



HW5G-3200-V2

取扱説明書



HYTEC INTER Co., Ltd.

第 1.3 版

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製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	2021 年 04 月 27 日	初版制定
第 1.1 版	2021 年 11 月 05 日	工事設計認証番号の変更
第 1.2 版	2022 年 12 月 15 日	ネットワーク監視機能の利用上注意点を追加
第 1.3 版	2023 年 9 月 15 日	MTU に関する記述変更、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。
- 本製品及び付属品を分解したり改造したりすることは絶対に行わないでください。
- 本製品及び付属品を直射日光の当たる場所や、温度の高い場所で使用しないでください。本体内部の温度が上がり、故障や火災の原因になることがあります。
- 本製品及び付属品を暖房器具などのそばに置かないでください。ケーブルの被覆が溶けて感電や故障、火災の原因になることがあります。
- 本製品及び付属品をほこりや湿気の多い場所、油煙や湯気のあたる場所で使用しないでください。故障や火災の原因になることがあります。
- 本製品及び付属品を重ねて使用しないでください。故障や火災の原因になることがあります。
- 通気口をふさがないでください。本体内部に熱がこもり、火災の原因になることがあります。
- 通気口の隙間などから液体、金属などの異物を入れないでください。感電や故障の原因になることがあります。
- 付属のACアダプタは本製品専用となります。他の機器には接続しないでください。また、付属品以外のACアダプタを本製品に接続しないでください。
- 本製品及び付属品の故障、誤動作、不具合、あるいは天災、停電等の外部要因によって、通信などの機会を逸したために生じた損害等の純粋経済損害につきましては、弊社は一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品及び付属品は、改良のため予告なしに仕様が変更される可能性があります。あらかじめご了承ください。

目次

1. 製品概要	13
2. モバイル NET 回線契約	13
3. 梱包物一覧	13
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	14
5.1. LED	14
5.1.1. 各 LED	14
5.2. 前面	15
5.3. 背面	15
5.4. SIM カードの取り付け/取り外し方法	16
6. WEB GUI での設定について	17
6.1. WEB GUI へのアクセス	17
6.1.1. PC システム要件	17
6.1.2. ログイン初期設定	17
6.1.3. ログイン手順	18
6.1.4. Web 表示言語の変更	19
6.2. LAN 側 IP アドレスの設定	20
6.3. 管理ユーザー名の変更	20
◇ 基本設定編	21
7. モバイル NET の設定	21
7.1. 物理インターフェースの設定	21
7.2. モバイル NET パラメータの設定	22
◇ 応用設定編	25
8. 基本ネットワーク	25
8.1. WAN およびアップリンク	25

8.1.1.	物理インタフェースリスト	25
8.1.2.	フェールオーバー機能	26
8.1.3.	物理インタフェースの設定	27
8.1.4.	接続設定	28
8.1.5.	WAN タイプ: モバイル NET の接続設定	28
8.1.5.1.	デュアル SIM フェールオーバー機能について	28
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	29
8.1.5.3.	SIM 転換のポリシーの設定	30
8.1.5.4.	SIM-A カードとの接続/SIM-B カードとの接続	31
8.1.5.5.	モバイル NET 接続の共有設定[Cellular Connection Common Configuration]	
	32	
8.1.6.	WAN タイプ: イーサネットの接続設定	33
8.1.6.1.	イーサネット WAN 設定	33
8.1.6.2.	静的IP WAN 設定	34
8.1.6.3.	動的IP WAN 設定	35
8.1.6.4.	PPPoE WAN 設定	36
8.1.6.5.	PPTP WAN 設定	37
8.1.6.6.	L2TP WAN 設定	38
8.1.7.	ネットワーク監視構成の設定	40
8.1.7.1.	ネットワーク監視構成の使用上の注意点	41
8.1.8.	負荷分散	42
8.1.8.1.	負荷分散の設定	42
8.1.8.2.	特定のウェイトの設定	43
8.1.8.3.	ユーザーポリシーリストの追加・編集	43
8.2.	LAN および VLAN	45
8.2.1.	イーサネット LAN	45
8.2.2.	追加 IP (LAN IP エイリアス) 機能	46
8.2.3.	仮想 LAN (VLAN)	47
8.2.4.	仮想 LAN (VLAN) の設定	47
8.2.4.1.	ポートベース VLAN ルールの設定	47
8.2.4.2.	IP 固定マッピングルールの設定	51
8.2.4.3.	ポートベース VLAN 間グループルーティング	51
8.2.4.4.	タグベース VLAN ルールの設定	52
8.2.5.	DHCP サーバー	54
8.2.5.1.	DHCP サーバーリスト	54
8.2.5.2.	DHCP サーバーの設定	55
8.2.5.3.	IP 固定マッピングルールの設定	56

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	57
8.2.5.5.	DHCP サーバーオプションの有効/無効	57
8.2.5.6.	DHCP サーバーオプションリストの追加/編集	58
8.2.5.7.	DHCP リレー構成リストの追加/編集	59
8. 3.	IPv6	60
8.3.1.	IPv6 接続タイプ	60
8.3.1.1.	静的 IPv6	60
8.3.1.2.	DHCPv6	60
8.3.1.3.	PPPoEv6	61
8.3.2.	IPv6 構成設定	61
8.3.2.1.	静的 IPv6 WAN タイプ構成	62
8.3.2.2.	DHCPv6 WAN タイプ構成	62
8.3.2.3.	PPPoE WAN タイプ構成	62
8.3.2.4.	LAN 構成	63
8.3.2.5.	アドレス自動構成	64
8. 4.	ポート転送	65
8.4.1.	ポート転送設定	65
8.4.1.1.	NAT ループバック	65
8.4.2.	仮想サーバー & 仮想コンピュータ	66
8.4.2.1.	仮想サーバー	66
8.4.2.2.	仮想コンピュータ	66
8.4.2.3.	仮想サーバーおよび仮想コンピュータの有効	67
8.4.2.4.	仮想サーバーの追加/編集	67
8.4.2.5.	仮想コンピュータの追加/編集	69
8.4.3.	DMZ およびパススルー	70
8.4.3.1.	DMZ (De Militarized Zone)	70
8.4.3.2.	VPN パススルー	70
8.4.3.3.	DMZ の設定	71
8.4.3.4.	VPN パススルーの設定	71
8. 5.	ルーティング	72
8.5.1.	静的ルーティング	72
8.5.1.1.	静的ルーティングの設定	72
8.5.1.2.	IPv4 静的ルーティングルールの追加/編集	73
8.5.2.	動的ルーティング	74
8.5.2.1.	RIPv1/RIPv2 ルーティング	74
8.5.2.2.	OSPF ルーティング	74
8.5.2.3.	BGP ルーティング	74
8.5.2.4.	RIP 設定	75

8.5.2.5.	OSPF 設定	75
8.5.2.6.	OSPF 領域リストの追加/編集	76
8.5.2.7.	BGP 設定	76
8.5.2.8.	BGP ネットワークリストの追加/編集	77
8.5.2.9.	BGP 近隣ルールの追加/編集	77
8.5.3.	ルーティング情報	78
8. 6.	DNS & DDNS	79
8.6.1.	動的 DNS の設定	79
8.6.2.	DNS リダイレクトの設定	80
8.6.3.	リダイレクトルールの定義	80
8. 7.	QoS	81
8.7.1.	QoS 設定	81
8.7.2.	システムリソース設定(ソフトウェア QoS)	81
8.7.3.	WAN インタフェースリソース設定	82
8.7.4.	QoS ルールの追加・編集	83
8. 8.	冗長機能	85
8.8.1.	VRRP 設定	85
9.	オブジェクト定義	86
9. 1.	スケジューリング	86
9.1.1.1.	タイムスケジュールリストの追加/編集	86
9.1.1.2.	期間定義の設定	87
9. 2.	外部サーバー	88
9.2.1.1.	外部サーバーリストの追加/編集	88
9. 3.	証明書	90
9.3.1.	ローカル証明書	90
9.3.1.1.	ローカル証明書の作成	90
9.3.1.2.	証明書のインポート	92
9.3.2.	信頼できる証明書	92
10.	セキュリティ	93
10. 1.	VPN	93
10.1.1.	IPSec	94
10.1.1.1.	IPSec の設定	94
10.1.1.2.	IPSec トンネルの追加/編集	94
10.1.1.3.	トンネル設定	94
10.1.1.4.	ローカル & リモート設定	95
10.1.1.5.	認証設定	96

10.1.1.6.	IKE フェーズ設定	96
10.1.1.7.	IKE プロポーザル定義	97
10.1.1.8.	IPSec フェーズ設定	97
10.1.1.9.	IPSec プロポーザル定義	97
10.1.2.	OpenVPN	99
10.1.2.1.	OpenVPN の設定	99
10.1.2.2.	OpenVPN クライアントリストの追加/編集	100
10.1.2.3.	OpenVPN クライアント詳細構成	101
10.1.3.	L2TP	104
10.1.3.1.	L2TP の設定	104
10.1.3.2.	L2TP サーバーの設定	104
10.1.3.3.	L2TP サーバーステータス	106
10.1.3.4.	ユーザーアカウントの追加・編集	106
10.1.3.5.	L2TP クライアントの設定	107
10.1.3.6.	L2TP クライアントリストの追加/編集	107
10.1.4.	PPTP	109
10.1.4.1.	PPTP の設定	109
10.1.4.2.	PPTP サーバーの設定	109
10.1.4.3.	PPTP サーバーステータス	110
10.1.4.4.	ユーザーアカウントの追加・編集	110
10.1.4.5.	PPTP クライアントの設定	111
10.1.4.6.	PPTP クライアントリストの追加/編集	111
10.1.5.	GRE	113
10.1.5.1.	GRE の設定	113
10.1.5.2.	GRE トンネルの追加/編集	113
10.2.	ファイヤーウォール	115
10.2.1.	パケットフィルター	115
10.2.1.1.	パケットフィルター設定	115
10.2.1.2.	パケットフィルタールの追加/編集	116
10.2.2.	URL ブロッキング	118
10.2.2.1.	URL ブロッキング設定	118
10.2.2.2.	URL ブロッキングルールの追加/編集	119
10.2.3.	MAC 制御	121
10.2.3.1.	MAC 制御設定	121
10.2.3.2.	MAC 制御ルールリストの追加/編集	122
10.2.4.	IPS	123
10.2.4.1.	IPS 設定	123
10.2.4.2.	侵入防止機能設定	124

10.2.5. オプション	125
10.2.5.1. ファイアウォールオプション設定	125
10.2.5.2. リモート管理者ホスト定義の編集	126
11. 管理(Administration).....	127
11.1. 設定と管理（本機ではサポートしていません）.....	127
11.1.1. コマンドスクリプト	127
11.1.2. TR-069	127
11.1.3. SNMP	127
11.1.4. Telnet & SSH	127
11.2. システム管理.....	128
11.2.1. パスワード及び MMI	128
11.2.1.1. ホスト名の設定	128
11.2.1.2. ユーザ名の変更.....	128
11.2.1.3. パスワードの変更	128
11.2.1.4. MMI(マネージメントインタフェース)の設定	129
11.2.2. システム情報.....	130
11.2.3. システムタイム	131
11.2.3.1. タイムサーバーと同期する	131
11.2.3.2. 手動でシステム時間を設定する.....	132
11.2.3.3. PC と手動で同期をとる	133
11.2.3.4. モバイル NET 無線回線の時刻通知を利用して同期をとる	133
11.2.4. システムログ.....	134
11.2.4.1. 表示および E メールログ履歴.....	134
11.2.4.2. ログタイプカテゴリ	135
11.2.4.3. E メールアラート.....	135
11.2.4.4. Syslogd.....	136
11.2.4.5. ログの保管	136
11.2.5. バックアップ及び復元.....	137
11.2.6. 再起動およびリセット.....	138
11.3. 診断	139
11.3.1. パケットアナライザ.....	139
11.3.1.1. 設定.....	139
11.3.1.2. キャプチャとフィルタの条件	140
11.3.2. 診断ツール.....	142
12. サービス.....	143
12.1. セルラーツールキット.....	143

12.1.1. データ使用量(データ使用量の制限)	143
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	144
12.1.2. SMS	145
12.1.2.1. SMS の設定	145
12.1.2.2. SMS 要約(サマリー)	145
12.1.2.3. 新規 SMS	146
12.1.2.4. SMS 受信トレイ	147
12.1.2.5. SMS 送信フォルダ	148
12.1.3. SIM PIN	149
12.1.3.1. SIM カードの選択(Configuration)	149
12.1.3.2. PUK 機能	150
12.1.3.3. SIM 機能 (PIN コードの設定)	150
12.1.4. 通信スキャン	151
12.2. SMS & イベント	152
12.2.1. マネージングイベント	152
12.2.2. 通知イベント	152
12.2.3. 設定	152
12.2.3.1. イベントマネージメントの設定	153
12.2.3.2. SMS コンフィグレーションの設定	153
12.2.3.3. SMS アカウントリスト追加/編集	154
12.2.3.4. Email サービスリストの追加/編集	155
12.2.3.5. リモートホストリストの追加/編集	156
12.2.4. マネージングイベント	157
12.2.4.1. マネージングイベントの設定	157
12.2.4.2. マネージングリストの追加/編集	158
12.2.5. 通知イベント	160
12.2.5.1. 通知イベントの設定	160
12.2.5.2. 通知イベントリストの追加/編集	160
13. スタータス	162
13.1. ダッシュボード	162
13.1.1. システム情報	162
13.1.2. システム情報履歴	163
13.1.3. ネットワークインタフェースステータス	163
13.2. 基本ネットワーク	164
13.2.1. WAN & アップリンク	164
13.2.2. WAN インタフェース IPv4 ネットワークステータス	164
13.2.3. WAN インタフェース IPv6 ネットワークステータス	164

13.2.4.	LAN インタフェースネットワークステータス.....	165
13.2.5.	Cellular[モバイル NET] Modem Status List.....	165
13.2.6.	インタフェーストラフィック統計.....	166
13.2.7.	LAN および VLAN.....	166
13.2.7.1.	クライアントリスト.....	166
13.2.8.	ダイナミック DNS.....	167
13.2.8.1.	DNS ステータスリスト.....	167
13. 3.	セキュリティ.....	168
13.3.1.	VPN.....	168
13.3.1.1.	IPSec トンネルステータス.....	168
13.3.1.2.	OpenVPN サーバステータス.....	168
13.3.1.3.	OpenVPN クライアントステータス.....	169
13.3.1.4.	L2TP サーバステータス.....	169
13.3.1.5.	L2TP クライアントステータス.....	169
13.3.1.6.	PPTP サーバステータス.....	169
13.3.1.7.	PPTP クライアントステータス.....	169
13.3.2.	ファイヤーウォール.....	170
13.3.2.1.	パケットフィルタステータス.....	170
13.3.2.2.	URL ブロッキングステータス.....	170
13.3.2.3.	MAC 制御ステータス.....	170
13.3.2.4.	IPS ステータス.....	171
13.3.2.5.	オプションステータス.....	171
13. 4.	管理(Administration).....	172
13.4.1.	設定と管理.....	172
13.4.2.	ログストレージ.....	172
13.4.2.1.	ストレージ情報ステータス.....	172
13. 5.	統計とレポート.....	173
13.5.1.	接続セッション.....	173
13.5.1.1.	インターネットサーフィンリスト.....	173
13.5.2.	ネットワークトラフィック.....	174
13.5.2.1.	ネットワークトラフィック統計.....	174
13.5.3.	ログイン統計.....	174
13.5.3.1.	デバイス管理者統計.....	174
13.5.3.2.	セルラー使用状況.....	175
13.5.3.3.	データ使用量記録.....	175
13.5.4.	セルラー信号.....	175
13.5.4.1.	セルラー信号記録.....	175

14. 製品仕様	176
15. 付属 AC アダプタ仕様.....	177
16. 製品保証	178

1. 製品概要

HW5G-3200-V2 は、-20～+60℃の広い動作温度に対応した産業用の 5G/LTE 対応ルーターです。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、5G/LTE 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) 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(4G) 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(オプションの場合もあります)契約された SIM 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、不足の品がありましたら、お手数ですがお買い上げの販売店までご連絡ください。

名 称	数 量
本体	1 台
5G/LTE アンテナ	4本
AC アダプタ	1 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



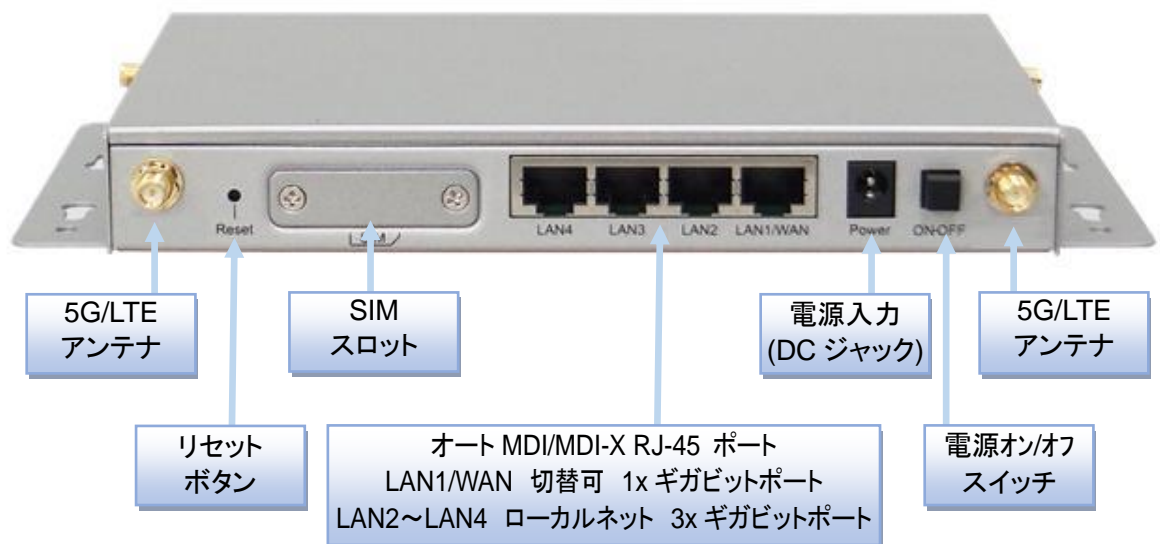
5.1.1. 各 LED

表示		説明
 ステータス	点灯	<ul style="list-style-type: none"> ● 橙 : 起動中です。 ● 緑 : 正常モードで動作中です。
	点滅	<ul style="list-style-type: none"> ● 橙の高速点滅: 復旧モードまたは異常状態です。
 5G/LTE 状態	点灯色	<ul style="list-style-type: none"> ● 緑 : 5G または LTE モードで通信中です。 ● 橙 : 3G で通信中です。
	点灯状態	<ul style="list-style-type: none"> ● 高速点滅 : 信号強度が0～30%です。 ● 低速点滅 : 信号強度が31%～60%です。 ● 点灯 : 信号強度が61～100%です。
 LAN ポート 状態(青色)	消灯	イーサネットケーブルが接続されていないか、リンクが確立していません。
	点灯	イーサネットのリンクが確立しています。
	点滅	イーサネット経由でデータが送受信されています。


5.2. 前面



5.3. 背面



リセットボタン

- ◆ リセットボタンを 10 秒～12 秒間押し続けてから放すと、設定を初期化することができます。
初期化動作に移行するとステータス LED(緑)  が高速に点滅します。

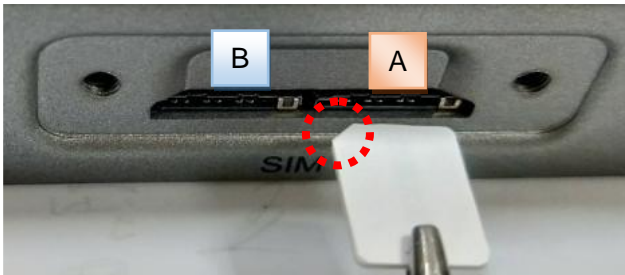
5.4. SIM カードの取り付け/取り外し方法

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 カバーを取り外します。

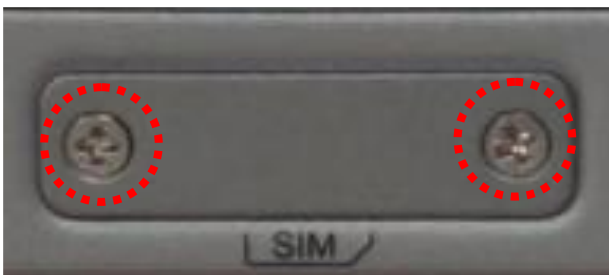


- ◆ SIM カードを挿入します。



SIM カードの切欠き方向を合わせてください。

- ◆ SIM カバーを取り付けます。



注意事項

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

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

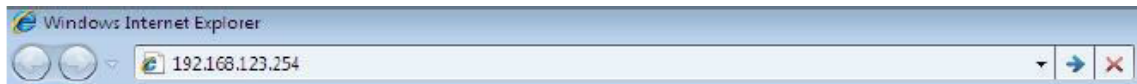
ネットワーク要件	PC にイーサネットアダプタが搭載されている
OS 要件	Windows®, Machintosh、Linux ベースの OS
Web ブラウザ要件	<ul style="list-style-type: none"> ・Internet Explorer 6.0 以降 ・Microsoft Edge ・Chrome 2.0 以降 ・Firefox 3.0 以降 ・Safari 3.0 以降

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 以外のホストアドレスに設定します。
- ◆ PC をデバイスの LAN ポートに接続します。
- ◆ ブラウザのアドレスバーに http://192.168.123.254 と入力して接続します。



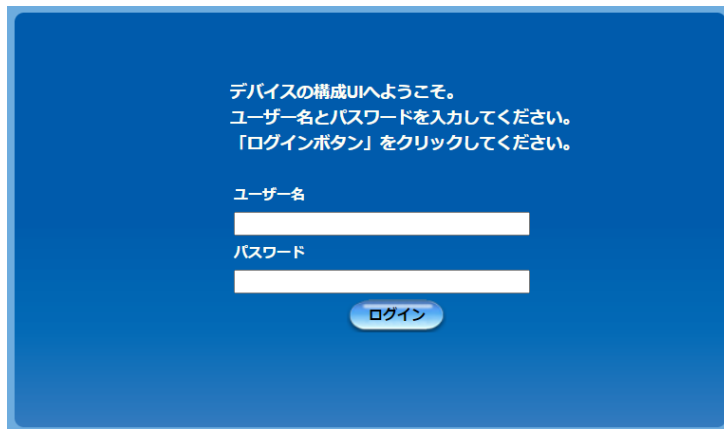
- ◆ ログイン画面が表示されますので、ユーザー名とパスワード「admin」を入力して、**ログイン** ボタンをクリックします。

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

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

(注1) ログインパスワードは 10 文字以上の設定が必要です。初期設定パスワードは使用できません。

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



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。ページ左上の**Language(言語)**を変更することで表記言語を変更できます。



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** 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。

項目	設定
▶ IPモード	静的IP
▶ LAN IPアドレス	<input type="text" value="192.168.123.254"/>
▶ サブネットマスク	<input type="text" value="255.255.255.0 (/24)"/>

- ◆ **保存** ボタンをクリックします。
- ◆ 保存後には新しい IP アドレスでログインし直す必要があります。

6.3. 管理ユーザー名の変更

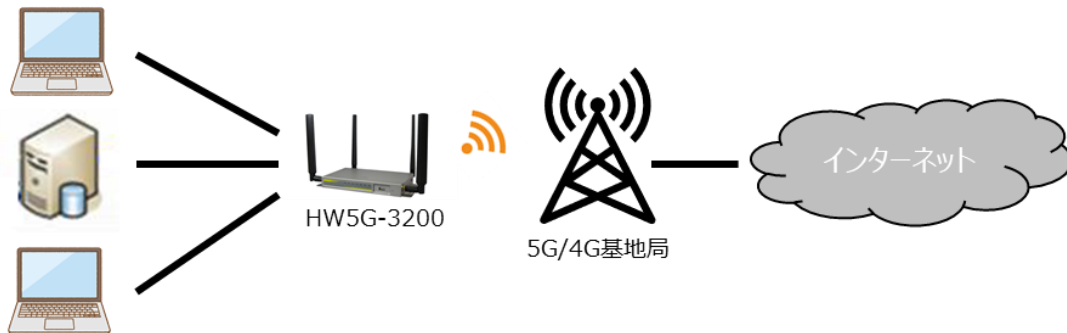
- ◆ 画面左側のメニューから、**管理(Administration)** ⇒ **システム管理** ⇒ **パスワード&MMI** の順にクリックします。
- ◆ 「ユーザー名」の **変更** ボタンを押し、管理用の新しいユーザー名と現在のパスワードを入力します。

項目	設定
▶ ユーザー名	admin 変更
▶ 新しいユーザーネーム	<input type="text"/>
▶ パスワード	<input type="password"/>

- ◆ **保存** ボタンをクリックします。
- ◆ 変更が成功するとログイン画面が表示されます。新しいユーザー名でログインしてください。

◇ 基本設定編

本章では、もっとも一般的な本機を 5G/4G/3G 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 の設定

モバイル NET 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. 物理インタフェースの設定

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** ⇒ **物理インタフェース**の順にクリックします。

物理インタフェース				ウィジェット
物理インタフェースリスト				
インタフェース名	物理インタフェース	動作モード	アクション	
WAN-1	モバイル NET	常にオン	<input type="button" value="編集"/>	
WAN-2	-	無効	<input type="button" value="編集"/>	

項目	説明
インタフェース名	インタフェース名を表示します。
物理インタフェース	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	<input type="button" value="編集"/> ボタンをクリックすると、設定変更を行うことができます。

◆ WAN-1 の編集をクリックします。

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	常にオン	編集
WAN-2	-	無効	編集

(注 1) 主回線の動作モードは「常にオン」となります。

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

◆ [保存](#)をクリックします。

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	常にオン	モバイル NET	編集
WAN-2	-	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。

3G/4G 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	<input type="checkbox"/> 有効

(注 1) スロット A に SIM が挿入されていることを確認してください。

(注 2) 自動機内モードは本機では使用できません。

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

SIM-A カードとの接続	
項目	設定
ネットワークタイプ	自動
ダイヤルアッププロファイル	手動設定
APN	xxxxx.net
IPタイプ	IPv4
PINコード	<input type="text"/> (選択的)
ダイヤルナンバー	<input type="text"/> (選択的)
アカウント	yyyyy@zzzzzzz (選択的)
パスワード	<input type="password"/> (選択的) パスワードは半角英数字を入力してください。 また大文字小文字にもご注意ください。
認証	CHAP
IPモード	動的IP
プライマリDNS	<input type="text"/> (選択的)
セカンダリDNS	<input type="text"/> (選択的)
ローミング	<input type="checkbox"/> 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。
パスワード	(ご契約に合わせて設定してください注)
認証	認証方式を選択します。(ご契約に合わせて設定してください)
IP モード	動的 IP を選択します。
プライマリ DNS	特定の DNS サーバーを使用したいときのみ設定を入力します。
セカンダリ DNS	
ローミング	本機は国内使用専用機器であるためサポートしていません。

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

◆[Cellular Connection Common Configuration{モバイル NET 共通設定}]を設定します。

Cellular Connection Common Configuration	
項目	設定
▶ 接続制御	自動再接続 ▼
▶ 時間スケジュール	(0) 常時 ▼
▶ MTU設定	<input checked="" type="checkbox"/> 有効 1430
▶ IPパススルー (セルラーブリッジ)	<input type="checkbox"/> 有効 固定MAC:
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	無効 ▼
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 10.0.0.1

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	<input checked="" type="checkbox"/> をはずし無効にします。 有効にすると、通信状況によりリポートする事象が確認されています。
IP パススルー	<input checked="" type="checkbox"/> をはずし無効にします。
NAT	<input checked="" type="checkbox"/> を入れ有効にします。
IGMP	無効を選択します。

WAN IP エイリアス	ご使用の機器ではこの機能はご使用になれません。
--------------	-------------------------

◆[ネットワークの監視構成]を設定します。

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

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

◆ ページ最後の **保存** ボタンをクリックして設定を保存してください。

◇ 応用設定編

これ以降は詳細な設定について説明します。

8. 基本ネットワーク

本ページ以降詳細な設定について説明します。

8.1. WAN およびアップリンク

本機は、二つの WAN インタフェースを搭載し、5G/4G/3G、イーサネットの中から 2 つを選択することが可能です。WAN 接続により LAN に接続された全ての PC、サーバー、スマートフォンがインターネットにアクセスできるようにします。WAN の物理インタ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、主インタフェース(WAN-1)を選択し、その後、WAN 接続のための情報の設定をします。



8.1.1. 物理インタフェースリスト

物理インタフェースリスト			
インタフェース名	物理インタフェース	動作モード	アクション
WAN-1	モバイル NET	常にオン	編集
WAN-2	-	無効	編集

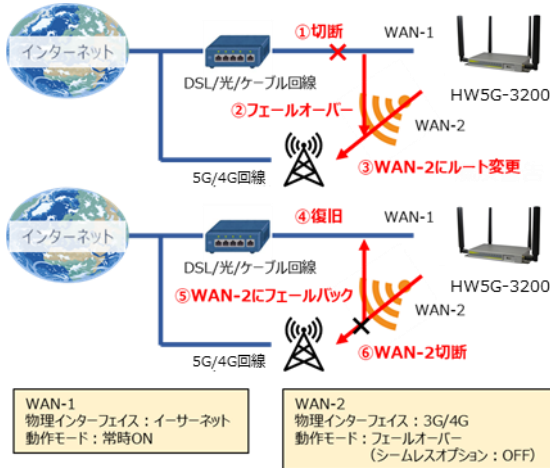
項目	説明
インタフェース名	インタフェース名を表示します。
物理インタフェース	物理インタフェースの種類を表示します。
動作モード	動作モードを表示します。
アクション	編集 ボタンをクリックすると、設定変更を行うことができます。

8.1.2. フェールオーバー機能

物理インタフェース WAN-1(主インタフェース)に回線の障害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。

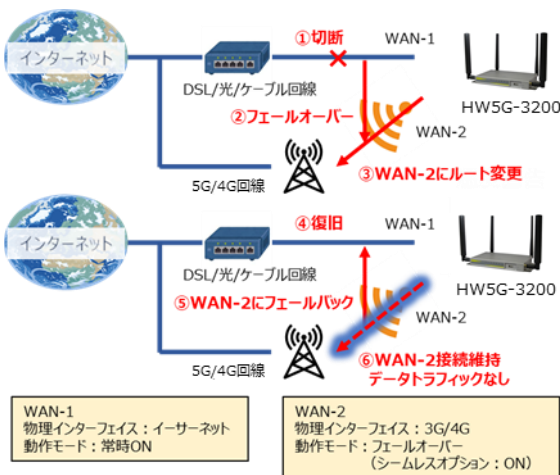
WAN-1 にイーサネットを WAN-2 にモバイル NET を割り当てたとすると、以下のような動作をします。

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

- (注1) ネットワークの監視は[接続設定]内の[ネットワーク監視構成]の設定により実行されます。切断検出時間は4秒以上となります。
- (注2) シームレスオプション OFF の場合は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. 物理インターフェースの設定

- ◆ 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**⇒**物理インターフェース**の順にクリックします。
- ◆ 物理インターフェースリスト内の WAN-1 または WAN-2 の**編集**ボタンをクリックします。

項目	設定
物理インターフェイス	モバイル NET ▼
動作モード	常にオン ▼
VLANタギング	<input type="checkbox"/> 有効 0 (1-4095)

保存

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

8.1.4. 接続設定

各々の物理インタ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 WAN-1 または WAN-2 の**編集**ボタンをクリックします。

8.1.5. WAN タイプ：モバイル NET 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

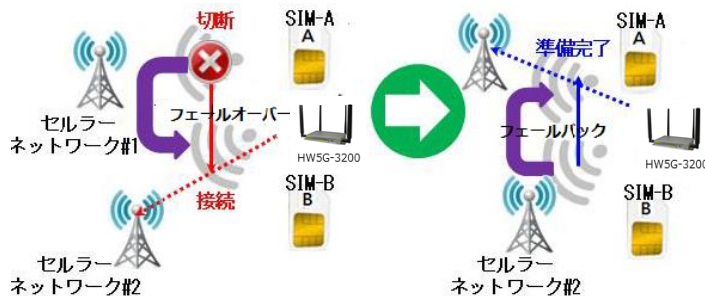
デュアル SIM フェールオーバーは 2 枚の SIM カード に対応し、モバイル NET を 2 回線使用したフェールオーバー機能を搭載しています。そのため、1 回線が不通に陥った時でも、もう 1 回線を利用し通信を継続することが可能です⁽¹⁾。また、フェールバック機能を組み合わせることにより様々な冗長性を確保することが可能となります。

1) SIM-A /SIM-B 優先あり、フェールバック無効



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

2) SIM-A /SIM-B 優先あり、フェールバック有効



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

(注 1) フェールオーバーが完了するまでには、各種設定にもよりますが最低でも 2 分以上の時間が必要です。フェールオーバーによる回線切り替え中の通信は保証されません。

(注 2) フェールバック確認中にも 1 分以上の時間が必要です。フェールバックにより優先回線に接続できる前または非優先回線に戻る前の通信は保証されません。

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

インターネット接続構成 (WAN-1)	
項目	設定
▶ WANタイプ	モバイル NET ▼

Cellular WAN Type Configuration	
項目	設定
▶ 優先SIMカード	SIM-Aのみ ▼
▶ 自動機内モード	<input type="checkbox"/> 有効

項目	説明
WAN タイプ	モバイル NET が工場出荷設定で選択されています。本設定は変更できません。
優先 SIM カード	[SIM-A は優先度が高い] 又は [SIM-B は優先度が高い]を選択 SIM カードスロットの優先順位を設定します。本設定の詳細はデュアル SIM フェールオーバー機能(7.5.1.1 項)を参照してください。 [SIM-A のみ] 又は [SIM-B のみ] を選択 選択した SIM 情報を使い接続をします。
自動機内モード	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」ボタンをクリックして設定項目画面を表示させます。

ポリシー設定	
項目	設定
▶ 接続失敗	<input type="text" value="0"/> (1-10) 回
▶ RSSI監視	<input type="checkbox"/> 有効 しきい値: - <input type="text" value="0"/> (-90~-113 dBm)
▶ ネットワーク・サービス	<input type="checkbox"/> 有効 LTE信号なし: <input type="text" value="0"/> (1~30 分)
▶ ローミング・サービス	<input type="checkbox"/> 有効 タイムアウト: <input type="text" value="0"/> (1~30 分)
保存	

項目	説明
接続失敗	モバイルNETの接続切り替えの回数を設定します。0に設定すると、切り替えが実行されません。
RSSI 監視	有効☑にすると、接続中のモバイル NET の受信レベルが設定値(-90~-113dBm)より低くなると、優先順位の高いSIM から低いSIM に転換し、接続を実行します。無効にすると、受信レベルを監視しません。
ネットワーク・サービス	有効☑にすると、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。

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	<input type="text"/>
▶ IPタイプ	IPv4 ▼
▶ PINコード	<input type="text"/> (選択的)
▶ ダイヤルナンバー	<input type="text"/> (選択的)
▶ アカウント	<input type="text"/> (選択的)
▶ パスワード	<input type="text"/> (選択的)
▶ 認証	自動 ▼
▶ IPモード	動的IP ▼
▶ プライマリDNS	<input type="text"/> (選択的)
▶ セカンダリDNS	<input type="text"/> (選択的)
▶ ローミング	<input type="checkbox"/> 有効

項目	説明
ネットワークタイプ	ネットワークタイプを[自動]固定です。
ダイアルアップ プロファイル	手動設定、自動検出から選択します。手動設定にすることを推奨しております。お使いの機器はプロファイルリストをサポートしていません。
APN	APN を入力します。(ご契約に合わせて設定します)
IP タイプ	IP タイプを選択します。(ご契約に合わせて設定します)
PIN コード(注 1)	PIN コードを入力します。(PIN コードを設定した SIM カードをお使いの場合、設定します)
ダイヤルナンバー	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、IP ゲートウェイの欄が表示されますので、ご契約に合わせて設定してください。
プライマリ DNS	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。

(※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[Cellular Connection Common Configuration]

Cellular Connection Common Configuration	
項目	設定
▶ 接続制御	自動再接続 ▼
▶ 時間スケジュール	(0) 常時 ▼
▶ MTU設定	<input checked="" type="checkbox"/> 有効 1430
▶ IPパススルー (セルラーブリッジ)	<input type="checkbox"/> 有効 固定MAC:
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	無効 ▼
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 10.0.0.1

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

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

8.1.6. WAN タイプ：イーサネットの接続設定

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

8.1.6.1. イーサネット WAN 設定

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

インターネット接続構成 (WAN - 1)	
項目	設定
WANタイプ	動的IP ▼

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

- ◆ WAN タイプを選択後、タイプ毎に必要な設定を行います。

8.1.6.2. 静的IP WAN 設定

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

静的IPWANタイプ構成	
項目	設定
▶ WAN IPアドレス	<input type="text"/>
▶ WANサブネットマスク	255.255.255.0 (/24) ▼
▶ WANゲートウェイ	<input type="text"/>
▶ プライマリDNS	<input type="text"/>
▶ セカンダリDNS	<input type="text"/> (選択的)
▶ MTU設定	<input type="checkbox"/> 有効
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	自動 ▼ IGMPプロキシ <input type="checkbox"/> 有効
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 <input type="text" value="10.0.0.1"/>

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

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

8.1.6.3. 動的IP WAN 設定

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

動的IPWANタイプ構成	
項目	設定
▶ ホスト名	<input type="text"/> (選択的)
▶ ISP登録アドレス	<input type="text"/> <input type="button" value="複製"/> (選択的)
▶ 接続制御	<input type="button" value="自動再接続"/> ▼
▶ MTU設定	<input type="checkbox"/> 有効
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	<input type="button" value="自動"/> ▼ IGMPプロキシ <input type="checkbox"/> 有効
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 <input type="text" value="10.0.0.1"/>

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

(注 1) 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示などに時間がかかることがあります。また、手動設定を選択した場合、WebGUI の[ステータス]→[基本ネットワーク]→[WAN&アップリンク]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。

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

8.1.6.4. PPPoE WAN 設定

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

項目	設定
▶ IPタイプ	IPv4 ▼
▶ PPPoEアカウント	<input type="text"/>
▶ PPPoEパスワード	<input type="text"/>
▶ プライマリDNS	<input type="text"/> (選択的)
▶ セカンダリDNS	<input type="text"/> (選択的)
▶ 接続制御	自動再接続 ▼
▶ サービス名	<input type="text"/> (選択的)
▶ 割り当てられたIPアドレス	<input type="text"/> (選択的)
▶ MTU設定	<input type="checkbox"/> 有効
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	無効 ▼
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 <input type="text" value="10.0.0.1"/>

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

(注 1) 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示などに時間がかかることがあります。また、手動設定を選択した場合、WebGUI の[ステータス]→[基本ネットワーク]→[WAN&アップリンク]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。

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

8.1.6.5. PPTP WAN 設定

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

PPTP WANタイプ構成	
項目	設定
▶ IPモード	動的IPアドレス ▼
▶ サーバー IPアドレス/名	<input type="text"/>
▶ PPTPアカウント	<input type="text"/>
▶ PPTPパスワード	<input type="text"/>
▶ 接続ID	<input type="text"/> (選択的)
▶ 接続制御	自動再接続 ▼
▶ MTU設定	<input type="checkbox"/> 有効
▶ MPPE	<input type="checkbox"/> 有効
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	無効 ▼
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 <input type="text" value="10.0.0.1"/>

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

項目	説明
	無効に設定してください。

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

(注2) IP モードで [静的 IP アドレス] を選択した時のみ表示されます。

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

8.1.6.6. L2TP WAN 設定

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

L2TP WANタイプ構成	
項目	設定
▶ IPモード	動的IPアドレス ▼
▶ サーバー IPアドレス/名	<input type="text"/>
▶ L2TPアカウント	<input type="text"/>
▶ L2TPパスワード	<input type="text"/>
▶ 接続制御	自動再接続 ▼
▶ MTU設定	<input type="checkbox"/> 有効
▶ サービスポート	ユーザー定義 ▼ <input type="text" value="1702"/>
▶ MPPE	<input type="checkbox"/> 有効
▶ NAT	<input checked="" type="checkbox"/> 有効
▶ IGMP	無効 ▼
▶ WAN IPエイリアス	<input type="checkbox"/> 有効 <input type="text" value="10.0.0.1"/>

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

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

(注 1) 接続設定でオンデマンドを選択した場合、切断状態から再接続するまで通信ができません。そのため Web ページ表示に時間がかかることがあります。また、手動設定を選択した場合、WebGUI の[ステータス]→[基本ネットワーク]→[WAN&アップリンク]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。

(注 2) IP モードで[静的 IP アドレス]を選択した時のみ表示されます。

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

8.1.7. ネットワーク監視構成の設定

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

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

保存 キャンセル

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

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

◆**保存**ボタンをクリックして設定を登録します。

8.1.7.1. 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、回線の正常性を判定しています。このターゲットホストからの応答が、モバイルネットの回線実行速度を上回るような大容量・高速データ通信を連続して行っていると、連続して大きく遅延することが起こります。その場合、ネットワーク異常と誤って判定してしまい、回線を切り替える(フェールオーバー)、または回線を復旧する目的で回線を切断します。このよう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。

8.1.8. 負荷分散

本機はモバイル NET WAN インタフェースとイーサネット WAN インタフェースの両方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。

項目	設定
負荷分散	<input checked="" type="checkbox"/> 有効
負荷分散手順	スマートウェイトによる ▼

保存 キャンセル

8.1.8.1. 負荷分散の設定

負荷分散機能の有効・無効の選択と負荷分散手順の選択をすることが可能です。

項目	設定
負荷分散	<input checked="" type="checkbox"/> 有効
負荷分散手順	スマートウェイトによる ▼

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	<p>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。</p> <ul style="list-style-type: none"> ◆スマートウェイトによる: 本機に組み込まれた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 インタフェースの指定された負荷比率(重み)に基づいて、各 WAN で転送された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ルールに基づいて利用可能な WAN インタフェースを介して、トラフィックを分散します。

- ◆ **保存** ボタンをクリックして設定を登録します。手順パラメータが必要な負荷分散手順を選択した場合は、パラメータを設定してから **保存** ボタンをクリックして設定を保存してください。

8.1.8.2. 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、各々の WAN の負荷分散比率を指定する必要があります。

ウェイト定義		
WAN ID	ウェイト	アクション
WAN - 1	55 %	<input type="button" value="編集"/>
WAN - 2	45 %	<input type="button" value="編集"/>

項目	説明
WAN ID	利用可能な WAN インタフェース名です。
ウェイト	<input type="button" value="編集"/> ボタン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。

8.1.8.3. 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。

ユーザーポリシーリスト <input type="button" value="追加"/> <input type="button" value="削除"/>						
ID	送信元IPアドレス	宛先IPアドレス	宛先ポート	WANインタフェース	有効	アクション
1	任意	任意	全部	WAN-1	<input checked="" type="checkbox"/>	<input type="button" value="編集"/> <input type="checkbox"/> 選択

◆ ボタンまたは ボタンをクリックすると[ユーザーポリシー構成]画面が表示されます。

ユーザーポリシー構成	
項目	設定
▶ 送信元IPアドレス	<input type="text" value="任意"/>
▶ 宛先IPアドレス	<input type="text" value="任意"/>
▶ 宛先ポート	<input type="text" value="全部"/>
▶ プロトコル	<input type="text" value="両方"/>
▶ WANインタフェース	<input type="text" value="WAN - 1"/>
▶ ポリシー	<input type="checkbox"/> 有効
<input type="button" value="保存"/>	

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。

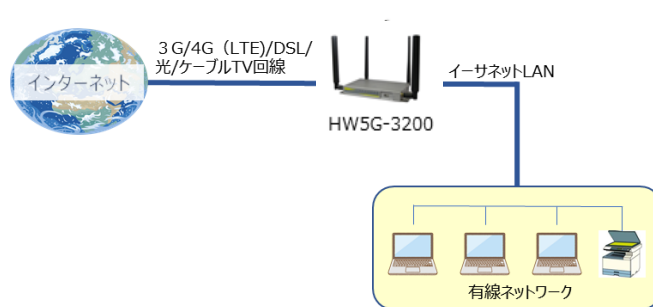
項目	説明
	<p>◆サブネット:送信元 IP アドレスのサブネットをIPv4形式/サブネットマスク(例: 192.168.123.0/24)で指定します。</p> <p>◆IP 範囲:送信元 IP アドレスをIPv4形式にて範囲で指定します。</p> <p>◆単一 IP:単一の送信元IPアドレスをIPv4形式にて指定します。</p>
宛先 IP アドレス	<p>宛先 IP アドレスを指定します。指定方法として以下の 5 つから選択することができます。</p> <p>◆任意: 特定の宛先 IP アドレスを指定しません。すべての宛先IPアドレスが対象になります。</p> <p>◆サブネット:宛先 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。</p> <p>◆IP 範囲:宛先 IP アドレスをIPv4形式にて範囲で指定します。</p> <p>◆単一 IP:単一の宛先IPアドレスをIPv4形式にて指定します。</p> <p>◆ドメイン名:宛先をドメイン名で指定します。</p>
宛先ポート	<p>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。</p> <p>◆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。</p> <p>◆ポート範囲:宛先ポートを範囲で指定します。</p> <p>◆単一ポート:単一の宛先ポートを指定します。</p> <p>◆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。</p>
プロトコル	プロトコルを[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**ボタンをクリックして、ルールを登録します。設定したルールが[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代表例です。

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

設定	
項目	設定
▶ IPモード	静的IP
▶ LAN IPアドレス	<input type="text" value="192.168.123.254"/>
▶ サブネットマスク	<input type="text" value="255.255.255.0 (/24)"/> ▼

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

◆ **保存** ボタンをクリックして設定を登録します。

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

8.2.2. 追加 IP（LAN IP エイリアス）機能

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

追加IP機能

追加

削除

ID	名称	インターフェイス	IPアドレス	サブネットマスク	有効	アクション
1	管理設定用	lo	192.168.1.1	255.255.255.0	<input checked="" type="checkbox"/>	編集 <input type="checkbox"/> 選択

追加IP構成

項目	設定
▶ 名称	<input type="text"/>
▶ インターフェイス	lo ▼
▶ IPアドレス	<input type="text"/>
▶ サブネットマスク	255.255.255.0 (/24) ▼
▶ 有効	<input type="checkbox"/>

保存

◆ **追加** ボタンをクリックすると[IP 追加構成]画面が表示されます。

◆ **保存** ボタンをクリックして設定を登録します。

項目	説明
名称	追加 IP アドレスの名称を入力します。(任意)
インタフェース	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 <input checked="" type="checkbox"/> します。

8.2.3. 仮想 LAN(VLAN)

仮想 LAN(VLAN)により、特定のスイッチまたはルーターデバイス下の論理ネットワークで、クライアントホストを特定の VLAN ID によりグループ化することができます。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。

設定	
項目	設定
VLANタイプ	ポートベース▼
システム保留されたVLAN ID	開始ID <input type="text" value="1"/> (1-4091) ~ 終了ID <input type="text" value="5"/>

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

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

8.2.4.1. ポートベース VLAN ルールの設定

ポートベースVLANリスト										追加	削除
名称	VLAN ID	VLAN タギング	NAT/ブリッジ	ポートメンバー	LAN IPアドレス	サブネットマスク	結合WAN	WAN VID	有効	アクション	
LAN	ネイティブ VLAN Tag 1	X	NAT	<input type="button" value="詳細"/>	192.168.123.254	255.255.255.0	すべての WAN	0	<input checked="" type="checkbox"/>	<input type="button" value="編集"/>	

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

ポートベースのVLAN構成	
項目	設定
▶ 名称	LAN
▶ VLAN ID	ネーティブVLAN
▶ VLANタギング	無効 ▼
▶ NAT/ブリッジ	NAT ▼
▶ ポートメンバー	ポート: <input checked="" type="checkbox"/> ポート-1 <input checked="" type="checkbox"/> ポート-2 <input checked="" type="checkbox"/> ポート-3 <input checked="" type="checkbox"/> ポート-4
▶ LAN to Join	<input type="checkbox"/> 有効 <input type="button" value="DHCP 1 ▼"/>
▶ WAN&WAN VID結合	<input type="button" value="すべてのWAN ▼"/> <input type="button" value="None"/>
▶ LAN IPアドレス	192.168.123.254
▶ サブネットマスク	255.255.255.0 (/24) ▼
▶ DHCPサーバー/リレー	サーバー ▼

項目	説明
名称	このルールの名称を表示します。初期名称が定義され、変更することはできません。
VLAN 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]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	<p>[DHCPサーバー]のタイプを定義します。</p> <p>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。</p> <ul style="list-style-type: none"> ・サーバー:VLAN グループに対して、DHCP サーバー機能を有効にします。DHCP サーバーで使用されるパラメータを指定する必要があります。 ・リレー:VLANグループのDHCPリレー機能を有効にするには、[リレー]を選択し、リレーするDHCPサーバーのアドレスを[DHCPサーバーIPアドレス]フィールドに入力します。 ・無効:VLANグループのDHCPサーバーが無効になります。
有効	<input checked="" type="checkbox"/> ボックスにチェックをして、本ルールを有効します。

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

▶ DHCPサーバー/リレー	サーバー ▼
▶ DHCPサーバー名	<input type="text"/>
▶ IPプール	開始アドレス: <input type="text" value="192.168.2.100"/> 終了アドレス: <input type="text" value="192.168.2.200"/>
▶ リース時間	<input type="text" value="86400"/> 秒
▶ ドメイン名	<input type="text"/> (選択的)
▶ プライマリーDNS	<input type="text"/> (選択的)
▶ セカンダリーDNS	<input type="text"/> (選択的)
▶ プライマリーWINS	<input type="text"/> (選択的)
▶ セカンダリーWINS	<input type="text"/> (選択的)
▶ ゲートウェイ	<input type="text"/> (選択的)
▶ 有効	<input type="checkbox"/>

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

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

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

▶ DHCPサーバー/リレー	<input type="text" value="リレー"/>
▶ DHCPサーバーIPアドレス	<input type="text"/>
▶ DHCP OPTION 82	<input type="checkbox"/>

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

- ◆ 有効項目のチェックボックスをチェックし本ルールを有効にします。
- ◆ **保存** ボタンをクリックしルールを登録します。登録されると[ポートベース VLAN ルール]にルールの内容が表示されます。

8.2.4.2. IP 固定マッピングルールの設定

MAC アドレスにより固定 IP アドレスを割り当てることができます。

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

IP 固定マッピングルールリスト 追加 削除			
MACアドレス	IPアドレス	有効	アクション
マッピングルール構成			
項目	設定		
▶ MACアドレス	<input type="text"/>		
▶ IPアドレス	<input type="text"/>		
▶ 有効	<input type="checkbox"/>		
保存			

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

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

8.2.4.3. ポートベース VLAN 間グループルーティング

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

VLANグループのインターネットアクセス定義		
VLAN IDs	メンバー	インターネットアクセス(WAN)
1	ポート : 1,2,3,4	許可 編集
VLAN間グループルーティング		
VLAN IDs	メンバー	アクション
		編集
		編集
		編集
		編集
保存		

- ◆ 各項目の **編集** ボタンをクリックしグループルーティング設定内容を編集します。

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

- ◆ **保存** ボタンをクリックしルールを登録します。

8.2.4.4. タグベース VLAN ルールの設定

タグベースの 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。

すべての LAN ポートの構成を表示するデフォルトルールがあります。本機は、最大 128 つのトラップイベントレシーバセットをサポートします。

タグベースVLANリスト

追加

削除

↑

×

VLAN ID	インタネット	ポートメンバー	ブリッジインターフェース	IPアドレス	サブネットマスク	アクション
ネイティブVLAN	<input checked="" type="checkbox"/>	ポート: <input type="checkbox"/> ポート-1 <input checked="" type="checkbox"/> ポート-2 <input checked="" type="checkbox"/> ポート-3 <input checked="" type="checkbox"/> ポート-4	DHCP 1			<div><div>編集</div><div><input type="checkbox"/> 選択</div></div>

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

◆表示される[タグベースの VLAN 構成]にルールを設定します。

タグベースのVLAN構成	
項目	設定
▶ VLAN ID	<input type="text" value="0"/>
▶ インタネットアクセス	<input checked="" type="checkbox"/> 有効
▶ ポートメンバー	ポート: <input type="checkbox"/> ポート-1 <input type="checkbox"/> ポート-2 <input type="checkbox"/> ポート-3 <input type="checkbox"/> ポート-4
▶ ブリッジインターフェース	<input type="text" value="DHCP 1"/>
保存	

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

◆**保存**ボタンをクリックしルールを登録します。登録されるとデータベース 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、工場出荷設定として本機の IP サブネットと同一であり、IP プール範囲が、「.100」から「.200」のゲートウェイの WEB UI の DHCP サーバーリストページに示されているよう、「.100」から「.200」)があらかじめ DHCP サーバーリストに登録されています。

8.2.5.1. DHCP サーバーリスト

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

The screenshot displays the 'DHCP Server List' configuration interface. At the top, there are tabs for 'DHCP Server List', 'Add', 'Delete', and 'DHCP Client List'. The main table lists the DHCP server configuration. Below this, there are sections for 'DHCP Server Options' and 'DHCP Relay Configuration', each with a table for adding, editing, or deleting entries. The 'DHCP Server Options' table has columns for ID, Option Name, DHCP Server Selection, Option Selection, Type, Value, Validity, and Action. The 'DHCP Relay Configuration' table has columns for ID, Proxy Name, LAN Interface, WAN Interface, Server IP, DHCP Relay Option 82, Validity, and Action. At the bottom, there are 'Save' and 'Cancel' buttons.

DHCPサーバー名	LAN IPアドレス	サブネットマスク	IPプール	リース時間	ドメイン名	プライマリDNS	セカンダリDNS	プライマリWINS	セカンダリWINS	ゲートウェイ	有効	アクション
DHCP 1	172.16.129.254	255.255.255.0	172.16.129.100-172.16.129.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	編集 固定マッピング

ID	オプション名	DHCPサーバー選択	オプション選択	タイプ	値	有効	アクション
----	--------	------------	---------	-----	---	----	-------

ID	代理名	LANインターフェース	WANインターフェース	サーバーIP	DHCPリレーオプション82	有効	アクション
----	-----	-------------	-------------	--------	----------------	----	-------

保存 キャンセル

- ◆ 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 PC/スマートフォンなど IP 機器に IP アドレス、サブネットマスクの割当て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** ボタンをクリックすると、DHCP サーバー構成画面が表示されます。

DHCPサーバー構成	
項目	設定
▶ DHCPサーバー名	<input type="text" value="DHCP 1"/>
▶ LAN IPアドレス	<input type="text" value="172.16.129.254"/>
▶ サブネットマスク	<input type="text" value="255.255.255.0 (/24)"/>
▶ IPプール	開始アドレス: <input type="text" value="172.16.129.100"/> 終了アドレス: <input type="text" value="172.16.129.200"/>
▶ リース時間	<input type="text" value="3600"/> 秒
▶ ドメイン名	<input type="text"/> (選択的)
▶ プライマリーDNS	<input type="text"/> (選択的)
▶ セカンダリーDNS	<input type="text"/> (選択的)
▶ プライマリWINS	<input type="text"/> (選択的)
▶ セカンダリーWINS	<input type="text"/> (選択的)
▶ ゲートウェイ	<input type="text"/> (選択的)
▶ サーバー	<input type="checkbox"/> 有効

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

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

8.2.5.3. IP 固定マッピングルールの設定

MAC アドレスにより固定 IP アドレスを割り当てることができます。

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

DHCPサーバーリスト

追加

削除

DHCPクライアントリスト

DHCPサーバー名	LAN IPアドレス	サブネットマスク	IPプール	リース時間	ドメイン名	プライマリDNS	セカンダリDNS	プライマリWINS	セカンダリWINS	ゲートウェイ	有効	アクション
DHCP 1	172.16.129.254	255.255.255.0	172.16.129.100-172.16.129.200	3600		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	<input checked="" type="checkbox"/>	<div>編集</div> <div>固定マッピング</div>

マッピングルールリスト

追加

削除

MACアドレス	IPアドレス	有効	アクション
9C:5C:8E:DB:86:F5	172.16.129.113	<input checked="" type="checkbox"/>	<div>編集</div> <div><input type="checkbox"/> 選択</div>

マッピングルール構成	
項目	設定
▶ MACアドレス	<input type="text" value="12:34:56:78:9A:BC"/>
▶ IPアドレス	<input type="text" value="172.16.129.113"/>
▶ ルール	<input checked="" type="checkbox"/> 有効
<input type="button" value="保存"/>	

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

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

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

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

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

DHCPクライアントリスト 固定マッピングにコピー					
LANインタフェース	IPアドレス	ホスト名	MACアドレス	残りのリース時間	アクション
イーサネット	動的 /172.16.129.113	HytecInter-001	16.5C.8B.DB.86.F5	00:33:43	<input type="checkbox"/> 選択

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

8.2.5.5. DHCP サーバーオプションの有効/無効

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

設定	
項目	設定
DHCPサーバーオプション	<input type="checkbox"/> 有効

項目	説明
DHCP サーバーオプション	有効にする場合に☑します。

DHCP オプション番号

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

8.2.5.6. DHCP サーバーオプションリストの追加/編集

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 追加 削除 ↑ ×							
ID	オプション名	DHCPサーバー選択	オプション選択	タイプ	値	有効	アクション

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

DHCPサーバーオプションの構成	
項目	設定
▶ オプション名	<input type="text" value="Option 1"/>
▶ DHCPサーバー選択	<input type="text" value="DHCP 1 ▼"/>
▶ オプション選択	<input type="text" value="DHCP OPTION 66 ▼"/>
▶ タイプ	<input type="text" value="単一IPアドレス ▼"/>
▶ 値	<input type="text"/>
▶ 有効	<input type="checkbox"/> 有効

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 <input checked="" type="checkbox"/> します。

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

8.2.5.7. DHCP リレー構成リストの追加/編集

本機は、最大6の DHCP リレー構成を登録できます。

DHCPリレー構成リスト 追加 削除 ↑ ×						
ID	代理名	LANインターフェース	WANインタフェース	サーバーIP	DHCPリレーオプション82	有効

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

DHCPリレー設定	
項目	設定
▶ 代理名	<input type="text"/>
▶ LANインターフェース	LAN ▼
▶ WANインタフェース	WAN - 1 ▼
▶ サーバーIP	<input type="text"/>
▶ DHCP OPTION 82	<input type="checkbox"/>
▶ 有効	<input type="checkbox"/>

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

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

8.3. IPv6

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

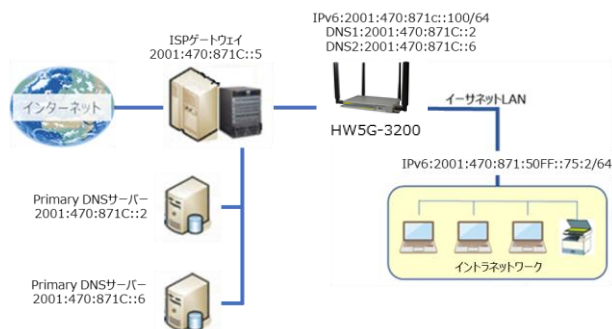
- (注 1) IPv6 を使用するためにはインターネットプロバイダ (ISP) が IPv6 に対応していなければなりません。
 (注 2) モバイル NET WAN インタフェースを使用している場合は、IPv6 を IPv4 でカプセル化します。契約回線が IPv6 に対応しているかを確認してください。

8.3.1. IPv6 接続タイプ

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

8.3.1.1. 静的 IPv6

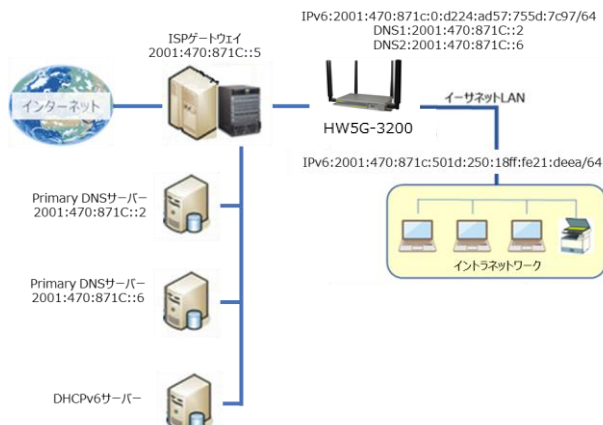
静的 IPv6 は、静的 IPv4 と同様な IP アドレッシングをします。静的 IPv6 動作には、IPv6 アドレス、IPv6 デフォルトゲートウェイアドレス、および、IPv6 DNS を手動で設定する必要があります。



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

8.3.1.2. DHCPv6

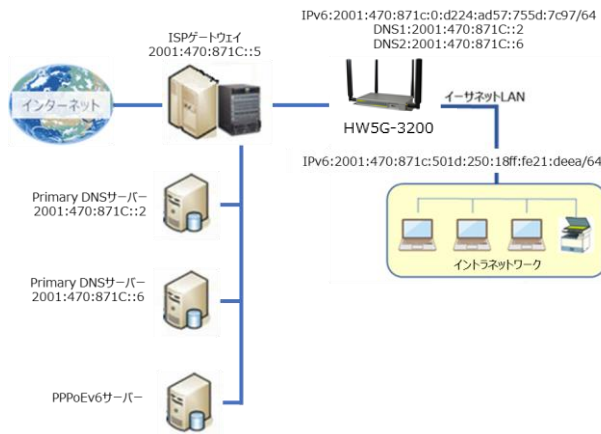
IPv6 の DHCP サーバーは、IP アドレス、DNS サーバーアドレス、および、その他の可能なデータを DHCP クライアントに送信して自動的に設定します。また、サーバーは、アドレスのリース時間と



IPv6 アドレスの更新のためにサーバーに再接続する時刻を送信します。クライアントは、IPv6 アドレスを更新する要求を再送信する必要があります。左図は、DHCPv6 IP アドレッシングを示します。ISP の DHCPv6 サーバーが、IPv6 アドレス、IPv6 デフォルトゲートウェイアドレス、および、IPv6 DNS をクライアントホストに自動的に割り当てます。

8.3.1.3. PPPoEv6

PPPoEv6 サーバーは、PPPoEv6 クライアントの要求に基づいて、構成パラメータを提供します。PPPoEv6 サーバーが、クライアントからの要求を取得し、正常に認証すると、サーバーは、IP アド



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

その他の必要なパラメータを送信し、クライアントを自動的に構成します。

8.3.2. 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。

IPv6構成	
項目	設定
▶ IPv6	<input type="checkbox"/> 有効
▶ WAN接続タイプ	IPv6 ▾

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

(注1) モバイル NETWAN インタフェースの場合はIPv6のみの選択になります。

8.3.2.1. 静的 IPv6 WAN タイプ構成

静的IPv6 WAN接続タイプ構成	
▶ IPv6アドレス	<input type="text"/>
▶ サブネットプレフィックス長	<input type="text"/>
▶ デフォルトゲートウェイ	<input type="text"/>
▶ プライマリーDNS	<input type="text"/>
▶ セカンダリーDNS	<input type="text"/>
▶ MLDスヌーピング	<input type="checkbox"/> 有効

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。

◆ 次に LAN 構成の設定を行います。

8.3.2.2. DHCPv6 WAN タイプ構成

DHCPv6WANタイプ構成	
▶ DNS	<input checked="" type="radio"/> サーバーから <input type="radio"/> 特定DNS
▶ プライマリーDNS	<input type="text"/>
▶ セカンダリーDNS	<input type="text"/>
▶ MLDスヌーピング	<input type="checkbox"/> 有効

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。

8.3.2.3. PPPoE WAN タイプ構成

PPPoEv6WAN接続タイプ構成	
▶ アカウント	<input type="text"/>
▶ パスワード	<input type="password"/>
▶ サービス名	<input type="text"/>
▶ 接続制御	自動再接続（常にオン）
▶ MTU	<input type="text"/>
▶ MLDスヌーピング	<input type="checkbox"/> 有効

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

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

◆ 次に LAN 構成に進みます。

8.3.2.4. LAN 構成

LAN構成	
▶ グローバルアドレス	<input type="text"/> /64
▶ リンクローカルアドレス	fe80::250:18ff:fe70:403

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

◆ 次にアドレス自動構成の設定に進みます。

8.3.2.5. アドレス自動構成

アドレス自動構成	
▶ 自動構成	<input checked="" type="checkbox"/> 有効
▶ 自動構成タイプ	[ステートフル▼]
▶ IPv6アドレス範囲 (開始)	XXX:: [] /64
▶ IPv6アドレス範囲 (終了)	XXX:: [] /64
▶ IPv6アドレス寿命	[] (秒)

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

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

8.4. ポート転送

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

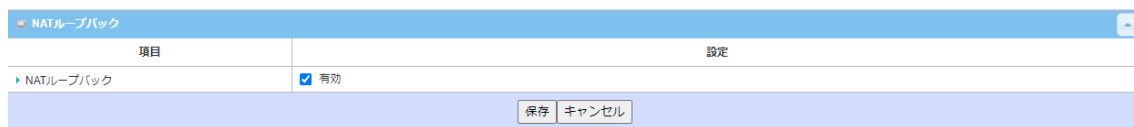
(注) NAT 機能の有効/無効は WAN ポートの接続設定内にあります。(詳細は 8.1 項 WAN およびアップリンクを参照してください。)

8.4.1. ポート転送設定

8.4.1.1. NAT ループバック

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

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



項目	設定
NATループバック	<input checked="" type="checkbox"/> 有効

保存 キャンセル

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

◆ 設定終了後に**保存**ボタンをクリックして、設定を保存します。

8.4.2. 仮想サーバー&仮想コンピュータ

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

設定

項目		設定						
▶ 仮想サーバー		<input checked="" type="checkbox"/> 有効						
▶ 仮想コンピュータ		<input checked="" type="checkbox"/> 有効						

仮想サーバーリスト

追加

削除

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

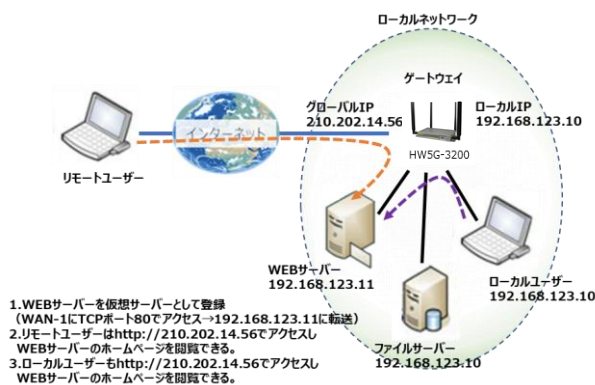
仮想コンピュータリスト

追加

削除

ID	グローバルIP		ローカルIP	有効	アクション
1	118.18.81.44		10.0.75.102	<input checked="" type="checkbox"/>	<div>編集</div> <div>選択</div>

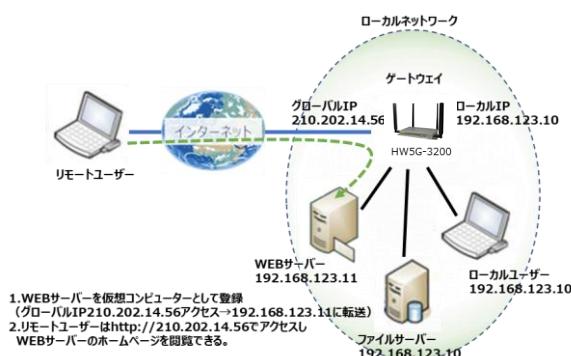
8.4.2.1. 仮想サーバー



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

8.4.2.2. 仮想コンピュータ

仮想コンピュータとは、TCP/IP プロトコルによる外部からのグローバル IP アドレスへのアクセス



を全て特定のローカルネットワーク内のサーバーなどIP機器(仮想コンピュータ)1台のみに転送する機能です。本機能は固定グローバルIPアドレス契約などの環境で使います。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。

8.4.2.3. 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。

設定	
項目	設定
▶ 仮想サーバー	<input checked="" type="checkbox"/> 有効
▶ 仮想コンピュータ	<input checked="" type="checkbox"/> 有効

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

- ◆ **保存**ボタンをクリックして、設定を保存します。

8.4.2.4. 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。

仮想サーバーリスト 追加 削除									
ID	WANインタフェース	サーバーIP	送信元IP	プロトコル	パブリックポート	プライベートポート	時間スケジュール	有効	アクション

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

仮想サーバールール設定	
項目	設定
▶ WANインタフェース	<input checked="" type="checkbox"/> 全部 <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2
▶ サーバーIP	<input type="text"/>
▶ 送信元IP	<input type="text" value="任意"/>
▶ プロトコル	<input type="text" value="TCP(6) & UDP(17)"/>
▶ パブリックポート	<input type="text" value="単一ポート"/> <input type="text"/>
▶ プライベートポート	<input type="text" value="Single Port"/> <input type="text"/>
▶ 時間スケジュール	<input type="text" value="(0) 常時"/>
▶ ルール	<input type="checkbox"/> 有効

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 または WAN-2 が選択できます。
サーバーIP	仮想サーバーのローカルネットワーク IP アドレスを指定します。
送信元IP	<p>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。</p> <p>◆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。</p> <p>◆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。</p> <p>◆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。</p>
プロトコル	<p>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。</p> <p>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。</p>
パブリックポート	<p>プロトコルで UDP、TCP および UDP&TCP を選択した時に、仮想サーバーへの転送を許可する TCP ポート(サービス)番号を指定します。</p> <p>◆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。</p> <p>◆単一ポート: 任意の TCP ポート番号一つを指定します。</p> <p>◆ポート範囲: 任意の TCP ポート番号を範囲で指定します。</p>
プライベートポート	<p>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 ポート(サービス)番号を指定します。ポート範囲を指定する場合、同じ数の範囲を指定してください。</p> <p>◆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。</p> <p>◆単一ポート: 任意の TCP ポート番号一つを指定します。</p> <p>◆ポート範囲: 任意の TCP ポート番号を範囲で指定します。</p>
時間スケジュール	<p>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。</p> <p>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。</p>
ルール	[有効]にチェックを入れると、この仮想サーバールールが有効になります。

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

8.4.2.5. 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。

仮想コンピュータリスト 追加 削除 ↑ ×				
ID	グローバルIP	ローカルIP	有効	アクション

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

仮想コンピュータルール設定		
グローバルIP	ローカルIP	有効
<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

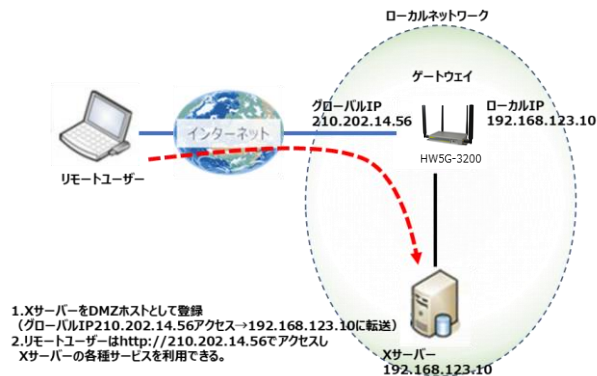
項目	説明
グローバル IP	仮想コンピュータへの転送を許可する、本機 WAN 側の IP アドレスを指定します。
ローカルIP	仮想コンピュータにローカル IP アドレスを指定します。
有効	[有効]にチェックを入れると、この仮想コンピュータルールが有効になります。

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

8.4.3. DMZ およびパススルー

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

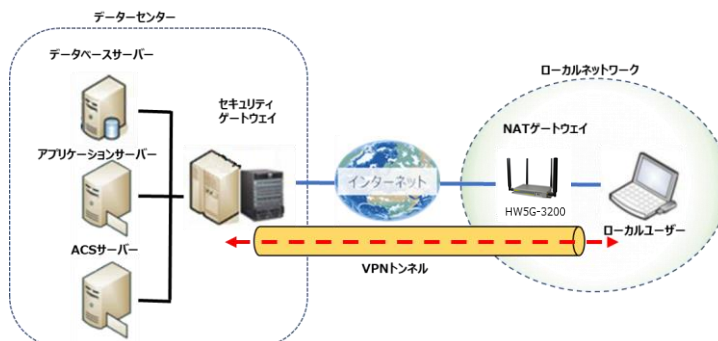
8.4.3.1. DMZ (De Militarized Zone)



X サーバーをローカルエリアネットワークに配置した場合、リモートユーザーがサーバーからのサービスを要求する場合には、このサーバーを DMZ ホストとなるように設定する必要があります。左図はリモートユーザーがグローバル IP 210.202.14.56 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。

8.4.3.2. VPN パススルー



アドレス変換機能 (NAT) が動作している場合、ローカルエリアネットワークに接続されたローカルユーザーが、直接外部のセキュアネットワークにアクセスするための VPN トネリングを構成することはできません。本機は、VPN パススルー機能

により、ローカルユーザーが任意のデータセンターなどのセキュアネットワークにアクセスできるよう設定できます。

8.4.3.3. DMZ の設定

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

設定	
項目	設定
DMZ	<input type="checkbox"/> 有効 <input checked="" type="checkbox"/> 全部 <input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 DMZホスト: <input type="text"/>
パススルーの有効化	<input checked="" type="checkbox"/> IPSec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP

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

- ◆ **保存** ボタンをクリックして、設定を登録します。

8.4.3.4. VPN パススルーの設定

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

パススルーの有効化	<input checked="" type="checkbox"/> IPSec <input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP
-----------	---

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

- ◆ **保存** ボタンをクリックして、設定を登録します。

8.5. ルーティング

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

8.5.1. 静的ルーティング

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

8.5.1.1. 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。

設定	
項目	設定
静的ルーティング	<input checked="" type="checkbox"/> 有効

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

◆ **保存** ボタンをクリックして、設定を登録します。

8.5.1.2. IPv4 静的ルーティングルールを追加/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。

IPv4 静的ルーティングルールリスト 追加 削除 ↑ ×							
ID	宛先IP	サブネットマスク	ゲートウェイIP	インターフェイス	メトリック	有効	アクション

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

IPv4 静的ルーティングルール構成	
項目	設定
▶ 宛先IP	<input type="text"/>
▶ サブネットマスク	255.255.255.0 (/24) ▼
▶ ゲートウェイIP	<input type="text"/>
▶ インターフェイス	自動 ▼
▶ メトリック	<input type="text"/>
▶ ルール	<input type="checkbox"/> 有効

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。メトリックとは経路の距離を示し 0 が最短となります。
ルール	[有効] にチェックを入れると、この静的ルーティングルールが有効になります。

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

8.5.2. 動的ルーティング

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

8.5.2.1. RIPv1/RIPv2 ルーティング

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

8.5.2.2. OSPF ルーティング

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

8.5.2.3. 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 によりルートと到達可能性の情報を交換し、ローカルネットワーク内のルーターとそのルーティング情報を共有します。

8.5.2.4. 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。

RIP構成	
項目	設定
▶ RIP	無効 ▼

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

- ◆**保存**ボタンをクリックして、設定を登録します。

8.5.2.5. 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。

OSPF構成	
項目	設定
▶ OSPF	<input type="checkbox"/> 有効
▶ ルーターID	<input type="text"/>
▶ 認証	None ▼
▶ バックボーンサブネット	<input type="text"/>

項目	説明
OSPF	[有効]ボックスにチェックすると、OSPF プロトコルが有効になります。
ルーターID	OSPF プロトコル上の本機のルーターID(本機 IP アドレス)を指定します。
認証	<p>OSPF プロトコルで使用する認証方法を選択します。</p> <p>◆None;、OSPF プロトコルの認証が無効です。</p> <p>◆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。</p> <p>◆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。</p>
バックボーンサブネット	OSPF プロトコルで使用するバックボーンサブネットを指定します。 サブネットアドレス/マスク長(10.24.0.0/16 など)形式です。

- ◆**保存**ボタンをクリックして、設定を登録します。

8.5.2.6. 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。

IPv4静的ルーティングルールリスト 追加 削除 ↑ ×							
ID	宛先IP	サブネットマスク	ゲートウェイIP	インターフェイス	メトリック	有効	アクション

◆ **追加**ボタンまたは**編集**ボタンをクリックすると[OSPF 領域構成]画面が表示されます。

OSPF領域構成 ↑ ×	
項目	設定
▶ 領域サブネット	<input type="text"/>
▶ 領域ID	<input type="text"/>
▶ 領域	<input type="checkbox"/> 有効
保存	

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

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

8.5.2.7. 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。

BGP構成 ↑ ×	
項目	設定
▶ BGP	<input type="checkbox"/> 有効
▶ ASN	<input type="text"/>
▶ ルーターID	<input type="text"/>

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 プロトコルで使用する、本機の ANS 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 사용되는 IPv4 形式のルーターID です。

8.5.2.8. 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。

BGPネットワークリスト 追加 削除			
ID	ネットワークサブネット	有効	アクション

◆ **追加** ボタンまたは **編集** ボタンをクリックすると[BGP ネットワーク構成]画面が表示されます。

BGPネットワーク構成	
項目	設定
▶ ネットワークサブネット	IP : <input type="text"/> 255.255.255.0 (/24) ▼
▶ ネットワーク	<input type="checkbox"/> 有効
保存	

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

8.5.2.9. 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。

近隣IPリスト 追加 削除				
ID	近隣IP	リモートASN	有効	アクション

◆ **追加** ボタンまたは **編集** ボタンをクリックすると[BGP 近隣構成]画面が表示されます。

BGP近隣構成	
項目	設定
▶ 近隣IP	<input type="text"/>
▶ リモートASN	<input type="text"/>
▶ 近隣	<input type="checkbox"/> 有効
保存	

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

8.5.3. ルーティング情報

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

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

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

8. 6. DNS & DDNS

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

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

8.6.1. 動的 DNS の設定

項目	設定
▶ DDNS	<input type="checkbox"/> 有効
▶ WANインタフェース	WAN-1 ▼
▶ プロバイダ	No-IP.com ▼
▶ ホスト名	<input type="text"/>
▶ ユーザー名/E-Mail	<input type="text"/>
▶ パスワード/キー	<input type="text"/>

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/ TZO.com / DynamicDO!.jp(Free)/ DynamicDO!.jp(Charge) (注1) サービスは内容により有償/無償があります。詳細は各 DDNS サービス プロバイダのホームページで確認してください。 (注2) TZO.com はサービスを停止しているため、ご利用頂けません。
ホスト名	DDNSサービスプロバイダに登録した動的DNSのホスト名(63文字以下)を指定します。
ユーザー名/E-Mail	DDNSサービスのユーザー名またはEメールアドレスを指定します。
パスワード/キー	DDNSサービスのパスワードまたはキーを指定します。

◆ **保存** ボタンをクリックして設定を保存します。

8.6.2. DNS リダイレクトの設定

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

DNSリダイレクト	
項目	設定
DNSリダイレクト	<input type="checkbox"/> 有効

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。このルールに従い、本機は特定のデータトラフィックを特定のホストにリダイレクトすることができます。

8.6.3. リダイレクトルールの定義

リダイレクトルール 追加 削除					
ID	マッピングルール	条件	説明	有効	アクション

◆**追加**ボタンをクリックすると、[リダイレクトルール]画面が表示されます。

リダイレクトルール 保存					
項目	設定				
マッピングルール	<table border="1"> <thead> <tr> <th>ドメイン名</th> <th>IP</th> </tr> </thead> <tbody> <tr> <td><input type="text"/> (*は任意)</td> <td><input type="text"/></td> </tr> </tbody> </table>	ドメイン名	IP	<input type="text"/> (*は任意)	<input type="text"/>
ドメイン名	IP				
<input type="text"/> (*は任意)	<input type="text"/>				
条件	常時 ▼				
説明	<input type="text"/>				
有効	<input type="checkbox"/> 有効				

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

8.7. QoS

本機は、ネットワークサービス品質を維持するために、柔軟な QoS ルールを搭載しています。QoS ルールでは帯域幅、接続セッション、優先度付きキュー、DSCP(DiffServ Code Point)の4種類の情報をもとに、データ送受信の制御を行います。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。

8.7.1. 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。

設定	
項目	設定
▶ QoSタイプ	ソフトウェア ▾ <input type="checkbox"/> 有効
▶ フレキシブル帯域幅管理	<input type="checkbox"/> 有効

項目	説明
QoS タイプ	<p>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。</p> <p>◆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。</p> <p>◆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管理の制御条件のみが有効になります。</p>
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**ボタンをクリックして設定を保存します。

8.7.2. システムリソース設定（ソフトウェア QoS）

システムリソース構成	
項目	設定
▶ システムキューのタイプ	帯域幅キュー ▾ 6 (1~6)
▶ WANインタフェース	WAN - 1 ▾

WANインタフェースリソース	
項目	設定
▶ アップストリーム帯域幅	150 Mbps ▾
▶ ダウンストリーム帯域幅	150 Mbps ▾
▶ 総接続セッション数	30000 (1~100000)

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 インターフェイス	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応されます。

8.7.3. 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。

8.7.4. 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。

QoSルールリスト									
	追加	削除	消去	再起動					
インターフェイス	グループ	サービス	リソース	制御機能	方向	制御対象	時間スケジュール	有効	アクション

◆ **追加** ボタンまたは **編集** ボタンをクリックすると [QoS ルール構成] 画面が表示されます。

QoSルール構成	
項目	設定
▶ インターフェイス	すべてのWAN ▼
▶ グループ	送信元MACアドレス ▼ <input type="text"/>
▶ サービス	全部 ▼
▶ リソース	帯域幅 ▼
▶ 制御機能	最小レートおよび最大レート設定 ▼ <input type="text"/> --- <input type="text"/> Mbps ▼
▶ QoS方向	送信 ▼
▶ 時間スケジュール	(0) 常時 ▼
▶ ルール 有効	<input type="checkbox"/> 有効

保存 キャンセル

項目	説明
インターフェイス	QoSルールを適応するWANインタフェースを[すべてのWAN]、[WAN-1]および[WAN-2]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]または[IP]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。
サービス	<p>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。</p> <ul style="list-style-type: none"> ◆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ルールを適応させます。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。

項目	説明
リソース/制御機能	<p>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を以下となります。</p> <p>◆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。</p> <p>◆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。</p> <p>◆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。</p> <p>◆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。</p>
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、8.1.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**ボタンをクリックして、ルールを登録します。設定したルールが[QoSルールリスト]に表示されます。

8.8. 冗長機能

本機は、VRRP(Virtual Router Redundancy Protocol)を搭載しており、コアルーター(マスタールーター)またはL2スイッチで障害が発生した場合、自動的に冗長ルーターとしてコアルーターの代わりに機能することができます。

(注1) 本機能は WAN 回線切断でのルーター切り替えには対応していません。

8.8.1. VRRP 設定

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

設定	
項目	設定
▶ VRRP	<input type="checkbox"/> 有効
▶ 仮想サーバーID	<input type="text"/> (1-255)
▶ 仮想サーバーの優先度	<input type="text"/> (最小 1 ~ 254最大)
▶ 仮想サーバーIPアドレス	<input type="text"/>

項目	説明
VRRP	[有効]にチェックを入れると、VRRP機能が有効になります。
仮想サーバーID	本機のVRRP仮想サーバーIDを指定します。値の範囲は1～255です。
仮想サーバー優先度	本機の VRRP 仮想サーバー優先度を指定します。 値の範囲は 1～254 で、254 が最優先となります。
仮想サーバー IP アドレス	本機のVRRP仮想サーバーIPアドレスを指定します。

◆ **保存**ボタンをクリックして設定を保存します。

9. オブジェクト定義



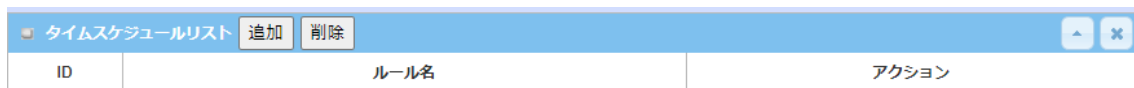
9.1. スケジューリング

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

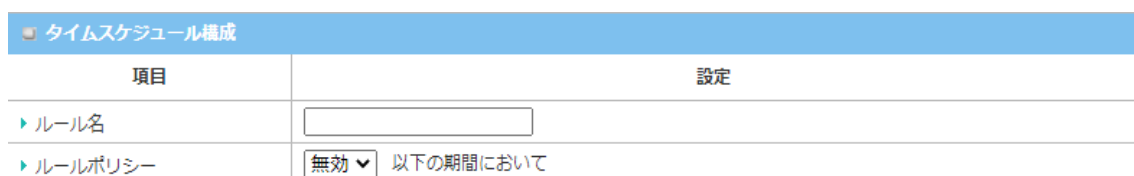
◆ 画面左側のメニューから、**オブジェクト定義**⇒**スケジューリング**⇒**設定**の順にクリックします。



9.1.1.1. タイムスケジュールリストの追加/編集



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



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

9.1.1.2. 期間定義の設定

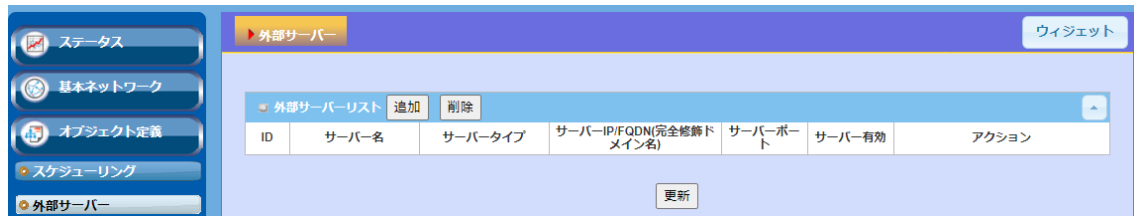
期間定義			
ID	曜日	開始時間 (hh:mm)	終了時間 (hh:mm)
1	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
2	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
3	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
4	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
5	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
6	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
7	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>
8	- 一つを選択する - ▼	<input type="text"/>	<input type="text"/>

項目	説明
曜日	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。
終了時間	選択した曜日の終了時間を指定します。

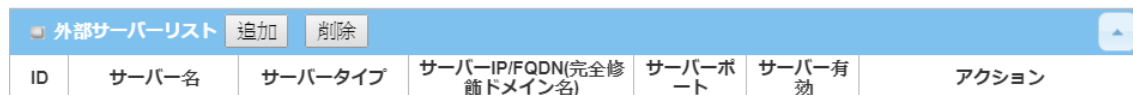
9.2. 外部サーバー

いくつかの外部サーバーを定義することができます。

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



9.2.1.1. 外部サーバーリストの追加/編集



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

項目	説明
サーバー名	ルールを識別するためのサーバー名を指定します。
サーバータイプ	<p>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。</p> <p>◆Eメールサーバー: 追加設定項目あり</p> <p> ユーザー名: 文字列形式: 任意のテキスト</p> <p> パスワード: 文字列形式: 任意のテキスト</p> <p>◆Syslogサーバー: 追加設定項目なし</p>

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

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

9.3. 証明書

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

9.3.1. ローカル証明書

9.3.1.1. ローカル証明書の作成

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

ローカル証明書リスト 追加 追加 削除						
ID	名称	サブジェクト	発行	効力	アクション	

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

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

ローカル証明書設定	
項目	設定
名称	<input type="text"/> 自己署名: <input type="checkbox"/>
キー	キータイプ: RSA ▼ キー長さ: 1024-bits ▼ ダイジェストアルゴリズム: SHA-1 ▼
サブジェクト名	国 (C) : <input type="text"/> 州 (ST) : <input type="text"/> 場所 (L) : <input type="text"/> 組織 (O) : <input type="text"/> 組織単位 (OU) : <input type="text"/> 共通名 (CN) : <input type="text"/> Eメール: <input type="text"/>
追加属性	パスフレーズ: <input type="text"/> 非公式名: <input type="text"/>
SCEP登録	有効: <input type="checkbox"/> SCEPサーバー: --- オプション --- ▼ 追加 CA証明書: <input type="text"/> CA登録証明書: --- オプション --- ▼ (選択的) CA識別子: <input type="text"/> (選択的)

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

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

9.3.1.2. 証明書のインポート

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

The screenshot shows a software interface for importing certificates. It consists of two main sections. The top section, titled 'Import', has buttons for '追加' (Add), '適用' (Apply), and 'キャンセル' (Cancel). Below this is a 'ファイルの選択' (File Selection) button and a message 'ファイルが選択されていません' (File is not selected). The bottom section, titled 'PEMエンコード' (PEM Encode), has buttons for '適用' (Apply) and 'キャンセル' (Cancel). Below this is a large, empty rectangular text area for pasting text.

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

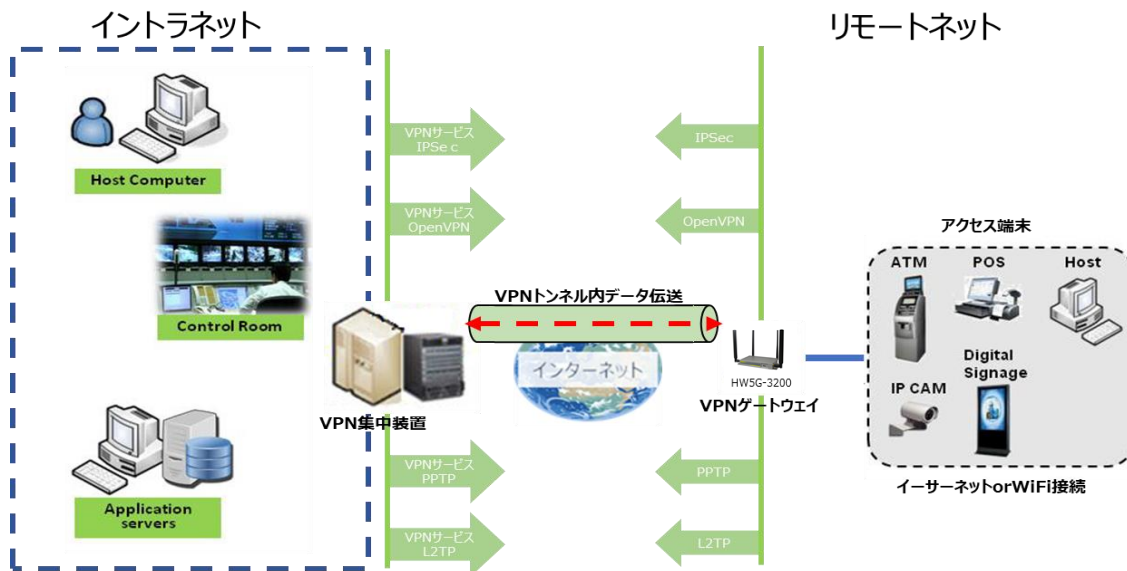
9.3.2. 信頼できる証明書

本機能はサポートしていません。

10. セキュリティ

10.1. VPN

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



10.1.1. IPSec

インターネットプロトコルセキュリティ(IPSec)は、通信セッションの各 IP パケットを認証および暗号化することにより、インターネットプロトコル(IP)通信を保護するためのプロトコルです。

IPSecVPNトンネルはIPSec クライアント(イニシエーター)とサーバー(レスポnder)の間に確立されます。本機は、IPSec クライアントとしてもサーバーとしても動作できるのでさまざまなリモートデバイスとのトンネル確立できます。

10.1.1.1. IPSec の設定

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

項目	設定
IPSec	<input type="checkbox"/> 有効
最大同時IPSecトンネル	16

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、16です。

◆ **保存**ボタンをクリックして、設定を登録します。

10.1.1.2. IPSecトンネルの追加/編集

IPSec Tunnel List 追加 削除 更新							
ID	トンネル名	インターフェイス	リモートゲートウェイ	リモートサブネット	ステータス	有効	アクション

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

10.1.1.3. トンネル設定

項目	設定
トンネル	<input type="checkbox"/> 有効
トンネル名	IPSec #1
インターフェイス	WAN-1
トンネルシナリオ	Site-to-Site(Tunnel mode)
トンネルTCP MSS	Auto 0 (64~1500 Bytes)
ICMP Keep alive	<input type="checkbox"/> 有効 Max. fail times 3 Interval 30 (secs.) Source Addr. Destination Addr.
カプセル化プロトコル	ESP
IKEバージョン	v1

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。
インタフェース	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。
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、Tunnel TCPMSSのサイズを定義します。 自動: すべてのデバイスがこのパラメーターを自動的に調整します。 手動: Tunnel TCPMSSの期待される値を指定します。値の範囲は64～1500バイトです。
ICMP Keep alive	[有効]にチェックを入れると、ICMP Keep aliveが有効になります。 キープアライブ機能が有効になっている場合: 失敗試行の数、チェック間隔、ICMPパケットの送信元/宛先IPアドレスを指定する必要があります。 値の範囲: 失敗した試行と時間間隔は1～999。
カプセル化プロトコル	カプセル化プロトコルを「ESP」または「AH」から選択します。
IKE バージョン	IKEバージョンを「v1」または「v2」から選択します。 (注)カプセル化プロトコルに「AH」が選択されている場合、IKEバージョンは無効になります。

10.1.1.4. ローカル & リモート設定

ローカル&リモート 設定															
項目	設定														
ローカルサブネットリスト	<table border="1"> <thead> <tr> <th>ID</th> <th>サブネット IP アドレス</th> <th>サブネットマスク</th> <th>アクション</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text" value="172.16.129.0"/></td> <td><input type="text" value="255.255.255.0(24)"/></td> <td><input type="button" value="削除"/></td> </tr> <tr> <td colspan="4"><input type="button" value="追加"/></td> </tr> </tbody> </table>	ID	サブネット IP アドレス	サブネットマスク	アクション	1	<input type="text" value="172.16.129.0"/>	<input type="text" value="255.255.255.0(24)"/>	<input type="button" value="削除"/>	<input type="button" value="追加"/>					
ID	サブネット IP アドレス	サブネットマスク	アクション												
1	<input type="text" value="172.16.129.0"/>	<input type="text" value="255.255.255.0(24)"/>	<input type="button" value="削除"/>												
<input type="button" value="追加"/>															
リモートサブネットリスト	<table border="1"> <thead> <tr> <th>ID</th> <th>サブネット IP アドレス</th> <th>サブネットマスク</th> <th>アクション</th> </tr> </thead> <tbody> <tr> <td>1</td> <td><input type="text"/></td> <td><input type="text" value="255.255.255.0(24)"/></td> <td><input type="button" value="削除"/></td> </tr> <tr> <td colspan="4"><input type="button" value="追加"/></td> </tr> </tbody> </table>	ID	サブネット IP アドレス	サブネットマスク	アクション	1	<input type="text"/>	<input type="text" value="255.255.255.0(24)"/>	<input type="button" value="削除"/>	<input type="button" value="追加"/>					
ID	サブネット IP アドレス	サブネットマスク	アクション												
1	<input type="text"/>	<input type="text" value="255.255.255.0(24)"/>	<input type="button" value="削除"/>												
<input type="button" value="追加"/>															
リモートゲートウェイ	<input type="text"/> (IPアドレス/FQDN(完全修飾ドメイン名))														

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

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

10.1.1.5. 認証設定

認証	
項目	設定
キー管理	IKE+プリシェアキー (最小2文字)
ローカルID	タイプ: ユーザー名 ID: (選択的)
リモートID	タイプ: ユーザー名 ID:

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

IKEフェーズ	
項目	設定
ネゴシエーションモード	メインモード
X-Auth	なし X-Authアカウント (選択的) ユーザー名: パスワード:
デッドピア検出 (DPD)	<input checked="" type="checkbox"/> 有効 タイムアウト: 180 (秒) 遅延: 30 (秒)
フェーズ1キークライフタイム	14400 (秒) (最大: 86400)

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

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

10.1.1.7. IKE プロポーザル定義

IKEプロポーザル定義				
ID	暗号化	認証	DHグループ	定義
1	AES-128 ▼	SHA1 ▼	グループ2 ▼	<input checked="" type="checkbox"/> 有効
2	AES-128 ▼	MD5 ▼	グループ2 ▼	<input checked="" type="checkbox"/> 有効
3	DES ▼	SHA1 ▼	グループ2 ▼	<input checked="" type="checkbox"/> 有効
4	3DES ▼	SHA1 ▼	グループ2 ▼	<input checked="" type="checkbox"/> 有効

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

IPSecフェーズ	
項目	設定
フェーズ2キーライフタイム	28800 (秒) (最大: 86400)

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秒以内に指定します。

10.1.1.9. IPSec プロポーザル定義

IPSecプロポーザル定義				
ID	暗号化	認証	PFSGroup	定義
1	AES-128 ▼	SHA1 ▼	グループ2 ▼	<input checked="" type="checkbox"/> 有効
2	AES-128 ▼	MD5 ▼		<input checked="" type="checkbox"/> 有効
3	DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> 有効
4	3DES ▼	SHA1 ▼		<input checked="" type="checkbox"/> 有効

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

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

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

10.1.2. OpenVPN

OpenVPN は、事前共有キーまたは証明書を使って、お互いに認証したトンネルを構築します。また、サーバー&クライアント形式のトンネル技術です。加えて、OpenVPN は「TAP:レイヤ3レベル」と「TUN:レイヤ2レベル」の2つのトンネル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	設定
▶ OpenVPN	<input checked="" type="checkbox"/> 有効
▶ クライアント	クライアント▼
▶ OpenVPN設定ファイル	<input type="checkbox"/> 有効 アップグレード

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

◆ **保存**ボタンをクリックして、設定を登録します。

10.1.2.2. OpenVPN クライアントリストの追加/編集

OpenVPNクライアントリスト													
ID	クライアント名	インターフェイス	プロトコル	ポート	トンネルシナリオ	リモートIP/FQDN(完全修飾ドメイン名)	リモートサブネット	リダイレクトインターネットトラフィック	NAT	認証モード	暗号化方法	ハッシュ・アルゴリズム	有効

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

項目	設定
OpenVPNクライアント名	OpenVPN Client #1
インターフェイス	WAN-1
プロトコル	TCP ポート: 4430
トンネルシナリオ	TUN
リモートIP/FQDN(完全修飾ドメイン名)	
リモートサブネット	<input type="checkbox"/> 有効 255.255.255.0(24)
リダイレクトインターネットトラフィック	<input type="checkbox"/> 有効
NAT	<input checked="" type="checkbox"/> 有効
認証モード	TLS CA証明書: クライアント証明書: クライアントキー: 証明書を設定してください。
暗号化方法	Blowfish
ハッシュ・アルゴリズム	SHA-1
LZO 圧縮	適応
Persistキー	<input checked="" type="checkbox"/> 有効
Persistトンネル	<input checked="" type="checkbox"/> 有効
詳細構成	編集
トンネル	<input type="checkbox"/> 有効

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。
インタフェース	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443自動設定)を使用します。 ◆UDP: OpenVPNはUDPプロトコル(ポート番号1194自動設定)を使用します。
トンネルシナリオ	OpenVPNが使用するトンネルシナリオを「TUN」または「TAP」から選択します。
リモート IP/FQDN	OpenVPNサーバーのIPアドレスまたはFQDNを指定します。
リモートサブネット	OpenVPAサーバーのサブネットとサブネットマスクを指定します。
リダイレクトインターネットトラフィック	[有効]にチェックを入れると、リダイレクトインターネットトラフィック機能が有効になります。
NAT	[有効]にチェックを入れると、NAT機能が有効になります。
認証モード	認証モードを「TLS」または「静的キー」から選択します。 ◆TLS: OpenVPNはTLS認証モードを使用し、CA証明書、クライアント証明書を使用します。 ◆静的キー: OpenVPNは静的キー認証モードを使用し、ローカルエンド

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

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

10.1.2.3. OpenVPN クライアント詳細構成

OpenVPNクライアント詳細構成	
項目	設定
▶ TLS Cipher	なし ▼
▶ TLS Auth. キー (選択的)	<input type="text"/> (選択的)
▶ ユーザー名 (選択的)	<input type="text"/> (選択的)
▶ パスワード (選択的)	<input type="text"/> (選択的)
▶ TAPのブリッジ先	VLAN 1 ▼
▶ ファイアウォール保護	<input type="checkbox"/> 有効
▶ クライアント IPアドレス	動的 IP ▼
▶ トンネルMTU	1500
▶ トンネルのUDP断片	1500
▶ トンネルのUDPMSS-Fix	<input type="checkbox"/> 有効
▶ nsCertType検証	<input type="checkbox"/> 有効

▶ TLS再ネゴシエーション時間(秒)	3600 (秒)
▶ 接続再試行(秒)	-1 (秒)
▶ DNS	自動的 ▼
▶ 追加構成	<div></div>

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

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

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

10.1.3. L2TP

Layer 2 トンネリングプロトコル(L2TP)は、仮想プライベートネットワーク(VPN)をサポートするため、または ISP によるサービスの提供の一部として使用されるトンネリングプロトコルです。それ自体は暗号化や機密性を提供しません。むしろ、プライバシーを提供するためにトンネル内を通過する暗号化プロトコルに依存しています。

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	設定
L2TP	<input type="checkbox"/> 有効
クライアント/サーバー	サーバー ▼

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**ボタンをクリックして、設定を登録します。

10.1.3.2. L2TP サーバーの設定

項目	設定
L2TPサーバー	<input type="checkbox"/> 有効
インターフェイス	すべてのWAN ▼
L2TP over IPsec	<input type="checkbox"/> 有効 プリシェアキー <input type="text"/> (最小2文字)
サーバー仮想IP	<input type="text"/> 192.168.10.1
IPプール開始アドレス	<input type="text"/> 10
IPプール終了アドレス	<input type="text"/> 17
認証プロトコル	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE暗号化	<input type="checkbox"/> 有効 40 bits ▼
サービスポート	<input type="text"/> 1701

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。
インタフェース	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のプレ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ローカルエリア仮想IPアドレスを指定します。

項目	説明
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。 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-CHAR v2」から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、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。
サービスポート	L2TPトネリングのサービスポートを以下から選択し、必要があればサービスポートを指定します。 <ul style="list-style-type: none"> ◆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 サーバステータス

接続されている L2TP クライアントの情報が表示されます。表示される情報は、[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]があります。必要に応じてリスト上の[切断]ボタンをクリックして、L2TP トネリングを切断することができます。

L2TP サーバステータス 更新				
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	アクション
リモートからの接続なし				

10.1.3.4. ユーザーアカウントの追加・編集

L2TP サーバ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。

ユーザーアカウントリスト 追加 削除				
ID	ユーザー名	パスワード	有効	アクション

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

ユーザーアカウント設定		
ユーザー名	パスワード	アカウント
<input type="text"/>	<input type="text"/>	<input type="checkbox"/> 有効
保存		

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]ボックスをチェックすると、本アカウントが有効になります。

◆[保存]ボタンをクリックして、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

L2TPクライアント構成	
項目	設定
L2TPクライアント	<input type="checkbox"/> 有効

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

◆ **保存** ボタンをクリックして、設定を登録します。

10.1.3.6. L2TP クライアントリストの追加/編集

L2TPクライアントリスト&ステータス								
ID	トンネル名	インターフェイス	バーチャルIP	リモートIP/FQDN(完全修飾ドメイン名)	リモートサブネット	ステータス	有効	アクション

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

L2TPクライアント構成	
項目	設定
トンネル名	L2TP #1
インターフェイス	WAN1 ▼
L2TP over IPsec	<input type="checkbox"/> 有効 プリシェアキー <input type="text"/> (Min.8ビット)
リモートLNSIP/FQDN(完全修飾ドメイン名)	<input type="text"/>
MTU	1500
リモートLNSポート	1701
ユーザー名	<input type="text"/>
パスワード	<input type="text"/>
トンネルパスワード(選択的)	<input type="text"/>
リモートサブネット	<input type="text"/>
認証プロトコル	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE暗号化	<input type="checkbox"/> 有効
NAT before Tunneling	<input type="checkbox"/> 有効
LCPエコータイプ	自動 間隔 <input type="text"/> 30 秒 最大故障回数 <input type="text"/> 6 回
サービスポート	自動 ▼ <input type="text"/> 0
トンネル	<input type="checkbox"/> 有効

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。
インタフェース	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。
L2TP over IPsec	[有効]にチェックを入れると、L2TP over IPsecモード(IPsecによる暗号化)を有効にします。有効にした場合は文字長8～32のプレシェアキーを指定します。

項目	説明
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-CHAR v2」から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、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]ボックスをチェックすると、本ルールが有効になります。

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

10.1.4. PPTP

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

10.1.4.1. PPTP の設定

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

項目	設定
▶ PPTP	<input type="checkbox"/> 有効
▶ クライアント/サーバー	サーバー ▼

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	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。

◆ 保存ボタンをクリックして、設定を登録します。

10.1.4.2. PPTP サーバーの設定

項目	設定
▶ PPTPサーバー	<input type="checkbox"/> 有効
▶ インターフェイス	すべてのWAN ▼
▶ サーバー仮想IP	192.168.0.1
▶ IPプール開始アドレス	10
▶ IPプール終了アドレス	17
▶ 認証プロトコル	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
▶ MPPE暗号化	<input type="checkbox"/> 有効 40 bits ▼

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。
インタフェース	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ローカルエリア仮想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。

項目	説明
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-CHAR v2」から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、PPTP 接続用のMPPE (Microsoft Point-to-Point Encryption)セキュリティが有効になります。L2TPサーバーが対応していると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。

10.1.4.3. PPTP サーバーステータス

接続されているPPTPクライアントの情報が表示されます。表示される情報は、[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]があります。必要に応じてリスト上の切断ボタンをクリックして、PPTP トネリングを切断することができます。

PPTPサーバーステータス 更新				
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	アクション
リモートからの接続なし				

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。

ユーザーアカウントリスト 追加 削除				
ID	ユーザー名	パスワード	有効	アクション

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

ユーザーアカウント設定		
ユーザー名	パスワード	アカウント
<input type="text"/>	<input type="password"/>	<input type="checkbox"/> 有効
保存		

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]ボックスをチェックすると、本アカウントが有効になります。

◆保存ボタンをクリックして、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

PPTPクライアント構成	
項目	設定
PPTPクライアント	<input type="checkbox"/> 有効

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

◆ 保存ボタンをクリックして、設定を登録します。

10.1.4.6. PPTP クライアントリストの追加/編集

PPTPクライアントリスト & ステータス								
ID	トンネル名	インターフェイス	バーチャルIP	リモート IP/FQDN(完全修飾ドメイン名)	リモートサブネット	ステータス	有効	アクション

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

PPTPクライアント構成	
項目	設定
トンネル名	PPTP #1
インターフェイス	WAN1 ▼
リモートIP/FQDN(完全修飾ドメイン名)	
MTU	1500
ユーザー名	
パスワード	
リモートサブネット	
認証プロトコル	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> MS-CHAP <input type="checkbox"/> MS-CHAP v2
MPPE暗号化	<input type="checkbox"/> 有効
NAT before Tunneling	<input type="checkbox"/> 有効
LCPエコータイプ	自動 ▼
	間隔 30 秒 最大故障回数 6 回
トンネル	<input type="checkbox"/> 有効

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。
インタフェース	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。
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。

項目	説明
リモートサブネット	リモートサブネットをIPアドレス/ネットマスク(例: 192.168.123.100/24)のフォーマットで指定します。0.0.0.0/0を指定するとL2TPトンネルがデフォルトゲートウェイとして扱われ、全てのパケットはPPTPトンネルを通過するようになります。
認証プロトコル	PPTP接続に使用する認証プロトコルを「PAP」、「CHAP」、「MS-CHAP」および「MS-CHAR v2」から指定します。複数の認証プロトコルを指定することができます。
MPPE 暗号化	[有効]にチェックをすると、PPTP接続用のMPPE (Microsoft Point-to-Point Encryption) セキュリティが有効になります。L2TPサーバーが対応しているときのみ有効にしてください。MPPE暗号化が有効の場合、認証プロトコル PAP/CHAPは使用できません。
NAT before Tunneling	[有効]にチェックをすると、PPTPトンネルを通過する前にNAT機能によるアドレス変換が有効になります。
LCP エコータイプ	PPTPトンネルのLCPエコータイプを以下から選択します。 ◆自動: 自動的に間隔および最大故障回数を指定します ◆ユーザー定義: 間隔(1~99,999秒)および最大故障回数(1~999回)の範囲で指定します。 ◆無効: LCPエコーは無効です。
トンネル	[有効]ボックスをチェックすると、本ルールが有効になります。

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

10.1.5. GRE

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

10.1.5.1. GRE の設定

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

設定	
項目	設定
GREトンネル	<input type="checkbox"/> 有効
最大同時GREトンネル	32

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

GREトンネルリスト 追加 削除										
ID	トンネル名	インターフェイス	トンネルIP	リモートIP	MTU	キー	TTL	リモートサブネット	有効	アクション

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

GREルール構成	
項目	設定
トンネル名	GRE #1
インターフェイス	WAN1 ▼
トンネルIP	IP: <input type="text"/> マスク: <input type="text"/> (選択的)
リモートIP	<input type="text"/>
MTU	<input type="text"/>
キー	<input type="text"/> (選択的)
TTL	<input type="text"/>
リモートサブネット	<input type="text"/>
トンネル	<input type="checkbox"/> 有効

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。
インタフェース	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。

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

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

10.2. ファイヤーウォール

ファイ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、コンテンツフィルタ、MAC 制御、アプリケーションフィルタ、IPS、およびいくつかのファイアウォールオプションが含まれます。

10.2.1. パケットフィルタ

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

◆ 画面左側のメニューから、**セキュリティ⇒ファイヤーウォール⇒パケットフィルタ**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	設定
パケットフィルタ	<input type="checkbox"/> 有効
ブラックリスト/ホワイトリスト	規則に一致するものを拒否する ▼
ログアラート	<input type="checkbox"/> ログアラート

項目	説明
パケットフィルタ	[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]ボックスにチェックを入れると、イベントログが有効になります。

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

10.2.1.2. パケットフィルタールの追加/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。

パケットフィルタ											追加	削除	↑	×
ID	ルール名	入力 インター フェース	出力 インター フェース	送信元IP	宛先IP	送信元MAC	プロ トコ ル	送信元ポート	宛先ポート	時間 スケジ ュール	有効	ア クシ ョ ン		

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

パケットフィルタ規則構成	
項目	設定
▶ ルール名	Rule1
▶ 入力インターフェース	任意 ▼
▶ 出力インターフェース	任意 ▼
▶ 送信元IP	任意 ▼
▶ 宛先IP	任意 ▼
▶ Source MAC	任意 ▼
▶ プロトコル	任意(0) ▼
▶ 送信元ポート	ユーザー定義サービス ▼ <input type="text"/> - <input type="text"/>
▶ 宛先ポート	ユーザー定義サービス ▼ <input type="text"/> - <input type="text"/>
▶ 時間スケジュール	(0) 常時 ▼
▶ ルール	<input type="checkbox"/> 有効

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

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

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

10.2.2. URL ブロッキング

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

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



10.2.2.1. URL ブロッキング設定

項目	設定
URL ブロッキング	<input checked="" type="checkbox"/> 有効
ブラックリスト/ホワイトリスト	規則に一致するものを拒否する ▼
ログアラート	<input type="checkbox"/> 有効

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

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

10.2.2.2. URL ブロッキングルールの追加/編集

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

URLブロッキングルールリスト 追加 削除 ↑ ×							
ID	ルール名	送信元IP	送信元MAC	URL/ドメイン名/キーワード	宛先ポート	時間スケジュール	有効 アクション

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

URLブロッキングルール構成	
項目	設定
▶ ルール名	<input type="text" value="Rule1"/>
▶ 送信元IP	<input type="text" value="任意"/>
▶ Source MAC	<input type="text" value="任意"/>
▶ URL/ドメイン名/キーワード	<input type="text"/>
▶ 宛先ポート	<input type="text" value="任意"/>
▶ スケジュール	<input type="text" value="(0) 常時"/>
▶ ルール	<input type="checkbox"/> 有効

保存 キャンセル

項目	説明
ルール名	識別のためのURLブロッキングルール名(30文字以内)を指定します。
送信元 IP アドレス	<p>Web 要求を送信する IP アドレスを指定します。</p> <p>◆任意: 全ての送信元 IP アドレスがフィルタされます。</p> <p>◆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。</p> <p>◆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。</p>
Source MAC	<p>送信元の MAC アドレスを指定します。</p> <p>◆任意: 全ての送信元 MAC アドレスがフィルタされます。</p> <p>◆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。</p>
URL/ドメイン名/ キーワード	<p>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。</p> <p>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。</p>
宛先ポート	<p>宛先サービスポート番号を指定します。</p> <p>◆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。</p> <p>◆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。</p> <p>◆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。</p>

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

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

10.2.3. MAC 制御

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

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



10.2.3.1. MAC 制御設定

項目	設定
MAC制御	<input checked="" type="checkbox"/> 有効
ブラックリスト/ホワイトリスト	登録されたMACアドレスを拒否 ▼
ログアラート	<input checked="" type="checkbox"/> 有効
LAN PCリストからの既知のMAC	172.16.129.113(WTech-PC01) ▼ コピー先

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

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

10.2.3.2. MAC 制御ルールリストの追加/編集

MAC 制御ルールを登録します。ルールは 20 ルールまで登録できます。

MAC制御ルールリスト 追加 削除 ↑ ×					
ID	ルール名	MACアドレス	スケジュール	有効	アクション
1	私のPC	11:22:33:44:55:66	(0) 常時	<input checked="" type="checkbox"/>	編集 <input type="checkbox"/> 選択

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

MAC制御ルールの設定			
ルール名	MACアドレス (使用: 作成する)	時間スケジュール	有効
<input type="text" value="Rule2"/>	<input type="text" value="9C-5C-8E-DB-86-F5"/>	<input type="text" value="(0) 常時"/>	<input checked="" type="checkbox"/>
保存			

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

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

10.2.4. IPS

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

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



10.2.4.1. IPS 設定



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

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

10.2.4.2. 侵入防止機能設定

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

侵入防止機能	
項目	設定
▶ SYNフラッド防御	<input type="checkbox"/> 有効 <input type="text" value="300"/> パケット/秒 (10~10000)
▶ UDPフラッド防御	<input type="checkbox"/> 有効 <input type="text" value="300"/> パケット/秒 (10~10000)
▶ ICMPフラッド防御	<input type="checkbox"/> 有効 <input type="text" value="300"/> パケット/秒 (10~10000)
▶ ポートスキャン防御	<input type="checkbox"/> 有効 <input type="text" value="200"/> パケット/秒 (10~10000)
▶ Land Attackのブロック	<input type="checkbox"/> 有効
▶ Ping of Deathのブロック	<input type="checkbox"/> 有効
▶ IP Spoofのブロック	<input type="checkbox"/> 有効
▶ TCP Flag Scanのブロック	<input type="checkbox"/> 有効
▶ Smurfのブロック	<input type="checkbox"/> 有効
▶ Tracerouteのブロック	<input type="checkbox"/> 有効
▶ Fraggle Attackのブロック	<input type="checkbox"/> 有効
▶ ARPスプーフィング防御	<input type="checkbox"/> 有効 <input type="text" value="300"/> パケット/秒 (10~10000)

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

◆ **保存** ボタンをクリックして設定を保存します。

10.2.5. オプション

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

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



10.2.5.1. ファイアウォールオプション設定

ファイアウォールオプション	
項目	設定
ステルスモード	<input type="checkbox"/> 有効
SPI	<input checked="" type="checkbox"/> 有効
WANからのPing/パケットを破棄する	<input type="checkbox"/> 有効

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

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

10.2.5.2. リモート管理者ホスト定義の編集

WAN から本機にアクセスできる管理者ホストを 5 つ設定できます。

- ◆ **編集** ボタンをクリックすると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。

リモート管理者ホスト定義							
ID	インターフェイス	プロトコル	IP	サブネットマスク	サービスポート	有効	アクション
1	All WAN ▼	HTTP ▼	任意のIPアドレス ▼		80	<input checked="" type="checkbox"/>	編集
2	All WAN	HTTPS	任意のIPアドレス	N/A	443	<input type="checkbox"/>	編集
3	All WAN	HTTPS	任意のIPアドレス	N/A	443	<input type="checkbox"/>	編集
4	All WAN	HTTPS	任意のIPアドレス	N/A	443	<input type="checkbox"/>	編集
5	All WAN	HTTPS	任意のIPアドレス	N/A	443	<input type="checkbox"/>	編集

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

- ◆ **保存** ボタンをクリックして設定を保存します。

11. 管理(Administration)

11.1. 設定と管理（本機ではサポートしていません）

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

11.1.1. コマンドスクリプト

この機能はサポートしていません。

11.1.2. TR-069

この機能はサポートしていません。

11.1.3. SNMP

この機能はサポートしていません。

11.1.4. Telnet & SSH

この機能はサポートしていません。

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

ホスト名	
項目	設定
ホスト名	<input type="text"/>

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

11.2.1.2. ユーザ名の変更

ユーザー名	
項目	設定
ユーザー名	admin 変更

項目	説明
ユーザー名 (注 1)	変更 ボタン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 ボタンで新しいユーザー名の変更登録をします。

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

11.2.1.3. パスワードの変更

パスワード	
項目	設定
旧/パスワード	<input type="password"/>
新/パスワード	<input type="password"/>
新/パスワード確認	<input type="password"/>

項目	説明
旧パスワード	現在のパスワードを入力します。

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

11.2.1.4. MMI(マネージメントインタフェース)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	設定
ログイン	誤ったパスワードをチェック&試行回数: <input type="text" value="3"/> (回)
ログインタイムアウト	<input checked="" type="checkbox"/> 有効 <input type="text" value="300"/> (秒)
GUIアクセスプロトコル	<input type="text" value="http/https"/> ▼
HTTPS証明書のセットアップ	<input checked="" type="radio"/> デフォルト <input type="radio"/> 証明書リストから選択 証明書: <input type="text"/> キー: <input type="text"/>
HTTP圧縮	<input type="checkbox"/> gzip <input type="checkbox"/> deflate
HTTPバインディング	<input checked="" type="checkbox"/> DHCP 1
システム起動モード	<input type="text" value="通常起動モード"/> ▼

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

11.2.2. システム情報

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

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

システム情報	
項目	設定
▶ モデル名	HW5G3200-V2
▶ デバイスのシリアル番号	ZZ21100052
▶ カーネルバージョン	2.6.36
▶ ファームウェアバージョン	0HI06S0.L41_a41.0HI0_05271800
▶ システムタイム	Sun, 18 Apr 2021 18:56:56 +0900
▶ デバイス稼働時間	0day 0hr 36min 25sec

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

- 2) **更新** ボタンのクリックでシステムタイムが更新されます。

11.2.3. システムタイム

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]および[セルラーモジュール]から選択することができます。

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

11.2.3.1. タイムサーバーと同期する

項目	設定
同期方法	タイムサーバー ▼
タイムゾーン	* タイムゾーンオフセットマニュアル設定... ▼ GMT +8
オートシンクロ	タイムサーバー: <input type="text"/> 利用可能なタイムサーバー (RFC-868): 自動 ▼
夏時間	<input type="checkbox"/> 有効
NTPサーバーサービス	<input type="checkbox"/> 有効
即時同期	アクティブ

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

11.2.3.2. 手動でシステム時間を設定する

システムタイム構成	
項目	設定
▶ 同期方法	マニュアル ▼
▶ タイムゾーン	* タイムゾーンオフセットマニュアル設定... GMT +8
▶ 夏時間	<input type="checkbox"/> 有効
▶ 日付と時刻を手動で設定する	2019 ▼ / 3 ▼ / 28 ▼ (年/月/日) 15 ▼ : 07 ▼ : 52 ▼ (時:分:秒)
▶ NTPサーバーサービス	<input type="checkbox"/> 有効

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

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

11.2.3.3. PC と手動で同期をとる

WebUI で本機にアクセス中の PC と同期をとります。

システムタイム構成	
項目	設定
同期方法	PC
NTPサーバーサービス	<input type="checkbox"/> 有効
即時同期	アクティブ

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

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

11.2.3.4. モバイル NET 無線回線の時刻通知を利用して同期をとる

モバイル NET 回線から時刻データを取得し同期することができます。

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

システムタイム構成	
項目	設定
同期方法	セルラーモジュール
タイムゾーン	タイムゾーンオフセットマニュアル設定... GMT +9
NTPサーバーサービス	<input type="checkbox"/> 有効
即時同期	アクティブ

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

11.2.4. システムログ

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

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

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

11.2.4.1. 表示および E メールログ履歴

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

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

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

Web ログリスト例

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)(csm 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	<input checked="" type="checkbox"/> システム <input checked="" type="checkbox"/> 攻撃 <input checked="" type="checkbox"/> ドロップ <input checked="" type="checkbox"/> ログインメッセージ <input type="checkbox"/> 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。

11.2.4.4. Syslogd

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

Syslogd	<input type="checkbox"/> 有効	サーバー: --- オプション --- 追加
	ログタイプカテゴリ: <input type="checkbox"/> システム <input type="checkbox"/> 攻撃 <input type="checkbox"/> ドロップ <input type="checkbox"/> ログインメッセージ <input type="checkbox"/> デバッグ	

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

11.2.4.5. ログの保管

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

ストレージでログの保管	<input type="checkbox"/> 有効
	選択デバイス: 内部
	ログファイル名: syslog
	分割ファイル: <input type="checkbox"/> 有効 ファイルサイズ: 200 KB
	間隔: <input type="checkbox"/> 有効 1440 (1 ~ 10080 Minutes)
	Max Records: 3000 (5~10000)
ログファイルをダウンロードする clear logs	
ログタイプカテゴリ: <input type="checkbox"/> システム <input type="checkbox"/> 攻撃 <input type="checkbox"/> ドロップ <input type="checkbox"/> ログインメッセージ <input type="checkbox"/> デバッグ	

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

項目	説明
ログタイプカテゴリ	ログタイプカテゴリ項を参照してください。

11.2.5. バックアップ及び復元

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

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

項目	設定
▶ FWアップグレード	Web UI経由 ▼ FWアップグレード
▶ バックアップ設定	ダウンロード ▼ Web UI経由
▶ オートリストア設定	<input type="checkbox"/> 有効 保存Conf. クリアConf. Conf.情報
▶ ユーザー定義ロゴ	ダウンロード ▼ Web UI経由 設定リセット
▶ ユーザー定義CSS	編集 : ダウンロード ▼ Web UI経由 設定リセット

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	
ユーザー定義 CSS	

- 2) **保存**ボタンをクリックして設定を登録します。

11.2.6. 再起動およびリセット

本機を再起動したり、設定を工場出荷設定にリセットしたりすることができます。

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

システム管理	
項目	設定
▶ 再起動	今すぐ ▼ <input type="button" value="再起動"/>
▶ デフォルト設定に戻す	<input type="button" value="設定リセット"/>

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

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

11.3. 診断

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



11.3.1. パケットアナライザ

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

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

11.3.1.1. 設定

項目	設定
パケットアナライザ	<input type="checkbox"/> 有効
ファイル名	<input type="text"/>
ファイル分割	<input type="checkbox"/> 有効 ファイルサイズ: <input type="text" value="200"/> KB ▼
パケットインターフェイス	<input type="checkbox"/> WAN-1 <input type="checkbox"/> WAN-2 <input type="checkbox"/> WiFi-1 <input type="checkbox"/> VAP-1 <input type="checkbox"/> VAP-2

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

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

11.3.1.2. キャプチャとフィルタの条件

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

項目	設定
Filter	<input type="checkbox"/> 有効
ソースMAC	<input type="text"/>
ソースIP	<input type="text"/>
ソースポート	<input type="text"/>
宛先MAC	<input type="text"/>
宛先IP	<input type="text"/>
宛先ポート	<input type="text"/>

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

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

11.3.2. 診断ツール

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

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

項目	設定
▶ Pingテスト結果	ホストIP: <input type="text"/> 外部インタフェース: 自動 LANソース: デフォルト Ping
▶ Tracertテスト結果	ホストIP: <input type="text"/> インターフェイス: 自動 UDP Tracert
▶ Wake on LAN	<input type="text"/> 起動

項目	説明
Ping テスト結果	<p>ホスト IP に宛先を入力し、Ping ボタンをクリックすることで、Ping テストを行うことができます。</p> <p>テスト結果は画面下部に下図のように表示されます。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Ping結果</p> <pre> Pingでテストしたログ: PING 192.168.123.29 (192.168.123.29): 56 data bytes 64 bytes from 192.168.123.29: icmp_seq=0 ttl=128 time=2.9 ms 64 bytes from 192.168.123.29: icmp_seq=1 ttl=128 time=0.9 ms 64 bytes from 192.168.123.29: icmp_seq=2 ttl=128 time=0.7 ms 64 bytes from 192.168.123.29: icmp_seq=3 ttl=128 time=1.4 ms --- 192.168.123.29 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.7/1.4/2.9 ms </pre> </div>
Tracert テスト結果	<p>ホスト IP に宛先を入力し、Tracert ボタンをクリックすることで、トレースルートテストを行うことができます。</p> <p>テスト結果は画面下部に下図のように表示されます。</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">トレースルート結果</p> <pre> トレースルートでテストしたログ: 1 192.168.123.29 (192.168.123.29) 2.676 ms 1.522 ms 1.229 ms </pre> </div>
Wake on LAN	この機能はサポートしていません。

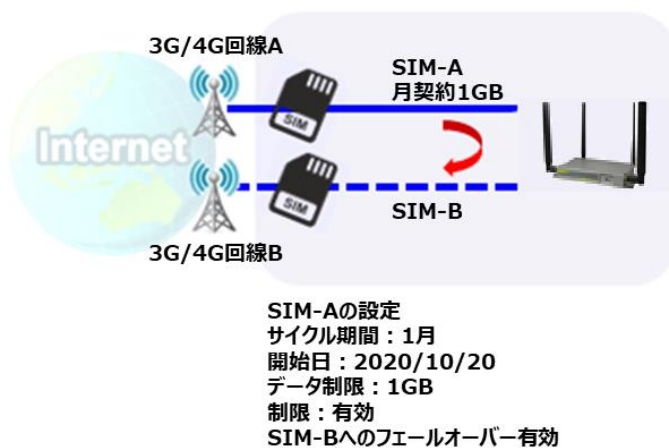
12. サービス

12.1. セルラーツールキット

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



12.1.1. データ使用量（データ使用量の制限）



モバイル NET のデータプランでは、データ使用量が制限されている契約があります。この場合、データ使用量が制限を超えると、スループットの低下、請求金額が増えるなどが発生します。本機ではデータ使用量機能により、データ使用量を監視し、接続を切断したり SIM-B へ切り替えをしたりを自動的に行うことができます。データ容量制限による

SIM 切り替え機能を使用する場合は、SIM-B へのフェールオーバー機能が有効でなければなりません。

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

3G/4Gデータ使用量プロファイルリスト								
ID	SIM情報	キャリアー名	サイクル期間	開始日	データ制限	接続制限	有効	アクション

(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ィールリストの追加/編集

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

- ◆ **追加**または**編集**ボタンをクリックすると、モバイル NET データ使用量プロフィール設定画面が表示されます。

モバイル NET データ使用量プロフィール設定	
項目	設定
▶ SIM選択	モバイル NET ▼ SIM A ▼
▶ キャリアー名	<input type="text"/>
▶ サイクル期間	日単位 ▼ <input type="text"/>
▶ 開始日	2021 ▼ / 5 ▼ / 28 ▼
▶ データ制限	<input type="text"/> KB ▼
▶ 接続制限	<input type="checkbox"/> 有効
▶ 制限有効化	<input checked="" type="checkbox"/> 有効
保存	

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。 本機のインターフェースはモバイル NET 固定です。
キャリア名	プロフィー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、プロフィールが有効になります。

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

12.1.2. SMS

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

(注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	設定
物理インターフェイス	Cellular-1 ▼
SMS	<input checked="" type="checkbox"/> 有効 SIMステータス: SIM_A
SMSストレージ	SIMカードのみ ▼
SMS容量	<input type="checkbox"/> 有効 & 利用可能な容量を保持する (1-10)

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

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

12.1.2.2. SMS 要約(サマリー)

SMS の受信および送信の状況を表示します。

項目	設定
未読のSMS	0
受信済SMS	24
SMSを送信しました。	0
残りSMS	15

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

12.1.2.3. 新規 SMS

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

項目	設定
▶ 受取人	<input type="text"/> (国際フォーマットには '+'を使用し、複数の受信機には ';'を使用します)
▶ テキストメッセージ	<div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> 入力の長さ: 0
▶ 結果	

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

12.1.2.4. SMS 受信トレイ

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

SMS受信トレイリスト 更新 削除 閉じる 前 1 次 次				
ID	電話番号から	タイムスタンプ	SMS テキストプレビュー	アクション
1	0901-1111-1111	2021/01/07 08:33:30	I wish	詳細 <input type="checkbox"/> Reply フォワード

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

12.1.2.5. SMS 送信フォルダ

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

SMS送信フォルダ 削除 閉じる 前 1 次に				
ID	受取人	タイムスタンプ	SMS テキストプレビュー	アクション
1	090 1111 1111 1111	2020/01/01 10:22:04	連絡ください。	詳細 <input type="checkbox"/>

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

12.1.3. SIM PIN

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サービスプロバイダーが各加入者を識別するための情報が入力されており、不正アクセスを防ぐために SIM カードで PIN コードを有効にすることは、簡単で効果的な方法です。本機では WebGUI を介して SIM カードの PIN コードを有効化および管理できます。

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

12.1.3.1. SIM カードの選択 (Configuration)

PIN コードを書き換える SIM カードを選択します。

項目	説明
物理インタフェース	「Cellular-1[モバイル NET-1]」固定です。
SIM ステータス	<p>選択した SIM カードと SIM カードのステータスを示します。</p> <p>ステータスは、Ready, Not Insert, or SIM PIN と表示されます。</p> <p>◆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。</p> <p>◆Not Insert: その SIM スロットに SIM カードが挿入されていません。</p> <p>◆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。</p>
SIM 選択	<p>SIM PIN を設定する SIM カードを「SIM-A」または「SIM-B」から選択します。</p> <p>切り替え ボタンを押すと、SIM カードをもう一つカードに切り替えます。その後、SIM カードを設定できます。</p>

12.1.3.2. PUK 機能

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

項目	設定
▶ PUKステータス	ロックされていません
▶ 残り回数	10
▶ PUKコード	<input type="text"/> (8桁)
▶ 新しいPINコード	<input type="text"/> (4~8桁)

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

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

12.1.3.3. SIM 機能 (PIN コードの設定)

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

項目	設定
▶ PINロック	<input type="checkbox"/> 有効 PINコード: <input type="text"/> (4~8桁)
▶ 残り回数	3

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

◆**PIN コード変更**ボタンをクリックすると、以下の画面が表示されます。

Item	Setting
▶ Current PIN Code	<input type="text"/> (4~8 digits)
▶ New PIN Code	<input type="text"/> (4~8 digits)
▶ Verified New PIN Code	<input type="text"/> (4~8 digits)

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

12.1.4. 通信スキャン

本機能はサポートしていません。

12.2. SMS & イベント

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



12.2.1. マネージングイベント

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

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

12.2.2. 通知イベント

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

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

12.2.3. 設定

- ◆ 画面左側のメニューから、**サービス**⇒**SMS&イベント**⇒**設定**の順にクリックします。
- ◆ 各項目の設定が完了したら、**保存**ボタンをクリックして、設定を保存します。

12.2.3.1. イベントマネージメントの設定

設定	
項目	設定
イベントマネージメント	<input type="checkbox"/> 有効

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

12.2.3.2. SMS コンフィグレーションの設定

SMSコンフィグレーション	
Item	Setting
メッセージ接頭辞	<input type="checkbox"/> 有効
物理インターフェイス	Cellular-1 SIMステータス: SIM_A
処理後の管理対象SMSの削除	<input type="checkbox"/> 有効

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。
物理インタフェース	本機では Cellular-1[モバイル NET-1]固定です。対象となる SIM Slot が表示されます。
処理後の管理対象 SMS の削除	[有効]にチェックを入れると、受信したマネージングイベント SMS を処理した後に削除します。

12.2.3.3. SMS アカウントリスト追加/編集

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

SMSアカウントリスト						
追加		削除				
ID	電話番号	電話説明	アプリケーション	確認済みのSMSを送信する	有効	アクション

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

SMSアカウント構成	
項目	設定
▶ 電話番号	特定番号 ▼ <input type="text"/>
▶ 電話説明	<input type="text"/>
▶ アプリケーション	<input type="checkbox"/> イベント設定トリガー <input type="checkbox"/> イベント通知ハンドル
▶ 確認済みのSMSを送信する	<input type="checkbox"/> 有効
▶ 有効	<input checked="" type="checkbox"/> 有効
保存	

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

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

12.2.3.4. Email サービスリストの追加/編集

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

ID	Eメールサーバー	Emailアドレス	有効	アクション
----	----------	-----------	----	-------

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

項目	設定
Eメールサーバー	--- Option --- ▼
Emailアドレス	<input type="text"/>
有効	<input checked="" type="checkbox"/> 有効

保存

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

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

12.2.3.5. リモートホストリストの追加/編集

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

リモートホストリスト							
		追加	削除				
ID	ホスト名	ホストIP	プロトコルタイプ	ポート番号	プレフィックスメッセージ	サフィックスメッセージ	有効
アクション							

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

リモートホスト設定	
項目	設定
▶ ホスト名	<input type="text"/>
▶ ホストIP	<input type="text"/>
▶ プロトコルタイプ	TCP ▼
▶ ポート番号	<input type="text"/>
▶ プレフィックスメッセージ	<input type="text"/>
▶ サフィックスメッセージ	<input type="text"/>
▶ 有効	<input type="checkbox"/>
保存	

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

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

12.2.4. マネージングイベント

- ◆ 画面左側のメニューから、**サービス**⇒**SMS & イベント**⇒**マネージングイベント**の順にクリックします。
- ◆ 設定、マネージングリストの追加が終了したら、**保存**ボタンをクリックして設定を登録します。

12.2.4.1. マネージングイベントの設定

設定	
項目	設定
▶ マネージングイベント	<input type="checkbox"/> 有効

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

12.2.4.2. マネージングリストの追加/編集

<div> <div>マネージングリスト</div> <div>追加</div> <div>削除</div> </div> <div> <div>↑</div> <div>×</div> </div>						
ID	イベント名	イベント	トリガタイプ	説明	有効	アクション
1	ネットワークステータス	SNMP Trap なし なし	期間	ネットワークステータス	<input checked="" type="checkbox"/>	<div>編集</div> <div>選択</div>

◆ **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。

マネージングコンフィグレーション	
項目	設定
イベント名	<input type="text"/>
イベント	<div>なし ▼</div> <div>and なし ▼</div> <div>and なし ▼</div>
トリガタイプ	期間 ▼
間隔	<input type="text" value="0"/> (0~86400 秒)
説明	<input type="text"/>
アクション	<input type="checkbox"/> Network Status <input type="checkbox"/> WAN <input type="checkbox"/> LAN&VLAN <input type="checkbox"/> WiFi <input type="checkbox"/> NAT <input type="checkbox"/> ファイヤーウォール <input type="checkbox"/> VPN <input type="checkbox"/> GRE <input type="checkbox"/> System Manage <input type="checkbox"/> 管理 (Administration) <input type="checkbox"/> リモートホスト
管理イベント	<input checked="" type="checkbox"/> 有効

保存

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	<p>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。</p> <p>SMS: テキストボックスに SMS メッセージを指定します。</p> <p>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。</p>
トリガタイプ	<p>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。</p> <p>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。</p> <p>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。</p>
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	<p>ネットワークステータス、または定義したイベントが発生したときに実行する少なくとも 1 つの休止アクションを指定します。</p> <p>ネットワークステータス: ネットワークステータスを取得します。</p> <p>WAN: WAN の接続/切断、モバイル NET のモード設定を変更します。</p> <p>LAN & VLAN: LAN1/WAN、LAN2 ポートリンクのオン/オフ設定を変更します。</p> <p>NAT: 仮想サーバールールのオン/オフ、DMZ オン/オフ設定を変更します。</p> <p>ファイアウォール: リモート管理者ホスト ID のオン/オフ設定を変更します。</p> <p>VPN: IPSec トンネルのオン/オフ、PPTP クライアントのオン/オフ、L2TP クライアントのオン/オフ、OpenVPN クライアントのオン/オフ設定を変更します。</p> <p>GRE: GRE トンネルのオン/オフ設定を変更します。</p> <p>システム管理: 本機ではサポートしていません。</p> <p>管理: バックアップ構成、復元構成、再起動、現在の設定をデフォルトとして保存設定を変更します。</p> <p>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。</p>
管理イベント	[有効]にチェックを入れると、このマネージングイベントが有効になります。

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

12.2.5. 通知イベント

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

12.2.5.1. 通知イベントの設定

設定	
項目	設定
通知イベント	<input type="checkbox"/> 有効

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

12.2.5.2. 通知イベントリストの追加/編集

通知イベントルールは最大 128 ルールが登録できます。

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

通知イベント設定	
項目	設定
イベント名	<input type="text"/>
イベント	<div>なし ▼</div> <div>and なし ▼</div> <div>and なし ▼</div>
トリガタイプ	期間 ▼
間隔	<input type="text" value="0"/> (0~86400 秒)
説明	<input type="text"/>
Delay to send	<input type="text"/> (0~3600 秒)
アクション	<input type="checkbox"/> SMS <input type="checkbox"/> Syslog <input type="checkbox"/> SNMPトラップ (v1及びv2cのみをサポートします) <input type="checkbox"/> Eメールアラート <input type="checkbox"/> リモートホスト <input type="checkbox"/> System
時間スケジュール	(0) 常時 ▼
通知イベント	<input checked="" type="checkbox"/> 有効
保存	

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

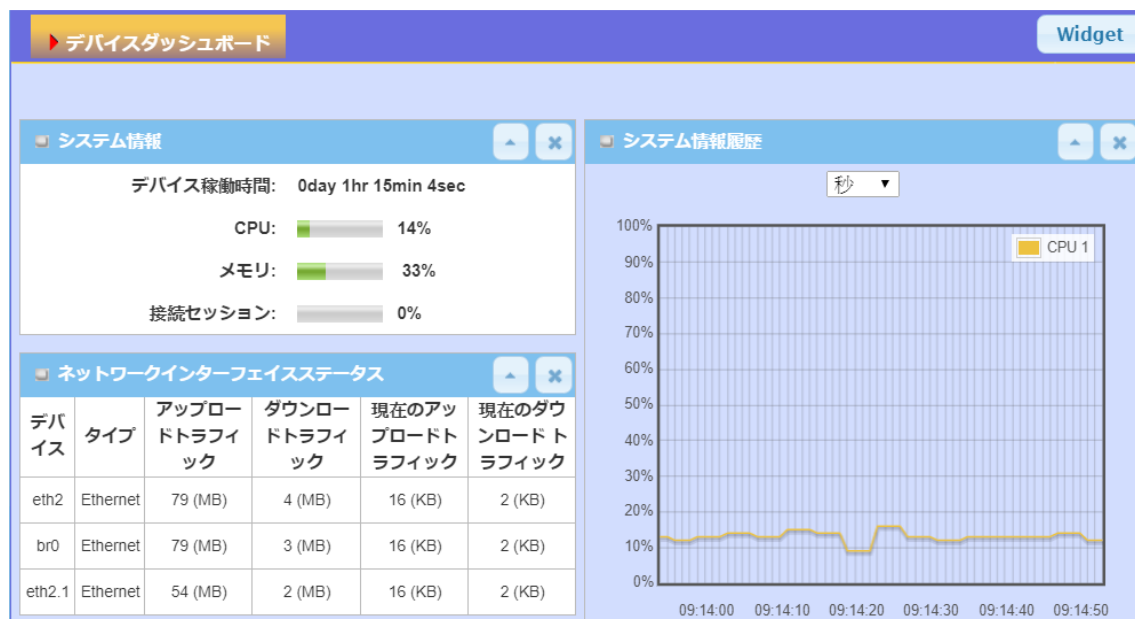
- ◆ **保存** ボタンをクリックして、通知イベントを登録します。追加/編集した通知イベントが[通知イベントリスト]に表示されます。

13. スタータス

13.1. ダッシュボード

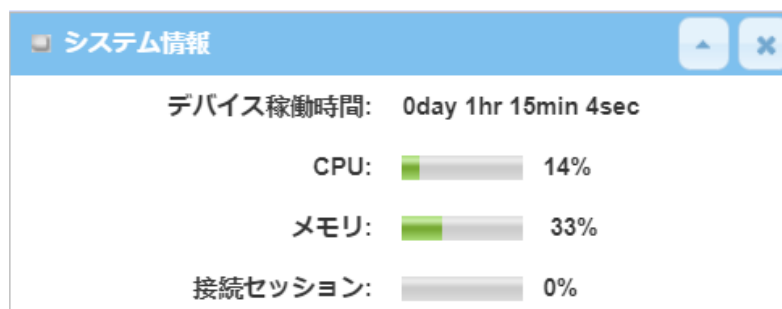
[デバイスダッシュボード]ウィンドウには、ゲートウェイの動作ステータスをすばやく把握するためのグラフまたは表に現在の各種ステータスが表示されます。システム情報、システム情報履歴、および、ネットワークインターフェースステータスが表示されます。表示は 1 秒ごとに更新されます。

◆ 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。



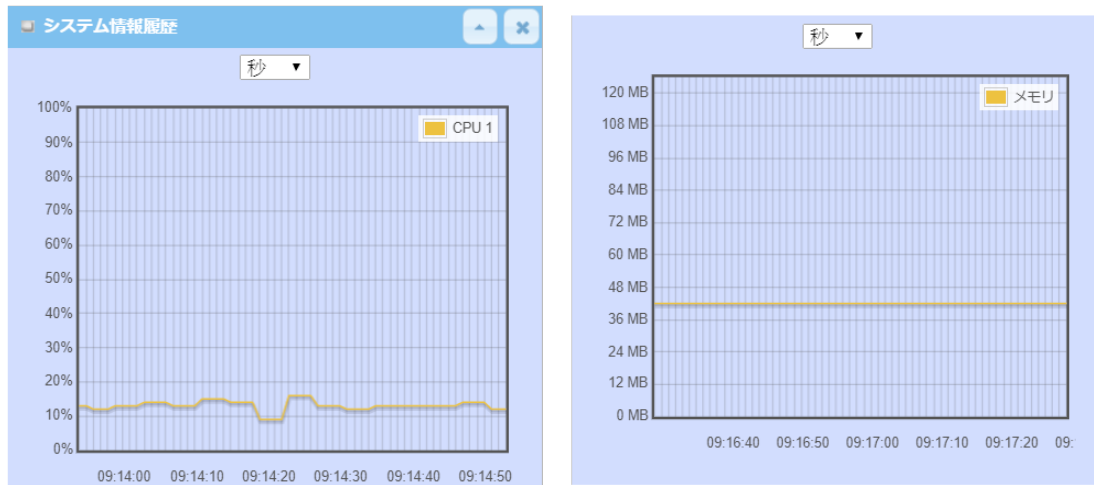
13.1.1. システム情報

[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ースステータス

ネットワークインターフェースステータス					
デバイス	タイプ	アップロードトラフィック	ダウンロードトラフィック	現在のアップロードトラフィック	現在のダウンロードトラフィック
eth2	Ethernet	85 (MB)	4 (MB)	701 (KB)	19 (KB)
br0	Ethernet	85 (MB)	4 (MB)	699 (KB)	16 (KB)
eth2.1	Ethernet	61 (MB)	2 (MB)	701 (KB)	17 (KB)

[ネットワークインターフェースステータス]画面には、ゲートウェイの各ネットワークインターフェ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。

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。

The screenshot shows the 'WAN & Upstream' status window. The left sidebar has a menu with 'ステータス' (Status) selected. The main content area has tabs for 'WAN&アップリンク', 'LANおよびVLAN', and 'ダイナミックDNS'. The 'WAN&アップリンク' tab is active, showing three expandable sections:

- WAN-インタフェースIPv4 ネットワークステータス**: A table with columns: 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. It lists WAN-1 and WAN-2.
- WAN-インタフェースIPv6 ネットワークステータス**: A table with columns: 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. It lists WAN-1.
- LAN-インタフェースネットワークステータス**: A table with columns: IPv4アドレス, IPv4サブネットマスク, IPv6リンク-ローカルアドレス, IPv6グローバルアドレス, MACアドレス, アクション. It lists a single LAN interface.
- Cellular Modem Status List**: A table with columns: 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. It lists the 'モバイル NET' interface.

13.2.2. WAN インタフェース IPv4 ネットワークステータス

IPv4 ネットワークの各種ステータス情報が表示されます。

編集をクリックすると接続設定に移動します。

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	モバイル NET	モバイル NET	NAT	100.126.162.52	255.255.255.248	100.126.162.53	59.190.146.81, 59.190.147.17	N/A	接続 0 day 0:05:02	編集
WAN-2		無効								編集

13.2.3. WAN インタフェース IPv6 ネットワークステータス

IPv6 ネットワークの各種ステータス情報が表示されます。

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

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	
WAN-1		無効				

13.2.4. LAN インタフェースネットワークステータス

LAN ネットワークの各種ステータスが表示されます。

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

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

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	IPv6リンクローカルアドレス	IPv6グローバルアドレス	MACアドレス	アクション
172.16.129.254	255.255.255.0	fe80::250:18ff:fe6a:7182	/64	00:50:18:6A:71:82	IPv4を編集する IPv6を編集する

13.2.5. 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」、「SCC 信号情報」および「エラーメッセージ」の詳細な状態情報が表示されます。

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	MV31	接続	87% (-59dBm)	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
モバイル NET	MV31	355979860004163	T99W175	T99W175.F0.1.0.0.8.PN.001.1 [Mar 04 2021 00:00:00]	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
SIM-A	準備完了	3 / 10	N/A			

サービス情報							
オペレーター	MCC	MNC	サービス種類	帯	LAC	TAC	Cell ID
N/A	440	20	WCDMA	N/A	2DB3	N/A	468010D

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

信号強度と品質					
RSSI	RSRP	RSRQ	SINR	RSCP	EcIo
-71	-101	-10	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

13.2.6. インタフェーストラフィック統計

WAN-1 および WAN-2 インタ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 ボタンでトラフィック情報をリセットできます。

インタフェーストラフィック統計				
ID	インターフェイス	受信パケット(Mb)	送信パケット(Mb)	アクション
WAN-1	3G/4G	1265.55	468.6	設定リセット
WAN-2		-	-	

13.2.7. LAN および VLAN

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

13.2.7.1. クライアントリスト

本機LANに接続されているデバイスの情報が表示されます。

LANクライアントリスト				
LANインタフェース	IPアドレス	ホスト名	MACアドレス	残りのリース時間
イーサネット	動的 / 172.16.129.113	WinBox-1131	9C-5C-5E-05-F5	00:50:02

13.2.8. 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。

13.2.8.1. DNS ステータスリスト

ダイナミック DNS の状態が表示されます。

更新ボタンで最新の情報を表示します。

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
hwt5g3200-v2-01.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。

編集ボタンをクリックするとIPSec の設定画面に移動します。

IPSecトンネルステータス 編集							
ID	トンネル名	トンネルシナリオ	ローカルサブネット	リモートIP/FQDN(完全修飾ドメイン名)	リモートサブネット	接続タイム	ステータス

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。

編集ボタンをクリックすると、OpenVPN サーバーの設定画面に移動します。

OpenVPNサーバーステータス 編集					
ID	ユーザー名	リモートIP/FQDN(完全修飾ドメイン名)		バーチャルIP/Mac	ステータス

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 ボタンをクリックすると、OpenVPN クライアントの設定画面に移動します。

OpenVPNクライアントステータス 編集 詳細							
ID	OpenVPNクライアント名	インターフェイス	リモートIP/FQDN(完全修飾ドメイン名)	リモートサブネット	バーチャルIP	接続タイム	接続状態

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

詳細なOpenVPNクライアント				
ID	TUN/TAP読み取り(bytes)	TUN/TAP書き込み(bytes)	TCP/UDP読み取り(bytes)	TCP/UDP書き込み(bytes)

13.3.1.4. L2TP サーバステータス

L2TP サーバトンネリングの設定と現在のステータスが表示されます。

編集 ボタンをクリックすると、L2TP サーバの設定画面に移動します。

L2TPサーバステータス 編集						
ID	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	接続タイム	ステータス

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 ボタンをクリックすると、L2TP クライアントの設定画面に移動します。

13.3.1.6. PPTP サーバステータス

PPTP トンネリングの設定と現在のステータスが表示されます。

編集 ボタンをクリックすると、PPTP サーバの設定画面に移動します。

PPTPサーバステータス 編集						
ID	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	接続タイム	ステータス

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 ボタンをクリックすると、PPTP クライアントの設定画面に移動します。

PPTPクライアントステータス 編集							
ID	PPTPクライアント名	インターフェイス	バーチャルIP	リモートIP/FQDN(完全修飾ドメイン名)	デフォルトゲートウェイ/リモートサブネット	接続タイム	ステータス

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. パケットフィルタステータス

パケットフィルタリングのログ履歴が表示されます。

編集ボタンをクリックすると、パケットフィルタ設定画面に移動します。

パケットフィルタ		編集			
有効化フィルタールール	検出コンテンツ	IP	タイム		

13.3.2.2. URL ブロッキングステータス

URL ブロッキングのログ履歴が表示されます。

編集ボタンをクリックすると、URL ブロッキング設定画面に移動します。

URLブロッキング		編集			
有効化されたブロックルール	ブロックされたURL	IP	タイム		

13.3.2.3. MAC 制御ステータス

MAC 制御のログ履歴が表示されます。

編集ボタンをクリックすると、MAC 制御設定画面に移動します。

MAC制御		編集			
有効化された制御ルール	ブロックされたMACアドレス	IP	タイム		

13.3.2.4. IPS ステータス

IPS のログ履歴が表示されます。

編集ボタンをクリックすると、IPS 設定画面に移動します。

IPS 編集		
検出された侵入	IP	タイム

13.3.2.5. オプションステータス

オプションの設定とログ履歴が表示されます。

編集ボタンをクリックすると、オプション設定画面に移動します。

オプション 編集			
ステルスモード	SPI	WANからのPingパケットを破棄する	リモート管理者管理
無効	有効	無効	IP: 114.134.201.23, User Name: admin, Time: Nov 1 07:33:08

13.4. 管理(Administration)

13.4.1. 設定と管理

本機ではサポートしていません。

13.4.2. ログストレージ

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

13.4.2.1. ストレージ情報ステータス

ログ保管メディアの現在の状態が表示されます。

更新ボタンで最新の情報が表示されます。

ストレージ情報				
デバイスの説明	使用量	ファイル・システム	スピード	ステータス
内部ストレージ	2 / 8192 KB	JFFS2	N/A	Ready
更新				

13.5. 統計とレポート

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

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

13.5.1. 接続セッション

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

13.5.1.1. インターネットサーフィンリスト

本機で管理している接続トラフィック情報が表示されます。

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

前、**次に**、**最初**および**最後**ボタンをクリックして、表示ページを変更します。

更新ボタンをクリックすると、リストが最新の情報になります。

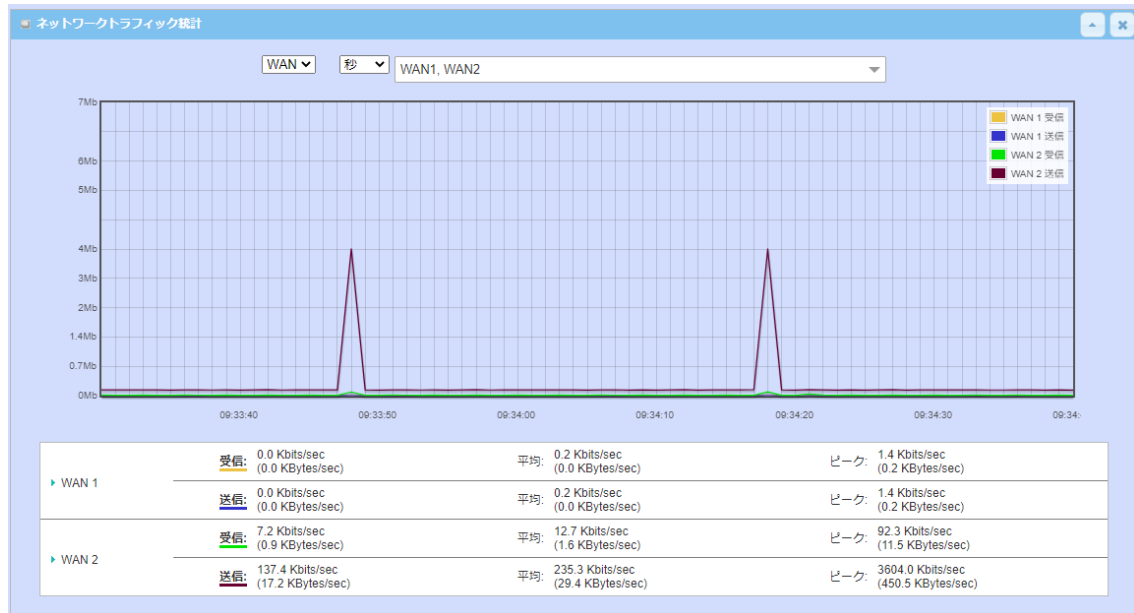
Export(.xml)および Export(.csv)ボタンをクリックすると、リストをPC内に選択したファイル形式で取り込むことができます。

13.5.2. ネットワークトラフィック

◆画面左側のメニューから、**ステータス**⇒**統計とレポート**⇒**ネットワークトラフィック**の順にクリックします。

13.5.2.1. ネットワークトラフィック統計

WAN1/WAN2 のトラフィックダイアグラムと統計情報が表示されます。



13.5.3. ログイン統計

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

13.5.3.1. 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。

デバイス管理者統計				
前 次 最初 最後 Export(.xml) Export(.csv) 更新				
ユーザー名	プロトコルタイプ	IPアドレス	Info	デューレーションタイム
admin	HTTP	172.16.129.249	Login Fail	2018/01/01 09:00~
admin	HTTP	172.16.129.249	Admin	2018/01/01 09:00~
admin	HTTP	172.16.129.113	Admin	2020/10/30 19:33~
admin	HTTP	114.134.201.23	Admin	2020/10/31 12:04~

前、**次に**、**最初**および**最後**ボタンをクリックして、表示ページを変更します。

更新ボタンをクリックすると、リストが最新の情報になります。

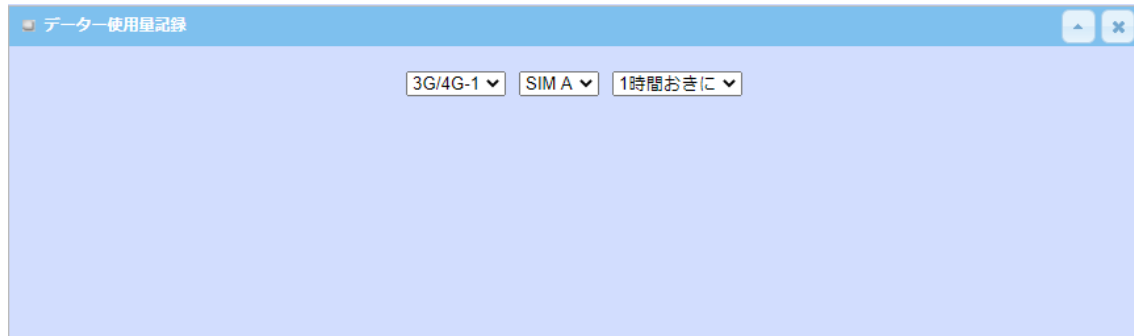
Export(.xml)および Export(.csv)ボタンをクリックすると、リストをPC内に選択したファイル形式で取り込むことができます。

13.5.3.2. 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。

13.5.3.3. データ使用量記録

「SIM-A」または「SIM-B」から選択した 5G/4G (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。

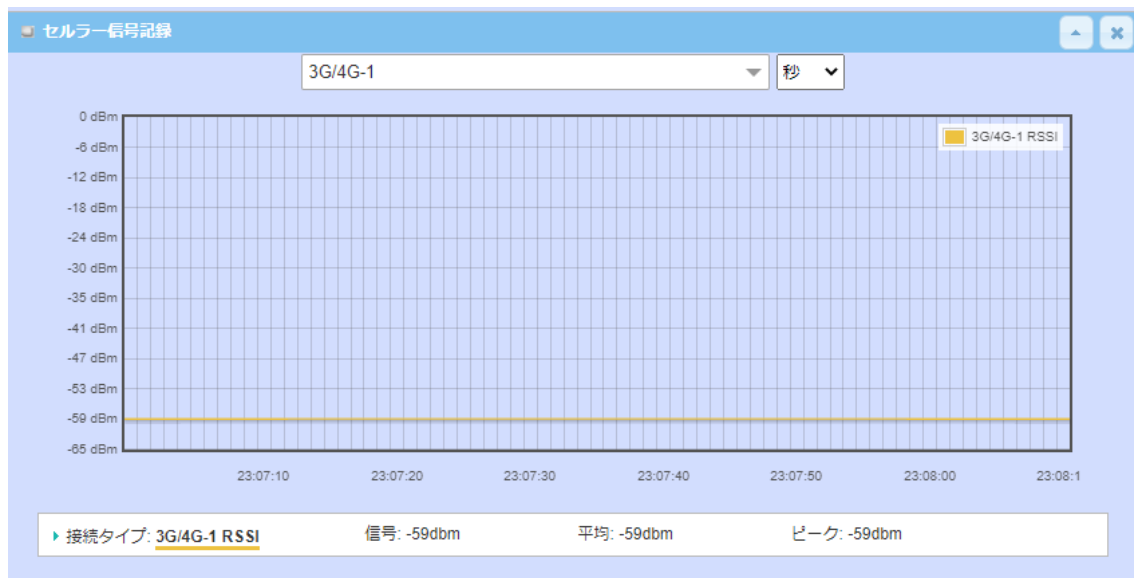


13.5.4. セルラー信号

◆ 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。

13.5.4.1. セルラー信号記録

5G/4G/3G の信号強度の履歴をグラフおよび現在値、平均値およびピーク値を表示します。更新間隔を「秒」、「分」または「時間」より選択できます。



14. 製品仕様

製品型番		HW5G-3200-V2
商品コード		189-AM03-0004
5G/LTE	対応バンド	TDD 5G: n77/n78/n79 (新周波数帯表記)
		FDD 5G: n1/n3/n8/n21 (新周波数帯表記)
		FDD LTE: B1/B3/B8/B18/B19/B26
		TDD LTE: B39/B41/B42
		WCDMA: B1/B8/B9/B19
	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)
イーサネット	対応キャリア	NTT docomo、KDDI、Softbank
	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<4x4MIMO> / 4xSMA(F)コネクタ
	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
プロトコル	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)
	LAN	DHCP サーバー、Tag/ポートベース VLAN
	TCP/IP	IPv4/IPv6 Dual Stack
	ポート制御	NAT/Port Forwarding/DMZ/VPN パススルー
	ルーティング	Static/RIP1,2/OSPF/BGP
セキュリティ	QoS	帯域幅/優先度/セッション制限
	VPN	IPsec/OpenVPN/PPTP/L2TPv2/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		64 台以下を推奨
LED 表示		ステータス(緑/橙), モバイル NET 信号(緑/橙), LAN1/WAN、LAN2~LAN4(青)
その他	USB ポート	USB 2.0 Type-A(F) コネクタ (ログストレージ USB メモリ用)
防水・防塵		なし
電源		AC100~240V/本体のみ:DC5V~18V(DC ジャック)
消費電力	AC100V 入力	最大 11W (AC アダプタ含む)
	本体消費電力	最大 9.5W (DC12V 入力時)
動作温度		-30 ~ +60℃
保存温度		-40 ~ +85℃
相対湿度		10 ~ 95% (結露なきこと)
本体寸法		(W)225mm x (D)115mm x (H)25mm (突起物含まず)
本体重量		765g 以下
認定		工事設計認証番号: 003-210239 技術基準適合認定番号: D200139003 VCCI Class A / PSE (AC アダプタ) 本体、添付品 RoHS 10 対応
製品保証期間		1.5 年間
付属品		5G/LTE アンテナ x4、AC アダプタ x1

15. 付属 AC アダプタ仕様

製品名	TRE25120-A-23G13 AC アダプタ	
商品コード	167-CN01-0018	
電源	入力	AC 100～240V
	出力	DC 12V (DC ジャック)
動作温度	-20～+60℃	
保存温度	-20～+85℃	
認定	RoHS、PSE ほか	

16. 製品保証

- ◆ 故障かなと思われた場合には、弊社カスタマサポートまでご連絡ください。

- 1) 修理を依頼される前に今一度、この取扱説明書をご確認ください。
- 2) 本製品の保証期間内の自然故障につきましては無償修理させていただきます。
- 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いただ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いただきます。
（修理できない場合もあります）
 - 1) 使用上の誤り、お客様による修理や改造による故障、損傷
 - 2) 自然災害、公害、異常電圧その他外部に起因する故障、損傷
 - 3) 本製品に水漏れ・結露などによる腐食が発見された場合
- ◆ 保証期間を過ぎますと有償修理となりますのでご注意ください。
- ◆ 一部の機器は、設定を本体内に記録する機能を有しております。これらの機器は修理時に設定を初期化しますので、お客様が行った設定内容は失われます。恐れ入りますが、修理をご依頼頂く前に、設定内容をお客様にてお控えください。
- ◆ 本製品に起因する損害や機会の損失については補償致しません。
- ◆ 修理期間中における代替品の貸し出しは、基本的に行っておりません。別途、有償サポート契約にて対応させて頂いております。有償サポートにつきましてはお買い上げの販売店にご相談ください。
- ◆ 本製品の保証は日本国内での使用においてのみ有効です。

製品に関するご質問・お問い合わせ先

ハイテクインター株式会社

カスタマサポート

TEL 0570-060030

E-mail support@hytec.co.jp

受付時間 平日 9:00～17:00