HW5G-3311-DS

取扱説明書



HYTEC INTER Co., Ltd.

第 1.1 版

管理番号:RFD-26MA0007-01.1

ご注意

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

電波障害自主規制について

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

改版履歴

第 1.0 版	2026 年 9 月 15 日	初版制定
第 1.1 版	2026 年 10 月 7 日	表記揺れ・誤記修正

ご使用上の注意事項

◆ 本製品及び付属品をご使用の際は、取扱説明書に従って正しい取り扱いをしてください。

◆ 本製品は、一般事務用、通常の産業等の一般的用途を想定した製品であり、ハイセイフティ用途*での設備や機器としての使用またはこれらに組込んでの使用は意図されておりません。これらの設備や機器、システムなどに本製品を使用され、本製品の故障等により、人身事故、火災事故、社会的な損害などが生じても当社はいかなる責任も負いかねます。お客様が、本製品をハイセイフティ用途に使用される場合は、必要な安全性を確保する措置を施す等十分な配慮をお願いします。

◆ 本製品を分解したり改造したりすることは絶対に行わないでください。

◆ 本製品をほこりや湿気の多い場所、油煙や湯気のあたる場所で使用しないでください。故障や火災の原因になることがあります。

◆ 本製品を重ねて使用しないでください。故障や火災の原因になることがあります。

◆ 通気口の隙間などから液体、金属などの異物を入れないでください。感電や故障の原因になることがあります。

◆ 本書の中に含まれる情報は、当社（ハイテクインター株式会社）の所有するものであり、当社の同意なしに、全体または一部を複写または転載することは禁止されています。

◆ 本製品及び付属品は、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。

＊ 極めて高度な信頼性や安全性が要求され、機器の故障、誤動作により、信頼性や安全性が確保されない場合、生命、身体や財産等に損害を及ぼす恐れがある用途

目次

1. 製品概要 14

2. モバイル NET 回線契約 14

3. 梱包物一覧 14

4. 設定および保守時の注意 14

4.1. 熱に関する注意事項 14

5. 製品外観 15

5.1. LED 15

5.1.1. 各 LED 15

5.2. 前面 16

5.3. 背面 16

5.4. SIM カードの取り付け/取り外し方法 17

5.5. 電源の接続 18

6. WEB GUI での設定について 19

6.1. Web GUI へのアクセス 19

6.1.1. PC システム要件 19

6.1.2. ログイン初期設定 19

6.1.3. ログイン手順 19

6.1.4. Web 表示言語の変更 20

6.2. LAN 側 IP アドレスの設定 21

6.3. 管理ユーザー名の変更 21

✧ 基本設定編 22

7. モバイル NET(5G/LTE)の設定 22

7.1. 物理インターフェイスの設定 22

7.2. モバイル NET パラメータの設定 24

✧ 応用設定編 27

8. 基本ネットワーク 27
8.1. WAN およびアップリンク 27
8.1.1. 物理インターフェイスリスト 27
8.1.2. フェールオーバー機能 28
8.1.3. 物理インタフェースの設定 29
8.1.4. 接続設定 30
8.1.5. WAN インタフェース：モバイル NET(5G/LTE)の接続設定 30
8.1.5.1. デュアル SIM フェールオーバー機能について 30
8.1.5.2. インターネット接続構成およびモバイル NET の WAN タイプ[Cellular WAN Type]構成 31
8.1.5.3. SIM 転換のポリシーの設定 32
8.1.5.4. SIM-A カードとの接続/SIM-B カードとの接続 33
8.1.5.5. モバイル NET 接続の共有設定 34
8.1.6. WAN インタフェース :WiFi モジュール1の設定 35
8.1.6.1. インターネット接続構成 35
8.1.6.2. WiFi Uplink WAN Type Configuration 35
8.1.6.3. WiFi アップリンク スキャン画面 36
8.1.7. WAN インタフェース：イーサネットの接続設定 37
8.1.7.1. イーサネット WAN 設定 37
8.1.7.2. 静的IP WAN 設定 38
8.1.7.3. 動的IP WAN 設定 39
8.1.7.4. PPPoE WAN 設定 40
8.1.8. ネットワーク監視構成の設定 41
8.1.8.1. ネットワーク監視構成の使用上の注意点 42
8.1.9. 負荷分散 43
8.1.9.1. 負荷分散の設定 43
8.1.9.2. 特定のウェイトの設定 44
8.1.9.3. ユーザーポリシーリストの追加・編集 44
8.2. LAN および VLAN 46
8.2.1. イーサネット LAN 46
8.2.2. 追加 IP 機能 47
8.2.3. 仮想 LAN(VLAN) 48
8.2.4. 仮想 LAN(VLAN)の設定 48
8.2.4.1. ポートベース VLAN ルールの設定 48
8.2.4.2. IP 固定マッピングルールの設定 52
8.2.4.3. ポートベース VLAN 間グループルーティング 52
8.2.4.4. タッグベース VLAN ルールの設定 53

8.2.5. DHCP サーバー 55
8.2.5.1. DHCP サーバーリスト 55
8.2.5.2. DHCP サーバーの設定 56
8.2.5.3. IP 固定マッピングルールの設定 57
8.2.5.4. DHCP クライアントリストの表示/マッピングルールへのコピー 58
8.2.5.5. DHCP サーバーオプションの有効/無効（未サポート） 58
8.2.5.6. DHCP サーバーオプションリストの追加/編集（未サポート） 59
8.2.5.7. DHCP リレー構成リストの追加/編集 60
8.3. WiFi 61
8.3.1. WiFi モジュール 1 62
8.3.1.1. 基本構成の設定 62
8.3.1.2. WiFi 構成の設定 62
8.3.1.3. VAP 構成 63
8.3.2. ワイヤレスクライアントリスト 65
8.3.2.1. ターゲット WiFi の選択 65
8.3.2.2. クライアントリスト 65
8.3.3. 詳細構成 66
8.3.3.1. ターゲット WiFi の選択 66
8.3.3.2. 詳細構成 66
8.3.4. アップリンクプロファイル 68
8.3.4.1. アップリンクプロファイルの設定 68
8.3.4.2. アップリンクプロファイルの作成 68
8.3.4.3. アップリンクプロファイルの追加/編集（スキャン） 70
8.4. IPv6 71
8.4.1. IPv6 接続タイプ 71
8.4.1.1. Static IPv6 71
8.4.1.2. PPPoEv6 71
8.4.1.3. DHCPv6 72
8.4.2. IPv6 構成設定 72
8.4.2.1. Static IPv6 WAN タイプ構成 73
8.4.2.2. PPPoE WAN タイプ構成 74
8.4.2.3. DHCPv6 WAN タイプ構成 74
8.4.2.4. アドレス自動構成 75
8.5. ポート転送 76
8.5.1. ポート転送設定 76
8.5.1.1. NAT ループバック 76
8.5.2. 仮想サーバー＆仮想コンピュータ 77
8.5.2.1. 仮想サーバー 77

8.5.2.2. 仮想コンピュータ 77
8.5.2.3. 仮想サーバーおよび仮想コンピュータの有効 78
8.5.2.4. 仮想サーバーの追加/編集 78
8.5.2.5. 仮想コンピュータの追加/編集 80
8.5.3. スペシャル AP&ALG 81
8.5.3.1. 設定 81
8.5.3.2. スペシャル AP リストの編集 81
8.5.4. DMZ およびパススルー 83
8.5.4.1. DMZ（De Militarized Zone） 83
8.5.4.2. VPN パススルー 83
8.5.4.3. DMZ の設定 84
8.5.4.4. VPN パススルーの設定 84
8.6. ルーティング 85
8.6.1. 静的ルーティング 85
8.6.1.1. 静的ルーティングの設定 85
8.6.1.2. IPv4 静的ルーティングルールの追加/編集 86
8.6.2. 動的ルーティング 87
8.6.2.1. RIPv1/RIPv2 ルーティング 87
8.6.2.2. OSPF ルーティング 87
8.6.2.3. BGP ルーティング 87
8.6.2.4. RIP 設定 88
8.6.2.5. OSPF 設定 88
8.6.2.6. OSPF 領域リストの追加/編集 89
8.6.2.7. BGP 設定 89
8.6.2.8. BGP ネットワークリストの追加/編集 90
8.6.2.9. BGP 近隣ルールの追加/編集 90
8.6.3. ルーティング情報 91
8.7. DNS & DDNS 92
8.7.1. 動的 DNS の設定 92
8.7.2. DNS Mapping の設定 93
8.7.3. マッピングルールの定義 93
8.7.4. DNS リダイレクトの設定 94
8.7.5. リダイレクトルールの定義 94
8.8. QoS 95
8.8.1. QoS 設定 95
8.8.2. ソフトウェア QoS 95
8.8.2.1. システムリソース構成 95
8.8.2.2. WAN インタフェースリソース設定 96

8.8.2.3. QoS ルールの追加・編集 96
8.8.3. ハードウェア QoS 98
8.8.3.1. WAN インタフェースリソースの設定 98
8.8.3.2. QoS ルールの追加・編集 98
8.8.3.3. キューの設定 100
9. オブジェクト定義 101
9.1. スケジューリング 101
9.1.1. タイムスケジュールリストの追加/編集 101
9.1.2. 期間定義の設定 101
9.2. グルーピング 103
9.2.1. ホストグループ 103
9.2.1.1. ホストグループ構成 103
9.3. 外部サーバー 104
9.3.1. 外部サーバーリストの追加/編集 104
9.4. 証明書 106
9.4.1. 設定 106
9.4.1.1. ルート CA の作成 106
9.4.2. ローカル証明書 107
9.4.2.1. ローカル証明書の作成 107
9.4.2.2. 証明書のインポート 108
9.4.3. 信頼できる証明書 109
9.4.4. 発行証明書 110
9.4.5. 証明書設定方法 111
9.4.5.1. Root CA の秘密鍵/公開鍵の生成 111
9.4.5.2. サーバ証明書とその秘密鍵の生成 111
9.4.5.3. クライアント側への CA の公開鍵の登録 111
9.4.5.4. クライアント証明書とその秘密鍵の生成とインポート 112
10. セキュリティ 113
10.1. VPN 113
10.1.1. IPSec 114
10.1.1.1. IPSec の設定 114
10.1.1.2. IPSec トンネルの追加/編集 114
10.1.1.3. トンネル設定 114
10.1.1.4. ローカル＆リモート設定 115
10.1.1.5. 認証設定 116
10.1.1.6. IKE フェーズ設定 116

10.1.1.7. IKE プロポーザル定義 117
10.1.1.8. IPSec フェーズ設定 117
10.1.1.9. IPSec プロポーザル定義 117
10.1.2. OpenVPN 118
10.1.2.1. OpenVPN の設定 118
10.1.2.2. OpenVPN サーバー構成 119
10.1.2.3. OpenVPN サーバーの詳細構成 121
10.1.2.4. OpenVPN クライアントリストの追加/編集 122
10.1.2.5. OpenVPN クライアント詳細構成 124
10.1.3. L2TP 126
10.1.3.1. L2TP の設定 126
10.1.3.2. L2TP サーバーの設定 126
10.1.3.3. L2TP サーバーステータス 128
10.1.3.4. ユーザーアカウントの追加・編集 128
10.1.3.5. L2TP クライアントの設定 129
10.1.3.6. L2TP クライアントリストの追加/編集 129
10.1.4. PPTP 131
10.1.4.1. PPTP の設定 131
10.1.4.2. PPTP サーバーの設定 131
10.1.4.3. PPTP サーバーステータス 132
10.1.4.4. ユーザーアカウントの追加・編集 132
10.1.4.5. PPTP クライアントの設定 132
10.1.4.6. PPTP クライアントリストの追加/編集 133
10.1.5. GRE 135
10.1.5.1. GRE の設定 135
10.1.5.2. GRE トンネルの追加/編集 135
10.1.6. EoGRE 137
10.1.6.1. EoGRE の設定 137
10.1.6.2. EoGRE トンネルの追加/編集 137
10.1.6.3. TAG ID List 139
10.1.6.4. WireGuard の設定 140
10.1.6.5. WireGuard サーバー構成 140
10.1.6.6. ピア構成の設定 142
10.1.6.7. WireGuard の Client 設定 142
10.2. ファイヤーウォール 144
10.2.1. パケットフィルター 144
10.2.1.1. パケットフィルタ設定 144
10.2.1.2. パケットフィルタルールの追加/編集 144

10.2.2. URL ブロッキング 147
10.2.2.1. URL ブロッキング設定 147
10.2.2.2. URL ブロッキングルールの追加/編集 147
10.2.3. MAC 制御 149
10.2.3.1. MAC 制御ルールリストの追加/編集 150
10.2.4. IPS 151
10.2.4.1. IPS 設定 151
10.2.4.2. 侵入防止機能設定 152
10.2.5. オプション 153
10.2.5.1. ファイヤーウォールオプション設定 153
10.2.5.2. IPv6 Firewall Options 153
10.2.5.3. リモート管理者ホスト定義の編集 153
10.3. 認証 155
10.3.1. MAC 認証 155
10.3.1.1. MAC 認証の設定 155
10.3.1.2. ユーザーリストの作成 156
11. 管理(Administration) 157
11.1. 設定と管理 （本機ではサポートしておりません） 157
11.1.1. コマンドスクリプト 157
11.1.2. Device Management 157
11.1.3. RESTful 157
11.1.4. SNMP 157
11.1.5. Telnet & SSH 157
11.2. システム管理 158
11.2.1. パスワード及び MMI 158
11.2.1.1. ホスト名の設定 158
11.2.1.2. ユーザー名の変更 158
11.2.1.3. パスワードの変更 158
11.2.1.4. MMI（マネージメントインタフェース）の設定 159
11.2.2. システム情報 160
11.2.3. システムタイム 160
11.2.3.1. タイムサーバーと同期する 160
11.2.3.2. 手動でシステム時間を設定する 161
11.2.3.3. PC と手動で同期をとる 162
11.2.3.4. GPS を利用して同期をとる 162
11.2.4. システムログ 163
11.2.4.1. 表示および E メールログ履歴 163

11.2.4.2. ログタイプカテゴリ 164
11.2.4.3. E メールアラート 164
11.2.5. バックアップ及び復元 165
11.2.6. 再起動およびリセット 165
11.3. FTP 166
11.3.1. サーバー構成 166
11.3.1.1. FTP サーバー設定 166
11.3.1.2. SFTP サーバ設定 167
11.3.2. ユーザーアカウント 167
11.3.2.1. ユーザーアカウントリスト 167
11.4. 診断 168
11.4.1. 診断ツール 168
11.4.2. イーサネットポートセットアップ 169
11.4.2.1. Ethernet Port Setup 169
11.4.2.2. Ethernet Port Setup List 169
11.4.3. ハートビート監視 170
11.4.3.1. ハートビート監視構成 170

12. サービス 171

12.1. セルラーツールキット 171
12.1.1. データ使用量（データ使用量の制限） 171
12.1.1.1. モバイル NET データ使用量プロファイルリストの追加/編集 172
12.1.2. SMS 173
12.1.2.1. SMS の設定 173
12.1.2.2. SMS 要約 173
12.1.2.3. 新規 SMS 174
12.1.2.4. SMS 受信トレイ 174
12.1.3. SIM PIN 175
12.1.3.1. SIM カードの選択（Configuration） 175
12.1.3.2. PUK 機能 175
12.1.3.3. SIM 機能 （PIN コードの設定） 176
12.1.4. 通信スキャン 176
12.2. SMS＆イベント 177
12.2.1. 設定 177
12.2.1.1. イベントマネージメントの設定 177
12.2.1.2. SMS コンフィギュレーションの設定 177
12.2.1.3. SMS アカウントリスト 178
12.2.1.4. Email サービスリストの追加/編集 179

12.2.1.5. リモートホストリストの追加/編集 179
12.2.2. マネージングイベント 180
12.2.2.1. マネージングイベントの設定 180
12.2.2.2. マネージングリストの追加/編集 181
12.2.3. 通知イベント 183
12.2.3.1. 通知イベントの設定 183
12.2.3.2. 通知イベントリストの追加/編集 183
12.3. 位置追跡 185
12.3.1. GNSS 185
12.3.1.1. 設定 185
12.3.1.2. リモートホストリストの追加/編集 187
12.4. 電源制御 188
12.4.1. イグニッションセンス 188
13. ステータス 189
13.1. ダッシュボード 189
13.1.1. システム情報 189
13.1.2. システム情報履歴 190
13.1.3. ネットワークインターフェイスステータス 190
13.2. 基本ネットワーク 191
13.2.1. WAN & アップリンク 191
13.2.1.1. WAN インタフェース IPv4 ネットワークステータス 191
13.2.1.2. WAN インタフェース IPv6 ネットワークステータス 191
13.2.1.3. LAN インタフェースネットワークステータス 192
13.2.1.4. Cellular[モバイル NET] Modem Status List 192
13.2.1.5. インタフェーストラフィック統計 193
13.2.2. LAN および VLAN 193
13.2.2.1. クライアントリスト 193
13.2.3. Wifi 193
13.2.3.1. WiFi モジュール1 バーチャル AP リスト 193
13.2.3.2. WiFi モジュール1 アップリンクステータス 193
13.2.3.3. WiFi モジュール1IDS ステータス 194
13.2.3.4. WiFi モジュール1トラフィック統計 194
13.2.4. ダイナミック DNS 194
13.2.4.1. DNS ステータスリスト 194
13.3. セキュリティ 195
13.3.1. VPN 195
13.3.1.1. IPSec トンネルステータス 195

13.3.1.2. OpenVPN サーバーステータス 195
13.3.1.3. OpenVPN クライアントステータス 196
13.3.1.4. L2TP サーバーステータス 196
13.3.1.5. L2TP クライアントステータス 196
13.3.1.6. PPTP サーバーステータス 196
13.3.1.7. PPTP クライアントステータス 196
13.3.2. ファイヤーウォール 197
13.3.2.1. パケットフィルター 197
13.3.2.2. URL ブロッキング 197
13.3.2.3. MAC 制御 197
13.3.2.4. IPS 197
13.3.2.5. オプション 197
13.4. 管理（Administration） 198
13.4.1. 設定と管理 198
13.4.2. ログストレージ 198
13.4.2.1. ストレージ情報ステータス 198
13.4.3. GNSS 198
13.4.3.1. GNSS 情報 198
13.5. 統計とレポート 199
13.5.1. 接続セッション 199
13.5.1.1. Connection Session List 199
13.5.2. ログイン統計 199
13.5.2.1. デバイス管理者統計 199
13.5.2.2. セルラー使用状況 200
13.5.2.3. データ使用量記録 200
13.5.3. セルラー信号 200
13.5.3.1. セルラー信号記録 200
14. 製品仕様 201
15. 製品保証 203

1. 製品概要

HW5G-3311-DS は、-30～+60℃の広い動作温度に対応した産業用の 5G/LTE 対応ルータです。ノンスタンドアローンおよびスタンドアローン構成モバイルネットワーク 5G対応モジュールが搭載されており、高速な通信が可能となります。また、2 回線を使用することにより、主回線が故障した場合に副回線に切り替えるフェールオーバー機能を搭載しています。

（注１） 5G の通信速度は通信状態に左右されるため、4G/LTE よりも低速になる場合があります。
（注２） 本機搭載イーサネットポートは 1000BASE-T 規格であるため、1Gbps よりも高速になることはありません。
（注３） 本書および WebGUI 上でモバイル NET および Cellular の表記がありますが、NR Sub6 5G/LTE の接続のことを示しています。

2. モバイル NET 回線契約

本機では、5G 通信契約された SIM（オプションの場合もあります）をご利用ください。LTE(4G)契約の SIM はご使用いただけない場合があります。

3. 梱包物一覧

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

名　称	数 量
本体	1 台
5G/LTE アンテナ	4 個
WiFi アンテナ	2 個
電源用ターミナルブロック	1 個
マウントブラケット	2 個
マウントブラケット取付けネジ	4 個

4. 設定および保守時の注意

4.1. 熱に関する注意事項



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

5. 製品外観

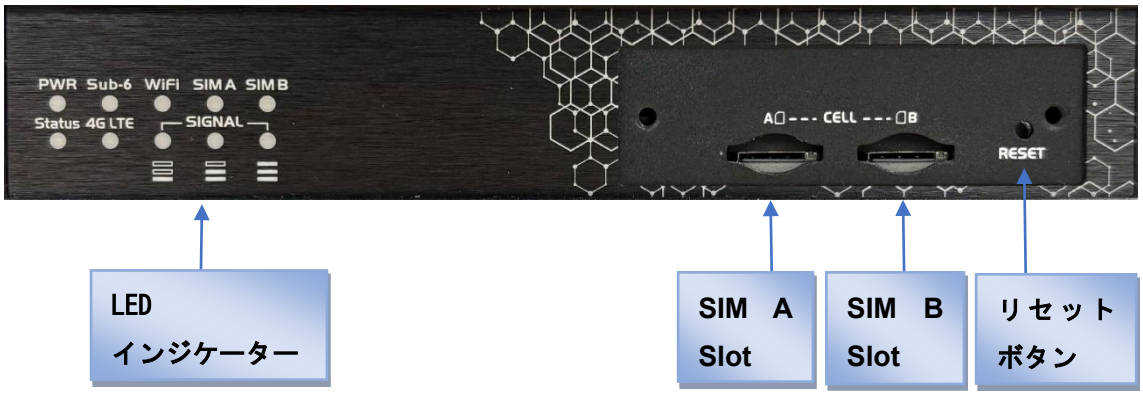
5.1. LED



5.1.1. 各 LED

表示		説明
PWR	点灯	正常に給電されている状態です。
Status	低速点滅	正常モードで動作中です。
	高速点滅	復旧モードまたは異常状態です。
WiFi	消灯	WiFi が無効になっています。
	点灯	WiFi が有効になっています。
	点滅	WiFi 経由でデータが送受信されています。
Sub-6	消灯	5G が無効になっています。
	点灯	5G モードで通信中です。
4G LTE	消灯	LTE が無効になっています。
	点灯	LTE モードで通信中です。
SIM A	消灯	SIM が挿入されていないか、使用されていません。
	点灯	SIM A スロットが使用中です。
SIM B	消灯	SIM が挿入されていないか、使用されていません。
	点灯	SIM B スロットが使用中です。
SIGNAL	点灯	信号強度が 0～30%です。
SIGNAL	点灯	信号強度が 31～60%です。
SIGNAL	点灯	信号強度が 61～100%です。

5.2. 前面

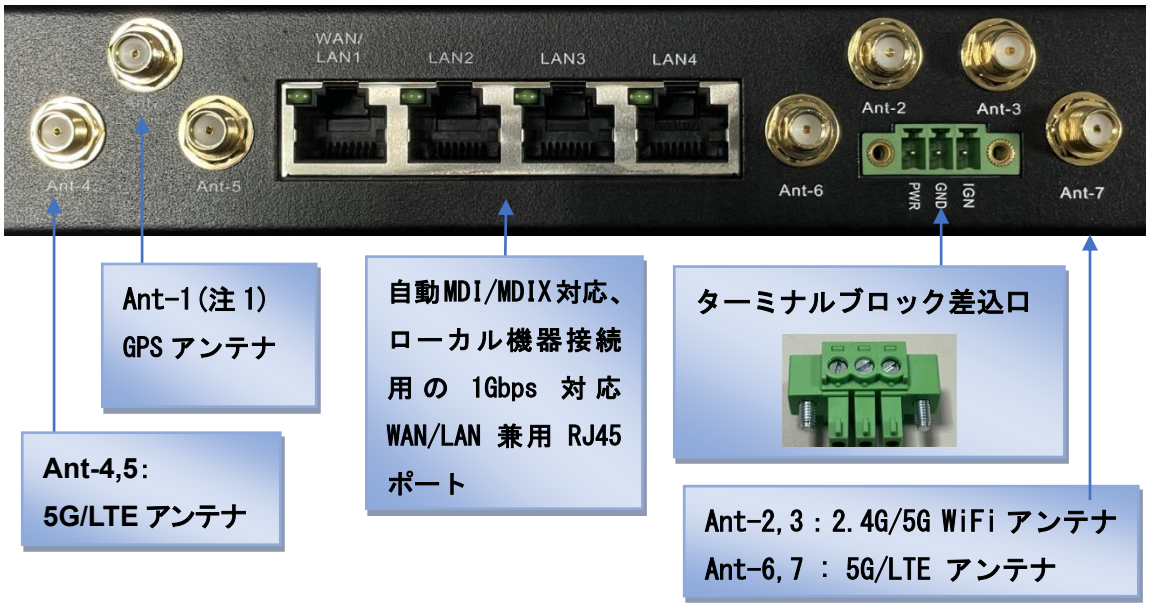


リセットボタン

リセットボタンを10秒ほど長押しするとStatusランプが高速点滅します。

その状態でリセットボタンを離すと、設定が初期化されます。

5.3. 背面



(注意 1) GPS アンテナは付属しておりません

5.4. SIM カードの取り付け/取り外し方法

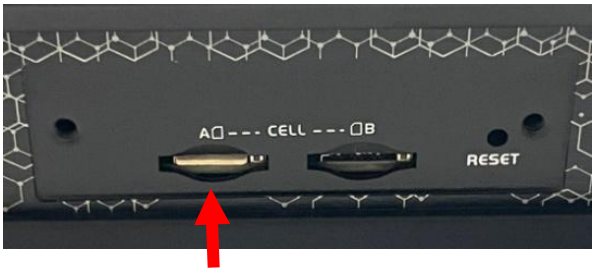
SIM カードの取り付け/取り外し方法について説明します。

※SIM カードの着脱は電源を落とした状態で行ってください。

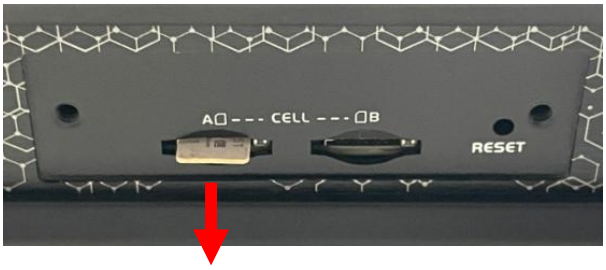
◆ SIM カバーを取り外します。



◆ SIM カードを挿入します。



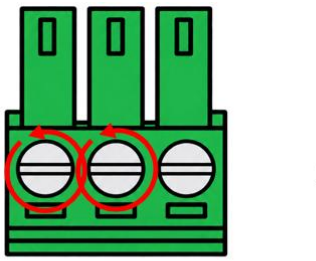
◆ SIM を押し込むと取り外すことができます。

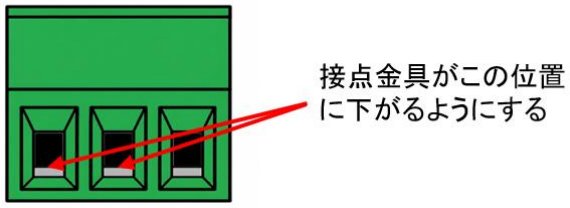


5.5. 電源の接続

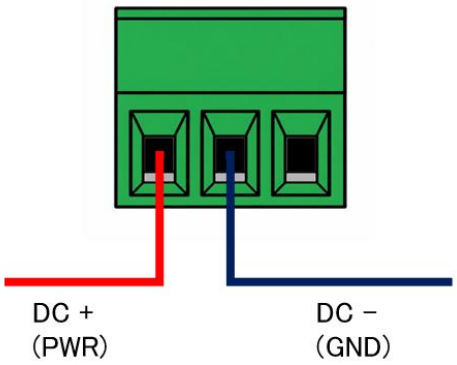
電源用ターミナルブロックと電源の接続について説明します。

1) 接続する端子の上部ネジを左に回し、内部の接点金具を下げてください。
端子は左から PWR、GND、IGN です。IGN 端子はイグニッションセンス機能で使用します。
（[12.4 電源制御] 参照）

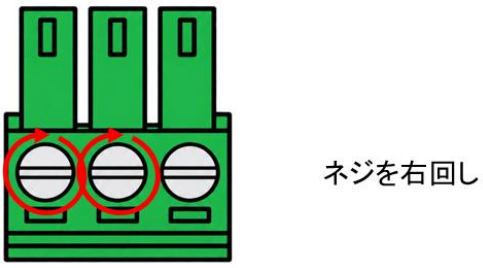




2) 電源ケーブルを、極性を間違えない様に電源用ターミナルブロックの穴に挿入してください。



3) 上部ネジを右に回し、電源ケーブルが外れない様に固定してください。



4) 本体へ電源用ターミナルブロックを接続します。

注意事項

DC 電源の極性を間違えると、本機及び電源の破損・発煙・発火の原因になりますので、電源を入れる前に再度確認してください。

6. WEB GUI での設定について

6.1. Web GUI へのアクセス

6.1.1. PC システム要件

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

6.1.2. ログイン初期設定

項目	初期値
IP アドレス	192.168.123.254
ユーザー名	admin
パスワード	admin

6.1.3. ログイン手順

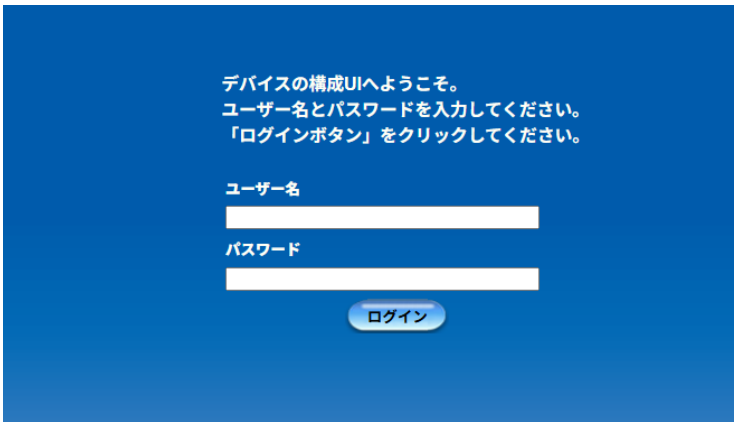
◆ 接続する PC の IP アドレスを 192.168.123.0/24 のネットワークの 192.168.123.254 以外の IP アドレスに設定します。

◆ PC を本機の LAN ポートに接続します。

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

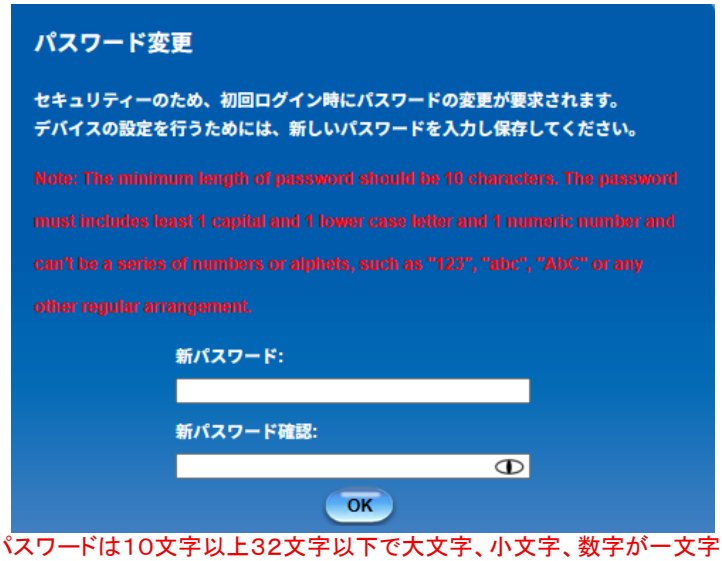


◆ ログイン画面が表示されますので、ユーザー名とパスワード[admin]を入力して、ログイン を クリックします。



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

◆ 初回ログイン時に管理パスワードの変更を行います。



パスワードは10文字以上32文字以下で大文字、小文字、数字が一文字以上含まれている必要があります。
また、123, abc, AbC のような連続した数字や文字列は使用できません。

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



6.1.4. Web 表示言語の変更

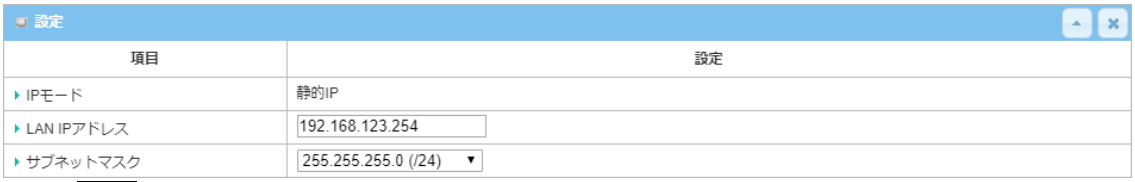
◆ 工場出荷時点では WEB GUI は日本語表示です。ページ右上の言語を変更することで表記言語を変更できます。



6.2. LAN 側 IP アドレスの設定

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

◆ LAN IP アドレスとサブネットマスクを設定します。



◆ 保存をクリックします。

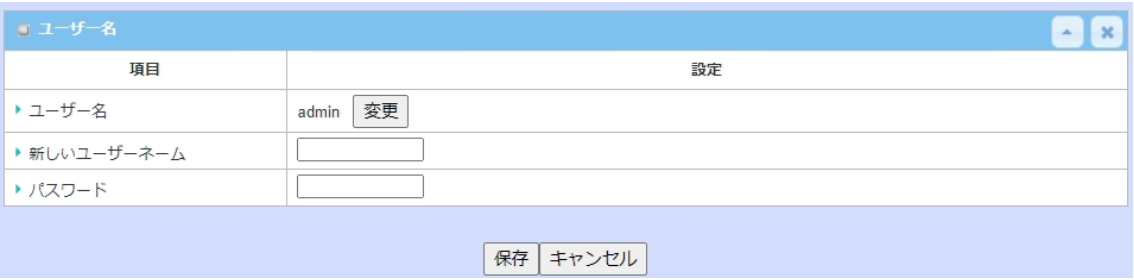
◆ 保存後に新しい IP アドレスでログインし直す必要があります。

6.3. 管理ユーザー名の変更

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

◆ [ユーザー名]の変更を押し、管理用の新しいユーザー名と現在のパスワードを入力します。

◆ 保存をクリックします。



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

✧ 基本設定編

本章では、本機を 5G/LTE 回線でインターネットに接続するための設定について説明します。



7. モバイル NET(5G/LTE)の設定

モバイル NET(5G/LTE)回線経由でインターネットに接続するための設定を行います。

7.1. 物理インターフェイスの設定

注）本設定は工場出荷時のままで問題ありません。

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



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

◆ WAN-1 の編集をクリックします。



（注１） WAN-1 の動作モードは[常にオン]となります。

◆ [物理インターフェイス]を[モバイル NET]に設定します。ISP(プロバイダ)により VLAN タギングが指定されている場合は、有効をチェックして VLAN ID を入力します。

◆ 保存をクリックします。

7.2. モバイル NET パラメータの設定

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

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	モバイル NET(5G/LTE)	常にオン	モバイル NET	編集
WAN-2	-	無効	-	編集
WAN-3	-	無効	-	編集

◆ WAN-1 の編集をクリックします。

◆ [モバイル NET WAN タイプ構成]を[SIM-A のみ]に設定します。

モバイル NET WANタイプ構成

項目	設定
優先SIMカード	SIM-Aのみ
自動機内モード	有効

（注１） SIM スロット A に SIM が挿入されていることを確認してください。
（注２） 自動機内モードは本機では未サポートです。

◆ [SIM-A カードとの接続]をご契約の回線の指定に合わせて設定します。

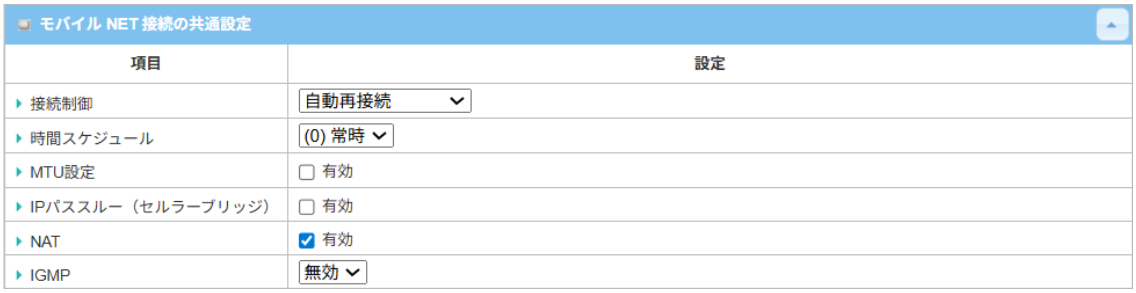
SIM-Aカードとの接続

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	自動
IPモード	動的IP
プライマリーDNS	(選択的)
セカンダリーDNS	(選択的)
ローミング	有効

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

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

◆ [モバイル NET 接続の共通設定]の設定をします。



項目	説明
接続制御	自動再接続を選択します。
時間スケジュール	(0)常時固定です。
MTU 設定	☑をはずし無効にします。
IP パススルー	☑をはずし無効にします。
NAT	☑を入れ有効にします。
IGMP	無効を選択します。

◆ [ネットワークの監視構成]を設定します。



項目	説明
ネットワーク監視構成	☑をいれて有効化します。本設定は、基地局から切断された場合の復旧に必要です。ただし、通信量が連続して多い場合に本機能が正常に動作せず、切断→接続を繰り返すことがあります。その場合には本機能を無効にしてください。
チェック方法	工場出荷時設定です。
読み込み確認	
クエリ間隔	
レイテンシーしきい値	工場出荷時設定です。
失敗しきい値	
ターゲット1	
ターゲット2	

ページ最後の保存をクリックして設定を保存してください。

✧ 応用設定編

これ以降は詳細な設定について説明します。

8. 基本ネットワーク

基本ネットワーク設定について説明します。

8.1. WAN およびアップリンク

本機は 3 つの WAN インタフェースを備えており、インターネットへの接続を可能にします。本項目では、WAN の物理インタフェースおよびインターネットにアクセスするための様々な設定を行うことができます。各 WAN インタフェースに対して、物理インタフェースを選択し、その後インターネットに接続するための情報を設定します。



8.1.1. 物理インターフェイスリスト

物理インターフェイスリスト

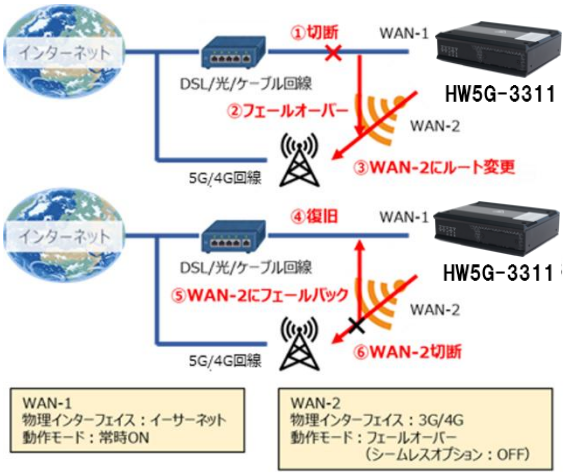
インターフェイス名	物理インターフェイス	動作モード	アクション
WAN-1	モバイル NET(5G/LTE)	常にオン	編集
WAN-2	-	無効	編集
WAN-3	-	無効	編集

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

8.1.2. フェールオーバー機能

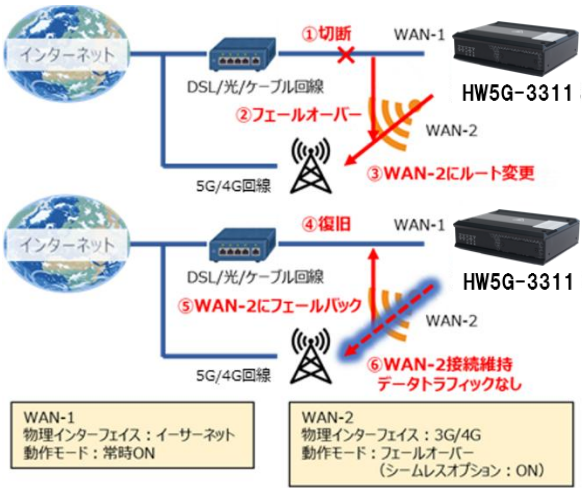
物理インタフェースWAN-1（主インタフェース）に回線の障害などが発生し通信が遮断した時に、WAN-2（副インタフェース）に自動的に切り替える機能がフェールオーバー機能です。
WAN-1 にイーサネットを WAN-2 にモバイル NET を割り当てたとすると、以下のような動作をします。

1) フェールオーバー（シームレスオプション：OFF）



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

2) フェールオーバー（シームレスオプション：ON）



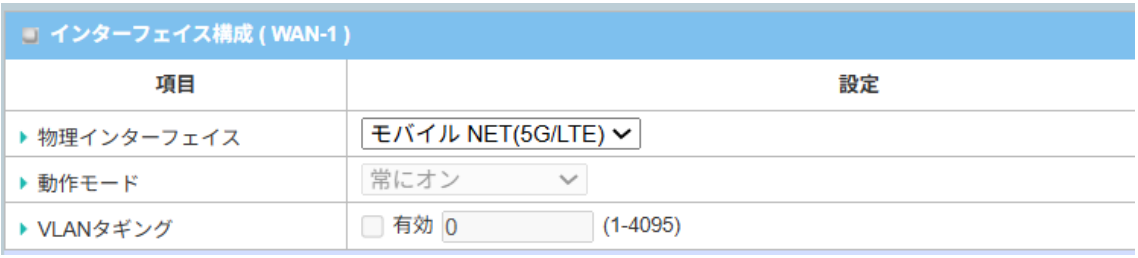
シームレスオプションを ON に設定すると、主回線である WAN-1 と同じく副回線の WAN-2も同時に接続を開始します。この時に WAN-2 でデータの送受信は行われません。WAN-1 が切断されたときに、WAN-2 のデータ送受信を開始します。WAN-1 復旧時にはデータ送受信が WAN-1 側に移行しますが、WAN-2 は接続を維持します。このように、WAN-2 のバックアップ接続動作が無い分フェールオーバーにかかる切り替え時間が短縮できます。

（注１） ネットワークの監視は接続設定内の[ネットワーク監視構成]の設定により実行されます。切断検出時間は 4 秒以上となります。
（注２） シームレスオプション OFF の場合は 5G/4G の接続を実行するため、WAN-2 のデータ送受信開始まで最低でも1分以上必要となります。
（注３） フェールオーバーはルート変更を伴うため、データ送受信を継続できないことがあります。この場合はデータ送受信のリスタートを実施してください。

8.1.3. 物理インタフェースの設定

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

◆ 物理インターフェイスリスト内のいずれかの WAN の編集をクリックします。



項目	説明
物理インターフェイス	設定する物理インタフェースを以下から選択します。 ・イーサネット ・モバイル NET(5G/LTE) ・WiFi モジュール 1
動作モード	動作モードを以下から選択します。(WAN-2, WAN-3 のみ) ◆無効 :編集中の WAN インタフェースを無効にします。 ◆ 常に有効:編集中の WAN インタフェースを常に有効にします。 ◆フェールオーバー:バックアップの接続として動作します。主回線の接続が切断された場合に有効になります。 さらに、”シームレス”にチェックをすると、副回線はアクティブ状態でスタンバイし、主回線の接続が切断された場合に、より短時間で切り替わります。
VLAN タギング	ISP(プロバイダ)によって VLAN タギング設定が必要な時に、有効にして契約に合わせた VLAN ID(1～4094)を入力します。

8.1.4. 接続設定

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

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

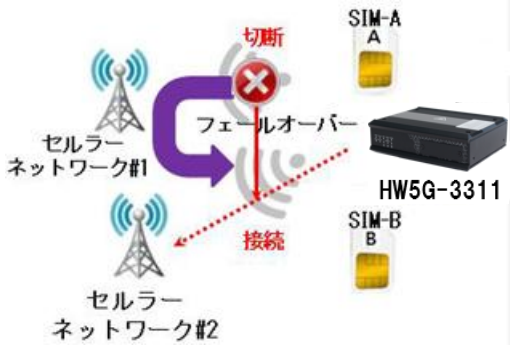
◆ インターネット接続リスト内の編集したい WAN インタフェースの編集をクリックします。

8.1.5. WAN インタフェース：モバイル NET(5G/LTE)の接続設定

8.1.5.1. デュアル SIM フェールオーバー機能について

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

1) SIM-A /SIM-B 優先あり、フェールバック無効



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

2) SIM-A /SIM-B 優先あり、フェールバック有効



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

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

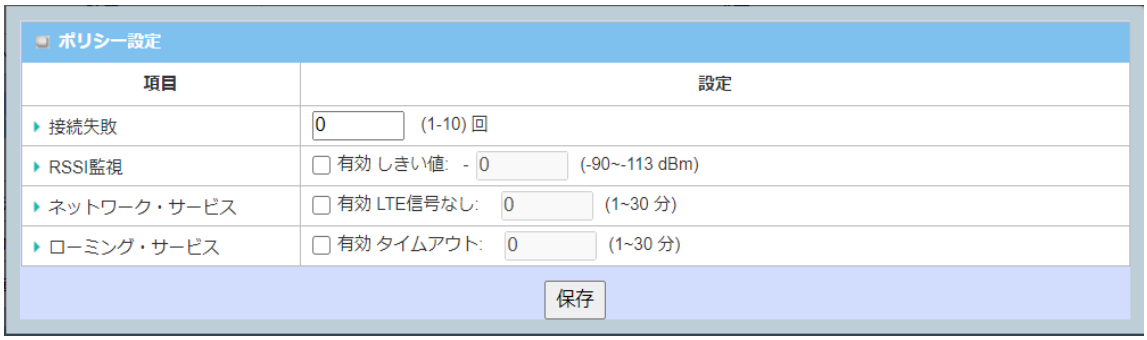
8.1.5.2. インターネット接続構成およびモバイル NET の WAN タイプ[Cellular WAN Type]構成



項目	説明
WAN タイプ	[モバイル NET]のみ選択可能です。
優先 SIM カード	◆ [SIM-A は優先度が高い] 又は [SIM-B は優先度が高い]を選択 SIM カードスロットの優先順位を設定します。本設定の詳細はデュアル SIM フェールオーバー機能（8.1.5.1 項）を参照してください。 ◆ [SIM-A のみ] 又は [SIM-B のみ] を選択 選択した SIM スロットの SIM を使い接続をします。
自動機内モード	本機ではサポートしておりません。チェックを外して無効にしてください。
SIM 転換のポリシー	SIM-A/B の切り替えのためのポリシーが設定できます。[SIM-A は優先度が高い]または[SIM-B は優先度が高い]を選択した場合に表示されます。

8.1.5.3. SIM 転換のポリシーの設定

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



項目	説明
接続失敗	SIM 間フェールオーバーを行うまでの、連続接続失敗回数を設定します。接続に設定した回数連続で失敗した時点でもう一方の SIM へ切り替えます。0の時はフェールオーバーしません。
RSSI 監視	[有効]にチェックを入れると、接続中のモバイル NET の受信レベルが設定値(-113～-90)より低くなると、 優先順位の高い SIM スロットから、優先順位の低い SIM スロットへ切り替えます。無効にすると、受信レベルを監視しません。
ネットワーク･サービス	[有効]にチェックを入れると、モバイル NET 信号が設定時間（1～30 分）内に受信できないときに、優先順位の高い SIM から低い SIM に転換し、接続を実行します。 無効にすると、即時切替えします。
ローミング･サービス	国内使用専用機であるため本機能は使用できません。無効にしてください。

8.1.5.4. SIM-A カードとの接続/SIM-B カードとの接続

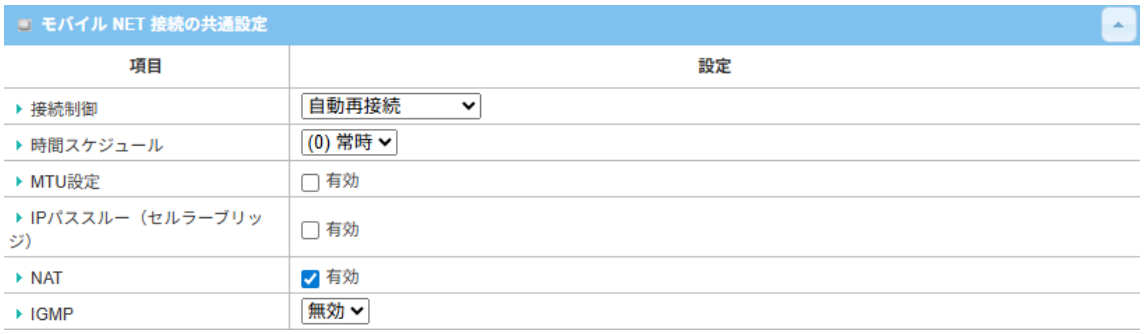
モバイル NET 回線のご契約に合わせて、設定するパラメータです。



項目	説明
ネットワークタイプ	自動：5G/LTE を基地局に合わせて自動選択します。 LTE のみ：LTE の基地局のみと LTE で接続します。 5G SA：5G SA の基地局のみと接続します。 5G NSA：5G NSA の基地局のみと接続します。
ダイアルアップ プロファイル	手動設定、自動検出から選択します。手動設定にすることを推奨しております。本機は APN プロファイルリストをサポートしておりません。
APN	APN を入力します。（ご契約に合わせて設定します）
IP タイプ	IP タイプを選択します。（ご契約に合わせて設定します）
PIN コード	PIN コードを入力します。（PIN コードを設定した SIM カードをお使いの場合、設定します）
ダイヤルナンバー	接続先ダイヤルナンバーを入力します。（ご契約に合わせて設定します）
アカウント	認証に使用するアカウントとパスワードを入力します。
パスワード	
認証	認証方式を選択します。（ご契約に合わせて設定します）
IP モード	動的 IP、静的 IP から選択します。（ご契約に合わせて設定します） 静的 IP を選択すると、IP アドレス、IP サブネットマスク、デフォルトゲートウェイの欄が表示されますので、ご契約に合わせて設定してください。
プライマリ DNS	DNS の設定を入力します。（ご契約に合わせて設定します）
セカンダリ DNS	
ローミング	日本国内使用専用機器のため、本機能はサポートしておりません。

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

8.1.5.5. モバイル NET 接続の共有設定



項目	説明
接続制御	インターネット接続の制御方法を選択します。 ◆自動再接続：常時インターネットに接続します。（推奨） ◆オンデマンド接続：インターネットアクセスの要求があるときに接続します。 ◆手動接続：必要な時に接続します。
時間スケジュール	(0)常時固定です。
MTU 設定	MTU を 512～1500 の範囲で指定できます。
IP パススルー	有効にするとブリッジモードで動作し、LAN 端末 1 台に対して直接 WAN IP を割り当てます。 このため、接続できる LAN 端末は1台のみとなります。 （注１） WAN-1 に設定されているときのみ利用可能です。 （注２） ブリッジモードであるため NAT 機能は利用できません。
NAT	NAT（NAPT）の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。

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

◆ [保存]をクリックして設定を登録します。必要があれば 8.1.8［ネットワーク監視構成］に進みます。

8.1.6. WAN インタフェース :WiFi モジュール 1 の設定

Wi-Fi モジュールは、外部の WiFi ネットワークを WAN 回線として使用するインタフェースです。接続先の SSID、認証方式、パスワードなどを設定することで、本機を外部の Wi-Fi アクセスポイントに接続できます。

本機能は IEEE 802.11b/g/n/ax および IEEE802.11a/n/ac/ax に対応しており、インフラストラクチャモードで接続します。

8.1.6.1. インターネット接続構成



項目	説明
WAN タイプ	[アップリンク] のみ選択可能です。

8.1.6.2. WiFi Uplink WAN Type Configuration



項目	説明
AP に接続	スキャンボタンをクリックすると、近隣の WiFi アップリンクのアクセスポイントを選択できます。また、プロファイルを作成することでも、アップリンクネットワークへ接続することができます。(詳細は 8.3.4 項アップリンクプロファイルを参照してください。)
ネットワークタイプ	WiFi アップリンク接続のネットワークタイプを[NAT Mode]または[NAT Disable]から選択します。 ◆NAT Mode:WiFi アップリンク接続で NAT 機能が有効になります。 ◆NAT Disable:NAT 機能が無効になります。アップリンクネットワークには一台の機器のみが参加できます。
IP モード	IP モードを静的 IPアドレスまたは動的IPアドレスから選択します。(接続する WiFi アップリンクネットワークに合わせて設定します。)
ホスト名	ホスト名を指定します。特に指定のない場合は空欄にします。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続:常時インターネットに接続します。 ◆オンデマンド接続:インターネットアクセスの要求があるときに接続します。

	◆手動接続：手動で必要な時に接続します。
マクシマムアイドルタイム	無通信状態になった時に自動的にインターネット接続を切断するまでの時間を指定します。値の範囲:300～86400
高速ローミング	国内使用専用機であるため本機能は使用できません。無効にしてください。
高速ローミングチャネル	

◆ 保存をクリックして設定を登録します。必要があれば 8.1.8［ネットワーク監視構成］に進みます。

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

8.1.6.3. WiFi アップリンク スキャン画面

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

Wireless APリスト

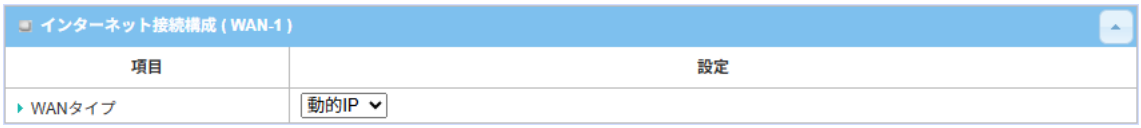
SSID	BSSID	チャネル	モード	セキュリティ	信号強度	アクション	
[redacted]	58:c1:[redacted]	1	b/g/nミックス	WPA2-PSK(AES)	65%	セキュリティキー:	適用
[redacted]	58:c1:[redacted]	1	b/g/nミックス	WPA2-PSK(AES)	76%	セキュリティキー:	適用
[redacted]	04:ab:[redacted]79	4	b/g/nミックス	WPA2-PSK(AES)	44%	セキュリティキー:	適用
Staff_2.4G	00:50:[redacted]ec	5	b/g/nミックス	WPA2-PSK(AES)	60%	セキュリティキー:	適用
HWL-2511-SS-[redacted]	00:03:[redacted]35	6	b/g/nミックス	WPA2-PSK(AES)	100%	セキュリティキー:	適用
[redacted]	00:19:[redacted]b6	9	b/g/nミックス	WPA2-PSK(AES)	81%	セキュリティキー:	適用
[redacted]	02:3a:[redacted]:3a	10	b/gミックス	(WEP)	81%	Open HEX キー 1 セキュリティキー:	適用
[redacted]	00:3a:[redacted]:3a	10	b/g/nミックス	WPA2-PSK(AES)	76%	セキュリティキー:	適用
[redacted]	6c:e4:[redacted]8b	11	b/g/nミックス	WPA2-PSK(AES)	39%	セキュリティキー:	適用

8.1.7. WAN インタフェース：イーサネットの接続設定

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

8.1.7.1. イーサネット WAN 設定

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

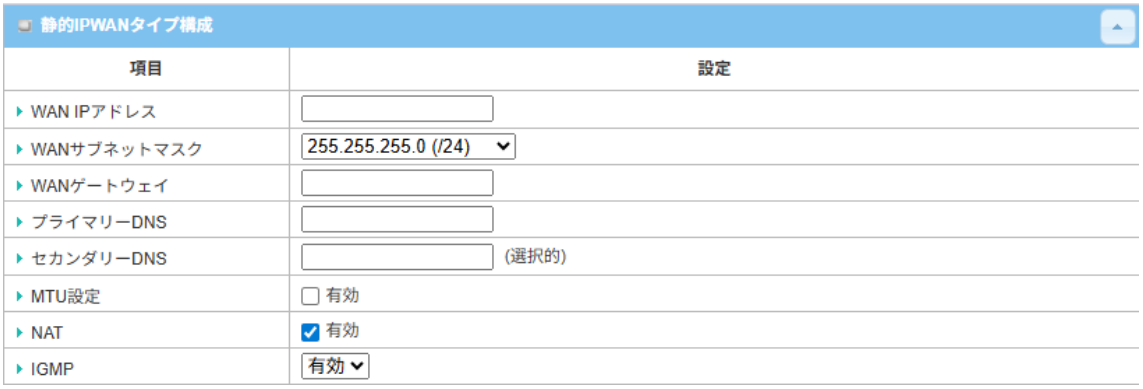


項目	説明
WAN タイプ	ISP（プロバイダ）の接続方式に合わせて WAN タイプを選択します。 ◆静的 IP：ISP（プロバイダ）から指定された WAN 側 IP アドレスを使用します。 ◆動的IP：DHCP サーバーから割り当てられる WAN 側 IP アドレスを使用します。本機の電源 ON の度にグルーバル IP アドレスが変わる可能性があります。 ◆PPPoE：PPP over Ethernet プロトコルで接続し、WAN 側IPアドレスはプロトコル上で割り当てられます。

◆ WAN タイプを選択後、タイプ毎に必要な設定を行います。

8.1.7.2. 静的IP WAN 設定

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



項目	説明
WAN IP アドレス	WAN ネットワークの IP アドレスを指定します。
WAN サブネットマスク	WAN ネットワークのサブネットマスクを指定します。
WAN ゲートウェイ	WAN ネットワークのゲートウェイIPアドレスを指定します。
プライマリーDNS	WAN ネットワークのプライマリ DNS の IP アドレスを指定します。
セカンダリーDNS	WAN ネットワークのセカンダリ DNS の IP アドレスを指定します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
NAT	NAT（NAPT）の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。

◆ 保存をクリックして設定を登録します。必要があれば 8.1.8 [ネットワーク監視構成]に進みます。

8.1.7.3. 動的IP WAN 設定

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



項目	説明
ホスト名	ホスト名を指定します。特に指定のない場合は空欄にします。
接続制御(注 1)	インターネット接続の制御方法を選択します。 ◆自動再接続:常時インターネットに接続します。(推奨) ◆オンデマンド接続:インターネットアクセスの要求があるときに接続します。 ◆手動接続:必要な時に接続します。
MTU 設定	有効をチェックして、MTU を 512～1500 の範囲で指定します。
NAT	NAT(NAPT)の有効/無効を設定します。
IGMP	IGMPモニタリングおよびIGMPプロキシ機能の有効/無効を設定します。

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

◆ [保存]をクリックして設定を登録します。必要があれば 8.1.8 [ネットワーク監視構成]に進みます。

8.1.7.4. PPPoE WAN 設定

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



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

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

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

8.1.8. ネットワーク監視構成の設定

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



項目	説明
ネットワーク監視構成	[有効]にチェックをすると、ネットワーク監視機能が動作します。
チェック方法	ネットワークの監視方法を選択します。 ◆DNS クエリ:DNS クエリを使用して、ターゲットの DNS サーバーに問合せパケットを送信します。 ◆ICMP チェック:ターゲットに ICMP パケットを送信します。
読み込み確認	[有効]にチェックすると、データ伝送によりネットワークが混雑しているときに、未応答の DNS クエリまたは ICMP 要求を無視することができます。この機能により、誤ったリンクダウン判断を防止することができます。
クエリ間隔	DNS クエリまたは ICMP 要求の送信間隔を指定します。 値の範囲は 2 秒以上です。
レイテンシーしきい値	DNS クエリまたは ICMP 要求の応答遅延しきい値を指定します。値の範囲は 2000～3000ms です。
失敗しきい値	DNS クエリまたは ICMP 要求の失敗限界回数を指定します。値の範囲は1～40 回です。
ターゲット 1	DNS 問合せまたは ICMP 要求を送信する最初のターゲットホストを選択します。 ◆DNS1:WAN のプライマリーDNS を使用します。 ◆DNS2:WAN のセカンダリーDNS を使用します。 ◆他のホスト:ターゲットになるホストの IP アドレスを指定します。DNS クエリを使用する場合は、DNS サーバーである必要があります。

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

◆ 保存をクリックして設定を登録します。

8.1.8.1. ネットワーク監視構成の使用上の注意点

ネットワーク監視構成はネットワーク越しのターゲットホストからの応答を監視することで、回線の疎通を判定しています。このターゲットホストからの応答が、高負荷時は応答遅延が判定閾値を超える場合があります。その場合、ネットワーク異常と誤って判定してしまい、フェールオーバーや回線断が発生します。この様な意図しない回線切断が発生する場合や大容量・高速データ通信を連続して行う場合は、ネットワーク監視機能を無効に設定してください。

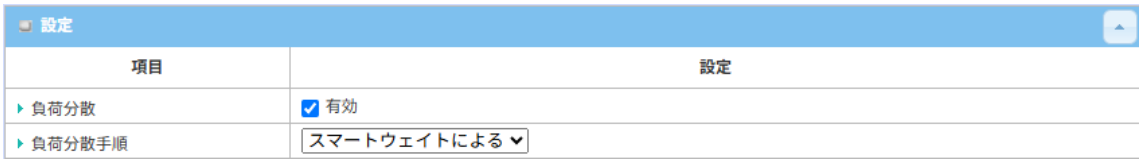
8.1.9. 負荷分散

本機はモバイル NET、WiFi アップリンク、および、イーサネット WAN インタフェースを使用した通信が可能で、各々のインタフェースへの負荷を分散させることができます。負荷分散の方法として[スマートウェイトによる]、[特定のウェイトによる]、および[ユーザーポリシーによる]から選択することができます。

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

8.1.9.1. 負荷分散の設定

負荷分散機能の有効/無効と負荷分散の設定を行います。

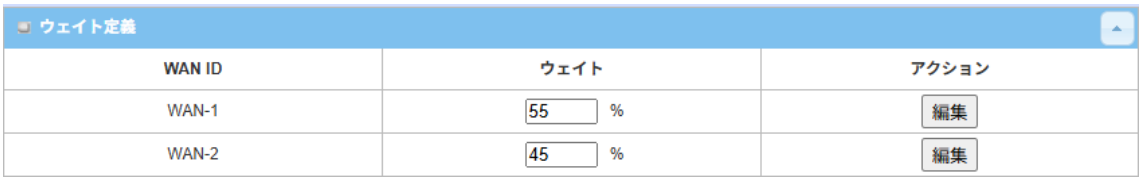


項目	説明
負荷分散	[有効]にチェックをすると、負荷分散機能が動作します。
負荷分散手順	負荷分散手順を選択します。負荷分散手順には以下の 3 つの方法があります。 ◆スマートウェイトによる：スマートウェイトアルゴリズムに基づいて、自動的に負荷分散機能を実行します。 ◆特定のウェイトによる：各 WAN インタフェースへ指定した比率に基づいて、各 WAN へ転送するセッションの比率を調整します。 ◆ユーザーポリシーによる：ユーザーが定義したポリシーに基づいてトラフィックを分散します。

◆ 保存をクリックして設定を保存します。

8.1.9.2. 特定のウェイトの設定

負荷分散手順で[特定のウェイトによる]を選択した場合は、各 WAN の負荷分散比率を指定する必要があります。



項目	説明
WAN ID	利用可能な WAN インタフェースです。
ウェイト	編集をクリックして各インタフェースの分散比率を指定します。 値の範囲は1～99 で、全ての比率の合計が 100%になるように設定する必要があります。

8.1.9.3. ユーザーポリシーリストの追加・編集

負荷分散手順で[ユーザーによる]を選択した場合は、[ユーザーポリシーリスト]が表示されます。



◆ 追加または編集をクリックすると[ユーザーポリシー構成]画面が表示されます。



項目	説明
送信元 IP アドレス	送信元 IP アドレスを指定します。 指定方法として以下の 4 つから選択することができます。 ◆任意：特定の送信元 IP アドレスを指定しません。すべての送信元IPアドレスが対象になります。 ◆サブネット：送信元 IP アドレスのサブネットをIPv4形式/サブネットマスク（例：192.168.123.0/24）で指定します。 ◆IP 範囲：送信元 IP アドレスをIPv4形式にて範囲で指定します。 ◆単一 IP：単一の送信元IPアドレスをIPv4形式にて指定します。

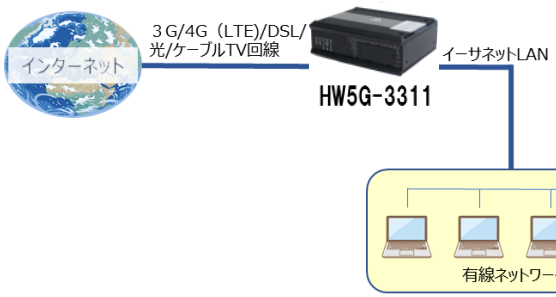
項目	説明
宛先 IP アドレス	宛先 IP アドレスを指定します。 指定方法として以下の 5 つから選択することができます。 ◆任意：特定の宛先 IP アドレスを指定しません。すべての宛先IPアドレスが対象になります。 ◆サブネット：宛先 IP アドレスのサブネットをIPv4形式/サブネットマスク（例：192.168.123.0/24）で指定します。 ◆IP 範囲：宛先 IP アドレスをIPv4形式にて範囲で指定します。 ◆単一 IP：単一の宛先IPアドレスをIPv4形式にて指定します。 ◆ドメイン名：宛先をドメイン名で指定します。
宛先ポート	宛先ポートを指定します。指定方法として以下の 4 つから選択することができます。 ◆全部：特定の宛先ポートを指定しません。すべての宛先ポートが対象になります。 ◆ポート範囲：宛先ポートを範囲で指定します。 ◆単一ポート：単一の宛先ポートを指定します。 ◆既知のアプリケーション：ドロップダウンリストで定義されている既知のアプリケーションのサービスポートを選択します。
プロトコル	[両方]、[TCP]および[UDP]から選択します。
WAN インタフェース	本ポリシーで使用する WAN インタフェースを選択します。ドロップダウンリストには選択可能な WAN インタフェースが表示されます。
ポリシー	[有効]にチェックをすると、本ユーザーポリシーが有効になります。

◆ 保存をクリックして、ルールを登録します。設定したルールが[ユーザーポリシーリスト]に表示されます。

8. 2. LAN および VLAN

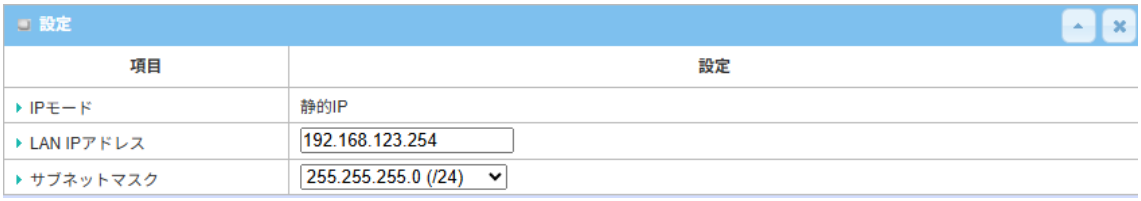
LAN（ローカルエリアネットワーク）関連の設定を行います。

8.2.1. イーサネット LAN



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

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



項目	説明
IP モード	LAN IP モードが表示されます。
LAN IP アドレス	本機の LAN IP アドレスを入力します。本機を介したネットワーク通信をする時、LAN 内の端末はこの LAN IP アドレスをデフォルトゲートウェイとして設定する必要があります。
サブネットマスク	ドロップダウンリストから、LAN IP アドレスの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)。

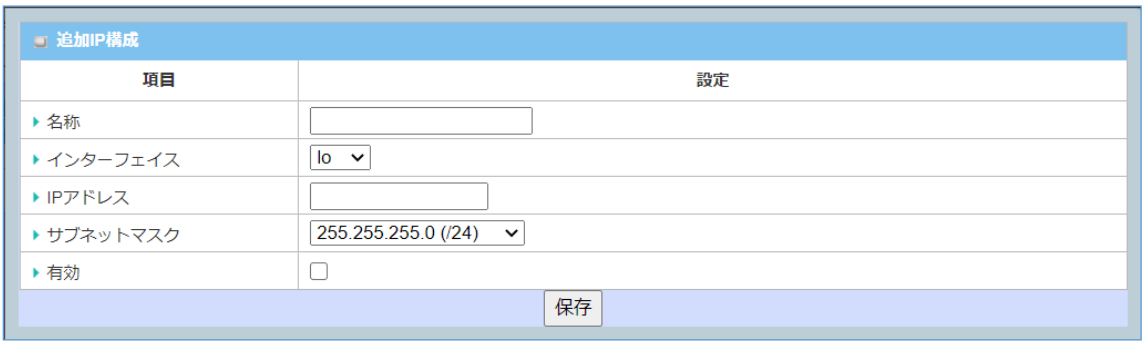
◆ 保存をクリックして設定を登録します。

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

8.2.2. 追加 IP 機能

本機は、LAN IP エイリアス機能を搭載しています。本ゲートウェイに追加 LAN IP を設定し、その追加 IP を使って、本機にアクセスすることができます。





◆ 追加または編集をクリックすると[IP 追加構成]画面が表示されます。

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

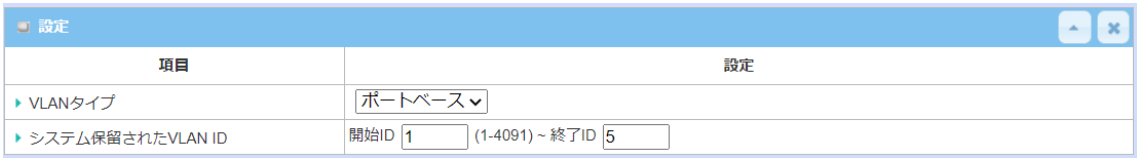
8.2.3. 仮想 LAN(VLAN)

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

8.2.4. 仮想 LAN(VLAN)の設定

ポートベースの VLAN を使用することで、LAN ポートのグルーピングなどがポート単位で設定できます。

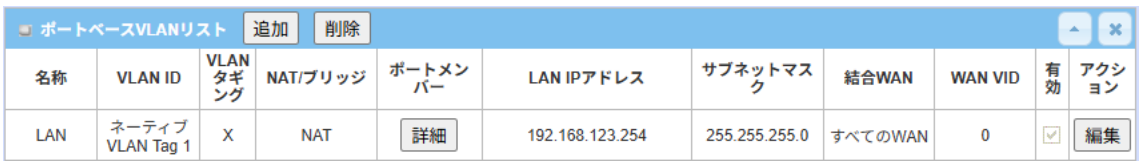
◆ 画面左側のメニューから、基本ネットワーク⇒LAN および VLAN⇒仮想 LAN の順にクリックします。



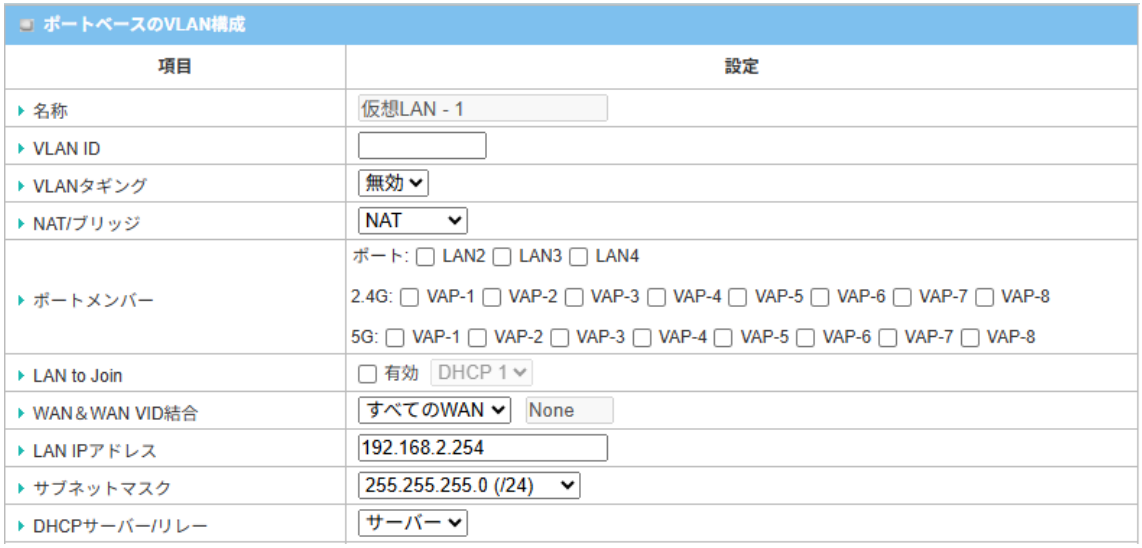
◆ ポートベースまたはタグベース VLAN リストにルールを追加し、適用をクリックして設定を有効にします。

項目	説明
VLAN タイプ	VLAN タイプを選択します。 ポートベース：各 LAN ポート/VAP に VLAN ID を指定します。 タグベース：選択すると[タッグベース VLAN リスト]テーブル画面に切り替わります。VLAN ID を追加し、この VLAN ID のメンバーと DHCP サーバーを指定します。
システム保留された VLAN ID	システムで利用する VLAN ID 範囲を指定します。設定で利用する VLAN ID は、この範囲外の ID を指定してください。 値の範囲：1~4091

8.2.4.1. ポートベース VLAN ルールの設定



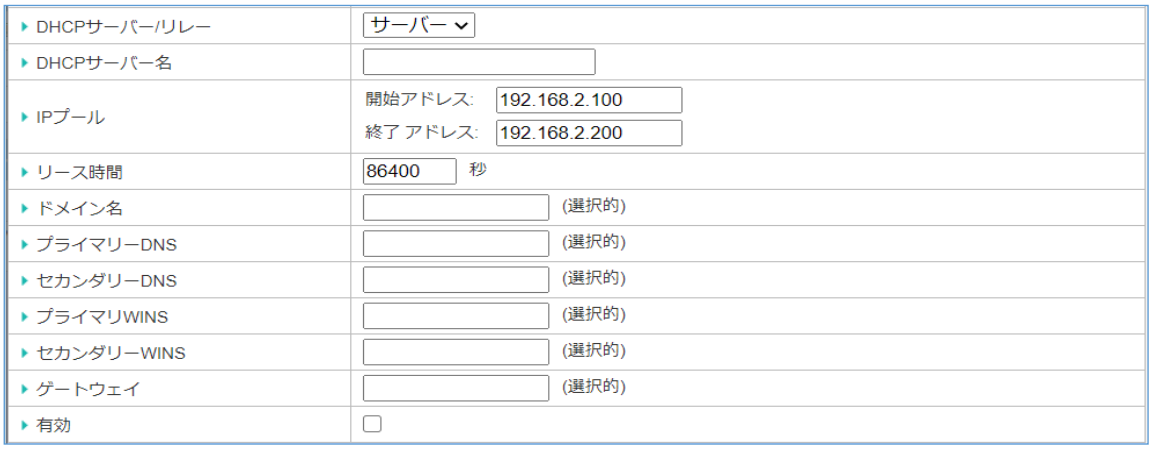
ポートベース VLAN リストにある追加または編集をクリックしルールを入力します。



項目	説明
名称	このルールの名称を表示します。名称は変更できません。
VLAN ID	VLAN ID 番号を定義します。範囲は 1～4094 です。
VLAN タギング	[有効]を選択すると、ルールは[VLAN ID]および[ポートメンバー]の構成に従ってアクティブになります。 [無効]を選択すると、ルールは[ポートメンバー]の構成に従ってアクティブになります。
NAT/ブリッジ	ルールの[NAT]モードまたは[ブリッジ]モードを選択します。
ポートメンバー	ルールに追加する LAN ポートと VAP を選択します。
LAN to Join	[有効]をチェックしこの VLAN グループで使用する DHCP サーバーを選択します。[有効]を選択すると、これ以降の項目は入力できなくなります。
WAN＆WAN VID 結合	インターネットへのアクセスを許可する[WAN-1]、[WAN-2]、[WAN-3]、または[すべての WAN]を選択します。 （注１） [Bridge(ブリッジ)]モードが選択されている場合は、WAN を選択して、VID を入力する必要があります。
LAN IP アドレス	このルールが使用する DHCP サーバーの[IP アドレス]を割り当てます。この IP アドレスは、本機の IP アドレスです。
サブネットマスク	DHCP サーバーの[サブネットマスク]を選択します。

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

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



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

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



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

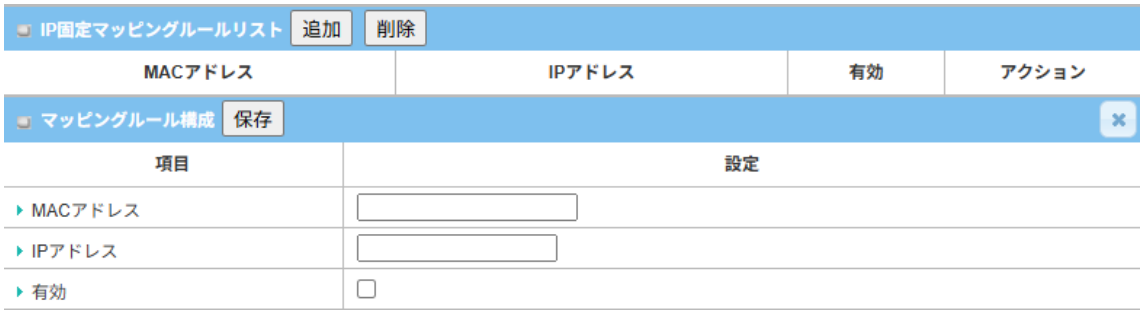
◆ 有効項目にチェックをいれ、本ルールを有効にします。

◆ 保存をクリックしルールを登録します。登録すると〔ポートベース VLAN ルール〕に内容が表示されます。

8.2.4.2. IP 固定マッピングルールの設定

MAC アドレスごとの固定 IP アドレスを設定することができます。

◆ IP 固定マッピングルールリストにある追加または編集をクリックしルールを入力します



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

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

8.2.4.3. ポートベース VLAN 間グループルーティング

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



◆ 各項目の編集をクリックしグループルーティング設定内容を編集します。

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

◆ 保存をクリックしルールを登録します。

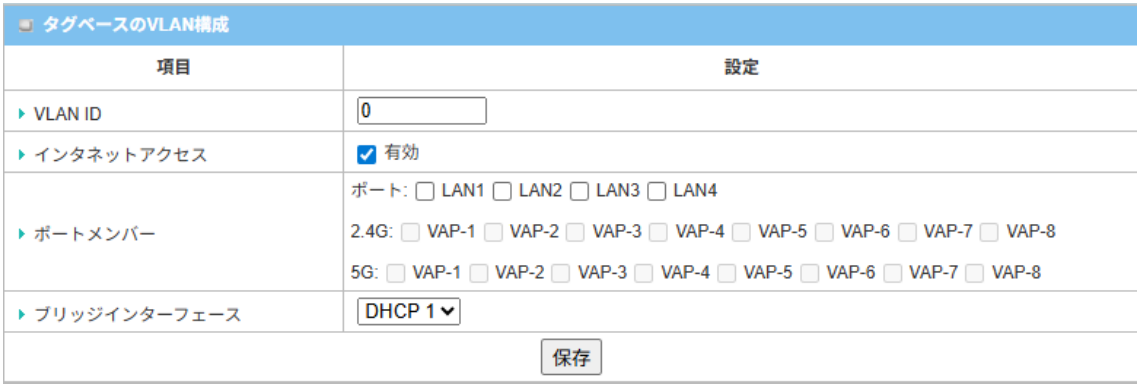
8.2.4.4. タッグベース VLAN ルールの設定

タッグベースの VLAN を使用することで、LAN ポートのグルーピングなどが VLAN ID 単位で設定できます。



◆ 仮想 LAN の設定画面にある[VLAN タイプ]でタッグベースを選択すると、タッグベース VLAN リストが表示されます。追加または編集をクリックしてルールを追加します。

◆ [タグベースの VLAN 構成]にルールを設定します。



項目	説明
VLAN ID	VLAN ID 番号を指定します。
インタネットアクセス	[有効]にチェックを入れると、VLAN グループのメンバーがインターネットにアクセスできるようになります。
ポートメンバー	各ポートにチェックを入れると、VLAN グループに参加することができます。
ブリッジ インターフェース	事前に登録された DHCP サーバーを選択します。(DHCP サーバーの登録については 8.2.5 項を参照してください。)

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

8.2.5. DHCP サーバー

本機は DHCP サーバー機能を搭載しています。また、VLAN グループからの DHCP 要求に応答するために最大 4 つの DHCP サーバーを構築できます（詳細は 8.2.3 項仮想 LAN を参照してください）。また、工場出荷時には、本機の LAN と同一サブネットで、末尾 100～200 の IP アドレスを配布する DHCP サーバー設定が登録されています。

8.2.5.1. DHCP サーバーリスト

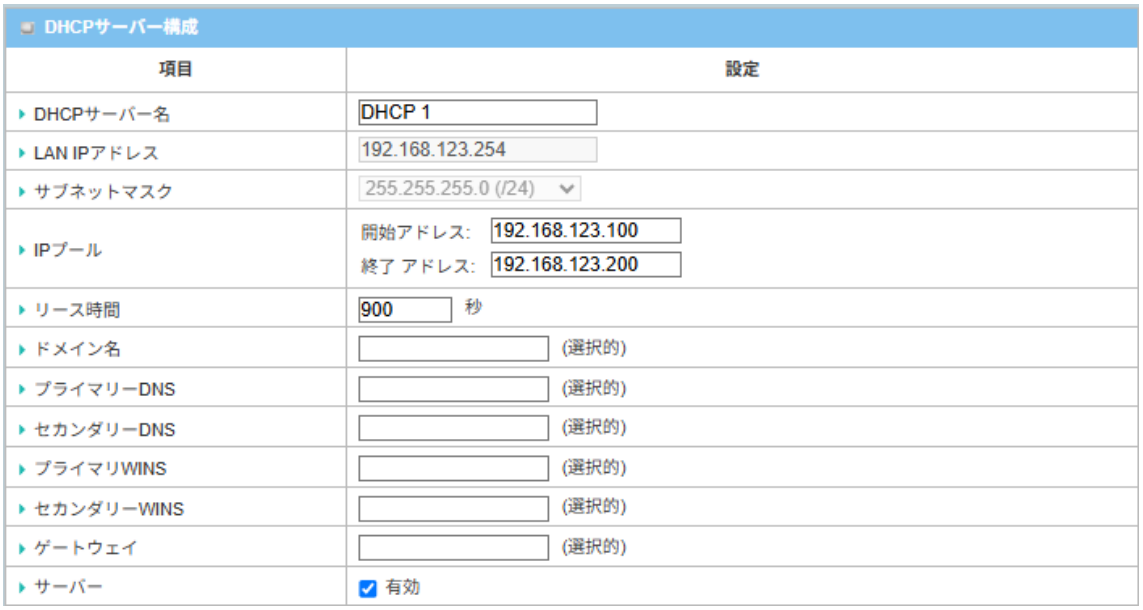
◆ 画面左側のメニューから、基本ネットワーク⇒LAN および VLAN⇒DHCP サーバーの順にクリックします。



◆ DHCP サーバーリストに DHCP ルールを追加/編集/登録することで、LAN ポートに接続された IP 機器に IP アドレス、サブネットマスクの割当とデフォルトゲートウェイや DNS サーバーアドレスの通知を行うことができます。

8.2.5.2. DHCP サーバーの設定

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



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

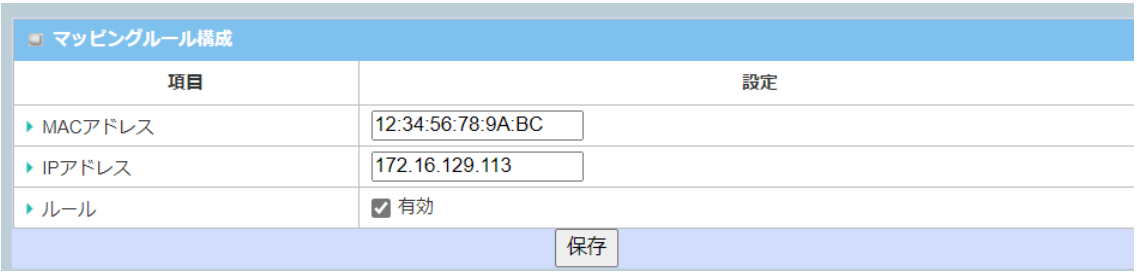
◆ 保存をクリックして設定を登録します。登録した内容が DHCP サーバーリストに表示されます。

8.2.5.3. IP 固定マッピングルールの設定

MAC アドレスにより固定 IP アドレスを割り当てることができます。

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





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

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

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

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

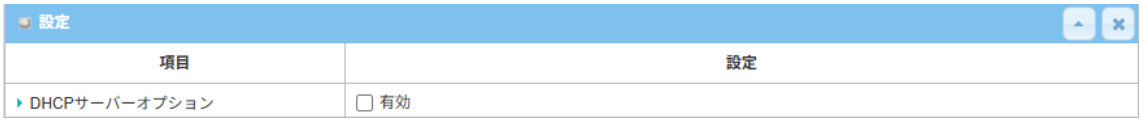
◆ DHCP サーバーリストにある DHCP クライアントリストをクリックすると、
本機が DHCP で割り当てている機器の情報が表示されます。



◆ マッピングルールにコピーする場合は、登録する IP 機器のアクション欄にチェックを入れ、固定マッピングにコピーをクリックすると、マッピングリストに登録されます。

8.2.5.5. DHCP サーバーオプションの有効/無効（未サポート）

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



項目	説明
DHCP サーバーオプション	有効にする場合に☑します。

DHCP オプション番号

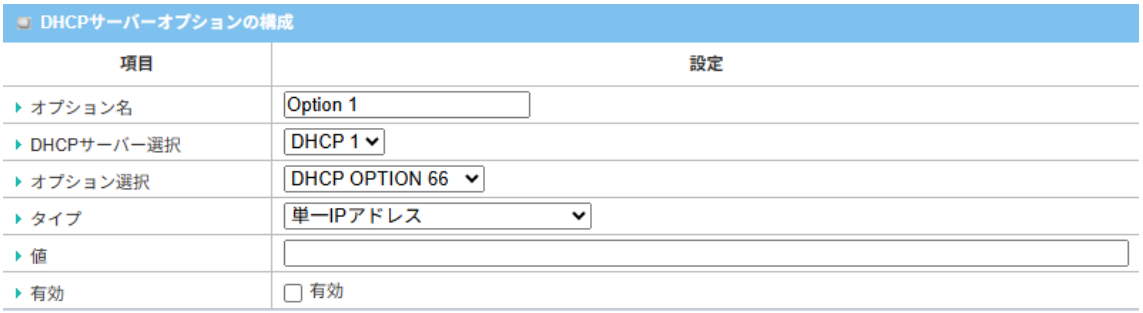
オプション番号	説明
42	NTP サーバーの IP アドレス[RFC 2132]
66	TFTP サーバー名[RFC 2132]
72	WWW サーバーIP アドレス[RFC 2132]
114	URL[RFC 8910]
150	TFTP サーバーのアドレス、イーサブート、GRUB 設定[RFC 5859]
160	URL[RFC 7710]

8.2.5.6. DHCP サーバーオプションリストの追加/編集（未サポート）

本機は、最大 99 の DHCP サーバーオプション設定を登録できます。



◆ DHCP サーバーオプションリストにある追加または編集をクリックすると、DHCP サーバーオプションの構成画面が表示されます。



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

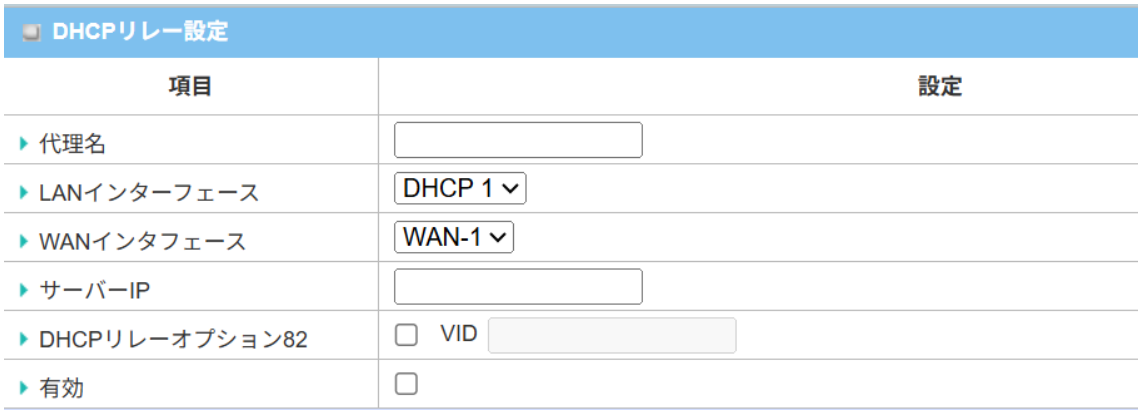
◆ 保存をクリックしルールを登録します。登録した内容が DHCP サーバーオプションリストに追加されます。

8.2.5.7. DHCP リレー構成リストの追加/編集

本機は、最大6つの DHCP リレー構成を登録できます。



◆ DHCP リレー構成リストにある追加または編集をクリックすると、DHCP リレー設定画面が表示され、各項目を入力しルールを作成します。



項目	説明
代理名	DHCP リレーオプション名を入力します。任意名称を入力します。
LAN インターフェース	リレー機能を適用する LAN を指定します。
WAN インタフェース	DHCP サーバーへの転送に使用する WAN インタフェースを選択します。
サーバーIP	DHCP 要求を転送する DHCP サーバーの IP アドレスを指定します。
DHCP オプション 82	リレーエージェント情報オプション(Option82)を有効にします。
有効	ルールを有効にする場合に☑します。

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

8.3. WiFi

本機にスマートフォンや PC などの端末を接続するための WiFi 設定を行います。
ご利用の環境に合わせて、SSID、認証方式、パスワードなどを設定し、WiFi アクセスポイントを構成します。
また、必要に応じて VAP を設定することで、ネットワークを分けて管理することができます。

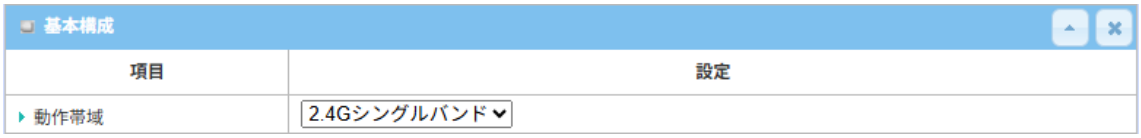


8.3.1. WiFi モジュール 1

WiFi モジュールの設定を行います。

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

8.3.1.1. 基本構成の設定



項目	説明
動作帯域	Wifi モジュールの動作帯域を指定します。 2.4G シングルバンド、5G シングルバンドから選択できます。

8.3.1.2. WiFi 構成の設定



項目	説明
WiFi モジュール	[有効]にチェックを入れると WiFi 機能が有効になります。
チャネル	チャネルを[自動]に設定した場合は、選択の基準として[AP 番号]または[干渉の少なさ]のいずれかを指定できます。また、自動で選択するチャネルの範囲をチェックを入れて指定します。物理インタフェースで設定した方の帯域のチャネルは固定です。
WiFi システム	使用する Wi-Fi の通信規格（IEEE 802.11 準拠）を指定します。選択可能な規格は、周波数帯によって以下の通り異なります。 2.4G シングルバンド : [802.11 b のみ], [802.11b/g ミックス], [802.11b/g/n ミックス], [802.11b/g/n/ax Mixed] から選択します。 5G シングルバンド: [802.11a のみ], [802.11a/n ミックス], [802.11a/n/ac Mixed], [802.11a/n/ac/ax Mixed] のいずれかから選択します。
グリーン AP	チェックを入れると、グリーン AP 機能が有効になります。 グリーン AP が有効の時、出力を抑えて省電力で動作します。
VAP 分離	有効にすると、異なる VAP に接続している端末同士の通信が遮断されます。初期状態では、この機能は有効に設定されています。
時間スケジュール	時間による動作制限を行う場合は、予め設定した時間スケジュールを選択します。それ以外は(0)常時を選択します。

8.3.1.3. VAP 構成

本機では VAP を 2.4G シングルバンドと 5G シングルバンドそれぞれで 8 個まで設定できます。
WiFi アップリンクとして動作している帯域の VAP は7個までとなります。



VAP リストの追加または編集をクリックし、VAP 構成画面を表示させます。
VAP2 の場合:



項目	説明
SSID	任意の SSID を入力します。
最大 STA	AP に同時接続できる端末の最大数を制限できます。 制限を設ける場合はチェックを入れ、上限台数を入力してください。
認証	ネットワークを保護するための認証方式を選択します。選択した方式により、パスワードや RADIUS サーバーの設定が必要になります。 **オープン:** 802.1x 有効にすると、端末は RADIUS サーバーによって認証されます。以下の項目を設定してください。 • RADIUS サーバーIP(初期値:0.0.0.0) • RADIUS サーバーポート(初期値:1812) • RADIUS 共有キー **共有:**認証のために、事前共有 WEP キーを設定します **自動:**端末からの要求に応じて自動的に[オープン]または[共有]を選択します。802.1x を有効にすると、端末は RADIUS サーバーによって認証されます。以下の項目を設定してください。 • RADIUS サーバーIP(初期値:0.0.0.0) • RADIUS サーバーポート(初期値:1812) • RADIUS 共有キー **WPA2 または WPA3:**端末は RADIUS サーバーによって認証されます。以下の項目を設定してください。 • RADIUS サーバーIP(初期値:0.0.0.0)

	• RADIUS サーバーポート（初期値：1812） • RADIUS 共有キー **WPA2-PSK または WPA3-SAE**:認証には、RADIUS サーバーの代わりに事前共有キーを使用します。 **WPA2-PSK/WPA3-SAE** :WPA2-PSK および WPA3-SAE の両方の設定を備えています。端末は、WPA2-PSK または WPA3-SAE のいずれかの方式で本機に接続します。
暗号化	選択した認証方式に応じて設定可能な暗号化方式がリストに表示されます。適切な方式を選択し、必要なキーを入力してください。 なし：暗号化を行いません。 WEP：最大 4 つの WEP キーを登録でき、使用するキーを 1 つ選択します。キーの入力形式は[HEX]または[ASCII]から選択します。 TKIP：8～63 文字の事前共有キーを入力します。 AES：8～63 文字の事前共有キーを入力します。セキュリティの観点からこちらの使用を推奨します。 TKIP/AES：TKIP と AES の混合モードです。端末は TKIP または AES のいずれかの方式で接続できます。8～63 文字の事前共有キーを入力します。
STA 分離	有効にすると、異なる VAP に接続している端末同士の通信が遮断されます。
ブロードキャスト SSID	有効にチェックを入れると、SSID のブロードキャスト機能が有効になり、 周囲の端末から、この SSID を検索して接続できるようになります。
有効	チェックを入れると有効になります。

保存をクリックしルールを登録します。登録したルールは[VAP リスト]に反映されます.

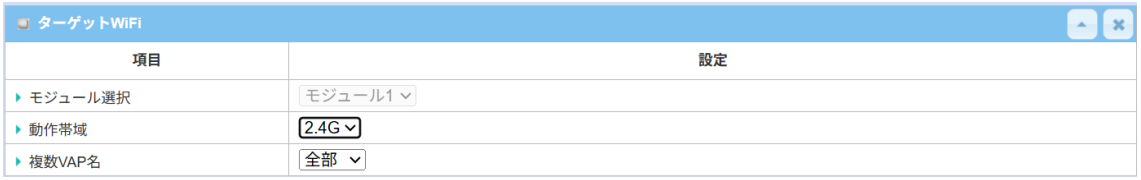
（注１） WEP、Shared Key および TKIP は安全性が低いため、新しい設定では使用しないでください。WPA2-PSK（AES）または WPA3-SAE を使用してください。

8.3.2. ワイヤレスクライアントリスト

このデバイスに関連付けられているクライアント情報を表示できます。

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

8.3.2.1. ターゲット WiFi の選択



項目	説明
モジュール選択	モジュール1で固定です。
動作帯域	クライアント情報を確認したい帯域を 2.4G、5G から選択します。
複数 VAP 名	利用しているクライアント情報を表示する VAP 名を表示します。 デフォルトでは[すべての VAP]です。

8.3.2.2. クライアントリスト

8.3.2.1 で選択した VAP に関連付けられているクライアントの情報が表示されます。



項目	説明
IP アドレスの設定＆アドレス	動的：IP アドレスが DHCP サーバーから割り当てられたことを示します。 静的：端末側で手動設定された固定の IP アドレスであることを示します。
ホスト名	WiFi 機器のホスト名を表示します。
MAC アドレス	WiFi 機器の MAC アドレスを表示します。
モード	通信している WiFi モードを表示します。
レート(注 1)	WiFi 機器と本機の想定物理データレートを表示します。 この値は実効スループットではありません。
RSSI0,RSSI1	クライアント本機間の受信信号強度(RSSI)を表示します。 RSSI0,RSSI1 はそれぞれの WiFi アンテナでの RSSI を示します。
信号	WiFi 機器間の信号強度をパーセントで表示します。
インターフェイス	WiFi 機器が接続している VAP 番号を表示します。

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

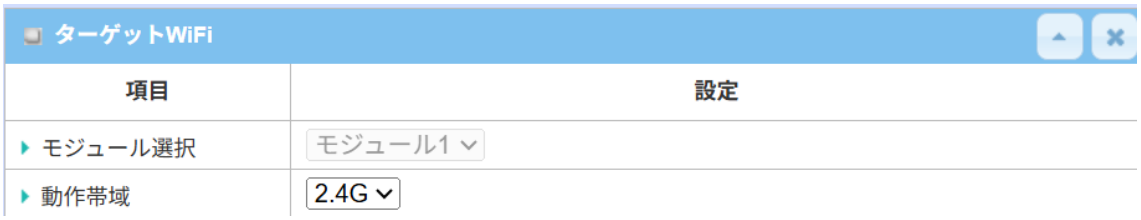
更新をクリックすると直ちにクライアントリストが更新されます。

8.3.3. 詳細構成

本機は専門的な知識を持つユーザー向けに、設置環境に合わせて Wi-Fi のパフォーマンスを最適化するための高度な設定項目を用意しています。Wi-Fi 技術に精通していない場合は、これらの設定は初期値のまま変更しないでください。不適切な設定を行うと、通信速度の低下や接続不良の原因となる場合があります。

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

8.3.3.1. ターゲット WiFi の選択



項目	説明
モジュール選択	モジュール1で固定です。
動作帯域	詳細設定を行う動作帯域を 2.4G、5G から選択します。

8.3.3.2. 詳細構成

動作帯域を 5G に設定したときの詳細構成



項目	説明
規制領域	設定できない項目です.
ビーコン間隔	ビーコンパケットを送信する時間間隔を設定します。ビーコンパケットには SSID やチャネル ID、セキュリティ設定が含まれます。
DTIM 間隔	省電力モードの端末に対して、受信待ちのデータがあることを知らせる間隔を設定します。
RTS しきい値	指定したサイズ以上のフレームを送信するときに、RTS/CTS を使用するためのしきい値を指定します。小さい値を設定すると通信速度が極端に低下する可能性があります。
断片化	Wi-Fi 通信でのパケット断片化の最大サイズを指定します。小さなサイズで断片化するとノイズの多い環境で有利になります。通信環境が良い場合は、最大サイズを指定します。
WMM	Wi-Fi 経由で音声や動画などのマルチメディアデータを送信する際の遅延やジッタを制御する機能です。
ショート GI	OFDM シンボル間のガードインターバルを短縮します。通信環境が良好な場合は通信効率が向上しますが、反射や干渉が多い環境では通信が不安定になることがあります。
TX レート	データ送信速度を指定します。[最高]を選択すると、本機は信号強度に応じて適切なデータレートを選択します。
RF 帯域幅	通信に使用する帯域幅を設定します。
送信パワー	Wi-Fi の電波出力レベルを設定して通信範囲を制御します。
5G バンドステアリング	[有効]にチェックを入れると、2.4GHz 帯と 5GHz 帯を自動で切り替えて通信が安定する可能性があります。
WIDS	すべての通信パケットを分析して統計を作成する機能です。詳細な状況は左の項目のステータス⇒基本ネットワーク⇒WiFi タブから確認できます。
Dynamic Frequency Selection	[有効]にチェックを入れると、5 GHz 帯でレーダー波を検出した場合に、無線送信を停止し、使用可能な別のチャネルへ切り替えます。
Associate RSSI Threshold	通信品質を維持するために、端末が AP に接続できる最低の RSSI 値を設定します。初期値は-75dBm です。

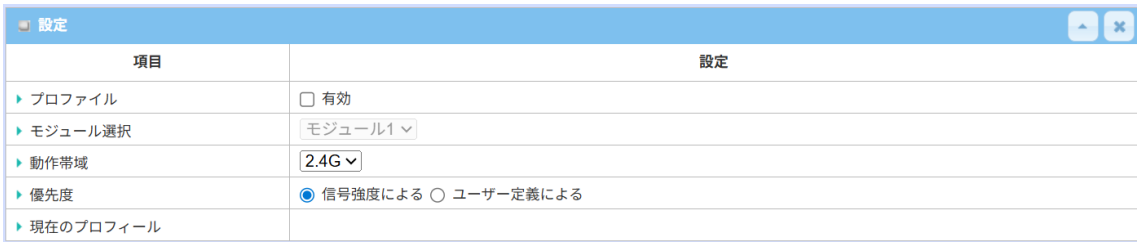
保存をクリックし、詳細設定を適用します

8.3.4. アップリンクプロファイル

本機はイーサネット WAN やモバイル NET WAN と同様に、Wi-Fi 経由で別のアクセスポイントに接続する Wi-Fi アップリンク機能を備えています。これにより上位ネットワークやホストに接続できるようになります。

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

8.3.4.1. アップリンクプロファイルの設定



項目	説明
プロファイル	[有効]にチェックを入れるとプロファイル機能が有効になります。8.1.3 物理インタフェースで設定されている動作帯域のみ有効にできます。
モジュール選択	モジュール1で固定です。
動作帯域	WiFiモジュールの動作帯域を 2.4G、5G から選択します。
優先度	接続するワイヤレスアップリンクネットワークの選択方法を指定します。信号強度、またはユーザー定義の優先度から選択できます。 信号強度による:信号が最も強いアップリンクネットワークに接続します。 ユーザー定義による:優先度が最も高いネットワークに接続します。 1 が最も高く、16 が最も低い優先度となります。
現在のプロフィール	プロファイルが有効で、接続が完了した後に、現在のプロファイル名が表示されます。

8.3.4.2. アップリンクプロファイルの作成

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



プロファイルリストにある追加または編集をクリックすると、プロファイル構成画面が表示されます。



項目	説明
プロファイル名	アップリンクプロファイル名を入力します。
ネットワーク ID	SSID を入力します。[スキャン]をクリックして使用可能な AP 情報を取得し、アップリンクネットワークとして選択することもできます。 リストからアクセスポイント選択すると、チャネル、SSID,認証、暗号化、MAC アドレスが自動的に入力されます。あとは必要に応じて接続用のキーを入力するだけで設定が完了します。
チャネル	通信に使用する無線チャネルを選択します。
認証	認証方式を選択します。
暗号化	必要に応じて暗号の設定を行います。
MAC アドレス	接続先 AP の MAC アドレスを指定します。
優先度	[ユーザー定義による]を選択した場合は、アップリンクプロファイルの優先順位を設定します。優先度は 1(優先度高)から 16(優先度低)です。
有効	[有効]にチェックを入れると、プロファイルが有効化されます。

8.3.4.3. アップリンクプロファイルの追加/編集（スキャン）

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

Wireless APリスト

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

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

8.4. IPv6

IPv6 では、用途に応じてグローバルユニキャストアドレス、ユニークローカルアドレス、リンクローカルアドレスなどを使用します。IPv6 では一般に NAT を必要としませんが、ネットワーク設計によってはアドレス変換を使用する場合があります。また、IPv6 を使用しても通信速度の向上が保証されるわけではありません。

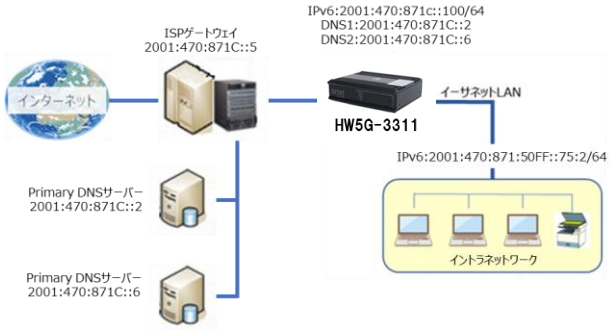
（注１） IPv6 を使用するためには ISP（プロバイダ）が IPv6 に対応していなければなりません。
（注２） WAN-1 の物理インタフェースに“イーサネット”を指定した場合には、Static IPv6 および PPPoEv6、それ以外のインタフェースを指定した場合は DHCPv6 のみ設定可能です。

8.4.1. IPv6 接続タイプ

IPv6 のネットワークに接続する方法として Static IPv6、DHCPv6 および PPPoEv6 があります。ご契約の ISP(プロバイダ)の指定に従って選択します。

8.4.1.1. Static IPv6

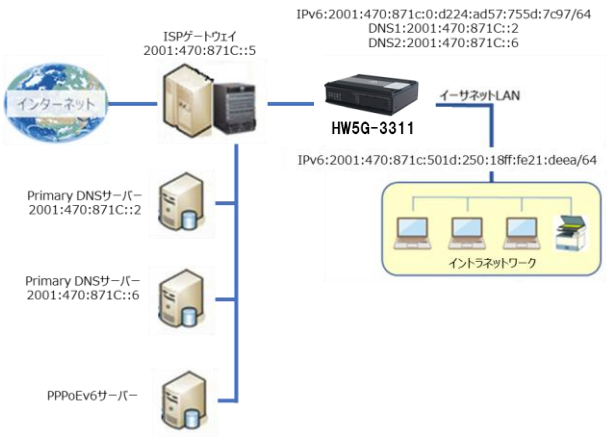
Static IPv6 は、静的 IPv4 と同様な IP アドレッシングをします。Static IPv6 動作には、IPv6 アドレス、IPv6 デフォルトゲートウェイアドレス、および、IPv6 DNS を手動で設定する必要があります。



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

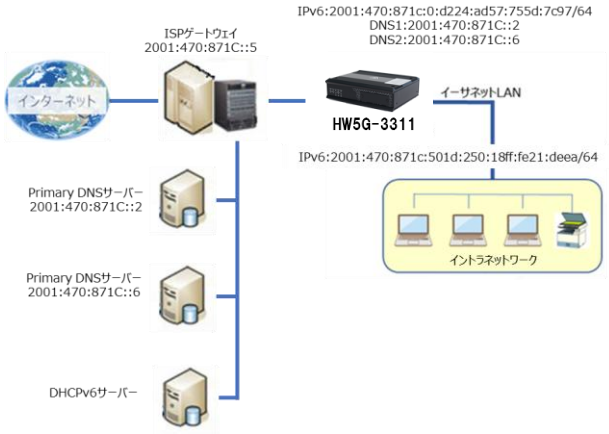
8.4.1.2. PPPoEv6

PPPoE セッションの確立と認証が完了すると、IPv6CP で IPv6 通信に使用するインタフェース識別子をネゴシエートします。グローバル IPv6 アドレス、DNS サーバーアドレス、および LAN へ配布するプレフィックスは、契約や通信事業者の方式に応じて、RA、DHCPv6、DHCPv6-PD などで取得します。左図は、PPPoE による IPv6 アドレッシングを示しています。 ISP 側の PPPoEv6 サーバーは、PPPoEv6 クライアントからの要求を受信すると IPv6 構成を提供します。PPPoEv6 サーバーが、クライアントからの要求を取得し、正常に認証すると、サーバーは、IP アドレス、DNS サーバーアドレス、および、その他の必要なパラメータを送信し、クライアントを自動的に構成します。



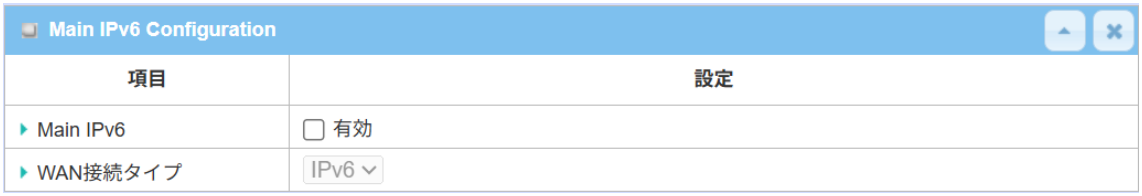
8.4.1.3. DHCPv6

IPv6 の DHCP サーバーは、IP アドレス、DNS サーバーアドレス、および、その他の可能なデータを DHCP クライアントに送信して自動的に設定します。また、サーバーは、アドレスのリース時間と IPv6 アドレスの更新のためにサーバーに再接続する時刻を送信します。クライアントは、IPv6 アドレスを更新する要求を再送信する必要があります。左図は、DHCPv6 IP アドレッシングを示します。IPv6 アドレス、DNS サーバーなどの情報は DHCPv6 から取得します。デフォルトルータは、ICMPv6 Router Advertisement（RA）から取得します。



8.4.2. IPv6 構成設定

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

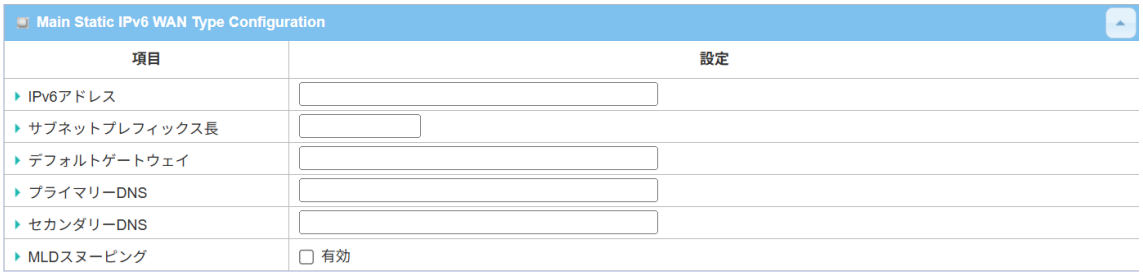


画面左側のメニューから、基本ネットワーク⇒IPv6⇒設定の順にクリックします。

項目	説明
IPv6	[有効]にチェックを入れると、IPv6機能が有効になります。
WAN 接続タイプ (注1)	IPv6接続を確立するIPv6 WAN接続タイプを指定します。 ご契約のISP(プロバイダ)が静的IPv6接続であれば、[Static IPv6]を選択し、[Static IPv6 WANタイプ構成]に進みます。 PPPoEv6アカウント接続の場合は、[PPPoEv6]を選択します。 物理インタフェースのWAN1が“イーサネット”ではない場合は[IPv6]のみ選択でき、DHCPv6の設定が行えます。

（注１） 物理インタフェースは WAN&アップリンク⇒物理インタフェースから変更できます。

8.4.2.1. Static IPv6 WAN タイプ構成



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

（注１） 詳しい情報が必要な場合は、ご利用の ISP（プロバイダ）にご確認ください。

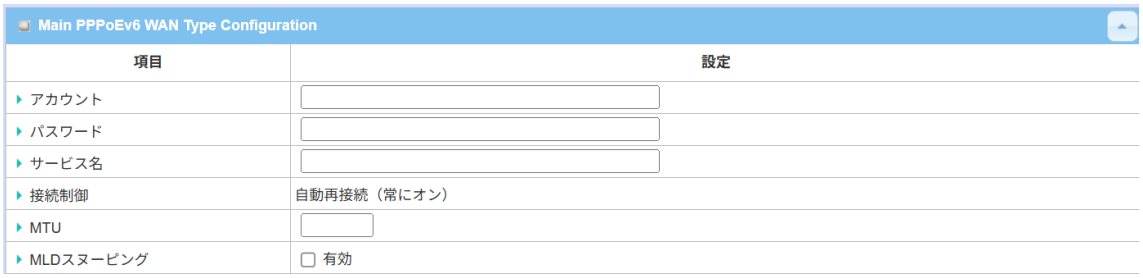
LAN 構成



項目	説明
グローバルアドレス	LAN側端末に配布するIPv6プレフィックス を入力します。
リンクローカルアドレス	本機のLAN側リンクローカルアドレスが表示されます。

（注２） 詳しい情報が必要な場合は、ご利用の ISP（プロバイダ）にご確認ください。

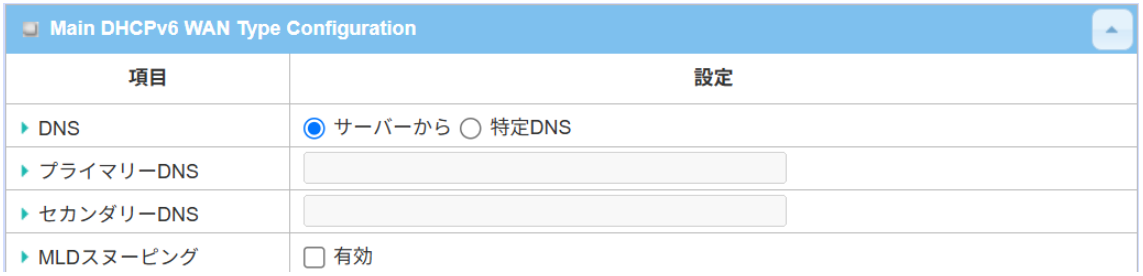
8.4.2.2. PPPoE WAN タイプ構成



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

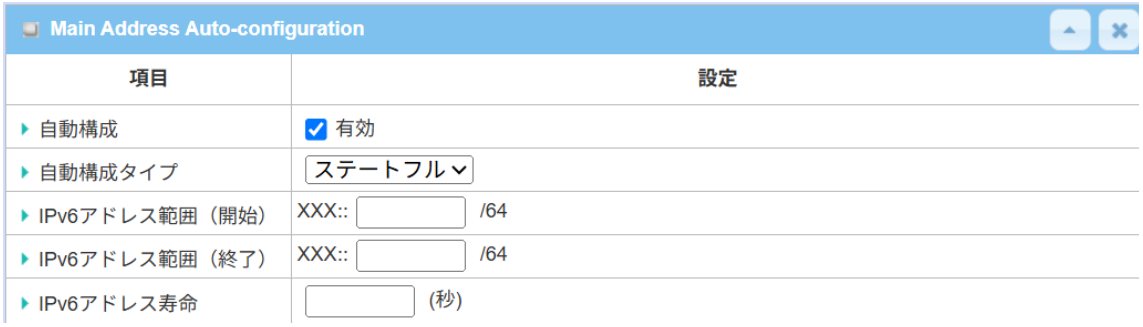
（注３） 詳しい情報が必要な場合は、ご利用の ISP（プロバイダ）にご確認ください。

8.4.2.3. DHCPv6 WAN タイプ構成



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

8.4.2.4. アドレス自動構成



項目	説明
自動構成	[有効]チェックを入れると、自動構成機能を有効になります。
自動構成タイプ	IPv6接続を確立する自動構成タイプを選択します。 ステートレス：ローカルエリアネットワークをSLAAC + RDNSSとなるように管理します。 ステートフル：ローカルエリアネットワークをステートフルとなるように管理します。IPv6アドレス範囲（開始）とIPv6アドレス範囲（終了）を設定する必要があります。WAN-1が“イーサネット”ではない場合選択できません。
IPv6 アドレス範囲（開始）	LAN端末に対するDHCPv6範囲の開始IPv6アドレスを入力します。値の範囲は0001～FFFFです。本項目は自動構成タイプにステートフルを選択した時のみ表示されます。
IPv6 アドレス範囲（終了）	LAN端末に対するDHCPv6範囲の終了IPv6アドレスを入力します。値の範囲は0001～FFFFです。本項目は自動構成タイプにステートフルを選択した時のみ表示されます。
IPv6 アドレス寿命	IPv6アドレスの有効時間（秒単位）を入力します。値の範囲は0～65535です。

◆ 設定終了後に保存ボタンをクリックして、設定を保存し本機を再起動します。

8.5. ポート転送

IPv4 プロトコルで運用中のネットワークにおいて、一つのグローバル IP アドレスを複数の LAN の IP 機器で共用することを可能にするのが、ネットワークアドレス変換（NAT または NAPT）機能です。一方、この機能が動作していると、インターネットなど外部から、LAN に接続された IP 機器に直接アクセスできなくなります。本機ではポート転送（ポートフォワーディング）機能を搭載し、外部から LAN 内のサーバーなどIP機器にアクセスできます。

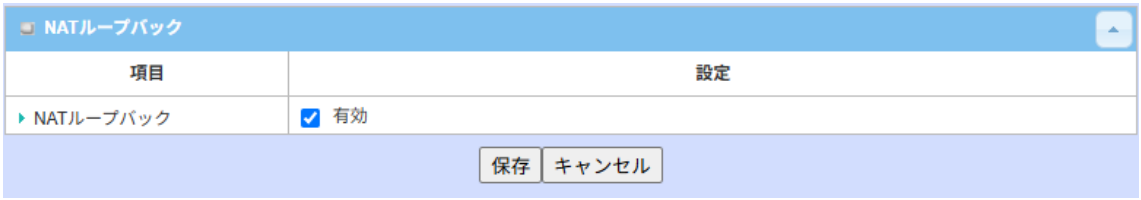
（注）NAT 機能の有効/無効は WAN インタフェースの接続設定内にあります。（詳細は 8.1 章 WAN およびアップリンクを参照してください。）

8.5.1. ポート転送設定

8.5.1.1. NAT ループバック

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

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



項目	説明
NAT ループバック	[有効]にチェックを入れると、NAT ループバック機能が有効になります。

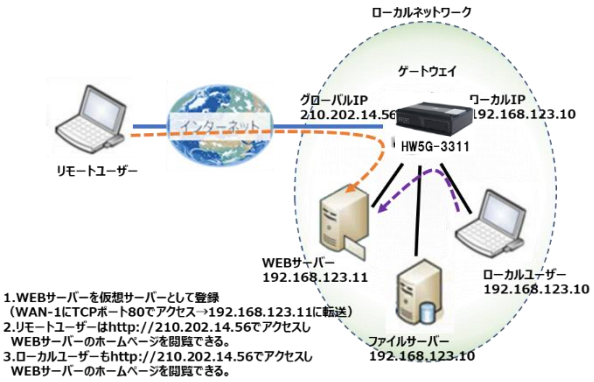
◆ 設定終了後に保存をクリックして、設定を保存します。

8.5.2. 仮想サーバー＆仮想コンピュータ

アドレス変換機能(NAT)が有効なネットワーク構成における、WAN 側から LAN 内の各種サーバーなどホストへのアクセス設定を行います。



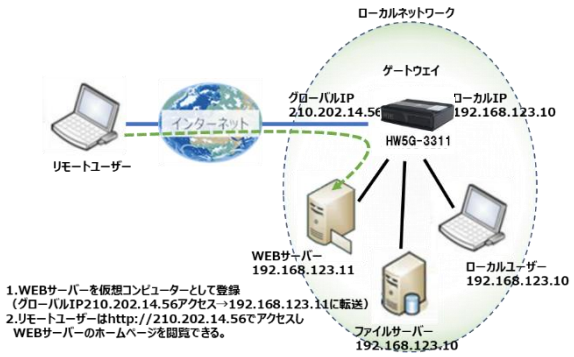
8.5.2.1. 仮想サーバー



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

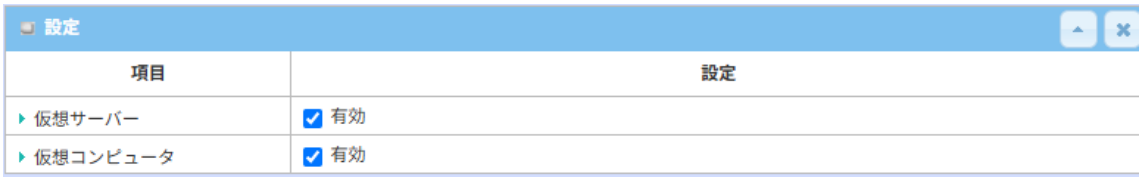
8.5.2.2. 仮想コンピュータ

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



8.5.2.3. 仮想サーバーおよび仮想コンピュータの有効

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

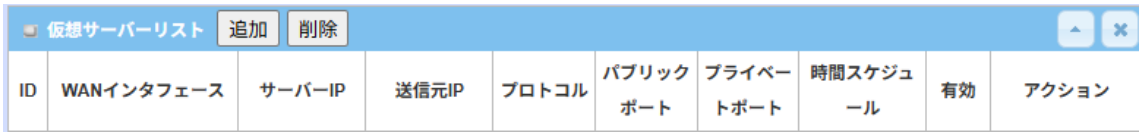


項目	説明
仮想サーバー	[有効]にチェックを入れると、仮想サーバー転送機能が有効になります。
仮想コンピュータ	[有効]にチェックを入れると、仮想コンピュータ転送機能が有効になります。

◆ 保存をクリックして、設定を保存します。

8.5.2.4. 仮想サーバーの追加/編集

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



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

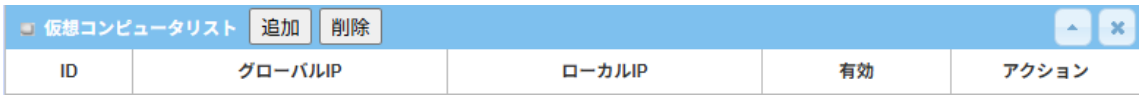


項目	説明
WAN インタフェース	仮想サーバーへのポート転送を許可するWANインタフェースを選択します。全部、WAN-1,WAN-2 および WAN-3 が選択できます。
サーバーIP	仮想サーバーの LAN IP アドレスを指定します。
送信元IP	外部アクセスを許可する送信元の IP アドレスを指定します。指定方法は以下の 3 種類があります。 ◆任意：全ての送信元の IP アドレスで仮想サーバーへの転送が許可されます。 ◆特定の IP アドレス：一つの送信元 IP アドレスのみが仮想サーバーへの転送が許可されます。 ◆IP 範囲：送信元の IP アドレスが指定した範囲であるときに仮想サ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

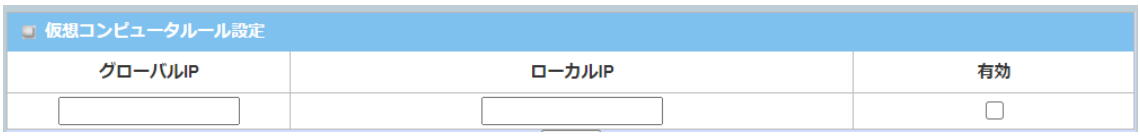
◆ 保存をクリックして、ルールを登録します。設定したルールが［仮想サーバーリスト］に表示されます。

8.5.2.5. 仮想コンピュータの追加/編集

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



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



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

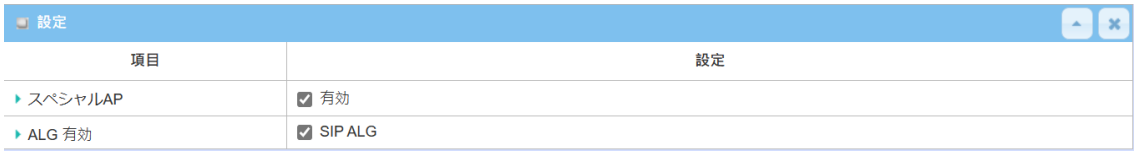
◆ 保存をクリックして、ルールを登録します。設定したルールが[仮想コンピュータリスト]に表示されます。

8.5.3. スペシャル AP&ALG

本機能は、特定のアプリケーションの通信をルータで正しく処理するための設定です。トリガポートに対応して一時的にポートを開放するスペシャル AP 機能と、データ内部の通信情報を適切に変換する SIP ALG 機能により、オンラインゲームや通話アプリなどの通信トラブルを解決します。本項目では、特定のルールに基づいたスペシャル AP をカスタム設定できます。最大8つまでルールを作成可能です。

◆ 画面左側のメニューから、基本ネットワーク⇒ポート転送⇒スペシャル AP&ALG の順にクリックします。

8.5.3.1. 設定

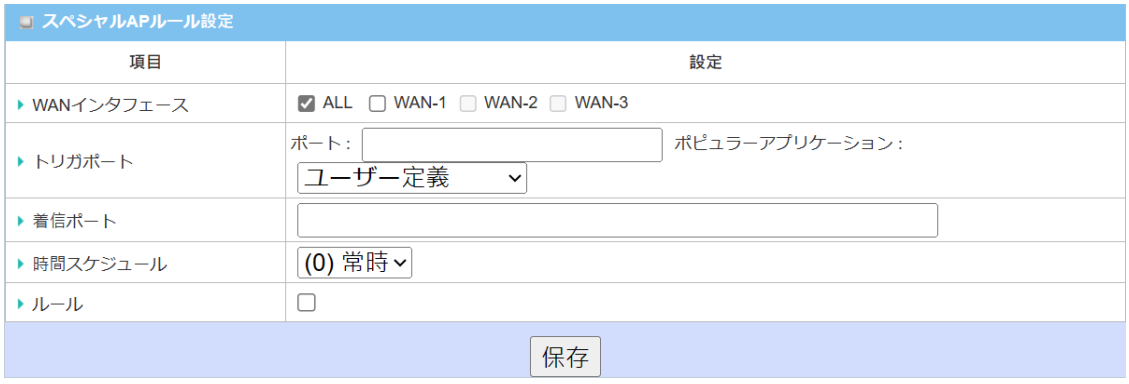


項目	説明
スペシャル AP	[有効]にチェックを入れると、スペシャル AP 機能が有効になります。
ALG 有効	[有効]にチェックを入れると、SIP ALG 機能が有効になります。有効にすると、SIP パケット内の IP アドレスやポート情報を NAT 環境に合わせて自動変換します。

8.5.3.2. スペシャル AP リストの編集



◆ 追加または編集をクリックすると、[スペシャル AP ルール設定]画面が表示されます。



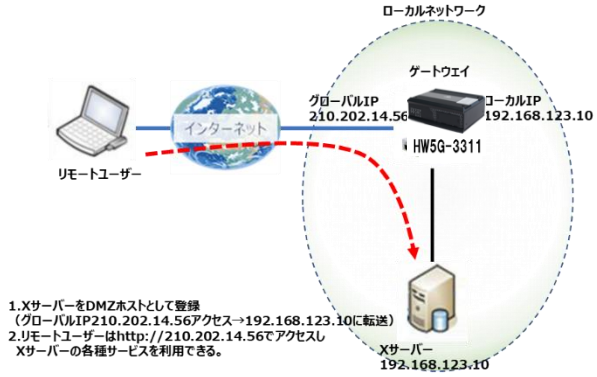
項目	説明
WAN インタフェース	パケットを入力する WAN インタフェースを選択します。
トリガポート	トリガーポートまたはポート範囲を入力してください。ドロップダウンリストでユーザー定義を選択した場合に有効です。

項目	説明
	ドロップダウンリストからポピュラーアプリケーションを選択した場合は、対応するトリガーポートと着信ポートが自動的に設定されます。
着信ポート	着信ポートを入力してください。ドロップダウンリストでユーザー定義を選択した場合に有効です。 ドロップダウンリストからポピュラーアプリケーションを選択した場合は、対応する受信ポートが自動的に設定されます。
時間スケジュール	ルールが有効になる時間スケジュールを指定します。 常時(0)または[スケジューリング]で定義されたスケジュールリストから選択できます。
ルール	チェックを入れると、ルールが有効化されます。

8.5.4. DMZ およびパススルー

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

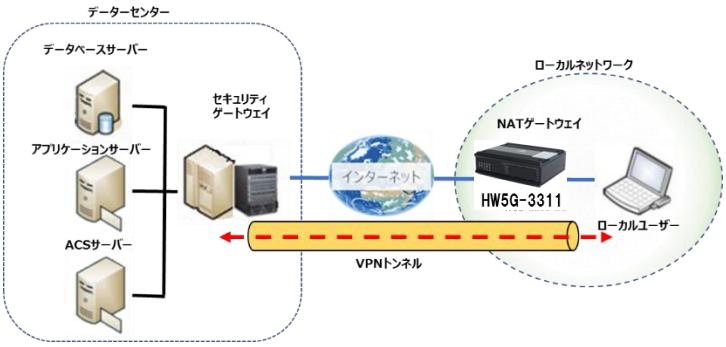
8.5.4.1. DMZ(De Militarized Zone)



図中 X サーバーをローカルエリアネットワークに配置した場合、リモートユーザーがサーバーからのサービスを要求する場合には、このサーバーを DMZ ホストとなるように設定する必要があります。

左図はリモートユーザーがグローバル IP210.202.14.56 のゲートウェイにアクセスすることで X サーバーからサービスを要求することができます。本機は、仮想サーバーの登録ルール以外の外部アクセスを直接 DMZ ホストに転送します。

8.5.4.2. VPN パススルー



一部の VPN プロトコルでは、NAT を越えて接続するための補助機能が必要です。VPN パススルーを有効にすると、選択した VPN プロトコルの通信を LAN 側から WAN 側へ通過させます。

8.5.4.3. DMZ の設定

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



項目	説明
有効	[有効]にチェックを入れると、DMZ 機能が有効になります。
ポート	DMZ を許可するインタフェースを全部、WAN-1 および WAN-2 から選択します。
DMZ ホスト	DMZ ホストにする LAN 内機器のローカル IP アドレスを指定します。

◆ 保存をクリックして、設定を登録します。

8.5.4.4. VPN パススルーの設定

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



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

◆ 保存をクリックして、設定を登録します。

8.6. ルーティング

複数のサブネット間で通信ができるようにするには、データパケットが適切な経路を経由する必要があります。それぞれのサブネット間の通信はルータがルーティングを行うことで、実現しています。ルーティングテーブルを手動設定する[静的ルーティング]とルータ間でルーティングテーブルを構築する[動的ルーティング]があります。本機では、静的ルーティング、RIPv1/RIPv2、OSPF および BGP を使用した動的ルーティングに対応しています。

8.6.1. 静的ルーティング

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

8.6.1.1. 静的ルーティングの設定

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

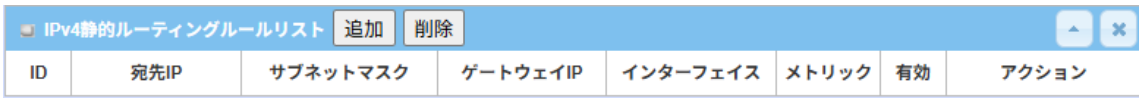


項目	説明
静的ルーティング	[有効]にチェックを入れると、静的ルーティング機能が有効になります。

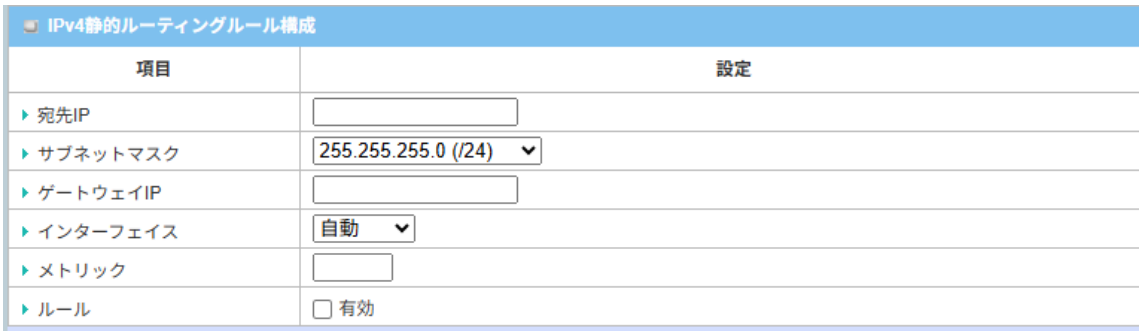
◆ 保存をクリックして、設定を登録します。

8.6.1.2. IPv4 静的ルーティングルールの追加/編集

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



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



項目	説明
宛先 IP	この静的ルーティングルールの宛先 IP を指定します。
サブネットマスク	この静的ルーティングルールのサブネットマスクを選択します。
ゲートウェイ IP	この静的ルーティングルールのゲートウェイ IP を指定します。
インターフェイス	この静的ルーティングルールのインタフェースを選択します。[自動]、または、利用可能な[WAN/LAN]インタフェースが選択できます。
メトリック	この静的ルーティングルールのメトリックです。値の範囲は 0~255 です。優先順位を示し、小さいほど優先順位は高いです。
ルール	[有効]にチェックを入れると、この静的ルーティングルールが有効になります。

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

8.6.2. 動的ルーティング

適用型ルーティングとも呼ばれる動的ルーティングは、近隣するルータのルーティングテーブルを共有し、ネットワーク状態変化に適用しながら、ルートを選択します。そのため、ネットワークが多数のサブネットで構成される場合にネットワーク管理を簡易にします。本機に搭載する RIP（Routing Information Protocol）は小規模ネットワークに適しており、OSPF（Open Short Pass First）は中規模のネットワークに適しています。

8.6.2.1. RIPv1/RIPv2 ルーティング

RIP は、宛先までに経由するルータ数をメトリックとして経路を選択します。到達可能な最大メトリックは 15 で、16 は到達不能を表します。ルーティングループの影響を抑えるため、スプリットホライズンやルートポイズニングなどを使用します。

8.6.2.2. OSPF ルーティング

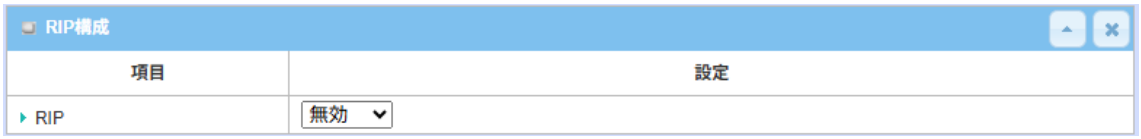
OSPF は、ルータ間でリンクステート情報を LSA として交換し、最短経路を計算するルーティングプロトコルです。OSPF ネットワークはエリアに分割でき、バックボーンエリアである Area 0 が各エリアを接続します。

8.6.2.3. BGP ルーティング

BGP（Border Gateway Protocol）とは、インターネット上のシステム間など大規模ネットワークで使用される動的ルーティングプロトコルの一つです。BGP ピア間で到達可能なネットワーク情報と経路選択ポリシーを交換します

8.6.2.4. RIP 設定

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

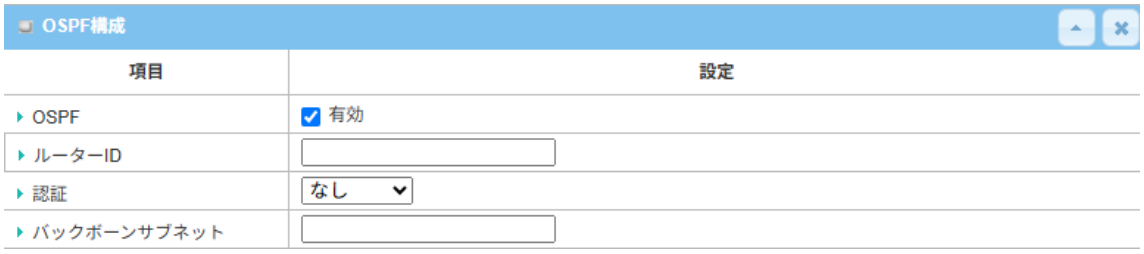


項目	説明
RIP	RIP プロトコルの動作を選択します。 無効：RIP プロトコルが無効になります。 RIPv1：RIPv1 プロトコルが有効になります。 RIPv2：RIPv2 プロトコルが有効になります。

◆ 保存をクリックして、設定を登録します。

8.6.2.5. OSPF 設定

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



項目	説明
OSPF	[有効]にチェックを入れると、OSPF プロトコルが有効になります。
ルーターID	OSPF プロトコル上の本機のルータ ID（本機 IP アドレス）を指定します。
認証	OSPF プロトコルで使用する認証方法を選択します。 ◆None: OSPF プロトコルの認証が無効です。 ◆テキスト: OSPF プロトコルでは、指定された[Key]によるテキスト認証が有効になります。 ◆MD5: OSPF プロトコル上では指定された[ID（範囲 1~255）]と[Key]による MD5 認証が有効になります。
バックボーンサブネット	OSPF で経路情報を交換するバックボーンエリアのサブネットを指定します。隣接ルータと接続しているネットワークを、サブネットアドレス/マスク長形式で入力します。

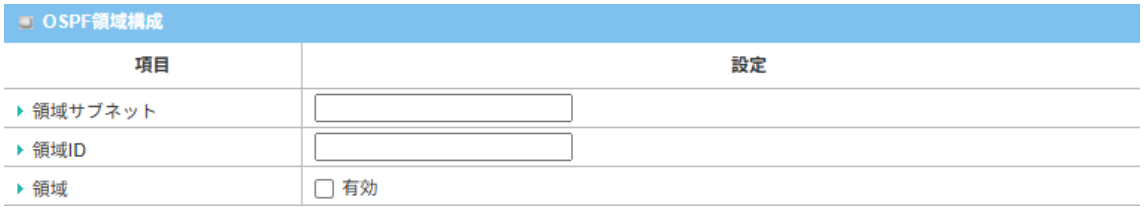
◆ 保存をクリックして、設定を登録します。

8.6.2.6. OSPF 領域リストの追加/編集

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



◆ 追加または編集をクリックすると[OSPF 領域構成]画面が表示されます。

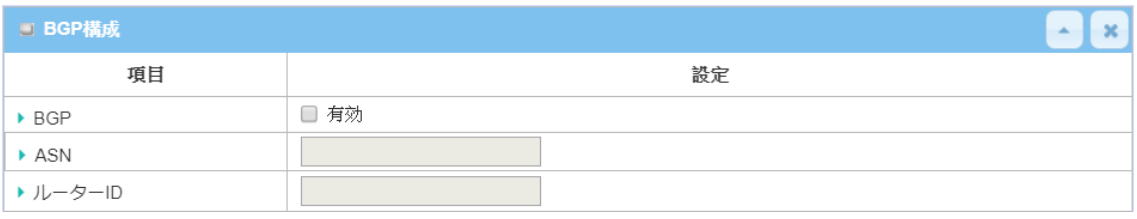


項目	説明
領域サブネット	OSPF 領域に所属させる本機のサブネットを指定します。 指定したサブネットの経路情報が、該当する OSPF 領域で扱われます。 サブネットアドレス/マスク長形式で入力します。
領域 ID	OSPF 領域を識別するための ID を指定します。 IPv4 アドレス形式で入力します。同じ領域に所属する OSPF ルータでは、同じ領域 ID を指定してください。
領域	[有効]にチェックを入れると、この OSPF 領域ルールが有効になります。

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

8.6.2.7. BGP 設定

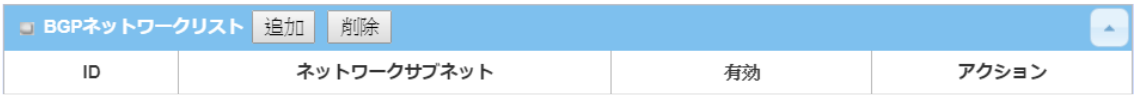
◆ 画面左側のメニューから、基本ネットワーク⇒ルーティング⇒動的ルーティングの順にクリックします。



項目	説明
BGP	[有効]にチェックを入れると、BGP プロトコルが有効になります。
ASN	BGP プロトコルで使用される、本機の AS 番号です。 値の範囲は 1～ 4294967295 です。
ルーターID	BGP プロトコルで使用される IPv4 形式のルータ ID です。

8.6.2.8. BGP ネットワークリストの追加/編集

BGP ネットワークリストには、全ての BGP ネットワークルールのパラメータが表示されます。



◆ 追加または編集をクリックすると[BGP ネットワーク構成]画面が表示されます。



項目	説明
ネットワーク サブネット	BGP プロトコルで使用される本機のサブネットを指定します。 IPv4 形式の IP アドレスの指定とサブネットマスクを選択します。
ネットワーク	[有効]にチェックを入れると、この BGP ネットワークルールが有効になります。

保存をクリックして、ルールを登録します。設定したルールが[BGP ネットワークリスト]に表示されます。

8.6.2.9. BGP 近隣ルールの追加/編集

BGP 近隣 IP リストには、全ての BGP 近隣 IP ルールのパラメータが表示されます。



◆ 追加または編集をクリックすると[BGP 近隣構成]画面が表示されます。



項目	説明
近隣 IP	本機の近隣 IP を指定します。 IPv4 形式の IP アドレスで入力します。
リモート ASN	本機のリモート ASN 番号を指定します。 値の範囲は 1～ 4294967295 です。
近隣	[有効]にチェックを入れると、この BGP 近隣ルールが有効になります。

保存をクリックして、ルールを登録します。設定したルールが[BGP 近隣 IP リスト]に表示されます。

8.6.3. ルーティング情報

静的ルーティング、動的ルーティング、およびポリシールーティングで構成された本機のルーティング情報を表示します。

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

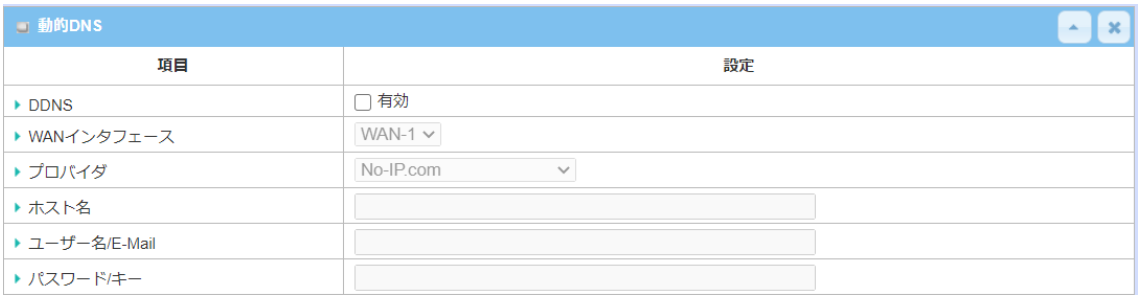


8. 7. DNS & DDNS

DDNS は、変動する WAN 側 IP アドレスとドメイン名を対応付ける機能です。LAN 内の機器へ外部から接続するには、DDNS に加えて、ポート転送とファイアウォールの許可設定が必要です。通信事業者の CGNAT 環境など、WAN 側に外部から到達可能な IP アドレスが割り当てられない場合は、DDNS を設定しても外部から接続できません。

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

8.7.1. 動的 DNS の設定



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

◆ 保存をクリックして設定を保存します。

8.7.2. DNS Mapping の設定

DNS マッピングは、指定したホスト名の問い合わせに対して、設定した IP アドレスを返します。



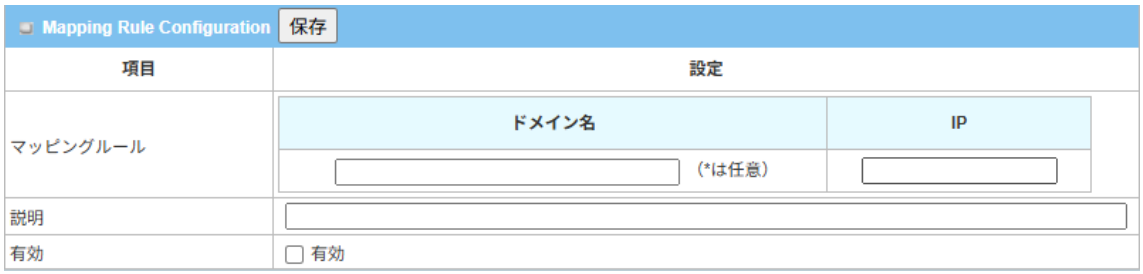
項目	説明
DNS Mapping	[有効]にチェックを入れると、DNS mapping機能が有効になります。

DNS Mapping 機能を有効にした場合、マッピングルールを作成する必要があります。

8.7.3. マッピングルールの定義



◆ 追加をクリックすると、[Mapping Rule Configuration]画面が表示されます。

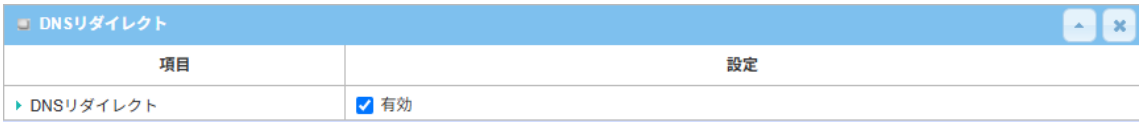


項目	説明
マッピングルール	ドメイン名：指定したドメイン名への通信を次のIPに転送します。 IP:転送先のIPアドレスを指定します。
説明	このルールの説明を 63 文字以内に入力できます。
有効	[有効]にチェックを入れると、本ルールが有効になります。

◆ 保存をクリックして、本ルールを登録します。

8.7.4. DNS リダイレクトの設定

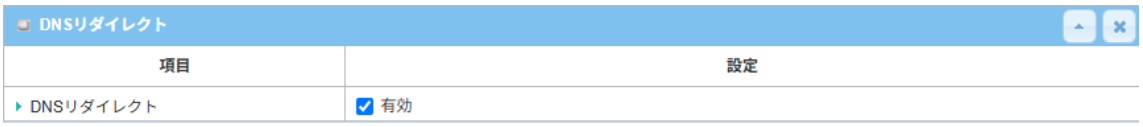
DNS リダイレクトとは、あらかじめ設定した特定のドメインを指定した DNS サーバーに転送する機能です。



項目	説明
DNS リダイレクト	[有効]にチェックを入れると、DNSリダイレクト機能が有効になります。

DNS リダイレクト機能を有効にした場合、リダイレクトルールを作成する必要があります。

8.7.5. リダイレクトルールの定義



◆ 追加をクリックすると、[Redirect Rule Configuration]画面が表示されます。



項目	説明
Domain Name	指定したドメイン名を次のDNSサーバに問い合わせます。
DNS Server	問い合わせる DNS サーバの IP アドレスを指定します。
有効	[有効]にチェックを入れると、本ルールが有効になります。

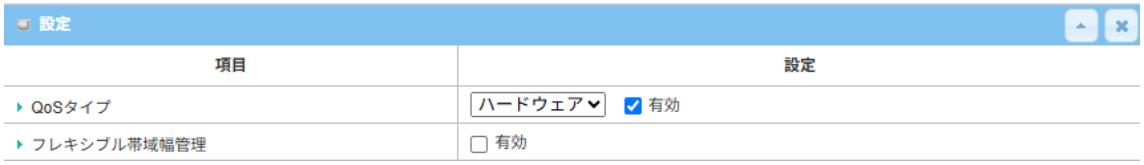
◆ 保存をクリックして、本ルールを登録します。

8.8. QoS

本機は、ネットワークサービス品質を維持するために、QoS を搭載しています。ソフトウェア QoS では帯域幅、接続セッション、優先度付きキュー、DSCP をもとに、データ送受信の制御を行えます。また、本機には自動調整アルゴリズムにより現在の帯域幅使用状況に基づいた帯域幅分散を行うフレキシブル帯域幅管理機能を搭載し、透過的にネットワーク性能を最大限に引き上げることが可能です。

8.8.1. QoS 設定

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



項目	説明
QoS タイプ	ドロップダウンリストからQoSタイプを選択し、[有効]にチェックを入れると、QoSが有効になります。 ◆ソフトウェア：QoSをソフトウェア処理で実行するため、柔軟な条件でQoSルールを指定できます。 ◆ハードウェア：QoSをハードウェア処理で実行します。そのため、ハードウェアの送受信帯域制御およびバッファー管理の制御条件のみが有効になります。
フレキシブル帯域幅管理	[有効]にチェックを入れると、フレキシブル帯域幅管理機能が有効になります。

◆ 保存をクリックして設定を保存します。

8.8.2. ソフトウェア QoS

8.8.2.1. システムリソース構成



項目	説明
システムキューの タイプ	QoSで利用するシステムキューのタイプを指定します。システムキューでは以下の2種類が選択できます。 ◆帯域幅キュー: 帯域幅でQoSを実行するキューを使用します。 ◆優先度キュー: 優先度でQoSを実行するキューを使用します。 また、キューで使用する最大優先度を指定します。値の範囲は1～6です。
WAN インタフェース	プルダウンメニューから WAN インタフェースを選択します。それ以降の設定は選択した WAN インタフェースに適用されます。

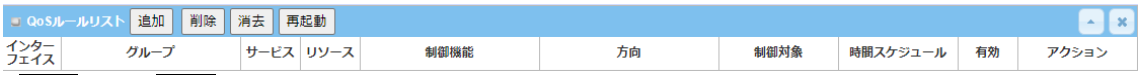
8.8.2.2. WAN インタフェースリソース設定

WAN インタフェースのアップストリーム（送信）、ダウンストリーム（受信）の帯域幅および総接続セッション数を指定できます。

項目	説明
アップストリーム 帯域幅	アップストリーム（送信）帯域幅を指定します。値の範囲は1～1000Mbps（1～1024000Kbps）です。WANインタフェースがモバイルNETの場合は、接続モードに合わせて設定する必要があります。
ダウンストリーム 帯域幅	ダウンストリーム（受信）帯域幅を指定します。値の範囲は1～1000Mbps（1～1024000Kbps）です。WAN インタフェースがモバイル NET の場合は、接続モードに合わせて設定する必要があります。
総接続セッション数	総接続セッション数を指定します。接続されるホスト端末が多い程大きな値を設定する必要があります。値の範囲は 1～100,000 です。

8.8.2.3. QoS ルールの追加・編集

QoS 機能を有効にしてシステムリソースを設定した後は、運用形態に合わせて詳細な QoS ルールを設定する必要があります。本機では最大 128 の QoS ルールを追加することができます。



追加または編集をクリックすると[QoS ルール構成]画面が表示されます。



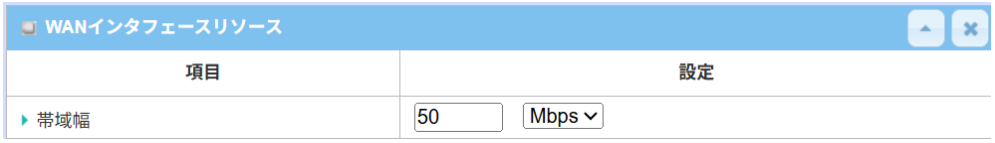
項目	説明
インターフェイス	QoSルールを適用するWANインタフェースを[すべてのWAN]、[WAN-1]、[WAN-2]および[WAN-3]より選択します。
グループ	QoS ルールを適用するグループを[送信元 MAC アドレス]、[IP]、[ホスト名]から選択します。 [IP]を選択した場合は、サブネットアドレス(例:192.168.123.0)を指定し、サブネットマスクをプルダウンメニューから選択します。 [ホスト名]を選択した場合は、[オブジェクト定義]⇒[グルーピング]で設定したホストグループを選択できます。
サービス	QoS ルールに適用するサービスを指定します。サービスタイプは以下より選択します。 ◆全部: すべてのサービスタイプにQoSルールが適用されます。 ◆DSCP:TOSフィールド内のDSCP値でQoSルールを適用させます。この場合、プルダウンメニューから適用するDSCP値を選択します。 ◆TOS:[最小化コスト]、[最大化信頼性]、[最大化スループット]および[最小化遅延]を選択し、TOSフィールド情報からQoSルールの適合を判断します。 ◆ユーザー定義パケット:ユーザー定義のポート番号範囲とプロトコル(TCP&UDP/TCP/UDP)を指定します。 ◆既知のサービス:プルダウンメニューからQoSルールを適用する既知のサービスを選択します。
リソース/制御機能	QoS ルールのリソースタイプと対応する制御機能を指定します。 指定可能なリソースと制御機能は以下のとおりです。 ◆帯域幅: 帯域幅によるQoS制御を行います。 帯域の最小レートと最大レートを指定します。値の範囲は1～1000Mbps(1～1024000Kbps)です。 ◆接続セッション: 接続セッションによるQoS制御を行います。 接続セッション最大値を指定します。値の範囲は1～100,000です。 ◆優先度キュー: 優先度キューによりQoS制御を行います。 優先度を指定します。値範囲は1～6です。 ◆DiffServコンポーネント:DSCPフィールドによりQoS制御を行います。 利用するDSCP値をプルダウンメニューから選択します。
QoS 方向	QoS ルールを適用するトラフィックの方向(送信/受信/両方)を指定します。
時間スケジュール	あらかじめ設定した時間スケジュールに則り本ルールを適用します。時間スケジュールの設定については、9.1.項のスケジューリングを参照してください。
ルール有効	[有効]にチェックを入れると、本 QoS ルールが有効になります。

◆ 保存をクリックして、ルールを登録します。設定したルールが[QoSルールリスト]に表示されます。

8.8.3. ハードウェア QoS

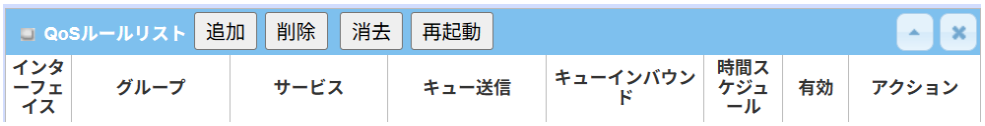
8.8.3.1. WAN インタフェースリソースの設定

WAN 全体で利用する帯域幅を指定します。

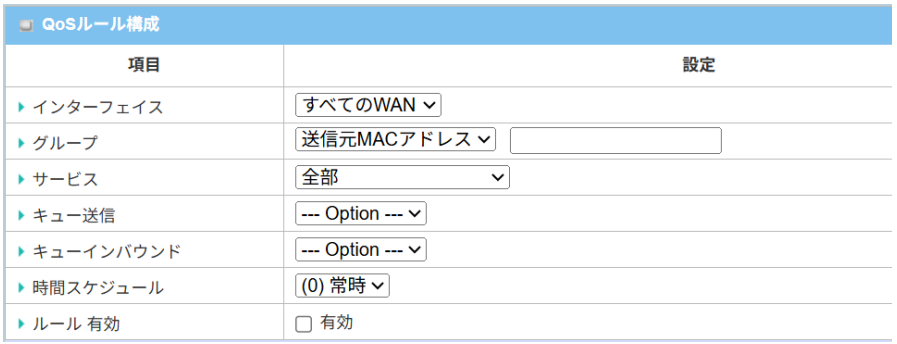


8.8.3.2. QoS ルールの追加・編集

QoS 機能を有効にしてシステムリソースを設定した後は、運用形態に合わせて詳細な QoS ルールを設定する必要があります。本機では最大 128 の QoS ルールを追加することができます。



追加または編集をクリックすると[QoS ルール構成]画面が表示されます。



項目	説明
インターフェイス	QoSルールを適用するWANインタフェースを[すべてのWAN]、[WAN-1]、[WAN-2]および[WAN-3]より選択します。
グループ	QoS ルールを適用するグループを[送信元 MAC アドレス]、[IP]、[ホスト名]から選択します。 [IP]を選択した場合は、サブネットアドレス(例:192.168.123.0)を指定し、サブネットマスクをプルダウンメニューから選択します。 [ホスト名]を選択した場合は、[オブジェクト定義]⇒[グルーピング]で設定したホストグループを選択できます。
サービス	QoS ルールに適用するサービスを指定します。サービスタイプは以下より選択します。 ◆全部: すべてのサービスタイプにQoSルールが適用されます。 ◆DSCP:TOSフィールド内のDSCP値でQoSルールを適用させます。この場合、プルダウンメニューから適用するDSCP値を選択します。 ◆TOS:[最小化コスト]、[最大化信頼性]、[最大化スループット]および[最小化遅延]を選択し、TOSフィールド情報からQoSルールの適合を判断します。 ◆ユーザー定義パケット:ユーザー定義のポート番号範囲とトランスポートプロトコル

項目	説明
	(TCP&UDP/TCP/UDP)を指定します。 ◆既知のサービス:プルダウンメニューからQoSルールを適用する既知のサービスを選択します。
キュー送信	本ルールに適用する送信キューを設定します。 設定しなかった場合は、Default-Outboundの送信キューが適用されます。 キューの設定方法は8.8.3.3を参照してください。
キューインバウンド	本ルールに適用する受信キューを設定します。 設定しなかった場合は、Default-inboundの受信キューが適用されます。 キューの設定方法は 8.8.3.3 を参照してください。
時間スケジュール	あらかじめ設定した時間スケジュールに則り本ルールを適用します。時間スケジュールの設定については、9.1.項のスケジューリングを参照してください。
ルール有効	[有効]にチェックを入れると、本 QoS ルールが有効になります。

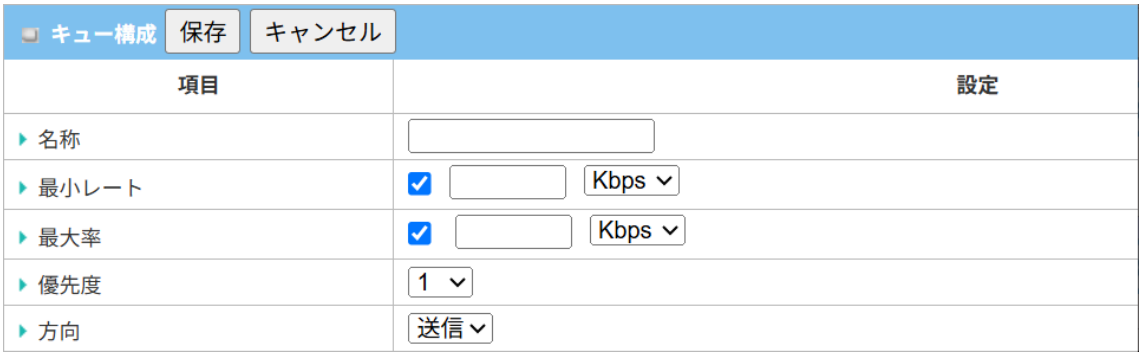
◆ 保存をクリックして、ルールを登録します。設定したルールが[QoSルールリスト]に表示されます。

8.8.3.3. キューの設定

ハードウェア QoS のルールの設定で適用するキューの設定を行います。



追加または編集をクリックすると[QoS ルール構成]画面が表示されます。



項目	説明
名称	本ルールの任意の名称を入力します。 Default-inbound および Default-Outbound の名称は固定です。
最小レート	回線混雑時でも、このキューに最低限保証する通信速度を指定します。
最大レート	このキューが使用できる通信速度の最大値を指定します。
優先度	通信を処理する優先順位を指定します（数字が小さいほど最優先）。 Default-inbound および Default-Outbound では優先度は固定です。
方向	受信/送信どちらの方向に適用するキューかを設定します。 Default-inbound および Default-Outbound では方向は固定です。

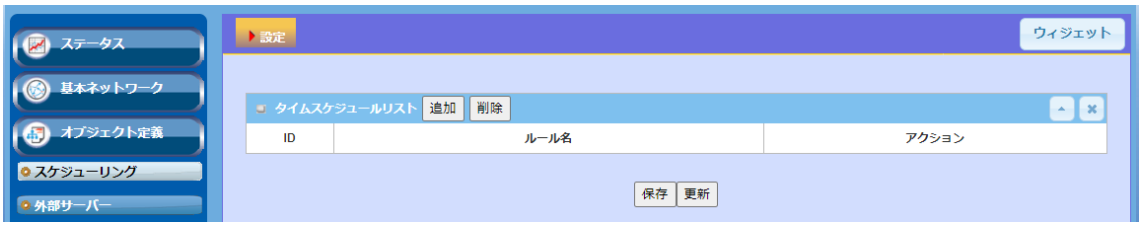
◆ 保存をクリックして、ルールを登録します。設定したルールが[キューリスト]に表示されます。

9. オブジェクト定義

9.1. スケジューリング

本機の各機能で使用するタイムスケジュールを追加または編集します。。

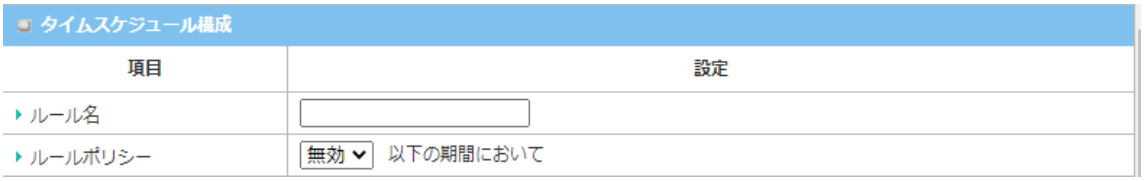
◆ 画面左側のメニューから、オブジェクト定義⇒スケジューリング⇒設定の順にクリックします。



9.1.1. タイムスケジュールリストの追加/編集



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



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

9.1.2. 期間定義の設定



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

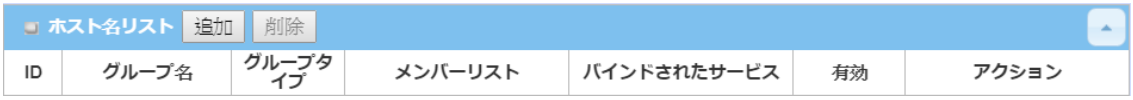
◆ [保存]をクリックして、設定を保存します。

9.2. グルーピング

9.2.1. ホストグループ

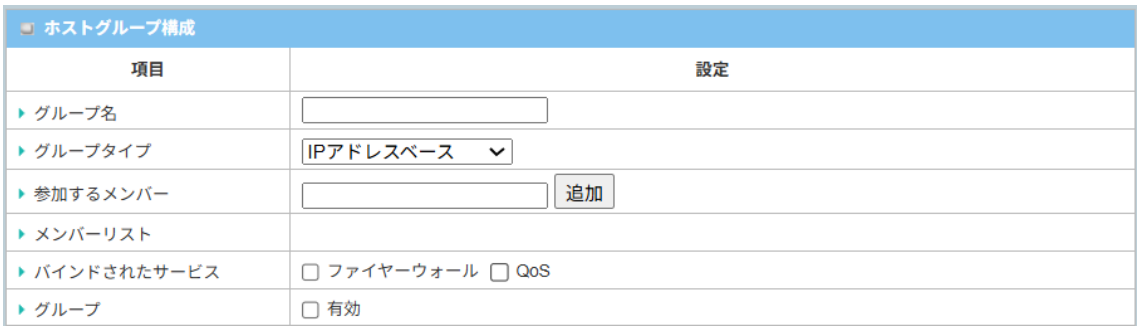
ここで設定したグループはファイヤーウォールおよび QoS の対象として選択できます。複数のホストを同じ条件で制御する場合に使用します。

画面左側のメニューから、オブジェクト定義⇒グルーピング⇒ホストグループの順にクリックします。



◆ 追加または編集をクリックすると、[ホストグループ構成]画面が表示されます。

9.2.1.1. ホストグループ構成

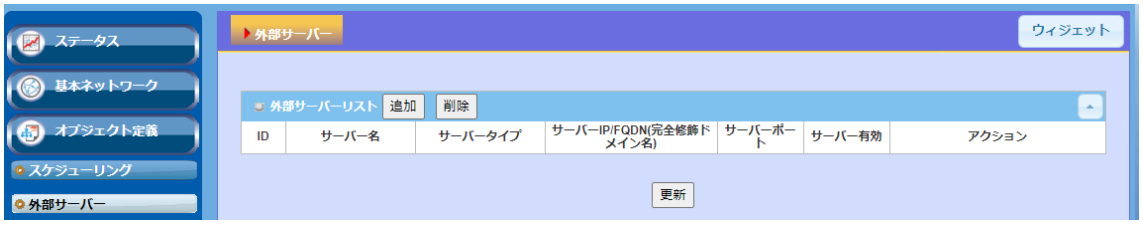


項目	説明
グループ名	任意のグループ名を入力します。
グループタイプ	ホストグループのグループタイプを選択します。IPアドレスベース、MACアドレスベースのいずれかから選択できます。 IPアドレスベースを選択した場合は、参加するメンバーの項目にIPアドレスのみ、MACアドレスベースを選択した場合はMACアドレスのみを追加できます。
参加するメンバー	グループにメンバーを追加するには、選択したグループタイプに応じたメンバー情報を入力し、[参加]をクリックします。1つずつ追加してください。
メンバーリスト	グループに含まれるメンバーを表示します。
バインドされたサービス	ホストグループを適用するサービスを関連付けます。ファイヤーウォールを有効にすると、作成したグループをファイヤーウォール機能で使用できるようになります。QoSも同様です。
グループ	[有効]にチェックを入れると、ホストグループのルールが有効になります。

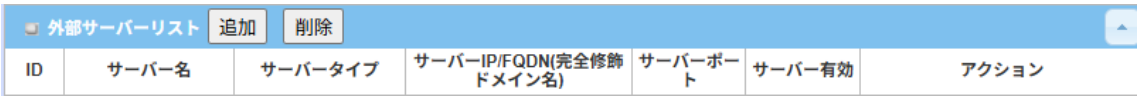
9.3. 外部サーバー

外部の SMTP サーバーや RADIUS サーバーを定義します。

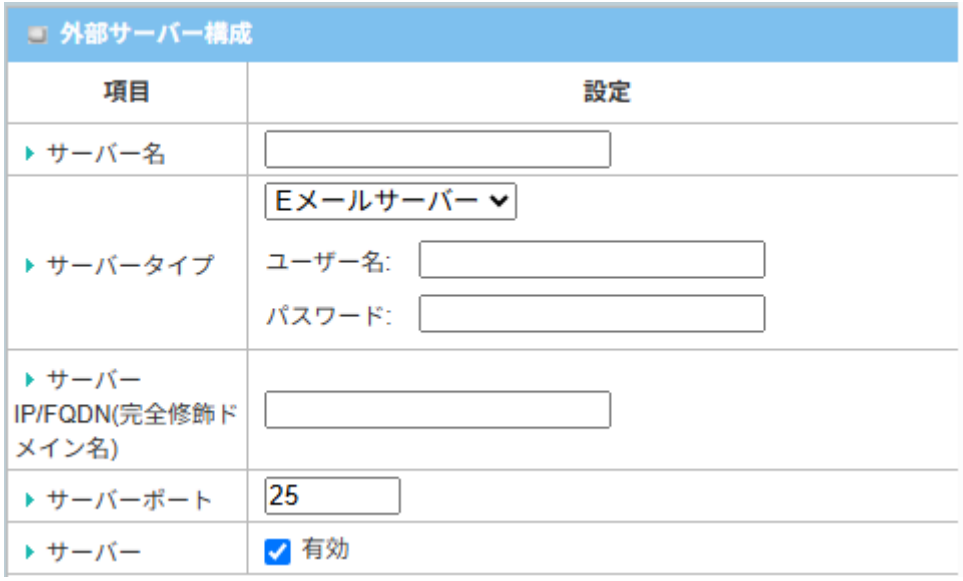
◆ 画面左側のメニューから、オブジェクト定義⇒外部サーバーの順にクリックします。



9.3.1. 外部サーバーリストの追加/編集



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



項目	説明
サーバー名	ルールを識別するためのサーバー名を指定します。
サーバータイプ	外部サーバーのサーバータイプを以下から選択し、サーバーにアクセスするために必要なパラメーターを指定します。 ◆Eメールサーバー：追加設定項目あり ユーザー名：文字列形式：任意のテキスト パスワード：文字列形式：任意のテキスト ◆Syslogサーバー：追加設定項目なし ◆RADIUSサーバー：追加設定項目あり プライマリ： プリシェアキー（事前共有キー）：文字列形式<任意のテキスト> 認証プロトコル：CHAPまたはPAPから選択します。 セッションタイムアウト：値の範囲は1～60分。 アイドルタイムアウト：値の範囲は1～15分。
サーバ IP/FQDN	外部サーバー用に使用するIPアドレスまたはFQDNを指定します。
サーバーポート または 認証ポート	外部サーバー用に使用するポートを指定します。特定のサーバータイプを選択した場合、初期サーバーポート番号が指定されています。 ◆Eメールサーバー：25 ◆Syslogサーバー：514 ◆RADIUSサーバー：1812
アカウンティングポート	外部RADIUSサーバーを選択する場合は、使用するアカウンティングポートを1～65535の範囲で指定します。
サーバー	[有効]にチェックを入れ、本ルールを有効します。

◆ 保存をクリックして、ルールを登録します。

設定したルールが[外部サーバーリスト]に表示されます。

9.4. 証明書

証明書は TLS によるセキュリティの重要な要素で、攻撃者が安全な Web サイトやその他のサーバーを偽装することを防ぎます。また、電子メールの暗号化やコード署名などの重要な用途でも使用されます。IPSec や OpenVPN の証明書を利用した認証で利用できます。

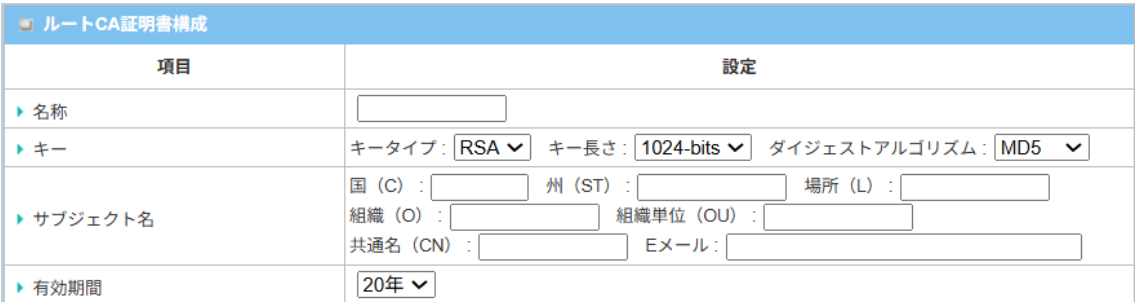
9.4.1. 設定

9.4.1.1. ルート CA の作成

◆ 画面左側のメニューから、オブジェクト定義⇒証明書⇒設定します。



◆ 生成をクリックすると、[ルート CA 証明書構成]画面が表示されます。



項目	説明
名称	証明書名を入力します。これが、証明書ファイル名になります。
キー	証明書のキー属性を指定します。 ◆公開鍵暗号システム：RSAのみがサポート ◆キービット長：[1024]、[1536]、[2048]から選択 ◆証明書の署名暗号化：[MD5]または[SHA-1]
サブジェクト名	証明書の情報を指定します。 ◆Country(C)（国（C））は、組織が所在する国の2文字のISOコードです。 ◆State(ST)（州（ST））は、組織が所在する州です。 ◆Location(L)（場所（L））は、組織が所在する場所です。 ◆Organization(O)（組織（O））は、組織の名称です。 ◆Organization Unit(OU)（組織単位（OU））は、組織単位の名称です。 ◆Common Name(CN) 証明書の対象を識別する名前を入力します。 ◆Email（Eメール）は、組織のEメールです。これは、Eメールアドレス設定でなければなりません。
有効期間	証明書の有効期間を指定します。

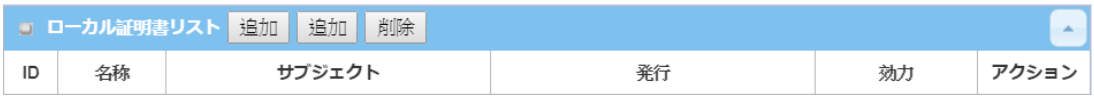
保存をクリックして、証明書を登録します。登録すると、[ルート CA]に設定が表示されます。

（注１） RSA 2048 bit 以上および SHA-256 以上を使用してください。RSA 1024/1536 bit、MD5 および SHA-1 は安全性が低いため、新しい証明書では使用しないでください。旧機器との互換性のために使用する場合は、接続範囲と利用期間を限定してください。

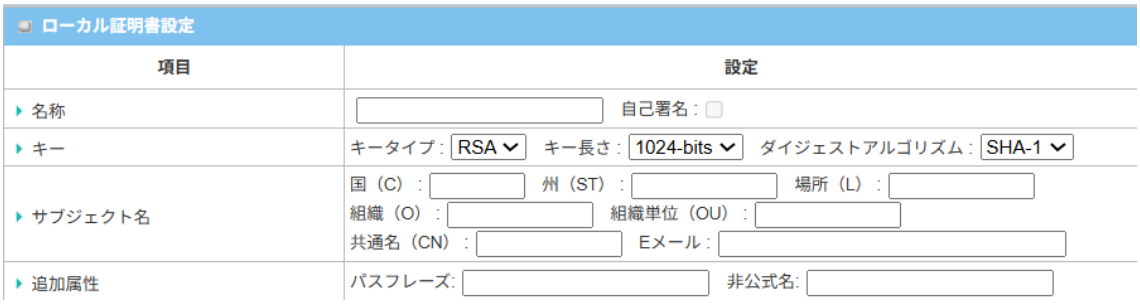
9.4.2. ローカル証明書

9.4.2.1. ローカル証明書の作成

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



◆ 画面左側の追加をクリックすると、[ローカル証明書構成]画面が表示されます。

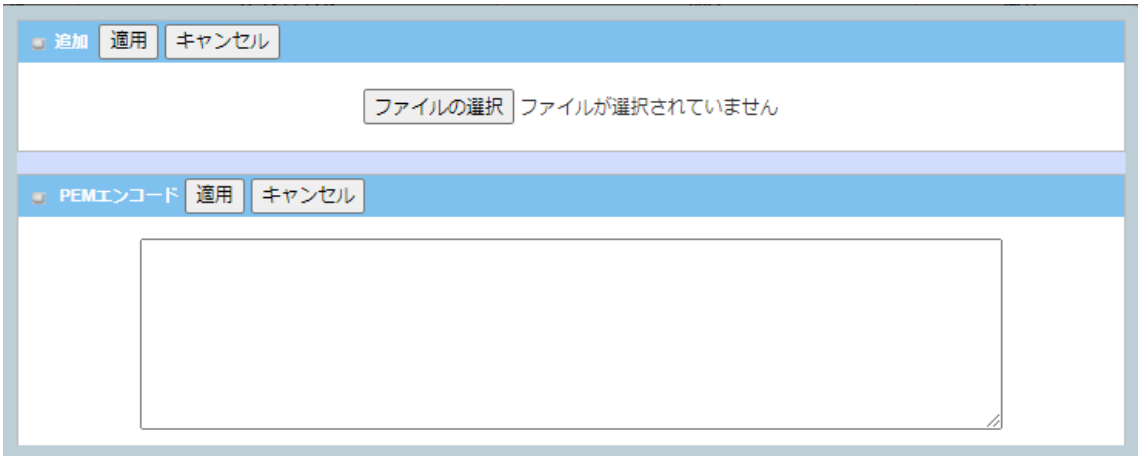


項目	説明
名称	証明書名を入力します。これが、証明書ファイル名になります ◆自己署名にチェックが入っている場合は、ルートCAにより署名されます。 ◆自己署名にチェックが入っていない場合、証明書署名要求(CSR)が生成されます。
キー	証明書のキー属性を指定します。 ◆公開鍵暗号システム:RSAのみがサポート ◆キービット長:[1024]、[1536]、[2048]から選択 ◆証明書の署名暗号化:[MD5]または[SHA-1]
サブジェクト名	証明書の情報を指定します。 ◆Country(C)(国(C))は、組織が所在する国の2文字のISOコードです。 ◆State(ST)(州(ST))は、組織が所在する州です。 ◆Location(L)(場所(L))は、組織が所在する場所です。 ◆Organization(O)(組織(O))は、組織の名称です。 ◆Organization Unit(OU)(組織単位(OU))は、組織単位の名称です。 ◆Common Name(CN)(共通名(CN))は、組織の名称です。 ◆Email(Eメール)は、組織のEメールです。これは、Eメールアドレス設定でなければなりません。
追加属性	証明書を生成するための追加情報を指定します。

保存をクリックして、証明書を登録します。

9.4.2.2. 証明書のインポート

右側の追加をクリックすると、[追加]画面が表示されます。既存の証明書ファイルから証明書を追加すること、または、証明書として PEM でエンコードされた文字列を直接貼り付けることができます。



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

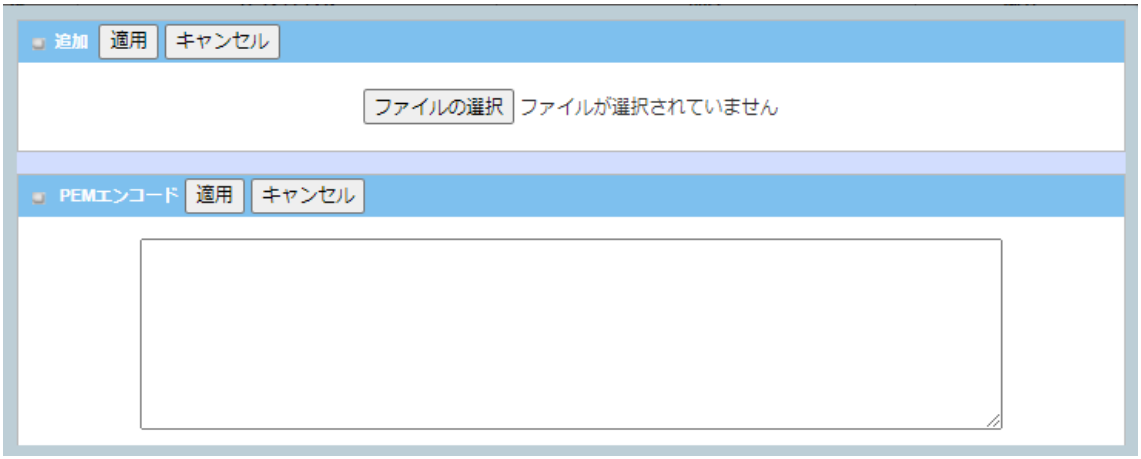
9.4.3. 信頼できる証明書

信頼できる[CA 証明書][クライアント証明書][クライアントキー]を設定します。

◆ 画面左側のメニューから、オブジェクト定義⇒証明書⇒信頼できる証明書の順にクリックします。

◆ 追加したい証明書、キーの項目の追加をクリックすると、インポート画面が表示されます。証明書ファイル、キーファイルから追加すること、または、PEM でエンコードされた文字列を直接貼り付けることができます。

※クライアントキーは、クライアント証明書の秘密鍵です。

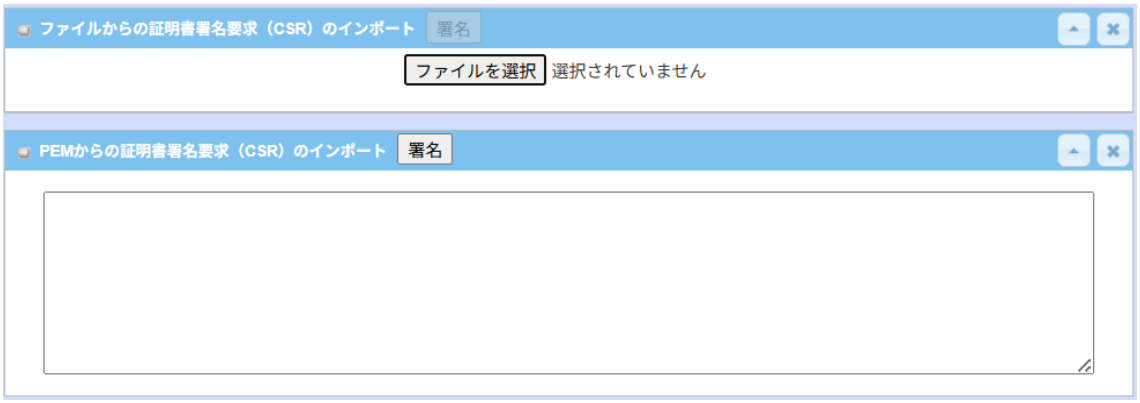


項目	説明
追加	ユーザーのコンピュータから証明書ファイルを選択し、適用をクリックして、指定した証明書ファイルをゲートウェイにインポートします。
PEM エンコード	PEMエンコードされた証明書文字列を直接入力（コピーアンドペースト）することができます。また、適用をクリックして、指定した証明書をゲートウェイにインポートすることができます。
適用	適用をクリックして、証明書をインポートします。

9.4.4. 発行証明書

証明書署名要求(CSR)をインポートし、ルート CA で署名を行います。

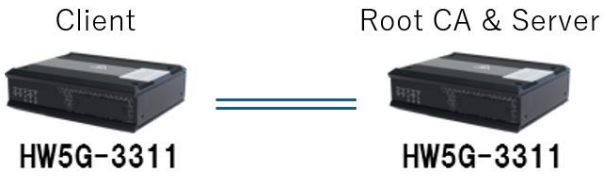
◆ 画面左側のメニューから、オブジェクト定義⇒証明書⇒発行証明書の順にクリックします。



項目	説明
ファイルからの証明書署名要求(CSR)のインポート	本機にインポートするコンピュータ証明書署名要求(CSR)ファイルを選択します。
PEM からの証明書署名要求(CSR)のインポート	PEMエンコードされた署名要求を直接入力（コピーアンドペースト）します。
署名	署名をクリックし、インポートしたCSRをルートCAより署名します

9.4.5. 証明書設定方法

OpenVPN の TLS 認証や IPsec などで使用する証明書の下図のような
最小構成での設定方法について説明します。

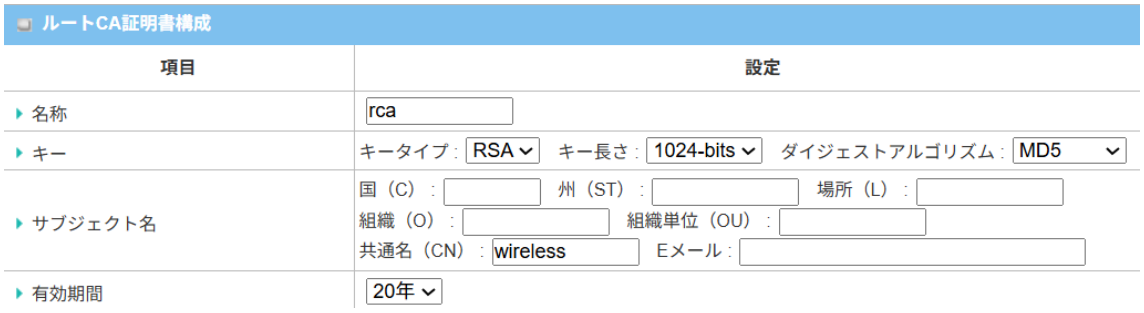


最小構成で必要な証明書

Root CA & Server	CA 公開鍵/秘密鍵, CA で署名したサーバ証明書とその秘密鍵
Client	CA の公開鍵, CA により署名されたクライアント証明書とその秘密鍵

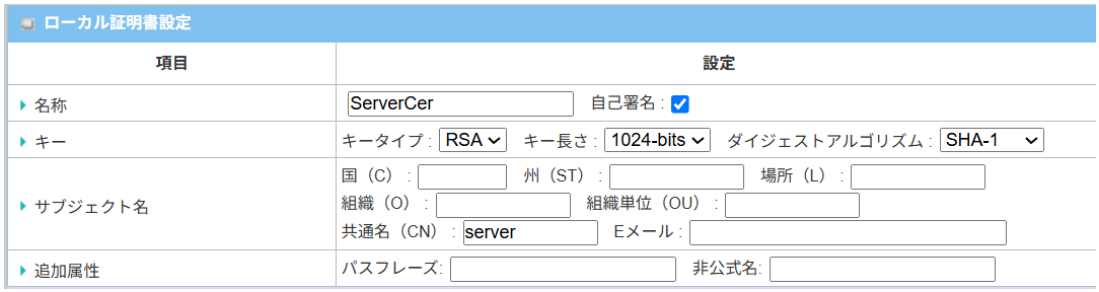
9.4.5.1. Root CA の秘密鍵/公開鍵の生成

1.Server 側のオブジェクト定義⇒証明書⇒設定⇒ルート CA の生成をクリックします。
2.任意の名称・キー・サブジェクト名・有効期限を入力し保存をクリックします。
※Root CA の秘密鍵は表示されません。



9.4.5.2. サーバ証明書とその秘密鍵の生成

1.Server 側のオブジェクト定義⇒証明書⇒ローカル証明書の左側の追加をクリックします。
2.自己署名にチェックを入れ任意の名称・キー・サブジェクト名・有効期限を入力し保存をクリック
※ 自己署名は通常、自身の秘密鍵で署名することを意味するが、
本機では自身で定義したルート CA 証明書で署名を行う。



9.4.5.3. クライアント側への CA の公開鍵の登録

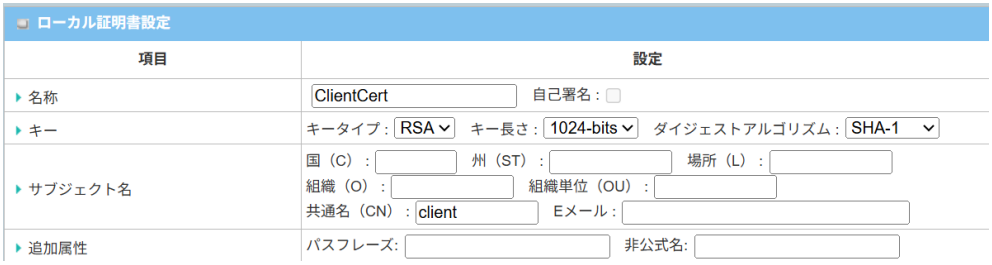
1.Server 側のオブジェクト定義⇒証明書⇒設定⇒ルート CA から 9.4.5.1 で設定したルート CA のビューをクリックし、表示された画面より CA 公開鍵をダウンロードする。
2.Client 側のオブジェクト定義⇒証明書⇒信頼できる証明書⇒信頼できる CA 証明書リストの追加をクリック。先ほどダウンロードした CA 公開鍵を選択し、適用をクリックします。



9.4.5.4. クライアント証明書とその秘密鍵の生成とインポート

1.Client 側のオブジェクト定義⇒証明書⇒ローカル証明書の左側の追加をクリックします。

2.自己署名オフで、任意の名称・キー・サブジェクト名・有効期限を入力し保存をクリックします。



3.アクションのビューから証明書と証明書キーをダウンロードします。



4.Server 側のオブジェクト定義⇒証明書⇒発行証明書に先ほどダウンロードしたクライアントの証明書をインポートし署名をクリックします。

5.CA により署名されたクライアント証明書が表示されるのでダウンロードします。



6.Client 側のオブジェクト定義⇒証明書⇒ローカル証明書の右側の追加をクリックして CA より署名されたクライアント証明書をインポートします。



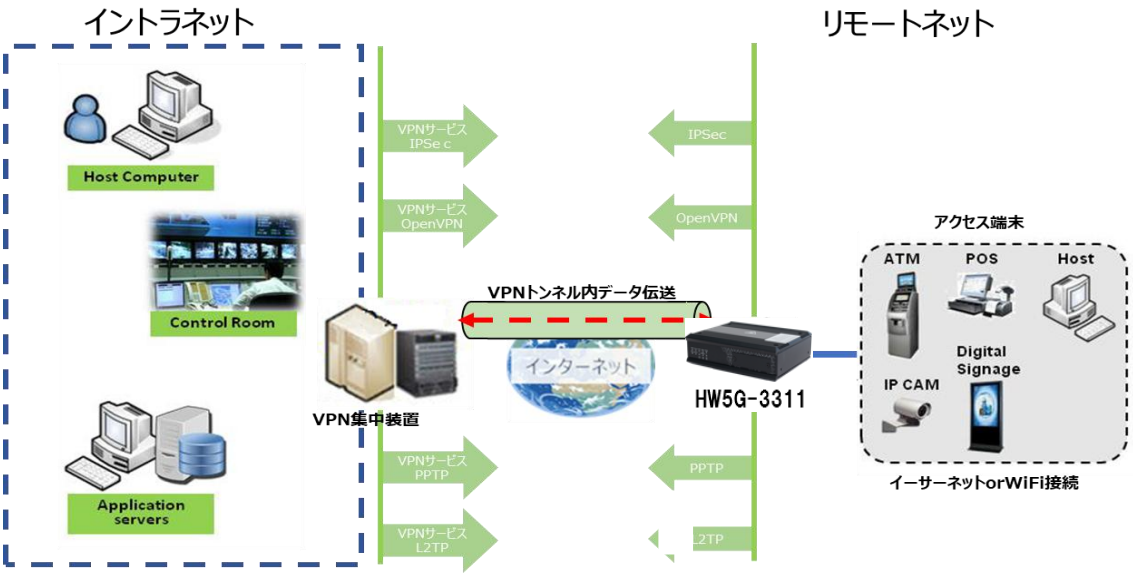
7.Client 側のオブジェクト定義⇒証明書⇒信頼できる証明書にクライアント証明書キーをインポートします。



10. セキュリティ

10. 1. VPN

VPN は、離れたネットワークまたは端末間に仮想的な通信経路を構成する機能です。使用するプロトコルと設定に応じて、通信の暗号化、相手の認証およびデータの完全性確認を行います。GRE および L2TP 単体には暗号化機能がないため、暗号化が必要な場合は IPsec などと組み合わせて使用してください。



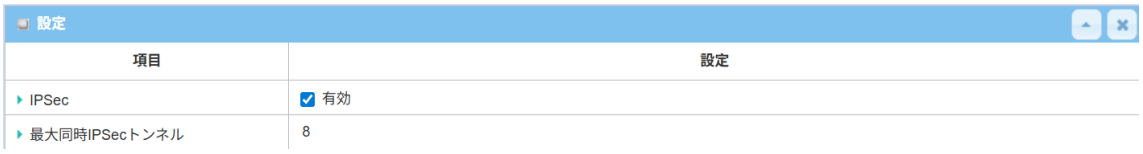
10.1.1. IPSec

IPsec（Internet Protocol Security）は、通信セッションで送受信される各 IP パケットを認証および暗号化し、IP 通信を保護するためのプロトコルです。

IPsec VPN トンネルは、IPsec クライアント（イニシエーター）と IPsec サーバー（レスポンダー）の間に確立されます。本機は、IPsec クライアントと IPsec サーバーのどちらとしても動作できるため、さまざまなリモートデバイスとの間にトンネルを確立できます。

10.1.1.1. IPSec の設定

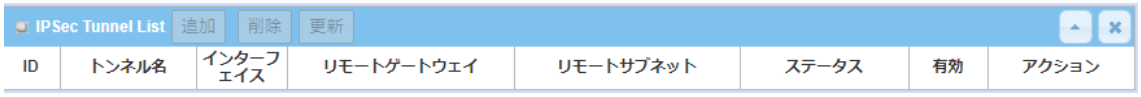
◆ 画面左側のメニューから、セキュリティ⇒VPN⇒IPSec の順にクリックします。



項目	説明
IPSec	[有効]にチェックを入れると、IPSecVPNが有効になります。
最大同時 IPSec トンネル	本機の場合、8です。

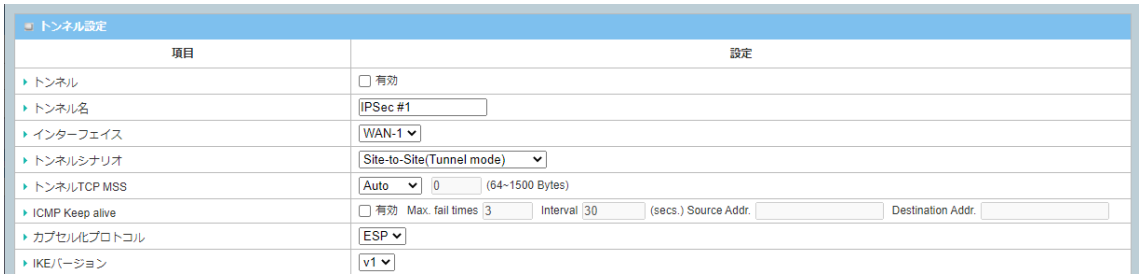
◆ 保存をクリックして、設定を登録します。

10.1.1.2. IPSec トンネルの追加/編集



◆ 追加または編集をクリックすると、[設定]画面が表示されます。[トンネル設定]、[ローカル＆リモート設定]、[認証]、[IKE フェーズ]、[IKE プロポーザル定義]、[IPSec フェーズ]および[IPSec プロポーザル定義]の項目を設定します。

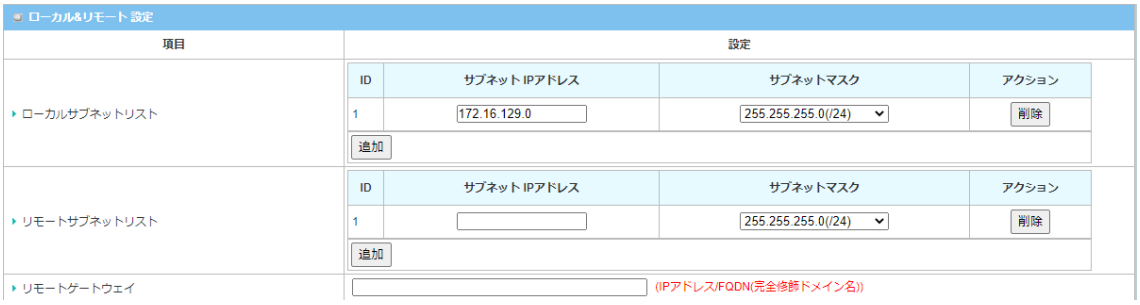
10.1.1.3. トンネル設定



項目	説明
IPSec	[有効]にチェックを入れると、トンネル有効になります。
トンネル名	識別のためのトンネル名（19文字以下）を指定します。
インターフェイス	IPSecトンネルを確立するインタフェースを[WAN]および[LAN]から選択します。

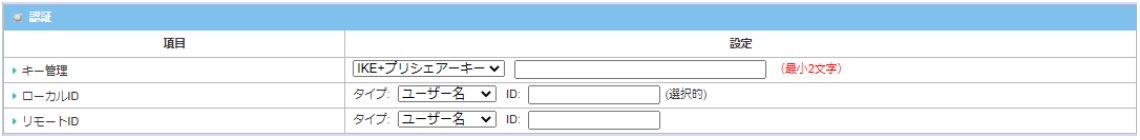
項目	説明
トンネルシナリオ	アプリケーションのドロップダウンボックスから、IPSecトンネリングシナリオを選択します。 ◆Site to Site：サブネット間接続 ◆Site to Host: サブネット→ホスト間接続 ◆Host to Site:ホスト→サブネット接続 ◆Host to Host：ホスト→ホスト接続
トンネル TCP MSS	ドロップダウンボックスから選択して、Tunel TCPMSSのサイズを定義します。 Auto：すべてのデバイスがこのパラメータを自動的に調整します。 Manual：Tunel TCPMSSの期待される値を指定します。値の範囲は64～1500バイトです。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

10.1.1.4. ローカル＆リモート設定



項目	説明
ローカルサブネットリスト	ローカルサブネットのIPアドレスとサブネットマスクを指定します。 ローカルサブネットが複数ある場合は追加で追加します。
リモートサブネットリスト	リモートサブネットのIPアドレスとサブネットマスクを指定します。 リモートサブネットが複数ある場合は追加で追加します。
リモートゲートウェイ	リモートゲートウェイのIPアドレスまたはFQDNを指定します。

10.1.1.5. 認証設定



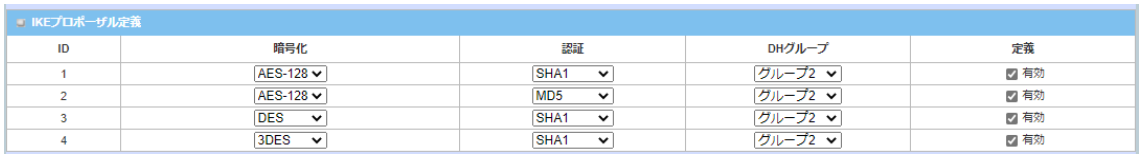
項目	説明
キー管理	キー管理方法を選択します。 ◆IKE+事前共有キー：キー（8～32文字）を指定します。 ◆IKE+X.509：証明書を使用して認証します。証明書の詳細は証明書の項目を参照してください。
ローカル ID	IPSecトンネルのローカルIDを指定します。IDの形式は[ユーザー名]、[FQDN]、[User@FQDN]または[キーID]から選択し、それぞれに適合したフォーマットでIDを指定します。
リモート ID	IPSecトンネルのリモートIDを指定します。IDの形式は[ユーザー名]、[FQDN]、[User@FQDN]または[キーID]から選択し、それぞれに適合したフォーマッ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

10.1.1.6. IKE フェーズ設定



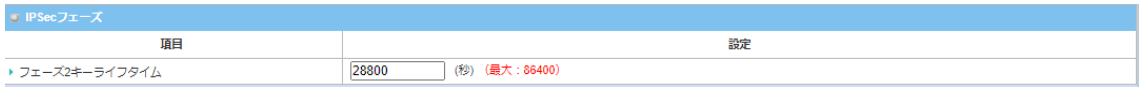
項目	説明
ネゴシエーションモード	IKEv1では、メインまたはアグレッシブモードを選択します。XAuthを使用する場合はIKEv1を選択してください。IKEv2ではメインモード、アグレッシブモードおよびXAuthは使用しません。
X-Auth	IPSecトンネルのX-Authの役割を[サーバー]、[クライアント]または[なし]から選択します。XAuthを使用する場合はIKEv1を選択してください。 ◆サーバー：、X-Authサーバーになります。X-Authアカウントをクリックして、リモートX-Authクライアントアカウントを作成します。 ◆クライアント；このゲートウェイは、X-Authクライアントになります。X-Authサーバーゲートウェイによって認証されるユーザー名とパスワードを指定します。 ◆なし：：X-Auth認証は無効です。
デッドピア検出（DPD）	[有効]にチェックを入れて、DPD機能を有効します。タイムアウトおよび遅延時間を0～999秒の範囲で指定します。
フェーズ 1 キーライフタイム	フェーズ1キーライフタイムを30～86400秒の範囲で指定します。

10.1.1.7. IKE プロポーザル定義



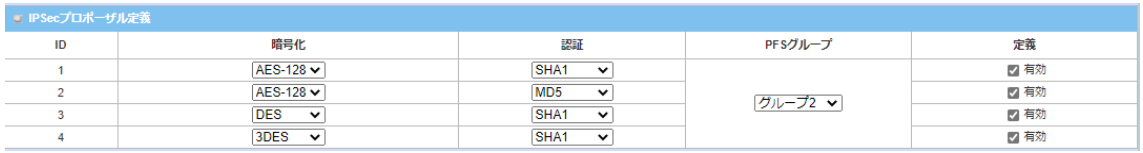
項目	説明
暗号化	IKE（フェーズ1）の暗号化方式を[DES]、[3DES]、[AES-auto]、[AES-128]、[AES-192]または[AES-256]から選択します。
認証	認証時の暗号化方法を[なし]、[MD5]、[SHA1]または[SHA2-256]から選択します。
DH グループ	DH（Diffie-Hellman）グループを選択します。
定義	[有効]にチェックを入れると、このIKEプロポーザルが有効になります。

10.1.1.8. IPSec フェーズ設定



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

10.1.1.9. IPSec プロポーザル定義



項目	説明
暗号化	IPSecデータ通信の暗号化方式を[なし]、[DES]、[3DES]、[AES-auto]、[AES-128]、[AES-192]または[AES-256]から選択します。[なし]はカプセル化プロトコルが[AH]の場合のみ使用できます。
認証	整合性／認証アルゴリズムを[なし]、[MD5]、[SHA1]または[SHA2-256]から選択します。[なし]および[SHA2-256]はカプセル化プロトコルが[ESP]の場合のみ使用できます。
PFS グループ	PFS（Perfect Forward Security）グループを選択します。
定義	[有効]にチェックを入れると、このIPSecプロポーザルが有効になります。

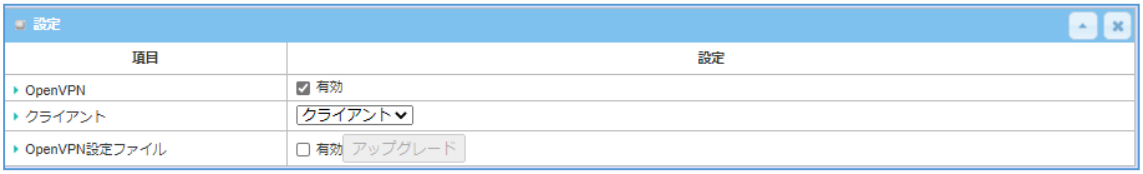
◆ 保存をクリックして、ルールを登録します。設定したルールが[IPSec トンネルリスト]に表示されます。

10.1.2. OpenVPN

OpenVPN は、事前共有キーまたは証明書を使って、お互いに認証するサーバー＆クライアント形式のトンネリング技術です。加えて、OpenVPN は[TUN：レイヤ3レベル]と[TAP：レイヤ2レベル]の 2 つのトンネリングモードに対応しています。

10.1.2.1. OpenVPN の設定

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



項目	説明
OpenVPN	[有効]にチェックを入れると、OpenVPNが有効になります。
クライアント	サーバーもしくはクライアントを選択します。
OpenVPN 設定ファイル	[有効]にチェックを入れると、事前設定ファイルからのクライアント起動が有効になります。アップグレードをクリックして、新規事前設定ファイルをアップロードすることができます。 （注）本機能を有効にすると、クライアントルールの設定ができなくなります。

◆ 保存をクリックして、設定を登録します。

10.1.2.2. OpenVPN サーバー構成



項目	説明
OpenVPN サーバー	[有効]にチェックを入れると、OpenVPNサーバーが有効になります。
プロトコル	OpenVPNクライアントの制御プロトコルを[UDP]または[TCP]から選択し、必要があればポート番号も指定します。 ◆TCP：OpenVPNはTCPプロトコル（ポート番号4430自動設定）を使用します。 ◆UDP：OpenVPNはUDPプロトコル（ポート番号1194自動設定）を使用します。
ポート	OpenVPNにサーバーに接続するためのポートを指定します。
トンネルシナリオ	OpenVPNが使用するトンネルシナリオを[TUN]または[TAP]から選択します。
リモート IP/FQDN	OpenVPNサーバーのIPアドレスまたはFQDNを指定します。
リモートサブネット	OpenVPNサーバーのサブネットとサブネットマスクを指定します。
リダイレクトインターネットトラフィック	[有効]にチェックを入れると、リダイレクトインターネットトラフィック機能が有効になります。
NAT	[有効]にチェックを入れると、NAT機能が有効になります。
認証モード	認証モードを[TLS]または[静的キー]から選択します。 ◆TLS：OpenVPNはTLS認証モードを使用し、CA証明書、クライアント証明書を使用します。 ◆静的キー：OpenVPNは静的キー認証モードを使用し、ローカルエンドポイントIPアドレス、リモートエンドポイントIPアドレス、静的キーの項目が表示されます。
ローカルエンドポイント IP アドレス	OpenVPNゲートウェイのローカルエンドポイントIPアドレスを指定します。この項目は認証モードで[静的キー]を選択した時のみ利用可能です。

項目	説明
リモートエンドポイント IP アドレス	リモートOpenVPNゲートウェイのリモートエンドポイントIPアドレスを指定します。この項目は認証モードで[静的キー]を選択した時のみ利用可能です。
静的キー	静的キーを指定します。この項目は認証モードで[静的キー]を選択した時のみ利用可能です。
サーバー仮想 IP	サーバー仮想IPを指定します。この項目は認証モードで[TLS]を選択したときのみ利用可能です。
DHCP プロキシモード	[有効]にチェックを入れるとDHCP-プロキシモードが有効になります。 この項目はトンネルシナリオで[TAP]を選択したときのみ利用可能です。
IP プール	OpenVPNサーバーの仮想IPプールを設定します。この項目はトンネルシナリオで[TAP]を選択しており、DHCPプロキシモードがオフの時に設定可能です。
ゲートウェイ	OpenVPNサーバーのゲートウェイを設定します。この項目はトンネルシナリオで[TAP]を選択しており、DHCPプロキシモードがオフの時に設定可能です。
ネットマスク	OpenVPNサーバーのネットマスクを設定します。この項目はトンネルシナリオで[TAP]を選択しており、DHCPプロキシモードがオフの時に設定可能です。
リダイレクト デフォルトゲートウェイ	[有効]にチェックを入れ、リダイレクトデフォルトゲートウェイ機能を有効にします。有効の時、VPN接続している機器はすべてOpenVPNサーバー経由で通信するようになります。
暗号化方法	暗号化方法を[AES-256]、[AES-192]、[AES-128]または[なし]から選択します。
ハッシュ・アルゴリズム	ハッシュ・アルゴリズム[SHA-1]、[MD5]、[MD4]、[SHA2-256]、[SHA2-512]、[なし]または[無効]から選択します。
LZO 圧縮	LZO圧縮方法を[適用]、[はい]、[いいえ]または[デフォルト]から選択します。旧機器との互換性が必要な場合にのみ有効にしてください。
Persist キー	[有効]にチェックを入れると、Persistキー機能が有効になります。
Persist トンネル	[有効]にチェックを入れると、Persistトンネル機能が有効になります。
詳細構成	必要に応じて、編集をクリックすると詳細構成画面が表示されます。
トンネル	[有効]にチェックを入れると、本ルールが有効になります。

10.1.2.3. OpenVPN サーバーの詳細構成



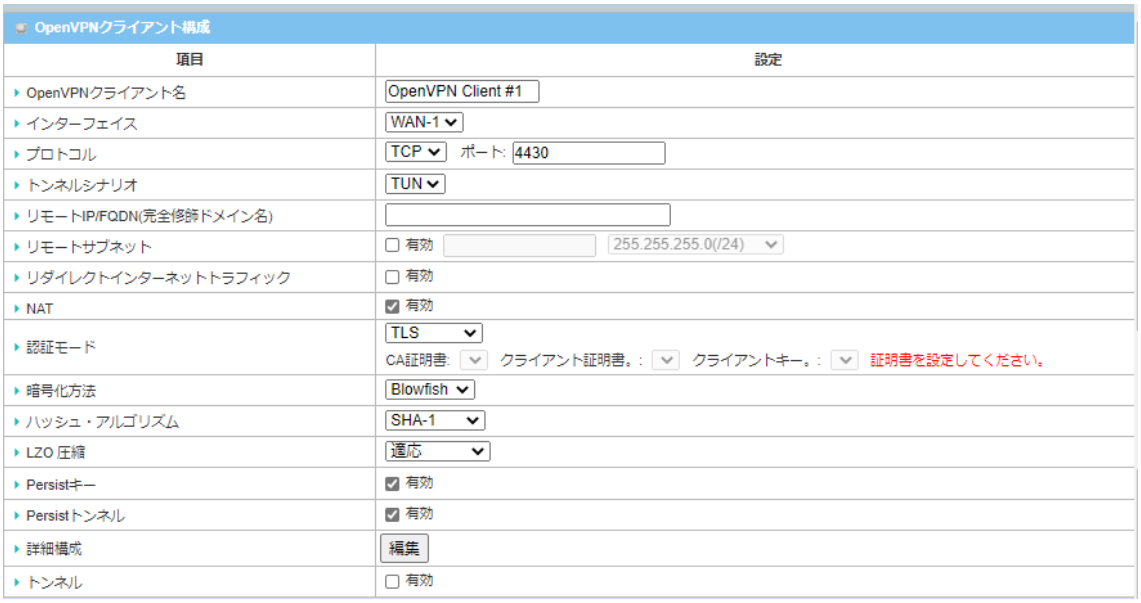
項目	説明
TLS Cipher	TLS暗号方式を[なし]、[TLS-RSA-WITH-RC4-MD5]、[TLS-RSA-WITH-AES128-SHA]、[TLS-RSA-WITH-AES256-SHA]、[TLS-DHE-DSS-AES128-SHA]または[TLS-DHE-DSS-AES256-SHA]から選択します。TLS暗号は、認証モードでTLSが選択されている場合のみ有効になります。
TLS Auth.キー（選択的）	OpenVPNサーバーTLS認証を要求している場合に、接続するためのキーを指定します。認証モードでTLSが選択されている場合のみ有効になります。
クライアント間	[有効]にチェックを入れると、異なるOpenVPNクライアント間の通信を有効にします。
CN の複製	[有効]にチェックを入れるとCNの複製機能を有効にします。この機能を有効にすると、同じVPN設定ファイルで複数端末がVPN接続できます。
トンネル MTU	トンネルを通過させるパケットのMTUを100～1500の間で指定します。VPNオーバーヘッドにより通信ができなくなる可能性があるため推奨値は1400です。
トンネルの UDP 断片化	トンネルのUDP断片化（フラグメント）時のパケットサイズを0～1500の範囲で指定します。プロトコルで”UDP”が選択されているときのみ利用できます。
トンネル UDP MSS-Fix	[有効]にチェックを入れると、トンネルUDP MSS-Fix機能が有効になります。プロトコルで”UDP”が選択されているときのみ利用できます。
CCD—Dir デフォルトファイル	本機ではサポートしておりません。
クライアント接続スクリプト	本機ではサポートしておりません。
追加構成	本機ではサポートしておりません。

◆ 保存をクリックして、設定を登録します。登録されると[OpenVPN サーバーリスト]にルールが表示されます。

10.1.2.4. OpenVPN クライアントリストの追加/編集



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

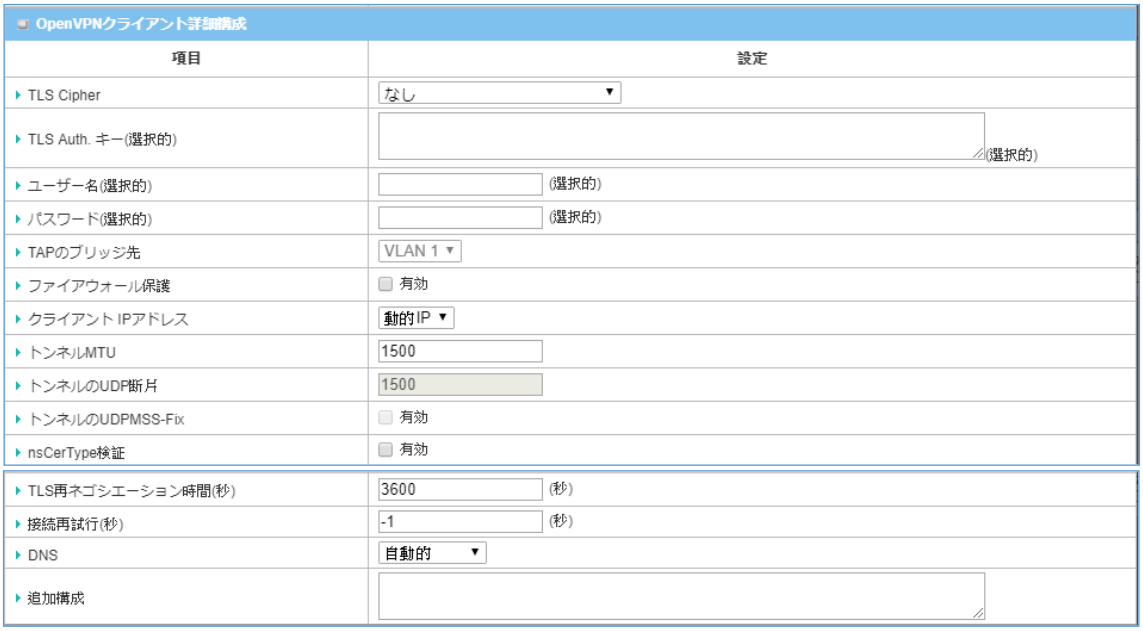


項目	説明
OpenVPN クライアント名	識別のため32文字以下のクライアント名を指定します。
インターフェイス	OpenVPNクライアントトンネルを確立するインタフェースを選択します。
プロトコル	OpenVPNクライアントの制御プロトコルを[UDP]または[TCP]から選択し、必要があればポート番号も指定します。 ◆TCP：OpenVPNはTCPプロトコル（ポート番号4430自動設定）を使用します。 ◆UDP：OpenVPNはUDPプロトコル（ポート番号1194自動設定）を使用します。
トンネルシナリオ	OpenVPNが使用するトンネルシナリオを[TUN]または[TAP]から選択します。
リモート IP/FQDN	OpenVPNサーバーのIPアドレスまたはFQDNを指定します。
リモートサブネット	OpenVPAサーバーのサブネットとサブネットマスクを指定します。
リダイレクトインターネットトラフィック	[有効]にチェックを入れると、OpenVPNサーバがデフォルトゲートウェイとして設定されます。
NAT	[有効]にチェックを入れると、NAT機能が有効になります。
認証モード	認証モードを[TLS]または[静的キー]から選択します。 ◆TLS：OpenVPNはTLS認証モードを使用し、CA証明書、クライアント証明書を使用します。 ◆静的キー：OpenVPNは静的キー認証モードを使用し、ローカルエンドポイントIPアドレス、リモートエンドポイントIPアドレス、静的キーの項目が表示されます。

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

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

10.1.2.5. OpenVPN クライアント詳細構成



項目	説明
TLS Cipher	TLS暗号方式を[なし]、[TLS-RSA-WITH-RC4-MD5]、[TLS-RSA-WITH-AES128-SHA]、[TLS-RSA-WITH-AES256-SHA]、[TLS-DHE-DSS-AES128-SHA]または[TLS-DHE-DSS-AES256-SHA]から選択します。TLS暗号は、認証モードでTLSが選択されている場合のみ有効になります。
TLS Auth.キー(選択的)	OpenVPNサーバーTLS認証を要求している場合に、接続するためのキーを指定します。認証モードでTLSが選択されている場合のみ有効になります。
ユーザー名(選択的)	サーバー認証に使用するユーザー名を指定します。認証モードでTLSが選択されている場合のみ有効になります。
パスワード(選択的)	サーバー認証に使用するパスワードを指定します。認証モードでTLSが選択されている場合のみ有効になります。
TAP のブリッジ先	TAPトンネルシナリオでTAPインタフェースを選択します。この機能により、LAN側へブリッジ接続されます。トンネルシナリオでTAPが選択され、NATが無効のとき利用可能となります。
ファイヤーウォール保護	[有効]にチェックを入れると、ファイヤーウォール保護機能が有効になります。本機能はNATが有効の時のみ利用可能です。
クライアント IP アドレス	OpenVPNクライアントの仮想IPアドレスの付与方法を[動的IP]または[静的IP]から選択します。[静的IP]を選択した時は、仮想IPアドレスとそのサブネットマスクを指定します。
トンネル MTU	トンネルを通過させるパケットのMTUを100～1500の間で指定します。

項目	説明
	VPNオーバーヘッドにより通信ができなくなる可能性があるため推奨値は1400です。
トンネルの UDP 断片化	トンネルのUDP断片化（フラグメント）時のパケットサイズを0～1500の範囲で指定します。プロトコルで"UDP"が選択されているときのみ利用できます。
トンネル UDP MSS-Fix	[有効]にチェックを入れると、トンネルUDP MSS-Fix機能が有効になります。プロトコルで"UDP"が選択されているときのみ利用できます。
nsCertType 検証	本機ではサポートしておりません。
TLS 再ネゴシエーション間隔	TLS再ネゴシエーションの時間間隔を1～86400（秒）の範囲で指定します。
接続再試行	接続再試行の時間間隔を1～86400（秒）の範囲で指定します。 1以下は接続再試行が必要ないことを意味します。
DNS	DNSの方法を[自動]または[手動]から選択します。[手動]選択した場合は、プライマリDNSおよびセカンダリDNSを手動で指定します。
追加構成	本機ではサポートしておりません。

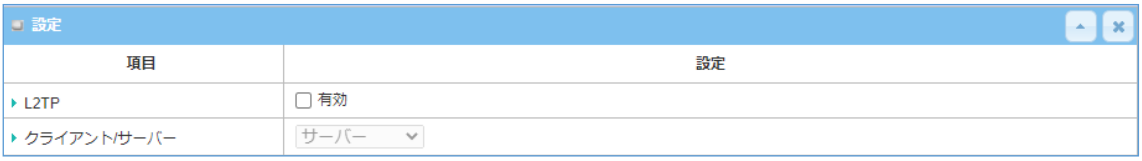
◆ 保存をクリックして、設定を登録します。登録されると[OpenVPN クライアントリスト]にルールが表示されます。

10.1.3. L2TP

L2TP は、VPN の構築や、ISP（プロバイダ）によるサービス提供の一部に使用されるトンネリングプロトコルです。L2TP 自体には、通信を暗号化して機密性を確保する機能はありません。そのため、通信の機密性を確保するには、トンネル内を通過するデータを別の暗号化プロトコルで保護する必要があります。

10.1.3.1. L2TP の設定

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



項目	説明
L2TP	[有効]にチェックを入れると、L2TPトンネリングが有効になります。
クライアント/サーバー	設定するロール（クライアントまたはサーバー）を指定します。

◆ 保存をクリックして、設定を登録します。

10.1.3.2. L2TP サーバーの設定



項目	説明
L2TP サーバー	[有効]にチェックを入れると、L2TPサーバー設定が有効になります。
インターフェイス	L2TPトンネルを確立するインタフェースを[WAN]または[LAN]から選択します。[WAN-1]しか選択できない場合があります。
L2TP over IPSec	[有効]にチェックを入れると、L2TP over IPSecモード（IPSecによる暗号化）を有効にします。有効にした場合は文字長8～32のプリシェアキーを指定します。
サーバー仮想 IP	本機のL2TPサーバーで使用するサーバ仮想IPアドレスを指定します。
IP プール開始アドレス	L2TPトンネルのクライアントに付与するIPの開始アドレスを指定します。 値の範囲は1～255です。
IP プール終了アドレス	L2TPトンネルのクライアントに付与するIPの終了アドレスを指定します。

項目	説明
	値の範囲は1～255です。
認証プロトコル	L2TPクライアントを認証する認証プロトコルを[PAP]、[CHAP]、[MS-CHAP]および[MS-CHAP v2]から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、L2TP接続用のMPPE（Microsoft Point-to-Point Encryption）セキュリティが有効になります。MPPE暗号化が有効の場合、認証プロトコルPAP/CHAPは使用できません。
サービスポート	L2TPトンネリングのサービスポートを以下から選択し、必要があればサービスポートを指定します。 ◆自動：自動的にサービスポートを割り振ります。 ◆1701 (for Cisco)：CISCO L2TPサーバー接続時に選択します。 ◆ユーザー定義：1～65535の範囲の任意のポート番号を指定します。

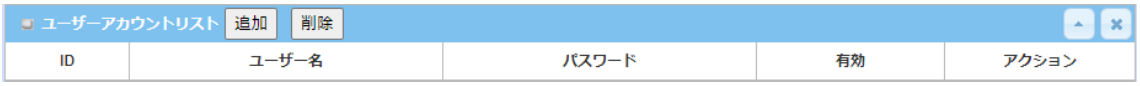
10.1.3.3. L2TP サーバーステータス

接続中の L2TP クライアントに関する情報が表示されます。表示項目は、[ユーザー名]、[リモート IP]、[リモート仮想 IP]、[リモートコール ID]、および[アクション]です。必要に応じて、一覧の[切断]をクリックすると、対象の L2TP 接続を切断できます。

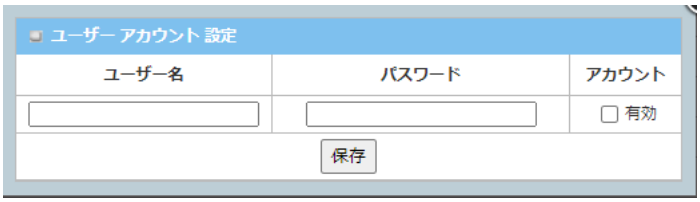


10.1.3.4. ユーザーアカウントの追加・編集

L2TP サーバーで使用するユーザーアカウントを最大10まで指定することができます。



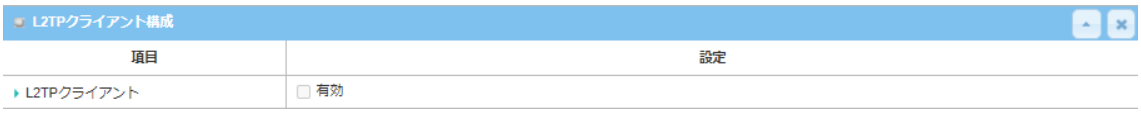
◆ 追加または編集をクリックすると、[ユーザーアカウント設定]画面が表示されます。



項目	説明
ユーザー名	ユーザー名を指定します。文字数は1～32文字です。
パスワード	該当ユーザーのパスワードを指定します。文字数は1～32文字です。
アカウント	[有効]にチェックを入れると、本アカウントが有効になります。

◆ 保存をクリックして、設定を登録します。登録されると[ユーザーアカウントリスト]にアカウントが表示されます。

10.1.3.5. L2TP クライアントの設定



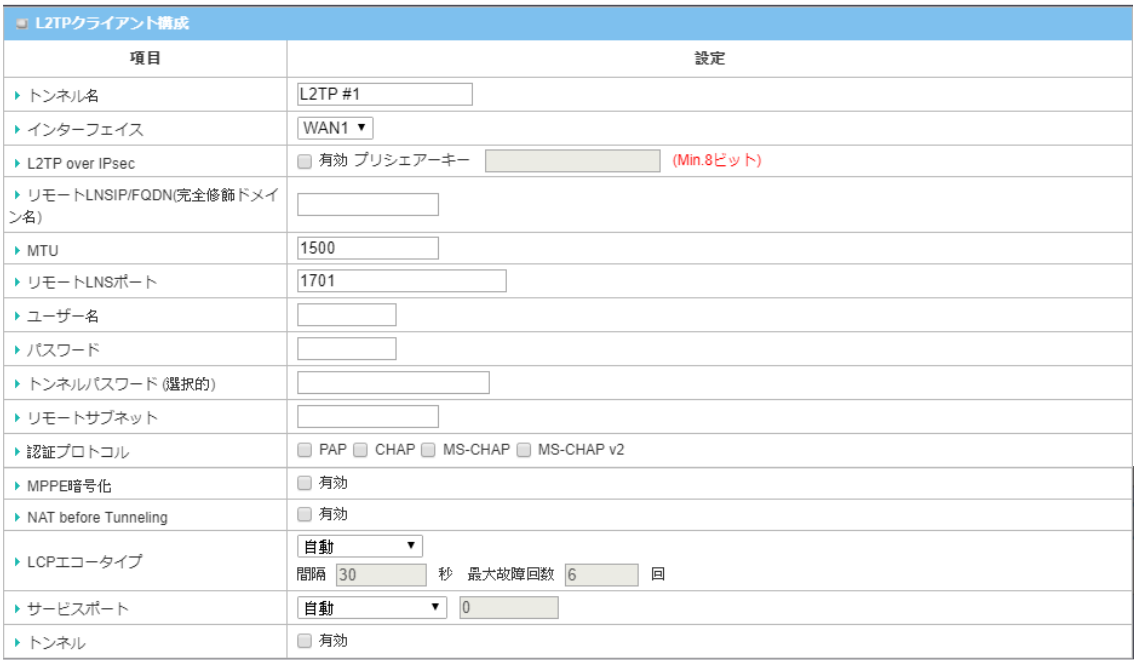
項目	説明
L2TP クライアント	[有効]にチェックを入れると、L2TPクライアント設定が有効になります。

◆ 保存をクリックして、設定を登録します。

10.1.3.6. L2TP クライアントリストの追加/編集



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



項目	説明
トンネル名	識別のため32文字以下のトンネル名を指定します。
インターフェイス	L2TPトンネルを確立するインタフェースを[WAN]または[LAN]から選択します。[WAN-1]しか選択できない場合があります。
MTU	L2TPトンネルを通過させるパケットのMTUを64～1500の間で指定します。VPNオーバーヘッドにより通信ができなくなる可能性があるため推奨値は1400です。
L2TP over IPSec	[有効]にチェックを入れると、L2TP over IPSecモード(IPSecによる暗号化)を有効にします。有効にした場合は文字長8～32のプレシェアキーを指

項目	説明
	定します。
リモート LNS IP/FQDN	L2TPサーバーのIPアドレスまたはFQDNを入力します。
リモート LNS ポート	L2TPトンネルのリモートLNSポートを1～65535の範囲で指定します。通常は“1701”を使用します。
ユーザー名	L2TPサーバーに接続するためのユーザー名（32文字以下）を指定します。
パスワード	L2TPサーバーに接続するためのパスワードを指定します。
トンネリングパスワード	L2TPサーバーの要求など必要があれば、L2TPトンネリング用のトンネリングパスワードを指定します。
リモートサブネット	リモートサブネットをIPアドレス/ネットマスク（例：192.168.123.100/24）のフォーマットで指定します。0.0.0.0/0を指定するとL2TPトンネルがデフォルトゲートウェイとして扱われ、全てのパケットはL2TPトンネルを通過するようになります。
認証プロトコル	L2TP接続に使用する認証プロトコルを[PAP]、[CHAP]、[MS-CHAP]および[MS-CHAP v2]から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、L2TP接続用のMPPE（Microsoft Point-to-Point Encryption）セキュリティが有効になります。L2TPサーバーが対応しているときのみ有効にしてください。MPPE暗号化が有効の場合、認証プロトコルPAP/CHAPは使用できません。
NAT before Tunneling	[有効]にチェックをすると、L2TPトンネルを通過する前にNAT機能によるアドレス変換が有効になります。
LCP エコータイプ	L2TPトンネルのLCPエコータイプを以下から選択します。 ◆自動：自動的に間隔および最大故障回数を指定します ◆ユーザー定義：間隔（1～99,999秒）および最大故障回数（1～999回）の範囲で指定します。 ◆無効：LCPエコーは無効です。
サービスポート	L2TPトンネリングのサービスポートを以下から選択し、必要があればサービスポートを指定します。 ◆自動：自動的にサービスポートを割り振ります。 ◆1701 (for Cisco)：CISCO L2TPサーバー接続時に選択します。 ◆ユーザー定義：1～65535の範囲の任意のポート番号を指定します。
トンネル	[有効]にチェックを入れると、本ルールが有効になります。

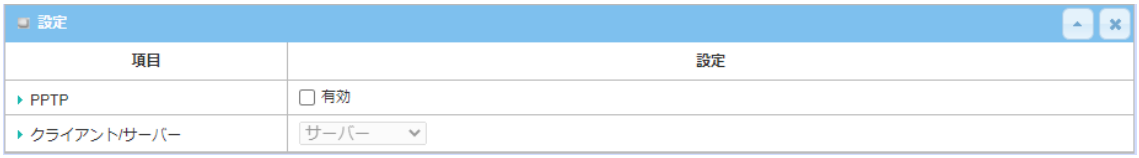
◆ 保存をクリックして、ルールを登録します。設定したルールが[L2TP クライアントリスト]に表示されます。

10.1.4. PPTP

PPTP は VPN を構築するためのトンネリングプロトコルです。PPTP では、TCP による制御チャネルと、PPP パケットをカプセル化するための GRE トンネルを使用します。複数の認証方式および暗号化レベルに対応し、Windows では標準の PPTP 機能として利用できます。機は PPTP クライアント機能と PPTP サーバー機能を備えています。[クライアント]を選択すると本機から PPTP サーバーへ接続し、[サーバー]を選択すると PPTP クライアントからの接続を受け付けます。

10.1.4.1. PPTP の設定

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



項目	説明
PPTP	[有効]にチェックを入れると、PPTPトンネリングが有効になります。
クライアント/サーバー	クライアントまたはサーバーを指定します。

◆ 保存をクリックして、設定を登録します。

10.1.4.2. PPTP サーバーの設定

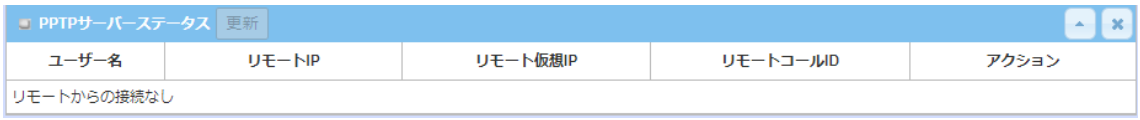


項目	説明
PPTP サーバー	[有効]にチェックを入れると、PPTPサーバー設定が有効になります。
インターフェイス	PPTPトンネルを確立するインタフェースを[WAN]または[LAN]から選択します。[WAN-1]しか選択できない場合があります。
サーバー仮想 IP	本機のPPTPサーバーで使用する仮想IPアドレスを指定します。
IP プール開始アドレス	PPTPトンネルのクライアントに付与するIPの開始アドレスを指定します。 値の範囲は1～255です。
IP プール終了アドレス	PPTPトンネルのクライアントに付与するIPの終了アドレスを指定します。 値の範囲は1～255です。
認証プロトコル	PPTPクライアントを認証する認証プロトコルを[PAP]、[CHAP]、[MS-CHAP]および[MS-CHAP v2]から指定します。複数の認証プロトコルを指

項目	説明
	定することができます。
MPPE 暗号化	[有効]にチェックをすると、PPTP接続用のMPPE（Microsoft Point-to-Point Encryption）セキュリティが有効になります。MPPE暗号化が有効の場合、認証プロトコルPAP/CHAPは使用できません。

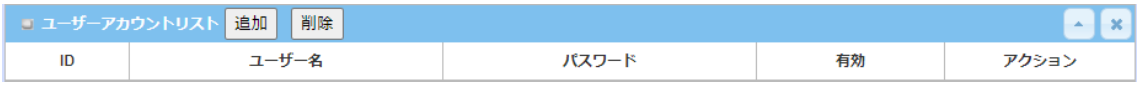
10.1.4.3. PPTP サーバーステータス

接続中の PPTP クライアントに関する情報が表示されます。表示項目は、[ユーザー名]、[リモート IP]、[リモート仮想 IP]、[リモートコール ID]、および[アクション]です。必要に応じて、一覧の[切断]をクリックすると、対象の L2TP 接続を切断できます。

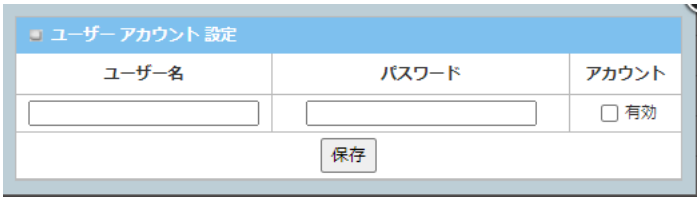


10.1.4.4. ユーザーアカウントの追加・編集

PPTP サーバーで認証するユーザーアカウントを最大10まで指定することができます。



◆ 追加または編集をクリックすると、[ユーザーアカウント設定]画面が表示されます。



項目	説明
ユーザー名	ユーザー名を指定します。文字数は1～32文字です。
パスワード	該当ユーザーのパスワードを指定します。文字数は1～32文字です。
アカウント	[有効]にチェックを入れると、本アカウントが有効になります。

◆ 保存をクリックして、設定を登録します。登録されると[ユーザーアカウントリスト]にアカウントが表示されます。

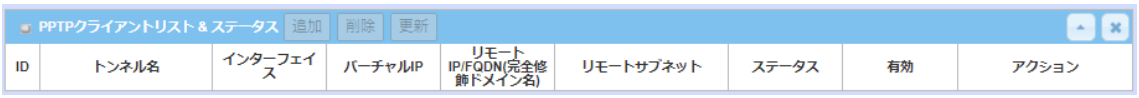
10.1.4.5. PPTP クライアントの設定



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

◆ 保存をクリックして、設定を登録します。

10.1.4.6. PPTP クライアントリストの追加/編集



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



項目	説明
トンネル名	識別のため32文字以下のトンネル名を指定します。
インターフェイス	PPTPトンネルを確立するインタフェースを[WAN]または[LAN]から選択します。[WAN-1]しか選択できない場合があります。
リモート IP/FQDN	PPTPサーバーのIPアドレスまたはFQDNを入力します。
MTU	PPTPトンネルを通過させるパケットのMTUを64～1500の間で指定します。VPNオーバーヘッドにより通信ができなくなる可能性があるため推奨値は1400です。
ユーザー名	PPTPサーバーに接続するためのユーザー名（32文字以下）を指定します。
パスワード	PPTPサーバーに接続するためのパスワードを指定します。
リモートサブネット	リモートサブネットをIPアドレス/ネットマスク（例：192.168.123.0/24）のフォーマットで指定します。0.0.0.0/0を指定するとPPTPトンネルがデフォルトゲートウェイとして扱われ、全てのパケットはPPTPトンネルを通過するようになります。

項目	説明
認証プロトコル	PPTP接続に使用する認証プロトコルを[PAP]、[CHAP]、[MS-CHAP]および[MS-CHAP v2]から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、PPTP接続用のMPPE（Microsoft Point-to-Point Encryption）セキュリティが有効になります。PPTPサーバーが対応しているときのみ有効にしてください。MPPE暗号化が有効の場合、認証プロトコルPAP/CHAPは使用できません。
NAT before Tunneling	[有効]にチェックをすると、PPTPトンネルを通過する前にNAT機能によるアドレス変換が有効になります。
LCP エコータイプ	PPTPトンネルのLCPエコータイプを以下から選択します。 ◆自動：自動的に間隔および最大故障回数を指定します ◆ユーザー定義：間隔（1～99,999秒）および最大故障回数（1～999回）の範囲で指定します。 ◆無効：LCPエコーは無効です。
トンネル	[有効]にチェックを入れると、本ルールが有効になります。

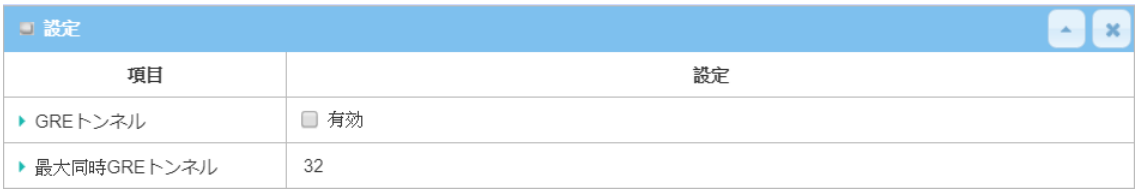
◆ 保存をクリックして、ルールを登録します。設定したルールが[PPTP クライアントリスト]に表示されます。

10.1.5. GRE

GRE は、シスコシステムズによって開発されたトンネリングプロトコルで、インターネットを介した仮想的なポイントツーポイントリンク内に、さまざまなネットワーク層プロトコルをカプセル化します。GRE 自体には、通信を暗号化する機能はありません。

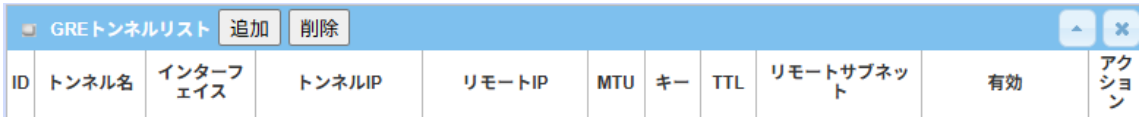
10.1.5.1. GRE の設定

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



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

10.1.5.2. GRE トンネルの追加/編集



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



項目	説明
トンネル名	識別のためのトンネル名(9文字以下)を指定します。

項目	説明
インターフェイス	GREトンネルを確立するインタフェースを[WAN]または[LAN]から選択します。[WAN-1]しか選択できない場合があります。
トンネル IP	GREトンネルの仮想インターフェースに割り当てるIPアドレスを入力し、対応するサブネットマスクを選択します。
リモート IP	リモートGREトンネルゲートウェイのIPアドレスを指定します。通常、リモートGREゲートウェイのグローバルIPアドレス（パブリックIPアドレス）と同一です。
MTU	GREトンネルを通過させるパケットのMTUを64～1500の間で指定します。
キー	GREの接続キーを0～999,999,999の範囲で指定します。 キーは空欄のままでも構いません。
TTL	GREトンネルのTTLホップカウント値を1～255の範囲で指定します。
リモートサブネット	GREトンネル先のリモートサブネットをIPアドレス／ネットマスク（例：192.168.123.100/24）のフォーマットで指定します。
トンネル	[有効]にチェックを入れると、本ルールが有効になります。

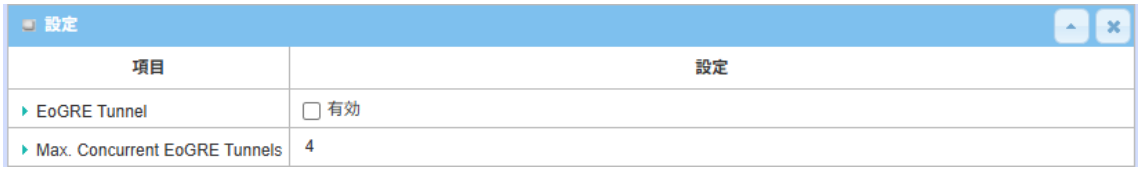
保存をクリックして、ルールを登録します。設定したルールが[GRE トンネルリスト]に表示されます。

10.1.6. EoGRE

前項の GRE トンネリングを使用し L2 情報を含むデータを伝送するプロトコルです。このプロトコルにより同一サブネットのネットワークをリモートにも拡張することができます。

EoGRE の場合 VPN オーバーヘッドの影響により、通信ができなかったり遅くなったりする症状が発生します。その場合は、通信する端末の送信パケット長を適宜短くするなど対策が必要になります。(推奨値:ポート MTU サイズ:1400)

10.1.6.1. EoGRE の設定



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

項目	説明
EoGRE Tunnel	[有効]にチェックを入れると、EoGRE トンネリングが有効になります。
Max Connection EoGRE Tunnel	本機の場合、4 です。

10.1.6.2. EoGRE トンネルの追加/編集



◆ 追加をクリックすると、[GRE ルール構成]画面が表示されます。

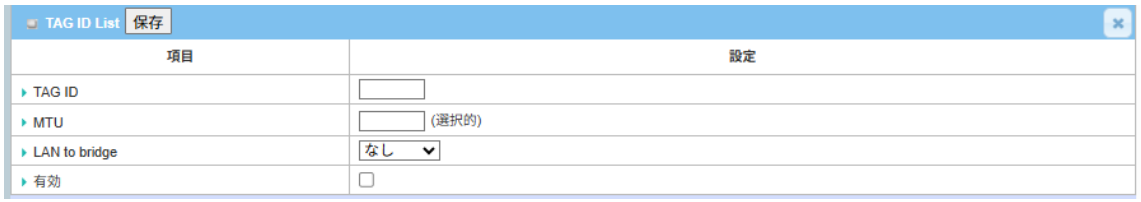


項目	説明
トンネル名	識別のためのトンネル名（9 文字以下）を指定します。
インターフェイス	EoGRE トンネルを確立するインタフェースを[WAN]または[LAN]から選択します。[WAN1]しか選択できない場合があります。
トンネル IP	GRE トンネルの仮想インターフェースに割り当てる IP アドレスを入力し、対応するサブネットマスクを選択します。
リモート IP	リモート EoGRE トンネルゲートウェイの IP アドレスを指定します。通常、リモート EoGRE ゲートウェイのグローバル IP アドレス（パブリック IP アドレス）と同一です。
MTU	EoGRE トンネルを通過させるパケットの最大サイズを 64～1500 の間で指定します。MTU は空欄のままでも構いません。
キー	EoGRE の接続キーを 0～999,999,999 の範囲で指定します。指定した場合は接続相手のキーと合わせる必要があります。 使用しない場合キーは空欄のままでも構いません。
TTL	GRE トンネルの TTL ホップカウント値を 1～255 の範囲で指定します。 TTL は空欄のままで構いません。
LAN to Bridge	EoGRE トンネルを接続するローカル側 LAN セグメントを指定する項目です。
トンネル	［有効］にチェックを入れると、本ルールが有効になります。

10.1.6.3. TAG ID List

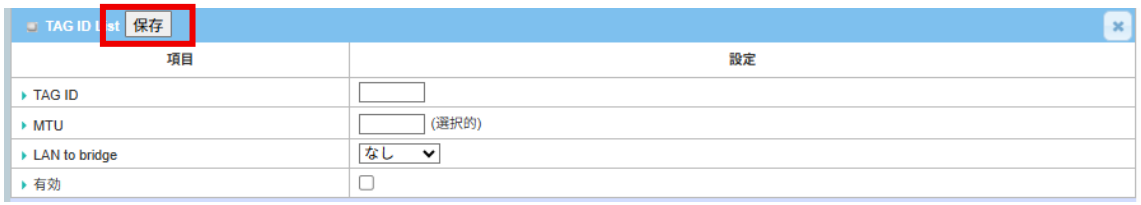


◆ 追加をクリックすると、[TAG ID List]画面が表示されます。



項目	説明
TAG ID	EoGRE で延長する VLAN ID を入力します。
MTU	EoGRE トンネルを通過させるパケットの最大サイズを 64～1500 の間で指定します。MTU は空欄のままでも構いません。
LAN to Bridge	延長する VLAN の DHCP 名を選択します。
有効	[有効]にチェックを入れると、本ルールが有効になります。

設定項目の上部にある保存をクリックしてルールを保存します。



WireGuard

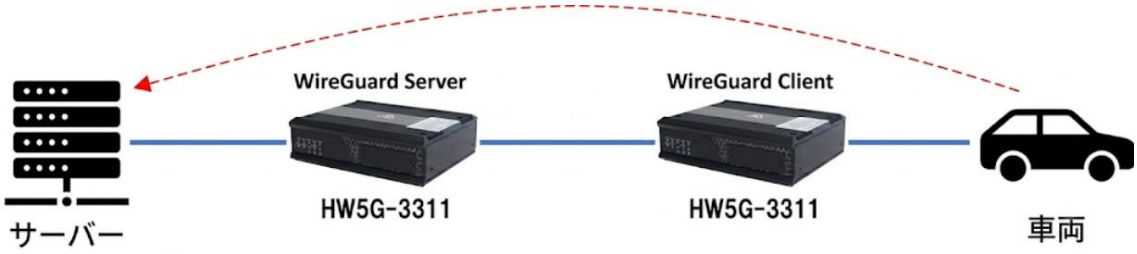
WireGuard は、高速かつセキュアな VPN プロトコルです。従来の VPN と比較して、複雑な証明書の管理などを必要とせず、シンプルな設定だけで容易に VPN 環境を構築できるのが特徴です。また、UDP ベースでステートレスな設計のため、回線断からの復旧が他 VPN よりも早いことが強みです。

活用ケース

・車載カメラの映像や位置情報データなどのリアルタイム転送

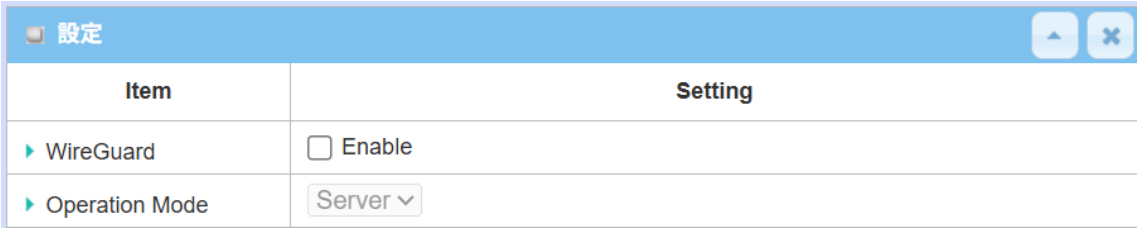
・車両搭載機器から本社ネットワークへのセキュアな通信アクセス

・通信環境が頻繁に変動する移動車両における、安定した拠点間接続の維持



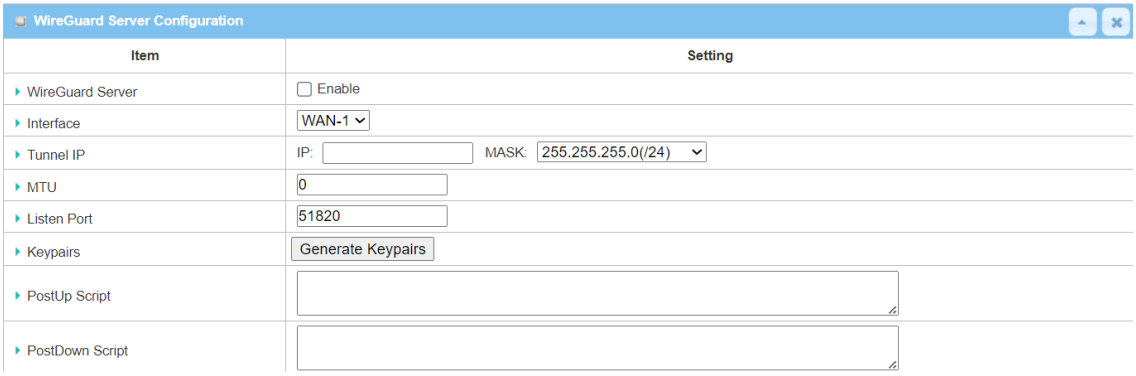
10.1.6.4. WireGuard の設定

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



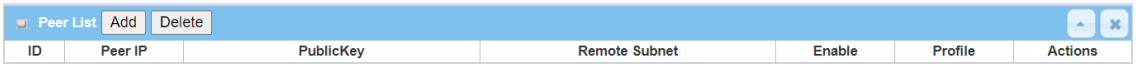
項目	説明
WireGuard	[Enable]にチェックを入れると、WireGuard 機能が有効になります。
Operation Mode	[Server]もしくは[Client]から選択します。

10.1.6.5. WireGuard サーバー構成

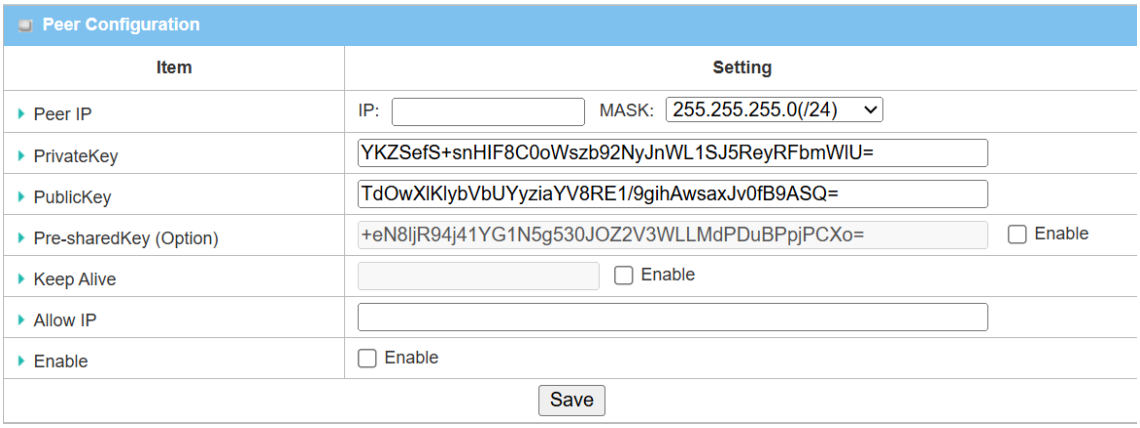


項目	説明
WireGuard Server	[Enable]にチェックを入れると WireGuard Server 機能を有効にします。
Interface	サーバーのトンネリングに使用する物理インタフェースを定義します。
Tunnel IP	仮想トンネル IP を指定します。
MTU	WireGuardトンネルを通過させるパケットの最大サイズを 500～1500 の間で指定します
Listen Port	待ち受けポートを指定します。
Keypairs	[Generate Keypairs]をクリックすると、 サーバーの秘密鍵と公開鍵が生成されます。
PostUP Script	本機ではサポートしておりません。
PostDown Script	本機ではサポートしておりません。

10.1.6.6. ピア構成の設定



◆ [Add]をクリックすると、[Peer Configuration]画面が表示されます。



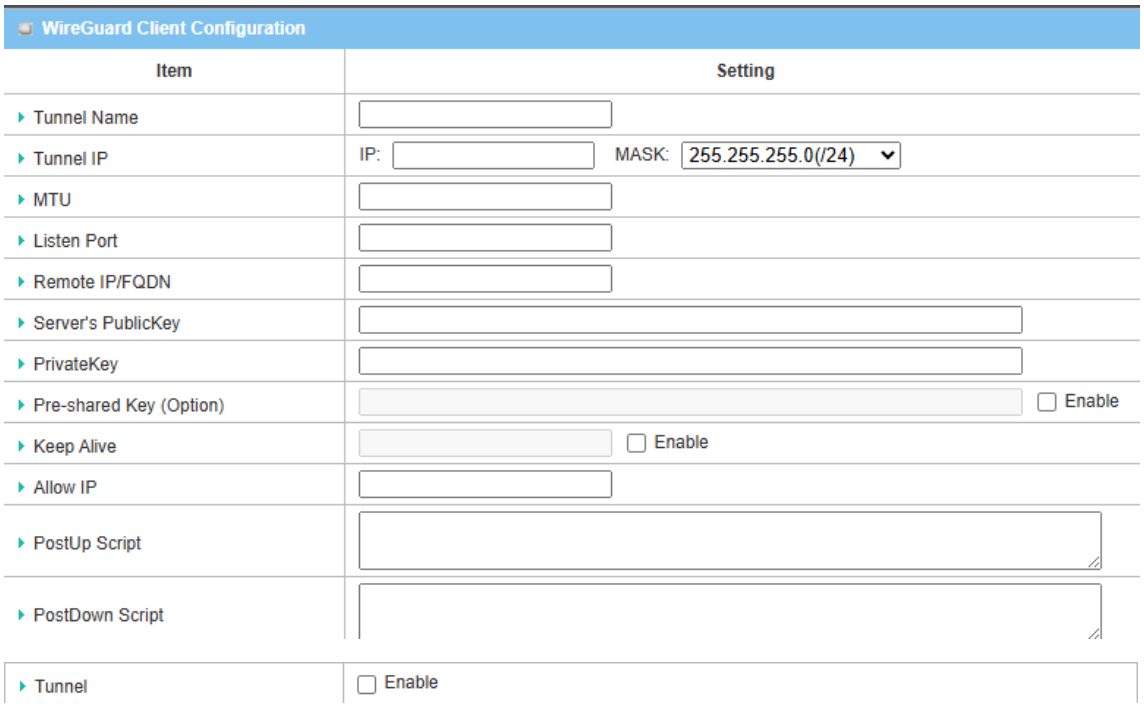
項目	説明
Peer IP	Peer IP を指定します。
PrivateKey(注 1)	クライアントの秘密鍵を自動で生成します。
PublicKey(注 1)	クライアントの公開鍵を自動で生成します。
Pre-sharedKey	[Enable]をクリックするとプリシェアドキー機能が有効になります。 任意のプリシェアドキーを指定します。
Keep Alive	[Enable]にチェックを入れると Keep Alive 機能が有効になります。接続維持のために指定した秒数ごとに対向機にパケットを送信します。5-60（s）の範囲で指定可能です。
Allow IP	このピアへ送信する宛先ネットワークと、このピアから受信を許可する送信元ネットワーク（入力例：192.168.123.0/24）を入力します。通常、リモートゲートウェイの LAN 側サブネットと同一です。
Enable	[Enable]にチェックを入れると、ピア設定が有効になります。

（注１） クライアント側で生成した公開鍵を登録する場合は、PrivateKey を空欄にし、PublicKey にクライアント側で生成された公開鍵を入力し保存してください。

10.1.6.7. WireGuard の Client 設定



項目	説明
WireGuard Client	[Enable]にチェックを入れると、WireGuard Client 機能が有効になります。



◆ [Add]をクリックすると、[WireGuard Client Configuration]画面が表示されます。

項目	説明
Tunnel Name	任意のトンネル名を入力します。
Tunnel IP	仮想トンネル IP を指定します。
MTU	WireGuardトンネルを通過させるパケットの最大サイズを 500～1500 の間で指定します。
Listen Port	待ち受けポートを指定します。
Remote IP/FQDN	リモートトンネルゲートウェイの IP アドレスを指定します。通常、リモートゲートウェイのグローバル IP アドレスと同一です。
Server's PublicKey	サーバー側で生成されたサーバーの公開鍵を入力します。
PrivateKey	サーバー側で生成されたクライアントの秘密鍵を入力します。
Pre-shared Key	[Enable]をクリックするとプリシェアドキー機能が有効になります。 任意のプリシェアドキーを指定します。
Keep Alive	[Enable]にチェックを入れると Keep Alive 機能が有効になります。接続維持のために秒数ごとに対向機に小さなパケットを送信します。5-60（s）の範囲で指定可能です。
Allow IP	このピアへ送信する宛先ネットワークと、このピアから受信を許可する送信元ネットワーク（入力例：192.168.123.0/24）を入力します。通常、リモートゲートウェイの LAN 側サブネットと同一です。
PostUP Script	本機ではサポートしておりません。
PostDown Script	本機ではサポートしておりません。
Tunnel	[Enable]にチェックを入れると、設定が有効になります。

10. 2. ファイヤーウォール

ファイヤーウォール機能には、パケットフィルタ、URL ブロッキング、MAC 制御、IPS、およびいくつかのファイヤーウォールオプションが含まれます。

10.2.1. パケットフィルター

入力インタフェース/出力インタフェース/送信元 IP/宛先 IP/送信元 MAC/プロトコル/送信元・宛先ポートに基づいたパケットのフィルタリングを設定できます。

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

10.2.1.1. パケットフィルタ設定



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

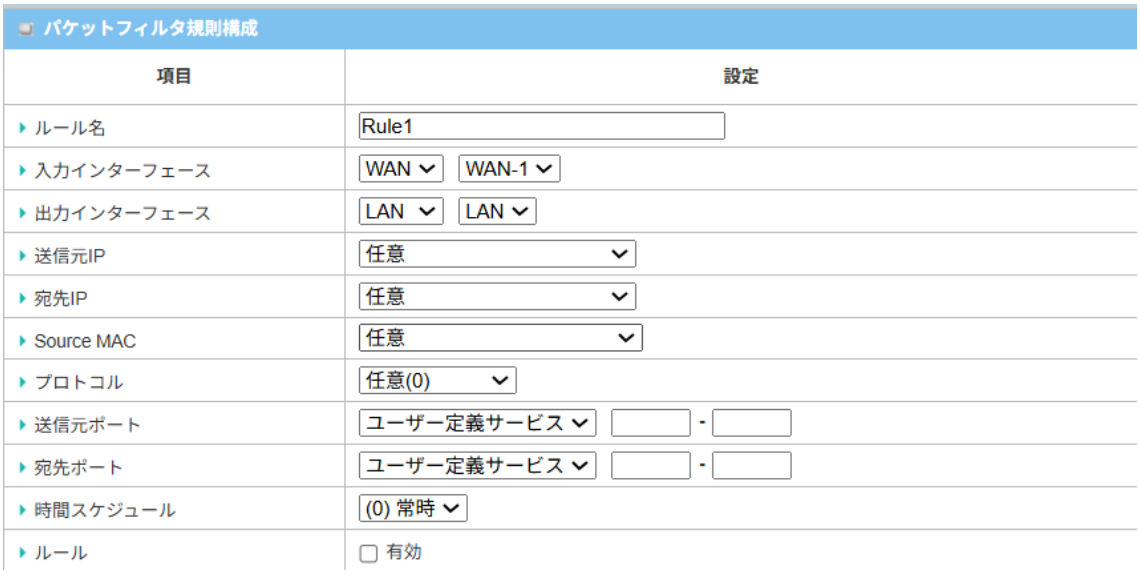
◆ 保存をクリックして設定を保存します。

10.2.1.2. パケットフィルタルールの追加/編集

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



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



項目	説明
ルール名	識別のためのパケットフィルタルール名（30 文字以内）を指定します。
入力インターフェース	パケットの入力インタフェースを[LAN]または[WAN]から選択します。
出力インターフェース	パケットの出力インタフェースを[LAN]または[WAN]から選択します。
送信元 IP アドレス	フィルタリングパケットを送信する IP アドレスを指定します。 ◆任意：全ての送信元 IP アドレスがフィルタされます。 ◆特定の IP アドレス：特定の IP アドレスからのパケットをフィルタします。 ◆IP 範囲：特定範囲の IP アドレスからのパケットをフィルタします。 ◆IP アドレスベースグループ:[グルーピング]で設定した IP アドレスベースグループからのパケットをフィルタします。
宛先 IP アドレス	フィルタリングパケットの宛先 IP アドレスを指定します。 ◆任意：全ての宛先 IP アドレスがフィルタされます。 ◆特定の IP アドレス：特定の宛先 IP アドレスへのパケットをフィルタします。 ◆IP 範囲：特定範囲の宛先 IP アドレスへのパケットをフィルタします。 ◆IP アドレスベースグループ:[グルーピング]で設定した IP アドレスベースグループからのパケットをフィルタします。
Source MAC	送信元の MAC アドレスを指定します。 ◆任意：全ての送信元 MAC アドレスがフィルタされます。 ◆Static MAC Address：特定の送信元MACアドレスのパケットをフィルタします。 ◆MAC Address-based Group：[グルーピング]で設定した MAC アドレスベースグループからのパケットをフィルタします。
プロトコル	フィルタリングを行うプロトコルを選択します。 ICMPv4、UDP、TCP、GRE、ESP、SCTP およびユーザー定義が選択できます。選択項目右の（）内の数字は IP プロトコル番号を表しています。ユーザー定義は任意の IP プロトコル番号を指定します。任意を選択すると全てのプロトコルでフィルタされます。

項目	説明
送信元ポート	プロトコルでTCP，UDP、任意を指定したときに送信元サービスポート番号を指定します。 ◆既知のサービス：よく使われるプロトコルから一つを選択します。 ◆ユーザー定義サービス：任意のポート番号を範囲で指定します。
宛先ポート	プロトコルでTCP，UDP、任意を指定したときに宛先サービスポート番号を指定します。 ◆既知のサービス：よく使われるプロトコルから一つを選択します。 ◆ユーザー定義サービス：任意のポート番号を範囲で指定します。
時間スケジュール	本フィルタリングルールが有効になる時間スケジュールを指定します。 常時(0)または[スケジュール設定]で定義されたスケジュールリストから選択できます。
ルール	[有効]にチェックを入れると、本ルールが有効になります。

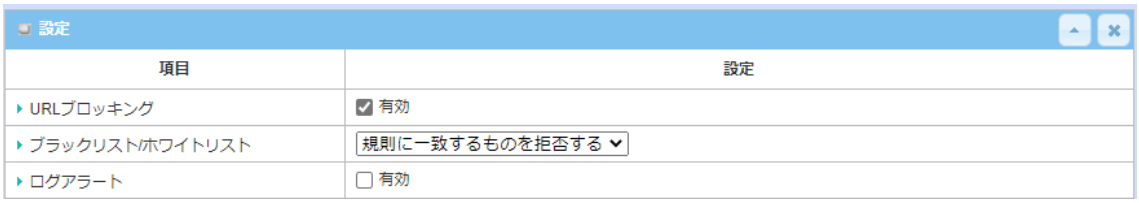
◆ 保存をクリックして、ルールを登録します。設定したルールが[パケットフィルタ]に表示されます。

10.2.2. URL ブロッキング

URL ブロッキング機能では、受信および送信される Web リクエストを許可または遮断することで、通信をフィルタリングできます。完全な URL だけでなく、ドメイン名の一部やキーワードを指定したフィルタリングも可能です。

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

10.2.2.1. URL ブロッキング設定



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

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

10.2.2.2. URL ブロッキングルールの追加/編集

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



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



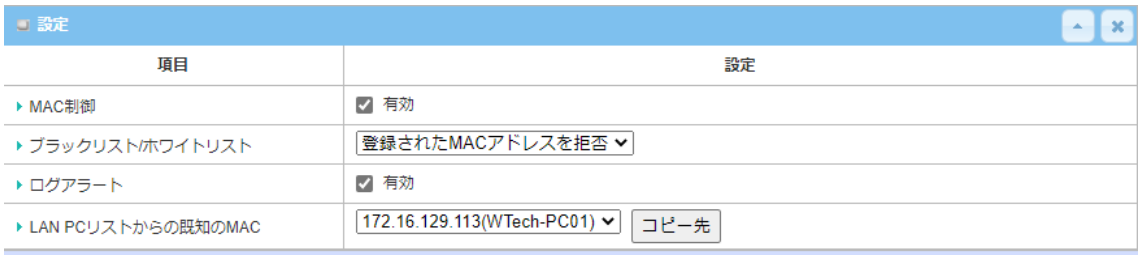
項目	説明
ルール名	URL ブロッキングルール名を設定します。
送信元 IP アドレス	Web 要求を送信する IP アドレスを指定します。 ◆任意：全ての送信元 IP アドレスがフィルタされます。 ◆特定の IP アドレス：特定の IP アドレスからのパケットをフィルタします。 ◆IP 範囲：特定範囲の IP アドレスからのパケットをフィルタします。 ◆IP アドレスベースグループ:[グルーピング]で設定した IP アドレスベースグループからのパケットをフィルタします。
Source MAC	送信元の MAC アドレスを指定します。 ◆任意：全ての送信元 MAC アドレスがフィルタされます。 ◆Static MAC Address：特定の送信元MACアドレスのパケットをフィルタします。 ◆MAC Address-based Group：[グルーピング]で設定した MAC アドレスベースグループからのパケットをフィルタします。
URL/ドメイン名/ キーワード	検査する[完全な URL]、[一部のドメイン名]または[一部のキーワード]を指定します。 条件一致した場合の通過許可かブロックかは、ブラックリスト/ホワイトリストの設定に依存します。
宛先ポート	宛先サービスポート番号を指定します。 ◆任意：全てのポート番号がブロッキングの対象になります。 ◆特定のサービスポート：ブロッキング対象の特定のサービスポート番号を指定します。 ◆ポート範囲：ブロッキング対象の特定のサービスポート番号を範囲で指定します。
時間スケジュール	本フィルタリングルールが有効になる時間スケジュールを指定します。 常時(0)または[スケジュール設定]で定義されたスケジュールリストから選択できます。
ルール	[有効]にチェックを入れると、本ルールが有効になります。

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

10.2.3. MAC 制御

ネットワークに接続する機器の MAC アドレスに基づいて、パケットの通過を許可または遮断できます。特定の MAC アドレスを持つクライアントからの通信を拒否する場合は、[MAC 制御]でブラックリストを設定します。

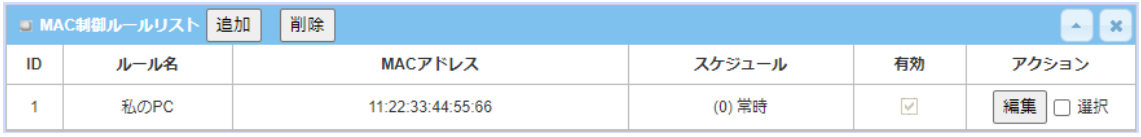
◆ 画面左側のメニューから、セキュリティ⇒ファイヤーウォール⇒MAC 制御の順にクリックします。



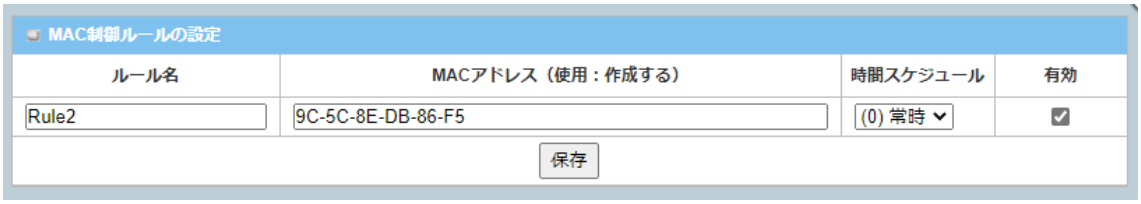
項目	説明
MAC 制御	[有効]にチェックを入れると、MAC制御機能が有効になります。
ブラックリスト/ ホワイトリスト	MAC制御のモードを以下から選択します。 ◆登録されたMACアドレスを拒否する(ブラックリスト):MAC制御ルールと一致するものをブロックします。 ◆登録されたMACアドレスを許可する(ホワイトリスト):MAC制御ルールと一致するもののみ許可します。
ログアラート	[有効]にチェックを入れると、イベントログが有効になります。
LAN PC リストからの既知の MAC	LAN クライアントリストから MAC アドレスを選択します。コピー先をクリックして、選択した MAC ア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

10.2.3.1. MAC 制御ルールリストの追加/編集

MAC 制御ルールを登録します。ルールは 20 ルールまで登録できます。



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



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

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

10.2.4. IPS

IPS は、ネットワークやシステムを監視し、不正または悪意のあるアクセスを検出・防止するセキュリティ機能です。不正アクセスを検出して関連情報を記録するとともに、該当する通信を遮断し、その結果を通知します。必要に応じて IPS 機能を有効にし、一覧に示された不正アクセスを監視できます。また、[ログ警告]を有効にすると、該当する不正アクセスが検出された際に、侵入イベントがログに記録されます。

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

10.2.4.1. IPS 設定



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

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

10.2.4.2. 侵入防止機能設定

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



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

◆ 保存をクリックして設定を保存します。

10.2.5. オプション

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

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

10.2.5.1. ファイヤーウォールオプション設定



項目	説明
ステルスモード	[有効]にチェックを入れると、ステルスモード機能が有効になります。 有効にすると、WANからのポートスキャンに本機が応答しなくなります。
SPI	[有効]にチェックを入れると、SPI機能が有効になります。
WAN からの Ping パケットを破棄する	[有効]にチェックを入れると、WAN からの PING に応答しなくなります。

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

10.2.5.2. IPv6 Firewall Options

本機能はサポートしておりません。

10.2.5.3. リモート管理者ホスト定義の編集

WAN から本機にアクセスできる管理者ホストを 5 つ設定できます。

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



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

◆ 保存をクリックして設定を保存します。

（注１） WAN 側からリモート管理を行う場合は、HTTPS を使用してください。HTTP では認証情報が暗号化されないため、安全でないネットワークでは使用しないでください。

10. 3. 認証

一部の環境では、インターネット通信の許可に RADIUS サーバーを使用します。許可された端末のみインターネット接続ができ、許可されていない端末の通信は遮断されます。

10.3.1. MAC 認証

MAC 認証機能を有効にすると、指定したインタフェースからの通信は自動的に MAC 認証処理の対象となります。

本機は RADIUS サーバーと連携し、認証処理に必要なユーザー情報を送信します。

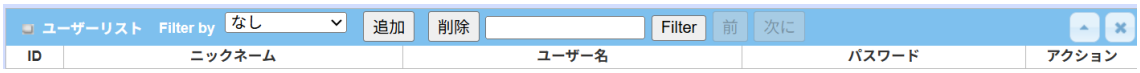
◆ 画面左側のメニューから、セキュリティ⇒認証⇒MAC 認証の順にクリックします。

10.3.1.1. MAC 認証の設定

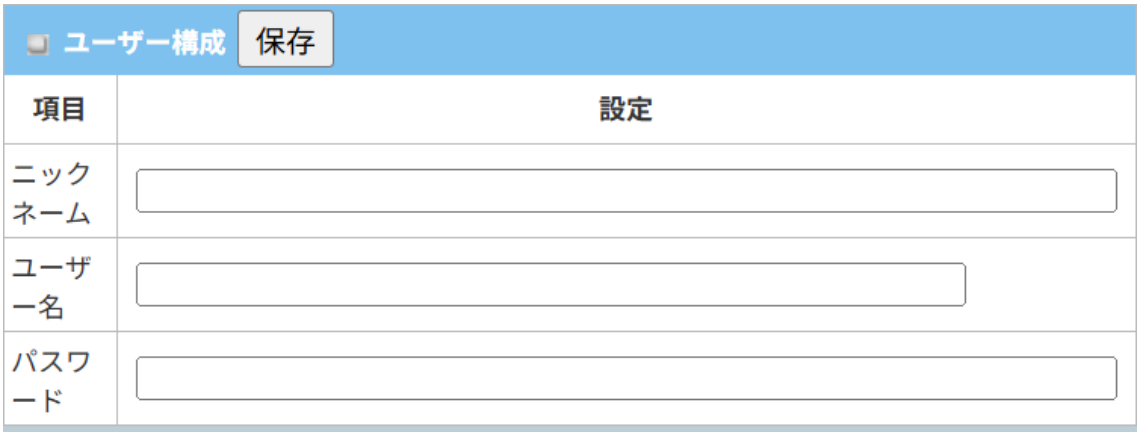


項目	説明
MAC 認証	[有効]にチェックを入れると、MAC認証が有効になります。
Radius サーバー	認証に使用する外部 RADIUS サーバーを指定します。MAC 認証を有効にすると、本機は接続したクライアントの情報を RADIUS サーバーへ送信して認証を行います。 注意：RADIUS サーバーが接続されているインタフェースは選択しないでください。
LAN インタフェース	MAC 認証を適用するネットワークインタフェースを選択します。LAN またはポートベースの VLAN のインタフェースを少なくとも 1 つ選択してください。
クライアント接続アイドル時間	クライアント接続が切れるまでの時間を秒単位で指定します。 クライアントが指定した時間内にネットワークへアクセスしなかった場合、その認証は無効になります。

10.3.1.2. ユーザーリストの作成



◆ 追加または編集をクリックすると、[ユーザー構成]画面が表示されます。



項目	説明
ニックネーム	ユーザーの任意のニックネームを入力します。
ユーザー名	ユーザーの MAC アドレスを入力します。
パスワード	パスワードを設定します。

◆ 保存をクリックしてユーザー構成を保存します。

11. 管理(Administration)

11. 1. 設定と管理 （本機ではサポートしておりません）

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

11.1.1. コマンドスクリプト

この機能はサポートしておりません。

11.1.2. Device Management

この機能はサポートしておりません。

11.1.3. RESTful

この機能はサポートしておりません。

11.1.4. SNMP

この機能はサポートしておりません。

11.1.5. Telnet & SSH

この機能はサポートしておりません。

11.2. システム管理

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

11.2.1. パスワード及び MMI

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

11.2.1.1. ホスト名の設定



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

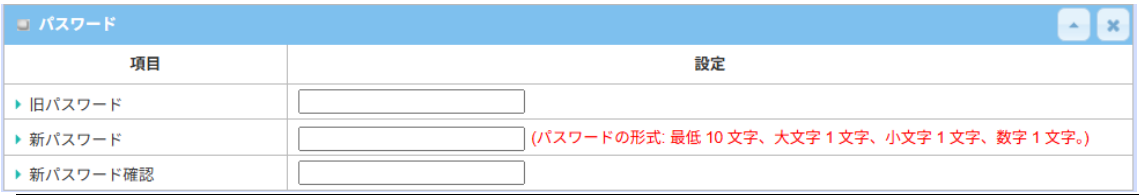
11.2.1.2. ユーザー名の変更



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

(注 1) ユーザー名の変更を実施すると新ユーザー名による Web GUI のログインが必要になります。

11.2.1.3. パスワードの変更



項目	説明
旧パスワード	現在のパスワードを入力します。
新パスワード	パスワードは 10～32 文字で入力し、大文字、小文字、数字および使用可能な記号を組み合わせてください。AbC,123 などもパスワードに含めることはできません。
新パスワード確認	確認のためもう一度新しいパスワードを入力してください。

◆ 保存をクリックして新パスワードを登録します。

11.2.1.4. MMI（マネージメントインタフェース）の設定

本設定は管理者が本機へ WebUI でアクセスするための管理情報を制御します。



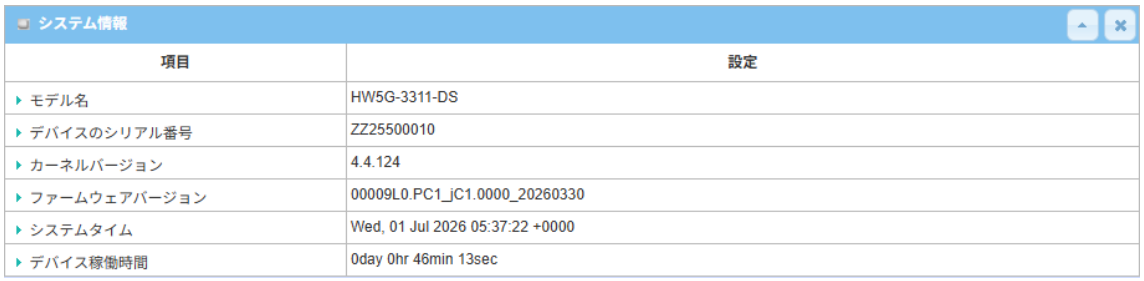
項目	説明
ログイン	ログイン試行回数の上限を設定します。設定範囲は 3~10 回です。パスワードを間違えて、このカウントを超えたログイン試行を行った場合は、30 秒間はログイン試行がロックされます。
ログインタイムアウト	自動ログアウト機能の有効/無効と、自動ログアウトするまでの無操作監視秒数を設定します。設定範囲は 60~3600 秒です。
GUI アクセスプロトコル	GUI アクセスに使用するプロトコルを選択します。[http/https]、[http のみ]、[https のみ]の選択が可能です。
HTTPS 証明書のセットアップ	本機の WebUI 用証明書の詳細設定を行います。本設定は証明書リストを作成する必要があります。
HTTP 圧縮	http を圧縮したい場合に br, gzip およびデフレートにチェックをします。
HTTP バインディング	WebUI をバインドする DHCP サーバーを選択します。

◆ 保存をクリックして MMI 設定を登録します。

11.2.2. システム情報

本機のデバイス情報を確認できます。

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



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

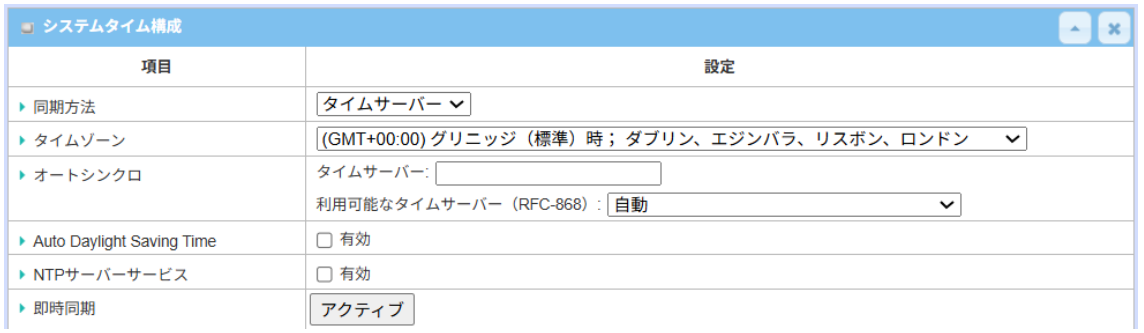
◆ 更新のクリックで情報が更新されます。

11.2.3. システムタイム

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

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

11.2.3.1. タイムサーバーと同期する

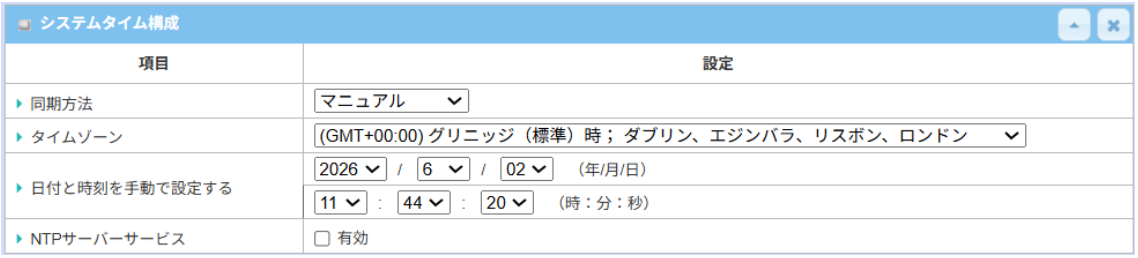


項目	説明

同期方法	[タイムサーバー]を選択します。
タイムゾーン	本機設置所在地のタイムゾーンを選択します。。
オートシンクロ	利用可能な公開タイムサーバーをリストから選択します。独自タイムサーバーを利用する場合は、そのタイムサーバーの IP アドレスを指定します。
NTP サーバサービス	[有効] にチェックを入れると、本機に LAN での NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
即時同期	アクティブをクリックするとすぐに時刻同期を行います。

◆ 保存をクリックして同期方式などの設定を保存します。

11.2.3.2. 手動でシステム時間を設定する

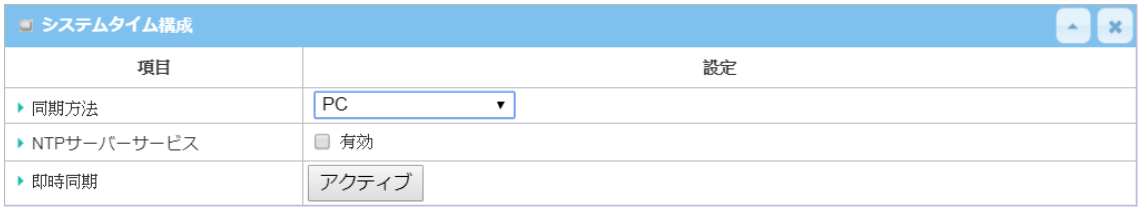


項目	説明
同期方法	[マニュアル]を選択します。
タイムゾーン	本機設置所在地のタイムゾーンを選択します。
日付と時刻を手動で設定する	現在の日付（年/月/日）と時刻を（時:分:秒）を入力します。
NTP サーバサービス	[有効]にチェックを入れると、本機に LAN の NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。

◆ 保存をクリックして同期方式などの設定を保存します。

11.2.3.3. PC と手動で同期をとる

WebUI で本機にアクセス中の PC と同期をとります。



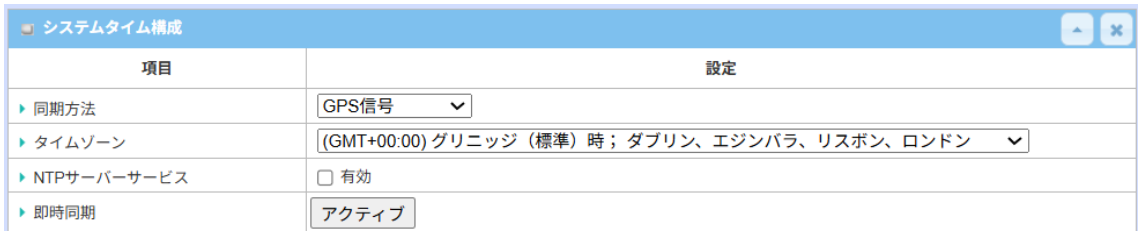
項目	説明
同期方法	[PC]を選択します。
NTP サーバサービス	[有効]にチェックを入れると、本機に LAN での NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
即時同期	アクティブをクリックすると、PC の時刻と即時に同期をとります。

◆ 保存をクリックして同期方式などの設定を保存します。

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

11.2.3.4. GPS を利用して同期をとる

GPS から時刻データを取得し同期します。



項目	説明
同期方法	[GPS]を選択します。
タイムゾーン	本機設置所在地のタイムゾーンを選択します。
NTP サーバサービス	[有効]にチェックを入れると、本機に LAN での NTP サーバーが有効になり、接続 IP 機器との時刻同期を行うことができます。
即時同期	アクティブをクリックすると、即時に GPS から取得した時刻に同期します。

◆ 保存をクリックして同期方式などの設定を保存します。

11.2.4. システムログ

システムログ画面では、本機の動作ログを表示、検索および保存できます。
（注１） 本機能はハイテクインター株式会社によるサポート時のみに使用します。ログ内容などの詳細資料の提供は致しておりません。

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

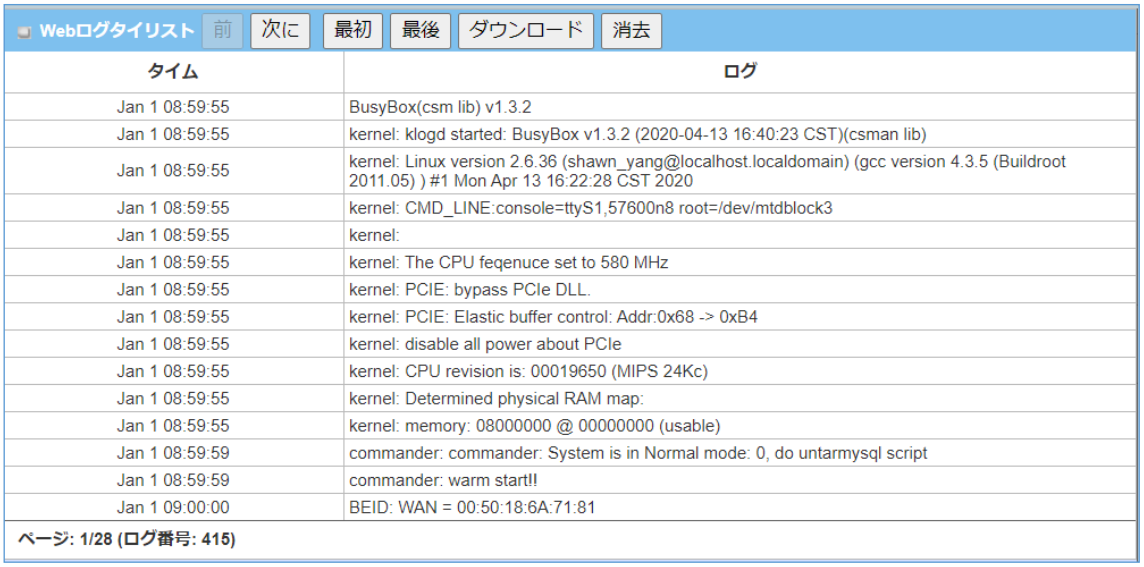


11.2.4.1. 表示および E メールログ履歴

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

項目	説明
ビュー	ビューをクリックすると、ログ履歴を表示します。
Email Now	本機ではサポートしておりません。

Web ログリスト例



Webログタイリスト 前 次に 最初 最後 ダウンロード 消去

タイム	ログ
Jan 1 08:59:55	BusyBox(csm lib) v1.3.2
Jan 1 08:59:55	kernel: klogd started: BusyBox v1.3.2 (2020-04-13 16:40:23 CST)(csman lib)
Jan 1 08:59:55	kernel: Linux version 2.6.36 (shawn_yang@localhost.localdomain) (gcc version 4.3.5 (Buildroot 2011.05)) #1 Mon Apr 13 16:22:28 CST 2020
Jan 1 08:59:55	kernel: CMD_LINE:console=ttyS1,57600n8 root=/dev/mtdblock3
Jan 1 08:59:55	kernel:
Jan 1 08:59:55	kernel: The CPU feqenuce set to 580 MHz
Jan 1 08:59:55	kernel: PCIE: bypass PCIe DLL.
Jan 1 08:59:55	kernel: PCIE: Elastic buffer control: Addr:0x68 -> 0xB4
Jan 1 08:59:55	kernel: disable all power about PCIe
Jan 1 08:59:55	kernel: CPU revision is: 00019650 (MIPS 24Kc)
Jan 1 08:59:55	kernel: Determined physical RAM map:
Jan 1 08:59:55	kernel: memory: 08000000 @ 00000000 (usable)
Jan 1 08:59:59	commander: commander: System is in Normal mode: 0, do untarmysql script
Jan 1 08:59:59	commander: warm start!!
Jan 1 09:00:00	BEID: WAN = 00:50:18:6A:71:81

ページ: 1/28 (ログ番号: 415)

11.2.4.2. ログタイプカテゴリ

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



Webログタイプカテゴリ システム 攻撃 ドロップ ログインメッセージ デバッグ

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

11.2.4.3. E メールアラート

本機能はサポートしていません。

11.2.5. バックアップ及び復元

デバイスのファームウェアのアップグレードやデバイス設定のバックアップ/復元を行うことができます。

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



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

◆ 保存をクリックして設定を登録します。

11.2.6. 再起動およびリセット

本機の再起動、および工場出荷設定へのリセットを行います。

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



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

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

11.3. FTP

FTP（File Transfer Protocol）は、ネットワーク上のクライアントとサーバー間でファイルを転送するための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/サーバーのパッシブ方式で動作します。

11.3.1. サーバー構成

本機のログファイルを取得するための FTP/FTPS,SFTP のサーバーの設定を行います。

◆ 画面左側のメニューから、管理（Administration）⇒FTP⇒サーバー構成の順にクリックします。

11.3.1.1. FTP サーバー設定



項目	説明
FTP	[有効]にチェックを入れると、FTP サーバー機能が有効になります。
FTP ポート	FTP 接続のポート番号を指定します。
タイムアウト	FTP 接続のタイムアウト時間を指定します。
最大接続 IP アドレスごと	同じ IP アドレスに登録できるクライアント数を指定します。
最大 FTP クライアント	FTP 接続の最大クライアント数を指定します。
PASV モード	[有効]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 モードが有効になります
PASV のポート範囲	PASV 形式に割り当てるポートを 1024-65535 の範囲で指定します。
PASV モードで自動に外部 IP をレポートする	[有効]にチェックを入れると、PASV コマンドへの応答時に IP アドレスを通知する機能が有効になります。
ASCII 転送モード	[有効]にチェックを入れると ASCII モードでのデータ転送が有効になります。初期設定ではバイナリモードでのデータ転送をサポートしてます。
FTPS（FTP over SSL/TLS）	[有効]にチェックを入れると、FTPS を用いた通信が有効になります。

◆ 保存をクリックして設定を登録します。

11.3.1.2. SFTP サーバ設定



項目	説明
SFTP	[有効]にチェックを入れると、SFTP サーバー機能が有効になります。
SFTP ポート	SFTP 接続のポート番号を指定します。

11.3.2. ユーザーアカウント

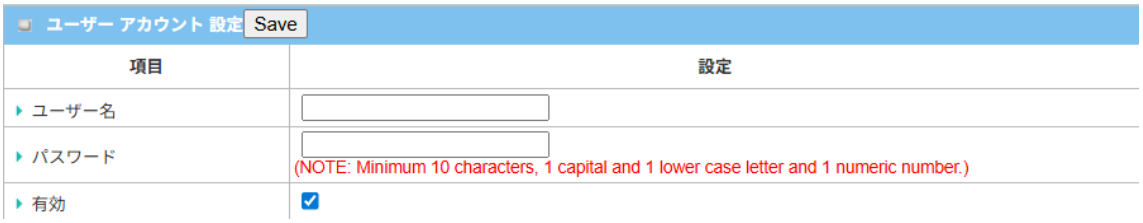
ログファイルが取得可能なクライアントのユーザーアカウントの設定を行います。

◆ 画面左側のメニューから、管理(Administration)⇒FTP⇒ユーザーアカウントの順にクリックします。

11.3.2.1. ユーザーアカウントリスト



[追加]をクリックすると、[ユーザーアカウント設定]画面が表示されます。



項目	説明
ユーザー名	FTP サーバーへのログイン用のユーザー名を設定します。
パスワード	FTP サーバーへのログイン用のパスワードを設定します。
有効	チェックを入れると設定が有効になります。

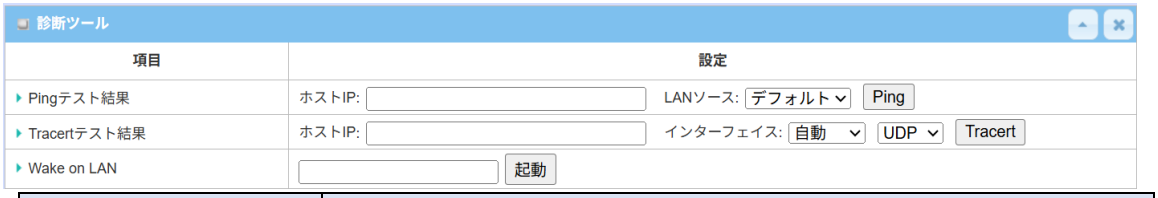
11.4. 診断

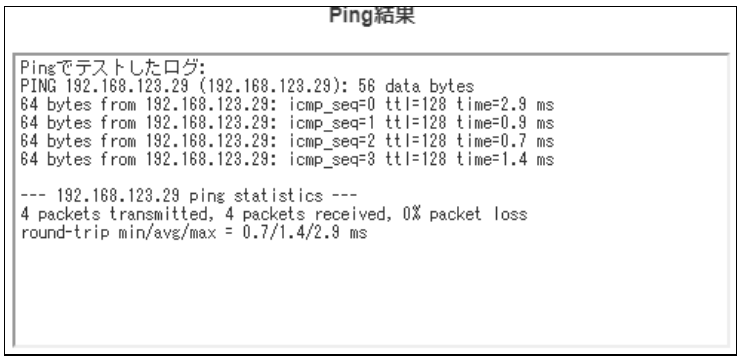
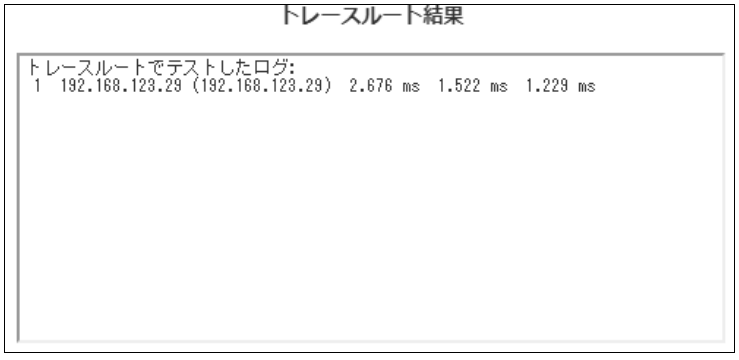
本機およびネットワークで発生した異常の原因調査に使用できる、簡易ネットワーク診断ツールが搭載されています。

11.4.1. 診断ツール

Ping および Tracert による疎通確認を行えます。

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



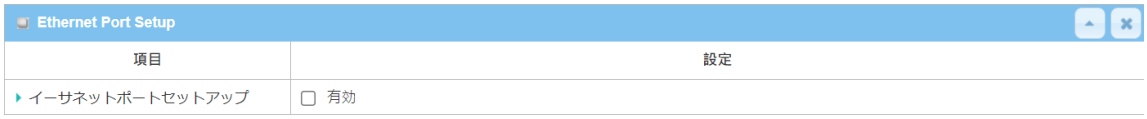
項目	説明
Ping テスト結果	ホスト IP に宛先を入力し、Ping をクリックすることで、Ping テストを行うことが出来ます。 テスト結果は画面下部に下図のように表示されます。 
Tracert テスト結果	ホスト IP に宛先を入力し、Tracert をクリックすることで、トレースルートテストを行うことが出来ます。 テスト結果は画面下部に下図のように表示されます。 
Wake on LAN	この機能はサポートしておりません。

11.4.2. イーサネットポートセットアップ

イーサネットポートの設定を行います。

◆ 画面左側のメニューから、管理（Administration）⇒診断⇒イーサネットポートセットアップの順にクリックします。

11.4.2.1. Ethernet Port Setup



項目	説明
イーサネットポートセットアップ	[有効]にチェックを入れると、イーサネットポートセットアップ機能が有効になります。

11.4.2.2. Ethernet Port Setup List



項目	説明
リンク	リンクダウンまたはリンクアップを選択し、イーサネットインタフェースの状態を切り替えます。※Down を選択し、有効にすると選択したポートで通信できなくなります。
有効	チェックを入れると、設定が有効になります。
アクション	[編集]をクリックすると、設定ができるようになります。

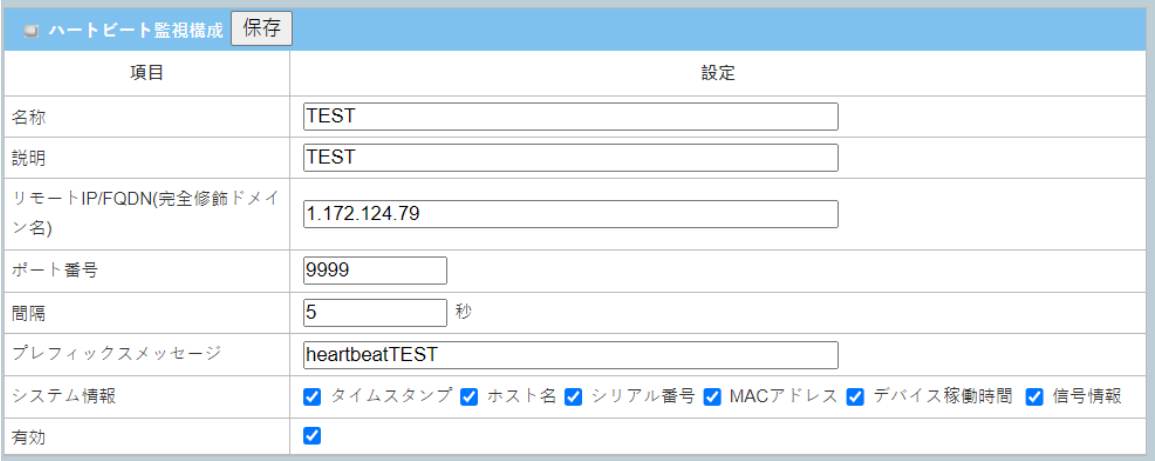
11.4.3. ハートビート監視

ハートビート監視は、指定したホストへ一定間隔で UDP パケットを送信し、本機が正常に動作していることを通知する機能です。本機が正常に通信を維持できているかを確認するために使用します

11.4.3.1. ハートビート監視構成

◆ 画面左側のメニューから、管理(Administration)⇒診断⇒ハートビート監視の順にクリックします。

◆ 追加または編集をクリックすることで[ハートビート監視構成]画面が表示されます。



項目	説明
名称	任意の名称を入力します
説明	構成の説明を入力します。
リモート IP/FQDN (完全修飾ドメイン名)	リモートアドレス(IPv4 または、FQDN)を指定します。
ポート番号	送信するポート番号を設定します。
間隔	送信間隔を設定します。
プレフィックスメッセージ	リモート IP にアクセスする際の識別子として、プレフィックスメッセージの文字列を指定できます。
システム情報	送信するデバイス情報を指定します。
有効	チェックを入れると設定が有効になります。

◆ [保存]をクリックして、設定を保存します。

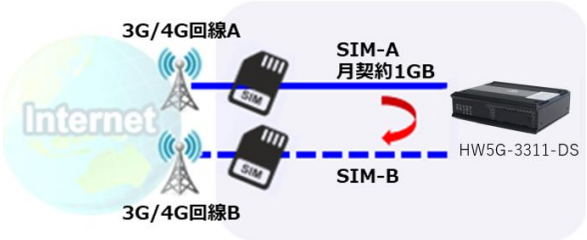
12. サービス

12. 1. セルラーツールキット

セルラーツールキットでは、[データ使用量の監視]、[SMS]、および[SIM PIN コード変更]など、モバイルネットワークに関する設定を行えます。セルラーツールキットを使用する前に、有効な SIM カードを挿入してください。



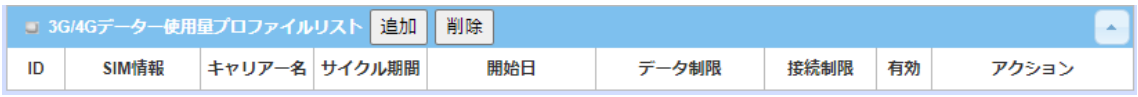
12.1.1. データ使用量（データ使用量の制限）



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

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

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

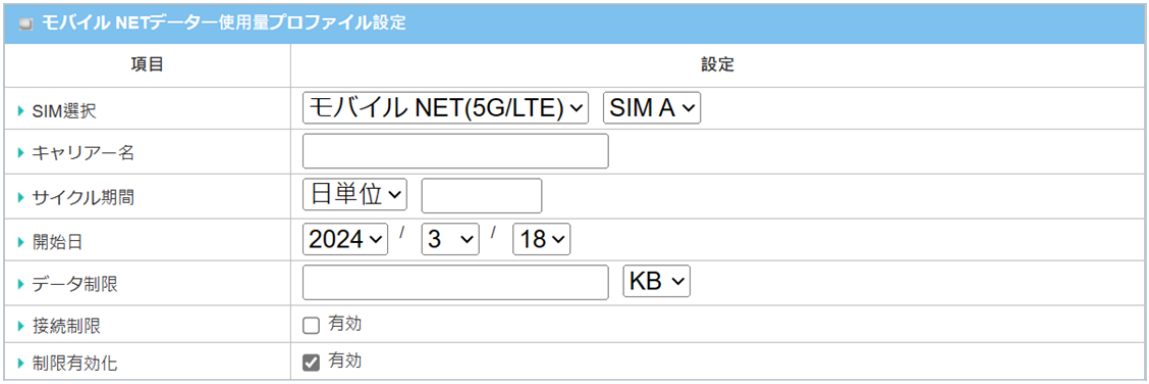


（注１） 本機の監視するデータ使用量は通信業者と異なる場合があります。制限の容量を契約より小さく設定することを推奨します。本機能の不動作による追加通信量などに関して一切責任を負いかねます。

12.1.1.1. モバイル NET データ使用量プロファイルリストの追加/編集

モバイル NET データ使用量プロファイルは最大 4 ルールまで登録できます。

◆ 追加または編集をクリックすると、モバイル NET データー使用量プロファイル設定画面が表示されます。



項目	説明
SIM 選択	SIM カードを[SIM-A]または[SIM-B]から選択します。通常は優先選択された SIM カードを選択します。 本機のインタフェースはモバイル NET(5G/LTE)固定です。
キャリア名	プロファイルの識別のために使用されるキャリア名を指定します。
サイクル期間	データ使用量をリセットする期間を[日単位]、[週単位]または[月単位]から選択します。日単位を選択した場合は、日数を 1～90 日までの範囲で指定します。
開始日	データ使用量監視を開始する日付を指定します。過去の日付の場合は、統計情報が正しく表示されない場合があります。
データ制限	選択したサイクル期間での制限容量を指定します。範囲は 1～999 で、[KB]、[MB]または[GB]の単位を選択できます。
接続制限	[有効]にチェックを入れると、データ使用量が容量制限を超えた場合に、強制的にモバイル NET 接続が切断されます。
制限有効化	[有効]にチェックを入れると、プロファイルが有効になります。

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

12.1.2. SMS

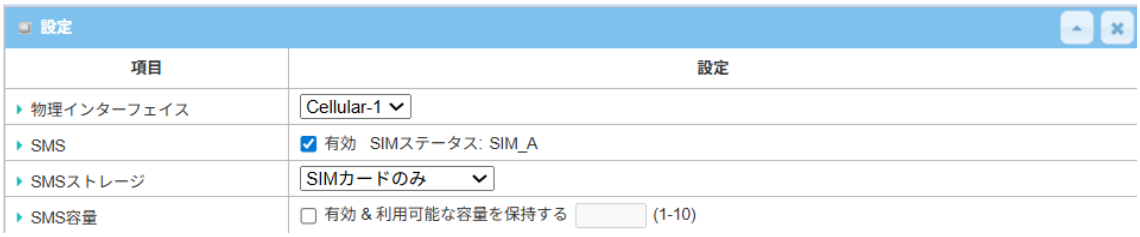
本機では、Web GUI からモバイル NET の SMS 機能が使用できます。この機能で、携帯電話やスマートフォンに短いメッセージを送信/受信することができます。

（注 1） 本機能を使用するためには SMS が使用できる回線契約が必要です。

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

12.1.2.1. SMS の設定

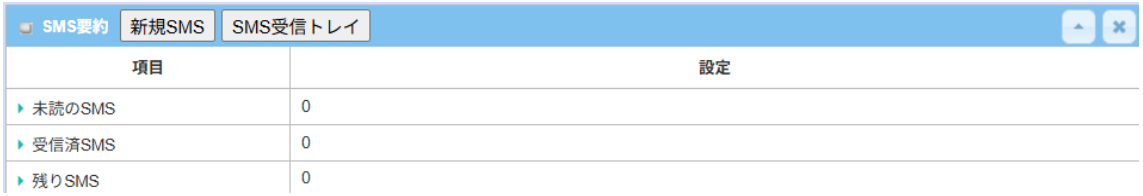
SMS を送受信するための条件を設定します。



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

12.1.2.2. SMS 要約

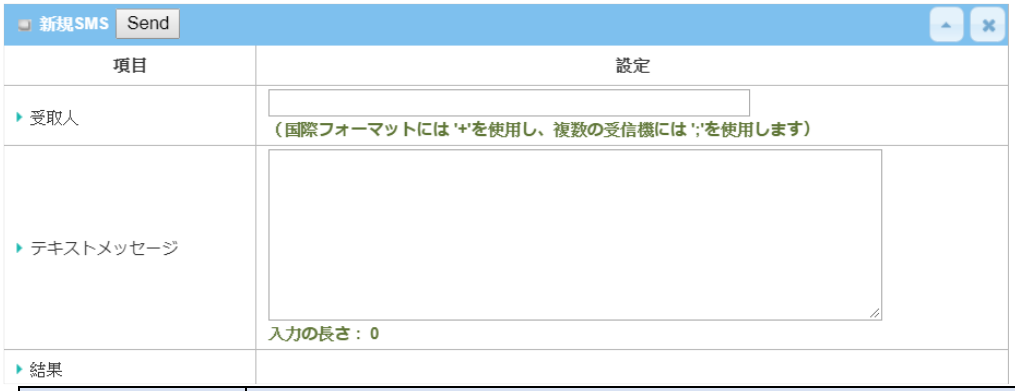
SMS の受信および送信の状況を表示します。



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

12.1.2.3. 新規 SMS

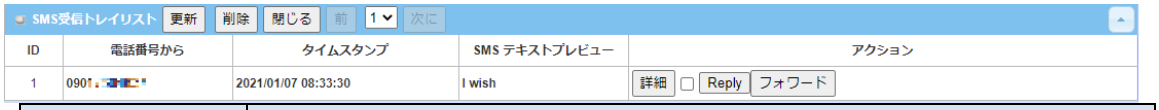
◆ SMS 要約にある、新規 SMS をクリックすると、[新規 SMS]画面が表示されます。この画面から、SMS メッセージの作成・送信を行うことができます。



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

12.1.2.4. SMS 受信トレイ

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



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

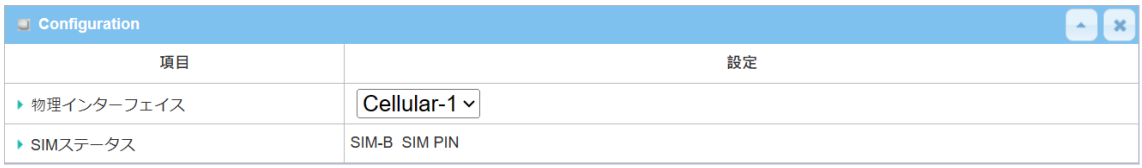
12.1.3. SIM PIN

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

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

12.1.3.1. SIM カードの選択（Configuration）

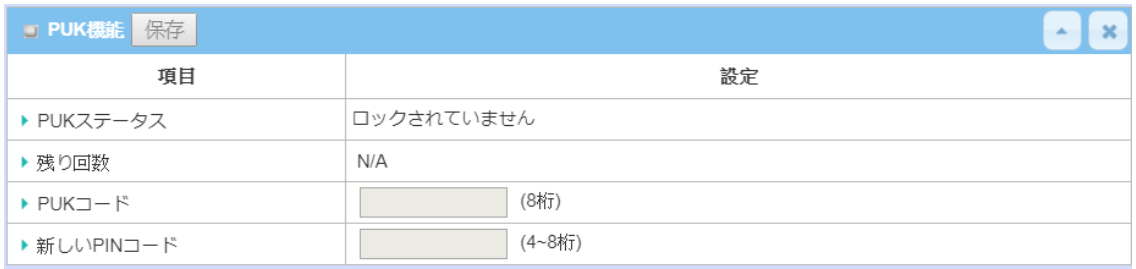
PIN コードを書き換える SIM カードを選択します。



項目	説明
物理インターフェイス	SIM PIN を変更するセルラーインタフェースを選択します。
SIM ステータス	選択した SIM カードと SIM カードのステータスを示します。 ステータスは、Ready, Not Insert, or SIM PIN と表示されます。 ◆Ready: SIM カードが挿入され、使用できる状態です。 PIN 保護のない SIM カードであるか、正しい PIN コードで SIM カードのロックが解除されています。 ◆Not Insert: その SIM スロットに SIM カードが挿入されていません。 ◆SIM PIN: SIM カードは PIN コードで保護されており、正しい PIN コードでロック解除されていません。 その SIM カードはまだロックされた状態です。

12.1.3.2. PUK 機能

PIN の誤入力回数が上限に達した場合は、通信事業者から PUK を取得し、SIM のブロックを解除してください。PUK コードで SIM カードのロックを解除すると、SIM ロック機能が自動的に有効になります。



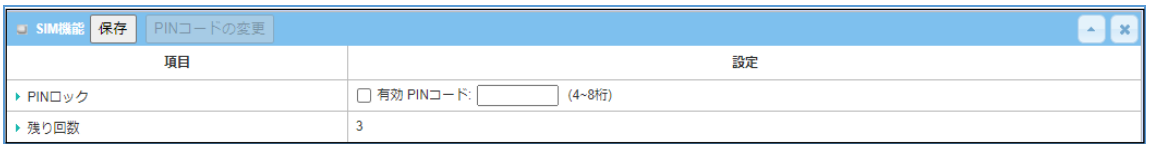
項目	説明
PUK ステータス	PUK の状態を表示します。 ◆ロックされていません：PIN コードエラー限界以内で PUK でロックされていません。 ◆ロックされています：PIN コードエラー限界に達し PUK でロックされています。
残り回数	PUK ロック解除の残りの試行回数を表します。
PUK コード	PUK ロック解除ステータスで SIM カードのロックを解除できる PUK コード（8 桁）を指定します。
新しい PIN コード	SIM カードの新しい PIN コード（4～8 桁）を入力します。

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

（注１） 誤った PUK を繰り返し入力すると、SIM が恒久的に使用できなくなる場合があります。PUK が不明な場合は入力せず、通信事業者へお問い合わせください。

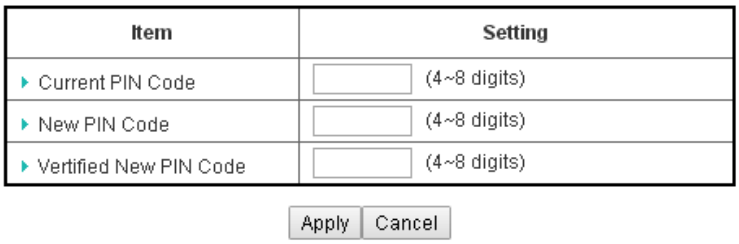
12.1.3.3. SIM 機能 （PIN コードの設定）

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



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

◆ PIN コード変更をクリックすると、以下の画面が表示されます。



◆ 現在の PIN コードと新しい PIN コードを入力して、Apply をクリックしてください。

12.1.4. 通信スキャン

本機能はサポートしていません。

12. 2. SMS＆イベント

本機には、ネットワーク管理者がプロファイルごとにイベントと応答動作を設定し、機器の状態や情報を取得できる機能が搭載されています。

12.2.1. 設定

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

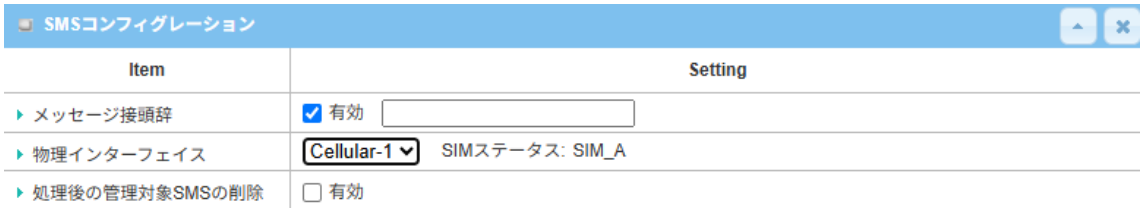
◆ 各項目の設定が完了したら、保存をクリックして、設定を保存します。

12.2.1.1. イベントマネージメントの設定



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

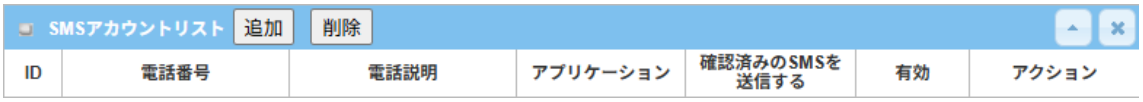
12.2.1.2. SMS コンフィギュレーションの設定



項目	説明
メッセージ接頭辞	[有効]にチェックを入れると、受信SMSの解析が有効になります。 また、マネージングイベントを識別するための接頭辞(プリフィックス文字列)を指定します。
物理インターフェイス	本機では Cellular-1 固定です。対象となるSIMスロットが表示されます。
処理後の管理対象の SMS の削除	[有効]にチェックを入れると、受信したマネージングイベントSMSを処理した後に削除します。

12.2.1.3. SMS アカウントリスト

イベント通知用の SMS アカウントを設定します。 最大 5 つのアカウントをサポートします



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

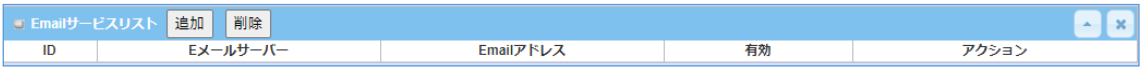


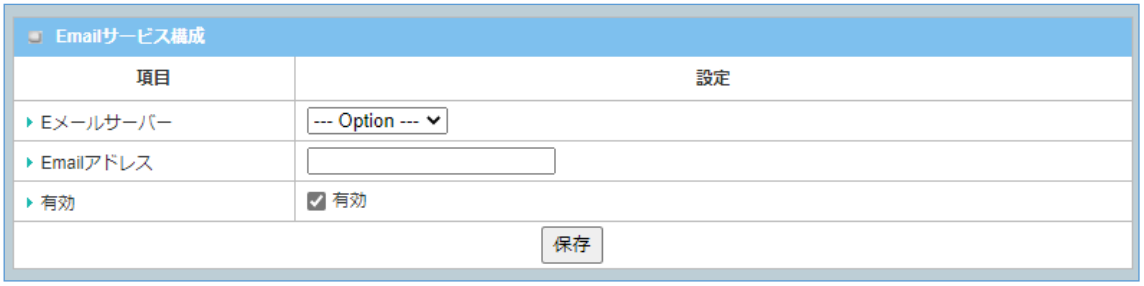
項目	説明
電話番号	SMS による遠隔操作を許可する送信元電話番号を入力します。通知先を指定する項目ではありません。
電話説明	SMS の簡単な説明を記入します。
アプリケーション	アプリケーション(動作)タイプ[イベント設定トリガー]および[イベント通知ハンドル]にチェックを入れると、それぞれの動作が有効になります。
確認済みの SMS を送信する	[有効]にチェックを入れると、SMS応答機能が有効になります
有効	[有効]にチェックを入れると設定した SMS アカウントが有効になります。

12.2.1.4. Email サービスリストの追加/編集

イベント通知用の E メールアドレスを設定します。 最大 5 件設定できます

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





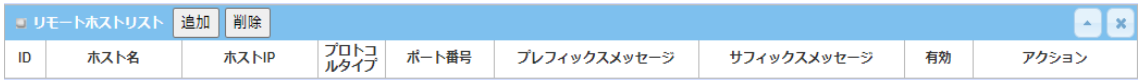
項目	説明
E メールサーバー	電子メールサーバープロファイルを選択します。外部電子メールサーバーは[オブジェクト定義]⇒[外部サーバー]から登録します。
Email アドレス	宛先の電子メールアドレスを指定します。
有効	[有効]にチェックを入れると、この Email サービスが有効になります。

◆ 保存をクリックして、Email サービスを登録します。追加/編集した Email サービスが[E-mail サービスリスト]に表示されます。

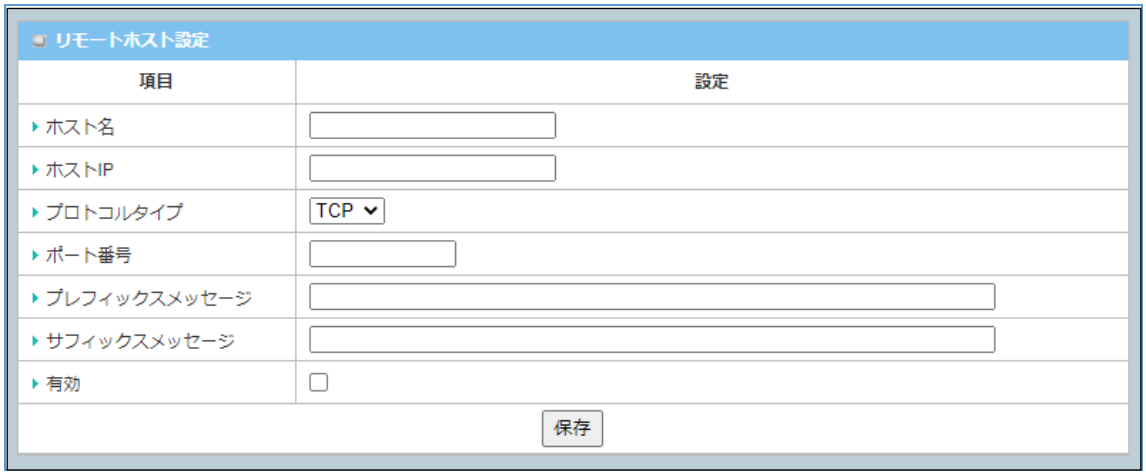
12.2.1.5. リモートホストリストの追加/編集

イベント発生時に通知または接続確認を行うリモートホストを登録します。

最大 10 件のプロファイルをサポートします。



◆ 追加をクリックすると、[リモートホスト設定]画面が表示されます。



12.2.2. マネージングイベント

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

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

12.2.2.1. マネージングイベントの設定



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

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

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

12.2.2.2. マネージングリストの追加/編集



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



項目	説明
イベント名	識別のためのイベント名を指定します。
イベント	イベントタイプを[SMS]または[SNMP トラップ]から選択し、イベント識別子/プロファイルを指定します。 イベントは最大 3 つのイベント条件を指定でき、すべての条件が同時に成立したときにイベントが発行されます。 SMS:テキストボックスに SMS メッセージを指定します。 SNMP:テキストボックスに SNMP トラップイベントメッセージを指定します。SNMP による本機の監視および設定取得には対応しておりません。
トリガタイプ	イベントトリガーのタイプを[期間]または[1 回]を指定します。 期間:[期間]を選択し、時間間隔を指定します。指定したイベント条件が成立すると、イベントはすべての時間間隔で繰り返しトリガーされます。 1 回:[1 回]を選択すると、指定したイベント条件が成立したときに、イベントが 1 回だけトリガーされます。
間隔	繰り返しイベントトリガーの時間間隔を指定します。値の範囲は 0～86400 秒です。
説明	マネージングルールの説明を記述します。
アクション	ネットワークステータス、または定義したイベントが発生したときに実行する少なくとも 1 つのアクションを指定します。 Network Status:ネットワークステータスを取得します。 System Manage:本機ではサポートしていません。 管理(Administration):再起動します。 再起動するためにはトリガタイプを[1 回]に設定する必要があります。
管理イベント	[有効]にチェックを入れると、このマネージングイベントが有効になります。

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

12.2.3. 通知イベント

本機が監視する内部イベントの発生をトリガーとして、あらかじめ設定した SMS や電子メールなどを使用して、イベントの発生を管理者に通知します。

◆ 画面左側のメニューから、サービス⇒SMS＆イベント⇒通知イベントの順にクリックします。
◆ 設定、通知イベントリストの追加が終了したら、保存をクリックして設定を登録します

12.2.3.1. 通知イベントの設定

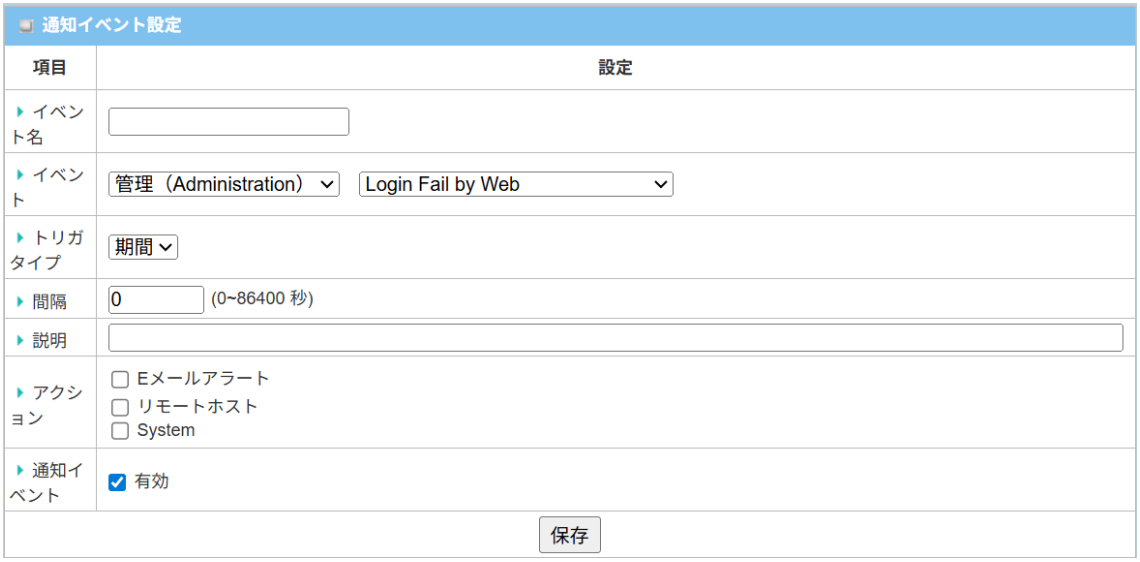


項目	説明
通知イベント	[有効]にチェックを入れると、通知イベントが有効になります。

12.2.3.2. 通知イベントリストの追加/編集

通知イベントルールは最大 128 ルールが登録できます。

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



項目	説明
イベント名	識別のためのイベント名を指定します。
イベント	通知したいイベントタイプと対応するイベント設定を指定します。
トリガタイプ	イベントトリガーのタイプを[期間]または[1 回]を指定します。 期間:[期間]を選択し、時間間隔を指定します。その間隔内で複数回イベントが発生しても通知は一回しかトリガされません。 1 回:[1 回]を選択すると、指定イベント条件が成立するたびにトリガされます。
間隔	繰り返しイベントのトリガの時間間隔を指定します。値の範囲は 0～86400 秒です。
説明	通知イベントの説明を記述します。
アクション	ネットワークステータス、または定義したイベントが発生したときに実行する少なくとも 1 つのアクションを指定します。 SMS:アラート設定した SMS にメッセージを送信します。 Email;:アラート:設定した Email アドレスに E メールを送信します リモートホスト:リモートホストプロファイルを選択します。 System : イベントが発生した30秒後に再起動します。
通知イベント	[有効]にチェックを入れると、この通知イベントが有効になります。

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

12.3. 位置追跡

GNSS の設定を行います。ログのダウンロード/削除およびログを送信するリモートホストの設定ができます。

12.3.1. GNSS

◆ 画面左側のメニューから、サービス⇒位置追跡の順にクリックします。

◆ GNSS の設定が終了したら、保存をクリックして設定を登録します。

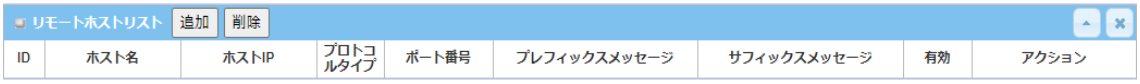
12.3.1.1. 設定



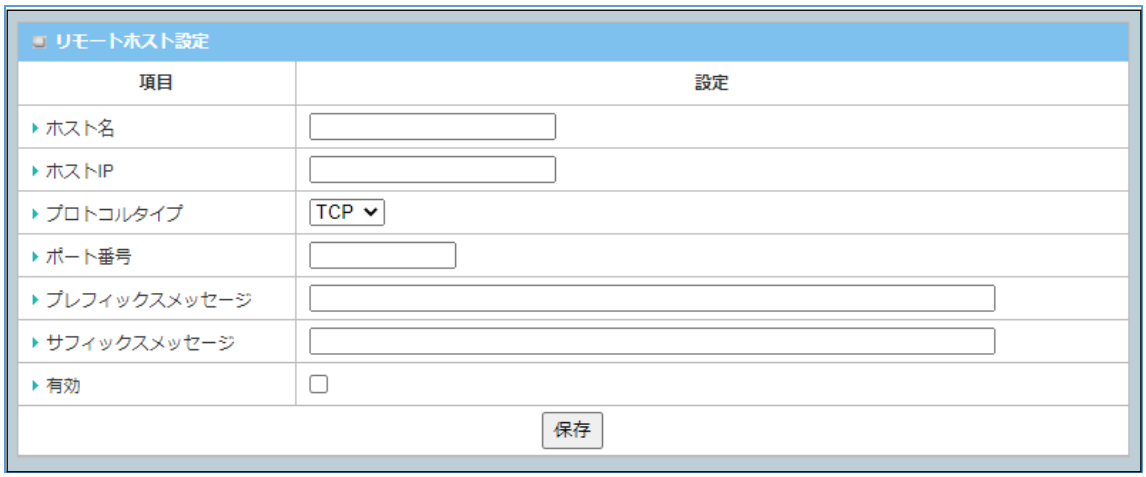
項目	説明
GNSS	[有効]をクリックすると、GNSS 機能が有効になります。
GNSS タイプ	使用する GNSS タイプを[GPS]または[GPS+GLONASS]から選択します。
GNSS メッセージタイプ	GPS データの送信または記録に使用する GNSS メッセージタイプを 1 つ以上選択します。NMEA 規格のセンテンスとして、GGA、GLL、GSA、GSV、RMC、VTG から選択できます。ネットワーク帯域幅の無駄な消費を防ぐため、必要なタイプのみを選択してください。
データの保管	・有効:[有効]にチェックを入れると、データの保管機能が有効になります。 ・選択デバイス:ログデータを保存するデバイスを、内部または外部から選択します。 ・間隔:連続するデータログを取得する時間間隔を指定します。デフォルトは 5 秒です。 値の範囲:5～60 秒 ・データ形式:データ形式を RAW または GPX から選択します。 ・データファイル名:ファイル名を設定します。 ・分割ファイル:チェックを入れると、ファイル分割機能が有効になります。 ・Type:ファイルの分割条件を、時間またはログファイルのサイズから設定します。 ・ログファイルのダウンロード ログファイルを選択し、[ログファイルのダウンロード]をクリックすると、Web 設定画面からファイルをダウンロードできます。保存データ形式に GPX を指定した場合は、標準の GPX 形式に変換されてダウンロードされます。

12.3.1.2. リモートホストリストの追加/編集

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



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



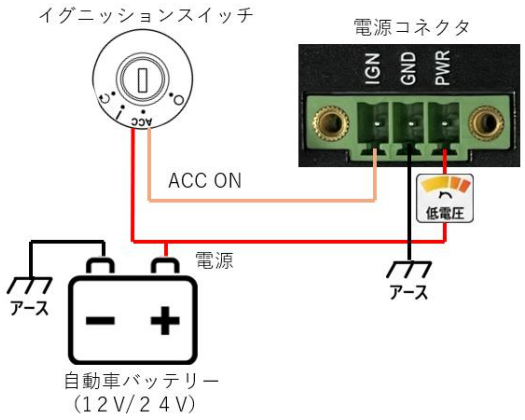
項目	説明
ホスト名	リモートホストプロファイル名を指定します。名前の長さは 64 文字以下です。
ホスト IP	リモートホストの IPv4 フォーマットで IP アドレスを指定します。
プロトコルタイプ	リモートホストにアクセスするためのプロトコルを指定します。 TCP または UDP から選択します。
ポート番号	リモートホストにアクセスするためのポート番号を指定します。 値の範囲は 1～65535 です。
プレフィックスメッセージ	必要に応じて、リモートホストにアクセスするための事前に決められた ID としてプレフィックスメッセージ(64 文字以下)を指定します。
サフィックスメッセージ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

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

12.4. 電源制御

IGN（ACC）信号が ON になると本機を起動し、OFF になると設定した遅延時間の経過後に本機をシャットダウンします。これにより、接続している外部電源の不要な電力消費を抑えることができます。

IGN 端子への接続方法については、[5.5 電源の接続]を参照してください。



本機の電力制御は、車両エンジン停止後のオフ遅延タイマー設定、バッテリー低下検知による自動シャットダウン、およびイグニッション検知によるバッテリー上がり防止のための制御が可能です。

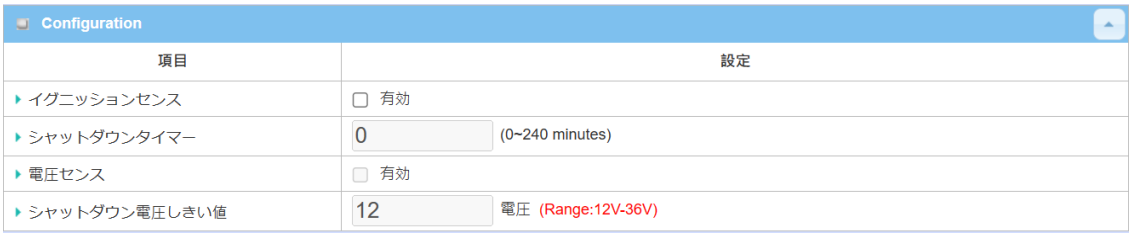
◆ 活用ケース

・エンジンがオフの状態でのサーバーへの車載カメラ映像のアップロード

・一時的な停車の際のインターネット接続の維持

12.4.1. イグニッションセンス

◆ 画面左側のメニューから、サービス⇒電源制御⇒イグニッションセンスの順にクリックします。



項目	説明
イグニッションセンス(注 1)	[有効]をクリックすると、イグニッションセンス機能が有効になります。
シャットダウンタイマー	シャットダウンの条件を満たした時に本機の電源をオフにするまでの時間を設定します。0 を指定した場合は、IGN ピンへの電圧供給がなくても電源はオフになりません。
電圧センス（注 2）	[有効]をクリックすると、電圧センス機能が有効になります。 ACC OFF の状態で入力電圧が指定のしきい値を下回ると、本機はシャットダウンタイマーを無視し、即座にシャットダウンします。 （ACC ON の状態で入力電圧がしきい値を下回ってもシャットダウンされません）
シャットダウン電圧しきい値	本機をシャットダウンする電圧しきい値を設定します。

◆ 設定が完了したら、保存をクリックして設定を登録します。

（注 1） 初期設定では、イグニッションセンス機能は無効です。有効にすると、ターミナルブロックのIGNピンから電力が検出されるまで本製品の電源は入りません。

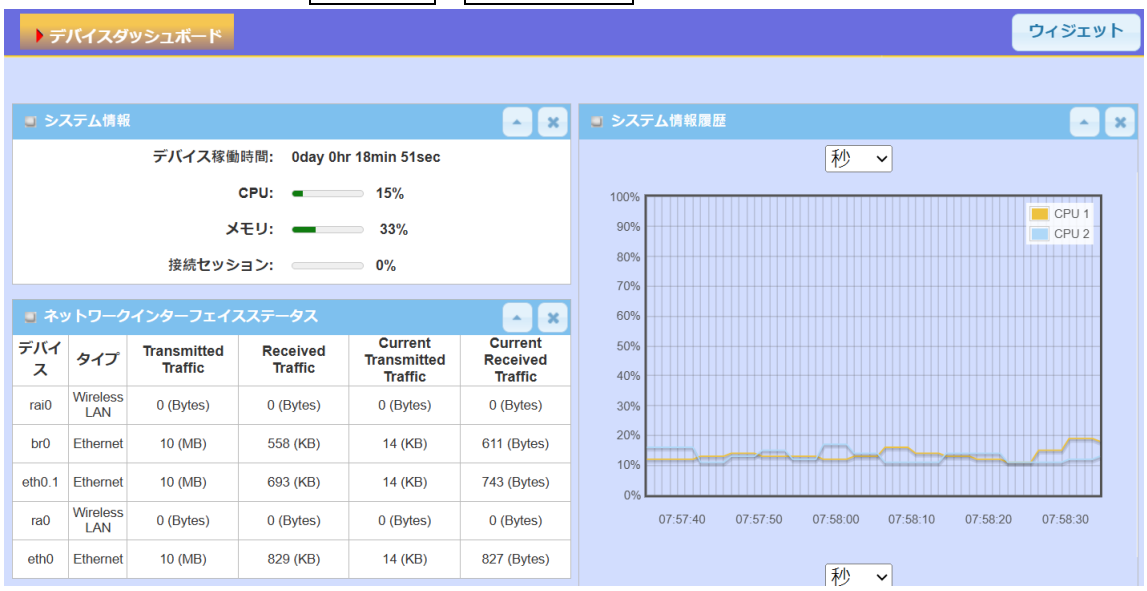
（注 2） バッテリーが完全に上がってしまうことを防ぐための機能です。

13. ステータス

13. 1. ダッシュボード

[デバイスダッシュボード]には、本機の動作ステータスを把握するためのグラフや表で現在の状態を表示します。システム情報、システム情報履歴、および、ネットワークインタフェースステータスが表示されます。表示は 1 秒ごとに更新されます。

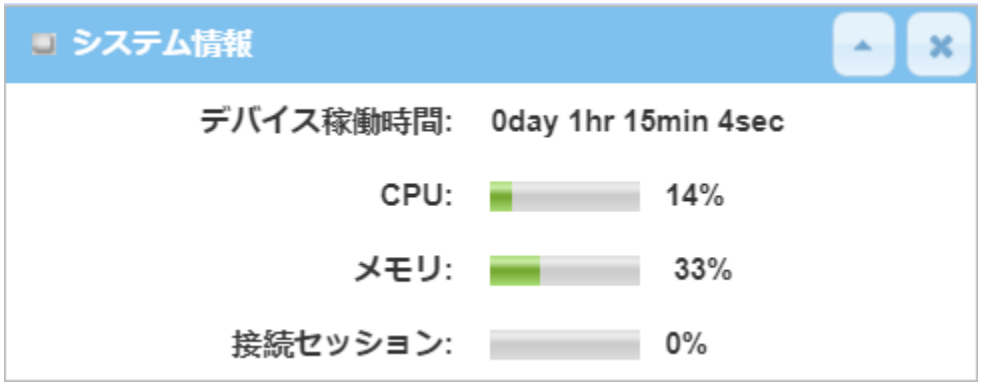
画面左側のメニューから、ステータス⇒ダッシュボードの順にクリックします。



デバイス	タイプ	Transmitted Traffic	Received Traffic	Current Transmitted Traffic	Current Received Traffic
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
br0	Ethernet	10 (MB)	558 (KB)	14 (KB)	611 (Bytes)
eth0.1	Ethernet	10 (MB)	693 (KB)	14 (KB)	743 (Bytes)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
eth0	Ethernet	10 (MB)	829 (KB)	14 (KB)	827 (Bytes)

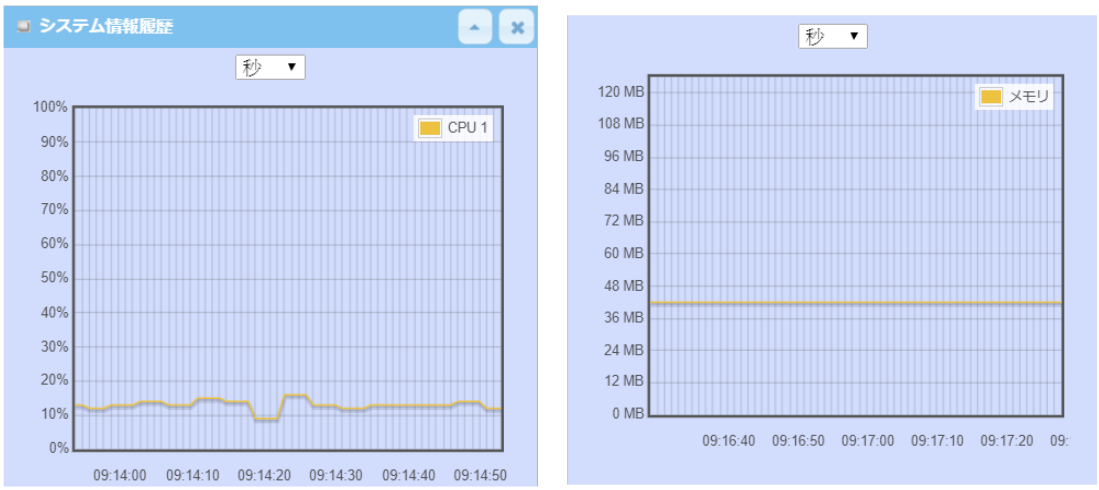
13.1.1. システム情報

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



13.1.2. システム情報履歴

[システム情報履歴]画面には、CPU とメモリの統計グラフが表示されます。



13.1.3. ネットワークインターフェイスステータス

[ネットワークインターフェイスステータス]画面には、本機の各ネットワークインタフェースの統計情報が表示されます。統計情報には、インタフェースタイプ、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	Transmitted Traffic	Received Traffic	Current Transmitted Traffic	Current Received Traffic
rai0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
br0	Ethernet	216 (MB)	8 (MB)	22 (KB)	2 (KB)
eth0.1	Ethernet	217 (MB)	8 (MB)	22 (KB)	2 (KB)
apcli0	WiFi	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
ra0	Wireless LAN	0 (Bytes)	0 (Bytes)	0 (Bytes)	0 (Bytes)
eth0	Ethernet	217 (MB)	9 (MB)	22 (KB)	3 (KB)

13. 2. 基本ネットワーク

13.2.1. WAN & アップリンク

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

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



13.2.1.1. WAN インタフェース IPv4 ネットワークステータス

IPv4 ネットワークの各種ステータス情報が表示されます。

編集をクリックすると接続設定に移動します。



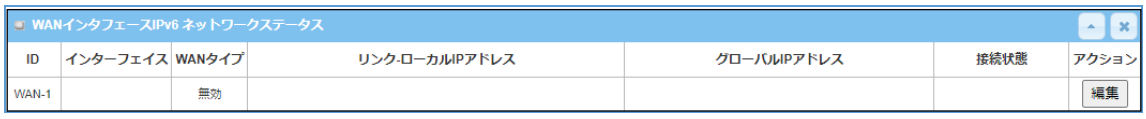
WANインタフェースIPv4 ネットワークステータス

ID	インターフェイス	WANタイプ	ネットワークタイプ	IP Addr.	サブネットマスク	ゲートウェイ	DNS	MACアドレス	接続状態	アクション
WAN-1	Cellular(5G/LTE)	Cellular	NAT	25.94.150.241	255.255.255.252	25.94.150.242	168.95.1.1, 168.95.192.1	N/A	切断中… -	編集

13.2.1.2. WAN インタフェース IPv6 ネットワークステータス

IPv6 ネットワークの各種ステータス情報が表示されます。

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



WANインタフェースIPv6 ネットワークステータス

ID	インターフェイス	WANタイプ	リンク-ローカルIPアドレス	グローバルIPアドレス	接続状態	アクション
WAN-1		無効				編集

13.2.1.3. LAN インタフェースネットワークステータス

LAN ネットワークの各種ステータスが表示されます。

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

IPv6 を編集するをクリックすると、IPv6 の設定画面に移動します。

LANインタフェースネットワークステータス

IPv4アドレス	IPv4サブネットマスク	MACアドレス	アクション
192.168.12.53	255.255.255.0	00:50:18:00:0F:35	IPv4を編集する

13.2.1.4. Cellular[モバイル NET] Modem Status List

モバイル NET の無線通信の各種ステータスが表示されます。

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

Cellular Modem Status List

インターフェイス	カード情報	リンクステータス	信号強度	ネットワーク名	アクション
モバイル NET(5G/LTE)	FCUN69-WWD	切断	N/A	N/A	詳細

＜詳細情報例＞

モデム情報

インターフェイス	モジュール名	IMEI/MEID	ハードウェアバージョン	ファームウェアバージョン	温度	Bandリスト
N/A	FCUN69-WWD	016564000036746	N/A	L0303_JP	N/A	3G LTE 5G

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
N/A	SIMカードが挿入されていません	N/A / N/A	N/A	+CME ERROR: 3	N/A	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
N/A	N/A	N/A	N/A	N/A	N/A	N/A

CS / PS ジスタステータス	PS添付ステータス	ローミングステータス
無登録 / 無登録	取り外す	ローミングしていません

LTE Signal Strength and Quality

Band	RSSI	RSRQ	RSRP	SINR
N/A	N/A	N/A	N/A	N/A

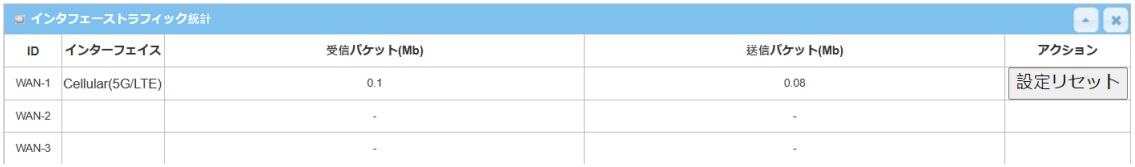
エラーメッセージ

索引	エラーの説明
1	N/A

13.2.1.5. インタフェーストラフィック統計

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

設定リセットでトラフィック情報をリセットできます。



13.2.2. LAN および VLAN

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

13.2.2.1. クライアントリスト

本機LANに接続されているデバイスの情報が表示されます。



13.2.3. Wifi

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

13.2.3.1. WiFi モジュール1 バーチャル AP リスト

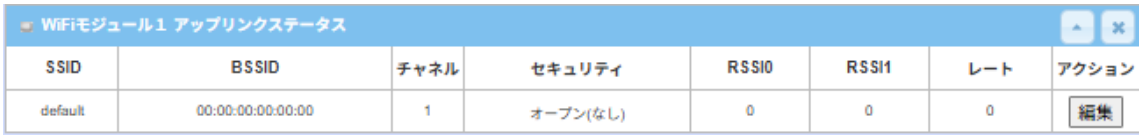
すべての仮想 AP 情報が表示されます。編集をクリックすると接続設定に移動します。



13.2.3.2. WiFi モジュール1 アップリンクステータス

本機と他機器の接続状況や通信品質が表示されます。

編集をクリックすると接続設定に移動します。



13.2.3.3. WiFi モジュール1IDS ステータス

[認証フレーム][関連付け要求フレーム][再関連付け要求フレーム][プローブ要求フレーム][分離フレーム][認証取り消しフレーム][EAP 要求フレーム][悪意のあるデータフレーム]を受信した回数を表示します。

WiFiモジュール1 IDSステータス

認証フレーム	関連付け要求フレーム	再関連付け要求フレーム	プローブ要求フレーム	分離フレーム	認証取消しフレーム	EAP要求フレーム	悪意のあるデータフレーム	アクション
0	0	0	0	0	0	0	0	設定リセット

※基本ネットワーク⇒WiFi⇒詳細構成から WIDS 機能を有効にする必要があります。

13.2.3.4. WiFi モジュール1トラフィック統計

ネットワーク上で送受信されたすべてのパケット数を VAP ごとに表示します。

WiFiモジュール1 トラフィック統計

操作バンド	ID	受信パケット	送信パケット
2.4G	VAP-1	0	0
2.4G	VAP-2	0	0
2.4G	VAP-3	0	0
2.4G	VAP-4	0	0
2.4G	VAP-5	0	0
2.4G	VAP-6	0	0

13.2.4. ダイナミック DNS

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

13.2.4.1. DNS ステータスリスト

ダイナミック DNS の状態が表示されます。更新で最新の情報を表示します。

DNSステータスリスト

ホスト名	プロバイダ	実効IP	最終更新ステータス	最終更新時刻
hy[illegible]-01.ddns.net	No-IP.com	146.99.185.134	Ok	2020/10/31 22:49:35

13. 3. セキュリティ

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



13.3.1. VPN

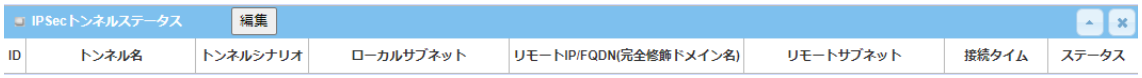
VPN ステータスウィンドウには、VPN トンネルの全体的なステータスが表示されます。表示は 5 秒ごとに更新されます。

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

13.3.1.1. IPSec トンネルステータス

IPSec VPN 接続設定と現在のステータスが表示されます。

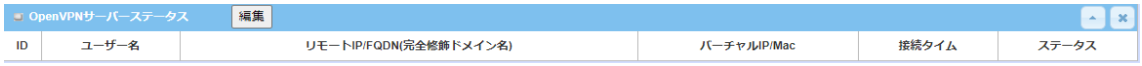
編集をクリックすると IPSec の設定画面に移動します。



13.3.1.2. OpenVPN サーバーステータス

OpenVPN サーバーの接続状態が表示されます。

編集をクリックすると、OpenVPN サーバーの設定画面に移動します。



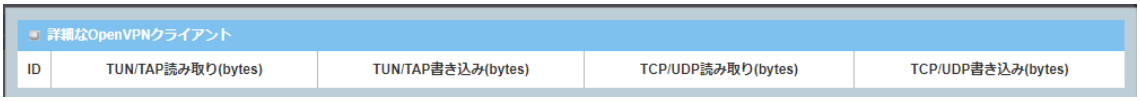
13.3.1.3. OpenVPN クライアントステータス

OpenVPN による接続状態が表示されます。

編集をクリックすると、OpenVPN クライアントの設定画面に移動します。



詳細をクリックすると、クライアントのデータ通信ステータスが表示されます。



13.3.1.4. L2TP サーバーステータス

L2TP サーバートンネリングの設定と現在のステータスが表示されます。

編集をクリックすると、L2TP サーバーの設定画面に移動します。



13.3.1.5. L2TP クライアントステータス

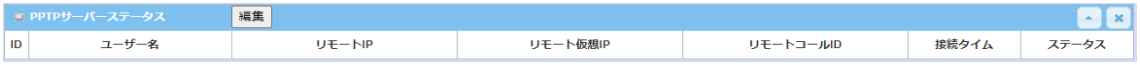
L2TP トンネリングの設定と現在のステータスが表示されます。

編集をクリックすると、L2TP クライアントの設定画面に移動します。

13.3.1.6. PPTP サーバーステータス

PPTPトンネリングの設定と現在のステータスが表示されます。

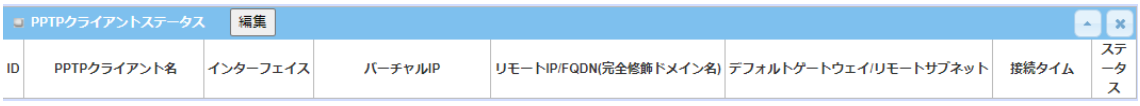
編集をクリックすると、PPTP サーバーの設定画面に移動します。



13.3.1.7. PPTP クライアントステータス

PPTPトンネリングの設定と現在のステータスが表示されます。

編集をクリックすると、PPTP クライアントの設定画面に移動します。



13.3.2. ファイヤーウォール

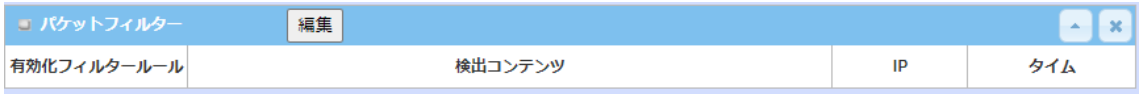
ファイヤーウォールステータスウィンドウには、ファイヤーウォールの全体的な設定とステータスが表示されます。表示は 5 秒ごとに更新されます。

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

13.3.2.1. パケットフィルター

パケットフィルタリングのログ履歴が表示されます。

編集をクリックすると、パケットフィルター設定画面に移動します。



13.3.2.2. URL ブロッキング

URL ブロッキングのログ履歴が表示されます。

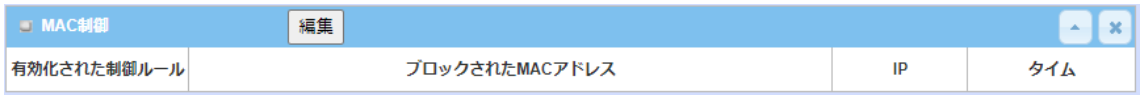
編集をクリックすると、URL ブロッキング設定画面に移動します。



13.3.2.3. MAC 制御

MAC 制御のログ履歴が表示されます。

編集をクリックすると、MAC 制御設定画面に移動します。



13.3.2.4. IPS

IPS のログ履歴が表示されます。

編集をクリックすると、IPS 設定画面に移動します。



13.3.2.5. オプション

オプションの設定とログ履歴が表示されます。

編集をクリックすると、オプション設定画面に移動します。



13. 4. 管理(Administration)

13.4.1. 設定と管理

本機ではサポートしていません。

13.4.2. ログストレージ

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

13.4.2.1. ストレージ情報ステータス

ログ保管メディアの現在の状態が表示されます。

更新で最新の情報が表示されます。



13.4.3. GNSS

◆ 画面左側のメニューから、ステータス⇒管理(Administration)⇒GNSS の順にクリックします。

13.4.3.1. GNSS 情報

現在の GNSS 測位情報のステータスが表示されます。

更新で最新の情報が表示されます。



13.5. 統計とレポート

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

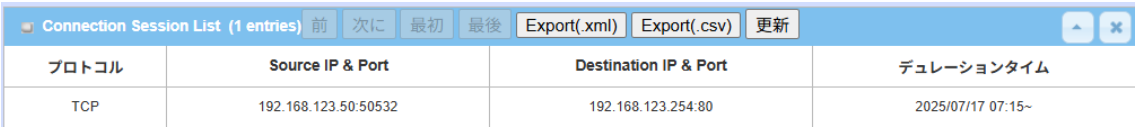


13.5.1. 接続セッション

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

13.5.1.1. Connection Session List

本機で管理している接続トラフィック情報が表示されます。



前、次に、最初および最後をクリックして、表示ページを変更します。

更新をクリックすると、リストが最新の情報になります。

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

13.5.2. ログイン統計

13.5.2.1. デバイス管理者統計

本機へのログイン履歴が表示されます。



前、次に、最初および最後をクリックして、表示ページを変更します。

更新をクリックすると、リストが最新の情報になります。

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

13.5.2.2. セルラー使用状況

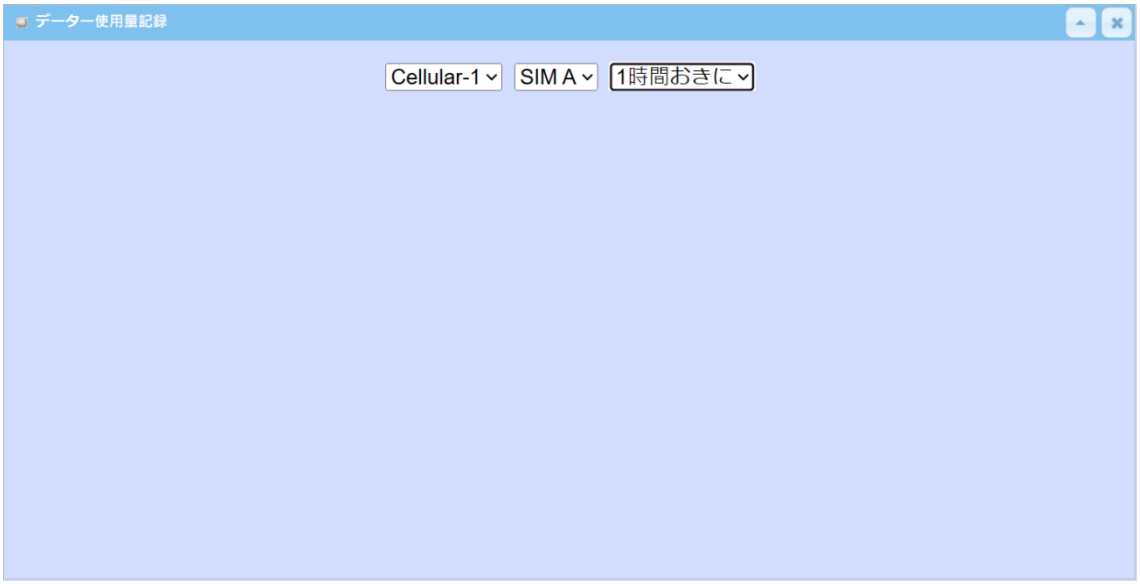
◆ 画面左側のメニューから、ステータス⇒統計とレポート⇒セルラー使用状況の順にクリックします。

13.5.2.3. データ使用量記録

[SIM-A]または[SIM-B]から選択したセルラーインタフェースのデータ使用量記録が表示されます。使用量の記録頻度を[1 時間おき]または[毎日]から選択できます。

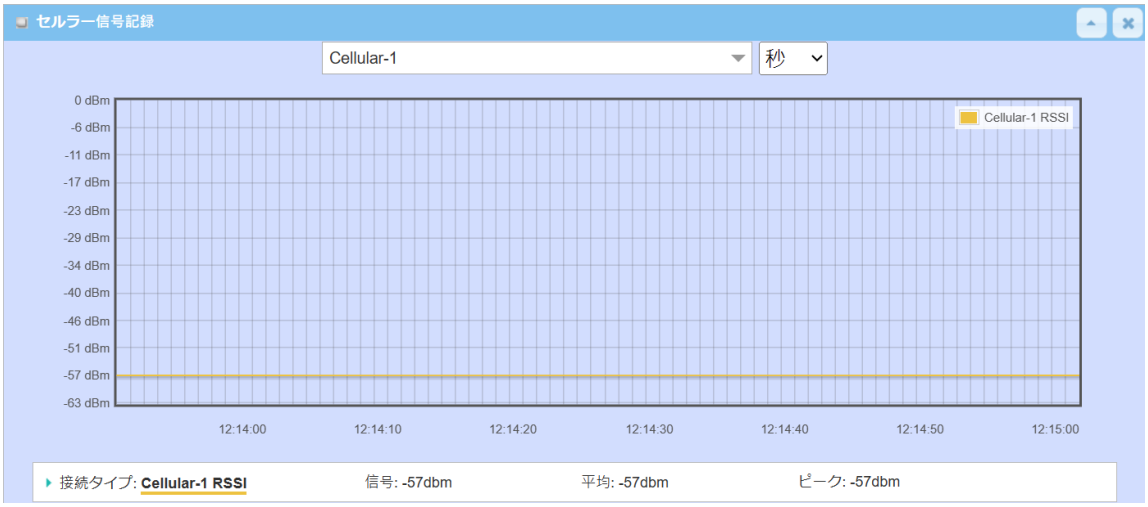
13.5.3. セルラー信号

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



13.5.3.1. セルラー信号記録

セルラー信号強度の現在値、平均値、ピーク値および時間推移のグラフを表示します。



14. 製品仕様

製品型番		HW5G-3311-DS
商品コード		189-HY01-0002
5G/LTE	対応バンド	TDD NR5G: n40/n41/n77/n78/n79
		FDD NR5G: n1/n3/n8/n26/n28
		FDD LTE: B1/B3/B8/B18/B19/B26/B28
		TDD LTE: B39/B41/B42
	MIMO	DL：対応、UL：対応 （MIMO 対応バンドのみ）
	対応 5G ネットワーク	スタンドアローン(SA)/ノンスタンドアローン(NSA)
	対応キャリア	NTT docomo、KDDI
	対応 SIM カード/Slot 数	nano SIM / 2 Slot
	アンテナ/インタフェース	外部アンテナ / 4xSMA(F)コネクタ
無線 LAN	伝送方式	IEEE802.11 ax/ac/n/g/b/a
	通信周波数	2.4GHz /5GHz 帯
	セキュリティ	WPA2-PSK（AES）, WPA/WPA2-PSK(TKIP/AES), WPA2/WPA3-PSK(AES/SAE)
	機能	仮想 AP, 自動チャネル選択, STA 分離機能, WMM, WIDS, MU-MIMO
	アンテナ/インタフェース	外部アンテナ / 2xSMA(M)コネクタ
GNSS	対応周波数	1575.42MHz(L1C/A,B1I), 1598.06～1605.38MHz(L1)
	対応衛星システム	GPS/GLONASS
	位置追跡	デバイス内保存/リモートホスト
	アンテナ/インタフェース	外部アンテナ（オプション） / 1xSMA(F)コネクタ
イーサネット	対応速度/規格	10/100/1000BASE-T、オートネゴシエーション、 オート MDI/MDI-X、フローコントロール
	インタフェース	LAN ポート：3x RJ-45 コネクタ WAN ポート：1x RJ-45 コネクタ（LAN1/WAN 兼用、排他利用）
プロトコル	LAN	DHCP サーバー、タグ/ポートベース VLAN
	TCP/IP	IPv4/IPv6 Dual Stack
	ポート制御	NAT/Port Forwarding/DMZ/VPN パススルー
	ルーティング	Static/RIP1,2/OSPF/BGP
	QoS	帯域幅/優先度/セッション制限
セキュリティ	VPN	IPsec/OpenVPN/PPTP/L2TPv2/WireGuard/GRE/EoGRE
	ファイヤーウォール	SPI Firewall/IPS/MAC, Packet, URL 各種フィルタ
管理機能	設定	Web GUI
	診断ツール	PING/TRACERT
	ステータス表示	装置(CPU/メモリ)/ネットワーク/モバイル/セキュリティ情報
推奨接続機器数		LAN+WiFi 合計 32 台以下、WiFi16 台以下
LED 表示		ステータス（青）, モバイル NET 信号（青）, LAN1/WAN、LAN2～LAN4（緑）
防塵・防水性能		なし
電源		DC9V～36V、イグニッションセンス機能 （3 ピンターミナルブロック：PWR／GND／IGN）
消費電力	本体消費電力	最大 14W
動作温度		-30 ～ +60℃
保存温度		-40 ～ +85℃
相対湿度		10 ～ 95% （結露なきこと）
本体寸法		(W)160mm x (D)126mm x (H)47mm (突起物含まず)
本体重量		995g

認証等	工事設計認証番号(無線 LAN):020-240155 工事設計認証番号(5G NR/LTE):003-240124 技術基準適合認証番号:D240098003 VCCI Class A 本体、添付品 RoHS 10 対応
製品保証期間	1 年間
付属品	5G/LTE アンテナ x4、WiFi アンテナ x2、 電源用ターミナルブロック x1、マウントブラケット x2 マウントブラケット取付けネジ x4

15. 製品保証

◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

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

初期不良保証期間:

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

製品保証期間:

《本体》ご購入日より **1年間**（お預かりによる修理、または交換対応）

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

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

◆ 保証期間を過ぎますと有償修理となりますのでご注意ください。

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

◆ 本製品に起因する損害や機会の損失については補償致しません。

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

◆ 本製品の保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社 カスタマサポート

受付時間： 平日（土日祝日、年末年始、当社休業日を除く） 9:00～17:00

TEL： 0570-060030

問合せフォーム：https://hytec.co.jp/contact/technical_support_form.html

Copyright © 2026
HYTEC INTER Co., Ltd.