



# マイクロリサーチ デバイス管理サービス

## MRL-IDM

### ユーザー向け運用マニュアル

ver.1.1.5

## はじめに

本マニュアルは、「マイクロリサーチ デバイス管理サービス」運用マニュアルです。

以下 MRL-IDM や本システムと出てくる箇所は「マイクロリサーチ デバイス管理サービス」のことを指します。

本編は、ユーザー向けに、運用していくにあたってのフロー、操作手順などについて記されております。

### ■本書の内容について

- 本書では、MR-GMxシリーズのデバイスを、総称して「**デバイス**」として表記します。

固有の機能や、説明箇所には、それぞれの型番を明記しておりますのでご注意ください。

- 以下の文字は非常に間違いやすいので注意して下さい。

半角数字「1」(イチ)と半角アルファベット小文字「l」(エル)、半角アルファベット大文字「I」(アイ)

半角数字「0」(ゼロ)と半角アルファベット小文字「o」(オー)、半角アルファベット大文字「O」(オー)

- 本書では一部の語句について略語表記している箇所があります。

- 本書中の設定画面は開発中のものです。実際の仕様と異なる場合があります。

- 以下のマークが付いている箇所は本システムをお使い頂く上で必ず確認または注意して頂きたい項目です。

確認

ここに記載されている内容を必ず確認・注意して下さい。

- 本書の内容は将来予告なしに変更することがあります。

- ・「Chatwork」は Chatwork 株式会社の商標または登録商標です。
- ・「slack」は、Slack Technologies, Inc.の登録商標です。
- ・「Microsoft Teams」は、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- ・その他、本書に記載されている会社名、商品名は各社の商標または登録商標です。

## 注意事項

MRL-IDM をご利用頂く前に以下の内容をあらかじめご確認下さい。

### ■デバイスの動作モードについて

MRL-IDM は、ルーターモード以外(アクセスポイントモード、ユニバーサルリピーターモード)で動作しているデバイスでは利用できません。

### ■デバイスのファームウェアバージョンについて

MRL-IDM をご利用頂く場合、デバイス側のファームウェアを以下のバージョン以降にバージョンアップする必要があります。

MR-GM3 シリーズ: v1.04.02 以降

MR-GM3L シリーズ: v1.04.02 以降

MR-GM3-W: v1.04.02 以降

上記より古いバージョンをご利用の方は、必ずファームウェアバージョンアップを行ってからご利用を開始して下さい。

MR-GM5A シリーズ、MR-GM5L シリーズは、出荷ファームウェアより対応可能です。

### ■デバイスの MAC アドレスについて

MRL-IDM では、デバイスの MAC アドレスで機器の判別を行います。

MRL-IDM 上でデバイスの MAC アドレスを正しく登録しないと、死活監視やステータスメールの取得が正しく行われませんのでご注意下さい。



デバイスの MAC アドレスは、本体底面のシール・設定画面等で確認する事ができます。

### ■デバイスグループの設定について

MRL-IDM では、デバイスをグループで管理します。

MRL-IDM で異なる機種(MR-GM3 シリーズ、MR-GM3L シリーズ、MR-GM5A シリーズ、MR-GM5L シリーズ)を混在して使用する場合は、必ず機種毎にデバイスグループを分けて登録して下さい。

**例: MR-GM3-DKS、MR-GM3-M、MR-GM3L-DKS、MR-GM3L-M を混在して使用する場合**

デバイスグループ A: MR-GM3-DKS、MR-GM3-M

デバイスグループ B: MR-GM3L-DKS、MR-GM3L-M

## もくじ

1. MRL-IDM とは？ .....	1
2. MRL-IDM における管理者・ユーザーの役割 .....	3
3. ユーザーの役割 .....	4
3-1. デバイスの登録 .....	5
3-1-1. デバイスの MAC アドレスとシリアル No の確認 .....	5
3-1-2. デバイスを登録する .....	6
3-1-3. デバイスの入れ替え手順 .....	9
3-2. アラートの設定 .....	10
3-2-1. 死活監視アラート条件設定について .....	11
3-2-2. ステータスアラート条件設定について .....	18
3-2-3. アラート通知先設定 .....	25
3-2-4. ステータスアラート条件の設定例 .....	28
3-3. デバイスの状態を確認する .....	29
3-3-1. デバイス監視 .....	29
3-3-2. デバイスのログを確認する .....	30
3-3-3. 傾向をグラフで確認する .....	34
3-3-4. WEB 通信 .....	35
3-4. 新しいファームウェアの適用 .....	37
3-4-1. MRL-IDM 上でファームウェアのバージョンを指定する .....	38
3-4-2. ファームウェアの更新 .....	39
3-5. サジェストについて(ビジネスプランのみ) .....	40
3-6. デバイスの設定(MR-GM3/MR-GM3L) .....	41
3-6-1. HTTP 回線監視の設定 .....	41
3-6-2. NTP クライアント機能の設定 .....	42
3-6-3. メール送信機能の設定 .....	43
3-6-4. タイマー自動ファームウェア更新機能の設定 .....	45
3-6-5. WAN 側からの設定(リモート設定)を許可する .....	47
3-7. デバイスの設定(MR-GM5A/MR-GM5L) .....	49
3-7-1. HTTP 回線監視の設定 .....	49
3-7-2. NTP クライアント機能の設定 .....	50
3-7-3. メール送信機能の設定 .....	51
3-7-4. タイマー自動ファームウェア更新機能の設定 .....	53
3-7-5. WAN 側からの設定(リモート設定)を許可する .....	55
4. 画面操作説明 .....	57
4-1. MRL-IDM へのログイン .....	58
4-2. デバイス管理 .....	59
4-2-1. 新規登録 .....	61

4-2-2. 編集 .....	63
4-2-3. 削除 .....	65
4-3. デバイス監視 .....	66
4-4. ファームウェア更新 .....	67
4-4-1. 新規登録 .....	69
4-4-2. 編集 .....	70
4-4-3. 削除 .....	71
4-5. 死活監視アラート条件設定 .....	72
4-5-1. 新規登録 .....	74
4-5-2. 編集 .....	76
4-5-3. 削除 .....	77
4-6. ステータスアラート条件設定 .....	78
4-6-1. 新規登録 .....	81
4-6-2. 編集 .....	83
4-6-3. 削除 .....	84
4-7. HTTP 監視 URL 設定 .....	85
4-7-1. 新規登録 .....	86
4-7-2. 編集 .....	87
4-7-3. 削除 .....	88
4-8. ステータスメールログ設定 .....	89
4-8-1. 新規登録 .....	90
4-8-2. 編集 .....	91
4-8-3. 削除 .....	92
4-9. アラート通知先設定 .....	93
4-9-1. 新規登録 .....	94
4-9-2. 編集 .....	95
4-9-3. 削除 .....	96
4-10. 死活監視アラートログ .....	97
4-10-1. 詳細 .....	99
4-11. ステータスアラートログ .....	100
4-11-1. 詳細 .....	102
4-12. HTTP 監視ログ .....	103
4-13. ステータスメールログ .....	105
4-13-1. 詳細 .....	107
4-14. デバイスオペレーションログ .....	108
4-14-1. 詳細 .....	110
5. MRL-IDM に関するお問い合わせ .....	111

## 1. MRL-IDM とは？

「MRL-IDM」は、MR-GMx シリーズのデバイス（以下**デバイス**という表記だけの場合は、**MR-GMx シリーズのデバイス**のことを指します。また、今後、他のマイクロリサーチ社製デバイスも随時追加予定ですので、あえてデバイスと表記することもあります。）をクラウドで一元的に管理し、デバイスの死活監視・ステータス監視、ファームウェアの自動更新を可能にするためのシステムです。

本システムは、WEB システムとして、下記の機能を提供します。

### ●デバイス管理

デバイスの個々の機体を登録し、管理する機能。

### ●デバイス監視

デバイスからの HTTP 通信による回線監視機能、あるいはメール送信機能により、状態を監視する機能。

### ●死活監視アラート条件設定

デバイスグループ毎に、どのような間隔で死活監視を行い、どこにアラートを通知するかを設定する機能。

### ●ステータスアラート条件設定

デバイスグループ毎に、デバイスから送られてくるステータスメールログを解析し、デバイスの状態からアラートを通知するために条件を設定する機能。

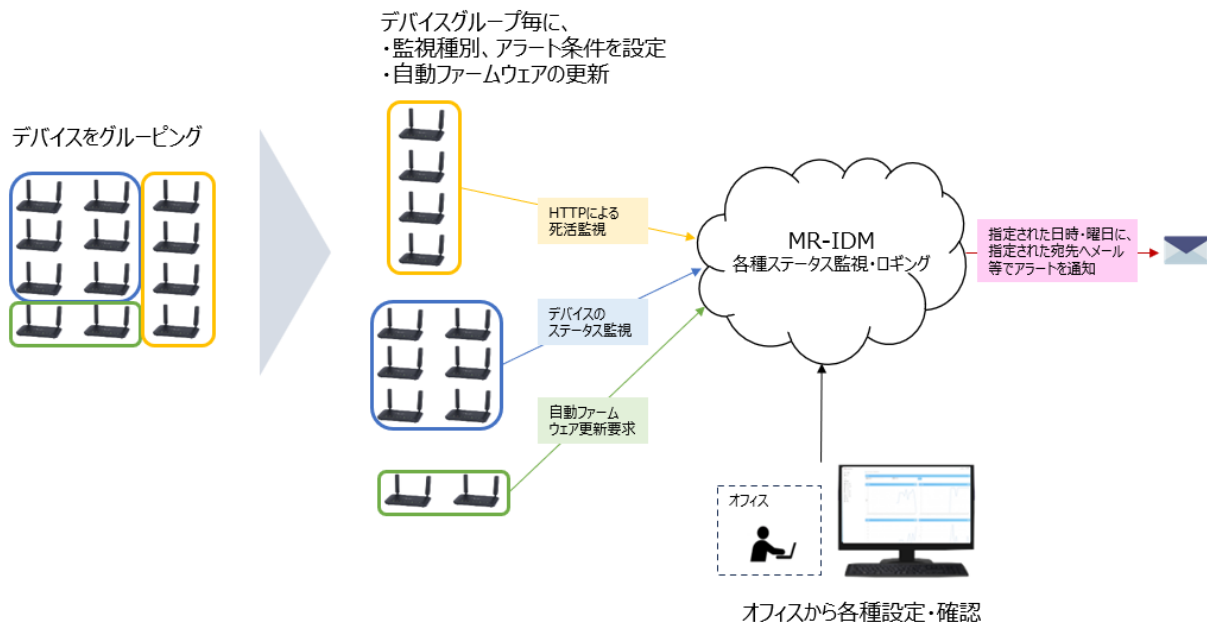
### ●ログ管理

各種ログ（死活監視アラートログ、ステータスアラートログ、HTTP 監視ログ、ステータスメールログ、デバイスオペレーションログ）を保持し、過去の履歴を辿れる機能。

### ●ファームウェア更新

デバイスグループ毎（機種毎）に、ファームウェアダウンロード用 URL を設定し、ファームウェアバージョンを適用。自動ファームウェア更新を行う機能。

### ■利用イメージ



また、本システムをご利用の際は、必要に応じてデバイス本体側で以下の設定を行って下さい。

・**デバイスの死活監視を行う場合**

→HTTP 回線監視の設定で、MRL-IDM 用の監視 URL を追加して下さい。

・**メール送信機能、タイマー自動ファームウェア更新機能を使用する場合**

→NTP クライアント機能の設定を行って下さい。

・**デバイスのステータス監視を行う場合**

→メール送信設定で、メール送信の宛先に MRL-IDM 用のメールアドレスを設定して下さい。

・**自動ファームウェア更新を行う場合**

→ファームウェアダウンロード URL にデバイスグループに設定した FW 更新 URL を設定して下さい。

・**リモート設定を行う場合**

→WAN 側からの設定を許可する設定をして下さい。

設定方法については「3-6.デバイスの設定(MR-GM3/MR-GM3L)」 「3-7.デバイスの設定(MR-GM5A/MR-GM5L)」を参照して下さい。

## 2. MRL-IDM における管理者・ユーザーの役割

運用面における、本システムの管理者・ユーザーの役割は以下に分類できます。

管理者	<ul style="list-style-type: none"> <li>・企業内のユーザー管理者 MRL-IDM を利用してデバイス管理を行う管理者ユーザー</li> <li>・ルール: 企業に1人。ユーザーからの昇格は不可 管理者の情報(名前、メールアドレス)は変更可能</li> <li>・ユーザーとともに、自社内のデバイスの運用管理のポリシーを決定 <ul style="list-style-type: none"> <li>- デバイスのグルーピング</li> <li>- 担当ユーザーとデバイスグループの紐づけ</li> <li>- 監視・アラートなど運用ポリシー決定</li> </ul> </li> <li>・ユーザーのサポート</li> </ul>
ユーザー	<ul style="list-style-type: none"> <li>・一般ユーザー MRL-IDM を利用してデバイス管理を行う</li> <li>・管理者とともに、自社内のデバイスの運用管理のポリシーを決定</li> <li>・デバイスのキッティング、登録、運用</li> <li>・アラート運用(ログ確認など状態監視)</li> <li>・新しいファームウェアの適用</li> </ul>

また、「管理者」でログインした場合と、「ユーザー」でログインした場合で表示されるメニュー項目が異なります。



※サジェストはビジネスプランのみ表示されます。

管理者とユーザーを明確に分けていない場合、管理者が行う運用とユーザーが行う運用が重なります。

本マニュアルでは、ユーザーの方がこのシステムを運用するにあたって、どのようなシナリオケースがあるか、またどのように設定するのかなどを中心に記載していきます。

また、「4.画面操作説明」で各画面についての詳細を説明していますので、そちらもご確認下さい。



### 3. ユーザーの役割

ユーザーが本システムを運用する際の役割として以下が考えられます。

- デバイスの登録と管理
- 死活監視アラート、ステータスアラートの条件設定
- デバイスの状態を確認する
- 新しいファームウェアの適用

主に「デバイス監視」を利用することになりますが、運用が開始する前には「デバイス管理」や、「死活監視アラート条件設定」、「ステータスアラート条件設定」を行います。

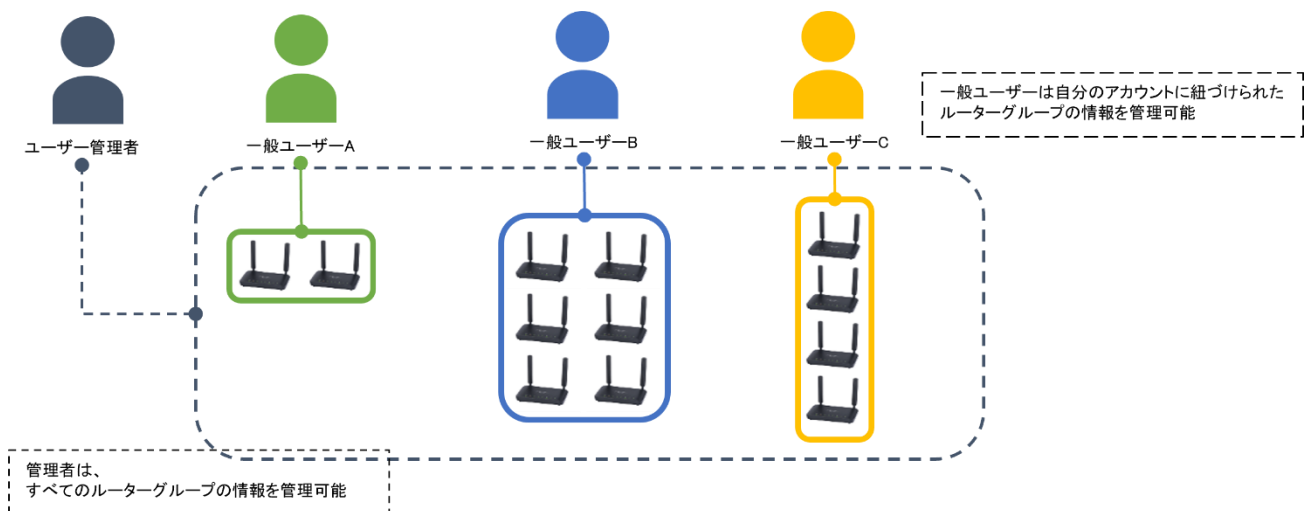
管理者権限でないと、デバイスグループを登録・変更できませんので、運用中変更が必要な場合は、管理者にお問い合わせ下さい。

また、ログイン時のパスワードを忘れた場合やメールアドレスが変更になった場合は、管理者権限で「ユーザーアカウント管理」から確認、設定を行う必要がありますので、その際も管理者にお問い合わせ下さい。

ユーザーは、自分の管轄の「デバイスグループ」に関する情報にだけアクセスできます。

他のユーザーのデバイスグループにはアクセスできません。

下図のような全体構造になっています。



以降、運用におけるそれぞれのケースについて説明していきます。

### 3-1. デバイスの登録

MRL-IDM にデバイスを登録する方法を説明します。

#### 3-1-1. デバイスの MAC アドレスとシリアル No の確認

MRL-IDM は、デバイスを MAC アドレスで判別します。

MRL-IDM にデバイスを登録するには、デバイスの有線 LAN ポートの MAC アドレスの情報が必須です。

また、シリアル No も登録すると、よりデバイスを管理しやすくなります。

デバイスを登録する前に、デバイスの MAC アドレスとシリアル No を確認して下さい。

- デバイス本体の底面シールに MAC アドレスとシリアル No (S/N) が記載されています。



- 設定画面トップ(状態表示・ステータス)画面でも、有線 LAN ポートの MAC アドレスは確認できます。

#### 【MR-GM3 の例】

有線LAN	
IPアドレス	192.168.0.1
サブネットマスク	255.255.255.0
DHCPサーバー	有効
MACアドレス	00:10:38:xx:xx:xx

- 既にデバイスのメール送信機能を使用している場合は、メールの Subject(題名)でも有線 LAN ポートの MAC アドレスを確認することができます。(青線部分が MAC アドレスです。)

MR-GM3 00:10:38:xx:xx:xx Status

確認

シリアル No は、底面のシール以外に確認する事はできません。

### 3-1-2. デバイスを登録する

①MRL-IDM にログインして下さい。

<https://mrlidm.jp/>

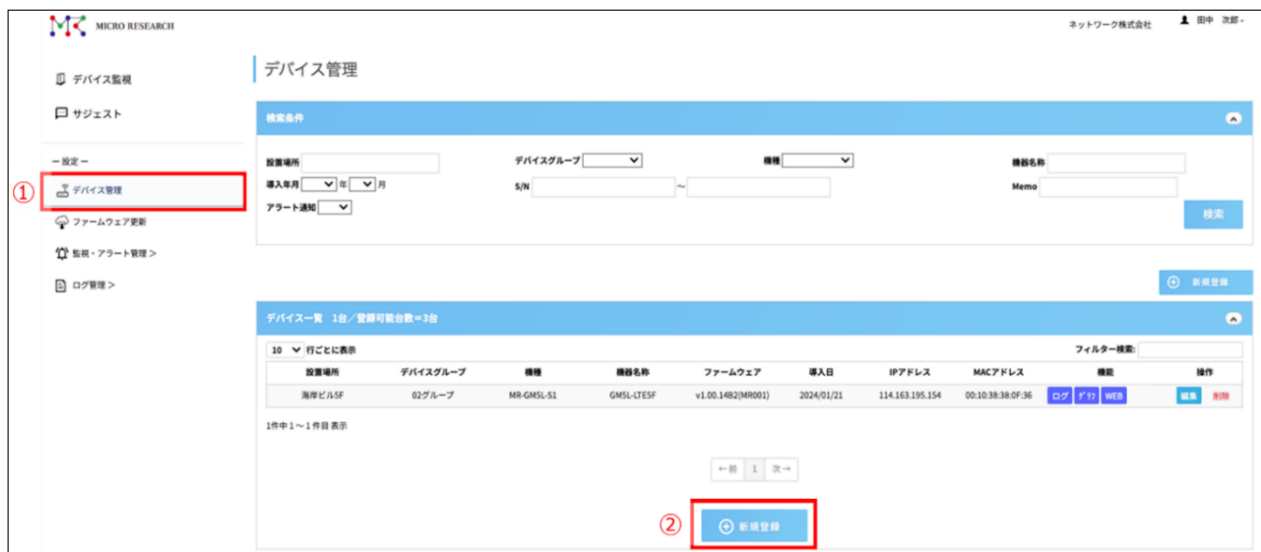
上記 URL にアクセスするとログイン画面が開きます。



The login form is titled "ログイン" (Login). It contains two input fields: "ID" and "パスワード" (Password). Below these fields is a blue button labeled "ログイン" (Login).

管理者より通知された、ID、パスワードでログインして下さい。

②「デバイス管理」メニューをクリックして下さい。



The screenshot shows the "デバイス管理" (Device Management) page. On the left sidebar, the "デバイス管理" menu item is highlighted with a red box and a circled 1. The main content area has a search bar at the top with fields for "設置場所" (Installation Location), "デバイスグループ" (Device Group), "機種" (Model), "機種名" (Model Name), "導入年月" (Introduction Year/Month), "S/N", and "アラート通知" (Alert Notification). Below the search bar is a table titled "デバイス一覧 1台/登録可能台数=3台" (Device List 1 device/Total registrable devices=3). The table has columns for "設置場所" (Installation Location), "デバイスグループ" (Device Group), "機種" (Model), "機種名" (Model Name), "ファームウェア" (Firmware), "導入日" (Introduction Date), "IPアドレス" (IP Address), "MACアドレス" (MAC Address), "機能" (Function), and "操作" (Action). The table contains one row of data. At the bottom right of the table, there is a "新規登録" (New Registration) button, which is highlighted with a red box and a circled 2.

設置場所	デバイスグループ	機種	機種名	ファームウェア	導入日	IPアドレス	MACアドレス	機能	操作
海岸ビル5F	02グループ	MR-GMSL-S1	GMSL-LTESF	v1.00.1482(MR001)	2024/01/21	114.163.195.154	00:10:38:38:0F:36	ログ デリ WEB	編集 削除

「新規登録」ボタンをクリックして下さい。

デバイス 新規登録

×

設置場所

機器名称 必須

MACアドレス 必須

デバイスグループ 必須

▼

アラート通知 必須

有効▼

S/N

導入日

IPアドレス

WEBポート

WEBログインID

WEBパスワード


Memo

登録

閉じる

設置場所	デバイスの設置場所を入力して下さい。
機器名称	デバイスの名称を入力して下さい。 <b>デバイスの判別がつくように個別の設定値にする事を推奨します。</b>
MAC アドレス	デバイスの LAN ポート MAC アドレスを入力して下さい。 デバイスの LAN ポート MAC アドレスは、底面のシールや設定画面で確認する事ができます。 「MAC:001038xxxxxx」の「001038xxxxxx」を入力して下さい。 <b>MRL-IDM はデバイスを MAC アドレスで判別します。MAC アドレスが正しく設定されていないと MRL-IDM を利用する事はできませんのでご注意ください。</b>
デバイスグループ	このデバイスが所属するデバイスグループを選択して下さい。
アラート通知	死活監視アラート通知、ステータスアラート通知の有効・無効を設定します。 無効の場合、アラートチェック、ログ表示を行いません。
S/N	デバイスのシリアル No を入力して下さい。 デバイスの底面に貼られているシールの「S/N:GMxxxxxxxxxx」の GMxxxxxxxxxx を入力して下さい。
導入日	導入設置日を選択して下さい。
IP アドレス	デバイスの WAN 側 IP アドレスを入力して下さい。 リモート設定を行う場合、ここで設定した IP アドレスへアクセスします。 空欄にした場合、ステータスメールで取得したIPアドレスへアクセスします。
WEB ポート	デバイスの WEB 設定ポート番号を入力して下さい。 デバイス側で WEB 設定ポート番号を変更している場合は、変更したポート番号を入力して下さい。

WEB ログイン ID	デバイスの設定画面にログインするためのログイン ID を保存する場合、入力して下さい。 空欄にした場合、ログインIDの入力を求められます。 (MR-GM3 シリーズ、MR-GM3L シリーズのみ保存可能です)
WEB パスワード	デバイスの設定画面にログインするためのパスワードを保存する場合、入力して下さい。 空欄にした場合、パスワードの入力を求められます。 (MR-GM3 シリーズ、MR-GM3L シリーズのみ保存可能です)
Memo	デバイスに関するメモを入力できます。

	<p>リモートでデバイスの設定画面にアクセスするためには、以下の条件が必要です。</p> <ul style="list-style-type: none"> <li>・デバイスの WAN 側 IP アドレスがグローバル IP アドレスである事。</li> <li>・デバイス側で「WAN 側からの設定画面へのアクセスを許可する設定」がされている事。</li> </ul> <p>デバイス側の設定方法については、以下を参照して下さい。</p> <p>MR-GM3/MR-GM3L:「3-6-5.WAN 側からの設定 (リモート設定) を許可する」 MR-GM5A/MR-GM5L:「3-7-5.WAN 側からの設定 (リモート設定) を許可する」</p>
---	---

「登録」ボタンを押して、保存して下さい。

デバイス一覧に、登録したデバイスの情報が表示されていることを確認して下さい。

現在のプランでのデバイス登録可能台数に達している場合、「新規登録」ボタンをクリックすると下記エラーメッセージが表示されます。この場合、未使用のデバイスを削除するか、プランの変更について管理者に相談して下さい。

すでに登録台数に達しています。デバイスを削除してから登録するか、プランを変更してください。

現在の登録可能台数は、デバイス一覧の上部に現在登録されているデバイスの数と登録可能台数が表記されています。

デバイス一覧 3台／登録可能台数=20台

以降は、この画面から、デバイスに関する操作、編集が行えます。

デバイス一覧 1台／登録可能台数=3台									
10	行ごとに表示	フィルター検索:							
設置場所	デバイスグループ	機種	機器名称	ファームウェア	導入日	IPアドレス	MACアドレス	機能	操作
海岸ビル5F	02グループ	MR-GM3-DKS	MR-GM3LTEIF	v1.04.02(MR001)	2022/10/30	192.168.1.100	00:10:38:77:21:69	ログ グラフ WEB	編集 削除
1件中 1 ~ 1 件目 表示									
<input type="button" value="← 前"/> <input type="button" value="1"/> <input type="button" value="次 →"/>									
<input type="button" value="新規登録"/>									


デバイスのステータスメールログを見る、「ログ」ボタンをクリックして下さい。

各種指標をグラフで見たい時は、「グラフ」ボタンをクリックして下さい。

デバイスをリモート設定したい場合は、「WEB」ボタンをクリックして下さい。

デバイス情報を編集したい場合は、「編集」ボタンをクリックして下さい。

デバイスを撤去する場合は、デバイス情報を「削除」して下さい。

	デバイス情報を削除した場合、削除したデバイスのログも同時に削除されますのでご注意下さい。
---	--

### 3-1-3. デバイスの入れ替え手順

デバイスが故障した場合等に、機器の入れ替えが必要になった場合の手順について説明します。

- ①デバイス管理設定(編集)で、当該機器の「アラート通知」を無効に設定変更します。  
それによりアラート通知が送信されなくなります。



- ②以下のどちらかの方法で機器の入れ替えを実施して下さい。

**方法 1:「デバイス管理」画面で撤去した機器のデバイス情報を削除して、新たな機器を新規登録する。**

この方法の場合、当該デバイスの各種ログは全て削除されます。

**方法 2:「デバイス管理」画面(編集)で当該機器の MAC アドレス、S/N(シリアル No)を、新たな機器の情報に変更する。**

方法 1、方法 2、どちらも問題ありませんが、入れ替える機種が変更になる場合は注意が必要です。

**例:MR-GM3 シリーズから MR-GM3L シリーズへ入れ替え等**

MRL-IDM で「自動ファームウェア更新」をご利用の場合、機種別、デバイスグループ別にファームウェア更新 URL を設定します。

異なる機種のファームウェアを適用する(例えば MR-GM3 シリーズに MR-GM3L シリーズのファームウェアを適用する等)と故障の原因となります。

同じファームウェアを適用できる機種は、以下の 4 種類のグループが存在します。

MR-GM3 シリーズ、MR-GM3L シリーズ、MR-GM5A シリーズ、MR-GM5L シリーズ

機種を変更する場合は、入れ替え後の機種が所属できる既存のデバイスグループに変更するか、管理者に依頼してデバイスグループを新規作成して下さい。

また、その場合はデバイス側の「ファームウェアダウンロード URL」の設定変更も必要になります。



デバイスグループは、機種ごと(MR-GM3 シリーズ、MR-GM3L シリーズ、MR-GM5A シリーズ、MR-GM5L シリーズ)で分けて登録下さい。

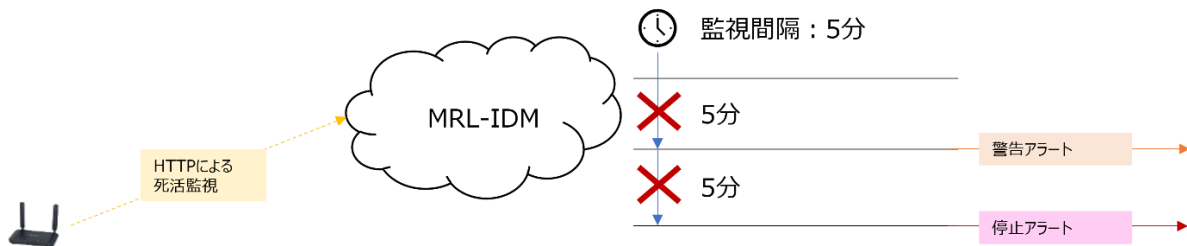
- ③方法 2 で入れ替えた場合は、デバイス管理設定(編集)で、当該機器の「アラート通知」を有効に戻して下さい。

### 3-2. アラートの設定

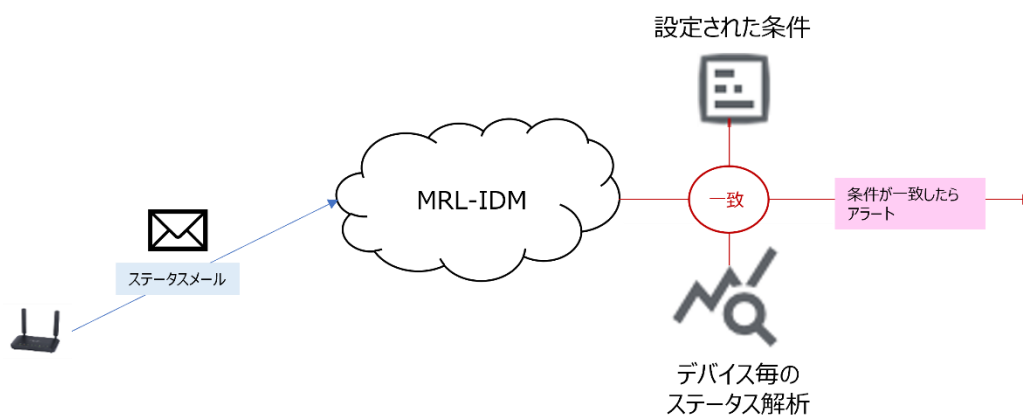
MRL-IDM で提供する監視、アラートについては、2 種類の監視があります。

- 死活監視アラート
- ステータスアラート

- 死活監視アラートは、デバイスから送信される通信を MRL-IDM 上で監視して、設定された監視間隔の時間通信が無い場合アラートを送信します。



- ステータス監視アラートは、デバイスから送られてくるステータス(各種データ)メールの情報をもとに、どの項目がどのようになったらアラートを送るか設定された条件と、MRL-IDM のステータス解析結果が一致したらアラートを送信します。



「どの指標がどうなったらアラートを送るか」、御社のアラートポリシーをもとに、デバイスグループ毎にアラートの設定を行なって下さい。

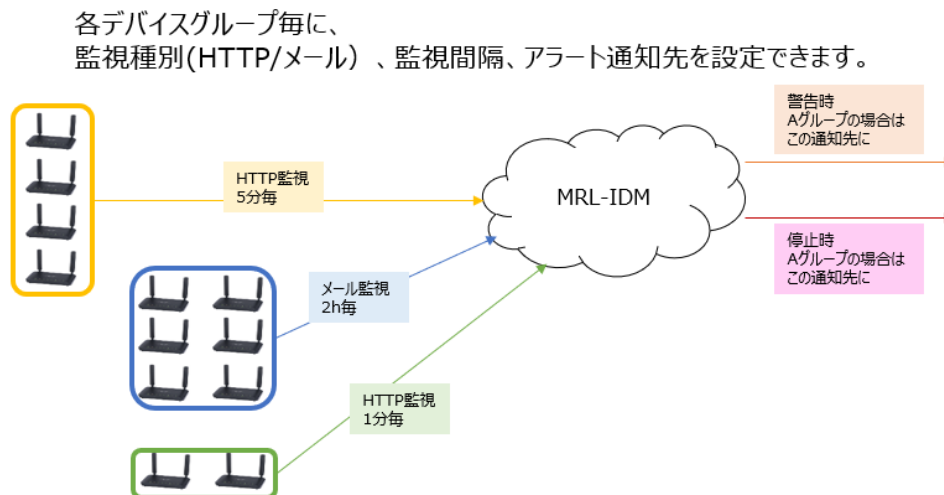
また、MRL-IDM 上では、アラートの条件はデバイスグループ単位で設定する機能となります。  
運用上さらにデバイスグループが必要になった場合は、管理者にデバイスグループの追加を依頼して下さい。

### 3-2-1. 死活監視アラート条件設定について

確認

死活監視を行う場合、死活監視アラート条件設定は必須です。  
死活監視アラート条件設定を行っていない場合や、登録済みの死活監視アラート条件設定を無効にすると設定に紐づけされたデバイスの死活監視は行われませんのでご注意ください。

死活監視アラート条件設定は、デバイスシリーズ、デバイスグループごとに、監視種別、監視間隔、アラート通知先を設定できます。



死活監視アラート条件設定メニューで、

- ・どのデバイスグループを対象とした設定か？
- ・デバイスシリーズは？
- ・監視種別は？(HTTP 監視 or メール監視)
- ・監視間隔は？
- ・アラート通知先は？

を紐づけて、死活監視を行います。

また、アラート通知した際のログは、ログ管理の死活監視アラートログに保存されます。

一覧を見ると、すでに、[デフォルト設定]という名前で、太字で表示されている条件があるかもしれません。

これは、管理者アカウントが設定した、全てのデバイスグループ共通のデフォルトとして設定されている条件になります。

この[デフォルト設定]がある場合、特に個別にデバイスグループ毎に条件を設定しなくても、死活監視は動作します。

死活監視アラート条件一覧 2件						
デバイスグループ	監視種別	監視間隔	警告時通知先	停止時通知先	状態	操作
★[デフォルト設定]	HTTP監視 (GMSL)	5分	警告の時の通知先	緊急時	有効	
[個別設定] 02グループ A(01グループ)	HTTP監視 (HTTP監視)	5分	警告の時の通知先	緊急時	有効	編集 削除

2件中 1 ~ 2 件目 表示

管理者アカウントが設定した「デフォルト設定」の死活監視アラート条件

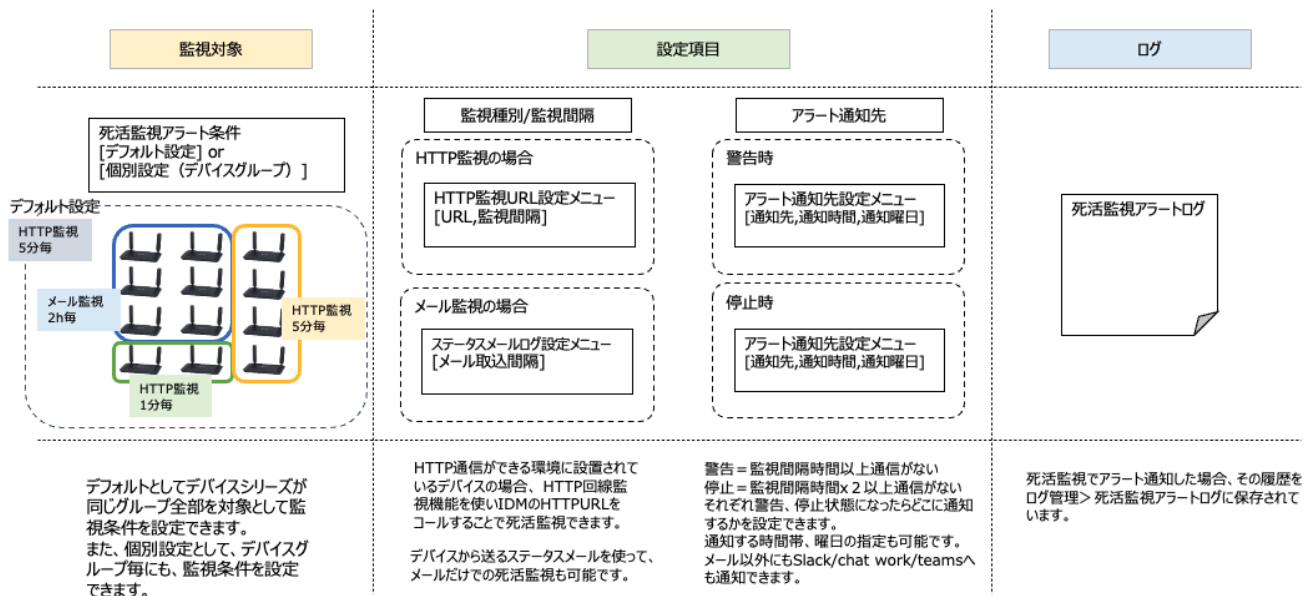
他のユーザーと共同管理しているデバイスグループ

[デフォルト設定]と違う条件、通知先で、自分の管理するデバイスグループについて条件を設定したい場合は、まず管理者に確



認をとって、[個別設定]として登録してください。

[デフォルト設定]と[個別設定]がある場合、個別設定が優先されます。



このような構成で、設定を行います。[デフォルト設定]と特に条件が変わらない場合、[デフォルト設定]のままご利用下さい。

具体的な操作の流れを説明します。

- ①「監視・アラート管理」>「死活監視アラート条件設定」メニューをクリックして下さい。



- ②「新規登録」ボタンをクリックして下さい。

×

死活監視アラート条件 新規登録

デバイスシリーズ **必須**

デバイスグループ **必須**

未選択です

監視種別 **必須**

監視間隔 **必須**

通知先 **必須**

警告時: **新規登録**

停止時: **新規登録**

状態 **必須**

有効

※条件を登録しなかったら「新規登録」で各条件を登録してください。

※「編集」で今選択されている条件の編集を行うことができます。


登録

閉じる

デバイスシリーズ	どのデバイスシリーズを対象とするかを選択して下さい。
デバイスグループ	条件を適用するデバイスグループを選択して下さい。 デバイスグループは重複して条件を設定することはできません。
監視種別	HTTP 監視かメール監視を選択します。

<b>監視間隔</b>	<p>【HTTP 監視】:監視間隔は「HTTP 監視 URL 設定」メニューで設定した「HTTP 監視間隔」の値が採用されます。</p> <p>【メール監視】:監視間隔は「ステータスメールログ設定」メニューで設定した「取り込み間隔」の値が採用されます。</p> <p>・監視間隔の横に表示される「新規登録」を押すと、新たに HTTP 監視 URL やステータスメールログを作成することができます。</p> <p>・監視間隔を選択すると、監視間隔時間がテキストで表示されるようになります。ここで「編集」を押すと、そのまま HTTP 監視 URL やステータスメールログの編集を行い、間隔時間を変更することができます。</p>
<b>通知先(警告時、停止時)</b>	<p>アラート通知先を選択して下さい。</p> <p>アラート通知先の設定については「3-2-3.アラート通知先設定」を参照して下さい。</p>
<b>状態</b>	<p>有効＝死活監視チェックを行い、監視ログも保存されます。</p> <p>無効＝死活監視チェックが行われず、監視ログも保存されません。</p>

「登録」ボタンを押して、保存して下さい。

	[デフォルト設定]は、管理者アカウントでのみ登録、編集、削除が行えます。
---	--------------------------------------

## ●死活監視種別について

### 【HTTP 監視】

HTTP による死活監視は、デバイス側の回線監視機能の HTTP 送信機能を使用して死活監視を行います。

Wireless Router for Mobile  
**MR-GM3**

設定項目  
 状態表示  
 簡易設定  
 動作モード設定  
 無線LAN設定  
 ネットワーク設定  
 LAN設定  
**WAN設定**  
 スタティックルーティング設定  
 簡易DNS設定  
 ファイアウォール設定  
 VPN設定  
 QoS設定  
 マネージメント  
 再起動  
 ログアウト

### WAN設定

WAN側（ETH1またはUSB）接続モード等の設定を行います。

プライマリ接続モード	モバイルデータカード(内蔵)	プライマリ接続モード設定
セカンダリ接続モード	未使用	セカンダリ接続モード設定

☐ UPnPを有効にする  
☒ IPsecパススルーを有効にする  
☒ PPTPパススルーを有効にする  
☒ L2TPパススルーを有効にする  
☐ IPv6パススルーを有効にする  
☐ NetBIOS over TCP/IP、Microsoft-DSの透過を有効にする  
☒ 高速パケット処理(FastPath)を有効にする

UDPセッション時間(単方向) 60 (0~3600秒)  
 UDPセッション時間(双方向) 90 (0~3600秒)  
 IP変換 セッション数 2048 (2048~8192)

WAN側からのPing応答：無効

アタック検出 5 1秒間に許容するPingアクセス数。(0~100)  
 WAN側からの設定画面ログオン：有効  
 アタック検出 30 30秒間に許容する最大TCP/IPコネクション数。(0~100)

回線監視機能 HTTPによる監視 ▼

発行間隔 5分 ▼

連続失敗検出回数 2 (1~60)

☐ 回線監視通信の送信元にLAN側IPアドレスを使用する

宛先1 <https://mrlidm.jp/monitoring/>

宛先2 www.

宛先3 www.

設定保存

MRL-IDM の「HTTP 監視 URL 設定」で作成した監視 URL を「宛先」に設定して下さい。

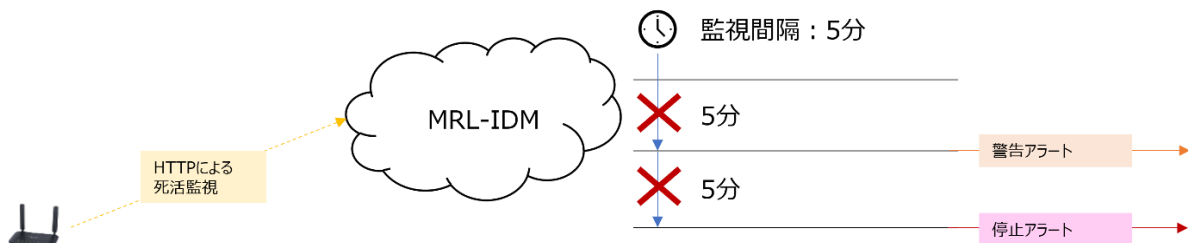
確認

宛先は MRL-IDM の HTTP 監視 URL 以外も設定して下さい。

MRL-IDM の監視 URL のみ設定した場合、MRL-IDM のメンテナンス等でHTTP通信が不通になるとデバイスが回線障害と判断して回線の再接続やシステムの再起動等のリカバリ動作を行います。

また、発行間隔は MRL-IDM の監視間隔設定より短くなるようにして下さい。

例:MRL-IDM の「HTTP 監視 URL 設定」の監視間隔が 10 分の場合、発行間隔を 5 分で設定して下さい。



監視間隔で設定した時間、デバイス側から通信がなかった場合は、警告と判断します。

監視間隔で設定した時間、2 回連続でデバイス側から通信がなかった場合は、停止と判断します。

通知先で指定したアラート通知先へ通知を行います。

## 【メール監視】

メール監視は、デバイス側のメール送信機能で送られてくるステータスメールを使用して死活監視を行います。  
HTTP 回線監視が使えない環境でお使いの場合は、こちらを選択して下さい。

Wireless Router for Mobile  
**MR-GM3**

設定項目

- 状態表示
- 簡易設定
- 動作モード設定
- 無線LAN設定
  - ネットワーク設定
  - ファイアウォール設定
  - VPN設定
  - QoS設定
- マネージメント
  - システム設定
  - 時刻情報・タイマー再起動設定
  - DDNS設定
  - メール送信設定**
  - システムログ
  - ファームウェア更新
  - 設定保存・読み込み
  - ユーザー・パスワード設定
- 再起動
- ログアウト

### メール送信設定

メール送信設定を行います。

☒ メール送信機能を有効にする

メール送信サーバー: mail.mrlidm.jp

メール送信サーバーポート番号: 587 (1~65535)

送信元メールアドレス: @mrlidm.jp

宛先メールアドレス: system01@mrlidm.jp

接続保護: なし

☐ StartTLS(RFC 3207) 拡張をしない

認証方法: 平文

ユーザー名:

パスワード:

☐ メール送信グリーティングメッセージ(EHLO)に送信元メールアドレスのドメインを使用する

☒ WANインターフェース有効時のメール送信を有効にする

☒ 定期メール送信を有効にする

送信間隔: 2 時 0 分 0 秒 (0~24時間)

☐ 時刻指定メール送信を有効にする

メール送信スケジュール

☐ 毎日

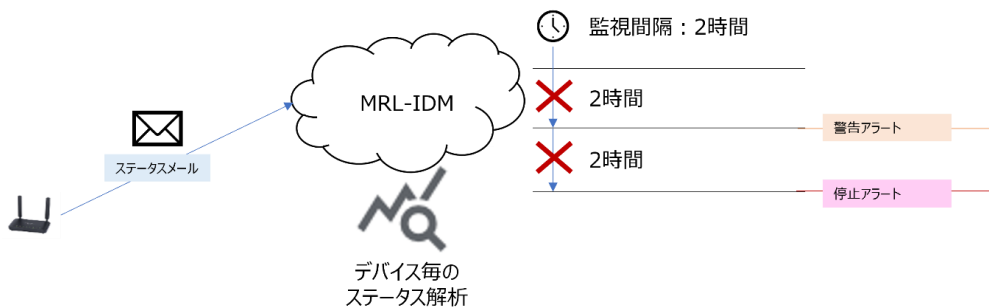
☐ 日曜 ☐ 月曜 ☐ 火曜 ☐ 水曜 ☐ 木曜 ☐ 金曜 ☐ 土曜

メール送信実施時刻: 0 時 0 分

☒ 装置起動時のメール送信を有効にする

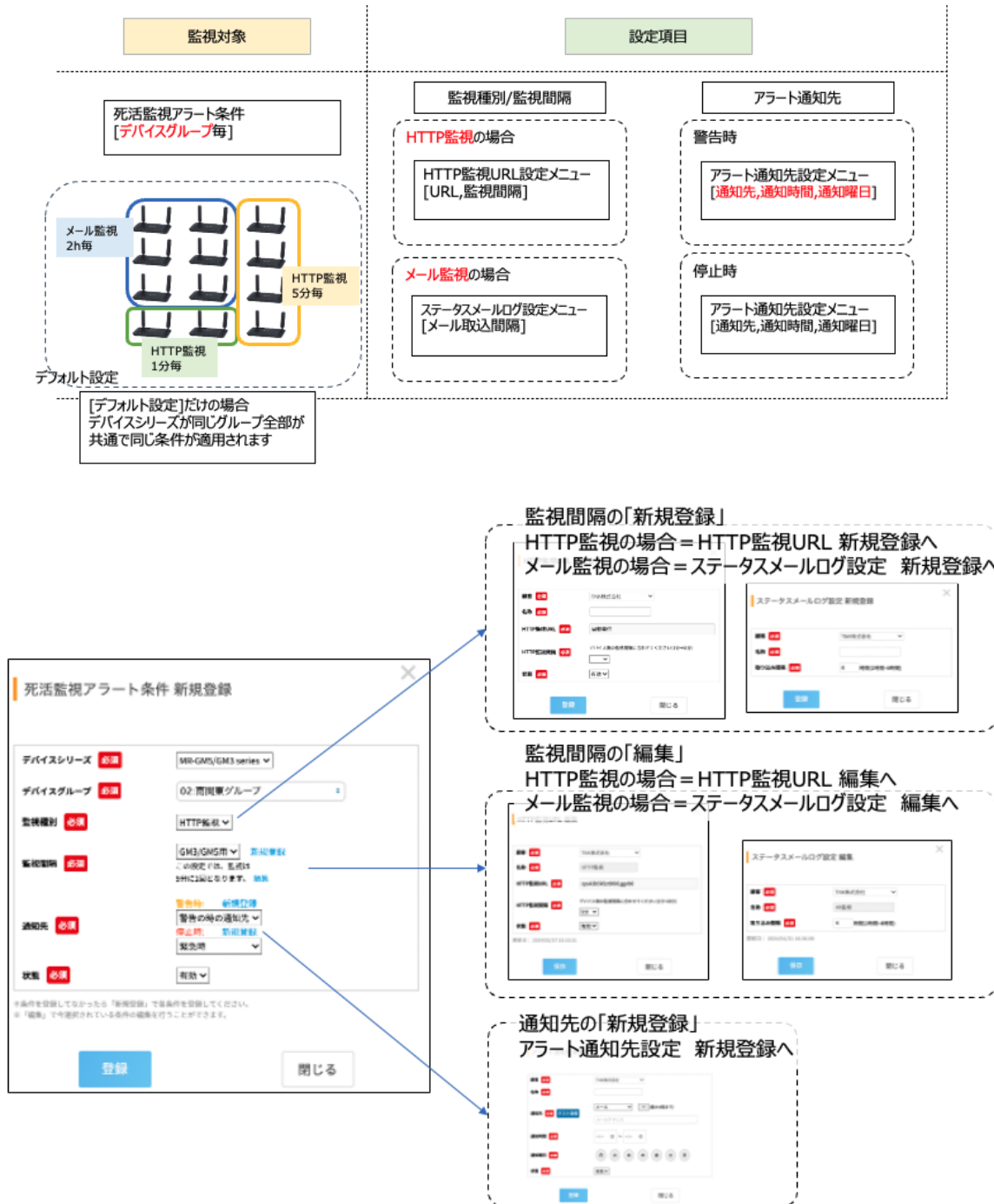
☐ プロセス再起動時のメール送信を有効にする

☐ 有線LANのLinkUP/LinkDOWNによるメール送信を有効にする



メール監視の場合、死活監視とステータス監視を兼ねることができます。  
メール監視の場合、ステータスメールログの取り込み間隔時間になります。(分単位の監視はできません。)

死活監視アラート条件設定画面と、他の設定との遷移関係は下図のようになります。



「死活監視アラート条件設定」画面から、「HTTP 監視 URL 設定」、「ステータスメールログ設定」の新規登録・編集、「アラート通知先設定」の新規登録が可能になっています。

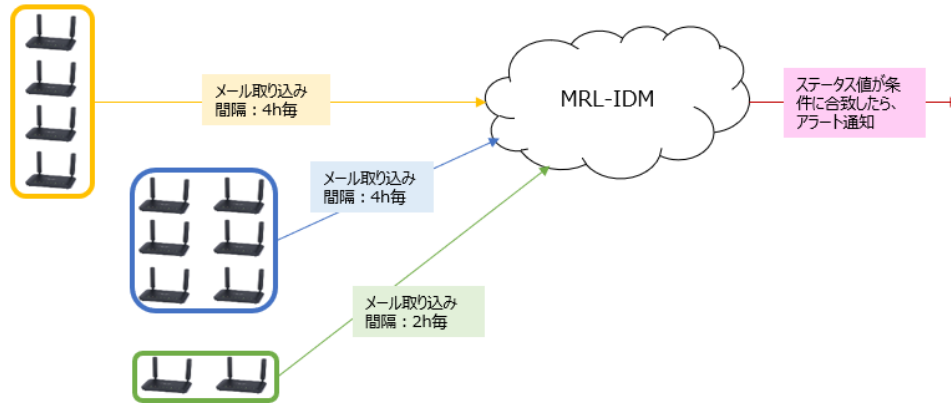
「HTTP 監視 URL 設定」の新規登録や編集方法については「4-7.HTTP 監視 URL 設定」を参照して下さい。

「ステータスメールログ設定」の新規登録や編集方法については「4-8.ステータスメールログ設定」を参照して下さい。

### 3-2-2. ステータスアラート条件設定について

ステータスアラート条件設定は、デバイスグループごとに、デバイスのステータスが条件に合致したらアラートを通知します。

各デバイスグループ毎に、  
デバイスのステータスを見てどういったアラートを送るか？を設定する画面になります。



ステータスアラート条件設定メニューで、

- ・どのデバイスグループを対象とした設定か？
- ・どのデバイスシリーズか？
- ・どのステータスが
- ・どうなったら？
- ・アラート通知先は？

を紐づけて、ステータス監視を行います。

また、アラート通知した際のログは、ログ管理のステータスアラートログに保存されます。

一覧を見ると、すでに、[デフォルト設定]という名前で、太字で表示されている条件があるかもしれません。

死活監視アラート条件と同様に、これは、管理者アカウントが設定した、全てのデバイスグループ共通のデフォルトとして設定されている条件になります。

この[デフォルト設定]がある場合、特に個別にデバイスグループ毎に条件を設定しなくても、ステータスアラートは動きます。

管理者アカウントが設定した「デフォルト設定」のステータスアラート条件

デバイスグループ	詳細名	発生条件	値	監視間隔	通知先	操作
★[デフォルト設定]	メール送信のトリガー	一致	WAN interface Active	4時間	緊急時	
[個別設定] 02グループ / 01グループ	メール送信のトリガー	一致	WAN interface Active	2時間	警告の時の通知先	編集 削除

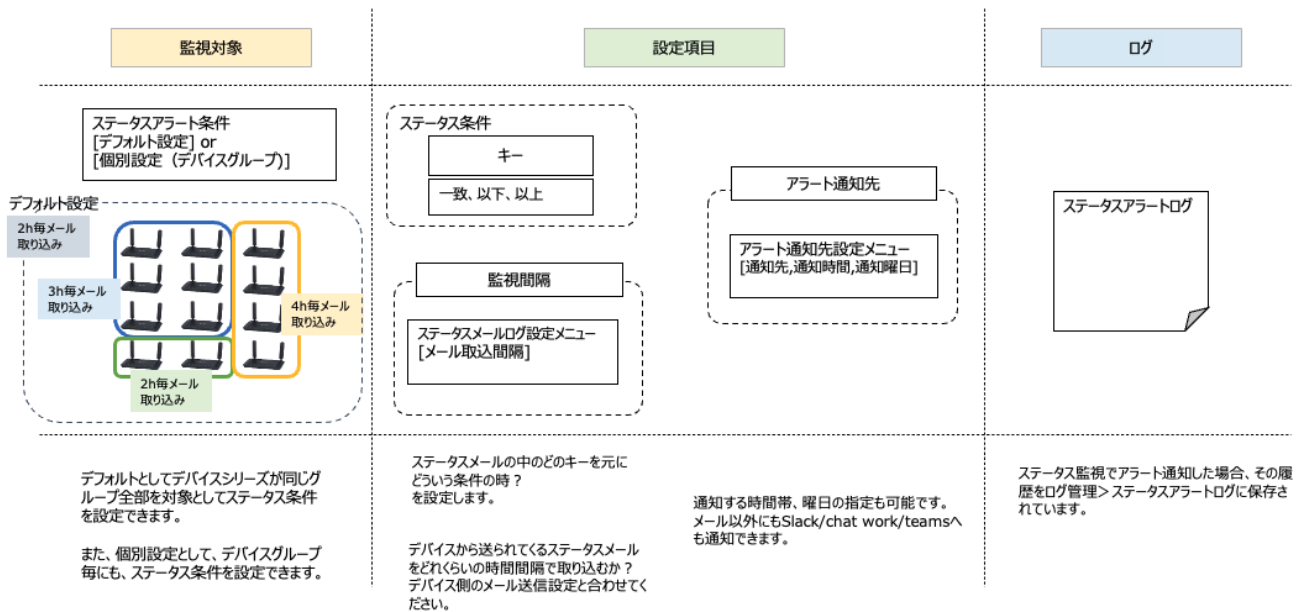
2件中1～2件目 表示

他のユーザーと共同管理しているデバイスグループ

[デフォルト設定]と違う条件、通知先で、自分の管理するデバイスグループについて条件を設定したい場合は、まず管理者に確認をとって、[個別設定]として登録してください。

[デフォルト設定]と[個別設定]がある場合、個別設定が優先されます。

ステータスアラート条件の設定は下図のような構成になります。





### デバイスから送信されるステータスの例:

- ・メールの送信トリガー(回線接続やシステムの再起動)
- ・アンテナ(SQ)
- ・受信信号強度(RSSI)

※ステータスメールで送信される内容についての詳細は、各製品のユーザーズマニュアルをご参照下さい。

これらのステータスがどういう値になった時、アラートを送るのか？を設定するのが、「ステータスアラート条件設定」メニューになります。

具体的な操作の流れを説明します。

- ①「監視・アラート管理」>「ステータスアラート条件設定」メニューをクリックして下さい。

The screenshot shows the MRL-IDM web interface. On the left sidebar, the menu 'ステータスアラート条件設定' (Status Alert Condition Setting) is highlighted with a red box and a circled number 1. The main content area shows the 'ステータスアラート条件設定' page with a search bar and a table of existing conditions. At the bottom right, the '新規登録' (New Registration) button is highlighted with a red box and a circled number 2.

- ②「新規登録」ボタンをクリックして下さい。

ステータスアラート条件 新規登録

デバイスグループ

必須

未選択です

デバイスシリーズ

必須

詳細名

必須

送信条件

必須

値

必須

監視間隔

必須

通知先

必須

新規登録

登録

閉じる

※条件を登録してなかったら「新規登録」で各条件を登録してください。  
※「編集」で今選択されている条件の編集を行うことができます。

<b>デバイスグループ</b>	デバイスグループを選択して下さい。 デバイスグループは重複して条件を設定することはできません。
<b>デバイスシリーズ</b>	使用するデバイスシリーズを選択して下さい。 (MR-GM3 series/MR-GM5 series) デバイスシリーズにより、詳細名の選択肢が変わります。
<b>詳細名</b>	詳細名(条件とするステータス名)を選択して下さい。
<b>送信条件</b>	ステータスアラート送信の条件を表示します。(値と一致・以上・以下)
<b>値</b>	ステータスアラート送信の条件の値を表示します。
<b>監視間隔</b>	監視間隔(ステータスメールログ設定)を選択して下さい。
<b>通知先</b>	アラート通知先を選択して下さい。 アラート通知先の設定については「3-2-3.アラート通知先設定」を参照して下さい。

「登録」ボタンを押して、保存して下さい。

監視間隔については、「ステータスメールログ設定」で設定します。

ステータスメールログ設定 編集

名称 必須 2h監視

取り込み間隔 必須 2 時間(2時間-8時間)

更新日: 2024/01/21 18:36:22

保存 閉じる

ここで設定された、取り込み間隔の時間毎に、デバイスから送られてきたステータスメールを解析します。

ステータスメールログ一覧 2件

名称	取り込み間隔	操作
4h監視	4	編集 削除
2h監視	2	編集 削除

2件中 1 ~ 2 件目 表示

← 前 1 次 →

新規登録

デバイス側で設定した、定期メール送信間隔に合わせるようにして下さい。

Wireless Router for Mobile  
MR-GM3

設定項目

- 状態表示
- 簡易設定
- 動作モード設定
- 無線LAN設定
- ネットワーク設定
- ファイアウォール設定
- VPN設定
- QoS設定
- マネージメント
- システム設定
- 時刻情報・タイマー再起動設定
- DDNS設定
- メール送信設定
- システムログ
- ファームウェア更新
- 設定保存・読み込み
- ユーザー・パスワード設定
- 再起動
- ログアウト

## メール送信設定

メール送信設定を行います。

☒ メール送信機能を有効にする

メール送信サーバー

メール送信サーバーポート番号 587 (1~65535)

送信元メールアドレス @mrlidm.jp

宛先メールアドレス system01@mrlidm.jp

接続保護 なし

☐ StartTLS(RFC 3207) 拡張をしない

認証方法 平文

ユーザー名

パスワード

☐ メール送信グリーティングメッセージ(EHLO)に送信元メールアドレスのドメインを使用する

☒ WANインターフェース有効時のメール送信を有効にする

☒ 定期メール送信を有効にする

送信間隔 2 時 0 分 0 秒 (0~24時間)

☐ 時刻指定メール送信を有効にする

メール送信スケジュール

☐ 毎日

☐ 日曜 ☐ 月曜 ☐ 火曜 ☐ 水曜 ☐ 木曜 ☐ 金曜 ☐ 土曜

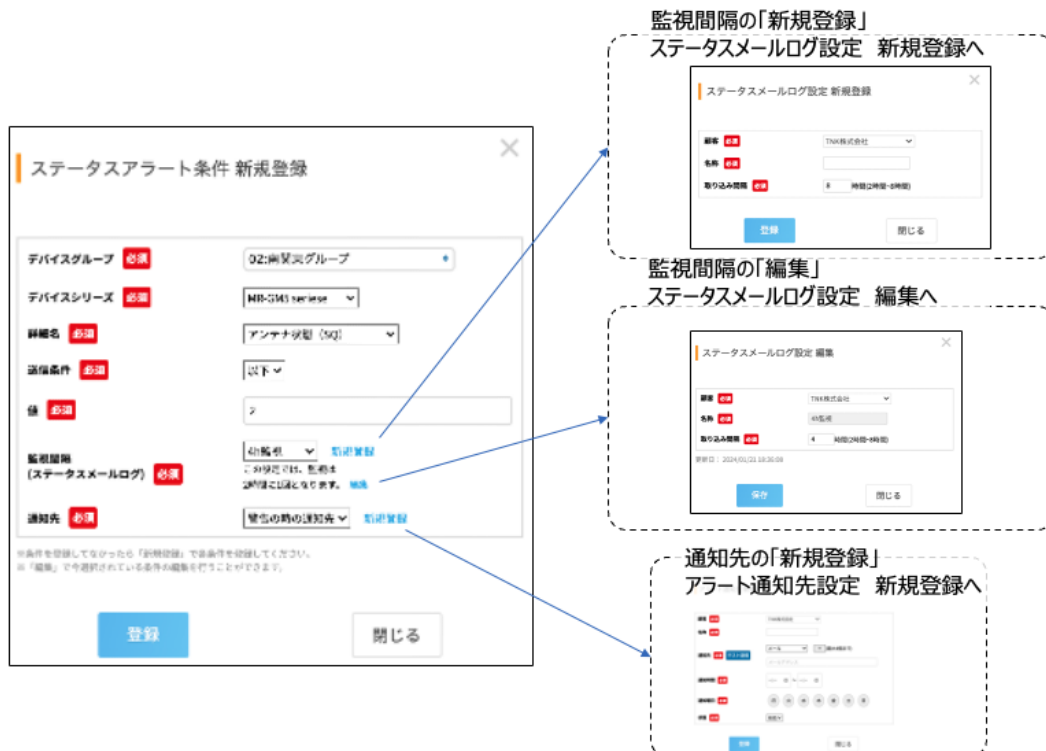
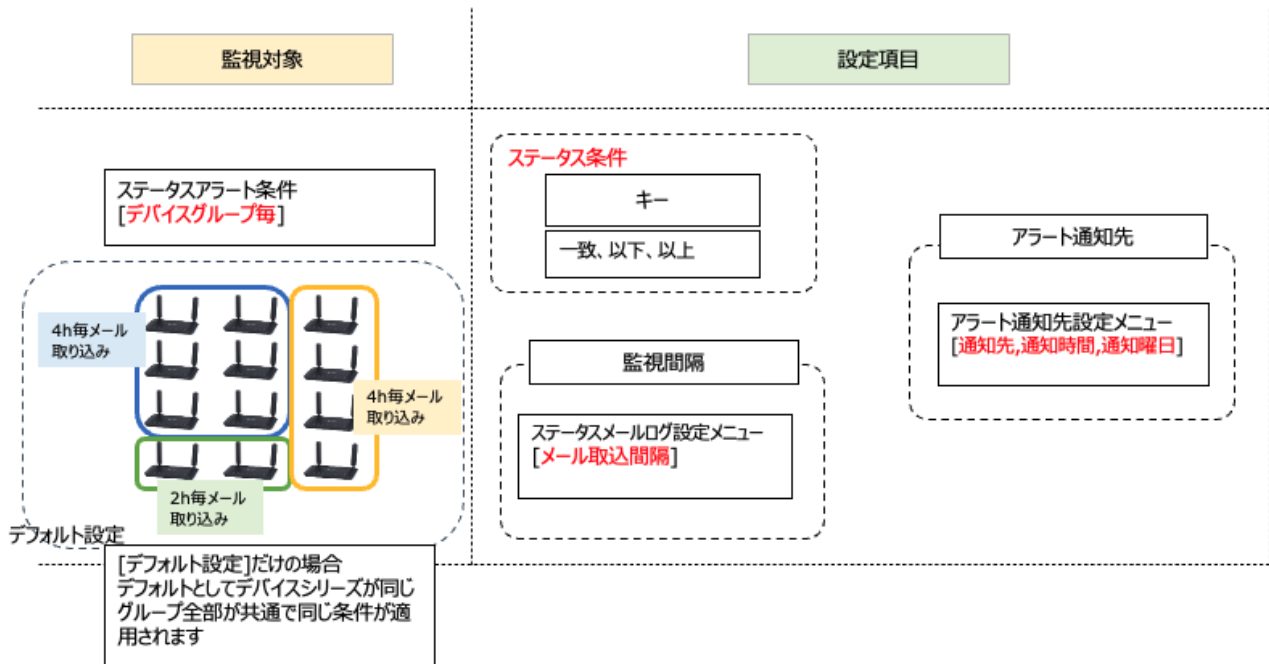
メール送信実施時刻 0 時 0 分

☒ 装置起動時のメール送信を有効にする

☐ プロセス再起動時のメール送信を有効にする

☐ 有線LANのLinkUP/LinkDOWNによるメール送信を有効にする

ステータスアラート条件設定画面と、他の設定との遷移関係は下図のようになります。



「ステータスアラート条件設定」画面から、「ステータスメールログ設定」の新規登録・編集、「アラート通知先設定」の新規登録が可能になっています。

「ステータスメールログ設定」の新規登録や編集方法については「4-8.ステータスメールログ設定」を参照して下さい。

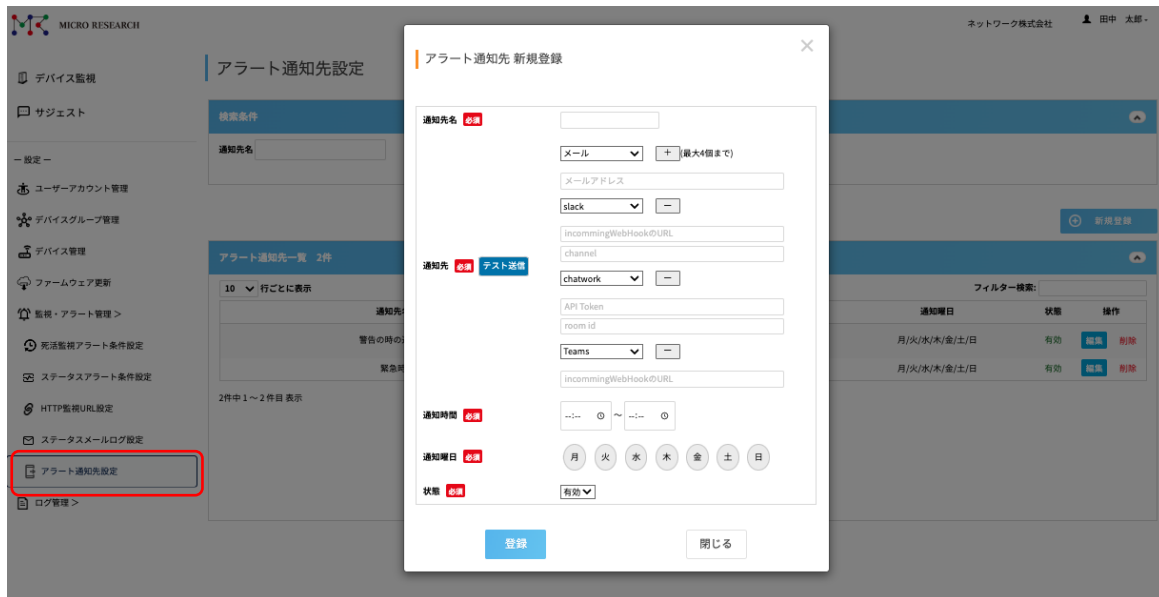
「アラート通知先設定」の設定方法については「3-2-3.アラート通知先設定」を参照して下さい。



### 3-2-3. アラート通知先設定

アラート通知先設定について説明します。

アラート通知先は、「監視・アラート管理」>「アラート通知先設定」メニューで設定できます。



スタンダードプランの場合、メールのみ、通知先は1つまで設定可能です。

ビジネスプランの場合、「メール」「slack」「chatwork」「Microsoft Teams※」から選択可能です。通知先は最大4つまで設定可能です。

※Microsoft Teams は Microsoft 365 Business Basic 以上である必要があります。

また、通知時間、通知曜日を設定できますので、警告時、停止時で通知先のツール、時間帯などを分けてアラート通知先を作成する事が可能です。

通知時間 必須	09:00 ~ 18:00
通知曜日 必須	月 火 水 木 金 土 日

確認

通知時間で 0:00 をまたいだ設定はできません。(0:00~23:59 で一日となります)

動作しない設定例: 9:30~2:30、9:30~0:00、0:00~0:00

動作する設定例: 9:30~23:59・0:00~23:59

各通知先の設定について説明します。

## ■メール

メールアドレスを入力して下さい。


**slack**

slack の場合、「Incoming Webhook」を利用して、slack の指定したチャンネルに通知を行います。

slack 公式の Webhook URL 作成ページを開きます。

https://(御社の slack URL).slack.com/apps/new/A0F7XDUAZ--incoming-webhook-

①のチャンネルを選択し、②「Incoming Webhook インテグレーションの追加」ボタンをクリックします。



## Incoming Webhook

Send data into Slack in real-time.

Please note, this is a legacy custom integration - an outdated way for teams to integrate with Slack. These integrations lack newer features and they will be deprecated and possibly removed in the future. **We do not recommend their use.** Instead, we suggest that you check out their replacement: [Slack apps](#).

Incoming Webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details described later.

[Message Attachments](#) can also be used in Incoming Webhooks to display richly-formatted messages that stand out from regular chat messages.

⚠ Slack のインテグレーションを使うのは初めてですか？

Slack の [はじめ方](#) ガイドをチェックして、最も一般的なタイプのインテグレーション、自分でインテグレーションをビルドする際のヒントを確認しましょう。 [開発者として登録](#) して、開発対象について Slack にお知らせいただいたり、今後の API のアップデートを受け取ったりすることもできます。

### チャンネルへの投稿

まず Incoming Webhook がメッセージ ① を投稿するチャンネルを選択します。

または新しいチャンネルを作成する

② Incoming Webhook インテグレーションの追加

Incoming Webhook を作成することで、[Slack API サービス利用規約](#) に同意したものとみなされます。

Webhook URL が生成されますので、この URL を MRL-IDM の「アラート通知先」を作成するときに入力して下さい。

## セットアップの手順

Slack ヘデータの送信を開始できるように、着信 Webhook の設定に必要なステップを順を追って説明します。


Webhook URL

メッセージの送り方

上記の Webhook URL にデータを送信するには 2 つオプションがあります:

閉じる

設定するチャンネル名は「#警告」など、#を忘れずに登録するようにして下さい。

The screenshot shows a dropdown menu for selecting a Slack channel. The selected channel is "#alert".

## ■Chatwork

Chatwork の場合、「API Token」と「room id」を指定します。

API Token については、chatwork 公式の「APIトークンの発行方法」に従い API トークンを発行して下さい。

<https://help.chatwork.com/hc/ja/articles/115000172402->

[API%E3%83%88%E3%83%BC%E3%82%AF%E3%83%B3%E3%82%92%E7%99%BA%E8%A1%8C%E3%81%99%E3%82%8B](https://help.chatwork.com/hc/ja/articles/115000172402-)

room id については、公式の「ルーム ID を確認する」に従い確認して下さい。

<https://help.chatwork.com/hc/ja/articles/360000142942-%E3%83%AB%E3%83%BC%E3%83%A0ID%E3%82%92%E7%A2%BA%E8%AA%8D%E3%81%99%E3%82%8B>

準備ができましたら、アラート通知先で、chatwork を選択して API Token と room id を入力して下さい。



## ■Microsoft Teams

Microsoft Teams の場合、Teams の「Incoming Webhook」を利用して、指定したチャンネルにアラートを送信します。

Microsoft 公式の Webhook 作成方法については、下記ページをご参照下さい。

<https://learn.microsoft.com/ja-jp/microsoftteams/platform/webhooks-and-connectors/how-to/add-incoming-webhook?tabs=newteams%2Cdotnet>

ご利用の Microsoft Teams のバージョンにより設定方法が異なりますので、ご確認の上、設定して下さい。

準備ができましたら、アラート通知先で、Teams を選択して URL を入力して下さい。





### 3-2-4. ステータスアラート条件の設定例

ステータスアラート条件の設定例を記載します。

下記は、ステータスメールログ設定とデバイスのメール送信機能が有効である事が前提となります。

#### ■WAN 側回線が接続された場合に、アラート通知する例

この場合、デバイス側のメール送信機能で「WAN インターフェース有効時のメール送信を有効にする」にチェックを入れる必要があります。

The screenshot shows the 'ステータスアラート条件 編集' (Status Alert Condition Edit) dialog box. The fields are as follows:

- デバイスグループ (Device Group): 01グループ (01 Group)
- デバイスシリーズ (Device Series): GM3 series
- 詳細名 (Detail Name): メール送信のトリガー (Email Send Trigger)
- 送信条件 (Send Condition): 一致 (Match)
- 値 (Value): WAN interface Active
- 監視間隔 (Monitoring Interval): 2時間監視 (2 hours monitoring). Note: この設定では、監視は2時間に1回となります。(In this setting, monitoring is once every 2 hours.)
- 通知先 (Notification Destination): 警告 (Warning). Note: 新規登録 (New registration).

デバイスシリーズ: 使用しているデバイスシリーズ名を選択して下さい。  
詳細名: 「メール送信のトリガー」を選択して下さい。  
送信条件: 「一致」を選択して下さい。  
値: 「WAN interface Active」を入力して下さい。

#### ■デバイスが起動した場合に、アラート通知する例

この場合、デバイス側のメール送信機能で「装置起動時のメール送信を有効にする」にチェックを入れる必要があります。

The screenshot shows the 'ステータスアラート条件 編集' (Status Alert Condition Edit) dialog box. The fields are as follows:

- デバイスグループ (Device Group): 01グループ (01 Group)
- デバイスシリーズ (Device Series): GM3 series
- 詳細名 (Detail Name): メール送信のトリガー (Email Send Trigger)
- 送信条件 (Send Condition): 一致 (Match)
- 値 (Value): Smtpexec Power on Started 00 seconds ago
- 監視間隔 (Monitoring Interval): 2時間監視 (2 hours monitoring). Note: この設定では、監視は2時間に1回となります。(In this setting, monitoring is once every 2 hours.)
- 通知先 (Notification Destination): 警告 (Warning). Note: 新規登録 (New registration).

デバイスシリーズ: 使用しているデバイスシリーズ名を選択して下さい。  
詳細名: 「メール送信のトリガー」を選択して下さい。  
送信条件: 「一致」を選択して下さい。  
値: 「Smtpexec Power on Started 00 seconds ago」を入力して下さい。  
※数値部分(秒数)は無視されます。

#### ■アンテナ(SQ)の値が2以下だった場合に、アラート通知する例

The screenshot shows the 'ステータスアラート条件 編集' (Status Alert Condition Edit) dialog box. The fields are as follows:

- デバイスグループ (Device Group): 01グループ (01 Group)
- デバイスシリーズ (Device Series): GM3 series
- 詳細名 (Detail Name): アンテナ状態 (SQ) (Antenna Status (SQ))
- 送信条件 (Send Condition): 以下 (Below)
- 値 (Value): 2
- 監視間隔 (Monitoring Interval): 2時間監視 (2 hours monitoring). Note: この設定では、監視は2時間に1回となります。(In this setting, monitoring is once every 2 hours.)
- 通知先 (Notification Destination): 警告 (Warning). Note: 新規登録 (New registration).

デバイスシリーズ: 使用しているデバイスシリーズ名を選択して下さい。  
詳細名: 「アンテナ状態 (SQ)」を選択して下さい。  
送信条件: 「以下」を選択して下さい。  
値: 「2」を入力して下さい。

### 3-3. デバイスの状態を確認する

運用を開始したデバイスの状態を定期的に確認する場合やアラートを受信した場合にデバイスの状態を確認する方法を説明します。

デバイス監視メニューを基点に、状態確認やログ、設定から状況把握などを行なっていきます。

#### 3-3-1. デバイス監視

MRL-IDM にログインすると最初に「デバイス監視」メニューが開きます。

デバイス監視

Check Me!

・監視・アラート管理で、HTTP監視URLが監視に紐づいていないようです。「[HTTP監視URL設定](#)」をご確認ください。

デバイス一覧 3件
 

(ここに表示されていないデバイスは、まだ死活監視の設定がされていません。[死活監視設定](#)をしてください。)

10 行ごとに表示
 フィルター検索:

状態	受信種別	日時	設置場所	機種	機器名称	IPアドレス	MACアドレス	詳細
稼働		2024/05/16 11:22:06	海岸ビル1F	MR-GM3-M	MR-GM3LTE1F		00:10:38:	ログ データ WEB
警告		2024/03/08 14:12:21	海岸ビル2F	MR-GM3-M	MR-GM3LTE2F		00:10:38:	ログ データ WEB
稼働		2024/05/16 11:12:06	海岸ビル3F	MR-GM3-D KS	MR-GM3LTE3F		00:10:38:	ログ データ WEB

3件中 1 ~ 3 件目 表示

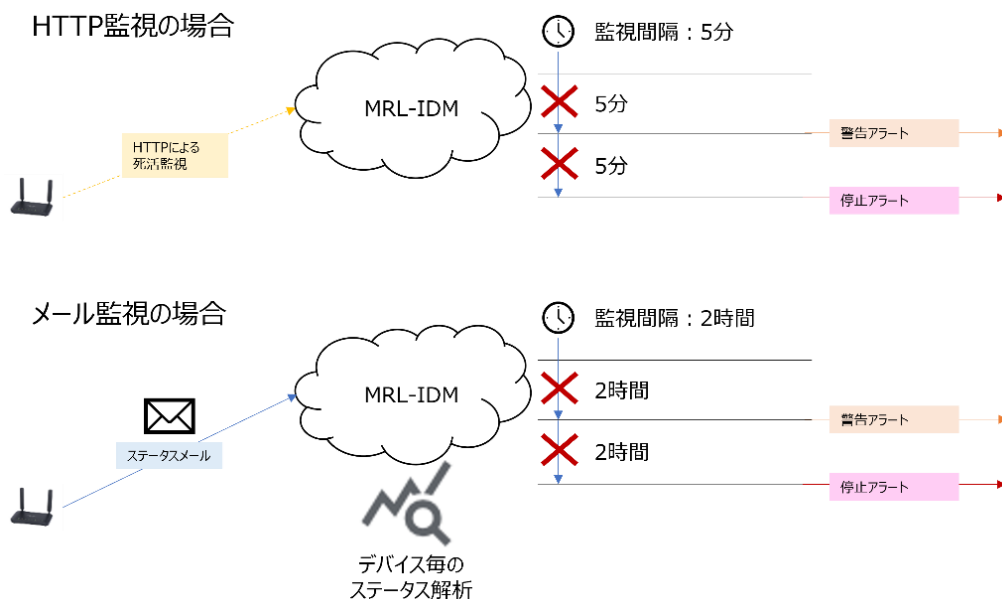
← 前 1 次 →

「状態」の列に、デバイスの現時点の状態が表示されています。状態は以下の 3 段階あります。

稼働	デバイスからの死活監視通信を監視間隔で設定した通りに受信している状態です。
警告	デバイスからの死活監視通信を 1 回受信できていない状態です。
停止	デバイスからの死活監視通信を 2 回連続で受信できていない状態です。

※デバイスの状態を見るには、まず、「[死活監視アラート条件設定](#)」を行うようにして下さい。

警告・停止の表示はそれぞれの死活監視アラート条件で設定された内容に基づき、どれくらいの時間デバイスからの通信が止まっていたかによって変わりますのでご注意ください。



3-3-2. デバイスのログを確認する

各デバイスのログを見るには、以下の通りになります。

- ① デバイス監視のデバイス一覧から「ログ」ボタンをクリックして、「ステータスメールログ」を確認する。
- ② 「ログ管理」メニューから、それぞれのログを確認する。
  - ・死活監視アラートログ
  - ・ステータスアラートログ
  - ・HTTP 監視ログ
  - ・ステータスメールログ
  - ・デバイスオペレーションログ

デバイス監視メニューのデバイス一覧で検索した結果の一覧から、ログを確認したいデバイスを見つけて下さい。

デバイス一覧 3件									
(ここに表示されていないデバイスは、まだ死活監視の設定がされていません。死活監視設定をしてください。)									
10	行ごとに表示		フィルター検索:						
状態	受信種別	日時	設置場所	機種	機器名称	IPアドレス	MACアドレス	詳細	
稼働	📧	2024/05/16 11:22:06	海岸ビル1F	MR-GM3-M	MR-GM3LTE1F		00:10:38:...	ログ	グラフ WEB
稼働	📧	2024/05/16 11:12:06	海岸ビル2F	MR-GM3-M	MR-GM3LTE2F		00:10:38:...	ログ	グラフ WEB
稼働	📧	2024/05/16 11:12:06	海岸ビル3F	MR-GM3-D KS	MR-GM3LTE3F		00:10:38:...	ログ	グラフ WEB
3件中 1 ~ 3 件目 表示									

フィルター検索	
フィルター検索:	設置場所、機種、機器名称、IP アドレス、MAC アドレスなど一覧に表示されている項目で、部分一致で絞り込みをかけられます。

画面の説明							
状態	デバイスの稼働状態を表示します。 <table><tr><td>稼働</td><td>デバイスからの死活監視通信を監視間隔で設定した通りに受信している状態です。</td></tr><tr><td>警告</td><td>デバイスからの死活監視通信を 1 回受信できていない状態です。</td></tr><tr><td>停止</td><td>デバイスからの死活監視通信を 2 回連続で受信できていない状態です。</td></tr></table>	稼働	デバイスからの死活監視通信を監視間隔で設定した通りに受信している状態です。	警告	デバイスからの死活監視通信を 1 回受信できていない状態です。	停止	デバイスからの死活監視通信を 2 回連続で受信できていない状態です。
稼働	デバイスからの死活監視通信を監視間隔で設定した通りに受信している状態です。						
警告	デバイスからの死活監視通信を 1 回受信できていない状態です。						
停止	デバイスからの死活監視通信を 2 回連続で受信できていない状態です。						
受信種別	死活監視の受信種別を表示します。 <table><tr><td>📧</td><td>HTTP 通信での死活監視時に表示されます。</td></tr><tr><td>✉️</td><td>メールでの死活監視時に表示されます。</td></tr></table>	📧	HTTP 通信での死活監視時に表示されます。	✉️	メールでの死活監視時に表示されます。		
📧	HTTP 通信での死活監視時に表示されます。						
✉️	メールでの死活監視時に表示されます。						
日時	HTTP 通信での死活監視時は、HTTP 通信を受信した最新の日時が表示されます。 メールでの死活監視時は、ステータスメールログの最新の登録日時が表示されます。						
設置場所	デバイス登録時に設定した設置場所が表示されます。						
機種	デバイスの機種名が表示されます。 MRL-IDM がデバイスからステータスメールを受信していない場合、空欄になります。						
機器名称	デバイス登録時に設定した機器名称が表示されます。						
IP アドレス	HTTP 通信での死活監視時は、HTTP 通信の送信元 IP アドレスが表示されます。 メールでの死活監視時は、ステータスメールログの WAN 側 IP アドレスが表示されます。						
MAC アドレス	デバイス登録時に設定した MAC アドレスが表示されます。						
ログ	ステータスメールログ画面に遷移します。						
グラフ	デバイスステータスグラフ画面に遷移します。						
WEB	デバイスの「WAN 側の設定を許可する設定」を行っている場合、WEB 通信でデバイスの設定画面を操作できます。操作・設定内容については、MR-GMx シリーズのユーザーマニュアルをご参照下さい。						

「ログ」ボタンをクリックすると「ステータスメールログ」に画面に移ります。  
(この時、選択したデバイスのログだけに絞り込まれます。)

ステータスメールログ

検索条件

設置場所

デバイスグループ

機種

機器名称

S/N

IPアドレス

MACアドレス

期間

～

検索

ステータスメールログ一覧 461件

10

行ごとに表示

フィルター検索:

エクスポート

登録日時	設置場所	デバイスグループ	機種	機器名称	S/N	IPアドレス	MACアドレス	ログ種別	メール受信日時	ログ内容
2024/05/13 13:44:03	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 13:39:54	詳細
2024/05/13 11:44:03	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 11:41:15	詳細
2024/05/13 11:44:03	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 11:36:02	詳細
2024/05/13 11:44:03	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 11:36:00	詳細
2024/05/13 11:44:03	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 10:24:19	詳細
2024/05/13 09:44:02	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 09:05:58	詳細
2024/05/13 09:44:02	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 09:05:56	詳細
2024/05/13 07:44:02	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 07:30:13	詳細
2024/05/13 05:44:02	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 05:28:59	詳細
2024/05/13 03:44:02	海岸ビル1F	01グループ	MR-GM3-DKS	MR-GM3LTE1F	GM30		00:10:38:	メール	2024/05/13 03:27:44	詳細

461件中 1 ～ 10 件目 表示

← 前

1

2

3

4

5

次 →

画面の説明：検索条件	
設置場所	設置場所を指定します。
デバイスグループ	デバイスグループを選択します。
機種	機種を選択します。
機器名称	機器名称を指定します。
S/N	シリアル No を指定します。
IPアドレス	IP アドレスを指定します。
MACアドレス	MAC アドレスを指定します。
期間	ログ期間を指定します。

該当デバイスの、「詳細」ボタンをクリックすると、その時のデバイスの状態が詳細に見られます。

詳細

メールデータ

メール受信日時:2024/05/09 17:46:23

メール送信のトリガー	Periodical
起動経過時間	1days:2:6:8s
ファームウェアバージョン	v1.04.02(MR001)
ファームウェアビルド日時	Tue Oct 24 17:39:22 JST 2023
コンフィグバージョン	Default:22 Current:22
システム負荷	0.00 0.00 0.00 1/37
RAM使用量	17312 KB / 114064 KB
ROM使用量	mtd1: 3512 KB / 10240 KB
機種名	MR-GM3-DKS
装置名称	MR-GM3
NTPクライアントの同期状態	Synchronized

WAN情報(GM3)

WAN接続モード	Mobile Card(Built-in MODULE)
SIMカードの電話番号	
内蔵通信モジュールの端末識別番号	
LTE通信網の圏内・圏外 (1=圏内、0=圏外)	1
アンテナ状態 (0~4)	4
受信信号強度	-51dBm
LTEの周波数帯 (LTE frequency band)	100
内蔵通信モジュールのバージョン	11-18
モジュールキャリア選択値	0,2
WAN側IPアドレス	

WLAN情報(GM3)

無線LAN1のSSID	MR-GM3 5G
無線LAN1の動作モード	AP
無線LAN1の周波数	5 GHz (A+N+AC)
無線LAN1のチャンネル番号	36
無線LAN1の暗号モード	WPA2 Mixed
無線LAN1のBSSID	00:10:38:
無線LAN1のクライアント数	0
無線LAN2のSSID	MR-GM3 2.4G
無線LAN2の動作モード	AP
無線LAN2の周波数	2.4 GHz (B+G+N)
無線LAN2のチャンネル番号	6
無線LAN2の暗号モード	WPA2 Mixed
無線LAN2のBSSID	00:10:38:
無線LAN2のクライアント数	0

LAN情報(GM3)

LANポートIPアドレス	192.168.0.1
LANポートサブネットマスク	255.255.255.0
LANポートMACアドレス	00:10:38:
DHCPサーバーの状態 (Active=有効、Inactive=無効)	Active
eth0ポートのリンク状態	Link Up
DDNSのドメイン名	

登録日時: 2024/05/09 18:49:02

閉じる

また、「ログ管理」メニューでは、様々なログを確認することができます。

ログ管理 >

ログ保存期間設定

死活監視アラートログ

死活監視でアラートが送信された時のログ

ステータスアラートログ

ステータス監視でアラートが送信された時のログ

HTTP監視ログ

HTTP監視をご利用の場合、HTTP監視用URLが呼ばれたログ

ステータスメールログ

デバイスから送られてきたステータスメールの解析結果ログ

デバイスオペレーションログ

デバイスに対してMRL-IDMから操作を行った時のログ

HTTP監視ログ

検索条件

設置場所

デバイスグループ

機種

機器名称

S/N

IPアドレス

MACアドレス

期間

検索

HTTP監視ログ一覧 107件

10 行ごとに表示

フィルター検索:

エクスポート

登録日時	設置場所	デバイスグループ	機種	機器名称	S/N	IPアドレス	MACアドレス	ログ種別
2024/03/20 18:10:39	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 18:05:34	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 18:00:29	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:55:24	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:50:19	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:45:14	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:40:09	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:35:04	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視

107件中 1 ~ 10 件目 表示

← 前

1

2

3

4

5

次 →

それぞれのログ画面の詳細な操作説明については、「4.画面操作説明」をご確認下さい。

### 3-3-3. 傾向をグラフで確認する

デバイスの状態の傾向をグラフで確認できます。

デバイス一覧 3件								
(ここに表示されていないデバイスは、まだ死活監視の設定がされていません。死活監視設定をしてください。)								
10	行ごとに表示		フィルター検索:					
状態	受信種別	日時	設置場所	機種	機器名称	IPアドレス	MACアドレス	詳細
🟢稼働	🟢	2024/05/16 11:22:06	海岸ビル1F	MR-GM3-M	MR-GM3LTE1F		00:10:38:...	ログ <b>グラフ</b> WEB
🟢稼働	🟢	2024/05/16 11:12:06	海岸ビル2F	MR-GM3-M	MR-GM3LTE2F		00:10:38:...	ログ <b>グラフ</b> WEB
🟢稼働	🟢	2024/05/16 11:12:06	海岸ビル3F	MR-GM3-D KS	MR-GM3LTE3F		00:10:38:...	ログ <b>グラフ</b> WEB

3件中 1 ~ 3 件目 表示

デバイスの「グラフ」ボタンをクリックして下さい。グラフ表示画面が開きます。



各デバイスシリーズで確認できるグラフは以下の通りです。(2024 年 11 月現在)

#### ●MR-GM3/MR-GM3L シリーズ

- ・アンテナ状態 (SQ)
- ・受信信号強度 (RSSI)
- ・RAM 使用量
- ・Loadavg
- ・受信 BPS
- ・受信 PPS
- ・送信 BPS
- ・送信 PPS

#### ●MR-GM5A/MR-GM5L

- ・アンテナ状態 (SQ)
- ・受信信号強度 (RSSI)
- ・受信電力 (RSRP)
- ・受信品質 (RSRQ)
- ・メモリ使用量
- ・CPU 使用率
- ・受信 BPS
- ・受信 PPS
- ・送信 BPS
- ・送信 PPS

グラフの値は、1 日に受信したステータスメールログの値の平均値です。

ビジネスプランのユーザーの場合、「ログ管理」>「ログ保存期間設定」で設定したログ保存期間分のログからグラフデータを作成しています。

表示期間は、30 日、60 日、90 日、120 日、150 日、180 日で、当日から何日前までのデータを表示するか選択できます。

※スタンダードプランのユーザーの場合、表示は 7 日固定になります。

### 3-3-4. WEB 通信

「WAN 側からの設定(リモート設定)を許可する」設定を行っているデバイスの場合は、「WEB」ボタンをクリックすると、遠隔でデバイス本体の設定画面にログインし、操作することができます。

WAN 側がグローバル IP アドレスある事が前提となりますのでご注意ください。

デバイス一覧 3件								
(ここに表示されていないデバイスは、まだ死活監視の設定がされていません。死活監視設定をしてください。)								
10	行ごとに表示		フィルター検索:					
状態	受信種別	日時	設置場所	機種	機器名称	IPアドレス	MACアドレス	詳細
稼働	Q	2024/05/16 11:22:06	海岸ビル1F	MR-GM3-M	MR-GM3LTE1F	192.168.1.1	00:10:38:00:00:00	ログ データ WEB
稼働	Q	2024/05/16 11:12:06	海岸ビル2F	MR-GM3-M	MR-GM3LTE2F	192.168.1.2	00:10:38:00:00:00	ログ データ WEB
稼働	Q	2024/05/16 11:12:06	海岸ビル3F	MR-GM3-D KS	MR-GM3LTE3F	192.168.1.3	00:10:38:00:00:00	ログ データ WEB

3件中 1 ~ 3 件目 表示

デバイス本体の設定画面が開きます。

「デバイス管理」で、WEB ログイン ID、WEB パスワードを空欄にした場合は、デバイス本体へのログイン ID、パスワードの入力が求められます。

デバイス 編集

設置場所

海岸ビル1F

機器名称 必須

MR-GM3LTE1F

MACアドレス 必須

00:10:38:00:00:00

デバイスグループ 必須

03グループ

アラート通知 必須

有効

機種

MR-GM3-M

S/N

GM300000000000

導入日

2024/02/02

IPアドレス

WEBポート

80

WEBログインID

WEBパスワード

Memo

デジタルサイネージ用

登録日: 2024/02/02 17:22:53

更新日: 2024/04/26 20:31:45

保存

閉じる

確認

MR-GM5A/MR-GM5L の場合、WEB ログイン ID、WEB パスワードの保存はできません。



MR-GM5A/MR-GM5L の場合は、ポップアップウィンドウで別ウィンドウとして設定画面が開きますので、ブラウザ側で「mrlidm.jp ドメインの場合はポップアップを許可する」ように設定して下さい。



こちらは、デバイス本体へのログイン ID、パスワードですので、ご注意ください。  
(MRL-IDM へのログイン ID/パスワードではありません。)





操作方法については、MR-GMxシリーズのユーザーマニュアルをご参照下さい。

**確認** 閉域網やプライベートネットワークに接続しているデバイスの場合、MRL-IDM から設定画面にアクセスすることはできません。

### 3-4.新しいファームウェアの適用

新しいファームウェアが公開された場合、マイクロリサーチのホームページや MRL-IDM 上で情報が公開されます。  
MRL-IDM の「ファームウェア更新」メニューで登録した URL を、事前にデバイス側のファームウェアダウンロード URL に設定しておくことで、MRL-IDM 側の操作でデバイスのファームウェアを更新する事が可能です。

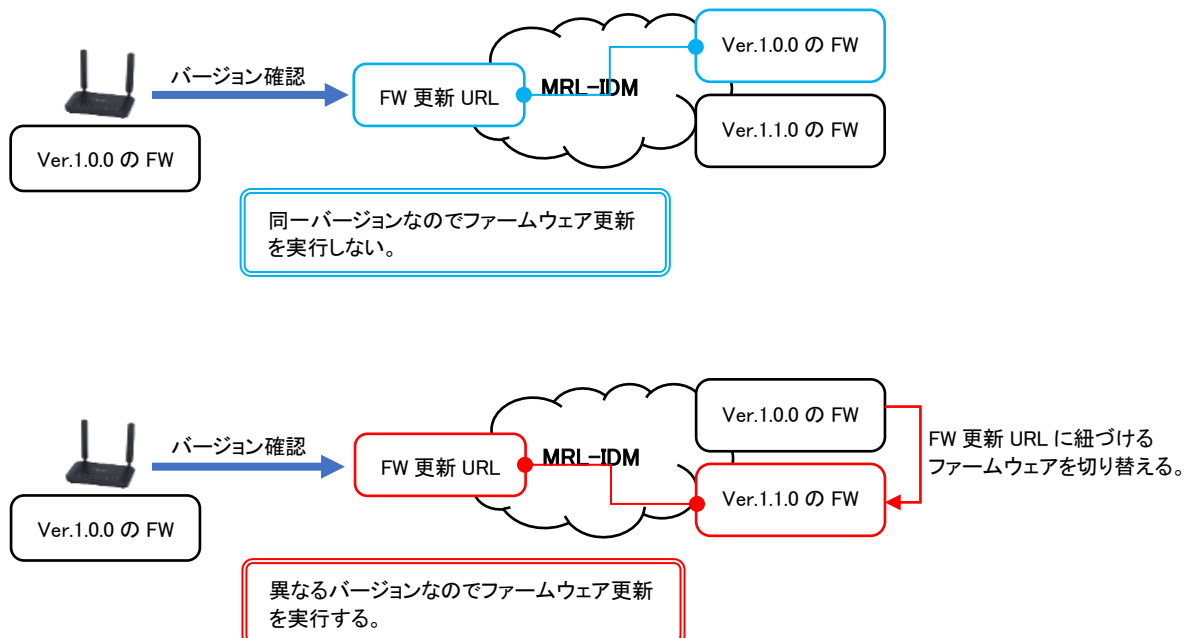
	<p>MRL-IDM のファームウェア管理でバージョンを指定するだけでは更新されません。 必ず事前にデバイス側の設定メニュー「ファームウェア更新」で MRL-IDM 上で設定した FW 更新 URL を登録して下さい。 デバイス側の設定については以下を参照して下さい。 「3-6-4.タイマー自動ファームウェア更新機能の設定」(MR-GM3/MR-GM3L) 「3-7-4.タイマー自動ファームウェア更新機能の設定」(MR-GM5A/MR-GM5L)</p>
---	---


	<p><b>ファームウェアの対象機種を間違えると、ファームウェア更新が失敗し、修理が必要となる場合がありますので、注意して下さい。</b></p>
---	---

まず、MR-GMx シリーズのタイマー自動ファームウェア更新機能の流れについて説明します。

- 1) MR-GMx シリーズは、タイマー自動ファームウェア更新機能に設定されたスケジュールに従い、設定された URL へファームウェアのバージョン確認を行います。
- 2) 設定された FW 更新 URL に紐づけされたファームウェアバージョンがデバイス自身のバージョンと異なる場合、ファームウェアをダウンロードしてファームウェア更新を実行します。  
設定された URL に紐づけされたファームウェアバージョンが同一の場合は、ファームウェア更新を実行しません。

MRL-IDM では、MRL-IDM で設定したファームウェア更新 URL に紐づけるファームウェアのバージョンを切り替えることにより、デバイスのファームウェアを更新するか、更新しないかを遠隔操作する仕組みを提供します。



	<p><b>MRL-IDM 上で FW のバージョンを変更すると、その FW 更新 URL を設定している全てのデバイスが更新されます。適用するファームウェアの検証を十分行ってから、MRL-IDM 側で切り替える事を推奨します。</b></p>
---	--

### 3-4-1. MRL-IDM 上でファームウェアのバージョンを指定する

運用上、新しいファームウェアの適用が決定しましたら、MRL-IDM 上で FW 更新 URL の編集でバージョンを指定して下さい。  
この FW 更新 URL が設定されているデバイスグループの全てのデバイスで更新が行われます。

確認

F/W 更新 URL の新規登録の方法については、「4-4.ファームウェア更新」を参照して下さい。

該当機種のファームウェア URL に紐づくファームウェアのバージョンを変更します。  
MRL-IDM にログインして、「ファームウェア更新」メニューをクリックして下さい。



ファームウェアを適用するデバイスグループ(F/W 機種)の「編集」ボタンをクリックして下さい。  
編集画面が開きますので、F/W バージョン名で、適用するファームウェアを選択して[保存]ボタンをクリックして下さい。

×

ファームウェア更新URL 編集

デバイスシリーズ(FW対応機種) 必須

MR-GM5L :[MR-GM5L]

デバイスグループ 必須

02:南関東グループ

FWバージョン名 必須

v2. (MR001)

送信プロトコル 必須

HTTPS

URL

https://

状態 必須

有効

更新日:

保存

閉じる

新たに適用したい、新しいバージョンを指定します

確認

ファームウェアのバージョンダウンは動作保証外となります。

#### 3-4-2. ファームウェアの更新

デバイス側で設定されたスケジュール(曜日・時刻)になると、ファームウェアバージョンの確認が実行されます。  
デバイスのファームウェアバージョンと MRL-IDM の F/W 更新 URL に紐づけられたファームウェアバージョンが異なる場合  
ファームウェアの更新が実行され、新しいファームウェアが適用されます。



ファームウェア更新時は、回線の切断とデバイスの再起動が行われます。  
デバイス側のスケジュールの設定については、運用上影響が無い曜日、時刻を設定して下さい。

以上が、ファームウェア自動更新の流れになります。

### 3-5. サジェストについて(ビジネスプランのみ)

MRL-IDM のシステムが検知した、お客様が設定された内容についてサジェストします。  
サジェストはビジネスプランのユーザーのみが使える機能です。

#### デバイス監視

##### Check Me!

- ・ステータス監視中に、MRL-IDMがデバイス本体のHTTP監視用URLの設定について何かおかしい点を見ました。「[サジェスト](#)」をご確認ください。
- ・監視・アラート管理で、HTTP監視用URLが監視に紐づいていないようです。「[HTTP監視用URL設定](#)」をご確認ください。
- ・監視・アラート管理で、ステータスメール設定が監視に紐づいていないようです。「[ステータスメールログ設定](#)」をご確認ください。
- ・アラート通知先設定が、どの監視にも紐づいていないようです。「[アラート通知先設定](#)」をご確認ください。

「デバイス監視」画面の上部に「Check Me!」と表示されている部分がサジェスト項目になります。

例えばHTTP 監視 URL を作成したが死活監視アラート条件に紐づけられていない設定があると、以下のようにサジェストします。

田中 太郎さん、[GM5L用] が作られてから1日以上経っていますが、まだ死活監視アラート条件に紐づいていません。これらのURLは利用されていますか？

死活監視に設定した URL が、どの死活監視アラートにも紐づけられていない可能性がありますので、念の為に確認下さい。

このように、MRL-IDM ではお客様が見逃している可能性がある設定について、「サジェスト」する機能を搭載しています。  
MRL-IDM はお客様が「各種ネットワークデバイスを安全に効率よく運用するため」の手助けをするためのシステムです。  
今後もサジェストする内容は増えていきますので、ご活用下さい。

### 3-6.デバイスの設定(MR-GM3/MR-GM3L)

MRL-IDM を利用するために必要な、デバイス(MR-GM3/MR-GM3L)の各種設定について説明します。

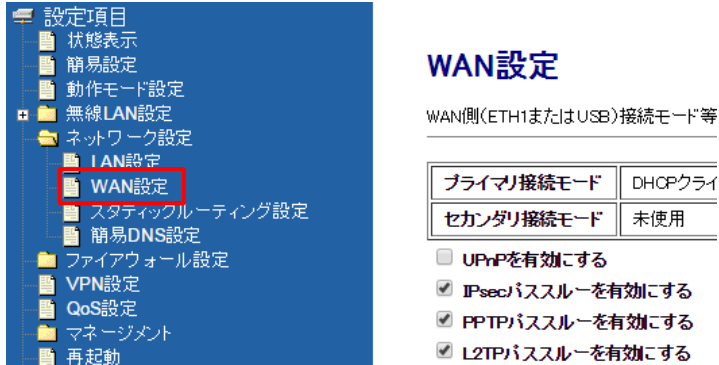
#### 3-6-1.HTTP 回線監視の設定

MRL-IDM で死活監視を行うための、HTTP 回線監視の設定について説明します。



デバイスの死活監視を行わない場合は、本設定は不要です。

①「ネットワーク設定」から「WAN 設定」を開いて下さい。



②「回線監視機能」の設定を行って下さい。

回線監視機能	HTTPによる監視▼
発行間隔	15分▼
連続失敗検出回数	2 (1~60)
<input type="checkbox"/> 回線監視通信の送信元にLAN側IPアドレスを使用する	
宛先1	https://mrlidm.jp/monitoring/
宛先2	www.
宛先3	www.
設定保存	

#### ■回線監視機能

プルダウンメニューで「HTTPによる監視」を選択して下さい。

#### ■発行間隔

発行間隔を選択して下さい。(1/5/10/15/30/45/60 分) MRL-IDM で設定した監視間隔より短く設定してください。  
(例:MRL-IDM の死活監視間隔 30 分の場合、MR-GM3 側は 15 分にします。)

#### ■連続失敗検出回数

任意の回数を設定して下さい。

ここで設定した回数、連続して監視に失敗すると、回線切断状態と判断して、回線の再接続や再起動等のリカバリ処理を行います。

#### ■宛先1~3

宛先1に MRL-IDM の「監視・アラート管理」内「HTTP 監視 URL 設定」登録時発行の URL を入力してください。



宛先は MRL-IDM の HTTP 監視 URL 以外も設定して下さい。  
MRL-IDM の監視 URL のみ設定した場合、MRL-IDM のメンテナンス等で HTTP 通信が不通になるとデバイスが回線障害と判断して回線の再接続やシステムの再起動等のリカバリ動作を行います。

設定が終わりましたら、[設定保存]ボタンをクリックしてください。

再起動を行うと設定が反映されます。

### 3-6-2.NTP クライアント機能の設定

ステータスメールを送信するためとタイマーファームウェア自動更新を行うための、NTP クライアント機能の設定について説明します。

<div>確認</div>	デバイスのステータス監視、タイマーファームウェア自動更新を行わない場合、本設定は不要です。
	メール送信機能を使用する場合、「NTP クライアント機能」を有効にする事を推奨します。 日時情報が合っていない状態でメールを送信すると、送信日時が不正なメールとしてメールサーバーに拒否されることがありますのでご注意ください。
	「タイマー自動ファームウェア更新機能」は、「NTP クライアント機能」による時刻取得が正常に行われた場合にのみ動作します。

①「マネージメント」から「時刻情報・タイマー再起動設定」を開いて下さい。

②「NTP クライアント機能を有効にする」にチェックを入れて下さい。

**時刻情報・タイマー再起動設定**

本機の時刻情報の設定を行います。

NTPクライアント機能を有効に設定する場合、任意の曜日・時間に本機を自動的に再起動させることが可能です。

現在の時刻 2024 年 5 月 28 日 15 時 54 分 25 秒

タイムゾーン (GMT+09:00)Osaka, Sapporo, Tokyo

☒ NTPクライアント機能を有効にする

NTPサーバー ☐ ntp1.jst.mfeed.ad.jp ☐ 0.0.0.0  
(NTPサーバーのアドレスを設定)

再起動機能


③NTPサーバーをプルダウンメニューから選択するか、任意のNTPサーバーのアドレスを入力して下さい。

設定が完了したら、[設定保存]ボタンをクリックしてください。

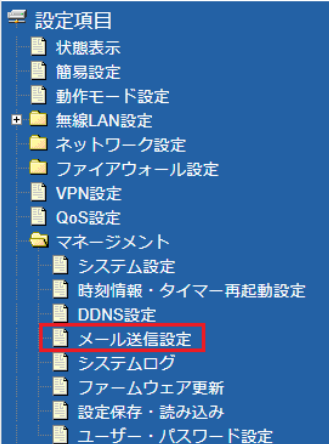
再起動を行うと設定が反映されます。

### 3-6-3.メール送信機能の設定

MRL-IDM でステータスメールを受信するための、メール送信機能の設定について説明します。

	<p>デバイスのステータス監視を行わない場合、本設定は不要です。</p> <p>メール送信機能を使用する場合、「NTP クライアント機能」を有効にする事を推奨します。</p> <p>日時情報が合っていない状態でメールを送信すると、送信日時が不正なメールとしてメールサーバーに拒否されることがありますのでご注意ください。</p>
---	---

①「マネージメント」から「メール送信設定」を開いて下さい。



## メール送信設定

メール送信設定を行います。

---

- ☒ メール送信機能を有効にする
  - メール送信サーバー
  - メール送信サーバーポート番号
  - 送信元メールアドレス
  - 宛先メールアドレス
  - 接続保護

②「メール送信設定」画面が開きます。

## メール送信設定

メール送信設定を行います。

---

☒ メール送信機能を有効にする

メール送信サーバー

メール送信サーバーポート番号

(1~65535)

送信元メールアドレス

宛先メールアドレス

接続保護

認証方法

ユーザー名

パスワード

☐ メール送信グリーティングメッセージ(EHLO)に送信元メールアドレスのドメインを使用する

☒ WANインターフェース有効時のメール送信を有効にする

☒ 定期メール送信を有効にする

送信間隔

時  分  秒 (0~24時間)

☐ 時刻指定メール送信を有効にする

メール送信スケジュール

メール送信実施時刻

時  分

☒ 装置起動時のメール送信を有効にする

☐ プロセス再起動時のメール送信を有効にする

☐ 有線LANのLinkUP/LinkDOWNによるメール送信を有効にする

メール送信テストを行う

設定保存

43




- メール送信機能を有効にする(チェックボックス)にチェックを入れてください。
- メール送信サーバー: **mail.mrlidm.jp**
- メール送信サーバーポート番号: **587**
- 送信元メールアドレス: **MRL-IDM より通知された送信用メールアドレスを入力してください。**
- 宛先メールアドレス: **MRL-IDM より通知された宛先メールアドレスを入力してください。**  
(別途宛先を追加する場合は,(カンマ)で区切って入力してください。)
- 接続保護: **なし**
- 認証方法: **平文**
- ユーザー名、パスワード: **MRL-IDM より通知されたユーザー名、パスワードを入力してください。**
- WAN インターフェース有効時のメール送信を有効にする(チェックボックス)  
WAN 側回線の接続検知時にアラートを通知したい場合は、チェックを入れて下さい。
- 定期メール送信機能を有効にする(チェックボックス)  
メールによる死活監視を利用する、もしくはステータスメールログ機能を使用する場合はチェックを入れて、送信間隔の設定を行ってください。
  - \* **メールによる死活監視を行う場合、送信間隔はステータスメールログ取り込み時間より短くしてください。**
  - \* **送信間隔を 0 時 0 分 0 秒で設定した場合、メール送信は行われません。**
- 装置起動時のメール送信を有効にする(チェックボックス)  
装置の起動検知時にアラートを通知したい場合は、チェックを入れて下さい。

設定が終わりましたら、[設定保存]ボタンをクリックしてください。  
再起動を行うと設定が反映されます。

### 3-6-4.タイマー自動ファームウェア更新機能の設定

MRL-IDM でファームウェア自動更新を行うための、タイマー自動ファームウェア更新機能の設定について説明します。

	デバイスのファームウェア自動更新を行わない場合は、本設定は不要です。
	「タイマー自動ファームウェア更新機能」は、「NTP クライアント機能」による時刻取得が正常に行われた場合にのみ動作します。
	ファームウェア更新が実行されると、回線の切断と機器の再起動が行われます。 スケジュールの設定については、運用上影響が無い曜日、時刻を設定して下さい。

①「マネージメント」から「ファームウェア更新」を開いて下さい。

設定項目

- 状態表示
- 簡易設定
- 動作モード設定
- 無線LAN設定
- ネットワーク設定
- ファイアウォール設定
- VPN設定
- QoS設定
- マネージメント
  - システム設定
  - 時刻情報・タイマー再起動設定
  - DDNS設定
  - メール送信設定
  - システムログ
  - ファームウェア更新**
  - 設定保存・読み込み

## ファームウェア更新

ファームウェアの更新を行います。

**注意事項**

- ファームウェア更新中は、本機の電源を切ったりク
- ファームウェア更新作業は必ず有線LAN経由で行っ
- ファームウェア更新を行うパソコンと本機を1対1で
- (本機に接続されている他のネットワーク機器は、
- ファームウェア更新後、ダウンロードした設定ファ
- 必ず読み込んでください。

②「タイマー自動ファームウェア更新機能を有効にする」にチェックを入れて下さい。

☒ **タイマー自動ファームウェア更新機能を有効にする**

ファームウェアダウンロードURL


**スケジュール**

☐ 毎日
☐ 日曜 ☐ 月曜 ☐ 火曜 ☐ 水曜 ☐ 木曜 ☐ 金曜 ☐ 土曜

更新実施時刻  時  分  
(0~23) (0~59)

③MRL-IDM にログインして「ファームウェア更新」メニューをクリックして下さい。

④該当機種用のファームウェア更新 URL の URL コピーをクリックして下さい。

FW更新URL一覧 1件						
FW機種	デバイスグループ	FWバージョン名	URL	URLコピー	状態	操作
MR-GM3-D/K/S/DK/DKS/M	01グループ	v1.04.02(MR001)	https://mrlidm.jp/fw-download/		有効	<a href="#">編集</a> <a href="#">削除</a>



**ファームウェアの対象機種を間違えると、ファームウェア更新に失敗して修理が必要となる場合がありますので、注意して下さい。**

⑤コピーした URL をファームウェアダウンロード URL 欄にペースト(貼り付け)して下さい。

☒ タイマー自動ファームウェア更新機能を有効にする

ファームウェアダウンロードURL

スケジュール

☐ 毎日

☒ 日曜

☐ 月曜

☐ 火曜

☐ 水曜

☐ 木曜

☐ 金曜

☐ 土曜


更新実施時刻  時  分

(0~23) (0~59)

設定保存

⑥スケジュールを設定して下さい。

- ・毎日:毎日バージョン確認を行います。
- ・日曜～土曜:曜日を指定してバージョン確認を行います。
- ・更新実施時刻:バージョン確認を実行する時刻を入力して下さい。

  
注意



ファームウェア更新時は、回線の切断とデバイスの再起動が行われます。  
スケジュールの設定については、運用上影響が無い曜日、時刻を設定して下さい。

設定が終わりましたら、[設定保存]ボタンをクリックしてください。

再起動を行うと設定が反映されます。

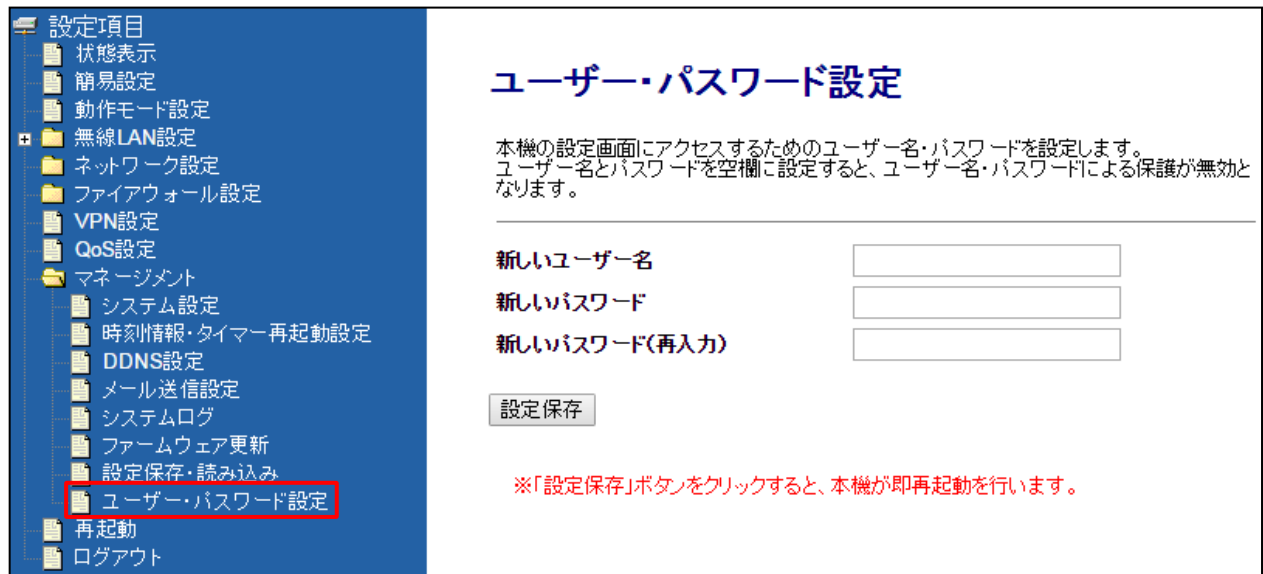
### 3-6-5.WAN 側からの設定(リモート設定)を許可する

MRL-IDM でリモート設定を行うための、「ユーザー・パスワード設定」と「IP フィルタリング設定」について説明します。

	<p>デバイスのリモート設定を行わない場合、本設定は不要です。</p> <p>リモートでデバイスの設定画面にアクセスするためには、デバイスの WAN 側 IP アドレスがグローバル IP アドレスである必要があります。</p>
	<p>WAN側から設定を許可する場合、設定画面にログインするためのユーザー名、パスワードを変更する事を強く推奨します。</p>

①「マネージメント」から「ユーザー・パスワード設定」を開いて下さい。

「ユーザー・パスワード設定」画面が開きます。



設定項目

- 状態表示
- 簡易設定
- 動作モード設定
- 無線LAN設定
  - ネットワーク設定
  - ファイアウォール設定
  - VPN設定
  - QoS設定
  - マネージメント
    - システム設定
    - 時刻情報・タイマー再起動設定
    - DDNS設定
    - メール送信設定
    - システムログ
    - ファームウェア更新
    - 設定保存・読み込み
    - ユーザー・パスワード設定**
  - 再起動
  - ログアウト

## ユーザー・パスワード設定

本機の設定画面にアクセスするためのユーザー名・パスワードを設定します。  
ユーザー名とパスワードを空欄に設定すると、ユーザー名・パスワードによる保護が無効となります。

新しいユーザー名

新しいパスワード

新しいパスワード(再入力)

※「設定保存」ボタンをクリックすると、本機が即再起動を行います。

②ユーザー名、パスワードを工場出荷値のまま利用している場合は、必ずユーザー名、パスワードを変更して下さい。

#### ■新しいユーザー名

設定画面にアクセスするためのユーザー名を入力して下さい。

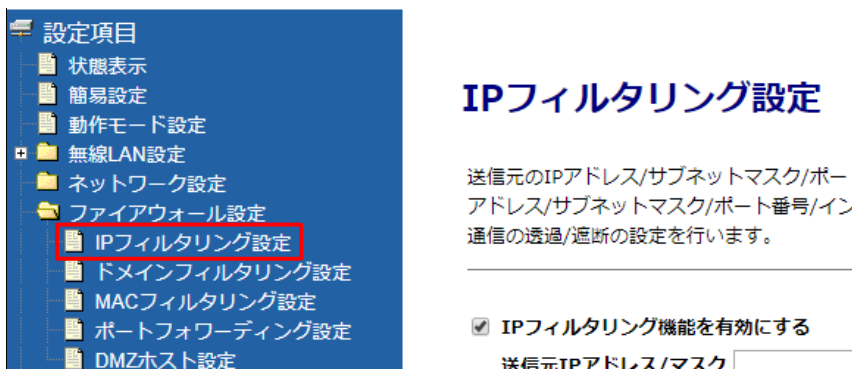
#### ■新しいパスワード、新しいパスワード再入力

設定画面にアクセスするためのパスワードを入力して下さい。

③[設定保存]ボタンをクリックすると即再起動します。

再起動後、変更後のユーザー名、パスワードを要求されますので、設定画面にログインしなおして下さい。

④「ファイアウォール設定」から「IP フィルタリング設定」を開いて下さい。



設定項目

- 状態表示
- 簡易設定
- 動作モード設定
- 無線LAN設定
  - ネットワーク設定
  - ファイアウォール設定
    - IPフィルタリング設定**
    - ドメインフィルタリング設定
    - MACフィルタリング設定
    - ポートフォワーディング設定
    - DMZホスト設定

## IPフィルタリング設定

送信元のIPアドレス/サブネットマスク/ポートアドレス/サブネットマスク/ポート番号/イン通信の透過/遮断の設定を行います。

☒ IPフィルタリング機能を有効にする

送信元IPアドレス/マスク

⑤「IP フィルタリング機能を有効にする」にチェックを入れ、以下のテーブルを追加して下さい。

☒ IPフィルタリング機能を有効にする

送信元IPアドレス/マスク  /  (1~32)  
 宛先IPアドレス/マスク  /  (1~32)  
 プロトコル TCP ▼  
 送信元ポート  -  (0~65535)  
 宛先ポート 80 - 80 (0~65535)  
 送信元インターフェース WAN ▼  
 宛先インターフェース 自機 ▼  
 フィルタ動作 透過 ▼  
 コメント  (半角英数字20文字以内)  

リストへ登録・設定保存

■送信元IP アドレス/マスク

空欄にして下さい。

■宛先IP アドレス/マスク

空欄にして下さい。

■プロトコル

「TCP」を選択して下さい。

■送信元ポート

空欄にして下さい。

■宛先ポート

「80」を入力して下さい。

Web ポート(アクセスポート番号)を変更している場合は、変更したポート番号を入力して下さい。

※10080 は WEB ブラウザのセキュリティ上の問題で使用できないので設定しないでください。

■送信元インターフェース

「WAN」を選択して下さい。

■宛先インターフェース

「自機」を選択して下さい。

■フィルタ動作

「透過」を選択して下さい。

⑥設定が終わりしましたら、[リストへ登録・設定保存]ボタンをクリックして下さい。

IP フィルタリング登録リストに登録されます。

IPフィルタリング 登録リスト (64エントリまで登録可能)									
送信元P/マスク	宛先P/マスク	プロトコル	送信元ポート	宛先ポート	送信元IF	宛先IF	フィルタ動作	コメント	選択
any	any	TCP	any	80 - 80	WAN	自機	透過		<input type="checkbox"/>
選択したエントリを編集		選択したエントリを一つ上げる		選択したエントリを一つ下げる					
選択したエントリを削除		全て削除							

登録が完了すると、WAN 側から設定画面にログインする事が可能になります。

### 3-7.デバイスの設定(MR-GM5A/MR-GM5L)

MRL-IDM を利用するために必要な、デバイス(MR-GM5A/MR-GM5L)の各種設定について説明します。

#### 3-7-1.HTTP 回線監視の設定

MRL-IDM で死活監視を行うための、HTTP 回線監視の設定について説明します。



デバイスの死活監視を行わない場合は、本設定は不要です。

①「ネットワーク設定」から「WAN 設定」を開いて下さい。



②回線監視機能」の設定を行って下さい。

WAN回線監視	
回線監視:	HTTPによる監視 ▼
初期発行間隔:	未使用 ▼
発行間隔:	5分 ▼
連続失敗検出回数:	2 回 (1~60回)
宛先1:	https://mrlidm.jp/monitoring/
宛先2:	www.
宛先3:	www.

#### ■回線監視機能

プルダウンメニューで「HTTPによる監視」を選択して下さい。

#### ■初期発行間隔

回線接続後に回線監視を開始するまでの待ち時間(1/5/15/30/45/60 分)を設定します。

「未使用」を選択した場合、発行間隔の設定で開始します。

#### ■発行間隔

発行間隔を選択して下さい。(1/5/10/15/30/45/60 分)MRL-IDM で設定した監視間隔より短く設定してください。

(例:MRL-IDM の死活監視間隔 30 分の場合、MR-GM5A/MR-GM5L 側は 15 分にする。)

#### ■連続失敗検出回数

任意の回数を設定して下さい。ここで設定した回数、連続して監視に失敗すると、回線切断状態と判断して、回線の再接続や再起動等のリカバリ処理を行います。

#### ■宛先1~3

宛先1に MRL-IDM の「監視・アラート管理」内「HTTP 監視 URL 設定」登録時発行の URL を入力してください。



宛先は MRL-IDM の HTTP 監視 URL 以外も設定して下さい。

MRL-IDM の監視 URL のみ設定した場合、MRL-IDM のメンテナンス等で HTTP 通信が不通になるとデバイスが回線障害と判断して回線の再接続やシステムの再起動等のリカバリ動作を行います。

設定が終わりましたら、[設定保存]ボタンをクリックしてください。

再起動を行うと設定が反映されます。

### 3-7-2.NTP クライアント機能の設定

ステータスメールを送信するためとタイマーファームウェア自動更新を行うための、NTP クライアント機能の設定について説明します。

<div>確認</div>	デバイスのステータス監視、タイマーファームウェア自動更新を行わない場合、本設定は不要です。
	メール送信機能を使用する場合、「NTP クライアント機能」を有効にする事を推奨します。 日時情報が合っていない状態でメールを送信すると、送信日時が不正なメールとしてメールサーバーに拒否されることがありますのでご注意ください。
	「タイマー自動ファームウェア更新機能」は、「NTP クライアント機能」による時刻取得が正常に行われた場合にのみ動作します。

- ①「マネージメント」から「時刻情報 設定」を開いて下さい。
- ②「NTP クライアント機能」で有効(ラジオボタン)を選択して下さい。

IoT Gateway  
MR-GM5L

ステータス  
+ ネットワーク  
+ ファイアウォール  
+ 付加機能  
- マネージメント  
  システム 設定  
  時刻情報 設定  
  メール送信 設定  
  システム ログ  
  ファームウェア更新  
  設定保存・読み込み  
  ログイン 設定  
  再起動

**時刻情報 設定**  
このページでは本機の時刻情報の設定が行えます。  
NTPクライアント機能を有効にすることでシステムの時刻を維持することができます。

現在時刻: 2024 年 9 月 11 日 11 時 11 分 32 秒

タイムゾーン選択: Asia/Tokyo (UTC+09:00)

NTPクライアント機能 ☒ 有効 ☐ 無効

SNTP サーバー: ntp1.jst.mfeed.ad.jp

設定保存 再読み込み

- ③NTPサーバーをプルダウンメニューから選択して下さい。

設定が終わりましたら、[設定保存]ボタンをクリックしてください。  
再起動を行うと設定が反映されます。

### 3-7-3.メール送信機能の設定

MRL-IDM でステータスメールを受信するための、メール送信機能の設定について説明します。

<div>確認</div>	<p>デバイスのステータス監視を行わない場合、本設定は不要です。</p> <p>メール送信機能を使用する場合、「NTP クライアント機能」を有効にする事を推奨します。</p> <p>日時情報が合っていない状態でメールを送信すると、送信日時が不正なメールとしてメールサーバーに拒否されることがありますのでご注意ください。</p>
---------------	---

①「マネージメント」から「メール送信設定」を開いて下さい。

ステータス  
+ ネットワーク  
+ ファイアウォール  
+ 付加機能  
- マネージメント  
システム 設定  
時刻情報 設定  
**メール送信機能 設定**  
システム ログ  
ファームウェア更新  
設定保存・読み込み  
ログイン 設定

**メール送信機能 設定**  
このページではメール送信機能の設定が行えます。

メール送信機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
サーバーアドレス:	
サーバーポート:	0
接続保護:	なし <input type="button" value="▼"/> <input type="checkbox"/> StartTLS(RFC 3207)拡張を
送信サーバー:	認証方式: なし <input type="button" value="▼"/>
ユーザー名:	

②「メール送信設定」画面が開きます。

**メール送信機能 設定**  
このページではメール送信機能の設定が行えます。

メール送信機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
サーバーアドレス:	mail.mrlidm.jp
サーバーポート:	587
接続保護:	なし <input type="button" value="▼"/> <input type="checkbox"/> StartTLS(RFC 3207)拡張を行わない
送信サーバー:	認証方式: 平文 <input type="button" value="▼"/>
ユーザー名:	
パスワード:	*****
送信元メールアドレス:	@mrlidm.jp <input type="checkbox"/> メール送信グリーティングメッセージ(EHLO)に送信元メールアドレスのドメインを使用する
宛先メールアドレス:	system01@mrlidm.jp
送信トリガー:	<input checked="" type="checkbox"/> WANインターフェース有効時のメール送信を有効にする <input checked="" type="checkbox"/> 定期メール送信を有効にする 2 時 0 分 0 秒 (0~24時間) <input type="checkbox"/> 時刻指定メール送信を有効にする ※ <input type="checkbox"/> 毎日 <input type="checkbox"/> 日 <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土 メール送信実施時刻 0 時 0 分 <input checked="" type="checkbox"/> 装置起動時のメール送信を有効にする <input type="checkbox"/> 有線LANのLinkUP/LinkDOWNによるメール送信を有効にする
<div>メール送信テストを行う</div>	

※: 本機能は、NTP等により時刻同期された状態でのみ動作します。

設定保存

■メール送信機能: 有効 (ラジオボタン) を選択して下さい。

■サーバーアドレス: **mail.mrlidm.jp**

■サーバーポート番号: **587**

■接続保護: **なし**

■認証方法: **平文**




- ユーザー名、パスワード:MRL-IDM より通知されたユーザー名、パスワードを入力してください。
- 送信元メールアドレス:MRL-IDM より通知された送信用メールアドレスをここに入力してください。
- 宛先メールアドレス:MRL-IDM より通知された宛先メールアドレスを入力してください。  
(別途宛先を追加する場合は、(カンマ)で区切って入力してください。)
- WAN インターフェース有効時のメール送信を有効にする(チェックボックス)  
WAN 側回線の接続検知時にアラートを通知したい場合は、チェックを入れて下さい。
- 定期メール送信機能を有効にする(チェックボックス)  
メールによる死活監視を利用する、もしくはステータス監視機能を使用する場合はチェックを入れて、送信間隔の設定を行ってください。
  - \* メールによる死活監視を行う場合、送信間隔はステータスメールログ取り込み時間より短くしてください。
  - \* 送信間隔を 0 時 0 分 0 秒で設定した場合、メール送信は行われません。
- 装置起動時のメール送信を有効にする(チェックボックス)  
装置の起動検知時にアラートを通知したい場合は、チェックを入れて下さい。

設定が終わりましたら、[設定保存]ボタンをクリックしてください。  
再起動を行うと設定が反映されます。

### 3-7-4.タイマー自動ファームウェア更新機能の設定

MRL-IDM でファームウェア自動更新を行うための、タイマー自動ファームウェア更新機能の設定について説明します。

	デバイスのファームウェア自動更新を行わない場合は、本設定は不要です。
	「タイマー自動ファームウェア更新機能」は、「NTP クライアント機能」による時刻取得が正常に行われた場合にのみ動作します。
	ファームウェア更新が実行されると、回線の切断と機器の再起動が行われます。 スケジュールの設定については、運用上影響が無い曜日、時刻を設定して下さい。

①「マネージメント」から「ファームウェア更新」を開いて下さい。




②「自動ファームウェア更新」で有効(ラジオボタン)を選択して下さい。



③MRL-IDM にログインして「ファームウェア更新」メニューをクリックして下さい。

④該当機種用のファームウェア更新 URL の URL コピーをクリックして下さい。

FW更新URL一覧 1件						
FW機種	デバイスグループ	FWバージョン名	URL	URLコピー	状態	操作
MR-GM5L	05グループ	v1.00.14(MR001)	https://mrlidm.jp/fw-download/		有効	<a href="#">編集</a> <a href="#">削除</a>


	ファームウェアの対象機種を間違えると、ファームウェア更新に失敗して修理が必要となる場合がありますので、注意して下さい。
---	---

⑤コピーした URL をファームウェアダウンロード URL 欄にペースト(貼り付け)して下さい。

自動ファームウェア更新	
自動ファームウェア更新:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 ※
ファームウェアダウンロードURL:	<input type="text" value="https://mrlidm.jp/fw-download/"/>
曜日:	<input type="checkbox"/> 毎日 <input checked="" type="checkbox"/> 日 <input type="checkbox"/> 月 <input type="checkbox"/> 火 <input type="checkbox"/> 水 <input type="checkbox"/> 木 <input type="checkbox"/> 金 <input type="checkbox"/> 土
ファームウェア更新時刻:	23 時 0 分
※: 自動ファームウェア更新機能は、NTP等により時刻同期された状態でのみ動作します。	
<input type="button" value="設定保存"/>	

⑥スケジュールを設定して下さい。



- ・毎日: 毎日バージョン確認を行います。
- ・日曜～土曜: 曜日を指定してバージョン確認を行います。
- ・更新実施時刻: バージョン確認を実行する時刻を入力して下さい。

	ファームウェア更新時は、回線の切断とデバイスの再起動が行われます。 スケジュールの設定については、運用上影響が無い曜日、時刻を設定して下さい。
---	--

設定が終わりましたら、[設定保存]ボタンをクリックしてください。  
再起動を行うと設定が反映されます。

### 3-7-5.WAN 側からの設定(リモート設定)を許可する

MRL-IDM でリモート設定を行うための、「ログイン設定」と「アクセス制御設定」について説明します。

	<p>デバイスのリモート設定を行わない場合、本設定は不要です。</p> <p>リモートでデバイスの設定画面にアクセスするためには、デバイスの WAN 側 IP アドレスがグローバル IP アドレスである必要があります。</p>
	<p>WAN側から設定を許可する場合、設定画面にログインするためのユーザー名、パスワードを変更する事を強く推奨します。</p>

①「マネージメント」から「ログイン設定」を開いて下さい。

「ログイン設定」画面が開きます。

ステータス  
+ ネットワーク  
+ ファイアウォール  
+ 付加機能  
- マネージメント  
システム 設定  
時刻情報 設定  
メール送信機能 設定  
システム ログ  
ファームウェア更新  
設定保存・読み込み  
**ログイン 設定**  
再起動

#### ログイン 設定

このページでは本機の設定画面にアクセスするためのアカウント設定が行えます。

##### GUIアクセス設定

GUIポート:	8080
ユーザー名:	
パスワード:	

設定保存

②ユーザー名、パスワードを工場出荷値のまま利用している場合は、必ずユーザー名、パスワードを変更して下さい。

#### ■GUI ポート

設定画面にアクセスするための WEB ポート番号を工場出荷値から変更する場合、設定して下さい。(工場出荷値:80)

※10080 は WEB ブラウザのセキュリティ上の問題で使用できないので設定しないでください。

#### ■ユーザー名

設定画面にアクセスするためのユーザー名を入力して下さい。

#### ■パスワード

設定画面にアクセスするためのパスワードを入力して下さい。

③[設定保存]ボタンをクリックして画面が切り替わりましたら、[後で再起動]をクリックして下さい。

④「ファイアウォール設定」から「アクセス制御 設定」を開いて下さい。

ステータス  
+ ネットワーク  
- ファイアウォール  
IP フィルター 設定  
IPv6 フィルター 設定  
MAC フィルター 設定  
ドメインフィルター 設定  
ポートフォワーディング 設定  
**アクセス制御 設定**  
DMZ 設定

#### アクセス制御 設定

このページでは本機への通信を透過/遮断するプロトコルとIPアドレス

アクセス制御機能:	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
WAN側からのPING アタック検出:	1 1秒間に1回
WAN側からのHTTP アタック検出:	30 30秒間に1回

※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作します。

設定保存 設定反映

- ⑤「アクセス制御機能」で有効(ラジオボタン)を選択して、[設定保存]ボタンをクリックして下さい。

**アクセス制御 設定**  
このページでは本機への通信を透過/遮断するプロトコルとIPアドレスの登録、編集、削除および表示が行なえます。

アクセス制御機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容するPINGアクセス数。(0 - 100) ※
WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容する最大TCP/IP(HTTP)コネクション数。(0 - 100) ※

※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作します。

- ⑥以下の各設定を行って下さい。

インターフェース:	WAN ▼
送信元 IPアドレス / マスク:	<input type="text"/> / <input type="text"/>
サービス名:	<input type="checkbox"/> Any <input checked="" type="checkbox"/> http <input type="checkbox"/> ping
動作:	<input type="radio"/> 遮断 <input checked="" type="radio"/> 透過

■インターフェース

プルダウンメニューで「WAN」を選択して下さい。

■送信元IP アドレス/マスク

空欄にして下さい。

■サービス名

「http」にチェックを入れて下さい。

■動作

「透過」を選択して下さい。

- ⑦設定が完了しましたら、[追加]ボタンをクリックして下さい。

アクセス制御 登録リストに登録されます。

アクセス制御 登録リスト				
選択	インターフェース	IPアドレス	サービス	動作
<input type="checkbox"/>	WAN	Any	http	透過

- ⑧[設定反映]ボタンをクリックして下さい。

再起動を行うと設定が反映されます。

**アクセス制御 設定**  
このページでは本機への通信を透過/遮断するプロトコルとIPアドレスの登録、編集、削除および表示が行なえます。

アクセス制御機能:	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
WAN側からのPING アタック検出:	<input type="text" value="1"/> 1秒間に許容するPINGアクセス数。(0 - 100) ※
WAN側からのHTTP アタック検出:	<input type="text" value="30"/> 30秒間に許容する最大TCP/IP(HTTP)コネクション数。(0 - 100) ※

※: 本機能は、WAN側からのアクセスを登録しているサービスに対して動作します。

## 4. 画面操作説明

MRL-IDM が提供する、各メニューについて説明します。

ユーザーがログインした時のメニュー表示です。

各メニューの操作について説明していきます。



#### 4-1. MRL-IDM へのログイン

下記 URL にアクセスして下さい。

・

ログイン画面が開きます。



The image shows a login form titled "ログイン" (Login). It contains two input fields: "ID" and "パスワード" (Password). Below these fields is a blue button labeled "ログイン" (Login).

マイクロリサーチより通知された、ログイン情報に記載されている ID、パスワードでログインして下さい。

## 4-2. デバイス管理

「デバイス管理」画面について説明します。

「デバイス管理」メニューでは、ログインするとユーザーが管理するデバイスグループのデバイス一覧が表示されます。

検索条件部分でデバイスグループや導入時期により検索ができます。

デバイス管理

検索条件

設置場所

導入年月

アラート通知

デバイスグループ

S/N

機種

機種名称

Memo

検索

新記録

デバイス一覧 3台/登録可能台数=20台

10 行ごとに表示

フィルター検索:

設置場所	デバイスグループ	機種	機器名称	ファームウェア	導入日	IPアドレス	MACアドレス	機能	操作
海岸ビル1F	03グループ	MR-GM3-M	MR-GM3LTE1F	v1.04.02(MR001)	2024/02/02		00:10:38:	ログ デュ WEB	編集 削除
海岸ビル2F	02グループ	MR-GM3-M	MR-GM3LTE2F	v1.04.02(MR001)	2024/03/07		00:10:38:	ログ デュ WEB	編集 削除
海岸ビル3F	03グループ	MR-GM3-DKS	MR-GM3LTE3F	v1.04.02(MR001)	2024/03/07		00:10:38:	ログ デュ WEB	編集 削除

3件中 1 ~ 3 件目 表示

← 前

1

次 →

新記録

### 画面の説明: 検索条件

設置場所	デバイス登録時に設定した設置場所で検索します。
デバイスグループ	デバイスグループ名で検索します。
機種	機種名で検索します。
機器名称	デバイス登録時に設定した機器名称を検索します。
導入年月	デバイス登録時に設定した導入年月で検索します。
S/N	デバイス登録時に設定したシリアル No で検索します。 1 台のシリアル No を検索する場合は、両方の入力欄に同じシリアル No を入力して下さい。 範囲での検索も可能ですが必ずしも連番ではございません。検索範囲に漏れている可能性もありますのでご注意下さい。
アラート通知	アラート通知の有効/無効を選択します。

登録台数が多い場合、「検索条件」の各種検索を活用して検索して下さい。

登録時に、わかりやすい設置場所名、機器名称、導入年月を設定する事を推奨します。



画面の説明: 一覧	
デバイス一覧 3台／登録可能台数=20台	現在登録されているデバイスの数と、今のプランで登録可能なデバイスの登録可能台数が表示されています。
フィルター検索: <input type="text"/>	一覧に表示されている項目を部分一致で絞り込みをかける事ができます。
設置場所	デバイス登録時に設定した設置場所が表示されます。
デバイスグループ	デバイスが登録されているデバイスグループが表示されます。
機種	デバイスの機種名が表示されます。 MRL-IDM がデバイスからステータスメールを受信していない場合、空欄になります。
機器名称	デバイス登録時に設定した機器名称が表示されます。
ファームウェア	デバイスのファームウェアバージョンが表示されます。 MRL-IDM がデバイスからステータスメールを受信していない場合、空欄になります。
導入日	デバイス登録時に設定した導入日が表示されます。
IP アドレス	デバイスのWAN側IPアドレスが表示されます。 MRL-IDM がデバイスからステータスメールを受信していない場合、空欄になります。
MAC アドレス	デバイス登録時に設定した MAC アドレスが表示されます。
ログ	デバイスのデバイスオペレーションログ画面に遷移します。
グラフ	デバイスのグラフ画面に遷移します。
WEB	デバイスのリモート設定が可能になっている場合、WEB 通信でデバイスの設定画面を操作できます。 操作・設定内容については、MR-GMx シリーズのユーザーマニュアルをご参照下さい。
編集	デバイス管理の編集画面が開きます。
削除	デバイスの削除画面が開きます。 デバイスを削除した場合、ログも同時に削除されますのでご注意ください。
+ 新規登録	新規登録画面が開きます。

<div>確認</div>	<p>リモートでデバイスの設定画面にアクセスするためには、以下の条件が必要です。</p> <ul style="list-style-type: none"> <li>・デバイスの WAN 側 IP アドレスがグローバル IP アドレスである事。</li> <li>・デバイス側で「WAN 側からの設定画面へのアクセスを許可する設定」がされている事。</li> </ul> <p>デバイス側の設定方法については、MR-GMx シリーズのユーザーズマニュアルを参照して下さい。</p>
---------------	---

#### 4-2-1. 新規登録

「新規登録」ボタンをクリックして下さい。

デバイス 新規登録

設置場所

機器名称 必須

MACアドレス 必須

デバイスグループ 必須

アラート通知 必須

S/N

導入日

IPアドレス

WEBポート

WEBログインID

WEBパスワード


Memo

登録

閉じる

設置場所	設置場所を入力して下さい。
機器名称	デバイスの名称を入力して下さい。 <b>デバイスの判別がつくように個別の設定値にする事を推奨します。</b>
MAC アドレス	デバイスの LAN ポート MAC アドレスを入力して下さい。 デバイスの LAN ポート MAC アドレスは、底面のシールや設定画面で確認する事ができます。 「MAC:001038xxxxxx」の「001038xxxxxx」を入力して下さい。 <b>MRL-IDM はデバイスを MAC アドレスで判別します。MAC アドレスが正しく設定されていないと MRL-IDM を利用する事はできませんのでご注意ください。</b>
デバイスグループ	このデバイスが所属するデバイスグループを選択して下さい。
アラート通知	死活監視アラート通知、ステータスアラート通知の有効・無効を設定します。 無効の場合、アラートチェック、ログ表示を行いません。
S/N	デバイスのシリアル No を入力して下さい。 デバイスの底面に貼られているシールの「S/N:GMxxxxxxxxxx」の GMxxxxxxxxxx を入力して下さい。
導入日	導入設置日を選択して下さい。
IP アドレス	デバイスの WAN 側 IP アドレスを入力して下さい。 リモート設定を行う場合、ここで設定した IP アドレスへアクセスします。 空欄にした場合、ステータスメールで取得したIPアドレスへアクセスします。

WEB ポート	デバイスの WEB 設定ポート番号を入力して下さい。 デバイス側で WEB 設定ポート番号を変更している場合は、変更したポート番号を入力して下さい。
WEB ログイン ID	デバイスの設定画面にログインするためのログイン ID を保存する場合、入力して下さい。 空欄にした場合、ログインIDの入力を求められます。 (MR-GM3 シリーズ、MR-GM3L シリーズのみ保存可能です)
WEB パスワード	デバイスの設定画面にログインするためのパスワードを保存する場合、入力して下さい。 空欄にした場合、パスワードの入力を求められます。 (MR-GM3 シリーズ、MR-GM3L シリーズのみ保存可能です)
Memo	デバイスに関するメモを入力できます。

	<p>リモートでデバイスの設定画面にアクセスするためには、以下の条件が必要です。</p> <ul style="list-style-type: none"> <li>・デバイスの WAN 側 IP アドレスがグローバル IP アドレスである事。</li> <li>・デバイス側で「WAN 側からの設定画面へのアクセスを許可する設定」がされている事。</li> </ul> <p>デバイス側の設定方法については、MR-GMx シリーズのユーザーズマニュアルを参照して下さい。</p>
---	---

「登録」ボタンを押して、保存して下さい。

デバイス一覧に、登録したデバイスの情報が表示されていることを確認して下さい。

現在のプランでのデバイス登録可能台数に達している場合、「新規登録」ボタンをクリックすると下記エラーメッセージが表示されます。

この場合、未使用のデバイスを削除するか、プランを変更してから新規登録して下さい。

すでに登録台数に達しています。デバイスを削除してから登録するか、プランを変更してください。

OK

4-2-2. 編集

該当デバイスの「編集」ボタンをクリックして下さい。

デバイス 編集

設置場所

海岸ビル1F

機器名称 必須

MR-GM3LTE1F

MACアドレス 必須

00:10:38:

デバイスグループ 必須

03グループ

アラート通知 必須

有効

機種

MR-GM3-M

S/N

GM3

導入日

2024/02/02

IPアドレス

WEBポート

80

WEBログインID

WEBパスワード

Memo

デジタルサイネージ用

登録日: 2024/02/02 17:22:53

更新日: 2024/04/26 20:31:45

保存

閉じる

設置場所	設置場所を入力して下さい。
機器名称	デバイス機器の名称を入力して下さい。
MAC アドレス	デバイスの LAN ポート MAC アドレスを入力して下さい。 デバイスの LAN ポート MAC アドレスは、底面のシールや設定画面で確認する事ができます。 「MAC:001038xxxxxx」の「001038xxxxxx」を入力して下さい。 <b>MRL-IDM はデバイスを MAC アドレスで判別します。</b> <b>MAC アドレスが正しく設定されていないと MRL-IDM を利用する事はできませんのでご注意下さい。</b>
デバイスグループ	このデバイスが所属するデバイスグループをして下さい。
アラート通知	死活監視アラート通知、ステータスアラート通知の有効・無効を設定します。 無効の場合、アラートチェック、ログ表示を行いません。
機種	デバイスからのメールを受信するとメール情報から取得して自動で機種が表示されます。 (自動判定入力)
S/N	デバイスのシリアル No を入力して下さい。 デバイスの底面に貼られているシールの「S/N:GMxxxxxxxxxx」の GMxxxxxxxxxx を入力して下さい。
導入日	導入設置日を選択して下さい。
IP アドレス	デバイスの WAN 側 IP アドレスを入力して下さい。 リモート設定を行う場合、ここで設定した IP アドレスへアクセスします。 空欄にした場合、ステータスメールで取得したIPアドレスへアクセスします。

WEB ポート	デバイスの WEB 設定ポート番号を入力して下さい。 デバイス側で WEB 設定ポート番号を変更している場合は、変更したポート番号を入力して下さい。
WEB ログイン ID	デバイスの設定画面にログインするためのログイン ID を保存する場合、入力して下さい。 空欄にした場合、ログインIDの入力を求められます。 (MR-GM3 シリーズ、MR-GM3L シリーズ、のみ保存可能です)
WEB パスワード	デバイスの設定画面にログインするためのパスワードを保存する場合、入力して下さい。 空欄にした場合、パスワードの入力を求められます。 (MR-GM3 シリーズ、MR-GM3L シリーズのみ保存可能です)
Memo	デバイスに関するメモを入力できます。

<div> <div></div> <div>確認</div> </div>	<p>リモートでデバイスの設定画面にアクセスするためには、以下の条件が必要です。</p> <ul style="list-style-type: none"> <li>・デバイスの WAN 側 IP アドレスがグローバル IP アドレスである事。</li> <li>・デバイス側で「WAN 側からの設定画面へのアクセスを許可する設定」がされている事。</li> </ul> <p>デバイス側の設定方法については、MR-GMx シリーズのユーザーズマニュアルを参照して下さい。</p>
--	---

「保存」ボタンをクリックして下さい。デバイスイ覧に戻ります。

#### 4-2-3. 削除



デバイスを削除した場合、ログも同時に削除されますのでご注意ください。

削除するデバイスの「削除」をクリックして下さい。

×

デバイス 削除

設置場所

海岸ビル1F

機器名称

MR-GM3LTE1F

MACアドレス

00:10:38:

デバイスグループ

01グループ ▾

アラート通知

有効 ▾

機種

MR-GM3-M

S/N

GM3

導入日

2024/02/02

IPアドレス

WEBポート

80

WEBログインID

WEBパスワード

Memo

登録日：2024/02/02 17:22:53

更新日：2024/04/28 11:19:09

削除

閉じる

削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、確認アラート画面が開きます。

このデバイスを削除しますか？

OK

キャンセル

「OK」をクリックするとデバイスが削除されます。

削除しない場合は「キャンセル」ボタンをクリックして下さい。

#### 4-3. デバイス監視

「デバイス監視」画面について説明します。

ユーザーアカウントでログインすると、そのユーザーが管理するデバイスグループのデバイスのみが表示されます。

デバイスの稼働状況「稼働」「警告」「停止」が表示され、そのデバイスの「ログ」、「グラフ」、「WEB」(リモート設定)画面に遷移することができます。

デバイス監視

Check Me!

・監視・アラート管理で、HTTP監視用URLが監視に紐づいていないようです。「[HTTP監視用URL設定](#)」をご確認ください。

デバイス一覧 3件

(ここに表示されていないデバイスは、まだ死活監視の設定がされていません。[死活監視設定](#)をしてください)

10

▼ 行ごとに表示

フィルター検索:

状態	受信種別	日時	設置場所	機種	機器名称	IPアドレス	MACアドレス	詳細
稼働		2024/05/16 11:22:06	海岸ビル1F	MR-GM3-M	MR-GM3LTE1F		00:10:38:	ログ グラフ WEB
停止		2024/03/08 14:12:21	海岸ビル2F	MR-GM3-M	MR-GM3LTE2F		00:10:38:	ログ グラフ WEB
稼働		2024/05/16 11:12:06	海岸ビル3F	MR-GM3-D KS	MR-GM3LTE3F		00:10:38:	ログ グラフ WEB

3件中1～3件目表示

← 前

1

次 →

画面の説明	
サジェスト (ビジネスプランのみ)	MRL-IDM の設定について矛盾した設定等を検知した場合、メッセージを表示します。
フィルター検索	状態、日時、設置場所、機種、機器名称、IP アドレス、MAC アドレスなど一覧に表示されている項目の部分一致で絞り込みをかける事ができます。
状態	<div> <div>稼働</div> <div>警告</div> <div>停止</div> </div> <div> <div>デバイスからの死活監視通信を監視間隔で設定した通りに受信している状態です。</div> <div>デバイスからの死活監視通信を1回受信できていない状態です。</div> <div>デバイスからの死活監視通信を2回連続で受信できていない状態です。</div> </div>
受信種別	<div> <div>死活監視の受信種別を表示します。</div> <div> <div></div> <div>HTTP 通信での死活監視時に表示されます。</div> </div> <div> <div></div> <div>メールでの死活監視時に表示されます。</div> </div> </div>
日時	HTTP 通信での死活監視時は、HTTP 通信を受信した最新の日時が表示されます。 メールでの死活監視時は、ステータスメールログの最新の登録日時が表示されます。
設置場所	デバイス登録時に設定した設置場所が表示されます。
機種	デバイスの機種名が表示されます。 MRL-IDM がデバイスからステータスメールを受信していない場合、空欄になります。
機器名称	デバイス登録時に設定した機器名称が表示されます。
IP アドレス	HTTP 通信での死活監視時は、HTTP 通信の送信元 IP アドレスが表示されます。 メールでの死活監視時は、ステータスメールログの WAN 側 IP アドレスが表示されます。
MAC アドレス	デバイス登録時に設定した MAC アドレスが表示されます。
ログ	ステータスメールログ画面に遷移します。
グラフ	デバイスステータスグラフ画面に遷移します。
WEB	デバイスのリモート設定が可能になっている場合、WEB 通信でデバイスの設定画面を操作できます。 操作・設定内容については、MR-GMx シリーズのユーザーマニュアルをご参照下さい。

#### 4-4. ファームウェア更新

「ファームウェア更新」画面について説明します。

ユーザーアカウントでログインすると、そのユーザーが管理するバイスグループの FW 更新用 URL が一覧で表示されます。

ファームウェア更新

新規登録

FW更新URL一覧 2件

10 行ごとに表示

フィルター検索:

デバイスシリーズ(FW対応機種)	デバイスグループ	FWバージョン名	URL	URLコピー	状態	操作
MR-GM5L series (MR-GM5L)	02:南関東グループ	v2. (MR00 1)	https://		有効	編集 削除
MR-GM3 series (MR-GM3-D/K/S/DK/DKS/M/W)	01:南関東グループ	v1.	http://		有効	編集 削除

2件中 1 ~ 2 件目 表示

← 前

1

次 →


新規登録


画面の説明：一覧	
フィルター検索:	FW 機種、デバイスグループ、FW バージョン名、URL、状態など一覧に表示されている項目の部分一致で絞り込みをかける事ができます。
デバイスシリーズ(FW 対応機種)	ファームウェアの対象機種名を表示します。
デバイスグループ	URL に紐づくデバイスグループ名を表示します。
FW バージョン名	URL に適用されているファームウェアバージョンを表示します。
URL	F/W 更新 URL を表示します。 この URL をデバイス側「自動ファームウェア更新」設定の「ファームウェアダウンロード URL」に設定して下さい。
	URL をクリップボードにコピーします。
編集	編集画面が開きます。
削除	削除画面が開きます。
新規登録	新規登録画面が開きます。



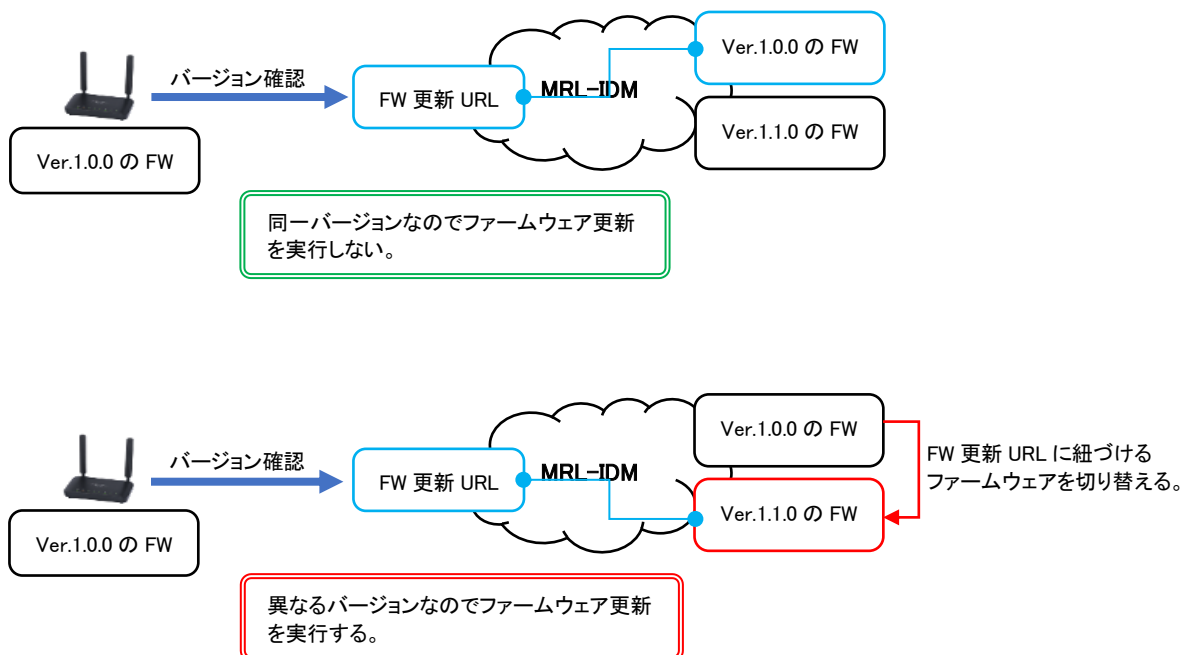
利用可能なファームウェア情報が、MRL-IDM で公開されます。

本画面で作成した URL を、あらかじめデバイス側の「ファームウェア更新」設定の「ファームウェアダウンロード URL」に指定しておくことで、指定されたバージョンのファームウェアに更新する事が可能です。

 確認	<b>MRL-IDM のファームウェア管理でバージョンを指定するだけではファームウェアは更新されません。</b> <b>必ずデバイス側「自動ファームウェア更新」設定の「ファームウェアダウンロード URL」に、あらかじめ MRL-IDM で発行した URL を登録しておいて下さい。</b>
---	---

 注意	<b>対象機種を間違えるとファームウェア更新に失敗し、修理が必要となる場合がありますのでご注意ください。</b>
---	--

MRL-IDM では、FW(ファームウェア)更新 URL に紐づけるファームウェアのバージョンを指定する、という運用方法になります。



#### 4-4-1. 新規登録

「新規登録」ボタンをクリックして下さい。

×

ファームウェア更新URL 編集

デバイスシリーズ(FW対応機種) 必須

MR-GM5L :[MR-GM5L]

デバイスグループ 必須

02:南関東グループ

FWバージョン名 必須

v2. (MR001)

送信プロトコル 必須

HTTPS

URL

https://

状態 必須


有効

更新日:

保存

閉じる

デバイスシリーズ(FW 対応機種)	対象となるファームウェアを適用する機種グループを選択して下さい。
デバイスグループ	ファームウェア更新 URL を適用するデバイスグループを選択して下さい。
FW 機種	対象となるファームウェアを適用する機種グループを選択して下さい。
FW バージョン名	マイクロリサーチから通知されたバージョン名を選択して下さい。 次回バージョンアップ時にここで選択したファームウェアが適用されるようになります。
URL	自動発行されます。 この URL をデバイス側「自動ファームウェア更新」設定の「ファームウェアダウンロード URL」に設定して下さい。
状態	有効/無効が選択できます。 無効にすると、この URL を参照しているデバイスは自動バージョンアップが実行されなくなります。



**対象機種を間違えるとファームウェア更新に失敗し、修理が必要となる場合がありますのでご注意ください。**

「登録」ボタンを押して、保存して下さい。

FW 更新 URL 一覧に、登録した FW 更新 URL の情報が表示されていることを確認して下さい。

#### 4-4-2. 編集

FW 更新 URL に紐づくファームウェアのバージョンを変更する場合や、デバイスグループを変更する場合、ファームウェア更新 URL 編集操作を行って下さい。

編集する FW 更新 URL の「編集」ボタンをクリックして下さい。

×

ファームウェア更新URL 削除

デバイスシリーズ(FW対応機種) 必須

MR-GM5L :[MR-GM5L]

デバイスグループ 必須

02:南関東グループ

FWバージョン名 必須

v2. (MR001)

送信プロトコル 必須

HTTPS

URL

https://

状態 必須

有効

更新日:

削除

閉じる

デバイスシリーズ(FW 対応機種)	編集不可です。
デバイスグループ	ファームウェアを適用するデバイスグループを変更できます。
FW 機種	編集不可です。
FW バージョン名	ここで選択したファームウェアバージョンが適用されます。
URL	編集不可です。 デバイス側の「ファームウェアダウンロード URL」に、この URL が設定されている場合、デバイス側で設定したスケジュールでこの URL に対してバージョンチェックを行います。 デバイス本体と FW 更新 URL に紐づけたファームウェアバージョンが異なる場合、ファームウェア更新が実行されます。
状態	有効/無効が選択できます。 無効にすると、デバイスは自動バージョンアップされなくなります。

「保存」ボタンを押して、保存して下さい。

FW 更新 URL 一覧に、登録した FW 更新 URL の情報が表示されていることを確認して下さい。

<div>確認</div>	<b>ファームウェアのバージョンダウンは動作保証外となります。</b>
---------------	-------------------------------------

#### 4-4-3. 削除

削除する FW 更新 URL の「削除」ボタンをクリックして下さい。



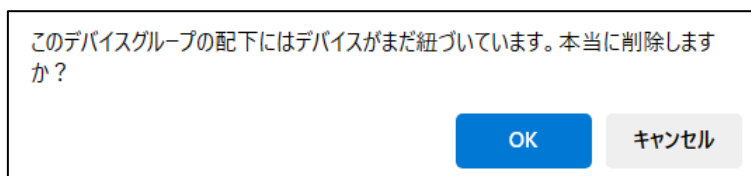
削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、以下の確認メッセージが表示されます。



「OK」をクリックすると削除されます。「キャンセル」をクリックすると閉じます。

削除する設定のデバイスグループの配下にデバイスが紐づいている場合、以下の確認メッセージが表示されます。



デバイス側でこの URL を使っている可能性があるので、削除しても問題が無いか再度確認して下さい。

「OK」をクリックすると削除されます。

削除された URL がデバイスに登録されている場合、自動バージョンアップは行われなくなります。

## 4-5. 死活監視アラート条件設定

「死活監視アラート条件設定」画面について説明します。

ユーザーアカウントでログインすると自分が管理するデバイスグループ分の設定のみが表示されます。

死活監視アラート条件設定

検索条件

デバイスグループ

検索

死活監視アラート条件一覧 2件

10

並び替え

フィルター検索:

デバイスグループ	監視種別	監視間隔	警告時通知先	停止時通知先	状態	操作
★[デフォルト設定]	HTTP監視 {GMSL}	5分	警告時の通知先	緊急時	有効	
[個別設定] 01グループ/02グループ	HTTP監視 {HTTP監視}	1分	警告時の通知先	緊急時	有効	編集 削除

2件中1～2件目表示

前

1

次

新規登録

### 画面の説明: 検索条件

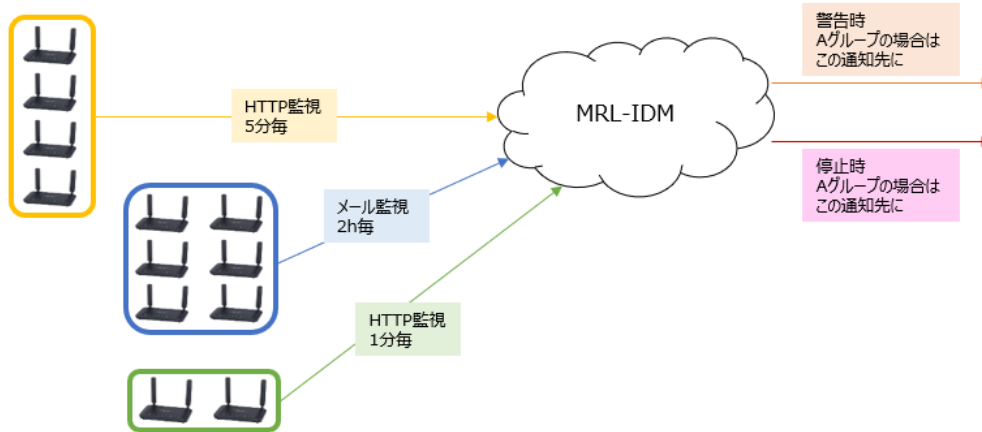
<div>デバイスグループ</div>	デバイスグループ名で検索します。
---------------------	------------------

### 画面の説明: 一覧

<div>フィルター検索:</div>	デバイスグループ名、監視種別、監視間隔、警告時通知先、停止時通知先、状態など一覧に表示されている項目の部分一致で絞り込みをかける事ができます。
<div>デバイスグループ</div>	設定に紐づけされたデバイスグループ名を表示します。 「デフォルト設定」: 管理者アカウントが全グループ共通として設定した設定になります。 「個別設定+デバイスグループ名」: デバイスグループ指定で個別に設定した項目が表示されています。デフォルト設定の編集削除などは管理者アカウントのみ操作可能です。
<div>監視種別</div>	死活監視の種別を表示します。 HTTP 監視: デバイスの HTTP 監視機能により死活監視を行います。 メール監視: デバイスのメール送信機能により死活監視を行います。
<div>監視間隔</div>	死活監視の監視間隔を表示します。
<div>警告時通知先</div>	警告時アラートの通知先設定名を表示します。
<div>停止時通知先</div>	停止時アラートの通知先設定名を表示します。
<div>状態</div>	死活監視アラート条件設定の有効・無効を表示します。
<div>編集</div>	編集画面が開きます。
<div>削除</div>	削除画面が開きます。
<div>新規登録</div>	新規登録画面が開きます。

死活監視アラート条件設定は、デバイスシリーズ、デバイスグループごとに、監視種別、監視間隔、アラート通知先を設定できます。

各デバイスグループ毎に、  
監視種別(HTTP/メール)、監視間隔、アラート通知先を設定できます。



死活監視アラート条件設定メニューで、

- ・デバイスシリーズは？
- ・どのデバイスグループを対象とした設定か？
- ・監視種別は？(HTTP 監視 or メール監視)
- ・監視間隔は？
- ・アラート通知先は？

を紐づけて、死活監視を行います。

また、アラート通知した際のログは、ログ管理の死活監視アラートログに保存されます。

監視対象	設定項目		ログ
<div>死活監視アラート条件 [デフォルト設定] or [個別設定 (デバイスグループ)]</div> <div>デフォルト設定</div> <div> <div>HTTP監視 5分毎</div> <div>メール監視 2h毎</div> <div>HTTP監視 5分毎</div> <div>HTTP監視 1分毎</div> </div>	<div>監視種別/監視間隔</div> <div>HTTP監視の場合</div> <div>HTTP監視URL設定メニュー [URL, 監視間隔]</div> <div>メール監視の場合</div> <div>ステータスメールログ設定メニュー [メール取込間隔]</div>	<div>アラート通知先</div> <div>警告時</div> <div>アラート通知先設定メニュー [通知先, 通知時間, 通知曜日]</div> <div>停止時</div> <div>アラート通知先設定メニュー [通知先, 通知時間, 通知曜日]</div>	<div>死活監視アラートログ</div>
<p>デフォルトとしてデバイスシリーズが同じグループ全部を対象として監視条件を設定できます。 また、個別設定として、デバイスグループ毎にも、監視条件を設定できます。</p>	<p>HTTP通信ができる環境に設置されているデバイスの場合、HTTP回線監視機能を使いIDMのHTTPURLをコールすることで死活監視できます。 デバイスから送るステータスメールを使って、メールだけの死活監視も可能です。</p>	<p>警告 = 監視間隔時間以上通信がない 停止 = 監視間隔時間×2以上通信がない それぞれ警告、停止状態になったらどこに通知するかを設定できます。 通知する時間帯、曜日の指定も可能です。 メール以外にもSlack/chat work/teamsへも通知できます。</p>	<p>死活監視でアラート通知した場合、その履歴をログ管理＞死活監視アラートログに保存されています。</p>

確認

「デフォルト設定」は管理者のみ登録・編集・削除が可能な項目です。

#### 4-5-1. 新規登録

「新規登録」ボタンをクリックして下さい。

死活監視アラート条件 新規登録
✕

**デバイスシリーズ** 必須

**デバイスグループ** 必須

**監視種別** 必須

**監視間隔** 必須

**通知先** 必須

**状態** 必須

警告時:
新規登録

停止時:
新規登録

※条件を登録しなかったら「新規登録」で各条件を登録してください。

※「編集」で今選択されている条件の編集を行うことができます。

登録

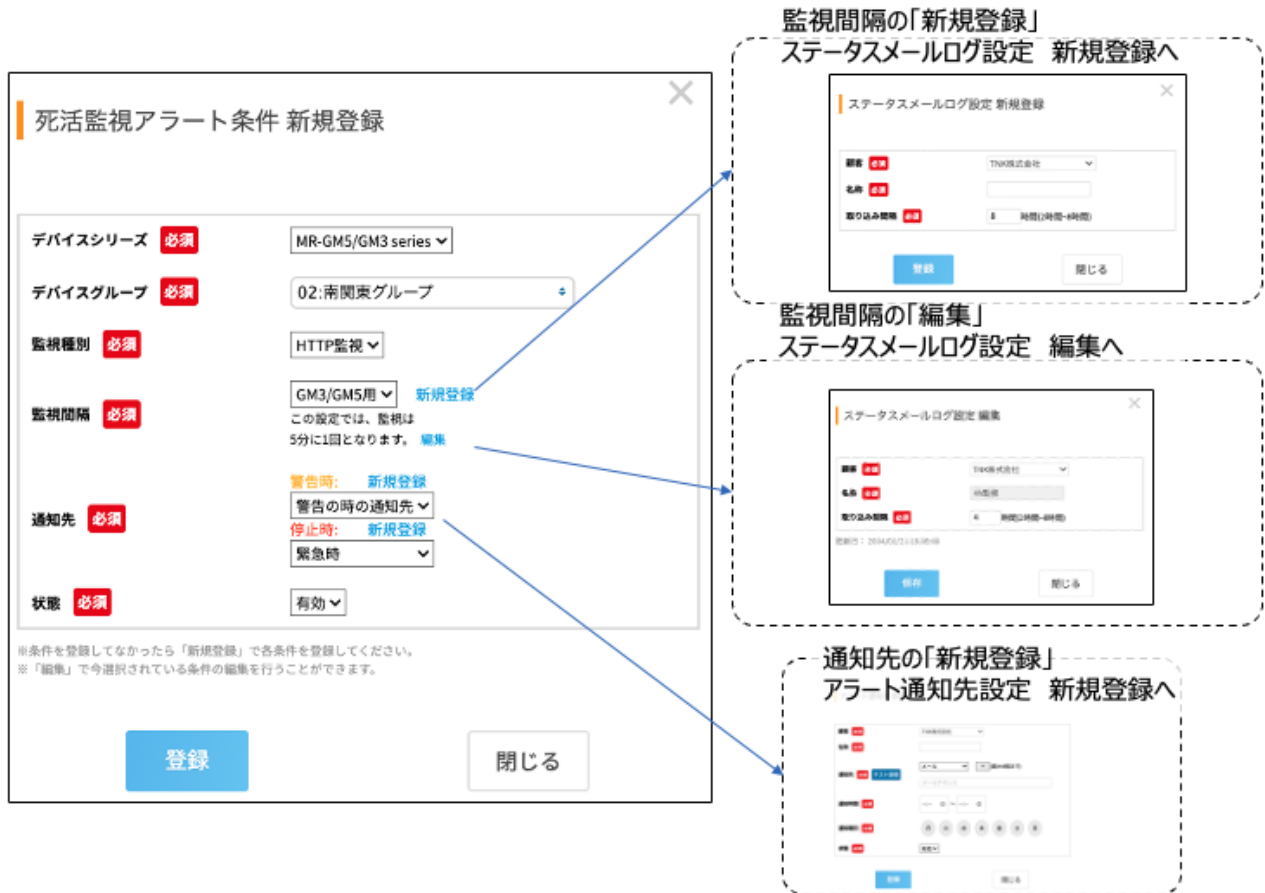
閉じる

デバイスシリーズ	どのデバイスシリーズを対象とするかを選択して下さい。
デバイスグループ	デバイスグループを選択して下さい。 デバイスグループは重複して条件を設定することはできません。
監視種別	HTTP 監視かメール監視を選択して下さい。
監視間隔	<p>【HTTP 監視】: 監視間隔は「HTTP 監視 URL 設定」メニューで設定した「HTTP 監視間隔」の設定値が適用されます。</p> <p>【メール監視】: 監視間隔は「ステータスメールログ設定」メニューで設定した「取り込み間隔」の設定値が適用されます。</p> <p>・監視間隔の横に表示される「新規登録」を押すと、新たに HTTP 監視 URL やステータスメールログを作成することができます。</p> <p>・監視間隔を選択すると、監視間隔時間がテキストで表示されるようになります。ここで「編集」を押すと、HTTP 監視 URL やステータスメールログの編集を行い、間隔時間を変更することができます。</p>
通知先(警告時、停止時)	「アラート通知先設定」で設定した通知先を選択して下さい。
状態	<p>有効: 死活監視チェックを行い、監視ログも保存されます。</p> <p>無効: 死活監視チェックが行われず、監視ログも保存されません。</p>

「登録」ボタンを押して、保存して下さい。

死活監視アラート条件一覧に、今登録した条件の情報があることを確認して下さい。

「死活監視アラート条件設定」画面と、他の設定との遷移関係は下図のようになります。



「死活監視アラート条件設定」画面から、「HTTP 監視 URL 設定」、「ステータスメールログ設定」の新規登録・編集、「アラート通知先設定」の新規登録が可能です。



4-5-2. 編集

編集する死活監視アラート条件の「編集」ボタンをクリックして下さい。

死活監視アラート条件 編集

デバイスシリーズ 必須

MR-GM5/GM3 series

デバイスグループ 必須

02:南関東グループ, 01:南関東グループ

監視種別 必須

HTTP監視

監視間隔 必須

GM3/GM5用

新規登録

この設定では、監視は5分に1回となります。

編集

通知先 必須

警告時: 新規登録

警告の時の通知先

停止時: 新規登録

緊急時

状態 必須

有効

更新日: 2024/09/12 18:46:56

※条件を登録しなかったら「新規登録」で各条件を登録してください。  
※「編集」で今選択されている条件の編集を行うことができます。

保存

閉じる

デバイスグループ	デバイスグループを選択して下さい。 デバイスグループは重複して条件を設定することはできません。
監視種別	HTTP 監視かメール監視を選択して下さい。
監視間隔	【HTTP 監視】:監視間隔は「HTTP 監視 URL 設定」メニューで設定した「HTTP 監視間隔」の設定値が適用されます。 【メール監視】:監視間隔は「ステータスメールログ設定」メニューで設定した「取り込み間隔」の設定値が適用されます。 ・監視間隔の横に表示される「新規登録」を押すと、新たに HTTP 監視 URL やステータスメールログを作成することができます。 ・監視間隔を選択すると、監視間隔時間がテキストで表示されるようになります。ここで「編集」を押すと、HTTP 監視 URL やステータスメールログの編集を行い、間隔時間を変更することができます。
通知先(警告時、停止時)	「アラート通知先設定」で設定した通知先を選択して下さい。
状態	有効: 死活監視チェックを行い、監視ログも保存されます。 無効: 死活監視チェックが行われず、監視ログも保存されません。

「保存」ボタンをクリックして下さい。死活監視アラート条件一覧に戻ります。

#### 4-5-3. 削除

削除する死活監視アラート条件の「削除」をクリックして下さい。

×

死活監視アラート条件 削除

デバイスシリーズ

MR-GM5/GM3 series ▼

デバイスグループ

02:南関東グループ ▼

監視種別

HTTP監視 ▼

監視間隔

GM3/GM5用 ▼ 新規登録

この設定では、監視は5分に1回となります。 編集

通知先

警告時: 新規登録

警告の時の通知先 ▼

停止時: 新規登録

緊急時 ▼

状態

有効 ▼

更新日: 2024/09/12 21:13:52

※条件を登録しなかったら「新規登録」で各条件を登録してください。

※「編集」で今選択されている条件の編集を行うことができます。

削除

閉じる

削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、以下の確認メッセージが表示されます。

この設定を削除しますか？

OK

キャンセル

「OK」をクリックすると削除されます。「キャンセル」をクリックすると閉じます。

削除する設定のデバイスグループに他の設定が紐づいている場合、以下の確認メッセージが表示されます。

このデバイスグループは使用中です。本当に削除しますか？

OK

キャンセル

削除しても問題が無いか再度確認して下さい。

「OK」をクリックすると削除されます。

他のユーザーと共有しているグループがある場合は、削除できません。

他のユーザーが管理しているデバイスグループ(03:北関東グループ)がこの条件に紐づいています。他のデバイスグループの紐付けを解除してからでないと削除できません。あるいは管理者に削除してもらうようにしてください。

OK

4-6. ステータスアラート条件設定

「ステータスアラート条件設定」画面について説明します。  
ユーザーアカウントでログインすると、自分が管理するデバイスグループ分の設定のみが表示されます。

ステータスアラート条件設定

検索条件

デバイスグループ

デバイスシリーズ

詳細名

送信条件

検索

新規登録

ステータスアラート条件一覧 2件

10

行ごとに表示

フィルター検索:

デバイスグループ	詳細名	送信条件	値	監視間隔	通知先	操作
★[デフォルト設定]	メール送信のトリガー	一致	WAN interface Active	4時間	緊急時	<div>編集</div> <div>削除</div>
[個別設定] 01グループ	メール送信のトリガー	一致	WAN interface Active	2時間	警告の時の通知先	<div>編集</div> <div>削除</div>

2件中1～2件目表示

← 前

1

次 →



新規登録

画面の説明: 検索条件

デバイスグループ	デバイスグループ名で検索します。
デバイスシリーズ	デバイスシリーズで検索します。 GM3 series/GM5 series から選択します。
詳細名	デバイスシリーズを選択することで、そのデバイスシリーズに関する詳細名が選択できるようになります。
送信条件	送信条件で検索します。

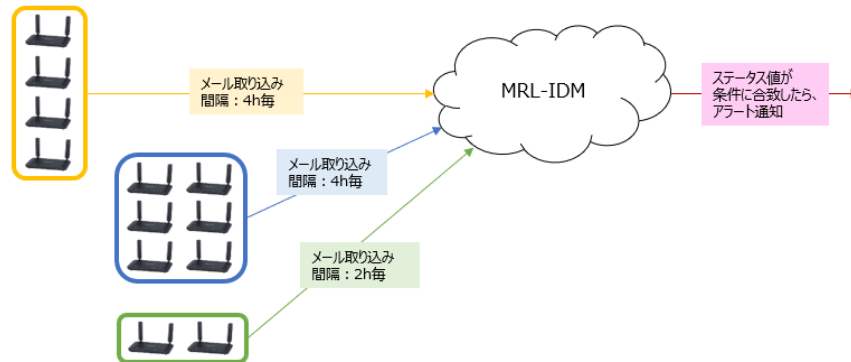
画面の説明: 一覧

フィルター検索:	デバイスグループ名、詳細名、送信条件、値、監視間隔、通知先など一覧に表示されている項目の部分一致で絞り込みをかける事ができます。
デバイスグループ	設定に紐づけされたデバイスグループ名を表示します。 「デフォルト設定」: 管理者アカウントが全グループ共通として設定した設定になります。 「個別設定+デバイスグループ名」: デバイスグループ指定で個別に設定した項目が表示されています。デフォルト設定の編集削除などは管理者アカウントのみ操作可能です。
詳細名	詳細名（条件とするステータス名）を表示します。
送信条件	ステータスアラート送信の条件を表示します。（一致・以下・以上）
値	ステータスアラート送信の条件の値を表示します。
監視時間	ステータスメールログの取り込み間隔を表示します。
通知先	アラート条件に合致したときのアラート通知先設定名を表示します。
編集	編集画面が開きます。

	削除画面が開きます。
	新規登録画面が開きます。

## ステータスアラート条件設定とは？

各デバイスグループ毎に、  
デバイスのステータスを見てどういったアラートを送るか？を設定する画面になります。



デバイスのステータスは、各デバイス側のメール送信機能の設定を行い、MRL-IDM へステータスメールを送信して下さい。

## デバイスから送信されるステータスの例：

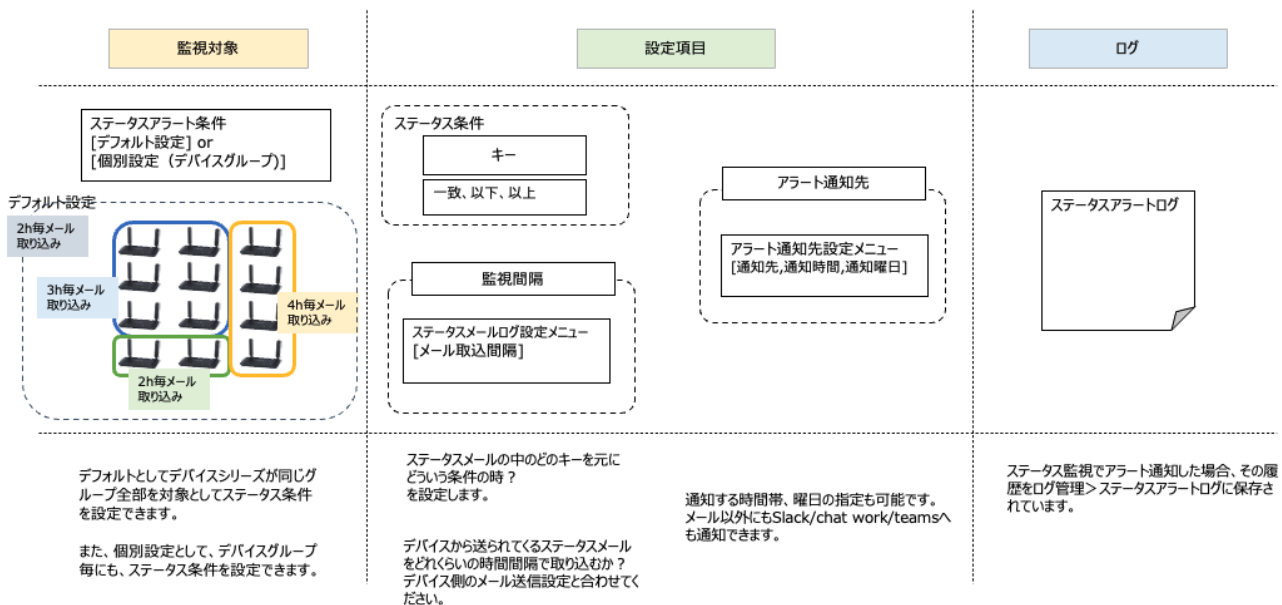
- ・メールの送信トリガー（回線の接続やシステムの再起動）
- ・アンテナ状態（SQ）
- ・受信信号強度（RSSI）

ステータスアラート条件設定メニューで、

- ・どのデバイスグループを対象とした設定か？
- ・どのデバイスシリーズか？
- ・どのステータスが
- ・どうなったら？
- ・アラート通知先は？

を紐づけて、ステータス監視を行います。

また、アラート通知した際のログは、ログ管理のステータスアラートログに保存されます。



#### 4-6-1. 新規登録

「新規登録」ボタンをクリックして下さい。

ステータスアラート条件 新規登録

デバイスグループ

必須

未選択です

デバイスシリーズ

必須

詳細名

必須

送信条件

必須

値

必須

監視間隔

必須

通知先

必須

新規登録

新規登録

※条件を登録しなかったら「新規登録」で各条件を登録してください。  
※「編集」で今選択されている条件の編集を行うことができます。

登録

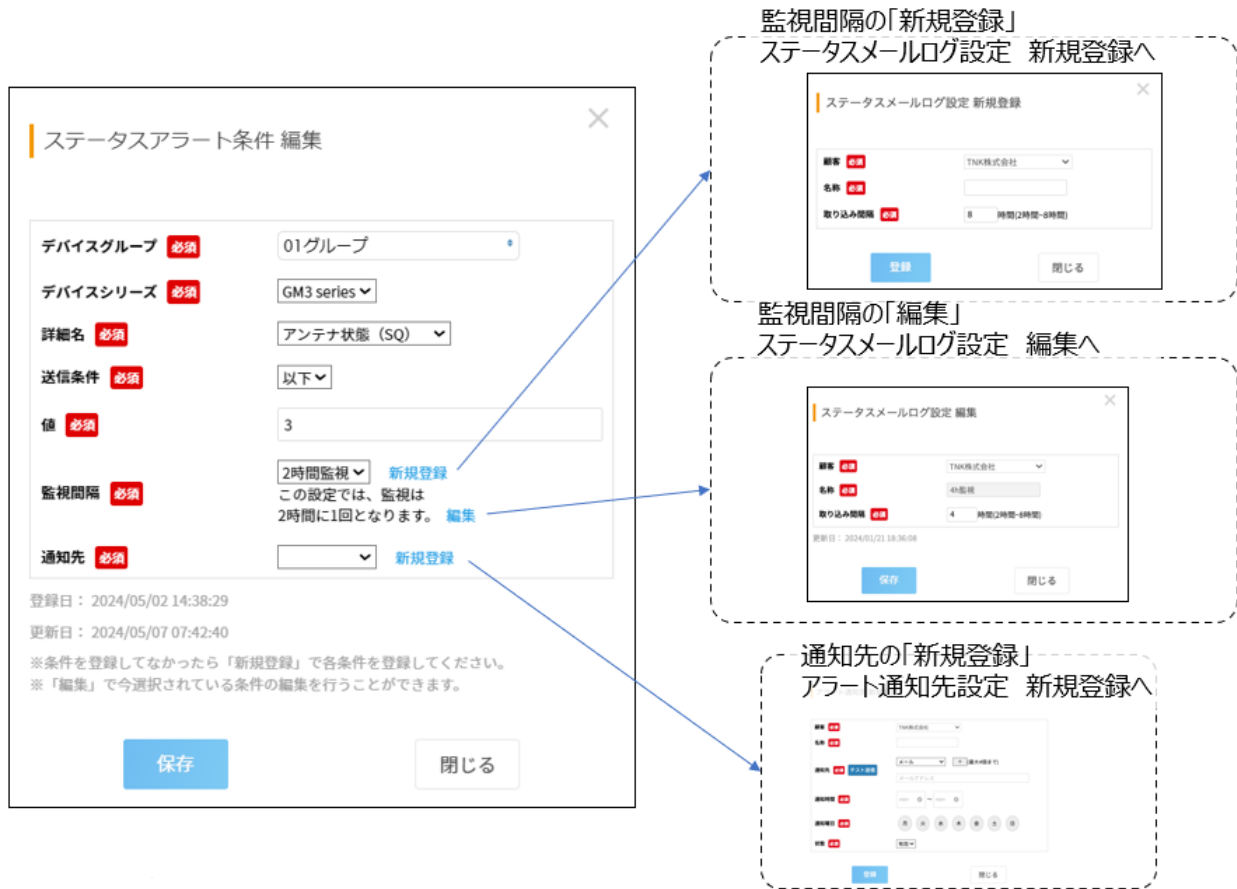
閉じる

デバイスグループ	デバイスグループを選択して下さい。 デバイスグループは重複して条件を設定することはできません。
デバイスシリーズ	使用するデバイスシリーズを選択して下さい。 (MR-GM3 series/MR-GM5 series) デバイスシリーズにより、詳細名の選択肢が変わります。
詳細名	詳細名(条件とするステータス名)を選択して下さい。
送信条件	ステータスアラート送信の条件を選択して下さい。 (値と一致・以上・以下)
値	ステータスアラート送信の条件の値を設定して下さい。
監視間隔	監視間隔(ステータスメールログ設定)を選択して下さい。
通知先	アラート通知先を選択して下さい。

「登録」ボタンを押して、保存して下さい。

ステータスアラート条件一覧に、登録した条件の情報があることを確認して下さい。

「ステータスアラート条件設定」画面と、他の設定との遷移関係は下図のようになります。



「ステータスアラート条件設定」画面から、「ステータスメールログ設定」の新規登録・編集、「アラート通知先設定」の新規登録が可能になっています。

4-6-2. 編集

編集するステータスアラート条件の「編集」ボタンをクリックして下さい。

×

ステータスアラート条件 編集

デバイスグループ 必須

01グループ

デバイスシリーズ 必須

GM3 series

詳細名 必須

アンテナ状態 (SQ)

送信条件 必須

以下

値 必須

3

監視間隔 必須

2時間監視

新規登録

この設定では、監視は2時間に1回となります。

編集

通知先 必須

警告通知先

新規登録

登録日：2024/05/02 14:38:29

更新日：2024/05/07 07:42:40

※条件を登録しなかったら「新規登録」で各条件を登録してください。

※「編集」で今選択されている条件の編集を行うことができます。

保存

閉じる

デバイスグループ	デバイスグループを選択して下さい。 デバイスグループは重複して条件を設定することはできません。
デバイスシリーズ	使用するデバイスシリーズを選択して下さい。 (MR-GM3 series/MR-GM5 series) デバイスシリーズにより、詳細名の選択肢が変わります。
詳細名	詳細名(条件とするステータス名)を選択して下さい。
送信条件	ステータスアラート送信の条件を設定して下さい。 (値と一致・以上・以下)
値	ステータスアラート送信の条件の値を設定して下さい。
監視間隔	監視間隔(ステータスメールログ設定)を選択して下さい。
通知先	アラート通知先を選択して下さい。

「保存」ボタンをクリックして下さい。ステータスアラート条件一覧に戻ります。



#### 4-6-3. 削除

削除するステータスアラート条件の「削除」をクリックして下さい。

×

ステータスアラート条件 削除

デバイスグループ

01グループ

デバイスシリーズ

GM3 series

詳細名

アンテナ状態 (SQ)

送信条件

以下

値

3

監視間隔

2時間監視

新規登録

この設定では、監視は2時間に1回となります。

編集

通知先

警告通知先

新規登録

登録日：2024/05/02 14:38:29

更新日：2024/05/07 07:42:40

※条件を登録しなかったら「新規登録」で各条件を登録してください。

※「編集」で今選択されている条件の編集を行うことができます。

削除

閉じる

削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、以下の確認メッセージが表示されます。

この設定を削除しますか？

OK

キャンセル

「OK」をクリックすると削除されます。「キャンセル」をクリックすると閉じます。

他のユーザーと共有しているグループがある場合は、削除できません。

他のユーザーが管理しているデバイスグループ(03:北関東グループ)がこの条件に紐づいています。他のデバイスグループの紐付けを解除してからでないと削除できません。あるいは管理者に削除してもらうようにしてください。

OK

## 4-7. HTTP 監視 URL 設定

「HTTP 監視 URL 設定」画面について説明します。  
ユーザーアカウントでログインすると、自社内で登録した HTTP 監視 URL が表示されます。

HTTP監視URL設定

検索条件

名称

検索

新規登録

HTTP監視URL一覧 1件

10 行ごとに表示

フィルター検索:

名称	デバイスシリーズ	URL	URLコピー	監視間隔	状態	操作
GM3/GM5用	MR-GM5/GM3 series	https://		5	有効	編集 削除

1件中 1 ～ 1 件目 表示

← 前

1

次 →

新規登録

### 画面の説明：サジェスト

#### サジェスト (ビジネスプランのみ)

HTTP 監視 URL を作成してから 1 日以上経過しても、死活監視アラート条件に紐づけられていない URL があった場合、メッセージが表示されます。(HTTP 監視 URL をデバイス側に設定しても、死活監視アラートに紐づいていないと HTTP 監視チェックは行われません。また HTTP 監視ログにも残りません。)

### 画面の説明：検索条件

名称

HTTP 監視の設定名称で検索します。

### 画面の説明：一覧

フィルター検索:

名称、URL、監視間隔、状態など一覧に表示されている項目の部分一致で絞り込みをかけられます。

名称

設定名称を表示します。

デバイスシリーズ

どのデバイスシリーズ用の URL かを表示します。

URL

HTTP 監視の URL を表示します。



URL をクリップボードにコピーします。

監視間隔

HTTP 監視の間隔(分単位)を表示します。

状態

設定の有効・無効を表示します。

編集

編集画面が開きます。

削除

削除画面が開きます。

新規登録

新規登録画面が開きます。

#### 4-7-1. 新規登録

「新規登録」ボタンをクリックして下さい。

HTTP監視URL 新規登録

名称 必須

デバイスシリーズ 必須

▼

送信プロトコル 必須

▼

HTTP監視URL 必須

自動発行

HTTP監視間隔 必須

デバイス側の発行間隔より長くしてください(1分~60分)

▼

状態 必須

有効▼

登録

閉じる

名称	この HTTP 監視 URL の名称を設定して下さい。 ここで設定した名称が、死活監視アラート条件で表示されます。
デバイスシリーズ	どのデバイスシリーズを対象とする HTTP 監視 URL か選択して下さい。
HTTP 監視 URL	(自動発行)
HTTP 監視間隔	HTTP 監視間隔を選択します。 ビジネスプラン=1 分~60 分で指定します。 スタンダードプラン=30 分固定です。
状態	有効/無効が選択できます。 状態を「無効」にすると、デバイスが URL に対して HTTP 回線監視を行なっても応答を返さなくなります。

「登録」ボタンを押して、保存して下さい。

HTTP 監視 URL 一覧に、登録した情報があることを確認して下さい。

<div>確認</div>	死活監視アラート通知の間隔は、HTTP 監視間隔の時間が適用されます。 例:HTTP 監視間隔を「30 分」で設定した場合、30 分間隔でアラート通知されます。
---------------	---

4-7-2. 編集

編集する HTTP 監視 URL の「編集」ボタンをクリックして下さい。

×

HTTP監視URL 編集

名称 必須

GM3/GM5用

デバイスシリーズ 必須

MR-GM5/GM3 series

送信プロトコル 必須

HTTPS

HTTP監視URL 必須

https://

HTTP監視間隔 必須

デバイス側の発行間隔より長くしてください(1分-60分)  
5分

状態 必須

有効

更新日：2024/09/12 18:48:13

保存

閉じる

名称	この HTTP 監視 URL の名称を設定して下さい。 ここで設定した名称が、死活監視アラート条件で表示されます。
デバイスシリーズ	編集不可です。
HTTP 監視 URL	編集不可です。
HTTP 監視間隔	HTTP 監視間隔を選択します。 ビジネスプラン=1 分～60 分で指定します。 スタンダードプラン=30 分固定です。
状態	有効/無効が選択できます。 状態を「無効」にすると、デバイスが URL に対して HTTP 回線監視を行なっても応答を返さなくなります。

「保存」ボタンをクリックして下さい。HTTP 監視 URL 一覧に戻ります。

状態を「無効」にするときに、すでに死活監視アラートの条件に紐づいている場合、

「死活監視アラート条件設定で、この URL を利用している条件があります。  
まず紐づきを解除してから無効、あるいは削除して下さい。」

と表示され、更新されません。まず、死活監視アラート条件から削除してから、「無効」にするようにして下さい。

#### 4-7-3. 削除

削除する HTTP 監視 URL の「削除」ボタンをクリックして下さい。

HTTP監視URL 削除

名称 GM3/GM5用

デバイスシリーズ MR-GM5/GM3 series ▼

送信プロトコル HTTPS ▼

HTTP監視URL https://

HTTP監視間隔 デバイス側の発行間隔より長くしてください(1分~60分)  
5分 ▼

状態 有効 ▼

更新日: 2024/09/12 18:48:13

削除 閉じる

削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、以下の確認メッセージが表示されます。

このHTTP監視用URLを削除しますか？

OK キャンセル

「OK」をクリックすると削除されます。「キャンセル」をクリックすると閉じます。

もし、削除しようとしている URL がまだ死活監視アラート条件のどれかに紐づいている場合、

「この HTTP 監視用 URL は死活監視アラート条件に設定されています。  
まず死活監視アラート条件から外してから、こちらを削除するようにして下さい。」

と表示され、削除することはできません。まず紐づけを解いてから削除するようにしましょう。

#### 4-8. ステータスメールログ設定

「ステータスメールログ設定」画面について説明します。

デバイスから送られてくるステータスメールログの取り込み間隔時間を設定して、ステータスアラート条件設定で指定します。  
ユーザーアカウントでログインすると、自社内で登録されたステータスメールログ設定が表示されます。

ステータスメールログ設定

検索条件

名称

検索

新規登録

ステータスメールログ一覧 2件

10 行ごとに表示

フィルター検索:

名称	取り込み間隔	操作
4h監視	4	編集 削除
2h監視	2	編集 削除

2件中 1 ～ 2 件目 表示

← 前

1

次 →

新規登録

画面の説明: サジェスト	
<p><b>サジェスト</b> (ビジネスプランのみ)</p>	<p>ステータスメールログの設定を登録してから 1 日以上経過しても、死活監視アラート条件にもステータスアラート条件にも紐づけられていない設定があった場合にメッセージが表示されます。(ステータスアラート条件に紐づけられないとメールの取り込みは行われません。またステータスメールログにも残りません。)</p>

画面の説明: 検索条件	
<p>名称</p>	<p>ステータスメールログ名称を指定します。 「検索」ボタンをクリックすると、絞り込まれます。</p>

画面の説明: 一覧	
<p>フィルター検索:</p>	<p>名称、取り込み間隔、状態など一覧に表示されている項目の部分一致で絞り込みをかけられます。</p>
<p>名称</p>	<p>設定名称を表示します。</p>
<p>取り込み間隔</p>	<p>ステータスメールの取り込み間隔(時間単位)を表示します。</p>
<p>編集</p>	<p>編集画面が開きます。</p>
<p>削除</p>	<p>削除画面が開きます。</p>
<p>新規登録</p>	<p>新規登録画面が開きます。</p>

#### 4-8-1. 新規登録

「新規登録」ボタンをクリックして下さい。

×

ステータスメールログ設定 新規登録

名称 **必須**

取り込み間隔 **必須**

時間(2時間~8時間)

登録

閉じる

名称	ステータスメールログ設定の名称を設定して下さい。
取り込み間隔	デバイスからのステータスメールログの取り込み間隔を指定して下さい。この間隔時間はデバイス側のメール送信設定の送信間隔と合わせるようにして下さい。

「登録」ボタンをクリックして下さい。ステータスメールログ一覧に戻ります。  
ステータスメールログ一覧に、登録した情報があることを確認して下さい。

<div>確認</div>	ステータスアラート通知の間隔は、取り込み間隔の時間が適用されます。 例: 取り込み間隔を「2 時間」で設定した場合、2 時間間隔でアラート通知されます。
---------------	---

4-8-2. 編集

編集するステータスメールログ設定の「編集」ボタンをクリックして下さい。

×

ステータスメールログ設定 編集

名称 必須

4h監視

取り込み間隔 必須

4 時間(2時間~8時間)

更新日：2024/01/21 18:36:08

保存

閉じる

名称	このステータスメールログ設定の名称を設定して下さい。
取り込み間隔	デバイスからのステータスメールログの取り込み間隔を設定して下さい。この間隔時間はデバイス側のメール送信設定の送信間隔と合わせるようにして下さい。

「保存」ボタンをクリックして下さい。ステータスメールログ一覧に戻ります。



#### 4-8-3. 削除

削除するステータスログ設定の「削除」ボタンをクリックして下さい。



ステータスメールログ設定 削除

名称 4h監視

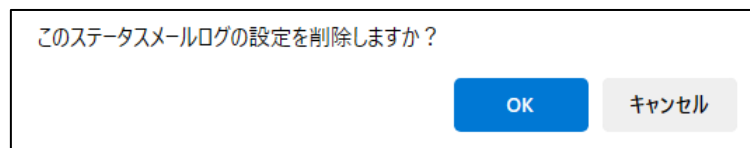
取り込み間隔 4 時間(2時間~8時間)

更新日：2024/01/21 18:36:08

削除 閉じる

削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、以下の確認メッセージが表示されます。



このステータスメールログの設定を削除しますか？

OK キャンセル

「OK」をクリックすると削除されます。「キャンセル」をクリックすると閉じます。

もし、削除しようとしているステータスメールログ設定がまだ死活監視アラート条件かステータスアラート条件のどれかに紐づいている場合、

「このステータスメールログは死活監視アラート条件に設定されています。  
まず死活監視アラート条件から外してから、こちらを削除するようにして下さい。」

と表示され、削除することはできません。まず紐づけを解いてから削除するようにしましょう。

#### 4-9. アラート通知先設定

「アラート通知先設定」画面について説明します。

アラート条件が合致した場合に、アラート通知を送る宛先についての情報を登録します。

ユーザーアカウントでログインすると、自社内で登録されたアラート通知先が表示されます。

アラート通知先設定

検索条件

通知先名

検索

新規登録

アラート通知先一覧 2件

10 行ごとに表示

フィルター検索:

通知先名	通知先	通知時間	通知曜日	状態	操作
警告の時の通知先	メール/chatwork/ slack/Teams	00:00~23:59	月/火/水/木/金/土/日	有効	<div>編集</div> <div>削除</div>
緊急時	メール/chatwork	00:00~23:59	月/火/水/木/金/土/日	有効	<div>編集</div> <div>削除</div>

2件中 1 ~ 2 件目 表示

← 前

1

次 →

新規登録

##### 画面の説明: サジェスト

<p>サジェスト (ビジネスプランのみ)</p>	アラート通知先を作成してから 1 日以上経過しても、死活監視アラート条件にも、ステータスアラート条件にも紐づけられていない設定があった場合、メッセージが表示されます。
------------------------------	---

##### 画面の説明: 検索条件

<p>通知先名</p>	アラート通知先名を指定します。
-------------	-----------------

##### 画面の説明: 一覧

<p>フィルター検索:</p>	通知先名、通知先、通知時間、通知曜日、状態など一覧に表示されている項目の部分一致で絞り込みをかけられます。
通知先名	通知先の設定名を表示します。
通知先	通知先の種別を表示します。
通知時間	通知する時間帯を表示します。
通知曜日	通知する曜日を表示します。
状態	設定の有効・無効を表示します。
<div>編集</div>	編集画面が開きます。
<div>削除</div>	削除画面が開きます。
<div> <div>+</div> 新規登録 </div>	新規登録画面が開きます。

#### 4-9-1. 新規登録

「新規登録」ボタンをクリックして下さい。



The form is titled "アラート通知先 新規登録" (Alert Notification Destination New Registration). It contains the following fields and controls:

- 通知先名 必須** (Notification Name Required): A text input field.
- 通知先 必須** (Notification Destination Required): A dropdown menu with "メール" (Email) selected, followed by a "+" button and the text "(最大4個まで)" (Up to 4 maximum).
- メールアドレス** (Email Address): A text input field.
- 通知時間 必須** (Notification Time Required): Two time selection fields separated by a tilde (~), each with a clock icon.
- 通知曜日 必須** (Notification Day of Week Required): Seven circular buttons for days of the week: 月 (Monday), 火 (Tuesday), 水 (Wednesday), 木 (Thursday), 金 (Friday), 土 (Saturday), 日 (Sunday).
- 状態 必須** (Status Required): A dropdown menu with "有効" (Valid) selected.

At the bottom, there are two buttons: "登録" (Register) in blue and "閉じる" (Close) in white.

<b>通知先名</b>	アラート通知先設定の名称を設定して下さい。
<b>通知先</b>	メール/slack/chat work/teams から選択します。 ビジネスプランの場合、「+」ボタンを押すことで最大 4 つまで通知先を増やすことができます。
<b>通知時間</b>	ここで指定した時間内のみアラート通知を送信します。 0:00 をまたいだ設定を行った場合動作しません。 0:00～23:59 で一日となります。
<b>通知曜日</b>	ここで指定した曜日のみアラート通知を送信します。
<b>状態</b>	有効/無効が選択できます。 状態を「無効」にすると、アラート通知を行いません。

「登録」ボタンをクリックして下さい。アラート通知先一覧に戻ります。

通知先について	
メール	メールアドレスを設定して下さい。
slack	「Incomming WebHook」の URL と、「channel」を設定して下さい。
chatwork	「API token」と「room id」を設定して下さい。
teams	「Incomming WebHook」の URL を設定して下さい。

4-9-2. 編集

編集するアラート通知先の「編集」ボタンをクリックして下さい。

アラート通知先 編集

通知先名 必須

緊急時

メール

+

最大4個まで

taro.tanaka@network.net

通知先 必須

テスト送信

chatwork

-

f772d129ac5de9183d2f33333333333

3433533333

通知時間 必須

00:00

~

23:59

通知曜日 必須

月

火

水

木

金

土

日

状態 必須

有効

更新日：2024/01/03 19:07:57

保存

閉じる

通知先名	アラート通知先設定の名称を設定して下さい。
通知先	メール/slack/chat work/teams から選択します。 ビジネスプランの場合、「+」ボタンを押すことで最大 4 つまで通知先を増やすことができます。
通知時間	ここで指定した時間内にしか通知は送られません。 0:00 をまたいだ設定を行った場合、動作しません。0:00～23:59 で一日となります。
通知曜日	ここで指定した曜日にしか通知は送られません。
状態	有効/無効が選択できます。

「保存」ボタンをクリックして下さい。アラート通知先一覧に戻ります。

状態を「無効」にする場合、すでに死活監視アラートかステータスアラートの条件に紐づいていると、

「このアラート通知先は死活監視アラート条件に設定されています。  
まず死活監視アラート条件から外してから、こちらを削除するようにして下さい。」

と表示され、更新されません。まず、アラート条件から削除してから、「無効」に変更して下さい。

#### 4-9-3. 削除

削除するアラート通知先の「削除」ボタンをクリックして下さい。

アラート通知先 削除

通知先名 緊急時

メール (最大4個まで)

taro.tanaka@network.net

通知先 テスト送信 chatwork

f772d129ac5de9183d2f6f33333333333

343353333

通知時間 00:00 ~ 23:59

通知曜日 月 火 水 木 金 土 日

状態 有効

更新日: 2024/01/03 19:07:57

削除 閉じる

削除しない場合は「閉じる」ボタンをクリックして下さい。

「削除」ボタンをクリックすると、以下の確認メッセージが表示されます。

このアラート通知先を削除しますか?

OK キャンセル

「OK」をクリックすると削除されます。「キャンセル」をクリックすると閉じます。

もし、削除しようとしているアラート通知先がまだ死活監視アラート条件、ステータスアラート条件のどれかに紐づいている場合、

「このアラート通知先は死活監視アラート条件に設定されています。  
まず死活監視アラート条件から外してから、こちらを削除するようにして下さい。」

と表示され、削除することはできません。まず紐づけを解いてから削除するようにしましょう。

4-10. 死活監視アラートログ

「死活監視アラートログ」画面について説明します。  
死活監視で警告状態、停止状態を検知してアラートを送った履歴を閲覧することができます。  
ユーザーアカウントでログインすると、自分が管理するデバイスグループ分のログが表示されます。

確認

死活監視アラート通知の間隔は、HTTP 監視 URL 設定の HTTP 監視間隔の時間が適用されます。  
例: HTTP 監視間隔を「30 分」で設定した場合、30 分間隔でアラート通知されます。

死活監視アラートログ

検索条件

デバイスグループ

機種

機器名称

通知先

アラート送信日

検索

死活監視アラート一覧 3件

10

行ごとに表示

フィルター検索:

エクスポート

送信日時	デバイスグループ	機種	機器名称	アラートタイプ	通知先	アラート内容
2024/03/18 16:06:31	01グループ	MR-GM3-M	海岸ビルA棟9F	HTTP監視	警告の時の通知先	<a href="#">詳細</a>
2024/03/17 19:58:32	01グループ	MR-GM3-M	海岸ビルA棟9F	HTTP監視	緊急時	<a href="#">詳細</a>
2024/03/17 19:53:31	01グループ	MR-GM3-M	海岸ビルA棟9F	HTTP監視	警告の時の通知先	<a href="#">詳細</a>

3件中 1 ~ 3 件目 表示



← 前


1

次 →

画面の説明: 検索条件

デバイスグループ	デバイスグループを選択します。
機種	機種を選択します。
機器名称	機器名称を指定します。
通知先	通知先を指定します。
アラート送信日	アラート送信日を指定します。

画面の説明:一覧	
フィルター検索: <input type="text"/>	送信日時、デバイスグループ、機種、機器名称、アラートタイプ、通知先など一覧に表示されている項目の部分一致で絞り込みをかけられます。
送信日時	アラート通知を送信した日時を表示します。
デバイスグループ	デバイスグループ名を表示します。
機種	機種名を表示します。
機器名称	機器名称を表示します。
アラートタイプ	死活監視のタイプを表示します。 HTTP 監視: HTTP 通信に死活監視 メール監視: メールによる死活監視
通知先	アラートを送信したアラート通知先設定名を表示します。
	アラート内容の詳細画面が開きます。
 エクスポート	現在画面に表示されている内容が CSV でエクスポートされます。 ビジネスプランのみの機能となります。

	死活監視アラート通知の間隔は、HTTP 監視 URL 設定の HTTP 監視間隔の時間が適用されます。 例: HTTP 監視間隔を「30 分」で設定した場合、30 分間隔でアラート通知されます。
---	--

4-10-1. 詳細

該当アラートログの「詳細」ボタンをクリックして下さい。

詳細

項目	内容
アラート種別	警告
対象デバイス	海岸ビルA棟9F
アラート送信日時	2024/03/18 16:06:31
アラート通知先	警告の時の通知先

送信日時：2024/03/18 16:06:31

閉じる

アラート種別	警告 or 停止が表示されます。
対象デバイス	機器名称を表示します。
アラート送信日時	アラート送信日時が表示されます。
アラート通知先	アラートを送信したアラート通知先設定名を表示します。

「閉じる」ボタンをクリックして下さい。死活監視アラート一覧に戻ります。



4-11. ステータスアラートログ

「ステータスアラートログ」画面について説明します。  
ステータス監視で設定されている条件と合致した場合に送られるアラートの履歴を閲覧することができます。  
ユーザーアカウントでログインすると、自分が管理するデバイスグループ分のログのみが表示されます。

確認

ステータスアラート通知の間隔は、ステータスメールログ設定の「取り込み間隔」の時間が適用されます。  
例: 取り込み間隔を「2 時間」で設定した場合、2 時間間隔でアラート通知されます。

ステータスアラートログ

検索条件

デバイスグループ

機種

機器名称

通知先

詳細名

アラート送信日

アラートメール本文

検索

ステータスアラート一覧 0件

10

行ごとに表示

フィルター検索:

エクスポート



送信日時	デバイスグループ	機種	機器名称	詳細名	メール件名	メール内容
データがありません						

0件 表示

← 前

次 →

画面の説明: 検索条件	
デバイスグループ	デバイスグループを選択します。
機種	機種を選択します。
機器名称	機器名称を指定します。
通知先	通知先を選択します。
詳細名	詳細名を選択します。
アラート送信日	アラート送信日を指定します。
アラートメール本文:	アラートメール本文中の文字列を指定します。 SQ に関するアラートメールだけを抽出する場合などには、SQ と指定して下さい

画面の説明：一覧	
フィルター検索: <input type="text"/>	送信日時、デバイスグループ、機種、機器名称、詳細名、メール件名など一覧に表示されている項目の部分一致で絞り込みをかけられます。
送信日時	アラート通知を送信した日時を表示します。
デバイスグループ	デバイスグループ名を表示します。
機種	機種名を表示します。
機器名称	機器名称を表示します。
詳細名	アラートの詳細名(キー)を表示します。
メール件名	アラートの件名を表示します。
	詳細画面が開きます。
 エクスポート	現在画面に表示されている内容が CSV でエクスポートされます。 ビジネスプランのみの機能となります。

#### 4-11-1. 詳細

該当アラートログの「詳細」ボタンをクリックして下さい。

アラート通知履歴 詳細

アラート件名

【MRL-IDM】ステータスアラート通知

本文

MR-GM3LTE1Fのステータスチェックで、  
メール送信のトリガー(Trigger)が指定された値「WAN interface Active」一致になりました。  
Trigger : WAN interface Active

送信日時 : 2024/05/08 12:41:02

閉じる

通知先に送信された内容が表示されます。

「閉じる」ボタンをクリックして下さい。ステータスアラート一覧に戻ります。

## 4-12. HTTP 監視ログ

「HTTP 監視ログ」画面について説明します。

デバイスから HTTP 監視用 URL をコールした履歴を閲覧することができます。

ユーザーアカウントでログインすると、自分が管理するデバイスグループ分のログのみが表示されます。



HTTP 監視ログは、直近 3 時間のログは全て表示されます。  
3 時間以上経過したログは「1 時間ごと、または IP アドレスが変化した前後のログ」のみが表示されます。  
送信元 IP アドレスが変化したログは色違いで表示されます。

HTTP監視ログ

検索条件

設置場所

デバイスグループ

機種

機器名称

S/N

IPアドレス

MACアドレス

期間

～

検索

HTTP監視ログ一覧 107件

10 行ごとに表示

フィルター検索:

エクスポート

登録日時	設置場所	デバイスグループ	機種	機器名称	S/N	IPアドレス	MACアドレス	ログ種別
2024/03/20 18:10:39	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 18:05:34	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 18:00:29	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:55:24	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:50:19	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:45:14	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:40:09	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視
2024/03/20 17:35:04	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM-		00:10:38:	HTTP監視

107件中 1 ～ 10 件目 表示

← 前

1

2

3

4

5

次 →

画面の説明: 検索条件	
設置場所	設置場所を指定します。
デバイスグループ	デバイスグループを選択します。
機種	機種を選択します。
機器名称	機器名称を指定します。
S/N	シリアル No を指定します。
IPアドレス	IP アドレスを指定します。
MACアドレス	MAC アドレスを指定します。
期間	ログの期間を指定します。

画面の説明:一覧	
フィルター検索: <input type="text"/>	登録日時、設置場所、デバイスグループ、機種、機器名称、S/N、IP アドレス、MAC アドレス、ログ種別など一覧に表示されている項目の部分一致で絞り込みをかけられます。
受信日時	HTTP 監視通信を受信した日時を表示します。
設置場所	デバイス登録時に設定した設置場所を表示します。
デバイスグループ	デバイスグループを表示します。
機種	機種名を表示します。 ステータスメールを受信していない場合、空欄になります。
機器名称	デバイス登録時に設定した機器名称を表示します。
S/N	デバイス登録時に設定したシリアル No が表示されます。
IP アドレス	HTTP 監視通信の送信元 IP アドレスを表示します。
MAC アドレス	デバイス登録時に設定した MAC アドレスが表示されます。
ログ種別	「HTTP 監視」と表示されます。
<div>↓ エクスポート</div>	現在画面に表示されている内容が CSV でエクスポートされます ビジネスプランのみの機能となります。

4-13. ステータスメールログ

「ステータスメールログ」画面について説明します。  
デバイスから送られてきたステータスメールログを取り込んで解析したものが保存されており、ログ保存期間中に閲覧することができます。  
ユーザーアカウントでログインすると、自分が管理するデバイスグループ分のログのみが表示されます。

ステータスメールログ

検索条件

設置場所

デバイスグループ

機種

機器名称

S/N

IPアドレス

MACアドレス

期間

メール送信のトリガー

検索

ステータスメールログ一覧 229件


10 行ごとに表示

フィルター検索:

登録日時	設置場所	デバイスグループ	機種	機器名称	S/N	IPアドレス	MACアドレス	ログ種別	メール受信日時	ログ内容
2024/09/12 17:54:04	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 16:28:14	<a href="#">詳細</a>
2024/09/12 15:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 14:27:00	<a href="#">詳細</a>
2024/09/12 13:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 12:25:46	<a href="#">詳細</a>
2024/09/12 11:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 10:24:32	<a href="#">詳細</a>
2024/09/12 11:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 08:23:23	<a href="#">詳細</a>
2024/09/12 09:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 08:23:25	<a href="#">詳細</a>
2024/09/12 07:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 07:33:44	<a href="#">詳細</a>
2024/09/12 05:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 05:32:30	<a href="#">詳細</a>
2024/09/12 03:54:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 03:31:17	<a href="#">詳細</a>
2024/09/12 01:53:03	海岸ビル 1F	01:南関東グループ	MR-GM3-M	GM3-M(test)		192.168.1.100	00:10:38:37:75:A0	メール	2024/09/12 01:30:03	<a href="#">詳細</a>

エクスポート

画面の説明: 検索条件	
設置場所	設置場所を指定します。
デバイスグループ	デバイスグループを選択します。
機種	機種を選択します。
機器名称	機器名称を指定します。
S/N	シリアル No を指定します。
IPアドレス	IP アドレスを指定します。
MACアドレス	MAC アドレスを指定します。
期間	ログの期間を指定します。
メール送信のトリガー	メール送信のトリガーを指定します。 例えば Smtplexec Power on Started を指定して、起動時のメールログのみ抽出する等ができます。

画面の説明:一覧	
フィルター検索: <input type="text"/>	登録日時、設置場所、デバイスグループ、機種、機器名称、S/N、IP アドレス、MAC アドレス、ログ種別など一覧に表示されている項目の部分一致で絞り込みをかけられます。
登録日時	ステータスメールログを登録した日時を表示します。 ステータスメールログ設定で設定した時間の間隔で登録されます。 例:2 時間で設定した場合、2 時間間隔で登録されます。
設置場所	デバイス登録時に設定した設置場所を表示します。
デバイスグループ	デバイスグループを表示します。
機種	機種名を表示します。
機器名称	デバイス登録時に設定した機器名称を表示します。
S/N	デバイス登録時に設定したシリアル No が表示されます。
IP アドレス	デバイスの WAN 側 IP アドレスを表示します。
MAC アドレス	デバイス登録時に設定した MAC アドレスが表示されます。
ログ種別	「メール」と表示されます。
メール受信日時	MRL-IDM がメールを受信した日時を表示します。
<div>詳細</div>	詳細画面が開きます。
<div>            エクスポート         </div>	現在画面に表示されている内容が CSV でエクスポートされます ビジネスプランのみの機能となります。

#### 4-13-1. 詳細

該当ログの「詳細」ボタンをクリックして下さい。  
デバイスから送られてきたステータスメールの内容を解析して表示します。

詳細

メールデータ  
メール受信日時:2024/05/09 17:46:23

メール送信のトリガー	Periodical
起動経過時間	1days:2:6:8s
ファームウェアバージョン	v1.04.02(MR001)
ファームウェアビルド日時	Tue Oct 24 17:39:22 JST 2023
コンフィグバージョン	Default:22 Current:22
システム負荷	0.00 0.00 0.00 1/37
RAM使用量	17312 KB / 114064 KB
ROM使用量	mtd1: 3512 KB / 10240 KB
機種名	MR-GM3-DKS
装置名称	MR-GM3
NTPクライアントの同期状態	Synchronized

WAN情報(GM3)

WAN接続モード	Mobile Card(Built-in MODULE)
SIMカードの電話番号	
内蔵通信モジュールの端末識別番号	
LTE通信網の圏内・圏外 (1=圏内、0=圏外)	1
アンテナ状態 (0~4)	4
受信信号強度	-51dBm
LTEの周波数帯 (LTE frequency band)	100
内蔵通信モジュールのバージョン	11-18
モジュールキャリア選択値	0,2
WAN側IPアドレス	

WLAN情報(GM3)

無線LAN1のSSID	MR-GM3 5G
無線LAN1の動作モード	AP
無線LAN1の周波数	5 GHz (A+N+AC)
無線LAN1のチャンネル番号	36
無線LAN1の暗号モード	WPA2 Mixed
無線LAN1のBSSID	00:10:38:
無線LAN1のクライアント数	0
無線LAN2のSSID	MR-GM3 2.4G
無線LAN2の動作モード	AP
無線LAN2の周波数	2.4 GHz (B+G+N)
無線LAN2のチャンネル番号	6
無線LAN2の暗号モード	WPA2 Mixed
無線LAN2のBSSID	00:10:38:
無線LAN2のクライアント数	0

LAN情報(GM3)

LANポートIPアドレス	192.168.0.1
LANポートサブネットマスク	255.255.255.0
LANポートMACアドレス	00:10:38:
DHCPサーバーの状態 (Active=有効、Inactive=無効)	Active
eth0ポートのリンク状態	Link Up
DDNSのドメイン名	

登録日時: 2024/05/09 18:49:02

閉じる

「閉じる」ボタンをクリックして下さい。ステータスメールログ一覧に戻ります。



4-14. デバイスオペレーションログ

デバイスオペレーションログメニューでは、デバイスに対して MRL-IDM 上から行った操作、WEB 通信で遠隔からデバイスの設定などのログを閲覧することができます。

確認

デバイスオペレーションログが保存されるのは、MR-GM3 シリーズ、MR-GM3L シリーズのみです。

ユーザーアカウントでログインすると、自分が管理するデバイスグループ分の一覧が表示されます。

デバイスオペレーションログ

検索条件

設置場所

デバイスグループ

機種

機種名称

S/N

IPアドレス

MACアドレス

期間

検索

デバイスオペレーションログ一覧 5件

10 行ごとに表示

フィルター検索:

登録日時	設置場所	デバイスグループ	機種	機種名称	S/N	IPアドレス	MACアドレス	ログ種別	ログ内容
2024/03/18 18:46:34	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM30		00:10:38:	WEB通信	詳細
2024/03/15 15:49:26	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM30		00:10:38:	WEB通信	詳細
2024/03/15 15:37:57	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM30		00:10:38:	WEB通信	詳細
2024/03/15 15:37:37	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM30		00:10:38:	WEB通信	詳細
2024/03/15 15:36:26	海岸ビル9F	01グループ	MR-GM3-M	海岸ビルA棟9F	GM30		00:10:38:	WEB通信	詳細



5件中 1 ~ 5 件目 表示

← 前

1

次 →

画面の説明: 検索条件	
設置場所	設置場所を指定します。
デバイスグループ	デバイスグループを選択します。
機種	機種を選択します。
機種名称	機器名称を指定します。
S/N	シリアル No を指定します。
IPアドレス	IP アドレスを指定します。
MACアドレス	MAC アドレスを指定します。
期間	ログの期間を指定します。

画面の説明:一覧	
フィルター検索: <input type="text"/>	操作日時、設置場所、デバイスグループ、機種、機器名称、S/N、IP アドレス、MAC アドレス、ログ種別など一覧に表示されている項目の部分一致で絞り込みをかけられます。
操作日時	操作した日時を表示します。
設置場所	デバイス登録時に設定した設置場所を表示します。
デバイスグループ	デバイスグループを表示します。
機種	機種名を表示します。
機器名称	デバイス登録時に設定した機器名称を表示します。
S/N	デバイス登録時に設定したシリアル No が表示されます。
IP アドレス	デバイスの WAN 側 IP アドレスを表示します。
MAC アドレス	デバイス登録時に設定した MAC アドレスが表示されます。
ログ種別	「WEB 通信」と表示されます。
	詳細画面が開きます。
 エクスポート	現在画面に表示されている内容が CSV でエクスポートされます ビジネスプランのみの機能となります。

#### 4-14-1. 詳細

該当ログの「詳細」ボタンをクリックして下さい。



デバイスに対して行った操作「WEB 通信」のログの内容が表示されます。  
「閉じる」ボタンをクリックして下さい。デバイスオペレーションログ一覧に戻ります。

## 5. MRL-IDM に関するお問い合わせ

MRL-IDM に関するお問い合わせは、サポート直通電話番号にお電話下さい。



お問い合わせ頂く前に、サポート規定をご確認下さい。

MRL 製品サポート規定 <https://www.mrl.co.jp/supports/support-policy/>

### 株式会社マイクロリサーチ ユーザーサポートセンター

■サポート直通電話番号: 03-3458-9031

土日、祝日を除く 10:00～12:00、13:00～17:00

■サポート直通 FAX 番号: 03-3458-9030

■インターネットホームページ

URL : <https://www.MRL.co.jp> (トップページ)

当社からのお知らせ、最新情報の提供を行なっています。

### お問い合わせいただく際のお願い

お電話でお問い合わせいただく際に、弊社から本人確認をさせていただきます。

・管理者名、ユーザー名、住所、MRL-IDM のログイン ID

をご準備下さい。

お問い合わせいただく際に必要な情報：

- ◆登録されている企業名（ユーザー名）
- ◆登録されている住所
- ◆MRL-IDM のログイン ID
- ◆お問い合わせ内容

