

通信モジュール内蔵 無線 LAN 対応 IoT ゲートウェイ

MR-GM5A

ユーザーズマニュアル



はじめに

通信モジュール内蔵 無線 LAN IoT ゲートウェイ MR-GM5A をお買い上げ頂き、誠にありがとうございます。

本マニュアルは MR-GM5A ユーザーズマニュアルです。

本製品を正しくお使い頂くために、本書をよくお読み下さい。

また、本書は保証書とともに大切に保管して下さい。

以下の製品名は米国 Microsoft Corporation の米国およびその他の国における商標です。

Microsoft® Windows® 11 Operating System

Microsoft® Windows® 10 Operating System

その他、本書に記載されている会社名、商品名は各社の商標または登録商標です。

■本製品のご利用に当たって以下の項目をあらかじめご了承下さい。

- ご使用の際は取扱説明書にしたがって正しい取り扱いをして下さい。
- 本製品を使用できるのは日本国内のみです。本製品を海外で使用された場合、当社は一切その責任を負いません。
This equipment is designed for use in Japan only and cannot be used in any other country.
- 本製品の故障、誤動作、不具合あるいは天災や停電等の外的要因によって発生した、純粋経済損失、精神的損害等につきましては、当社は一切その責任を負いません。
- 取扱説明書の内容については、万全を期して作成しておりますが万一不審な点、記載漏れ等、お気付きの点がありましたら、ユーザーサポートへご連絡下さい。
- 本製品の取扱説明書の瑕疵(誤記等)によって発生した障害、損害についての保証の範囲は、本製品の修理、交換に限ります。
- 本製品を運用した結果の影響については、当社は一切その責任を負いません。
- ソフトウェア仕様、ハードウェア仕様、外観、付属品および、取扱説明書などの内容は将来予告なしに変更することがあります。
- 商品に搭載されているソフトウェアの解析(逆コンパイル、逆アセンブル、リバースエンジニアリングなど)、コピー、転売、改造を行うことを禁止します。
- 本説明書中の設定画面は開発中のものです。実際の仕様と異なる場合があります。

■本書中のマークについて

本製品を安全に正しく使用頂き、お客様や財産への損害を防ぐために、以下のマークの記されている内容を必ずお読み下さい。

 警告	本表示を無視して誤った取り扱いをすると、人が死亡あるいは重傷を負う可能性が想定される内容を示します。
 注意	本表示を無視して誤った取り扱いをすると、人が傷害を負う可能性が想定される内容、および物的損害の発生が想定される内容を示します。
 お願い	本表示を無視して誤った取り扱いをすると、本製品の本来の性能を発揮出来なかったり、機能停止を招く内容を示します。

■本書中の表記について

- 以下の文字は非常に間違いやすいので注意して下さい。
半角数字「1」(イチ)と半角アルファベット小文字「l」(エル)、半角アルファベット大文字「I」(アイ)
半角数字「0」(ゼロ)と半角アルファベット小文字「o」(オー)、半角アルファベット大文字「O」(オー)
- 本書では一部の語句について略語表記している箇所があります。

本書での表記	正式な呼称
PC	パソコン、コンピュータ、端末等
Windows 11	Microsoft® Windows® 11 Operating System
Windows 10	Microsoft® Windows® 10 Operating System
Windows	上記 2 つのオペレーションシステムの総称

- 以下のマークが付いている箇所は本製品をお使い頂く上で必ず確認または注意して頂きたい項目です。

 確認	ここに記載されている内容を必ず確認・注意して下さい。
---	----------------------------

注意事項

一本製品使用時の注意事項

- 高精度な制御や微弱な信号を取り扱う電子機器の近くでは、本製品の電源をお切り下さい。電子機器が誤動作するなど影響を与える場合があります。

【ご注意頂きたい電子機器の例】

補聴器、植込み型心臓ペースメーカーおよび植込み型除細動器、その他医用電気機器、火災報知器、自動ドア、その他の自動制御機器など

※参考:「医用電気機器への電波の影響を防止するための携帯電話端末等の使用に関する指針」(電波環境協議会[平成9年4月])

- 飛行機内や病院内等、使用を禁止された区域では、本製品の電源をお切り下さい。飛行機内や病院内等、使用を禁止された区域で本装置に電源を供給すると、医用電気機器、高精度な制御や微弱な信号を取り扱う電子機器に影響を与える可能性があります。医療機関内における使用については、各医療機関の指示に従って下さい。
- 自動車内で使用した場合、車載電子機器に影響を与える可能性があります。十分な対電磁波保護がされているか自動車販売店にご確認のうえ、ご使用になることをお奨めします。

一无線 LAN の電波に関する注意事項

- 本製品が使用する周波数帯域では、産業・科学・医療用機器のほか、他の同種無線局、工場の製造ライン等で使用される移動体識別用構内無線局、および免許を要しない特定小電力無線局、アマチュア無線局等(以下、「他の無線局」と略す)が運用されています。万一、本製品と「他の無線局」との間に電波干渉が発生した場合は、速やかに本製品の使用チャンネルを変更するか、使用場所を変えるか、または機器の運用を停止(電波の発射を停止)して下さい。
- 5GHz帯を使用する場合、W52(36、40、44、48ch)、W53(52、56、60、64ch)の屋外での使用は法令により禁じられています。本製品を屋外で使用する場合、無線 LAN1(5GHz)の基本設定で「屋外モード」を「有効」に設定して使用して下さい。

設定方法については、「4-1.無線 LAN1(5GHz)」(27 ページ)を参照して下さい。

屋内とは四方が壁に囲われた建造物の内部の空間をいい、駅のホームや自動車や電車など乗り物の中は屋外の扱いとなりますので注意して下さい。

- 本製品の無線 LAN 機能が使用する電波は、一般家屋で使用されている木材やガラス等は通過しますが、金属は通過しません。コンクリートの壁でも、内部に金属補強材が使われている場合は通過しません。
- ビル内等の比較的広いフロアであっても、フロア内に金属製パーティション等の遮蔽物がある場合、通信できないことがあります。
- 本製品を使用することにより、テレビ、ラジオ、携帯電話等に雑音が入る場合、以下のように対処して下さい。
 - ・本製品の設置場所や向きを変える。
 - ・雑音が入る機器と本製品の距離を離す。
 - ・雑音が入る機器と本製品の電源を、それぞれ別の場所から取る。

一无線 LAN を使用する際の注意事項

- 通信速度最大 1201Mbps(規格値)、867Mbps(規格値)、300Mbps(規格値)、54Mbps(規格値)、11Mbps(規格値)は、IEEE802.11 の無線 LAN 規格で定められたデータ通信速度の最大値であり、実際のデータ通信速度(実効値)ではありません。
- IEEE802.11b、IEEE802.11g および IEEE802.11n を使用する機器が混在している場合は、スループットが低下することがあります。
- 無線 LAN の伝送距離や通信速度は、使用環境や周辺環境により大きく変動します。

ー無線 LAN のセキュリティについてー

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。その反面、電波はある範囲内であれば障害物(壁等)を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

- 通信内容を盗み見られる。
 - 悪意ある第三者が、電波を故意に傍受し、
 - ・ID やパスワード又はクレジットカード番号等の個人情報
 - ・メールの内容
 - 等の通信内容を盗み見られる可能性があります。
- 不正に侵入される。
 - 悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
 - ・個人情報や機密情報を取り出す。(情報漏洩)
 - ・特定の人物になりすまして通信し、不正な情報を流す。(なりすまし)
 - ・傍受した通信内容を書き換えて発信する。(改ざん)
 - ・コンピュータウイルスなどを流しデータやシステムを破壊する。(破壊)
 - 等の行為をされてしまう可能性があります。

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

本製品は工場出荷時に、以下の無線 LAN セキュリティ設定が施されています。

- ・暗号モード: WPA3 Transition
- ・事前共有鍵(暗号キー): 機器ごとに設定済み

お客様がセキュリティ問題発生の可能性を少なくするためには、本製品をご使用になる前に、必ず本製品のセキュリティに関する全ての設定をマニュアルにしたがって行って下さい。

- 参考: 4-1-3.セキュリティ設定(5GHz 無線 LAN)(31 ページ)
- 4-2-3.セキュリティ設定(2.4GHz 無線 LAN)(43 ページ)

無線 LAN セキュリティの設定について、お客様ご自身で対処できない場合には、当社ユーザーサポートセンターまでお問い合わせ下さい。

セキュリティ対策を行わない、あるいは無線 LAN の仕様上、特殊な方法でセキュリティ設定が破られる等により、問題が発生してしまった場合、当社ではこれによって生じた損害に対する責任を負いかねます。

セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様ご自身の判断と責任においてセキュリティに関する設定を行い、製品を使用して下さい。

安全にお使い頂くために

本製品を安全にお使い頂くために、以降の内容を必ずお読み下さい。

ご使用にあたって



警告

本製品は一般のオフィスや家庭用 OA 機器として設計されております。極めて高い信頼性を要求されるシステム(幹線通信機器、電算機システム、医療システム等)では使用しないで下さい。

本製品を医療機器や、心臓ペースメーカー、植込み型除細動器を装着している人の近くで使用しないで下さい。医療機器の誤動作の原因となります。

本製品を飛行機内や病院内等、電波の使用を禁止・制限された区域で使用しないで下さい。飛行機の計器類や医療機器の誤動作の原因となります。

落雷の恐れがある場合は、本製品の使用を直ちに中止し、接続されているケーブルを取り外して下さい。落雷により本製品及び本製品が接続されている機器の故障、発煙、発火の可能性があります。なお、落雷等の天災による故障の場合、保証期間内であっても有償修理となりますので、あらかじめご了承下さい。

本製品から煙が出たり、異臭が発生した場合等、異常状態のまま使用すると、火災、感電の原因となります。その際は電源アダプターをコンセントから外して煙が出なくなる、もしくは異臭が消えることを確認した後、当社ユーザーサポートへご連絡下さい。

本製品を風呂場やシャワー室等、水のかかる場所で使用しないで下さい。漏電して、火災、感電、故障の原因となります。

本製品の近くに花瓶や植木鉢、コップ、化粧品、薬品等の液体が入った容器、または小さな金属等を置かないで下さい。これらの異物が本製品の内部に混入した場合、火災、感電、故障の原因となります。

本製品の内部に水や金属等の異物が混入した場合、すぐに本製品の電源アダプターをコンセントから外した後、当社ユーザーサポートへご連絡下さい。そのまま使用すると火災、感電の原因となります。

電源アダプターを風通しの悪い狭い場所に設置しないで下さい。過熱し、火災や破損の原因となることがあります。

電源アダプター本体を宙吊りに設置しないで下さい。電源プラグと電源アダプター間に隙間が生じ、ほこりによる火災が発生する可能性があります。電源アダプターは容易に抜き差し可能な電源コンセントに差し込んで下さい。

濡れた手で電源アダプターを抜き差ししないで下さい。火災、感電、故障の原因となります。

電源アダプターのプラグにドライバー等の金属が触れないようにして下さい。火災、感電、故障の原因となります。

電源アダプターは必ず付属のものを使用し、それ以外のものは絶対に使用しないで下さい。火災、感電、故障の原因となります。

電源アダプターのケーブルを傷つけたり、無理な力を加えたり、ものを乗せたりすることはお止め下さい。火災、感電、故障の原因となります。

電源アダプターのケーブルが破損した状態(芯線の露出、断線等)のまま使用しないで下さい。火災、感電、故障の原因となります。

電源アダプターは確実に根本まで差し込んで下さい。また、電源アダプターのプラグとコンセントの間のほこりは定期的(半年に1回程度)に取り除いて下さい。そのまま放置すると火災の原因となります。

電源アダプターを抜き差しするときは、必ず電源アダプター本体を持って行って下さい。電源アダプターのケーブルを引っ張るとケーブルが破損し、火災、感電の原因となります。

AC100V の家庭用電源以外では使用しないで下さい。また、たこ足配線をしないで下さい。火災、感電、故障の原因となります。

梱包のポリ袋などは、小さいお子様の手の届く所に置かないで下さい。小さいお子様がかぶったり、飲み込んだりすると、呼吸を妨げる危険があります。

ガソリンスタンドなど、引火、爆発の恐れがある場所では、使用しないで下さい。

本製品を落下させたり、強い衝撃を与えてしまった場合、本製品の電源アダプターをコンセントから外した後、当社ユーザーサポートへご連絡下さい。そのまま使用すると火災、故障の原因となります。

本製品を分解・改造しないで下さい。火災、感電、故障の原因となります。また、故障した場合、保証期間内であっても保証を受けられなくなります。

本体(コネクタ一部)、電源アダプターに液体が入ったりしないよう、また本体(コネクタ一部)、電源アダプター、ケーブル類、コネクタ類を濡らさぬようご注意ください。漏電して火災、感電、故障の原因となります。

本製品の内部や周囲でエアダスターやスプレー等、可燃性ガスを使用したスプレーを使用しないで下さい。引火による爆発、火災の原因となることがあります。

当社がご用意する外部アンテナ以外のアンテナを使用しないで下さい。

当社がご用意する外部アンテナ以外を使用した場合、電波法の規定に抵触する可能性があります。

 注意	<p>本製品の動作中は本製品内部及び外側が熱くなることがあります。本製品のそばにビニール等、熱に弱い物を置かないで下さい。また、本製品を他の機器の上に設置しないで下さい。変色、変形の原因となります。</p>
	<p>本製品の動作中は本製品の内部及び外側が熱くなることがあります。長時間皮膚に接触すると低温やけどの原因となる場合がありますのでご注意下さい。</p>
	<p>本製品を不安定な場所へ設置しないで下さい。また、本製品の上にものを置かないで下さい。バランスが崩れて倒れたり、落下して怪我や本製品の故障の原因となります。</p>
	<p>本製品を壁に取り付けるときは、本製品の重みにより落下しないようにしっかりと取り付け設置して下さい。落下して怪我や本製品の故障の原因となります。</p>
	<p>本製品の上に乗らないで下さい。特に小さなお子様のいるご家庭ではご注意下さい。本製品が破損しケガや感電の原因となります。</p>
	<p>本製品を以下の環境で使用・保管・放置しないで下さい。火災、感電、故障の原因となります。</p> <ul style="list-style-type: none"> ・室内または製品周辺の温度や湿度が極端に高い、または低い場所 ・結露がある場所 ・ほこりが多い場所 ・腐食性ガスが発生する場所 ・不安定な場所 ・直射日光が当たる場所 ・急激な温度変化が起こる場所 ・静電気が発生しやすい場所 ・水などがかかりやすい場所 ・油煙が当たる場所 ・製品周辺に発熱する器具や燃えやすい物がある場所
	<p>本製品の通気孔をふさいだり、重ねて設置しないで下さい。本製品内部に熱がこもり加熱故障、火災の原因となります。</p>
	<p>本製品に各種ケーブルや SIM カードを接続する・外す際は、必ず本製品及び他の機器の電源を OFF にして下さい。感電、故障の原因となります。</p>
	<p>本製品を長期間無人で使用する際は、必ず定期的に保守/点検を行って下さい。</p>
	<p>本製品を長期間ご使用にならないときは、安全のため必ず電源アダプターを電源コンセントから抜いて下さい。</p>
	<p>本製品のお手入れは、電源を切った状態で行って下さい。</p>
	<p>本製品の汚れのお手入れは、柔らかい布で軽く拭き取って下さい。ベンジンやシンナー等の薬品を使用すると、人体に有害な気体が発生したり、本製品の変形や変色の原因となることがあります。</p>
	<p>本製品背面の各コネクタに異物を挿入しないで下さい。感電、故障の原因となります。</p>
	 お願い
<p>本商品とコードレス電話機や電子レンジなどの電波を放射する装置との距離が近すぎると通信速度が低下したり、データ通信が切れる場合があります。また、コードレス電話機の通話にノイズが入ったり、発信・着信が正しく動作しない場合があります。このような場合は、お互いを数メートル以上離してお使い下さい。</p>	
<p>動作中にケーブル類が外れたり、接続が不安定になると、誤動作の原因となり、大切なデータを失うことがあります。動作中はコネクタの接続部に触れることは絶対にしないで下さい。</p>	

セキュリティについて

本製品を使用するにあたり、設定画面へのログイン ID、パスワードを変更することを強く推奨します。

ログイン ID、パスワードを変更しない場合、ネットワーク上の他の機器等から MR-GM5A の設定や情報を見られたり、書き換えられる可能性があります。

【工場出荷値】

ログイン ID: admin パスワード: passwd

これは、セキュリティの面で非常に危険です。

ログイン ID、パスワードを変更することにより、安全に MR-GM5A を使用することができます。

ログイン ID、パスワードの設定方法については、「8-7.ログイン 設定」(135 ページ)を参照して下さい。

内蔵通信モジュールについて

本製品は、電波法に基づく技術基準適合証明、および電気通信事業法に基づく技術適合認定を受けた通信機器を内蔵しております。

1.MR-GM5A の概要.....	1
1-1.主な特長.....	1
1-2.各部の名称.....	3
2.初期設定を行う.....	4
2-1.各機器との接続.....	4
2-2.有線 LAN パソコンで初期設定を行う.....	6
2-2-1.Windows 11/10.....	6
2-3.無線 LAN パソコンで初期設定を行う.....	9
2-3-1.Windows 11/10.....	9
2-4.設定画面へのログオン.....	13
2-4-1.設定画面へのログオン.....	13
2-4-2.設定画面が開かないとき.....	15
2-5.初期設定・内蔵モバイル接続設定例.....	16
3.ステータス画面.....	19
3-1.認証情報.....	19
3-2.システム.....	20
3-3.無線 LAN1、無線 LAN2.....	21
3-4.有線 LAN.....	22
3-5.WAN 回線運用.....	23
3-6.有線 WAN.....	23
3-7.WAN 内蔵モバイル.....	25
3-8.WAN USB モバイル.....	26
4.無線 LAN 設定.....	27
4-1.無線 LAN1 (5GHz).....	27
4-1-1.基本 設定.....	27
4-1-2.拡張 設定.....	29
4-1-3.セキュリティ 設定.....	31
4-1-4.アクセス制御 設定.....	34
4-1-5.サイトサーベイ.....	36
4-1-6.WPS 設定.....	37
4-2.無線 LAN2 (2.4GHz).....	39
4-2-1.基本 設定.....	39
4-2-2.拡張 設定.....	41
4-2-3.セキュリティ 設定.....	43
4-2-4.アクセス制御 設定.....	46
4-2-5.サイトサーベイ.....	48
4-2-6.WPS 設定.....	49
4-3.マルチ SSID 設定例.....	51
4-3-1.基本 SSID の設定.....	52
4-3-2.マルチ SSID1 の設定.....	53
4-3-3.基本 SSID セキュリティ設定.....	55
4-3-4.マルチ SSID1 セキュリティ設定.....	56
4-4.無線 LAN クライアントモード設定.....	57
4-4-1.LAN 設定 (LAN ポート IP アドレスの変更).....	58
4-4-2.DHCP 設定 (DHCP サーバー機能の無効化).....	58
4-4-3.無線 LAN 基本設定 (クライアントモードへ変更).....	59
4-4-4.サイトサーベイから接続する.....	60
4-4-5.手動設定で接続する.....	61

4-5.ユニバーサルリピーターモード設定	63
4-4-1.LAN 設定 (LAN ポート IP アドレスの変更)	64
4-4-2.DHCP 設定 (DHCP サーバー機能の無効化)	64
4-5-3.無線 LAN 基本設定 (ユニバーサルリピーターモードの設定)	65
4-5-4.無線 LAN セキュリティ設定	66
5.ネットワーク設定	68
5-1.LAN 設定	68
5-1-1.LAN ポート IP アドレス設定	68
5-1-2.DHCP サーバー設定	69
5-2.WAN 設定	71
5-2-1.内蔵モバイル設定	72
5-2-2.USB モバイル設定	74
5-2-3.有線 WAN 設定: DHCP	76
5-2-4.有線 WAN 設定: 固定 IP	77
5-2-5.有線 WAN 設定: PPPoE	78
5-2-6.有線 WAN 設定: transix (DS-Lite)	79
5-2-7.有線 WAN 設定: IPoE IPv6	80
5-2-8.有線 WAN 設定: Bridge	81
5-2-9. WAN 設定: 共通設定	82
5-3.IPsec 設定	85
5-3-1.VPN 設定画面	85
5-3-2.VPN 接続先の設定画面	86
5-4.回線冗長化設定 (コールド・スタンバイ)	89
5-4-1.回線冗長化機能 (コールド・スタンバイ方式) の仕様について	89
5-4-2.WAN 設定 (回線冗長化設定)	90
5-5.回線冗長化設定 (ホット・スタンバイ)	92
5-5-1.回線冗長化機能 (ホット・スタンバイ方式) の仕様について	92
5-5-2.WAN 設定 (回線冗長化設定)	93
6.ファイアウォール	95
6-1.IP フィルター 設定	95
6-2.IPv6 フィルター 設定	98
6-3.MAC フィルター 設定	101
6-4.ドメインフィルター 設定	103
6-5.ポートフォワーディング 設定	105
6-6.アクセス制御 設定	108
6-7.DMZ 設定	110
6-8.WAN 側から設定画面へアクセスする場合の設定方法	111
6-9.WAN 側からの Ping 応答を返す場合の設定方法	113
7.付加機能	115
7-1.簡易 DNS 設定	115
7-2.ダイナミック DNS 設定	117
7-3.ルーティング 設定	119
7-4. IPv6 アドレス配布 設定	121
8.マネージメント	122
8-1.システム 設定	122
8-2.時刻情報 設定	123
8-3.メール送信機能 設定	124
8-4.システム ログ	128
8-4-1. システムログ設定	128
8-4-2.システムログ表示例	129
8-5.ファームウェア更新	132

8-6.設定保存・読み込み	134
8-7.ログイン 設定	135
8-8.再起動	136
8-8-1.自動再起動(タイマー再起動)	136
9.仕様	137
10.Q&A	138
11.ユーザーサポート	151
ユーザーサポートについて	151
お問い合わせ頂く際のお願い	151
本製品の修理について	151

1.MR-GM5A の概要

1-1.主な特長

MR-GM5A の主な特長について説明します。

●LTE/3G 対応通信モジュール内蔵

LTE/3G 対応の通信モジュールを内蔵しています。
SIM カードを挿すだけで、複数台の端末からモバイル通信網へ接続する事ができます。

●有線 WAN 対応

有線ブロードバンド回線で利用する事ができます。
DHCP クライアント接続、PPPoE クライアント接続、IP アドレス固定接続に対応しています。

●USB ポート搭載

USB タイプのモバイルデータカードを接続して利用する事ができます。

●IPv6 (IPv6 over IPv4) 対応

transix (DS-Lite 方式) に対応しています。(有線 WAN ポートのみ)
より高速な IPv6 インターネット通信を利用する事ができます。

●回線監視機能

設定した宛先に定期的に PING による応答確認や HTTP アクセスによる応答確認を行い、回線状態の監視を行うことができます。
応答が得られなかった場合に回線の再接続を行う、通信モジュールを再起動する等の動作を行い、接続状態を復旧します。

●回線冗長化機能

プライマリー接続、セカンダリー接続を設定し、回線監視失敗時に接続を切り替える事ができます。
回線障害発生時に WAN 側接続モードを切り替えるコールド・スタンバイ方式と、2 種類の WAN 側接続を同時に行い回線障害発生時にゲートウェイを切り替えるホット・スタンバイ方式に対応しています。

●VPN (IPsec) 通信対応

IPsec 接続機能を搭載していますので、セキュアな拠点間通信環境を構築する事が可能です。

●無線 LAN 対応

無線 LAN 通信規格として 2.4GHz 帯 (IEEE 802.11b/g/n) のほか、5GHz 帯 (IEEE802.11 a/n/ac/ax) に対応しています。
※接続可能な無線 LAN 端末台数は、5GHz 帯、2.4GHz 帯それぞれに最大 31 台となります。

●Wi-Fi6 (IEEE802.11ax) 対応

Wi-Fi6 (IEEE802.11ax) に対応しています。(5GHz 帯のみ)
より高速で安定した無線 LAN 通信が可能です。

●WPA3-SAE (AES)、WPA2-PSK (TKIP/AES)、WPA-PSK (TKIP/AES)、WEP (64/128bit) 対応

無線 LAN セキュリティ方式として、「WPA3-SAE」、「WPA2-PSK」、「WPA-PSK」、「WEP」に対応しています。
WPA3 を利用する事により、より安全でセキュアな無線 LAN 通信が可能です。

●無線 LAN 簡単設定 WPS 搭載

ボタンを押すだけで、無線 LAN 接続設定、無線 LAN セキュリティ設定を自動的に行う「WPS」に対応しています。

●マルチ SSID 対応

5GHz 帯無線 LAN、2.4GHz 帯無線 LAN それぞれに 2 つの SSID を追加することができます。
追加した SSID にそれぞれ別のセキュリティ設定を行う事により、セキュリティの異なる無線 LAN グループを同時に接続することができます。

●無線 LAN クライアント機能

MR-GM5A を無線 LAN クライアントとして、他の MR-GM5A や MR-GM3 (無線 LAN アクセスポイント) に接続することができます。
有線 LAN ポートしか持たない機器を無線 LAN で接続することができます。

※本機能については当社製品 (MR-GM5A、MR-GM3) との接続のみ動作保証します。
他社無線 LAN 製品との接続については、動作保証及びユーザーサポートの対象外です。

●ユニバーサルリピーター機能

MR-GM5A をユニバーサルリピーターモードで動作させることにより、他の MR-GM5A や MR-GM3 (無線 LAN アクセスポイント) の無線 LAN 通信を中継することができます。

※本機能については当社製品 (MR-GM5A、MR-GM3) との接続のみ動作保証します。
他社無線 LAN 製品との接続については、動作保証及びユーザーサポートの対象外です。

●自動再起動機能

設定したスケジュール (曜日・時刻指定・稼働時間) やシステム起動時間で、自動的に再起動させることができます。
無人環境などで、より安定した運用を行うことができます。

●IP フィルター/ドメインフィルター/MAC フィルター機能

特定の IP アドレス、プロトコル、ポート番号の通信、特定のドメイン名宛の通信、特定の MAC アドレスの通信を制限することができます。

●ポートフォワーディング機能

インターネット側 IP アドレス宛の特定の通信を、LAN 内の特定の IP アドレスへ転送することができます。

LAN 内へ転送する際、宛先ポート番号を別のポート番号へ変換することも可能です。

また、全ての通信を LAN 内の特定の IP アドレスへ転送する、DMZ ホスト機能にも対応しています。

●簡易 DNS 機能

ホスト名と IP アドレスを MR-GM5A に登録することにより、MR-GM5A を簡易 DNS サーバーとして使用することが可能です。

●DHCP サーバー機能

LAN 内のパソコンに、IP アドレス等 TCP/IP 設定を自動的に割り当てる事ができます。

また、特定の MAC アドレスに対して特定の IP アドレスを割り当てる「固定 IP アドレス付与機能」にも対応しています。

●DDNS 機能

外部 DDNS (ダイナミック DNS) サービスを利用して、IP アドレスとドメイン名を自動的に結びつけることができます。

※本機能は外部の DDNS サービスを利用します。そのため、サービス提供元の仕様変更やサービス内容の変更により、利用できなくなる場合がありますのであらかじめご了承下さい。

●メール送信機能

MR-GM5A の状態をメールで送信する事ができます。

WAN 側の回線接続時に送信する、定期的な送信する、特定の曜日の特定の時間に送信する等のスケジュール設定も可能です。

●設定画面のログイン ID、パスワード変更可能

設定画面のログインID、パスワードを変更する事が可能です。

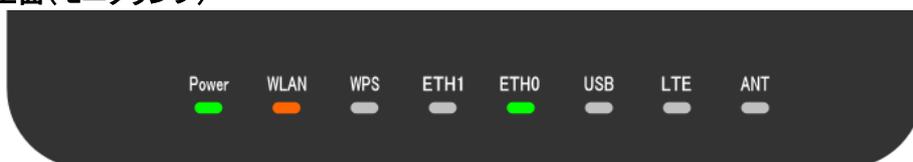
●ギガビットイーサネット対応

ギガビットイーサネットに対応した有線ポートを 2 ポート搭載しています。

1-2.各部の名称

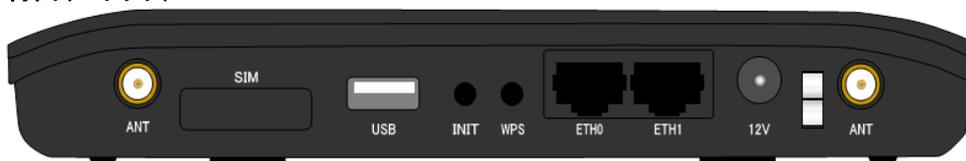
モニタランプとコネクタ類の名称について説明します。

■上面(モニタランプ)



Power	電源が ON のときに点灯します。
WLAN	無線 LAN の状態を表します。 オレンジ点灯:無線 LAN1(5GHz)、無線 LAN2(2.4GHz)、両方が有効 赤点灯:無線 LAN1(5GHz)のみ有効 緑点灯:無線 LAN2(2.4GHz)のみ有効 点滅:無線 LAN クライアントが通信中 消灯:無線 LAN 機能が無効
WPS	本機の WPS 機能が動作中に点滅します。 WPS ボタンを押すと 2 分間点滅します。WPS 接続が完了すると消灯します。
ETH1	有線 LAN ポート 1 のリンク状態を示します。 ※工場出荷値は有線 WAN ポートとして動作しています。
ETH0	有線 LAN ポート 0 のリンク状態を示します。
USB	USB ポートの状態を示します。 USB モバイルデータカードの初期化動作中に点滅します。 USB モバイルデータカードの認識が完了すると点灯します。
LTE	内蔵通信モジュールの動作状態を示します。 内蔵通信モジュールの初期化中・回線接続中に点滅します。 回線接続が完了すると点灯します。
ANT	内蔵モジュールのアンテナ状態を示します。 緑点灯:LTE で通信確立中、アンテナ数 3 本以上 緑点滅:LTE で通信確立中、アンテナ数 2 本以下 赤点灯:3G で通信確立中、アンテナ数 3 本以上 赤点滅:3G で通信確立中、アンテナ数 2 本以下

■背面(コネクタ)



ANT	別売りの内蔵通信モジュール用外部アンテナを接続します。
SIM	SIM カードを挿入するスロットです。SIM スロットは標準 SIM カード(25×15mm)サイズです。
USB	USB タイプのモバイル通信カードを接続するための USB ポートです。
INIT	設定を工場出荷値に戻すためのボタンです。 本製品の電源を入れた状態で、INIT ボタンを 8 秒以上押して下さい。 8 秒以上押したら INIT ボタンを放して下さい。起動が完了すると初期化完了です。
WPS	WPS 接続を行うためのボタンです。 WPS ボタンを押すと WPS ランプが 2 分間点滅します。WPS 接続が完了すると消灯します
ETH0	有線 LAN ポート 0 です。
ETH1	工場出荷値は WAN 側ポートとして動作しています。 有線 LAN パソコンから初期設定を行う場合は、必ず ETH0 ポートに接続して行って下さい。 有線 WAN 設定の接続モードを「Bridge」に設定すると、LAN ポートとして動作します。 詳しくは「5-2-8.有線 WAN 設定:Bridge」(81 ページ)を参照して下さい。
12V	電源アダプター用コネクタです。付属の専用電源アダプターを接続します。

2.初期設定を行う

本製品の初期設定手順について説明します。

2-1.各機器との接続

本製品と各機器との接続方法を説明します。

1.電源アダプター脱落防止クランプと内蔵通信モジュール用外部アンテナ(別売り)の取り付け 電源プラグ左の穴に「電源アダプター脱落防止クランプ」を差し込んで下さい。



「ANT」端子に内蔵通信モジュール用外部アンテナを取り付けて下さい。

「ANT」端子にアンテナを差し込み、右に回して下さい。



注意

外部アンテナを取り付ける際は、コネクター部分を強く締めすぎないようにご注意下さい。
無理な力を加えると、MR-GM5A 本体が破損する恐れがありますのでご注意下さい。
お取り扱いの誤りにより発生した故障については、製品保証期間内であっても有償修理となります。



2.SIM カードの取り付け



注意

SIM カードの抜き差しを行う際は、必ず本製品の電源を落とした後 20 秒程度待ってから行って下さい。
電源を投入したまま抜き差しを行うと、SIM カードが破損する恐れがありますのでご注意下さい。
SIM カードの抜き差しを行う際は、SIM カードの接点面(金属部分)に触れないように注意して下さい。
SIM カードの接点面を直接接触すると手脂やほこりなどが付着し、SIM カードの接触不良が発生したり、SIM カードが破損する恐れがありますのでご注意下さい。
SIM カードは MR-GM5A 本体に対して水平に抜き差しして下さい。
斜めに差す等、強引に抜き差しを行うと、MR-GM5A 本体や SIM カードが破損する恐れがありますのでご注意下さい。お取り扱いの誤りにより発生した故障については、製品保証期間内であっても有償修理となります。

SIM カードを利用する場合は、ゴムカバーを外し、SIM カードスロットに SIM カードを挿入して下さい。

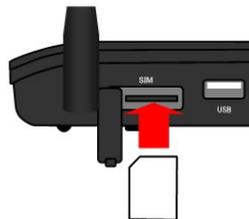
1)ゴムカバーの右側をつまみ
ゴムカバーを開けて下さい。



3)ゴムカバーを閉めて下さい。



2) SIM カードの切り欠き側を先にして、接点面を下に向けて差し込んで下さい。
(SIM カードの向きを間違えないようにご注意下さい。)
SIM カードはカチッと音がするまで差し込んで下さい。

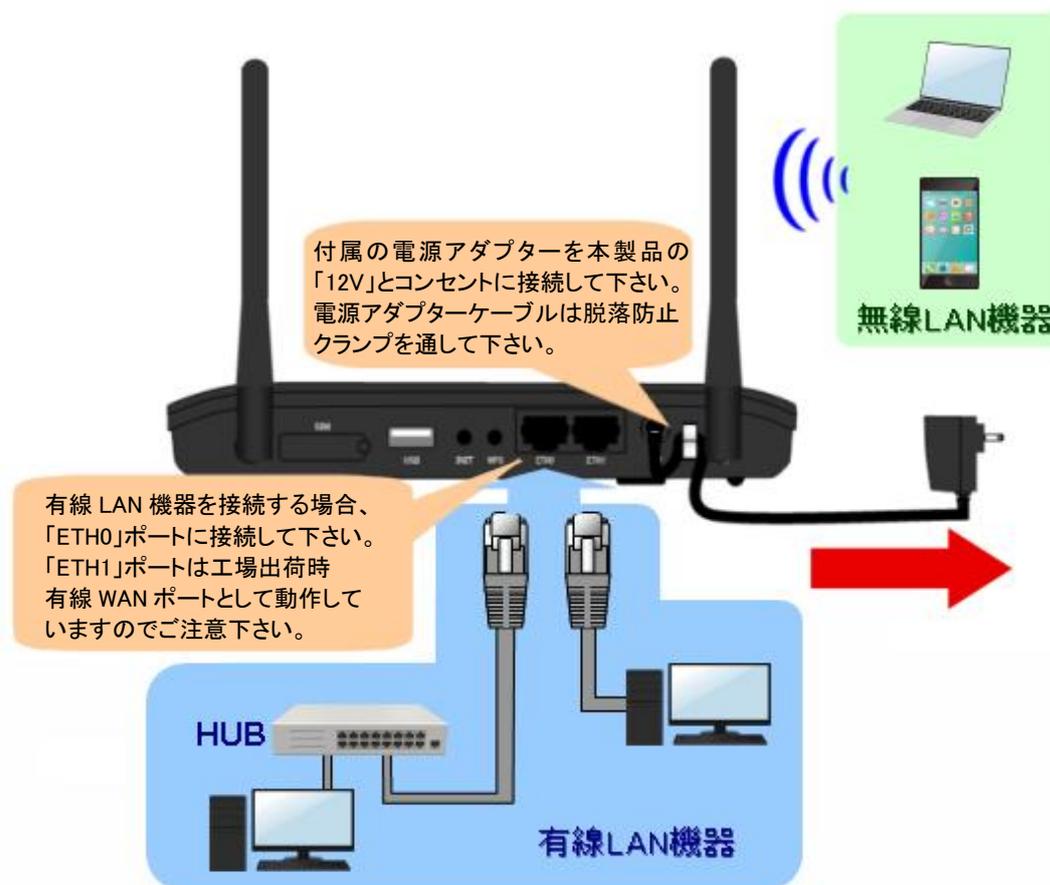


確認

SIM スロットは標準 SIM カード(25×15mm)サイズです。

3.各機器との接続

以下のように各機器と接続を行って下さい。



 警告	必ず付属の専用電源アダプターを使用して下さい。 専用電源アダプター以外を使用すると、発煙、感電、火災、または製品の誤動作や故障の原因となります。
	電源アダプターケーブルを脱落防止クランプに通す際は、ケーブルに余裕を持たせて下さい。 無理な力を加えると、本体や電源アダプターが破損する恐れがありますのでご注意下さい。

 確認	初期設定は必ず「ETH0」ポートに接続したパソコンから行って下さい。 「ETH1」ポートは工場出荷値、有線 WAN ポートとして設定されています。 有線 WAN 設定の接続モードを「Bridge」に設定すると、LAN ポートとして動作します。 詳しくは「5-2-8.有線 WAN 設定: Bridge」(81 ページ)を参照して下さい。
---	---

4.LEDの確認

「Power」、「WLAN」(※1)、「ETH0ポート」(※2)のLEDが点灯している事を確認して下さい。



※1:無線 LAN 機能を無効にしている場合、WLAN は点灯しません。(工場出荷値有効)

※2:有線 LAN パソコンを接続していない場合、ETH0 は点灯しません。

以上で各機器との接続は完了です。

■有線 LAN パソコンで初期設定を行う場合
「2-2.有線 LAN パソコンで初期設定を行う」(6 ページ)へ進んで下さい。

■無線 LAN パソコンで初期設定を行う場合
「2-3.無線 LAN パソコンで初期設定を行う」(9 ページ)へ進んで下さい。

2-2.有線 LAN パソコンで初期設定を行う

パソコンの設定について説明します。
以降 Windows を例に説明します。

はじめに

ご利用のパソコンにイーサネットボード(ネットワークカード)が正しくセットアップされているか確認して下さい。
確認方法については、各 OS(オペレーティングシステム)のマニュアルやイーサネットボードのマニュアル等を参照して下さい。

各 OS(オペレーティングシステム)の設定画面は、バージョンアップ等により変更となる場合があります。

2-2-1.Windows 11/10

以下の手順で設定を行って下さい。

- ① Windows を起動して下さい。

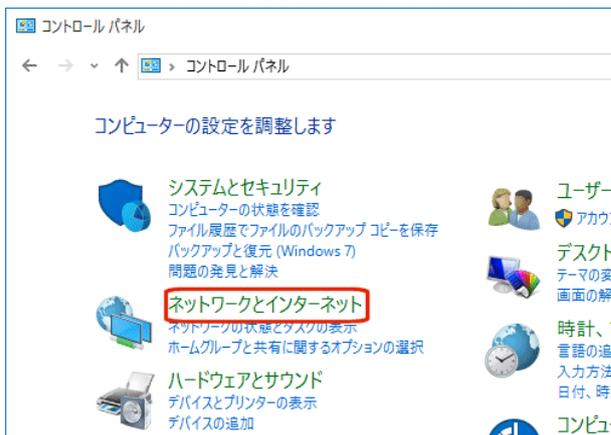


Administrator(管理者)権限のあるユーザーアカウントでログオンして下さい。

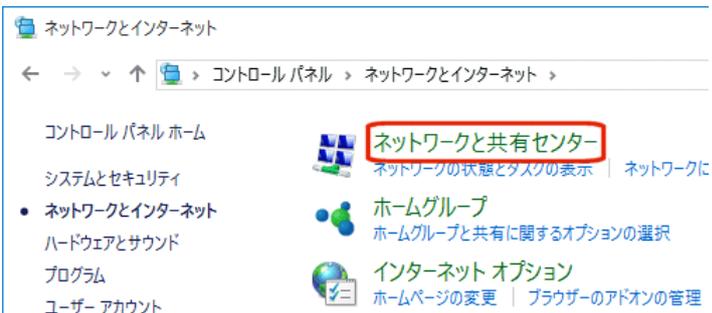
- ②「デスクトップ」を表示して下さい。

- ③[スタートメニュー]→[すべてのアプリ]→「Windows ツール」(Windows システムツール)→[コントロールパネル]をクリックして下さい。

- ④[コントロールパネル]が開きますので、[ネットワークとインターネット]をクリックして下さい。



- ⑤[ネットワークとインターネット]が開きますので、[ネットワークと共有センター]をクリックして下さい。



〈次ページへ進んで下さい〉

⑥ [ネットワークと共有センター]が開きますので、[イーサネット]をクリックして下さい。

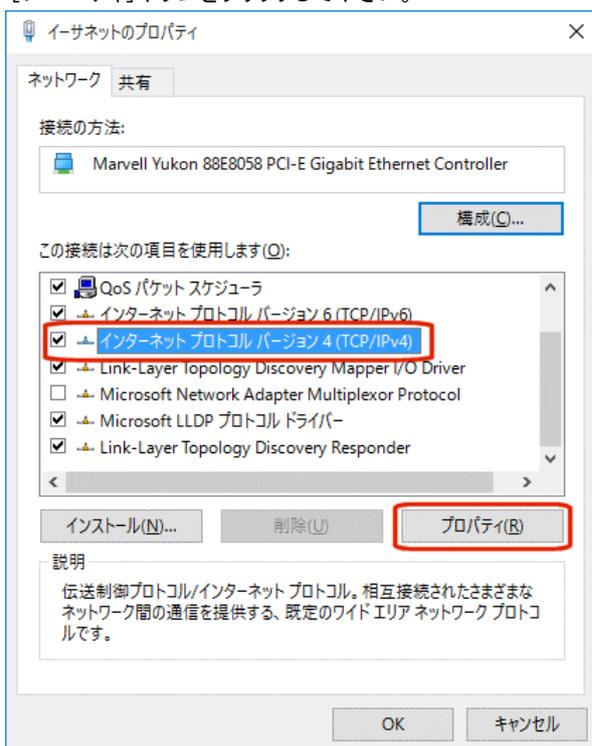


⑦ [イーサネットの状態]が開きますので、[プロパティ]ボタンをクリックして下さい。

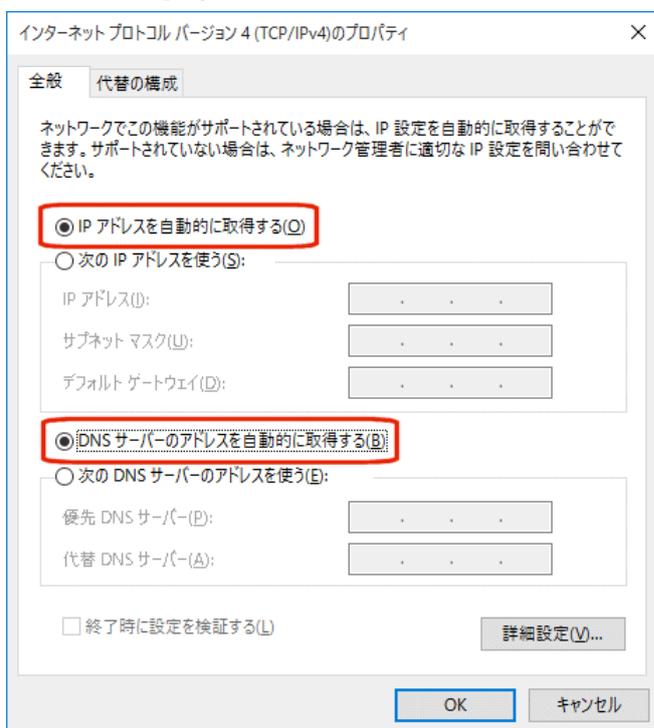


<次ページへ進んで下さい>

- ⑧ [イーサネットのプロパティ]が開きますので、一覧の中の[インターネット プロトコル バージョン 4(TCP/IPv4)]を選択して、[プロパティ]ボタンをクリックして下さい。



- ⑨ [IP アドレスを自動的に取得する]、及び [DNS サーバーのアドレスを自動的に取得する]を選択して、[OK]ボタンをクリックして下さい。



各画面で[OK]ボタンをクリックして下さい。

以上で設定は完了です。

「2-4.設定画面へのログオン」(13 ページ)へ進んで下さい。

2-3.無線 LAN パソコンで初期設定を行う

無線 LAN のパソコンで初期設定を行う場合の、パソコンの設定について説明します。
以降 Windows を例に説明します。

はじめに
ご利用のパソコンに無線 LAN アダプターが正しくセットアップされているか確認して下さい。 確認方法については、無線 LAN アダプターのマニュアル等を参照して下さい。
本項目では、各 OS(オペレーティングシステム)の標準の無線 LAN 接続について説明しています。 無線 LAN アダプターに付属の無線 LAN クライアントソフト(ユーティリティソフト)を利用する場合は、無線 LAN アダプターのマニュアル等を参照して下さい。
OS(オペレーティングシステム)の設定画面は、バージョンアップ等により変更となる場合があります。

2-3-1.Windows 11/10

以下の手順で無線 LAN 接続を行って下さい。

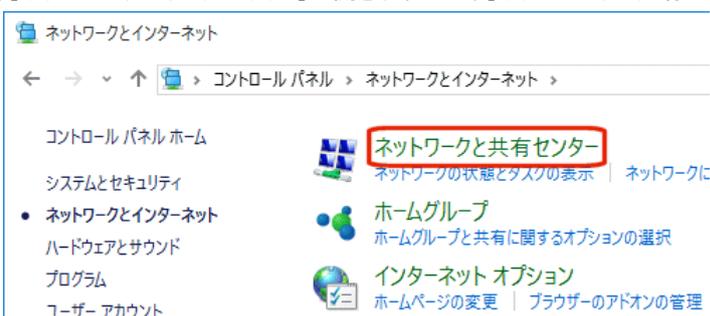
- ①Windows を起動して下さい。

	Administrator(管理者)権限のあるユーザーアカウントでログオンして下さい。
---	---

- ②「コントロールパネル」を開いて下さい。
③[ネットワークとインターネット]をクリックして下さい。



- ④[ネットワークとインターネット]が開きますので、[ネットワークと共有センター]をクリックして下さい。

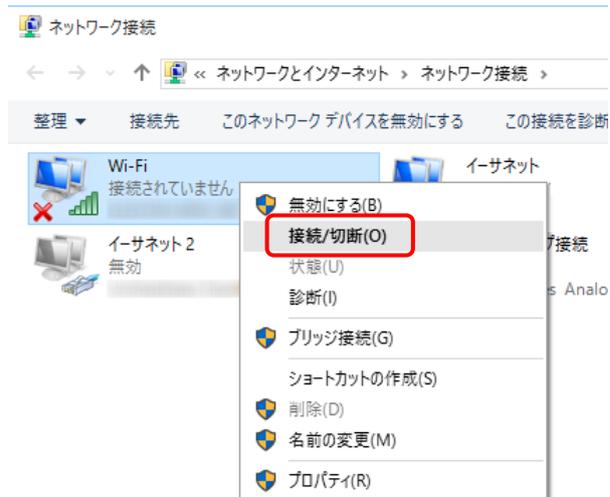


〈次ページへ進んで下さい〉

⑤[ネットワークと共有センター]が開きますので、[アダプターの設定の変更]をクリックして下さい。



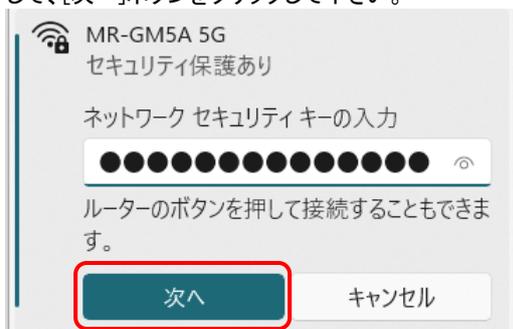
⑥[Wi-Fi]アイコンを右クリックして、[接続/切断]を選択して下さい。



⑦Wi-Fi ネットワークのリストが表示されますので、「MR-GM5A 5G」もしくは「MR-GM5A 2.4G」をクリックし、[接続]ボタンをクリックして下さい。（「自動的に接続」は必要に応じてチェックを入れて下さい。）

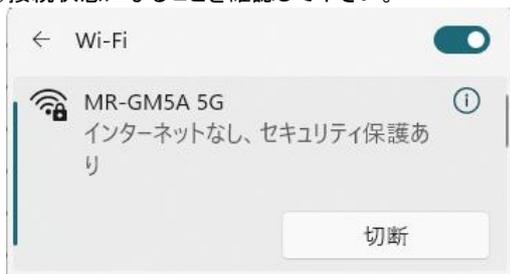


⑧セキュリティキー（暗号キー）を要求されますので、本製品底面に貼付されているシールに記載されている KEY を入力して、[次へ]ボタンをクリックして下さい。



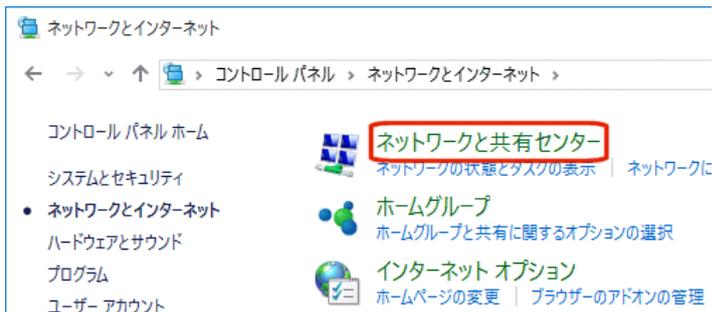
<次ページへ進んで下さい>

⑨接続状態になることを確認して下さい。

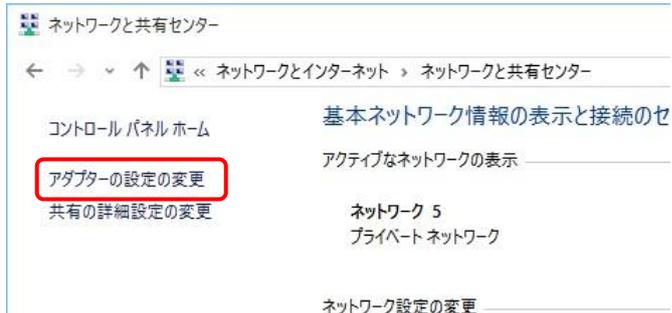


確認 「このネットワークに接続できません」と表示された場合、手順⑧で入力したセキュリティキー（暗号キー）に誤りがないか再度確認して下さい。

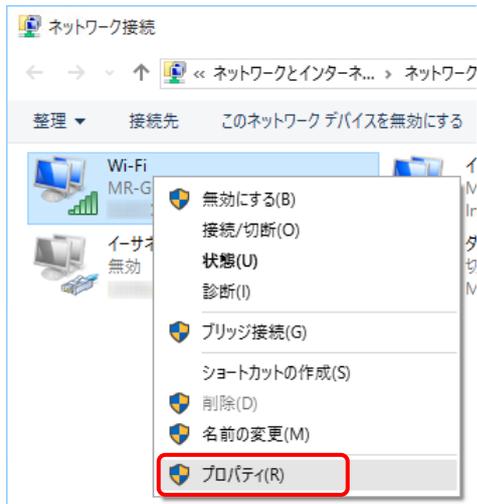
⑩[コントロールパネル]の[ネットワークとインターネット]から[ネットワークと共有センター]をクリックして下さい。



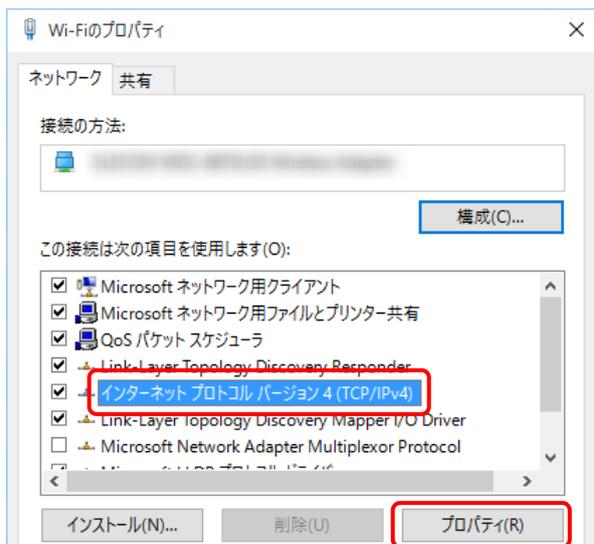
⑪[ネットワークと共有センター]が開きますので、[アダプターの設定の変更]をクリックして下さい。



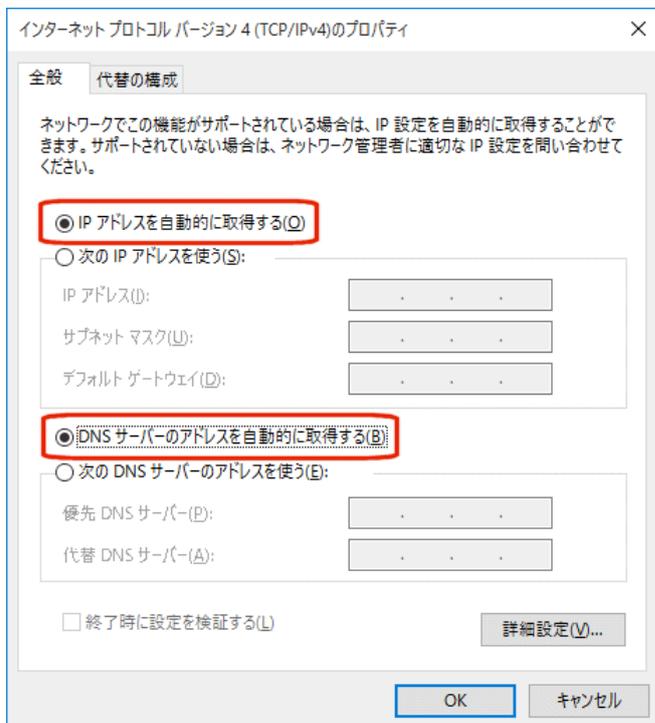
⑫[Wi-Fi]アイコンを右クリックして、[プロパティ]を選択して下さい。



- ⑬ [Wi-Fi のプロパティ]が開きますので、一覧の中の[インターネット プロトコル バージョン 4 (TCP/IPv4)]を選択して、[プロパティ]ボタンをクリックして下さい。



- ⑭ [IP アドレスを自動的に取得する]、及び [DNS サーバーのアドレスを自動的に取得する]を選択して、[OK]ボタンをクリックして下さい。



以上で無線 LAN の接続は完了です。

「2-4.設定画面へのログオン」(13 ページ)へ進んで下さい。

2-4.設定画面へのログオン

設定画面へのログオン方法について説明します。

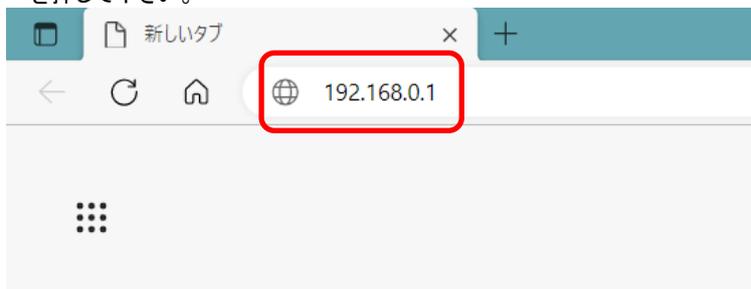
2-4-1.設定画面へのログオン(本ページ)

2-4-2.設定画面が開かないとき(15 ページ)

2-4-1.設定画面へのログオン

WWW ブラウザを起動し、設定画面へログオンして下さい。

①WWW ブラウザのアドレス入力欄に、本製品の LAN 側 IP アドレス(工場出荷値:192.168.0.1)を入力して、Enter(Return)キーを押して下さい。



②ユーザー認証画面が表示されますので、「ユーザー名」に **admin** (半角英小文字)、「パスワード」に **passwd** (半角英小文字)と入力して、[サインイン]ボタンをクリックして下さい。

A screenshot of a user authentication page. The page title is "このサイトにアクセスするにはサインインしてください". Below the title, it says "http://192.168.0.1 では認証が必要となります" and "このサイトへの接続は安全ではありません". There are two input fields: "ユーザー名" (Username) with "admin" entered, and "パスワード" (Password) with "passwd" entered (masked with dots). Both input fields are highlighted with red rectangular boxes. Below the fields are two buttons: "サインイン" (Sign In) in blue and "キャンセル" (Cancel) in grey. The "サインイン" button is also highlighted with a red rectangular box.

確認

「ユーザー名」と「パスワード」を入力する際、半角大文字と小文字を間違えないよう注意して下さい。
(大文字と小文字を間違えると設定画面にログオンすることができません。)

確認

上記のユーザー認証画面が表示されない場合は「2-4-2.設定画面が開かないとき」(15 ページ) を参照して下さい。

- ③以下の警告画面が表示されますので、[確認]ボタンをクリックして下さい。
※以下の画面は初期設定時のみ表示されます。[確認]ボタンをクリックすると下記メッセージは表示されなくなります。

セキュリティ警告：パスワード変更のお願い

初期のパスワードを使用し続けると、不正侵入等のリスクが高まります。
ログイン設定ページからパスワードを変更していただくようお願いします。
また、セキュリティを強化するため、定期的なパスワードの変更もお勧めします。

- ④「ログイン設定」画面が開きますので、ログイン設定を工場出荷値から変更して下さい。

ログイン 設定

このページでは本機の設定画面にアクセスするためのアカウント設定が行えます。

GUIアクセス設定	
GUIポート:	<input style="width: 80%;" type="text" value="80"/>
ユーザー名:	<input style="width: 80%;" type="text" value="admin"/>
パスワード:	<input style="width: 80%;" type="password" value="....."/>

- ⑤[設定保存]ボタンをクリックすると以下の画面が表示されますので[今すぐ再起動]ボタンをクリックして再起動して下さい。

設定は正常に保存されました。

変更を動作に反映させるためには、本機を再起動する必要があります。
今すぐ再起動しますか？

- ⑥再起動のカウントダウンが完了すると、ユーザー認証が再度表示されますので、変更後のユーザー名、パスワードを入力して、[サインイン]ボタンをクリックして下さい。

- ⑦「ステータス」画面(トップ画面)が表示されます。

IoT Gateway**MR-GM5A**

ステータス

- + 無線LAN
- + ネットワーク
- + ファイアウォール
- + 付加機能
- + マネージメント

デバイスステータス

このページでは基本設定と現在ステータスを表示します。

システム
機種名
装置名称
稼働時間
ファームウェア バージョン
ビルド日時
CPU使用率
メモリー使用率

以上で設定画面へのログオン完了です。

- 「2-5.初期設定・内蔵モバイル接続設定例」(16 ページ) へ進んで下さい。

2-4-2.設定画面が開かないとき

設定画面が開けない場合、以下の内容を確認して下さい。

●有線 LAN パソコンの場合、パソコンと ETH0 ポートが正しく接続されていますか？

ETH0 の LED が点灯している事を確認して下さい。

工場出荷時、ETH1 ポートは WAN ポートとして動作しているため、ETH1 ポートから設定画面は開けません。

初期設定は必ず ETH0 ポートから行って下さい。

●本製品に付属の電源アダプターを接続していますか？

他製品の電源アダプター等を接続した場合、本製品は正しく動作しません。

必ず本製品に付属の電源アダプターを接続して下さい。

●パソコンのイーサネットアダプター/無線 LAN アダプターは正常に動作していますか？

パソコンのイーサネットアダプター/無線 LAN アダプターのマニュアルを参照し、正常に動作していることを確認して下さい。

●パソコンにネットワークアダプターが複数セットアップされていませんか？

パソコンにネットワークアダプターが複数セットアップされている場合は、MR-GM5A に接続していないネットワークアダプターを一時的に無効(未使用)にして下さい。

●WWW ブラウザが「プロキシサーバーを使用する」設定になっていませんか？

本製品の設定を行う際は、WWW ブラウザを「プロキシサーバーを使用しない」設定にする必要があります。

WWW ブラウザを「プロキシサーバーを使用しない」設定にして下さい。

●ファイアウォール・セキュリティ対策ソフトウェア等が起動・常駐していませんか？

本製品の設定を行うパソコンにファイアウォール・セキュリティ対策ソフトウェアが起動・常駐している場合、本製品の設定を始める前に一時的に「終了」するか「無効」にして下さい。

ソフトウェアの操作方法(終了・無効にする方法、ファイアウォール機能を停止する方法等)については、ソフトウェアのマニュアルを参照して下さい。

●WWW ブラウザのキャッシュを削除してみてください。

以下、Microsoft Edge でキャッシュを削除する例です。

- 1.Microsoft Edge 画面右上の[⋯]をクリックして[設定]をクリックして下さい。
- 2.[プライバシー、検索、サービス]をクリックして下さい。
- 3.「閲覧データをクリア」欄の[クリアするデータの選択]ボタンをクリックして下さい。
- 4.「キャッシュされた画像とファイル」にのみチェックを入れ、他のチェックは外して下さい。
- 5.[今すぐクリア]ボタンをクリックして下さい。
- 6.Microsoft Edge を再起動し、再度設定画面にログオンできるか確認して下さい。

2-5.初期設定・内蔵モバイル接続設定例

内蔵モバイルを使用して接続する設定例について説明します。

	本項目では、内蔵モバイルでの基本的な接続設定のみを説明しています。
	有線WANポートやUSBモバイルを使用する場合は、「5-2.WAN 設定」(71ページ)を参照して下さい。

①ネットワークから「WAN 設定」をクリックして下さい。



スクリーンショットは、左側のメニューで「WAN 設定」が赤い枠で囲われており、右側の「WAN 設定」画面が示されています。右側の画面には「WAN回線運用」セクションがあり、「WANバックアップ:」が「無効」に設定されています。また、「WAN回線設定」ボタンがあり、「有線WAN」「内蔵モバイル」「USBモバイル」の3つのボタンがあります。赤い注釈が「各WAN回線設定ボタンを押下すると、このページで変更」とあります。

②「WAN 設定」画面が開きますので、「WAN 回線設定」の[内蔵モバイル]ボタンをクリックして下さい。



スクリーンショットは「WAN 設定」画面の「WAN回線設定」ボタンが赤い枠で囲われており、「内蔵モバイル」ボタンが選択されている状態を示しています。赤い注釈が「各WAN回線設定ボタンを押下すると、このページで変更した内容は保存されません。」とあります。

③「内蔵モバイル設定」画面が開きます。
「内蔵モバイル WAN」を「有効」にして下さい。



スクリーンショットは「内蔵モバイル設定」画面で、「内蔵モバイル WAN:」の「有効」ラジオボタンが赤い枠で囲われており、選択されている状態を示しています。その他の項目には「接続先:」のプルダウンメニュー、ユーザー名とパスワードの入力欄、APNの入力欄、CIDのプルダウンメニュー（値は1）、および発信先電話番号の入力欄（値は*99***1#）があります。

〈次ページへ進んで下さい〉

④以下の設定を行って下さい。

内蔵モバイル設定	
このページでは内蔵モバイルによるWAN接続設定が行えます。	
内蔵モバイル WAN:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
接続先:	<input type="text" value=""/>
ユーザー名:	<input type="text" value=""/>
パスワード:	<input type="text" value=""/>
APN:	<input type="text" value=""/>
CID:	<input type="text" value="1"/>
発信先電話番号:	<input type="text" value="*99***1#"/>

■接続先

利用する契約プラン名を選択して下さい。

契約プランを選択すると、ユーザー名、パスワード、APN、CID、発信先電話番号が自動的に設定されます。

任意のユーザー名、パスワード、APN、電話番号を設定する場合は「その他」を選択して下さい。

■ユーザー名、パスワード、APN、CID、発信先電話番号

接続先で契約プランを選択すると、ユーザー名、パスワード、APN、CID、発信先電話番号が自動的に設定されます。

接続先で「その他」を選択すると、任意の値が設定できます。

	「発信先電話番号」に SIM カードの電話番号は入力しないで下さい。
	「発信先電話番号」は、契約プロバイダの指定が無い場合「*99***1#」(初期値)のままご利用下さい。
	接続情報に関する最新情報は以下のサイトをご参照下さい。
	MR-GM5A 内蔵通信モジュール設定情報
	https://www.mrl.co.jp/products/gm5a/gm5a_series_sim/

⑤設定が完了しましたら、画面一番下へスクロールして[設定]ボタンをクリックして下さい。

DNS:	<input type="text" value="自動取得"/>
プライマリー DNSサーバー:	<input type="text" value=""/>
セカンダリー DNSサーバー:	<input type="text" value=""/>
接続待ち時間:	<input type="text" value="0"/> 時 <input type="text" value="0"/> 分 <input type="text" value="10"/> 秒
接続リトライ:	<input type="text" value="5"/>
内蔵モバイルから時刻を取得:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
電波強度取得間隔:	<input type="text" value="60"/> (0~3600秒)
電波強度不足検出回数:	<input type="text" value="3"/> (1~100回)
電波強度ログ出力間隔:	<input type="text" value="60"/> (1~3600回)
<input checked="" type="button" value="設定"/>	<input type="button" value="戻る"/>

	本画面で表示される他の設定項目の説明については、「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。
---	---

〈次ページへ進んで下さい〉

⑥「WAN 設定」画面に戻りますので、「プライマリー接続モード」で「内蔵モバイル」を選択して下さい。

WAN 設定	
このページではWANインターフェースの設定が行なえます。	
WAN回線運用	
WANバックアップ	無効
プライマリー接続モード	内蔵モバイル
セカンダリー接続モード	無効
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	<input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>

各WAN回線設定ボタンを押下すると、このページで変更した内容は保存されません。

⑦画面一番下へスクロールして[設定保存]ボタンをクリックして下さい。

NAPTセッション設定	
UDPセッション時間(単方向)	30 (0~3600秒)
UDPセッション時間(双方向)	180 (0~3600秒)
IP変換セッション数	15420 (2000~20000)
<input type="button" value="設定保存"/>	

⑧以下の画面が表示されますので、[今すぐ再起動]ボタンをクリックして下さい。

設定は正常に保存されました。
変更を動作に反映させるためには、本機を再起動する必要があります。 今すぐ再起動しますか？
<input type="button" value="今すぐ再起動"/> <input type="button" value="後で再起動"/>

⑨以下のカウントダウン画面が表示されますので、画面が切り替わるまでお待ち下さい。

システム再起動中です。しばらくお待ちください。 56
本機を再起動しています。
1分程度待っても画面が表示されない場合は、Webブラウザを閉じてから再度アクセスしてください。 LANインターフェースのIPアドレスを変更した場合は、新しい設定に合わせたIPアドレスにアクセスしてください。

⑩「ステータス」画面(トップ画面)に戻りましたら設定は完了です。

本体の「LTE」ランプが点滅から点灯状態に変わりましたら回線接続完了です。
インターネット接続が可能な事を確認して下さい。

ETH1ポートをLANポートとして使用する場合、以下の設定を行って下さい。
①「ネットワーク」→「WAN 設定」をクリックして、「WAN 回線運用」欄の[有線 WAN]ボタンをクリックして下さい。
②「接続モード」で「Bridge」を選択して[設定]ボタンをクリックして下さい。
③「WAN 設定」画面に戻りますので[設定保存]ボタンをクリックし、[今すぐ再起動]ボタンをクリックして下さい。

3.ステータス画面

ステータス画面で表示される項目について説明します。

3-1.認証情報

デバイスステータス
このページでは基本設定と現在ステータスを表示します。

システム	
機種名	MR-GM5A-L1
装置名称	MR-GM5A
稼働時間	1:00

認証情報

[認証情報]ボタンをクリックすると、本製品の認証情報が表示されます。

本体

 **R** 217-241376
 **T** D24-0103001

内蔵モバイル

 **R** 218-458961
 **T** ADF21-0008018

閉じる

3-2. システム

システム		認証情報
機種名	MR-GM5A-L1	
装置名称	MR-GM5A	
稼働時間	1:15	
ファームウェアバージョン	v [REDACTED] (MR001)	
ビルド日時	[REDACTED] JST 2024	
CPU使用率	1%	
メモリー使用率	29%	

機種名	機種名が表示されます。
装置名称	装置名称(任意設定)が表示されます。 装置名称は「8-1.システム 設定」(122 ページ)で設定可能です。
稼働時間	起動してからの経過時間が表示されます。 1時間未満の場合「##min」 1時間以上1日未満の場合「##:##」 1日以上の場合「# days,##:##」と表示されます。
ファームウェアバージョン	ファームウェアバージョンが表示されます。
ビルド日時	ファームウェアがリリースされた日時が表示されます。
CPU 使用率	CPU 使用率が表示されます。
メモリー使用率	メモリー使用率が表示されます。

3-3.無線 LAN1、無線 LAN2

●無線 LAN1、無線 LAN2（無線 LAN1 は 5GHz、無線 LAN2 は 2.4GHz 有効時に表示）

無線LAN1	
動作モード	アクセスポイント
バンド	5 GHz (A+N+AC+AX)
SSID	MR-GM5A 5G
チャンネル番号	36
暗号モード	WPA3 Transition
BSSID	00:10:38: [REDACTED]
接続中クライアント数	0

無線LAN2	
動作モード	アクセスポイント
バンド	2.4 GHz (B+G+N)
SSID	MR-GM5A 2.4G
チャンネル番号	1
暗号モード	WPA3 Transition
BSSID	00:10:38: [REDACTED]
接続中クライアント数	0

動作モード	現在の無線 LAN 動作モードが表示されます。
バンド	現在選択されている無線 LAN のバンド(周波数)が表示されます。
SSID	現在設定されている SSID が表示されます。
チャンネル番号	現在選択されている無線 LAN チャンネル番号が表示されます。
暗号モード	現在選択されている無線 LAN の暗号モード(セキュリティ設定)が表示されます。
BSSID	MAC アドレスが表示されます。
接続中クライアント数	接続している無線 LAN クライアント数が表示されます。

●マルチ SSID 使用時

マルチ SSID 使用時は、基本 SSID の下にマルチ SSID の情報が表示されます。

無線LAN1	
動作モード	アクセスポイント
バンド	5 GHz (A+N+AC+AX)
SSID	MR-GM5A 5G
チャンネル番号	100
暗号モード	WPA3 Transition
BSSID	00:10:38: [REDACTED]
接続中クライアント数	0

無線LAN1 マルチSSID1	
バンド	5 GHz (A+N+AC+AX)
SSID	MR-GM5A 5G VAP0
暗号モード	WPA3 Transition
BSSID	00:10:38: [REDACTED]
接続中クライアント数	0

3-4.有線 LAN

有線LAN	
IPアドレス	192.168.0.1
サブネットマスク	255.255.255.0
MACアドレス	001038
DHCP サーバー	有効
IPv6 アドレス	
IPv6 リンク ローカル アドレス	

IP アドレス	本製品の IP アドレスが表示されます。
サブネットマスク	本製品のサブネットマスクが表示されます。
MAC アドレス	本製品の有線 LAN(ETH0 ポート) MAC アドレスが表示されます。
DHCP サーバー	DHCP サーバー機能の動作状況(有効/無効)が表示されます。
IPv6 アドレス	LAN ポートの IPv6 アドレスが表示されます。 IPv6 設定有効時に表示されます。
IPv6 リンク ローカル アドレス	LAN ポートの IPv6 リンクローカルアドレスが表示されます。 IPv6 設定有効時に表示されます。

3-5.WAN 回線運用

WAN回線運用	
WANバックアップ	ホット・スタンバイ 回線切替
WAN インターフェース	内蔵モバイル設定
DNS サーバー	

WAN バックアップ	回線冗長化のモードを表示します。 回線冗長化未使用の場合は「無効」と表示されます。
WAN インターフェース	現在の WAN インターフェースを表示します。
DNS サーバー	現在参照している WAN 側 DNS サーバーIP アドレスを表示します。
回線切替(ボタン)	回線冗長化を使用時に、プライマリー接続とセカンダリー接続を手動で切り替えます。

3-6.有線 WAN

●DHCP クライアント、固定 IP 接続時

有線WAN	
インターフェース	nas0_0
接続モード	IPoE
IPアドレス	192.168.10.3
ゲートウェイ	192.168.10.1
MACアドレス	00:10:38: [redacted]
IPv6 リンクローカル アドレス	[redacted]
ステータス	接続

インターフェース	「nas0_0」と表示されます。
接続モード	「IPoE」と表示されます。
IP アドレス	WAN ポートの IPv4 アドレスが表示されます。
ゲートウェイ	WAN 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。
IPv6 リンク ローカル アドレス	WAN ポートの IPv6 リンクローカルアドレスが表示されます。 IPv6 設定有効時に表示されます。
ステータス	WAN ポートの接続状態を表示します。

●PPPoE 接続時

有線WAN	
インターフェース	ppp0_nas0_0
接続モード	PPPoE
IPアドレス	[redacted]
ゲートウェイ	[redacted]
MACアドレス	00:10:38: [redacted]
ステータス	接続

インターフェース	「ppp0_nas0_0」と表示されます。
接続モード	「PPPoE」と表示されます。
IP アドレス	WAN ポートの IPv4 アドレスが表示されます。
ゲートウェイ	WAN 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。
ステータス	WAN ポートの接続状態を表示します。

●transix (DS-Lite)接続時

有線WAN	
インターフェース	nas0_0
接続モード	transix (DS-Lite)
ステータス	接続
IPv6 リンクローカルアドレス	
AFTR アドレスモード	自動設定

インターフェース	「nas0_0」と表示されます。
接続モード	「transix (DS-Lite)」と表示されます。
ステータス	WAN ポートの接続状態を表示します。
IPv6 リンク ローカル アドレス	WAN ポートの IPv6 リンクローカルアドレスが表示されます。
AFTR アドレスモード	AFTR アドレスモードを表示します。
AFTR アドレス	AFTR アドレスモードで手動設定を行った場合の AFTR アドレスが表示されます。 AFTR アドレスを手動設定にした場合のみ表示されます。

●Bridge 設定時

有線WAN	
インターフェース	nas0_0
接続モード	Bridged

インターフェース	「nas0_0」と表示されます。
接続モード	「Bridged」と表示されます。

3-7.WAN 内蔵モバイル

WAN 内蔵モバイル				
インターフェース	usb0			
状態	回線接続			
IPアドレス	[REDACTED]			
端末識別番号(IMEI)	[REDACTED]			
SIM識別番号(ICCID)	[REDACTED]			
電話番号	080 [REDACTED]			
回線種別	LTE			
電波強度(アンテナ)	4			
電波強度(RSSI)	-51dBm			
受信電力(RSRP)	-81dBm			
受信品質(RSRQ)	-9dB			
基地局番号(Cell ID)	[REDACTED]			
BAND(ARFCN)	[REDACTED]			
周辺基地局	Cell ID	ARFCN	RSRP	RSRQ
	[REDACTED]	[REDACTED]	-89.00dBm	-15.50dB
	[REDACTED]	[REDACTED]	-89.00dBm	-15.50dB
モジュールファームウェアバージョン	19005.9000.08.02.00.03			

インターフェース	「usb0」と表示されます。
状態	モジュール起動待ち →内蔵通信モジュールが起動中です。 接続処理中 →回線の接続処理中、または回線切断状態です。 回線接続 →回線が接続状態です。
IP アドレス	取得したインターネット側 IP アドレスが表示されます。
端末識別番号(IMEI)	内蔵通信モジュールの端末識別番号が表示されます。
SIM 識別番号(ICCID)	SIM カードの識別番号が表示されます。
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。
回線種別	LTE で接続時は「LTE」と表示されます。 3G で接続時は「3G」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(0~4)を表します。
電波強度(RSSI)	電波強度が表示されます。
受信電力(RSRP)	受信電力が表示されます。
受信品質(RSRQ)	受信品質が表示されます。
基地局番号(Cell ID)	基地局番号が表示されます。
BAND(ARFCN)	LTE の周波数帯(ARFCN frequency)を表示します。
周辺基地局情報	周辺の基地局情報を表示します。
モジュールファームウェアバージョン	内蔵通信モジュールのファームウェアバージョンを表示します。

3-8.WAN USB モバイル

WAN USBモバイル	
インターフェース	ppp2
状態	回線接続
IPアドレス	
電波強度(アンテナ)	4
電波強度(RSSI)	-51dBm

インターフェース	「ppp2」と表示されます。
状態	接続処理中 →回線の接続処理中、または回線切断状態です。 回線接続 →回線が接続状態です。
IP アドレス	取得したインターネット側 IP アドレスが表示されます。
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(0~4)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。

4.無線 LAN 設定

無線 LAN 設定について説明します。

4-1.無線 LAN1 (5GHz)

無線 LAN1 (5GHz) の設定について説明します。



本製品を屋外で使用する場合は、「屋外モード」を「有効」に設定して下さい。

4-1-1.基本 設定

無線 LAN1 (5GHz) の基本設定について説明します。

設定メニューの「無線 LAN」の「無線 LAN1 (5GHz)」より「基本設定」をクリックして下さい。

「無線 LAN1 基本設定」画面が開きます。

<p>ステータス</p> <ul style="list-style-type: none">- 無線LAN- 無線LAN1 (5GHz)<li style="border: 2px solid red;">基本 設定拡張 設定セキュリティ 設定アクセス制御 設定サイトサーベイWPS 設定+ 無線LAN2 (2.4GHz)- ネットワークLAN 設定WAN 設定+ VPN+ ファイアウォール+ 付加機能+ マネージメント	<p>無線LAN1 基本 設定</p> <p>このページでは無線LANの基本的なパラメーターの設定が行えます。</p> <p><input type="checkbox"/> 無線LANを無効にする</p> <table border="1"><tr><td>バンド:</td><td>5 GHz (A+N+AC+AX) ▾</td></tr><tr><td>モード:</td><td>アクセスポイント ▾ マルチSSID設定</td></tr><tr><td>SSID:</td><td>MR-GM5A 5G</td></tr><tr><td>帯域幅:</td><td>80MHz ▾</td></tr><tr><td>サイドバンド制御:</td><td>自動 ▾</td></tr><tr><td>屋外モード:</td><td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効</td></tr><tr><td>チャンネル番号:</td><td>自動(DFS) ▾</td></tr><tr><td>電波出力 (%):</td><td>100% ▾</td></tr><tr><td>帯域:</td><td>自動 ▾</td></tr><tr><td>ブロードキャスト SSID:</td><td><input checked="" type="radio"/> 有効 <input type="radio"/> 無効</td></tr><tr><td>クライアント間通信遮断:</td><td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効</td></tr><tr><td>マルチキャストをユニキャストに変換:</td><td><input checked="" type="radio"/> 有効 <input type="radio"/> 無効</td></tr><tr><td>接続中クライアント数:</td><td>クライアント 表示</td></tr></table> <p><input type="checkbox"/> ユニバーサルリピーター機能を有効にする</p> <p>リピーター SSID: repeater_ssid1</p> <p style="text-align: center;">設定保存</p>	バンド:	5 GHz (A+N+AC+AX) ▾	モード:	アクセスポイント ▾ マルチSSID設定	SSID:	MR-GM5A 5G	帯域幅:	80MHz ▾	サイドバンド制御:	自動 ▾	屋外モード:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	チャンネル番号:	自動(DFS) ▾	電波出力 (%):	100% ▾	帯域:	自動 ▾	ブロードキャスト SSID:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	クライアント間通信遮断:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	マルチキャストをユニキャストに変換:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	接続中クライアント数:	クライアント 表示
バンド:	5 GHz (A+N+AC+AX) ▾																										
モード:	アクセスポイント ▾ マルチSSID設定																										
SSID:	MR-GM5A 5G																										
帯域幅:	80MHz ▾																										
サイドバンド制御:	自動 ▾																										
屋外モード:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効																										
チャンネル番号:	自動(DFS) ▾																										
電波出力 (%):	100% ▾																										
帯域:	自動 ▾																										
ブロードキャスト SSID:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効																										
クライアント間通信遮断:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効																										
マルチキャストをユニキャストに変換:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効																										
接続中クライアント数:	クライアント 表示																										

■無線 LAN を無効にする

無線 LAN 機能を無効にする場合、チェックを入れて下さい。

■バンド

初期値「5GHz (A+N+AC+AX)」のままご利用下さい。

本製品側で周波数を固定する必要がある場合にのみ、以下から選択して下さい。

- | | |
|------------------|-------------------------------|
| 5GHz (A) | :IEEE 802.11a で固定します。 |
| 5GHz (N) | :IEEE 802.11n で固定します。 |
| 5GHz (A+N) | :IEEE 802.11a/n で固定します。 |
| 5GHz (AC) | :IEEE 802.11ac で固定します。 |
| 5GHz (N+AC) | :IEEE 802.11n/ac で固定します。 |
| 5GHz (A+N+AC) | :IEEE 802.11a/n/ac で固定します。 |
| 5GHz (A+N+AC+AX) | :IEEE 802.11a/n/ac/ax で固定します。 |

■モード

ルーターとして利用する場合は、初期値「アクセスポイント」のままご利用下さい。

無線 LAN クライアントモードで使用する場合は、「クライアント」を選択して下さい。

「無線 LAN クライアントモード」については「4-4.無線 LAN クライアントモード設定」(57 ページ)を参照して下さい。

<次ページへ進んで下さい>

4-1-2. 拡張 設定

無線 LAN1 (5GHz) の基本設定について説明します。

設定メニューの「無線 LAN」の「無線 LAN1 (5GHz)」より「拡張 設定」をクリックして下さい。

「無線 LAN1 拡張設定」画面が開きます。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーベイ WPS 設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール + 付加機能 + マネージメント	無線LAN1 拡張 設定 このページでは無線LANの高度なパラメーターの設定が行えます。	
	ビーコン間隔:	<input type="text" value="100"/> (100-1024 ミリ秒)
	DTIM 間隔:	<input type="text" value="1"/> (1-255)
	プリアンブルタイプ:	<input checked="" type="radio"/> Long プリアンブル <input type="radio"/> Short プリアンブル
	ショート ガード インターバル:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	送信ビームフォーミング:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	基本バンド 設定:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 <input type="text" value="Prefer 5GHz"/>
	OFDMA:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	802.11k サポート:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	<input type="button" value="設定保存"/>	

■ビーコン間隔(工場出荷値:100)

無線電波の送出間隔を設定します。

確認 設定値を小さくすると通信品質は上がりますが、他の無線機器と干渉する可能性が高くなります。

■DTIM 間隔(工場出荷値:1)

省電力モードで動作する無線 LAN クライアントに対して、送信待ちデータがあることを伝えるブロードキャストやマルチキャストのメッセージ間隔を設定します。

■プリアンブルタイプ(工場出荷値:Long プリアンブル)

無線 LAN クライアント間のデータ転送エラーを検出する CRC の長さを選択します。

Short プリアンブルは伝送速度を速くすることができますが、旧型の無線 LAN クライアントを使用する場合は、互換性を確保するために「Long プリアンブル」のままご利用下さい。

■ショート ガード インターバル(工場出荷値:有効)

時間差で届くデータの干渉を防ぎます。

確認 ショート ガード インターバルを有効にすることでデータ通信の効率を上げることができますが、反射波の影響を受けやすくなり、データ通信全体のスループットに影響を与える場合があります。

■送信ビームフォーミング(工場出荷値:無効)

送信ビームフォーミングを有効にした場合、ビームフォーミングに対応した機器同士が互いの方向に向けて指向性の高い電波を送りますので、電波強度を向上させる事ができます。

■マルチユーザー MIMO(工場出荷値:無効)

送信ビームフォーミングを有効にした場合に表示されます。

複数の無線 LAN クライアントが同時に通信を行った際の通信速度の低下を抑えます。

■基本バンド(工場出荷値:無効)

無線 LAN1 (5GHz) と無線 LAN2 (2.4GHz) を同一 SSID、セキュリティ設定にして、どちらに優先して接続するか選択します。

確認 有効にすると、選択した無線 LAN 周波数の SSID 設定、セキュリティ設定のみ変更可能となります。(選択していない無線 LAN 周波数の SSID 設定、セキュリティ設定は変更不可となります。)

■OFDMA(工場出荷値:無効)

周波数帯域を複数の帯域に分割して複数の無線 LAN クライアントが同時に通信を行った際の通信速度の低下を抑えます。OFDMA を利用するには、無線 LAN クライアント側も OFDMA に対応している必要があります。

<次ページへ進んで下さい>

■802.11k サポート(工場出荷値:無効)

近隣無線 LAN アクセスポイントの情報を共有する規格です。

これにより、無線 LAN クライアントは、より最適な無線 LAN アクセスポイントへのローミングが可能です。

802.11k を利用するには、無線 LAN クライアント側も 802.11k に対応している必要があります。

■802.11v サポート(工場出荷値:無効)

802.11k サポート有効した場合には表示されます。

無線 LAN アクセスポイントの管理情報を強化する規格です。

これにより、最適な無線 LAN アクセスポイントへのローミングや接続維持の効果が見込まれます。

802.11v を利用するには、無線 LAN クライアント側も 802.11v に対応している必要があります。

■設定保存(ボタン)

設定した内容を保存する場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

4-1-3.セキュリティ 設定

無線 LAN1 (5GHz) の基本設定について説明します。

設定メニューの「無線 LAN」の「無線 LAN1 (5GHz)」より「セキュリティ 設定」をクリックして下さい。

「無線 LAN1 セキュリティ 設定」画面が開きます。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーベイ WPS 設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール + 付加機能 + マネージメント	<h4 style="color: #0056b3;">無線LAN1 セキュリティ 設定</h4> <p style="color: #0056b3;">このページでは無線LANのセキュリティの設定が行えます。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">SSID タイプ:</td> <td>Root AP - MR-GM5A 5G ▾</td> </tr> <tr> <td>暗号モード:</td> <td>WPA3 Transition ▾</td> </tr> <tr> <td>H2E:</td> <td><input checked="" type="radio"/> 可能 <input type="radio"/> 必須</td> </tr> <tr> <td>管理フレーム保護 (802.11w):</td> <td><input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須</td> </tr> <tr> <td>SHA256 暗号:</td> <td><input type="radio"/> 無効 <input checked="" type="radio"/> 有効</td> </tr> <tr> <td>暗号方式:</td> <td><input checked="" type="checkbox"/> AES</td> </tr> <tr> <td>ブロードキャスト暗号鍵 更新間隔:</td> <td><input type="text" value="86400"/></td> </tr> <tr> <td>事前共有鍵:</td> <td><input type="text" value="....."/> <input type="checkbox"/> パスワード表示</td> </tr> </table>	SSID タイプ:	Root AP - MR-GM5A 5G ▾	暗号モード:	WPA3 Transition ▾	H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須	管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須	SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	暗号方式:	<input checked="" type="checkbox"/> AES	ブロードキャスト暗号鍵 更新間隔:	<input type="text" value="86400"/>	事前共有鍵:	<input type="text" value="....."/> <input type="checkbox"/> パスワード表示
SSID タイプ:	Root AP - MR-GM5A 5G ▾																
暗号モード:	WPA3 Transition ▾																
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須																
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須																
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効																
暗号方式:	<input checked="" type="checkbox"/> AES																
ブロードキャスト暗号鍵 更新間隔:	<input type="text" value="86400"/>																
事前共有鍵:	<input type="text" value="....."/> <input type="checkbox"/> パスワード表示																

■ SSID タイプ

セキュリティ設定を行う SSID を選択して下さい。

マルチ SSID を設定している場合、SSID ごとにセキュリティ設定が必要です。

■ 暗号モード

暗号モードを選択し、以降の各項目を設定して下さい。

● 暗号モード: WPA3 Transition

暗号モードを「WPA3-Personal」、もしくは「WPA2-Personal」で接続可能なモードに設定します。

暗号モード:	WPA3 Transition ▾
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	<input type="text" value="86400"/>
事前共有鍵:	<input type="text" value="....."/> <input type="checkbox"/> パスワード表示

H2E	初期値のままご利用下さい。(固定設定・変更不可)
管理フレーム保護 (802.11w)	初期値のままご利用下さい。(固定設定・変更不可)
SHA256 暗号	初期値のままご利用下さい。(固定設定・変更不可)
暗号方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵	任意の事前共有鍵(暗号キー)を入力して下さい。 半角英数字で 8 文字以上、64 文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WPA3

暗号モードを「WPA3-Personal」に設定します。

暗号モード:	WPA3
H2E:	<input type="radio"/> 可能 <input checked="" type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input type="radio"/> 可能 <input checked="" type="radio"/> 必須
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵: <input type="checkbox"/> パスワード表示

H2E	初期値のままご利用下さい。(固定設定・変更不可)
管理フレーム保護 (802.11w)	初期値のままご利用下さい。(固定設定・変更不可)
SHA256 暗号	初期値のままご利用下さい。(固定設定・変更不可)
暗号方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵 更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵	任意の事前共有鍵(暗号キー)を入力して下さい。 半角英数字で8文字以上、64文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WPA2-Mixed

暗号モードを「WPA2-Personal」、もしくは「WPA-Personal」で接続可能なモードに設定します。

暗号モード:	WPA2 Mixed
WPA 暗号方式:	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
WPA2 暗号方式:	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵フォーマット:	文字列
事前共有鍵: <input type="checkbox"/> パスワード表示

WPA 暗号化方式 WPA2 暗号化方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵 更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵フォーマット	事前共有鍵の形式を選択して下さい。
事前共有鍵	事前共有鍵フォーマットにしたがって、事前共有鍵(暗号キー)を入力して下さい。 文字列の場合は、半角英数字で8文字以上、64文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WPA2

暗号モードを「WPA2-Personal」に設定します。

暗号モード:	WPA2
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
WPA2 暗号方式:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵フォーマット:	文字列
事前共有鍵: <input type="checkbox"/> パスワード表示

管理フレーム保護 (802.11w)	必要に応じて設定を変更して下さい。 特に変更の必要がない場合は、初期値「可能」のままご利用下さい。
SHA256 暗号	必要に応じて設定を変更して下さい。 特に変更の必要がない場合は、初期値「無効」のままご利用下さい。
WPA2 暗号化方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵フォーマット	事前共有鍵の形式を選択して下さい。
事前共有鍵	事前共有鍵フォーマットにしたがって、事前共有鍵(暗号キー)を入力して下さい。 文字列の場合は、半角英数字で8文字以上、64文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WEP

暗号モードを「WEP」に設定します。

暗号モード:	WEP
認証:	<input type="radio"/> オープンシステム認証 <input type="radio"/> 共有鍵認証 <input checked="" type="radio"/> 自動
鍵の長さ:	64ビット
鍵のフォーマット:	文字列(半角英数5文字)
暗号鍵: <input type="checkbox"/> パスワード表示

認証	WEP の認証方式を選択して下さい。 特に変更の必要がない場合は、「自動」のまま使用して下さい。
暗号鍵の長さ	暗号鍵の長さを選択して下さい。
暗号鍵のフォーマット	事前共有鍵の形式を選択して下さい。
暗号鍵	「暗号鍵の長さ」、「暗号鍵のフォーマット」に合わせて任意の暗号鍵(暗号キー)を入力して下さい。

●暗号モード:なし

通信を暗号化しません。

 注意	暗号モードを「無効」に設定する場合の危険性をご理解頂いた上で選択して下さい。
--	--

暗号モード:	なし
--------	----

■設定保存(ボタン)

設定した内容を保存する場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

4-1-4. アクセス制御 設定

無線 LAN1 (5GHz) のアクセス制御設定について説明します。

アクセス制御設定について
アクセス制御設定 (MAC アドレスによるアクセス制御) は基本 SSID にも適用されず、マルチ SSID には適用されませんのでご注意ください。

設定メニューの「無線 LAN 設定」の「無線 LAN1 (5GHz)」より「アクセス制御設定」をクリックして下さい。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーベイ WPS 設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール	無線LAN1 アクセス制御 設定 このページでは無線LANのアクセス制御の設定が行えます。許可リストを選択すると、選択すると、登録されたMACアドレスは接続できなくなります。 モード: <input type="text" value="無効"/> ▼ MACアドレス: <input type="text"/> 追加 アクセス制御 登録リスト <table border="1"><thead><tr><th>選択</th><th>MACアドレス</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td></td></tr></tbody></table>	選択	MACアドレス	<input type="checkbox"/>	
選択	MACアドレス				
<input type="checkbox"/>					

「無線 LAN1 アクセス制御設定」画面が開きます。

無線LAN1 アクセス制御 設定 このページでは無線LANのアクセス制御の設定が行えます。許可リストを選択すると、登録されたMACアドレスのみが接続できます。拒否リストを選択すると、登録されたMACアドレスは接続できなくなります。									
モード:	<input type="text" value="許可リスト"/> ▼ 設定保存								
MACアドレス:	<input type="text" value="00:10:38:44:44:44"/>								
追加									
アクセス制御 登録リスト									
<table border="1"><thead><tr><th>選択</th><th>MACアドレス</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>00:10:38:11:11:11</td></tr><tr><td><input type="checkbox"/></td><td>00:10:38:22:22:22</td></tr><tr><td><input type="checkbox"/></td><td>00:10:38:33:33:33</td></tr></tbody></table>	選択	MACアドレス	<input type="checkbox"/>	00:10:38:11:11:11	<input type="checkbox"/>	00:10:38:22:22:22	<input type="checkbox"/>	00:10:38:33:33:33	
選択	MACアドレス								
<input type="checkbox"/>	00:10:38:11:11:11								
<input type="checkbox"/>	00:10:38:22:22:22								
<input type="checkbox"/>	00:10:38:33:33:33								
<input type="button" value="選択した登録を編集"/> <input type="button" value="選択した登録を上げる"/> <input type="button" value="選択した登録を下げる"/> <input type="button" value="選択した登録を削除"/> <input type="button" value="全て削除"/>									

■モード

MAC アドレスによるアクセス制御モードを選択して下さい。

無効	MAC アドレスによるアクセス制御を行いません。
許可リスト	無線 LAN 接続を許可したい MAC アドレスを登録します。登録した MAC アドレス以外からの無線 LAN 接続は拒否します。
拒否リスト	無線 LAN 接続を拒否したい MAC アドレスを登録します。登録した MAC アドレス以外からの無線 LAN 接続は許可します。

■設定保存(ボタン)

設定した内容を保存する場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■MAC アドレス

アクセス制御を行う MAC アドレスを入力して下さい。

■追加(ボタン)

設定内容が MAC アドレス登録リストに追加されます。

〈次ページへ進んで下さい〉

■**選択した登録を編集(ボタン)**

アクセス制御 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。

■**選択した登録を上げる(ボタン)**

アクセス制御 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。

■**選択した登録を下げる(ボタン)**

アクセス制御 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。

■**選択したエントリを削除(ボタン)**

アクセス制御 登録リストの「選択」にチェックを入れたものが削除されます。

■**全て削除(ボタン)**

アクセス制御 登録リストの内容全てが削除されます。

4-1-5. サイトサーベイ

他の無線 LAN アクセスポイントの状況を表示するサイトサーベイ画面について説明します。
設定メニューの「無線 LAN 設定」の「無線 LAN1 (5GHz)」より「サイトサーベイ」をクリックして下さい。
「無線 LAN1 サイトサーベイ」画面が開きます。



無線LAN1 サイトサーベイ
このページでは他の無線LANアクセスポイントの状況を表示します。

SSID	BSSID	チャンネル	タイプ	暗号モード	電波強度(%)
		36 (A+N+AC) 80MHz	AP	WPA-PSK/WPA2-PSK	57
		36 (A+N+AC) 80MHz	AP	WPA2-PSK	47
		36 (A+N+AC) 80MHz	AP	WPA2-PSK	41
		132 (A+N+AC) 80MHz	AP	WPA2-PSK	34
		132 (A+N+AC) 80MHz	AP	WPA2-PSK	34
		36 (A+N+AC) 80MHz	AP	WPA2-PSK	20

再読み込み 次へ

- **SSID**
他の無線 LAN アクセスポイントの SSID を表示します。
- **BSSID**
他の無線 LAN アクセスポイントの MAC (物理) アドレスを表示します。
- **チャンネル**
他の無線 LAN アクセスポイントのチャンネル及び周波数を表示します。
- **タイプ**
他の無線 LAN アクセスポイントの動作モードを表示します。
- **暗号モード**
他の無線 LAN アクセスポイントの暗号モードを表示します。
- **信号強度 (%)**
他の無線 LAN アクセスポイントの信号強度 (%) を表示します。
- **再読み込み (ボタン)**
サイトサーベイ画面を再読み込みします。
- **次へ (ボタン)**
MR-GM5A を無線 LAN クライアントモードで設定した場合に使用するボタンです。
「無線 LAN クライアントモード」については「4-4.無線 LAN クライアントモード設定」(57 ページ)を参照して下さい。

4-1-6.WPS 設定

WPS 接続機能の設定、操作について説明します。

WPS 機能について
本製品の WPS 機能はプッシュボタン方式と PIN コード方式に対応しています。
WPS 機能を使用するためには、無線 LAN クライアント側も WPS に対応している必要があります。
暗号モードが WPA3-Personal の場合 WPS 接続はできません。
基本 SSID のみ WPS 接続が可能です。

設定メニューの「無線 LAN 設定」の「無線 LAN1 (5GHz)」より「WPS 設定」をクリックして下さい。

ステータス
- 無線LAN
- 無線LAN1 (5GHz)
基本設定
拡張設定
セキュリティ設定
アクセス制御設定
サイトサーベイ
WPS 設定
+ 無線LAN2 (2.4GHz)
+ ネットワーク

無線LAN1 WPS 設定
このページでは無線LANのWPS(Wi-Fi Protected Setup)の
をかけずにアクセスポイントに接続できます。

WPS機能 無効

WPS ステータス:

セルフPINコード:

Pushボタン 設定:

設定保存 リセット

「無線 LAN1 WPS 設定」画面が開きます。

無線LAN1 WPS 設定
このページでは無線LANのWPS(Wi-Fi Protected Setup)の設定が行えます。この機能を使用すると、無線LANクライアントの設定が自動同期し、手間
をかけずにアクセスポイントに接続できます。

WPS機能 無効

WPS ステータス: 構成済み 未構成

セルフPINコード: 12345670

Pushボタン 設定:

設定保存 リセット

現在のセキュリティ設定

認証	暗号モード	暗号鍵/事前共有鍵
WPA3 Transition	AES	

クライアントPINコード:

■WPS 機能 無効

WPS 機能を利用しない場合、チェックを入れて下さい。

■WPS ステータス

WPS 機能の状態を表示します。

WPS 機能を使用して接続すると、「構成済み」が選択された状態になります。

■セルフ PIN コード

本製品の PIN コードを表示します。

■[PIN 再生成](ボタン)

本製品の PIN コードを再生成します。

■Push ボタン設定([セットアップ開始]ボタン)

プッシュボタン方式で WPS 接続を開始します。

本製品の WPS ランプが点滅し、2 分間待ち受け状態となります。

<次ページへ進んで下さい>

■[設定保存](ボタン)

WPS 機能の有効/無効を切り替えた場合にクリックして下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■[リセット](ボタン)

本画面で入力した値をリセットするためのボタンです。

■現在のセキュリティ設定

基本 SSID の「認証方式」、「暗号モード」、「暗号鍵/事前共有鍵」を表示します。

■クライアント PIN コード

PIN コード方式で接続する場合の無線 LAN クライアントの PIN コードを入力します。

4-2.無線 LAN2 (2.4GHz)

無線 LAN2(2.4GHz)の設定について説明します。

4-2-1.基本 設定

無線 LAN2(2.4GHz)の基本設定について説明します。

設定メニューの「無線 LAN」の「無線 LAN2 (2.4GHz)」より「基本設定」をクリックして下さい。

「無線 LAN2 基本設定」画面が開きます。

ステータス - 無線LAN + 無線LAN1 (5GHz) - 無線LAN2 (2.4GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーバイ WPS設定 + ネットワーク + ファイアウォール + 付加機能 + マネージメント	無線LAN2 基本設定 このページでは無線LANの基本的なパラメーターの設定が行えます。
	<input type="checkbox"/> 無線LANを無効にする
	バンド: 2.4 GHz (B+G+N) ▼
	モード: アクセスポイント ▼ マルチSSID設定
	SSID: MR-GM5A 2.4
	帯域幅: 40MHz ▼
	サイドバンド制御: 上位 ▼
	チャンネル番号: 自動 ▼
	電波出力 (%): 100% ▼
	帯域: 自動 ▼
	ブロードキャスト SSID: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	クライアント間通信遮断: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	マルチキャストをユニキャストに変換: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	接続中クライアント数: クライアント表示

■無線 LAN を無効にする

無線 LAN 機能を無効にする場合、チェックを入れて下さい。

■バンド

初期値「2.4GHz (B+G+N)」のままご利用下さい。

本製品側で周波数を固定する必要がある場合にのみ、以下から選択して下さい。

- 2.4GHz (B) :IEEE 802.11b で固定します。
- 2.4GHz (G) :IEEE 802.11g で固定します。
- 2.4GHz (N) :IEEE 802.11n で固定します。
- 2.4GHz (B+G) :IEEE 802.11b/g で固定します。
- 2.4GHz (G+N) :IEEE 802.11g/n で固定します。
- 2.4GHz (B+G+N) :IEEE 802.11b/g/n で固定します。

■モード

ルーターとして利用する場合は、初期値「アクセスポイント」のままご利用下さい。

無線 LAN クライアントモードで使用する場合は、「クライアント」を選択して下さい。

「無線 LAN クライアントモード」については「4-4.無線 LAN クライアントモード設定」(57 ページ)を参照して下さい。

■マルチ SSID 設定(ボタン)

マルチ SSID の設定を行います。

マルチ SSID 設定については 4-3.マルチ SSID 設定例」(51 ページ)を参照して下さい。

■SSID

無線 LAN アクセスポイントを識別するための名前を入力して下さい。

■帯域幅

チャンネルの帯域幅を設定します。

(「IEEE802.11 n」を選択した場合にのみ表示されます。)

■サイドバンド制御

初期値「上位」のままご利用下さい。(チャンネル番号で自動以外を選択し、帯域幅で 40MHz を選択し場合にのみ変更可能)

〈次ページへ進んで下さい〉

■チャンネル番号

無線 LAN のチャンネル番号を設定します。
通常は初期値「自動」のままご利用下さい。

■電波出力 (%)

本製品の通信出力を設定します。
通常は初期値「100%」のままご利用下さい。

■帯域 (伝送速度)

伝送速度を設定します。
通常は初期値「自動」のままご利用下さい。
本製品側で伝送速度を固定する必要がある場合にのみ、変更して下さい。

■ブロードキャスト SSID

「SSID」をブロードキャスト (同時通報) メッセージとして送信する場合は「有効」にして下さい。
「SSID」を隠す場合は「無効」にして下さい。

	「無効」に設定すると、無線 LAN クライアントから検索できなくなります。
	「無効」に設定すると、WPS 機能も無効になります。

■クライアント間通信遮断

無線 LAN2 (2.4GHz) の無線 LAN クライアント間の通信を遮断します。

	無線 LAN1 (5GHz) と無線 LAN2 (2.4GHz) 間の通信を遮断する場合は、無線 LAN1 (5GHz) と無線 LAN2 (2.4GHz) のマルチ SSID 設定画面の「マルチ SSID 間通信遮断」を有効に設定して下さい。 「マルチ SSID 間通信遮断」が無効の場合、5GHz (無線 LAN1) と 2.4GHz (無線 LAN2) 間の通信は遮断されませんのでご注意ください。 「4-3-2. マルチ SSID1 の設定」(53 ページ) を参照して下さい。
---	--

■マルチキャストをユニキャストに変換

マルチキャストのデータをユニキャストに変換します。

■接続中クライアント 表示 (ボタン)

接続している無線 LAN クライアントの情報 (別ウィンドウ) を表示します。

接続中クライアント
このページでは接続中の無線LANクライアントのステータスを表示します。

MACアドレス	送信パケット数	受信パケット数	送信速度 (Mbps)	省電力	有効期限 (秒)
XXXXXXXXXX	303	260	864	yes	240

再読み込み 閉じる

■設定保存 (ボタン)

設定を保存します。
「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。
引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

4-2-2. 拡張 設定

無線 LAN2 (2.4GHz) の基本設定について説明します。

設定メニューの「無線 LAN」の「無線 LAN2 (2.4GHz)」より「拡張 設定」をクリックして下さい。

「無線 LAN2 拡張設定」画面が開きます。

ステータス - 無線LAN + 無線LAN1 (5GHz) - 無線LAN2 (2.4GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーベイ WPS設定 + ネットワーク + ファイアウォール + 付加機能 + マネージメント	無線LAN2 拡張設定 このページでは無線LANの高度なパラメーターの設定が行えます。
	ビーコン間隔: <input type="text" value="100"/> (100-1024 ミリ秒)
	DTIM 間隔: <input type="text" value="1"/> (1-255)
	プリアンブルタイプ: <input checked="" type="radio"/> Long プリアンブル <input type="radio"/> Short プリアンブル
	ショート ガード インターバル: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	送信ビームフォーミング: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	基本バンド 設定: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 <input type="text" value="Prefer 2.4GHz"/>
	802.11k サポート: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	<input type="button" value="設定保存"/>

■ビーコン間隔(工場出荷値: 100)

無線電波の送出間隔を設定します。

	設定値を小さくすると通信品質は上がりますが、他の無線機器と干渉する可能性が高くなります。
---	--

■DTIM 間隔(工場出荷値: 1)

省電力モードで動作する無線 LAN クライアントに対して、送信待ちデータがあることを伝えるブロードキャストやマルチキャストのメッセージ間隔を設定します。

■プリアンブルタイプ(工場出荷値: Long プリアンブル)

無線 LAN クライアント間のデータ転送エラーを検出する CRC の長さを選択します。

Short プリアンブルは伝送速度を速くすることができますが、旧型の無線 LAN クライアントを使用する場合は、互換性を確保するために「Long プリアンブル」のままご利用下さい。

■ショート ガード インターバル(工場出荷値: 有効)

時間差で届くデータの干渉を防ぎます。

	ショート ガード インターバルを有効にすることでデータ通信の効率を上げることができますが、反射波の影響を受けやすくなり、データ通信全体のスループットに影響を与える場合があります。
---	---

■送信ビームフォーミング(工場出荷値: 無効)

ビームフォーミングを有効にした場合、ビームフォーミングに対応した機器同士が互いの方向に向けて指向性の高い電波を送りますので、電波強度を向上させる事ができます。

■マルチユーザー MIMO(工場出荷値: 無効)

送信ビームフォーミングを有効にした場合に表示されます。

複数の無線 LAN クライアントが同時に通信を行った際の通信速度の低下を抑えます。

■基本バンド(工場出荷値: 無効)

無線 LAN1 (5GHz) と無線 LAN2 (2.4GHz) を同一 SSID、セキュリティ設定にして、どちらに優先して接続するか選択します。

	有効にすると、選択した無線 LAN 周波数の SSID 設定、セキュリティ設定のみ変更可能となります。(選択していない無線 LAN 周波数の SSID 設定、セキュリティ設定は変更不可となります。)
---	---

<次ページへ進んで下さい>

■802.11k サポート(工場出荷値:無効)

近隣無線 LAN アクセスポイントの情報を共有する規格です。

これにより、無線 LAN クライアントは、より最適な無線 LAN アクセスポイントへのローミングが可能です。

802.11k を利用するには、無線 LAN クライアント側も 802.11k に対応している必要があります。

■802.11v サポート(工場出荷値:無効)

802.11k サポート有効した場合には表示されます。

無線 LAN アクセスポイントの管理情報を強化する規格です。

これにより、最適な無線 LAN アクセスポイントへのローミングや接続維持の効果が見込まれます。

802.11v を利用するには、無線 LAN クライアント側も 802.11v に対応している必要があります。

■設定保存(ボタン)

設定した内容を保存する場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

4-2-3.セキュリティ 設定

無線 LAN1 (2.4GHz) の基本設定について説明します。

設定メニューの「無線 LAN」の「無線 LAN2 (2.4GHz)」より「セキュリティ 設定」をクリックして下さい。

「無線 LAN2 セキュリティ 設定」画面が開きます。

ステータス - 無線LAN + 無線LAN1 (5GHz) - 無線LAN2 (2.4GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーバイ WPS設定 + ネットワーク + ファイアウォール + 付加機能 + マネージメント	<h4 style="color: #0056b3;">無線LAN2 セキュリティ 設定</h4> <p style="font-size: small;">このページでは無線LANのセキュリティの設定が行えます。</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 30%;">SSID タイプ:</td> <td>Root AP - MR-GM5A 2.4 ▾</td> </tr> <tr> <td>暗号モード:</td> <td>WPA3 Transition ▾</td> </tr> <tr> <td>H2E:</td> <td><input checked="" type="radio"/> 可能 <input type="radio"/> 必須</td> </tr> <tr> <td>管理フレーム保護 (802.11w):</td> <td><input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須</td> </tr> <tr> <td>SHA256 暗号:</td> <td><input type="radio"/> 無効 <input checked="" type="radio"/> 有効</td> </tr> <tr> <td>暗号方式:</td> <td><input checked="" type="checkbox"/> AES</td> </tr> <tr> <td>ブロードキャスト暗号鍵 更新間隔:</td> <td><input type="text" value="86400"/></td> </tr> <tr> <td>事前共有鍵:</td> <td><input type="text" value="....."/></td> </tr> </table>	SSID タイプ:	Root AP - MR-GM5A 2.4 ▾	暗号モード:	WPA3 Transition ▾	H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須	管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須	SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効	暗号方式:	<input checked="" type="checkbox"/> AES	ブロードキャスト暗号鍵 更新間隔:	<input type="text" value="86400"/>	事前共有鍵:	<input type="text" value="....."/>
SSID タイプ:	Root AP - MR-GM5A 2.4 ▾																
暗号モード:	WPA3 Transition ▾																
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須																
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須																
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効																
暗号方式:	<input checked="" type="checkbox"/> AES																
ブロードキャスト暗号鍵 更新間隔:	<input type="text" value="86400"/>																
事前共有鍵:	<input type="text" value="....."/>																

■ SSID タイプ

セキュリティ設定を行う SSID を選択して下さい。

マルチ SSID を設定している場合、SSID ごとにセキュリティ設定が必要です。

■ 暗号モード

暗号モードを選択し、以降の各項目を設定して下さい。

● 暗号モード: WPA3 Transition

暗号モードを「WPA3-Personal」、もしくは「WPA2-Personal」で接続可能なモードに設定します。

暗号モード:	WPA3 Transition ▾
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	<input type="text" value="86400"/>
事前共有鍵:	<input type="text" value="....."/> <input type="checkbox"/> パスワード表示

H2E	初期値のままご利用下さい。(固定設定・変更不可)
管理フレーム保護 (802.11w)	初期値のままご利用下さい。(固定設定・変更不可)
SHA256 暗号	初期値のままご利用下さい。(固定設定・変更不可)
暗号方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵	任意の事前共有鍵(暗号キー)を入力して下さい。 半角英数字で 8 文字以上、64 文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WPA3

暗号モードを「WPA3-Personal」に設定します。

暗号モード:	WPA3
H2E:	<input type="radio"/> 可能 <input checked="" type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input type="radio"/> 可能 <input checked="" type="radio"/> 必須
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵: <input type="checkbox"/> パスワード表示

H2E	初期値のままご利用下さい。(固定設定・変更不可)
管理フレーム保護 (802.11w)	初期値のままご利用下さい。(固定設定・変更不可)
SHA256 暗号	初期値のままご利用下さい。(固定設定・変更不可)
暗号方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵	任意の事前共有鍵(暗号キー)を入力して下さい。 半角英数字で8文字以上、64文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WPA2-Mixed

暗号モードを「WPA2-Personal」、もしくは「WPA-Personal」で接続可能なモードに設定します。

暗号モード:	WPA2 Mixed
WPA 暗号方式:	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
WPA2 暗号方式:	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵フォーマット:	文字列
事前共有鍵: <input type="checkbox"/> パスワード表示

WPA 暗号化方式 WPA2 暗号化方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵フォーマット	事前共有鍵の形式を選択して下さい。
事前共有鍵	事前共有鍵フォーマットにしたがって、事前共有鍵(暗号キー)を入力して下さい。 文字列の場合は、半角英数字で8文字以上、64文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WPA2

暗号モードを「WPA2-Personal」に設定します。

暗号モード:	WPA2
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
WPA2 暗号方式:	<input type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵フォーマット:	文字列
事前共有鍵: <input type="checkbox"/> パスワード表示

管理フレーム保護 (802.11w)	必要に応じて設定を変更して下さい。 特に変更の必要がない場合は、初期値「可能」のままご利用下さい。
SHA256 暗号	必要に応じて設定を変更して下さい。 特に変更の必要がない場合は、初期値「無効」のままご利用下さい。
WPA2 暗号化方式	初期値のままご利用下さい。(固定設定・変更不可)
ブロードキャスト暗号鍵更新間隔	ブロードキャスト暗号鍵の更新間隔を設定します。 通常は「86400」のままご利用下さい。
事前共有鍵フォーマット	事前共有鍵の形式を選択して下さい。
事前共有鍵	事前共有鍵フォーマットにしたがって、事前共有鍵(暗号キー)を入力して下さい。 文字列の場合は、半角英数字で8文字以上、64文字以下で設定して下さい。 「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

●暗号モード:WEP

暗号モードを「WEP」に設定します。

暗号モード:	WEP
認証:	<input type="radio"/> オープンシステム認証 <input type="radio"/> 共有鍵認証 <input checked="" type="radio"/> 自動
鍵の長さ:	64ビット
鍵のフォーマット:	文字列(半角英数5文字)
暗号鍵: <input type="checkbox"/> パスワード表示

認証	WEP の認証方式を選択して下さい。 特に変更の必要がない場合は、「自動」のまま使用して下さい。
暗号鍵の長さ	暗号鍵の長さを選択して下さい。
暗号鍵のフォーマット	事前共有鍵の形式を選択して下さい。
暗号鍵	「暗号鍵の長さ」、「暗号鍵のフォーマット」に合わせて任意の暗号鍵(暗号キー)を入力して下さい。

●暗号モード:なし

通信を暗号化しません。

 注意	暗号モードを「無効」に設定する場合の危険性をご理解頂いた上で選択して下さい。
---	--

暗号モード:	なし
--------	----

■設定保存(ボタン)

設定を保存します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は、[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

4-2-4. アクセス制御 設定

無線 LAN1 (2.4GHz) のアクセス制御設定について説明します。

アクセス制御設定について
アクセス制御設定 (MAC アドレスによるアクセス制御) は基本 SSID にも適用されます。 マルチ SSID には適用されませんのでご注意ください。

設定メニューの「無線 LAN 設定」の「無線 LAN2 (2.4GHz)」より「アクセス制御設定」をクリックして下さい。

ステータス - 無線LAN + 無線LAN1 (5GHz) - 無線LAN2 (2.4GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーベイ WPS 設定 + ネットワーク + ファイアウォール	無線LAN2 アクセス制御 設定 このページでは無線LANのアクセス制御の設定が行えます。許可リストを選択すると、選択すると、登録されたMACアドレスは接続できなくなります。 モード: <input type="text" value="無効"/> ▼ MACアドレス: <input type="text"/> 追加 アクセス制御 登録リスト <table border="1"><thead><tr><th>選択</th><th>MACアドレス</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td></td></tr></tbody></table>	選択	MACアドレス	<input type="checkbox"/>	
選択	MACアドレス				
<input type="checkbox"/>					

「無線 LAN2 アクセス制御設定」画面が開きます。

無線LAN1 アクセス制御 設定 このページでは無線LANのアクセス制御の設定が行えます。許可リストを選択すると、登録されたMACアドレスのみが接続できます。拒否リストを選択すると、登録されたMACアドレスは接続できなくなります。 モード: <input type="text" value="許可リスト"/> ▼ 設定保存 MACアドレス: <input type="text" value="00:10:38:44:44:44"/> 追加 アクセス制御 登録リスト <table border="1"><thead><tr><th>選択</th><th>MACアドレス</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>00:10:38:11:11:11</td></tr><tr><td><input type="checkbox"/></td><td>00:10:38:22:22:22</td></tr><tr><td><input type="checkbox"/></td><td>00:10:38:33:33:33</td></tr></tbody></table> 選択した登録を編集 選択した登録を上げる 選択した登録を下げる 選択した登録を削除 全て削除	選択	MACアドレス	<input type="checkbox"/>	00:10:38:11:11:11	<input type="checkbox"/>	00:10:38:22:22:22	<input type="checkbox"/>	00:10:38:33:33:33
選択	MACアドレス							
<input type="checkbox"/>	00:10:38:11:11:11							
<input type="checkbox"/>	00:10:38:22:22:22							
<input type="checkbox"/>	00:10:38:33:33:33							

■モード

MAC アドレスによるアクセス制御モードを選択して下さい。

無効	MAC アドレスによるアクセス制御を行いません。
許可リスト	無線 LAN 接続を許可したい MAC アドレスを登録します。 登録した MAC アドレス以外からの無線 LAN 接続は拒否します。
拒否リスト	無線 LAN 接続を拒否したい MAC アドレスを登録します。 登録した MAC アドレス以外からの無線 LAN 接続は許可します。

■設定保存(ボタン)

設定した内容を保存する場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■MAC アドレス

アクセス制御を行う MAC アドレスを入力して下さい。

■追加(ボタン)

設定内容が MAC アドレス登録リストに追加されます。

<次ページへ進んで下さい>

■**選択した登録を編集(ボタン)**

アクセス制御 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。

■**選択した登録を上げる(ボタン)**

アクセス制御 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。

■**選択した登録を下げる(ボタン)**

アクセス制御 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。

■**選択したエントリを削除(ボタン)**

アクセス制御 登録リストの「選択」にチェックを入れたものが削除されます。

■**全て削除(ボタン)**

アクセス制御 登録リストの内容全てが削除されます。

4-2-5. サイトサーベイ

他の無線 LAN アクセスポイントの状況を表示するサイトサーベイ画面について説明します。
 設定メニューの「無線 LAN 設定」の「無線 LAN2 (2.4GHz)」より「サイトサーベイ」をクリックして下さい。
 「無線 LAN2 サイトサーベイ」画面が開きます。



無線LAN2 サイトサーベイ
 このページでは他の無線LANアクセスポイントの状況を表示します。

SSID	BSSID	チャンネル	タイプ	暗号モード	電波強度(%)
XXXXXXXXXX	XXXXXXXXXX	1 (B+G+N) 40MHz	AP	WPA-PSK/WPA2-PSK	70
XXXXXXXXXX	XXXXXXXXXX	6 (B+G+N) 20MHz	AP	WPA-PSK/WPA2-PSK	48
XXXXXXXXXX	XXXXXXXXXX	6 (B+G+N) 20MHz	AP	WPA-PSK/WPA2-PSK	48
XXXXXXXXXX	XXXXXXXXXX	1 (B+G+N) 40MHz	AP	WPA2-PSK	46
XXXXXXXXXX	XXXXXXXXXX	1 (B+G+N) 20MHz	AP	WPA2-PSK	44
XXXXXXXXXX	XXXXXXXXXX	1 (B+G+N) 20MHz	AP	WPA2-PSK	43
XXXXXXXXXX	XXXXXXXXXX	9 (B+G+N) 20MHz	AP	WPA-PSK/WPA2-PSK	11

再読み込み 次へ

- **SSID**
他の無線 LAN アクセスポイントの SSID を表示します。
- **BSSID**
他の無線 LAN アクセスポイントの MAC (物理) アドレスを表示します。
- **チャンネル**
他の無線 LAN アクセスポイントのチャンネル及び周波数を表示します。
- **タイプ**
他の無線 LAN アクセスポイントの動作モードを表示します。
- **暗号モード**
他の無線 LAN アクセスポイントの暗号モードを表示します。
- **信号強度 (%)**
他の無線 LAN アクセスポイントの信号強度 (%) を表示します。
- **再読み込み (ボタン)**
サイトサーベイ画面を再読み込みします。
- **次へ (ボタン)**
MR-GM5A を無線 LAN クライアントモードで設定した場合に使用するボタンです。
「無線 LAN クライアントモード」については「4-4. 無線 LAN クライアントモード設定」(57 ページ)を参照して下さい。

4-2-6.WPS 設定

WPS 接続機能の設定、操作について説明します。

WPS 機能について
本製品の WPS 機能はプッシュボタン方式と PIN コード方式に対応しています。
WPS 機能を使用するためには、無線 LAN クライアント側も WPS に対応している必要があります。
暗号モードが WPA3-Personal の場合 WPS 接続はできません。
基本 SSID のみ WPS 接続が可能です。

設定メニューの「無線 LAN 設定」の「無線 LAN2(2.4GHz)」より「WPS 設定」をクリックして下さい。

ステータス
- 無線LAN
+ 無線LAN1 (5GHz)
- 無線LAN2 (2.4GHz)
基本設定
拡張設定
セキュリティ設定
アクセス制御設定
サイトサーベイ
WPS 設定
+ ネットワーク

無線LAN2 WPS 設定

このページでは無線LANのWPS(Wi-Fi Protected Setup)の
をかけずにアクセスポイントに接続できます。

WPS機能 無効

WPS ステータス:

セルフPINコード:

Pushボタン 設定:

設定保存 リセット

「無線 LAN2 WPS 設定」画面が開きます。

無線LAN2 WPS 設定

このページでは無線LANのWPS(Wi-Fi Protected Setup)の設定が行えます。この機能を使用すると、無線LANクライアントの設定が自動同期し、手間
をかけずにアクセスポイントに接続できます。

WPS機能 無効

WPS ステータス: 構成済み 未構成

セルフPINコード: 12345670

Pushボタン 設定:

設定保存 リセット

現在のセキュリティ設定

認証	暗号モード	暗号鍵/事前共有鍵
WPA3 Transition	AES	

クライアントPINコード:

■WPS 機能 無効

WPS 機能を利用しない場合、チェックを入れて下さい。

■WPS ステータス

WPS 機能の状態を表示します。

WPS 機能を使用して接続すると、「構成済み」が選択された状態になります。

■セルフ PIN コード

本製品の PIN コードを表示します。

■[PIN 再生成](ボタン)

本製品の PIN コードを再生成します。

■Push ボタン設定([セットアップ開始]ボタン)

プッシュボタン方式で WPS 接続を開始します。

本製品の WPS ランプが点滅し、2 分間待ち受け状態となります。

〈次ページへ進んで下さい〉

■[設定保存](ボタン)

WPS 機能の有効/無効を切り替えた場合にクリックして下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■[リセット](ボタン)

本画面で入力した値をリセットするためのボタンです。

■現在のセキュリティ設定

プライマリーSSID の「認証方式」、「暗号モード」、「暗号鍵/事前共有鍵」を表示します。

■クライアント PIN コード

PIN コード方式で接続する場合の無線 LAN クライアントの PIN コードを入力します。

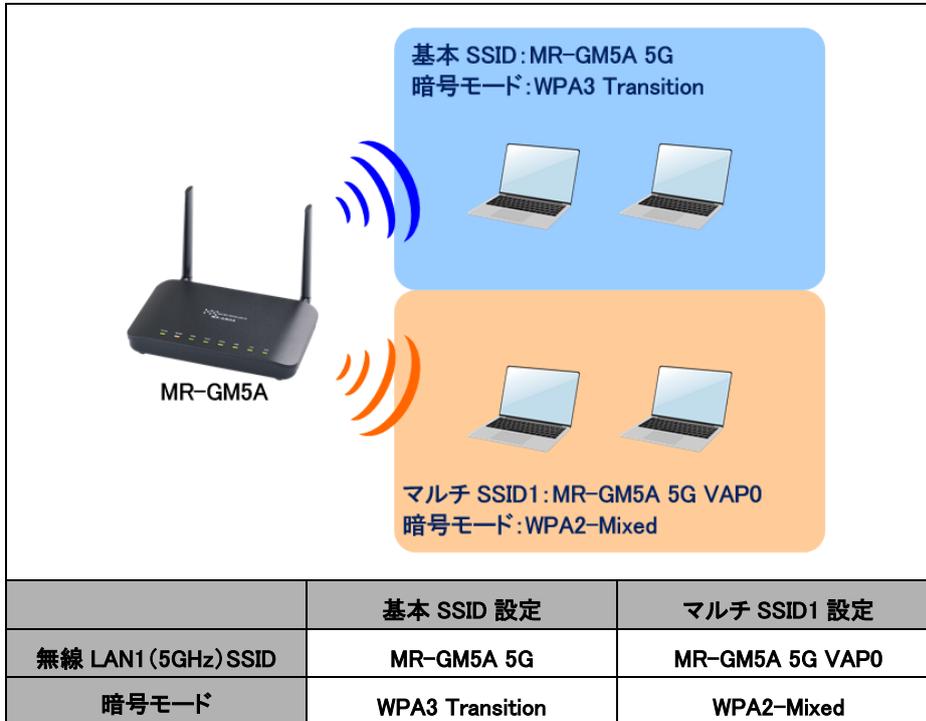
4-3. マルチ SSID 設定例

マルチ SSID の設定について説明します。

本製品に複数の SSID を設定することにより、セキュリティ設定の異なる複数の無線 LAN グループを同時に接続する事ができます。

無線 LAN1 (5GHz)、無線 LAN2(2.4GHz)それぞれに最大 2 つの SSID を追加する事ができます。

以下の使用環境を例に設定方法を説明します。



以下の各設定を行って下さい。

- 4-3-1.基本 SSID の設定
- 4-3-2.マルチ SSID1 の設定
- 4-3-3.基本 SSID セキュリティ設定 (WPA3 Transition)
- 4-3-4.マルチ SSID1 セキュリティ設定 (WPA2-Mixed)

4-3-1.基本 SSID の設定

以下の手順で基本 SSID の設定を行って下さい。

設定メニューの「無線 LAN 設定」の「無線 LAN1 (5GHz)」より「基本設定」をクリックして下さい。

「無線 LAN1 基本設定」画面が開きます。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本設定 + 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーベイ WPS設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール + 付加機能 + マネージメント	無線LAN1 基本設定 このページでは無線LANの基本的なパラメーターの設定が行えます。
	<input type="checkbox"/> 無線LANを無効にする
	バンド: 5 GHz (A+N+AC+AX) ▼
	モード: アクセスポイント ▼ マルチSSID設定
	SSID: MR-GM5A 5G
	帯域幅: 80MHz ▼
	サイドバンド制御: 自動 ▼
	チャンネル番号: 自動(DFS) ▼
	電波出力 (%): 100% ▼
	帯域: 自動 ▼
	ブロードキャスト SSID: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	クライアント間通信遮断: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	マルチキャストをユニキャストに変換: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	接続中クライアント数: クライアント表示

■バンド

「5GHz (A+N+AC+AX)」を選択して下さい。

■モード

「アクセスポイント」を選択して下さい。

■SSID

基本の SSID を入力して下さい。

本設定例の場合、「MR-GM5A 5G」のままご利用下さい。

	本画面で表示される他の設定については必要に応じて行って下さい。 詳しくは「4-1-1.基本 設定」(27 ページ)を参照して下さい。
---	---

設定が終わりましたら、[設定保存]ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

4-3-2. マルチ SSID1 の設定

以下の手順でマルチ SSID1 の設定を行って下さい。
[マルチ SSID 設定] ボタンをクリックして下さい。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーバイ WPS設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール + 付加機能 + マネージメント	無線LAN1 基本設定 このページでは無線LANの基本的なパラメーターの設定が行えます。
	<input type="checkbox"/> 無線LANを無効にする
	バンド: 5 GHz (A+N+AC+AX) ▼
	モード: アクセスポイント ▼ マルチSSID設定
	SSID: MR-GM5A 5G
	帯域幅: 80MHz ▼
	サイドバンド制御: 自動 ▼
	チャンネル番号: 自動(DFS) ▼
	電波出力 (%): 100% ▼
	帯域: 自動 ▼
	ブロードキャスト SSID: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	クライアント間通信遮断: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効
	マルチキャストをユニキャストに変換: <input checked="" type="radio"/> 有効 <input type="radio"/> 無効
	接続中クライアント数: クライアント表示
	<input type="checkbox"/> ユニバーサルリピーター機能を有効にする
リピーター SSID: repeater_ssid1	
設定保存	

「マルチ SSID 設定」画面が開きます。

マルチSSID設定 このページではマルチSSIDの設定が行えます。		
マルチSSID間通信遮断	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	
No.:	マルチSSID1	マルチSSID2
マルチSSID機能:	<input checked="" type="checkbox"/> 有効にする	<input type="checkbox"/> 有効にする
バンド:	5 GHz (A+N+AC+AX) ▼	5 GHz (A+N+AC+AX) ▼
SSID:	MR-GM5A 5G VAP0	MR-GM5A 5G VAP1
帯域:	自動 ▼	自動 ▼
ブロードキャスト SSID:	有効 ▼	有効 ▼
WMM サポート:	有効 ▼	有効 ▼
クライアント間通信遮断:	無効 ▼	無効 ▼
マルチキャストをユニキャストに変換:	有効 ▼	有効 ▼
接続中クライアント:	クライアント表示	クライアント表示
設定保存		

■ マルチ SSID 間通信遮断

SSID 間の通信を遮断する場合「有効」を選択して下さい。

 **無線 LAN1 (5GHz) と無線 LAN2 (2.4GHz) 間の通信を遮断する場合は、無線 LAN1 (5GHz) と無線 LAN2 (2.4GHz) 両方の「マルチ SSID 間通信遮断」を有効に設定して下さい。**
「マルチ SSID 間通信遮断」が無効の場合、5GHz (無線 LAN1) と 2.4GHz (無線 LAN2) 間の通信は遮断されませんのでご注意下さい。

〈次ページへ進んで下さい〉

■ **マルチ SSID 機能**

「有効にする」にチェックを入れて下さい。

■ **バンド**

「5GHz (A+N+AC+AX)」を選択して下さい。

■ **SSID**

マルチ SSID1 の SSID を入力して下さい。

本設定例の場合、「MR-GM5A 5G VAP0」のままご利用下さい。

■ **帯域**

通常は「自動」のままご利用下さい。

必要に応じて変更して下さい。

■ **WMM サポート**

WMM(Wi-Fi Multimedia)を有効にすることで、マルチメディアの通信の遅延を抑えます。

通常は「有効」のままご利用下さい。

■ **クライアント間通信遮断**

無線 LAN クライアント間の通信を遮断します。

■ **マルチキャストをユニキャストに変換**

マルチキャストのデータをユニキャストに変換します。

■ **接続中クライアント 表示 (ボタン)**

接続している無線 LAN クライアントの情報 (別ウィンドウ) を表示します。

設定が終わりましたら、[設定保存] ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

4-3-3.基本 SSID セキュリティ設定

以下の手順で基本 SSID のセキュリティ設定を行って下さい。
設定メニューの「無線 LAN 設定」の「無線 LAN1 (5GHz)」より「セキュリティ設定」をクリックして下さい。
「無線 LAN1 セキュリティ設定」画面が開きます。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーバイ WPS 設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール + 付加機能 + マネージメント	無線LAN1 セキュリティ 設定 このページでは無線LANのセキュリティの設定が行えます。	
	SSID タイプ:	Root AP - MR-GM5A 5G ▾
	暗号モード:	WPA3 Transition ▾
	H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
	管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
	SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
	暗号方式:	<input checked="" type="checkbox"/> AES
	ブロードキャスト暗号鍵 更新間隔:	86400
	事前共有鍵:

SSID タイプ:	Root AP - MR-GM5A 5G ▾
暗号モード:	WPA3 Transition ▾
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵: <input type="checkbox"/> パスワード表示

■ SSID タイプ

「Root AP - MR-GM5A 5G」を選択して下さい。

■ 暗号モード

「WPA3 Transition」を選択して下さい。

■ ブロードキャスト暗号鍵 更新間隔

通常は「86400」のままご利用下さい。

必要に応じて変更して下さい。

■ 事前共有鍵

任意の事前共有鍵(暗号キー)を入力して下さい。

半角英数字で8文字以上、64文字以下で設定して下さい。

「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

設定が終わりましたら、[設定保存]ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

4-3-4. マルチ SSID1セキュリティ設定

以下の手順でマルチ SSID1 のセキュリティ設定を行って下さい。

SSID タイプ:	AP1 - MR-GM5A 5G VAP0 ▾
暗号モード:	WPA2 Mixed ▾
WPA 暗号方式:	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
WPA2 暗号方式:	<input checked="" type="checkbox"/> TKIP <input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵フォーマット:	文字列 ▾
事前共有鍵: <input type="checkbox"/> パスワード表示

■ SSID タイプ

「**AP1 - MR-GM5A 5G VAP0**」を選択して下さい。

■ 暗号モード

「WPA2-Mixed」を選択して下さい。

■ ブロードキャスト暗号鍵 更新間隔

通常は「86400」のままご利用下さい。

必要に応じて変更して下さい。

■ 事前共有鍵フォーマット

事前共有鍵の形式を選択して下さい。

■ 事前共有鍵

事前共有鍵フォーマットにしたがって、事前共有鍵(暗号キー)を入力して下さい。

「パスワード表示」にチェックを入れると、設定した事前共有鍵が表示されます。

設定が終わりましたら、[設定保存]ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、[今すぐ再起動]ボタンを押して下さい。

以上でマルチ SSID の設定は完了です。

4-4.無線 LAN クライアントモード設定

MR-GM5A を無線 LAN クライアントとして、他の無線 LAN アクセスポイントに接続する方法について説明します。

確認	本機能については当社製品(MR-GM5A、MR-GM3)との接続のみ動作保証します。 他社無線 LAN 製品との接続については、動作保証及びユーザーサポートの対象外です。
	無線 LAN クライアント機能は、無線 LAN1 (5GHz)、無線 LAN2 (2.4GHz) どちらか片方のみで利用可能です。 両方を無線 LAN クライアントとして使用する事はできません。
	設定を行う前に、接続先無線 LAN アクセスポイントの SSID、暗号モード、事前共有鍵(暗号キー)の情報を 用意して下さい。

以下の使用環境を例に設定方法を説明します。



以下の各設定を行って下さい。

- 4-4-1.LAN 設定 (LAN ポート IP アドレスの変更)
- 4-4-2.DHCP 設定 (DHCP サーバ機能の無効化)
- 4-4-3.無線 LAN 基本設定 (クライアントモードへ変更)
- 4-4-4.サイトサーベイから接続する (アクセスポイントのブロードキャスト SSID が有効の場合)
- 4-4-5.手動設定で接続する (アクセスポイントのブロードキャスト SSID が無効の場合)

4-4-1.LAN 設定 (LAN ポート IP アドレスの変更)

アクセスポイントや他の機器と IP アドレスが重複しないように、MR-GM5A の LAN ポート IP アドレスを変更します。
以下の手順で設定を行って下さい。
設定メニューの「ネットワーク設定」より「LAN 設定」をクリックして下さい。

ステータス + 無線LAN - ネットワーク LAN 設定 WAN 設定 + VPN + ファイアウォール + 付加機能 + マネージメント	LAN 設定 このページではLANインターフェースの設定が行えます。IPアドレス、
	インターフェース名: br0
	IPアドレス: 192.168.0.254
	サブネットマスク: 255.255.255.0
	DHCP 設定

■IP アドレス

LAN 内の他の機器と重複しない IP アドレスを設定して下さい。

4-4-2.DHCP 設定 (DHCP サーバー機能の無効化)

LAN 内に他の DHCP サーバーが存在する場合は、MR-GM5A の DHCP サーバー機能を無効に設定します。

DHCP 設定	
DHCP モード:	<input checked="" type="radio"/> なし <input type="radio"/> DHCP サーバー
IP 付与範囲:	192.168.0.2 - 192.168.0.30 <input type="button" value="クライアント表示"/>
リース期限:	86400 秒 (-1を指定すると無期限リースになります。)
ドメイン名:	MR-GM5A
DNS オプション:	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定
プライマリー DNSサーバー:	<input type="text"/>
セカンダリー DNSサーバー:	<input type="text"/>
<input type="button" value="設定保存"/> <input type="button" value="固定IPアドレス付与"/>	

■DHCP モード

LAN 内に他の DHCP サーバーが存在する場合、「なし」を選択して下さい。

設定が終わりしたら、[設定保存]ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

4-4-3.無線 LAN 基本設定(クライアントモードへ変更)

無線 LAN のモードをクライアントに変更します。
(以降、無線 LAN ポート 1(5GHz)の画面を例に説明します。)

設定メニューの「無線 LAN 設定」の「無線 LAN1(5GHz)」より「基本設定」をクリックして下さい。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーベイ WPS 設定 + 無線LAN2 (2.4GHz)	無線LAN1 基本 設定 このページでは無線LANの基本的なパラメーターの設定が行えます。 <input type="checkbox"/> 無線LANを無効にする バンド: 5 GHz (A+N+AC+AX) ▾ モード: クライアント ▾ SSID: MR-GM5A 5G 帯域幅: 80MHz ▾
---	---

■モード

「**クライアント**」を選択して下さい。

設定が終わりましたら、「設定保存」ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、「今すぐ再起動」ボタンを押して下さい。

再起動完了後は、「4-4-1.LAN 設定(LAN ポート IP アドレスの変更)」(58 ページ)で設定した LAN 側 IP アドレスを入力してして設定画面にログインし直して下さい。

確認

DHCP サーバー機能を無効にした場合、以降の設定はパソコンの IP アドレスを固定して行って下さい。

4-4-4. サイトサーベイから接続する

接続先アクセスポイントが SSID をブロードキャストしている場合、サイトサーベイから接続する事が可能です。
 設定メニューより無線 LAN クライアント機能を使用する無線 LAN ポート(「無線 LAN1 (5GHz)」 「無線 LAN2 (2.4GHz)」)の「サイトサーベイ」をクリックして下さい。
 (以降、無線 LAN ポート 1 (5GHz) の画面を例に説明します。)
 無線 LAN アクセスポイントの一覧が表示されますので、接続先アクセスポイントを選択し、[次へ]ボタンをクリックして下さい。

ステータス

- 無線LAN
- 無線LAN1 (5GHz)
- 基本設定
- 拡張設定
- セキュリティ設定
- アクセス制御設定
- サイトサーベイ**
- WPS設定
- + 無線LAN2 (2.4GHz)
- + ネットワーク
- + ファイアウォール
- + 付加機能
- + マネージメント

無線LAN1 サイトサーベイ

このページでは他の無線LANアクセスポイントの状況を表示します。

SSID	BSSID	チャンネル	タイプ	暗号モード	電波強度(%)	選択
MR-GM5A 5G	00:10:38: [REDACTED]	100 (A+N+AC+AX) 80MHz	AP	WPA3/WPA2-PSK	67	<input checked="" type="radio"/>
[REDACTED]	[REDACTED]	36 (A+N+AC+AX) 80MHz	AP	WPA3/WPA2-PSK	65	<input type="radio"/>
[REDACTED]	[REDACTED]	64 (A+N+AC) 80MHz	AP	WPA2-PSK	61	<input type="radio"/>
[REDACTED]	[REDACTED]	48 (A+N+AC) 80MHz	AP	WPA2-PSK	55	<input type="radio"/>
[REDACTED]	[REDACTED]	40 (A+N+AC+AX) 80MHz	AP	no	52	<input type="radio"/>
[REDACTED]	[REDACTED]	56 (A+N+AC) 80MHz	AP	WPA2-PSK	47	<input type="radio"/>
[REDACTED]	[REDACTED]	40 (A+N+AC+AX) 80MHz	AP	WPA3/WPA2-PSK	41	<input type="radio"/>

再読み込み 次へ

確認

サイトサーベイに接続先アクセスポイントが表示されない場合、アクセスポイントが SSID をブロードキャストしていない可能性があります。
 その場合は、「4-4-5. 手動設定で接続する」(61 ページ)の手順で接続設定を行って下さい。

アクセスポイントへ接続するための事前共有鍵(暗号キー)を入力して[接続]ボタンをクリックして下さい。

暗号モード: WPA3 Transition

認証モード: Enterprise (RADIUS) Personal (Pre-Shared Key)

H2E: Capable Required

管理フレーム保護 (802.11w): None Capable Required

SHA256 暗号: Disable Enable

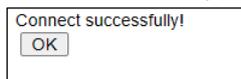
WPA2 暗号方式: TKIP AES

事前共有鍵フォーマット: Passphrase

事前共有鍵:

戻る 接続

以下のメッセージが表示されるたら[OK]ボタンをクリックして下さい。



設定メニューより「ステータス」をクリックして下さい。
 クライアントモードで設定した無線 LAN のステータスが「接続」と表示されていれば接続完了です。

無線LAN1	
動作モード	クライアント
バンド	5 GHz (A+N+AC+AX)
SSID	MR-GM5A 5G
チャンネル番号	100
暗号モード	WPA3
BSSID	00:10:38: [REDACTED]
ステータス	接続

4-4-5. 手動設定で接続する

接続先アクセスポイントのブロードキャスト SSID が無効の場合、手動設定で接続して下さい。

- ① 設定メニューより無線 LAN クライアント機能を使用する無線 LAN ポート(「無線 LAN1 (5GHz)」 「無線 LAN2 (2.4GHz)」)の「基本設定」をクリックして下さい。
(以降、無線 LAN ポート 1 (5GHz) の画面を例に説明します。)

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーベイ WPS設定 + 無線LAN2 (2.4GHz)	無線LAN1 基本設定 このページでは無線LANの基本的なパラメーターの設定が行えます。	
	<input type="checkbox"/> 無線LANを無効にする	
	バンド:	5 GHz (A+N+AC+AX) ▼
	モード:	クライアント ▼
	SSID:	MR-GM5A 5G
	帯域幅:	80MHz ▼
	<input type="button" value="設定保存"/>	

■モード

「**クライアント**」を選択して下さい。

■SSID

接続先アクセスポイントの SSID を入力して下さい。

- ② 設定が終わりましたら、[設定保存]ボタンをクリックして下さい。
「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

- ③ 設定メニューより無線 LAN クライアント機能を使用する無線 LAN ポート(「無線 LAN1 (5GHz)」 「無線 LAN2 (2.4GHz)」)の「セキュリティ設定」をクリックして下さい。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーベイ WPS設定 + 無線LAN2 (2.4GHz) + ネットワーク + ファイアウォール + 附加機能 + マネージメント	無線LAN1 セキュリティ設定 このページでは無線LANのセキュリティの設定が行えます。	
	SSID タイプ:	Root Client - MR-GM5A 5G ▼
	暗号モード:	WPA3 Transition ▼
	H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
	管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
	SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
	暗号方式:	<input checked="" type="checkbox"/> AES
	ブロードキャスト暗号鍵 更新間隔:	86400
	事前共有鍵:
	<input type="button" value="設定保存"/>	

■モード

「**Root Client - “接続アクセスポイントの SSID”**」を選択して下さい。

■事前共有鍵

アクセスポイントへ接続するための事前共有鍵(暗号キー)を入力して下さい。

- ④ 設定が終わりましたら、[設定保存]ボタンをクリックして下さい。
「設定は正常に保存されました。」と表示されますので、「今すぐ再起動」ボタンを押して下さい。

〈次ページへ進んで下さい〉

- ⑤再起動が完了しましたら、設定メニューより「ステータス」をクリックして下さい。
クライアントモードで設定した無線 LAN のステータスが「接続」と表示されていれば接続完了です。

無線LAN1	
動作モード	クライアント
バンド	5 GHz (A+N+AC+AX)
SSID	MR-GM5A 5G
チャンネル番号	100
暗号モード	WPA3
BSSID	00:10:38: [REDACTED]
ステータス	接続

4-5.ユニバーサルリピーターモード設定

MR-GM5A を無線 LAN 中継機として、他の無線 LAN アクセスポイントに接続するユニバーサルリピーターモードの設定について説明します。

確認

**本機能については当社製品(MR-GM5A、MR-GM3)との接続のみ動作保証します。
他社無線 LAN 製品との接続については、動作保証及びユーザーサポートの対象外です。**

設定を行う前に、接続先無線 LAN アクセスポイントの SSID、暗号モード(WPA、WEP 等)、セキュリティキー(暗号キー/事前共有キー)の情報を用意して下さい。

以下の使用環境を例に設定方法を説明します。



以下の各設定を行って下さい。

4

エラー! 参照元が見つかりません。

4-5-3.無線 LAN 基本設定

4-5-4.無線 LAN セキュリティ設定

4-5-1.LAN 設定 (LAN ポート IP アドレスの変更)

アクセスポイントや他の機器と IP アドレスが重複しないように、MR-GM5A の LAN ポート IP アドレスを変更します。
以下の手順で設定を行って下さい。
設定メニューの「ネットワーク設定」より「LAN 設定」をクリックして下さい。

ステータス + 無線LAN - ネットワーク LAN 設定 WAN 設定 + VPN + ファイアウォール + 付加機能 + マネージメント	LAN 設定 このページではLANインターフェースの設定が行えます。IPアドレス、
	インターフェース名: br0
	IPアドレス: 192.168.0.254
	サブネットマスク: 255.255.255.0
	DHCP 設定

■IP アドレス

LAN 内の他の機器と重複しない IP アドレスを設定して下さい。

4-5-2.DHCP 設定 (DHCP サーバー機能の無効化)

LAN 内に他の DHCP サーバーが存在する場合は、MR-GM5A の DHCP サーバー機能を無効に設定します。

DHCP 設定	
DHCP モード:	<input checked="" type="radio"/> なし <input type="radio"/> DHCP サーバー
IP 付与範囲:	192.168.0.2 - 192.168.0.30 <input type="button" value="クライアント表示"/>
リース期限:	86400 秒 (-1を指定すると無期限リースになります。)
ドメイン名:	MR-GM5A
DNS オプション:	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定
プライマリー DNSサーバー:	<input type="text"/>
セカンダリー DNSサーバー:	<input type="text"/>
<input type="button" value="設定保存"/> <input type="button" value="固定IPアドレス付与"/>	

■DHCP モード

LAN 内に他の DHCP サーバーが存在する場合、「なし」を選択して下さい。

設定が終わりましたら、[設定保存]ボタンをクリックして下さい。

「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

4-5-3.無線 LAN 基本設定(ユニバーサルリピーターモードの設定)

- ①設定メニューの「無線 LAN 設定」よりユニバーサルリピーター機能を使用する無線 LAN ポート(「無線 LAN1(5GHz)」 「無線 LAN2(2.4GHz)」)の「基本設定」をクリックして下さい。
(以降、無線 LAN ポート 1(5GHz)の画面を例に説明します。)
「基本設定」画面が開きます。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本設定 拡張設定 セキュリティ設定 アクセス制御設定 サイトサーベイ WPS設定 + 無線LAN2 (2.4GHz)	無線LAN1 基本設定 このページでは無線LANの基本的なパラメーターの設定が行えます。 <input type="checkbox"/> 無線LANを無効にする バンド: 5 GHz (A+N+AC+) モード: アクセスポイント SSID: MR-GM5A 5G 帯域幅: 80MHz
--	---

- ②無線 LAN 動作モードで「**アクセスポイント**」を選択して下さい。
SSID に MR-GM5A の SSID を入力して下さい。

無線LAN1 基本設定 このページでは無線LANの基本的なパラメーターの設定が行えます。	
<input type="checkbox"/> 無線LANを無効にする	
バンド:	5 GHz (A+N+AC+AX)
モード:	アクセスポイント
SSID:	MR-GM5A 5G
帯域幅:	80MHz
サイドバンド制御:	自動

- ③「ユニバーサルリピーター機能を有効にする」にチェックを入れて下さい。
リピーターSSID に接続先アクセスポイントの SSID を入力して下さい。
設定が終わりましたら、[設定保存]ボタンをクリックして下さい。

接続中クライアント数:	クライアント表示
<input checked="" type="checkbox"/> ユニバーサルリピーター機能を有効にする	
リピーター SSID:	MRL_AP
設定保存	

「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

4-5-4.無線 LAN セキュリティ設定

以下の手順で無線 LAN セキュリティ設定を行って下さい。

- ①設定メニューの「無線 LAN 設定」よりユニバーサルリピーター機能を使用する無線 LAN ポート(「無線 LAN1 (5GHz)」 「無線 LAN2 (2.4GHz)」)の「セキュリティ設定」をクリックして下さい。
「無線 LAN セキュリティ設定」画面が開きます。

ステータス - 無線LAN - 無線LAN1 (5GHz) 基本 設定 拡張 設定 セキュリティ 設定 アクセス制御 設定 サイトサーバイ WPS 設定	無線LAN1 セキュリティ 設定 このページでは無線LANのセキュリティの設定が行えます。 SSID タイプ: Root AP - MR-GM5A 5G 暗号モード: WPA3 Transition H2E: <input checked="" type="radio"/> 可能 <input type="radio"/> 必須 管理フレーム保護 (802.11w): <input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須 SHA256 暗号: <input type="radio"/> 無効 <input checked="" type="radio"/> 有効
---	--

- ②「SSID タイプ」で「Root AP - “MR-GM5A の SSID”」を選択して下さい。
MR-GM5A に接続するための「暗号モード」「暗号キー」の設定等を行って下さい。

無線LAN1 セキュリティ 設定 このページでは無線LANのセキュリティの設定が行えます。	
SSID タイプ:	Root AP - MR-GM5A 5G
暗号モード:	WPA3 Transition
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵: <input type="checkbox"/> パスワード表示
設定保存	

- ③「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

- ④「SSID タイプ」で「Repeater AP - “接続先アクセスポイントの SSID”」を選択して下さい。
接続先アクセスポイントのセキュリティ設定に合わせて、「暗号モード」「暗号キー」の設定等を行って下さい。

無線LAN1 セキュリティ 設定 このページでは無線LANのセキュリティの設定が行えます。	
SSID タイプ:	Repeater AP - MRL_AP
暗号モード:	WPA3 Transition
H2E:	<input checked="" type="radio"/> 可能 <input type="radio"/> 必須
管理フレーム保護 (802.11w):	<input type="radio"/> なし <input checked="" type="radio"/> 可能 <input type="radio"/> 必須
SHA256 暗号:	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
暗号方式:	<input checked="" type="checkbox"/> AES
ブロードキャスト暗号鍵 更新間隔:	86400
事前共有鍵: <input type="checkbox"/> パスワード表示
設定保存	

- ⑤設定が終わりましたら、[設定保存]ボタンをクリックして下さい。
「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

⑥再起動が完了した後、「ステータス」画面の「無線 LAN リピーターインターフェース」の「ステータス」が「接続」と表示されていれば無線 LAN アクセスポイントと接続完了です。

無線LAN1	
動作モード	アクセスポイント
バンド	5 GHz (A+N+AC+AX)
SSID	MR-GM5A 5G ※1
チャンネル番号	44
暗号モード	WPA3 Transition
BSSID	00:10:38:3d:31:92
接続中クライアント数	0

無線LAN リピーターインターフェース	
動作モード	クライアント
SSID	MRL_AP※2
暗号モード	WPA2
BSSID	00:10:38:37:86:12
ステータス	接続

MR-GM5A に設定した SSID(※1)に接続すると、リピーターインターフェースで接続した無線 LAN アクセスポイント(※2)の通信が中継されます。

5. ネットワーク設定

ネットワーク設定についてします。

5-1. LAN 設定

本製品の IP アドレス設定、DHCP サーバー設定について説明します。
「ネットワーク」から「LAN 設定」をクリックして下さい。

ステータス + 無線LAN - ネットワーク LAN 設定 WAN 設定 + VPN + ファイアウォール + 付加機能 + マネージメント	LAN 設定 このページではLANインターフェースの設定が行えます。IPアドレス、 <table border="1"><tr><td>インターフェース名:</td><td>br0</td></tr><tr><td>IPアドレス:</td><td><input type="text" value="192.168.0.1"/></td></tr><tr><td>サブネットマスク:</td><td><input type="text" value="255.255.255.0"/></td></tr></table> DHCP 設定	インターフェース名:	br0	IPアドレス:	<input type="text" value="192.168.0.1"/>	サブネットマスク:	<input type="text" value="255.255.255.0"/>
インターフェース名:	br0						
IPアドレス:	<input type="text" value="192.168.0.1"/>						
サブネットマスク:	<input type="text" value="255.255.255.0"/>						

5-1-1. LAN ポート IP アドレス設定

LAN 設定 このページではLANインターフェースの設定が行えます。IPアドレス、サブネットマスクなどの設定を変更できます。	
インターフェース名:	br0
IPアドレス:	<input type="text" value="192.168.0.1"/>
サブネットマスク:	<input type="text" value="255.255.255.0"/>



注意

本製品の IP アドレス(工場出荷値: 192.168.0.1)を変更する場合、他のパソコン、ルーター等と IP アドレスが衝突しないように注意して下さい。
万が一、他のパソコン等と本製品の IP アドレスが衝突してしまった場合、本製品の設定画面が開けない、他のネットワーク機器に障害が発生する等、さまざまなトラブルの原因となりますので注意して下さい。

■ インターフェース名

「br0」固定です。

■ IP アドレス

本製品の LAN 側 IP アドレスを設定します。
工場出荷状態では「192.168.0.1」が設定されています。

■ サブネットマスク

本製品のサブネットマスクを設定します。
工場出荷状態では「255.255.255.0」が設定されています。

5-1-2.DHCP サーバー設定

DHCP 設定	
DHCP モード:	<input type="radio"/> なし <input checked="" type="radio"/> DHCP サーバー
IP 付与範囲:	<input type="text" value="192.168.0.2"/> - <input type="text" value="192.168.0.30"/> <input type="button" value="クライアント表示"/>
サブネットマスク:	<input type="text" value="255.255.255.0"/>
リース期限:	<input type="text" value="86400"/> 秒 (-1を指定すると無制限リースになります。)
ドメイン名:	<input type="text" value="MR-GM5A"/>
ゲートウェイアドレス:	<input type="text" value="192.168.0.1"/>
DNS オプション:	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定
プライマリー DNSサーバー:	<input type="text"/>
セカンダリー DNSサーバー:	<input type="text"/>
<input type="button" value="設定保存"/> <input type="button" value="固定IPアドレス付与"/>	

■ DHCP モード(ラジオボタン)

DHCP サーバー機能の有効/無効を切り替えます。

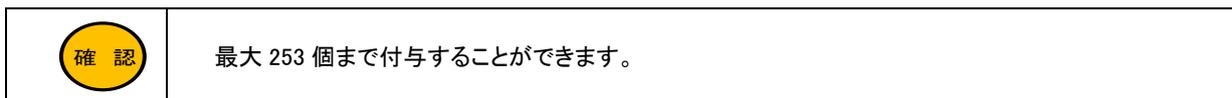
なし :DHCP サーバーを無効にします。

DHCP サーバー :DHCP サーバーを有効にします。

■ IP 付与範囲

DHCP サーバー機能を有効にした場合の付与 IP アドレス範囲を設定します。

工場出荷状態では「192.168.0.2～192.168.0.30」の範囲が設定されています。



■ サブネットマスク

付与するサブネットマスクを設定します。

工場出荷状態では「255.255.255.0」が設定されています。

■ リース期限

付与する IP アドレスのリース期限(時間)を設定します。

工場出荷状態では「86400 秒」(24 時間)が設定されています。-1 を指定すると無制限リースとなります。

■ ドメイン名

DHCP サーバー機能で割り当てるドメイン名を設定します。

初期値は「MR-GM5A」が設定されています。

通常は初期値のままお使い下さい。

■ ゲートウェイアドレス

DHCP サーバー機能で割り当てるゲートウェイアドレスを設定します。

初期値は MR-GM5A の LAN ポート IP アドレスが設定されています。

通常は初期値のままお使い下さい。

■ DNS オプション(ラジオボタン)

自動設定: DNS サーバーとして、MR-GM5A の LAN ポート IP アドレスを付与します。

手動設定: DNS サーバーとして付与する IP アドレスを設定します。DNS サーバーは 2 つまで設定することができます。

■ 設定保存(ボタン)

設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

<次ページへ進んで下さい>

■クライアント表示(ボタン)

DHCP サーバーから IP アドレスを取得しているクライアントの情報(別ウィンドウ)を表示します。

DHCPクライアント		
このページではIPアドレスをリースしたクライアントのIPアドレス、MACアドレス、リース期限を表示します。		
IPアドレス	MACアドレス	有効期限(秒)
192.168.0.2	00:10:38:xx:xx:xx	79141
再読み込み 閉じる		

■固定 IP アドレス付与(ボタン)

固定 IP アドレス付与設定画面が開きます。

MAC(物理)アドレスにより、固定の IP アドレスを付与します。

DHCP 固定IPアドレス付与 設定	
このページではMACアドレスをベースとした固定IPアドレス付与の設定を行います。	
状態:	<input checked="" type="checkbox"/> 登録を有効にする
MACアドレス:	<input type="text"/>
付与IPアドレス:	<input type="text"/>
登録 設定反映 戻る	

●状態(チェックボタン)

登録する固定 IP アドレス付与情報の有効にする場合チェックを入れて下さい。

●MAC アドレス

付与する機器の MAC アドレスを入力します。

●付与 IP アドレス

付与する IP アドレスを入力して下さい。

●登録(ボタン)

入力した内容が登録リストに追加されます。

	最大 8 エントリまで登録可能です。
---	--------------------

●設定反映(ボタン)

設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は、「今すぐ再起動」ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

固定IPアドレス付与 登録リスト			
選択	状態	MACアドレス	付与IPアドレス
<input type="checkbox"/>	有効	00-10-38-11-11-11	192.168.0.5
選択した登録を編集 選択した登録を削除 全て削除			

●選択した登録を編集(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。

●選択した登録を削除(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。

5-2.WAN 設定

WAN 設定について説明します。

「ネットワーク」から「WAN 設定」をクリックして下さい。

「WAN 設定」画面が表示されます。

ステータス
+ 無線LAN
- ネットワーク
 LAN 設定
 WAN 設定
 + VPN
+ ファイアウォール
+ 付加機能
+ マネージメント

WAN 設定
このページではWANインターフェースの設定が行えます。

WAN回線運用

WANバックアップ:	無効
プライマリ接続モード:	有線WAN
セカンダリ接続モード:	有線WAN
プライマリ通信確認間隔:	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定:	有線WAN 内蔵モバイル USBモバイル

各WAN回線設定ボタンを押下すると、このページで変更

使用する WAN 側接続モードに応じて、各項目を参照して下さい。

5-2-1.内蔵モバイル設定(72 ページ)

5-2-2.USB モバイル設定(74 ページ)

5-2-3.有線 WAN 設定:DHCP(76 ページ)

5-2-4.有線 WAN 設定:固定 IP(77 ページ)

5-2-5.有線 WAN 設定:PPPoE(78 ページ)

5-2-6.有線 WAN 設定:transix(DS-Lite)(79 ページ)

5-2-7.有線 WAN 設定:IPoE IPv6(80 ページ)

5-2-8.有線 WAN 設定:Bridge(81 ページ)



ETH1ポートをLANポートとして使用する場合、「5-2-8.有線WAN設定:Bridge」を行って下さい。

WAN 側接続モードの設定が完了したら、「5-2-9. WAN 設定:共通設定」(82 ページ)へ進んで下さい。

5-2-1.内蔵モバイル設定

[内蔵モバイル]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	有線WAN 内蔵モバイル USBモバイル

各WAN回線設定ボタンを押下すると、このページで変更し

「内蔵モバイル設定」画面が開きます。

「内蔵モバイル WAN」を「有効」にして下さい。

内蔵モバイル設定	
このページでは内蔵モバイルによるWAN接続設定が行えます。	
内蔵モバイル WAN:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
接続先:	<input type="text"/>
ユーザー名:	<input type="text"/>
パスワード:	<input type="text"/>
APN:	<input type="text"/>
CID:	1
発信先電話番号:	*99***1#
MTUサイズ:	1420 (64~1492)
DNS:	自動取得
プライマリー DNSサーバー:	<input type="text"/>
セカンダリー DNSサーバー:	<input type="text"/>
接続待ち時間:	0 時 1 分 0 秒 (0~16時間)

■接続先

利用する契約プラン名を選択して下さい。

契約プランを選択すると、キャリア選択、ユーザー名、パスワード、APN、CID、発信先電話番号が自動的に設定されます。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。

■ユーザー名、パスワード、APN、CID、発信先電話番号

接続先で契約プランを選択すると、ユーザー名、パスワード、APN、CID、発信先電話番号が自動的に設定されます。接続先で「その他」を選択すると、任意の値が設定できます。

	「発信先電話番号」に SIM カードの電話番号は入力しないで下さい。
	「発信先電話番号」は、契約プロバイダの指定が無い場合「*99***1#」(初期値)のままご利用下さい。
	接続情報に関する最新情報は以下のサイトをご参照下さい。 MR-GM5A 内蔵通信モジュール設定情報 https://www.mrl.co.jp/products/gm5a/gm5a_series_sim/

■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。
設定可能範囲は「64~1492」(バイト)です。

■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ー/セカンダリーDNS サーバーの 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。

■接続待ち時間

ここで設定した時間内に応答が無い場合、再接続を行います。
通常は初期値「1 分」のままご利用下さい。

<次ページへ進んで下さい>

接続リトライ:	<input type="text" value="5"/> 回 (0~9回)
デバイス再起動リトライ:	<input type="text" value="5"/> 回 (0~9回)
内蔵モバイルから時刻を取得:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
電波強度取得間隔:	<input type="text" value="60"/> 秒 (0~3600秒)
電波強度不足検出回数:	<input type="text" value="3"/> 回 (1~100回)
電波強度ログ出力間隔:	<input type="text" value="60"/> 回 (0~3600回)
<input type="button" value="設定"/> <input type="button" value="戻る"/>	

■接続リトライ

ここで設定した回数連続して失敗した場合、内蔵通信モジュールの電源を OFF/ON します。通常は初期値「5 回」のままご利用下さい。

■デバイス再起動リトライ

ここで設定した回数、内蔵通信モジュールの電源の OFF/ON が行われた場合、MR-GM5A を再起動します。「0 回」を設定した場合、再起動しません。

■内蔵モバイルから時刻を取得

内蔵通信モジュールから時刻情報を取得します。

	<p>内蔵モバイルが接続時に時刻を取得します。 内蔵モバイル未接続時は時刻取得できません。</p>
---	---

■電波強度取得間隔

ここで設定した間隔で電波強度を取得します。

■電波強度不足検出回数

ここで設定した回数連続で電波強度不足 (Signal Quality 0) を検出すると再接続を行います。

■電波強度ログ出力間隔

ここで設定した回数電波強度を取得するとログに出力します。

設定が終わりましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定: 共通設定」(82 ページ)へ進んで下さい。

5-2-2.USB モバイル設定

[USB モバイル]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	有線WAN 内蔵モバイル USBモバイル

各WAN回線設定ボタンを押下すると、このページで変更し

「USB モバイル設定」画面が開きます。

「USB モバイル WAN」を「有効」にして下さい。

USBモバイル設定	
このページではUSBモバイルによるWAN接続設定が行えます。	
USBモバイル WAN:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
接続先:	<input type="text"/>
キャリア:	自動
ユーザー名:	<input type="text"/>
パスワード:	<input type="text"/>
APN:	<input type="text"/>
CID:	1
発信先電話番号:	*99***1#
PDPタイプ:	IP
MTUサイズ:	1490 (64~1492)
DNS:	自動取得
プライマリー DNSサーバー:	<input type="text"/>
セカンダリー DNSサーバー:	<input type="text"/>

■接続先

利用する契約プラン名を選択して下さい。

契約プランを選択すると、キャリア選択、ユーザー名、パスワード、APN、CID、発信先電話番号が自動的に設定されます。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。

■キャリア

通常は「自動」のままご利用下さい。

■ユーザー名、パスワード、APN、CID、発信先電話番号

接続先で契約プランを選択すると、ユーザー名、パスワード、APN、CID、発信先電話番号が自動的に設定されます。接続先で「その他」を選択すると、任意の値が設定できます。

■PDP タイプ

通常は「IP」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。設定可能範囲は「64~1492」(バイト)です。

■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ー/セカンダリーDNS サーバーの 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。

〈次ページへ進んで下さい〉

PPP認証方式:	自動 ▾
PPP接続待ち時間:	0 時 3 分 0 秒 (0~16時間)
PPP接続リトライ:	5 回 (0~9回)
USBデバイス検出待ち時間:	5 分 0 秒 (0~1時間)
USBデバイス検出リトライ回数:	5 回 (0~9回)
USBデバイス切替待ち時間:	0 秒 (0~99秒)
追加ATコマンド:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 <input type="text"/>
<input type="button" value="設定"/> <input type="button" value="戻る"/>	

■ PPP 認証方式

PPP 認証方式を設定します。「PAP」認証、「CHAP」認証の固定設定が可能です。通常は初期値「自動」のままご利用下さい。

■ PPP 接続待ち時間

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「3 分」のままご利用下さい。

■ PPP 接続リトライ

ここで設定した回数連続して失敗した場合、USB ポートの電源を OFF/ON します。通常は初期値「5 回」のままご利用下さい。

■ USB デバイス検出待ち時間

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。「0 秒」の場合、USB データカードが応答するまで待ち続けます。



回線冗長化機能有効時は、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、回線(デフォルトゲートウェイ)を切り替えます。

■ USB デバイス検出リトライ回数

ここで設定した回数、USB ポートの電源を OFF/ON が行われた場合に MR-GM5A が再起動します。通常は初期値「5 回」のままご利用下さい。

■ USB データカード切替待ち時間

USB データカードのモードを切り替えるまでの待ち時間を設定します。通常は初期値「0 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、「有効」を選択し、AT コマンドを入力して下さい。

設定が完了しましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定: 共通設定」(82 ページ)へ進んで下さい。

5-2-3.有線 WAN 設定:DHCP

「WAN 設定」画面の[有線 WAN]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	<input checked="" type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>

各WAN回線設定ボタンを押下すると、このページで変更し

「有線 WAN 設定」画面が開きますので各項目の設定を行って下さい。

有線WAN設定 このページでは有線WANインターフェースの設定が行なえます。	
接続モード:	IPoE
IP プロトコル:	IPv4
WAN IP 設定:	
タイプ:	<input type="radio"/> 固定IP <input checked="" type="radio"/> DHCP
IPアドレス:	
サブネットマスク:	
ゲートウェイ:	
MTUサイズ:	1500 (64~1500)
DNS:	自動取得
プライマリー DNSサーバー:	
セカンダリー DNSサーバー:	
接続待ち時間:	0 時 1 分 0 秒 (0~16時間)
<input type="button" value="設定"/> <input type="button" value="戻る"/>	

■接続モード

「IPoE」を選択して下さい。

■IP プロトコル

「IPv4」を選択して下さい。

「IPv6」「IPv4/IPv6」を選択した場合の IPv6 の設定については「5-2-7.有線 WAN 設定:IPoE IPv6」(80 ページ)を参照して下さい。

■タイプ

「DHCP」を選択して下さい。

■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。

通常は初期値のままご利用下さい。

設定可能範囲は「64~1500」(バイト)です。

■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ー/セカンダリーDNS サーバーの 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。

■接続待ち時間

通常は変更せず初期値「1 分」のままご利用下さい。

設定が終わりましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定:共通設定」(82 ページ)へ進んで下さい。

5-2-4.有線 WAN 設定:固定 IP

「WAN 設定」画面の[有線 WAN]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	<input checked="" type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>

各WAN回線設定ボタンを押下すると、このページで変更し

「有線 WAN 設定」画面が開きますので各項目の設定を行って下さい。

有線WAN設定 このページでは有線WANインターフェースの設定が行なえます。	
接続モード:	IPoE
IP プロトコル:	IPv4
WAN IP 設定:	
タイプ:	<input checked="" type="radio"/> 固定IP <input type="radio"/> DHCP
IPアドレス:	192.168.254.254
サブネットマスク:	255.255.255.0
ゲートウェイ:	192.168.254.1
MTUサイズ:	1500 (64~1500)
DNS:	手動設定
プライマリー DNSサーバー:	192.168.254.1
セカンダリー DNSサーバー:	192.168.254.2
接続待ち時間:	0 時 1 分 0 秒 (0~16時間)
<input type="button" value="設定"/> <input type="button" value="戻る"/>	

■接続モード

「IPoE」を選択して下さい。

■IP プロトコル

「IPv4」を選択して下さい。

「IPv6」「IPv4/IPv6」を選択した場合の IPv6 の設定については「5-2-7.有線 WAN 設定 :IPoE IPv6」(80 ページ)を参照して下さい。

■タイプ

「固定 IP」を選択して下さい。

■IP アドレス、サブネットマスク、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。

通常は初期値のままご利用下さい。

設定可能範囲は「64~1500」(バイト)です。

■DNS

「手動設定」を選択してプライマリー/セカンダリーDNS サーバーの 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。

設定が終わりましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定: 共通設定」(82 ページ)へ進んで下さい。

5-2-5.有線 WAN 設定:PPPoE

「WAN 設定」画面の[有線 WAN]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	有線WAN 内蔵モバイル USBモバイル

各WAN回線設定ボタンを押下すると、このページで変更し

「有線 WAN 設定」画面が開きますので各項目の設定を行って下さい。

有線WAN設定	
このページでは有線WANインターフェースの設定が行えます。	
接続モード:	PPPoE
PPPoE 設定:	
ユーザー名:	
パスワード:	
サービス名:	
MTUサイズ:	1452 (64~1492)
DNS:	自動取得
プライマリー DNSサーバー:	
セカンダリー DNSサーバー:	
認証方式:	AUTO
接続待ち時間:	0 時 1 分 0 秒 (0~16時間)
設定	戻る

■接続モード

「PPPoE」を選択して下さい。

■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。

■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。
設定可能範囲は「64~1492」(バイト)です。

■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ー/セカンダリーDNS サーバーの 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。

■認証方式

PPP 認証方式を設定します。「PAP」認証、「CHAP」認証の固定設定が可能です。
通常は初期値「AUTO」のままご利用下さい。

■接続待ち時間

PPPoE 接続待ち時間を設定します。
通常は変更せず初期値「1 分」のままご利用下さい。

設定が完了したら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定: 共通設定」(82 ページ)へ進んで下さい。

5-2-6.有線 WAN 設定 :transix (DS-Lite)

「WAN 設定」画面の[有線 WAN]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	有線WAN 内蔵モバイル USBモバイル

各WAN回線設定ボタンを押下すると、このページで変更し

「有線 WAN 設定」画面が開きますので各項目の設定を行って下さい。

有線WAN設定	
このページでは有線WANインターフェースの設定が行えます。	
接続モード:	transix (DS-Lite)
IPv6 WAN 設定:	
アドレス取得方法:	自動検出
AFTR アドレスモード:	<input checked="" type="radio"/> 自動設定 <input type="radio"/> 手動設定
AFTR アドレス:	<input type="text"/>
設定	戻る

■接続モード

「transix (DS-Lite)」を選択して下さい。

■アドレス取得方法

「自動検出」固定設定です。

■AFTR アドレスモード、AFTR アドレス

ご契約のプロバイダから指定が無い場合は「自動設定」のままご利用下さい。
指定がある場合は、「手動設定」を選択し、AFTR アドレスを入力して下さい。

設定が終わりましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定 : 共通設定」(82 ページ)へ進んで下さい。

5-2-7.有線 WAN 設定:IPoE IPv6

「WAN 設定」画面の[有線 WAN]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN
プライマリ通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	<input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>

各WAN回線設定ボタンを押下すると、このページで変更し

「有線 WAN 設定」画面が開きますので各項目の設定を行って下さい。

有線WAN設定	
このページでは有線WANインターフェースの設定が行えます。	
接続モード:	IPoE
IP プロトコル:	IPv6
IPv6 WAN 設定:	
アドレス取得方法:	自動検出
<input type="button" value="設定"/>	<input type="button" value="戻る"/>

■接続モード

「IPoE」を選択して下さい。

■IP プロトコル

「IPv6」もしくは「IPv4/IPv6」を選択して下さい。

■WAN IPv6 設定:アドレス取得方法:

「自動検出」固定設定です。

IPv6 アドレスの取得方法(SLAAC/DHCPv6)は自動判別されます。

設定が終わりましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定: 共通設定」(82 ページ)へ進んで下さい。

5-2-8.有線 WAN 設定:Bridge



ETH1ポートをLANポートとして使用する場合、本設定を行って下さい。

[有線 WAN]ボタンをクリックして下さい。

セカンダリー接続モード	有線WAN ▼
プライマリー通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	有線WAN 内蔵モバイル USBモバイル

各WAN回線設定ボタンを押下すると、このページで変更し

有線 WAN 設定が開きますので各項目の設定を行って下さい。

有線WAN設定

このページでは有線WANインターフェースの設定が行なえます。

接続モード: Bridge ▼

設定 戻る

■接続モード

「Bridge」を選択して下さい。

設定が終わりましたら[設定]ボタンを押して下さい。

「5-2-9. WAN 設定: 共通設定」(82 ページ)へ進んで下さい。

5-2-9. WAN 設定:共通設定

WAN 設定画面の設定項目について説明します。

WAN 設定	
このページではWANインターフェースの設定が行なえます。	
WAN回線運用	
WANバックアップ	無効
プライマリ接続モード	内蔵モバイル
セカンダリ接続モード	無効
プライマリ通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	<input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>
各WAN回線設定ボタンを押下すると、このページで変更した内容は保存されません。	

■ WAN バックアップ

- ・無効 : 回線冗長化機能を使用しません。
- ・コールド・スタンバイ : 回線冗長化機能(コールド・スタンバイ方式)を使用します。
回線障害検出時に WAN 側接続モードをセカンダリ接続モードへ切り替えます。
設定方法については「5-4.回線冗長化設定(コールド・スタンバイ)」(89 ページ)を参照して下さい。
- ・ホット・スタンバイ : 回線冗長化機能(ホット・スタンバイ方式)を使用します。
プライマリ接続とセカンダリ接続を同時に行い、回線障害検出時にゲートウェイをセカンダリ接続モードへ切り替えます。
設定方法については「5-5.回線冗長化設定(ホット・スタンバイ)」(92 ページ)を参照して下さい。

	回線冗長化機能を使用する場合、WAN 回線監視設定は必須です。
	有線 WAN 設定で IPv6 プロトコル有効時は、回線冗長化機能は使用できません。

■ プライマリ接続モード(選択必須)

プライマリ接続モードで使用する WAN 側接続モードを選択して下さい。

回線冗長化機能を使用しない場合、こちらだけ設定して下さい。

■ セカンダリ接続モード

回線冗長化機能を使用する場合、セカンダリ接続モードで使用する WAN 側接続モードを選択して下さい。

	有線 WAN 設定を「Bridge」に設定した場合、有線 WAN を選択する必要はありません。
---	---

■ プライマリ通信確認間隔(コールド・スタンバイ設定時のみ)

セカンダリ接続で動作中にプライマリ接続の通信を確認する場合、確認間隔の時間を入力して下さい。

セカンダリ接続へ切り替え後、ここで設定した時間経過すると一度プライマリ接続へ切り替えます。

プライマリ接続へ切り替え後に WAN 回線監視を行い、成功すればプライマリ接続のまま動作します。

失敗した場合は、もう一度セカンダリ接続に切り替えます。

「0時0分0秒」(初期値)の場合は、プライマリ接続の通信確認を行いません。

■ 有線 WAN、内蔵モバイル、USB モバイル(ボタン)

各 WAN 側接続モードを設定します。

設定方法については、それぞれ以下を参照して下さい。

- 5-2-1.内蔵モバイル設定(72 ページ)
- 5-2-2.USB モバイル設定(74 ページ)
- 5-2-3.有線 WAN 設定:DHCP(76 ページ)
- 5-2-4.有線 WAN 設定:固定 IP(77 ページ)
- 5-2-5.有線 WAN 設定:PPPoE(78 ページ)
- 5-2-6.有線 WAN 設定:transix(DS-Lite)(79 ページ)
- 5-2-7.有線 WAN 設定:IPoE IPv6(80 ページ)
- 5-2-8.有線 WAN 設定:Bridge(81 ページ)

<次ページへ進んで下さい>

WAN回線監視	
回線監視:	行わない
初期発行間隔:	未使用
発行間隔:	1分
連続失敗検出回数:	1回 (1~60回)
<input type="checkbox"/> 回線監視通信の送信元にLAN側IPアドレスを使用する	
宛先1:	<input type="text"/>
宛先2:	<input type="text"/>
宛先3:	<input type="text"/>

■回線監視

- ・行わない : 回線監視を行いません。
- ・PING による監視 : PING 応答があった場合に回線接続状態と判断します。
- ・HTTP による監視 : 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。

	回線冗長化機能を使用する場合、WAN 回線監視設定は必須です。
	有線 WAN 設定で IPv6 プロトコル有効時は、回線監視機能は使用しないで下さい。

■初期発行間隔

回線接続後に回線監視を開始するまでの時間を設定します。
 10/20/30/40/50 秒、1 分/1 分 30 秒/2 分/3 分/5 分
 「未使用」を選択した場合、発行間隔の設定で開始します。

■発行間隔

監視間隔を設定します。
 PING による監視: (10/20/30/40/50 秒、1/5/10/15/30/45/60 分)
 HTTP による監視: (1/5/10/15/30/45/60 分)

■連続失敗検出回数

ここで設定した回数、連続して監視に失敗すると、回線切断状態と判断します。

■回線監視通信の送信元に LAN 側 IP アドレスを使用する(チェックボックス)

回線監視通信を VPN 接続先拠点と行う場合チェックを入れて下さい。

■宛先 1~3

監視先を FQDN(ドメイン名)もしくは IP アドレスで設定して下さい。

	設定した全ての宛先への監視に失敗した場合、回線切断状態と判断します。 いずれかの宛先への監視に成功した場合は、回線接続状態と判断します。
	回線冗長化未使用時は、「監視失敗」の連続回数が連続失敗検出回数に達すると、回線の再接続を行います。(内蔵モバイル、USB モバイル、有線 WAN(PPPoE)接続時) 有線 WAN(DHCP、固定 IP)接続の場合、回線監視に失敗してもリカバリ処理は行われません。
	回線冗長化使用時は、「監視失敗」の連続回数が連続失敗検出回数に達すると、セカンダリー接続への切り替えを行います。 コールド・スタンバイでセカンダリー接続後に回線監視に失敗した場合、MR-GM5A は再起動します。 ホット・スタンバイでセカンダリー接続後に回線監視に失敗した場合、プライマリー接続へ切り替えます。
	FQDN の名前解決はできても PING や HTTP リクエストに応答しない宛先を登録した場合、応答無しと判断しますのでご注意ください。
	PING による監視で URL を設定する場合は、「https://」「http://」は入れずに設定して下さい。
	IPv6 アドレスは設定できません。

〈次ページへ進んで下さい〉

NAPTセッション設定	
UDPセッション時間(単方向)	30 (0~3600秒)
UDPセッション時間(双方向)	180 (0~3600秒)
IP変換セッション数	15420 (2000~20000)
設定保存	

■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 30 秒、双方向 180 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(15420)のままご利用下さい。

■設定保存(ボタン)

本画面の設定が終わりましたら押して下さい。
以下の画面が表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。
引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

設定は正常に保存されました。

変更を動作に反映させるためには、本機を再起動する必要があります。
今すぐ再起動しますか？

今すぐ再起動

後で再起動

5-3.IPsec 設定

VPN(IPsec)接続設定について説明します。

	WAN 側接続モードで IPV6 使用時は、VPN(IPsec) 接続は使用できません。
---	--

設定メニューの「ネットワーク」→「VPN」→「IPsec 設定」をクリックして下さい。

「IPsec設定」画面が開きます。



No.	選択	状態	接続名
1	<input type="radio"/>	-	-
2	<input type="radio"/>	-	-

5-3-1.VPN 設定画面



No.	選択	状態	接続名	識別ID	接続先アドレス	ステータス
1	<input checked="" type="radio"/>	有効	IPsec-VPN	MR-GM5	**** * * * *	接続
2	<input type="radio"/>	-	-	-	-	-
3	<input type="radio"/>	-	-	-	-	-

■IPsec(ラジオボタン)

IPsec VPN 機能の有効/無効を切り替えます。

■設定保存(ボタン)

IPsec VPN 機能の有効/無効を切り替えた際に動作に反映させます。

■VPN 接続情報

登録されている VPN 接続情報と接続状態を表示します。

接続情報は 3 つまで登録できます。

■選択(ラジオボタン)

「編集」「削除」を行う VPN 接続情報を選択します。

■選択した登録を編集(ボタン)

選択した VPN 接続情報を編集します。

■選択した登録を削除(ボタン)

選択した接続情報を削除します。

5-3-2VPN 接続先の設定画面

IPsec 設定画面で接続先情報を選択し、[選択した登録を編集]ボタンをクリックすると「IPsec VPN 接続先の設定」画面が開きます。

IPsec VPN接続先の設定	
このページではIPsec VPN接続先の設定を行えます。	
接続先 No. 1	
状態	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
接続名	<input type="text" value="IPsec-VPN"/>
ローカル側	
識別ID種別	<input type="text" value="FQDN"/> ▼
識別ID(FQDN)	<input type="text" value="MR-GM5"/>
通信対象アドレス	<input type="text" value="192.168.0.1/24"/>
リモート側	
識別ID種別	<input type="text" value="FQDN"/> ▼
識別ID(FQDN)	<input type="text" value="example"/>
接続先アドレス	<input type="text" value="*** ***/***/**"/>
通信対象アドレス1	<input type="text" value="192.168.100.0/24"/>
通信対象アドレス2	<input type="text"/>
通信対象アドレス3	<input type="text"/>

状態(ラジオボタン)	本画面で設定する VPN 接続情報を有効にする場合、有効を選択して下さい。
接続名	接続名称を任意で設定して下さい。 半角英数字 30 文字まで入力可能です。
ローカル側	
識別 ID 種別	接続先 VPN 機器の識別方法に合わせて選択して下さい。 IP アドレス: IP アドレスを通知します。 FQDN: FQDN 形式で通知します。 ユーザーFQDN: ユーザーFQDN 形式で通知します。 テキスト: テキスト形式で通知します。
識別 ID	識別 ID 種別に合わせて入力して下さい。 IP アドレス: 本製品の WAN 側 IP アドレスを入力して下さい。 FQDN/ユーザーFQDN/テキスト: 識別名を入力して下さい。
通信対象アドレス	ローカル側のネットワークアドレス(もしくは IP アドレス)を入力して下さい。
リモート側	
識別 ID 種別	接続先 VPN 機器の識別方法に合わせて選択して下さい。 IP アドレス: IP アドレスで通知を受けます。 FQDN: FQDN 形式で通知を受けます。 ユーザーFQDN: ユーザーFQDN 形式で通知を受けます。 テキスト: テキスト形式で通知を受けます。
識別 ID	識別 ID 種別に合わせて入力して下さい。 IP アドレス: 接続先 VPN 機器の WAN 側 IP アドレスを入力して下さい。 FQDN/ユーザーFQDN/テキスト: 接続先 VPN 機器の識別名を入力して下さい。
接続先アドレス	接続先 VPN 機器の WAN 側 IP アドレスを入力して下さい。
通信対象 1~3 IP アドレス	接続先のネットワークアドレス(もしくは IP アドレス)を入力して下さい。 「0.0.0.0/0」を設定すると、VPN 接続がデフォルトゲートウェイに設定されます。

<次ページへ進んで下さい>

セキュリティ設定	
鍵交換モード	アグレッシブ▼
通信圧縮	使用しない▼
ローカル側 事前共有鍵	password
リモート側 事前共有鍵	password
IKE バージョン	自動▼
IKE 暗号アルゴリズム	DES▼
IKE 認証アルゴリズム	MD5▼
DH グループ	DH2▼
IKE ライフタイム	28800 (300 - 86400秒)
IKE キープアライブ	<input type="radio"/> 有効(DPD) <input checked="" type="radio"/> 無効
DPD	発行間隔 5 (1 - 600秒) タイムアウト 60 (1 - 3600秒)
ESP 暗号アルゴリズム	AES 128▼
ESP 認証アルゴリズム	SHA1▼
PFS グループ	DH2▼
ESP ライフタイム	28800 (300 - 28800秒)
<input type="button" value="設定"/> <input type="button" value="戻る"/>	

セキュリティ設定	
鍵交換モード	鍵交換モードを選択して下さい。 アグレッシブ:アグレッシブモードで鍵交換します。 メイン:メインモードで鍵交換します。
通信圧縮	データ圧縮を使用する場合、「使用する」を選択して下さい。
ローカル側 事前共有鍵	接続先 VPN 機器の事前共有鍵を設定します。
リモート側 事前共有鍵	リモートから送信される事前共有鍵を設定します。
IKE バージョン	使用する IKE のバージョンを指定して下さい。 自動の場合、IKEv2、IKEv1を自動判別します。
IKE 暗号アルゴリズム	IKE の暗号化方式を選択して下さい。 (DES/3DES/BLOWFISH/AES 128/AES 192/AES 256)
IKE 認証アルゴリズム	IKE の認証方式を選択して下さい。 (MD5/SHA1/SHA256)
DH グループ	DH(Diffie-Hellman)のパラメーターを選択して下さい。 (未指定/DH1/DH2/DH5)
IKE ライフタイム	ISAKMP SA の生存時間を入力して下さい。
IKE キープアライブ	DPD (Dead Peer Detection)メッセージによる IPsec トンネルの通信断を検出する場合、有効を選択して下さい。
DPD	DPD メッセージの発行間隔、タイムアウト時間を入力して下さい。 DPD 設定は、レスポнда側と一致する値を設定して下さい。
ESP 暗号アルゴリズム	ESP の暗号化方式を選択して下さい。 (DES/3DES/AES 128/AES 192/AES 256)
ESP 認証アルゴリズム	ESP の認証方式を選択して下さい。 (HMAC-MD5/HMAC-SHA1/HMAC-SHA256)
PFS グループ	PFS(Perfect Forward Security)のパラメーターを選択して下さい。 (未指定/DH1/DH2/DH5)
ESP ライフタイム	IPsec SA の生存時間を入力して下さい。

<次ページへ進んで下さい>

全ての設定が終わりましたら、[設定保存]ボタンをクリックして下さい。
以下の画面が表示されますので、すぐに設定を反映させる場合は[今すぐ再起動]ボタンを、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。

設定は正常に保存されました。

変更を動作に反映させるためには、本機を再起動する必要があります。
今すぐ再起動しますか？

今すぐ再起動

後で再起動

再起動が完了すると、VPN 設定画面に設定した VPN 接続情報が追加されます。
接続が完了すると、ステータスが「接続」と表示されます。

No.	選択	状態	接続名	識別ID	接続先アドレス	ステータス
1	<input checked="" type="radio"/>	有効	IPsec-VPN	MR-GM5	*** **	接続
2	<input type="radio"/>	-	-	-	-	-
3	<input type="radio"/>	-	-	-	-	-

選択した登録を編集 選択した登録を削除

5-4.回線冗長化設定（コールド・スタンバイ）

回線冗長化（コールド・スタンバイ方式）の設定について説明します。

プライマリー接続が不通状態となった場合に、自動的にセカンダリー接続に切り替えます。

セカンダリー接続に切り替え後、定期的にプライマリー接続の回線状態を確認する事も可能です。

	有線WAN設定でIPv6有効時は、回線冗長化機能は使用できません。
---	-----------------------------------

5-4-1.回線冗長化機能（コールド・スタンバイ方式）の仕様について

■プライマリー接続、セカンダリー接続で組み合わせ可能な接続モードは以下の通りです。

プライマリー接続(メイン)	セカンダリー接続(バックアップ)
内蔵モバイル	USB モバイル
内蔵モバイル	有線 WAN(DHCP/IP 固定/PPPoE)
USB モバイル	内蔵モバイル
USB モバイル	有線 WAN(DHCP/IP 固定/PPPoE)
有線 WAN(DHCP/IP 固定/PPPoE)	内蔵モバイル
有線 WAN(DHCP/IP 固定/PPPoE)	USB モバイル

■コールド・スタンバイ方式は、プライマリー接続モードとセカンダリー接続モードの切り替えによる排他使用です。

■回線冗長化機能で有線 WAN を組み合わせる場合、ETH1 ポートは有線 WAN ポート固定動作となります。
ETH1 ポートは有線 LAN ポートとして使用できなくなります。

■プライマリー接続からセカンダリー接続への切り替え契機は以下の通りです。

- ・回線監視失敗時
- ・回線接続失敗時(内蔵モバイル、USB モバイル、PPPoE クライアント使用時)
- ・USB モバイルデバイス未検出時(USB デバイス検出待ち時間設定による)
- ・DHCP クライアントによる IP アドレス取得失敗時
- ・ステータス画面「WAN 回線運用」の「回線切替」ボタンをクリックした時

■セカンダリー接続からプライマリー接続への切り替え契機は以下の通りです。

- ・プライマリー通信確認間隔(時間)経過時
- ・ステータス画面「WAN 回線運用」の「回線切替」ボタンをクリックした時
- ・MR-GM5A の再起動時

■セカンダリー接続後、以下の契機で MR-GM5A が再起動します。

- ・回線監視失敗時
- ・回線接続失敗時(内蔵モバイル、USB モバイル、PPPoE クライアント使用時)
- ・USB モバイルデバイス未検出時(USB デバイス検出待ち時間設定による)
- ・DHCP クライアントによる IP アドレス取得失敗時

■セカンダリー接続に切り替え後にプライマリー接続の回線状態を確認する際は、セカンダリー接続が一度切断されますのでご注意ください。

5-4-2.WAN 設定(回線冗長化設定)

回線冗長化設定を行う前に

回線冗長化設定を行う前に、プライマリ接続、セカンダリ接続で使用するWAN側接続モードの設定を行って下さい。

各接続モードの設定については以下を参照して下さい。

「5-2-1.内蔵モバイル設定」(72 ページ)

「5-2-2.USB モバイル設定」(74 ページ)

「5-2-3.有線 WAN 設定:DHCP」(76 ページ)

「5-2-4.有線 WAN 設定:固定 IP」(77 ページ)

「5-2-5.有線 WAN 設定:PPPoE」(78 ページ)

「ネットワーク」から「WAN 設定」をクリックして下さい。

「WAN 設定」画面が表示されます。

ステータス + 無線LAN - ネットワーク LAN 設定 WAN 設定 + VPN + ファイアウォール + 付加機能 + マネージメント	WAN 設定 このページではWANインターフェースの設定が行えます。 WAN回線運用 WANバックアップ: 無効 プライマリ接続モード: 有線WAN セカンダリ接続モード: 有線WAN プライマリ通信確認間隔: 0 時 0 分 0 秒 (0秒~24時間) WAN回線設定: 有線WAN 内蔵モバイル USBモバイル <small>各WAN回線設定ボタンを押下すると、このページで変更</small>
--	---

WAN回線運用	
WANバックアップ	コールド・スタンバイ
プライマリ接続モード	有線WAN
セカンダリ接続モード	内蔵モバイル
プライマリ通信確認間隔	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定	有線WAN 内蔵モバイル USBモバイル <small>各WAN回線設定ボタンを押下すると、このページで変更した内容は保存されません。</small>

■WAN バックアップ

「コールド・スタンバイ」を選択して下さい。

■プライマリ接続モード

プライマリ接続モードで使用する WAN 側接続モードを選択して下さい。

■セカンダリ接続モード

セカンダリ接続モードで使用する WAN 側接続モードを選択して下さい。

■プライマリ通信確認間隔

セカンダリ接続で動作中にプライマリ接続の通信を確認する場合、確認間隔の時間を入力して下さい。

セカンダリ接続へ切り替え後、ここで設定した時間経過すると一度プライマリ接続へ切り替えます。

プライマリ接続へ切り替え後に WAN 回線監視を行い、成功すればプライマリ接続のまま動作します。

失敗した場合は、もう一度セカンダリ接続に切り替えます。

「0時0分0秒」(初期値)の場合は、プライマリ接続の通信確認を行わず、セカンダリ接続に切り替わった後は、MR-GM5A を再起動するまでセカンダリ接続のまま動作します。

<次ページへ進んで下さい>

WAN回線監視	
回線監視:	PINGによる監視 ▼
初期発行間隔:	未使用 ▼
発行間隔:	1分 ▼
連続失敗検出回数:	3 (1~60回)
宛先1:	example1.co.jp
宛先2:	example2.co.jp
宛先3:	example3.co.jp

■ 回線監視機能

「PINGによる監視」もしくは「HTTPによる監視」のいずれかを選択して下さい。
「PINGによる監視」は PING 応答があった場合に回線接続状態と判断します。
「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。

	回線冗長化機能を使用する場合、回線監視設定は必須です。
	本項目に誤った設定を行うと回線冗長化機能が正しく動作しませんのでご注意ください。
	回線監視機能の設定はプライマリー接続・セカンダリー接続共通となります。

■ 初期発行間隔

回線接続後に回線監視を開始するまでの時間を設定します。
10/20/30/40/50 秒、1 分/1 分 30 秒/2 分/3 分/5 分
「未使用」を選択した場合、発行間隔の設定で開始します。

■ 発行間隔

監視間隔を設定します。
PING による監視: (10/20/30/40/50 秒、1/5/10/15/30/45/60 分)
HTTP による監視: (1/5/10/15/30/45/60 分)

■ 連続失敗検出回数

ここで設定した回数、連続して監視に失敗すると、回線切断状態と判断します。

■ 宛先 1~3

監視先を FQDN(ドメイン名)もしくは IP アドレスで設定して下さい。

	設定した全ての宛先への監視に失敗した場合、回線切断状態と判断します。
	いずれかの宛先への監視に成功した場合は、回線接続状態と判断します。
	回線冗長化使用機能時は、「監視失敗」の連続回数が連続失敗検出回数に達すると、セカンダリー接続への切り替えを行います。
	コールド・スタンバイでセカンダリー接続後に回線監視に失敗した場合、MR-GM5A は再起動します。
FQDN の名前解決はできるが PING や HTTP リクエストに回答しない宛先を登録した場合、応答無しと判断しますのでご注意ください。	

UDPセッション時間(双方向):	180 (0~3600秒)
IP変換 セッション数:	15420 (2000~20000)
<div style="border: 1px solid red; padding: 2px; display: inline-block;">設定保存</div>	

■ 設定保存(ボタン)

本画面の設定が終わりましたら押して下さい。
以下の画面が表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。
引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

設定は正常に保存されました。

変更を動作に反映させるためには、本機を再起動する必要があります。
今すぐ再起動しますか？

5-5.回線冗長化設定（ホット・スタンバイ）

回線冗長化(ホット・スタンバイ方式)の設定について説明します。

プライマリー接続とセカンダリー接続を同時接続し、プライマリー接続が不通状態となった場合に、自動的にゲートウェイをセカンダリー接続に切り替える機能です。

	有線WAN設定でIPv6有効時は、回線冗長化機能は使用できません。
---	-----------------------------------

5-5-1.回線冗長化機能(ホット・スタンバイ方式)の仕様について

■プライマリー接続、セカンダリー接続で組み合わせ可能な接続モードは以下の通りです。

プライマリー接続(メイン)	セカンダリー接続(バックアップ)
内蔵モバイル	USB モバイル
内蔵モバイル	有線 WAN(DHCP/IP 固定/PPPoE)
USB モバイル	内蔵モバイル
USB モバイル	有線 WAN(DHCP/IP 固定/PPPoE)
有線 WAN(DHCP/IP 固定/PPPoE)	内蔵モバイル
有線 WAN(DHCP/IP 固定/PPPoE)	USB モバイル

■回線冗長化機能で有線 WAN を組み合わせる場合、ETH1 ポートは有線 WAN ポート固定動作となります。ETH1 ポートは有線 LAN ポートとして使用できなくなります。

■プライマリー接続からセカンダリー接続への切り替え契機は以下の通りです。

- ・回線監視失敗時
- ・回線接続失敗時(内蔵モバイル、USB モバイル、PPPoE クライアント使用時)
- ・USB モバイルデバイス未検出時(USB デバイス検出待ち時間設定による)
- ・DHCP クライアントによる IP アドレス取得失敗時
- ・ステータス画面「WAN 回線運用」の「回線切替」ボタンをクリックした時

■セカンダリー接続からプライマリー接続への切り替え契機は以下の通りです。

- ・回線監視失敗時
- ・回線接続失敗時(内蔵モバイル、USB モバイル、PPPoE クライアント使用時)
- ・USB モバイルデバイス未検出時(USB デバイス検出待ち時間設定による)
- ・DHCP クライアントによる IP アドレス取得失敗時
- ・プライマリー通信確認間隔(時間)経過時
- ・ステータス画面「WAN 回線運用」の「回線切替」ボタンをクリックした時
- ・MR-GM5A の再起動時

5-5-2.WAN 設定(回線冗長化設定)

回線冗長化設定を行う前に

回線冗長化設定を行う前に、プライマリ接続、セカンダリ接続で使用するWAN側接続モードの設定を行って下さい。

各接続モードの設定については以下を参照して下さい。

- 「5-2-1.内蔵モバイル設定」(72 ページ)
- 「5-2-2.USB モバイル設定」(74 ページ)
- 「5-2-3.有線 WAN 設定:DHCP」(76 ページ)
- 「5-2-4.有線 WAN 設定:固定 IP」(77 ページ)
- 「5-2-5.有線 WAN 設定:PPPoE」(78 ページ)

「ネットワーク」から「WAN 設定」をクリックして下さい。

「WAN 設定」画面が表示されます。

ステータス + 無線LAN - ネットワーク LAN 設定 WAN 設定 + VPN + ファイアウォール + 付加機能 + マネージメント	<h3>WAN 設定</h3> <p>このページではWANインターフェースの設定が行えます。</p> <table border="1"> <thead> <tr> <th colspan="2">WAN回線運用</th> </tr> </thead> <tbody> <tr> <td>WANバックアップ:</td> <td>無効 ▼</td> </tr> <tr> <td>プライマリ接続モード:</td> <td>有線WAN ▼</td> </tr> <tr> <td>セカンダリ接続モード:</td> <td>有線WAN ▼</td> </tr> <tr> <td>プライマリ通信確認間隔:</td> <td>0 時 0 分 0 秒 (0秒~24時間)</td> </tr> <tr> <td>WAN回線設定:</td> <td> <input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/> </td> </tr> </tbody> </table> <p style="color: red; font-size: small;">各WAN回線設定ボタンを押下すると、このページで変更</p>	WAN回線運用		WANバックアップ:	無効 ▼	プライマリ接続モード:	有線WAN ▼	セカンダリ接続モード:	有線WAN ▼	プライマリ通信確認間隔:	0 時 0 分 0 秒 (0秒~24時間)	WAN回線設定:	<input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>
WAN回線運用													
WANバックアップ:	無効 ▼												
プライマリ接続モード:	有線WAN ▼												
セカンダリ接続モード:	有線WAN ▼												
プライマリ通信確認間隔:	0 時 0 分 0 秒 (0秒~24時間)												
WAN回線設定:	<input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>												

WAN回線運用	
WANバックアップ:	ホット・スタンバイ ▼
プライマリ接続モード:	有線WAN ▼
セカンダリ接続モード:	内蔵モバイル ▼
プライマリ通信確認間隔:	0 時 0 分 0 秒 (0秒~24時間)
WAN回線設定:	<input type="button" value="有線WAN"/> <input type="button" value="内蔵モバイル"/> <input type="button" value="USBモバイル"/>

各WAN回線設定ボタンを押下すると、このページで変更した内容は保存されません。

■WAN バックアップ

「ホット・スタンバイ」を選択して下さい。

■プライマリ接続モード

プライマリ接続モードで使用する WAN 側接続モードを選択して下さい。

■セカンダリ接続モード

セカンダリ接続モードで使用する WAN 側接続モードを選択して下さい。

■プライマリ通信確認間隔

セカンダリ接続で動作中にプライマリ接続の通信を確認する場合、確認間隔の時間を入力して下さい。

セカンダリ接続へ切り替え後、ここで設定した時間経過すると一度プライマリ接続へ切り替えます。

プライマリ接続へ切り替え後に WAN 回線監視を行い、成功すればプライマリ接続のまま動作します。

失敗した場合は、もう一度セカンダリ接続に切り替えます。

「0 時 0 分 0 秒」(初期値)の場合は、プライマリ接続の通信確認を行わず、セカンダリ接続に切り替わった後は、MR-GM5A を再起動するまでセカンダリ接続のまま動作します。

<次ページへ進んで下さい>

WAN回線監視	
回線監視:	PINGによる監視 ▼
初期発行間隔:	未使用 ▼
発行間隔:	1分 ▼
連続失敗検出回数:	3 (1~60回)
宛先1:	example1.co.jp
宛先2:	example2.co.jp
宛先3:	example3.co.jp

■ 回線監視機能

「PINGによる監視」もしくは「HTTPによる監視」のいずれかを選択して下さい。
「PINGによる監視」は PING 応答があった場合に回線接続状態と判断します。
「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。

	回線冗長化機能を使用する場合、回線監視設定は必須です。
	本項目に誤った設定を行うと回線冗長化機能が正しく動作しませんのでご注意ください。
	回線監視機能の設定はプライマリー接続・セカンダリー接続共通となります。

■ 初期発行間隔

回線接続後に回線監視を開始するまでの時間を設定します。
10/20/30/40/50 秒、1 分/1 分 30 秒/2 分/3 分/5 分
「未使用」を選択した場合、発行間隔の設定で開始します。

■ 発行間隔

監視間隔を設定します。
PINGによる監視: (10/20/30/40/50 秒、1/5/10/15/30/45/60 分)
HTTPによる監視: (1/5/10/15/30/45/60 分)

■ 連続失敗検出回数

ここで設定した回数、連続して監視に失敗すると、回線切断状態と判断します。

■ 宛先 1~3

監視先を FQDN(ドメイン名)もしくは IP アドレスで設定して下さい。

	設定した全ての宛先への監視に失敗した場合、回線切断状態と判断します。
	いずれかの宛先への監視に成功した場合は、回線接続状態と判断します。
	回線冗長化使用機能時は、「監視失敗」の連続回数が連続失敗検出回数に達すると、セカンダリー接続への切り替えを行います。
	ホット・スタンバイでセカンダリー接続後に回線監視に失敗した場合、プライマリー接続へ切り替えます。
FQDN の名前解決はできるが PING や HTTP リクエストに回答しない宛先を登録した場合、応答無しと判断しますのでご注意ください。	

UDPセッション時間(双方向):	180 (0~3600秒)
IP変換セッション数:	15420 (2000~20000)
<div style="border: 2px solid red; padding: 2px; display: inline-block;">設定保存</div>	

■ 設定保存(ボタン)

本画面の設定が終わりましたら押して下さい。
以下の画面が表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。
引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

設定は正常に保存されました。

変更を動作に反映させるためには、本機を再起動する必要があります。
今すぐ再起動しますか？

6.ファイアウォール

IP フィルター設定、IPv6 フィルター、MAC フィルター設定、ドメインフィルター設定、ポートフォワーディング設定、アクセス制御設定、DMZ 設定について説明します。

6-1.IP フィルター 設定

IPv4アドレス、プロトコルを基に通信を透過・遮断する、IP フィルター設定について説明します。

	最大 128 エントリまで登録可能です。
---	----------------------

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

「IP フィルター 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク - ファイアウォール IP フィルター 設定 IPv6 フィルター 設定 MAC フィルター 設定	<h3 style="color: #800080;">IP フィルター 設定</h3> <p>このページではLANの送受信パケットに対するIPフィルター登録、編集、削除、</p> <table border="1" style="width: 100%;"><tr><td>LANからWAN宛通信の基本動作:</td><td><input type="radio"/> 遮断 <input checked="" type="radio"/> 透過</td></tr><tr><td>WANからLAN宛通信の基本動作:</td><td><input checked="" type="radio"/> 遮断 <input type="radio"/> 透過</td></tr></table> <p style="text-align: center;"><input type="button" value="設定保存"/> <input type="button" value="設定反映"/></p>	LANからWAN宛通信の基本動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過	WANからLAN宛通信の基本動作:	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
LANからWAN宛通信の基本動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過				
WANからLAN宛通信の基本動作:	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過				

IP フィルター 設定

このページではLANの送受信パケットに対するIPフィルター登録、編集、削除、および表示が行えます。

LANからWAN宛通信の基本動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過
WANからLAN宛通信の基本動作:	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過

■LAN から WAN 宛通信の基本動作(ラジオボタン)

LAN から WAN 宛へ送信される通信の基本動作を設定します。

■WAN から LAN 宛通信の基本動作(ラジオボタン)

WAN から LAN 宛へ送信される通信の基本動作を設定します。

■設定保存(ボタン)

IP フィルターの基本動作を変更した場合に押して下さい。

■設定反映(ボタン)

IP フィルターの設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

<次ページへ進んで下さい>

方向:	LAN送信 ▼
プロトコル:	Any ▼
送信元 IPアドレス/マスク:	<input type="text"/> / <input type="text"/>
送信元 ポート:	<input type="text"/> - <input type="text"/>
宛先 IPアドレス/マスク:	<input type="text"/> / <input type="text"/>
宛先 ポート:	<input type="text"/> - <input type="text"/>
動作:	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
<input type="button" value="追加"/>	

■方向

LAN 送信: LAN ポートから送信される通信を対象とします。

LAN受信: LANポートが受信する通信を対象とします。

■プロトコル

対象とするプロトコルを選択して下さい。

- Any** : 以下の全てのプロトコルを対象とします。
- TCP** : TCP プロトコルを対象とします。
- UDP** : UDP プロトコルを対象とします。
- ICMP** : ICMP (PING) 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。

■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。

■送信元ポート

プロトコルで「TCP」「UDP」「TCP+UDP」を選択した場合のみ入力可能です。

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 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。

■宛先ポート

プロトコルで「TCP」「UDP」「TCP+UDP」を選択した場合のみ入力可能です。

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。

■動作(ラジオボタン)

登録するフィルターの動作を選択して下さい。

■追加(ボタン)

入力した内容が登録リストに追加されます。

	最大 128 エントリまで登録可能です。
	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。

<次ページへ進んで下さい>

IPフィルター 登録リスト							
選択	方向	プロトコル	送信元 IPアドレス	送信元ポート	宛先 IPアドレス	宛先ポート	動作
<input type="checkbox"/>	LAN送信	TCP	10.0.0.1/28		Any	80	透過
<input type="checkbox"/>	LAN送信	TCP	Any		Any	80	遮断

■ **選択した登録を編集(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。

■ **選択した登録上げる(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。

■ **選択した登録を下げる(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。

■ **選択した登録を削除(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。

6-2.IPv6 フィルター 設定

IPv6 アドレス、プロトコルを基に通信を透過・遮断する、IPv6 フィルター設定について説明します。

確認

最大 128 エントリまで登録可能です。

設定メニューの「ファイアウォール」より「IPv6 フィルター 設定」をクリックして下さい。

「IPv6 フィルター 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク - ファイアウォール IP フィルター 設定 IPv6 フィルター 設定 MAC フィルター 設定	IPv6 フィルター 設定 このページではLANの送受信パケットに対するIPフィルター登録、編集、削除、 LANからWAN宛通信の基本動作: <input type="radio"/> 遮断 <input checked="" type="radio"/> 透過 WANからLAN宛通信の基本動作: <input checked="" type="radio"/> 遮断 <input type="radio"/> 透過 設定保存 設定反映
--	---

IPv6 フィルター 設定

このページではLANの送受信パケットに対するIPフィルター登録、編集、削除、および表示が行えます。

LANからWAN宛通信の基本動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過
WANからLAN宛通信の基本動作:	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
設定保存	設定反映

■LAN から WAN 宛通信の基本動作(ラジオボタン)

LAN から WAN 宛へ送信される通信の基本動作を設定します。

■WAN から LAN 宛通信の基本動作(ラジオボタン)

WAN から LAN 宛へ送信される通信の基本動作を設定します。

■設定保存(ボタン)

IP フィルターの基本動作を変更した場合に押して下さい。

■設定反映(ボタン)

IP フィルターの設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

<次ページへ進んで下さい>

方向:	LAN送信 ▾
プロトコル:	Any ▾
送信元 IPアドレス/マスク:	<input type="text"/> / <input type="text"/>
送信元 ポート:	<input type="text"/> - <input type="text"/>
宛先 IPアドレス/マスク:	<input type="text"/> / <input type="text"/>
宛先 ポート:	<input type="text"/> - <input type="text"/>
動作:	<input checked="" type="radio"/> 遮断 <input type="radio"/> 透過
<input type="button" value="追加"/>	

■方向

LAN 送信: LAN ポートから送信される通信を対象とします。

LAN受信: LANポートが受信する通信を対象とします。

■プロトコル

対象とするプロトコルを選択して下さい。

- Any** : 以下の全てのプロトコルを対象とします。
- TCP** : TCP プロトコルを対象とします。
- UDP** : UDP プロトコルを対象とします。
- ICMPv6** : ICMPv6(PING)プロトコルを対象とします。

■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。

■送信元ポート

プロトコルで「TCP」「UDP」「TCP+UDP」を選択した場合のみ入力可能です。

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 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。

■宛先ポート

プロトコルで「TCP」「UDP」「TCP+UDP」を選択した場合のみ入力可能です。

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。

■動作(ラジオボタン)

登録するフィルターの動作を選択して下さい。

■追加(ボタン)

入力した内容が登録リストに追加されます。

	最大 128 エントリまで登録可能です。
	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。

<次ページへ進んで下さい>

IPv6フィルター 登録リスト							
選択	方向	プロトコル	送信元 IPアドレス	送信元ポート	宛先 IPアドレス	宛先ポート	動作
<input type="checkbox"/>	LAN送信	Any	Any	Any	2001:db8::/128	Any	透過
<input type="checkbox"/>	LAN送信	Any	Any	Any	Any	Any	遮断

■ **選択した登録を編集(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。

■ **選択した登録上げる(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。

■ **選択した登録を下げる(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。

■ **選択した登録を削除(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。

6-3.MAC フィルター 設定

MAC(物理)アドレスを基に通信を透過・遮断する、MAC フィルター設定について説明します。

	MAC フィルタリング機能は、LAN→MR-GM5A、LAN→インターネット方向の通信に適用されます。
	本設定で遮断登録した MAC アドレスからは設定画面にアクセスできなくなります。
	最大 128 エントリまで登録可能です。

設定メニューの「ファイアウォール」より「MAC フィルター 設定」をクリックして下さい。

「MAC フィルター 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク - ファイアウォール IP フィルター 設定 IPv6 フィルター 設定 MAC フィルター 設定 ドメインフィルタ 設定 ポートフォワーディング 設定	MAC フィルター 設定 このページではLANの送受信パケットに対するMACアドレスフィルタ登録、編集、削除、
	LANからWAN宛通信の基本動作: <input type="radio"/> 遮断 <input checked="" type="radio"/> 透過
	<input type="button" value="設定保存"/> <input type="button" value="設定反映"/>
	送信元 MACアドレス: <input type="text"/> 動作: <input checked="" type="radio"/> 遮断 <input type="radio"/> 透過

MAC フィルター 設定

このページではLANの送受信パケットに対するMACアドレスフィルタ登録、編集、削除、および表示が行えます。

LANからWAN宛通信の基本動作: 遮断 透過

■LAN から WAN 宛通信の基本動作(ラジオボタン)

MACフィルターの基本動作を設定します。

遮断: 透過で登録した MAC アドレス以外を遮断します。

透過: 遮断で登録した MAC アドレス以外を透過します。

■設定保存(ボタン)

MAC フィルターの基本動作を変更した場合に押して下さい。

■設定反映(ボタン)

MAC フィルターの設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

送信元 MACアドレス:	<input type="text"/>
動作:	<input type="radio"/> 遮断 <input type="radio"/> 透過
<input type="button" value="追加"/>	

■送信元 MAC アドレス

送信元の MAC アドレスを入力して下さい。

■動作(ラジオボタン)

登録するフィルターの動作を選択して下さい。

<次ページへ進んで下さい>

■追加(ボタン)

入力した内容が登録リストに追加されます。

	最大 128 エントリまで登録可能です。
---	----------------------

MACフィルター 登録リスト		
選択	送信元 MACアドレス	動作
<input type="checkbox"/>	001038111111	遮断

選択した登録を編集 選択した登録を上げる 選択した登録を下げる 選択した登録を削除 全て削除

■選択した登録を編集(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。

■選択した登録上げる(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。

■選択した登録を下げる(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。

■選択した登録を削除(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。

6-4.ドメインフィルター 設定

特定のドメイン名への通信を遮断する、ドメインフィルター 設定について説明します。

確認	ドメインフィルター機能は、LAN→WAN 方向の通信に適用されます。
	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。
	DNS 名前解決で得られた IP アドレスがドメインフィルターの対象となります。
	ドメインフィルター機能を使用する場合、接続する端末の DNS サーバーとして MR-GM5A の LAN ポート IP アドレスを指定する必要があります。
	1 つの IP アドレスに複数のドメイン名が設定されている場合、意図した動作にならない場合があります。
最大 128 エントリまで登録可能です。	

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

「ドメインフィルター 設定」画面が開きます。

ステータス
+ 無線LAN
+ ネットワーク
- ファイアウォール
IP フィルター 設定
IPv6 フィルター 設定
MAC フィルター 設定
ドメインフィルター 設定
ポートフォワーディング 設定

ドメインフィルター 設定
ドメイン名/プロトコル/ポート番号の組み合わせに一致した通信を遮断します。

ドメインフィルター機能: 有効 無効

設定保存 設定反映

ドメイン名:

プロトコル: Any ▼

ドメインフィルター 設定
ドメイン名/プロトコル/ポート番号の組み合わせに一致した通信を遮断します。

ドメインフィルター機能: 有効 無効

設定保存 設定反映

ドメイン名:

プロトコル: Any ▼

宛先ポート: -

コメント:

追加

■ドメインフィルター機能(ラジオボタン)

ドメインフィルター機能の有効/無効を切り替えます。

■設定保存(ボタン)

ドメインフィルターの有効/無効を変更した場合に押して下さい。

■設定反映(ボタン)

ドメインフィルターの設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■ドメイン名

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 : 以下の全てのプロトコルを対象とします。
- 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。
- TCP+UDP : TCP、UDP プロトコル両方を対象とします。

<次ページへ進んで下さい>

■宛先ポート

プロトコルで「TCP」「UDP」「TCP+UDP」を選択した場合のみ入力可能です。

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。

■追加(ボタン)

入力した内容が登録リストに追加されます。

	最大 128 エントリまで登録可能です。
---	----------------------

ドメインフィルター 登録リスト				
選択	ドメイン名	プロトコル	宛先ポート	コメント
<input type="checkbox"/>	example.com	TCP	443	example.com

選択した登録を編集 選択した登録を上げる 選択した登録を下げる 選択した登録を削除 全て削除

■選択した登録を編集(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。

■選択した登録上げる(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。

■選択した登録を下げる(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。

■選択した登録を削除(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。

6-5.ポートフォワーディング 設定

ポートフォワーディング 設定について説明します。

ポートフォワーディング機能を使用することにより、WAN 側 IP アドレス宛の通信を LAN 側へフォワード(転送)することができます。

	ポートフォワーディング設定には、「使用するプロトコル」、「使用するポート番号」の情報が必要です。
	ポートフォワーディング設定と DMZ 設定を同時に設定した場合、ポートフォワーディング設定が優先されます。
	本設定で ICMP プロトコルを登録した場合、ポートフォワーディング設定が優先され、アクセス制御設定の WAN 側からの PING に応答する設定は無効になります。
	本設定で設定するポート番号と設定画面のアクセスポート番号 (GUI ポート番号) が重複した場合、ポートフォワーディング設定が優先され、WAN 側からの設定画面へのアクセスは無効になります。 設定画面へのアクセスポート番号 (GUI ポート番号) の変更方法については「8-7.ログイン 設定」(135 ページ)を参照して下さい。
	インターネットからポートフォワーディング機能により LAN 側の端末へアクセスする場合、プロバイダから付与される IP アドレスが「グローバル IP アドレス」である必要があります。 付与される IP アドレスが「プライベート IP アドレス」の場合は、インターネットからアクセスする事はできません。
最大 64 エントリまで登録可能です。	

設定メニューの「ファイアウォール」より「ポートフォワーディング 設定」をクリックして下さい。

「ポートフォワーディング 設定」画面が開きます。



ポートフォワーディング 設定

このページではWAN側から受信した通信を特定のLAN側装置に転送する設定の登録、編集、削除、



■ポートフォワーディング(ラジオボタン)

ポートフォワーディング機能の有効/無効を切り替えます。

■設定保存(ボタン)

ポートフォワーディング機能の有効/無効を変更した場合に押して下さい。

■設定反映(ボタン)

ポートフォワーディングの設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

<次ページへ進んで下さい>

WAN インターフェース:	Any ▼
プロトコル:	TCP ▼
受信ポート:	<input type="text"/> - <input type="text"/>
変換先アドレス:	<input type="text"/>
変換先ポート:	<input type="text"/>
コメント:	<input type="text"/>
<input type="button" value="追加"/>	

■インターフェース

ポートフォワーディングを行う WAN 側インターフェースを指定して下さい。

Any : 全ての WAN 側インターフェースを対象とします。

有線 WAN : 有線 WAN 接続を対象とします。

内蔵モバイル : 内蔵モバイル接続を対象とします。

USB モバイル : USB モバイル接続を対象とします。

	有効にしている WAN 側インターフェースが表示されます。
---	-------------------------------

■プロトコル

対象とするプロトコルを選択して下さい。

TCP : TCP プロトコルを対象とします。

UDP : UDP プロトコルを対象とします。

ICMP : ICMP (PING) 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。

■受信ポート

フォワード(転送)するポート番号を入力して下さい。

ポート番号を範囲で指定する事も可能です。

単独のポート番号を指定する場合は、左の入力欄にポート番号を入力して下さい。

■変換先 IP アドレス

フォワード(転送)する LAN 側端末の IP アドレスを入力して下さい。

	変換先の端末は IP アドレスを固定設定することを推奨します。
---	---------------------------------

■変換先ポート

LAN 側端末へ転送する際の転送先ポート番号を設定します。

宛先ポート番号を別のポート番号へ変換して転送することができます。

	受信ポートを範囲で指定した場合、範囲の受信ポート宛の通信が変換先ポートへ変換されます。
---	---

■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。

■追加(ボタン)

入力した内容が登録リストに登録されます。

	最大 64 エントリまで登録可能です。
---	---------------------

<次ページへ進んで下さい>

ポートフォワーディング 登録リスト						
選択	I/F	プロトコル	受信ポート	変換先アドレス	変換先ポート	コメント
<input type="checkbox"/>	Any	TCP	80	192.168.0.100	---	Webサーバー

■ **選択した登録を編集(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。

■ **選択した登録上げる(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。

■ **選択した登録を下げる(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。

■ **選択した登録を削除(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。

	<p>WAN 側からアクセスする場合、本製品の WAN 側の IP アドレスを指定して下さい。 WAN 側の IP アドレスは、ステータス画面(19 ページ)の「IP アドレス」欄で調べることができます。</p>
---	--

6-6. アクセス制御 設定

本機へのアクセス制御、PING 応答、アタック検出の設定を行います。



WAN 側から設定画面へのアクセスを許可する場合、必ずユーザー名、パスワードを変更して下さい。
ユーザー名、パスワードの変更方法については「8-7.ログイン 設定」(135 ページ)を参照して下さい。



ポートフォワーディング設定で設定するポート番号と設定画面のアクセスポート番号(GUIポート番号)が重複した場合、ポートフォワーディング設定が優先され、WAN 側からの設定画面へのアクセスは無効になります。設定画面へのアクセスポート番号(GUIポート番号)の変更方法については「8-7.ログイン 設定」(135 ページ)を参照して下さい。

ポートフォワーディング設定で設定画面へのアクセスポート番号と同じポート番号や ICMP を登録した場合、あるいは DMZ 設定を有効にした場合、それらの機能が優先され、アクセス制御設定は無効になります。

インターネット経由で設定画面へアクセスする場合や PING に応答させる場合は、WAN 側の IP アドレスがグローバル IP アドレスである必要があります。

最大 8 エントリまで登録可能です。

設定メニューの「ファイアウォール」より「アクセス制御 設定」をクリックして下さい。

「アクセス制御 設定」画面が開きます。

■ アクセス制御機能(ラジオボタン)

アクセス制御機能の有効/無効を切り替えます。

■ WAN 側からの PING アタック検出

1 秒間に許容する WAN 側からの PING アクセス数を設定します。

■ WAN 側からの HTTP アタック検出

30 秒間に許容する WAN 側からの最大 HTTP コネクション数を設定します。

30 秒間にここで設定した回数を超えて HTTP コネクションを受信した場合、その送信元 IP アドレスからのアクセスを 300 秒間拒否します。

■ 設定保存(ボタン)

アクセス制御機能の有効/無効、アタック検出の設定を変更した場合に押して下さい。

■ 設定反映(ボタン)

アクセス制御の設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

〈次ページへ進んで下さい〉

インターフェース:	LAN ▾
送信元 IP アドレス / マスク:	<input type="text"/> / <input type="text"/>
サービス名:	<input type="checkbox"/> Any <input type="checkbox"/> http <input type="checkbox"/> ping
動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過
<input type="button" value="追加"/>	

■ インターフェース

アクセス制御を行うインターフェースを指定して下さい。

LAN : LAN 側からのアクセス制御を設定します。

WAN : WAN 側からのアクセス制御を設定します。

■ 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指定する場合入力して下さい。

指定しない (Any) 場合は空欄にして下さい。

■ サービス名 (チェックボックス)

対象とするサービス名を指定して下さい。

Any : 本機への通信全てを対象とします。

http : http (設定画面へのログオン) を対象とします。

ping : ping (PING 応答) を対象とします。

■ 動作 (ラジオボタン)

登録するアクセス制御の動作を選択して下さい。

■ 追加 (ボタン)

入力した内容が登録リストに登録されます。

	最大 8 エントリまで登録可能です。
---	--------------------

アクセス制御 登録リスト				
選択	インターフェース	IP アドレス	サービス	動作
<input type="checkbox"/>	WAN	Any	http	透過
<input type="checkbox"/>	WAN	Any	ping	透過

■ 選択した登録を編集 (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。

■ 選択した登録上げる (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。

■ 選択した登録を下げる (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。

■ 選択した登録を削除 (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。

	WAN 側からアクセスする場合、本製品の WAN 側の IP アドレスを指定して下さい。 WAN 側の IP アドレスは、ステータス画面 (19 ページ) の「IP アドレス」欄で調べることができます。
---	--

6-7.DMZ 設定

DMZ 設定について説明します。

DMZ 機能を使用することにより、WAN 側 IP アドレス宛の全ての通信を、LAN 内の特定の IP アドレスへ転送することができます。

 注意	転送先 IP アドレスに設定した端末は、セキュリティが低下しますので注意して下さい。 (必要に応じて、端末側でセキュリティ対策を行って下さい。)
---	---

 確認	DMZ 設定とポートフォワーディング設定を同時に使用した場合、ポートフォワーディング設定が優先されます。 DMZ 設定を有効にした場合、「WAN 側からの Ping 応答を返す」設定と「WAN 側から設定画面へのログオンを許可する」設定は無効になります。 インターネットから DMZ 機能により LAN 側の端末へアクセスする場合、プロバイダから付与される IP アドレスが「グローバル IP アドレス」である必要があります。 付与される IP アドレスが「プライベート IP アドレス」の場合は、インターネットからアクセスする事はできません。
---	---

設定メニューの「ファイアウォール」より「DMZ 設定」をクリックして下さい。

「DMZ 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク - ファイアウォール IP フィルター 設定 IPv6 フィルター 設定 MAC フィルター 設定 ドメインフィルター 設定 ポートフォワーディング 設定 アクセス制御 設定 DMZ 設定	<h3>DMZ 設定</h3> <p>このページではインターネットからアクセス可能なホストが設定できます。</p> <table border="1" style="width: 100%;"><tr><td>DMZ ホスト:</td><td><input checked="" type="radio"/> 有効 <input type="radio"/> 無効</td></tr><tr><td>DMZ ホスト IP アドレス:</td><td><input type="text" value="192.168.0.100"/></td></tr></table> <p style="text-align: center;"><input type="button" value="設定保存"/></p>	DMZ ホスト:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	DMZ ホスト IP アドレス:	<input type="text" value="192.168.0.100"/>
DMZ ホスト:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効				
DMZ ホスト IP アドレス:	<input type="text" value="192.168.0.100"/>				

■DMZ ホスト(ラジオボタン)

DMZ ホスト機能の有効/無効を切り替えます。

■DMZ ホスト IP アドレス

フォワード(転送)する LAN 側端末の IP アドレスを入力して下さい。

 確認	転送先の端末は IP アドレスを固定設定することを推奨します。
---	---------------------------------

■設定保存(ボタン)

設定内容を保存します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

6-8.WAN 側から設定画面へアクセスする場合の設定方法

WAN 側から設定画面へアクセスする場合の設定方法について説明します。



「WAN 側から設定画面へアクセスする」設定にする場合、必ずユーザー名、パスワードを変更して下さい。
変更方法は「8-7.ログイン 設定」(135 ページ)を参照して下さい。

- ①設定メニューの「ファイアウォール」より「アクセス制御 設定」をクリックして下さい。
「アクセス制御 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク - ファイアウォール IP フィルター 設定 IPv6 フィルター 設定 MAC フィルター 設定 ドメインフィルター 設定 ポートフォワーディング 設定 アクセス制御 設定 DMZ 設定	アクセス制御 設定 このページでは本機への通信を透過/遮断するプロトコルとIPアドレス アクセス制御機能: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 WAN側からのPING アタック検出: 1 1秒間に許容 WAN側からのHTTP アタック検出: 30 30秒間に許容 ※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作し 設定保存 設定反映 インターフェース: LAN
---	--

- ②アクセス制御機能で「有効」(ラジオボタン)を選択して、「設定保存」ボタンをクリックして下さい。
「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

アクセス制御 設定 このページでは本機への通信を透過/遮断するプロトコルとIPアドレスの登録、編集、削除および表示が行なえます。	
アクセス制御機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
WAN側からのPING アタック検出:	1 1秒間に許容するPINGアクセス数。(0 - 100) ※
WAN側からのHTTP アタック検出:	30 30秒間に許容する最大TCP/IP(HTTP)コネクション数。(0 - 100) ※
※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作します。	
設定保存	設定反映

- ③以下の各設定を行って下さい。

インターフェース:	WAN
送信元IPアドレス/マスク:	
サービス名:	<input type="checkbox"/> Any <input checked="" type="checkbox"/> http <input type="checkbox"/> ping
動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過
追加	

■ インターフェース

プルダウンメニューで「WAN」を選択して下さい。

■ 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指定する場合入力して下さい。

指定しない(Any)場合は空欄にして下さい。

■ サービス名

「http」にチェックを入れて下さい。

■ 動作

「透過」を選択して下さい。

<次ページへ進んで下さい>

- ④設定が完了したら、[追加]ボタンをクリックして下さい。
アクセス制御 登録リストに登録されます。

アクセス制御 登録リスト				
選択	インターフェース	IPアドレス	サービス	動作
<input type="checkbox"/>	WAN	Any	http	透過

- ⑤[設定反映]ボタンをクリックして下さい。
[今すぐ再起動]ボタンをクリックすると、再起動後に設定が反映されます。

アクセス制御 設定	
このページでは本機への通信を透過/遮断するプロトコルとIPアドレスの登録、編集、削除および表示が行なえます。	
アクセス制御機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容するPINGアクセス数。(0 - 100) ※
WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容する最大TCP/IP(HTTP)コネクション数。(0 - 100) ※
※: 本機能は、WAN側からのアクセスに登録しているサービスに対して動作します。	
<input type="button" value="設定保存"/>	<input type="button" value="設定反映"/>

6-9.WAN 側からの Ping 応答を返す場合の設定方法

WAN 側からの PING に応答を返す場合の設定方法について説明します。

- ①設定メニューの「ファイアウォール」より「アクセス制御 設定」をクリックして下さい。
「アクセス制御 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク - ファイアウォール IP フィルター 設定 IPv6 フィルター 設定 MAC フィルター 設定 ドメインフィルター 設定 ポートフォワーディング 設定 アクセス制御 設定 DMZ 設定	<h3>アクセス制御 設定</h3> <p>このページでは本機への通信を透過/遮断するプロトコルとIPアドレス</p> <table><tr><td>アクセス制御機能:</td><td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効</td></tr><tr><td>WAN側からのPING アタック検出:</td><td><input type="text" value="1"/> 1秒間に許容</td></tr><tr><td>WAN側からのHTTP アタック検出:</td><td><input type="text" value="30"/> 30秒間に許容</td></tr></table> <p>※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作し</p> <p><input type="button" value="設定保存"/> <input type="button" value="設定反映"/></p> <p>インターフェース: <input type="text" value="LAN"/></p>	アクセス制御機能:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容	WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容
アクセス制御機能:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効						
WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容						
WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容						

- ②アクセス制御機能で「有効」(ラジオボタン)を選択して、[設定保存]ボタンをクリックして下さい。
「設定は正常に保存されました。」と表示されますので、「後で再起動」ボタンを押して下さい。

<h3>アクセス制御 設定</h3> <p>このページでは本機への通信を透過/遮断するプロトコルとIPアドレスの登録、編集、削除および表示が行なえます。</p>	
アクセス制御機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容するPINGアクセス数。(0 - 100) ※
WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容する最大TCP/IP(HTTP)コネクション数。(0 - 100) ※
※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作します。	
<input type="button" value="設定保存"/>	<input type="button" value="設定反映"/>

- ③以下の各設定を行って下さい。

インターフェース:	<input type="text" value="WAN"/>
送信元 IP アドレス/マスク:	<input type="text"/> / <input type="text"/>
サービス名:	<input type="checkbox"/> Any <input type="checkbox"/> http <input checked="" type="checkbox"/> ping
動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過
<input type="button" value="追加"/>	

■ インターフェース

プルダウンメニューで「WAN」を選択して下さい。

■ 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指定する場合入力して下さい。
指定しない(Any)場合は空欄にして下さい。

■ サービス名

「ping」にチェックを入れて下さい。

■ 動作

「透過」を選択して下さい。

<次ページへ進んで下さい>

- ④設定が完了しましたら、[追加]ボタンをクリックして下さい。
アクセス制御 登録リストに登録されます。

アクセス制御 登録リスト				
選択	インターフェース	IPアドレス	サービス	動作
<input type="checkbox"/>	WAN	Any	ping	透過

- ⑤[設定反映]ボタンをクリックして下さい。
[今すぐ再起動]ボタンをクリックすると、再起動後に設定が反映されます。

アクセス制御 設定	
このページでは本機への通信を透過/遮断するプロトコルとIPアドレスの登録、編集、削除および表示が行なえます。	
アクセス制御機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容するPINGアクセス数。(0 - 100) ※
WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容する最大TCP/IP(HTTP)コネクション数。(0 - 100) ※
※: 本機能は、WAN側からのアクセスに登録しているサービスに対して動作します。	
<input type="button" value="設定保存"/>	<input type="button" value="設定反映"/>

7.付加機能

簡易 DNS 設定、ダイナミック DNS 設定、ルーティング設定について説明します。

7-1.簡易 DNS 設定

簡易 DNS 設定について説明します。

設定メニューの「付加機能」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。

ステータス + 無線LAN + ネットワーク + ファイアウォール - 付加機能 簡易DNS設定 ダイナミックDNS設定 ルーティング設定 IPv6アドレス配布設定 + マネージメント	簡易DNS設定 このページでは簡易DNS機能の設定が行えます。 簡易DNS機能: <input type="radio"/> 有効 <input checked="" type="radio"/> 無効 設定保存 設定反映 IPアドレス: <input type="text"/> ホスト名: <input type="text"/> コメント: <input type="text"/>
---	---

簡易DNS機能:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
設定保存	設定反映
IPアドレス:	<input type="text"/>
ホスト名:	<input type="text"/>
コメント:	<input type="text"/>
追加	



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-GM5A の IP アドレスを設定する必要があります。

■簡易 DNS 機能(ラジオボタン)

簡易 DNS 機能の有効/無効を切り替えます。

■設定保存(ボタン)

簡易 DNS 機能の有効/無効を変更した場合に押して下さい。

■設定反映(ボタン)

簡易 DNS の設定内容を動作に反映させる場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■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。

■追加(ボタン)

入力した内容を簡易 DNS テーブルに登録します。



最大 64 エントリまで登録可能です。

〈次ページへ進んで下さい〉

簡易DNS 登録リスト			
選択	IPアドレス	ホスト名	コメント
<input type="checkbox"/>	10.0.0.254	www.example.com	Webサーバー
<input type="button" value="選択した登録を編集"/> <input type="button" value="選択した登録を上げる"/> <input type="button" value="選択した登録を下げる"/> <input type="button" value="選択した登録を削除"/> <input type="button" value="全て削除"/>			

■ **選択した登録を編集(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。

■ **選択した登録上げる(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。

■ **選択した登録を下げる(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。

■ **選択した登録を削除(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。

7-2.ダイナミック DNS 設定

ダイナミック DNS 設定について説明します。



本機能は外部のダイナミック DNS サービスを利用します。
そのため、サービス提供元の仕様変更やサービス内容の変更により、利用できなくなる場合がありますのであらかじめご了承ください。

はじめに

現在対応しているダイナミック DNS サービスは以下の 4 つです。

「DynDNS」、「No-IP」、「Dynamic DO!.jp」、「MyDNS.JP」

他のダイナミック DNS サービスはご利用頂けませんのであらかじめご了承ください。

ダイナミック DNS 機能の設定を行う前に、各公式サイトにてアカウント登録とホスト名(ドメイン名)の取得を行って下さい。

DynDNS 公式サイト(英語)

<http://www.dyndns.com/>

No-IP 公式サイト(英語)

<http://www.no-ip.com/>

Dynamic DO!.jp 公式サイト(日本語)

<http://ddo.jp/>

MyDNS.JP 公式サイト(日本語)

<http://www.mydns.jp/>

設定メニューの「付加機能」より「ダイナミック DNS 設定」をクリックして下さい。

「ダイナミック DNS 設定」画面が開きます。

<p>ステータス</p> <ul style="list-style-type: none">+ 無線LAN+ ネットワーク+ ファイアウォール- 付加機能<li style="border: 2px solid red; padding: 2px;">ダイナミックDNS 設定ルーター設定IPv6アドレス配布 設定+ マネージメント	<h3 style="color: #0056b3;">ダイナミックDNS 設定</h3> <p>このページではダイナミックDNS設定が行えます。</p> <table border="1" style="width: 100%;"><tr><td>状態:</td><td><input checked="" type="checkbox"/> 登録を有効にする</td></tr><tr><td>DDNS プロバイダー:</td><td><input type="text" value="DynDNS.org"/></td></tr><tr><td>ホスト名:</td><td><input type="text"/></td></tr><tr><td>ユーザー名:</td><td><input type="text"/></td></tr><tr><td>パスワード:</td><td><input type="password"/></td></tr></table>	状態:	<input checked="" type="checkbox"/> 登録を有効にする	DDNS プロバイダー:	<input type="text" value="DynDNS.org"/>	ホスト名:	<input type="text"/>	ユーザー名:	<input type="text"/>	パスワード:	<input type="password"/>
状態:	<input checked="" type="checkbox"/> 登録を有効にする										
DDNS プロバイダー:	<input type="text" value="DynDNS.org"/>										
ホスト名:	<input type="text"/>										
ユーザー名:	<input type="text"/>										
パスワード:	<input type="password"/>										

<h3 style="color: #0056b3;">ダイナミックDNS 設定</h3> <p>このページではダイナミックDNS設定が行えます。</p>	
状態:	<input checked="" type="checkbox"/> 登録を有効にする
DDNS プロバイダー:	<input type="text" value="DynDNS.org"/>
ホスト名:	<input type="text"/>
ユーザー名:	<input type="text"/>
パスワード:	<input type="password"/>
<input type="button" value="追加登録"/> <input type="button" value="上書き登録"/> <input type="button" value="削除"/>	

- 登録を有効にする(チェックボックス)
登録する情報を有効にする場合、チェックを入れて下さい。
- DDNS プロバイダー
利用するダイナミック DNS サービス名を選択して下さい。
- ホスト名
取得したホスト名(ドメイン名)を入力して下さい。
「Dynamic DO!.jp」の場合は不要です。
- ユーザー名
登録したユーザー名(もしくはメールアドレス)を入力して下さい。
「Dynamic DO!.jp」の場合は登録したドメインを入力して下さい。
- パスワード
登録したパスワードを入力して下さい。

〈次ページへ進んで下さい〉

■追加登録(ボタン)

入力したダイナミック DNS 情報を登録します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

	最大 8 エントリまで登録可能です。
---	--------------------

■上書き登録(ボタン)

登録リストを「選択」すると、入力欄に現在の設定情報が表示されます。

設定情報を編集(設定内容を変更)した後に[上書き登録]ボタンを押して下さい。変更した情報が上書き登録されます。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■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。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

ダイナミックDNS 登録リスト					
選択	状態	ホスト名	ユーザー名	サービス	ステータス
<input type="radio"/>	有効	example1.com	user	mydns	更新成功
<input type="radio"/>	有効	example2.com	user	dyndns	更新成功

	ダイナミック DNS の更新に成功すると、ステータス欄に「更新成功」と表示されます。
---	--

7-3.ルーティング 設定

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、ルーティング設定について説明します。
設定メニューの「付加機能」より「ルーティング設定」をクリックして下さい。
「ルーティング 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク + ファイアウォール - 付加機能 簡易DNS 設定 ダイナミックDNS 設定 ルーティング 設定 IPv6アドレス配布 設定 + マネージメント	ルーティング 設定 このページでは静的なルーティング情報の登録、編集、削除、およびル
	状態: <input checked="" type="checkbox"/> 登録を有効にする
	宛先: <input type="text"/>
	サブネットマスク: <input type="text"/>
	ゲートウェイ: <input type="text"/>
	メトリック: <input type="checkbox"/>

ルーティング 設定 このページでは静的なルーティング情報の登録、編集、削除、およびルーティング情報の表示が行えます。	
状態: <input checked="" type="checkbox"/> 登録を有効にする	
宛先: <input type="text"/>	
サブネットマスク: <input type="text"/>	
ゲートウェイ: <input type="text"/>	
メトリック: <input type="checkbox"/>	
<input type="button" value="追加"/> <input type="button" value="設定反映"/> <input type="button" value="IPルーティング情報表示"/>	

	デフォルトゲートウェイは WAN 側インターフェース固定となります。
---	------------------------------------

- 登録を有効にする(チェックボックス)
登録する情報を有効にする場合、チェックを入れて下さい。
- 宛先
宛先(送信先)の IP アドレスを入力して下さい。
- サブネットマスク
宛先(送信先)の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。
- 追加(ボタン)
入力したルーティング情報を登録します。

	最大 8 エントリまで登録可能です。
---	--------------------

- 設定反映(ボタン)
アクセス制御の設定内容を動作に反映させる場合に押して下さい。
「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

<次ページへ進んで下さい>

■IP ルーティング情報表示(ボタン)

現在のルーティング情報(別ウィンドウ)を表示します。

IPルーティング情報

このページでは現在のルーティング情報を一覧表示します。

宛先	サブネットマスク	ゲートウェイ	メトリック	インターフェース
0.0.0.0	0.0.0.0	***.***.***.***	0	eth1
..***.***	255.255.255.240	*	0	eth1
127.0.0.0	255.255.255.0	*	0	lo
192.168.0.0	255.255.255.0	*	0	br0

再読み込み

閉じる

スタティック ルーティング 登録リスト

選択	状態	宛先	サブネットマスク	ゲートウェイ	メトリック
<input type="checkbox"/>	有効	192.168.1.0	255.255.255.0	192.168.0.254	1

選択した登録を編集

選択した登録を上げる

選択した登録を下げる

選択した登録を削除

全て削除

■選択した登録を編集(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。

■選択した登録上げる(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。

■選択した登録を下げる(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。

■選択した登録を削除(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。

7-4. IPv6 アドレス配布 設定

LAN インターフェースの IPv6 アドレスの自動配布設定について説明します。
設定メニューの「付加機能」より「IPv6 アドレス配布 設定」をクリックして下さい。
「IPv6 アドレス配布 設定」画面が開きます。

ステータス + 無線LAN - ネットワーク LAN 設定 WAN 設定 + VPN + ファイアウォール - 付加機能 簡易DNS 設定 ダイナミックDNS 設定 ルーティング 設定 IPv6アドレス配布 設定 + マネージメント	IPv6アドレス配布 設定
	このページではLANインターフェースのIPv6アドレス自動配布の設定が行えます。
	プレフィックス配布モード: SLAAC(RA) ▼
	プレフィックス モード: WAN 取得 ▼
	WAN インターフェース: 有線WAN ▼
	DNSサーバー配布モード: RDNSS & DHCPv6 ▼
	RAのDNS配布情報(O flag): DHCPv6 ▼
	IPv6 DNS モード: プロキシ ▼
	設定保存

■プレフィックス配布モード

LAN 内への IPv6 アドレスの配布方法を設定します。
「SLAAC(RA)」固定設定です。

■プレフィックスモード

プレフィックスの設定を WAN 側から取得します。
「WAN 取得」固定設定です。

■WAN インターフェース

「有線 WAN」固定設定です。

■DNS サーバー配布モード

DNS サーバー情報を RDNSS もしくは DHCPv6 のどちらで配布するかを設定します。
「RDNSS&DHCPv6」固定設定です。

■RA の DNS 配布情報(O flag)

DNS の配布情報を設定します。
DHCPv6: DNS サーバーアドレスを DHCPv6 で配布します。
RDNSS: DNS サーバーアドレスを RDNSS オプションで配布します。

■IPv6 DNS モード

「プロキシ」固定設定です。
IPv6 DNS サーバーアドレスとして、MR-GM5A のアドレスを付与します。

■設定保存(ボタン)

IPv6 アドレス配布の設定内容を動作に反映させる場合に押して下さい。
「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

8. マネージメント

システム 設定、時刻情報 設定、メール送信機能 設定、システム ログ、ファームウェア更新、設定保存・読み込み、ログイン 設定、再起動について説明します。

8-1. システム 設定

MR-GM5A の装置名称の設定、言語設定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 設定」をクリックして下さい。
「システム 設定」画面が開きます。

ステータス	システム 設定
+ 無線LAN	このページでは本装置全般の設定が行えます。
+ ネットワーク	装置名称設定
+ ファイアウォール	装置名称: <input type="text" value="MR-GM5A"/>
+ 付加機能	多国語設定
- マネージメント	言語選択: <input type="text" value="日本語"/>
システム 設定	<input type="button" value="設定保存"/>
時刻情報 設定	
メール送信 設定	
システム ログ	
ファームウェア更新	
設定保存・読み込み	
ログイン 設定	
再起動	

■装置名称

MR-GM5A の装置名称(ニックネーム)を設定します。

本項目で設定した装置名称は、「ステータス」画面、メール送信機能のメール内容、リモートログに表示されます。

■言語選択

設定画面の言語を選択します。日本語と英語が選択できます。

■設定保存(ボタン)

システム 設定を変更した場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

8-2.時刻情報 設定

時刻情報設定について説明します。

確認

内蔵モバイル接続時は、内蔵通信モジュールから時刻情報を取得する事も可能です。
設定方法については、「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。

設定メニューの「マネージメント」より「時刻情報 設定」をクリックして下さい。

「時刻情報 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク + ファイアウォール + 付加機能 - マネージメント システム 設定 時刻情報 設定 メール送信 設定 システム ログ ファームウェア更新 設定保存・読み込み	時刻情報 設定 このページでは本機の時刻情報の設定が行えます。 NTPクライアント機能を有効にすることでシステムの時刻を維持することができます。 <table border="1"><tr><td>現在時刻:</td><td>2025 年 7 月 16 日 16 時 29 分 44 秒</td></tr><tr><td>タイムゾーン選択:</td><td>Asia/Tokyo (UTC+09:00) ▼</td></tr><tr><td>NTPクライアント機能</td><td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効</td></tr><tr><td>SNTP サーバー:</td><td><input type="radio"/> ntp1.jst.mfeed.ad.jp ▼ <input type="text"/> (サーバー指定)</td></tr></table> <p>設定保存 再読み込み</p>	現在時刻:	2025 年 7 月 16 日 16 時 29 分 44 秒	タイムゾーン選択:	Asia/Tokyo (UTC+09:00) ▼	NTPクライアント機能	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	SNTP サーバー:	<input type="radio"/> ntp1.jst.mfeed.ad.jp ▼ <input type="text"/> (サーバー指定)
現在時刻:	2025 年 7 月 16 日 16 時 29 分 44 秒								
タイムゾーン選択:	Asia/Tokyo (UTC+09:00) ▼								
NTPクライアント機能	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効								
SNTP サーバー:	<input type="radio"/> ntp1.jst.mfeed.ad.jp ▼ <input type="text"/> (サーバー指定)								

■現在時刻

本製品の「現在の時刻」情報を表示します。

確認

再起動及び自動再起動を実行した場合、現在の時刻は「1970年1月1日9時0分0秒」に戻ります。

■タイムゾーン選択

日本の標準時間帯「Asia Tokyo (UTC+09:00)」が選択されていることを確認して下さい。

■NTP クライアント機能(ラジオボタン)

インターネット上の NTP サーバーを利用して本製品の時刻情報を調整する場合、有効を選択して下さい。

■SNTP サーバー

NTP クライアント機能を使用する際、参照する NTP サーバーを指定します。

•ntp1.jst.mfeed.ad.jp、ntp2.jst.mfeed.ad.jp、ntp3.jst.mfeed.ad.jp

→インターネットマルチフィード(MFEED) 時刻情報提供サービス for Public を参照します。

•サーバー指定

→上記以外の NTP サーバーを参照する場合、アドレスを入力して下さい。

確認

プルダウンメニューの NTP サーバーは、インターネットマルチフィード株式会社提供のものです。
<https://www.mfeed.ad.jp/ntp/>

■設定保存(ボタン)

時刻情報 設定を変更した場合に押して下さい。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■再読み込み(ボタン)

本画面を再読み込みします。

8-3.メール送信機能 設定

メール送信機能 設定について説明します。

	<p>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、もしくは「内蔵通信モジュールから時刻取得」(内蔵モバイル接続時)する事を推奨します。</p> <p>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ください。</p> <p>「NTP クライアント機能」については、「8-2.時刻情報 設定」(123 ページ) を参照して下さい。</p> <p>「内蔵通信モジュールから時刻取得」設定については、「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。</p>
---	--

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

「メール送信機能 設定」画面が開きます。

<p>ステータス</p> <ul style="list-style-type: none">+ 無線LAN+ ネットワーク+ ファイアウォール+ 付加機能- マネージメント システム 設定 時刻情報 設定 メール送信 設定 システム ログ ファームウェア更新 設定保存・読み込み	<h3>メール送信 設定</h3> <p>このページではメール送信の設定が行えます。</p> <table border="1"><tr><td>メール送信機能:</td><td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効</td></tr><tr><td>サーバーアドレス:</td><td><input type="text"/></td></tr><tr><td>サーバーポート:</td><td><input type="text" value="0"/></td></tr><tr><td>接続保護:</td><td><input type="text" value="なし"/> <input type="checkbox"/> StartTLS(RFC 3207)拡張を</td></tr><tr><td>送信サーバー:</td><td>認証方式: <input type="text" value="なし"/></td></tr><tr><td></td><td>ユーザー名: <input type="text"/></td></tr></table>	メール送信機能:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	サーバーアドレス:	<input type="text"/>	サーバーポート:	<input type="text" value="0"/>	接続保護:	<input type="text" value="なし"/> <input type="checkbox"/> StartTLS(RFC 3207)拡張を	送信サーバー:	認証方式: <input type="text" value="なし"/>		ユーザー名: <input type="text"/>
メール送信機能:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効												
サーバーアドレス:	<input type="text"/>												
サーバーポート:	<input type="text" value="0"/>												
接続保護:	<input type="text" value="なし"/> <input type="checkbox"/> StartTLS(RFC 3207)拡張を												
送信サーバー:	認証方式: <input type="text" value="なし"/>												
	ユーザー名: <input type="text"/>												

<h3>メール送信機能 設定</h3> <p>このページではメール送信機能の設定が行えます。</p>	
メール送信機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
サーバーアドレス:	<input type="text"/>
サーバーポート:	<input type="text" value="0"/>
接続保護:	<input type="text" value="なし"/> <input type="checkbox"/> StartTLS(RFC 3207)拡張を行わない
送信サーバー:	認証方式: <input type="text" value="なし"/>
	ユーザー名: <input type="text"/>
	パスワード: <input type="text"/>
	送信元メールアドレス: <input type="text"/> <input type="checkbox"/> 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
宛先メールアドレス:	<input type="text"/>

- **メール送信機能(ラジオボタン)**
メール送信機能の有効/無効を切り替えます。
- **サーバーアドレス**
メール送信サーバーのアドレスを入力して下さい。
- **サーバーポート**
メール送信サーバーのポート番号を入力して下さい。
- **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。

〈次ページへ進んで下さい〉

■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。
- GRAM-MD5 : GRAM-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。

■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。

■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

■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。

送信トリガー:	<input type="checkbox"/> WANインターフェース有効時のメール送信を有効にする
	<input type="checkbox"/> 定期メール送信を有効にする 0 時 0 分 0 秒 (0~24時間)
	<input type="checkbox"/> 時刻指定メール送信を有効にする ※ <input type="checkbox"/> 毎日 <input type="checkbox"/> 日 <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土 メール送信実施時刻 0 時 0 分
	<input type="checkbox"/> 装置起動時のメール送信を有効にする
	<input type="checkbox"/> 有線LANのLinkUP/LinkDOWNによるメール送信を有効にする
<input type="button" value="メール送信テストを行う"/>	
<small>※: 本機能は、NTP等により時刻同期された状態でのみ動作します。</small>	
<input type="button" value="設定保存"/>	

■WAN インターフェース有効時のメール送信を有効にする(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。

■定期メール送信を有効にする(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。

	定期メール送信間隔を 0 時 0 分 0 秒で設定すると、メールは送信されませんのでご注意ください。
---	--

■時刻指定メール送信を有効にする(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。

	「時刻指定メール送信」は、「NTP クライアント機能」による時刻情報取得、もしくは「内蔵通信モジュールから時刻取得」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。

■設定保存(ボタン)

設定内容を保存します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■メールの内容例

```
件名 :MR-GM5 00:10:38:**:**:** Status ←MR-GM5A の LAN ポート MAC アドレス

WAN interface Active ←メール送信のトリガー
System Information
Device Name MR-GM5A ←装置名称
System MR-GM5A-L1 ←機種名
Uptime 0days:0:1:26s ←起動経過時間
Version v2.xx.xx(MR001) ←ファームウェアバージョン
Build Date Fri Oct 18 16:47:05 JST 2024

CPU Usage 0%
Memeory Usage 29%
DNS Server ***.**.**.**.**.**.###.###.###.### ←現在の WAN 側 DNS サーバーIP アドレス
IPv4 Default Gateway ***.**.**.**.**.** ←現在の WAN 側デフォルトゲートウェイ IP アドレス
IPv6 Default Gateway

WLAN Information
Mode Access Point ←無線 LAN1 の動作モード
Band 5GHz(A+N+AC+AX) ←無線 LAN1 の周波数
Ssid MR-GM5A 5G ←無線 LAN1 の SSID
Channel 100 ←無線 LAN1 のチャンネル番号
Encryption WPA3 Transition ←無線 LAN1 の暗号モード
Bssid 00:10:38:3d:31:92
Connecting Clients 0 ←無線 LAN1 に接続しているクライアント数
wlan0 Disable. ←マルチ SSID1 の状態
wlan0 Disable. ←マルチ SSID2 の状態

LAN Information
IP Address 192.168.0.1 ←LAN ポート IP アドレス
Subnet Mask 255.255.255.0 ←LAN ポートサブネットマスク
Mac Address 001038***** ←LAN ポート MAC アドレス
DHCP Server Active ←DHCP サーバーの状態
IPv6 Address
IPv6 Local Address

Current WAN Interface Information
Wan Backup Action Disabled ←回線冗長化機能の設定
Current WAN Interface Built-in Module ←プライマリー接続の接続モード

Wired WAN Interface Information ←有線 WAN ポートの情報
Disable

LTE Built-in Module WAN Information ←内蔵モバイルの情報
Interface usb0
Status Connecting
IP Address ***.**.**.**.**.** ←WAN 側 IP アドレス
IMEI ***** ←内蔵通信モジュールの端末識別番号
ICCID ***** ←SIM カードの識別番号
CNUM 080***** ←SIM カードの電話番号
Range LTE ←回線種別
SQ 4 ←内蔵通信モバイルのアンテナ状態
RSSI -51dBm ←受信信号強度
RSRP -66.4 ←受信電力
RSRQ -6.2 ←受信品質
Cell ID *** ←基地局番号 (Cell ID)
BAND(ARFCN) 1300 ←LTE の周波数帯 (LTE frequency band)
Module FW Version 19005.9000.08.02.00.03 ←内蔵通信モジュールのファームウェアバージョン

USB Mobile Data Card WAN Information ←USB モバイルの情報
Disable

Current WAN interface statictics information
RX Bytes 33467 ←受信バイト数
RX Packets 141 ←受信パケット数
TX Bytes 15399 ←送信バイト数
TX Packets 151 ←送信パケット数
```

■メール送信のトリガーについて

メールの先頭に、メール送信のトリガー(要因)が記載されます。

WAN interface Active	WAN インターフェース有効時のメール送信
Smtpeexec Power on Started xx seconds ago	装置起動時のメール送信
Periodical	定期メール送信
Schedule	時刻指定メール送信
LAN (eth0)Link Up /LAN (eth0)Link Down	有線 LAN の LinkUP/LinkDOWN によるメール送信

8-4. システム ログ

システム ログ機能について説明します。

	システムログに表示される日時は、本製品内部の時刻情報です。 MR-GM5A が時刻設定を行っていない場合、正確な日時は表示されませんのでご注意ください。 「NTP クライアント機能」については、「8-2.時刻情報 設定」(123 ページ) を参照して下さい。 「内蔵通信モジュールから時刻取得」設定については、「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。
	設定画面で表示されるログは最新の 200 行です。

8-4-1. システムログ設定

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」画面が開きます。



■システム ログ(ラジオボタン)

システム ログの有効/無効を切り替えます。

■ログレベル

ログの出力レベルを選択します。

「Informational」の場合、「Emergency」「Alert」「Critical」「Error」「Warning」「Notice」「Informational」のログが表示されます。通常は初期値「Informational」のままご利用下さい。

※ログレベルの設定はローカルログにのみ適用されます。(リモートログには適用されません。)

■モード

ローカル : 設定画面にのみ出力します。

リモート : リモートへのみ出力します。

両方 : ローカルとリモート両方へ出力します。

■サーバーIP アドレス

リモートログを受信するパソコンの IP アドレスを入力して下さい。

	リモートログを受信する IP アドレスを複数設定することはできません。(単一 IP アドレスのみ設定可能)
---	---

■サーバーUDP ポート

リモートログの UDP ポート番号を設定します。

■リモートログに装置名称を表示する

リモートログに装置名称を表示する場合、有効に設定して下さい。

■設定保存(ボタン)

設定内容を保存します。「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

■再読み込み(ボタン)

本画面で表示されているシステムログを最新の状態に更新します。

■ログ クリア(ボタン)

システムログを消去します。

■ファイルに保存(ボタン)

システムログをファイルに保存します。

8-4-2.システムログ表示例

■内蔵モバイル接続時の表示例

```

daemon.info ltemd: ltemd start connection
daemon.info ltemd: Within the LTE radio range:1, Signal Quality:4, Received Signal Strengths(RSSI):25(-63 dBm),
Band:6100, CellID:76, RSRP:-94.0, RSRQ:-14.5 ←LTE 圏内・圏外、アンテナ状態(SQ)、電波強度(RSSI)、LTE の周波
数帯(LTE frequency band)
daemon.info statecheck: statecheck SCK_LTEM_DHCP_BOUND_CHECK, Start ltem_dhcp_bound check, set bound check
timer 60
kern.info udhcpd: udhcp client (v0.9.8) started
daemon.notice systemd: usb0 down
kern.err kernel: [ 52.890000] GobiNet 3-1:1.4 usb0: kevent 12 may have been dropped
daemon.notice systemd: usb0 up
kern.err kernel: [ 53.070000] GobiNet::158::ether_to_ip_fixup usb0 skb h_proto is 0806 will drop
kern.err kernel: [ 53.070000] GobiNet::2292::GobiNetDriverTxFixup Packet Dropped
kern.err kernel: [ 54.530000] GobiNet::158::ether_to_ip_fixup usb0 skb h_proto is 0806 will drop
kern.err kernel: [ 54.530000] GobiNet::2292::GobiNetDriverTxFixup Packet Dropped
kern.err kernel: [ 55.760000] GobiNet::158::ether_to_ip_fixup usb0 skb h_proto is 0806 will drop
kern.info udhcpd: Lease of ***.***.***.*** obtained, lease time 7200 ←プロバイダから取得した WAN 側 IP アドレス
daemon.notice systemd: usb0 up
daemon.notice systemd: usb0 up
daemon.info statecheck: statecheck SCK_LTEM_DHCP_BOUND_CHECK, Stop ltem_dhcp_bound check
kern.err kernel: [ 55.760000] GobiNet::2292::GobiNetDriverTxFixup Packet Dropped
kern.err kernel: [ 57.530000] GobiNet::158::ether_to_ip_fixup usb0 skb h_proto is 0806 will drop
daemon.info statecheck: statecheck SCK_REMOTE_COMM_CONFIRM_START, Start remote communication confirm,
interval 90
daemon.info dnsmasq[2587]: started, version 2.80 cachesize 150
daemon.info dnsmasq[2587]: compile time options: IPv6 GNU-getopt no-DBus no-i18n no-IDN no-DHCP no-Lua no-
TFTP no-contrack ipset auth no-DNSSEC loop-detect inotify no-dumpfile
daemon.info dnsmasq[2587]: using nameserver ***.***.***.111#53(via usb0) ←プロバイダから取得した DNS アドレス
daemon.info dnsmasq[2587]: using nameserver ***.***.***.222#53(via usb0) ←プロバイダから取得した DNS アドレス
daemon.info dnsmasq[2587]: using local addresses only for domain wpad.MR-GM5A
daemon.info dnsmasq[2587]: reading /var/resolv.conf
daemon.info dnsmasq[2587]: using nameserver ***.***.***.111#53(via usb0)
daemon.info dnsmasq[2587]: using nameserver ***.***.***.222#53(via usb0)
daemon.info dnsmasq[2587]: using local addresses only for domain wpad.MR-GM5A
daemon.warn dnsmasq[2587]: ignoring nameserver 127.0.0.1 - local interface
daemon.warn dnsmasq[2587]: ignoring nameserver ::1 - local interface
daemon.err dnsmasq[2587]: failed to load names from /etc/hosts: No such file or directory
daemon.info dnsmasq[2587]: read /var/hosts - 2 addresses

```

ltemd start connection	回線接続が開始されると表示されます。
Within the LTE radio range:1, Signal Quality:4, Received Signal Strengths(RSSI):25(-63 dBm), Band:6100, CellID:76, RSRP:-94.0, RSRQ:-14.5	LTE 圏内・圏外、アンテナ状態(SQ)、電波強度(RSSI)、LTE の周波数帯(LTE frequency band)、基地局番号(Cell ID)、受信電力(RSRP)、受信品質(RSRQ)を表示します。
Lease of ***.***.***.*** obtained, lease time 7200	プロバイダから IP アドレスを取得した場合に表示されます。
ltemd: LTE Module ether start error.	内蔵モバイルでの接続に失敗した場合に表示されます。ユーザー名、パスワード、APN、発信先電話番号等、接続情報に誤りが無いか確認して下さい。

■再起動に関するシステムログ

Router reboot by GUI.	設定画面から再起動した場合に表示されます。リモートログにのみ表示されます。
Router reboot by timer reboot setting.	タイマー再起動機能により、再起動した場合に表示されます。リモートログにのみ表示されます。

■無線 LAN 接続に関するシステムログ表示例

```
wlan0: STA **:~::~:~::~:~::~ IEEE 802.11: associated ←プライマリ SSID へ接続開始
RTW: [STA] r-idx:0 mac: ~::~:~::~:~::~ aid:1 mid:3 band:1 ch-bw-ofst:100-2-1
RTW: setkey_hdl: set group key for 00:10:38::~:~::~:~::~ kid:1 type:1 algo:AES
RTW: setkey_hdl: set group key for 00:10:38::~:~::~:~::~, kid:4 type:2 algo:BIP_CMAC_128
wlan0: STA **:~::~:~::~:~::~ WPA: pairwise key handshake completed (RSN) ←認証完了(接続完了)
```

wlan0:	無線 LAN 5GHz のプライマリ SSID に関するログです。
wlan0-vap0:、wlan0-vap1	無線 LAN 5GHz のマルチ SSID に関するログです。
wlan1:	無線 LAN 2.4GHz のプライマリ SSID に関するログです。
wlan1-vap0:、wlan1-vap1	無線 LAN 2.4GHz のマルチ SSID に関するログです。
RTW: OnDeAuth(wlan0) reason=1, ta::~:~::~:~::~:~::~ [WARNING][BB]Error Set Pwr Macid for STA not exist!!	無線 LAN 認証に失敗した場合には表示されます。
STA **:~::~:~::~:~::~ IEEE 802.11: disassociated	無線 LAN クライアントが切断された場合には表示されます。

■回線監視機能に関するシステムログ

Remote confirm receive ping reply from ~::~:~::~:~::~	宛先アドレスから Ping 応答が得られた場合には表示されます。
Remote confirm can't receive ping reply from ~::~:~::~:~::~	宛先アドレスから Ping 応答が得られなかった場合には表示されます。
Remote confirm receive http reply xxx from http://example.com/	宛先アドレスから http の応答が得られた場合には表示されます。
Can't connect http://example.com/ Can't send request to http://example.com/	宛先アドレスから http の応答が得られなかった場合には表示されます。
Remote comm confirm received reply from any hosts.	回線監視機能により、いずれかの宛先から応答が得られた場合には表示されます。
remote_comm_confirm failed count # remote_confirm_retry num #	回線監視機能により、全ての宛先から応答が得られなかった場合に表示されます。

■回線冗長化機能に関するシステムログ

WAN cold standby backup interface change ##### to #####.	回線冗長化機能(コールド・スタンバイ方式)で、プライマリー接続からセカンダリー接続へ切り替わった際に表示されます。
WAN cold standby backup check primary interface ##### to #####.	回線冗長化機能(コールド・スタンバイ方式)で、プライマリー通信確認間隔設定により、プライマリー接続へ切り替わった際に表示されます。
WAN backup secondary(#####) failed, reboot now.	回線冗長化機能(コールド・スタンバイ方式)で、セカンダリー接続での回線監視に失敗して再起動した際に表示されます。
WAN hot standby backup interface change ##### to #####.	回線冗長化機能(ホット・スタンバイ方式)で、回線切り替え時に表示されます。
#####は WAN 側接続モードを表します。 WiredWAN: 有線 WAN 接続 Built-in Module: 内蔵モバイル接続 USB Mobile Data Card: USB モバイル接続	

■NTP クライアントに関するシステムログ

NTP client successfully.	時刻同期が成功した場合には表示されます。
NTP client fail, retry 30sec later...	時刻同期が失敗した場合には表示されます。30 秒後にリトライします。

■DDNS 機能に関するシステムログ

DDNS update successfully.	DDNS 更新成功時に表示されます。
DDNS update fail, retry 60sec later...	DDNS 更新失敗時に表示されます。60 秒後にリトライします。

■DHCP サーバー機能に関するシステムログ

udhcpd: sending ACK to 192.168.0.2 ifindex 33 for xx-xx-xx-xx-xx-xx	DHCP のリクエストに対して、IP アドレスを付与したときに表示されます。
--	--

■設定画面へのログインに関するシステムログ

Authentication successful for admin from ::ffff:192.168.0.2	設定画面へのログイン(認証)に成功したときに表示されます。 (ユーザーID「admin」で「192.168.0.2」からログイン)
Authentication attempt failed for from ::ffff:192.168.0.2 because: Bad Password	設定画面へのログイン(認証)に失敗したときに表示されます。 (「192.168.0.2」からログイン)

8-5.ファームウェア更新

ファームウェアのバージョンアップ方法について説明します。

ファームウェアバージョンアップ時の注意
最新ファームウェアは弊社サポート&ダウンロードページより入手して下さい。 https://www.mrl.co.jp/supports/
ダウンロードしたファームウェアに同梱されている Readme を必ずお読み下さい。 バージョンアップ作業は、Readme を確認してから行って下さい。
ファームウェアのバージョンアップを行うパソコンでは、セキュリティソフト等、他のアプリケーションは停止して下さい。 他のアプリケーション等が動作していると、バージョンアップに失敗する恐れがあります。

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。

「ファームウェア更新」画面が開きます。

ステータス
+ 無線LAN
+ ネットワーク
+ ファイアウォール
+ 付加機能
- マネージメント
 システム 設定
 時刻情報 設定
 メール送信 設定
 システム ログ
 ファームウェア更新
 設定保存・読み込み
 ログイン 設定
 再起動

ファームウェア更新

このページではファームウェアの更新が行えます。
ファームウェア更新中は、本機の電源を切ったりケーブルを抜いたりしないでください。

今すぐファームウェア更新を行う

ファイルの選択 ファイルが選択されていません

ファームウェア更新開始 リセット

自動ファームウェア更新

自動ファームウェア更新: 有効 無効 ※

ファームウェアダウンロードURL:

毎日

ファームウェア更新

このページではファームウェアの更新が行えます。
ファームウェア更新中は、本機の電源を切ったりケーブルを抜いたりしないでください。

今すぐファームウェア更新を行う

ファイルの選択 ファイルが選...れていません

ファームウェア更新開始 リセット

- [参照]、または[ファイルを選択](ボタン)
バージョンアップファイルを選択して開きます。
- ファームウェア更新開始(ボタン)
バージョンアップファイルを開いた後、バージョンアップを開始します。
- リセット(ボタン)
バージョンアップファイルの選択をリセットします。

〈次ページへ進んで下さい〉

自動ファームウェア更新	
自動ファームウェア更新:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 ※
ファームウェアダウンロードURL:	<input type="text"/>
曜日:	<input type="checkbox"/> 毎日 <input type="checkbox"/> 日 <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土
ファームウェア更新時刻:	0 時 0 分
※: 自動ファームウェア更新機能は、NTP等により時刻同期された状態でのみ動作します。	
設定保存	

	<p>「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が必要です。</p> <p>「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、もしくは「内蔵通信モジュールから時刻取得」(内蔵モバイル接続時)が正常に行われた場合にのみ動作します。</p> <p>「NTP クライアント機能」については、「8-2.時刻情報 設定」(123 ページ)を参照して下さい。</p> <p>「内蔵通信モジュールから時刻取得」設定については、「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。</p>
---	---

■自動ファームウェア更新(ラジオボタン)

自動ファームウェア更新機能を使用する場合、「有効」を選択して下さい。

■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。

■曜日

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。

バージョンアップサーバーに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。
- ・ファームウェア更新時刻 : 更新確認を実行する時刻を入力して下さい。

■設定保存(ボタン)

自動ファームウェア更新の設定内容を保存します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

8-6.設定保存・読み込み

設定内容をファイルに保存する、保存した設定ファイルを読み込む、設定を工場出荷値に戻す方法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「設定保存・読み込み」をクリックして下さい。
「設定保存・読み込み」画面が開きます。

設定保存・読み込み
このページでは設定のファイル保存と設定ファイル読み込み、および工場出荷設定に戻すことができます。

設定をファイルに保存:

設定をファイルから読み込む: ファイルが選択されていません

設定を工場出荷値に戻す:

■設定をファイルに保存(ボタン)

現在の設定をファイルとして保存します。

■設定をファイルから読み込む

ファイルから設定を読み込みます。

■[ファイルの選択]、または[参照](ボタン)

保存した設定ファイルを選択して開きます。

■[読込](ボタン)

参照した設定ファイルの内容を設定に反映します。

ボタンを押すと即再起動します。

■設定を工場出荷値に戻す 実行(ボタン)

設定内容を工場出荷状態に戻します。

「設定を工場出荷値に戻してもよろしいですか？」とメッセージが表示されます。

[OK]ボタンを押すと即再起動します。

8-7.ログイン 設定

設定画面へのログオンするためのユーザー名、パスワードの設定方法について説明します。



ユーザー名、パスワードを変更する事を強く推奨します。
特に「WAN 側から設定画面へのログオンを許可する」設定にしている場合、必ず変更して下さい。

設定メニューの「マネージメント」より「ログイン 設定」をクリックして下さい。

「ログイン 設定」画面が開きます。

ステータス + 無線LAN + ネットワーク + ファイアウォール + 付加機能 - マネージメント システム 設定 時刻情報 設定 メール送信 設定 システム ログ ファームウェア更新 設定保存・読み込み ログイン 設定 再起動	ログイン 設定 このページでは本機の設定画面にアクセスするためのアカウント設定が行えます。
	GUIアクセス設定
	GUIポート: <input type="text" value="80"/>
	ユーザー名: <input type="text" value="admin"/>
	パスワード: <input type="password" value="....."/>
	<input type="button" value="設定保存"/>

■GUI ポート

設定画面へのアクセスポート番号を「80(www-http)」から変更できます。

本設定は、LAN 側/WAN 側共通となりますので LAN 側からも変更したポート番号でログオンする必要があります。

変更後は「http://192.168.0.1:10000」のように「http://MR-GM5A の IP アドレス:(コロン) 変更したポート番号」の形式で設定画面にログオンして下さい。

	ポート番号を変更する場合は、「1024～65534」の範囲(10000 以降推奨)で設定して下さい。 「1～1023」を設定してしまうと、ブラウザソフト側の制限で設定画面にログオンできなくなる可能性がありますのでご注意ください。
	「10080」はブラウザ側のセキュリティ制限で設定画面にログオンできなくなる可能性がありますので設定しないで下さい。
	ポート番号を変更する場合、変更後のポート番号を忘れないように注意して下さい。 ポート番号が分からなくなってしまった場合、INIT ボタンによる設定初期化以外に救済措置はありません。
	ポートフォワーディング設定にここで設定したポート番号を登録する、もしくは DMZ ホスト機能を有効にすると、これらの機能が優先され WAN 側から設定画面にログオンできなくなります。

■ユーザー名

設定画面にアクセスするためのユーザー名を入力して下さい。

■パスワード

設定画面にアクセスするためのパスワードを入力して下さい。

■設定保存(ボタン)

設定内容を保存します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。

引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

8-8.再起動

本装置の再起動、自動再起動(タイマー再起動)の設定を行う「再起動」画面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「再起動」をクリックして下さい。

「再起動」画面が開きます。

ステータス + 無線LAN + ネットワーク + ファイアウォール + 付加機能 - マネージメント システム 設定 時刻情報 設定 メール送信 設定 システム ログ ファームウェア更新 設定保存・読み込み ログイン 設定 再起動	再起動 このページでは本機の再起動を行います。 今すぐ再起動 <input type="button" value="再起動"/> 自動再起動 モード: <input type="text" value="無効"/> 曜日: <input type="checkbox"/> 毎日 <input type="checkbox"/> 日 <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土 時刻: <input type="text" value="0"/> 時 稼働時間: <input type="text" value="24"/> 時 <small>※: 曜日時刻指定による再起動機能は、NTP等により時刻同期さ</small>
--	--

■今すぐ再起動 再起動(ボタン)

本装置を再起動します。

8-8-1.自動再起動(タイマー再起動)

自動再起動	
モード:	<input type="text" value="無効"/> ※
曜日:	<input type="checkbox"/> 毎日 <input type="checkbox"/> 日 <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土
時刻:	<input type="text" value="0"/> 時 <input type="text" value="0"/> 分
稼働時間:	<input type="text" value="24"/> 時 <input type="text" value="0"/> 分 <input type="text" value="0"/> 秒
<small>※: 曜日時刻指定による再起動機能は、NTP等により時刻同期された状態でのみ動作します。</small>	
<input type="button" value="設定保存"/>	

■モード

自動再起動機能を設定します。

- ・曜日時刻指定 : スケジュールにより再起動を行います。
- ・稼働時間指定 : システム稼働時間により再起動を行います。

 確認	曜日時刻指定の再起動は、「NTP クライアント機能」による時刻情報取得、もしくは「内蔵通信モジュールから時刻取得」(内蔵 LTE 接続時)が正常に行われた場合にのみ動作します。 「NTP クライアント機能」については、「8-2.時刻情報 設定」(123 ページ)を参照して下さい。 「内蔵通信モジュールから時刻取得」設定については、「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。
---	---

■曜日・時刻

再起動を行うスケジュールを設定します。

- ・毎日 : 毎日再起動します。
- ・日曜～土曜 : 曜日を指定して再起動します。
- ・時刻 : 再起動を実行する時刻を入力して下さい。

■稼働時間

再起動を行う間隔(稼働時間)を入力して下さい。現在の稼働時間は、ステータス画面(19 ページ)で確認することができます。

 確認	稼働時間は、システム再起動(もしくは電源 OFF/ON)時にクリアされます。
---	--

■設定保存(ボタン)

自動再起動機能の設定内容を保存します。

「設定は正常に保存されました。」と表示されますので、設定を動作に反映させる場合は[今すぐ再起動]ボタンを押して下さい。引き続き他の設定を行う場合は「後で再起動」ボタンを押して下さい。

9.仕様

MR-GM5A 仕様		
分類	仕様	
4G/3G 内蔵通信モジュール	対応周波数	4G Cat.4 (800MHz/900MHz/1.5GHz/1.8GHz/2.1GHz/2.5GHz) : Band 1/3/8/11/18/19/21/26/28/41 3G (800MHz/2.1GHz) : Band 1/6/8/19
	通信方式	FDD-LTE/TDD-LTE/3G(HSPA+)
	SIM スロット	標準 SIM(25×15mm)サイズ
	アンテナ	背面 SMA コネクタ×2
USB ポート	1 ポート (USB2.0 TypeA コネクタ)	
有線 LAN ポート	2 ポート (RJ-45) 10BASE-T/100BASE-TX: AUTO MDI/MDI-X 対応 1000BASE-T: Master/Slave 対応 (有線 WAN 接続の場合、ETH1 ポートが有線 WAN ポートとして動作)	
無線 LAN 規格	5GHz 無線 LAN: IEEE802.11 a/n/ac/ax 2.4GHz 無線 LAN: IEEE802.11 b/g/n (接続可能な無線 LAN 端末台数は、5GHz 帯、2.4GHz 帯それぞれに最大 48 台まで)	
無線 LAN アンテナ	内部アンテナ×2	
無線LANセキュリティ	WPA3-SAE (AES)、WPA2-PSK (AES/TKIP)、WPA-PSK (AES/TKIP)、 WEP (128/64bit) MAC アドレスフィルタリング (プライマリ-SSID のみ)、ステルス SSID マルチ SSID、無線 LAN セパレータ機能	
ルーター機能	NAPT (IP マスカレード)、DHCP サーバー、 ポート開放 (ポートフォワーディング、ポートマッピング、DMZ ホスト)、 IP フィルター、ドメインフィルター、MAC フィルター、 IPv6 接続機能 (IPv4 over IPv6、有線 WAN 接続のみ)、 VPN (IPsec) 接続機能	
電源アダプター	AC アダプター 入力: 100VAC 50/60Hz 出力: DC12V 2A	
筐体	176(W) × 110(D) × 25(H) mm (本体のみ・突起部を除く)	
重量	約 240g (本体のみ)	
環境条件	温度: 0~45°C 湿度: 25~85% (結露しないこと)	
環境対応	RoHS 指令準拠	

10.Q&A

本製品を使用する上での Q&A 集です。

本製品が正しく動作しないときや、不明な点があるときに参照して下さい。

設定時の Q&A	139
Q.ランプが点灯しない。.....	139
Q.設定画面へログオンできない。.....	140
Q.パスワードを入力しても設定画面へログオンできない。.....	141
Q.管理者パスワードを忘れたため、設定画面へログオンできなくなった。.....	141
Q.SSID が検索できない。.....	141
Q.SSID と事前共有鍵(暗号キー)を知りたい。.....	142
Q.ポートを空けたい。.....	142
Q.サーバーやネットワークカメラを公開したい。.....	142
Q.インターネット側からの Ping に応答させたい。.....	142
Q.インターネット側から設定画面へログオンしたい。.....	142
Q.無線 LAN セパレータ機能を設定したい。.....	143
Q.ETH1 ポートが LAN ポートとして使用できない。.....	143
Q.自動再起動(タイマー再起動)を設定したい。.....	143
Q.アクセス制御設定がマルチ SSID に反映されない。.....	143
設定後の Q&A	144
Q.LTE ランプが点灯しない。.....	144
Q.USB ランプが点灯しない。.....	144
Q.有線 LAN 接続でインターネットへ接続できない。.....	144
Q.無線 LAN 接続でインターネットへ接続できない。.....	145
Q.回線が切断される。.....	146
Q.回線の接続・切断を繰り返す。.....	147
Q.回線冗長化機能が動作しない。.....	147
Q.回線冗長化機能でセカンダリー接続に切り替わった後プライマリー接続に戻らない。.....	147
Q.インターネットに接続できるが、速度が遅い。.....	147
Q.本体 IP アドレスを変更した後、設定画面へログオンできなくなった。.....	147
Q.WAN 側から設定画面が開けない。.....	148
Q.WAN 側からの Ping に応答しない。.....	148
Q.プロバイダから自動取得した IP アドレスを知りたい。.....	148
Q.UPnP 対応ソフトウェアが動作しない。.....	148
Q.固定 IP アドレス付与機能が動作しない。.....	149
Q.メール送信機能で送信したメールが受信できない。.....	149
Q.スケジュールによる自動再起動が動作しない。.....	149
その他の Q&A	150
Q.ファームウェアバージョンや MAC アドレスを知りたい。.....	150
Q.設定を工場出荷値に戻したい。.....	150

Q.ランプが点灯しない。

A.以下の各項目を確認して下さい。

■「Power」ランプが点灯しない。

本製品付属の専用電源アダプターを使用しているか確認して下さい。
他製品の電源アダプターは使用できませんのでご注意ください。

■「WLAN」ランプが点灯しない。

本製品の無線 LAN 機能が有効になっているか確認して下さい。
無線 LAN 基本設定 の「無線 LAN 機能を無効にする」にチェックが入っている場合はチェックを外して下さい。
「4.無線 LAN 設定」(27 ページ)を参照して下さい。

■「LTE」ランプが点灯しない。

LTE ランプが点滅、もしくは消灯している場合、内蔵通信モジュールでの回線接続が完了していません。

- ・SIM カードが正しく取り付けられているか確認して下さい。
「2-1.各機器との接続」(4 ページ)を参照して下さい。
- ・内蔵通信モジュール用外部アンテナが正しく取り付けられているか確認して下さい。
「2-1.各機器との接続」(4 ページ)を参照して下さい。
- ・接続 ID、パスワード、APN、電話番号が正しく設定されているか確認して下さい。
「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。

■「USB」ランプが点灯しない。

USB モバイルデータカードを認識していません。
WAN 設定で「USB モバイル」が有効になっているか確認して下さい。
「5-2-2.USB モバイル設定」(74 ページ)を参照して下さい。
WAN 設定を確認しても認識しない場合は、モバイルデータカードを一度取り外し、再度接続して下さい。
抜き差ししても認識しない場合は、本製品の電源を入れなおして下さい。

■「ETH0」、「ETH1」が点灯しない。

- ・LAN ケーブルが正しく接続されているか確認して下さい。
接触不良等を起こしていないか確認して下さい。
- ・LAN ケーブルを交換してみてください。
LAN ケーブルを別の物に交換してみてください。
- ・本製品とパソコンの間に HUB を経由している場合、パソコンを本製品に直接接続してみてください。
HUB を経由せずに接続できるか確認して下さい。

Q.設定画面へログオンできない。

A.以下の各項目を確認して下さい。

■製品付属の専用電源アダプターを接続していますか？

(本製品の電源は ON になっていますか？)

他の電源アダプターを接続した場合、本製品は正しく動作しません。

必ず本製品に付属の専用電源アダプターを接続して下さい。

(パソコンの電源を ON にする前に、本製品の電源を ON にして下さい。)

■本製品が起動中ではありませんか？

本体上面の「Power」ランプ「Status1」ランプが点灯するまでお待ち下さい。

■パソコンと本製品が正しく接続されていますか？

・有線 LAN の場合

LAN ケーブルが正しく接続されているか確認して下さい。

・無線 LAN の場合

パソコン側の無線 LAN アダプターが正しくセットアップされているか確認して下さい。

確認方法については、無線 LAN アダプターのマニュアル等を参照して下さい。

■初期設定の場合、ETH0 ポートに接続していますか？

有線 LAN パソコンから初期設定を行う場合、必ず ETH0 ポートに接続して下さい。

ETH1 ポートは工場出荷値、WAN ポートとして動作していますので、ETH1 ポートから設定画面を開くことはできません。

■パソコンのイーサネットポート/無線 LAN アダプターは正常に動作していますか？

パソコン、またはイーサネットボード/無線 LAN アダプターのマニュアルを参照し、正常に動作していることを確認して下さい。

■パソコンにネットワークアダプターが複数セットアップされていませんか？

パソコンにネットワークアダプター(無線 LAN も含む)が複数セットアップされている場合は、MR-GM5A に接続していないネットワークアダプターを一時的に無効(未使用)にして下さい。

■本製品の DHCP サーバーを使用する(工場出荷値)場合、IP アドレスが正しく取得されていますか？

パソコンが IP アドレスを正しく取得できているか確認して下さい。

【MR-GM5A が工場出荷値の場合】

IP アドレス: 192.168.0.2~192.168.0.30 のいずれか

サブネットマスク: 255.255.255.0

デフォルトゲートウェイ: 192.168.0.1

プライマリ DNS: 192.168.0.1

■WWW ブラウザが「プロキシサーバーを使用する」設定になっていませんか？

本製品の設定を行う際は、WWW ブラウザを「プロキシサーバーを使用しない」設定にする必要があります。

以下の方法で、WWW ブラウザを「プロキシサーバーを使用しない」設定にして下さい。

■WWW ブラウザのキャッシュを削除してみてください。

以下、Microsoft Edge でキャッシュを削除する例です。

- 1.Microsoft Edge 画面右上の[⋯]をクリックして[設定]をクリックして下さい。
- 2.[プライバシー、検索、サービス]をクリックして下さい。
- 3.「閲覧データをクリア」欄の[クリアするデータの選択]ボタンをクリックして下さい。
- 4.「キャッシュされた画像とファイル」にのみチェックを入れ、他のチェックは外して下さい。
- 5.[今すぐクリア]ボタンをクリックして下さい。
- 6.Microsoft Edge を再起動し、再度設定画面にログオンできるか確認して下さい。

■ファイアウォール/セキュリティ対策ソフトウェア等が起動・常駐していませんか？

設定を行うパソコンにファイアウォール/セキュリティ対策ソフトウェアがインストールされている・常駐している場合、設定を始める前に、ソフトウェア側の動作・設定を一時的に以下のように変更して下さい。

(ファイアウォール/セキュリティ対策ソフトウェアが、本製品との通信を遮断してしまう場合があります。)

- ・ファイアウォール/セキュリティ対策ソフトウェアのセキュリティレベル設定を「一番低いレベル」へ変更する。
 - ・ファイアウォール/セキュリティ対策ソフトウェアをいったん無効にする。
- 変更方法等について、詳しくはソフトウェアのマニュアルを参照して下さい。

Q.パスワードを入力しても設定画面へログオンできない。

A.以下の各項目を確認して下さい。

■パスワードを間違えていませんか？

正しいパスワードを入力して下さい。

パスワードがわからなくなってしまった場合は、設定を初期化して下さい。

詳しくは以下を参照して下さい。

Q.管理者パスワードを忘れたため、設定画面へログオンできなくなった。(次項)

■他製品の設定画面を開いていませんか？

WWW ブラウザに入力しているアドレスに間違いがないか確認して下さい。

本製品の本体 IP アドレスが工場出荷値の場合は「http://192.168.0.1/」を入力しているか確認して下さい。

Q.管理者パスワードを忘れたため、設定画面へログオンできなくなった。

A.以下の手順で設定を初期化して下さい。

 確認	設定内容は全て初期化されます。
---	-----------------

- 1) 本製品の電源を入れて下さい。
- 2) 電源投入から本製品が起動するまで 1 分程度お待ち下さい。
- 3) 本体背面の INIT ボタンを **8 秒以上**押し続けて下さい。
- 4) 8 秒以上たったら INIT ボタンを放して下さい。
- 5) 再起動が完了すると設定が初期化されます。

Q.SSID が検索できない。

A. 以下の各項目を確認して下さい。

■本製品のブロードキャスト SSID 設定が有効になっているか確認して下さい。

本製品のブロードキャスト SSID 設定が「無効」になっている場合、SSID は検索できません。

ブロードキャスト SSID 設定については以下を参照して下さい。

- ・5GHz 無線 LAN 設定
→「4-1-1.基本 設定」(27 ページ)
- ・2.4GHz 無線 LAN 設定
→「4-2-1.基本 設定」(39 ページ)

■パソコン側無線 LAN アダプターが正しくセットアップされているか確認して下さい。

パソコン側無線 LAN アダプターが正しくセットアップされていること、正しく動作していることを確認して下さい。

確認方法については、無線 LAN アダプターのマニュアル等を参照して下さい。

■無線 LAN の電波状況を改善して下さい。

- ・本製品と無線 LAN クライアントの距離を短くして下さい。
- ・本製品と無線 LAN クライアントの間に障害物がある場合は、取り除いて下さい。
- ・本製品の無線 LAN チャンネル番号を変更して下さい。
無線 LAN チャンネル番号の変更方法については以下を参照して下さい。
 - ・5GHz 無線 LAN 設定
→「4-1-1.基本 設定」(27 ページ)
 - ・2.4GHz 無線 LAN 設定
→「4-2-1.基本 設定」(39 ページ)

Q.SSID と事前共有鍵(暗号キー)を知りたい。

A. 本製品の設定画面で確認して下さい。

SSID は、設定画面の「無線 LAN 設定」の「基本設定」で確認することができます。
詳しくは以下を参照して下さい。

- ・5GHz 無線 LAN 設定
→「4-1-1.基本 設定」(27 ページ)
- ・2.4GHz 無線 LAN 設定
→「4-2-1.基本 設定」(39 ページ)

設定されている事前共有鍵(暗号キー)は、設定画面の「無線 LAN 設定」の「セキュリティ設定」で確認することができます。
詳しくは以下を参照して下さい。

- ・5GHz 無線 LAN 設定
→「4-1-3.セキュリティ 設定」(31 ページ)
- ・2.4GHz 無線 LAN 設定
→「4-2-3.セキュリティ 設定」(43 ページ)

 確認

工場出荷値の事前共有鍵(暗号キー)は、本製品底面に貼付されているシールに記載されている「KEY」で確認する事ができます。

Q.ポートを開けたい。

A.「ファイアウォール」→「ポートフォワーディング設定」を行って下さい。

ポートを開ける必要がある場合は、ポートフォワーディング設定を行って下さい。
詳しくは、「6-5.ポートフォワーディング 設定」(105 ページ)を参照して下さい。

Q.サーバーやネットワークカメラを公開したい。

A.「ファイアウォール」→「ポートフォワーディング設定」を行って下さい。

詳しくは、「6-5.ポートフォワーディング 設定」(105 ページ)を参照して下さい。

Q.インターネット側からの Ping に応答させたい。

A.「ファイアウォール」→「アクセス制御設定」を行って下さい。

詳しくは、「6-9.WAN 側からの Ping 応答を返す場合の設定方法」(113 ページ)を参照して下さい。

 確認

インターネット上から実行された PING に応答させる場合、プロバイダから付与される IP アドレスが「グローバル IP アドレス」である必要があります。
付与される IP アドレスが「プライベート IP アドレス」の場合は、インターネット上からアクセスする事はできませんのでご注意下さい。

Q.インターネット側から設定画面へログオンしたい。

A.「ファイアウォール」→「アクセス制御設定」を行って下さい。

詳しくは、「6-8.WAN 側から設定画面へアクセスする場合の設定方法」(111 ページ)を参照して下さい。

 確認

インターネット上から設定画面にアクセスする場合、プロバイダから付与される IP アドレスが「グローバル IP アドレス」である必要があります。
付与される IP アドレスが「プライベート IP アドレス」の場合は、インターネット上からアクセスする事はできませんのでご注意下さい。

 注意

「WAN 側から設定画面へのログオンを許可する」設定にする場合、必ずユーザー名、パスワードを変更して下さい。変更方法は「8-7.ログイン 設定」(135 ページ)を参照して下さい。

Q.無線 LAN セパレータ機能を設定したい。

A.無線 LAN 基本設定の「クライアント間 通信遮断」を有効にしてください。

詳しくは以下を参照してください。

- ・5GHz 無線 LAN 設定
→「4-1-1.基本 設定」(27 ページ)
- ・2.4GHz 無線 LAN 設定
→「4-2-1.基本 設定」(39 ページ)

	<p>無線 LAN1 (5GHz)と無線 LAN2 (2.4GHz)間の通信を遮断する場合は、無線 LAN1 (5GHz)と無線 LAN2 (2.4GHz)のマルチ SSID 設定画面の「マルチ SSID 間通信遮断」を有効に設定してください。 「マルチ SSID 間通信遮断」が無効の場合、5GHz(無線 LAN1)と 2.4GHz(無線 LAN2)間の通信は遮断されませんのでご注意ください。 「4-3-2.マルチ SSID の設定」(53 ページ)を参照してください。</p>
---	---

マルチ SSID のクライアント間通信遮断を行う場合は、マルチ SSID 設定内の「クライアント間 通信遮断」を有効にしてください。

詳しくは、「4-3.マルチ SSID 設定例」(51 ページ)を参照してください。

Q.ETH1 ポートが LAN ポートとして使用できない。

A.以下の各項目を確認してください。

■工場出荷設定の場合、ETH1 ポートは有線 WAN ポートとして動作しています。

ETH1 ポートを LAN ポートとして使用する場合は、以下の手順で設定を変更してください。

- ①「ネットワーク」→「WAN 設定」をクリックして、「WAN 回線運用」欄の[有線 WAN]ボタンをクリックして下さい。
- ②「接続モード」で「Bridge」を選択して[設定]ボタンをクリックして下さい。
- ③「WAN 設定」画面に戻りますので[設定保存]ボタンをクリックし、[今すぐ再起動]ボタンをクリックして下さい。

■回線冗長化設定で、有線 WAN 接続を組み合わせた設定を行っていませんか？

回線冗長化設定で、有線 WAN 接続を組み合わせた設定を行うと、ETH1 ポートは有線 WAN ポート固定動作となります。

Q.自動再起動(タイマー再起動)を設定したい。

A.「マネージメント」→「再起動」で設定して下さい。

詳しくは、「8-8-1.自動再起動(タイマー再起動)」(136 ページ)を参照して下さい。

Q.アクセス制御設定がマルチ SSID に反映されない。

A. アクセス制御設定は、プライマリ SSID にのみ適用されます。

プライマリ SSID 以外には適用されませんのでご注意ください。

Q.LTE ランプが点灯しない。

A.以下の各項目を確認して下さい。

- SIM カードが開通しているか確認して下さい。
SIM カードが使用できる状態になっているか、通信事業者にご確認下さい。
- SIM カードを正しく認識しているか確認して下さい。
ステータス画面で、電話番号、識別番号等が表示されているか確認して下さい。
「3-7.WAN 内蔵モバイル」(25 ページ)を参照して下さい。
電話番号や識別番号が正しく表示されていない場合は、SIM カードを抜き差しして下さい。
- WAN 側接続モードが「内蔵モバイル」になっている事を確認して下さい。
「5-2-9. WAN 設定: 共通設定」(82 ページ)を参照して下さい。
- 接続 ID、パスワード、APN、電話番号が正しく設定されているか確認して下さい。
「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。
- 内蔵通信モジュール用外部アンテナが正しく取り付けられているか確認して下さい。
「2-1.各機器との接続」(4 ページ)を参照して下さい。

Q.USB ランプが点灯しない。

A.以下の各項目を確認して下さい。

- USB モバイルデータカードを認識していません。
USB モバイルデータカードを一度取り外し、再度接続して下さい。
抜き差ししても認識しない場合は、本製品の電源を入れなおして下さい。
- WAN 側接続モードが「USB モバイル」になっている事を確認して下さい。
「5-2-9. WAN 設定: 共通設定」(82 ページ)を参照して下さい。
- 接続 ID、パスワード、APN、電話番号が正しく設定されているか確認して下さい。
「5-2-2.USB モバイル設定」(74 ページ)を参照して下さい。

Q.有線 LAN 接続でインターネットへ接続できない。

A.以下の各項目を確認して下さい。

- LAN ケーブルが正しく接続されているか確認して下さい。
本製品の ETH のリンクランプが点灯しているか確認して下さい。
点灯していない場合は、接触不良を起こしていないか、LAN ケーブルに異常がないか等、確認して下さい。
- 本製品の DHCP サーバー機能を使用している場合は、IP アドレスが正しく取得できているか確認して下さい。
以下の手順で確認して下さい。
(本製品の LAN 側 IP アドレス、及び DHCP サーバーの設定が工場出荷値の例です。)

■Windows 確認手順

1. コマンドプロンプトを起動して下さい。
2. 「ipconfig」(半角英文字)と入力して Enter キーを押して下さい。
3. 「IPv4 アドレス」欄に「192.168.0.2~192.168.0.30」(どれか 1 つ)が表示されているか、確認して下さい。

■Mac OS X 確認手順

1. [アップルメニュー]から[システム環境設定]を選択して下さい。
2. [ネットワーク]をダブルクリックして下さい。
3. [Ethernet]を選択して下さい。
4. [IP アドレス]欄に「192.168.0.2~192.168.0.30」(どれか 1 つ)が表示されているか、確認して下さい。

■内蔵通信モジュールを使用している場合、LTE ランプが点灯しているか確認して下さい。

LTE ランプが消灯・点滅している場合、回線接続が完了していません。

以下の各項目を確認して下さい。

- ・SIM カードが開通しているか確認して下さい。
SIM カードが使用できる状態になっているか、通信事業者にご確認下さい。
- ・SIM カードを正しく認識しているか確認して下さい。
ステータス画面で、電話番号、識別番号等が表示されているか確認して下さい。
「3-7.WAN 内蔵モバイル」(25 ページ)を参照して下さい。
電話番号や識別番号が正しく表示されていない場合は、SIM カードを抜き差しして下さい。
- ・WAN 側接続モードが「内蔵モバイル」になっている事を確認して下さい。
「5-2-9. WAN 設定: 共通設定」(82 ページ)を参照して下さい。
- ・接続 ID、パスワード、APN、電話番号が正しく設定されているか確認して下さい。
「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。
- ・内蔵通信モジュール用外部アンテナが正しく取り付けられているか確認して下さい。
「2-1.各機器との接続」(4 ページ)を参照して下さい。
- ・LTE/3G の電波状況が良好か確認して下さい。
電波強度はステータス画面「3-7.WAN 内蔵モバイル」(25 ページ)で確認する事ができます。
電波状況が悪い場合は、設置場所を変える等して下さい。

■USB モバイルデータカードを使用している場合、USB ランプが点灯しているか確認して下さい。

- ・USB ランプが消灯している場合
USB モバイルデータカードを一度取り外し、再度接続して下さい。
抜き差ししても認識しない場合は、本製品の電源を入れなおして下さい。
- ・USB ランプが点滅を繰り返している場合
USB モバイル設定が正しく行われているか確認して下さい。
「5-2-2.USB モバイル設定」(74 ページ)を参照して下さい。

■有線 WAN 接続でご利用の場合、WAN 側回線を ETH1ポートに接続しているか確認して下さい。

■有線 WAN(PPPoE)接続でご利用の場合、接続 ID、パスワードが正しいか確認して下さい。

Q.無線 LAN 接続でインターネットへ接続できない。

A. 以下の各項目を確認して下さい。

- 無線 LAN アダプターが正しくセットアップされているか確認して下さい。
パソコン側の無線 LAN アダプターが正しくセットアップされているか確認して下さい。
確認方法については、無線 LAN アダプターのマニュアル等を参照して下さい。
- 無線 LAN 環境を確認して下さい。
 - ・本製品と無線 LAN クライアントの距離を短くして下さい。
 - ・本製品と無線 LAN クライアントの間に障害物がある場合は、取り除いて下さい。
 - ・本製品の無線 LAN チャンネル番号を変更して下さい。
無線 LAN チャンネル番号の変更方法については以下を参照して下さい。
 - ・5GHz 無線 LAN 設定
→「4-1-1.基本 設定」(27 ページ)
 - ・2.4GHz 無線 LAN 設定
→「4-2-1.基本 設定」(39 ページ)
- 本製品と無線 LAN クライアントの無線 LAN セキュリティ設定が一致しているか確認して下さい。
本製品に設定されているセキュリティ設定が無線 LAN クライアント側と一致しているか確認して下さい。
セキュリティ設定については以下を参照して下さい。
 - ・5GHz 無線セキュリティ設定
→「4-1-3.セキュリティ 設定」(31 ページ)
 - ・2.4GHz 無線セキュリティ設定
→「4-2-3.セキュリティ 設定」(43 ページ)

〈次ページへ進んで下さい〉

- 本製品の DHCP サーバー機能を使用している場合は、IP アドレスが正しく取得できているか確認して下さい。
以下の手順で確認して下さい。
(本製品の LAN 側 IP アドレス、及び DHCP サーバーの設定が工場出荷値の例です。)

■Windows 確認手順

※Windows に管理者権限でログインした後、以下の作業を行って下さい。

- 1.コマンドプロンプトを起動して下さい。
- 2.「ipconfig」(半角英文字)と入力して Enter キーを押して下さい。
- 3.「IPv4 アドレス」欄に「192.168.0.2~192.168.0.254」(どれか 1 つ)が表示されているか、確認して下さい。

■Mac OS X 確認手順

- 1.[アップルメニュー]から[システム環境設定]を選択して下さい。
- 2.[ネットワーク]をダブルクリックして下さい。
- 3.[AirMac]を選択して下さい。
- 4.[TCP/IP]タブをクリックして下さい。
- 5.[IP アドレス]欄に「192.168.0.2~192.168.0.254」(どれか 1 つ)が表示されているか、確認して下さい。

- 内蔵通信モジュールを使用している場合、LTE ランプが点灯しているか確認して下さい。

LTE ランプが消灯・点滅している場合、回線接続が完了していません。

以下の各項目を確認して下さい。

- ・SIM カードが開通しているか確認して下さい。
SIM カードが使用できる状態になっているか、通信事業者にご確認下さい。
- ・SIM カードを正しく認識しているか確認して下さい。
ステータス画面で、電話番号、識別番号等が表示されているか確認して下さい。
「3-7.WAN 内蔵モバイル」(25 ページ)を参照して下さい。
電話番号や識別番号が正しく表示されていない場合は、SIM カードを抜き差しして下さい。
- ・WAN 側接続モードが「内蔵モバイル」になっている事を確認して下さい。
「5-2-9. WAN 設定: 共通設定」(82 ページ)を参照して下さい。
- ・接続 ID、パスワード、APN、電話番号が正しく設定されているか確認して下さい。
「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。
- ・内蔵通信モジュール用外部アンテナが正しく取り付けられているか確認して下さい。
「2-1.各機器との接続」(4 ページ)を参照して下さい。
- ・LTE/3G の電波状況が良好か確認して下さい。
電波強度はステータス画面「3-7.WAN 内蔵モバイル」(25 ページ)で確認する事ができます。
電波状況が悪い場合は、設置場所を変える等して下さい。

- USB モバイルデータカードを使用している場合、USB ランプが点灯しているか確認して下さい。

- ・USB ランプが消灯している場合
USB モバイルデータカードを一度取り外し、再度接続して下さい。
抜き差ししても認識しない場合は、本製品の電源を入れなおして下さい。
- ・USB ランプが点滅を繰り返している場合
USB モバイル設定が正しく行われているか確認して下さい。
「5-2-2.USB モバイル設定」(74 ページ)を参照して下さい。

- 有線 WAN 接続でご利用の場合、WAN 側回線を ETH1 ポートに接続しているか確認して下さい。

- 有線 WAN (PPPoE) 接続でご利用の場合、接続 ID、パスワードが正しいか確認して下さい。

Q.回線が切断される。

- A.モバイル回線の場合、通信中であっても一定時間でプロバイダ側から回線が切断されることがあります。

切断されるまでの時間はプロバイダにより異なりますので、詳細は契約プロバイダにお問い合わせ下さい。

Q.回線の接続・切断を繰り返す。

A.回線監視機能に誤った FQDN(ドメイン名)・IP アドレスを登録していませんか？

回線監視機能 に登録した全ての宛先への応答確認に連続して失敗すると、回線の接続・切断。再起動を繰り返します。登録した FQDN・IP アドレスに誤りがないか確認して下さい。
回線監視機能については「5-2-9. WAN 設定:共通設定」(82 ページ)を参照して下さい。

Q.回線冗長化機能が動作しない。

A.回線監視機能が有効になっているか確認して下さい。

回線冗長化機能を使用するためには、回線監視機能を有効にする必要があります。
回線監視機能については「5-2-9. WAN 設定:共通設定」(82 ページ)を参照して下さい。

Q.回線冗長化機能でセカンダリー接続に切り替わった後プライマリー接続に戻らない。

A.以下の各項目を確認して下さい。

- コールド・スタンバイ方式の場合、プライマリー通信確認間隔の設定を確認して下さい。
プライマリー通信確認間隔が「0」で設定されていると、MR-GM5A を再起動するまでプライマリー接続には戻りません。
プライマリー通信確認間隔設定については「5-2-9. WAN 設定:共通設定」(82 ページ)を参照して下さい。
- ホット・スタンバイ方式の場合、MR-GM5A を再起動するまでプライマリー接続には戻りません。
MR-GM5A を再起動して下さい。

Q.インターネットに接続できるが、速度が遅い。

A.以下の各項目を確認して下さい。

- 回線事業者側で速度制限をしていないか確認して下さい。
モバイル通信をご利用の場合、回線事業者側で速度制限をしている場合があります。
速度制限については、ご契約の回線事業者にお問い合わせ下さい。
- 内蔵通信モジュール用外部アンテナが正しく取り付けられているか確認して下さい。
「2-1.各機器との接続」(4 ページ)を参照して下さい。
- ファイアウォール/セキュリティ対策ソフトウェア等が起動・常駐していませんか？
インターネット通信を常時監視するソフトウェアが起動・常駐している場合、いったん停止(終了)した後、再度確認して下さい。詳しくはソフトウェアのマニュアルを参照して下さい。

Q.本体 IP アドレスを変更した後、設定画面へログオンできなくなった。

A.以下の各項目を確認して下さい。

- パソコンの IP アドレスを自動取得で設定している場合、IP アドレスの開放/再取得を行って下さい。
以下の方法で IP アドレスの開放/再取得を行って下さい。
 - Windows の例
※Windows に管理者権限でログインした後、以下の作業を行って下さい。
 - 1) コマンドプロンプトを起動して下さい。
 - 2) 「ipconfig /release」と入力して[Enter]キーを押して下さい。
 - 3) 「IPv4 アドレス」欄が「0.0.0.0」になります。
 - 4) 「ipconfig /renew」と入力して[Enter]キーを押して下さい。
 - 5) 「IPv4 アドレス」欄に正しい IP アドレスが表示されているか確認して下さい。
- パソコンの IP アドレスを固定で設定している場合、本製品と同じネットワークに設定されているか確認して下さい。
- WWW ブラウザのアドレス欄に変更後の IP アドレスを正しく入力しているか確認して下さい。

Q.WAN 側から設定画面が開けない。

A.以下の各項目を確認して下さい。

■アクセス制御設定が正しく行われているか確認して下さい。

「6-6.アクセス制御 設定」(108 ページ)を参照して下さい。

■アタック検出設定を確認して下さい。

アタック検出の値が少なすぎないか確認して下さい。(推奨 30 以上)

アタック検出の設定については「6-6.アクセス制御 設定」(108 ページ)を参照して下さい。

■「ポートフォワーディング設定」、「DMZ ホスト設定」を確認して下さい。

「ポートフォワーディング設定」、「DMZ ホスト設定」を確認して下さい。

「6-5.ポートフォワーディング 設定」(105 ページ)

「6-7.DMZ 設定」(110 ページ)

ポートフォワーディング設定の宛先ポート番号に設定画面へのアクセスポート番号と同じ番号を登録する、もしくは DMZ ホスト機能を有効にすると、これらの機能が優先され、「WAN 側から設定画面へログオンする」設定は無効になります。

■プロバイダから付与される IP アドレスがグローバル IP アドレスか確認して下さい。

インターネット上から設定画面にアクセスする場合、プロバイダから付与される IP アドレスが「グローバル IP アドレス」である必要があります。付与される IP アドレスが「プライベート IP アドレス」の場合は、インターネット上からアクセスする事はできませんのでご注意下さい。

付与される IP アドレスが「グローバル IP アドレス」かどうかは、ご利用のプロバイダに確認して下さい。

Q.WAN 側からの Ping に応答しない。

A.以下の各項目を確認して下さい。

■アクセス制御設定が正しく行われているか確認して下さい。

「6-6.アクセス制御 設定」(108 ページ)を参照して下さい。

■「ポートフォワーディング設定」、「DMZ ホスト設定」を確認して下さい。

「ポートフォワーディング設定」、「DMZ ホスト設定」を確認して下さい。

「6-5.ポートフォワーディング 設定」(105 ページ)

「6-7.DMZ 設定」(110 ページ)

ポートフォワーディング設定に ICMP を登録する、もしくは DMZ ホスト機能を有効にすると、これらの機能が優先され、「WAN 側からの Ping に応答を返す」設定は無効になります。

■プロバイダから付与される IP アドレスがグローバル IP アドレスか確認して下さい。

インターネット上から実行された PING に応答させる場合、プロバイダから付与される IP アドレスが「グローバル IP アドレス」である必要があります。付与される IP アドレスが「プライベート IP アドレス」の場合は、インターネット上からアクセスする事はできませんのでご注意下さい。

付与される IP アドレスが「グローバル IP アドレス」かどうかは、ご利用のプロバイダに確認して下さい。

Q.プロバイダから自動取得した IP アドレスを知りたい。

A.設定画面トップの「現在の動作状況」で確認することができます。

設定画面トップの「ステータス」画面の「WAN 内蔵モバイル構成」欄の「IP アドレス」で確認することができます。

詳しくは「3-7.WAN 内蔵モバイル」(25 ページ)を参照して下さい。

Q.UPnP 対応ソフトウェアが動作しない。

A.本製品は UPnP 機能に対応していません。

Q.固定 IP アドレス付与機能が動作しない。

A.以下の各項目を確認して下さい。

■固定 IP アドレス付与機能が有効になっているか確認して下さい。

LAN 設定画面の DHCP サーバー 固定 IP アドレス付与設定が「有効」になっているか確認して下さい。
「5-1-2.DHCP サーバー設定」(69 ページ)を参照して下さい。

■固定付与する IP アドレスが DHCP サーバーの付与範囲に含まれている事を確認して下さい。

固定付与する IP アドレスは、MR-GM5A の DHCP サーバー機能が付与する範囲に含まれている必要があります。
「5-1-2.DHCP サーバー設定」(69 ページ)を参照して下さい。

■DHCP サーバー 固定 IP アドレス付与リストに登録した MAC アドレスが正しいか確認して下さい。

イーサネットアダプターのマニュアル等を参照し、登録した MAC アドレスに間違いがないか確認して下さい。

Q.メール送信機能で送信したメールが受信できない。

A.NTP クライアント機能が有効になっているか確認して下さい。

MR-GM5A の内部日時が実際の時間と大きく食い違っている場合、メールサーバー側に不正なメールとして拒否される事があります。

■内蔵通信モジュールを使用している場合

→「ネットワーク設定」→「WAN 設定」→「内蔵モバイル」を開き、「内蔵モジュールから時刻取得を行う」にチェックが入っているか確認して下さい。
詳しくは「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。

■「NTP クライアント機能」を使用している場合

→「時刻情報・設定」画面を開き「現在時刻」が正しいか確認して下さい。
詳しくは「8-2.時刻情報 設定」(123 ページ)を参照して下さい。

Q.スケジュールによる自動再起動が動作しない。

A.スケジュールによる自動再起動は、NTPクライアント機能で時刻取得に成功した場合に動作します。

■内蔵通信モジュールを使用している場合

→「ネットワーク設定」→「WAN 設定」→「内蔵モバイル」を開き、「内蔵モジュールから時刻取得を行う」にチェックが入っているか確認して下さい。
詳しくは「5-2-1.内蔵モバイル設定」(72 ページ)を参照して下さい。

■「NTP クライアント機能」を使用している場合

→「時刻情報・設定」画面を開き「現在時刻」が正しいか確認して下さい。
詳しくは「8-2.時刻情報 設定」(123 ページ)を参照して下さい。

Q.ファームウェアバージョンや MAC アドレスを知りたい。

A.設定画面トップの「ステータス」画面で確認することができます。

詳しくは「3.ステータス画面」(19 ページ)を参照して下さい。

Q.設定を工場出荷値に戻したい。

A.以下の手順で設定を初期化して下さい。

- 1) 本製品の電源を入れて下さい。
- 2) 電源投入から本製品が起動するまで 1 分程度お待ち下さい。
- 3) 本体背面の INIT ボタンを **8 秒以上**押し続けて下さい。
- 4) 8 秒以上たったら INIT ボタンを放して下さい。
- 5) 再起動が完了すると設定が初期化されます。

11.ユーザーサポート

ユーザーサポートについて

	お問い合わせ頂く前に、サポート規定をご確認下さい。 MRL 製品サポート規定 https://www.MRL.co.jp/supports/support-policy/
---	---

本製品のユーザーサポートは以下で行っています。

株式会社マイクロリサーチ ユーザーサポートセンター

■サポート直通電話番号：03-3458-9031

土日、祝日、年末年始を除く 10:00～12:00、13:00～17:00

■お問い合わせフォーム

<https://www.MRL.co.jp/contact/support-inquiry/>

■インターネットホームページ

URL： <https://www.MRL.co.jp> (トップページ)

当社からのお知らせ、最新情報の提供を行っています。本製品のファームウェア等、こちらで提供しています。

お問い合わせ頂く際のお願い

お問い合わせ頂く際は、以下の各項目についてあらかじめご確認(メモ等)して頂くことで、よりスムーズなサポートを受けることが出来ます。

- ◆お名前
- ◆製品名(型番)
- ◆ファームウェアバージョン
- ◆接続されているパソコン等の台数
- ◆使用しているイーサネットボードのメーカー名・型番
- ◆使用しているパソコンの OS 及びバージョン
- ◆使用している SIM カードのキャリア名やご契約プラン名、接続 ID、パスワード、APN 等の接続情報
- ◆使用している USB モバイルデータカードのメーカー名・型番
- ◆具体的な症状(エラーメッセージ等も含め、できる限り詳細に。)
- ◆ご住所/電話番号・FAX 番号
- ◆製造番号
- ◆設定内容
- ◆使用しているパソコン等のメーカー名・型番

	お問い合わせ頂く前に、Q&A 集 の内容を確認して下さい。
---	-------------------------------

本製品の修理について

	修理をご依頼頂く前に、修理規定をご確認下さい。 MRL 製品修理規定 https://www.MRL.co.jp/supports/repair-policy/
---	---

本製品が故障してしまった場合、以下の項目をご確認のうえ、弊社修理センターへ送付して下さい。

(修理品送付に伴う送料は、送り主負担とさせていただきます。)

- 修理品には必ず、使用環境、故障状況等を詳しくお書き添え下さい。
- 修理期間中の代替機のお貸し出しは行っておりませんので、あらかじめご了承下さい。
- 修理品の設定内容は動作確認のため初期化されますので、あらかじめご了承下さい。
- 保証期間中は無償で修理を行います。
ただし、以下の場合には有償修理となりますのでご了承下さい。
 - ◆保証書が同梱されていない場合。
 - ◆保証書の所定事項が未記入の場合。
 - ◆誤った操作等により発生した故障や破損の場合。
 - ◆落雷、火災等の事故により発生した故障や破損の場合。

	分解・改造が行われた製品については、一切のサポートおよび修理サービスをお断りさせていただきます。
---	--

- 修理品の送付先は以下の通りです。

株式会社マイクロリサーチ 修理センター

〒140-0004 東京都品川区南品川 2-2-10 南品川 Nビル 2F

株式会社マイクロリサーチ