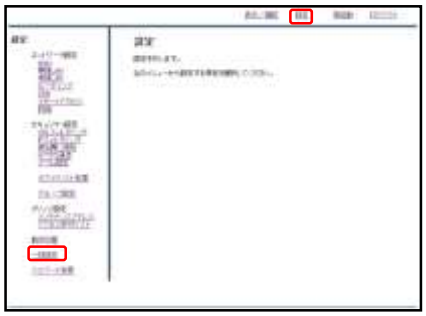
プロフェッショナル
モード設定

・プロフェッショナルモード設定 目次

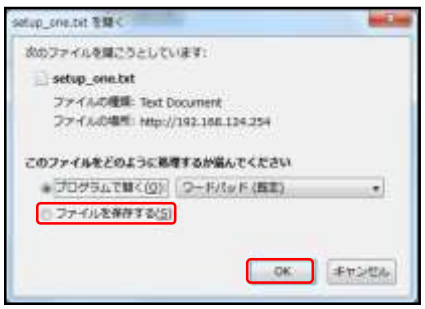
1, バックアップファイルの取得

バックアップの為、MRBの設定ファイル
をエクスポートします



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。

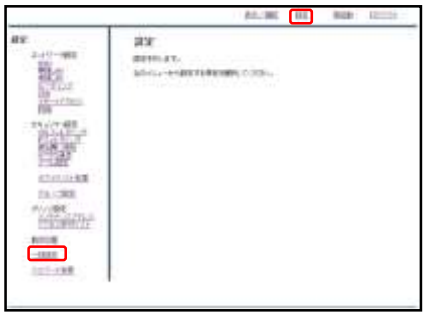


③ダイアログが表示されますので、
”ファイルを保存する”を選択し、『OK』をクリック
します。任意の場所に保存し、作業は完了です。

なお、ダウンロードされるファイルのタイトル
は”**setup_one.txt**” です。

1-2, バックアップファイルの反映

保存しておいた設定ファイルをインポートし、バックアップの反映を行います



①MRB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『参照』をクリックし、予め用意したMRBのコンフィグファイルを選択し、『設定』をクリックします。

③『設定』をクリックします。

④『設定』をクリックします。

⑤上のような画面が表示され、設定は完了です。

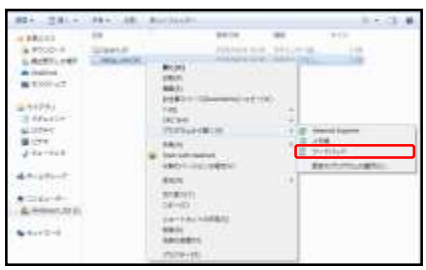
2, 設定ファイルの編集

・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。

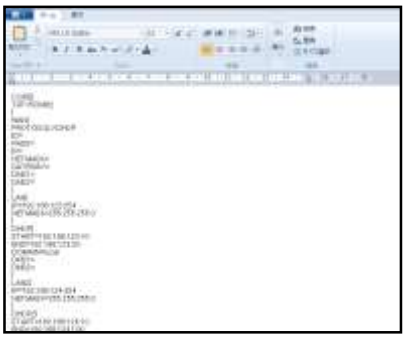
**※設定を間違えると機械が動作しなくなる恐れがありますので、プロフェッショナルモードでの設定の際はバックアップの取得をお願い致します。
なお、設定ミスによる動作不良の責任は負いかねますのでご了承ください。**

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, バックアップファイルの取得”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”を選択します。



②”ワードパッド”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。

**※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。
MRBが正しく機能しなくなります。**

3-1, プロフェッショナルモード設定例概要

3-2 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
- LTE設定(MRB-50Lのみ対応)
- 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

3-3 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

3-4 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、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
- タグVLAN
- インバウンドポリシー
- syslog出力

※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。

3-2, 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 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。
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=0 }	“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。

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（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
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。

[MRB-500のみ]WAN側副回線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設定（PPPoE）[副回線]	WAN2{ PROTOCOL=PPPoE ID=××××@××× 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。
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。

[MRB-500のみ]WAN側副回線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
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
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。

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
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 ・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。

その他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。

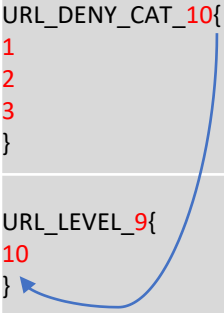
設定項目	記入例	備考
ブリッジ	BRIDGE{ }	ブリッジ利用の際は記入例そのままにコンフィグに記載。
ブリッジ時の管理IP	BRIDGE_MANAGE_IP{ CONFIG=ON/OFF IP=111.111.111.11 NETMASK=255.255.0.0 }	”CONFIG=”：利用する場合は”ON” “IP=”：メンテナンスアドレス “NETMASK=”：サブネットマスク
ブリッジ時の通過許可IP	BRIDGE_ALLOW_IP{ 7f9e89bf7b515974b75bd1e2e4c79972 192.168.11.1 32 }	・ハッシュ値 ・通過許可IPアドレス ・ネットマスク長 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設定 **※MRB番号でのVPNはIPv6アドレス利用時のみ可能です**	VPN{ 08a68eec37af94301db96679e95673ca 1 1 2 mr-5 test 1 61.51.41.31 192.168.112.0 1 1 }	・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 / 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 ・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 ・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。

※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

3-3, フィルタリング設定

IP/URLの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_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_9{ 2 METHOD=1 }	
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 }	
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。
URLフィルタのレベル設定(カスタムカテゴリ)	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。

※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

HTTPSの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_9{ 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” “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_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。

※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。

グループ分け設定、メールの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
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 ・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 の順に1行に記載。 複数設定の際は改行して同様に記載。
メール検知機能	MAIL_9{ 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 “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)
メール検知機能 ブラック/ホワイトリスト追加	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 }	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 ・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。

3-4, プロフェッショナルモード固有の設定

以下はプロフェッショナルモードでのみ設定可能な項目となります。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。

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

(“info”と入力すると2~8の重要度のログが送信される)

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。

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 ・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。

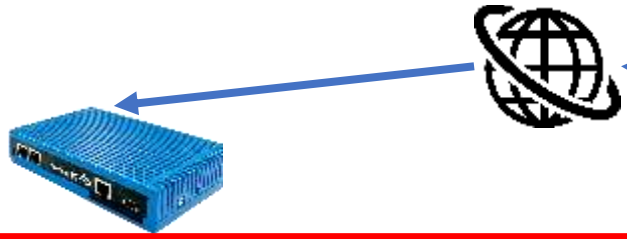
プロトコル	**内容**
PING	ICMPでのエコー要求を許可する
ICMP	ICMPプロトコルすべてを許可する
TCP	指定したポートのTCP通信を許可する
UDP	指定したポートのUDP通信を許可する
ANY	すべての通信を許可する

4-1, 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

①

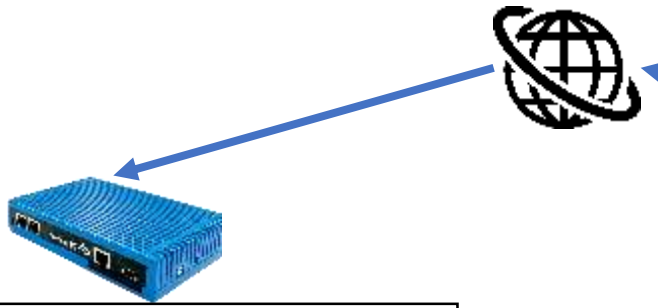


グローバル固定IP:12.34.56.78
事前共有鍵を『psktrtsecret1』
ユーザ情報を『user1,trtpass11』と設定
リモートアクセス用IPとして172.23.0.10-20を用意

この設定をプロフェッショナルモードにより行います。

IP:12.34.56.78へアクセスします
接続方式はL2TP/IPsec
認証方式は事前共有鍵
ユーザ名はuser1
ユーザパスワードはtrtpass11
として設定

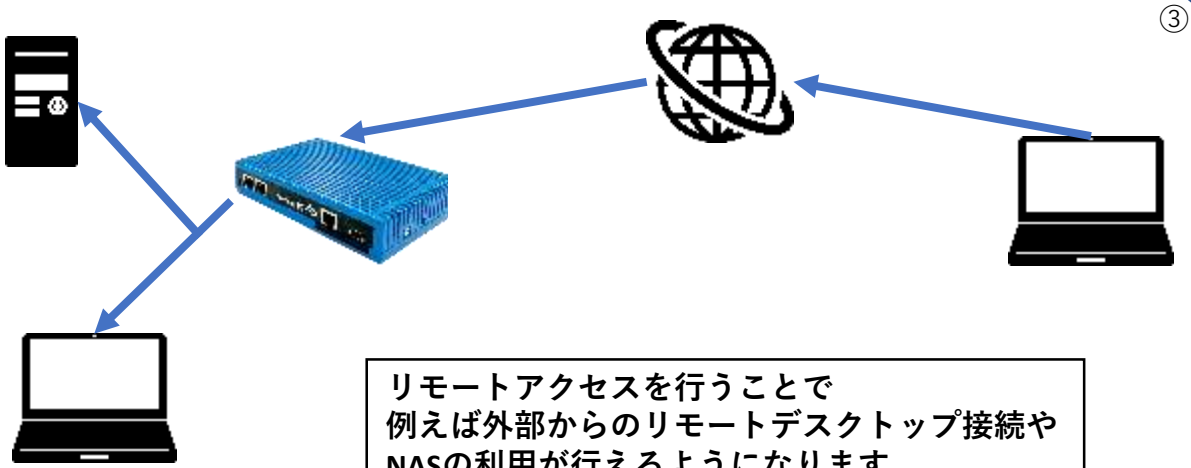
②



事前共有鍵とユーザ情報が正しいので
アクセスを許可します
IPアドレス172.23.0.10を与えます

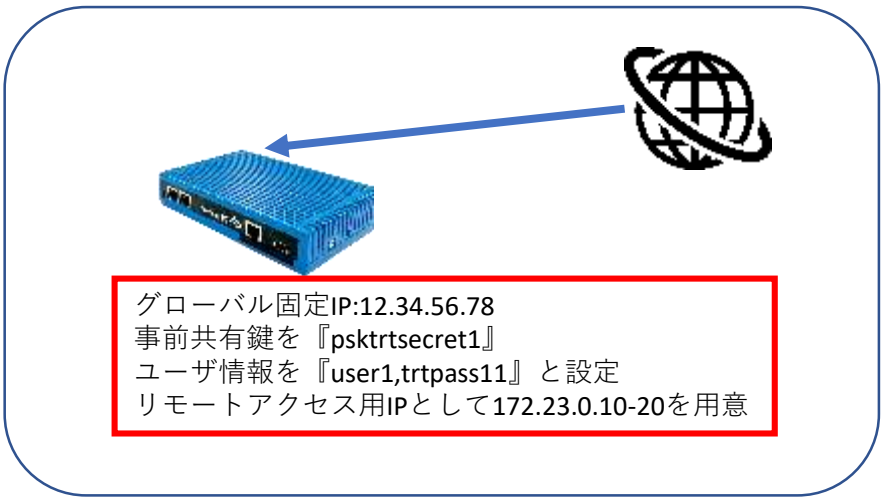
IPアドレス172.23.0.10をもらって
MRBに接続できました

③



**リモートアクセスを行うことで
例えば外部からのリモートデスクトップ接続や
NASの利用が行えるようになります。**

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出来ます。

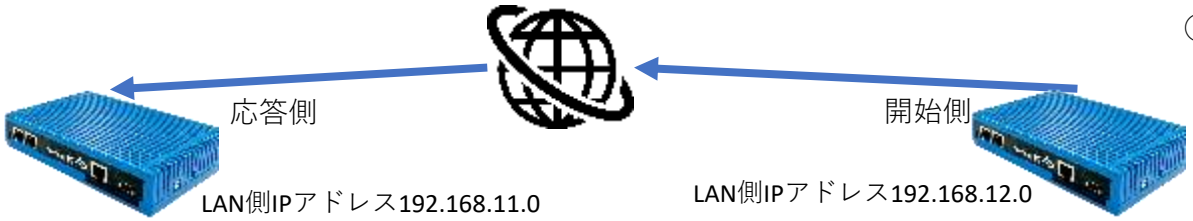
設定項目	記入例	備考
リモートアクセス	REMOTE_ACCESS{	
	CONFIG=ON	利用する場合はON
	IP=172.23.0.1	リモートアクセス用のMRBのIP
	CLIENT_RANGE=172.23.0.10-172.23.0.20	リモートアクセス用の端末のIP
	DNS=8.8.8.8	プライマリDNS
	DNS=8.8.4.4	セカンダリDNS
	PSK=psktrtsecret1	事前共有鍵
	USER=user1 trtpass11	ユーザ情報1(ID パスワード)
	USER=user2 trtpass22	ユーザ情報2(ID パスワード)
	}	

4-2, VPN設定について

VPN設定についての補足説明です。

MRBのVPN接続イメージ

①

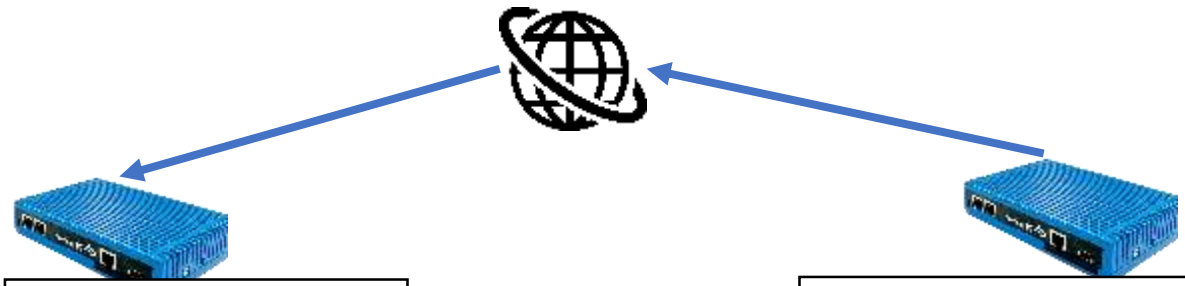


グローバル固定IP:61.51.41.31
事前共有鍵を『mr-5』
接続用IDを『test』と設定
接続先LAN側IPを192.168.12.0/24と指定
この設定で接続を受け付けます

IP:61.51.41.31へアクセスします。
事前共有鍵を『mr-5』
接続用IDを『test』と設定
接続先LAN側IPを192.168.11.0/24と指定
この設定で接続を要求します

これらの設定をプロフェッショナルモードにより行います。

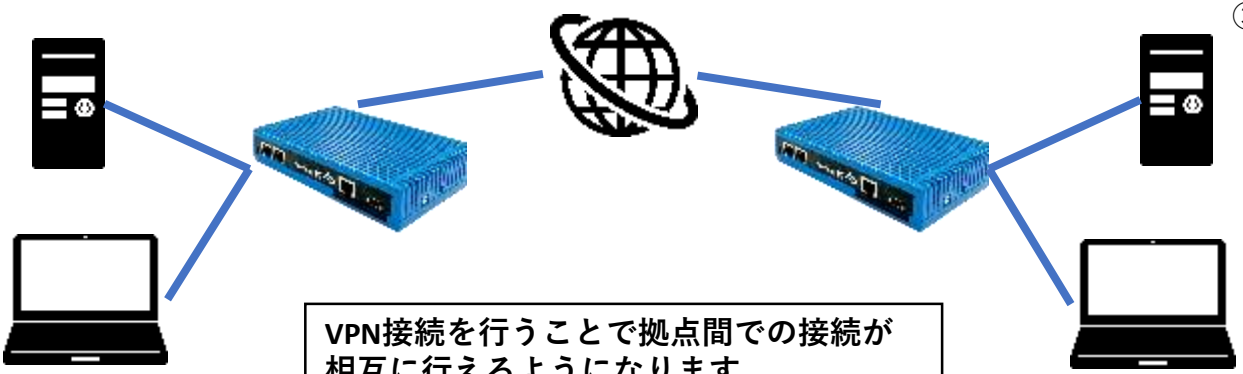
②



事前共有鍵とIDが正しいので
VPN接続を許可します。

接続が許可されたので、
VPN接続が開始されました。

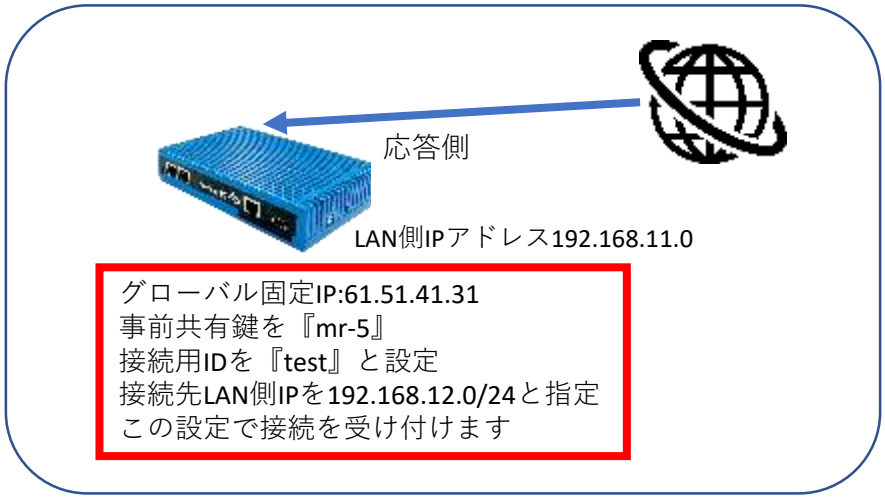
③



**VPN接続を行うことで拠点間での接続が
相互に行えるようになります。**

※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。

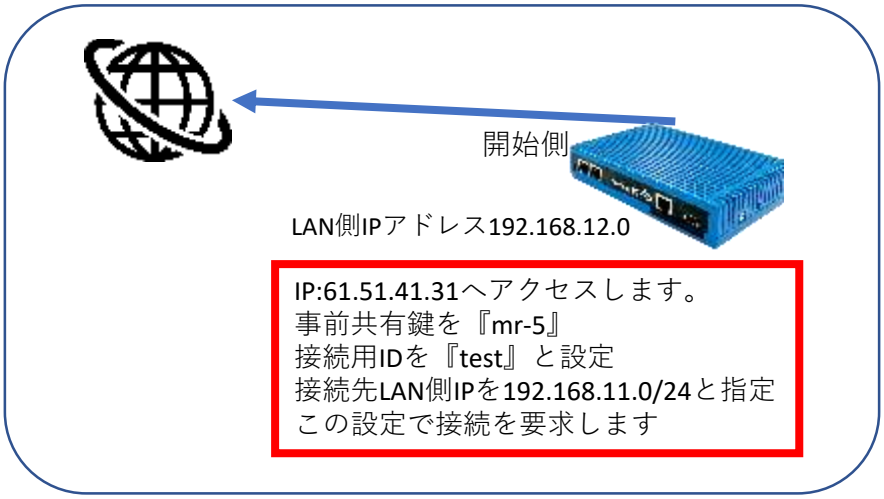


応答側設定例：
以下の記入例に従って設定ファイルに項目を追加/変更し保存することで、VPN接続設定を行うことが出来ます。
(実際にコンフィグを編集する場合、各項目は改行ではなく空白で区切って記載してください)

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	開始側なので2
	mr-5	事前共通鍵
	Test	開始側指定のID
	1	相手に固定IPを知らせるので1
	61.51.41.31	固定IP
	192.168.12.0	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
	2	IKEv2で接続するので2
	}	
VPNネットワーク設定	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。



応答側設定例：
以下の記入例に従って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出来ます。
(実際にコンフィグを編集する場合、各項目は改行ではなく空白で区切って記載してください)

設定項目	記入例	備考
VPN設定(開始側)	VPN{	
	2eb84e83830b72c05d3b12dfd05ced16	ハッシュ値
	1	VPN番号
	1	有効なVPNなら1 / 無効なVPNなら2
	1	開始側なので1
	mr-5	事前共通鍵
	61.51.41.31	応答側の固定IP
	2	相手にIDを知らせるので2
	test	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
	2	IKEv2で接続するので2
	}	
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。