SUNCORPORATION

通信モジュール一体型ルータ

Rooster SC

取扱説明書

第 2.0.0 版

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

更新履歴

更新日	Rev.	更新内容
2023.06.30	1.0.0	初版
2023.07.03	1.0.1	「9 章 制限・注意事項」を追加。その他注意事項を追記。
2023.08.09	1.0.2	「9-2 定期再起動サービス機能についての制限」について FWv1.0.1.2 で修正された旨を追記。
2023.10.25	1.1.0	「WAN ハートビート機能」の追加機能の説明、「IPsec 機能」の説明を追加
2024.01.31	1.2.0	LAN インターフェース設定の追加機能の説明を追加 モバイルインターフェース設定の追加機能の説明を追加 Web 設定ツール設定、CLI (SSH Server)設定、DNS フィルター機能の説明を新規作成
2024.04.30	1.3.0	「WAN ハートビート機能」の追加機能の説明を追加 「ユーザーログ機能」の説明を追加 「IPsec 機能」について接続設定例を追加 「IP フィルター」機能について Web 設定ツール、CLI のポート番号を変更した際の注意点を追記
2024.07.30	1.4.0	「トリガー機能」の説明を追加 「PPTP サーバ機能」の説明を追加 「L2TP/IPsec サーバ機能」の説明を追加 「GNSS 機能」の説明を追加 SE のパケット処理順序について説明を追加
2025.01.28	1.4.1	「ご使用時の取り扱いについて」文言の修正
2025.04.25	2.0.0	3-1. Web 設定ツールのログイン方法について v2.0.0.X のファームウェアに合わせて記載を修正 5-4. ファームウェアのアップデート方法について v2.0.0.X へアップデートする際の注意事項を追記 「LAN インターフェース設定」について追加機能を追記 「モバイルインターフェース設定」について追加機能を追記 「IPsec」機能について追加機能を追記、IKEv1 アグレッシブモード使用時の注意を追記 9 章 Rooster SE の破棄方法を追加

はじめに

この度は 弊社 SE をご使用頂き、誠にありがとうございます。
本取扱説明書では、SE の取扱方法および諸注意をまとめておりますので、正確・安全なご使用のため、ご使用前に必ずご一読頂けますようお願い致します。

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。
memo	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、「SE220」を「本製品」または「SE」と省略して記載しております。

商標について

「Rooster」および「Rooster」ロゴは、サン電子株式会社の登録商標です。
「SunDMS」は、サン電子株式会社の登録商標です。
「docomo」は、NTT ドコモの商標または登録商標です。
「Softbank」および「ソフトバンク」の名称、ロゴは日本国およびその他の国におけるソフトバンクグループ株式会社の登録商標または商標です。
「au」は、KDDI 株式会社の商標または登録商標です。
「4G LTE」は、国際電気通信連合(ITU)が LTE を「4G」と呼称することを認めた声明に準じております。
「Windows」は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
「Chrome」は米国 Google LLC の商標または登録商標です。
「イーサネット」は富士フイルムビジネスイノベーション株式会社の登録商標です。
その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。
本文中の各社の商標または登録商標には、TM、®マークは表示しておりません。

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）

本書ではお使いになる人や他の人への危害、財産への損害を未然に防止するため、必ずお守りいただくことを、次のように説明しています。

■表示内容を無視して誤った使い方をしたときに使用者や他の人に生じる危害や損害の程度を次の表示で区分しています。

 警 告	この表示は、死亡または重症を負う危険性が想定される内容を表示しています。
 注 意	この表示は、障害を負う可能性及び物的損害の発生が想定される場合を表しています。

■本文中で使われている図記号の意味は次の通りです。

	禁止することを示します。 具体的な内容が図中に示されます。
	注意することを示します。 具体的な内容が図中に示されます。
	指示・強制することを示します。 具体的な内容が図中に示されます。

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、本装置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、本体一体型の取り付け部にネジを使用して固定してください。
他の取り付け金具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。

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。ただし本装置の使用については、各医療機関の指示に従うようにしてください。

- 本装置を医用電気機器に密着して使用しないでください。
- 本装置を病室、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、本装置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、治療室には本装置を持ち込まないでください。

強制

本装置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、事前に本装置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-20～70℃、湿度は 25～85%の範囲でご使用ください。
- 使用中、本装置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、本装置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、本装置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。
- 本装置に貼付してある銘版シール（製造番号等印字シール）を剥がさないでください。

お客様が本装置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。

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ことができる装置です。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、本装置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。

電波障害自主規制（VCCI）

本製品は情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラス A 機器です。

クラス A 機器

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

目次

1章　概要

この章では、SE 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、LTE 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。

また、GNSS 対応によって位置情報を利用する事が可能になります。

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 カード挿入口に接続する必要があります。

1-2. 主な特長

通信モジュール単体で動作

従来の機種ではホスト CPU に持たせていた制御機能を通信モジュールに集約することで製品を小型化しています。

LTEマルチキャリア対応

NTT ドコモ、ソフトバンク、KDDI、各 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自由です。

２枚のnano SIM対応で冗長運用が可能

nano SIM を２枚同時に装着することで２回線に対応します。これにより１台で２キャリアの冗長化が可能となり、通信障害などが発生した場合でも他通信網に切り替え通信が途切れることを防ぎます。

（自動切り替えはファームウェアアップデートで実現）

GNSS対応

GNSS 対応により位置情報を取得することが可能です。タクシーやバスなど移動体での利用シーンに対応します。

内蔵アンテナで簡単設置

LTE アンテナが内蔵されており、別途外部アンテナを用意することなく、本製品を簡単に設置できます。電波状態の悪い環境では、外部アンテナも接続可能です。

広い入力電圧対応

下限 5V を維持したまま上限を 32V（±5%）まで引き延ばし、車載案件に対応できるようになります。

Web設定ツールによる設定

Web 設定ツールによる本製品の設定を行うことができます。

高スループットを実現

映像転送にもストレスのない高スループットを実現します。

長期安定運用（ASC)

電波状態による通信エラーなどを防ぐため、死活監視、定期リセット機能など自己復帰が可能な機能 ASC を搭載し、無線環境下でも安定運用を提供します。

SunDMS搭載

安定した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で提供します。

低消費電力

最大消費電力は 5.5 W 以下となるため低消費電力に抑えます。

コンパクトボディ

小型で場所を取らず、本体と取り付け部が一体型となっているため、購入後すぐに設置して使用することができます。

広い温度範囲

動作温度範囲を-20℃～70℃と厳しい環境下でも運用が可能です。

1-3. 設定フロー

SE を使用してインターネット接続を行う場合、 2 までの設定を行ってください。
3～4 の設定は、必要に応じて行ってください。

1. SE の設置

・同梱物の確認

➔ 『1-4. 同梱物の確認』

・機器の接続

➔ 『2-3. PC との接続方法』

・クライアント PC の設定

➔ 『2-6. パソコンの設定』

2. 導入時の設定

・ログインパスワードの設定

➔ 『3-1. Web 設定ツールのログイン方法』

➔ 『3-2. Web 設定ツールの概要』

➔ 『3-3. ログインパスワードの設定』

・モバイル通信接続の設定

➔ 『3-5. モバイルインターフェース設定』

3. メンテナンス

・ソフトウェアの更新

➔ 『5-4. ファームウェアのアップデート方法』

4. 各種設定（必要な場合のみ）

➔ 『4 章. 運用』

➔ 『5 章. メンテナンス設定』

➔ 『6 章. 各種サービス設定』

➔ 『7 章. ネットワーク設定』

1-4. 同梱物の確認

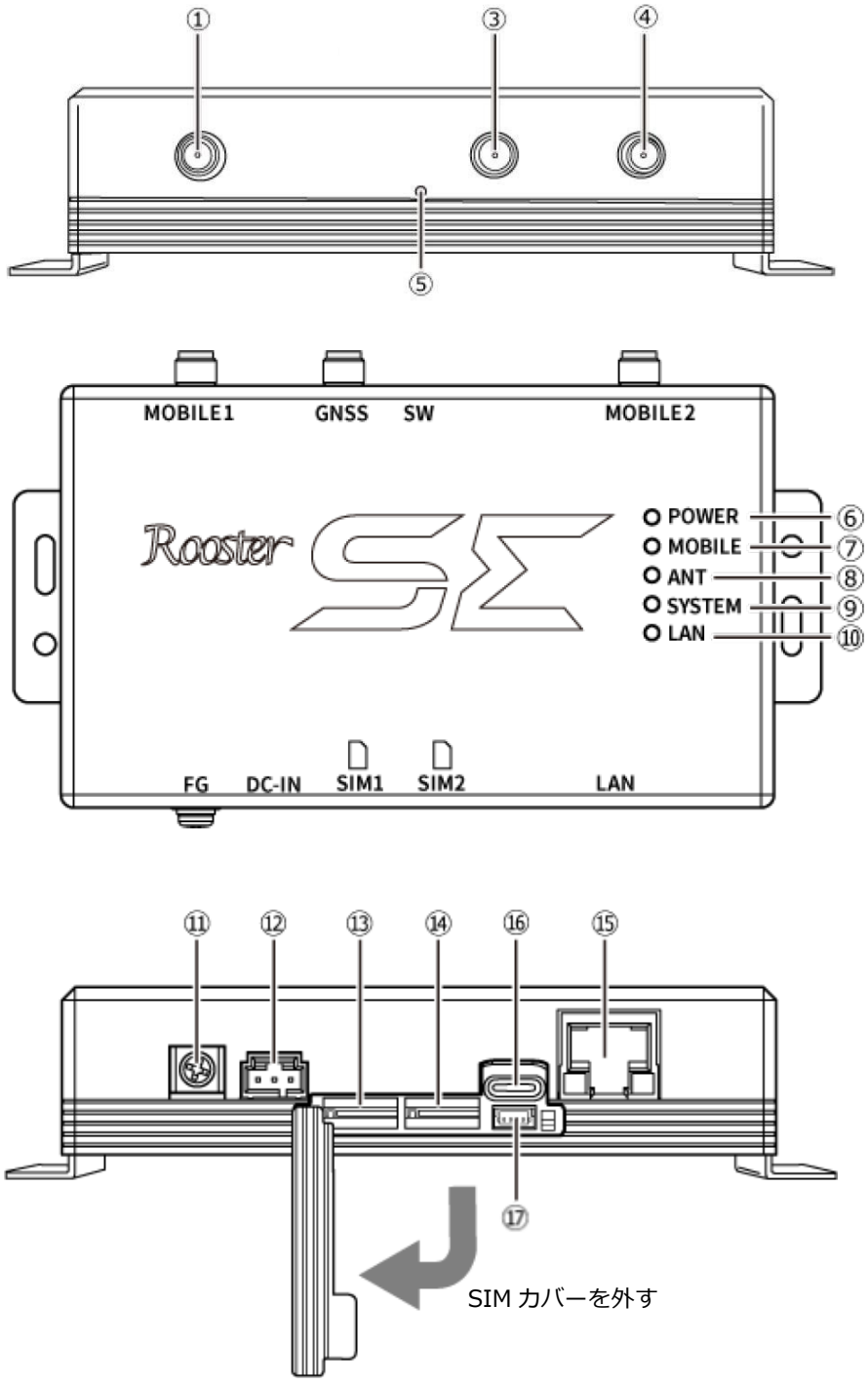
パッケージには、次のものが同梱されています。

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。

- SE 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


①
③
④
⑤
MOBILE1
GNSS
SW
MOBILE2
Rooster
POWER
MOBILE
ANT
SYSTEM
LAN
⑥
⑦
⑧
⑨
⑩
FG
DC-IN
SIM1
SIM2
LAN
⑪
⑫
⑬
⑭
⑯
⑮
⑰
SIM カバーを外す

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。
③	GNSS コネクタ（SMA）	外部アンテナ（GNSS 通信用）を接続します。（※１）（※２）
④	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。
⑤	SW タクトスイッチ	先の細い樹脂等の導電性のないピンや棒などを使って３秒以上押し続けると、SYSTEM ランプが緑点滅した状態で、MOBILE ランプ、ANT ランプの順で点滅・消灯し、工場出荷時に戻った後、再起動します。 タクトスイッチを使用して初期化する場合は『5-2. 設定情報の初期化』をご覧ください。
⑥	POWER ランプ	SE の起動状態が表示されます。
⑦	MOBLE ランプ	モバイル通信端末の動作状態が表示されます。
⑧	ANT ランプ	電波状態を表示します。
⑨	SYSTEM ランプ	SE の動作状態を表示します。
⑩	LAN ランプ	LAN ポート（⑮）への LAN 接続機器の接続状態が表示されます。
⑪	FG 端子	アース線を接続します。
⑫	DC IN コネクタ	DC 電源プラグを接続します。
⑬	SIM１カード挿入口	nano SIM カード（12.3×8.8mm）を挿入します。
⑭	SIM２カード挿入口	nano SIM カード（12.3×8.8mm）を挿入します。
⑮	LAN ポート	LAN ケーブルで LAN 接続機器、ハブなどを接続します。
⑯	USB type C コネクタ（※３）	開発メンテナンス用（ファームウェアアップデート用）。
⑰	デバッグコネクタ（※３）	開発メンテナンス用（デバッグ用）。

※１ GNSS アンテナはアクティブタイプのものを使用してください。

※２ モバイル通信用アンテナを接続しないでください。間違えて接続した場合、モバイル通信用アンテナが破損する可能性があります。

※３ このコネクタはお客様が使用するためのものではありません。ケーブルを接続すると、本製品が正常に動作しない可能性があります。

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。

➲本装置の寸法については『付録 外形寸法』をご覧ください。

⑯の USB ポートと⑰のデバッグコネクタは絶対に使用しないでください。
使用した場合、製品が正常に動作しない場合があります。

- ⑪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アンテナを使用する場合、①④に本装置に適した外部モバイルアンテナをご使用ください。
- LAN ポートには WAN 回線は接続できません。
- SIM カバーを本体から完全に外すことはできません。SIM カバーを強く引っ張らないように注意してください。破損するおそれがあります。

1-6. ランプの状態と働き

ランプ状態説明

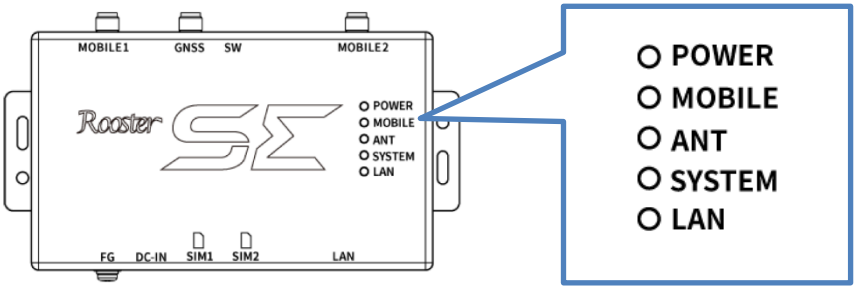
ランプ状態	補足
点灯	点灯状態が続く状態です。
消灯	消灯状態が続く状態です。
点滅	点灯と消灯を繰り返す状態です。
早い点滅	点滅より速く点灯と消灯を繰り返す状態です。
遅い点滅	点滅より遅く点灯と消灯を繰り返す状態です。

ランプ点灯・点滅パターン一覧

名称	ランプ状態	補足
POWER	消灯	電源が入っていません。
	点灯	電源が入っていて、使用可能な状態です。
MOBILE	消灯	接続が行われていません。
	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。
ANT	点灯（赤色）	モバイル通信圏外、モバイル通信未使用、 モバイル通信圏内（電波 0 :-115dBm 未満）
	点滅（赤色）	モバイル通信圏内（電波 1：-115～-105dBm）
	点滅（緑色）	モバイル通信圏内（電波 2：-105～-95dBm）
	点灯（緑色）	モバイル通信圏内（電波 3：-95dBm 以上）
SYSTEM	消灯	通常時
	点滅（緑色）	システム起動中です。
	点滅（赤色）	エラーが起きている状態です。
LAN	消灯	リンクしていません。
	点灯	リンクしています。
	速い点滅	データが流れています。

memo LAN が 10BASE でリンクしている場合は LED が点灯・点滅せず、消灯した状態になる可能性が有ります。データ通信は正常に行うことができます。

ランプの表示と状態　早見表

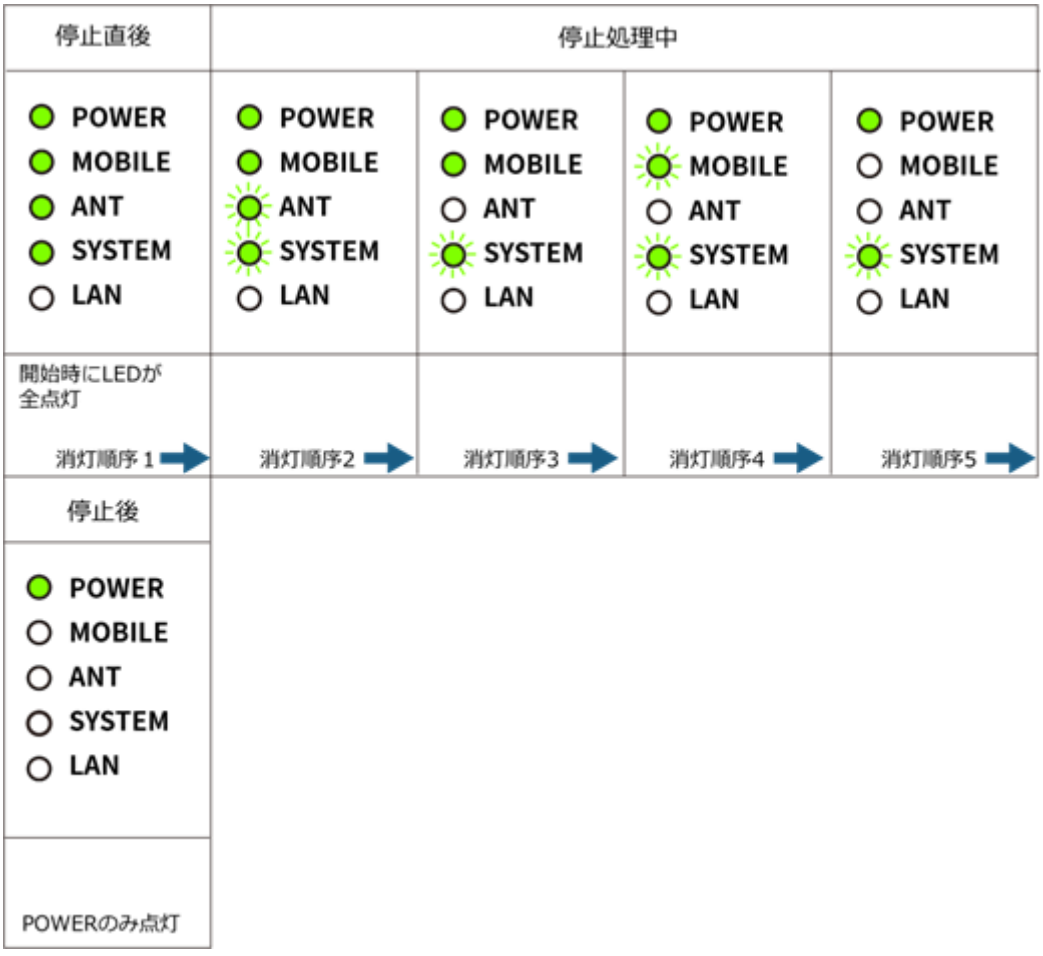


- 電源投入時

通電直後	起動中1	起動中2	各機能起動中		
POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN
点灯順序1 →	点灯順序2 →	点灯順序3 →	1秒間隔で点滅 点灯順序4 →	点灯順序5 →	点灯順序6 →

各機能起動中	起動完了
POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN
点灯順序 →	POWERのみ点灯

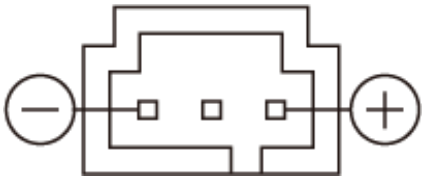
- 停止時



- モバイル通信用アンテナ強度

圏外	電波弱い	電波やや弱い	電波普通
POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN	POWER MOBILE ANT SYSTEM LAN
POWERが緑色で点灯し、ANTが橙色で点灯します。	POWERが緑色で点灯し、ANTが橙色で点滅します。	POWERが緑色で点灯し、ANTが緑色で点滅します。	POWERが緑色で点灯し、ANTが緑色で点灯します。

1-7. 電源コネクタ



電源仕様

入力電圧	DC5～32V（±5%）
消費電流	待受時：約 100 mA（DC12V） 通信時：約 200 mA（DC12V） 通信時最大：約 450 mA（DC12V）
消費電力	5.5W（最大）
リップル	200mVp-p 以下
コネクタ	Molex 3 ピン 70553-0002

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。

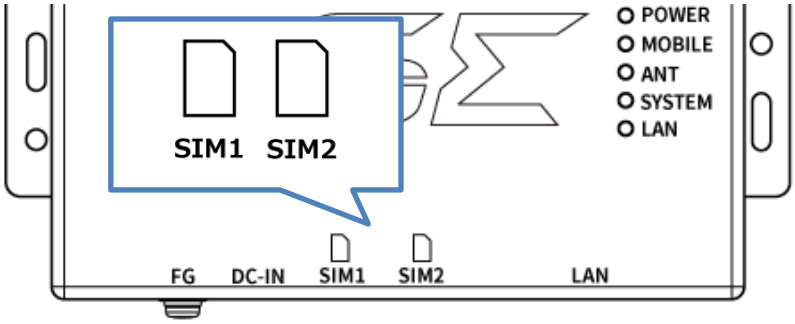
2章　導入時の設定

この章では、SE の設置方法や PC との接続方法について説明します。

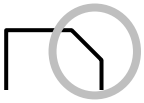
2-1. SIMカードの挿入方法

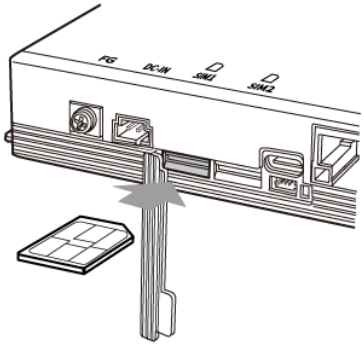
1．SIM カードの挿入口を確認します。SIM の挿入口は、本体側面にあり、天面には挿入口を示す SIM のイラストが印字されています。

2．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 SIM1 と SIM2 の 2 つがあります。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（〇部分の切りかけの位置を図に合わせた方向）で「カチッ」と音がし、ロックされるまで挿入してください。

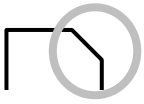


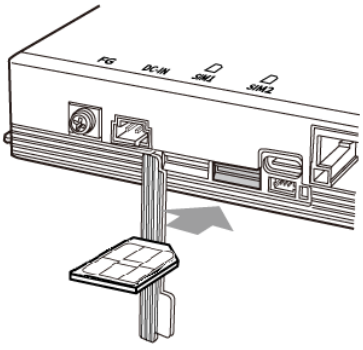
SIM1 の挿入口に入れる場合





SIM2 の挿入口に入れる場合

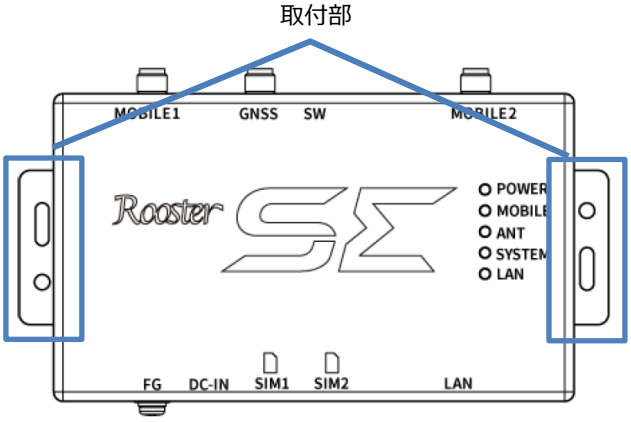




2-2. 取り付け例

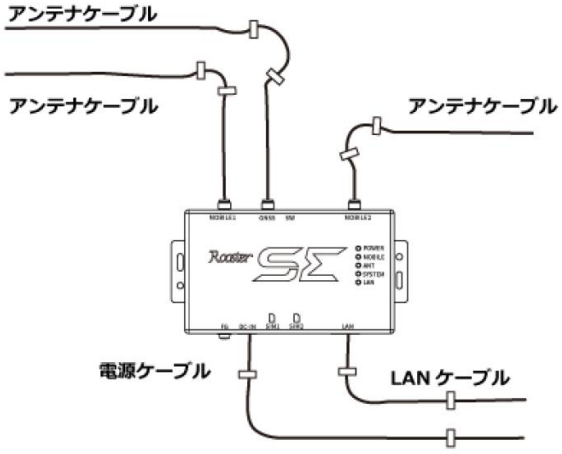
1．SE の取り付け部が固定されるよう、取り付け場所にあらかじめ直径 3.5mm の穴を 2 箇所開け、お客様でご用意いただいたΦ3mm ネジで固定します。

▶ 取り付け場所は、平滑な場所をお選びください。

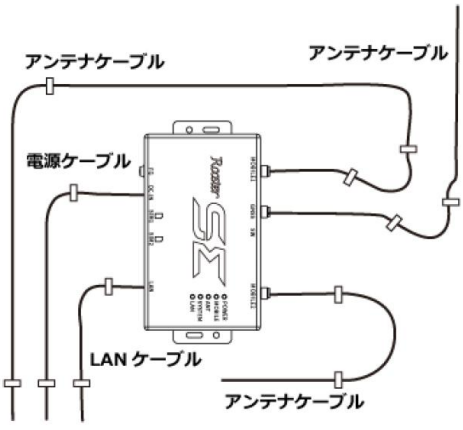


2. ケーブルを接続します。

ケーブルの接続例 (水平)



ケーブルの接続例 (垂直)



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。
- 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。
- 振動、衝撃が継続的にかかるような場所に設置する場合は、SIM カード挿入口を下向きに設置しないでください。
- DC ケーブル、LAN ケーブル、アンテナケーブルなどのケーブル類は、ケーブルの共振により製品のコネクタに過大な応力が加わる恐れがあります。製品本体にストレスを与えないように設置面にしっかり固定してください。

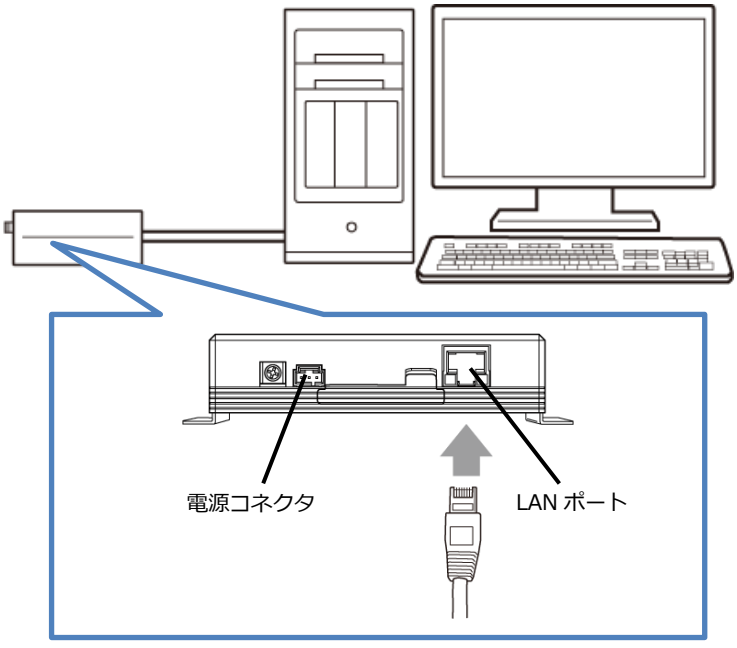
2-3. PCとの接続方法

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. SE 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. LAN 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. SE 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 SE 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。
- 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、本装置設置後、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装置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。
- 本装置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

SE 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。
  （docomo、au、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。
- SE 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。

- 接続名（APN）
- 認証プロトコル
- 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。

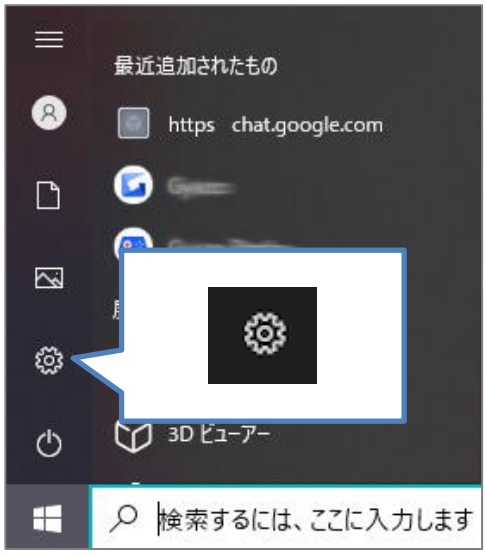
2-6. パソコンの設定

SE 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。

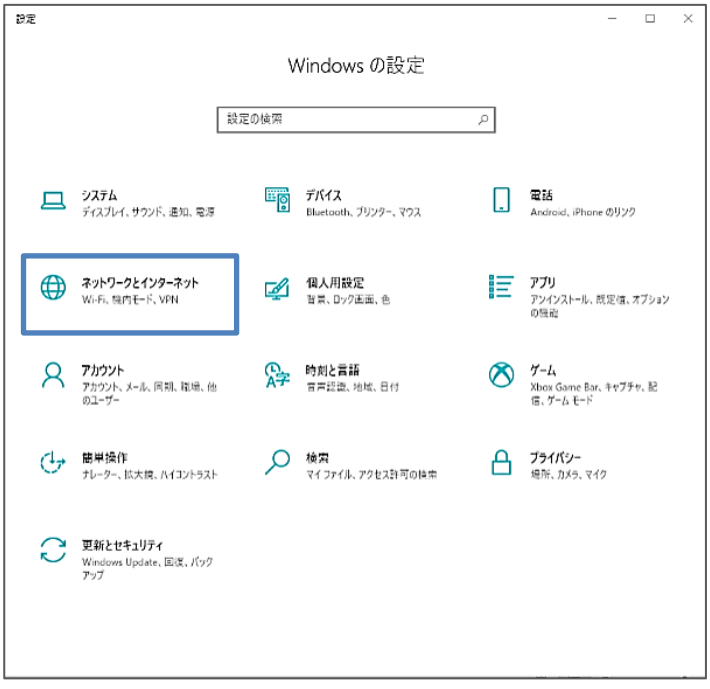
その設定方法については、ネットワークカードおよび Windows のマニュアル等をご覧ください。

2-6-1. Windowsのネットワーク設定（Windows10）

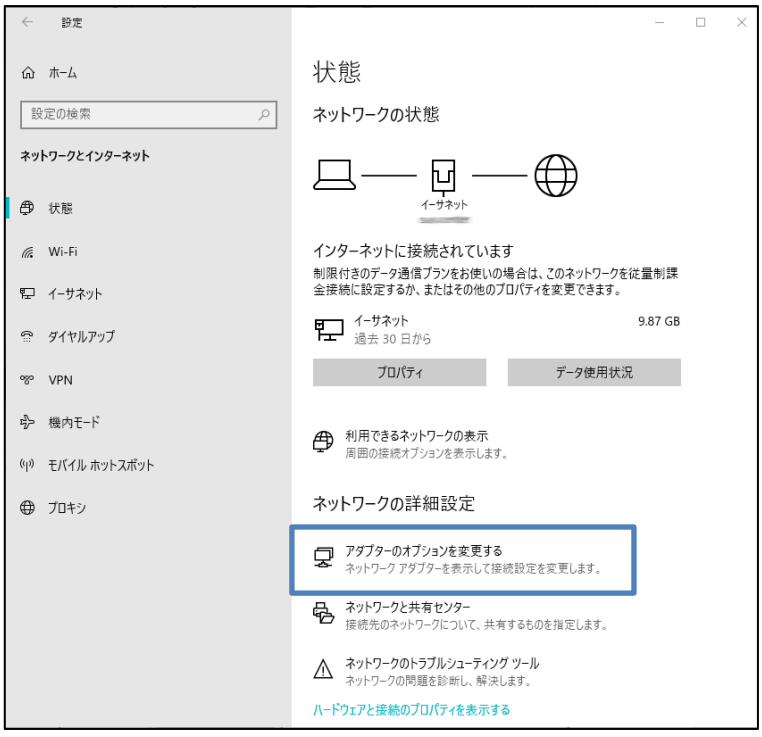
1. パソコンには管理者権限でログインしてください。
2. スタート画面から［設定］を開きます。



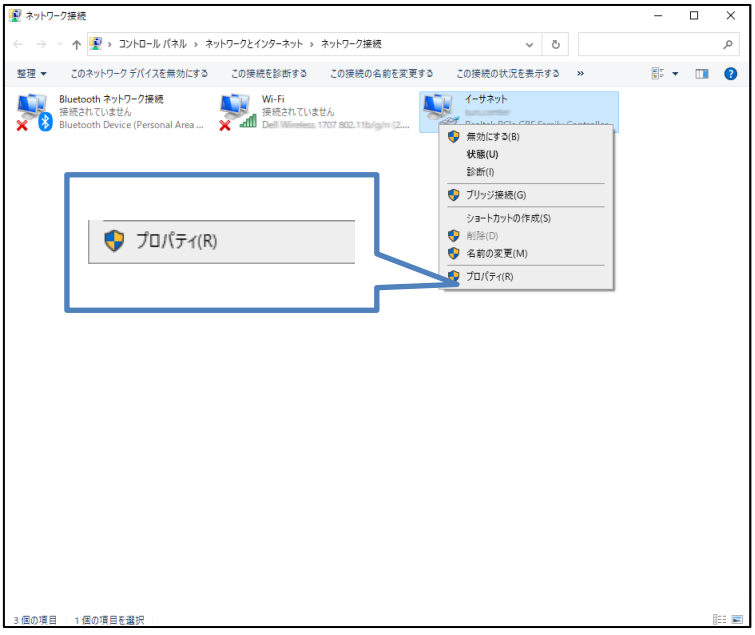
3. 「ネットワークとインターネット」を開きます。



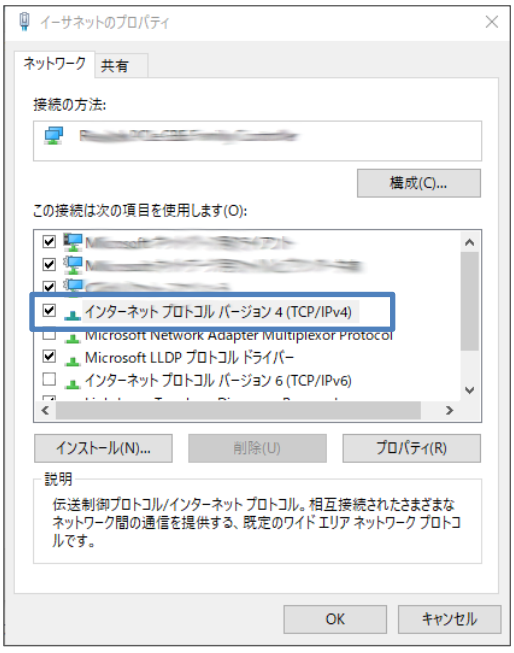
4. 「ネットワークの状態」から「アダプターのオプションを変更する」を開きます。



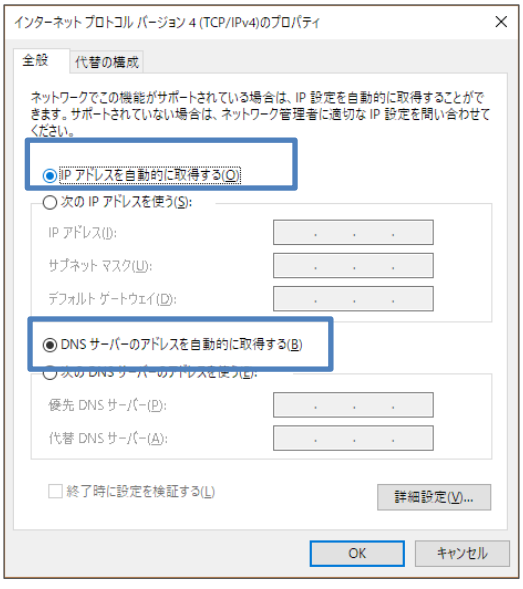
5. [イーサネット] を右クリックし、 [プロパティ] をクリックします。
   イーサネットのプロパティが表示されます。



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。

9．

「IP アドレスを自動的に取得する」に設定されている場合は通信のタイミング等によって Web 設定ツールにアクセスするのに時間がかかるケースが発生する可能性が有ります。その場合は、「次の IP アドレスを使う」を選択し、IP アドレスに 192.168.62.XX を設定して固定の IP アドレスでアクセスを行ってください。

3章　初期設定

この章では、Web 設定ツールの概要を説明します。また、Web 設定ツールを使ってパスワード変更やモバイル通信を行うための手順を説明します。

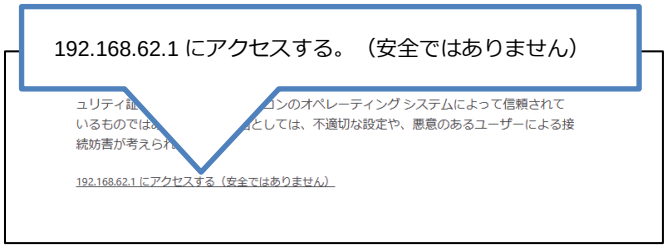
3-1. Web設定ツールのログイン方法

ログインボタンクリック時や設定ツール操作中にページの読み込み表示等が数分間続く場合はブラウザをリロード（F5）するなどして再度表示してログインからやり直してください。SE の FW バージョン更新後、ブラウザのキャッシュが残っている場合に更新前の FW バージョンの Web 設定ツールが表示されることがあります。SE の FW バージョン更新後は Web ブラウザのキャッシュを削除し、再接続してください。

1. Web ブラウザ（Google Chrome）を起動します。
2. Web ブラウザのアドレス入力欄に、SE の LAN インターフェース IP アドレス「https://192.168.62.1/」（工場出荷時状態）を入力し、Enter キーを押します。

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

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

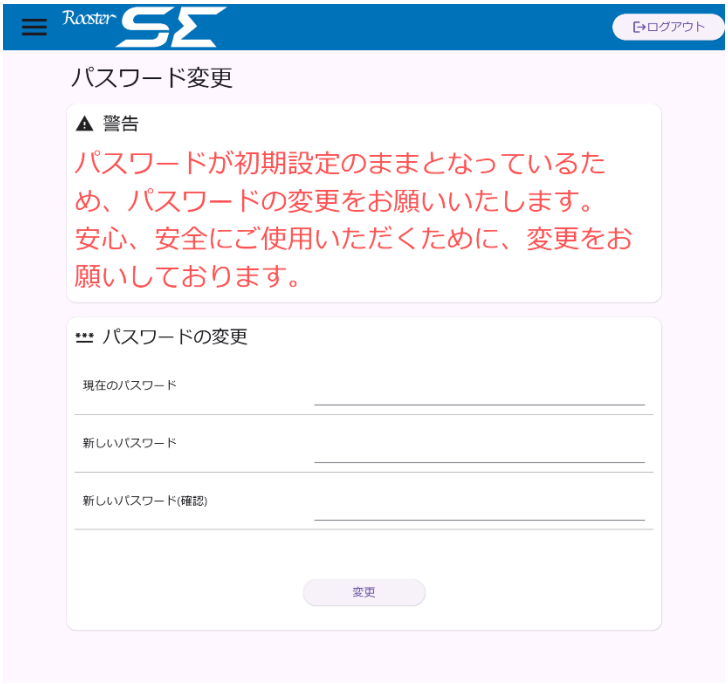


5. Web 設定ツールのログインページが表示されます。ユーザー名に「admin」、パスワードに「12345678」（工場出荷時状態）を入力します。

6. 「ログイン」をクリックします。

7. 工場出荷状態でのログイン時はパスワードの変更が必ず必要です。

「現在のパスワード」に工場出荷状態のパスワードを、「新しいパスワード」、「新しいパスワード(確認)」に新しく設定するパスワードを入力し、「変更」ボタンをクリックしてパスワードの変更を行ってください。



設定ツールの工場出荷状態の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下さい。

➲ 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、『3-2. ログインパスワードの設定』をご覧ください。

8.Web 設定ツールの画面が表示されます。

3-2. Web設定ツールの概要

各種設定、情報表示は Web 設定ツールで行います。各設定画面に進むには、左メニューを選択します。

> ログイン後、デフォルトパスワードを使用している場合は、「システム」- 「パスワード変更」画面が表示されます。

Web設定ツール画面の説明

設定画面	説明
ステータス	現在の状態や各種情報が表示されます。 一時的に SIM を切り替えるなどの操作も行えます。
インターフェース	LAN、モバイルインターフェースの設定ができます。
ネットワーク	MAC フィルタリング ルーティング IP フィルター NAT IPsec DNS フィルタリング L2TP/IPsec PPTP の設定ができます。
サービス	DDNS DNS ログ SunDMS 定期再起動 WAN ハートビート Web 設定ツール CLI GNSS トリガーの設定ができます。
ログ	システムログ ユーザーログ

設定画面	説明
	ブートログが表示されます。ログのダウンロード、削除も行えます。
システム	再起動・シャットダウン ユーザー名・パスワードの変更 設定情報ファイルの取得・適用 ファームウェアのアップデート 診断情報の取得が行えます。

3-3. ユーザー名・パスワードの設定

ログインユーザー名及び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「12345678」に設定されています。

ログインパスワードの変更：

1. Web 設定ツールのメニューから［システム］をクリックし、サブメニューから「ユーザー名・パスワード変更］をクリックし、［ユーザー名・パスワード管理］画面に入ります。

2. ［現在のパスワード］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. ［新しいパスワード（確認）］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. ［変更］ボタンをクリックして、設定を保存します。

6. パスワード変更後自動的にログアウトされログイン画面が表示されます。
   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。
- 入力可能な文字数は、半角英数字で 8 文字以上 127 文字以下までです。
- 8 文字未満のパスワードは設定できません。
- 記号を含む文字列はパスワードに設定できません。
- Web 設定ツール及び、CLI のユーザー名、パスワードは共通となります。

工場出荷状態のパスワードは初回ログイン時に変更が必須となります。
その際、推測されにくいパスワードにして下さい。

ユーザー名の変更：

1. Web 設定ツールのメニューから［システム］をクリックし、サブメニューから「ユーザー名・パスワード変更］をクリックし、［ユーザー名・パスワード管理］画面に入ります。

2. ［新しいユーザー名］に新しく設定するユーザー名を入力します。

3. ［変更］ボタンをクリックして、設定を保存します。

4. ユーザー名変更後自動的にログアウトされログイン画面が表示されます。
   新しく設定したユーザー名で再度ログインします。

memo
- 入力可能な文字は、半角英小文字、数字、「-」「_」「.」で、３２文字以下までです。
- 先頭の文字に数字、「-」は使用できません。
- ４文字未満のユーザー名は設定できません。

変更はすぐに反映されます。システムに反映される際、ログイン中の CLI のセッションが全て終了され、CLI(SSH Server)機能が再起動されます。CLI(SSH Server)機能の設定が変更されかつ「設定を保存」されている場合は変更された設定で CLI 機能が再起動されます。

3-4. LANインターフェース設定

LAN インターフェースの IP アドレス、DHCP サーバ設定を変更する場合に設定を行います。

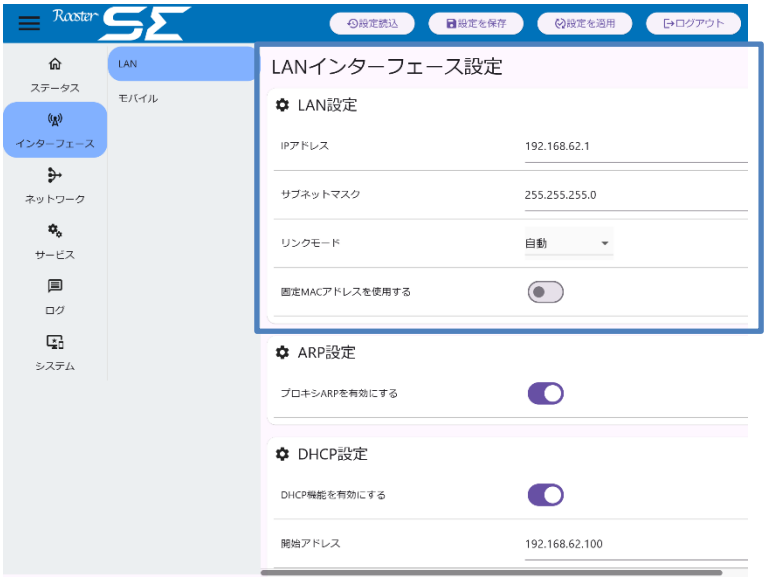
3-4-1. LAN設定

LAN インターフェースの IP アドレス、サブネットマスクを変更する場合に設定を行います。

又、必要があれば LAN のリンクモード等の設定を行います。

工場出荷時状態の LAN インターフェースの IP アドレスは「192.168.62.1」に設定されています。

1. Web 設定ツールのメニューから、[インターフェース] – [LAN] をクリックし、 [LAN インターフェース設定] 画面に入ります。



2. 以下の設定を行います。

設定項目	内容
IP アドレス	LAN インターフェースに割り当てる IP アドレスを設定します。 ▶ 初期設定では、192.168.62.1 に設定されています。
サブネットマスク	LAN インターフェースのサブネットマスクを設定します。 ▶ 初期設定では、255.255.255.0 に設定されています。
リンクモード	LAN インターフェースのリンクモードを設定します。 ▶ 初期設定では、「自動」に設定されています。
固定 MAC アドレスを使用する	LAN インターフェースの MAC アドレスを固定とするかを設定します。 ▶ 初期設定では、「無効(ランダム)」に設定されています。

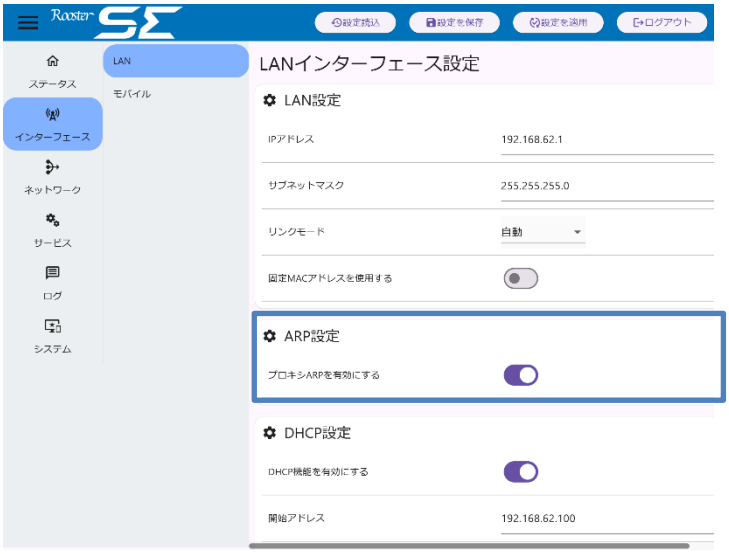
3. ［設定を保存］ボタンをクリックして、設定を保存します。

IP アドレスを設定し再起動した後は、一旦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。
IP アドレスに 169.254.4.0～169.254.4.255 を設定しないでください。
初期設定時、リンクモードは「自動（オートネゴシエーション）」に設定されています。
オートネゴシエーション未対応のデバイスとの通信を行う際や、スピード・Duplex を固定にしたい場合に設定を行ってください。リンクモードは起動時「自動」で 1 度リンクアップし、ランプの状態と働きの「各機能起動中」にスピード、Duplex を設定値に変更する動作となります。

3-4-2. ARP設定

LAN インターフェースの ARP に関する設定を行います。

1. Web 設定ツールのメニューから、[インターフェース] – [LAN] をクリックし、 [LAN インターフェース設定] 画面に入ります。



2. 以下の項目を設定します。

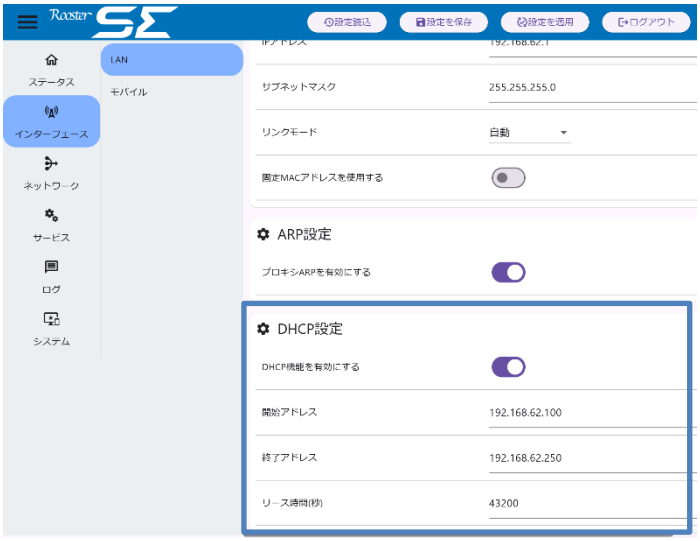
設定項目	内容
プロキシ ARP を有効にする	LAN インターフェースのプロキシ ARP 機能の有効・無効を設定します。 ▶ 初期状態では、「有効」に設定されています。

4. ［設定を保存］ボタンをクリックして、設定を保存します。

3-4-3. DHCP設定

DHCP サーバ機能の設定を変更する場合に設定を行います。

1. Web 設定ツールのメニューから、[インターフェース] – [LAN] をクリックし、 [LAN インターフェース設定] 画面に入ります。



2. デフォルト状態では、DHCP 機能は有効になっています。
   DHCP 機能を使用しない場合、［DHCP 機能を有効にする］右側のボタンをクリックします。

3. 以下の項目を設定します。

設定項目	内容
開始アドレス	割り当てる IP アドレスの開始アドレスを入力します。
終了アドレス	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、［開始アドレス］が「192.168.62.100」、［終了アドレス］が「192.168.62.250」と設定されています。
リース時間(秒)	DHCP サーバが IP アドレスをクライアントに割り当てる時間を設定します。 ▶ 初期設定では、［リース時間(秒)］が「43200」（12 時間）と設定されています。

4. ［設定を保存］ボタンをクリックして、設定を保存します。

> 開始 IP アドレス、終了 IP アドレスに 169.254.4.0～169.254.4.255 を設定しないでください。
> 開始 IP アドレス、終了 IP アドレスには LAN インターフェースのネットワークアドレスの範囲内のアドレスを設定してください。

3-5. モバイルインターフェース設定

3-5-1. SIMスロット・アンテナ設定

使用するアンテナと使用する SIM スロットを変更する場合に設定を行います。

1. Web 設定ツールのメニューから、［インターフェース］－［モバイル］をクリックし、「モバイルインターフェース設定」画面に入ります。

2. 以下の設定を行います。

設定項目	内容
使用するアンテナ	MOBILE1: MOBILE1 で使用するアンテナをプルダウンメニューの［内部アンテナ］、［外部アンテナ］ から選択します。 ▶ 初期設定では、［内部アンテナ］に設定されています。
	MOBILE2: MOBILE2 で使用するアンテナをプルダウンメニューの［内部アンテナ］、［外部アンテナ］ から選択します。 ▶ 初期設定では、［内部アンテナ］に設定されています。
使用する SIM スロット	使用する SIM スロットをプルダウンメニューの［sim1］、［sim2］から選択します。 ▶ 初期設定では、［使用する SIM スロット］が［sim1］に設定されています。

3. ［設定を保存］ボタンをクリックして、設定を保存します。

「使用する SIM スロット」が SIM2 に設定されている場合で、SIM2 スロットに SIM カードが挿入されていない場合は SIM1 スロットが使用されます。
MOBILE1 は送受信を行う main アンテナとなります。
MOBILE2 は受信のみを行う div アンテナとなります。

3-5-2. 監視機能設定

モバイル通信の監視機能設定を行います。

SIM 監視機能：
SIM カードが挿入されていない事を検知した場合に本体の再起動を行う機能です。
稼働中に SIM の接触不良等不測の事態が発生し、SIM カードが認識できなくなった場合に本体再起動を試みて復旧を試みる機能となります。

モバイルサービス状態(圏外)監視機能：
モバイルサービス状態が登録以外の状態が 10 分間継続した場合に本体の再起動を行う機能です。

SIM 監視機能を有効に設定した場合は必ず使用する SIM スロットに SIM カードを挿入した状態で起動してください。SIM カードが挿入されていない場合、本体の再起動が繰り返される可能性があります。

1. Web 設定ツールのメニューから、［インターフェース］–［モバイル］をクリックし、「モバイルインターフェース設定」画面に入ります。

2. 以下の設定を行います。

設定項目	内容
SIM 監視機能を有効にする	SIM 監視機能の有効・無効を設定します。 ▶ 初期設定では、「無効」に設定されています。
モバイルサービス状態(圏外)監視機能を有効にする	圏外監視機能の有効・無効を設定します。 ▶ 初期設定では、「無効」に設定されています。

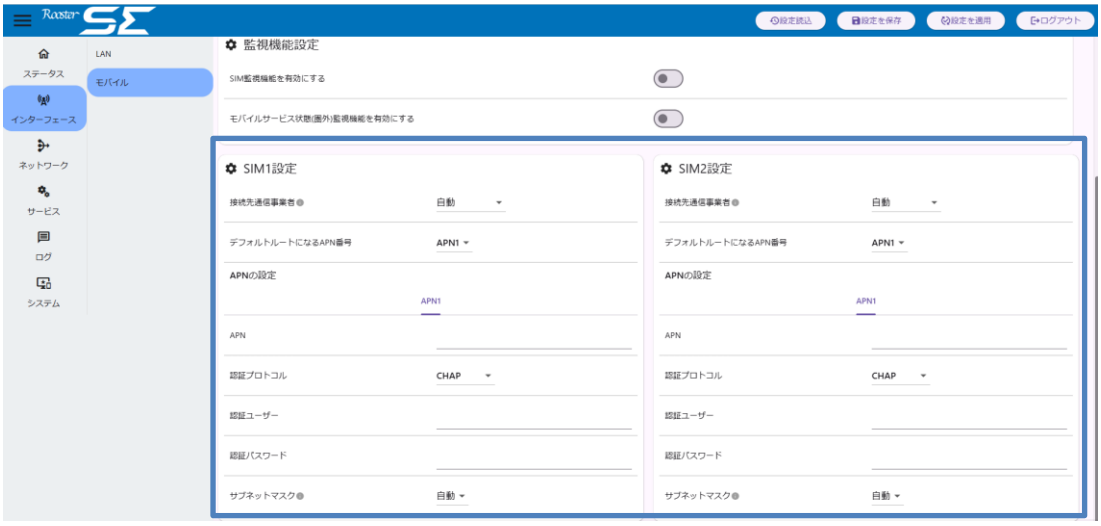
3. ［設定を保存］ボタンをクリックして、設定を保存します。

3-5-3. モバイル通信設定

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）
・認証プロトコル
・ユーザー名
・パスワード

1. Web 設定ツールのメニューから、［インターフェース］－［モバイル］をクリックし、「モバイルインターフェース設定」画面に入ります。



2. ［SIM1 設定］、［SIM2 設定］において、以下の項目の入力を行います。

設定項目	内容
接続先通信事業者	接続先の通信事業者を設定します。 ▶ 初期設定では、「自動」に設定されています。
APN	ご契約のプロバイダの APN（アクセスポイントネーム）を入力します。
認証プロトコル	認証プロトコルをプルダウンメニューの［認証なし］、［PAP］、［CHAP］、［CHAP/ PAP］より選択します。
認証ユーザー	ご契約の SIM のユーザー名を入力します。
認証パスワード	ご契約の SIM のパスワードを入力します。
サブネットマスク	モバイルインターフェースに割り当てるサブネットマスクを設定します。 ▶ 初期設定では、「自動」に設定されています。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

5. 再起動後、Web 設定ツールに再ログインし、［ステータス］－［モバイルインターフェース］をクリックし、［モバイルインターフェース情報］画面に情報が表示されていることを確認します。

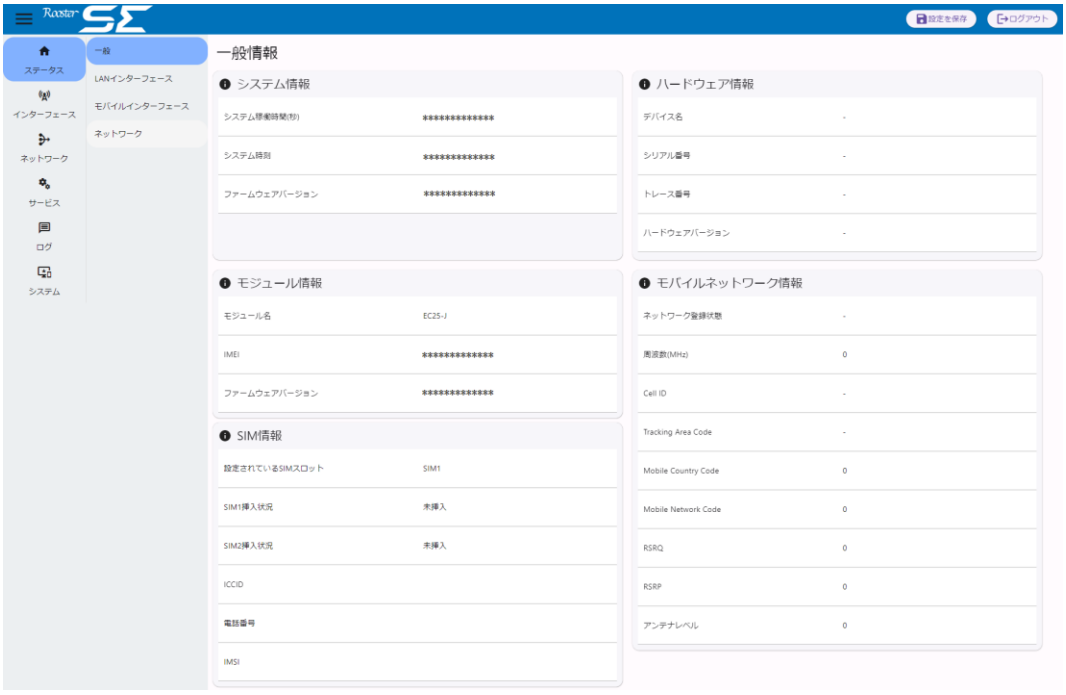
「接続先通信事業者」は、特定の SIM カードを使用する際等
必要な場合にのみ設定してください。
「サブネットマスク」は、閉域網で使用する場合等モバイルインターフェースの
ネットワークアドレスを意識する必要がある場合のみ設定してください。

4章　運用

この章では、SE の運用に必要な操作、ステータス画面の見方について説明します。

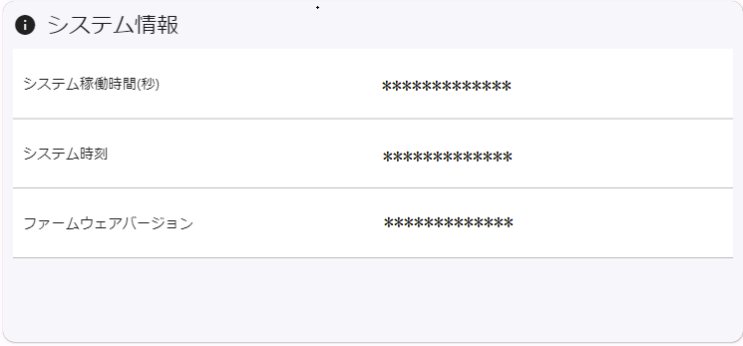
4-1. 一般ステータス確認

通信状態や端末の情報などは、［一般情報］画面で確認します。
Web 設定ツールのメニューから、［ステータス］－［一般］をクリックし、「一般情報」画面に入ります。



4-1-1. システム情報

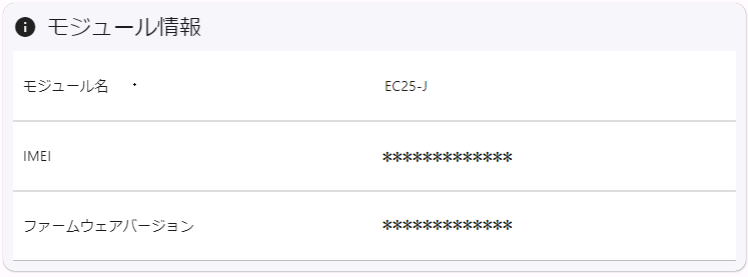
システム情報が表示されます。



項目	内容
システム稼働時間(秒)	起動してから経過した時間（秒数）が表示されます。
システム時刻	内部に保存されている時刻が表示されます。 ▶モバイル通信モジュールが時刻情報を取得できたタイミングでシステム時刻が補正されます。 ▶電源断時の時刻情報は保持されません。
ファームウェアバージョン	現在のファームウェアバージョンが表示されます。

4-1-2. モジュール情報

内蔵されている通信モジュール情報が表示されます。



項目	内容
モジュール名	モジュール名が表示されます。
IMEI	通信モジュールの IMEI が表示されます。
ファームウェアバージョン	通信モジュールのファームウェアバージョンが表示されます。

4-1-3. SIM情報

SIM に関する情報は、設定ツールのメニューから「ステータス」-「一般」をクリックして表示される「SIM 情報」、から確認することができます。又、一時的に SIM を切り替えるための切り替えボタンがあります。

項目	内容
SIM 切り替え	SIM スロットを「使用している SIM スロット」からもう一方のスロットへ切り替えます。
使用している SIM スロット	現在使用している SIM スロットが表示されます。
SIM1 挿入状況	SIM1 スロットの SIM カード挿入状況が表示されます。
SIM2 挿入状況	SIM2 スロットの SIM カード挿入状況が表示されます。
ICCID	現在使用している SIM カードの ICCID 情報が表示されます。
電話番号	現在使用している SIM カードの電話番号が表示されます。
IMSI	現在使用している SIM カードの IMSI 情報が表示されます。

SIM 切り替えを行う際は、3-5-3 で両方の SIM スロットの接続設定がされていること、両方の SIM スロットに SIM が挿入されていることを確認してください。
設定がされていない場合や SIM が挿入されていない場合は切り替えに失敗します。

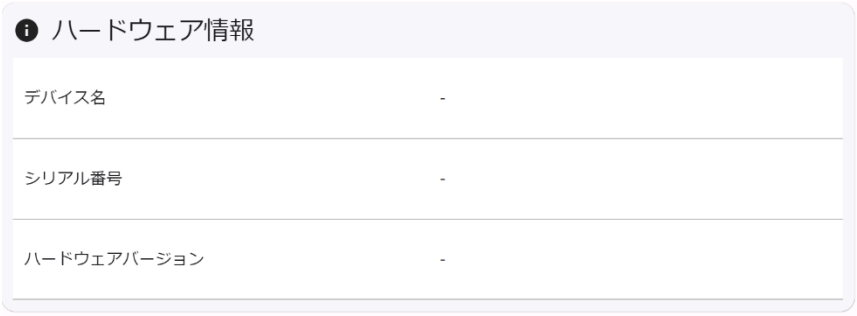
4-1-4. モバイルネットワーク情報

回線のステータス情報は、設定ツールのメニューから「ステータス」-「一般」をクリックして表示される「モバイルネットワーク情報」から確認することができます。

項目	内容
ネットワーク登録状態	現在接続している回線のネットワーク登録状態が表示されます。
周波数(MHz)	現在接続している回線の周波数(MHz) が表示されます。
Cell ID	現在接続している回線の Cell ID が表示されます。
Tracking Area Code	現在接続している回線の Tracking Area Code が表示されます。
Mobile Country Code	現在接続している回線の Mobile Country Code が表示されます。
Mobile Network Code	現在接続している回線の Mobile Network Code が表示されます。
RSRQ	現在接続している回線の RSRQ (基準信号受信品質) が表示されます。
RSRP	現在接続している回線の RSRP (基準信号受信電力) が表示されます。
アンテナレベル	現在接続している回線のアンテナレベルが表示されます。 0：極めて弱い 1：弱い 2：普通 3：強い

4-1-5. ハードウェア情報

ハードウェア情報が表示されます。



項目	内容
デバイス名	デバイス名が表示されます。
シリアル番号	シリアル番号が表示されます。
ハードウェアバージョン	ハードウェアバージョンが表示されます。

4-2. LANインターフェースステータス確認

LAN インターフェースのステータス情報は、設定ツールのメニューから「ステータス」- 「LAN インターフェース」をクリックして表示される「LAN 情報」、「DHCP リース情報」から確認することができます。

4-2-1. LANインターフェース情報

LAN 情報

項目	内容
MAC アドレス	インターフェースの MAC アドレスが表示されます。 ▶ 仮想 MAC アドレスが割り当てられているため、SE を再起動するたびに変化します。
IP アドレス	インターフェースの IP アドレスが表示されます。
ネットマスク	インターフェースのネットマスクが表示されます。
DHCP 機能	インターフェースの DHCP サーバ機能の有効・無効の状態が表示されます。

4-2-2. DHCPリース情報

DHCP リース情報

項目	内容
ホスト名	クライアントのホスト名が表示されます。
IP アドレス	クライアントに払い出した IP アドレスが表示されます。
MAC アドレス	クライアントの MAC アドレスが表示されます。
リース終了時間	払い出した IP アドレスの有効期間が終了する時刻が表示されます。

4-3. モバイルインターフェースステータス確認

モバイルインターフェースのステータス情報は、設定ツールのメニューから「ステータス」-「モバイルインターフェース」をクリックして表示される「モバイル 1 情報」から確認することができます。

4-3-1. モバイルインターフェース情報

項目	内容
APN 番号	接続の APN 番号が表示されます。 ※v.1.3 時点では 1 固定となります。
最終情報取得時刻	最後に情報を取得した時刻が表示されます。
IP アドレス	モバイルインターフェースの IP アドレスが表示されます。
プライマリ DNS サーバアドレス	プライマリ DNS サーバアドレスが表示されます。
セカンダリ DNS サーバアドレス	セカンダリ DNS サーバアドレスが表示されます。

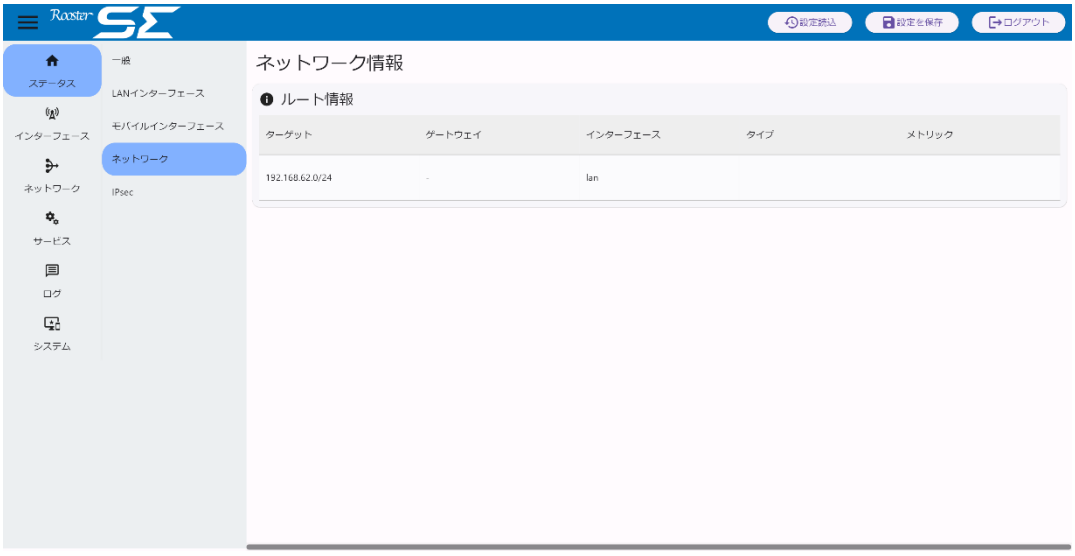
項目	内容
送信したパケット数	モバイルインターフェースから送信されたパケットの数が表示されます
受信したパケット数	モバイルインターフェースで受信したパケットの数が表示されます。
破棄した送信パケット数	破棄した送信パケットの数が表示されます。
破棄した受信パケット数	破棄した受信パケットの数が表示されます。
送信したバイト数	モバイルインターフェースから送信されたバイト数が表示されます。
受信したバイト数	モバイルインターフェースで受信したバイト数が表示されます。

パケット数・バイト数の表示はモバイル接続が切断されるとリセットされます。

4-4. ネットワークステータス確認

ネットワークのルーティング情報は、設定ツールのメニューから「ステータス」-「ネットワーク」をクリックして表示される「ルート情報」から確認することができます。

4-4-1. ルート情報



項目	内容
ターゲット	ターゲットの IP アドレス及びネットマスクが表示されます。
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。
インターフェース	出力インターフェースが表示されます。
タイプ	そのルートのタイプが表示されます。 ※IPsec 設定を行った場合、「blackhole」が表示されます。
メトリック	ルートのメトリックが表示されます。 ※IPsec 設定を行った場合に表示されます。

4-5. IPsec情報確認

IPsec の接続情報は、設定ツールのメニューから「ステータス」-「IPsec」をクリックして表示される「IPsec 情報」から確認することができます。

4-5-1. IPsec接続情報

項目	内容
設定名	IPsec 設定ページで設定した設定名が表示されます。
接続先アドレス	接続先のアドレスが表示されます。
接続先ネットワーク	接続先ネットワークアドレスが表示されます。
状態	接続状態が表示されます。 接続済み：接続先と接続が完了した状態です。 接続中　：接続先に対して接続を施行しています。 未接続　：接続していません。 エラー　:認証等が上手く出来ず接続が完了できなかった状態です。 不明　　：IPsec 機能が無効等で接続状態が取得できない状態です。

4-6. L2TP/IPsec情報確認

L2TP/IPsec の接続情報は、設定ツールのメニューから「ステータス」-「L2TP/IPsec」をクリックして表示される「L2TP/IPsec 情報」から確認することができます。

4-6-1. L2TP/IPsec接続情報

項目	内容
サーバ起動状態	L2TP/IPsec サーバの起動状態が表示されます。 アクティブ　　：サーバが起動している状態です。 インアクティブ：サーバが停止している状態です。
ユーザー名	ユーザー名が表示されます。
割り当てアドレス	ユーザーに割り当てられた IP アドレスが表示されます。
状態	接続状態が表示されます。 接続済み：接続先と接続が完了した状態です。 未接続　：接続していません。

4-7. PPTP情報確認

PPTP の接続情報は、設定ツールのメニューから「ステータス」-「PPTP」をクリックして表示される「PPTP 情報」から確認することができます。

4-7-1. PPTP接続情報

項目	内容
サーバ起動状態	PPTP サーバの起動状態が表示されます。 アクティブ　　：サーバが起動している状態です。 インアクティブ：サーバが停止している状態です。
ユーザー名	ユーザー名が表示されます。
割り当てアドレス	ユーザーに割り当てられた IP アドレスが表示されます。
状態	接続状態が表示されます。 接続済み：接続先と接続が完了した状態です。 未接続　：接続していません。

4-8. GNSS(位置)情報確認

現在地の情報は、設定ツールのメニューから「ステータス」-「GNSS」をクリックして表示される「GNSS 情報」から確認することができます。

「GNSS」機能が無効になっている場合は位置情報を表示する事が出来ません。
事前に機能が有効であることを確認の上使用してください。

SE が内部で定期的に取得している位置情報の最新値が表示されます。
「位置情報更新」をクリックした時間と「最終取得時刻」は異なる可能性が有ります。又、電波環境等によって位置情報が取得できなくなった場合は最後に取得できた位置情報が表示されます。

4-8-1. GNSS(位置)情報

項目	内容
位置情報更新ボタン	位置情報を取得します。
最終取得時刻	位置情報を取得できた最後の時刻が表示されます。 YYYY-MM-DDTHH-MM-SSZ 形式で表示されます。
緯度	緯度が表示されます。 XX.XXXXXX 度(-90 ~ 90)として表示されます。
経度	経度が表示されます。 XXX.XXXXXX 度 (-180 ~ 180)として表示されます。

4-9. SEの再起動・シャットダウン

再起動とシャットダウンは［再起動・シャットダウン］で行います。
Web 設定ツールのメニューから、［システム］－［再起動・シャットダウン］をクリックし、「再起動／シャットダウン」画面に入ります。

4-9-1. 再起動

[再起動を実行] の設定項目にて、[実行] ボタンをクリックします。

SE 本体の再起動が始まります。

約 60 秒後に自動的にブラウザがリロードされログインページが表示されます。

> 再起動が完了するまで、2 分程度かかります。
> ブラウザが自動リロードしてもログイン画面が表示されない場合は、再度リロードを行ってください。

4-9-2. シャットダウン

> 可能な限りシャットダウンを実行してから電源をお切りください。
> シャットダウンせず電源を切る場合、フラッシュメモリの寿命が縮んだり、ファイルシステムが破損したりする可能性があります。

[シャットダウンを実行] の設定項目にて、[実行] ボタンをクリックします。

SE 本体のシャットダウンが始まります。

十分に時間をおいてから電源をお切りください。

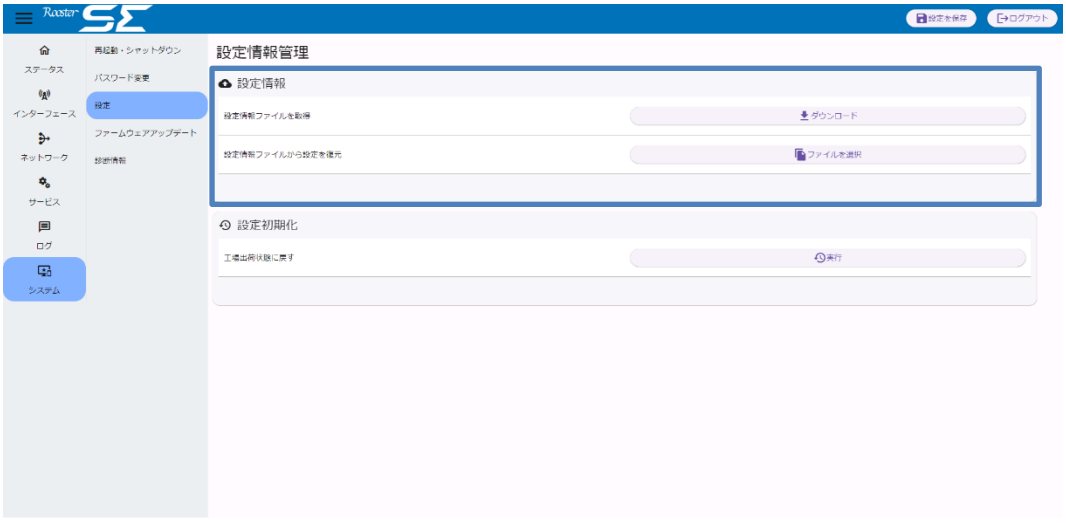
> シャットダウンが完了するまで、2 分程度かかります。

5章　メンテナンス設定

この章では、SE 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等について説明します。

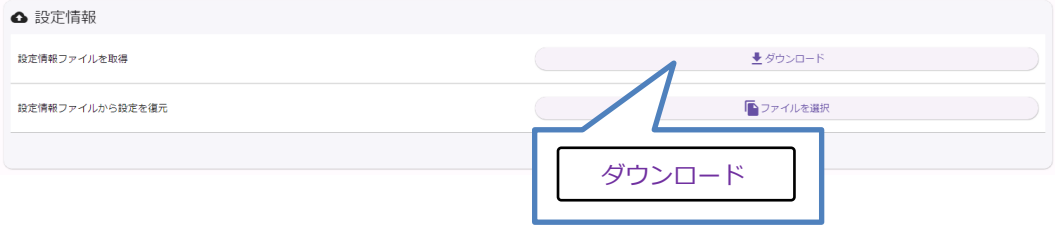
5-1. 設定情報の保存、復元

設定ツールのメニューから、［システム］－［設定］ をクリックし、「設定情報管理」画面に入ります。



5-1-1. 現在の設定を保存

現在の設定情報の保存を行います。



1. ［設定情報ファイルを取得］の［ダウンロード］ボタンをクリックします。
2. SE の設定情報ファイル「yyyy-mm-dd-rooster-se-backup」がダウンロードされます。

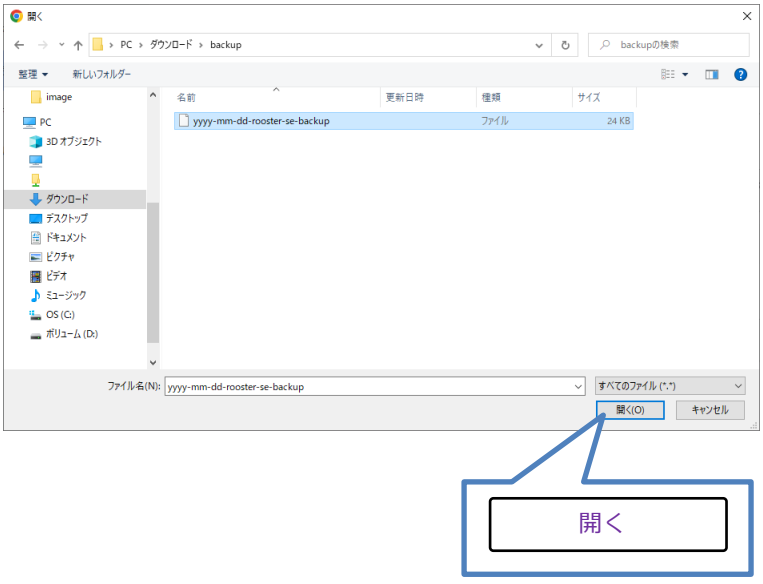
5-2-2. 保存した設定の復元

過去に保存された設定ファイルからの復元を行います。

> 工場出荷状態のパスワードを含んだ設定情報ファイルからは設定の復元を行う事ができません。

1. ［設定情報ファイル］の［ファイルを選択］ボタンをクリックします。

2. 復元を行う設定情報ファイル「yyyy-mm-dd-rooster-se-backup」の選択し、「開く」をクリックします。



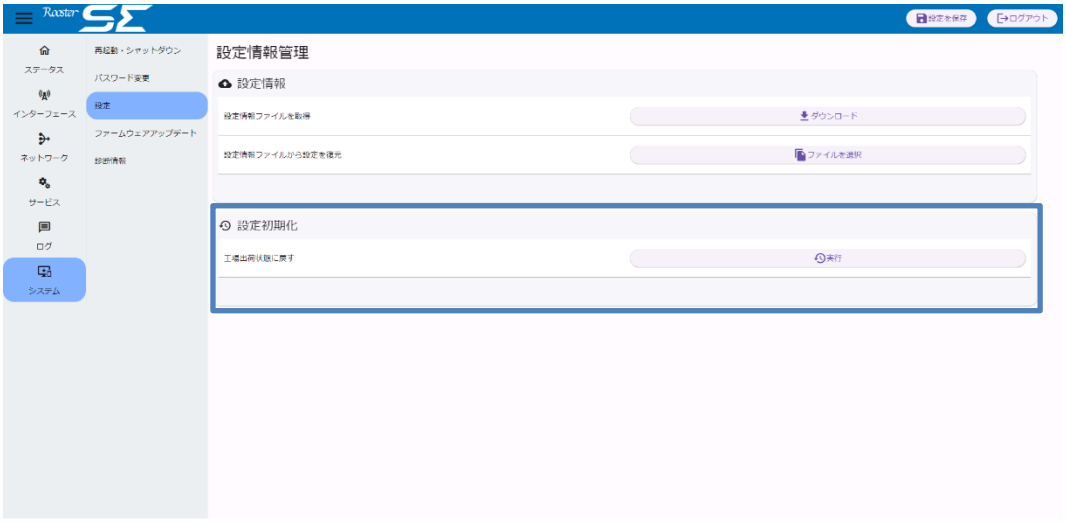
3. 「バックアップファイルのアップロードに成功しました。再起動後設定が反映されます。」が表示されます。

4. SE の再起動を行います。

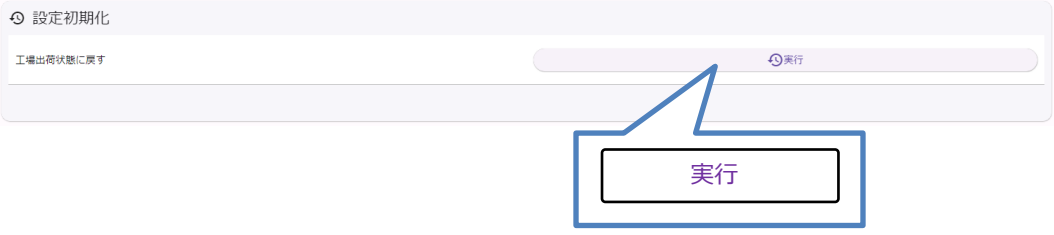
➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

5-2. 設定情報の初期化

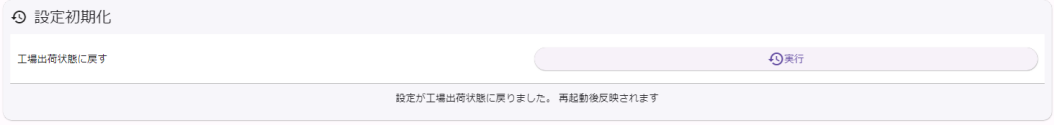
設定ツールのメニューから、［システム］－［設定］ をクリックします。
「設定情報管理」の画面が表示されます。



1. ［工場出荷時状態に戻す］の［実行］ボタンをクリックします。



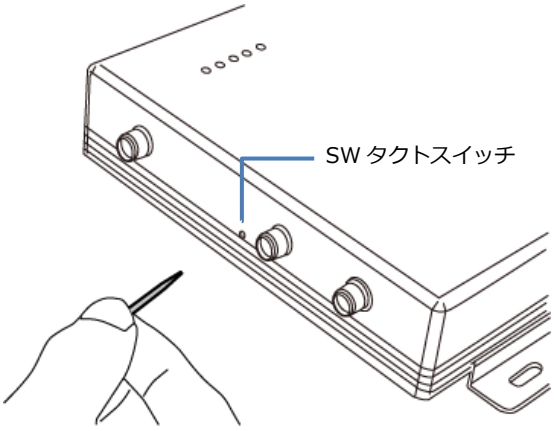
2. 「設定が工場出荷状態に戻りました。再起動後反映されます」が表示されます。



3. ポップアップを閉じると、ログイン画面に戻ります。工場出荷状態のユーザー名・パスワードで再ログインしてください。

「実行」後設定が工場出荷状態に戻ります。「再起動」又は、「設定を適用」後に設定が反映されます。
ユーザー名及びパスワードは「実行」後、再起動前に反映されます。工場出荷時のパスワードで再度ログインしてください。

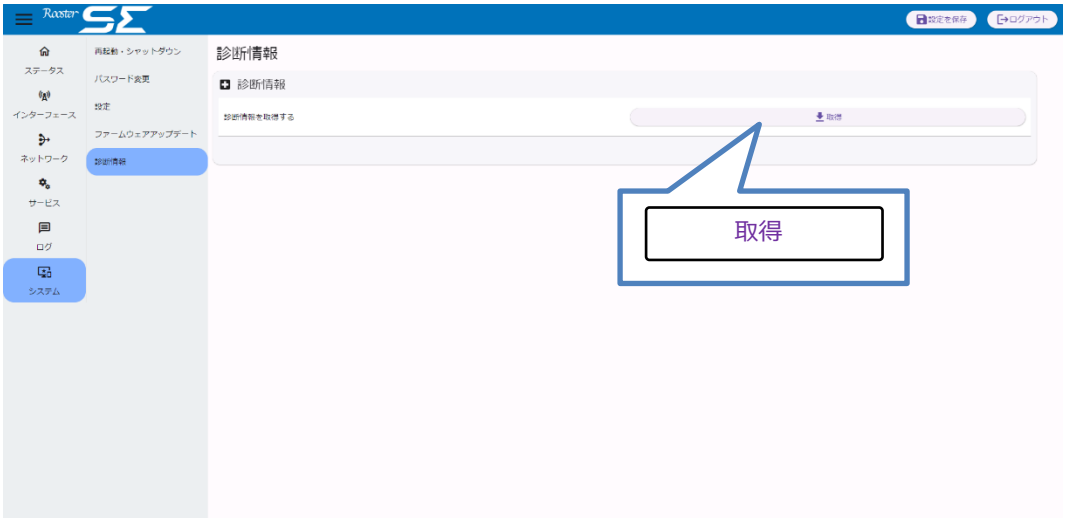
memo SE 本体にある SW タクトスイッチを先の細い樹脂等の導電性のないピンや棒で長押し（3秒以上）することで設定情報の初期化を行うこともできます。



5-3. 診断情報の取得

診断情報の取得ページでは、本装置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、［システム］－［診断情報］をクリックします。
   「診断情報」のページが表示されます



2. 「取得」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

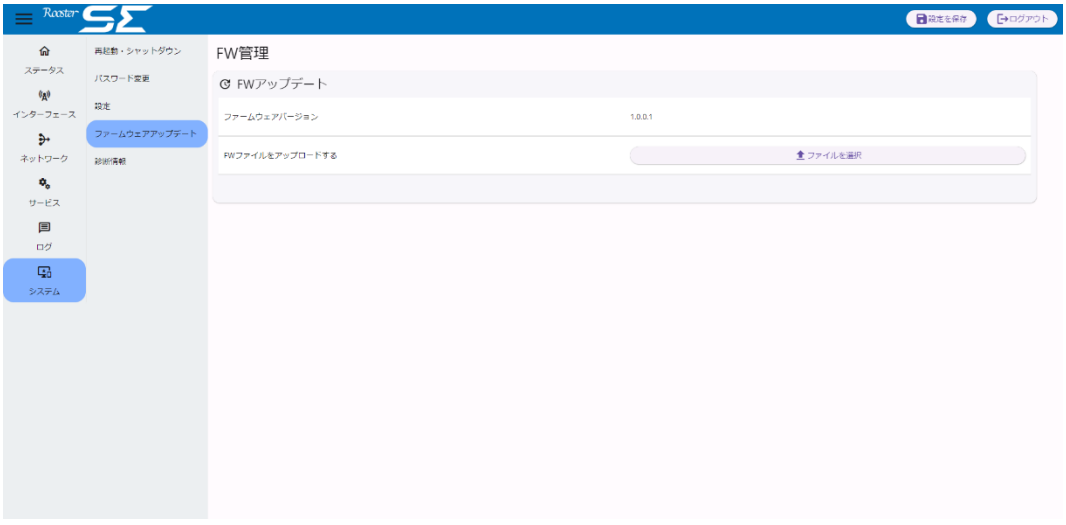
5-4. ファームウェアのアップデート方法

ブラウザのキャッシュ機能によって、Web 設定ツールがキャッシュされている場合、ファームウェアをアップデートしても Web 設定ツールの見た目が更新されない場合があります。ファームウェアアップデート後、Web 設定ツールにアクセスする場合は、ブラウザのキャッシュを削除して読み込み直してください。

V2.0.0.X へアップデートする際は、設定されているパスワードが工場出荷状態でない事を確認してください。工場出荷状態のパスワードが設定されている状態で、ファームウェアのアップデートが行われた場合、アップデート自体は完了しますが、起動時に保存されている設定情報は読み込まず、工場出荷状態の設定で動作します。

1. 設定ツールのメニューから、［システム］－［ファームウェアアップデート］をクリックします。

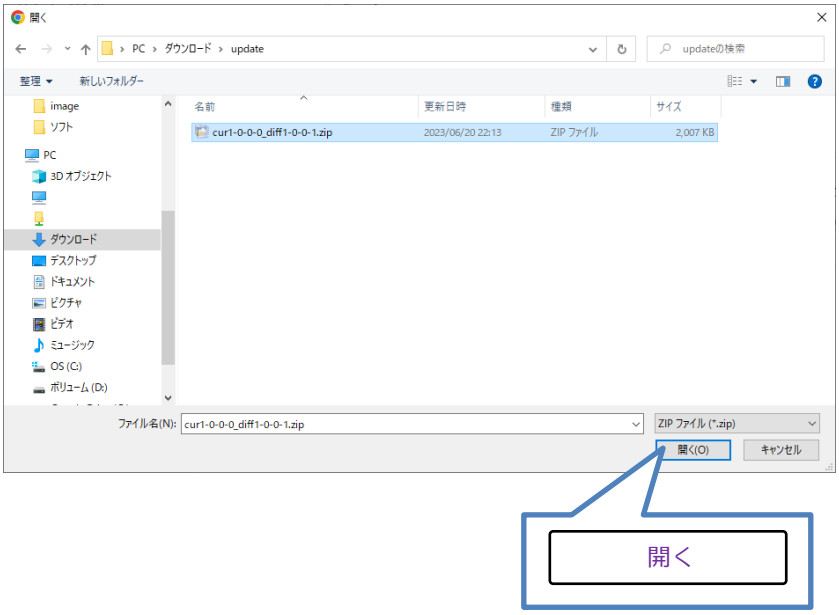
   「FW 管理」画面が表示されます。



2. 「ファイルを選択」ボタンをクリックし、ダウンロードしたアップデートプログラムファイル「＊.zip」を指定します。

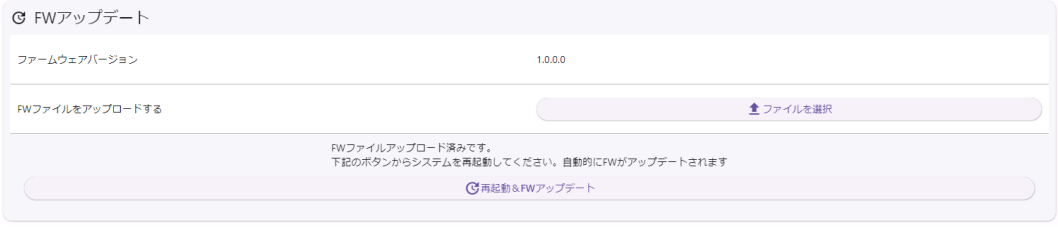
3. 弊社から提供するアップデートプログラムデータ「curx-x-x-x_diffy-y-y-y.zip」の選択し、「開く」をクリックします。

x-x-x-x 部分が現在のファームウェアバージョンと一致する事を確認してください。
y-y-y-y にアップデートされます。



4. 「FW ファイルアップロード済みです」が表示されましたら、「再起動&FW アップデート」ボタンをクリックします。

   SE が再起動し、FW アップデートが開始されます。



ファームウェアのアップデート完了するまで、5 分程度かかります。アップデート中は、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。
FW 更新中は POWER LED のみが点灯した状態となります。FW アップデートが完了すると自動的に SE が再起動します。

5. 十分に時間をおいてから Web 設定ツールをリロードして再度アクセスしてください。

ファームウェアのイメージファイルは数 MByte 以上になることがあります。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。

6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。

6-1. DDNSサービス

【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 SE にアクセスする場合、SE 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。SE では、変化するグローバル IP アドレスをダイナミック DNS サーバを利用する機能によって、上記問題を解決することができます。

1. Web 設定ツールのメニューから、［サービス］－［DDNS］をクリックし、「DDNS 設定」画面に入ります。

2. 以下の設定を行います。

設定項目	内容
機能を有効にする	DDNS サービスを使用する場合に有効に設定します。 ▶　初期設定では、［無効］に設定されています。
監視するインターフェース	IP アドレスの変化を監視するインターフェースを指定します。 「自動」、「モバイルインターフェース（APN1）」の何れかを選択します。 ▶　初期設定では、［自動］に設定されています。
強制登録間隔(分)	設定された時間（分）経過した際に、IP アドレスの変化がなくても強制的にサーバに IP アドレスの登録を行います。 ▶　初期設定では、［5 分］に設定されています。
DDNS プロバイダ	DDNS サービス提供者から提示されたプロバイダ名を設定します。 ▶　初期設定では、［www.suncomm.jp］に設定されています。
ユーザー名	DDNS サービス提供者から提示されたユーザー名を設定します。
パスワード	DDNS サービス提供者から提示されたパスワードを設定します。
ドメイン	DDNS サービス提供者から提示されたドメインを設定します。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

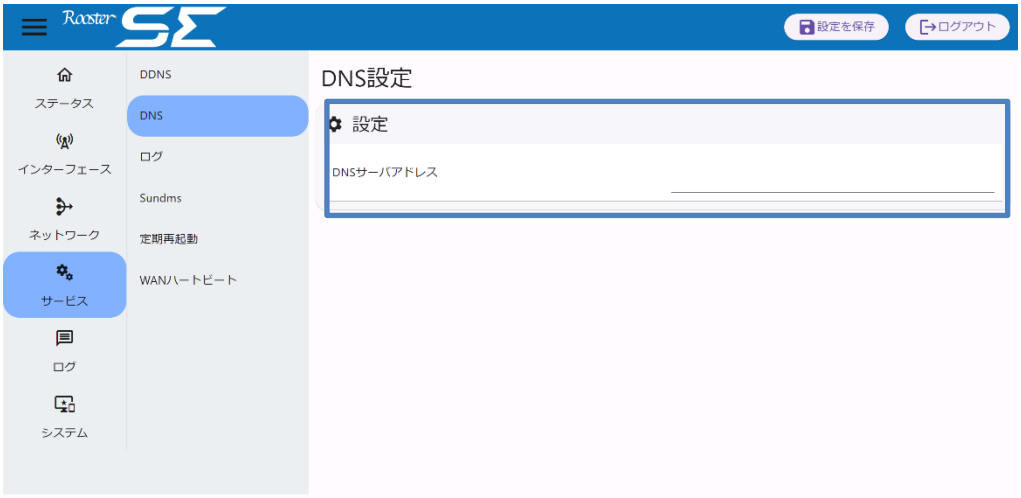
➔ 再起動の方法については、『4-9-1.再起動』を参照ください。

「www.suncomm.jp」プロバイダ以外についてはサポート対象外です。

6-2. DNSサービス

『3-4-2. DHCP 設定』が「無効」に設定されている場合は本サービスも無効となります。

1. Web 設定ツールのメニューから、［サービス］－［DNS］をクリックし、「DNS 設定」画面に入ります。



2. 以下の設定を行います。

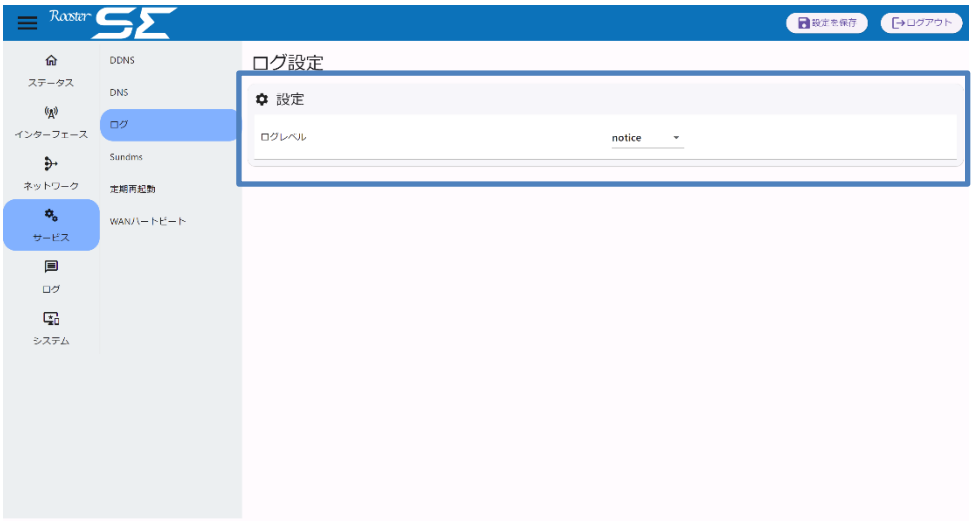
設定項目	内容
DNS サーバアドレス	設定された DNS サーバを使用してアドレス解決を行います。 ▶ 初期設定では、モバイルインターフェースから自動取得した DNS サーバを使用して名前解決されます。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

6-3. ログサービス

1. Web 設定ツールのメニューから、［サービス］－［ログ］をクリックし、「ログ設定」画面に入ります。



2. 以下の設定を行います。

設定項目	内容
ログレベル	出力するログのレベルを設定します。 ▶ 初期設定では、［notice］に設定されています。 設定可能項目： debug | information | notice | warning | error | critical | alert | emergency

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

特別な理由がない限り設定を変更しないことをお勧めしております。
「emergency」~「warning」以上を設定した場合弊社でサポートが必要な際に解析ができない場合がございます。

6-4. SunDMSサービス

【SunDMS について】
「SunDMS」は弊社が運用する、SE 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ことができます。
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/dms/

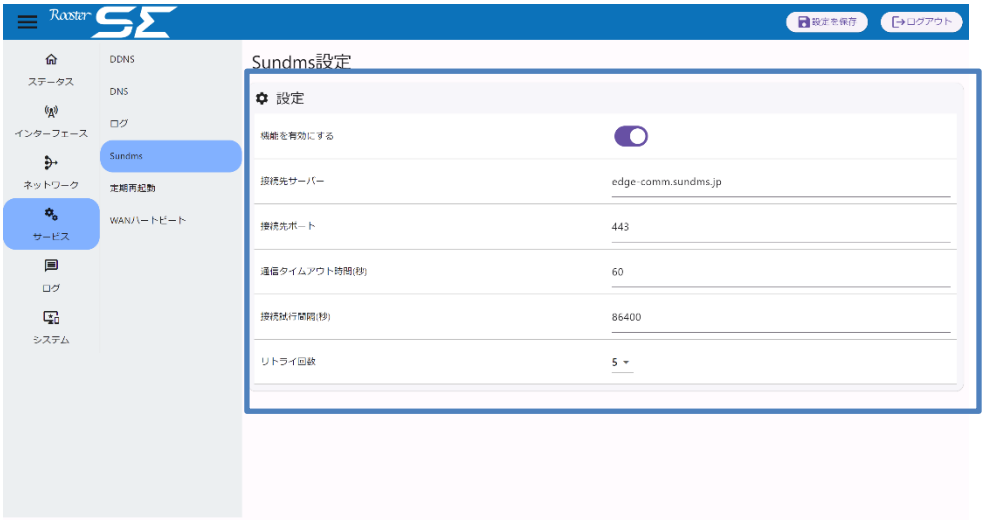
※SunDMS をご使用の際は、別途お申し込みが必要です。
　詳細につきましては、上記 URL もしくは、弊社営業部までお問い合わせください。
※一部有償サービスとなります。

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 10MByte 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. Web 設定ツールのメニューから、［サービス］－［SunDMS］をクリックし、「SunDMS 設定」画面に入ります。



2. 以下の設定を行います。

設定項目	内容
機能を有効にする	SunDMS 機能を使用しない場合は、本チェックボックスを無効に設定します。 ▶ 初期設定では、［有効］に設定されています。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

その他の項目は基本的に変更しないでください。

6-5. 定期再起動サービス

定期再起動サービスが有効で、適用されている場合は、シャットダウン後も通電中であればサービスが動作し続けます。設定した間隔の再起動時刻になった際に自動的に再起動します。

1. Web 設定ツールのメニューから、［サービス］－［定期再起動］をクリックし、「定期再起動設定」画面に入ります。

2. 以下の設定を行います。

設定項目	内容
機能を有効にする	自動再起動サービスを有効に設定します。 ▶ 初期設定では、［無効］に設定されています。
実行間隔（日）	設定された間隔（日）で定期的に再起動を行います。 ▶ 初期設定では、［1 日間隔］に設定されています。 設定範囲：1 ~ 7 (日)
再起動時刻（時）	設定された時刻（時）に再起動行います。 ▶ 初期設定では、［0 時］に設定されています。 設定範囲：0 ~ 23 (時)
再起動分散時間（分）	設定された分数内で SE のシリアル番号を元に計算された時間に再起動を行います。 再起動時刻 0 時、再起動分散時間を 20 分に設定した場合、 0 時 00 分 ~ 0 時 20 分の個体ごとにランダムな時間に再起動します。 ▶ 初期設定では、［0 分］に設定されています。 0 の場合、分散は行わず、設定された再起動時刻に再起動します。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

6-6. WANハートビートサービス

【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。
アクションは設定順に、基本設定に設定した監視条件が満たされるたびに繰り返し実行されます。

例：
SIM 切り替えアクションを 1 つ設定した場合
条件を満たす⇒SIM 切り替え実行⇒条件を満たす⇒SIM 切り替え実行

SIM 切り替えアクション、Sleep アクションを 1 つずつ設定した場合
条件を満たす⇒SIM 切り替え実行⇒Sleep 実行⇒条件を満たす⇒SIM 切り替え実行⇒Sleep 実行

【SunDMS WAN ハートビートについて】
送信モードを SunDMS に設定した場合、SunDMS WAN ハートビートとして動作します。
監視先ホストを設定する事が困難な場合に、信頼性の高い SunDMS サーバをハートビートの送信先として指定する事が出来る機能です。

1. Web 設定ツールのメニューから、［サービス］－［WAN ハートビート］をクリックし、「WAN ハートビート設定」画面に入ります。

2. 以下の設定を行います。

項目	内容
機能を有効にする	WAN ハートビートサービスの有効・無効を切り替えます。 工場出荷状態では、無効に設定されています。
送信モード	ハートビートの送信モードを選択します。 設定範囲: 通常 | SunDMS ※SunDMS モードは SunDMS 有償スタンダードサービス契約済みのお客様向けのモードです。

項目	内容
送信先	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、ドメイン名を手動で設定することもできます。
送信間隔(秒)	設定された間隔（秒）で WAN ハートビートを実行します。 ・設定範囲：1 ~ 600
送信タイムアウト(秒)	設定された時間（秒）実行した WAN ハートビートの応答を待ちます。この時間内に応答が送信先から無い場合失敗とカウントします。
アクション閾値(回)	設定された回数連続で WAN ハートビートが失敗した場合にアクションを実行します。
アクション ※複数設定可能	設定された回数連続で WAN ハートビートが失敗した場合に実行されます。 設定可能項目： SIM 切り替え | SIM 切り替え＋時間経過で切り戻し | Sleep | 再起動 SIM 切り替え： SIM スロットを現在使用していない別のスロットに切り替え、回線接続を行います。 SIM 切り替え+時間経過で切り戻し： 時間経過か切り替え先の SIM でハートビートが失敗した場合に切り替え前の SIM に切り戻します。 設定するには「時間経過で SIM を切り戻す」にチェックを入れ、「最大切り戻し時間」を設定します。 ※「時間経過で SIM を切り戻す」が有効で最大切り戻し時間が設定されている場合、SIM を切り戻すまで次のアクションは実行されません。 Sleep： 指定した秒数間何もせず待機します。 再起動： 本体を再起動します。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

6-7. Web設定ツール

【Web 設定ツールのアカウントロック機能について】
Web 設定ツールへのブルートフォース攻撃等の対策として、一定回数以上 Web 設定ツールへのログインに失敗した場合に、対象アカウントへのログインを３０分間ロックします。

【安全にお使い頂くために】
Rooster SE の Web 設定ツールは工場出荷時の設定では LAN インターフェース配下の機器からのみ接続可能な状態となっています。インターネット側からのアクセスを許可する場合には IPFilter の設定等が必要です。
Web 設定ツールを無条件でインターネットへ公開する場合、悪意を持った第３者等から攻撃を受け、SE の設定を変えられ運用不可の状態にされる等のリスクがあります。
使用環境や用途に応じて適切なアクセス制限を設定頂く事をお勧めしています。

Web 設定ツールをインターネットに公開しない(工場出荷時の設定)
MAC フィルタリング機能を使用して LAN インターフェース配下からアクセスできる機器を限定する
IP フィルタリング機能を使用して、アクセスが可能な機器を限定する
閉域網 SIM を使用して、通信経路全体が保護されたネットワークで使用する
VPN 機能を使用してセキュアなセッションを通してのみインターネット側からのアクセスができるようにする
Web 設定ツールの待ち受けポート番号を変更する

通信プロトコルを「http」に設定した場合、Web 設定ツールとデバイス間の通信が平文となり、パスワード等を盗み取られる恐れがあります。設定を行う際は注意をしてください。
待ち受けポートに他のサービスが使用しているポートは設定しないでください。
初期設定の場合の使用ポート：[22(CLI(SSH)), 443(Web 設定ツール), 53(DNS), 67(DHCP), 6000]

通信プロトコルを「http」に設定し、インターネット側からのアクセスを許可する場合は、Rooster SE と接続を行う機器間の通信経路全体が閉域網等保護されたネットワークで完結する環境又は、IPsec 接続設定を行う等により通信経路の全体にわたって保護される環境のいずれかで使用してください。

1. Web 設定ツールのメニューから、［サービス］－［Web 設定ツール］をクリックし、「Web 設定ツール設定」画面に入ります。

2. 以下の設定を行います。

設定項目	内容
通信プロトコル	使用する通信プロトコルを設定します。 ▶ 初期設定では、［https］に設定されています。 設定可能項目： http | https
待ち受けポート番号	待ち受けを行うポート番号を設定します。 ▶ 初期設定では、［443］に設定されています。 設定範囲：1 ~ 65535

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

6-8. CLI (SSH Server)

【CLI(SSH Server)機能について】
SSH で SE にアクセスして、各機能の設定、各種情報取得、メンテナンスを行う事が出来る機能です。CLI の使用方法や使用できるコマンドについては、「RoosterSE_CLI 設定機能説明書」をご確認ください。ここでは CLI 設定機能を使用する為の SSH Server に関わる設定を行うことが出来ます。

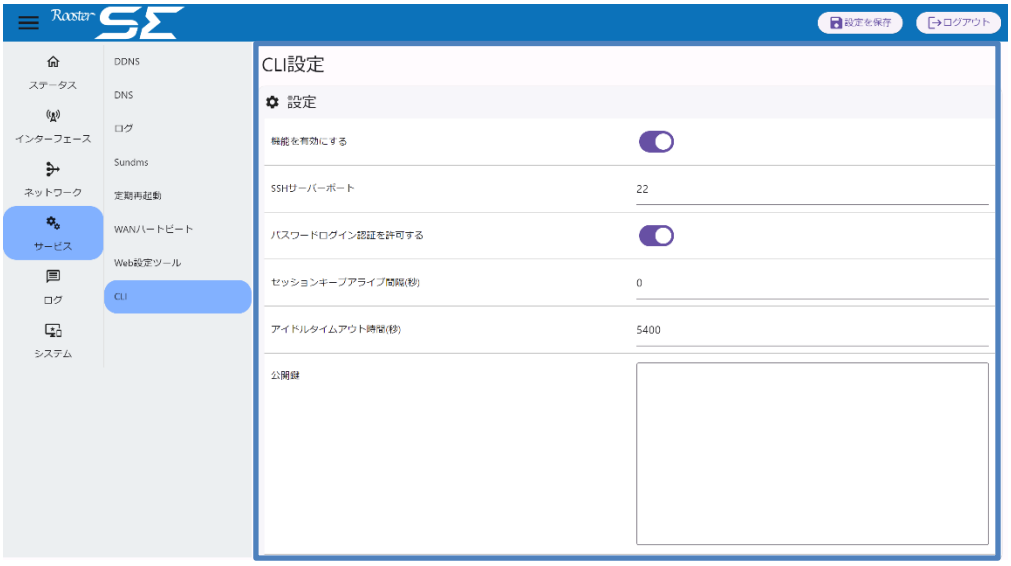
【CLI(SSH Server)機能のアカウントロック機能について】
CLI(SSH Server)へのブルートフォース攻撃等の対策として、ログイン認証に失敗し切断したクライアントに対して一定時間の接続拒否ペナルティを付与します。

【安全にお使い頂くために】
Rooster SE の CLI は工場出荷時の設定では LAN インターフェース配下の機器からのみ接続可能な状態となっています。インターネット側からのアクセスを許可する場合には IPFilter の設定等が必要です。
CLI を無条件でインターネットへ公開する場合、悪意を持った第 3 者等から攻撃を受け、SE の設定を変えられ運用不可の状態にされる等のリスクがあります。
使用環境や用途に応じて適切なアクセス制限を設定頂く事をお勧めしています。

CLI をインターネットに公開しない(工場出荷時の設定)
MAC フィルタリング機能を使用して LAN インターフェース配下からアクセスできる機器を限定する
IP フィルタリング機能を使用して、アクセスが可能な機器を限定する
閉域網 SIM を使用して、通信経路全体が保護されたネットワークで使用する
VPN 機能を使用してセキュアなセッションを通してのみインターネット側からのアクセスができるようにする
CLI の待ち受けポート番号を変更する

公開鍵認証では一部使用できないプロトコルがあります。
弊社では、「ECDSA-256」、「ECDSA-384」、「ECDSA-521」、「ED25519」でログインが出来ることを確認しております。
パスワードログイン認証機能を無効にした場合、公開鍵認証でしかログインできません。注意してください。
初期設定では、LAN 側からのみ SSH Server へのアクセスが可能な IP フィルタルールが設定されています。お使いの環境に合わせて、IP フィルターの設定も変更してください。
SSH サーバーポートに他のサービスが使用しているポートは設定しないでください。
初期設定の場合の使用ポート：[22(CLI(SSH)), 443(Web 設定ツール), 53(DNS), 67(DHCP), 6000]

1. Web 設定ツールのメニューから、［サービス］－［CLI］をクリックし、「CLI 設定」画面に入ります。



2. 以下の設定を行います。

設定項目	内容
機能を有効にする	SSH Server 機能の有効・無効を設定します。 ▶ 初期設定では、［有効］に設定されています。 ※ v1.2.0.X 未満から FW アップデートした端末で、v1.2.0.X 未満で作成した設定情報を使用している場合は初期状態が「無効」になります。
SSH サーバーポート	待ち受けを行うポート番号を設定します。 ▶ 初期設定では、［22］に設定されています。 設定範囲：1 ~ 65535
パスワードログイン認証機能を許可する	パスワードでのログインを許可するかを設定します。 ▶ 初期設定では、「有効」に設定されています
セッションキープアライブ間隔(秒)	SSH Server からクライアントへ生存確認パケットを送信する間隔を設定します。「0」を設定した場合は、キープアライブパケットは送信されません。 ▶ 初期設定では、「0」に設定されています。
アイドルタイムアウト時間(秒)	一定時間通信がない場合に、セッションを切断するまでの時間を設定します。 「0」を設定した場合は、アイドルタイムアウトが無効になります。 ▶ 初期設定では、「5400」に設定されています。
公開鍵	公開鍵認証で使用する「admin」ユーザーの公開鍵を設定します。 設定範囲：最大 512 文字

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

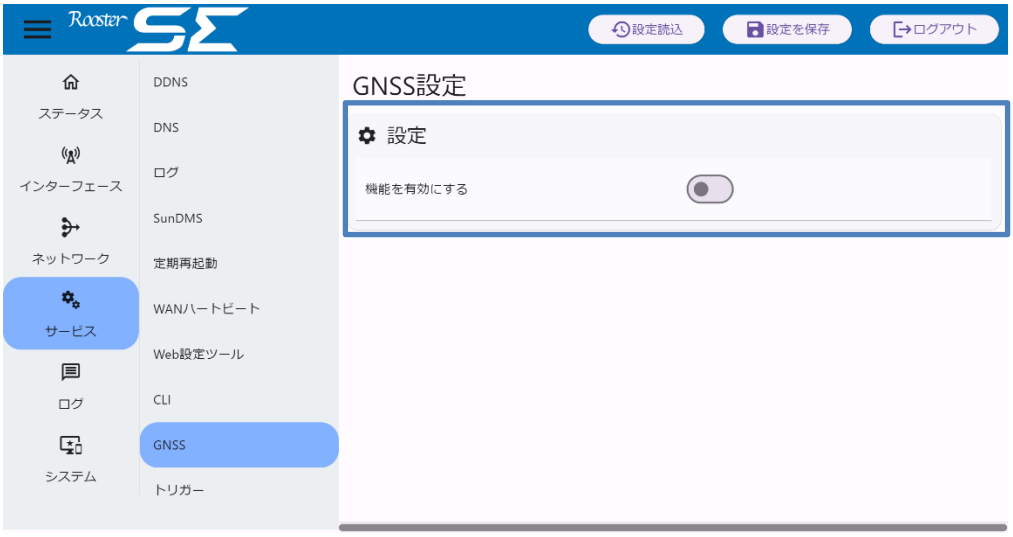
➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

6-9. GNSS

【GNSS 機能について】
GNSS 機能は衛星から信号を受信して位置情報を取得する為の機能です。
本機能が有効に設定されている場合、起動時に通信モジュールの GNSS 測位機能を有効にし、位置測位を開始します。本機能が有効な場合、Web 設定ツール及び CLI で、現在地の取得が可能になります。又、SunDMS サーバへの位置情報の送信が行われます。

別途 GNSS 信号受信用アンテナが必要となります。
場所や環境によっては衛星からの信号をうまく受信できず位置情報の測位が出来ない可能性が有ります。

1. Web 設定ツールのメニューから、［サービス］－［GNSS］をクリックし、「GNSS 設定」画面に入ります。



2. 以下の設定を行います。

設定項目	内容
機能を有効にする	GNSS 機能の有効・無効を設定します。 ▶ 初期設定では、［無効］に設定されています。

3. ［設定を保存］ボタンをクリックして、設定を保存します。
4. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

6-10. トリガー

【トリガー機能について】
トリガー機能は設定されたイベントを契機に単一のアクションを行う機能です。

1. Web 設定ツールのメニューから、［サービス］－［トリガー］をクリックし、「トリガー設定」画面に入ります。

2. 以下の設定を行います。

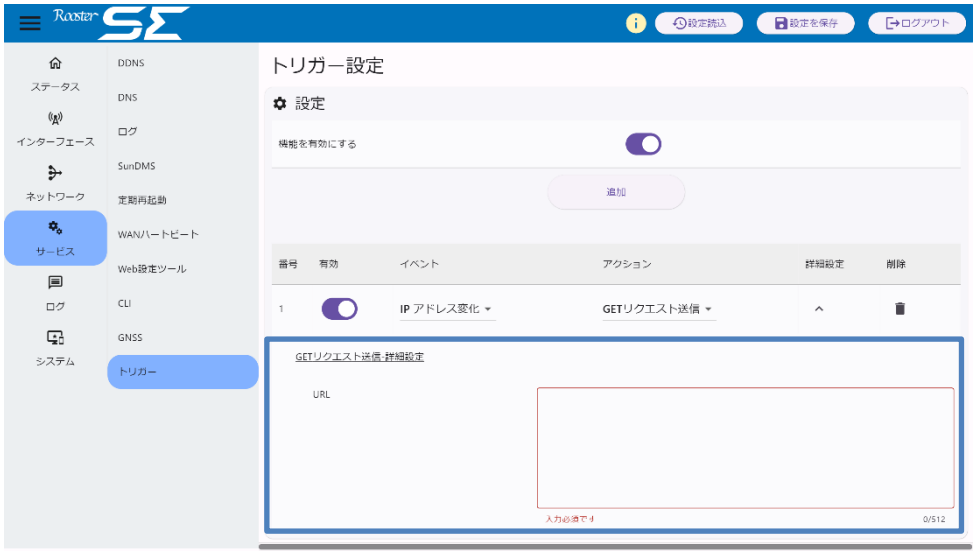
設定項目	内容
機能を有効にする	トリガー機能の有効。無効を設定します。 ▶ 初期設定では、［無効］に設定されています。

3. トリガー設定を追加するには「追加」ボタンをクリックします。

4. 以下の設定を行います。

設定項目	内容
有効	トリガー設定の有効。無効を設定します。 ▶ 設定追加段階では、［有効］になります。
イベント	アクションを実行する契機となるイベントを設定します。
アクション	イベントが発生した場合に実行するアクションを設定します。
詳細設定	イベント・アクションの詳細な設定を行います。
削除	トリガー設定を削除します。

5. ［詳細設定］ボタンをクリックし、設定したイベント・アクションについての詳細な設定を行います。



イベントの詳細設定：

イベント名	設定項目	内容
IP アドレス変化	なし	

アクションの詳細設定：

イベント名	設定項目	内容
GET リクエスト送信	URL	GET リクエストを送信する最大 512 文字の URL を設定します。 ※http 又は https から始まる文字列を指定してください。

6. ［設定を保存］ボタンをクリックして、設定を保存します。
7. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

7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。

7-1. MACフィルタリング

> 有効なルールが 1 件もない場合は、LAN インターフェース向けのすべての通信が許可されます。有効なルールが 1 件でもある場合は、有効なルールの MAC アドレスを持つ端末からの通信のみが許可されます。設定を誤った場合等にイーサネット経由で設定ツールにアクセスできなくなる可能性が有るため、慎重に設定を行ってください。
> ※本ルールで許可されたパケットはその後『7-3. IP フィルター』のルールに従い処理されます

1. Web 設定ツールのメニューから、［ネットワーク］－［MAC フィルタリング］をクリックし、「MAC フィルター設定」画面に入ります。

2. ルールを追加するには「追加」ボタンをクリックします。

3. 下記について設定します。

設定項目	内容
MAC アドレス	通信を許可する端末の MAC アドレスを入力します。
有効	該当のルールを有効にします。 無効に設定された場合は該当のルールが無視されます。 ▶ ルールを追加後は「有効」に設定されています。
削除	該当のルールを削除したい場合に使用します。 ボタンをクリックすると該当のルールが削除されます。

4. ［設定を保存］ボタンをクリックして、設定を保存します。
5. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

memo MAC フィルタリングの設定は最大 10 件まで行えます。

7-2. スタティックルーティング

1. Web 設定ツールのメニューから、［ネットワーク］－［ルーティング］をクリックし、「ルーティング設定」画面に入ります。

2. 設定を追加するには「追加」ボタンをクリックします。

3. 以下の設定を行います。

設定項目	内容
宛先アドレス	宛先ネットワークアドレスを入力します。 ▶ 入力は必須です。
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。
出力インターフェース	この設定を適用するインターフェースを選択します。 設定項目： LAN インターフェース | モバイルインターフェース（APN1）
ネクストホップアドレス	ネクストホップのアドレスを入力します。 ▶ 入力は任意です。
削除	該当の設定を削除します。 削除するにはボタンをクリックします。

4. ［設定を保存］ボタンをクリックして、設定を保存します。
5. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

memo スタティックルートの設定は最大 10 件まで行えます。

7-3. IPフィルター

SE はパケットを送受信する際に下記の図のような順序でパケットを処理します。「ローカル/プロセス」は、SE 内で動作しているプロセスでパケットの送受信を行うものを指します。（Web 設定ツール、SSH サーバ、SunDMS プロセス等）

適切なルールを設定する事で悪意を持つ第 3 者からの攻撃や不正アクセスなどを遮断し、防ぐことが出来ます。

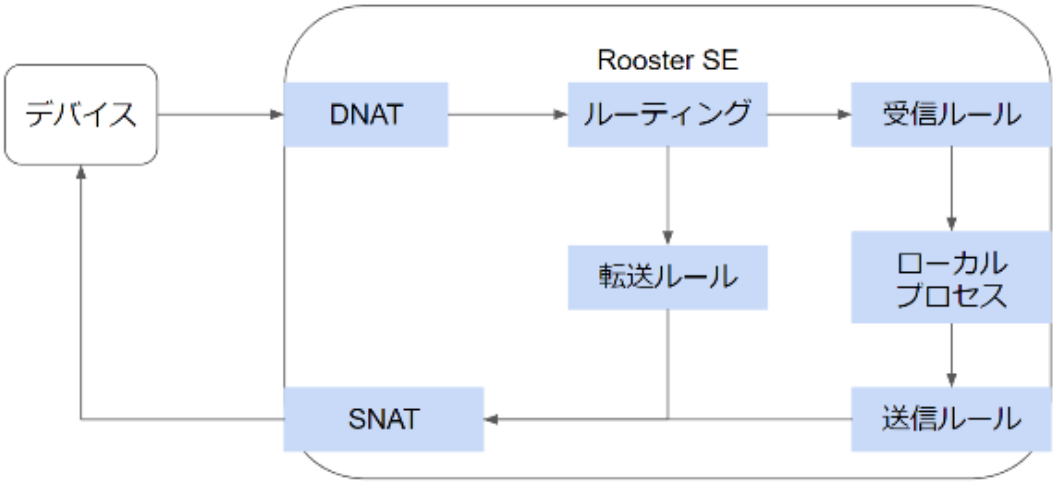
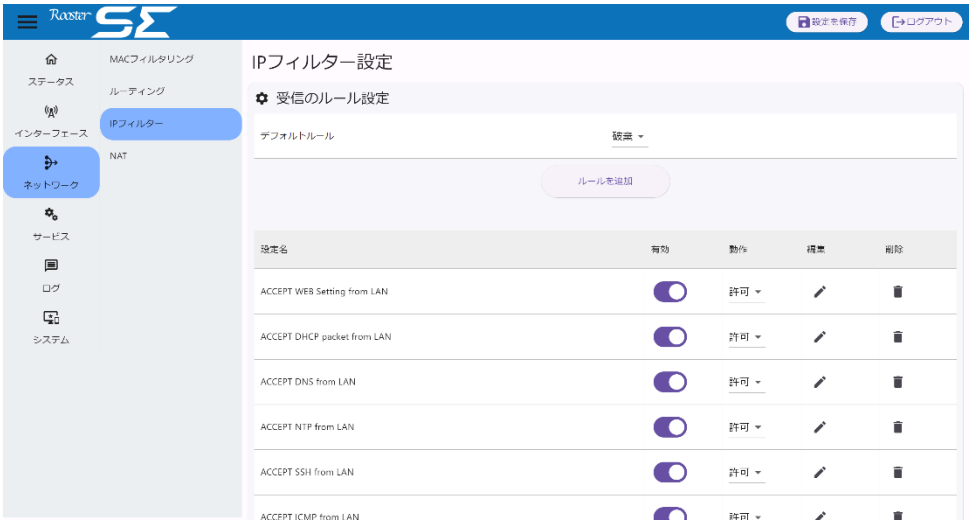


図 7-3-1 パケット処理の流れ

Web 設定ツールのメニューから、［ネットワーク］－［IP フィルター］をクリックし、「IP フィルター設定」画面に入ります。



memo IP フィルターの設定は各ルール最大 32 件まで行えます。

7-3-1. 受信のルール

受信のルールは、は下記の図のように青線の経路を通る通信の際に適用されます。SE の WEB 設定ツールや、CLI へアクセスする為の通信等、主に SE の各インターフェスに割り当てられたアドレス宛の通信がマッチします。

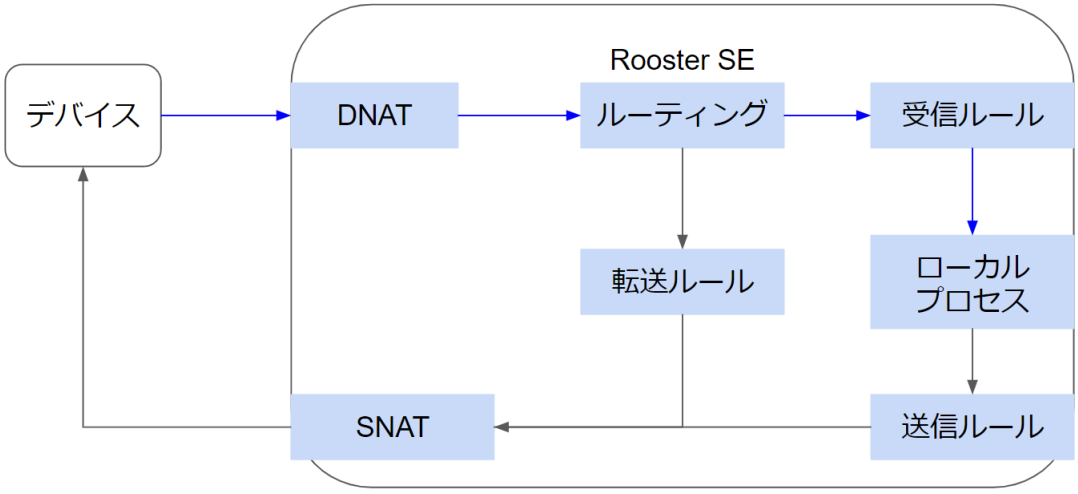
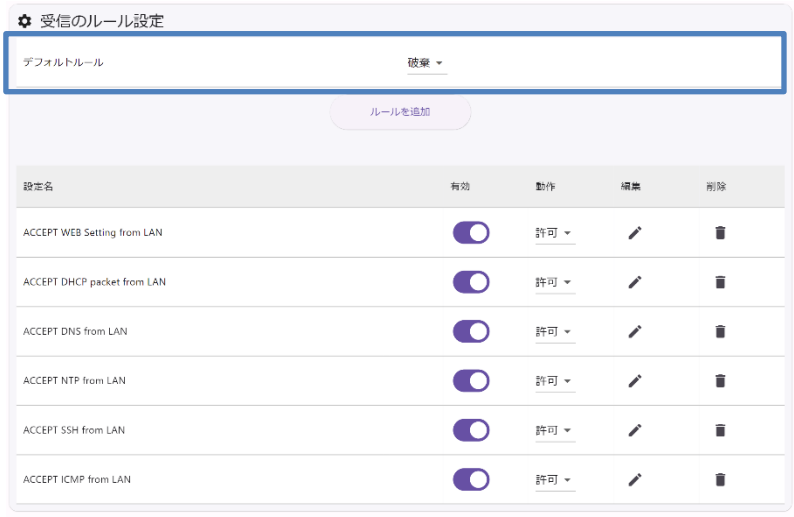


図 7-3-1-1 受信ルール適用時のパケットの流れ

工場出荷状態では、PC と SE を LAN ケーブルで接続してセットアップするための必要最低限のルールが設定されています。設定されているルールの削除、編集したりすると設定ツールにアクセスできなくなってしまったりする可能性が有ります。工場出荷状態のルールを止むを得ず削除する場合は慎重に行ってください。
Web 設定ツールや CLI のポート番号の設定を変更する場合は IP フィルターの受信のルールの追加又は変更が必要です。

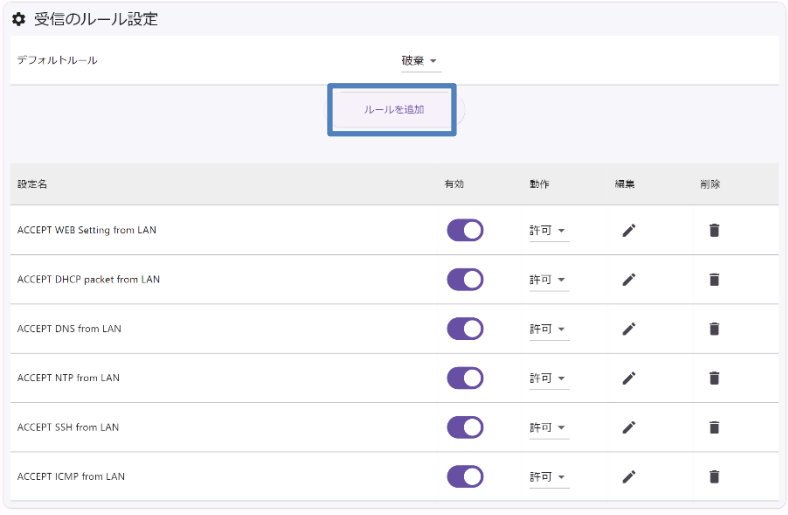
工場出荷状態では、デフォルトルールが「破棄」に設定されており、外部からの不正なパケット等を遮断しています。デフォルトルールを「許可」に設定すると、外部からの不正なパケット等を通してしまう可能性が有りますので、気を付けて設定を行ってください。
又、インターネット経由で SE の WEB 設定ツール及び CLI にアクセスできるようにすると、悪意を持った第 3 者からの不正アクセス攻撃を受けやすくなります。次のような対策を講じ、不正アクセスを受けにくくして頂く事をお勧めします。
① ログインパスワードを強固なものにする。
②「送信元 IP アドレス/プレフィックス」設定や、「送信元ポート/範囲」を設定し、アクセスできるデバイスの範囲を制限する。
③WEB 設定ツール、CLI の待ち受けポートを変更し、Well Known ポートを使用しないようにする。

1. デフォルトルールを変更する場合は下記について設定を行います。



設定項目	内容
デフォルトルール	設定されている個別のルールにマッチしない通信について適用される基本的なルールを設定します。 ▶ 初期設定では、［破棄］に設定されています。

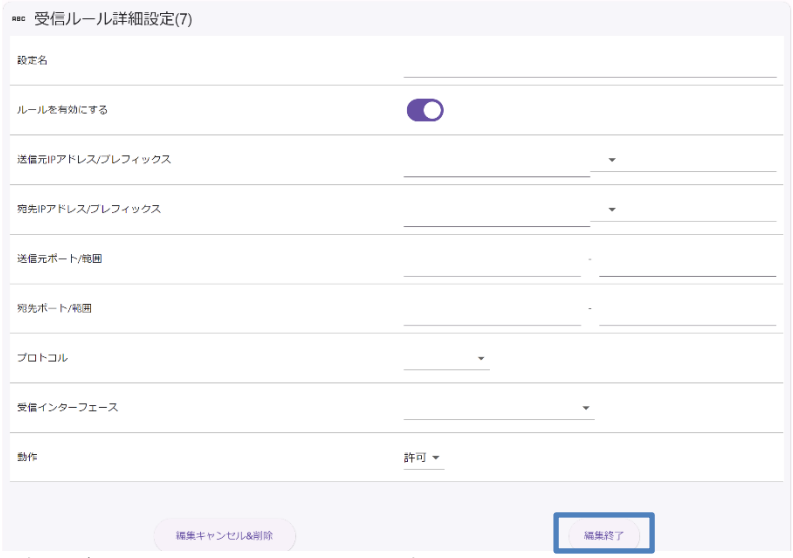
2. ルールを追加するには「ルールを追加」ボタンをクリックします。



3. 詳細設定画面が表示されます。下記について設定を行います。

設定項目	内容
設定名	任意の識別名を設定します。設定された値は動作に影響しません。
ルールを有効にする	該当のルールを有効に設定します。一時的にルールを無効にしたい場合等に無効に設定してください。 ▶ 初期設定時は「有効」に設定されています。
送信元 IP アドレス/プレフィックス	送信元の IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
宛先 IP アドレス/プレフィックス	宛先 IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
送信元ポート/範囲	送信元のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
宛先ポート/範囲	宛先のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［数字指定する］のいずれかを指定します。 ［数字指定する］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「数字指定する」を選択した場合は、プロトコル番号を設定します。
ICMP タイプ	「プロトコル」にて「ICMP」を選択した場合は、ICMP タイプを設定します。 「全て」、「Echo reply」、「Echo request」、「数字指定する」のいずれかを選択します。
ICMP タイプ/コード番号	「ICMP タイプ」にて「数字指定する」を選択した場合は ICMP タイプとコードの番号を設定します。
受信インターフェース	この設定を適用する受信方向のインターフェースを選択します。 「空白」、「LAN インターフェース」、「モバイルインターフェース（APN1）」の何れかを選択します。 空白： 全てのインターフェースが対象となります。 LAN インターフェース：LAN インターフェースで受信したパケットが対象となります。 モバイルインターフェース（APN１）：モバイルインターフェース（APN１）で受信したパケットが対象となります。
動作	このルールにマッチしたパケットをどうするか設定します。 「許可」、「破棄」、「拒否」の何れかを選択します。

4. 設定後、「編集終了」ボタンをクリックします。
   ▶ 編集を途中でやめたい場合、ルールの追加をやめる場合は「編集キャンセル＆削除」ボタンをクリックします。



5 「設定を保存」ボタンをクリックして設定を保存します。

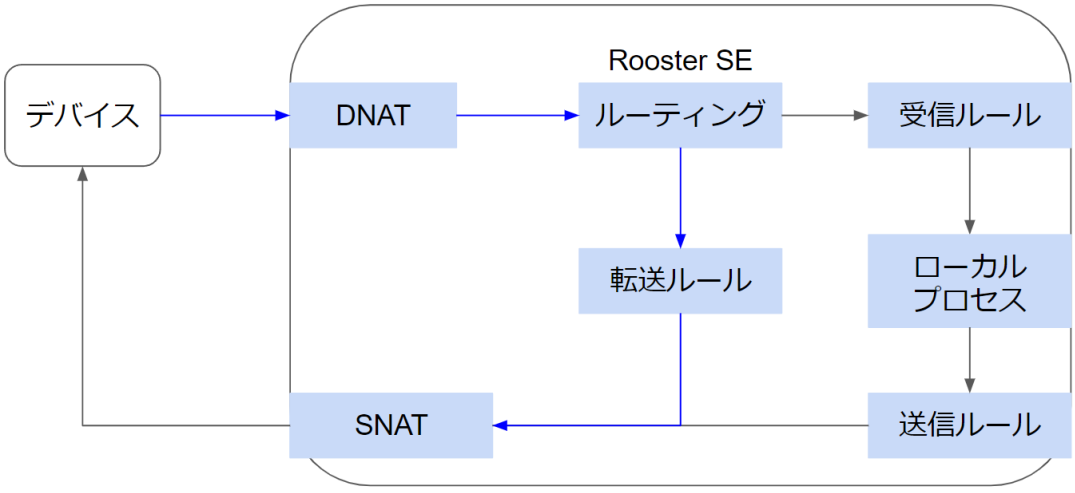
6. 設定を適用する場合は、SE を再起動します。

> ➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

7-3-2. 転送のルール

転送のルールは、下記の図の青線の経路を通るパケットにマッチします。例えばデバイスから、インターネット上のサーバへアクセスする通信等、ルーティングによってパケットが転送される通信にマッチします。

例えば DNAT 設定を行い遠隔地から SE の LAN 配下に接続されているデバイスと通信をする場合、図の「DNAT」部でパケットが処理され、宛先アドレス・ポートが変換されます。変換されたパケットは、「ルーティング」部で処理され「転送ルール」を通り、LAN インターフェースから LAN 配下のデバイスに転送される流れとなり「転送のルール」にマッチします。



1. デフォルトルールを変更する場合は下記について設定を行います。

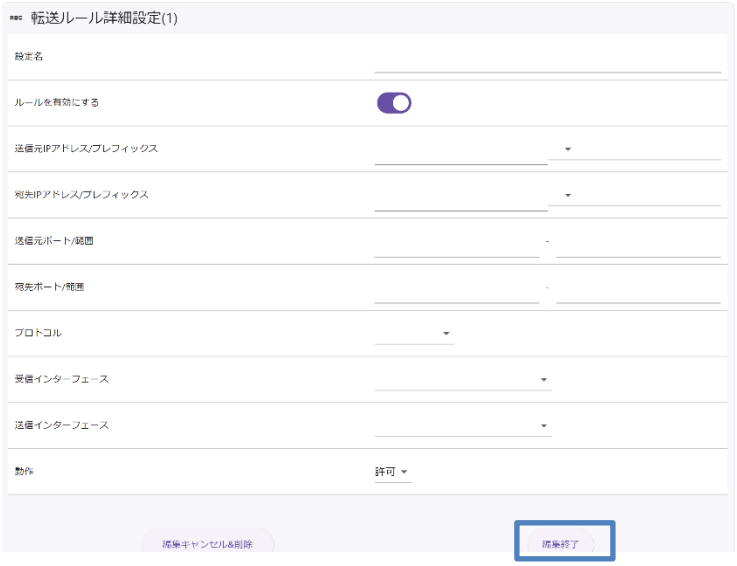
設定項目	内容
デフォルトルール	設定されている個別のルールにマッチしない通信について適用される基本的なルールを設定します。 ▶ 初期設定では、［許可］に設定されています。

2. ルールを追加するには「ルールを追加」ボタンをクリックします。

3. 詳細設定画面が表示されます。下記について設定を行います。

設定項目	内容
設定名	任意の識別名を設定します。設定された値は動作に影響しません。
ルールを有効にする	該当のルールを有効に設定します。一時的にルールを無効にしたい場合等に無効に設定してください。 ▶ 初期設定時は「有効」に設定されています。
送信元 IP アドレス/プレフィックス	送信元の IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
宛先 IP アドレス/プレフィックス	宛先 IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
送信元ポート/範囲	送信元のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
宛先ポート/範囲	宛先のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［数字指定する］のいずれかを指定します。 ［数字指定する］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「数字指定する」を選択した場合は、プロトコル番号を設定します。
ICMP タイプ	「プロトコル」にて「ICMP」を選択した場合は、ICMP タイプを設定します。 「全て」、「Echo reply」、「Echo request」、「数字指定する」のいずれかを選択します。
ICMP タイプ/コード番号	「ICMP タイプ」にて「数字指定する」を選択した場合は ICMP タイプとコードの番号を設定します。
受信インターフェース	この設定を適用する受信方向のインターフェースを選択します。 「空白」、「LAN インターフェース」、「モバイルインターフェース（APN1）」の何れかを選択します。 空白： 全てのインターフェースが対象となります。 LAN インターフェース：LAN インターフェースで受信したパケットが対象となります。 モバイルインターフェース（APN 1）：モバイルインターフェース（APN 1）で受信したパケットが対象となります。
送信インターフェース	この設定を適用する送信方向のインターフェースを選択します。 「空白」、「LAN インターフェース」、「モバイルインターフェース（APN1）」の何れかを選択します。 空白： 全てのインターフェースが対象となります。 LAN インターフェース：LAN インターフェースから送信されるパケットが対象となります。 モバイルインターフェース（APN 1）：モバイルインターフェース（APN 1）から送信されるパケットが対象となります。
動作	このルールにマッチしたパケットをどうするか設定します。 「許可」、「破棄」、「拒否」の何れかを選択します。

4. 設定後、「編集終了」ボタンをクリックします。
   ▶ 編集を途中でやめたい場合、ルールの追加をやめる場合は「編集キャンセル＆削除」ボタンをクリックします。

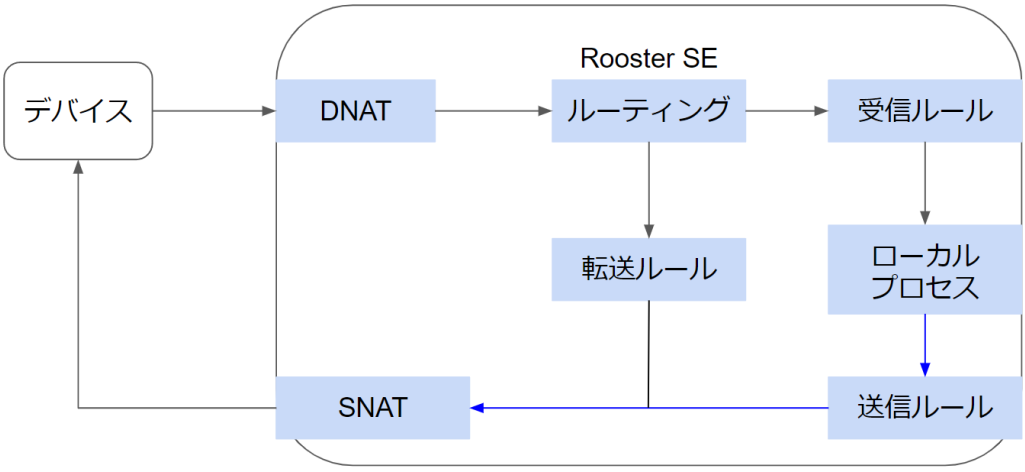


5. 「設定を保存」ボタンをクリックして設定を保存します。
6. 設定を反映する場合は SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

7-3-3. 送信のルール

送信のルールは図の青線の経路を通るパケットにマッチします。主に、SE の「ローカル/プロセス」からパケットを送信する場合にマッチします。（SE から SunDMS サーバへの通信等）



工場出荷状態では、デフォルトルールが「許可」に設定されています。「破棄」に設定する場合、SE から送信する通信が破棄され、一部の機能が使用できなくなる可能性が有ります。送信のルールを設定する際は、必要に応じて下記の通信を「許可」する設定を追加してください。

①「ホスト名の名前解決」：
宛先ポート：53
プトロコル：UDP

➔ SE がホスト名の解決を行うために必要な設定です。②～⑥でも本設定が必要となります。

②「SunDMS」機能：
宛先ポート：443
プロトコル：TCP
送信インターフェース：モバイルインターフェース(APN1)

③「DDNS」機能
宛先ポート：80
プロトコル：TCP
送信インターフェース：モバイルインターフェース（APN1）

④「トリガー」機能
宛先ポート：GET リクエスト送信先のポート番号
プトロコル：TCP

⑤「WAN ハートビート」機能：
プロトコル：ICMP
ICMP タイプ：Echo request

⑥「SunDMS WAN ハートビート」機能：
宛先 IP アドレス: ハートビート送信先のアドレス
プロトコル:ICMP
ICMP タイプ:Echo request

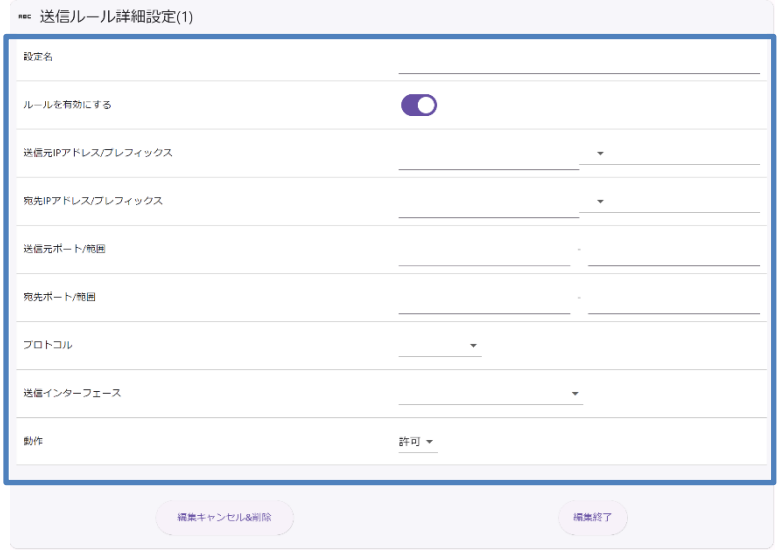
⑦「SunDMS 後位端末死活監視」機能：
宛先 IP アドレス: ハートビート送信先のアドレス
プロトコル:ICMP
ICMP タイプ:Echo request

1. デフォルトルールを変更する場合は下記について設定を行います。

設定項目	内容
デフォルトルール	設定されている個別のルールにマッチしない通信について適用される基本的なルールを設定します。 ▶ 初期設定では、［許可］に設定されています。

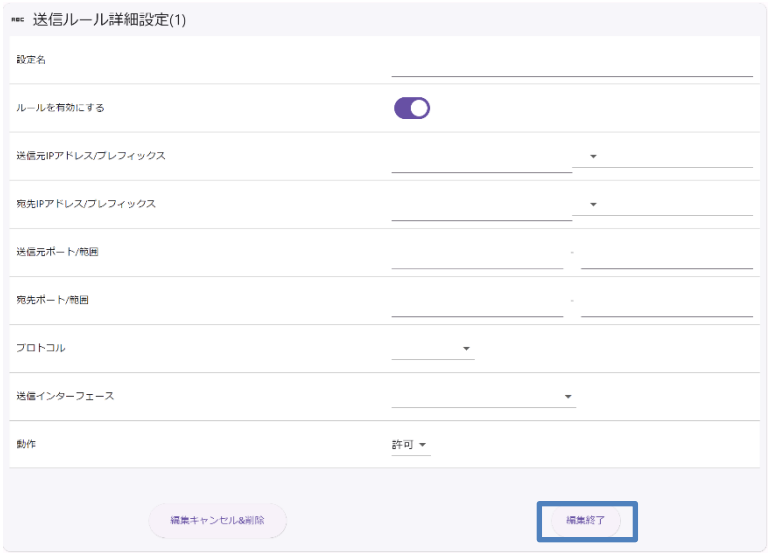
2. ルールを追加するには「ルールを追加」ボタンをクリックします。

3. 詳細設定画面が表示されます。下記について設定を行います。



設定項目	内容
設定名	任意の識別名を設定します。設定された値は動作に影響しません。
ルールを有効にする	該当のルールを有効に設定します。一時的にルールを無効にしたい場合等に無効に設定してください。 ▶ 初期設定時は「有効」に設定されています。
送信元 IP アドレス/プレフィックス	送信元の IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
宛先 IP アドレス/プレフィックス	宛先 IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
送信元ポート/範囲	送信元のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
宛先ポート/範囲	宛先のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［数字指定する］のいずれかを指定します。 ［数字指定する］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「数字指定する」を選択した場合は、プロトコル番号を設定します。
ICMP タイプ	「プロトコル」にて「ICMP」を選択した場合は、ICMP タイプを設定します。 「全て」、「Echo reply」、「Echo request」、「数字指定する」のいずれかを選択します。
ICMP タイプ/コード番号	「ICMP タイプ」にて「数字指定する」を選択した場合は ICMP タイプとコードの番号を設定します。
送信インターフェース	この設定を適用する送信方向のインターフェースを選択します。 「空白」、「LAN インターフェース」、「モバイルインターフェース（APN1）」の何れかを選択します。 空白： 全てのインターフェースが対象となります。 LAN インターフェース：LAN インターフェースから送信されるパケットが対象となります。 モバイルインターフェース（APN 1）：モバイルインターフェース（APN 1）から送信されるパケットが対象となります。
動作	このルールにマッチしたパケットをどうするか設定します。 「許可」、「破棄」、「拒否」の何れかを選択します。

4. 設定後、「編集終了」ボタンをクリックします。
   ▶ 編集を途中でやめたい場合、ルールの追加をやめる場合は「編集キャンセル＆削除」ボタンをクリックします。



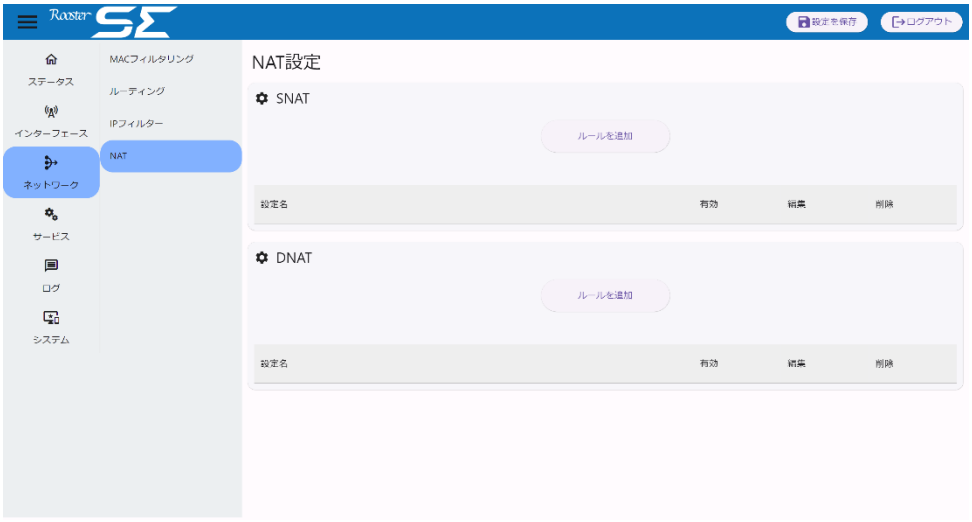
5. 「設定を保存」ボタンをクリックして設定を保存します。
6. 設定を反映する場合は SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

7-4. NAT

NAT 機能は、送信元・宛先の IP アドレスやポート番号を変換する際に使用する機能です。
遠隔地から SE の LAN 配下の機器へアクセスする場合等、ポートフォワード設定を行う場合は DNAT 設定を行い、宛先 IP・ポートを変換する事でアクセスが可能になります。

Web 設定ツールのメニューから、［ネットワーク］－［NAT］をクリックし、「NAT 設定」画面に入ります。

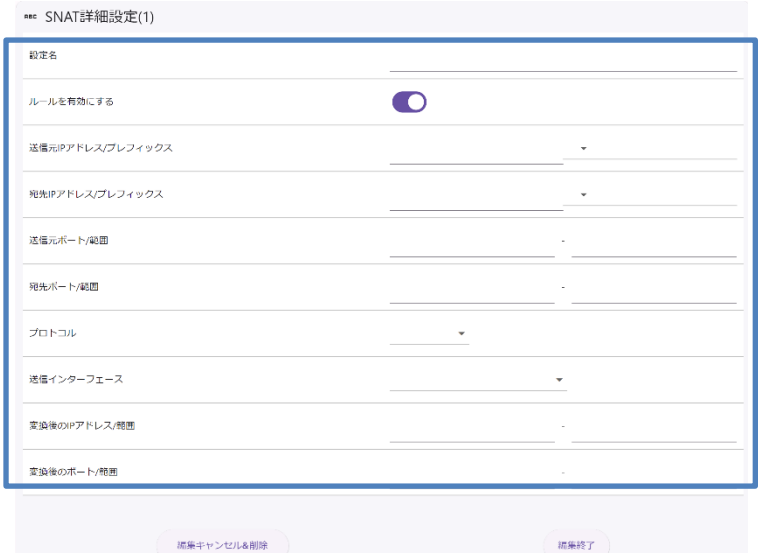


NAT の設定は SNAT、DNAT それぞれ最大 32 件まで行えます。

7-4-1. SNAT

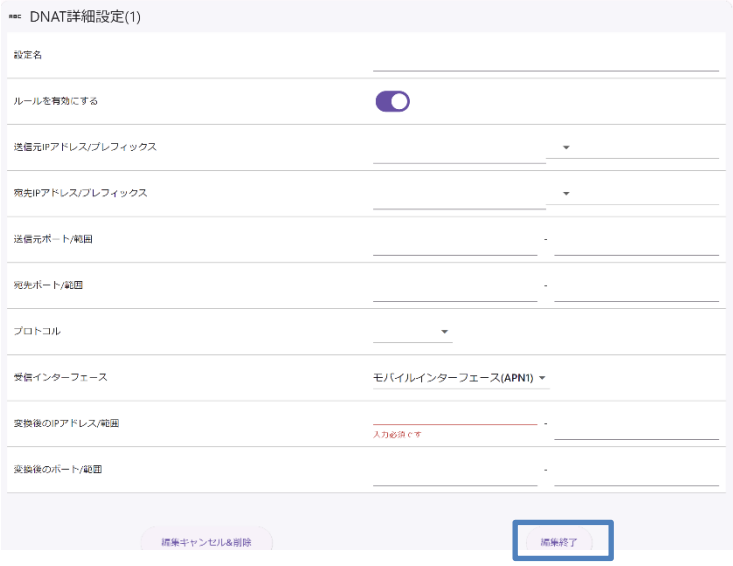
1. ルールを追加するには「ルールを追加」ボタンをクリックします。

2. 詳細設定画面が表示されます。下記について設定を行います。



設定項目	内容
設定名	任意の識別名を設定します。設定された値は動作に影響しません。
ルールを有効にする	該当のルールを有効に設定します。一時的にルールを無効にしたい場合等に無効に設定してください。 ▶ 初期設定時は「有効」に設定されています。
送信元 IP アドレス/プレフィックス	送信元の IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
宛先 IP アドレス/プレフィックス	宛先 IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
送信元ポート/範囲	送信元のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
宛先ポート/範囲	宛先のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［数字指定する］のいずれかを指定します。 ［数字指定する］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「数字指定する」を選択した場合は、プロトコル番号を設定します。
送信インターフェース	この設定を適用する送信方向のインターフェースを選択します。 「空白」、「LAN インターフェース」、「モバイルインターフェース（APN1）」の何れかを選択します。 空白： 全てのインターフェースが対象となります。 LAN インターフェース：LAN インターフェースから送信されるパケットが対象となります。 モバイルインターフェース（APN1）：モバイルインターフェース（APN1）から送信されるパケットが対象となります。 IPsec インターフェース 1~4: IPsec インターフェースから送信されるパケットが対象となります。
変換後の IP アドレス/範囲	変換後の IP アドレスとその範囲を設定します。 設定は任意です。192.0.2.1 – 192.0.2.10 と設定した場合は、192.0.2.1 から 192.0.2.10 までの IP アドレスに変換されます。 192.0.2.1 – と設定した場合は、192.0.2.1 に変換されます。
変換後のポート/範囲	変換後のポート番号を設定します。 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートの範囲で変換されます。1 – と設定した場合は、1 番ポートに変換されます。

3. 設定後、「編集終了」ボタンをクリックします。
   ▶ 編集を途中でやめたい場合、ルールの追加をやめる場合は「編集キャンセル＆削除」ボタンをクリックします。



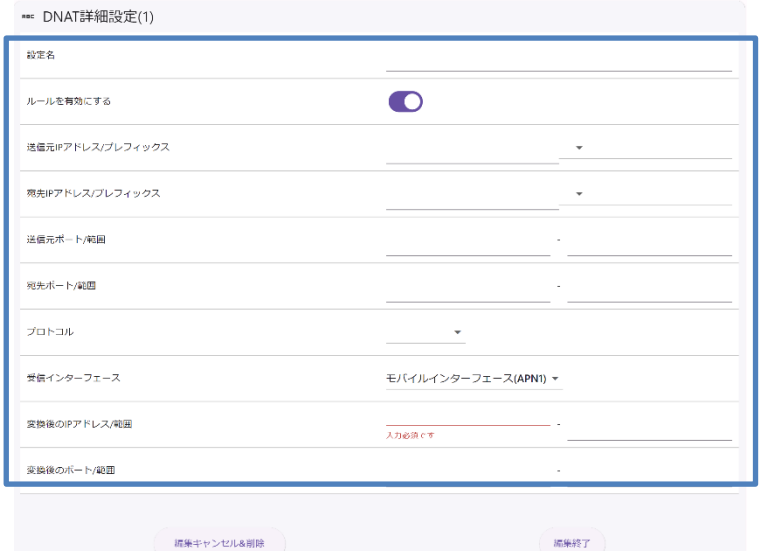
4. 「設定を保存」ボタンをクリックして設定を保存します。
5. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

7-4-2. DNAT

1. ルールを追加するには「ルールを追加」ボタンをクリックします。

2. 詳細設定画面が表示されます。下記について設定を行います。



設定項目	内容
設定名	任意の識別名を設定します。設定された値は動作に影響しません。
ルールを有効にする	該当のルールを有効に設定します。一時的にルールを無効にしたい場合等に無効に設定してください。 ▶ 初期設定時は「有効」に設定されています。
送信元 IP アドレス/プレフィックス	送信元の IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
宛先 IP アドレス/プレフィックス	宛先 IP アドレスとそのプレフィックスを設定します。 ▶ 設定は任意です。プレフィックスを設定した場合は、IP アドレスも設定する必要があります。
送信元ポート/範囲	送信元のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
宛先ポート/範囲	宛先のポート番号を設定します。 ▶ 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートが対象となります。1 – と設定した場合は、1 番ポートのみ対象となります。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［数字指定する］のいずれかを指定します。 ［数字指定する］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「数字指定する」を選択した場合は、プロトコル番号を設定します。
受信インターフェース	この設定を適用する受信方向のインターフェースを選択します。 「LAN インターフェース」、「モバイルインターフェース（APN1）」の何れかを選択します。 LAN インターフェース：LAN インターフェースで受信したパケットが対象となります。 モバイルインターフェース（APN 1）：モバイルインターフェース（APN 1）で受信したパケットが対象となります。 IPsec インターフェース 1~4: IPsec インターフェースから送信されるパケットが対象となります。
変換後の IP アドレス/範囲	変換後の IP アドレスとその範囲を設定します。 設定は任意です。192.0.2.1 – 192.0.2.10 と設定した場合は、192.0.2.1 から 192.0.2.10 までの IP アドレスに変換されます。 192.0.2.1 – と設定した場合は、192.0.2.1 に変換されます。
変換後のポート/範囲	変換後のポート番号を設定します。 設定は任意です。1 – 10 と設定した場合は、1 番ポートから 10 番ポートの範囲で変換されます。1 – と設定した場合は、1 番ポートに変換されます。

7-5. 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。

IPsec 接続未完了時は自装置ネットワークから接続先ネットワークへの通信パケットは全て破棄されます。IPsec 接続完了後自動的に自装置ネットワークから接続先ネットワークへの静的ルートが設定され、ネットワーク間で通信ができるようになります。

UDP 500, 4500 ポート、ESP プロトコル(プロトコル番号 50)を使用します。IP フィルター機能で受信のルールに該当のルールを追加してください。

1. Web 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、「IPsec 設定」画面に入ります。

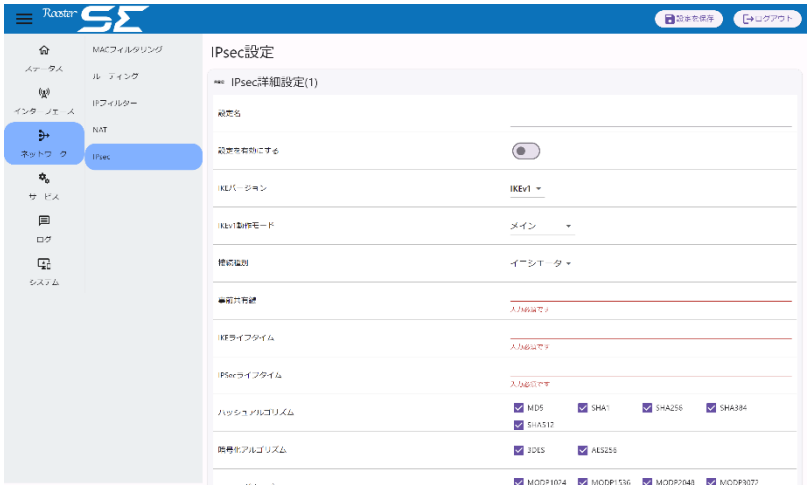
2. 機能を有効にする場合は「機能を有効にする」にチェックを入れます。

3. IKE version2 を使用し、DPD の設定を変更する場合は、下記について設定します。

設定項目	内容
IKEv2 DPD タイムアウト(秒)	接続確認用のパケットの応答タイムアウト時間のベース時間を設定します。
IKEv2 DPD 再送回数	接続確認用のパケットの再送回数を設定します。

IKEv2 使用時の接続確認用パケットの応答タイムアウト時間は下記の計算式で計算されます。
各再送のタイムアウト = IKEv2 DPD タイムアウト(秒) * 1.8 ^ (再送回数 – 1)
初期設定時は DPD タイムアウト 4、再送回数 5 に設定されており、切断を検知して、再接続を行うまでの時間は、165 秒後となります。

4. 設定を編集するには「編集」ボタンをクリックします。
5. 下記について設定します。



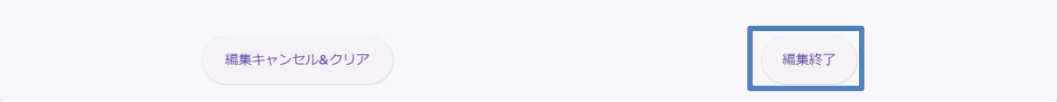
設定項目	内容
設定名	任意の設定名を設定します。
設定を有効にする	設定を有効にする場合はチェックを入れます。
IKE バージョン	IPsec 接続の IKE バージョンを設定します。 設定範囲：IKEv1 | IKEv2
IKEv1 動作モード	IKEv1 選択時、動作モードを設定します。 設定範囲：メイン | アグレッシブ ※IKEv1 使用時、アグレッシブモードは接続種別：イニシエータでのみ使用が可能です。レスポンダ設定時はアグレッシブモードでの接続はできません。
接続種別	接続種別を設定します。 設定範囲：イニシエータ | レスポンダ ※接続種別がイニシエータの場合は本体起動後自動的に接続を行います。 レスポンダの場合自発的に接続は行わず対向機からの接続を待ちます。
事前共有鍵	認証時に使用する事前共有鍵を設定します。 設定範囲：半角 1 ~ 64 (文字)
IKE ライフタイム	IKE の寿命を設定します。 設定範囲：600 ~ 86400 (秒)

設定項目	内容
IPsec ライフタイム	IPsec の寿命を設定します。 設定範囲：600 ~ 86400(秒)
ハッシュアルゴリズム	接続時に使用するハッシュアルゴリズムを設定します。 ※必ず 1 つ以上選択してください。
暗号化アルゴリズム	接続時に使用する暗号化アルゴリズムを設定します。 ※必ず 1 つ以上選択してください。
PFS(DH グループ)	接続時に使用する PFS(DH グループ)を設定します。 ※必ず 1 つ以上選択してください。 ※v2.0.0.X 時点では PFS は必ず有効になります。
接続先アドレス	接続先のアドレスを設定します。 IP アドレス形式・FQDN 形式・any を入力することができます。 FQDN 形式の場合は名前解決されます。 ※any は接続種別が「レスポンダ」の時のみ設定可能です。全ての IP アドレスからの接続を許容します。
接続先ネットワークアドレス/プレフィックス	接続先のネットワークアドレスとそのプレフィックスを設定します。
拡張接続先ネットワークアドレス/プレフィックス	接続先に複数のネットワークが存在する場合にネットワークアドレスとそのプレフィックスを設定します。
接続先に割り当てる仮想 IP アドレス	接続先に仮想の IP アドレスを割り当てる場合に設定します。 ※接続種別が「レスポンダ」の時のみ設定可能です。
接続先識別子	認証時に使用する接続先の識別子を設定します。 任意の文字列・IP アドレスを入力することができます。 ※省略時は接続先アドレスが使用されます。 ※拠点間で同じ値を設定しているのに接続がうまくできない場合は下記のように設定をしてください。 FQDN 形式の場合：先頭に@を付ける（@example.com） USER_FQDN 形式の場合：先頭に@@を付ける(@@ユーザー名@ドメイン)
自装置 IP アドレス	自装置の IP アドレスを設定します。 IP アドレス形式・FQDN 形式・any を入力することができます。 FQDN 形式の場合は名前解決されます。 any 入力時は、自動的に最適なインターフェースの IP アドレスが使用されます。
自装置ネットワークアドレス/プレフィックス	自装置側のネットワークアドレスとそのプレフィックスを設定します。
拡張自装置ネットワークアドレス/プレフィックス	自装置側に複数のネットワークが存在する場合にネットワークアドレスとそのプレフィックスを設定します。
仮想 IP アドレスの割り当てを要求する	接続先に対して仮想 IP アドレスの割り当て要求を行う際に設定します。
自装置識別子	認証時に使用する自装置側の識別子を設定します。 任意の文字列・IP アドレスを入力することができます。 ※省略時は自装置 IP アドレスが使用されます。 ※拠点間で同じ値を設定しているのに認証がうまく通らない場合は下記のように設定をしてください。 FQDN 形式の場合：先頭に@を付ける（@example.com） USER_FQDN 形式の場合：先頭に@@を付ける(@@ユーザー名@ドメイン)
DPD を有効にする	DPD を有効にする場合に設定します。
DPD インターバル	DPD 有効時に生存確認用メッセージを送信する間隔を指定します。 設定範囲：1 ~ 600(秒)

設定項目	内容
DPD タイムアウト	DPD 有効時に対向機からの通信が本項目の秒数間ない場合に、SA を破棄して、接続しなおします。 設定範囲：1 ~ 86400(秒)
メモ	任意のメモを残しておくことができます。

4　設定後、「編集終了」ボタンをクリックします。

▶　編集を途中でやめたい場合、ルールの追加をやめる場合は「編集キャンセル＆クリア」ボタンをクリックします。



5.　［設定を保存］ボタンをクリックして、設定を保存します。

6.　設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

memo　IPsec の設定は最大 4 件まで行えます。

7-5-1. 既定のIPsec接続設定

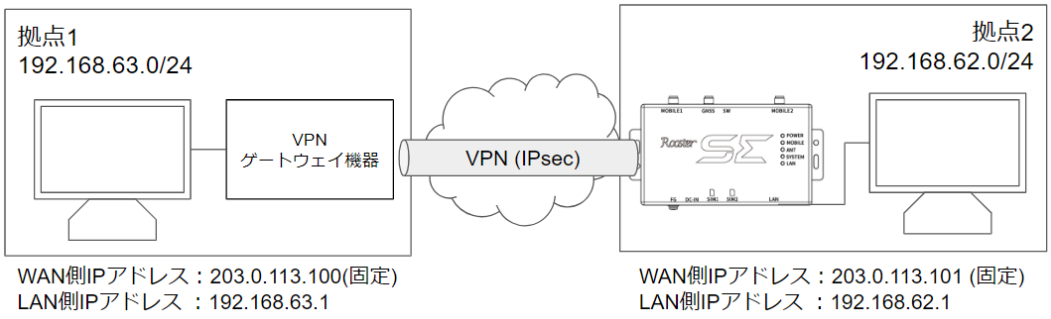
他社製 IPsec 機器と接続を行う場合、以下の表を参考に設定を行ってください。

SE 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 プトロコル)	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	MODP1024、MODP1536、MODP2048、MODP3072、MODP4096、MODP6144、MODP8192
識別子（ホスト ID）	自動判別(グローバル IP アドレス、文字列、User-FQDN)
IKE Life Time	経過時間による設定
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
IPsec Life Time	経過時間による設定
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）	必ず行う MODP1024、MODP1536、MODP2048、MODP3072、MODP4096、MODP6144、MODP8192

Diffie-Hellman-Group について、数字が大きくなるほどキーの計算に時間がかかります。回線速度等環境によっては、計算時間よりも応答の待ち時間の方が早くなり頻繁に通信のリトライが発生し期待通り通信出来ない場合があります。ご注意ください。
MODP8192 は、レスポンダ設定時は使用できません。

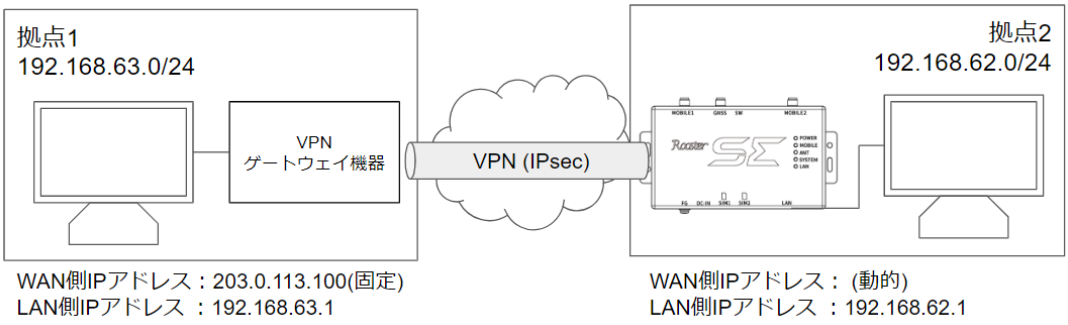
7-5-2. 2点間のWAN側IPアドレスが固定の場合の設定例



SE のサンプル設定：

設定項目	内容
設定名	test-ipsec1
設定を有効にする	有効
IKE バージョン	IKEv1
接続種別	イニシエータ
事前共有鍵	test-key
IKE ライフタイム	86400
IPsec ライフタイム	86400
ハッシュアルゴリズム	SHA256
暗号化アルゴリズム	AES256
PFS(DH グループ)	MODP2048
接続先アドレス	203.0.113.100
接続先ネットワークアドレス /プレフィックス	192.168.63.0/24
接続先識別子	-
自装置 IP アドレス	any
自装置ネットワークアドレス /プレフィックス	192.168.62.0/24
自装置識別子	-
DPD を有効にする	有効
DPD インターバル	60
DPD タイムアウト	300
メモ	-

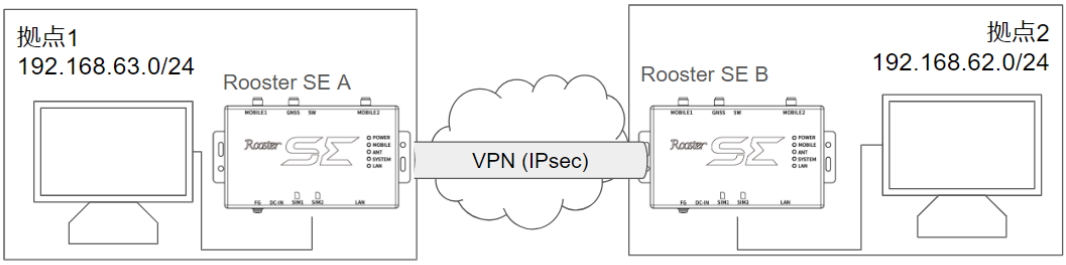
7-5-3. WAN側IPアドレスの一方が固定、SEが動的の場合の設定例



SE のサンプル設定：

設定項目	内容
設定名	test-ipsec2
設定を有効にする	有効
IKE バージョン	IKEv1
接続種別	イニシエータ
事前共有鍵	test-key
IKE ライフタイム	86400
IPsec ライフタイム	86400
ハッシュアルゴリズム	SHA256
暗号化アルゴリズム	AES256
PFS(DH グループ)	MODP2048
接続先アドレス	203.0.113.100
接続先ネットワークアドレス /プレフィックス	192.168.63.0/24
接続先識別子	-
自装置 IP アドレス	any
自装置ネットワークアドレス /プレフィックス	192.168.62.0/24
自装置識別子	test@test
DPD を有効にする	有効
DPD インターバル	60
DPD タイムアウト	300
メモ	-

7-5-4. SE同士で、ダイナミックDNSを利用した場合



WAN側IPアドレス：DDNS(test.suncomm.net)
LAN側IPアドレス ：192.168.63.1

WAN側IPアドレス： (動的)
LAN側IPアドレス ：192.168.62.1

SE A のサンプル設定：

設定項目	内容
設定名	test-ipsec3-b
設定を有効にする	有効
IKE バージョン	IKEv1
接続種別	レスポンダ
事前共有鍵	test-key
IKE ライフタイム	86400
IPsec ライフタイム	86400
ハッシュアルゴリズム	SHA256
暗号化アルゴリズム	AES256
PFS(DH グループ)	MODP2048
接続先アドレス	any
接続先ネットワークアドレス /プレフィックス	192.168.62.0/24
接続先識別子	se-b@test
自装置 IP アドレス	any
自装置ネットワークアドレス /プレフィックス	192.168.63.0/24
自装置識別子	se-a@test
DPD を有効にする	有効
DPD インターバル	60
DPD タイムアウト	300
メモ	-

SE B のサンプル設定：

設定項目	内容
設定名	test-ipsec3-a
設定を有効にする	有効
IKE バージョン	IKEv1
接続種別	イニシエータ
事前共有鍵	test-key
IKE ライフタイム	86400
IPsec ライフタイム	86400
ハッシュアルゴリズム	SHA256
暗号化アルゴリズム	AES256
PFS(DH グループ)	MODP2048
接続先アドレス	test.suncomm.net
接続先ネットワークアドレス /プレフィックス	192.168.63.0/24
接続先識別子	se-a@test
自装置 IP アドレス	any
自装置ネットワークアドレス /プレフィックス	192.168.62.0/24
自装置識別子	se-b@test
DPD を有効にする	有効
DPD インターバル	60
DPD タイムアウト	300
メモ	-

7-6. DNSフィルタリング

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う機能です。

DHCP 機能が無効になっている場合は、本機能も無効になります。
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. Web 設定ツールのメニューから、［ネットワーク］－［MAC フィルタリング］をクリックし、「MAC フィルター設定」画面に入ります。

2. 下記について設定します。

設定項目	内容
デフォルトルール	設定されているルールに該当しないドメイン名に対するデフォルトのルールを設定します。 ▶ 初期設定時は「名前解決する」に設定されています。

特定のドメインの名前解決のみを行い、通信に制限をかけたい場合は、「デフォルトルール」を「名前解決しない」に設定し、ルール追加で名前解決をするルールを追加してください。

2. ルールを追加するには「追加」ボタンをクリックします。

3. 下記について設定します。

設定項目	内容
ドメイン	対象のドメインを設定します。 ドメインのマッチ条件については注意欄を確認してください。
動作	該当のドメインについて名前解決をするか・しないかを設定します。 設定範囲：名前解決する | 名前解決しない
有効	該当のルールを有効にします。 無効に設定された場合は該当のルールが無視されます。 ▶ ルールを追加後は「有効」に設定されています。
削除	該当のルールを削除したい場合に使用します。 ボタンをクリックすると該当のルールが削除されます。

4. ［設定を保存］ボタンをクリックして、設定を保存します。
5. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

memo DNS フィルタリングの設定は最大 10 件まで行えます。
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）

ドメインの扱いとマッチ条件は次の通りです。
ドメイン名の扱い：
・ドメイン名の先頭の「.」は無視する(example.com と.example.com を同様に扱います)

ルールのマッチ条件（次の条件全てを満たしたものがマッチします）：
・設定したドメイン名に対して完全一致または後方一致
・各ラベルが完全一致
例：
ドメイン名に「example.com」を設定した場合

ドメイン名	判定
example.com	〇 (完全一致)
www.example.com	〇 (後方一致)
XXXexample.com	× (後方一致だが、ラベル(XXXexample) が example と完全に一致していない)

又、複数のルールを設定した場合は、下記の条件のルールが適用されます。
・より多くのラベルが一致するルール
・同じ数のラベルが一致する場合は、先に設定されているルール

7-7. L2TP/IPsec

L2TP/IPsec サーバ機能は SE がサーバとして L2TP/IPsec 接続の待ち受けを行う機能です。SE に対して遠隔から VPN 接続が可能になります。

最大 4 ユーザーまで設定、接続できます。

IPsec 接続と併用する場合に IPsec 接続用の共通鍵か、L2TP/IPsec 接続用の共通鍵かの区別が不可能となる設定ケースがあります。その場合、L2TP/IPsec、IPsec 接続時にどちらの事前共通鍵でも接続が出来てしまう可能性が有りますのでご注意ください。

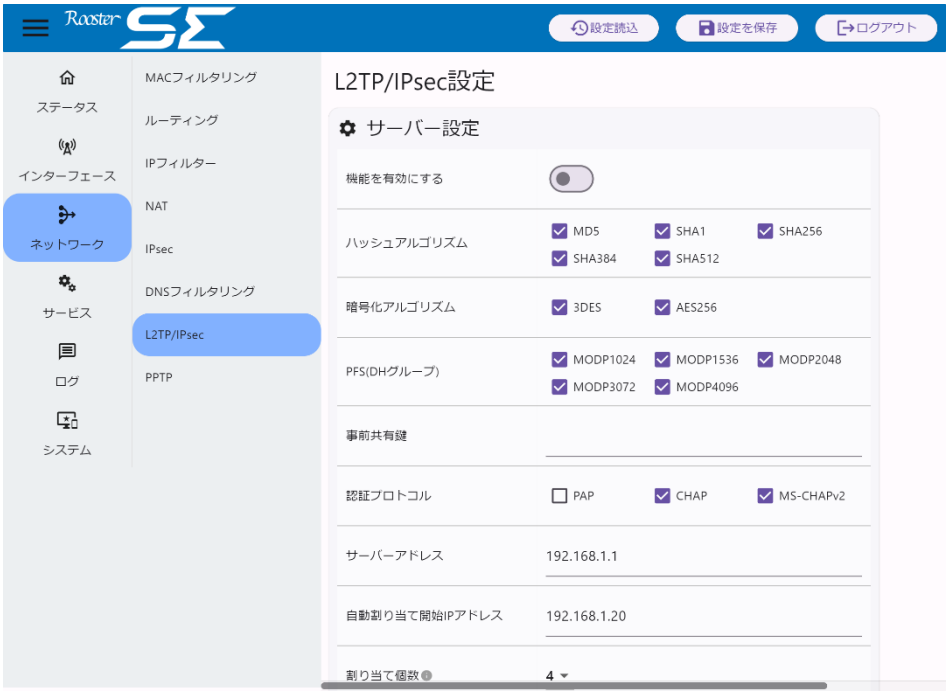
ユーザーに IP アドレスの固定割り当てを行い、同名のユーザーで複数のクライアントから接続を行った場合は先に接続したユーザーが通信を行う事が出来ます。

同一のグローバル IP アドレスからは 1 クライアントのみ接続が可能です。

UDP 500, 1701, 4500 ポート、ESP プロトコル(プロトコル番号 50)を使用します。IP フィルター機能で受信のルールに該当のルールを追加してください。

Windows 端末から接続を行った場合、7 時間 36 分程度で切断される事があります。
切断される場合は再接続を行ってください。

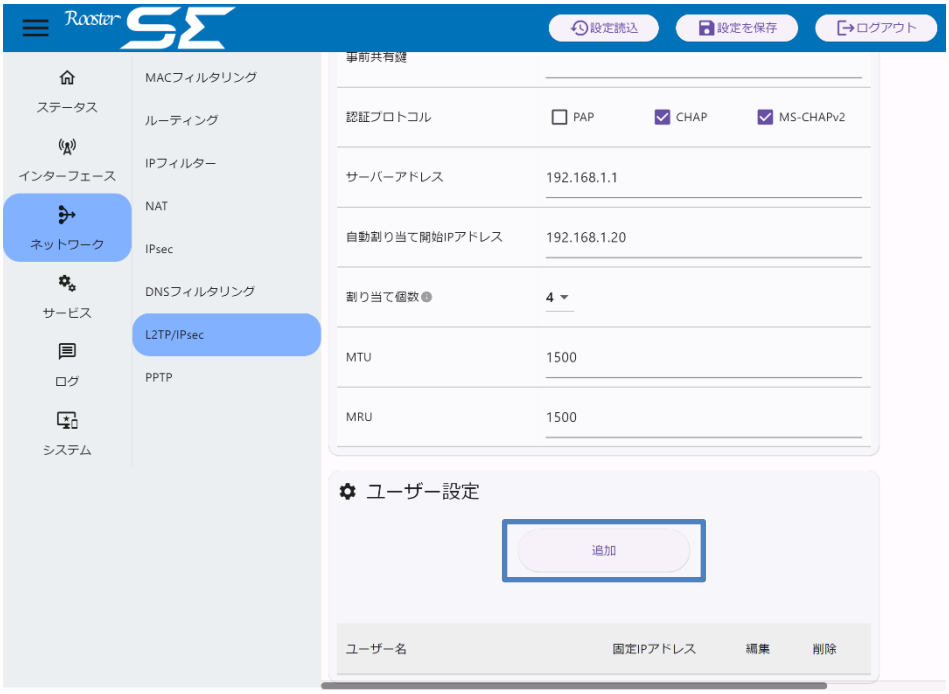
1. Web 設定ツールのメニューから、［ネットワーク］－［L2TP/IPsec］をクリックし、「L2TP/IPsec 設定」画面に入ります。



2. 下記について設定します。

設定項目	内容
機能を有効にする	機能の有効・無効を設定します。
ハッシュアルゴリズム	接続を受け付けるハッシュアルゴリズムを設定します。
暗号化アルゴリズム	接続を受け付ける暗号化アルゴリズムを設定します。
PFS(DH グループ)	接続を受け付ける PFS(DH グループ)を設定します。
事前共有鍵	IPsec 接続部の事前共有鍵を設定します。
認証プロトコル	ユーザー認証に使用するプロトコルを設定します。
サーバアドレス	L2TP/IPsec サーバの IP アドレスを設定します。
自動割り当て開始 IP アドレス	サーバがクライアントに割り当てる IP アドレスの開始アドレスを設定します。
割り当て個数	クライアントに割り当てる最大個数を設定します。
MTU	接続によって生成されるインターフェースの MTU を設定します。
MRU	接続によって生成されるインターフェースの MRU を設定します。

3. 接続するユーザーを追加するには「追加」ボタンをクリックします。



4. 下記について設定します。

設定項目	内容
ユーザー名	接続するユーザーのユーザー名を設定します
パスワード	接続するユーザーのパスワードを設定します
固定 IP アドレス	ユーザーに固定の IP アドレスを割り当てる際は IP アドレスを設定します
メモ	このユーザーに関するメモを設定します。

5. ［設定を保存］ボタンをクリックして、設定を保存します。
6. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

7-8. PPTP

PPTP サーバ機能は SE がサーバとして PPTP 接続の待ち受けを行う機能です。SE に対して遠隔から VPN 接続が可能になります。

最大 4 ユーザーまで設定、接続できます。

PPTP 接続後は 1 分毎にクライアントに対し PPTP の echo request を送信します。この request に対して応答が得られない場合はクライアントの接続を切断します。この echo request は LCP echo とは別物で LCP echo の有効状態に関わらず送信されます。

ユーザーに IP アドレスの固定割り当てを行い、同名のユーザーで複数のクライアントから接続を行った場合は先に接続したユーザーが通信を行う事が出来ます。

TCP 1723 ポート、GRE プロトコル(プロトコル番号 47)を使用します。IP フィルター機能で受信のルールに該当のルールを追加してください。

1. Web 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、「PPTP 設定」画面に入ります。

2. 下記について設定します。

設定項目	内容
機能を有効にする	機能の有効・無効を設定します。
認証プロトコル	ユーザー認証に使用するプロトコルを設定します。
MPPE	MPPE の使用について必須・拒否を設定します。
MPPE オプション	MPPE が必須の場合に MPPE のオプションを設定します。 ※v1.4 時点では 128bit 固定となります。
サーバアドレス	PPTP サーバのＩＰアドレスを設定します。
自動割り当て開始ＩＰアドレス	クライアントに自動的に割り当てるアドレスの開始ＩＰアドレスを設定します。
割り当て個数	クライアントに割り当てるアドレスの最大個数を設定します。
LCP echo を有効にする	LCP echo の有効・無効を設定します。
LCP echo 閾値	LCP echo 失敗時の閾値を設定します。 ※設定された閾値回数 LCP echo が失敗した場合は切断します。
LCP echo 送信間隔	LCP echo の送信間隔を設定します。
MTU	生成されるインターフェースの MTU を設定します。
MRU	生成されるインターフェースの MRU を設定します。

3. 接続するユーザーを追加するには「追加」ボタンをクリックします。

4. 下記について設定します。

設定項目	内容
ユーザー名	接続するユーザーのユーザー名を設定します
パスワード	接続するユーザーのパスワードを設定します
固定 IP アドレス	ユーザーに固定の IP アドレスを割り当てる際は IP アドレスを設定します
メモ	このユーザーに関するメモを設定します。

5. ［設定を保存］ボタンをクリックして、設定を保存します。
6. 設定を適用する場合は、SE を再起動します。

➲ 再起動の方法については、『4-9-1.再起動』を参照ください。

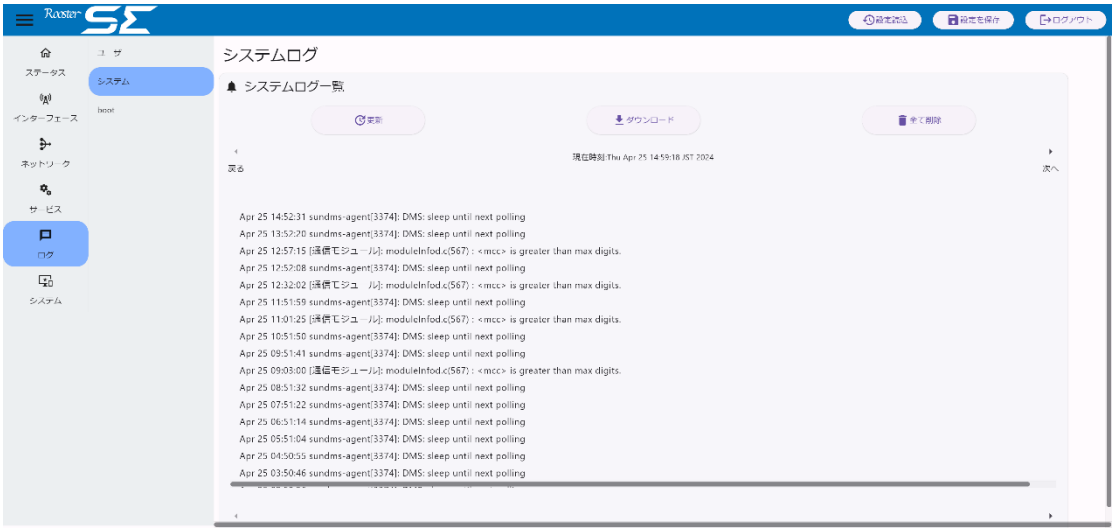
8章　ログの参照方法

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。

8-1. システムログの参照

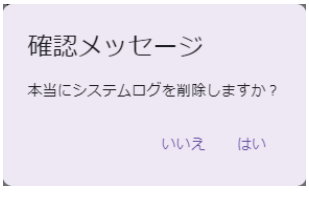
> SE は電源断時に時刻情報を保持することができません。
> 起動直後のログや、時刻が補正されるまでのログについては現在時刻と異なる時刻が表示されることがあります。

1. 設定ツールのメニューから、［ログ］－［システム］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。
   ログの発生した時刻と、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。



2. 各ボタンを以下のように操作します。

項目	内容
更新	最新のログを表示させるために「更新」ボタンをクリックします。
ダウンロード	ログのデータをダウンロードするために「ダウンロード」ボタンをクリックします。 「yyyy-mm-dd-rooster-se-syslog.tar」ファイルがダウンロードされます。
すべて削除	ログデータを削除するために「すべて削除」ボタンをクリックします。 ポップアップが表示され、「はい」をクリックするとログデータが削除されます。



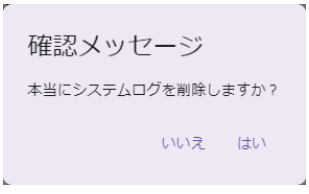
8-2. ユーザーログの参照

> SE は電源断時に時刻情報を保持することができません。
> 起動直後のログや、時刻が補正されるまでのログについては現在時刻と異なる時刻が表示されることがあります。

1. 設定ツールのメニューから、［ログ］－［ユーザー］をクリックします。
   ユーザーログ一覧のページが表示されます。
   ログの発生した時刻と、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。

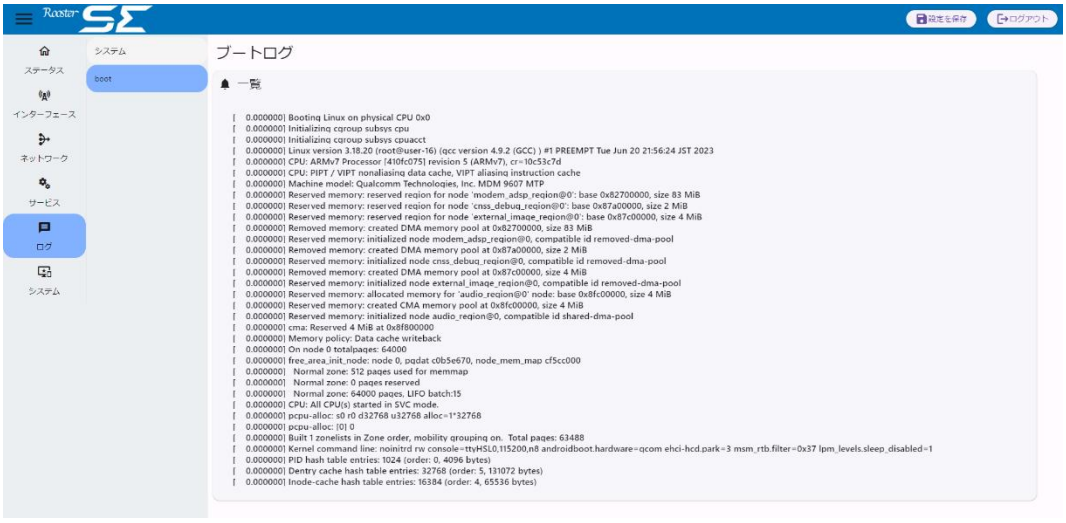
2. 各ボタンを以下のように操作します。

項目	内容
更新	最新のログを表示させるために「更新」ボタンをクリックします。
ダウンロード	ログのデータをダウンロードするために「ダウンロード」ボタンをクリックします。 「yyyy-mm-dd-rooster-se-userlog.tar」ファイルがダウンロードされます。
すべて削除	ログデータを削除するために「すべて削除」ボタンをクリックします。 ポップアップが表示され、「はい」をクリックするとログデータが削除されます。



8-3. bootログの参照

1. 設定ツールのメニューから、［ログ］－［boot］をクリックします。
   「ブートログ」のページが表示されます。
   ログの発生した時刻と、ブートに関するログが表示されます。
   下に行くほど、より新しいログとなります。



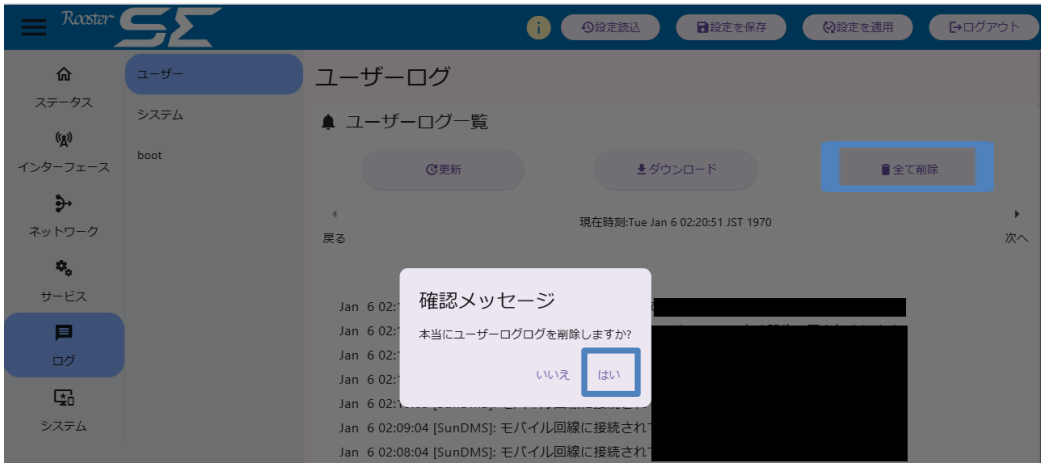
9章　SEの破棄方法

この章では、Rooster SE 内の情報資産を削除し、安全に破棄いただく方法を説明します。

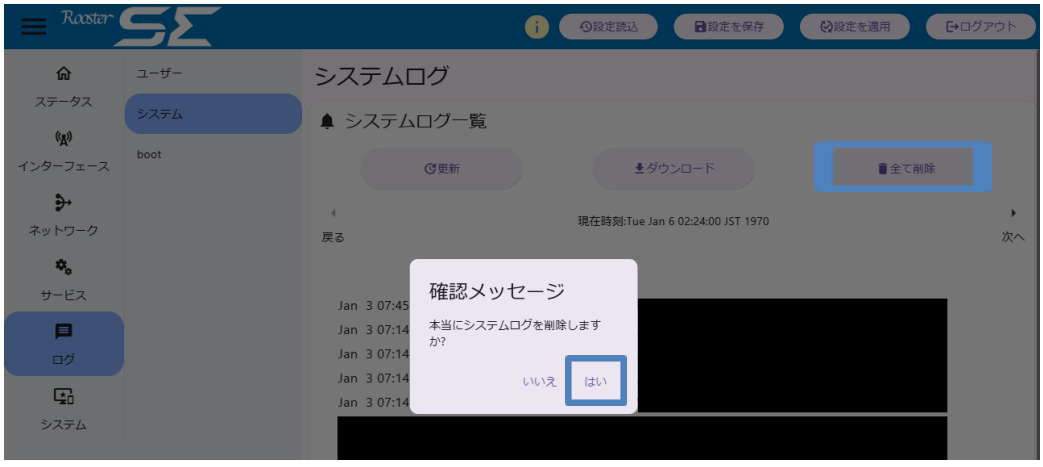
9-1. 破棄手順

Rooster SE 内の情報資産等を削除し、安全に破棄するには下記の手順を実施します。

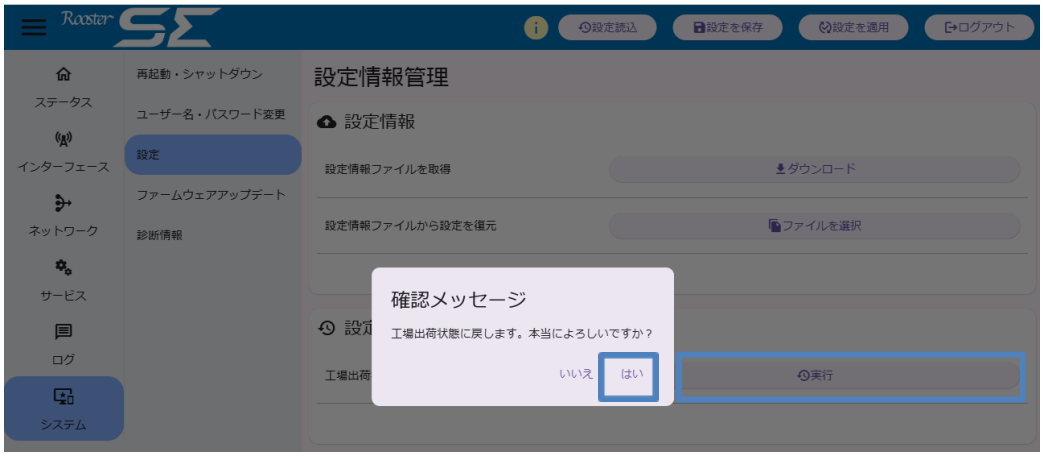
1. ［ログ］－［ユーザー］をクリックし、[ユーザーログ]ページを開きます。
2. [すべて削除]をクリックし、確認メッセージについて[はい]をクリックしてログを削除します。



3. ［ログ］－［システム］をクリックし、[システムログ]ページを開きます。
4. [すべて削除]をクリックし、確認メッセージについて[はい]をクリックしてログを削除します。



5. ［システム］－［設定］をクリックし、設定情報管理ページを開きます。
6. 工場出荷状態に戻す項目の[実行]をクリックし、確認メッセージについて[はい]をクリックして設定を工場出荷状態に戻します。



7. Rooster SE への電源供給を切り、本体から SIM カードを取り除きます。

10章 制限・注意事項

この章では、現時点での制限事項、特に注意すべき事項について説明します。

10-1. 設定ツールについての注意事項

10-1-1. 入力できる文字列について

設定ツールの「ユーザー名」、「パスワード」は「半角英数字」のみ、それ以外のテキストフィールドでは、「半角英数字」、「. (ピリオド)」、「- (ハイフン)」、「: (コロン)」、「 (スペース文字)」、「?」、「"」のみ入力されることを想定しております。想定されていない文字を設定した場合の動作は保証することができません。又、WEB 設定ツールでテキストフィールドに「"」を設定する場合は「¥"」と入力してください。

10-1-2. Web設定ツールの読み込みが続いてしまう状態について

通信の状況などによって Web 設定ツールの読み込み中の表示が続く場合があります。数分間この状態が続く場合は、Web ブラウザをリロードして、ログインからやり直してください。Web ブラウザをリロードするとログイン画面が表示されます。Web ブラウザをリロードしてもログイン画面に戻らない場合は、「Crtl+Shift+R」キー等でキャッシュクリアを伴うリロードをし、再度ログインからやり直してください。

10-1-3. ブラウザの拡大率について

Web 設定ツールを使用する際は、ブラウザの拡大率を 100%にして頂く事をお勧めしております。縮小、拡大した場合に設定ツールの表示が崩れてしまう可能性が有りますのでご注意ください。

10-2. モバイル通信に関しての注意事項

特定の SIM によっては、誤った設定を行うと LED 表示上は接続できているように見えるが、実際に通信は行えない事象が発生する可能性が有ります。モバイルインターフェースに IP アドレスが割り当てられているかについても確認をしてください。

付録

製品仕様

品名		SE220
コード		11S-RSE-220
JAN コード		4907940130797
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 MVNO)
対応 UIM カード		nano SIM×2
有線インターフェース	LAN	100BASE-TX /10BASE-T×1 ポート （MDI/MDI-X 自動判別）
モバイル インターフェース	アンテナコネクタ	SMA レセプタクル×2
	LTE Band	B1(1920~1980MHz(UL)、2110~2170MHz(DL))
		B3(1710~1785MHz(UL)、1805~1880MHz(DL))
		B8(880~915MHz(UL)、925~960MHz(DL))
		B18(815~830MHz(UL)、860~875MHz(DL))
		B19(830~845MHz(UL)、875~890MHz(DL))
		B26(814~849MHz(UL)、859~894MHz(DL))
		B41(2555~2655MHz(UL)、2555~2655MHz(DL))
GNSS インターフェース	アンテナコネクタ	SMA レセプタクル×1
	プロトコル	NMEA 0183（GPS, GLONASS, BeiDou/Compass, Galileo, QZSS）
ハードウェア	搭載モジュール	Quectel 「EC25-J」 設計認証番号：ADF18-0088018 工事設計認証番号：018-190011
	LED	5 個（緑 3 個、赤/緑 2 個）
	タクトスイッチ	1 個 (初期化用)
	温度センサ	ケース内 1 系統
	電圧監視	DCIN 電圧 1 系統
	内蔵アンテナ	LTE 用アンテナ ×２（外部アンテナと個別切り替え）
電源	入力電圧	DC 5V～32V ±5%
	消費電流	待受時：約 100mA(DC12V) 通信時：約 200mA(DC12V) 通信時最大：約 450mA(DC12V)
	消費電力	5.5W(最大)
	リップル	200mVp-p 以下
	コネクタ	Molex 3pin コネクタ 70553-0002
環境条件	動作温度	-20℃～70℃
	動作湿度	25%～85%（結露なきこと）
	保存温度	-30℃～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 DC ラインノイズ	 ±2kV パルス幅 100ns/1000ns (弊社オプション AC アダプタの AC ラインに印加) ±2kV パルス幅 100ns/1000ns（DC-IN ラインに印加）

	耐静電気性（※1） 接触放電 気中放電	 ±8kV（LAN コネクタ外周部に印加） ±8kV（LAN 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 30Hz～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 120g
外形寸法		約 111 (W) × 66 (D) × 26 (H) 単位 mm （突起部、取付部除く） 約 135 (W) × 74 (D) × 30 (H) 単位 mm （突起部、取付部含む）
材質	ケース	樹脂
	固定具	ケースと一体型
サポートプロトコル	Ethernet	CSMA/CD
	ルーティング	IPv4
DHCP	サーバ	LAN 側 (リース時間設定可)、最大 253 クライアント
アドレス変換		NAT/IP マスカレード、DNAT（32 件）、SNAT（32 件）
サーバ公開		バーチャルサーバ（DNAT）
スタティックルーティングテーブル		最大 10 件
アップデート		Web ブラウザによるアップデート
		SunDMS によるアップデート
		SSH によるアップデート
ダイナミック DNS		SunDMS（suncomm.DDNS）（※2）
WAN ハートビート	相手先	任意のアドレス/FQDN 設定可能/SunDMS
	送信間隔	可能（1 秒～）
電源制御		ハードウェアタイマによる監視
ハードウェア ウォッチドッグ	信号タイミング	常時監視（100ms 毎）
	発動条件	定期信号不受信後即時
	発動動作	本体電源 OFF から 10 秒後に再起動
ダイヤルアップ自動発信条件		常時接続
回線冗長化		SIM1/SIM2 での冗長化
モバイル通信端末情報		自局電話番号、アンテナレベル、RSRP、RSRQ、エリアコード、基地局 ID、周波数帯域、IP アドレス取得可能
VPN（IPsec）	鍵交換プロトコル	IKEv1、IKEv2
	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	modp1024、modp1536、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 4 件
	セッションキープ設定	可能
	キープアライブ設定	可能

	バックアップ設定	別 VPN 装置への接続設定可能（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）	暗号化	GRE
	接続可能数	最大 4 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
	IPsec DH Group	modp1024、modp1536、modp2048、modp3072、modp4096
	接続可能数	最大 4 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
		Web ブラウザによる各種ログ表示
		SSH による各種ログ表示
		SunDMS から取得
ログの内容		パケット通過ログ パケット遮断ログ モバイル通信端末ログ IPsec ログ PPTP ログ L2TP/IPsec ログ アドレス解決ログ DHCP ログ WAN ハートビートログ LTE 関連 ログ SunDMS ログ システムログ ※一部のログはファームウェアアップデートにて対応予定
設定情報管理		Web 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
		SunDMS からの取得・保存
フィルタリング	FORWARD	32 件
	INPUT	32 件
	OUTPUT	32 件
	DNS フィルタリング	10 件
	MAC フィルタリング	10 件
インターネット経由のリモートセットアップ		可能（Web ブラウザ/SSH/SunDMS）
時刻管理		モバイル通信モジュールより自動取得
SunDMS		死活監視
		標準ファームウェア更新
		再起動指示（コールドリブート）
		システムログ取得
		設定ファイル取得
		共通設定ファイル一括更新

	個別設定ファイル一括更新
	接続モードと通信頻度設定変更
	供給電圧、筐体内温度アラート設定
	電波受信強度、電波品質の表示とアラート設定
	データ出力
	IP アドレス確認（ダイナミック DNS 契約者のみ）(※2)
	後位端末死活監視（ICMP）
	電波環境調査
	IP アドレス表示（機器アクセス）
	位置情報表示
	SunDMS WAN ハートビート
	接続情報の更新
MTBF	300,000 時間
製品含有化学物質	RoHS2 対応
規格	VCCI Class A JIS D 1601-1995 3 種-A 種（自動車部品振動試験規格） JIS E 4031:2013 区分 1 等級 B（鉄道車両部品の振動・衝撃試験規格）
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、GNSS 用アンテナ、AC アダプタ ※3

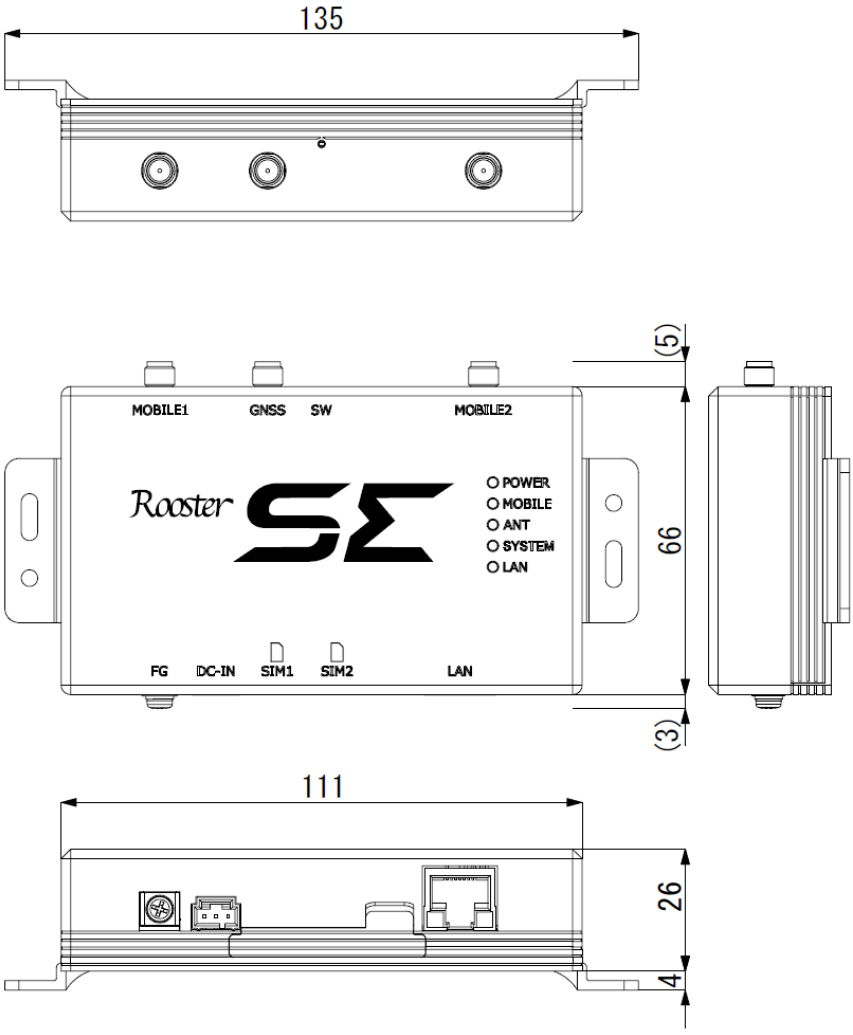
※1　表記の数値は、試験装置による試験性能値です。
　　また、ノイズや静電気を印加し続けた際の動作を保証するものではございません。

※2　弊社が運営する SunDMS のダイナミック DNS サービスです。

※3　利用にあたっては別途オプション品をご購入ください。

外形寸法

単位:mm



※公差含む

品名	SE220
外形寸法	約 111 (W) × 66 (D) × 26 (H) 単位 mm（突起部、取付部除く） 約 135 (W) × 74 (D) × 30 (H) 単位 mm（突起部、取付部含む）
重量	約 120g

最新情報の入手

本製品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/se220/

ご質問・お問い合わせ

本製品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　0587-53-7606
- メール　support-suncomm@sun-denshi.co.jp
- 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

SE 取扱説明書 **Ver.2.0.0**

サン電子株式会社
2025 年 4 月発行 (20250425)