

# 基本設定 2/2

## 目次

6. ルーティング設定 .....	2
7. グループ設定 .....	4
7.1 グループ編集 .....	4
7.2 コレダケトオス .....	7
7.3 グループ別フィルタリング .....	10
8. ホワイトリスト申請／処理 .....	12
8.1 ホワイトリスト申請 .....	12
8.2 ホワイトリスト申請処理 .....	13
9. TCPMSS 設定 .....	15
10. VPN 接続 .....	17
10.1 VPN 応答側（親）の設定 .....	17
10.2 VPN 開始側（子）の設定 .....	22
10.3 VPN（MRB 接続）の設定 .....	26
11. ログ閲覧 .....	30
11.1 閲覧できるログ .....	30
11.2 ログ閲覧時の操作 .....	32
11.3 クラウドログの閲覧 .....	34

## 6. ルーティング設定

本項では、MRB がルータとして機能する際のルーティング設定の手順について記載します。

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



② 『追加』をクリックします。



- ③ ルーティングするネットワーク情報と宛先ゲートウェイを入力し、『追加』をクリックします。

The screenshot shows a web interface for network settings. On the left is a sidebar menu with categories like 'ネットワーク設定' (Network Settings), 'セキュリティ設定' (Security Settings), and 'グループ設定' (Group Settings). The main area is titled 'ネットワーク設定' (Network Settings) and contains a 'ルーティング' (Routing) section. Under 'ルーティング追加' (Add Routing), there are three input fields: 'ネットワーク' (Network) with the value '1.1.1.1', 'ネットマスク' (Netmask) with '255.255.255.0', and 'ゲートウェイ' (Gateway) with '192.168.1.1'. Below these fields are buttons for '消去' (Delete), '戻る' (Back), and '追加' (Add). The '追加' button is highlighted with a red box.

- ④ 入力した 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。

This screenshot is similar to the previous one, showing the 'ネットワーク設定' (Network Settings) page. The 'ルーティング' (Routing) section now shows the '設定しますか?' (Confirm?) question. The input fields for 'ネットワーク' (1.1.1.1), 'ネットマスク' (255.255.255.0), and 'ゲートウェイ' (192.168.1.1) are now populated with text. The '追加' (Add) button remains highlighted with a red box, and the '戻る' (Back) button is also visible below it.

## 7. グループ設定

本項では、MRB で配下端末をグループ分けし、グループごとにセキュリティ設定する手順について記載します。

### 7.1 グループ編集

本項では、MRB で配下端末にグループを割り当てる手順について記載します。

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。

The screenshot shows the 'セキュリティ設定' (Security Settings) page. The left sidebar contains a '設定' (Settings) menu with categories like 'ネットワーク設定' (Network Settings) and 'セキュリティ設定' (Security Settings). The main content area is titled 'セキュリティ設定' and includes 'グループ設定' (Group Settings) for 'グループ 1'. Below this, there are tabs for 'URLフィルタリング', 'IPフィルタリング', '振る舞い検知', 'HTTPS通信', and 'メール設定'. Under the 'IPフィルタリング' tab, there are buttons for '戻る' (Back), '消去' (Delete), and '追加' (Add), which is highlighted with a red box. Below these buttons are labels for 'タイプ' (Type) and 'ルール' (Rule). At the bottom right, there are buttons for '修正' (Modify) and '削除' (Delete).

- 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『追加』をクリックします。

This screenshot shows the 'セキュリティ設定' (Security Settings) page with the 'IPフィルタリング' (IP Filtering) tab selected. The 'ルール追加' (Add Rule) section prompts the user to choose a specification method. Two radio buttons are present: 'IPアドレス' (IP Address), which is selected and highlighted with a red box, and 'IPアドレス範囲' (IP Address Range). Below this, the 'ルール' (Rule) section has a text input field containing '192.168.123.10', also highlighted with a red box. Underneath, there are labels for 'IPアドレス' (with an example '例: 192.168.123.1'), '開始IPアドレス-終了IPアドレス' (192.168.123.1-192.168.123.10), and 'ネットワークアドレス' (192.168.123.0/24). At the bottom, there are buttons for '戻る' (Back), '消去' (Delete), and '追加' (Add), with the '追加' button highlighted in red. Additionally, there are two radio buttons for 'DHCP固定IPから設定' (Set from DHCP fixed IP) and 'DHCPリース情報から設定' (Set from DHCP lease information).

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。

表示/確認 設定 再起動 ログアウト	
<b>設定</b>	<b>セキュリティ設定</b>
ネットワーク設定	グループ設定
<a href="#">WAN</a>	グループ 1
<a href="#">無線LAN</a>	ルール追加
<a href="#">有線LAN</a>	追加しますか？
<a href="#">ルーティング</a>	タイプ IPアドレス
<a href="#">VPN</a>	ルール 192.168.123.10
<a href="#">リモートアクセス</a>	
<a href="#">詳細</a>	<input type="button" value="追加"/>
セキュリティ設定	<input type="button" value="戻る"/>
<a href="#">URLフィルタリング</a>	
<a href="#">IPフィルタリング</a>	
<a href="#">振る舞い検知</a>	
<a href="#">HTTPS通信</a>	
<a href="#">メール設定</a>	
<a href="#">今回のみ接続を許可</a>	
ホワイトリスト処理	
<a href="#">グループ設定</a>	
ブリッジ設定	
<a href="#">メンテナンスアドレス</a>	
<a href="#">アクセス許可リスト</a>	
<a href="#">動作切替</a>	
<a href="#">一括設定</a>	
<a href="#">パスワード変更</a>	

## 7.2 コレダケトオス

本項では、MRB でコレダケトオス（許可された IP/URL 以外とは通信が出来ない特別なグループ）を設定する手順について記載します。

- 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。



- 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。

[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 <a href="#">WAN</a> <a href="#">無線LAN</a> <a href="#">有線LAN</a> <a href="#">ルーティング</a> <a href="#">VPN</a> <a href="#">リモートアクセス</a> <a href="#">詳細</a>  セキュリティ設定 <a href="#">URLフィルタリング</a> <a href="#">IPフィルタリング</a> <a href="#">振る舞い検知</a> <a href="#">HTTPS通信</a> <a href="#">メール設定</a> <a href="#">今回のみ接続を許可</a>  ホワイトリスト処理  <a href="#">グループ設定</a>  ブリッジ設定 <a href="#">メンテナンスアドレス</a> <a href="#">アクセス許可リスト</a>  <a href="#">動作切替</a>  <a href="#">一括設定</a>  <a href="#">パスワード変更</a>	<b>セキュリティ設定</b>  グループ設定  コネクタオス  ルール追加  追加しますか？  タイプ   IPアドレス  ルール   192.168.126.10  <div style="text-align: right; margin-top: 10px;"><input style="border: 2px solid red;" type="button" value="追加"/> <input type="button" value="戻る"/></div>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### 7.3 グループ別フィルタリング

本項では、グループごとにフィルタリング強度を設定する手順について記載します。

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、フィルタリング設定のページをご確認ください。

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  
URLフィルタリング  
IPフィルタリング  
振る舞い検知  
HTTPS通信  
メール設定  
今回のみ接続を許可

ホワイトリスト処理  
グループ設定

ブリッジ設定  
メンテナンスアドレス  
アクセス許可リスト

動作切替

一括設定

パスワード変更

### セキュリティ設定

グループ設定

グループ 1

URLフィルタリング IPフィルタリング 振る舞い検知 HTTPS通信 メール設定

戻る 消去 追加 修正 削除

タイプ ルール 修正 削除

## 8. ホワイトリスト申請／処理

本項では、ホワイトリスト申請、ホワイトリスト申請処理の手順について記載します。

### 8.1 ホワイトリスト申請

Web サイトがブロックされた際に、管理者の方に解除申請（ホワイトリスト申請）を行うことができます。本項では申請の手順について記載します。

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

### MRB-50 ブロック情報

---

**URLフィルターによりブロックされました。**

サイト	http://yahoo-mbga.jp
フィルター	ゲーム
IPアドレス	192.168.123.10

サイトの再評価をします。  
反映されるまでに、数日要します。  
(全てのMRB-50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。  
また同じカテゴリーのページも閲覧可能になり、ログが残ります。

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MRB-50のみ反映されます。)

- ② このような画面が表示されましたら、申請は完了です。管理者の方にご連絡ください。

### ブロックリクエスト設定

---

**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://yahoo-mbga.jp
-------	----------------------

## 8.2 ホワイトリスト申請処理

本項では、ホワイトリスト申請に対しての処理の手順について記載します。

- 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。

[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  
[URLフィルタリング](#)  
[IPフィルタリング](#)  
[振る舞い検知](#)  
[HTTPS通信](#)  
[メール設定](#)  
[今回のみ接続を許可](#)

ホワイトリスト処理  
  
[グループ設定](#)

ブリッジ設定  
[メンテナンスアドレス](#)  
[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

### セキュリティ設定

#### ホワイトリスト要求処理

設定しますか？

グループ	要求者	日付	タイプ	対象	対応
100	192.168.123.10	2023/01/23	URL	<a href="#">yahoo-mbga.jp</a>	拒否

## 9. TCPMSS 設定

本項では、パケットの長さを整える TCPMSS 設定の手順について記載します。

(ADSL 通信や、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。



- ② TCPMSS(バイト)の記入欄を任意の値に変更し、『次へ』をクリックします。

(フレッツ ADSL, ひかり電話利用の場合は"1414"、フレッツ光プレミアム利用の場合は"1398"を使用します。)



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。

[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

- [URLフィルタリング](#)
- [IPフィルタリング](#)
- [振る舞い検知](#)
- [HTTPS通信](#)
- [メール設定](#)
- [今回のみ接続を許可](#)

[ホホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

- [メンテナンスアドレス](#)
- [アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

## ネットワーク設定

詳細

TCPMSS (バイト)	1500
--------------	------

設定しますか?

確認  
戻る

## 10. VPN 接続

本項では、MRB 同士で VPN を構築する手順について記載します。

### 10.1 VPN 応答側（親）の設定

本項では、MRB 同士で VPN を構築する際、固定 IP を使用する側の設定手順について記載します。

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『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、『追加』をクリックします。

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

※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。

[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  
[URLフィルタリング](#)  
[IPフィルタリング](#)  
[振る舞い検知](#)  
[HTTPS通信](#)  
[メール設定](#)  
[今回のみ接続を許可](#)

[ホホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定  
[メンテナンスアドレス](#)  
[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

**ネットワーク設定 - VPN追加**

[消去](#)
[戻る](#)
[VPN追加](#)

No. 1

設定  有効  無効

タイプ  開始側  応答側  MRB接続

リモートサイト   
(開始側はIP、応答側はID、MRB接続は機械番号)

ローカルサイト  グローバル固定IP  ID  無し  
  
(グローバル固定IP、ID、MRB接続は入力無し)

事前共通鍵

チェックアドレス  (相手側のLANアドレス)

IKEバージョン  IKEv2  IKEv1

UDPカプセル化  有効  無効

[追加](#)
[修正](#)
[削除](#)

リモートネットワーク   ネットワーク   [修正](#)   [削除](#)

- ④ VPN相手のネットワークアドレスとネットマスクを入力し、『追加』をクリックします。

The screenshot shows the 'VPN' configuration page. On the left is a navigation menu with categories like 'ネットワーク設定' (Network Settings), 'セキュリティ設定' (Security Settings), and 'ブリッジ設定' (Bridge Settings). The main area is titled 'ネットワーク設定 - VPN' and shows 'No. 1 リモートネットワーク追加' (Add Remote Network No. 1). Two input fields are present: 'ネットワーク (プレフィックス)' with the value '192.168.124.0' and 'ネットマスク (プレフィックス長)' with the value '255.255.255.0'. A red box highlights these two fields. Below the fields are buttons for '消去' (Delete), '戻る' (Back), and '追加' (Add). The '追加' button is highlighted with a red box.

- ⑤ 『追加』をクリックします。

The screenshot shows the same VPN configuration page, but now the '追加' button has been clicked. The main area now shows 'No. 1 リモートネットワーク追加 確認' (Add Remote Network No. 1 Confirmation). The input fields are now read-only and show the values '192.168.124.0' for the network and '24' for the netmask. The '追加' button remains highlighted with a red box.

⑥ 上の『VPN 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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

### ネットワーク設定 - VPN追加

**VPN追加**

No. 1

設定  有効    無効

タイプ  開始側    応答側    MRB接続

リモートサイト   
(開始側はIP、応答側はID、MRB接続は機械番号)

ローカルサイト  グローバル固定IP    ID    無し  
  
(グローバル固定IP、ID、MRB接続は入力無し)

事前共通鍵

チェックアドレス  (相手側のLANアドレス)

IKEバージョン  IKEv2    IKEv1

UDPカプセル化  有効    無効

リモートネットワーク

	追加	修正	削除
ネットワーク	修正	削除	削除
192.168.124.0/24	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

⑦ 『VPN 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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

### ネットワーク設定 - VPN追加 確認

**VPN追加**

No. 1

設定 有効

タイプ 応答側

リモートサイト 11111 (ID)

ローカルサイト 10.10.10.10 (グローバル固定IP)

事前共通鍵 \*\*\*\*\*

チェックアドレス 192.168.124.1

IKEバージョン IKEv2

UDPカプセル化 有効

リモートネットワーク

	追加	修正	削除
ネットワーク	修正	削除	削除
192.168.124.0/24	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

⑧ 『VPN 設定』をクリックし、設定を反映させたら完了です。

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

- [URLフィルタリング](#)
- [IPフィルタリング](#)
- [振る舞い検知](#)
- [HTTPS通信](#)
- [メール設定](#)
- [今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

- [メンテナンスアドレス](#)
- [アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN

VPN設定ボタンを選択してシステムに反映させてください。

消去 追加 修正 削除

No.	設定	タイプ	リモートサイト	ローカルサイト	修正	削除
1	有効	応答制	11111 (ID)	10.10.10.10 (IP)	<input type="radio"/>	<input type="checkbox"/>

## 10.2 VPN 開始側（子）の設定

本項では、MRB 同士で VPN を構築する際、固定 IP を使用しない側の設定手順について記載します。

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『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、『追加』をクリックします。

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

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  
[URLフィルタリング](#)  
[IPフィルタリング](#)  
[振る舞い検知](#)  
[HTTPS通信](#)  
[メール設定](#)  
[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定  
[メンテナンスアドレス](#)  
[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN追加

[消去](#) [戻る](#) [VPN追加](#)

No. 1

設定  有効  無効

タイプ  開始側  応答側  MRB接続

リモートサイト   
(開始側はIP、応答側はID、MRB接続は機械番号)

ローカルサイト  グローバル固定IP  ID  無し  
  
(グローバル固定IP、ID、MRB接続は入力無し)

事前共通鍵

チェックアドレス  (相手側のLANアドレス)

IKEバージョン  IKEv2  IKEv1

UDPカプセル化  有効  無効

[追加](#) [修正](#) [削除](#)

リモートネットワーク ネットワーク [修正](#) [削除](#)

④ VPN 相手のネットワークアドレスとネットマスクを入力し、『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  
[URLフィルタリング](#)  
[IPフィルタリング](#)  
[振る舞い検知](#)  
[HTTPS通信](#)  
[メール設定](#)  
[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定  
[メンテナンスアドレス](#)  
[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN

No. 1 リモートネットワーク追加

ネットワーク (プレフィックス)

ネットマスク (プレフィックス長)

[消去](#) [追加](#)

[戻る](#)

- ⑤ 『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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN

No. 1 リモートネットワーク追加 確認

ネットワーク 192.168.1.0

ネットマスク 24

- ⑥ 右上の『VPN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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN追加

No. 1

設定  有効  無効

タイプ  開始側  応答側  MRB接続

リモートサイト   
(開始側はIP、応答側はID、MRB接続は機械番号)

ローカルサイト  グローバル固定IP  ID  無し  
  
(グローバル固定IP、ID、MRB接続は入力無し)

事前共通鍵

チェックアドレス  (相手側のLANアドレス)

IKEバージョン  IKEv2  IKEv1

UDPカプセル化  有効  無効

リモートネットワーク

ネットワーク	修正	削除
192.168.1.0/24	<input type="radio"/>	<input type="checkbox"/>

⑦ 右上の『VPN 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

- [URLフィルタリング](#)
- [IPフィルタリング](#)
- [振る舞い検知](#)
- [HTTPS通信](#)
- [メール設定](#)
- [今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

- [メンテナンスアドレス](#)
- [アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN追加 確認

**VPN追加**

No.	1
設定	有効
タイプ	開始側
リモートサイト	10.10.10.10 (グローバル固定IP)
ローカルサイト	11111 (ID)
事前共通鍵	****1
チェックアドレス	192.168.1.1
IKEバージョン	IKEv2
UDPカプセル化	有効
リモートネットワーク	<u>ネットワーク</u>
	192.168.1.0/24

⑧ 『VPN 設定』をクリックし、設定を反映させたら完了です。

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

- [URLフィルタリング](#)
- [IPフィルタリング](#)
- [振る舞い検知](#)
- [HTTPS通信](#)
- [メール設定](#)
- [今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

- [メンテナンスアドレス](#)
- [アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN

VPN設定ボタンを選択してシステムに反映させてください。

**VPN設定**

No.	設定	タイプ	リモートサイト	ローカルサイト	修正	削除
1	有効	開始側	10.10.10.10 (IP)	11111 (ID)	<input type="radio"/>	<input type="checkbox"/>

### 10.3 VPN (MRB 接続) の設定

本項では、MRB 同士で VPN を構築する際、機械番号を使用する設定の手順について記載します。

※VPN 接続する各拠点で設定する必要があります。

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『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、『追加』をクリックします。

設定	有効
タイプ	MRB 接続
リモートサイト	MRB の機械番号
ローカルサイト	”なし”を選択
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	無効

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  
URLフィルタリング  
IPフィルタリング  
振る舞い検知  
HTTPS通信  
メール設定  
今回のみ接続を許可

ホワイトリスト処理

グループ設定

ブリッジ設定  
メンテナンスアドレス  
アクセス許可リスト

動作切替

一括設定

パスワード変更

ネットワーク設定 - VPN追加

削除 戻る VPN追加

No. 1

設定  有効  無効

タイプ  開始側  応答側  MRB接続

リモートサイト   
(開始側はIP、応答側はID、MRB接続は機械番号)

ローカルサイト   
(グローバル固定IP、ID、MRB接続は入力無し)

事前共通鍵

チェックアドレス  (相手側のLANアドレス)

IKEバージョン  IKEv2  IKEv1

UDPカプセル化  有効  無効

リモートネットワーク ネットワーク **追加** 修正 削除  
修正 削除

④ VPN 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/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  
URLフィルタリング  
IPフィルタリング  
振る舞い検知  
HTTPS通信  
メール設定  
今回のみ接続を許可

ホワイトリスト処理

グループ設定

ブリッジ設定  
メンテナンスアドレス  
アクセス許可リスト

動作切替

一括設定

パスワード変更

ネットワーク設定 - VPN

No. 1 リモートネットワーク追加

ネットワーク  (プレフィックス)

ネットマスク  (プレフィックス長)

削除 追加

戻る

- ⑤ 『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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN

**No. 1 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

- ⑥ 右上の『VPN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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN追加

No. 1

設定  有効  無効

タイプ  開始側  応答側  MRB接続

リモートサイト   
(開始側はIP、応答側はID、MRB接続は機械番号)

ローカルサイト  グローバル固定IP  ID  無し  
  
(グローバル固定IP、ID、MRB接続は入力無し)

事前共通鍵

チェックアドレス  (相手側のLANアドレス)

IKEバージョン  IKEv2  IKEv1

UDPカプセル化  有効  無効

リモートネットワーク ネットワーク  修正  削除

192.168.124.0/24

⑦ 右上の『VPN 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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN追加 確認

[VPN追加](#)

No.	1				
設定	有効				
タイプ	MRB接続				
リモートサイト	500119 (MRB接続)				
事前共通鍵	****1				
チェックアドレス	192.168.124.10				
IKEバージョン	IKEv2				
UDPカプセル化	無効				
リモートネットワーク	<u>ネットワーク</u>				
	192.168.124.0/24				

⑧ 『VPN 設定』をクリックし、設定を反映させたら完了です。

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

[URLフィルタリング](#)

[IPフィルタリング](#)

[振る舞い検知](#)

[HTTPS通信](#)

[メール設定](#)

[今回のみ接続を許可](#)

[ホワイトリスト処理](#)

[グループ設定](#)

ブリッジ設定

[メンテナンスアドレス](#)

[アクセス許可リスト](#)

[動作切替](#)

[一括設定](#)

[パスワード変更](#)

ネットワーク設定 - VPN

VPN設定ボタンを選択してシステムに反映させてください。

[VPN設定](#)

[消去](#) [追加](#) [修正](#) [削除](#)

No.	設定	タイプ	リモートサイト	ローカルサイト	修正	削除
1	有効	MRB接続	500119 (MRB接続)	無し	<input type="radio"/>	<input type="checkbox"/>

## 11. ログ閲覧

本項では、MRB で検閲したログの閲覧手順について記載します。

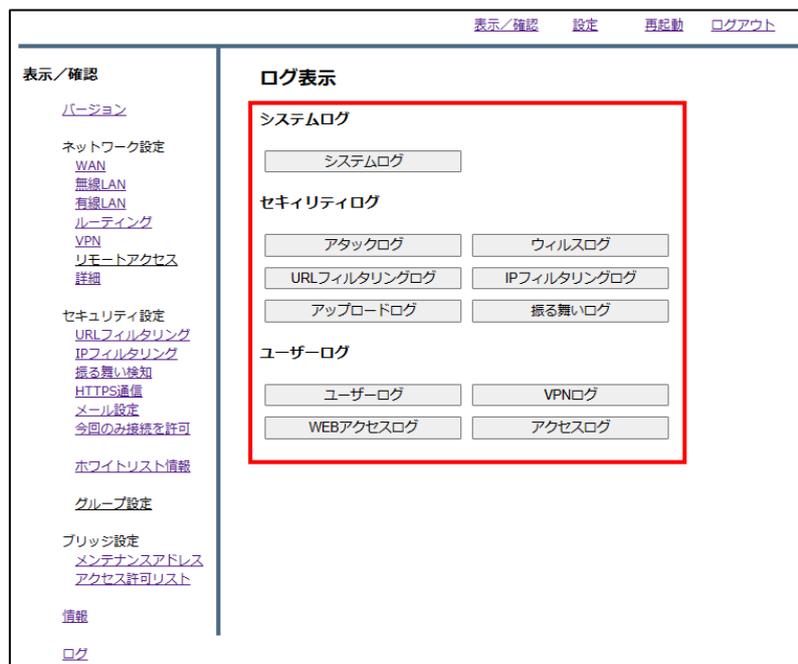
### 11.1 閲覧できるログ

本項では、ログの閲覧手順とログの種類について記載します。

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通りです。

ログ種別	内容
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	外部からアタックされた場合に記録されます。
ウイルスログ	ダウンロードしようとしたファイルがウイルス判定された場合に記録されます。また、ウイルス判定メール、スパム判定メール受信時にもログが記録されます。
URL フィルタリングログ	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	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 アクセス以外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。

## 11.2 ログ閲覧時の操作

本項では、ログを閲覧する際の操作について記載します。

- 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、現在閲覧している日付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 閲覧ログ操作は以下の通りです。

- ① …現在閲覧しているログ番号/すべてのログ件数です。
- ② …1 ページあたり 100 件ごとに閲覧するログを指定できます。
- ③ …ログ一覧に戻ります。
- ④ …現在閲覧しているログページ/すべてのログページです。
- ⑤ …ログページの遷移ができます。
- ⑥ …閲覧しているログの日付です。
- ⑦ …閲覧するログの日付を変更できます。[最新のログ]は本日のログです。
- ⑧ …閲覧している日付のログをダウンロードします。

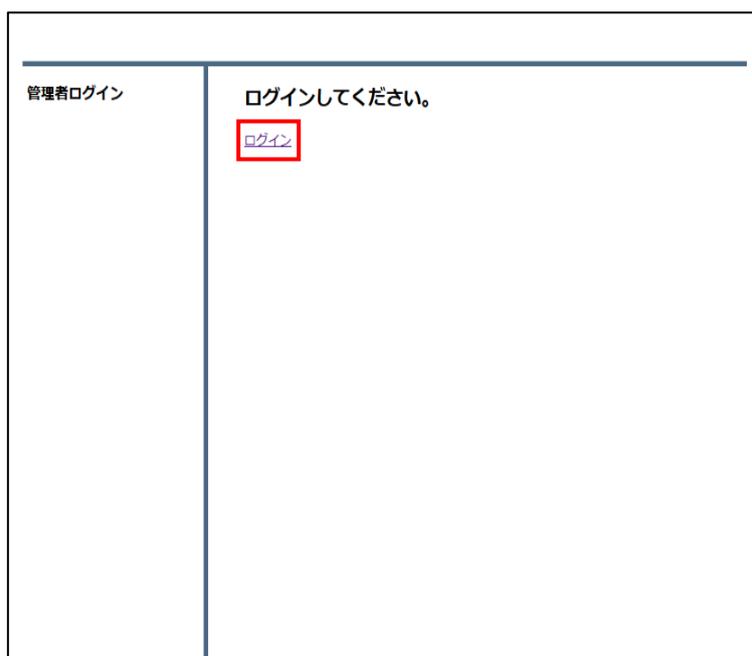
### 11.3 クラウドログの閲覧

本項では、クラウドログを閲覧する際の操作について記載します。

- ① 管理画面にログインする際に、『クラウドログイン』をクリックします。



- ② 『ログイン』をクリックします。



- ③ MRB 番号（機器コード）、ローカルログインで使用する管理者ユーザ、パスワードを入力し、『ログイン』をクリックします。

- ④ ログ一覧、リストの文字から閲覧したいログをクリックします。

クラウド ログビューアー

ログアウト

daily weekly

リストの文字をクリックすると、当該のログにジャンプします

URLブロック一覧(サイトカテゴリー)	0	URLブロック一覧(宛先IPアドレス)	0	アタック検知一覧	0
0	0	0	0	0	0
その値	0	その値	0	その値	0
IPブロック一覧(宛先IPアドレス)	0	IPブロック一覧(宛先IPアドレス)	0	ウイルス(スパムメール検知一覧)	0
0	0	0	0	0	0
その値	0	その値	0	その値	0
あるまい検知一覧(宛先IPアドレス)	69.173.158.64	あるまい検知一覧(宛先IPアドレス)	192.168.11.12	VPN接続状況	90
90	90	0	0	0	0
その値	0	その値	0	その値	0

⑤ 閲覧ログ操作は以下の通りです。

**ユーザー ログ一覧 2024/11/21**

日付	時刻	操作/登録申請情報	ホワイトリスト登録申請ユーザ
2024/11/21	14:35:59	SETUP_MODE	-
2024/11/21	15:28:46	SETUP_ONE_OUT	-
2024/11/21	15:29:01	SETUP_ONE_IN	-
2024/11/21	15:42:54	SETUP_LAN	-
2024/11/21	15:42:54	SETUP_LAN	-
2024/11/21	15:42:54	SETUP_LAN	-
2024/11/21	15:44:49	SETUP_ONE_OUT	-
2024/11/21	15:45:53	SETUP_ONE_IN	-
2024/11/21	15:45:57	SETUP_ONE_OUT	-
2024/11/21	15:46:16	SETUP_URLFILTERING_LEVEL	-

閲覧ログ: 13件 / ログ総数: 13件

- ① …現在閲覧しているログの件数/すべてのログ件数です。
- ② …閲覧するログの日付を変更できます。[最新のログ]は本日のログです。
- ③ …閲覧するログページを指定できます。
- ④ …ログページの遷移ができます。
- ⑤ …検索メニューを表示し、時刻・キーワードでログを検索できます。

検索メニュー    検索リセット

時刻検索:                      時間検索の場合、こちらも入力:                      フリーワード検索

hh:mm:ss, hh:mm                      hh:mm:ss, hh:mm                     

**検索**

- ⑥ …閲覧しているログをダウンロードできます。