

プロフェッショナル
モード
コンフィグー覧

・プロフェッショナルモードコンフィグー覧 目次

プロフェッショナルモードについて	P.3
設定ファイルの編集	P.6
1 ネットワーク設定	P.8
1-1 WAN設定	
1-2 有線LAN設定	
1-3 無線LAN設定	
1-4 ブリッジ設定/ルーティング設定/TCPMSS設定	
1-5 VPN設定	
1-6 リモートアクセス設定	
1-7 VLAN設定/インバウンドポリシー設定	
2 フィルタリング設定	P.15
2-1 グループ設定	
2-2 IP/URLフィルタリング設定	
2-3 HTTPSフィルタリング設定	
2-4 メールフィルタリング設定	
2-5 カテゴリ別URLフィルタリング設定	
3 WANモード切り替え/LTEモード設定(MRB-50L専用)	P.22
3-1 WANモード切り替え設定/LTEモード設定	
プロフェッショナルモード補足	P.24
リモートアクセス設定について	
VPN設定について	

プロフェッショナル モードについて

プロフェッショナルモードでの設定について

2-2 設定ファイルの編集

- ・プロフェッショナルモードでは、設定ファイルを編集、インポートすることでMRBの本体設定を一括で行うことが可能です。『設定ファイルの編集』では、設定ファイルの編集方法を説明します。

※設定を間違えると機会が動作しなくなる恐れがありますので、プロフェッショナルモードでの設定の際はバックアップの取得をお願い致します。なお、設定ミスによる動作不良の責任は負いかねますのでご了承ください。

2-3 ネットワーク設定

- ・『ネットワーク設定』では、ネットワークに関する設定について以下の項目の設定例を紹介します。

- ・WAN設定
- ・有線LAN設定
- ・無線LAN設定(MRB-50/MRB-50Lのみ対応)
- ・ブリッジ/ルーティング/TCPMSS設定
- ・VPN設定

2-4 フィルタリング設定

- ・『フィルタリング設定』では、フィルタリングに関する設定について以下の項目の設定例を紹介します。

- ・フィルタリンググループ設定
- ・IP/URLフィルタリング設定
- ・メール/HTTPSフィルタリング設定

2-5 プロフェッショナルモード固有の設定

・『プロフェッショナルモード固有の設定』では、WebUIからは編集ができない設定について以下の項目の設定例を紹介します。

- ・ リモートアクセス設定
- ・ URLカテゴリフィルタリング設定

※VPN設定、リモートアクセス設定については『3,プロフェッショナルモード設定補足』をお読み頂き、詳細な説明を合わせてご確認ください。

※未設定の項目に関しては、エクスポートした設定ファイルには記述されませんので、編集の際は項目ごと追記をお願いします。

設定ファイルの編集

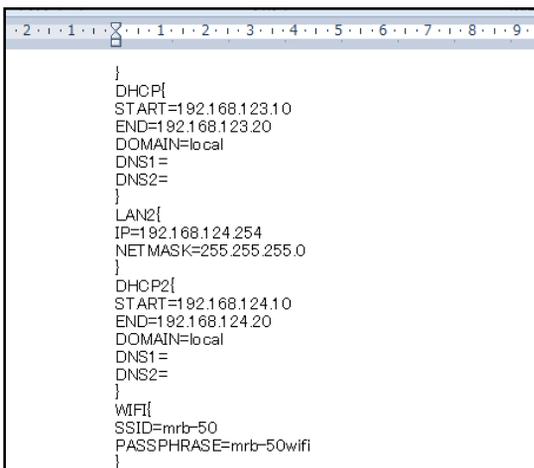
本体設定の一括変更のため、予めダウンロードした設定ファイルを編集します。



①“1,本体設定のバックアップ”でダウンロードしたファイルを右クリックし、“プログラムから開く”→“規定のプログラムの選択”をクリックします。



②プログラムの一覧より“ワードパッド”を選択し、『OK』をクリックします。



③次ページからの設定記入例に従いコンフィグの編集を行ってください。

※テキスト最上部に表示されている
CODE{
TRT=XXXXXX
}
の編集は行わないでください。
MRBが正しく機能しなくなる恐れがあります。

ネットワーク設定

WAN側のネットワーク設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

設定項目	記入例	備考
WAN設定 (PPPoE)	<pre>WAN{ PROTOCOL=PPPoE ID=xxxx@xxx PASS=zzzzzz IP= NETMASK= GATEWAY= DNS1= DNS2= }</pre>	<pre>"PROTOCOL=" : "PPPoE" "ID=" : ID "PASS=" : パスワード その他の部分は空白にする。</pre>
WAN設定 (DHCP)	<pre>WAN{ PROTOCOL=DHCP ID= PASS= IP= NETMASK= GATEWAY= DNS1= DNS2= }</pre>	<pre>"PROTOCOL=" : "DHCP" その他の部分は空白にする。</pre>
WAN設定 (固定IP)	<pre>WAN{ PROTOCOL=Fix ID= PASS= IP=192.168.111.111 NETMASK=255.255.255.0 GATEWAY=192.168.111.1 DNS1=192.168.111.1 DNS2= }</pre>	<pre>"PROTOCOL=" : "Fix" "IP=" : WAN側IPアドレス "NETMASK=" : ネットマスク "GATEWAY=" : ゲートウェイ "DNS1=" : プライマリDNS "DNS2=" : セカンダリDNS その他の部分は空白にする。</pre>

有線LANのネットワーク設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
有線LAN設定	LAN2{ CONFIG=ON/OFF IP=192.168.124.254 NETMASK=255.255.255.0 }	”CONFIG=”：使用する場合は”ON” ”IP=”：LAN側IPアドレス情報 ”NETMASK=”：サブネットマスク
有線DHCP設定	DHCP2{ CONFIG=ON/OFF START=192.168.124.10 END=192.168.124.100 DOMAIN=local DNS1= DNS2= }	”CONFIG=”：使用する場合は”ON” ”START=”：DHCP先頭IP ”END=”：DHCP終端IP
DHCP固定設定 (クライアントの固定IPの指定を指定する。DHCPの範囲内は割り当てないこと。)	DHCP_FIXED{ a06dec9e44e7e3ba10d5b22da8ba94c9 00:23:5A:D7:09:05 192.168.124.11 trtclient001 }	・ハッシュ値 ・クライアントのMacアドレス ・指定するIPアドレス ・任意のクライアント名の順に1行に記載。 複数設定の際は改行して同様に記載。

無線LANのネットワーク設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

※無線LAN設定はMRB-50/MRB-50Lのみの設定項目です。

設定項目	記入例	備考
無線LAN設定	LAN{ CONFIG=ON/OFF IP=192.168.123.254 NETMASK=255.255.255.0 }	”CONFIG=”：使用する場合は”ON” ”IP=”：LAN側IPアドレス情報 ”NETMASK=”：サブネットマスク
無線DHCP設定	DHCP{ CONFIG=ON/OFF START=192.168.123.10 END=192.168.123.100 DOMAIN=local DNS1= DNS2= }	”CONFIG=”：使用する場合は”ON” ”START=”：DHCP先頭IP ”END=”：DHCP終端IP
DHCP固定設定 (クライアントの固定IPの指定を指定する。DHCPの範囲内は割り当てないこと。)	DHCP_FIXED{ a06dec9e44e7e3ba10d5b22da8ba94c9 00:23:5A:D7:09:05 192.168.124.11 trtclient001 }	・ハッシュ値 ・クライアントのMacアドレス ・指定するIPアドレス ・任意のクライアント名の順に1行に記載。 複数設定の際は改行して同様に記載。
Wi-fi設定	WIFI{ SSID=mrb-50 PASSPHRASE=mrb-50wifi STEALTH=0 WIFIPROTOCOL=3 CHANNEL=40 }	”SSID=”：SSID ”PASSPHRASE=”：パスワード ”STEALTH=”：“1”なら非公開SSID “0”なら公開SSID ”WIFIPROTOCOL=”：“1”なら802.11b “2”なら802.11g “3”なら802.11n ”CHANNEL=”：802.11b/gの場合 1~13 802.11nの場合 40~64(8刻み)

ブリッジ/ルーティング/TCPMSSの設定は以下の例に従って記載してください。赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
ブリッジ	BRIDGE{ }	ブリッジ利用の際は記入例そのままにコンフィグに記載。
ブリッジ時の管理IP	BRIDGE_MANAGE_IP{ CONFIG=ON/OFF IP=111.111.111.11 NETMASK=255.255.0.0 }	"CONFIG="：利用する場合は"ON" "IP="：メンテナンスアドレス "NETMASK="：サブネットマスク
ブリッジ時の通過許可IP	BRIDGE_ALLOW_IP{ 7f9e89bf7b515974b75bd1e2e4c79972 192.168.11.1 32 }	・ハッシュ値 ・通過許可IPアドレス ・ネットマスク長の順に1行に記載。 複数設定の際は改行して同様に記載。
静的ルーティング設定	ROUTE{ 2b49b928fc4199b8101614b9cd62ad1 192.168.22.0 255.255.0.0 192.168.11.1 }	・ハッシュ値 ・ルートIP ・サブネットマスク ・ゲートウェイの順に1行に記載。 複数設定の際は改行して同様に記載。
TCPMSS設定	TCPMSS{ 1414 }	フレッツADSL,ひかり電話利用環境の場合は1414、フレッツ光プレミアムの場合は1398と記載。 (デフォルト値は1500)

VPNの設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
VPN設定(応答側)	VPN{ 08a68eec37af94301db96679e95673ca 1 1 2 mr-5 test 0 * 192.168.112.0 1 }	<ul style="list-style-type: none"> ・ハッシュ値 ・VPN番号 ・設定有効：1 / 設定無効：2 ・開始側：1 / 応答側：2 ・事前共通鍵 ・応答側：リモートID 開始側：相手側固定IP ・応答側：0 固定IPでのVPN：1 IDでのVPN：2
VPN設定(開始側)	VPN{ 2eb84e83830b72c05d3b12dfd05ced16 1 1 1 mr-5 61.51.41.31 2 test 192.168.11.0 1 }	<ul style="list-style-type: none"> ・応答側：* 固定IPでのVPN1：開始側固定IP IDでのVPN2：リモートID ・相手側LANアドレス ・UDPカプセル化ON：1/OFF：0 <p>の順に1行に記載。</p>
VPNネットワーク 設定	VPN_NET{ b0abb130d1f685921d7bd770e834de81 1 10.10.1.0 16 }	<ul style="list-style-type: none"> ・ハッシュ値 ・VPN番号 ・IPアドレス ・ネットマスク <p>の順に1行に記載。 複数設定の際は改行して同様に記載。 VPN番号はVPN設定に対応させる。</p>

※UDPカプセル化とは...
NAPTを経由してVPN通信を行う際にNAPTによる宛先変換を可能にするための機能です

リモートアクセス受信の設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

設定項目	記入例	備考
リモートアクセス	<pre>REMOTE_ACCESS{ CONFIG=ON IP=172.23.0.1 CLIENT_RANGE=172.23.0.10-172.23.0.20 DNS=8.8.8.8 DNS=8.8.4.4 PSK=psktrtsecret1 USER=user1 trtpass11 USER=user2 trtpass22 }</pre>	<p>”CONFIG=”：使用する場合は”ON”</p> <p>”IP=”：リモートアクセス用IP</p> <p>”CLIENT_RANGE=”：DHCP範囲</p> <p>”DNS=”：DNSサーバ (上がプライマリ、下がセカンダリ)</p> <p>”PSK=”：事前共有鍵</p> <p>”USER=”：利用ユーザ (前半がID、後半がパスワード)</p> <p>ユーザを複数登録する際は改行して同様に記載。</p>

※設定の際は”補足：リモートアクセス設定について”をご確認ください。

VLAN/インバウンドポリシーの設定は以下の例に従って記載してください。赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
VLAN	<pre>VLAN2{ 1 10 192.168.1.0 24 1 20 172.16.0.0 16 }</pre>	<ul style="list-style-type: none"> ・ 1 ・ VLAN番号 ・ ネットワークアドレス ・ ネットマスク の順に1行に記載。 複数設定の際は改行して同様に記載。
インバウンド ポリシー	<pre>ALLOW_INBOUND{ 12ce235094606eef87cd8c8d75e8c5b3 0.0.0.0/0 0.0.0.0/0 PING 44efe78ca2167357d15f7faf2bfceba4 1.1.1.1/32 1.1.1.1/32 TCP 1-65535 233d37de5b76802fa5a0a24d0e9286ef 192.168.0.0/16 192.168.2.0/24 ANY d5a9e9db4748b743d6c4ead082d9bd1f 3.3.3.3/32 3.3.3.3/32 ICMP dee4aaa62dbb1fdaea563cd060509ab7 4.4.4.4/32 44.4.4.4/32 UDP 3 }</pre>	<ul style="list-style-type: none"> ・ ハッシュ値 ・ 接続元IPアドレス/ネットマスク ・ 接続先IPアドレス/ネットマスク ・ プロトコル (TCP,UDP,PING,ICMP,ANY) ・ ポート番号(TCP,UDPのみ) の順に1行に記載。 複数設定の際は改行して同様に記載。

フィルタリング設定

フィルタリンググループの設定は以下の例に従って入力してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
グループ設定 (グループ名の変更)	<pre>GROUP{ 1 ec9ec38870b67838b0d095f9c1521539 GROUP1 0 2 6c78d5207b9074eac13ec7edc8c847f2 GROUP2 0 3 130fe12eb38db8784a4899a74e4960bd GROUP3 0 }</pre>	<ul style="list-style-type: none"> ・グループ番号(デフォルトグループは100) ・ハッシュ値 ・グループ名 ・0 <p>の順に1行に記載。 複数設定の際は改行して同様に記載。</p>
グループポリシー (グループへのIP割当)	<pre>GROUP_POLICY{ 1 178b2e3785fd38171b8fde6f2f4659fe 1 192.168.124.11 32 * 0 0 1 66c45c1b122713087e85f60549a0f14d 2 192.168.124.100 32 192.168.124.110 0 0 }</pre>	<ul style="list-style-type: none"> ・グループ番号 ・ハッシュ値 ・単一指定：1 / 範囲指定2 ・IPアドレス(範囲指定なら先頭IP) ・ネットマスク長 ・単一指定：* ・範囲指定：終端IPアドレス ・“0”2つ <p>の順に1行に記載。 複数設定の際は改行して同様に記載。</p>

IP/URLフィルタリング設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
URLフィルタの レベル設定	URL_LEVEL_9{ 2 }	末尾の数字で設定するグループを指定。 (デフォルトグループは100) 記載する数字は 高：1 中：2 低：3 なし：9 に対応。
IPフィルタの レベル設定	IP_LEVEL_9{ 2 }	
振る舞いフィルタ のレベル設定	BEHAVIOR_LEVEL_9{ 2 }	
URLフィルタの ホワイトリスト	URL_WHITE_9{ f15d461b1a1dc80efa85f7c6aa1f865b 0 www.example.co.jp 29252e6919566f4d5156a59fb0d9b5cb 0 example.org }	末尾の数字で設定するグループを指定。 (デフォルトグループは100) ・ハッシュ値 ・0 ・URL の順に1行に記載。 複数設定の際は改行して同様に記載。 URLは正規表現による記載が可能。
URLフィルタの ブラックリスト	URL_BLACK_9{ f15d461b1a1dc80efa85f7c6aa1f865b 0 www.example.co.jp f686fab203c770588504a557f77109ee 0 www.example.com }	
IPフィルタの ホワイトリスト	IP_WHITE_9{ f15d461b1a1dc80efa85f7c6aa1f865b 123.123.123.123 32 f686fab203c770588504a557f77109ee 222.111.111.222 32 }	末尾の数字で設定するグループを指定。 (デフォルトグループは100) ・ハッシュ値 ・IPアドレス ・ネットマスク の順に1行に記載。 複数設定の際は改行して同様に記載。
IPフィルタの ブラックリスト	IP_BLACK_9{ f15d461b1a1dc80efa85f7c6aa1f865b 123.123.123.123 32 f686fab203c770588504a557f77109ee 222.111.111.222 32 }	

HTTPS検知設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
https通信検知	HTTPS_9{ HTTPS=ON / OFF }	末尾の数字で設定するグループを指定。(デフォルトグループは100) "HTTPS="：利用する場合は"ON"
https通信のURL ホワイトリストの 設定	URL_HTTPS_9{ ea0ea7696d6d44dd79e31a33bd112585 0 www.aaa.com }	末尾の数字で設定するグループを指定。(デフォルトグループは100) ・ハッシュ値 ・0 ・URL の順に1行に記載。 複数設定の際は改行して同様に記載。
https通信のIP ホワイトリストの 設定	IP_HTTPS_9{ ca87c597a0e1488b3c0e721db0303fae 11.22.33.44 32 }	末尾の数字で設定するグループを指定。(デフォルトグループは100) ・ハッシュ値 ・IPアドレス ・ネットマスク の順に1行に記載。 複数設定の際は改行して同様に記載。

メール検知設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

設定項目	記入例	備考
メール検知機能	<pre>MAIL_9{ MAIL=ON/OFF SPAM=ON/OFF VIRUS=ON/OFF SSL=ON/OFF SUBJECT=-SPAM- SUBJECTVIRUS=-VIRUS- }</pre>	<p>末尾の数字で設定するグループを指定。(デフォルトグループは100)</p> <p>”MAIL=”：利用する場合は”ON”</p> <p>”SPAM=”：利用する場合は”ON”</p> <p>”VIRUS=”：利用する場合は”ON”</p> <p>”SUBJECT=”：スパム判定時メールタイトルに表示される文言</p> <p>”SUBJECTVIRUS=”：ウイルス判定時メールタイトルに表示される文言 (スパムとウイルスを同時に検知した際は、ウイルス判定の文言が優先)</p>
mail black/white リスト追加	<pre>MAIL_WHITE_9{ 11d5c032a95612ed6e7c4b1f34f83af2 0 white1@test.com 22d5c032a95612ed6e7c4b1f34f83af2 0 white1@test.com } MAIL_BLACK_9{ 88d5c032a95612ed6e7c4b1f34f83af2 0 black1@test.com 25d5c032a95612ed6e7c4b1f34f83af2 0 black2@test.com }</pre>	<p>末尾の数字で設定するグループを指定。(デフォルトグループは100)</p> <ul style="list-style-type: none"> ・ハッシュ値 ・0 ・メールアドレス <p>の順に1行に記載。 複数設定の際は改行して同様に記載。</p>

URLフィルタリングのカテゴリ指定設定は以下の例に従って入力してください。
赤字部分を編集することで設定の変更が可能です。

設定項目	記入例	備考
URLフィルタのカテゴリ指定	URL_DENY_CAT_10{ 1 2 3 }	末尾の数字でフィルタグループを指定。(数字は10~99から選択) 禁止したいカテゴリナンバーを1行あたり1つずつ記載。
URLフィルタのレベル設定	URL_LEVEL_9{ 10 }	末尾の数字で設定するグループを指定。(デフォルトグループは100) カテゴリフィルタに対応する10~99の数字を記載。

上記2つの項目をコンフィグに記載した場合、
グループ9のURLフィルタリングはカテゴリ1,2,3にのみ対応する。
といった設定が行われます。

※数字とカテゴリの対応一覧は次ページにあります

URLカテゴリフィルタリングのカテゴリ一覧表です。
プロフェッショナルモードより編集を行う際にご確認ください。

1 不動産	43 水着/下着
2 コンピュータセキュリティ情報	44 不審なサイト
3 金融	45 子供向け
4 ビジネス/経済	46 憎悪/人種差別
5 コンピュータ一般技術情報	47 オンラインストレージ
6 オークション	48 暴力/乱暴
7 ショッピング	49 キーロガー/モニタツール
8 カルト/オカルト	50 検索エンジン
9 旅行/観光	51 インターネットポータル
10 危険ドラッグ/麻薬	52 Web広告
11 アダルト/ポルノ	53 不正行為
12 日用雑貨	54 グロテスク
13 軍事	55 Webメール
14 SNS	56 マルウェアサイト
15 デッドサイト	57 フィッシング詐欺
16 株式/投資	58 プロキシ/匿名プロキシ
17 教育/訓練	59 スパイウェア/アドウェア
18 出会い系	60 音楽
19 性教育	61 政府
20 宗教	62 ヌード
21 娯楽/芸術	63 ニュースメディア
22 個人サイト/ブログ	64 非合法/違法
23 法律	65 コンテンツ配信
24 地元情報	66 インターネット通信
25 ストリーミング	67 ボットネット
26 仕事検索	68 妊娠中絶
27 ギャンブル	69 健康と医療
28 翻訳	70 スпамソース
29 参考文献/学術調査	71 スпамURL
30 シェアウェア/フリーウェア	72 スпамソースが疑われるサイト
31 P2P	73 公開プロキシ
32 マリファナ	74 動的コンテンツ
33 ハッキング	75 パークドメイン
34 ゲーム	76 酒/煙草
35 哲学/政治的支援	77 プライベートIP
36 武器	78 画像/動画検索
37 有料サイト	79 ファッション/美容
38 狩り/釣り	80 レクリエーション/趣味
39 社会/団体	81 自動車/バイク
40 教育	82 Webホスティング
41 グリーティングカード	83 食べ物
42 スポーツ	

※2017/9/6時点での一覧となります。

WANモード切替/LTE設定 定 (MRB-50L専用設定)

WANモード設定/LTE設定は以下の例に従って記載してください。
赤字部分を編集することで設定の変更が可能です。

※MRB-50L固有の設定です。他の機械では適用できません。

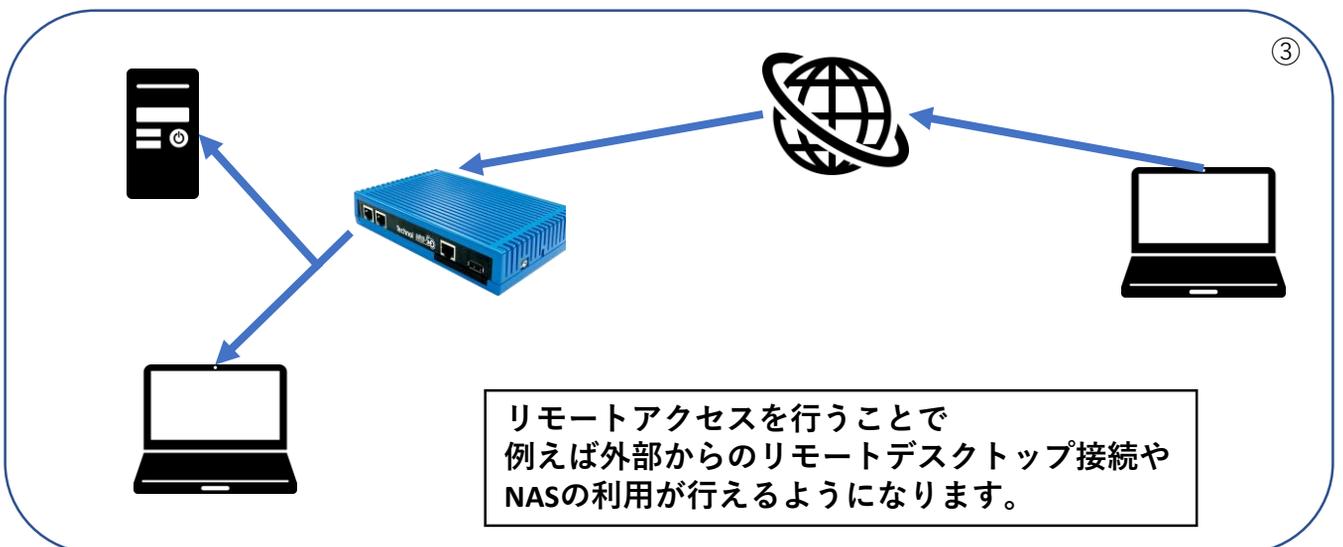
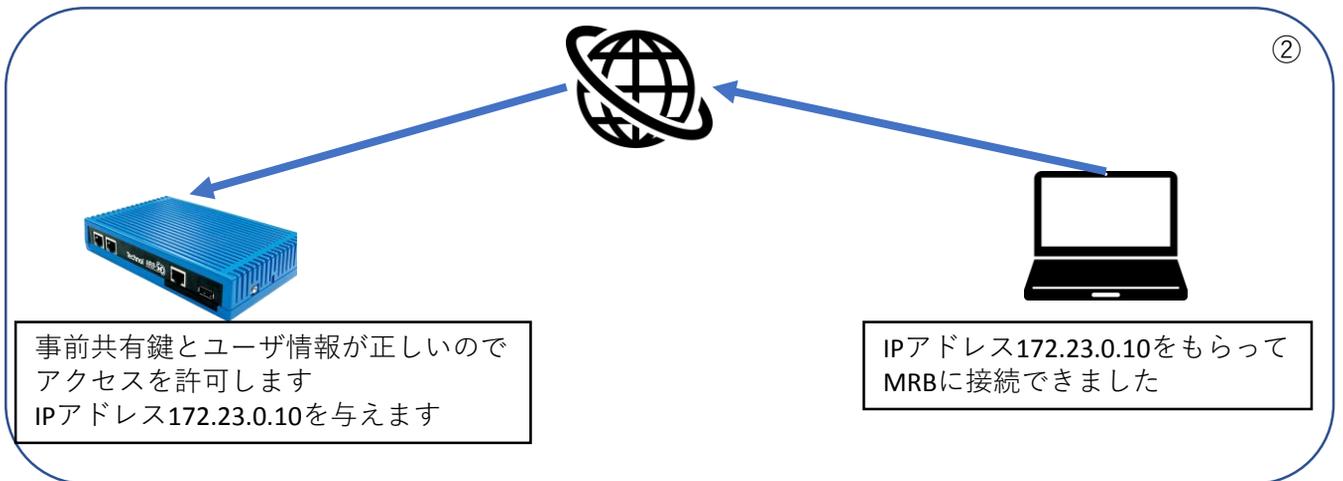
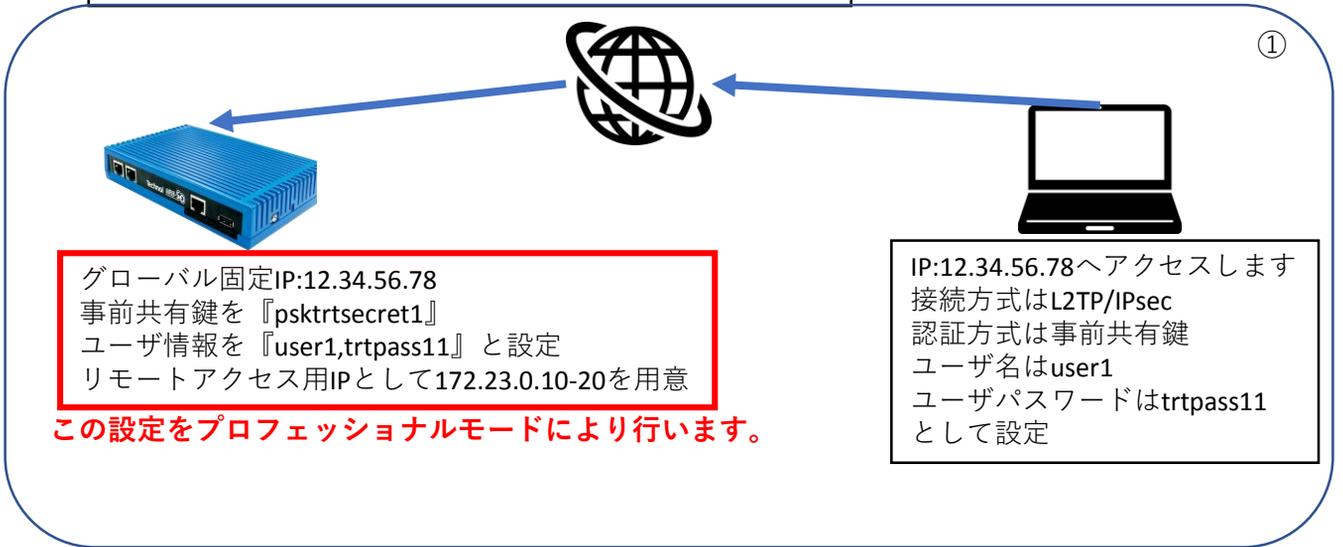
設定項目	記入例	備考
WANモード設定 (有線回線/ LTE回線)	WAN_USE{ 1 }	WAN側使用回線を指定。 記載する数字は 有線回線：1 LTE回線：2 に対応。
LTE設定	LTE{ APN=technol.com ID=example@technol.com PASS=password IP= GATEWAY= DNS1= DNS2= CARRIER=0 }	“APN=”：APN “ID=”：ID “PASS=”：パスワード “CARRIER=”：“0”なら自動 “1”ならDocomo “2”ならAU(mineo) “3”ならAU(UQmobile) “4”ならSoftBank その他の部分は指定がなければ空白にする。

プロフェッショナル モード設定補足

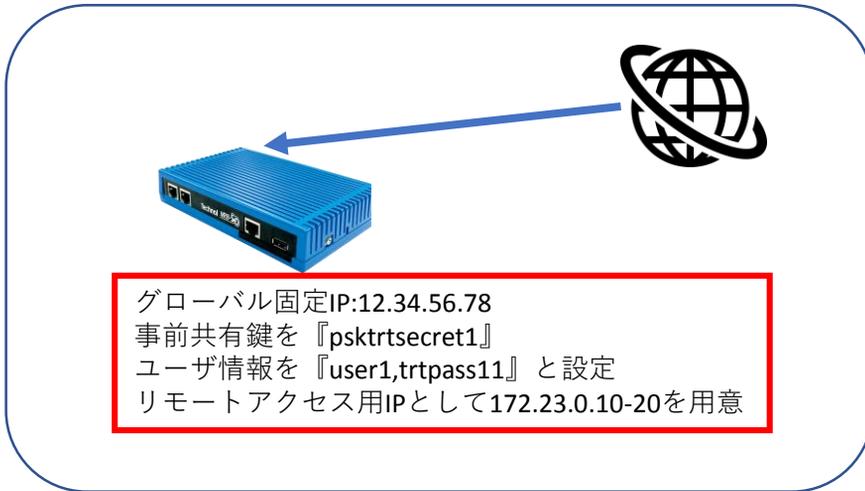
リモートアクセス設定 について

リモートアクセス設定についての補足説明です。

MRBのリモートアクセス接続イメージ



プロフェッショナルモードでのリモートアクセス設定の記入例です。



```

REMOTE_ACCESS{
CONFIG=ON
IP=172.23.0.1
CLIENT_RANGE=172.23.0.10-172.23.0.20
DNS=8.8.8.8
DNS=8.8.4.4
PSK=psktrtsecret1
USER=user1 trtpass11
USER=user2 trtpass22
}
    
```

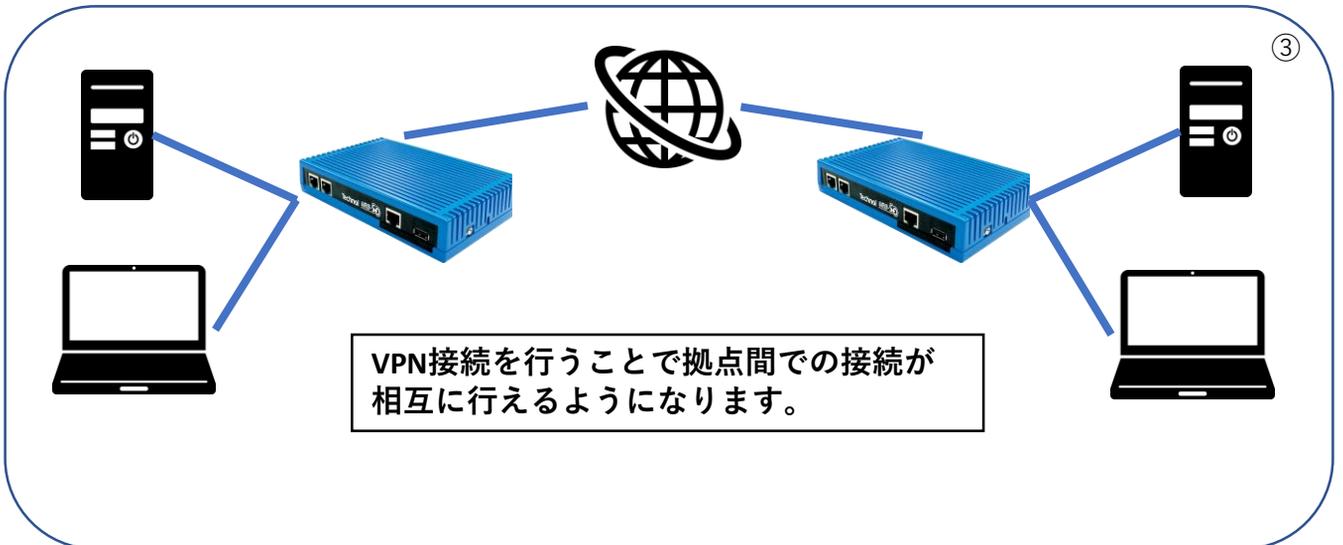
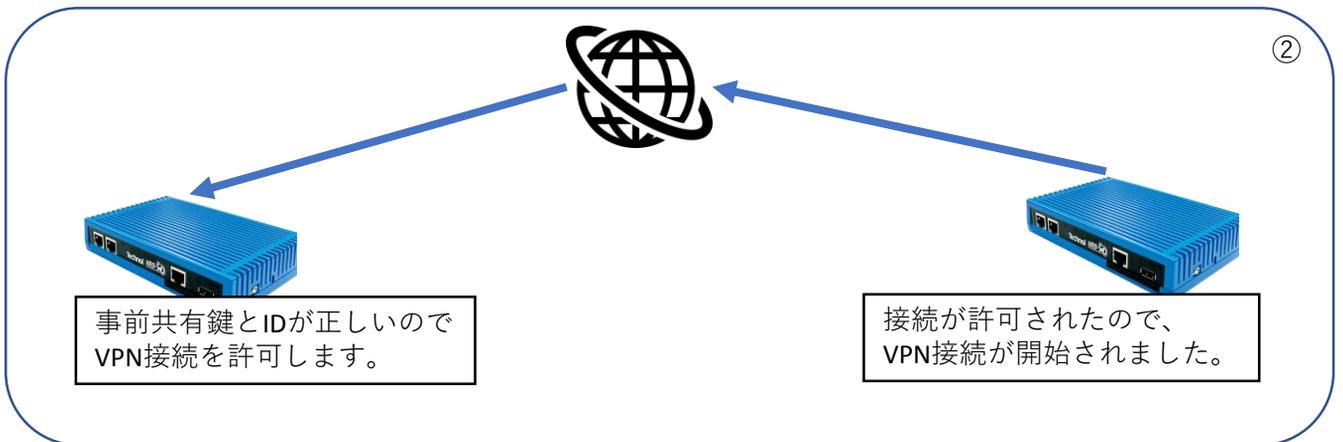
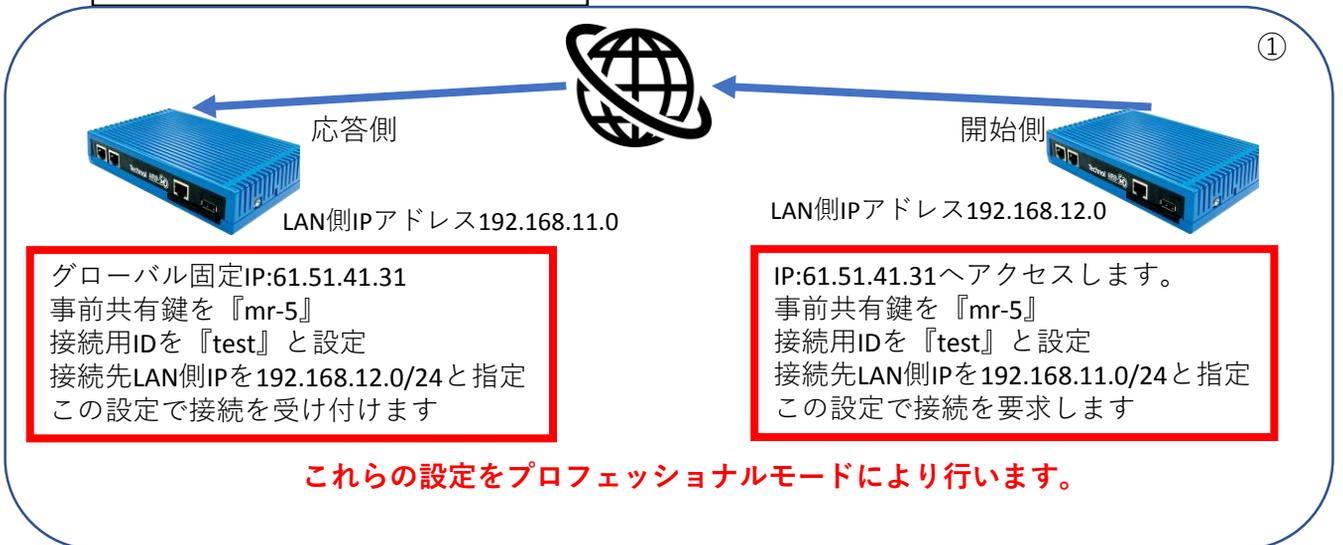
以下の記入例に従って、左図のように設定ファイルに項目を追加/変更し保存することで、リモートアクセス設定を行うことができます。

設定項目	記入例	備考
リモートアクセス	REMOTE_ACCESS{	
	CONFIG=ON	利用する場合はON
	IP=172.23.0.1	リモートアクセス用のMRBのIP
	CLIENT_RANGE=172.23.0.10-172.23.0.20	リモートアクセス用の端末のIP
	DNS=8.8.8.8	プライマリDNS
	DNS=8.8.4.4	セカンダリDNS
	PSK=psktrtsecret1	事前共有鍵
	USER=user1 trtpass11	ユーザ情報1(ID パスワード)
	USER=user2 trtpass22	ユーザ情報2(ID パスワード)
}		

VPN設定について

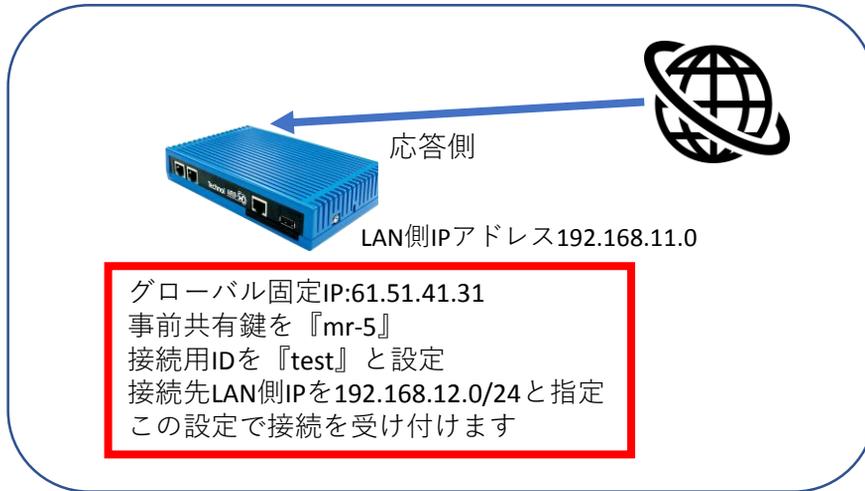
VPN設定についての詳細説明です。

MRBのVPN接続イメージ



※VPN接続には最低1つのグローバル固定IPが必要になります。

プロフェッショナルモードでのVPN接続設定(応答側)の記入例です。



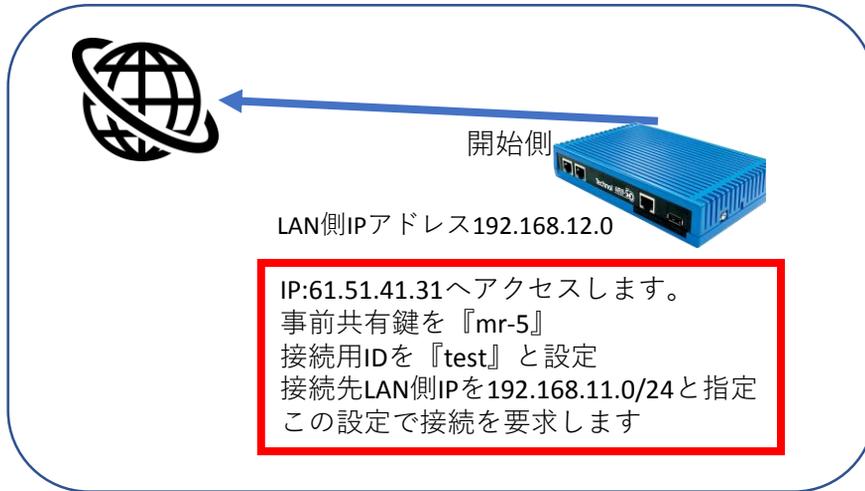
```
VPN{
08a68eec37af94301db96679e95673ca 1 1 2 mr-5 test 0 * 192.168.12.0
}
VPN_NET{
b0abb130d1f685921d7bd770e834de81 1 192.168.12.0 24
}
```

応答側設定：
以下の記入例に従って、左図のように設定ファイルに項目を追加/変更し保存することで、VPN接続設定を行うことができます。

設定項目	記入例	備考
VPN設定(応答側)	VPN{	
	08a68eec37af94301db96679e95673ca	ハッシュ値
	1	VPN番号
	1	有効なVPNなら1 / 無効なVPNなら2
	2	2
	mr-5	事前共通鍵
	Test	リモートID
	0	0
	*	*
	192.168.12.0	相手側LANアドレス
VPNネットワーク設定	1	UDPカプセル化有効なら1/無効なら0
	}	
	VPN_NET{	
	b0abb130d1f685921d7bd770e834de81	ハッシュ値
	1	VPN番号
192.168.12.0	IPアドレス	
24	ネットマスク	
}		

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。

プロフェッショナルモードでのVPN接続設定(開始側)の記入例です。



```
VPN{
2eb84e83830b72c05d3b12dfd05ced16 1 1 1 mr-5 61.51.41.31 2 test 192.168.11.0
}
VPN_NET{
b0abb130d1f685921d7bd770e834de81 1 192.168.11.0 24
}
```

開始側設定：

以下の記入例に従って、左図のように設定ファイルに項目を追加/変更し保存することで、VPN接続設定を行うことができます。

設定項目	記入例	備考
VPN設定(開始側)	VPN{	
	2eb84e83830b72c05d3b12dfd05ced16	ハッシュ値(32文字)
	1	VPN番号
	1	有効なVPNなら1/無効なVPNなら2
	1	1
	mr-5	事前共通鍵
	61.51.41.31	相手側固定IP
	2	固定IPでのVPNなら1/IDでのVPNなら2
	test	固定IPでのVPNなら開始側固定IP/IDでのVPNならID
	192.168.11.0	相手側LANアドレス
1	UDPカプセル化有効なら1/無効なら0	
}		
VPNネットワーク設定	VPN_NET{	
	b0abb130d1f685921d7bd770e834de81	ハッシュ値
	1	VPN番号
	192.168.11.0	IPアドレス
	24	ネットマスク
}		

※ハッシュ値は任意でユニークな32文字の16進数文字列を入力してください。