

2019/01/08 : ver. 1.0.0

### ·全体目次 1/2

基本設定

P. 4

- 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
- 11 ログ閲覧

#### HTTPSフィルタリング P.87

- 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

### ·全体目次 2/2



- 1 LTEモードの設定
- 2 使用回線モード切替



·基本設定 目次 1/2

1	ログイン	P. 7
2	<u>ログインパスワードの変更</u>	P. 10
3	WAN設定	P. 13
	B-1 PPPoE設定	
	3-2 DHCP設定	
	3-3 固定IP設定	
4	LAN設定	P. 22
	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	P. 36
	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	P. 45
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	

### ·基本設定 目次 2/2

<u></u> <u>グループ設定</u>	P. 56
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	P. 65
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	P. 70
10 VPN接続	P. 72
10 <u>VPN接続</u> 10-1 IKEv2:VPN応答側(親)の設定	P. 72
10 <u>VPN接続</u> 10-1 IKEv2:VPN応答側(親)の設定 10-2 IKEv2:VPN開始側(子)の設定	P. 72
<ol> <li>10 <u>VPN接続</u></li> <li>10-1 IKEv2: VPN応答側(親)の設定</li> <li>10-2 IKEv2: VPN開始側(子)の設定</li> <li>11 <u>ログ閲覧</u></li> </ol>	P. 72 P. 81
<ol> <li>10 <u>VPN接続</u></li> <li>10-1 IKEv2: VPN応答側(親)の設定</li> <li>10-2 IKEv2: VPN開始側(子)の設定</li> <li>11 <u>ログ閲覧</u></li> <li>11-1 閲覧できるログの確認</li> </ol>	P. 72 P. 81

11-2 ログ閲覧時の操作

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。

 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。 ロジイン

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。



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					
ネットワーク設定 WAN	ハードウェア	1.0.1				
無待LAN 有徐LAN ルーティング	ソフトウェア	2.0.3				
セキュリティ設定 URLフィルタリング	URLフィルタリング	1.0.1				
<u>P-2ィルタリン2</u> 振る間い接知	Pフィルタリング	1.0.1				
<u>ホワイトリスト情報</u> <u>グループ設定</u>	振る輝い検知	1.0.1				
プリッジ設定 <u>メッテナンスアドレス</u> アクセス許可リスト						
信奉经						
모켓						

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。





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。



			表示/確認	設定	再起動	<u>ログアウト</u>
表示/確認	バージョン					
ネットワーク設定 WAN	ハードウェア	1.0.1				
無禄LAN 有禄LAN ルーティング	ソフトウェア	2.0.3				
セキュリティ設定 URLフィルタリング	URLフィルタリング	1.0.1				
Pフィルタリング 描る舞い特知	₽フィルタリング	1.0.1				
ホワイトリスト情報	振る舞い検知	1.0.1				
ブリッジ設定 <u>メンテナンスアドレス</u> アクセス許可リスト						
情報						
<u>07</u>						

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)



## 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	西起動	ログアウト
表示/確認	バージョン					
<u>パージョン</u> ネットワーク設定	ハードウェア	1.0.1				
WAN 無縁LAN 有様LAN ルーティング	ソフトウェア	203				
セキュリティ設定 LIRI フィルタリング	URLフィルタリング	1.0.1				
アフィルタリング 語る舞い味知	Pフィルタリング	1.0.1				
<u>ホワイトリスト情報</u> グループ設定	振る舞い接知	1.0.1				
プリッジ撤定 メンテナンスアドレス アクセス許可リスト						
<u>1846</u>						
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。



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。

# 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。

		表示/確認	設定	<u>再起動</u>	ログアウト
設定	ネットワーク設定				
ネットワーク設定 WAN	WAN				
高級LAN 有線LAN ルーティング	接続タイプ 固定P接続				
セキュリティ設定 URLフィルタリング	P7FL2				
アフィルタリング 振る舞い特知	ネットマスク				
<u>ホワイトリスト処理</u>	ゲートウェイ				
<u>シルーン設定</u> ブリッジ設定	DNS1				
メンテナンスアドレス アクセス許可リスト	DN52	⊐┛			
動作切替					
0.02.188	浦去			次へ	
	戻る			-	

③各項目を記入し、『次へ』をクリッ クします。



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。

# 4,LAN設定



### 有線LAN接続でのゲートウェイの設定を行います。

設定         設定           キッピー/2歳ま         総定行います。           電子・クリー/2歳ま         総定行います。           電子・クリー/2歳ま         本の/ニュークら総まする項目を観知してびたい。           マロー/2点のジェークの分岐まする項目を観知してびたい。         アレー・クラインスクロー/2点のジェークら総まする項目を観知してびたい。           ビー/2点のジェークの分岐まする項目を観知してびたい。         アレー・クラインスクロー/2点のジェークら総まする項目を観知してびたい。           プレー/2点のジェークの分岐まする項目を観知してびたい。         アレー・クラインスクロー/2点のジェークら総まする項目を観知してびたい。           プレー/2点の目のののからいとのからり、アレー・クラインスクロー/2点の目のののののからいとのからり、アレー・クラインスクロー/2点の目ののののののののののののののののののののののののののののののののののの			表示/確認	設定	再起動	ログアウト
	は ま 3 - 317 - 久和史 1 - 317 - 久和史 1 - 317 - 久和史 1 - 317 - 2012 - 2012 1 - 317 - 2012 - 2012 1 - 317 - 2012 - 2012 - 1 - 1 - 2012 - 2012 - 1 - 2012 - 2012 - 2012 - 1 - 2012 - 2012 - 2012 - 1 - 2012 - 2012 - 2012 - 2012 - 1 - 2012 - 2012 - 2012 - 2012 - 1 - 2012 - 2012 - 2012 - 2012 - 2012 - 1 - 2012 - 20	設定 線定を行います。 本のメニュークら総定する項目を獲	現してください。			

①管理画面にログイン後、右上の『設 定』をクリックし、左の『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。

※DHCP運用する際はブリッジモードでも DHCPをOFFにしないようにお願い致します。

			<u>表示/確認</u>	設定	再起動	<u>ログアウト</u>
	<b>ネットワー</b> 有線LAN 利用する P7ドレス ネットマスク 済去	ク設定 図 192.166.124.254 255.255.0	<u>此</u> 无人頭紹		高記論	<u>92721</u>
<u>バスワード変更</u>						

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。

		表示/確認	設定	<u>再起動</u>	ログアウト
設定 ネットワープ設定 第6日 第6日 第6日 第6日 第1日 第1日 第1日 第1日 第1日 第1日 第1日 第1日 第1日 第1	設定 設定を行います。 左のメニューから設定する項目を確	挟してください。			
セキュリティ設定 <u>URLフィルタリング</u> アフィルタリング 振る葉、1株短 HTTPS通信 ホワイトリスト処理 グループ始定					
プリッジ酸定 <u>メンテナンスアドレス</u> アクセス許可リスト 動作切登 <u>一括般定</u>					
<u>バスワード変更</u>					

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。

※DHCP運用する際はブリッジモードでも DHCPをOFFにしないようにお願い致します。



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。

	6	1
		<i></i>

		表示/確認	設定	再起動	<u>ログアウト</u>
定	無線LAN				
ネットワーク設定 WAN	設定しました。				
無線LAN 有線LAN	Pアドレス	192.168.123.254			
VPN	ネットマスク	255.255.255.0			
<u>リモートアクセス</u> 詳細	無線アクセス識別子	mrb-50_024			
セキュリティ設定	無縁アクセスパスワード	m*******			
URL7/1/91/2	SSIDを公開しない(ステルス)	OFF			
語る舞い検知	チャンネル	13			
HTTPS通信 メール設定 ホワイトリスト処理 グループ設定	WFIプロトコル	ε			
	開始アドレス	192.168.123.10			
	終了アドレス	192.168.123.30			
-11	配布ドメイン	local			
メンテナンスアドレス アクセス許可リスト	DNS1				
	DNS2				
動作切替					
一括設定					
バスワード変更					

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。

### ※Wi-Fiは5GHz,2.4GHzのいずれか片方でのみ動作します。



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。

		表示/確認	設定	再起動	<u>ログアウト</u>
設定	無線LAN				
	無線LAN アプドレス キットマスク 無ポプウにススタフド SSDを公職しない(ステルス) WFプロトコル チャンネル 開始アドレス 林丁プドレス 松丁プドレス レス WFJ DN51 DN51 DN51	192.168.123.254 255.255.295.0 mrb-50,024 m******* CFF ε 13 192.168.123.10 192.168.123.30 local			
<u>動作切替</u> 一括設定 バスワード変更	BLEUK YA' I			- 確認 反る	

無線LAN

設定しました。

Pアドレス

ネットマスク

チャンネル WFプロトコル

開始アドレス

終了アドレス

配布ドメイン

DNS1 DNS2

無線アクセス識別子

無縁アクセスバスワード

SSIDを公開しない(ステルス)

設定

ネットワーク設定

WAN 無線LAN 有線LAN ルーティング

リモートアクセス 詳細

ミキュリティ設定

Pフィルタリン 振る舞い検知 HTTPS道信 メール設定

ホワイトリスト処理

ブリッジ酸定 <u>メンテナンスアドレス</u> アクセス許可リスト

<u>動作切替</u> 一括設定 バスワード変更

グループ設定

表示/確認 設定

192.168.123.254

255.255.255.0

mrb-50\_024

m\*\*\*\*\*\*\*

192.168.123.10

192.168.123.30

OFF

13 6

local

再起動 ログアウト

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。

## 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。



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。



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ましたら作業 は完了です。 5, ブリッジモード


#### 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。

	表示/理説	設定	再起動	ログアウト
<ul> <li>使い</li> <li>キーシーク地定</li> <li>単の</li> <li>レントン</li> <li>単の</li> <li>レントン</li> <li>単の</li> <li>レントン</li> <li>単の</li> <li>レントン</li> <li>レン</li> <li>レン</li></ul>	設定 服をおいます。 本のメニューから設定する項目を翻説してください。			

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。



## 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。



⑤URL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。

		表示/確認	設定	<u>再起勤</u>	<u>ログアウト</u>
<ul> <li></li></ul>	設定 超定され、ます。 左のメニューカや設定する項目を選択い	てくだきい。			

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『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。



## 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。





⑤IP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。





#### 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

### "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。

登定 ネットワーク設定 WAN 有限LAN は、一天一、「「」	セキュリティ設定 ヴループ設定			10.00	קנומ
VPN	191	01.4×197	1738	SET SE	2017
リモートアクセス	コレダクトオス	0	0 認定		
セキュリティ設定 URLフィルダリング	グループ 1	1	0 設定	-	10
アフィルタリング	グループ 2	2	0 設定	0	12
10100795-11024	グループ 3	3	0 設定	0	15
<u> </u>	デフォルト	100	全て		
2ルーフ起来 プリッジ税を メンテナンスアドレス アクセンドロリスト 動作切置 パスワード変更					

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。

	表示/確認	設定	再起動 ログアウト
セキュリティ設定 グループ設定 コレダクトオス			
URL2(1)がりング 戻る 消去 タイプ ルー	דעניפאראס (דיין דיין דיין דיין דיין דיין דיין דיי		振る舞い味知 加の ( ) R正 ( ) 利応 修正 (利称)
	セキュリティ設定 グループ設定 ユレダクトオス (R.2(ルクリング) 度る 油油 タイプ ル	たご/第四 セキュリティ設定 グルーフ設定 コレタクトオス ロスフムがりング アントがりング アントがりング アントがリング アント オート	武元/第回 前立     セキュリティ設定     グループ設定     コルタウトオス     「R2(1/0)0/グ P2(1/0)0/グ     「度る 作法     タイプ ルール

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出来ます。

(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

# ホワイトリスト申請

#### 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 ヘブロック解除の申請を行うことが出来ます。

RLノイルン	ーによりブロッ	ックされました。	
サイト	http://aux	ctions yshoo co.jp	
フィルター	オークショ	v	
Pアドレス	192.168.2	6.24	
ታብኑወቅ	評価を申請	今回のみ接続を許可	ホンイトリストに意味を申請
サイトの再評価をし	辞価を申請 ます。	今回のみ接続を許可 ご注意ください。 10分類アクセン可能になります	ボンイドリムドに登録さ中語 管理者としての設定が必要です。

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	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。				
対像URL	http://wactions.vehoo.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 理を行うことが出来ます。

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
IKEv2: 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。

	表示/確認	設定	再起動	<u>ログアウト</u>
<b>設定</b> ネットワーク設定 <u>WAN</u> 互信LAN (VPN) クセス 詳細	設定 最後を行います。 本のメニューから設定する項目を離死してください。			
セキュリティ設定 <u>URLフィルタリング</u> アフィルタリング 振る無い検知 メール設定 ホワイトリスト処理				
クループ設定 プリッジ数定 メ <u>ンテナンスアドレス</u> アクセス許可リスト				
<u>動作切替</u> バ <u>スワード変更</u>				

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。

表定 ネットワーク設定	ネットワーク設定		
WAN 無線LAN 有線LAN ルーティング	WPN距加 消去	<b>E</b> &	VPH6B70
VPN リモートアクセス 詳細	No.	1	
セキュリティ設定	設定	有効	◎ 無効
URLフィルタリング IPフィルタリング	タイプ	◎ 開始信用 ◎	応答例
振る舞い検知	リモートサイト	任意の文字列	(開始側まP、応答側まD)
メール設定	ローカルサイト	●グローバル固定₽	0 D
ホワイトリスト処理		応答側グローバルIP	(グローバル固定IP、ID)
<u>グループ設定</u>	事約共通鍵	•••••	
ブリッジ設定	チェックアドレス	111.111.111.1	(相手側のLANアドレス)
アクセス許可リスト	IKEパージョン	IKEv2	© KEv1
動作切替	UDPカブセル化	◎ 有効	◎ 無効
一括設定		- 20	
<u>バスワード変更</u>	リモートネットワーク	<u>ポットワーク</u>	10 12正 1198 修正 削除

※UDPカプセル化とは… ルータを経由してVPN通信を行うための機能です。 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…"グローバル固定IP"を選択し、 固定IPを記入 事前共通鍵…相手側と取り決めた任意のワード チェックアドレス…相手側のLAN側IPアドレス IKEバージョン…"IKEv2"を選択 UDPカプセル化…有効



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。

史定	ネットワーク設定		
ネットワーク設定 WAN 毎時 AM	VPN追加		
有線LAN ルーティング VPN	消去	6	<b>VPN6直力</b> D
<u>リモートアクセス</u> 詳細	No.	1	
42 + - 11 = 49/P	設定	◎ 有効	◎ 無効
URL7/1/9/2/2	タイプ	<ul> <li>開始開</li> </ul>	<ul> <li>応答側</li> </ul>
10-2110-27222 振る舞い秋知	リモートサイト	任意の文字列	(開始側はP、応答側はD)
メール設定	ローカルサイト	● グローバル固定PP	O D
ホワイドリスト処理		応答側グローバルIP	(グローバル固定P、D)
<u>グループ設定</u>	事前共通鍵	•••••	
ブリッジ設定	チェックアドレス	111.111.111.1	(相手側のLANアドレス)
<u>メンテナンスアドレス</u> アクセス許可リスト	IKEパージョン	KEv2	© IKEv1
動作切替	UDPカプセル 化	有効	◎ 無効
一括設定			
<u>バスワード変更</u>	リモートネットワーク	<u>ポ</u> ル ネットワーク	10 P8止 別除 修正 削除
		111.111.111.0/24	0

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。 IKEv2: 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。

設定	設定		
ネットワーク設定	鍛定を行います。		
有線LAN グ VPN ジセス 詳細	左のメニューから設定する項目を離訳してください。		
セキュリティ設定 URLフィルタリング アフィルタリング 振る舞い検知 メール設定			
ホワイドリスト処理			
<u>グループ設定</u>			
プリッジ設定 <u>メンテナンスアドレス</u> アクセス許可リスト			
動作切替			
<u>バスワード変更</u>			

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。

ネットワーク設定 <u>WAN</u>	VPN追加		
<u>月線LAN</u> ルーティング VPN リエートマクセッ	消去	戻る	VPNieho
<del>詳細</del>	No.	1	
セキュリティ設定	設定	◎ 有効	◎ 無効
アフィルタリング アフィルタリング	タイプ	<ul> <li>INDERIO</li> </ul>	◎ 応答側
HTTPS: A (B	リモートサイト	応答側グローバルIP	(開始側はP、応答側はD)
<u>&gt;=//ag.e.</u>	ローカルサイト	◎ グローバル圏定₽	D
1024F92F98F		任意の文字列	(グローバル固定P、D)
2ルーフ設定	事前共連鍵	•••••	
ブリッジ設定 メンテナンスアドレス マクセン体部リスト	チェックアドレス	111.111.111.1	(相手側のLANアドレス)
22GA81-12AL	IKEバージョン	KEv2	© KEv1
一括設定	UDPカプセル化	◎ 有効	◎ 無効
パスワード変更	リモートネットワーク	道力 ネットワーク	0 修正 削除 修正 削除

※UDPカプセル化とは… ルータを経由してVPN通信を行うための機能です。 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…グローバル固定IP ローカルサイト…"ID"を選択し、 開始側の設定したIDを記入 事前共通鍵…相手側と取り決めた任意のワード チェックアドレス…相手側のLAN側IPアドレス IKEバージョン…"IKEv2"を選択 UDPカプセル化…有効



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。

# 11,ログ閲覧

閲覧できるログの確認

#### MRBで検閲した通信のログを閲覧することができます。

			表示/確認	設定	再起動	ログアウト
表示/確認	バージョン					
<u>パージョン</u> ネットワーク設定	ハードウェア	1.0.1				
WAN 無確LAN 有確LAN	ソフトウェア	2.0.31				
詳細	URLフィルタリング	1.0.1				
URLフィルタリング アフィルタリング 振る舞い検知	Pフィルタリング	1.0.1				
HTTPS通信 メール設定	振る舞い検知	1.0.1				
<u>ホワイトリスト情報</u> <u>グループ設定</u>						
プリッジ設定 <u>メンテナンスアドレス</u> アクセス許可リスト						

①管理画面にログイン後、 左側の『ログ』をクリックします。



 ②各ボタンをクリックすることでそれ ぞれのログを閲覧することができます。

③各ログの内容については以下のとおりです。

#### ・システムログ ...MRBで動作したシステムのログです。(通信のログではありません) ・アタックログ ...外部からのアタックされた場合に記録されます ・ウィルスログ ...ダウンロードしたデータがウイルスだった場合に記録されます ・URLフィルタリングログ ...WEB閲覧時、URLフィルタリングにて通信をブロックした場合に記録されます ・IPフィルタリングログ ...WEB閲覧時、IPフィルタリングにて通信をブロックした場合に記録されます ・アップロードログ …データを外部にアップロードした際に記録されます ・振る舞いログ …WEBサイト以外からの通信をブロックした際に記録されます ・ユーザーログ …ユーザがMRB管理画面にて行った操作が記録されます ・WEBアクセスログ …アクセスしたWEBサイトが記録されます

- ・アクセスログ
- …WEBサイト以外のアクセスが記録されます

## ログ閲覧時の操作

#### MRBで検閲した通信のログを閲覧を確認する際の操作です。

			表示/確認	設定	再起動	ログアウト
表示/確認	バージョン					
<u>パージョン</u> ネットワーク設定	ハードウェア	1.0.1				
WAN 無確LAN 有確LAN	ソフトウェア	2.0.31				
ボモーション (税定)	URLフィルタリング	1.0.1				
URLフィルタリング アフィルタリング 揺る舞い状知	Pフィルダリング	1.0.1				
HTTPS通信 メール設定	振る舞い検知	1.0.1				
<u>ホワイトリスト情報</u> <u>グループ設定</u>						
ブリッジ設定 <u>メンテナンスアドレス</u> アクセス許可リスト						

①管理画面にログイン後、 左側の『ログ』をクリックします。



 ②閲覧したいログのボタンをクリック します。



③クリックしたボタンに対応するログ が表示されます。 また、『ダウンロード』をクリックす ることで、現在閲覧している最大300 件分のログデータをテキスト形式でダ ウンロードすることができます。 ④閲覧ログの操作は以下のとおりです。





## HTTPSフィルタリング

### ・HTTPSフィルタリング設定 目次

1	MRB	の設定	P. 89
2	<u>証明</u>	書のダウンロード	P. 91
3	<u>PCの</u>	設定	P. 93
	3-1	IE/Chromeの場合	
	3-2	FireFoxの場合	
4	<u>クラ</u>	イアント証明書を利用する場合	P. 101
	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。

	表示/確認	<u>設定</u>	<u>再起動</u>	<u>ログアウト</u>
歳定     ネットワーク設定     WAN     有強AN     北ーティング     VPN     リモーナアクセス     詳細     詳細     詳細	設定 設定を形います。 左のメニューから確定する項目を勘凡してください。			
セキュリティ設定 <u>URLフィルタリング</u> 1000年10月7日 1000年10月7日 1000年10月7日 ホワイトリスト処理 グリーニ対応				
2012-7382 プリッジ酸定 メンテナンスアドレス アクセン詳可ジスト 動作切覧 バスワード変更				
	•			

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。

) · ひみつのフォルダ	<ul> <li>49 ひみつのフォルダの検索</li> </ul>	۶
整理 ▼ 新しいフォルダー	E •	0
≥ ZS(2, 2)       2 9720-F       2 9720-F       2 8250,58*       2 8250,58*       2 8250,58*       2 827,58*       2 827,58*       2 827,58*       2 827,78*       2 827,78*       2 827,78*       2 827,78*       3 82-597		
ファイル名(N): cacert.der		
ファイルの種類(T): der File (*.der)		
フォルダーの非表示	保存(S) キャンセ	96

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, PC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。



 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。

証明書の情報     この CA ルート証明書は信頼されていません。信頼を有効にするには     この CA ルート証明書は信頼されていません。信頼を有効にするには     この近明書を信頼されたルート証明確関のストアにインストールしてくだ     さい。					
-	発行先: 発行者:	mrb200019ca mrb200019ca	—		
	有効期間	2017/01/05 <b>から</b> 2027/01/08			
5	四月書の詳細について	<b>119月書のインストール①</b> 発行者のステートメン 表示します。	(S)		

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。



 (1) FireFox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。

証明書マネージャ		×
あなたの証明書 個人証明書 サーバ証明書 認証	局証明書 その他	
認証局を識別するため以下の証明書が登録され	ています:	
証明書名と発行者名	セキュリティデバイス	r,
⊿TC TrustCenter GmbH TC TrustCenter Class 3 CA II	Builtin Object Token	*
⊿Technol mrb200019ca	Software Security Device	
TeliaSonera Root CA v1 ⊿thawte, Inc.	Builtin Object Token	
thawte Primary Root CA - G3	Builtin Object Token	-
表示( <u>V</u> ) 信頼性を設定( <u>E</u> ) インボ	<b>ニート(<u>M</u>)</b> エクスポート( <u>X</u> ) 削除ま	たは信頼しない( <u>D</u> )
		ОК

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 認しましたら、『OK』をクリックして 証明書のインポートは完了です。





### 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。

	表示/確認	設定	再起動	ログアウト
読定     ネットワーク設定     WAN     石積(AN	設定 総定を行います。 左のノニューから続定する項目を激用してください。			
セキュリティ設定 URLフィルタリング アフィルタリング HTTPS連信 ホワイドリスト長理				
<u>グループ設定</u> プリッジ設定 メンテナンスアドレス アクセス詳可りスト 動作切覧 バスワード次準				

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。



### 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。

	表示/確認	設定	<u>再起動</u>	<u>ログアウト</u>
	設定 裁定を行います。 友のメニューから撤定する項目を選択してください。			
セキュリティ級定 レモノンルタリング ドフマルタリング 「TTPS連信 ボワイドリスト処理 グループ設定				
プリッジ設定 水 <u>テナンスアドレス</u> アクセス許可リスト 動作切置 バスワード変更				

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


# 1, Outlookの設定確認



①**Outlook**を起動し、左上の『ファイ ル』をクリックします。

ファイル	ホーム	送受信	フォルダー	表示 🔉	実行したい作業をノ	いっして	ください
 新しい 電子メール	新しい アイテム ▼	<ul><li>新しい</li><li>会議</li></ul>	惊 ▲ 私 ・ 削時	こ 古いアイテム の整理	♀ 返信 ♀ 全員に返信 ♀ 転送		どうして、 そのまで、 その. ***********************************
新規	作成	TeamViewer	Ĭ	11陸	返信		カイック操作

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。

	アカウント	の変更
POP と IMAP のアカウント設定 お使いのアカウントのメール サー	バーの設定を入力してください。	Ť
ユーザー情報		アカウント設定のテスト
名前(Y):	n-shibata	アカウントをテストして、入力内容が正しいかどうかを確認することをお勧め
電子メール アドレス(E):	n-shibata@technol.jp	08.91
サーバー情報		アカウント設定のテスト(T)
アカウントの種類(A):	IMAP 🗸	
受信メール サーバー(I):	imap.technol.jp	✓ 「次へ」をワリックした5アカワント設定を目動的にデストする     (S)
送信メール サーバー (SMTP)(O):	smtp.technol.jp	
メール サーバーへのログオン情報		
アカウント名(U):	n-shibata@technol.jp	
パスワード(P):	*******	1/51/2010/05/3-7/2 9/10
₹/(ス)	フードを保存する(R)	and the second
①メール サーバーがセキュリティで発展されたパスワード認証 (SPA) に対応している場合には、チェック ポックスをオンにして(ださい(Q)		[ 詳釋語語文定(M) ]
		< 戻る(B) 次へ(N) > 本ヤンセル

④『詳細設定』をクリックします。

インターネット電子メール設定					
全般 送信サーバー 詳細設定					
サーバーのポート番号					
受信サーバー (IMAP)(I): 143					
使用する暗号化接続の種類(E): なし 🗸					
送信サーバー (SMTP)(O): 587					
使用する暗号化接続の種類(C): なし 💙					
サーバーのタイムアウト(T)					
短い 🗢 長い 1分					
フォルダー					
ルートフォルターのバス(F):					
送信済みアイテム					
□ 送信済みアイテムのコピーを保存しない(D)					
削除済みアイテム					
□ アイテムを削除対象としてマークするが、自動的には移動しない(K)					
則体対象としてマークとれたアイテムは、メールパックス内のアイテムが消去されたときに完全に削除されます。					
✓オンライン中にフォルダーを切り替えたらアイテムを消去する(P)					
OK +77211					

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。

	アカウン	ND変更		
POP と IMAP のアカウント設定 お使いのアカウントのメール サー	バーの設定を入力してください。	×.		
ユーザー情報		アカウント設定のテスト		
名前(Y):	n-shibata	アカウントをテストして、入力内容が正しいかどうかを確認することをお勧め		
電子メール アドレス(E):	n-shibata@technol.jp	089+		
サーバー情報 アカウントの種類(A): IMAP ✓		アカウント設定のテスト(T)		
受信メール サーバー(I):	imap.technol.jp	↓ 【次へ】をクリックしたらアガワント設定を目動的にナストする (S)		
送信メール サーバー (SMTP)(O):	smtp.technol.jp			
メール サーバーへのログオン情報				
アカウント名(U):	n-shibata@technol.jp			
パスワード(P):	*******	オフラインにしておびール: すべて		
2.172	フードを保存する(R)	and the second		
メール サーバーがセキュリティで保 ている場合には、チェック ポックスを	纏されたパスワード認証 (SPA) に対応し オンにして伏さい(Q)	\$¥#832定(M)		
		< 戻る(B 次へ(N) > キャンセル		

⑥『次へ』をクリックします。

<del>ፓ</del> スト ን	クカウント設定	
すべてのテストが完了しました。[閉じる]をクリックして続	行してください。	中止(S) 閉じる(C)
タスク ✓ 受信メール サーバー (IMAP) へのログオン ✓ テスト電子メール メッセージの送信	状況 完了 完了	

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。

	表示/確認 設定 再起動 ログアウト
<b>設定</b> ネットワーク設定 WAN 有強LAN ルーティング VFN リモートアクセス 詳細	設定 設定若います。 左のノニューから設定する項目を離祝してください。
セキュリティ級定 レスフルタリング ドアフルタリング 加多速、採知 正一ル級定 大ワイドリスト処理 グループ設定	
ーーーー ブリッジ設定 <u>シンテナンスアドレス</u> アクセス許可リスト <u>動作切音</u> バスワード変更	

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。

		表示/確認 設定	<u>再起動 ログアウト</u>
設定	セキュリティ設定		
ネットワーク設定	メール設定		
MAN 有線LAN	デフォルトグループ		
<u>VPN</u> リモートアクセス 詳細	設定しますか?		
セキュリティ設定 URLフィルタリング	メール愛信(MAP、POP3)	利用する	
振る舞い検知	スパム検知機能	利用する	
メール設定	スパム表示件名	-MRBSpam-	
<u>ホワイトリスト処理</u> グループ設定	ウィルス検知機能	利用する	
プリッジ設定	ウィルス表示件名	-VIRUS-	
<u>メンテナンスアドレス</u> アクセス許可リスト	セキュア通信	利用する	
動作切替			
<u>バスワード変更</u>			() () () () () () () () () () () () () (

### 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。

許可アドレス設定

### 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。

	表示/確認	設定	再起動	<u>ログアウト</u>
<ul> <li>設定</li> <li>ネットワープ設定 WAN 私子でグラ The アーアンウセス FTB ビキュリティ設定 はュンパルクシアグ デュンクセンス デュングション ボング・ロンス ボング・</li></ul>	設定 設定者刊します。 左のノニューカら説定する項目を選択してください。			

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『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。

	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 有荷LAN ルーティング VFN リモートアクセス 詳細	設定 総定を行います。 左のメニューから設定する項目を離脱してください。
セキュリティ数定 リスニッパルタリング アフィルタリング 振る悪い状知 アール設定 ホワイトリスト処理	
<u>グループ設定</u> プリッジ設定 メ <u>ンテナンスアドレス</u> アクセス許可リスト 動作切査	
<u>パスワード変更</u>	

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。



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。



 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。

全般 詳細 証明のバス	するには
<b>発行先</b> : mrb200019ca <b>発行者:</b> mrb200019ca <b>有効期間</b> 2017/01/05 <b>から</b> 2027/01/03	
<b>証明書のインストールの</b> 範囲用書の注意になってあってはます。	ステートメント(S) OK

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 モード設定

### ・プロフェッショナルモード設定 目次

1	本体	本設定のバックアップ	P. 134
	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	<u>プ</u> г	コフェッショナルモードによる設定変更	P. 141
	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	<u>プ</u> ロ	コフェッショナルモード設定補足	P. 163
	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	
	3-3	syslogサーバの設定例	

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。

			表示/確認	設定	再起動	<u>ログアウト</u>
表示/確認	バージョン			(	D	
<u>ハーション</u> ネーットワーク設定 WAN	ハードウェア	2.0.1				
無確LAN 有線LAN ルーティング	ソフトウェア	2.0.23				
<u>VPN</u> <u>リモートアクセス</u> 詳細	URLフィルタリング	1.0.1				
セキュリティ設定 URLフィルタリング	Pフィルタリング	1.0.1				
<u>Pフィルタリング</u> 振る輝い検知 HTTPS通信 メール設定	振る舞い検知	1.0.1				
ホワイトリスト情報						
グループ設定						
プリッジ設定 メンテナンスアドレス アクセス許可リスト						
情報						
<u>ログ</u>						

①MRBにログイン後、右上の『設定』 をクリックします。

		表示/確認	設定	再起動	<u>ログアウト</u>
設定 キットワーン設定 NRM 無価(A) 有価(A) 有価(A) パモーテンジ パモートアクセス IFE IFE	設定 設定を行います。 左のノニューから設定する項目を離れ	してください。			
セキュリティ級定 リスニフィルタリング アフィルタリング 振る薄い特知 HTTPS通信 メニル設定 ホロイムレスト加速					
グループ設定 プリッジ設定 シテナンスアドレス アクセス許可リスト					
動作切替 一括設定 バスワード変更					

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。

setup_one.bxt を開く					
次のファイルを開こうとしています:					
📋 setup_one.txt					
ファイルの種類: Text Document					
ファイルの場所: http://192.168.124.254					
このファイルをどのように処理するか選んでください					
⑦ プログラムで開く( <u>O</u> ): Windows ワードパッド アプリ… ▼					
<ul> <li>ファイルを保存する(<u>s</u>) (4)-1</li> </ul>					
○ 今後この種類のファイルは同様に処理する( <u>A</u> )					
<b>④-2</b>					
OK キャンセル					

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。



### 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。

			<u>表示/確認</u>	設定	再起動	<u> ログアウト</u>
表示/確認	バージョン			(	1	
バージョン ネットワーク設定	ハードウェア	2.0.1				
WAIN 無縁LAN 有縁LAN ルーティング	ソフトウェア	2.0.23				
<u>VPN</u> リモートアクセス 詳細	URLフィルタリング	1.0.1				
セキュリティ設定 URLフィルタリング	Pフィルタリング	1.0.1				
PD-11/タリング 振る舞い検知 HTTPS通信 メール設定	振る舞い検知	1.0.1				
ホワイドリスト情報						
グループ設定						
プリッジ設定 メンテナンスアドレス アクセス許可リスト						
情報						
<u>05</u>						

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。

		表示/確認	設定	再起動	<u>ログアウト</u>
また、 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	一括設定 全ての最密想いました。しばらく	お称ろください。			

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)	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。

### 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。\_\_\_\_\_

設定項目	記入例	備考
有線LAN設定	LAN2{ CONFIG= <mark>ON/OFF</mark> 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
<b>DHCPIP固定設定</b> (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= <mark>ON/OFF</mark> 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
DHCPIP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 }	<pre>"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802.11g "CHANNEL=":802.11b/gの場合 1~13 802.11nの場合 40~64(8刻み)</pre>

### 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。

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= <mark>ON/OFF</mark> 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 <mark>192.168.22.0 255.255.0.0 192.168.11.1</mark> }	・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 1 61.51.41.31 192.168.112.0 1 1 }	<ul> <li>ハッシュ値</li> <li>VPN番号</li> <li>設定有効:1/設定無効:2</li> <li>開始側:1/応答側:2</li> <li>事前共通鍵</li> <li>応答側:開始側指定のID 開始側:相手側の固定IP</li> <li>相手にIPを知らせる:1 相手にIDを知らせる:2</li> <li>固定IP or ID</li> <li>相手側LANアドレス</li> <li>UDPカプセル化ON:1/OFF:0</li> <li>IKEv1:1/IKEv2:2</li> <li>の順に1行に記載。</li> </ul>
VPN設定(開始側)	VPN{ 2eb84e83830b72c05d3b12dfd05ced16 1 1 1 mr-5 61.51.41.31 2 test 192.168.11.0 1 1 }	
VPNネットワーク 設定	VPN_NET{ b0abb130d1f685921d7bd770e834de81 <mark>1 10.10.1.0 16</mark> }	<ul> <li>・ハッシュ値</li> <li>・VPN番号</li> <li>・IPアドレス</li> <li>・ネットマスク</li> <li>の順に1行に記載。</li> <li>複数設定の際は改行して同様に記載。</li> <li>VPN番号はVPN設定に対応させる。</li> </ul>

※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

# 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。

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 }	<ul> <li>・グループ番号</li> <li>・ハッシュ値</li> <li>・単一指定:1/範囲指定2</li> <li>・IPアドレス(範囲指定なら先頭IP)</li> <li>・ネットマスク長</li> <li>・単一指定:*</li> <li>範囲指定:終端IPアドレス</li> <li>・"0"2つ</li> <li>の順に1行に記載。</li> <li>複数設定の際は改行して同様に記載。</li> </ul>

### 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。

設定項目	記入例	備考	
URLフィルタの レベル設定	URL_LEVEL <mark>_9{</mark> <mark>2</mark> }	末尾の数字で設定するグループを指	
IPフィルタの レベル設定	IP_LEVEL <mark>_9</mark> { <mark>2</mark> }	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	
振る舞いフィルタ のレベル設定	BEHAVIOR_LEVEL_ <mark>9</mark> { <mark>2</mark> }	に対応。	
URLフィルタの ホワイトリスト	URL_WHITE_9{ f15d461b1a1dc80efa85f7c6aa1f865b0 www.example.co.jp 29252e6919566f4d5156a59fb0d9b5cb0 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{ f15d461b1a1dc80efa85f7c6aa1f865b0 www.example.co.jp f686fab203c770588504a557f77109ee0 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述 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き 定。(デフォルトグループは100) ・ハッシュ値	
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	・IPアトレス ・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/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。

設定項目	記入例	備考	
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- }	<ul> <li>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)</li> <li>"MAIL=":利用する場合は"ON"</li> <li>"SPAM=":利用する場合は"ON"</li> <li>"VIRUS=":スパム判定時メール タイトルに表示される文言</li> <li>"SUBJECTVIRUS=":ウイルス判定 時メールタイトルに表示される文言</li> <li>(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)</li> </ul>	
mail black/white 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。	
https通信検知	HTTPS <mark>9{</mark> HTTPS= <mark>ON / OFF</mark> }	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	<pre> URL_HTTPS_9{ ea0ea7696d6d44dd79e31a33bd1125850 www.aaa.com }</pre>		
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。	

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/ 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。



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	REMOTE_ACCESS{	"CONFIG=":使用する場合は"ON"
	CONFIG=ON	"IP=": リモートアクセス用IP
	IP=172.23.0.1	"CLIENT_RANGE=":DHCP範囲
	CLIENT_RANGE=172.23.0.10-172.23.0.20	"DNS=":DNSサーバ
	DNS=8.8.8.8	(上がプライマリ、下がセカンダリ)
	DNS=8.8.4.4	"PSK=":事前共有鍵
	PSK=psktrtsecret1	"USER=":利用ユーザ
	USER=user1 trtpass11	(前半がID、後半がパスワード)
	USER=user2 trtpass22	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。

#### SYSLOG出力設定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
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=": <b>以下の表の"priority"を参考に指定</b>

#### ※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)

URLカテゴリフィルタリングのカテゴリー覧表です。 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 **2**コンピュータセキュリティ情報 3 余融 4ビジネス/経済 5コンピューター般技術情報 6オークション 7ショッピング 8カルト/オカルト 9旅行/観光 10 危険ドラッグ/麻薬 11アダルト/ポルノ 12日用雑貨 13軍事 14 SNS 15 デッドサイト 16株式/投資 17教育/訓練 18出会い系 19性教育 20宗教 21 娯楽/芸術 22個人サイト/ブログ 23法律 24 地元情報 25ストリーミング 26仕事検索 27ギャンブル 28翻訳 29参考文献/学術調查 30シェアウェア/フリーウェア 31 P2P 32マリファナ 33 ハッキング 34ゲーム 35 哲学/政治的支援 36 武器 37 有料サイト 38 狩り/釣り 39社会/団体

40教育 41 グリーティングカード 42スポーツ 43水着/下着 44不審なサイト 45子供向け 46 憎悪/人種差別 47オンラインストレージ 48暴力/乱暴 49キーロガー/モニタツール 50検索エンジン 51インターネットポータル 52Web広告 53不正行為 54 グロテスク 55 Webメール 56マルウェアサイト 57フィッシング詐欺 58 プロキシ/匿名プロキシ 59 スパイウェア/アドウェア 60音楽 61政府 62 ヌード 63ニュースメディア 64非合法/違法 65 コンテンツ配信 66インターネット通信 67ボットネット 68妊娠中絶 69健康と医療 70スパムソース 74動的コンテンツ 75パークドメイン 76酒/煙草 78画像/動画検索 79ファッション/美容 80レクリエーション/趣味 81自動車/バイク 82Webホスティング

※2019/1/8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



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
	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
リエート アクセフ	DNS=8.8.8.8	プライマリDNS
リビードノリセス	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{	
	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 <b>2</b>
	mr-5	事前共通鍵
VPN設定(応答側)	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_NET{	
	b0abb130d1f685921d7bd770e834de81	ハッシュ値
VDNラットワーク設定	1	VPN番号
VPINA クトワーク設定	192.168.12.0	IPアドレス
	24	ネットマスク
	}	

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{	
	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
VPN設定(開始側)	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_NET{	
	b0abb130d1f685921d7bd770e834de81	ハッシュ値
	1	VPN番号
VPNネットワーク設定	192.168.11.0	IPアドレス
	24	ネットマスク
	}	

# syslogサーバの設定例

# MRBのsyslog受信を行うために、受信サーバで設定を行います。 例として、rsyslogで受信する際の設定例を記載します。\_\_\_\_\_

<pre># For more information see /usr/share/doc/rsyslog-*/rsyslog_conf.html # If you experience problems, see http://www.rsyslog.com/doc/troubleshoot.html</pre>	
<pre>#### MODULES #### # The imjournal module bellow is now used as a message source instead of imuxsock. \$ModLoad imuxsock # provides support for local system logging (e.g. via logger command) \$ModLoad imjournal # provides access to the systemd journal #\$ModLoad imklog # reads kernel messages (the same are read from journald) #\$ModLoad immark # providesMARK message capability # Provides UDP syslog reception #\$MODULES UDP Syslog reception #\$MODULES ####</pre>	①/etc/rsyslog.confを開きます。 ②UDPで受信するなら上、TCPで受信す るなら下の
# Provides TCP syslog reception \$ModLoad imtcp \$InputTCPServerRun 514	"Provides syslog reception"のコメントア ウトを取り除きます。
#### GLOBAL DIRECTIVES ####	
# Where to place auxiliary files \$WorkDirectory /var/lib/rsyslog	
# Use default timestamp format \$ActionFileDefaultTemplate RSYSLOG_TraditionalFileFormat	
# File syncing capability is disabled by default. This feature is usually not required, # not useful and an extreme performance hit #\$ActionFileEnableSync on	
# Include all config files in /etc/rsyslog.d/ \$IncludeConfig /etc/rsyslog.d/*.conf	

# Include all config files in /etc/rsyslog.d/ \$IncludeConfig /etc/rsyslog.d/*.conf		③"#### RULES ####"の記述の上に
# Turn off message reception via local log socket; # local messages are retrieved through imjournal now. \$OmitLocalLogging on		\$template mrbsyslog, "ファイルパス"
# File to store the position in the journal \$IMJournalStateFile imjournal.state		tromhost –ip, !isequal, "127.0.0.1" -?mrbsyslog
### mrb syslog test ### \$template remotehost,"/var/log/hosts/%HOSTNAME%.log" :fromhost-ip, !isequal, "127.0.0.1" -?remotehost & ~		と入力し、保存します。
#### RULES ####		
 # Log all kernel messages to the console. # Logging much else clutters up the screen. #kern.*	/dev/console	
<pre># Log anything (except mail) of level info or higher. # Don't log private authentication messages! *.info;mail.none;authpriv.none;cron.none</pre>	/var/log/messages	
# The authpriv file has restricted access. authpriv.*	/var/log/secure	
# Log all the mail messages in one place. mail.*	-/var/log/maillog	

# MRB-50L LTEモードセッ トアップ

# ・MRB-50L LTEモード設定 目次

1	LTEモードの設定	P. 175
2	使用回線モード切替	P. 179

# 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。

			表示/確認	設定	再起動	<u>ログアウト</u>
設定	ネットワーク	設定				
ネットワーク設定 WAN構成	LTE設定					
WAN 無確LAN	APN	m2m4biz.softba	nk			
有線LAN ルーティング	ユーザ名	m2mbiz				
リモートアクセス 詳細	パスワード	m****z				
セキュリティ設定 URLフィルタリング	固定IPアドレス					
HTTPS遺信	リモートIPアドレス					
メール設定 ホワ-イトリスト処理	DNS1					
グループ設定	DNS2					
プリッジ設定 メンテナンスアドレス アクセス許可リスト	キャリア	自動	)			
動作切替		Dブラン Aプラン1				
一括設定	消去	Aプラン2 5プラン	$\square$		(次へ)	
<u>バスワード変更</u>	=7			_		2
	戻る	J				

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(Mineo)
Aプラン2	:	au(UQmobile)
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。



#### ⑦左のような画面が表示されましたら、 SIMカードの設定作業は完了です。

# 2,使用回線モード切替

# 使用するWAN回線を切り替えます。

		表示/確認	設定	再起動	<u>ログアウト</u>
設定	設定 総定を行います。 本のメニューから設定する項目を選択して	Krau.	(1	)	
セキュリティ設定 URL2-1/49/27 アクス・49/27 形式用いたが 形式の 「TTSS通信 メール設定 ポプロイヤノスト処理 グループ設定					
<ul> <li>フリッジ酸定 メデチンスアドレス アクセン目のリスト</li> <li>動作切置</li> <li>パスワード変更</li> </ul>					

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。