SUNCORPORATION

デュアル SIM 対応ルータ

Rooster DRX

AdvancedWeb 設定機能説明書

第 3.2.0 版

本書では、DRX をアドバンストモード時における WebUI の操作方法について記載しております。
対象バージョンファームウェアバージョン：Version 3.2.0 以降

はじめに

本書は、DRX シリーズ共通です。お買い上げ頂いた機種と各コマンドの対応関係は、下記の機種マークで表しております。

DRX5510 DRX5010 DRX5002

機種マークが記載している機種のみ そのコマンドに対応しております。
機種マークが記載していない機能は、全機種で対応しております。
ご確認の上ご使用ください。

目次

1章　アドバンストWeb設定の導入

パソコンから DRX に接続して、アドバンスト Web 設定ツールの表示やパスワード変更などの初期設定をするまでの手順を説明します。

> 工場出荷状態ではシンプルモードで起動しますのでアドバンストモードに切り替えてください。切り替え方法については『RoosterDRX 取扱説明書』Web サービス 項目を参照ください。

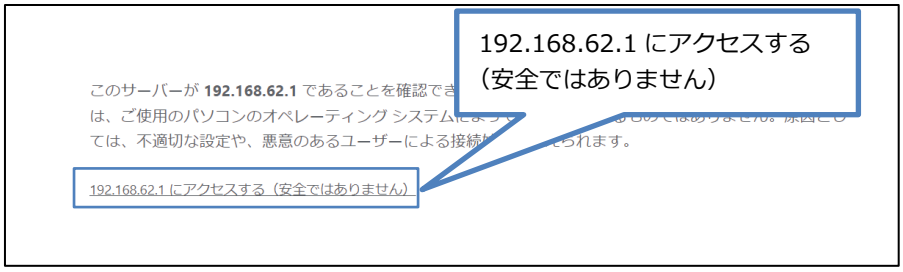
1-1. アドバンストWeb設定ツールへのログイン方法

1．　WWW ブラウザを起動します。

2．　WWW ブラウザのアドレス入力欄に、DRX の LAN 側 IP アドレス「https://192.168.62.1/」（工場出荷時状態）を入力し、Enter キーを押します。

3．　SSL の警告ページが表示されますので、「詳細設定」をクリックします。

4．「192.168.62.1 にアクセスする。(安全ではありません)」をクリックします。



・SSL 警告ページはローカル環境で暗号化通信を可能にするためにローカル SSL サーバ証明書を使っており、それによる警告であり、http 通信に比べ、セキュリティは頑丈になります。
・SSL 警告ページはブラウザ、ブラウザのバージョンによって異なっています。

5．Web 設定ツールのログインページが表示されます。ユーザー名に「root」、パスワードに「root」（工場出荷時状態）を入力します。

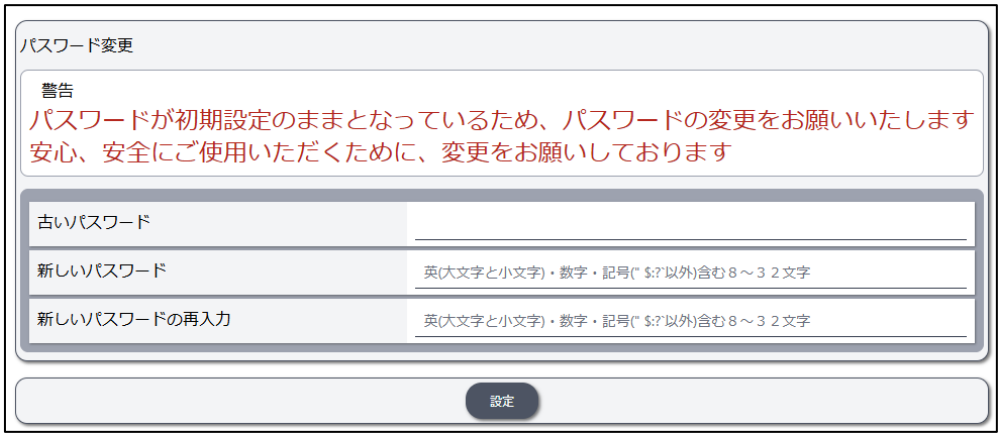
一定時間内に連続でユーザー名、もしくはパスワードを間違えてログイン操作を繰り返した場合以下の表示となり、一定時間ログインできなくなります。

アカウントがロックされています
しばらく時間をおいてからログインしてください

上記表示となった場合、しばらく待ってから WWW ブラウザの画面更新を行い再度正しいユーザー名、パスワードでログイン操作をしてください。

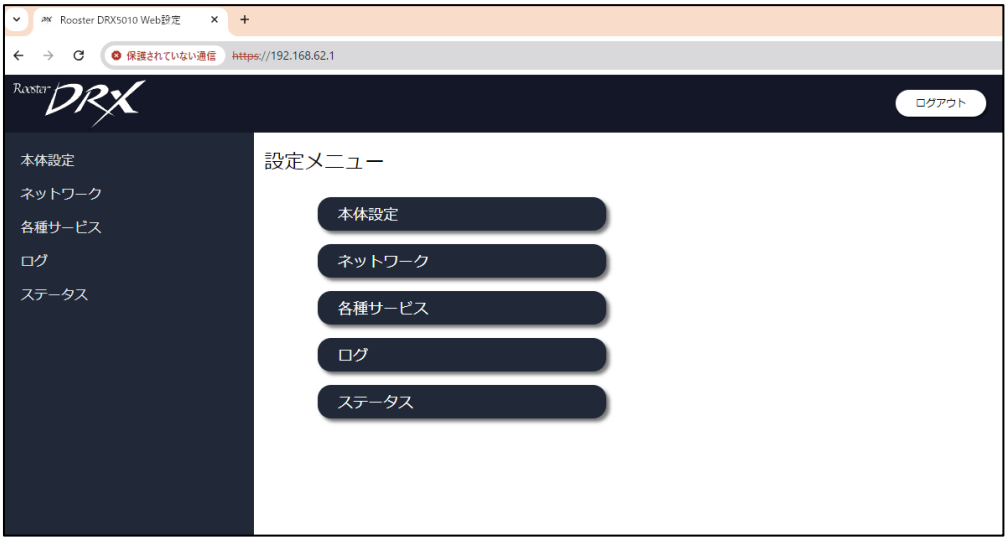
6．ユーザー名、パスワード入力した後、［ログイン］ボタンをクリックもしくは［ENTER］キーを押します。

7．　パスワードを工場出荷状態の設定から変更していない場合、パスワード変更画面が表示されます。
新しいパスワードを英(大文字と小文字)・数字・記号(" $:?`以外)含む８～32 文字で設定して「変更」をクリックします。
パスワードを変更した場合、ログインページが表示されます。
新しく設定したパスワードで再度ログインします。



設定ツールの初期パスワードはログイン時に必ず変更してください。
その際、英(大文字と小文字)・数字・記号(" $:?`以外)含む８～32 文字にしてください。
上記のパスワード変更画面以外のパスワードの変更方法、及びパスワード変更に関する注意事項は、RoosterDRX_取扱説明書『2-7.入力できない記号一覧』をご覧ください。

8．　DRX のアドバンスト Web 設定ツールが表示されます。



memo
- ブラウザのタブには「Rooster DRX5510」「Rooster DRX5010」「Rooster DRX5002」と表示されており、接続している機種が判別できます。

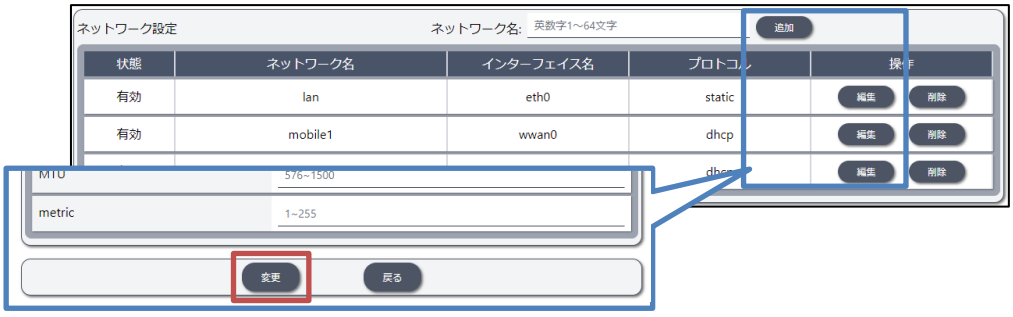
・ログイン後、無通信状態で「２時間１５分」が過ぎるとセッションが切れます。
・DRX と通信を行うとセッションタイムはリセットされます。
・セッションが切れてから通信を再開するとログイン画面へ移動し、再ログインが必要になります。

1-2. ［変更］、［設定］ボタンの違い

memo
- 変更：設定画面上のみ一時的な変更をします。
- 設定：変更内容を不揮発性メモリに保存し、設定を適用動作します。

1-2-1.　[変更]ボタンについて

1．　リスト画面にて［追加］もしくは［編集］で表示される詳細設定ページにて［変更］ボタンが確認できます。



2．　詳細設定画面で内容を記入し、［変更］ボタン押下で一時的に保存されます。

1-2-2.　[設定]ボタンについて

1．　［設定］ボタンは「設定の保存」、「一時保存の本体への反映」「設定の本体への反映」が行われ、設定内容が動作するようになります。

- ［変更］は一時保存のみで「設定の保存」「設定の本体への反映」は行われません。
- ［変更］ボタンで一時保存された設定はページ移動では消えませんが、DRX 本体を再起動すると設定は消えます。
- ［変更］ボタン押下後は、必ず［設定］ボタンを押して設定を反映させてください。

1-3. 入力できる文字

入力できる文字は特に記載がない限り 半角文字のみとなります。マルチバイト文字（日本語など）は入力できません。

日本語文字が入力できる記載のある項目は日本語文字のみ入力できます。日本語以外の言語、ダイアクリティカルマーク　は入力できません。

2章　本体設定

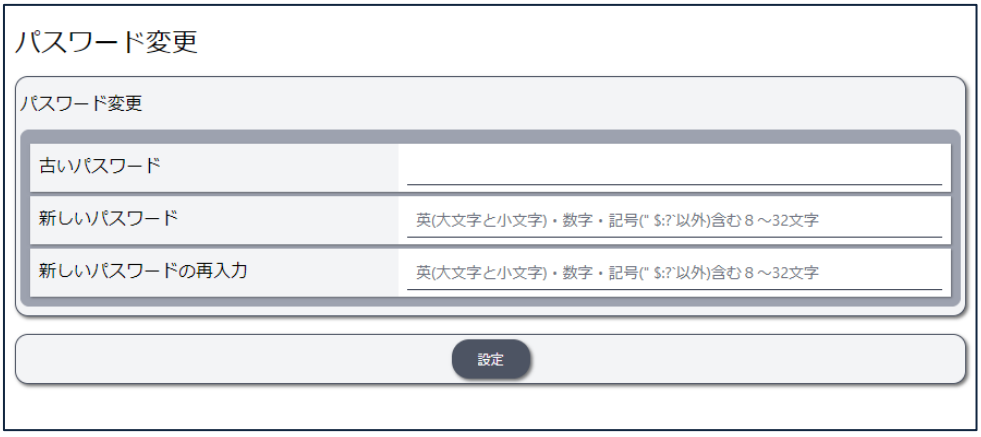
この章では、DRX に設定した情報の保存・読込方法、ファームウェアのアップデート、時刻制御、診断情報などについて説明します。

2-1. パスワード変更

現在ログインしているアカウントのログインパスワードを変更する場合に設定を行います。

工場出荷時状態のパスワードは「root」に設定されています。（管理者アカウントの場合）

1．　設定ツールのメニューから、［本体設定］－［パスワード変更］をクリックします。
「パスワードの変更」ページが表示されます。



2．　［古いパスワード］に、現在使用しているパスワードを入力します。

3．　新しいパスワード］に、新しく設定するパスワードを入力します。

4．　［再入力］に、［新しいパスワード］に入力したパスワードを再度入力します。

5．　［設定］ボタンをクリックして、設定を反映させます。

6．　設定の反映後、ログインページへ移動します。
新しく設定したパスワードで再度ログインします。

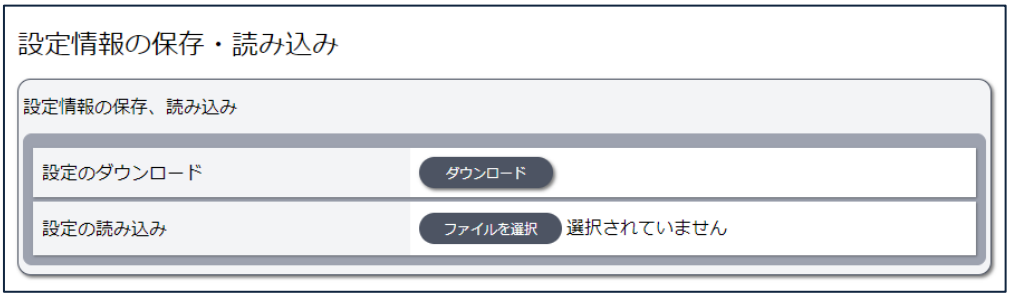
memo
- 入力したパスワードはすべて、「●」で表示されます。
- 入力可能な文字数は、半角英数字、記号で 32 文字までです。
- 8 文字未満のパスワードは設定できません。

初期パスワードはログイン時に必ず変更してください。
その際、英(大文字と小文字)・数字・記号(" $:?`以外)含む 8 ～32 文字の推測されにくいパスワードにしてください。

詳細は『RoosterDRX_取扱説明書の 2-7.入力できない記号一覧』をご覧ください。

2-2. 設定情報の保存・読み込み

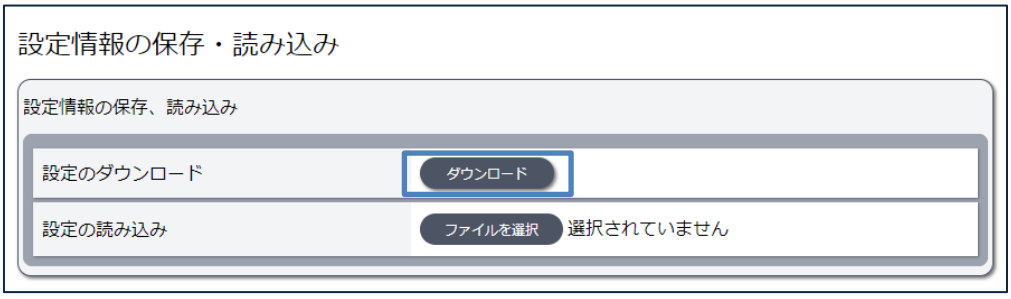
設定ツールのメニューから、［本体設定］－［設定情報の保存、読み込み］ をクリックします。
「設定情報の保存、読み込み」のページが表示されます。



2-2-1.　現在の設定を保存

現在の設定情報の保存を行います。

1．　［設定のダウンロード］の［ダウンロード］ボタンをクリックします。



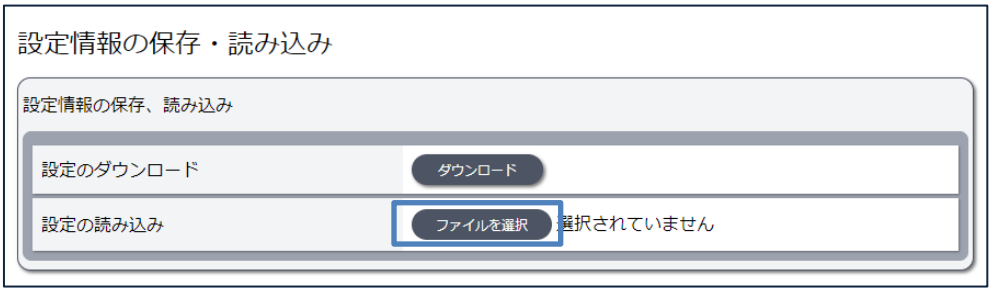
2．　保存先を指定する場合は、［名前を付けて保存］を選択して、保存先を指定します。
DRX の設定情報「DRX-backup-config.cnf」が、指定した保存先にダウンロードされます。

memo

- DRX の保存ファイル「DRX-backup-config」の拡張子「.cnf」あり、なしが存在していますが、保存ファイルのフォーマットの変更はありませんのでファイル名を変更してお使いください。

2-2-2. 保存した設定の読み込み

1．　［設定の読み込み］の［ファイルを選択］ボタンをクリックし、読み込みを行う設定情報ファイルがある場所を指定します。



2．　［読み込み開始］ボタンをクリックします。

3．　DRX の設定が保存時の設定に書き戻されます。

・設定の読み込みにおいて、異なる機種「DRX シリーズ」の設定情報ファイルの読み込みは動作保証ができませんのでご注意ください。
また動作させている FW バージョン以外で取得した設定情報ファイルは、１つ古いバージョンで動作させている時に取得した設定情報ファイルのみが対象となります。
・ログインパスワードが工場出荷状態の設定情報は読み込むことができません。

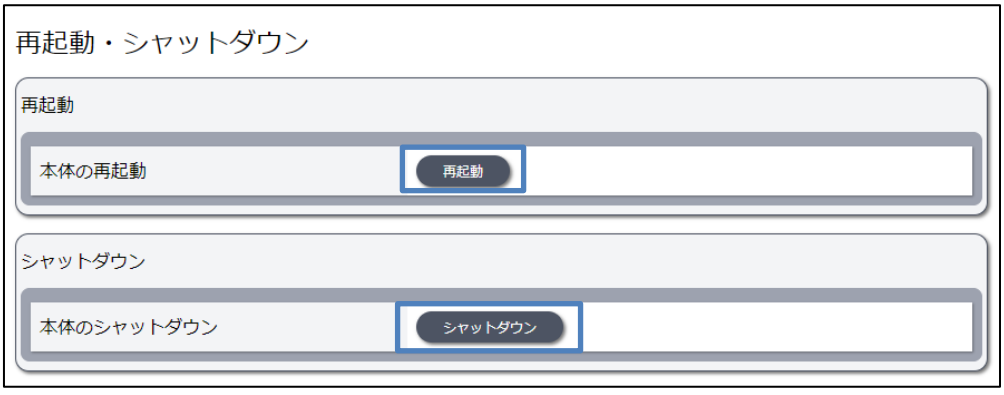
2-3. 設定の消去

1. 設定ツールのメニューから、［本体設定］－［設定の消去］ をクリックします。
「設定の消去」のページが表示されます。

2. 「工場出荷時の設定に戻す］場合は［消去］ ボタンをクリックします。
確認ダイアログで［はい］をクリックすると本体が再起動後、自動的にシンプル WebUI に移行します。

2-4. 再起動・シャットダウン

1. 設定ツールのメニューから、［本体設定］－［再起動・シャットダウン］をクリックします。
「再起動・シャットダウン」ページが表示されます。



2-4-2. 再起動

1. DRX の再起動の場合［再起動］ボタンをクリックします。
確認ダイアログで［はい］をクリックすると「再起動」開始から 3 分後に自動的にログイン画面に移行します。

> 再起動が完了するまで、3 分程度かかります。

2-4-3. シャットダウン

1. DRX のシャットダウンの場合［シャットダウン］ボタンをクリックします。
確認ダイアログで［はい］をクリックします。
2. シャットダウン後、本体の power ランプ以外のランプが消灯したら電源を抜きます。

2-5. ファームウェアアップデート

1．　設定ツールのメニューから、［本体設定］－［ファームウェアアップデート］をクリックします。
「ファームウェアアップデート」ページが表示されます。

2．　［ファイルを選択］ボタンをクリックして、ダウンロードしたアップデートプログラムデータ「＊.rsys」のある場所を指定します。

3．　［アップデート開始］ボタンをクリックします。
確認ダイアログで［はい］をクリックすると、DRX のファームウェアがアップデートされます。

・ログインパスワードが工場出荷状態のままの場合はアップデートができません。
ログインパスワード変更後にアップデートを行ってください。
➲ ログインパスワードの変更は『2-1.パスワード変更』をご覧ください。
・ファームウェアのイメージファイルは 60M バイト以上あります。従量課金のご契約でのダウンロードにはご注意ください。
・ファームウェアバージョン 3.x.x から 2.x.x へダウングレードを行った場合、設定情報が初期化され工場出荷状態となりますのでご注意ください。

DRX5010　DRX5002

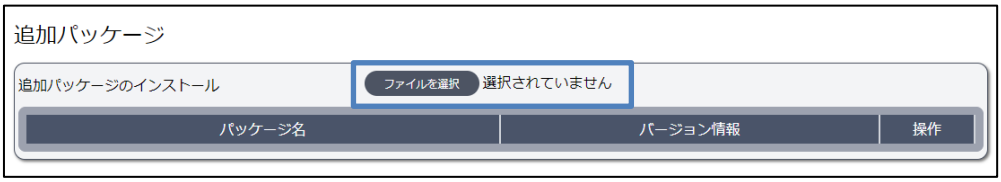
ファームウェアのアップデートでは完了するまで、10 分程度かかります。アップデート中は、絶対に電源が OFF とならないようにしてください。動作不能となる恐れがあります。これにより動作不能となった場合、有償修理となりますのでご注意願います。

memo
ブートエリアが 2 面（A 面、B 面）ありますので、必要に応じ両面とも書き換えたい場合は 2 回連続してアップデートを行ってください。
（2 回連続してアップデートすることで A 面、B 面両面を書き換える操作となります）

2-6. 追加パッケージ

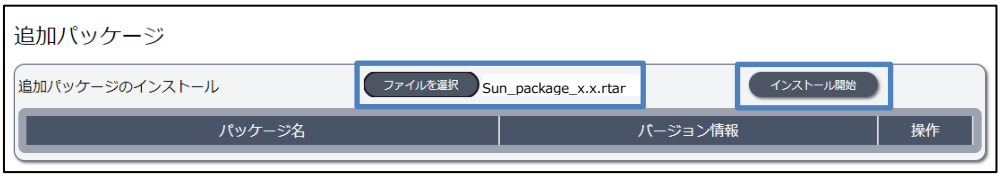
本製品上で動作する追加パッケージを管理できます。サン電子㈱が提供する DRX 向けの追加パッケージをインストール、アンインストールすることができます。

設定ツールのメニューから、［本体設定］－［追加パッケージ］をクリックします。「追加パッケージ」ページが表示されます。



2-6-1.　追加パッケージのインストール

1．　［ファイルを選択］ボタンをクリックして、提供されたデータ「＊.rtar」のある場所を指定します。
［インストール開始］ボタンをクリックします。

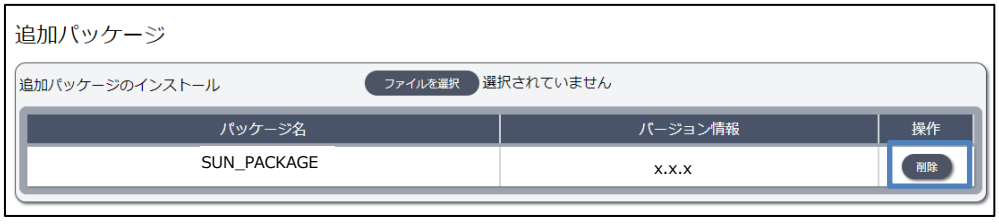


2．　インストールが完了すると再起動確認ダイアログが表示されます。
［はい］をクリックすると再起動して「追加パッケージ」が適用されます。

> memo　他にも「＊.rfrm」、「＊.bin」の追加パッケージに対応しています。

2-6-2.　追加パッケージのアンインストール

1．　アンインストールするパッケージリストの［削除］ボタンをクリックします。
確認ダイアログが表示されると［はい］をクリックします。



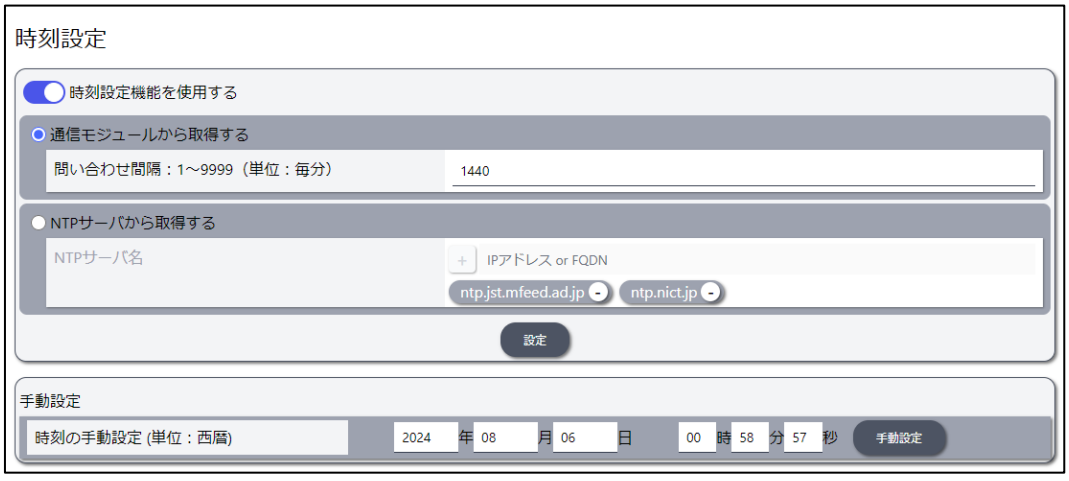
2．　パッケージ削除完了後、再起動の確認ダイアログが表示されると［はい］をクリックします。

> **追加パッケージはインストール・アンインストール後、再起動することで実行されますので必ず再起動してください。**

2-7. 時刻設定

> ここで設定される時刻は、DRX のログ表示などに使用されます。

設定ツールのメニューから、［本体設定］－［時刻設定］をクリックします。
「時刻設定」ページが表示されます。



2-7-1.　通信モジュールから取得する場合

1．　［通信モジュールから取得する］チェックをオンにします。

2．　［問い合わせ間隔］を入力します。（1～9999 分毎）
　　指定された間隔で通信モジュールに問い合わせを行い、時刻を同期します。

3．　[設定] ボタンをクリックします。
　　通信モジュールから取得した時刻に調整されます。

> ［通信モジュールから取得する］を使用するには、接続可能な APN 名を設定する必要があります。

2-7-2.　NTPサーバから取得する場合

公開 NTP サービスを利用する場合は、インターネットに接続している必要があります。

1．［NTP サーバ機能を使用する］チェックをオンにし、NTP サーバを登録します。

2．登録した「サーバ名」もしくは「IP アドレス」を入力すると［＋］ボタンが有効になります。
［＋］ボタンを押すとリストに登録されます。

3．リストから削除する場合は［－］ボタンを押します。

4．登録完了後、［設定］ボタンをクリックして、設定を反映させます。

memo　NTP サーバは２つ以上登録可能ですが、先に登録した NTP サーバが優先されます。

2-7-3.　手動で時刻の設定を行う場合

1．［手動設定］の各欄に、現在の時刻を入力します。

2．［手動設定］ボタンをクリックします。
直ちに設定した時刻に調整されます。

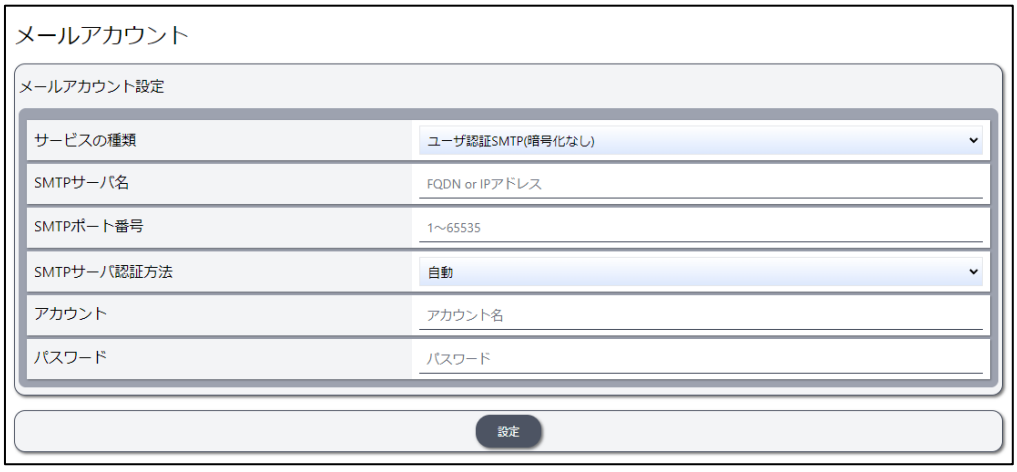
「時刻設定機能を使用する」設定になっていても、「手動設定」により時刻が変更されます。
また、時刻設定機能による時刻変更を行わない場合、「時刻設定機能を使用する」のチェックをオフにする必要があります。

2-8. メールアカウント

ここで設定されるメールアカウントは、「トリガー」機能を利用してメール送信が可能です。
メールの送信が必要ない場合、メールアカウントの設定の必要はありません。

トリガーを利用してメールを 送信する場合は「4-8-11. トリガーアクション：メール」をご確認ください。

1．　設定ツールのメニューから、[本体設定] – [メールアカウント設定] をクリックします。
「メールアカウントの設定」ページが表示されます。



2．　以下の設定を行います。

項目	内容
サービスの種類	メールサーバの種類を選択します。 「ユーザ認証 SMTP（暗号化なし）」「ユーザ認証 SMTP over SSL」「ユーザ認証 SMTP STARTTLS」のいずれかを選んでください。
SMTP サーバ名	送信メールサーバ名を設定します。
SMTP ポート番号	送信ポート番号を設定します。(省略可)
SMTP-AUTH	SMTP サーバの認証方法を選択します。「自動」、「PLAIN」、「LOGIN」、「CRAM-MD5」、「DIGEST-MD5」のいずれかを選んでください。
アカウント	メールアカウント名を設定します。
パスワード	使用するメールアカウントのパスワードを入力します。

上記の設定で不明な部分につきましては、インターネットプロバイダ、あるいはサーバ管理者までお問い合わせください。

3．　[設定] ボタンをクリックして、設定を反映させます。

2-9. おやすみモード

DRX の省電力の制御を行います。この機能は定期的に DRX をサスペンド（消費電力を抑えた待機状態）することにより、電力の消費を抑えることができます。

レジューム（復帰して通常状態）する条件としては、スケジュール以外に WakeOn 着信（『4-3. WakeOn 着信の設定』）があります。 DRX5010 DRX5002

memo
- サスペンド・・省電力モードとなり、通信できない状態となります。
- レジューム・・通常動作に戻り、通信可能な状態となります。

モバイル通信端末のオンライン ファームウェア アップデートを行うときは、おやすみモードを使用しないでください。

2-9-1. おやすみモード設定

1. 設定ツールのメニューから、[本体設定] – [おやすみモード] をクリックします。
「おやすみモードの設定」ページが表示されます。

2. 設定の追加にスケジュール名を入力し、[追加] をクリックすると、詳細設定画面が表示されます。

以下の項目を入力し、［変更］ボタンを押します。

項目	内容
スケジュール名	任意のスケジュール名。半角英数字で入力してください。 おやすみモードスケジュール設定のスケジュール名になります。
サスペンド曜日	サスペンドさせたい曜日を選択します。
サスペンド時刻	サスペンドさせたい時刻を設定します。
レジューム曜日	レジュームさせたい曜日を選択します。
レジューム時刻	レジュームさせたい時刻を設定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。

3．　［おやすみモードを使用する］チェックをオンにします。

4．　［設定］をクリックします。
確認ダイアログで「設定を有効にするためシステムを再起動する必要があります」画面が表示されますので、［はい」をクリックします。

5．　個々のスケジュールを変更する場合は、［スケジュールリストの設定］をクリックして、変更するスケジュール欄の［操作］項目の［編集］をクリックして、内容を変更します。また、スケジュールを削除する場合は、［削除］をクリックします。

memo　スケジュール名の変更はできません。スケジュール名を変更する場合は、スケジュールを削除して再入力してください。

2-9-2.　おやすみモード設定例

条件

以下の条件でおやすみモードを設定する場合の例について説明します。

- 月曜日から金曜日まで 21 時 00 分～ 8 時 00 分まで省電力で使用する。
- 土曜日、日曜日は全日省電力で使用する。

設定

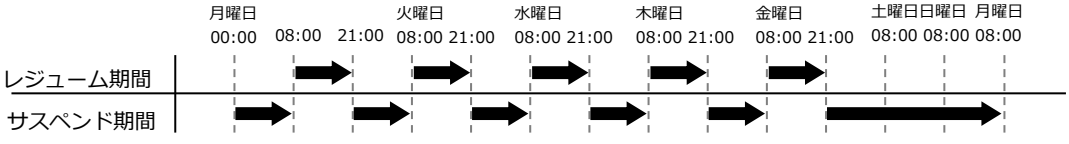
1．「おやすみモードの設定」ページで以下の設定を行います。

- ［おやすみモード機能を使用する］にチェックをオンにします。
- ［スケジュールリストの設定］をクリックします。
- 月曜日～金曜日までのスケジュールを作成します。
- 月曜日～金曜日の［サスペンド時刻］を 21 時 00 分に設定します。
- 月曜日～金曜日の［レジューム曜日］を翌日に設定します。
- 月曜日～金曜日の［レジューム時刻］を 8 時 00 分に設定します。
- ［設定］ボタンをクリックします。

「スケジュール設定」ページで［追加］ボタンをクリックし、［サスペンド曜日］、［サスペンド時刻］、［レジューム曜日］、［レジューム時刻］を下図のように設定します。

おやすみモード設定例の状態遷移

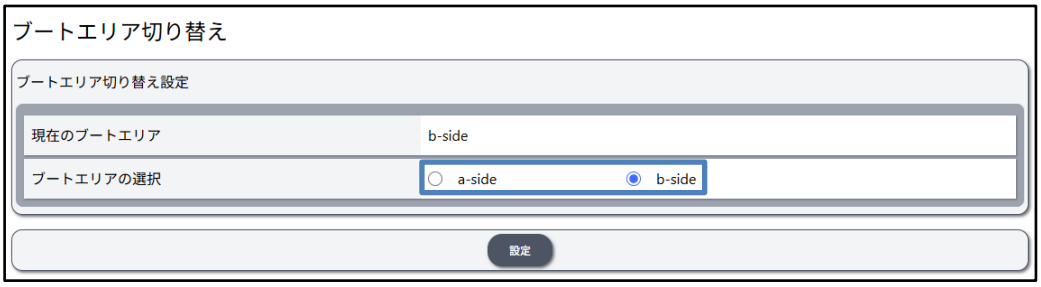
上記の設定によるおやすみモードの状態遷移は次のようになります。



2-10. ブートエリア切り替え

本製品には長期的に安定した動作を実現する為に、ファームウェアの領域を 2 つ持っています。
ブートエリアページでは、明示的に起動するブートエリアを変更できます。
また、本製品起動時にファームウェアの領域でエラーが発生した場合に、自動的に別の面のファームウェアを使用します。

1. 設定ツールのメニューから、[本体設定] – [ブートエリア切り替え] をクリックします。
   「ブートエリア切り替え設定」ページが表示されます。



2. 「現在のブートエリア」には起動されているサイド面が表示されています。
3. ブートエリアを切り替える場合は現在のブートエリアと違うエリアを選択し、[設定] ボタンをクリックします。
   ブートエリアの切り替え確認ダイアログで [はい] を選択すると DRX が「再起動」します。

FW バージョン v3.0.0 以降から v2.6.x 以前に切り替えた場合、設定が初期化されます。

2-11. 電源制御

DRX の電源の制御を行います。この機能は定期的に DRX の電源を ON/OFF することにより、より安定した運用を行うことを目的とします。

1．　設定ツールのメニューから、［本体設定］－［電源制御］をクリックします。
「電源制御」のページが表示されます。

2．ハードウェアの電源制御の設定を行います。

項目	内容
ハードウェアの自動電源 ON/OFF 機能を使用する	ハードウェアの電源制御を使用の場合、チェックをオンにします。
間隔	ハードウェアの電源制御の間隔１～７(日)のいずれかを設定します。
再起動時刻を指定	再起動時刻を指定の場合、チェックをオンにします。
再起動時刻	ハードウェアの電源制御を実行する時刻(hh:mm 形式)を設定します。

3．ソフトウェアの電源制御の設定を行います。

項目	内容
ソフトウェアの自動電源 ON/OFF 機能を使用する	ソフトウェアの電源制御を使用の場合、チェックをオンにします。
再起動時刻	ソフトウェアの電源制御を実行する時刻(hh:mm 形式)を設定します。
再起動時刻を分散する	再起動時刻を分散する場合、チェックをオンにします。
分散時間	再起動時の分散時間１～120(分)を設定します。
間隔指定、曜日指定	［間隔指定］、［曜日指定］の中、使用する機能を選択します。 ▶［間隔指定］の場合、間隔１～７(日)のいずれかを設定します。 ▶［曜日指定］の場合、［月］、［火］、［水］、［木］、［金］、［土］、［日］で実行したい曜日をチェックをオンにします。

4．選択した設定でよければ［設定］ボタンをクリックします。

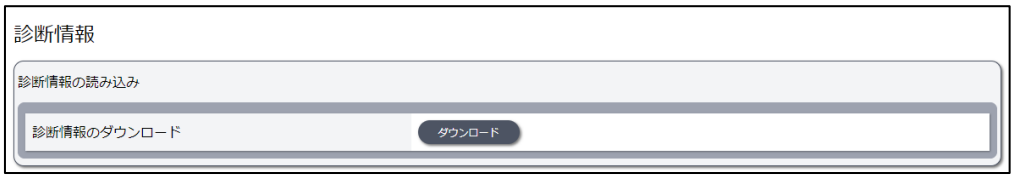
5．確認ダイアログ［設定を有効にするためシステムを再起動する必要があります］が表示されますので、［はい］をクリックしてください

電源制御の詳細は『RoosterDRX 取扱説明書』の電源制御をご参照ください。

2-12. 診断情報

診断情報の取得ページでは、本製品の現在の情報をまとめたファイルを取得できます。

1．　設定ツールのメニューから、［本体設定］－［診断情報］をクリックします。
「診断情報の取得」のページが表示されます。



2．　ダウンロードボタンをクリックし、診断情報を取得します。

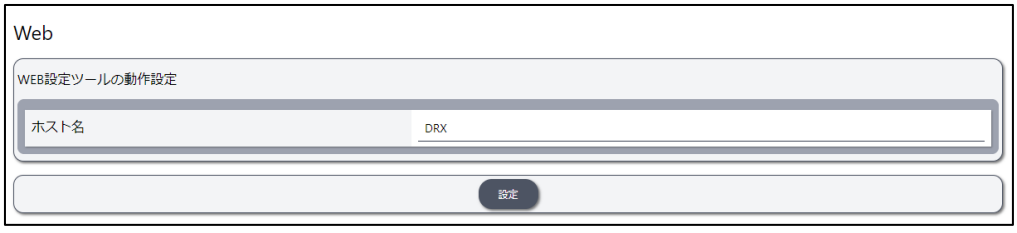
memo　取得できるファイルは、弊社解析用の特殊なファイルです。

使用状況により取得するファイルが大きくなること（10MB 以上）がありますので、従量課金の回線からダウンロードする場合はご注意ください

2-13. ホスト名

本体のホスト名を設定します。

1．　設定ツールのメニューから、［本体設定］－［ホスト名］をクリックします。
「ホスト名」のページが表示されます。



2．　以下の設定を行ってください。

項目	内容
ホスト名	本体のホスト名、半角英数字（1～253 文字）を入力します。

2-14. ユーザーアカウント管理

ログインアカウント管理の設定をします。

アカウントの種類は、管理者、一般ユーザの 2 種類あります。

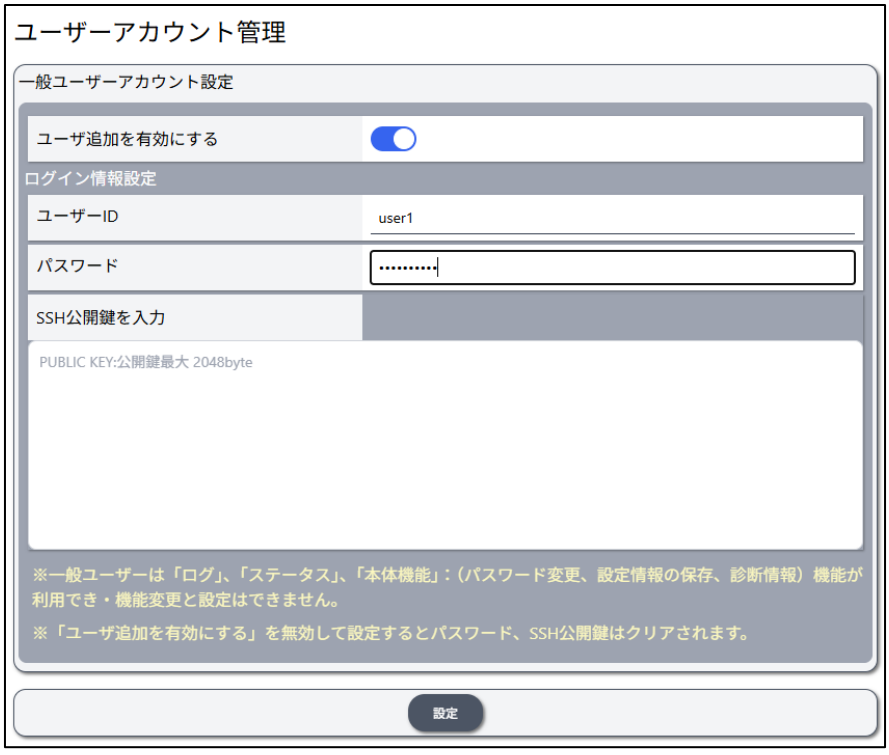
管理者では、全ての設定、操作が可能です。

一般ユーザでは、一部の設定、操作が可能です。

- ・本体設定：［パスワード変更］設定、［設定情報のファイルダウンロード］、［診断情報の取得］
- ・各種サービス：［SSH 接続］公開鍵 設定
- ・ログ：［最新ログ再読み込み］、［全てのログ取得］
- ・ステータス：［コマンド実行］

2-14-1. ユーザーアカウント作成

1. 設定ツールのメニューから、［本体設定］－［ユーザーアカウント管理］をクリックします。
「ユーザーアカウント管理」のページが表示されます。



2. 一般ユーザのアカウントを作成する場合は、［一般ユーザーアカウント設定］にて［ユーザ追加を有効にする］のチェックをオンにします。
3. ［ユーザーID］に、一般ユーザーのログイン時に使用するユーザ名を入力します。
4. ［パスワード］に、一般ユーザーのログイン時に使用するパスワードを入力します。
5. CLI にて SSH 公開鍵でログインする場合、［SSH 公開鍵］に公開鍵を入力します。（任意）
6. ［設定］ ボタンをクリックして、設定内容を反映させます。

memo
- ［ユーザーID］には、英小文字・数字で 1 文字目は必ず英小文字、4 文字以上 32 文字以下で入力ください。

- アカウント名として入力できない文字列は以下の通りです。
  root、rooster、suncorp、daemon、ftp、network、nobody、dnsmasq、unbound、
  管理者アカウント名設定で設定された文字列
- ［パスワード］には、大文字、小文字、数字、記号を含む、8 文字以上 32 文字以下で入力ください。入力できない記号を含む文字列は設定できません。

詳細は『RoosterDRX_取扱説明書の 2-7.入力できない記号一覧』をご覧ください。

有効に設定した後に無効に変更する場合、［ユーザーID］の ID も削除してください。

旧 FW バージョンからの一般ユーザ設定の引継ぎについての注意：
一般ユーザの追加操作を FW バージョン v3.1.0 以前で行った設定で FW バージョン v3.2.0 以降にバージョンアップした場合、

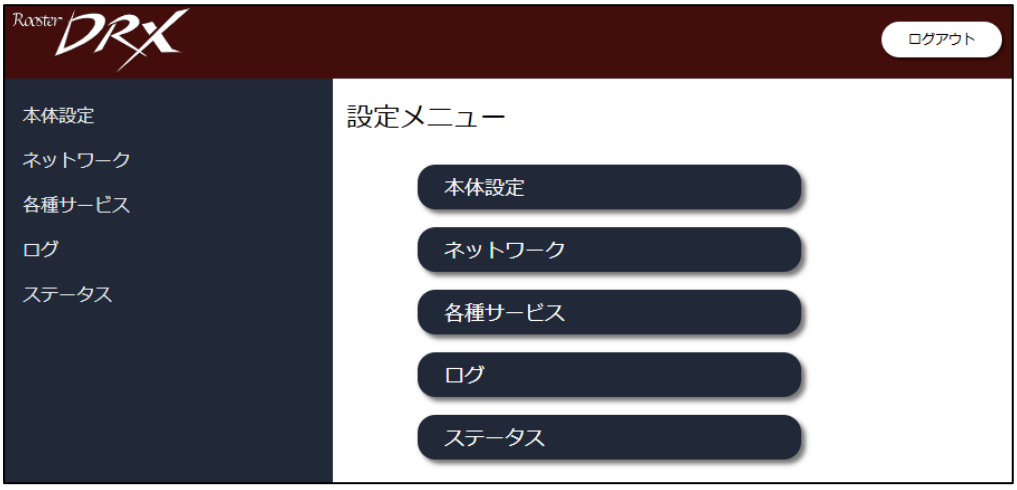
- 一般ユーザ名で使えない文字(大文字、記号)が入っている場合、ログインできますが、パスワード変更が出来なくなります。管理者ユーザでログインして、一般ユーザを再度 作成し直してください。
- FW バージョンアップした直後は CLI から一般ユーザでログインできません。CLI から一般ユーザでログインしたい場合、以下の手順を踏んでください。
  1. 一般ユーザで AdvancedWebUI でログインする。（1 度だけで結構です）
  2. 管理者アカウントにて、CLI で一般ユーザのアカウント追加（set account regist コマンド）で作成し直してください。

一般ユーザを追加した設定状態で FW のバージョンダウン（v3.1.0 以前）を行わないでください。

2-14-2. 一般ユーザーアカウントログイン方法

1. 一般ユーザーアカウントのログイン方法はログインの場合は［ログアウト］をクリックし、ログイン画面へ移動します。

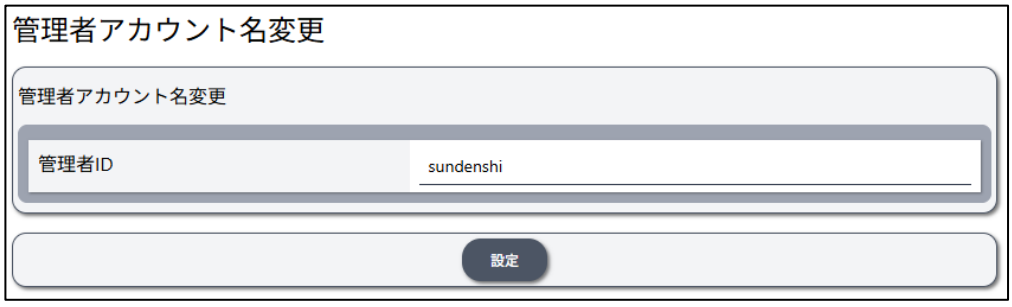
2. ［ユーザーアカウント管理］画面で作成された［ユーザーID］と［パスワード］をログイン画面にて［ユーザー名］と［パスワード］の入力フォームに入力し、［ログイン］ボタンをクリックします。
3. ログイン完了後、以下の画面が表示されます。


Roaster DRX
ログアウト
本体設定
ネットワーク
各種サービス
ログ
ステータス
設定メニュー
本体設定
ネットワーク
各種サービス
ログ
ステータス

2-15. 管理者アカウント名変更

ログインするアカウントのユーザ名（管理者 ID）を「root」から変更することができます。

1．　設定ツールのメニューから、［本体設定］－［管理者アカウント名変更］をクリックします。
「管理者アカウント名変更」のページが表示されます。



2．［管理者 ID］に、root から変更したい管理者アカウント名を入力します。

3．［設定］ボタンをクリックします。

4．設定の反映後、ログインページへ移動します。
新しく設定した管理者 ID で再度ログインします。

memo

- ［管理者 ID］には、英小文字、数字、1 文字目は必ず英小文字、4 文字以上 32 文字以下で入力ください。
- 管理者 ID として入力できない文字は以下の通りです。
  rooster、suncorp、daemon、ftp、network、nobody、dnsmasq、unbound、
  別途アカウントで設定された文字列

3章　ネットワーク

この章では、インターフェイス、モバイル、VPN、ファイアウォール、NAT など、詳細なネットワーク設定について説明します。

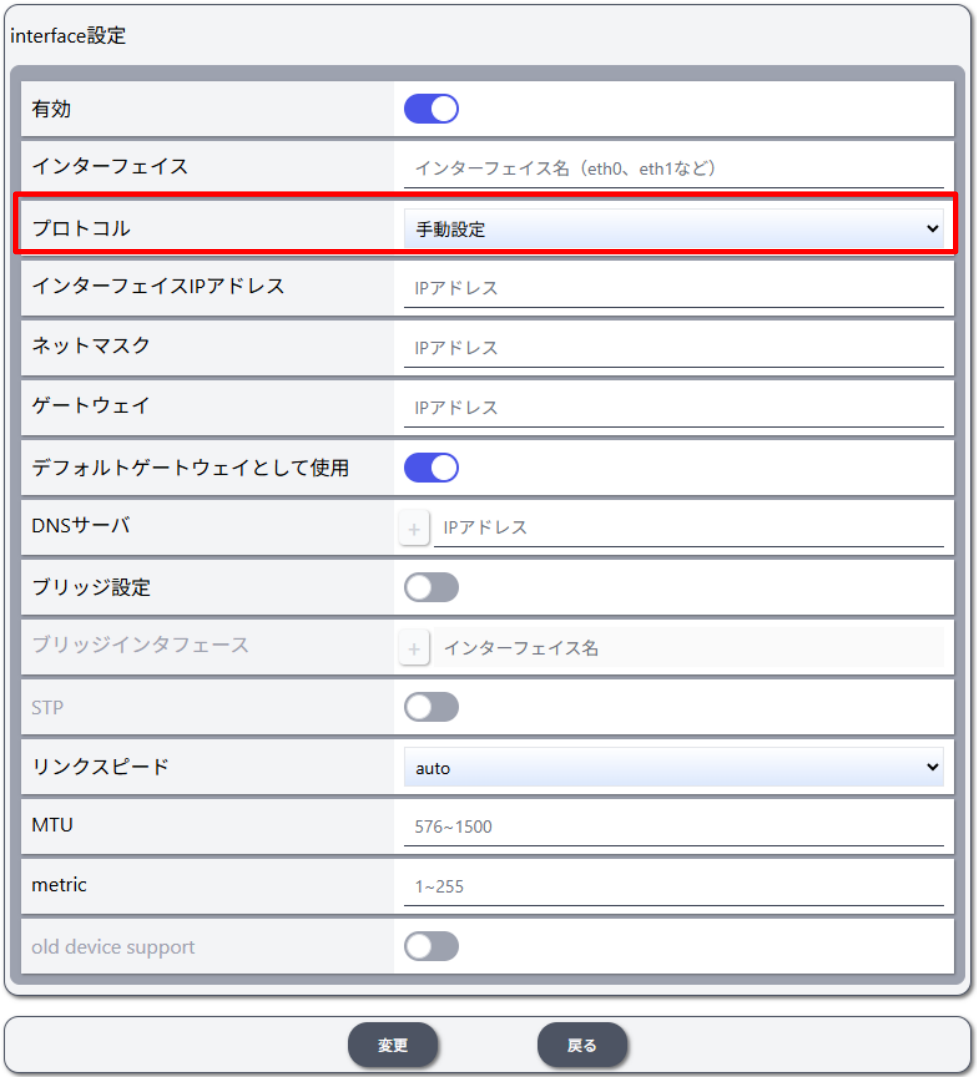
3-1. インターフェイス

LAN/WAN やモバイル通信用の物理インターフェイス、VPN で使用する仮想インターフェイスの設定を行います。

1. 設定ツールのメニューから、［ネットワーク］－［インターフェイス］をクリックします。
「インターフェイス」設定画面が表示されます。

2. インターフェイスを追加する場合は、［ネットワーク設定］にて［ネットワーク名］を入力し［追加］ボタンをクリックします。

3.［ネットワーク名］を入力し［追加］をクリックすると詳細設定画面が表示されます。



4.詳細設定画面ではプロトコル［手動設定］、［DHCP クライアント］、［PPP］、［PPPoE］、［VPN］、［unmanaged（IPsec）］項目選択にあわせて設定画面が変化します。

5.設定済みの項目を変更する場合は、［編集］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。

6 . [設定] ボタンをクリックして、設定内容を反映させます。

DRX5510 では MBIM モード固定となります。 DRX5510

ネットワーク名［mobile1］は［削除］できません。
Mobile1 の設定変更の場合［編集］をご利用ください。
・実インターフェイス名は、usb0(ECM モード)又は wwan0(MBIM モード)のみ設定可能です。
wwan0(MBIM モード)で使用する場合、以下の！欄も参照ください。
・プロトコルは、
実インターフェイス名が usb0 の場合、static 又は dhcp-client のみ設定可能です。
実インターフェイス名が wwan0 の場合、dhcp-client のみ設定可能です。
ネットワーク名が mobile1 以外の場合、実インターフェイス名を usb0、wwan0 に設定することはできません。

DRX5010 DRX5002

「モバイル通信端末の FW バージョン」が古い(v14-12 以前)場合
(DRX 製造番号で DRX5010 は DR01047047933 以前、DRX5002 DR00247047933 以前が対象となります)
・MBIM モードに設定して動作させた場合、通信できなくなりますのでご注意ください。その場合は そのまま ECM モードでお使いいただくか、「モバイル通信端末の FW」を MBIM に対応した FW(v14-18 以上)にバージョンアップをしてください。
・「モバイル通信端末の FW バージョンアップ」はお客様にて実施いただけます。弊社ホームページから『DRX 通信モジュールアップデート ソフトウェア』をダウンロードいただきバージョンアップを実施ください。
・「モバイル通信端末の FW バージョン」は、モバイル通信端末ステータス画面の「モバイル通信端末情報一覧」欄の「バージョン」項目でご確認いただけます。

3-1-1.　手動設定

1．　プロトコルを［手動設定］に設定します。

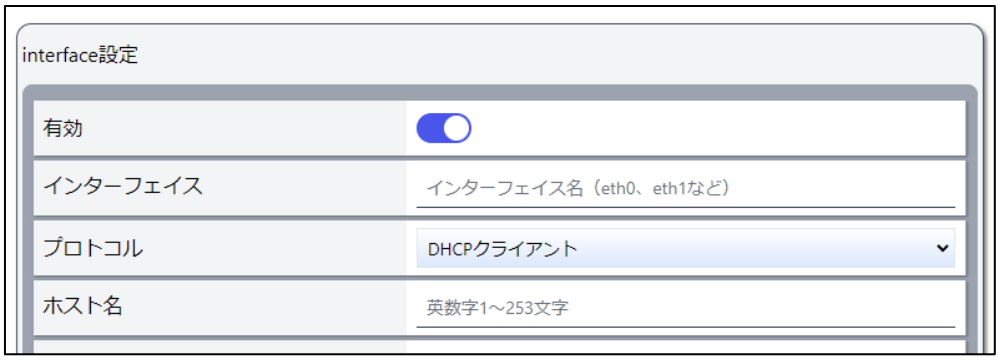
2．　以下の設定を行ってください。

項目	内容
有効	設定のインターフェイスを使用の場合、チェックをオンにします。
インターフェイス	インターフェイス［eth0］（LAN1 コネクタ）、［eth1］（WAN/LAN2 コネクタ）、任意のインターフェイス名を入力します。
インターフェイス IP アドレス	インターフェイスに設定する IP アドレスを入力します。
ネットマスク	インターフェイス IP アドレスのネットマスクを入力します。
ゲートウェイ	ゲートウェイ IP アドレスを設定します。
デフォルトゲートウェイとして使用	ゲートウェイをデフォルトゲートウェイとして使用の場合、チェックをオンにします。
DNS サーバ	DNS サーバ IP アドレスを設定します。 ▶DNS サーバ IP アドレスを入力後、［＋］ボタンをクリックで複数の IP アドレスが入力できます。 ▶ピアの DNS サーバを使用がオフの場合、設定が有効になります。
ピアの DNS サーバを使用	ピアの DNS サーバを使用する場合、チェックをオンにします。
ブリッジ設定	ブリッジインタフェースを使用する場合、チェックをオンにします。
ブリッジインタフェース	ブリッジ対象のインターフェイスを設定します。 ▶必ず物理インターフェイス名を入力してください。 インターフェイス名は［＋］ボタンをクリックで複数入力できます。
STP	STP を使用する場合、チェックをオンにします。
リンクスピード	インターフェイスのリンクスピードを設定します。 ▶auto：接続先の機器に合わせて最適なモードを設定します ▶1000M-Full：1Gbps 全二重通信を行います ▶100M-Full：100Mbps 全二重通信を行います ▶10M-Full：10Mbps 全二重通信を行います
MTU	インターフェイスの MTU 値を設定します。
metric	インターフェイスのメトリック値を設定します。
old-device-support	LAN デバイスの旧デバイスサポートを設定します。 本設定は旧デバイス（IEEE 802.3ab 確定前の規格非準拠な通信相手）と接続を試行するかを設定します。 ▶ファームウェアバージョン 3.0.0 以前からアップデートした場合は enable となります。 有効に設定した場合､接続機器によっては接続が不安定となることがあります。その場合は無効に設定ください。

STP 設定は、eth0 と eth1 をブリッジ（WAN を LAN とする）して使用する場合、無効に設定しないでください。

3-1-2.　DHCPクライアント

1．　プロトコルを［DHCP クライアント］に設定します。



2．　以下の設定を行ってください。

項目	内容
有効	設定のインターフェイスを使用の場合、チェックをオンにします。
インターフェイス	インターフェイス［eth0］、［eth1］、任意のインターフェイス名を入力します。
ホスト名	DHCP リクエスト時のホスト名を設定します。 ▶設定が無い場合、［本体設定］の［ホスト名］となります。 ➲ ホスト名は子機に IP が割り当てられた場合、「5-13.システムログ」で確認できます。

※その他の項目は、[手動設定] の項目説明を参照ください。

3-1-3. PPP

1．　プロトコルを［PPP］に設定します。

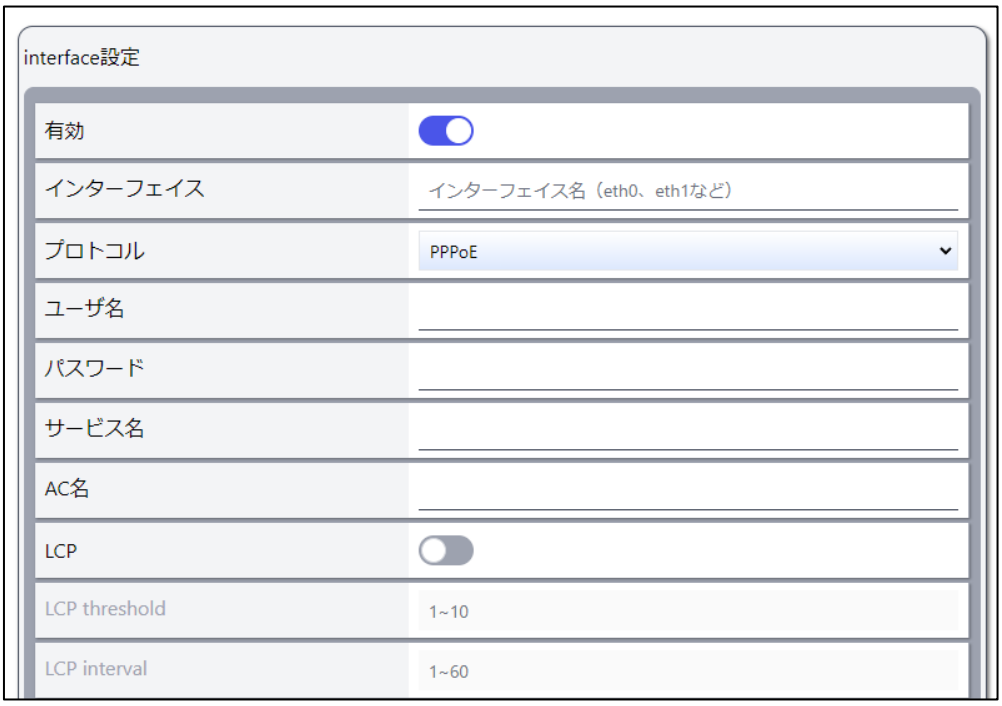
2．　以下の設定を行ってください。

項目	内容
有効	設定のインターフェイスを使用の場合、チェックをオンにします。
インターフェイス	インターフェイス［eth0］、［eth1］、任意のインターフェイス名を入力します。

※その他の項目は、[手動設定] の項目説明を参照ください。

3-1-4. PPPoE

1．　プロトコルを［PPPoE］に設定します。



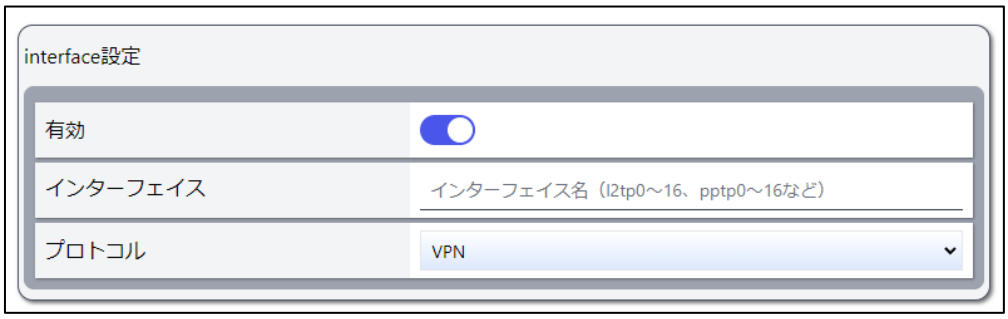
2．　以下の設定を行ってください。

項目	内容
ユーザ名	認証するためのユーザ ID を設定します。
インターフェイス	インターフェイス［eth1］を設定します。
パスワード	認証するためのパスワードを設定します。
サービス名	サービス名を設定します。(指定無い時は空欄)
AC 名	Access Concentrator 名を設定します。
LCP	LCP 機能を使用する場合は、チェックをオンにします。
LCP threshold	LCP エコーの監視回数を設定します。
LCP interval	LCP エコーの監視間隔を設定します。

※その他の項目は、［手動設定］の項目説明を参照ください。

3-1-5. VPN

1．　プロトコルを［VPN］に設定します。



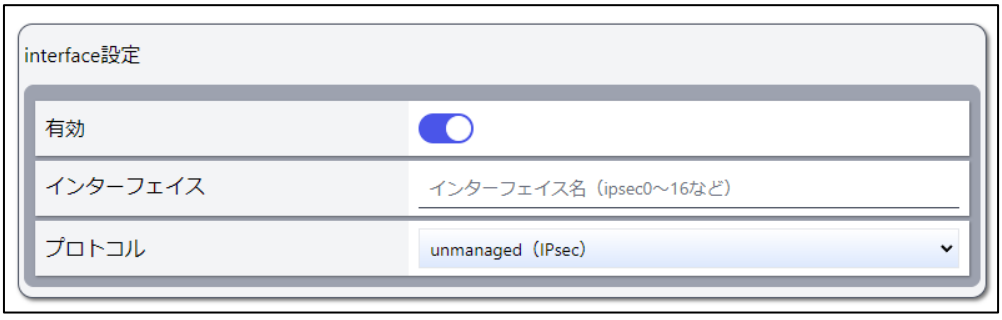
2．　以下の設定を行ってください。

項目	内容
インターフェイス	VPN に使用するインターフェイス名を設定します。 ▶L2TP/IPsec の場合、l2tp0～l2tp16 に設定します。 ▶pptp の場合、pptp0～pptp16 に設定します。 VPN 設定時、インターフェイス名が特定しやすい名前に設定することをお勧めします。 vpn0～vpn16 など任意のインターフェイス名も可能です。

※その他の項目は、[手動設定] の項目説明を参照ください。

3-1-6. unmanaged（IPsec）

1．　プロトコルを［unmanaged (IPsec)］に設定します。



2．　以下の設定を行ってください。

項目	内容
インターフェイス	VPN IPsec に使用するインターフェイス名を設定します。

※その他の項目は、[手動設定] の項目説明を参照ください。

3-2. モバイル

設定ツールのメニューから、［ネットワーク］－［モバイル］をクリックします。
「モバイル」設定画面が表示されます。

3-2-1.　SIM設定

1.［モバイル］画面の上部に「SIM 設定」が表示されます。

DRX5510

DRX5010　DRX5002

2. 以下の設定を行います。

項目	内容
SIM1 スロットを有効にする	SIM1 の SIM カードスロットを有効にする場合は、チェックをオンにします。 ・通信業者を選択 DRX5510 [ドコモ]、[KDDI]、[ローミング] DRX5010　DRX5002 [ドコモ]、[ソフトバンク]、[KDDI]、[ローミング] から選択します。 ・MVNO　DRX5010　DRX5002 仮想移動体通信事業者の SIM カードの場合は、チェックをオンにします。 ・PIN コードを設定 ご契約中の SIM カードの PIN コードを入力します。 PIN コードが設定されていない場合は、空白になります。
SIM2 スロットを有効にする	SIM2 の SIM カードスロットを有効にする場合は、チェックをオンにします。 ・通信業者を選択 DRX5510 [ドコモ]、[KDDI]、[ローミング] DRX5010　DRX5002 [ドコモ]、[ソフトバンク]、[KDDI]、[ローミング] から選択します。 ・MVNO　DRX5010　DRX5002 仮想移動体通信事業者の SIM カードの場合は、チェックをオンにします。 ・PIN コードを設定 ご契約中の SIM カードの PIN コードを入力します。 PIN コードが設定されていない場合は、空白になります。

3 . [設定] ボタンをクリックして、設定内容を反映させます。

・安定通信、安定運用のため、契約された SIM に適合した通信事業者を設定してください。
・必ず 5G 対応の SIM をご使用ください。 DRX5510

3-2-2.　プロファイル

DRX ではモバイル通信を行う場合、モバイル通信端末の設定が必要になります。
ご契約のモバイル端末の事業者からご提供された情報をご用意ください。
・APN（アクセスポイントネーム）・ID　・パスワード
・必ず 5G 対応の SIM をご使用ください。 DRX5510

1 . ［モバイル］画面の下部に「プロファイル」が表示されます。

2 . プロファイル番号を追加する項目にプロファイルの番号を入力し、[追加] ボタンをクリックします。
「モバイルプロファイルの詳細設定」の画面が表示されます。

DRX5510

DRX5010　DRX5002

以下の設定を行ってください。

項目	内容
No	1～8 の間で番号を表示します。
APN	ご契約のプロバイダのアクセスポイントネームを入力します。
ID	ご契約の SIM の ID を入力します。
パスワード	ご契約の SIM のパスワードを入力します。
PDP タイプ	[IP] を選択します。
認証プロトコル	認証プロトコルを、[自動]、[PAP]、[CHAP]より選択します。
SIM 番号	1、2 のいずれかを設定します。 ▶番号 1 が SIM 挿入口の SIM1、番号 2 が SIM2 となります。
PLMN MCC No. (ローミング時有効)	MCC 番号(3 桁)を入力します。 ▶MCC 番号が未入力の場合は MNC も未入力にしてください。 ▶MCC 番号を入力の場合は MNC も入力してください。 接続可能な MCC,MNC につきましては SIM 発行元にお問い合わせください。
PLMN MNC No. (ローミング時有効)	MNC 番号(2～3 桁)を入力します。 ▶MNC 番号が未入力の場合は MCC も未入力にしてください。 ▶MNC 番号を入力した場合は MCC も入力してください。 接続可能な MCC,MNC につきましては SIM 発行元にお問い合わせください。
無線接続方式 DRX5510	無線接続方式を、[5G + LTE]、[5G]、[LTE] より設定します。
NR モード DRX5510	NR モードを、[NSA + SA]、[NSA]、[SA] より設定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 64 文字までの英数字の文字列を入力できます。

- 「接続先通信事業者」は SIM 番号に指定した SIM が「ローミング」に設定されている場合のみ適用されます。
- 「ローミング」以外に設定されている場合は SIM スロット設定で指定した通信事業者が適用されます。

➲ SIM スロットの設定につきましては『3-2-1. SIM 設定』を参照してください。

DRX5510

- 「無線接続方式」に [5G] を設定した場合、「NR モード」は [NSA+SA]、[SA] で、かつ SA エリアでのみ接続可能となります。
- 「NR モード」に [NSA] を設定した場合、「無線接続方式」は [5G+LTE]のみ接続可能となります。
- SIM 契約が IPv6 対応のみの 5G SA の場合、接続できません。

3. [変更] ボタンをクリックすると設定内容が反映され、「モバイル」のページに戻ります。

[戻る] ボタンをクリックするとプロファイルは追加されず、「モバイル」のページに戻ります。

4.「モバイル」のページに戻ると、追加したプロファイル一覧が表示されています。

プロファイルの設定内容を変更する場合は、プロファイル名の操作項目にて［編集］をクリックし設定内容を変更します。また、プロファイルを削除する場合は、操作項目の［削除］をクリックしてプロファイルを削除します。

起動時、デフォルトプロファイルに設定されたプロファイルに自動的に接続します。
プロファイル設定が無い状態で、新規にプロファイルを作成した場合、作成したプロファイルが自動的にデフォルトプロファイルに設定されます。
デフォルトプロファイルが[未設定]の場合、自動的に接続しません。モバイル通信端末ステータス画面で接続操作をしてください。

3-2-3.　モバイル設定

1.　［モバイル］画面の中部に「モバイル設定」が表示されます。

2.　モバイル通信を使う場合は［モバイル通信を使用する］のチェックをオンにします。

3.　プロファイル一覧の No を選択して［設定］ボタンをクリックしてください。
選択したプロファイル No がデフォルトプロファイルとして設定されます。

4.　［自動リセットを有効にする］はモバイル通信端末を自動リセットするかどうかを設定します。

5.　［間隔：1～7（単位：日）］はモバイル通信端末自動リセットの周期を設定します。

回線が接続されている場合は、回線切断時にリセットを行います。

3-2-4.　アンテナの設定

memo　DRX では、使用するアンテナとして内部アンテナと外部アンテナを設定し、設置する環境に応じてどちらかを選択することができます。

1．設定ツールのメニューから、［ネットワーク］－［モバイル］－［アンテナ設定］をクリックします。

「アンテナ」のページが表示されます。

2．[使用アンテナ] 項目で、以下の設定を行います。

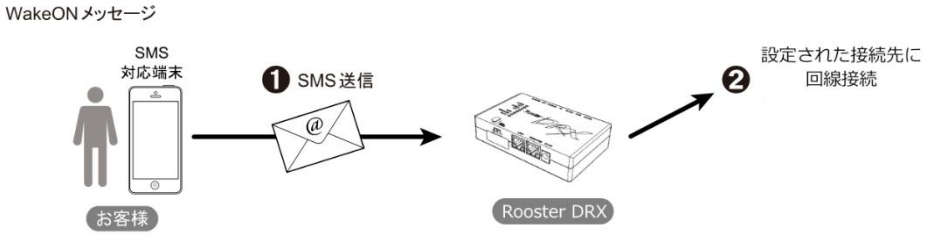
項目	内容
内部アンテナ	内部アンテナを使用します。
外部アンテナ	外部アンテナを使用します。

3．［変更］ボタンをクリックし、モバイル画面にて
[設定] ボタンをクリックして、設定内容を反映させます。

外部アンテナを選択した場合、
・外部アンテナ MOBILE1、MOBILE2、MOBILE3、MOBILE4　DRX5510
・外部アンテナ MOBILE1、MOBILE2　DRX5010　DRX5002
に本製品に適合したモバイル通信用アンテナを接続してください。

3-2-5.　WakeOn着信の設定

【WakeOn 着信について】
WakeOn 着信とは、おやすみモードにより省電力モードとなったモバイル通信端末に、遠隔地から操作して回線接続を可能にする機能です。
SMS による着信に対応しています。



1．　設定ツールのメニューから、［ネットワーク］－［モバイル］－［WakeOn 着信設定］をクリックします。
「WakeOn 着信設定」のページが表示されます。

2．　WakeOn 着信機能を使用する場合は、「WakeOn 着信を行う」のチェックをオンにします。

3．　認証キーの設定を行います。

項目	内容
認証キー	WakeOn メッセージの文字列による認証を行えます。 「WakeOn 着信を行う」設定を有効にした時に設定できます。 認証キーは、（受信したメッセージの先頭文字）～（設定された認証キー文字数）までを比較し、一致した場合は成功となります。 ただし、一文字でも異なった場合は認証失敗となります。

4．　SMS の着信番号の認証に使用する電話番号を追加します。

5．　以下の設定を行います。

項目	内容
電話番号	WakeOn 着信相手先の電話番号を入力します。 電話番号の数字部分のみが一致するかを判断します。 ▶ 電話番号のー（ハイフン）は、入力してもしなくても構いません。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 64 文字までの英数字の文字列を入力できます。

6．　[追加] ボタンをクリックし、電話番号を登録します。

7．　［変更］ボタンをクリックし、モバイル画面にて
[設定] ボタンをクリックして、設定内容を反映させます。

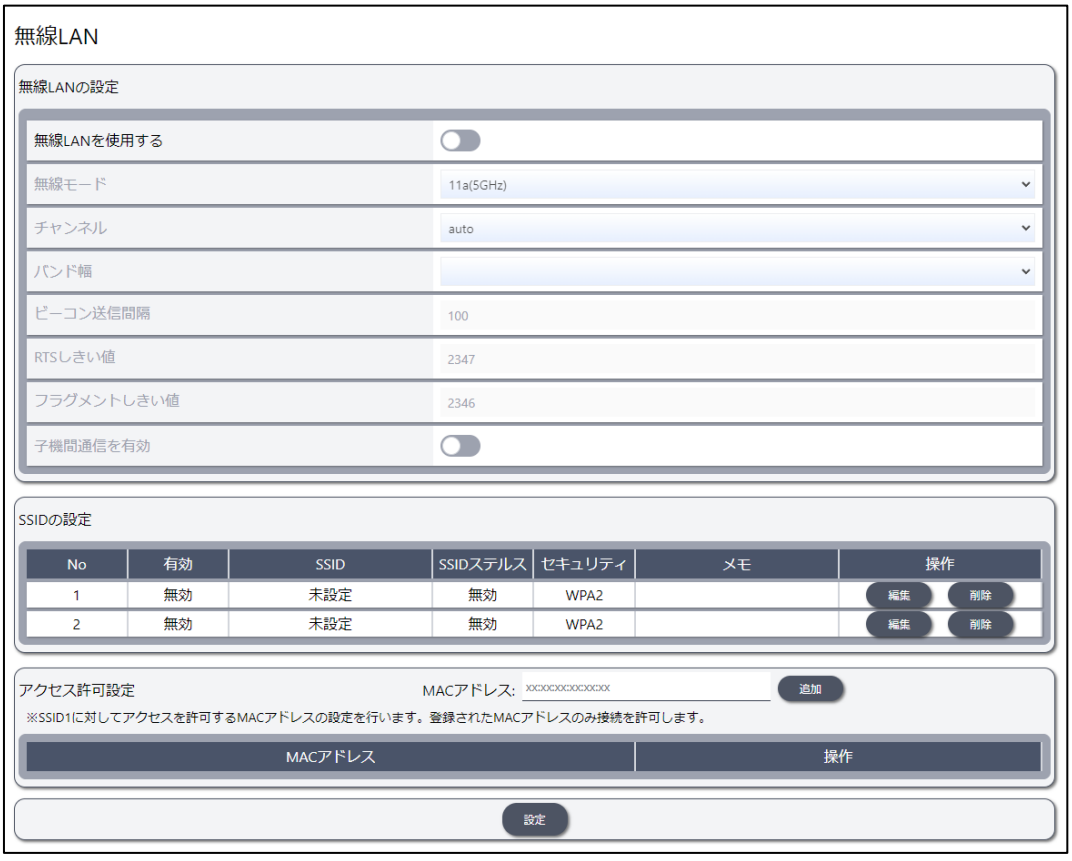
WakeOn 着信があると、モバイル通信端末ログに記録されます。

おやすみモードによるサスペンド状態から、WakaOn 着信によりレジュームさせることができます。

DRX5010　DRX5002

3-3. 無線LAN DRX5510 DRX5010

設定ツールのメニューから、［ネットワーク］－［無線 LAN］ をクリックします。
「無線 LAN」のページが表示されます。



「無線 LAN」のページでは、以下の設定を行います。

設定項目	説明
無線 LAN 設定	無線 LAN の詳細情報を登録します。
SSID 設定	SSID の詳細情報を設定します。
アカウント許可設定	MAC アドレスの登録を行います。

- 接続可能な無線 LAN 端末数は最大 20 台となります。

3-3-1.　無線LAN設定

1．　以下の設定を行います。

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>無線 LAN を使用する</td><td>無線 LAN を使用する場合は、チェックをオンにします。</td></tr>
<tr><td>無線モード、チャンネル、バンド幅</td><td>使用する無線 LAN の無線モード（周波数）、チャンネル、バンド幅を設定します。
▶チャンネルとバンド幅の数値は周波数によって異なります。
<table>
<tr><th>無線モード</th><th>チャンネル</th><th>バンド幅</th></tr>
<tr><td>11a(5GHz)</td><td>Auto、36ch、40ch、44ch、48ch</td><td>-</td></tr>
<tr><td rowspan="2">11a/n(5GHz)</td><td>Auto、36ch、40ch、44ch、48ch</td><td>20MHz</td></tr>
<tr><td>Auto、38ch、46ch</td><td>40MHz</td></tr>
<tr><td rowspan="3">11ac(5GHz)</td><td>Auto、36ch、40ch、44ch、48ch</td><td>20Mhz</td></tr>
<tr><td>Auto、38ch、46ch</td><td>40MHz</td></tr>
<tr><td>Auto、42ch</td><td>80MHz</td></tr>
<tr><td>11b(2.4GHz)</td><td>Auto、1ch、2ch、3ch、4ch、5ch、6ch、7ch、8ch、9ch、10ch, 11ch、12ch、13ch</td><td>-</td></tr>
<tr><td>11b/g(2.4GHz)</td><td>Auto、1ch、2ch、3ch、4ch、5ch、6ch、7ch、8ch、9ch、10ch, 11ch、12ch、13ch</td><td>-</td></tr>
<tr><td>11b/g/n(2.4GHz)</td><td>Auto、1ch、2ch、3ch、4ch、5ch、6ch、7ch、8ch、9ch、10ch, 11ch、12ch、13ch</td><td>-</td></tr>
</table></td></tr>
<tr><td>ビーコン送信間隔</td><td>ビーコンは無線ネットワークを同期させるためにアクセスポイントから一定間隔で送信するパケットになります。
・初期値：100ms
・設定範囲：50～4000ms</td></tr>
<tr><td>RTS しきい値</td><td>RTS しきい値は送信要求パケットのサイズになります。
・初期値：2346byte
・設定範囲：1～2347byte</td></tr>
<tr><td>フラグメントしきい値</td><td>フラグメントしきい値は、パケットが断片化される時のパケットサイズになります。
・初期値：2346byte
・設定範囲：256～2346byte（偶数値のみ）</td></tr>
<tr><td>子機間通信を有効</td><td>無線 LAN の子機同士の通信を有効にする場合、チェックをオンにします。</td></tr>
</table>

2．［設定］ボタンをクリックして、設定を反映させます。

「子機間通信を有効」の設定は「同一 SSID 間の子機間通信」を有効にする機能です。異なる SSID（SSID1 と SSID2 の子機同士）の通信はこちらの設定と関係なく、通信することができます。

・無線モードで 5GHz は屋内専用になります。屋外では使用しないでください。
・使用環境によって温度上昇した際、機器の保護を目的として無線 LAN の通信速度を自動的に抑制する場合があります。

3-3-2. SSIDの設定

1．SSID の設定は［No.1］または［No.2］の [操作] 項目にて [編集] をクリックします。

2．［削除］ボタンをクリックすると SSID の項目は削除されず設定内容が初期化されます。

3．「SSID の詳細設定」のページが表示されます。

4．以下の設定を行います。

項目	内容
SSID	SSID を入力します。
SSID ステルス	ネットワーク名一覧から SSID を参照できないようにビーコン信号の停止を行う場合に有効にします。 ・初期値：無効
セキュリティ	安全性を強化するための規格を選択します。 ・初期値：WPA2 ・規格：WEP、WPA、WPA2、WPA/WPA2
WEP キー	WEP キーの番号を入力します。 ［セキュリティ］を［WEP］にした場合のみ設定します。 ・WEP キー：５文字又は１３文字
暗号化方式	［セキュリティ］を［WPA］、［WPA2］、［WPA/WPA2］に設定した場合に設定します。 ・初期値：AES ・方式名：TKIP，AES，TKIP/AES
暗号化キー管理方式	PSK 固定となります。 ・初期値：PSK
事前共有キー	［セキュリティ］を［WPA］、［WPA2］、［WPA/WPA2］に設定した場合に設定します。 8～63 文字以内
DTIM 間隔	DTIM 間隔は、ビーコン送信の何回毎に DTIM 情報を含めるかのインターバルを設定します。（DTIM とは無線 LAN の省電力モードの無線クライアントに対して、パケットが送信待ちであることを伝える情報です） ・初期値：1 回 ・設定範囲：１～255 回
キー更新間隔	［セキュリティ］を［WPA］、［WPA2］、［WPA/WPA2］に設定した場合に設定します。キーの更新間隔を入力します。 ・初期値：600 秒 ・設定範囲：1～86,400 秒
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

5．［変更］ボタンをクリックすると設定が一時保存され、「無線 LAN」ページに戻ります。［戻る］ボタンをクリックすると、設定した内容を反映しないで「無線 LAN」ページに戻ります。

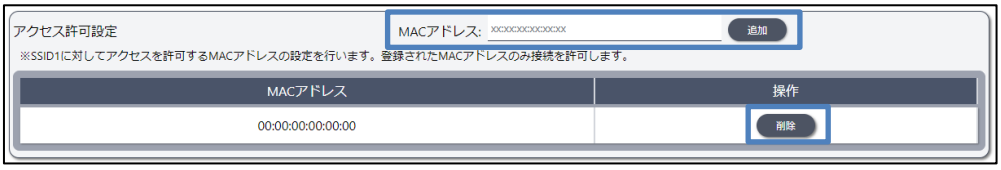
6．［設定］ボタンをクリックして、設定を反映させます。

3-3-3. アクセス許可設定

無線 LAN へのアクセスを許可する MAC アドレスの設定を行います。

> アクセス許可設定の MAC フィルタリング機能は、SSID1 にのみ有効となります。

1. ［MAC アドレスの追加］にて無線 LAN 接続を許可したい MAC アドレスを入力します。
［追加］をクリックすると MAC アドレスのリストに項目が追加されます。



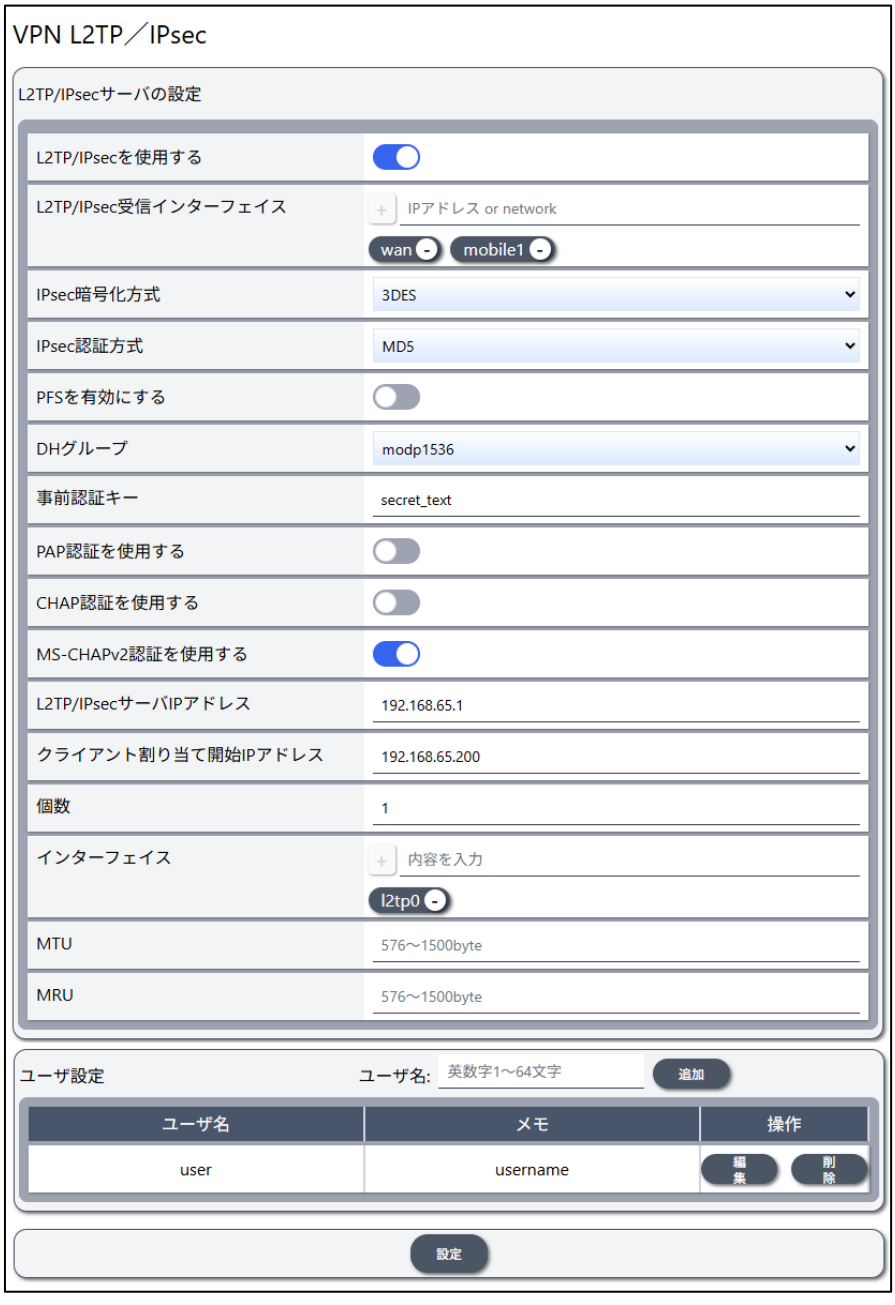
2. ［削除］をクリックすると、表示されている設定が削除されます。
3. ［設定］ボタンをクリックして、設定を反映させます。

3-4. VPN L2TP/IPsec

【L2TP/IPsec について】
L2TP/IPsec はパケット全体の暗号化の仕組みを持たない L2TP において IPsec を併用させることで、データの機密性や完全性を確保した VPN を実現します。2 台のコンピュータの間で情報を暗号化して送受信するので、インターネットを通じて安全に情報をやり取りできます。

- WindowsPC(Windows10 以降)より接続する場合、接続できないことがあります。接続できない場合は、弊社ホームページ（https://www.sun-denshi.co.jp/sc/product_service/router/）よりレジストリ変更のファイルをダウンロードし、レジストリ変更を行ってください。

5．　設定ツールのメニューから、［ネットワーク］－［VPN L2TP/IPsec］をクリックします。
「VPN L2TP／IPsec」リストのページが表示されます。



6．　L2TP/IPsec を使用する場合、［L2TP/IPsec を使用する］チェックをオンにします。

7．　以下の設定を行います。

項目	内容
L2TP/IPsec 受信インターフェイス	L2TP/IPsec パケットを受信する WAN 側の IP アドレス、もしくはネットワーク名を設定します。 受信インターフェイスは複数選択できます。
IPsec 暗号化方式	［3DES］または［AES256bit］のいずれかを選択します。
IPsec 認証方式	［MD5］、［SHA-1］、［SHA-256］、［SHA-384］、［SHA-512］のいずれかを選択します。
PFS を有効	PFS（Perfect Forward Secrity）を有効にする場合は、チェックをオンにします。
DH グループ	［modp1536］、［modp1024］、［modp2048］、［modp3072］、［modp4096］、［modp6144］、［modp8192］のいずれかを選択します。
事前認証キー	IPsec 通信を行うために使用する認証用キーフレーズを設定します。2 点間で同じ値を設定します。 使用できる文字は英数文字と、―（マイナス）、＿（アンダースコア）、@（アットマーク）、．（ピリオド）です。
PPP 認証方式	PPP 認証方式を選択します。 ［PAP］、［CHAP］、［MS-CHAPv2］から選択します。（複数選択することもできます。）
L2TP/IPsec サーバ IP アドレス	L2TP サーバ IP アドレスを設定します。 • L2TP サーバ IP は LAN(eth0) IP と異なるネットワーク IP を指定します。 ▶LAN IP：192.168.62.1　≠　L2TP/IPsec サーバ：192.168.63.1
クライアント割り当て開始 IP アドレス	クライアントに割り当てたい IP アドレスを設定します。 • 割り当て開始 IP アドレスは「L2TP/IPsec サーバ IP アドレス」と同じネットワークを設定します。 ▶L2TP サーバ：192.168.63.x ＝ 開始 IP アドレス:192.168.63.y •割り当て開始 IP アドレス、第 4 オクテット目は「L2TP/IPsec サーバ IP アドレス」第 4 オクテット目と異なる IP を指定します。 ▶L2TP サーバ：192.168.63.1 ＝ 開始 IP アドレス:192.168.63.2
個数	開始 IP アドレスからのアドレスの個数を指定します。ユーザの個数分指定します。 ▶［クライアント割り当て IP アドレス］を「192.168.63.150」、［個数］を「10」と設定した場合、「192.168.63.150～192.168.63.159」が、PPTP で使用する IP アドレスの範囲となります。
インターフェイス	L2TP/IPsec で使用する、インターフェイスを設定します。 ▶インターフェイスを設定する数は、「個数」で設定した数分追加する必要があります。 ➲ インターフェイスは『3-1-5.VPN』をご確認の上、設定してください。
MTU	MTU の値を設定します。
MRU	MRU の値を設定します。

8．　L2TP/IPsec 設定の追加を行いたい場合は、［追加］ボタンをクリックします。

9．　設定済みの項目を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「L2TP/IPsec の詳細設定」ページが表示されます。

１０. 以下の設定を行います。

項目	内容
ユーザー名	ユーザー名を表示します。
パスワード	認証させるパスワードを設定します。
固定 IP アドレス	固定 IP アドレスを設定します。 ▶指定しない場合、自動で IP アドレスが割り当てられます。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

１１. ［変更］ボタンをクリックすると設定が一時保存され、「L2TP/IPsec」リストのページに戻ります。
［戻る］ボタンをクリックすると、設定した内容を反映しないで「L2TP/IPsec」のリストのページに戻ります。

3-5. VPN PPTP

1．　設定ツールのメニューから、［ネットワーク］－［VPN PPTP］をクリックします。
「VPN PPTP」リストのページが表示されます。

2．　以下の設定を行います。

項目	内容
PPTP サーバを使用する	PPTP サーバを使用する場合は、チェックをオンにします。
認証方式（複数選択可）	認証方式を、[PAP]、[CHAP]、[MS-CHAPv2] より選択します。（複数選択可） ▶MS-CHAPv2 を選択した場合、［required］、［no40］、［no56］、［stateless］MPPE のオプション設定ができます。
PPTP サーバ IP アドレス	PPTP サーバ IP アドレスを設定します。 • PPTP サーバ IP は LAN(eth0) IP と異なるネットワーク IP を指定します。 ▶LAN IP：192.168.62.1　≠ PPTP サーバ：192.168.63.1
クライアント割り当て開始 IP アドレス	クライアントに割り当てたい IP アドレスを設定します。 • 割り当て開始 IP アドレスは「PPTP サーバ IP アドレス」と同じネットワークを設定します。 ▶PPTP サーバ：192.168.63.x ＝ 開始 IP アドレス:192.168.63.y •割り当て開始 IP アドレス、第 4 オクテット目は「PPTP サーバ IP アドレス」第 4 オクテット目と異なる IP を指定します。 ▶PPTP サーバ：192.168.63.1 ＝ 開始 IP アドレス:192.168.63.2
個数	開始 IP アドレスからのアドレスの個数を指定します。ユーザの個数分指定します。 ▶［クライアント割り当て IP アドレス］を「192.168.63.150」、［個数］を「10」と設定した場合、「192.168.63.150～192.168.63.159」が、PPTP で使用する IP アドレスの範囲となります。
インターフェイス	PPTP で使用する、インターフェイスを設定します。 ▶インターフェイス数は「個数」で設定した数分追加する必要があります。 ➲ インターフェイスは『3-1-5.VPN』をご確認の上、設定してください。
LCP エコーを使用する	LCP エコーを使用する場合は、チェックをオンにします。 ▶［LCP エコーを使用する］をオンにした場合、［LPC エコー監視回数］、［LPC エコー監視間隔］の閾値が設定できます。
LPC エコー監視回数	LPC エコー監視回数 1-10 （単位：回）を設定します。
LPC エコー監視間隔	LPC エコー監視間隔 1-60 （単位：秒）を設定します。
MTU	MTU の値を設定します。
MRU	MRU の値を設定します。

3．PPTP の設定を追加する場合は、［設定の追加］にて［ユーザ名］を入力し［追加］ボタンをクリックします。

設定済みの項目を変更する場合は、［編集］をクリックします。

［削除］をクリックすると、表示されている設定が削除されます。

［追加］ボタン、または［編集］をクリックすると、「PPTP の詳細設定」ページが表示されます。

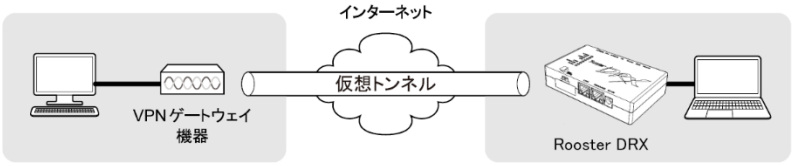
4．以下の設定を行います。

項目	内容
ユーザ名	認証させるユーザ名を設定します。
パスワード	認証させるパスワードを設定します。
固定 IP アドレス	固定 IP アドレスを設定します。 ▶指定しない場合、自動で IP アドレスが割り当てられます。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

5．［変更］ボタンをクリックすると設定が一時保存され、「PPTP」リストのページに戻ります。
［戻る］ボタンをクリックすると、設定した内容を反映しないで「PPTP」のリストのページに戻ります。

3-6. VPN IPsec

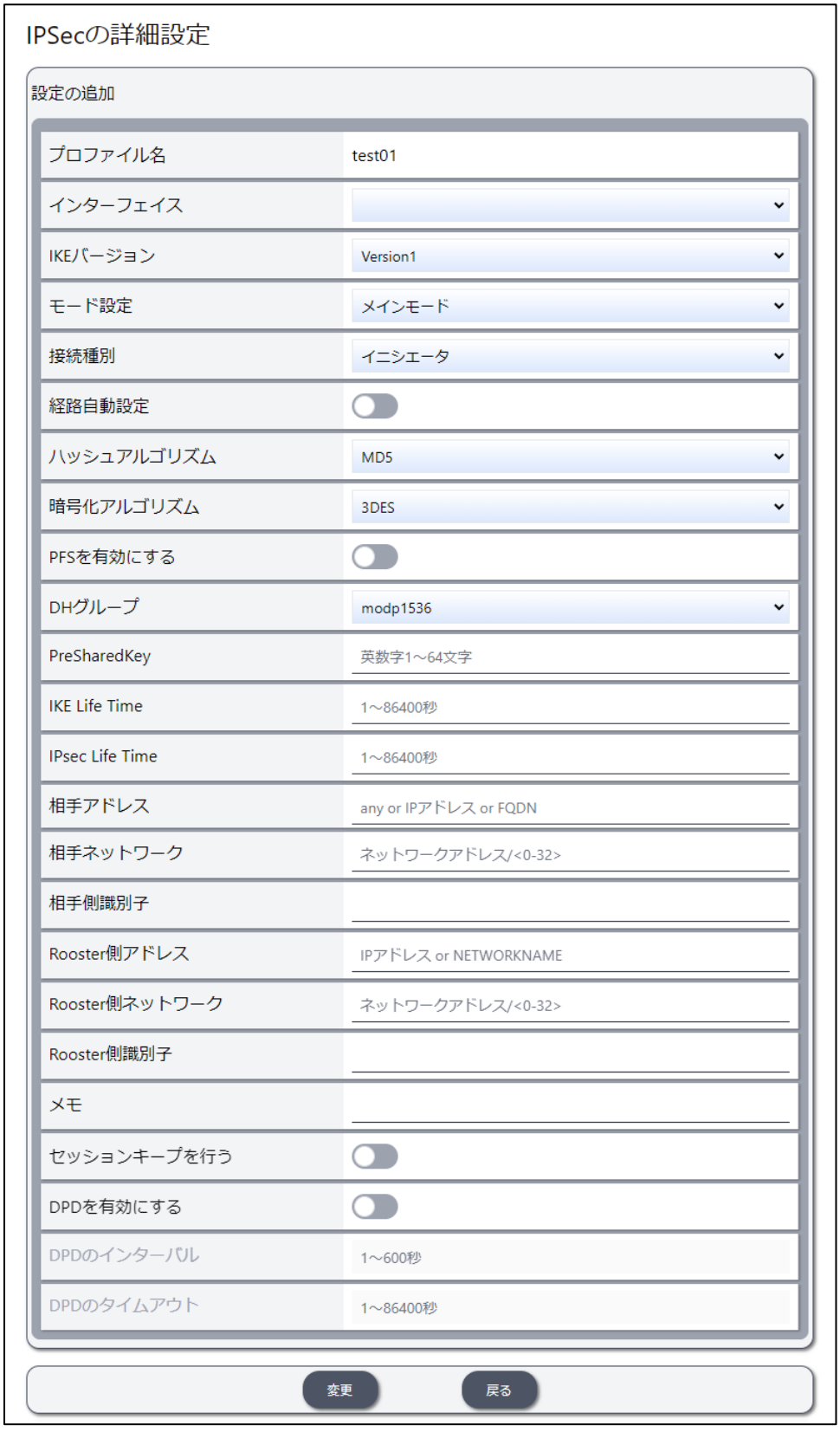
【IPsec について】
IPsec は暗号技術を用いて、IP パケット単位でデータの改ざん防止や秘匿機能を提供するプロトコルです。インターネットなどの公共的なネットワークで、あたかも専用線接続のような、秘匿性の高いネットワークを実現させるための仕組みです。



1．　設定ツールのメニューから、［ネットワーク］－［IPsec］をクリックします。
「IPsec」のページが表示されます。

2．　IPsec の設定を追加する場合は、［設定の追加］にて［プロファイル名］を入力し［追加］ボタンをクリックします。

設定済みの項目を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「IPsec の詳細設定」ページが表示されます。



3．　以下の設定を行います。

項目	内容
プロファイル名	プロファイル名を半角英数字で入力します。 プロファイル名は英文字を含めてください。数字だけのプロファイル名は無効となります。
インターフェイス	IPsec で使用する、インターフェイス『3-1. インターフェイス』を設定します。
IKE バージョン	IKE バージョン［Version 1］、［Version 2］のいずれかを選択します。
モード設定	［メインモード］または［アグレッシブモード］のいずれかを選択します。
接続種別	［イニシエータ］または［レスポンダ］のいずれかを選択します。 ［イニシエータ］は IKE 接続要求を行います。 ［レスポンダ］は IKE の待ち受けを行います。
経路自動設定	相手側、Rooster 側ネットワークアドレスの経路を自動的に設定する場合、オンにします。
ハッシュアルゴリズム	ハッシュアルゴリズムを設定します。 ［MD5］、［SHA-1］、［SHA-256］、［SHA-384］、［SHA-512］のいずれかを選択します。
暗号化アルゴリズム	［AES256bit］または［3DES］のいずれかを選択します。
PFS を有効にする	PFS（Perfect Forward Security）を有効にする場合は、チェックをオンにします。
DH グループ	［modp1536］、［modp1024］、［modp2048］、［modp3072］、［modp4096］、［modp6144］、［modp8192］のいずれかを選択します。
PreSharedKey	IPsec 通信を行うために使用する英数文字列の認証用キーフレーズを設定します。2 点間で同じ値を設定します。 使用できる文字は英数文字と、―（マイナス）、＿（アンダースコア）、@（アットマーク）、．（ピリオド）です。
IKE Life Time	IKE の寿命を秒単位で指定します。 ▶1200 秒以上 86400 秒以内で設定してください。
IPsec Life Time	IPsec の寿命を秒単位で指定します。 ▶1200 秒以上 86400 秒以内で設定してください。
相手 IP アドレス	IPsec 通信を行う相手先のグローバル IP アドレスを指定します。ホスト名での指定も可能です。モード設定が［アグレッシブ］で接続種別が［レスポンダ］の場合、相手 IP アドレスには「0.0.0.0」と設定してください。
相手ネットワーク	IPsec 通信を行う相手先のローカルネットワークアドレスとサブネットマスクを「A.B.C.D/E」形式で指定します。(相手側 ID)
相手側識別子	アグレッシブモードで接続する際に、IPsec 通信で互いに相手を識別するために設定します。2 点間で同じ値を設定します。「@」を含んだ文字列にて指定します。例）@test もしくはグローバル IP アドレスを設定する必要がある場合があります。
Rooster 側 IP アドレス	メインモードで接続する際に Rooster に割り当てられるグローバル IP アドレスを指定します。ホスト名での指定も可能です。 また、以下に示すネットワークインターフェイスでの指定も可能です。 lan : LAN wan : WAN mobile1 : モバイル通信端末
Rooster 側ネットワーク	Rooster 側のローカルネットワークアドレスとサブネットマスクを「A.B.C.D/E」形式で指定します。(Rooster 側 ID)
Rooster 側識別子	アグレッシブモードで接続する際に、IPsec 通信で互いに相手を識別するために設定します。2 点間で同じ値を設定します。「@」を含んだ文字列にて指定します。例）@test もしくはグローバル IP アドレスを設定する必要がある場合があります。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

項目	内容
セッションキープを行う	チェックをオンにした場合、IPsec 接続が切断されると、自動的に再接続を行うようになります。接続種別で［レスポンダ］を選択された場合は、チェックをオンにしても動作しません。
DPD を有効にする	チェックをオンにした場合、IPsec 接続が切断されると、リアルタイムに切断を検出するようになります。 DPD 有効時［DPD のインターバル］、［DPD のタイムアウト］の閾値が設定できます。

4．［変更］ボタンをクリックすると設定が一時保存され、「IPsec」リストのページに戻ります。
［戻る］ボタンをクリックすると、設定した内容を反映しないで「IPsec」のリストのページに戻ります。

- IPsec の接続が完了するまでに 1 ～3 分程度かかります。通信を行う前に、ping コマンド等で接続状態を確認することをお勧めします。
- DPD を有効にする際は対向機の DPD 設定も有効にしてください。
- 本製品の LAN ポートが LINK していない場合、相手のネットワークから LAN 側 IP へのアクセスができません。

以下の条件で「Rooster 側識別子」設定項目に Rooster 側のグローバル IP を設定する必要があります。
・「モード設定」が「メインモード」の場合

他社製 IPsec 機器と接続を行う場合、以下の表を参考に設定を行ってください。

DRX 既定の IPsec 接続設定

項目	既定の設定内容
基本設定	
データ圧縮（IPcomp プロトコル）	圧縮は使用しない。
鍵交換方式	IKE（Internet Key Exchange）を使って、SA の合意を通信時に自動的に行う。（手動設定は行わない。）
IKE の設定	
接続試行回数	無限回（制限なし）
ハッシュアルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
認証方式	Pre-Shared Key（共通鍵）認証方式
Pre-Shared Key （共通鍵）の設定	自分側と相手側両方に、同じキーフレーズを設定。
暗号化アルゴリズム	AES256bit、3DES
Diffie-Hellman-Group	DH Group 2
識別子（ホスト ID）	「@」を含んだ文字列にて指定 もしくはグローバル IP アドレス
IKE Life Time	経過時間による設定のみ。
IKE フェーズ 2 （IPsec SA の作成） の設定	
セキュリティプロトコル	ESP のみ。
IPsec Life Time	経過時間による設定のみ。
カプセル化モード	トンネリングモード
暗号化アルゴリズム	AES256bit、3DES
ハッシュアルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
PFS（Diffie-Hellman の再計算）	設定により行います。

- 必要に応じて、IPsec 対向機の NAT トラバーサルを有効にしてください
- IKE Version1 では暗号化アルゴリズム「AES256bit」、ハッシュアルゴリズム「SHA-256」の組み合わせは使用できません、IKE Version2 は設定できます。

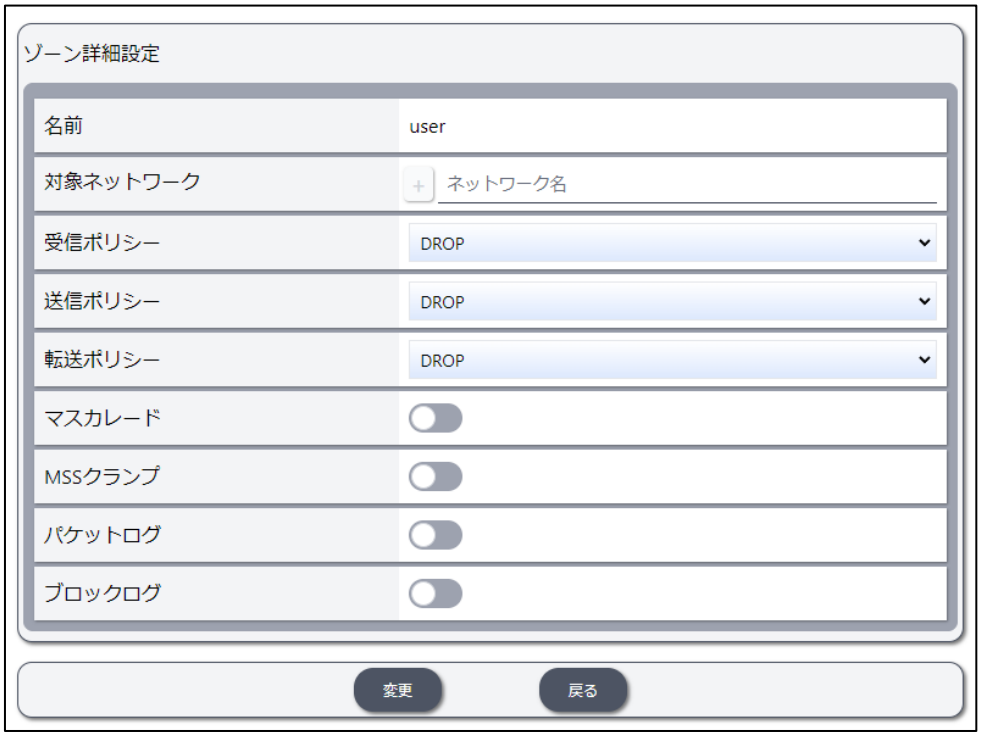
3-7. ファイアウォール基本設定

1．　設定ツールのメニューから、［ネットワーク］－［ファイアウォール基本設定］をクリックします。
「ファイアウォール基本設定」リストのページが表示されます。

2．　ファイアウォールの「デフォルトポリシー設定」、「オプションを設定」を変更する場合、
以下の設定を行います。

項目	内容
デフォルトポリシー設定	受信：Input のデフォルトポリシー設定します。 ▶受け付ける［ACCEPT］、拒絶する［REJECT］、破棄する［DROP］のいずれかを指定します。 送信：Output のデフォルトポリシー設定します。 ▶受け付ける［ACCEPT］、拒絶する［REJECT］、破棄する［DROP］のいずれかを指定します。 転送：Forward のデフォルトポリシー設定します。 ▶受け付ける［ACCEPT］、拒絶する［REJECT］、破棄する［DROP］のいずれかを指定します。
オプション設定	syn-flood 保護：SYN フラッド攻撃対策を有効にする場合、オンにします。
	drop-invalid 無効：無効なパケットを遮断する場合、オンにします。
	ゾーンに属さないパケットの通過ログ有効：通過ログを記録する場合、オンにします。
	ゾーンに属さないパケットの遮断ログ有効：遮断ログを記録する場合、オンにします。

3．「ゾーンの設定」を追加する場合は、［ゾーン名］を入力し［追加］ボタンをクリックします。
設定済みの項目を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「ゾーンの詳細設定」ページが表示されます。

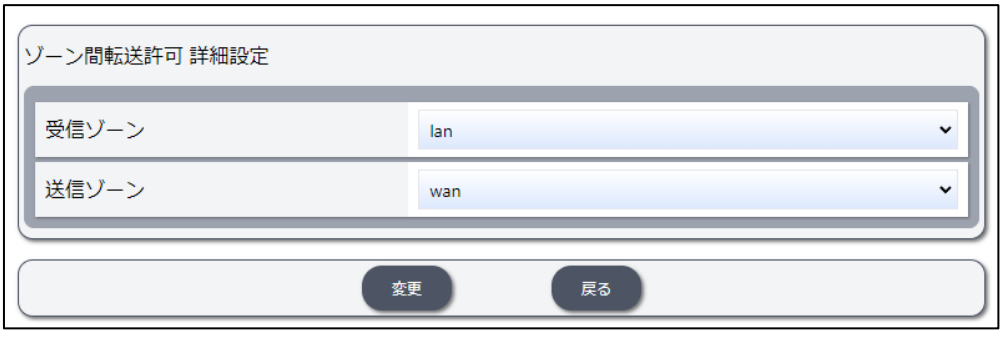


4．　以下の設定を行います。

項目	内容
名前	ゾーン名を表示します。
対象ネットワーク	ゾーンに対象ネットワークを設定します。 ▶対象ネットワークを設定する場合は、ネットワーク名に入力すると［＋］ボタンが有効になります、［＋］ボタンを押すとネットワークリストに登録されます。 ▶ネットワーク名入力→［＋］押下で複数の対象ネットワークが登録できます。
受信ポリシー	ゾーンの受信（INPUT）ポリシーを選択します。 ▶受け付ける［ACCEPT］、拒絶する［REJECT］、破棄する［DROP］のいずれかを指定します。
送信ポリシー	ゾーンの送信（OUTPUT）ポリシーを選択します。 ▶受け付ける［ACCEPT］、拒絶する［REJECT］、破棄する［DROP］のいずれかを指定します。
転送ポリシー	ゾーンの転送（FORWARD）ポリシーを選択します。 ▶受け付ける［ACCEPT］、拒絶する［REJECT］、破棄する［DROP］のいずれかを指定します。
マスカレード	マスカレード（ゾーン NAT）を使用する場合、オンにします。 ▶オンにした場合、転送パケットの送信元 IP の書き換えを行います。
MSS クランプ	MSS クランプ（mss-clamp）を使用する場合、オンにします。
パケットログ	ゾーンを通過するパケットログを記録する場合、オンにします。 ➲『5-15.通過ログ』にパケットを表示する場合は［オプション設定］の［ゾーンに属さないパケットの通過ログ有効］をオンにする必要があります。
ブロックログ	ゾーンに遮断されたパケットログを記録する場合、オンにします。 ➲『5-16.遮断ログ』にパケットを表示する場合は［オプション設定］の［ゾーンに属さないパケットの遮断ログ有効］をオンにする必要があります。

5．「ゾーン間転送許可設定」を追加する場合は、［追加］ボタンをクリックします。

設定済みの項目を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「ゾーン間転送許可設定」ページが表示されます。



6．　以下の設定を行います。

項目	内容
受信ゾーン	受信ゾーンに使用するネットワークを選択します。
送信ゾーン	送信ゾーンに使用するネットワークを選択します。

7．［ファイアウォール 基本設定］変更後［設定］ボタンをクリックして、設定内容を反映させます。

3-8. ファイアウォールフィルタ

1．　設定ツールのメニューから、［ネットワーク］－［ファイアウォールフィルタ］をクリックします。
「ファイアウォールフィルタ」リストのページが表示されます。

DRX の設定を行う WebUI や CLI の接続を許可する設定は、以下の環境
・DRX の設定を行う GUI や CLI を表示する機器とルータ間の通信経路全体が閉域網等保護されたネットワークで完結する環境
・IPSec 接続設定を行う等により通信経路の全体にわたって保護される環境
のいずれかのみで使用し、インターネットに接続している環境では接続を許可にする設定はしないでください。

2．「フィルタ設定」を追加する場合は、［追加］ボタンをクリックします。

設定済みの項目を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「ファイアウォールフィルタ」ページが表示されます。

3．　以下の設定を行います。

項目	内容
No.	ファイアウォールフィルタリング設定の通し番号が表示されます。
有効	設定のファイアウォールフィルタリングを使用の場合、チェックをオンにします。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。
プロトコル	フィルタの protocol を設定します。 プロトコル番号の入力　または［ah］、［esp］、［gre］、［icmp］、［tcp］、［udp］のいずれか指定します。 ［all］：全てのプロトコルを対象になります。 ▶プロトコル番号、プロトコル名を入力すると［＋］ボタンが有効になります、［＋］ボタンを押すとプロトコルリストに登録されます。
ICMP タイプ	許可したい ICMP タイプを以下のタイプのいずれか指定します。 ［address-mask-reply］、［address-mask-request］、［communication-prohibited］、［destination-unreachable］、［echo-reply］、［echo-request］、［fragmentation-needed］、［host-precedence-violation］、［host-prohibited］、［host-redirect［host-unknown］、［host-unreachable］、［ip-header-bad］、［network-prohibited］、［network-redirect］、［network-unknown］、［network-unreachable］、［parameter-problem］、［port-unreachable］、［precedence-cutoff］、［protocol-unreachable］、［redirect］、［required-option-missing］、［router-advertisement］、［router-solicitation］、［source-quench］、［source-route-failed］、［time-exceeded］、［timestamp-reply］、［timestamp-request］、［tos-host-redirect］、［tos-host-unreachable］、［tos-network-redirect］、［tos-network-unreachable］、［ttl-zero-during-reassembly］、［ttl-zero-during-transit］ ［any］：全ての ICMP タイプを許可します。 ▶ICMP タイプを入力すると［＋］ボタンが有効になります、［＋］ボタンを押すとプロトコルリストに登録されます。
フィルタタイプ	フィルタのタイプを設定します。 ［受信ルール（INPUT）］、［送信ルール（OUTPUT）］、［転送ルール（FORWARD）］のいずれか指定します。
送信元ゾーン	送信元ゾーンを設定します。 ➲『3-7.ファイアウォール基本設定』の「ゾーン設定」で登録している設定している「ゾーン名」が表示されます。 [any]：全てのゾーンを対象になります。
送信元 IP	フィルタリングを行う送信元 IP アドレスを設定します。
送信元ポート	フィルタリングを行う送信元ポート番号を、1～65535 の番号を指定します。 又は「-」記号を開始、終了ポートの間に入れ、<1～65535>- <1～65535>形式で範囲指定します。
宛先 IP	フィルタリングを行う宛先 IP アドレスを設定します。
宛先ポート	フィルタリングを行うポート番号を、1～65535 の番号を指定します。 １つのポートのみを登録する場合、開始ポートのみを入力します。 又は「-」記号を開始、終了ポートの間に入れ、<1～65535>- <1～65535>形式で範囲指定します。
送信元 MAC アドレス	フィルタリングを行う送信元 MAC アドレスを設定します。
その他	l2tp にて、ipsec 暗号化されたパケットのみ通過させる拡張設定を行う。 その他は［none］、［L2TP/IPsec Accept］のいずれかを設定します。 ▶None を選択すると無効になります。 ▶L2TP/IPsec Accept を選択すると設定が有効になります。

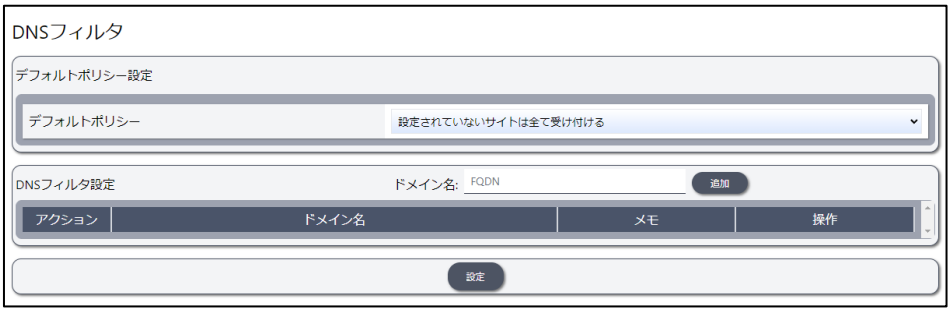
4．［ファイアウォールフィルタ］変更後［設定］ボタンをクリックして、設定内容を反映させます。

3-9. DNSフィルタ

【DNS フィルタリングについて】
・DNS フィルタリングは本製品の DNS サービスの DNS リレー機能で実現し、本製品と後位端末から問い合わせのあった DNS クエリに対してフィルタリングを行います。
・後位端末が直接ネット上の DNS サーバにアクセスした場合、本機能は機能しませんので、ご注意ください。

1．　設定ツールのメニューから［ネットワーク］－［DNS フィルタ］をクリックします。

「DNS フィルタ」リストのページが表示されます。



2．　DNS フィルタリング設定を行った項目以外のサイトのアクセスをどう処理するかにより、「基本ポリシー」の

・「設定されていないサイトはすべて通す」
・「設定されていないサイトはすべて遮断する」

のうちいずれかを選択します。

3．　DNS フィルタリングの設定を追加する場合は、［設定の追加］にて［ドメイン名］を入力し、［追加］ボタンをクリックします。
既存の設定を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「DNS フィルタの詳細設定」ページが表示されます。

4．　以下の設定を行います。

項目	内容
ドメイン名を入力	DNS フィルタリングを行うドメイン名（サイト）を半角で入力します。 ・入力文字範囲：1～253
動作	［受け付ける］、［遮断する］のいずれかを指定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

5．［変更］ボタンをクリックすると設定が一時保存され、「DNS フィルタリング」リストのページに戻ります。［戻る］ボタンをクリックすると、設定した内容を反映しないで「DNS フィルタリング」のリストのページに戻ります。

memo
・DNS フィルタリングにドメイン名を追加後、サイトの「許可」「遮断」の動作確認はコマンド実行の nslookup でご確認ください。
➲ nslookup については『6-14. コマンド実行』をご覧ください。
・Windows PC の場合、DNS 情報を保持（キャッシュ）しているため、正常な動作が確認できない可能性があります、PC の DNS キャッシュを削除して確認する場合はコマンドプロンプト(cmd) にて「ipconfig /flushdns」で削除することができます。（「ipconfig /displaydns」で PC の DNS 情報が確認できます）
・「設定されていないサイトはすべて遮断する」設定で使用する場合、本製品自身が使用するドメイン名を許可に設定ください。
（SunDMS、suncomm.DDNS、SMTP サーバ、ハートビート設定など）

memo
・設定のドメイン名の DNS フィルタリング判定は完全一致、後方一致になります。
例）
設定ドメイン名：「sun-denshi.co.jp」　　動作：遮断

完全一致：sun-denshi.co.jp	遮断する
後方一致：www.sun-denshi.co.jp	遮断する
前方一致：sun-denshi.example.co.jp	遮断しない
部分一致：www.sun-denshi.co.jp.example.com	遮断しない

3-10. NAT

1．　設定ツールのメニューから［ネットワーク］－［NAT］をクリックします。

「NAT」リストのページが表示されます。

2．　送信先 NAT（DNAT）設定を追加する場合は、［設定の追加］にて［シーケンス番号］を入力し、［追加］ボタンをクリックします。

既存の設定を変更する場合は、［編集］をクリックします。

［削除］をクリックすると、表示されている設定が削除されます。

［追加］ボタン、または［編集］をクリックすると、「送信先 NAT の詳細設定」ページが表示されます。

3．　以下の設定を行います。

項目	内容
No	送信先 NAT の設定番号が表示されます。
有効	送信先 NAT を有効にする場合はオンにします。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。
プロトコル	プロトコル番号もしくは［all］、［ah］、［esp］、［gre］、［icmp］、［TCP］、［UDP］のいずれかを指定します。
送信元ゾーン	送信元に使用するゾーンを選択します。 ➲ ゾーンリストは『3-7.ファイアウォール基本設定』の「ゾーン設定」で設定が表示されます。
宛先ゾーン	宛先に使用するゾーンを選択します。 ➲ ゾーンリストは［any］と『3-7.ファイアウォール基本設定』の「ゾーン設定」で設定とが表示されます。
送信元 IP	送信元の IP アドレス、もしくは CIDR を設定します。
送信元ポート	送信元のポート番号 1 ～65535 を設定します。 又は「-」記号を開始、終了ポートの間に入れ、<1～65535>- <1～65535>形式で範囲指定します。
宛先 IP	宛先の IP アドレス、もしくは CIDR を設定します。
宛先ポート	宛先のポート番号 1 ～65535 を設定します。 又は「-」記号を開始、終了ポートの間に入れ、<1～65535>- <1～65535>形式で範囲指定します。
書換後の宛先 IP アドレス	書換後の宛先 IP アドレスを設定します。
書換後の宛先ポート	書換後の宛先ポート番号 1 ～65535 を設定します。

SimpleWeb 設定ツールの「バーチャルサーバ」機能はこちらの送信先 NAT で実現可能です。

4．　［変更］ボタンをクリックすると設定が一時保存され、「NAT」リストページに戻ります。

［戻る］ボタンをクリックすると、設定した内容を反映しないで「NAT」リストページに戻ります。

5．　送信元 NAT（SNAT）設定を追加する場合は、［設定の追加］にて［シーケンス番号］を入力し、［追加］ボタンをクリックします。
既存の設定を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「送信元 NAT の詳細設定」ページが表示されます。

6．　以下の設定を行います。

項目	内容
No	送信元 NAT の設定番号が表示されます。
有効	送信元 NAT を有効にする場合はオンにします。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。
プロトコル	プロトコル番号もしくは［all］、［ah］、［esp］、［gre］、［icmp］、［TCP］、［UDP］のいずれかを指定します。
送信元ゾーン	送信元に使用するゾーンを選択します。 ➲ ゾーンリストは［any］と『3-7.ファイアウォール基本設定』の「ゾーン設定」で設定が表示されます。
宛先ゾーン	宛先に使用するゾーンを選択します。 ➲ ゾーンリストは『3-7.ファイアウォール基本設定』の「ゾーン設定」で設定とが表示されます。
送信元 IP	送信元の IP アドレス、もしくは CIDR を設定します。
送信元ポート	送信元のポート番号 1 ～65535 を設定します。 又は「-」記号を開始、終了ポートの間に入れ、<1～65535>- <1～65535>形式で範囲指定します。
宛先 IP	宛先の IP アドレス、もしくは CIDR を設定します。
宛先ポート	宛先のポート番号 1 ～65535 を設定します。 又は「-」記号を開始、終了ポートの間に入れ、<1～65535>- <1～65535>形式で範囲指定します。
書換後の送信元 IP アドレス	書換後の送信元 IP アドレスを設定します。
書換後の送信元ポート	書換後の送信元ポート番号 1 ～65535 を設定します。

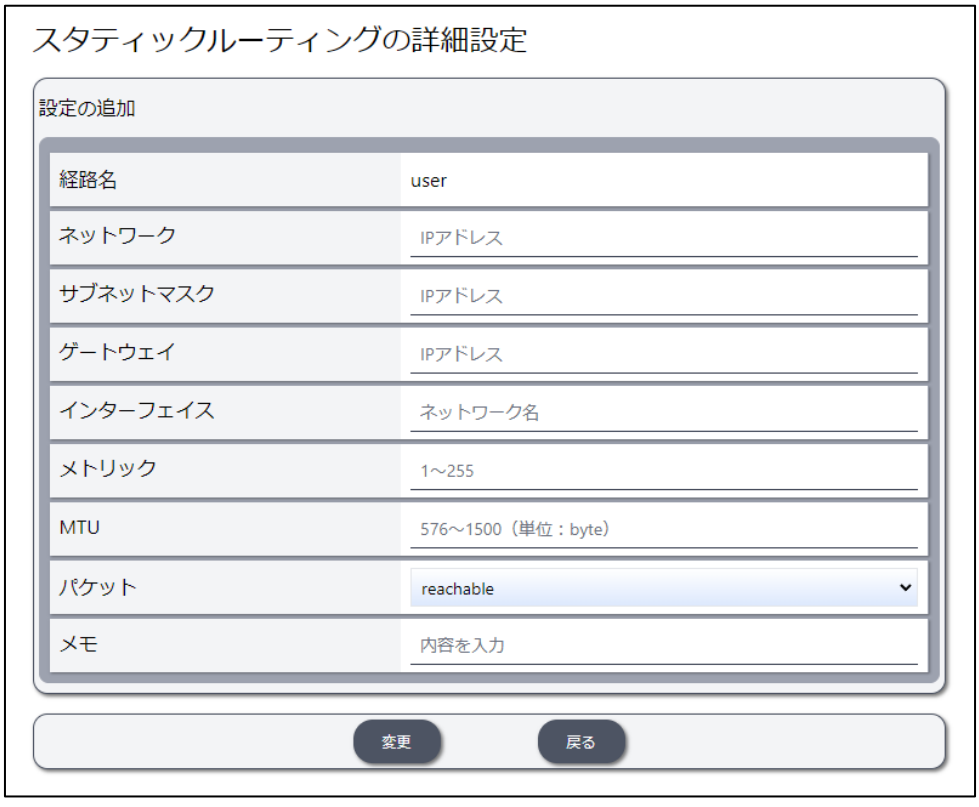
7．［変更］ボタンをクリックすると設定が一時保存され、「NAT」リストのページに戻ります。［戻る］ボタンをクリックすると、設定した内容を反映しないで「NAT」のリストのページに戻ります。

8．［設定］ボタンをクリックして、設定内容を反映させます。

3-11. スタティックルーティング

1．　設定ツールのメニューから、［ネットワーク］－［スタティックルーティング］をクリックします。
「スタティックルーティング」リストのページが表示されます。

2．　スタティックルートの設定を追加する場合は、［経路名］を入力し、［追加］ボタンをクリックします。
設定済みのスタティックルーティング設定を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「スタティックルーティングの詳細設定」ページが表示されます。



3．　以下の設定を行います。

項目	内容
経路名	経路名が表示されます。
ネットワーク	宛先ネットワークアドレスを入力します。
サブネットマスク	上記ネットワークのサブネットマスクを入力します。
ゲートウェイ	上記ネットワークのゲートウェイアドレスを入力します。
インターフェイス	インターフェイスはネットワーク名を設定します。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。
メトリック	経路のメトリック値 1 ～255 を入力します。
MTU	経路の MTU 値 576～1500（単位：byte）を入力します。
パケット	経路の状態［reachable］、［unreachable］、［blackhole］のいずれかを選択します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

4．［変更］ボタンをクリックすると設定が一時保存され、「スタティックルーティング」リストのページに戻ります。
［戻る］ボタンをクリックすると、設定した内容を反映しないで「スタティックルーティング」リストページに戻ります。

5．［設定］ボタンをクリックして、設定内容を反映させます。

4章　各種サービス

この章では、ネットワークをより快適に利用するための各種サービスの設定について説明します。

4-1. ダイナミックDNS

1．　設定ツールのメニューから、［各種サービス］－［ダイナミック DNS］をクリックします。
「ダイナミック DNS」のページが表示されます。

2．［ダイナミック DNS サービスを利用する］チェックをオンにし、以下の設定を行います。

項目	内容
インターフェイス	どのインターフェイスのグローバル IP アドレスを通知するかを選択します。 ［WAN］、［モバイル通信端末］、［自動］ のいずれかを指定します。 ▶［自動］の場合、デフォルトゲートウェイのインターフェイスとなります。 デフォルトルートに設定するインターフェイスを指定してください。
アドレスの確認間隔	指定されたダイナミック DNS サービスに、設定された時間（分）ごとに確認を行います。 ・設定範囲：5～9999
DDNS の強制更新間隔	指定されたダイナミック DNS サービスへ、設定された時間（分）ごとに更新を行います。強制更新間隔は、アドレスの確認間隔より長い時間を設定してください。 ・設定範囲：5～9999
サービスの種類	アドレス解決に使用するダイナミック DNS サービスを選択します。 ［suncomm.DDNS］、［その他］ のいずれかを指定します。 ダイナミック DNS サービスとして suncomm.DDNS を使用される場合は、別途契約または登録が必要となります。詳細につきましては、下記の URL をご覧ください。 「suncomm.DDNS」 https://www.sun-denshi.co.jp/sc/product_service/service/ddns ▶サン電子（株）が運用する有償でのダイナミック DNS サービスです。別途、ご契約が必要となりますので、上記 URL をご覧ください。また、「suncomm.DDNS」機能を利用して、お客様独自にダイナミック DNS サーバを設置・運用いただくことも可能です。「suncomm.DDNS」のプロトコル仕様につきましては、機密保持契約成立後、開示させていただきます。なお、本件は法人のお客様に限らせていただきます。

3．ダイナミック DNS 提供事業者から発行された［サーバ名］、［ホスト名］、［アカウント］、［パスワード］を入力します。

4．［設定］ボタンをクリックして、設定内容を反映させます。

- プライベート IP の場合、通知は行いません。
- アドレス解決のダイナミック DNS サービスと回線バックアップを併用しないようにしてください。
- アドレス解決のダイナミック DNS サービスは、デフォルトルートを 2 つ以上の設定には対応しておりません。

4-2. DNS

1. 設定ツールのメニューから、［各種サービス］－［DNS］をクリックします。
「DNS」のページが表示されます。

2. 全てのネットワークからの問い合わせに応答する場合は、「同一ローカルネットワークからの問い合わせのみ応答する」を無効に設定します。

3. DNS リレーをするサーバを指定する場合は、「サーバ IP アドレス」を入力すると［＋］ボタンが有効になり、［＋］ボタンを押すとリストに登録されます。

4. DNS ホストを追加する場合は、［ドメイン名］を入力し、［追加］ボタンをクリックします。
設定済みの DNS ホストを変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「DNS」ページが表示されます。

5. 以下の設定を行います。

項目	内容
ドメイン名	ドメイン名が表示されます。
IP アドレス	IP アドレスを入力します。

6．［変更］ボタンをクリックすると設定が一時保存され、「DNS」ページに戻ります。
［戻る］ボタンをクリックすると、設定した内容を反映しないで「DNS」ページに戻ります。

7．［設定］ボタンをクリックして、設定内容を反映させます。

4-3. DHCP

1．　設定ツールのメニューから、［各種サービス］－［DHCP］をクリックします。
「DHCP」のページが表示されます。

2．「DHCP 設定」
DHCP を追加する場合は、［DHCP サーバ名］を入力し、［追加］ボタンをクリックします。
設定済みの DHCP サーバ設定を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「DNS」ページが表示されます。

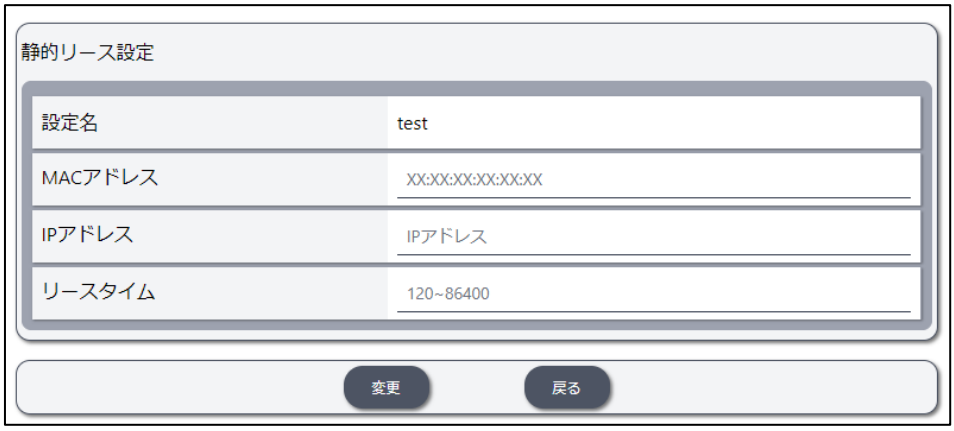
3．　以下の設定を行います。

項目	内容
有効	DHCP サーバを有効にする場合は、チェックをオンにします。
動的 IP アドレスのリース	DHCP サーバの動的アドレスの割り当ての有効／無効設定を行います。
リース開始 IP アドレス	割り当てる IP アドレスの開始アドレスを入力します。
リース終了 IP アドレス	割り当てる IP アドレスの終了アドレスを入力します。 ▶初期設定では、［リース開始 IP アドレス］が「192.168.62.100」、［リース終了 IP アドレス］が「192.168.62.149」と設定されています。

項目	内容
ネットマスク	DHCP サーバより配信する IP アドレスのネットマスクを設定します。
ゲートウェイ	ゲートウェイは複数登録可能で［＋］ボタンが有効になり、［＋］ボタンを押すとリストに登録されます。
DNS サーバ	DNS サーバは複数登録可能で［＋］ボタンが有効になり、［＋］ボタンを押すとリストに登録されます。

［対象ネットワーク］が「lan」の場合、［リース開始・終了 IP アドレス］項目は lan のインターフェイス設定の IP ネットワークのアドレスが使用されます。
［対象ネットワーク］が「lan」以外の場合は、設定どおりに動作します。

4．静的リースを追加する場合は、［設定名］を入力し、［追加］ボタンをクリックします。
設定済みの DHCP サーバ設定を変更する場合は、［編集］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［編集］をクリックすると、「DNS」ページが表示されます。



5．以下の設定を行います。

項目	内容
設定名	DHCP サーバの静的 IP アドレス設定名が表示されます。
MAC アドレス	DHCP サーバの静的 IP アドレスに使用する MAC アドレスを入力します。
IP アドレス	IP アドレスを入力します。
リースタイム	リースタイム 120-86400（単位：秒）を設定します。

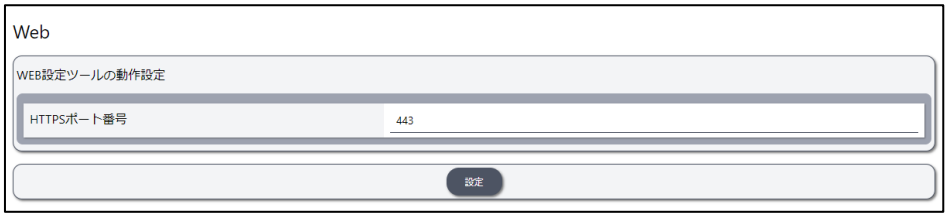
6．［変更］ボタンをクリックすると設定が一時保存され、「DHCP」ページに戻ります。
［戻る］ボタンをクリックすると、設定した内容を反映しないで「DHCP」ページに戻ります。

7．［設定］ボタンをクリックして、設定内容を反映させます。

4-4. Web

1．　設定ツールのメニューから、［各種サービス］－［Web］をクリックします。

「Web」のページが表示されます。



2．　以下の設定を行います。

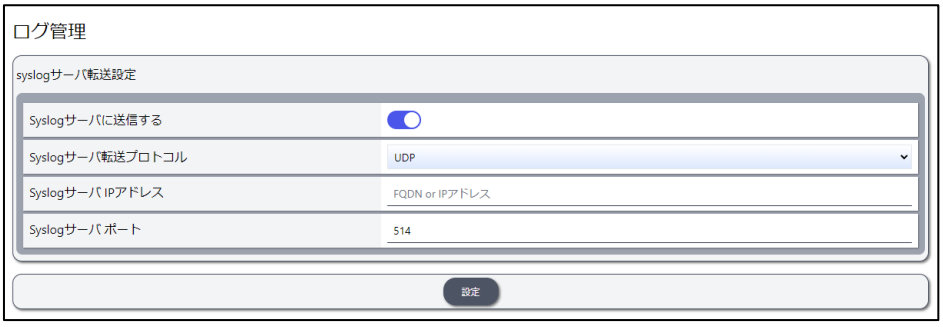
項目	内容
HTTPS ポート番号	アドバンスト Web 設定ツールのポート 1 ～65535 を入力します。

3．［設定］ボタンをクリックして、設定内容を反映させます。

ポート番号を DRX が使用するポート番号（SSH : 22、DNS : 53、IPsec : 500／4500、PPTP : 1723、L2TP : 1701 など）は設定しないでください。設定すると Web 設定画面にアクセスできなくなります

4-5. syslogサーバ転送

1．　設定ツールのメニューから、［各種サービス］－［syslog サーバ転送］をクリックします。
「syslog サーバ転送」のページが表示されます。



2．　以下の設定を行います。

項目	内容
Syslog サーバに送信する	「Syslog サーバに送信する」を有効にする場合は、チェックをオンにします。
Syslog サーバ転送プロトコル	転送する syslog メッセージのプロトコルを指定します。
Syslog サーバ IP アドレス	ユーザログを転送する syslog サーバのアドレスまたは FQDN を設定します。
Syslog サーバ ポート	ユーザログを転送する syslog サーバのポート 1 ～65535 を設定します。

3．　［設定］ボタンをクリックして、設定内容を反映させます。

4-6. SunDMS

1．　設定ツールのメニューから、［各種サービス］－［SunDMS］をクリックします。
「SunDMS」のページが表示されます。

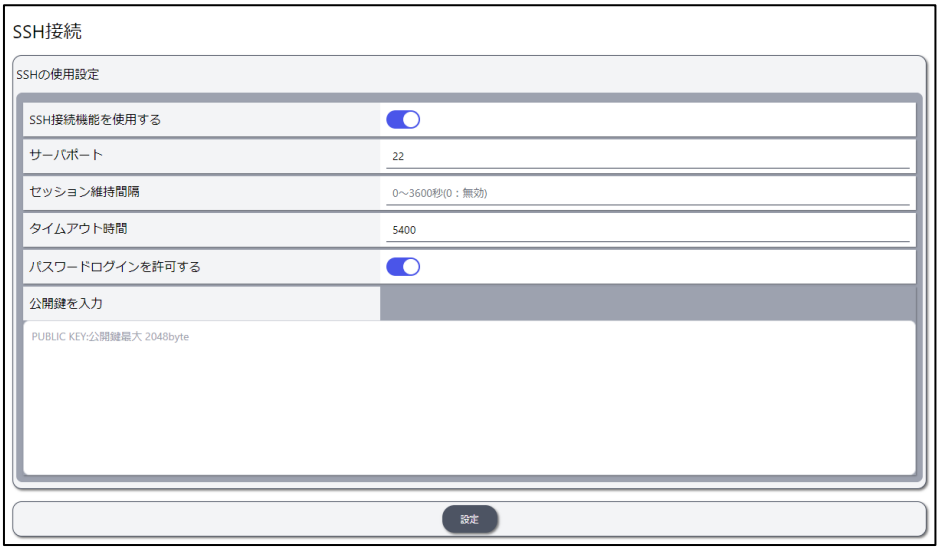
2．　以下の設定を行います。

項目	内容
SunDMS 機能を使用する	「SunDMS 機能を使用する」を有効にする場合は、チェックをオンにします。
SunDMS サーバ名	SunDMS サーバ名のアドレスまたは FQDN を指定します。
ポート番号	SunDMS サーバの接続先ポート番号 1 ～65535 を設定します。
プロキシサーバアドレス	プロキシサーバのアドレスまたは FQDN を設定します。
プロキシサーバポート番号	プロキシサーバポート番号 1 ～65535 を設定します。

3．　［設定］ボタンをクリックして、設定内容を反映させます。

4-7. SSH接続

1．　設定ツールのメニューから、［各種サービス］－［SSH 接続］をクリックします。
「SSH 接続」のページが表示されます。



2．　以下の設定を行います。

項目	内容
SSH 接続機能を使用する	「SSH 接続機能を使用する」を有効にする場合は、チェックをオンにします。
サーバポート	SSH サーバの接続先ポート番号 1 ～65535 を設定します。
セッション維持間隔	SSH サーバとの SSH セッション維持のためのデータを送信する間隔を設定します。
タイムアウト時間	SSH サーバとのタイムアウト時間を設定します。
パスワードログインを許可する	SSH サーバのパスワードログインの有効にする場合は、チェックをオンにします。 ▶無効にする場合は公開鍵設定をしておかないとログインできなくなります。公開鍵の設定につきましては『公開鍵を入力』に公開鍵を入力してください。
公開鍵を入力	root ユーザの SSH 公開鍵を設定します。 公開鍵データの「鍵値」のみを入力します。 設定例： AAAAB3Nza...(省略)...U6cv7nNloO7OWUBhMue38z1FRB5Uhu0ZkskJVot

3．　［設定］ボタンをクリックして、設定内容を反映させます。

memo　ログインしているアカウントの設定を行います。

4-8. トリガー

1. 設定ツールのメニューから、［各種サービス］－［トリガー］をクリックします。
「トリガー設定」のページが表示されます。

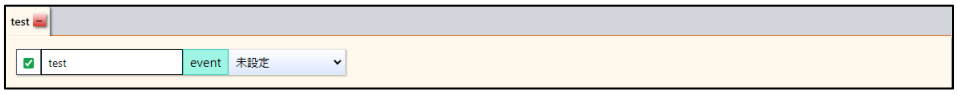
2. ［追加するトリガー名]を入力し、［+］ボタンをクリックするとトリガーの追加ができます。

トリガー機能は設定されたイベントを契機に複数のアクションを行う機能です。
トリガーイベントが発生したら、設定したアクションをシーケンス番号順（最大 16 件）に実行します。

トリガーの契機になるイベントは以下となります。

- インターフェイスのリンクアップ・リンクダウン
- ハートビートの到達・不到達
- 対象インターフェイスの IP アドレス変化
- 一定時間の経過(周期イベント)
- モバイル通信のアンテナレベル変化
- SunDMS WAN ハートビートの到達・不到達
- 指定時刻
- データ通信量

イベント設定は［未設定］、［link］、［heartbeat］、［ip-change］、［period］、［antenna-level］、［sundms-heartbeat］、［time］、［traffic］となります。

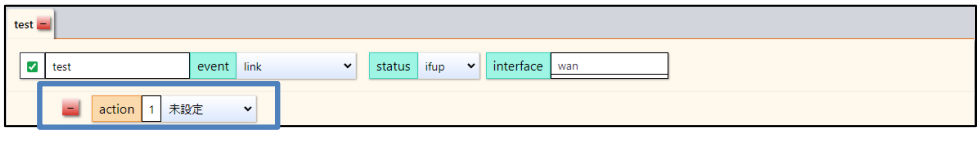


詳細はトリガーイベントの項目を参照ください。

トリガーで実施されるアクションは以下となります。

- 指定アドレスへのメール送信
- 本体、又はモバイル通信端末の再起動
- 指定したトリガーイベントの有効化・無効化
- 指定時間ウェイト
- ルート設定変更
- モバイル通信端末の接続プロファイル変更
- IPsec の有効化・無効化

アクション設定は［mail］、［reboot］、［trigger］、［wait］、［route］、［switch-profile］、［ipsec]となります。

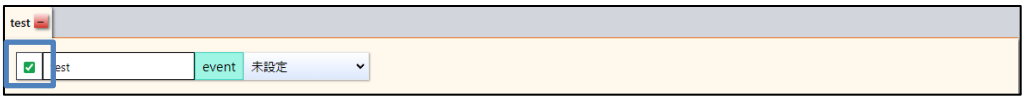


詳細はトリガーアクションの項目を参照ください。

・トリガー機能は、DRX が起動してから 3 分後に有効となります。
・各入力フォーム「インターフェイス」、「interval」、「threshold」など入力必須の場合、赤枠になっていますので入力して緑色になるように入力する必要があります。

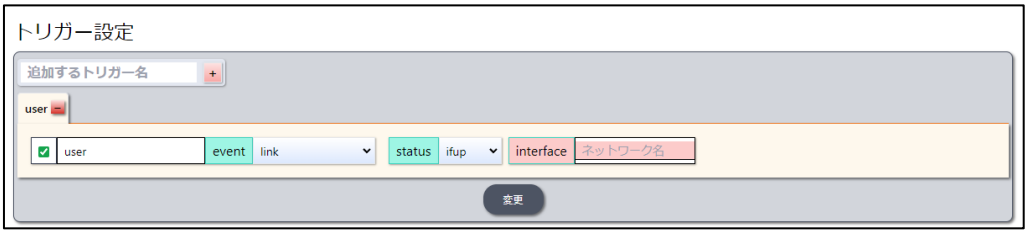
4-8-1. トリガーの使用設定

トリガー設定を有効にする場合、チェックをオンにします。



4-8-2. トリガーイベント：リンク状態

リンク状態の変化で動作するトリガーイベントを設定します。



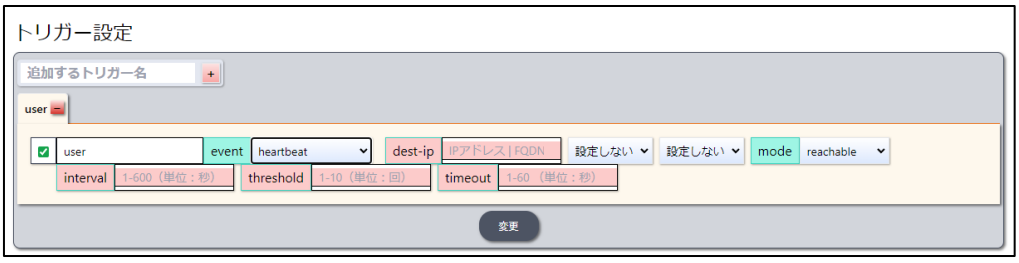
以下の設定を行います。

項目	内容
event	インターフェイスのリンク状態の変化によるイベントは［link］を設定します。
status	インターフェイスのリンク状態は［ifup］、［ifdown］、［both］のいずれかを設定します。 ▶ifup　：リンクアップ時、イベント発生します。 ▶ifdown　：リンクダウン時、イベント発生します。 ▶both　：リンクアップおよびリンクダウン時、イベント発生します。
interface	インターフェイス設定のネットワーク名を設定します。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-3. トリガーイベント：ハートビート

ハートビートの状態変化で動作するトリガーイベントを設定します。



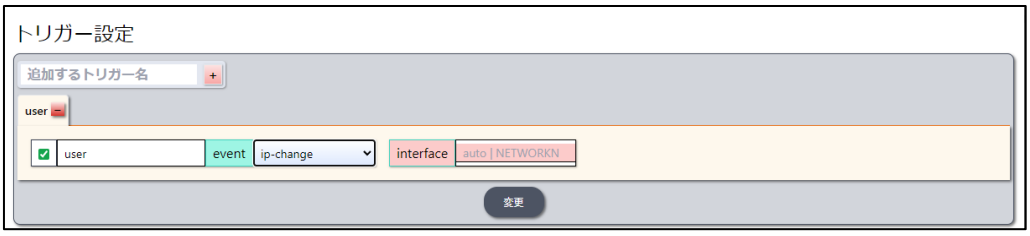
以下の設定を行います。

項目	内容
event	ハートビートの状態変化によるイベントは［heartbeat］を設定します。
dest-ip	送信先の IP アドレスもしくは FQDN を入力します。
src-ip(設定しない)	送信元を［設定しない］、［src-ip］のいずれかを設定します。 ▶設定しない　：送信元の IP アドレスを省略します。 ▶src-ip：［src-ip］を設定した場合は IP アドレスを入力する必要があります。
interface(設定しない)	インターフェイスは［設定しない］、［interface］のいずれかを設定します。 ▶設定しない　：インターフェイス入力を省略します。 ▶interface：［interface］を設定した場合はネットワーク名を入力する必要があります。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。
mode	mode は［reachable］、［unreachable］のいずれかを設定します。 ▶reachable：疎通成功時の設定です。 ▶unreachable：疎通失敗時の設定です。
interval	ハートビートのインターバル 1-600（単位：秒）で設定します。
threshold	ハートビートの閾値 1-10（単位：回）で設定します。
timeout	ping のタイムアウト 1-60 （単位：秒）で設定します。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-4. トリガーイベント：IPアドレス変化

IP アドレスの変化で動作するトリガーイベントを設定します。



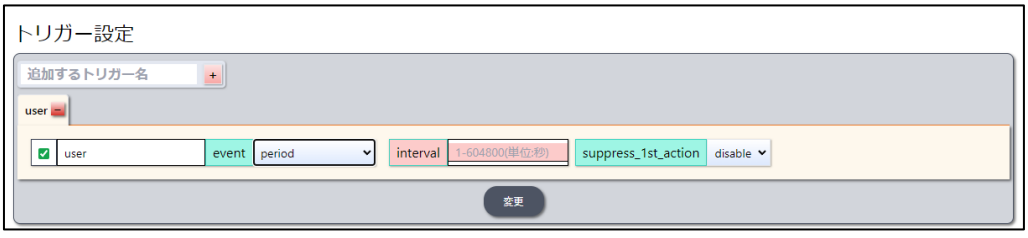
以下の設定を行います。

項目	内容
event	IP アドレスの変化によるイベントは［ip-change］を設定します。
interface	インターフェイス設定は「auto」もしくは「ネットワーク名」を入力します。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-5. トリガーイベント：周期イベント

定期的に動作するトリガーイベントを設定します。



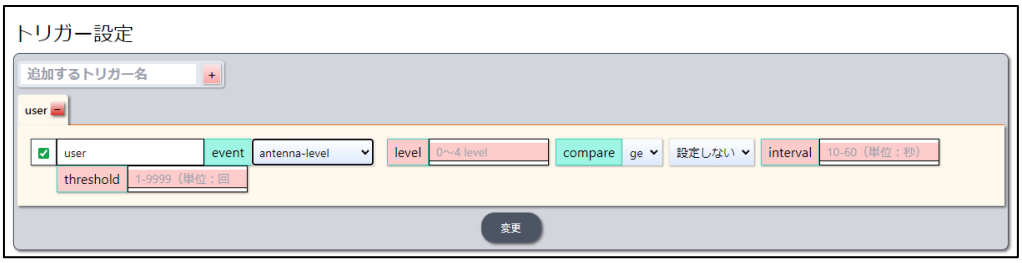
以下の設定を行います。

項目	内容
event	定期的に動作するイベントは［period］を設定します。
interval	周期の時間設定 1～604800 (単位：秒) を設定します。
suppress_1st_action	enable： 周期イベント実行開始から、1 回目のアクションを発生させない disable： 周期イベント実行開始から、1 回目のアクションが発生する

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-6. トリガーイベント：アンテナレベル

アンテナレベルの状態変化で動作するトリガーイベントを設定します。



以下の設定を行います。

項目		内容
event		アンテナレベルの状態変化によるイベントは［antenna-level］を設定します。
level		アンテナレベル 0～4 に設定します。
compare		アンテナレベルの条件を設定します。 ▶ge: level 以上の場合イベントが発生します。 ▶le: level 以下の場合イベントが発生します。
quality	条件	電波品質の設定は［設定しない］、［and］、［or］のいずれかを設定します。 ▶設定しない　：電波品質の設定を省略します。 ▶and：アンテナレベル、電波品質の条件が共に成立する場合に発生場合、設定します。 ▶or：アンテナレベル、電波品質の条件どちらかが成立する場合に発生場合、設定します。
	［and］、［or］設定の場合	電波品質の条件を設定します。 ▶ge: quality 以上の場合イベントが発生します。 ▶le: quality 以下の場合イベントが発生します。 電波品質(-30～0) に設定します。
interval		アンテナレベル取得インターバル 10～60（単位：秒）に設定します。
threshold		アンテナレベル取得閾値 1～9999（単位：回）に設定します。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-7. トリガーイベント：SunDMS WANハートビート

SunDMS WAN ハートビートの状態変化で動作するトリガーイベントを設定します。

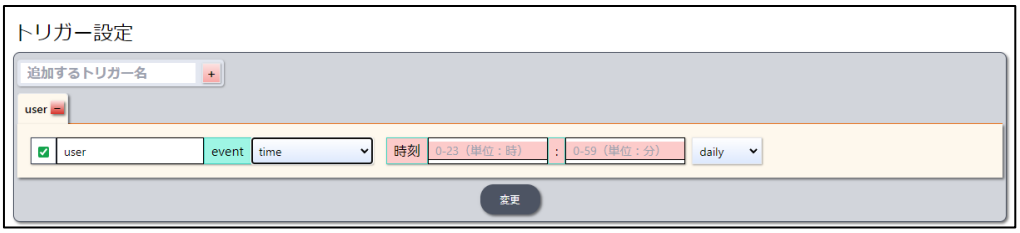
以下の設定を行います。

項目	内容
event	SunDMS WAN ハートビートの状態変化によるイベントは［sundms-heartbeat］を設定します。
dest-ip	送信先の FQDN を入力します。
interface(設定しない)	インターフェイスは［設定しない］、［interface］のいずれかを設定します。 ▶設定しない　：インターフェイス入力を省略します。 ▶interface：［interface］を設定した場合はネットワーク名を入力する必要があります。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。
mode	mode は［reachable］、［unreachable］のいずれかを設定します。 ▶reachable：疎通成功時の設定です。 ▶unreachable：疎通失敗時の設定です。
interval	ハートビートのインターバル 2-1440（単位：分）で設定します。
threshold	ハートビートの閾値 1-10（単位：回）で設定します。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-8. トリガーイベント：時刻

時刻で動作するトリガー設定を設定します。



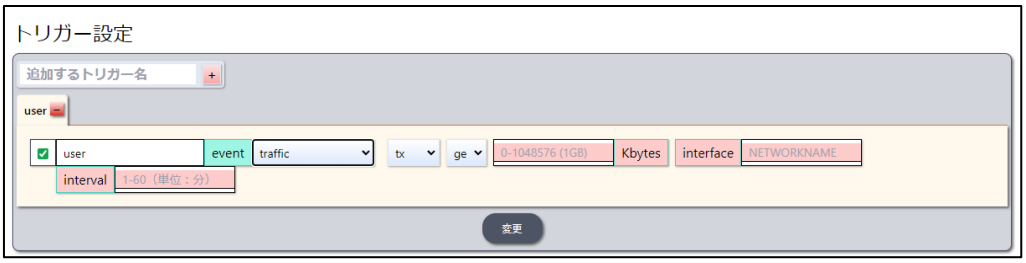
以下の設定を行います。

項目		内容
event		時刻によるイベントは［time］を設定します。
時刻		トリガーを実行する時刻(hh:mm 形式)を設定します。
パラメータ	daily	毎日設定時刻に動作します。
	weekly	毎週指定曜日の指定時刻に動作します。 ▶[sun] [mon] [tue] [wed] [thu] [fri] [sat] 実施する曜日を指定します。(複数指定可能)
	every-other-week	隔週指定曜日の指定時刻に動作します。隔週は ISO 8601 で定義される週番号が奇数の週です。 ▶[sun] [mon] [tue] [wed] [thu] [fri] [sat] 実施する曜日を指定します。
	monthly	毎月指定日（day）もしくは週・曜日（week）の指定時刻に動作します。 ▶［day］を指定した場合、実施する日 1～31 (単位:日) を指定します。 ▶［week］を指定した場合、実施する週 1～5 (単位:週目) と、[sun] [mon] [tue] [wed] [thu] [fri] [sat]の実施する曜日を指定します。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-9. トリガーイベント:通信量

インターフェイスの通信量で動作するトリガーイベントを設定します。



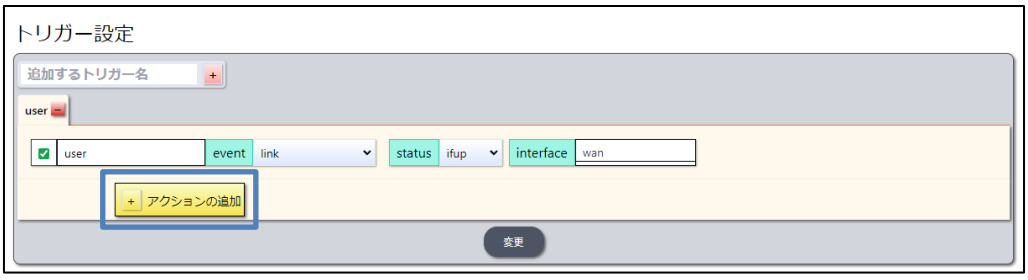
以下の設定を行います。

項目	内容
event	インターフェイスの通信量によるイベントは［traffic］を設定します。
監視	インターフェイスの通信量の監視は［tx］、［rx］、［both］のいずれかを設定します。 ▶tx:送信パケットを監視します。 ▶rx:受信パケットを監視します。 ▶both:送信+受信パケットを監視します。
traffic 条件・サイズ	動作条件は［ge］、［le］のいずれかを設定します。 ▶ge: SIZE 以上でイベント発生 ▶le: SIZE 以下でイベント発生 インターフェイスの通信の指定サイズ 0～1048576(単位:kByte)を設定します。
interface	インターフェイス設定は「ネットワーク名」を入力します。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。
interval	通信料の監視のインターバル 1-60（単位：分）で設定します。

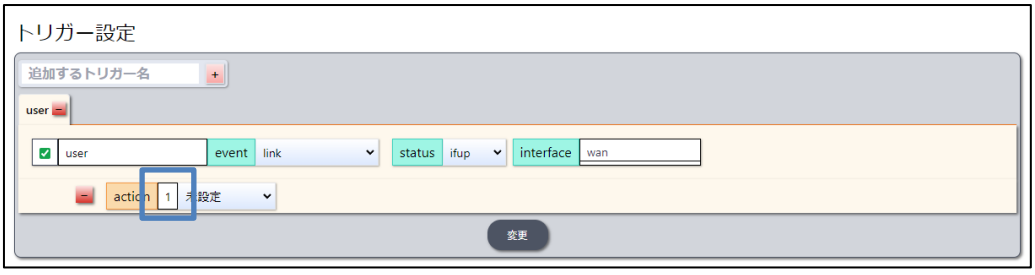
設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-10. トリガーアクションの追加・動作順番設定

1．　イベントを作成完了後、［変更］－［アクションの追加］をクリックします。



2．　アクションの動作順番、［変更］－［アクションの追加］をクリックします。



4-8-11. トリガーアクション：メール

イベント発生時にメールを送信するアクションを設定します。

以下の設定を行います。

項目	内容
action	イベント発生時にメールを送信するアクションは［mail］を設定します。
to	送信先のメールアドレスを入力します。
from(設定しない)	送信元のメールアドレスを［設定しない］、［from］のいずれかを設定します。 ▶設定しない　：送信元のメールアドレスを省略します。 ▶from：［from］を設定した場合はメールアドレスを入力する必要があります。
title(設定しない)	メールタイトルは［設定しない］、［title］のいずれかを設定します。 ▶設定しない　：メールタイトルを省略します。 ▶title：［title］を設定した場合はメールタイトル（最大 1024 バイト）を入力する必要があります。 ▶日本語入力可能（UTF-8）です。
Message(設定しない)	メール本文は［設定しない］、［message］のいずれかを設定します。 ▶設定しない　：メール本文入力を省略します。 ▶message：［message］を設定した場合はメール本文（最大 1024 バイト）を入力する必要があります。 ▶日本語入力可能（UTF-8）です。 ▶メール本文に%IP%を入れるとメッセージに IP アドレスが入ります。 ▶%PROFILE{PROFILENUMBER}_SIM%で{PROFILENUMBER}で指定されたプロファイルの SIM 挿入状態が入ります。 ・SIM が挿入されている場合：挿入済 ・SIM が挿入されていない場合：未挿入 ・指定したプロファイル設定がない場合：プロファイル未定義
notice-ip(設定しない)	インターフェイスの IP アドレス通知は［設定しない］、［notice-ip］のいずれかを設定します。 ▶設定しない　：notice-ip を省略します。 ▶notice-ip：［notice-ip］を設定した場合は「auto」もしくは「ネットワーク名」を入力します。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。 ▶インターフェイスに［auto］を入力した場合、デフォルトルートのインターフェイスの IP アドレスとなります。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

memo　［Messages］項目で IP アドレスを送信する場合で、［notice-ip］項目が auto または未設定、同じ条件のデフォルトルートが複数の場合は、どちらかの IP アドレスが送信されます。

4-8-12. トリガーアクション：再起動

イベント発生時に再起動させるアクションを設定します。

以下の設定を行います。

項目	内容
action	イベント発生時に再起動させるアクションは［reboot］を設定します。
reboot	リブートの項目［system］、［mobile］、［ipsec］のいずれかを設定します。 ▶system:本体再起動が発生します。 ▶mobile:モバイル通信端末の再起動が発生します。 ▶ipsec:IPsec の再起動が発生します。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-13. トリガーアクション：トリガー

イベント発生時に設定済みのトリガー設定の有効／無効を変化させるアクションを設定します。

以下の設定を行います。

項目	内容
action	イベント発生時に再起動させるアクションは［trigger］を設定します。
トリガー名	設定済みのトリガー名を入力します。 ➲『4-8. トリガー』で［追加するトリガー名］の設定済みのトリガーではない場合は［変更］失敗します。
トリガー動作	トリガー動作設定［enable］、［disable］、［handover］のいずれかを設定します。 ▶enable：指定されたトリガーの有効化 ▶disable：指定されたトリガーの無効化 ▶handover：このトリガーと他のトリガーの有効無効を入れ替え

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

> 設定するトリガー自身の有効／無効を変化させることも可能です。
> 但し、自身のトリガーに対して handover を指定した場合の動作は保証しません。

4-8-14. トリガーアクション：ウェイト

イベント発生時に一定時間を待つアクションを設定します。

以下の設定を行います。

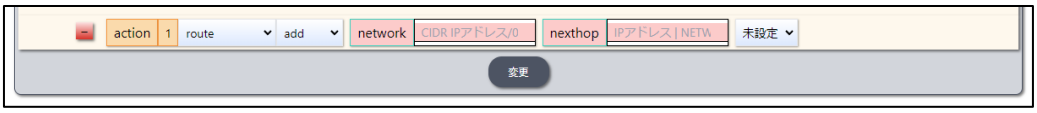
項目	内容
action	イベント発生時に一定時間を待つアクションは［wait］を設定します。
wait	待ち時間 1～7200（単位：秒）を設定します。
variance	待ち時間を分散させるか［enable］、［disable］のいずれかを設定します。 ▶enable：wait 設定を最大とする製造番号をキーとする擬似乱数によって待ち時間が変化します。 ▶disable：wait 設定の待ち時間となります。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

> トリガーアクションは、途中で中断できないため処理が重ならないように配慮し設定ください。

4-8-15. トリガーアクション：ルート

イベント発生時に経路を追加／削除を行うアクションを設定します。



以下の設定を行います。

項目	内容
action	イベント発生時に経路を追加／削除を行うアクションは［route］を設定します。
route 動作	route 動作［add］、［remove］のいずれかを設定します。 ▶add:設定の経路を追加します。 ▶remove: 設定の経路を削除します。
network	宛先 IP アドレス/<1-32>を入力します。
nexthop	転送先 IP アドレスもしくはネットワーク名を入力します。 ➲ ネットワーク名については『3-1. インターフェイス』でご確認ください。
metric(設定しない)	メトリックは［設定しない］、［metric］のいずれかを設定します。 ▶設定しない　：metric を省略します。 ▶metric：［metric］を設定した場合はメトリックの設定 1～255 を入力します。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

4-8-16. トリガーアクション：プロファイル変更

イベント発生時に指定したプロファイルに接続するアクションを設定します。

以下の設定を行います。

項目	内容
action	イベント発生時に指定したプロファイルに接続するアクションは［switch-profile］を設定します。
switch-profile	モバイルのプロファイル番号１～８を入力します。 ➲ モバイル設定『3-2-2. プロファイル』のプロファイル番号をご確認ください。

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

memo　アクション実行後、切り替え後の動作を確認するトリガーを設定する場合、WAIT アクションを入れてタイミングを図ることをお勧めします。（5 分程度）

4-8-17. トリガーアクション：IPsec

イベント発生時に IPsec プロファイル設定の有効／無効を変化させるアクションを設定します。

以下の設定を行います。

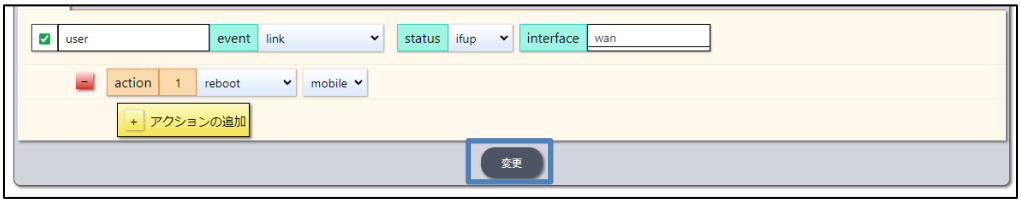
項目	内容
action	イベント発生時に再起動させるアクションは［trigger］を設定します。
IPsec プロファイル名	設定済みの IPsec プロファイル名を入力します。 ➲『3-6. VPN IPsec』で設定された［プロファイル名］ではない場合は［変更］失敗します。
IPsec 動作	IPsec プロファイルの動作設定［enable］、［disable］のいずれかを設定します。 ▶enable：指定された IPsec プロファイルの有効化 ▶disable：指定された IPsec プロファイルの無効化

設定後、［変更］ボタンをクリックして設定内容を一時保存します。

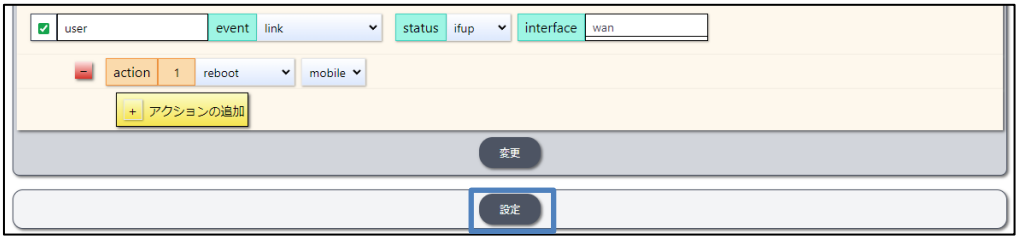
既に有効化している状態から 更に有効化した場合、一旦 IPsec セッションを切断します。

4-8-18. トリガー設定

1．［変更］ボタンクリック後、［設定］ボタンが表示されます。



2．［設定］ボタンをクリックすると設定が保存され、反映されます。

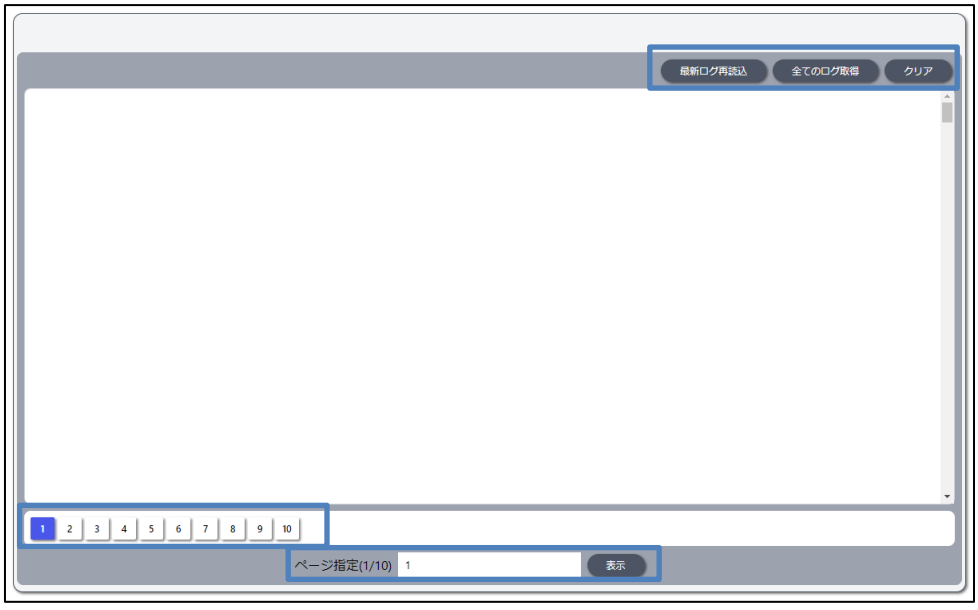


5章　ログ

この章では、各動作のログを参照する方法について説明します。

5-1. ログ画面のボタンについて

各ログ画面共通に使用されるボタンを説明します。



以下のログページのボタンを説明します。

項目	内容
［最新ログ再読込］ボタン	［最新ログ再読込］ボタンをクリックすると最新のログを取得し、ページ情報が更新されます。
［全てのログ修得］ボタン	［全てのログ取得］ボタンをクリックすると該当ページの全て情報を圧縮形式「ファイル名.tar.gz」で取得します。
［クリア］ボタン	［クリア］ボタンをクリックすると該当ページの全てのログ情報を削除します。
ページボタン	ログ情報は 1 ページ 500 行表示します、500 行毎にページが増えていき、ページボタンが増えていきます。 ベージを移動する場合は［ n ］ボタンをクリックします。
［表示］ボタン	ベージ指定入力にページ番号を入力し、［表示］ボタンをクリックすると入力番号のページに移動できます。

5-2. モバイル通信端末ログ

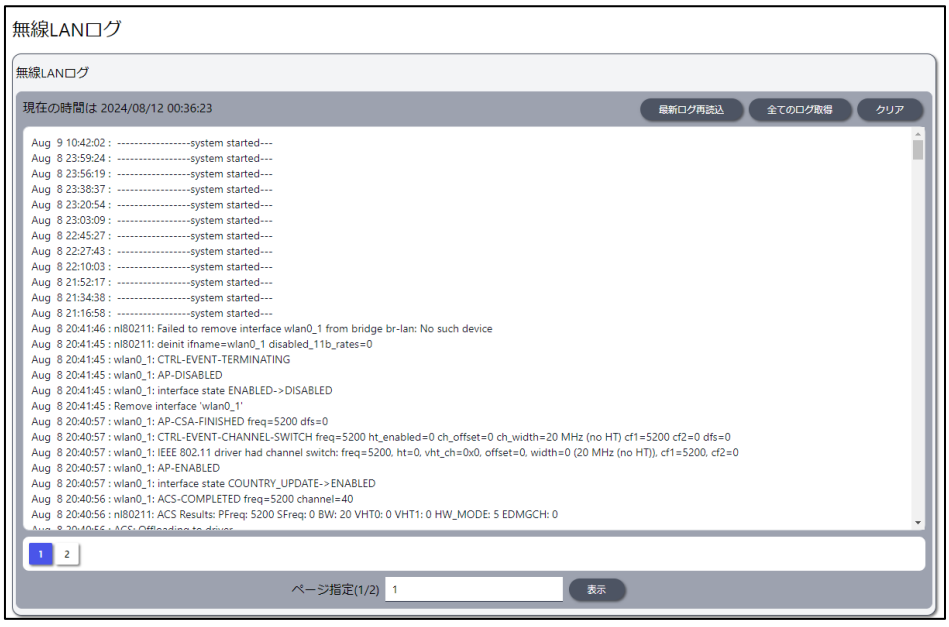
1．　設定ツールのメニューから、［ログ］－［モバイル通信端末ログ］をクリックします。モバイル通信端末ログ一覧のページが表示されます。

項目	内容
記録時刻とログ	ログの発生した時刻と、モバイル通信端末の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-3. 無線LANログ DRX5510 DRX5010

1．　設定ツールのメニューから、［ログ］－［無線 LAN ログ］をクリックします。

無線 LAN ログ一覧のページが表示されます。

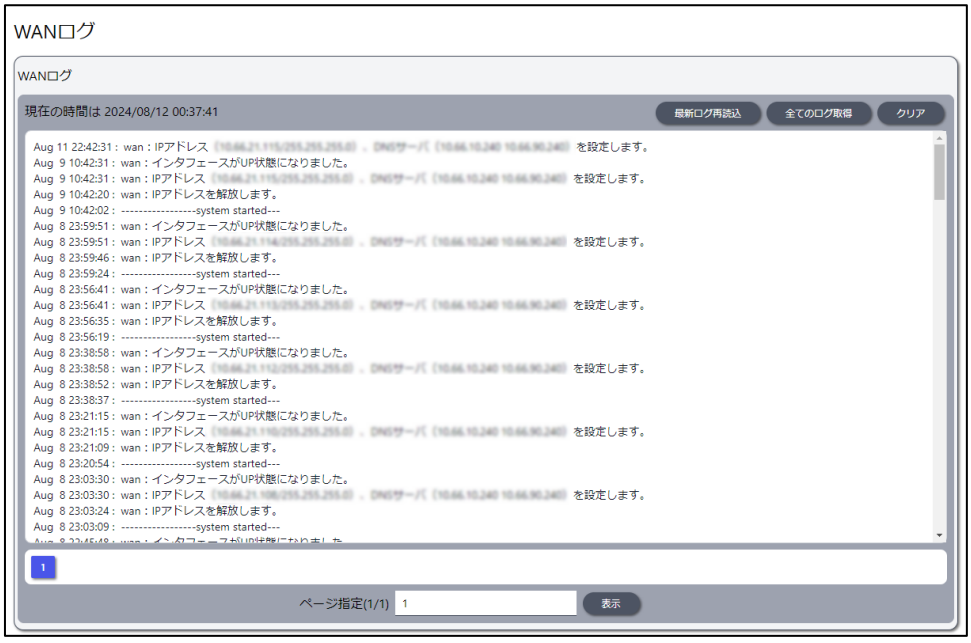


項目	内容
記録時刻とログ	ログの発生した時刻と、無線 LAN の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-4. WANログ

1．　設定ツールのメニューから、［ログ］－［WAN ログ］をクリックします。

WAN ログ一覧のページが表示されます。

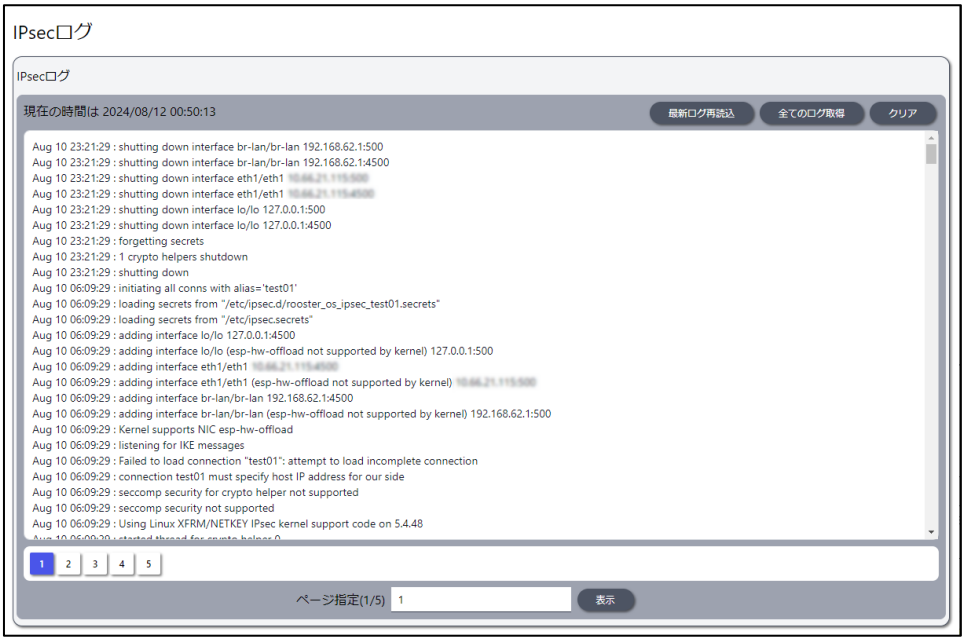


項目	内容
記録時刻とログ	ログの発生した時刻と、WAN の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-5. IPsecログ

1．　設定ツールのメニューから、［ログ］－［IPsec ログ］をクリックします。

IPsec ログ一覧のページが表示されます。

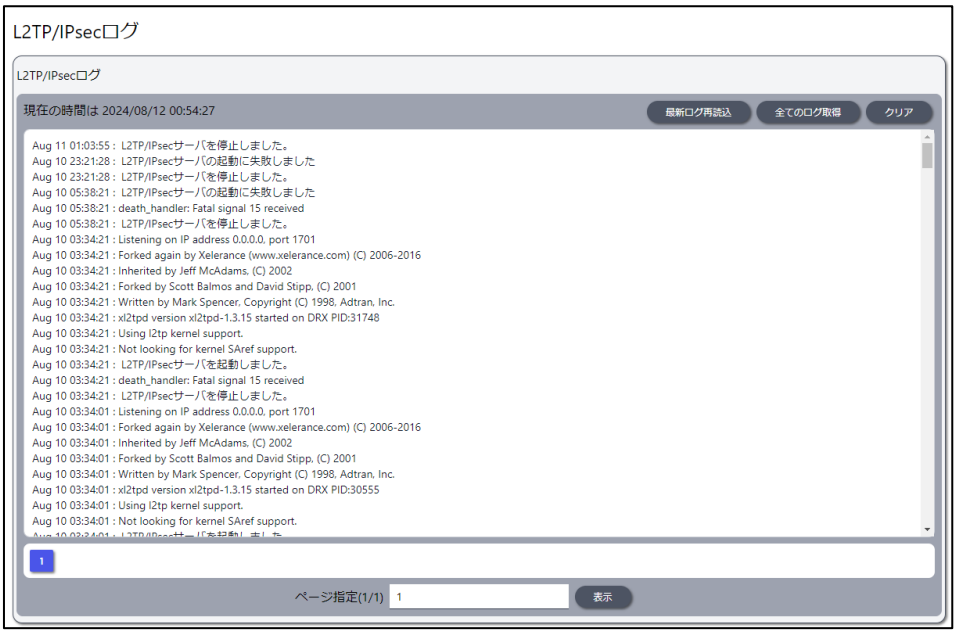


項目	内容
記録時刻とログ	ログの発生した時刻と、IPsec の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-6. L2TP/IPsecログ

1．　設定ツールのメニューから、［ログ］－［L2TP/IPsec ログ］をクリックします。

L2TP/IPsec ログ一覧のページが表示されます。

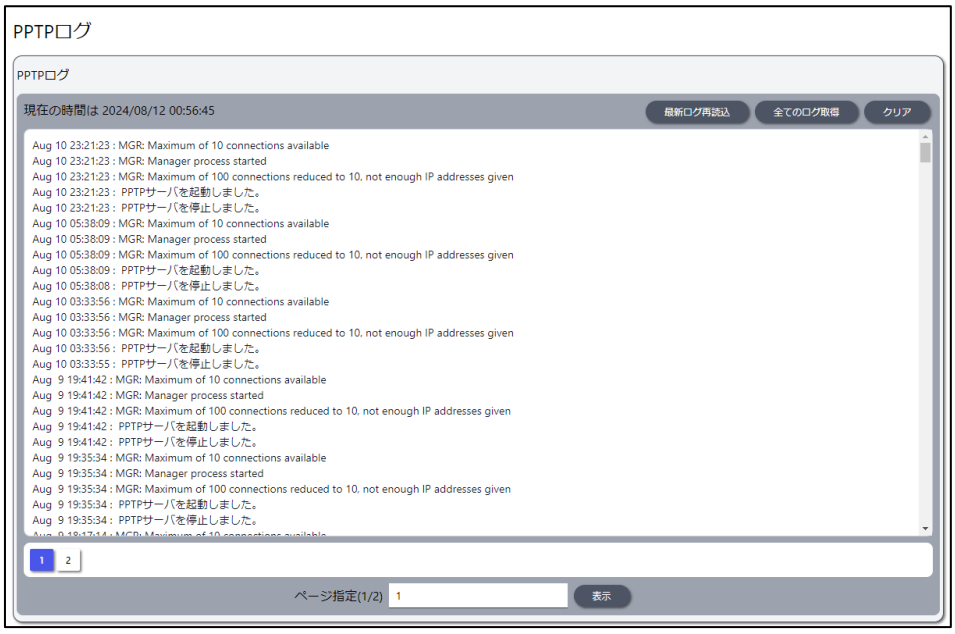


項目	内容
記録時刻とログ	ログの発生した時刻と、L2TP/IPsec の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-7. PPTPログ

1．　設定ツールのメニューから、［ログ］－［PPTP ログ］をクリックします。

PPTP ログ一覧のページが表示されます。

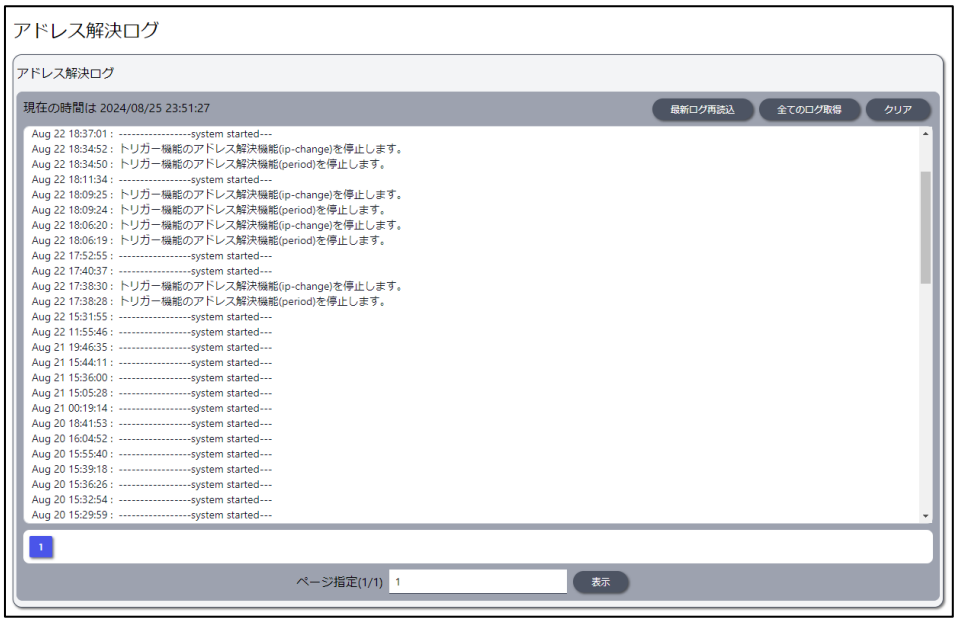


項目	内容
記録時刻とログ	ログの発生した時刻と、PPTP の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-8. アドレス解決ログ

1．　設定ツールのメニューから、［ログ］－［アドレス解決ログ］をクリックします。

アドレス解決ログ一覧のページが表示されます。

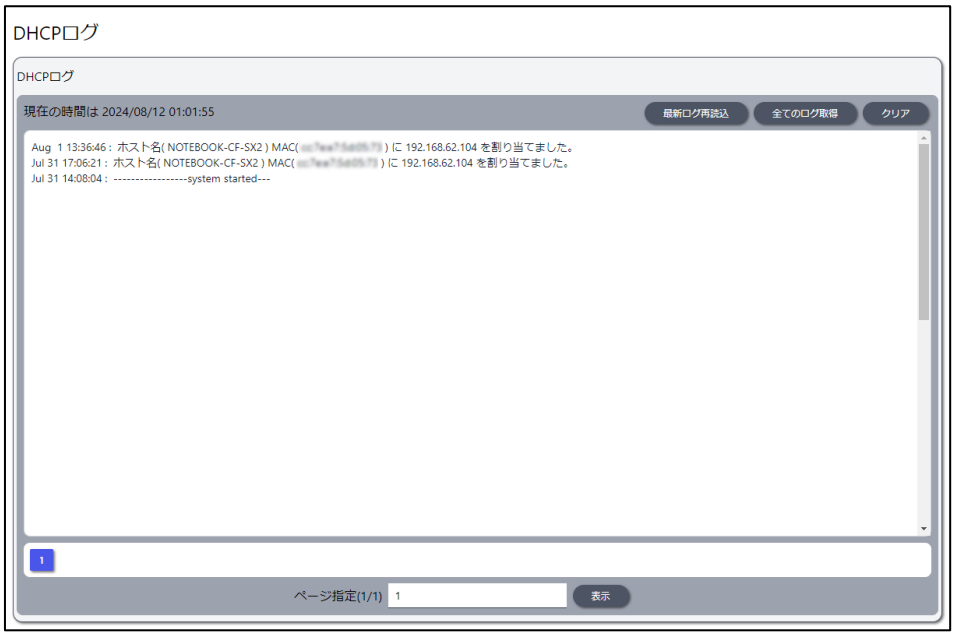


項目	内容
記録時刻とログ	ログの発生した時刻と、アドレス解決の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-9. DHCPログ

1．　設定ツールのメニューから、［ログ］－［DHCP ログ］をクリックします。

DHCP ログ一覧のページが表示されます。



項目	内容
記録時刻とログ	ログの発生した時刻と、DHCP の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-10. WANハートビートログ

1．　設定ツールのメニューから、［ログ］－［WAN ハートビートログ］をクリックします。

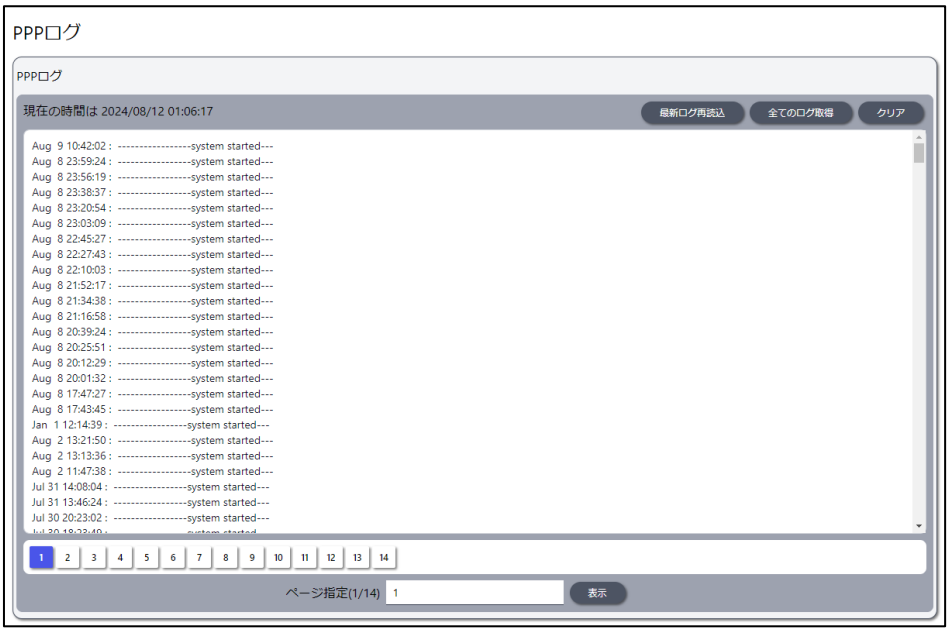
WAN ハートビートログ一覧のページが表示されます。

項目	内容
記録時刻とログ	ログの発生した時刻と、WAN ハートビートの動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-11. PPPログ

1．　設定ツールのメニューから、［ログ］－［PPP ログ］をクリックします。

PPP ログ一覧のページが表示されます。

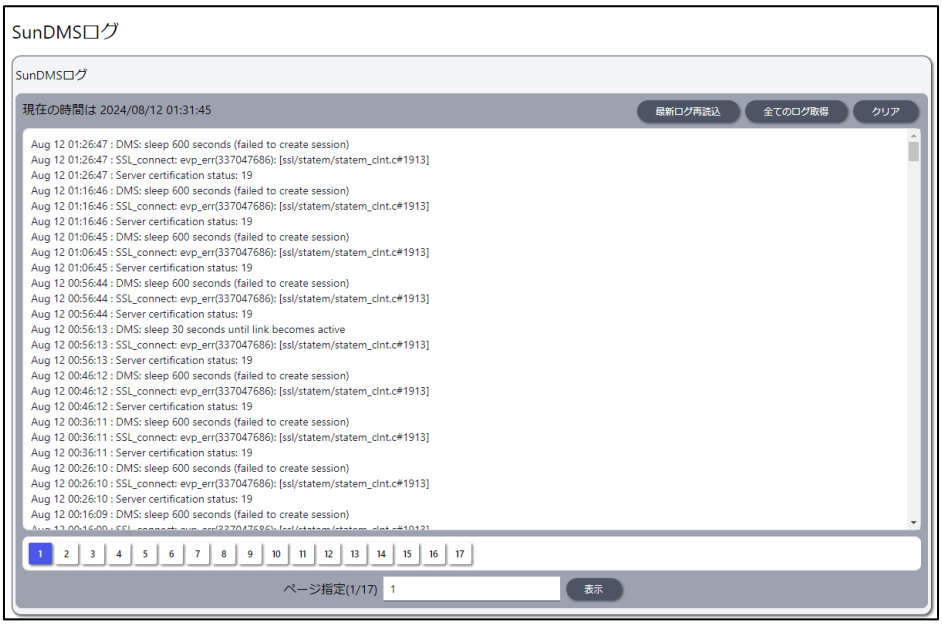


項目	内容
記録時刻とログ	ログの発生した時刻と、PPP の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-12. SunDMSログ

1．　設定ツールのメニューから、［ログ］－［SunDMS ログ］をクリックします。

SunDMS ログ一覧のページが表示されます。



項目	内容
記録時刻とログ	ログの発生した時刻と、SunDMS の動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-13. トリガーログ

1．　設定ツールのメニューから、［ログ］－［トリガーログ］をクリックします。

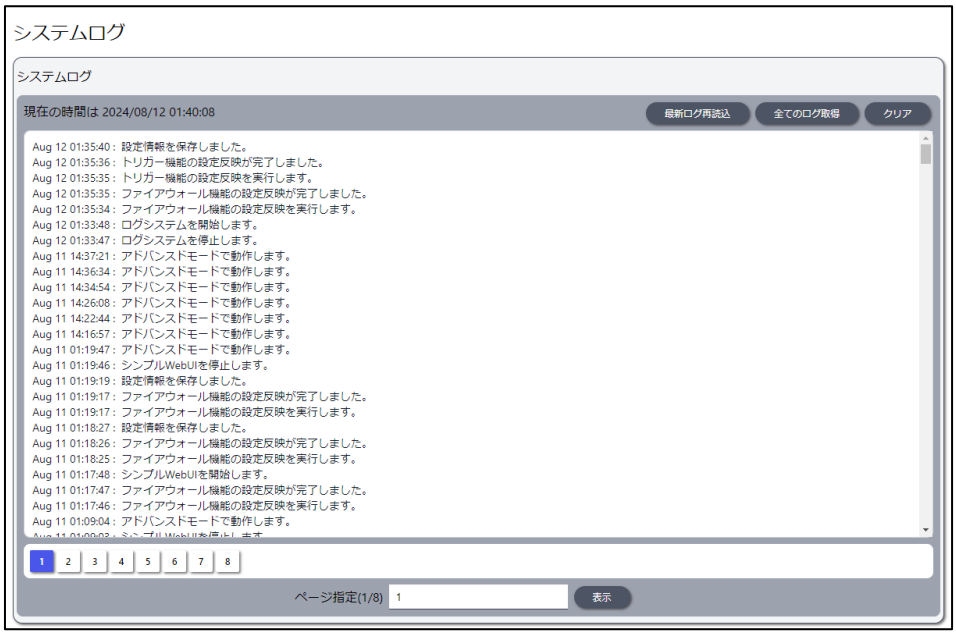
トリガーログ一覧のページが表示されます。

項目	内容
記録時刻とログ	ログの発生した時刻と、トリガーの動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-14. システムログ

1．　設定ツールのメニューから、［ログ］－［システムログ］をクリックします。

システムログ一覧のページが表示されます。

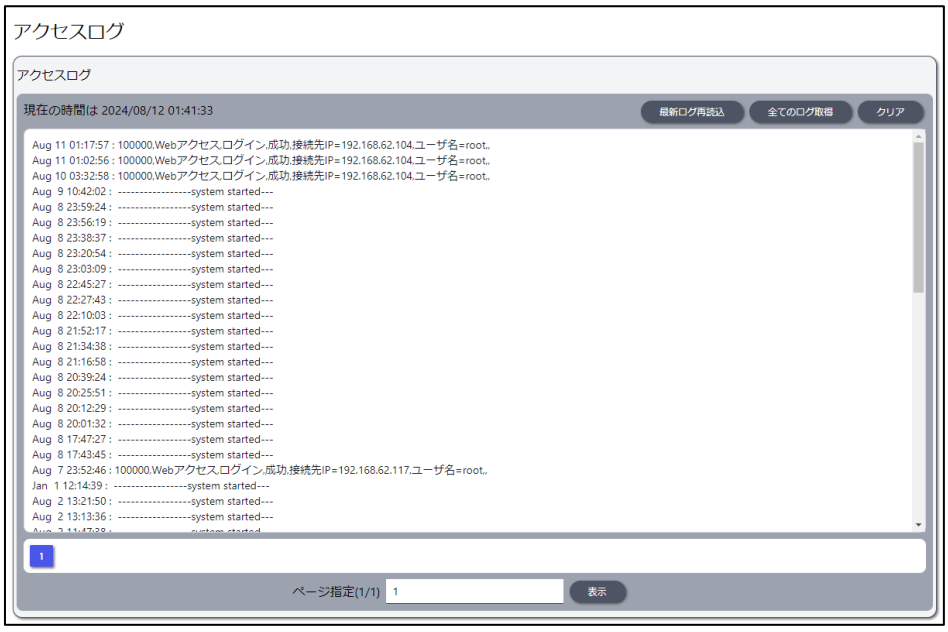


項目	内容
記録時刻とログ	ログの発生した時刻と、システムの動作状態が表示されます。 上に行くほど、より新しいログとなります。

5-15. アクセスログ

1．　設定ツールのメニューから、［ログ］－［アクセスログ］をクリックします。

アクセスログ一覧のページが表示されます。



項目	内容
記録時刻とログ	ログの発生した時刻と、アクセスの動作状態が表示されます。 上に行くほど、より新しいログとなります。

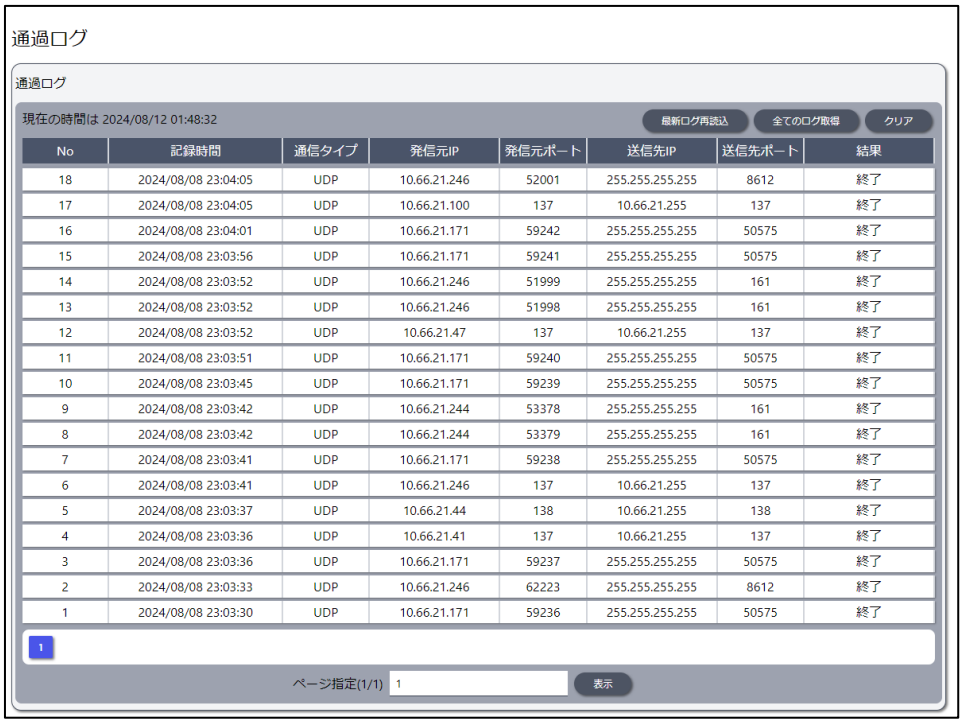
アクセスログフォーマット

No.	項目名	内容説明
1	詳細コード	数字 6 桁による状態コード 機能（処理・操作内容毎）３桁　＋　結果３桁 ・機能 100：　Web アクセス 101：　AdvWeb アクセス 102：　CLI アクセス 【その他 将来拡張用】 ・結果 000：ログイン成功 001：ログイン成功（キャッシュ超過） 010：ログイン失敗（パスワード間違い） 011：ログイン失敗（アカウント無し） 020：ログイン失敗（アカウントロック実施中） 021：ログイン失敗（アカウントロック開始） 【その他 将来拡張用】
2	処理内容	（Web アクセス、AdvWeB アクセス、CLI アクセス）※その他 将来拡張用
3	操作内容	（ログイン）　※その他 将来拡張用
4	結果	（成功、失敗）　※その他 将来拡張用
5～9	詳細１～４	処理・操作内容による詳細内容を記載する任意項目

5-16. 通過ログ

1．　設定ツールのメニューから、［ログ］－［通過ログ］をクリックします。

通過ログ一覧のページが表示されます。

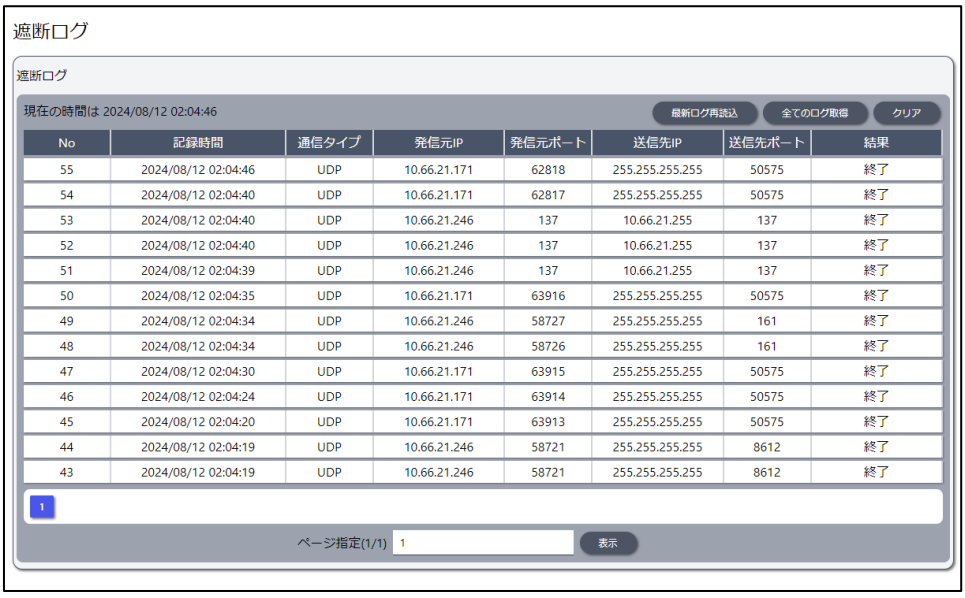


項目	内容
No.	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 DRX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
通信タイプ	IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
発信元 IP	通信の起点になる機器の IP アドレスが表示されます。
発信元ポート	通信の起点になる機器の使用ポート番号が表示されます。
送信先 IP	通信の宛先になる機器の IP アドレスが表示されます。
送信先ポート	通信の宛先になる機器の使用ポート番号が表示されます。
結果	通信が終了した理由が表示されます。 • 「正常終了」、「終了」 通信が行われた時に表示されます。 • 「タイムアウト」 通信セッション確立後、通信が途中で終了、あるいは終了フラグを確認できなかった時に表示されます。

5-17. 遮断ログ

1．　設定ツールのメニューから、［ログ］－［遮断ログ］をクリックします。

遮断ログ一覧のページが表示されます。



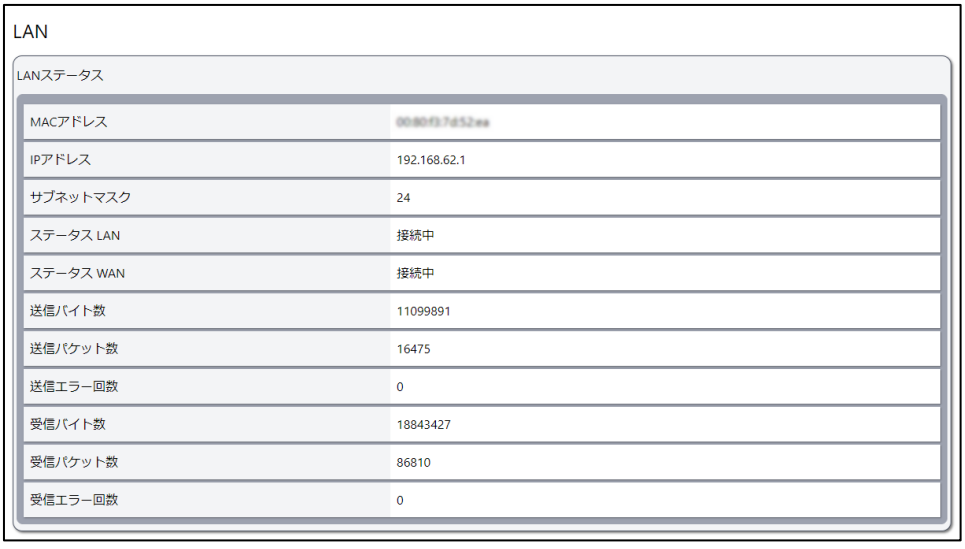
項目	内容
No.	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。DRX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
通信タイプ	IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
発信元 IP	通信の起点になる機器の IP アドレスが表示されます。
発信元ポート	通信の起点になる機器の使用ポート番号が表示されます。
送信先 IP	通信の宛先になる機器の IP アドレスが表示されます。
送信先ポート	通信の宛先になる機器の使用ポート番号が表示されます。

6章　ステータス

この章では、各動作のステータスを参照する方法について説明します。

6-1. LAN

1．　LAN 内の通信状態は、設定ツールのメニューから、［ステータス］-［LAN］をクリックして表示される「LAN ステータス表示画面」から確認することができます。



項目	内容
MAC アドレス	DRX の MAC アドレスが表示されます。
IP アドレス	DRX の IP アドレスが表示されます。
サブネットマスク	DRX のサブネットマスクが表示されます。
[LAN/WAN 構成の場合] ステータス 　LAN: 　WAN: [LAN/LAN 構成の場合] ステータス 　Bridge-LAN1: 　Bridge-LAN2:	 LAN ポートへの LAN 接続機器の接続状態が表示されます。 WAN ポートへの LAN 接続機器の接続状態が表示されます。 LAN1 ポートへの LAN 接続機器の接続状態が表示されます。 LAN2 ポートへの LAN 接続機器の接続状態が表示されます。
送信バイト数	DRX から送信したデータの総バイト数が表示されます。
送信パケット数	DRX から送信したデータの総パケット数が表示されます。
送信エラー回数	DRX からデータ送信を行った際に発生したエラー回数の総計が表示されます。
受信バイト数	DRX で受信したデータの総バイト数が表示されます。
受信パケット数	DRX で受信したデータの総パケット数が表示されます。
受信エラー回数	DRX がデータ受信を行った際に発生したエラー回数の総計が表示されます。

6-2. モバイル通信端末

1．　設定ツールのメニューから、［ステータス］－［モバイル通信端末］をクリックします。

「モバイル通信端末ステータス」のページが表示されます。

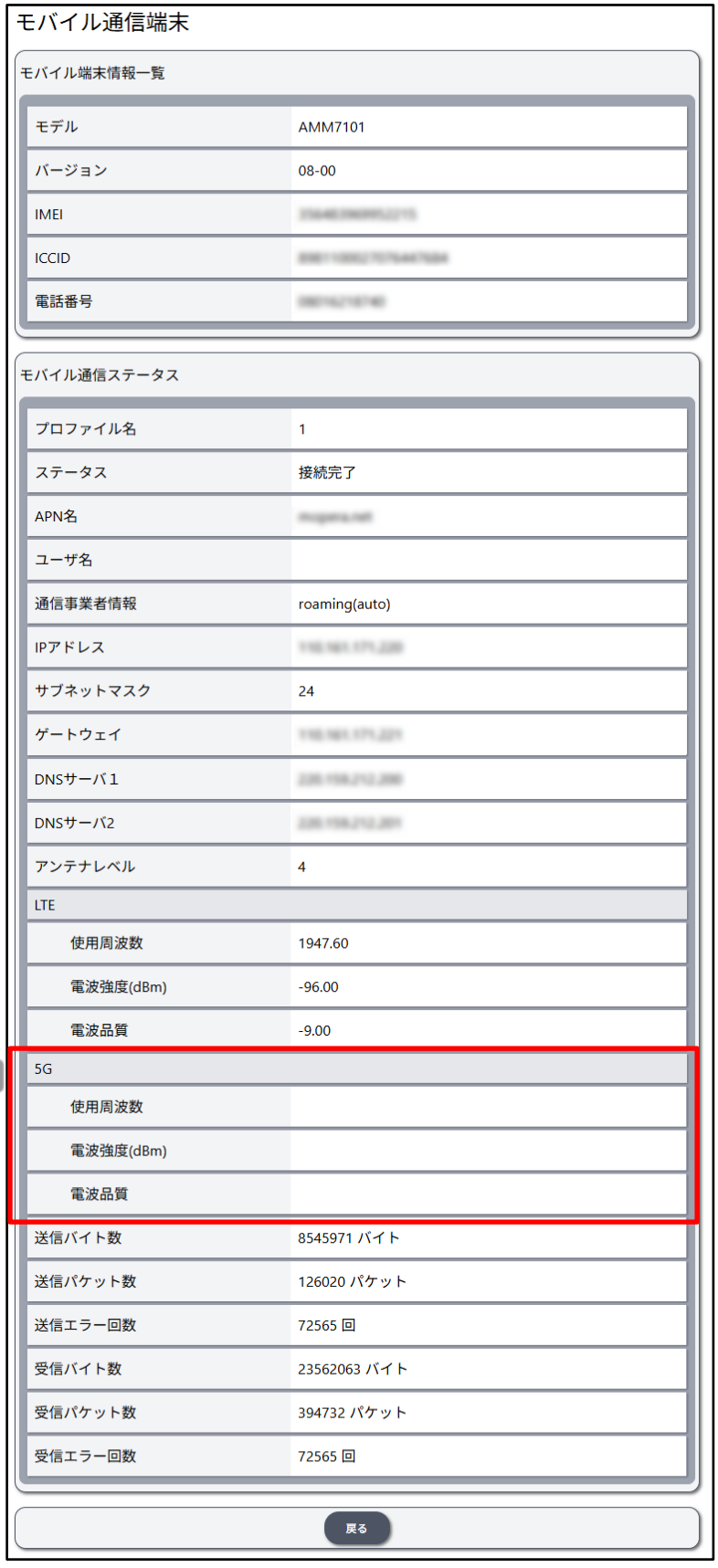
モバイル通信端末のステータス一覧

項目		内容
プロファイル		現在接続している回線の接続先の設定番号を表示します。
接続先 情報		現在接続している回線の接続先を表示します。 未接続時は空白になります。
接続先 メモ		現在接続している回線の接続先のメモを表示します。 未接続時は空白になります。
ステータス		設定した回線の接続の現在の状態が表示されます。 ［詳細表示］をクリックすると、現在の状態をより詳しく参照できます。 ➲ ステータスの詳細については、『ステータス項目の状態一覧』をご覧ください。
操作	［接続#1～#8］	それぞれの回線の接続先に対する接続動作を行います。
	［切断］	接続中の回線に対する切断動作を行います。
	［無効］	設定を無効にします。 次回、［有効］をクリックするまで設定内容を使えないようにします。
	［有効］	設定を有効にします。 次回、［無効］になっている設定を再度使えるようにします。

ステータス項目の状態一覧

ステータス表示	状態	MOBILE ランプの状態
使用しない	モバイル通信端末を無効と設定した状態です。	消灯
停止	モバイル通信端末は正常に認識されていますが、SIM が未挿入、キャリアの接続設定が正しく行われていない、プロファイル未登録などの原因で、モバイル通信端末が動作できない状態です。	消灯
処理中	モバイル通信サービス起動中、設定変更中などモバイル通信端末の初期化処理を行っている状態です。	消灯
未接続	モバイル通信サービスは動作していますが、APN に接続していない状態です。操作欄に接続可能なプロファイルの接続ボタンが表示されます。	消灯
接続試行中	APN への接続処理を行っている状態です。 「プロファイル名」、「接続先 情報」、「接続先 メモ」に接続対象の情報が表示されます。	点滅
接続完了	APN に接続して、モバイル通信可能な状態です。 「プロファイル名」、「接続先 情報」、「接続先 メモ」に接続対象の情報が表示されます。	点灯
切断中	接続完了状態から切断処理を行っている状態です。	消灯

2．　モバイル通信端末内の通信状態の詳細は、［モバイル通信端末ステータス］－［詳細表示］をクリックして表示される「モバイル通信端末通信の詳細表示」から確認することができます。



モバイル通信端末

モバイル端末情報一覧

モデル	AMM7101
バージョン	08-00
IMEI	
ICCID	
電話番号	

モバイル通信ステータス

プロファイル名	1
ステータス	接続完了
APN名	
ユーザ名	
通信事業者情報	roaming(auto)
IPアドレス	
サブネットマスク	24
ゲートウェイ	
DNSサーバ１	
DNSサーバ2	
アンテナレベル	4
LTE	
使用周波数	1947.60
電波強度(dBm)	-96.00
電波品質	-9.00
5G	
使用周波数	
電波強度(dBm)	
電波品質	
送信バイト数	8545971 バイト
送信パケット数	126020 パケット
送信エラー回数	72565 回
受信バイト数	23562063 バイト
受信パケット数	394732 パケット
受信エラー回数	72565 回

戻る

DRX5510

モバイル端末情報一覧

項目	内容
モデル	モバイル通信端末のモデル名が表示されます。
バージョン	モバイル通信端末の FW バージョンが表示されます。
IMEI	モバイル通信端末の IMEI が表示されます。
ICCID	モバイル通信端末の ICCID 値が表示されます。
電話番号	SIM の電話番号が表示されます。

モバイル通信ステータス

項目	内容
プロファイル名	現在接続している回線の接続先の設定番号を表示します。
ステータス	設定した回線の接続の現在の状態が表示されます。
APN 名	設定したアクセスポイントへの APN 名が表示されます。
ユーザ名	設定したユーザ名が表示されます。
通信事業者情報	現在接続している通信事業者の情報が表示されます。
使用周波数	モバイル通信端末の使用周波数(MHz) が表示されます。
アンテナレベル	アンテナレベルが表示されます。
電波強度	モバイル通信端末の電波強度(dBm) が表示されます。
電波品質	モバイル通信端末の電波品質が表示されます。
IP アドレス	プロバイダおよび接続先から割り当てられた、IP アドレスが表示されます。
サブネットマスク (＊1)	サブネットマスクを表示されます。
ゲートウェイ (＊1)	ゲートウェイの IP アドレスが表示されます。(*2)
DNS サーバ 1 (＊1)	DNS サーバ 1 の IP アドレスが表示されます。
DNS サーバ 2 (＊1)	DNS サーバ 2 の IP アドレスが表示されます。
送信バイト数	モバイル通信端末で送信したデータの総バイト数が表示されます。
送信パケット数	モバイル通信端末で送信したデータの総パケット数が表示されます。
送信エラー回数	モバイル通信端末でデータ送信を行った際に発生した、エラー回数の総計が表示されます。
受信バイト数	モバイル通信端末で受信したデータの総バイト数が表示されます。
受信パケット数	モバイル通信端末で受信したデータの総パケット数が表示されます。
受信エラー回数	モバイル通信端末でデータ受信を行った際に発生した、エラー回数の総計が表示されます。

*1：MBIM モードのみの表示となります。ECM モードでは表示されません。

*2：ネットワーク上形式的な IP アドレスのため、実際のネットワーク上には存在しません。

6-3. 無線LAN　DRX5510　DRX5010

1．　設定ツールのメニューから、［ステータス］－［無線 LAN］をクリックします。

「無線 LAN」のページが表示されます。

無線 LAN ステータス

項目	内容
「接続中」	無線 LAN に接続している子機が存在している状態です。
「切断中」	無線 LAN に接続している子機が存在していない状態です。

無線 LAN 一覧

項目	内容
No.	無線 LAN に接続している子機の接続番号が表示されます。
MAC アドレス	無線 LAN に接続している子機の MAC アドレスが表示されます。
SSID	無線 LAN に接続している子機の SSID の名前が表示されます。

6-4. WAN

1．　WAN 内の通信状態は、設定ツールのメニューから、［ステータス］－［WAN］をクリックして表示される「WAN ステータス表示画面」から確認することができます。

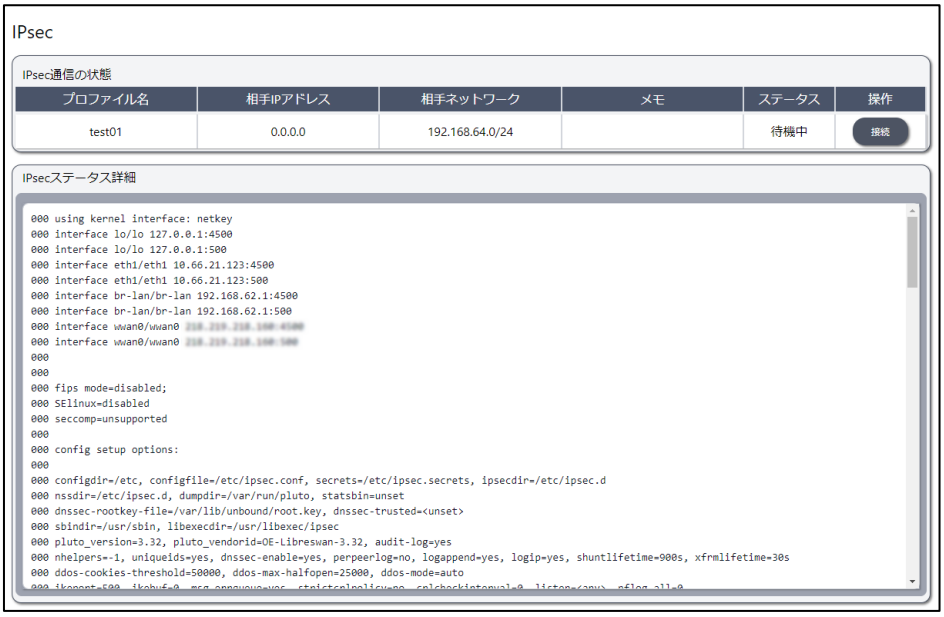
[LAN/WAN 構成の場合]（IP 自動取得、IP 手動設定、PPPoE 接続を選択）

項目		内容
操作	［接続／切断］ボタン	• WAN 側と切断中は［接続］ボタンが表示されます。WAN 側との通信を接続する場合はクリックします。 • WAN 側と接続中は［切断］ボタンが表示されます。WAN 側との通信を切断する場合はクリックします。
	［DHCP 再取得］ボタン	DHCP を再取得します。
MAC アドレス		MAC アドレスが表示されます。
IP アドレス		WAN 側の IP アドレスが表示されます。
サブネットマスク		WAN 側のサブネットマスクが表示されます。
ゲートウェイ		WAN 側のデフォルトゲートウェイが表示されます。
DNS サーバ 1		プライマリ DNS サーバが表示されます。
DNS サーバ 2		セカンダリ DNS サーバが表示されます。
送信バイト数		WAN 側に送信したデータの総バイト数が表示されます。
送信パケット数		WAN 側に送信したデータの総パケット数が表示されます。
送信エラー回数		WAN 側にデータ送信を行った際に発生したエラー回数の総計が表示されます。
受信バイト数		WAN 側から受信したデータの総バイト数が表示されます。
受信パケット数		WAN 側から受信したデータの総パケット数が表示されます。
受信エラー回数		WAN 側からデータ受信を行った際に発生したエラー回数の総計が表示されます。

6-5. IPsec

1．　設定ツールのメニューから、［ステータス］－［IPsec］をクリックします。

IPsec ステータスのページが表示されます。



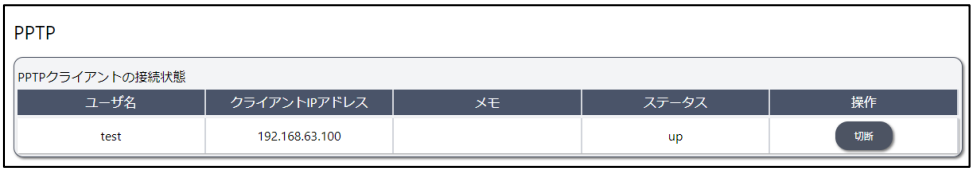
項目		内容
プロファイル名		IPsec 設定のプロファイル名が表示されます。 英文字を含めたプロファイル名を設定ください。 （数字だけのプロファイル名は無効となります）
相手 IP アドレス		IPsec 通信を行う相手先のアドレスが表示されます。
相手ネットワーク		IPsec 通信を行う相手先のローカルネットワークアドレスが表示されます。
メモ		メモに設定された文字列が表示されます。
ステータス		設定した IPsec の現在の状態が表示されます。 ➲ ステータスの詳細については、『ステータス一覧』をご覧ください。
操作	［接続］	接続動作を行います。
	［切断］	切断動作を行います。
IPsec ステータス詳細		IPsec のステータスの詳細が表示されます。

ステータス一覧

ステータス表示	状態	VPN ランプの状態
処理中	IPsec 接続設定を行っています。	消灯
待機中	IPsec 接続設定は行われていますが、IPsec 接続を試みていない状態です。	消灯
接続試行中	IPsec 接続を行おうとしています。この状態が長く続く場合、設定が間違っているか、相手側がオフラインになっている等の問題で接続できない可能性があります。	消灯
接続完了	IPsec 接続が正常に行えた状態です。	点灯

6-6. PPTP

1．　設定ツールのメニューから、［ステータス］－［PPTP］をクリックします。PPTP ステータスのページが表示されます。



項目		内容
No.		PPTP 設定の通し番号が表示されます。
ユーザ名		設定したユーザ名が表示されます。
クライアント割り当て IP アドレス		クライアントに割り当てた IP アドレスが表示されます。
メモ		メモに設定された文字列が表示されます。
ステータス		設定した PPTP の現在の状態が表示されます。 ➲ ステータスの詳細については、『ステータス一覧』をご覧ください。
操作	［切断］	切断動作を行います。

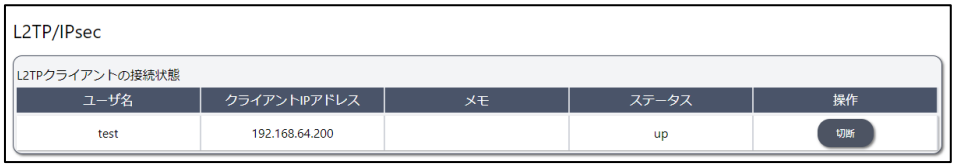
ステータス一覧

ステータス表示	状態	VPN ランプの状態
(空白)	PPTP 設定が無効になっています。	消灯
未接続	PPTP 接続設定は行われていますが、PPTP 接続を試みていない状態です。	消灯
接続中	PPTP 接続が正常に行えた状態です。	点灯

6-7. L2TP/IPsec

1．　設定ツールのメニューから、［ステータス］－［L2TP/IPsec］をクリックします。

L2TP/IPsec ステータスのページが表示されます。



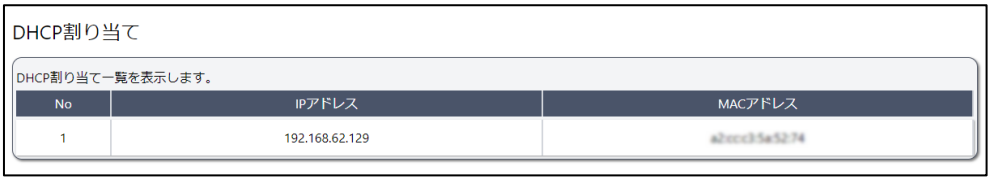
項目		内容
No.		L2TP/IPsec 設定の通し番号が表示されます。
ユーザ名		設定したユーザ名が表示されます。
クライアント割り当て IP アドレス		クライアントに割り当てた IP アドレスが表示されます。
メモ		メモに設定された文字列が表示されます。
ステータス		設定した L2TP/IPsec の現在の状態が表示されます。 ➲ ステータスの詳細については、『ステータス一覧』をご覧ください。
操作	［切断］	切断動作を行います。

ステータス一覧

ステータス表示	状態	VPN ランプの状態
(空白)	L2TP/IPsec 設定が無効になっています。	消灯
未接続	L2TP/IPsec 接続設定は行われていますが、L2TP/IPsec 接続を試みていない状態です。	消灯
接続中	L2TP/IPsec 接続が正常に行えた状態です。	点灯

6-8. DHCP割り当て

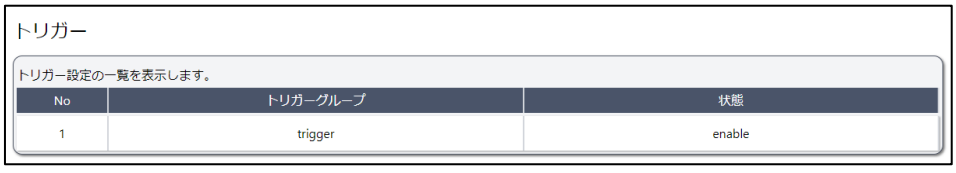
1．　DRX の DHCP テーブルは、設定ツールのメニューから、［ステータス］－［DHCP 割り当て］をクリックして表示される「DHCP 割り当て」から確認することができます。



項目	内容
IP アドレス	DRX LAN 内にある LAN 接続機器に割り当てた IP アドレスが表示されます。
MAC アドレス	上記の IP アドレスを付与された、LAN 接続機器の MAC アドレスが表示されます。 DRX を再起動すると、DHCP テーブルはすべてリセットされます。 再起動後、クライアントからの IP アドレス割り当て要求を受けたタイミングで、再度 DHCP テーブルに登録されます。

6-9. トリガー

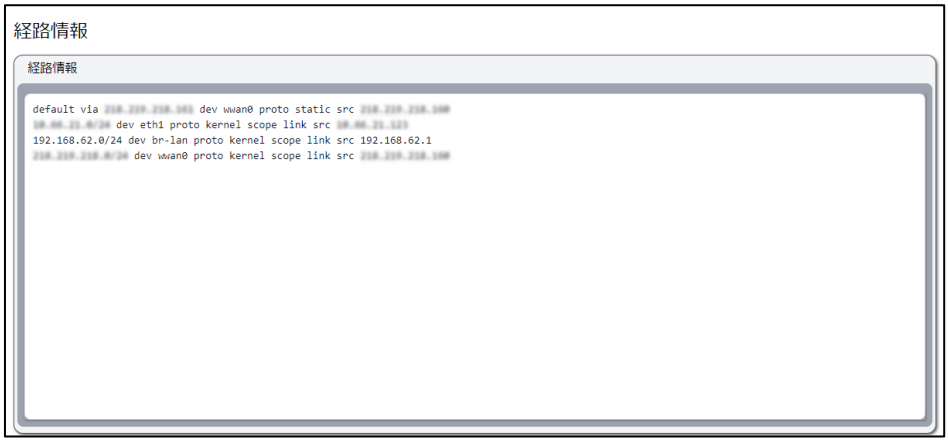
1．　設定ツールのメニューから、［ステータス］－［トリガー］をクリックします。
トリガーステータスのページが表示されます。



項目	内容
トリガーグループ	作成したトリガーのトリガー名が表示されます。
状態	トリガーの状態が表示されます。 有効：enable 無効：disable

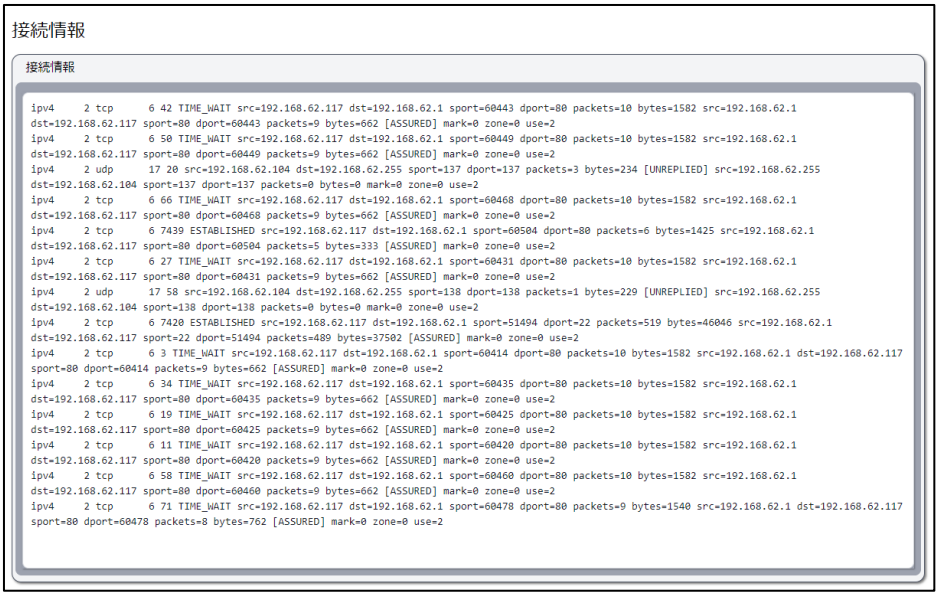
6-10. 経路情報

1．　設定ツールのメニューから、［ステータス］－［経路情報］をクリックします。
経路情報のページが表示されます。



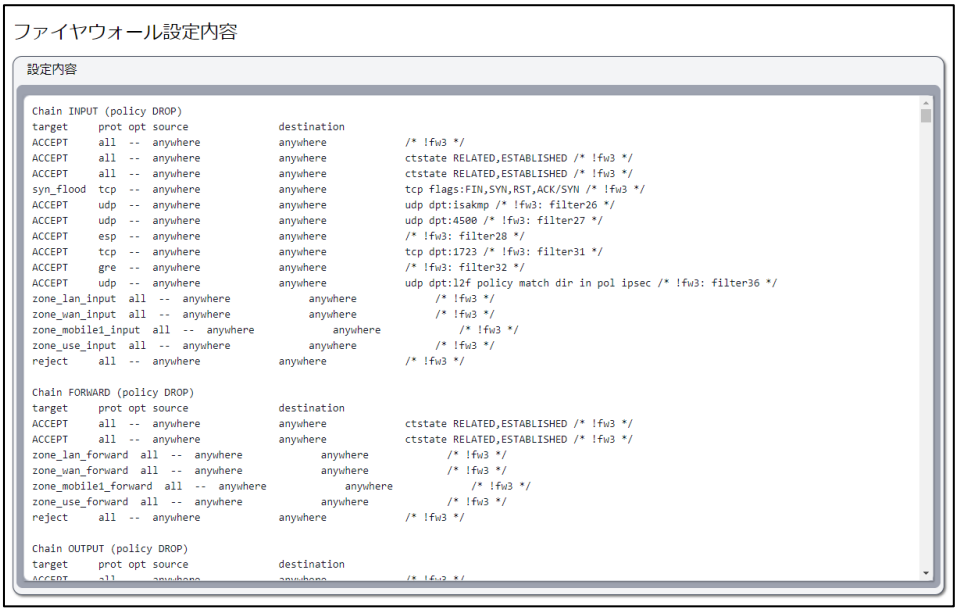
6-11. 接続情報

1．　設定ツールのメニューから、［ステータス］－［接続情報］をクリックします。
接続情報のページが表示されます。



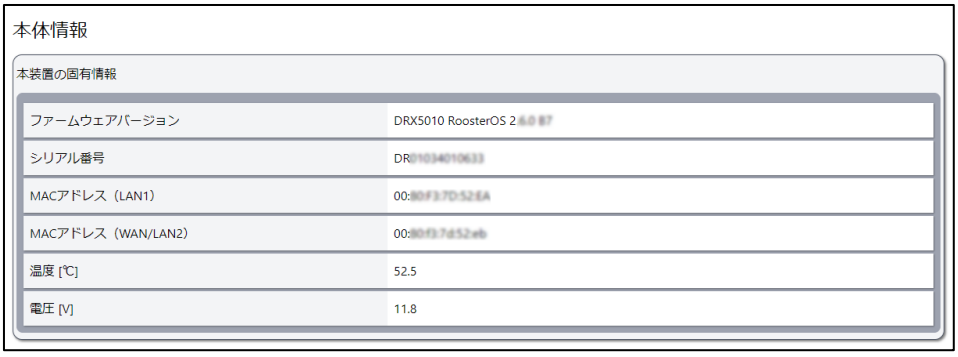
6-12. ファイアウォール設定内容

1．　設定ツールのメニューから、［ステータス］－［ファイアウォール設定］をクリックします。
ファイアウォール設定のページが表示されます。



6-13. 本体情報

1．　設定ツールのメニューから、［ステータス］－［本体情報］をクリックします。
本体情報のページが表示されます。



項目	内容
ファームウェアバージョン	ファームウェアバージョンが表示されます。
シリアル番号	DRX の本体のシリアル番号が表示されます。
MAC アドレス（LAN1）	LAN 1 側の MAC アドレスが表示されます。
MAC アドレス（WAN/LAN2）	WAN/LAN2 側の MAC アドレスが表示されます。
温度［℃］	DRX の本体内部の温度が表示されます。
電圧［V］	DRX の電圧が表示されます。

6-14. コマンド実行

1. 設定ツールのメニューから、［ステータス］－［コマンド実行］をクリックします。
   コマンド実行のページが表示されます。

2. Ping

項目	内容
宛先	ネットワークの疎通を確認する IP アドレスを入力します。
送信元	送信元のネットワーク名を選択します。

3. Traceroute

項目	内容
宛先	ネットワーク経路のリストを表示する IP アドレスを入力します。
送信元	送信元のネットワーク名を選択します。

4. Nslookup

項目	内容
ドメイン	FQDN 名から IP アドレスを表示するドメイン名を入力します。

5. Arp

項目	内容
動作	［show］：ARP テーブルを表示します。 ［clear］：ARP テーブルを消去します。
IP	ARP テーブルを表示または消去する IP アドレスを入力します。

6. 使用する機能に必要な情報を入れてから［実行］ボタン押します。
7. コマンド実行後、「実行結果」に実行内容が表示されます。

サポートのご案内

最新情報の入手

DRX に関する最新情報は、弊社ホームページから入手することができます。
また、バージョンアップ情報につきましても公開しております。

- 製品紹介ページ
  https://www.sun-denshi.co.jp/sc/product_service/router/

ご質問・お問い合わせ

DRX に関するご質問やお問い合わせは、下記へご連絡願います。

ユーザーサポートセンター

- 電話　050-1726-3104　(旧 0587-53-7606 ※変更となりました)
- メール　support@schd.sun-denshi.co.jp
  (旧 support-suncomm@sun-denshi.co.jp ※変更となりました)
- 受付時間　月曜～金曜　10:00～16:00（12:00～13:00 を除く）
  祝日、弊社休日を除く

Rooster DRX
アドバンスト Web 設定機能説明書　Ver.3.2.0

サン電子株式会社
2025 年 12 月発行　(251215)