

MRBオンライン マニュアル

・全体目次

基本設定

- 1 ログイン
- 2 ログインパスワードの変更
- 3 WAN設定
- 4 LAN設定
- 5 ブリッジモード
- 6 セキュリティ設定
- 7 グループ設定
- 8 ホワイトリスト申請/処理
- 9 TCPMSS設定
- 10 VPN設定

HTTPSフィルタリング

- 1 HTTPSフィルタリング設定
- 2 証明書のダウンロード
- 3 証明書のインポート
- 4 クライアント証明書を利用する場合

メールフィルタリング

- 1 Outlookの設定確認
- 2 MRBの設定
- 3 SSLでメールを受信している場合

プロフェッショナルモード

- 1 本体設定のバックアップ
- 2 プロフェッショナルモードによる本体設定変更
- 3 プロフェッショナルモード設定補足

MRB-50L LTEモードセットアップ

- 1 LTEモードの設定
- 2 使用回線モード切替

基本設定

目次

- 1 ログイン
- 2 ログインパスワードの変更
- 3 WAN設定
 - 3-1 PPPoE設定
 - 3-2 DHCP設定
 - 3-3 固定IP設定
- 4 LAN設定
 - 4-1 有線LAN設定
 - 4-2 無線LAN設定
 - 4-3 Wi-Fi設定
 - 4-4 クライアント固定IP設定
- 5 ブリッジモード
 - 5-1 メンテナンスアドレス設定
 - 5-2 動作モードの切替
 - 5-3 アクセス許可リスト
- 6 セキュリティ設定
 - 6-1 URLフィルタリング
 - 6-2 個別URLフィルタリング
 - 6-3 IPフィルタリング
 - 6-4 個別IPフィルタリング
- 7 グループ設定
 - 7-1 グループ編集
 - 7-2 コレダケトオス
 - 7-3 グループ別フィルタリング
- 8 ホワイトリスト申請/処理
 - 8-1 ホワイトリスト申請
 - 8-2 ホワイトリスト申請処理
- 9 TCPMSS設定
- 10 VPN接続
 - 10-1 VPN応答側(親)の設定
 - 10-2 VPN開始側(子)の設定

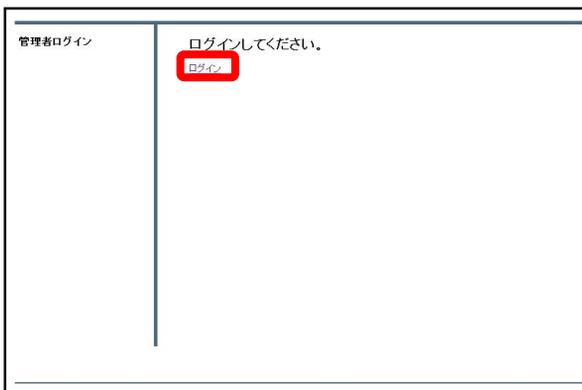
1, ログイン

MRBの操作を行うために管理コンソールにログインします。

 192.168.124.254

①管理コンソールにログインするため、ブラウザのURL入力部分に『192.168.124.254』と入力し、確定(Enter)してください。

※MRB-50内蔵Wi-Fiでのアクセスの場合、『192.168.123.254』と入力して下さい。



管理者ログイン

ログインしてください。

②左のような画面が表示されましたら『ログイン』をクリックしてください。



管理者ログイン

管理者ユーザ root
パスワード ●●●●

③管理者ユーザ欄に『root』、パスワード欄に『mr-5』と入力し、『ログイン』をクリックしてください。

表示/確認		設定	再起動	ログアウト
表示/確認	バージョン			
バージョン	ハードウェア	1.0.1		
ネットワーク設定	ソフトウェア	2.0.3		
WPA 無線LAN 有線LAN ルーティング	URLフィルタリング	1.0.1		
セキュリティ設定	Fフィルタリング	1.0.1		
URLフィルタリング ファイアウォール 匿名接続検知	匿名接続検知	1.0.1		
ホストリスト情報				
グループ設定				
プリンタ設定				
メンテナンスモード メンテナンスモード アクセス制御リスト				
情報				
ログ				

④左のような画面が表示されましたら、ログイン作業は完了です。

※管理者ユーザ/パスワードを正しく入れてもログイン出来ない場合。

192.168.124.254/show_login2.cgi

⑤ブラウザのURL入力欄に『http://192.168.124.254/show_login2.cgi』と入力し、確定(Enter)してください。

※MRB-50内蔵Wi-Fiでのアクセスの場合、『192.168.123.254/show_login2.cgi』と入力して下さい。

管理者ログイン

管理者ユーザ(リカバリ)

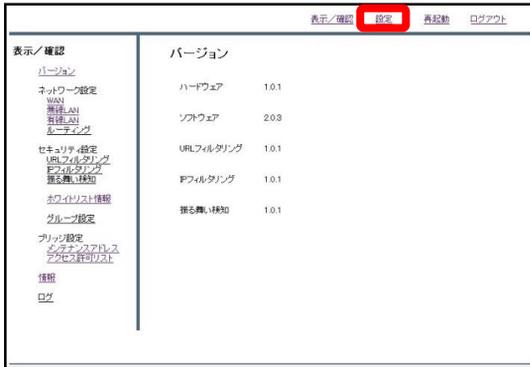
パスワード

ログイン

⑥左のようにログイン画面が表示されましたら、通常と同様に管理ユーザに『root』/パスワードに『mr-5』と入力してください。

2, ログインパスワード の変更

セキュリティ向上の為、 管理コンソールへのログインパスワードを変更します。



①管理画面にログインをし、右上の『設定』をクリックします。



②左下の『パスワード変更』をクリックします。



③入力欄に新しいパスワードを入力し、『変更』をクリックします。
(パスワードは8～16文字で設定してください)

管理者ログイン

管理者ユーザ root

パスワード ●●●●●●●●

ログイン

④設定後、ログイン画面が出てきますので、新しいパスワードを入力し、『ログイン』をクリックしてください。

表示/確認 設定 再起動 ログアウト

表示/確認	バージョン
バージョン	
ネットワーク設定	ハードウェア 1.0.1
無線LAN 有線LAN イーサネット	ソフトウェア 2.0.0
セキュリティ設定	URLフィルタリング 1.0.1
ウイルス対策 IPフィルタリング 匿名化機能	IPフィルタリング 1.0.1
ウイルスリスト情報	匿名化機能 1.0.1
グループ設定	
プリンタ設定	
メンテナンス アップデート アップデートリスト	
情報	
ログ	

⑤ログインに成功すれば、パスワード変更作業は完了です。

3, WAN設定

PPPoE設定

PPPoE接続でMRBを利用する場合の設定方法です。



①管理画面にログイン後、右上の『設定』をクリックし、左の『WAN』をクリックします。



②『PPPoE』をラジオボタンより選択し、『次へ』をクリックします。



③入力欄にプロバイダ情報を記入し、『次へ』をクリックします。

DHCP設定

DHCP接続のローカルルータでMRBを利用する場合の設定方法です。



①管理画面にログイン後、右上の『設定』をクリックし、左の『WAN』をクリックします。



②『DHCP』をラジオボタンより選択し、『次へ』をクリックします。



③『確認』をクリックして、設定は完了です。

固定IP設定

固定IP接続のローカルルータでMRBを利用する場合の設定方法です。



①管理画面にログイン後、右上の『設定』をクリックし、左の『WAN』をクリックします。



②『固定IP』をラジオボタンより選択し、『次へ』をクリックします。



③各項目を記入し、『次へ』をクリックします。

4, LAN設定

有線LAN設定

有線LAN接続でのゲートウェイの設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左の『有線LAN』をクリックします。



②『利用する』にチェックを入れ、IPアドレスとネットマスクを入力します。ここで入力したIPアドレスがデフォルトゲートウェイとなります。ゲートウェイの設定後、『DHCP設定』をクリックします。



③DHCPを利用する場合は『利用する』にチェックを入れ、前の画面で設定したネットワークに合わせてDHCPの開始アドレスと終了アドレスを入力します。特定のサーバを利用する場合は『配布ドメイン』『DNS』の欄に入力しますが、そうでない場合は『配布ドメイン』の欄に"local"と入力し、『次へ』をクリックします。



④ 『次へ』 をクリックします。



⑤ 内容を確認し、正しければ『確認』をクリックします。



⑥ 左のような画面が表示されましたら、設定は完了です。

無線LAN設定

無線LAN接続でのゲートウェイの設定を行います。

※MRB-50/MRB-50Lのみの設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左の『無線LAN』をクリックします。



②『利用する』にチェックを入れ、IPアドレスとネットマスクを入力します。ここで入力したIPアドレスがデフォルトゲートウェイとなります。ゲートウェイの設定後、『DHCP設定』をクリックします。



③ DHCPを利用する場合は『利用する』にチェックを入れ、前の画面で設定したネットワークに合わせてDHCPの開始アドレスと終了アドレスを入力します。特定のサーバを利用する場合は『配布ドメイン』『DNS』の欄に入力しますが、そうでない場合は『配布ドメイン』の欄に"local"と入力し、『次へ』をクリックします。



④ 『次へ』 をクリックします。



⑤ 内容を確認し、正しければ『確認』 をクリックします。



⑥ 左のような画面が表示されましたら、設定は完了です。

引き続き次ページからのWi-Fi設定マニュアルをご確認ください。

Wi-Fi設定

MRBでWi-Fiを利用する場合の設定方法です。

※MRB-50/MRB-50Lのみの設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左の『無線LAN』をクリックします。



②左下『WiFi設定』をクリックします。



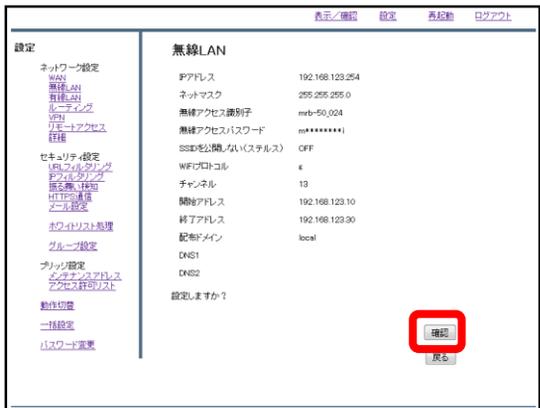
③以下の各項目を入力します。

- **無線アクセス識別子**...端末からWi-Fiを検索した際に表示されるIDです。
- **無線アクセスパスワード**...端末からWi-Fiでアクセスする際のパスワードです。
- **SSIDを表示しない(ステルス)**...チェックを入れた場合、端末のWi-Fi一覧に表示されなくなります。
- **WiFiプロトコル**...無線接続の際のプロトコルです。接続する端末に対応しているものを選択してください。
- **チャンネル**...無線のチャンネルです。できるだけ干渉の少ないものを選択してください。

入力が完了したら『次へ』をクリックします。



④ 『次へ』 をクリックします。



⑤ 内容を確認し、正しいければ『確認』をクリックします。



⑥ 左のような画面が表示されましたら、設定は完了です。

クライアント固定IP設定

MRBで端末の利用するIPを決定する場合の設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左の『有線LAN』をクリックします。



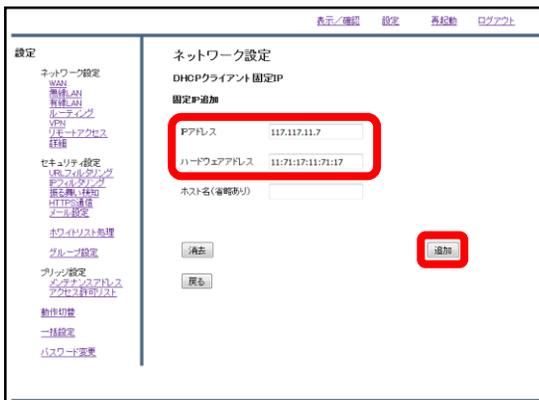
②右下『DHCP設定』をクリックします。



③『利用する』にチェックが入っていることを確認し、右下『クライアント固定IP』をクリックします。



④ 『追加』 をクリックします。



⑤ 端末に指定したいIPを『IPアドレス』に、その端末のMACアドレス『ハードウェアアドレス』に入力し『追加』をクリックします。



⑥ 内容を確認し、正しければ『追加』をクリックします。

表示/確認 設定 再起動 ログアウト

設定

ネットワーク設定

WAN
無線LAN
有線LAN
ルーティング
VPN
リモートアクセス
詳細

セキュリティ設定
IPフィルタリング
ファイアウォール
匿名化/詳細
HTTPS保護
メール保護

ホストリスト管理
グループ設定

ブリッジ設定
スタティックアドレス
アドレス許可リスト

動作確認
一括設定
パスワード変更

ネットワーク設定

DHCPクライアント固定IP

参照 ファイルが選択されていません。

アップロード(置換) アップロード(追加)

ダウンロード

戻る 消去 追加 修正 削除

IPアドレス	ハードウェアアドレス	ホスト名	修正	削除
192.168.1.23	F0:42:1C:89:4F:4C	trtclient001	○	✖
117.117.11.7	11:71:17:11:71:17	trtclient003	○	✖

⑦一覧を確認し、登録した端末が表示されていることを確認したら作業は完了です。



5, ブリッジモード

メンテナンスアドレス 設定

ブリッジモードで使用する際にMRBにアクセスするためのアドレスを設定します。



①管理画面にログイン後、右上の『設定』をクリックし、左下の『動作切替』をクリックします。



②下段の”ブリッジモード用メンテナンスアドレス設定”の『設定』をクリックします。



③入力欄に任意のIPアドレスとネットワークを記入し、『次へ』をクリックします。

(設定するIPはMRBを設置しているネットワークと別のセグメントに設定してください。)



④入力内容を確認し、内容が正しければ『確認』をクリックして設定は完了です。

※MRBの管理画面が開けなくなりますので、設定したメンテナンスアドレスは忘れないようにお願いします。

動作モードの切替

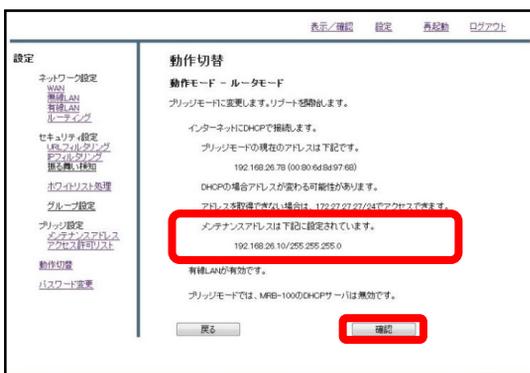
MRBの動作モード(ルータ/ブリッジ)を切り替える際の設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左下の『動作切替』をクリックします。



②上段の"動作モード"の『変更』をクリックします。



③設定したメンテナンスアドレスを確認し、よければ『確認』をクリックして設定は完了です。

※MRBのIPをDHCPで指定している場合に、ブリッジモードへの切り替えを行う場合は、メンテナンスアドレスの設定を先に行ってください。

アクセス許可リスト

MRBがブリッジモードの際、WAN側からMRBを含む配下の端末にアクセスが必要な場合に設定してください。



①管理画面にログイン後、右上の『設定』をクリックし、左の『アクセス許可リスト』をクリックします。



②画面中央の『追加』をクリックします。



③WAN側からアクセスする端末のIPアドレスを記入し、『追加』をクリックします。

※IPアドレスはネットワークではなくアクセスする端末ごとに記入してください。



④ 記入したIPを確認し、正しければ『追加』をクリックして作業は完了です。

6, セキュリティ設定

URLフィルタリング

URLフィルタの強度設定を行います。

※お客様からの要望がない限り、URLフィルタは『弱』に設定してください。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『URLフィルタリング』をクリックします。



②ラジオボタンよりフィルタリングのレベルを選択し、『次へ』をクリックします。



③設定を確認し、正しければ『確認』をクリックして設定は完了です。

個別URLフィルタリング 登録

特定のURLに対してのブロック/スルーの設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『URLフィルタリング』をクリックします。



②指定するURLをブロックする場合は『ブラックリスト』、ブロックを解除する場合は『ホワイトリスト』をクリックします。



③『追加』をクリックします。



④ 記入欄にブロック/スルーしたいURLを入力し、『追加』をクリックします。

※http://は入力しないでください。



⑤ URLを確認し、正しければ『追加』をクリックして設定は完了です。

IPフィルタリング

IPフィルタの強度設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『IPフィルタリング』をクリックします。



②ラジオボタンよりフィルタリングのレベルを選択し、『次へ』をクリックします。



③設定を確認し、正しければ『確認』をクリックして設定は完了です。

個別IPフィルタリング 登録

特定のIPに対してのブロック/スルーの設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『IPフィルタリング』をクリックします。



②指定するIPをブロックする場合は『ブラックリスト』、ブロックを解除する場合は『ホワイトリスト』をクリックします。



③『追加』をクリックします。



④ 記入欄にブロック/スルーしたいIPを入力し、『追加』をクリックします。

※ネットワーク単位で指定する場合は、IPの後ろに"/24"などセグメントを追加してください。



⑤ IPを確認し、正しければ『追加』をクリックして設定は完了です。

7, グループ設定

MRB配下のIPをセキュリティ設定ごとに区分します。

※グループ割当設定を行っていないIPはデフォルトグループに所属しています。



①管理画面にログインし、右上の『設定』をクリックし、左の『グループ設定』をクリックします。



②“編集”のラジオボタンより、設定を行うグループを選択し、『編集』をクリックします。



③『追加』をクリックします。



④単独で指定する場合は"IPアドレス"、範囲で指定する場合は"IPアドレス範囲"のラジオボタンをクリックし、例に習って"ルール"の記入欄にIPアドレスを記入します。



⑤入力したIPアドレスとタイプを確認し、正しければ『追加』をクリックして設定は完了です。

「コレダケトオス」は許可されたIP/URL以外にはアクセスが出来ない、特別なグループです。



①管理画面にログインし、右上の『設定』をクリックし、左側の『グループ設定』をクリックします。



②「編集」のラジオボタンより『コレダケトオス』を選択し、『編集』をクリックします。



③『追加』をクリックします。



①単独で指定する場合は"IPアドレス"、範囲で指定する場合は"IPアドレス範囲"のラジオボタンをクリックし、例に習って"ルール"の記入欄にIPアドレスを記入します。



②入力したIPアドレスとタイプを確認し、正しければ『追加』をクリックして設定は完了です。

グループごとのフィルタリング強度を設定します。

※グループ別フィルタリング設定はIPを割り当てているグループにのみ行ってください。



①右上の『設定』をクリックし、左側の『グループ設定』をクリックします。



②"編集"のラジオボタンより、設定を行うグループを選択し、『編集』をクリックします。



③『URLフィルタリング』『メール設定』等をクリックすることで、選択したグループのフィルタリング設定を行うことができます。

(具体的な設定方法に関しては、各マニュアルをご確認ください。)

8, ホワイトリスト 申請/処理

閲覧しようとしたWebサイトがブロックされている場合、管理者の方へブロック解除の申請を行うことができます。

URLフィルターによりブロックされました。

サイト	http://actions.yahoo.co.jp
フィルター	オークション
IPアドレス	192.168.26.24

サイトの再評価を申請。
反映されるまでに、数日要します。
(全てのTRTSに反映されます。)

ご注意ください。
10分間アクセス可能になります。
また同じIPアドレスのページも数回可能になり、ログインします。

管理者としての設定が必要です。
管理者の方に伝えてください。
(このTRTSのみ反映されます。)

①Webサイトがブロックされた場合、左のような画面が表示されます。右下『ホワイトリストに登録を申請』をクリックしてください。

ホワイトリストに登録を申請しました。管理者の方に連絡してください。

対象URL <http://actions.yahoo.co.jp>

②左のような画面が表示されましたら、申請は完了です。管理者の方に連絡してください。

ホワイトリスト 申請処理

管理者の方は利用者からのWebサイトアクセス許可の申請に対して処理を行うことができます。



①管理画面にログイン後、右上の『設定』をクリックし、左の『ホワイトリスト処理』をクリックします。



②申請があったWebサイトに対して、ラジオボタンにより"許可"、"拒否"を選択し、『設定』をクリックします。



③対応を確認し、正しければ『設定』をクリックして処理は完了です。

9, TCPMSS設定

通信環境に応じてパケットの長さを整える設定です。ADSL通信、ひかり電話のルータが上位に存在する場合に設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左の『詳細』をクリックします。



②TCPMSS(バイト)の記入欄を"1414"に変更し、『次へ』をクリックします。



③入力を確認し、正しければ『確認』をクリックして設定は完了です。

10, VPN接続

VPN応答側(親)の設定

MRB同士でVPNを構築する際、固定IPを使用する側の設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『VPN』をクリックします。



②『追加』をクリックします。



③以下の表を参考に設定項目を記入欄に入力します。

設定...有効
タイプ...応答側
リモートサイト...開始側と取り決めた任意のID
ローカルサイト...選択せず、空欄
事前共通鍵...開始側と取り決めた任意のワード
チェックアドレス...開始側のLAN側IPアドレス



④入力が終わりましたら、下側の『追加』をクリックします。



⑤VPN相手のネットワークアドレスとネットマスクを記入し、『追加』をクリックします。



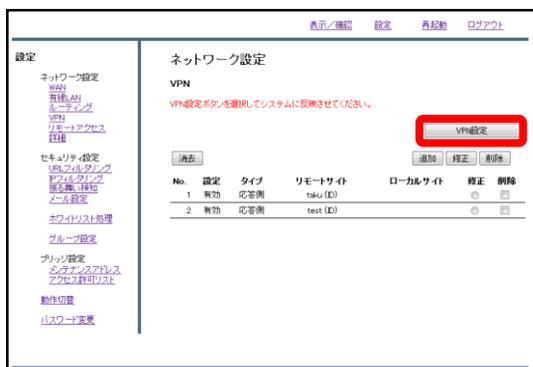
⑥内容を確認し、正しければ『追加』をクリックします。



⑦右上の『VPN追加』をクリックします。



⑧設定内容を確認し、正しければ『VPN追加』をクリックします。



⑨『VPN設定』をクリックし、設定を反映させたら完了です。

VPN開始側(子)の設定

MRB同士でVPNを構築する際、固定IPを使用しない側の設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『VPN』をクリックします。



②『追加』をクリックします。



③以下の表を参考に設定項目を記入欄に入力します。

設定...有効
タイプ...開始側
リモートサイト...応答側のWAN側IPアドレス
ローカルサイト...IDを選択し、応答側と取り決めた任意のIDを入力
事前共通鍵...応答側と取り決めた任意のワード
チェックアドレス...開始側のLAN側IPアドレス

表示の確認 設定 再起動 ログアウト

設定

ネットワーク設定

VPN追加

削除 戻る VPN追加

No. 2

設定 有効 無効

タイプ 開始側 応答側

リモートサイト 192.168.111.11 （開始側はP、応答側はID）

ローカルサイト ガローバル固定IP ID

（開始側の場合のみ） 12.34.56.78

事前共通鍵 *****

チェックアドレス 192.168.124.254 （相手側のLANアドレス）

リモートネットワーク ネットワーク

④入力が終わりましたら、下側の『追加』をクリックします。

表示の確認 設定 再起動 ログアウト

設定

ネットワーク設定

VPN

No. 2 リモートネットワーク追加

ネットワーク	192.168.124.0
ネットマスク	255.255.255.0

削除 戻る 追加

⑤VPN相手のネットワークアドレスとネットマスクを記入し、『追加』をクリックします。

表示の確認 設定 再起動 ログアウト

設定

ネットワーク設定

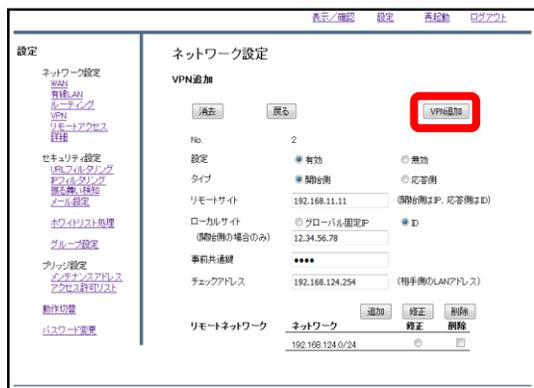
VPN

No. 2 リモートネットワーク追加 確認

ネットワーク	192.168.124.0
ネットマスク	24

戻る 追加

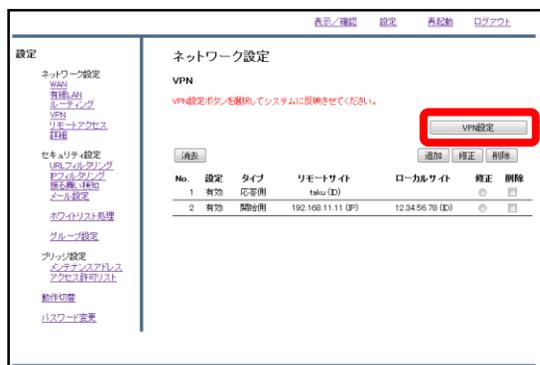
⑥内容を確認し、正しければ『追加』をクリックします。



⑦右上の『VPN追加』をクリックします。



⑧設定内容を確認し、正しければ『VPN追加』をクリックします。



⑨『VPN設定』をクリックし、設定を反映させたら完了です。

HTTPS フィルタリング

・目次

- 1 HTTPSフィルタリング設定
- 2 証明書のダウンロード
- 3 証明書のインポート
 - 3-1 IE/Chromeの場合
 - 3-2 FireFoxの場合
- 4 クライアント証明書を利用する場合
 - 4-1 対象外URL設定
 - 4-2 対象外IP設定

1, MRBの設定

HTTPSフィルタリング機能により、暗号化されたWebサイトもフィルタリングが可能になります。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS通信』をクリックします。



②『利用する』を選択し、『次へ』をクリックします。



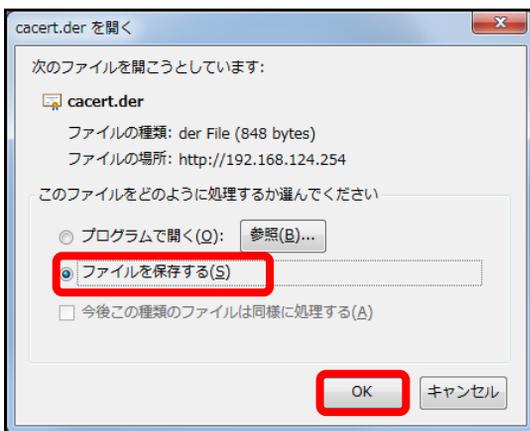
③『確認』をクリックして設定は完了です。

2, 証明書の ダウンロード

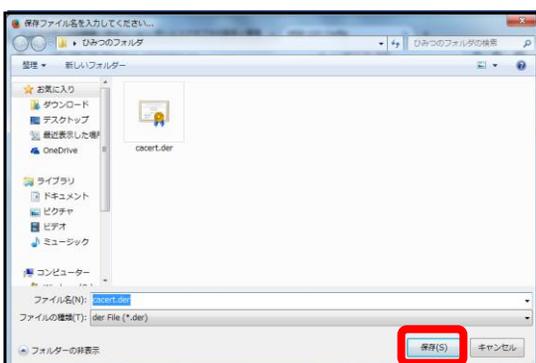
HTTPSフィルタリング機能で使用する証明書をダウンロードします。



①管理画面にログイン後、左側『情報』をクリックし、『証明書ダウンロード』をクリックします。



②左のようなダイアログが表示されましたら、ラジオボタンより『ファイルを保存する』を選択し、『OK』をクリックします。



③分かりやすいフォルダ(デスクトップ等)に移動し、『保存』をクリックしましたら、証明書のダウンロードは完了です。

3, 端末での設定

IE/Chrome利用の場合

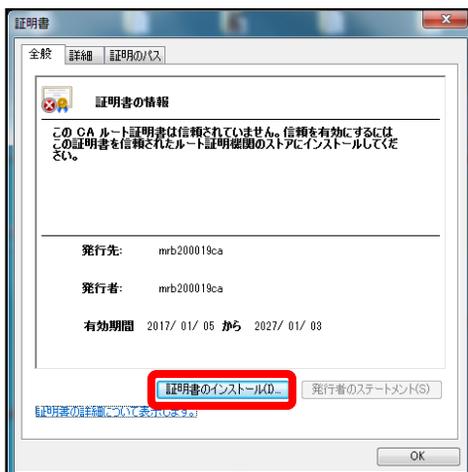
IEまたはChromeをご利用の場合、ダウンロードしたMRBの証明書をインポートする際の手順です。



①ダウンロードした証明書をダブルクリックします。



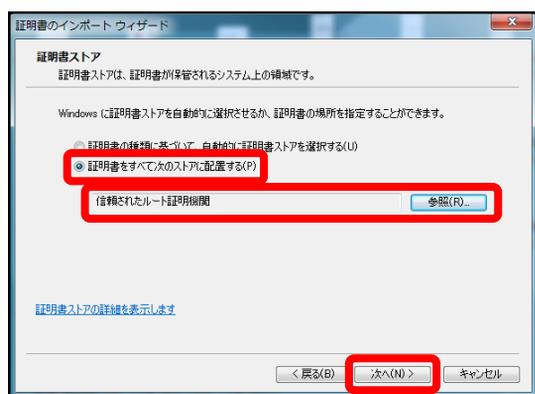
②左のようなダイアログが表示されますので、『開く』をクリックします。



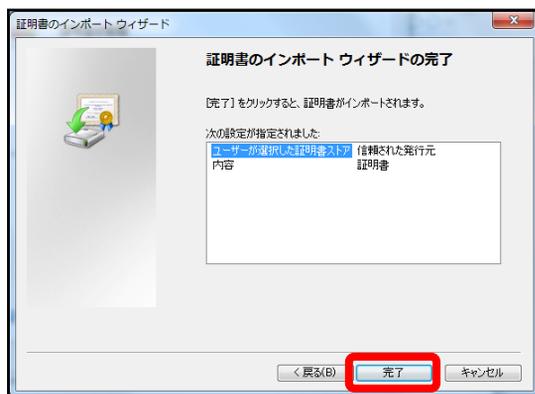
③『証明書のインストール』をクリックします。



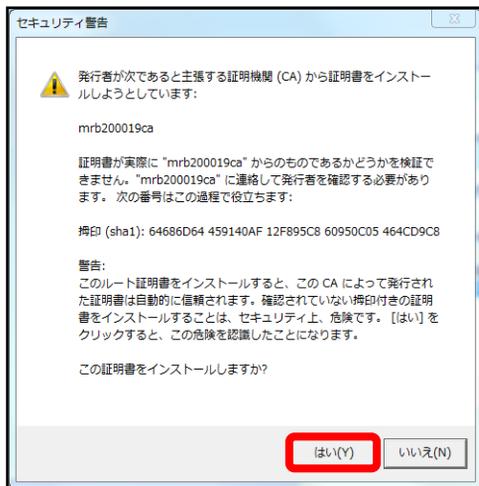
④左のようなポップアップが表示されますので、『次へ』をクリックします。



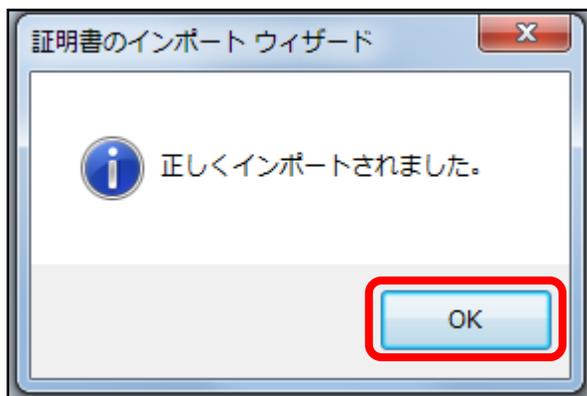
⑤ラジオボタンより『証明書をすべて次のストアに配置する』を選択し、『参照』より“信頼されたルート証明機関”を選択して『次へ』をクリックします。



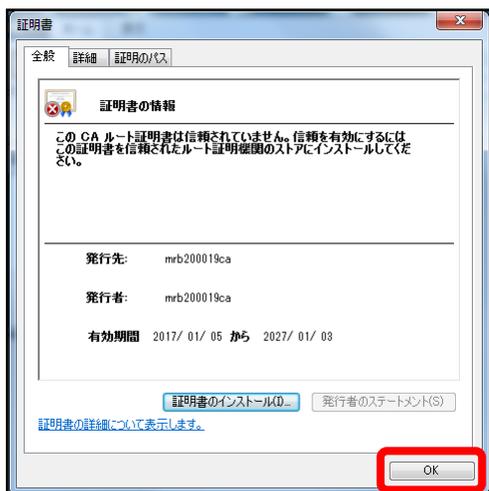
⑥内容を確認し、正しければ『完了』をクリックします。



④左のような警告が表示されますが、『はい』をクリックします。



⑦左のようなポップアップが表示されましたら『OK』をクリックします。



⑧『OK』をクリックして証明書のインポート作業は完了です。

FireFox利用の場合

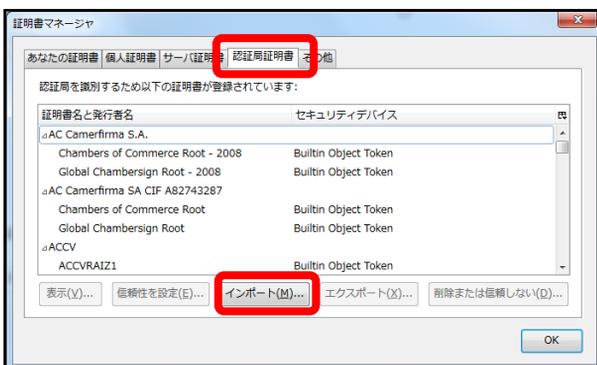
Firefoxをご利用の場合、ダウンロードしたMRBの証明書をインポートする際の手順です。



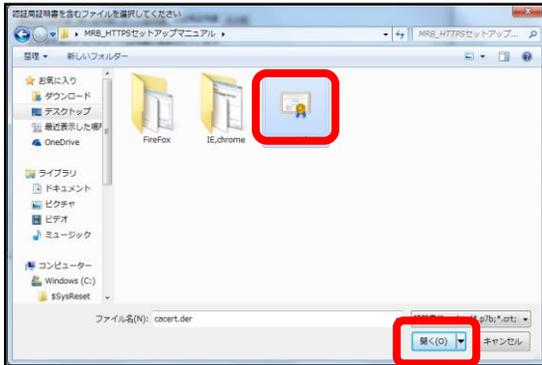
①Firefoxのブラウザを開き、右上の『メニュー』より『オプション』を選択します。



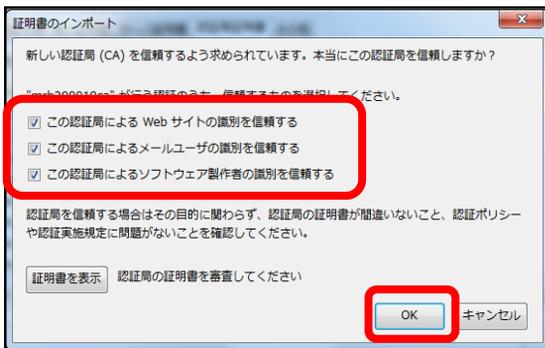
②左側『詳細』をクリックし、『証明書』タブより『証明書を表示』をクリックします。



③ポップアップが表示されましたら、『認証局証明書』タブより『インポート』をクリックします。



④ダイアログが表示されますので、ダウンロードした証明書を選択し、『開く』をクリックします。



⑤表示される3つのチェックボックスの全てにチェックを入れて『OK』をクリックします。



⑥証明書一覧に発行者名"Technol"の『mrb...』という証明書があることを確認したら、『OK』をクリックして証明書のインポートは完了です。

4, クライアント証明書 を利用する場合

対象外URL設定

HTTPSフィルタリングを活用している際にネットバンキング等でクライアント証明書を使用する場合に行う設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS通信』をクリックします。



②『対象外URL』をクリックします。



③『追加』をクリックします。



④URL記入欄にクライアント証明書を使用するサイトのURLを入力し、『追加』をクリックします。

※http://の入力は不要です。



⑤入力したURLを確認し、正しければ『追加』をクリックして設定は完了です。

対象外IP設定

HTTPSフィルタリングを活用している際にネットバンキング等でクライアント証明書を使用する場合に行う設定です。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『HTTPS通信』をクリックします。



②『対象外IP』をクリックします。



③『追加』をクリックします。



④IP記入欄にクライアント証明書を使用するサイトのIPアドレスとサブネットマスク長を入力し、『追加』をクリックします。

※サブネットマスク長は入力を省略した場合、32に設定されます。



⑤入力したIPアドレスを確認し、正しければ『追加』をクリックして設定は完了です。

メールフィルタリング

MRBを経由したメール受信の際、スパムとウイルスの判定を行うための設定マニュアルです。

※現在動作を保証しているのはOutlookのみです。

・目次

- 1 Outlookの設定確認
 - 1-1 メールアカウント設定の確認
- 2 MRBの設定
 - 2-1 メール検疫機能の設定
 - 2-2 許可アドレス設定
 - 2-3 検知アドレス設定
- 3 SSLでメール受信をご利用の場合
 - 3-1 証明書のダウンロード
 - 3-2 証明書の導入

1, Outlookの設定確認

メールアカウント設定 の確認

MRBの設定を行う前にOutlookでのメール設定を確認します。

①Outlookを起動し、左上の『ファイル』をクリックします。

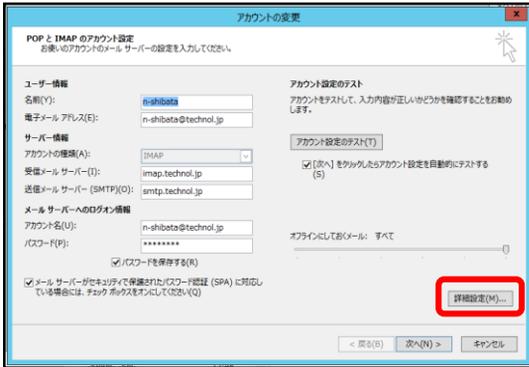


②『情報』タブより『アカウントの設定』をクリックします。

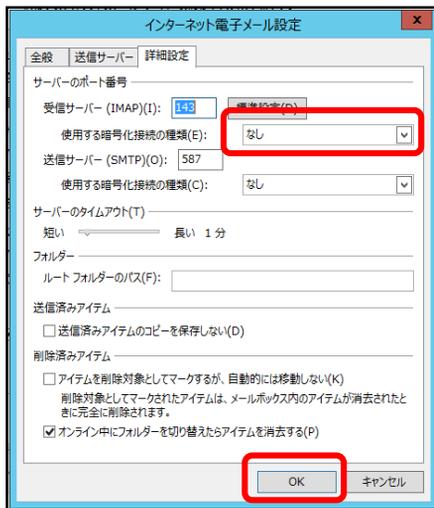


③設定を行うメールアドレスをダブルクリックします。



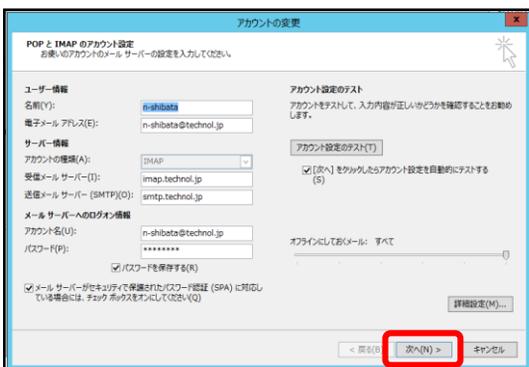


④ 『詳細設定』 をクリックします。

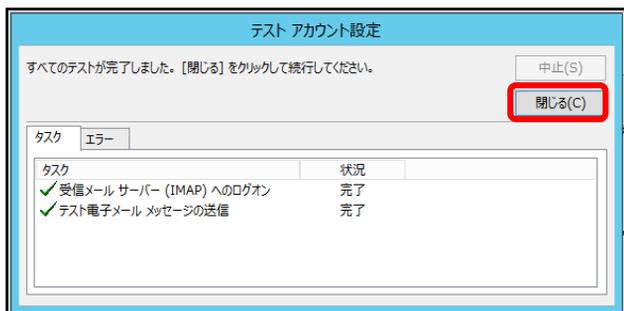


⑤ 『詳細設定』 タブを開き、“受信サーバー”の“使用する暗号化接続の種類”を確認します。

『SSL/TLS』もしくは『STARTTLS』と指定されていた場合は**“3,SSLでメール受信をご利用の場合”**に従って証明書のインポート作業を行って下さい。確認後、『OK』をクリックします。



⑥ 『次へ』 をクリックします。



⑦接続確認が行われますので、終了後『閉じる』を押して確認作業は完了です。

2, MRBの設定

メール検疫機能の設定

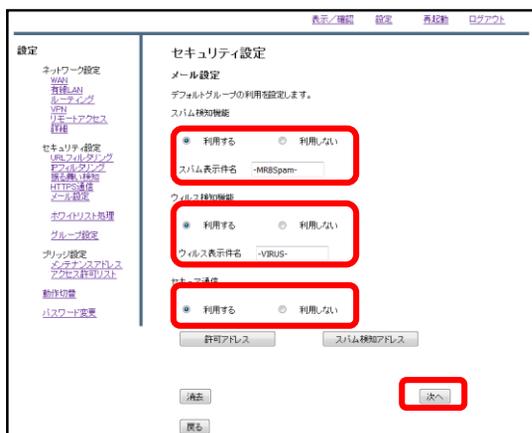
MRBを経由するメールを検疫するための設定を行います。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『メール設定』をクリックします。

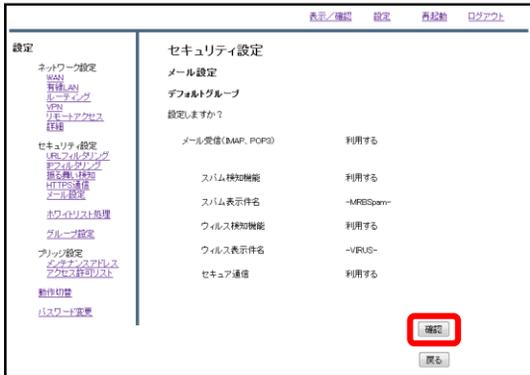


②メール受信のラジオボタンより『利用する』を選択し、『次へ』をクリックします。



③スパム検知、ウイルス検知を利用する場合はそれぞれのラジオボタンより『利用する』を選択し、メールの受信をSSLで行っている場合はセキュア通信のラジオボタンより『利用する』を選択して『次へ』をクリックします。

※スパム検知は送信元アドレス、ウイルス検知は添付ファイルをそれぞれチェックします。



④設定内容を確認し、正しければ『確認』をクリックして設定は完了です。

信頼できる宛先がスパムメールと判定される場合、許可アドレスとして設定します。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『メール設定』をクリックします。



②メール受信のラジオボタンより『利用する』を選択し、『次へ』をクリックします。



③『許可アドレス』をクリックします。



④ 『追加』 をクリックします。



⑤ メールアドレス記入欄にスパム判定から除外するメールアドレスを入力し、『追加』 をクリックします。



⑥ 入力したメールアドレスを確認し、正しければ『追加』 をクリックして設定は完了です。

検知アドレス設定

スパムメールとして判定させたいメールアドレスが存在する場合、
検知アドレスとして設定します。



①管理画面にログイン後、右上の『設定』をクリックし、左側の『メール設定』をクリックします。



②メール受信のラジオボタンより『利用する』を選択し、『次へ』をクリックします。



③『スパム検知アドレス』をクリックします。



④『追加』をクリックします。



⑤メールアドレス記入欄にスパムとして検知させたいメールアドレスを記入し、『追加』をクリックします。



⑥入力したメールアドレスを確認し、正しければ『追加』をクリックします。

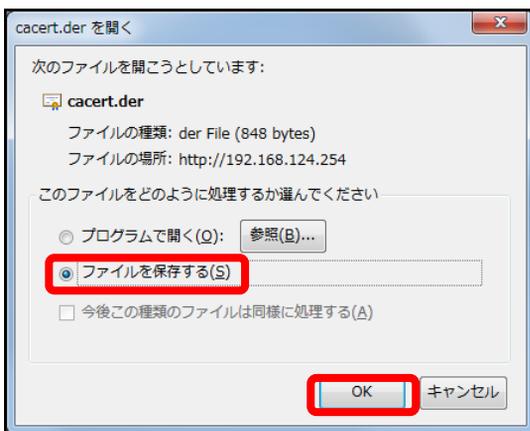
3, SSLでメール受信を ご利用の場合

証明書のダウンロード

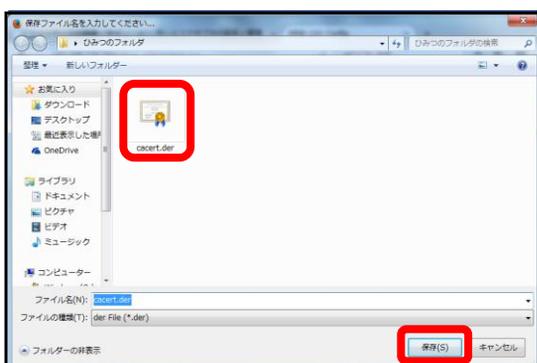
SSLで受信したメールを検疫する際の証明書をダウンロードします。



①管理画面にログイン後、左側『情報』をクリックし、『証明書ダウンロード』をクリックします。



②左のようなダイアログが表示されましたら、ラジオボタンより『ファイルを保存する』を選択し、『OK』をクリックします。



③分かりやすいフォルダ(デスクトップ等)に移動し、『保存』をクリックしましたら、証明書のダウンロードは完了です。

証明書のインポート

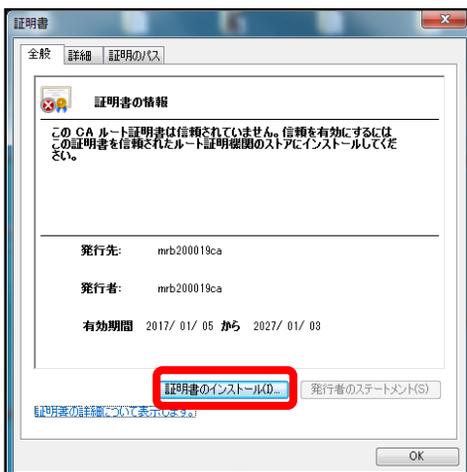
SSLで受信したメールを検疫する際、ダウンロードしたMRBの証明書をインポートする際の手順です。



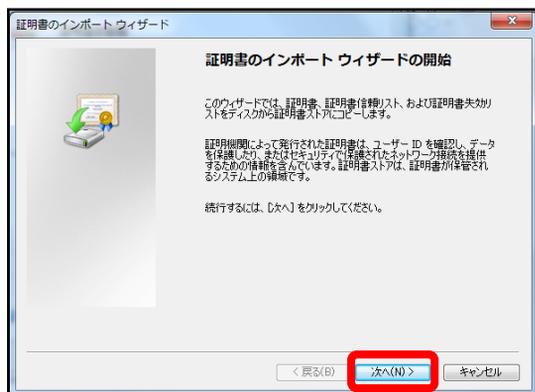
①ダウンロードした証明書をダブルクリックします。



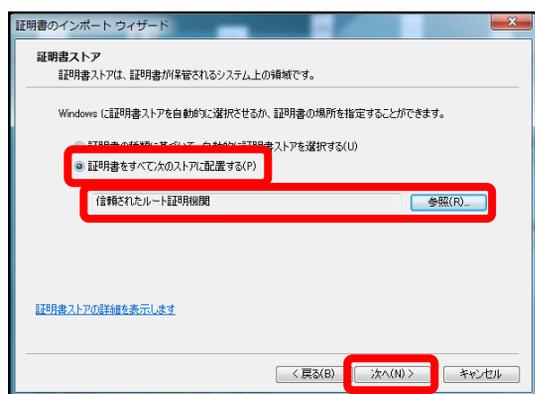
②左のようなダイアログが表示されますので、『開く』をクリックします。



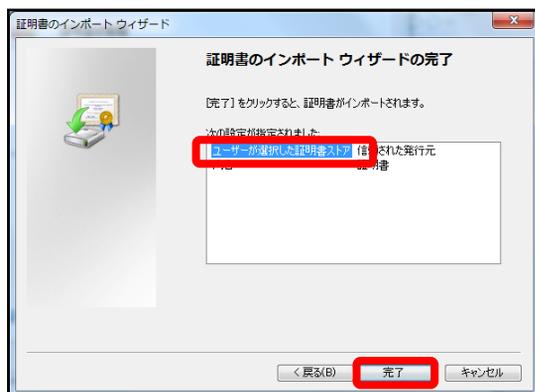
③『証明書のインストール』をクリックします。



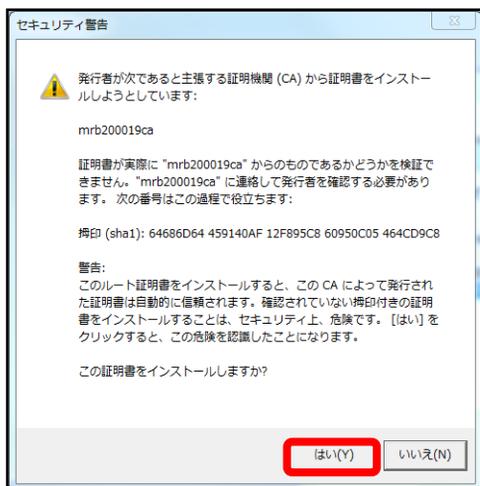
④左のようなポップアップが表示されますので、『次へ』をクリックします。



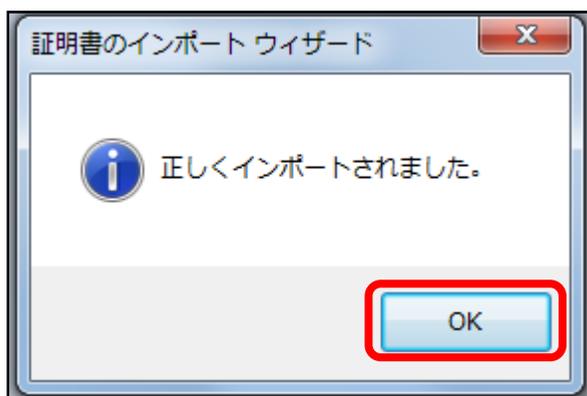
⑤ラジオボタンより『証明書をすべて次のストアに配置する』を選択し、『参照』より“信頼されたルート証明機関”を選択して『次へ』をクリックします。



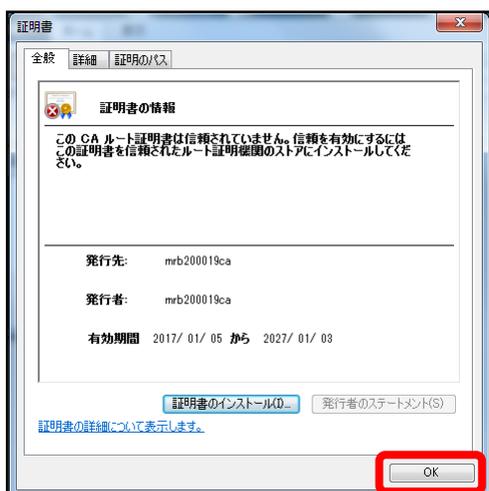
⑥内容を確認し、正しければ『完了』をクリックします。



④左のような警告が表示されますが、『はい』をクリックします。



⑦左のようなポップアップが表示されましたら『OK』をクリックします。



⑧『OK』をクリックして証明書のインポート作業は完了です。

プロフェッショナル モードでの機能

・目次

1 本体設定のバックアップ

1-1 バックアップファイルの取得

1-2 バックアップファイルの反映

2 プロフェッショナルモードによる本体設定変更

2-1 プロフェッショナルモードについて

2-2 設定ファイルの編集

2-3 ネットワーク設定

2-4 フィルタリング設定

2-5 WANモード切り替え (MRB-50L専用設定)

2-6 プロフェッショナルモード固有の設定

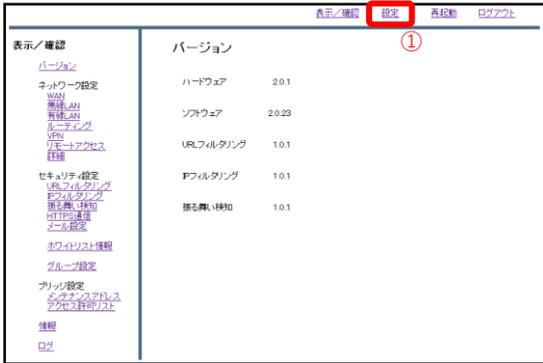
3 プロフェッショナルモード設定補足

3-1 リモートアクセス設定について

3-2 VPN設定について

1, 本体設定の バックアップ

MRBの設定ファイルバックアップの為、MRBの設定ファイルをエクスポートします。



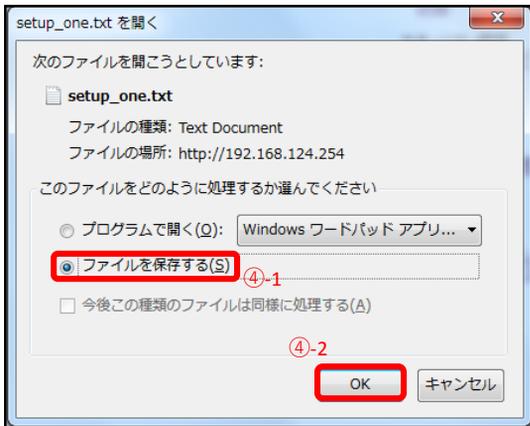
①MRBにログイン後、右上の『設定』をクリックします。



②設定項目左下の『一括設定』をクリックします。



③『ダウンロード』をクリックします。



④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。

バックアップファイル の反映

予め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』をクリックします。



②設定項目左下の『一括設定』をクリックします。



③『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ます。その後『設定』をクリックします。(ブラウザによってはドラッグ&ドロップでも選択が可能です)



④ 『設定』 をクリックします。



⑤左のような画面が表示され、設定は完了です。

2, プロフェッショナル モードによる設定変更

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합니다。

- ・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합니다。

- ・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。

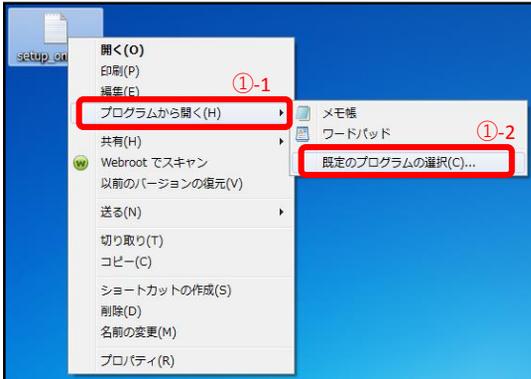
- ・リモートアクセス設定
- ・URLカテゴリフィルタリング設定

※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

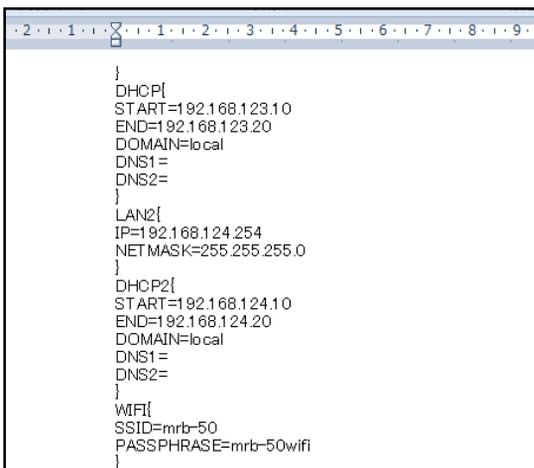
本体設定の一括変更のため、予めダウンロードした設定ファイルを編集します。



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。

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 }	<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
VPN設定(開始側)	VPN{ 2eb84e83830b72c05d3b12dfd05ced16 1 1 1 mr-5 61.51.41.31 2 test 192.168.11.0 }	<ul style="list-style-type: none"> 固定IPでのVPN：1 IDでのVPN：2 ・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 <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>

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：4 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 }	・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。
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
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 }	・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/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
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) "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)</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) ・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。</p>
https通信検知	<pre>HTTPS_9{ HTTPS=ON / OFF }</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) "HTTPS="：利用する場合は"ON"</p>
https通信のURL ホワイトリストの 設定	<pre>URL_HTTPS_9{ ea0ea7696d6d44dd79e31a33bd112585 0 www.aaa.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) ・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。</p>
https通信のIP ホワイトリストの 設定	<pre>IP_HTTPS_9{ ca87c597a0e1488b3c0e721db0303fae 11.22.33.44 32 }</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) ・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。</p>

WANモード切替/LTE設定 (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)	WAN_USE{ 1 }	WAN側使用回線を指定。 記載する数字は 有線回線：1
WANモード設定 (LTE回線)	WAN_USE{ 2 }	LTE回線：2 に対応。
LTE設定	LTE{ APN=technol.com ID=example@technol.com PASS=password IP= GATEWAY= DNS1= DNS2= }	“APN=”：APN “ID=”：ID “PASS=”：パスワード 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
URLフィルタの カテゴリ指定	<pre>URL_DENY_CAT_10{ 1 2 3 }</pre>	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	<pre>URL_LEVEL_9{ 10 }</pre>	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。
<p>※数字とカテゴリの対応一覧は次ページにあります</p>		

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。

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>	"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。

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	

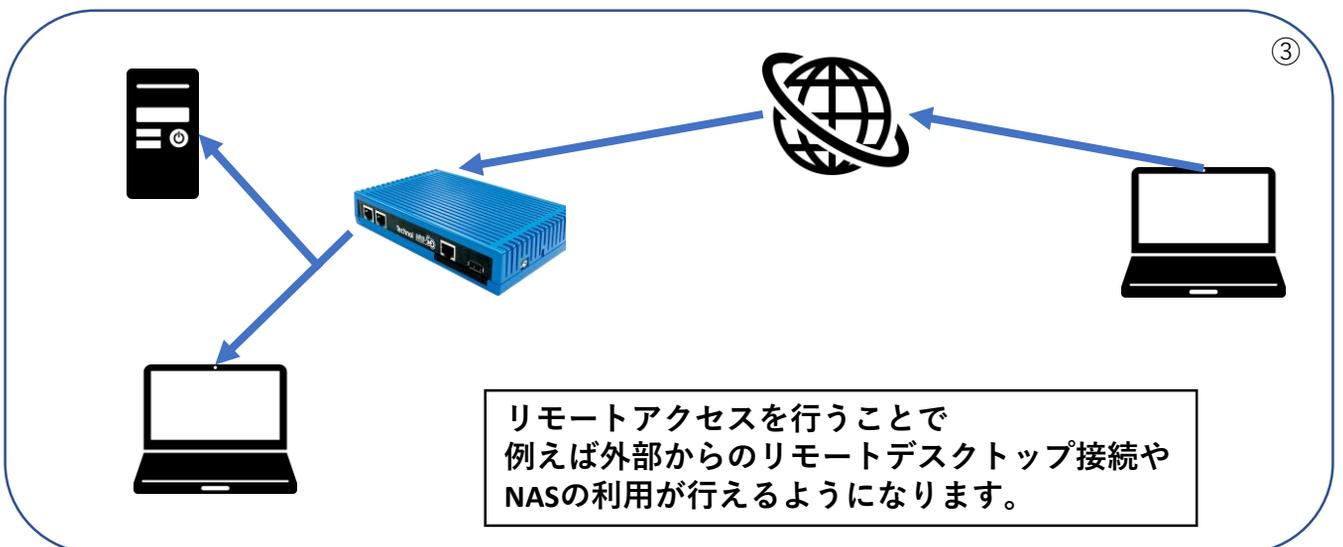
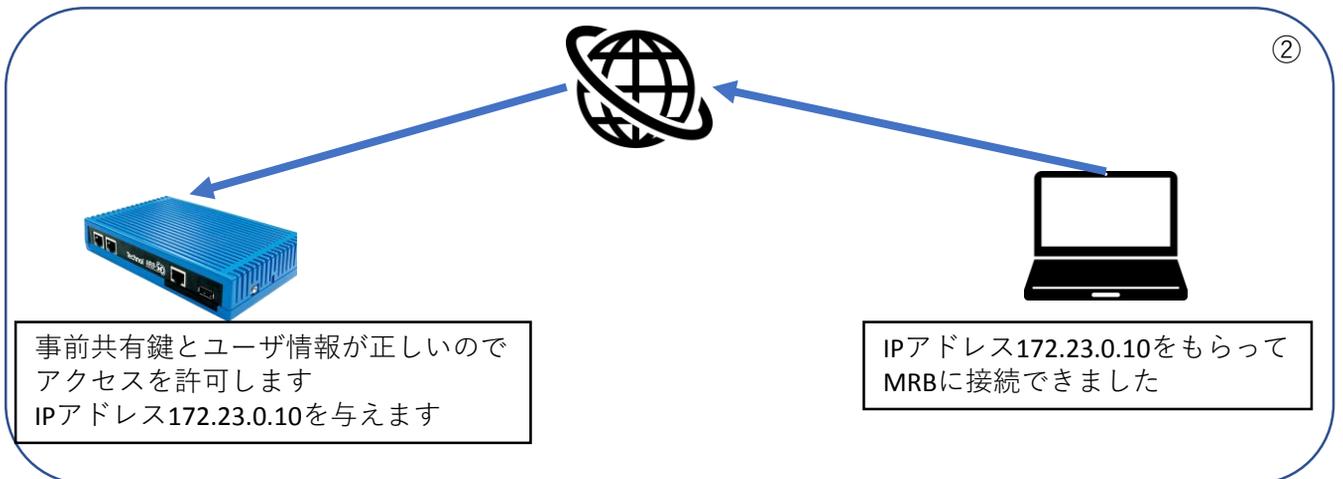
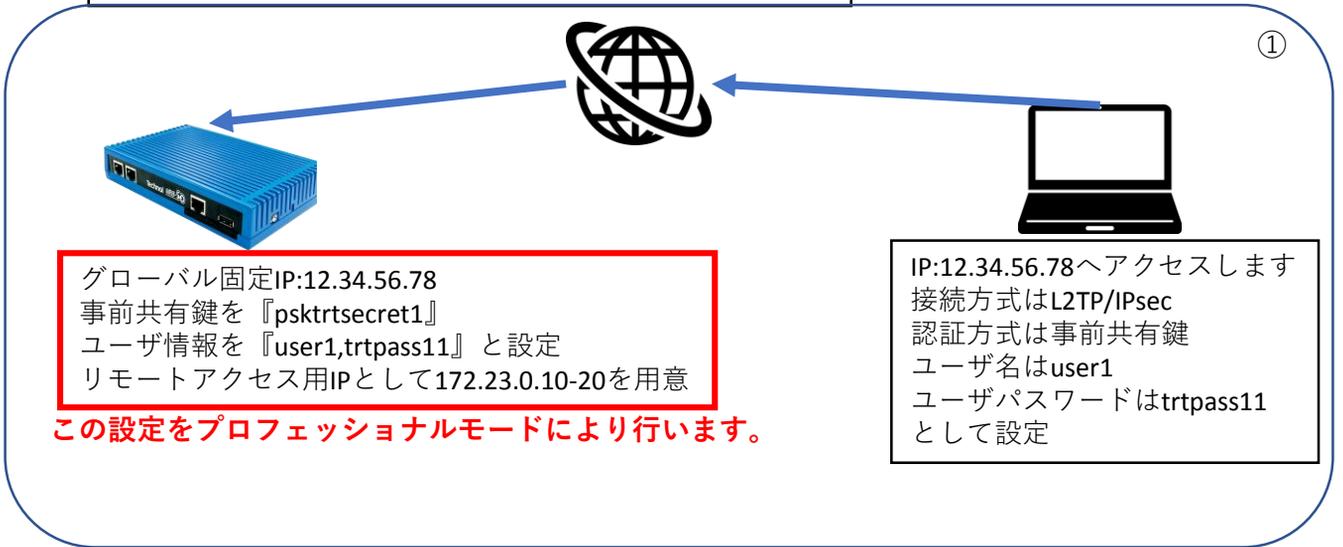
※2017/9/6時点での一覧となります。

3, プロフェッショナル モード設定補足

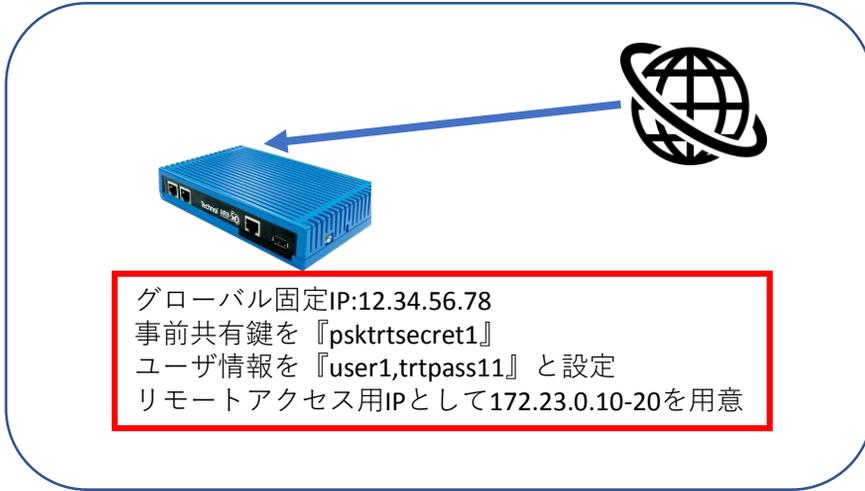
リモートアクセス設定 について

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
}
    
```

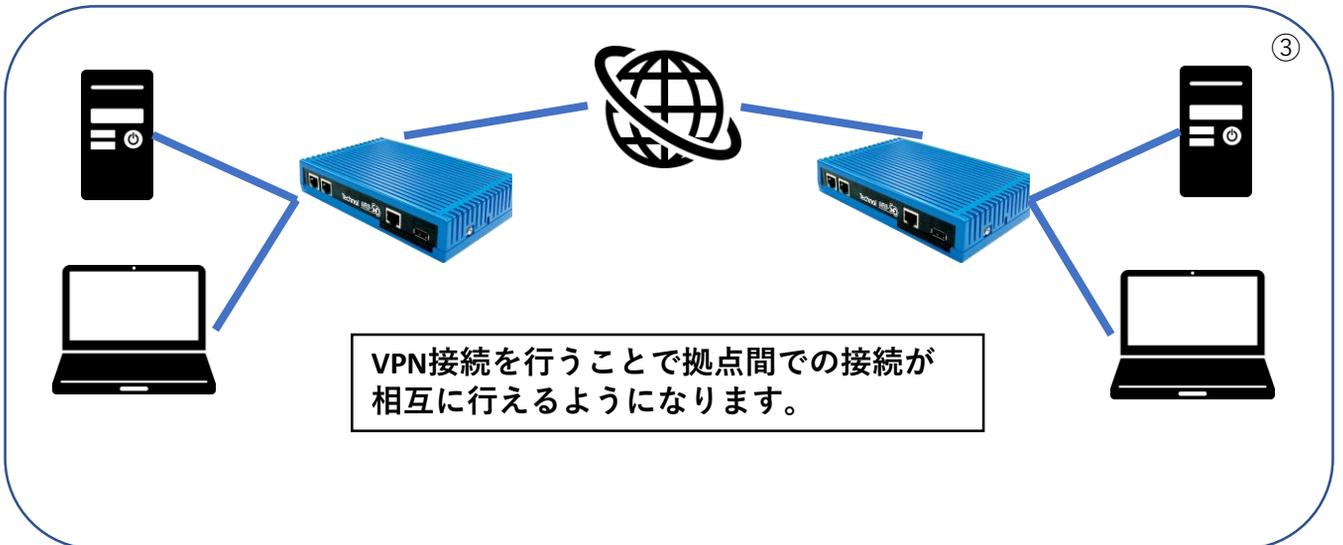
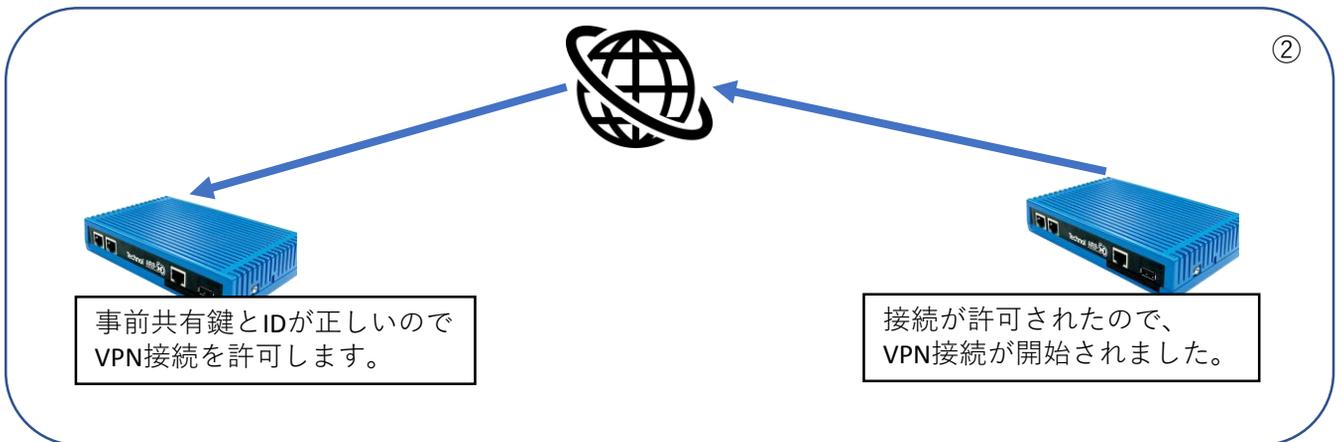
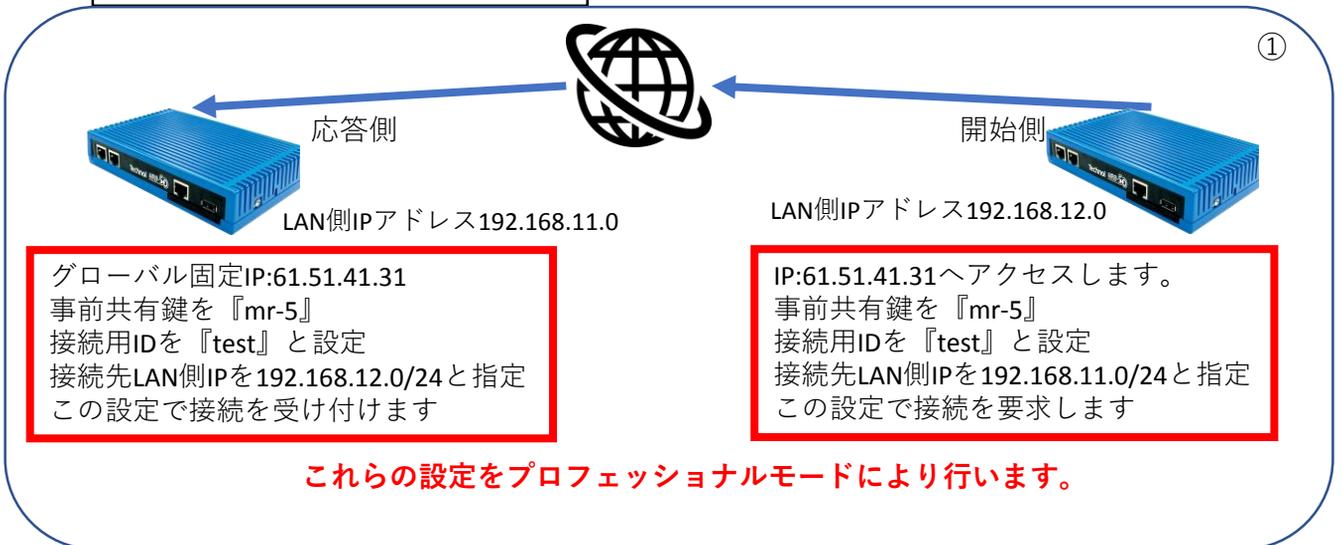
以下の記入例に従って、左図のように設定ファイルに項目を追加/変更し保存することで、リモートアクセス設定を行うことができます。

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

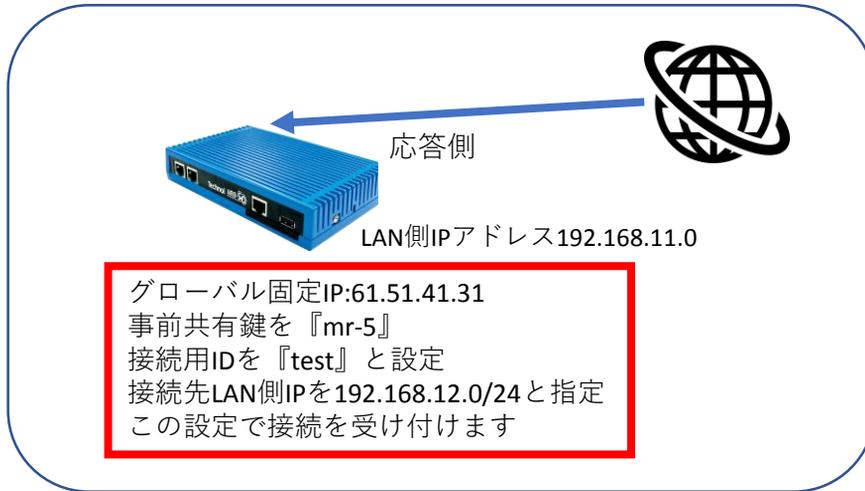
VPN設定についての詳細説明です。

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。



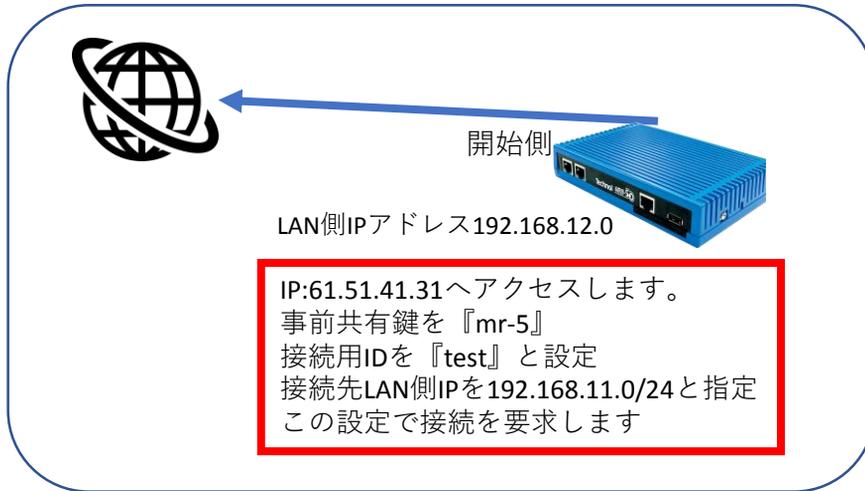
```
VPN{
08a68eec37af94301db96679e95673ca 1 1 2 mr-5 test 0 * 192.168.12.0
}
VPN_NET{
b0abb130d1f685921d7bd770e834de81 1 192.168.12.0 24
}
```

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	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
	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
}		
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。

MRB-50L LTEモードセッ
トアップ

・目次

- 1 LTEモードの設定
- 2 使用回線モード切替

1, LTEモードの設定

使用するSIMカードに合わせたLTE回線の設定を行います。



① MRB-50LにSIMカードを図の向きでカチッと音がするまで挿入します。

※対応しているSIMカードのサイズは標準SIMサイズです。



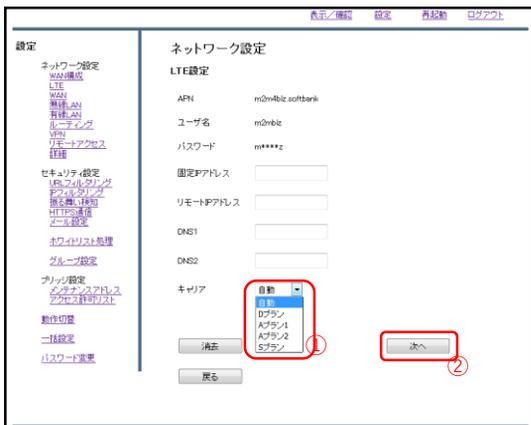
②付属のアンテナを”LTE ANT1”と”LTE ANT2”と書かれた部分に取り付けます。



③管理画面にログインし、右上『設定』をクリックし、左側『LTE』をクリックします。

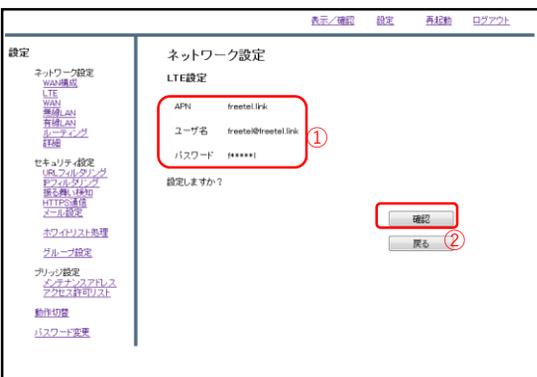


④挿入したSIMカードのAPN,ユーザ名,パスワードを記入し、『詳細』をクリックします。



⑤挿入したSIMのキャリアをプルダウンより選択し、『次へ』をクリックします。なお、選択肢の対応は以下のとおりです。

- | | |
|-------|----------------|
| 自動 | : 自動識別 |
| Dプラン | : Docomo |
| Aプラン1 | : au(UQmobile) |
| Aプラン2 | : au(Mineo) |
| Sプラン | : SoftBank |



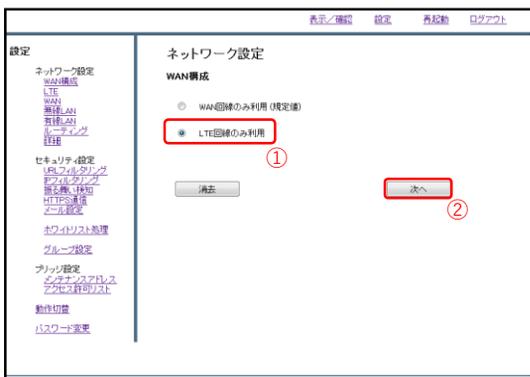
⑥入力内容を確認し、正しければ『確認』をクリックします。

2, 使用回線モード切替

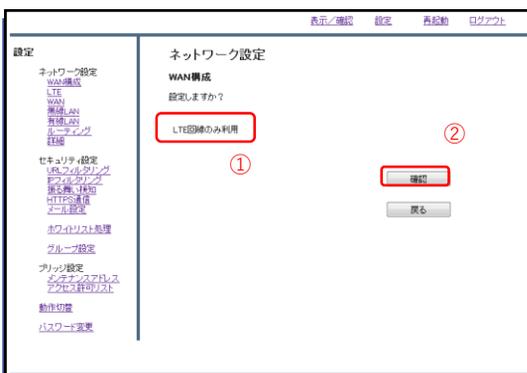
使用するWAN回線を切り替えます。



①右上の『設定』をクリックし、左側『WAN構成』をクリックします。



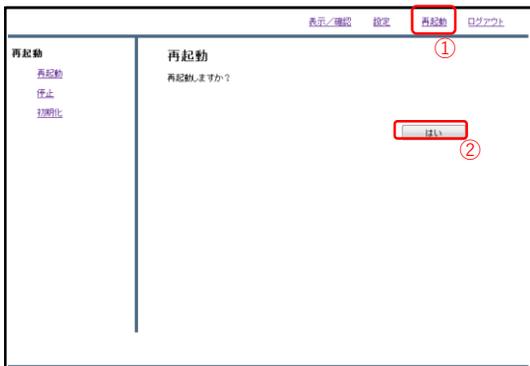
②ラジオボタンより『LTE回線のみ利用』を選択し、『次へ』をクリックします。



③入力した設定を確認し、正しければ『確認』をクリックします。



④左のような画面が表示されましたら、設定は完了です。



⑤右上『再起動』をクリックし、『はい』をクリックします。再起動完了後、再度管理画面にログインします。



⑥ログイン完了後、左下『情報』をクリックし、『LTE回線使用状態』が“接続中”となっていることを確認し、設定は完了です。

※WAN側を有線回線に切り替える場合は、『WAN構成』にて『WAN回線のみ使用』を選択して設定を行った後、別紙“MRB-50かんたんセットアップマニュアル”をご確認の上、WAN回線のセットアップを行って下さい。