MICRO RESEARCH

MR-GM2
ファームウェア V3.00.00 補足説明書

本書では、ファームウェア V3.00.00 で追加された新機能や変更点について説明します。
本書に記載されている以外の内容については、ユーザーズマニュアルを参照して下さい。

株式会社マイクロリサーチ

はじめに

ファームウェア Ver3.00.00 へのバージョンアップは設定内容を引き継ぐことはできません。
必ず設定の初期化を行って下さい。
また、旧バージョンで保存した設定ファイルを読み込む事はできません。
手動での再設定を行って下さい。

Ver3.00.00 の変更点

ファームウェア Ver3.00.00 で変更された点は以下の通りです。

●状態表示の表示項目を追加（3 ページ）

●設定メニュー「ネットワーク設定」内「モバイルデータカード設定」を「WAN 設定」へ変更（5 ページ）

●有線 WAN 動作モードを追加（6 ページ）

●USB モバイルデータカード設定画面の「接続先」設定の内容変更（9 ページ）

●WAN 設定画面に以下の設定を追加（9 ページ）
「PPP 接続待ち時間」、「USB モジュール検出待ち時間」、「USB モジュール電源 OFF 時間」
「追加 AT コマンド」、「高速パケット処理(FastPath)」、「UDP セッション時間」、「IP 変換　セッション数」

●HTTP 回線監視に対応（12 ページ）

●「スタティックルーティング設定」を追加（13 ページ）

●「簡易 DNS 設定」を追加（15 ページ）

●「IP フィルタリング設定」を追加（17 ページ）
上記に伴い、「ポートフィルタリング設定」を削除

●「WAN 側からの Ping に応答を返す」の設定仕様を変更（20 ページ）

●「WAN 側から設定画面へのログオンを許可する」の設定仕様を変更（22 ページ）

●「ドメインフィルタリング設定」を追加（24 ページ）

●「QoS 設定」を追加（25 ページ）

●タイマー再起動機能に「稼働時間指定による再起動」を追加（27 ページ）

●「メール送信設定」を追加（28 ページ）

●システムログの工場出荷値設定を「無効」から「有効」に変更（30 ページ）

●「WAN 側からの Web 設定アクセスログを有効にする」、「LAN 側からの Web 設定アクセスログを有効にする」設定を追加（30 ページ）

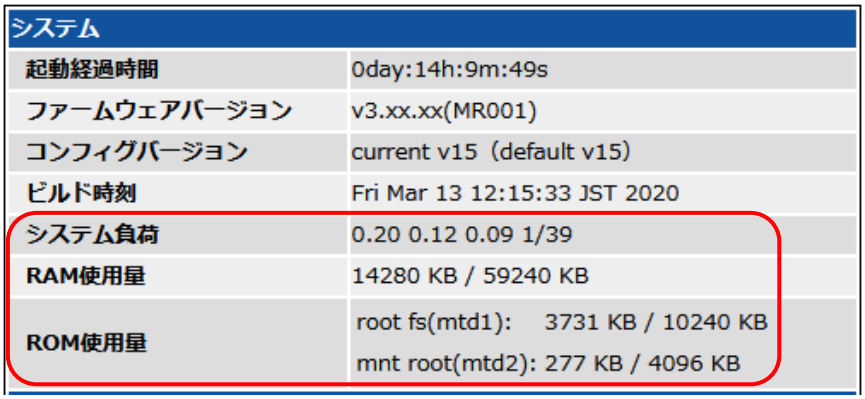
●「タイマー自動ファームウェア更新設定」を追加（31 ページ）

●無線 LAN 設定の拡張設定に「無線 LAN/有線 LAN 間　通信遮断」を追加（32 ページ）

1.状態表示画面

状態表示画面で追加された項目について説明します。

■システム



システム	
起動経過時間	0day:14h:9m:49s
ファームウェアバージョン	v3.xx.xx(MR001)
コンフィグバージョン	current v15 (default v15)
ビルド時刻	Fri Mar 13 12:15:33 JST 2020
システム負荷	0.20 0.12 0.09 1/39
RAM使用量	14280 KB / 59240 KB
ROM使用量	root fs(mtd1): 3731 KB / 10240 KB mnt root(mtd2): 277 KB / 4096 KB

システム負荷	システムの負荷状況が表示されます。
RAM 使用量	RAM の使用量が表示されます。
ROM 使用量	ROM の使用量が表示されます。

■モバイルデータカード(USB) (USB モバイルデータカード使用時に表示)

モバイルデータカード		
USB状態	回線接続中	
IPアドレス	xxx.xxx.xxx.xxx	更新
電話番号	080xxxxxxxx	
電波強度(アンテナ)	4	
電波強度(RSSI)	-65dBm	

電話番号	SIM カードの電話番号が表示されます。 情報を取得できなかった場合「不明」もしくは「取得失敗」と表示されます。
電波強度(アンテナ)	内蔵通信モジュールのアンテナ状態が表示されます。 数字はアンテナの数(1～4)を表します。 情報を取得できなかった場合「不明」もしくは「取得失敗」と表示されます。
電波強度(RSSI)	電波強度が表示されます。 情報を取得できなかった場合「不明」もしくは「取得失敗」と表示されます。

■有線 WAN （有線 WAN ポート使用時に表示）

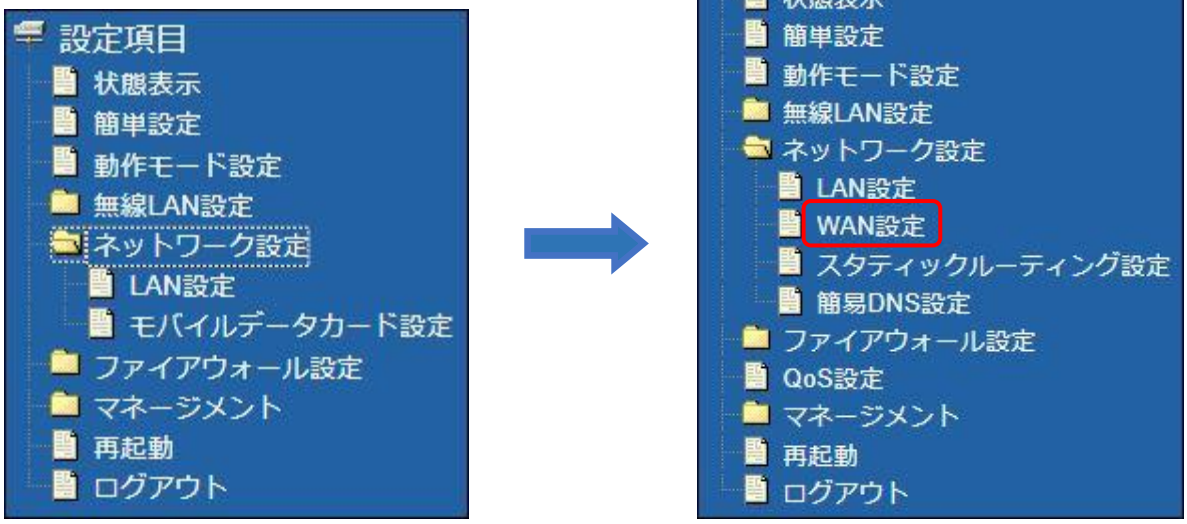
有線WAN （ETH1）	
接続モード	DHCPクライアント
IPアドレス	xxx.xxx.xxx.xxx
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	xxx.xxx.xxx.xxx
MACアドレス	00:10:38:xx:xx:xx

接続モード	**DHCP クライアント** →DHCP クライアントにより IP アドレスを取得した状態です。 **DHCP サーバーから IP アドレス取得中** →DHCP サーバーから IP アドレスを取得中、または IP アドレスが取得できない状態です。 **PPPoE 接続中** →PPPoE により回線接続中です。 **PPPoE 切断状態** →PPPoE 接続が切断中、または PPPoE 接続ができない状態です。 **IP アドレス固定 接続中** →回線接続中です。 **IP アドレス固定 切断状態** →WAN ポートがリンクダウンしている状態です。
IP アドレス	WAN ポート（ETH1 ポート）の IP アドレスが表示されます。
サブネットマスク	WAN ポート（ETH1 ポート）のサブネットマスクが表示されます。
デフォルトゲートウェイ	WAN ポート（ETH1 ポート）のデフォルトゲートウェイアドレスが表示されます。
MAC アドレス	WAN ポート（ETH1 ポート）の MAC アドレスが表示されます。

2.ネットワーク設定

「ネットワーク設定」メニューで変更された項目について説明します。

設定メニュー「ネットワーク設定」内「モバイルデータカード設定」が「WAN 設定」へ表示が変更になりました。

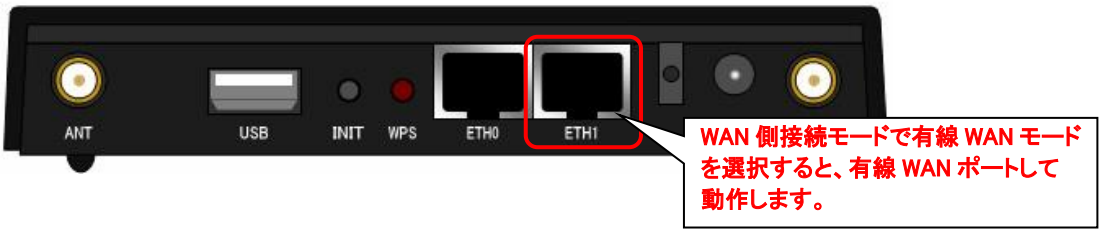


3.WAN 設定画面

「WAN 設定」画面で追加・変更された項目について説明します。

「ネットワーク設定」→「WAN 設定」→「WAN 側接続モード」に「IP アドレス固定（ETH1）」、「DHCP クライアント（ETH1）」、「PPPoE クライアント（ETH1）」が追加されました。

■ETH1 コネクタについて



ETH1ポートは工場出荷時、有線 LAN ポートとして動作しています。

WAN 側接続モードを「IP アドレス固定（ETH1）」、「DHCP クライアント（ETH1）」、「PPPoE クライアント（ETH1）」で設定した場合、有線 WAN ポートとして動作します。

WAN 側接続モードを「モバイルデータカード（USB）」（工場出荷値）で設定した場合は、有線 LAN ポートとして動作します。

3-1. IP アドレス固定

IP アドレス固定(ETH1)について説明します。

WAN 側接続モードで「**IP アドレス固定(ETH)**」を選択し、以下の各設定を行って下さい。

■IP アドレス、サブネットマスク、デフォルトゲートウェイ

WAN 側の IP アドレス、サブネットマスク、デフォルトゲートウェイを入力して下さい。

■MTU サイズ

MTU(Maximum Transmission Unit)サイズを変更する場合、MTU サイズを入力して下さい。
通常は初期値「1500」のままご利用下さい。

■DNS

プライマリ DNS、セカンダリ DNS に DNS サーバーIP アドレスを入力して下さい。
DNS サーバーを使用しない場合「未使用」を選択して下さい。

3-2. DHCP クライアント

DHCP クライアント(ETH1)について説明します。

WAN 側接続モードで「**DHCP クライアント(ETH)**」を選択し、以下の各設定を行って下さい。

■ホスト名

WAN 側ネットワーク管理者から指定があった場合、ホスト名を入力して下さい。
指定が無い場合は、初期値のままご利用下さい。

■MTU サイズ

MTU(Maximum Transmission Unit)サイズを変更する場合、MTU サイズを入力して下さい。
通常は初期値「1500」のままご利用下さい。

■DNS

DNS サーバーIP アドレスを自動取得する場合「自動取得」を選択して下さい。
DNS サーバーIP アドレスを設定する場合「手動設定」を選択してプライマリ DNS、セカンダリ DNS に DNS サーバーIP アドレスを入力して下さい。
DNS サーバーを使用しない場合「未使用」を選択して下さい。

3-3. PPPoE クライアント

PPPoE クライアント（ETH1）について説明します。

WAN 側接続モードで「**PPPoE クライアント（ETH1）**」を選択し、以下の各設定を行って下さい。

■ユーザー名、パスワード

契約資料を参照して「認証 ID（ユーザー名）」、「認証パスワード」を入力して下さい。

■サービス名

契約プロバイダから特に指定がない場合は空欄にして下さい。

■接続モード

接続モードを選択して下さい。

常時接続

→常に回線接続状態になります。回線が切断されると自動再接続を行います。

自動接続・切断

→インターネットへの接続要求を検出し回線の自動接続を行います。
無通信監視時間で設定した時間、無通信状態が続くと自動切断します。

■無通信待機時間

接続モードで「自動接続・切断」を選択した場合に設定可能です。
ここで設定した時間、無通信状態が続くと自動切断します。

■MTU

MTU（Maximum Transmission Unit）サイズを変更する場合、MTU サイズを入力して下さい。
通常は初期値「1452」のままご利用下さい。

■DNS

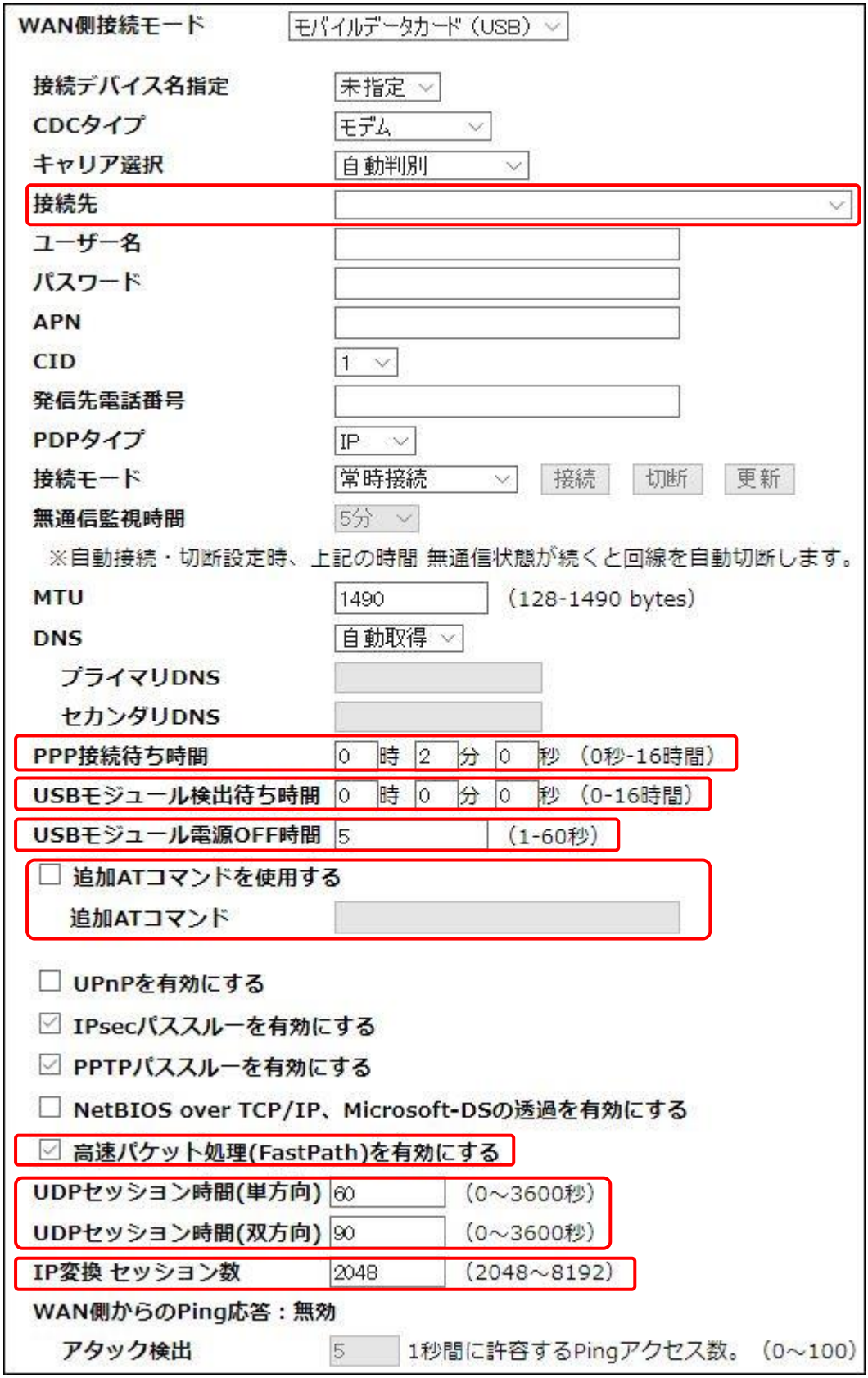
DNS サーバーIP アドレスを自動取得する場合「自動取得」を選択して下さい。
DNS サーバーIP アドレスを設定する場合「手動設定」を選択してプライマリ DNS、セカンダリ DNS に DNS サーバーIP アドレスを入力して下さい。

■PPP 接続待ち時間

PPP 接続の応答待ち時間を設定します。
ここで設定した時間内に応答が無い場合、PPP の再接続を行います。
通常は初期値「40 秒」のままご利用下さい。

4.モバイルデータカード設定画面

「モバイルデータカード(USB)」で追加・変更された項目について説明します。



■接続先

接続先に登録されている内容を以下の通り変更しました。
接続先を選択すると、ユーザー名、パスワード、APN、発信先電話番号が自動入力されます。
任意のユーザー名、パスワード、APN、発信先電話番号を設定する場合は「その他」を選択して下さい。

接続先	ユーザー名	パスワード	APN	発信先電話番号
ソフトバンク 法人データ通信プランフラット(4G)	biz4g	biz4g	bizflat4g.softbank	*99#
ワイモバイル LTE プラン LTE フラット	em	em	em.std	*99***1#
NTT ドコモ mopera U Xi データ通信 /FOMA パケット通信	mopera	mopera	mopera.net	*99***1#
KDDI Speed USB STICK U03			kwx2.au-net.ne.jp	*99***1#

確 認	接続先は設定保存後に再度画面を開いた場合、空欄(未選択の状態)になります。 これは仕様であり異常ではありません。

■PPP 接続待ち時間

PPP 接続の応答待ち時間を設定します。
ここで設定した時間内に応答が無い場合、PPP の再接続を行います。
通常は初期値「2 分」のままご利用下さい。

■USB モジュール検出待ち時間

USB データカードが応答するまでの待ち時間を設定します。
ここで設定した時間内に USB データカードが応答しない場合、USB ポートの電源を OFF/ON します。
USB ポートの電源 OFF/ON を 10 回繰り返しても応答しない場合、MR-GM2 が再起動します。
通常は初期値「0 秒」のままご利用下さい。

■USB モジュール電源 OFF 時間

MR-GM2 再起動時に USB データカードの電源を OFF にする時間を設定します。
通常は初期値「5 秒」のままご利用下さい。

■追加 AT コマンドを使用する

追加 AT コマンドを使用する場合、「追加 AT コマンドを使用する」チェックを入れ、AT コマンドを入力して下さい。
複数の AT コマンドを設定する場合「¥n」もしくは「¥n」で区切って入力して下さい。

■高速パケット処理(FastPath)を有効にする

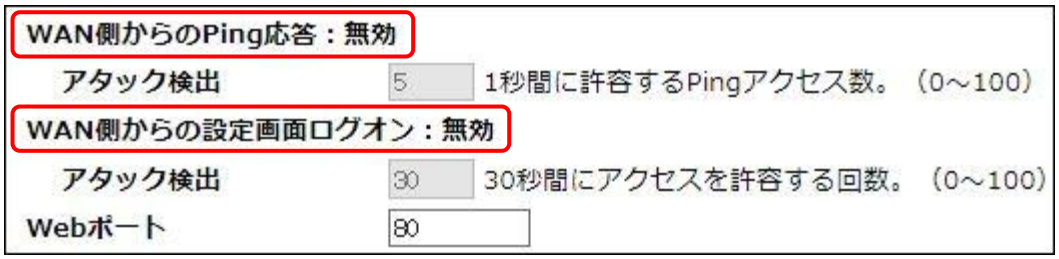
高速パケット処理(ファストパス)を無効にする場合、チェックを外して下さい。

■UDP セッション時間(単方向)、UDP セッション時間(双方向)

UDP パケットのセッション情報の保持時間を設定します。通常は初期値(単方向 60 秒、双方向 90 秒)のままご利用下さい。

■IP 変換セッション数

IP アドレス変換の最大セッション数を設定します。
通常は初期値(2048)のままご利用下さい。



■WAN 側からの Ping 応答

WAN 側からの Ping 応答の状態を表示します。

有効にする場合は、「9. WAN 側からの Ping 応答を返す設定方法」(20 ページ)を参照して下さい。

・アタック検出

WAN 側からの Ping 応答が有効の時に設定が可能です。

1 秒間にここで設定した回数を超えて Ping を受信した場合、その送信元 IP アドレスからの Ping を 300 秒間拒否します。

■WAN 側から設定画面へのログオン

WAN 側から設定画面ログオンの状態を表示します。

有効にする場合は、「10. WAN 側から設定画面へのログオンを許可する設定方法」(22 ページ)を参照して下さい。

・アタック検出

WAN 側から設定画面ログオンが有効の時に設定が可能です。

30 秒間にここで設定した回数を超えて SYN フラグ(接続要求)を受信した場合、その送信元 IP アドレスからの SYN フラグを 300 秒間拒否します。

確 認	回数が少なすぎると、正しいログオンでの操作でも拒否されてしまう可能性があります。 通常は初期値「30」のままご利用下さい。

5.回線監視機能設定

「回線監視機能設定」で追加された項目について説明します。

「ネットワーク設定」→「WAN 設定」

■回線監視機能（HTTP による監視）

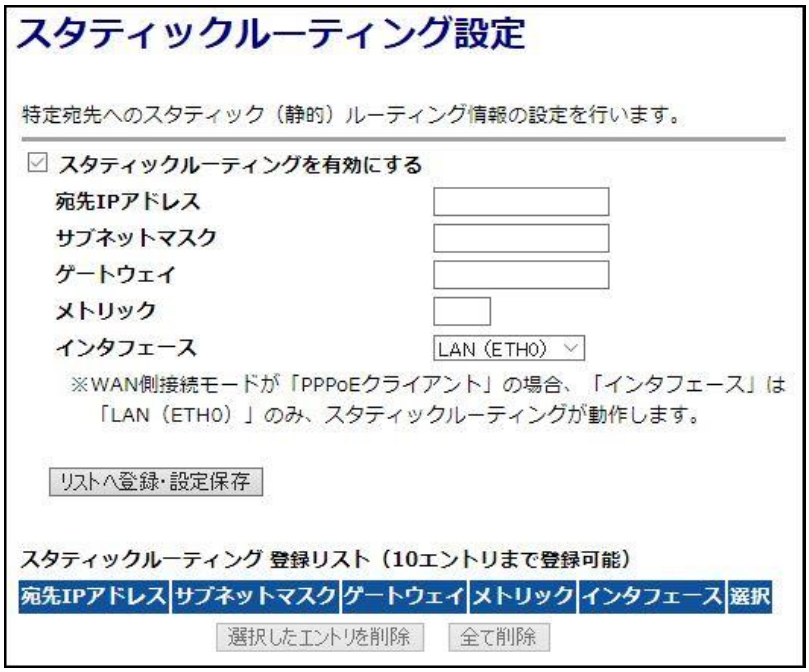
HTTP リクエストによる回線監視が可能です。
HTTP 監視機能を使用する場合、「HTTP による監視」を選択して下さい。
「HTTP による監視」は HTTP リクエストに対して応答があった場合に回線接続状態と判断します。

6.スタティックルーティング設定

設定メニュー「ネットワーク設定」内「スタティックルーティング設定」が追加されました。

特定の宛先への通信をLAN内の別のルーターへルーティングするための、「スタティックルーティング設定」について説明します。

設定メニューの「ネットワーク設定」より「スタティックルーティング設定」をクリックして下さい。「スタティックルーティング設定」画面が開きます。



■スタティックルーティングを有効にする（チェックボックス）
スタティックルーティング機能を有効にする場合、チェックを入れて下さい。

■宛先 IP アドレス、サブネットマスク
宛先（送信先）の IP アドレス/サブネットマスクを入力して下さい。

■ゲートウェイ
ルーティング先ゲートウェイ（LAN 内の別ルーター）の IP アドレスを入力して下さい。

■メトリック
メトリック（ルーティングの優先順位）を入力して下さい。
ルーティング先ゲートウェイが複数存在しない場合は、「1」を入力して下さい。

■インタフェース
「LAN(ETH0)」か「WAN(ETH1)」のどちらかを選択して下さい。

■リストへ登録・設定保存（ボタン）
入力した内容を登録リストに登録します。
[今すぐ再起動]ボタンを押すと動作に反映されます。
引き続き設定を行う場合は[後で再起動]ボタンをクリックして下さい。

■選択したエントリを削除（ボタン）

スタティックルーティング登録リストの「選択」にチェックを入れたものを削除されます。
[今すぐ再起動]ボタンを押すと動作に反映されます。
引き続き設定を行う場合は[後で再起動]ボタンをクリックして下さい。

■全て削除（ボタン）

スタティックルーティング登録リストの「選択」にチェックを入れたものを削除されます。
[今すぐ再起動]ボタンを押すと動作に反映されます。
引き続き設定を行う場合は[後で再起動]ボタンをクリックして下さい。

7.簡易 DNS 設定

新機能「簡易 DNS 設定」について説明します。

設定メニューの「ネットワーク設定」より「簡易 DNS 設定」をクリックして下さい。「簡易 DNS 設定」画面が開きます。

確 認	簡易 DNS 機能を使用するためには、パソコン等端末の DNS サーバーIP アドレスに MR-GM2 の IP アドレスを設定する必要があります。

■IP アドレス

登録するホストの IP アドレスを入力して下さい。

■ホスト名

登録するホスト名を半角英数字で入力して下さい。

Windows パソコンから本機能を利用する場合は必ず「.」(ドット)を含むホスト名を設定して下さい。

■コメント

登録する設定内容が判別しやすいように、コメントを入力して下さい。

■設定保存（ボタン）

入力した内容を簡易 DNS テーブルに登録します。

[今すぐ再起動]ボタンを押すと動作に反映されます。

引き続き設定を行う場合は後で[再起動]ボタンをクリックして下さい。

確 認	最大 10 エントリまで登録可能です。

■選択したエントリを削除（ボタン）

簡易 DNS テーブルの「選択」にチェックを入れたものを削除されます。
[今すぐ再起動]ボタンを押すと動作に反映されます。引き続き設定を行う場合は後で「再起動]ボタンをクリックして下さい。

■全て削除（ボタン）

簡易 DNS テーブルの内容全てを削除します。
[今すぐ再起動]ボタンを押すと動作に反映されます。
引き続き設定を行う場合は後で[再起動]ボタンをクリックして下さい。

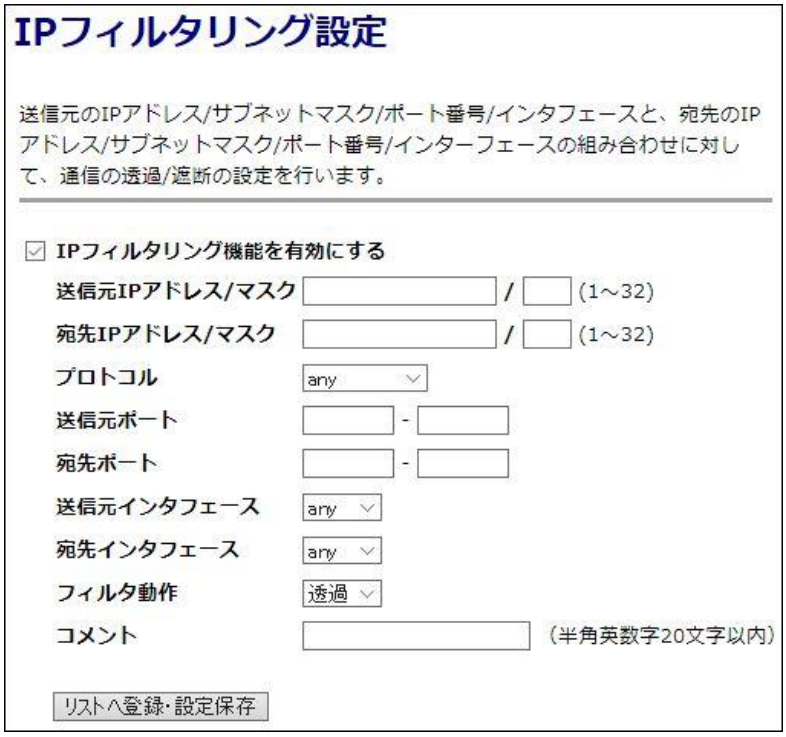
8.IP フィルタリング設定

「ポートフィルタリング設定」が削除され「IP フィルタリング設定」が追加されました。

IP アドレス、プロトコルを基に通信を透過する、IP フィルタリング設定について説明します。

確 認	IP フィルタリング機能は、透過が基本動作となります。
	IP フィルタリングの対象となるのは、LAN→WAN、WAN→LAN、LAN→自機、WAN→自機方向のみです。LAN→LAN 方向を設定する事はできません。
	IP フィルタリング機能は、設定保存、登録リストの編集が即動作に反映されます。

設定メニューの「ファイアウォール設定」より「IP フィルタリング設定」をクリックして下さい。「IP フィルタリング設定」画面が開きます。



■IP フィルタリング機能を有効にする（チェックボックス）

IP フィルタリング機能を有効にする場合、チェックを入れて下さい。
チェックを外した場合、登録リストに関係無く全て透過します。

■送信元 IP アドレス/マスク

送信元の IP アドレスとサブネットマスクを入力して下さい。
指定しない（any）場合は空欄にして下さい。

■宛先 IP アドレス/マスク

宛先の IP アドレスとサブネットマスクを入力して下さい。
指定しない（any）場合は空欄にして下さい。

■プロトコル

対象とするプロトコルを選択して下さい。

any	:全てのプロトコルを対象とします。
TCP+UDP	:TCP、UDP プロトコル両方を対象とします。
TCP	:TCP プロトコルを対象とします。
UDP	:UDP プロコルを対象とします。
ICMP	:ICMP（PING）プロトコルを対象とします。

■送信元ポート

送信元のポート番号を入力して下さい。（範囲設定可）
単一ポートを対象とする場合は、左側の入力欄のみ設定して下さい。
ポート番号を指定しない（any）場合は、空欄にして下さい。

■宛先ポート

宛先のポート番号を入力して下さい。（範囲設定可）
単一ポートを対象とする場合は、左側の入力欄のみ設定して下さい。
ポート番号を指定しない（any）場合は、空欄にして下さい。

■送信元インターフェース、宛先インターフェース

対象とする通信の方向を選択します。

any	:WAN ポート、LAN ポート両方を対象とします。（自機は含まれません。）
WAN	:WAN ポートを対象とします。
LAN	:LAN ポートを対象とします。
自機	:MR-GM2 への通信を対象とします。（宛先インターフェースにのみ表示）

送信元インターフェース：LAN 宛先インターフェース：WAN とした場合、LAN→WAN 方向
送信元インターフェース：WAN 宛先インターフェース：LAN とした場合、WAN→LAN 方向となります。

確 認	IP フィルタリングの対象となるのは、LAN→WAN、WAN→LAN、LAN→自機、WAN→自機方向のみです。LAN→LAN 方向を設定する事はできません。

■フィルタ動作

登録するフィルタの動作を選択して下さい。

■コメント

登録する設定内容が判別しやすいように、コメントを入力して下さい。

■リストへ登録・設定保存（ボタン）

入力した内容が登録リストに登録され、動作に反映されます。

確 認	最大 64 エントリまで登録可能です。

送信元/宛先フィルタリング 登録リスト（64エントリまで登録可能）

送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
111.111.111.111/28	any	TCP	any	80 - 80	WAN	LAN	透過		☐
any	any	TCP	any	80 - 80	WAN	LAN	遮断		☐

選択したエントリを編集　選択したエントリを一つ上げる　選択したエントリを一つ下げる

選択したエントリを削除　全て削除

確認	送信元 IP アドレス、宛先 IP アドレス、及び送信元ポート番号、宛先ポート番号の両方を設定した場合は「AND 条件」となります。
	登録リストの順番が、そのまま処理の「優先順位」になります。

■選択したエントリを編集（ボタン）

登録リストの「選択」にチェックを入れたものを編集します。

■選択したエントリを一つ上げる（ボタン）

登録リストの「選択」にチェックを入れたものを一つ上に移動します。

■選択したエントリを一つ下げる（ボタン）

登録リストの「選択」にチェックを入れたものを一つ下に移動します。

確認	複数のエントリを同時に移動する事はできません。

■選択したエントリを削除（ボタン）

登録リストの「選択」にチェックを入れたものを削除します。

■全て削除（ボタン）

登録リストの内容全てを削除します。

<設定例 1：IP アドレス「111.111.111.111/32」宛の通信のみ許可する>

送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
any	111.111.111.111/32	any	any	any	LAN	WAN	透過		☐
any	any	any	any	any	LAN	WAN	遮断		☐

<設定例 2：IP アドレス「111.111.111.111/32」からの通信のみ、LAN 内の WEB サーバーへのアクセスを許可する>

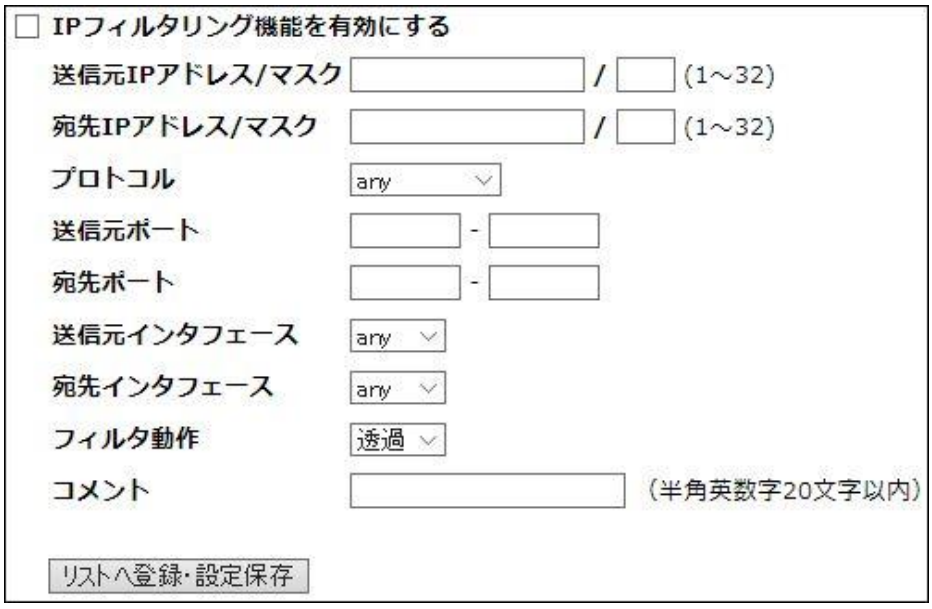
送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
111.111.111.111/32	any	TCP	any	80 - 80	WAN	LAN	透過		☐
any	any	TCP	any	80 - 80	WAN	LAN	遮断		☐

9. WAN 側からの Ping 応答を返す設定方法

WAN 側から設定画面へのログオンを許可する設定を行う場合、以下の手順で設定を行って下さい。

設定メニューの「ファイアウォール設定」より「IPフィルタリング設定」をクリックして下さい。

「IP フィルタリング機能を有効にする」にチェックを入れ、以下のテーブルを追加して下さい。



■送信元IP アドレス/マスク

特定の IP アドレスからの PING にのみ応答する場合、対象のIPアドレスとサブネットマスクを入力して下さい。
指定しない場合は空欄にして下さい。

■宛先IP アドレス/マスク

空欄にして下さい。

■プロトコル

「ICMP」を選択して下さい。

■送信元ポート

空欄にして下さい。

■宛先ポート

空欄にして下さい。

■送信元インターフェース

「WAN」を選択して下さい。

■宛先インターフェース

「自機」を選択して下さい。

■フィルタ動作

「透過」を選択して下さい。

設定が終わりましたら、[リストへ登録・設定保存]ボタンをクリックして下さい。

IP フィルタリング登録リストに登録されます。

送信元/宛先フィルタリング 登録リスト（64エントリまで登録可能）

送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
any	any	ICMP	any	any	WAN	自機	透過		☐

選択したエントリを編集　選択したエントリを一つ上げる　選択したエントリを一つ下げる

選択したエントリを削除　全て削除

登録が完了すると、WAN 側からの PING に応答します。

登録後、「ネットワーク設定」→「WAN 設定」内の「WAN 側からの PING 応答」のステータスが有効に変わり、アタック 検出設定が可能になります。

●設定例：IP アドレス「111.111.111.111/32」からの PING にのみ応答を返す

送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
111.111.111.111/32	any	ICMP	any	any	WAN	自機	透過		☐

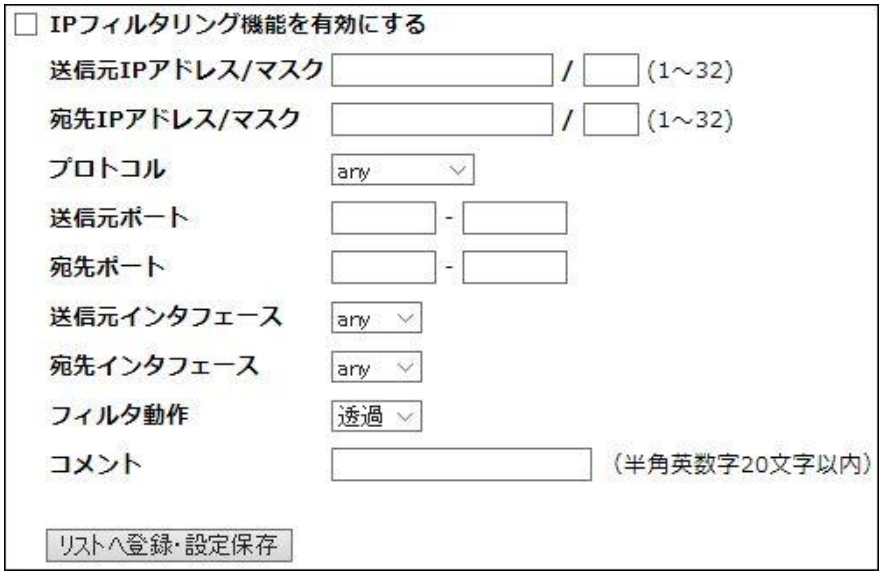
※複数の IP アドレスからの PING に応答を返す場合、上記フィルタを複数登録して下さい。

10. WAN 側から設定画面へのログオンを許可する設定方法

「WAN 側から設定画面へのログオンを許可する設定」を行う場合、以下の手順で設定を行って下さい。

設定メニューの「ファイアウォール設定」より「IPフィルタリング設定」をクリックして下さい。

「IP フィルタリング機能を有効にする」にチェックを入れ、以下のテーブルを追加して下さい。



■送信元IP アドレス/マスク

特定の IP アドレスからのみ設定画面へのログオンを許可する場合、対象のIPアドレスとサブネットマスクを入力して下さい。指定しない場合は空欄にして下さい。

■宛先IP アドレス/マスク

空欄にして下さい。

■プロトコル

「TCP」を選択して下さい。

■送信元ポート

空欄にして下さい。

■宛先ポート

「80」を入力して下さい。

Web ポート(アクセスポート番号)を変更している場合は、変更したポート番号を入力して下さい。

■送信元インターフェース

「WAN」を選択して下さい。

■宛先インターフェース

「自機」を選択して下さい。

■フィルタ動作

「透過」を選択して下さい。

設定が終わりましたら、[リストへ登録・設定保存]ボタンをクリックして下さい。

IP フィルタリング登録リストに登録されます。

送信元/宛先フィルタリング 登録リスト（64エントリまで登録可能）

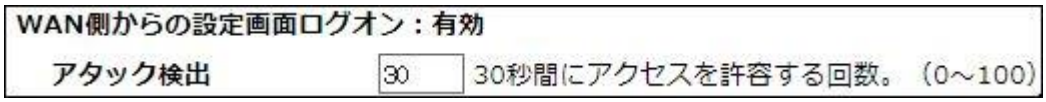
送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
any	any	TCP	any	80 - 80	WAN	自機	透過		☐

選択したエントリを編集　選択したエントリを一つ上げる　選択したエントリを一つ下げる

選択したエントリを削除　全て削除

登録が完了すると、WAN 側から設定画面にログインする事が可能になります。

登録後、「ネットワーク設定」→「WAN 設定」内の「WAN 側からの設定ログオン」のステータスが有効に変わり、アタッ ク検出設定が可能になります。



●設定例：IP アドレス「111.111.111.111/32」からの設定画面へのログオンのみ許可する

送信元IP/マスク	宛先IP/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
111.111.111.111/32	any	TCP	any	80 - 80	WAN	自機	透過		☐

※複数の IP アドレスからの設定画面へのログオンを許可する場合、上記フィルタを複数登録して下さい。

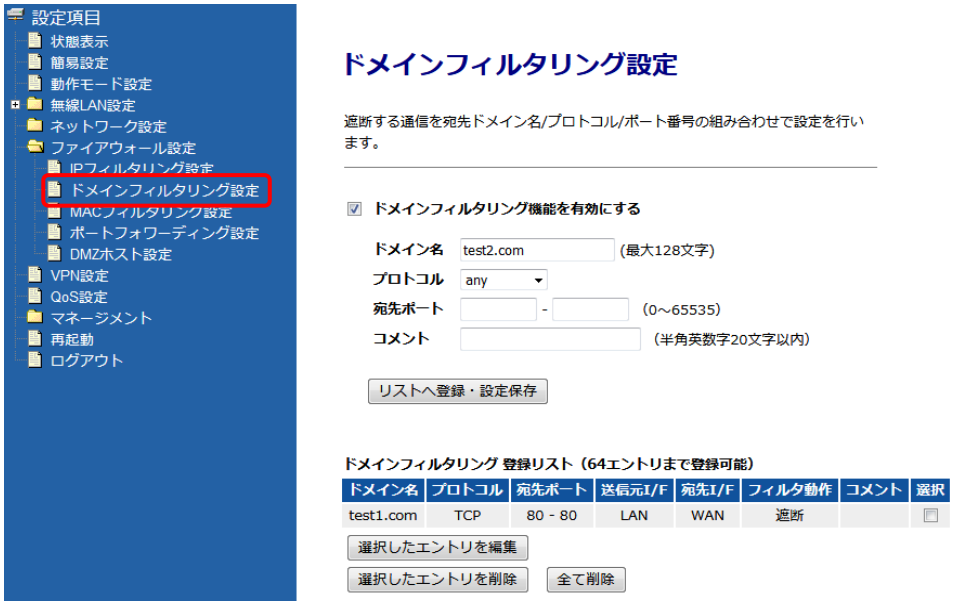
11. ドメインフィルタリング

新機能「ドメインフィルタリング設定」について説明します。

確認	ドメインフィルタリング機能は、透過が基本動作となります。
	ドメインフィルタリング機能は、LAN→WAN 方向の通信に適用されます。

設定メニューの「ファイアウォール設定」より「ドメインフィルタリング設定」をクリックして下さい。

「ドメインフィルタリング設定」画面が開きます。



■ドメインフィルタリング機能を有効にする（チェックボックス）

ドメインフィルタリング機能を有効にする場合、チェックを入れて下さい。

■ドメイン名

遮断するドメイン名を入力して下さい。

■プロトコル

対象とするプロトコルを選択して下さい。

any	：全てのプロトコルを対象とします。
TCP+UDP	：TCP、UDP プロトコル両方を対象とします。
TCP	：TCP プロトコルを対象とします。
UDP	：UDP プロコルを対象とします。
ICMP	：ICMP（PING）プロトコルを対象とします。

■宛先ポート

宛先のポート番号を入力して下さい。（範囲設定可）

単一ポートを対象とする場合は、左側の入力欄のみ設定して下さい。

ポート番号を指定しない（any）場合は、空欄にして下さい。

■コメント

登録する設定内容が判別しやすいように、コメントを入力して下さい。

■リストへ登録・設定保存（ボタン）

入力した内容が登録リストに登録され、動作に反映されます。

確認	最大 64 エントリまで登録可能です。

■選択したエントリを編集（ボタン）

登録リストの「選択」にチェックを入れたものを編集します。

■選択したエントリを削除（ボタン）

登録リストの「選択」にチェックを入れたものを削除します。

■全て削除（ボタン）

登録リストの内容全てを削除します。

12.QoS 設定

通信速度を制限する「QoS 設定」について説明します。

設定メニューの「QoS 設定」をクリックして下さい。

「QoS 設定」画面が開きます。

■QoS を有効にする（チェックボックス）

QoS 機能を有効にする場合、チェックを入れて下さい。

■自動上り速度制限を有効にする（チェックボックス）

QoS ルールに基づいて上り帯域を制限します。

QoS ルールに合致しない通信の上り帯域は 100Mbps（制限無し）になります。

■自動下り速度制限を有効にする（チェックボックス）

QoS ルールに基づいて下り帯域を制限します。

QoS ルールに合致しない通信の下り帯域は 100Mbps（制限無し）になります。

■手動上り速度制限を指定(Kbps)

「自動上り速度制限を有効にする」のチェックを外した場合に設定可能です。

全体の上り帯域の制限値を設定します。

QoS ルールに合致した通信は、QoS ルールの上り帯域に制限されます。

■手動下り速度制限を指定(Kbps)

「自動下り速度制限を有効にする」のチェックを外した場合に設定可能です。

全体の下り帯域の制限値を設定します。

QoS ルールに合致した通信は、QoS ルールの下り帯域に制限されます。

■QoS ルール登録

QoS ルールを登録します。

■アドレスタイプ

速度制限の対象とするアドレスのタイプを選択します。

■IP アドレス(範囲)

アドレスタイプで IP アドレスを選択した場合、IP アドレスを入力します。

単一 IP アドレスを指定する場合は、左右の入力欄に同じ IP アドレスを入力して下さい。

■MAC アドレス

アドレスタイプで MAC アドレスを選択した場合、MAC アドレスを入力します。

■モード

速度制限のモードを選択します。

最低帯域保証:保証する最低速度を設定します。

最大帯域制限:最大速度を設定します。

■上り帯域、下り帯域

上り、下りの帯域を Kbps 単位で設定します。

確認	制限無しの状態で回線速度を計測し、実際の帯域内に収まるように設定して下さい。
	登録する QoS ルールの帯域の合計で 100Mbps 以内に収まるように設定して下さい。
	手動速度制限を行う場合、手動速度制限に設定した値より小さい値を設定して下さい。 手動速度制限より大きい値を設定すると、手動速度制限で設定した値で制限されますのでご注意下さい。 例)手動速度制限:30000Kbps QoS ルール:50000Kbps 上記の場合、QoS ルールに合致した通信は 30000Kbps で制限されます。

■コメント

登録する設定内容が判別しやすいように、コメントを入力して下さい。

■リストへ登録・設定保存(ボタン)

入力した内容が QoS ルール登録リストに登録され、動作に反映されます。

QoSルール 登録リスト (10エントリまで登録可能)

IPアドレス	MACアドレス	モード	上り帯域	下り帯域	コメント	選択
192.168.0.10 - 192.168.0.20	----	最大帯域制限	500	500	Client	☐
----	001038222222	最低帯域保証	1000	1000	Client	☐

選択したエントリを削除　全てを削除

確認	最大 64 エントリまで登録可能です。

■選択したエントリを削除(ボタン)

登録リストの「選択」にチェックを入れたものが削除され、動作に反映されます。

■全て削除(ボタン)

登録リストの内容全てが削除され、動作に反映されます。

13.稼働時間指定による再起動

「稼働時間指定による再起動」について説明します。

設定メニューの「マネージメント」より「.時刻情報・タイマー再起動設定」をクリックして下さい。

再起動機能で「稼働時間指定」を選択して下さい。

再起動を行う間隔（システム稼働時間）を入力して下さい。

現在のシステム起動経過時間は、状態表示画面で確認する事ができます。

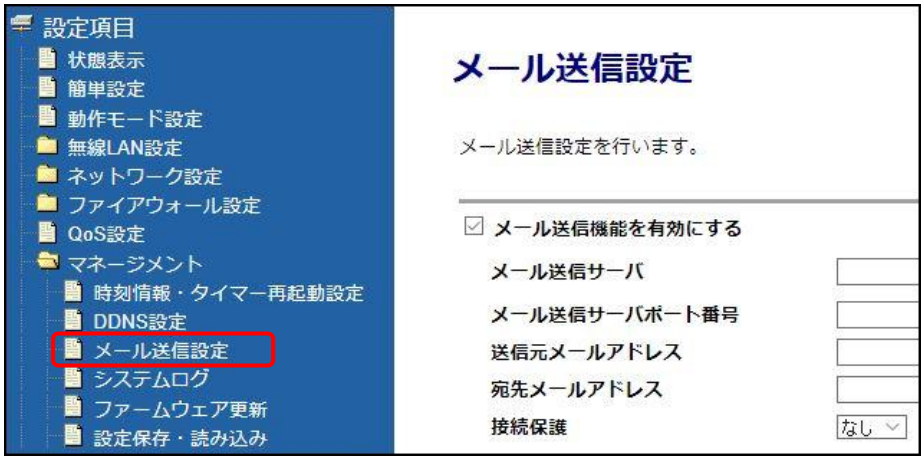
確 認	システム起動経過時間は、システム再起動（もしくは電源 OFF/ON）時にクリアされます。 設定変更時のプロセス再起動ではクリアされません。

14.メール送信機能

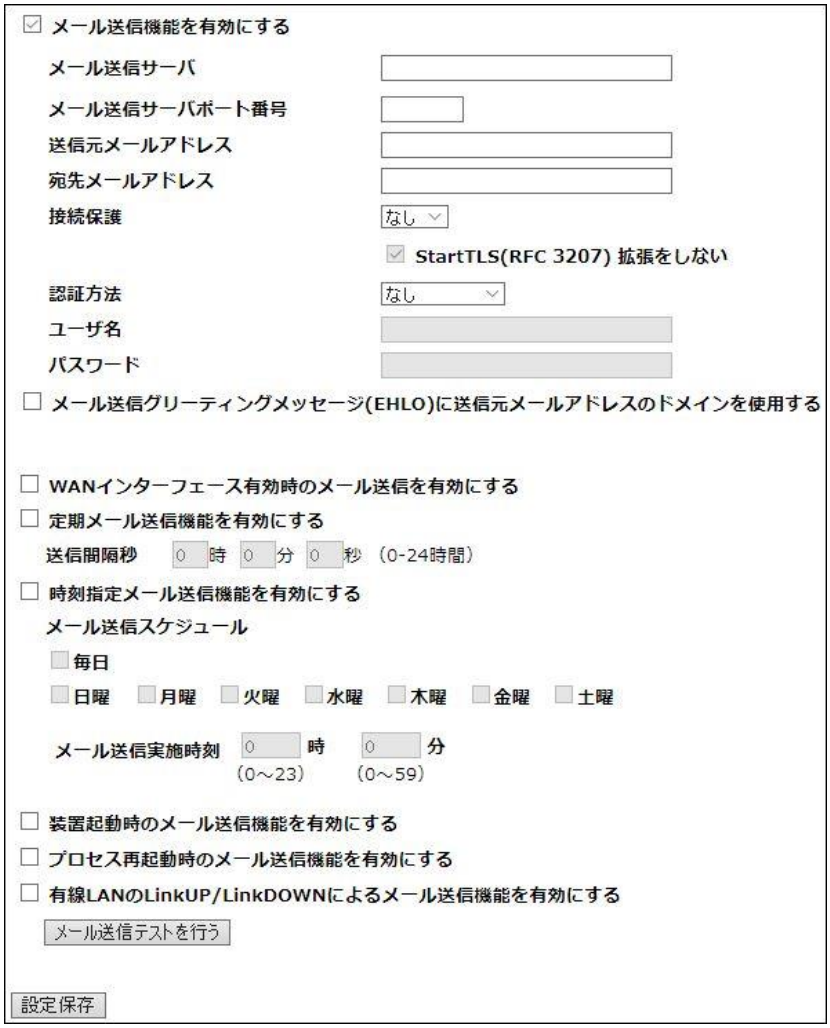
新機能「メール送信設定」について説明します。

確 認	メール送信機能を使用する場合、「NTP クライアント機能」を有効にする事を推奨します。 日時情報が合っていない状態でメールを送信すると、送信日時が不正なメールとしてメールサーバーに拒否される事がありますのでご注意下さい。

設定メニューの「マネージメント」より「メール送信設定」をクリックして下さい。



「メール送信設定」画面が開きます。



■メール送信機能を有効にする(チェックボックス)
メール送信機能を利用する場合、チェックを入れて下さい。

■メール送信サーバー
メール送信サーバーのアドレスを入力して下さい。

■メール送信サーバーポート番号
メール送信サーバーのポート番号を入力して下さい。

■送信元メールアドレス
送信元のメールアドレスを入力して下さい。
メールはここで設定したメールアドレスから送信されます。

■宛先メールアドレス
送信先のメールアドレスを入力して下さい。
メールはここで設定したメールアドレス宛てに送信されます。

■接続保護
SMTP サーバーへの接続保護を選択して下さい。
なし　:暗号化しません。
TLS　:暗号化に TLS を使用します。

■StartTLS (RFC 3207)拡張をしない(チェックボックス)
StartTLS 拡張を行わない場合チェックを入れて下さい。

■認証方法
SMTP の認証方法を選択して下さい。
なし　:認証しません。
平文　:平文で認証します。
CRAM-MD5　:CRAM-MD5 で認証します。

■ユーザー名、パスワード
SMTP 認証のためのユーザー名、パスワードを入力して下さい。

■メール送信グリーティングメッセージ(EHLO)に送信元メールアドレスのドメインを使用する(チェックボックス)
SMTP 接続時に送信元の名前解決を行う必要がある場合、チェックを入れて下さい。

■WAN インターフェース有効時にメール送信を行う(チェックボックス)
WAN 側回線接続時にメールを送信する場合チェックを入れて下さい。

確 認	有線 WAN 接続で IP アドレス固定設定時はメール送信されません。

■定期メール送信機能を有効にする(チェックボックス)
定期的にメールを送信する場合チェックを入れて下さい。
送信間隔秒に送信間隔を入力して下さい。

■時刻指定メール送信機能を有効にする(チェックボックス)
特定のスケジュールでメールを送信する場合チェックを入れて下さい。
・毎日
→毎日送信します。
・日曜～土曜
→曜日を指定して送信します。
・メール送信実施時刻
→送信を実行する時刻を入力して下さい。

確 認	「時刻指定メール送信機能」は、「NTP クライアント機能」による時刻情報取得が正常に行われた場合にのみ動作します。

■装置起動時のメール送信を有効にする(チェックボックス)
システム再起動時にメールを送信する場合チェックを入れて下さい。

■プロセス再起動時のメール送信を有効にする(チェックボックス)
プロセス再起動時にメールを送信する場合チェックを入れて下さい。

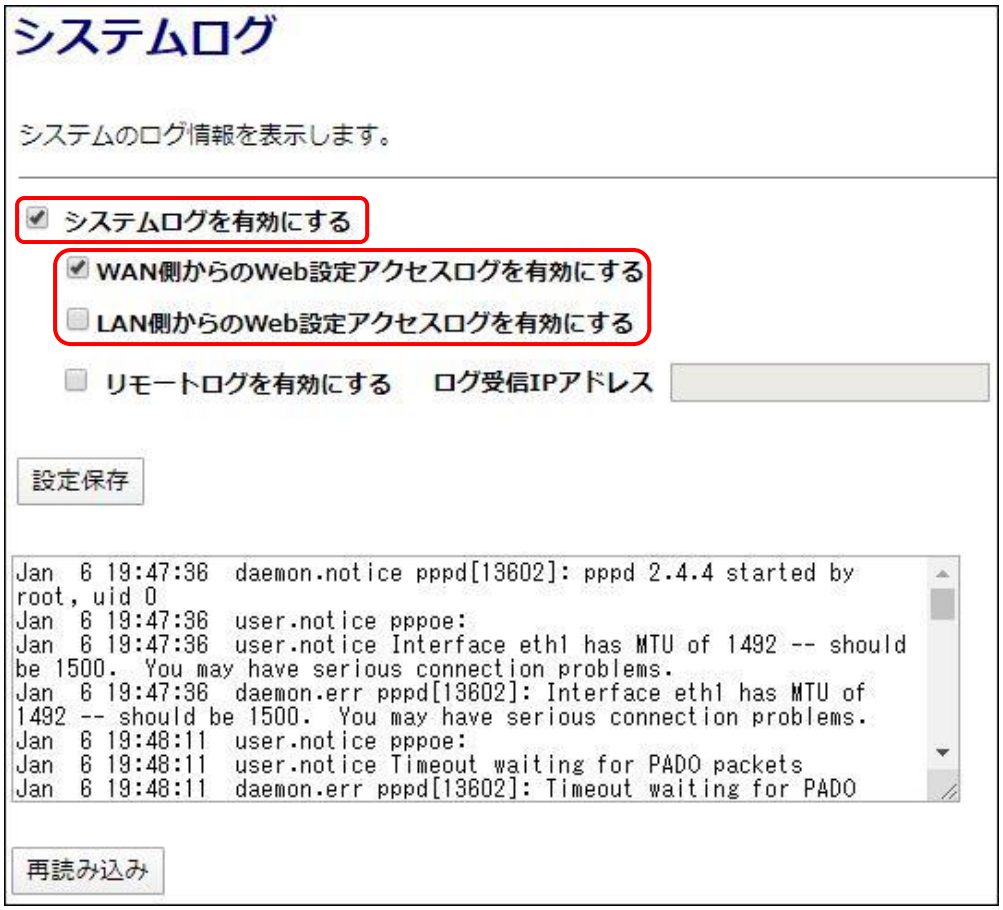
■有線 LAN の LinkUP/LinkDOWN によるメール送信を有効にする(チェックボックス)
有線 LAN ポートのリンクアップ/リンクダウン時にメールを送信する場合チェックを入れて下さい。

■メール送信テストを行う(ボタン)
メール送信テストを行うためのボタンです。

15.システムログ

システムログ機能の追加・変更された項目について説明します。

設定メニューの「マネージメント」より「システムログ」をクリックして下さい。



■システムログを有効にする（チェックボックス）

システムログの工場出荷値設定を「無効」から「有効」に変更しました。

■WAN 側からの Web 設定アクセスログを有効にする（チェックボックス）

WAN 側から設定画面へのアクセスがあった際に、アクセスログを表示します。

■LAN 側からの Web 設定アクセスログを有効にする（チェックボックス）

LAN 側から設定画面へのアクセスがあった際に、アクセスログを表示します。

16.ファームウェア更新設定

ファームウェア更新機能で追加された項目について説明します。

設定メニューの「マネージメント」より「ファームウェア更新」をクリックして下さい。

「タイマー自動ファームウェア更新機能を有効にする」設定が追加されました。

確 認	「タイマー自動ファームウェア更新機能」を利用するには、別途バージョンアップサーバーをご用意頂く必要があります。
	「タイマー自動ファームウェア更新機能」は、「NTP クライアント機能」による時刻情報取得が正常に行われた場合にのみ動作します。

■タイマー自動ファームウェア更新機能を有効にする（チェックボックス）

タイマー自動ファームウェア更新機能を使用する場合、チェックを入れて下さい。

■ファームウェアダウンロード URL

バージョンアップサーバーの URL を入力します。

■スケジュール

ファームウェア更新確認を行うスケジュールを設定します。
更新ファイルがある場合はファームウェア更新を実施します。

・毎日
→毎日更新確認します。
・日曜～土曜
→曜日を指定して更新確認します。
・更新実施時刻
→更新確認を実行する時刻を入力して下さい。

タイマー自動ファームウェア更新機能の設定を変更した場合、[設定保存]ボタンをクリックして下さい。

17.無線 LAN 拡張設定

「無線 LAN 拡張設定」画面で追加された項目について説明します。

無線 LAN 設定の拡張設定に「無線 LAN/有線 LAN 間　通信遮断」を追加しました。

■無線 LAN/有線 LAN 間　通信遮断

無線 LAN と有線 LAN ポート間の通信遮断の有効/無効を切り替えます。
工場出荷値は「無効」(通信可能)です。

【ファームウェア V3.00.00 補足説明書　以上】