SUNCORPORATION

デュアル SIM 対応ルータ

Rooster DRX

取扱説明書　第 2.6.3 版

https://www.sun-denshi.co.jp/sc/

はじめに

表記について

本取扱説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しております。

	人体に危険を及ぼしたり、装置に大きなダメージを与えたりする可能性があることを示しています。 必ずお守りください。
	機能停止を招いたり、各種データを消してしまったりする可能性があることを示しています。 十分に注意してください。
	関連する情報を記載しています。参考にお読みください。

製品名について

本取扱説明書では、「DRX5010」「DRX5002」を「本製品」または「DRX」と省略して記載しております。
各機種の対応機能については、対応機能一覧をご覧ください。

商標について

ソフトウェアに関する重要なお知らせ

本製品に組み込まれたソフトウェアは、複数の独立したソフトウェアコンポーネントで構成され、個々のソフトウェアコンポーネントは、それぞれ にサン電子株式会社または第三者の著作権が存在します。
これらのソフトウェアコンポーネントの中には、フリーソフトウェアに該当するものがあり、GNU General PublicLicense または Lesser General Public License 以下、「GPL/LGPL」といいます）のライセンスに基づき実行形式のソフトウェアコンポーネントを配布する条件として、当該コンポーネントのソースコードの入手を可能にするように求めています。
当該「GPL/LGPL」の対象となるソフトウェアコンポーネントに関しては、弊社サポートセンターまでお問い合わせください。なお、ソースコードの内容等についてのご質問はお答えしかねますので、予め御了承ください。
「GPL/LGPL」の適用を受けないソフトウェアコンポーネント及びサン電子株式会社自身 が開発もしくは作成したソフトウェアコンポーネントは、ソースコード提供の対象とはなりませんのでご了承ください。
「GPL/LGPL」に基づいて配布されるソフトウェアコンポーネントは無償でお客様に使用許諾されますので、適用法令の範囲内で、当該ソフトウェアコンポーネントの保証は、明示かつ黙示であるかを問わず一切ありません。適用法令の定め、又は書面による合意がある場合を除き、著作権者や当該ソフトウェアコンポーネントの変更・再配布を為し得る者は、当該ソフトウェアコンポーネントを使用したこと、又は使用できないことに起因する一切の損害についてなんらの責任も負いません。
当該ソフトウェアコンポーネントの使用条件や遵守いただかなければならない事項等の詳細は、各「GPL/LGPL」をお読みください。
本製品に組み込まれた「GPL/LGPL」の対象となるソフトウェアコンポーネントをお客様自身でご利用頂く場合は、対応するライセンスをよく読んでから、ご利用くださるようにお願い致します。
尚各ライセンスはサン電子株式会社以外の第三者による規定のため､原文(英文)は以下のホームページをご覧いただくようにお願いします。

- https://www.sun-denshi.co.jp/sc/gpl.html

安全上のご注意（必ずお守りください）

ここに記載している注意事項は、安全に関わる重要な内容ですので、必ず守ってください。
本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。

警告	この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。
注意	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関する拡大損害を示しています。
禁止	禁止行為（してはいけないこと）を示しています。
強制	強制行為（必ずしなければいけないこと）を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。
いずれも重要な内容を記載していますので、必ず守ってください。

警告


分解禁止

本製品を分解したり、改造したりしないでください。

➔ 感電、火災、故障の原因になります。


禁止

近くに雷が発生したときには電源プラグを本体から抜いてご使用をお控えください。

➔ 落雷が火災、感電、故障の原因となるときがあります。


禁止

本製品に水などの液体をかけたり、異物を入れたりしないでください。

➔ 感電や火災、故障の原因になります。万一、本製品に液体がかかったり、異物が入ったりした場合は、電源プラグを本体から抜いて、点検修理を依頼してください。


強制

製品から煙、異臭、異常音が発生した場合は、電源プラグを本体から抜き、本製品を接続している機器からケーブルを取り外してください。また、点検修理を依頼してください。

➔ 火災の原因になります。


禁止

電源ケーブルを傷つけないでください。

➔ 感電、火災の原因になります。


強制

本製品を設置、移動する時は、電源プラグを抜いてください。

➔ 故障、火災の原因になります。


禁止

梱包のポリ袋などは、小さいお子様の手の届く所に置かないでください。

➔ 小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。


強制

AC アダプタ使用時、AC アダプタは確実に根元まで差し込んでください。また、AC アダプタとコンセント周辺のほこりは、定期的（半年に一回程度）に取り除いてください。

➔ 電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。


禁止

強い衝撃を与えたり、落下させたり、投げ付けたりしないでください。

➔ 機器の故障、火災の原因となります。


禁止

ガソリンスタンドなど、引火、爆発の恐れがある場所では、使用しないでください。

➔ プロパンガス、ガソリンなど引火性ガスや粉塵が発生する場所で使用すると、爆発や火災の原因となります。


禁止

電子レンジなどの加熱調理機や高圧容器に、本製品を入れないでください。

➔ 機器の発熱、発煙、発火や回路部品を破損させる原因となります。


強制

指定アンテナ以外の外部アンテナを接続しないでください。

➔ 指定以外の外部アンテナを接続した場合、電波法の規定に抵触する可能性があります。

⚠注 意

禁止

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

➔ 本製品の故障や破損などによって、発煙、発火、感電の原因になります。
下記の環境には、特にご注意ください。

- 製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所

禁止

専用の電源プラグまたは規格に合った電源以外を使用しないでください。

➔ 他の電源を使用すると、故障、火災の原因になります。

禁止

本製品を壁等に固定する際には、専用の固定セット(取り付け金具、ネジ)を使用してください。
他の取り付け金具およびネジの使用や直接のネジ止めによる固定は行わないでください。

強制

30cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

➔ そのまま使用すると、重大な事故になる可能性があります。

禁止

本製品は日本国内向けに設計されています。

➔ 海外ではご使用にならないでください。

この装置は、クラスＡ機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。
この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

医用電気機器近くでの取り扱いについて

本記載の内容は「医療機関における携帯電話等の使用に関する指針(平成 26 年 8 月 19 日)」（電波環境協議会）および「各種電波利用機器の電波が植込み型医療機器等へ及ぼす影響を防止するための指針(平成 30 年 7 月)」（総務省）を参考にしています。

警告

強制

医療機関(病床数 20 床未満の診療所も含む)では次のことを守って使用してください。ただし本製品の使用については、各医療機関の指示に従うようにしてください。

- 本製品を医用電気機器に密着して使用しないでください。
- 本製品を病室、診療室で使用する場合には、医用電気機器から 1m 程度以上離してください。
- 待合室、ロビー、食堂、廊下、エレベータホール等で医用電気機器を使用している患者がいる場合、本製品を医用電気機器から 1m 程度以上離してください。
- 手術室、集中治療室（ICU）、検査室、治療室には本製品を持ち込まないでください。

強制

本製品を植込み型医療機器の装着部位から 15cm 程度以上離してください。

➔ 15cm 程度の離隔距離が確保できない恐れがある場合には、事前に本製品の電源を切ってください。

自宅療養などにより医療機関の外で、埋込み型医療機器を使用される場合には、電波による影響について個別に医用電気機器メーカーなどにご確認ください。

ご使用時の取り扱いについて

ご使用にあたってのお願い

- 本製品周辺で静電気的障害を発生させないでください。
  - ➔ 本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。
- 本製品はていねいに取り扱ってください。
  - ➔ 本製品に強いショックを与えると破損の原因になります。
- 本製品のお手入れは、電源を切った状態で行ってください。
  - ➔ 誤動作や故障の原因になります。
- 本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。汚れがひどい場合は、柔らかい布に台所中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。
  - ➔ 揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。
- 極端な高温、低温は避けてください。
  - ➔ 温度は-20～65℃、湿度は 25～85%の範囲でご使用ください。
- 使用中、本製品が温かくなることがありますが、異常ではありませんのでそのままご使用ください。
- 長い時間連続して通信をした場合など、本製品が熱くなることがありますので取り扱いにご注意ください。
- 一般の電話機やテレビ・ラジオなどをお使いになっている近くで使用すると、影響を与える場合がありますので、なるべく離れた場所でご使用ください。
- お使いになる環境や接続する外部装置によっては、本製品がノイズによる影響を受け、無線特性が劣化する場合があります。
- 本製品に貼付してある銘板シール（製造番号等印字シール）を剥がさないでください。
  - ➔ 本シールは、技術基準適合証明、技術基準適合認証を取得していることを示すものであり、剥がした状態での使用は法律で禁止されています。

お客様が本製品を利用して公衆に著しく迷惑をかける不良行為を行った場合、法律、条例（迷惑防止条例等）に従い処罰されることがあります。

ご使用後の破棄あたって

本製品をご使用後 破棄される場合に安全な破棄を実現するため、以下の項目を実施することを推奨いたします。

- 本製品内の設定を初期化してください。
- 本製品内のログを削除してください。
- SunDMS をご使用の場合は、SunDMS の Rooster 登録を削除してください。

地球環境保全のため、次のことにご協力ください。

- 本製品および付属品は、不燃物として処分してください。
- 廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
- 一般ごみとして、家庭で焼却処分しないでください。
- 処分方法によっては有害物質が発生する可能性があります。

ご注意

- 本製品は日本の法規制に準拠しており、日本国内での使用を想定して設計されています。
  ➔ 海外でのご使用をお考えの場合は、弊社までご相談ください。
- 本製品は、医療・原子力・航空・海運・軍事・宇宙産業など 人命に関わる場合や高度な安全性・信頼性を必要とするシステムや機器としての使用またはこれらに組み込んでの使用を意図した設計・製造はしておりません。
  このようなシステムや機器としての使用またはこれらに組み込んで本製品が使用されることで、お客様もしくは第三者に損害が生じても、かかる損害が直接的または間接的または付随的なものであるかどうかにかかわりなく、 当社としましては一切の責任を負いません。お客様の責任において、このようなシステムや機器としての使用またはこれらに組み込んで使用する場合には、事前に使用環境・条件を考慮し十分に評価を実施した上でご使用ください。
- 取扱説明書について、次の点にご注意ください。
  1. 本製品は無線によるデータ通信を行う事が出来る装置です。本製品の不具合、誤動作又は停電、回線障害、その他の外部要因によって通信障害が発生したために生じた損害等については、当社としては責任を負いかねますので、あらかじめご了承ください。
  2. 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
  3. 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
  4. 本取扱説明書の内容につきましては、万全を期して作成致しましたが、万一ご不審な点や、ご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点等ございましたら、当社までご連絡ください。
  5. 適用した結果の影響につきましては、4 項にかかわらず責任を負いかねますので、ご了承ください。
  6. 本取扱説明書で指示されている内容につきましては、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害につきましては、保証期間内であっても責任を負いかねますので、ご了承ください。
- 高精度な制御や微弱な信号を取り扱う電子機器の近くでは、本製品の電源を切ってください。
  ➔ 電波により電子機器が誤作動するなどの悪影響を及ぼす原因となります。

  【ご注意いただきたい電子機器の例】
  補聴器、植込み型心臓ペースメーカおよび植込み型除細動器、その他医用電気機器、その他の自動制御機器など。植込み型心臓ペースメーカおよび植込み型除細動器、その他医用電気機器を使用される方は、各医用電気機器メーカーもしくは販売業者に電波による影響についてご確認ください。
- アンテナ（内蔵アンテナを使用の場合は本製品）は人体から 20cm 以上離れた場所に設置してください。
  他の機器のアンテナや無線機と同じ場所に設置したり、一緒に使用したりしないでください。
- 外部アンテナの設置について
  本製品に複数の外部アンテナを接続する場合（LTE、5G、無線 LAN など）や他の無線用アンテナ・無線機能内蔵装置の近傍に設置する際は、電波干渉を避けるため、各アンテナ間を一定距離（目安 20cm 以上）離して設置してください。
  性能低下や、通信が途絶える、通信ができない等の原因となります。
  ロッドアンテナを本製品に取り付ける場合は、なるべくアンテナ同士の距離が広がる様に取り付けいただくことをお勧めします。

ご使用機種の対応機能について

機能ごとの対応機能の一覧

本マニュアルは、DRX シリーズ全製品に共通するマニュアルです。
お使いの DRX がどの機能に対応しているかは、下記の対応表でご確認ください。また、各機能の中で機種により差分がある箇所には、下記の機種マークで場合分けして記載しております。

DRX5010 DRX5002

機能 / 機種(DRX50xx)	DRX5010	DRX5002
時刻設定	○	○
おやすみモード	○	○
電源制御	○	○
LAN	○	○
WAN	○	○
モバイル通信 (NTT ドコモ、KDDI、ソフトバンク)	○	○
WakeOn 着信	○	○
無線 LAN(WLAN)	○	−
回線バックアップ	○	○
モバイル副回線監視	○	○
アドレス解決	○	○
DNS	○	○
DHCP	○	○
CLI	○	○
WEB	○	○
WAN ハートビート	○	○
SunDMS	○	○
ログ管理	○	○
PPTP パススルー	○	○
IPsec パススルー	○	○
スタティックルーティング	○	○
フィルタリング (FORWORD、MAC、INPUT、DNS)	○	○
バーチャルサーバ	○	○
DMZ	○	○
IPsec	○	○
PPTP	○	○
L2TP/IPsec	○	○

無線LANご使用時におけるセキュリティに関するご注意 DRX5010

無線 LAN では LAN ケーブルを使用する代わりに電波を利用してパソコン等と無線 LAN アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。
その反面、電波はある範囲内であれば障害物（壁等）を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

[通信内容を盗み見られる]
悪意ある第三者が、電波を故意に傍受し、
・ID やパスワード又はクレジットカード番号等の個人情報
・メールの内容
等の通信内容を盗み見られる可能性があります。

[不正に侵入される]
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、
・個人情報や機密情報を取り出す（情報漏洩）
・特定の人物になりすまして通信し、不正な情報を流す（なりすまし）
・傍受した通信内容を書き換えて発信する（改ざん）
・コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）
などの行為をされてしまう可能性があります。

本来、無線 LAN 製品は、セキュリティに関する仕組みを持っていますので、その設定を正しく行って製品を使用することで、上記問題が発生する可能性は少なくなります。
セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

無線LANの電波に関するご注意 DRX5010

1. 5GHz帯域の電波の屋外での使用は電波法により禁じられています。
2. 本製品は IEEE802.11n(2.4GHz帯), IEEE802.11g, IEEE802.11b通信利用時、2.4GHz帯域の電波を使用しており、同じ周波数帯を電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が使用しています。
   ・電子レンジの近くで本製品を使用しないでください。無線LANの通信に影響します。
   ・近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認ください。
   ・万が一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに周波数を変更ください。
   ・その他、本製品から移動体識別用の特定小電力無線局に対して有害な電波干渉の事例が発生した場合、弊社ユーザーサポートセンターまでお問い合わせください。
3. 本製品は IEEE802.11n(2.4GHz帯), IEEE802.11g, IEEE802.11b通信利用時、2.4GHz全帯域を使用する無線設備であり移動体識別装置の帯域を回避可能です。変調方式としてDS-SS方式及びOFDM方式を採用しております。
4. 新4K8K衛星放送と無線LANが相互に電波干渉し、無線LANの通信や衛星放送の受信に影響することがあります。シールド性能の高い適切な衛星放送用受信設備を使用してください。詳しくは、総務省のホームページ（4K放送･8K放送 情報サイト）を参照ください。

目次

1章　DRXの概要

この章では、DRX の概要や特長、外観などについて説明します。

1-1. 概要

本製品は 4G モバイル通信モジュールを内蔵したルータです。

各社 LTE パケット通信サービスを利用し、パケット通信を行うことができます。

本製品では、4G モバイル通信モジュールをモバイル通信端末と記載しています。
本製品を LTE ネットワークへ接続するためには、各通信事業者とのご契約と、SIM カードを内部 SIM カードソケットに装着する必要があります。

本製品には、電気通信事業法第 56 条第 2 項の規定に基づく端末機器の設計について認証を受けた以下の設備が組み込まれております。
・ 機器名称：AMM574、設計認証番号：D190148003

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 3,7 および 19 に規定される以下の設備が組み込まれております。
・ 機器名称：AMM574、工事設計認証番号：003-190181

1-2. 主な特長

無線LAN機能を搭載　DRX5010

無線 LAN アクセスポイント機能（親機）を搭載し、別途機器を追加することなくタブレットなどの無線 LAN 装置と接続できます。

2 枚SIM対応で冗長運用が可能

SIM スロットが 2 個備わっており、それぞれ異なるキャリアの SIM を挿入することで冗長化が実現します。これにより通信障害発生時に主回線から副回線に切り替えお客様の大切な通信を継続します。

また定期的に副回線を接続、確認するモバイル副回線確認機能で、バックアップの健全性を確認させることができます。

内蔵アンテナで簡単設置

WAN 側へ通信するためのアンテナが内蔵されており別途アンテナを購入する必要はなく設置が簡単にできます。また、内蔵アンテナで通信が困難な場合、外部アンテナの接続が可能です。
（例：金属製ボックスに DRX 本体を納める場合等）

高スループットを実現

高速通信可能で大容量通信（高解像度のネットワークカメラ等）を行う現場に最適です。また、VPN 通信時も高速となりリモートメンテナンス運用もスムーズに実現します。
※RX シリーズと比較

各種VPN機能に対応

IPsecVPN、PPTP（サーバ機能）、L2TP/IPsec v2（サーバ機能）に対応しております。
※L2TP/IPsec v3 対応予定

LTEマルチキャリア対応

NTT ドコモ、ソフトバンク、KDDI 及び各種 MVNO に対応しており、キャリアに合わせて機器を選定する必要がなく、設置後のキャリア見直しも対応可能です。

長期安定運用実現

電波状態による通信エラーなどを防ぐため、定時リセット設定や、死活監視など、自己復帰が可能な機能 ASC（Autonomous Stable Connection）を搭載し、無人環境下でも安定運用が可能です。

広い温度範囲

動作温度範囲を-20～65℃と厳しい IoT/M2M の環境下でも安定運用が可能です。

低消費電力

「おやすみモード」を搭載し、通信を行っていない待機時に消費電力を抑えることができます。

IoT/M2M 遠隔管理サービス「SunDMS」搭載

Rooster シリーズの安心・安定運用をより高い次元で行うため、ファームウェアの更新やログ、温度電圧管理、死活監視などの遠隔集中管理機能を無償（一部有償あり）で提供します。

1-3. 設定フロー

DRX を使用してインターネット接続を行う場合、最低限 2 までの設定を行ってください。
3 の設定は、必要に応じて行ってください。

1．DRX の設置
- ・同梱物の確認
  - ➲『1-4. 同梱物の確認』
- ・機器の接続
  - ➲『2-3. Rooster DRX の接続方法』
- ・クライアント PC の設定
  - ➲『2-6. パソコンの設定』

↓

2．DRX の設置
- ・LAN、ログインパスワード、時刻設定
  - ➲『3-2. LAN の設定』
  - ➲『3-3. ログインパスワードの設定』
  - ➲『3-4. 時刻の設定』
- ・モバイル通信端末の設定、または WAN の設定
  - ➲『4 章 モバイル通信端末の設定』
  - ➲『3-8. WAN の設定』

↓

3．DRX の詳細設定（必要な場合のみ）
- ・無線 LAN の設定 DRX5010
  - ➲『5 章 無線 LAN の設定』
- ・着信設定
  - ➲『4-3. WakeOn 着信の設定』
- ・各種サービス
  - ➲『3-5. メールアカウントの設定』
  - ➲『7 章 各種サービス設定』
  - ➲『7-3-1. アドバンスドモード』
- ・ネットワーク設定
  - ➲『8 章 ネットワーク設定』

1-4. 同梱物の確認

パッケージには、次のものが同梱されています。

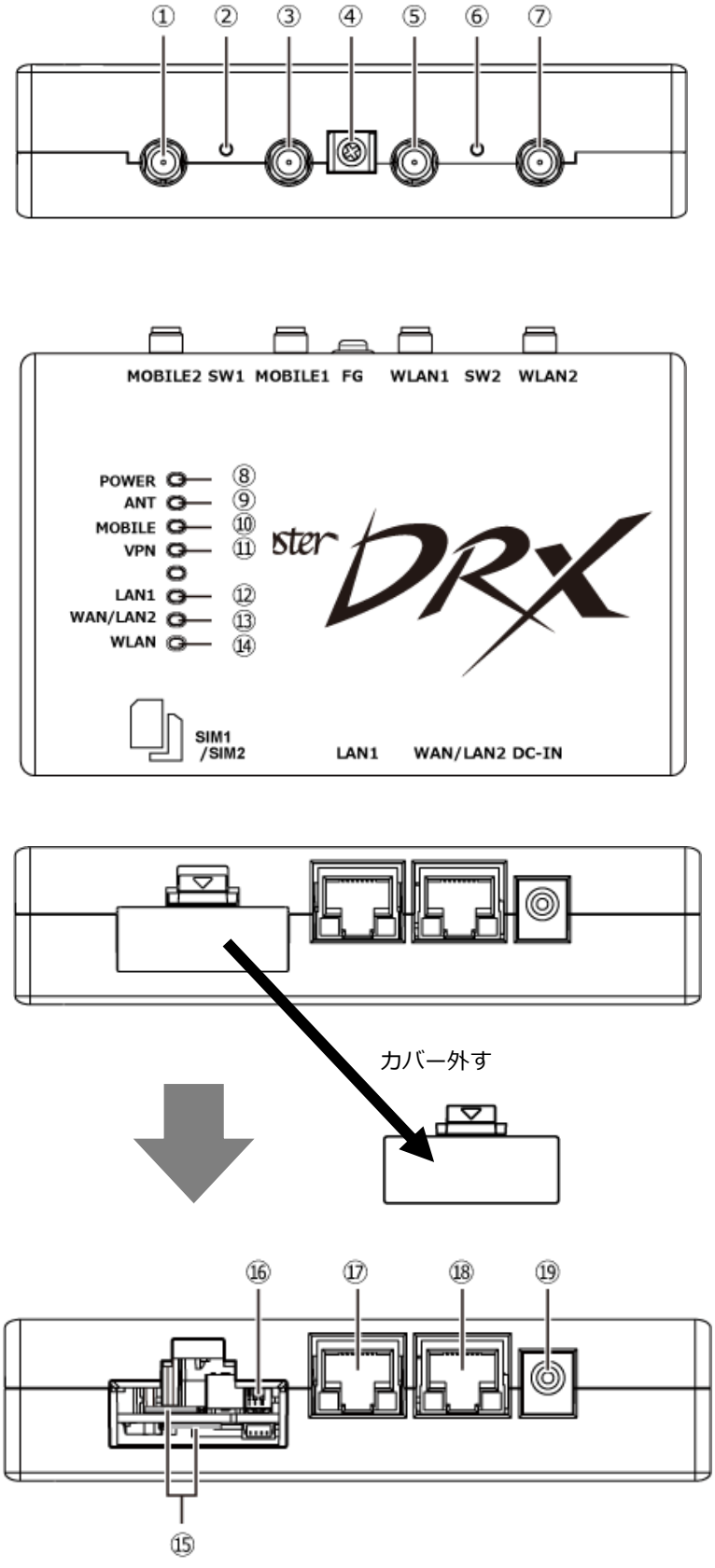
万一不足しているものがありましたら、お買い求めの販売店、もしくはサポートセンターにご連絡ください。

DRX

- DRX 本体　1 台
- スタートアップマニュアル（保証書付）　1 部

> 付属品に LAN ケーブル、アンテナおよび AC アダプタ等の電源は含まれません。
> 設定で使用する LAN ケーブルにつきましてはご利用の接続機器の速度に合わせてご用意ください。
> - LAN ケーブル：カテゴリ 5e 以上
> - アンテナ、AC アダプタ：
>   オプション品として取り扱っております。弊社サポートまでお問い合わせください。

1-5. 各部名称と機能



【DRX5010 の場合】

No.	名称	機能
①	MOBILE2 コネクタ（SMA）	外部アンテナ（モバイル通信用）を接続します。
② ⑥	SW1 スイッチ SW2 スイッチ	SW1 スイッチを先の細いピンなどを使って 3 秒以上押し続けると、シャットダウンします。 SW1 スイッチと SW2 スイッチを同時に 3 秒以上押し続けると、一旦全点灯（ANT 赤以外）した後、WLAN ランプ、VPN ランプ、MOBILE ランプ、ANT 緑ランプの順で消灯し、工場出荷時の設定に戻り、再起動します。 SW1、および SW2 スイッチを使用して初期化する場合は、『6-2. 設定情報の消去』をご覧ください。
③	MOBILE1 コネクタ（SMA）	外部アンテナ（モバイル通信用）を接続します。
④	FG 端子	アース線を接続します。
⑤	WLAN1 コネクタ（無線 LAN）	外部アンテナ（無線 LAN 通信用）を接続します。 DRX5010
⑦	WLAN2 コネクタ（無線 LAN）	外部アンテナ（無線 LAN 通信用）を接続します。 DRX5010
⑧	POWER ランプ	DRX の通電状態が表示されます。
⑨	ANT ランプ	電波状態を表示します。
⑩	MOBILE ランプ	モバイル通信端末の動作状態が表示されます。
⑪	VPN ランプ	VPN セッション（IPsec、PPTP、LT2TP/IPsec）の動作状態が表示されます。
⑫	LAN1 ランプ	LAN1 ポート（⑰）への LAN 接続機器の接続状態が表示されます。
⑬	WAN / LAN2 ランプ	WAN/LAN2 ポート（⑱）への WAN/LAN 接続機器の接続状態が表示されます。
⑭	WLAN ランプ	無線 LAN の通信状態が表示されます。 DRX5010
⑮	SIM カード挿入口 (上：SIM1、下：SIM2)	nano SIM カード (12.3×8.8mm) を挿入します。 挿入口は上下各 1 ずつあり、 2 枚の SIM カードを挿入できます。
⑯	DIP スイッチ	拡張用
⑰	LAN1 ポート	LAN ケーブルで LAN 接続機器、ハブなどを接続します。
⑱	WAN/LAN2 ポート	LAN ケーブルで WAN 接続機器や LAN 接続機器、ハブなどを接続します。 ➲ LAN2 ポートとして使用する場合は『3-8.WAN の設定』を「LAN として使用」に選択してください。
⑲	DC IN コネクタ	DC 電源プラグを接続します。

➲それぞれのランプの状態は、『1-6. ランプの状態と働き』をご覧ください。
本製品の寸法については『2-2. 取り付け例（オプションの固定金具を使用した場合）』をご覧ください。

- 電源を OFF にするときは、②の SW1 スイッチでシャットダウンすることを推奨します。
- ④の FG 端子の接続は必須ではありませんが、お客様の使用用途に応じて必要と思われる場合は接続してご利用ください。
- 設置場所の電波状況が悪く内部アンテナを使用せずに外部モバイルアンテナを使用する場合、①③に本製品に適した外部アンテナをご使用ください。
- ⑰の LAN1 ポートには WAN 回線は接続できません。
- ⑰の LAN1 ポート、⑱の WAN/LAN2 ポートは全 2 重対応の機器と接続ください。
  （半 2 重での接続は非対応です）
- SIM カードの抜き差しをするときは DRX の電源を OFF にしてから行ってください。
- 無線 LAN を使用する場合、⑤⑦に本製品に適した無線 LAN アンテナを接続する必要があります。 DRX5010

1-6. ランプの状態と働き

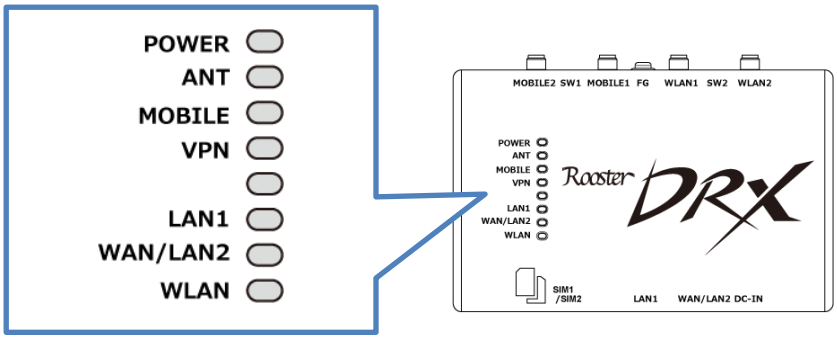
ランプ状態説明

ランプ状態	補足
消灯	消灯状態が続く状態です。
点灯	点灯状態が続く状態です。
点滅	点灯と消灯を１秒に１回の間隔で繰り返す状態です。
早い点滅	点滅より速く点灯と消灯を繰り返す状態です。
遅い点滅	消灯状態から４秒に１回点滅します。

ランプ点灯・点滅パターン一覧

名称	ランプ状態	補足
POWER	**点灯**	電源が入っていて、使用可能な状態です。
	点滅	起動中、またはおやすみモードへの移行中です。
	遅い点滅	おやすみモード中です。
	消灯	電源が入っていません。
VPN	**点灯**	VPN 接続が確立された状態です。
	消灯	VPN 接続が行われておりません。
MOBILE	**点滅**	接続を試行している状態です。
	点灯	接続が確立された状態です。
	消灯	接続が行われていません。
ANT	**点灯**	モバイル通信圏内（電波 4: -101dBm 以上）
	点滅	モバイル通信圏内（電波 3：-113～-103dBm）
	点滅	モバイル通信圏内（電波 2：-121～-115dBm）
	点灯	モバイル通信圏内（電波 1：-131～-123dBm）
	消灯	モバイル通信圏外（電波 0 ：-131dBm 未満）、モバイル通信未使用
LAN・WAN	**早い点滅**	データが流れています。
	点灯	リンクしています。
	消灯	リンクしていません。
WLAN DRX5010	**点灯**	無線 LAN が動作状態です。
	消灯	無線 LAN が停止状態です。

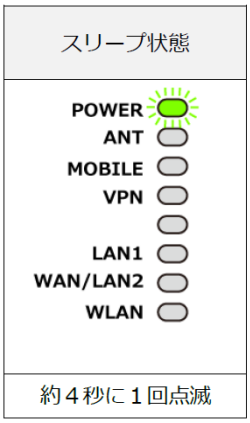
ランプの表示と状態　早見表



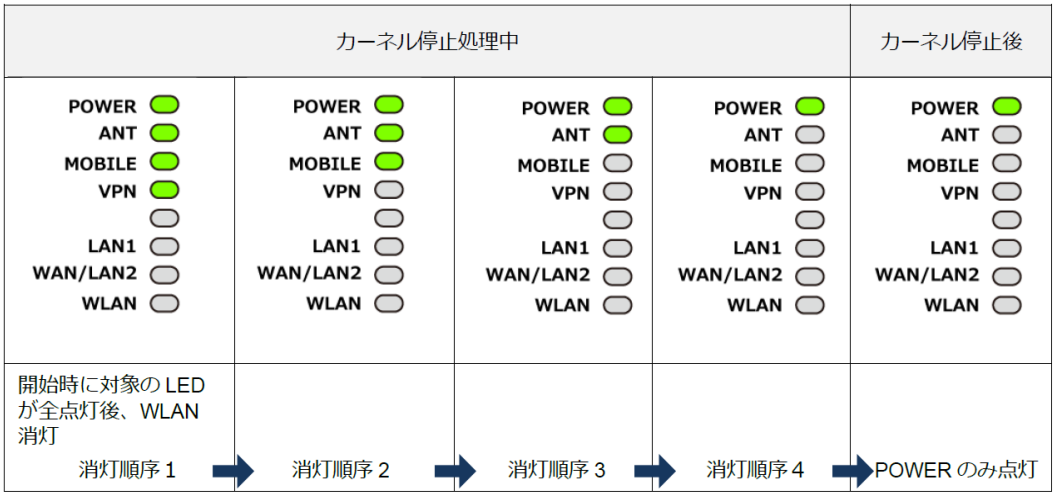
- 電源投入時

通電直後	起動中	カーネル起動中		
POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN	POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN	POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN	POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN	POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN
	→ 1秒間隔で点滅	→ 点灯順序 1	→ 点灯順序 2	→ 点灯順序 3 →
カーネル起動中	各機能起動中	起動完了		
POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN	POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN	POWER ANT MOBILE VPN LAN1 WAN/LAN2 WLAN		
→ 点灯順序 4	→	→		

- スリープ時



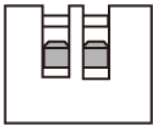
- 停止時



「ランプの表示と状態」は DRX5010 を基準にマニュアルの記載をしております。
また、名称のないランプは点灯しません。

1-7. DIPスイッチ

DIP スイッチは『全て OFF』（下側に倒す）でご使用ください。



DIP スイッチが全て OFF の状態

- DIP スイッチの変更は、電源が OFF の状態で行ってください。
- DIP スイッチを変更した場合、正常に動作しません。誤って変更してしまった場合は必ず DIP スイッチを工場出荷状態（全て OFF）に戻してください。

1-8. 電源コネクタ

電源仕様

電圧	DC5～27.4V（±5%）
電流	1A 以上（12V 時）（12W 以上）
電圧リップル	100mVp-p 以下
電源コード	電流容量　2A 以上
コネクタ	丸型 DC 電源ジャック(中心+極) 内径 2.1mm 外径 5.5mm

使用される電源はあらかじめ動作確認の上ご使用ください。

本体、又はモバイル通信モジュールのファームウェア更新中は電源を切断しないでください。

電源を切断する場合、SW1 スイッチ（『1-5. 各部名称と機能』）を押下するか、CLI コマンドでシャットダウンした後に行うことを推奨します。

2章　DRXの導入

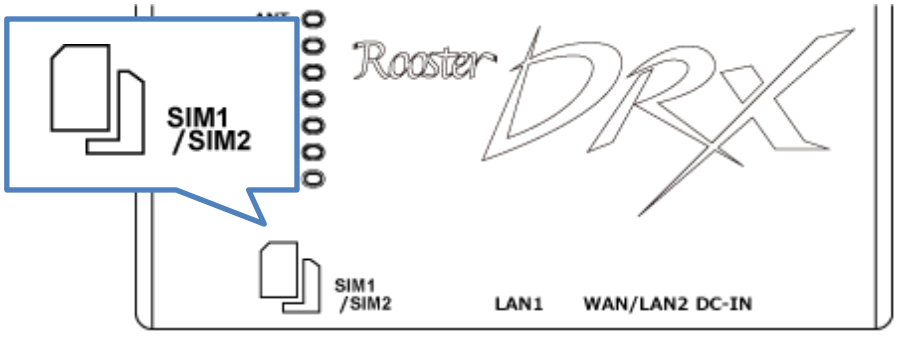
この章では、DRX の設置方法や接続方法、初期設定について説明します。

2-1. SIMカードの挿入方法

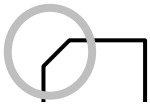
1．DRX の電源を OFF にします。

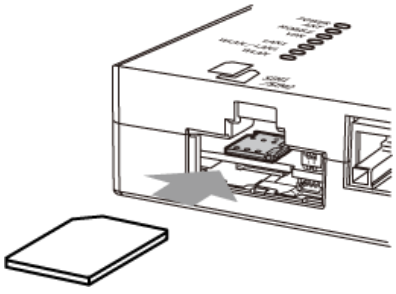
2．SIM カードの挿入口を確認します。SIM の挿入口は、DRX 側面にあり、天面には挿入口を示す SIM のイラストが印字されています。

3．SIM 挿入口のカバーを外し、SIM カードを挿入します。SIM の挿入口は 2 つあり、上部の SIM1 と下部の SIM2 に分かれています。SIM カードは、本体に表示されている SIM のイラストと同じ向きで「カチッ」と音がし、ロックされるまで挿入してください。

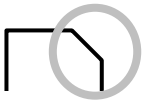


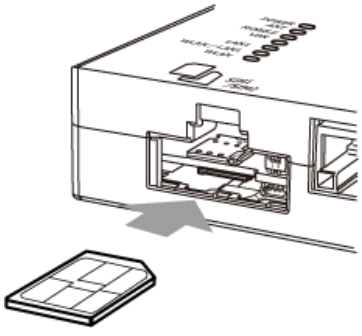
SIM1 の挿入口に入れる場合





SIM2 の挿入口に入れる場合

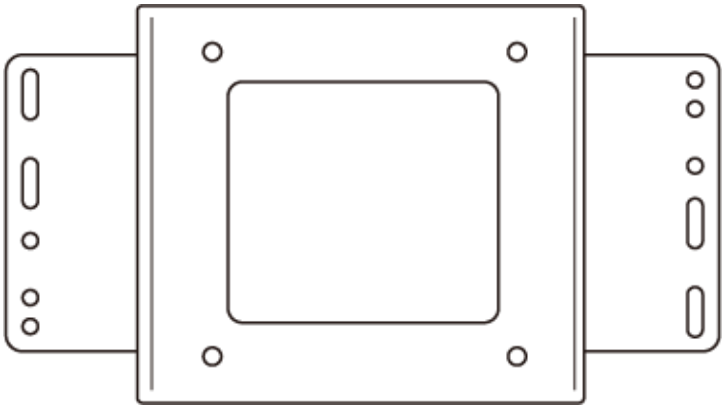




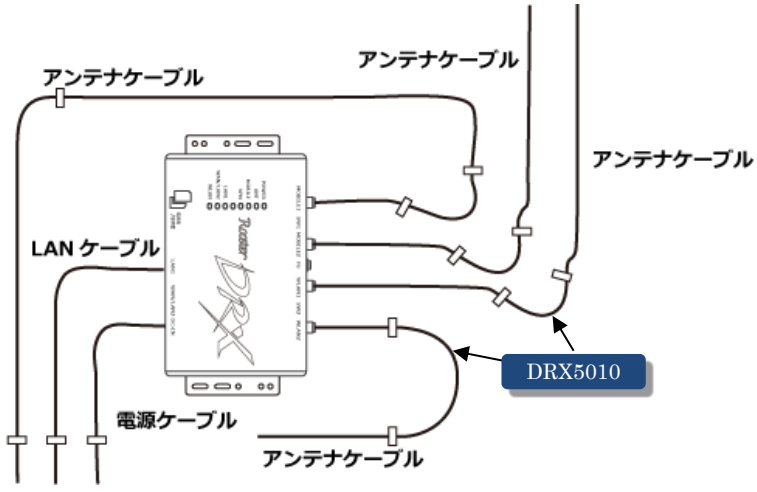
2-2. 取り付け例（オプションの固定金具を使用した場合）

1．直径 3.5mm の取り付け穴を 137mm の間隔で、2 箇所開け、お客様でご用意いただいたネジで本製品を固定します。詳細は、固定金具マニュアルを参照ください。

▶ 取り付け場所は、平滑な場所をお選びください。



2．ケーブルを接続します。



ケーブルの接続例

3．アンテナをコネクタに接続します。

設置の注意事項

- 設置場所は平滑な場所をお選びください。また、本製品設置後、ケーブルの抜き差しが十分行えるようなスペースがある場所をお選びください。
- ケーブル類の引きまわしはコネクタに無理な力がかからないように余裕を持たせてください。
- ケーブル類を伝わる水滴が、本製品に侵入しないように、コネクタ近くで一旦コネクタより下方にケーブル類を引きまわしてください。
- 接続するアンテナは、本製品に適合したアンテナをご使用ください。
- 無線 LAN 通信アンテナとモバイル通信用アンテナを間違えて接続するとコネクタが壊れますのでご注意ください。 DRX5010
- アンテナの接続には無理な力が加わることのないようにご注意ください。
  （締め付けトルク値 0.9(N・m)で取り付けてください）
- 適合したアンテナについては弊社までお問い合わせください。
- SIM カード挿入口を下向きに設置しないでください。

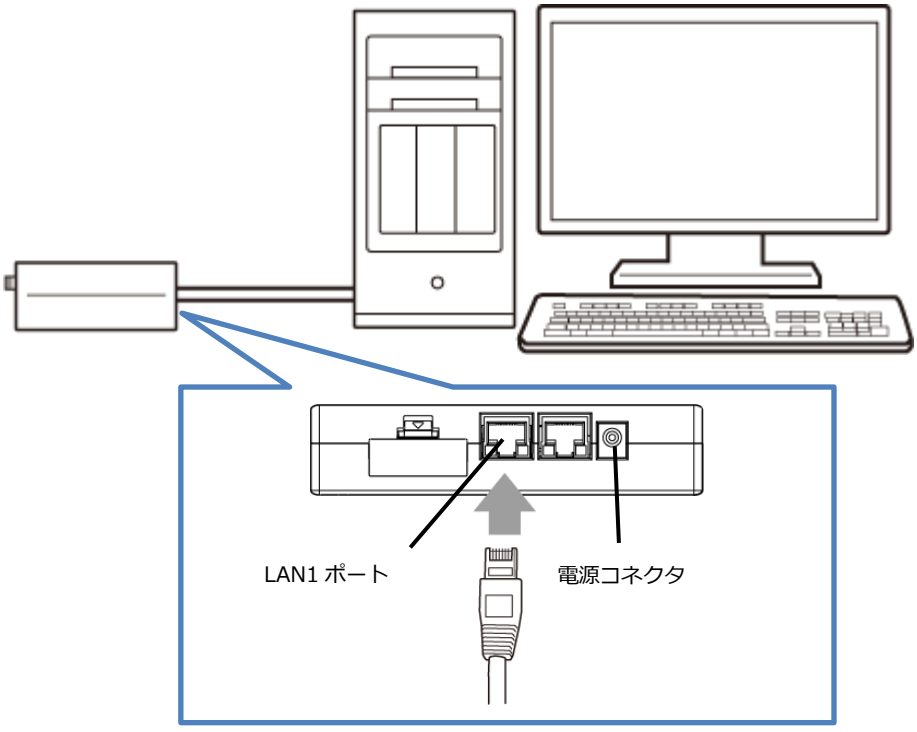
2-3. DRXの接続方法

DRX の設定画面へのアクセスは LAN ポートからのみとなります。
設定を行う場合は、パソコンをご用意ください。

2-3-1. 必要な環境

- TCP/IP が利用できる OS（Windows、MacOS、各種 UNIX など）を搭載し、イーサネットポートを搭載したパソコン
- LAN ケーブル
- Google Chrome のブラウザ
  ▶ 上記以外のブラウザでは、正常に動作しない可能性があります。

2-3-2. 接続方法



1. DRX とパソコンの電源が入っていないことを確認してください。
2. LAN1 ポートにクライアントとなるパソコンを接続してください。
3. アンテナをアンテナコネクタに接続します。(外部アンテナを接続する場合)
4. DRX の電源コネクタに電源プラグを接続してください。次に、電源プラグに給電を開始してください。AC アダプタ使用時は、AC アダプタをコンセントに接続してください。
5. パソコンの電源を入れてください。

- 電源は、指定 (オプション品) のもの、または DRX の電源規格に合ったものを使用してください。それ以外の電源を使用すると、故障・誤作動の原因になります。その場合の故障は、保証対象外となりますのでご了承願います。
- LAN ケーブルは、カテゴリ 5e 以上で通信速度に対応したケーブルをご利用ください。

2-4. 設置上のご注意

- 設置場所は、平滑な場所をお選びください。また、本製品設置後、コネクタの抜き差しが十分行えるようなスペースがある場所をお選びください。
- ケーブル類の引きまわしは、コネクタに無理な力がかからないように余裕を持たせてください。
- ケーブル類を伝わる水滴が本製品内部に侵入しないように、コネクタ近くで一旦コネクタより下方にケーブル類を引きまわしてください。
- 本製品は雷サージ対策を行っていません。LAN を介して接続されている外部装置側や電源装置で対策を行ってください。

2-5. ご利用環境の確認

DRX とパソコンを接続するためにはパソコンに LAN 環境が必要です。

LAN 環境がない場合には、ご利用のパソコンにあわせて LAN 機器をご用意ください。

- パソコンで LAN ポートが標準で装備されていない場合、LAN アダプタをご利用のパソコンにあわせて増設してください。

通信事業者と、必要に応じてプロバイダとの契約が完了している必要があります。

以下についてご確認願います。

- LTE 回線を利用した回線事業者との契約が完了している必要があります。
- インターネット接続サービスであるプロバイダへの契約が完了している必要があります。
  （moperaU、Softbank 等）
  事業者によっては回線事業者とプロバイダが同じ契約の場合があります。
  その場合別途プロバイダへの契約は必要ありません。
- DRX の設定には、以下の情報が必要になります。回線事業者またはプロバイダとの契約時に提供されている情報をご用意ください。不明な場合はご契約の回線事業者またはプロバイダへお問い合わせください。

  - 接続先名（APN）
  - ID
  - パスワード
  - ネームサーバ（DNS サーバ）の IP アドレス（設定が必要な場合）

> 接続先名（APN）は、料金コースによって異なりますので、お間違えのないように十分ご注意ください。

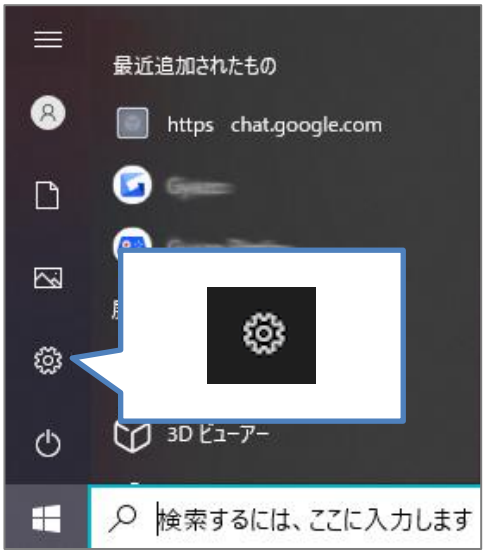
2-6. パソコンの設定

DRX にアクセスできるように、クライアントパソコンに DHCP クライアントの設定をします。DHCP を使用しない場合は、各パソコンに手動で IP を設定する必要があります。

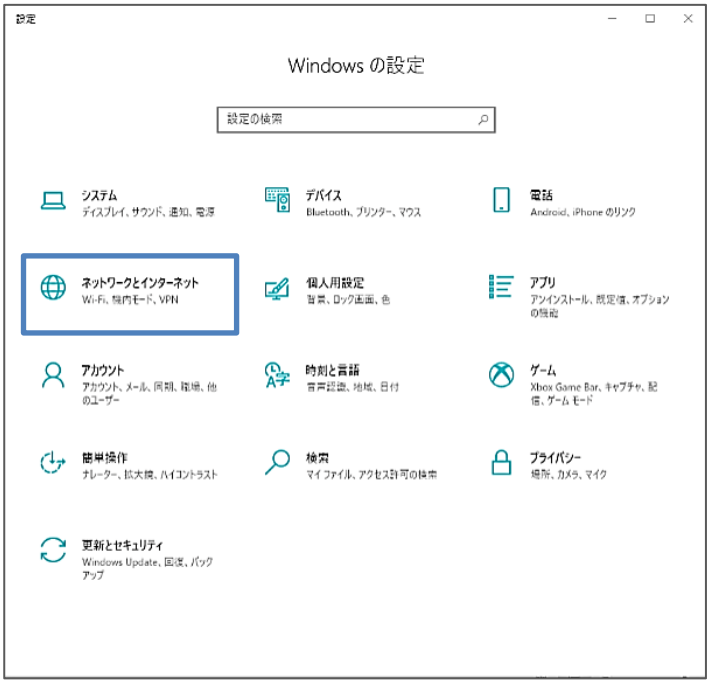
その設定方法については、ネットワークカードおよび Windows のマニュアル等をご覧ください。

2-6-1. Windowsのネットワーク設定（Windows10）

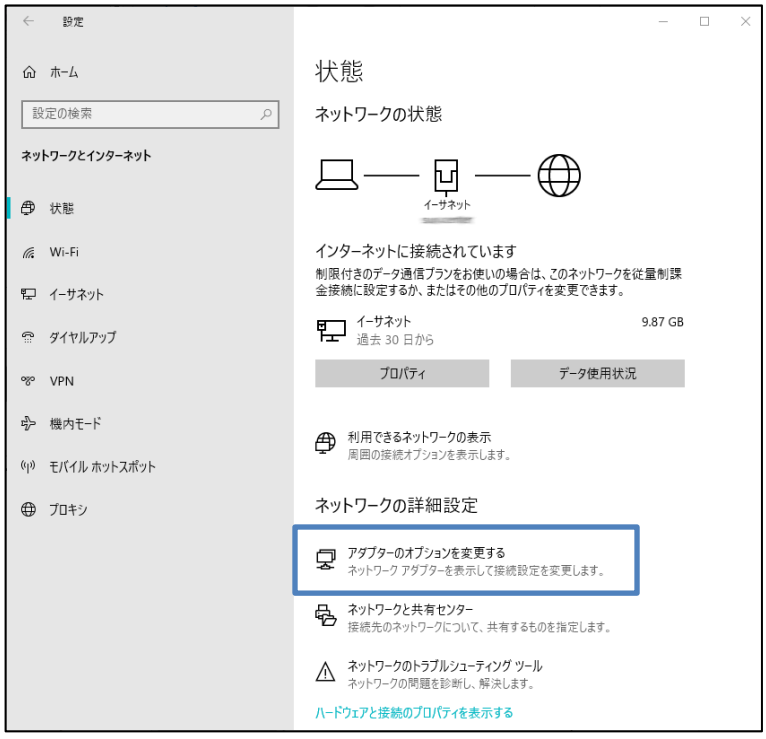
1. パソコンには管理者権限でログインしてください。
2. スタート画面から［設定］を開きます。



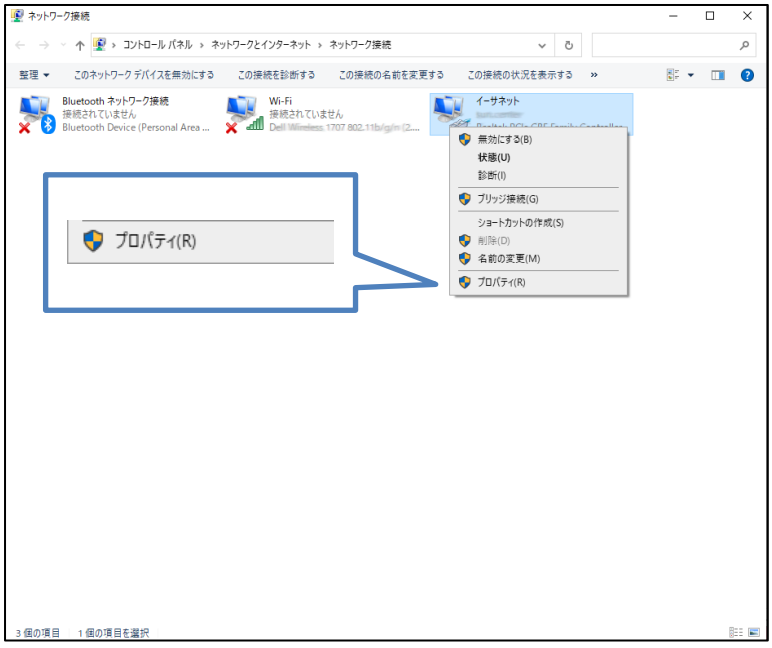
3.「ネットワークとインターネット」を開きます。



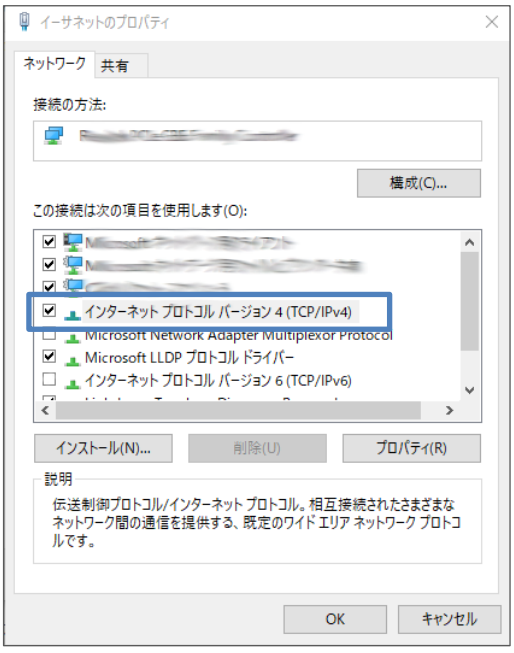
4．「ネットワークの状態」から「アダプターのオプションを変更する」を開きます。



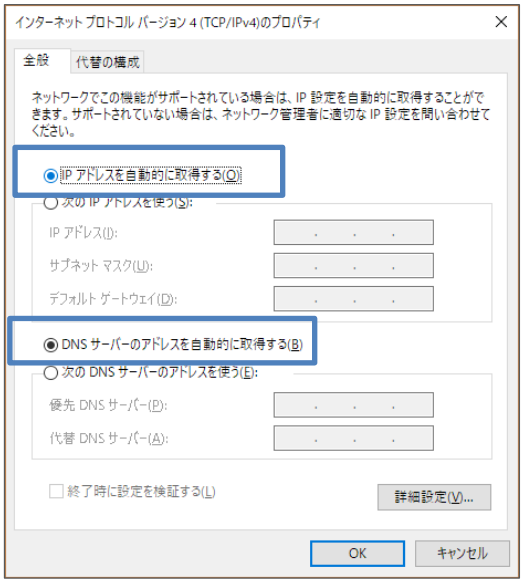
5．［イーサネット］を右クリックし、［プロパティ］をクリックします。
　イーサネットのプロパティが表示されます。



6．［インターネットプロトコルバージョン 4（TCP/Ipv4）］を選び、［プロパティ］ボタンをクリックします。インターネットプロトコルバージョン 4（TCP/Ipv4）のプロパティが表示されます。



7．［IP アドレスを自動的に取得する］、［DNS サーバのアドレスを自動的に取得する］を選択します。



8．［OK］ボタンをクリックしてダイアログを閉じます。
「ローカルエリア接続のプロパティ」画面も、［OK］ボタンをクリックして閉じます。

2-7. 入力できない記号一覧

2-7-1. ログインパスワード

ログインパスワードの設定変更では以下の記号を設定、使用できません。

␣	スペース	“	ダブルクォーテーション	$	ドルマーク
:	コロン	?	クエスチョンマーク	`	バッククォーテーション

2-7-2. ID、APN、パスワード

ID、APN、パスワード、メモ等では以下の記号を含む文字列は設定、使用できません。

#	シャープ	¥	円マーク	&	アンド/アンパサンド
$	ドルマーク	“	ダブルクォーテーション	<	小なり
‘	シングルクォーテーション	`	バッククォーテーション	>	大なり
␣	スペース	( )	カッコ （＊1)	;	セミコロン （＊1)
{ }	中カッコ	[ ]	大カッコ	?	クエスチョンマーク
,	コンマ	~	チルダ	|	バーティカルバー
^	キャレット	=	イコール		

＊1：アドバンスモードでの WebUI では設定可能ですが、
シンプルモードでの WebUI、CLI では設定できません。

3章　DRXの初期設定

ここでは、パソコンから DRX に接続して、LAN の設定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。

memo 【設定モードについて】
DRX の設定は 2 つのモードがあります。
・シンプルモード
一般的な機能を簡易に操作で設定が出来るモードです。（工場出荷状態）
WWW ブラウザから Web 設定ツールを操作することで各種設定を行います。
SSH による CLI コマンドからは情報出力やログ取得などが可能です。（設定は不可）
・アドバンスドモード
上級者を対象にした詳細な設定が可能となるモードです。
WWW ブラウザから Web 設定ツールや、SSH による CLI コマンドで操作することで各種設定を行うモードです。

3-1. Web設定ツール（シンプルモード）へのログイン方法

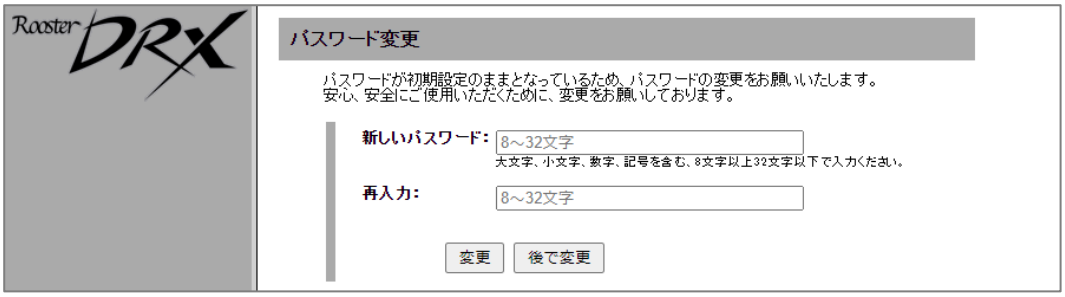
1. WWW ブラウザを起動します。
2. WWW ブラウザのアドレス入力欄に、DRX の LAN 側 IP アドレス「http://192.168.62.1/」（工場出荷時状態）を入力し、Enter キーを押します。

ログインダイアログボックスが表示されます。

3. ユーザー名に「root」、パスワードに「root」（工場出荷時状態）と入力した後、［OK］ボタンをクリックします。

4. 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大文字、小文字、数字、記号を含む、8 文字以上 32 文字以下で設定して［変更］をクリックします。
［後で変更］ボタンをクリックしても次の画面に進みますが、ログイン後に必ずパスワードを変更ください。また、パスワードを変更するまでログイン後にパスワード変更画面が表示されます。

   パスワードを変更した場合、再度ログインダイアログボックスが表示されます。
新しく設定したパスワードで再度ログインします。

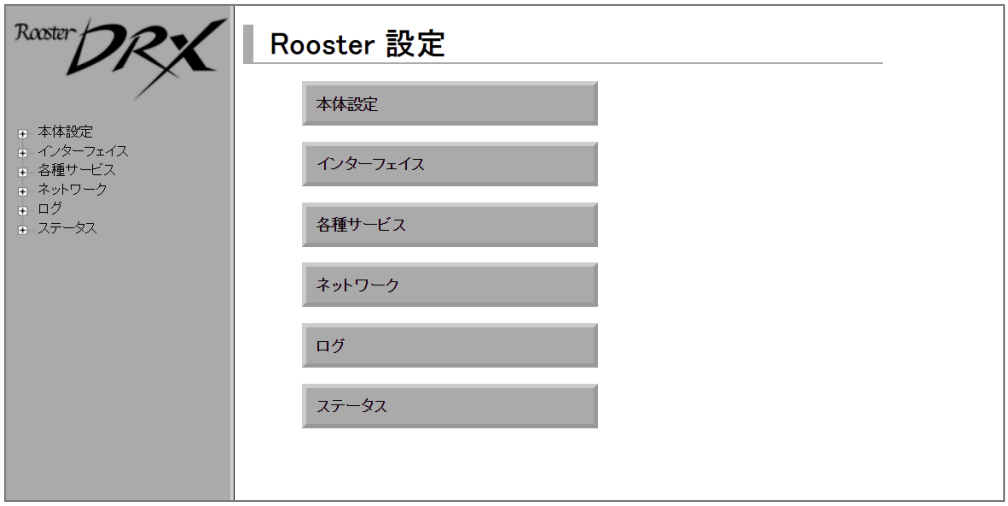


設定ツールの初期パスワードはログイン時に必ず変更してください。
その際、推測されにくいパスワードにしてください。

➲ 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、『3-3.ログインパスワードの設定』『2-7.入力できない記号一覧』をご覧ください。

5. DRX の設定ツールが表示されます。

- 設定ツールは JavaScript を使用しています。WWW ブラウザの JavaScript をオンにしてから設定を行ってください。
- 設定ツールを表示し、しばらく放置すると、一旦ログアウト処理を行います。その後、設定ツールにアクセスすると、再度ログインダイアログボックスが表示されます。
- ここで入力するユーザー名、パスワードは、DRX の設定ツールにアクセスするためのもので、プロバイダから提供されるユーザー名、パスワードとは異なるものです。



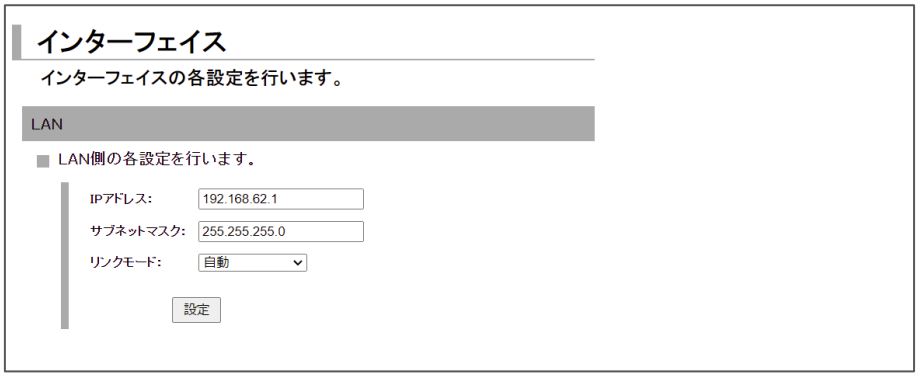
以降の設定画面で、連続して［設定］ボタンをクリックしたとき「他画面が設定反映中の為、失敗しました」と表示される場合があります。
その時は時間をあけてもう一度［設定］ボタンをクリックしてください。

memo
- タイトルバーには「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。

3-2. LANの設定

DRX の LAN 側 IP アドレスを変更する場合に設定を行います。
工場出荷時状態の LAN 側 IP アドレスは「192.168.62.1」に設定されています。

1. 設定ツールのメニューから、［インターフェイス］－［LAN］をクリックします。
「LAN 側設定」のページが表示されます。



2.［IP アドレス］、［サブネットマスク］に、新しく設定する DRX の LAN 側 IP アドレス、
サブネットマスクを入力します。

3.［リンクモード］に、以下の項目のいずれかを設定します。
- 自動
- 1000Mbps-Full
- 100Mbps-Full
- 10Mbps-Full

4.［設定］ボタンをクリックして、設定を反映させます。

> IP アドレス変更後は、一旦 WWW ブラウザを閉じてしばらくお待ちください。その後、新しく設定した IP アドレスで再度設定ツールにログインします。
> なお、変更前と異なるネットワークアドレス帯の IP アドレスに変更した場合、
> （例.192.168.62.1⇒192.168.0.1 に変更）DRX、パソコン共に再起動を行ってください。

> [リンクモード］設定・変更後は DRX の再起動を行ってください。

> IP アドレスに 192.168.225.0～192.168.225.255 を設定しないでください。

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。

LAN/WAN 構成の場合

LAN/LAN 構成の場合

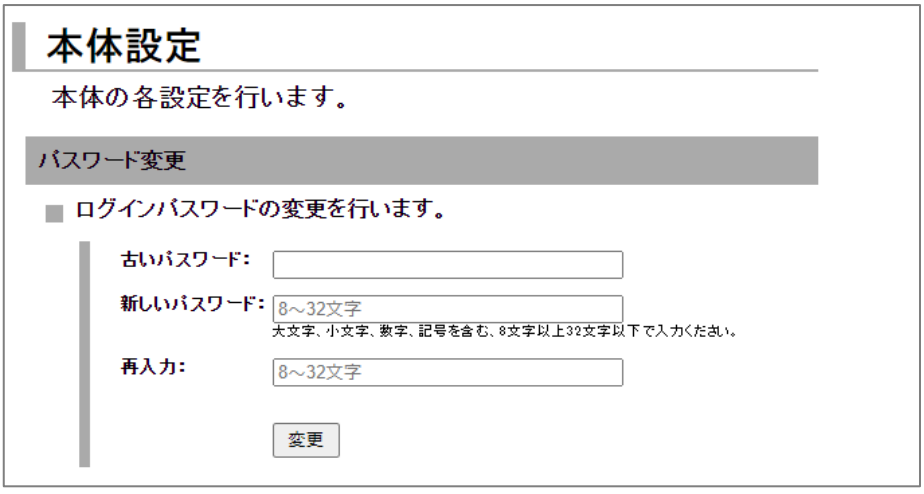
項目	内容
MAC アドレス	DRX の MAC アドレスが表示されます。
IP アドレス	DRX の IP アドレスが表示されます。
サブネットマスク	DRX のサブネットマスクが表示されます。
[LAN/WAN 構成の場合] ステータス LAN: WAN: [LAN/LAN 構成の場合] ステータス Bridge-LAN1: Bridge-LAN2:	 LAN ポートへの LAN 接続機器の接続状態が表示されます。 WAN ポートへの LAN 接続機器の接続状態が表示されます。 LAN1 ポートへの LAN 接続機器の接続状態が表示されます。 LAN2 ポートへの LAN 接続機器の接続状態が表示されます。
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。

3-3. ログインパスワードの設定

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。

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. ログインダイアログボックスが表示されます。新しく設定したパスワードで再度ログインします。

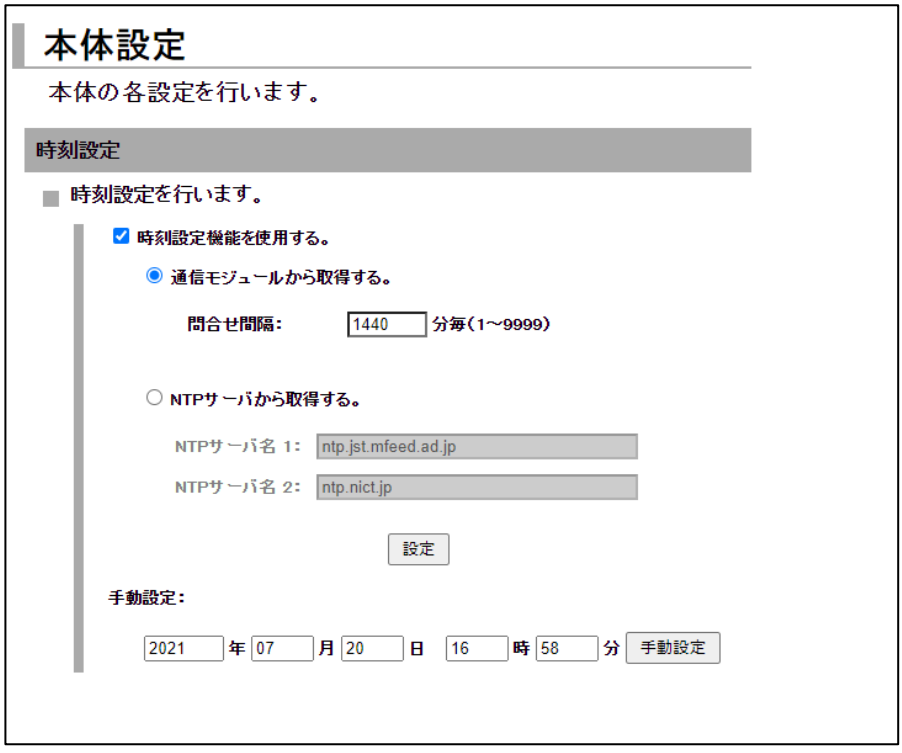
memo
- 入力したパスワードはすべて、「●」で表示されます。
- 大文字、小文字、数字、記号を含む、8 文字以上 32 文字以下で入力ください。
- 入力できない記号を含む文字列はパスワードに設定できません。
  ➲ 詳細は『2-7.入力できない記号一覧』をご覧ください。
- ユーザー名の変更はできません。「root」のみとなります。

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、推測されにくいパスワードにしてください。

3-4. 時刻の設定

> 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。

1. 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。



3-4-1. モバイル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）
指定された間隔でモバイル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。
モバイル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。

3-4-2. NTPサーバから取得する場合

この機能を使用するには、インターネットに接続している必要があります。

➲ インターネット接続設定の詳細は、『3-8.WAN の設定』、および『４章モバイル通信端末の設定』をご覧ください。

1. ［NTP サーバ機能を使用する］チェックをオンにし、以下の設定を行います。

項目	内容
NTP サーバ名 1	時刻を問い合わせる NTP サーバアドレス 1 を入力します。
NTP サーバ名 2	時刻を問い合わせる NTP サーバアドレス 2 を入力します。

2. ［設定］ボタンをクリックして、設定を反映させます。

3-4-3. 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。

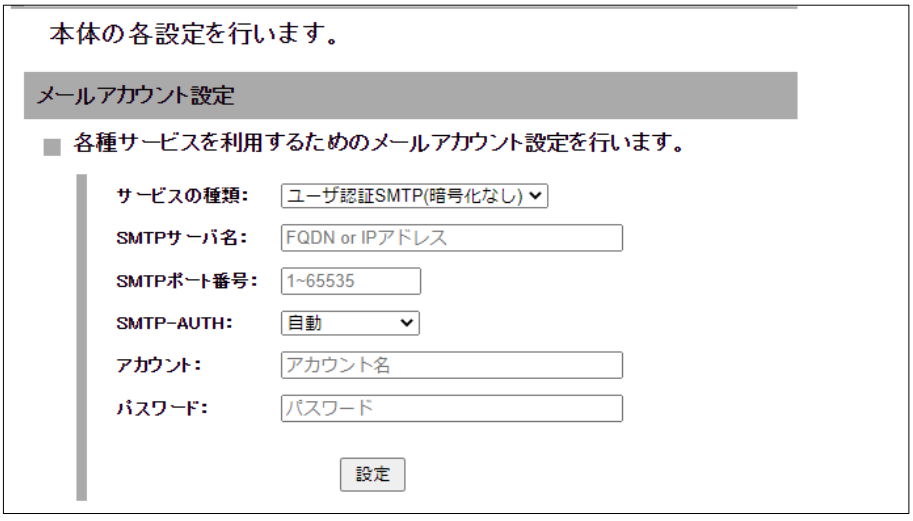
   直ちに設定した時刻に調整されます。

［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。

3-5. メールアカウントの設定

> ここで設定されるメールアカウントは、DRX のメール送信によるアドレス解決機能に使用されます。メール送信によるアドレス解決機能を使用する必要がない場合、メールアカウントの設定の必要はありません。
>
> ➲ アドレス解決機能の詳細は、『7-1.アドレス解決機能』をご覧ください。

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。 ➲ パスワードは『2-7.入力できない記号一覧』をご確認の上、設定してください。

> 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。

3-6. おやすみモードの設定

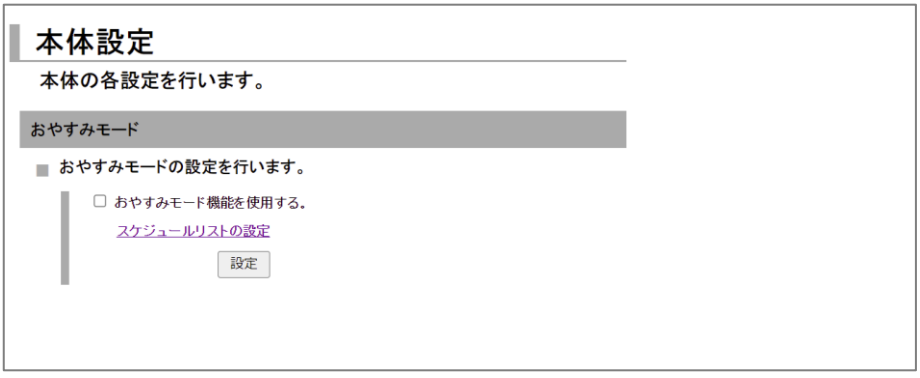
DRX の省電力の制御を行います。この機能は定期的に DRX をサスペンド（消費電力を抑えた待機状態）することにより、電力の消費を抑えることができます。

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。

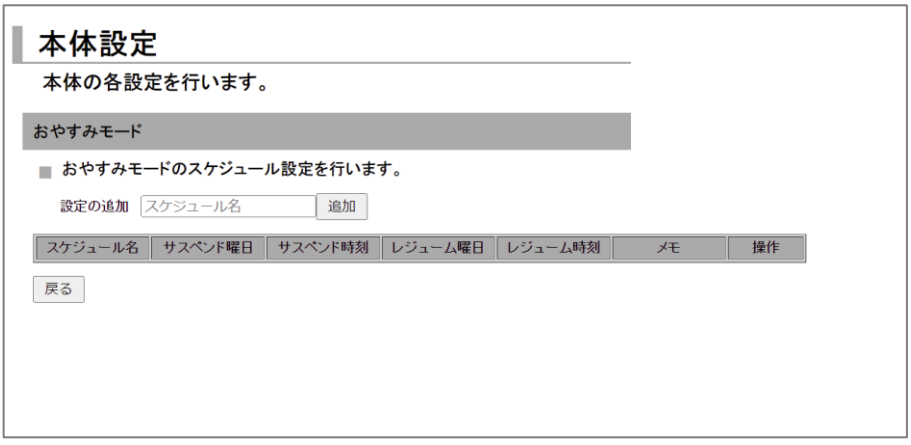
memo
- サスペンド…… 省電力モードとなり、通信できない状態となります。
- レジューム…… 通常動作に戻り、通信可能な状態となります。

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。

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。
既にスケジュールリストの設定が完了している場合は、［おやすみモードを使用する］チェックをオンにし［設定］ボタンをクリックして、設定を反映させます。



2．スケジュールの設定を行っていない場合は、［スケジュールリストの設定］をクリックし、スケジュールの追加を行います。
[設定の追加] に任意のスケジュール名を入力します。半角英数字で入力してください。



3．[追加] をクリックし、スケジュールの詳細を設定します。

以下の項目を入力します。

項目	内容
スケジュール名	おやすみモードスケジュール設定のスケジュール名が表示されます。
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。

4．［設定］をクリックします。「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、［後で再起動する］を選択してから［戻る］をクリックして「おやすみモード」ページに戻ってください。
その後、［おやすみモード機能を使用する］にチェックをオンにし、［設定］をクリックすると「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、［再起動する」をクリックします。

> memo 設定可能なスケジュールの設定は 7 件まで行えます。

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 [変更] 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した場合は、変更したスケジュールが別名保存されます。

3-6-1. 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。

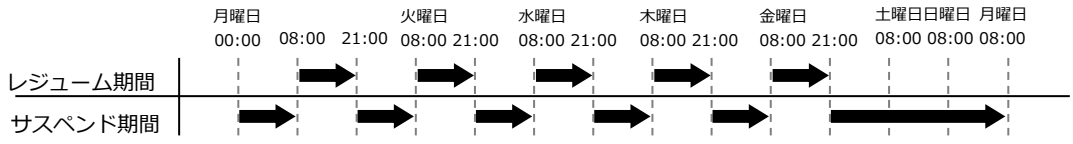
- ［おやすみモード機能を使用する］にチェックをオンにします。
- ［スケジュールリストの設定］をクリックします。
- 月曜日～金曜日までのスケジュールを作成します。
- 月曜日～金曜日の［サスペンド時刻］を 21 時 00 分に設定します。
- 月曜日～金曜日の［レジューム曜日］を翌日に設定します。
- 月曜日～金曜日の［レジューム時刻］を 8 時 00 分に設定します。
- ［設定］ボタンをクリックします。

「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。

以上で条件が設定されました。

おやすみモード設定例の状態遷移

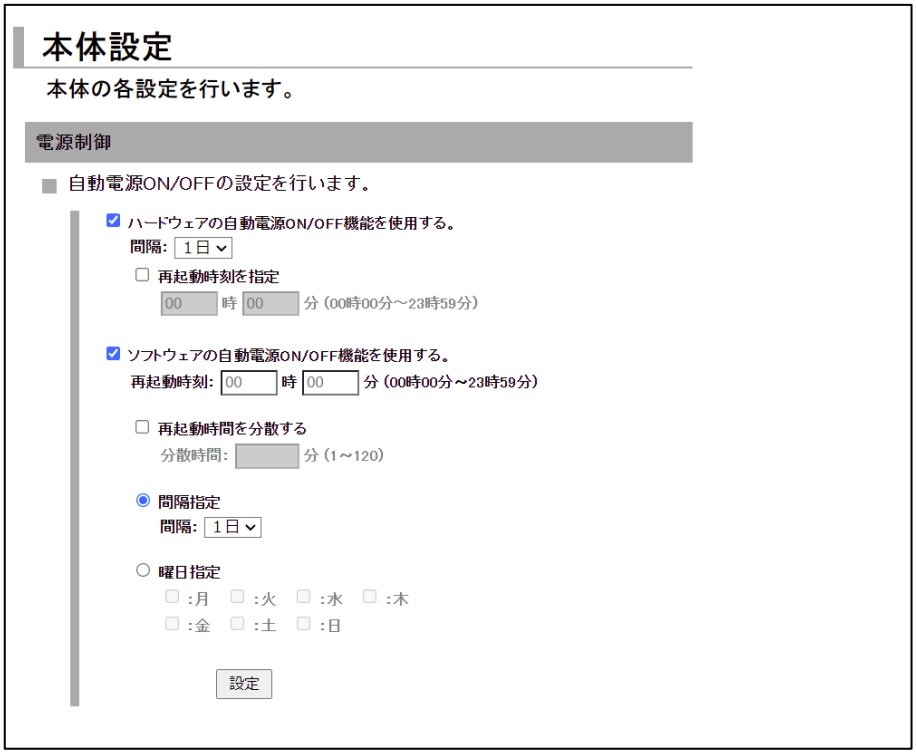
上記の設定によるおやすみモードの状態遷移は次のようになります。



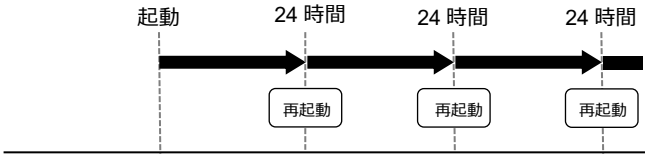
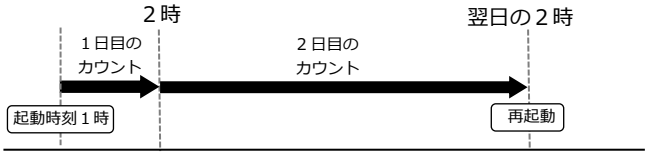
3-7. 電源制御

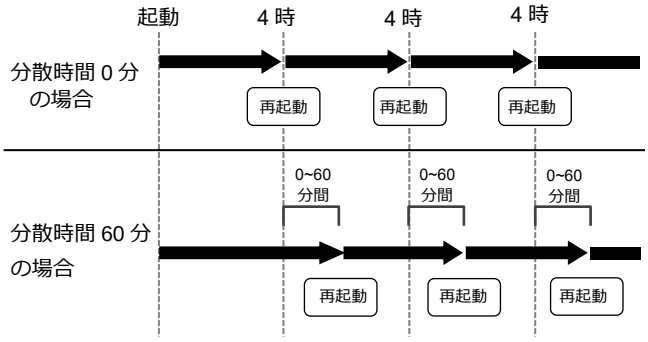
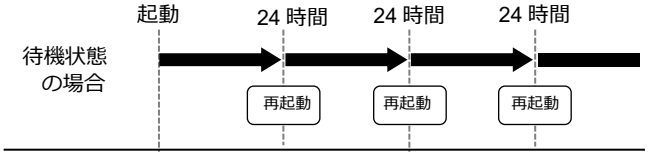
DRX の電源の制御を行います。この機能は定期的に DRX の電源を ON/OFF することにより、より安定した運用を行うことを目的とします。

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．以下の設定を行います。

項目	内容
ハードウェア	ハードウェアの電源を ON/OFF するための設定です。 使用する場合はチェックをオンにし、以下の設定を行ってください。 ▶ソフトウェアの設定が何らかの影響にて動作しなかった時の保険的な機能です。 • 間隔指定 間隔を 1～7 日の間で設定します。 <例> ハードウェア：1 日間隔　の場合  • 再起動時刻を指定 再起動させたい時刻を指定します。24 時間表記にて設定します。 回線がつながっている状態でも、設定時間になるとハードウェアが再起動します。ソフトウェアの設定が何らかの影響にて動作しなかった時の保険的な機能です。ハードウェアの設定時間は目安ですので、実際の動作時間は多少前後します。 • 再起動時刻を指定の反映 設定した時刻と起動した時刻によって指定の再起動の日付が変わります。 ▶ハードウェア再起動が動いてからは指定の時刻で再起動が行われます。 <例> ハードウェア：２日間隔、２時の設定 ● DRX 起動が 1 時の場合  ● DRX 起動が 3 時の場合 

項目	内容
ソフトウェア	ソフトウェア上で DRX の電源を ON/OFF するための設定です。使用する場合はチェックをオンにし、以下の設定を行ってください。 • 再起動時刻指定 再起動させたい時刻を指定します。24 時間表記にて設定します。 • 再起動時間を分散する 個体ごとに再起動する時間を分散させます。 複数台設置時に同時に再起動時間した場合のネットワーク上の輻輳を防ぐため、製造番号を元にした乱数を使い、指定された再起動時間から再起動を遅らせます。1～120 分の間で設定します。 <分散時間　設定例> 毎日 4 時に再起動　の場合  • 間隔指定 一定間隔で DRX の電源を ON/OFF するための設定です。 使用する場合はチェックをオンにし、１～７日の間で設定を行ってください。 <間隔指定　設定例> 間隔 1 日　の場合  • 曜日指定 特定の曜日に DRX の電源を ON/OFF するための設定です。 使用する場合は、月曜～日曜のいずれかのチェックをオンにします。複数の曜日選択が可能です。

3. 選択した設定でよければ［設定］ボタンをクリックします。

4. ［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、［再起動］をクリックしてください。

3-8. WANの設定

DRX の WAN 側のネットワーク設定を行います。

1. 設定ツールのメニューから、［インターフェイス］－［WAN］をクリックします。
「WAN 側設定」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
IP 自動取得	WAN 側の IP を自動で取得する場合は、チェックをオンにします。
IP 手動設定	WAN 側の IP を手動で設定する場合は、チェックをオンにします。
PPPoE 接続	PPPoE 接続を行う場合は、チェックをオンにします。
LAN として使用	WAN ポートを LAN として使用（LAN/LAN 構成として使用）する場合は、チェックをオンにします。
IP アドレス	IP 手動設定を選択した場合は、WAN 側の IP アドレスを設定します。
サブネットマスク	IP 手動設定を選択した場合は、WAN 側のサブネットマスクを設定します。
デフォルトゲートウェイ	IP 手動設定を選択した場合は、WAN 側のデフォルトゲートウェイを設定します。
DNS サーバ 1	IP 手動設定を選択した場合は、プライマリ DNS サーバを設定します。
DNS サーバ 2	IP 手動設定を選択した場合は、セカンダリ DNS サーバを設定します。
ID	PPPoE 接続を選択した場合は、認証するための ID を設定します。
パスワード	PPPoE 接続を選択した場合は、認証するためのパスワードを設定します。 ➲ パスワードは『2-7.入力できない記号一覧』をご確認の上、設定してください。
サービス名	PPPoE 接続を選択した場合は、サービス名を設定します。(指定無い時は空欄)
リンクモード	通信速度を自動、1000Mbps、100Mbps、10Mbps から選択します。

項目	内容
NAT を使用する	NAT 機能を使用する場合は、チェックをオンにします。
デフォルトゲートウェイとして使用する	インタフェースを有効化した時に、自動的にデフォルトルートを設定する場合はチェックをオンにします。

- WAN とモバイル通信端末を両方に使用する場合は、片方のインタフェースのみ「デフォルトゲートウェイとして使用する」チェックをオンにしてください。

3. ［設定］ボタンをクリックして、設定を反映させます。

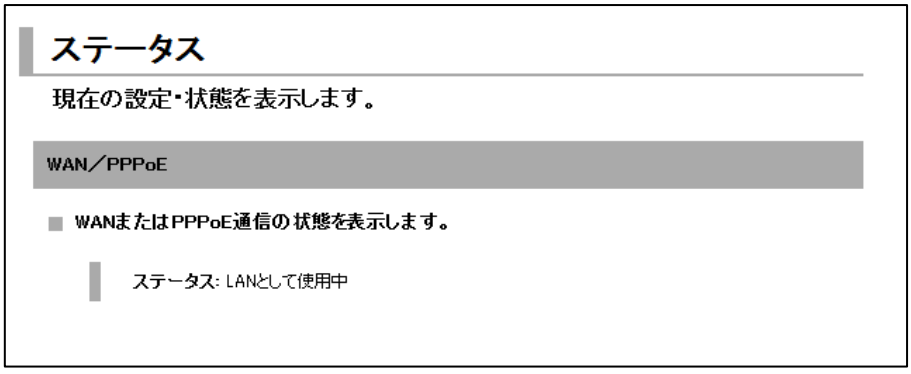
WAN 内の通信状態は、設定ツールのメニューから、［ステータス］－［WAN］をクリックして表示される「WAN/PPPoE ステータス表示画面」から確認することができます。

[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。
ステータス		設定した WAN の現在の状態が表示されます。
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。

項目	内容
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。

[LAN/LAN 構成の場合]（LAN として使用を選択）



項目	内容
ステータス	設定した WAN 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、『WAN のステータス一覧』をご覧ください。

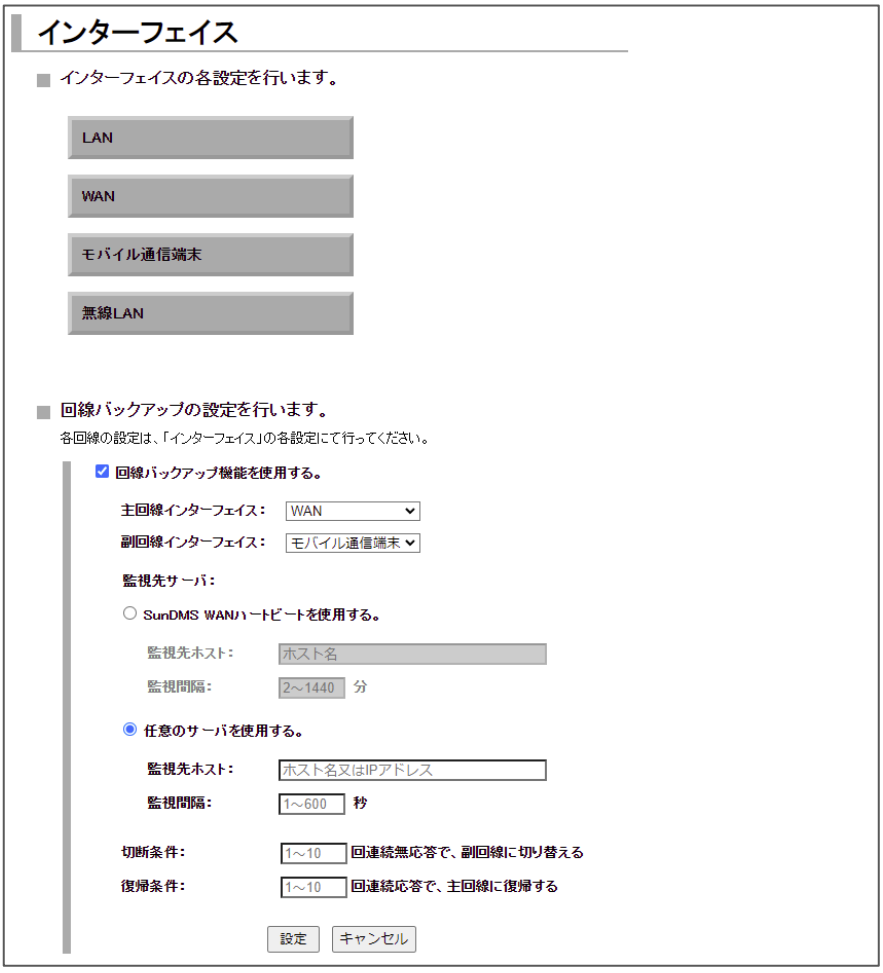
WAN のステータス一覧

ステータス表示	状態
ケーブル未接続	LAN ケーブルが接続されていない状態です。
未接続	接続が切断されている状態です。
接続中	接続が正常に行われている状態です。
LAN として使用中	LAN/LAN 構成で使用中の状態です。

3-9. 回線バックアップの設定

memo 【回線バックアップについて】
回線バックアップとは通信監視を行い応答が無い場合に回線を切り替える機能です。
主回線インタフェースから監視先ホストへ ping 応答を監視し、応答が無い場合に副回線インタフェースにデフォルトゲートウェイを切り替えます。

1. 設定ツールのメニューから、［インターフェイス］をクリックします。
「インターフェイス」のページが表示されます。



2. [回線バックアップ機能を使用する] チェックをオンにし、以下の設定を行います。

項目		内容
主回線インターフェイス 副回線インターフェイス		主回線、副回線として使用するインタフェース回線を選択します。 ［WAN］、［モバイル通信端末］のいずれかを指定します。
「SunDMS WAN ハートビートを使用する」	監視先ホスト	主回線の健全性を ping で監視するための「SunDMS WAN ハートビート」のドメイン名を指定します。 監視先ホストが応答しない場合、副回線に切り替わります。 また監視先ホストが応答した場合、主回線に切り替わります。 ➲「SunDMS WAN ハートビート」のサービスの詳細は『 7-7. SunDMS サービス 』をご覧ください。
	監視間隔	監視先ホストに監視を行う時間の間隔（分）を指定します。

項目		内容
「任意のサーバを使用する」	監視先ホスト	主回線の健全性を ping で監視するための IP アドレス、もしくはドメイン名を指定します。 指定する IP アドレスはグローバル IP アドレスまたは VPN 接続先のネットワーク IP アドレスです。 監視先ホストが応答しない場合、副回線に切り替わります。 また監視先ホストが応答した場合、主回線に切り替わります。
	監視間隔	監視先ホストに監視を行う時間の間隔（秒）を指定します。
切断条件		切断と判断する監視回数を指定します。 監視先ホストの応答が指定回数連続して無い場合、”主回線が切断した”と判断します。 切断したと判断された場合、主回線→副回線へ切り替えます。
復帰条件		復帰と判断する監視回数を指定します。 監視先ホストの応答が指定回数連続して応答した場合、”主回線が復帰した”と判断します。 復帰したと判断された場合、副回線→主回線へ切り替えます。

3. ［設定］ボタンをクリックします。

4. 設定完了後、DRX を再起動し、設定を反映させます。

- 主回線と副回線に使用されるインタフェースのデフォルトゲートウェイを以下のように設定してください。
  - ・主回線の「デフォルトゲートウェイとして使用する」チェックをオン
  - ・副回線の「デフォルトゲートウェイとして使用する」チェックをオフ

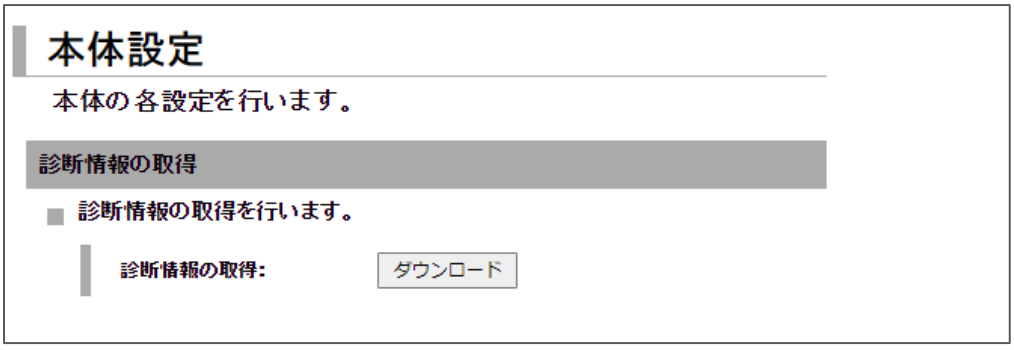
- 副回線を WAN 固定 IP で使用する際は［監視先ホスト］にて IP アドレスを指定してください。（ドメイン名は使用できません）
- ［監視先ホスト］にドメイン名を指定することはできますが、デフォルトルートの DNS サーバに接続できない場合、正常に動作しなくなるときがあります。ドメイン名ではなくなるべく IP アドレスを指定することをお勧めします。

- 回線バックアップを使用する場合、短い間隔で ping を繰り返し（ping コマンドにおけるオプションなど）行わないでください。
  切り替わった後の回線で ping が正常に行われない場合があります。
- スタティックルーティングや IPsec 設定のルーティング経路は、回線バックアップの機能では切り替わりません。
- 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。
- モバイル副回線監視と併用できません。

3-10. 診断情報の取得

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。

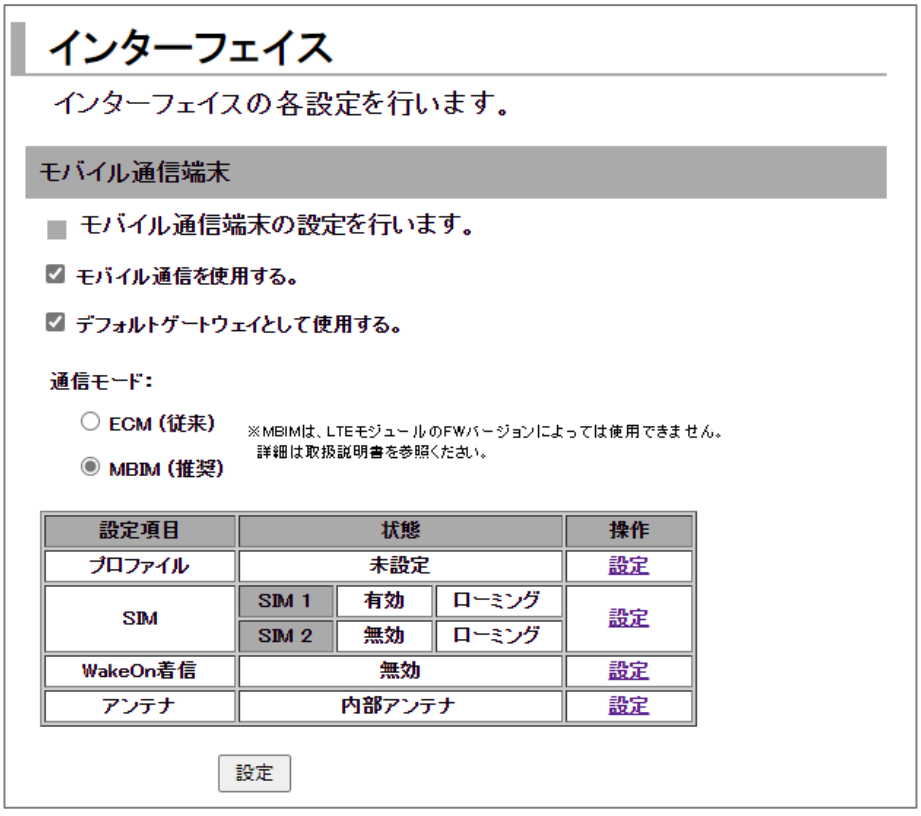
! 使用状況により取得するファイルが大きくなること（10MB 以上）がありますので、従量課金の回線からダウンロードする場合はご注意ください

4章　モバイル通信端末の設定

ここでは、Web 設定ツールを使用して、モバイル通信を行うための初期設定のパソコンの手順について説明します。

4-1. プロファイルの追加

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



1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］をクリックします。
「モバイル通信端末」のページが表示されます。

2. [モバイル通信を使用する] のチェックをオンにします。

3. デフォルトゲートウェイとして使用する場合は、[デフォルトゲートウェイとして使用する] のチェックをオンにしてください。

- WAN とモバイル通信端末を両方に使用する場合は、片方のインタフェースのみ「デフォルトゲートウェイとして使用する」チェックをオンにしてください。

4 . [通信モード] を設定します。

各モードは以下の通りです。

項目	内容
ECM（従来）	FW バージョン 2.5.0 以前で使用していた従来からのモードです。 モバイル通信端末内に NAT 変換が入っており、プライベート IP（192.168.225.0/24）が割り当たる通信を行うモードです。
MBIM（推奨）	FW バージョン 2.6.0 以降で選択できる新規のモードです。 **「モバイル通信端末の FW バージョン」が古い場合動作しません。（以下！欄を参照ください）** モバイル通信端末内に NAT 変換は無く直接グローバル IP が割り当たるモードです。 MBIM モードの設定を推奨します。

「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 は 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、CLI から「show mobile」コマンドでご確認いただけます。

IPsec をお使いで ECM モードから MBIM モードへ変更される場合、実運用に適用する前に MBIM モード設定で IPsec の動作検証を行う事をお勧めします。
ECM と MBIM ではモバイル通信端末内のネットワーク構成が違うため、IPsec 設定を調整する必要がある場合があります。

5 . [設定] ボタンをクリックします。

SIM2 枚の回線契約を同時に接続することはできません。どちらか片方の SIM での接続となります。

工場出荷時の設定では、モバイル通信端末は 24 時ごとにリセット（再起動）する設定がされています。
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。

モバイル通信端末内において特定の IP アドレス（192.168.225.0/24）が内部的に使用されます。
このためこの特定の IP アドレスはお客様ネットワークにおいては使用できません。

6. 設定ツールのメニューから［インターフェイス］–［モバイル通信端末］–［プロファイル］をクリックします。「プロファイル」のページが表示されます。

7. プロファイルを追加する項目にプロファイル番号を 1～8 の範囲で入力し、[追加] ボタンをクリックします。
「プロファイルの詳細設定」の画面が表示されます。

以下の設定を行ってください。

項目	内容
No	プロファイル番号を表示します。
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。 ➲ ID およびパスワードは『2-7.入力できない記号一覧』をご確認の上、設定してください。 ❗ 設定できない文字が含まれている場合は、インターネットサービスプロバイダ、あるいはネット

項目	内容
	ワーク管理者に上記の文字を使用しない ID・パスワードに変更をご依頼ください。
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。
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。
接続先通信事業者	以下のいずれかを設定します。 自動 ドコモ (440 10) ソフトバンク (440 20) KDDI (440 50) KDDI (440 51) KDDI (440 52) ▸ カッコ（）内の数字は MCC,MNC を示しています。 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。
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『4-2. SIM カードスロットの設定』を参照してください。

7．［設定］ ボタンをクリックして、設定内容を反映させます。

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

8．「プロファイル」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。

デフォルトプロファイルを選択し、［設定］ ボタンをクリックしてください。

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 [変更] 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。

memo

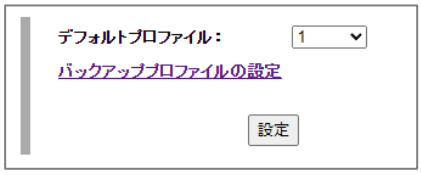
起動時、デフォルトプロファイルに設定されたプロファイルに自動的に接続します。
プロファイル設定が無い状態で、新規にプロファイルを作成した場合、作成したプロファイルが自動的にデフォルトプロファイルに設定されます。
デフォルトプロファイルが[未設定]の場合、自動的に接続しません。モバイル通信端末ステータス画面で接続操作をしてください。

➲ 切断・接続方法については、『4.5. 切断・接続方法』をご覧ください。

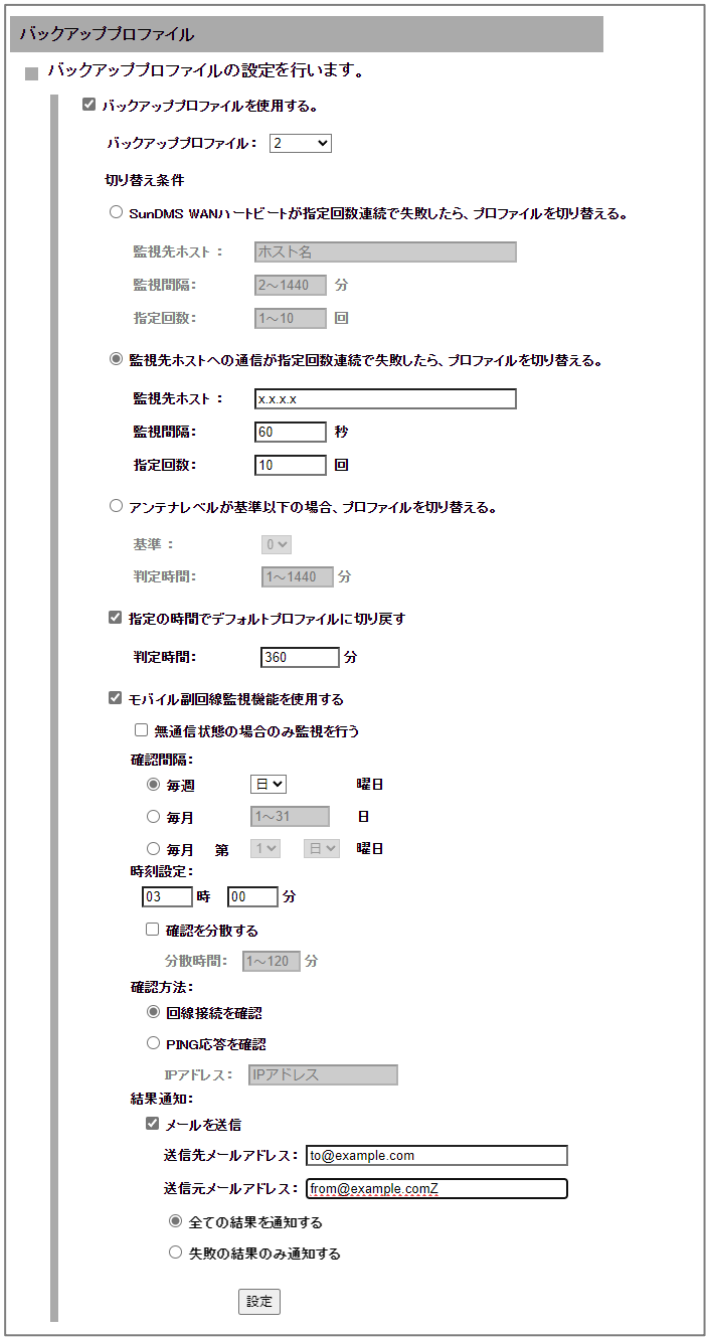
4-1-1. バックアッププロファイル（モバイル副回線）の設定

バックアッププロファイルはデフォルトプロファイル設定の SIM が通信障害、契約終了などにより通信ができない状態に陥った時、条件に合わせて自動でバックアッププロファイル（モバイル副回線）に切り替わる機能です。

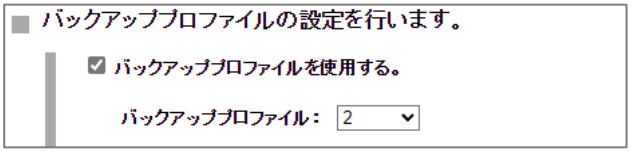
1. 「プロファイル」画面の［バックアッププロファイルの設定］をクリックします。



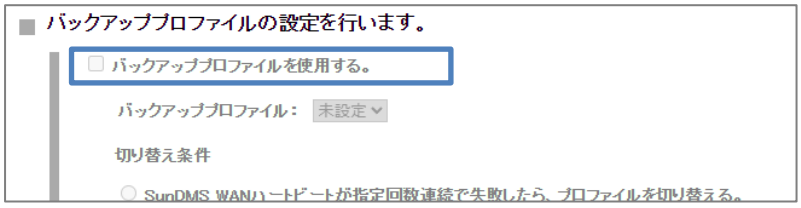
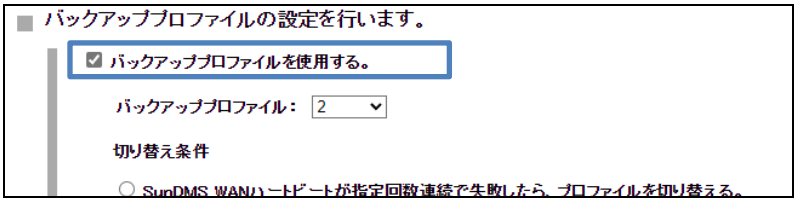
2. 「バックアッププロファイル」画面が表示されます。



3．［バックアッププロファイルを使用する］のチェックをオンにします。

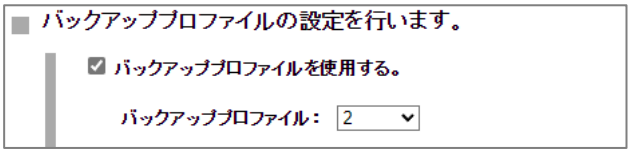


［バックアッププロファイルを使用する］を設定する場合はプロファイルを２件以上設定が必要です。
登録件数が２件未満の場合は選択できません。

登録件数	画面表示
０～１件	 「バックアッププロファイル使用不可」
２～８件	 「バックアッププロファイル使用可能」

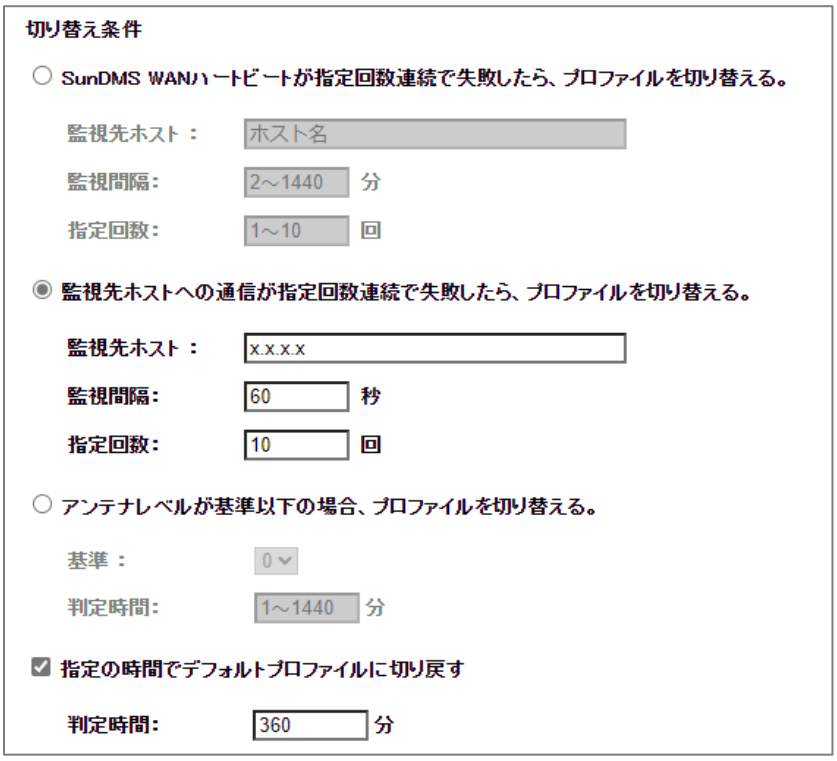
4．バックアッププロファイルのプロファイルを選択ください。

設定したプロファイルの中から、バックアッププロファイルとするプロファイル番号を選択ください。



バックアッププロファイルに［未設定］、［デフォルトプロファイルの設定番号］は設定できません。

5．［切り替え条件］を
・［SunDMS WAN ハートビートが指定回数連続で失敗したら、プロファイルを切り替える］
・［監視先ホストへの通信が指定回数連続で失敗したら、プロファイルを切り替える］
・［アンテナレベルが基準以下の場合、プロファイルを切り替える］
の三つの条件のうち一つを選択して設定を行います。



6．［SunDMS WAN ハートビートが指定回数連続で失敗したら、プロファイルを切り替える］の条件の場合は以下を設定します。

項目	内容
監視先ホスト	デフォルトプロファイル設定のモバイル通信の健全性を ping で監視するための「SunDMS WAN ハートビート」のドメイン名を指定します。 ➲「SunDMS WAN ハートビート」のサービスの詳細は『 7-7. SunDMS サービス 』をご覧ください。
監視間隔	監視先ホストに対して監視を行う間隔(分)を指定します。 ・設定範囲：2～1440
指定回数	リトライする回数を指定します。 ［監視先ホスト］に対して［監視間隔］で ping を実施し［指定回数］連続で失敗した場合、プロファイルを切り替えます。 ・設定範囲：1～10

7．「監視先ホストへの通信が指定回数連続で失敗したら、プロファイルを切り替える］の条件の場合は以下を設定します。

項目	内容
監視先ホスト	デフォルトプロファイル設定のモバイル通信の健全性を ping で監視するための IP アドレス、もしくはドメイン名を指定します。 監視先ホストが応答しない場合、プロファイルを切り替えます。
監視間隔	監視先ホストに対して監視を行う時間の間隔（秒）を指定します。 ・設定範囲：1～600

項目	内容
指定回数	リトライする回数を指定します。 ［監視先ホスト］に対して［監視間隔］で ping を実施し［指定回数］連続で失敗した場合、プロファイルを切り替えます。 ・設定範囲：1～10

8．［アンテナレベルが基準以下の場合、プロファイルを切り替える］の条件の場合は以下を設定します。

項目	内容
基準	デフォルトプロファイル設定のモバイル通信のアンテナレベル（通信状況）の監視するための基準を指定します。 ・基準アンテナレベル： 0～3 ➲ 基準アンテナレベルの詳細は『1-6 ランプ点灯・点滅パターン一覧』の『ANT』をご覧ください。
判定時間	アンテナレベルが設定基準以下の状態が連続して判定時間(分)経過した場合、プロファイルを切り替えます。 ・判定時間：1～1440

9．［指定の時間でデフォルトプロファイルに切り戻す］の条件の場合はチェックボックスをオンにして、以下を設定します。

項目	内容
判定時間	バックアッププロファイルに切り替わってから判定時間(分)経過した場合、強制的にデフォルトプロファイルに切り替えます。 ・判定時間：1～1440

１０．［設定］ボタンをクリックして、設定を反映させます。

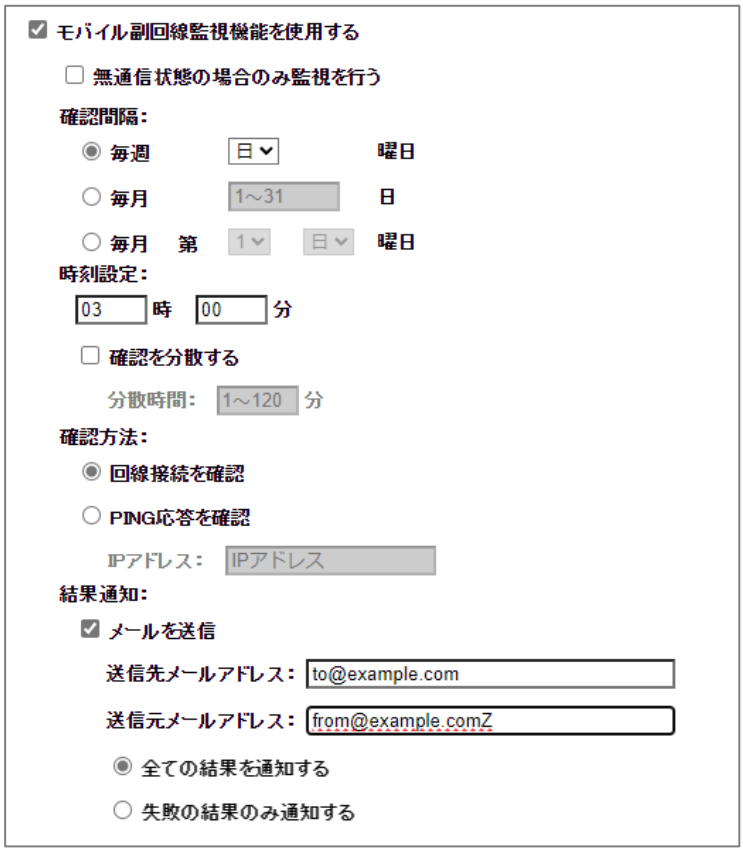
memo
- バックアッププロファイルに切り替わった後、デフォルトプロファイルに戻る条件としては以下となります。
  ・「切り替え条件」が再び成立したとき
  ・モバイル通信端末をリセットしたとき
  ・DRX が再起動したとき
  それ以外の条件でデフォルトプロファイルに戻したい場合などは、アドバンスドモードにて設定してください。
- ［指定の時間でデフォルトプロファイルに切り戻す］は、
  ［SunDMS WAN ハートビートが指定回数連続で失敗したら、プロファイルを切り替える］
  ［監視先ホストへの通信が指定回数連続で失敗したら、プロファイルを切り替える］
  ［アンテナレベルが基準以下の場合、プロファイルを切り替える］
  の いずれかの条件と併用して設定することができます。

!
・プロファイルのリストから デフォルトプロファイルやバックアッププロファイルに設定したプロファイルを削除した場合、バックアッププロファイルの設定が無効になります。
・プロファイルが切り替わった後、切り替え条件が適用されるのは５分後になります。

4-1-2. モバイル副回線監視の設定

> memo モバイル副回線監視は、バックアッププロファイル設定により設定されたプロファイルを定期的に接続し、通信可能な状態であるかを確認する機能です。

1．「バックアッププロファイル」画面の［モバイル副回線監視機能を使用する］をクリックします。



2．以下の設定を行います。

項目	内容
無通信状態の場合のみ監視を行う	チェックボックスをオンにした場合、指定された時刻から 5 分間モバイルへの IP パケット送出がされなかった場合にのみ監視を行います。 ▶オフにした場合、通信の有無に関係無く指定された時刻に監視を開始します。
確認間隔	監視を行うタイミングを設定します。 • ［毎週］を選択した場合 毎週のどの曜日に監視を行うかを設定します。 ［日］～［土］曜日を設定します。 • ［毎月］を選択した場合 毎月の何日に監視を行うを設定します。 ［1］～［31］日を設定します。 ▶月やうるう年によっては実施できない無い月が発生しますのでご考慮の上設定ください。（2 月 30 日など） • ［毎月 第何曜日］を選択した場合 毎月の第何週目の何曜日に監視を行うかを設定します。 週は［1］～［5］週目を選択します。 曜日は［日］～［土］曜日を選択します。 ▶月やうるう年によっては実施できない無い月が発生しますのでご考

項目	内容
	慮の上設定ください。
時刻設定	確認間隔で設定された日の何時に監視を行うかを設定します。 24 時間表記にて設定します。
確認を分散する	個体毎に監視する時間を分散さる場合に、オンにします。 複数台設置時に同時に監視を行った場合のネットワーク上の輻輳を防ぐため、製造番号を元にした乱数を使い、指定された時刻設定から監視の実施を遅らせます。
分散時間	［確認を分散する］をオンにした場合、分散させたい間隔を 1～120 分の範囲で設定します。
確認方法	確認する方法を選択します。 ・［回線接続を確認］を選択した場合 指定されたバックアッププロファイルで回線が接続するかを確認します。 ▶バックアッププロファイルの回線を接続するのみでデータ通信は発生しません。 ・［PING 応答を確認］を選択した場合 指定されたバックアッププロファイルで回線を接続し、指定された IP アドレスに PING を実施し疎通するかを確認します。 ▶バックアッププロファイルの回線でデータ通信が発生します。
結果通知	確認した結果をメール送信したい場合、チェックボックスをオンにします。 送信したいメールアドレスを［送信先メールアドレス］に入力してください。 ・［すべての結果を通知する］を選択した場合 確認に成功失敗の結果にかかわらず、指定されたメールに通知します。 ・［失敗の結果のみを通知する］を選択した場合 確認に失敗した場合にのみ指定されたメールに通知します。 ➲ 設定方法は『3-5. メールアカウントの設定』をご覧ください。

3．［設定］ボタンをクリックします。

4．設定完了後、DRX を再起動し、設定を反映させます。

memo
・モバイル副回線監視が成功した場合、
「トリガー(SbLnMntSuccess)の有効化を実行します」
とトリガログに出力されます。
また、このメッセージが出力されない場合は失敗となります。
・通信があり監視を行わなかった場合、
「SbLnMntChkTrafficNG: 周期イベントが発生しました」
とトリガログに出力されます。

!
・モバイル副回線監視は以下の場合は実施されません。結果通知も送信されません。
－モバイル通信が無効になっている場合
－バックアッププロファイル機能の条件によりバックアッププロファイルに切り替わている場合
・結果通知はデフォルトプロファイルの接続で送信します。デフォルトプロファイルで接続できない場合、結果通知が送信されません。
・回線バックアップ機能と併用設定ができません。
・モバイルをデフォルトルートと設定してください。

!
［無通信状態の場合のみ監視を行う］を設定では、SunDMS 通信、監視先ホストへの疎通確認通信、NTP へのアクセスや、ネットワーク側からアクセスに対する応答（ICMP など）も監視対象です。これらの通信があった場合は監視を行いません。

4-2. SIMカードスロットの設定

1. 設定ツールのメニューから、［インターフェイス］–［モバイル通信端末］–［SIM］をクリックします。「SIM カードスロット」のページが表示されます。

2. 以下の設定を行います。

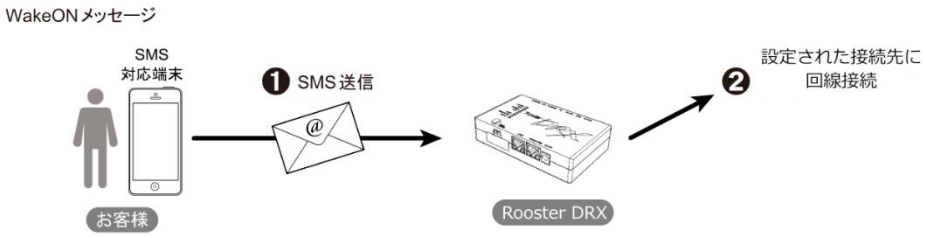
項目	内容
SIM1 スロットを有効にする	SIM1 の SIM カードスロットを有効にする場合は、チェックをオンにします。 ・通信業者を選択 [ドコモ]、[ソフトバンク]、[KDDI]、[ローミング] から選択します。 ・MVNO 仮想移動体通信事業者の SIM カードの場合は、チェックをオンにします。 ・PIN コードを設定 ご契約中の SIM カードの PIN コードを入力します。 PIN コードが設定されていない場合は、空白になります。
SIM2 スロットを有効にする	SIM2 の SIM カードスロットを有効にする場合は、チェックをオンにします。 ・通信業者を選択 [ドコモ]、[ソフ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

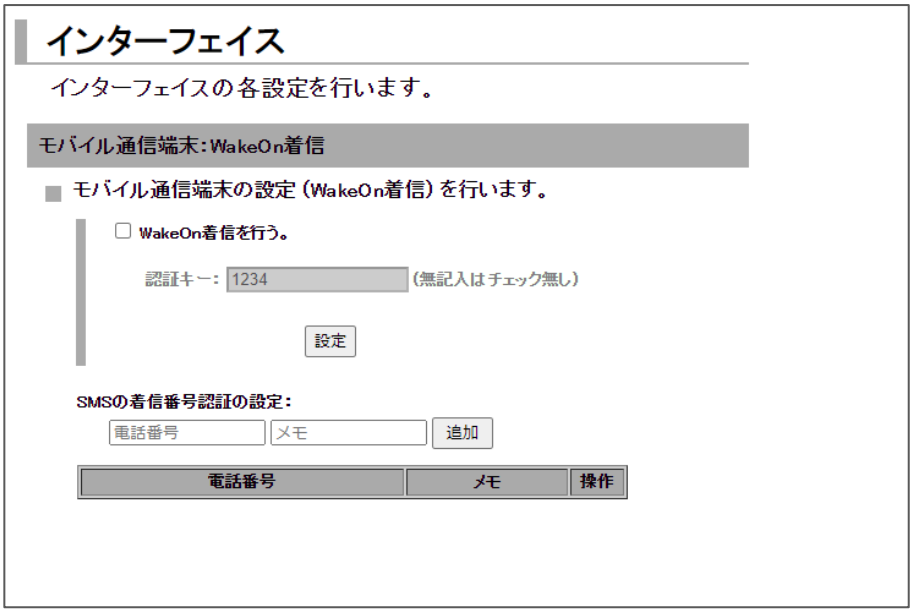
4-3. WakeOn着信の設定

【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、［インターフェイス］－［モバイル通信端末］－［WakeOn 着信］をクリックします。

「WakeOn 着信」のページが表示されます。



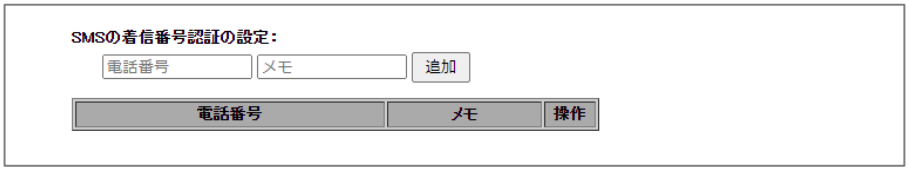
2. WakeOn 着信機能を使用する場合は、「WakeOn 着信を行う」のチェックをオンにします。

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. [設定] ボタンをクリックして、設定内容を反映させます。

5. SMS の着信番号の認証に使用する電話番号を追加します。



6. 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－（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。

memo 着信番号認証の設定は最大 16 件まで行えます。

7. [追加] ボタンをクリックし、電話番号を登録します。

! WakeOn 着信があると、モバイル通信端末ログに記録されます。

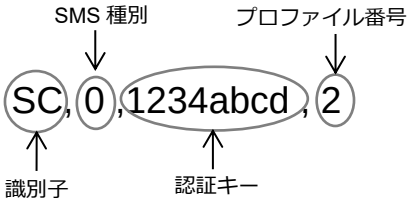
Wake On SMSメッセージ

認証キーが空白の場合は、識別子、SMS 種別、プロファイル番号が送信され、プロファイル番号がデフォルト設定しているプロファイルに接続され、識別子と SMS 種別が表示されます。
設定項目は半角英数字のみです。また、項目と項目の間は必ずコンマで区切ってください。

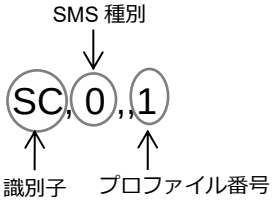
項目	要否	最大文字数	説明
識別子	必須	2	SC 本機能のメッセージであることを示す文字列 大文字小文字の区別なし
SMS 種別	必須	2	0：WakeOn
認証キー	任意	16	この文字列が［認証キー］設定と一致しない場合、受信した SMS は無視されます。
プロファイル番号	任意	2	モバイル回線接続を行うプロファイル番号 無記入の場合、デフォルトプロファイルとなります。

Wake On SMS メッセージ設定例

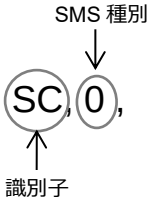
【認証キーありで、プロファイル 2 に接続の場合】



【認証キーなしで、プロファイル 1 に接続の場合】



【認証キーなしで、デフォルトプロファイルに接続の場合】

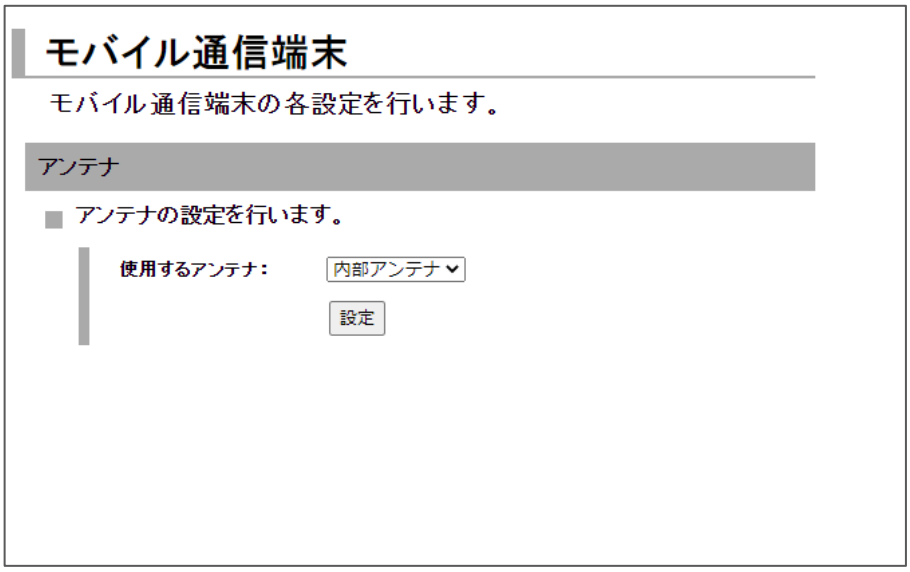


4-4. アンテナの設定

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、［インターフェイス］－［モバイル通信端末］－［アンテナ］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。

［設定］ボタンをクリックして、設定を反映させます

外部アンテナを選択した場合、外部アンテナ MOBILE1、MOBILE2 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。

4-5. 切断・接続方法

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

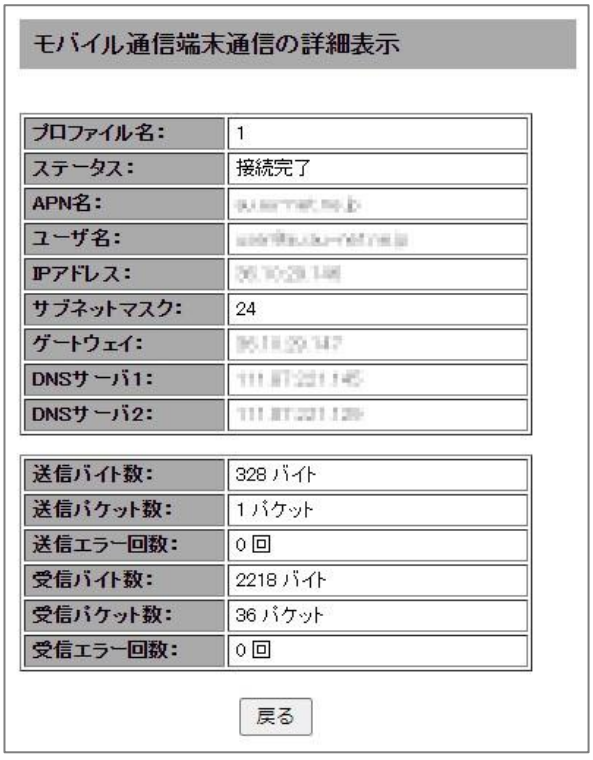
項目		内容
プロファイル名		現在接続している回線の接続先の設定番号を表示します。
接続先 情報		現在接続している回線の接続先を表示します。 未接続時は空白になります。
接続先 メモ		現在接続している回線の接続先のメモを表示します。 未接続時は空白になります。
ステータス		設定した回線の接続の現在の状態が表示されます。 ［詳細表示］をクリックすると、現在の状態をより詳しく参照できます。 ➲ ステータスの詳細については、『ステータス項目の状態一覧』をご覧ください。
操作	［接続#1～#8］	それぞれの回線の接続先に対する接続動作を行います。
	［切断］	接続中の回線に対する切断動作を行い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

ステータス表示	状態	MOBILE ランプの状態
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。



【MBIM モードの場合】

項目	内容
ステータス	設定したダイヤルアップ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。
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（*）	サブネットマスクを表示されます。
ゲートウェイ （*）	ゲートウェイの IP アドレスが表示されます。
DNS サーバ 1 （*）	DNS サーバ 1 の IP アドレスが表示されます。
DNS サーバ 2 （*）	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。

項目	内容
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。

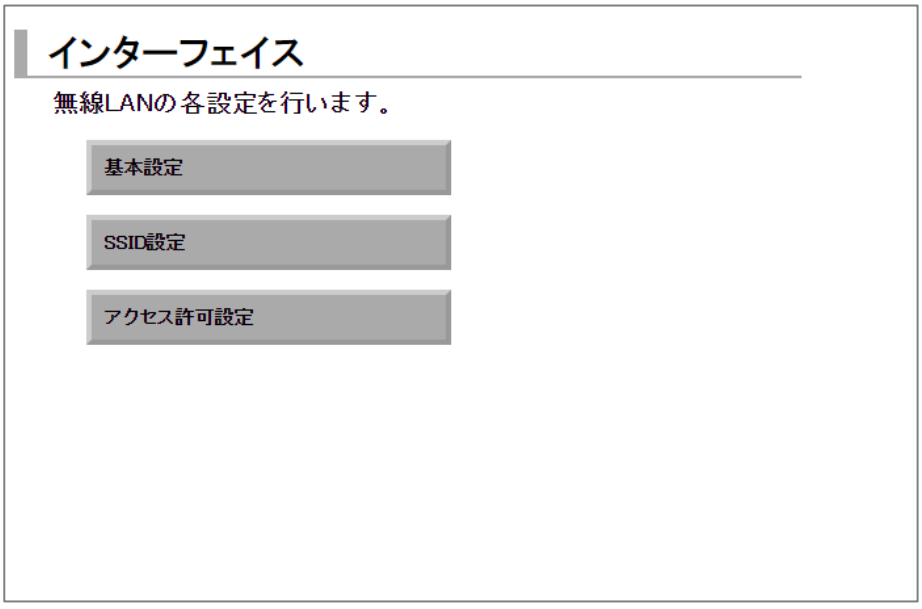
(＊) MBIM モードのみの表示となります。ECM モードでは表示されません。

5章　無線LANの設定 DRX5010

この章では、DRX の無線 LAN の基本設定、SSID の設定、無線 LAN にアクセスを許可する MAC アドレスの設定について説明します。

設定ツールのメニューから、［インターフェイス］－［無線 LAN］ をクリックします。

「インターフェイス 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。

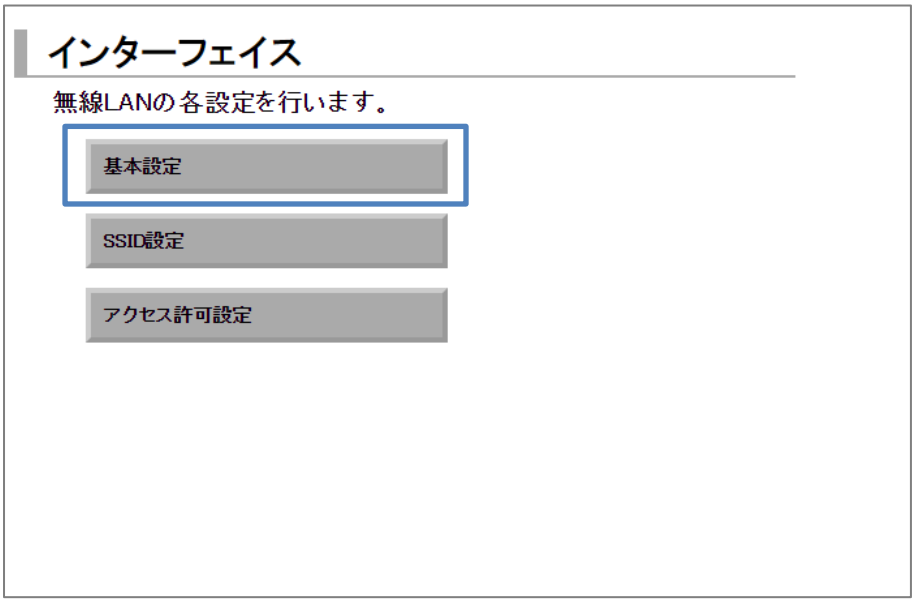
設定項目	説明
基本設定	無線 LAN の詳細情報を登録します。
SSID 設定	SSID の詳細情報を設定します。
アカウント許可設定	MAC アドレスの登録を行います。

- 接続可能な無線 LAN 端末数は最大 20 台となります。

5-1. 基本設定

無線 LAN を使用する場合の基本設定を行います。

1. 「インターフェイス 無線 LAN」のページにて、[基本設定] をクリックします。



2.「基本設定」のページが表示されます。

3．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は、チェックをオンにします。</td></tr>
</table>

4．［設定］ボタンをクリックして、設定を反映させます。

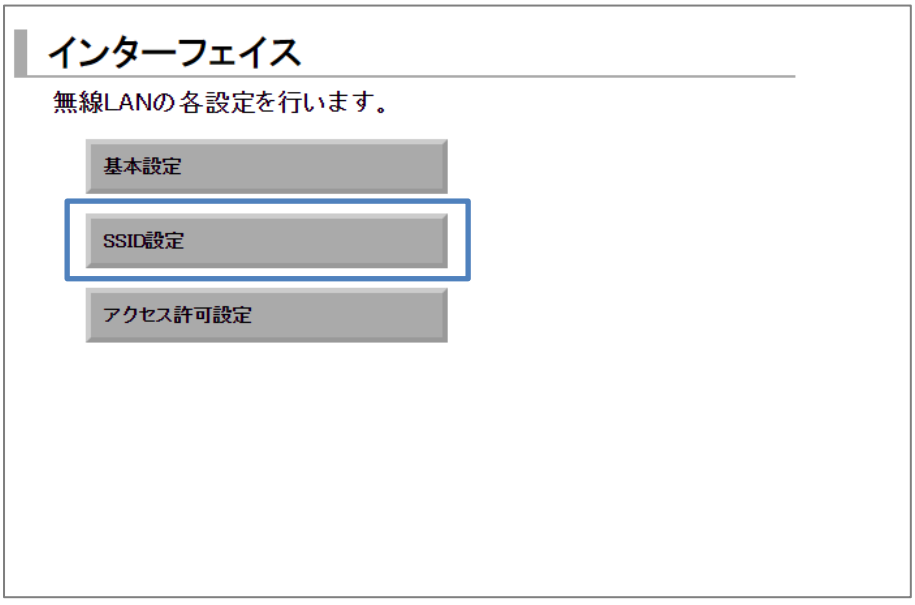
「子機間通信を有効」の設定は「同一 SSID 間の子機間通信」を有効にする機能です。異なる SSID（SSID1 と SSID2 の子機同士）の通信はこちらの設定と関係なく、通信することができます。

・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。

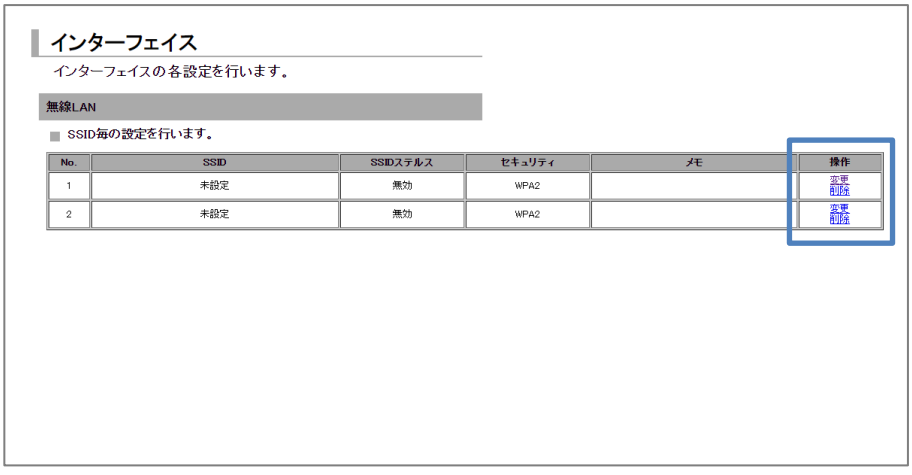
5-2. SSIDの設定

SSID の設定を行います。

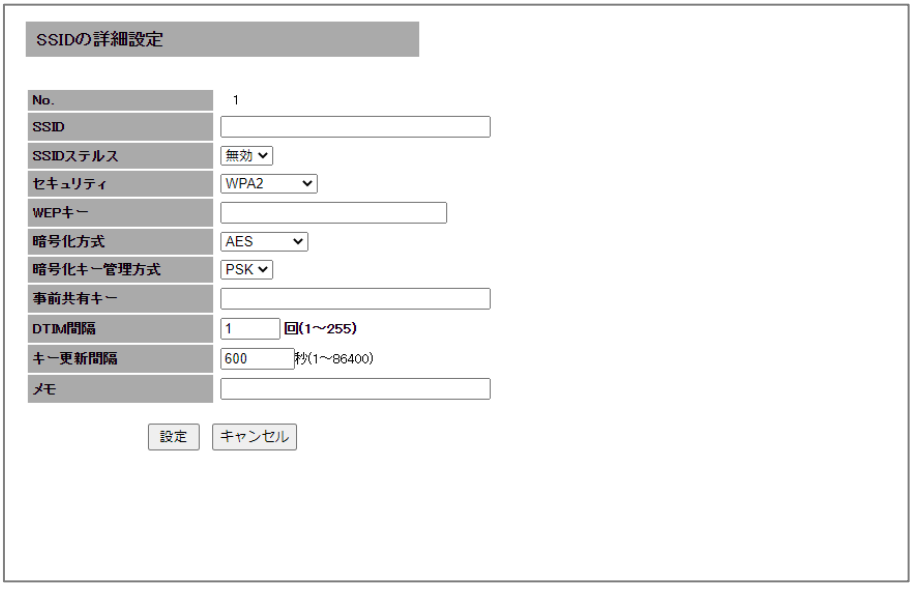
1. 「インターフェイス 無線 LAN」のページにて、[SSID 設定] をクリックします。



2. 「SSID 設定」のページが表示されます。［No.1］または［No.2］の [操作] 項目にて [変更] をクリックします。



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。

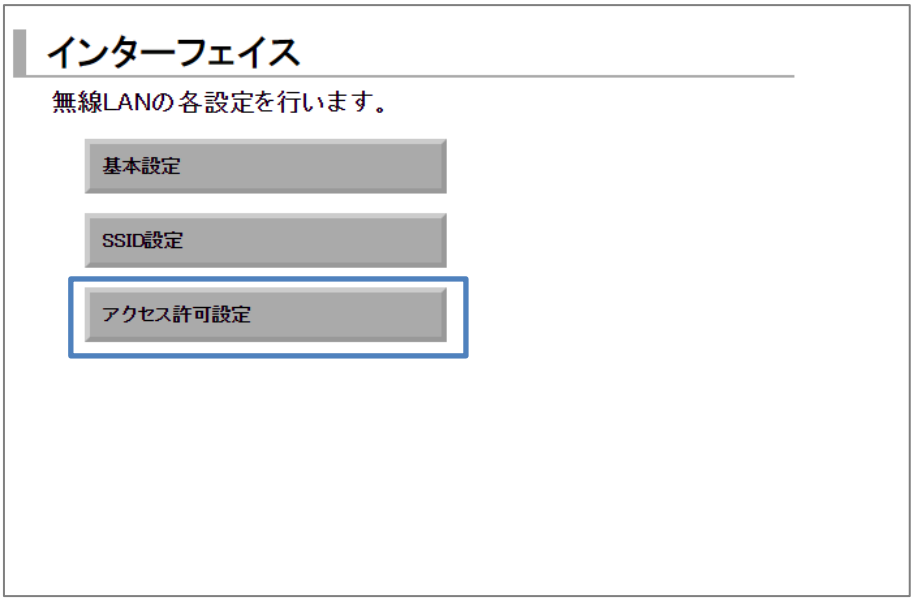
5. ［設定］ボタンをクリックして、設定を反映させます。

5-3. アクセス許可設定

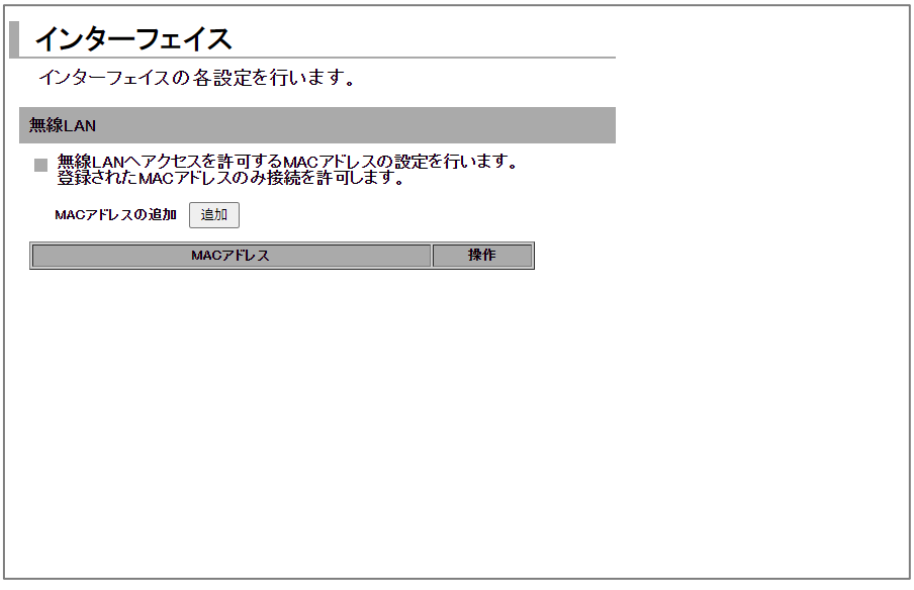
無線 LAN へのアクセスを許可する MAC アドレスの設定を行います。

> 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. 「インターフェイス 無線 LAN」のページにて、[アクセス許可設定] をクリックします。



3.「無線 LAN - アクセス許可設定」のページが表示されます。［MAC アドレスの追加］にて［追加］をクリックします。



4．「MAC フィルタリングの詳細設定」ページが表示されます。
無線 LAN 接続を許可したい MAC アドレスを入力します。

5．［設定］ボタンをクリックして、設定を反映させます。

6章　DRXのメンテナンス

この章では、DRX に設定した情報の保存方法や、ファームウェアのアップデート、再起動などについて説明します。

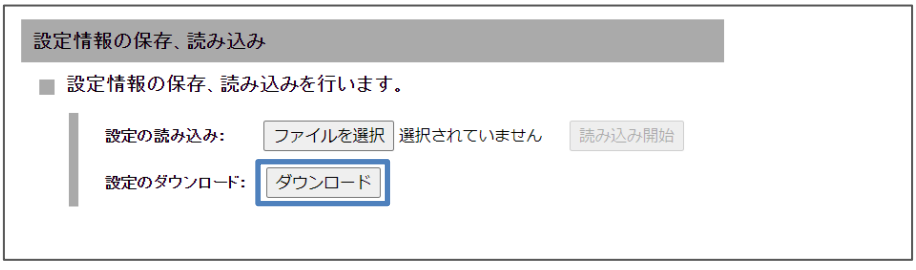
6-1. 設定情報の保存、読み込み

1. 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。

6-1-1.　現在の設定を保存

現在の設定情報の保存を行います。

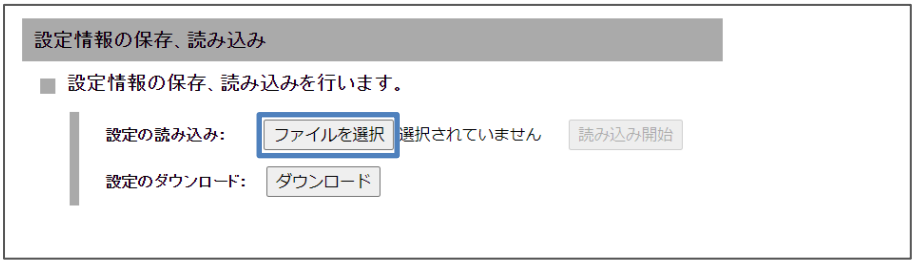
1．［設定のダウンロード］の［ダウンロード］ボタンをクリックします。



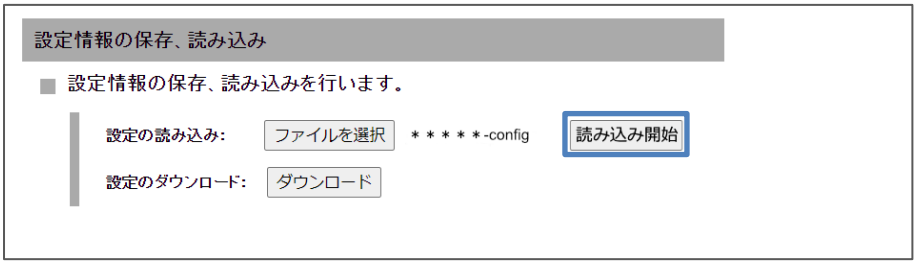
2．保存先を指定する場合は、［名前を付けて保存］を選択して、保存先を指定します。
DRX の設定情報「DRX-backup-config.cnf」ファイルが、指定した保存先にダウンロードされます。

6-1-2. 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「-config」の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。



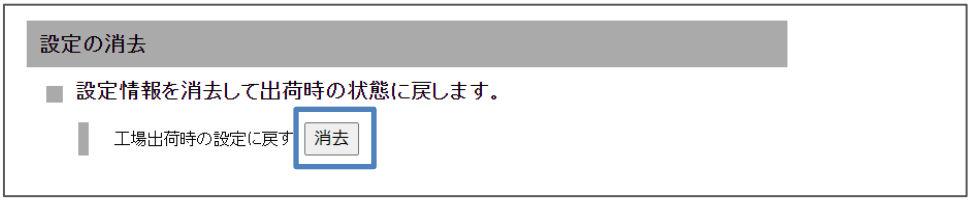
3　DRX の設定が保存時の設定に書き戻されます。

> 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。

6-2. 設定情報の消去

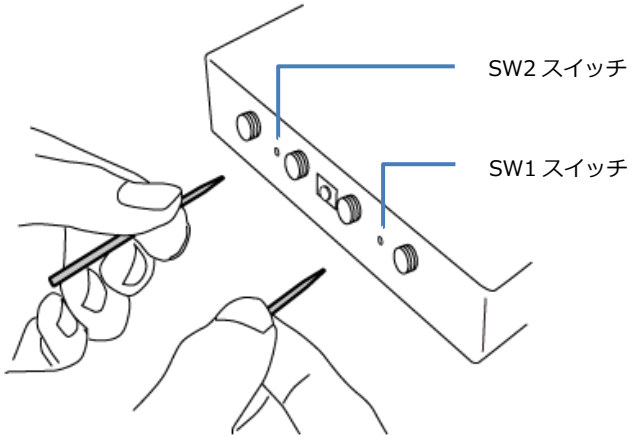
1. 設定ツールのメニューから、［本体設定］–［設定の消去］ をクリックします。
   「設定の消去」のページが表示されます。

2. ［工場出荷時の設定に戻す］の 消去 ボタンをクリックします。



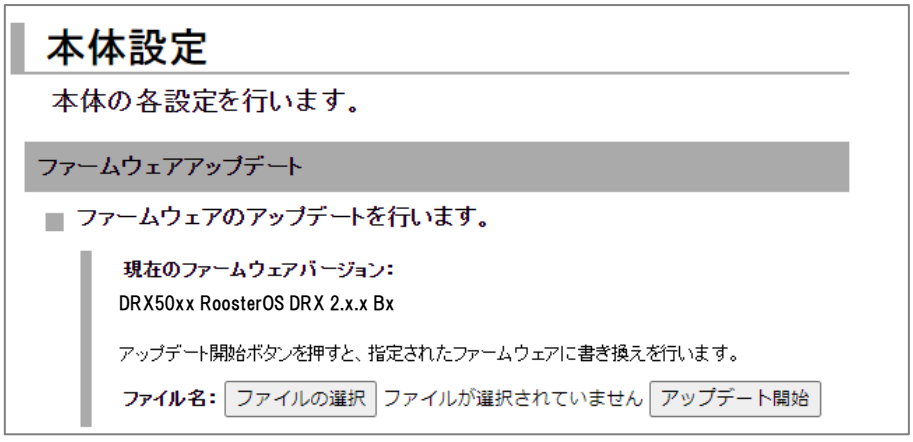
確認ダイアログで［OK］をクリックすると、DRX が再起動し、設定が工場出荷時の状態にリセットされます。

memo 設定情報の初期化は、DRX 本体にある SW1 および SW2 スイッチを同時に長押し（3 秒以上）でも行うことができます。

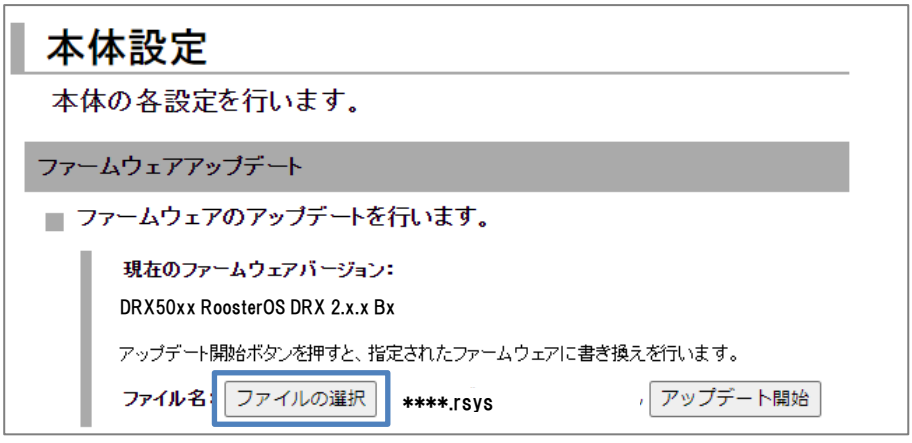


6-3. ファームウェアのアップデート方法

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。
「ファームウェアのアップデート」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［OK］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。

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
・ファームウェアのアップデートでは追加パッケージ(＊.rtar ファイル)がインストールできます。
・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。
・インストールされている追加パッケージの一覧を確認、または削除を行う場合は、CLI かアドバンスモード WebUI から操作してください。

6-4. 再起動

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

2. ［再起動］ボタンをクリックします。

> 再起動が完了するまで、3 分程度かかります。

6-5. モバイル通信端末のメンテナンス

モバイル通信端末の情報表示や制御を CLI で行うことができます。
・電話番号、IMEI、アンテナレベル、その他モバイル通信端末情報の表示
・モバイル通信端末のリセット
・電波周波数の取得
詳細は「Rooster DRX CLI 設定機能説明書」をご覧ください。

6-6. シャットダウン

DRX の電源を切断するときは、シャットダウン操作をした後に電源を切断することをお勧めします。

シャットダウン操作は、以下の方法があります。

・SW1 スイッチを押下する

➔ 詳細は『1-5. 各部名称と機能』をご覧ください。

・CLI コマンドを実行する

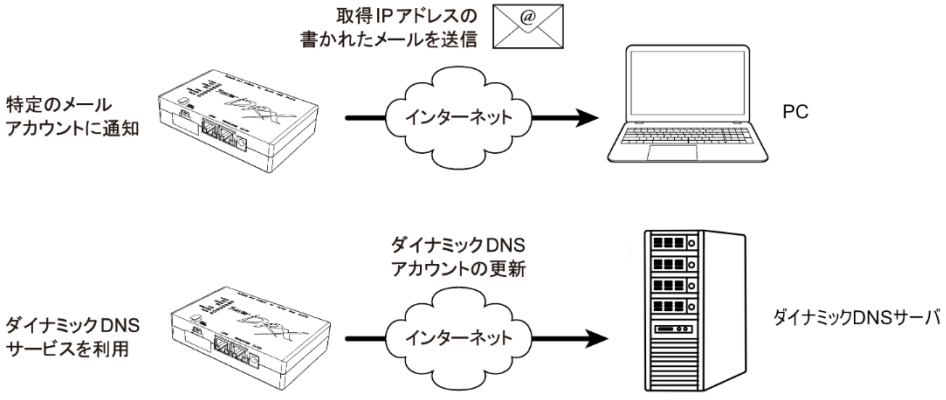
➔ 詳細は『Rooster DRX CLI 設定機能説明書』をご覧ください。

7章　各種サービス設定

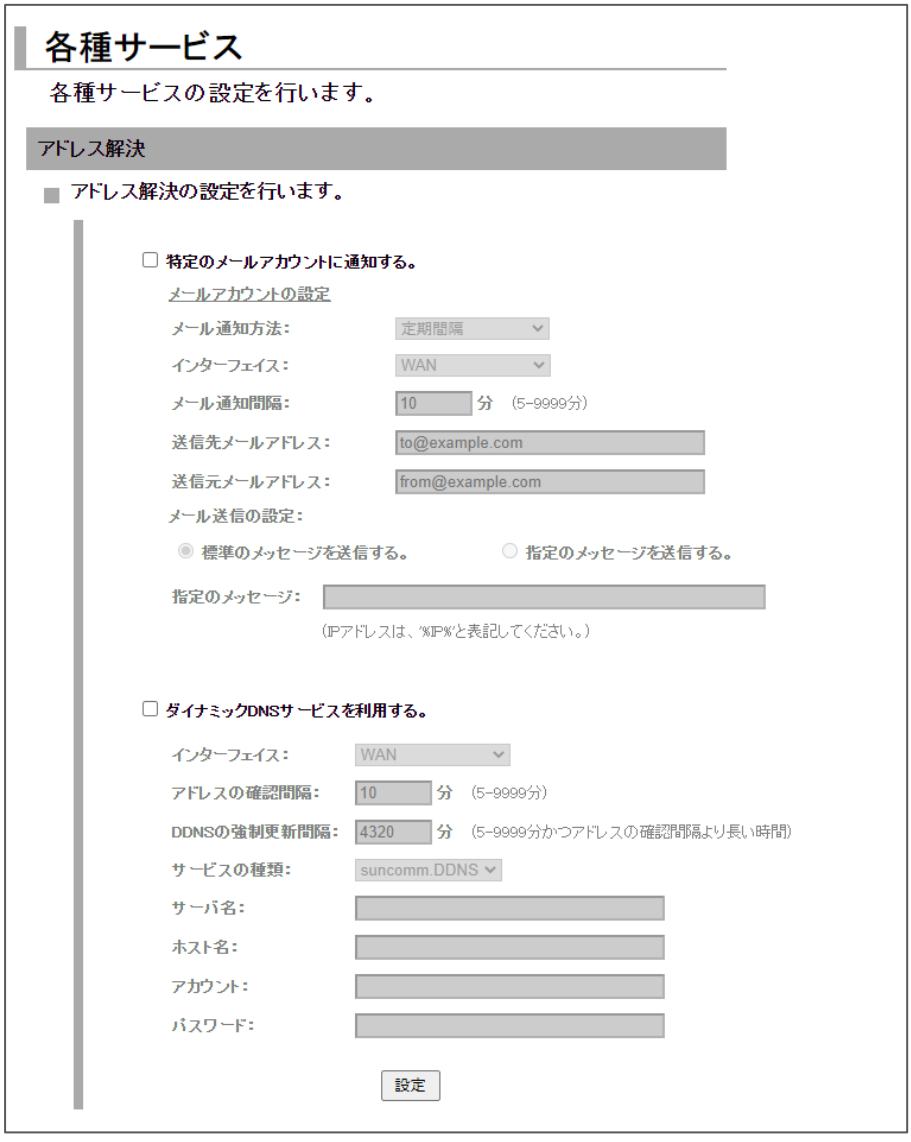
この章では、ネットワークをより快適に利用するための各種サービスの設定について説明します。

7-1. アドレス解決機能

【アドレス解決機能について】
外部ネットワークから、インターネットに接続された DRX にアクセスする場合、DRX に割り当てられたグローバル IP アドレスの情報が必要になりますが、通常のインターネット接続ではインターネットに接続するたびに、グローバル IP アドレスは任意に変化します。
DRX では、変化するグローバル IP アドレスを指定メールアカウントに通知する機能、ダイナミック DNS サーバを利用する機能のいずれかの方法によって、上記問題を解決することができます。



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



アドレス解決機能を使用する場合は、以下の設定を行います

7-1-1. IPアドレスを指定メールアカウントに通知する設定

1. ［特定のメールアカウントに通知する］チェックをオンにし、以下の設定を行います。

項目	内容
メールアカウントの設定	➲ 設定方法は『3-5. メールアカウントの設定』をご覧ください。 ❗ 引き続いて［メールアカウントの設定］も行う場合は、ここで一度［設定］ボタンをクリックして、設定内容を反映させます。［設定］ボタンより先に［メールアカウントの設定］をクリックすると、設定した内容が破棄されます。
メール通知方法	メールの通知方法を選択します。 ［定期間隔］、［IP アドレス変更時］ のいずれかを指定します。
インターフェイス	どのインタフェースのグローバル 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フェースとなります。
メール通知間隔	「メールの通知方法」を「定期間隔」とした場合に設定します。 指定メールアカウントに、設定された時間（分）ごとにメール送信します。 ・設定範囲：5～9999
送信先メールアドレス	グローバル IP アドレスを通知させたいメールアドレスを入力します。
送信元メールアドレス	送信者のメールアドレスを入力します。 ▶通常、「メールアカウント」設定で設定したアカウントのメールアドレスを設定します。 ❗ 送信元メールアドレスの入力がないと、メールサーバによってはメールが送信されない場合があります。
メール送信の設定	通知メールのメッセージ内容を指定したい場合は、［指定のメッセージを送信する］を選択します。必要がなければ、［標準のメッセージを送信する］を選択します。 標準のメッセージは、以下のような形式で送信されます。 【送信メールの例】 タイトル：Rooster IP Report 送信者：Rooster（DR0101A000000）⇒カッコ内は Rooster DRX の　製造番号 内容：Rooster IP-Address Report v0.01. S/N=DR0101A000000　⇒ DRX の製造番号 IP=10.20.30.40　⇒ 割り当てられたグローバル IP アドレス 文字列を指定して入力を行う場合、指定のメッセージ入力フォームに、「%IP%」（「 」は不要）と入力すると、取得したグローバル IP アドレスに変換されて通知されます。 ▶【割り当てグローバル IP アドレスが"11.22.33.44"の場合】 設定内容：http:// %IP%/mobile 実際に送信されるメッセージ：http://11.22.33.44/mobile

2. ［設定］ボタンをクリックして、設定内容を反映させます。

7-1-2. ダイナミックDNSサービスを利用する設定

1．［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	どのインタフェースのグローバル 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フェースとなります。 ❗ デフォルトルートに設定するインタフェー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。

2．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。

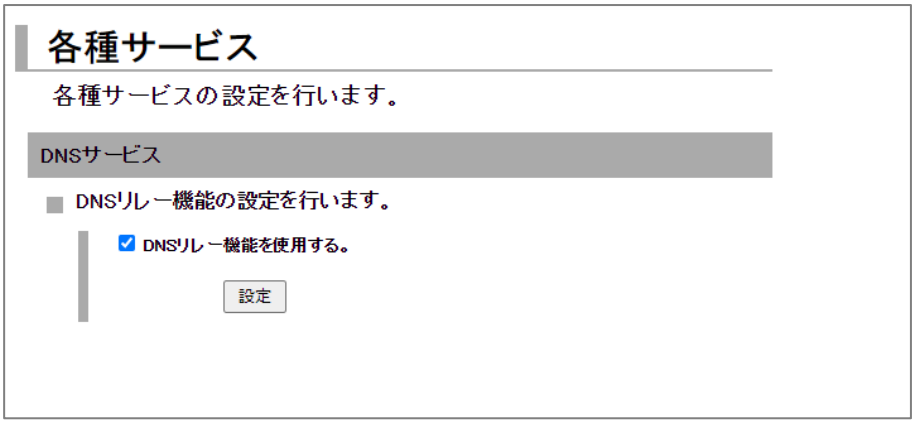
➲ パスワードは『2-7.入力できない記号一覧』 をご確認の上、設定してください。

3．［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。

7-2. DNSサービス

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



2. DNS リレー機能を使用する場合、［DNS リレー機能を使用する］チェックをオンにします。
3. ［設定］ボタンをクリックして、設定内容を反映させます。

DNS リレー機能を使用するかしないかによって、接続機器 TCP/IP 設定の DNS サーバ設定方法が異なってきます。以下のうち該当する設定を行ってください。

DNSリレー機能を使用する場合

DRX に接続されている PC を下記のいずれかの設定を行います。

➲『2-6-1. Windows のネットワーク設定』

- DNS サーバアドレスを自動的に取得するように設定します。
- DNS サーバアドレスを指定する場合、DRX の LAN IP アドレス、またはプロバイダ指定の DNS サーバ（ネームサーバ）アドレスを指定します。

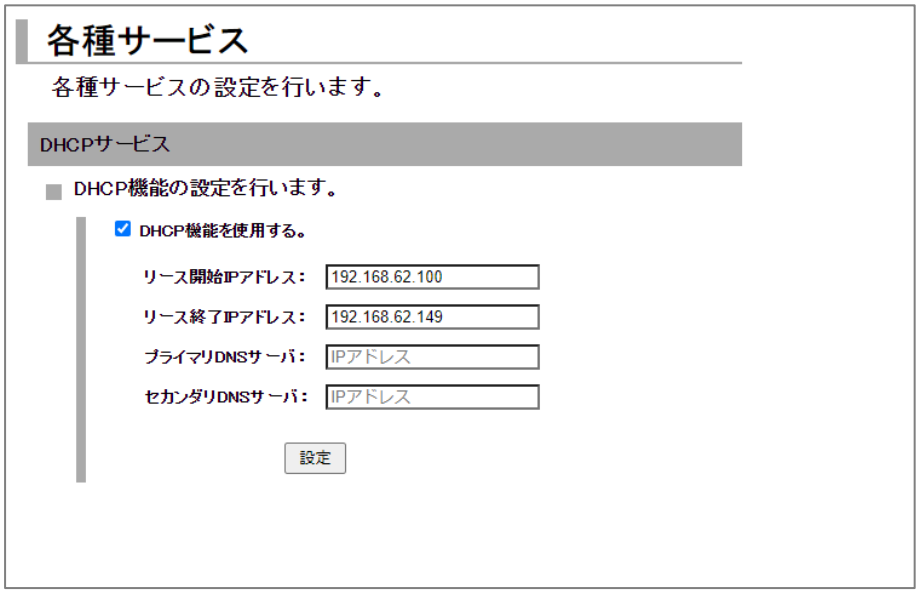
DNSリレー機能を使用しない設定の場合

自動取得されないので、指定する必要があります。
プロバイダ指定の DNS サーバ（ネームサーバ）アドレスを指定します。

DNS リレー機能は、DRX と同一ネットワーク内の機器のみに応答します。

7-3. DHCPサービス

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



2. DHCP 機能を使用する場合、［DHCP 機能を使用する］チェックをオンにします。

3. 以下の項目を設定します。

項目	内容
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。
プライマリ DNS サーバ	DHCP で配布するプライマリ DNS サーバを指定します。
セカンダリ DNS サーバ	DHCP で配布するセカンダリ DNS サーバを指定します。

4.［設定］ボタンをクリックして、設定内容を反映させます。

リース開始 IP アドレス、リース終了 IP アドレスに 192.168.225.0～192.168.225.255 を設定しないでください。

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 割り当て一覧］をクリックして表示される「DHCP 割り当て表示画面」から確認することができます。

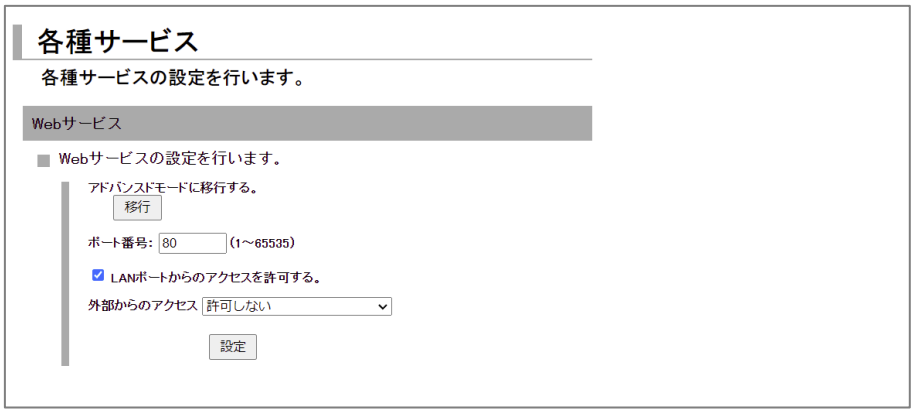
項目	内容
IP アドレス	DRX LAN 内にある LAN 接続機器に割り当てた IP アドレスが表示されます。
MAC アドレス	上記の IP アドレスを付与された、LAN 接続機器の MAC アドレスが表示されます。 DRX を再起動すると、DHCP テーブルはすべてリセットされます。 再起動後、クライアントからの IP アドレス割り当て要求を受けたタイミングで、再度 DHCP テーブルに登録されます。

DHCP 機能は、DRX と同一ネットワーク内の機器のみに応答します。

7-4. Webサービス

【Web サービスについて】
Web サービスは、DRX の Web 設定ツールにアクセスを行う機能です。
設定により LAN ポートまたは WAN から、Web 設定ツールにアクセスできるポートを決定することができます。

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



2．「アドバンスドモードに移行する」の「移行」ボタンをクリックします。

➲ アドバンスドモードの詳細は『7-4-1. アドバンスドモード』をご覧ください。

【設定モードについて】
DRX の設定は 2 つのモードがあります。
・シンプルモード
一般的な機能を簡易に操作で設定が出来るモードです。（工場出荷状態）
WWW ブラウザから Web 設定ツールを操作することで各種設定を行います。
SSH による CLI コマンドからは情報出力やログ取得などが可能です。（設定は不可）
・アドバンスドモード
上級者を対象にした詳細な設定が可能となるモードです。
WWW ブラウザから Web 設定ツールや、SSH による CLI コマンドで操作することで各種設定を行うモードです。

3．「ポート番号」で、Web サービスで使用するポート番号を入力します。
ポート番号は 80 か 1024 以上を設定してください。

WWW ブラウザからの接続例：
ポート番号を 50000 にした場合、「http://192.168.62.1:50000」

4．以下の設定を行います。

項目	内容
LAN ポートからのアクセスを許可する	チェックをオンにすると、LAN ポートと無線 LAN（DRX5010）からの設定ツールへのログインができます。 オフにすると、LAN ポートからのログインができません。
外部からのアクセスを許可する	WAN 側からの設定ツールへのログインを許可するポリシーを設定します。 ［許可しない］、［全て許可する］、［INPUT フィルタリングに従う］から選択します。

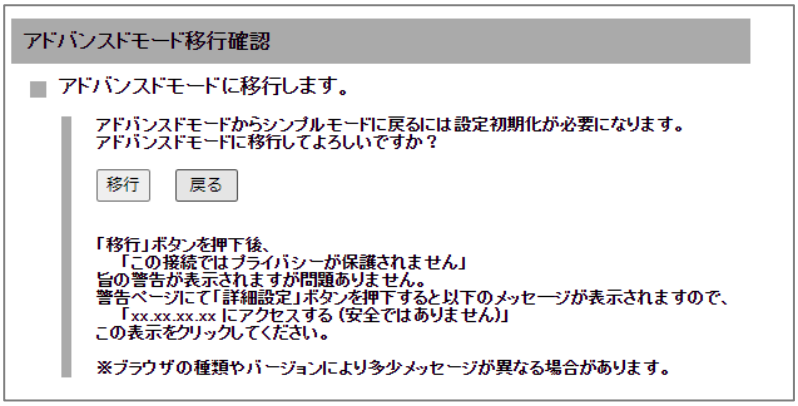
「LAN ポートからのアクセスを許可する」のチェックをオフにする場合は、外部からのアクセスが接続できることを確認してからチェックをオフにする必要があります。
この設定を間違えると、どこからも設定変更できなくなります。
設定を間違えた場合は、工場出荷時の状態に戻す必要があります。

5．［設定］ボタンをクリックして、設定内容を反映させます。

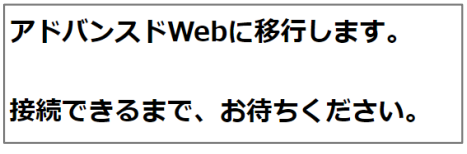
7-4-1. アドバンスドモード

「アドバンスドモード」へ移行すると「シンプルモード」（現在の GUI 操作画面）には戻れません。
戻るには設定初期化が必要となります。

1．「アドバンスドモードに移行確認」画面の［移行］ボタンをクリックします。



2．少し待つと、以下の画面が表示されます。



3．更に少し待つと、［この接続ではプライバシーが保護されません］などのメッセージが表示されますが問題ありません。この画面の［詳細設定］ボタンを押下すると［xx.xx.xx.xx にアクセスする（安全ではありません）］が表示されますので、この文字をクリックしてください。

4．［アドバンスモードのログイン画面］が表示され、アドバンスモードの移行は完了しました。
以降、Web ブラウザから操作する場合は『RoosterDRX アドバンスモード Web 設定機能説明書』、または CLI コマンドで操作する場合は『Rooster DRX CLI 設定機能説明書』をご覧ください。

memo

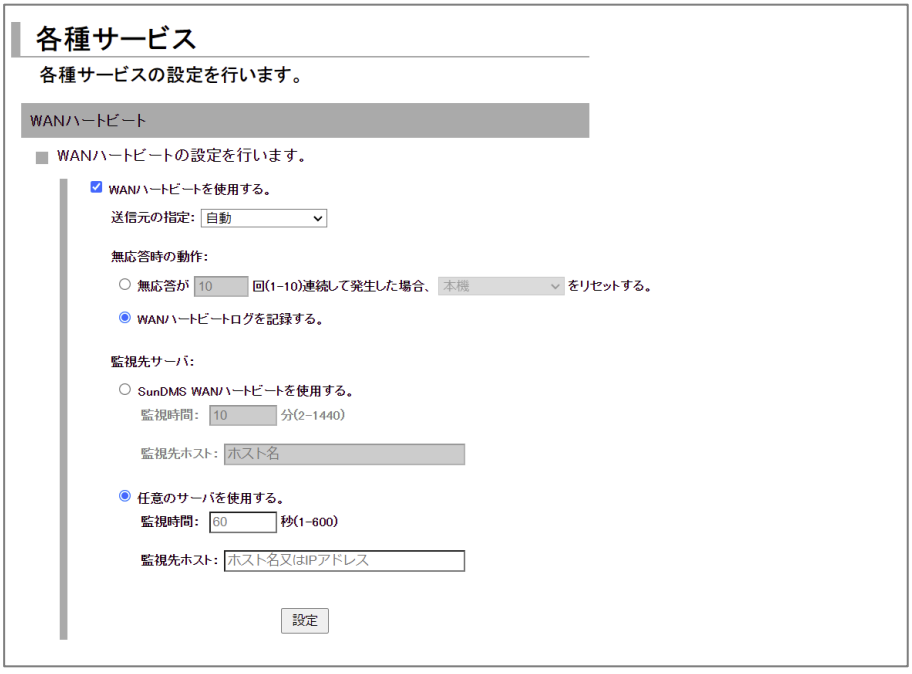
シンプルモード：
一般的な機能を簡易に操作で設定が出来るモードです。（工場出荷状態）
WWW ブラウザから Web 設定ツールを操作することで各種設定を行います。
SSH による CLI コマンドからは情報出力やログ取得などが可能です。（設定は不可）
➲詳細は『3-1. Rooster Web 設定ツール』をご覧ください。

アドバンスドモード：
上級者を対象にした詳細な設定が可能となるモードです。
WWW ブラウザから Web 設定ツールや、SSH による CLI コマンドで操作することで各種設定を行うモードです。
➲詳細は『RoosterDRX アドバンスモード Web 設定機能説明書』、『Rooster DRX CLI 設定機能説明書』をご覧ください。

7-5. WANハートビート機能

【WAN ハートビート機能について】
WAN ハートビート機能は、WAN 側のネットワークが正常に動いているかどうかの確認を行うための機能です。

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



2．［WAN ハートビートを使用する］チェックをオンにします。

3．以下の設定を行います。

項目		内容
送信元の指定		送信元のインタフェースを指定します。 ［自動］、［LAN］、［WAN］、［モバイル通信端末］から選択します。 IPsec 接続先の監視先ホストを指定する場合、[自動]にしてください。
［無応答時の動作］		WAN ハートビートで、接続状態の確認ができなかった場合に行う動作を選択します。 • 無応答が[指定回数] 連続して発生した場合、[本機／モバイル通信端末]をリセットします。 [指定回数] 連続して失敗した時点で、[本機]もしくは[モバイル通信端末]を再起動します。 • WAN ハートビートログを記録します。 再起動は行わず、設定された監視時間ごとに WAN ハートビートログに「失敗」のログを記録します。
［SunDMS WAN ハートビートを使用する。］	監視先ホスト	WAN ハートビートを行う「SunDMS WAN ハートビート」のドメイン名を指定します。 ➲「SunDMS WAN ハートビート」のサービスの詳細は『 7-7. SunDMS サービス 』をご覧ください。
	監視時間	「SunDMS WAN ハートビート」に監視を行う時間の間隔（分）を指定します。 ・設定範囲：2～1440
［任意のサーバを使用する。］	監視先ホスト	WAN ハートビートを行う相手先を指定します。相手先 IP アドレスまたは、ドメイン名を指定します。 指定する IP アドレスはグローバル IP アドレスまたは VPN 接続先のネットワーク IP アドレスです。
	監視時間	監視先ホストに監視を行う時間の間隔（秒）を指定します。 ・設定範囲：1～600

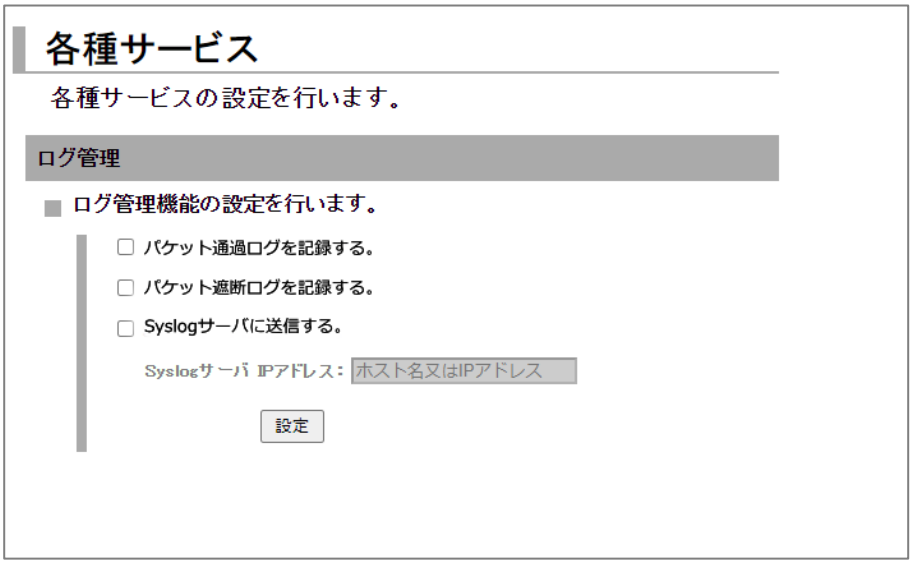
4．［設定］ボタンをクリックして、設定内容を反映させます。

従量制課金でご契約の場合は、設定しないようにしてください。
意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。

回線バックアップ、バックアッププロファイル、モバイル副回線監視 と併用設定する場合、監視時間の設定によっては動作が干渉する場合があります。干渉しあわないよう適切な設定をしてください。

7-6. ログ管理

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



2. パケット通過ログの記録を行う場合は、［パケット通過ログを記録する］チェックをオンにします。

3. パケット遮断ログの記録を行う場合は、［パケット遮断ログを遮断する］チェックをオンにします。

4. Syslog サーバでログ管理を行う場合は、［Syslog サーバに送信する］チェックをオンにし、Syslog サーバのローカル IP アドレスを入力します。この設定を行った場合、DRX のログを Syslog サーバへ送信します。

> パケット通過ログ パケット遮断ログは syslog サーバに送信されません。

5. ［設定］ボタンをクリックして、設定内容を反映させます。

> ログ管理画面の表示は 5 秒ほどかかりますが、設定内容によって画面表示までの時間が遅くなる場合があります。ご了承ください。

7-7. SunDMSサービス

【SunDMS について】
「SunDMS」は弊社が運用する、DRX のより安心・安定運用を目的とした、デバイスの集中管理サービスです。SunDMS ではデバイスの死活監視や状態の取得、設定の変更／取得・再起動処理・ログ取得・ファームウェア更新の操作を遠隔集中管理から無償で行う事ができます。
詳細については、以下の URL を参照してください。

「SunDMS」
https://www.sun-denshi.co.jp/sc/product_service/service/dms/

※SunDMS をご使用の際は、別途お申し込みが必要です。
　詳細につきましては、上記 URL もしくは、弊社営業部までお問い合わせください。
※一部有償サービスとなります。

SunDMS サービス機能はインターネット上の SunDMS サーバと通信を行います。
従量データプラン契約の SIM をご使用の場合は、通信料が高額となる場合がありますのでご注意ください。

【通信量の目安】
1 回の死活監視に 6KByte 程度のデータ通信が発生します。SunDMS で死活監視の間隔を 1 時間に 1 回と設定した場合、1 ヵ月で約 4.3MByte 程度の通信が発生します。
また、ログ取得を行った場合は 1 回で最大約 66MByte 程度のデータ通信が発生します。
(上記、通信量は目安となります。回線状況により変動します)

SunDMS サービスはインターネット上の SunDMS サーバに接続を行います。
工場出荷状態では SunDMS サービスが有効に設定されていますので、閉域網へ接続する場合など SunDMS サーバへ接続させたくない場合、以下の手順で無効に設定ください。

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

2. 初期状態で、［SunDMS 機能を使用する］チェックはオンになっています。
   SunDMS サービスを停止したい場合は、［SunDMS 機能を使用する］チェックをオフにします。
   SunDMS サービスを使用したい場合は、オンにします。（工場出荷状態）

3. ［SunDMS サーバ名］は工場出荷設定から変更しないでください。（システム管理者から指定された場合のみ変更ください ）

4. ［設定］ボタンをクリックして、設定内容を反映させます。

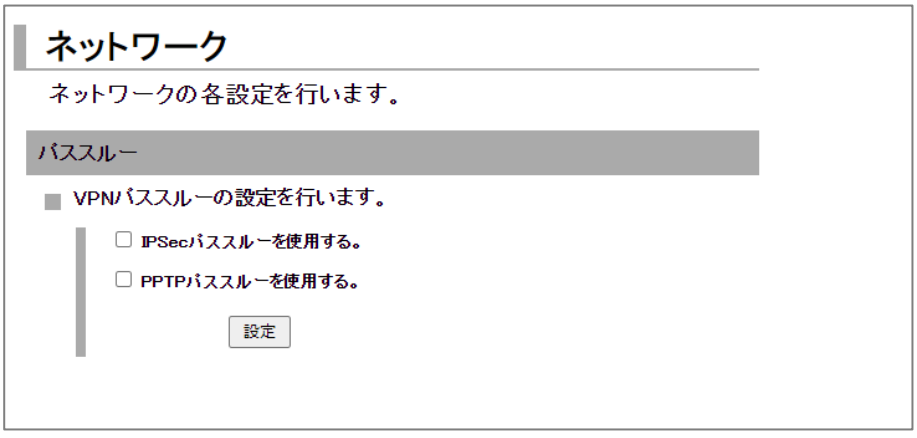
8章　ネットワーク設定

この章では、VPN やフィルタリングなど、詳細なネットワーク設定について説明します。

8-1. VPNパススルー

memo 【VPN パススルーについて】
VPN パススルーの設定を行うと、DRX 以外の別の端末が VPN サーバやクライアントとして動作する時、各 VPN プロトコルを通過させることができるようになります。
VPN パススルーは 1 セッションのみとなります。

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



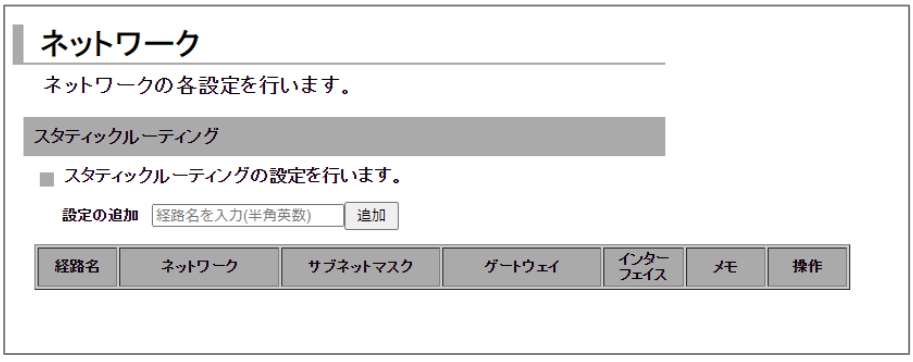
2. 後位端末で IPSec をご利用される場合、［IPSec パススルーを使用する］のチェックをオンにします。

3. 後位端末で PPTP をご利用される場合、［PPTP パススルーを使用する］のチェックをオンにします。

4. [設定] ボタンをクリックして、設定内容を反映させます。

8-2. 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．スタティックルーティングの設定を追加する場合は、［設定の追加］にて［経路名］を入力し、［追加］ボタンをクリックします。設定値は英数文字で入力ください。
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、［変更］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。

3．［追加］ボタン、または［変更］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。

> memo スタティックルートの設定は最大 128 件まで行えます。

3. 以下の設定を行います。

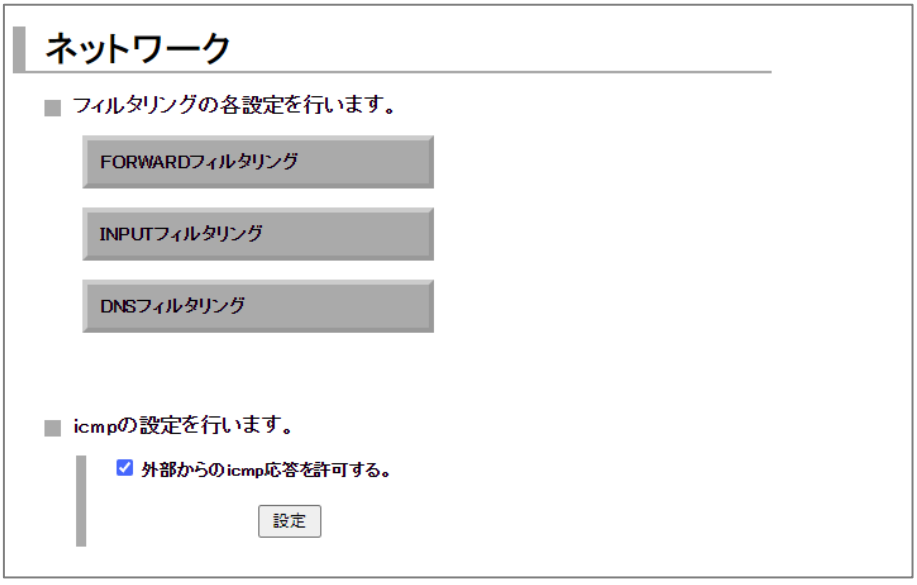
項目	内容
経路名	スタティックルーティングの経路名が表示されます。
ネットワーク	宛先ネットワークアドレスを入力します。
サブネットマスク	上記ネットワークのサブネットマスクを入力します。
ゲートウェイ	上記ネットワークのゲートウェイアドレスを入力します。
インターフェイス	この設定を適用するインタフェースを選択します。 ［WAN］、［モバイル通信端末］、［LAN］ のいずれかを指定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 64 文字までの英数字の文字列を入力できます。

4. ［設定］ボタンをクリックすると、「スタティックルーティング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「スタティックルーティング」のリストのページに戻ります。

8-3. フィルタリング

8-3-1. ICMP応答 フィルタリング

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



2. 外部からの ICMP に応答させない場合、「外部からの icmp 応答を許可する」のチェックをオフにします。

3. ［設定］ボタンをクリックして、設定内容を反映させます。

8-3-2. FORWARDフィルタリング

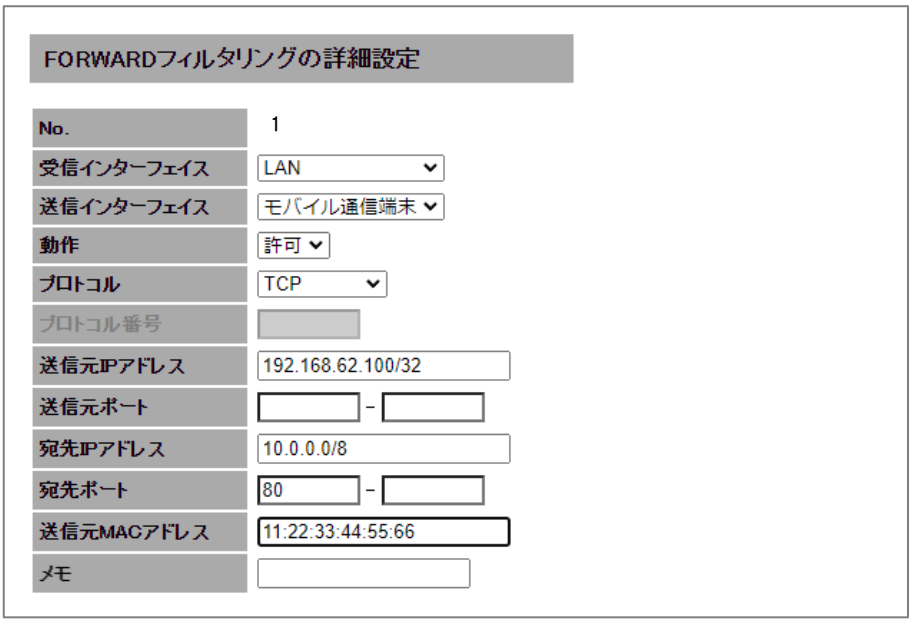
1．設定ツールのメニューから、［ネットワーク］－［フィルタリング］－［FORWARD］をクリックします。
「FORWARD フィルタリング」リストのページが表示されます。

2．FORWARD フィルタリング設定を行った項目以外のパケットをどう処理するかにより、「基本ポリシー」の
・「設定されていないパケットはすべて通す」
・「設定されていないパケットはすべて遮断する」
のうちいずれかを選択します。

> ・設定済みの項目については、「基本ポリシー」の設定に関わらず、個別に設定した動作が適用されます。
> ・VPN（IPsec、PPTP、L2TP/IPsec）間の通信は「基本ポリシー」を「設定されていないパケットはすべて遮断する」に設定した場合、DRX から送信方向の通信を遮断します。許可したい場合は許可する FORWARD フィルタリング設定の追加してください。
> ➲ IPsec 設定の詳細は、『8-6. IPsec』をご覧ください。

3．FORWARD フィルタリング設定を追加する場合は、［設定の追加］にて［No］を入力し、［追加］ボタンをクリックします。設定値は 1～128 です。
設定済みの FORWARD フィルタリング設定を変更する場合は、［変更］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。

4． ［追加］ボタン、または［変更］をクリックすると、「FORWARD フィルタリングの詳細設定」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
No.	FORWARD フィルタリング設定の通し番号が表示されます。
受信インターフェイス	この設定を適用する受信方向のインタフェースを選択します。 ［LAN］、［WAN］、［モバイル通信端末］、［全て］のいずれかを指定します。
送信インターフェイス	この設定を適用する送信方向のインタフェースを選択します。 ［LAN］、［WAN］、［モバイル通信端末］、［全て］のいずれかを指定します。
動作	［許可］、［遮断］のいずれかを指定します。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［ユーザ指定］のいずれかを指定します。 ［ユーザ指定］の場合は、プロトコル番号も指定します。
プロトコル番号	［プロトコル］にて「ユーザ指定」を選択した場合は、プロトコル番号を設定します。
送信元 IP アドレス	FORWARD 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	FORWARD フィルタリングを行う送信元ポート番号を、1～65535 の番号で範囲指定します。
宛先 IP アドレス	FORWARD 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	FORWARD フィルタリングを行うポート番号を、1～65535 の番号で範囲指定します。 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。
送信元 MAC アドレス	FORWARD フィルタリングを行う送信元 MAC アドレスを設定します。
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。 ▶半角 64 文字までの英数字の文字列を入力できます。

6．［設定］ボタンをクリックすると、「FORWARD フィルタリング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「FORWARD フィルタリング」のリストのページに戻ります。

memo FORWARD フィルタリングの設定は最大 128 件まで行えます。

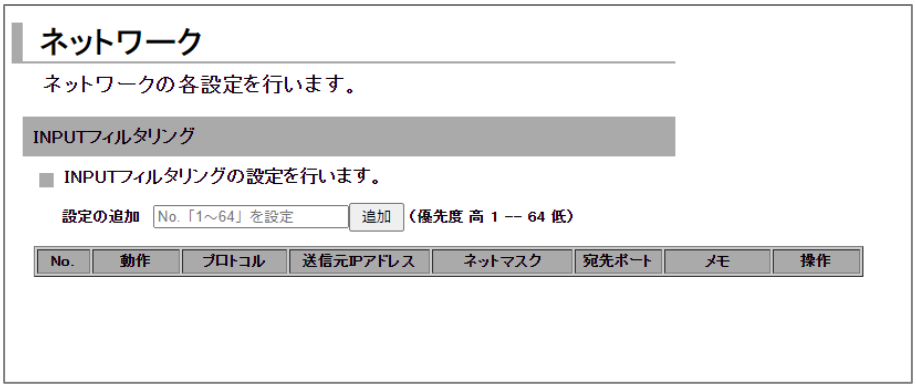
「基本ポリシー」を「設定されていないパケットはすべて遮断する」に設定した場合は、新たにフィルタリングの設定を行う必要があります。

バーチャルサーバ設定で「FORWARD フィルタリングに従う」を選択した場合、「ポート番号」ではなく「サーバのポート番号」で設定ください。

8-3-3. INPUTフィルタリング

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

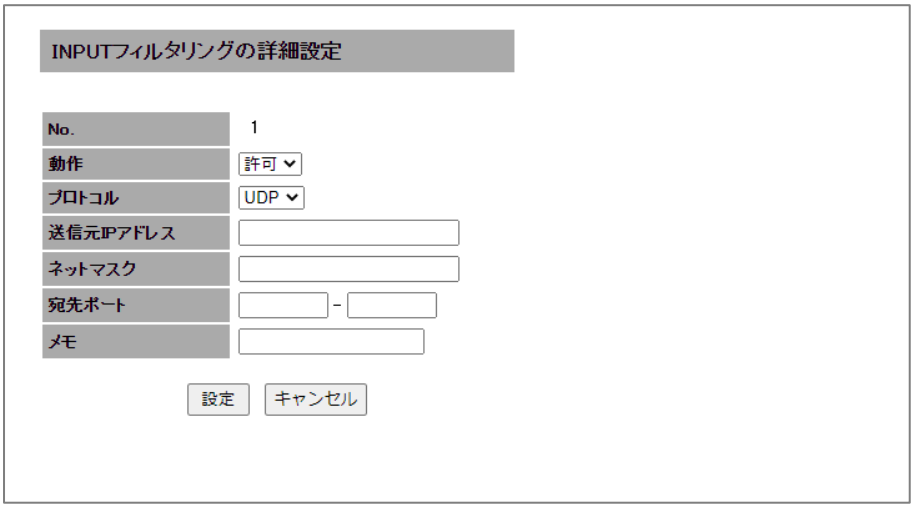
> memo INPUT フィルタリングの設定は、「Web サービスの設定」の [外部からのアクセス] で [INPUT フィルタリングに従う] を選択することにより、有効になります。



4．INPUT 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［No］を入力し、［追加］ボタンをクリックします。設定値は 1～64 です。
既存の設定を変更する場合は、［変更］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。

5．［追加］ボタン、または［変更］をクリックすると、「INPUT フィルタリングの詳細設定」ページが表示されます。

> memo INPUT フィルタリングの設定は最大 64 件まで行えます。



3. 以下の設定を行います。

項目	内容
No.	INPUT フィルタリング設定の通し番号が表示されます。
動作	INPUT フィルタリングの動作を指定します。［許可］のみ。
プロトコル	［UDP］、［TCP］のいずれかを指定します。
送信元 IP アドレス	INPUT フィルタリングを行う送信元アドレスを設定します。
ネットマスク	INPUT フィルタリングを行う送信元サブネットマスクを指定します。
宛先ポート	INPUT フィルタリングを行うポート番号を、1～65535 の番号で範囲指定します。
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。

4. ［設定］ボタンをクリックすると、「INPUT フィルタリング」リストのページに戻り、設定した内容が反映されます。[キャンセル] ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「INPUT フィルタリング」のリストのページに戻ります。

8-3-4. DNSフィルタリング

【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、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］－［フィルタリング］－［DNS］をクリックします。
「DNS フィルタリング」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、［変更］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［変更］をクリックすると、「DNS フィルタリングの詳細設定」ページが表示されます。

> memo DNS フィルタリングの設定は最大 64 件まで行えます。

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	［許可］、［遮断］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. ［設定］ボタンをクリックすると、「DNS フィルタリング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「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 SSH で接続し、CLI コマンドで「nslookup FQDN」でご確認ください。

・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）

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

8-4. バーチャルサーバ

【バーチャルサーバ機能について】
バーチャルサーバ機能は、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能です。
通常、LAN に設置されている機器は、ローカル IP アドレスを持っており、グローバル IP アドレスでアクセスを行うことはできません。
バーチャルサーバ機能を利用し、プロトコル・TCP/UDP ポート番号を指定することによって、LAN 内のどの接続機器へ向けての通信であるか特定できるようになるため、グローバル IP アドレスからのアクセスが行えるようになります。
バーチャルサーバ機能は DMZ と同時に使用することはできません。

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

2. バーチャルサーバの設定を追加する場合は、［設定の追加］にて［No］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、［変更］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。

3. ［追加］ボタン、または［変更］をクリックすると、「バーチャルサーバの詳細設定」ページが表示されます。

memo バーチャルサーバの設定は最大 32 件まで行えます。

4.以下の設定を行います。

項目	内容
No.	バーチャルサーバ設定の通し番号が表示されます。
インターフェイス	バーチャルサーバの設定を行うインタフェースを指定します。 ［WAN］、［モバイル通信端末］、［全て］ のいずれかを指定します。
プロトコル	［UDP］、［TCP］、［all］のいずれかを指定します。
ポート番号	WAN 側で受け付けるポート番号の範囲を指定します。 開始ポート番号を 1～65535 までの番号で指定します。 終了ポート番号を 1～65535 までの番号で指定します。 ▶「＊」などのワイルドカードでの指定は行えません。 ▶ポート番号を 1 つのみ指定する場合、開始ポート番号のみを入力します。
サーバの IP アドレス	バーチャルサーバとして外部に公開する機器の IP アドレスを指定します。
サーバのポート番号	LAN 側のサーバに転送するポート番号を、1～65535 までの番号で指定します。 指定しない場合は「開始ポート番号」「終了ポート番号」と同じポート番号となります。 指定した場合は「サーバのポート番号」1 つだけとなります。
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。
外部からのアクセス	WAN 側からのサーバへのアクセスを許可するポリシーを設定します。 ［全て許可する］、［FORWARD フィルタリングに従う］から選択します。

5. ［設定］ボタンをクリックすると、「バーチャルサーバ」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「バーチャルサーバ」のリストのページに戻ります。

! 外部からのアクセス設定で「FORWARD フィルタリングに従う」を選択した場合、［サーバのポート番号］で「FORWARD フィルタリング」を設定してください。

8-5. DMZ

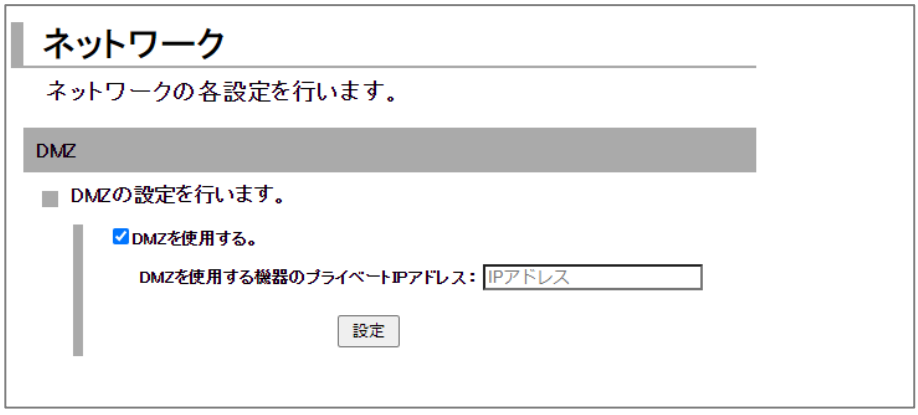
【DMZ 機能について】
DMZ 機能は、バーチャルサーバ機能と同様、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能ですが、ポート番号が不明な場合でも設定できます。
ポート番号が特定できない通信を行いたい場合などに最適な設定です。ただし、以下の点にご注意願います。

- DRX では、DMZ として設定できる機器は一台のみとなります。
- DMZ として設定された機器には、フィルタリングの設定が全く適用されなくなり、セキュリティが弱くなるため、DMZ として設定された機器にてセキュリティ設定をする必要があります。

➲ フィルタリングの設定については、『8-3. フィルタリング』をご覧ください。

- DMZ 機能はバーチャルサーバと同時に使用することはできません。

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



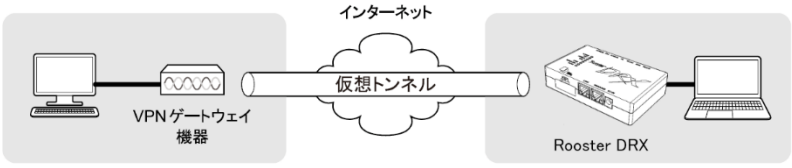
2. DMZ を使用する場合、［DMZ を使用する］チェックをオンにします。

3. ［DMZ を使用する機器のプライベート IP アドレス］に、DMZ として設定する機器のプライベート IP アドレスを入力します。

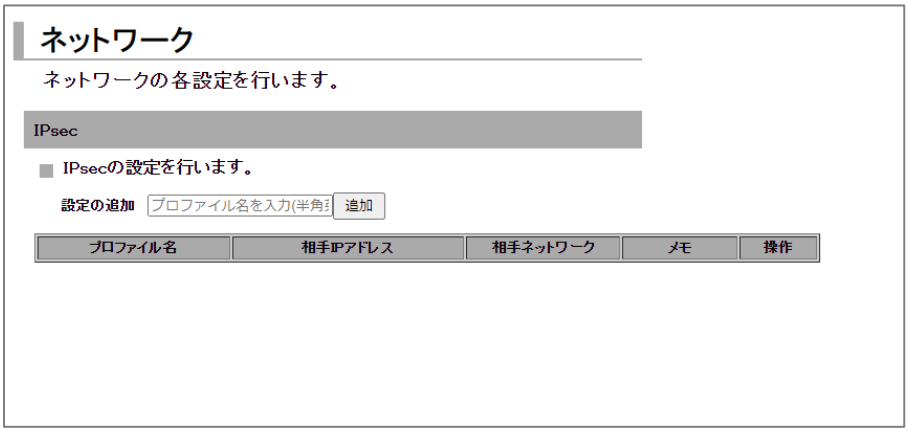
4. ［設定］ボタンをクリックして、設定内容を反映させます。

8-6. 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。

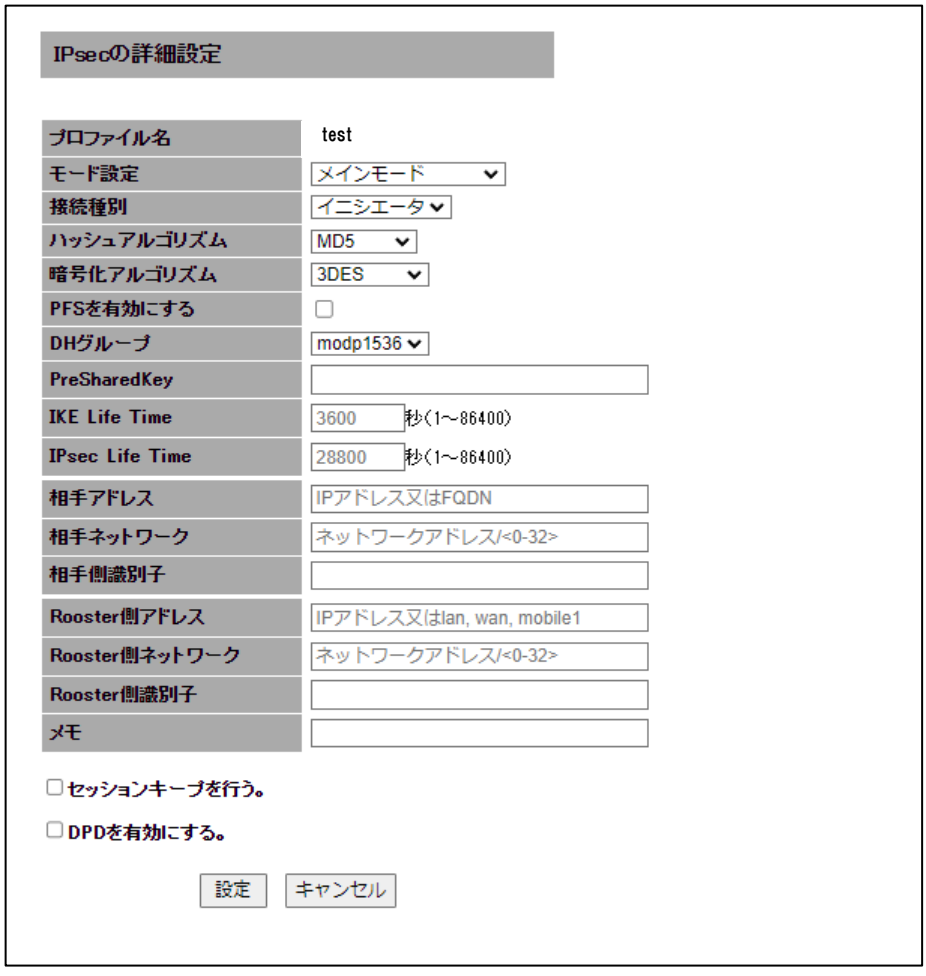


2．IPsec の設定を追加する場合は、［設定の追加］にて［プロファイル名］を入力し［追加］ボタンをクリックします。［プロファイル名］は英数文字 16 文字以下で入力ください。数字だけのプロファイル名は無効となります。
設定済みの項目を変更する場合は、［変更］をクリックします。
［削除］をクリックすると、表示されている設定が削除されます。

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

IPsec の設定は最大 16 件まで行えます。

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。



4．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が表示されます。
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。
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］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。
IKE Life Time	IKE の寿命を秒単位で指定します。 ▶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。 ▶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。 0.0.0.0 を設定した場合、「自動」となります。 また、以下に示すネットワークインタフェー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。
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「interval:30 秒、timeout:120 秒」に設定されます。

5．［設定］ボタンをクリックして、設定内容を反映させます。
「IPsec」リストのページに戻ると、設定した内容が反映されています。
［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「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。
- Rooster 側 IP アドレスを 0.0.0.0 に設定した場合、モバイルなどのインタフェースが UP したときに IPsec サービスを再起動します。そのため接続中の IPsec セッションは一旦切断されます。
- モバイル通信端末の通信モード設定で ECM モードから MBIM モードに切り替えて使用される場合、実運用に適用する前に MBIM モード設定で IPsec の動作検証を行う事をお勧めします。詳細は『４章モバイル通信端末の設定』を参照ください。

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
- 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、この組み合わせを利用する場合はアドバンスドモードで IKEv2 に設定してください。

8-6-1. IPsec通信の接続／切断方法

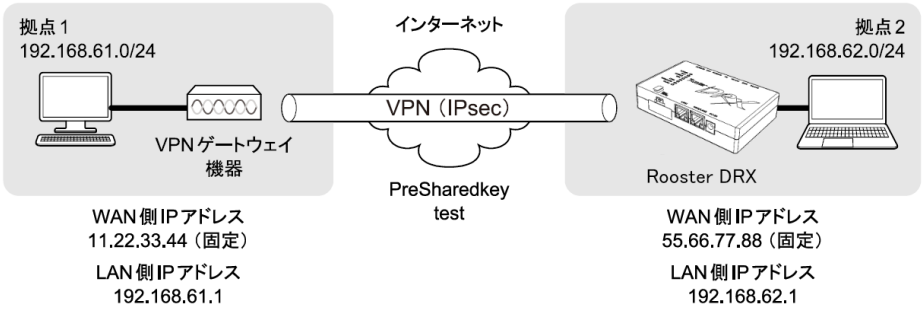
1. 設定ツールのメニューから、［ステータス］－［IPsec］をクリックします。
   IPsec ステータスのページが表示されます。

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。

ステータス一覧

ステータス表示	状態	VPN ランプの状態
無効	IPsec 設定が無効になっています。	消灯
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

8-6-2. 2点間のWAN側IPアドレスが固定の場合



DRXの設定例

IPsecの詳細設定

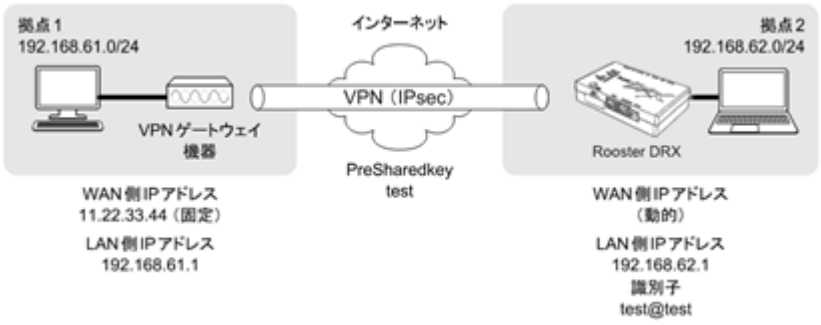
プロファイル名	test1
モード設定	メインモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	3DES
PFSを有効にする。	☑
DHグループ	modp1536
PreSharedKey	test
IKE Life Time	3600 秒(1～86400)
IPsec Life Time	28800 秒(1～86400)
相手アドレス	11.22.33.44
相手ネットワーク	192.168.61.0/24
相手側識別子	11.22.33.44
Rooster側アドレス	55.66.77.88
Rooster側ネットワーク	192.168.62.0/24
Rooster側識別子	55.66.77.88
メモ	

☐ セッションキーブを行う。

☐ DPDを有効にする。

設定 キャンセル

8-6-3. WAN側IPアドレスの一方が固定、DRXが動的の場合



DRXの設定例

IPsecの詳細設定

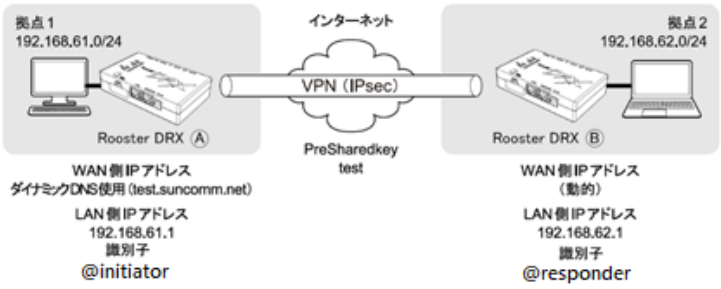
プロファイル名	test2
モード設定	アグレッシブモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	3DES
PFSを有効にする。	☑
DHグループ	modp1536
PreSharedKey	test
IKE Life Time	3600 秒(1～86400)
IPsec Life Time	28800 秒(1～86400)
相手アドレス	11.22.33.44
相手ネットワーク	192.168.61.0/24
相手側識別子	11.22.33.44
Rooster側アドレス	wan
Rooster側ネットワーク	192.168.62.0/24
Rooster側識別子	test@test
メモ	

☐ セッションキープを行う。

☐ DPDを有効にする。

設定 キャンセル

8-6-4. DRX同士で、ダイナミックDNSを利用した場合



DRX Ⓐの設定例

IPsecの詳細設定

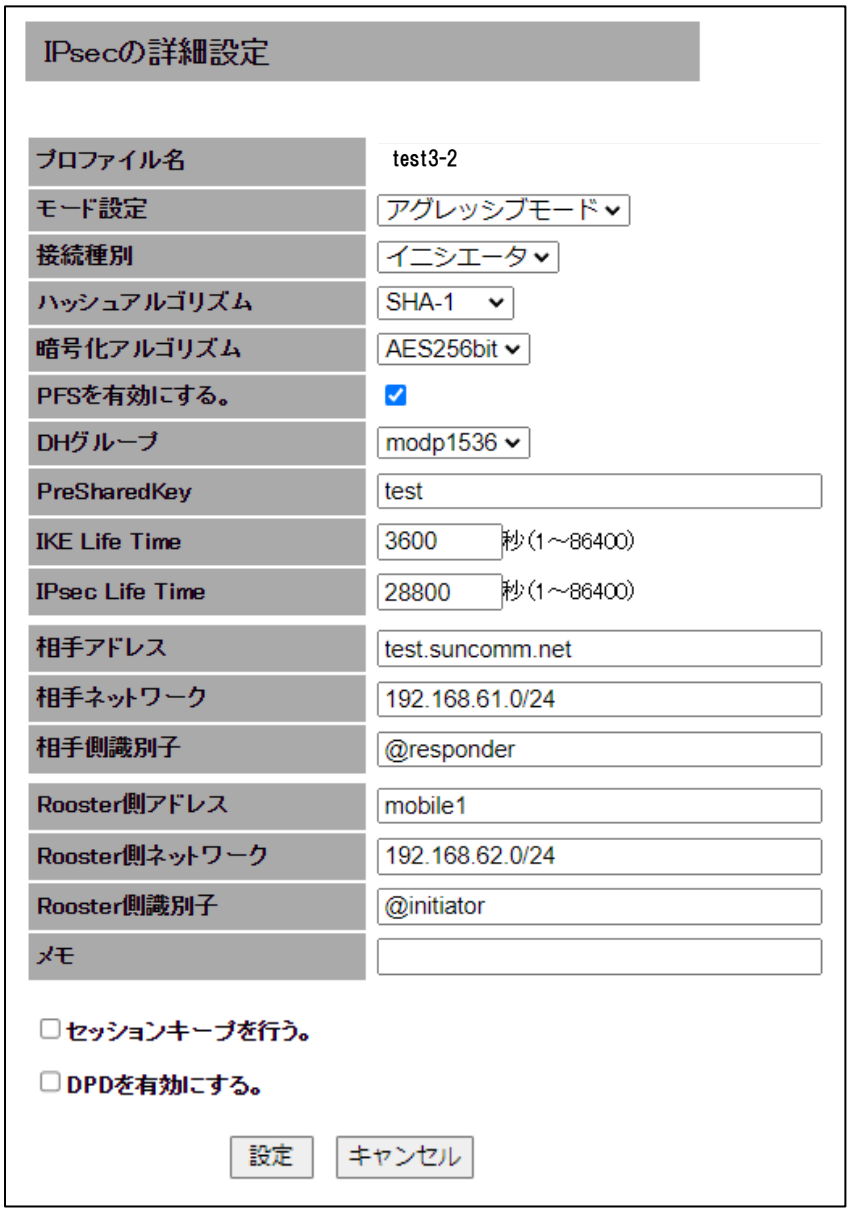
プロファイル名	test3-1
モード設定	アグレッシブモード
接続種別	レスポンダ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	AES256bit
PFSを有効にする。	☑
DHグループ	modp1536
PreSharedKey	test
IKE Life Time	3600 秒(1～86400)
IPsec Life Time	28800 秒(1～86400)
相手アドレス	0.0.0.0
相手ネットワーク	192.168.62.0/24
相手側識別子	@initiator
Rooster側アドレス	mobile1
Rooster側ネットワーク	192.168.61.0/24
Rooster側識別子	@responder
メモ	

☐ セッションキーブを行う。

☐ DPDを有効にする。

設定 キャンセル

DRX Ⓑの設定例

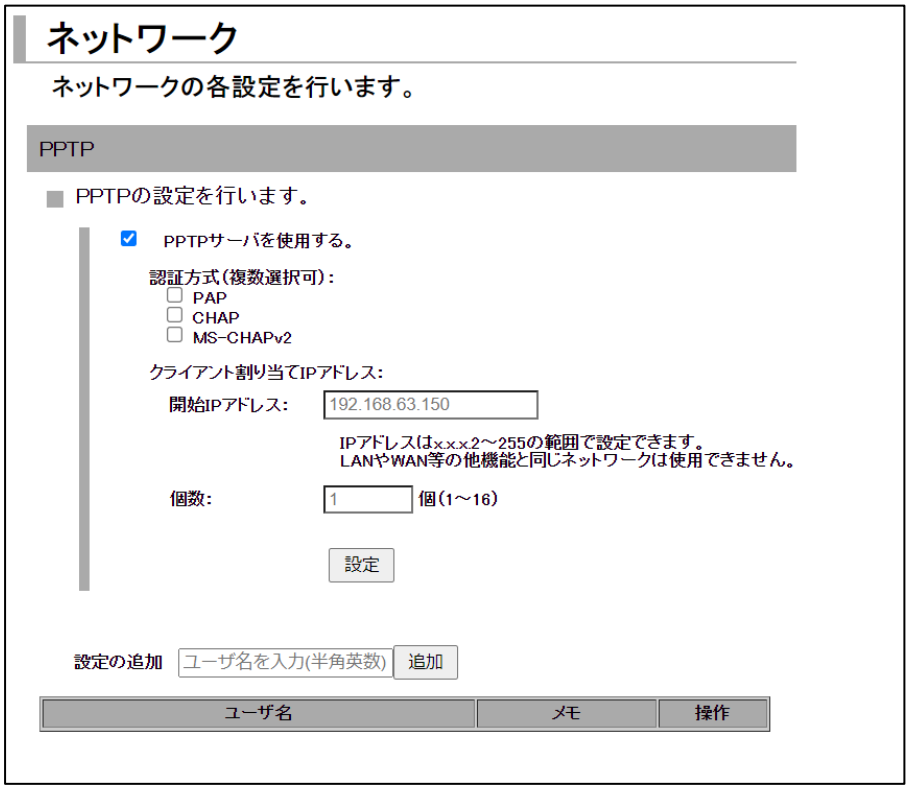


- モバイル回線をレスポンダとして使用する場合、イニシエータ側に WAN ハートビートでレスポンダの IP を監視し、無応答の動作は「本体」「モバイル通信端末」リセットを設定してください。

8-7. PPTP

【PPTP について】
PPTP は暗号通信のためのプロトコルです。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。

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



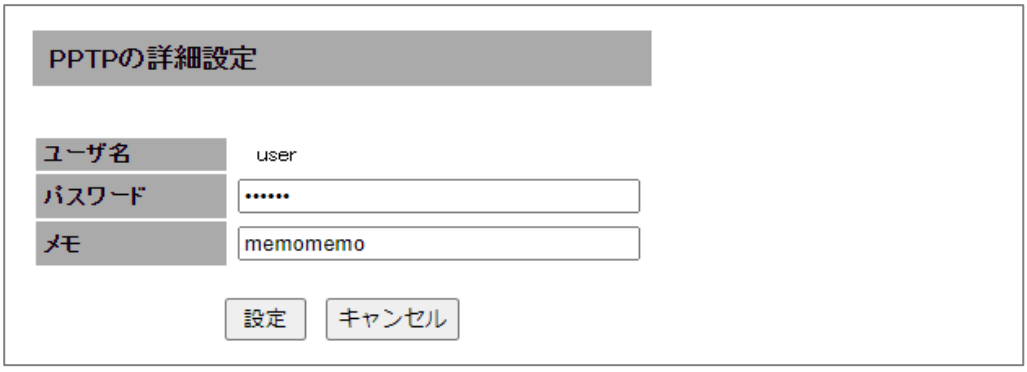
2. 以下の設定を行います。

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）
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い IP アドレスを設定します。 • 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。 • 個数 PPTP で使用する、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。 ▶［開始 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。 ▶第 4 オクテット目は 1 が使用できません。 2 以降を設定ください。
個数	IP アドレスの個数を設定します。 設定範囲：1～16

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。［ユーザ名］は英数文字で入力ください。
設定済みの項目を変更する場合は、［変更］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。

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

> memo PPTP の設定は最大 16 件まで行えます。



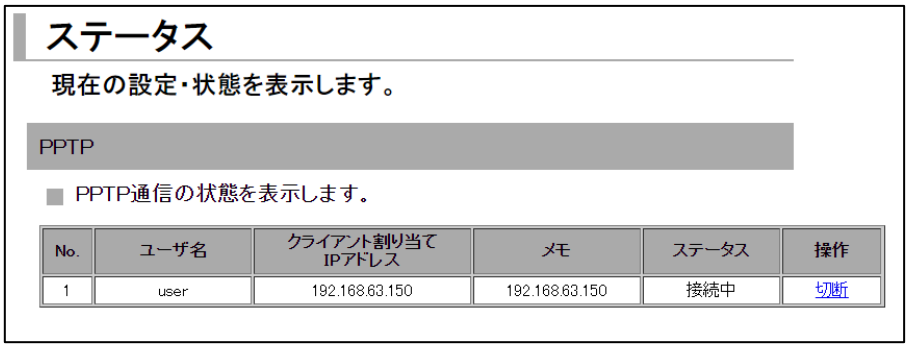
5. 以下の設定を行います。

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。 ➲ パスワードは『2-7.入力できない記号一覧』をご確認の上、設定してください。
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. ［設定］ボタンをクリックすると、「PPTP」リストのページに戻り、設定した内容が反映されます。
［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「PPTP」のリストのページに戻ります。

8-7-1. PPTP通信のステータス表示

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

同一グローバル IP 上の複数クライアントから PPTP 接続された場合、クライアント割り当て IP アドレスが正しく表示されない場合があります。

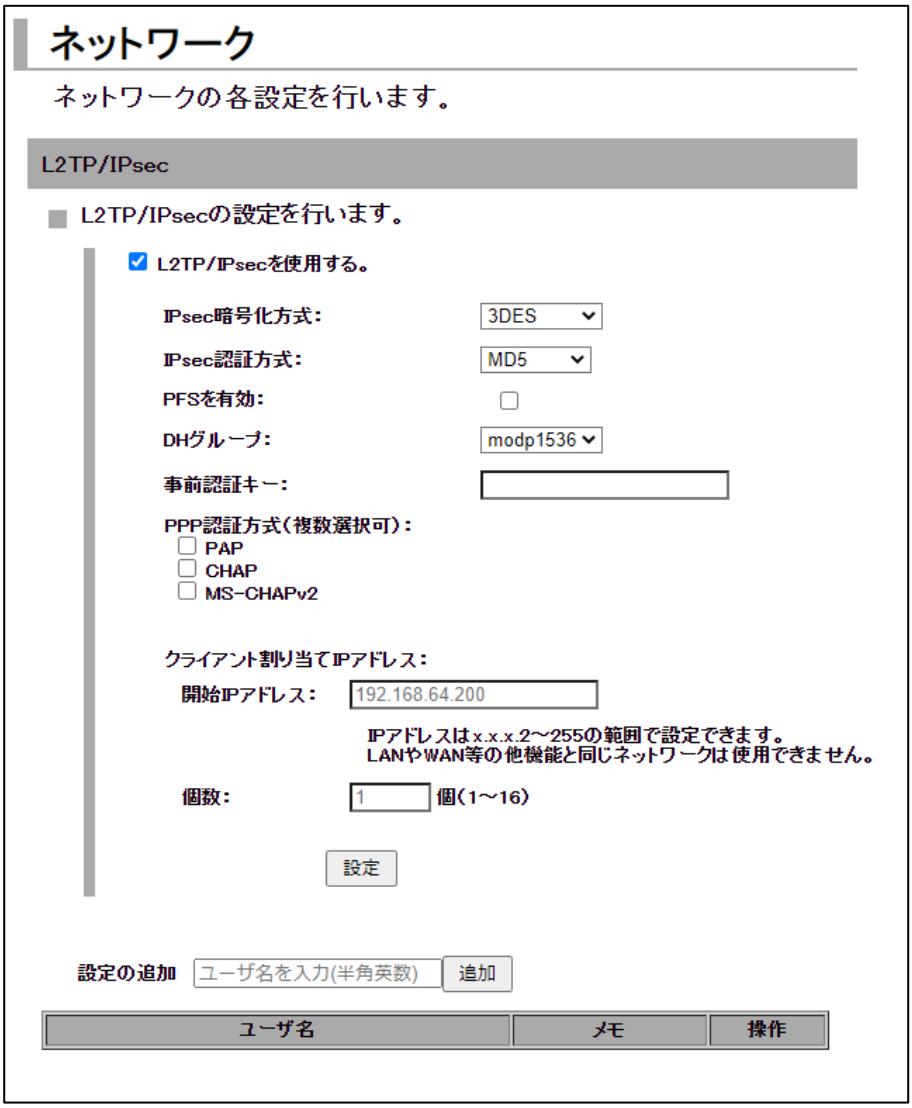
PPTP 接続から DRX へのアクセスは、［クライアント割り当て IP アドレス］の第 4 オクテット目が 1 の IP アドレスになります。
（192.168.63.150 の場合、192.168.63.1）

8-8. 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/）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。

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



2. 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。

3. 以下の設定を行います。

項目	内容
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］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。
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。）
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い IP アドレスを設定します。 • 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。 • 個数 L2TP/IPsec で使用する、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。 ▶［開始 IP アドレス］を「192.167.64.200」、［個数］を「10」と設定した場合、「192.168.64.200～192.168.64.209」が、L2TP/IPsec で使用する IP アドレスの範囲となります。 ▶第 4 オクテット目は 1 が使用できません。2 以降を設定ください。

5. L2TP/IPsec 設定の追加を行いたい場合は、［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。［ユーザ名］は英数文字で入力ください。
設定済みの項目を変更する場合は、［変更］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. ［追加］ボタン、または［変更］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。

memo L2TP/IPsec の設定は最大 16 件まで行えます。

5. 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。 ➲ パスワードは『2-7.入力できない記号一覧』をご確認の上、設定してください。
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. ［設定］ボタンをクリックすると、「L2TP/IPsec」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「L2TP/IPsec」のリストのページに戻ります。

8-8-1. L2TP/IPsec通信のステータス表示

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

L2TP/IPsec 接続から DRX へのアクセスは、［クライアント割り当て IP アドレス］の第 4 オクテット目が 1 の IP アドレスになります。
（192.168.64.200 の場合、192.168.64.1）

9章　ログの参照方法

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。

memo
・DRX 起動時に、回線ログ、サービスログ、その他のログに、下記ログが出力されます。
「-----------------system started---」
・本章で紹介するログの参照方法の他に、全てのログを一括でパソコンにアップロードする方法があります。詳細は「Rooster DRX CLI 設定機能説明書」の upload コマンドをご覧ください。

9-1. パケット通信ログ

工場出荷時状態では、DRX への負荷を軽減させるため、パケット通信ログは記録しない設定になっています。
パケット通信ログを記録させる場合は、［ログ管理］の設定で「パケット通過ログを記録する」、または「パケット遮断ログを記録する」のチェックをオンに設定してください。

➲ 設定方法は、『7-5. ログ管理』をご覧ください。

9-1-1. パケット通過ログ

1. 設定ツールのメニューから、［ログ］－［パケット通信ログ］ －［通過ログ］をクリックします。
パケット通過ログ一覧のページが表示されます。

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	結果
1	2021/07/01 10:30:16	ICMP	192.168.62.200	0	[redacted]	0	終了
2	2021/07/01 10:30:17	ICMP	[redacted]	0	192.168.62.200	0	終了
3	2021/07/01 10:30:19	ICMP	192.168.62.200	0	[redacted]	0	終了
4	2021/07/01 10:30:19	ICMP	[redacted]	0	192.168.62.200	0	終了
5	2021/07/01 10:30:20	ICMP	192.168.62.200	0	[redacted]	0	終了
6	2021/07/01 10:30:20	ICMP	[redacted]	0	192.168.62.200	0	終了
7	2021/07/01 10:30:20	ICMP	192.168.62.200	0	[redacted]	0	終了
8	2021/07/01 10:30:20	ICMP	[redacted]	0	192.168.62.200	0	終了
9	2021/07/01 10:30:21	ICMP	192.168.62.200	0	[redacted]	0	終了
10	2021/07/01 10:30:21	ICMP	[redacted]	0	192.168.62.200	0	終了

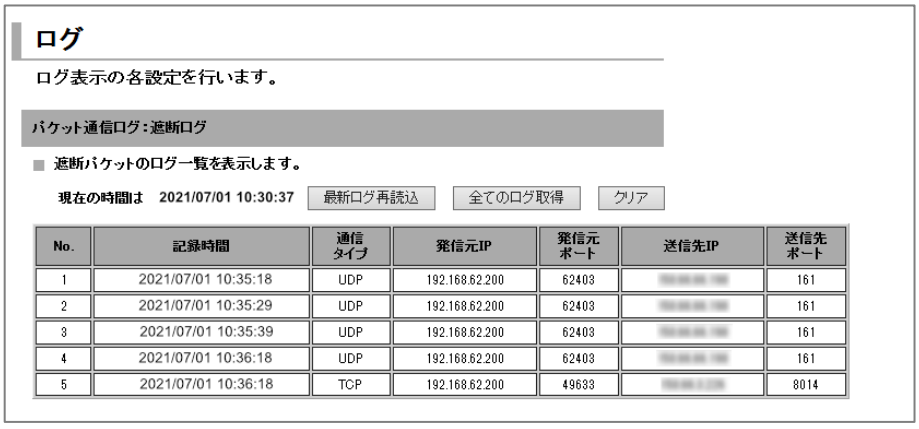
項目	内容
No.	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。DRX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
通信タイプ	IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
発信元 IP	通信の起点になる機器の IP アドレスが表示されます。
発信元ポート	通信の起点になる機器の使用ポート番号が表示されます。
送信先 IP	通信の宛先になる機器の IP アドレスが表示されます。

項目	内容
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。 • 「終了」 正常に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。

通過ログでは、フィルタリングで設定したセッションに関連した通信は出力されません。例えば FTP の制御セッション（TCP21 番）をフィルタリングで許可した場合、制御セッションの通信は通過ログに出力されますが、制御セッションに関連したデータセッション（TCP20 番）の通信は出力されません。

9-1-2. パケット遮断ログ

1. 設定ツールのメニューから、［ログ］－［パケット通信ログ］－［遮断ログ］をクリックします。
   パケット遮断ログ一覧のページが表示されます。



No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート
1	2021/07/01 10:35:18	UDP	192.168.62.200	62403	[redacted]	161
2	2021/07/01 10:35:29	UDP	192.168.62.200	62403	[redacted]	161
3	2021/07/01 10:35:39	UDP	192.168.62.200	62403	[redacted]	161
4	2021/07/01 10:36:18	UDP	192.168.62.200	62403	[redacted]	161
5	2021/07/01 10:36:18	TCP	192.168.62.200	49633	[redacted]	8014

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。

9-2. 回線ログ

9-2-1. 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］－［回線ログ］－［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。

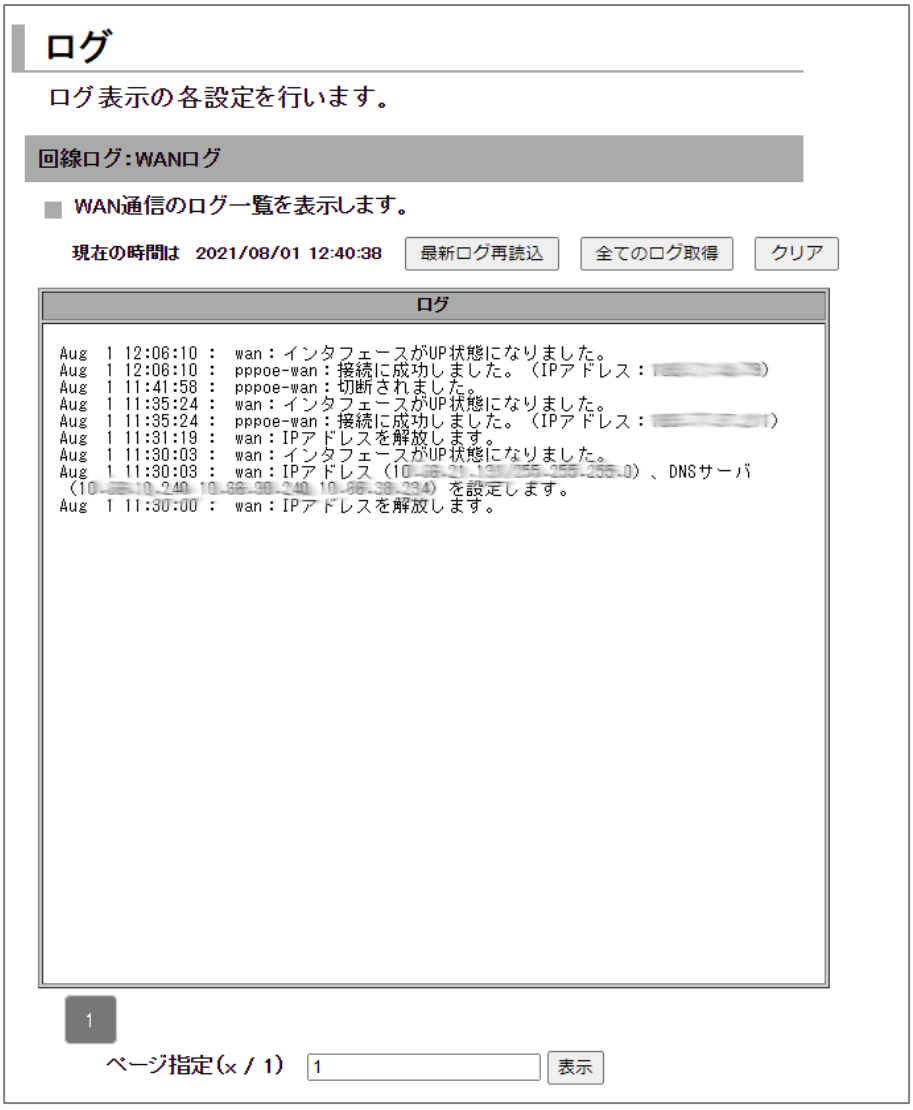
9-2-2. 無線LANログ DRX5010

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［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。

9-2-3. WANログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［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。

9-2-4. IPsecログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［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。 IPsec 接続が成功すると、「IPsec が接続完了しました」と表示されます。 接続できない場合、IPsec の設定に誤りがないかどうかご確認ください。 ➲ IPsec の設定につきましては、『8-6. IPsec』をご覧ください。

9-2-5. PPTPログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［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
記録時間とログ	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。

9-2-6. L2TP/IPsecログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［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
記録時間とログ	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。

9-3. サービスログ

9-3-1. アドレス解決ログ

1. 設定ツールのメニューから［ログ］－［サービスログ］－［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
記録時間とログ	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。 アドレス解決機能の動作状態が表示されます。 「アドレス解決プロセスは異常終了しました」となる場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。
	【アドレス解決をメール送信で行っている場合】 • 「SMTP メールサーバ設定内容に異常があります」 メールアカウント設定にいずれかが未登録の時に表示されます。 • 「デフォルトゲートウェイがありません:」 デフォルトゲートウェイが設定されていない場合に表示されます。 • 「WAN が接続されました」 WAN'が接続された時に表示されます。 • 「モバイル通信端末'が接続されました」 モバイル通信端末'が接続された時に表示されます。 • 「現在の IP (xxx.xxx.xxx.xxx) をメールでユーザ認証(SMTP)にて送信します」 メール送信前に表示されます。 • 「メール送信に失敗しました:」 メール送信失敗した時に表示されます。
	【アドレス解決を suncomm.DDNS で行っている場合】 • 「suncomm.DDNS サーバエラー」 suncomm.DDNS の設定に誤りがある場合に表示されます。

9-3-2. DHCPログ

1. 設定ツールのメニューから、［ログ］－［サービスログ］－［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
記録時間とログ	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。

9-3-3. WANハートビートログ

1. 設定ツールのメニューから、［ログ］–［サービスログ］–［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
記録時間とログ	ログの発生した時刻と、WAN ハートビート機能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。

9-3-4. PPPログ

1. 設定ツールのメニューから、［ログ］–［サービスログ］–［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
記録時間とログ	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。

9-3-5. SunDMSログ

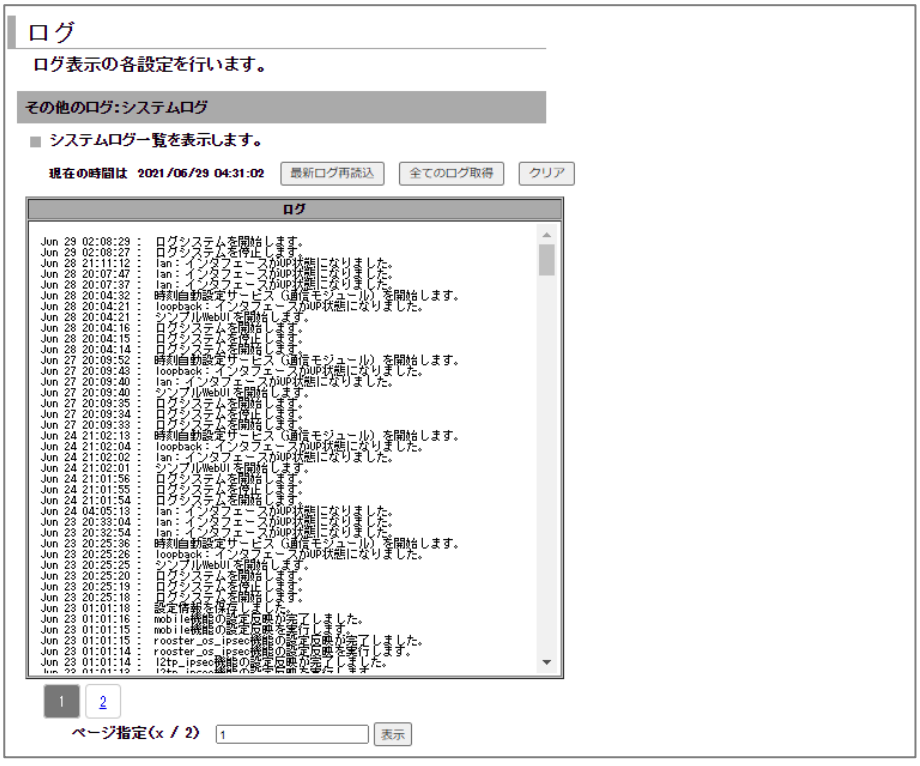
1. 設定ツールのメニューから、［ログ］－［サービスログ］－［SunDMS ログ］をクリックします。
   SunDMS ログ一覧のページが表示されます。

項目	内容
記録時間とログ	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。

9-4. その他ログ

9-4-1. システムログ

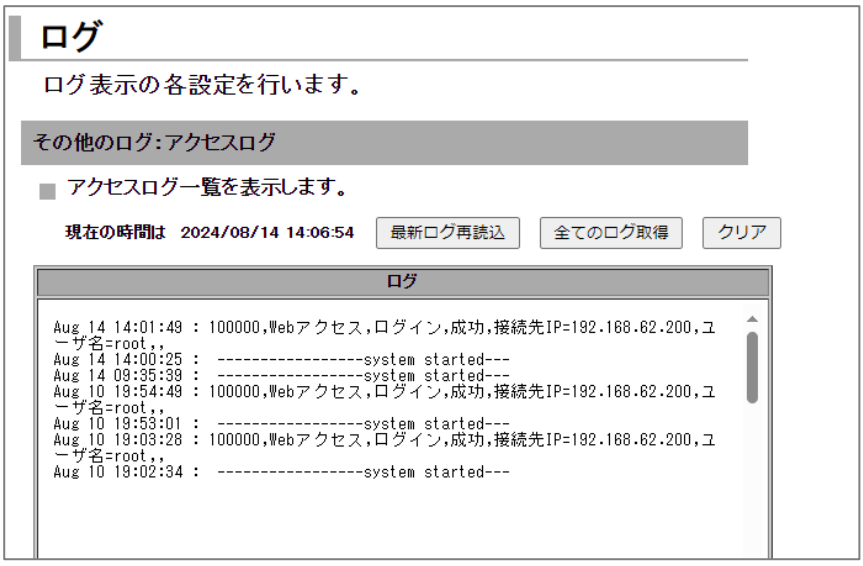
1. 設定ツールのメニューから、［ログ］－［その他ログ］－［システムログ］をクリックします。
   システムログ一覧のページが表示されます。



項目	内容
記録時間とログ	ログの発生した時刻と、DRX のシステムに関するログが表示されます。 上に行くほど、より新しいログとなります。

9-4-2. アクセスログ

1. 設定ツールのメニューから、［ログ］－［その他ログ］－［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
記録時間とログ	ログの発生した時刻と、DRX へのアクセスに関するログが表示されます。 上に行くほど、より新しいログとなります。 ログフォーマットはコンマ区切りで、各列の内容は下記アクセスログフォーマットとなります。

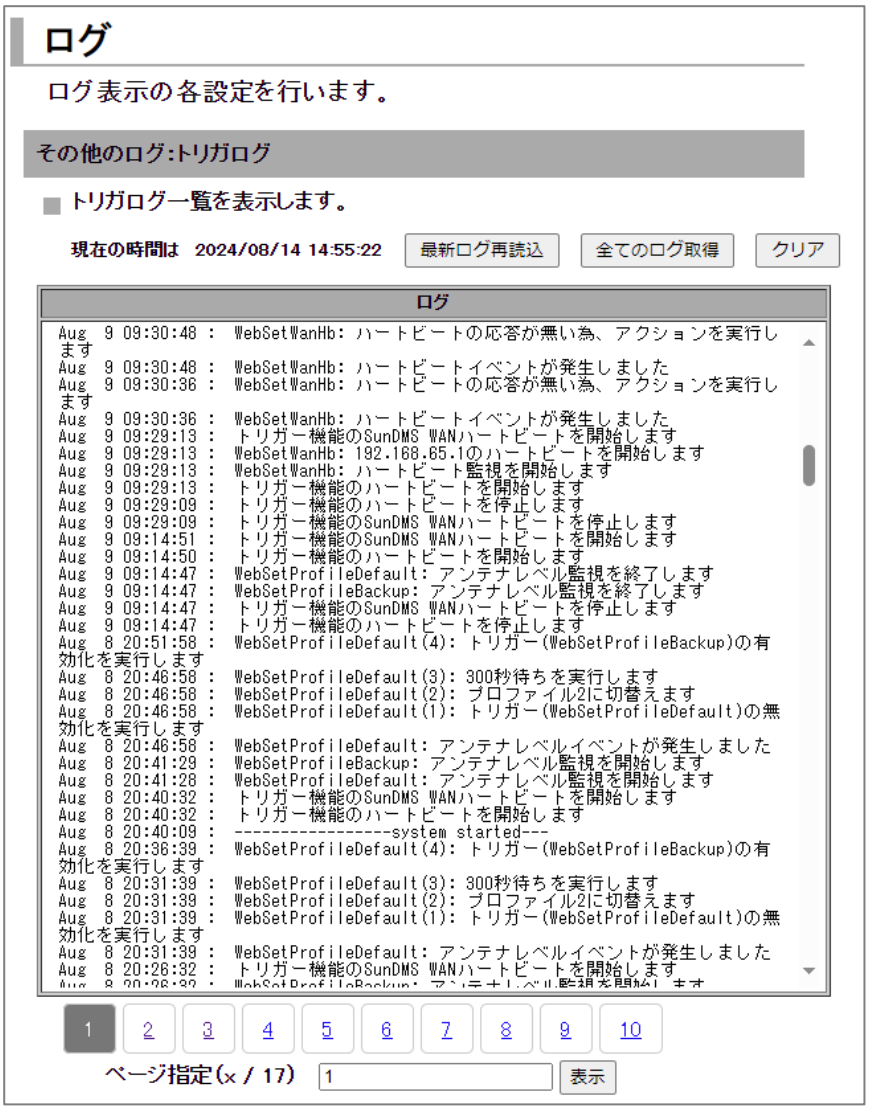
アクセスログフォーマット

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 【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） 【その他 将来拡張用】	
2	処理内容	（Web 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	

※現 FW バージョンでは WebUI のログインのみの対応となります。将来 FWUPDATE にて CLI などにて対応していきます。

9-4-3. トリガログ

1. 設定ツールのメニューから、［ログ］－［その他ログ］－［トリガログ］をクリックします。
   トリガログ一覧のページが表示されます。



項目	内容
記録時間とログ	ログの発生した時刻と、DRX のトリガ設定の動作状況に関するログが表示されます。 上に行くほど、より新しいログとなります。

10章 その他 実行可能な機能

この章では､本マニュアルに記載されているシンプルモード Web 設定ツールでは実行できない機能について説明しています。

実行可能な機能一覧

CLI、アドバンスモード WebUI からでのみ実行できる機能があります。

以下がその機能の一覧となります。

- TFTP/FTP を利用した設定ファイルのアップデート
- TFTP/FTP を利用したログファイルのアップロード
- モバイル通信モジュールのリセット
- 電話番号の表示
- IMEI（モバイル通信モジュール製品番号）の表示
- アンテナレベルの表示
- モバイル通信端末 電波周波数の表示
- モバイル通信端末情報一覧の表示
- PING の実行
- 本製品のシリアル番号表示
- ARP キャッシュ表示
- 現在の設定一覧表示
- 温度センサの温度表示
- 電源電圧の電圧表示
- NTP の状態表示
- ルーティングの状態表示
- DNS による名前解決の表示
- 各機能にて詳細機能の設定
- トリガ機能の設定、状態表示

memo

➔ アドバンスドモードの詳細は『7-4-1. アドバンスドモード』をご覧ください。

機能の詳細は『RoosterDRX アドバンスモード Web 設定機能説明書』､『Rooster DRX CLI 設定機能説明書』をご覧ください。

付録

製品仕様

品名		DRX5010　（上段）
		DRX5002　（下段）
コード		11S-DRX5010
		11S-DRX5002
JAN コード		4907940130728
		4907940130742
対応回線	モバイルデータ通信	LTE (NTT ドコモ、KDDI、ソフトバンク)
	各種ブロードバンド回線	○
対応 UIM カード		nanoSIM×2
インタフェース	イーサネット	1000BASE-T / 100BASE-TX /10BASE-T×2 ポート （MDI/MDI-X 自動判別　全 2 重）
	アンテナコネクタ	SMA×2
	無線インタフェース	B1(1920~1980MHz(UL)、2110~2170MHz(DL))
		B8(880~915MHz(UL)、925~960MHz(DL))
		B18(815~830MHz(UL)、860~875MHz(DL))
		B19(830~845MHz(UL)、875~890MHz(DL))
		B39(1880~1920MHz(UL)、1880~1920MHz(DL))
無線 LAN インタフェース DRX5010	対応周波数	2.4GHz 帯 5GHz 帯(切り替え)
	通信規格	IEEE.802.11a/b/g/n/ac
	動作モード	アクセスポイント （※最大接続可能無線 LAN 端末数：20 台）
	帯域幅	シングル、デュアル、クワッドチャンネル
	アンテナコネクタ	SMA レセプタクル リバースタイプ ×2
ハードウェア	モバイル通信モジュール	AM Co.,Ltd「AMM574」
	CPU	main:NXP LS1012A(600MHz)
		sub:Renesas R5F10(8MHz)
	メインメモリ	512MB（DDR3）
	フラッシュメモリ	NOR-Flash:4MB(ブート)
		NAND-Flash:512MB(システム、ログ)
	LED	7 個（赤/緑 1 個、緑 6 個） DRX5010
		6 個（赤/緑 1 個、緑 5 個） DRX5002
	DIP スイッチ	2 ビット 1 個
	Push スイッチ	2 個 (初期化、シャットダウン)
	温度センサ	ケース内 1 系統
	電圧センサ	DCIN 電圧 1 系統
	内蔵アンテナ	LTE 用アンテナ ×2

電源	入力電圧	DC 5~27.4V (±5%)
	消費電流	待受時：約 300mA(DC12V) 通信時：約 450mA(DC12V) DRX5010 約 380mA(DC12V) DRX5002 通信時最大：約 800mA(DC12V)
	消費電力	12W(最大)／7W(平均)／0.8W(おやすみモード) DRX5010
		12W(最大)／5W(平均)／0.8W(おやすみモード) DRX5002
	リップル	100mVp-p 以下
	コネクタ	丸型 DC 電源ジャック(中心+極)　外径 5.5mm　内径 2.1mm
環境条件	動作温度	-20～65℃
	動作湿度	25～85%（結露なきこと）
	保存温度	-20～80℃
	保存湿度	25～85%（結露なきこと）
	耐ノイズ性　※1	
	AC ラインノイズ	±2000V パルス幅 100ns/1000ns
	DC ラインノイズ	±2000V パルス幅 100ns/1000ns
	耐静電気性　※1	
	接触放電	±10kV（LAN/WAN コネクタ外周部に印加）
	気中放電	±10kV（LAN/WAN コネクタ外周部に印加）（アンテナコネクタを除く）
	振動条件	装置単体において、加速度 19.6m/s²（2g）、振動周波数 30～100Hz の振動（1 掃引時間 20 分）を上下/左右/前後に加えた後に、各部の損傷、部品などに脱落がなく、機能・性能に問題ないこと
重量		約 250g（本体のみ） DRX5010
		約 240g（本体のみ） DRX5002
外形寸法		約 128(W) × 81(D) ×29 (H)　単位 mm （突起部、取付金具除く）
材質	ケース	PC 樹脂
	下面	鋼板
サポートプロトコル	Ethernet	CSMA/CD
	ルーティング	IPv4
	認証	PAP、CHAP、MS-CHAP、MS-CHAPv2
	WAN プロトコル	PPP
	管理プロトコル	SNMPv2 ※4
DHCP	サーバ	LAN 側最大 253 クライアント （DNS サーバ IP 指定、リース時間設定可）
	クライアント	有線接続
アドレス変換		NAT/IP マスカレード、DNAT、SNAT
VPN パススルー		IPsec、PPTP
サーバ公開		バーチャルサーバ (最大 32 件設定可) DMZ ホスト（1 件設定可）
スタティックルーティングテーブル		最大 128 件登録可能
アップデート		WWW ブラウザによるアップデート SSH によるアップデート (ftp/tftp サーバからダウンロード) SunDMS によるアップデート

ダイナミック DNS		SunDMS（suncomm.DDNS）※2
アドレス解決	インタフェース指定	○
	アドレス登録	1 件
	プロトコル	SMTP
	更新時間設定	可能（5 分～）
	e-mail 送信	○
WAN ハートビート 相手先		任意のアドレス/FQDN 設定可能
WAN ハートビート 送信間隔		可能(1 分~)
電源制御		ハードウェアおよびソフトウェア モバイル通信端末
ハードウェア ウォッチドッグ	信号タイミング	常時監視(1 秒毎)
	発動条件	信号不受信から 90 秒後
	発動動作	本体電源 OFF から 10 秒後に再起動
有線 WAN 接続方式		固定 IP、DHCP、PPPoE（Numbered 接続）
ダイヤルアップ自動発信条件		常時接続
回線冗長化		有線/モバイル回線での冗長化
		SIM1/SIM2 での冗長化
モバイル副回線監視		バックアップ回線の定期的な監視
Wake On(呼び起こし)		SMS 受信
モバイル通信端末情報		自局電話番号、アンテナレベル、電波強度、電波品、IMEI、ICCID、使用周波数取得
VPN（IPsec）	鍵交換プロトコル	IKEv1、v2
	暗号化	AES256bit、3DES
	認証アルゴリズム	SHA-1、SHA-256、SHA-384、SHA-512、MD5
	アルゴリズム	IKE（メインモード、アグレッシブモード）
	DH Group	modp1536、modp1024、modp2048、modp3072、modp4096、modp6144、modp8192
	接続要求	イニシエータ、レスポンダ
	接続可能数	最大 16 件
	セッションキープ設定	可能
	バックアップ設定	別装置への接続可能　※4 （1 セッションにつき 1 件）
	LifeTime 設定	可能
	NAT トラバーサル	可能
VPN（PPTP）機能	暗号化	GRE
	接続可能数	最大 16 件
	認証方式	PAP、CHAP、MS-CHAPv2
VPN （L2TPv2 サーバ）	IPsec 暗号化	AES256bit、3DES
	IPsec 認証方式	SHA-1、SHA-256、SHA-384、SHA-512、MD5
	接続可能数	最大 16 件
	PPP 認証方式	PAP、CHAP、MS-CHAPv2

ロギング		本体内蔵の不揮発性メモリへ保存、 WWW ブラウザによる各種ログ表示、 SSH による各種ログ表示、 SSH による ftp サーバへの全ログ保存、 Syslog での出力、SunDMS から取得
ログの内容		パケット通過、パケット遮断、モバイル通信端末、WAN、 アドレス解決、 WAN ハートビート、DHCP、IPsec、PPTP、 L2TP、PPP、システム、SunDMS、アクセス、トリガ 無線 LAN DRX5010
設定情報管理		WWW ブラウザによるファイル保存、読み込み SSH 上でのコマンドによる読み込み、書き込み SSH による ftp/tftp サーバからの読み込み SunDMS からの取得・保存
フィルタリング	FORWARD	128 件
	INPUT	64 件
	DNS	64 件
	MAC	○
インターネット経由のリモートセットアップ		可能 (GUI/SSH)
時刻管理	設定方法	NTP サーバ設定/ 手動設定 / モバイル通信モジュールより取得
	更新時間設定	可能（モバイル通信モジュールから取得する場合のみ）
おやすみモード		○
サン電子 IoT デバイス遠隔管理サービス SunDMS		死活監視 ファームウェア更新 再起動指示(コールドリブート) ログファイル取得/更新 電圧・温度アラート 各ステータス情報 ~~以下有償サービス~~ スタンダードサービス プライベート接続サービス
MTBF		180,000 時間 DRX5010
		230,000 時間 DRX5002
規格		JIS D 1601-1995 3 種-A 種 (自動車部品振動試験規格) VCCI クラス A
保証		1 年間
付属品		スタートアップマニュアル（保証書付き）
オプション品		外部 LTE アンテナ、AC アダプタ、固定金具　※3

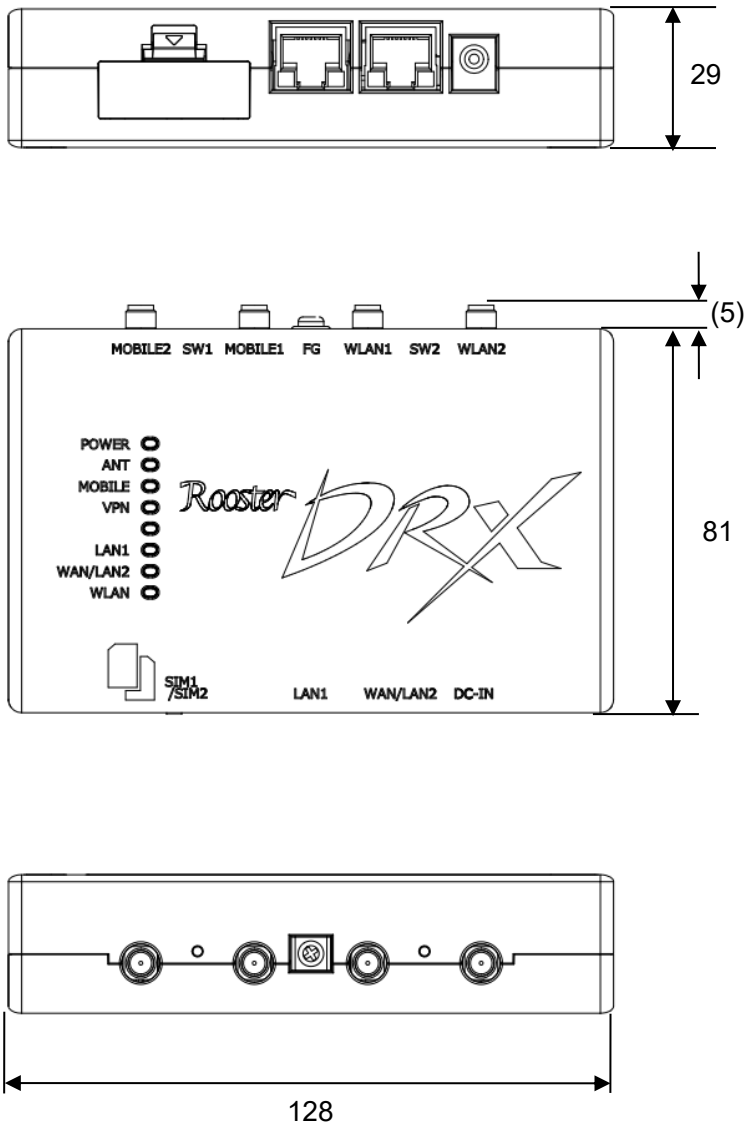
※1 表記の数値は、試験装置による試験性能値です。また、振動やノイズ、静電気を印加し続けた際の動作を保証するものではありません。

※2 弊社が運営する SunDMS 有償オプションのダイナミック DNS サービスです。

※3 ご利用にあたっては別途オプション品をご購入ください。

※4 対応予定

外形寸法



（単位 mm）　※公差含む

名称	DRX5010 / DRX5002
外形寸法	約 W128 × D81 ×H29 mm （突起部、取付金具除く）
重量	約 250g DRX5010 約 240g DRX5002

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 取扱説明書　Ver.2.6.3a

サン電子株式会社
2025 年 11 月発行　(2501030)