プロフェッショナル
モード設定

Technol

目次

※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。

※設定を間違えると機械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。

1. 本体設定のバックアップ

本項では、バックアップファイル（設定ファイル）を取得、反映する手順について記載します。

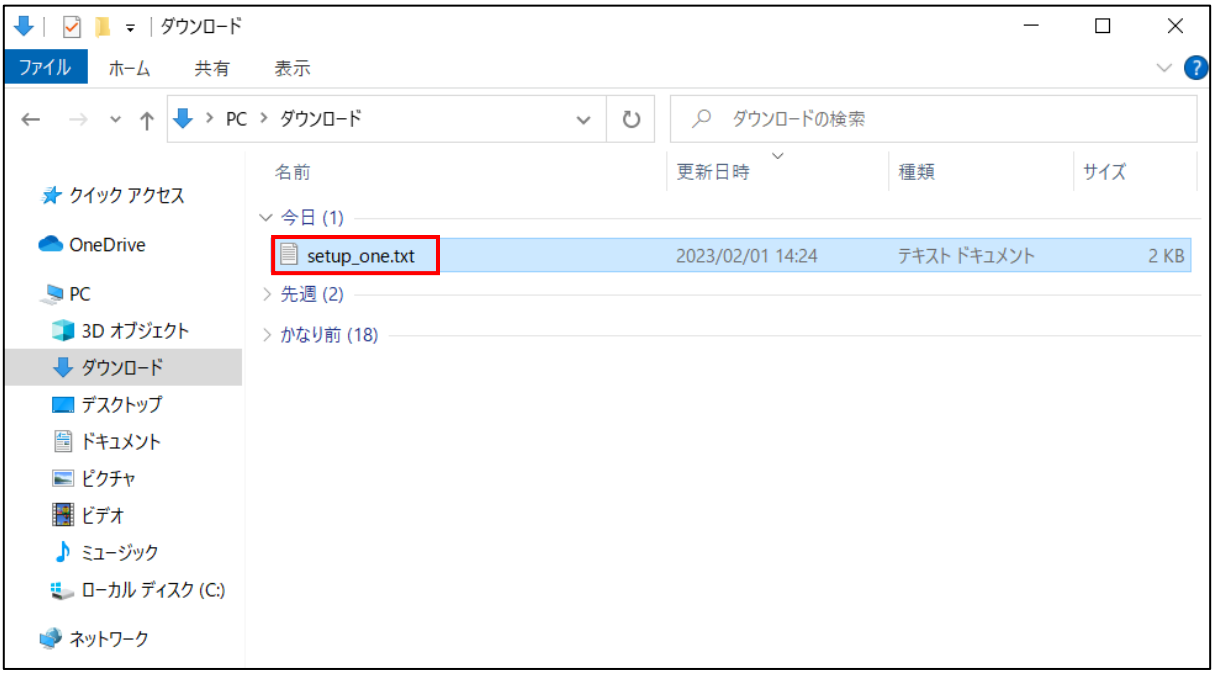
1.1 バックアップファイルの取得

本項では、バックアップファイルの取得手順について記載します。

① MRB にログイン後、右上の『設定』をクリックし、左下の『一括設定』をクリックします。

② 『ダウンロード』をクリックします。

③ “setup_one.txt”（バックアップファイル）がダウンロードされていることを確認して完了です。



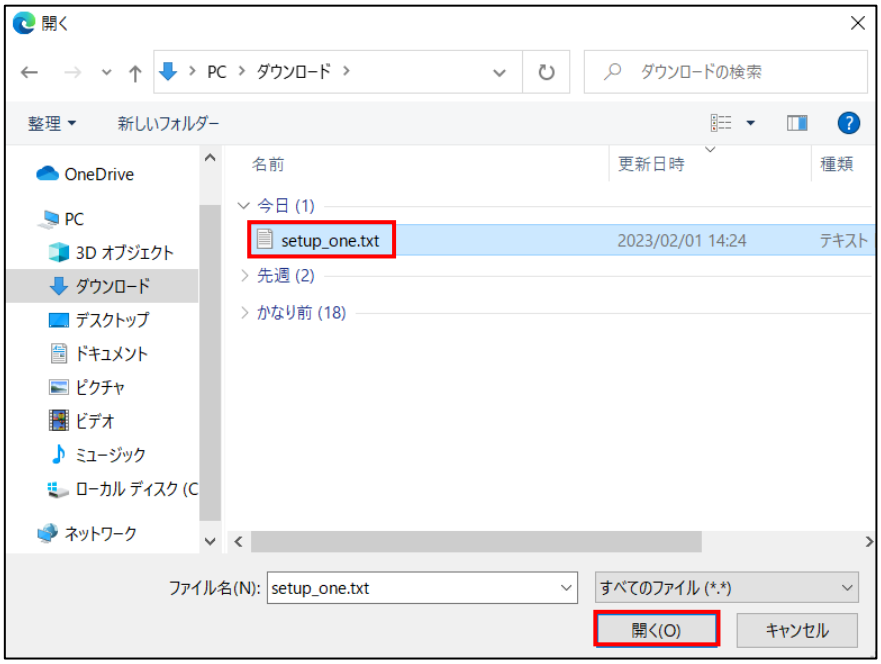
1.2　バックアップファイルの反映

本項では、バックアップファイルの反映（インポート）手順について記載します。

① MRB にログイン後、右上の『設定』をクリックし、左下の『一括設定』をクリックします。

② 『ファイルの選択』をクリックします。

③ 予め用意した MRB のバックアップファイルを選択し、『開く』をクリックします。



④ 『設定』をクリックします。

⑤ 『設定』をクリックして完了です。

※取得したバックアップファイルを別の機械にインポートする場合、
テキスト最上部に表示されている
CODE{
TRT=XXXXXX
}
の記述は削除してください。
誤った MRB の機械コードを認識してしまい、正しく機能しなくなります。

2. プロフェッショナルモード設定例

本項では、設定ファイルの設定例を記載します。

2.1 ネットワーク設定

本項では、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記載します。

・WAN 設定
・LAN 設定
・ブリッジ／ルーティング／TCPMSS 設定
・VPN 設定

※VPN 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。

2.1.1 WAN 設定

WAN 側のネットワーク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

WAN モード設定
[MRB-50L/500 のみ]
	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[MRB-50L のみ]
		冗長回線：3 ※1
		に対応。

WAN 設定
(PPPoE)
	WAN{
	PROTOCOL=PPPoE
	ID=xxxx@xxx
	PASS=zzzzzz
	IP=
	NETMASK=
	GATEWAY=
	DNS1=
	DNS2=
	}
		PROTOCOL：PPPoE
		ID：ID
		PASS：パスワード
		その他の部分は空白にする。

※1　MRB-50L で冗長回線に設定した場合、LTE が副回線になります。

設定項目	記入例	備考

WAN 設定
（DHCP）
	WAN{
	PROTOCOL=DHCP
	ID=
	PASS=
	IP=
	NETMASK=
	GATEWAY=
	DNS1=
	DNS2=
	}
		PROTOCOL：DHCP
		その他の部分は空白にする。

WAN 設定
（固定 IP）
	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=
	}
		PROTOCL：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。

LTE 設定
[MRB-50L のみ]
	LTE{
	APN=technol.com
	ID=example@technol.com
	PASS=password
	IP=
	GATEWAY=
	DNS1=
	DNS2=
	CARRIER=5
	}
		APN：APN
		ID：ID
		PASS：パスワード
		CARRIER：1 なら Docomo
		2 なら AU(mineo)
		3 なら AU(UQmobile)
		4 なら SoftBank
		5 なら自動設定
		その他の部分は指定がなければ空白にする。

IPv6_WAN 設定
（自動接続 SLAAC）
[HGW が存在しないとき]
	WAN_IPV6{
	METHOD=RA
	IPV6=
	PREFIX=64
	}
		METHOD：RA
		IPV6：空白
		PREFIX：64

設定項目	記入例	備考

WAN 設定
（IPv6 トンネル使用）
	WAN{
	PROTOCOL=V6Tunnel
	ID=
	PASS=
	IP=
	NETMASK=
	GATEWAY=
	DNS1=
	DNS2=
	}
		PROTOCL： V6Tunnel
		その他の部分は空白にする。

IPv6_WAN 設定
（プレフィックス デリゲート）
[HGW が存在する とき]
	WAN_IPV6{
	METHOD=PD
	IPV6=
	PREFIX=64
	}
		METHOD：PD
		IPV6：空白
		PREFIX：64

v6 プラス
利用設定
	WAN_IPV6_TUNNEL{
	TYPE=3
	TUNNELIP=192.168.111.111
	IFID=0001:0002:0003:0004
	BR=1000:2000:3000:4000
	SERVER=http://server.example
	USER=username
	PASS=password
	}
		TYPE：3
		TUNNELIP：固定 IP アドレス
		IFID：インターフェース ID
		BR：BR アドレス
		SERVER：再設定 URL
		USER：再設定ユーザ ID
		PASS：再設定パスワード

v6 コネクト
利用設定
	WAN_IPV6_TUNNEL{
	TYPE=4
	TUNNELIP=192.168.111.111
	IFID=0001:0002:0003:0004
	BR=1000:2000:3000:4000
	SERVER=
	USER=
	PASS=
	}
		TYPE： 4
		TUNNELIP：固定 IPv4 アドレス
		IFID：インターフェース ID
		BR：トンネル終端 IPv6 アドレス
		その他の部分は空白にする。

WAN 設定（MRB-500 のみ副回線の設定）

設定項目	記入例	備考

WAN 設定
（PPPoE）
[副回線]
	WAN2{
	PROTOCOL=PPPoE
	ID=xxxx@xxx
	PASS=zzzzzz
	IP=
	NETMASK=
	GATEWAY=
	DNS1=
	DNS2=
	}
		PROTOCOL：PPPoE
		ID：ID
		PASS：パスワード
		その他の部分は空白にする。

WAN 設定
（DHCP）
[副回線]
	WAN2{
	PROTOCOL=DHCP
	ID=
	PASS=
	IP=
	NETMASK=
	GATEWAY=
	DNS1=
	DNS2=
	}
		PROTOCOL：DHCP
		その他の部分は空白にする。

WAN 設定
（固定 IP）
[副回線]
	WAN2{
	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=
	}
		PROTOCL：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。

IPv6_WAN 設定
（自動接続 SLAAC）
[HGW が存在しない　とき]
[副回線]
	WAN2_IPV6{
	METHOD=RA
	IPV6=
	PREFIX=64
	}
		METHOD：RA
		IPV6：空白
		PREFIX：64

設定項目	記入例	備考

WAN 設定
（IPv6 トンネル使用）
[副回線]
	WAN2{
	PROTOCOL=V6Tunnel
	ID=
	PASS=
	IP=
	NETMASK=
	GATEWAY=
	DNS1=
	DNS2=
	}
		PROTOCL：V6Tunnel
		その他の部分は空白にする。

IPv6_WAN 設定
（プレフィックスデリゲート）
[HGW が存在するとき]
[副回線]
	WAN2_IPV6{
	METHOD=PD
	IPV6=
	PREFIX=64
	}
		METHOD：PD
		IPV6：空白
		PREFIX：64

v6 プラス
利用設定
[副回線
	WAN2_IPV6_TUNNEL{
	TYPE=3
	TUNNELIP=192.168.111.111
	IFID=0001:0002:0003:0004
	BR=1000:2000:3000:4000
	SERVER=http://server.example
	USER=username
	PASS=password
	}
		TYPE：3
		TUNNELIP：固定 IP アドレス
		IFID：インターフェース ID
		BR：BR アドレス
		SERVER：再設定 URL
		USER：再設定ユーザ ID
		PASS：再設定パスワード

v6 コネクト
利用設定
[副回線]
	WAN2_IPV6_TUNNEL{
	TYPE=4
	TUNNELIP=192.168.111.111
	IFID=0001:0002:0003:0004
	BR=1000:2000:3000:4000
	SERVER=
	USER=
	PASS=
	}
		TYPE：4
		TUNNELIP：固定 IPv4 アドレス
		IFID：インターフェース ID
		BR：トンネル終端 IPv6 アドレス
		その他の部分は空白にする。

2.1.2　LAN 設定(MRB-50/50L/100/500)

LAN 側のネットワーク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

有線 LAN 設定	LAN2{
	CONFIG=ON/OFF
	IP=192.168.124.254
	NETMASK=255.255.255.0
	IPV6=ON/OFF
	}
		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
		IPV6：IPv6 を使用する場合は ON

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

無線 LAN 設定	LAN{
	CONFIG=ON/OFF
	IP=192.168.123.254
	NETMASK=255.255.255.0
	IPV6=ON/OFF
	}
		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
		IPV6：IPv6 を使用する場合は ON

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

設定項目	記入例	備考

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
		40~48(4 刻み)

端末 IP 固定設定
(DHCP の範囲内は割り当てないこと。)
	DHCP_FIXED{
	a06dec9e44e7e3ba10d5b22da8ba94c9
	00:00:00:00:00:00 192.168.124.11 trtclient001
	}
		・ハッシュ値 ※1
		・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。

※1　ハッシュ値は 32 桁で一意の値である必要があります。

2.1.3　LAN 設定(MRB-51/200)

LAN 側のネットワーク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

LAN 設定	LAN{
	CONFIG=ON/OFF
	IP=192.168.124.254
	NETMASK=255.255.255.0
	IPV6=ON/OFF
	}
		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
		IPV6：IPv6 を使用する場合は ON

DHCP 設定	DHCP{
	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

2.1.4　ブリッジ／ルーティング／TCPMSS 設定

ブリッジ／ルーティング／TCPMSS 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
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 ※1
		・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 ※1
		・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)

※1　ハッシュ値は 32 桁で一意の値である必要があります。

2.1.5　VPN 設定

VPN 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

VPN 設定	VPN{
	08a68eec37af94301db96679e95673ca 1 1 2
	mr-5 test 1 61.51.41.31 192.168.112.0 1 1
	}
		・ハッシュ値 ※1
		・VPN 番号
		・設定有効：1 / 設定無効：2
		・開始側：1 / 応答側：2
		MRB 番号：3
		・事前共通鍵
		・応答側　：開始側指定の ID
		開始側　：応答側の固定 IP
		MRB 番号：相手側の機械番号
		・相手に IP を知らせる　：1
		相手に ID を知らせる　：2
		IP / ID を使用しない　：3
		・固定 IP or ID or *(なしのとき)
		・相手側 LAN アドレス
		・UDP カプセル化 ON：1
		OFF：0 ※2
		・IKEv1：1　/　IKEv2：2
		の順に 1 行に記載。

VPN ネットワーク設定	VPN_NET{
	b0abb130d1f685921d7bd770e834de81 1
	10.10.1.0 16
	}
		・ハッシュ値 ※1
		・VPN 番号
		・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。
		VPN 番号は VPN 設定に対応させる。

※1　ハッシュ値は 32 桁で一意の値である必要があります。

※2　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。

2.2　フィルタリング設定

本項では、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記載します。

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

2.2.1　URL/IP フィルタリング設定

URL/IP フィルタリング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 フィルタのレベル設定	URL_LEVEL_100{
	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 フィルタリングのみ判別方式も指定。
		METHOD=の後に
		スコア：1　脅威：2　スコアと脅威：3
		の対応するものを記載。

IP フィルタのレベル設定	IP_LEVEL_100{
	2
	METHOD=1
	}	

振る舞いフィルタのレベル設定	BEHAVIOR_LEVEL_100{
	2
	}	

URL フィルタのホワイトリスト	URL_WHITE_100{
	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 ※1
		・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_100{
	f15d461b1a1dc80efa85f7c6aa1f865b 0
	www.example.co.jp
	f686fab203c770588504a557f77109ee 0
	www.example.com
	}	

※1　ハッシュ値は 32 桁で一意の値である必要があります。

設定項目	記入例	備考

IP フィルタの
ホワイトリスト
	IP_WHITE_100{
	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 ※1
		・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_100{
	f15d461b1a1dc80efa85f7c6aa1f865b
	123.123.123.123 32
	f686fab203c770588504a557f77109ee
	222.111.111.222 32
	}	

URL フィルタの
カテゴリ指定
(カスタムカテゴリ)
	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。 ※2

URL フィルタの
レベル設定
(カスタムカテゴリ)
	URL_LEVEL_100{
	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)
		カテゴリフィルタグループに対応する
		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。

※1　ハッシュ値は 32 桁で一意の値である必要があります。
※2　数字とカテゴリの対応一覧は下記 URL の「URL フィルタリングリスト（全プロダクト共通)」を参照下さい。
https://www.mrb-security.jp/support/download

2.2.2　HTTPS フィルタリング設定

HTTPS フィルタリング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

HTTPS 通信検知	HTTPS_100{
	HTTPS=ON / OFF
	IP=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 ※1
		IP：HTTPS 通信時、IP フィルタリングを利用する場合は ON

HTTPS 通信の URL ホワイトリストの設定	URL_HTTPS_100{
	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 ※2
		・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_100{
	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 ※2
		・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。

※1　HTTPS 通信フィルタリングを正常に行うため、各端末へ MRB 証明書のインポート作業が必要となります。MRB 証明書のインポート手順については、手順書『HTTPS フィルタリング設定』を参照ください。

※2　ハッシュ値は 32 桁で一意の値である必要があります。

2.2.3　グループ設定

グループ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

グループ設定	GROUP{
	0 142de12bb38de8456458cca74e5470b1 GROUP0 1
	1 ec9ec38870b67838b0d095f9c1521539 GROUP1 0
	2 6c78d5207b9074eac13ec7edc8c847f2 GROUP2 0
	3 130fe12eb38db8784a4899a74e4960bd GROUP3 0
	}
		グループポリシーを使用する際に必須の記述です。
		左の例をそのままコピーして使用してください。

グループポリシー
（グループへの IP 割当）
	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
	}
		・グループ番号
		・ハッシュ値 ※1
		・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 を 2 つ
		の順に 1 行に記載。
		複数設定の際は改行して同様に記載。

※1　ハッシュ値は 32 桁で一意の値である必要があります。

2.2.4　メールフィルタリング設定

メールフィルタリング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

メール検知機能	MAIL_100{
	MAIL=ON/OFF
	SPAM=ON/OFF
	VIRUS=ON/OFF
	SSL=ON/OFF
	SUBJECT=-SPAM-
	SUBJECTVIRUS=-VIRUS-
	}
		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)
		MAIL：利用する場合は ON
		SPAM：利用する場合は ON
		VIRUS：利用する場合は ON
		SUBJECT：スパム判定時メールタイトルに表示される文言 ※1
		SUBJECTVIRUS：ウイルス判定時メールタイトルに表示される文言 ※1
		(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)

メール検知機能
ブラック/ホワイトリスト追加
	MAIL_WHITE_100{
	11d5c032a95612ed6e7c4b1f34f83af2 0 white1@test.com
	22d5c032a95612ed6e7c4b1f34f83af2 0 white1@test.com
	}
	MAIL_BLACK_100{
	88d5c032a95612ed6e7c4b1f34f83af2 0 black1@test.com
	25d5c032a95612ed6e7c4b1f34f83af2 0 black2@test.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 ※2
		・0
		・メールアドレス
		の順に 1 行に記載。
		複数設定の際は改行して同様に記載。

※1　メールタイトルを設定する SUBJECT、SUBJECTVIRUS ではハイフンの連続表記「--」は設定出来ません。

※2　ハッシュ値は 32 桁で一意の値である必要があります。

2.2.5　メールサーバ設定

メールサーバ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。

※MRB-51 のみ対応

設定項目	記入例	備考

メールサーバ	MAILSERVER{
	f0fdb4c3f58e3e3f8e77162d893d3055
	111.111.111.111 32
	}
		・ハッシュ値 ※1
		・メールサーバ IP
		・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。

※1　ハッシュ値は 32 桁で一意の値である必要があります。

2.3　プロフェッショナルモード固有の設定

本項では、WebGUI 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
・syslog 送信設定
・タグ VLAN 設定
・インバウンドポリシー設定

・

※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。

2.3.1　リモートアクセス設定

リモートアクセス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

リモートアクセス	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
	}
		CONFIG：使用する場合は ON
		IP：　リモートアクセス用 IP
		CLIENT_RANGE：DHCP 範囲
		DNS：DNS サーバ
		（上がプライマリ、下がセカンダリ）
		PSK：事前共有鍵
		USER：利用ユーザ
		（前半が ID、後半がパスワード）
		ユーザを複数登録する際は改行して同様に記載。

上記の例をコンフィグに記載した場合、
L2TP/IPsec により事前共有鍵 psktrtsecret1 でアクセスが可能になり、
user1 はパスワード trtpass11 で、User2 はパスワード trtpass22 で利用できる。
という設定が行われます。

2.3.2　syslog 送信設定

syslog 送信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

SYSLOG 送信設定	SYSLOG{
	ENABLE=1
	PROTOCOL=TCP or UDP
	SERVER=192.168.123.123
	PRIORITY=*
	}
		ENABLE：利用する場合は 1
		PROTOCOL：TCP or UDP
		SERVER：syslog を送付する IP
		PRIORITY：*
		以下の表の”priority”を参考に指定

※syslog 送信に使用するポートは 514 番です

重要度	PRIORITY	内容
0	*	すべてのログ
1	debug	デバッグ情報
2	info	情報
3	notice	通知
4	warn	警告
5	err	一般的なエラー
6	crit	致命的なエラー
7	alert	緊急に対処すべきエラー
8	emerg	システムが落ちるような状態

※重要度の小さい“PRIPRITY“を設定すると、
　それより重要度の大きいログはすべて送信されます

2.3.3　タグ VLAN 設定(MRB-50/50L/100/500)

タグ VLAN 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

タグ VLAN 設定	VLAN2{
	1 10 192.168.111.1 24
	1 20 192.168.112.1 24
	1 30 172.26.0.1 16
	}
		・1
		・タグ番号
		・ネットワークアドレス
		の順に 1 行に記載。
		複数設定の際は改行して同様に記載。

※設定時、LAN と書かれたポートがトランクポートとして機能します。
　タグ番号は 3 から 10 まで設定可能です。(1, 2 は設定不可です。)

2.3.4　タグ VLAN 設定(MRB-51/200)

タグ VLAN 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

タグ VLAN 設定	VLAN{
	1 10 192.168.111.1 24
	1 20 192.168.112.1 24
	1 30 172.26.0.1 16
	}
		・1
		・タグ番号
		・ネットワークアドレス
		の順に 1 行に記載。
		複数設定の際は改行して同様に記載。

※設定時、LAN と書かれたポートがトランクポートとして機能します。
　タグ番号は 3 から 10 まで設定可能です。(1, 2 は設定不可です。)

2.3.5　インバウンドポリシー設定(MRB-50/50L/100/500)

インバウンドポリシー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

インバウンド
ポリシー設定
	ALLOW_INBOUND{
	12ce235094606eef87cd8c8d75e8c5b3
	0.0.0.0/0 0.0.0.0/0 PING
	44efe78ca2167357d15f7faf2bfceba4
	1.1.1.1/32 192.168.0.0/16 TCP 1-65535
	233d37de5b76802fa5a0a24d0e9286ef
	2.2.2.2/32 192.168.3.0/24 ANY
	d5a9e9db4748b743d6c4ead082d9bd1f
	192.168.0.0/16 192.168.0.1/32 ICMP
	dee4aaa62dbb1fdaea563cd060509ab7
	4.4.44.4/32 44.4.4.4/32 UDP 3
	}
		・ハッシュ値 ※1
		・送信元 IP(OUT)
		・送信先 IP(IN)
		・プロトコル
		・ポート番号(TCP,UDP の場合)
		の順に 1 行に記載。
		複数設定の際は改行して同様に記載。

※1　ハッシュ値は 32 桁で一意の値である必要があります。

プロトコルは下表を参照ください。

プロトコル	内容
PING	ICMP でのエコー要求を許可する
ICMP	ICMP プロトコルすべてを許可する
TCP	指定したポートの TCP 通信を許可する
UDP	指定したポートの UDP 通信を許可する
ANY	すべての通信を許可する

2.3.6　インバウンドポリシー設定(MRB-51/200)

インバウンドポリシー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

インバウンドポリシー
MRB-51 / 200 対応
	INBOUND_POLICY{
	7f9e89bf7b515974b75bd1e2e4c79972
	192.168.11.1 192.168.12.1 1 999 1
	
	[IP の範囲指定]
	7f9e89bf7b515974b75bd1e2e4c79972
	192.168.11.1-192.168.11.5
	192.168.12.1-192.168.12.5
	6 20 1
	
	[IP のネットワーク指定]
	7f9e89bf7b515974b75bd1e2e4c79972
	192.168.11.0/24 192.168.12.0/24 17
	80 1
	
	[ポートの複数/範囲指定]
	7f9e89bf7b515974b75bd1e2e4c79972
	192.168.11.1 192.168.12.1 6
	20,55000-55015 1
	}
		・ハッシュ値 ※1
		・送信元 IP（OUT）
		・送信先 IP（IN）
		・プロトコル番号
		（以下の表を参考にしてください）
		・ポート番号（TCP, UDP の場合）
		・1
		の順に 1 行に記載。
		複数設定の際は改行して同様に記載。

※1　ハッシュ値は 32 桁で一意の値である必要があります。

プロトコル番号は下表を参照ください。

プロトコル	プロトコル番号	内容
TCP	6	指定したポートの TCP 通信を許可する
UDP	17	指定したポートの UDP 通信を許可する
GRE	47	GRE プロトコルすべてを許可する
ESP	50	ESP プロトコルすべてを許可する
AH	51	AH プロトコルすべてを許可する
ICMP	1	ICMP プロトコルすべてを許可する
ANY	999	すべての通信を許可する

3. プロフェッショナルモード設定補足

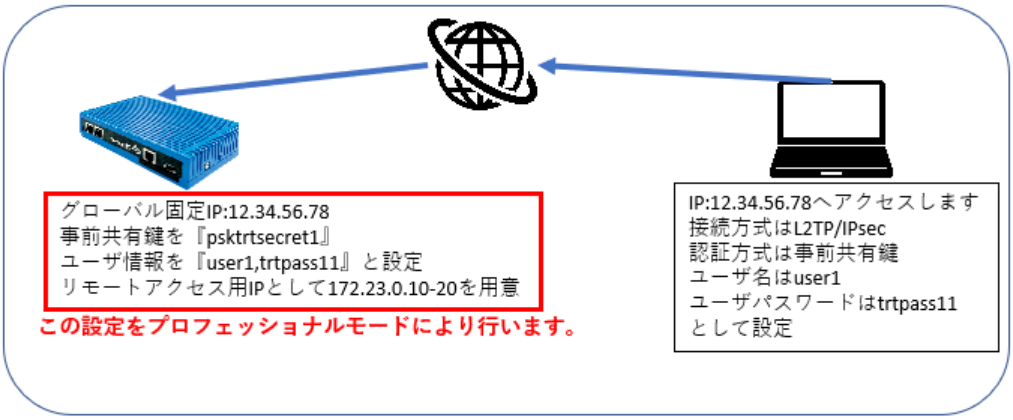
本項では、リモートアクセス設定と VPN 設定についての補足説明を記載します。

3.1 リモートアクセス設定

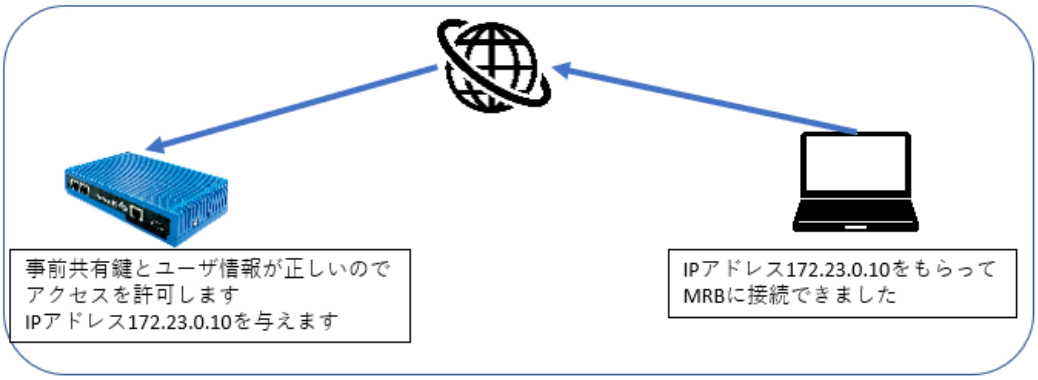
本項では、リモートアクセス設定についての補足説明を記載します。

・MRB のリモートアクセス接続イメージ

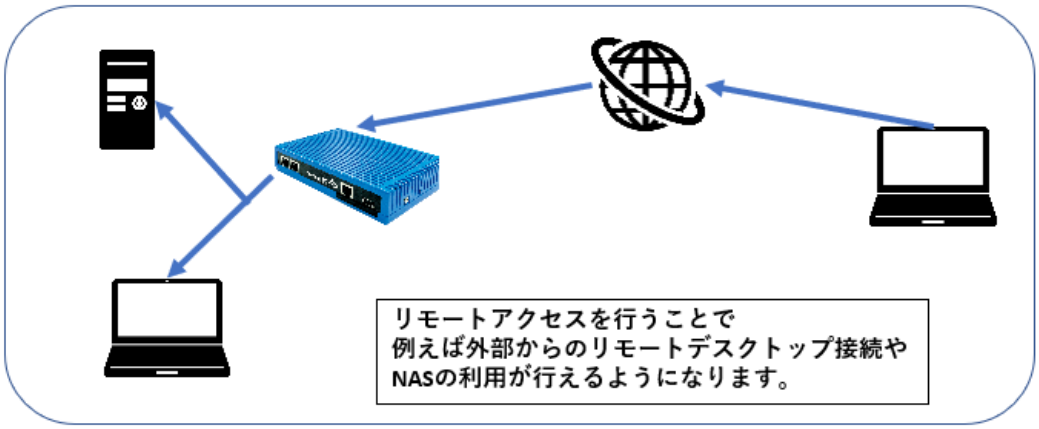
①



②



③

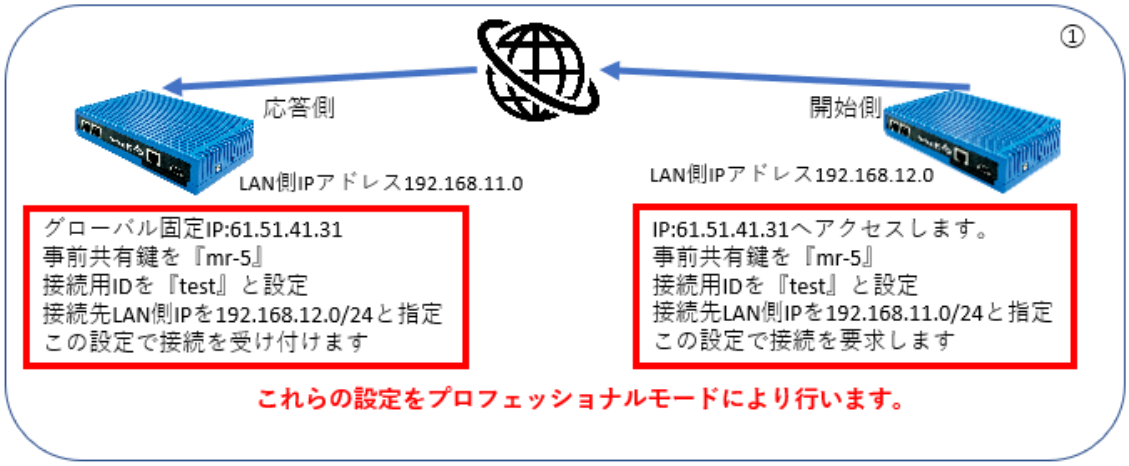


3.2　VPN 設定

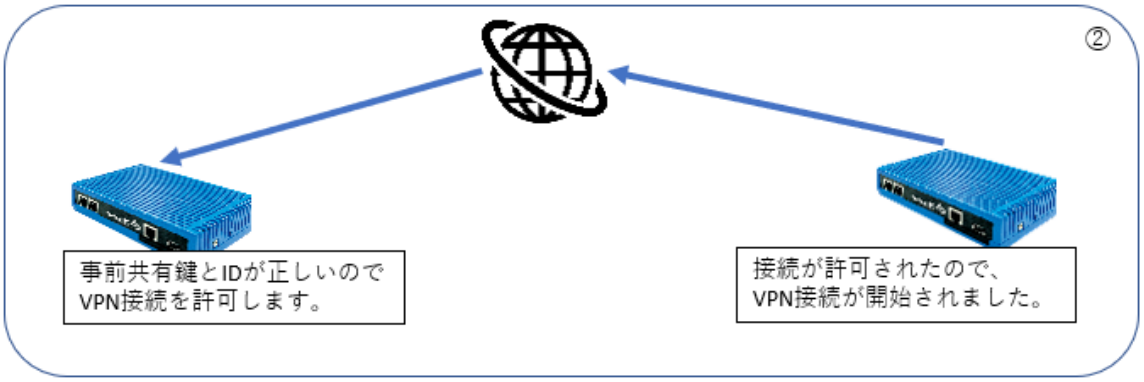
本項では、VPN 設定についての補足説明を記載します。

・MRB の VPN 接続イメージ

①



②



③