当なし	「キャンセル」ボタンをクリックして、構成した内容を元の設定に復元します。

モバイル NET 接続の共通構成の設定

Cellular(4G/LTE)に対する共通構成を変更することができます。

モバイル NET 接続の共通設定		
項目	**設定値**	**説明**
接続制御	デフォルトは、「自動再接続」です	・**「自動再接続」**が選択されている場合 物理リンクが接続されている場合、常に、インターネット接続を維持することを意味します。 ・**「オンデマンド接続」**が選択されている場合 データトラフィックが検出されたときのみ、インターネット接続が確立されることを意味します。 ・**「手動接続」**が選択されている場合 手動で接続をダイアルアップするために、[接続]ボタンをクリックする必要があることを意味します。 詳細は、ステータス > 基本ネットワーク > 「WAN＆アップリンク」タブに進んでください。

		注_1：このフィールドは、基本ネットワーク ＞ WAN ＞ 物理インターフェイス ＞ 「動作モード」が、「常にオン」に選択されている場合のみ利用可能です。 注_2：自動接続が選択されているとき、自動再接続が正常に動作していることを確認するため、別なネットワーク監視機能を有効しなければなりません。
最大アイドル時間	1. 任意の設定 2. デフォルトは、「600 秒」です	接続アイドルタイムアウト時にインターネット接続を切断する最大アイドル時間を指定します。 値の範囲：300～86400 注：このフィールドは、接続制御スキームとして「オンデマンド接続」、または「手動接続」が選択されている場合のみ利用可能です。
時間 スケジュール	1. 入力必須 2. デフォルトは、「(0)常時」です	「(0)常時」が選択されている場合、この WAN は、常に動作中であることを意味します。 別なスケジュールルールを設定したい場合は、選択する他のオプションがあります。詳細については、オブジェクト定義 ＞スケジュール設定に進んでください。
MTU 設定	1. 入力必須 2. デフォルトは「1430」です 3. 文字列形式：整数	モバイル NET 接続に対する MTU（最大伝送単位）を指定します。 値の範囲：512～1500（自動の場合は、0 を設定します）
IP パススルー（セルラーブリッジ）	1. デフォルトは、チェックなしです 2. Fixed MAC（固定 MAC）に対する文字列形式：MAC アドレス（例えば、00:50:18:aa:bb:cc）	「有効」ボックスにチェックが入っている場合、デバイスは、初めて接続するローカル LAN クライアントに対して、直接 WAN IP を割り当てることを意味します。 しかし、Fixed MAC（固定 MAC）に非ゼロ値が入力されている場合、この MAC アドレスを持つクライアントのみが、WAN IP アドレスを取得できることを意味します。 注 1：このフィールドは、モバイル NET-n が、WAN-1 に設定されている場合のみ利用可能です。 注 2：IP パススルーがオンである場合、NAT および WAN IP エイリアスは、機能が再度無効されるまで利用できません。
NAT	デフォルトは、チェックありです	有効ボックスのチェックを外して、NAT 機能を無効します。
IGMP	デフォルトは、「無効」です	「自動」を選択し、IGMP 機能を有効します。 有効ボックスにチェックを入れて、IGMP ゲートウェイを有効します。
WAN IP エイリアス	1. デフォルトは、チェックなしです 2. 文字列形式： IP アドレス（IPv4 タイプ）	有効ボックスにチェックを入れて、「WAN IP エイリアス」を有効し、割り当てる IP アドレスを入力します。

ネットワーク監視構成

項目	設定値	説明
ネットワーク監視構成	デフォルトは、チェックあり（有効）です	有効ボックスにチェックを入れると、ネットワーク監視機能が有効になります。
チェック方法	デフォルトは、「DNS クエリ」です	「DNS クエリ」、または「ICPM チェック」を選択して、WAN リンクを検出します。 「DNS クエリ」を使って、システムは、DNS クエリパケットをターゲット 1、およびターゲット 2 で指定される宛先に送信することにより、接続を確認します。 「ICPM チェック」を使って、システムは、ICMP 要求パケットを指定された宛先に送信することにより、接続を確認します。
読み込み確認		ゲートウェイは、WAN&インターフェイスを介して転送されたパケットがあることを検出すると、「特定のパケット」の送信を停止します。 **・レイテンシーしきい値（待ち時間しきい値）**： アプリケーションの接続が良好である必要がある場合は、この関数を使用することをお勧めします。 **・失敗しきい値**： ルーターが、WAN リンクダウンステータスを認識する前の検出される切断を指定します。切断を確認する前にしきい値に対する切断検出時間を入力します。
クエリ間隔		クエリ間隔は、「チェック方法」項目の「DNS クエリ」、または「ICPM チェック」の間の送信間隔を定義します。
デフォルト 1	デフォルトは、「DNS1」です	デフォルト 1（デフォルトは、DNS1）は、DNS クエリ/ICMP 要求を送信する最初のターゲットを指定します。 DNS1：ターゲットにあるプライマリーDNS を設定します。 DNS2：ターゲットであるセカンダリーDNS を設定します。 ゲートウェイ：現在のゲートウェイをターゲットに設定します。 他のホスト：ターゲットである IP アドレスを入力します。

デフォルト 2	デフォルトは 、「なし」です	デフォルト 2 は、DNS クエリ/ ICMP 要求を送信する 2 番目のターゲットを指定します。 なし：2 番目のターゲットは必要ありません。 DNS1：ターゲットにあるプライマリーDNS を設定します。 DNS2：ターゲットであるセカンダリーDNS を設定します。 ゲートウェイ：現在のゲートウェイをターゲットに設定します。 他のホスト：ターゲットである IP アドレスを入力します。
保存	該当なし	[保存]ボタンをクリックして、構成を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、構成した内容を元の設定に復元します。

2-2. LAN および VLAN

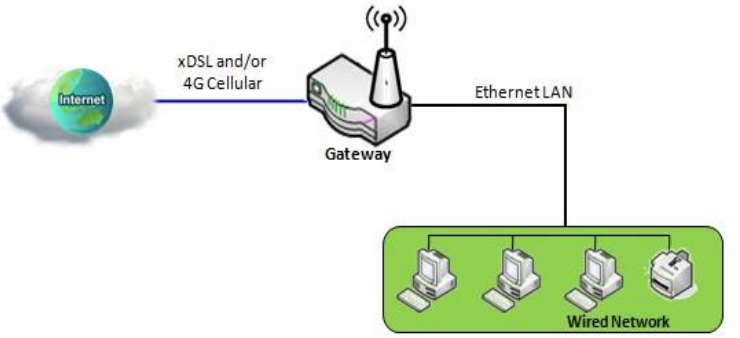
この選択により、LAN および VLAN の構成が提供されます。
VLAN は、オプション機能です。購入したゲートウェイの製品仕様に依存します。

基本ネットワーク ＞ [LAN および VLAN]

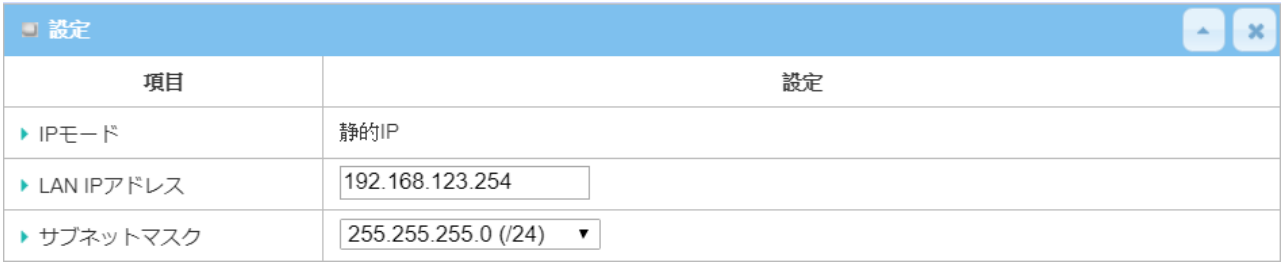
2.2.1 イーサネット LAN

基本ネットワーク ＞ [LAN および VLAN] ＞ [イーサネット LAN] タブを開きます。

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。
次の図は、コンピュータを配線して相互接続するネットワークを示しています。



IPv4 イーサネット LAN 設定を行うには、次の手順に従ってください。



項目	設定値	説明
IP モード	該当なし	関連する構成に従って、ゲートウェイの LAN IP モードを示します。

		・**静的 IP**:少なくとも 1 つの WAN インターフェイスが有効になっている場合、LAN IP モードは、静的 IP モードで固定されます。 ・**動的 IP**：使用可能な WAN インターフェイスがすべて無効になっている場合、LAN IP モードは、動的 IP モードになります。
LAN IP アドレス	1. 入力必須 2. デフォルトで 、192.168.123.254 が設定されています	本デバイスのローカル IP アドレスを入力します。 ネットワーク上のネットワークデバイスは、本デバイスの LAN 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。この設定は必要があれば変更することができます。 注：これは Web UI の IP アドレスでもあります。変更した場合、Web UI を表示するにはブラウザに新しい IP アドレスを入力する必要があります。
サブネットマスク	1. 入力必須 2. デフォルトで、255.255.255.0（/24）が設定されています。	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	該当なし	[保存]ボタンをクリックして、構成を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、構成した内容を元の設定に復元します。

追加 IP の作成/編集

本ゲートウェイは、特別な管理のために LAN IP エイリアス機能を提供します。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、本ゲートウェイにアクセスすることができます。

[追加]ボタンが適用されると、「追加 IP 構成」画面を表示します。

項目	設定値	説明
名称	1. 任意の設定	エイリアス IP アドレスの名称を入力します。
インターフェイス	1. 入力必須 2. デフォルトは、「lo」です	インターフェイスタイプを指定します。 Io または br0 になります。
IP アドレス	1. 任意の設定 2. デフォルトで、192.168.123.254 が設定されています	本デバイスに対する追加 IP アドレスを入力します。
サブネットマスク	1. 入力必須 2. デフォルトで、255.255.255.0（/24）が設定されています	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）～255.255.255.255（/32）
保存	該当なし	[保存]ボタンをクリックして、構成を保存します。

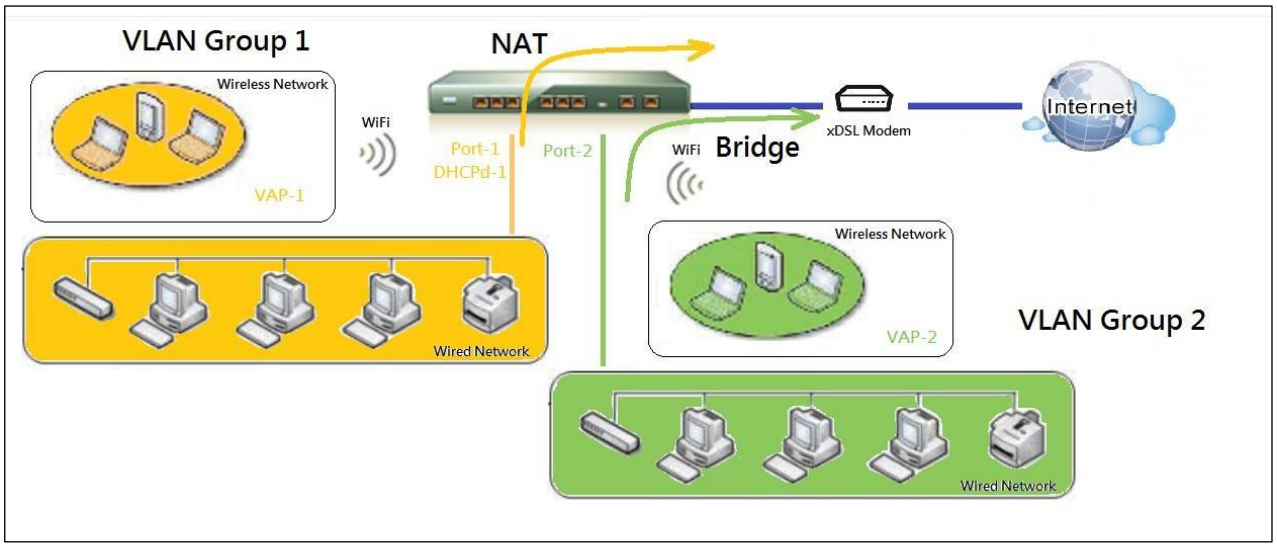
2.2.2　仮想 LAN（VLAN）

仮想 LAN（VLAN）は、特定のスイッチまたはルーターデバイスの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。このゲートウェイでは、ポートベースの VLAN とタグベースの VLAN の両方を使用できます。これらの機能を使用すると、ローカルネットワークを複数の「仮想 LAN」に分割することができます。一部のアプリケーションのシナリオでは一般的な要件です。
例えば、SMB にはさまざまな部門があります。同一部門内のすべてのクライアントホストは、アクセス権限と QoS プロパティが同じである必要があります。部門をポートベースの VLAN またはタグベースの VLAN のいずれかにグループとして割り当てることができます。次に、プランで構成します。ISP のサービス（IPTV など）によっては、ルーターが「VLAN タグ」をサポートしてしない場合があります。このサービスに必要なすべてのデバイスを、1 つのタグベースの VLAN としてグループ化できます。

ゲートウェイに物理イーサネット LAN ポートが 1 つしかない場合は、ポートベースの VLAN を有効にすると、非常に限られた構成しか使用できません。

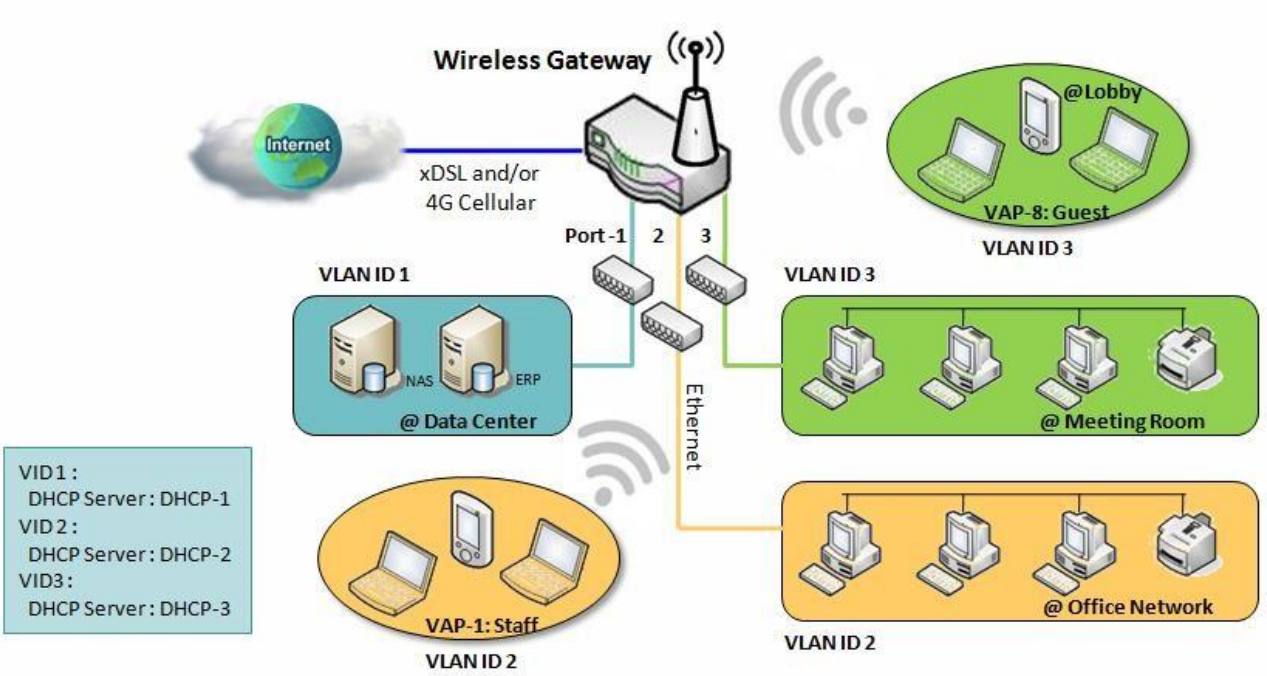
➢ Port-based VLAN（ポートベースの VLAN）

ポートベースの VLAN 機能では、インターネットサーフィン、マルチメディアの利用、VoIP 通話などの差別化サービスで、イーサネットポート、ポート 1～ポート 4、WiFi 仮想アクセスポイント、VAP-1～VAP-8 をグループ化することができます。各 VLAN グループには 2 種類の動作モード（NAT とブリッジ）を適用できます。NAT VLAN グループごとに 1 台の DHCP サーバーが割り当てられ、グループホストメンバーは、このサーバーの IP アドレスを取得できます。これにより、各ホストはビジネスアクセスゲートウェイの NAT メカニズムによりインターネットサーフィンを行うことができるようになります。ブリッジモードでは、イントラネットパケットフローは各種のサービスのため、VLAN タグが設定された WAN トランクポートから上部リンクに送信されます。



ポートベースの VLAN は、論理 LAN セグメントを形成する有線または無線ゲートウェイのイーサネットまたは仮想 AP 上のポートのグループです。
以下に例をあげます。
例えば、ある企業では、管理者は 3 つのネットワークセグメント、［ロビー］/［ミーティングルーム］、［オフィス］、［データセンター］を計画します。［ワイヤレ

スゲートウェイ］で、管理者は［ロビー］/［ミーティングルーム］セグメントに VLAN ID 3 を設定しました。VLAN グループには、NAT モードおよび DHCP-3 サーバーが装備された Port-3 および VAP-8（SSID：Guest）が含まれます。また、［オフィス］セグメントには VLAN ID 2 を設定しました。VLAN グループには、NAT モードおよび DHCP-2 サーバーが装備された Port-2 および VAP-1（SSID：Staff）が含まれます。
最後に、管理者は、［Data Center（データセンター）］セグメントに VLAN ID 1 も設定しました。この VLAN グループには、Port-1 があり、次の図のように WAN インターフェイスへの NAT モードが設定されています。

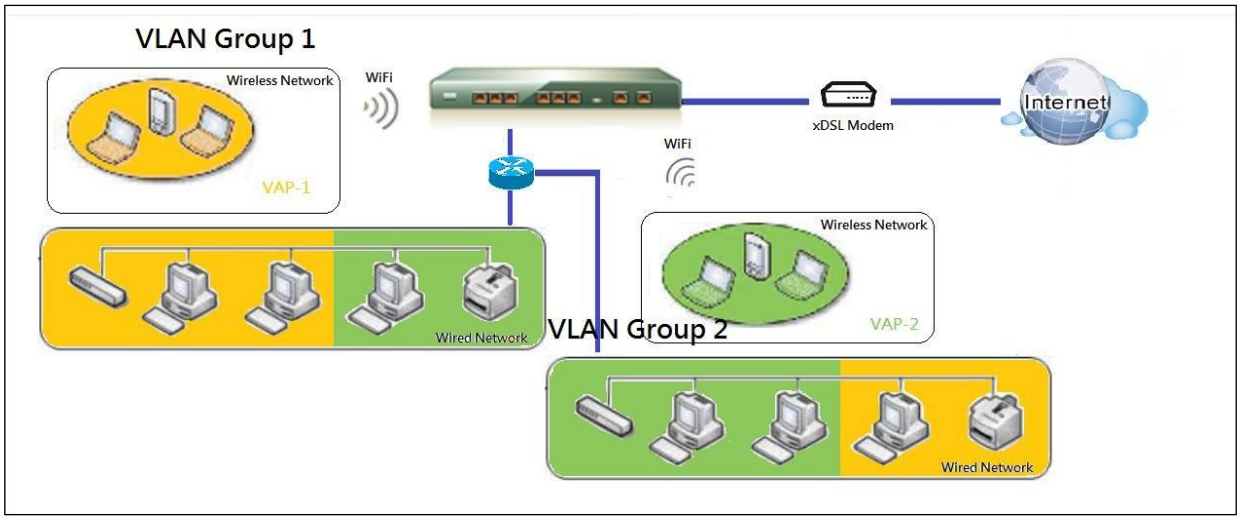


上記はゲートウェイでイーサネット LAN ポートが 3 つある場合の一般的な例です。しかし、デバイスにイーサネット LAN ポートが 1 つしかない場合、そのデバイスには 1 つの VLAN グループしか存在しません。このような状況では、ポートベースの VLAN 構成では、NAT モードとブリッジモードの両方をサポートしています。

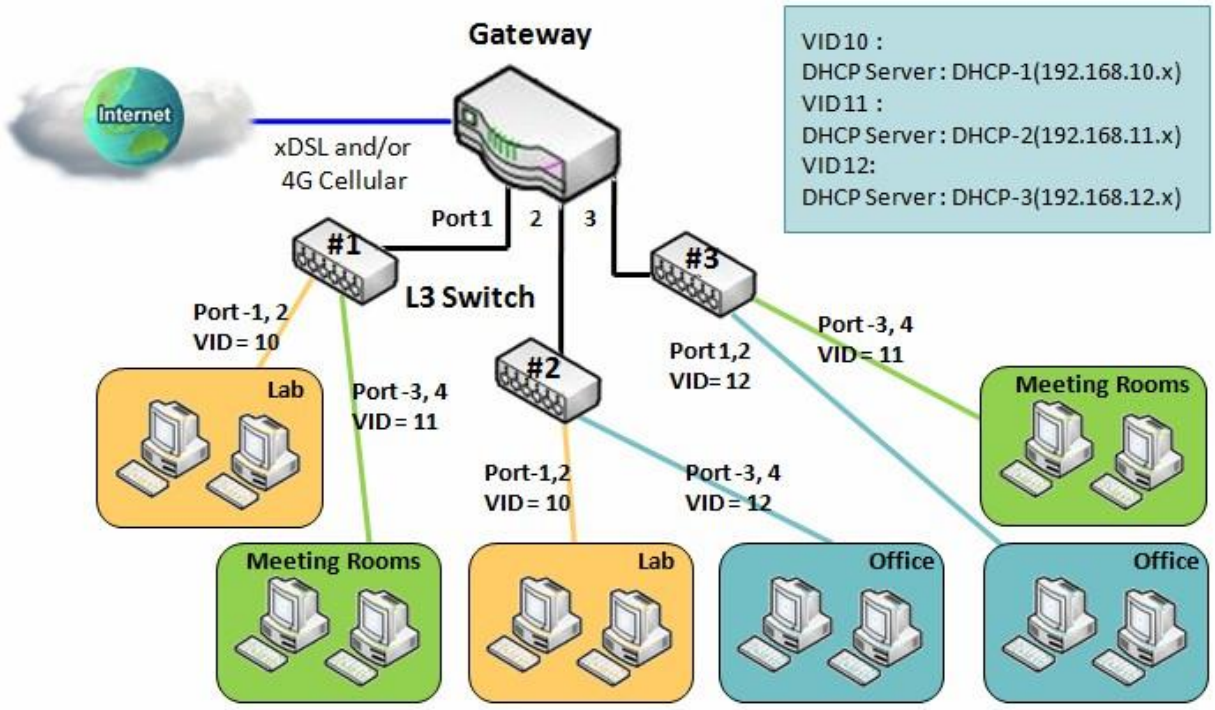
➢ Tag-based VLAN（タグベースの VLAN）

タグベースの VLAN 機能は、イーサネットポート、ポート 1～ポート 4、および、WiFi 仮想アクセスポイント（VAP-1～VAP-8）をイントラネットにサブネットを展開するための異なる VLAN タグとともにグループ化できます。すべてのパケットフローで、インターネット用の同じ物理イーサネットポートを使用する場合でも、複数の VLAN タグを使用することができます。これらのフローは、異なるタグがあるためそれぞれ異なる場所に転送されます。この方法は、地理的に異なる場所にあるホストを同じワークグループとしてグループ化する場合に便利です。

タグベースの VLAN は VLAN トランクとも呼ばれています。VLAN トランクはルーターデバイスから異なる VLAN ID のパケットフローをすべて収集し、イントラネットに送信します。タグ付けされた VLAN の VLAN メンバーシップは、ポートで受信されたパケットフレーム内の VLAN ID 情報で判別されます。さらに、管理者は VLAN スイッチを使用して、VLAN トランクを VLAN ID に基づき複数のグループに分けることもできます。以下に例をあげます。



例えば、ある企業では、管理者は 3 つのネットワークセグメント、 [Lab（研究室）] / [Meeting Room（ミーティングルーム）] 、 [Office（オフィス）] を計画します。セキュリティ VPN ゲートウェイで、管理者は、 [Office（オフィス）] セグメントに VLAN ID 12 を設定しました。この VLAN グループには DHCP-3 サーバーがあり、192.168.12.x サブネットを構築しています。また、
[Meeting Rooms（ミーティングセグメント）] セグメントには、VLAN ID 11 を設定しました。この VLAN グループには DHCP-2 サーバーがあり、イントラネット専用の 192.168.11.x サブネットを構築しています。つまり、VLAN 11 グループのクライアントホストはいずれもインターネットにアクセスできません。最後に、 [Lab（研究室）] セグメントには、VLAN ID 10 を設定しました。この VLAN グループには DHCP-1 サーバーがあり、192.168.10.x サブネットを構築しています。

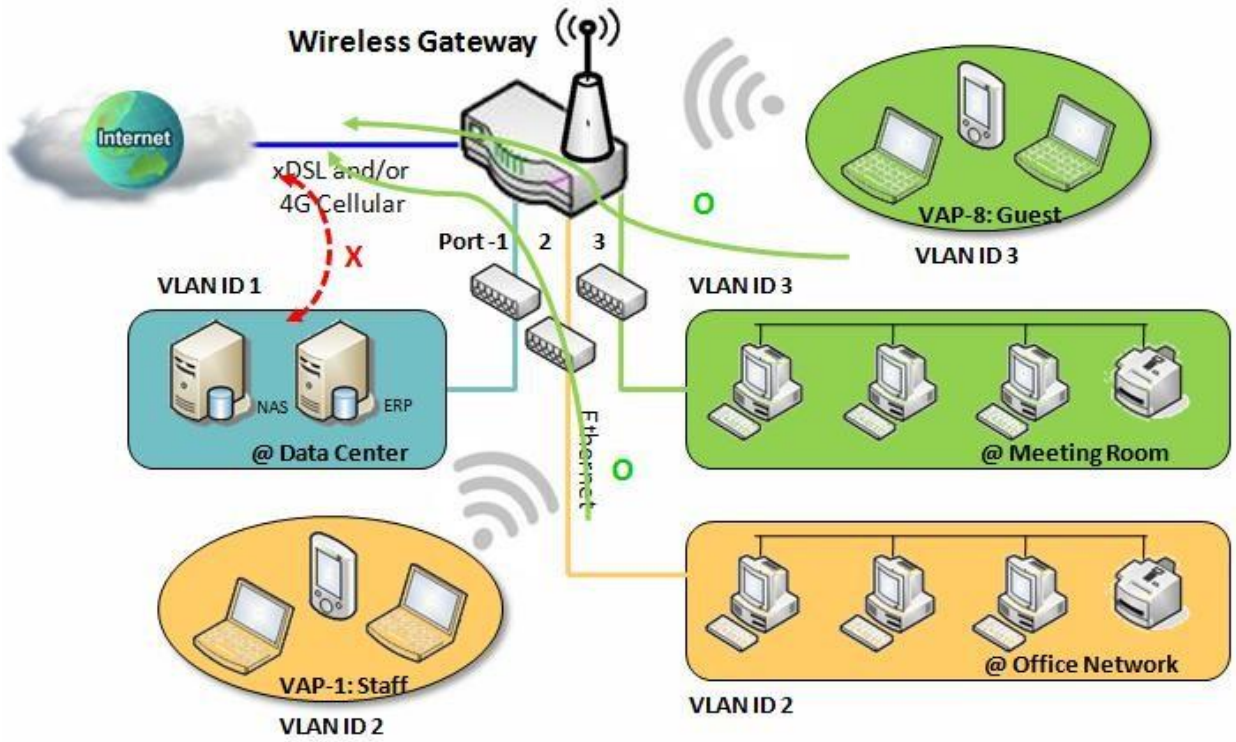


➢VLAN Groups Access Control（VLAN グループアクセス制御）

管理者は、すべての VLAN グループに対するインターネットアクセス権を指定できます。また、どの VLAN グループが互いに通信できるかを構成することもできます。

VLAN Group Internet Access（VLAN グループのインターネットアクセス）

管理者は、ある 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するかどうかを指定できます。次の例では、VID が 2 および 3 の VLAN グループはインターネットにアクセスできますが、VID が 1 の VLAN グループはインターネットにアクセスできません。つまり、［Meeting Room（ミーティングルーム）］の訪問者と［Office（オフィス）］のスタッフはインターネットにアクセスできます。しかし、データセンター内のコンピュータ/サーバーは、セキュリティの配慮からインターネットにアクセスできません。データセンターのサーバーは、信頼されたスタッフだけが使用するか、セキュリティ保護されたトンネルからアクセスします。

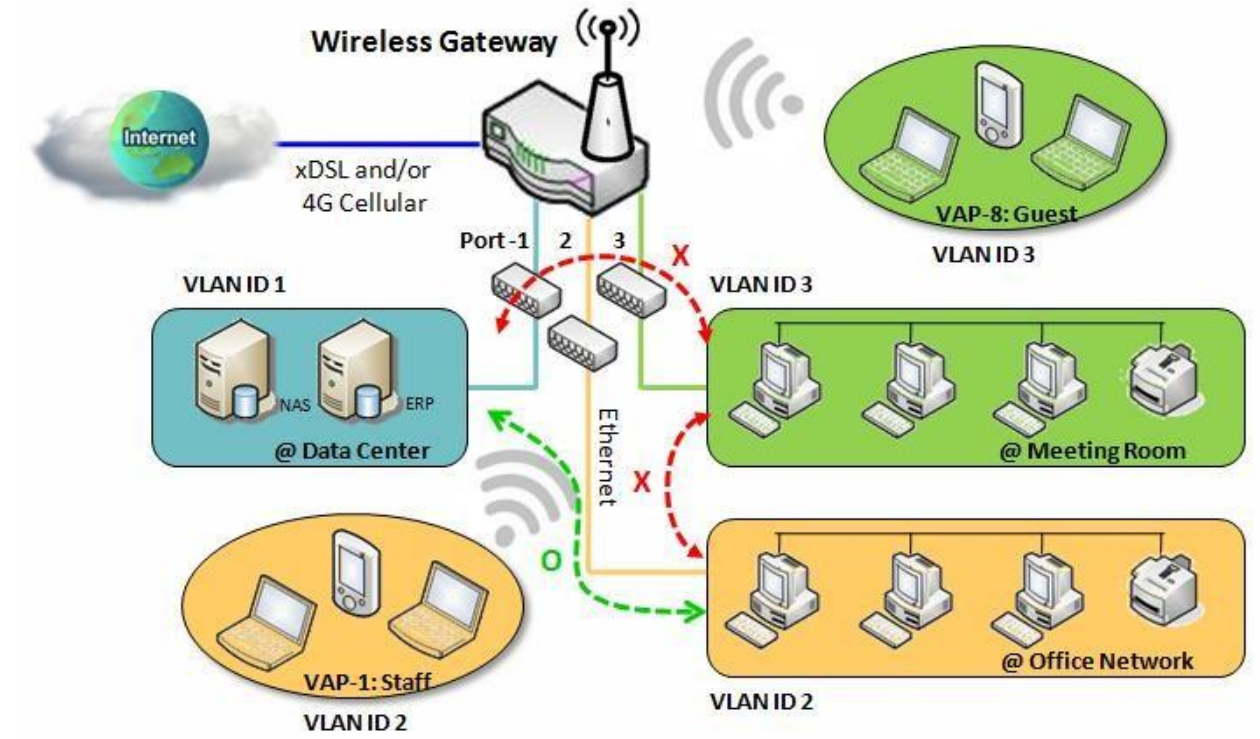


Inter VLAN Group Routing（VLAN 間グループルーティング）：

ポートベースのタグを使用する場合、管理者はある VLAN グループのメンバーホストが別の VLAN グループのメンバーホストと通信できるようにするかどうかを指定できます。これが通信ペアで、1 つの VLAN グループが複数の通信ペアに参加することができます。しかし、通信ペアには推移的なプロパティがありません。

例えば、A は B と通信でき、B が C と通信できる場合でも、A が C と通信できるとは限りません。

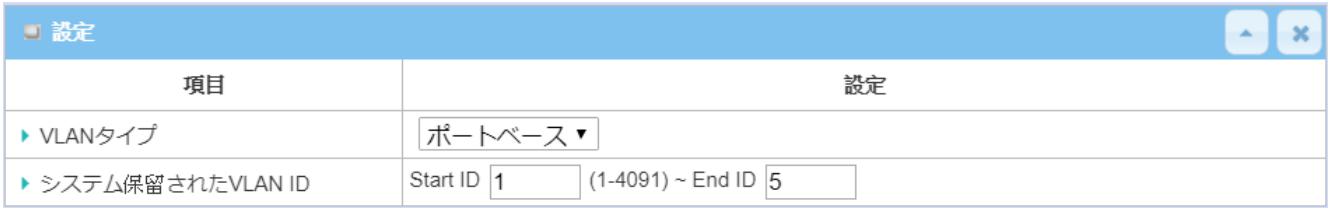
次の図はその例です。VID が 1、および 2 の VLAN グループは相互に通信できますが、VID 1 と VID 3 の間、および VID 2 と VID 3 の間では通信ができません。



VLAN 設定

基本ネットワーク ＞ **[LAN および VLAN]** ＞ **[仮想 LAN] タブ**に進みます。

VLAN 機能を使用すると、ローカルネットワークを複数の仮想 LAN に分割することができます。ポートベース、およびタグベースの VLAN タイプがあります。
適用するものを選択してください。



項目	設定値	説明
VLAN タイプ	デフォルトは、「ポートベース」です	ローカルサブネットを整理するために採用する VLAN タイプを選択します。 **・ポートベース**：ポートベースの VLAN では、各 LAN ポートにルールを追加することができ、VLAN ID を使用して高度な制御を行うことができます。 **・タッグベース**：タグベースの VLAN では、VLAN ID を追加し、この VLAN ID にメンバーと DHCP サーバーを選択できます。［タグベース VLAN リスト］テーブルに移動します。
システムに保留された VLAN ID	デフォルトは、「1～5」です	システム動作用に予約されている VLAN ID 範囲を指定します。ポートベース/タグベースの VLAN グループ化の場合は、予約された範囲外の ID のみを使用してください。 値の範囲：1～4091
保存	該当なし	[適用]ボタンをクリックして、構成を保存します。

ポートベースの VLAN - VLAN ルールの作成/編集

ポートベースの VLAN を使用すると、各 LAN ポートをカスタム設定できます。すべての LAN ポートの構成を表示するデフォルトルールがあります。最大ルール番号は、LAN ポート番号に基づいています。

［追加/編集］ボタンをクリックすると、［ポートベースの VLAN 構成］画面を表示します。

ポートベースVLANリスト　追加　削除

名称	VLAN ID	VLAN タギング	NAT/ブリッジ	ポートメンバー	LAN IPアドレス	サブネットマスク	結合WAN	WAN VID	有効	アクション
LAN	ネーティブ VLAN Tag 1	X	NAT	詳細	192.168.123.254	255.255.255.0	すべての WAN	0	☑	編集

ここには、以下 3 つのセクションがあります。

［ポートベースの VLAN 構成］、［IP 固定マッピングルールリスト］、［VLAN 間グループルーティング］

［ポートベースの VLAN 構成］

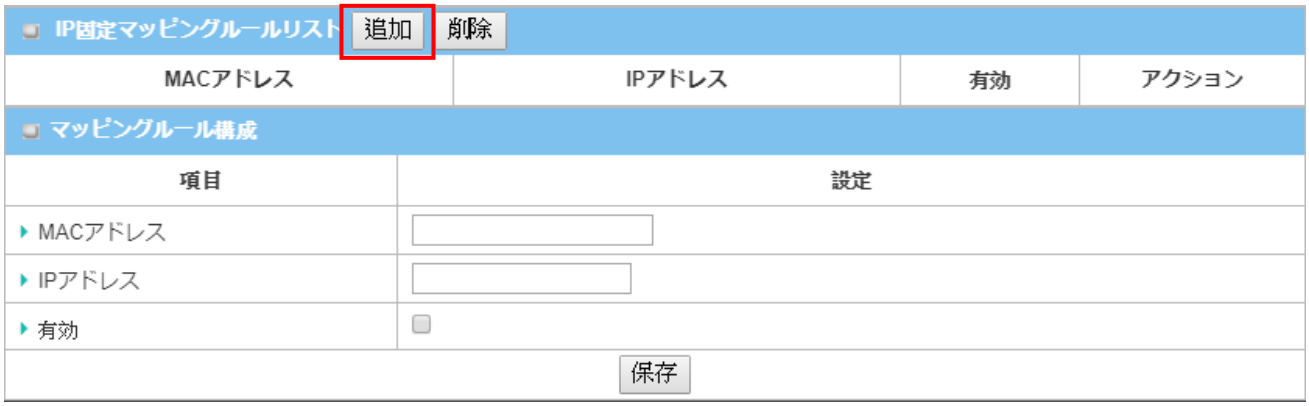
ポートベースのVLAN構成

項目	設定
名称	LAN
VLAN ID	ネーティブVL
VLANタギング	無効
NAT/ブリッジ	NAT
ポートメンバー	ポート: ☑ ポート-1 ☑ ポート-2 ☑ ポート-3 ☑ ポート-4 5G: ☑ VAP-1 ☑ VAP-2 ☑ VAP-3 ☑ VAP-4 ☑ VAP-5 ☑ VAP-6 ☑ VAP-7 ☑ VAP-8
LAN to Join	☐ 有効 DHCP 1
WAN&WAN VID結合	すべてのWAN None
LAN IPアドレス	192.168.123.254
サブネットマスク	255.255.255.0 (/24)
DHCPサーバー/リレー	サーバー
DHCPサーバー名	DHCP 1
IPプール	開始アドレス: 192.168.123.100 終了 アドレス: 192.168.123.200
リース時間	3600 秒
ドメイン名	(選択的)
プライマリーDNS	(選択的)
セカンダリーDNS	(選択的)
プライマリWINS	(選択的)
セカンダリーWINS	(選択的)
ゲートウェイ	(選択的)
有効	☑

項目	設定値	説明
名称	1.入力必須 2.文字列形式：デフォルトテキストあり	このルールの名称を定義します。 デフォルトテキストがあり、変更することはできません。
VLAN ID	入力必須	VLAN ID 番号を定義します。範囲は 1～4094 です。
VLAN タギング	デフォルトは、「無効」です	・「有効」が選択されている場合、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」が選択されている場合、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	デフォルトは、「NAT」です	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	デフォルトは、チェックなしです	ルールに追加する LAN ポートと VAP を選択します。 注：利用可能なメンバーリストは、購入した製品によって異なる場合があります。
WAN&WAN VID 結合	デフォルトは、「すべての WAN」です	インターネットへのアクセスを許可する「WAN」または「すべての WAN」を選択します。 注：[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	入力必須	ルールが使用した 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、ゲートウェイ IP です。
サブネットマスク	デフォルトで、255.255.255.0（/24）が選択されています	DHCP サーバーの [サブネットマスク] を選択します。
DHCP サーバー/リレー	デフォルトは、「サーバー」です	[DHCP サーバー] のタイプを定義します。 選択できるタイプは [サーバー]、[リレー]、および [無効] の 3 つです。 • 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、[DHCP サーバーIP アドレス] フィールドに入力します。 • サーバー：VLAN グループに対して、DHCP サーバー機能を有効にするには、[サーバー] を選択し、DHCP サーバーの設定を指定する必要があります。 • 無効：[無効] を選択すると、VLAN グループの DHCP サーバー機能が無効になります。
DHCP サーバーIP アドレス/DHCP リレーの場合のみ）	入力必須	DHCP サーバーの [リレー] タイプを選択した場合、ゲートウェイが割り当てられた DHCP サーバーに DHCP 要求をリレーする [DHCP サーバーIP アドレス] を割り当てます。
DHCP サーバー名	入力必須	指定した VLAN グループの DHCP サーバーの名前を定義します。
IP プール	入力必須	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 サーバーから 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	入力必須	DHCP サーバーが新しいデバイスにリースする IP アドレスの期間を定義します。 デフォルトでは、[リース時間] は 3600 秒です。
ドメイン名	文字列形式は任意のテキストです	本 DHCP サーバーのドメイン名です。 値の範囲：0～31 文字
プライマリーDNS	IPv4 形式です	本 DHCP サーバーのプライマリーDNS です。
セカンダリーDNS	IPv4 形式です	本 DHCP サーバーのセカンダリーDNS です。
プライマリーWINS	IPv4 形式です	本 DHCP サーバーのプライマリーWINS です。
セカンダリーWINS	IPv4 形式です	本 DHCP サーバーのセカンダリーWINS です。
ゲートウェイ	IPv4 形式です	本 DHCP サーバーのゲートウェイです。
有効	デフォルトは、チェックなしです	有効ボックスにチェックをして、本ルールを有効します。
保存	該当なし	[保存] ボタンをクリックして、構成を保存します。
キャンセル	該当なし	[キャンセル] ボタンをクリックして、構成した内容を元の設定に復元します。

また、VLAN グループの DHCP サーバーが必要な場合は、[IP 固定マッピングルールリスト] に IP ルールを追加できます。
[追加] ボタンが適用されると、「マッピングルール構成」画面を表示します。



項目	設定値	説明
MAC アドレス	入力必須	DHCP サーバーが一致させる [MAC アドレス] ターゲットを定義します。
IP アドレス	入力必須	DHCP サーバーが割り当てる [IP アドレス] を定義します。 上記のフィールドに入力された [MAC アドレス] からの要求がある場合、DHCP サーバーは、この [IP アドレス] を、その [MAC アドレス] がルールに一致するクライアントに割り当てます。
有効	デフォルトは、チェックなしです	ボックスにチェックをして、本ルールを有効にします。
保存	該当なし	[保存] ボタンをクリックして、構成を保存します。

注：Web ブラウザがリフレッシュされた後に変更を適用するには、必ず [適用] ボタンをクリックして、VLAN ページに戻ってください。

ポートベースの VLAN - VLAN 間グループルーティング

［VLAN 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」画面を表示します。

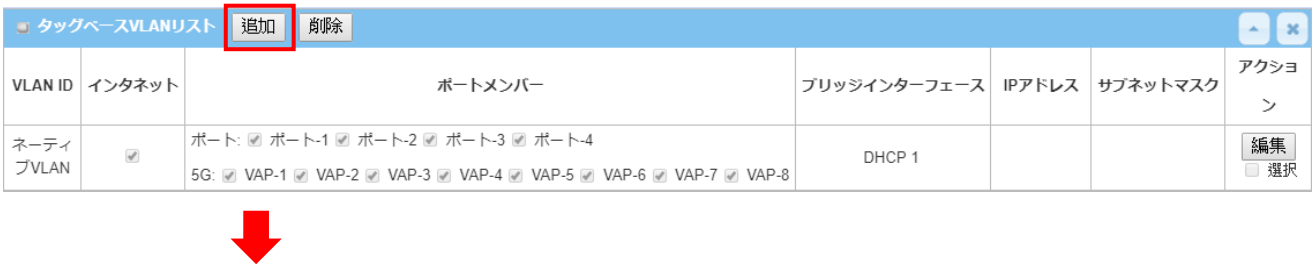
［編集］ボタンが適用されると、これに類似した画面が表示されます。

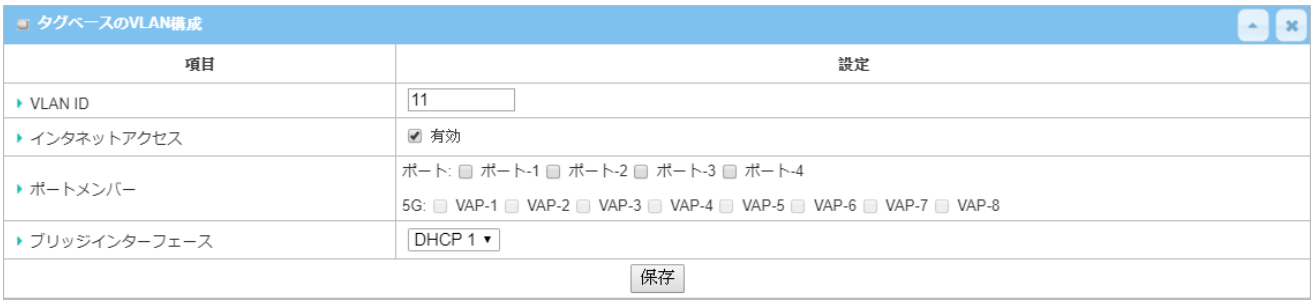
項目	設定値	説明
VLAN グループインターネットアクセス定義	デフォルトは、すべてのボックスにチェックありです	デフォルトでは、すべてのボックスがチェックされ、すべての VLAN ID メンバーが WAN インターフェイスにアクセスできることを示します。 特定の VLAN ID ボックスのチェックを外すと、VLAN ID メンバーがインターネットにアクセスできなくなります。 注：VLAN ID 1 は、常に使用できます。LAN ルールのデフォルトの VLAN ID です。その他の VLAN ID は、有効になっている場合にのみ使用できます。

VLAN 間グループルーティング	デフォルトは、ボックスのチェックなしです	期待される 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。 デフォルトでは、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	該当なし	[保存] ボタンをクリックして、構成を保存します。

タッグベースの VLAN を使用すると、VLAN ID に従って各 LAN ポートをカスタマイズできます。すべての LAN ポートおよび VAP の構成を表示するデフォルトルールがあります。
ルーターは、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。

[追加] ボタンが適用されると、[タグベースの VLAN 構成] 画面を表示します。



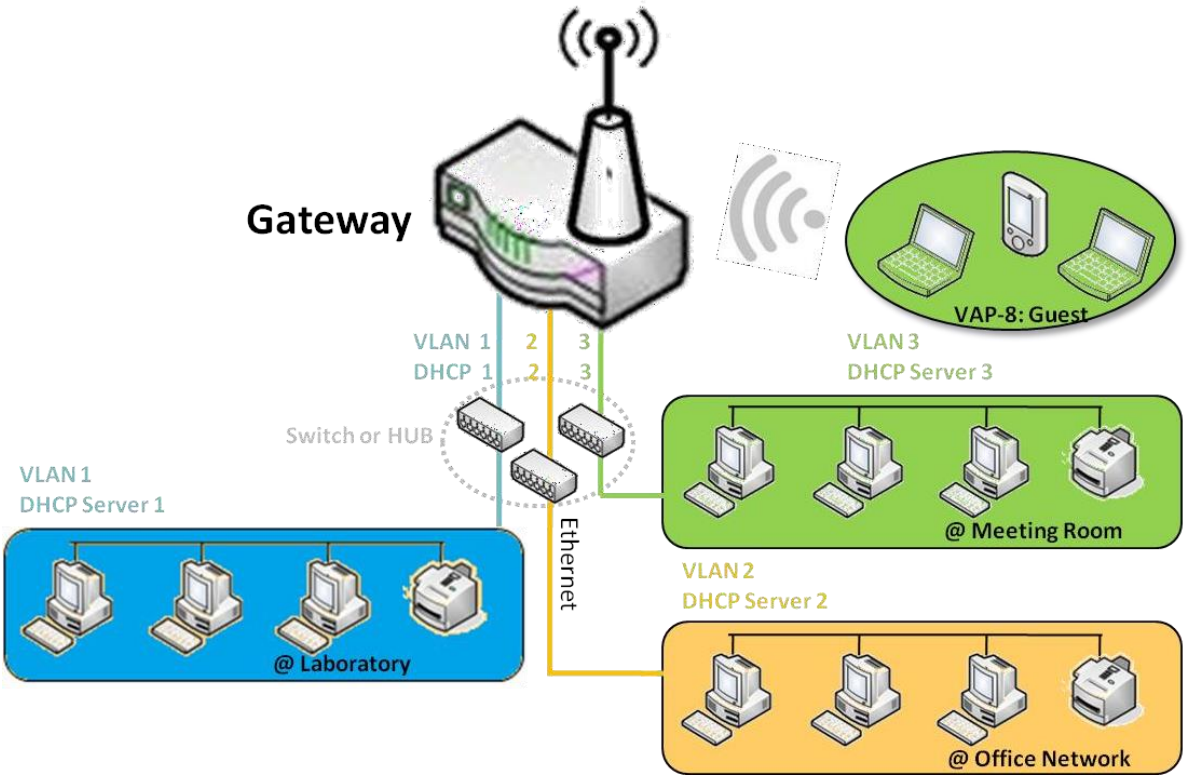


項目	設定値	説明
VLAN ID	入力必須	VLAN ID 番号を定義します。範囲は 6～4094 です。
インターネットアクセス	デフォルトは、すべてのボックスにチェックありです	[有効] ボックスをクリックすると、VLAN グループのメンバーがインターネットにアクセスできるようになります。
ポートメンバー	デフォルトは、ボックスのチェックは外されています	LAN ポートボックスにチェックを入れて、VLAN グループに参加します。
ブリッジインターフェース	デフォルトで、「DHCP1」が選択されています	この VLAN グループのメンバーに [ブリッジインターフェース] を選択します。 VLAN 用の DHCP サーバーを作成または編集するには、基本ネットワーク > LAN および VLAN > 「DHCP サーバー」を参照してください。
保存	該当なし	[保存] ボタンをクリックして、構成を保存します。 注：[保存] ボタンをクリックした後、[適用] ボタンをクリックして設定を適用します。

2.2.3　DHCP サーバー

➢DHCP サーバー

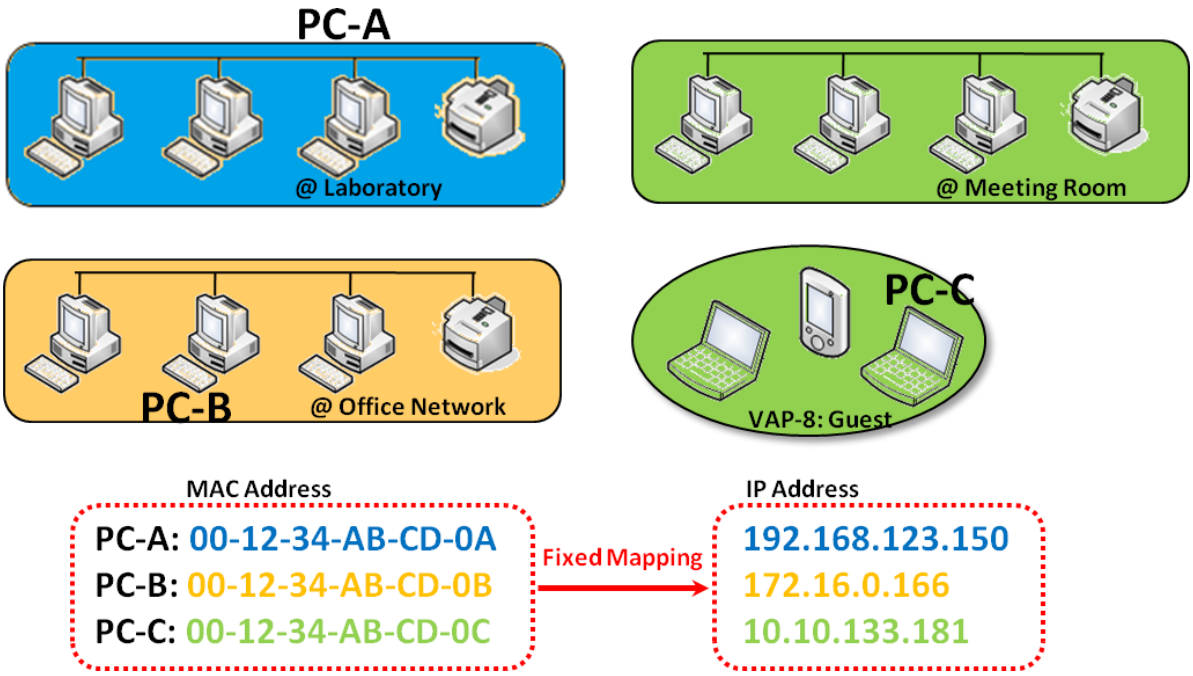
ゲートウェイは、異なる VLAN グループからの DHCP 要求を満たすために最大 4 台の DHCP サーバーをサポートします（詳細については、VLAN のセクションを参照してください）。また、LAN IP アドレスがゲートウェイ LAN インターフェイスと同じものであるデフォルト設定（デフォルトサブネットマスク設定が「255.255.255.0」、デフォルト IP プール範囲が、ゲートウェイの WEB UI の DHCP サーバーリストページに示されているよう、「.100」から「.200」）が 1 つあります。



ユーザーは、「DHCP サーバーリスト」の背後にある[追加]ボタンをクリックするか、リストの各 DHCP サーバーの最後にある[編集]ボタンをクリックし、現在の設定を編集することにより、DHCP サーバー構成を追加することができます。
また、DHCP サーバーを選択し、「選択」チェックボックスと[削除]ボタンをクリックすることにより、DHCP サーバーを削除することができます。

➢固定マッピング

DHCP クライアントリストにターゲットがすでに存在していた場合、ユーザーは、固定 IP アドレスを割り当て、特定のクライアント MAC アドレスを選択してからコピーすることができます。または、ターゲットの MAC アドレスの接続準備ができていないとき、事前に手動でいくつかの他のマッピングルールを追加することができます。



DHCP サーバーリスト

基本設定 > [LAN および VLAN] > [DHCP サーバー] タブに進みます。

DHCP サーバー設定では、DHCP サーバーポリシーを作成およびカスタマイズして、ローカルエリアネットワーク（LAN）上のデバイスに IP アドレスを割り当てることができます。

DHCP サーバー設定

DHCP サーバーポリシーの作成/編集

ゲートウェイを使用すると、DHCP サーバーポリシーをカスタム設定することができます。複数の LAN ポートが利用可能な場合、LAN（または VLAN グループ）ごとに 1 つのポリシーを定義し、最大 4 つのポリシーをサポートできます。

[追加]ボタンが適用されると、DHCP サーバー構成画面を表示します。

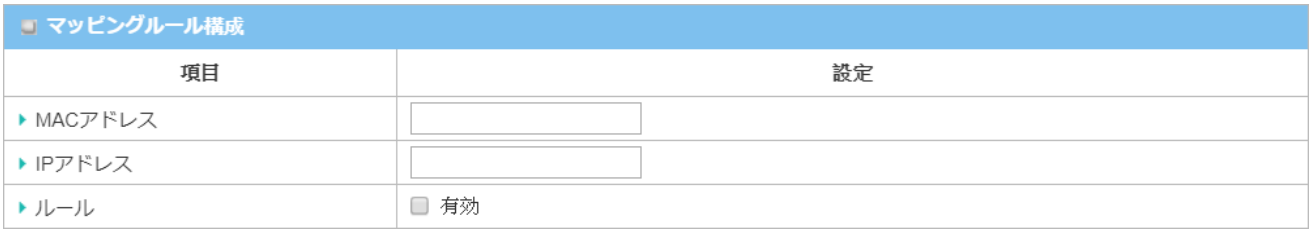
項目	設定値	説明
サーバー名	1. 文字列形式は任意のテキストです 2. 入力必須	DHCP サーバー名を入力します。 理解しやすい名称を入力します。
LAN IP アドレス	1. IPv4 形式です 2. 入力必須	本 DHCP サーバーの IP アドレスです。
サブネットマスク	デフォルトで、255. 255. 255. 0 (/24) が設定されています	本 DHCP サーバーのサブネットマスクです。
IP プール	1. IPv4 形式です 2. 入力必須	本 DHCP サーバーの IP プールです。このフィールドに入力される開始アドレスとこのフィールドに入力される終了アドレスで構成されます。
リース時間	1. 数値文字列形式です 2. 入力必須	本 DHCP サーバーのリース時間です。 値の範囲：300～604800 秒。
ドメイン名	文字列形式は任意のテキストです	本 DHCP サーバーのドメイン名です。
プライマリーDNS	IPv4 形式です	本 DHCP サーバーのプライマリーDNS です。
セカンダリーDNS	IPv4 形式です	本 DHCP サーバーのセカンダリーDNS です。
プライマリーWINS	IPv4 形式です	本 DHCP サーバーのプライマリーWINS です。
セカンダリーWINS	IPv4 形式です	本 DHCP サーバーのセカンダリーWINS です。
ゲートウェイ	IPv4 形式です	本 DHCP サーバーのゲートウェイです。
サーバー	デフォルトは、チェックなしです	有効ボックスにチェックをして、本 DHCP サーバーを有効します。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。

DHCP サーバー上のマッピングルールの作成/編集

ゲートウェイを使用すると、DHCP サーバー上のマッピングルールをカスタム設定することができます。これは、最大 64 のルールセットをサポートします。

[固定マッピング]ボタンが適用されると、「マッピングルールリスト」画面を表示します。

[追加]ボタンが適用されると、マッピングルール構成画面を表示します。



項目	設定値	説明
MAC アドレス	1. MAC アドレスの文字列形式です 2. 入力必須	本マッピングルールの MAC アドレスです。
IP アドレス	1. IPv4 形式です 2. 入力必須	本マッピングルールの IP アドレスです。
ルール	デフォルトは、 チェックなしです	有効ボックスにチェックをして、本ルールを有効します。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。

DHCP クライアントリストの表示/コピー

[DHCP クライアントリスト]ボタンが適用されると、「DHCP クライアントリスト」画面を表示します。

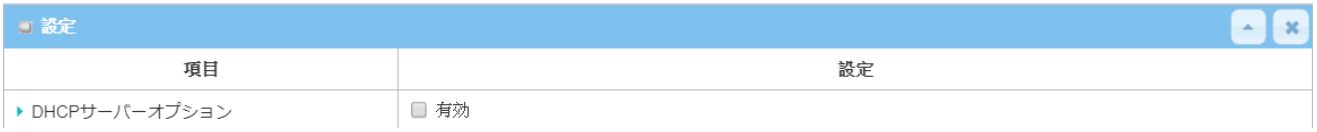
DHCP クライアントが選択され、[固定マッピングにコピー]ボタンが適用されると、DHCP クライアントの IP、および MAC アドレスが、特定の DHCP サーバー上のマッピングルールリストに自動的に適用されます。

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。

[有効]ボタンをクリックして、DHCP オプション機能を有効します。DHCP サーバーは、DHCPOFFER DHCPACK パッケージの送信において、予想されるオプションを追加します。

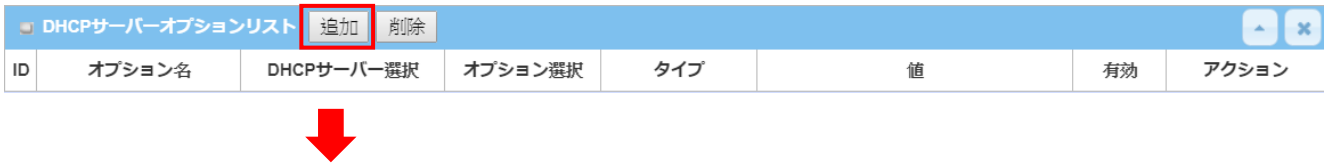
オプション	意味	RFC
66	TFTP サーバー名	[RFC 2132]
72	デフォルトの World Wide Web サーバー	[RFC 2132]
114	URL	[RFC 3679]



DHCP サーバーオプションの作成/編集

ゲートウェイは、最大 99 のオプション設定をサポートします。

［追加/編集］ボタンが適用されると、「DHCP サーバーオプション構成」画面を表示します。

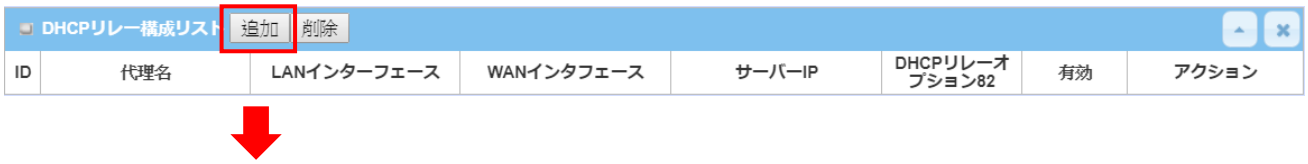


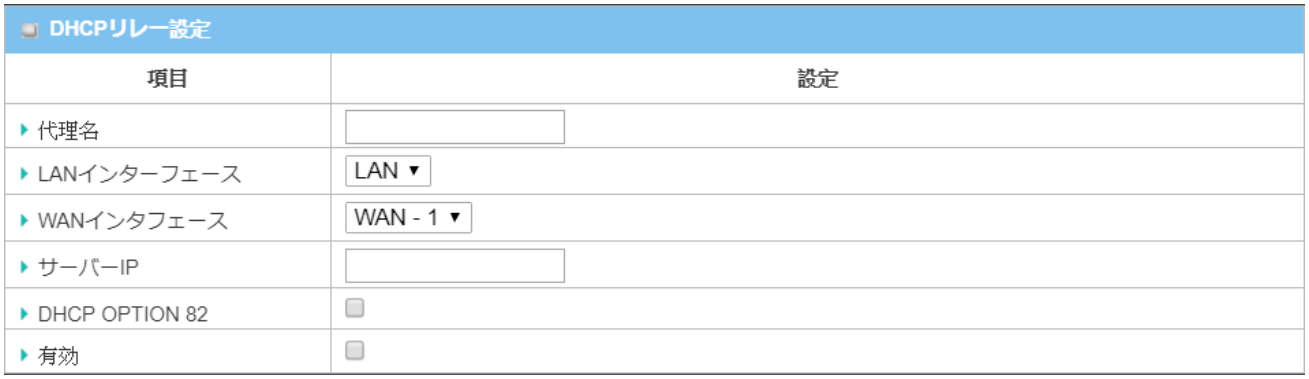
<table>
<tr><th>項目</th><th>設定値</th><th colspan="3">説明</th></tr>
<tr><td>オプション名</td><td>1.文字列形式は任意のテキストです
2.入力必須</td><td colspan="3">DHCP サーバーオプション名を入力します。
理解しやすい名称を入力します。</td></tr>
<tr><td>サーバー選択</td><td>利用可能な全 DHCP サーバーのドロップダウンリストです。</td><td colspan="3">このオプションが適用される DHCP サーバーを選択します。</td></tr>
<tr><td>オプション選択</td><td>1.入力必須
2.デフォルトで「OPTION 66」が選択されています</td><td colspan="3">ドロップダウンリストから特定のオプションを選択します。
これは、Option 66、Option 72 または Option 144、のいずれかになります。
tftp の場合は、Option 66
www の場合は、Option 72
URL の場合は、Option 144</td></tr>
<tr><td rowspan="9">タイプ</td><td rowspan="9">DHCP サーバーオプションの値のタイプのドロップダウンリスト</td><td colspan="3">異なるオプションは、異なる値のタイプを持ちます。</td></tr>
<tr><td rowspan="2">66</td><td colspan="2">単一 IP アドレス</td></tr>
<tr><td colspan="2">単一 FQDN</td></tr>
<tr><td>72</td><td colspan="2">「,」により区切られた IP アドレスリスト</td></tr>
<tr><td>114</td><td colspan="2">単一 URL</td></tr>
<tr><td>42</td><td colspan="2">「,」により区切られた IP アドレスリスト</td></tr>
<tr><td>150</td><td colspan="2">「,」により区切られた IP アドレスリスト</td></tr>
<tr><td rowspan="2">160</td><td colspan="2">単一 IP アドレス</td></tr>
<tr><td colspan="2">単一 FQDN</td></tr>
<tr><td>値</td><td>1. IPv4 形式です
2. FQDN 形式です
3. IP リストです
4. URL 形式です
5. 入力必須</td><td colspan="3">次のタイプに準拠する必要があります：
タイプ　　値</td></tr>
<tr><td rowspan="2">66</td><td>単一 IP アドレス</td><td>IPv4 形式です</td></tr>
<tr><td>単一 FQDN</td><td>FQDN 形式です</td></tr>
<tr><td>72</td><td>「,」により区切られた IP アドレスリスト</td><td>「,」により区切られた IPv4 形式</td></tr>
<tr><td>114</td><td>単一 URL</td><td>URL 形式です</td></tr>
<tr><td>有効</td><td>デフォルトは、チェックなしです</td><td colspan="3">有効ボックスにチェックをして、本ルールを有効します。</td></tr>
<tr><td>保存</td><td>該当なし</td><td colspan="3">［保存］ボタンをクリックして、構成を保存します。</td></tr>
</table>

DHCP リレーの作成/編集

ゲートウェイは、最大 6 の DHCP リレー構成をサポートします。

［追加/編集］ボタンが適用されると、「DHCP リレー設定」を表示します。





項目	設定値	説明
代理名	1. 文字列形式は任意のテキストです 2. 入力必須	DHCP リレー名を入力します。 理解しやすい名称を入力します。
LAN インターフェース	1. 入力必須 2. デフォルトは、「LAN」です	DHCP リレー機能で適用するドロップダウンリストの LAN インターフェースを選択します。
WAN インタフェース	1. 入力必須 2. デフォルトは、「WAN-1」です	DHCP リレー機能で適用するドロップダウンリストの WAN インタフェースを選択します。使用可能な WAN インタフェース、および L2TP 接続にすることができます。
サーバーIP	入力必須	ゲートウェイが指定された WAN インターフェイスを介して割り当てられた DHCP サーバーに DHCP 要求を中継する DHCP サーバーの IP アドレスを割り当てます。
有効	デフォルトは、チェックなしです	有効ボックスにチェックをして、本設定を有効にします。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。

2-3. WiFi　【未対応】

本製品ではサポートされていない機能です。

2-4. IPv6　【未対応】

本製品ではサポートされていない機能です。

2-5. ポート転送

基本ネットワーク ＞ ［ポート転送］

ネットワークアドレス変換（NAT）とは、トラフィックルーティングデバイスを通過中に、インターネットプロトコル（IP）データグラムパケットヘッダー内のネットワークアドレス情報を変更することによって、1 つの IP アドレス空間を別の IP アドレス空間に再マッピングする方法です。この技術は、もともとすべてのホストの番号再設定を行うことなく、IP ネットワーク内のトラフィックを容易に再ルーティングするために使用されていました。これは、IPv4 アドレスの枯渇に直面し、グローバルアドレス空間への割り当てを節約するための一般的で不可欠なツールとなっています。お客様が購入された製品が埋め込みを行い、NAT 機能を有効します。また、[基本ネットワーク] - [WAN&アップリンク] - [接続設定] - [WAN タイプ構成]ページ、で NAT 機能を無効化することができます。

通常、企業ゲートウェイの背後にあるすべてのローカルホストまたはサーバーは、NAT ファイアウォールで保護されています。NAT ファイアウォールは、認識できないパケットをフィルタリングしてイントラネットを保護します。したがって、すべてのローカルホストは、外部には見えません。ポート転送またはポートマッピングとは、通信要求を 1 つのアドレスとポート番号の組み合わせから、割り当てられたものにリダイレクトする機能です。この技術は、最も一般的に、宛先 IP アドレスとポート番号を再マッピングすることにより、ゲートウェイ（外部ネットワーク）の反対側のホストに利用可能な保護または偽装（内部）ネットワーク上に存在するホスト上のサービスを行うために使用されます。

2.5.1　設定

NAT ループバック

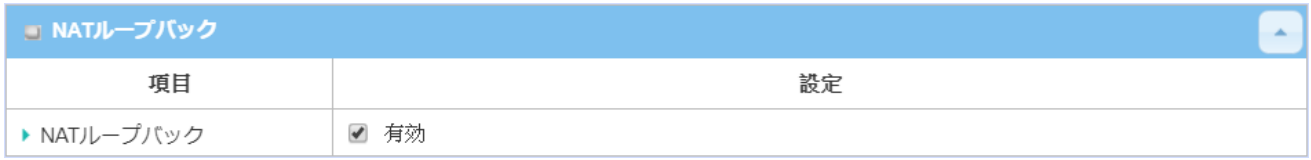
この機能を使用すると、内部 NAT ローカルネットワークから WAN グローバル IP アドレスにアクセスできます。サーバーをネットワーク内で実行する場合に便利です。例えば、LAN 側でメールサーバーを設定した場合、NAT ループバック機能を有効すると、ローカルデバイスはゲートウェイのグローバル IP アドレスを使用して、このメールサーバーにアクセスできます。いずれの側でも、LAN 側または WAN 側で電子メールサーバーにアクセスしている場合は、メールサーバーの IP アドレスを変更する必要はありません。

構成設定

基本設定 > **［ポート転送］** > **［設定］タブ**に進みます。

NAT ループバックにより、ローカルネットワーク内から WAN IP アドレスにアクセスできます。

NAT ループバックの有効



項目	設定値	説明
NAT ループバック	デフォルトは、チェックなしです	ボックスにチェックをして、本設定を有効します。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。
キャンセル	該当なし	［キャンセル］ボタンをクリックして、構成した内容を元の設定に復元します。

2.5.2　仮想サーバー＆仮想コンピュータ

設定

項目	設定
仮想サーバー	有効
仮想コンピュータ	有効

仮想サーバーリスト　追加　削除

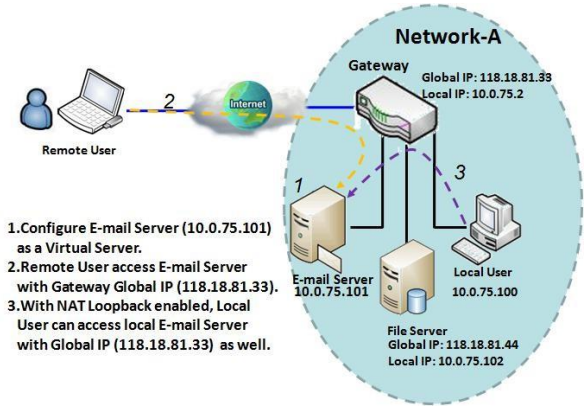
ID	WANインタフェース	サーバーIP	送信元IP	プロトコル	パブリックポート	プライベートポート	時間スケジュール	有効	アクション
1	全部	10.0.75.101	任意	TCP(6) & UDP(17)	25	15	(0) 常時	☑	編集 選択
2	全部	10.0.75.102	任意	TCP(6) & UDP(17)	110	110	(0) 常時	☑	編集 選択

仮想コンピュータリスト　追加　削除

ID	グローバルIP	ローカルIP	有効	アクション
1	118.18.81.44	10.0.75.102	☑	編集 選択

「仮想サーバー」、「NAT ループバック」、「仮想コンピュータ」など、ゲートウェイ内で実装されているいくつかの重要なポート転送機能があります。
これは、外出先でオフィスゲートウェイの背後にある様々なサーバーにアクセスする必要がある企業スタッフにとっては必要です。「仮想サーバー」機能を使って、これらのサーバーを設定することができます。出張後、元の設定を変更せずに LAN 側からグローバル IP を使って、これらのサーバーにアクセスする場合は、NAT ループバックを用いて、実現することができます。
「仮想コンピュータ」とは、NAT ゲートウェイの背後にあるホストであり、その IP アドレスは、グローバルなものであり、外部から見えます。NAT の背後にあるため、ゲートウェイファイアウォールによって保護されています。仮想コンピュータを構成するには、仮想コンピュータのローカル IP をグローバル IP にマッピングしてください。

仮想サーバーおよび NAT ループバック

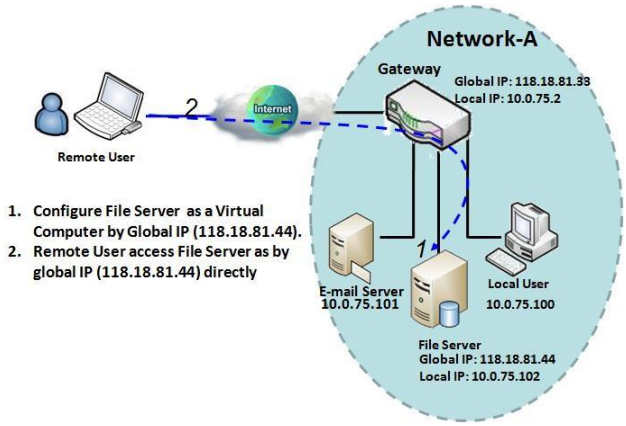


「仮想サーバー」を用いることにより、インターネットに存在するサーバーであるかのように、ゲートウェイのグローバル IP アドレスまたは FQDN を使用してサーバーにアクセスすることができます。しかし、実際には、これらのサーバーは、イントラネットに配置され、物理的にゲートウェイの後ろにあります。ゲートウェイは、ポートによるサービス要求を LAN サーバーに転送し、LAN サーバーから WAN 側の要求者に応答を転送します。
例に示すように、E メール仮想サーバーは、SMTP サービスポート 25 と POP3 サービスポ

ート 110 を含む、ネットワーク A のイントラネットに、IP アドレス 10.0.75.101 のサーバーに配置されるように定義されています。したがって、リモートユーザーは、 WAN 側からゲートウェイのグローバル IP 118.18.81.33 を使って、E メールサーバーにアクセスすることができます。しかし、実際の E メールサーバーは LAN 側にあり、ゲートウェイは、電子メールサービス用のポート転送を担当します。

NAT ループバックを使用すると、内部 NAT ローカルネットワークから WAN グローバル IP アドレスにアクセスできます。サーバーをネットワーク内で実行する場合に便利です。例えば、LAN 側でメールサーバーを設定した場合、NAT ループバック機能を有効すると、ローカルデバイスはゲートウェイのグローバル IP アドレスを使用して、このメールサーバーにアクセスできます。いずれの側でも、LAN 側または WAN 側で電子メールサーバーにアクセスしている場合は、メールサーバーの IP アドレスを変更する必要はありません。

仮想コンピュータ

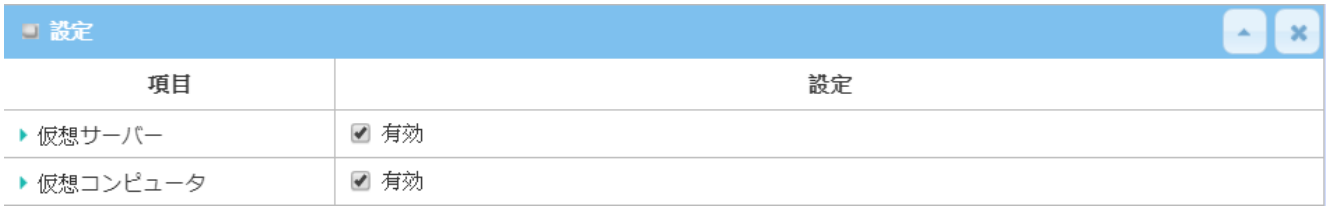


「仮想コンピュータ」を使用すると、LAN ホストをグローバル IP アドレスに割り当て、外部に見えるようにすることができます。その間、これらは、ゲートウェイファイアウォールにより、イントラネット内のクライアントホストとして保護されます。例えば、ローカル側の IPアドレスが 10.0.75.102、グローバル IPアドレスが 118.18.82.44 のLAN側のFTPファイルサーバーを設定した場合、リモートユーザーは、NAT ゲートウェイの背後に隠れている、ファイルサーバーにアクセスできます。これは、ゲートウェイが、IP アドレス 118.18.82.44 に対するすべてのアクセスを処理し、アクセス要求をファイルサーバーに転送し、サーバーからの応答を外部に送信するためです。

仮想サーバー&仮想コンピュータの設定

基本設定 > ［ポート転送］ > ［仮想サーバー＆仮想コンピュータ］タブに進みます。

仮想サーバー＆仮想コンピュータの有効



項目	設定値	説明
仮想サーバー	デフォルトは、チェックなしです	ボックスにチェックを入れると、ポート転送機能が有効になります。

仮想コンピュータ	デフォルトは、チェックありです	ボックスにチェックを入れると、ポート転送機能が有効になります。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。
キャンセル	該当なし	［キャンセル］ボタンをクリックして、設定をキャンセルします。

仮想サーバーの作成/編集

ゲートウェイを使用すると、仮想サーバールールをカスタム設定することができます。
最大 20 のルールベースの仮想サーバーセットをサポートします。

[追加]ボタンが適用されると、「仮想サーバールール構成」画面を表示します。

項目	設定値	説明
WAN インターフェイス	1. 入力必須 2. デフォルトは、「全部」です	選択したインターフェイスが、ゲートウェイのパケット入力インターフェイスになるように定義します。 フィルタリングするパケットが、WAN-x から来ている場合は、このフィールドで WAN-x を選択します。 任意のインターフェイスからゲートウェイに入ってくるパケットに対して、「全部」を選択します。 WAN-x が有効な場合、WAN-x ボックスを選択することができます。 注：利用可能なチェックボックス（WAN-1～WAN-4）は、製品の WAN インターフェイスの数により異なります。
サーバーIP	入力必須	このフィールドは、上記の WAN インターフェイス設定で選択されたインターフェイスの IP アドレスを指定するためのフィールドです。
プロトコル	入力必須	・「ICMPv4」を選択： パケットフィルタルールのプロトコルが、ICMPv4 であることを意

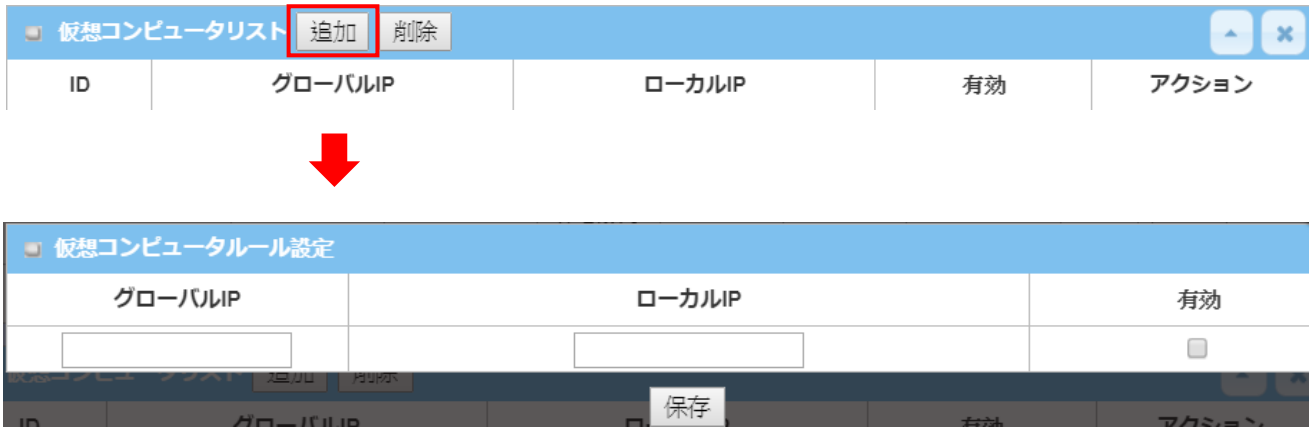
		味します。時間スケジュールのルールに適用し、それ以外の場合は、（常時）にします。 （オブジェクト定義＞「スケジュール設定」を参照） その後、有効ボックスにチェックを入れ、このルールを有効します。 ・「TCP」を選択： パケットフィルタルールの 「プロトコル」が TCP であることを意味します。 「パブリックポート」は、既知のサービスから事前定義されたポートを選択し、「プライベートポート」は、パブリックポート」番号と同じです。 「パブリックポート」は、「単一ポート」を選択してポート番号を指定し、「プライベートポート」は、「単一ポート」番号を設定することができます。 「パブリックポート」は、「ポート範囲」を選択してポート範囲を指定し、「プライベートポート」は、 「単一ポート」または「ポート範囲」を選択できます。 値の範囲： パブリックポート、プライベートポートの場合、1～65535 です。 ・「UDP」を選択： パケットフィルタルールの「プロトコル」が、UDP であることを意味します。 「パブリックポート」は、「既知のサービス」から事前定義されたポートを選択し、「プライベートポート」は、「パブリックポート」番号と同じです。「パブリックポート」は、「単一ポート」を選択してポート番号を指定し、「プライベートポート」は、 「単一ポート」番号を設定することができます。 「パブリックポート」は、「ポート範囲」を選択してポート範囲を選択できます。 値の範囲： パブリックポート、プライベートポートの場合、1～65535 です。 ・「TCP&UDP」を選択： パケットフィルタルールの「プロトコル」が、TCP および UDP であることを意味します。 「パブリックポート」は、「既知のサービス」から事前定義されたポートを選択し、「プライベートポート」は、「パブリックポート」番号と同じです。「パブリックポート」は、「単一ポート」を選択してポート番号を指定し、「プライベートポート」は、「単一ポート」番号を設定することができます。 「パブリックポート」は、「ポート範囲」を選択してポート範囲を指定し、「プライベートポート」は、「単一ポート」または「ポート範囲」を選択できます。 値の範囲：パブリックポート、プライベートポートの場合、1～65535 です。 ・「GRE」を選択： パケットフィルタルールの「プロトコル」が、GRE であることを意味します。 ・「ESP」を選択：

		パケットフィルタルールの「プロトコル」が、ESP であることを意味します。 ・**「SCTP」**を選択： パケットフィルタルールの「プロトコル」が、SCTP であることを意味します。 ・**「ユーザー定義」**を選択： パケットフィルタルールの「プロトコル」が、ユーザー定義であることを意味します。プロトコル番号に対して、ポート番号を入力します。
時間スケジュール	入力必須	時間スケジュールのルールに適用し、それ以外の場合は、「(0)常時」にします。 （「オブジェクト定義」の「スケジュール設定」を参照）
ルール	1. 任意の設定です 2. デフォルトは、チェックなしです	有効ボックスにチェックを入れると、ルールが有効になります。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。

仮想コンピュータの作成/編集

ゲートウェイを使用すると、仮想コンピュータルールをカスタム設定することができます。最大 20 のルールベースの仮想コンピュータセットをサポートします。

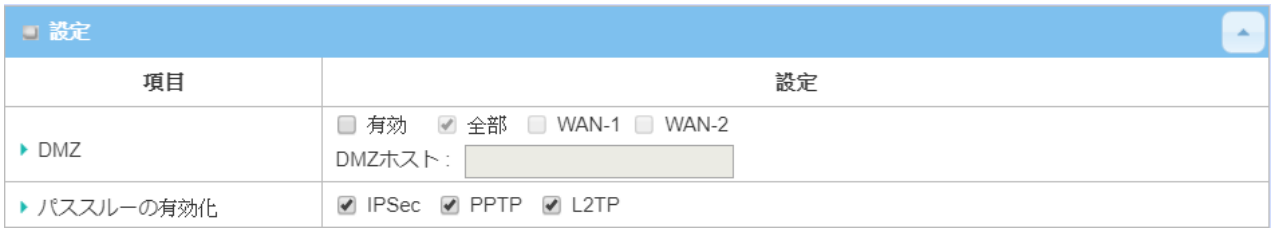
[追加]ボタンが適用されると、「仮想コンピュータルール設定」画面を表示します。



項目	設定値	説明
グローバル IP	入力必須	WAN IP の IP アドレスを指定するためのフィールドです。
ローカル IP	入力必須	LAN IP の IP アドレスを指定するためのフィールドです。
有効	該当なし	ボックスにチェックを入れると、ルールが有効になります。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。

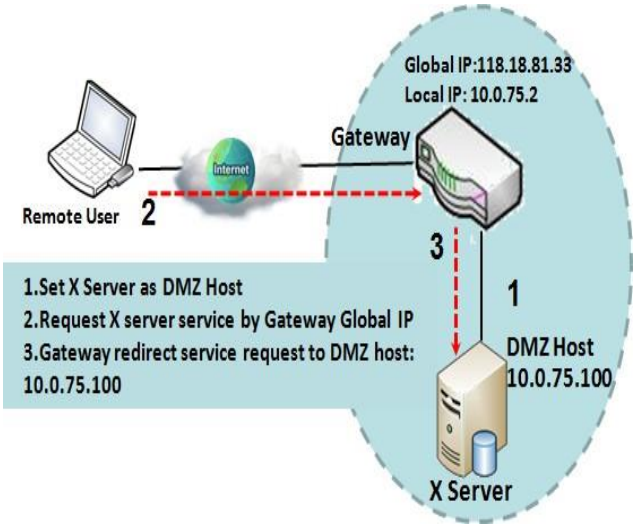
2.5.3　DMZ およびパススルー

DMZ ホストとは、インターネットサイバースペースに露出していますが、ゲートウェイデバイスによるファイアウォール保護範囲内にあるホストです。したがって、この機能により、コンピュータは、インターネットゲーム、テレビ会議、インターネット電話および他の特別なアプリケーションの双方向通信を実行することができます。特定のアプリケーションが、NAT メカニズムによってブロックされている場合、この問題を解決するために LAN コンピュータを DMZ ホストとして指定することができます。



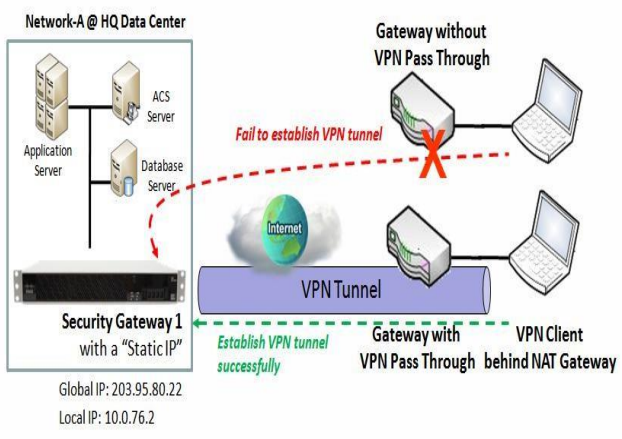
DMZ 機能を使用すると、NAT ゲートウェイの背後にある DMZ ホストに対するすべての通常パケットをゲートウェイが通過させるよう要求することができます（これは、これらのパケットが、ゲートウェイ内のアプリケーションまたはイントラネット内の他のクライアントホストによって受信されることが予想されない場合に限ります）。確かに、DMZ ホストも、ゲートウェイのファイアウォールにより保護されています。機能を有効にし、必要に応じて、イントラネットにホストを持つ DMZ ホストを指定します。

DMZ のシナリオ



ネットワーク管理者が、NAT ゲートウェイの背後にあるホストにいくつかのサービスデーモンを設定して、リモートユーザーが、サーバーからのサービスを積極的に要求できるようにする場合、このホストを DMZ ホストとして構成する必要があります。図に示すように、IP アドレスが 10.0.75.100 の DMZ ホストとして、X サーバーがインストールされています。次に、リモートユーザーは、グローバル IP アドレスが 118.18.81.33 であるゲートウェイが提供するように、X サーバーからサービスを要求することができます。ゲートウェイは、構成された仮想サーバーまたはアプリケーションに属さないパケットを直接 DMZ ホストに転送します。

VPN パススルーのシナリオ



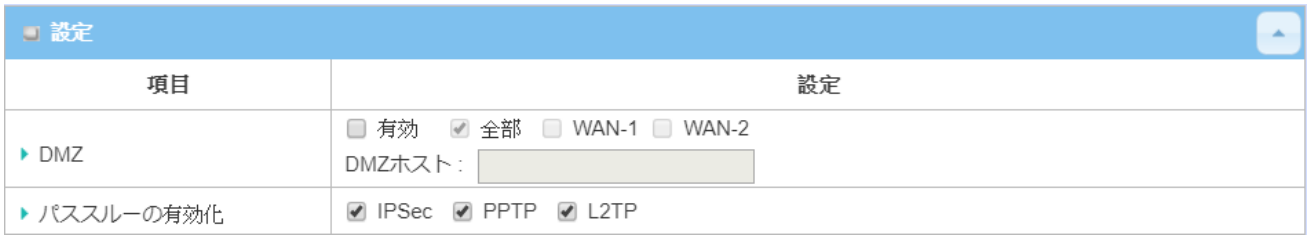
VPN トラフィックは、TCP、または UDP 接続と異なるため、NAT ゲートウェイによりブロックされます。NAT ゲートウェイの背後にある VPN クライアントから開始される VPN 接続のパススルー機能をサポートするため、ゲートウェイは、そのようなアプリケーションに対して、何らかの種類の VPN パススルー機能を実装する必要があります。ゲートウェイは、IPSec、PPTP、および L2TP 接続のパススルー機能をサポートしています。対応するチェックボックスにチェックを入れて、有効してください。

DMZ およびパススルーの設定

基本設定 > ［ポート転送］ > ［DMZ およびパススルー］タブに進みます。

DMZ ホストとは、インターネットサイバースペースに露出していますが、ゲートウェイデバイスによるファイアウォール保護範囲内にあるホストです。

DMZ およびパススルーの有効にする



項目	設定値	説明
DMZ	1. 入力必須 2. デフォルトは、「全部」です	「有効」にチェックを入れると、DMZ 機能が有効になります。選択したインターフェイスをゲートウェイのパケット入力インターフェイスに定義し、DMZ ホストフィールドのホスト LAN IP の IP アドレスに入力します。 フィルタリングするパケットが、WAN-x から来ている場合は、このフィールドで WAN-x を選択します。任意のインターフェイスからルーターに入ってくるパケットに対して、「全部」を選択します。 WAN-x が有効な場合、WAN-x ボックスを選択することができます。 注：利用可能なチェックボックス（WAN-1～WAN-4）は、製品の WAN インターフェイスの数により異なります。

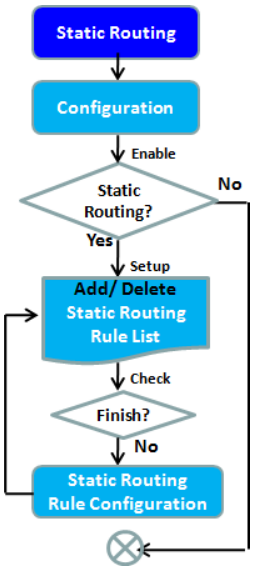
パススルーの有効化	デフォルトは、チェックありです	ボックスにチェックを入れ、IPSec、PPTP および L2TP に対するパススルー機能を有効します。 パススルー機能を有効すると、ゲートウェイの背後にある VPN ホストは、引き続きリモート VPN サーバーに接続できます。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。
キャンセル	該当なし	［キャンセル］ボタンをクリックして、構成した内容を元の設定に復元します。

2-6. ルーティング

基本ネットワーク ＞ ［ルーティング］

ルーターやサブネットが複数ある場合は、ルーティング機能を有効にして、パケットが適切なルーティングパスを経由し、複数のサブネットが相互に通信できるようにする必要があります。ルーティングとは、ネットワーク内で最適なパスを選択するプロセスです。
これは、パケット交換技術を使用して、電子データネットワーク（インターネットなど）のような多くの種類のネットワークで実行されます。ルーティングプロセスは、通常、様々なネットワーク宛先へのルート記録を保持するルーティングテーブルに基づいて転送を指示します。したがって、効率的なルーティングのためには、ルーターのメモリに保持されているルーティングテーブルを構築することが非常に重要です。ほとんどのルーティングアルゴリズムは、一度に１つのネットワークパスしか使用しません。
ルーティングテーブルには、特定の宛先サブネットの事前定義されたルーティングパスが記録されます。これは、静的ルーティングです。ただし、ルーティングテーブルの内容が、RIP、OSPF、BGP などのプロトコルを使用して、取得したルーティングパスを近隣のルーターから記録する場合。これは、動的ルーティングです。これらの両方のルーティングアプローチを１つずつ説明します。

2.6.1　静的ルーティング



設定　[ヘルプ]

項目	設定
静的ルーティング	☑ 有効

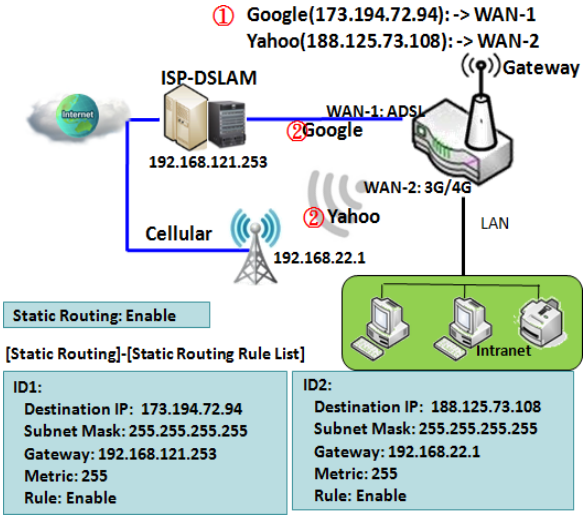
IPv4静的ルーティングルールリスト　追加　削除

ID	宛先IP	サブネットマスク	ゲートウェイIP	インターフェイス	メトリック	有効	アクション

IPv4静的ルーティングルール構成

項目	設定
宛先IP	
サブネットマスク	255.255.255.0 (/24)
ゲートウェイIP	
インターフェイス	自動
メトリック	
ルール	☐ 有効

「静的ルーティング」機能を使用すると、ゲートウェイのルーティングテーブルに格納する一部の専用ホスト/サーバーまたはサブネットのルーティングパスを定義することができます。ゲートウェイは、着信パケットをルーティングテーブルに基づき、異なるピアゲートウェイにルーティングします。静的ルーティング情報をゲートウェイルーティングルールリストに定義する必要があります。



ゲートウェイの管理者は指定したい場合、どのパケット、どのゲートウェイ・インタフェースを経由して転送するのか、および、どのピアゲートウェイで目的地に転送するのか、「静的ルーティング」機能によって実行できます。イントラネットからの専用パケットフローは、手動でシステムルーティングテーブルに定義されて、既定義されたピアゲートウェイと相応ゲートウェイ・インターフェイスを経由して目的地にルーティングされます。
図のように、目的地が Google にアクセスする場合、ルール 1 は ADSL としてインターフェイスを設定し、ルーティングゲートウェイは IP-DSLAM ゲートウェイ 192.168.121.253 となります。 Google へのすべてのパケットは WAN-1 を経由します。 同じ方式で、Yahoo へのアクセスはルール 2 にも適用されます。ルール 2 は、インタフェースとして Cellular (4G/LTE) を設定します。

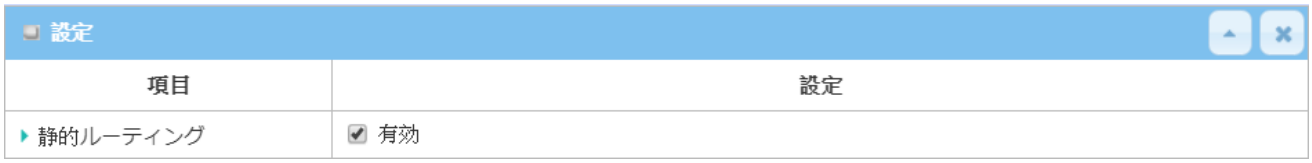
静的ルーティングの設定

基本ネットワーク > ［ルーティング］ > ［静的ルーティング］タブに進みます。

静的ルーティング機能には、「設定」、「静的ルーティングルールリスト」、「静的ルーティングルール構成」の 3 つの構成ウィンドウがあります。
「設定」ウィンドウでは、グローバル静的ルーティング機能を有効することができます。既にルーティングルールがある場合でも、ルーティングを一時的に無効化する場合は、「有効」チェックボックスのチェックを外して、無効化します。
「静的ルーティングルールリスト」ウィンドウには、定義済みのすべての静的ルーティングルールエントリが一覧表示されます。
[追加]、または[編集]ボタンを使って、1 つの新しい静的ルーティングルールを追加および作成する、または、既存の静的ルーティングルールを変更します。
[追加]、または[編集]ボタンが適用されると、静的ルーティングルールを定義するための「静的ルーティングルール構成」ウィンドウが表示されます。

静的ルーティングの有効

有効ボックスにチェックを入れ、「静的ルーティング」機能を有効します。

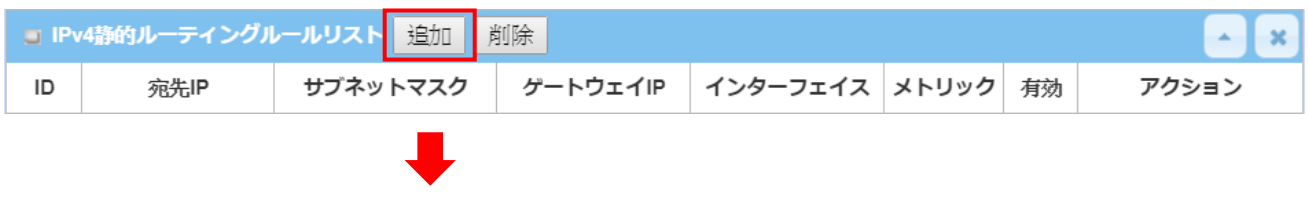


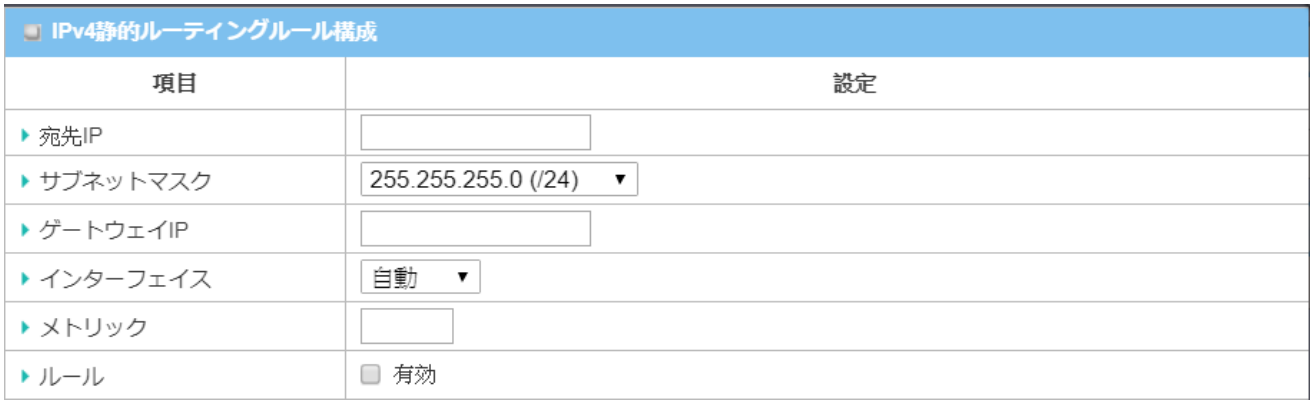
項目	設定値	説明
静的ルーティング	デフォルトは、 チェックなしです	チェックを入れると、この機能が有効になります。

静的ルーティングルールの作成/編集

静的ルーティングルールリストには、すべての静的ルーティングルールエントリの設定パラメータが表示されます。静的ルーティングルールを構成するには、専用ホスト/サーバーまたはサブネットの宛先 IP アドレスおよびサブネットマスク、ピアゲートウェイの IP アドレス、メトリックおよびルールアクティベーションを含む関連パラメータを指定する必要があります。

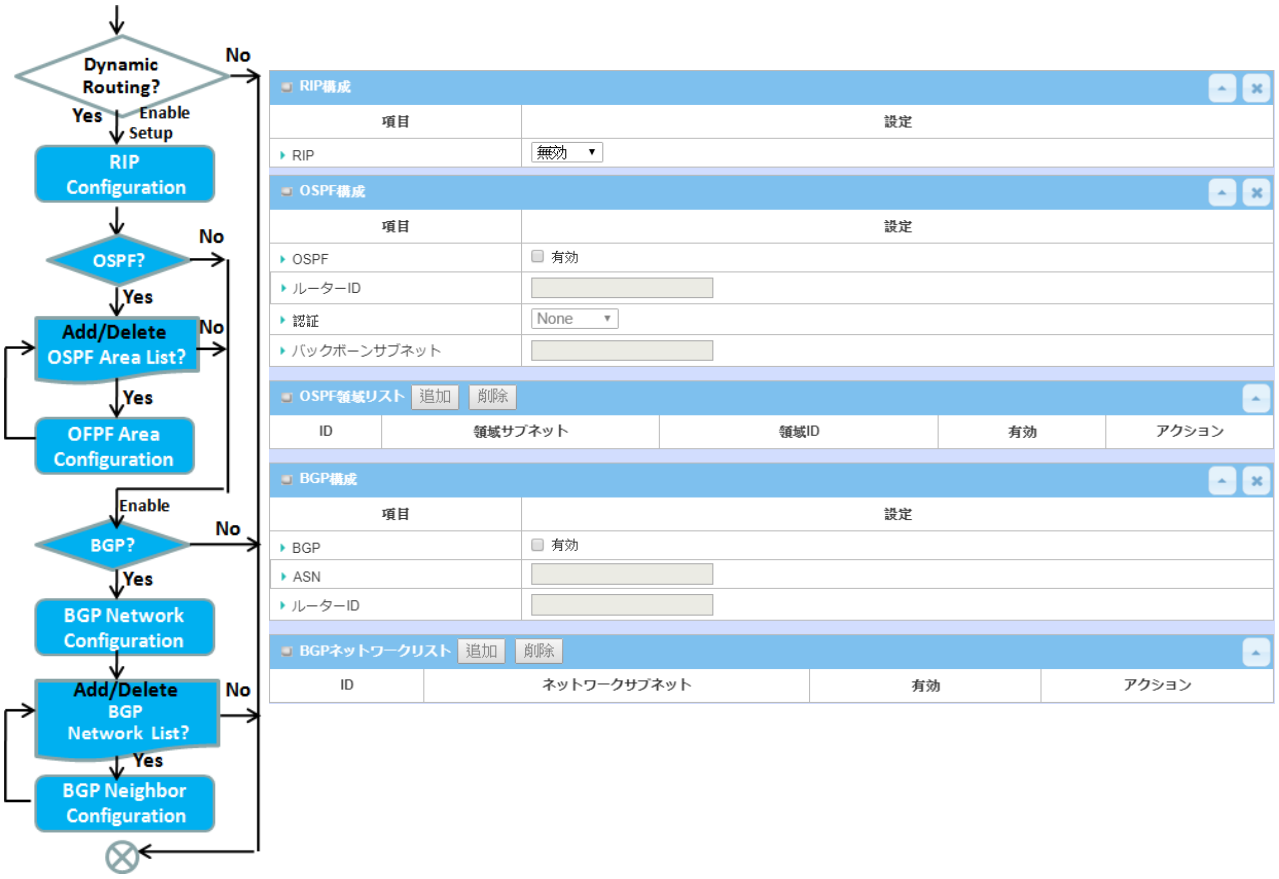
ゲートウェイを使用すると、静的ルーティングルールをカスタム設定することができます。これは、最大 64 のルールセットをサポートします。
[追加]ボタンが適用されると、「静的ルーティングルール構成」画面が表示されます。一方、各静的ルーティングルールの終端の[編集]ボタンを使って、ルールを変更することができます。





IPv4静的ルーティングルール構成		
項目	設定値	説明
宛先 IP	1. IPv4 形式です 2. 入力必須	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	デフォルトで、 255.255.255.0（/24） が設定されています	この静的ルーティングルールのサブネットマスクを指定します。
ゲートウェイ IP	1. IPv4 形式です 2. 入力必須	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	デフォルトは、 「自動」です	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 インターフェイスにすることができます。
メトリック	1. 数値文字列形式です 2. 入力必須	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：0～255
ルール	デフォルトは、 チェックなしです	有効ボックスにチェックを入れると、ルールが有効になります。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。

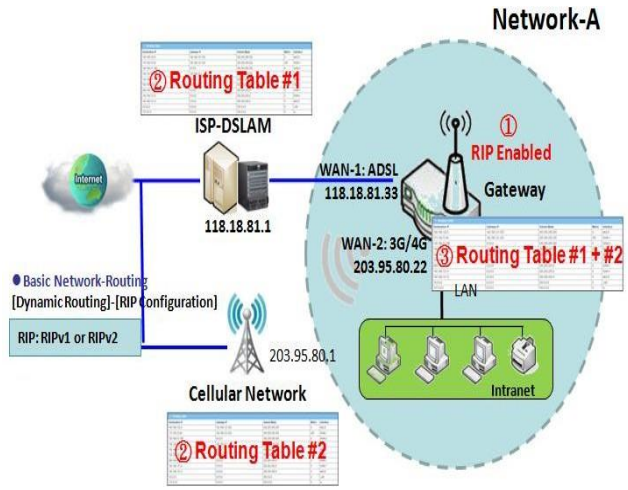
2.6.2　動的ルーティング



適応型ルーティングとも呼ばれる動的ルーティングは、パスが宛先によって特徴付けられるシステムの能力を記述し、パスがネットワーク状態の変化に応答して、システムを通過するパスを変更します。
本ゲートウェイは、ルーティングテーブルを自動的に確立するために、RIPv1 / RIPv2（ルーティング情報プロトコル）、OSPF（オープン最短パスファースト）、BGP（ボーダーゲートウェイプロトコル）などの動的ルーティングプロトコルをサポートしています。動的ルーティング機能は、ネットワークに多数のサブネットがある場合に非常に便利です。一般的に、RIP は小規模のネットワークに適しています。OSPF は中規模のネットワークに適しています。BGP は大規模なネットワークインフラストラクチャで多く使用されます。

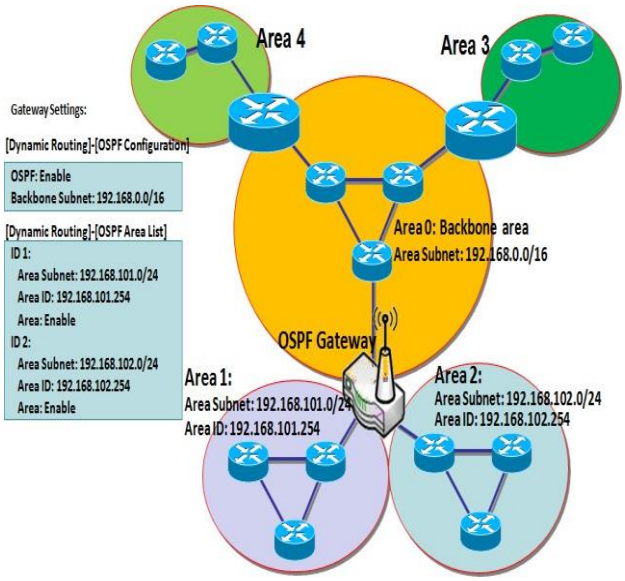
サポートされる動的ルーティングプロトコルは、次のように説明されています。

RIP のシナリオ



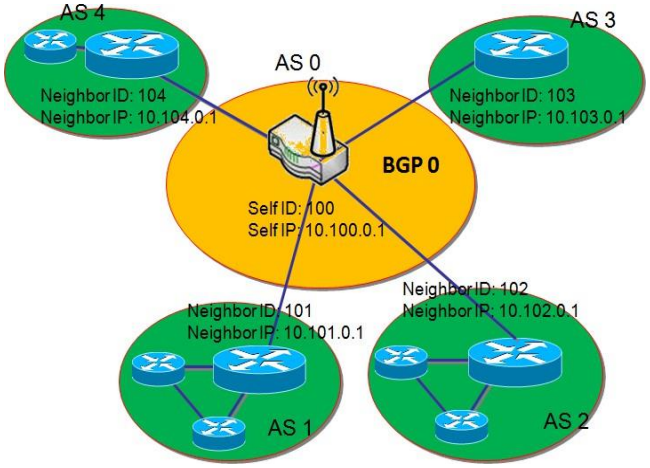
ルーティング情報プロトコル（RIP）とは、ルートメトリックとしてホップカウントを使用する、最も古い距離ーベクトルルーティングプロトコルの 1 つです。RIP は、送信元から宛先に対するパスで許可されるホップカウントに制限を実装することによって、ルーティングループを防止します。許可される RIP の最大ホップカウントは 15 です。しかし、このホップ制限により、RIP がサポートできるネットワークサイズも制限されます。16 のホップカウントは無限遠とみなされます。つまり、パスは到達不能とみなされます。RIP は、スプリットホライズン、ルートポイズニングおよびホールドダウンメカニズムを実装して、間違ったルーティング情報が伝播されないようにします。

OSPF のシナリオ



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。これは、大規模な企業ネットワークで最も広く使用されている IGP（Interior Gateway Protocol）です。使用可能なルーターからリンクステート情報を収集し、ネットワークのトポロジマップを構築します。トポロジは、宛先 IP アドレスのみに基づいてデータグラムをルーティングするルーティングテーブルとして提示されます。
ネットワーク管理者は、企業バックボーンからルーティングテーブルを取得し、企業バックボーンにリンクされていない他のルーターにルーティング情報を転送するために、大規模な企業ネットワークに OSPF ゲートウェイを配置することができます。
通常、OSPF ネットワークは、ルーティング領域に細分され、
管理を簡素化し、トラフィックとリソースの使用率を最適化します。
図に示すように、OSPF ゲートウェイは、エリア 0 のバックボーンゲートウェイからルーティング情報を収集し、そのルーティング情報をバックボーンにないエリア 1 とエリア 2 のルーターに転送します。

BGP のシナリオ



Border Gateway Protocol（BGP）とは、インターネット上の自律システム（AS）間でルーティング と到達可能性の情報を交換するために設計された標準的な外部ゲートウェイプロトコルです。通常、パス、ネットワークポリシー、または、ルールセットに基づいてルーティングを決定します。
ほとんどの ISP は、BGP を使って、相互間のルーティングを確立します（特にマルチホームの場合）。非常に大規模なプライベート IP ネットワークも内部的に BGP を使用します。ある AS 内の主要な BGP ゲートウェイは、ルーティング情報を交換するため、いくつかの他の境界ゲートウェイとリンクします。
これは、AS 内で収集したデータを他の AS 内のすべてのルーターに配布します。
図に示すように、BGP 0 は AS 0 を支配するゲートウェイです（自己 IP は 10.100.0.1、および、自己 ID は 100 です）。これは、インターネット内の他の BGP ゲートウェイとリンクします。このシナリオは、ある ISP のサブネットと他の ISP のサブネットがリンクするようなものです。BGP プロトコルで動作することにより、BGP 0 は、インターネット内の他の BGP ゲートウェイからルーティング情報を収集することができます。そして、ルーティングデータをその支配された AS 内のルーターに転送します。最後に、AS 0 にあるルーターは、パケットを他の AS にルーティングする方法を理解します。

動的ルーティングの設定

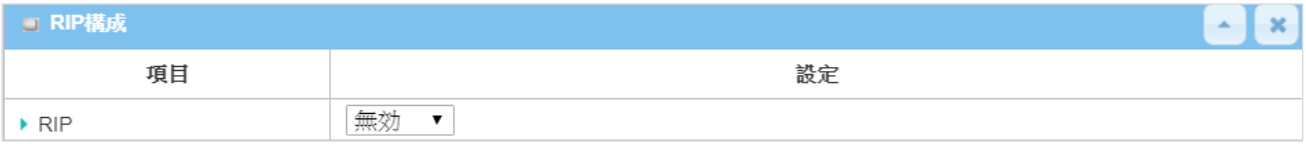
基本ネットワーク > **［ルーティング］** > **［動的ルーティング］タブ**に進みます。

動的ルーティング設定により、オフィス設定に基づき、ルーター経由で RIP、OSPF、および、BGP プロトコルをカスタマイズすることができます。

「動的ルーティング」ページには、動的ルーティング機能用の 7 つの設定ウィンドウがあります。「RIP 構成」、「OSPF 構成」、「OSPF 領域リスト」、「OSPF 領域構成」、「BGP 構成」、「BGP 近隣リスト」、「BGP 近隣構成」ウィンドウです。
RIP、OSPF、および、BGP プロトコルは、個別に構成することができます。
「RIP 構成」ウィンドウでは、有効または無効化する RIP プロトコルのバー ジョンを選択することができます。「OSPF 構成」ウィンドウでは、OSPF 動的ルーティングプロトコルを有効し、そのバックボーンサブネットを指定することができます。
さらに、「OSPF 領域リスト」ウィンドウには、OSPF ネットワーク内のすべての定義済み領域が一覧表示されます。
ただし、「BGP 構成」ウィンドウでは、BGP 動的ルーティングプロトコルを有効して、自己 ID を指定することができます。「BGP 近隣リスト」ウィンドウには、BGP ネットワーク内のすべての定義済みの近隣が一覧表示されます。

RIP 構成

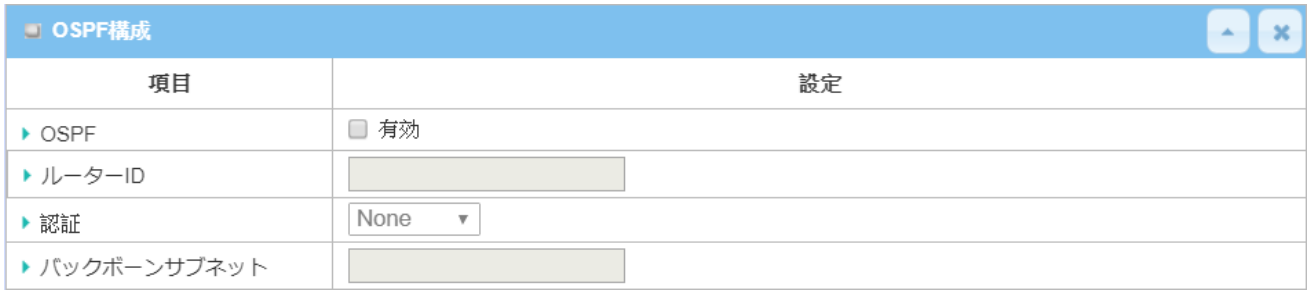
RIP 構成設定では、オフィス設定に基づき、ルーター経由で RIP プロトコルをカスタマイズすることができます。



項目	設定値	説明
RIP	デフォルトは、 「無効」です	「無効」を選択すると、RIP プロトコルが無効されます。 RIP v1 を選択すると、RIPv1 プロトコルが有効されます。 RIP v2 を選択すると、RIPv2 プロトコルが有効されます。

OSPF 構成

OSPF 構成設定では、オフィス設定に基づき、ルーター経由で OSPF プロトコルをカスタマイズすることができます。



項目	設定値	説明
OSPF	デフォルトは、 チェックなしです	有効ボックスにチェックをつけると、OSPF プロトコルを有効にします。
ルーターID	1.IPv4 形式です 2.入力必須	OSPF ロトコル上のこのルーターのルーターID です。
認証	デフォルトは、 「なし」です	OSPF プロトコル上のこのルーターの認証方法です。 ・**「なし」**を選択すると、OSPF プロトコル上の Authentication（認証）が無効化されます。 ・**「テキスト」**を選択すると、OSPF プロトコル上のこのフィールドに Key（キー）が入力された Text Authentication（テキスト認証）が有効化されます。 ・**「MD5」**を選択すると、OSPF プロトコル上のこれらのフィールドに ID と Key（キー）が入力された MD5 Authentication（MD5 認証）が有効化されます。
バックボーンサブネット	1.Classless Inter Domain Routing（CIDR）サブネットマスク表記法です。 （例：192.168.1.0/24） 2.入力必須	OSPF プロトコル上のこのルーターのバックボーンサブネットです。

OSPF 領域ルールの作成/編集

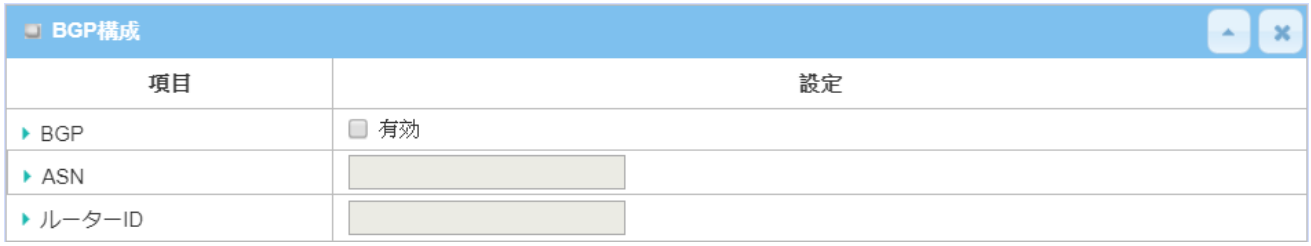
ゲートウェイにより、OSPF 領域リストのルールをカスタマイズすることができます。
これは、最大 32 のルールセットをサポートします。

[追加]ボタンが適用されると、「OSPF 領域ルール構成」画面を表示します。

OSPF 領域構成		
項目	設定値	説明
領域サブネット	1.Classless Inter Domain Routing （CIDR）サブネットマスク表記法です。（例：192.168.1.0/24） 2.入力必須	OSPF 領域リスト上のこのルーターの領域サブネットです。
領域 ID	1.IPv4 形式です 2.入力必須	OSPF 領域リスト上のこのルーターの領域 ID です。
領域	デフォルトは、チェックなしです	有効ボックスにチェック入れて、本ルールを有効にします。
保存	該当なし	[保存]ボタンをクリックして、構成を保存します。

BGP 構成

BGP 構成では、ルーター設定を通して、BGP プロトコルをカスタマイズすることができます。

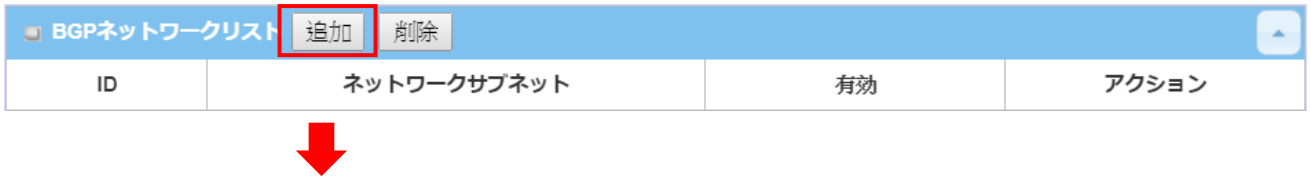


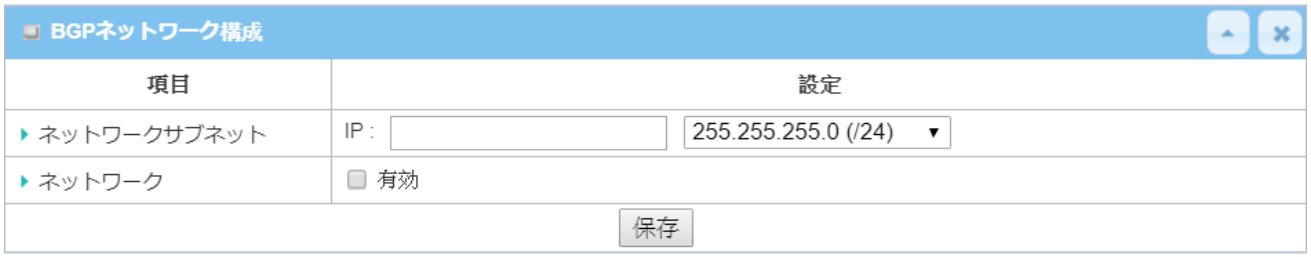
BGP ネットワーク構成		
項目	設定値	説明
BGP	デフォルトは、 チェックなしです	チェックをつけると、BGP プロトコルを有効にします。
ASN	1. 数値文字列形式です 2. 入力必須	BGP プロトコル上のこのルーターの ASN Number（ASN 番号）です。 値の範囲：1～4294967295
ルーターID	1. IPv4 形式です 2. 入力必須	BGP プロトコル上のこのルーターのルーターID です。

BGP ネットワークルールの作成/編集

ゲートウェイを使用すると、BGP ネットワークルールをカスタム設定することができます。これは、最大 32 のルールセットをサポートします。

[追加]ボタンが適用されると、「BGP ネットワークルール構成」画面を表示します。





項目	設定値	説明
ネットワーク サブネット	1. IPv4 形式です 2. 入力必須	BGP ネットワークリスト上のこのルーターのネットワークサブネットです。このフィールドには IP アドレスと選択されたサブネットマスクが入力されています。
ネットワーク	デフォルトは、 チェックなしです	有効ボックスにチェックをつけると、本ルールを有効にします。
保存	該当なし	[保存]ボタンをクリックして、構成を保存します。

BGP 近隣ルールの作成/編集

ゲートウェイを使用すると、BGP 近隣ルールをカスタム設定することができます。
これは、最大 32 のルールセットをサポートします。

[追加]ボタンが適用されると、「BGP 近隣ルール構成」画面を表示します。

項目	設定値	説明
近隣 IP	1. IPv4 形式です 2. 入力必須	BGP 近隣リスト上の、このルーターの NeighborIP（近隣 IP）です。
リモート ASN	1. 数値文字列形式です 2. 入力必須	BGP 近隣リスト上の、このルーターの RemoteASN（リモート ASN）です。 値の範囲： 1～4294967295
近隣	デフォルトは、 チェックなしです	有効ボックスのチェックをつけて、本ルールを有効にします。
保存	該当なし	[保存]ボタンをクリックして、構成を保存します。

2.6.3　ルーティング情報

ルーティング情報により、ルーティングテーブルおよびポリシールーティング情報を表示することができます。
ポリシールーティング情報は、負荷分散機能が有効になっていて、負荷分散戦略がユーザーポリシーである場合にのみ使用できます。

基本ネットワーク > **［ルーティング］** > **［ルーティング情報］タブ**に進みます。

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
10.91.182.128	255.255.255.240	0.0.0.0	0	WAN-2
192.168.11.0	255.255.255.0	0.0.0.0	0	WAN-1
192.168.123.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
118.0.0.0	255.0.0.0	0.0.0.0	0	WAN-1
118.0.0.0	255.0.0.0	0.0.0.0	0	WAN-2
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

項目	設定値	説明
宛先 IP	該当なし	宛先 IP のルーティング記録です。IPv4 形式です。
サブネットマスク	該当なし	サブネットマスクのルーティング記録です。IPv4 形式です。
ゲートウェイ IP	該当なし	ゲートウェイ IP のルーティング記録です。IPv4 形式です。
メトリック	該当なし	メトリックのルーティング記録です。数値文字列形式です。
インターフェイス	該当なし	インターフェイスタイプのルーティング記録です。文字列形式です。

ポリシールーティング情報

ポリシールーティングソース	送信元IP	宛先IP	宛先ポート	WANインタフェース
負荷分散	-	-	-	-

項目	設定値	説明
ポリシールーティングソース	該当なし	ソースのポリシールーティングです。文字列形式です。
送信元 IP	該当なし	送信元 IP のポリシールーティングです。IPv4 形式です。
宛先 IP	該当なし	宛先 IP のポリシールーティングです。IPv4 形式です。
宛先ポート	該当なし	宛先ポートのポリシールーティングです。文字列形式です。
WAN インタフェース	該当なし	WAN インタフェースのポリシールーティングです。文字列形式です。

2-7. DNS および DDNS　【未対応】

本製品ではサポートされていない機能です。

第3章. オブジェクト定義

3-1. スケジュール設定

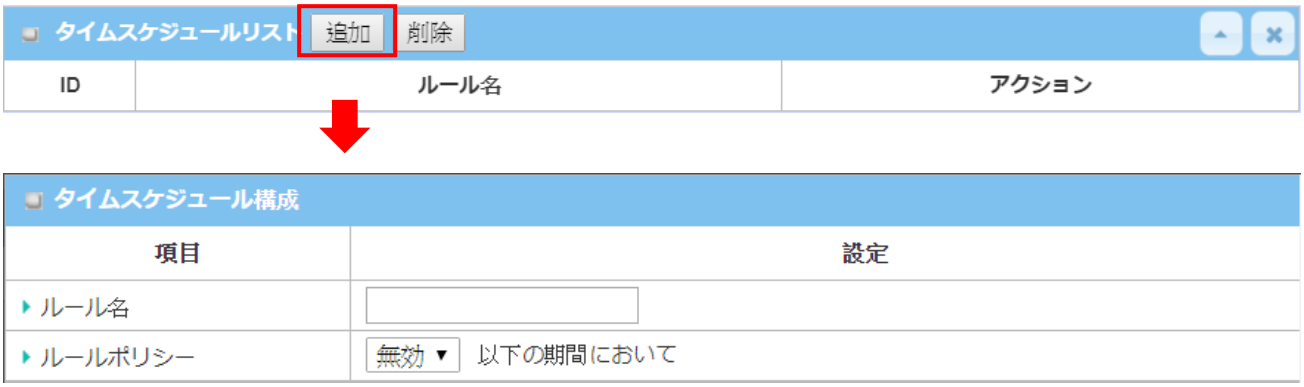
スケジュール設定は、他の機能に適用可能なタイムスケジュールルールを追加/削除する機能を提供します。

3.1.1　スケジュール設定構成

オブジェクト定義 > **［スケジューリング］** > **［設定］タブ**に進みます。

項目	設定値	説明
追加	該当なし	[追加]ボタンをクリックして、タイムスケジュールルールを構成します。
削除	該当なし	[削除]ボタンをクリックして、選択したルールを削除します。

[追加]ボタンが適用されると「タイムスケジュール構成」、および「期間定義」画面を表示します。



項目	設定値	説明
ルール名	文字列：任意のテキスト	ルール名を設定します。
ルールポリシー	デフォルトは、「無効」です	以下の期間において、機能の無効/有効を適用します。

項目	設定値	説明
週日	メニューから選択	毎日または曜日のいずれかを選択します。
開始時間	時間フォーマット（hh:mm）	選択した曜日の開始時間です。
終了時間	時間フォーマット（hh:mm）	選択した曜日の終了時間です。
保存	該当なし	[保存]ボタンをクリックして、設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、設定をキャンセルします。

3-2. ユーザー　【未対応】

本製品ではサポートされていない機能です。

3-3. グループ化　【未対応】

本製品ではサポートされていない機能です。

3-4. 外部サーバー　【未対応】

本製品ではサポートされていない機能です。

3-5. 証明書　【未対応】

本製品ではサポートされていない機能です。

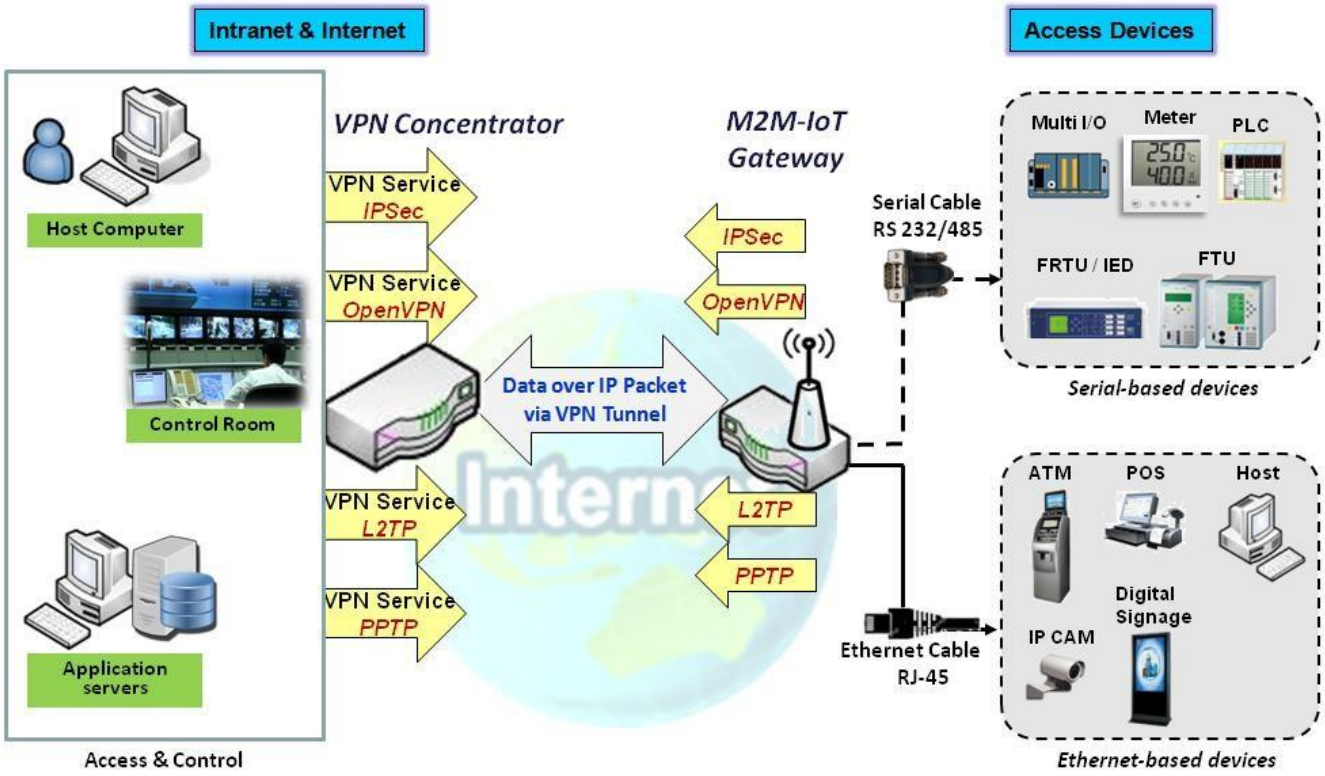
第4章. フィールド通信　【未対応】

本製品ではサポートされていない機能です。

第5章. セキュリティ

5-1. VPN

仮想プライベートネットワーク（VPN）はプライベートネットワークをインターネットなどのパブリックネットワークにまたがって拡張する機能です。これにより、コンピュータはプライベートネットワークに直接接続しているかのようにして、共有ネットワークやパブリックネットワークにまたがってデータの送受信を行うことができます。また、プライベートネットワークの機能、セキュリティ、管理ポリシーを利用することができます。この機能を利用するには、専用の接続続や暗号化、またはその両方を使用して仮想ポイントツーポイント接続を確立します。トンネル技術では、カプセル化プロトコル、暗号化アルゴリズム、ハッシュアルゴリズムを利用することにより、データの機密性、データの送信元認証、データの統合性を実現します。



本製品シリーズは、IPSec、OpenVPN、L2TP（over IPSec）、PPTP、GRE など、データ転送のために複数サイト間で安全なトンネルを確立するためのさまざまなトンネリング技術をサポートしています。

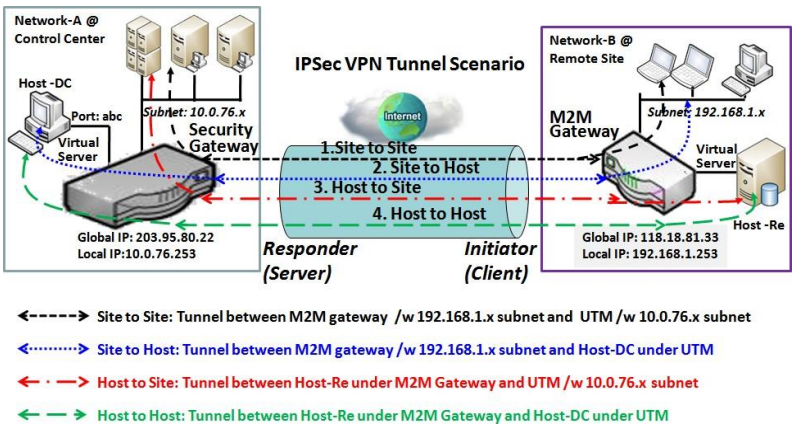
※OpenVPN、PPTP、GRE は、本製品ではサポートされていない機能です。

5.1.1　IPSec

IPSec（インターネットプロトコルセキュリティ）は、IP（インターネットプロトコル）通信をセキュリティ保護するために、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プロトコルスイートです。IPSec には、セッション開始時にエージェント間で相互認証を行い、セッション中に使用する暗号キーのネゴシエーションを行うためのプロトコルが含まれます。

IPSec クライアントとサーバーの間で、IPSec VPN トンネルが確立されます。IPSec VPN クライアントは「イニシエーター」、IPSec VPN サーバーは「レスポンダ」と呼ばれることもあります。このゲートウェイは、さまざまな役割として構成したり、さまざまなリモートデバイスとのトンネル数を確立したりすることができます。VPN 接続を設定する前に、トンネリングのシナリオタイプを決定する必要があります。

IPSec トンネルのシナリオ



IPSec トンネルを構築するには、IPSec ピアの背後にあるホストがリモートサイトまたはホストにアクセスできる場合は、リモートゲートウェイのグローバル IP とオプションのサブネットを入力する必要があります。このような構成では、次の 4 つのシナリオがあります。

Site to Site（サイト間）:
両方のゲートウェイのリモートゲートウェイ IP とサブネットを設定する必要があります。IPSec トンネルが確立すると、両方のゲートウェイの背後にあるホストは、トンネルを介して互いに通信することができます。

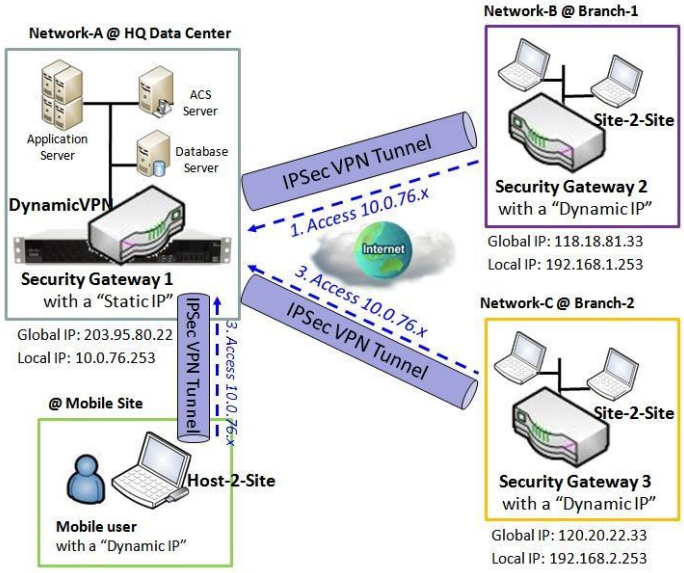
Site to Host（サイトからホスト）:
Site to Host（サイトからホスト）は、サブネット内のクライアントとアプリケーショ

ンサーバー（ホスト）間のトンネリングに適しています。図のように、M2M ゲートウェイの背後にあるクライアントは、Site to Host VPN トンネルを介して、コントロールセンターにあるホスト「Host-DC」にアクセスすることができます。

Host to Site（ホストからサイト）:
対照的に、単一ホスト（またはモバイルユーザー） がイントラネット内のリソースにアクセスするためには、ホストからサイトへのシナリオを適用することができます。

Host to Host（ホスト間）:
Host to Host（ホスト間）は、2 つの単一ホストの間に VPN トンネルを構築するための特別な構成です。

動的 VPN サーバーのシナリオ



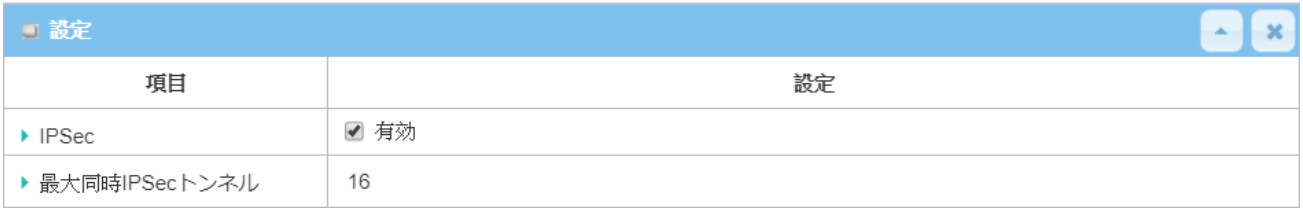
動的 VPN サーバーのシナリオは、特に動的 IP を使用するモバイルクライアントの場合、リモートサイトで複数のトンネルを構築する効率的な方法です。このシナリオでは、ゲートウェイはサーバー（レスポンダ） の役割のみになり、「Static IP（静的 IP）」または「FQDN」が必要です。
これにより、多くの VPN クライアント（イニシエータ）が、さまざまなトンネルシナリオに接続できるようになります。要するに、単純な動的 VPN サーバー設定では、多くの VPN クライアントが、サーバーに接続することができます。
しかし、ハブアンドスポークのメカニズムと比較して、動的 VPN サーバー経由で、任意の 2 つのクライアント間で直接通信することはできません。
購入したゲートウェイの場合は、WAN インターフェイスごとに 1 つの動的 VPN サーバーを構成することができます。

IPSec の設定

セキュリティ > [VPN] > [IP Sec] タブに進みます。

IPSec 設定により、IPSec トンネルを作成および構成することができます。

IPSec の有効



項目	設定値	説明
IPSec	デフォルトは、チェックなしです	有効ボックスにチェックをすると、IPSec 機能を有効にします。
最大同時 IPSec トンネル	製品仕様に依存します	指定された値は、同時 IPSec トンネル接続の最大数を制限します。 ※購入したモデルのデフォルト値は異なる場合があります。
保存	該当なし	[保存]ボタンをクリックして、設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、設定をキャンセルします。

IPSec トンネルの作成/編集

IPSec トンネル設定をさらに構成する前に、IPSec 有効ボックスにチェックが入っていることを確認して有効にしてください。

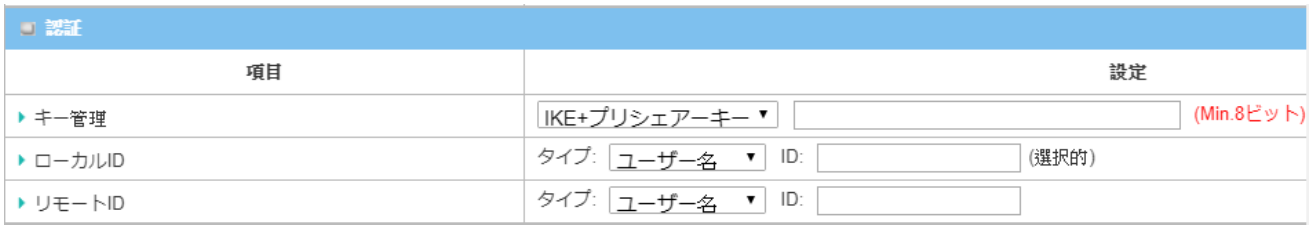
［追加/編集］ボタンが適用されると、構成画面を表示します。

トンネル構成、ローカルおよびリモート構成、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 プロポーザル定義です。
ローカルとリモートの両方の VPN デバイスのトンネルの詳細を設定する必要があります。

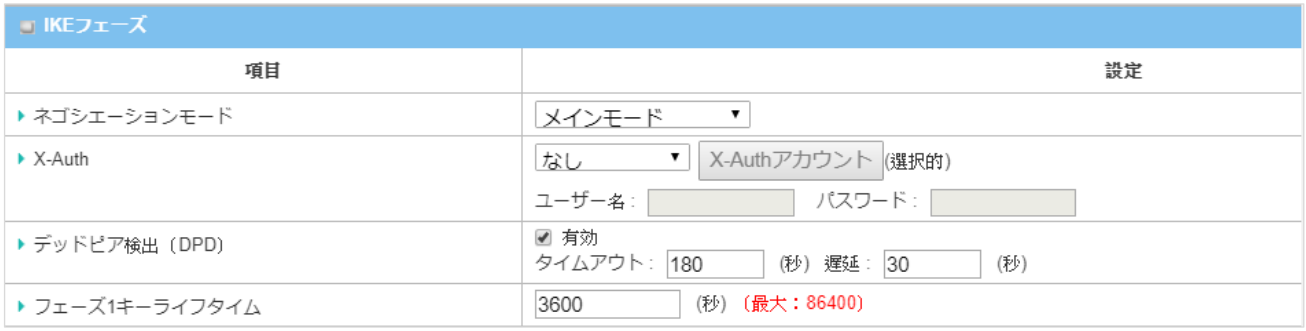
トンネル構成		
項目	設定値	説明
トンネル	デフォルトは、チェックなしです	有効ボックスにチェックを入れると、IPSec トンネルを有効にします。
トンネル名	1. 入力必須 2. 文字列形式は、任意のテキストです	トンネル名（識別しやすい名称）を入力します。 値の範囲： 1～19 文字
インターフェイス	1. 入力必須 2. デフォルトは、「WAN-1」です	IPSec トンネルを確立するインターフェイスを選択します。これは、利用可能な WAN および LAN インターフェイスにすることができます。
トンネルシナリオ	1. 入力必須 2. デフォルトは、「Site-to-site」です	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（サイト間）、Site-to-Host（サイトからホスト）、Host-to-Site（ホストからサイト）、または、Host-to-Host（ホスト間）から選択します。 LAN インターフェイスが選択されている場合は、Host-to-Host（ホスト間）シナリオのみが利用可能です。 ・Site-to-Site、Site-to-Host、Host-to-Site、IPSec は、トンネルモードでのみ動作します。それらの違いは、サブネットの数です。 ・Host-to-Host（ホスト間）では、IPSec は、転送モードで動作します。
トンネル TCP MSS	1. 入力必須 2. デフォルトは、「Auto」です 3. 最大 1500	IPSec トラフィックの場合、項目は、自動的に TCP MSS を 3 方向ハンドシェイクで調整します。 これは、VPN 外部インターフェイスで有効になっている［Adjust TCP MSS（TCP MSS の調整）］オプションに関係なく発生します。 値の範囲：64～1500Bytes
カプセル化 プロトコル	1. 入力必須 2. デフォルトは、「ESP」です	この IPSec トンネルのドロップダウンボックスから、カプセル化プロトコルを選択します。 利用可能なカプセル化は、「ESP」と「AH」です。

IKE バージョン	1. 入力必須 2. デフォルトは、「v1」です	この IPSec トンネルの IKE バージョンを指定します。 v1 または v2 を選択します。 注：トンネルシナリオの動的 VP オプションが選択されている場合、または、カプセル化プロトコルで「AH」が選択されている場合、IKE バージョンは使用できません。

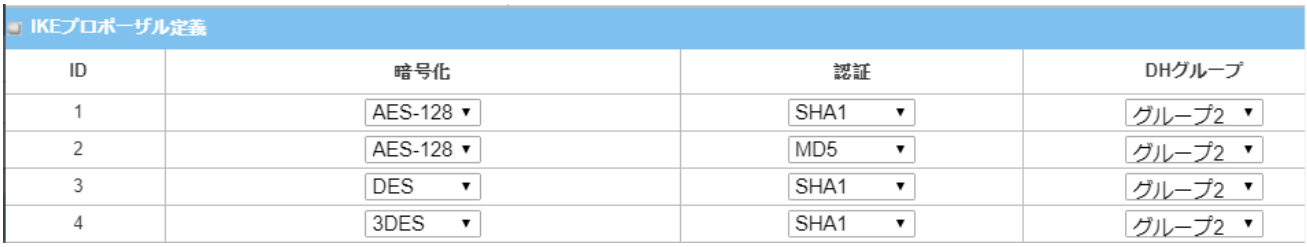
ローカル＆リモート設定		
項目	**設定値**	**説明**
ローカル サブネットリスト	1. 入力必須	ローカルサブネット IP アドレスとサブネットマスクを指定します。 ［追加］、または［削除］ボタンをクリックして、ローカルサブネットを追加、または削除します。 注_1：トンネルシナリオの 動的 VPN を選択すると、使用できるサブネットは 1 つだけになります。 注_2：トンネルシナリオの Host-to-Site、または Host-to-Host を選択すると、ローカルサブネットは使用できなくなります（[追加] ボタンは押せません）。 注_3： Hub and Spoke（ハブアンドスポーク）の Hub and Spoke（ハブアンドスポーク）オプションを選択すると、使用できるサブネットは 1 つだけになります。 ［有効］ボックスにチェックを入れ、トラフィックのリダイレクト機能を有効します。
リモート サブネットリスト	1. 入力必須	リモートサブネット IP アドレスとサブネットマスクを指定します。 ［追加］、または［削除］ボタンをクリックして、リモートサブネット設定を追加/削除します。
リモート ゲートウェイ	1. 入力必須 2. フォーマットには、IPv4 アドレス、または FQDN を使用することができます	リモートゲートウェイを指定します。



認証構成		
項目	設定値	説明
キー管理	1. 入力必須 2. 事前共有キー： 8～32 文字	この IPSec トンネルのドロップダウンボックスから、キー管理を選択します。 IKE+プリシェアーキー（事前共有キー）：キー（8～32 文字）を設定する必要があります。 IKE+X.509：認証するための証明書が必要です。 IKE+X.509 は、証明書が正しく構成されている場合にのみ使用できます。 このマニュアルの「証明書」セクション、および、Web ベースユーティリティの［オブジェクト定義］ >「証明書」を参照してください。 **※「証明書」は、本製品では対応しておりません。** ・手動：認証するためのキーID を入力する必要があります。 手動キー構成については、後述の手動キー管理のセクションで説明します。
ローカル ID	任意の設定	認証するこの IPSec トンネルのローカル ID を指定します。 ローカル ID の「ユーザー名」を選択し、ユーザー名を入力します。 ユーザー名にはすべての数字を含めることはできますが、すべてを数字にすることはできません。 ・ローカル ID の「FQDN」を選択し、FQDN を入力します。 ・ローカル ID の「User@FQDN」を選択し、User@FQDN を入力します。 ・ローカル ID の「キーID」を選択し、キーID（英字または数字）を入力します。
リモート ID	任意の設定	認証するこの IPSec トンネルのリモート ID を指定します。 リモート ID の「ユーザー名」を選択し、ユーザー名を入力します。ユーザー名にはすべての数字を含めることはできますが、すべてを数字にすることはできません。 ・リモート ID の「FQDN」を選択し、FQDN を入力します。 ・リモート ID の「User@FQDN」を選択し、User@FQDN を入力します。 ・リモート ID の「キーID」を選択し、「キーID」（英字または数字）を入力します。 注：トンネルシナリオの Dynamic VPN（動的 VPN）を選択すると、リモート ID は、使用することができません。

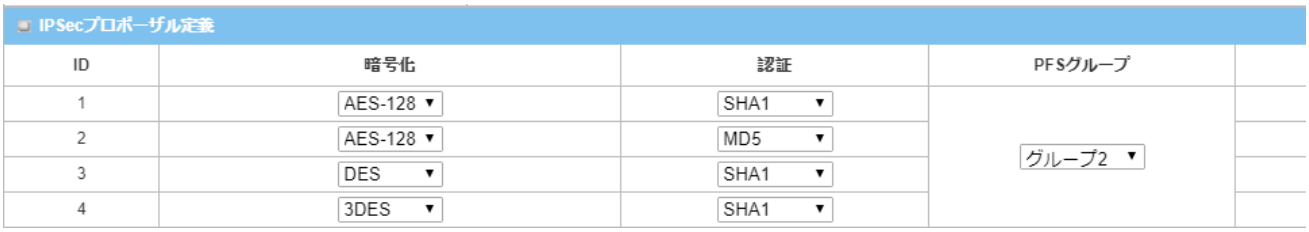


IKEフェーズ		
項目	設定値	説明
ネゴシエーションモード	デフォルトは、「メインモード」です	この IPSec トンネルのネゴシエーションモードを指定します。「メインモード」、または「アグレッシブモード」を選択します。
x-Auth	デフォルトは、「なし」です	この IPSec トンネルの X-Auth の役割を指定します。「サーバー」、「クライアント」、「なし」から選択します。 ・**なし**が選択された場合：X-Auth 認証は不要です。 ・**サーバー**が選択された場合：このゲートウェイは、X-Auth サーバーになります。X-Auth Account（X-Auth アカウント）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**が選択された場合：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入力します。 注： トンネルシナリオで、Dynamic VPN（動的 VPN）を選択すると、X-Auth クライアントは使用できなくなります。
デッドピア検出（DPD）	1. デフォルトは、チェックありです 2. デフォルトタイムアウトは 180 秒、遅延は 30 秒です	有効ボックスにチェックを入れて、DPD 機能を有効します。 タイムアウト、および遅延時間を秒単位で指定します。 「タイムアウト」と「遅延」の値の範囲： 0～999 秒
フェーズ 1 キーライフタイム	1. 入力必須 2. デフォルトは 3600 秒です 3. 最大 86400 秒	フェーズ 1 キーライフタイムを指定します。 値の範囲： 30～86400



IKEプロポーザル定義		
項目	設定値	説明
プロポーザル定義	入力必須	・「暗号化」方法を指定します。 DES / 3DES / AES-128 / AES-192 / AES-256 から指定します。 ・「認証」方法を指定します。 なし /MD5 / SHA1 / SHA2-256 から指定します。 ・「DH グループ」を指定します。 なし /グループ 1 /グループ 2 /グループ 5/ グループ 14/グループ 15/グループ 16 /グループ 17 / グループ 18 から指定します。 有効ボックスにチェックを入れて、この設定を有効します。

IPSecフェーズ		
項目	設定値	説明
フェーズ 2 キーライフタイム	1. 入力必須 2. デフォルトは、28800 秒です	フェーズ 2 キーライフタイムを指定します。 値の範囲： 30～86400

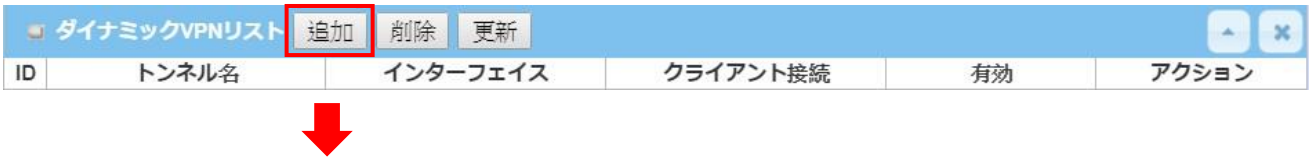


IPSecプロポーザル定義		
項目	設定値	説明
プロポーザル定義	入力必須	・「暗号化」方法を指定します。 なし / DES / 3DES / AES-128 / AES-192 / AES-256 から指定します。 注：「なし」は、カプセル化プロトコルが、AH として設定されている場合にのみ使用できます。 ESP カプセル化には使用できません。 ・「認証」方法を指定します。 なし / MD5 / SHA1 / SHA2-256 から指定します。

		注：「なし」、および「SHA2-256」は、カプセル化プロトコルが、「ESP」として設定されている場合にのみ使用できます。AH カプセル化には使用できません。 ・「PFS グループ」を指定します。 なし /グループ 1 /グループ 2 /グループ 5 / グループ 14 /グループ 15 /グループ 16 /グループ 17 /グループ 18 です。 有効ボックスにチェックを入れて、この設定を有効します。
保存	該当なし	［保存］をクリックして、設定を保存します。
もとに戻す	該当なし	［元に戻す］をクリックして、設定をキャンセルします。
前へ	該当なし	［前へ］をクリックして、前ページに戻ります。

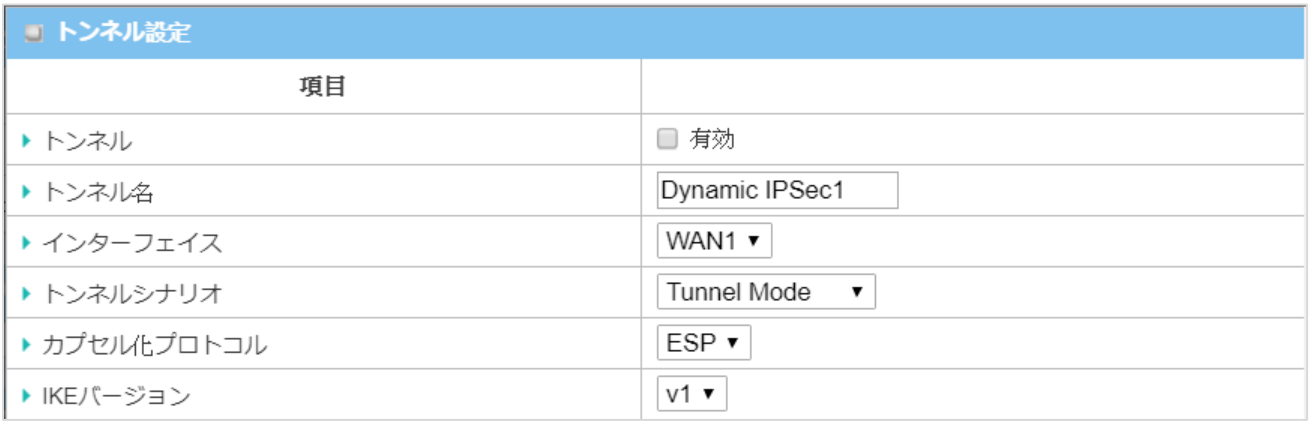
動的 VPN サーバーリストの作成/編集

サイト/ホスト/サイト/ホストシナリオ用の IPSec VPN トンネルを作成する場合と同様に、［編集］ボタンが適用されると、一連の構成画面が表示されます。



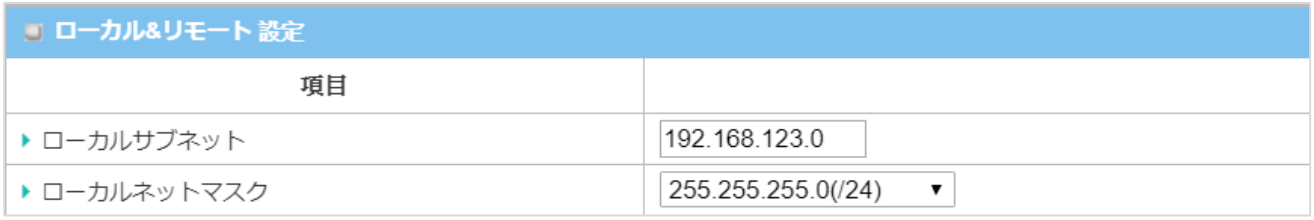
トンネル構成、ローカルおよびリモート構成、認証、IKE フェーズ、IKE プロポーザル定義、IPSec フェーズ、および IPSec プロポーザル定義です。
動的 VPN サーバーとしてゲートウェイのトンネルの詳細を構成する必要があります。

注：購入したゲートウェイの場合は、WAN インターフェイスごとに 1 つの動的 VPN サーバーを構成することができます。

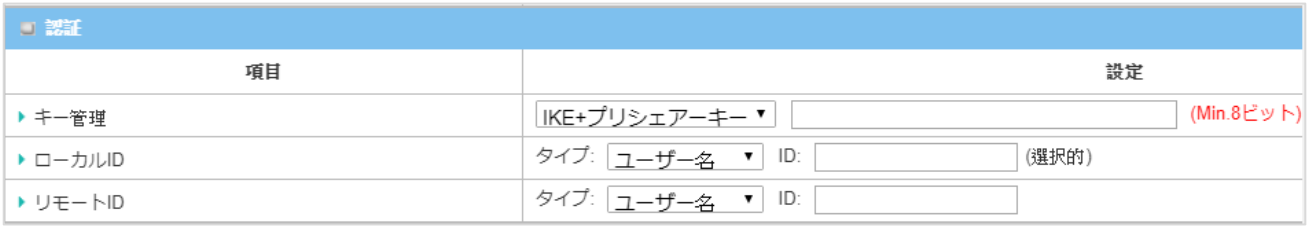


トンネル構成		
項目	**設定値**	**説明**
トンネル	デフォルトは、チェックなしです	有効ボックスにチェックを入れ、動的 IPSec VPN トンネルを有効します。
トンネル名	1. 入力必須	トンネル名を入力します。識別しやすい名称を入力しま

	2.4 文字列形式は、任意テキストです	す。 値の範囲： 1～19 文字
インターフェイス	1.入力必須 2.デフォルトは、「WAN-1」です	IPSec トンネルを確立する WAN インターフェイスを選択します。
トンネルシナリオ	1.入力必須 2.デフォルトは、「動的 VPN」です	IPSec トンネリングシナリオは、動的 VPN に固定されています。
カプセル化プロトコル	1.入力必須 2.デフォルトは、「ESP」です	この IPSec トンネルのドロップダウンボックスから、カプセル化プロトコルを選択します。利用可能なカプセル化は、「ESP」と「AH」です。
IKE バージョン	1.入力必須 2.デフォルトは、V1 です	の IPSec トンネルの IKE バージョンを指定します。v1 または v2 を選択します 注： トンネルシナリオの動的 VP が選択されている場合、または、カプセル化プロトコルの AH が選択されている場合、IKE バージョンは使用できません。



ローカルおよびリモート設定		
項目	設定値	説明
ローカルサブネット	入力必須	ローカルサブネット IP アドレスを指定します。
ローカルネットマスク	入力必須	ローカルサブネットマスクを指定します。



認証構成		
項目	設定値	説明
キー管理	1.入力必須 2.プリシェアーキー：8～32 文字	この IPSec トンネルのドロップダウンボックスから、キー管理を選択します。 IKE+プリシェアーキー（事前共有キー）：キー（8～32 文字）を設定する必要があります。

ローカル ID	任意の設定	認証するこの IPSec トンネルの「ローカル ID」を指定します。 ・ローカル ID の「ユーザー名」を選択し、ユーザー名を入力します。ユーザー名にはすべての数字を含めることはできますが、すべてを数字にすることはできません。 ・ローカル ID の「FQDN」を選択し、FQDN を入力します。 ・ローカル ID の「User@FQDN」を選択し、User@FQDN を入力します。 ・ローカル ID の「キーID」を選択し、キーID（英字または数字）を入力します。
リモート ID	任意の設定	認証するこの IPSec トンネルの Remote ID（リモート ID）を指定します。 ・リモート ID の User Name（ユーザー名）を選択し、ユーザー名を入力します。 ユーザー名にはすべての数字を含めることはできますが、すべてを数字にすることはできません。 ・リモート ID の「FQDN」を選択し、FQDN を入力します。 ・リモート ID の「User@FQDN」を選択し、User@FQDN を入力します す。 ・リモート ID の「キーID」を選択し、キーID（英字または数字）を入力します。 注：Tunnel Scenario（トンネルシナリオ）の Dynamic VPN（動的 VPN） オプションを選択すると、Remote ID（リモート ID）は、使用することができません。

残りの 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設定については、前のセクションで説明した IPSec トンネルの作成と同じです。関連する説明を参照してください。

5.1.2　OpenVPN　【未対応】

本製品ではサポートされていない機能です。

5.1.3　L2TP

L2TP（レイヤー2 トンネリングプロトコル）とは、仮想プライベートネットワーク（VPN）をサポートするためのトンネリングプロトコルで、ISP のサービスの一環として提供されることもあります。
これ自体には暗号化や機密保持機能はありません。トンネル内を通過する暗号化プロトコルによりプライバシーを実現しています。このゲートウェイは、同時に L2TP サーバーと L2TP クライアントの動作を行います。

L2TP サーバー：
クライアントが、L2TP トンネルを作成するには、静的 IP または FQDN が必要です。また、クライアントログイン認証用の「ユーザーアカウントリスト」（ユーザー名/パスワード）も保持します。 接続された各 L2TP クライアントに仮想 IP を割り当てるための

仮想 IP プールがあります。

L2TP Client（L2TP クライアント）：

これは、動的 IP を備えたリモートオフィス内のモバイルユーザーまたはゲートウェイです。

トンネルを設定するには、「ユーザー名」、「パスワード」、およびサーバーのグローバル IP を取得する必要があります。

さらに、メイン接続としての各トンネルの動作モード、別のトンネルのフェールオーバー、または、負荷バランストンネルを識別して全体の帯域幅を増やす必要があります。

パケットフローのために「リモートサブネット」を決定する必要があります。

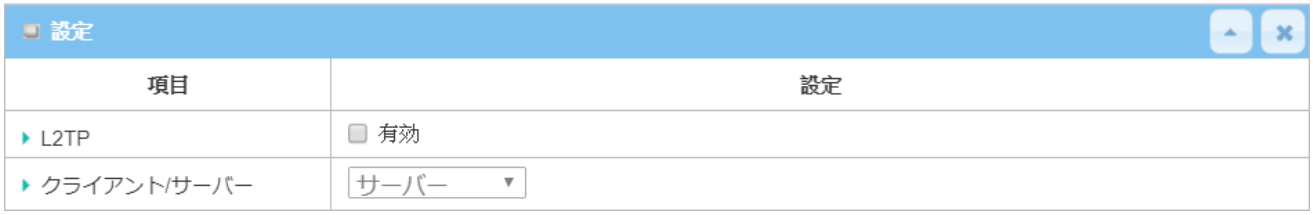
さらに、「リモートサブネット」パラメータで、L2TP トンネルを通過するトラフィックの種類を定義することもできます。

L2TP 設定

セキュリティ > [VPN] > [L2TP] タブに進みます。

L2TP 設定により、L2TP トンネルを作成および構成することができます。

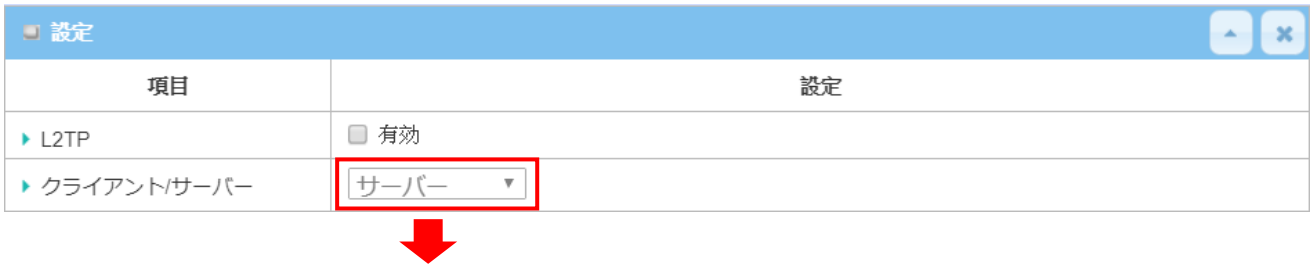
L2TP の有効



項目	設定値	説明
L2TP	デフォルトは、チェックありです	有効ボックスにチェックをすると、L2TP 機能を有効にします。
クライアント/サーバー	入力必須	L2TP の役割を指定します。 ゲートウェイが使用するサーバー、 またはクライアントの役割を選択します。
保存	該当なし	[保存]ボタンをクリックして、設定を保存します。

■ L2TP サーバーとして

「クライアント/サーバー」項目で、「サーバー」を選択すると、L2TP サーバー構成を表示します。



L2TPサーバー構成		
項目	設定値	説明
L2TP サーバー	デフォルトは、チェックありです	有効ボックスにチェックをすると、L2TP サーバーを有効にします。
インターフェイス	1. 入力必須 2. デフォルトは、「すべてのWAN-1」です	選択したインターフェイスをこの L2TP トンネルに使用するように定義します。
L2TP over IPSec	デフォルトは、チェックありです	有効ボックスをクリックすると、L2TP over IPSec が有効になり、プリシェアーキー（事前共有キー）（8～32 文字）を入力する必要があります。
サーバー仮想 IP	入力必須	L2TP サーバー仮想 IP を指定します。 この L2TP サーバーローカル仮想 IP として設定されます。
IP プール 開始アドレス	入力必須	仮想 IP プールの L2TP サーバー開始 IP を指定します。 L2TP クライアントに割り当てる開始 IP として設定されます。 値の範囲： 1～255
IP プール 終了アドレス	入力必須	仮想 IP プールの L2TP サーバー終了 IP を指定します。 L2TP クライアントに割り当てる終了 IP として設定されます。 値の範囲： 1～255
認証プロトコル	入力必須	L2TP クライアントを認証する L2TP サーバーに対して、単一、または複数の認証プロトコルを選択します。 利用可能な認証プロトコルは、PAP / CHAP / MS-CHAP / MS-CHAP v2 です。
MPPE 暗号化	入力必須	MPPE プロトコルをサポートするかどうかを指定します。 有効ボックスをクリックして、MPPE を有効にし、ドロップダウンボックスから、40 ビット/ 56 ビット/ 128 ビットを選択します。 注：MPPE 暗号化が有効になっている場合、認証プロトコル PAP/CHAP オプションは使用できません。
サービスポート	入力必須	L2TP サーバーが使用するサービスポートを指定します。 値の範囲： 1～65535

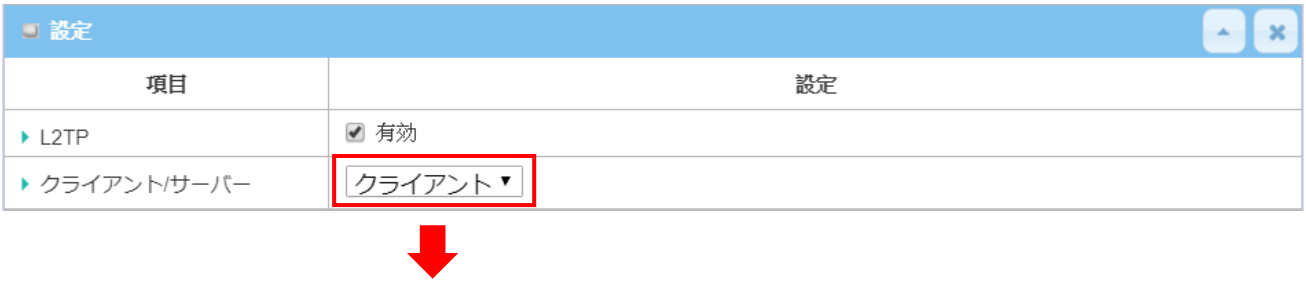
保存	該当なし	［保存］をクリックして、設定を保存します。
もとに戻す	該当なし	［元に戻す］をクリックして、設定をキャンセルします。

L2TPサーバーステータス		
項目	設定値	説明
L2TP サーバー ステータス	該当なし	接続されている L2TP クライアントのユーザー名、リモート IP、リモート仮想 IP、およびリモートコール ID が表示されます。 ［更新］ボタンをクリックして、L2TP クライアント情報を更新します。

ユーザーアカウントリスト		
項目	設定値	説明
ユーザー アカウントリスト	最大 10 の ユーザーアカウント	これは、L2TP 認証ユーザーアカウントエントリです。リモートクライアントのアカウントを作成および追加して、ゲートウェイデバイスへの L2TP VPN 接続を確立することができます。 ［追加］ボタンをクリックして、ユーザーアカウントを追加します。 ユーザー名とパスワードを入力します。次に、有効ボックスにチェックを入れて、ユーザーを有効します。 ［保存］ボタンをクリックして、新規ユーザーアカウントを保存します。 選択したユーザーアカウントは、［削除］ボタンをクリックすると完全に削除できます。 値の範囲： 1～32 文字

■ L2TP クライアントとして

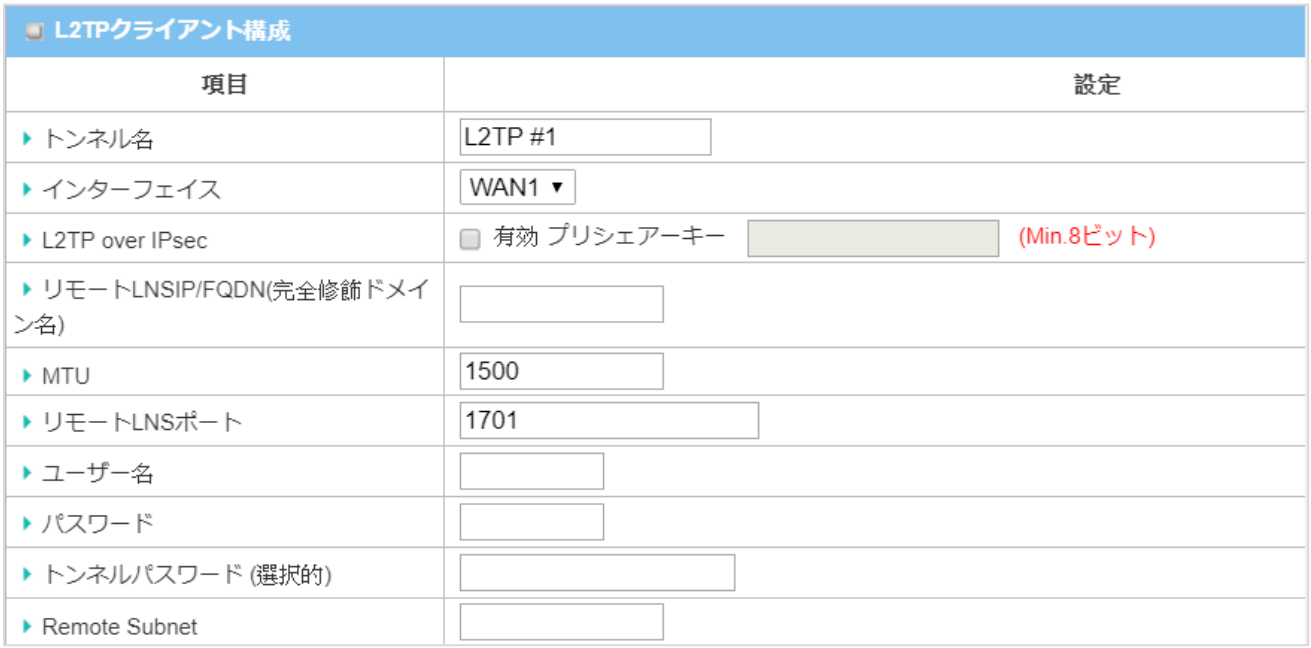
「クライアント/サーバー」項目で、「クライアント」を選択すると、一連の L2TP クライアント構成を表示します。

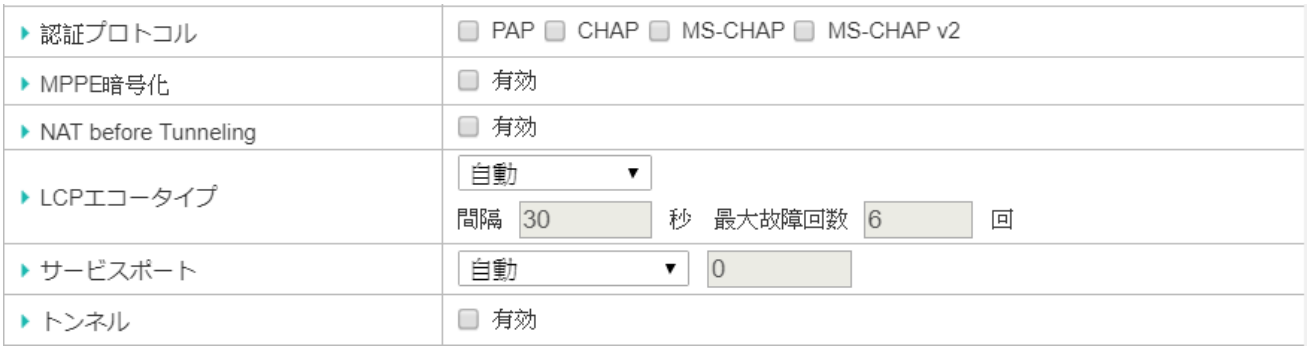


L2TPクライアント構成		
項目	設定値	説明
L2TP クライアント	デフォルトは、チェックなしです	有効ボックスにチェックを入れ、ゲートウェイの L2TP クライアントロールを有効にします。
保存	該当なし	［保存］をクリックして、設定を保存します。
もとに戻す	該当なし	［元に戻す］をクリックして、設定をキャンセルします。

L2TP クライアントの作成/編集

［追加/編集］ボタンが適用されると、一連の構成画面を表示します。





L2TPクライアント構成		
項目	設定値	説明
トンネル名	入力必須	トンネル名を入力します。識別しやすい名称を入力します。 値の範囲： 1～32 文字
インターフェイス	入力必須	選択したインターフェイスをこの L2TP トンネルに使用するように定義します。 （WAN-1 は、WAN-1 インターフェイスが有効な場合のみ利用可能です） 他の WAN インターフェイス（WAN-2 など）でも同様です。
L2TP over IPsec	デフォルトは、チェックありです	有効ボックスにチェックを入れ、L2TP over IPSec を有効し、さらに、プリシェアーキー（事前共有キー）（8～32 文字）を指定します。
リモート LNSIP/FQDN（完全修飾ドメイン名）	入力必須	L2TP サーバーのパブリック IP アドレス、または FQDN を入力します。
MTU	1. 入力必須 2. デフォルトは、「1500」です 3. 最大 1500	I2TP トラフィックの場合、項目は、自動的に TCP MSS を 3 方向ハンドシェイクで調整します。 これは、VPN 外部インターフェイスで有効になっている［MTU］オプションに関係なく発生します。 値の範囲：64～1500Bytes
リモート LNS ポート	1. 入力必須 2. デフォルトは、「1701」です	この L2TP トンネルのリモート LNS ポートを入力します。 値の範囲： 1～65535
ユーザー名	入力必須	L2TP サーバーに接続するときに認証される、この L2TP トンネルのユーザー名を入力します。 値の範囲： 0～32 文字
パスワード	入力必須	L2TP サーバーに接続するときに認証される、この L2TP トンネルのパスワードを入力します。
トンネルパスワード（選択的）	デフォルトは、チェックありです	この L2TP トンネルが認証するためのトンネリングパスワードを入力します。
リモートサブネット	入力必須	この L2TP トンネルが L2TP サーバーに到達するためのゲートウェイを指定します。 リモートサブネットを選択すると、リモートサブネットというもう 1 つの設定を指定する必要があります。これは、

		L2TP VPN サーバーのイントラネット用です。したがって、PPTP クライアントピアでは、宛先が専用サブネット内にあるパケットは、PPTP VPN トンネル経由で転送されます。 その他は、L2TP クライアントピアのセキュリティゲートウェイの現在のルーティングポリシーに基づいて転送されます。 リモートサブネットフォーマットは、IP アドレス/ネットマスク（例：10.0.0.2/24）でなければなりません。
認証プロトコル	入力必須	この L2TP トンネルの認証プロトコルを指定することができます。 PAP / CHAP / MS-CHAP / MS-CHAP v2 をクリックします -> プロトコルは、どのボックスをクリックするかを有効にします。
MPPE 暗号化	デフォルトは、チェックありです	L2TP サーバーが、MPPE プロトコルをサポートするかどうかを指定します。 有効ボックスをクリックして、MPPE を有効します。 注：MPPE 暗号化が有効になっている場合、「認証プロトコル」項目の PAP/CHAP オプションは使用できません。
LCP エコータイプ	デフォルトは、「自動」です	この L2TP トンネルの LCP エコータイプを指定します。 これは、「自動」、「ユーザー定義」、「無効」から指定します。 ・**自動**：システムが、間隔および 最大故障回数を設定します。 ・**ユーザー定義**：間隔、および最大故障回数を入力します。間隔のデフォルト値は 30 秒で、最大故障回数は 6 回です。 ・**無効**：LCP エコーを無効化します。 値の範囲：間隔時間は、1～99999、故障回数は、1～999です
サービスポート	入力必須	この L2TP トンネルが使用するサービスポートを指定します。 「自動」、「1701（Cisco の場合）」、「ユーザー定義」から指定します。 ・**自動**： システムがサービスポートを決定します。 ・**1701（Cisco の場合）**：システムは、CISCO L2TP Server に接続するためにポート 1701 を使用します。 ・**ユーザー定義**：サービスポートを入力します。 デフォルト値は 0 です。 値の範囲： 0～65535
トンネル	デフォルトは、チェックありです	有効ボックスにチェックを入れて、この L2TP トンネルを有効にします。
保存	該当なし	［保存］をクリックして、設定を保存します。
もとに戻す	該当なし	［元に戻す］をクリックして、設定をキャンセルします。
前へ	該当なし	［前へ］をクリックして、前ページに戻ります。

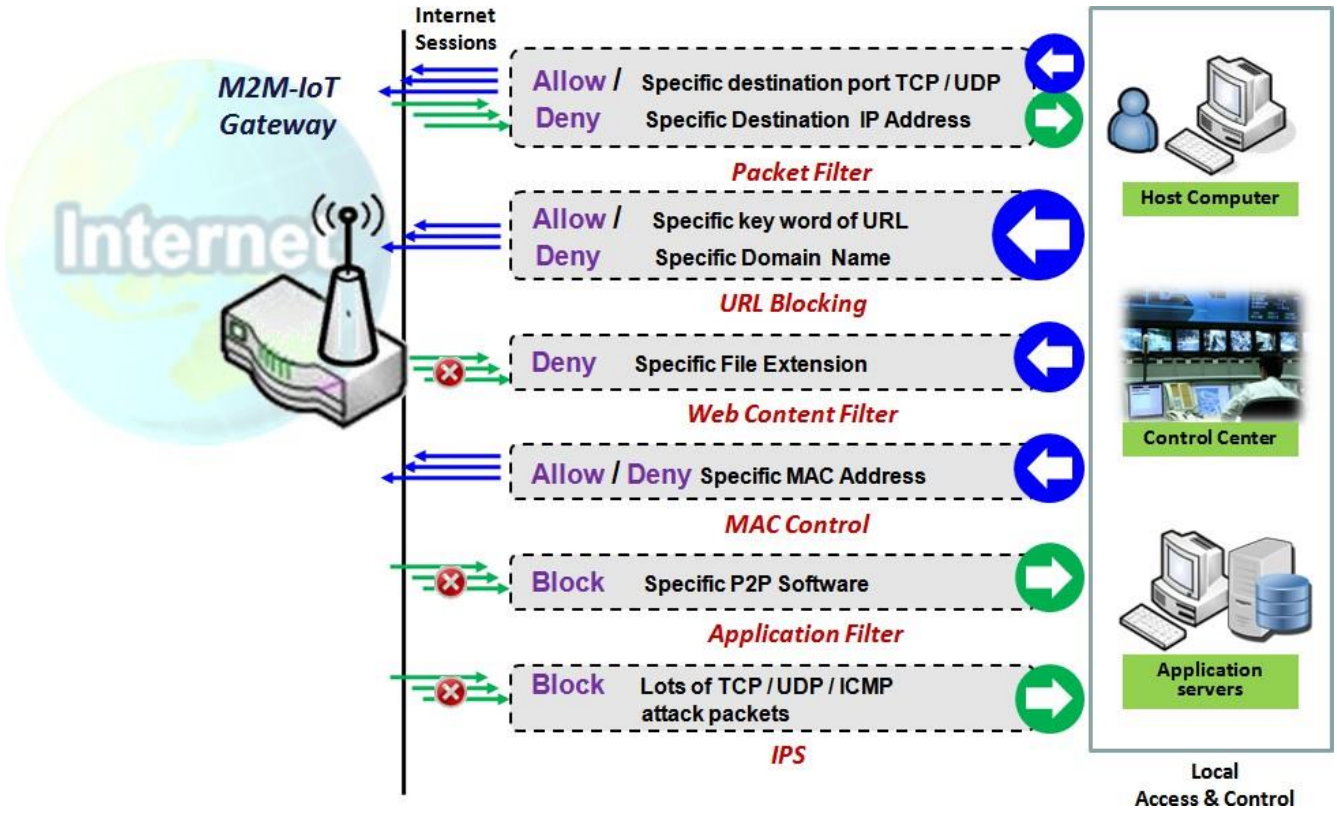
5.1.4　PPTP　【未対応】

本製品ではサポートされていない機能です。

5.1.5　GRE　【未対応】

本製品ではサポートされていない機能です。

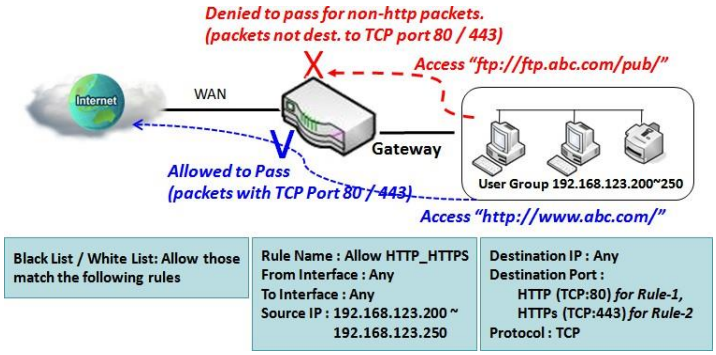
5-2. ファイアウォール



5.2.1　パケットフィルター

「パケットフィルター」機能を使用すると、受信パケットと送信パケットのいくつかのフィルタリングルールを定義することができます。したがって、ゲートウェイは、通過を許可するパケットと拒否するパケットを制御することができます。パケットフィルタルールでは、パケットがゲートウェイに入り、出るインターフェイス、送信元と宛先のIPアドレス、および宛先サービスのポートタイプとポート番号を示す必要があります。さらに、ルールが有効される予定を示す必要があります。

ホワイトリストシナリオによるパケットフィルタ



図に示すように、「パケットフィルタルールリスト」をホワイトリスト（以下のルールと一致するようにする）として指定し、ルールを定義します。ルール 1 は HTTP パケットの通過を許可し、ルール 2 は HTTPS パケットの通過を許可します。
このような構成では、ゲートウェイは、WAN ポートを通過する TCP ポート 80 または 443 を対象とする IP 範囲 192.168.123.200 から 250 までの HTTP および HTTPS パケットのみを許可します。

パケットフィルタ設定

セキュリティ > ［ファイヤーウォール］ > ［パケットフィルター］タブに進みます。

パケットフィルタ設定では、パケットフィルタポリシーを作成およびカスタマイズして、オフィス設定に基づいて、特定の受信/送信パケットをルーター経由で許可または拒否することができます。

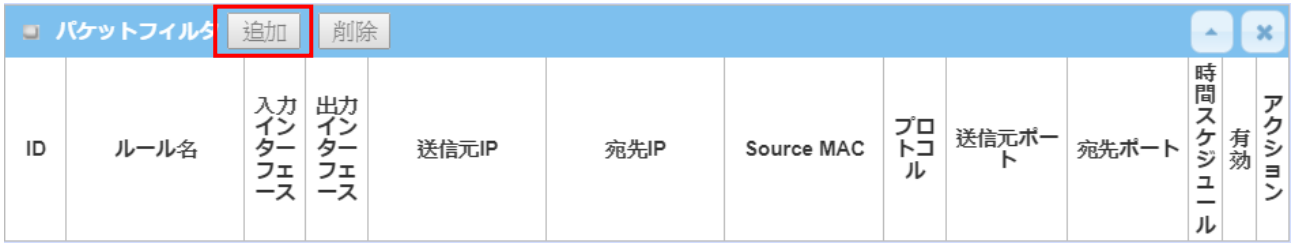
パケットフィルターの有効

項目	設定値	説明
パケットフィルター	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、パケットフィルタ機能を有効にします。
ブラックリスト/ホワイトリスト	次の設定ルールに相応しい時にアクセスを拒否します	「規則に一致するものを拒否する」を選択すると、名前に示されているように、ルールで指定されたパケットはブラックリストに表示されます。 対照的に、「規則に一致するものを許可する」を選択してホワイトリストを指定し、このパケットを通過させ、残りをブロックします。
ログアラート	デフォルトは、チェックなしです	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	該当なし	［保存］ボタンをクリックして、構成を保存します。
元に戻す	該当なし	［元に戻す］ボタンをクリックして、設定をキャンセルします。

パケットフィルタルールの作成/編集

ゲートウェイにより、パケットフィルタリングルールをカスタマイズすることができます。これは、最大 20 のフィルタルールセットをサポートします。

［追加］ボタンが適用されると、「パケットフィルタ規則」画面を表示します。



項目	設定値	説明
ルール名	1. 文字列形式は任意のテキストです 2. 入力必須	パケットフィルタルール名を入力します。覚えやすい名称を入力します。 値の範囲：1～30 文字
入力 インターフェース	1. 入力必須 2. デフォルトは、「任意」です	選択したインターフェイスが、ルーターのパケット入力インターフェイスになるように定義します。フィルタリングするパケットが、LAN to WAN（LAN から WAN）から来ている場合は、このフィールドで「LAN」を選択します。 または、VLAN-1 to WAN（VLAN-1 から WAN）を選択し、このフィールドで 「VLAN-1」を選択します。 その他の例として、VLAN-1 to VLAN-2（VLAN-1 から VLAN-2）があります。VLAN-1 to WAN（VLAN-1 から WAN） 任意のインターフェイスからルーターに入ってくるパケットに対して、「任意」を選択します。 2 つの同一のインターフェイス（すなわち、VLAN-1 to VLAN-1（VLAN-1 から VLAN-1）は、ルーターにより受け入れられないことに注意してください。
出力 インターフェース	1. 入力必須 2. デフォルトは、「任意」です	選択したインターフェイスが、ルーターのパケット出力インターフェイスになるように定義します。フィルタリングするパケットが、LAN to WAN（LAN から WAN）から入る場合は、このフィールドで「WAN」を選択します。 または、VLAN-1 to WAN（VLAN-1 から WAN）を選択し、このフィールドで 「WAN」を選択します。 その他の例として、VLAN-1 to VLAN-2（VLAN-1 から VLAN-2）があります。VLAN-1 to WAN（VLAN-1 から WAN） 任意のインターフェイスからルーターから出ていくパケットに対して、「任意」を選択します。 2 つの同一のインターフェイス（すなわち、VLAN-1 to VLAN-1（VLAN-1 から VLAN-1）は、ルーターにより受け入れられないことに注意してください。
送信元 IP	1. 入力必須 2. デフォルトは、「任意」です	このフィールドは、送信元 IP アドレスを指定するためのフィールドです。 任意の IP アドレスからのパケットをフィルタするには、「任意」を選択します。IP アドレスからのパケットをフィルタリングするには、「特定の IP アドレス」を選択します。 特定の範囲の IP アドレスからのパケットをフィルタリングするには、「IP 範囲」を選択します。事前定義されたグループからのパケットをフィルタリングするには、「IP アドレスベースグループ」を選択します。 注：利用可能にするには、グループをあらかじめ定義しておく必要があります。 オブジェクト定義 > グルーピング >「ホストグループ」を参照してください。 [追加ルール]ボタンをクリックしてグループを作成することもできます。 ※「グルーピング」は、本製品では対応しておりません。

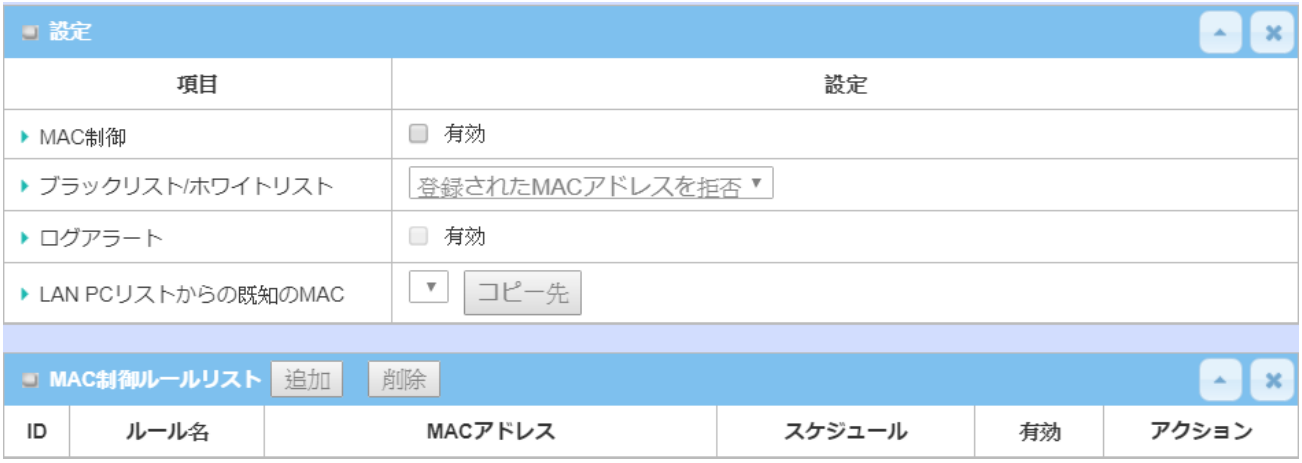
宛先 IP	1. 入力必須 2. デフォルトは、「任意」です	このフィールドは、宛先 IP アドレスを指定するためのフィールドです。 任意の IP アドレスに入るパケットをフィルタするには、「任意」を選択します。 このフィールドに入力した IP アドレスに入るパケットをフィルタリング するには、「特定の IP アドレス」を選択します。 このフィールドに入力した IP アドレスの範囲に入るパケットをフィルタリングするには、「IP 範囲」を選択します。 事前定義されたグループに入るパケットをフィルタリングするには、「IP アドレスベースグループ」を選択します。 注：利用可能にするには、グループをあらかじめ定義しておく必要があります。 オブジェクト定義 > グルーピング > 「ホストグループ化」を参照してください。 [追加ルール]ボタンをクリックしてグループを作成することもできます。[追加ルール]ボタンで設定した内容は「ホストグループ化」設定画面にも表示されます。 ※「グルーピング」は、本製品では対応しておりません。
Source MAC	1. 入力必須 2. デフォルトは、「任意」です	このフィールドは、Source MAC address（ソース MAC アドレス）を指定するためのフィールドです。 任意の MAC アドレスからのパケットをフィルタするには、「任意」を選択します。 MAC アドレスからのパケットをフィルタリングするには、「特定の MAC アドレス」を選択します。 事前定義されたグループからのパケットをフィルタリングするには、「MAC アドレスベースグループ」を選択します。 注：このオプションを利用可能にするには、グループをあらかじめ定義 しておく必要があります。 オブジェクト定義 > グルーピング >「ホストグループ化」を参照してください。 [追加ルール]ボタンをクリックしてグループを作成することもできます。 ※「グルーピング」は、本製品では対応しておりません。
プロトコル	1. 入力必須 2. デフォルトは、「任意（0）」です	■「任意」を選択すると、プロトコルパケットがすべてフィルタされます。 次に、「送信元ポート」で、「既知のサービス」が選択されている場合は、事前定義済ポートのドロップダウンボックスで選択し、そうでない場合は、「ユーザー定義サービス」を選択して、ポート範囲を指定します。 次に、「宛先ポート」で、「既知のサービス」が選択されている場合は、事前定義済ポートのドロップダウンボックスで選択し、そうでない場合は、「ユーザー定義サービス」を選択して、ポート範囲を指定します。 値の範囲：「送信元ポート」、「宛先ポート」の場合、1～65535 です。
		■「ICMPv4」を選択すると、ICMPv4 パケットをフィルタリングします。

		■「TCP」を選択すると、TCP パケットをフィルタリングします。 次に、「送信元ポート」で、「既知のサービス」が選択されている場合は、事前定義済ポートのドロップダウンボックスで選択し、そうでない場合は、「ユーザー定義サービス」を選択して、ポート範囲を指定します。 次に、「宛先ポート」で、「既知のサービス」が選択されている場合は、事前定義済ポートのドロップダウンボックスで選択し、そうでない場合は、「ユーザー定義サービス」を選択して、ポート範囲を指定します。 値の範囲：「送信元ポート」、「宛先ポート」の場合、1～65535 です。
		■「UDP」を選択すると、UDP パケットをフィルタリングします。 次に、Source Port（送信元ポート）で、Well-known Service（よく知ら れているサービス）が選択されている場合は、事前定義済ポートドロップダウンボックスを選択し、そうでない場合は、User-defined Service（ユーザー定義サービス）を選択して、ポート範囲を指定します。 次に、Destination Port（宛先ポート）で、Well-known Service（よく 知られているサービス）が選択されている場合は、事前定義済ポートドロップダウンボックスを選択し、そうでない場合は、User-defined Service（ユーザー定義サービス）を選択して、ポート範囲を指定します。 値の範囲：Source Port（ソースポート）、Destination Port（宛先ポート）の場合、1～65535 です。
		■「GRE」を選択すると、GRE パケットをフィルタリングします。
		■「SCTP」を選択すると、SCTP パケットをフィルタリングします。
		■「ユーザー定義」を選択すると、指定したポート番号のパケットをフィルタリングします。 次に、「Protocol Number」（プロトコル番号）にポート番号を入力します。
時間スケジュール	入力必須	時間スケジュールをこのルールに適用し、それ以外の場合は、「(0) 常時」にします。 ドロップダウンリストが空の場合、「時間スケジュール」が事前設定されていることを確認します。 オブジェクト定義 >スケジュール設定 >「設定」タブを参照します。
ルール	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、本ルールを有効にし、設定を保存します。
保存	該当なし	[保存]をクリックして、設定を保存します。
キャンセル	該当なし	[キャンセル]をクリックして、設定をキャンセルします。

5.2.2　URL ブロッキング【未対応】

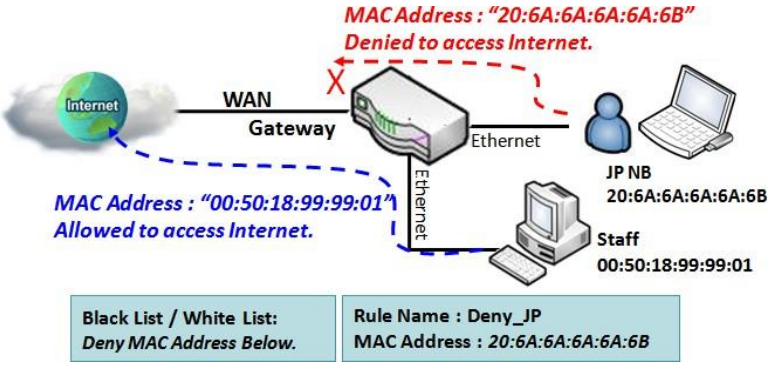
本製品ではサポートされていない機能です。

5.2.3　MAC 制御



「MAC制御」を使用すると、デバイスの MACアドレスに基づいて、ユーザーごとに異なるゲートウェイにアクセス権を割り当てることができます。管理者が特定のMACアドレスを持つクライアントホストからのトラフィック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に基づき拒否することができます。

ブラックリストシナリオによる MAC 制御



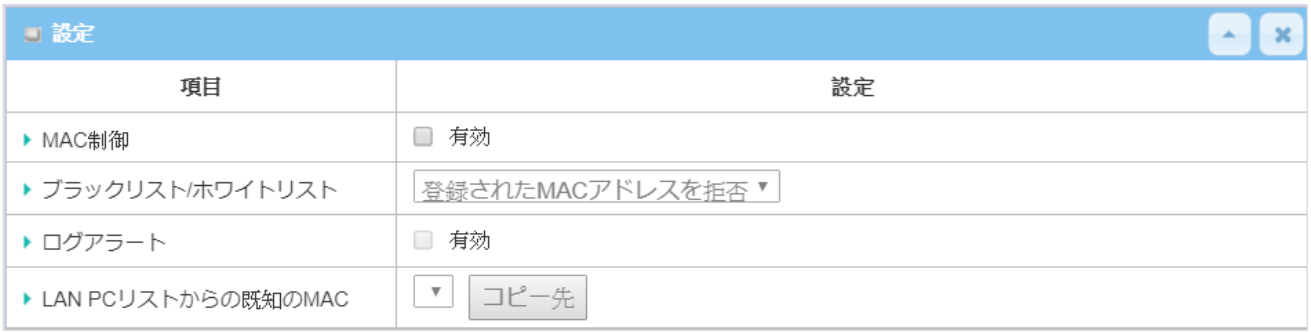
図に示すように、MAC制御機能を有効にし、「MAC制御ルールリスト」をブラックリストとし、「JP NB」からの接続要求を自身のMACアドレス（20:6A:6A:6A:6A:6B）で拒否するゲートウェイのMAC制御ルールを1つ設定します。
システムは、「JP NB」からゲートウェイへの接続をブロックしますが、他の接続は許可します。

MAC 制御設定

セキュリティ ＞ ［ファイヤーウォール］ ＞ ［MAC 制御］タブに進みます。

MAC 制御設定により、MAC アドレスポリシーを作成およびカスタマイズして、
特定の送信元 MAC アドレスを持つパケットを許可、または拒否することができます。

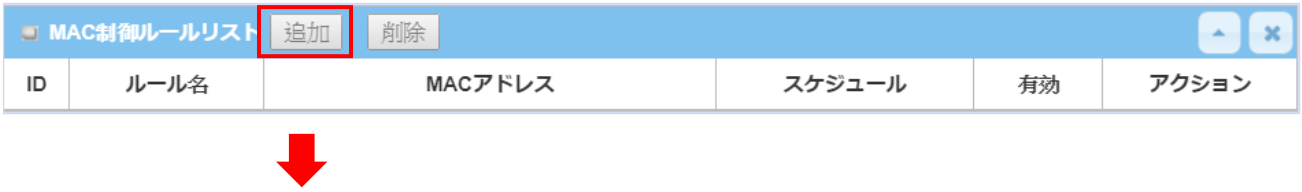
MAC 制御の有効



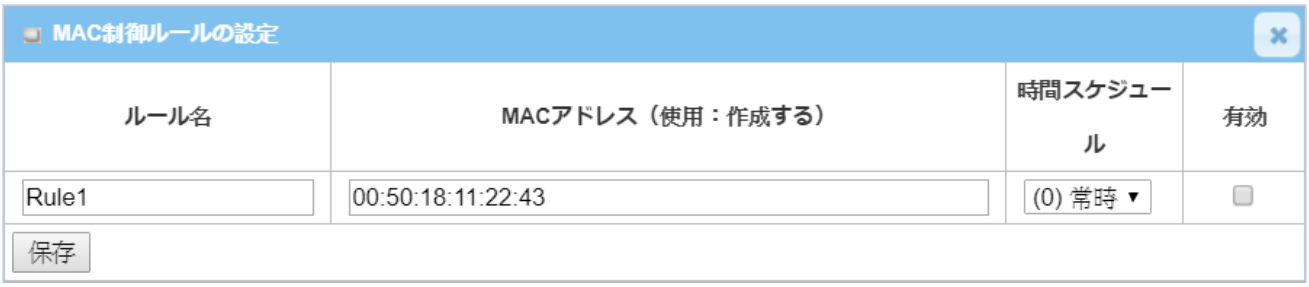
項目	設定値	説明
MAC 制御	デフォルトは、チェックなしです	有効ボックスにチェックを入れ、MAC フィルタ機能を有効にします。
ブラックリスト/ホワイトリスト	デフォルトは、「登録された MAC アドレスを拒否」です	「登録された MAC アドレスを拒否」を選択すると、名前に示されているように、ルールで指定されたパケットはブロックされます（ブラックリストに表示されます）。 対照的に、「登録された MAC アドレスを許可」を使用して、ホワイトリストを指定し、このパケットを通過させ、残りをブロックします。
ログアラート	デフォルトは、チェックなしです	有効ボックスにチェックを入れると、Event Log（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	該当なし	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」をフィルタルールにコピーします。
保存	該当なし	[保存]ボタンをクリックし、設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックし、設定をキャンセルします。

MAC制御ルールの作成/編集

ゲートウェイは、最大 20 のフィルタルールセットをサポートします。
制御ルールを作成する前に、「MAC制御」が有効になっていることを確認してください。
[追加]ボタンが適用されると、「MAC制御ルールの設定」画面が表示されます。



MAC制御ルールの設定



項目	設定値	説明
ルール名	1. 文字列形式は任意のテキストです 2. 入力必須	MAC 制御ルール名を入力します。 覚えやすい名称を入力します。
MAC アドレス	1. MAC アドレスの文字列形式です 2. 入力必須	ルールをフィルタリングするソース MAC アドレスを指定します。
時間スケジュール	入力必須	時間スケジュールをこのルールに適用し、それ以外の場合は「(0) 常時」にします。 ドロップダウンリストが空の場合、時間スケジュールが事前設定されていることを確認します。 オブジェクト定義 >スケジュール設定> 「設定」タブを参照します。
有効	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、本ルールを有効にし、設定を保存します。
保存	該当なし	[保存]ボタンをクリックし、設定を保存します。

5.2.4　コンテントフィルター【未対応】

本製品ではサポートされていない機能です。

5-2-5. アプリケーションフィルター　【未対応】

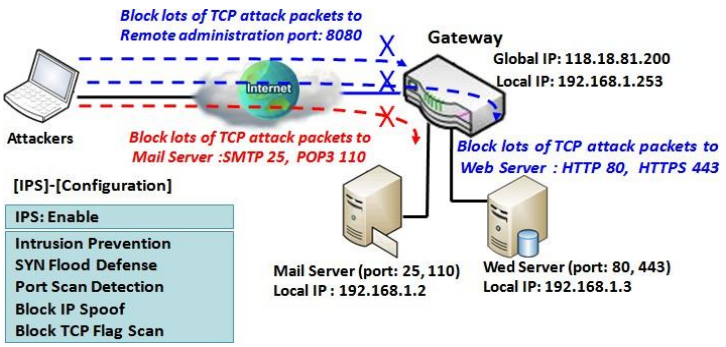
本製品ではサポートされていない機能です。

5.2.6　IPS

インターネットにアプリケーションサーバーを提供するには、管理者は、サービスの特定のポートを開く必要があります。しかし、インターネット上のサービスポートを開くことには、常に、いくつかのリスクがあります。このような攻撃のリスクを回避するには、IPS 機能を有効することが重要です。

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ティビティ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装置です。IPS の主な機能は、悪意のあるアクティビティを特定すること、そのアクティビティに関する情報を記録すること、およびそのアクティビティをブロック/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、リストの侵入アクティビティ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システムにより記録されます。

IPS のシナリオ



図に示すように、ゲートウェイは、電子メールサーバー、Webサーバーとして機能し、リモート管理用の TCPポート 8080を提供します。
したがって、リモートユーザー、または未知のユーザーは、インターネットからこれらのサービスを要求することができます。
IPS を有効にすると、ゲートウェイはサービスを含むTCP ポート（25、80、110、443、および、8080）を含む着信攻撃パケットを検出することができます。これは、攻撃パケットをブロックし、通常アクセスがゲートウェイを通過できるようにします。

IPS設定

セキュリティ > ［ファイヤーウォール］ > ［IPS］ タブに進みます。

Intrusion Prevention System（IPS：侵入防御システム）設定では、侵入防止ルールをカスタマイズし、悪意のあるパケットを防ぐことができます。

IPS ファイヤーウォールの有効

項目	設定値	説明
IPS	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、IPS 機能を有効にします。
ログアラート	デフォルトは、 チェックなしです	有効ボックスにチェックを入れると、Event Log（イベントログ）が有効になります。
保存	該当なし	[保存]ボタンをクリックし、設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックし、設定をキャンセルします。

侵入防止ルールの設定

ルーターにより、有効する侵入防止ルールを選択することができます。
防御機能を有効にするには、IPS が有効になっていることを確認してください。

項目	設定値	説明
SYN フラッド防御 UDP フラッド防御 ICMP フラッド防御	1. 入力必須 2. デフォルトは、チェックなしです 3. トラフィックしきい値はデフォルトで「300」に設定されています 4. 値の範囲は 10～10000 です	有効ボックスにチェックを入れてこの侵入防止ルールを有効にし、このフィールドにトラフィックしきい値を入力します。 値の範囲：10～10000
ポートスキャン防御	1. 入力必須 2. デフォルトは、チェックなしです 3. トラフィックしきい値は、デフォルトで「200」に設定されています 4. 値の範囲は 10～10000 です	有効ボックスにチェックを入れてこの侵入防止ルールを有効にし、このフィールドにトラフィックしきい値を入力します。 値の範囲：10～10000
LandAttack のブロック 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	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、この侵入防止ルールを有効にします。

ARP スプーフィング防御	1. 入力必須 2. デフォルトは、チェックなしです 3. トラフィックしきい値は、デフォルトで「300」に設定されています 4. 値の範囲は 10～10000 です	有効ボックスにチェックを入れてこの侵入防止ルールを有効にし、このフィールドにトラフィックしきい値を入力します。 値の範囲：10～10000
保存	該当なし	[保存]ボタンをクリックし、設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックし、設定をキャンセルします。

5.2.7　オプション

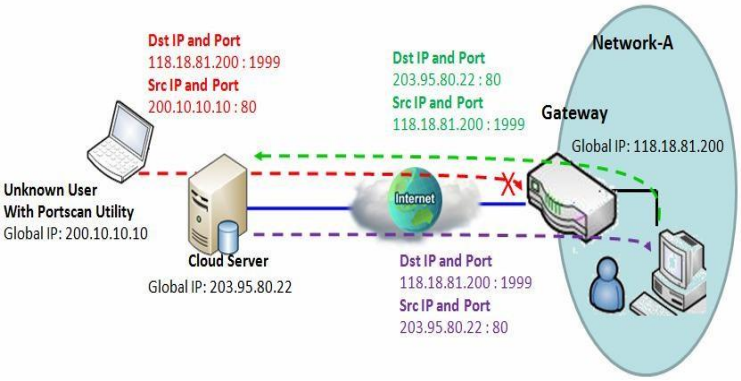
このページには、さらに便利なファイアウォールオプションがいくつかあります。

「ステルスモード」は、ゲートウェイが WAN からのポートスキャンに応答しないようにするため、インターネット上での検出や攻撃の影響を受けにくくなります。

「SPI」は、ゲートウェイがゲートウェイを通過する間に、ゲートウェイが 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を記録することを可能にし、ゲートウェイはすべての着信パケットをチェックしてこのパケットが有効かどうかを検出します。

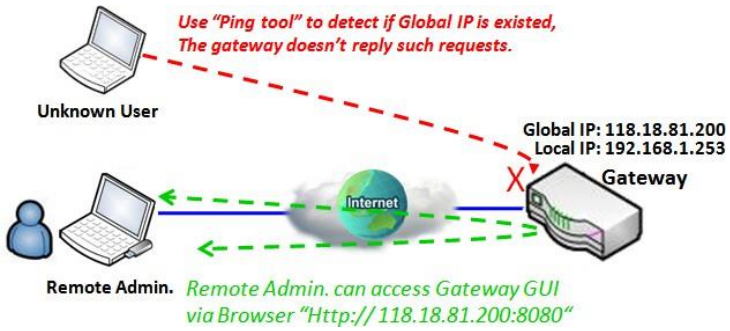
「WAN からの Ping パケットを破棄する」により、WAN 側のホストが、このゲートウェイにpingを実行できなくなります。最後に、「リモート管理者ホスト」を使用すると、リモートホストから管理タスクを実行することができます。この機能を有効にすると、指定した IP アドレスでのみリモート管理を実行できるようになります。

SPI シナリオの有効



図に示すように、ゲートウェイのIPアドレスは、WANインターフェイスについては、118.18.81.200、LAN インターフェイスについては、192.168.1.253 です。これは、NATゲートウェイとして機能します。ネットワーク-A のユーザーは、ゲートウェイ経由でクラウドサーバーにアクセスします。
時々、未知のユーザーが、パケットをシミュレートしますが、異なるソースIPを使用してマスカレードします。SPI機能をゲートウェイで有効すると、未知のユーザーからのそのようなパケットがブロックされます。

WAN およびリモート管理者ホストの Ping を破棄するシナリオ



「WANからのPingの破棄」により、WAN側のすべてのホストは、このゲートウェイが ICMPパケットに応答する pingを実行できなくなります。ローカルユーザがインターネットをサーフィンしているときにセキュリティリークを防ぐために、「WANからのPingの破棄」機能を有効します。

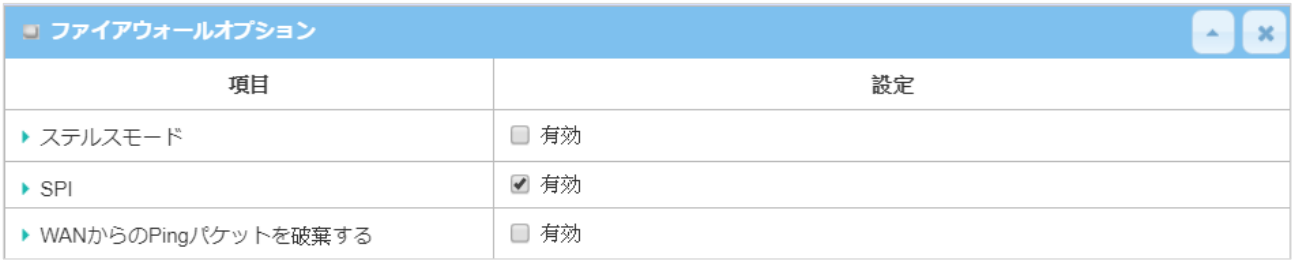
リモート管理者は、ゲートウェイのグローバルIPを知っており、TCP 8080 ポート経由でゲートウェイ GUIにアクセスすることができます。

ファイアウォールオプション設定

セキュリティ ＞ ［ファイヤーウォール］ ＞ ［オプション］タブに進みます。

ファイヤーウォールオプションの設定により、ネットワーク管理者はファイヤーウォールの動作を変更し、リモートルータのアクセス制御を有効することができます。

ファイアウォールオプションの有効



項目	設定値	説明
ステルスモード	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、ステルスモード機能を有効にします。
SPI	デフォルトは、 チェックありです	有効ボックスにチェックを入れ、SPI 機能を有効にします。
WAN からの Ping パケットを破棄する	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、WAN からの Ping の破棄機能を有効にします。

リモート管理者ホストの定義

ルーターにより、ネットワーク管理者は、ルーターをリモート管理することができます。

ネットワーク管理者は、特定のIPアドレスとサービスポートを割り当てて、ルーターにアクセスすることができます。

各IDの[編集]ボタンをクリックすると、編集可能になります。

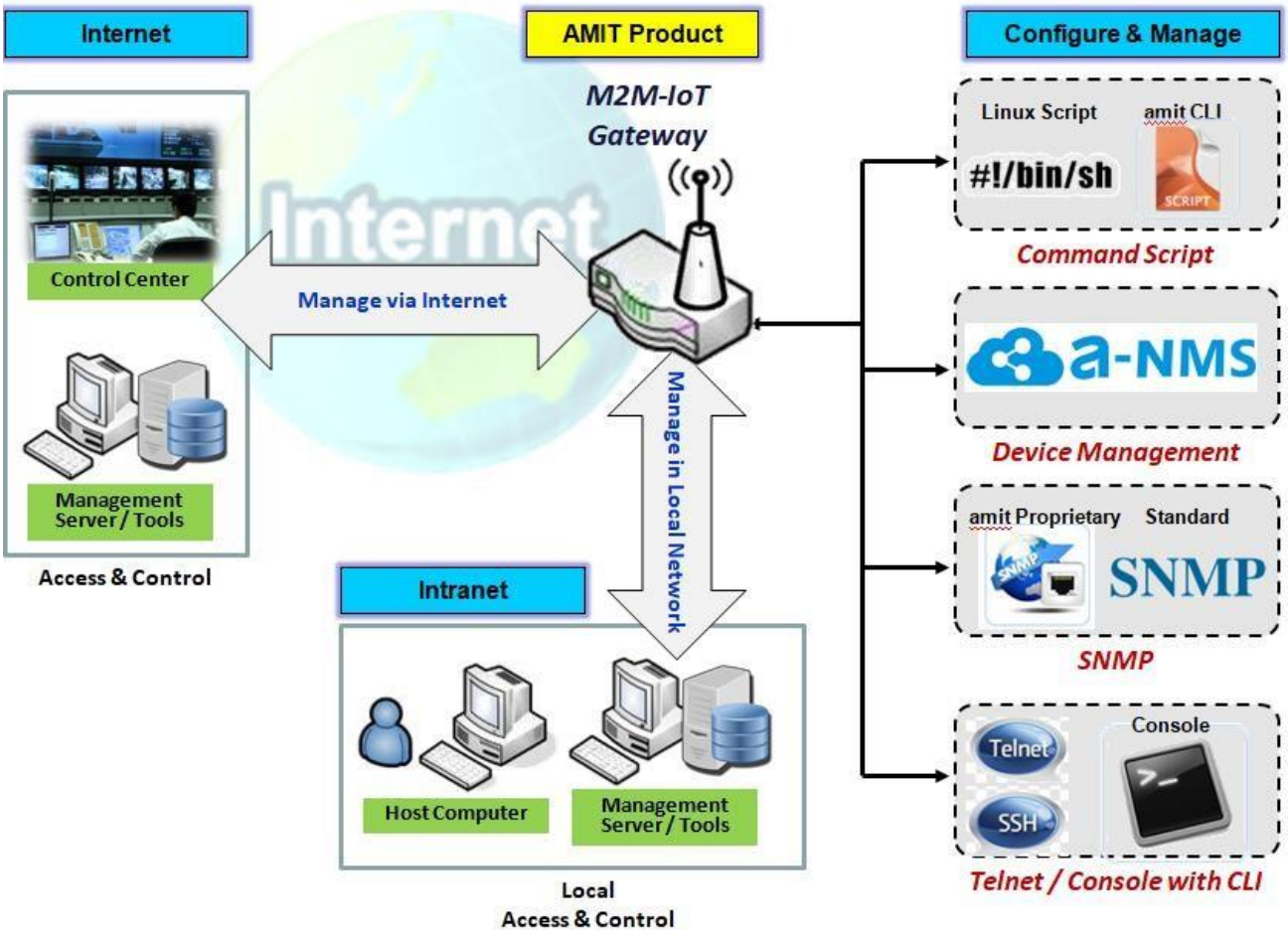
リモート管理者ホスト定義

ID	インターフェイス	プロトコル	IP	サブネットマスク	サービスポート	有効	アクション
1	All WAN	HTTP	任意のIPアドレス	N/A	80	☐	編集
2	All WAN	HTTP	任意のIPアドレス	N/A	80	☐	編集
3	All WAN	HTTP	任意のIPアドレス	N/A	80	☐	編集
4	All WAN	HTTP	任意のIPアドレス	N/A	80	☐	編集
5	All WAN	HTTP	任意のIPアドレス	N/A	80	☐	編集

項目	設定値	説明
プロトコル	デフォルトは、「HTTP」です	ルーターアクセスの場合、HTTP または HTTPS 方式を選択します。
IP	入力必須	このフィールドは、リモートアクセスのアクセス権を割り当てるためのリモートホストを指定するためのフィールドです。 「任意 IP」を選択して、すべてのリモートホストを許可します。 「特定 IP」を選択して、特定のサブネットからのリモートホストを許可します。 このフィールドに入力された IP アドレスと、サブネットを構成するために選択されたサブネットマスクです。
サービスポート	1. HTTP のデフォルトは、「80」です 2. HTTPS のデフォルトは、「443」です	このフィールドは、サービスポートを HTTP または HTTPS 接続に指定するためのフィールドです。 値の範囲： 1～65535
有効	デフォルトは、チェックなしです	有効ボックスにチェックをして、本ルールを有効にします。
保存	該当なし	[保存]ボタンをクリックして本ルールを有効にし、設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックし、設定をキャンセルします。

第6章. 管理（Administration）

6-1. 設定と管理



構成と管理は、コンピュータシステムを含む分散システムの企業全体の管理を指します。集中管理には、会社の規模、ITスタッフの専門知識、使用される技術の量に関連する時間と労力のトレードオフがあります。
本デバイスは、コマンドスクリプト、デバイス管理、SNMP、Telnet with CLIなど、多くのシステム管理プロトコルをサポートしています。
これらの構成は、「設定および管理」セクションで行うことができます。

6-1-1. コマンドスクリプト

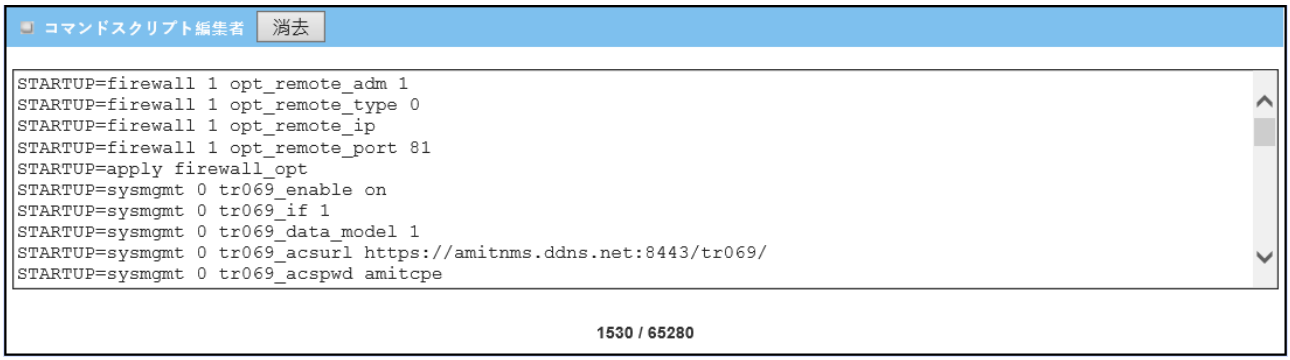
※コマンドスクリプトはサポートされていない機能です。
コマンドスクリプト構成とは、管理者が事前定義された構成をプレーンテキスト形式で設定し、起動時に構成を適用できるようにするアプリケーションです。

管理（Administration）> 設定と管理 > 「コマンドスクリプト」タブに進みます。

コマンドスクリプト構成の有効

項目	設定値	説明
コマンドスクリプト	デフォルトは、チェックなしです	［有効］ボックスにチェックを入れ、コマンドスクリプト機能を有効します。
スクリプトのバックアップ	該当なし	［Web UI 経由］ボタンをクリックして、既存のコマンドスクリプトを.txt ファイルにバックアップします。 以下の「スクリプト名」項目で、スクリプトファイル名を指定することができます。
スクリプトのアップロード	該当なし	［Web UI 経由］ボタンをクリックして、既存のコマンドスクリプトを指定した.txt ファイルからアップロードします。
スクリプト名	1. 任意の設定 2. 任意の有効なファイル名	スクリプトバックアップのスクリプトファイル名を指定するか、選択したアップロードスクリプトファイル名を表示します。 値の範囲： 0～32 文字
バージョン	1. 任意の設定 2. 任意の設定	適用されたコマンドスクリプトのバージョン番号を指定します。 値の範囲： 0～32 文字
説明	1. 任意の設定 2. 任意の設定	適用されるコマンドスクリプトの簡単な説明を入力します。
更新時刻	該当なし	最後のコマンドスクリプトアップロードのアップロード時刻を記録します。

プレーンテキストコマンドスクリプトの編集/バックアップ



上記のように、構成画面でプレーンテキスト構成設定を編集することができます。

プレーンテキスト構成		
項目	設定値	説明
クリーン	該当なし	テキストエリアをクリーンします。 （すでに保存されている設定をさらにクリーンにするには、[保存]ボタンをクリックしてください）。
バックアップ	該当なし	構成をバックアップ・ダウンロードします。
保存	該当なし	構成を保存します。

サポートされているプレーンテキスト構成の項目を次のリストに示します。
標準のLinuxコマンドで実行できる設定については、それらをスクリプトファイルに入れて、STARTUPコマンドでsystem configureに適用することができます。
対応するLinuxコマンドが構成されていない構成については、独自のコマンドセットで構成することができます。

Telnetによるプレーンテキストシステム構成

前述のWebスタイルのプレーンテキスト設定に加えて、ゲートウェイシステムでは、Telnet CLIを使用した構成を行うことができます。
管理者は、独自のtelnetコマンド「txtConfig」と関連するアクション項目を使用して、単純なシステム構成を実行することができます。

コマンド形式は次のとおりです：txtConfig (action) [option]

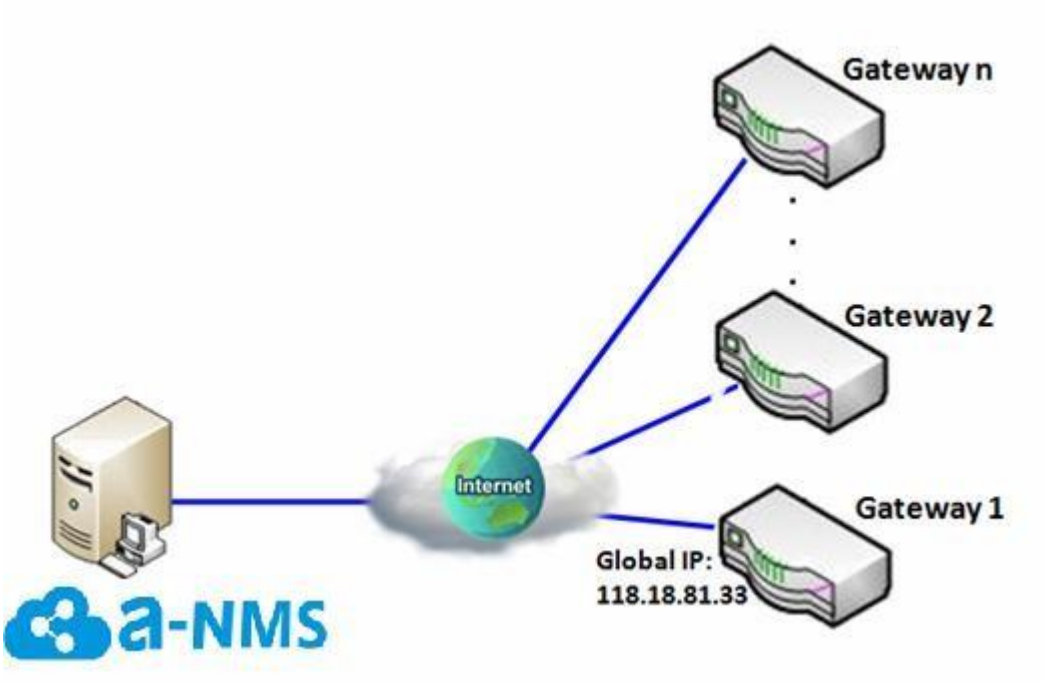
項目	設定値	説明
複製	出力ファイル	構成コンテンツをデータベースから複製し、構成ファイルとして保管します。 （例：txtConfig clone /tmp/config） 構成ファイルの内容は、上記のプレーンテキストコマンドと同じです。このアクションは、「バックアップ」プレーンテキスト設定の実行とまったく同じです。
コミット	既存のファイル	構成内容をデータベースにコミットします。 （例：txtConfig commit /tmp/config）

有効	該当なし	プレーンテキストシステム構成を有効します。 （例：txtConfig enable）
無効	該当なし	プレーンテキストシステム構成を無効します。 （例：txtConfig disable）
run_immediately	該当なし	データベースでコミットされた構成内容を適用します。 （例：txtConfig run_immediately）
run_immediately	既存のファイル	適用する構成ファイルを割り当てます。 （例：txtConfig run_immediately /tmp/config）

6-1-2. Device Management

※Device Management はサポートされていない機能です。

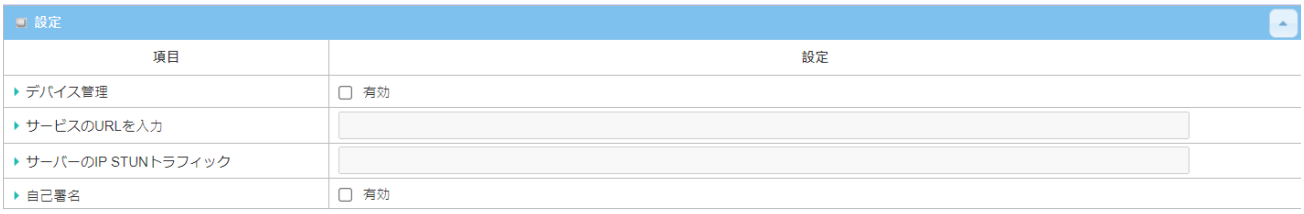
管理（Administration） ＞ 設定と管理 ＞ 「Device Management」タブ



シナリオの説明

a-NMSプラットフォームは、これらのゲートウェイを構成し、最新のFWでアップグレードし、監視することができます。

リモートゲートウェイは、各期間に実行するジョブについて a-NMS プラットフォームに問い合わせます。a-NMS プラットフォームは、ゲートウェイにいくつかの緊急ジョブの実行を要求できます。



項目	設定値	説明
デバイス管理	1.デフォルトは、 チェックなしです	有効ボックスにチェックを入れて、 Device Management を有効にします。
サービスの URL を入力	1.入力必須	a-NMS 管理者に依頼し、a-NMS の URL を提供して、手動で設定することができます。
サーバーの IP STUN トラフィック	1.デフォルトは、 空白です	サーバーのパブリック IP、またはドメイン名を指定します。
自己署名	1.デフォルトは、 チェックありです	自身を証明するために発行する証明書を有効にする場合は、有効ボックスにチェックを入れます。

6-1-3. SNMP

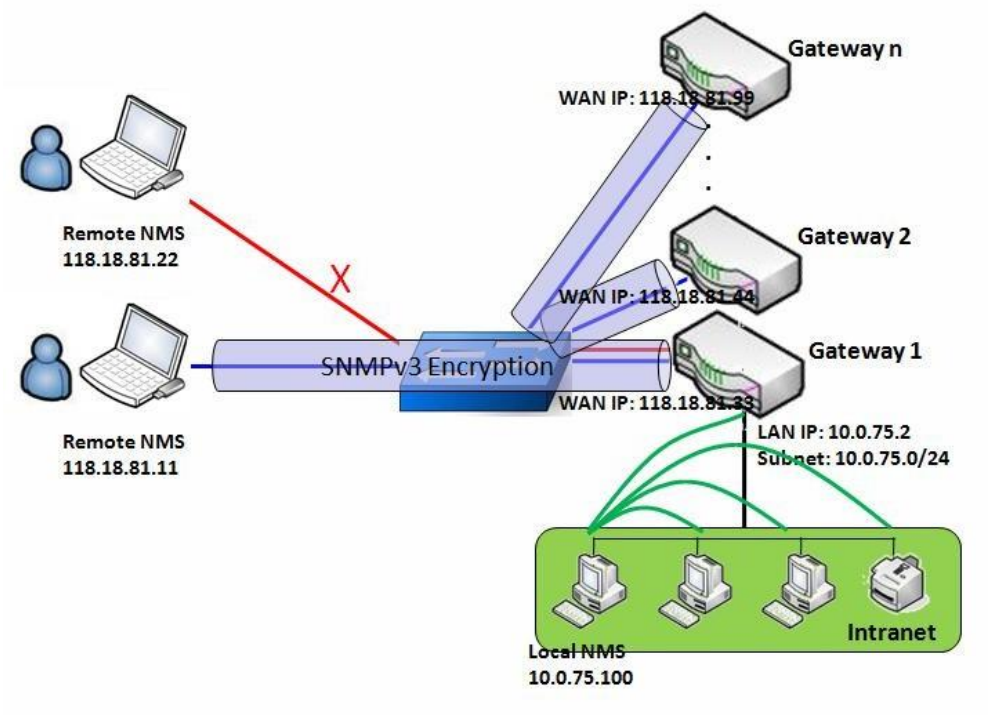
SNMP（簡易ネットワーク管理プロトコル）は、簡単に言えば、ユーザーが端末値のポーリングと設定、およびネットワークイベントの監視により、リモートでコンピュータネットワークを管理できるようにするためのプロトコルです。

一般的なSNMPの使用例では、1台または複数の管理用コンピュータ（マネージャ）が、コンピュータネットワークのホストやデバイスのグループの監視や管理を行います。管理対象システムは、エージェントと呼ばれるソフトウェアコンポーネントを常時実行し、SNMP経由で情報をマネージャに報告します。

SNMPエージェントは管理対象システムに関する管理データを変数として提供します。このプロトコルでは、これらの変数をリモートで変更することにより、アクティブな管理タスク（構成の変更と適用など）を実行することもできます。SNMP経由でアクセスできる変数は階層別にまとめられます。これらの階層やその他のメタデータ（変数の型や説明など）はMIB（管理情報ベース）に記述されていま す。

本デバイスではSNMPエージェント用に複数の公開MIBと1つの非公開MIBを使用できます。使用できるMIBは次の通りです：
MIB-II（RFC1213、IPv6を含む）、IF-MIB、IP-MIB、TCP-MIB、UDP-MIB、SMIv1 および SMIv2、SNMPv2-TMおよびSNMPv2-MIB、および、AMIB（AMITプライベートMIB）

SNMP 管理シナリオ



シナリオの適用タイミング

SNMPネットワーク管理システム（NMS）には、2つのアプリケーションシナリオがあります。ローカル NMS は、イントラネット上にあり、イントラネット内の SNMP プロトコルをサポートするすべてのデバイスを管理します。もう1つは、スイッチまたは UDP転送機能を備えたルーターを使用して、WAN インターフェイスが相互に接続されているデバイスを管理する Remote NMS（リモートNMS）です。一部のデバイスを管理し、すべてがSNMPプロトコルをサポートしている場合は、アプリケーションシナリオの1つ、特にイントラネット内のデバイスの管理を使用してください。

シナリオ説明

NMSサーバーは、SNMPプロトコルを使用して管理対象デバイスを監視および設定することができます。これらのデバイスは、UDP パケットが NMS から到達できる場所に配置されています。

管理対象デバイスは、緊急のトラップイベントを NMS サーバーに報告します。

プロトコルの SNMPv3 バージョンを使用すると、SNMP コマンドと応答の送信を保護することができます。

特権 IP アドレスを持つリモート NMS は、デバイスを管理できますが、他のリモート NMS は管理できません。

パラメータの設定例

次の表に、上図のゲートウェイ 1 の例として、LAN および WAN インターフェイスで「SNMP」を有効にした場合のパラメータ設定を示します。
表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path（構成パス）	[SNMP]-[Configuration（構成）]
SNMP Enable（SNMP有効）	■ LAN ■ WAN
Supported Versions（サポートバージョン）	■ v1 ■ v2c ■ v3
Get/Set Community（コミュニティの取得/設定）	読み取りコミュニティ/書き込みコミュニティ
Trap Event Receiver 1 （トラップイベントレシーバ 1）	118.18.81.11
WAN Access IP Address（WANアクセスIPアドレス）	118.18.81.11

Configuration Path （構成パス）	[SNMP]-[User Privacy Definition（ユーザープライバシー定義）]		
ID	1	2	3
User Name（ユーザー名）	UserName1	UserName2	UserName3
Password（パスワード）	Password1	Password2	Disable（無効）
Anthentiation 認証	MD5	SHA-1	Disable（無効）

Encryption（暗号化）	DES	Disable（無効）	Disable（無効）
Privacy Mode（プライバシーモード）	authPriv	authNoPriv	noAuthNoPriv
Privacy Key（プライバシーキー）	12345678	Disable（無効）	Disable（無効）
Authority（権限）	Read/Write（読み取り/書き込み）	Read（読み取り）	Read（読み取り）
Enable（有効）	Enable（有効）	Enable（有効）	Enable（有効）

シナリオ操作手順

上図では、NMS サーバーは、イントラネットまたは UDP到達可能ネットワーク内の複数のデバイスを管理することができます。「Gateway1（ゲートウェイ1）」は、管理対象デバイスの1つであり、LANインターフェイスでは 10.0.75.2、WAN-1インターフェイスでは 118.18.81.33 の IPアドレスを持ちます。これは、NATルーターとして機能します。

最初の段階で、NMSマネージャは、すべての管理対象デバイスの関連情報を準備し、NMS システムに記録します。次に、NMSシステムは、SNMP get コマンドを使用して、すべての管理対象デバイスのステータスを取得します。

管理者が、管理対象デバイスを構成したい場合、NMSシステムで、SNMP set コマンドを使用して管理することができます。マネージャが、SNMPv3 プロトコルを使用して「Gateway1（ゲートウェイ1）」を構成する場合、「UserName1」アカウントが使用されます。アカウントの権限が「Read/Write（読み取り/書き込み）」であるため、「UserName1」アカウントのみが「Gateway1（ゲートウェイ1）」に NMSからの設定を受け入れることができます。

管理対象デバイスに緊急イベントを送信すると、デバイスはトラップイベントレシーバにトラップを発行します。NMS自体は、その中にあります。

NMSと管理対象デバイス間で送信されたSNMPコマンドと応答を保護する場合は、SNMPv3 バージョンのプロトコルを使用します。

特権IPアドレスを持つNMSのみ、「Gateway1（ゲートウェイ1）」を WANインターフェイス経由で管理できるため、特権IPアドレスを持たないリモートNMSは、「Gateway1（ゲートウェイ1）」を管理することができません。

SNMP設定

管理（Administration） ＞ 設定と管理 ＞ 「SNMP」タブに進みます。

SNMPを使用すると、インターフェイス、バージョン、アクセス制御、トラップレシーバなどのSNMP関連設定を構成することができます。

SNMPの有効

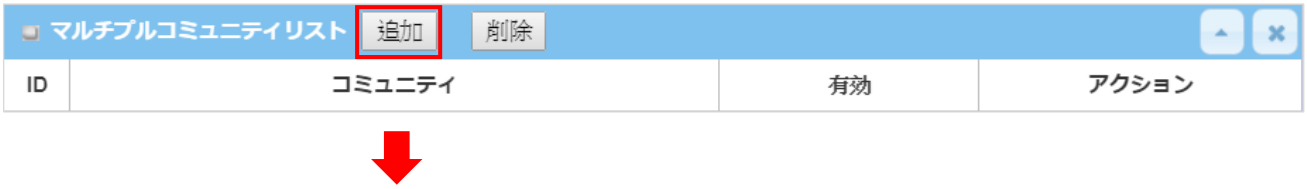
項目	設定値	説明
SNMP 有効	1. デフォルトは、チェックなしです	SNMP のインターフェイスを選択し、SNMP 機能を有効にします。 LAN ボックスにチェックを入れると、SNMP 機能が有効になり、LAN 側から SNMP にアクセスできます。 WAN ボックスにチェックを入れると、SNMP 機能が有効になり、WAN 側から SNMP にアクセスできます。
WAN インタフェース	1. デフォルトは、「すべての WAN」です	基本ネットワーク WAN-1～WAN-n の設定が完了したら、WAN-1～WAN-n を選択することができます。
サポートバージョン	1. v1 ボックスは、デフォルトでチェックありです 2. v2c ボックスは、デフォルトでチェックありです	SNMP のバージョンを選択します。 v1 ボックスにチェックが入っているとき。 バージョン 1 で、SNMP にアクセスすることができます。 v2 ボックスにチェックが入っているとき。 バージョン 2c で、SNMP にアクセスすることができます。 v3 ボックスにチェックが入っているとき。 バージョン 3 で、SNMP にアクセスすることができます。
SNMP ポート	1. 文字列形式：任意のポート番号 2. デフォルト SNMP ポートは、161 です 3. 入力必須	SNMP Port（SNMP ポート）を指定します。 任意のポート番号を入力することができます。しかし、ポート番号を使用しないようにする必要があります。 値の範囲： 1～65535
遠隔アクセスの設定（Limited	1. 文字列形式：任意の Ipv4 アドレス	WAN の Remote Access IP（リモートアクセス IP）を指定します。

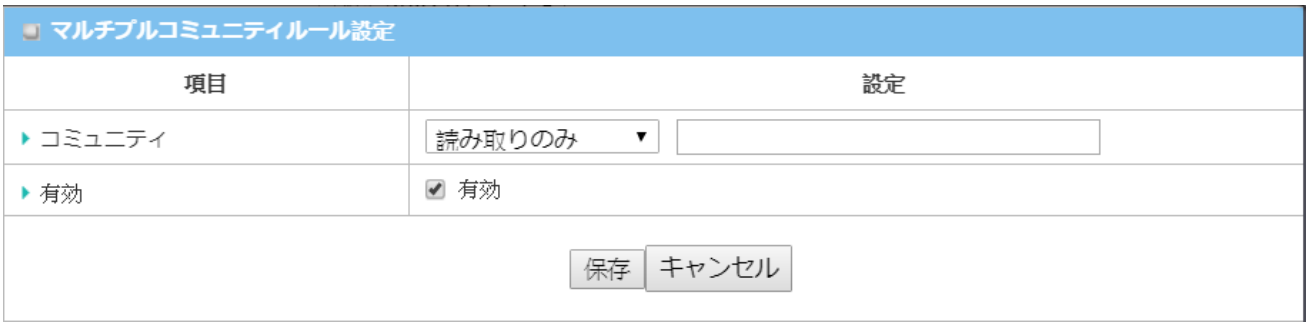
Remote Access IP)		特定の IP アドレスを選択した場合。これは、この IP アドレスだけが、WAN 側から SNMP にアクセスできることを意味します。 特定の IP 範囲を選択した場合。これは、この IP 範囲だけが、WAN 側から SNMP にアクセスできることを意味します。 ブランクのままにしておくと、任意の IP アドレスが、WAN 側から SNMP にアクセスできることを意味します。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
元に戻す	該当なし	[元に戻す]ボタンをクリックして、設定をキャンセルします。

複数コミュニティの作成/編集

SNMPを使用すると、バージョン1、およびバージョン2のユーザーのアクセス制御をカスタマイズすることができます。ルーターは、最大10のコミュニティセットをサポートします。

［追加］ボタンが適用されると、「マルチプルコミュニティルール構成」画面が表示されます。





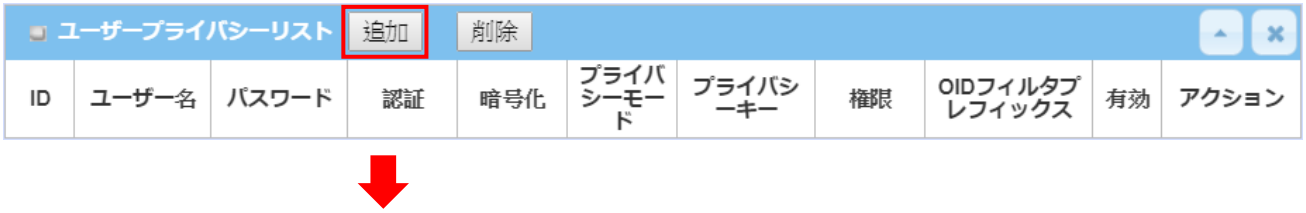
項目	設定値	説明
コミュニティ	1. デフォルトは、「読み取りのみ」です 2. 入力必須 3. 文字列形式：任意のテキスト	「読み取りのみ」、または「読み取り書き込み」アクセスが許可されるこのバージョン 1、またはバージョン v2c ユーザーのコミュニティをそれぞれ指定します。 コミュニティの最大長は 32 です。
有効	1. デフォルトは、チェックありです	このバージョン 1、またはバージョン v2c ユーザーを有効にするには、「有効」にチェックをします。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。

元に戻す	該当なし	[元に戻す]ボタンをクリックして、設定をキャンセルします。
前へ	該当なし	[前へ]ボタンをクリックして、最後のページに戻ります。

ユーザープライバシーの作成/編集

SNMPを使用すると、バージョン3のユーザーのアクセス制御をカスタマイズすることができます。ルーターは、最大128のユーザープライバシーセットをサポートします。

［追加］ボタンが適用されると、「ユーザープライバシールール設定」画面が表示されます。



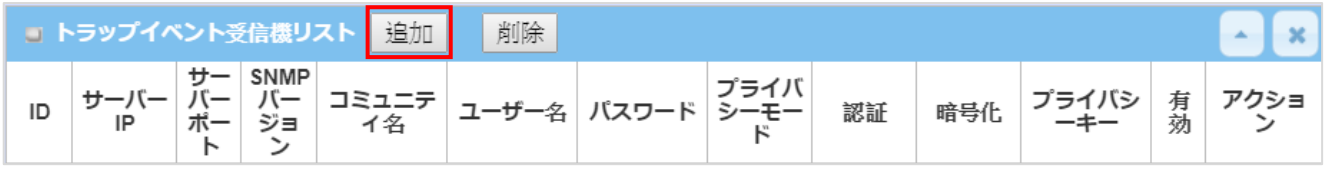
項目	設定値	説明
ユーザー名	1. 入力必須 2. 文字列形式： 任意のテキスト	このバージョン 3 ユーザーの「ユーザー名」を指定します。 値の範囲：1～32 文字
パスワード	1. 文字列形式： 任意のテキスト	「プライバシーモード」が「authNoPriv」、または「authPriv」の場合、このバージョン 3 ユーザーの「パスワード」を指定する必要があります。 値の範囲： 8～64 文字
認証	1. デフォルトは、「なし」です	「プライバシーモード」が「authNoPriv」、または「authPriv」の場合、このバージョン 3 ユーザーの Authentication（認証タイプ）を指定する必要があります。 使用する認証タイプ MD5 / SHA-1 を選択します。

暗号化	1.デフォルトは、「なし」です	「プライバシーモード」が「authPriv」の場合、このバージョン 3 ユーザーの「暗号化」プロトコルを指定する必要があります。使用する暗号化プロトコル DES / AES を選択します。
プライバシーモード	1.デフォルトは、「noAuthNoPriv」です	このバージョン 3 ユーザーの「プライバシーモード」を指定します。 ・「noAuthNoPriv」を選択： 認証タイプと暗号化プロトコルは使用しません。 ・「authNoPriv」を選択： 「認証」および「パスワード」を指定する必要があります。 ・「authPriv」を選択： 「認証」、「パスワード」、「暗号化」および「プライバシーキー」を指定する必要があります。
プライバシーキー	1.文字列形式：任意のテキスト	「プライバシーモード」が、「authPriv」の場合、このバージョン 3 ユーザーの「プライバシーキー」(8～64 文字) を指定する必要があります。
権限	1.デフォルトは、「読み取り」です	「読み取り専用」(GET および GETNEXT)、または 「読み取り/書き込み」(GET、GETNEXT および SET) アクセスを許可する、このバージョン 3 ユーザーの権限をそれぞれ指定します。
OID フィルタプレフィックス	1.デフォルトは、「1」です 2.入力必須 3.文字列形式：任意の有効な OID	「OID フィルタプレフィックス」は、このバージョン 3 ユーザーのアクセスを、指定された OID をルートとするサブツリーに制限します。 値の範囲： 1～2080768
有効	1.デフォルトは、チェックありです	有効にチェックをつけると、バージョン 3 ユーザーを有効にします。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。しかし、SNMP 機能には適用されません。SNMP メインページに戻るとき「Click on save button to apply your changes（変更を適用するには保存ボタンをクリックしてください)」と表示され、メインページの［保存］ボタンをクリックするように促します。
元に戻す	該当なし	[元に戻す]ボタンをクリックして、設定をキャンセルします。
前へ	該当なし	[前へ]ボタンをクリックして、最後のページに戻ります。

トラップイベントレシーバの作成/編集

SNMPを使用すると、トラップイベント受信機をカスタム設定することができます。
ルーターは、最大4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。

［追加］ボタンが適用されると、「トラップイベント受信機ルール設定」画面が表示されます。
デフォルトのSNMPバージョンは v1です。設定画面には、バージョン1の必須項目が表示されます。



v2c を選択すると、構成画面はバージョンを除いて、v1とまったく同じになります。
v3 を選択すると、構成画面にバージョン3トラップの設定項目が追加されます。

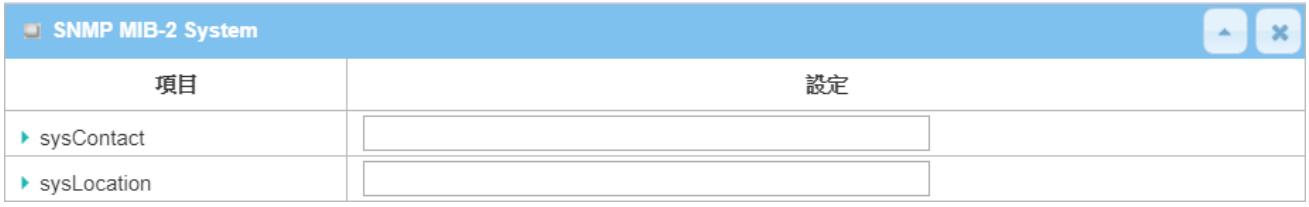
項目	設定値	説明
サーバーIP	1. 入力必須 2. 文字列形式：任意の Ipv4 アドレス	トラップサーバーIP を指定します。 DUT はサーバーIP にトラップを送信します。

サーバーポート	1.文字列形式：任意のポート番号 2.デフォルト SNMP トラップポートは 162 です 3.入力必須	トラップ「サーバーポート」を指定します。 任意のポート番号を入力することができます。 しかし、ポート番号を使用しないようにする必要があります。 値の範囲：1～65535
SNMP バージョン	1.デフォルトは、v1 です。	トラップのバージョンを選択します。 ・v1 を選択： 設定画面には、バージョン 1 の必須項目が表示されます。 ・v2c を選択： 設定画面には、バージョン 2c の必須項目が表示されます。 ・v3 を選択： 設定画面には、バージョン 3 の必須項目が表示されます。
コミュニティ名	1.v1 および v2c は入力必須 2.文字列形式：任意のテキスト	このバージョン 1 またはバージョン v2c トラップのコミュニティ名を指定します。 値の範囲：1～32 文字
ユーザー名	1.v3 は入力必須 2.文字列形式：任意のテキスト	このバージョン 3 トラップの「ユーザー名」を指定します。 値の範囲：1～32 文字
パスワード	1.v3 は入力必須 2.文字列形式：任意のテキスト	「プライバシーモード」が「authNoPriv」、または「authPriv」の場合、このバージョン 3 トラップの「パスワード」を指定する必要があります。 値の範囲：8～64 文字
プライバシーモード	1.v3 は入力必須 2.デフォルトは、「noAuthNoPriv」です	このバージョン 3 トラップの「プライバシーモード」を指定します。 ・「noAuthNoPriv」を選択： 認証タイプと暗号化プロトコルは使用しません。 ・「authPriv」を選択： 「Authentication」（認証）、および「パスワード」を指定する必要があります。 ・「authPriv」を選択： 「Authentication」（認証）、「パスワード」、「暗号化」および「プライバシーキー」を指定する必要があります。
認証	1.v3 は入力必須 2.デフォルトは、「なし」です	「プライバシーモード」が「authNoPriv」、または「authPriv」の場合、このバージョン 3 トラップの「認証タイプ」を指定する必要があります。 使用する認証タイプ MD5 / SHA-1 を選択します。
暗号化	1.v3 は入力必須 2.デフォルトは、「なし」です	「プライバシーモード」が、「authPriv」の場合、このバージョン 3 トラップの「暗号化」プロトコルを指定する必要があります。 使用する暗号化プロトコル DES / AES を選択します。
プライバシーキー	1.v3 は入力必須 2.文字列形式：任意のテキスト	「プライバシーモード」が、「authPriv」の場合、このバージョン 3 トラップの「プライバシーキー」（8～64 文字）を指定する必要があります。

有効	1. デフォルトは、チェックありです	有効にチェックをつけると、このトラップレシーバを有効にします。
保存	該当なし	［保存］ボタンをクリックして、構成を保存します。しかし、SNMP 機能には適用されません。SNMP メインページに戻るとき「Click on save button to apply your changes（変更を適用するには保存ボタンをクリックしてください)」と表示され、メインページの［保存］ボタンをクリックするように促します。
元に戻す	該当なし	[元に戻す]ボタンをクリックして、設定をキャンセルします。
前へ	該当なし	[前へ]ボタンをクリックして、最後のページに戻ります。

SNMP MIBーシステムの指定

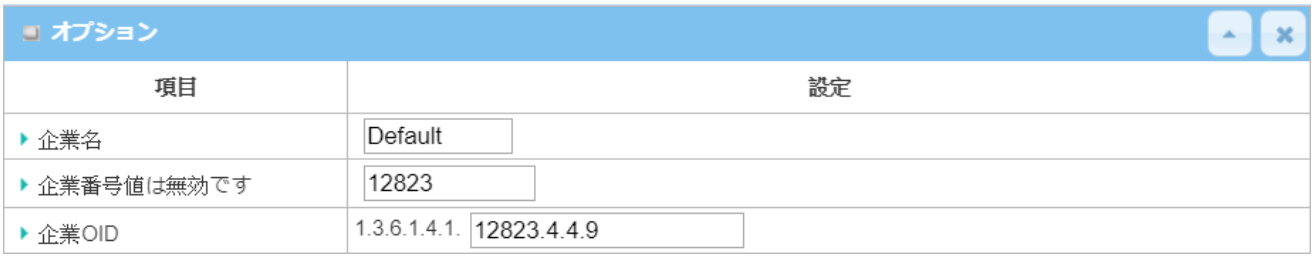
必要に応じて、MIB-2 システムに必要な情報を指定することもできます。



項目	設定値	説明
sysContact	1. 任意設定 2. 文字列形式：任意のテキスト	MIB-2 システムの連絡先情報を指定します。 値の範囲：0～64 文字
sysLocation	1. 任意設定 2. 文字列形式：任意のテキスト	MIB-2 システムの位置情報を指定します。 値の範囲：0～64 文字

SNMP オプションの編集

特定のプライベートMIBを使用する場合は、企業名、番号、およびOIDを入力する必要があります。



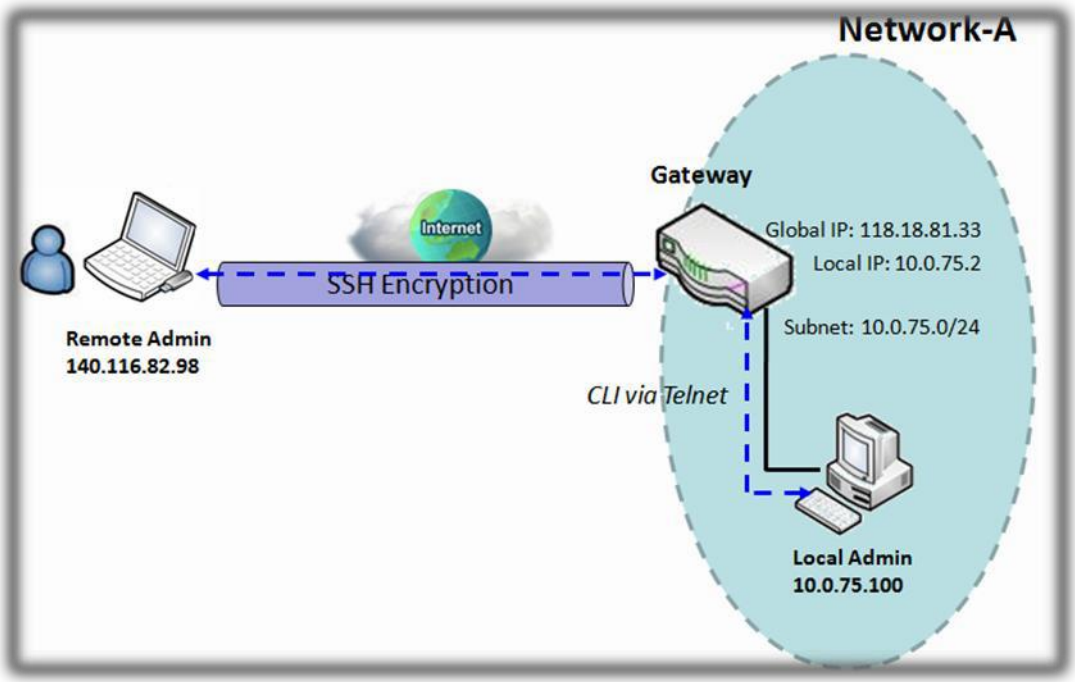
項目	設定値	説明
企業名	1. デフォルトは、「AMIT」です 2. 入力必須 3. 文字列形式：任意のテキスト	特定のプライベート MIB の企業名を指定します。 値の範囲：1～10 文字、A～Z、a～z、0～9、「-」、「_」。

企業番号値は無効です	1.デフォルトは、「12823」です （AMIT の企業番号） 2.入力必須 3.文字列形式：任意の数字	特定のプライベート MIB の企業番号を指定します。 値の範囲：1～2080768
企業 OID	1.デフォルトは、 1.3.6.1.4.1.12823.4.4.9 （AMIT の企業 OID） 2.入力必須 3.文字列形式：任意の有効な OID	特定のプライベート MIB の企業 OID を指定します。各 OID 番号の範囲は 1～2080768 です。 企業 OID の最大長は 31 です。 7 番目の番号は、企業番号と同一でなければなりません。
保存	該当なし	［保存］ボタンをクリックして、変更を SNMP 機能に適用します。
元に戻す	該当なし	[元に戻す]ボタンをクリックして、設定をキャンセルします。

6-1-4. Telnet & SSH

コマンドラインインターフェイス（CLI）はコマンドラインユーザーインターフェイス、コンソール ユーザーインターフェイスとも呼ばれています。これはコンピュータプログラムを操作する方法のひとつで、ユーザー（またはクライアント）がプログラムに対して、連続するテキスト行（コマンドライン）の形式でコマンドを実行します。このインターフェイスには通常コマンドラインシェルが実装されています。これは、コマンドをテキスト入力として受け取り、所定のオペレーティング システムの機能に変換します。一般的に、コマンドラインインターフェイスがあるプログラムの方が、スクリプトによる自動化が簡単にできます。本デバイスでは Telnet と SSH（Secure Shell）CLIの両方が使用できます。デフォルトのサービスポートはそれぞれ 23 と 22 です。

Telnet および SSH のシナリオ



シナリオの適用タイミング

ゲートウェイ管理者が、イントラネットまたはインターネットのリモートサイトから管理する場合、「Telnet」または「SSH」ユーティリティを使用して、「Telnet with CLI」機能を使用することができます。

シナリオ説明

ローカル管理者またはリモート管理者は、特権ユーザー名とパスワードで、「Telnet」または「SSH」ユーティリティを使用して、ゲートウェイを管理することができます。
ローカル管理者とゲートウェイ間、または、リモート管理者とゲートウェイ間のデータパケットは、プレーンテキストまたは暗号化されたテキストにすることができます。ローカル管理者用の イントラネットでは、「Telnet」ユーティリティを使用するプレーンテキストであり、リモート管理者用の暗号化されたテキストは、「SSH」ユーティリティを使用することを推奨します。

パラメータの設定例

次の表に、上図のゲートウェイ1の例として、LAN および WAN インターフェイスで「Telnet with CLI」を有効にした場合のパラメータ設定を示します。
表に記載されていないパラメータには、デフォルト値を使用します。

Configuration Path（構成パス）	[Telnet with CLI]-[Configuration（構成）]
Telnet with CLI	LAN： ■ EnableWAN： ■ Enable
Connection Type（接続タイプ）	Telnet： サービスポート 23 ■ Enable SSH： サービスポート 22 ■ Enable

シナリオ操作手順

上図では、「ローカル管理者」または「リモート管理者」が、イントラネットまたはインターネットの「ゲートウェイ」を管理することができます。「ゲートウェイ」は、ネットワーク-A のゲートウェイであり、イントラネットのサブネットは 10.0.75.0/24 です。これは、LAN インターフェイスに対して 10.0.75.2、WAN-1 インターフェイスに対して 118.18.81.33 の IP アドレスを持っています。これは、NAT ゲートウェイとして機能します。

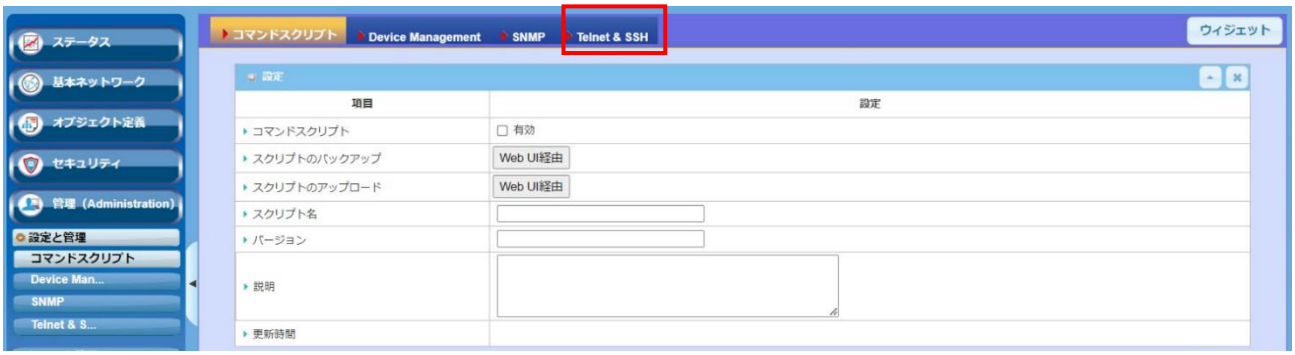
イントラネットの「ローカル管理者」は、特権アカウントで「Telnet」ユーティリティを使用して、ゲートウェイにログインします。

または、インターネットの「リモート管理者」は、特権アカウントで「SSH」ユーティリティを使用して、ゲートウェイにログインします。

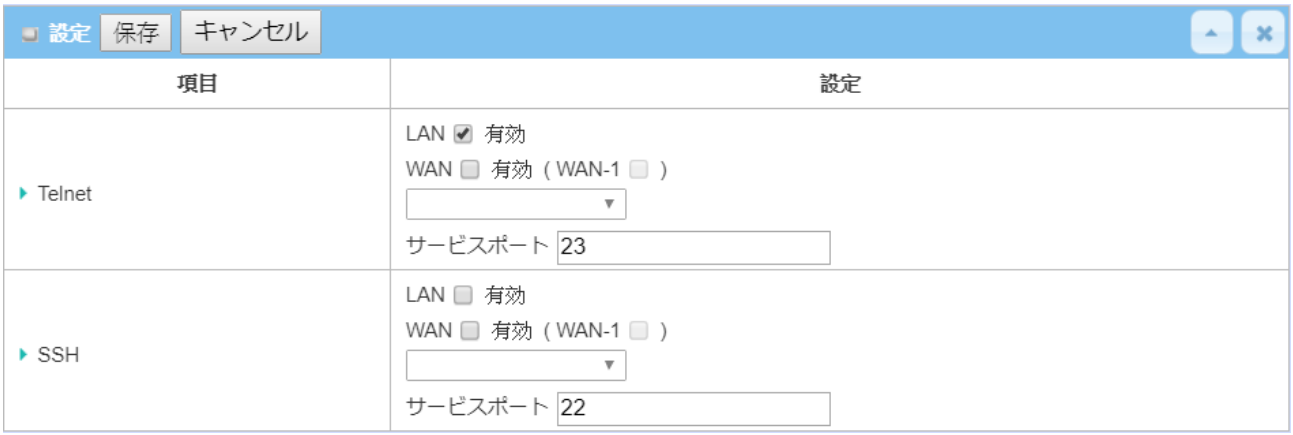
ゲートウェイ管理者は、ゲートウェイの前にいるかのようにデバイスを制御することができます。

Telnet with CLI設定

管理（Administration） ＞ 設定と管理 ＞ 「Telnet & SSH」タブに進みます。



Telnet with CLI 設定により、管理者は従来の Telnetプログラムを通じてこのデバイスにアクセス することができます。端末にログインする前に、関連する設定とパスワードを慎重に設定してください。
パスワード管理部分では、TelnetとSSHのロギングに、rootパスワードを設定することができます。



項目	設定値	説明
Telnet	1. デフォルトは、LAN 有効ボックスにチェックありです 2. 「サービスポート」のデフォルトは、「23」です	有効ボックスにチェックを入れ、Telnet サービスを有効します。対応するサービスを提供するサービスポートの数を設定することができます。 値の範囲： 1～65535
SSH	1. デフォルトは、LAN 有効ボックスにチェックありです 2. 「サービスポート」のデフォルトは、「22」です	有効ボックスにチェックを入れ、SSH サービスを有効します。対応するサービスを提供するサービスポートの数を設定することができます。 値の範囲： 1～65535
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、設定をキャンセルします。

項目	設定値	説明
パスワード	1. 文字列：任意のテキスト（空白文字を含みません） 2. Telnet のデフォルトパスワードは、「wirelessm2m」です	古いパスワードを入力し、新しいパスワードを指定して、root パスワードを変更します。 注： デバイスを展開する前に、デフォルトの Telnet パスワードを変更することを強くお勧めします。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
元に戻す	該当なし	[元に戻す]ボタンをクリックして、設定をキャンセルします。

6-2. システム操作

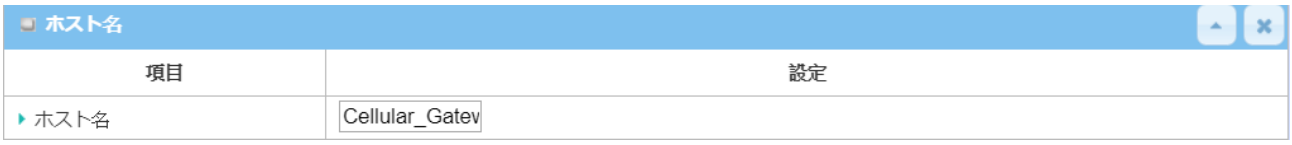
システム操作により、ネットワーク管理者は、Web ベースのユーティリティアクセスパスワードの変更、システム情報、システム時刻、システムログ、ファームウェア/設定のバックアップと復元、リセットおよび再起動などのシステム設定を管理することができます。

6-2-1. パスワードおよび MMI

管理（Administration）＞[システム管理] ＞[パスワード & MMI] タブに進みます。

ホスト名の設定

ホスト名画面で、ネットワーク管理者はゲートウェイのホスト名を設定/変更できます。



項目	設定値	説明
ホスト名	デフォルトは空白です	ゲートウェイのホスト名を入力します。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、設定をキャンセルします。

ユーザー名の変更

ユーザー名画面では、ネットワーク管理者は Webベースの MMIログインアカウントをアクセスゲートウェイに変更できます。

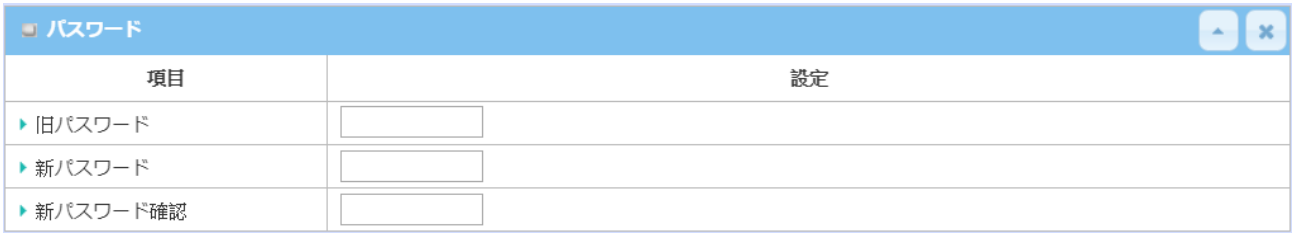
[変更]ボタンをクリックし、新しいユーザー名設定を入力します。

項目	設定値	説明
ユーザー名	Web にログインする時、デフォルトのユーザー名は「admin」です	現在のログインアカウントのユーザー名を表示します。
新しいユーザーネーム	文字列：任意のテキスト	新しいユーザー名を入力して、現在の設定を置き換えます。

パスワード	文字列：任意のテキスト	現在のパスワードを入力して、ユーザー名の設定を変更する権限があるかどうかを確認します。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、設定をキャンセルします。

パスワードの変更

パスワード変更画面では、ネットワーク管理者は、WebベースのMMIログインパスワードをアクセスゲートウェイに変更することができます。



項目	設定値	説明
旧パスワード	1.文字列：任意のテキスト 2.Web ベースの MMI のデフォルトパスワードは、「admin」です	現在のパスワードを入力して、パスワードの変更をロック解除できるようにします。
新パスワード	文字列：任意のテキスト	新パスワードを入力します。
新パスワード確認	文字列：任意のテキスト	再度、新パスワードを入力し、確認します。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして設定をキャンセルします。

アクセスのための MMI 設定の変更

これは、管理者が管理のためにゲートウェイにアクセスできるようにするゲートウェイのWebベースの MMアクセスです。

ゲートウェイの WebベースのMMIは、アイドル時間が経過すると自動的にログアウトします。この設定により、管理者は自動ログアウトを有効にし、ログアウトアイドル時間を設定することができます。

ログインタイムアウトを無効にすると、システムは管理者を自動的にログアウトしません。

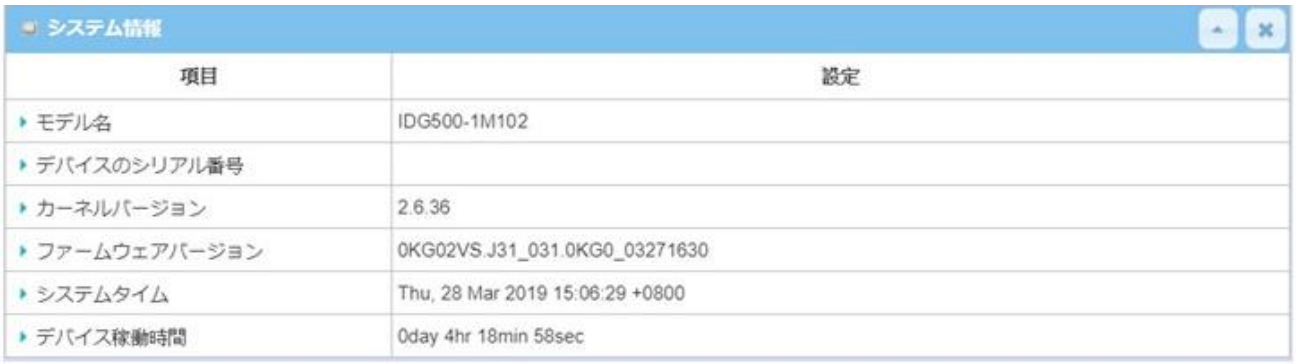
項目	設定値	説明
ログイン	デフォルトは、「3 回」です	ログイン試行カウント値を入力します。値の範囲： 3～10。誤ったパスワードを使って、カウント値を超えて Web GUI にログインしようとすると、「Already reaching maximum Password- Guessing times, please wait a few seconds!（すでに最大パスワード試行回数に達しています。数秒お待ちください！）」という警告メッセージが表示され、次のログイン試行は無視されます。
ログイン タイムアウト	デフォルトは、チェックありです	有効ボックスにチェックを入れ、自動ログアウト機能を有効にし、最大アイドル時間を指定します。 値の範囲： 30～65535。
GUI アクセス プロトコル	デフォルトは、「http/https」です	GUIアクセスに使用するプロトコルを選択します。 http/https、http only、https only から選択可能です。
HTTPS 証明書のセットアップ	デフォルトは、「デフォルト」です	［https Access Protocol（https アクセスプロトコル）］が選択されている場合は、HTTPs 証明書のセットアップを使用して、さらに構成を行うことができます。 デフォルトのままにするか、ドロップダウンリストから期待される 証明書とキーを選択することができます。 証明書の構成については、オブジェクト定義 > 「証明書」のセクションを参照してください。 ※オブジェクト定義 >「証明書」は、本製品では対応しておりません。
HTTP 圧縮	デフォルトは、チェックなしです	任意の圧縮方法が望ましい場合は、ボックスをチェックします。 gzip、デフレート（deflate）が選択可能です。

HTTP バインディング	デフォルトは、 「DHCP-1」です	httpアクセスでバインドする DHCP サーバーを選択します。
システム 起動モード	デフォルトは、「通常起動モード」です	システムを起動するために採用されるシステム起動モードを選択します。 ・通常起動モード: 起動時間が長くなり、デバイスの起動中に完全なファームウェアイメージチェックが行われます。 ・速い起動モード: デバイスの起動中にファームウェアイメージを確認することなく、起動時間が通常起動より約 5～10秒短縮されます。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
キャンセル	該当なし	[キャンセル]ボタンをクリックして、設定をキャンセルします。

6-2-2. 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購入したゲートウェイのデバイス情報をすばやく調べることができます。

管理（Administration） > **［システム管理］> 「システム情報」タブ**に進みます。



項目	設定値	説明
モデル名	該当なし	この製品のモデル名が表示されます。
デバイスのシリアル番号	該当なし	この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	該当なし	製品の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	該当なし	製品のファームウェアバージョンが表示されます。
CPU 使用率	該当なし	CPU使用率をパーセントで表示します。
メモリ使用率	該当なし	デバイスのメモリ率をパーセントで表示します。
システムタイム	該当なし	このWebページを閲覧した現在のシステム時刻を表示します。
デバイス稼働時間	該当なし	前回の起動以降のデバイスの稼働時間の統計情報が表示されます。
更新	該当なし	[更新]ボタンをクリックして、直ちにシステム情報を更新します。

6-2-3. システムタイム

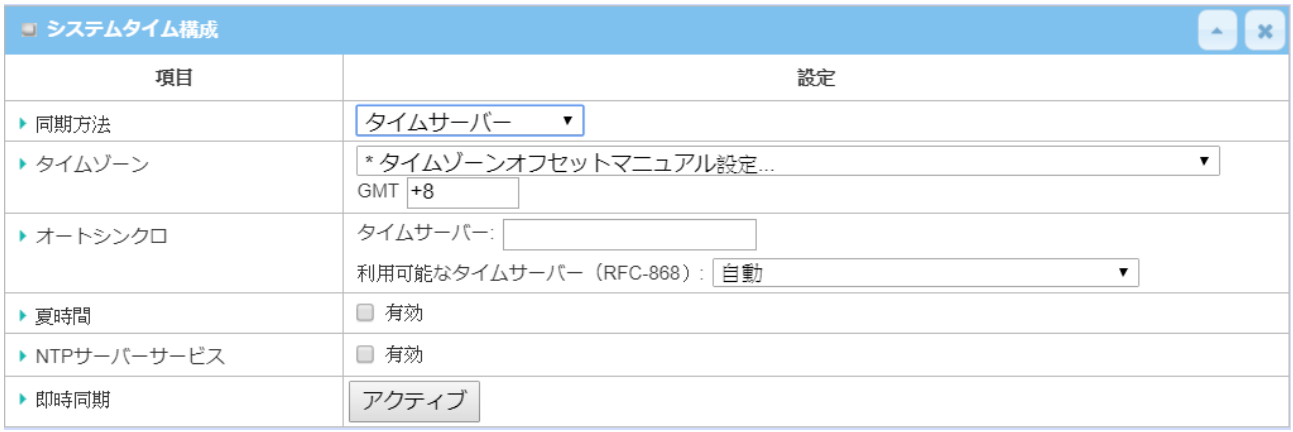
ゲートウェイは、管理者がゲートウェイのシステム時刻を設定するために、手動で設定および自動同期化された方法を提供します。サポートされる時刻は、［タイムサーバー］、［手動］、［PC］、［セルラーモジュール］のいずれかです。
最初に方法を選択し、次に残りの設定を構成します。
ゲートウェイのシステム時刻を手動で設定するのではなく、正しい時刻情報を設定してゲートウェイのシステム時刻として設定する簡単で迅速なソリューションが2つあります。

1番目は「タイマーサーバーとの同期」です。上記の時刻情報設定画面でのタイムゾーンとタイムサーバーの選択に基づいて、［Synchronize immediately（直ちに同期）］ボタンをクリックすると、システムは NTPプロトコルでタイムサーバーと通信し、システムの日付と時刻を取得します。

2 番目は「自分の PC と同期する」です。
方法を選択すると、システムは、その日付と時刻を管理 PC の時刻と同期させます。

管理（Administration）＞［システム管理］＞［システムタイム］タブに進みます。

■タイムサーバーと同期する

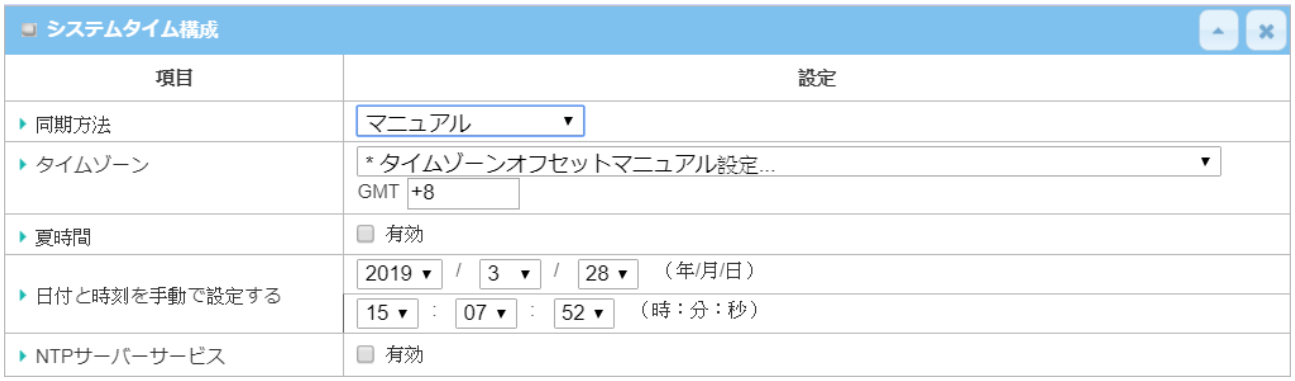


項目	設定値	説明
同期方法	1. 入力必須 2. デフォルトは、 「タイムサーバー」です	システム時刻の同期方法として**「タイムサーバー」**を選択します。
タイムゾーン	デフォルトは、 「GMT+00 :00」です	デバイスの所在地のタイムゾーンを選択します。
オートシンクロ	1. 入力必須 2. デフォルトは、「自動」です	有効ボックスにチェックを入れ、特定のNTPサーバーで時刻自動同期機能を有効します。 利用可能なサーバーが1つずつ時刻同期に使用されるよう、NTPサーバーのIP、または FQDN を入力するか、または自動モードのままにします。

夏時間	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、夏時間機能を有効します。 この機能を有効にする際、夏時間の開始日と終了日を指定する必要があります。
即時同期	該当なし	[アクティブ]ボタンをクリックすると、指定されたタイムサーバーとシステム時刻を即座に同期させることができます。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
更新	該当なし	[更新]ボタンをクリックして、直ちにシステム情報を更新します。

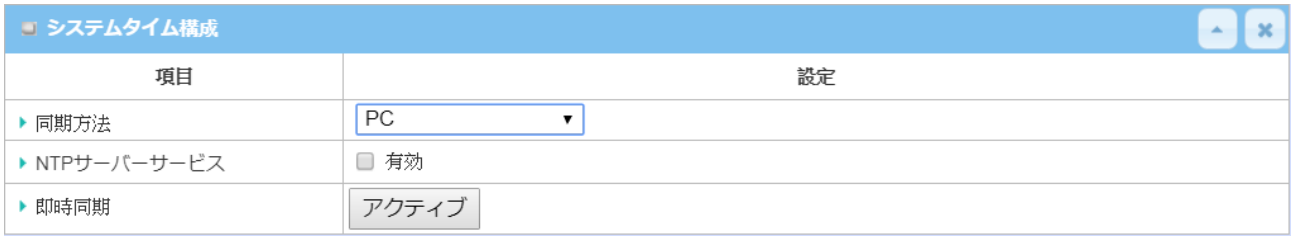
注：デバイスの正しいタイムゾーンを選択することを忘れないでください。
正しいタイムゾーンを選択しなかった場合、デバイスの現地時間ではなく、
UTC（協定世界時）の時刻が取得されます。

■手動で設定と同期する



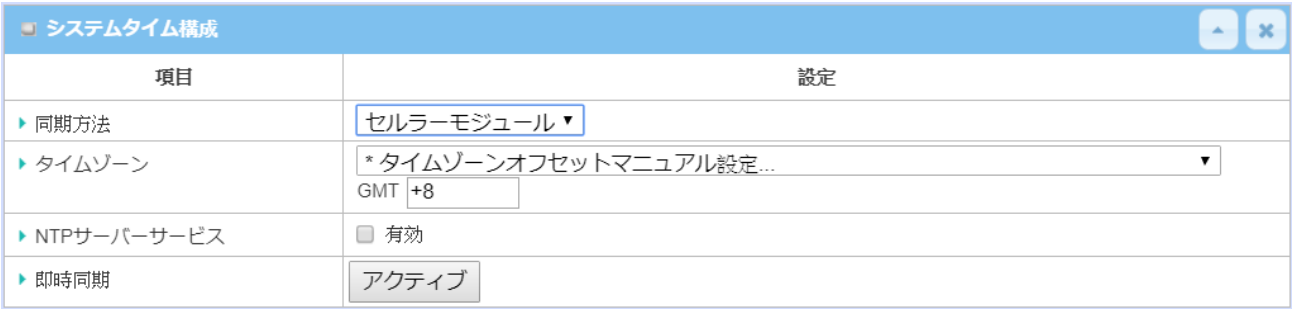
項目	設定値	説明
同期方法	1. 入力必須 2. デフォルトは、 「タイムサーバー」です	システム時刻の同期方法として、**「マニュアル」**を選択します。 これは、管理者が手動で日付と時刻を設定する必要があることを意味します。
タイムゾーン	デフォルトは、 「GMT+00 :00」です	デバイスの所在地のタイムゾーンを選択します。
夏時間	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、夏時間機能を有効します。 この機能を有効にする際、夏時間の開始日と終了日を指定する必要があります。
日付と時刻を手動で設定する	該当なし	時間自動同期機能を有効にしない場合は、日付（年/月/日）と時刻（時：分：秒）を手動で設定することもできます。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。

■PC と同期する



項目	設定値	説明
同期方法	1. 入力必須 2. デフォルトは、 「タイムサーバー」です	システム時刻の同期方法として**「PC」**を選択すると、システムが日付と 時刻を管理 PC の時刻に同期させます。
即時同期	該当なし	[アクティブ]ボタンをクリックすると、指定されたタイムサーバーとシステム時刻を即座に同期させることができます。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
更新	該当なし	[更新]ボタンをクリックして、直ちにシステム情報を更新します。

■セルラータイムサービスと同期する

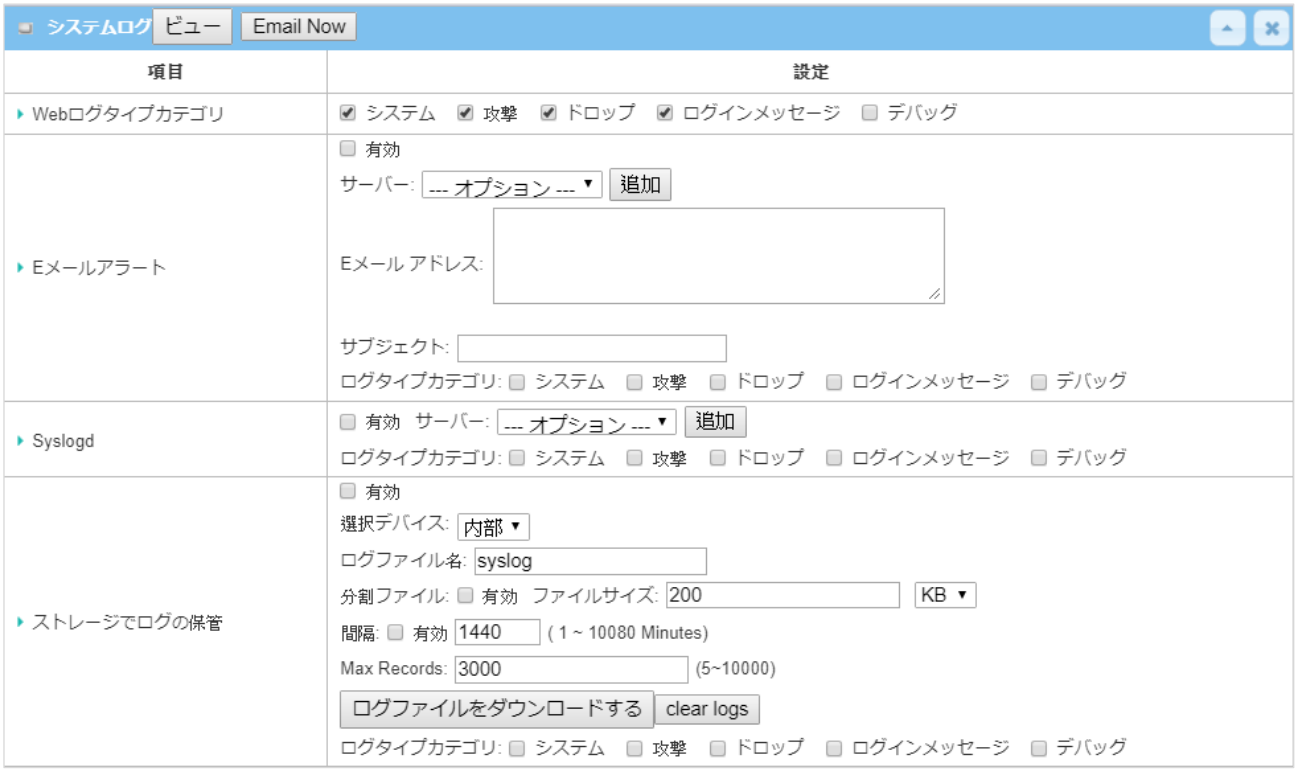


項目	設定値	説明
同期方法	1. 入力必須 2. デフォルトは、 「タイムサーバー」です	接続されたモバイル ISP から提供される時刻にシステムが日付と時刻を同期させるために、システム時刻の同期方法として、**「セルラーモジュール」**を選択します。 注：Cellular WAN インターフェイスを備えた製品でのみ使用できます。
タイムゾーン	デフォルトは、 「GMT+00 :00」です	デバイスの所在地のタイムゾーンを選択します。
即時同期	該当なし	[アクティブ]ボタンをクリックすると、指定されたタイムサーバーとシステム時刻を即座に同期させることができます。
保存	該当なし	[保存]ボタンをクリックして設定を保存します。
更新	該当なし	[更新]ボタンをクリックして、直ちにシステム情報を更新します。

6-2-4. 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する、さまざまなイベントログツールが含まれています。

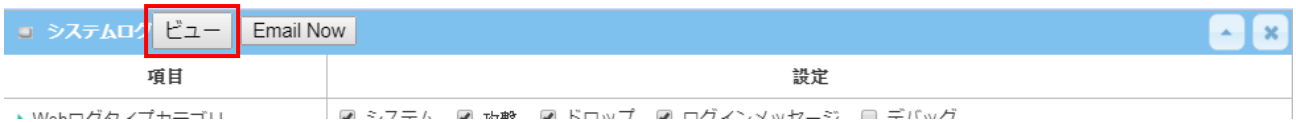
管理（Administration）> ［システム管理］> ［システムログ］タブに進みます。

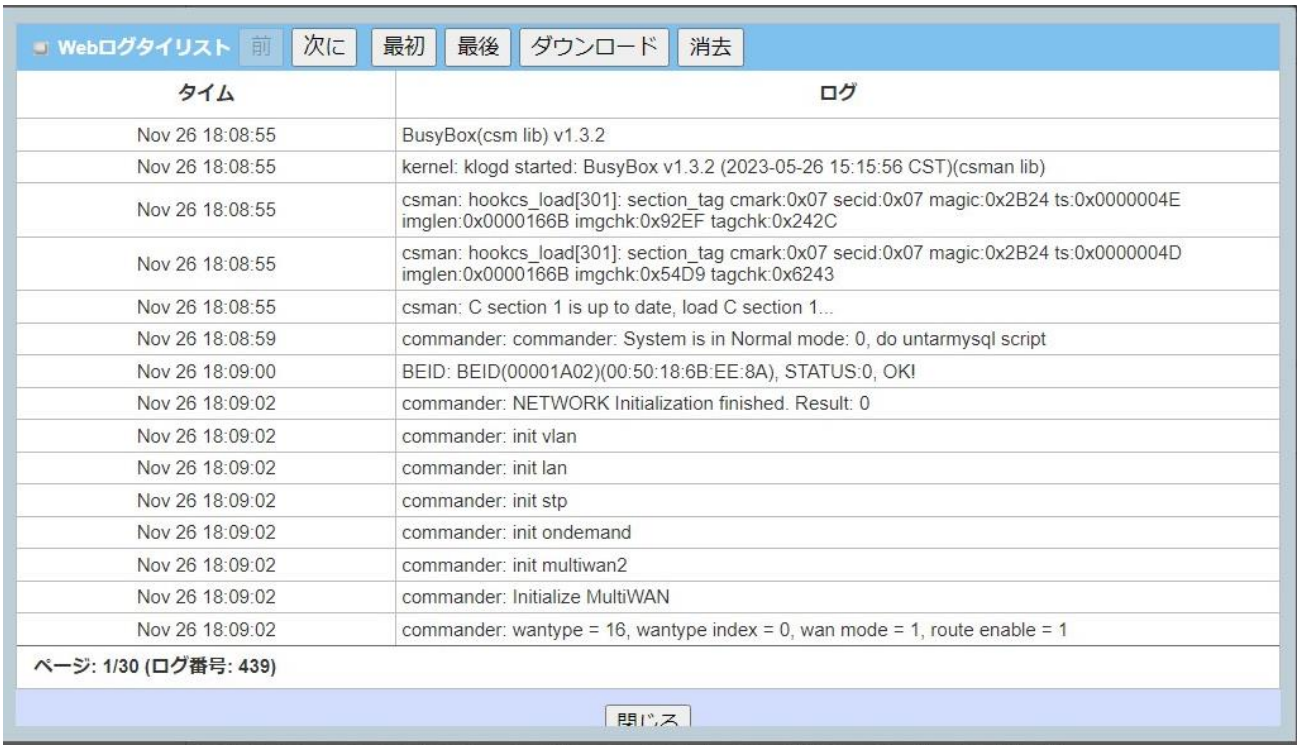


表示および Eメールログ履歴

ネットワーク管理者がゲートウェイのログ履歴を表示するための[ビュー]ボタンが用意されています。[Email Now]ボタンを使用すると、管理者はインスタントEメールを分析用に送信することができます。

項目	設定値	説明
[ビュー]ボタン	該当なし	[ビュー]ボタンをクリックすると、Web ログリストウィンドウにログ履歴が表示されます。
[Email Now]ボタン	該当なし	[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。





Webログリスト ウィンドウ		
項目	設定値	説明
時間列	該当なし	イベントタイムスタンプを表示します。
ログ列	該当なし	ログメッセージを表示します。

Webログリスト ボタンの説明		
ボタン	設定値	説明
前	該当なし	[前]ボタンをクリックして、前ページに移動します。
次	該当なし	[次]ボタンをクリックして、次ページに移動します。
最初	該当なし	[最初]ボタンをクリックして、最初のページにジャンプします。
最後	該当なし	[最後]ボタンをクリックして、最後のページにジャンプします。
ダウンロード	該当なし	[ダウンロード]ボタンをクリックして、tar ファイル形式でPCにログをダウンロードします。
消去	該当なし	[消去]ボタンをクリックして、すべてのログを消去します。
閉じる	該当なし	[閉じる]ボタンをクリックして、Webログリストウィンドウを閉じます。

Web ログタイプカテゴリ

Web ログタイプカテゴリ画面では、ネットワーク管理者は、前のセクションで説明したように、 記録するイベントのタイプを選択して、Webログリストウィンドウに表示することができます。[ビュー]ボタンをクリックすると、Web ログリストウィンドウにログ履歴が表示されます。

Webログタイプカテゴリ設定ウィンドウ		
項目	設定値	説明
システム	デフォルトは、チェックありです	チェックを入れ、システムイベントを記録し、Web ログリストウィンドウに表示します。
攻撃	デフォルトは、チェックありです	チェックを入れ、攻撃イベントを記録し、Webログリストウィンドウに表示します。
ドロップ	デフォルトは、チェックありです	チェックを入れ、ドロップイベントを記録し、Webログリストウィンドウに表示します。
ログインメッセージ	デフォルトは、チェックありです	チェックを入れ、ログイベントを記録し、Webログリストウィンドウに表示します。
デバッグ	デフォルトは、チェックありです	チェックを入れ、デバッグイベントを記録し、Webログリストウィンドウに表示します。

Eメールアラート

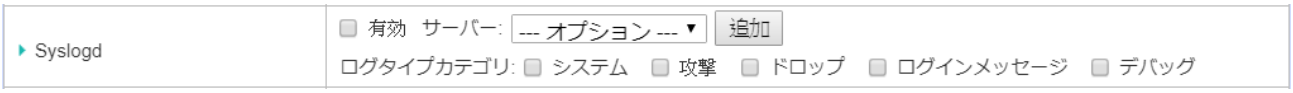
Eメールアラート画面では、ネットワーク管理者が、ログに記録するイベントの種類を選択し、 宛先電子メールアカウントに送信することができます。

Eメールアラート設定ウィンドウ		
項目	設定値	説明
有効	デフォルトは、チェックありです	有効ボックスにチェックを入れ、E メールアドレスの空白スペースで定義された宛先電子メールアカウントにイベントログメッセージを送信できるようにします。
サーバー	該当なし	Eメールを送信するには、「サーバー」のドロップダウンボックスからメールサーバーを1つ選択します。 何も利用できない場合は、[追加]ボタンをクリックして、送信メールサーバーを作成します。 また、オブジェクト定義 > 外部サーバー >「外部サーバー」タブから、送信メールサーバーを追加することもできます。 ※「外部サーバー」は、本製品では対応しておりません。

E メールアドレス	文字列：E メール形式	受信者のEメールアドレスを入力します。E メールアドレスをカンマ、セミコロン、またはセミコロンで区切ります。 Eメールアドレスを「myemail@domain.com」の形式で入力します。
サブジェクト	文字列：任意のテキスト	Eメールの件名を入力して、Eメールクライアントで簡単に識別できるようにします。
ログタイプカテゴリ	デフォルトは、チェックなしです	記録するイベントのタイプを選択し、指定されたEメールアカウントに送信します。 システム、攻撃、ドロップ、ログインメッセージ、デバッグ が利用可能です。

Syslogd

Syslogd 画面では、ネットワーク管理者が、ログに記録するイベントの種類を選択し、宛先 Syslogdサーバーに送信することができます。



Syslogd設定ウィンドウ		
項目	**設定値**	**説明**
有効	デフォルトは、チェックなしです	有効ボックスにチェックを入れ、Syslogd 機能を有効し、イベントログを Syslog サーバーに送信します。
サーバー	該当なし	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。 何も利用できない場合は、[追加]ボタンをクリックして、システムログサーバーを作成します。 また、オブジェクト定義 > 外部サーバー > 「外部サーバー」タブから、システムログサーバーを追加することもできます。 ※「外部サーバー」は、本製品では対応しておりません。
ログタイプカテゴリ	デフォルトは、チェックなしです	記録するイベントのタイプを選択し、指定されたシスログサーバーに送信します。 システム、攻撃、ドロップ、ログインメッセージ、デバッグ が利用可能です。

ログの保管

ログの保管画面では、ネットワーク管理者がログに記録するイベントの種類を選択し、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。

Syslogd設定ウィンドウ		
項目	設定値	説明
有効	デフォルトは、 チェックなしです	チェックを入れ、ログのストレージへの送信を有効します。
選択デバイス	デフォルトは、 「内部」です	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	デフォルトは、 チェックなしです	指定されたストレージに保存するログファイル名を入力します。
分割ファイル の有効	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、ログファイルが指定された制限に達 するたびにファイルを分割します。
分割ファイル のサイズ	デフォルトは、 「200KB」です	各分割ログファイルのファイルサイズ制限を入力します。 値の範囲： 10～1000。
間隔	デフォルトは、 「1440 分」です	システムは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： 1～10080。
間隔の有効	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、ログ間隔の設定を保存します。
ログタイプ カテゴリ	デフォルトは、 チェックなしです	送信するログの種類を確認します。 システム、攻撃、ドロップ、ログインメッセージ、デバッグが利用可能です。

ログの保管ボタンの定義		
項目	設定値	説明
ログファイルの ダウンロード	該当なし	[ログファイルをダウンロードする]ボタンをクリックして、ログファイルを tar ファイルにダウンロードします。

6-2-5. バックアップおよび復元

バックアップおよび復元ウィンドウでは、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。
工場出荷時の設定に加えて、特別な構成設定をカスタマイズされたデフォルト値としてカスタマイズすることもできます。このカスタマイズされたデフォルト値を使って、必要に応じて、デバイスを期待されるデフォルト設定にリセットすることができます。

管理（Administration）＞［システム管理］＞［バックアップおよび復元］タブに進みます。

ログの保管設定ウィンドウ		
項目	**設定値**	**説明**
FW アップグレード	デフォルトは、「Web UI 経由」です	新しいファームウェアが利用可能な場合は、[FW アップグレード]ボタンをクリックして、「Web UI 経由」または「ストレージ経由」でデバイスファームウェアをアップグレードします。 [FW アップグレード]をクリックし、[ファイルを選択]ボタンを使って、新しいファームウェアのファイル名を指定し、[アップグレード]ボタンをクリックして、本デバイスで FW アップグレードを開始します。GPL ポリシーからのファームウェアをアップグレードする場合は、「非公式ファームウェアの承諾」にチェックを入れてください。
バックアップ設定	デフォルトは、「ダウンロード」です	[Web UI 経由]ボタンをクリックすると、デバイスの設定をバックアップまたは復元できます。 ・ダウンロード：デバイス構成を config.bin ファイルにバックアップします。 ・アップロード：指定された構成ファイルをデバイスに復元します。 ・[Web UI 経由]：Web UI 経由で設定ファイルを取得します。

オートリストア設定 （自動復元構成）	デフォルトは、チェックなしです	有効ボックスにチェックを入れ、カスタマイズされたデフォルト設定機能を有効にします。 機能が有効になったら、[保存 Conf.]ボタンをクリックして、希望の設定をカスタマイズされたデフォルト設定として保存することができます。 また、[クリア Conf.]をクリックして、保存・カスタマイズされた構成を消去します。

6-2-6. 再起動およびリセット

特別な理由または状況によっては、ゲートウェイを再起動するか、デバイスの設定をデフォルト値にリセットする必要があります。
これらの操作を実行は、電源オン/オフ、デバイスパネルのリセットボタンを押す、または、Web GUIでも行うことができます。

管理（Administration） ＞ **［システム管理］** ＞ **［再起動およびリセット］タブ**に進みます。

再起動およびリセットウィンドウで、リセットボタンをクリックして、このデバイスを再起動し、リセットボタンをクリックして、このデバイスをデフォルト設定にリセットすることができます。

システム操作ウィンドウ		
項目	**設定値**	**説明**
再起動	デフォルトは、「今すぐ」です	[再起動]ボタンを押して直ちにゲートウェイを再起動する、または事前定義した時間スケジュールに再起動します。 ・**今すぐ**：直ちに再起動します。 ・**時間スケジュール**：指定した時刻にデバイスを自動的に再起動するには、事前定義済み自動再起動時間スケジュールルールを選択します。 時間スケジュールを定義するには、オブジェクト定義 >スケジューリング ＞ 「設定」タブに進みます。
デフォルト設定に戻す	該当なし	[設定リセット]ボタンをクリックし、デバイスの設定をデフォルト値にリセットします。

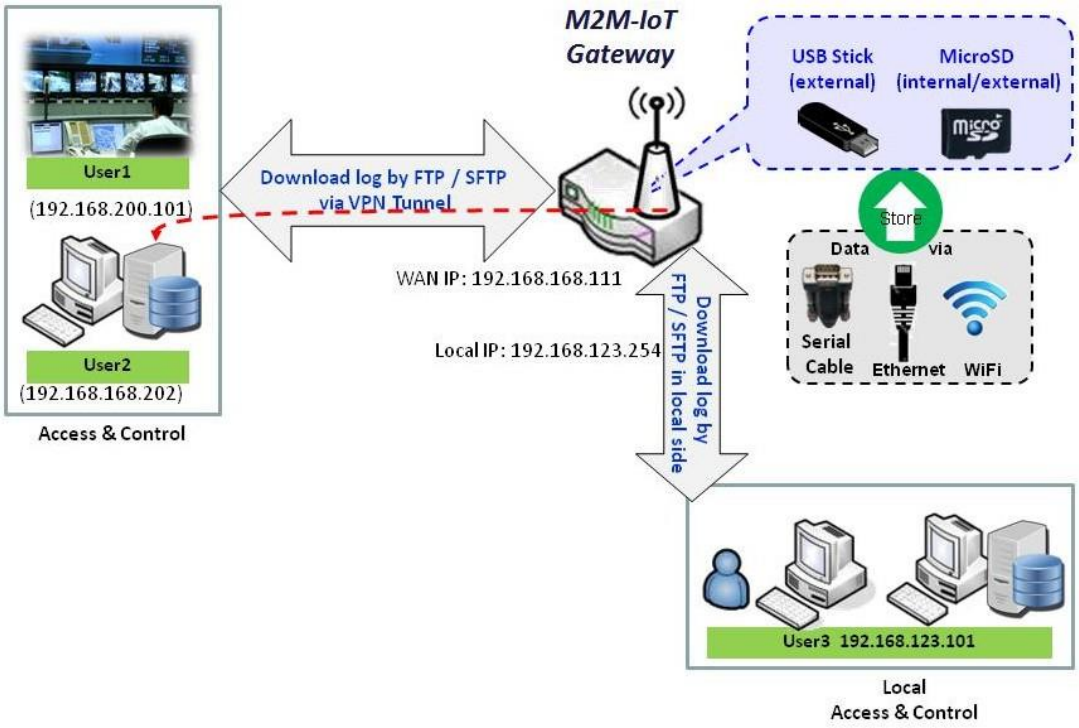
6-3. FTP

ファイル転送プロトコル（FTP）は、コンピュータネットワーク上のクライアントとサーバーの間で、コンピュータファイルを転送するために使用される標準的なネットワークプロトコルです。FTPは、クライアント/サーバーモデルアーキテクチャ上に構築され、クライアントとサーバーの間で別々の制御とデータ接続を使用します。 FTPユーザーは、通常、ユーザー名とパスワードの形式でクリアテキストサインインプロトコルで自分自身を認証できますが、サーバーが許可するように構成されている場合は匿名で接続できます。

ユーザー名とパスワードを保護し、コンテンツを暗号化する安全な伝送のために、FTPは、多くの場合、SSL/TLS（FTPS）で保護されます。 さらに、SSHファイル転送プロトコル（SFTP）が 代わりに使用されることもありますが、技術的には異なります。

このゲートウェイは、管理者が自分のコンピュータまたはデータベースにログファイルをダウンロードするためのFTP/SFTPサーバーを組み込んでいます。次の2つのセクションでは、FTPサーバーを構成し、サーバーにログインできるユーザーアカウントを作成できます。FTPサーバーにログインした後、ログディレクトリを参照したり、 保存されたログファイルをダウンロードしたり、ダウンロードしたファイルを削除したり、追加のデータログ用の記憶領域を増やしたりすることができます。

使用可能なログファイルは、システムログ（管理（Administration） >システム管理 >システムログ を参照）、ネットワークパケット（管理（Administration） >診断 >パケットアナライザ を参照）。
購入した製品でサポートされているさまざまなログ機能を適切に設定することで、FTP/SFTP接続経由でログをダウンロードできます。



6-3-1. サーバー構成

このセクションでは、関心のあるログファイルを取得するための組み込みFTPおよびSFTPサーバーを設定できます。

［（管理）Administration］ > ［FTP］ > ［サーバー構成］タブに進みます。

FTPサーバーを有効にする

構成		
項目	**設定値**	**説明**
FTP	デフォルトは、チェックなしです	［有効］ボックスにチェックを入れると、組み込み FTP サーバー機能が有効になります。 FTP サーバーを有効にすると、FTP 接続を介して、保存されたログファイルを取得または削除できます。 注：組み込み FTP サーバーはログダウンロード専用です。したがって、ストレージへのユーザーファイルのアップロードには書き込み権限が実装されていません。
FTP ポート	デフォルトは、「21」です	FTP 接続のポート番号を指定します。ゲートウェイは、指定されたポートで受信 FTP 接続を待ち受けます。 値の範囲： 1～65535
タイムアウト	デフォルトは、「300」です	FTP 接続の最大タイムアウト間隔を指定します。サポートされる範囲は 60～7200 秒です。
最大接続 IP アドレスごと	デフォルトは、「2」クライアントです	FTP 接続の同じ IP アドレスからの最大クライアント数を指定します。同じ IP アドレスから最大 5 つのクライアントがサポートされます。
最大 FTP クライアント数	デフォルトは、「2」クライアントです	FTP 接続の最大クライアント数を指定します。最大 32 のクライアントがサポートされています。
PASV モード	任意の設定	［有効］ボックスにチェックを入れると、FTP クライアントからの FTP 接続の PASV モードのサポートが有効になります。

PASV モードのポート範囲	デフォルトは、［Port 50000～50031］です	PASV 形式のデータ接続に割り当てるポート範囲を指定します。 値の範囲：1024～65535
PASV モードで自動に外部 IP をレポートする	任意の設定	［有効］ボックスにチェックを入れると、PASV コマンドに応答して IP アドレスの広告を無効にするサポートが有効になります。
ASCII 転送モード	任意の設定	［有効］ボックスにチェックを入れると、ASCII モードのデータ転送のサポートが有効になります。 デフォルトで、バイナリモードがサポートされています。
FTPS （FTP over SSL / TLS）	任意の設定	［有効］ボックスにチェックを入れ、SSL/TLS 経由のセキュアな接続のサポートを有効にします。

SFTPサーバーを有効にする

構成

項目	設定値	説明
SFTP	デフォルトは、チェックなしです	［有効］ボックスにチェックを入れると、組み込み SFTP サーバー機能が有効になります。 SFTP サーバーを有効にすると、セキュアな SFTP 接続を介して、保存されたログファイルを取得または削除できます。
SFTP ポート	デフォルトは、22 です	SFTP 接続のポート番号を指定します。ゲートウェイは、指定されたポートで受信 SFTP 接続を待ち受けます。 値の範囲： 1～65535

6-4. 診断

このゲートウェイは、管理者がトラブルシューティングを行い、ゲートウェイを通過する異常な動作または トラフィックの根本的な原因を見つけるための簡単なネットワーク診断ツールをサポートしています指定された インターフェイスまたは特定のソース/宛先ホストのパケットを記録するパケットアナライザと、ネットワーク接続の問題をテストする別のPing および Tracertツールがあります。

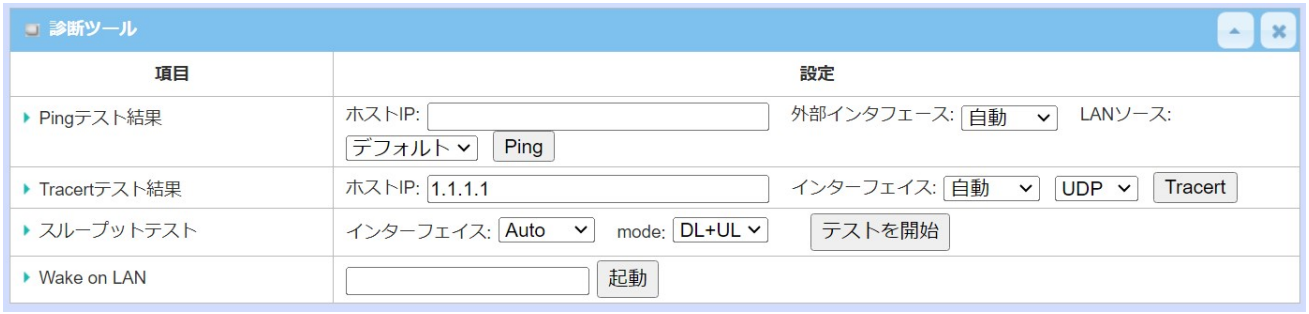
6-4-1. パケットアナライザ　【未対応】

本製品ではサポートされていない機能です。

6-4-2. 診断ツール

診断ツールは、ネットワーク管理者が、デバイスの接続を確認するためによく使用するネットワーク接続診断ツール（アプローチ）を提供します。

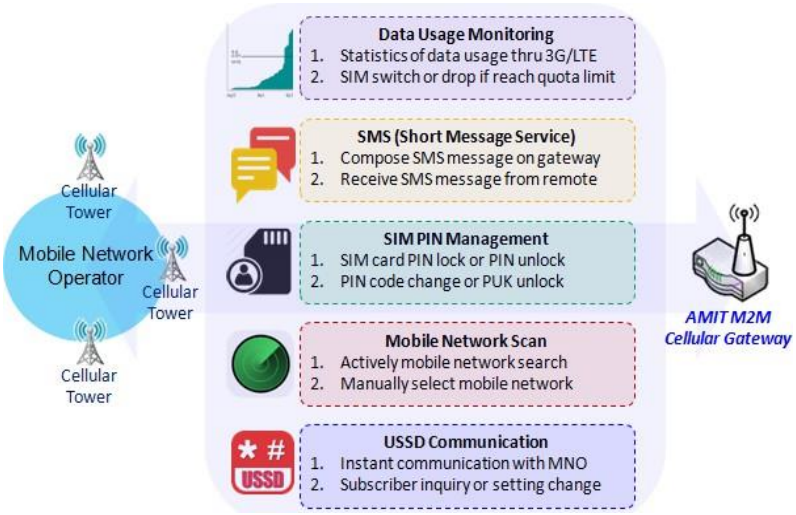
管理（Administration） ＞ **［診断］** ＞ **［診断ツール］タブ**に進みます。



※「Wake on LAN」項目は、本製品では対応しておりません。

第7章. サービス

7-1. セルラーツールキット



セルラーデータ接続以外にも、セルラー WANのデータ使用状況の監視、SMSによるテキストメッセージの送信、SIMカードの PINコードの変更、USSDコマンドによる通信事業者/ISPとの通信、診断目的のセルラーネットワークスキャンなどがあります。

「セルラーツールキット」セクションには、セルラーの構成やアプリケーションに関連するいくつかの便利な機能が含まれています。

ここでは、 SIM PIN、Network Scan（ネットワークスキャン）の設定を構成できます。このセクションの設定を続ける前に、有効なSIMカードをデバイスに挿入する必要があります。

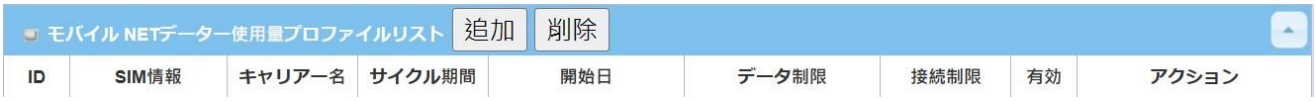
※SIM PIN・USSDは、本製品では対応しておりません。

7-1-1. データ使用量

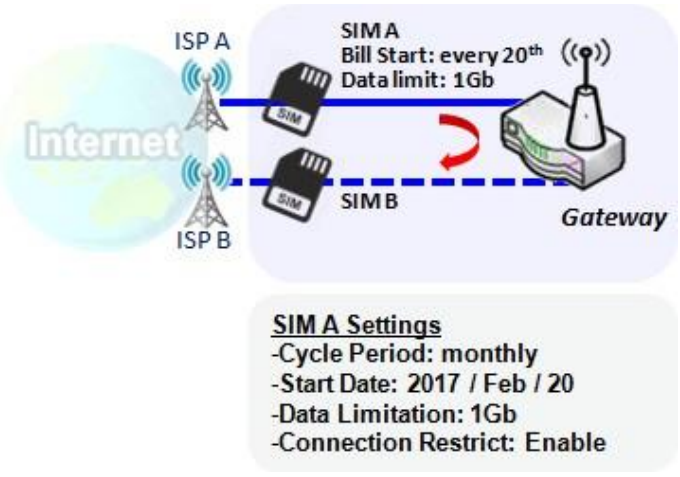
セルラー接続のデータプランの大部分は、データ使用量が制限されています。データ使用量が制限容量を超えると、毎日の運用に影響する可能性のある程度にデータスループットが大幅に低下したり、通信事業者/ISP が制限容量を超過したデータ使用量に課金するため、翌月に「請求が大幅に増える」現象が発生したりします。

データ使用量機能を使って、デバイスは、データ使用を継続的に監視し、措置を行います。データ使用量が制限容量に達すると、デバイスが、直ちにセルラーデータ接続を切断するように設定することができます。それ以外の場合、セカンダリSIMカードが挿入されている場合、デバイスは、セカンダリSIMに切り替わり、セカンダリSIMを使って、別のセルラーデータ接続を自動的に確立します。

データ使用量機能が有効になっている場合、セルラーデータ使用履歴は、
すべて、**サービス** 〉［セルラーツールキット］〉「セルラー使用量」タブで確認できます。



モバイルNETデータ使用量



データ使用量機能により、ゲートウェイ装置は、セルラーデータの使用状況を継続的に監視し、措置を行います。

この図では、SIM Aの制限容量は**1Gb**で、請求書の開始日は毎月**20日**です。このデバイスは、毎月20 日に新しいデータ使用量の計算を開始します。

接続制限の有効は、データ使用量が、制限容量（この場合は1Gb）に達すると、ゲートウェイデバイスに SIM Aのセルラー接続を強制的に切断させます。

SIMフェールオーバー機能が、**インターネット設定**で構成されている場合、ゲートウェイは、SIM Bに切り替え、新しいセルラーデータ接続を自動的に確立します。

データ使用量設定

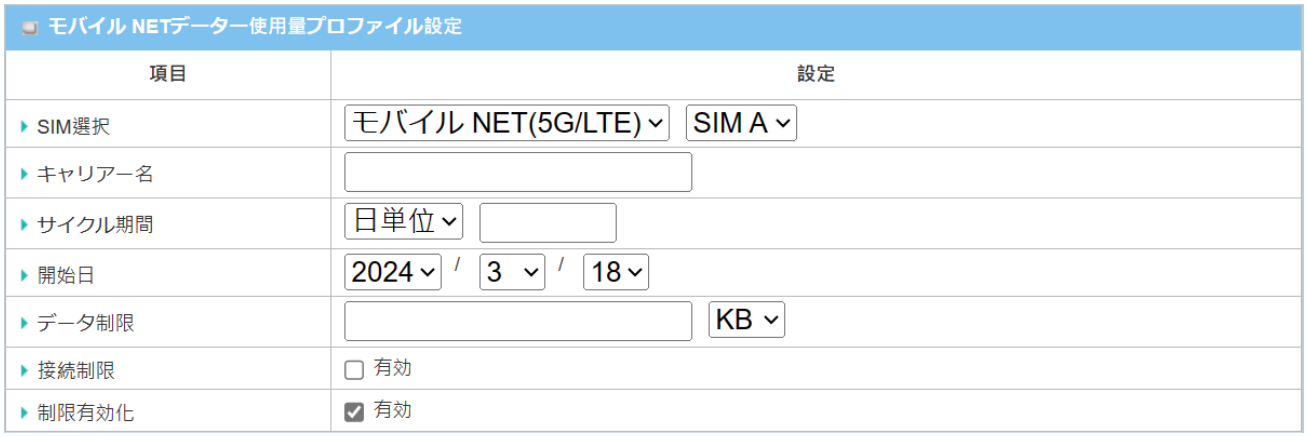
サービス > **［セルラーツールキット］** > **［データ使用量］タブ**に進みます。

データ使用量の設定を完了する前に、データプランに従って、請求書の開始日、請求期間、およびデータ使用量の制限を知る必要があります。この情報は、通信事業者またはISPに問い合わせることができます。

モバイルNET データ使用量プロファイルの作成/編集

[追加]ボタンが適用されると、「モバイルNETデータ使用量プロファイル設定」画面が表示されます。

ゲートウェイで使用される SIM カードごとに 1 つのプロファイルを使用して、最大 4 つのデータ使用量プロファイルを作成ですることがきます。



モバイルNETデータ使用量プロファイル構成		
項目	**設定値**	**説明**
SIM 選択	デフォルトは、「モバイル NET」、および「SIM A」です	セルラーインターフェイスと SIM カードを選択して、データ使用量プロファイルを構成します。 注：xxxx -2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
キャリアー名（通信事業者名）		識別のために、選択した SIM カードの通信事業者名を入力します。
サイクル期間	デフォルトは、「日単位」です	最初のボックスには、サイクル期間の 3 つのタイプがあります。 日単位、週単位、月単位です。 ・**日単位**：サイクル期間当たりについて、2 番目のボックスにさらに日数を指定する必要があります。 値の範囲：1～90 日 ・**週単位、月単位**：サイクル期間は 1 週間、または 1 ヶ月

		です。
開始日	該当なし	ネットワークトラフィックの測定を開始する日付を指定します。 過去の日付を選択しないでください。 日付を指定しない場合、トラフィック統計が正しく表示されません。
データ制限	該当なし	定義されたサイクル期間の許容データ制限を指定します。
接続制限	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、接続制限機能を有効にします。 指定されたサイクル期間中、実際のデータ使用量が許容データ制限を超えた場合、セルラー接続は強制的に切断されます。
制限有効化	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、データ使用量プロファイルを有効にします。

7-1-2. SMS

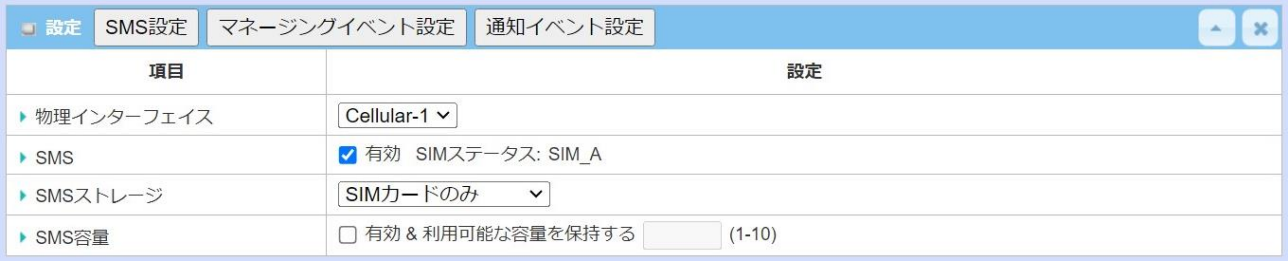
ショートメッセージサービス（SMS）とは、携帯電話で広く使用されているテキストメッセージング サービスです。これは、標準化された通信プロトコルを使用し、携帯電話またはセルラーデバイスが、短文テキストメッセージを瞬時かつ簡便に交換できるようにします。

SMS設定

サービス＞ ［セルラーツールキット］ ＞ ［SMS］タブに進みます。

このゲートウェイデバイスを使用すると、携帯電話で通常行うように、SMSテキストメッセージを送信したり、受信したSMSメッセージを参照したりすることができます。

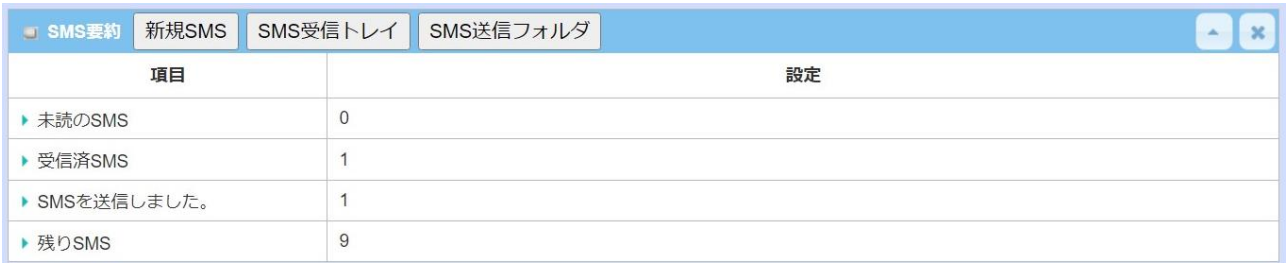
SMS 構成の設定



構成		
項目	**設定値**	**説明**
物理インターフェイス	デフォルトは、「Cellular-1」です	次の SMS 機能設定のセルラーインターフェイスを選択します。 注： Cellular-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SMS	デフォルトは、チェックありです	ボックスにチェックを入れると SMS 機能が有効になり、ボックスのチェックを外すと、SMS 機能が無効になります。
SMS ステータス	該当なし	現在の SIM のステータスに依存します。 可能な値は、SIM_A または SIM_B です。
SMS ストレージ	デフォルトは、「SIM カードのみ」です	SMS の格納場所です。 現在、選択できるのは「SIM カードのみ」です。
SMS 容量	デフォルトは、チェックなしです	有効ボックスをオンにして、使用可能なストレージスペースを予約してストレージが不足するのを防ぐために、メッセージ数の数値（1～10）を指定します。 SMS ストレージがいっぱいになると、最も古いメッセージが削除されます。
保存	該当なし	[保存]ボタンをクリックして、設定を保存します。

SMS 要約

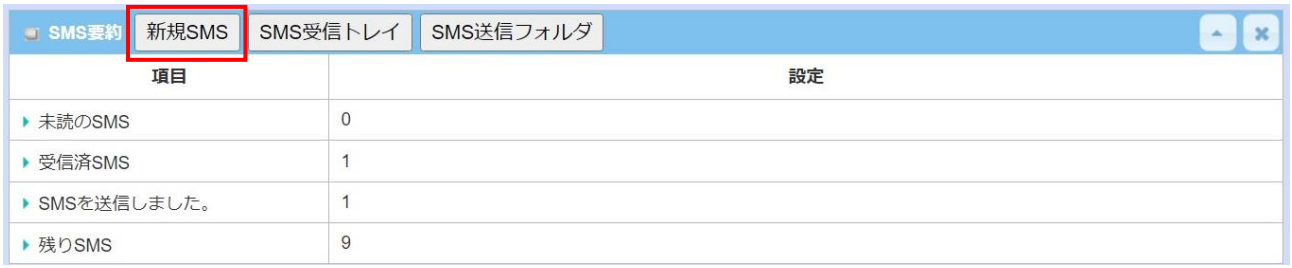
「未読の SMS」、「受信済 SMS」、「残り SMS」を表示し、送信する SMS 本文を編集し、SIM カードから SIM を読み取ります。



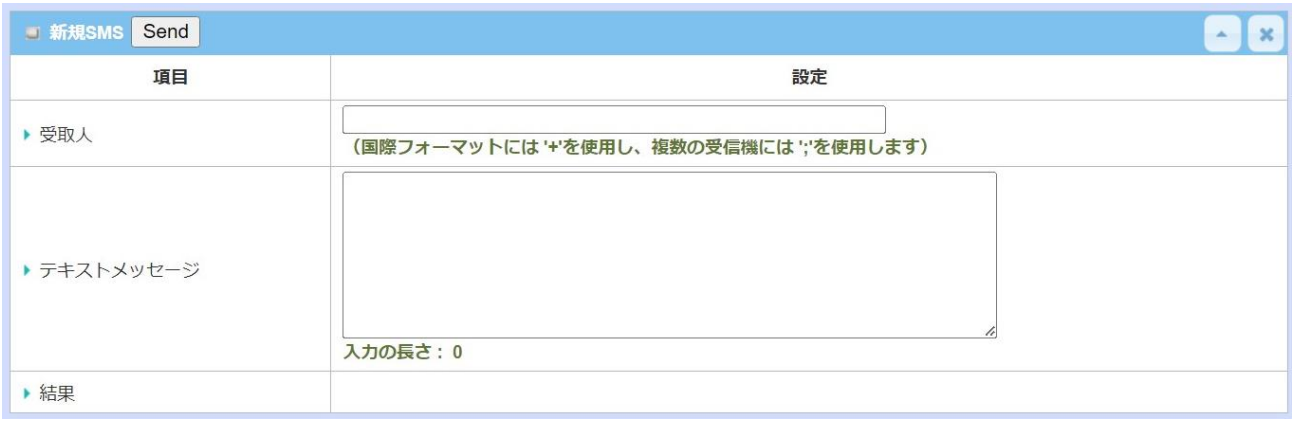
SMS要約		
項目	設定値	説明
未読の SMS	該当なし	初めて SIM カードをルーターに挿入すると、未読の SMS 値はゼロになります。 新しい SMS を受信し、読まなかった場合は、この値に 1 が加わります。
受信済 SMS	該当なし	この値は、SIM カードからの既存の SMS 数を記録します。 新しい SMS を受信すると、この値に 1 を加えた値になります。
SMS を 送信しました	該当なし	この値は発信 SMS の数を記録します。 1 つの SMS を送信する場合、この値に 1 を加えた値です。
残り SMS	該当なし	この値は SMS 容量から受信済 SMS を差し引いたものです。 新しい SMS を受信すると、この値から 1 が減算されます。
新規 SMS	該当なし	[新規 SMS]ボタンをクリックすると、新規 SMS 画面を表示します。 この画面から SMS の設定を行うことができます。 次のページの新規 SMS を参照してください。
SMS 受信トレイ	該当なし	[SMS 受信トレイ]ボタンをクリックすると、SMS 受信トレイリスト画面を表示します。 この画面から SMS を読む、削除、返信、転送ができます。 次のページの SMS 受信トレイリストを参照してください。
更新	該当なし	[更新]ボタンをクリックして、直ちに SMS summary（SMS 要約）を更新します。

新規 SMS

[新規SMS]ボタンが適用されると、「新規SMS」画面が表示されます。



この画面から SMSの設定を行うことができます。



新規SMS		
項目	設定値	説明
受取人	該当なし	SMS を送信する受信者を記述します。セミコロンを追加し、SMS をグループ化できる複数の受信者を作成する必要があります。
テキストメッセージ	該当なし	SMS を送信する SMS 本文を作成します。 ルーターは、SMS 本文の長さに対して最大 1023 文字をサポートします。
Send（送信）	該当なし	[Send]ボタンをクリックすると、上記テキストメッセージが SMS として送信されます。
結果	該当なし	SMS が正常に送信された場合は、Send OK（送信 OK）と表示されます。 それ以外の場合は、Send Failed（送信失敗）が表示されます。

SMS 受信トレイリスト

[SMS受信トレイ]ボタンが適用されると、「SMS受信トレイリスト」画面が表示されます。

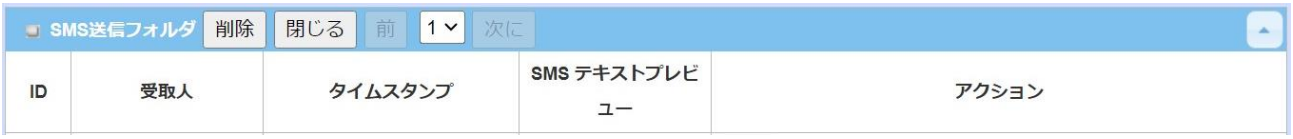
この画面から SMS を読む、削除、返信、転送ができます。

SMS受信トレイリスト		
項目	設定値	説明
ID	該当なし	番号または SMS です。
電話番号から	該当なし	SMS の発信者の電話番号です。
タイムスタンプ	該当なし	SMS を受信した時刻です。
SMS テキスト プレビュー	該当なし	SMS 本文をプレビューします。 [詳細]ボタンをクリックすると、特定のメッセージを読むことができます。
アクション	デフォルトは、チェックなしです	[詳細]ボタンをクリッして、SMS の詳細を読みます。 [Reply]（返信）/[フォワード]（転送）ボタンをクリックして、SMS に返信/転送します。 また、ボックスにチェックを入れ、[削除]ボタンをクリックすると、チェックされている SMS が削除されます。
更新	該当なし	「SMS 受信トレイリスト」を更新します。
削除	該当なし	「アクション」項目のチェックが入っている SMS を対象に削除します。
閉じる	該当なし	「SMS 受信トレイリスト」画面を閉じます。

SMS 送信フォルダ

[SMS送信フォルダ]ボタンが適用されると、「SMS送信フォルダ」画面が表示されます。

この画面から SMS を読んだり、削除したりすることができます。



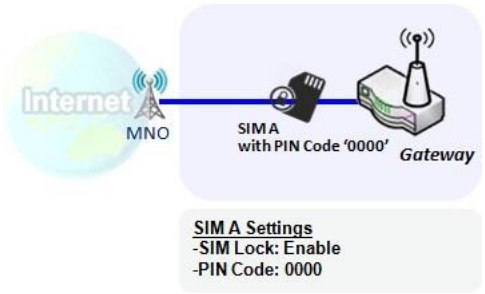
SMS送信トレイリスト		
項目	設定値	説明
ID	該当なし	番号または SMS です。
受取人	該当なし	送信された SMS の受信者リストです。
タイムスタンプ	該当なし	SMS を送信した時刻です。
SMS テキスト プレビュー	該当なし	SMS 本文をプレビューします。 [詳細]ボタンをクリックすると、特定のメッセージを読むことができます。
アクション	デフォルトは、 チェックなしです	[詳細]ボタンをクリッして、SMS の詳細を読みます。 また、ボックスにチェックを入れ、[削除]ボタンをクリックすると、チェックされている SMS が削除されます。
更新	該当なし	[SMS 送信トレイリスト]を更新します。
削除	該当なし	「アクション」項目のチェックが入っている SMS を対象に削除します。
閉じる	該当なし	「SMS 送信フォルダ」画面を閉じます。

7-1-3. SIM PIN

世界中でほとんどの場合、音声サービスまたはデータサーフィンのためにセルラーネットワークを 利用するには、エンドデバイスに SIM カード（つまり、UICC）を挿入する必要があります。 SIM カードは、通常、移動体通信事業者またはサービスプロバイダにより リリースされます。 各 SIM カードは、ネットワーク所有者またはサービスプロバイダが各加入者を識別するための固有の番号（いわゆる ICCID）を有します。SIM カードは、サービスプロバイダと加入者の間で重要な役割を果たすため、不正なアクセスを防ぐために SIM カードにはいくつかのセキュリティメカニズムが 必要です。

SIM カードで PIN コードを有効にすると、不正なアクセスからセルラーデバイスを簡単かつ効果的に保護することができます。本ゲートウェイデバイスを使用すると、Web GUI を通じて SIM カード上の PIN コードを有効かつ管理することができます。

SIM カード上の PIN コードの有効



本ゲートウェイデバイスでは、SIM カード上の PIN コードを 有効することができます。この例では、デフォルトの PIN コード「0000」を使って、3G-4G-1 の SIM-A で PIN コードを有効する方法を示します。

SIM カード上の PIN コードの変更

本ゲートウェイデバイスでは、SIM カード上の PIN コードを 変更することができます。上の例では、新しい PIN コードを「1234」に設定する場合は、 元の PIN コード「0000」を入力し、「1234」の新しい PIN コードを入力する必要があります。 入力した新しい PIN コードが正しいかどうかを確認するには、Verified New PIN Code（新しい PIN コードの検証）にもう一度 PIN コード 「1234」を入力する必要があります。

PUK コードによる SIM カードのロック解除

モバイル NET-1 WAN 設定ページで誤った PIN コードを 3 回以上 入力すると、SIM カードが PUK コードによりロックされます。その後、SIM カードのロックを解除する PUK コードを取得するには、サービス番号に電話する必要があります。この図では、PUK コードは「12345678」であり、新しい PIN コードは「5678」です。

SIM PIN 設定

サービス > ［セルラーツールキット］ > ［SMS PIN］タブに進みます。

SIM PIN 機能ウィンドウでは、SIM ロック（PIN コードで保護されていること）を有効または無効にするか、PIN コードを変更することができます。 また、前述したように、失敗試行の残り回数の情報を確認することもできます。これらの失敗試行を使い果たした場合は、SIM カードのロックを解除する PUK コードを取得する必要があります。

SIMカードの選択

構成		
項目	**設定値**	**説明**
物理 インターフェイス	デフォルトは、「モバイル NET-1」です	選択した SIM カードの SIM PIN 設定を変更するには、セルラーインターフェイス（モバイル NET-1 またはモバイル NET-2）を選択します。 注：モバイル NET-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM ステータス	該当なし	選択された SIM カードおよび SIM カードステータスの表示。 ステータスは、「準備完了」、「未挿入」、または「SIM PIN」です。 ・Ready（準備完了） -- SIM カードが挿入され、使用準備ができています。 PIN 保護のない SIM カードでも、SIM カードが正しい PIN コ

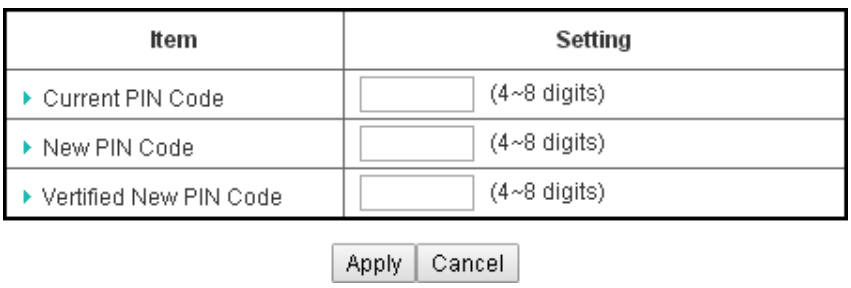
		ードでロック解除されていてもかまいません。 ・ Not Insert（未挿入） -- SIM スロットには SIM カードが挿入されていません。 ・SIM PIN -- SIM カードは PIN コードで保護されていますが、正しい PIN コードではまだロックされていません。この SIM カードはまだロックされた状態です。
SIM 選択	該当なし	SIM PIN をさらに構成するために、SIM カードを選択します。 ［切り替え］ボタンを押すと、ゲートウェイは、SIM カードを別のものに切り替えます。その後、SIM カードを構成することができます。

PINコードの有効/変更

PIN コード（パスワード）機能を有効/無効にし、PIN コード機能を変更します。

構成		
項目	設定値	説明
PIN ロック	SIM カードに依存します	有効チェックボタンにチェックを入れて、SIM ロック機能を有効します。初めて SIM ロック機能を有効する場合は、PIN コードも入力し、［保存］ボタンをクリックして、設定を適用します。
残り回数	SIM カードに依存します	SIM PIN ロック解除の残りの試行回数を表します。
保存	該当なし	［保存］ボタンをクリックして、設定を適用します。
PIN コードの変更	該当なし	［PIN コードの変更］ボタンをクリックして、PIN コード（パスワード）を変更します。 SIM ロック機能が有効になっていない場合、［PIN コードの変更］ボタンは無効になります。この場合、PIN コードを変更したい場合は、まず SIM ロック機能を有効して PIN コードを入力し、［保存］ボタンをクリックして、有効する必要があります。その後、［PIN コードの変更］ボタンをクリックして、PIN コードを変更することができます。

［PIN コードの変更］ボタンをクリックすると、以下の画面が表示されます。

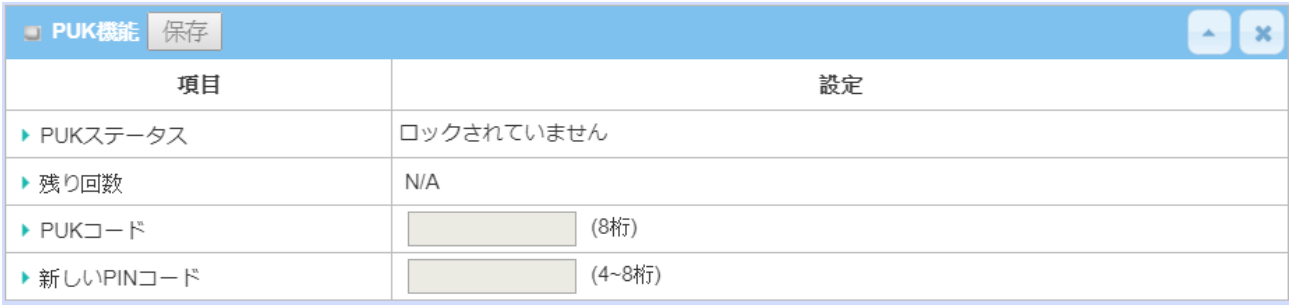


項目	設定値	説明
Current PIN Code（現在の PIN コード）	入力必須	SIM カードの現在の（古い）PIN コードを入力します。
New PIN Code（新しい PIN コード）	入力必須	変更したい新しい PIN コードを入力します。
Verified New PIN Code（新しい PIN コードの確認）	入力必須	再度、新しい PIN コードを確認します。
Apply（適用）	該当なし	［Apply］（適用）ボタンをクリックして、指定した新しい PIN コードを使って、PIN コードを変更します。
Cancel（キャンセル）	該当なし	変更をキャンセルして、現在の PIN コードを保存するには、［Cancel］（キャンセル）ボタンをクリックします。

注： 特定の SIM カードの PIN コードを変更した場合は、［基本ネットワーク］＞ WAN & アップリンク ＞ 接続設定 ＞ 「SIM カードとの接続」ページで、指定した対応する PIN コードも変更する必要があります。
そうしないと、無効な（古い） PIN コードを使って、間違った SIM PIN 試行が行われる可能性があります。

PUKコードを用いるロック解除

PUK 機能ウィンドウは、その SIM カードが PUK コードでロックされている場合にのみ利用可能です。SIM カードがロックされており、ロックを解除するには追加の PUK コードが必要です。通常、間違った PIN コードの試行が多すぎると、SIM 機能テーブルの残り回数が 0 になります。この場合、サービスプロバイダに連絡して SIM カード用の PUK コードを申請し、提供された PUK コードで ロックされた SIM カードの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。



PUK機能		
項目	設定値	説明
PUK ステータス	PUK Unlock（PUK ロック解除） / PUK	PUK ステータスの表示します。 ステータスは、PUK Lock（PUK ロック）または PUK Unlock（PUK ロック解除）になります。前述のように、SIM カードは、失敗 PIN コ

	Lock（PUK ロック）	ードの試行回数が多すぎると、PUK コードによってロックされます。 この場合、PUK Status（PUK ステータス）は、PUK Lock（PUK ロック）に変わります。通常の状況では、PUK Unlock（PUK ロック解除）表示されます。
残り回数	SIM カードに依存します	PUK ロック解除の残りの試行回数を表します。 注： 残り回数を 0 にしないでください。これは、SIM カードを永久的に損傷します。PUK コードがない場合は、ISP のヘルプに電話をかけ、正しい PUK を取得し、SIM ロックを解除してください。
PUK コード	入力必須	UK ロック解除状態にある SIM カードのロックを解除できる PUK コード（8 桁）を入力します。
新しい PIN コード	入力必須	SIM カードの新しい PIN コード（4～8 桁）を入力します。 忘れてしまった古い PIN コードを置き換えるには、新しい PIN コードを決定する必要があります。PIN コード（パスワード）は慎重に保管してください。
保存	該当なし	［保存］ボタンをクリックして、設定を適用します。

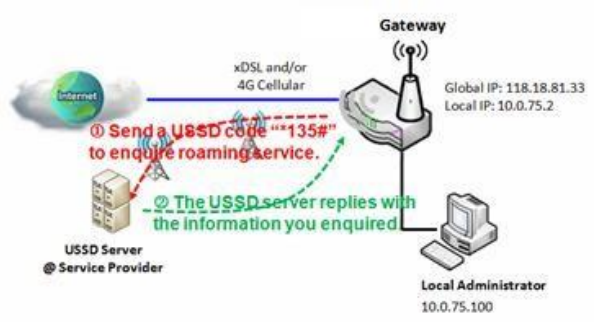
注：特定の SIM カードの PUK コードおよび PIN コードを変更した場合は、[基本ネットワーク] ＞ WAN &アップリンク ＞ 接続設定 ＞「SIM カードとの接続」ページで、指定した対応する PIN コードも変更する必要があります。
そうしないと、無効な（古い）PIN コードを使って、間違った SIM PIN 試行が行われる可能性があります。

7-1-4. USSD

非構造付加サービスデータ（USSD）は、GSMセルラー電話がサービスプロバイダのコンピュータと通信するためのプロトコルです。USSDは、WAPブラウジング、プリペイドコールバックサービス、モバイルマネーサービス、位置ベースのコンテンツサービス、メニューベースの情報サービスで使用され、またネットワーク上での電話の構成にも使用されます。

USSDメッセージの長さは、英数字で最大182文字です。ショートメッセージサービス（SMS）メッセージとは異なり、USSDメッセージは、USSDセッション中にリアルタイム接続を作成します。接続は開いたままで、一連のデータの双方向交換が可能です。これにより、USSDは、SMSを使用するサービスよりも応答性が良くなります。

USSD のシナリオ



USSD では、キャリア/ISP との即時双方向通信を行うことができます。図において、USSD コマンド「* 135#」は、データローミングサービスと呼ばれます。その USSD コマンドを通信事業者に送信した後、USSD Response（USSD 応答）ウィンドウで応答を取得することができます。USSD コマンドは、キャリア/ ISP によって異なることに注意してください。

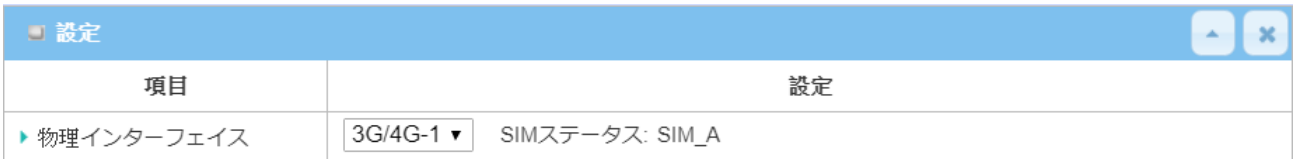
USSD 設定

サービス > **［セルラーツールキット］** > **［USSD］タブ**に進みます。

「USSD」ページには、USSD機能用の4つのウィンドウがあります。
「設定」ウィンドウで、USSD機能に使用される3G/4Gモジュール（物理インターフェイ

ス）を指定することができます。システムは、モジュールで現在どのSIMカードが使用されているかを表示します。
2番目のウィンドウは「USSDプロファイルリスト」です。これは、USSDセッションをアクティブ化するためのプリコマンドを保存している、定義済みのすべてのUSSDプロファイルを表示します。ウィンドウ内の［追加］ボタンを使用すると、新しいUSSDプロファイルを1つ追加し、3番目のウィンドウでプロファイルのコマンド「USSDプロファイル構成」を定義することができます。USSDサーバーに対するUSSD接続セッションのアクティベーションを開始する場合は、USSDプロファイルを選択するか、適切な事前コマンドを入力して、セッションの［送信］ボタンをクリックします。
USSDサーバーからの応答は、「USSD Command（USSDコマンド）」行の下に表示されます。「USSD Command（USSDコマンド）」フィールドに入力されたコマンドが送信されると、受信した応答が「USSD Response（USSD応答）」の空白スペースに表示されます。
ユーザーは、USSDコマンドを送信し、USSD応答をゲートウェイ経由で取得することにより、USSDサーバーと通信することができます。

USSD 設定

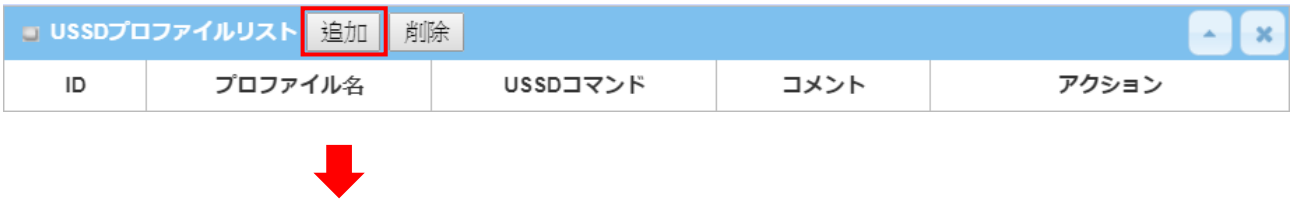


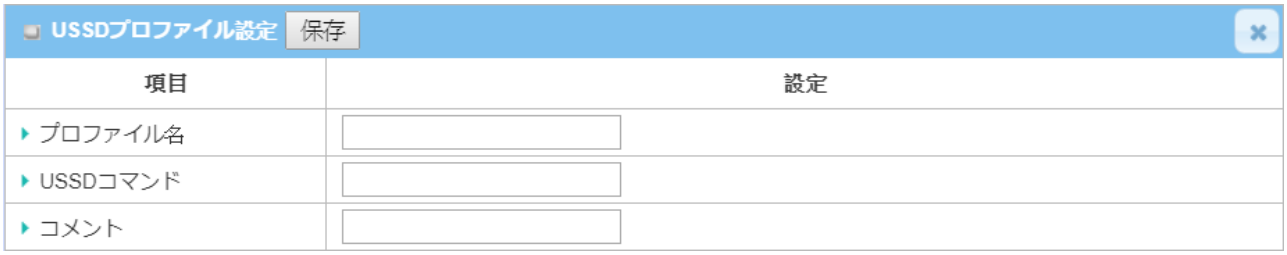
設定		
項目	設定値	説明
物理インターフェイス	デフォルトは、3G/4G-1 です	接続されたセルラーサービス（SIM_A または SIM_B で識別される）の USSD 設定を構成するには、セルラーインターフェイス（3G/4G-1 または 3G/4G-2）を選択します。 注：3G/4G-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM ステータス	該当なし	接続されたセルラーサービス（SIM_A または SIM_B で識別される）を表示します。

USSD プロファイルの作成/編集

セルラーゲートウェイを使用すると、USSDプロファイルをカスタム設定することができます。
これは、最大35のUSSDプロファイルをサポートします。

［追加］ボタンが適用されると、「USSDプロファイルリスト」画面を表示します。





設定		
項目	設定値	説明
プロファイル名	該当なし	USSD プロファイルの名称を入力します。
USSD コマンド	該当なし	プロファイル用に定義された USSD コマンドを入力します。 通常、数字キーパッド「0～9」、「*」、「#」で構成されるコマンド文字列です。USSD コマンドは、セルラーサービスと非常に関連しています。詳細については、サービスプロバイダに確認してください。
コメント	該当なし	プロファイルの簡単なコメントを入力します。

USSD 要求の送信

USSDコマンドを送信すると、USSD Response（USSD応答）画面が表示されます。
Clear（クリア）ボタンをクリックすると、USSD Respons（USSD応答）が消えます。

設定		
項目	設定値	説明
USSD プロファイル	該当なし	ドロップダウンリストから USSD プロファイル名を選択します。
USSD コマンド	該当なし	選択したプロファイルの USSD コマンド文字列が、ここに表示されます。
USSD 応答	該当なし	［送信］ボタンをクリックすると、USSD コマンドが送信されと、USSD Response（USSD 応答）画面が表示されます。対応するサービスの応答メッセージが表示され、サービス SMS が受信されます。

7-1-5. 通信スキャン

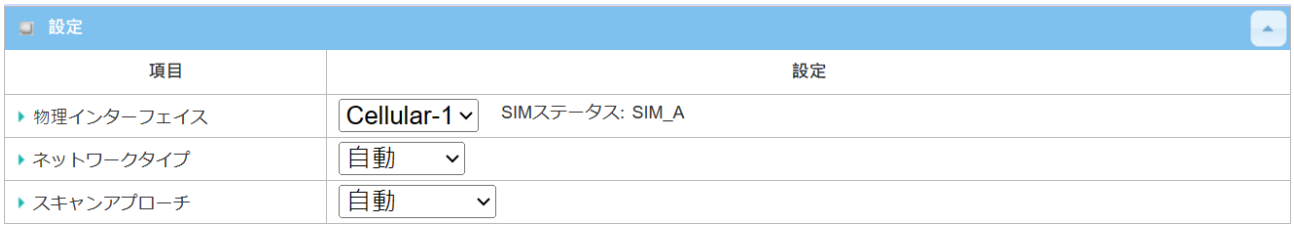
「通信スキャン」機能により、管理者は、各3G/4Gインターフェイスにおけるデータ通信のために、モバイルシステムに接続する方法をデバイスに指定することができます。例えば、管理者は、接続、3G、または、LTEに使用されるモバイルシステムの世代を指定することができます。
さらに、ゲートウェイデバイスが、モバイルシステムに自動的に接続するための接続シーケンスを定義することができます。また、管理者は、手動でモバイルシステムをスキャンし、対象となる操作システムを選択して、適用することができます。手動スキャンアプローチは、問題診断に使用されます。

ネットワークスキャン

サービス > **［セルラーツールキット］** > **［通信スキャン］タブ**に進みます。

「ネットワークスキャン」ページには、ネットワークスキャン機能用のウィンドウがあります。
「設定」ウィンドウで、ネットワークスキャンを実行するために使用する3G/4Gモジュール（物理インターフェイス）を選択することができます。システムは、現在モジュールで使用されているSIMカードを表示します。ネットワークスキャンを順次実行することにより、各3G/4G WANインターフェイスを設定することができます。対象とするモバイルシステムの世代（3G/LTE）の接続シーケンスを指定することもできます。

通信スキャン構成



設定		
項目	**設定値**	**説明**
物理インターフェイス	デフォルトは、「Cellular-1」です	通信スキャン機能のセルラーインターフェイス（Cellular-1 または Cellular-2）を選択します。 注：Cellular-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM ステータス	該当なし	接続されたセルラーサービス（SIM_A または SIM_B で識別される）を表示します。
ネットワークタイプ	デフォルトは、「自動」です	通信スキャン機能のネットワークタイプを指定します。これは、自動、Cat.M1、NB-IoT です。 ・「自動」を選択すると、ネットワークは、自動的に登録されます。 ・「優先」が選択されている場合は、まず、ネットワークが登録されます。

		・「のみ」が選択されている場合は、選択したネットワークのみが登録されます。
スキャン アプローチ	デフォルトは、 「自動」です	・「自動」を選択すると、セルラーモジュールが自動的に登録されます。 ・「手動」を選択すると、ネットワークプロバイダリスト画面を表示します。 ［Scan］ボタンを押すと、最も近い基地局をスキャンします。優先基地局を選択し（ボックスにチェックを入れて）、［Apply］ボタンをクリックして、設定を適用します。
保存	該当なし	［保存］ボタンをクリックして、設定を保存します

2番目のウィンドウは「ネットワークプロバイダリスト」ウィンドウです。
これは、設定ウィンドウの「スキャンアプローチ」で「手動」が選択されているときに表示されます。
［Scan］ボタンをクリックして1～3分待つと、検出されたモバイルオペレータシステムが表示されます。
［Apply］ボタンをもう一度クリックすると、専用の3G/4Gインターフェイス用のモバイルオペレータシステムに接続するためのシステムが起動します。

7-2. イベント処理

イベント処理とは、管理者が個々のプロファイルで事前定義されたイベント、ハンドラ、または、応答の動作を設定できるようにするアプリケーションです。イベント処理機能を適切に設定することで、管理者は、購入したゲートウェイ経由で簡単にステータスと情報を取得することができます。
サポートされるイベントは、管理イベントと通知イベントの2つのグループに分類されます。管理イベントとは、ゲートウェイを管理するため、または、ゲートウェイ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。管理イベントを受信すると、ゲートウェイは機能を変更し、管理に必要なステータスを同時に収集します。
通知イベントとは、いくつかの関連オブジェクトがトリガーされたイベントであり、イベントの発生時に対応するアクションを実行します。
これは、SMSメッセージ、電子メール、SNMPトラップなどで起こったことを管理者に警告するイベントです。
構成を容易にするために、管理者は、特定のイベントに即座に反応したり、高度に有用な目的でデバイスを管理したりするために、一般的な定義済みの管理/ 通知イベントプロファイルを作成および編集することができます。例えば、ゲートウェイのルーチンをメンテナンスするためにリモート管理SMS を送受信するなどです。このような管理および通知機能はすべて、イベント処理機能によって効果的に実現することができます。

提供されたプロファイルとイベントの要約リストは次のとおりです：

- プロファイル（ルール):
  - SMS の構成およびアカウント
  - Eメールアカウント
- 管理イベント：
  - トリガータイプ：SMS、SNMPトラップ
  - アクション：ネットワークステータスを取得する。 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、管理を構成する。
- 通知イベント：
  - トリガータイプ：接続変更（WAN、LANおよび VLAN、DDNS)、管理、および、データの使用。
  - アクション：SMS、Syslog、SNMPトラップ、または、Eメールアラートを使って管理者に通知します。

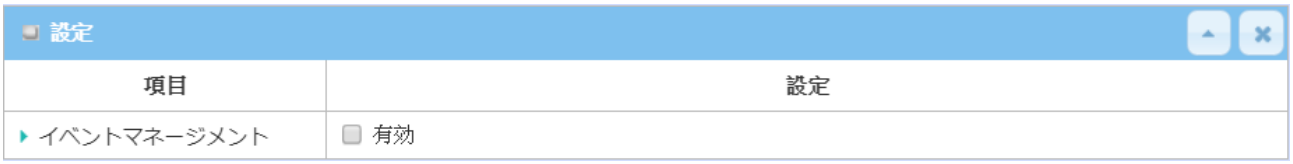
イベント処理機能を使用するには、まず、イベント管理設定を有効にして、提供されるプロファイル設定でイベントの詳細を構成する必要があります。個別の管理/通知イベント用に事前定義されたプロファイルを作成または編集することができます。プロファイル設定はいくつかの項目に分かれています。
つまり、SMSアカウント定義、電子メールサービス定義です。次に、各管理/通知イベントを、イベントのトリガー条件、および、イベントの対応するアクション（イベントに対する反応）を識別するように構成する必要があります。各イベントについて、複数のアクションを同時に有効することができます。

7-2-1. 構成

サービス > **［SMS&イベント］** > **［設定］タブ**に進みます。

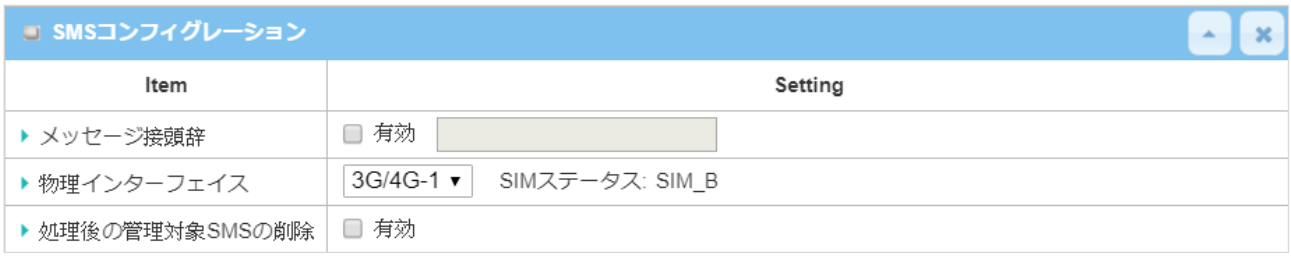
イベント処理とは、管理者が個々のプロファイルで事前定義されたイベント、ハンドラ、または、応答の動作を設定できるようにするサービスです。

イベント管理の有効



項目	設定値	説明
イベント マネージメント	デフォルトは、 チェックなしです	有効ボックスにチェックを入れ、本機能を有効します。

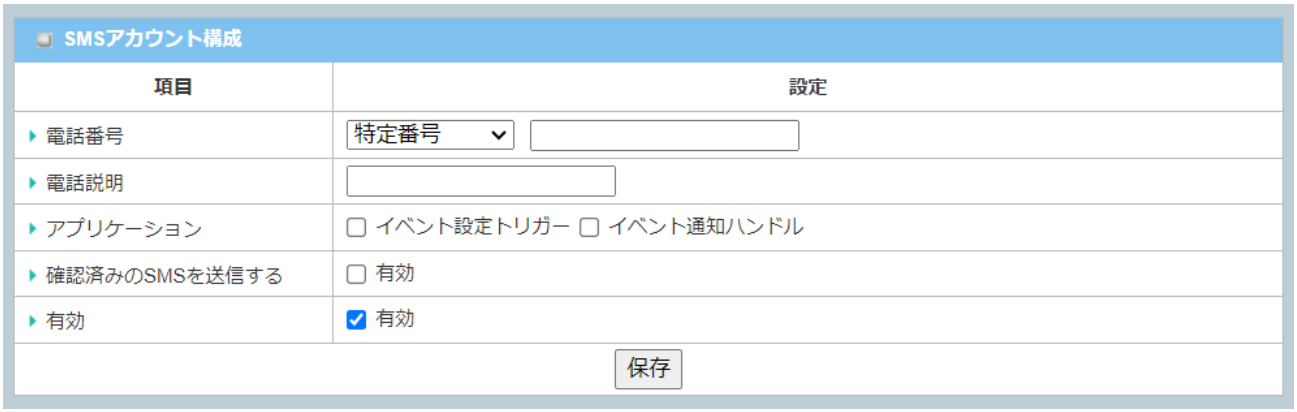
SMS 管理の有効



SMS構成		
項目	**設定値**	**説明**
メッセージ プレフィックス	デフォルトは、 チェックなしです	有効ボックスにチェック入れて、受信した SMS を検証するための SMS プレフィックスを有効します。 この機能を有効した後、チェックボックスの後にプレフィックスを入力する必要があります。受信した管理イベント SMS は、指定されたプレフィックスを初期識別子として持つ必要があり、対応するハンドラは、その後の処理に有効になります。
物理 インターフェイス	デフォルトは、 「Cellular-1」です	SMS 管理設定を構成するには、セルラーインターフェイス（Cellular-1、または Cellular-2）を選択します。 注： Cellular-2 は、デュアルセルラーモジュールを搭載した製品でのみ使用できます。
SIM ステータス	該当なし	接続されたセルラーサービス（SIM_A または SIM_B で識別される）を表示します。
処理後の管理対象 SMS の削除	デフォルトは、 チェックなしです	有効ボックスにチェックと入れ、受信した管理イベント SMS を処理された後に削除します。

SMS アカウントの作成/編集

SMSを介してゲートウェイを管理するために、SMSアカウントを設定します。
これは、最大5アカウントをサポートします。
［追加］ボタンをクリックして、SMSアカウントを構成することができます。



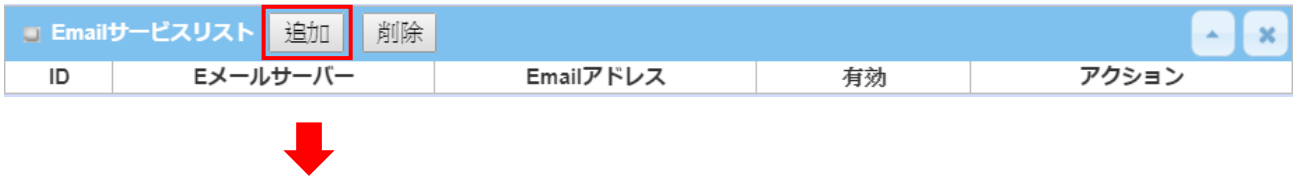
SMSアカウント構成		
項目	設定値	説明
電話番号	1. 携帯電話番号形式です 2. 入力必須	SMS アカウント識別子として携帯電話番号を指定します。 値の範囲：-1～32 桁
電話説明	1. 任意のテキスト 2. 任意の設定	SMS アカウントの簡単な説明を入力します。
アプリケーション	入力必須	アプリケーションタイプを指定します。 「イベント設定トリガー」、「イベント通知ハンドル」、または、両方を選択することが可能です。
確認済みの SMS を送信する	1. 任意の設定 2. デフォルトは、チェックなしです	SMS 応答機能を有効にするには、有効ボックスにチェックを入れます。 ゲートウェイは、SMS 管理イベントを受信するたびに、確認されたメッセージを送信者に送り返します。 確認されたメッセージは、「デバイスがコマンド xxxxx で SMS を受信しました」のような形式です。
有効	デフォルトは、チェックなしです	有効ボックスにチェック入れて、このアカウントを有効にします。
保存	該当なし	[保存]をクリックして、構成を保存します。

Eメールサービスアカウントの作成/編集

イベント通知のEメールサービスアカウントを設定します。

これは、最大5アカウントをサポートします。

［追加］ボタンをクリックして、Eメールアカウントを構成することができます。

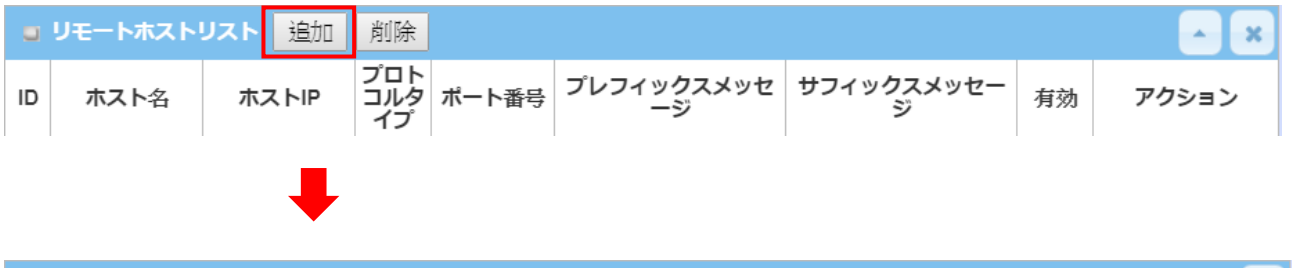


Eメールサービス構成		
項目	設定値	説明
E メールサーバー	デフォルトは、 「Option」です	E メールアカウント設定の「外部サーバー」設定から、 「E メールサーバー」プロファイルを選択します。
Email アドレス	1. インターネット E メールアドレス形式です 2. 入力必須	宛先 E メールアドレスを指定します。
有効	デフォルトは、 チェックなしです	有効ボックスにチェック入れて、このアカウントを有効にします。
保存	該当なし	[保存]をクリックして、設定を保存します。

リモートホストプロファイルの作成/編集

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

［追加］ボタンをクリックして、プロファイルを構成することができます。



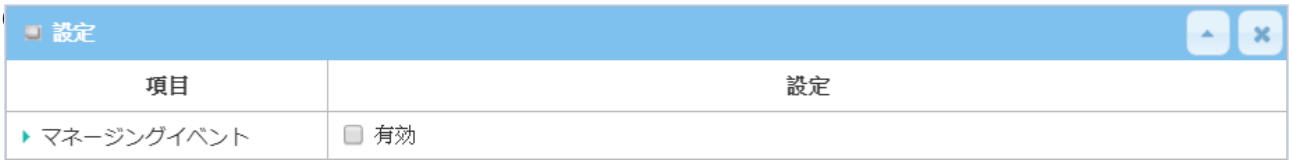
リモートホスト構成		
項目	**設定値**	**説明**
ホスト名	1. 文字列形式 2. 入力必須	ホスト名を指定します。 値の範囲：1～64 文字
ホスト IP	1. 入力必須 2. IP Address format.	リモートホストの場合は、IP を指定します。 IPv4 形式です。
プロトコルタイプ	1. 入力必須 2. デフォルトは「TCP」です	リモートホストの場合は、プロトコルを指定します。 「TCP」、または「UDP」形式です。
ポート番号	入力必須	リモートホストにアクセスするためのポート番号を指定します。 値の範囲：1～65535
プレフィックスメッセージ	1. 文字列形式 2. 任意の設定	プレフィックスメッセージ文字列を、リモートホストにアクセスするための事前定義された ID として指定します。 値の範囲：1～64 文字
サフィックスメッセージ	1. 文字列形式 2. 任意の設定	サフィックスメッセージ文字列を、リモートホストにアクセスするための事前定義された ID として指定します。 値の範囲：1～64 文字
有効	デフォルトは、チェックなしです	有効ボックスをクリックして、このプロファイル設定を有効します。
保存	該当なし	[保存]をクリックして、構成を保存します。

7-2-2. 管理イベント

サービス > ［SMS&イベント］> ［マネージングイベント］タブに進みます。

管理イベントにより、管理者は、イベントトリガー、ハンドラ、および、応答の間の関係（ルール）を定義することができます。

管理イベントの有効



項目	設定値	説明
マネージング イベント	デフォルトは、チェックなしです	有効ボックスにチェックを入れ、管理イベント機能を有効にします。

管理イベントルールの作成/編集

管理イベントルールの設定は、最大 128 ルールをサポートします。
[追加]ボタンが適用されると、[管理イベント構成]画面が表示されます。

管理イベント構成		
項目	設定値	説明
イベント	デフォルトは、SMS（または SNMP Trap）です	イベントタイプ（SMS、SNMP トラップ）およびイベント識別子/プロファイルを指定します。 ・**SMS**：SMS を選択し、テキストボックスのメッセージをイベントのトリガー条件として入力します。 ・**SNMP Trap**：SNMP Trap を選択し、テキストボックスにメッセージを入力して、SNMP トラップイベントを指定します。 注：利用可能なイベントタイプは、購入した製品によって異なる場合があります。
トリガタイプ	デフォルトは、「期間」です	イベントトリガーのタイプを間隔または 1 回のいずれかで指定します。 ・**期間**：期間を選択して時間間隔を指定すると、指定されたイベント条件が成立するたびに、その期間ごとにイベントが繰り返しトリガーされます。 ・**一回**：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	デフォルトは、「0」です	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：0～86400 秒。
説明	文字列形式：任意のテキスト	管理イベントの簡単な説明を入力します。
アクション	デフォルトは、チェックなしです	Network Status（ネットワークステータス）、または、予想されるイベントが発生したときに行う少なくとも 1 つの休止アクションを指定します。 ・**Network Status**（ネットワークステータス）：ネットワークステータスをイベントのアクションとして取得するには、Network Status（ネットワークステータス）チェックボックスを選択します。 ・**LAN&VLAN**：LAN&VLAN チェックボックスと関心のあるサブ項目（ポートリンクのオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。 ・**NAT**：NAT チェックボックスと関心のあるサブ項目（仮想サーバールー ルのオン/オフ、DMZ オン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。 ・**ファイヤーウォール**：ファイヤーウォールチェックボックスと関心のあるサブ項目（リモート管理者ホスト ID のオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。 ・**VPN**：VPN チェックボックスと関心のあるサブ項目（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）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。 ・**GRE**：GRE チェックボックスと関心のあるサブ項目（GRE トンネルのオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。 ・**System Manage**（システム管理）： System Manage チェックボックスと関心のあるサブ項目（WAN SSH サービスオン/オフ）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。

		・管理（Administration）：管理チェックボックスと関心にあるサブ項目（バックアップ構成、復元構成、再起動、デフォルトとして現在の設定を保存）を選択すると、ゲートウェイは、イベントのアクションとして設定を変更します。 **・リモートホスト**：リモートホストチェックボックスと、イベントのアクションとして定義したリモートホストプロ ファイルを選択します。 ※VPN（OpenVPN・PPTP・GRE）は、本製品では対応しておりません。 注：利用可能なイベントタイプは、購入した製品によって異なる場合があります。
管理イベント	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、管理イベント設定を有効にします。
保存	該当なし	[保存]をクリックして、構成を保存します。

7-2-3. 通知イベント

サービス > **[SMS&イベント]** > **[通知イベント] タブ**に進みます。

通知イベント設定により、管理者は、イベントトリガーとハンドラ間の関係（ルール）を定義することができます。

通知イベントの有効

項目	設定値	説明
通知イベント	デフォルトは、チェックなしです	有効ボックスにチェックを入れて、通知イベント機能を有効にします。

通知イベントルールの作成/編集

通知イベントルールを設定します。これは、最大 128ルールをサポートします。
[追加]ボタンが適用されると、[通知イベント設定]画面が表示されます。

通知イベント構成		
項目	設定値	説明
イベント	デフォルトは、「デジタル入力」または、「WAN」です	イベントタイプと対応するイベント設定を指定します。 サポートされているイベントタイプは次のとおりです ・**WAN**：特定の WAN イベントを指定するには、WAN とトリガー条件を選択 します。 ・**LAN&VLAN**：特定の LAN および LAN イベントを指定 するには、LAN＆VLAN（LAN および VLAN）とトリガー条件を選択します。 ・**管理**：特定の管理イベントを指定するには、Administration（管理）とトリガー条件を選択します。 ・**データ使用量**：特定のデータ使用状況イベントを指定するには、データ使用量、SIM Card（Cellular Service)、およびトリガー条件を選択します。 ※DDNS は、本製品では対応しておりません。 注： 利用可能なイベントタイプは、購入した製品によって異なる場合があります
説明	文字列形式：任意のテキスト	通知イベントの簡単な説明を入力します。
アクション	デフォルトは、チェックなしです	想定される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想定される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**：SMS を選択すると、ゲートウェイは、イベントのアクションとして定義されたすべての 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、Enable Checkbox（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**： SNMP トラップを選択すると、ゲートウェイは、イベントのアクションとして定義された SNMP イベント受信者に SNMP トラップを送信します。 ・**E メールアラート**： E メールアラートを選択すると、ゲートウェイは、イベントのアクションとして定義されたすべての 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**：リモートホストチェックボックスと、イベントのアクションとして定義したリモートホストプロファイルを選択します。 注：利用可能なイベントタイプは、購入した製品によって異なる場合があります。
時間スケジュール	デフォルトは、「0」です	通知イベントの時間スケジューリングルールを選択します。
通知イベント	デフォルトは、チェックなしです	有効ボックスをクリックして、通知イベント設定を有効にします。
保存	該当なし	[保存]をクリックして、構成を保存します。

7-3. 位置追跡【未対応】

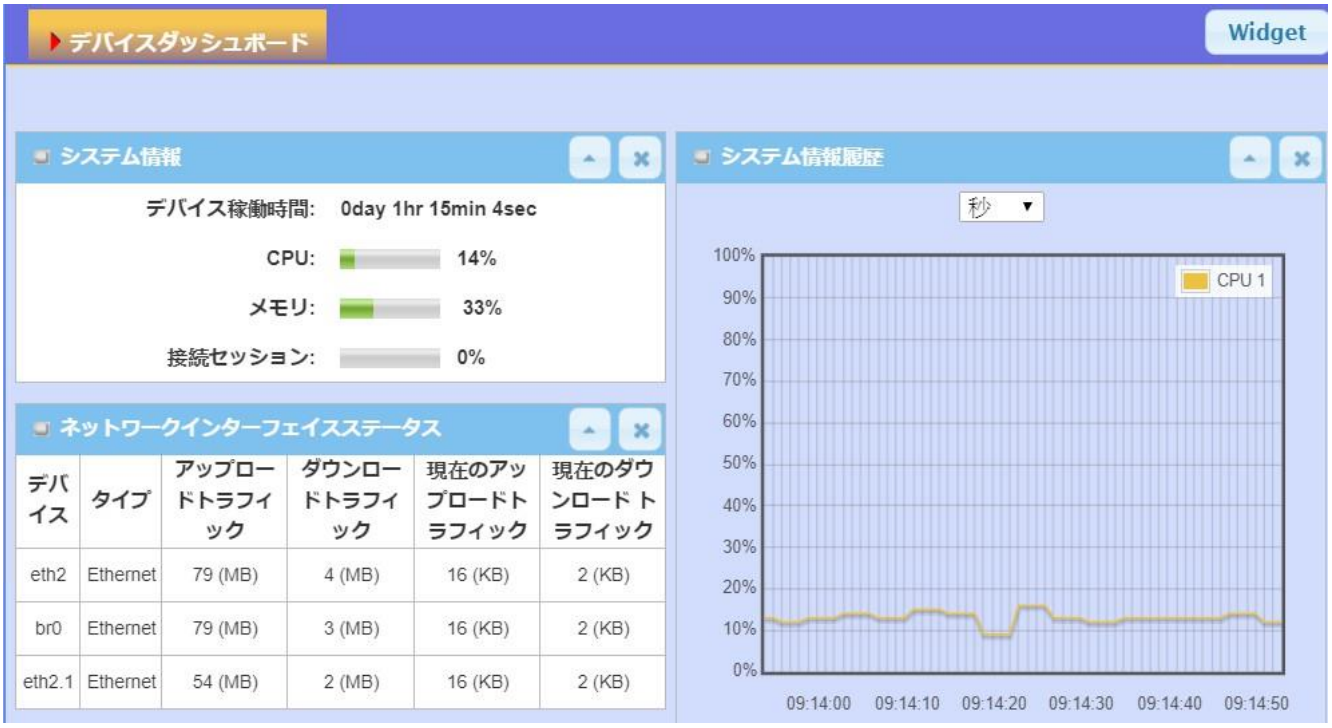
本製品ではサポートされていない機能です。

7-3-1. GNSS 【未対応】

本製品ではサポートされていない機能です。

第8章. ステータス

8-1. ダッシュボード



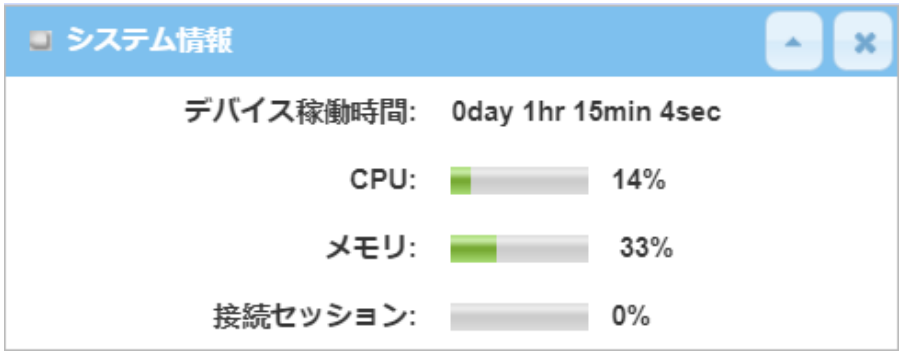
8-1-1. デバイスダッシュボード

［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ステータスが表示されます。これらは、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です。表示は1秒ごとに更新されます。

左側のメニューから、
ステータス > **［ダッシュボード］** > **［デバイスダッシュボード］タブ**を選択します。

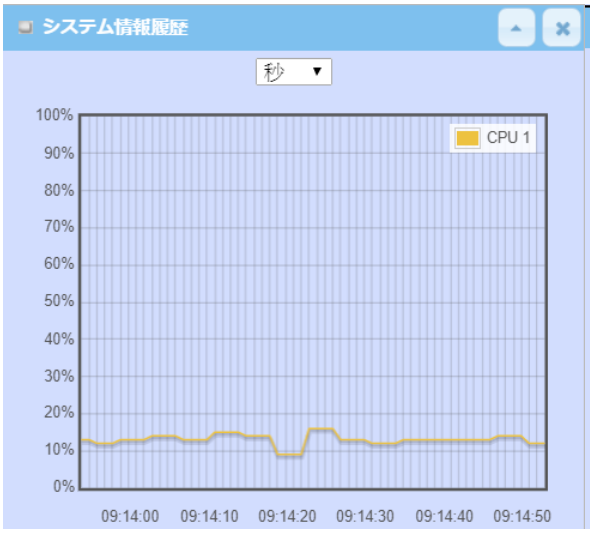
システム情報ステータス

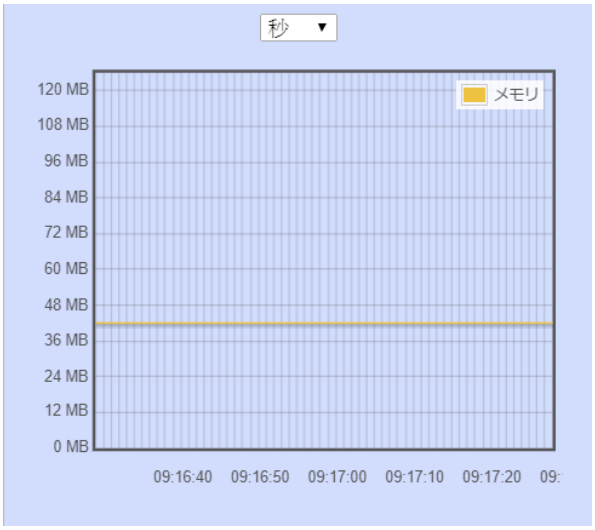
「システム情報」画面には、デバイス稼働時間、CPU、メモリのリソース使用率、および接続セッションが表示されます。



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。





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」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。

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)

8-2. 基本ネットワーク

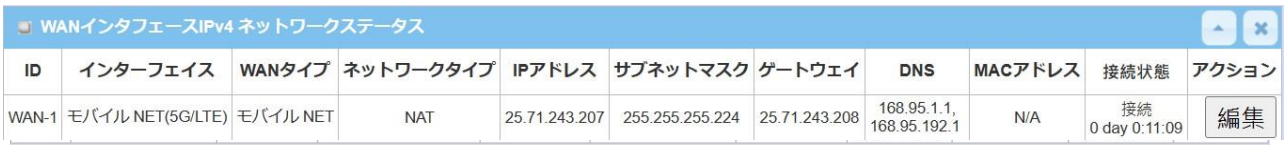
8-2-1. WAN&アップリンクステータス

詳細は、**ステータス** > **［基本ネットワーク］** > **［WAN&アップリンク］タブ**に進みます。

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。

WAN インターフェイス IPv4 ネットワークステータス

「WAN インターフェイス IPv4 ネットワークステータス」画面には、IPv4 ネットワークのステータス情報が表示されます。



WANインターフェイスIPｖ4ネットワークステータス		
項目	**設定値**	**説明**
ID	該当なし	対応する WAN インターフェイスの WAN ID を表示します。
インターフェイス	該当なし	WAN 物理インターフェイスのタイプを表示します。 購入したモデルに応じて、イーサネット、モバイル NET、USB モバイル NET を使用することができます。
WAN タイプ	該当なし	ISP から公開 IP アドレスを取得する方法を表示します。購入したモデルに応じて、 Static IP（静的 IP）、Dynamic IP（動的 IP）、PPPoE、PPTP、L2TP、モバイル NET、WiFi アップリンクを使用することができます。
ネットワークタイプ	該当なし	［NAT モード］、［ブリッジモード］、または［NAT 無効］を表示します。
IP Addr.	該当なし	インターネット接続用に ISP から取得したパブリック IP アドレスを表示します。 未構成の場合、デフォルト値は 0.0.0.0 です。
サブネットマスク	該当なし	インターネット接続用に ISP から取得したパブリック IP アドレスのサブネットマスクが表示されます。 未構成の場合、デフォルト値は 0.0.0.0 です。

ゲートウェイ	該当なし	インターネット接続用に ISP から取得したゲートウェイの IP アドレスを表示します。 未構成の場合、デフォルト値は 0.0.0.0 です。
DNS	該当なし	インターネット接続用に ISP から取得した DNS サーバーの IP アドレスを表示します。 未構成の場合、デフォルト値は 0.0.0.0 です。
MAC アドレス	該当なし	インターネットアクセスを許可する ISP の MAC アドレスを表示します。 注：すべての ISP がこのフィールドを必要とするわけではありません。
接続状態	該当なし	ISP に対するデバイスの接続状態を表示します。 ステータスは、「接続」、または「切断」です。
アクション	該当なし	この領域には機能ボタンがあります。 **[更新]ボタン**を使用すると、デバイスは、DHCP サーバーから IP アドレスを要求するように強制することができます。 注：[更新]ボタンは、DHCP WAN タイプを使用し、WAN 接続が切断されている場合に利用可能です。 **[解除]ボタン**を使用すると、デバイスは、IP アドレス設定をクリアして DHCP サーバーから切断することができます。 注：[解除]ボタンは、DHCP WAN タイプを使用し、WAN 接続が切断されている場合に利用可能です。 **[接続]ボタン**を使用すると、デバイスをインターネットに手動で接続することができます。 注：[接続]ボタンは、WAN タイプの接続制御が、「手動接続」に設定され（基本ネットワーク ＞ WAN&アップリンク ＞「インターネット設定」の[編集]ボタンを参照）、WAN 接続ステータスが切断の時に利用可能です。 **[切断]ボタン**を使用すると、デバイスをインターネットに 手動で切断することができます。 注：[接続]ボタンは、WAN タイプの接続制御が、「手動接続」に設定され（基本ネットワーク ＞ WAN&アップリンク ＞「インターネット設定」の[編集]ボタンを参照）、WAN 接続ステータスが接続の時に利用可能です。

LAN インターフェイスネットワークステータス

「LAN インターフェイスネットワークステータス」画面には、LAN ネットワークの IPv4 と IPv6 の情報が表示されます。

※本製品では「IPv6」は対応しておりません。

LANインターフェイスIPｖ4ネットワークステータス		
項目	**設定値**	**説明**
IPv4 アドレス	該当なし	ゲートウェイの現在の IPv4 IP アドレスを表示します。 また、これは、ルーターの Web ベースユーティリティにアクセスするために、ユーザーが使用する IP アドレスでもあります。
IPv4 サブネットマスク	該当なし	サブネットの現在のマスクを表示します。

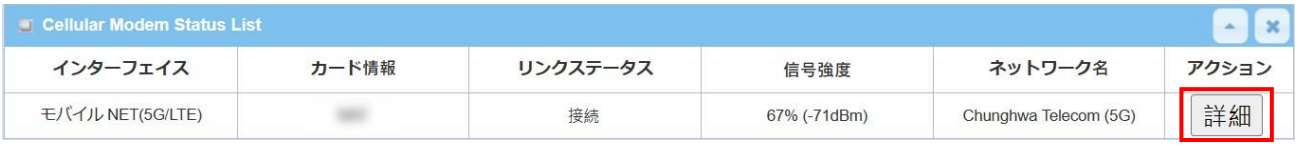
アクション	該当なし	[Pv4 編集する]ボタンを押すと、Web ベースのユーティリティが、イーサネット LAN 構成ページに移動します。 （基本ネットワーク ＞ LAN および VLAN ステータス ＞ 「イーサネット LAN」タブ） **※[IPv6 編集する]ボタンは、本製品では対応しておりません。**

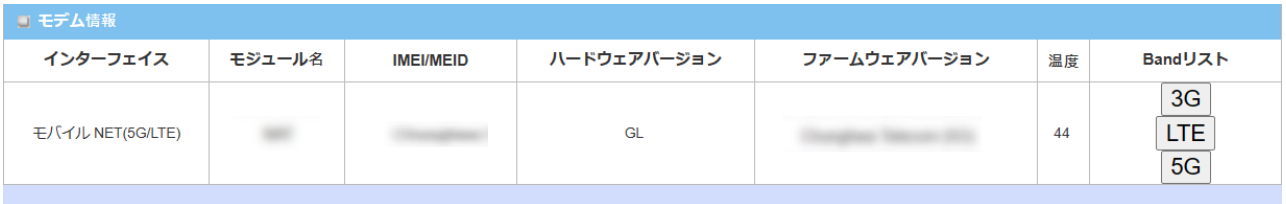
モバイル NET ステータス

「モバイル NET モデムステータスリスト」画面には、モバイル NET WAN ネットワークのステータス情報が表示されます。

モデムステータスリスト		
項目	**設定値**	**説明**
インターフェイス	該当なし	WAN 物理インターフェイスモバイル NET のタイプを表示します。 注：デバイスモデルによっては、2 つのモバイル NET モジュールをサポート するものもあります。 物理インターフェイス名は、モバイル NET-1、およびモバイル NET -2 になります。
カード情報	該当なし	ベンダーのモバイル NET モデム モデル名を表示します。
リンクステータス	該当なし	モバイル NET 接続ステータスを表示します。 表示するステータスは「接続中」、「接続」、「切断中」、「切断」です。
信号強度	該当なし	モバイル NET 無線信号レベルを表示します。
ネットワーク名	該当なし	サービスネットワーク通信事業者の名前が表示されます。
アクション	該当なし	[詳細]ボタンを押すと、詳細情報ウィンドウが表示されます。 モデム情報、SIM ステータス、サービス情報です。 詳細については、以下を参照してください。 注：現在、USB モバイル NET は、この機能をサポートしていません。

[詳細]ボタンを押すと、「モデム情報」、「SIM ステータス」、「サービス情報」、および「信号強度/品質」などのモバイル NET モデム情報ウィンドウを表示します。





SIMステータス

SIM	PINコードステータス	PIN / PUKコード残存時間	ICCID	IMSI	SMSC	MSISDN
SIM-A	準備完了	3 / 10	[redacted]	[redacted]	[redacted]	N/A

サービス情報

オペレーター	MCC	MNC	サービス種類	LAC	TAC	Cell ID
Chunghwa Telecom	466	92	E-UTRA-NR	N/A	8E30	960DD0D

CS / PS ジスタスステータス	PS添付ステータス	ローミングステータス
登録完了 / 登録完了	添付	ローミングしていません

LTE Signal Strength and Quality

Band	RSSI	RSRQ	RSRP	SINR
Band 3	-71	-11	-100	15

NR Signal Strength and Quality

Mode	Type	Band	RSSI	RSRQ	RSRP	SINR
NR5G_NSA	5G	78	N/A	-13	-86	18

SCC 信号情報

Type	Band	RSRP
PCC	3	-100
SCC 1	8	-108
SCC 2	3	-102

エラーメッセージ

索引	エラーの説明
1	N/A

インタフェーストラフィック統計

「インタフェーストラフィック統計」画面には、インタフェースの合計送信パケット数が表示されます。

インタフェーストラフィック統計

ID	インタフェーズ	受信パケット(Mb)	送信パケット(Mb)	アクション
WAN-1	3G/4G	3.65	3.71	Reset

インタフェーストラフィック統計		
項目	設定値	説明
ID	該当なし	対応する WAN インターフェイスの WAN ID を表示します。
インターフェイス	該当なし	WAN 物理インターフェイスのタイプを表示します。
受信パケット	該当なし	ダウンストリームパケットを表示します。 デバイスが再起動するとリセットされます。
送信パケット	該当なし	アップストリームパケットを表示します。 デバイスが再起動するとリセットされます。
アクション	該当なし	［設定リセット］ボタンをクリックすると統計情報全体がクリアされ、カウンターが 0 にリセットされます。

8-2-2. LAN および VLAN ステータス

詳細は、**ステータス** > **［基本ネットワーク］** > **［LAN および VLAN］タブ**に進みます。

クライアントリスト

「クライアントリスト」には、このゲートウェイに接続されている各デバイスの「LAN インターフェイス」、「IP アドレス」、「ホスト名」、「MAC アドレス」、および「残りのリース時間」が表示されます。表示は 5 秒ごとに更新されます。

LANクライアントリスト		
項目	設定値	説明
LAN インターフェイス	該当なし	LAN インターフェイスのクライアントレコードです。文字列形式です。
IP アドレス	該当なし	IP アドレスタイプと IP アドレスのクライアントレコードです。タイプは文字列フォーマットで、IP アドレスは IPv4 フォーマットです。
ホスト名	該当なし	ホスト名のクライアントレコードです。 文字列形式です。
MAC アドレス	該当なし	MAC アドレスのクライアントレコードです。 MAC アドレス形式です。
残りのリース時間	該当なし	残りリース時間のクライアントレコードです。 時間形式です。

8-2-3. 無線ステータス　【未対応】

本製品ではサポートされていない機能です。

8-2-4. ダイナミック DNS ステータス　【未対応】

本製品ではサポートされていない機能です。

8-3. セキュリティ

8-3-1. VPN

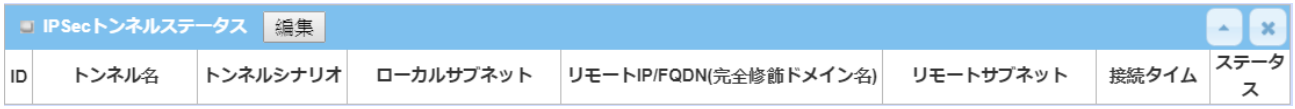
※OpenVPN、PPTP、GRE は、本製品ではサポートされていない機能です。

ステータス > ［セキュリティ］ > ［VPN］タブに進みます。

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。

IPSecトンネルステータス

IPSecトンネルステータスウィンドウには、IPSec VPN接続と現在の接続ステータスを確立するための設定が表示されます。



IPSecトンネルステータス		
項目	設定値	説明
トンネル名	該当なし	識別するために入力したトンネル名を表示します。
トンネルシナリオ	該当なし	指定されたトンネルシナリオを表示します。
ローカルサブネット	該当なし	指定されたローカルサブネットを表示します。
リモート IP/FQDN	該当なし	指定されたリモート IP/FQDN を表示します。
リモートサブネット	該当なし	指定されたリモートサブネットを表示します。
接続タイム	該当なし	IPSec トンネルの接続時間を表示します。
ステータス	該当なし	VPN 接続のステータスを表示します。ステータス表示は、Connected（接続）、Disconnected（切断）、Wait for traffic（トラフィック待ち）、および、Connecting（接続中）です。
編集ボタン	該当なし	［編集］ボタンをクリックして、IPSec 設定を変更すると、Web ベースのユーティリティにより、IPSec 設定ページにリダイレクトされます。（［セキュリティ］ > VPN > 「IPSec」タブ）

OpenVPNサーバーステータス

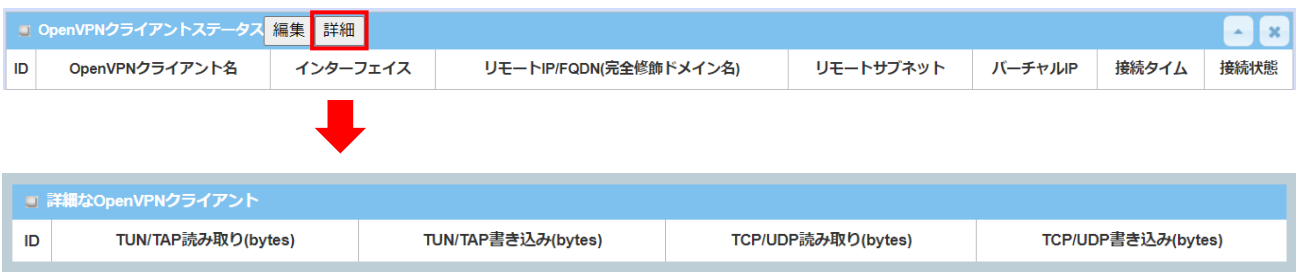
OpenVPN構成に従い、OpenVPNサーバー/クライアントステータスは、 サーバー側またはクライアント側からOpenVPN接続のステータスおよび統計情報を表示します。

OpenVPNサーバーステータス		
項目	設定値	説明
ユーザー名	該当なし	識別のために入力したクライアント名を表示します。
リモート IP/FQDN	該当なし	接続されている OpenVPN クライアントのパブリック IP アドレス（WAN IP アドレス）を表示します。
バーチャル IP/Mac	該当なし	接続された OpenVPN クライアントに割り当てられた仮想 IP/MAC アドレスを表示します。
接続タイム	該当なし	対応する OpenVPN トンネルの接続時間を表示します。
ステータス	該当なし	対応する OpenVPN トンネルの接続ステータスを表示します。 ステータスは、Connected（接続）または Disconnected（切断）です。

OpenVPNクライアントステータス

OpenVPNクライアントステータス		
項目	設定値	説明
OpenVPN クライアント名	該当なし	識別のために入力したクライアント名を表示します。
インターフェイス	該当なし	OpenVPN クライアント接続用に指定された WAN インターフェイスを表示します。
リモート IP/FQDN	該当なし	OpenVPN クライアント接続用に指定された WAN インターフェイスを表示します。
リモートサブネット	該当なし	指定されたリモートサブネットを表示します。
バーチャル IP	該当なし	
接続タイム	該当なし	対応する OpenVPN トンネルの接続時間を表示します。
接続状態	該当なし	対応する OpenVPN トンネルの接続ステータスを表示します。 ステータスは、Connected（接続）または Disconnected（切断）です。

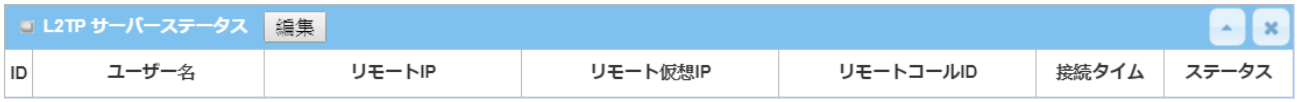
［詳細］ボタンをクリックすると、以下を表示します。



項目	設定値	説明
TUN/TAP 読み取り（bytes）	該当なし	OpenVPN クライアントの TUN/TAP 読み取りバイト数を表示します。
TUN/TAP 書き込み（bytes）	該当なし	OpenVPN クライアントの TUN/TAP 書き込みバイト数を表示します。
TCP/UDP 読み取り（bytes）	該当なし	OpenVPN クライアントの TCP/UDP 読み取りバイト数を表示します。
TCP/UDP 書き込み（bytes）	該当なし	OpenVPN クライアントの TCP/UDP 書き込みバイト数を表示します。

L2TP サーバー/クライアントステータス

L2TP サーバー/クライアントステータスは、 LT2TP トンネルを確立するための構成と現在の接続状態を示します。



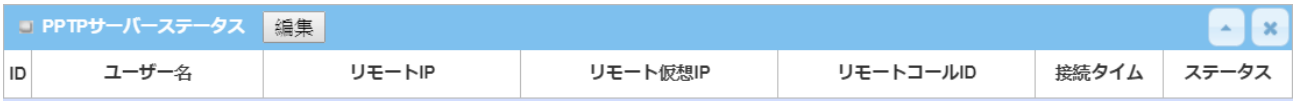
LNSTPサーバーステータス		
項目	設定値	説明
ユーザー名	該当なし	接続に使用されたユーザーのログイン名を表示します。
リモート IP	該当なし	接続されている L2TP クライアントのパブリック IP アドレス（WAN IP アドレス）を表示します。
リモート仮想 IP	該当なし	接続された L2TP クライアントに割り当てられた IP アドレスを表示します。
リモートコール ID	該当なし	L2TP クライアントのコール ID を表示します。
接続タイム	該当なし	L2TP トンネルの接続時間を表示します。
ステータス	該当なし	各 L2TP クライアント接続のステータスを表示します。 ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）を表示します。
編集	該当なし	［編集］ボタンをクリックして、L2TP サーバー設定を変更すると、Web ベースのユーティリティにより、L2TP サーバー設定ページにリダイレクトされます。 （［セキュリティ］ ＞ VPN ＞ 「L2TP」タブ）

L2TPクライアントステータス		
項目	設定値	説明
L2TP クライアント名	該当なし	指定された L2TP クライアントの名称を表示します。

インターフェイス	該当なし	ゲートウェイが、PPTP サーバーへの PPTP トンネリング接続を要求するために使用する WAN インターフェイスを表示します。
バーチャル IP	該当なし	L2TP サーバーの仮想 IP サーバーが割り当てた IP アドレスを表示します。
リモート IP/FQDN	該当なし	L2TP サーバーのパブリック IP アドレス（WAN IP アドレス）または FQDN を表示します。
デフォルトゲートウェイ/リモートサブネット	該当なし	デフォルトゲートウェイである L2TP サーバーに接続するためにインターネットに接続するために使用されるゲートウェイデバイスの指定された IP アドレスが表示されます。または、デフォルトゲートウェイが、L2TP サーバーに接続するために使用されていない場合は、他の指定されたサブネット（リモートサブネット）。
接続タイム	該当なし	L2TP トンネルの接続時間を表示します。
ステータス	該当なし	VPN 接続のステータスを表示します。ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）を表示します。
編集	該当なし	［編集］ボタンをクリックして、L2TP クライアント設定を変更すると、Web ベースのユーティリティにより、L2TP クライアント設定ページにリダイレクトされます。 （［セキュリティ］ > VPN > 「L2TP」タブ）

PPTP サーバー/クライアントステータス

L2TP サーバー/クライアントステータスは、 PPTP トンネルを確立するための構成と現在の接続状態を示します。



PPTPサーバーステータス		
項目	設定値	説明
ユーザー名	該当なし	接続に使用されたユーザーのログイン名を表示します。
リモート IP	該当なし	PPTP クライアントのパブリック IP アドレス（WAN IP アドレス）を表示します。
リモート仮想 IP	該当なし	接続された PPTP クライアントに割り当てられた IP アドレスを表示します。
リモートコール ID	該当なし	PTP クライアントのコール ID を表示します。
接続タイム	該当なし	PPTP トンネルの接続時間を表示します。
ステータス	該当なし	各 PPTP クライアント接続のステータスを表示します。ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）を表示します。
編集	該当なし	［編集］ボタンをクリックして、PPTP サーバー設定を変更すると、Web ベースのユーティリティにより、PPTP サーバー設定ページにリダイレクトされます。 （［セキュリティ］ > VPN > 「PPTP」タブ）

PPTPサーバーステータス		
項目	設定値	説明
PPTP クライアント名	該当なし	指定された PPTP クライアントの名称を表示します。
インターフェイス	該当なし	ゲートウェイが、PPTP サーバーへの PPTP トンネリング接続を要求するために使用する WAN インターフェイスを表示します。
バーチャル IP	該当なし	PPTP サーバーの仮想 IP サーバーが割り当てた IP アドレスを表示します。
リモート IP/FQDN	該当なし	PPTP サーバーのパブリック IP アドレス（WAN IP アドレス）または FQDN を表示します。
デフォルトゲートウェイ/リモートサブネット	該当なし	デフォルトゲートウェイである PPTP サーバーに接続するためにインターネットに接続するために使用されるゲートウェイデバイスの指定された IP アドレスが表示されます。または、デフォルトゲートウェイが、PPTP サーバーに接続するために使用されていない場合は、他の指定されたサブネット（リモートサブネット）。
接続タイム	該当なし	PPTP トンネルの接続時間を表示します。
ステータス	該当なし	VPN 接続のステータスが表示されます。ステータスに、Connected（接続）、Disconnect（切断）、および、Connecting（接続中）を表示します。
編集	該当なし	［編集］ボタンをクリックして、PPTP クライアント設定を変更すると、Web ベースのユーティリティにより、PPTP サーバー設定ページにリダイレクトされます。（[セキュリティ］ > VPN > PPTP タブ）

8-3-2. ファイヤーウォール

ステータス > ［セキュリティ］ > ［ファイヤーウォール］タブに進みます。

ファイヤーウォールのステータスと現在のファイヤーウォール設定を素早く表示します。また、ファイヤーウォールルールポリシーによって ドロップされたパケットのログ履歴が保持され、ファイアウォールオプションで指定された管理者のリモートログイン設定も含まれます。
表示は5秒ごとに更新されます。

アイコン[+]をクリックすると、ステータステーブルが展開され、ログ履歴が表示されます。
[編集]ボタンをクリックすると、画面が設定ページに切り替わります。

パケットフィルターステータス

パケットフィルターステータス		
項目	設定値	説明
有効化 フィルタルール	該当なし	パケットフィルタルール名です。
検出コンテンツ	該当なし	送信元 IP、宛先 IP、プロトコル、および宛先ポート（TCP または UDP）を含む記録されたパケット情報です。 文字列形式： ソース IP から宛先 IP へ： 宛先プロトコル（TCP または UDP）
IP	該当なし	記録されたパケットの送信元 IP（IPv4）です。
タイム	該当なし	記録されたパケットの日付と時刻。 日付と時刻の形式（ "月" "日" "時間"： "分"： "秒"）

注：パケットフィルタログアラートが有効になっていることを確認してください。
［セキュリティ］> ［ファイヤーウォール］>［パケットフィルター］タブを参照してください。
「ログアラート」にチェックを入れ、設定を保存します。

MAC制御ステータス

MAC制御ステータス		
項目	設定値	説明
有効制御ルール	該当なし	MAC Control Rule （MAC 制御ルール）名です。
ブロック MAC アドレス	該当なし	記録されたパケットの MAC アドレスです。

IP	該当なし	記録されたパケットの送信元 IP（IPv4）です。
タイム	該当なし	記録されたパケットの日付と時刻。 日付と時刻の形式 （″月″ ″日″ ″時間″：″分″：″秒″）

注：MAC Control Log Alert（MAC 制御ログアラート）が有効になっていることを確認します。
セキュリティ > ［ファイヤーウォール］>［MAC 制御］タブを参照してください。
「ログアラート」にチェックを入れ、設定を保存します。

IPS ステータス

IPファイアウィールステータス		
項目	設定値	説明
検出された侵入	該当なし	ブロックされているパケットの侵入タイプです。
IP	該当なし	記録されたパケットの送信元 IP（IPv4）です。
タイム	該当なし	記録されたパケットの日付と時刻。 日付と時刻の形式 （″月″ ″日″ ″時間″：″分″：″秒″）

注：IPS Log Alert（IPS ログアラート）が有効になっていることを確認します。
セキュリティ］> ［ファイヤーウォール］>［IPS］タブを参照してください。
「ログアラート」にチェックを入れ、設定を保存します。

ファイアウォールオプションステータス

ファイアウィールオプションステータス		
項目	設定値	説明
ステルスモード	該当なし	ファイアウォールオプション上で、ステルスモードの設定ステータスを有効または無効します。 文字列形式： Disable（無効）または Enable（有効）
SPI	該当なし	ファイアウォールオプション上で、SPI の設定ステータスを有効または無効します。 文字列形式： Disable（無効）または Enable（有効）
WAN からの Ping パケットを破棄する	該当なし	ファイアウォールオプション上で、WAN からの 破棄 Ping の設定ステータスを Enable（有効）または Disable（無効）にします。 文字列形式： Disable（無効）または Enable（有効）
リモート管理者管理	該当なし	リモート管理者の設定ステータスを Enable（有効）または Disable（無効）にします。 リモート管理者が有効になっている場合は、現在ログインしている管理者の送信元 IP アドレスとログインユーザー名とログイン時間が表示されます。

		形式 IP：「Source IP（ソース IP)」、ユーザー名： 「Login User Name（ログインユーザー名)」、時刻： 「Date time（日時)」 例 IP：192.168.127.39、ユーザー名：admin、時刻： Mar 3 01:34:13

注：ファイアウォールオプションログアラートが有効になっていることを確認します。
セキュリティ〉［ファイヤーウォール］〉［オプション］タブを参照してください。
「ログアラート」にチェックを入れ、設定を保存します。

8-4. 管理（Administration）

8-4-1. 設定と管理

ステータス > ［管理（Administration）］ > ［設定と管理］タブに進みます。

「設定と管理」ウィンドウには、リモートネットワークデバイスを管理するためのステータスが表示されます。デバイスで使用できる管理の種類は、購入したデバイスモデルによって異なります。よく使われるのは、SNMP、UPnPです。
表示は5秒ごとに更新されます。

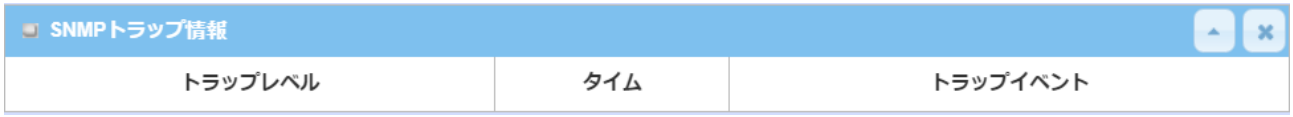
SNMP リンクステータス

SNMP Link Status（SNMPリンクステータス）画面には、現在有効なSNMP接続のステータスが表示されます。

SNMPリンクステータス		
項目	設定値	説明
ユーザー名	該当なし	認証のためのユーザー名を表示します。 これは、SNMP バージョン 3 でのみ利用可能です。
IP アドレス	該当なし	SNMP マネージャの IP アドレスを表示します。
ポート	該当なし	SNMP マネージャとの接続を維持するために使用されるポート番号を表示します。
コミュニティ	該当なし	SNMP バージョン 1 またはバージョン 2c のコミュニティのみを表示します。
認証モード	該当なし	SNMP バージョン 3 の認証方法のみを表示します。
プライバシーモード	該当なし	バージョン 3 のプライバシーモードのみを表示します。
SNMP バージョン	該当なし	使用されている SNMP のバージョンを表示します。

SNMPトラップ情報

SNMPトラップ情報画面には、現在受信しているSNMPトラップのステータスが表示されます。



SNMPトラップ情報		
項目	設定値	説明
トラップレベル	該当なし	トラップレベルを表示します。
タイム	該当なし	トラップイベントのタイムスタンプを表示します。
トラップイベント	該当なし	トラップ送信者の IP アドレスとイベントタイプを表示します。

8-4-2. ログストレージ

ステータス > 管理（Administration） > 「ログストレージ」タブに進みます。

ストレージ情報
ストレージ情報画面には、選択したデバイスストレージの現在のステータスが表示されます。
ステータスには、デバイスの選択、デバイスの説明、使用量、ファイルシステム、速度、ステータスが含まれます。

8-4-3. GNSS　【未対応】

本製品ではサポートされていない機能です。

8-5. 統計とレポート

8-5-1. 接続セッション

ステータス > **［統計とレポート］** > **［接続セッション］タブ**に進みます。

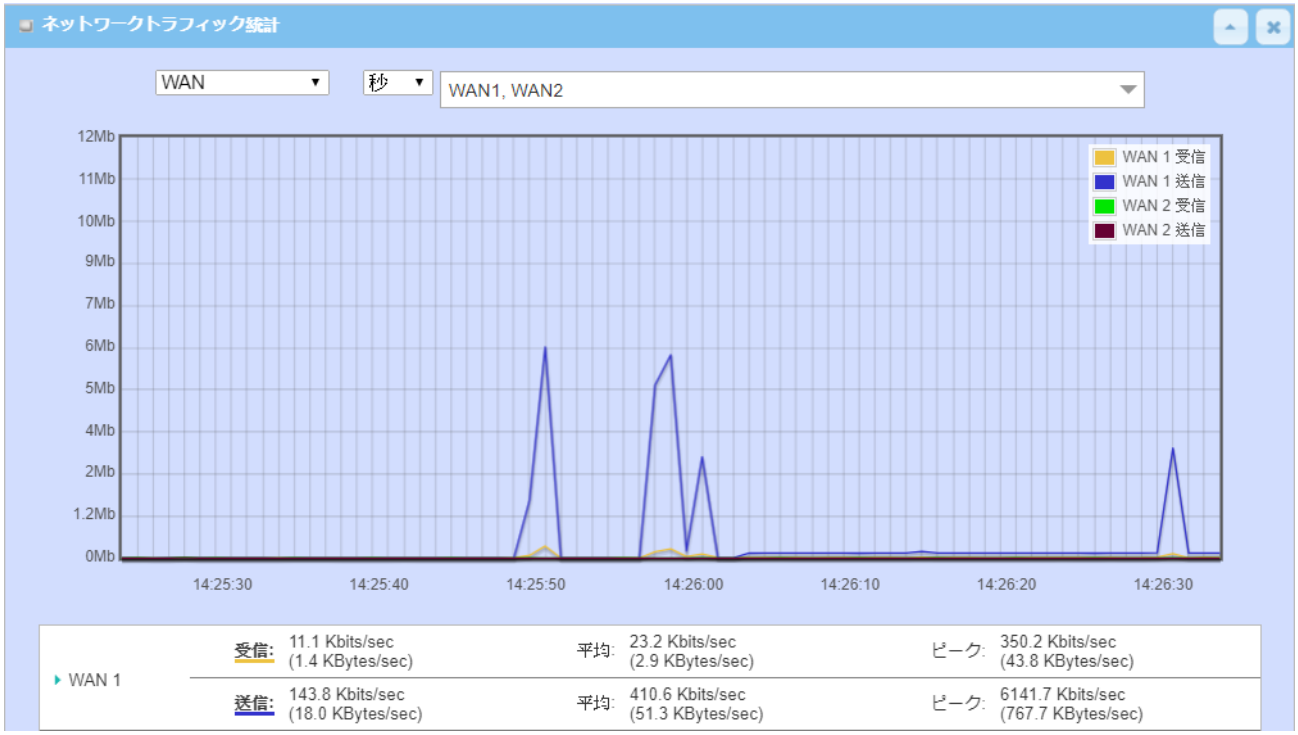
「インターネットサーフィンリスト」には、このルーター上の接続トラックを表示します。

インターネットサーフィン統計		
ボタン	**設定値**	**説明**
前	該当なし	[前]ボタンをクリックします。 トラックリストの前のページを表示します。
次に	該当なし	[次]ボタンをクリックします。 トラックリストの次のページを表示します。
最初	該当なし	[最初]ボタンをクリックします。 トラックリストの最初のページを表示します。
最後	該当なし	[最後]ボタンをクリックします。 トラックリストの最後のページを表示します。
Export(.xml)	該当なし	[Export(.xml)]ボタンをクリックします。 リストを xml ファイルにてエクスポートします。
Export(.csv)	該当なし	[Export(.csv)]ボタンをクリックします。 リストを csv ファイルにてエクスポートします。
更新	該当なし	[更新]ボタンをクリックして、リストを更新します。

8-5-2. ネットワークトラフィック

ステータス > **［統計とレポート］** > **［ネットワークトラフィック］タブ**に進みます。

「ネットワークトラフィック統計」画面には、選択したネットワークインターフェイスの履歴グラフが表示されます。インターフェイスドロップリストを変更し、監視するインターフェイスを選択できます。



8-5-3. ログイン統計

ステータス > ［統計とレポート］ > ［ログイン統計］タブに進みます。

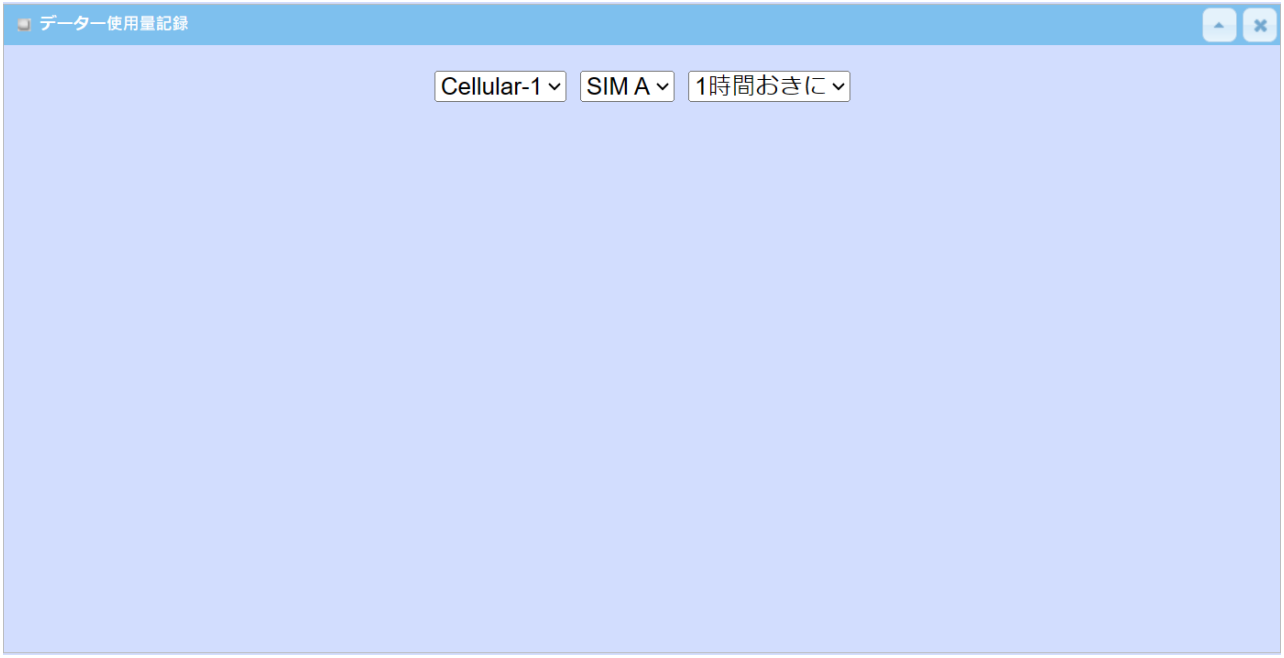
「デバイス管理者統計」には、ログイン情報が表示されます。

デバイス管理者統計		
ボタン	**設定値**	**説明**
前	該当なし	[前]ボタンをクリックします。 ログイン統計の前のページを表示します。
次に	該当なし	[次]ボタンをクリックします。 ログイン統計の次のページを表示します。
最初	該当なし	[最初]ボタンをクリックします。 ログイン統計の最初のページを表示します。
最後	該当なし	[最後]ボタンをクリックします。 ログイン統計の最後のページを表示します。
Export(.xml)	該当なし	[Export(.xml)]ボタンをクリックします。 ログイン統計を xml ファイルにてエクスポートします。
Export(.csv)	該当なし	[Export(.csv)]ボタンをクリックします。 ログイン統計を csv ファイルにてエクスポートします。
更新	該当なし	[更新]ボタンをクリックして、ログイン統計を更新します。

8-5-4. セルラー使用状況

ステータス ＞ ［統計とレポート］ ＞ ［セルラー使用状況］タブに進みます。

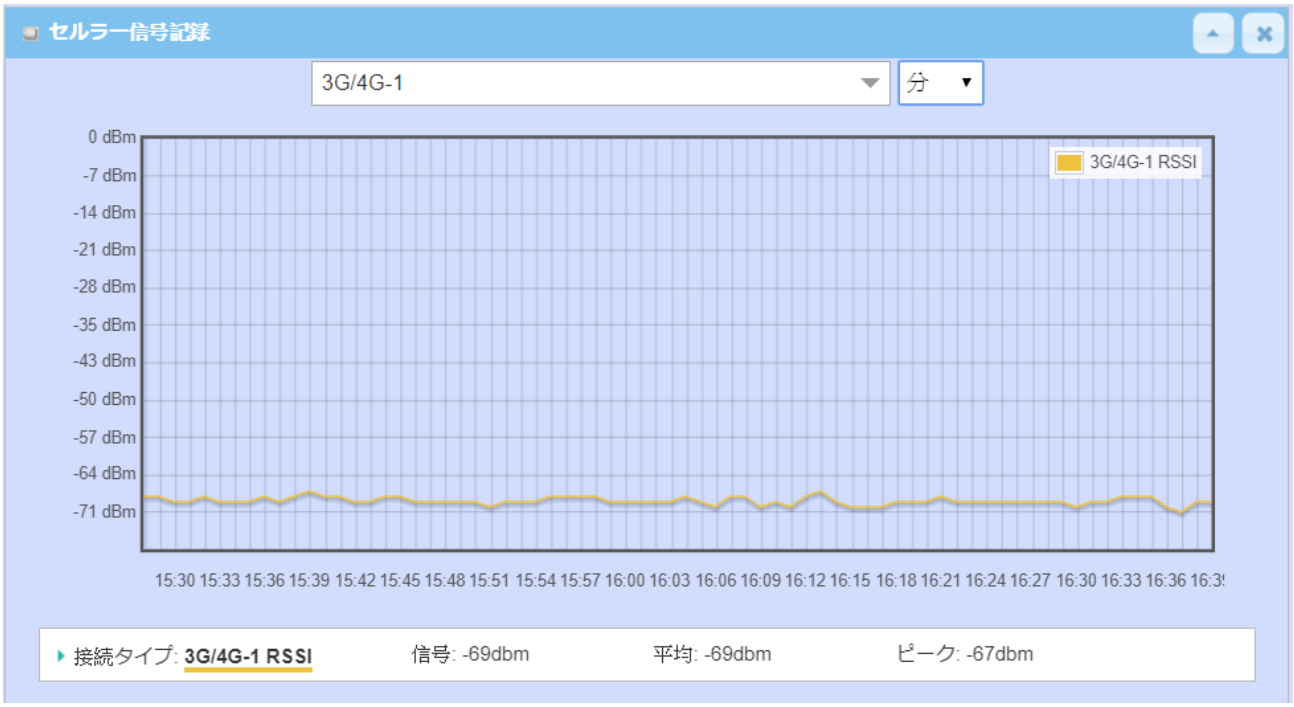
「セルラー使用状況」画面には、選択したセルラーインターフェイスのデータ使用状況統計が表示されます。
セルラーデータ使用状況は、1時間または1日に蓄積することができます。



8-5-5. セルラー信号

ステータス > **［統計とレポート］** > **［セルラー信号］タブ**に進みます。

「セルラー信号記録」画面には、選択したセルラーインターフェイスのデータ使用状況統計が表示されます。
セルラー信号記録は、1時間、または1日に蓄積することができます。



第9章. 改訂履歴

版	日付	内容
第 1.0 版	2024/12/05	初版

SIM Router IDG500V-0T501　取扱説明書

更新日：2024/12/05

株式会社バルテック