NEC

Aterm Biz シリーズ

Aterm SA3500G 機能詳細マニュアル

第 9.0 版　2020 年 10 月
ＮＥＣプラットフォームズ株式会社

※ファームウェアバージョン 3.6.9 に基づいて説明しています。

目次

1. はじめに

このたびは Aterm SA3500G をご利用いただき、まことにありがとうございます。

1. 本書は、Aterm SA3500G の機能、設置、設定について説明するものです。
2. 本書は、以下の章により構成されています。

3. 本製品の使用方法や設定方法を誤って使用した結果発生した通信料金やプロバイダ接続料金などの損失について、ＮＥＣプラットフォームズ株式会社では一切責任は負いかねますので、あらかじめご了承ください。

1.1. 制限事項および免責事項

(1) 本書の内容の一部、又は全部を無断転載･無断複写することは禁止されています。
(2) 本書の内容については、将来予告なしに変更することがあります。
(3) 本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り･記載もれなどお気づきの点がありましたら、お問い合わせ先にご連絡ください。
(4) 本製品の故障・誤動作・天災・不具合あるいは停電などの外部要因によって通信などの機会を逸したために生じた損害などの純粋経済損失につきましては、当社は一切その責任を負いかねますのであらかじめご了承ください。
(5) セキュリティ対策をほどこさず、あるいは、無線 LAN の仕様上やむをえない事情によりセキュリティの問題が発生してしまった場合、当社は、これによって生じた損害に対する責任は一切負いかねますのであらかじめご了承ください。
(6) せっかくの機能も不適切な扱いや不測の事態（例えば落雷や漏電など）により故障してしまっては能力を発揮できません。本書をよくお読みになり、記載されている注意事項を必ずお守りください。
(7) 本製品を快適にご利用いただくには、1000BASE-T、1,000Mbps の方式による接続を推奨します。
(8) 本製品はネットワーク上の脅威に対してそのリスクを低減させるための製品ですが、導入によりその脅威を完全に取り除くことを保証するものではありません。
(9) 本製品のセキュリティ・スキャン機能を利用するためには、インターネット接続環境が必要です。
(10) ライセンス契約期間を超えると、本製品は一切のセキュリティ・スキャン機能を停止いたします。

無線 LAN に関する免責事項

（1）無線 LAN の規格値は、本製品と同等の構成を持った機器との通信したときの理論上の最大値であり、実際のデータ転送速度を示すものではありません。
（2）本製品は他社製品との相互接続性を保証しておりません。
（3）無線 LAN の伝送距離や伝送速度は、壁や家具・什器などの周辺環境により大きく変動します。

1.2. 電波に関する注意事項

- 本製品は、技術基準適合証明を受けています。
- IEEE802.11n（2.4GHz）、IEEE802.11g、IEEE802.11b 通信利用時は、2.4GHz 帯域の電波を使用しており、この周波数帯では、電子レンジなどの産業・科学・医療機器の他、他の同種無線局、工場の製造ラインなどで使用される免許を要する移動体識別用構内無線局、免許を要しない特定小電力無線局、アマチュア無線局など（以下「他の無線局」と略す。）が運用されています。
  （1）本製品を使用する前に、近くで「他の無線局」が運用されていないことを確認してください。
  （2）万一、本製品と「他の無線局」との間に電波干渉が発生した場合は、速やかに本製品の使用チャネルを変更するか、使用場所を変えるか、または機器の運用を停止してください。
  （3）その他、電波干渉の事例が発生し、お困りのことが起きた場合には、お問い合わせ先にご連絡ください。
- 2.4GHz 帯使用の Bluetooth 機器と通信できません。
- IEEE802.11n、IEEE802.11g、IEEE802.11b 通信利用時は、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が回避可能です。変調方式として DS-SS 方式および、OFDM 方式を採用しており、与干渉距離は 40m です。

2.4　：2.4GHz 帯を使用する無線設備を示す
DS/OF ：DS-SS 方式および OFDM 方式を示す
4　：想定される干渉距離が 40m 以下であることを示す
■■■ ：全帯域を使用し、かつ移動体識別装置の帯域を回避可能であることを意味する

- 本製品を 2.4GHz 帯で使用し、チャネルを手動で設定する場合、一般社団法人 電波産業会の ARIB 規格により下記内容が推奨されています。
  「この機器を 2.4GHz 帯で運用する場合、干渉低減や周波数利用効率向上のため、チャネル設定として ch1,ch6,ch11 のいずれかにすることを推奨します。」
  ただし、無線 LAN 以外のシステムとの干渉を避けるために、推奨の 1,6,11ch 以外を使用しなければならない場合はこの限りではありません。
- デュアルチャネルを利用する場合は、同一周波数帯を使用する他の無線局に対して干渉を与える可能性があります。
  ・デュアルチャネルを「使用する」に設定する場合には、周囲の電波状況を確認して他の無線局に電波干渉を与えないことを事前にお確かめください。
  ・万一、他の無線局において電波干渉が発生した場合には、すぐに「使用しない」に設定を変更してください。

1.3. 情報処理装置など電波障害自主規制について

この装置は、クラスB機器です。この装置は、住宅環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　VCCI－B

1.4. 輸出に関する注意事項

本製品（ソフトウェアを含む）は日本国内仕様であり外国の規格などには準拠しておりません。本製品を日本国外で使用された場合、当社は一切責任を負いません。また、当社は本製品に関し海外での保守サービスおよび技術サポートなどは行っておりません。
本製品の輸出（非居住者への役務提供等を含む）に際しては、外国為替及び外国貿易法等、関連する輸出管理法等をご確認の上、必要な手続きをお取りください。
ご不明な場合、または輸出許可等申請手続きにあたり資料等が必要な場合は、お問い合わせ先にご相談ください。

1.5. **廃棄方法について**

この製品を廃棄するときは地方自治体の条例にしたがって処理してください。

なお、ＮＥＣは、法律にもとづき、使用済み製品（情報通信機器）回収／再資源化を有償にて行っています。

詳細については、こちらのページをご覧ください。

https://jpn.nec.com/eco/ja/recycle/method/it/

（使用済み製品はリサイクル可能な貴重な資源です。使用済み製品の回収にご協力ください。）

本製品を廃棄するときは、秘密情報の流出を回避するため、本製品に設定した内容やログ情報を消去する初期化を行ってください。初期化の方法は、5.6.15章を参照してください。

1.6. メンテナンスバージョンアップ機能に関する許諾について

メンテナンスバージョンアップ機能は、本製品のソフトウェアに重要な更新があった場合に、インターネットを介して自動でバージョンアップする機能です。

「重要な更新」とは、ＮＥＣプラットフォームズ株式会社（以下「当社」とします。）が本製品の機能を提供する上でソフトウェアのバージョンアップが必須と判断した場合（例えばセキュリティ上の不具合を改善するソフトウェアの更新など）を示します。重要な更新がある場合は、当社ホームページ（https://www.necplatforms.co.jp/）の「ニュース欄のお知らせ」にてご案内します。

メンテナンスバージョンアップ機能が開始されると、本製品が再起動するため、それまで接続していた通信が切断されます。また、従量制課金契約の場合、ソフトウェアダウンロードによる通信費用や、パケット通信量超過による速度制限が発生する場合があります。発生した通信費用はお客様ご負担となります。

本機能は、 本製品に関する情報のうち、本機能が動作するために必要な最小限度の機器情報・ネットワーク情報を当社が運用するサーバへ通知します。これらの情報は、本機能の実現と本製品や本機能の改善・向上のためだけに利用し、これ以外の目的では利用しません。また、これらの情報は、当社の取り扱い手続きに則り、適切な管理を行います。当社が第三者と連携して本機能を利用する場合につきましても、当社の取り扱い手続き同様に適切な管理を実施します。

本機能の初期値は有効（「使用する」）になっています。本機能に関して許諾いただけない場合は、下記手順で本機能を無効にしてください。
ただし、 本機能を無効にした場合、セキュリティ上の不具合を改善するような重要なソフトウェアの更新であっても、自動的にバージョンアップは行いません。改善前のソフトウェアをそのまま使用し続ける場合、悪意のある第三者から不正なアクセスをされる危険性が残る可能性があります。

本機能無効化の方法

1. 設定 Web にアクセスします。（5.4 章参照）
2. [TOP]-[メンテナンス]-[メンテナンス]画面を開きます。
3. 「メンテナンスバージョンアップ機能」の「使用する」のチェックを外します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。（5.5 章参照）

1.7. セキュリティ・スキャン機能に関する許諾について

本製品を使用する前に必ずご確認ください。

本製品を使用する場合は、本機能に関して許諾いただいたものとします。

セキュリティ・スキャン機能は、脅威検出を行うために、インターネットを介して以下の処理を行います。

- セキュリティ・スキャン機能で使用する情報ファイル（ウイルス情報など）の自動アップデート
- インターネットアクセスする URL の確認

従量制課金契約の場合、情報ファイルのダウンロードによる通信費用が発生したり、パケット通信量超過による速度制限が発生したりします。発生した通信費用はお客様ご負担となります。本機能では、本製品に関する情報のうち、本機能が動作するために必要な最小限度の機器情報をサーバへ通知します。これらの情報は、本機能の実現のためだけに利用し、これ以外の目的では利用しません。また、これらの情報は、当社の取り扱い手続きに則り、適切に管理を行います。当社が第三者と連携して実施する本機能につきましても、当社の取り扱い手続き同様に適切な管理を実施します。

1.8. ホーム IP ロケーション機能のご使用条件

ここでは、当社が提供するホーム IP ロケーション機能の使用条件を記載しています。

ホーム IP ロケーション機能を使用する場合は、機能を有効にする前に、こちらのご使用条件をご確認ください。機能を有効にされた場合は、ご使用条件にご同意いただけたものといたします。

ホーム IP ロケーション機能は、本製品をご使用になるお客様に、より便利にお使いいただけるよう、インターネットからホーム IP ロケーション名で本製品へのアクセスを可能とする機能です。

本機能は、以下の場合に有効になります。

- ルータモードに設定されている（初期値：「ブリッジモード」）
- WAN 側にグローバル IP アドレスが付与されている
- メンテナンスバージョンアップ機能が「ON」になっている（初期値：「ON」）
- ホーム IP ロケーション機能が「ON」になっている（初期値：「OFF」）

なお、機能が有効となる条件を満たしても、本製品へのアクセスが可能になるまで 1 時間程度要する場合があります。

また、ホーム IP ロケーション名は、本製品固有の名前になり、変更することはできません。

1. 使用権

本機能の提供は、本製品をご使用いただいているお客様に対して行います。

また、本製品を転売等された場合は、新たに本製品を所有されるお客様が本機能をご使用いただけます。

2. 禁止行為

本機能は、違法行為または以下の行為をされる場合、ご使用いただけません。

当社が機能使用に適さないと判断した場合、予告なく機能を停止させていただきます。

（1） 公序良俗に反する行為

（2） 営利目的に使用する行為

（3） 第三者の権利を侵害する行為またはその恐れのある行為

（4） 本機能の運営を阻害する行為またはその恐れのある行為

（5） 本機能を使用する権利を第三者に移譲する行為

（6） 本製品の偽装をする行為

3. 免責事項

当社は本機能を提供するにあたり、機能の提供維持、安定化に努めますが、当社の対応は下記のものとなります。

（1） 本機能の損害賠償

本機能によるお客様が被る損害については、いかなる場合も当社は一切の責任を負いません。

（2） 本機能の保証範囲

本機能は本製品と当社サーバにて機能動作を確認し、保証するものとなります。本機能ご使用にあたり、お客様のご使用環境に起因する機能、性能の動作保証やお客様のデータや機器に関する保証については、当社は一切の責任を負いません。

（3） 本機能の中断、停止

やむをえない理由または当社の都合により、本機能の中断・停止を予告なく行うことがあります。

（4） 本条件の変更

本条件の改定を予告なく行うことがあります。

4. 機器情報の扱い

本機能に必要な本製品の機器情報を当社のサーバに通知いたします。

（1） 通知される機器情報

・ お客様がご使用になっている本製品の機器情報

・ お客様がご使用になっている本製品のネットワーク情報

（2） 情報利用の目的について

本機能の実現と本製品や本機能の改善、向上のためにお客様の機器情報を利用いたします。

お客様の機器情報は、本機能およびメンテナンスバージョンアップ機能を実現するために利用し、これ以外の目的では利用いたしません。

（3） 情報の管理

当社が利用するお客様の情報につきましては、当社の取り扱い手続きに則り、適切な管理を行います。

当社が第三者と連携して実施する本機能につきましても、当社の取り扱い手続き同様に適切な管理を実施します。

5. その他

本機能は国内法に従い対応します。また、関連した紛争については、東京地方裁判所を第一審の専属的合意所轄裁判所とします。

1.9. ソフトウェア使用許諾契約書

ＮＥＣプラットフォームズ株式会社（以下「当社」といいます）は、当社の Aterm SA3500G（以下「本製品」といいます）に搭載しているソフトウェア（以下「本ソフトウェア」といいます）及び関連ドキュメント（以下「本ドキュメント」といいます）（本ソフトウェアと本ドキュメントを総称して以下「使用許諾物」といいます）を使用する権利をソフトウェア使用許諾契約書（以下「本契約」といいます）に基づきお客様に許諾し、お客様は本契約にご同意いただくものといたしますので、お客様は本製品をご使用になる前に、本契約書を注意してお読みください。お客様が本製品の使用を開始された場合には、本契約にご同意いただいたものといたします。お客様が本契約にご同意いただけない場合には、直ちに本製品の使用をお控えいただき、お支払を証明するものと一緒に同梱のすべての提供品を速やかにお買い上げいただいた販売店にご返却ください。この場合、お支払済みの代金をお返しいたします。

1. 使用権

(1)当社は、本ソフトウェアを本ドキュメントにしたがって、本製品においてのみご使用になる限定的で非独占的且つ譲渡不能な権利をお客様に許諾します。

(2)上記の使用権には、以下のことを実施する権利は含まれておりません。

(i) 使用許諾物の全体もしくは一部の複製、改変、翻訳、引用又は二次的著作物の作成すること。(ii)本製品及び本ドキュメントの全体又は一部を販売、賃貸、貸与、頒布、再使用許諾またはその他の方法で提供すること。(iii) 本ソフトウェアの全体もしくは一部のリバースエンジニアリング、ディコンパイル、逆アセンブルすること、またはその他の方法で使用許諾物の全体もしくは一部のソースコードを得ようと試みること。(iv) 使用許諾物に記載している、または埋込まれている著作権表示、商標表示、又はその他の財産権表示を消し去る、改変する、隠す、または判読し難くすること。 (v) 本ソフトウェアの全部又は一部を本製品以外で使用すること。(vi) 本ソフトウェアの全体又は一部を本製品と分離して提供すること。(vii) お客様の商業用ソフトウェアアプリケーションを開発するために本ソフトウェアを使用すること。(viii) 生命維持システム、体内埋込機器、原子力施設や原子力システム、又はその故障が死亡もしくは破局的な財物損害を招くこともあり得るその他の用途において使用許諾物を使用すること。(ix) 第三者に上記のいずれかを実施させる又は第三者に上記のいずれかの実施を許すこと。

(3)当社は、事前の書面によるお客様への通知により、お客様による本契約条件の遵守状況を確認する目的で、使用許諾物の使用及び利用状況を監査する権利を有するものとします。ただし、当該監査は、お客様の業務時間中においてお客様の業務の妨げにならない範囲で実施するものとします。

2. 知的財産権の帰属

本契約のいかなる規定も使用許諾物及び一切のアップデートプログラム（当社が作成したアップデートプログラムか否かを問いません）に関する無体財産権をお客様に移転させるものではなく、使用許諾物に関するすべての権利は当社又は当社への供給者に帰属します。

3. 無保証

(1)当社はお客様に対し使用許諾物に係る一切の保証をいたしません。

(2)当社は、別途お客様との間で締結するソフトウェア保守契約に基づき、使用許諾物のアップデート、機能追加、変更又はバグ修正（総称して以下「アップデート」といいます）をした場合は、かかるアップデートを行ったプログラムまたはアップデートのためのプログラム（以下「アップデートプログラム」といいます）またはかかるアップデートに関する情報をお客様に提供するものとします。ただし、当該プログラムまたは当該情報の提供の必要性、提供時期、提供方法などについては当社の判断に基づき決定するものとします。お客様に提供されたアップデートプログラムは使用許諾物の一部を構成するものとします。

4. 契約期間及び契約解除

(1)お客様は、契約解除日の 30 日以上前に当社に対する書面による通知により本契約を解除することができます。

(2)当社は、お客様が本契約のいずれかの規定を遵守しなかった場合、いつでも本契約を解除することができます。

(3)本契約の解除後、お客様はいかなる目的のためにも本製品及び本ドキュメントをご使用になれません。第 1 条第 2 項、第 1 条第 3 項、第 2 条、第 3 条、第 5 条、第 6 条、第 7 条、及び第 8 条は、本契約が解除された後にも効力が存続するものとします。

5. 輸出

お客様は、日本政府、米国政府、及び関連する外国政府の必要な許可を得ることなしに本製品及び本ドキュメントの全体又は一部を直接的又は間接的に輸出してはなりません。また、外国の規制などには準拠していないため、日本国外で使用することはできません。

6. 責任の限定

当社又は当社の販売店は、本契約から生じる、使用許諾物の使用もしくは使用不能から生じる代替物品もしくは代替サービスの調達コスト、逸失利益、間接損害、特別損害、派生的損害、付随的損害または懲罰的損害賠償金（損害発生につき当社が予見し、または予見し得た場合を含みます）について、いかなる責任も負わないものとします。また、当社又は当社の販売店が損害賠償責任を負う場合には、その法律上の構成の如何を問わず、お客様が支払った本製品の対価のうち使用許諾物の代金相当額をもってその上限とします。

7. 第三者ソフトウェア

本ソフトウェアには第三者から許諾されたソフトウェアコンポーネントを含みます。これらのソフトウェアコンポーネントには、本契約の規定は適用されず、それぞれの使用許諾条件が適用されるものとします。これらのソフトウェア及びその使用条件の詳細については、製品に同梱されている取扱説明書に記載されている本項目をご確認ください。

8. 一般規定

(1)本契約は、日本国の法律に準拠し、同国の法律にしたがって解釈されます。

(2)本契約にかかわる一切の紛争の解決については、東京地方裁判所をもって第一審の専属的合意管轄裁判所として解決するものとします。

(3)お客様は、当社の書面による事前の同意なしに本契約又は本契約上の権利もしくは義務を、任意、法律の運用、その他の態様にかかわらず、承継、譲渡もしくは委任してはなりません。

(4)本契約は、本契約の対象事項に関する当社とお客様との間の完全な合意を規定するものであり、従前の一切の了解、合意、意図の表明又は了解覚書に代わるものとします。

(5)The Software is a “commercial item” as that term is defined in 48 C.F.R. 2.101, consisting of “commercial computer software” and “commercial computer software documentation” as such terms are used in 48 C.F.R. 12.212. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4, NEC Platforms provides the Software to U.S. Government End Users only pursuant to the terms and conditions therein.

9. お問い合わせ先

Aterm Biz インフォメーションセンター（10 章を参照してください）へお問い合わせください。

1.10. 本製品の環境ポイント

- **包装材の配慮**：再生紙を使用しています。

1.11. 商標について

Aterm は、日本電気株式会社の登録商標です。

NetMeister、ホーム IP ロケーションは、NEC プラットフォームズ株式会社の登録商標です。

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。

Microsoft Azure は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

OSX、Safari は、米国および他の国々で登録された Apple Inc.の商標です。

Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。

Bluetooth は、Bluetooth SIG,Inc の登録商標です。

AWS、Amazon Web Services は、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。

本マニュアルおよび本製品に記載されている会社名、製品・サービス名は、各社の商標、または登録商標です。

1.12. 安全にお使いいただくために

本書には、あなたや他の人々への危害や財産への損害を未然に防ぎ、本製品を安全にお使いいただくために、守っていただきたい事項を示しています。その表示と図記号の意味は次のようになっています。内容をよく理解してから本文をお読みください。

本書中のマークの説明

⚠ 警　告：人が死亡する、または重傷 (※1) を負う可能性が想定される内容を示しています。

⚠ 注　意：人が軽傷 (※2) を負う可能性が想定される内容、および物的損害 (※3) のみの発生が想定される内容を示しています。

（※ 1） 重傷とは、失明、けが、やけど（高温・低温・化学）、感電、骨折、中毒などで後遺症が残るものおよび治療に入院・長期の通院を要するものをいう。

（※ 2） 軽傷とは、治療に入院や長期の通院を要さないけが、やけど、感電などをいう。

（※ 3） 物的損害とは、家屋・家財および家畜・ペットなどにかかわる拡大損害 を指す。

⚠ 警　告

電源

1. 日本国内 100V AC の電源以外では使用しないでください。火災、感電の原因となります。差し込み口が 2 つ以上ある壁の電源コンセントに他の電気製品の AC アダプタを差し込む場合は、合計の電流値が電源コンセントの最大値を超えないように注意してください。火災、感電、故障の原因となります。

- 電源コードを傷つけたり、破損したり、加工したり、無理に曲げたり、引っ張ったり、ねじったり、たばねたりしないでください。火災、感電の原因となります。また、重いものをのせたり、加熱したりすると電源コードが破損し、火災、感電の原因となります。
- AC アダプタは、たこ足配線にしないでください。たこ足配線にするとテーブルタップなどが過熱、劣化し、火災の原因となります。
- AC アダプタおよび電源コードは、必ず本製品に添付のものをお使いください。また、本製品に添付の AC アダプタおよび電源コードは、他の製品に使用しないでください。火災、感電、故障の原因となります。
- 本製品に添付の AC アダプタおよび電源コードは、必ず一体で使用し、他の AC アダプタや電源コードを組み合わせて使用しないでください。火災、感電、故障の原因となります。
- AC アダプタにものをのせたり布を掛けたりしないでください。過熱し、ケースや電源コードの被覆が溶けて火災、感電の原因となります。
- AC アダプタは風通しの悪い狭い場所（収納棚や本棚の後ろなど）に設置しないでください。過熱し、火災や破損の原因となることがあります。また、AC アダプタは、電源コンセントの近くに設置し、容易に抜き差し可能な状態でご使用ください。
- 本製品の AC アダプタは屋内専用ですので、屋外で使用しないでください。雨水などがかかり、感電、故障の原因となります。
- AC アダプタ本体が宙吊りにならないように設置してください。電源プラグと電源コンセント間に隙間が発生し、ほこりによる火災が発生する可能性があります。

こんな時には

- 万一、煙が出ている、変なにおいがするなどの異常状態のまま使用すると、火災、感電の原因となります。すぐに本製品の AC アダプタをコンセントから抜いてください。煙が出なくなるのを確認してから、お問い合わせ先にご連絡ください。お客様による修理は危険ですから絶対におやめください。
- 本製品を水や海水につけたり、ぬらしたりしないでください。万一内部に水が入ったり、ぬらしたりした場合は、すぐに本製品の AC アダプタをコンセントから抜いて、お問い合わせ先にご連絡ください。そのまま使用すると、火災、感電、故障の原因となることがあります。
- 本製品の通風孔などから内部に金属類や燃えやすいものなどの、異物を差し込んだり落としたりしないでください。万一、異物が入った場合は、すぐに本製品の AC アダプタをコンセントから抜いて、お問い合わせ先にご連絡ください。そのまま使用すると、火災、感電、故障の原因となることがあります。
- 電源コードが傷んだ状態（芯線の露出・断線など）のまま使用すると、火災、感電の原因となります。すぐに本製品の AC アダプタをコンセントから抜いて、お問い合わせ先にご連絡ください。
- 万一、本製品を落としたり破損したりした場合は、すぐに本製品の AC アダプタをコンセントから抜いて、お問い合わせ先にご連絡ください。そのまま使用すると、火災、感電の原因となることがあります。
- 本製品は人命に直接関わる医療機器や、極めて高い信頼性を要求されるシステム（幹線通信機器や電算機システムなど）では使用しないでください。社会的に大きな混乱が発生する恐れがあります。
- 本製品を分解・改造しないでください。火災、感電、故障の原因となります。
- ぬれた手で本製品を操作したり、接続したりしないでください。感電の原因となります。
- 本製品の内部や周囲でエアダスターやダストスプレーなど、可燃性ガスを使用したスプレーを使用しないでください。引火による爆発、火災の原因となります。

その他の注意事項

- 航空機内や病院内などの無線機器の使用を禁止された区域では、本製品の電源を切ってください。電子機器や医療機器に影響を与え、事故の原因となります。
- 本製品は、高精度な制御や微弱な信号を取り扱う電子機器や心臓ペースメーカなどの近くに設置したり、近くで使用したりしないでください。電子機器や心臓ペースメーカなどが誤動作するなどの原因となることがあります。また、医用電気機器の近くや病院内など、使用を制限された場所では使用しないでください。
- 本製品のそばに花びん、植木鉢、コップ、化粧品、薬品や水の入った容器、または小さな金属類を置かないでください。こぼれたり中に入ったりした場合、火災、感電、故障の原因となることがあります。
- 湯沸かし器や加湿器のそばなど、湿度の高いところでは設置および使用はしないでください。火災、感電、故障の原因となることがあります。
- 温泉地など、硫化水素の発生するところや、海岸などの塩分の多い場所で使用しないでください。本製品の寿命が短くなることがあります。
- 本製品の使用中や使用直後に、本製品本体やコネクタなどの突起物が高温になる場合があります。特に、本製品は金属ケースで覆われており、やけどなどの恐れがありますので注意してください。

⚠ 注 意

設置場所

- 直射日光の当たるところや、ストーブ、ヒータなどの発熱器のそばなど、温度の高いところに置かないでください。内部の温度が上がり、火災の原因となることがあります。
- 温度変化の激しい場所（クーラーや暖房機のそばなど）に置かないでください。本製品の内部に結露が発生し、火災、感電、故障の原因となります。
- 本製品は温度 0～40℃、湿度 10～90%の結露しない環境でご使用ください。
- 調理台のそばなど油飛びや湯気が当たるような場所、ほこりの多い場所に置かないでください。火災、感電、故障の原因となることがあります。
- ぐらついた台の上や傾いたところなど、不安定な場所に置かないでください。また、本製品の上に重いものを置かないでください。バランスがくずれて倒れたり、落下したりしてけがの原因となることがあります。
- 通風孔をふさがないでください。通風孔をふさぐと内部に熱がこもり、火災の原因となることがあります。次のような使いかたはしないでください。
  - ✓ 収納棚や本棚、箱などの風通しの悪い狭い場所に押し込む
  - ✓ じゅうたんや布団の上に置く
  - ✓ テーブルクロスなどを掛ける
- 本製品を重ね置きしないでください。重ね置きすると内部に熱がこもり、火災の原因となることがあります。縦置きでご使用になる場合は、必ず添付のスタンドを使用して、本製品の周囲に十分なスペースを確保してください。
- 本製品は垂直面以外の壁や天井などには取り付けないでください。振動などで落下し、故障、けがの原因となります。

電源

- 本製品の電源プラグはコンセントに確実に差し込んでください。抜くときは、必ず電源プラグを持って抜いてください。電源コードを引っ張るとコードが傷つき、火災、感電、故障の原因となることがあります。
- 本製品の電源プラグとコンセントの間のほこりは、定期的（半年に 1 回程度）に取り除いてください。火災の原因となることがあります。
- 本製品のお手入れをする際は、安全のため必ず AC アダプタをコンセントから抜いてください。感電の原因となることがあります。
- 移動させる場合は、本製品の AC アダプタをコンセントから抜き、外部の接続線を外したことを確認の上、行ってください。コードが傷つき、火災、感電の原因となることがあります。
- 長期間ご使用にならないときは、安全のため必ず本製品の AC アダプタをコンセントから抜いてください。
- 本製品の使用中や使用直後に AC アダプタが高温になる場合があります。やけどなどの恐れがありますので注意してください。

禁止事項

- 雷が鳴りだしたら、電源コードに触れたり周辺機器を接続したりしないでください。落雷による感電の原因となります。
- 本製品に乗らないでください。壊れてけがの原因となることがあります。
- オプションの外付けアンテナ利用時は、外付けアンテナで誤って目を傷つけないように注意してください。
- 外付けアンテナを持って本製品を持ち上げたり移動したりしないでください。故障や破損の原因となることがあります。

1.13. **本製品の故障を防ぐために**

本製品の本来の性能を発揮できなかったり、機能停止を招いたりする内容を示しています。

設置場所

- 次のようなところへの設置は避けてください。
  - ✓ 振動が多い場所
  - ✓ 気化した薬品が充満した場所や、薬品に触れる場所
  - ✓ 電気製品・AV・OA 機器などの磁気を帯びている場所や電磁波が発生している場所（電子レンジ、スピーカー、テレビ、ラジオ、蛍光灯、電気こたつ、インバータエアコン、電磁調理器など）
  - ✓ 高周波雑音を発生する高周波ミシン、電気溶接機などが近くにある場所
- 本製品をコードレス電話機やテレビ、ラジオなどの近くで使用すると、コードレス電話機の通話にノイズが入ったり、テレビ画面が乱れたりするなど受信障害の原因となることがあります。このような場合は、お互いを数 m 以上離してお使いください。
- 本製品と無線 LAN 端末の距離が近すぎるとデータ通信でエラーが発生する場合があります。このような場合は、お互いを 1m 以上離してお使いください。
- 本製品を壁掛けで使用する場合、同じ場所に長期間設置すると、壁紙が変色（色あせ）する場合があります。

禁止事項

- 落としたり、強い衝撃を与えたりしないでください。故障の原因となることがあります。
- 製氷倉庫など特に温度が下がるところに置かないでください。本製品が正常に動作しないことがあります。
- 本製品を移動するときは、接続コードを外してください。故障の原因となることがあります。
- 動作中に接続コード類が外れたり、接続が不安定になったりすると誤動作の原因となります。動作中は、コネクタの接続部には触れないでください。
- 本製品の電源を切った後、すぐに電源を入れ直さないでください。10 秒以上の間隔をあけてから電源を入れてください。すぐに電源を入れると電源が入らなくなることがあります。

日ごろのお手入れ

- ベンジン、シンナー、アルコールなどでふかないでください。本製品の変色や変形の原因となることがあります。汚れがひどいときは、薄い中性洗剤をつけた布をよくしぼって汚れをふき取り、やわらかい布でからぶきしてください。 ただし、コネクタ部分は、よくしぼった場合でもぬれた布では絶対にふかないでください。
- 水滴がついている場合は、乾いた布でふき取ってください。

1.14. データおよび無線 LAN のセキュリティについて

データの破損について

通信中に本製品の電源が切れたり、本製品を取り外したりすると、通信エラーが生じ、データが壊れることがあります。

ログ送信機能ご使用時におけるセキュリティに関するご注意

本製品のログ送信機能を使用する場合は、Syslogサーバとのデータの通信経路を暗号化するなどセキュアな通信経路を設定してください。

セキュリティ対策をほどこさずセキュリティの問題が発生してしまった場合、当社はこれによって生じた損害に対する責任は一切負いかねますのであらかじめご了承ください。

無線 LAN 製品ご使用時のセキュリティに関するご注意

無線 LAN では、Ethernet 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親機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危険性があります。
- 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）

  コンピュータウイルス等を流しデータやシステムを破壊する（破壊）

  等の行為の危険性があります。

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。

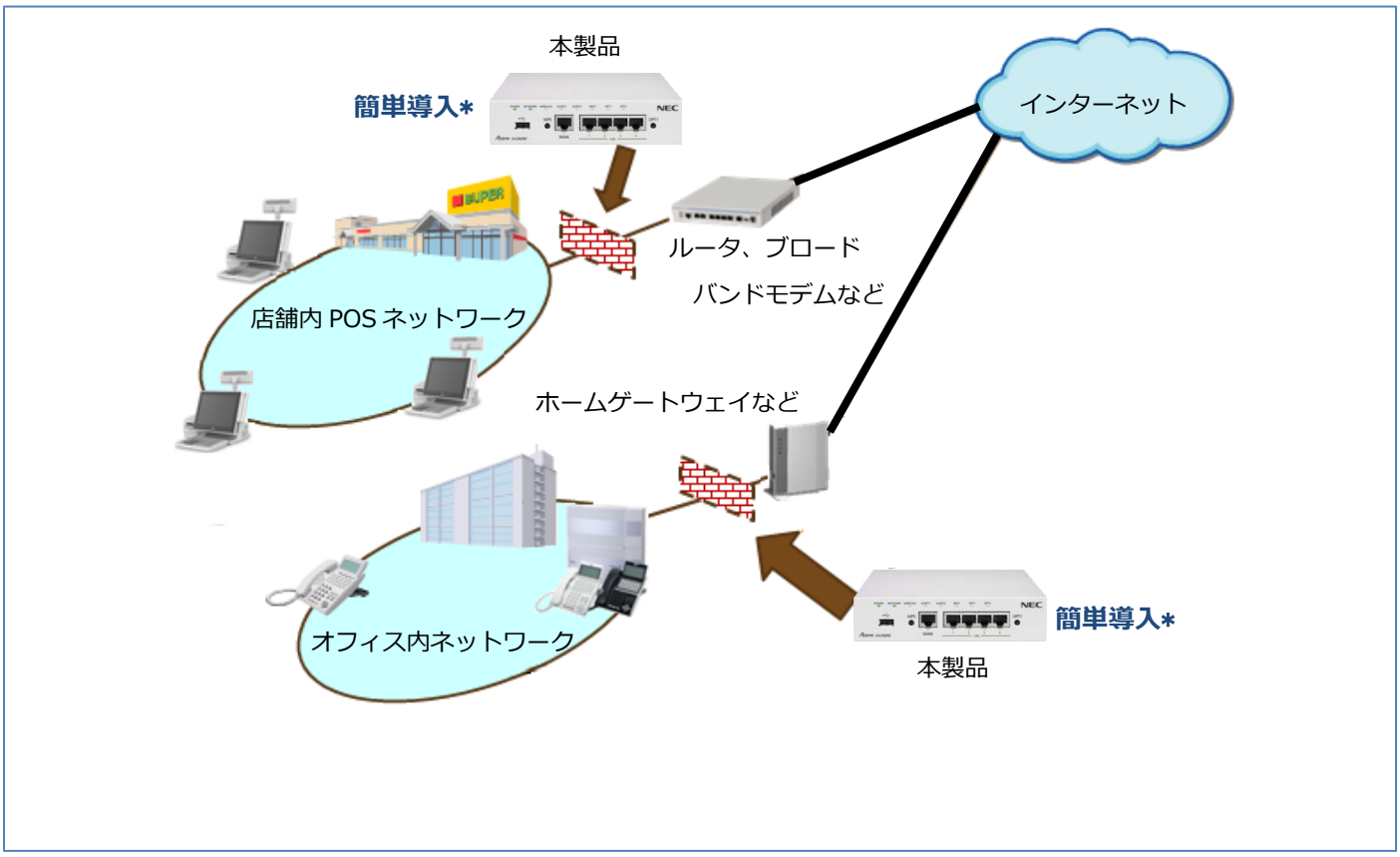
セキュリティ対策をほどこさず、あるいは、無線 LAN の仕様上やむをえない事情によりセキュリティの問題が発生してしまった場合、当社はこれによって生じた損害に対する責任は一切負いかねますのであらかじめご了承ください。

2. 製品について

本製品は、ネットワークの入口に設置するだけで、送受信するメールに添付されたファイルやWebからのダウンロードファイルに含まれたウイルスなどを検知・無害化、インターネットからの不正侵入の防止、社員が誤って危険なサイトにアクセスすることを防止するなど、複数の機能を１つにまとめ、様々なサイバー攻撃の脅威から自社のネットワークを防御するセキュリティアプライアンスです。本章では、本製品の概要と仕様について説明します。

2.1. 概要

高速転送を誇る Aterm 機器に高速処理可能なセキュリティ・スキャン機能を実装し、高速転送を可能にしながらセキュリティの高いネットワークを構築可能にする SMB 向けのセキュリティアプライアンスです。既存のネットワークを変更せずにセキュリティを高めたいお客様に適した機器です。



本製品は、ブリッジモード、ルータモードの 2 つのモードがあります。
お客様のネットワークに合わせてお使いいただけます。

2.2. **特長**

✓ 簡単設置

本製品はブリッジモードが利用でき、既存の社内ネットワーク構成を変えることなく、導入することができます。

本製品の設定は Web ブラウザを用いたシンプルでわかりやすい GUI で行えますので、ブリッジモードではネットワークの専門的な知識やセキュリティ機器に関する知識をお持ちでない方でも、設定・運用いただくことができます。

✓ 高速セキュリティエンジン

多くのセキュリティ端末は、セキュリティ・スキャン機能を使用すると常にネットワークの通信を管理／解析するため、ネットワークの転送スピードが遅くなりがちです。本製品は高速セキュリティエンジンを採用することで、セキュリティ・スキャン機能が有効な状態でも、約700Mbps[1]の高スループットを実現しています。

✓ 日本に合った安全対策を提供

株式会社ラック [2]とパートナー契約を締結し、同社が提供する JSIG、および JLIST(2020 年 7 月以降)を組み込んだシグネチャ（ウイルスなど定義ファイル）を採用しています。同社はグローバルにウイルス、不正プログラム、フィッシングサイトなどの情報を収集するだけでなく、日本の最新情報も加えて解析を行うことで、より日本のネットワーク環境に合ったシグネチャを提供しており、安全にネットワークを利用できます。本製品はこの最新のシグネチャをライセンス期間に合わせて定期的に自動更新して提供します。

✓ デバイスマップ機能

本製品の管理画面上で、配下ネットワークに属するデバイスを視覚的に確認できます。今まで管理しきれなかった社内ネットワークのデバイス構成がひと目でわかり、管理効率の向上が期待されます。

✓ 簡易 RADIUS 機能

本製品を簡易的な RADIUS サーバとして使用することができます。社内 LAN に不正なデバイスが接続できないよう、認証を設けることができます。認証用に別途サーバを構築する必要がなく、セキュアな接続環境を安価に実現いたします。

✓ NetMeister 機能

NetMeister から SA3500G のシリアル番号(製造番号)や接続状態、UTM ライセンス有効期限の確認、 SA3500G のコンフィグ管理やファームウェア更新などをリモートから操作できます。また、UTM 脅威レポートをご確認いただけます。

✓ UNIVERGE Aspire 連携

オフィスコミュニケーションゲートウェイ UNIVERGE Aspire WX（別売）[3]との連携により、脅威検出状態・新しいファームウェアの有無・ライセンスの有効期限をお手元の電話機で確認することができます。

✓ ルータ機能

管理画面（設定 Web）で動作モードをルータモードに変更できます。小規模ネットワーク上のルータの機能を本製品で兼ねることができます。ルータモードではネットワークの専門的な知識を必要とします。

✓ その他機能

管理画面（設定 Web）にて、ネットワークに接続されている端末の各種情報の確認と管理ができます。

脅威検出状況を日・週・月の時間単位で集計表示できます。また、端末ごとの集計も可能な上、検出が多い順に並べたグラフ表示にも対応し、潜在的な脅威リスクを把握し易くなります。管理画面では検出ログの確認や許可設定などもできます。

---

[1]当社の試験環境にて測定した結果です。

[2]株式会社ラックについて

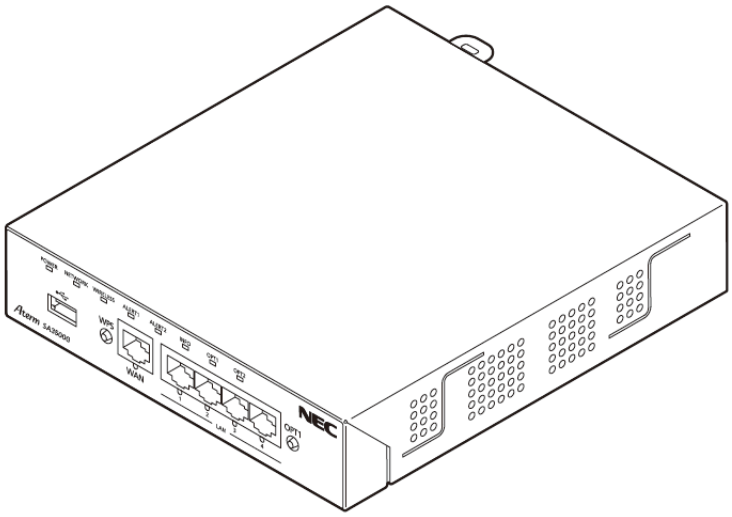
サイバーセキュリティ分野のリーディングカンパニーとして、業界屈指のセキュリティ技術を駆使し、セキュリティ対策に必要なすべての支援を先端の IT トータルソリューションサービスとして官公庁・企業・団体等のお客様に提供しています。不正アクセス監視のための JSOC(Japan Security Operation Center)を官公庁や大企業を主要顧客として運営、大企業向けハイエンドセキュリティ機器向けに攻撃分析情報「JSIG」を配信し、高い評価を受けています。セキュリティ事故発生時の緊急対策支援としてサイバー救急センターの運営も行っています。詳細は株式会社ラックの HP でご確認ください。（https://www.lac.co.jp/）

[3] UNIVERGE Aspire WX（https://www.necplatforms.co.jp/product/aspire_wx/）

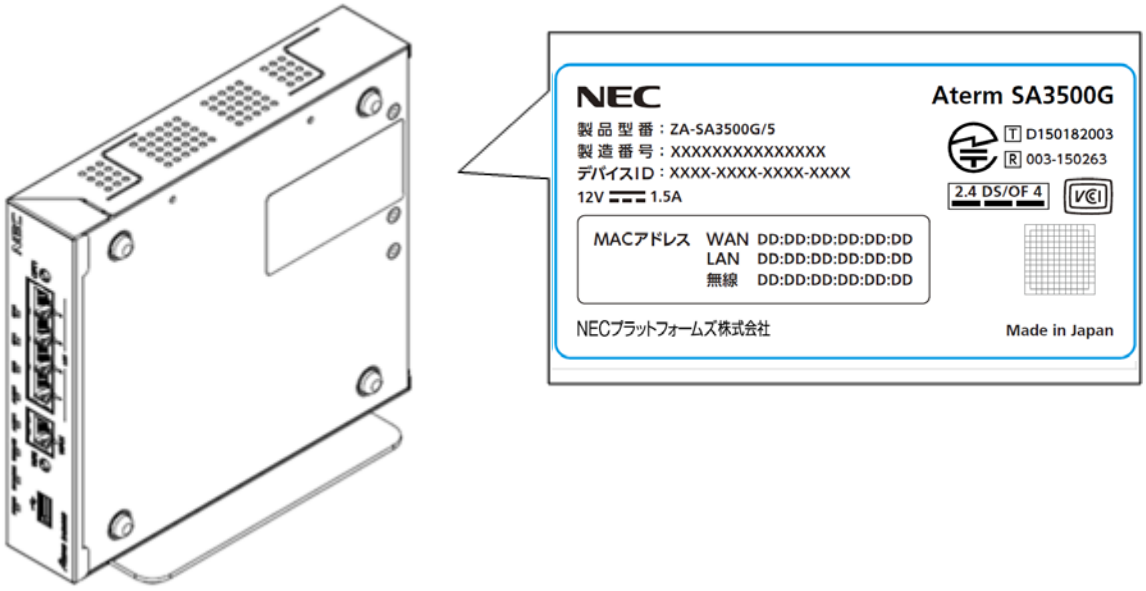
2.3. 製品仕様

2.3.1. 製品外観

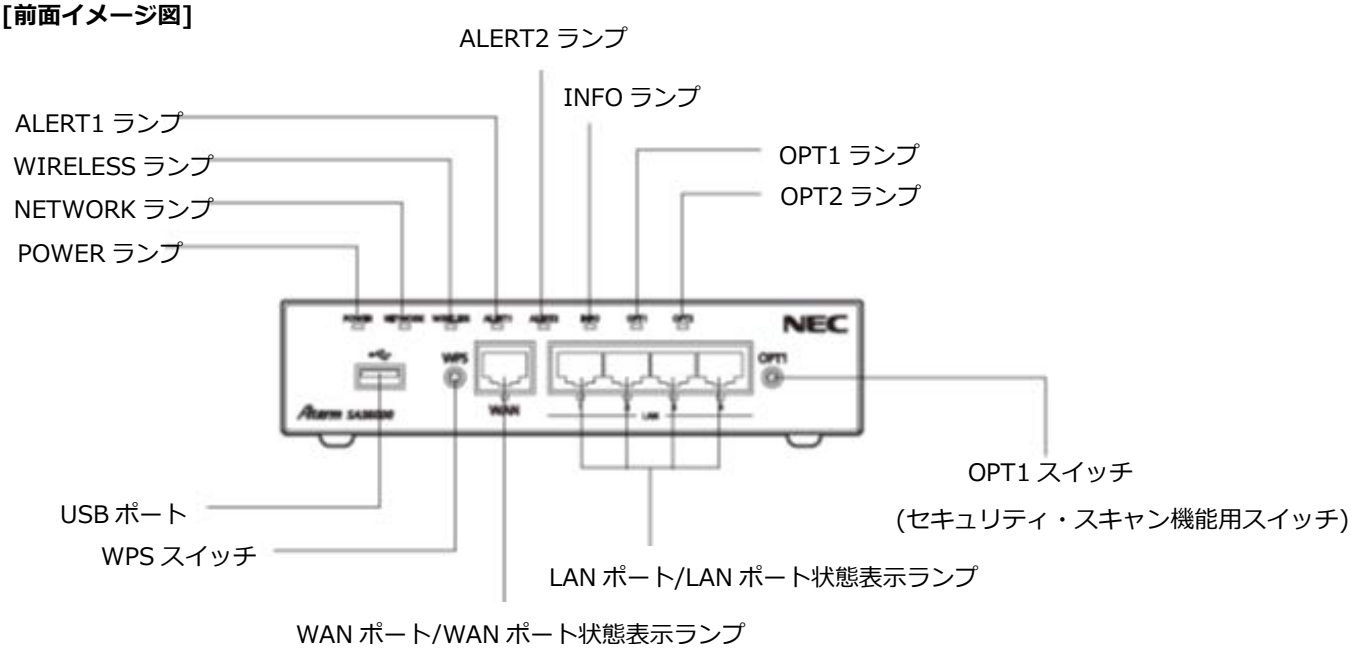
[斜視イメージ図]



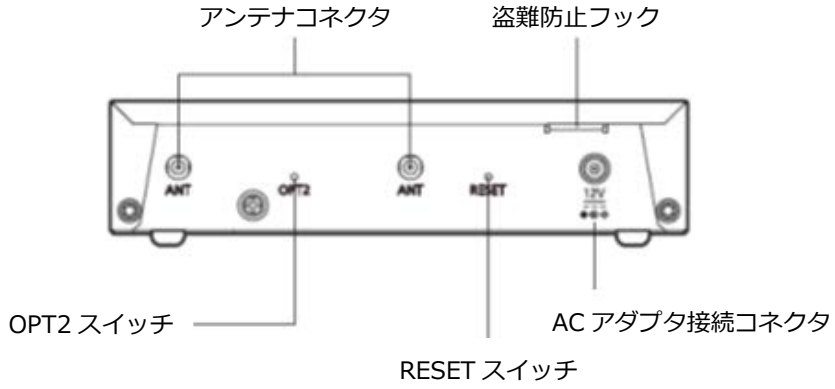
[底面イメージ図（スタンド取り付け時）]



[前面イメージ図]



[背面イメージ図]



2.3.2. **基本仕様**

[ハードウェアの主要諸元]

項目		仕様		備考
WAN インタフェース	物理ｲﾝﾀﾌｪｰｽ	8 ピン モジュラージャック（RJ-45）		UTP ケーブル(CAT5e 以上)
	ポート数	1 ポート		
	タイプ	1000BASE-T/100BASE-TX（IEEE802.3ab/IEEE802.3u） Auto MDI/MDI-X		
LAN インタフェース	物理ｲﾝﾀﾌｪｰｽ	8 ピン モジュラージャック（RJ-45）		UTP ケーブル(CAT5e 以上)
	ポート数	4 ポート		
	タイプ	1000BASE-T/100BASE-TX（IEEE802.3ab/IEEE802.3u） Auto MDI/MDI-X		
無線 LAN インタフェース	アンテナ	内蔵アンテナ、外付けアンテナ（オプション）		設定 Web でアンテナ切り替え選択 ※1
	IEEE802.11n	周波数帯域/チャネル	2.4GHz 帯(2400~2484MHz)/1~13ch	
		伝送速度	最大 300Mbps（HT40 の場合）	
	IEEE802.11g	周波数帯域/チャネル	2.4GHz 帯(2400~2484MHz)/1~13ch	
		伝送速度	54/48/36/24/18/12/9/6 Mbps	
	IEEE802.11b	周波数帯域/チャネル	2.4GHz 帯(2400~2484MHz)/1~13ch	
		伝送速度	11/5.5/2/1Mbps	
USB インタフェース	物理ｲﾝﾀﾌｪｰｽ	タイプ A コネクタ		※2
	ポート数	1 ポート		
	タイプ	USB2.0 Bus Power 対応（500mA 給電）		
ランプ	機能表示	3 色(緑/赤/橙) x8 POWER/NETWORK/WIRELESS/ALERT1/ALERT2/INFO/OPT1/OPT2		
	LAN/WAN 状態表示	LAN Link/ACT 状態表示（緑）x4 WAN Link/ACT 状態表示（緑）x1		
スイッチ		プッシュスイッチ（RESET/OPT1/OPT2/WPS）		
動作保証環境		温度：0~40℃ 湿度：10~90%		結露しないこと
保管条件		温度：-20～60℃ 湿度：90%以下		結露しないこと
外形寸法		約 174(W) x 195(D) x 40(H)mm		突起部/スタンドを除く
電源		EIAJ RC5320A Type4 DC ジャック DC12V/1.5A		専用 AC アダプタ(添付品)からの供給
専用 AC アダプタ		入力：100V AC ± 10% 50Hz/60Hz ± 5% 出力：DC12V/2.0A AC インレットタイプ		添付品
消費電力		35VA(21W)以下		
発熱量		75.9kJ/h=18.1kcal/h 以下		
本体質量		0.9kg 以下		スタンド、ネジ、ゴム足除く
冷却方式		自然空冷（ファンレス）		
設置方法		横置き、縦置き、壁掛け		壁掛けは壁掛けキット（オプション）により対応
筐体色		白（塗装）		ベース/背面は未塗装（材質色）
対応法令および品質規格		VCCI クラス B		
		電安法		
		電気通信事業法		
		電波法		

※1 伝送速度は、規格による理論上の速度であり、実速度は無線環境、接続機器に依存します。

※2 USB ポートはファームウェアバージョン 3.4.31 以降でご使用になれます。

[ファームウェアの主要諸元]

項目		仕様	備考
NAPT セッション管理		最大 30,000 セッション	機能の説明は 3.6.8 章を参照してください。
PPPoE セッション確立数		1 セッション	機能の説明は 3.6.9 章を参照してください。
DHCP サーバ	払い出し IP アドレスの最大数	250	機能の説明は 3.6.11 章を参照してください。 リース時間は設定 Web で変更可能です。5.7.7 章を参照してください。
	リース時間	24 時間	
無線 LAN 端末接続台数		32 台以下推奨	機能の説明は 3.7 章を参照してください。
ブリッジ	MAC アドレスラーニングテーブル数	最大 256 エントリ	機能の説明は 3.9.2 章を参照してください。
	MAC アドレスラーニングテーブルエージングタイマ	300 秒	
IPv4 パケットフィルタ		50 エントリ(インタフェースごと)	設定項目については 5.6.6 章を確認してください。
MAC アドレスフィルタリング	有線 LAN 端末	60 エントリ	設定項目については 5.6.7 章を確認してください。
	無線 LAN 端末	60 エントリ	
IPv4 静的ルーティングテーブル数		50 エントリ	設定項目については 5.7.12 章を確認してください。
NAT エントリ(ポートマッピングエントリ)		50 エントリ	設定項目については 5.7.10 章を参照してください。
セキュリティ・スキャン機能の個別許可	アンチウイルス	10 件	個別許可の設定可能件数については 5.8 章の各設定項目を参照してください。
	不正侵入防止	100 件	
	Web ガード	10 件	
	URL フィルタリング	100 件	
	URL キーワードフィルタリング	100 件	
SPI タイマ	TCP	初期値　900 秒(ブリッジモード) 初期値　3,600 秒(ルータモード)	SPI タイマの値を設定 Web で変更できます。5.8.3 設定については、章を参照してください。
	UDP	初期値　300 秒	
	ICMP	初期値　30 秒	
NAPT セッションタイマ	TCP	初期値　3,600 秒	TCP/UDP/ICMP の NAPT セッションタイマの値を設定 Web で変更できます。設定については、5.8.3 章を参照してください。
	UDP	初期値　300 秒	
	ICMP	初期値　30 秒	
	その他	初期値　600 秒	

2.3.3. **ランプ表示**

表示名称	ランプ表示	説明	備考
POWER	緑点灯	電源が入っている状態	通常状態
	橙点滅	FlashROM、USB ストレージへの書き込み中の状態	本製品の電源を OFF にしないでください。一定時間橙点滅後、他表示状態へ移行します。
	赤点灯	装置起動に失敗した状態	
	赤点滅 (5 秒) → 橙点滅 → 緑点灯	ファームウェアを復旧している状態	ファームウェアの復旧とは、起動用ファームウェアが破損している場合、工場出荷ファームウェアで復旧する動作のことです。
	消灯	電源が入っていない状態	
NETWORK （ブリッジ モード時）	橙点灯	IP アドレス取得済みの状態	
	橙点滅	IP アドレス取得処理中の状態	
	消灯	WAN ポートおよび LAN ポートのいずれのポートもリンクが確立していない状態	
NETWORK （ルータ モード時）	緑点灯	IP アドレス取得済みの状態	
	緑点滅	IP アドレス取得処理中の状態	
	消灯	WAN ポートのリンクが確立していない状態	
WIRELESS ※1	緑点灯	無線 LAN の通信が可能な状態	
	緑点滅	データが送受信されている状態	
	橙点滅	無線 LAN の設定（WPS）中の状態	
	赤点滅	無線 LAN の設定（WPS）に失敗した状態	
	消灯	無線 LAN を使用していない状態	
ALERT1	橙点灯	脅威を検出し除去した状態 ※2	橙点滅から 60 秒経過後
	橙点滅	脅威を検出してから 60 秒間の状態 ※2	
	消灯	脅威を検出していない状態	
ALERT2	緑点灯	セキュリティ・スキャン機能の準備中の状態	アクティベーション後、セキュリティ・スキャン機能動作前
	緑点滅	アクティベーション成功後、ファームウェア更新処理の完了待ちの状態	新しいファームウェアがある場合、アクティベーション成功後にファームウェア更新を行います。ファームウェア更新による再起動後、あるいはファームウェア更新が行われなかった場合は消灯状態へ移行します。
	橙点灯	アクティベーションしていない状態	
	橙点滅	アクティベーション処理中の状態	
	赤点灯	セキュリティ・スキャン機能のライセンス満了の状態	
	赤点滅	セキュリティ・スキャン機能のライセンス期限満了まで 60 日間を切った状態	
	消灯	セキュリティ・スキャン機能を利用可能な状態	
INFO	橙点灯	バージョンアップ可能なファームウェアがある状態	
	橙点滅	ファームウェアをバージョンアップ中の状態	正常終了後は再起動する 失敗した場合は橙点灯に戻る

	緑点滅	更新ファームウェアを確認している状態	緑点滅してから 3 秒後に以下の表示になります。 更新ファームウェアがあるとき：橙点灯 更新ファームウェアがないとき：消灯
	消灯	バージョンアップ可能なファームウェアがない状態	
OPT1 ※3	緑点灯	IPsec(クラウドサービス接続を含む)通信可能な状態	IPsec トンネル確立済み
	橙点灯	IPsec(クラウドサービス接続を含む)接続処理中の状態	IPsec トンネル未確立
	消灯	IPsec(クラウドサービス接続を含む)を使用していない状態	
OPT2	橙点灯	USB ストレージが使用可能の状態	
	緑点灯	USB ストレージが使用可能で、かつ、下記のいずれかの状態 ●USB ストレージへの設定値の保存に成功した状態 ●USB ストレージからの設定値の復元に成功した状態	
	赤点灯	USB ストレージが使用不可能の状態 USB ストレージが使用可能で、かつ、下記のいずれかの状態 ●USB ストレージへの設定値の保存に失敗した状態 ●USB ストレージからの設定値の復元に失敗した状態	
	消灯	USB ストレージが接続されていない状態 USB ストレージ以外の USB デバイスが接続されている状態	
WAN	緑点灯	WAN ポートのリンクが確立している状態	
	緑点滅	WAN ポートでデータの送受信中の状態	
	消灯	WAN ポートのリンクが確立していない状態	
LAN	緑点灯	LAN ポートのリンクが確立している状態	
	緑点滅	LAN ポートでデータの送受信中の状態	
	消灯	LAN ポートのリンクが確立していない状態	

※1　無線 LAN はファームウェアバージョン 3.1.26、3.1.34、3.1.35 ではルータモードでご使用になれます。3.2.29 以降ではルータモードとブリッジモード双方でご使用になれます。

※2　ALERT1 ランプが橙点灯/点滅する脅威の対象は、アンチウイルス（AV）と Web ガード（WG）です。本ランプが橙点灯/点滅していても脅威は既に除去されている状態です。

※3　IPsec はルータモード時の機能です。

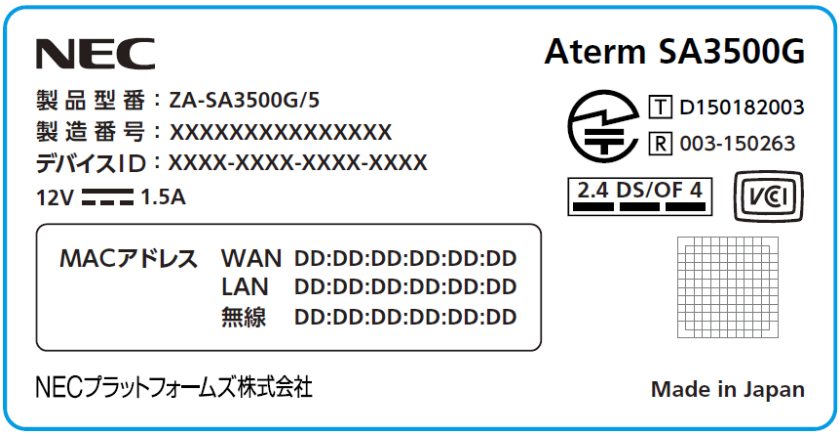
[メモ]

電源投入からシステム起動前は、すべてのランプが緑点灯します。

本製品が高負荷状態にあるときランプの点滅周期が遅くなる場合があります。

2.3.4. **装置ラベル**

■5 年ライセンス付き製品の表示例



製品型番

ZA-SA3500G/1　：1 年ライセンス付き製品

ZA-SA3500G/5　：5 年ライセンス付き製品

ZA-SA3500G/6　：6 年ライセンス付き製品

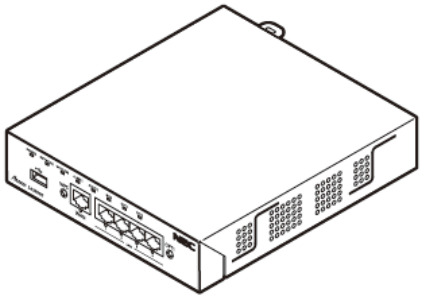
ZA-SA3500G/7　：7 年ライセンス付き製品

2.4. **構成品**

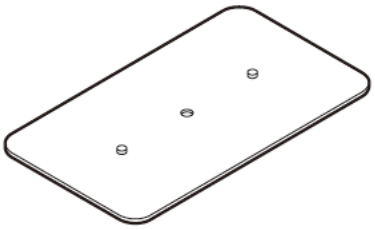
構成品が揃っていることを確認してください。

■構成品

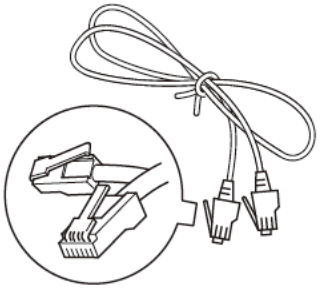
□SA3500G



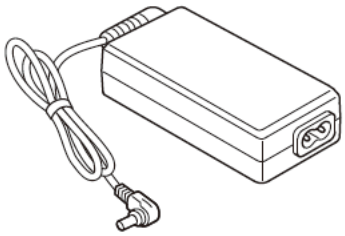
□スタンド



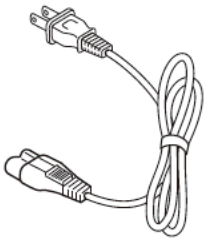
□Ethernet ケーブル
（ストレート、約 2m）



□AC アダプタ

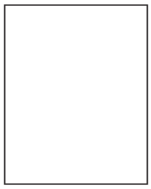


□電源コード

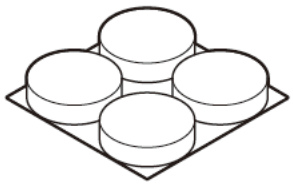


□取扱説明書

□本製品のご使用条件



□ゴム足（4 個）



□スタンド固定ネジ（1 本）

⚠ 警 告

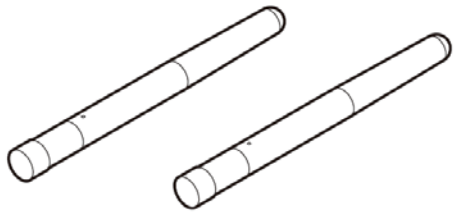
AC アダプタおよび電源コードは必ず本製品に添付のものをお使いください。また、本製品に添付の AC アダプタは、他の製品に使用しないでください。

火災、感電、故障の原因となります。

本製品のオプション品は次のとおりです。必要に応じてお買い求めください。

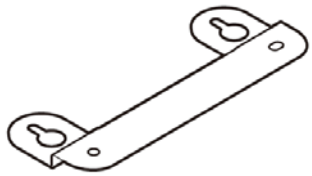
■オプション

□外付けアンテナ（2 本 1 組）（品番：ZA-SA/AN1）

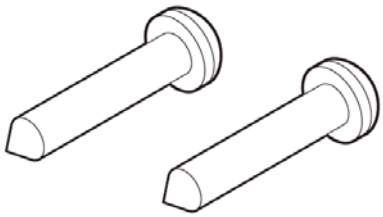


□壁掛けキット（品番：ZA-SA/MK1）

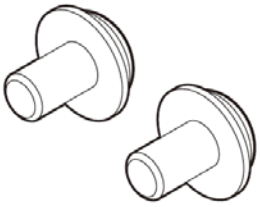
・壁掛け金具（1 個）



・木ネジ（2 本）

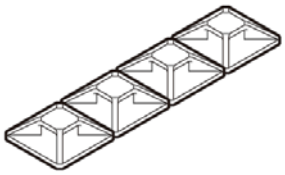


・壁掛け金具固定ネジ（2 本）



□USB クランプキット（品番：ZA-SA/UC1）

・USB 抜け防止用固定具（4 個）



・USB 抜け防止用ケーブルバンド（2 本）

※品番は、将来変更する場合があります。

3. 機能仕様

本製品の機能概要は次のとおりです。

機能	説明
セキュリティ・スキャン機能	● ファイアウォール（FW）、アンチウイルス（AV）、不正侵入防止（IPS）、Web ガード（WG）、URL フィルタリング（UF）、URL キーワードフィルタリング（KF）、アプリケーションガード（APG） ● セキュリティ・スキャン機能の関連ログや統計情報 ● メール通知 ● Aspire との連携 ● パトライトとの連携 ● セキュリティ情報の自動アップデート
基本機能	● トランスペアレントブリッジ機能 ● ルータ機能 ● NAT/NAPT ● DHCP クライアント/DHCP サーバ ● PPPoE ● IP パケットフィルタリング ● IPsec/IKEv1/IKEv2 ● MAC アドレスフィルタリング ● クラウドサービス設定
メンテナンス機能	● ネットワーク設定/確認 ● ファームウェア更新 ● 設定値の保存、復元 ● 設定の初期化 ● HTTP プロキシサーバ ● SNMPv1/SNMPv2c ● パケットダンプ ● NetMeister 機能
管理機能	● デバイス管理 ● デバイスマップ ● 簡易 RADIUS 機能
無線 LAN 機能	● IEEE802.11b/g/n(2.4GHz 帯) ● WPS

※ブリッジ機能とルータ機能は、同時動作しません。

※ファームウェアバージョンによる対応機能の違いは次のページを参照してください。

ファームウェアバージョンによる対応機能の違いは次のとおりです。

ファームウェアバージョン		3.5.9		3.5.12/ **3.6.9**	
対応動作モード		ブリッジ	ルータ	ブリッジ	ルータ
	ファイアウォール（FW）	○	○	○	○
	アンチウイルス機能（AV）	○	○	○	○
	アンチウイルス拡張スキャン	○	○	○	○
	不正侵入防止（IPS）	○	○	○	○
	Web ガード（WG）	○	○	○	○
	URL フィルタリング（UF）	○	○	○	○
	URL キーワードフィルタリング（KF）	○	○	○	○
	アプリケーションガード（APG）	○	○	○	○
	セキュリティログ	○	○	○	○
	メール通知	○	○	○	○
	パトライト連携	○	○	○	○
	Aspire 連携	○	○	○	○
	統計情報	○	○	○	○
	脅威検出の LED 表示	○	○	○	○
	デバイス管理	○	○	○	○
	デバイスマップ	○	○	○	○
	簡易 RADIUS 機能	○	○	○	○
	ファームウェア更新	○	○	○	○
	メンテナンスバージョンアップ	○	○	○	○
	時刻指定バージョンアップ	○	○	○	○
	手動ファームウェア更新(オンラインバージョンアップ)	○	○	○	○
	手動ファームウェア更新(ローカルファイル指定)	○	○	×	×
	設定値の初期化	○	○	○	○
	設定値の保存＆復元	○	○	○	○
	再起動	○	○	○	○
	時刻設定	○	○	○	○
	IPv4 パケットフィルタ	○	○	○	○
	MAC アドレスフィルタリング	○	○	○	○
	ping	○	○	○	○
	traceroute	○	○	○	○

	自己診断	○	○	○	○
	保守機能	○	○	○	○
	パケットダンプ	○	○	○	○
	NetMeister 機能	◯	×	○	×
	DNS リゾルバ機能	○	○	○	○
	IPv4 静的ルーティング	○	○	○	○
	NAPT	×	○	×	○
	PPPoE	×	○	×	○
	DHCP クライアント	○	○	○	○
	DHCP サーバ	×	○	×	○
	プロキシ DNS	×	○	×	○
	IPsec	×	○	×	○
	IKEv1	×	○	×	○
	IKEv2	×	○	×	○
	SNMPv1, SNMPv2c	○	○	○	○
	ホーム IP ロケーション機能	×	○	×	○
	クラウドサービス設定	×	○	×	○
	無線自動設定機能（WPS）	○	○	○	○
	無線暗号化	○	○	○	○
	マルチ SSID 機能	○	○	○	○
	ネットワーク分離機能	×	○	×	○
	デバイスの状態	○	○	○	○
	装置管理情報	○	○	○	○
	ルーティングテーブル	×	○	×	○
	BGP ピア状態	×	○	×	○
	VPN 接続状態	×	○	×	○
	VPN 統計情報	×	○	×	○
	MIB 情報	○	○	○	○
	イベントログ	○	○	○	○

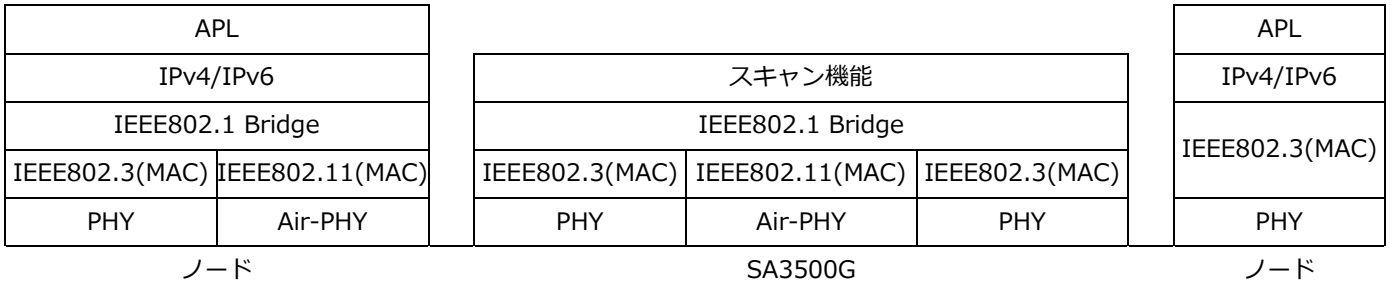
3.1. プロトコルスタック

本製品のプロトコルスタックのイメージは次のとおりです。

本製品は、入力インタフェースでセキュリティ・スキャン機能の検出対象パケットと検出対象外パケットに分類します。

3.1.1. ブリッジモード

[セキュリティ・スキャン機能の検出対象パケット]



※ セキュリティ・スキャン機能の検出対象は、IPv4 または IPv6 のパケットです。

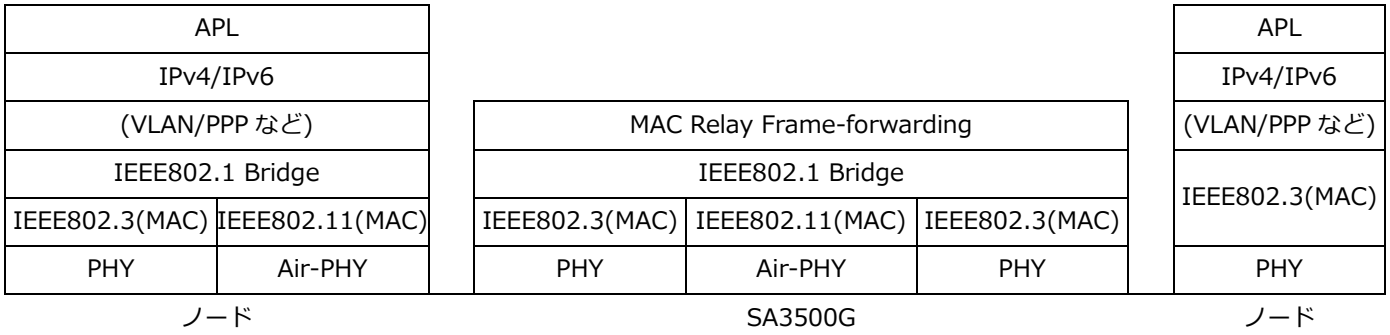
※ IPv4 over PPP over PPPoE, IPv6 over PPPv6 over PPPoE フレームに対応しています。

※ SSL/TLS パケットは一部のセキュリティ・スキャン機能のみ対応しています。

※ IP in IP パケットは、次のタイプをサポートしています。

IPv4 in IPv6、IPv6 in IPv4

[ブリッジングフレーム]

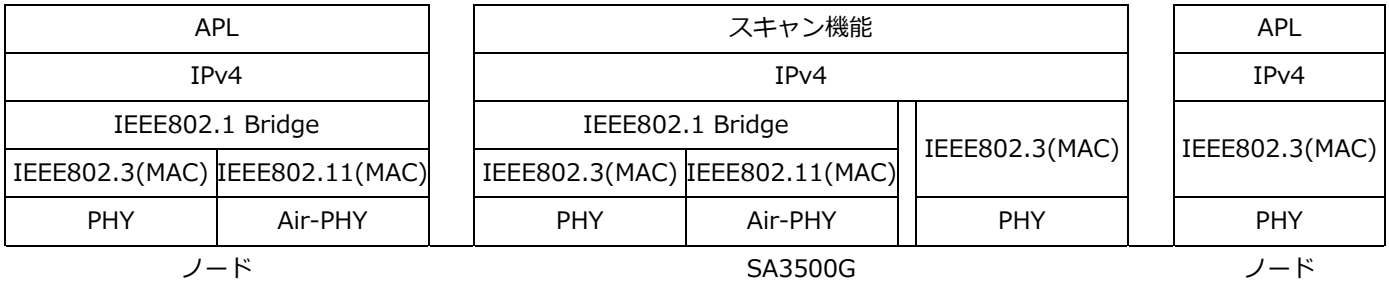


※ 下記 MAC フレームは通過しません。

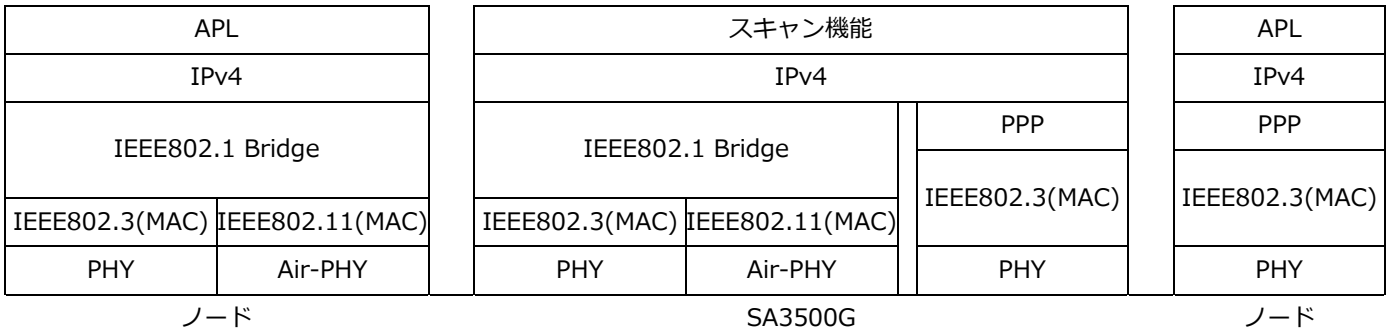
01-80-C2-00-00-03 IEEE802.1X EAPoL Frame

3.1.2. **ルータモード**

[DHCP、または固定 IP で WAN IP を設定する場合]



[PPPoE を使用する場合]



※ セキュリティ・スキャン機能の検出対象は、IPv4 パケットです。

※ SSL/TLS パケットは一部のセキュリティ・スキャン機能のみ対応しています。

3.2. **設置可能なネットワーク**

本製品を使用するには、次のネットワーク環境が必要です。

- 本製品がインターネット通信可能であること。[4]

  ・本製品自身に IPv4 アドレスが必要です。

  ・本製品は、次に述べる通信を必要とします。本製品の上位機器は、本製品の送受信トラフィックを許可してください。[5]

ファームウェアバージョン		3.1.26/3.1.34 /3.1.35		3.2.29/3.2.37 /3.2.45		3.3.20/3.3.26 /3.4.21/3.4.31/3.4.32 /3.5.9/3.5.12/**3.6.9**	
通信 ポート (プロトコル)	用途	ブリッジ	ルータ	ブリッジ	ルータ	ブリッジ	ルータ
TCP Port=80 (HTTP)	本製品のライセンス処理やシグネチャの更新、ファームウェア情報の取得および更新 ※URL フィルタリング機能で使用するポートは 3.3.10 章を参照してください。	○	○	○	○	○	○
TCP Port=443 (HTTPS)		○	○	○	○	○	○
TCP Port=8080 (URL フィルタリング)		○	○	—	—	—	—
TCP Port=8081 (URL フィルタリング)		—	—	○	○	—	—
UDP Port=53 (DNS)		○	○	○	○	○	○
UDP Port=67 (DHCP)	IP アドレス自動取得	○	○	○	○	○	○
UDP Port=123 (NTP)	本製品の時刻合わせ	○	○	○	○	○	○
TCP Port=17285 (アンチウイルス)	アンチウイルス機能の拡張スキャン機能を使用する場合	—	—	○	○	—	—
UDP Port=500 (ISAKMP)	IPsec 機能やクラウドサービス接続	—	—	—	○	—	○
UDP Port=4500 (ISAKMP)		—	—	—	○	—	○
TCP Port=179 (BGP)		—	—	—	—	—	○
Protocol=50 (ESP)		—	—	—	○	—	○
Protocol=1 (ICMP)	自己診断機能を使用する場合	—	—	○	○	○	○

※本製品の WAN/LAN ポートは、1000BASE-T/100BASE-TX のオートネゴシエーションで動作します。設定 Web にて速度固定の設定も可能です。

[4] 本製品のライセンス処理やシグネチャ（ウイルス情報などの定義ファイル）の更新処理で必要です。

[5] ファイアウォールを設置している場合など、必要に応じて、本トラフィックを許可してください。

3.2.1. **ブリッジモード**

対応可否欄： ○…制限事項はありません　○＊…一部制限があります（＊は補足説明欄を参照）　×…本製品は対応できません

ネットワーク	対応可否	補足説明
ルータ（ブロードバンドルータまたはホームゲートウェイを含む）を設置している。	○	
IPv6 のみのネットワークである	×	本製品の動作にはインターネットへ IPv4 プロトコルで接続できることが必要です。
VLAN を利用している	○＊	本製品を VLAN ネットワークの外側に設置してください。
IEEE802.1X で端末を認証している	○＊	本製品を IEEE802.1X 認証ネットワークの外側に設置してください。 ・本製品は EAPoL/EAP フレームを通過しません。

8.1 章のネットワーク接続構成例を参照してください。

ブリッジモードのときのみ、本製品は IPv6 パケットのインスペクションをします。一部制限としてファイアウォール機能については、インスペクションせずに通過させるか遮断かを設定 Web で選択します。設定は 5.8.3 章を参照してください。

3.2.2. **ルータモード**

対応可否欄： ○…制限事項はありません　○＊…一部制限があります（＊は補足説明欄を参照）　×…本製品は対応できません

ネットワーク	対応可否	補足説明
IPv4 のネットワークである	○	
IPv4/IPv6 混在のネットワークである	○*	本製品は、IPv6 パケットに対応していません。
IPv6 のみのネットワークである	×	本製品の動作にはインターネットへ IPv4 プロトコルで接続できることが必要です。
UPnP を使用する	×	本製品は UPnP に対応していません。
VLAN を利用している	○＊	本製品を VLAN ネットワークの外側に設置してください。
IEEE802.1X で端末を認証している	○＊	本製品を IEEE802.1X 認証ネットワークの外側に設置してください。 本製品は EAPoL/EAP フレームを通過しません。
VPN を利用している	○＊	本製品を VPN の外側に設置してください。

8.1 章のネットワーク接続構成例を参照してください。

3.3. セキュリティ・スキャン機能

3.3.1. セキュリティ・スキャン機能概要

本製品は、セキュリティ・スキャン機能として次の機能を提供します。

セキュリティ・スキャン機能	略称	検出タイプ	説明
ファイアウォール *1	FW	アクセス制御	DoS 攻撃の検出、SPI
アンチウイルス *2	AV	脅威検出	ウイルスの検出、無害化（データ書き換え）
不正侵入防止 *2	IPS	脅威検出	ネットワーク攻撃の防止
Web ガード *2	WG	Web アクセス制御	悪意のある Web サイトの検出、遮断
URL フィルタリング *2	UF	Web アクセス制御	Web サイトのカテゴリを識別、遮断
URL キーワードフィルタリング *2	KF	Web アクセス制御	お客様定義のキーワードを含む Web サイトの検出､遮断
アプリケーションガード *2	APG	アプリケーション アクセス制御	ネットワーク上のアプリケーションの識別、遮断

*1 ファイアウォール（FW）は、ファームウェアバージョン 3.2.29 でブリッジモード時にも対応しました。

*2 暗号化パケットは、アンチウイルス（AV）、不正侵入防止（IPS）、Web ガード（WG）、URL フィルタリング（UF）、URL キーワードフィルタリング（KF）、アプリケーションガード（APG）に対応していません。

※脅威検出時に通信の遮断を行わずに検出情報をログに残す機能もあります。本製品をお使いの環境で脅威の状況のみ確認したい場合にお使いください。ただし遮断動作はしませんので、お使いの環境でのセキュリティポリシーを考慮した上でお使いください。

3.3.2. スキャン対象トラフィック

スキャン対象トラフィックは次のとおりです。

モード	スキャン対象トラフィック
ブリッジモード	セキュリティ・スキャン機能の検出対象は、本製品の WAN ポートと LAN ポートを通過する IP パケットです。IPv4 および IPv6 のパケットが対象です。 ● PPPoE（PPP）フレームに対応しています。 ● SSL/TLS パケットは一部のセキュリティ・スキャン機能のみ対応しています。 ● IP in IP パケットは、次のタイプをサポートしています。 IPv4 in IPv6、IPv6 in IPv4 ※ファイアウォール機能を有効に設定した場合、IPv6 パケットを通過させるか、遮断するかの設定を、お使いの環境に合わせてください。
ルータモード	セキュリティ・スキャン機能の検出対象は、本製品の WAN ポートと LAN ポートを通過する IP パケットです。IPv4 パケットが対象です。 ● SSL/TLS パケットは一部のセキュリティ・スキャン機能のみ対応しています。 ※本製品は IPv6 のルーティング機能を搭載していないため、IPv6 のパケットのセキュリティ・スキャン機能には対応していません。

3.3.3. **あらかじめご了承ください**

本製品は、セキュリティリスクを低減させる製品です。すべてのセキュリティリスクの排除を保証するものではありません。
本製品の特性上、次の事象が発生する場合があります。

- 本製品は、シグネチャ（ウイルス定義などの情報）を定期的に更新します。シグネチャは、本製品のパフォーマンスを保つため、新しいパターンを追加する際に脅威としてリスクの低くなった古いパターンを削除することがあります。例えば、それまで遮断していたトラフィックが通過する、あるいは、それまで通過していたトラフィックを遮断する、といった事象が発生します。また、APG では、ブロック設定していたアプリケーションをスキャン対象から削除することもありますので、この場合はそのアプリケーションのトラフィックを許容することになります。他に、アプリケーションの仕様変更によりアプリケーションガード（APG）でブロックできなくなる場合があります。
- 本製品は、端末（本製品の LAN ポートの配下に設定しているパソコンなど）情報を管理し、端末ごとのトラフィックを監視します。このため、端末の数が増えると本製品の処理能力が低下する場合があります。

3.3.4. **サーバとの連携**

本製品は、サーバと連携して以下を行います。

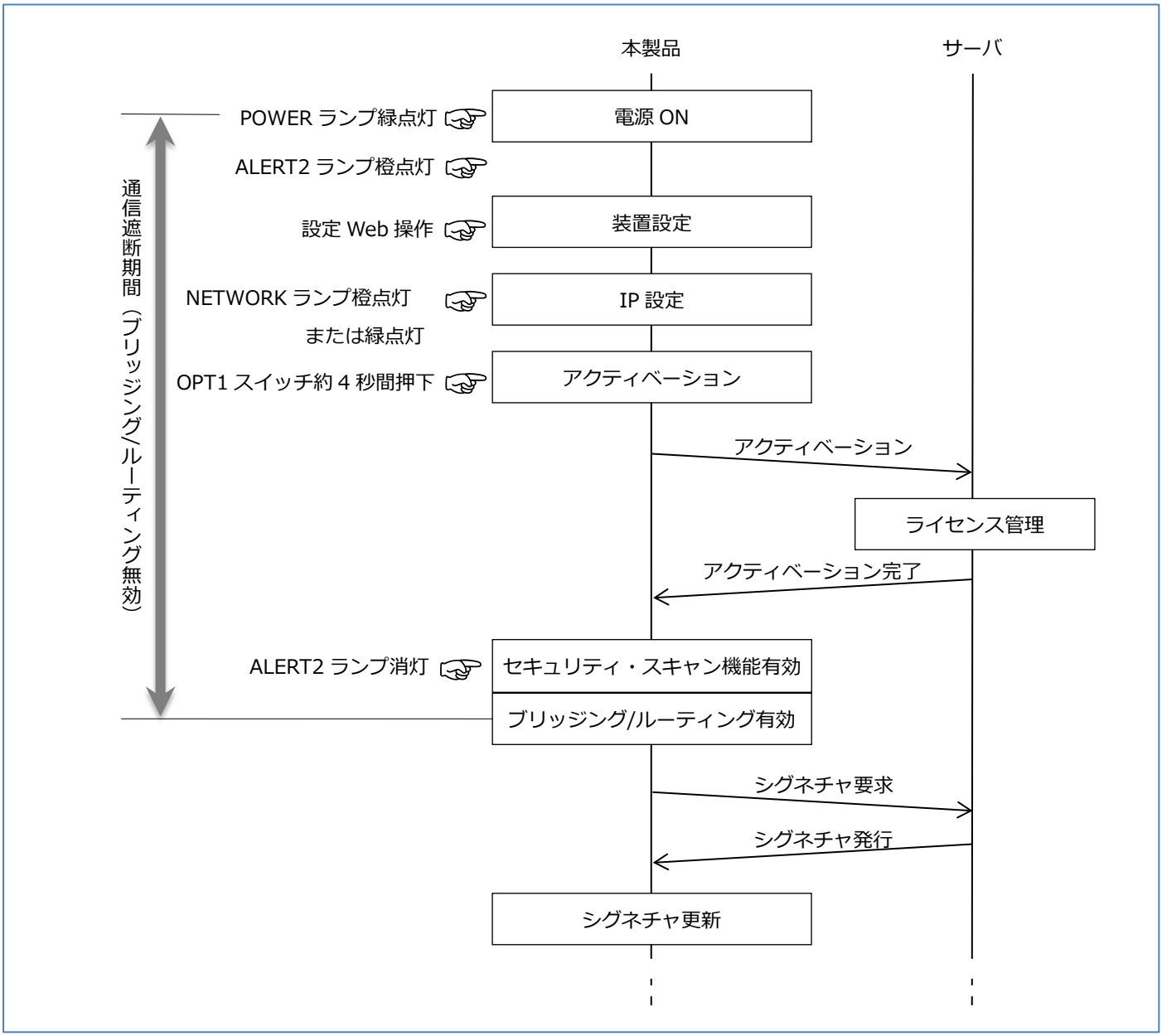
[用語説明]

ファイル	説明	補足
ライセンス	本製品のセキュリティ・スキャン機能のライセンスです。 本製品は、初回インターネット接続時にライセンスサーバにアクセスします。これにより、ライセンスサーバが本製品の管理を開始します。(アクティベーション) ライセンスサーバが本製品の管理を始めると、本製品は各種セキュリティサーバからシグネチャなどの応答を受信できるようになります。 ライセンスの状態は、ALERT2 ランプが点灯・消灯の状態で確認できます。 消灯:セキュリティ・スキャン動作中 緑点灯:ライセンスチェック前 橙点灯:アクティベーション前 ALERT2 ランプの状態の詳細は 2.3.3 章を参照してください。	
シグネチャ	各種脅威を検出する際に使用するデータベースです。 本製品を通過するトラフィック/ファイルに対し、シグネチャと一致するか否かを判断、制御します。 シグネチャは次の機能で使用します。 アンチウイルス（AV）、不正侵入防止（IPS）、Web ガード（WG）、アプリケーションガード（APG）	定期的に更新情報を確認します

[アクティベーション操作後の動作（新しいファームウェアがない場合）]

本製品のセキュリティ・スキャン機能のご使用には、初回起動時にアクティベーション操作が必要です。

アクティベーションは、「本製品の利用条件に合意し、本製品の利用を開始」することを意味します。



1. 本製品の初回起動時、本製品のシステムが起動すると ALERT2 ランプが橙点灯[6]します。
2. 本製品がインターネット通信できる状態に移行すると NETWORK ランプが橙点灯、または緑点灯します。
3. OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を約 4 秒間押し続けたら、放します。ALERT2 ランプが緑点灯に変わり、本製品はアクティベーションを開始します。
4. アクティベーションが完了しセキュリティ・スキャン機能を利用可能な状態になると ALERT2 ランプは消灯し、本製品はブリッジング動作/ルーティング機能を有効にします。[7]

※アクティベーション操作は、5.2.3 章を参照してください。

本動作はアクティベーション操作を行ったときに、本製品の新しいファームウェアがない場合のものです。

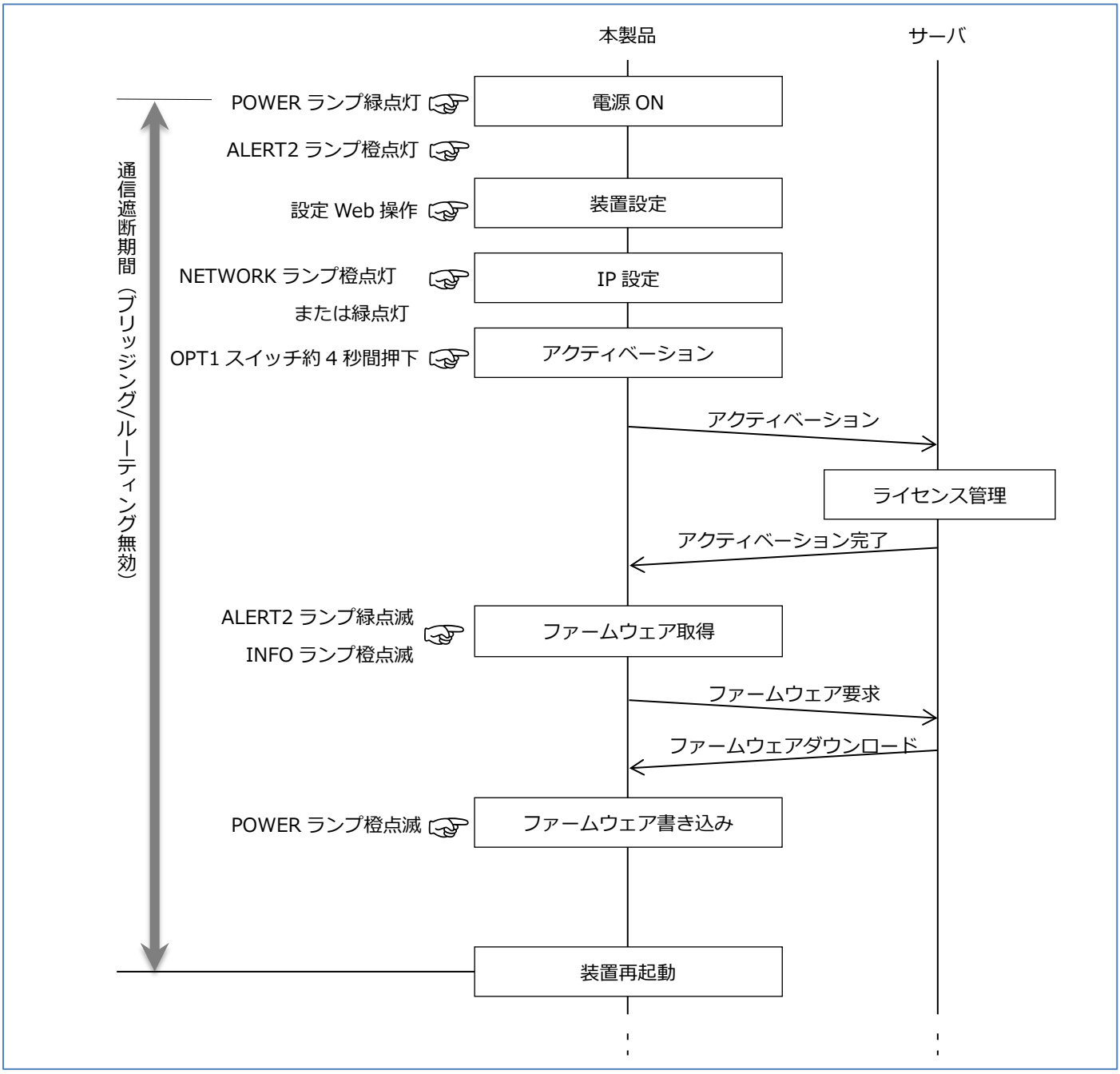
本製品の新しいファームウェアがある場合の動作は、[アクティベーション操作後の動作（新しいファームウェアがある場合）]を参照してください。

[6] ALERT2 ランプの橙点灯は、アクティベーション処理が終わっていないことを表します。

[7] この後、定期的に本製品のシグネチャの更新情報を確認します。

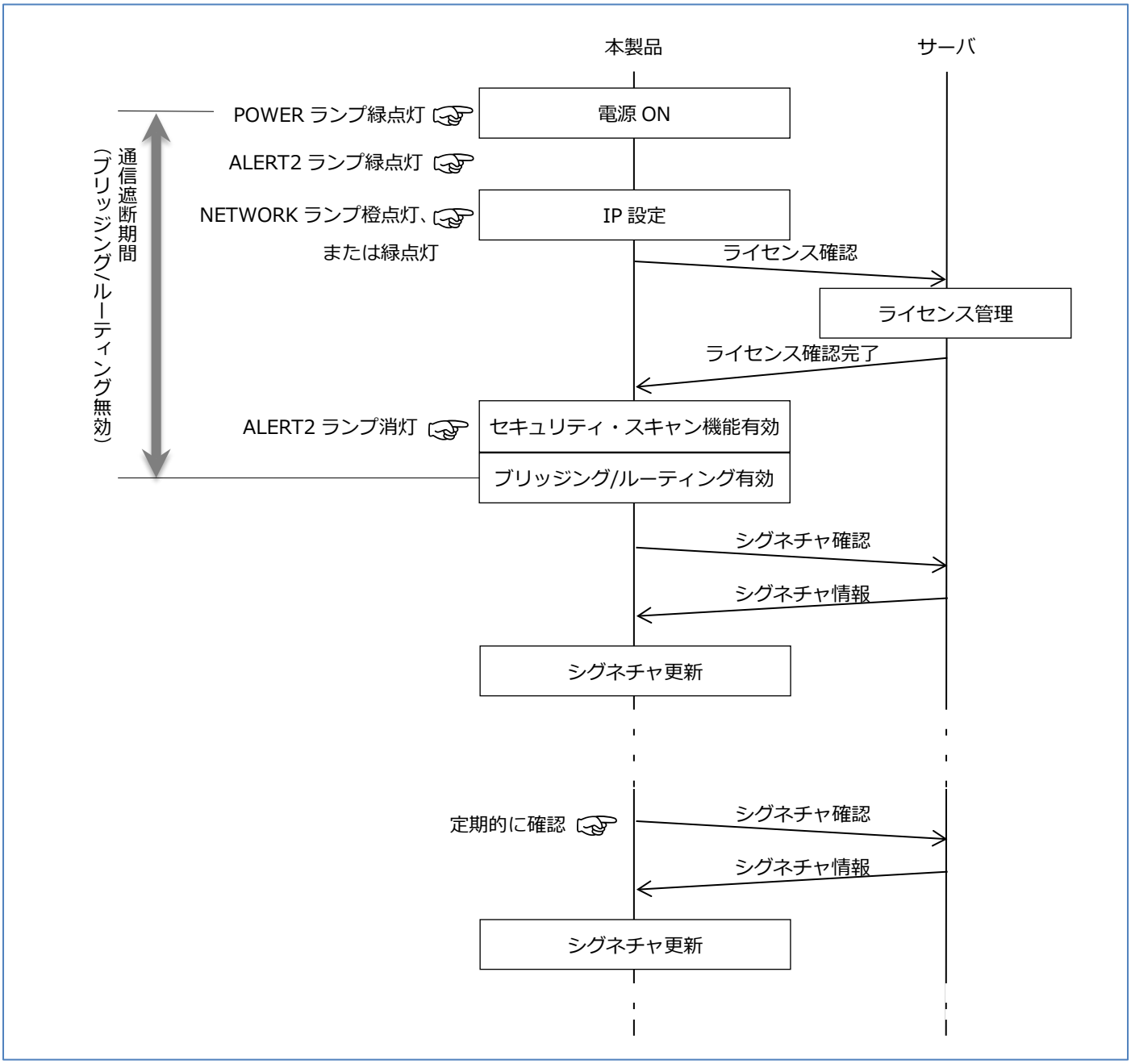
[アクティベーション操作後の動作（新しいファームウェアがある場合）]

アクティベーション操作を行ったときに、本製品の新しいファームウェアがある場合は、アクティベーション成功後にオンラインバージョンアップにより本製品のファームウェア更新を行います。アクティベーション成功後のオンラインバージョンアップの詳細は 5.2.3.1 章を参照してください。



[通常起動時の動作]

本製品起動時、ライセンスを確認します。サーバから確認完了の応答を受信すると本製品のセキュリティ・スキャン機能を有効にします。なお、セキュリティ・スキャン機能が有効になるまで、本製品のブリッジング機能・ルーティング機能は動作しません。



1. 本製品のシステムが起動すると ALERT2 ランプが緑点灯[8]します。
   このとき、セキュリティ・スキャン機能は準備中の状態です。
2. 本製品がインターネット通信できる状態に移行すると NETWORK ランプが橙点灯、または緑点灯します。
   このタイミングで、ライセンスの確認処理を実施します。
3. セキュリティ・スキャン機能を利用可能な状態になると ALERT2 ランプは消灯し、本製品はブリッジング動作/ルーティング動作を有効にします。
4. この後、定期的にシグネチャの更新情報を確認します。

[8] ALERT2 ランプの緑点灯は、セキュリティ・スキャン機能が無効の状態であることを表します。

3.3.5. **ライセンス満了時の動作**

本製品のセキュリティライセンス満了時の動作は以下のとおりです。

[ライセンス満了時の動作]

- セキュリティライセンスが満了すると、本製品のブリッジング機能/ルーティング機能を適宜無効にします。
  ※セキュリティ・スキャン機能無効時に本製品のパケット転送を行う場合は、5.8.2 章を参考に設定を変更してください。
  この設定はファームウェアバージョン 3.3.20 以降で対応しています。

ライセンスが満了したときに停止する機能は以下のとおりとなります。

機能	動作	参照
MAC アドレスフィルタリング	ライセンス期限が満了した後に本製品にアクセスした端末のアクセス履歴が表示されなくなります。	5.6.7 章
アンチウイルス	アンチウイルス機能が停止します。	5.8.4 章
不正侵入防止	不正侵入防止が機能停止します。	5.8.5 章
Web ガード	Web ガード機能が停止します。	5.8.6 章
URL フィルタリング	URL フィルタリング機能が停止します。 URL カテゴリクエリのカテゴリの確認結果が「カテゴリを確認できませんでした。」となります。	5.8.7 章
URL キーワードフィルタリング	URL キーワードフィルタリング機能が停止します。	5.8.8 章
アプリケーションガード	アプリケーションガード機能が停止します。	5.8.9 章
デバイスマップ	デバイスマップ画面で、本製品に接続された端末数の表示が「0」になります。	5.9.2 章
デバイス管理	デバイス管理対象端末の自動追加が停止します。アクセス履歴の参照で「追加可能なデバイスはありません。」と表示されます。	5.9.3 章
セキュリティ・スキャン機能のステータス	セキュリティ機能のシグネチャバージョン表示で情報欄が「-」となります。 シグネチャの定期更新が停止します。	6.1.3 章
セキュリティ・スキャン機能のセキュリティログ	日付が変わったときに、FlashROM にセキュリティログを保存する機能が停止します。	6.1.11 章
セキュリティ・スキャン機能の統計情報	日付が変わったときに、FlashROM に統計情報を保存する機能が停止します。 デバイス選択ダイアログの IP アドレス欄と情報欄の表示「-」となります。	6.1.12 章

[ライセンス満了の判定について]

- 次のどちらかの場合にライセンス満了と判定します。
  ・本製品に設定された時刻がライセンス期限を過ぎた場合。
  ・本製品がサーバにライセンス確認を行った結果、ライセンス期限満了と判定された場合。
  ライセンス満了、およびライセンス満了の 60 日前の時刻判定は、本製品に設定された時刻を基準にしています。正しく時刻判定するために、本製品の時刻は実際の時刻に合わせてお使いください。
- ライセンスが満了する 60 日前から、ALERT2 ランプが赤点滅します。
- ライセンスが満了すると ALERT2 ランプが赤点灯します。

[追加ライセンス(1 年)によるライセンス延長について]

1 年、5 年、6 年のライセンス付き製品に対して、基本保守を含むライセンス年数を 1 年(365 日)延長するために「Aterm SA3500G 追加ライセンス(1 年)」(品番：ZA-SA/LA1)を別売オプションで用意しています。本製品のライセンス延長可能期間は、ご利用開始日から初期ライセンス期間を含め最大 7 年です。本製品のライセンスを延長する場合は、本製品のライセンスが満了する前にご購入手続きをお願いいたします。なお、ライセンスが満了する 60 日前から、ALERT2 ランプが赤点滅しライセンス満了が近づいていることをお知らせします。

また、追加ライセンス(1 年)のご購入時には、専用の「購入申込書」に本製品の製造番号、デバイス ID、ライセンス満了日などの情報を記載いただく必要があります。 以下 URL の「製品説明・申込書記入要領」をよくお読みの上、本製品をご購入されました販売店・営業窓口へご注文をお願いいたします。

https://www.necplatforms.co.jp/product/security_ap/add_license.html

[追加ライセンス(1 年)ご購入後のライセンス満了日の確認作業について]

追加ライセンス(1 年)をご購入後に、当社のライセンスサポート係よりお客様のメールアドレス宛てに「Aterm SA3500G 追加ライセンス(1 年) 通知書」にて、延長後のライセンス満了日をお知らせいたします。本通知書が届きましたら、必ず通知書の案内にしたがって、本製品の設定 Web 画面で、ライセンス満了時刻(満了日)が延長されていることを確認してください。

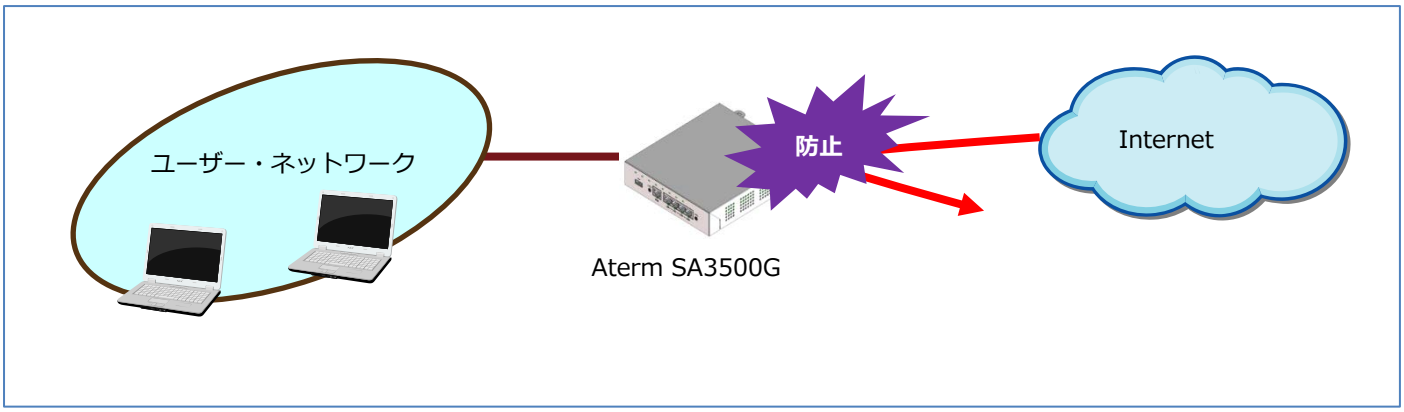
[ライセンス満了時刻(満了日)の確認手順]

- ファームウェアバージョン 3.4.21 以降をご利用の場合
  1.[TOP]-[セキュリティ]-[ステータス]画面を開きます。
  2.「ライセンス満了時刻」欄の満了時刻(満了日)を確認します。
  3.「Aterm SA3500G 追加ライセンス(1 年) 通知書」が届いているにもかかわらず、本製品の満了時刻(満了日)が延長されていない場合は、「ライセンスを確認する」ボタンを押下してください。
  ※「ライセンスを確認する」ボタンは、ファームウェアバージョン 3.4.21 以降に搭載されています。

- ファームウェアバージョン 3.3.26 以前をご利用の場合
  1.「Aterm SA3500G 追加ライセンス(1 年) 通知書」の案内にしたがって、確認してください。

3.3.6. **ファイアウォール（FW）**

DoS 攻撃などの不正アクセスを検出し、不正アクセスパケットを廃棄します。本製品はステートフルパケットインスペクション(SPI)機能により外部からの不正アクセスを遮断します。ステートフルパケットインスペクションとは、ファイアウォールを通過するパケットのデータを読み取り、内容を判断して動的にポートを開放・閉鎖する機能です。



[検出内容]

・WAN ポートからのアクセスパケット

・LAND 攻撃、Smurf 攻撃、IP スプーフィング攻撃

[脅威を検出した際の動作・通知の振る舞い]

検出時の動作	検出時の通知方法	検出状態の解除方法
外部からの不正アクセスを遮断、およびログ出力	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

[セキュリティ機能の停止方法]

セキュリティ機能の停止操作は、セキュリティリスクを増大させます。そのため、機能の停止はお客様の責任で実施してください。

停止方法	備考
「ファイアウォール設定」の「機能を使用する」のチェックを外し、無効に変更する（5.8.3 章参照）	

3.3.7. **アンチウイルス（AV）**

ウイルスや危険なコードが含まれるプログラムを検出した場合にプログラムを書き換え無害化する機能です。[9]

ホームページの閲覧やメール受信、その他のアプリケーションの通信を監視し、ダウンロードまたはアップロードするファイルにウイルスが混入していないかをチェックします。ダウンロードまたはアップロードするファイルにウイルスが混入している場合、ファイルの内容を書き換えてファイルを無害化します。

- 圧縮ファイルや複数のパケットにまたがるファイル（フラグメントパケット）に対応しています。
- 暗号化されている場合（SSL 通信やパスワード付き圧縮ファイル）は対応していません。

[検出内容]

ウイルス、スパイウェア、トロイの木馬、ワーム

[検出対象のプロトコル]

プロトコル	説明
HTTP	検出対象のポート番号　：1~65535 検出対象の HTTP メソッド　：GET（上り方向、下り方向）, POST（上り方向）
FTP	検出対象のポート番号　：20, 21
SMTP	検出対象のポート番号　：25, 587 検出対象のエンコード　：base64, quoted-printable, Uuencode 検出対象のファイル形式　：eml
POP3	検出対象のポート番号　：110 検出対象のエンコード　：base64, quoted-printable, Uuencode 検出対象のファイル形式　：eml
IMAP4	検出対象のポート番号　：143 検出対象のエンコード　：base64, quoted-printable, Uuencode

[9] 当該パケットを書き換えた後に送出します。（ファイルを書き換えるため、例えば、exe ファイルを実行できません）拡張スキャンをご利用の場合、パケットの書き換えのために通信を一度リセットすることがあります。詳細は 7.1.30 章を参照してください。

[検出対象のファイルタイプ]

シグネチャで検出を行うファイル：

ファームウェアバージョン	シグネチャで検出を行うファイル
Ver3.0.1 以降	・exe, dll, com, elf, scr, js

拡張スキャン有効時に当社で管理するデータベースサーバで検出を行うファイル:

ファームウェアバージョン	データベースサーバで検出を行うファイル
Ver3.2.29～3.5.12	・doc (doc(x), ppt(x), xls(x), msi), pdf, bat, cmd, vbs, wsf, com, js ※com, js はシグネチャとデータベースサーバの双方で検出を行います。
Ver3.6.9 以降	・doc (doc(x), ppt(x), xls(x), msi), pdf, bat, cmd, vbs, wsf, exe, dll, com, elf, scr, js ※exe, dll, com, elf, scr, js はシグネチャとデータベースサーバの双方で検出を行います。

[検出対象の圧縮ファイル]

gz, zip, rar, jar, apk

[圧縮ファイルのスキャンサイズ指定オプション]

スキャンする範囲（スキャンサイズ）を設定 Web で変更できます。

圧縮ファイルは圧縮した状態のファイルサイズを指定してください。

本機能をオフにした場合、ファイルのすべての範囲をスキャンします。

[個別許可設定]

特定のウイルスタイプを脅威検出対象外に設定できます。

[脅威を検出した際の動作・通知の振る舞い]

- ブロック設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ウイルス混入ファイルを無害化	・ALERT1 ランプ *1 橙点滅（60 秒）⇒橙点灯 ・セキュリティログにログ表示 （設定 Web にて閲覧が必要） ・メール通知 *2 ・Aspire の多機能電話のボタンランプ表示 *3 ・パトライト社対応機器でのランプ表示 *2	ALERT1 ランプの橙点灯は次のいずれかの方法で解除してください ・OPT1 スイッチを数秒間押し続ける ・設定 Web でセキュリティログを閲覧 ・Aspire の多機能電話による解除

*1：Web ガード機能による検出時も同様に通知します。

そのため、どちらの機能によって検出されたのかを確認するには、セキュリティログを閲覧してください。

*2：設定 Web で設定が必要です。(5.8.10 章参照)

*3：Aspire 側の設定が必要です。

- ログのみ設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ログ出力のみ	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

[セキュリティ機能の停止方法]

正常なファイルを脅威と誤検出する際は、次の方法により一時的に機能を停止してください。

セキュリティ機能の停止操作は、セキュリティリスクを増大させます。そのため、機能の停止はお客様の責任でご確認の上で実施してください。

停止方法	備考
「アンチウイルス設定」の「機能を使用する」のチェックを外し、無効に変更する（5.8.4 章参照）	

[**拡張スキャンについて]**

拡張スキャンは当社が管理するデータベースサーバに対象のファイルから計算した値を送信し、 データベースサーバ上でスキャン処理を行います。このためパケットの転送速度が低下する恐れがあります。 対象のファイル自体をデータベースサーバに送信することはありません。

拡張スキャンを使用するには、以下の TCP ポートが通信できる環境が必須です。

ファームウェアバージョン	使用するポート
Ver3.2.29～3.2.45	TCP ポート=17285
Ver3.3.20 以降	TCP ポート=443

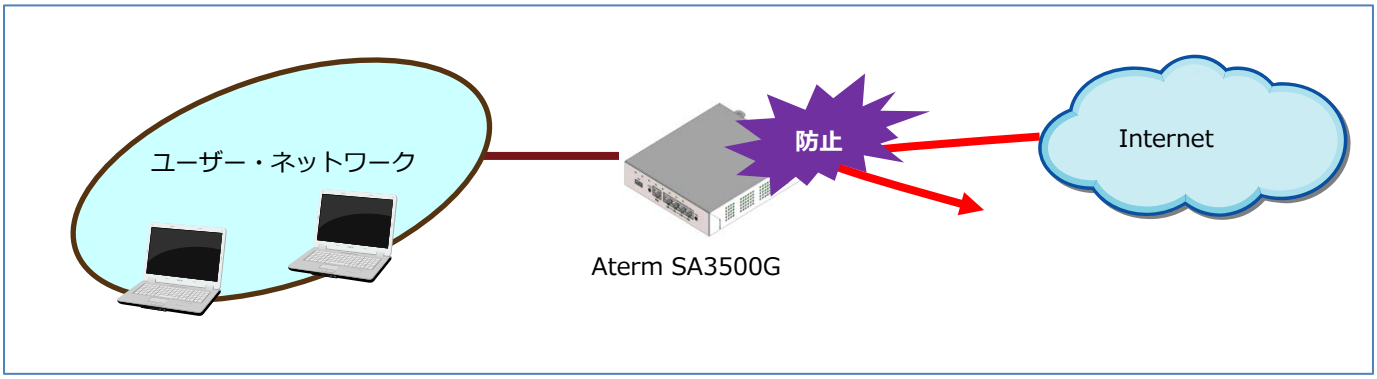
[メモ]

2019 年以降、国内で猛威を振るうマルウェア Emotet に感染した添付ファイルの無害化に対応しています。添付ファイルを無害化するため、添付ファイルを開くことが出来なくなります。

なお、新たな亜種も次々と確認されており、定期配信しているシグネチャなどにより対策を強化していますが、ご利用の皆様におかれましても、添付ファイル付きのメール等には十分ご注意いただくことを推奨しています。(2020 年 10 月現在)

3.3.8. **不正侵入防止（IPS）**

トラフィック内の攻撃コードなどの異常を検知し、異常を検知したトラフィックを遮断します。



あらかじめ登録された侵入手口のパターンとマッチングさせることにより検出し、通信を防止することで、ファイアウォールでは検知できないネットワークに対する攻撃を認識、防止することができます。

[検出内容]

異常プロトコル、異常トラフィック、ポートスキャン

[脅威を検出した際の動作・通知の振る舞い]

- ブロック設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
外部からの不正侵入アクセスを遮断、またはログ出力 *1	・セキュリティログにログ表示 （設定 Web にて閲覧が必要） ・メール通知 *2 ・パトライト社対応機器でのランプ表示 *2	–

*1： プロトコル不正を検出した場合は、通信を遮断せず、ログメッセージを出力します。
プロトコル不正とは、脅威が検出されない通信のうち、TCP/IP のプロトコルに完全にしたがっていない通信を意味します。
本通信は、脅威が検出されない通信であるため、遮断されません。もちろん、脅威を検出した場合は、その通信を遮断します。

*2： 設定 Web にて設定が必要です。(5.8.10 章参照)

- ログのみ設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ログ出力のみ	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

[個別許可設定]

脅威検出された特定の通信を脅威検出対象外に設定することができます。

[セキュリティ機能の停止方法]

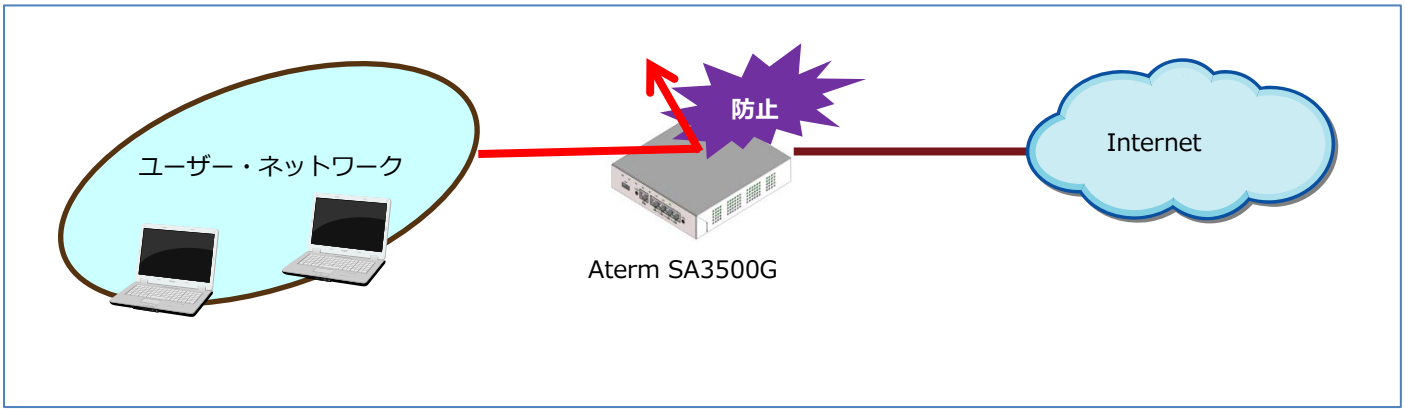
外部からの正常なアクセスを脅威と誤検出する際は、次の方法により一時的に機能を停止してください。

セキュリティ機能の停止操作は、セキュリティリスクを増大させます。そのため、機能の停止はお客様の責任でご確認の上で実施してください。

停止方法	備考
「不正侵入防止設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.5 章参照）	

3.3.9. **Web ガード（WG）**

フィッシングサイトや閲覧によってウイルス感染を起こすなどの危険な Web サイトへのアクセスをガードします。



[検出内容]

危険な Web サイトへのトラフィックを検出し、当該 Web サイトへのアクセスを遮断します。

トラフィックの種類	説明
HTTP トラフィック	URL のホスト名とパス名を使用して、危険な Web サイトへのトラフィックかどうかを判断します。
HTTPS トラフィック	URL のホスト名を使用して、危険な Web サイトへのトラフィックかどうかを判断します。

危険な Web サイトへのトラフィックだと判断した場合、次の動作により、当該 Web サイトへのアクセスを遮断します。

トラフィックの種類	説明
HTTP トラフィック（GET）	「危険なサイトへのアクセスを検出したため、通信をブロックしました。」の画面を表示します。
HTTP トラフィック（POST）	当該 Web サイトへの通信を遮断します。
HTTPS トラフィック（GET, POST）	当該 Web サイトとの SSL ハンドシェークを失敗させます。

[検出対象のプロトコル]

プロトコル	説明
HTTP	検出対象のポート番号　　：80 検出対象の HTTP メソッド　：GET, POST
HTTPS	検出対象のポート番号　　：443 検出対象の HTTP メソッド　：GET, POST

※HTTP1.0 は、検出できない場合があります。

※通信内容によっては 80 ポート以外も検出できる場合があります。

[個別許可設定]

特定の Web サイトへのアクセスを脅威検出対象外に設定することができます。

[脅威を検出した際の動作・通知の振る舞い]

- ブロック設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
該当 Web サイトへのアクセスを遮断	・ALERT1 ランプ *1 橙点滅（60 秒）⇒橙点灯 ・ブラウザにブロックした旨を表示 （HTTP のブロック表示例）  (HTTPS のブロック表示例) *2  ・セキュリティログにログ表示 （設定 Web にて閲覧必要） ・メール通知 *3 ・Aspire の多機能電話のボタンランプ表示 *4 ・パトライト社対応機器でのランプ表示 *3	・ALERT1 ランプの橙点灯は次のいずれかの方法で解除してください。 ●OPT1 スイッチを数秒間押し続ける ●設定 Web でセキュリティログを閲覧 ●Aspire の多機能電話による解除 ・ブラウザのブロック表示はブラウザを閉じて解除してください。

*1：アンチウイルス機能による検出時も同様に通知します。
そのため、どちらの機能の検出であるかの確認はセキュリティログを閲覧してください。

*2：HTTPS のブロック表示はブラウザにより異なります。表示例はブラウザが Internet Explorer 11 の場合です。

*3：設定 Web で設定が必要です。(5.8.10 章参照)

*4：Aspire 側の設定が必要です。

- ログのみ設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ログ出力のみ	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

[セキュリティ機能の停止方法]

正常な Web サイトを脅威と誤検出する際は、次の方法により一時的に機能を停止してください。

セキュリティ機能の停止操作は、セキュリティリスクを増大させます。そのため、機能の停止はお客様の責任でご確認の上で実施してください。

停止方法	備考
「Web ガード設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.6 章参照）	

[URL のチェック範囲]

HTTP トラフィックについては、URL のホスト部分、パス部分の両方を参照します。

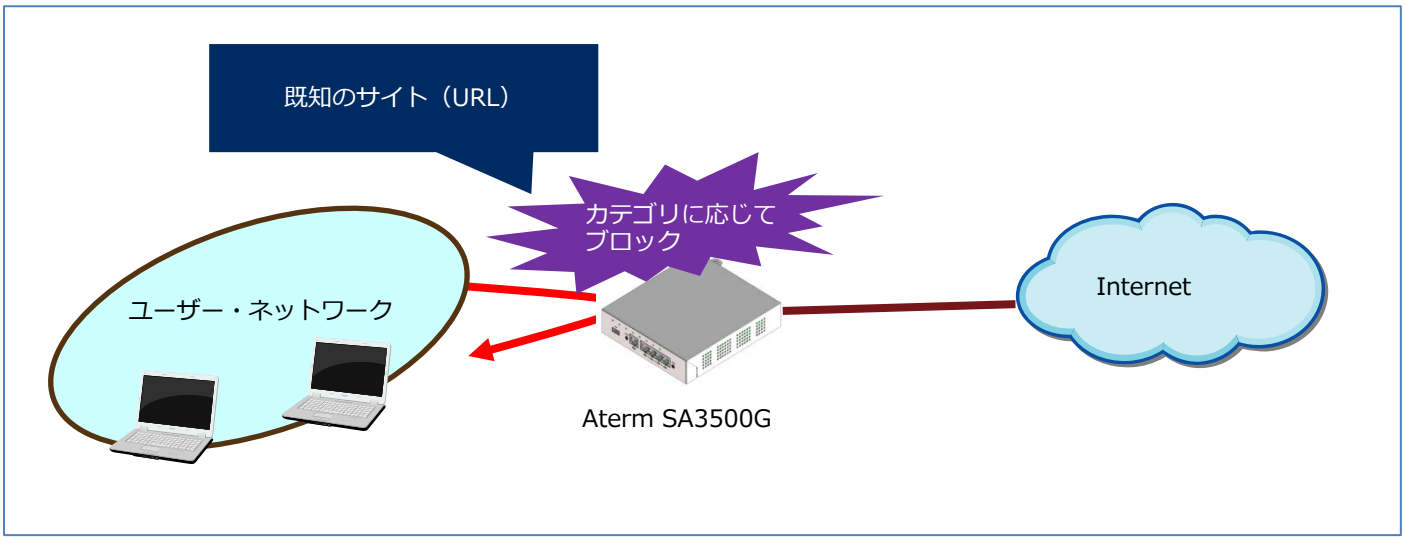
HTTPS トラフィックについては、URL のホスト部分のみ参照します。（パス部分は参照しません。）

この違いから、HTTP トラフィックの場合はホスト部分が同じトラフィックであってもパス部分が違えば検出結果が異なる場合があるのに対し、HTTPS トラフィックの場合はホスト部分が同じトラフィックの場合はパス部分が違っても検出結果は同じです。

3.3.10. **URL フィルタリング（UF）**

あらかじめ用意されている Web サイトのカテゴリを指定することで閲覧の制限を行います。

これにより、有害サイトや業務に無関係なサイトへのアクセスをブロックします。



Web 閲覧において、既知のサイト（URL）へのアクセスを Web サイトのカテゴリに応じて、遮断します。どのカテゴリに対して遮断するかをあらかじめ設定します。

※ファームウェアのバージョンにより本機能を使用する TCP ポートが異なります。

本機能をご使用になるには、以下の TCP ポートが通信できる環境が必須です。

ファームウェアバージョン	使用ポート
Ver3.1.35 以前	TCP ポート =8080
Ver3.2.29～3.2.45	TCP ポート =8081
Ver3.3.20 以降	TCP ポート =443

[検出内容]

危険な Web サイトなど、指定されたカテゴリの Web サイトへのトラフィックを検出し、当該 Web サイトへのアクセスを遮断します。

トラフィックの種類	説明
HTTP トラフィック	URL のホスト名とパス名を使用して、指定されたカテゴリの Web サイトへのトラフィックかどうかを判断します。
HTTPS トラフィック	URL のホスト名を使用して、指定されたカテゴリの Web サイトへのトラフィックかどうかを判断します。

指定されたカテゴリの Web サイトへのトラフィックと判断した場合、次の動作により、当該 Web サイトへのアクセスを遮断します。

トラフィックの種類	説明
HTTP トラフィック（GET）	「特定のカテゴリに属するサイトへのアクセスを検出したため、通信をブロックしました。」の画面を表示します。
HTTP トラフィック（POST）	当該 Web サイトへの通信を遮断します。
HTTPS トラフィック（GET, POST）	当該 Web サイトとの SSL ハンドシェークを失敗させます。

[検出対象のプロトコル]

プロトコル	説明
HTTP	検出対象のポート番号　　：80 検出対象の HTTP メソッド　：GET, POST
HTTPS	検出対象のポート番号　　：443 検出対象の HTTP メソッド　：GET, POST

※HTTP1.0 は、検出できない場合があります。

[個別許可設定]

特定の Web サイトへのアクセスを脅威検出対象外に設定することができます。

[脅威を検出した際の動作・通知の振る舞い]

- ブロック設定の場合

検出の状態	機能の動作	通知方法	通知の解除方法
脅威を検出	該当 Web サイトへのアクセスを遮断	・ブラウザにブロックした旨を表示 (HTTP のブロック表示例)*1  (HTTPS のブロック表示例) *2  ・セキュリティログにログ表示 （設定 Web にて閲覧必要） ・メール通知 *3 ・パトライト社対応機器でのランプ表示 *3	・ブラウザのブロック表示はブラウザを閉じて解除してください。
安全性未確認	該当 Web サイトへのアクセスを遮断	・ブラウザに「安全性を確認できませんでした。」と表示 （安全性未確認の表示例）  	・ブラウザのブロック表示はブラウザを閉じて、しばらくしてから再度アクセスしてください。 それでもアクセスできない場合はネットワーク接続を確認してください。

*1：ブロック表示内に指定されたカテゴリ名が表示されます。表示例は、“ポータル、検索サイト”にて検出された場合のものです。

*2：HTTPS のブロック表示はブラウザにより異なります。表示例はブラウザが Internet Explorer11 の場合のものです。

*3：設定 Web で設定が必要です。(5.8.10 章参照)

- ログのみ設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ログ出力のみ	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

[セキュリティ機能の停止方法]

正常な Web サイトを脅威と誤検出する際は、次の方法により一時的に機能を停止してください。

排除方法	備考
次のいずれかの方法で排除してください。 ● [カテゴリ設定]の詳細カテゴリの設定を「ブロック」から「許可」に変更する（5.8.7 章参照） ● 「URL フィルタリング設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.7 章参照）	・詳細カテゴリの設定を許可に変更した場合、その詳細カテゴリに属するすべてのサイトへのブロックを停止します。

[URL のチェック範囲]

本製品は、HTTP トラフィックについては、URL のホスト部分、パス部分の両方を参照します。

本製品は、HTTPS トラフィックについては、URL のホスト部分のみ参照します。（パス部分は参照しません。）

この違いから、HTTP トラフィックの場合はホスト部分が同じトラフィックであってもパス部分が違えば検出結果が異なる場合があるのに対し、HTTPS トラフィックの場合はホスト部分が同じトラフィックの場合はパス部分が違っても検出結果は同じです。

[カテゴリー覧]

カテゴリは 2 種類あります。

- スタンダードカテゴリ
- 個別カテゴリ

各カテゴリの内訳は、次の表を参照してください。

[メモ]

ファームウェアバージョン 3.1.35 以前の個別カテゴリリストは 74 項目ありました。ファームウェアバージョン 3.2.29 では個別カテゴリリストの冗長を見直して、62 項目に整理する最適化を行いました。

Ver3.1.35 以前のファームウェアから Ver3.2.29 にファームウェア更新を行った場合、カテゴリのブロック設定を引き継ぎます。

スタンダードカテゴリ

No	スタンダードカテゴリ	補足説明
1	全てのカテゴリ	個別カテゴリの No.1～No.62 を一括選択します。
2	アダルトサイトカテゴリ	個別カテゴリの No.1～No.10,No.13 を一括選択します。
3	危険サイトカテゴリ	個別カテゴリの No.32～No.35 を一括選択します。
4	SNS サイトカテゴリ	個別カテゴリの No.12,No.14,No.15,No.57, No.58 を一括選択します。
5	エンターテインメントサイトカテゴリ	個別カテゴリの No.11,No.16～No.20 を一括選択します。

個別カテゴリ

No	個別カテゴリ	補足説明
1	ポルノ Pornography	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
2	アダルトサイト Nudity and Potentially Adult Content	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
3	ギャンブル、宝くじ Gambling and Lottery	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。

4	アルコール、たばこ Alcohol and Tobacco	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
5	ドラッグ Abused Drug	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
6	過激論、人種差別 Ultraism	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
7	中絶 Abortion	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
8	犯罪行為 Criminal Actions	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
9	暴力的なサイト Violence and Bloody	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
10	気持ち悪いサイト Gross	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
11	ゲーム Game	[エンターテインメントサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
12	インスタントメッセージ Instant Messaging	[SNS サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
13	出会い系サイト Dating	[アダルトサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
14	ソーシャルネットワーク Social Network	[SNS サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
15	Web チャットルーム Web Chat Room	[SNS サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
16	ショッピング、オークション Shopping and Auction	[エンターテインメントサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
17	ミュージック Music	[エンターテインメントサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
18	コミック、アニメ Comics and Anime	[エンターテインメントサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
19	エンターテインメント、芸術 Entertainment and Arts	[エンターテインメントサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
20	ストリーミング、VoIP Streaming and VoIP	[エンターテインメントサイトカテゴリ]を[ブロックする]設定時に自動選択されます。
21	P2P Peer to Peer	
22	マルチメディアダウンロード Multimedia Download	
23	オンライン共有、ストレージ Online Sharing and Storage	
24	シェアウェア、フリーウェア Shareware and Freeware	

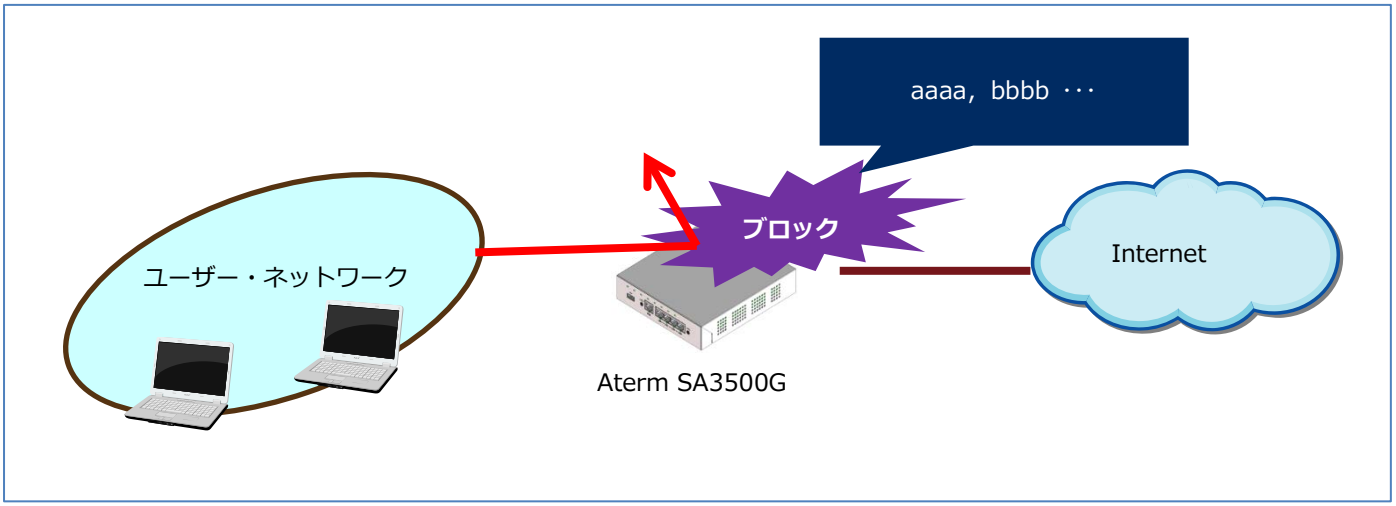
25	Web メール Web Mail	
26	システム更新 System and Antivirus Update	
27	コンテンツ配信サーバ Content Delivery Network	
28	Web サービス API Web Service API	
29	ネットワークサービス Network Service	
30	リモートコントロール Remote Control	
31	プロキシ、アノニマイザー Proxy and Anonymizers	
32	フィッシング詐欺 Phishing and Fraud	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
33	マルウェア Malware	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
34	BlackHat SEO サイト BlackHat SEO Sites	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
35	危険なアプリケーション Malicious APP	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
36	広告 Advertisments and Pop-Ups	
37	ポータル、検索サイト Portals and Search Engines	
38	輸送機関 Transportation	
39	不動産 Real Estate	
40	金融、保険 Finance and Insurance	
41	コンピュータ、IT Computers and Information Technology	
42	ビジネス、サービス Business and Service	
43	参考文献、研究 Reference and Research	
44	教育機関 Education	

45	軍隊、兵器 Military and Weapons	
46	政治、政府 Politics and Government	
47	協会、慈善団体 Associations and Charitable Organizations	
48	旅行 Travel	
49	飲食物 Food and Drink	
50	家、庭 Home and Garden	
51	健康、医学 Health and Medicine	
52	宗教、数秘術 Religion and Numerology	
53	スポーツ Sports	
54	自動車 Automobile and Vehicles	
55	求人情報 Job Search	
56	ニュース、メディア News and Media	
57	フォーラム、ニュースグループ Forums and Newsgroups	[SNS サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
58	ブログと個人サイト Blogs and Personal Sites	[SNS サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
59	不明なサイト Unrated	
60	ドメインパーキング Parking Domains	
61	デッドサイト Dead Sites	
62	プライベート IP アドレス Private IP Address	

3.3.11. URL キーワードフィルタリング（KF）

あらかじめ特定の文字列を登録しておくことで、Web サイト閲覧時において、該当の文字列が含まれている URL の Web サイトへのアクセスをブロックします。アクセスを禁止したい URL がある場合は、本機能を利用してアクセス禁止 URL の設定を行ってください。

任意の文字列（キーワード）は設定 Web で設定します。



[検出内容]

あらかじめ特定の文字列を登録しておくことで、Web サイト閲覧時において、該当の文字列が含まれている URL の Web サイトへのアクセスをブロックします。

プロトコル	説明	例
HTTP	・キーワードとして、URL 部の「ホスト名」と「パス名」にキーワードが含まれているか確認します	・キーワードに"example.com"を設定 → http://www.example.com がブロックされます。 ・キーワードに"violence"を設定 → http://www.example.com/violence がブロックされます。
HTTPS	・キーワードとして、URL 部の「ホスト名」にキーワードが含まれているか確認します ・「パス名」にキーワードが含まれていても判定対象外です	・キーワードに"example.com"を設定 → https://www.example.com がブロックされます。 ・キーワードに"violence"を設定 → https://www.example.com/violence はブロックされません。

該当の文字列が含まれている URL の Web サイトへのトラフィックと判断した場合、次の動作により、当該 Web サイトへのアクセスを遮断します。

トラフィックの種類	説明
HTTP トラフィック（GET）	「URL に指定されたキーワードが含まれるサイトへのアクセスを検出したため、通信をブロックしました。」の画面を表示します。
HTTP トラフィック（POST）	当該 Web サイトへの通信を遮断します。
HTTPS トラフィック（GET, POST）	当該 Web サイトとの SSL ハンドシェークを失敗させます。

[検出対象のプロトコル]

プロトコル	説明
HTTP	検出対象のポート番号　　：80 検出対象の HTTP メソッド　：GET, POST
HTTPS	検出対象のポート番号　　：443 検出対象の HTTP メソッド　：GET, POST

※HTTP1.0 は、検出できない場合があります。

<キーワードに該当の場合>

本製品は、任意のキーワードを含む Web サイトへのアクセスを検出したことを示すメッセージを端末に送信します。[10]

※HTTPS の場合は、SSL ハンドシェークを失敗させることで、該当する Web サイトへのトラフィックを遮断します。

[設定可能なキーワード]

使用可能文字　　：アスキーコードで 0x21-0x7e、マルチバイト文字（ただし、"'`$¥<> を除く）

キーワードの最大サイズ　：127 文字（127 バイト）

キーワードの登録可能数　：100 件

※複数のキーワードの組み合わせは指定できません。

※マルチバイト文字を使用した場合、設定可能な文字数は少なくなります。

[個別許可設定]

「キーワード設定」画面で「許可」に設定します。この設定で許可された通信は他のセキュリティ・スキャン機能(ファイアウォール機能を除く)の脅威検出対象外となります。

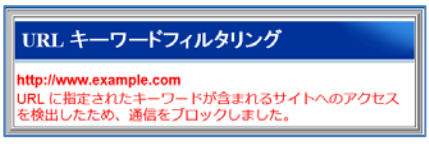
以下の例のように同一キーワード“nec”を含む複数の設定を行った場合は、「許可」の設定が「ブロック」よりも優先されます。当設定の場合、”nec”を含むすべての URL が許可されます。

“necplatforms.co.jp” を「ブロック」に設定

“nec”　　を「許可」に設定

[脅威を検出した際の動作・通知などの振る舞い]

- ブロック設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
URL に任意のキーワードを含む Web サイトへのアクセスを遮断	・ブラウザにブロックした旨を表示 （HTTP のブロック表示例）  (HTTPS のブロック表示例) *1  	・ブラウザのブロック表示はブラウザを閉じて解除してください。

[10] サイトによっては、メッセージが表示されない場合があります。

	・セキュリティログにログ表示 （設定 Web にて閲覧必要） ・メール通知 *2 ・パトライト社対応機器でのランプ表示 *2	

*1：HTTPS のブロック表示はブラウザにより異なります。表示例はブラウザが Internet Explorer 11 の場合です。

*2：設定 Web で設定が必要です。(5.8.10 章参照)

- ログのみ設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ログ出力のみ	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

- 許可設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
この設定で許可された通信は他のセキュリティ・スキャン機能の脅威検出対象外となります	–	–

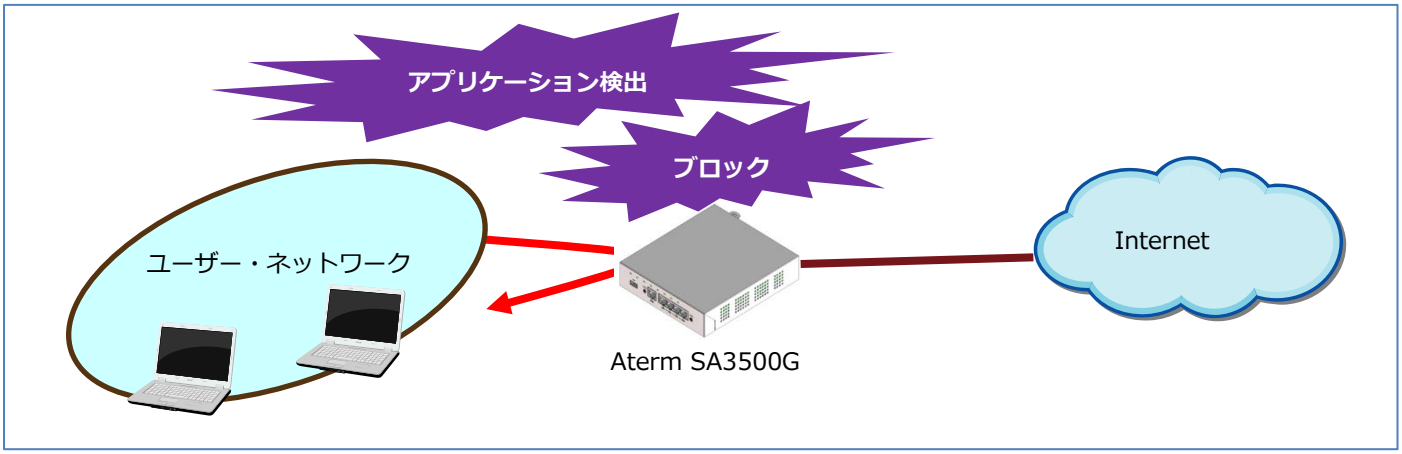
[意図しない検出の停止方法]

排除方法	備考
次のいずれかの方法で停止してください。 ● 「キーワード設定」で設定されたキーワードを「削除」ボタンにより削除する（5.8.8 章参照） ● 「キーワードフィルタリング設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.8 章参照）	

3.3.12. アプリケーションガード（APG）

ファイル交換ソフトや動画共有アプリ、メッセンジャーアプリなど、不特定多数の個人が情報交換可能なアプリケーションの利用を制限します。これにより、セキュリティ対策を行っていない相手や悪意のある相手からのウイルス感染と情報漏えいを防止します。

利用を制限するアプリケーション、トラフィックは設定 Web で設定します。



[検出対象のアプリケーション、プロトコル]

検出対象のアプリケーション、プロトコルを定期的に更新します。

最新の情報は、設定 Web で確認してください。

設定 Web の確認方法は、5.8.9 章を参照してください。

[シグネチャ更新により追加されるアプリケーションの動作設定]

ファームウェア Ver 3.5.12 までは、シグネチャ更新により追加されるアプリケーションの検出時の動作の初期値は「許可」でした。

ファームウェア Ver 3.6.9 以降は、シグネチャ更新により追加されるアプリケーションの検出時の動作をカテゴリ毎に「ブロック」・「ログのみ」・「許可」に設定することができます。

たとえば、新しいゲームアプリがシグネチャ更新により追加された場合、該当ゲームアプリを「ブロック」の設定にするには、設定 Web から該当ゲームアプリの設定を「許可」から「ブロック」に変更する必要がありました。

ファームウェア Ver 3.6.9 以降では、「ゲーム」カテゴリに追加されるアプリケーションの動作をあらかじめ「ブロック」に設定しておくことで、「ゲーム」カテゴリに追加されるアプリを自動的に「ブロック」に設定できます。

[脅威を検出した際の動作・通知などの振る舞い]

- ブロック設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
特定のアプリケーション、プロトコルの通信を遮断	・セキュリティログにログ表示（設定 Web にて閲覧必要） ・メール通知 *1 ・パトライト社対応機器でのランプ表示 *1	–

*1：設定 Web で設定が必要です。(5.8.10 章参照)

- ログのみ設定の場合

検出時の動作	検出時の通知方法	検出状態の解除方法
ログ出力のみ	・セキュリティログにログ表示 （設定 Web にて閲覧が必要）	–

[意図しない検出の停止方法]

停止方法	備考
次のいずれかの方法で停止してください。 ● [アプリケーションリスト]の該当アプリケーションの設定を「ブロック」から「許可」に変更する（5.8.9 章参照） ● 「アプリケーションガード設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.9 章参照）	

3.3.13. **セキュリティログ**

本製品のセキュリティ・スキャン機能の検出状況などをログメッセージで確認できます。

これらのログメッセージをパソコンなどに保存できます。

[ログメッセージの内容]

- 検出日時
- 検出機能名（FW、AV、IPS、WG、UF、KF、APG）
- 検出内容
- 検出対象の端末の IP アドレス

[ログの保存]

- ログメッセージの保存
  - 定期的に FlashROM にログファイルを保存します。
  - ログファイル保存領域の最大サイズは 500M バイト（目安として 100 万件）です。
    1M バイトごとにログファイルを生成して保存します。
    ログメッセージは、1 件あたり最大 1,000 バイトです。
    ログ保存領域を超えた場合は、古いログを削除して、新しいログを保存します。
  - ログファイルを保存中は POWER ランプが橙点滅しますので、電源を OFF にしないでください。
- 上記の他、設定 Web の操作による装置再起動のタイミングでログファイルを保存します。

※停電や電源断などの場合は、FlashROM に保存されていないログメッセージが失われます。

[設定 Web の操作]

- 設定 Web で最新から 1,000 件分のログメッセージを確認できます。
- 「クリア」ボタン押下で、セキュリティログを削除します。FlashROM に保存しているログファイルも削除します。
- ブロックした通信を脅威検出対象外（個別許可）に設定できます。個別許可の設定ができるセキュリティ機能は次のとおりです。

セキュリティ・スキャン機能	個別許可の設定可能件数	備考
アンチウイルス（AV）	10 件	
不正侵入防止（IPS）	100 件	
Web ガード（WG）	10 件	
URL フィルタリング（UF）	100 件	
URL キーワードフィルタリング(KF)	100 件	URL キーワードフィルタリング(KF)の「キーワード設定」画面で「許可」に設定します。この設定で許可された通信は他のセキュリティ・スキャン機能(ファイアウォール機能を除く)の脅威検出対象外となります。

[メモ]

- 初期化を行うと、FlashROM に保存しているログファイルを削除します。

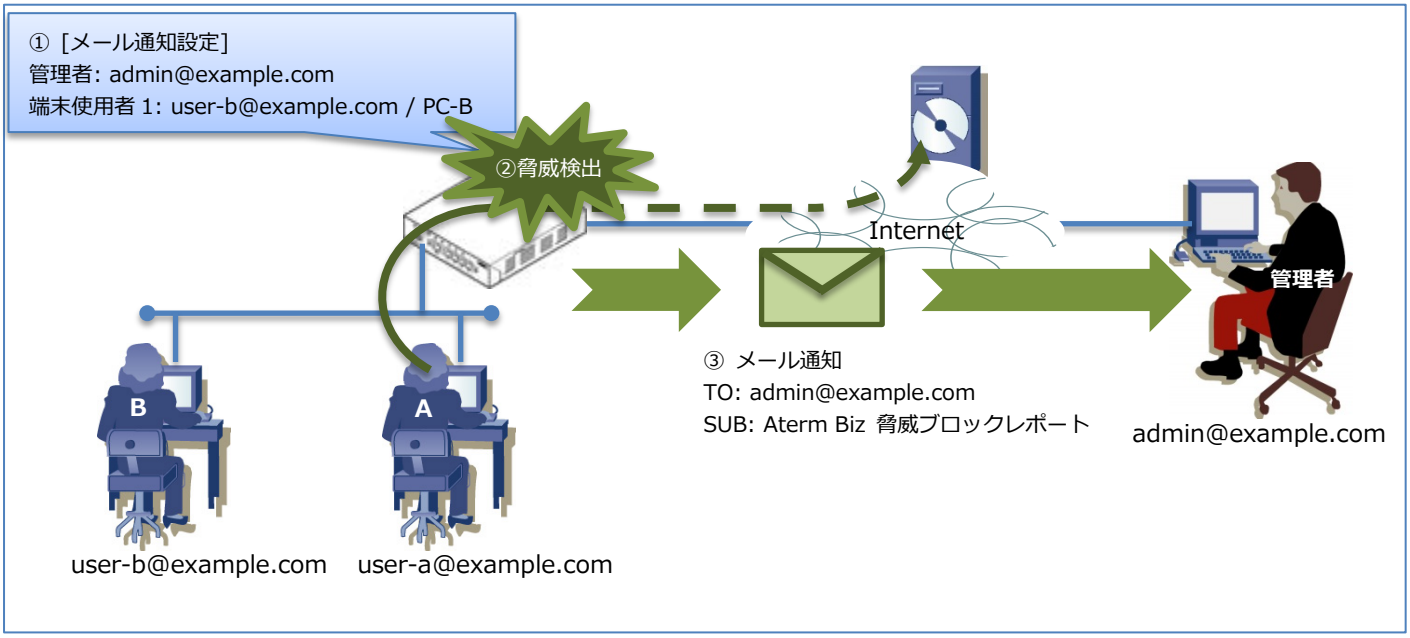
3.3.14. **メール通知**

脅威検出などのイベント発生時にメールでお知らせする機能です。

また、月別統計を月次レポートとして、管理者宛てにメール送付することもできます。

ファームウェアバージョン 3.2.29 よりメール通知の通知メッセージをカスタマイズできるように対応いたしました。

設定方法は 5.8.11 章を参照してください。



[上図の説明]

① メール通知で「管理者」と「端末 B」の情報を登録します。

② 本製品が、ユーザーA のトラフィックで『脅威検出』しました。

③ メール通知で管理者にのみ「Aterm Biz 脅威ブロックレポート」メールを送信します。

※ユーザーB のトラフィックで脅威を検出した場合は、管理者とユーザーB 宛てにメールを送信します。

[通知するタイミング]

- アンチウイルス（AV）検出時
- 不正侵入防止（IPS）検出時
- Web ガード（WG）脅威検出時
- URL フィルタリング（UF）脅威検出時
- URL キーワードフィルタリング（KF）脅威検出時
- アプリケーションガード（APG）検出時
- ファームウェアアップデート検出時
- ライセンス期限満了間近になったとき（ライセンス期限満了の 60 日前）
- ライセンス期限が満了したとき
- 月次レポートの送信時刻がきたとき

※脅威検出された通信が途中でリセットされるなどの理由によりやり直された場合、同じ通信内容で複数回の通知が行われる場合があります。

[通知先]

通知先は 2 種類あります。

通知先	設定内容	説明	登録可能数
管理者	管理者のメールアドレス	「通知する」に設定しているすべてのイベントが発生した場合、登録しているメールアドレス宛てに通知します。	3
端末使用者	端末情報（PC などの端末の MAC アドレス）とメールアドレスの組み合わせ	登録済みの端末からのパケット、または、端末宛てのパケットで脅威を検出した場合、当該端末に登録しているメールアドレス宛てに通知します。 （このイベントは、管理者にも通知します。）	50

[イベント詳細]

通知内容	イベント	通知タイミング	通知先	
			管理者	端末使用者
脅威検出	AV, WG, UF, KF, APG でガードした	イベント発生時 （装置再起動時の ALERT1 ランプ点灯のタイミングは通知対象外）	○	○
	IPS でガードした	イベント発生時	○	×
ライセンス情報	ライセンス期限満了間近（60 日前）	(1) 装置動作中にライセンス期限満了間近となったとき (2) 装置起動時、ライセンス期限満了間近のとき (3) 上記(1)または(2)を実行した後、ライセンス期限が満了するまで 24 時間ごと	○	×
	ライセンス期限満了	・装置動作中にライセンス期限満了となったとき ・装置起動時、ライセンス期限満了のとき	○	×
ファームウェアアップデート	更新可能なファームウェアを検出	イベント発生時	○	×
月次レポート	以下の内容を通知します。 ・前月分の統計情報 （全体の統計情報。月次レポートの送信時点から見て前月分のみを含めます。） ・ファームウェアアップデートの有無 ・ライセンス有効期限 ・URL フィルタリングとアプリケーションガードの通信情報	毎月 1 日の X 時 Y 分 （X は 0~23、Y は 0~59）	○	×

[メール送信失敗時の動作]

- メール送信に失敗した場合、最大 3 回（10 分後、30 分後、70 分後）リトライし、処理を終了します。
- リトライ対象のメール件数は、最大 10 件です。
- テストメール送信の場合は、メール送信に失敗した場合にリトライしません。

[メール通知内容]

通知内容	メール件名	メール内容	補足
脅威検出 (AV)	Aterm Biz 脅威ブロックレポート	以下の脅威をブロックしました。 タイプ:AV ウイルス名:*virus* ファイル:*filename* Protocol:*protocol* 時間: *yyyy/mm/dd hh:mm:ss* 端末:*IP* アドレス/*MAC*/コメント X-Forwarded-For: *IP* アドレス Date: *date* Subject: *subject* From: *from* To: *to*	・端末：LAN 側端末 ・Protocol ：AV 機能で脅威検出したプロトコル ・コメント：デバイス管理画面設定項目のコメント
脅威検出 (WG, KF)	Aterm Biz 脅威ブロックレポート	以下の脅威をブロックしました。 タイプ:*Function* URL:*url* 時間: *yyyy/mm/dd hh:mm:ss* 端末:*IP* アドレス/*MAC*/コメント X-Forwarded-For: *IP* アドレス	・タイプ：WG/KF ・端末：LAN 側端末 ・コメント：デバイス管理画面設定項目のコメント
脅威検出 (UF)	Aterm Biz 脅威ブロックレポート	以下の脅威をブロックしました。 タイプ:UF URL:*url* カテゴリ:*category* 時間: *yyyy/mm/dd hh:mm:ss* 端末:*IP* アドレス/*MAC*/コメント X-Forwarded-For: *IP* アドレス	・端末：LAN 側端末 ・コメント：デバイス管理画面設定項目のコメント
脅威検出 (APG)	Aterm Biz 脅威ブロックレポート	以下の脅威をブロックしました。 タイプ:APG アプリケーション:*application* 時間: *yyyy/mm/dd hh:mm:ss* 端末:*IP* アドレス/*MAC*/コメント X-Forwarded-For: *IP* アドレス	・端末：LAN 側端末 ・コメント：デバイス管理画面設定項目のコメント
脅威検出 (IPS)	Aterm Biz 脅威ブロックレポート	以下の脅威をブロックしました。 タイプ:IPS 攻撃元:*IP* アドレス 内容:*msg* 時間: *yyyy/mm/dd hh:mm:ss* 端末:*IP* アドレス/*MAC*/コメント X-Forwarded-For: *IP* アドレス	・コメント：デバイス管理画面設定項目のコメント
ライセンス情報 (有効期限間近)	Aterm Biz 情報通知	ライセンスが間もなく満了します。 デバイス ID: *xxxx...* 満了時刻: *yyyy/mm/dd hh:mm:ss*	

ライセンス情報 (有効期限満了)	Aterm Biz 情報通知	ライセンスの有効期限が満了しました。 デバイス ID: *xxxx...*	
ファームウェア アップデート	Aterm Biz 情報通知	新しいファームウェアが公開されました。 デバイス ID: *xxxx...* Ver:*x.x.x*	
月次レポート	Aterm Biz 月次レポート	*yyyy/mm* レポート [装置情報] デバイス ID: *xxxx*… [統計情報] AV:*block count/scan count* IPS:*block count/scan count* WG:*block count/scan count* UF:*block count/scan count* KF:*block count/scan count* APG:*block count/scan count* [通信情報] [ファームウェア更新情報] あり(or なし) [ライセンス有効期限] *yyyy/mm/dd hh:mm:ss*	通信情報は URL フィルタリングの上位 5 つのカテゴリの検出数とアプリケーションガードの上位 5 つのアプリケーションの検出数です。
テストメール	Aterm Biz テストメール	テストメールを送信しました。 デバイス ID: *xxxx...*	テストメール送信時

[**メール通知内容パラメータについて**]

パラメータ	**内容**	**通知条件**
X-Forwarded-For	HTTP ヘッダーに含まれている X-Forwarded-For ヘッダーまたは X-Tinyproxy ヘッダーの値	プロトコルが HTTP かつ HTTP ヘッダーに X-Forwarded-For ヘッダーまたは X-Tinyproxy ヘッダーが含まれている場合。 X-Forwarded-For ヘッダーと X-Tinyproxy ヘッダーが同時に含まれている場合は、先に記載されているヘッダーの値を記載します。
Date	脅威検出したメールの Date ヘッダーの値	プロトコルが smtp/pop3/imap の場合に記載します。値が空の場合でも空のまま記載します。
Subject	脅威検出したメールの表題	プロトコルが smtp/pop3/imap の場合に記載します。値が空の場合でも空のまま記載します。
From	送信元のメールアドレス	プロトコルが smtp/pop3/imap の場合に記載します。値が空の場合でも空のまま記載します。
To	送信先のメールアドレス	プロトコルが smtp/pop3/imap の場合に記載します。値が空の場合でも空のまま記載します。To が undisclosed-recipients であっても、そのまま記載します。

［メール通知内容（表示例）］

実際のメールの表示例を示します。

- **脅威検出メールの表示例**

件名	**Aterm Biz 脅威ブロックレポート**
本文	以下の脅威をブロックしました。 タイプ:AV ウイルス名:EICAR-Test-File ファイル:eicar.com Protocol:HTTP 時間:2020/01/17 12:00:00 端末:192.168.110.2/XX:XX:XX:XX:XX:XX/PC1 X-Forwarded-For:192.168.10.240

● **月次レポートの表示例**

件名	Aterm Biz 月次レポート
本文	2020/01 レポート [装置情報] xxxx-xxxx-xxxx-xxxx [統計情報] AV:0/100 IPS:0/100 WG:0/100 UF:50/100 KF:20/100 APG:10/100 [通信情報] <UF カテゴリ(上位 5 カテゴリ)> No カテゴリ 検出数 過去平均 ブロック数 -- ---------- ---------- ---------- ---------- 1 ニュース、メディア 1000 800 0 2 ブログ、個人サイト 900 300 0 3 スポーツ 400 500 400 4 コンピューター、IT 300 600 0 5 ギャンブル、宝くじ 200 20 0 <アプリケーション(上位 5 アプリケーション)> No アプリケーション 検出数 過去平均 ブロック数 -- ---------- ---------- ---------- ---------- 1 Google Drive (FileTransfer) 1000 800 0 2 Outlook.com (DataFlow) 900 300 900 3 Skype for Business (Login/Me 400 500 0 4 ○○アプリ 300 600 300 5 ○○乗換案内 200 20 0 [ファームウェア更新情報] なし [ライセンス有効期限] 2026/08/01 12:00:00

3.3.15. **パトライト連携**

本機能は脅威検出時にパトライトを点灯する機能です。

脅威検出時に本製品と通信可能なパトライトを 5 分間点灯(※)させることができます。

パトライトは別売（当社オプションではありません）です。

※赤が点灯します。

5 色表示に対応したパトライト製品の場合でも点灯するのは赤色です。

[当社動作確認済みパトライト製品]

- NHS-FV1/NHP-FV1/NHL-FV1
- NHS-FB1/NHP-FB1/NHL-FB1
- PHN-3FBE1

[設定方法]

パトライトの IP アドレス、ポート番号、通信プロトコル(TCP/UDP)を本製品に設定してください。

パトライト連携設定の詳細は、5.9.4 章を参照してください。

3.3.16. **Aspire 連携**

Aspire 連携機能はオフィスコミュニケーションゲートウェイ「UNIVERGE Aspire」との連携により、お手元の電話機で本製品の以下を行うことができます。これらの連携機能は本製品のファームウェアバージョン 3.4.21 以降と Aspire UX のファームウェアバージョン 8.00.00 以降、もしくは Aspire WX の初期ファームウェアバージョン以降の組み合わせで動作します。電話機の機能ボタンに割り当てられた機能については、「UNIVERGE Aspire」のマニュアルを参照してください。

[Aspire 連携にてできること]

- 電話機への以下の情報通知
  - ・脅威検出状態
  - ・更新ファームウェアの有無
  - ・ライセンス有効期限
- 本製品の設定 Web 画面と Aspire の Web プログラミング画面との相互リンク
- 周辺機器設定による本製品の設定 Web 画面へのデバイスマップ表示
- デバイスマップ上での IP 多機能電話機情報の参照

Aspire 主装置の設定をする前に、本製品を Aspire と接続するために以下の準備が必要です。

①本製品に固定 IP アドレスを設定します

※Aspire 連携をする際は SA3500G に固定 IP アドレスが必要です

②設定作業に使用する PC の IP アドレスを Aspire 主装置の IP アドレスと同じネットワークの IP アドレスに設定します。

[脅威検出状態]

電話機の機能ボタンランプ点灯と電話機の LCD で表示します。

消灯：脅威検出なし

赤点灯：脅威検出あり

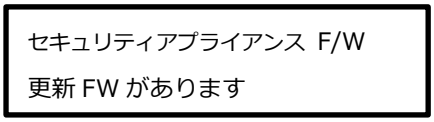
※点灯時にボタン押下でランプが消灯します。

脅威検出画面（電話機の画面イメージ）

[更新ファームウェアの有無]

電話機の更新ファームウェア確認の機能ボタンランプ押下したとき、LCD に更新ファームウェアの有無を表示します。

更新ファームウェアの表示画面（電話機の画面イメージ）



[ライセンス有効期限]

電話機のライセンス状態確認の機能ボタンランプ押下したとき、LCD にライセンス有効期限を表示します。

ライセンスの有効期限の表示画面（電話機の画面イメージ）

セキュリティアプライアンス License
License 有効期限[YYYY/MM/DD]

[Aspire の Web プログラミングと設定 Web の連携について]

本製品の設定 Web から Aspire の「Web プログラミング」の「ログイン画面」へリンクする「Aspire」アイコンを設けました。（ファームウェア Ver3.3.20~3.5.12）

「Web プログラミング」の「ログイン画面」へリンクするアイコン名を「Aspire」に変更しました。（ファームウェア 3.6.9 以降）

当アイコンは、本製品の[周辺機器設定]画面で Aspire の設定を行うと[TOP]画面に表示されます。

設定 Web の連携機能の設定方法は、5.9.4 章を参照してください。

3.3.17. **統計情報**

本製品のセキュリティ・スキャン機能の検出状況を統計情報で確認できます。

[統計情報の内容]

- FW/AV/IPS/WG/UF/KF/APG の各機能が遮断したパケット数、スキャンした数値です。
- AV/IPS/WG/UF/KF/APG の各機能の脅威検出時の動作設定をログのみにした場合、スキャンした数値がカウントされます。
- 日・週・月の時間単位で統計情報を表示します。
- 本製品が管理する端末ごともしくは全体のセキュリティ・スキャン機能の検出状況を表示できます。

セキュリティ・スキャン機能	統計情報	説明
ファイアウォール（FW）	ブロックしたパケット数	FW 機能で遮断したパケットの数
アンチウイルス（AV）	スキャンしたファイル数	AV 機能でスキャンしたファイルの数
	ブロックしたファイル数	AV 機能で内容を書き換えたファイルの数
不正侵入防止（IPS）	スキャンしたフロー数	IPS 機能でスキャンしたトラフィックフローの数
	ブロックしたフロー数	IPS 機能で遮断したトラフィックフローの数
Web ガード（WG）	スキャンした URL 数	WG 機能でスキャンした URL の数
	ブロックした URL 数	WG 機能で遮断した URL の数
URL フィルタリング（UF）	スキャンした URL 数	UF 機能でスキャンした URL の数
	ブロックした URL 数	UF 機能で遮断した URL の数
	カテゴリごとの検出した数	月ごとに UF 機能でスキャンした URL のカテゴリ単位の検出数
URL キーワードフィルタリング（KF）	スキャンした URL 数	KF 機能でスキャンした URL の数
	ブロックした URL 数	KF 機能で遮断した URL の数
アプリケーションガード（APG）	スキャンしたフロー数	APG 機能でスキャンしたアプリケーションのトラフィックフローの数
	ブロックしたフロー数	APG 機能で遮断したアプリケーションのトラフィックフローの数
	検出したアプリケーション数	月ごとに APG 機能でスキャンしたアプリケーションのトラフィックフロー数

[統計情報の保存]

- 定期的に FlashROM に保存します。
- 約 7 年分の統計情報を保存できます。それ以降は、古い日付の統計情報を削除して、新しい統計情報を保存します。
- 設定 Web の操作による装置再起動のタイミングで、それまでの統計情報を FlashROM に保存します。

※停電や電源断などの場合は、FlashROM に保存されていない統計情報が失われます。

[設定 Web の操作]

- 設定 Web で日・週・月の時間単位で統計情報を表示できます。
- 設定 Web で時間ごとの詳細とグラフを確認できます。
- 設定 Web の操作で、パソコンなどに統計情報を保存できます。
- 「クリア」ボタン押下で、統計情報を削除します。FlashROM に保存している統計情報も削除します。

[メモ]

- 初期化を行うと、FlashROM に保存している統計情報を削除します。
- 本製品の NTP クライアント機能とセキュリティ・スキャン機能は非同期に動作します。本製品の起動直後から本製品の装置時刻を設定するまで間の統計情報は、実際の年月日が反映されませんのでご注意ください。

本製品の装置時刻の仕様は、3.4.5 章を参照してください。

3.3.18. **脅威検出**

ウイルスなどの脅威を検出した場合、ALERT1 ランプが橙点灯し、脅威を検出したことを知らせます。

脅威を検出したことをお知らせする機能であり、本状態でもセキュリティ・スキャン機能は動作し続けます。

[対象機能]

- アンチウイルス機能でのウイルス検出時
- Web ガード機能でのトラフィック遮断時

[脅威検出時の動作仕様]

ALERT1 ランプの橙点滅/橙点灯でお知らせします。

ALERT1 ランプ状態	仕様
橙点滅	脅威検出から 60 秒間橙点滅します。
橙点灯	脅威検出から 60 秒後、橙点灯に移行します。脅威検出の解除まで、橙点灯します。
消灯	脅威未検出および脅威検出解除時に消灯します。

[脅威検出状態の解除]

下記操作により、脅威検出状態を解除できます。

- OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を ALERT1 ランプが消灯するまで数秒間押し続ける
- 設定 Web でセキュリティログを閲覧
- Aspire 連携機能をお使いの場合は、電話機の機能ボタンを押下する

[メモ]

「脅威検出状態」のときに本製品を再起動すると、「脅威検出状態」は解除されます。

3.3.19. **デバイス管理**

[本機能でできること]

- ご使用の LAN 端末情報を自動検出し、デバイス管理画面に表示します。（最大 100 台）
  表示する情報は、検出された端末の MAC アドレス、IP アドレス、OS などの関連情報、有線/無線の区分です。有線は本製品の LAN ポートに接続している端末で、無線は本製品に無線 LAN で帰属している端末を指します。
- 端末ごとに、端末識別のための任意のコメントや端末使用者のメールアドレス、メール通知の要否、端末ごとの統計情報収集の要否を設定できます。その際、設定された端末の情報は装置の FlashROM に保存されます。
- 任意の端末を登録することもできます。

ファームウェアバージョン 3.4.21 でデバイス管理の管理方式が選択できるようになりました。Ver3.3.26 以前のファームウェアではデバイス検出、管理方式は MAC アドレスで管理していました。ファームウェアバージョン 3.4.21 より IP アドレスを使用する管理方式をご利用できます。

IP アドレスを使用にすることにより、次の内容に対応できます。

- ネットワークを固定 IP アドレス運用している場合など、IP アドレス単位でデバイスを管理できます。
- IX シリーズのルータ、WA シリーズのルータを検出すると、デバイスマップ機能において専用のマークが表示されます。

※Aspire は管理方式にかかわらず専用のマークを表示します。
デバイスの管理方式は本製品の運用開始時に選択するようにしてください。設定方法は 5.9.3 章を参照してください。

[端末情報の更新タイミング]

本製品は、有線 LAN ポートもしくは無線 LAN に接続された端末の WAN 側との通信を検出し、デバイス管理画面に表示します。
設定Web でデバイス管理画面を開いたときに、最新の端末情報に更新されます。

[端末ごとの統計情報収集]

端末ごとの統計情報収集対象に設定すると次の情報が利用でき、潜在的な脅威リスクを把握しやすくなります。（最大 50 台）

- 端末ごとの統計情報表示
- ブロック数が多い順に並べたグラフ表示

[ご注意]

- デバイス管理の方式を MAC アドレス単位(初期値)から IP アドレス単位に変更した場合、保持している統計情報をクリアします。また、このとき、装置を再起動します。
- 本製品が管理する IP アドレスは IPv4 アドレスです。IP アドレス単位で運用時に、IPv6 トラフィックをカウントしません。

3.3.20. **デバイスマップ**

本製品の設定 Web 上で、有線 LAN ポートおよび無線 LAN に接続している端末を視覚的に確認できます。
本製品に接続されている LAN に接続されたデバイスをチェックできます。本製品を中心としたネットワーク構成を視覚的に確認したい場合にお使いください。設定 Web で物理 LAN ポートに任意の名前を付けて、よりネットワーク構成を確認しやすくすることができます。デバイスマップの設定方法は 5.9.2 章を参照してください。

[本機能でできること]

- MAC アドレスもしくは IP アドレスをキーに LAN 側に接続された端末の接続位置を見つけることができます。
- 物理 LAN ポートごとに固有の名前を付けて管理することができます。
- 設定 Web から該当の端末を選択し、選択した端末の詳細情報を確認することができます。
- 有線 LAN ポートもしくは無線 LAN に接続された端末との通信を検出し、視覚的に表示することができます。

[端末情報の更新タイミング]

有線 LAN ポートもしくは無線 LAN から WAN ポートへの通信を行った端末を検出してデバイスマップに表示します。
LAN-LAN ポート間で行われる通信は検出しません。端末の検出は毎時 30 分に行います。
デバイスマップの情報更新間隔の初期値は 1 時間ですが、設定 Web で変更することができます。

[デバイスの管理方式を IP アドレス単位で行うときの階層表示について]

本製品の LAN 側に下表に示す対象機器が接続されている場合は、デバイスマップ上に対象機器のアイコンを階層表示します。階層表示は、例えば IX2215 に IX2105 と WA2610-AP が接続されているなどのように、対象機器を多段で視覚化する表示方法です。ただし、周辺機器が NAT 機能を有効にしている場合、前述の例では IX2215 で WAN 側インタフェースに NAPT 設定を行った場合は対象機器のアイコンは表示されません。
また、本製品をルータモードでご利用の場合は、IPv4 静的ルーティング設定で本製品の LAN 側に接続されている周辺機器のルーティング設定を行っていただく必要があります。

本製品が階層表示を行う対象機器は以下のとおりです。

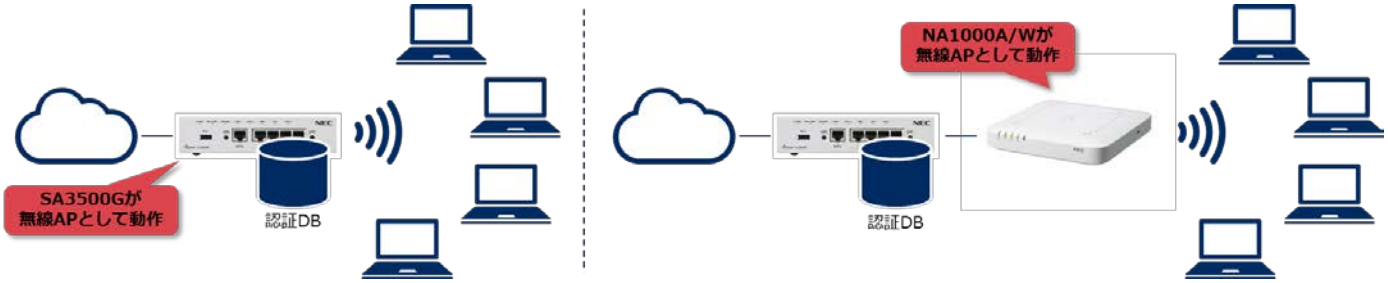
機種名	品名コード	備考
UNIVERGE IX2105	BE108821	https://jpn.nec.com/univerge/ix/
UNIVERGE IX2106	BE117769	
UNIVERGE IX2207	BE112155	
UNIVERGE IX2215	BE110711	
UNIVERGE WA2610-AP	BT0176-02610	https://jpn.nec.com/univerge/wa/
UNIVERGE WA2611-AP	BT0176-02611	
UNIVERGE WA2612-AP	BT0176-02612	

[デバイスの管理方式を IP アドレス単位で行うときの WAN 側の表示について]

本製品のデフォルトゲートウェイとして設置されている機器が上記表に該当する機器で、該当機器と本製品の SNMP コミュニティ名が同じであるとき、WAN 側のルータとして対象機器を示すアイコンがデバイスマップ上に表示されます。

3.3.21. **簡易 RADIUS 機能**

本機能を有効にすることで、社内ネットワークへ接続する LAN 端末の認証を行うことができます。LAN 端末のアカウント情報を本製品の認証 DB に登録しておくことで、許可した LAN 端末のみ社内ネットワークへの接続が可能となります。
MAC アドレスフィルタリング機能とあわせてお使いいただくことで、社内ネットワークへの不正接続を強固に防止することができます。簡易 RADIUS 機能の設定方法は 5.8.12 章を参照してください。



[本機能でできること]

- 本製品は RADIUS プロトコルの機能のうち、認証機能のみサポートしております。
- 認証方式は EAP-PEAP、EAP-TLS の 2 種類です。
- 無線 LAN 端末の認証方式として IEEE802.1X 認証をサポートしております。
- ルート証明書の生成は本製品が自動で行います。ユーザー登録後のクライアント証明書発行が簡単にできます。
- 本製品を RADIUS サーバとして動作させる場合、外部の RADIUS クライアントを最大 20 台登録できます。
- 本製品に登録可能なユーザー数は最大 200 ユーザーです。1 つのユーザーアカウントに最大 2 つまでクライアント証明書を発行できます。

- 本製品の無線 LAN 機能を有効にして、暗号化モードを[802.1x(EAP)]にしたとき、本製品が RADIUS クライアントとして動作します。
- 本製品内部の RADIUS クライアントを使用する場合、本製品に無線 LAN で接続された端末のみ認証対象となります。有線で LAN ポート接続された端末は、認証対象外です。
- 本製品が RADIUS クライアントとして動作するとき、本製品の RADIUS サーバを使用するか、外部の RADIUS サーバを使用するかを選択できます。
- 右側の構成例は、当社製品の NA1000A/W（別売）を無線 LAN アクセスポイントとして構成しています。本構成では NA1000A/W が RADIUS クライアント、本製品が RADIUS サーバとして動作します。
  NA1000A/W の仕様については以下の URL を参照してください。
  https://www.necplatforms.co.jp/product/na/

3.3.22. **パケット書き換え**

本製品がセキュリティ・スキャン機能使用時に行うパケット書き換え動作の対象から、指定した URL を除外することができます。

本製品はセキュリティ・スキャン機能が有効な状態で LAN-WAN 間に転送される HTTP パケットの特定のヘッダーの内容を書き換えます。この書き換えにより、アクセス先のウェブサイトによってはウェブサイト側が応答しない場合があります。この場合、アクセス先のウェブサイトの URL を除外 URL リストに追加してください。除外 URL リストに追加した URL へのアクセス時には、HTTP パケットの特定のヘッダーの内容の書き換えを行いません。これにより、応答しなかったウェブサイトにアクセスできるようになる場合があります。パケット書き換えの設定方法は 5.8.11.2 章を参照してください。

[除外 URL リスト]

パケット書き換え動作の対象から除外する URL を登録します。

- 先頭文字（サブドメイン部分）に「*」を使用できます。
- 先頭文字（サブドメイン部分）に「*」を使用している場合は、URL のチェックはサブドメイン部分をワイルドカードとして判断します。
- 先頭文字（サブドメイン部分）に「*」を使用していない場合は、URL のチェックは完全一致で判断します。
- パス部分の入力はできません。また、マルチバイト文字は使用できません。
- 入力できる URL の最大文字数は 127 文字です。
- 最大 100 件の URL を登録することが出来ます。

[ご注意]

- 機能を使用することで改善する事象は、特定のウェブサイトの仕様によるものです。
- 機能を使用してもウェブサイトにアクセスできない場合は、追加した URL を除外 URL リストから削除してください。
- 除外 URL リストに追加したウェブサイトでは、セキュリティ・スキャン機能が動作しない場合があります。
- 除外 URL リストには安全なウェブサイトのみを追加するようにしてください。

3.4. メンテナンス機能

本製品のファームウェアのバージョンアップやセキュリティ・スキャン機能で必要な情報更新など、本製品自身が使用するネットワーク機能について説明します。

3.4.1. ファームウェア更新動作

本製品のファームウェアの更新方法は、次の 3 つがあります。

1．メンテナンスバージョンアップ機能を使用してファームウェアを更新する方法
2．設定 Web を使用してファームウェアを更新する方法
3．OPT2 スイッチを使用してファームウェアを更新する方法

更新方法については 5.6.16 章を参照してください。

※他に緊急でファームウェアを更新することがあります。[11]
また、アクティベーション操作時に新しいファームウェアが存在する場合は、ファームウェアを更新します。アクティベーション操作時のファームウェア更新の流れについては 5.2.3 章を参照してください。

メンテナンスバージョンアップ機能のファームウェア更新動作には 2 種類あります。

- 設定 Web で設定した時刻に本製品のファームウェアを更新する
- INFO ランプ橙点灯させて、当社が管理するサーバに新しいファームウェアが存在することをお知らせする

ファームウェア更新動作では、本製品は再起動しますので、本製品を設置しているネットワークが約 3 分程度遮断されます。お使いのネットワークの運用に影響のない時間を設定いただき指定した時刻に行う方法を推奨しています。

[メモ]

- ファームウェアのバージョンアップでは、設定値を引き継ぎます。
  ただし、以下の機能については、初期値で利用している場合に設定値が変更となることがあります。
  (1)ファームウェアバージョン 3.5.9 以前から 3.5.12 以降に更新する場合
  - 無線 LAN 機能の SSID および暗号化キー　(詳細は 3.7 章を参照してください)

[時刻指定バージョンアップ]

新しいファームウェアがある場合、本製品のファームウェアを指定した時刻から 1 時間以内に自動更新します。

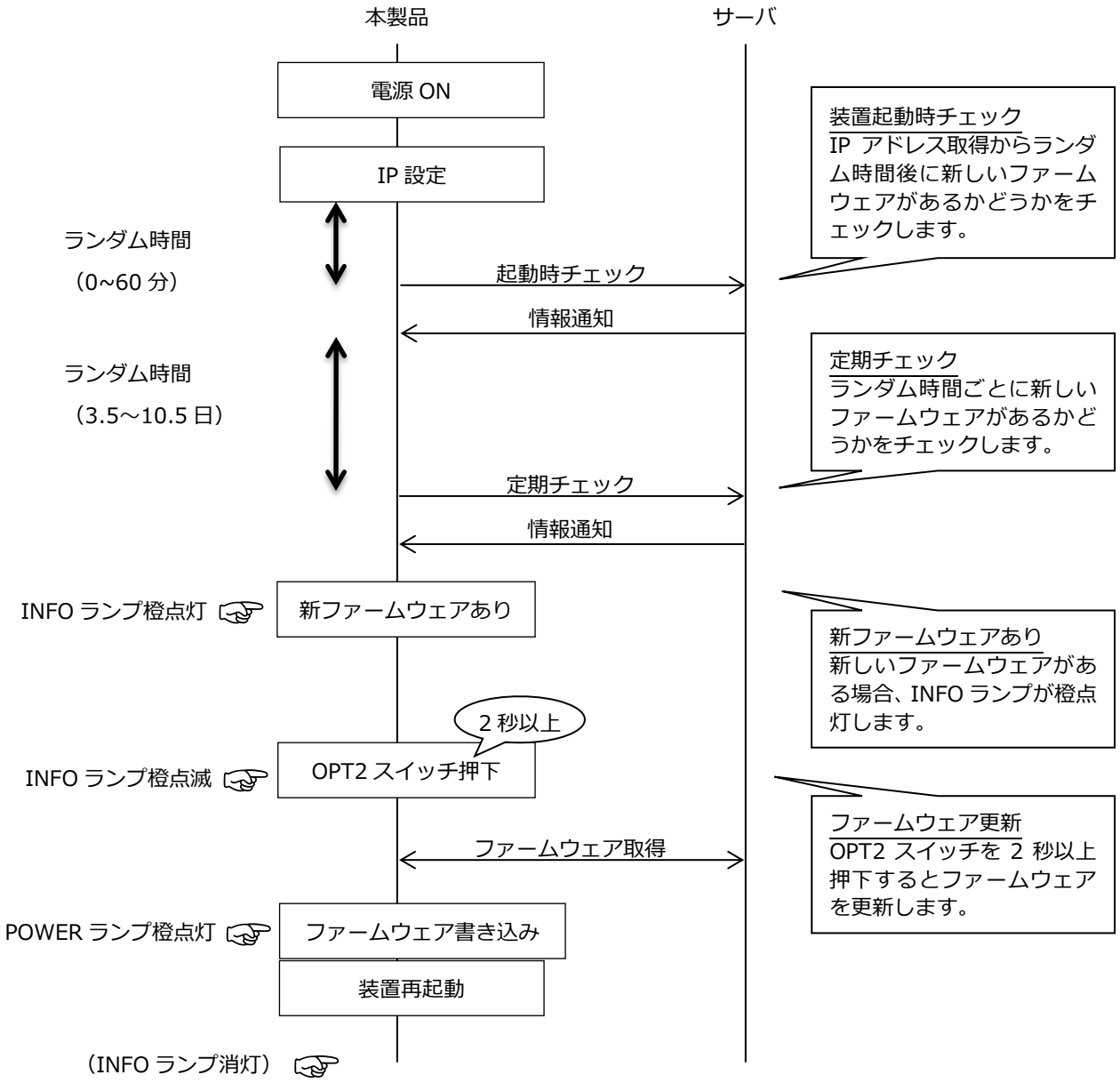
以下のタイミングで新しいファームウェアがあるか確認し、新しいファームウェアがある場合はダウンロードします。

- 装置起動から 0～60 分のランダム時刻
- その後は、3.5 日～10.5 日のランダム時刻

指定した時刻から 1 時間以内にファームウェアを自動更新します。

[11] 本製品に重大な問題が生じた場合など、お客様の操作なくファームウェアを更新することがあります。なお、本機能は無効化することができます（5.6.16 章参照）。

最新のファームウェアの有無チェック、および、ファームウェアの更新手順は次のイメージです。



ファームウェア更新に要する時間は約 5 分です。
更新の流れは以下のとおりです。

1) サーバからファームウェア(約 30MB)を取得します。
2) POWER ランプが橙点滅し、ファームウェアの書き込みが始まります。
   完了するまで約 2 分かかります。
3) 全ランプが緑点灯し装置が再起動します。
4) 装置の起動完了まで約 2 分かかります。
5) 装置起動後、INFO ランプが消灯していることを確認してください。

3.4.2. **設定値の初期化**

[初期化する内容]

本製品の初期化処理は、次の内容を工場出荷状態に戻します。

- 設定 Web で設定した情報（設定 Web のログイン時のパスワードも含みます）
- 運用中に更新されたシグネチャ（危険な Web サイトのリストなど）
- セキュリティ・スキャン機能のログメッセージ、および、統計情報

※アクティベーションした内容は初期化しませんので、再度アクティベーション操作は不要です。

※本製品内のルート証明書は再発行されます。初期化前のルート証明書とは異なりますのでご注意ください。

[初期化方法]

初期化操作には次の方法があります。

- 設定 Web（操作手順は 5.6.15 章を参照してください）
- RESET スイッチ（操作手順は 5.10.1 章を参照してください）

[メモ]

必要に応じて、次の情報をパソコンなどに保存してから、初期化してください。

- 設定 Web で設定した設定値
- セキュリティ・スキャン機能のログメッセージ、統計情報、イベントログ
  保存方法は 3.4.3 章を参照してください。
- ブリッジモード ⇔ ルータモードの切り替え（5.6.19 章もしくは 5.7.29 章を参照してください）
- ファームウェアのバージョンダウン（5.6.16 章を参照してください）
- MAC モード ⇔ IP モードの切り替え（5.9.3 章を参照してください）

簡易 RADIUS 機能を利用しルート証明書をパソコンなどへインポートしていた方は、新たに生成されたルート証明書を再インポートしてください。

初期化した後、設定 Web にアクセスするとウィザードを表示するので、動作モードを再度設定してください。

ファームウェアバージョン 3.5.12 以降で初期化した場合、以下の機能は初期値が設定されません。

(1) 無線 LAN 機能の SSID および暗号化キー

ファームウェアバージョン 3.5.12 以降のファームウェアでは脅威検出時の通知メッセージを HTML 形式で新規に設定することはできません。(詳細は 5.8.11.1 章を参照してください)

[ご注意]

設定値が保存されている USB ストレージを接続した状態で本製品を初期化した場合、本製品の再起動後に USB ストレージから設定値が復元されます。本製品を初期化する場合は USB ストレージを取り外してから行ってください。

3.4.3. **情報をパソコンなどに保存**

本製品の情報を設定 Web でパソコンなどに保存したり USB ストレージに保存したりすることができます。

[保存できる情報]

- 設定 Web で設定した設定値
  （設定 Web の「設定値の保存＆復元」画面で保存。5.6.14 章参照）
  （USB ストレージに保存。3.8 章参照）
- セキュリティ・スキャン機能のログメッセージ、統計情報
  （設定 Web の「セキュリティログ」「統計情報」画面で保存。6.1.11 章、6.1.12 章参照）
- イベントログ、装置状態の情報
  (設定 Web の「イベントログ」「保守機能」「パケットダンプ」画面で保存。6.1.10 章、5.6.18 章、6.1.16 参照）

3.4.4. **再起動**

本製品は、次のタイミングで再起動します。

- 設定 Web で「再起動」を指示した場合
- 設定 Web や RESET スイッチで「初期化」を指示した場合
- 設定 Web で設定を復元した場合
- 設定 Web で動作モードを変更した場合
- 設定 Web でデバイス管理モードを変更した場合
- ファームウェア更新後

初期化を伴わない再起動時は、セキュリティ・スキャン機能のログメッセージと統計情報、イベントログを FlashROM に保存します。

3.4.5. **時計機能**

本製品の時刻は、シグネチャの更新、セキュリティログ、統計情報、イベントログなどで使用します。

本製品の時刻は、

- NTP 機能を使用する
- 設定 Web から直接時刻を入力する

のどちらかの方法で設定できますが、NTP 機能を使用してください。

NTP 機能を使用せずに設定 Web で直接時刻を設定している場合は、本製品を起動するたびに時刻設定が必要です。

[メモ]

- 本製品の起動時の装置時刻は、2015/11/14 00:00:00 です。
  本製品の時刻設定手順は、5.6.13 章を参照してください。
- 本製品の時刻が不正の場合、セキュリティ・スキャン機能が動作しない場合があります。本製品の時刻は実際の時刻に合わせてお使いください。
- 手動設定していても、ライセンスサーバとの認証などのために正確な時刻が必要です。そのため、サーバとの連携の中で時刻は自動補正されます。
- NTP 機能は、SNTP version4 に準拠しています（RFC2030）。
  ユニキャストモードのみ対応しています。
  NTP 機能は、NTP サーバの指定が必要になります。

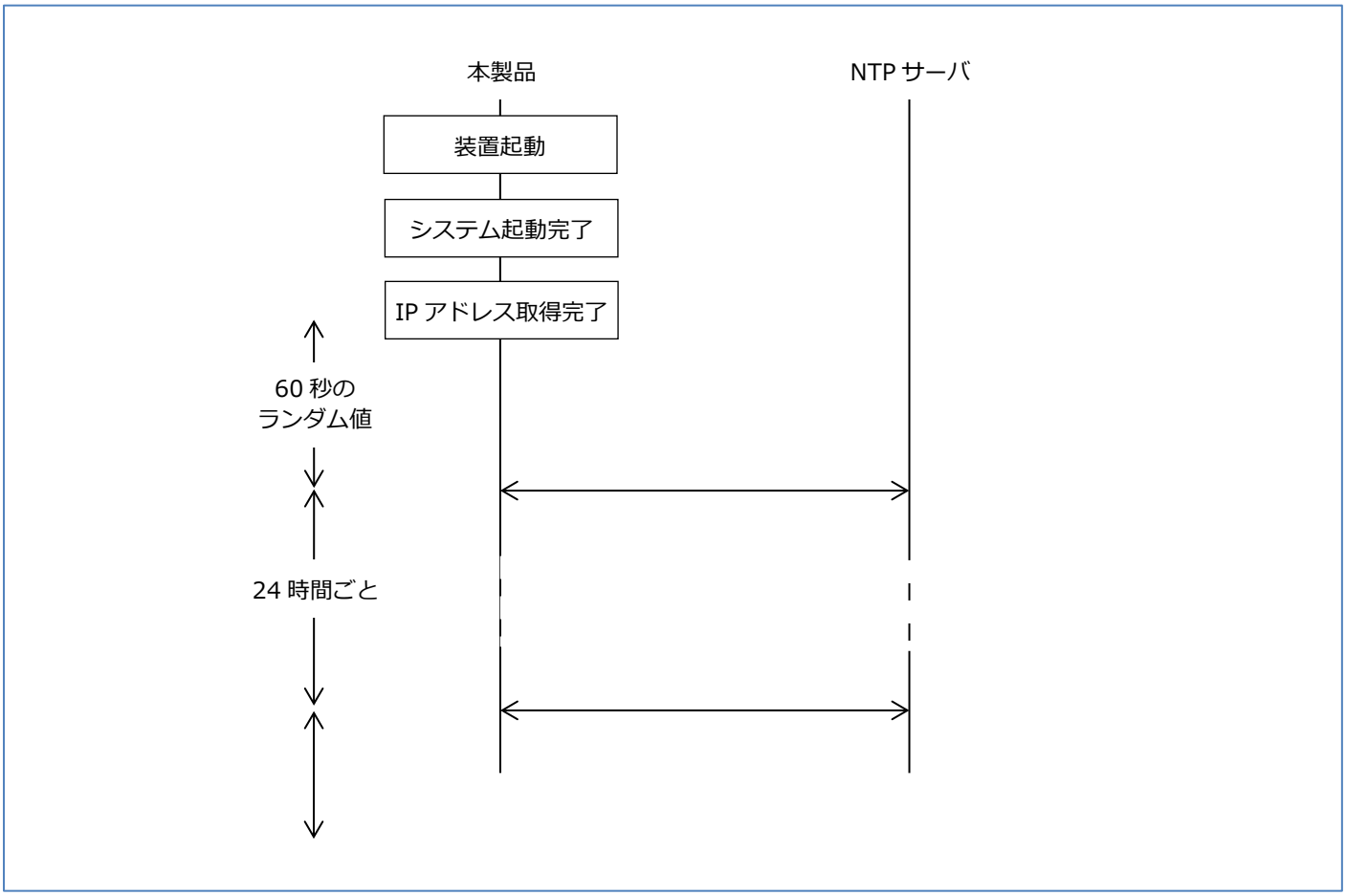
[NTP サーバの設定]

設定 Web で、NTP サーバのアドレスを変更できます。

NTP サーバは 1 台のみ指定できます。

[NTP 定期更新について]

NTP パケットの送信タイミングは次のとおりです。



ネットワーク障害などの理由で NTP サーバから応答がない場合などにより、NTP サーバとの通信に失敗した場合、次のように再送します。

- NTP サーバとの通信に失敗した場合、初回は 15 秒後にリトライします。
  リトライ回数は 5 回、リトライ間隔は前回の時間を倍にした時間です。
  その後は、60 分ごとにリトライします。
  ※リトライ間隔は次のとおりです。
  15, 30, 60, 120, 240, 3600, 3600 …（秒）

3.4.6. **HTTP プロキシサーバ対応**

お客様のネットワークが HTTP プロキシサーバ経由でインターネット接続している場合、本製品にもご利用の HTTP プロキシサーバを設定してください。
本製品のセキュリティ・スキャン機能のアップデートやファームウェアの更新などで、本製品自身がインターネット通信します。

3.4.7. **ping 送信によるネットワーク到達確認**

本製品の ping 機能は、本製品から ping パケットを送信し、本製品から対象端末への到達性を確認できます。

[ping 送信内容]

・ICMP Echo パケット
・5 回送信（1 秒間隔）
・タイムアウト値 … 1 秒

3.4.8. **traceroute 送信によるネットワーク経路確認**

本製品は対象ホストに対して traceroute を実行し、対象ホストまでのネットワークの経路を確認します。お客様が本製品をご使用になる環境で、インターネットまでの経路上に位置しているルータの確認や本製品の IPv4 静的ルーティングの設定を変更した場合にお使いください。

3.4.9. **自己診断機能**

自己診断機能は、本製品が正常に動作可能な状態か確認する機能です。本製品の設定内容やネットワーク構成に起因する問題の切り分けに使用します。
アクティベーションの前でも自己診断機能が使える様になりました。(ファームウェア Ver 3.6.9 以降)
初期設定の際のアクティベーションに失敗する場合などの問題の切り分けにもご利用いただけます。
操作手順の詳細は、6.1.15 章をご参照ください。

[確認する通信状態]

・WAN 側の接続状態
・本製品の設定状態
・サービスサーバへの疎通

3.4.10. **パケットダンプ機能**

パケットダンプ機能は、本製品の各インタフェースに到達したパケットをファイルに保存する機能です。設定 Web で、pcap 形式ファイルとしてダウンロードできます。pcap 形式に対応した任意のビューアアプリケーションなどを用いて内容を確認します。本製品の自発パケットも保存対象のパケットです。パケットダンプは本製品が関係する可能性がある障害発生時に、通信内容を確認するために取得いただき、情報提供いただく場合があります。
詳細は、6.1.16 章を参照してください。

[動作対象インタフェース]

- WAN インタフェース
- LAN インタフェース
- プライマリ SSID
- セカンダリ SSID

3.4.11. **イベントログ**

イベントログは、本製品の設定変更のログや通信のログを表示する機能です。保守の際の障害解析に必要な情報を収集します。イベントログはパソコンなどに保存できます。詳細は、6.1.10 章を参照してください。

[イベントログの内容]

- イベント発生日時
- イベントを検出した機能名称
- イベントの内容

[イベントログの保存]

- 定期的に FlashROM にログファイルを保存します。(毎時 00 分に保存します)
- ログファイル保存領域の最大サイズは 200M バイトです。
  ログ保存領域を超えた場合は、古いログを削除して、新しいログを保存します。
- ログファイルを保存中は POWER ランプが橙点滅しますので、電源を OFF にしないでください。

上記の他、設定 Web の操作による装置再起動のタイミングでイベントログファイルを FlashROM に保存します。

※停電や電源断などの場合は、FlashROM に保存されていないイベントログファイルが失われます。

[設定 Web の操作]

- 設定 Web で最新から 1,000 件分のイベントログを確認できます。
- イベントログを表示するレベルと、保存するレベルを設定できます。
- 「クリア」ボタン押下で、イベントログを削除します。FlashROM に保存しているログファイルも削除します。

[メモ]

- 初期化を行うと、FlashROM に保存しているログファイルを削除します。

3.4.12. **ログアウト機能**

ログアウトを実施することで、管理者が離席中に第三者による操作を防ぐことができます。自動ログアウト時間は変更することができます。設定方法は、5.6.12 章を参照してください。

[ログアウトのタイミング]

- [TOP]画面 右上の「ログアウト」ボタンを押下したとき
- 設定 Web の画面を操作してから 30 分間(初期値)無操作だったとき（自動ログアウト）

3.4.13. **SNMP**

本製品は、ネットワーク管理プロトコルとして SNMP（Simple Network Management Protocol）を搭載しており、SNMP マネージャにて本製品の MIB 情報の取得が可能です。また、イベントが発生した際に、トラップ情報を SNMP マネージャに送信します。

[注意]

- SNMP マネージャから本製品の設定変更を行うことはできません。
- プライベート MIB を使用できません。

[コミュニティ名]

SNMPによるネットワーク管理にはコミュニティ名が必要です。コミュニティ名は、SNMPマネージャから本製品へのアクセスが行われる際の確認に使用します。コミュニティ名はSNMPマネージャの設定に合わせて設定します。

[トラップ情報]

本製品では、トラップ情報の種別を指定して複数のSNMPマネージャにトラップ情報を送信できます。
本製品がサポートするトラップ情報は、SNMP 諸元を参照してください。

[プライベート MIB]

現在のバージョンで取得可能な情報はありません。

[取得できる情報の内容]

RFC1213(MIB-II)の以下 MIB グループに対応しています。

System ,Interface ,Address Translation , IP , ICMP , TCP, UDP , Transmission(dot3 のみ) , SNMP ,ifMIB

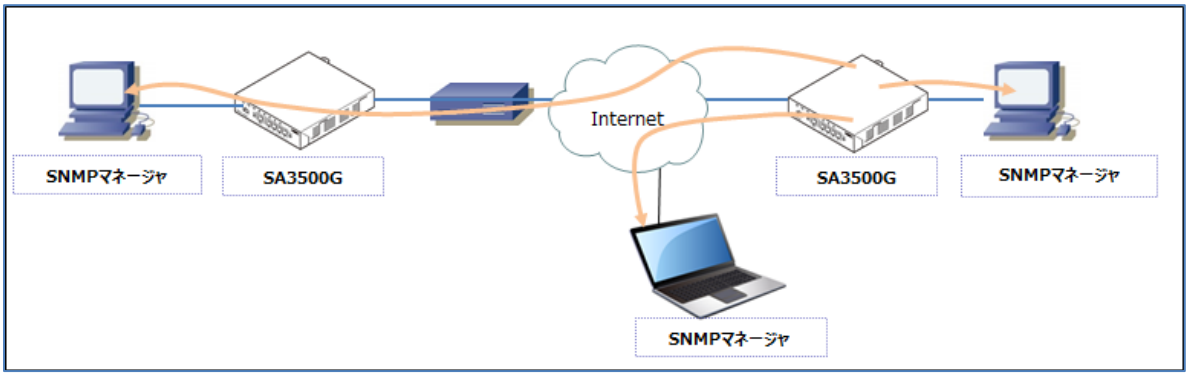
MIB グループ	管理している情報
System	システム情報
Interface	保有するハードのウェアインタフェース情報
Address Translation	IP アドレスと物理的なアドレスとの変換テーブル
IP	プロトコルの使用に関する情報
ICMP	ICMP の動作に関する情報
TCP	TCP の動作に関する情報
UDP	UDP の動作に関する情報
Transmission(dot3)	データ転送(イーサネットライクインタフェース)に関する情報
SNMP	SNMP に関する情報
ifMIB	インタフェース拡張情報
Bridge	ブリッジ動作に関する情報（ブリッジモードで運用時のみ取得可能です）

[SNMP 諸元]

項目	内容	備考
SNMP バージョン	SNMPv1/SNMPv2c	
アクセス制限	可能	最大 3 台の SNMP マネージャを設定可能
トラップ送信先設定	可能	最大 3 台の SNMP マネージャを設定可能
監視可能トラップ	0:cold-start	メニュー「SNMP トラップ送信時の遅延時間設定」にて最大 60 分の遅延が可能
	2:link-down	インタフェース(WAN、PPPoE)のリンクダウン
	3:link-up	インタフェース(LAN、WAN、PPPoE)のリンクアップ
	4:authentication-failure	
その他の設定可能項目	sysLocation	装置の物理的位置の設定
	sysContact	連絡先の設定
MIB 情報	MIB 情報の確認	設定 Web で装置内 MIB 情報を取得可能
	SNMP 統計情報クリア	SNMP 統計情報をクリア

[ユースケース]

SA3500G を使用した構成では自ネットワークの他、インターネットを介した SA3500G の MIB 情報の取得、トラップ通知ができます。



[トラップ通知の条件]

- cold-start は、電源 ON、または設定 Web の「再起動」操作による再起動後に通知します。
- authentication-failure は、本製品に設定したコミュニティ名と SNMP マネージャから送られたコミュニティ名が不一致の場合にトラップ通知します。
- 「SNMP 設定」画面で「設定」ボタンを押下すると、監視再開のため、WAN/LAN/PPPoE インタフェースのリンク状態(linkdown または linkup)のトラップを送出します。

3.4.14. **ホーム IP ロケーション機能**

ホーム IP ロケーション機能は、インターネットからホーム IP ロケーション名で本製品へのアクセスを可能とする機能です。
本機能は、以下の場合に有効になります。

- ルータモードに設定されている（初期値：「ブリッジモード」）
- WAN 側にグローバル IP アドレスが付与されている
- メンテナンスバージョンアップ機能が「有効」になっている（初期値：「有効」）
- ホーム IP ロケーション機能が「有効」になっている（初期値：「無効」）

※ホーム IP ロケーション機能を使用する場合は、機能を有効にする前に、1.8 章 「ホーム IP ロケーション機能のご使用条件」をご確認ください。機能を有効にされた場合は、ご使用条件にご同意いただけたものといたします。

[メモ]
ホーム IP ロケーション名は設定 Web で確認してください。(6.1.2 章を参照してください)
ホーム IP ロケーション名は、本製品固有の名前になり、変更することはできません。
機能が有効となる条件を満たしても、本製品へのアクセスが可能になるまで 1 時間程度要する場合があります。

3.4.15. **NetMeister 機能**

NetMeister は、当社のネットワーク機器管理をクラウド上で提供するサービスです。企業・団体等の管理体ごとに、対応しているネットワーク機器を一元管理することができます。

本製品は子機モードで動作します。NetMeister をご利用いただくには、親機モードで動作する装置が必要です。

利用環境は、[利用環境]を参照してください。

NetMeister の詳細については、以下の URL を参照してください。

https://www.necplatforms.co.jp/product/netmeister/

NetMeister では主に以下のサービスが利用できます。

サービス	概要
表示機能	• 本製品の製造番号を表示する • 本製品のファームウェアバージョンを表示する • 本製品の MAC アドレスを表示する • 本製品の IP アドレスを表示する • 装置稼働状態（稼働時間、CPU、メモリの状態）を表示する • フロントパネルの状態（LED 状態、Ether / USB の各ポートの接続状態、無線 LAN の on/off）を表示する • セキュリティ・スキャン機能のライセンス満了時刻を表示する • セキュリティ・スキャン機能で検出した脅威、通信に関するレポートを表示する [12] • セキュリティログの検索/閲覧/CSV 形式でのエクスポートを行う • 本製品の WAN ポートのトラフィック情報(Tx bps / Rx bps)を表示する • デバイスリストを表示する • デバイスマップを表示する
アクション機能	• 本製品のファームウェア更新を行う • 本製品の再起動を行う • 本製品の設定値を NetMeister に保存する • NetMeister に保存している設定値を本製品に反映する • 本製品の設定値の保存を行う • 本製品の装置状態の一括取得を行う
通知機能	• セキュリティ・スキャン機能で脅威をブロックしたときに通知する • セキュリティ・スキャン機能のライセンス満了が近づいたときに通知する • セキュリティ・スキャン機能のライセンスが満了したときに通知する • 本製品が予期せぬ再起動を行ったときに通知する
リモートログイン機能	• 外部のネットワークからインターネットを経由して本製品の設定 Web に接続する

設定方法は 5.6.9 章を参照してください。

[利用環境]

- 本製品のファームウェアバージョンが、3.5.9 以降である

[12] セキュリティ・スキャン機能で検出した脅威、通信に関するレポートは、セキュリティログ情報を運用サーバーに送信することにより作成しています。

- ブリッジモードに設定されている（初期値：「ブリッジモード」）
- NetMeister 機能が「有効」になっている（初期値：「無効」）
- 本製品の時刻が設定されている(初期値：ntp.nict.jp を使用する)
- お客様のネットワーク内に NetMeister Ver3.0 以降の親機モードに対応した装置が設置されている

  親機モードに対応した装置は別売です。お客様自身で用意してください。

  親機モードに対応した装置については以下の URL を参照してください。

  https://www.necplatforms.co.jp/product/netmeister/outline.html#anc-prd

3.4.15.1. **アクション機能**

NetMeister 上の操作により以下のアクションを実行することができます。

[ファームウェア更新]

本製品を最新のファームウェアに更新することができます。

[再起動]

本製品の再起動を行うことができます。

[設定値の NetMeister への保存]

本製品の設定値を NetMeister 上に保存することができます。

[設定値の反映]

NetMeister 上に保存している設定値を本製品に反映することができます。

[設定値の保存]

本製品の FlashROM に保存していない設定値を FlashROM に保存することができます。

[装置状態の一括取得]

保守者向けの情報を NetMeister 上に保存することができます。

保存できる情報は、設定 Web から保存できる情報と同じです。保存できる情報の詳細は 5.6.18 章を参照してください。

[ご注意]

ファームウェア更新、設定値の反映を実行すると、本製品は再起動します。

本製品の再起動中は、本製品に対して NetMeister から操作することはできません。

NetMeister 上に保存した設定値は、古いバージョンのファームウェアの装置には復元できません。

3.4.15.2. **アラーム通知**

以下のイベントの発生時に NetMeister にアラームを通知します。

通知内容に基づき NetMeister 上でアラームを表示することができます。

[セキュリティ・スキャン機能で脅威をブロックしたとき]

以下の機能で脅威をブロックしたときに、NetMeister にアラームを通知します。

- アンチウイルス
- 不正侵入防止

- Web ガード

一度アラームを通知すると、その後 30 分間は脅威をブロックしてもアラームを通知しません。

[セキュリティ・スキャン機能のライセンス満了が近づいたとき]

ライセンス期限満了間近（60 日前）になったときに、以下のタイミングで NetMeister にアラームを通知します。

(1) 装置動作中にライセンス期限満了間近となったとき

(2) 装置起動時、ライセンス期限満了間近のとき

(3) 上記(1)または(2)を実行した後、ライセンス期限が満了するまで 24 時間ごと

[セキュリティ・スキャン機能のライセンスが満了したとき]

ライセンス期限が満了したときに、以下のタイミングで NetMeister にアラームを通知します。

- 装置動作中にライセンス期限満了となったとき
- 装置起動時、ライセンス期限満了のとき

[予期せぬ再起動が発生したとき]

本製品が予期せぬ再起動をしたときに、NetMeister にアラームを通知します。

3.4.15.3. 脅威統計通知

[セキュリティ・スキャン機能で検出した脅威、通信の統計]

セキュリティ・スキャン機能で検出した脅威、通信の統計を NetMeister に通知します。通知した内容を元に、NetMeister 上で、セキュリティ・スキャン機能で検出した脅威、通信に関するレポートを表示することができます。

通知する内容は 1 時間分の内容です。

以下のタイミングで NetMeister に統計を通知します。

- 毎時 00 分になったとき（0 秒～600 秒のランダム時間が経過後に、前の 1 時間分の統計を通知します）

3.4.15.4. UTM 脅威分析

ファイアウォールを除くセキュリティ・スキャン機能で検出したセキュリティログを NetMeister にアップロードします。これらのセキュリティログは NetMeister 上で検索/閲覧/CSV 形式でのエクスポートをすることができます。

- 1 時間あたり最大 10MB(text 形式)までのログを自動アップロードします。

3.4.16. **ログ送信機能**

ログ送信機能は、本製品のログを syslog サーバに送信する機能です。設定方法は 5.6.11 章を参照してください。

syslog サーバはお客様自身で用意してください。

[送信プロトコル]

ログは UDP で送信します。

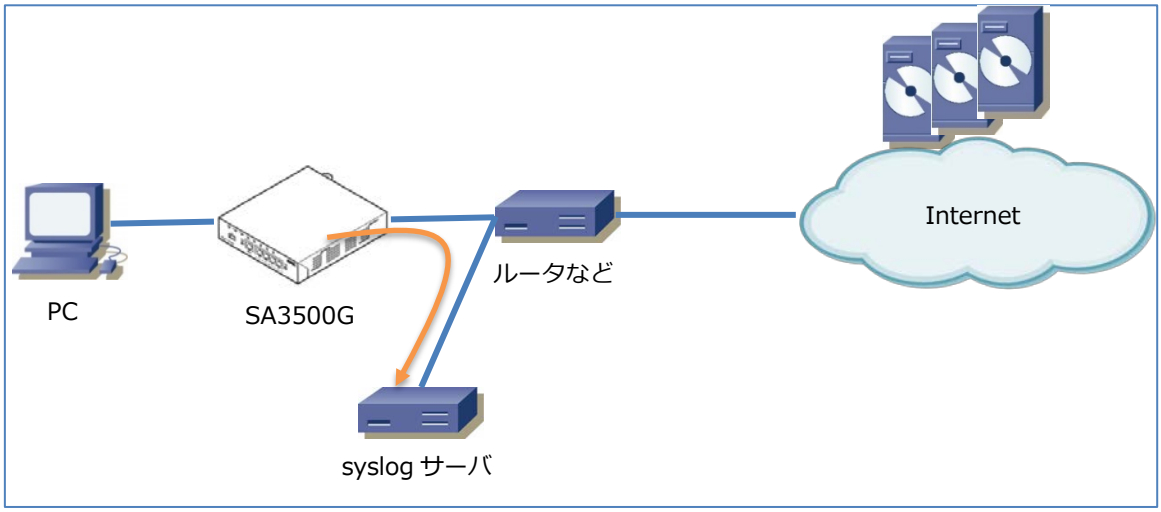
[送信対象ログ]

以下のログを送信できます。

- セキュリティログ
- イベントログ

[ユースケース]

お客様のネットワーク内に設置した syslog サーバにログを送信します。



[ログ送信機能使用時のセキュリティ対策について]

ログ送信機能使用時は、通信経路上でのデータの漏洩対策のためにデータの通信経路を暗号化するなどの対策を行ってください。

セキュリティ対策をほどこさずセキュリティの問題が発生してしまった場合、当社はこれによって生じた損害に対する責任は一切負いかねますのであらかじめご了承ください。

3.5. **ブリッジモードでの機能**

本製品のブリッジング機能は、トランスペアレントブリッジとして動作します。
ただし、セキュリティ・スキャン機能の検出対象のパケットは、この限りではありません。

[メモ]

本製品は通常のブリッジ機器と異なり、アップリンクインタフェースとダウンリンクインタフェースを区別します。
本製品の WAN ポートをインターネット側、LAN ポートをローカルエリア側に接続してください。
なお、ブリッジング動作自体は、アップリンクインタフェース、ダウンリンクインタフェースを区別しません。

本製品は下記 MAC フレームを通過しません。
01-80-C2-00-00-03 IEEE802.1X EAPoL Frame

[ご注意]

IP フラグメンテーションパケットのうち、いずれかのパケットを受信できない場合、本製品はその IP パケットを廃棄します。[13]

3.5.1. **物理インタフェース仕様**

- 物理インタフェースのリンクアップ、リンクダウンに同期して、IP アドレスを管理します。
  本製品のメンテナンス機能などで使用する IP アドレスを WAN/LAN インタフェースの Ethernet のいずれかのリンクアップ契機で取得、すべてがリンクダウンした契機で解放します。
- 本製品のインタフェースのリンクダウン検出タイミングは、「即時」です。

[13] 本製品は、IP フラグメンテーションパケットを一旦再構成します。パケットロスなどで IP パケットを再構成できない場合、その IP パケットを廃棄します。

3.5.2. **IP アドレス**

本製品の IP アドレスは次のとおりです。

インタフェース	IP アドレス	補足
WAN/LAN	次のいずれかの方法で設定してください。 ● 固定設定（設定 Web で設定します） ● DHCP クライアント機能で取得	本製品のセキュリティ・スキャン機能の更新や制御のため、インターネットにアクセスできる IPv4 アドレスが必要です。[14]
装置 IP	169.254.254.11/16	本製品へのアクセス専用 IP アドレスです。

[メモ]

設定 Web で固定の IP アドレスを設定する場合は、5.6.2 章を参照してください。

[DHCP クライアント]

DHCP クライアント機能は、RFC2131、RFC2132 に基本的にしたがっています。また、DHCP リレー機能に対応しています。

WAN インタフェース、LAN インタフェースの両方のインタフェースで動作します。

サポートしているメッセージは次のとおりです。

パケット方向	DHCP メッセ―ジ
送信	DISCOVER, REQUEST, RELEASE, DECLINE
受信	OFFER, ACK

3.5.3. **IPv4 静的ルーティング機能**

[基本仕様]

本製品は、ブリッジモードの IPv4 静的ルーティングに対応しています。

本製品は、次の機能にも対応しています。

- ホストルーティング

[静的ルーティングエントリ]

静的ルーティングエントリを 50 エントリ設定できます。

ブリッジモードの IPv4 静的ルーティングの設定については、5.6.5 章を参照してください。

[14] 本製品へのアクセス用 IP アドレス（169.254.254.11）とは別の IPv4 アドレスが必要です。

3.5.4. **IPv4 パケットフィルタリング**

[フィルタリングポイント]

本製品の IP パケットフィルタリング機能のフィルタリングポイントは、次の 4 つです。

・WAN インタフェースでの IPv4 パケット受信時

・WAN インタフェースでの IPv4 パケット送信時

・LAN/無線 LAN インタフェースでの IPv4 パケット受信時

・LAN/無線 LAN インタフェースでの IPv4 パケット送信時

[フィルタリング条件]

以下に説明するフィルタリングトリガを有します。

トリガ	説明
プロトコル	フィルタするプロトコルを指定します。 IP/TCP/UDP/ICMP/プロトコル番号で指定します。
TCP フラグ	プロトコルが TCP の場合、TCP フラグを指定できます。
Type/Code	プロトコルが ICMP の場合の Type と Code を指定できます。
送信元 IP アドレス	送信元 IP アドレス/マスク長を指定します。
送信元ポート番号	プロトコルが TCP または UDP の場合の送信元ポート番号を指定できます。
宛先 IP アドレス	宛先 IP アドレス/マスク長を指定します。
宛先ポート番号	プロトコルが TCP または UDP の場合の宛先ポート番号を指定できます。

フィルタ設定でフィルタ対象パケットにしたがって、次の設定をしてください。

※IPoE/PPPoE/IPsec1 はルータモード時に選択できます。

フィルタ対象パケット	対象インタフェース	フィルタタイプ	方向
IPoE→LAN	IPoE	転送 (転送パケット)	in
LAN→IPoE			out
IPoE→本製品		送受信 (本製品送受信パケット)	in
本製品→IPoE			out
PPPoE→LAN	PPPoE	転送 (転送パケット)	in
LAN→PPPoE			out
PPPoE→本製品		送受信 (本製品送受信パケット)	in
本製品→PPPoE			out
LAN→WAN (IPoE・PPPoE)	LAN	転送 (転送パケット)	in
WAN (IPoE・PPPoE)→LAN			out
LAN→本製品		送受信 (本製品送受信パケット)	in
本製品→LAN			out
IPsec1→LAN	IPsec1	転送 (転送パケット)	in
LAN→IPsec1			out
IPsec1→本製品		送受信 (本製品送受信パケット)	in
本製品→IPsec1			out

3.5.5. **MAC アドレスフィルタリング**

MACアドレスが登録されたLAN側端末の通信を許可できるようにする機能です。これにより、MAC アドレスが登録されていないLAN側端末からの通信を遮断することができます。
LAN側端末は有線LANインタフェースと無線LANインタフェースに接続された端末を指します。MACアドレスは有線LANと無線LANそれぞれ60件まで本製品に登録できます。
管理外のデバイス(PC、スマートフォンなど)からインターネットアクセスできないようにMACアドレスフィルタリングをご利用ください。

3.5.6. **Ethernet ポート設定**

イーサネットLANでは機器同士で通信速度（10 or 100）や通信モード（全二重 or 半二重）を合わせていなければ通信が不安定になる場合があります。本製品に接続するハブ等の機器がオートネゴシエーション機能に対応していない場合は、通信速度と通信モードメディア方式、フロー制御を設定Webで設定してください。設定方法は5.6.8章を参照してください。

3.5.7. **DNS リゾルバ**

[動作インタフェース]

WAN インタフェース

LAN インタフェース

[基本仕様]

- IPv4 で動作します。
- DNS サーバの IP アドレスを最大 2 アドレス管理します。

  DNS サーバの IP アドレスを次の方法で設定します。

  ・設定 Web で設定

  ・DHCP で取得した IPv4 アドレスを設定
- DNS-cache 機能を持ちます。

  ・A RR と AAAA RR をキャッシュします。

  ・キャッシュ数は最大 60 エントリです。

  ・キャッシュ時間は最大 5 分で、TTL 値が 5 分以内の場合は TTL 値にしたがってキャッシュします。

[動作仕様補足]

・再送は、2 秒間隔 3 回です。

・送信元ポート番号にランダムな値を使用します。

3.6. **ルータモードでの機能**

本製品は IPv4 ルータです。

[メモ]

本製品は通常のルータ機器と異なり、アップリンクインタフェースとダウンリンクインタフェースを区別します。

本製品の WAN ポートをインターネット側、LAN ポートをローカルエリア側に接続してください。

3.6.1. **物理インタフェース仕様**

- 物理インタフェースのリンクアップ、リンクダウンに同期して、IP アドレスを管理します。
  本製品の WAN インタフェースの IP アドレスを WAN インタフェースの Ethernet のリンクアップを契機に取得し、リンクダウンを契機で解放します。
- 本製品のインタフェースのリンクダウン検出タイミングは、「即時」です。

3.6.2. **IP アドレス**

本製品の IP アドレスは次のとおりです。

インタフェース	IP アドレス	補足
WAN	次のいずれかの方法で設定してください。 ● 固定設定（設定 Web で設定します） ● DHCP クライアント機能で取得 ● PPPoE 機能で取得	本製品のメンテナンス機能のうち、インターネット上のサーバと通信する必要のある機能は、WAN インタフェースの IP アドレスを使用して動作します。
LAN	初期値として 192.168.110.1/24 を設定しています。 変更する場合は、設定 Web から変更します。	LAN インタフェース、無線 LAN インタフェース共通です。
装置 IP	169.254.254.11/16	本製品へのアクセス専用 IP アドレスです。

3.6.3. **IPv4 静的ルーティング機能**

[動作インタフェース]

WAN インタフェース、LAN/無線 LAN インタフェース

[基本仕様]

本製品は、WAN インタフェースと LAN/無線 LAN インタフェースの間をルーティングします。

ゲートウェイの指定方法として、PPPoE インタフェース指定、IPsec1 インタフェース指定ができます。

※IPsec1 は IPsec の動作モードがルートベースのときに設定できます。

本製品は、IPv4 静的ルーティングに対応しています。

本製品は、次の機能にも対応しています。

- ホストルーティング
- ICMP Redirect メッセージ送信機能

[静的ルーティングエントリ]

静的ルーティングエントリを 50 エントリ設定できます。

[ICMP Redirect 機能]

ICMP Redirect メッセージを送信できます。お客様のネットワークで、ICMP Redirect メッセージの送信が好ましくない場合は、本機能を無効にしてください。

IPv4 静的ルーティングの設定については、5.7.12 章を参照してください。

3.6.4. **IPv4 パケットフィルタリング**

機能説明はブリッジモードと同じです。3.5.4 章を参照してください。

3.6.5. **MAC アドレスフィルタリング**

機能説明はブリッジモードと同じです。3.5.5章を参照してください。

3.6.6. **Ethernet ポート設定**

機能説明はブリッジモードと同じです。3.5.6 章を参照してください。

3.6.7. **MTU**

Maximum Transmission Unit (MTU)は、ネットワークにおいて 1 回の転送（1 フレーム）で送信できるデータの最大値を示す伝送単位のことです。MTU の値は利用される通信メディアやカプセル化の有無などによって変わります。例えばイーサネットでは最大 1,500 バイトです。本製品では MTU 値を設定 Web で変更できます。設定は 5.7.6 章を参照してください。

3.6.8. **NAPT**

[動作インタフェース]

WAN インタフェース、LAN/無線 LAN インタフェース

[基本仕様]

本製品の NAPT 方式は、Port-Restricted cone NAT です。

[補足]

Ver3.2.29 以降は、設定 Web から機能の有効/無効の設定ができます。設定については 5.8.3 章を参照してください。

[NAPT セッション管理]

- NAPT セッションを最大 30,000 セッション管理します。
- NAPT セッションの管理数が最大数を超えた場合、次の条件にしたがって古い NAPT セッションを削除し、新しい NAPT セッションを管理します。

優先度高　TCP > UDP（ポート番号 500, 4500）> 上記以外の IP パケット　優先度低

- NAPT セッション情報として、次の内容を管理します。
  - Internal IP Address（LAN インタフェースの IP アドレス）
  - External IP Address（WAN インタフェースの IP アドレス）
  - Remote IP Address（宛先の IP アドレス）
  - プロトコル（送信元ポート番号、宛先ポート番号を含む）

[NAPT セッションタイマ]

NAPT セッションタイマの初期値は次のとおりです。

TCP　：3,600 秒
UDP　：300 秒
ICMP　：30 秒
その他　：600 秒

TCP/UDP/ICMP の NAPT セッションタイマの値を設定 Web で変更できます。
設定については、5.8.3 章を参照してください。

[ポートマッピング]

ポートマッピングエントリを 50 エントリ設定できます。

[ALG 処理]

本製品で対応している ALG 処理は次のとおりです。
FTP, ICMP, VPN パススルー（PPTP, IPsec）

[MSS 調整]

本製品の WAN インタフェースで PPPoE を動作させている場合など、TCP MSS 値を最適な値に自動調整します。

3.6.9. **PPPoE**

[動作インタフェース]

WAN インタフェース

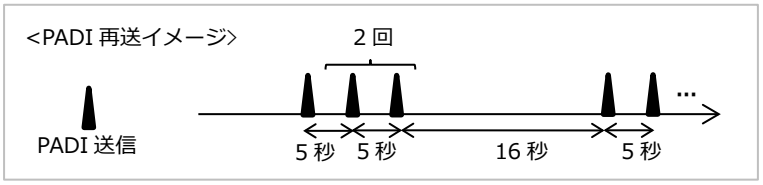
[基本仕様]

- PPPoE セッションを 1 セッション確立できます。
- PPPoE 機能は、RFC2516 に基本的にしたがっています。
- PPP 機能は、RFC1661 に基本的にしたがっています。
- IPCP 機能は、RFC1332 に基本的にしたがっています。
- 認証プロトコルは、PAP/CHAP をサポートしています。RFC1334 に基本的にしたがっています。
  ID、パスワードを設定することで、本製品の PPPoE 機能を有効にします。
  ID、パスワードの使用可能文字に関する仕様は次のとおりです。
  ・半角英数字、記号（アスキーコード：0x20~0x7e）
  ・最大 128 文字
- PPP Keepalive 機能を無効/有効にできます。

[PPPoE 送信タイミング]

- WAN インタフェースのリンクダウン→リンクアップ時
- WAN インタフェースに IP アドレスが設定されていない時
- PADI フレームの再送に関する仕様は次のとおりです。

  再送間隔　　：5 秒
  再送回数　　：2 回
  インターバル：16 秒



[メモ]

本製品の WAN インタフェースで、PPPoE と DHCP クライアント機能を同時に動作させることはできません。

3.6.10. **DHCP クライアント**

[動作インタフェース]

WAN インタフェース

[基本仕様]

- RFC2131、RFC2132 に基本的にしたがっています。また、DHCP リレー機能に対応しています。
- サポートしているメッセージは次のとおりです。

パケット方向	DHCP メッセージ
送信	DISCOVER, REQUEST, RELEASE, DECLINE
受信	OFFER, ACK

- DHCP サーバからの ACK メッセージ受信時、配布 IP アドレスの重複確認を ARP で実施します。
- DHCP サーバから配布された IP アドレスが、本製品の LAN インタフェースの IP アドレスと重複していた場合、DHCP RELEASE メッセージを送信し、その後、DHCP シーケンスを再開します。

[DHCP メッセージ送信タイミング]

RENEWING/REBINDING の送信タイミングは次のとおりです。

延長要求タイミング	宛先	送信回数	説明
RENEWING リースタイム×0.5	unicast	1	T1
	unicast(再送)	*	T2 までの残り時間が 60 秒以上であれば、その半分で送信。
REBINDING リースタイム×0.875	broadcast	1	T2
	broadcast(再送)	*	リースタイムまでの残り時間が 60 秒以上であれば、その半分で送信。

DISCOVER メッセージ送信タイミングは次のとおりです。

DISCOVER 送信タイミング	説明
DHCP 起動時	送信後、3 秒間応答がない場合は再送を行います。 再送は 2 回繰り返し、それでも応答がない場合は 20 秒経過後、再度送信処理を行います。 (応答がない場合は、3 秒→3 秒→23 秒→3 秒→3 秒・・・で送信)
リースタイム満了時	DHCP 起動時と同様に、送信後、3 秒間応答がない場合は再送を行います。 再送は 2 回繰り返し、それでも応答がない場合は 20 秒経過後、再度送信処理を行います。 (応答がない場合は、3 秒→3 秒→23 秒→3 秒→3 秒・・・で送信)

REQUEST メッセージ送信タイミングは次のとおりです。

REQUEST 送信タイミング	説明
OFFER 受信時	送信後、3 秒間 ACK を受信しない場合は再送を行います。 再送は 2 回繰り返し、それでも応答がない場合は 20 秒経過後、DISCOVER から処理をやり直します。 (応答がない場合は、3 秒→3 秒で送信。23 秒経過で DISCOVER 処理に戻る)
RENEWING/REBINDING	ACK は、次の REQUEST を送信するまで受信待ちする。

[メモ]

本製品の WAN インタフェースで、DHCP クライアントと PPPoE 機能を同時に動作させることはできません。

3.6.11. **DHCP サーバ**

[動作インタフェース]

LAN/無線 LAN インタフェース

[基本仕様]

- RFC2131、RFC2132 に基本的にしたがっています。DHCP リレー機能に対応していません。
- サポートしているメッセージは次のとおりです。

パケット方向	DHCP メッセージ
送信	OFFER, ACK
受信	DISCOVER, REQUEST, RELEASE, DECLINE

- 次の内容で OFFER メッセージ、ACK メッセージを送信します。

フィールド/option	初期値	補足
Your IP Address	割当アドレスから配布	最大 250 アドレスを配布
Subnet Mask [1]	255.255.255.0	設定変更可能
Router [3]	192.168.110.1	設定変更可能
Domain Name Server [6]	192.168.110.1	NAPT 機能有効時に LAN インタフェースの IP アドレスを設定
Domain Name [15]	（空欄：ユーザーの設定値を使用）	入力可能文字数：64 文字 入力可能文字列：半角英数字、!'()*-._~
NetBIOS Name Server [44]	（空欄：ユーザーの設定値を使用）	
IP Address Lease Time [51]	24 時間	設定変更可能（最大 72 時間） 0 を設定すると「無限」の意味になります

- DHCP クライアントに IP アドレス配布前、配布アドレスが使用中でないかの確認を ARP で実施します。
- DHCP DECLINE メッセージの仕様は次のとおりです。

  DECLINE メッセージを受信した場合、該当の IP アドレスを 3 分間配布しません。

3.6.12. **プロキシ DNSv4**

[基本仕様]

- IPv4 で動作します。
- ルータモード時のみ動作します。
- アップリンクインタフェース（WAN インタフェース）で DNS クライアント動作、ダウンリンクインタフェース（LAN/無線 LAN インタフェース）で DNS サーバ動作します。
  LAN/無線 LAN インタフェースに接続している端末から DNS query パケットを受信すると、DNS サーバに送信します。また、DNS サーバからの DNS response パケットを受信すると、端末に送信します。DNS サーバの IP アドレスを最大 2 アドレス管理します。
  DNS サーバの IP アドレスを次の方法で設定します。
  ・設定 Web で設定
  ・DHCP で取得した IPv4 アドレスを設定
  ・PPPoE で取得した IPv4 アドレスを設定
- DNS-cache 機能はありません。

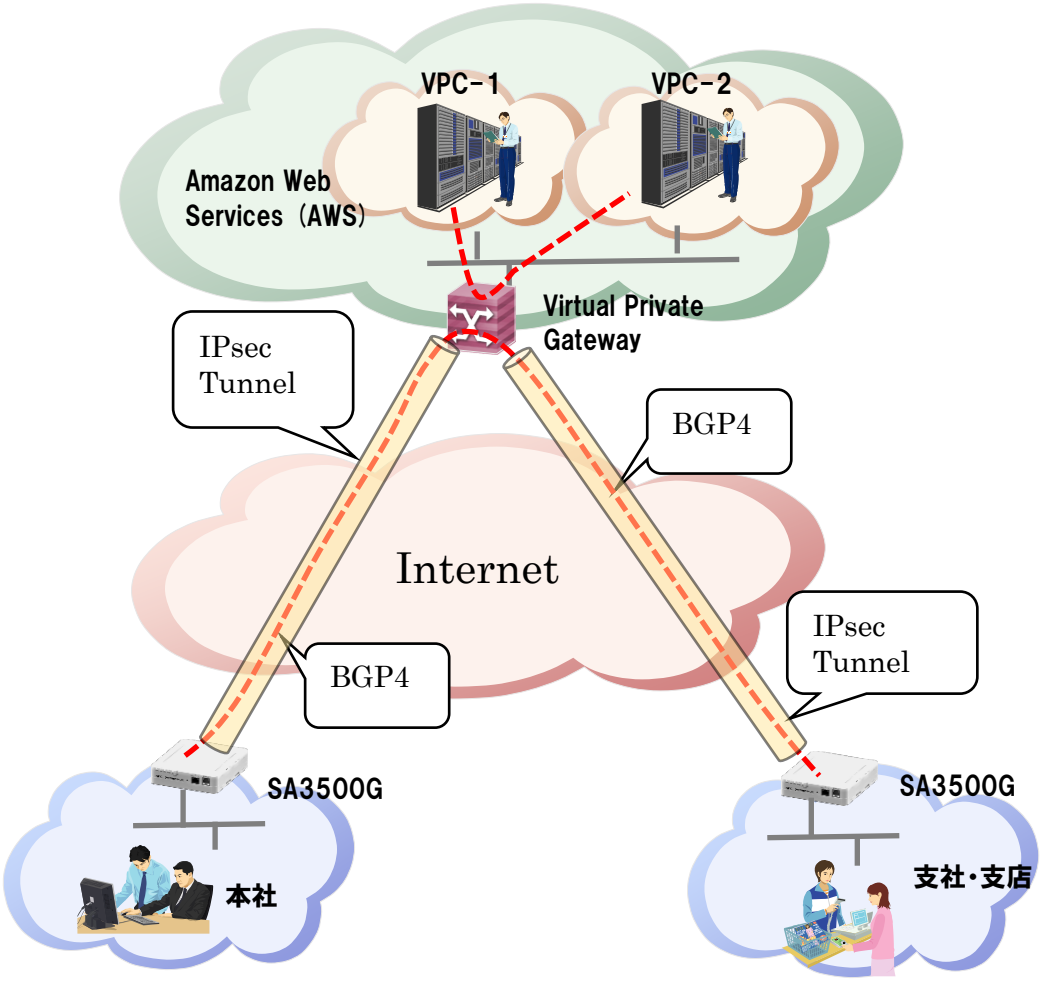
[動作仕様補足]

- 送信元ポート番号にランダムな値を使用します。

3.6.13. **クラウドサービス接続**

本製品は Amazon Web Service(AWS)や Microsoft Azure のクラウドサービスに接続することができます。クラウドサービス接続を使って、本社と支社・支店のデータ共有などのクラウドサービスを利用できます。

本製品を本社と支社・支店に設置して、クラウドサービス接続を行ったイメージが下図です。本製品はクラウドサーバと IPsec トンネルを確立して、本社から各拠点にアクセス、または各拠点から本社や他拠点にアクセスするために BGP4 を用いて動的にルーティングできるようにしています。Psec トンネルの中で BGP4 を動作させることで秘密性・信頼性を確保しています。クラウドサービス接続の設定方法は 5.7.15 章を参照してください。



クラウドサービスをご利用になるには、サービス事業者と契約してください。クラウドサービスの詳細はサービス事業者のホームページでご確認ください。

AWS：https://aws.amazon.com/jp/

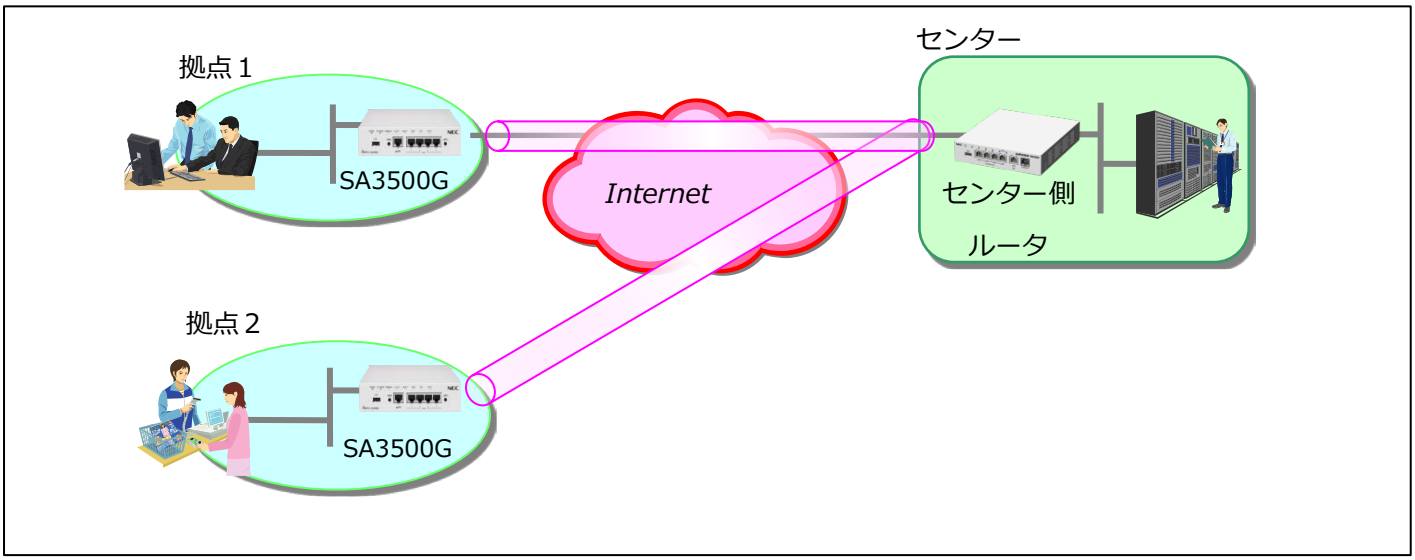
Azure：https://azure.microsoft.com/ja-jp/

3.6.14. **IPsec**

本製品は IPsec 通信に対応しています。IPsec とは、IP security Protocol の略で IP パケットを暗号化し、安全に通信を行うためのプロトコルで Internet-VPN に利用されています。

主な特長として、暗号化、認証の機能があります。暗号化として、データの暗号化により機密性を確保できます。認証として、通信相手の認証とパケットの改ざんを検出できます。

なお、本製品で行う IPsec 通信は、セキュリティ・スキャン機能が動作します。IPsec の設定方法は 5.7.16 章を参照してください。



Ver3.2.29 以降で IKEv2 が利用できます。

IKEv2 は IKEv1 との互換性はありませんが、IKEv1 のプロトコルでは不明確だった動作仕様が明確化されており、事前共有鍵以外の認証方式のサポート、耐障害性を考慮したプロトコル設計などが特徴となっています。設定内容は 5.7.16 章を参照してください。IKEv1 と IKEv2 は異なる点が多いので注意してください。

[暗号化]

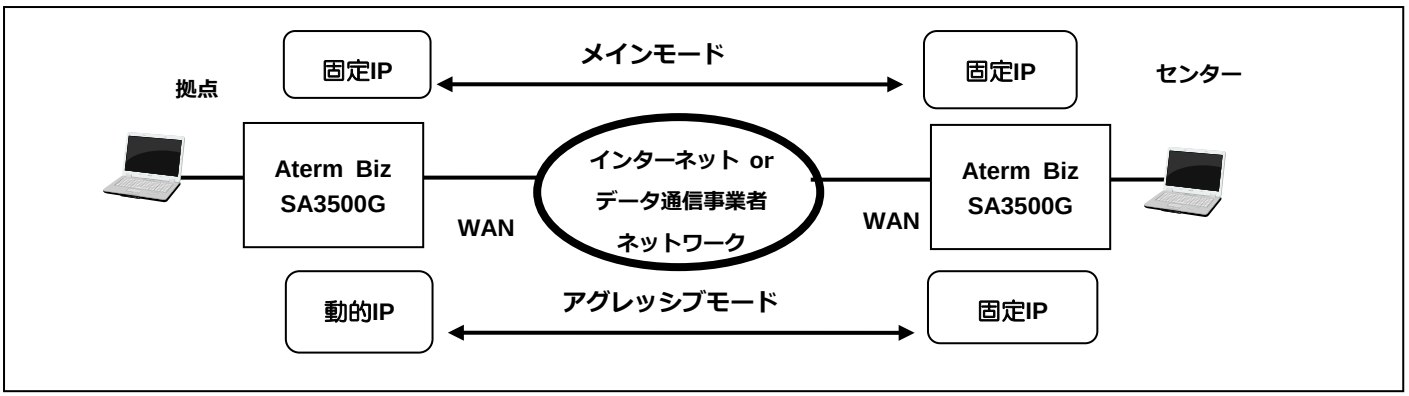
ESP（Encapsulated Security Payload）を使用した IP パケット全体を暗号化するトンネルモードをサポートしています。

■IKEv1

[鍵交換タイプ]

メインモードとアグレッシブモードをサポートしています。接続する回線種別（IP アドレスの割当方法）によって、鍵交換タイプを選択できます。

メインモード	：IPsec の両端の製品が固定 IP アドレスを有している場合に利用
アグレッシブモード	：一方の製品が動的 IP アドレスの場合に利用



■IKEv2

[IKEv2 の概要]

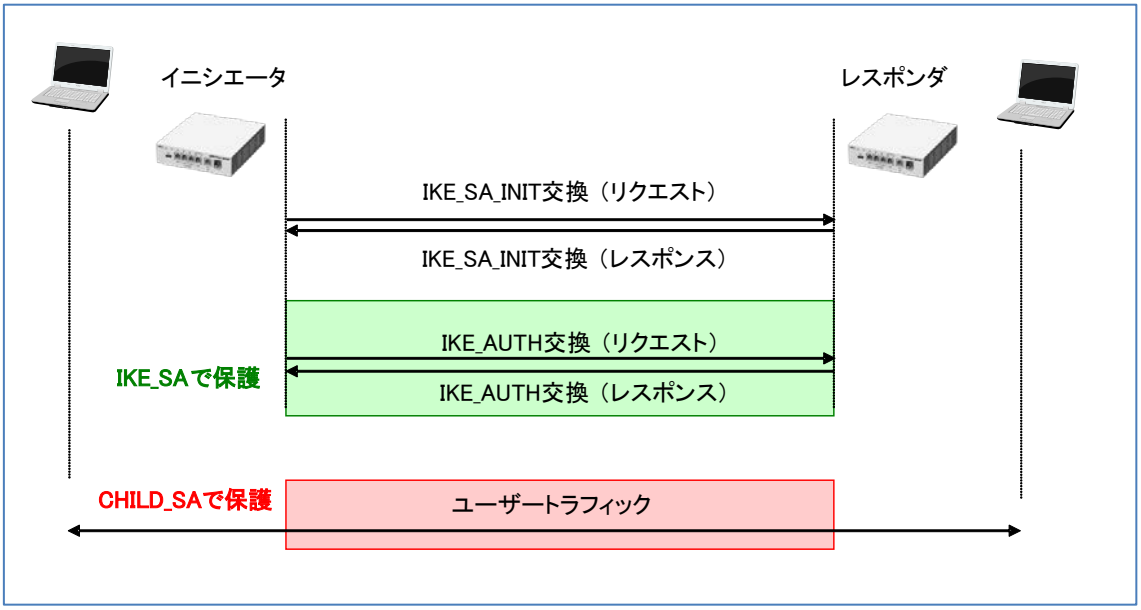
IKEv1 を利用していた方を対象に、IKEv2 機能の概要を説明します。IKEv2 は IKEv1 と互換性がなく、使われる用語も異なります。

- ISAKMP-SA, IPsec-SA 相当の機能は、それぞれ IKE-SA, Child-SA となります。
- ハッシュアルゴリズム相当の機能は、認証アルゴリズムと擬似乱数アルゴリズムです。
- メインモード、アグレッシブモードという概念はなくなり、動作は共通化されます。
- Phase1-ID、Phase2-ID も共通化され、一組の local-ID, remote-ID だけになります。

[鍵管理方式]

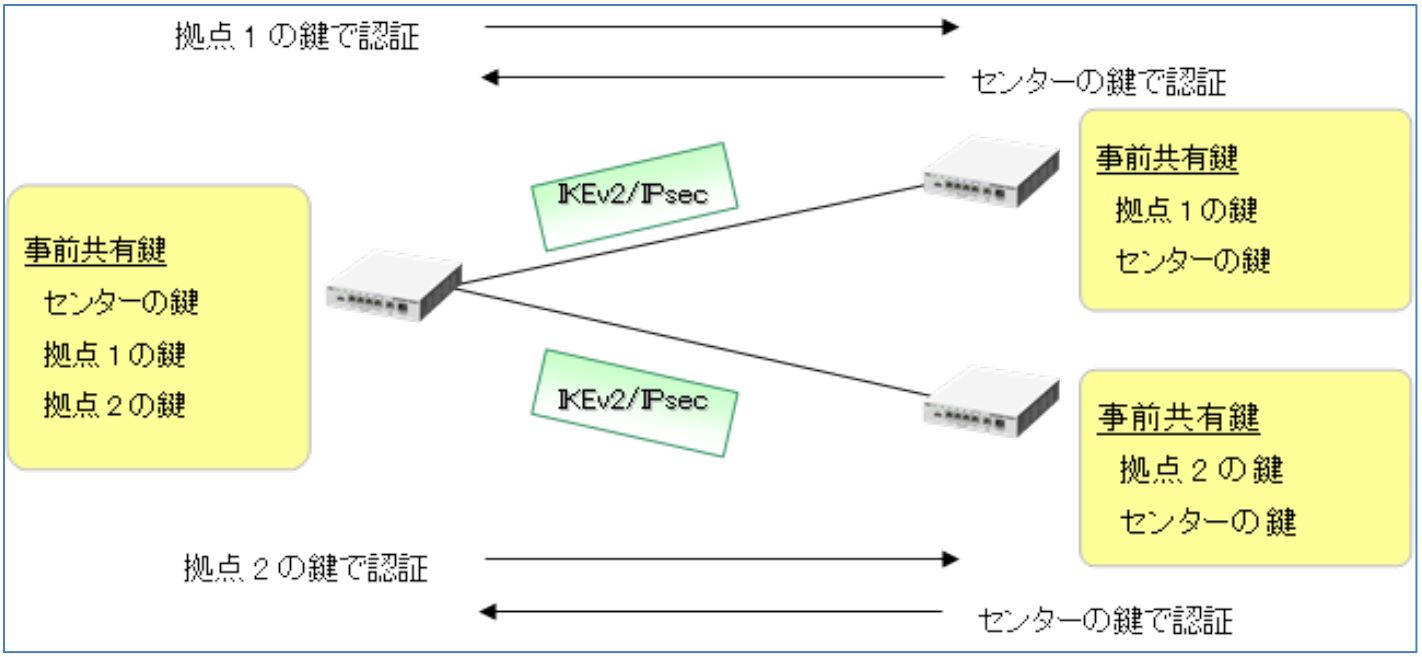
IKEv2 では、自装置用の事前共有鍵と相手装置用の事前共有鍵の設定がそれぞれ必要となります。

※IKEv1 の場合、自装置と相手装置で共通の事前共有鍵を使用します。



[IKEv2 シーケンス]

- ●IKE_SA_INIT 交換　：　IKE_SA の折衝と秘密鍵の共有
- ●IKE_AUTH 交換　：　相手認証と CHILD_SA の折衝



[接続方式]

IPsec トンネルを構築するために、常時接続とオンデマンド接続を選択できます。
「Rekey」の設定と関連付けることで、以下 3 パターンの設定を設定 Web から設定できます。

Rekey	接続形態	リキー方法
Enable	オンデマンド接続	生成された SA を使用した暗号化通信が存在する場合リキーを行う
No Rekey	オンデマンド接続	生成された SA を使用した暗号化通信の有無にかかわらずリキーを行わない
Always	常時接続	生成された SA を使用した暗号化通信が存在する場合リキーを行う

[IKE SA と IPsec SA の依存関係]

IPsec トンネルを構築・維持する制御パケットを送受信するための IKE SA を構築し、IKE SA を利用して実際の暗号化データを送受信するための IPsec SA を構築します。

[リキー]

通信路の秘匿性を保つためにリキーを行い、新しい SA を生成します。リキーした後は、新しい SA で通信します。ライフタイム満了後に古い SA を削除します。

[対向先と送信元の指定]

IPsec トンネルを構築するために、対向先 IP アドレスを指定します。送信元 IP アドレスは自動的に選択します。

[IPsec の動作モード]

動作モードとして、「ポリシーベース」と「ルートベース」の 2 種類があります。

ポリシーベース	IPsec 設定画面で設定したポリシーを満たす通信のみ、IPsec 通信します。
ルートベース	IPsec 用のトンネルインタフェースを生成し、そのインタフェースのルーティング設定にしたがって IPsec 通信します。

IPsec 設定画面の初期値は、ポリシーベースです。クラウドサービス接続は、それぞれルートベースが使用されます。

[フラグメント方式]

IPsec で暗号化すると、元の IP パケット長よりも長くなります。このため、実際に送信するときには、フラグメントが発生する場合があります。フラグメント方式には、暗号化してからフラグメントを行う「post-fragment」方式と、フラグメントしてから暗号化を行う「pre-fragment」方式があります。

IPsec 設定画面の初期値は、「post-fragment」方式です。

クラウドサービス接続においては、以下となります。

Amazon Web Service	「post-fragment」方式
Microsoft Azure (Route Based)	「pre-fragment」方式
Microsoft Azure (Policy Based)	「pre-fragment」方式

[IKE 制御パケットの再送]

IKE では制御シーケンスを監視し、シーケンスが正常に進まないときには IKE 制御パケットを再送します。

[IKE 拡張機能]

- IKE SA 削除

  IKE SA を削除するときに先立ち、その IKE SA を通して対向装置に DELETE メッセージ（DELETE PAYLOAD）を送信し、対向装置の対になっている IKE SA を削除できます。

- INITIAL-CONTACT

  IKE Phase1 を開始するときに、初回の IPsec 接続であることを対向先に通知する機能です。INITIAL-CONTACT を受信した相手装置は、IPsec 接続先が SA を消失したものとみなし、自分の持っている IPsec SA を削除します。

- Keepalive

  IKE SA を監視する DPD(Dead Peer Detection)-Keepalive 方式をサポートしています。

[IPsec 拡張機能]

- TCP MSS 書き換え

  IPsec トンネルを通過する IP パケットが TCP である場合、SYN パケットの TCP MSS 値を書き換えます。

- アンチリプレイ機能

  IPsec では、シーケンス番号を監視し、重複して受け取ったパケットを廃棄することによりリプレイ攻撃から防御します。アンチリプレイ機能は常に有効で動作します。

[その他]

- NAT/NAPT 同時動作（Split 動作）

[IPsec 諸元一覧]

項目			機能	
IKEv1	鍵交換方式		自動鍵(鍵交換プロトコル：IKEv1)	
	交換タイプ		メインモード、アグレッシブモード、クイックモード	
	IKE SA と IPsec SA の依存関係		Continuous-Channel SA 型	
	認証方式		事前鍵共有方式(pre-Shared Key)	
	サポートアルゴリズム	暗号化	3DES、AES-128、AES-192、AES-256	
		認証	HMAC-MD5、HMAC-SHA-1、HMAC-SHA-2-256	
	DH グループ		768bit(group1)、1024bit(group2)、1536bit(group5)、2048bit(group14)	
	SA	IKE ID 認証	ローカル ID、リモート ID (IPv4 アドレス指定、FQDN 指定、key-id 指定、user-FQDN 指定)	
		IKE 接続	再送間隔指定、再送回数指定	
		ライフタイム	時間設定	
		リキータイミング	残り時間設定	
	ソースアドレス指定		固定設定	
	対地数		1 対地	
IKEv1 拡張	IKE SA 削除		手動削除	
			delete payload 受信時の IKE SA 削除	
			IKE SA 削除時の delete payload 送信	
	IPsec SA/IKE SA のリキー拡張		常時接続	Traffic なしでも常時接続

			オンデマンド接続		Traffic ありでリキー Traffic ありでもリキーしない
	INITIAL-CONTACT 設定		単独送信(ペイロード付加なし)		
	Keepalive		DPD	送信間隔指定	
				リトライアウト回数指定	
	NAT トラバーサル		1 セッション		
	コミットビット		Phase1：アグレッシブモードのみ Phase2：レスポンダのみ		
IKEv2	鍵交換方式		自動鍵(鍵交換プロトコル：IKEv2)		
	認証方式		事前鍵共有方式(pre-Shared Key)		
			電子証明書	EAP-MD5	
				デジタル署名(拠点側のみ)	
	サポート アルゴリズム	暗号化	3DES、AES-128、AES-192、AES-256		
		認証	HMAC-MD5、HMAC-SHA-1、HMAC-SHA-2-256		
		PRF	HMAC-MD5、HMAC-SHA-1、HMAC-SHA-2-256		
	DH グループ		768bit(group1)、1024bit(group2)、 1536bit(group5)、2048bit(group14)		
	SA	IKE 認証	ローカル ID、リモート ID (IPv4 アドレス指定、FQDN 指定、key-id 指定、user-FQDN 指定)		
		IKE 接続	再送間隔指定、再送回数指定		
		ライフタイム	時間設定		
		リキータイミング	残り時間設定		
	ソースアドレス指定		固定設定		
	対地数		1 対地		
IKEv2 拡張	IKE SA 削除		手動削除		
			delete payload 受信時の IKE SA 削除		
			IKE SA 削除時の delete payload 送信		
	IPsec SA/IKE SA のリキー拡張		常時接続	Traffic なしでも常時接続	
			オンデマンド接続	Traffic ありでリキーする Traffic ありでもリキーしない	
	Keepalive		DPD	送信間隔指定	
				リトライアウト回数指定 (IKEv2 では IKE SA 再送間隔/再送回数が適用)	
	NAT トラバーサル		1 セッション		
	ネゴシエーション方向限定		both、initiator、responder		
IPsec	モード		トンネルモード		
	セキュリティプロトコル		ESP		
	サポート アルゴリズム	暗号化	3DES、AES-128、AES-192、AES-256、NULL		
		認証	HMAC-MD5-96、HMAC-SHA-1-96、HMAC-SHA-2-256-128		

	PFS		768bit(group1)、1024bit(group2)、1536bit(group5)、2048bit(group14)、無効	
	フラグメント方式		post-fragment	送信
				受信
			pre-fragment	送信
				受信
	SA	IPsec ID 認証	local-id/remote-id(IPv4 アドレス指定、IPv4 プリフィックス指定)	
		ライフタイム	時間設定、データ量設定	
		リキータイミング	残り時間指定	
IPsec 拡張	IPsec SA 削除		手動削除	
			delete payload 受信時の IPsec SA 削除	
			IPsec SA 削除時の delete payload 送信	
	DF ビット制御		AUTO(DF ビットを引き継ぐ)	
	TCP MSS 書き換え		固定、AUTO	
	アンチリプレイ防御		可能	
	IPsec 適用 ACL 設定（IP フィルタ）		Static、Dynamic	
その他	NAT/NAPT 同時動作		IPsec と NAT/NAPT による外部接続の同時動作可能	
	VPN パススルー		1 セッション(静的 NAPT 方式)	

[メモ]

IPsec のリモート ID と静的ルーティング設定の優先順位は次のとおりです。

IKE Phase2 のリモート ID を登録すると、自動で静的ルートを登録します。このルートは、通常の静的ルートより優先されます。IKE Phase2 のローカル ID に対するルートは、自動で静的ルートが登録されないので、IPv4 ルーティング設定を追加する必要があります。

※上記は IKEv1 についてですが、IKEv2 の IKE_AUTH 交換設定ローカルトラフィックセレクタ、リモートトラフィックセレクタについても同様となります。

[制限事項]

・複数サブネット対応状況は次のとおりです。

アグレッシブモード の responder でオンデマンド接続の場合、リモート ID に複数サブネットを指定できません。

3.7. **無線 LAN 機能**

本製品は、アクセスポイントとして動作します。

本製品は、IEEE802.11b/g/n(2.4GHz 帯)に対応しています。

アンテナは、内蔵アンテナと外付けアンテナがあり、どちらのアンテナで動作させるかを設定 Web で切り替えます。(初期値:内蔵アンテナ)

外付けアンテナはオプション品です。外付けアンテナ取り付け時の設定は 4.3 章を参照してください。

- SSID および暗号化キーはファームウェアバージョン 3.5.12 にて初期値を削除しました。
  SSID および暗号化キーを初期値のままで無線 LAN 機能を使用している場合は変更することをお勧めします。
  SSID および暗号化キーは必ず管理者自身が作成したものを使用してください。
  暗号化キーは複雑で長い文字列にして、安全性を高めることをお勧めします。
- ファームウェアバージョン 3.5.9 以前を使用中で、ファームウェアバージョン 3.5.12 以降に更新する場合、以下の条件で SSID および暗号化キーの設定値を引継ぎます。
  ・以下のいずれか、または、両方の条件を満たしている場合
  (a) 無線 LAN 機能を有効にしている
  (b) SSID および暗号化キーを初期値から変更している・

[メモ]

- ファームウェア更新後に初期化を行うとこれまでの SSID および暗号化キーの設定値は削除されます。

3.7.1. **無線 LAN**

無線主要機能一覧は以下の表のとおりです。

機能	説明	備考
マルチ SSID	SSID×2	
ESS-ID ステルス	有効/無効切り替え	
無線チャネル	1~13ch、自動選択	
デュアルチャネル	有効/無効切り替え	
暗号化方式	WPA-PSK（TKIP） WPA-PSK（AES） WPA2-PSK（TKIP） WPA2-PSK（AES） WPA/WPA2-PSK（TKIP） WPA/WPA2-PSK（AES） 802.1x（EAP）	
ネットワーク分離	有効/無効切り替え	ルータモードのみ設定可能です。
無線 LAN 端末接続台数	32 台以下推奨	無線 LAN 端末接続台数ならびにスループットについては、電波状態や建物の構造、製品の設置位置、クライアントの無線 LAN のアンテナ性能などで変わります。

[SSID]

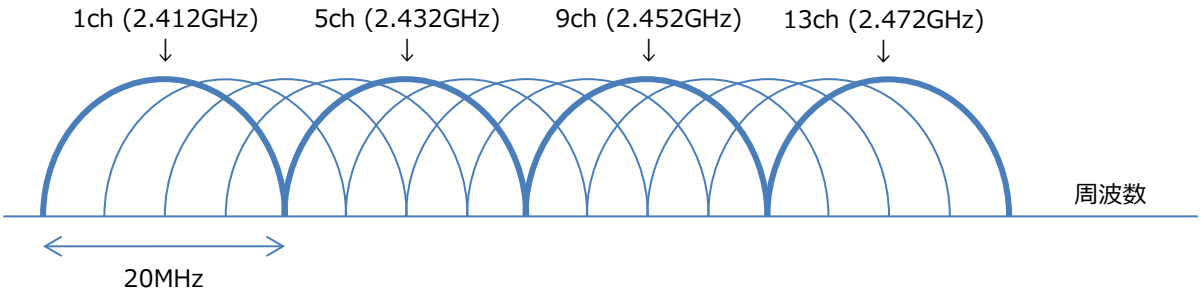
プライマリ SSID、セカンダリ SSID の 2 つの SSID を利用できます。

- SSID 名を設定 Web で変更できます。(初期値は未設定)
- ESS-ID ステルス機能は、本製品が送出するビーコンに SSID 情報を含めないことによって、本製品へのアクセスに関するセキュリティを高める機能です。

[無線チャネル]

無線チャネルとして、IEEE802.11b、IEEE802.11g ともに 1ch~13ch を使用できます。

■IEEE802.11g の場合



本製品が使用するチャネルの指定には、次の 2 とおりの方法があります。

No	方式	ch 選択範囲
1	本製品の無線 LAN 機能動作開始時、周囲のアクセスポイントを検出し、電波状態の良いチャネルを自動選択する	1ch~11ch の間で、電波状況の良いチャネルを自動選択
2	お客様が使用するチャネルを選択する	1ch~13ch の間で、任意のチャネルを選択 ※ただし、ご使用になる Wi-Fi 機器（スマートフォン、パソコン等）によっては、12ch 及び、13ch が使用できない場合があります。この場合は、本製品のチャネルを 11ch 以下に固定してください。

本製品は、無線 LAN 通信で利用する通信チャネルを 20MHz 幅から 40MHz 幅に拡大することで、約 2 倍の通信速度を実現するデュアルチャネル機能と呼ぶ機能を有しています。

本製品のデュアルチャネル機能を有効にした場合、次のチャネルを選択します。

制御チャネル	拡張チャネル
1	5
2	6
3	7
4	8
5	1
6	2
7	3
8	4
9	5

10	6
11	7
12	8
13	9

[暗号化方式]

本製品でサポートしている暗号化方式は次のとおりです。

WPA-PSK(TKIP)，WPA-PSK(AES)，WPA2-PSK(TKIP)，WPA2-PSK(AES)，WPA/WPA2-PSK(TKIP)，WPA/WPA2-PSK(AES)，802.1x（EAP）

他に「暗号化無効」を選択できます。

[ネットワーク分離]

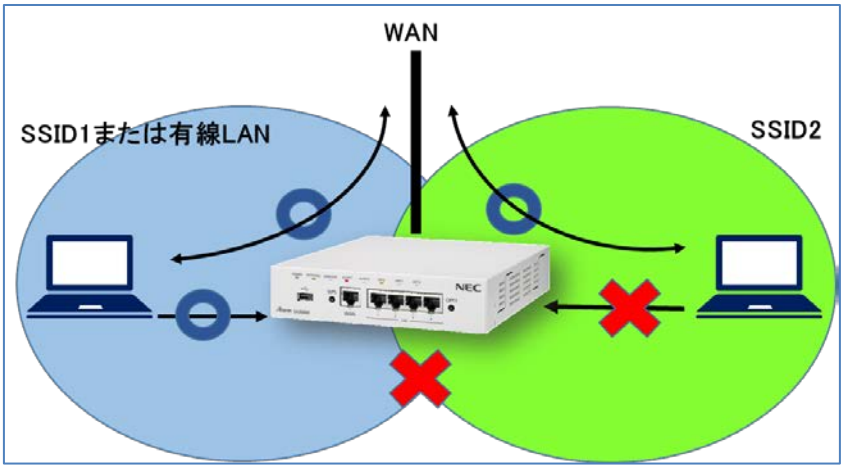
ネットワーク分離機能はマルチ SSID のそれぞれのネットワーク（SSID1/SSID2）に接続している端末や、有線で接続した端末へのアクセスを制限し、本製品に接続した他のネットワークから分離する機能です。なお、WAN 側が分離されることはありません。

ネットワーク分離機能はルータモードで使用できます。ブリッジモードではサポートしておりません。

SSID 2 のネットワーク分離機能を有効にすることで、次のネットワークを構築できます。

・SSID1、有線 LAN に接続している端末から SSID2 の端末にアクセスできます。インターネットおよび本製品の設定 Web にアクセス可能です。

・SSID2 から SSID1、有線 LAN の端末にアクセスできません。SSID2 から本製品の設定 Web にもアクセスできません。インターネットへのアクセスは可能です。



3.7.2. **WPS**

WPS-PBC（Wi-Fi Protected Setup-Push Button Configuration）に対応しています。

本製品前面の WPS スイッチを使用して、WPS-PBC に対応した無線 LAN 端末と Wi-Fi の自動設定を行うことができます。

設定 Web から WPS 機能の有効/無効の設定ができます。

なお、以下の状態のときには WPS 機能はご使用になれません。

・無線 LAN 機能が無効

・無線の MAC アドレスフィルタリング機能が有効

・プライマリ SSID の無線暗号化モードを TKIP、または、802.1x（EAP）に設定している

・プライマリ SSID の ESS-ID ステルス機能が有効

3.8. **USB ストレージ機能**

本章の内容は、ブリッジモード、およびルータモード共通の仕様です。

USB ポートに USB ストレージを接続することで、装置に保存された設定値の定期的な保存、設定 Web での設定保存時の保存、および設定値の復元が行えます。接続する USB ストレージが以下の動作条件を満たしている必要があります。

USB ストレージは別売（当社オプションではありません）です。

操作手順については、3.8.1 章、3.8.2 章を参照してください。

[USB ストレージの動作条件]

- USB マスストレージクラスに対応している
- FAT32 でフォーマットされている
- 1 つのパーティションのみである
- ボリュームサイズが 2TB を超えていない
- 暗号化機能がない
- 空き容量が 20MB 以上である

[動作確認済み USB ストレージ]

以下の SA3500G 製品 HP の「動作確認済み USB ストレージ」の項を参照してください。

https://www.necplatforms.co.jp/product/security_ap/function.html

[メモ]

- USB ストレージを本装置の USB ポートに接続すると、OPT2 ランプが橙点灯します。
  ※橙点灯しない場合は、[USB ストレージの動作条件]を確認してください。
- 設定値の保存、および設定値の復元に成功すると、OPT2 ランプが緑点灯します。
  ※緑点灯しない場合は、[USB ストレージの動作条件]を確認してください。
- 上記以外の OPT2 ランプの表示については 2.3.3 章を参照してください。
- USB ハブはご利用できません。

[ご注意]

- 規格外の USB デバイスを接続した場合、装置破損の恐れがありますので、ご注意ください。
- USB ストレージを取り付ける場合は、以下のことにご注意ください。
  ・必ず本製品の本体を押さえて取り付けてください。
  ・コネクタ部分に手を触れないようにしてください。
  ・コネクタの向きに注意して、無理に押し込まないようにしてください。

3.8.1. **設定値の保存**

動作条件を満たした USB ストレージが USB ポートに接続されている場合、次のタイミングで設定値を USB ストレージに自動保存します。バックアップ用のファイルと合わせて、2 つのファイルを保存します。
設定 Web から機能の有効/無効の設定ができます。設定については、5.6.14 章を参照してください。

[保存タイミング]

- 日付変更時(毎日 0 時 0 分)
- 設定 Web での設定保存時

[保存ファイル名]

- SA3500G_config.bin
- SA3500G_config.bin.bak　…バックアップ用

※USB ストレージの直下に保存します。

[USB ストレージへの保存手順]

1.「USB ストレージへの設定値の保存機能設定」を「有効」にします。(5.6.14 章参照)
2. USB ストレージを本装置の USB ポートに接続すると、OPT2 ランプが橙点灯します。
3. 設定値の「保存ボタン 保存 」を押下します。
4. USB ストレージに設定値が保存されます。
5. 設定値の保存に成功すると OPT2 ランプが緑点灯します。

※OPT2 ランプが緑点灯しない場合は、[USB ストレージの動作条件](3.8 章参照)などを確認してください。

[メモ]

- USB ストレージに保存された設定値を Windows パソコンなどで開く場合、ファイルの時刻情報は UTC となります。
- USB ストレージに保存できるのは、本製品の設定値のみです。
- 設定値には、設定 Web から設定した情報がすべて含まれます。

[ご注意]

- USB ストレージへの保存中は POWER ランプが橙点滅します。この場合は、USB ストレージを本製品から取り外したり、本製品の電源を OFF にしたりしないでください。アクセス中のデータが壊れる可能性があります。
- 同名のファイルが存在する場合、ファイルを上書きします。

3.8.2. **設定値の復元**

以下の条件を満たした状態で本製品を起動したとき、USB ポートに接続されている USB ストレージから設定値を復元して本製品が起動します。

[復元の条件]

- 初期化操作後の装置起動である
- USB ストレージの直下に設定値（SA3500G_config.bin または SA3500G_config.bin.bak）が保存されている
- 復元装置のファームウェアバージョンが、設定値を保存した装置のファームウェアバージョンと同一、もしくは、新しいバージョンである

[USB ストレージからの復元手順]

■初期化された装置に復元する場合

1. 本製品の電源を OFF にします。
2. USB ポートに設定値が保存された USB ストレージを接続します。
3. 本製品の電源を ON にします。
4. 装置起動時に USB ストレージから設定値が復元されます。
5. 設定値の復元に成功すると OPT2 ランプが緑点灯します。

■初期化されていない装置に復元する場合

1. 設定値が保存された USB ストレージを本装置の USB ポートに接続すると OPT2 ランプが橙点灯します。
2. 本製品の設定値を初期化します。(5.6.15 章参照)
3. 初期化後の装置起動時に USB ストレージの設定値が復元されます。
4. 設定値の復元に成功すると OPT2 ランプが緑点灯します。

※OPT2 ランプが緑点灯しない場合は、[復元の条件]、および、[USB ストレージの動作条件](3.8 章参照)を確認してください。

[ご注意]

- 設定値が保存されている USB ストレージを接続した状態で本製品を初期化した場合、本製品の再起動後に USB ストレージから設定値が復元されます。本製品を初期化する場合は USB ストレージを取り外してから行ってください。
- 復元装置のファームウェアバージョンより新しいバージョンのファームウェアの装置において保存した設定値は復元できません。

3.9. **その他の機能**

本章の内容は、ブリッジモード、およびルータモード共通の仕様です。

3.9.1. **トラフィック転送制限**

本製品は、下記のすべての条件を満たした場合にブリッジングまたはルーティング動作します。（参考：3.3.4 章）

- アクティベーションが成功しているとき
- ライセンスが有効期限内と確認されているとき [15]

[メモ]

設定により、ライセンス満了の際でもブリッジングまたはルーティング動作させることができます。

セキュリティ・スキャン設定の基本設定でパケット転送設定を有効にすることで、この制限を解除できます。設定方法は 5.8.2 章を参照してください。

また、本製品は TCP のハンドシェークが確認できない場合には、当該 TCP ストリームのパケットを廃棄する動作をします。この TCP ストリームを厳格にチェックする機能を解除する設定は、5.8.2 章を参照してください。

3.9.2. **MAC ラーニング**

MAC アドレスのラーニングテーブルのエージングタイマは 300 秒です。

MAC アドレスのラーニングテーブルを最大 256 エントリ管理します。

インタフェースのリンクダウンでは、該当する MAC ラーニングエントリを削除しません。

3.9.3. **PAUSE 機能**

IEEE802.3X PAUSE 機能に対応しています。

本機能の有効/無効を切り替えることができます。5.6.8 章を参照してください。

[動作インタフェース]

WAN インタフェース、LAN インタフェース

[対応モード]

symmetric mode

[15] 本製品は、装置起動のたびにライセンスを確認します。（3.3.4 章参照）

4. 設置

4.1. 設置

本章では、本製品の設置条件について説明します。

4.1.1. 環境条件

動作保証環境は次のとおりです。

温度：0~40℃

湿度：10~90%（結露しないこと）

4.1.2. 設置場所

設置する前に以下の章の警告事項、注意事項を必ずお読みください。

- 1.12 章 安全にお使いいただくために
- 1.13 章 本製品の故障を防ぐために

[設置スペース]

本製品は、本製品の周囲約 7cm 以内にパソコンや壁などのものがない場所に設置してください。

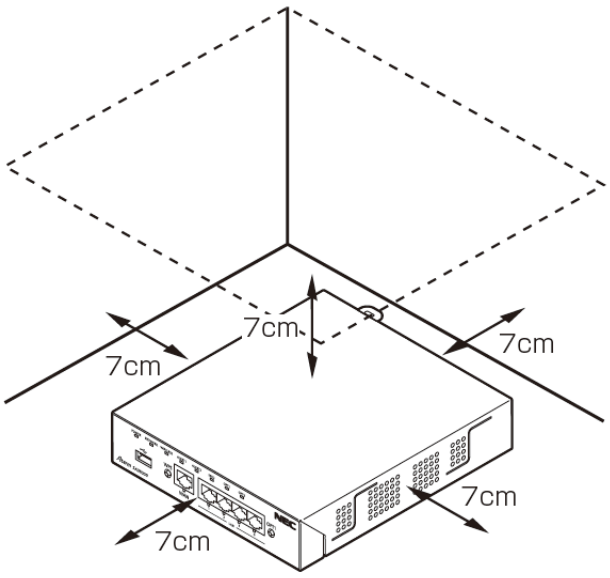
（底面は除きます。また、壁掛けの場合は壁掛け面を除きます。）

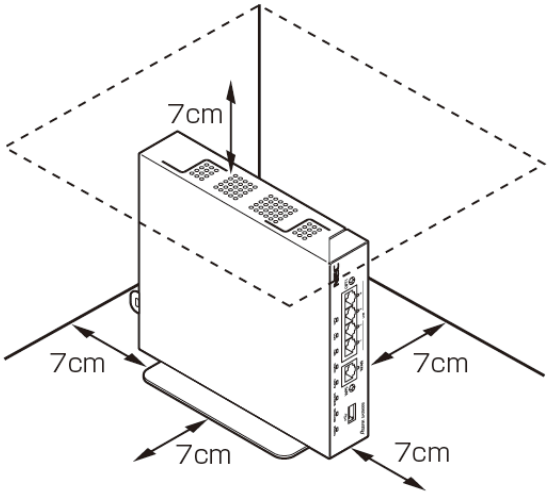
[警告]

- 本製品を落とさないでください。落下によって故障の原因となったり、そのまま使用すると火災、感電の原因となることがあります。万一、本製品を落としたり破損した場合は、すぐに本製品のACアダプタをコンセントから抜いて、お問い合わせ先にご連絡ください。

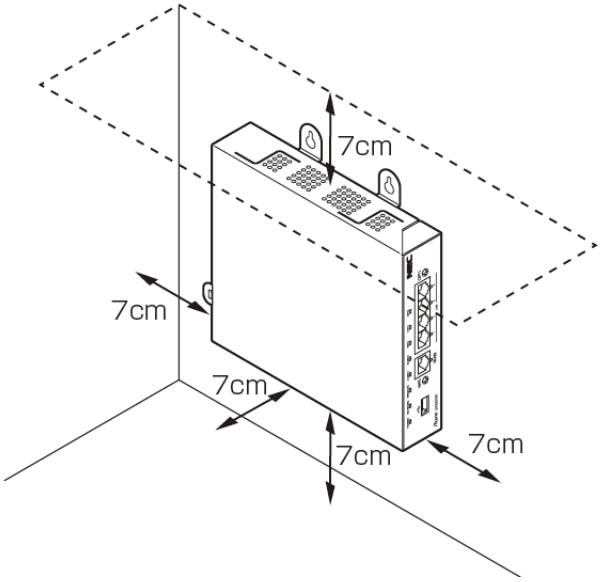
[注意]

- 大きな衝撃や振動などが加わる場所には設置しないでください。また、垂直面以外の壁や天井などには設置しないでください。振動などで落下し、故障、けがの原因となります。
- ベニヤ板などのやわらかい壁には設置しないでください。確実に固定できる場所に設置してください。ネジが外れ落下し、故障、けがの原因となります。
- 壁掛け設置されている状態で、本製品にケーブルを接続したり、スイッチの操作などを行う際には、必ず本製品を手で支えながら行ってください。落下すると、故障、けがの原因となります。
- 通風孔をふさがないでください。通風孔をふさぐと、内部に熱がこもり、火災の原因となることがあります。





（壁掛けの場合）



[警告]

AC アダプタを接続および設置する際は、以下のことにご注意ください。

- AC アダプタおよび電源コードは、必ず本製品に添付のものをお使いください。また、本製品に添付のAC アダプタおよび電源コードは、他の製品に使用しないでください。
- 本製品に添付のAC アダプタおよび電源コードは、必ず一体で使用し、他のAC アダプタや電源コードを組み合わせて使用しないでください。
- 風通しの悪い場所に設置しないでください。
- AC アダプタにものをのせたり布を掛けたりしないでください。
- AC アダプタ本体が宙吊りにならないよう設置してください。
- たこ足配線にしないでください。

[注意]

- 無線の内蔵アンテナは、筐体の側面にある 形のスリット部になります。この周辺にものを置かないでください。
- 外付けアンテナを使用する場合は、外付けアンテナが壁に接触しないように設置してください。
- 狭い場所や壁などに近づけて設置しないでください。内部に熱がこもり、破損したり火災の原因となることがあります。
- 本製品の上にものを置いたり、重ね置きはしないでください。

4.1.3. 設置手順

[開梱手順]

1. 開梱します。
2. 構成品が揃っていることを確認します。
   ・構成品は、2.4 章を参考にしてください。
3. 構成品が損傷していないことを確認します。
4. 製品本体の装置ラベル内容と梱包箱のラベル内容が一致していることを確認します。
   ・装置ラベルは、2.3.4 章を参考にしてください。

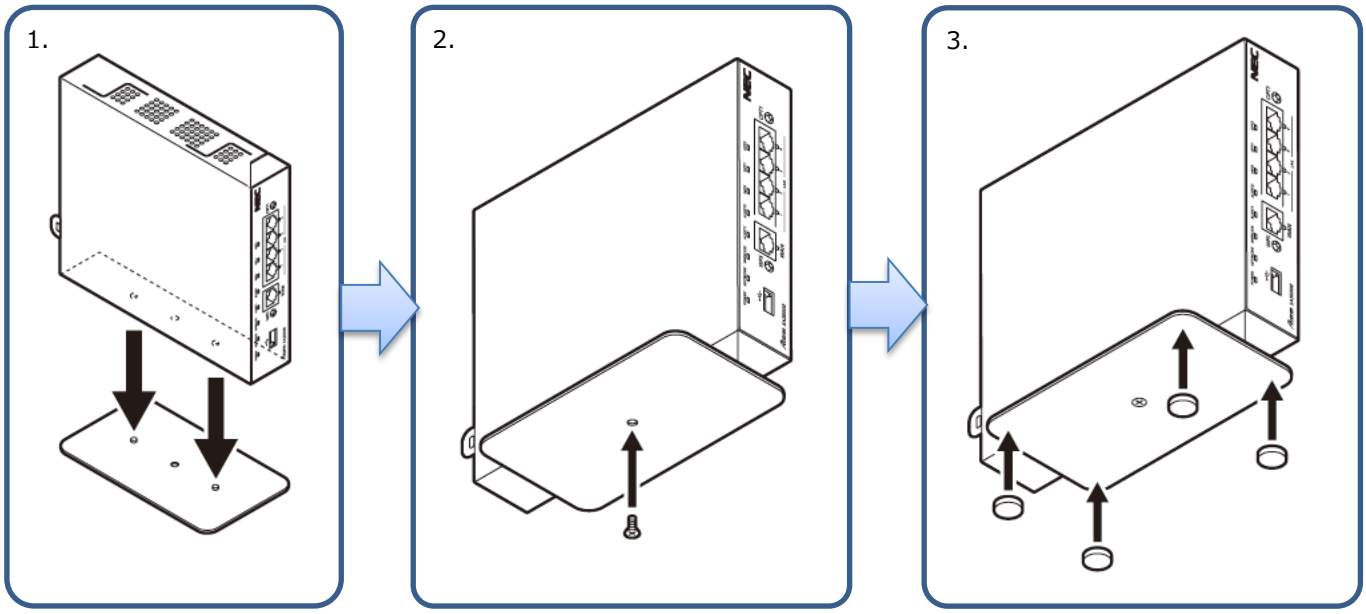
[設置手順]

■準備

プラスドライバーを用意してください。

■縦置きの場合

1. スタンド（添付品）を本体側面に差し込みます。
   スタンドの凸部を本体側面のスタンド用取り付け穴に差し込みます。
2. スタンドと本体側面をスタンド固定ネジ（添付品）で固定します。
3. ゴム足（添付品）をスタンド裏面に貼り付けます。

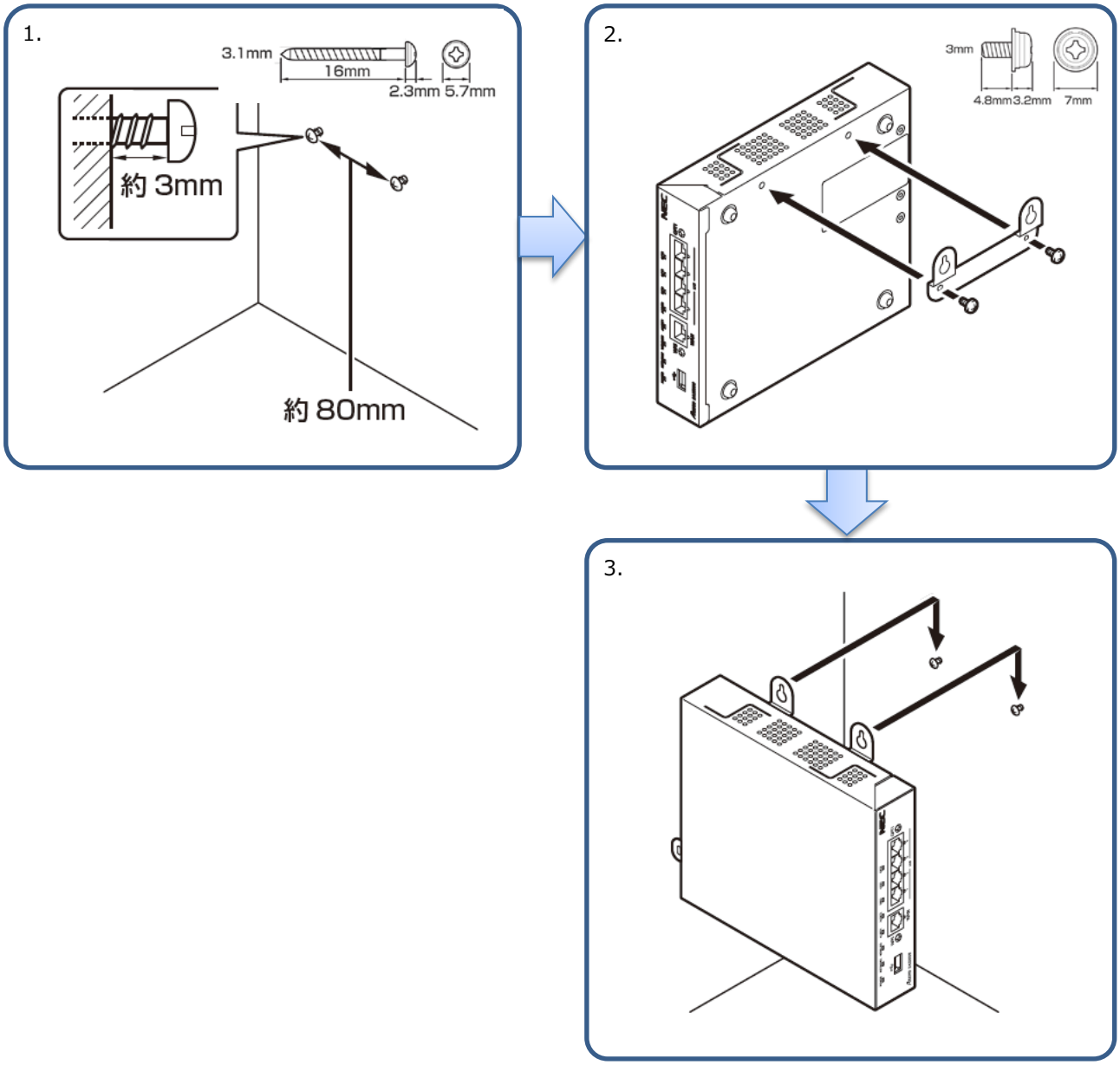


[注意]

- ゴム足は設置のための仮固定用であり、固定を保証するものではありません。過度の荷重を加えたり、ケーブルを引っ張ったりした場合に設置した床から離脱する恐れがあります。
- ほこり・ゴミなどがゴム足に付着すると床への密着強度が減少します。その場合には中性洗剤や水にてほこり・ゴミなどを洗い流してください。洗浄にて密着強度が増します。洗浄の際には、スタンドを本体から取り外してください。
- 添付のゴム足をご使用にならない場合には、お子様の手の届かない場所に保管してください。誤って飲み込んだ場合には医師の診断を受けてください。

■壁掛けの場合

1. 本体を取り付ける位置を決め、木ネジを壁の 2 箇所（80mm 離します）に水平に取り付けます。
   木ネジは最後まで締め込まず、壁から約 3mm 出るように取り付けてください。
2. 本体底面の壁掛け金具用取り付け穴に壁掛け金具を合わせ、壁掛け金具固定ネジで固定します。
3. 壁に取り付けた木ネジに本体の壁掛け金具を取り付けます。



[注意]

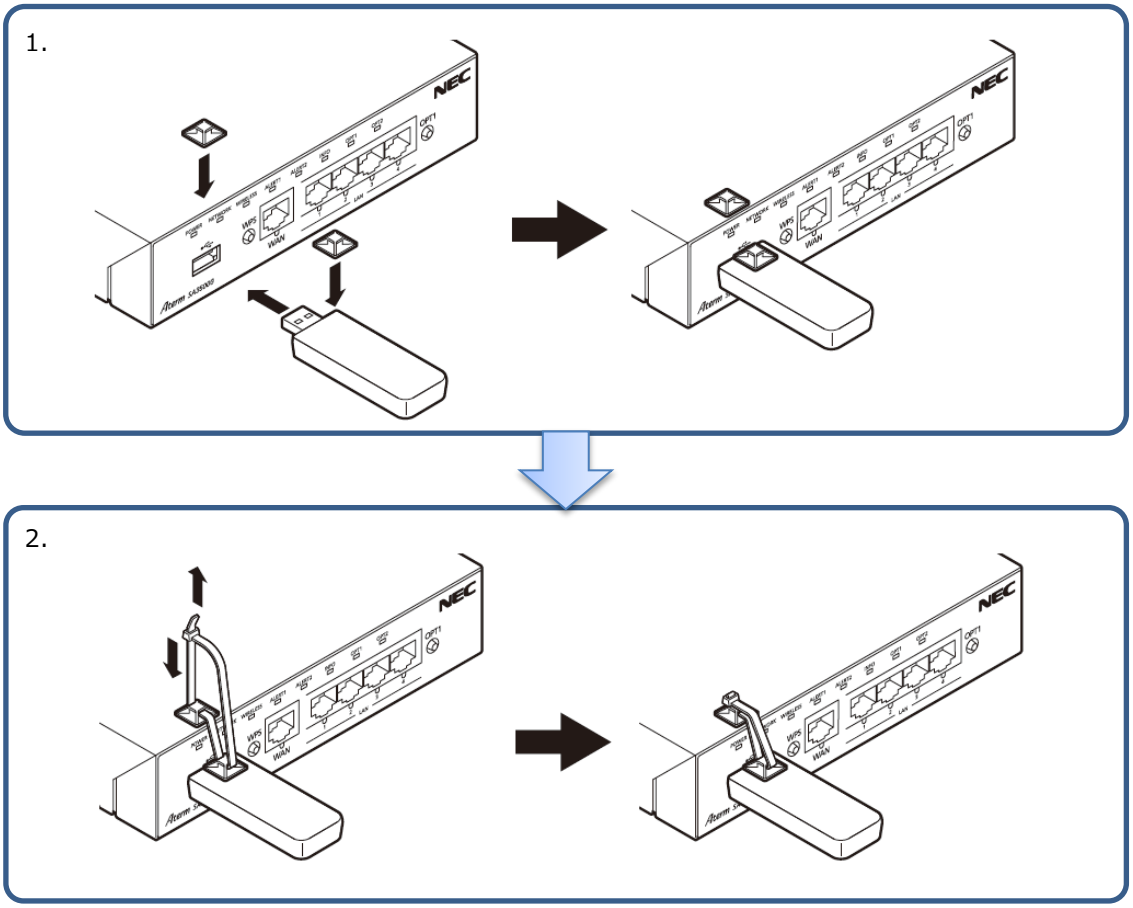
- 壁掛け時には落下すると危険ですので、大きな衝撃や振動などが加わる場所には設置しないでください。
- 本製品が落下すると危険ですので、ベニヤ板などのやわらかい壁への壁掛け設置は避け、確実に固定できる場所に設置してください。また、衝撃や振動を加えないでください。
- 本製品は垂直面以外の壁や天井などには取り付けないでください。振動などで落下し、故障、けがの原因となります。
- 壁掛け設置の状態で、ケーブルの接続やスイッチを操作する場合は、落下の危険がありますので、必ず本製品本体を手で支えながら作業してください。

4.2. **USB ストレージの固定**

本製品の USB ポートから USB ストレージが簡単に抜けないようにするため、USB クランプキット（品番：ZA-SA/UC1）をオプション（別売）として用意しています。

ケーブルバンドを一度使用すると、取り外すにはニッパーなどで切断する必要があります。
固定具とケーブルバンドによる固定は、USBストレージが動作できることを確認したあとにご使用ください。

1. USB 抜け防止用固定具を USB ストレージと本製品天面にそれぞれ貼り付けます。
   ※USB ストレージに貼り付ける USB 抜け防止用固定具の向きに注意してください。
   ※USB ストレージの形状によっては、USB 抜け防止用固定具を貼り付けられない場合があります。
2. USB 抜け防止用ケーブルバンドを取り付けます。
   ※USB 抜け防止用ケーブルバンドを強く引っ張ると、USB コネクタ周辺の破損や、USB 抜け防止用固定具が剥がれることがあります。
   ※USB 抜け防止用ケーブルの締め付け後、ケーブルバンドの余丁部分をニッパーなどで切り取ってください。



※USB ストレージを取り外す際は、必ずニッパーなどで USB 抜け防止用ケーブルバンドを切断してから USB ストレージを取り外してください。

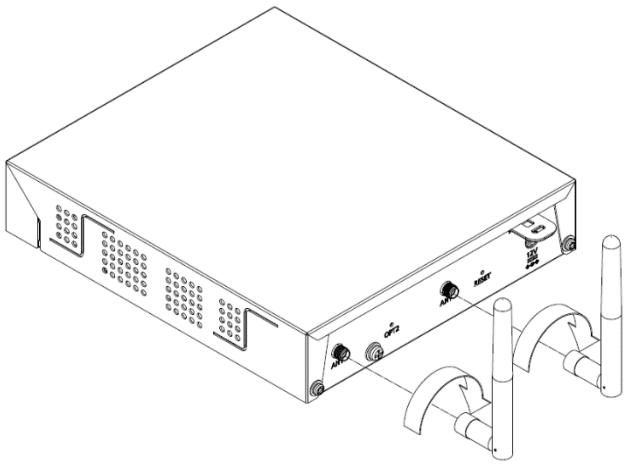
4.3. **外付けアンテナの取り付け**

本製品の無線 LAN 機能は、外付けアンテナ（品番：ZA-SA/AN1）をオプションとして用意しています。無線 LAN 機能は本製品の内蔵アンテナでも利用できますが、外付けアンテナを取り付けることで、無線 LAN 機能の速度や飛距離の向上を見込めます。

1. 外付けアンテナ（2 本）を本製品のアンテナコネクタ（2 箇所）に取り付けます。
   外付けアンテナは接続部分を本製品のアンテナコネクタに挿入し、指でアンテナ接続部分（滑り止めが付いたアンテナ根元部分）を矢印の方向に回して固定してください。
   ※ 外付けアンテナを本製品に取り付け後、アンテナを矢印と反対方向に回すと、外付けアンテナの接続が緩んで通信不良が発生する原因となります。外付けアンテナと本製品の接続が緩んでいないことを確認して使用してください。
   ※ オプションの外付けアンテナ（品番：ZA-SA/AN1）以外は、使用しないでください。
   ※ 外付けアンテナは 2 本 1 組です。必ず 2 本とも接続するようにしてください。
2. 外付けアンテナの角度を調整します。外付けアンテナの最適な角度は、お客様のネットワークにより異なります。設置場所、無線 LAN 速度、飛距離などの状況を見ながら調整してください。
   ※ 外付けアンテナを 90°以上傾けると、アンテナ内部のケーブルが切断して通信不良が発生する原因となりますので、無理に傾けないでください。
   ※ 外付けアンテナは回転するようになっています。十分な通信特性を得るために 2 本のアンテナが交差しないように設置してください。
   ※ アンテナは金属などの導電性のものから離して設置してください。感度低下の原因となります。
3. 工場出荷時の設定（初期値）は、内蔵アンテナを使用となっています。外付けアンテナを取り付けた場合は、設定 Web で、アンテナの設定を”内蔵アンテナ”から”外付けアンテナ”へ切り替えてください。

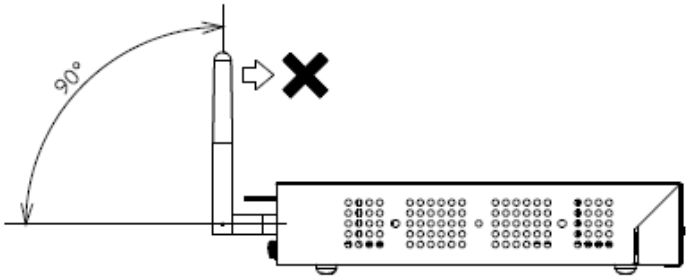
※ 落下などで外付けアンテナが破損した場合、速やかに外付けアンテナを交換するか、外付けアンテナを外して、アンテナの設定を“内蔵アンテナ”に切り替えてください

アンテナの取り付け



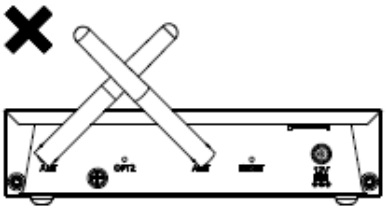
禁止事項 1.

外付けアンテナを 90°以上に傾けないでください。



禁止事項 2.

外付けアンテナを交差しないでください。*

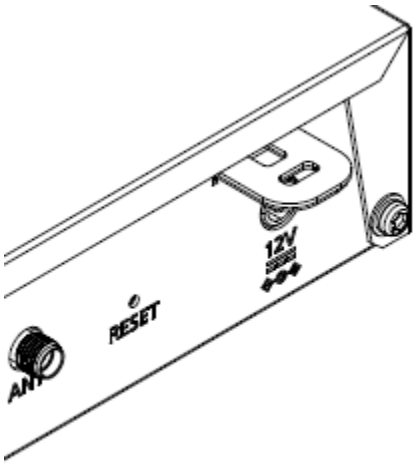


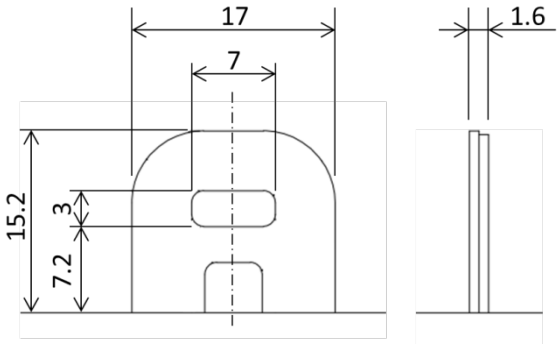
4.4. 盗難防止フックの使用方法

盗難防止フックは盗難防止用の鍵取り付け穴です。市販のセキュリティワイヤ※を取り付けることで、本製品を盗難から守ります。

※ セキュリティワイヤの鍵の形状によっては、盗難防止フックに入らない場合があります。セキュリティワイヤの選定では、鍵の形状にご注意ください。

盗難防止フック穴サイズ：7(W) x 3(D) x 1.6(H)mm



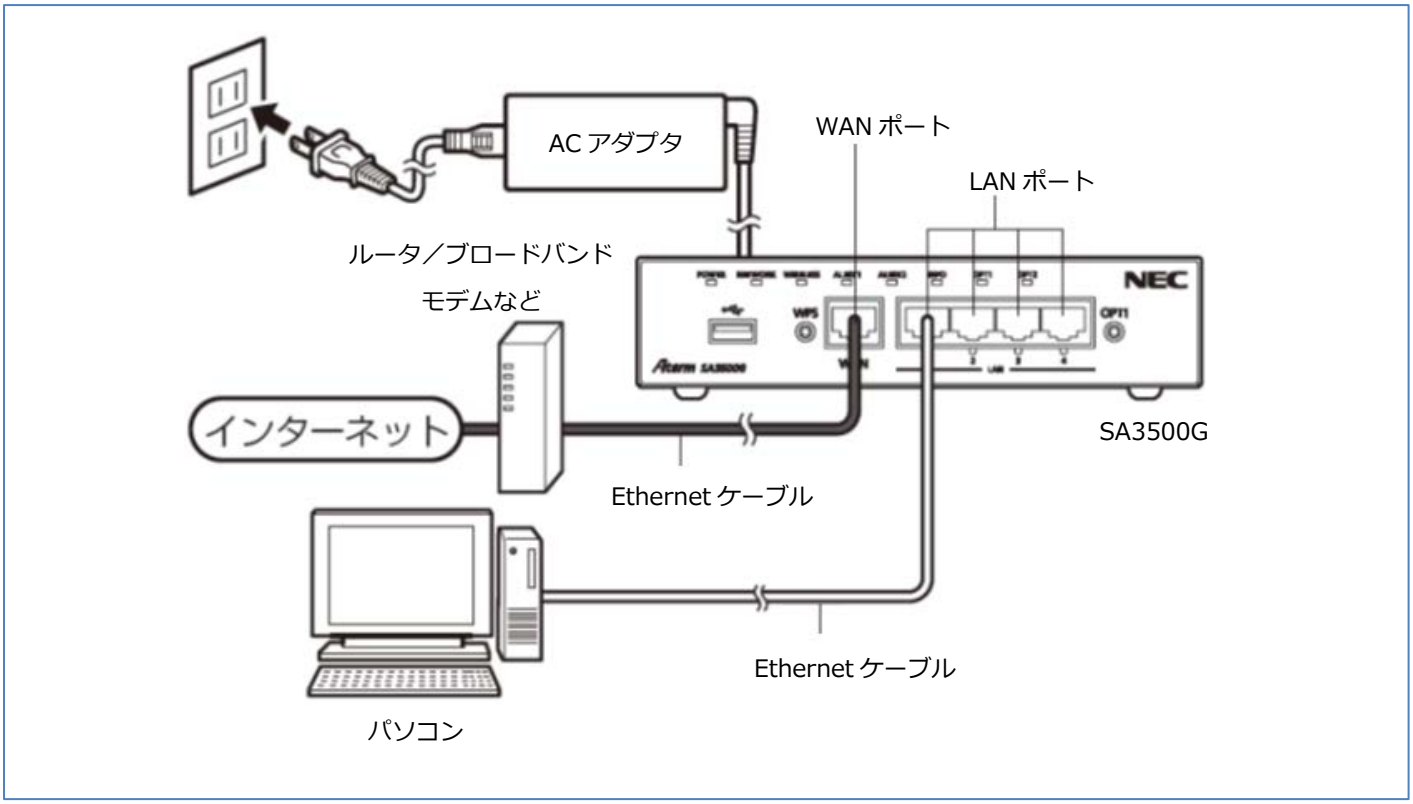


4.5. **ケーブルの接続**

ケーブル類は、下記のイメージで接続します。

お客様の環境によっては、SA3500G の設置場所が変わります。8.1 章に接続例を載せています。

また、SA3500G の WAN ポートにルータ／ブロードバンドモデムなどの上位機器を接続する場合は、上位機器が SA3500G からの必須の TCP/UDP パケットを通過できるようにしていただく必要があります。詳細は 3.2 章 動作可能なネットワークを参照してください。



1. 本製品の WAN ポート/LAN ポートと各種ネットワーク機器を Ethernet ケーブル（カテゴリ 5e 以上）で接続します。
   ※Ethernet ケーブルはお客様で用意してください。
2. パソコンなどを接続します。
3. AC アダプタと電源コードを接続し、AC アダプタを本製品の AC アダプタ接続コネクタに接続します。
4. 電源コードを電源コンセントに接続します。

本製品の起動中、起動後は、本製品の POWER ランプが緑点灯します。

5. 設定/設定内容確認

本製品は、設定 Web で設定します。

[本製品の設定画面]

本製品の設定画面は、大きく分けて 3 つのパートからなります。

- 本製品のネットワークに関する設定
  ・ブリッジモード
  ・ルータモード
- セキュリティ・スキャン機能に関する設定
- 構成管理機能に関する設定

他に初回装置起動時（または初期化後の装置起動時）のみ、初期設定のためのウィザードが実行されます。

ウィザードの動作モード選択とは、本製品をブリッジモードで動作させるか、ルータモードで動作させるかの選択です。

モードは、ウィザード実行時以外でも変更できます。

[動作確認済み Web ブラウザ]

下記 OS の Web ブラウザの動作を確認済みです。

OS	Web ブラウザのバージョン	備考
Windows 8.1	Internet Explorer 11 Google Chrome 85	
Windows 10	Internet Explorer 11 Google Chrome 85 Microsoft Edge 85	
OS X v10.14.1	Safari 13	

[メモ]

本製品を設定する際、設定に使用するパソコンの IP アドレスを特定の IP アドレスに設定する必要があります。（5.2 章を参照してください）

設定終了後は、元の設定に戻してください。

設定 Web を利用する際は、JavaScript を有効にする必要があります。

5.1. **アカウント**

設定 Web のログインアカウントは次のとおりです。

種別	説明	ID	パスワード
ユーザー用アカウント	お客様が通常アクセスする Web 画面です。	admin	初期値なし （ユーザーが設定）

5.2. 初回起動時設定フロー

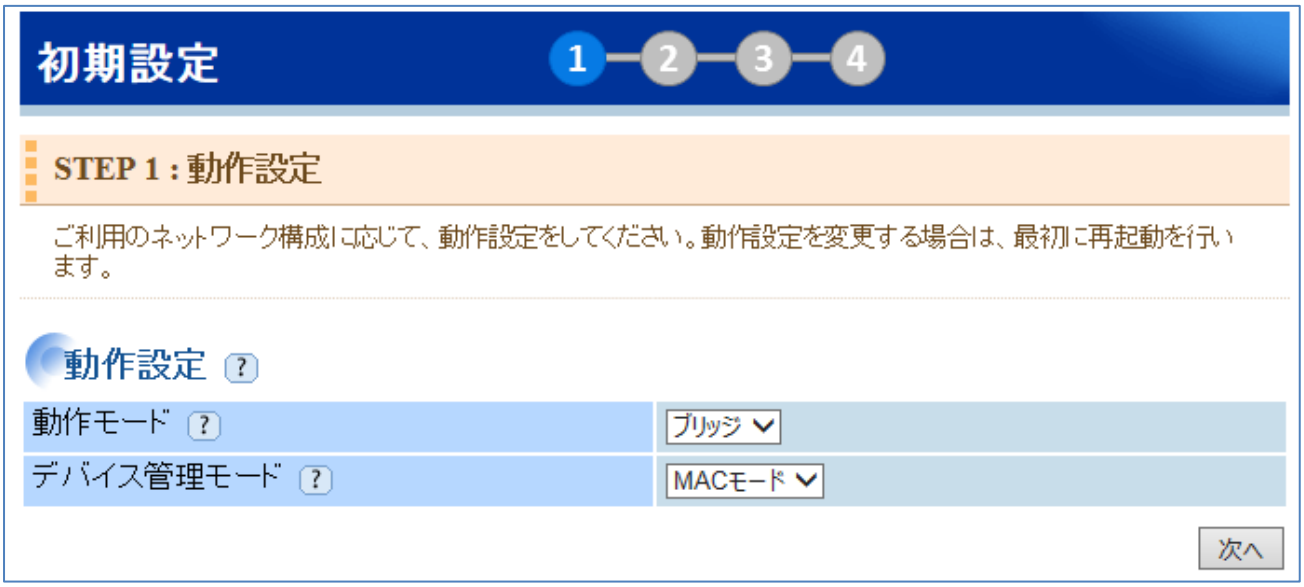
初回装置起動時は、次の操作が必要です。

- モード選択（ウィザードが動作します）
  - ・ブリッジモード（5.2.1 章参照）
  - ・ルータモード（5.2.2 章参照）
- アクティベーション操作（5.2.3 章参照）

5.2.1. ブリッジモードで動作させる場合

次の手順で設定します。

1. 本製品に各種ケーブルを接続します。（4.5 章を参照してください。）
2. 本製品を設定するパソコンの IP アドレスを 169.254.xxx.xxx/16 に設定します。
   （xxx は 1~254 の任意の整数です。169.254.254.11 以外の IP アドレスを設定してください。）
3. パソコンの Web ブラウザを開き、http://169.254.254.11/もしくは https://169.254.254.11/にアクセスします。
4. 設定ウィザードが開きます。
   STEP1 → STEP2 → STEP3→ STEP4 の順で設定してください。
5. **STEP1:** 動作モードと本製品が管理するデバイスの管理モードを選択します
   ブリッジモードを選択します。デバイス管理モードは Aspire や IX ルータなどとの連携機能をお使いでなければ初期値の MAC モードのままで構いません。



6. **STEP2:** 管理者パスワードを設定します。

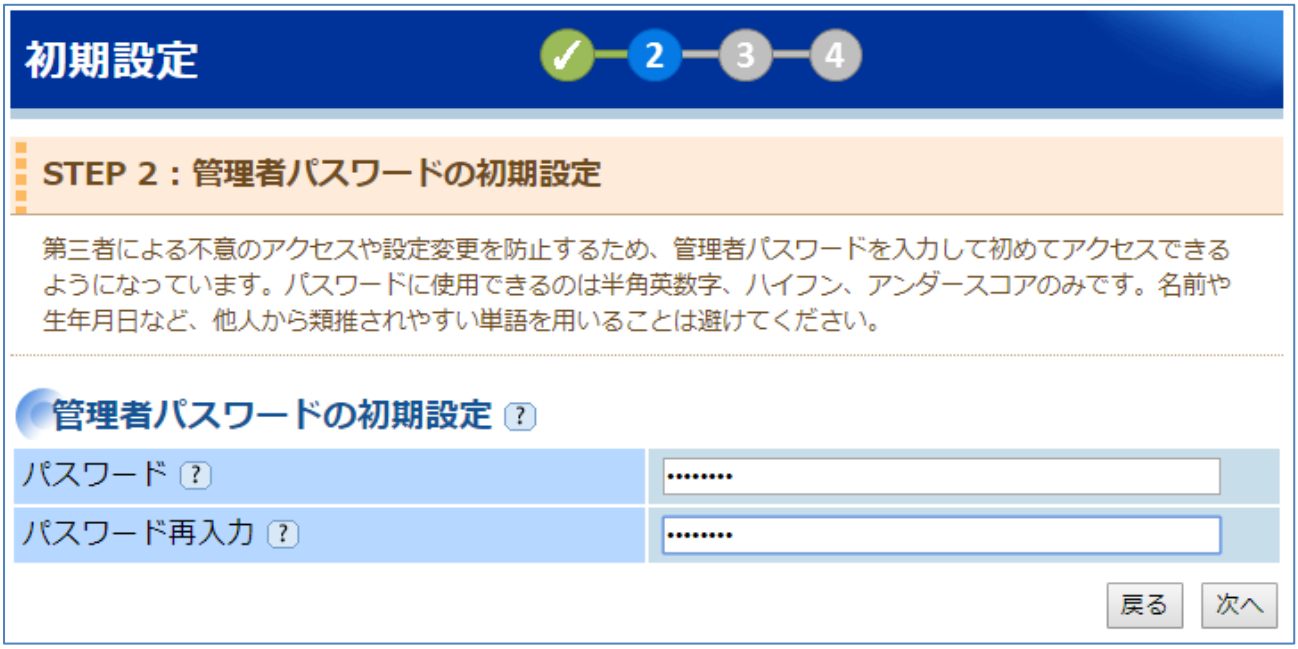
パスワードに使用できる文字は、半角文字 0～9,a～z,A～Z,-(ハイフン),_(アンダースコア)です。

入力可能文字数は、1～64 です。

※パスワードは複雑で長い文字列にして、安全性を高めることをお勧めします。

※管理者パスワードは、本製品を設定する場合に必要となりますので、控えておいてください。忘れた場合は、設定画面を開くことができず、本製品を初期化してすべての設定がやり直しになります。(5.6.15章参照)

※ここで設定したパスワードは、STEP4 の「設定完了」ボタン押下で FlashROM に保存します



※デバイス管理モードを IP モードに変更して再起動した場合、「戻る」ボタンは表示されません。

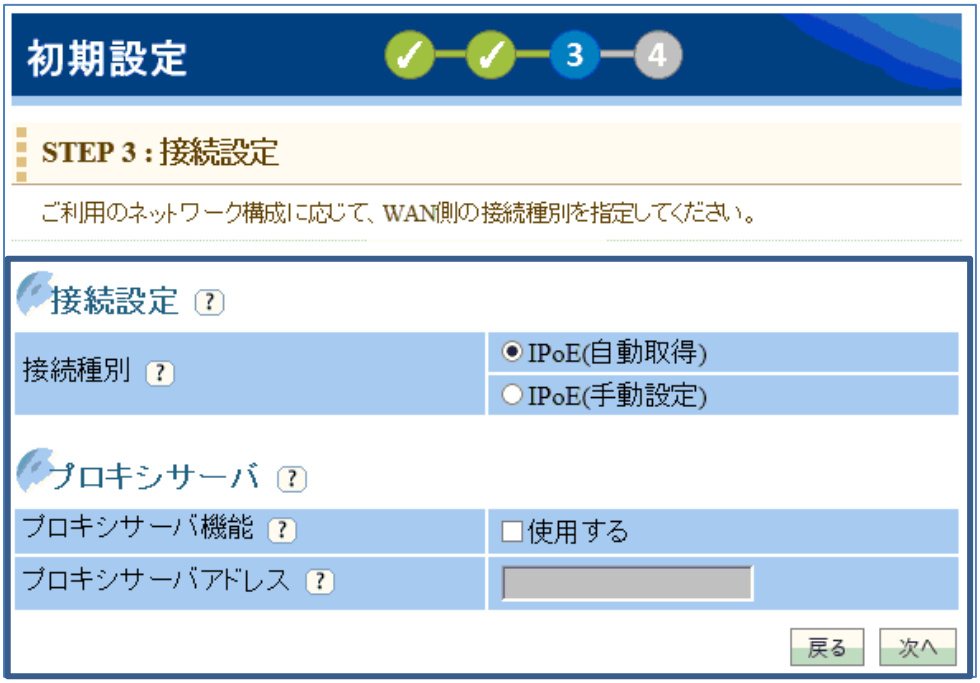
7. **STEP3：** 本製品の IP アドレス [16]に関して設定します

必ずお使いの環境にあわせて選択してください。

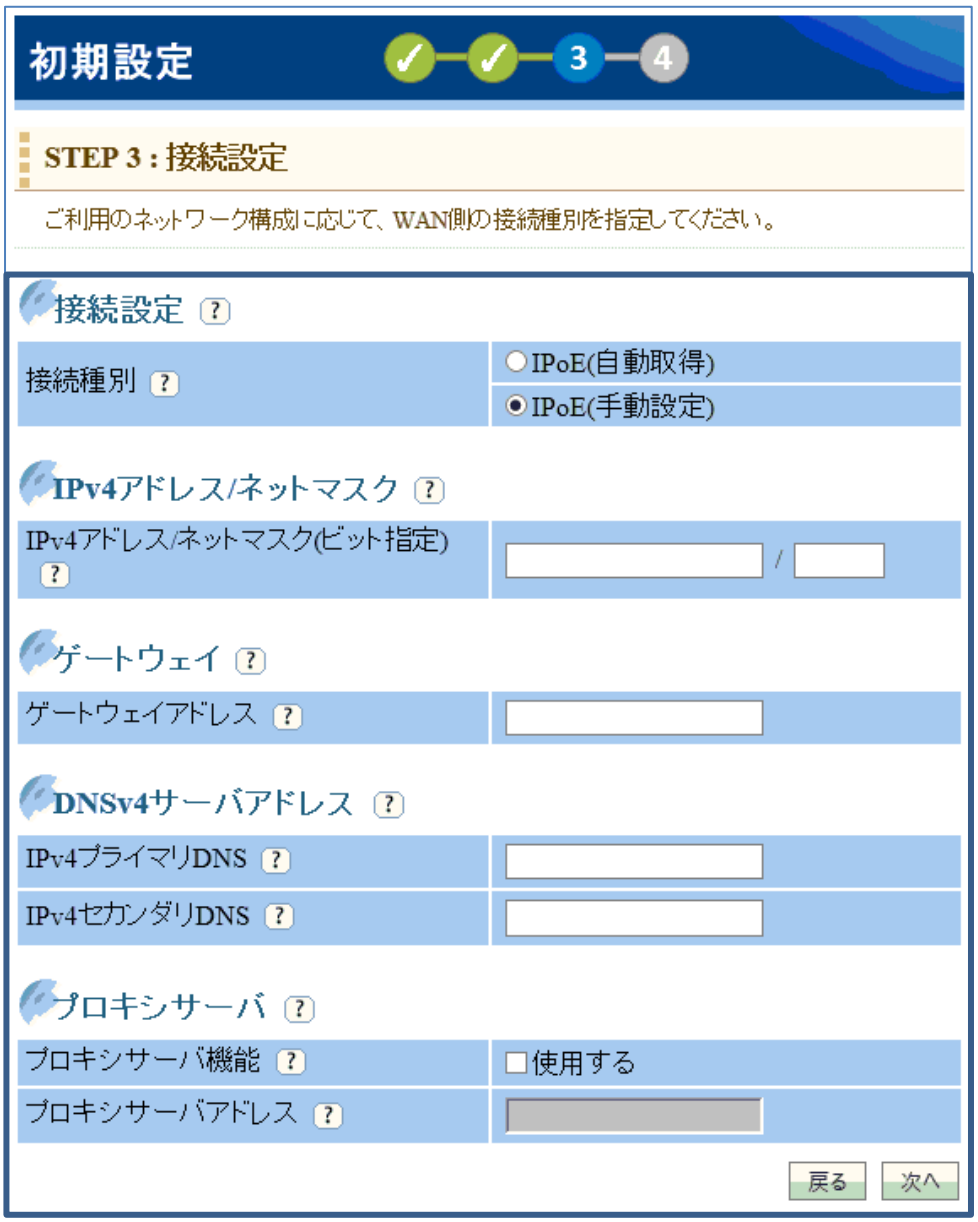
選択項目	説明
IPoE（自動取得）	本製品の IP アドレスを DHCP で取得する場合に選択します。 プロキシサーバを使用している場合は、下記項目を設定してください。 ● プロキシサーバアドレス ※プロキシサーバアドレスは「http://」または「https://」で始まるアドレスを入力します。 ポート番号(必須)はアドレスの最後に「:XXXXX」で指定します。
IPoE（手動設定）	本製品の IP アドレスを手動で設定する場合に選択します。 本項目を選択した場合、下記項目を設定してください。 ● IPv4 アドレス/ネットマスク（ビット指定） ● ゲートウェイアドレス ● IPv4 プライマリ DNS ● IPv4 セカンダリ DNS（任意） ● プロキシサーバアドレス ※プロキシサーバアドレスは「http://」または「https://」で始まるアドレスを入力します。 ポート番号(必須)はアドレスの最後に「:XXXXX」で指定します。

[16]本製品のセキュリティ・スキャン機能を使用するには、本製品に IPv4 アドレスが必要です

■IPoE(自動取得)を選択のとき



■IPoE(手動設定)を選択のとき

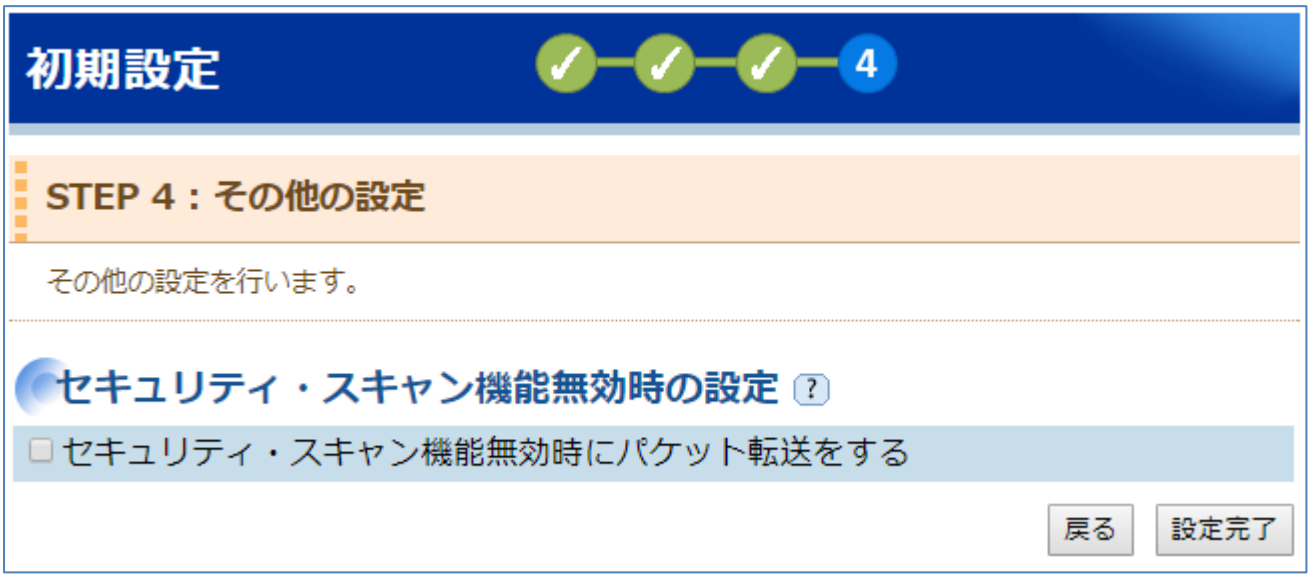


8. **STEP4：** その他の設定を行います。

お客様のセキュリティポリシーにしたがい適切な内容に設定してください。

セキュリティ・スキャン機能が無効の時にもパケット転送許可する場合はチェックを入れます。初期値はチェックなしです。

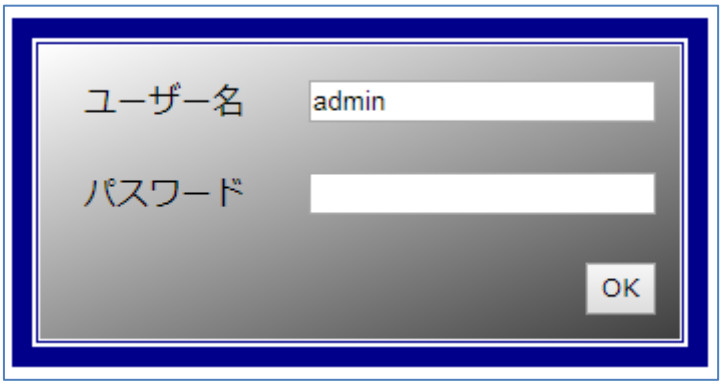
本製品のセキュリティのライセンスが満了したときなど、セキュリティ・スキャン機能が無効になるときがあります。その場合にパケット転送を行う場合はチェックを入れてください。



9. 本製品の設定 Web のログイン画面が開きますので、ユーザー名/パスワードを入力します。

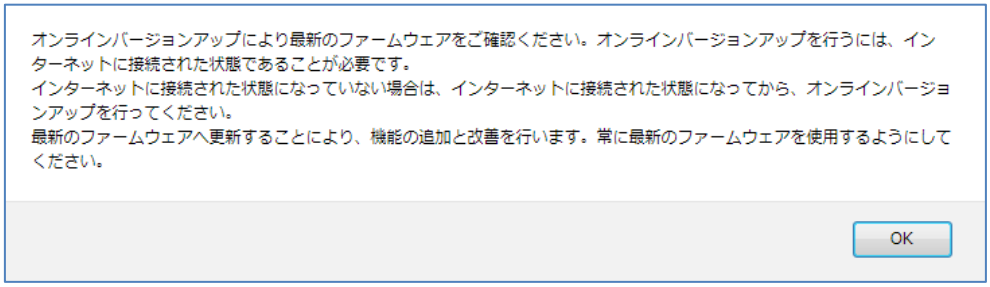
ユーザー名：admin

パスワード：手順 6（STEP2）で設定したパスワード



10.上記手順が完了するとファームウェア確認画面に移動します。

ポップアップの内容を確認の上、「OK」ボタンを押してください。



オンラインバージョンアップ機能により新しいファームウェアの有無を確認して、新しいファームウェアがある場合はファームウェアを更新します。(5.6.16 章を参照してください) ファームウェア更新に時間がかかる場合があります。時間の目安は 5.2.3 章を参照してください。

ファームウェア更新後は本製品が自動的に再起動します。本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

ファームウェア更新を行わない場合は、「トップページに戻る」を押してください

ファームウェア更新を行った場合は、本製品の再起動後に再度ブラウザから http://169.254.254.11/にアクセスしてください。

設定 Web のログイン画面が表示されます。ユーザー名/パスワードを入力すると、TOP 画面に移動します。

11.必要に応じて、本製品のネットワークに関して設定します。

詳細は 5.6 章を参照してください。

12.セキュリティ・スキャン機能に関して設定します。(5.8 章を参照してください。)

13.構成管理に関して設定します。(5.9 章を参照してください。)

14.設定を保存します。（5.5 章を参照してください。）

15.ここでアクティベーションします。（5.2.3 章を参照してください。）

アクティベーション操作は、初回起動時のみ実施します。

16.オンラインバージョンアップ機能により新しいファームウェアの有無を確認して、

新しいファームウェアがある場合はファームウェアを更新します。（5.6.16 章を参照してください）

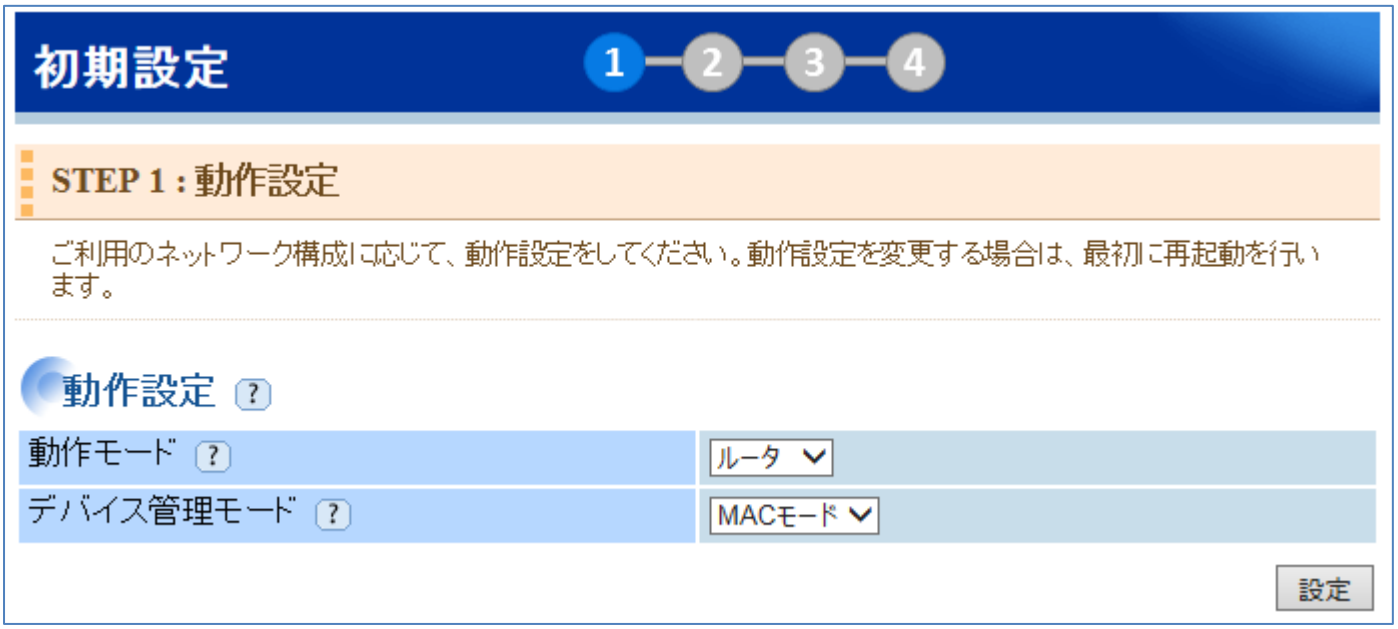
17.パソコンの IP アドレスを元に戻します。

※もともとお使いの設定に戻してください。

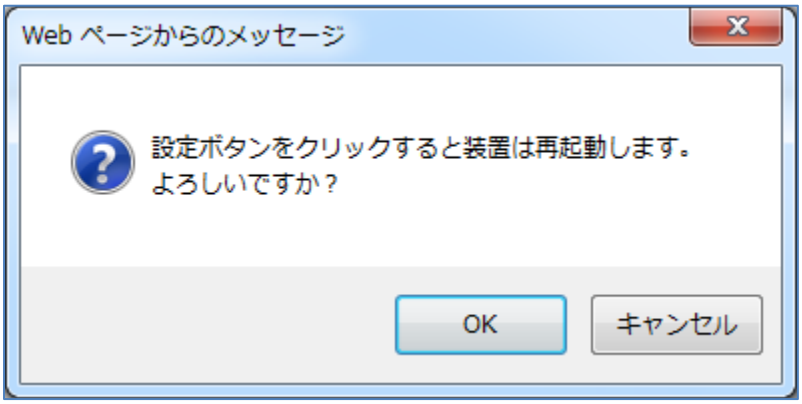
5.2.2. **ルータモードで動作させる場合**

次の手順で設定します。

1. 本製品に各種ケーブルを接続します。（4.5 章を参照してください。）
2. 本製品を設定するパソコンの IP アドレスを 169.254.xxx.xxx/16 に設定します。
   （xxx は 1~254 の任意の整数です。169.254.254.11 以外の IP アドレスを設定してください。）
3. パソコンの Web ブラウザを開き、http://169.254.254.11/もしくは https://169.254.254.11/にアクセスします。
4. 設定ウィザードが開きます。
   STEP1 → STEP2 → STEP3→ STEP4 の順で設定してください。
5. **STEP1:** 動作モードと本製品が管理するデバイスの管理モードを選択します
   ルータモードを選択します。デバイス管理モードは Aspire や IX ルータなどとの連携機能をお使いでなければ初期値の MAC モードのままで構いません。



※ルータモードの場合、本手順の後に再起動します。再起動を促すウィンドウで OK ボタンを押下すると再起動します。



6. **STEP2:** 管理者パスワードを設定します

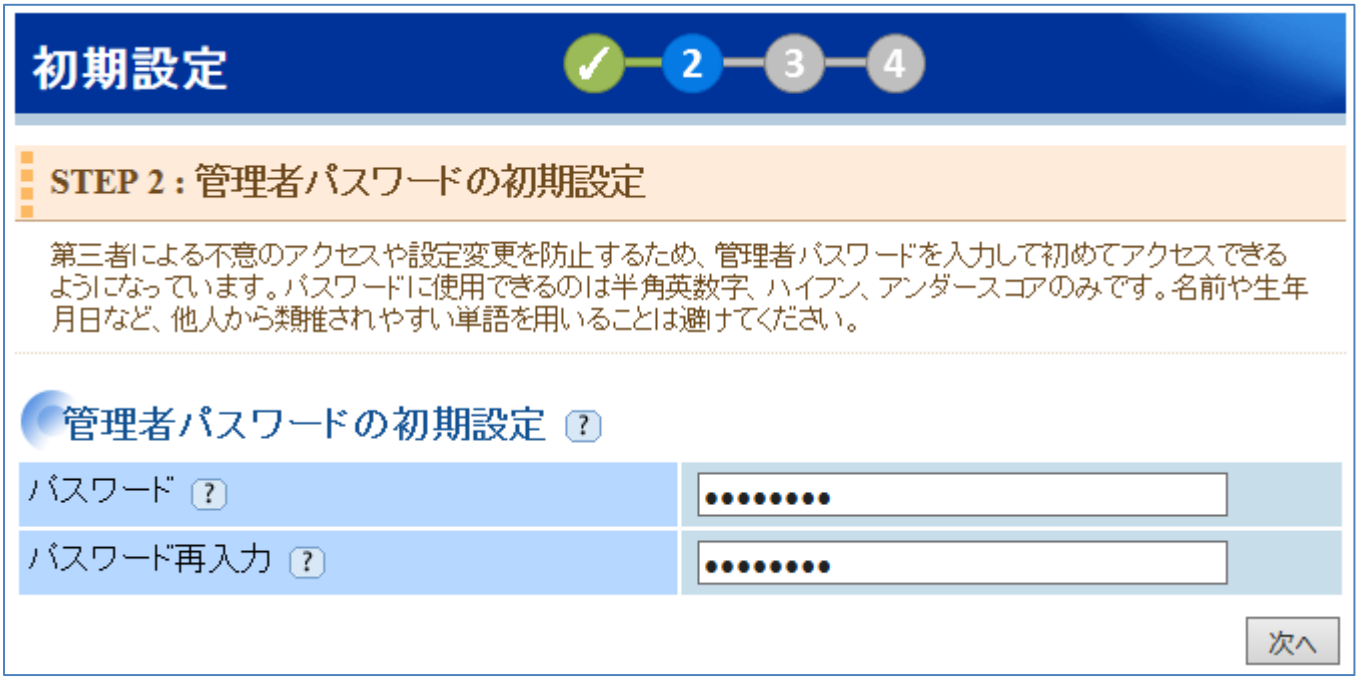
パスワードに使用できる文字は、半角文字 0～9,a～z,A～Z,-(ハイフン),_(アンダースコア)です。

入力可能文字数は、1～64 です。

※パスワードは複雑で長い文字列にして、安全性を高めることをお勧めします。

※管理者パスワードは、本製品を設定する場合に必要となりますので、控えておいてください。忘れた場合は、設定画面を開くことができず、本製品を初期化してすべての設定がやり直しになります。(5.6.15章参照)

※ここで設定したパスワードは、STEP4 の「設定完了」ボタン押下で FlashROM に保存します



7. **STEP3 :** アップリンクインタフェースのネットワークに関して設定します

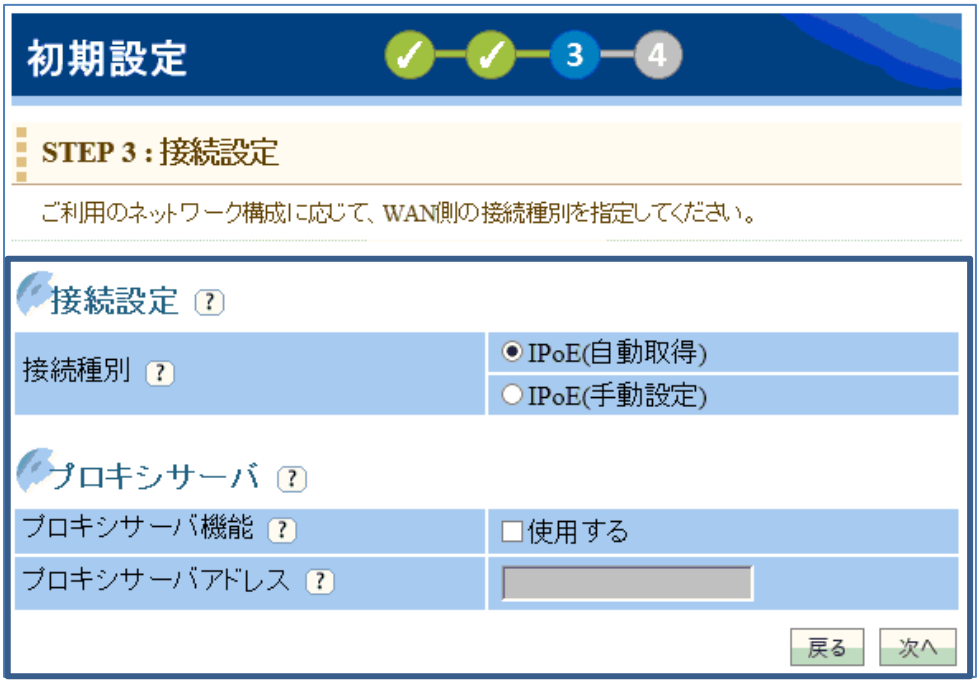
必ずお使いの環境にあわせて設定してください。

選択項目	説明
IPoE（自動取得）	本製品の WAN インタフェースの IP アドレス [17]を DHCP で取得する場合に選択します。 プロキシサーバを使用している場合は、下記項目を設定してください。 ● プロキシサーバアドレス ※プロキシサーバアドレスは「http://」または「https://」で始まるアドレスを入力します。 ポート番号(必須)はアドレスの最後に「:XXXXX」で指定します。
IPoE（手動設定）	本製品の WAN インタフェースの IP アドレスを手動で設定する場合に選択します。 本項目を選択した場合、下記項目を設定してください。 ● IPv4 アドレス/ネットマスク（ビット指定） ● ゲートウェイアドレス ● IPv4 プライマリ DNS ● IPv4 セカンダリ DNS（任意） ● プロキシサーバアドレス ※プロキシサーバアドレスは「http://」または「https://」で始まるアドレスを入力します。 ポート番号(必須)はアドレスの最後に「:XXXXX」で指定します。
PPPoE	本製品の WAN インタフェースの IP アドレスを PPP で取得する場合に選択します。 本項目を選択した場合、下記項目を設定してください。

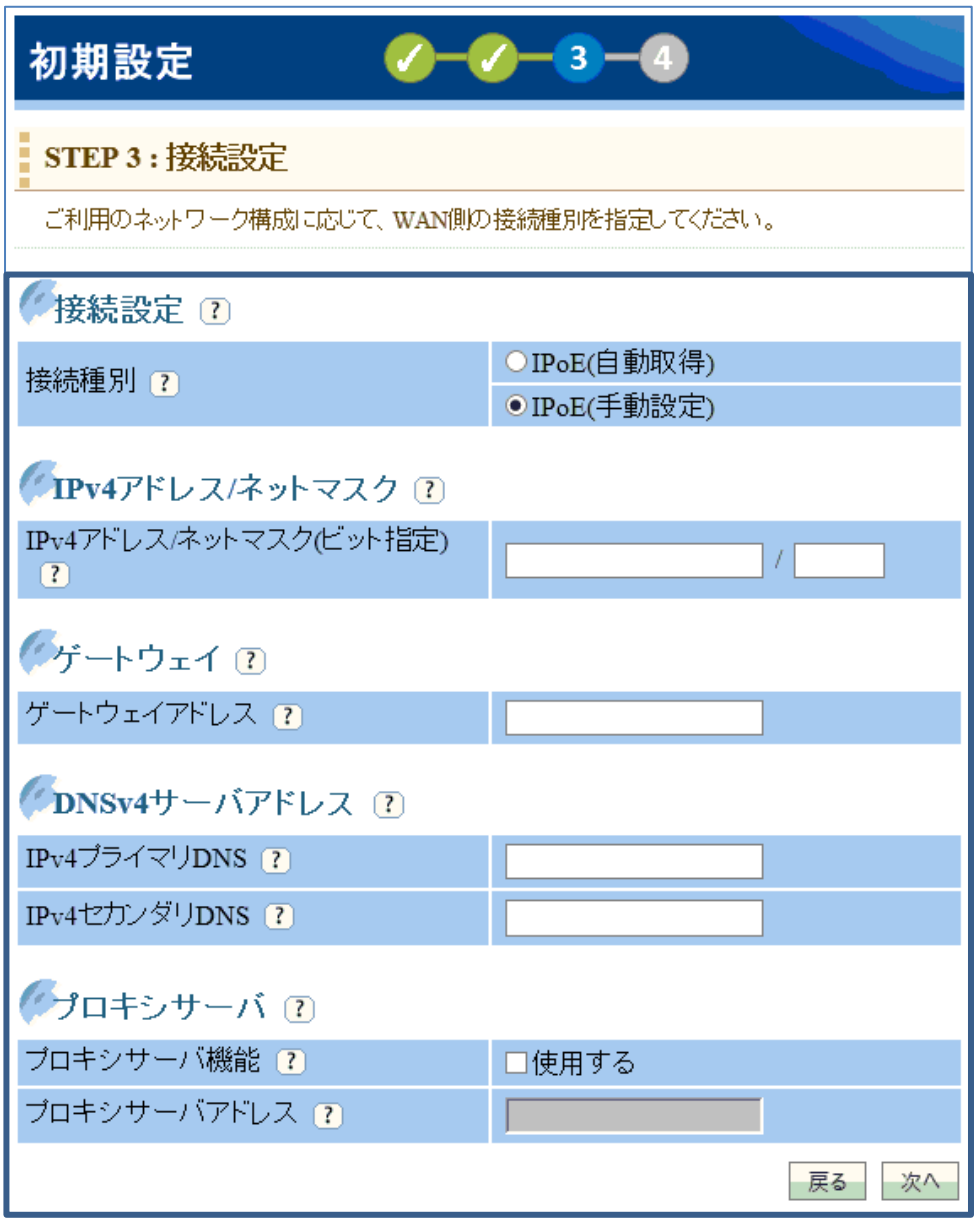
[17]本製品のセキュリティ・スキャン機能を使用するには、本製品に管理用の IPv4 アドレスが必要です

	● 認証用 ID ● 認証用パスワード ※認証用 ID、認証用パスワードで使用できる文字列は、半角英数字、記号（アスキーコード：0x20~0x7e）です。文字数は 128 文字まで設定できます。

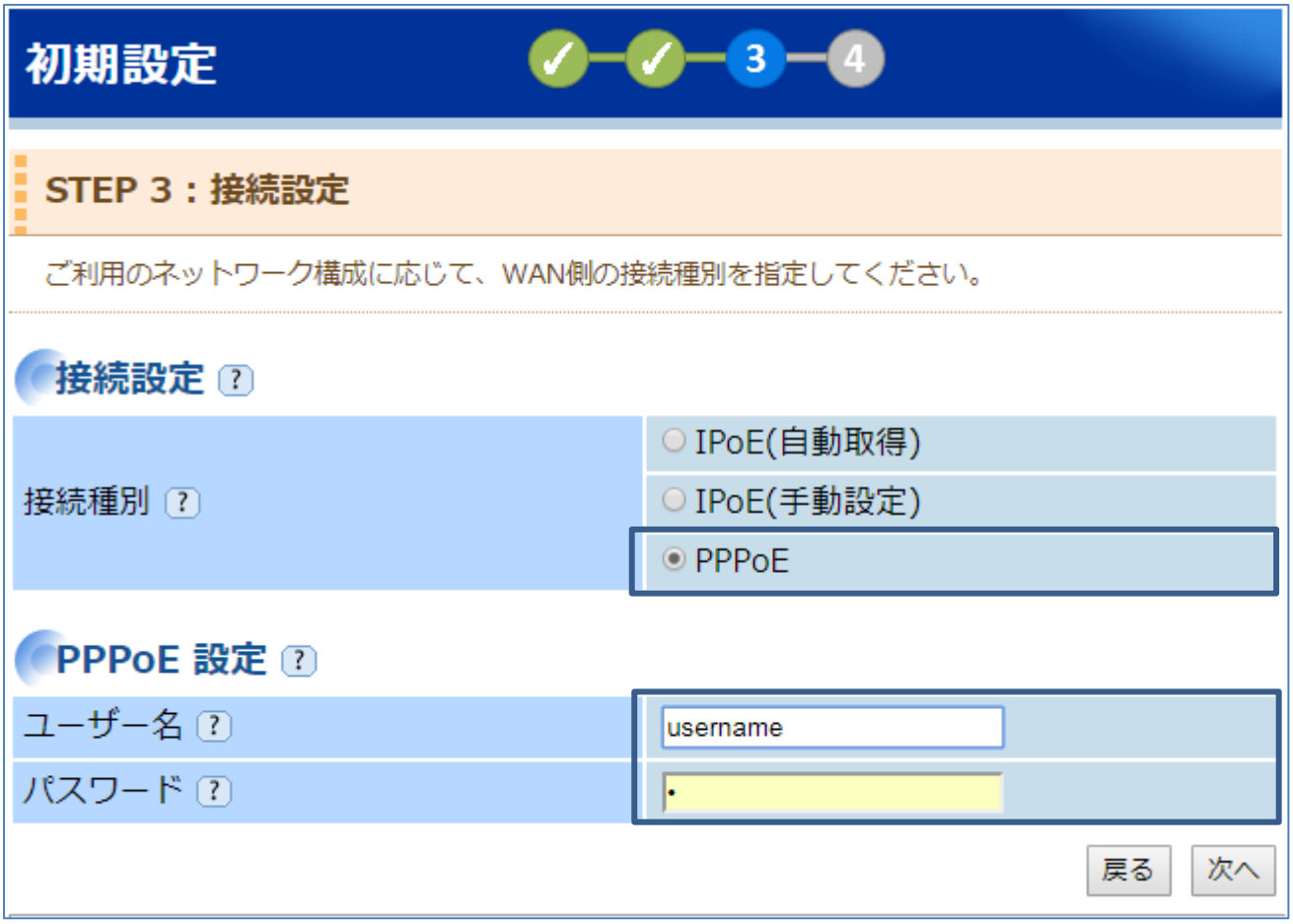
■IPoE(自動取得)を選択のとき



■IPoE(手動設定)を選択のとき



■PPPoE を選択のとき

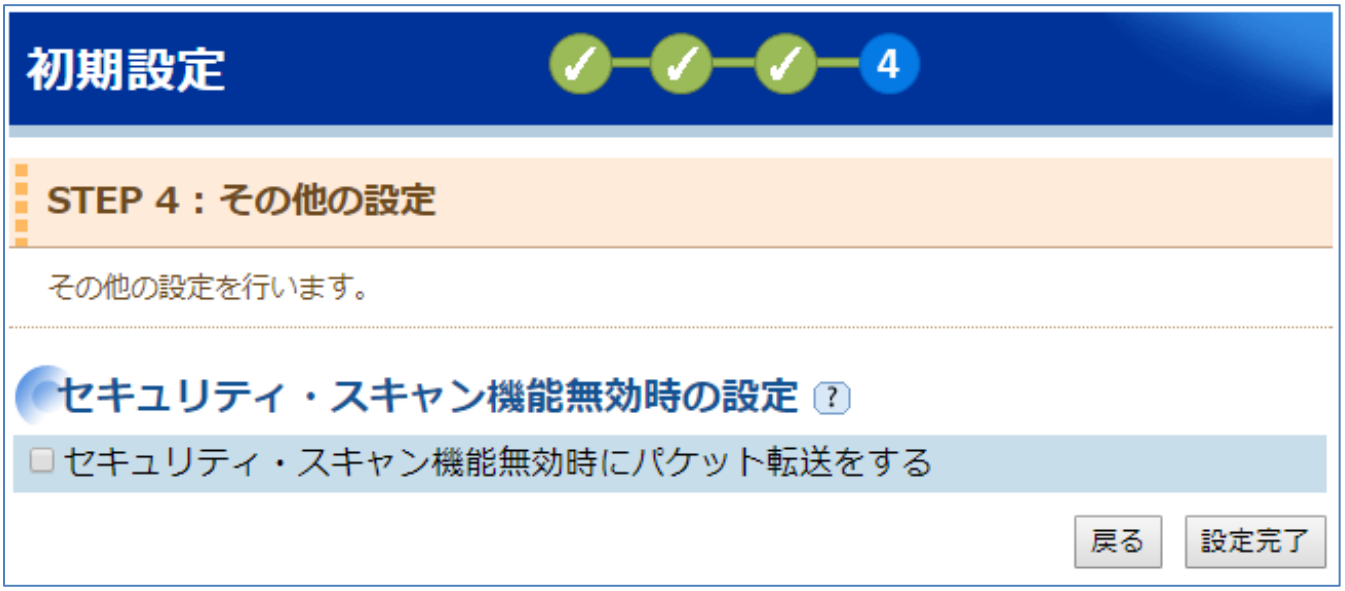


8. **STEP4：** その他の設定を行います。

お客様のセキュリティポリシーにしたがい適切な内容に設定してください。

セキュリティ・スキャン機能が無効の時にもパケット転送許可する場合はチェックを入れます。初期値はチェックなしです。

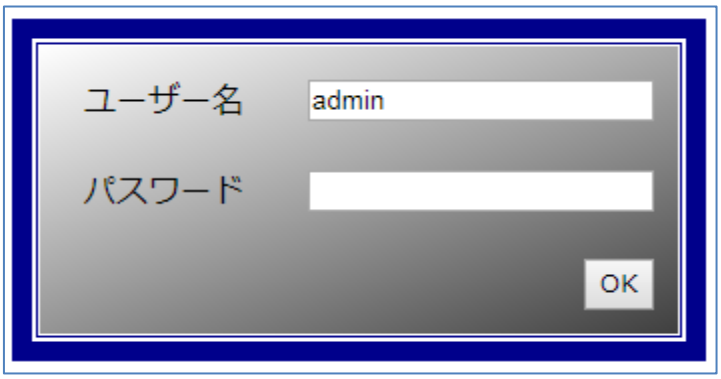
本製品のセキュリティのライセンスが満了したときなど、セキュリティ・スキャン機能が無効になるときがあります。その場合にパケット転送を行う場合はチェックを入れてください。



9. 本製品の設定 Web のログイン画面が開きますので、ユーザー名/パスワードを入力します。

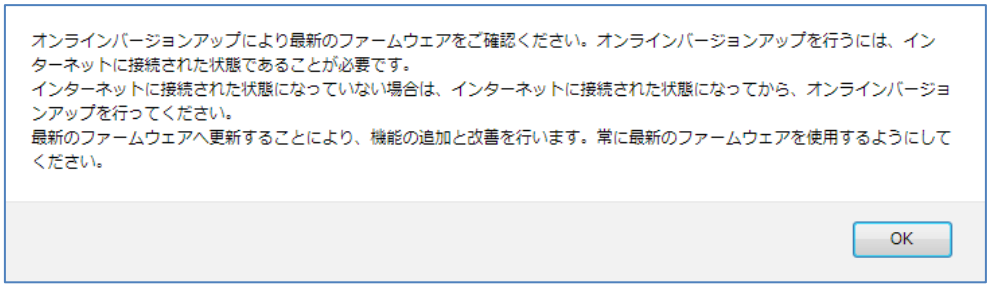
ユーザー名：admin

パスワード：手順 6（STEP2）で設定したパスワード



10. 上記手順が完了するとファームウェア確認画面に移動します。

ポップアップの内容を確認の上、OK ボタンを押してください。



オンラインバージョンアップ機能により新しいファームウェアの有無を確認して、新しいファームウェアがある場合はファームウェアを更新します。（5.6.16 章を参照してください）ファームウェア更新に時間がかかる場合があります。時間の目安は 5.2.3 章を参照してください。

ファームウェア更新後は本製品が自動的に再起動します。本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

ファームウェア更新を行わなかった場合は、「トップページに戻る」を押してください

ファームウェア更新を行った場合は、本製品の再起動後に再度ブラウザから http://169.254.254.11/にアクセスしてください。

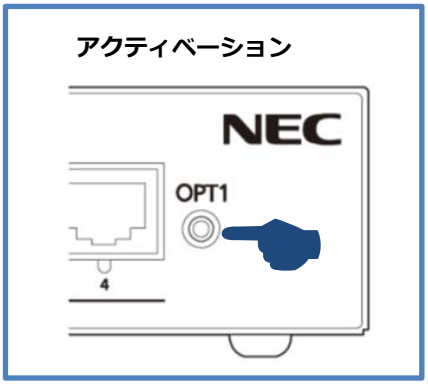
設定 Web のログイン画面が表示されます。ユーザー名/パスワードを入力すると、TOP 画面に移動します。

この表示がある場合、次のことが考えられます。

・アクティベーション未完了（初回時のみ）

・装置起動後のライセンスチェック未完了

11.本製品のネットワークに関して設定します。(5.7 章を参照してください。)
12.セキュリティ・スキャン機能に関して設定します。(5.8 章を参照してください。)
13.構成管理に関して設定します。(5.9 章を参照してください。)
14.設定を保存します。(5.5 章を参照してください。)
15.ここでアクティベーションします。(5.2.3 章を参照してください。)
　アクティベーション操作は、初回起動時のみ実施します。
16.オンラインバージョンアップ機能により新しいファームウェアの有無を確認して、
　新しいファームウェアがある場合はファームウェアを更新します。
　(5.6.16 章を参照してください)
17.パソコンの IP アドレスを元に戻します。
　※もともとお使いの設定に戻してください。



5.2.3. **アクティベーション**

本製品のセキュリティ・スキャン機能を使用するには、アクティベーション操作が必要です。
アクティベーション操作時に工場出荷時のファームウェアよりも新しいファームウェアが公開されている場合、本製品はアクティベーション成功の直後に自動でファームウェアの更新を行います。ファームウェアの更新には、ご利用のインターネット通信環境にもよりますが、5~20 分程度(注)の時間がかかります。(ご利用の回線速度により異なります)
アクティベーションが終了し、ALERT2 ランプが消灯するまでは本製品の電源を OFF にしないでください。

(注) ファームウェア更新にかかる時間の目安：回線速度　500 Kbps のとき　17 分
回線速度　1 Mbps のとき　11 分
回線速度　5 Mbps のとき　6 分
回線速度　50 Mbps 以上のとき　5 分

[実施タイミング]

初回起動時のみ。
本製品を設定し、インターネット通信可能になった時点（NETWORK ランプが緑点灯、または橙点灯）で後述の内容を操作してください。

[事前準備]

本製品がインターネット通信できる状態にしてください。
（ブリッジモード使用時 3.5.2 章参照）（ルータモード使用時 3.6.2 章参照）
※アクティベーション操作の前に本製品の各種設定の実施を推奨します。

[アクティベーション時のランプの推移]

OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を 4 秒間押し続けた(※)後のランプの推移は次のとおりです。
(※)アクティベーション操作

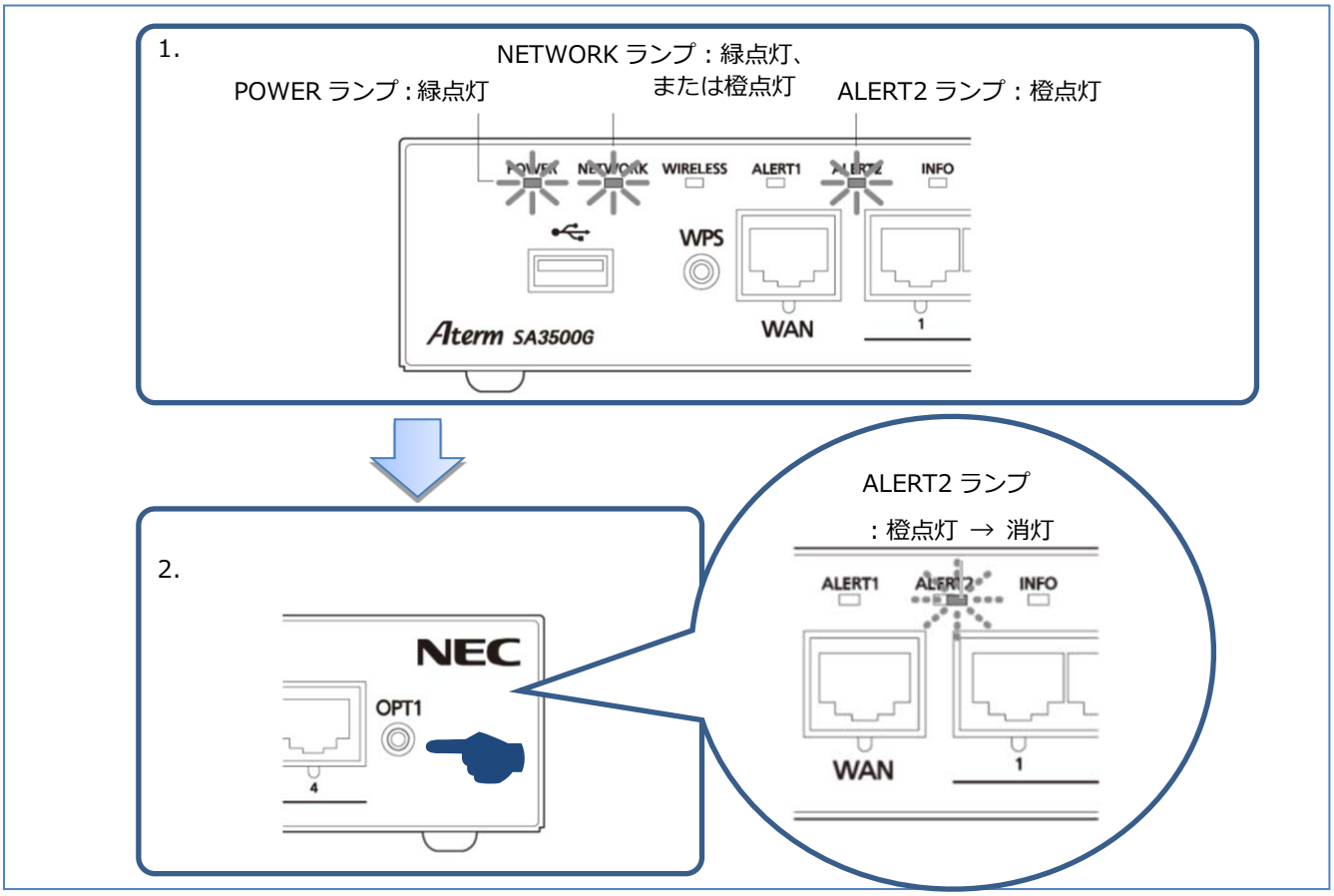
a)　新しいファームウェアがある場合

ALERT2 ランプ	橙点灯	⇨	橙点滅(瞬時)	⇨	緑点滅(2~10 分)	⇨	消灯	➡ (再起動)
INFO ランプ	消灯 or 橙点灯		橙点滅		橙点滅		消灯	

b)　新しいファームウェアがない場合

ALERT2 ランプ	橙点灯	⇨	橙点滅(瞬時)	⇨	消灯
INFO ランプ	消灯		消灯		消灯

[操作手順]



1. 本製品のランプが次の状態になっていることを確認します。（下記で説明していないランプは不問です）
   POWER ランプ　　… 緑点灯
   NETWORK ランプ　… 緑点灯、または橙点灯
   ALERT2 ランプ　　… 橙点灯

2. OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を約 4 秒間押し続けたら放します。
   (ALERT2 ランプが橙点滅するときがあります)

3. INFO ランプが橙点灯する場合、管理サーバに新しいファームウェアがあります。
4. INFO ランプの表示によって、動作が異なります。
   a) INFO ランプが橙点灯の場合
      ALERT2 ランプが緑点滅することを確認します。ALERT2 ランプが緑点滅したらアクティベーションは完了していますが、引き続きオンラインバージョンアップが開始されます。オンラインバージョンアップ中は INFO ランプが橙点滅します。オンラインバージョンアップ中は本製品の電源を OFF にしないでください。(5.2.3.1 章参照)
   b) INFO ランプが消灯の場合
      ALERT2 ランプが消灯することを確認します。ALERT2 ランプが消灯したらアクティベーションは完了です。

[メモ]

ライセンスの利用開始日は、アクティベーションが成功した日または、本製品納入後 31 日を経過したいずれかの早い日です。
アクティベーションが成功した後はアクティベーションを取り消すことはできません。

5.2.3.1. **アクティベーション成功後のオンラインバージョンアップ**

アクティベーション成功のあと、ALERT2 ランプが緑点滅、INFO ランプが橙点滅する場合は、オンラインバージョンアップが進行中です。オンラインバージョンアップは以下の流れで自動的に実行されます。

[オンラインバージョンアップの流れ]

1. 管理サーバからファームウェアをダウンロードします。ダウンロード中は POWER ランプが緑点灯、ALERT2 ランプが緑点滅、INFO ランプが橙点滅になります。

2. ファームウェアのダウンロードが完了すると、ファームウェアの書き込みを開始します。書き込み中は POWER ランプが橙点滅に変わります。ファームウェアの書き込み中は本製品の電源を OFF にしないでください。

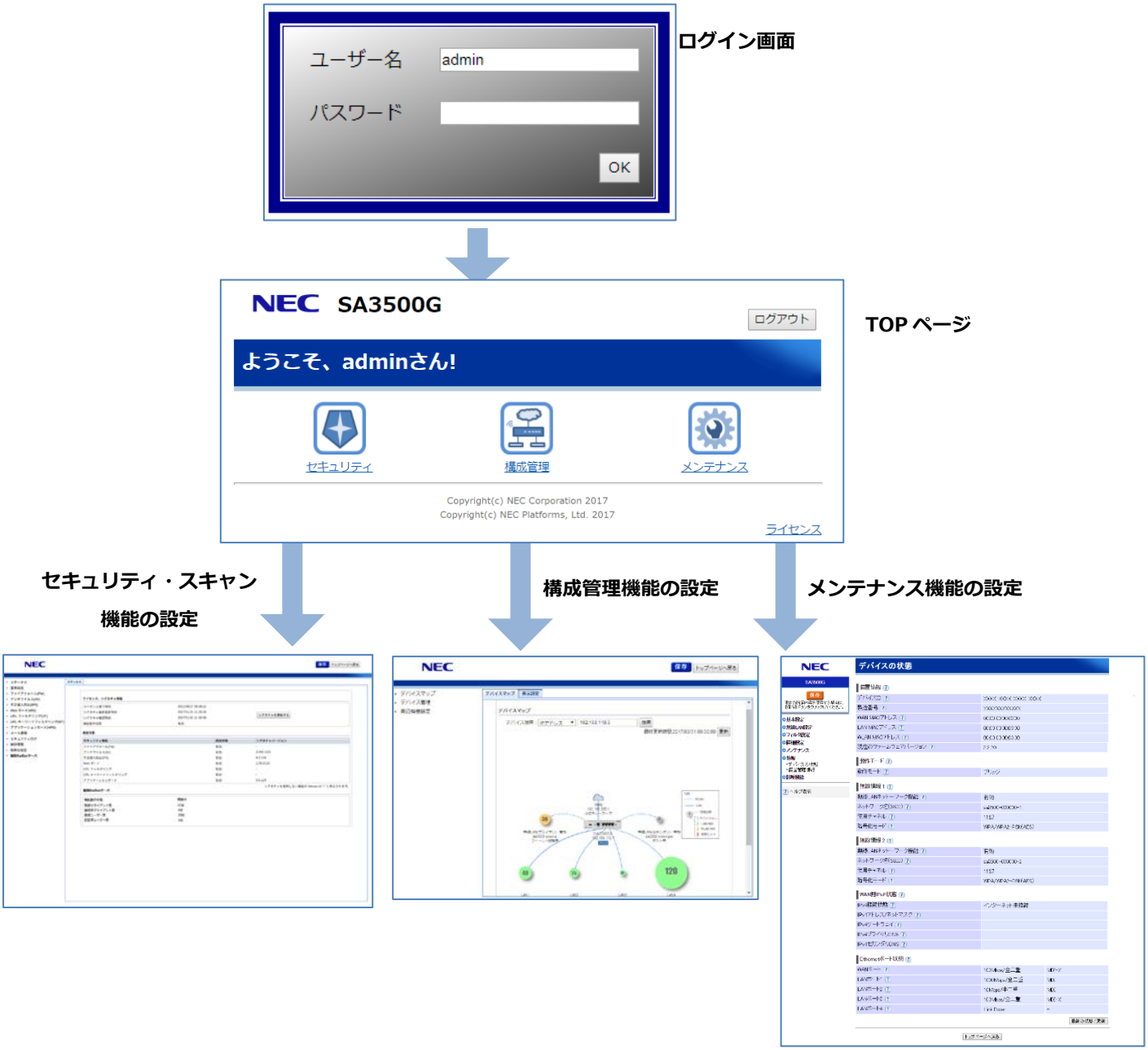
3. 本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

[ご注意]

WAN ポートに接続している Ethernet ケーブルが抜けるなどの事由でインターネットに接続できない状態が 10 分間続いた場合、ファームウェアの更新処理は中断され、INFO ランプは橙点灯状態になります。その後、ALERT2 ランプが自動的に消灯すれば、本製品のセキュリティ機能が動作している状態です。ALERT2 ランプが消灯しない場合はインターネットに本製品を接続し、再度 5.2.3 章の [操作手順] を初めから行ってください。

5.3. 設定画面構成

本製品の設定手順は次のとおりです。



※画面の表示内容は動作モードにより異なります。

「メンテナンス」の各画面構成は以下の章を参照してください。

ブリッジモード　　5.6.1 章

ルータモード　　5.7.1 章

[メモ]

ファームウェアバージョン 3.3.20 から、[デバイス管理]画面、および[パトライト連携]画面は、構成管理機能の画面に移動しました。

詳細は、5.9 章を参照してください。

5.4. 本製品へのログイン

本製品へのアクセス時のログインについて説明します。

1. 本製品の LAN ポートにパソコンを接続します。
2. ブリッジモードの場合は、パソコンの IP アドレスを 169.254.xxx.xxx/16(*1)に設定し、Web ブラウザで http://169.254.254.11/ にアクセスします。

   （*1）xxx は 1~254 の任意の整数。169.254.254.11 を除きます。

   ※パソコンに IP アドレスが割り当てられている場合、http://169.254.254.11/でアクセスできない場合があります。

   そのときはパソコンのルート設定を行ってください。Windows パソコンの設定例を以下に示します。

   1）コマンドプロンプトを管理者権限で起動します。

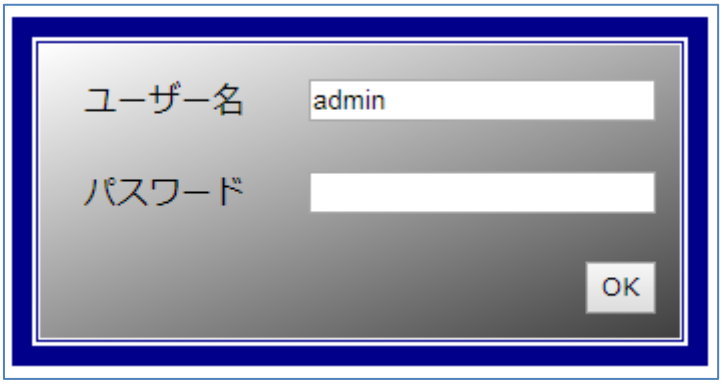
   2）次のコマンドを入力してリターンします。

   route add 169.254.0.0 mask 255.255.0.0 <パソコンに割り当てられた IP アドレス>

   ルータモードの場合は、Web ブラウザで http://192.168.110.1/（初期値）にアクセスします。なお、ブリッジモードの場合と同様、パソコンの IP アドレスを 169.254.xxx.xxx/16(*1)に設定し、Web ブラウザで http://169.254.254.11/ にアクセスすることもできます。

   HTTPS で設定 Web にアクセスできます。お客様のお使いの環境で、設定 Web へのアクセスの通信を暗号化したい場合にご利用ください。HTTPS アクセス時にご使用ブラウザのセキュリティの警告が表示する場合がありますが、問題ありませんので、そのままアクセスを続行してください。

3. ユーザー名/パスワードの入力画面が開きますので、ユーザー名とパスワードを入力して「OK」ボタンを押下します。



設定項目	値	備考
ユーザー名	admin	固定値
パスワード	（お客様が設定した管理者パスワード）*2	パスワードの変更方法は、5.6.12 章を参照してください。

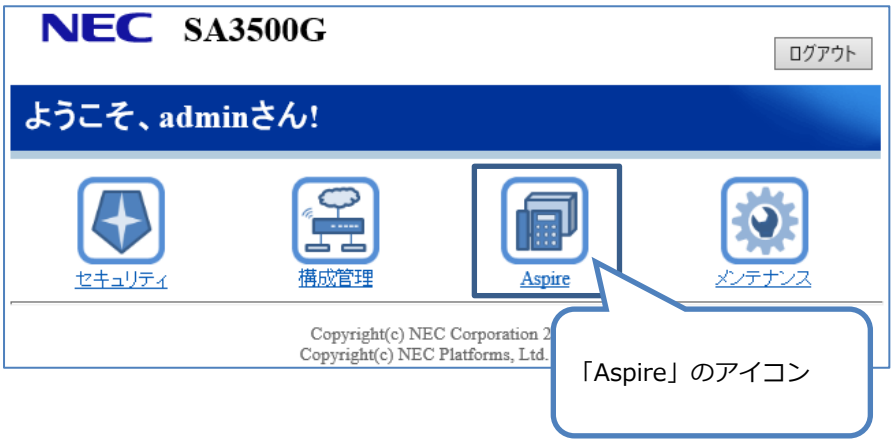
*2 初回起動時のウィザードで設定しています。（5.2.1 章、5.2.2 章参照）

4. TOP ページが開きます。

[メモ]

- パソコンの IP アドレスの設定を変更したときは、本製品の設定終了後、パソコンの IP アドレスの設定を元に戻してください。
- 初期設定では WAN 側から設定 Web にアクセスできません。 アクセスが必要な場合は、パケットフィルタ設定で許可設定が可能ですが、セキュリティ面ではご注意ください。

※本製品に Aspire の Web プログラミングと設定 Web の連携設定を行うと、[TOP]画面に以下の様に、「Aspire」のアイコンが表示されます。Aspire との連携設定の設定手順は 5.9.4 章を参照してください。



5.5. 設定の保存

「保存」ボタンは、セキュリティ画面、メンテナンス画面のどちらにもあります。

どちらの画面の「保存」ボタンでも、それまでに設定したすべての設定内容を FlashROM に保存します。

USB ストレージが USB ポートに接続されている場合は、FlashROM に保存するタイミングで USB ストレージにも設定内容を保存します。

保存ボタンの状態	説明
青	すべての設定を FlashROM に保存済みです。
橙点滅	FlashROM に保存していない設定値があります。 ※設定 Web に初めてログインする際に設定する「管理者パスワード」は、FlashROM に自動保存します。 「管理者パスワードの変更」画面で設定する管理者パスワードは、FlashROM に自動保存しません。

[セキュリティ画面]

「保存」ボタンが橙色で点滅している場合は、FlashROM に保存していない設定項目があることを示しています。

※メンテナンス画面で設定した設定値も FlashROM に保存します。

※上図はルータモードの画面例です。保存ボタンの位置は、ブリッジモードでも同じです。

[メンテナンス画面]

「保存」ボタンが橙色で点滅している場合は、FlashROM に保存していない設定項目があることを示しています。

※セキュリティ画面で設定した設定値も FlashROM に保存します。

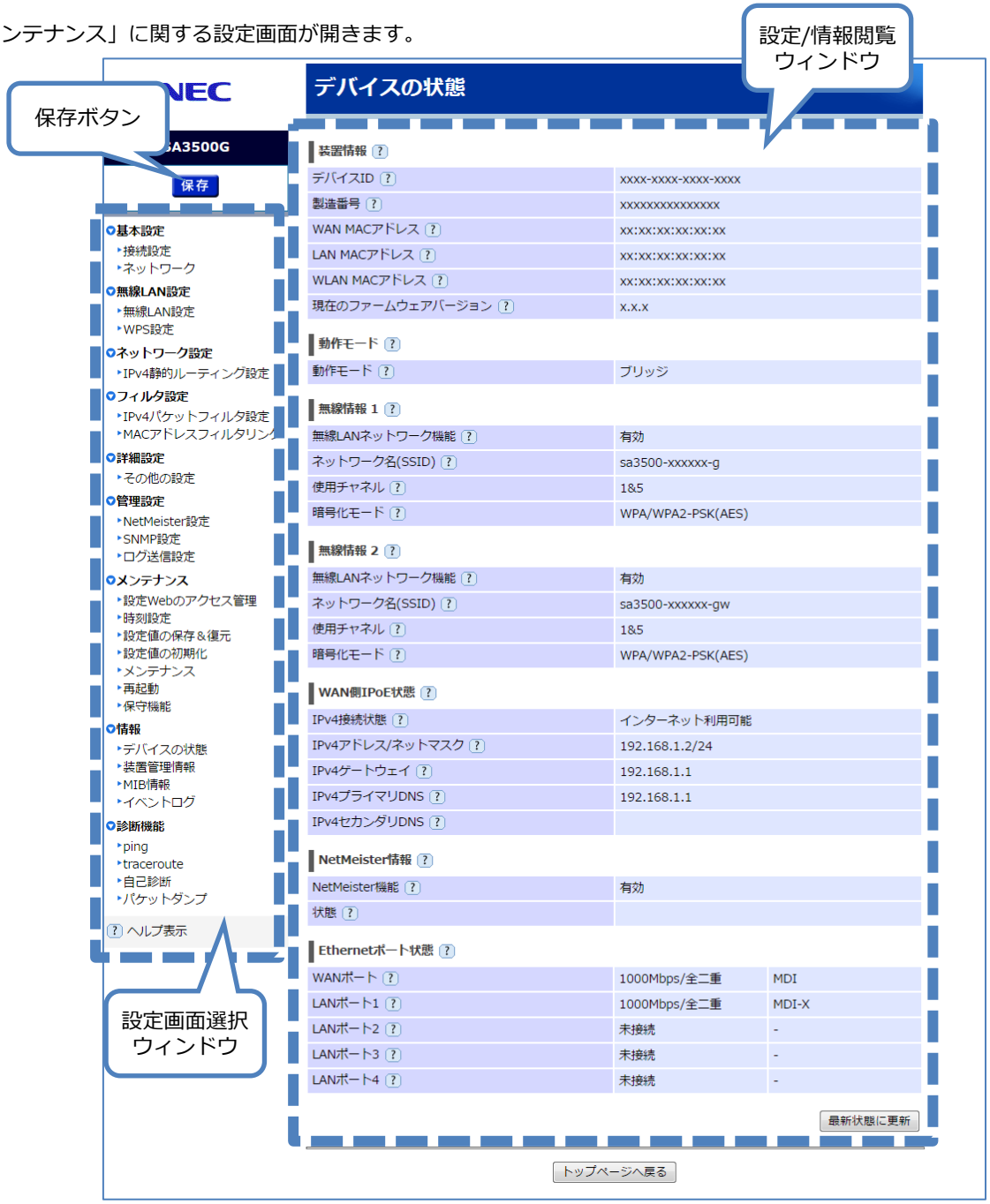
※上図はブリッジモードの画面例です。保存ボタンの位置は、ルータモードでも同じです。

5.6. メンテナンス（ブリッジモード）に関する設定

本製品のセキュリティ・スキャン機能以外の設定、および情報を閲覧します。

1. TOP ページで「メンテナンス」をクリックします。

2. 「メンテナンス」に関する設定画面が開きます。



5.6.1. **設定画面構成**

ブリッジモードのメンテナンスの設定画面構成は次のとおりです。

項目	説明	操作の必要性の有無/備考
メンテナンス（ブリッジモード）	ブリッジ機能、メンテナンス機能に関する設定	
基本設定	本製品のネットワークに関する設定	
接続設定	ルータモードへの切り替え ※切り替えは、本製品の再起動が必要です。	
ネットワーク	DHCP クライアント 本製品の IP アドレス、ゲートウェイ情報 DNS サーバ情報 HTTP プロキシサーバ	
無線 LAN 設定	本製品の無線 LAN 機能に関する設定	
無線 LAN 設定	無線 LAN の設定	
WPS 設定	WPS 機能の有効/無効設定	
ネットワーク設定		
IPv4 静的ルーティング設定	IPv4 静的ルーティングの設定	
フィルタ設定		
IPv4 パケットフィルタ設定	IPv4 パケットフィルタエントリの設定	
MAC アドレスフィルタリング	MAC アドレスフィルタリングの設定	
詳細設定		
その他の設定	Ethernet ポート設定	
管理設定	管理プロトコルに関する設定	
NetMeister 設定	NetMeister 機能の設定	
SNMP 設定	SNMPv1, SNMPv2c エージェントの設定	
ログ送信設定	syslog サーバへのログ送信機能の設定	
メンテナンス	本製品の設定やファームウェアに関する設定	
設定 Web のアクセス管理	管理者パスワードの設定 自動ログアウト時間の設定	管理者パスワードは、定期的な変更を推奨します
時刻設定	本製品の時刻に関する設定	初期値を推奨します
設定値の保存＆復元	本製品の設定の保存、および、復元	
設定値の初期化	本製品の設定の初期化の実行	
メンテナンス	ファームウェアに関する設定	必ず確認してください
再起動	再起動の実行	
保守機能	保守機能の設定	保守者向けの機能を有効にする設定です
情報	本製品のバージョンや動作状況の表示	
デバイスの状態	製品情報（デバイス ID、製造番号、MAC アドレス、バージョン情報） 動作モード 無線 LAN の状態 製品の IP アドレス	

	装置管理情報	Wi-Fi 帰属情報 ARP テーブル	
	MIB 情報	SNMP MIB 情報	
	イベントログ	本製品の動作ログ	Ver3.2.45 で追加
診断機能		ネットワーク到達確認の実施	
	ping	ping による到達確認の実施	
	traceroute	traceroute による経路確認の実施	
	自己診断	設定情報の確認、サーバへの到達確認の実施	
	パケットダンプ	本製品を通過するパケットのキャプチャを実施	

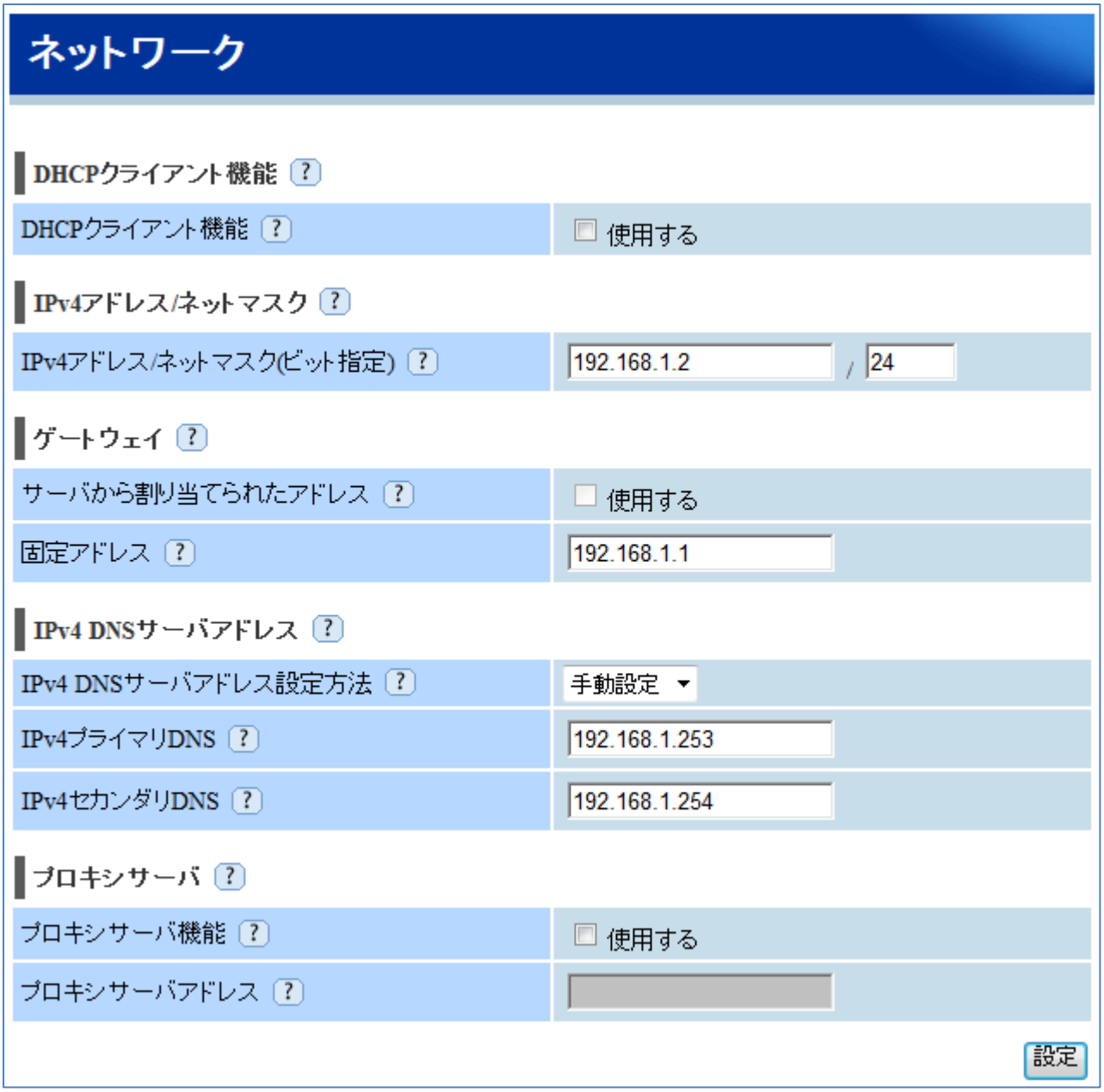
5.6.2. **本製品の IP アドレスの設定**

本製品の IP アドレスを本製品の DHCP クライアント機能で取得しない場合は、必ず実施してください。

本製品のセキュリティ・スキャン機能を使用するには、本製品にインターネットにアクセスできる IPv4 アドレスが必要です。

本製品の IPv4 アドレスを固定で設定する場合は、本章を参考に設定してください。

なお、本製品は、初期状態で DHCP クライアント機能が有効になっています。本製品の IPv4 アドレスを DHCP クライアント機能で取得する場合は、本章で説明する設定は不要です。



※お客様のインターネット接続ネットワークが、プロキシサーバ経由の場合、本製品のプロキシサーバ機能を有効にしてください。

本製品のセキュリティ・スキャン機能のアップデートやファームウェアの更新などで、本製品自身が通信します。

1. [TOP]-[メンテナンス]-[基本設定]-[ネットワーク]画面を開きます。
2. 本製品のネットワーク情報を入力します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、本設定を保存します。

設定項目	値	備考	初期値
DHCP クライアント機能	• チェック有…本製品の IP アドレスを DHCP クライアント機能で取得 • チェック無…本製品の IP アドレスを本設定画面で設定		有効
IPv4 アドレス/ネットマスク	本製品の管理用のIPv4アドレスおよびネットマスクを入力	IPv4 アドレスは、インターネット接続可能なアドレスを設定します。 ネットマスクを 10 進数表記で入力します。	未設定
ゲートウェイ	ゲートウェイ情報の設定		
サーバから割り当てられたアドレス	• チェック有…本製品のデフォルトゲートウェイアドレスを DHCP クライアント機能で取得 • チェック無…本製品のデフォルトゲートウェイアドレスを本設定画面で設定	DHCP クライアント機能を使用しない場合、本項目はグレーアウトします。	有効
固定アドレス	デフォルトゲートウェイアドレスを入力		未設定
IPv4 DNS サーバアドレス	DNS サーバアドレス情報の設定		
IPv4 DNS サーバアドレス設定方法	• 自動設定…本製品がアクセスする DNS サーバアドレスを DHCP クライアント機能で取得 • 手動設定…本製品がアクセスする DNS サーバアドレスを本設定画面で設定	DHCP クライアント機能を使用しない場合、 「手動設定」となります。 「手動設定」を選択した場合、「IPv4 プライマリ DNS」項目の設定が必須です。	自動設定
IPv4 プライマリ DNS	本製品がアクセスするプライマリ DNSv4 サーバアドレスを入力		未設定
IPv4 セカンダリ DNS	本製品がアクセスするセカンダリ DNSv4 サーバアドレスを入力	本設定項目は省略可能です。	未設定
プロキシサーバ	HTTP プロキシサーバ情報の設定		
プロキシサーバ機能	• チェック有…本製品のアップリンクインタフェース側にプロキシサーバを設置している • チェック無…本製品のアップリンクインタフェース側にプロキシサーバを設置していない		無効
プロキシサーバアドレス	HTTP プロキシサーバのアドレスとポート番号を設定します。設定形式は次のとおりです。 • http://[IP アドレス]:[ポート番号]/	お客様の HTTP プロキシサーバのアドレスおよびポート番号を設定してください。 入力可能文字列は、半角英数字および、下記の記号です。 - _ . ! * / = + : @ 入力可能文字数は、256 文字です。	未設定

		• http://[ドメイン名]:[ポート番号]/ • https://[IP アドレス]:[ポート番号]/ • https://[ドメイン名]:[ポート番号]/	HTTP で本製品の設定 Web にアクセスする場合、プロキシサーバは HTTP で設定してください。 HTTPS で本製品の設定 Web にアクセスする場合、プロキシサーバは HTTPS で設定してください。	

5.6.3. **無線 LAN の設定**

ブリッジモードではネットワーク分離機能はご使用になれません。

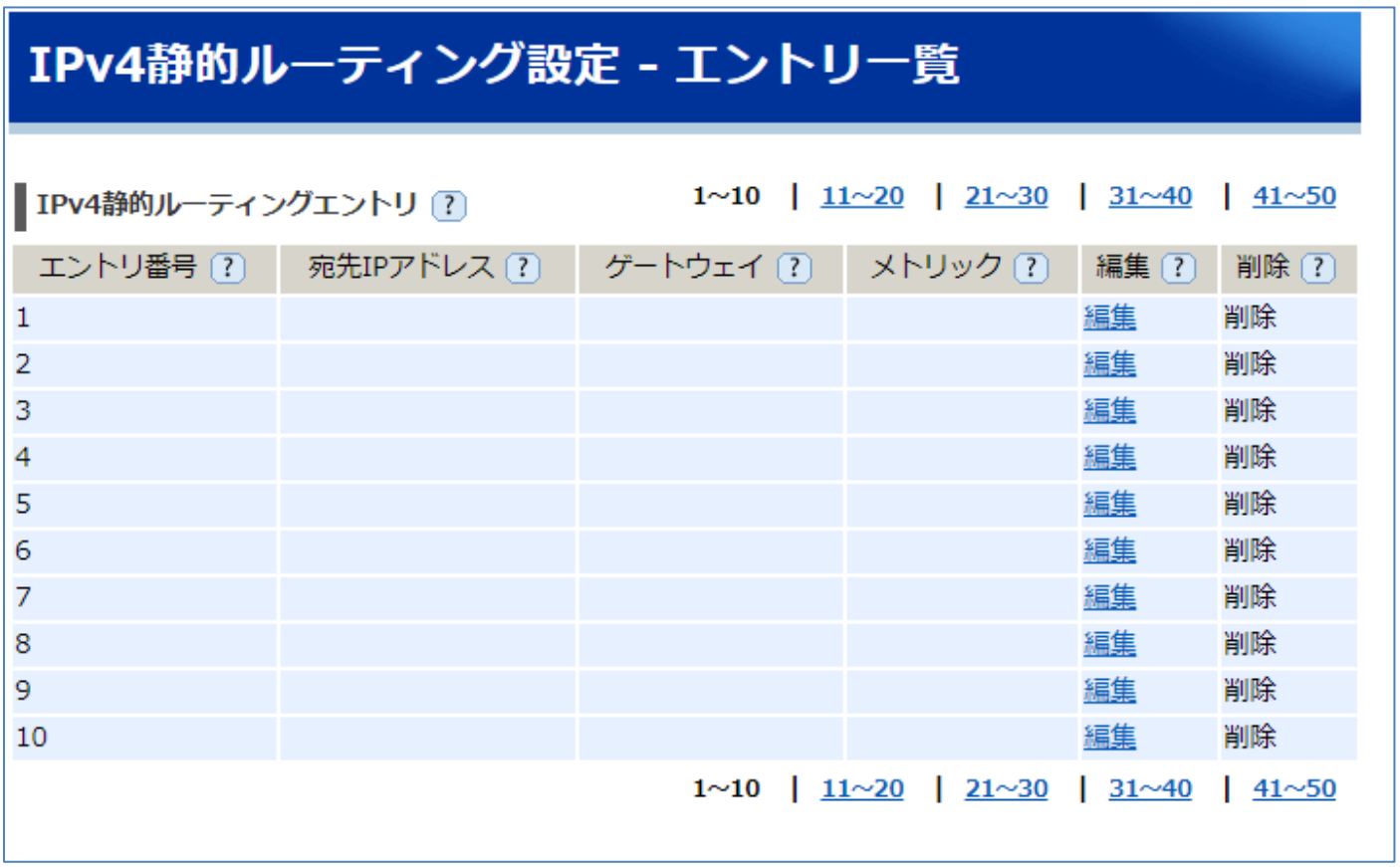
その他の設定項目の説明はメンテナンス（ルータモード）の 5.7.8 章を参照してください。

5.6.4. **WPS 設定**

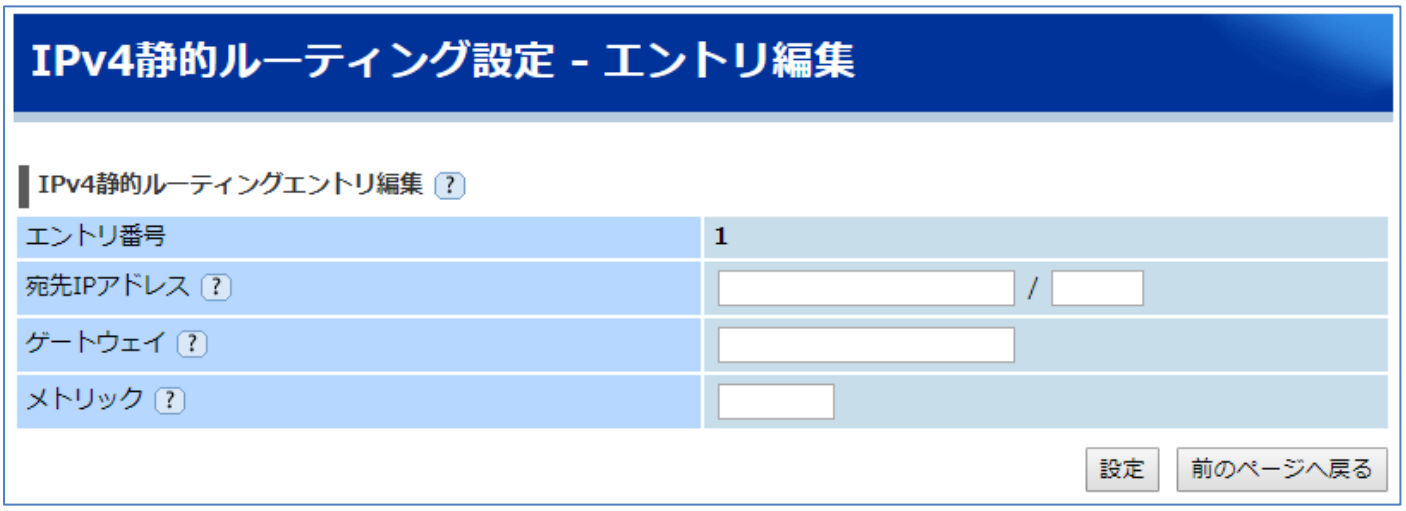
メンテナンス（ルータモード）と同じです。5.7.9 章を参照してください。

5.6.5. **IPv4 静的ルーティング設定**

静的ルーティングエントリを最大 50 エントリ追加できます。



1. [TOP]-[メンテナンス]-[ネットワーク設定]-[IPv4 静的ルーティング設定]画面を開きます。
2. 「編集」をクリックすると下記画面に遷移します。



3. ルーティングエントリ情報を設定します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
IPv4 静的ルーティングエントリ編集		50 エントリ設定できます。	
エントリ番号	エントリの番号が入ります。		未設定
宛先 IP アドレス	ルーティングエントリの宛先ネットワークを指定してください。		未設定
ゲートウェイ	ゲートウェイの IPv4 アドレスを設定してください。		未設定
メトリック	メトリック値を指定してください。 設定範囲は、1~255 です。	優先させたいルーティングエントリは、メトリック値を小さくします。	未設定

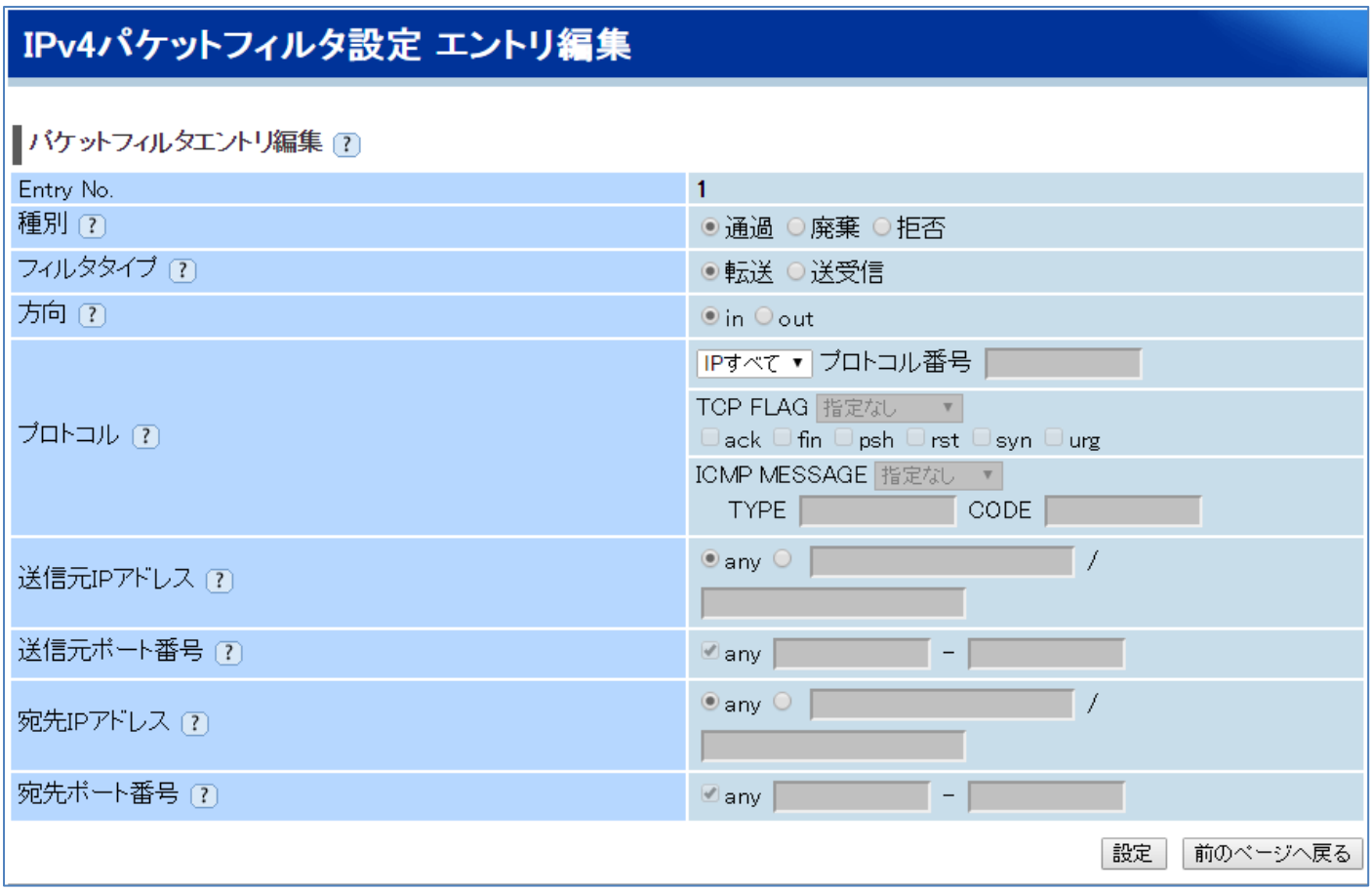
※マッチするエントリの内、より小さいサブネットの宛先 IP アドレスをもつエントリが優先して適用されます。サブネットが同一の場合は、メトリック値が小さいエントリが優先して適用されます。

5.6.6. **IPv4 パケットフィルタエントリに関する設定**

特定の条件を満たすパケットの通過や廃棄を設定できます。[18]

本機能はブリッジモードとルータモード共通の機能です。ブリッジモードでは対象インタフェースの選択がないという点だけ異なります。

1. [TOP]-[メンテナンス]-[フィルタ設定]- [IPv4 パケットフィルタ設定]画面を開きます。
2. 「編集」をクリックすると下記画面に遷移し、そのエントリのフィルタ設定を行います。



3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

[18] 初期状態で IPv4 パケットフィルタエントリを設定しています。変更、削除は可能ですが、そのまま利用していただくことを推奨します。

設定項目	値	備考	初期値
パケットフィルタエントリ編集		フィルタリングポイントごとに 50 エントリ設定できます。	
エントリ番号	エントリの番号が入ります。	エントリ番号 1 は初期状態で IPv4 パケットフィルタエントリを設定しています。変更、削除は可能ですが、そのまま利用していただくことを推奨します。	
種別	• 通過…本エントリに合致する IP パケットを通過 • 廃棄…本エントリに合致する IP パケットを廃棄（silently discard） • 拒否…本エントリに合致する IP パケットに対してエラーメッセージを送信 ・TCP: TCP reset を送信 ・TCP 以外: ICMP destination unreachable を送信		通過
フィルタタイプ	• 転送…本製品宛て以外の IP パケット • 送受信…本製品宛ての IP パケット		転送
方向	• in…本製品が受信する IP パケット • out…本製品が送信する IP パケット		in
プロトコル	• IP すべて…すべての IP パケット • ICMP • TCP • UDP • その他…上記以外の IP パケット（プロトコル番号で指定してください） • TCP FLAG…TCP パケットのうち、特定フラグの TCP パケットのみ対象にする場合に選択 • ICMP MESSAGE…ICMP パケットのうち、特定の ICMP メッセージのみ対象にする場合に選択		IP すべて
送信元 IP アドレス	• any…すべてを対象とする場合 • アドレス指定…特定の IP アドレスを指定する場合		any
送信元ポート番号	• any…すべてを対象とする場合 • ポート番号指定…特定のポートを指定する場合		未設定
宛先 IP アドレス	• any…すべてを対象とする場合 • アドレス指定…特定の IP アドレスを指定する場合		any
宛先ポート番号	• any…すべてを対象とする場合 • ポート番号指定…特定のポートを指定する場合		未設定

5.6.7. **MAC アドレスフィルタリングに関する設定**

特定の LAN 側端末のみ本製品と接続できるようにする機能です。

有線 LAN と無線 LAN それぞれ 60 エントリずつ登録することができます。

対象種別を選択し、「選択」ボタンを押下すると MAC アドレスエントリ画面が切り替わります。

■有線 LAN の MAC アドレスフィルタリング画面

1. [TOP]-[メンテナンス]-[フィルタ設定]-[MAC アドレスフィルタリング]画面を開きます。
2. 対象種別を選択で「有線 LAN」を選択します。
3. 「編集」をクリックしてエントリ編集画面に遷移し、接続を許可する有線の MAC アドレスを追加します。
4. MAC アドレスフィルタリング機能の「使用する」をチェックします。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
MAC アドレスフィルタリング			
対象種別を選択	• 有線 LAN…有線 LAN インタフェースの MAC アドレスフィルタリングを設定する場合に選択します。 • 無線 LAN…無線 LAN インタフェースの MAC アドレスフィルタリングを設定する場合に選択します。		有線 LAN
MACアドレスフィルタリング設定	MAC アドレスフィルタリング機能を有効にする場合、チェックします。	エントリがひとつもない状態だとチェックできません。	無効

※コメント欄はデバイス管理画面で LAN 端末に設定したコメントが表示されます。本製品のデバイス管理方式が MAC モードのときにコメントが表示されます。IP モードに変更した場合はコメントが削除されます。コメント欄の設定は 5.9.3 章を参照してください。

■無線 LAN の MAC アドレスフィルタリング画面

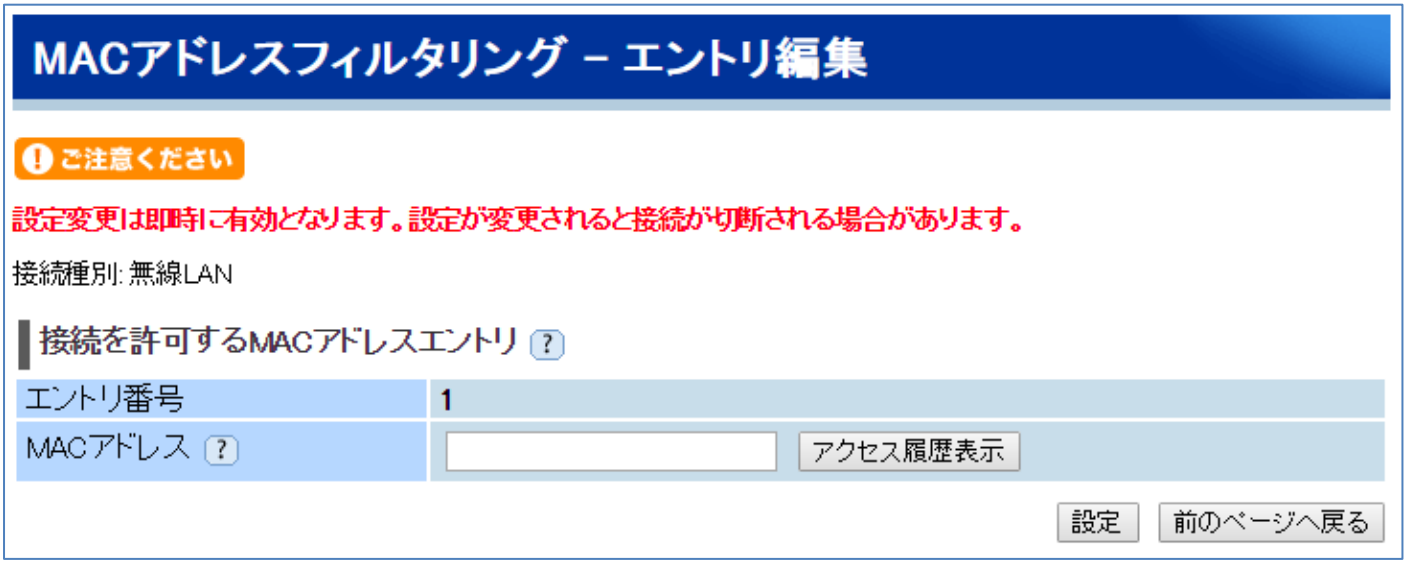
1. [TOP]-[メンテナンス]-[フィルタ設定]-[MAC アドレスフィルタリング]画面を開きます。
2. 対象種別を選択で「無線 LAN」を選択します。
3. 「編集」をクリックしてエントリ編集画面に遷移し、接続を許可する無線の MAC アドレスを追加します。
4. MAC アドレスフィルタリング機能を有効にする SSID をチェックします。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
MAC アドレスフィルタリング			
対象種別を選択	• 有線 LAN…有線 LAN インタフェースの MAC アドレスフィルタリングを設定する場合に選択します。 • 無線 LAN…無線 LAN インタフェースの MAC アドレスフィルタリングを設定する場合に選択します。		有線 LAN
有効にする SSID	• プライマリ SSID…プライマリ SSID に対して設定する場合、チェックします。 • セカンダリ SSID…セカンダリ SSID に対して設定する場合、チェックします。		無効

※コメント欄はデバイス管理画面で LAN 端末に設定したコメントが表示されます。コメント欄の設定は 5.9.3 章を参照してください。

■MAC アドレスフィルタリング エントリ編集画面

画面は無線 LAN のエントリ編集画面です。有線 LAN のエントリ編集画面も同じです。



1. 接続を許可する LAN 端末の MAC アドレスを入力します。
   「アクセス履歴表示」ボタンを押して、アクセス履歴のある MAC アドレスリストから選択することもできます。
2. 「設定」ボタンを押下します。
3. 「保存」ボタンを押下して、本設定を保存します。

設定項目	値	備考	初期値
MAC アドレスフィルタリングエントリ編集		有線 LAN と無線 LAN それぞれ 60 エントリずつ登録できます。	
エントリ番号	エントリの番号が入ります。		未設定
MAC アドレス	接続を許可する LAN 端末の MAC アドレスを入力します。		未設定

※「アクセス履歴表示」ボタンをクリックすると、本製品へのアクセス履歴を表示します。

5.6.8. **Ethernet ポート設定**

本製品は、WAN ポートと LAN ポートの通信モード、メディアタイプ、およびフロー制御を設定できます。通信モード、メディアタイプの初期値は自動設定（Auto Negosiation）です。お客様のご使用になる環境において、固定設定が必要な場合にご利用ください。

1. [TOP]-[メンテナンス]-[詳細設定]-[その他の設定]画面を開きます。
2. Ethernet ポートの WAN ポートと LAN ポート 1～LAN ポート 4 の通信速度/通信モードと MDI/MDI-X、フロー制御を設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
通信速度/通信モード	通信モードを以下から選択します。 - 自動設定(Auto Negosiation) - 1000Mbps/全二重 - 100Mbps/全二重 - 100Mbps/半二重 - 10Mbps/全二重 - 10Mbps/半二重	WAN ポートと LAN ポート 1～LAN ポート 4 の設定可能項目は同じです。 お客様の環境に合わせて設定ください。	自動設定
MDI/MDI-X	MDI/MDI-X モードを以下から選択します。 - 自動設定 - MDI - MDI-X	WAN ポートと LAN ポート 1～LAN ポート 4 の設定項目は同じです。 お客様の環境に合わせて設定ください。	自動設定
フロー制御	• チェック有…フロー制御を使用する場合 • チェック無…フロー制御を使用しない場合	WAN ポートと LAN ポート 1～LAN ポート 4 の設定可能項目は同じです。 お客様の環境に合わせて設定ください。	無効 ※1

※1：フロー制御はファームウェアバージョン 3.4.31 にて初期値を無効にしました。

[メモ]

- 「設定」ボタンを押下すると Ethernet ポートが一旦リンクダウンします。
- フロー制御は Ethernet ポートに接続する機器が IEEE 802.3x Pause フレームに対応している場合にのみ動作します。
- フロー制御が動作するポートと動作しないポートが混在する場合、通信速度が低下する可能性があります。

5.6.9. **NetMeister 設定**

本製品で NetMeister 機能をご利用になる場合、本画面で設定します。

※画面は NetMeister 機能を使用する場合の設定例です。

1. [TOP]-[管理設定]-[NetMeister 設定]-画面を開きます。
2. ご利用環境に応じた NetMeister の設定を入力します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、本設定を保存します。

設定項目	値	備考	初期値
基本設定			
NetMeister 機能	• チェック有…NetMeister 機能を使用する場合 • チェック無…NetMeister 機能を使用しない場合		無効
ホスト名（装置名）	NetMeister で管理する装置のホスト名を入力	使用可能文字：アスキーコードで 0x21-0x7e（ただし、” を除く） 入力可能文字数：2～63	未設定
IPv4 アドレス	本製品の IP アドレスを表示	本画面では入力できません。	–
ポート番号	本製品が待ち受けに使用するポート番号を入力	443,1024～65535 1024 以降を入力した場合、入力した値によっては使用できない場合があります。	443
グループ ID	NetMeister に登録したグループ ID を入力	使用可能文字：アスキーコードで 0x2d,0x30-0x39,0x61-0x7a 入力可能文字数：2～63 先頭と末尾に - は使用できません。	未設定
グループパスワード	NetMeister に登録したグループパスワードを入力	使用可能文字：アスキーコードで 0x21-0x7e（ただし、”?¥ を除く） 入力可能文字数：8～31	未設定
親機設定			
[親機 1] IPv4 アドレス	1 台目の親機の IP アドレスを入力		未設定
[親機 1] ポート番号	1 台目の親機のポート番号を入力	1～65535	443
[親機 2] IPv4 アドレス	2 台目の親機の IP アドレスを入力	2 台目の親機の設定は省略可能です。 NetMeister との接続を冗長化する場合に設定します。	未設定
[親機 2] ポート番号	2 台目の親機のポート番号を入力	1～65535	443
オプション設定			
アラーム通知	• チェック有…アラーム通知を使用する場合 • チェック無…アラーム通知を使用しない場合	NetMeister 上で本製品のアラームを表示する場合に有効にします。	有効
脅威統計通知	• チェック有…脅威統計通知を使用する場合 • チェック無…脅威統計通知を使用しない場合	NetMeister 上で本製品のセキュリティ・スキャン機能で検出した脅威、通信に関するレポートを表示する場合に有効にします。	有効
UTM 脅威分析	• チェック有…UTM 脅威分析を使用する場合 • チェック無…UTM 脅威分析を使用しない場合	NetMeister 上でセキュリティログを閲覧する場合に有効にします。設定を有効にした時点からのセキュリティログを NetMeister 上で閲覧できます。ログ	無効

			の反映には 5 分程度のタイムラグが発生します。	
	リモートログイン機能	• チェック有…リモートログイン機能を使用する場合 • チェック無…リモートログイン機能を使用しない場合	NetMeisterのリモートログイン機能による本製品への接続を許可する場合は有効にします。リモートログイン機能を使用するには、NetMeister 親機がインターネットから直接アクセス可能な装置である必要があります。	無効

5.6.10. **SNMP エージェントの設定**

SNMP を使用して、本製品の状態を監視、制御できます。

本製品がサポートしている SNMP のバージョンは、バージョン 1 とバージョン 2c です。

ブリッジモードで SNMP エージェント機能に対応しています。設定項目はルータモード時と同じです。詳細は 5.7.19 章を参照してください。

[注意]

ブリッジモードの WAN ポートはデフォルトで ICMP のフィルタが入っています。そのため、WAN 側にある SNMP マネージャから探索した場合、ICMP に応答しないので、SNMP エージェントとして見つかりません。この場合は、5.6.6 章を参考に通過フィルタを設定してください。

5.6.11. **ログ送信設定**

本製品でログ送信機能をご利用になる場合、本画面で設定します。

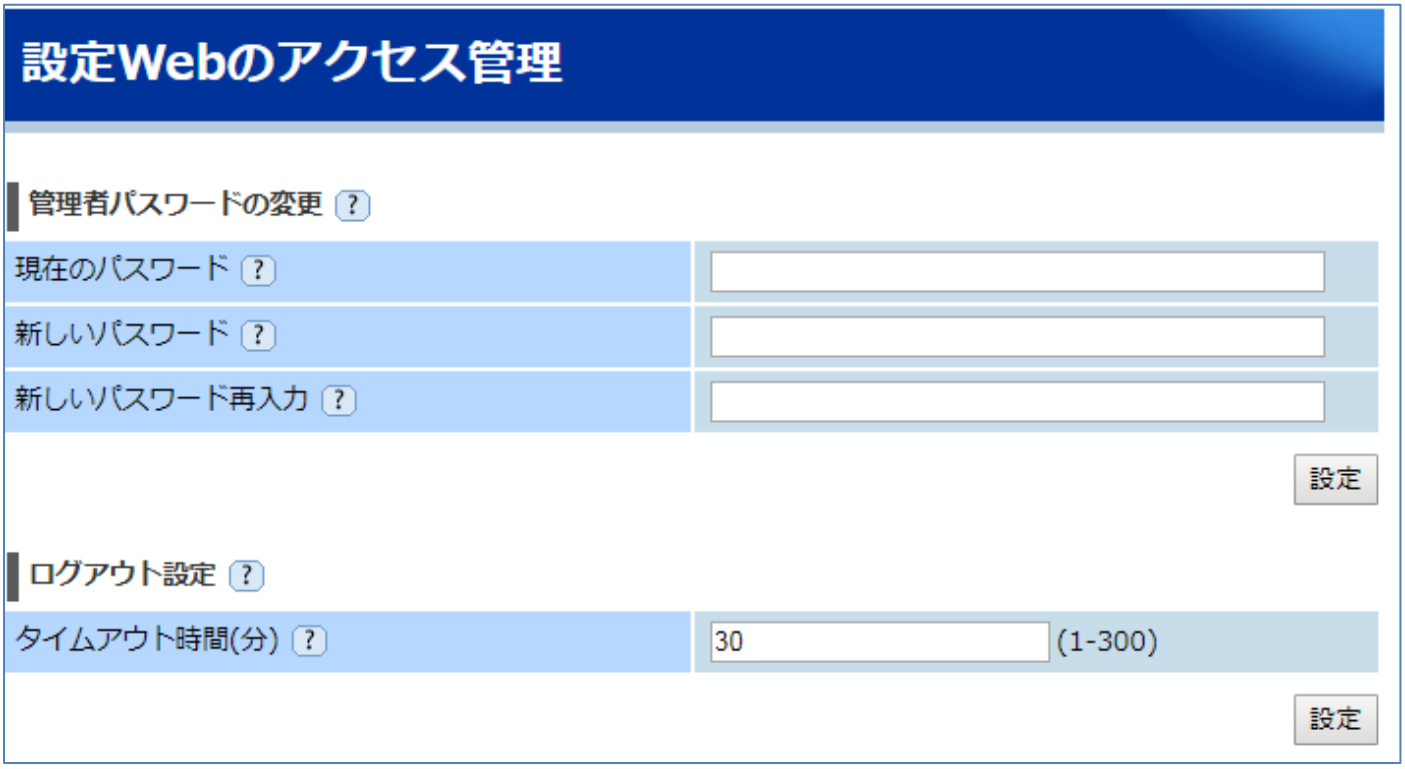
1. [TOP]-[管理設定]-[ログ送信設定]-画面を開きます。
2. ご利用環境に応じたログ送信の設定を入力します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、本設定を保存します。

設定項目	値	備考	初期値
ログ送信設定			
ログ送信機能	• チェック有…ログ送信機能を使用する場合 • チェック無…ログ送信機能を使用しない場合		無効
Syslog サーバアドレス	Syslog サーバの IP アドレスを入力		未設定
Syslog サーバポート番号	Syslog サーバのポート番号を入力	1～65535	514
送信設定			
イベントログ	• チェック有…イベントログを送信する場合 • チェック無…イベントログを送信しない場合		有効
ログレベル	イベント量 Emergency … 緊急 小 Alert … 警戒 Critical … 危機的 Error … エラー Warning … 警告 Notice … 通知 Informational … 情報提供 Debug … デバッグ 大	イベントログを送信するレベルを設定します。	Informational
セキュリティログ	• チェック有…セキュリティログを送信する場合 • チェック無…セキュリティログを送信しない場合		有効

5.6.12. **設定 Web のアクセス管理**

定期的に設定 Web にアクセスするパスワードを変更することを推奨します。

本製品にログインする際の管理者パスワード、ログアウトするまでの時間を設定（変更）します。



1. [TOP]-[メンテナンス]-[メンテナンス]-[設定 Web のアクセス管理]画面を開きます。
2. 管理者パスワードを変更します。
3. ログアウトのタイムアウト時間を設定します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、新しいパスワードを保存します。

※ 手順 5 実施後、ログイン用ユーザー名/パスワードの入力画面が表示されます（5.4 章参照）。新しいパスワードでログインしてください。

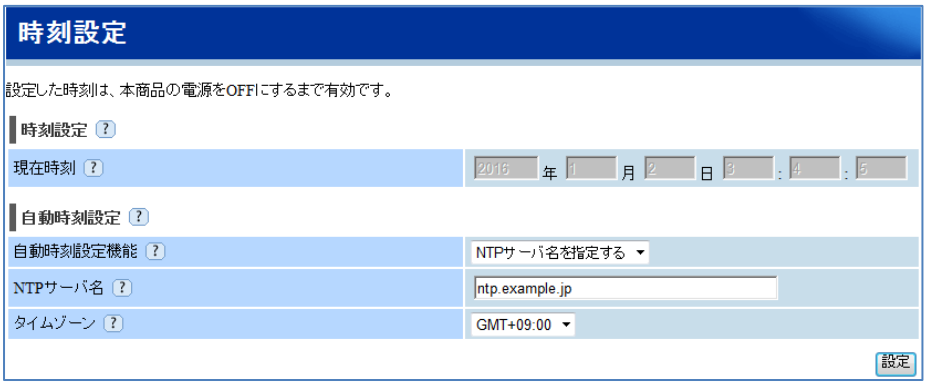
設定項目	値	備考	初期値
管理者パスワードの変更			
現在のパスワード	本製品へのログイン時に入力したパスワードを入力	使用可能文字は、半角文字 0～9,a～z,A～Z, -(ハイフン),_(アンダースコア)です。 入力可能文字数は、1～64 です。	未設定
新しいパスワード	新しいパスワードを入力	使用可能文字は、半角文字 0～9,a～z,A～Z, -(ハイフン),_(アンダースコア)です。 入力可能文字数は、1～64 です。	未設定
新しいパスワード再入力	設定項目「新しいパスワード」と同じ文字列を入力	使用可能文字は、半角文字 0～9,a～z,A～Z, -(ハイフン),_(アンダースコア)です。 入力可能文字数は、1～64 です。	未設定
ログアウト設定			
タイムアウト時間	設定 Web 上での最終操作後から自動ログアウトするまでの時間を入力	1～300 分	30 分

5.6.13. **時刻の設定**

本製品の時刻は、NTP サーバから時刻を取得します。

お客様で NTP サーバを指定する場合は、本章を参考に設定してください。NTP サーバ情報を 1 台設定できます。

本製品は、再起動時に時刻情報を保存しません（時刻情報をリセットします）。



[NTP サーバの変更]

1. [TOP]-[メンテナンス]-[メンテナンス]-[時刻設定]画面を開きます。
2. 自動時刻設定機能は「NTP サーバ名を指定する」を選択します。
3. NTP サーバのアドレスを入力します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

[タイムゾーンの変更]

1. [TOP]-[メンテナンス]-[メンテナンス]-[時刻設定]画面を開きます。
2. 自動時刻設定機能は「NTP サーバ名を指定する」を選択します。
3. タイムゾーンを変更します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

[NTP サーバを使用しない場合]

1. [TOP]-[メンテナンス]-[メンテナンス]-[時刻設定]画面を開きます。
2. 自動時刻設定機能は「使用しない」を選択します。
3. 現在時刻に時刻を入力します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

[メモ]

本製品の時刻は、再起動で初期値（2015/11/14 00:00:00）に戻ります。

NTP サーバを使用せず、設定 Web で装置時刻を設定している場合は、本製品を起動するたびに時刻設定してください。

設定項目	値	備考	初期値
自動時刻設定			
自動時刻設定機能	• 使用しない…NTPサーバを使用しない場合 • NTP サーバ名を指定する…NTP サーバを使用する場合	NTP サーバを使用しない場合、本製品の時刻は現在時刻欄に入力している時刻に設定されます。	NTP サーバ名を指定する
NTP サーバ名	NTP サーバ名を設定してください。	NICT 公開 NTP サービスの NTP サーバを指定しています。	ntp.nict.jp
タイムゾーン	タイムゾーンを選択してください。		GMT+09:00

5.6.14. 設定値の保存、復元

設定 Web で設定した設定値をパソコンなどに保存できます。

保存した設定値を本製品に復元することができます。

[設定値の保存]

1. [TOP]-[メンテナンス]-[メンテナンス]-[設定値の保存＆復元]画面を開きます。
2. 「ファイルへ保存」をクリックし、設定値を保存します。

[設定値の復元]

1. [TOP]-[メンテナンス]-[設定値の保存＆復元]画面を開きます。
2. 「設定ファイル」に 設定値の保存 で保存した設定値（bin ファイル）を入力し、「設定値の復元」ボタンを押下します。
3. 設定値を復元した後、本製品は再起動します。再起動完了で設定値の復元は完了です。

[メモ]

セキュリティ・スキャン機能は、完全に復元できない場合があります。パソコンに保存した設定値は、古いバージョンのファームウェアの装置には復元できません。

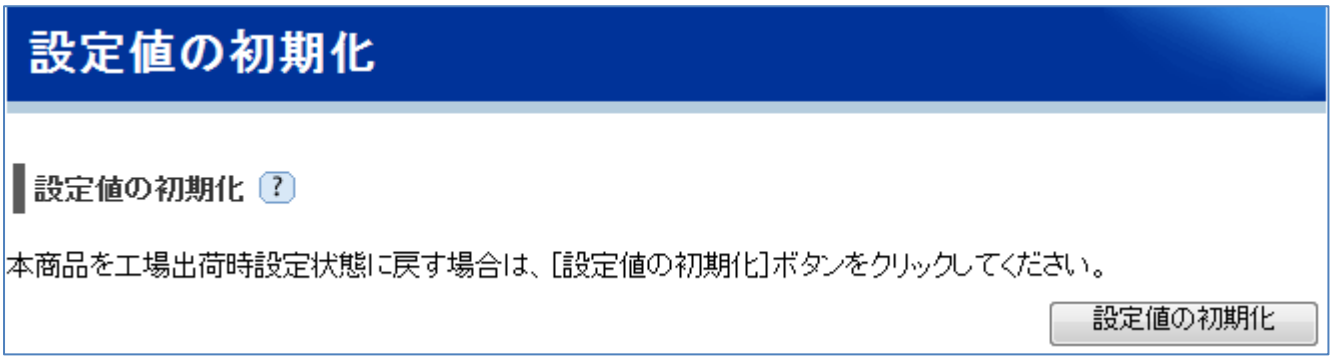
[USB ストレージへの設定値の保存機能設定]

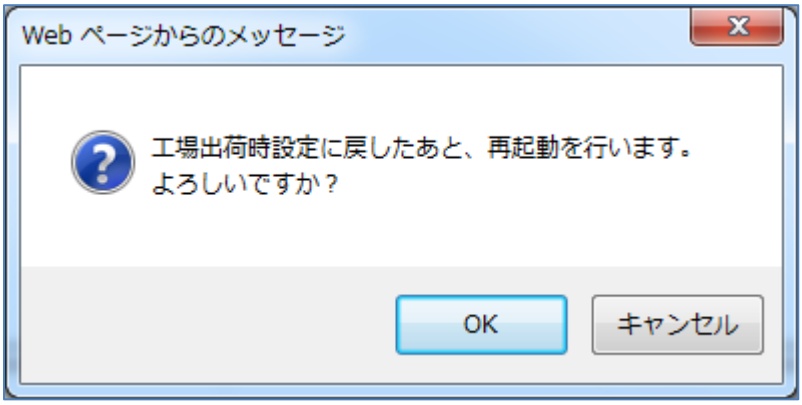
1. [TOP]-[メンテナンス]-[設定値の保存＆復元]画面を開きます。
2. USB ストレージへの設定値の保存機能を有効にする場合は「USB ストレージへの設定値の保存機能」の「使用する」をチェックします。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	説明	初期値
USB ストレージへの設定値の保存機能設定	USB ストレージへの設定値の保存機能を使用する場合は、本項目をチェックします。	無効

5.6.15. **設定値の初期化**

設定 Web で、設定値を初期状態に戻すことができます。





1. [TOP]-[メンテナンス]-[メンテナンス]-[設定値の初期化]画面を開きます。
2. 「設定値の初期化」ボタンを押下します。
3. 再起動する旨のメッセージウィンドウを表示しますので、「OK」ボタンを押下します。[19]
4. 本製品は自動的に再起動します。

[メモ]

アクティベーションした内容は初期状態に戻りません。このため、再度アクティベーションする必要はありません。

シグネチャは初期状態に戻ります。

セキュリティログ、統計情報、イベントログは削除されます。

スイッチ操作でも設定値を初期化できます。初期化する内容は設定 Web での初期化操作と同じです。

スイッチ操作による設定値の初期化は 5.10.1 章を参照してください。

[19] 「キャンセル」ボタンを押下した場合、設定値を初期化しません。

5.6.16. **ファームウェアの更新**

本製品のファームウェアは、次の方法で更新できます。

本製品に関するお客様の運用ポリシーにしたがい、ファームウェア更新方法を設定してください。

更新方法	説明
メンテナンスバージョンアップ機能を使用してファームウェアを更新	本製品が管理サーバに定期的にアクセスし、新しいファームウェアの有無を確認します。 新しいファームウェアの有無の確認タイミングについては、3.4.1 章を参照してください。 新しいファームウェアがある場合、本製品の INFO ランプが橙点灯します。 本機能での更新には、次の方法があります。 ● INFO ランプが橙点灯後に INFO ランプが緑点滅するまで OPT2 スイッチを 3 秒以上押し続ける方法 ● 設定 Web の[TOP]画面の「ファームウェア更新」ボタンを押下する方法 ● 時刻指定バージョンアップに時刻指定して、自動更新する方法 本機能の初期値は有効です。
設定 Web を使用して手動でファームウェアを更新	本製品のファームウェアの更新を設定 Web で実施します。 ● オンラインバージョンアップ機能を使用してファームウェアを更新 ● 「ローカルファイル指定」の更新はファームウェアバージョン 3.5.12 にて選択できないように変更しました。
OPT2 スイッチを使用してファームウェアを更新	設定 Web を使わずにスイッチ操作でファームウェア更新を行うこともできます。更新方法は 5.10.4 章を参照してください。

[メモ]

メンテナンスバージョンアップ機能について

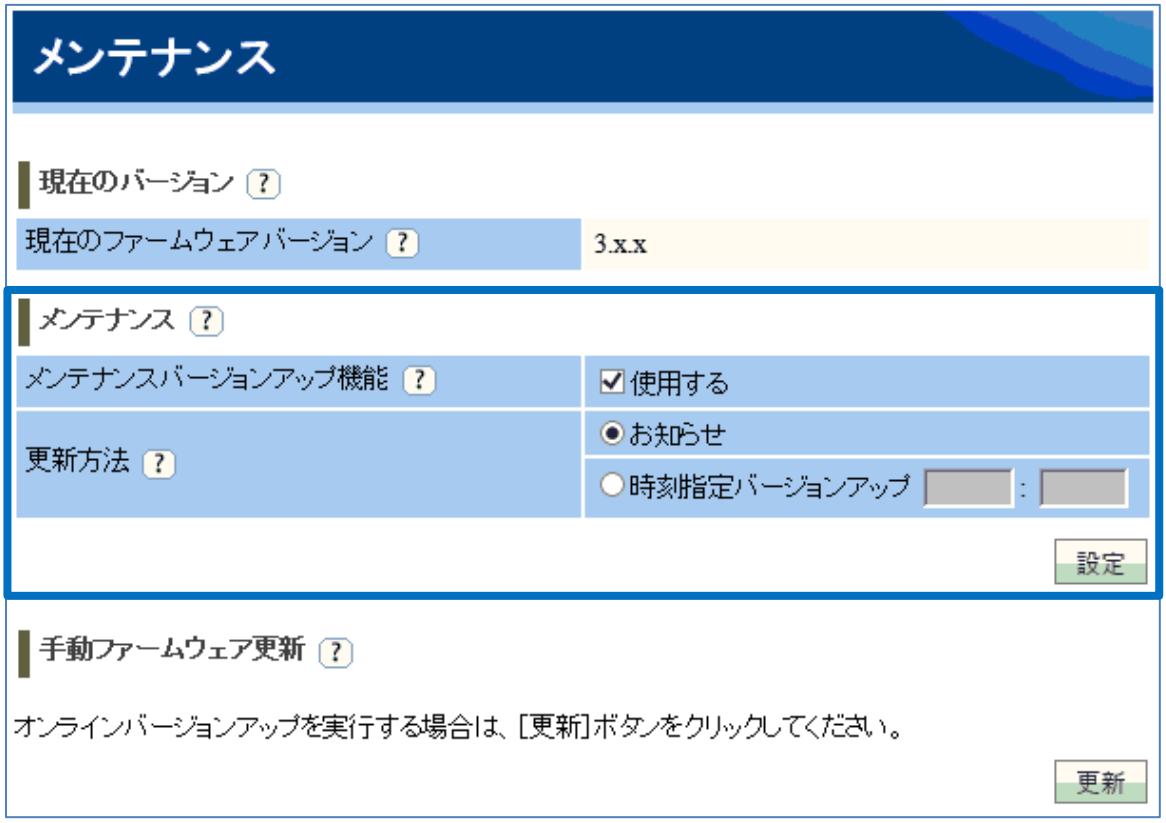
- 本機能が動作するために必要な最小限度の機器情報、ネットワーク情報を当社が運用する管理サーバに通知します。[20]
- 特定事由により、お客様の意図しないタイミングでファームウェアを自動更新する場合があります（ファームウェアの更新は本製品の再起動を伴います）。
- メンテナンスバージョンアップ機能を「使用しない」場合、新しいファームウェアの有無の確認、および、ファームウェアの自動更新を実施しません。

時刻指定バージョンアップについて

- 新しいファームウェアがある場合、本製品のファームウェアを指定した時刻から 1 時間以内に自動更新します。

[20] これらの情報は、本機能の実現と、本製品や本機能の改善、向上のためだけに利用し、これ以外の目的では利用しません。また、これらの情報は当社の取り扱い手続きに則り、適切に管理します。当社が第三者と連携して本機能を利用する場合につきましても、当社の取り扱い手続き同様に適切に管理します。

■メンテナンスバージョンアップ機能を使用する場合



[設定]

1. [TOP]-[メンテナンス]-[メンテナンス]-[メンテナンス]画面を開きます。
2. メンテナンスバージョンアップ機能を「使用する」にチェックを付けます（初期値は、チェックが付いています）。
3. 更新方法として「お知らせ」か「時刻指定バージョンアップ」を選択します。「時刻指定バージョンアップ」の場合は、自動更新させたい任意の時刻を設定します。設定範囲は、0:00～23:59 です。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

[ファームウェアの更新①]：「お知らせ」を選択し、OPT2 スイッチで更新する場合

1. 新しいファームウェアがある場合、本製品の INFO ランプが橙点灯します。
2. 本製品の OPT2 スイッチを 2 秒以上押し続けます。
3. ファームウェアの更新が始まると INFO ランプが橙点滅します。
   橙点滅したら、OPT2 スイッチを放してください。
4. ファームウェアの更新が完了すると、本製品は自動的に再起動します。
5. 本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

※ファームウェアの更新に失敗した場合、INFO ランプは橙点灯に戻ります。

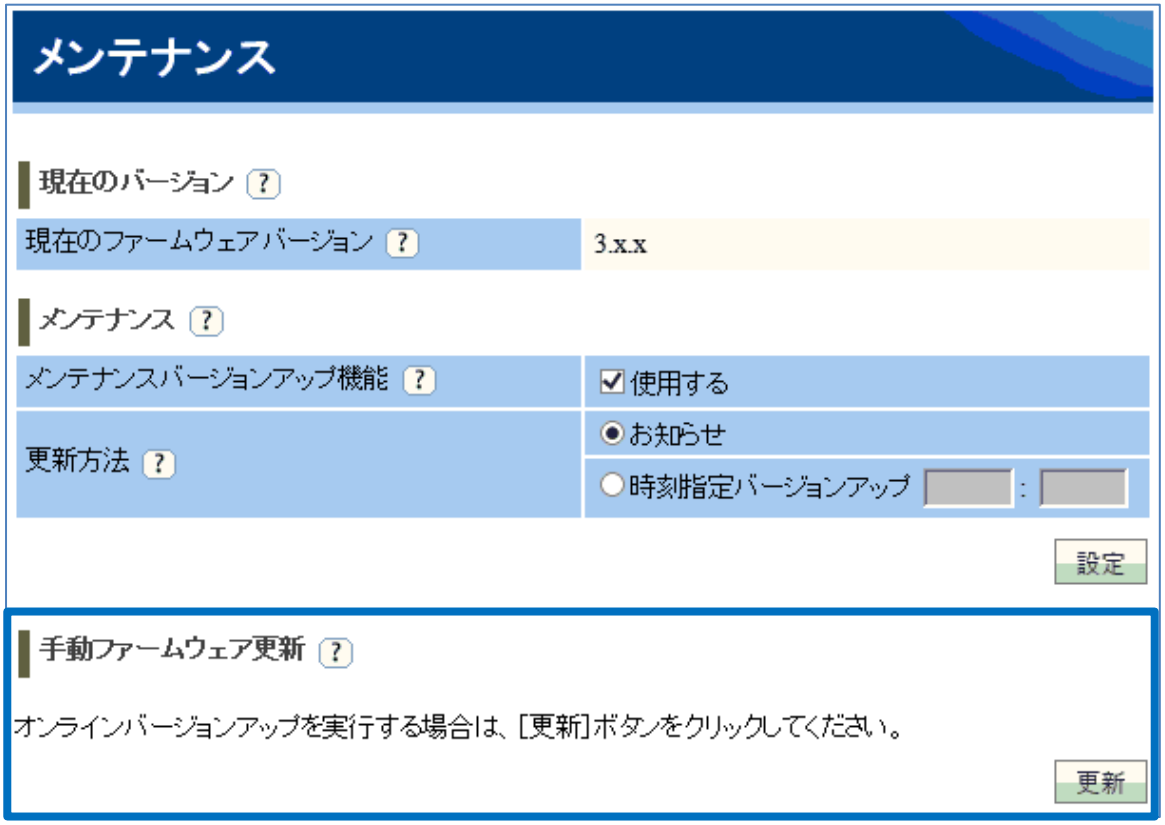
[ファームウェアの更新②]：「お知らせ」を選択し、設定 Web で更新する場合

1. 新しいファームウェアがある場合、本製品の INFO ランプが橙点灯します。
2. 設定 Web にアクセスします。
3. [TOP]画面の「ファームウェア更新」ボタンを押下します。
4. ファームウェアの更新が完了すると、本製品は自動的に再起動します。
5. 本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

[ファームウェアの更新③]:「時刻指定バージョンアップ」を選択した場合

1. 本製品が管理サーバにアクセスしたタイミングで新しいファームウェアがあると、本製品の INFO ランプが橙点灯します。このとき、本製品は管理サーバから新しいファームウェアをダウンロードします。
2. 「時刻指定バージョンアップ」で指定した時刻になりますと、指定した時刻から 1 時間以内に自動的にファームウェアを書き換えます。
3. ファームウェアの更新が完了すると、本製品は自動的に再起動します。
4. 本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

■設定 Web を使用して手動でバージョンアップする場合（オンラインバージョンアップ）



[設定]

1. [TOP]-[メンテナンス]-[メンテナンス]画面を開きます。
2. 「ファームウェア更新」の「更新」ボタンを押下します。
3. 「最新のバージョン」を表示するまで、そのまましばらく待ちます。
4. 「最新のバージョン」の数字が新しい場合は、「最新バージョンへ更新」ボタンを押下します。
   「現在のバージョン」と「最新のバージョン」が同じ場合はここで終了です。
5. 「OK」ボタンを押下します。
6. しばらくすると、画面に「ファームウェアを更新しています。しばらくしてから、再度、アクセスしてください。」と表示されます。
7. ファームウェアの更新が完了すると、本製品は自動的に再起動します。
8. 本製品が再起動し、NETWORK ランプが点灯していれば、ファームウェアの更新は完了です。

[メモ]

- ファームウェア更新中は電源を OFF しないでください。故障の原因となります。
- ファームウェアのバージョンアップでは、設定値を引き継ぎます。

5.6.17. **再起動**

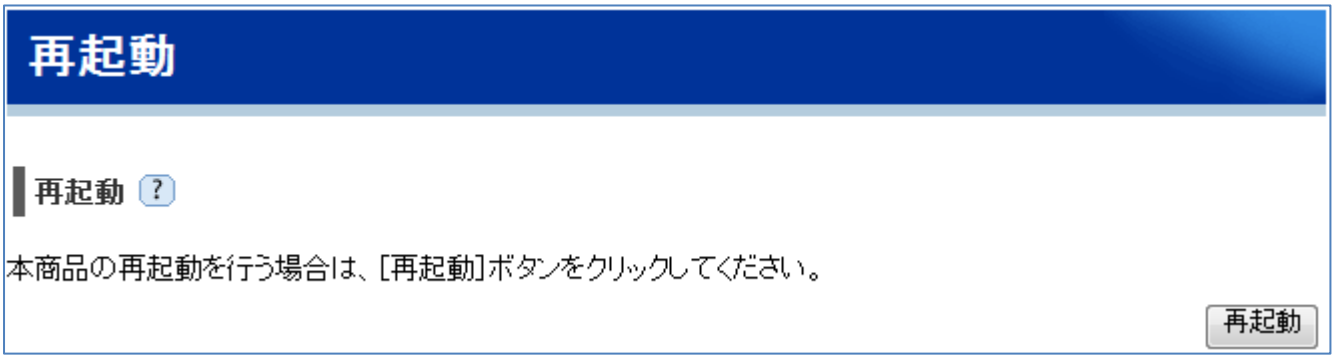
設定 Web で、本製品を再起動することができます。

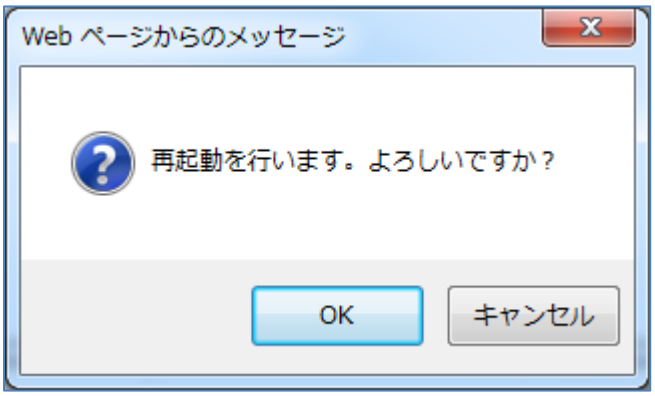
FlashROM に保存していない設定値がある場合、設定値の保存を促すメッセージを表示します。必要に応じて「保存」ボタンを押下し、設定値を FlashROM に保存してください。

[メモ]

本製品は次のタイミングでも再起動します。

- 設定値の初期化
- 設定値の復元
- ファームウェアの更新
- ブリッジモード ⇔ ルータモードの切り替え
- 設定 Web でデバイス管理モードの変更





1. [TOP]-[メンテナンス]-[メンテナンス]-[再起動]画面を開きます。
2. 「再起動」ボタンを押下します。
3. 再起動する旨のメッセージウィンドウを表示しますので、「OK」ボタンを押下します。
4. 本製品が再起動します。
5. 「再起動が完了しました」画面がポップアップしたら、「OK」ボタンを押下します。
6. 再起動は完了です。

5.6.18. **保守機能**

[保守機能設定]

設定 Web で、保守者が使用する保守機能を有効にすることができます。通常は無効のままでお使いください。保守機能をご使用になるには、保守アカウントが別途必要となります。

1. [TOP]-[メンテナンス]-[保守機能]画面を開きます。
2. 保守機能を有効にする場合は「保守機能」の「使用する」をチェックします。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

[装置状態の一括取得]

1. [TOP]-[メンテナンス]-[保守機能]画面を開きます。
2. 保守用のログ情報をパソコンなどに一括取得する場合は、「ファイルで取得」をクリックします。

装置状態の一括取得を行うと sa3500g_maintenance.zip というファイルを生成します。このファイルには、以下の情報が含まれます。

・セキュリティログ
・イベントログ
・統計情報
・本製品の設定ファイル
・運用中の固有情報であるファームウェアバージョンや製造番号

[解析情報出力]

1. [TOP]-[メンテナンス]-[保守機能]画面を開きます。
2. 「開始」ボタンをクリックすると、稼働中に解析情報が出力されるようになります。
3. 「停止」ボタンをクリックすると、解析情報の出力を停止します。

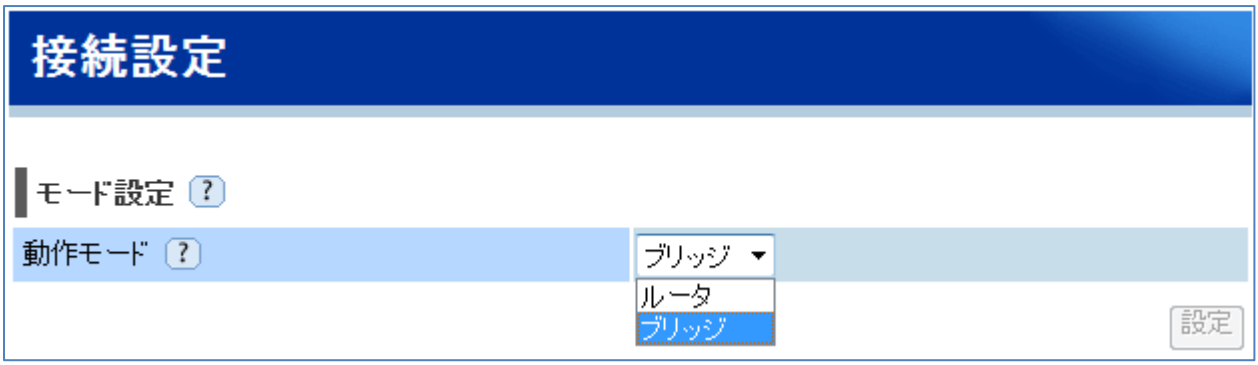
出力された解析情報は、装置状態の一括取得で生成されるファイルに含まれます。
「停止」ボタンのクリックのほか、装置が再起動した場合も解析情報の出力は停止されます。
本機能は保守担当者からの指示があった場合のみ実行してください。

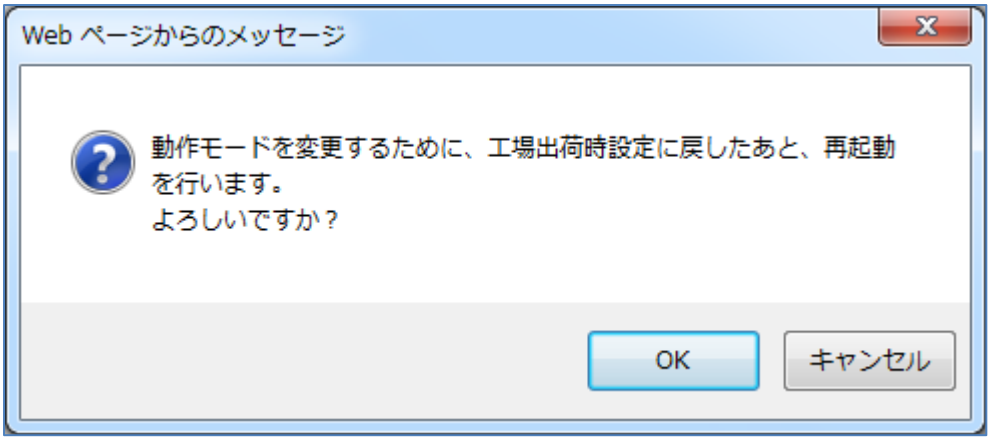
設定項目	説明	初期値
保守機能設定	保守機能を使用する場合は、本項目をチェックします。保守アカウントでの設定 Web ログインが可能になります。	無効
装置状態の一括取得	保守用のログ情報をパソコンなどに一括取得します。取得したログ情報は保守者向けの情報になります。	-
解析情報出力	装置稼働中に解析情報を内部出力します。装置状態の一括取得で、出力したファイルを取得できます。取得したファイルは保守者向けの情報になります。	停止

5.6.19. **ルータモードへの切り替え**

ルータモードに切り替える際、本製品を再起動します。

また、すべての設定を初期化します。





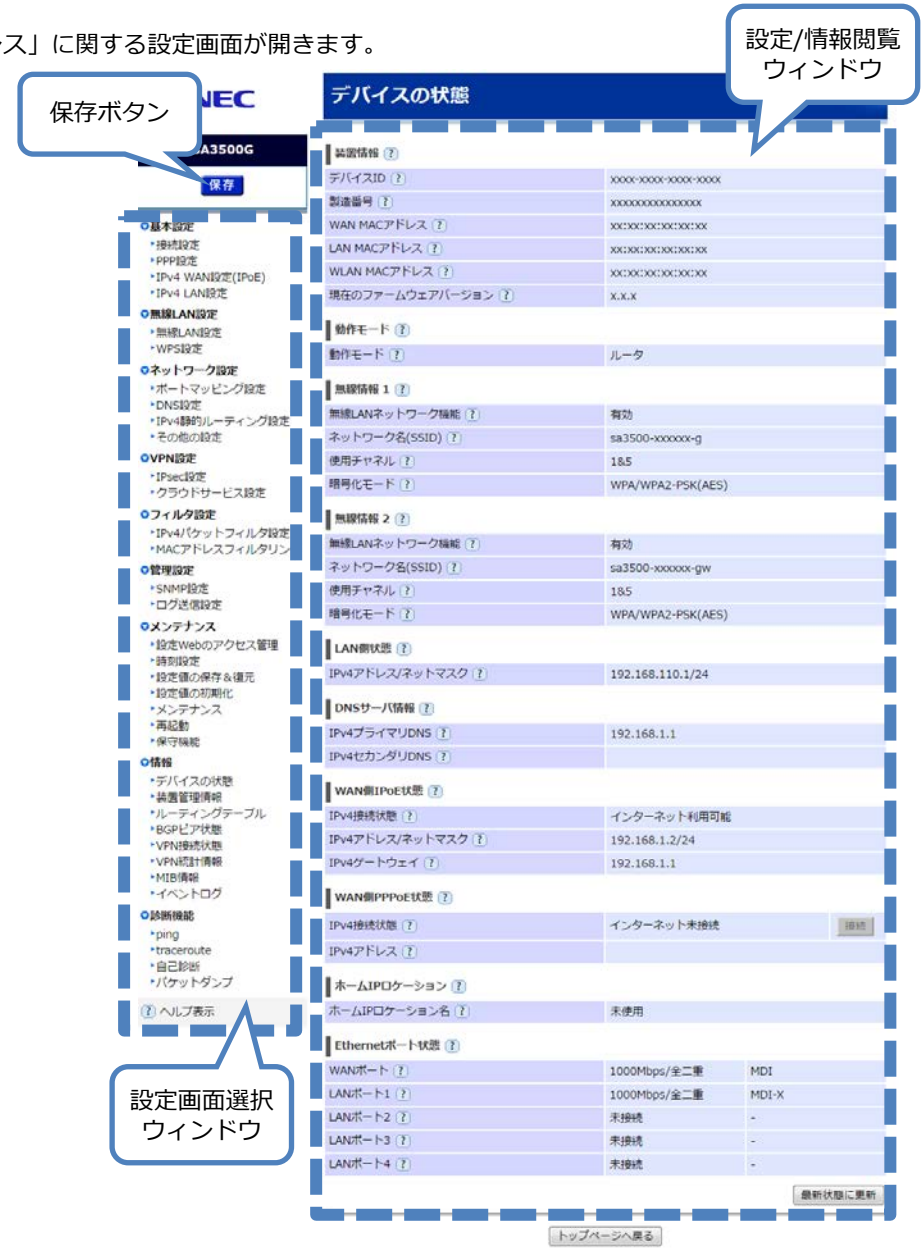
1. [TOP]-[メンテナンス]-[基本設定]-[接続設定]画面を開きます。
2. モード設定で「ルータ」を選択します。
3. 「設定」ボタンを押下します。
4. 再起動する旨のメッセージウィンドウを表示しますので、OK ボタンを押下します。
5. 再起動後、設定ウィザードの STEP2（管理者パスワード）が実行されます。5.2.2 章を参照し、設定してください。

5.7. メンテナンス（ルータモード）に関する設定

本製品のセキュリティ・スキャン機能以外の設定、および情報を閲覧します。

1. TOP ページで「メンテナンス」をクリックします。

2. 「メンテナンス」に関する設定画面が開きます。



5.7.1. **設定画面構成**

ルータモードのメンテナンスの設定画面構成は次のとおりです。

項目	説明	操作の必要性の有無/備考
メンテナンス（ルータモード）	ルータ、メンテナンスに関する設定	
基本設定	本製品のネットワークに関する設定	
接続設定	ブリッジモードへの切り替え WAN インタフェースの動作タイプの切り替え ※ブリッジモードへの切り替えは、本製品の再起動が必要です。	
PPP 設定	PPP の ID/パスワードの設定 PPP キープアライブの設定	
IPv4 WAN 設定（IPoE）	DHCP クライアントの設定 HTTP プロキシサーバの設定	
IPv4 LAN 設定	LAN インタフェースの IP アドレスの設定 DHCP サーバの設定	
無線 LAN 設定	無線 LAN に関する設定	
無線 LAN 設定	無線 LAN の設定	
WPS 設定	WPS 機能の有効/無効設定	
ネットワーク設定	本製品の静的ルーティングや DNS に関する設定	
ポートマッピング設定	ポートマッピングエントリの設定	
DNS 設定	DNS 機能の設定	
IPv4 静的ルーティング設定	静的ルーティングエントリの設定	
その他の設定	ICMP redirect パケット送信有無の設定	
VPN 設定	VPN 接続に関する設定	
IPsec 設定	IPsec/IKEv1/IKEv2 の設定	
クラウドサービス設定	クラウド接続を行う際の設定	
フィルタ設定	フィルタに関する設定	
IPv4 パケットフィルタ設定	IPv4 パケットフィルタエントリの設定	
MAC アドレスフィルタリング	MAC アドレスフィルタリングの設定	
管理設定	管理プロトコルに関する設定	
SNMP 設定	SNMPv1, SNMPv2c エージェントの設定	
メンテナンス	メンテナンスに関する設定	
設定 Web のアクセス管理	管理者パスワードの設定 自動ログアウト時間の設定	管理者パスワードは、定期的な変更を推奨します
時刻設定	本製品の時刻に関する設定	初期値を推奨します
設定値の保存＆復元	本製品の設定の保存、および、復元	設定変更したときは、設定値の保存を推奨します
設定値の初期化	本製品の設定の初期化の実行	
メンテナンス	ファームウェアに関する設定	必ず確認してください
再起動	再起動の実行	

	保守機能	保守機能の設定	保守者向けの機能を有効にする設定です
情報		本製品のバージョンや動作状況の表示	
	デバイスの状態	装置情報（デバイス ID、製造番号、MAC アドレス、バージョン情報） 動作モード 無線 LAN の状態 製品の IP アドレス	
	装置管理情報	DHCP サーバアドレスアドレス払い出し情報 Wi-Fi 帰属情報 ARP テーブル	
	ルーティングテーブル	本製品のルーティングテーブルの情報	
	BGP ピア状態	本製品が情報を交換する隣接ルータの情報	
	VPN 接続状態	IPsec SA、IKE SA の状態 IPsec SA、IKE SA の削除 証明書情報、証明書エクスポート	
	VPN 統計情報	IPsec トラフィックの統計情報	
	MIB 情報	SNMP MIB 情報	
	イベントログ	本製品の動作ログ	Ver3.2.45 で追加
診断機能		ネットワーク到達確認	
	ping	ping による到達確認の実施	
	traceroute	traceroute による経路確認の実施	
	自己診断	設定情報の確認、サーバへの到達確認の実施	
	パケットダンプ	本製品を通過するパケットのキャプチャを実施	

5.7.2. **LAN インタフェースの IP アドレス設定**

本製品の LAN インタフェースの IP アドレスを変更する場合などに設定します。

1. [TOP]-[メンテナンス]-[基本設定]-[IPv4 LAN 設定]画面を開きます。
2. お客様のネットワークに合わせて本製品の LAN インタフェースの IP アドレスを変更します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目		値	備考	初期値
IPv4 アドレス/ネットマスク			169.254.254.11/16 は、本製品の管理専用の IP アドレスです。	
	IPv4 アドレス/ネットマスク（ビット指定）	本製品の LAN インタフェースの IPv4 アドレスとサブネットマスクを設定してください。 サブネットマスクは、ビットで指定してください。	LAN インタフェースの IP アドレスを変更した場合は、本設定画面の「DHCP サーバ」の「割当アドレス」の設定も変更してください。 （5.7.7 章を参照してください）	192.168.110.1/24

5.7.3. **WAN インタフェースの IP アドレス設定**

本製品の WAN インタフェースの IP アドレスは、次の 3 とおりのいずれかの方法で設定します。

(a) 固定設定

(b) DHCP クライアント機能を使用して設定

(c) PPP 機能を使用して設定

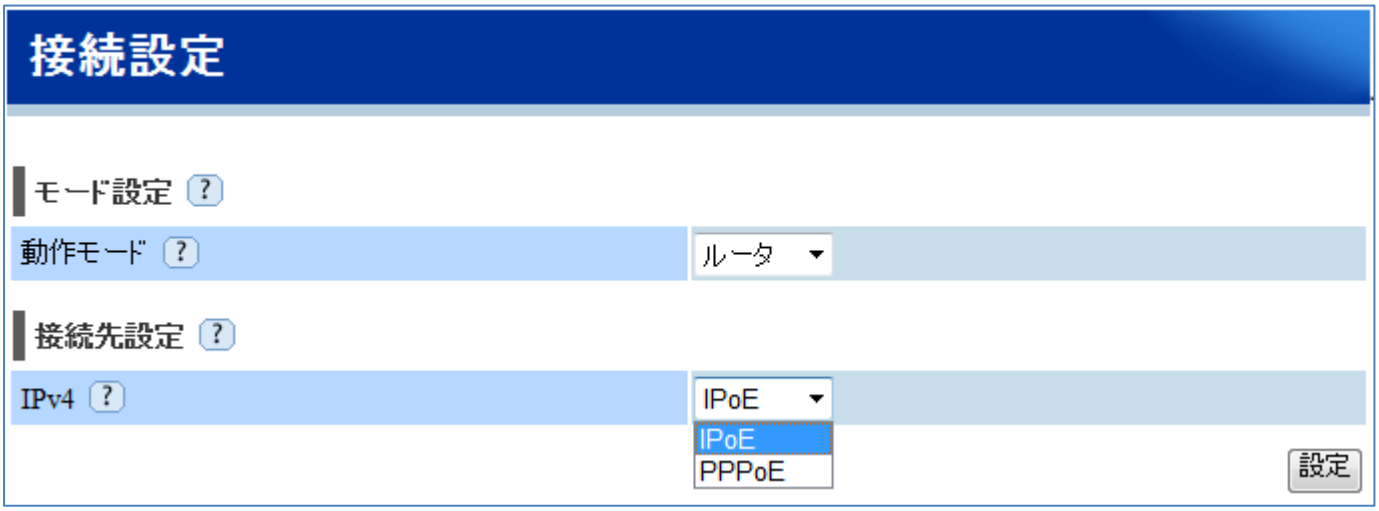
次の手順で設定します。

1. WAN インタフェースの動作タイプの選択
   [接続設定]画面で設定します
2. WAN インタフェースの各種設定
   [IPv4 WAN 設定（IPoE）]画面または[IPv4 WAN 設定（PPPoE）]画面のいずれかで設定します

	WAN インタフェースの IP アドレスの設定方法	手順 1 [接続設定]画面の「接続先設定」の設定値	手順 2 設定が必要な設定画面
(a)	固定設定	IPoE	IPv4 WAN 設定（IPoE） DNS 設定
(b)	DHCP クライアント機能を使用して設定	IPoE	IPv4 WAN 設定（IPoE）
(c)	PPP 機能を使用して設定	PPPoE	IPv4 WAN 設定（PPPoE）

■手順 1. WAN インタフェースの動作タイプの選択

本製品の WAN インタフェースの IP アドレスの設定で、IPoE または PPPoE を設定してください。



1. [TOP]-[メンテナンス]-[基本設定]-[接続設定]画面を開きます。
2. [接続先設定]-[IPv4]で、IPoE または PPPoE を選択します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
接続先設定	本製品の WAN インタフェースで動作させるプロトコルの選択		
IPv4	• IPoE…本製品の WAN インタフェースの IP アドレスを「固定設定」または「DHCP クライアント機能」で設定する場合に選択します。 • PPPoE…本製品の WAN インタフェースの IP アドレスを PPP で設定する場合に選択します。	DHCP クライアント機能、PPP 機能の各種設定は、別の設定画面で設定します。	IPoE

■手順 2. WAN インタフェースの各種設定

手順 1 で選択した内容によって設定する内容が変わります。

	WAN インタフェースの IP アドレスの設定方法	設定内容
(a)	固定設定	以降の内容を参照してください
(b)	DHCP クライアント機能を使用して設定	5.7.5 章を参照してください
(c)	PPP 機能を使用して設定	5.7.4 章を参照してください

本製品の WAN インタフェースの IP アドレスを固定設定する場合は、本製品の WAN インタフェースの IP アドレス設定の他、デフォルトゲートウェイアドレス、DNS サーバアドレスの設定が必要です。(5.7.11 章参照)

設定内容	設定画面
本製品の WAN インタフェースの IP アドレス	IPv4 WAN 設定（IPoE）
デフォルトゲートウェイアドレス	IPv4 WAN 設定（IPoE）
DNS サーバアドレス	DNS 設定

◆IP アドレス、デフォルトゲートウェイアドレスの設定

1. [TOP]-[メンテナンス]-[基本設定]-[IPv4 WAN 設定（IPoE）]画面を開きます。
2. DHCP クライアント機能のチェックボックスを外します。
3. 「IPv4 アドレス/ネットマスク」に IP アドレス情報を入力します。
4 「ゲートウェイ」の「固定アドレス」にデフォルトゲートウェイの IP アドレス情報を入力します。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
DHCP クライアント機能	• チェック有…本製品の WAN インタフェースのネットワーク情報を DHCP クライアント機能で取得する場合 • チェック無…本製品の WAN インタフェースのネットワーク情報に固定値を使用する場合	DHCP クライアント機能を使用しない場合は、[TOP]-[メンテナンス]-[ネットワーク設定]-[DNS 設定]で DNS サーバアドレス情報を設定してください。	有効
IPv4 アドレス/ネットマスク	本製品の WAN インタフェースの IPv4 アドレス情報		
IPv4 アドレス/ネットマスク（ビット指定）	本製品の WAN インタフェースの IPv4 アドレスとサブネットマスクを設定してください。 サブネットマスクは、ビットで指定してください。	DHCP クライアント機能を使用しない場合に設定できます。	未設定
ゲートウェイ	ゲートウェイアドレス情報		
サーバから割り当てられたアドレス	• チェック有…デフォルトゲートウェイのアドレスを DHCP サーバから取得する場合 • チェック無…デフォルトゲートウェイのアドレスを固定設定する場合		有効
固定アドレス	デフォルトゲートウェイの IP アドレスを設定してください。		未設定

◆DNS サーバアドレスの設定

5.7.11 章を参照してください。

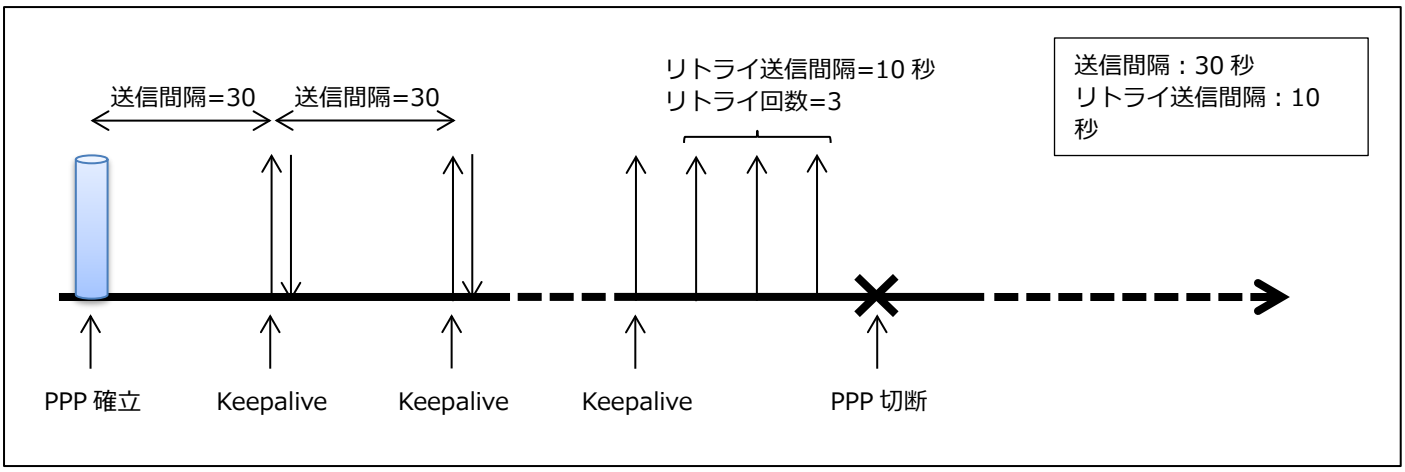
5.7.4. **PPP/PPPoE の設定**

本製品の PPP 機能は、PPP の認証用の ID/パスワードの設定が必須です。

1. [TOP]-[メンテナンス]-[基本設定]-[PPP 設定]画面を開きます。
2. PPP の認証用の ID とパスワードを設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
接続先の設定	PPP の認証に使用する ID とパスワードの設定 (通常は契約しているプロバイダから発行されています。)	PPP 認証プロトコルは、PAP と CHAP に対応しています。認証プロトコルを BAS（サーバ）の指示にしたがって自動で選択します。	
ユーザー名	PPP の認証に使用するユーザー名を設定してください。	使用可能文字列は、半角英数字、記号（アスキーコード：0x20~0x7e）です。 最大文字数は、128 文字です。	未設定
パスワード	PPP の認証に使用するパスワードを設定してください。	使用可能文字列は、半角英数字、記号（アスキーコード：0x20~0x7e）です。 最大文字数は、128 文字です。	未設定
PPP キープアライブ	PPP キープアライブ機能の設定		
PPP キープアライブ機能	• チェック有…PPP キープアライブ機能を使用する場合 • チェック無…PPP キープアライブ機能を使用しない場合	PPP キープアライブ機能を使用することで、BAS（サーバ）とセッションの切断を検知できます。一方、本製品の負荷が高いと PPP キープアライブ機能が適切に動作せず、PPP セッションの切断につながることがあります。	無効
LCP ECHO 送信間隔（秒）	PPP キープアライブパケットの送信間隔を 1~255 秒で設定します。	送信間隔を短くすると、異常検知のタイミングが早くなります。	未設定
LCP EHCO リトライ送信間隔（秒）	PPP キープアライブパケットの応答を受信できなかった場合の再送間隔を 1~255 秒で設定します。	送信間隔を短くすると、異常検知のタイミングが早くなります。	未設定
LCP ECHO リトライ回数（回）	本項目で設定した数の PPP キープアライブパケットを送信しても BAS（サーバ）から応答を受信できない場合に PPP セッションを切断します。1~255 の間で設定します。	送信間隔を短くすると、異常検知のタイミングが早くなります。	未設定

キープアライブに関するパラメータのイメージ図



5.7.5. **DHCP クライアントの設定**

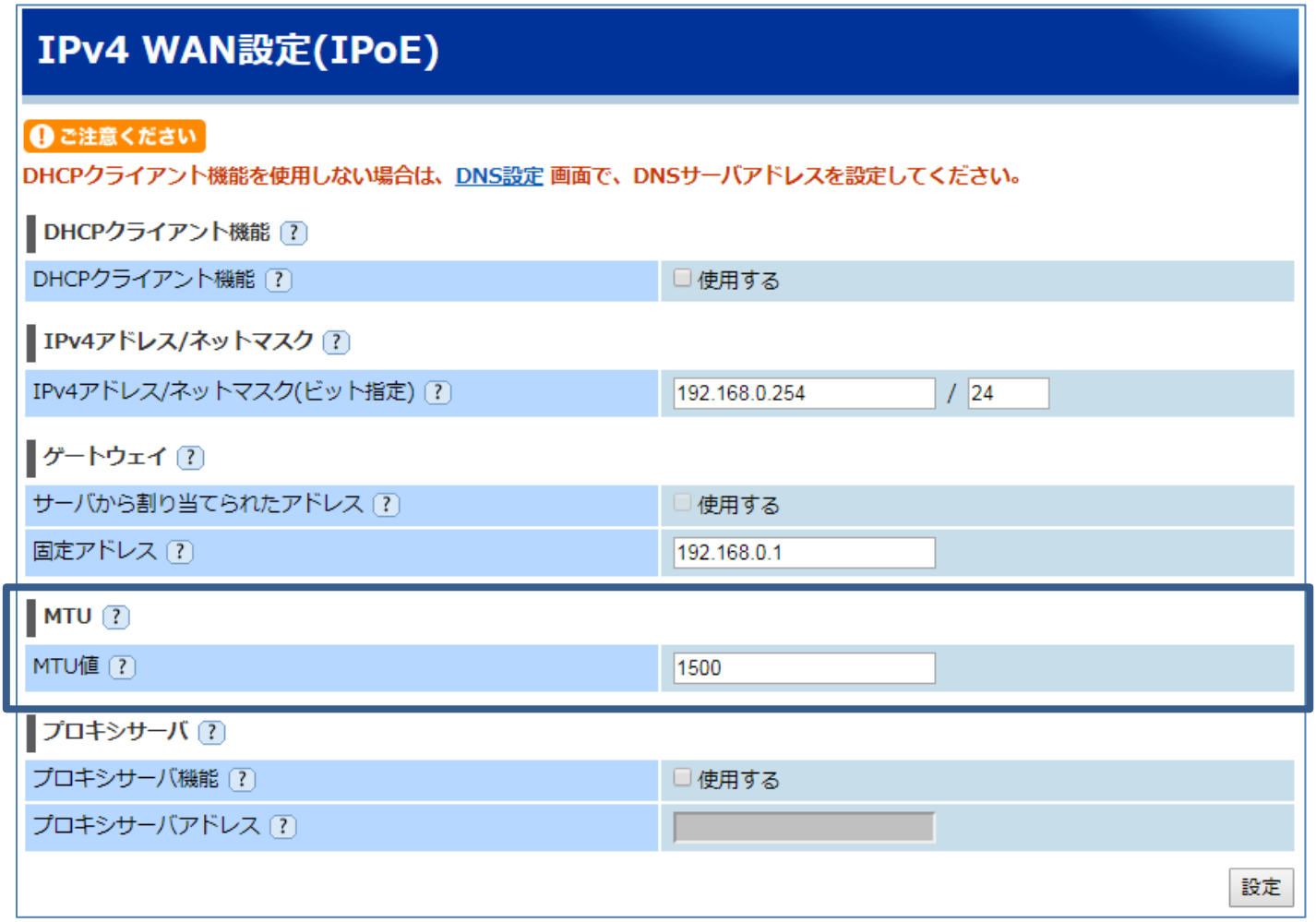
本製品の WAN インタフェースの IP アドレスを DHCP クライアントで取得する場合、本画面で設定します。

1. [TOP]-[メンテナンス]-[基本設定]-[IPv4 WAN 設定（IPoE）]画面を開きます。
2. 次の項目のチェックボックスをチェックします。
   - DHCP クライアント機能：DHCP クライアント機能
   - ゲートウェイ：サーバから割り当てられたアドレス
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

※各設定項目の説明については、5.7.3 章を参照してください。

5.7.6. **MTU の設定**

本製品の WAN インタフェースの MTU 値を変更する場合する場合、本画面で設定します。



1. [TOP]-[メンテナンス]-[基本設定]-[IPv4 WAN 設定（IPoE）]画面を開きます。
2. お客様のネットワークに合わせて変更します。MTU の値を設定します。範囲は 1000～1500(初期値)です。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
MTU	1000～1500	本製品の WAN インタフェースで動作させる MTU の値を設定します。IPoE モードで運用時のときに MTU の設定ができます。	1500

5.7.7. **DHCP サーバ**

本製品の LAN インタフェースの IP アドレスを変更した場合、DHCP サーバ機能の割当アドレスを変更してください。

1. [TOP]-[メンテナンス]-[基本設定]-[IPv4 LAN 設定]画面を開きます。
2. お客様のネットワークに合わせて変更します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

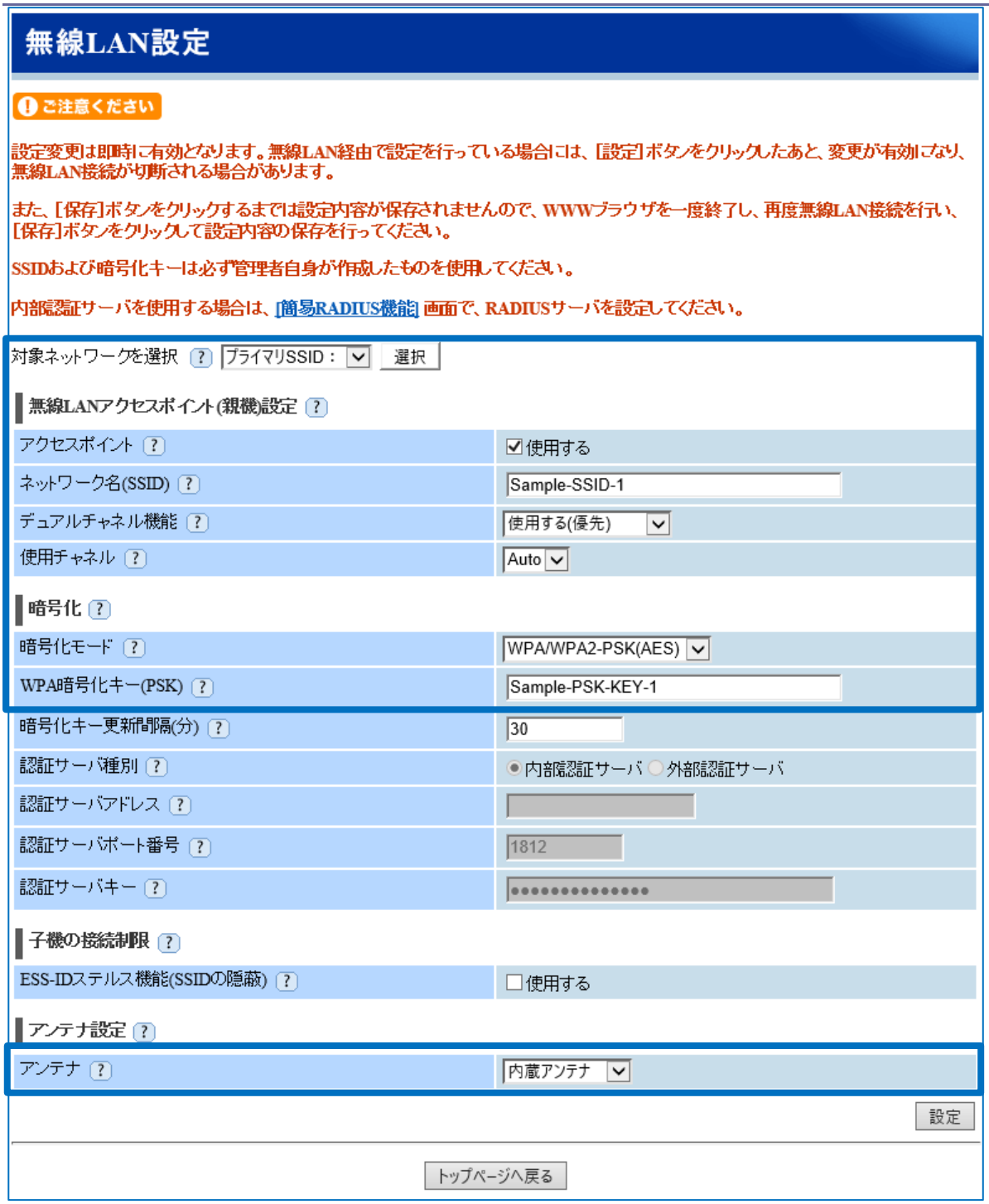
設定項目	値	備考	初期値
DHCP サーバ	本製品の DHCP サーバアドレスの設定		
DHCP サーバ機能	• チェック有…DHCP サーバ機能を使用する • チェック無…DHCP サーバ機能を使用しない		有効
リースタイム（時間）	リースタイムを設定します。設定範囲 1~72 時間です。'0' を設定すると無制限になります。	割当アドレス（DHCP サーバが配布可能な IP アドレス）の関係上、0 を推奨しません。	24
割当先頭アドレス	パソコンなどの DHCP クライアントに配布する IP アドレス範囲の先頭アドレスを設定してください。	割当アドレスは最大 250 です。	192.168.110.2
割当終了アドレス	パソコンなどの DHCP クライアントに配布する IP アドレス範囲の最後のアドレスを設定してください。	割当アドレスは最大 250 です。	192.168.110.251
ドメイン名	パソコンなどの DHCP クライアントに通知するドメイン名を設定してください。	最大文字数は、128 文字です。 DHCP の option15 の値です。	無効
WINS サーバ	パソコンなどの DHCP クライアントに通知する WINS サーバの IP アドレスを設定してください。	DHCP の option44 の値です。	無効

5.7.8. **無線 LAN の設定**

アンテナは、内蔵アンテナと外付けアンテナがあり、どちらのアンテナで動作させるかを設定 Web で切り替えます。

WPS のスイッチ操作については、5.10.5 章を参照してください。

5.7.8.1. **本製品を無線 LAN アクセスポイントとして使用する場合**



1. [TOP]-[メンテナンス] -[無線 LAN 設定]-[無線 LAN 設定]画面を開きます。
2. 「対象ネットワークを選択」に「プライマリ SSID：」が選択されていることを確認します。
3. 「アクセスポイント」の「使用する」をチェックし、各項目を入力したら、[設定] をクリックします。
   ・「ネットワーク名(SSID)」
   任意のネットワーク名を入力します。
   ※半角英数字、-（ハイフン）、_（アンダースコア）を使用して 32 文字以内で入力してください。
   なお、社内で使用している他の機器から出力されているネットワーク名（SSID）と同一の名称に設定することはできません。

・「暗号化モード」
「WPA/WPA2-PSK(AES)」が選択されていることを確認します。
・「WPA 暗号化キー(PSK)」
任意の WPA 暗号化キーを入力します。
※英数記号（0～9、a～z、A～Z、および?を除く記号）で 8～63 桁、
または、16 進数（0～9、a～f、A～F）で 64 桁を入力してください。
暗号化キーは複雑で長い文字列にして、安全性を高めることをお勧めします。

4. ポップアップ画面に「設定変更は即時に有効となります。・・・」と表示されますので、表示内容を確認のうえで「OK」をクリックします。
5. セカンダリ SSID を使用しない場合は、「保存」をクリックします。
プライマリ SSID の設定はこれで完了です。

6. セカンダリ SSID を使用する場合は、以下の設定を行います。
「対象ネットワークを選択」の「セカンダリ SSID：」を選択し、「選択」をクリックします。
7. 手順 3.にしたがいセカンダリ SSID の「ネットワーク名」と「WPA 暗号化キー(PSK)」を入力したら、［設定］をクリックします。
8. ポップアップ画面に「設定変更は即時に有効となります。・・・」と表示されますので、表示内容を確認のうえで「OK」をクリックします。
9. 「保存」をクリックします。
セカンダリ SSID の設定はこれで完了です。

[メモ]

外付けアンテナを使用している場合は、「アンテナ」を「外付けアンテナ」に変更します。

5.7.8.2. 本製品内部の RADIUS サーバで認証する場合

本製品内部の RADIUS サーバを使用する場合は、[簡易 RADIUS 機能]画面で RADIUS サーバを設定してください。詳細は 5.8.12 章を参照してください。

1. [TOP]-[メンテナンス]-[無線 LAN 設定]-[無線 LAN 設定]画面を開きます。
2. 「アクセスポイント」の「使用する」をチェックします。
3. 暗号化モードを「802.1x(EAP)」に変更します。
4. 「認証サーバ種別」は「内部認証サーバ」が選択されていることを確認します。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。
7. [TOP]-[セキュリティ]-[簡易 RADIUS 機能]画面で RADIUS サーバを設定します。
   詳細は 5.8.12 章を参照してください。

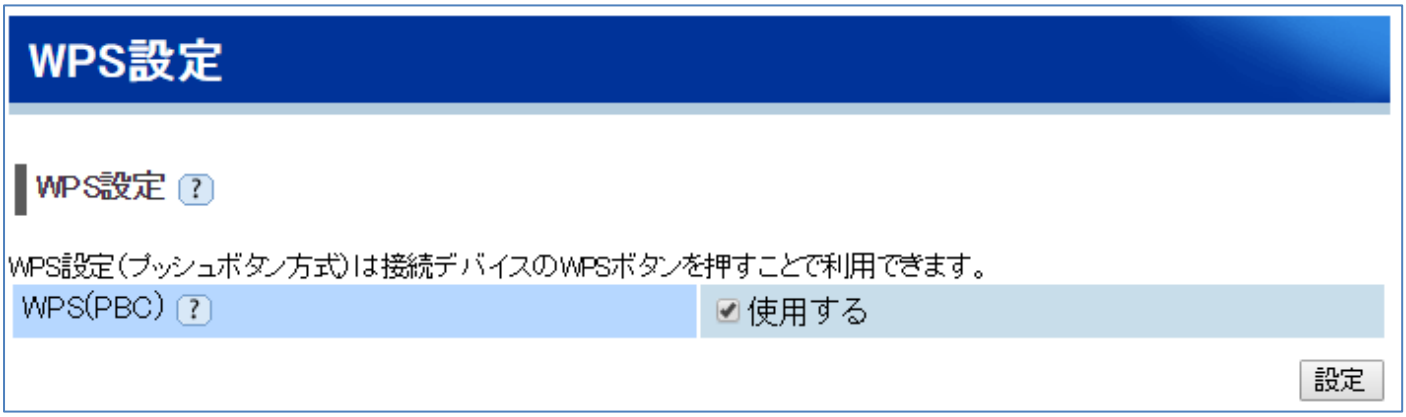
1. [TOP]-[メンテナンス]-[無線 LAN 設定]-[無線 LAN 設定]画面を開きます。
2. 「アクセスポイント」の「使用する」をチェックします。
3. 暗号化モードを「802.1x(EAP)」に変更します。
4. 「認証サーバ種別」を「外部認証サーバ」に変更します。
5. 外部認証サーバの設定値を入力します。
6. 「設定」ボタンを押下します。
7. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
対象ネットワークを選択	• プライマリ SSID • セカンダリ SSID		
無線 LAN アクセスポイント（親機）設定	アクセスポイントの設定		
アクセスポイント	• チェック有…無線 LAN 機能を使用する場合 • チェック無…無線 LAN 機能を使用しない場合		プライマリ、セカンダリともに無効
ネットワーク名（SSID）	SSID を設定します。	半角英数字、-(ハイフン)、_(アンダースコア)を使用して 32 文字以内で入力してください。 なお、他のネットワーク名(SSID)と同一の名称に設定することはできません。 ご利用のファームウェアバージョンでは SSID の初期値は自動設定されません。	未設定
デュアルチャネル機能	• 使用する • 使用しない	無線 LAN 通信で利用する通信チャネル幅を 20MHz 幅から 40MHz 幅に拡大することで、約 2 倍の通信速度（規格値最大 300Mbps）を実現する機能です。	使用する（プライマリでのみ設定可能）
使用チャネル	• Auto…1~11 チャネルの間で、空いているチャネルを自動選択する場合 • 1~13…チャネルを固定設定する場合		Auto（プライマリでのみ設定可能）
ネットワーク分離機能 ※ブリッジモードでは本設定項目はありません。	• チェック有…本機能を使用する場合 • チェック無…本機能を使用しない場合	ネットワーク分離機能は、3.7.1 章を参照してください。	プライマリ、セカンダリともに無効
暗号化			
暗号化モード	使用する暗号モードを選択します。 • 暗号化無効 • WPA-PSK（TKIP） • WPA-PSK（AES） • WPA2-PSK（TKIP） • WPA2-PSK（AES） • WPA/WPA2-PSK（TKIP） • WPA/WPA2-PSK（AES） • 802.1x（EAP）	暗号化モードを TKIP、または EAP に設定したとき、WPS 機能が無効になります。	プライマリ、セカンダリともに WPA/WPA2-PSK（AES）

WPA 暗号化キー（PSK）	暗号化キーを設定します。	英数記号(0～9、a～z、A～Z、?を除く記号)で 8～63 桁、または、16 進数(0～9、a～f、A～F)で 64 桁を入力してください。 ご利用のファームウェアバージョンでは WPA 暗号化キーの初期値は自動設定されません。	未設定
暗号化キー更新間隔（分）	暗号化キーの更新間隔を 1~1440 分で設定します。 0 を設定した場合、暗号化キーを更新しません。		プライマリ、セカンダリともに 30
認証サーバ種別	認証サーバ(RADIUS)の種別を選択します。 • 内部認証サーバ…本製品内部の RADIUS サーバ機能を使って認証する場合 • 外部認証サーバ…外部の RADIUS サーバを使って認証する場合	暗号化モードを 802.1x(EAP)に設定したときに、選択が可能になります。 内部認証サーバを使用する場合は、[簡易 RADIUS 機能]画面でサーバの設定をしてください。 外部認証サーバを使用する場合は、以下の認証サーバアドレス、認証サーバポート、認証サーバキーを設定してください。	無効
認証サーバアドレス	外部認証サーバの IP アドレスを入力します。		—
認証サーバポート	外部認証サーバのポート番号を入力します。	1~65535	—
認証サーバキー	外部認証サーバの認証キーを入力します。	半角英数字、半角記号で 128 文字以内	—
子機の接続制限			
ESS-ID ステルス機能（SSID の隠蔽）	無線 LAN 端末のアクセスポイント検索時に SSID を表示させないための機能です。 • チェック有…本機能を使用する場合 • チェック無…本機能を使用しない場合	ESS-ID ステルス機能のチェック入れたとき、WPS 機能が自動的に無効になります。	プライマリ、セカンダリともに無効
アンテナ設定	本製品は、内蔵アンテナと外付けアンテナがあります。	外付けアンテナはオプション品です。	
アンテナ	• 内蔵アンテナ…内蔵アンテナを使用する場合 • 外付けアンテナ…外付けアンテナを使用する場合	アンテナについては、4.3 章を参照してください。	内蔵アンテナ（プライマリでのみ設定可能）

5.7.9. **WPS 設定**

WPS 機能の有効/無効の設定は設定 Web で行うことができます。



1. [TOP]-[メンテナンス]-[無線 LAN 設定]-[WPS 設定]画面を開きます。
2. WPS 機能を有効にする場合は「WPS(PBC)」の「使用する」をチェックします。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

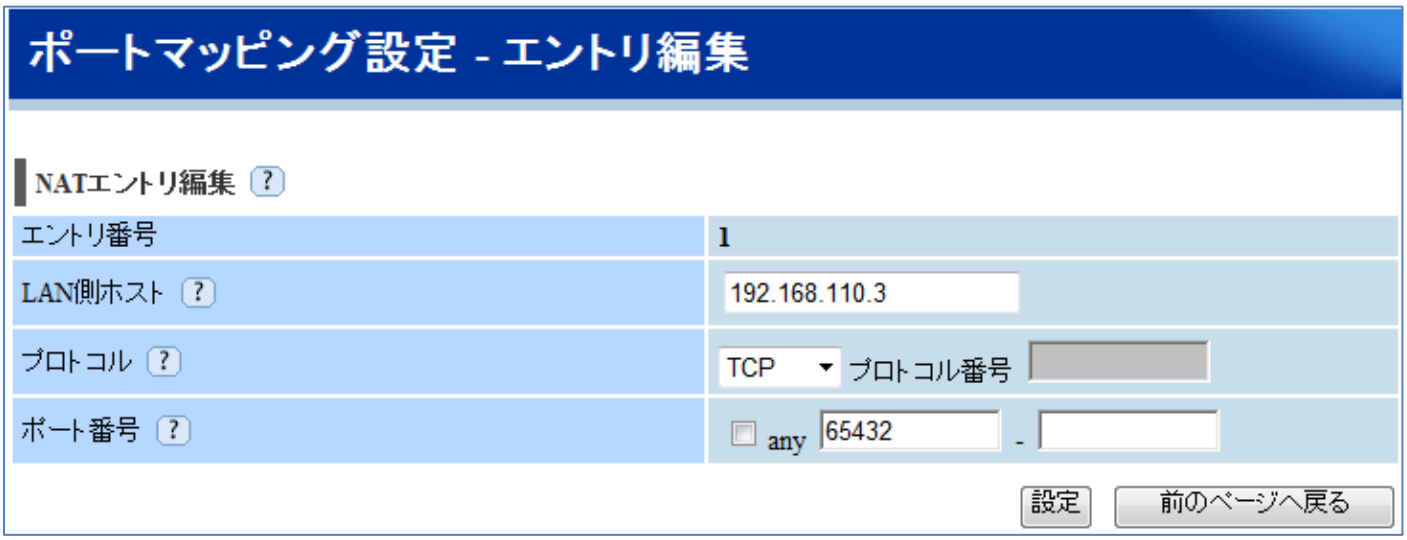
設定項目	説明	初期値
WPS（PBC）	WPS 機能を使用する場合は、本項目をチェックします。	有効

5.7.10. **ポートマッピングに関する設定**

ポートマッピングエントリの設定ができます。

[ポートマッピングエントリの設定]

1. [TOP]-[メンテナンス]-[ネットワーク設定]-[ポートマッピング設定]画面を開きます。
2. 「編集」をクリックすると下記画面に遷移します。

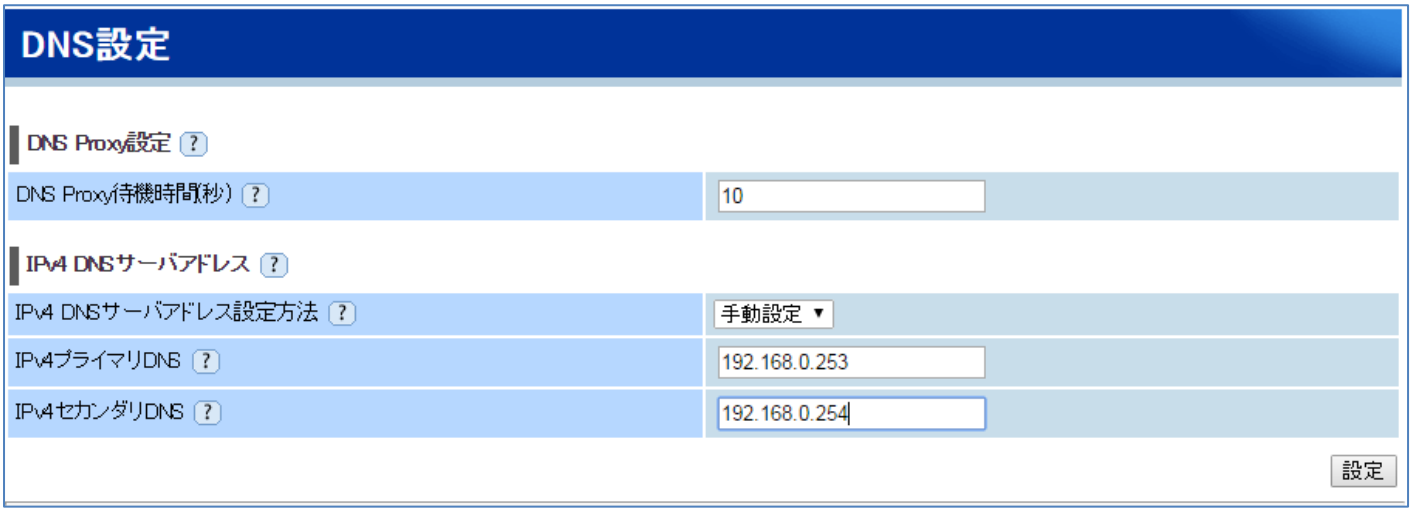


3. ポートマッピングエントリ情報を設定します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
NAT エントリ編集		50 エントリ設定できます。	
エントリ番号	エントリの番号が入ります。	エントリ番号が小さい方が優先されます。	未設定
LAN 側ホスト	ポートマッピング対象のホスト（パソコンなど）の IP アドレスを指定します。		未設定
プロトコル	ポートマッピングするプロトコルを選択します。 • TCP • UDP • ESP • その他 その他を選択した場合は、「プロトコル番号」にポートマッピング対象のプロトコル番号を入力します。		未設定
ポート番号	• any…すべてのポート番号が指定されます。 • ポート番号指定…ポートマッピング対象のポート番号を指定します。	「プロトコル」の項目で、TCP, UDP のいずれかを選択した場合に設定します。	未設定

5.7.11. DNS サーバの設定

WAN インタフェースの IP アドレスを固定で設定する場合、または DHCP や PPPoE で DNS サーバの取得ができない場合、DNS サーバアドレスを固定で設定してください。



1. [TOP]-[メンテナンス]-[ネットワーク設定]-[DNS 設定]画面を開きます。
2. DNS サーバのアドレス情報を設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
DNS Proxy 設定	本製品が DNS query パケットをプロキシしてから、DNS response パケットの受信を待つ時間を設定できます。	お客様のネットワークや使用状況に合わせて DNS の応答パケットのタイムアウト値を設定してください。	
DNS Proxy 待機時間（秒）	DNS query パケットの応答パケット（DNS response）受信までのタイムアウト値を設定してください。設定範囲は、1~50 秒です。		10
IPv4 DNS サーバアドレス	※本製品は、DNS サーバアドレス情報を最大 2 つまで管理します。	DHCP クライアント機能や PPP 機能で取得しても、手動設定した内容が優先されます。	
IPv4 DNS サーバアドレス設定方法	• 自動設定…DNS サーバアドレスの設定を DHCP クライアントまたは PPP で取得する場合 • 手動設定…DNS サーバアドレスの設定を固定値で設定する場合		自動設定
IPv4 プライマリ DNS	プライマリ DNS サーバの IPv4 アドレスを設定します。	最大文字数は、128 文字です。	未設定
IPv4 セカンダリ DNS	セカンダリ DNS サーバの IPv4 アドレスを設定します。	本設定項目は省略可能です。	未設定

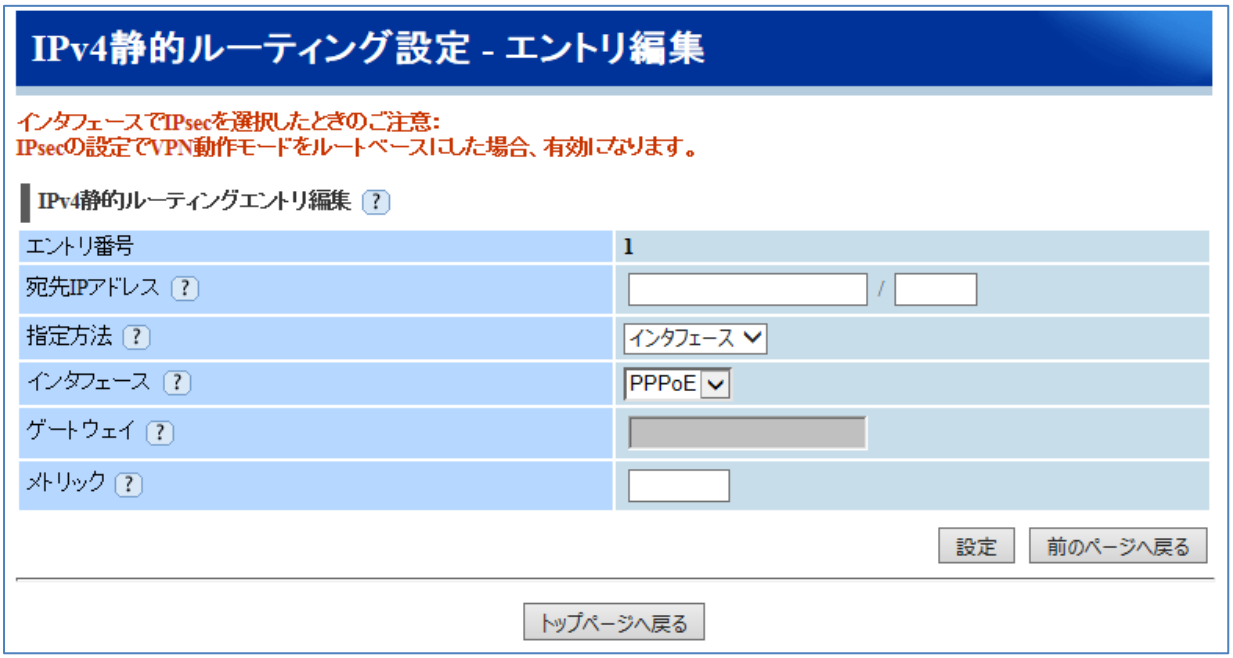
5.7.12. **IPv4 静的ルーティング**

静的ルーティングエントリを最大 50 エントリ追加できます。

※インタフェースで IPsec1 が選択されているときのご注意

IPsec の設定で VPN 動作モードをルートベースに設定しているときのみ、インタフェース“IPsec1”の設定が有効となります。

1. [TOP]-[メンテナンス]-[ネットワーク設定]-[IPv4 静的ルーティング設定]画面を開きます。
2. 「編集」をクリックすると下記画面に遷移します。



3. ルーティングエントリ情報を設定します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
IPv4 静的ルーティングエントリ編集		50 エントリ設定できます。	
エントリ番号	エントリの番号が入ります。		1
宛先 IP アドレス	ルーティングエントリの宛先ネットワークを指定してください。		未設定
指定方法	• インタフェース…ルーティング先をインタフェースで指定する場合 • ゲートウェイ…ルーティング先を IPv4 アドレスで指定する場合		インタフェース
インタフェース	• PPPoE か IPsec1 から選択します。	※インタフェースで IPsec1 を選択したときのご注意 IPsec の設定で VPN 動作モードにルートベースを設定したときに、IPv4 静的ルーティング設定が有効となります。	PPPoE
ゲートウェイ	ゲートウェイの IPv4 アドレスを設定してください。		未設定
メトリック	メトリック値を指定してください。 設定範囲は、1~255 です。	優先させたいルーティングエントリは、メトリック値を小さくします。	未設定

5.7.13. **Ethernet ポート設定**

メンテナンス（ブリッジモード）の設定と同じです。5.6.8 章を参照してください。

5.7.14. **ICMP Redirect メッセージに関する設定**

本製品は、ICMP Redirect メッセージを送信するようなパケットを受信した際、ICMP Redirect メッセージを送信するか、送信しないかを設定できます。

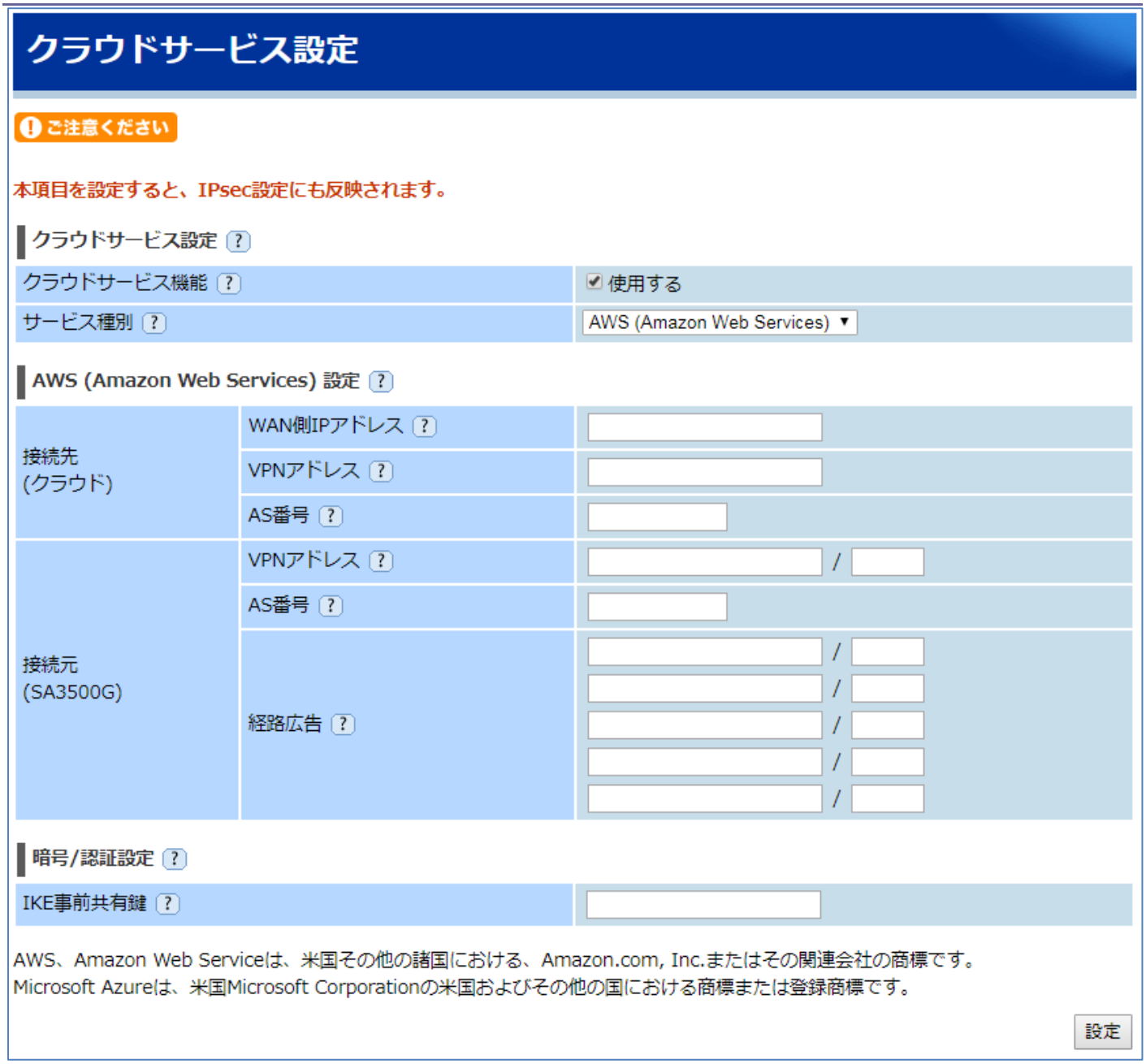
1. [TOP]-[メンテナンス]-[ネットワーク設定]-[その他の設定]画面を開きます。
2. ICMP Redirect メッセージを送信する場合は、チェックします。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
ICMP Redirect 機能	• チェック有…ICMP Redirect 対象のパケットを受信した場合に ICMP Redirect メッセージを送信します。 • チェック無…ICMP Redirect 対象のパケットを受信した場合でも ICMP Redirect メッセージを送信しません。		無効

5.7.15. **クラウドサービス設定**

本製品は、AWS や Azure のクラウド接続サービスをご使用になれます。AWS と Azure は設定項目が異なりますので、それぞれの設定画面を用意しています。

5.7.15.1. **Amazon Web Services**



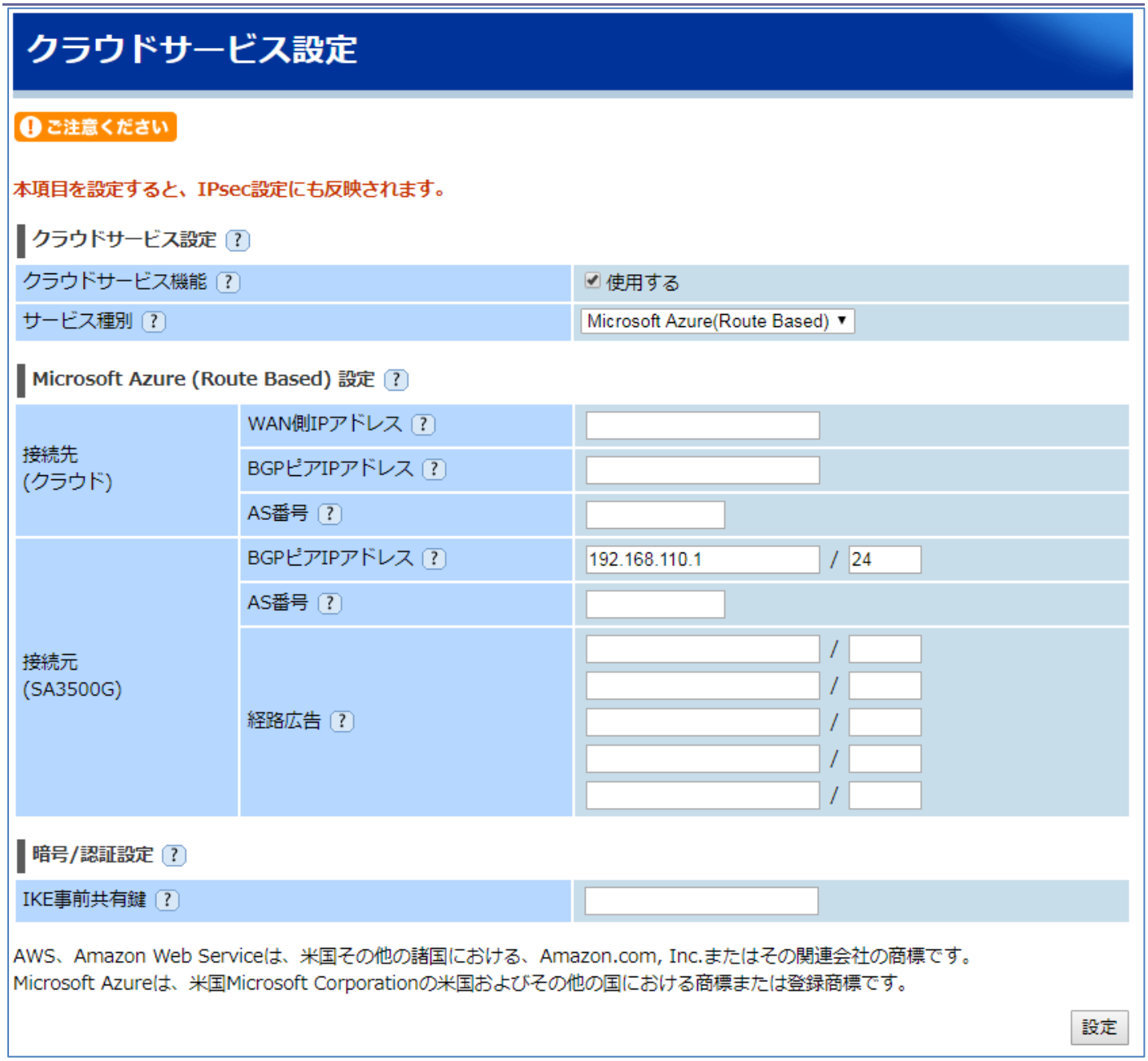
1. [TOP]-[メンテナンス]-[VPN 設定]-[クラウドサービス設定]画面を開きます。
2. クラウドサービス機能の使用するにチェックを入れるとサービス種別が選択できるようになります。
3. サービス種別からで AWS(Amazon Web Services)を選択します。
4. 接続先と接続元の設定をします。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。

設定項目		値	備考	初期値
クラウドサービス設定				
クラウドサービス機能		• チェック有…クラウドサービス機能を使用する場合 • チェック無…クラウドサービス機能を使用しない場合		無効
サービス種別		• AWS(Amazon Web Services) • Microsoft Azure(Route Based) • Microsoft Azure(Policy Based)		未設定
AWS(Amazon Web Services)設定				
接続先(クラウド)	WAN側IPアドレス	Outside IP Addresses: の Virtual Private Gateway のアドレスを設定します。		未設定
	VPN アドレス	Inside IP Addresses:の Virtual Private Gateway を設定します。		未設定
	AS 番号	BGP Configuration Options:の Virtual Private Gateway ASN(1～65535)を設定します。		未設定
接続元(SA3500G)	VPN アドレス	Inside IP Addresses: の Customer Gateway を設定します。		未設定
	AS 番号	BGP Configuration Options: の Customer Gateway ASN(1～65535)を設定します。		未設定
	経路広告	経路広告するネットワークアドレスとネットマスクを設定します。最大 5 つ設定できます。		未設定
暗号/認証設定				
IKE 事前共有鍵		半角で 1～64 文字 ASCII 記号 0x21～0x7e (「"、'、`、#、¥、$、スペース、?」を除く)		未設定

Amazon Web Services 設定を行うことで、次の固定値が設定されます。
IPsec の設定は IPsec 設定画面で変更することが可能ですが、クラウドサービス設定画面で設定した内容のままご使用になることを推奨します。IPsec 設定画面で設定内容を変更した場合、クラウド接続できなくなる可能性がありますのでご注意ください。
また、Amazon Web Services 側のサービス内容が変更になった場合、クラウドサービス設定画面で設定した内容では接続できなくなる可能性があります。

設定項目		値	備考
BGP4			
KeepAlive /Hold タイマ設定		Hold タイマ 30 秒、KeepAlive タイマ 10 秒	
最大経路受け入れ数設定		経路数 4096、warning-only 指定	
IPsec			
IPsec 設定	IPsec 機能	使用する	
	IKE バージョン	IKEv1	
	TCP/MSS 調整	自動	
IKE フェーズ 1 設定	鍵交換方式	メインモード	
	ローカル ID 指定	指定しない	
	リモート ID 指定	指定しない	
	暗号化アルゴリズム	AES128-CBC	
	認証アルゴリズム	HMAC-SHA1	
	DH-Group 選択	1024 bit	
	ライフタイム	28800 秒	
	DPD-Keepalive	使用する	
	DPD-Keepalive 送信間隔	10 秒	
	DPD-Keepalive リトライアウト回数	3 回	
	IKE 再送間隔指定	指定しない	
	IKE 再送回数指定	指定しない	
IKE フェーズ 2 設定	ローカル ID	指定しない	
	リモート ID	指定しない	
	暗号化アルゴリズム	AES128-CBC	
	認証アルゴリズム	HMAC-SHA1	
	ライフタイム	3600 秒	
	ライフタイムデータ量	指定しない	
	PFS	1024 bit	
	Commit-bit	使用しない	
	Rekey	Enable	
	Rekey 残り時間	指定しない	

5.7.15.2. **Microsoft Azure (Route Based)**



1. [TOP]-[メンテナンス]-[VPN 設定]-[クラウドサービス設定]画面を開きます。
2. クラウドサービス機能の使用するにチェックを入れるとサービス種別が選択できるようになります。
3. サービス種別から Microsoft Azure(Route Based)を選択します。
4. 接続先と接続元の設定と IKE 事前共有鍵の設定をします。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。

設定項目		値	備考	初期値
クラウドサービス設定				
クラウドサービス機能		• チェック有…クラウドサービス機能を使用する場合 • チェック無…クラウドサービス機能を使用しない場合		無効
サービス種別		• AWS(Amazon Web Services) • Microsoft Azure(Route Based) • Microsoft Azure(Policy Based)		未設定
Microsoft Azure(Route Based)				
接続先(クラウド)	WAN側IPアドレス	Virtual Private Gatewayのアドレスを設定します。		未設定
	BGP ピア IP アドレス	対向（ピア）の IP アドレスを設定します。		未設定
	AS 番号	割り当てられている AS 番号を設定します。		未設定
接続元(SA3500G)	BGP ピア IP アドレス	ローカルネットワークゲートウェイの BPG ピア IP アドレスを設定します。本製品に設定されている LAN 側 IP アドレスが自動的に入ります。		未設定
	AS 番号	割り当てられている AS 番号を設定します。		未設定
	経路広告	経路広告するルータのアドレスとネットマスクを設定します。最大 5 つ設定できます。		未設定
暗号/認証設定				
IKE 事前共有鍵		半角で 1～64 文字 ASCII 記号 0x21～0x7e (「"、'、`、#、¥、$、スペース、?」を除く)		未設定

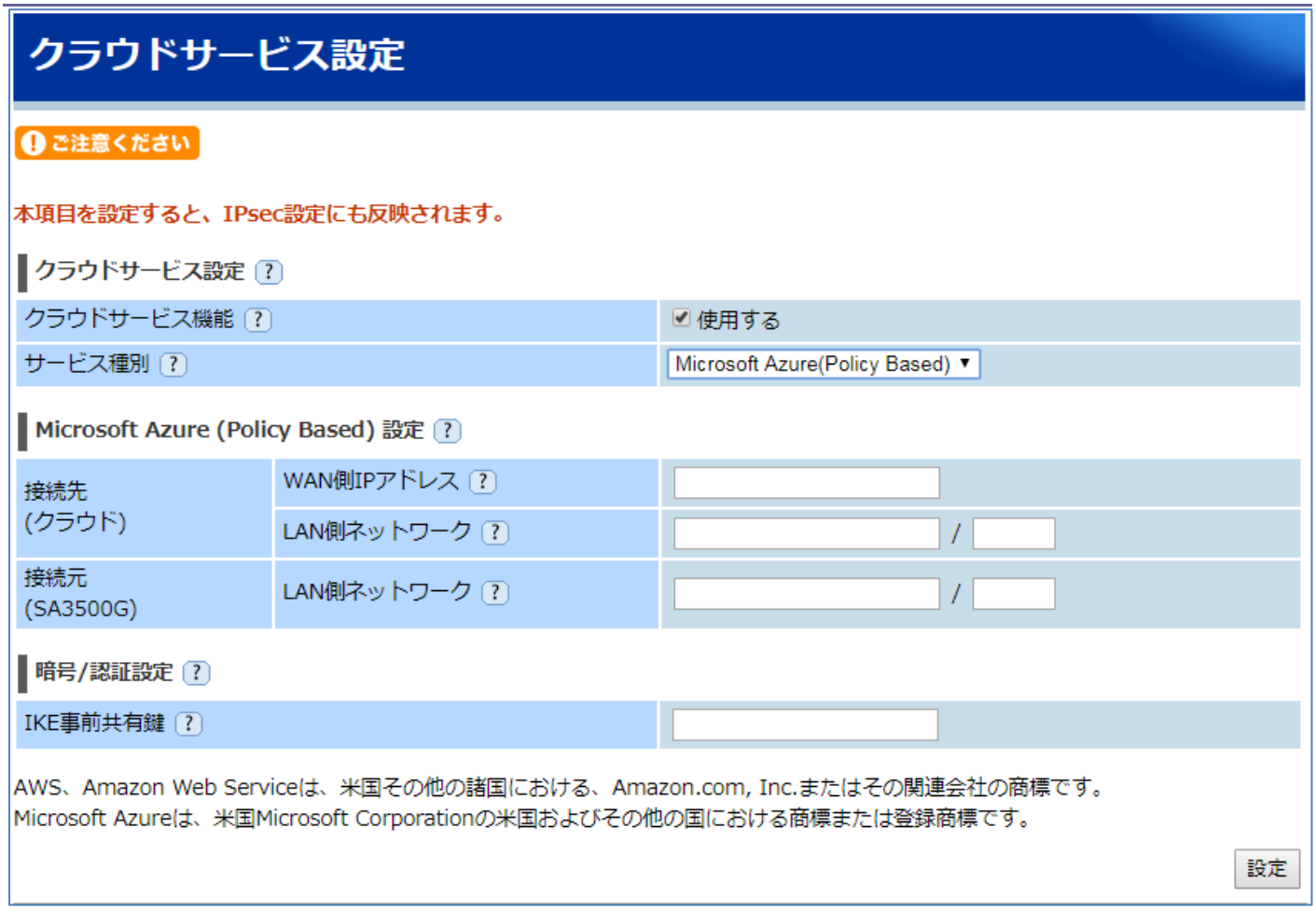
Microsoft Azure(Route Based)設定を行うことで、次の固定値が設定されます。

IPsec の設定は IPsec 設定画面で変更することが可能ですが、クラウドサービス設定画面で設定した内容のままご使用になることを推奨します。IPsec 設定画面で設定内容を変更した場合、クラウド接続できなくなる可能性がありますのでご注意ください。

また、Microsoft Azure 側のサービス内容が変更になった場合、クラウドサービス設定画面で設定した内容では接続できなくなる可能性があります。

設定項目			値	備考
BGP4				
	KeepAlive /Hold タイマ設定		Hold タイマ 30 秒、KeepAlive タイマ 10 秒	
	最大経路受け入れ数設定		経路数 4096、warning-only 指定	
	BGP ピア：マルチホップ設定		ホップ数 255	
IPsec				
	IPsec 設定	IPsec 機能	使用する	
		IKE バージョン	IKEv2	
		TCP/MSS 調整	1350byte 固定	
	IKE_SA_INIT 交換設定	ローカル ID 指定	指定しない	
		リモート ID 指定	指定しない	
		暗号化アルゴリズム	AES256-CBC	
		認証アルゴリズム	HMAC-SHA1	
		PRF アルゴリズム	HMAC-SHA1	
		DH-Group 選択	1024 bit	
		ライフタイム	10800 秒	
		DPD-Keepalive	使用する	
		DPD-Keepalive 送信間隔	10 秒	
		IKE 再送間隔指定	指定しない	
		IKE 再送回数指定	指定しない	
		ネゴシエーション方向限定	both	
	IKE_AUTH 交換設定	ローカルトラフィックセレクタ	設定しない	
		リモートトラフィックセレクタ	設定しない	
		暗号化アルゴリズム	AES256-CBC	
		認証アルゴリズム	HMAC-SHA1	
		ライフタイム	3600 秒	
		ライフタイムデータ量	指定しない	
		PFS	無効	
		Rekey	Enable	
		Rekey 残り時間	指定しない	

5.7.15.3. **Microsoft Azure (Policy Based)**



1. [TOP]-[メンテナンス]-[VPN 設定]-[クラウドサービス設定]画面を開きます。
2. クラウドサービス機能の使用するにチェックを入れるとサービス種別が選択できるようになります。
3. サービス種別から Microsoft Azure(Policy Based)を選択します。
4. 接続先と IKE 事前共有鍵の設定をします。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下します。

設定項目			値	備考	初期値
クラウドサービス設定					
	クラウドサービス機能		• チェック有…クラウドサービス機能を使用する場合 • チェック無…クラウドサービス機能を使用しない場合		無効
	サービス種別		• AWS(Amazon Web Services) • Microsoft Azure(Route Based) • Microsoft Azure(Policy Based)		未設定
Microsoft Azure(Policy Based)					
	接続先(クラウド)	WAN側IPアドレス	Virtual Private Gatewayのアドレスを設定します。		未設定
		LAN 側ネットワーク	LAN 側のネットワークアドレスとネットマスクを設定します。		未設定
	接続元(SA3500G)	LAN 側ネットワーク	本製品のLAN側のネットワークアドレスとネットマスクを設定します。		未設定
暗号/認証設定					
	IKE 事前共有鍵		半角で 1～64 文字 ASCII 記号 0x21～0x7e (「"、'、`、#、¥、$、スペース、?」を除く)		未設定

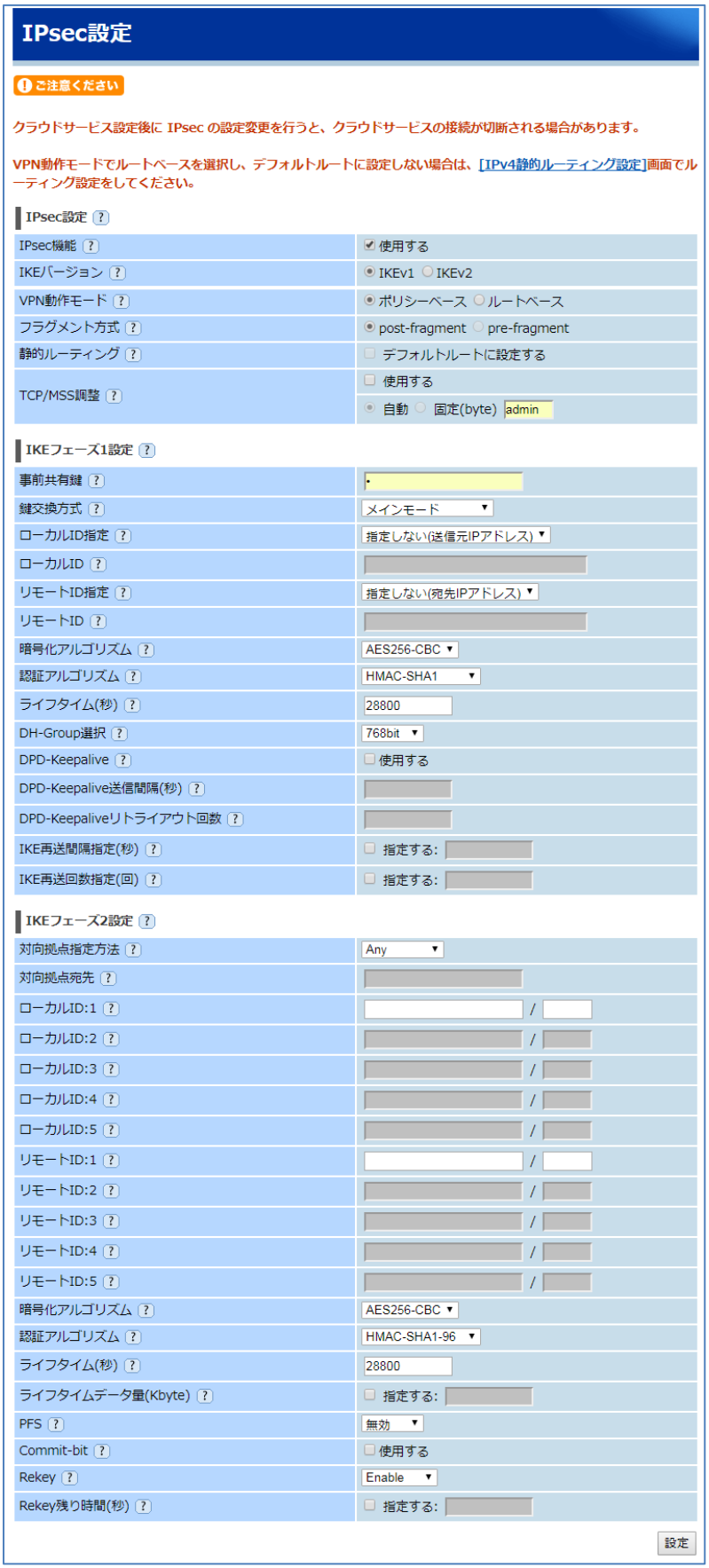
Microsoft Azure(Policy Based)設定を行うことで、次の固定値が設定されます。
IPsec の設定は IPsec 設定画面で変更することが可能ですが、クラウドサービス設定画面で設定した内容のままご使用になることを推奨します。IPsec 設定画面で設定内容を変更した場合、クラウド接続できなくなる可能性がありますのでご注意ください。
また、Microsoft Azure 側のサービス内容が変更になった場合、クラウドサービス設定画面で設定した内容では接続できなくなる可能性があります。

設定項目			値	備考
BGP4				
	BGP4 機能		無効	
IPsec				
	IPsec 設定	IPsec 機能	使用する	
		IKE バージョン	IKEv1	
		TCP/MSS 調整	1350byte 固定	
	IKE フェーズ 1 設定	鍵交換方式	メインモード	
		ローカル ID 指定	指定しない	
		リモート ID 指定	指定しない	
		暗号化アルゴリズム	AES128-CBC	
		認証アルゴリズム	HMAC-SHA1	
		DH-Group 選択	1024 bit	
		ライフタイム	28800 秒	
		DPD-Keepalive	使用しない	
		IKE 再送間隔指定	指定しない	
		IKE 再送回数指定	指定しない	
	IKE フェーズ 2 設定	暗号化アルゴリズム	AES128-CBC	
		認証アルゴリズム	HMAC-SHA1	
		ライフタイム	3600 秒	
		ライフタイムデータ量	指定しない	
		PFS	無効	
		Commit-bit	使用しない	
		Rekey	Enable	
		Rekey 残り時間	指定しない	

5.7.16. IPsec の設定

本製品は、IPsec をサポートしています。鍵交換方式として IKEv1 と IKEv2 をご使用になれます。IKEv1 と IKEv2 は設定項目が異なりますので、分けて記載します。

■IKEv1



1. [TOP]-[メンテナンス]-[VPN 設定]-[IPsec 設定]画面を開きます。
2. IKE バージョンで IKEv1 を選択します。
3. IPsec に関する設定を入力します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
IPsec 設定			
IPsec 機能	• チェック有…IPsec 機能を使用する場合 • チェック無…IPsec 機能を使用しない場合		無効
IKE バージョン	• IKEv1…IKEv1 の設定項目を開きます。 • IKEv2…IKEv2 の設定項目を開きます。		IKEv1
VPN 動作モード	• ポリシーベース…ポリシーに合致したトラフィックのみ VPN 通信の対象となります。 • ルートベース…トンネルインタフェースを作成して、そのインタフェースのルーティング設定にしたがったトラフィックが VPN 通信の対象となります。		ポリシーベース
フラグメント方式	• post-fragment • pre-fragment		post-fragment
静的ルーティング	• チェック有…デフォルトルートを使用する場合 • チェック無…デフォルトルートを使用しない場合	ルートベースを選択した場合に有効もしくは無効の設定ができます。	無効
TCP MSS 調整	• チェック有(自動)…IPsec トンネルを通過する TCP パケットの MSS 値を暗号化アルゴリズムに合わせて最適な値に書き換えます • チェック有(固定)…IPsec トンネルを通過する TCP パケットの MSS 値を指定された固定値に書き換えます • チェック無…IPsec トンネルを通過する TCP パケットの MSS 値を変更しません		無効
IKE フェーズ 1 設定			
事前共有鍵	半角で 1～64 文字 ASCII 記号 0x21～0x7e (「"、'、`、#、¥、$、スペース、?」を除く)	事前鍵共有方式のみサポートしています	未設定
鍵交換方式	• メインモード…本製品と対向の IPsec 機器のどちらも IPsec トンネルの IP アドレスが固定値の場合に選択します アグレッシブモード…本製品または対向の IPsec 機器のどちらか、またはいずれも IPsec トンネルの IP アドレスが不定値の場合に選択します	固定鍵方式をサポートしていません	メインモード
ローカル ID 指定	IKE フェーズ 1 で送信する自装置の ID ペイロードの入力形式を設定します。		指定しない（送信元 IP アドレス）

		• 指定しない（送信元 IP アドレス）…本製品の WAN インタフェースの IP アドレスを使用します • IP アドレス…IP アドレス • FQDN…ドメイン名 • Key-ID…任意の文字列 • User-FQDN…ユーザー名付きドメイン名		
	ローカル ID	「ローカル ID 指定」で選択した入力形式にしたがって ID を設定します。 • IP アドレス…IP アドレスの形式で設定してください • FQDN…ドメイン名の形式で設定してください。入力可能文字列は、英数半角 1～64 文字です。 • Key-ID…入力可能文字列は、英数半角 1～47 文字です。 • User-FQDN…"ユーザー名@ドメイン名”の形式で設定してください。入力可能文字列は、英数半角 3～160 文字です。 ※「FQDN」,「Key-ID」,「User-FQDN」では ASCII 記号 0x21~0x7e(「"、'、`、#、¥、$、スペース、=、?」を除く)が使用できます。	入力例） **IP アドレス**…192.0.2.3 **FQDN** … local.example.com **Key-ID**…LocalID-1 **User-FQDN** … user@example.com	未設定
	リモート ID 指定	IKE フェーズ 1 で送信する対向の IPsec 機器の ID ペイロードの入力形式を設定します。 • 指定しない（宛先 IP アドレス）…対向 IPsec 機器の WAN インタフェースの IP アドレスを使用します。IP アドレスが固定でない場合、未使用となります。 • IP アドレス…IP アドレス • FQDN…ドメイン名 • Key-ID…任意の文字列 • User-FQDN…ユーザー名付きドメイン名		指定しない（宛先 IP アドレス）
	リモート ID	「リモート ID 指定」で選択した入力形式にしたがって ID を設定します。 • IP アドレス…IP アドレスの形式で設定してください • FQDN…ドメイン名の形式で設定してください。入力可能文字列は、英数半角 1～64 文字です。 • Key-ID…入力可能文字列は、英数半角 1～47 文字です。 • User-FQDN…"ユーザー名@ドメイン名”の形式で設定してください。入力可能文字列は、英数半角 3～160 文字です。 ※「FQDN」,「Key-ID」,「User-FQDN」では ASCII 記号 0x21~0x7e(「"、'、`、#、¥、$、スペース、=、?」を除く)が使用できます。	入力例） **IP アドレス** … 192.0.2.222 **FQDN** … remote.example.com **Key-ID**…RemoteID-1 **User-FQDN** … adm@example.com	未設定
	暗号化アルゴリズム	IKE フェーズ 1 で利用する暗号化アルゴリズムを設定します。		AES256-CBC

		• AES256-CBC • AES192-CBC • AES128-CBC • 3DES-CBC		
	認証アルゴリズム	IKE フェーズ 1 で利用する認証アルゴリズムを設定します。 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-MD5		HMAC-SHA1
	ライフタイム（秒）	IKE SA の有効期間を設定します。 入力範囲は、300~691,200 秒です。	対向先の設定と比較して、短い方の値を使用します。設定したライフタイムの 70%から 85%の間でランダムにリキーします。	28800
	DH-Group 選択	Diffie-Hellman 鍵交換の暗号強度を設定します。 • 768bit • 1024bit • 1536bit • 2048bit		768bit
	DPD-Keepalive	IPsec トンネルの通信断の検出を目的とした DPD-Keepalive 機能の使用有無を設定します。 • チェック有…DPD-Keepalive 機能を使用する場合 • チェック無…DPD-Keepalive 機能を使用しない場合	DPD (Dead Peer Detection) 本機能を有効にした場合、DPD パケットを 30 秒間隔(初期値)で送信します。	無効
	DPD-Keepalive 送信間隔(秒)	IPsec トンネルの通信断の検出を目的とした DPD-Keepalive 機能の送信間隔を秒で設定します。		未設定
	DPD-Keepalive リトライアウト回数	IPsec トンネルの通信断の検出を目的とした DPD Keepalive 機能のリトライアウト回数を設定します。		未設定
	IKE 再送間隔指定(秒)	鍵交換のパケットが相手に届かないときに実施する再送間隔を秒で指定します。5～60 秒で設定できます。		指定しない
	IKE 再送回数指定(回)	鍵交換のパケットが相手に届かないときに実施する再送回数を指定します。2～10 回で設定できます。		指定しない
IKE フェーズ 2 設定				
	対向拠点指定方法	対向の IPsec 機器の指定方法を設定します。 • Any…対向の IPsec 機器の IP アドレスが固定でない場合に選択します • IP アドレス…対向の IPsec 機器の IP アドレスが固定の場合に選択します		Any

	対向拠点宛先	「対向拠点指定方法」で「IP アドレス」を選択した場合、IP アドレスを設定してください。		未設定
	ローカル ID:1~5	IKE フェーズ 2 で送信する自装置の ID ペイロード（IP アドレスとサブネットマスク）を設定します。	IPsec 通信の対向相手の ID に合わせて、設定してください。 IPsec 対象のサブネットが複数ある場合は、ローカル ID に複数入力してください。	未設定
	リモート ID:1~5	IKE フェーズ 2 で受信する自装置の ID ペイロード（IP アドレスとサブネットマスク）を設定します。	IPsec 通信の対向相手の ID に合わせて、設定してください。 IPsec 対象のサブネットが複数ある場合は、リモート ID に複数入力してください。	未設定
	暗号化アルゴリズム	IKE フェーズ 2 で利用する暗号化アルゴリズムを設定します。 • AES256-CBC • AES192-CBC • AES128-CBC • 3DES-CBC • NULL		AES256-CBC
	認証アルゴリズム	IKE フェーズ 2 で利用する認証アルゴリズムを設定します。 • HMAC-SHA1-96 • HMAC-SHA2-256 • HMAC-MD5-96		HMAC-SHA1-96
	ライフタイム（秒）	IPsec SA の有効期間を設定します。 入力範囲は、300~691,200 秒です。	対向先の設定と比較して、短い方の値を使用します。設定したライフタイムの 70%から 85%の間でランダムにリキーします。	28800
	ライフタイムデータ量(Kbyte)	IPsec SA 上で通信するデータ量を Kbyte で指定します。		指定しない
	PFS	• 無効…PFS を保証しません • 768bit…DH-Group1 を使用して PFS を保証 • 1024bit…DH-Group2 を使用して PFS を保証 • 1536bit…DH-Group5 を使用して PFS を保証 • 2048bit…DH-Group14 を使用して PFS を保証	PFS (Perfect Forward Secrecy)	無効

	Commit-bit	Commit ビット機能を使用するときにチェックします。Commit ビットは SA 確立時にセットします。本製品がレスポンダのときに Commit ビットをセットします。		使用しない
	Rekey	• Enable…IPsec 対象のトラフィックが発生した際に IKE ネゴシエーションを開始します。また、生成済みの SA を利用したトラフィックがある場合、リキーします。 • Always…IPsec 対象のトラフィックの有無に関係なく、本製品の WAN インタフェースに IP アドレスを設定した後に IKE ネゴシエーションを開始します。また、生成済みの SA を利用したトラフィックの有無にかかわらず、リキーします。 • No Rekey…IPsec 対象のトラフィックが発生した際に IKE ネゴシエーションを開始します。本モードの場合、リキーしません。		Enable
	Rekey 残り時間(秒)	Rekey 残り時間 (秒) が指定された値(30～345600 秒)以下となるタイミングで SA の自動更新を開始します。		未設定

■IKEv2

IPsec設定

ご注意ください

クラウドサービス設定後に IPsec の設定変更を行うと、クラウドサービスの接続が切断される場合があります。

VPN動作モードでルートベースを選択し、デフォルトルートに設定しない場合は、[IPv4静的ルーティング設定]画面でルーティング設定をしてください。

IPsec設定

IPsec機能	使用する
IKEバージョン	IKEv1 IKEv2
VPN動作モード	ポリシーベース ルートベース
フラグメント方式	post-fragment pre-fragment
静的ルーティング	デフォルトルートに設定する
TCP/MSS調整	使用する 自動 固定(byte)

IKE_SA_INIT交換設定

認証方式：自装置	事前共有鍵 EAP-MD5
認証方式：対向装置	事前共有鍵 EAP-MD5 デジタル署名： ファイルを選択 選択されていません
ローカルID指定	指定しない(送信元IPアドレス)
ローカルID	
リモートID指定	指定しない(宛先IPアドレス)
リモートID	
暗号化アルゴリズム	AES256-CBC
認証アルゴリズム	HMAC-SHA1
PRFアルゴリズム	HMAC-SHA1
ライフタイム(秒)	28800
DH-Group選択	768bit
DPD-Keepalive	使用する
DPD-Keepalive送信間隔(秒)	
IKE再送間隔指定(秒)	指定する:
IKE再送回数指定(回)	指定する:
ネゴシエーション方向限定	both

IKE_AUTH交換設定

対向拠点指定方法	Any
対向拠点宛先	
ローカルトラフィックセレクタ:1	/
ローカルトラフィックセレクタ:2	/
ローカルトラフィックセレクタ:3	/
ローカルトラフィックセレクタ:4	/
ローカルトラフィックセレクタ:5	/
リモートトラフィックセレクタ:1	/
リモートトラフィックセレクタ:2	/
リモートトラフィックセレクタ:3	/
リモートトラフィックセレクタ:4	/
リモートトラフィックセレクタ:5	/
暗号化アルゴリズム	AES256-CBC
認証アルゴリズム	HMAC-SHA1-96
ライフタイム(秒)	28800
ライフタイムデータ量(Kbyte)	指定する:
PFS	無効
Rekey	Enable
Rekey残り時間(秒)	指定する:

設定

1. [TOP]-[メンテナンス]-[VPN 設定]-[IPsec 設定]画面を開きます。
2. IKE バージョンで IKEv2 を選択します。
3. IPsec に関する設定を入力します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
IPsec 設定			
IPsec 機能	• チェック有…IPsec 機能を使用する場合 • チェック無…IPsec 機能を使用しない場合		無効
IKE バージョン	• IKEv1…IKEv1 の設定項目を開きます。 • IKEv2…IKEv2 の設定項目を開きます。		IKEv1
VPN 動作モード	• ポリシーベース…ポリシーに合致したトラフィックのみ VPN 通信の対象となります。 • ルートベース…トンネルインタフェースを作成して、そのトンネル VPN 通信のルートを作成します。		ポリシーベース
フラグメント方式	• post-fragment • pre-fragment		post-fragment
静的ルーティング	• チェック有…デフォルトルートを使用する場合 • チェック無…デフォルトルートを使用しない場合	ルートベースを選択した場合に有効もしくは無効の設定ができます。	無効
TCP MSS 調整	• チェック有(自動)…IPsec トンネルを通過する TCP パケットの MSS 値を暗号化アルゴリズムに合わせて最適な値に書き換えます • チェック有(固定)…IPsec トンネルを通過する TCP パケットの MSS 値を指定された固定値に書き換えます • チェック無…IPsec トンネルを通過する TCP パケットの MSS 値を変更しません		無効
IKE_SA_INIT 交換設定			
認証方式：自装置	本製品の認証方式を設定します。事前共有鍵と EAP-MD5 が選択できます。 事前共有鍵と EAP-MD5 で設定できる文字は以下のとおりです。 半角で 1～64 文字 ASCII 記号 0x21～0x7e (「"、'、`、#、¥、$、スペース、?」を除く)		未設定
認証方式：対向装置	対向装置の認証方式を設定します。事前共有鍵と EAP-MD5、デジタル署名が選択できます。 事前共有鍵と EAP-MD5 で設定できる文字は以下のとおりです。 半角で 1～64 文字 ASCII 記号 0x21～0x7e (「"、'、`、#、¥、$、スペース、?」を除く)		未設定

	ローカル ID 指定	対向装置へ送信する自装置の ID ペイロードの入力形式を設定します。 • 指定しない（送信元 IP アドレス）…本製品の WAN インタフェースの IP アドレスを使用します • IP アドレス…IP アドレス • FQDN…ドメイン名 • Key-ID…任意の文字列 • User-FQDN…ユーザー名付きドメイン名		指定しない（送信元 IP アドレス）
	ローカル ID	「ローカル ID 指定」で選択した入力形式にしたがって ID を設定します。 • IP アドレス…IP アドレスの形式で設定してください • FQDN…ドメイン名の形式で設定してください。入力可能文字列は、英数半角 1～64 文字です。 • Key-ID…入力可能文字列は、英数半角 1～47 文字です。 • User-FQDN…"ユーザー名@ドメイン名”の形式で設定してください。入力可能文字列は、英数半角 3～160 文字です。 ※「FQDN」,「Key-ID」,「User-FQDN」では ASCII 記号 0x21~0x7e(「"、'、`、#、¥、$、スペース、=、?」を除く)が使用できます。	入力例） **IP アドレス**…192.0.2.3 **FQDN**…local.example.com **Key-ID**…LocalID-1 **User-FQDN**…user@example.com	未設定
	リモート ID 指定	対向装置へ送信する対向の IPsec 機器の ID ペイロードの入力形式を設定します。 • 指定しない（宛先 IP アドレス）…対向 IPsec 機器の WAN インタフェースの IP アドレスを使用します。IP アドレスが固定でない場合、未使用となります。 • IP アドレス…IP アドレス • FQDN…ドメイン名 • Key-ID…任意の文字列 • User-FQDN…ユーザー名付きドメイン名		指定しない（宛先 IP アドレス）
	リモート ID	「リモート ID 指定」で選択した入力形式にしたがって ID を設定します。 • IP アドレス…IP アドレスの形式で設定してください • FQDN…ドメイン名の形式で設定してください。入力可能文字列は、英数半角 1～64 文字です。 • Key-ID…入力可能文字列は、英数半角 1～47 文字です。 • User-FQDN…"ユーザー名@ドメイン名”の形式で設定してください。入力可能文字列は、英数半角 3～160 文字です。 ※「FQDN」,「Key-ID」,「User-FQDN」では ASCII 記号 0x21~0x7e(「"、'、`、#、¥、$、スペース、=、?」を除く)が使用できます。	入力例） **IP アドレス**…192.0.2.222 **FQDN**…remote.example.com **Key-ID**…RemoteID-1 **User-FQDN**…adm@example.com	未設定

暗号化アルゴリズム	IKE_SA_INIT 交換で利用する暗号化アルゴリズムを設定します。 • AES256-CBC • AES192-CBC • AES128-CBC • 3DES-CBC		AES256-CBC
認証アルゴリズム	IKE_SA_INIT 交換で利用する認証アルゴリズムを設定します。 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-MD5		HMAC-SHA1
PRF アルゴリズム	擬似乱数関数 (PRF： pseudo-random function)を設定します。 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-MD5		HMAC-SHA1
ライフタイム（秒）	IKE SA の有効期間を設定します。 入力範囲は、300~691,200 秒です。	対向先の設定と比較して、短い方の値を使用します。設定したライフタイムの 70%から 85%の間でランダムにリキーします。	28800
DH-Group 選択	Diffie-Hellman 鍵交換の暗号強度を設定します。 • 768bit • 1024bit • 1536bit • 2048bit		768bit
DPD-Keepalive	IPsec トンネルの通信断の検出を目的とした DPD-Keepalive 機能の使用有無を設定します。 • チェック有…DPD-Keepalive 機能を使用する場合 • チェック無…DPD-Keepalive 機能を使用しない場合	DPD (DeadPeer Detection) 本機能を有効にした場合、DPD パケットを 30 秒間隔(初期値)で送信します。	無効
DPD-Keepalive 送信間隔(秒)	IPsec トンネルの通信断の検出を目的とした DPD-Keepalive 機能の送信間隔を秒で設定します。		未設定
IKE 再送間隔指定(秒)	鍵交換のパケットが相手に届かないときに実施する再送間隔を秒で指定します。5～60 秒で設定できます。		指定しない
IKE 再送回数指定(回)	鍵交換のパケットが相手に届かないときに実施する再送回数を指定します。2～10 回で設定できます。		指定しない

ネゴシエーション方向限定	IKE_SA_INIT 交換を双方向で行うか、イニシエータ側もしくはレスポンダ側で行うかを設定します。 • both…双方向 • initiator…イニシエータ側 responder…レスポンダ側		both
IKE_AUTH 交換設定			
対向拠点指定方法	対向の IPsec 機器の指定方法を設定します。 • Any…対向の IPsec 機器の IP アドレスが固定でない場合に選択します • IP アドレス…対向の IPsec 機器の IP アドレスが固定の場合に選択します		Any
対向拠点宛先	「対向拠点指定方法」で「IP アドレス」を選択した場合、IP アドレスを設定してください。		未設定
ローカルトラフィックセレクタ:1~5	自装置ネットワークの IP アドレスとサブネットマスクを設定します。	IPsec 通信の対向相手に合わせて、設定してください。 IPsec 対象のサブネットが複数ある場合は、ローカル ID に複数入力してください。	未設定
リモートトラフィックセレクタ:1~5	対向装置ネットワークの IP アドレスとサブネットマスクを設定します。	IPsec 通信の対向相手に合わせて、設定してください。 IPsec 対象のサブネットが複数ある場合は、リモート ID に複数入力してください。	未設定
暗号化アルゴリズム	IKE_AUTH 交換で利用する暗号化アルゴリズムを設定します。 • AES256-CBC • AES192-CBC • AES128-CBC • 3DES-CBC • NULL		AES256-CBC
認証アルゴリズム	IKE_AUTH 交換で利用する認証アルゴリズムを設定します。 • HMAC-SHA1-96 • HMAC-SHA2-256 • HMAC-MD5-96		HMAC-SHA1-96

	ライフタイム（秒）	IPsec SA の有効期間を設定します。 入力範囲は、300~691,200 秒です。	対向先の設定と比較して、短い方の値を使用します。設定したライフタイムの 70%から 85%の間でランダムにリキーします。	28800
	ライフタイムデータ量(Kbyte)	IPsec SA 上で通信するデータ量を Kbyte で指定します。		指定しない
	PFS	• 無効…PFS を保証しません • 768bit…DH-Group1 を使用して PFS を保証 • 1024bit…DH-Group2 を使用して PFS を保証 • 1536bit…DH-Group5 を使用して PFS を保証 • 2048bit…DH-Group14 を使用して PFS を保証	PFS (Perfect Forward Secrecy)	無効
	Rekey	• Enable…IPsec 対象のトラフィックが発生した際に IKE ネゴシエーションを開始します。また、生成済みの SA を利用したトラフィックがある場合、リキーします。 • Always…IPsec 対象のトラフィックの有無に関係なく、本製品の WAN インタフェースに IP アドレスを設定した後に IKE ネゴシエーションを開始します。また、生成済みの SA を利用したトラフィックの有無にかかわらず、リキーします。 • No Rekey…IPsec 対象のトラフィックが発生した際に IKE ネゴシエーションを開始します。本モードの場合、リキーしません。		Enable
	Rekey 残り時間(秒)	Rekey 残り時間（秒）が指定された値(30～345600 秒)以下となるタイミングで SA の自動更新を開始します。		未設定

[メモ]

IPsec のリモート ID と静的ルーティング設定の優先順位は次のとおりです。

VPN 動作モードがポリシーベースの場合、IKE Phase2 のリモート ID を登録すると、自動で静的ルートを登録します。このルートは、通常の静的ルートより優先されます。IKE Phase2 のローカル ID に対するルートは、自動で静的ルートは登録されないので、IPv4 ルーティング設定を追加する必要があります。

※上記は IKEv1 についてですが、IKEv2 の IKE_AUTH 交換設定ローカルトラフィックセレクタ、リモートトラフィックセレクタについても同様となります。

■IKE Phase1 のローカル ID とリモート ID の組み合わせによる動作　※IKEv2 では IKE_SA_INIT 交換が該当します

接続形態	ローカル ID	リモート ID	用途	備考
パターン 1	指定なし(ローカル WAN IP アドレス(サブネットなし))	指定なし（peer IP アドレス(サブネットなし))	○	
パターン 2	指定あり(文字列)(IP アドレス, FQDN, Key-ID, User-FQDN)	指定なし(peer IP アドレス(サブネットなし))	○	
パターン 3	指定なし(ローカル WAN IP アドレス(サブネットなし))	指定あり(文字列)(IP アドレス, FQDN, Key-ID, User-FQDN)	○	
パターン 4	指定あり(文字列)(IP アドレス, FQDN, Key-ID, User-FQDN)	指定あり(文字列)(IP アドレス, FQDN, Key-ID, User-FQDN)	○	
パターン 5	指定なし(ローカル WAN IP アドレス(サブネットなし))	指定なし(未使用)	○	宛先拠点 any 時
パターン 6	指定あり(文字列)(IP アドレス, FQDN, Key-ID, User-FQDN)	指定なし(未使用)	○	宛先拠点 any 時

■IKE Phase2 のローカル ID とリモート ID の組み合わせによる動作

・IPsec トンネル先のサブネット宛て接続は、単独（1 個）～複数（2-5 個)、または全サブネット宛ての接続が可能

・各サブネット接続時の IKE Phase2 のローカル ID、リモート ID の設定方法は次のとおりです。

N…2~5 個指定、ALL…すべてのサブネット

※IKEv2 では IKE_AUTH 交換のローカルトラフィックセレクタとリモートトラフィックセレクタが該当します。

接続形態	LAN-WAN 接続パターン	ローカル ID (ローカルトラフィックセレクタ)	リモート ID (リモートトラフィックセレクタ)
単独サブネット接続	1:1	1 個指定	1 個指定
	N:1	N 個指定	1 個指定
	ALL:1	0.0.0.0/0 もしくは指定なし（空欄）	1 個指定
複数サブネット接続	1:N	1 個指定	N 個指定
	N:N	N 個指定	N 個指定
	ALL:N	0.0.0.0/0 もしくは指定なし（空欄）	N 個指定
全サブネット接続*	1:ALL	1 個指定	0.0.0.0/0 もしくは指定なし（空欄）
	N:ALL	N 個指定	0.0.0.0/0 もしくは指定なし（空欄）
	ALL:ALL	0.0.0.0/0 もしくは指定なし（空欄）	0.0.0.0/0 もしくは指定なし（空欄）

* インターネット宛てのすべてのトラフィックを IPsec トンネル宛てにする場合

■リキータイミング

IKE フェーズ 1/フェーズ 2 のライフタイムから IKE SA/IPsec SA のリキータイミングを決定します。

なお、リキータイミングはライフタイムの 70%～85%の間でランダムに決定します。

※IKEv2 では IKE_SA_INIT 交換/ IKE_AUTH 交換のライフタイムが該当します

[例]

IKE フェーズ 1 ライフタイム 28800 秒の場合

28800 x 0.70 = 20160 秒 [最小値]

この間でリキーが実行される

28800 x 0.85 = 24480 秒 [最大値]

■IKEv1 の IKE フェーズ 1/フェーズ 2 のローカル ID、リモート ID を以下のように扱います。

					IKE (IKE Phase1)		IPsec (IKE Phase2)	
フェーズ	モード	動作	対地数	方向	local-id	remote-id	local-id	remote-id
IKE Phase1 (=Ph1)	main mode	initiator	1	送信	シーケンス 5 で送信	送信しない		
				対向からの受信	自局の remote-id と比較する	未使用		
		responder	1	送信	シーケンス 6 で送信	送信しない		
				対向からの受信	自局の remote-id と比較する	未使用		
	aggressive mode	initiator	1	送信	シーケンス 1 で送信	送信しない		
				対向からの受信	自局の remote-id と比較する	未使用		
		responder	1 (any) *	送信	シーケンス 2 で送信	送信しない		
				対向からの受信	自局の remote-id と比較する	未使用		
IKE Phase2 (=Ph2)	quic mode	initiator	1	送信			シーケンス 1 で送信	シーケンス 1 で送信
				対向からの受信			未使用	未使用
		responder	1	送信			シーケンス 2 で送信	シーケンス 2 で送信
				対向からの受信			自局の remote-id と比較する	自局の local-id と比較する

* initiator として動作する IPsec 機器を特定しませんが、確立できる IPsec トンネルは 1 本です。

■IKEv2 のローカル ID、リモート ID を以下のように扱います。

					IKEv2	
フェーズ	モード	動作	対地数	方向	local-id	remote-id
IKE AUTH 交換	-	initiator	1	送信	IKE AUTH 交換リクエストで送信	IKE AUTH 交換リクエストで送信
				対向からの受信	自局の remote-id と比較する	自局の local-id と比較する
		responder	1	送信	IKE AUTH 交換レスポンスで送信	IKE AUTH 交換レスポンスで送信
				対向からの受信	自局の remote-id と比較する	自局の local-id と比較する

■IKEv2 の認証方式組み合わせ動作

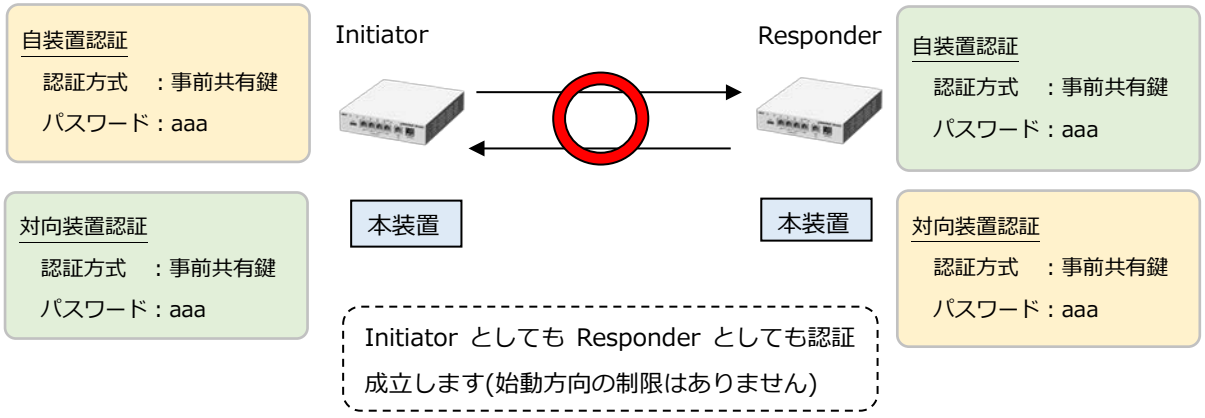
IKEv2 では自装置認証と対向装置認証をそれぞれ設定する必要があり、かつ、認証方式としても事前共有鍵認証、EAP-MD5 認証、デジタル署名認証の 3 つをサポートします。

※EAP-MD5 認証は被認証側のみサポート。デジタル署名認証は要求者側のみサポートします。

IKEv2 の認証が成立するパターン／成立しないパターンの設定例を以下に示します。

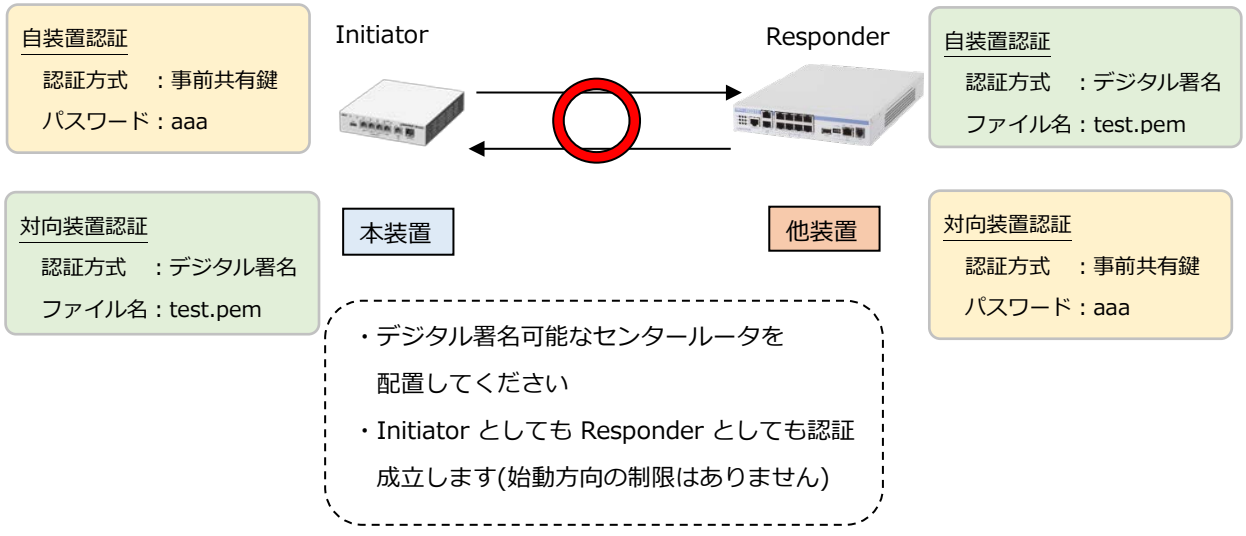
(1) 認証成立パターン①

すべて事前共有鍵のみで設定したパターンです。



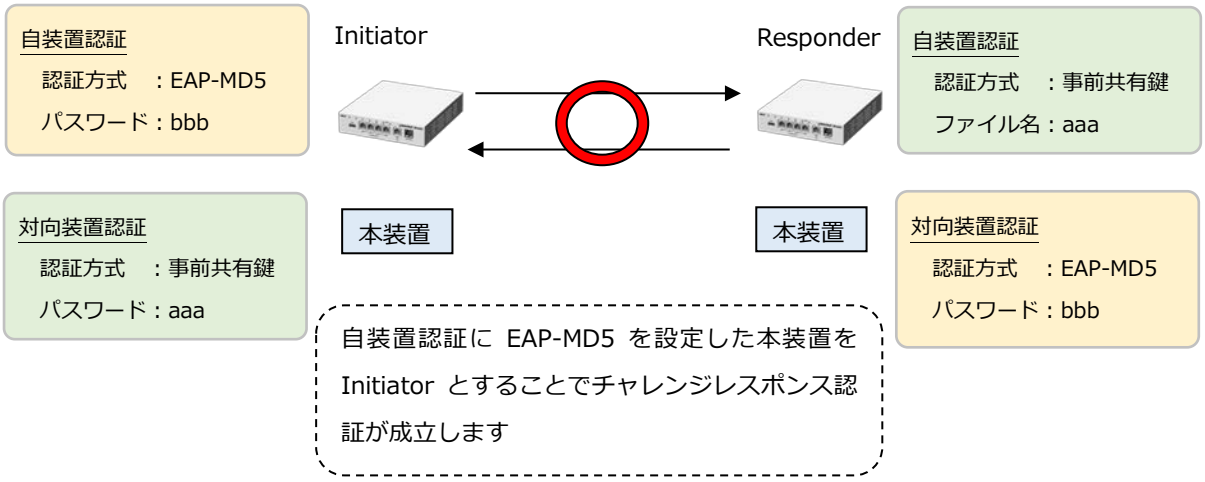
(2) 認証成立パターン②

事前共有鍵＋デジタル署名で設定したパターンです。



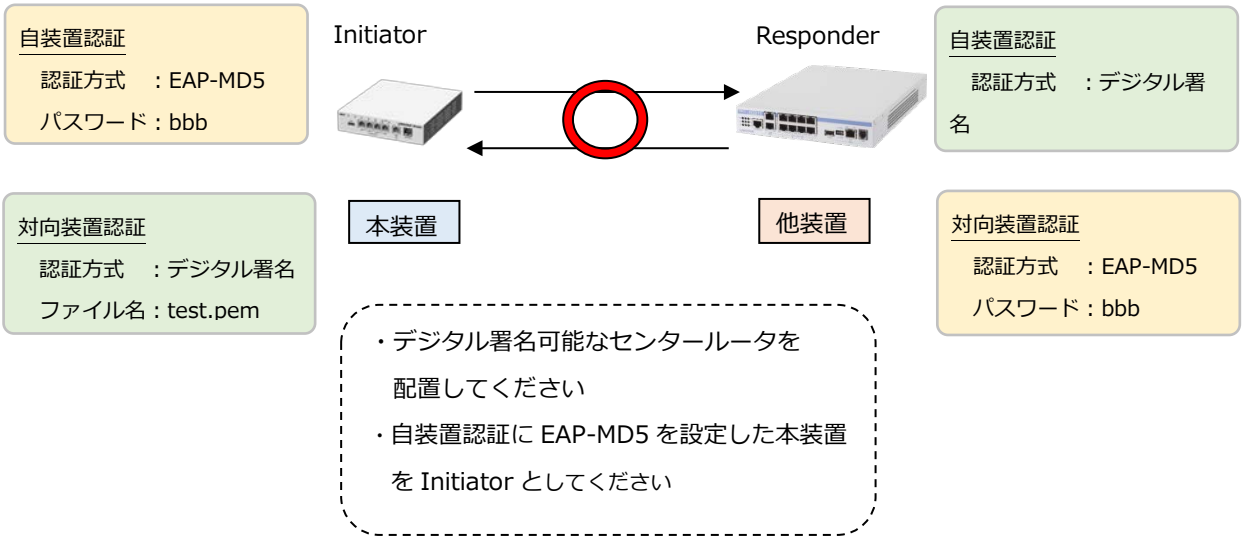
(3) 認証成立パターン③

EAP-MD5＋事前共有鍵で設定したパターンです。



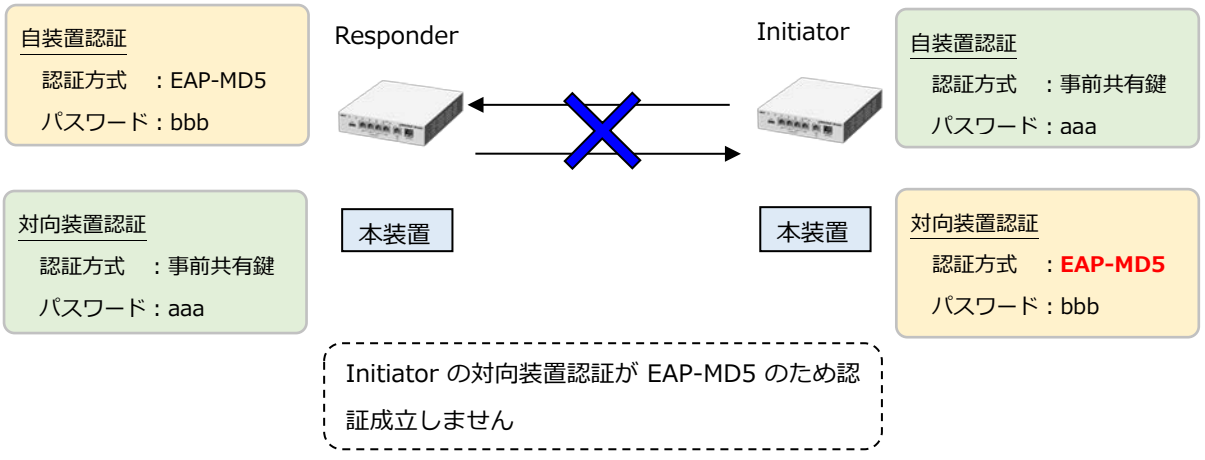
(4) 認証成立パターン④

EAP-MD5＋デジタル署名で設定したパターンです。



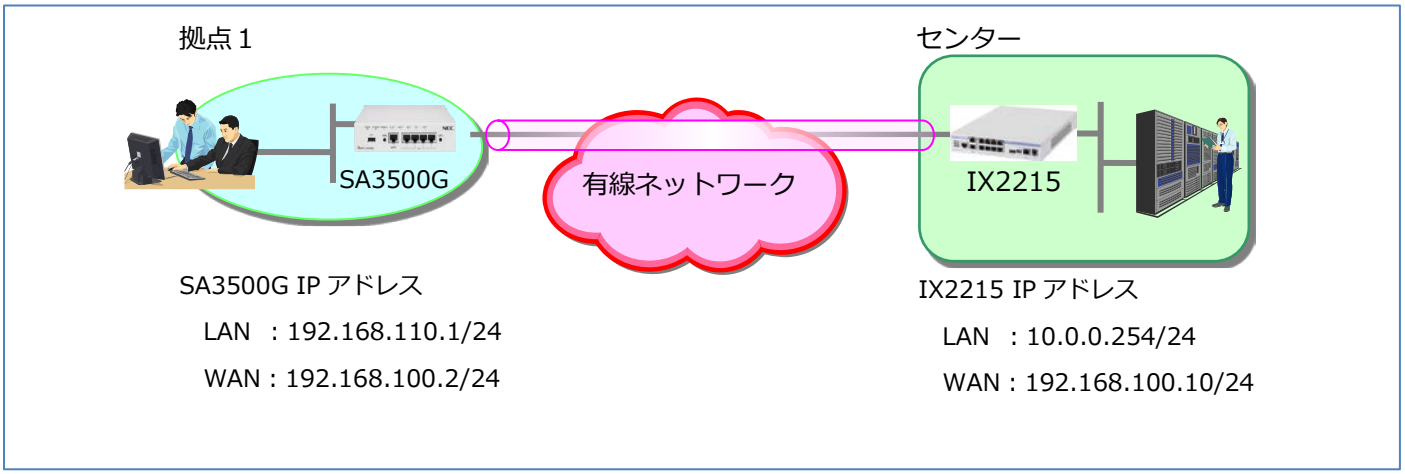
(5) 認証成立しないパターン

EAP-MD5＋事前共有鍵で設定したパターンです(始動方向誤り)。



[IPsec の設定例(IKEv1)]

本製品と IX2215 との間で IPsec 通信を行う場合の設定例を示します。



■拠点 1 SA3500G の設定

設定 Web の[IPsec 設定]で、次のように設定を行います。

IPsec設定	
IPsec機能	使用する
IKEバージョン	IKEv1 IKEv2
VPN動作モード	ポリシーベース ルートベース
フラグメント方式	post-fragment pre-fragment
静的ルーティング	デフォルトルートに設定する
TCP/MSS調整	使用する 自動 固定(byte)
IKEフェーズ1設定	
事前共有鍵	•••••
鍵交換方式	メインモード
ローカルID指定	指定しない(送信元IPアドレス)
ローカルID	
リモートID指定	指定しない(宛先IPアドレス)
リモートID	
暗号化アルゴリズム	AES256-CBC
認証アルゴリズム	HMAC-SHA1
ライフタイム(秒)	28800
DH-Group選択	768bit
DPD-Keepalive	使用する
DPD-Keepalive送信間隔(秒)	
DPD-Keepaliveリトライアウト回数	
IKE再送間隔指定(秒)	指定する:
IKE再送回数指定(回)	指定する:

IKEフェーズ2設定 ?

対向拠点指定方法 ?	IPアドレス ▼
対向拠点宛先 ?	192.168.100.10
ローカルID:1 ?	192.168.110.0 / 24
ローカルID:2 ?	/
ローカルID:3 ?	/
ローカルID:4 ?	/
ローカルID:5 ?	/
リモートID:1 ?	/
リモートID:2 ?	/
リモートID:3 ?	/
リモートID:4 ?	/
リモートID:5 ?	/
暗号化アルゴリズム ?	AES256-CBC ▼
認証アルゴリズム ?	HMAC-SHA1-96 ▼
ライフタイム(秒) ?	28800
ライフタイムデータ量(Kbyte) ?	指定する:
PFS ?	無効 ▼
Commit-bit ?	使用する
Rekey ?	Enable ▼
Rekey残り時間(秒) ?	指定する:

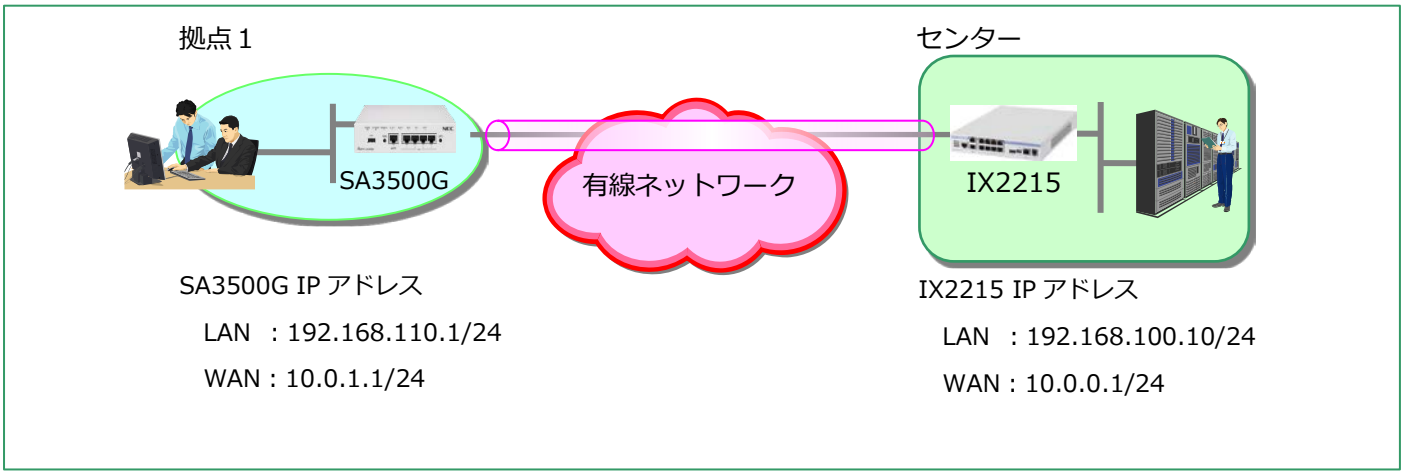
設定

■センター側 IX2215 の設定

設定 Web を開き、次のように VPN 設定を行います。

[IPsec の設定例(IKEv2)]

本製品と IX2215 との間で IKEv2 による IPsec 通信を行う場合の設定例を示します。



■拠点 1 SA3500G の設定

設定 Web の[IPsec 設定]で、次のように設定を行います。

IPsec設定	
IPsec機能	☑ 使用する
IKEバージョン	○ IKEv1 ◉ IKEv2
VPN動作モード	◉ ポリシーベース ○ ルートベース
フラグメント方式	◉ post-fragment ○ pre-fragment
静的ルーティング	☐ 使用する
TCP/MSS調整	☑ 使用する ◉ 自動 ○ 固定(byte)
IKE_SA_INIT交換設定	
認証方式：自装置	◉ 事前共有鍵 ••••• ○ EAP-MD5
認証方式：対向装置	◉ 事前共有鍵 ••••• ○ EAP-MD5 ○ デジタル署名： CAtest.pem ファイルを選択 選択されていません
ローカルID指定	指定しない(送信元IPアドレス)
ローカルID	
リモートID指定	指定しない(宛先IPアドレス)
リモートID	
暗号化アルゴリズム	AES256-CBC
認証アルゴリズム	HMAC-SHA1
PRFアルゴリズム	HMAC-SHA1
ライフタイム(秒)	28800
DH-Group選択	768bit
DPD-Keepalive	☐ 使用する
DPD-Keepalive送信間隔(秒)	
IKE再送間隔指定(秒)	☐ 指定する:
IKE再送回数指定(回)	☐ 指定する:
ネゴシエーション方向限定	both

IKE_AUTH交換設定

対向拠点指定方法	IPアドレス
対向拠点宛先	10.0.0.1
ローカルトラフィックセレクタ:1	192.168.110.0 / 24
ローカルトラフィックセレクタ:2	/
ローカルトラフィックセレクタ:3	/
ローカルトラフィックセレクタ:4	/
ローカルトラフィックセレクタ:5	/
リモートトラフィックセレクタ:1	/
リモートトラフィックセレクタ:2	/
リモートトラフィックセレクタ:3	/
リモートトラフィックセレクタ:4	/
リモートトラフィックセレクタ:5	/
暗号化アルゴリズム	AES256-CBC
認証アルゴリズム	HMAC-SHA1-96
ライフタイム(秒)	28800
ライフタイムデータ量(Kbyte)	指定する:
PFS	無効
Rekey	Enable
Rekey残り時間(秒)	指定する:

設定

■センター側 IX2215 の設定

ローカルコンソールから、次のように VPN 設定を行います。

```
!
ip route default 10.0.0.254
ip route 192.168.110.0/24 Tunnel0.0
!
ikev2 authentication psk id ipv4 10.0.1.1 key char hogehoge
ikev2 authentication psk id ipv4 10.0.0.1 key char hogehoge
!
ikev2 default-profile
  sa-proposal enc aes-cbc-256
  sa-proposal integrity sha1
  sa-proposal dh 768-bit
  sa-proposal prf sha1
!
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  no shutdown
!
interface GigaEthernet1.0
  ip address 192.168.100.10/24
  no shutdown
!
interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet1.0
  ikev2 child-lifetime 28800
  ikev2 child-pfs off
  ikev2 child-proposal enc aes-cbc-256
  ikev2 child-proposal integrity sha1
  ikev2 dpd off
  ikev2 local-authentication psk id ipv4 10.0.0.1
  ikev2 sa-lifetime 28800
  ikev2 local-ts ipv4 address 192.168.100.0/24
  ikev2 remote-ts ipv4 address 192.168.110.0/24
  ikev2 peer 10.0.1.1 authentication psk id ipv4 10.0.1.1
  no shutdown
!
```

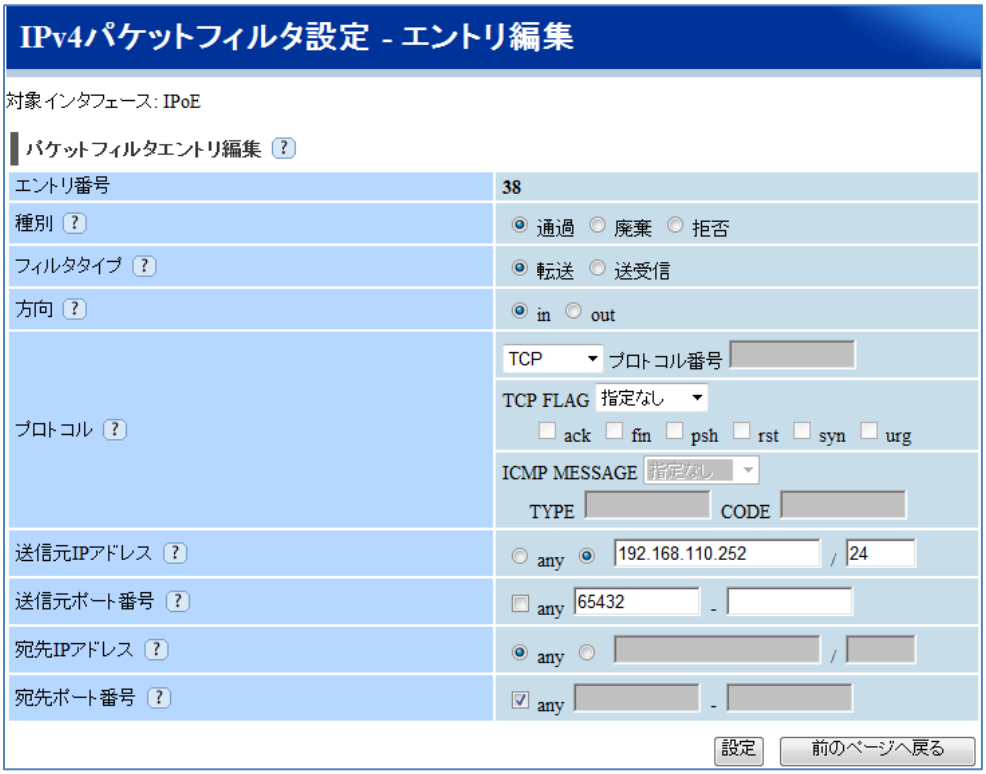
5.7.17. IPv4 パケットフィルタエントリに関する設定

対象のインタフェースを指定して、特定の条件を満たすパケットの通過や廃棄を設定します。

※対象インタフェースで IPsec1 を選択した場合のご注意

IPsec の設定で VPN 動作モードをルートベースに設定しているときのみ、対象インタフェース“IPsec1”の設定が有効となります。

1. [TOP]-[メンテナンス]-[フィルタ設定]- [IPv4 パケットフィルタ設定]画面を開きます。
2. 「対象インタフェースを選択」でフィルタリングポイントを選択します。「IPoE」、「PPPoE」、「LAN」、「IPsec1」から選択します。
3. 「編集」をクリックすると下記画面に遷移し、そのエントリのフィルタ設定を行います。



4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
パケットフィルタエントリ編集		フィルタリングポイントごとに50 エントリ設定できます。	
エントリ番号	エントリの番号が入ります。	エントリ番号 1～37 は初期状態でIPv4パケットフィルタエントリを設定しています。変更、削除は可能ですが、そのまま利用していただくことを推奨します。	38 以降は未設定
種別	• 通過…本エントリに合致する IP パケットを通過 • 廃棄…本エントリに合致する IP パケットを廃棄（silently discard） • 拒否…本エントリに合致する IP パケットに対してエラーメッセージを送信 ・TCP: TCP reset を送信 ・TCP 以外: ICMP destination unreachable を送信		通過
フィルタタイプ	• 転送…本製品宛て以外の IP パケット • 送受信…本製品宛ての IP パケット		転送
方向	• in…本製品が受信する IP パケット • out…本製品が送信する IP パケット		in
プロトコル	• IP すべて…すべての IP パケット • ICMP • TCP • UDP • その他…上記以外の IP パケット（プロトコル番号で指定してください） • TCP FLAG…TCP パケットのうち、特定フラグの TCP パケットのみ対象にする場合に選択 • ICMP MESSAGE…ICMP パケットのうち、特定の ICMP メッセージのみ対象にする場合に選択		IP すべて
送信元 IP アドレス	• any…すべてを対象とする場合 • アドレス指定…特定の IP アドレスを指定する場合		any
送信元ポート番号	• any…すべてを対象とする場合 • ポート番号指定…特定のポートを指定する場合		未設定
宛先 IP アドレス	• any…すべてを対象とする場合 • アドレス指定…特定の IP アドレスを指定する場合		any
宛先ポート番号	• any…すべてを対象とする場合 • ポート番号指定…特定のポートを指定する場合		未設定

5.7.18. **MAC アドレスフィルタリングに関する設定**

メンテナンス（ブリッジモード）の設定と同じです。5.6.7 章を参照してください。

5.7.19. **SNMP エージェントの設定**

SNMP を使用して、本製品の状態を監視、制御できます。

本製品がサポートしている SNMP のバージョンは、バージョン 1 とバージョン 2c です。

1. [TOP]-[メンテナンス]-[管理設定]-[SNMP 設定]画面を開きます。
2. SNMP に関する各種項目を設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
SNMP エージェント設定			
SNMP エージェント	• チェック有…SNMP 機能を使用する場合 • チェック無…SNMP 機能を使用しない場合	SNMP 機能を使用する場合はコミュニティ名の設定が必要です。	無効
装置の物理的位置（sysLocation）	装置の設置場所（sysLocation）をメモできます。 入力可能文字列：半角英数記号 文字数最大：64 文字	0x21～0x7e が使用できます。 使用不可文字列は　"　$　'　`　#　¥（バックスラッシュ）およびスペースです。	未設定
連絡先（sysContact）	連絡先（sysContact）をメモできます。 入力可能文字列：半角英数記号 文字数最大：64 文字	0x21～0x7e が使用できます。 使用不可文字列は　"　$　'　`　#　¥（バックスラッシュ）およびスペースです。	未設定
アクセス制限	特定の SNMP マネージャのみ本製品の SNMP 機能へのアクセスを許容するか、すべての SNMP マネージャからのアクセスを許容するかを設定します。 • チェック有…特定の SNMP マネージャのみアクセスを許容 • チェック無…すべての SNMP マネージャのアクセスを許容	本機能を使用する場合、1 つ以上の SNMP マネージャを設定してください。	無効
SNMP マネージャ 1～3	「アクセス制限」機能を使用する場合の SNMP マネージャの IP アドレスを設定します。		未設定
SNMP コミュニティ設定			
コミュニティ 1～3	SNMP のコミュニティ名を設定します。 入力可能文字列：半角記号 文字数最大：32 文字	0x21～0x7e が使用できます。 使用不可文字列は　"　$　'　`　#　¥（バックスラッシュ）およびスペースです。	未設定
SNMP トラップ設定			
SNMP トラップ	• チェック有…トラップ送信機能を使用する場合 • チェック無…トラップ送信機能を使用しない場合		無効
SNMP トラップ種別	送信するトラップの指定 • ALL…すべての種別のトラップを送信する場合 • トラップ設定…一部のトラップを送信する場合（本項目を選択した場合は、送信対象とするトラップのチェックボックスをチェックしてください）		ALL

		cold-start：電源 OFF から電源 ON の場合に送信 link-down：インタフェースがダウンした場合に送信 link-up:インタフェースが起動した場合に送信 auth-failure：コミュニティ名不一致により認証失敗した場合に送信		
	SNMP トラップ送信時の遅延時間設定（秒）	coldStart トラップを遅延させる時間を設定します。 設定範囲は、0~3,600 秒です。		5
表				
	No.1～3	• 連絡先…トラップの送信先の IP アドレス		未設定
		• コミュニティ…トラップを送信する際のコミュニティ名を「コミュニティ 1」「コミュニティ 2」「コミュニティ 3」から選択		コミュニティ 1
		• バージョン…SNMP バージョンを「v2c」「v1」から選択	v2c…SNMPv2c v1…SNMPv1	v2c

5.7.20. **ログ送信設定**

メンテナンス（ブリッジモード）の設定と同じです。5.6.11 章を参照してください。

5.7.21. **設定 Web のアクセス管理**

メンテナンス（ブリッジモード）の設定と同じです。5.6.12 章を参照してください。

5.7.22. **時刻の設定**

メンテナンス（ブリッジモード）の設定と同じです。5.6.13 章を参照してください。

5.7.23. **設定値の保存、復元**

メンテナンス（ブリッジモード）の設定と同じです。5.6.14 章を参照してください。

5.7.24. **設定値の初期化**

メンテナンス（ブリッジモード）の設定と同じです。5.6.15 章を参照してください。

5.7.25. **ファームウェアの更新**

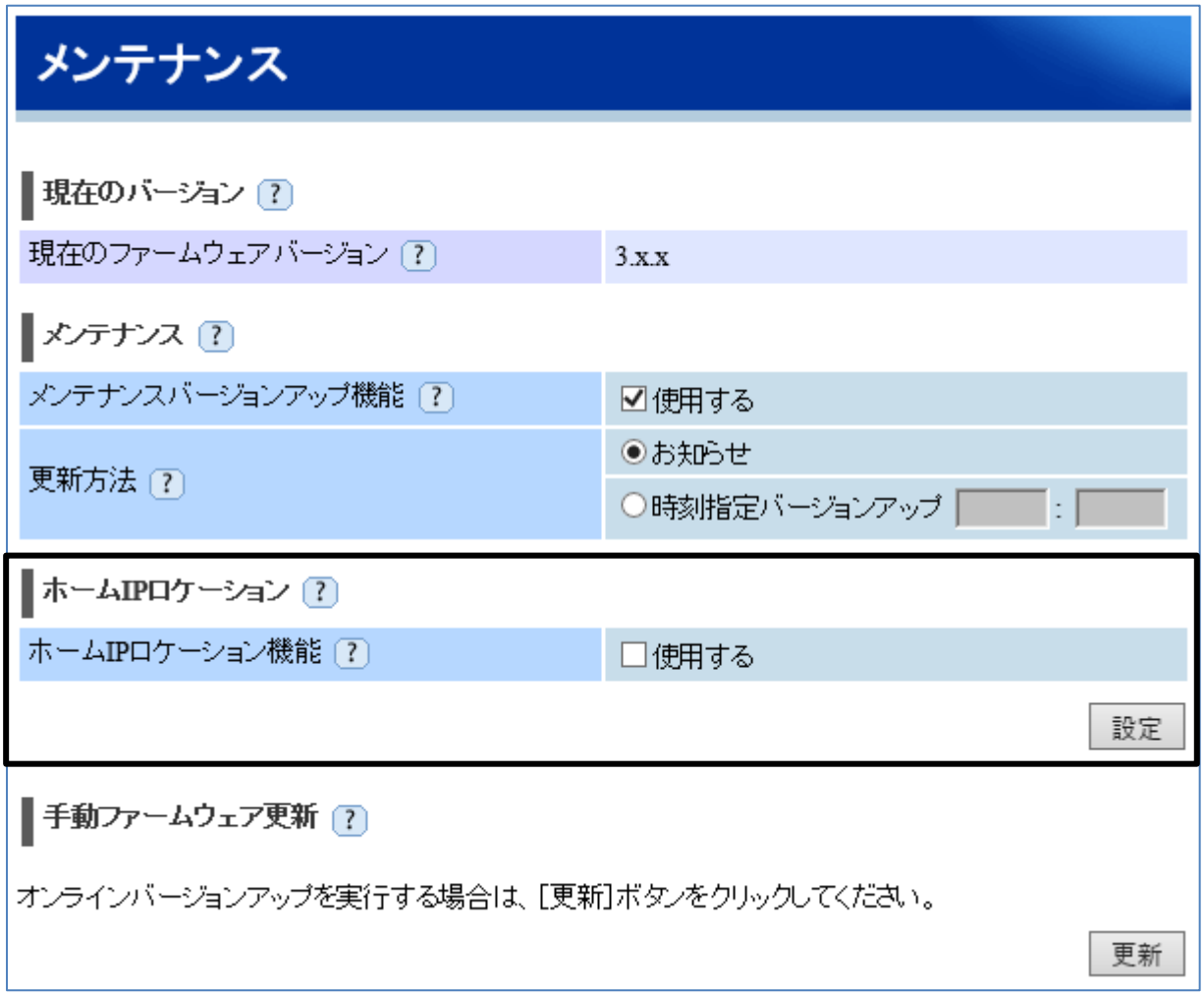
メンテナンス（ブリッジモード）の設定と同じです。5.6.16 章を参照してください。

5.7.26. **ホーム IP ロケーションの設定**

本機能は、本画面で設定します。また、下記条件にて有効になります。

- ルータモードに設定されている（初期値：「ブリッジモード」）
- WAN 側にグローバル IP アドレスが付与されている

■ホーム IP ロケーションの設定



1. [TOP]-[メンテナンス]-[メンテナンス]-画面を開きます。
2. 次の項目のチェックボックスをチェックします。
   ・メンテナンス：メンテナンスバージョンアップ機能（初期値：有効）
   ・ホーム IP ロケーション：ホーム IP ロケーション機能（初期値：無効）
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、本設定を保存します。

[ホーム IP ロケーション名の確認方法]

1. [TOP]-[メンテナンス]-[情報]-[デバイスの状態]の画面を開きます。（6.1.2 章を参照してください）
2. ホーム IP ロケーション：ホーム IP ロケーション名 で確認します。

[メモ]

インターネット側から本製品にホーム IP ロケーション名でアクセスできない場合には、ネットワーク環境を再確認してください。

5.7.27. **再起動**

メンテナンス（ブリッジモード）の設定と同じです。5.6.17 章を参照してください。

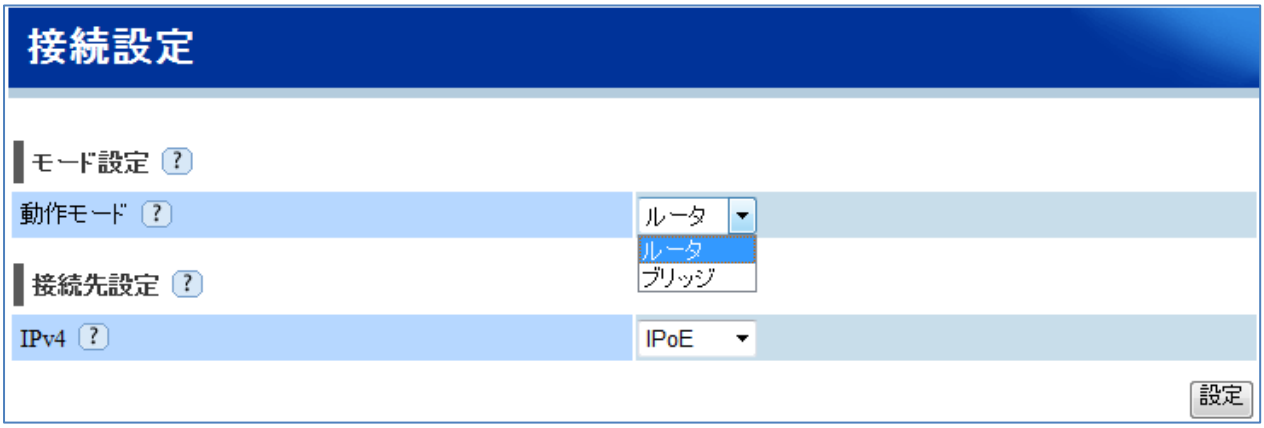
5.7.28. **保守機能**

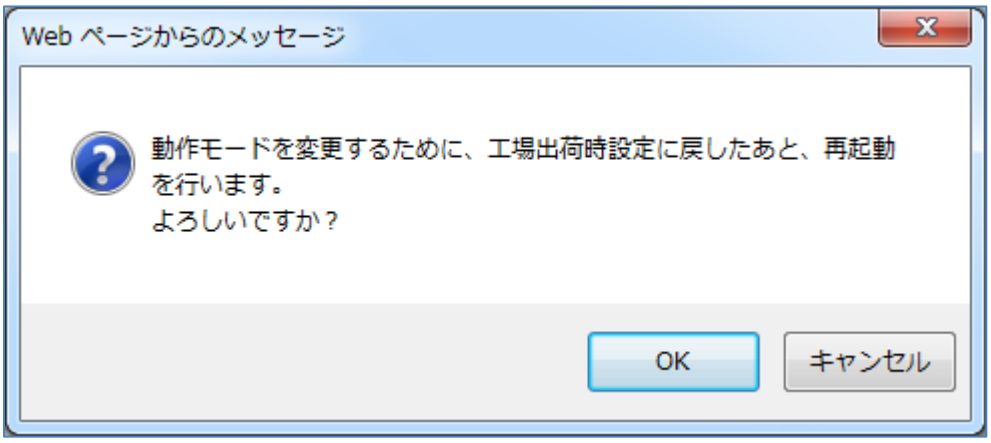
メンテナンス（ブリッジモード）の設定と同じです。5.6.18 章を参照してください。

5.7.29. **ブリッジモードへの切り替え**

ブリッジモードに切り替える際、本製品を再起動します。

また、すべての設定を初期化します。





1. [TOP]-[メンテナンス]-[基本設定]-[接続設定]画面を開きます。
2. モード設定で「ブリッジ」を選択します。
3. 「設定」ボタンを押下します。
4. 再起動する旨のメッセージウィンドウを表示しますので、OK ボタンを押下します。
5. 再起動後、設定ウィザードの STEP2（管理者パスワード）が実行されます。5.2.1 章を参照し、設定してください。

5.8. セキュリティ・スキャン機能に関する設定

[メモ]

セキュリティ・スキャン機能は、基本的にブリッジモード、ルータモードで共通です。

本製品のセキュリティ・スキャン機能の設定、および情報を閲覧します。

1. TOP ページで「セキュリティ」をクリックします。

2. セキュリティ・スキャン機能に関する設定画面が開きます。

※上図はルータモードの画面例です。保存ボタンの位置は、ブリッジモードでも同じです。

5.8.1. **設定画面構成**

セキュリティに関する設定画面構成は次のとおりです。

項目	説明	操作の必要性の有無/備考
セキュリティ	セキュリティ・スキャン機能に関する設定	セキュリティ検出レベルをお客様の状況に応じて、設定/変更してください
ステータス	セキュリティ・スキャン機能のライセンス情報 セキュリティ・スキャン機能の各機能の状態を表示 シグネチャの更新	
基本設定	セキュリティ無効時のパケット転送の有効設定 TCP ストリームの厳格チェックの有効設定	
ファイアウォール（FW）	DoS アタックに関する設定 SPI の設定 NAPT セッションタイマの設定	
アンチウイルス（AV）	ウイルススキャンに関する設定 個別許可の設定	
不正侵入防止（IPS）	IPS に関する設定 個別許可の設定	
Web ガード（WG）	特に危険な Web サイトへのアクセス可否の設定 Web ガードに関する設定 個別許可の設定	
URL フィルタリング（UF）	カテゴリ単位で Web サイトへのアクセス可否を設定 カテゴリの設定 個別許可の設定 指定の URL が該当するカテゴリの確認	
URL キーワードフィルタリング（KF）	特定 URL（キーワード）へのアクセス可否の設定 キーワードと検出時の動作の設定	
アプリケーションガード（APG）	アプリケーションの通信可否の設定 通信をブロックするアプリケーションの選択	
メール通知	イベントを通知するメールアドレスの設定 イベントの設定 メールアカウントの設定 イベント検出時の宛先メールアドレスの設定	
セキュリティログ	セキュリティ・スキャン機能に関係するログ表示 個別許可の設定	定期的な確認を推奨します
統計情報	セキュリティ・スキャン機能の統計情報の表示	定期的な確認を推奨します
高度な設定	脅威検出画面とメール通知の通知文編集	
簡易 RADIUS 機能	RADIUS 認証に関する設定	

5.8.2. 基本設定

パケット転送機能に関する設定を運用ポリシーにしたがい、適切な内容に設定してください。本製品はセキュリティ・スキャン機能のライセンスが満了したとき、もしくはセキュリティ・スキャン機能が準備中のときにパケット転送を遮断します。本機能を設定で解除することができます。

1. [TOP]-[セキュリティ]-[基本設定]画面を開きます。
2. パケット転送制限を解除する場合、本項目にチェックを入れます。
3. TCP ストリームの厳格チェック設定を行う場合、本項目にチェックを入れます。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、設定値を保存します。

設定項目	説明	初期値
セキュリティ・スキャン機能無効時の設定	セキュリティ・スキャン機能無効時にパケット転送する場合は、本項目をチェックします。	無効
TCP ストリームの厳格チェック設定	本製品は以下の場合に厳格チェックによるパケットの廃棄を行います。 ・TCP のハンドシェークが確認できない TCP セッションのパケット ・ICMP の request パケットが確認できない reply パケット（ping の reply など） 上記のパケットを転送する場合は、本項目をチェックします。なお、このとき当該パケットに対するセキュリティ・スキャンは行われません。	無効

5.8.3. ファイアウォール（FW）

ファイアウォール機能を運用ポリシーにしたがい、適切な内容に設定してください。動作モードによって設定項目が異なりますので、ブリッジモードとルータモードを分けて説明します。

[ブリッジモードの場合]

■ファイアウォール（FW）タブ

1. [TOP]-[セキュリティ]-[ファイアウォール（FW）]画面を開きます。
2. ファイアウォール機能の有効/無効の設定をします。初期値は無効です。無効に設定した場合は SPI 設定が設定不可となります。
3. SPI 設定をセキュリティポリシーにしたがって設定します。
4. DoS プロテクション機能をセキュリティポリシーにしたがって設定します。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下して、設定値を保存します。

設定項目	説明	初期値
ファイアウォール設定		
機能を使用する(IPv4)	ファイアウォール機能の有効/無効の設定をします。無効に設定した場合、SPI 設定はグレーアウトして設定ができなくなります。	無効
IPv6 通信をすべてブロックする	ブリッジモード時に IPv6 通信を通過させるか、遮断するかを設定します。	無効
SPI 設定	ステートフルパケットインスペクションに関する設定項目です。	
TCP	TCP establish のセッションタイマを設定します。 設定範囲は、30~86400 秒です。 ※上位ルータとして利用されることがある IX シリーズの SPI 設定(初期値:900 秒)に合わせて、初期値を 600 秒から 900 秒に変更しました。 (ファームウェア Ver 3.6.9 以降)	900

	UDP	UDP のセッションタイマを設定します。設定範囲は、30~86400 秒です。	300
	ICMP	ICMP のセッションタイマを設定します。 設定範囲は、30~86400 秒です。	30
DoS プロテクション		DoS 攻撃（Smurf 攻撃、IP スプーフィング攻撃）を検出し、これらのアクセスを廃棄する場合は、本項目をチェックします。 本機能を無効化した場合、Smurf 攻撃、IP スプーフィング攻撃のパケットを検出対象から外します。	無効

[ルータモードの場合]

■ファイアウォール（FW）タブ

1. [TOP]-[セキュリティ]-[ファイアウォール（FW）]画面を開きます。
2. ファイアウォール機能の有効/無効の設定をします。初期値は有効です。無効に設定した場合は SPI 設定が設定不可となります。
3. NAPT 有効インタフェースをセキュリティポリシーにしたがって設定します。チェックを外すと該当インタフェースの NAPT 機能が無効となります。
4. DoS プロテクション機能をセキュリティポリシーにしたがって設定します。
5. NAPT セッションタイマをネットワーク運用条件に合わせて設定します。
6. 「設定」ボタンを押下します。
7. 「保存」ボタンを押下して、設定値を保存します。

設定項目	説明	初期値
ファイアウォール設定		
機能を使用する	ファイアウォール機能の有効/無効の設定をします。無効に設定した場合、SPI 設定はグレーアウトして設定ができなくなります。 PPPoE 設定のとき、ファイアウォール機能は常に有効となり、無効に設定できません。	有効

NAPT 有効インタフェース	NAPT 機能を有効にするインタフェースにチェックを入れます。 ※ルータモードのときのみ、本設定項目が表示されます。	
IPoE	IPoE で NAPT を有効にする場合にチェックを入れます。	有効
PPPoE	PPPoE では NAPT は常に有効となります。	有効
SPI 設定	ステートフルパケットインスペクションに関する設定項目です。	
TCP	TCP establish のセッションタイマを設定します。 設定範囲は、30~86400 秒です。	3600
UDP	UDP のセッションタイマを設定します。 設定範囲は、30~86400 秒です。	300
ICMP	ICMP のセッションタイマを設定します。 設定範囲は、30~86400 秒です。	30
DoS プロテクション	DoS 攻撃（Smurf 攻撃、IP スプーフィング攻撃）を検出し、これらのアクセスを廃棄する場合は、本項目をチェックします。 本機能を無効化した場合、Smurf 攻撃、IP スプーフィング攻撃のパケットを検出対象から外します。	有効

※「NAPT 有効インタフェース」を無効にすると、ご使用の環境によってはインターネットにアクセスできなくなる場合があります。その場合は 7.1.17 章を参考に、本製品の上位側に接続しているネットワーク機器の設定を見直してください。

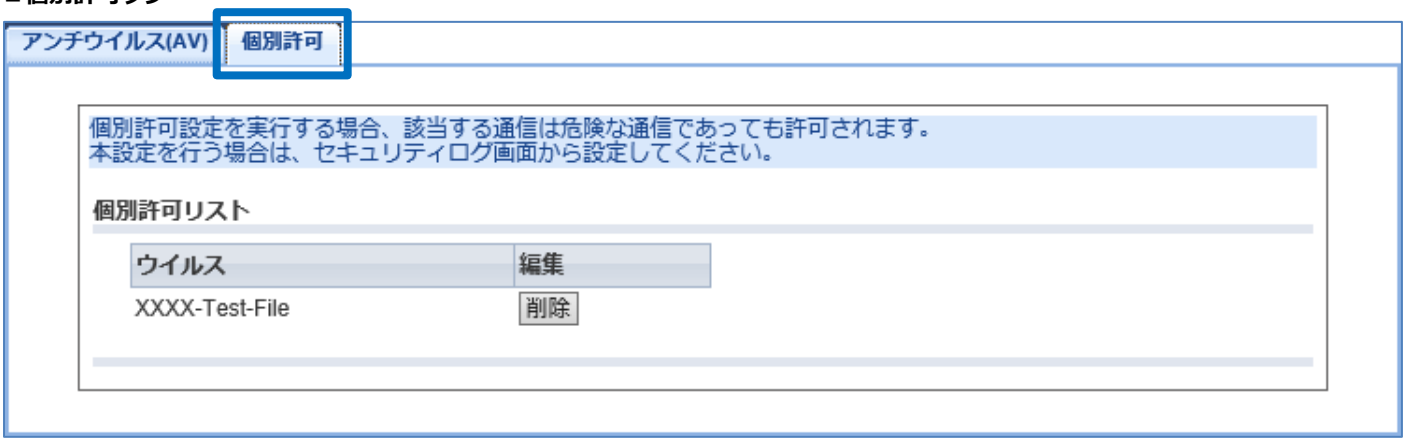
5.8.4. **アンチウイルス（AV）**

アンチウイルス機能を運用ポリシーにしたがい、適切な内容に設定してください。

■アンチウイルス（AV）タブ

1. [TOP]-[セキュリティ]-[アンチウイルス（AV）]画面を開きます。
2. アンチウイルス機能をセキュリティポリシーにしたがって設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、設定値を保存します。

■個別許可タブ



※画面は”XXXX-Test-File”を登録した表示例です。初期状態ではリストは設定されていません。

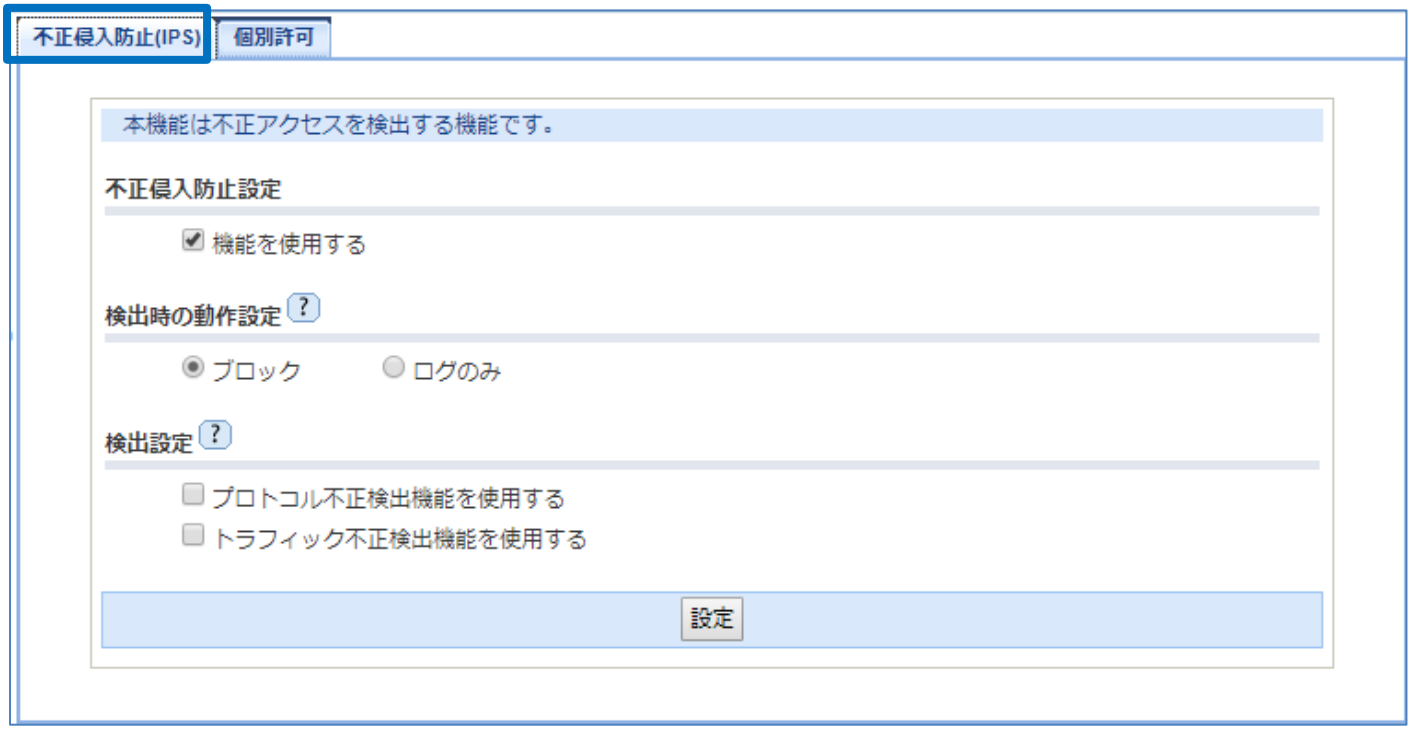
※本設定を行う場合は、セキュリティログ画面から設定してください。セキュリティログ画面の詳細は 6.1.11 章を参照してください。

設定項目	説明	初期値
アンチウイルス設定	アンチウイルス機能の使用有無の設定を行います。	
機能を使用する	ウイルスや危険なコードが含まれるプログラムを検出した場合にプログラムを書き換え無害化する機能を使用する場合は、本項目をチェックします。	有効
拡張スキャン設定	アンチウイルスの拡張スキャンを行う場合にチェックを入れます。	無効
検出時の動作設定	ウイルスを検出したときの動作を設定します。	
ブロック	ウイルスと検出したファイルを破壊し、ログ出力を行います。	ブロック
ログのみ	セキュリティリスクを検出したことを示すログ出力を行い、ウイルスと検出したファイルは破壊しません。	
圧縮ファイルのスキャン設定	圧縮ファイルをスキャンする場合、本製品内で一度解凍してからスキャンします。このため、本処理中は一時的に処理速度が低下します。 ● 次の圧縮ファイルに対応しています。 gz, zip, rar, jar, apk ● パスワードを設定した ZIP ファイルなどはスキャンできません。	
圧縮ファイルスキャン機能を使用する	圧縮ファイルをスキャンする場合は、本項目をチェックします。	有効
高圧縮率の圧縮ファイルをスキャンしない	圧縮率 200%以上の圧縮ファイルをスキャンしない場合は、本項目をチェックします。	有効
スキャンサイズ設定	スキャンサイズを設定します。	
スキャンサイズ設定を使用する	本機能を使用する場合は、本項目をチェックします。 チェックしない場合、ファイル全体をスキャンします。	有効
スキャン対象サイズ	スキャン範囲を指定します。1M バイト単位で、1M~100M バイトを指定できます。スキャン対象サイズを初期値よりも大きくすると処理速度が低下する可能性があります。 圧縮ファイルは圧縮した状態のファイルサイズを指定してください。	2M バイト
プロトコルのスキャン設定	アンチウイルス機能でスキャンするプロトコルを選択します。 ● アンチウイルス機能でスキャンできるプロトコルは、HTTP、FTP、SMTP、POP3、IMAP4 です。 ● 暗号化されたトラフィックはスキャンしません。例）SSL/TLS	すべて有効

設定項目	説明	初期値
個別許可リスト	アンチウイルス（AV）機能の検出対象外に設定されたウイルスタイプを表示します。設定はセキュリティログ画面から行ってください。 個別許可を実施する場合、該当する通信は危険な通信であっても許可されます。	
ウイルス	お客様により検出対象外に設定されたウイルスタイプを表示します。 登録可能件数　　：10 件	未設定
編集	検出対象外から削除する場合は「削除」ボタンを押下してください。	－

5.8.5. **不正侵入防止（IPS）**

不正侵入防止機能を運用ポリシーにしたがい、適切な内容に設定してください。



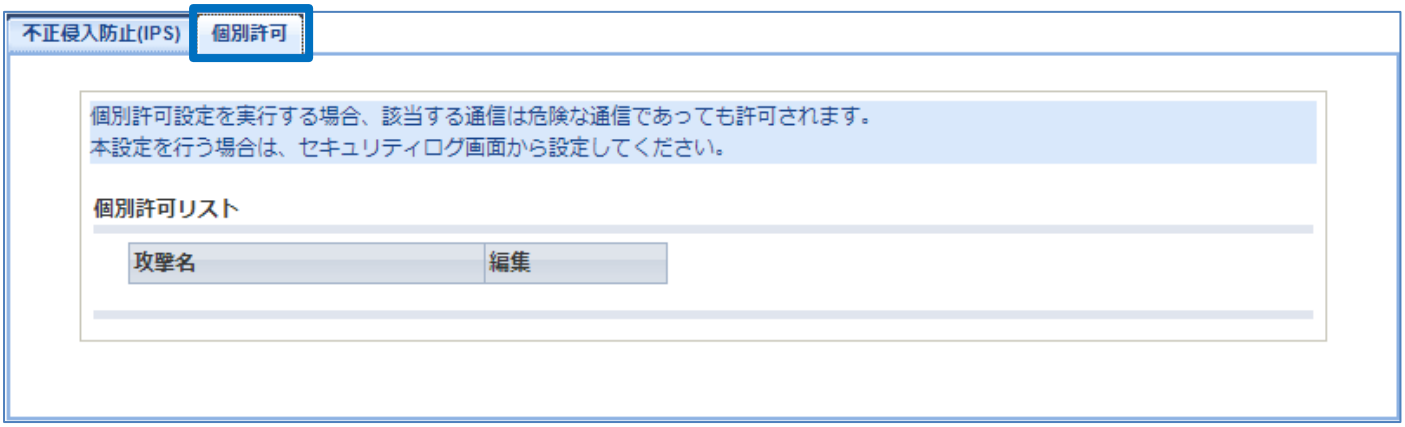
1. [TOP]-[セキュリティ]-[不正侵入防止（IPS）]画面を開きます。
2. 不正侵入防止機能をセキュリティポリシーにしたがって設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、設定値を保存します。

設定項目	説明	初期値
不正侵入防止設定	あらかじめ登録された侵入手口のパターンとマッチングさせることにより検出し、通信を防止することで、ファイアウォールでは検知できないネットワークに対する攻撃を認識、防止する機能を使用する場合は、本項目をチェックします。	有効
検出時の動作設定	不正アクセスを検出したときの動作を設定します。	
ブロック	不正アクセスをブロックし、ログ出力を行います。	ブロック
ログのみ	セキュリティリスクを検出したことを示すログ出力を行い、不正アクセスはブロックしません。	
検出設定	不正侵入防止の拡張機能を使用する場合は、本項目を設定します。 次のパケットを検出した場合に当該パケットを遮断するかどうかを設定します。	
プロトコル不正検出機能を使用する	RFC で規定されているプロトコルの仕様と比較して不正かどうかを検知します。不正を検出した場合、当該トラフィックの検出を示すログメッセージを出力する場合は、本項目をチェックします。[21] 動作設定を「ログのみ」で使用する場合は、本項目のチェックを外してください。	無効
トラフィック不正検出機能を使用する	本製品へのポートスキャンやフラッド攻撃など、通信の内容が不正かどうかを検知します。不正を検出した場合、当該トラフィックの検出を示すログメッセージを出力し当該パケットを遮断する場合は、本項目をチェックします。 動作設定を「ログのみ」で使用する場合は、本項目のチェックを外してください。	無効

[21] 正常なトラフィックを不正なトラフィックと検出する可能性があるため、トラフィックを遮断しません。

	本機能は、以下に示す攻撃のパターンを検出します。 ● TCP RST Scan 特定の送信元 IP/宛先 IP ペアの複数のポート間で、TCP 3-way handshake を短い時間に大量に行う攻撃。TCP 3-way handshake が TCP RST フラグにより不完全となる通信である場合に検出します。 ● TCP flood Scan 特定の送信元 IP/宛先 IP ペアの複数のポート間で、TCP half-open 通信を短い時間に大量に作成する攻撃。攻撃パケットに宛先ホストが応答する、しないに関わらず、攻撃として検出します。 ● UDP Scan 特定の送信元 IP/宛先 IP ペアで複数のポート間で UDP パケットの送信を短い時間に大量に行う攻撃。攻撃パケットに宛先ホストが ICMP port unreachable を応答し、サービスを運用しているポートの情報が攻撃者に知られる恐れがある場合に検出します。	

■個別許可タブ



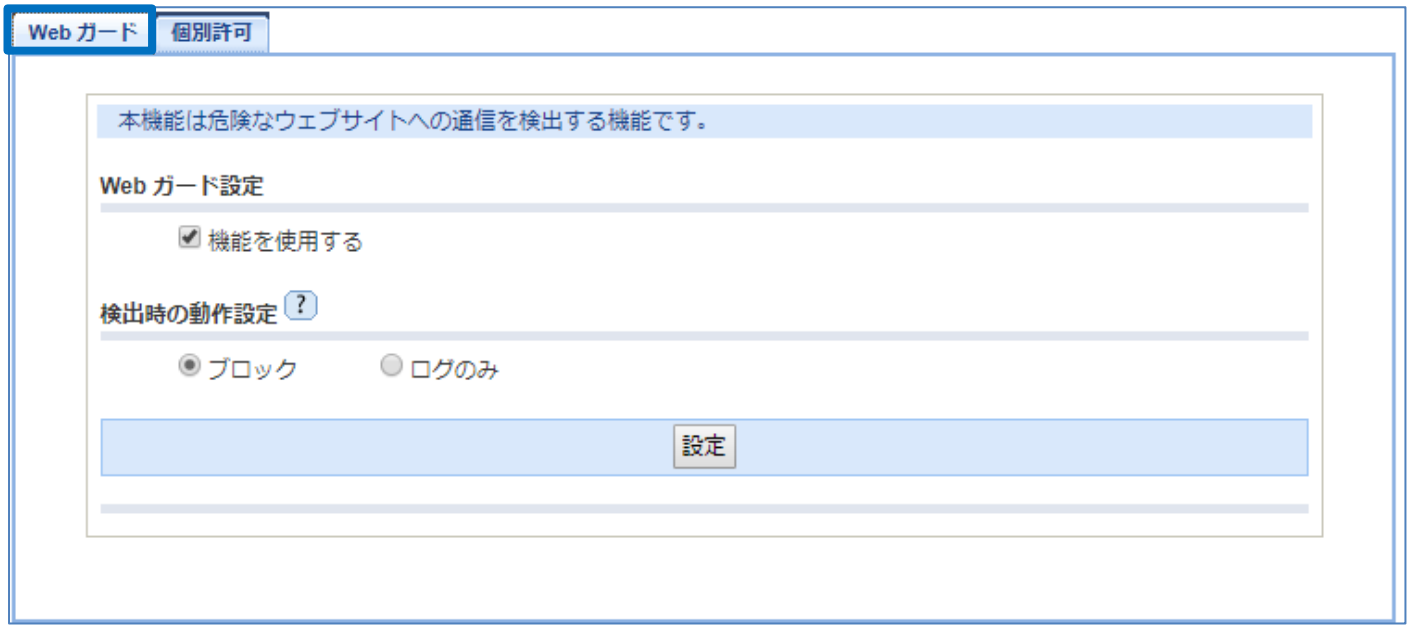
※画面は初期画面です。初期状態ではリストは設定されていません。追加した個別許可設定をリストから削除する場合は、削除したい攻撃名を選択した後に「削除」ボタンを押下してください。

設定項目	説明	初期値
個別許可リスト	不正侵入防止（IPS）機能の検出対象外に設定された攻撃名(シグネチャ)を表示します。設定はセキュリティログ画面から行ってください。 個別許可を実施する場合、該当する通信は危険な通信であっても許可されます。	
攻撃名	お客様により検出対象外に設定されたシグネチャを表示します。 登録可能件数　　：100 件	未設定
編集	検出対象外から削除する場合は「削除」ボタンを押下してください。	–

5.8.6. **Web ガード（WG）**

Web ガード機能を運用ポリシーにしたがい、適切な内容に設定してください。

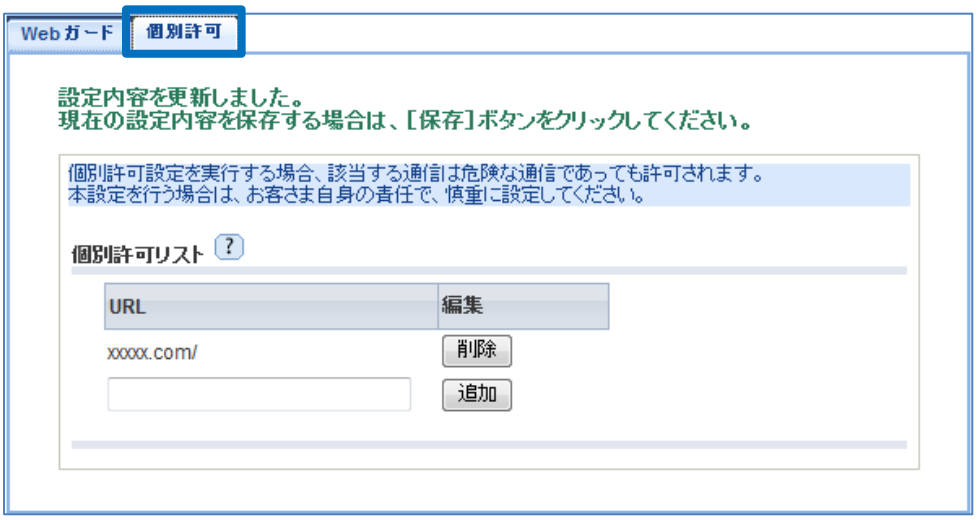
■Web ガードタブ



1. [TOP]-[セキュリティ]-[Web ガード（WG）]画面を開きます。
2. Web ガード機能をセキュリティポリシーにしたがって設定します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、設定値を保存します。

設定項目		説明	初期値
Web ガード設定		フィッシングサイトなどの危険な Web サイトへのトラフィックを検出した場合にそのトラフィックを遮断する機能を使用する場合は、本項目をチェックします。	有効
検出時の動作設定		危険なウェブサイトへの通信を検出したときの動作を設定します。	
	ブロック	危険なウェブサイトへの通信をブロックし、ログ出力を行います。	ブロック
	ログのみ	セキュリティリスクを検出したことを示すログ出力のみを行い、危険なウェブサイトへの通信はブロックしません。	

■個別許可タブ



※画面は”xxxxx.com/”を登録した表示例です。初期状態ではリストは設定されていません。

1. 個別許可したい URL を入力し、「追加」ボタンを押下します。
2. リストから削除する場合は、「削除」ボタンを押下します。

[メモ]

ホスト名は完全一致で、パス名は前方一致で判定します。

HTTPS の場合は、ホスト名のみで判定します。

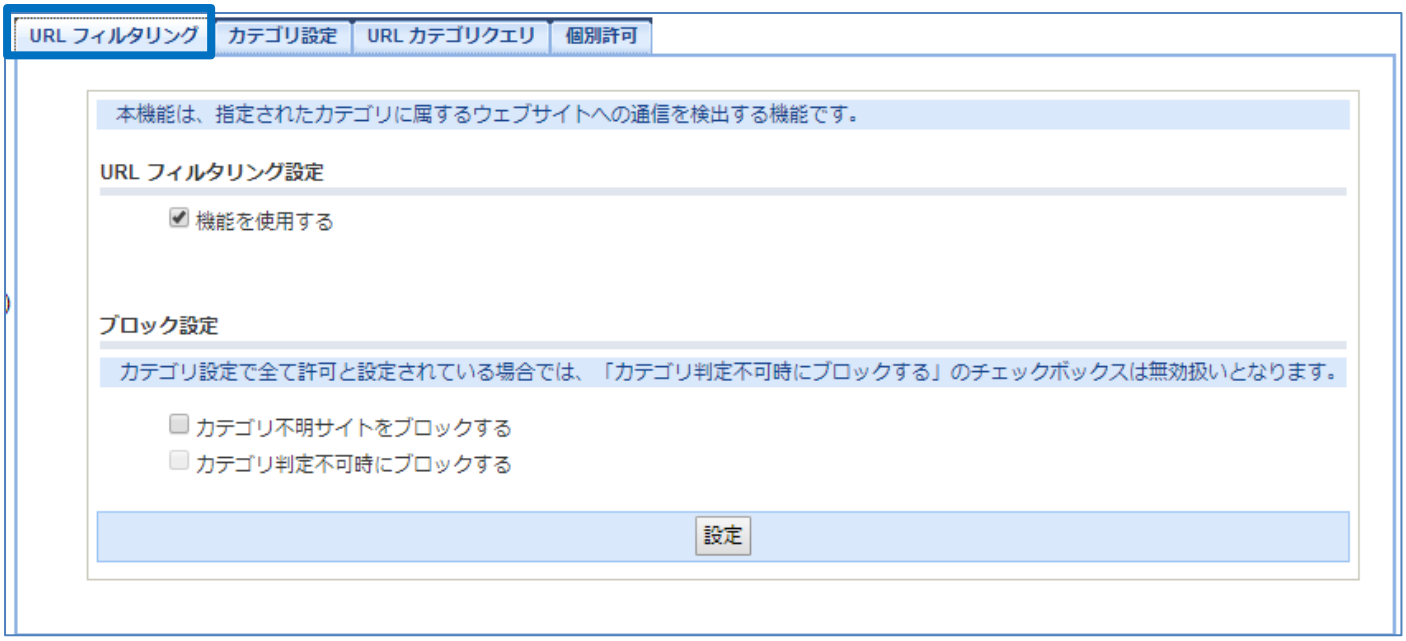
設定項目	説明	初期値
個別許可リスト	Web ガード（WG）機能の検出対象外に設定された URL を表示します。設定はセキュリティログ画面または本ページ内から行ってください。 個別許可を実施する場合、該当する通信は危険な通信であっても許可されます。	
URL	お客様により検出対象外に設定された URL を表示します。 URL にはホスト名とパス名を入力します。パス名は省略可能です。 URL には「http://」または「https://」は含めません。 ホスト名は完全一致で、パス名は前方一致で判定します。 HTTPS の場合は、ホスト名のみで判定します。 使用可能文字　：アスキーコードで 0x21-0x7e マルチバイト文字（ただし、"'`$¥<> を除く） URL の最大サイズ　：255 文字（255 バイト） [内訳] ホスト名部分で 127 文字（127 バイト） パス名部分で 127 文字（127 バイト） ホスト名とパス名の間の「/」で 1 文字（1 バイト） 登録可能件数　：10 件 ※マルチバイト文字を使用した場合、設定可能な文字数は少なくなります。	未設定
編集	検出対象に登録する場合は URL を入力して「追加」ボタンを押下してください。 検出対象外から削除する場合は「削除」ボタンを押下してください。	–

5.8.7. **URL フィルタリング（UF）**

URL フィルタリング機能を運用ポリシーにしたがい、適切な内容に設定してください。

タブ	説明
URL フィルタリングタブ	URL フィルタリング機能の使用有無を設定します。
カテゴリ設定タブ	各カテゴリ宛てのトラフィック動作を設定します。
URL カテゴリタブ	URL フィルタリング機能のカテゴリを設定します。
個別許可タブ	URL フィルタリング機能の個別許可を設定します。

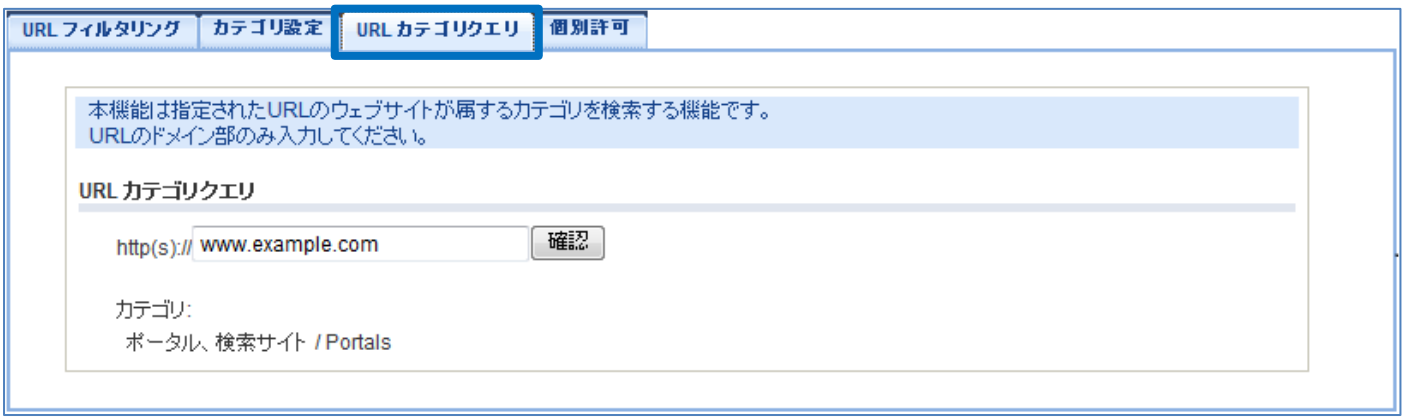
■URL フィルタリングタブ



■カテゴリ設定タブ

1. [TOP]-[セキュリティ]-[URL フィルタリング（UF）]画面を開きます。
2. [URL フィルタリング]タブをクリックし、[機能を使用する]をチェックし、「設定」ボタンを押下します。
3. [カテゴリ設定]タブをクリックし、次ページ以降の設定項目説明を参照の上で、URL フィルタリング機能をセキュリティポリシーにしたがって設定します。
   なお、設定可能なカテゴリの詳細は 3.3.10 章を参照してください。
4. [カテゴリ設定]タブの最下行の「設定」ボタンを押下します。
   ※「設定」ボタンを押し忘れると設定が有効になりませんので、ご注意ください。
5. 「保存」ボタンを押下して、設定値を保存します。

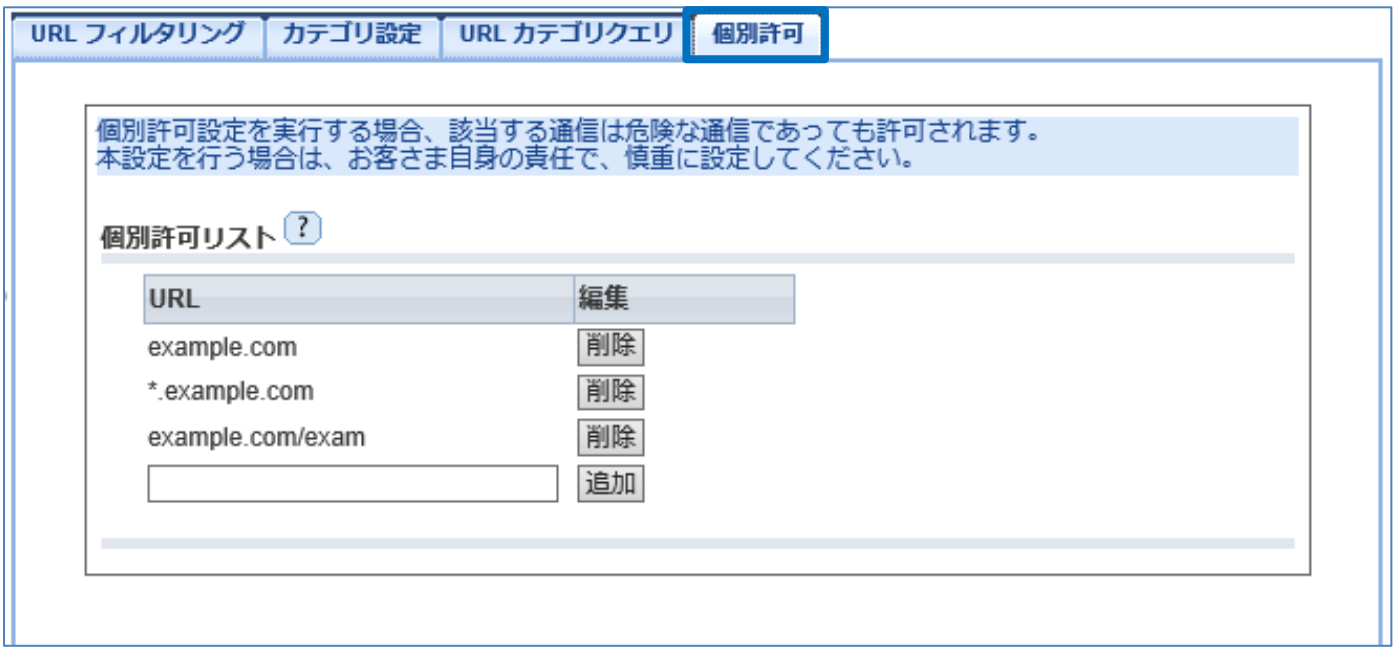
■URL カテゴリクエリタブ



※画面は”www.example.com”を確認した表示例です。初期状態では URL は入力されていません。

1. カテゴリを確認したい URL を入力し、「確認」ボタンを押下します。

■個別許可タブ



※画面は”example.com, *.example, example.com/exam”を登録した表示例です。初期状態ではリストは設定されていません。

1. 個別許可したい URL を入力し、「追加」ボタンを押下します。
2. リストから削除する場合は、「削除」ボタンを押下します。

[メモ]

個別許可リストは以下の２通りの書式で入力できます。

書式：*.<ドメイン名>

例：*.example.com

「*」(アスタリスク)を使用するとサブドメインをワイルドカードとして判定します。

書式：<ドメイン名>/<パス>

例：example.com/exam

ドメインは完全一致・パス名は前方一致で判定します。

設定項目	説明	初期値
URL フィルタリング設定	該当するカテゴリの Web サイトへのトラフィックを検出し、設定したカテゴリの動作にしたがい、トラフィックを通過/遮断する機能を使用する場合は、本項目をチェックします。 初期値はすべてのカテゴリが「許可」(通過) に設定されています。「スタンダード設定」、または「ブロックカテゴリ設定」で遮断するカテゴリを「ブロック」に設定してください。	有効
ブロック設定	カテゴリが不明または確認できない場合の動作を設定します。	
カテゴリ不明サイトをブロックする	カテゴリが不明の場合にブロックする場合は、本項目をチェックします。 本製品が利用するデータベースサーバに登録されていないサイトをブロックするという機能です。サイトの一例として公開されたばかりのサイトが該当します。	無効
カテゴリ判定不可時にブロックする	カテゴリが確認できない場合にブロックする場合は、本項目をチェックします。 本製品が利用するデータベースサーバとの通信に失敗した場合にブロックする機能です。	無効

設定項目	説明	初期値
スタンダード設定	複数のカテゴリを同時に設定する場合に使用します。	
全てのカテゴリ	すべてのカテゴリを一斉に設定できます。ブロック、ログのみ、許可のボタンをクリックして設定します。 ● ブロック・・・指定されたカテゴリに属するウェブサイトへの通信をブロックし、ログ出力を行います。 ● ログのみ・・・ログ出力のみを行い、指定されたカテゴリに属するウェブサイトへの通信はブロックしません。 ● 許可・・・・・すべてのカテゴリへの通信を許可します。	許可
アダルトサイトカテゴリ	下記のカテゴリが該当します。 ポルノ / Pornography アダルトサイト / Nudity and Potentially Adult Content ギャンブル、宝くじ / Gambling and Lottery アルコール、たばこ / Alcohol and Tobacco ドラッグ / Abused Drug 過激論、人種差別 / Ultraism 中絶 / Abortion 犯罪行為 / Criminal Actions 暴力的なサイト / Violent and Bloody 気持ち悪いサイト / Gross 出会い系サイト / Dating ブロック、ログのみ、許可のボタンをクリックして設定します。 ● ブロック・・・指定されたカテゴリに属するウェブサイトへの通信をブロックし、ログ出力を行います。 ● ログのみ・・・ログ出力のみを行い、指定されたカテゴリに属するウェブサイトへの通信はブロックしません。 ● 許可・・・・・アダルトサイトカテゴリへの通信を許可します。	許可

危険サイトカテゴリ	下記のカテゴリが該当します。 フィッシング詐欺 / Phishing and Fraud マルウェア / Malware BlackHat SEO サイト / BlackHat SEO Sites 危険アプリケーション / Malicious APPs ブロック、ログのみ、許可のボタンをクリックして設定します。 ● ブロック・・・指定されたカテゴリに属するウェブサイトへの通信をブロックし、ログ出力を行います。 ● ログのみ・・・セキュリティリスクを検出したことを示すログ出力のみを行い、指定されたカテゴリに属するウェブサイトへの通信はブロックしません。 ● 許可・・・・・危険サイトカテゴリへの通信を許可します。	許可
SNS サイトカテゴリ	下記のカテゴリが該当します。 インスタントメッセージ / Instant Messaging ソーシャルネットワーク / Social Network Web チャットルーム / Web Chat Room フォーラム、ニュースグループ / Forums and Newsgroups ブログと個人サイト / Blog and Personal Web ブロック、ログのみ、許可のボタンをクリックして設定します。 ● ブロック・・・指定されたカテゴリに属するウェブサイトへの通信をブロックし、ログ出力を行います。 ● ログのみ・・・セキュリティリスクを検出したことを示すログ出力のみを行い、指定されたカテゴリに属するウェブサイトへの通信はブロックしません。 ● 許可・・・・・SNS サイトカテゴリへの通信を許可します。	許可
エンターテインメントサイトカテゴリ	下記のカテゴリが該当します。 ゲーム / Game ショッピング、オークション / Shopping and Auction ミュージック / Music コミック、アニメ / Comics and Anime エンターテインメント、芸術 / Entertainment and Arts ストリーミング、VoIP / Streaming and VoIP ブロック、ログのみ、許可のボタンをクリックして設定します。 ● ブロック・・・指定されたカテゴリに属するウェブサイトへの通信をブロックし、ログ出力を行います。 ● ログのみ・・・セキュリティリスクを検出したことを示すログ出力のみを行い、指定されたカテゴリに属するウェブサイトへの通信はブロックしません。 ● 許可・・・・・エンターテインメントサイトカテゴリへの通信を許可します。	許可
ブロックカテゴリ設定	カテゴリごとに通過/遮断を選択する場合に使用します。	
個別カテゴリ	通過させるカテゴリは「許可」に、遮断するカテゴリは「ブロック」に設定します。 設定可能なカテゴリの詳細は、3.3.10 章を参照してください。	すべて許可

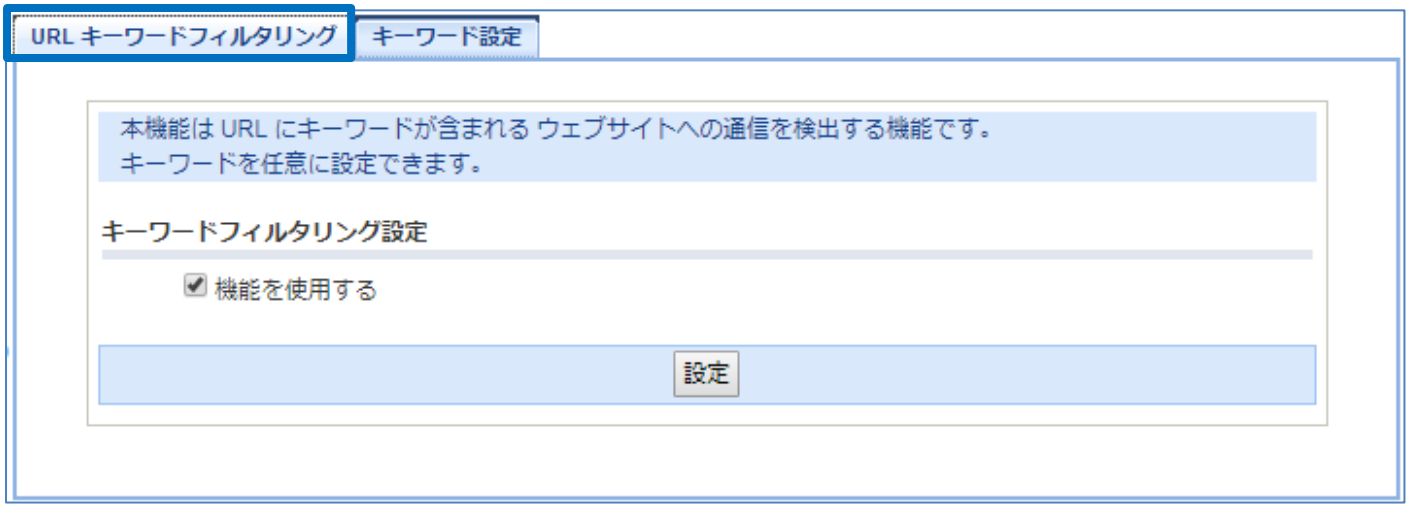
設定項目	説明	初期値
個別許可リスト	URL フィルタリング（UF）機能の検出対象外に設定された URL を表示します。設定はセキュリティログ画面または本ページ内から行ってください。 個別許可を実施する場合、対象の URL がブロック対象のカテゴリであっても許可されます。	
URL	お客様により検出対象外に設定された URL を表示します。 URL にはホスト名とパス名を入力します。パス名は省略可能です。 URL には「http://」または「https://」は含めません。 ホスト名の先頭文字に「*」(アスタリスク)を設定した場合は、ワイルドカードとして判定します。このときパスは入力できません。 ホスト名の先頭文字に「*」を設定していない場合は完全一致で、パス名は前方一致で判定します。 HTTPS の場合は、ホスト名のみで判定します。 使用可能文字　：アスキーコードで 0x21-0x7e マルチバイト文字（ただし、"'`$¥<> を除く） URL の最大サイズ　：255 文字（255 バイト） [内訳] ホスト名部分で 127 文字（127 バイト） パス名部分で 127 文字（127 バイト） ホスト名とパス名の間の「/」で 1 文字（1 バイト） 登録可能件数　：100 件 ※マルチバイト文字を使用した場合、設定可能な文字数は少なくなります。	未登録
編集	検出対象に登録する場合は URL を入力して「追加」ボタンを押下してください。 検出対象外から削除する場合は「削除」ボタンを押下してください。	－

5.8.8. URL キーワードフィルタリング（KF）

URL キーワードフィルタリング機能を運用ポリシーにしたがい、適切な内容に設定してください。

タブ	説明
URL キーワードフィルタリングタブ	URL キーワードフィルタリング機能の使用有無を設定します。
キーワード設定タブ	URL キーワードフィルタリング機能の「キーワード」と「動作」を設定します。

■URL キーワードフィルタリング



■キーワード設定

※画面は”example_.com”を登録した表示例です。初期状態ではキーワードは設定されていません。

1. [TOP]-[セキュリティ]-[URL キーワードフィルタリング（KF）]画面を開きます。
2. [URL キーワードフィルタリング]タブをクリックし、[機能を使用する]をチェックし、「設定」ボタンを押下します。
3. [キーワード設定]タブをクリックし、次ページの設定項目説明を参照の上で、URL キーワードフィルタリング機能をセキュリティポリシーにしたがって設定します。なお、キーワード設定の詳細は 3.3.11 章を参照してください。
4. 「保存」ボタンを押下して、設定値を保存します。

設定項目	説明	初期値
URL キーワードフィルタリング設定	任意のキーワードを含む Web サイトへのトラフィックを検出し、遮断する機能を使用する場合は、本項目をチェックします。 初期値ではキーワードは設定されていません。遮断するキーワードを設定してください。 HTTP　：キーワードとして、URL 部の「ホスト名」と「パス名」にキーワードが含まれているか確認します。 HTTPS　：キーワードとして、URL 部の「ホスト名」にキーワードが含まれているか確認します。	有効

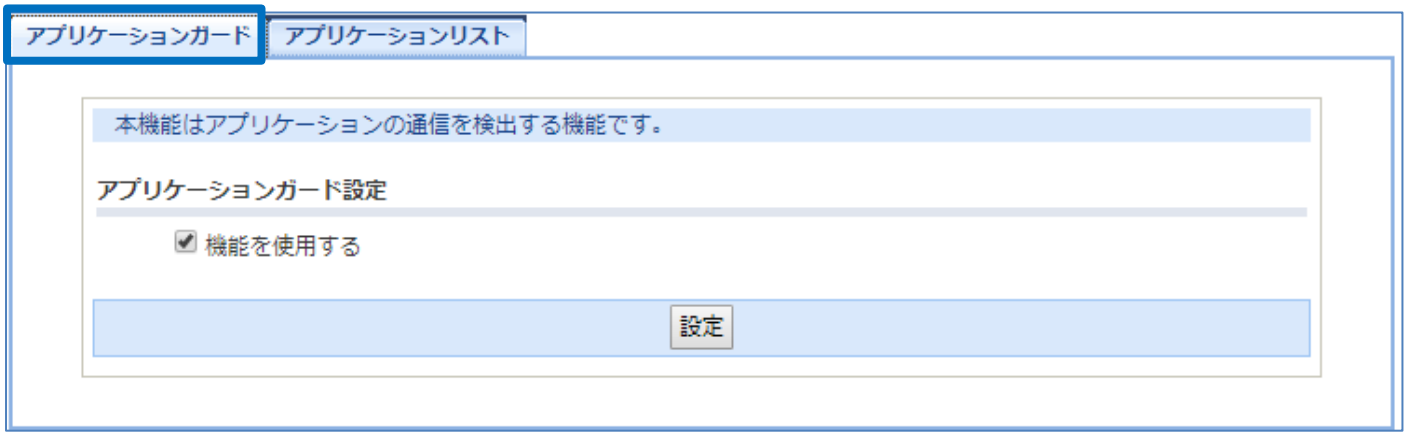
設定項目		説明	初期値
キーワードリスト		任意の「キーワード」の追加、削除を設定します。	
	キーワード	キーワード設定の詳細は 3.3.11 章を参照してください。 使用可能文字　　：アスキーコードで 0x21-0x7e 　　マルチバイト文字（ただし、"'`$¥<> を除く） キーワードの最大サイズ　：127 文字（127 バイト） キーワードの登録可能数　：100 件 ※マルチバイト文字を使用した場合、設定可能な文字数は少なくなります。	未設定
	動作	ブロック：URL にキーワードが含まれるウェブサイトへの通信をブロックし、ログ出力を行います。 ログのみ：セキュリティリスクを検出したことを示すログ出力のみを行い、URL にキーワードが含まれるウェブサイトへの通信はブロックしません。 許可　：URL にキーワードが含まれるウェブサイトへの通信を許可します。検出時のログ出力を行いません。 アプリケーションガード(APG)のブロック時の URL を登録すると、APG において過検知でブロックされた通信などを許可することができます。	–
	編集	キーワード追加の場合は「追加」ボタンを押下します。 設定済みキーワードの削除の場合は「削除」ボタンを押下します。	–

5.8.9. アプリケーションガード（APG）

アプリケーションガード機能を運用ポリシーにしたがい、適切な内容に設定してください。

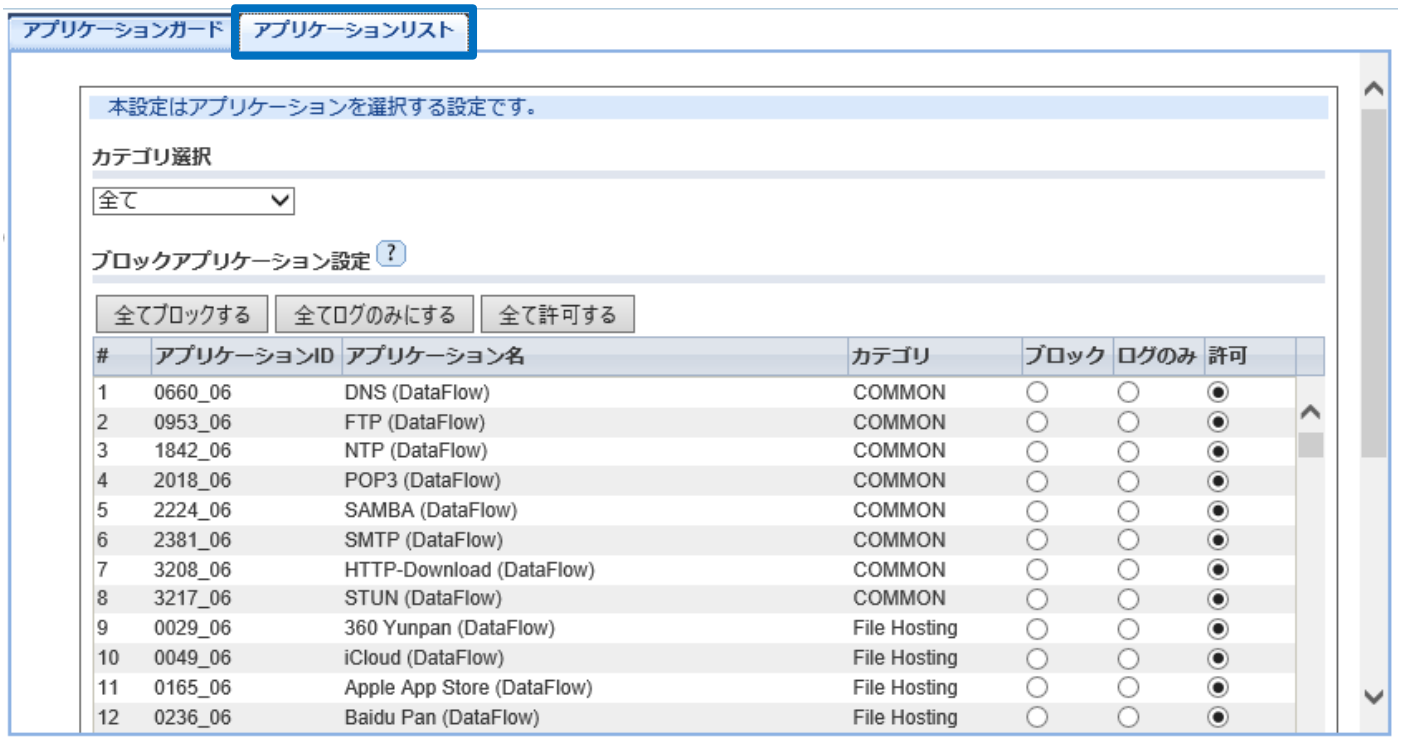
タブ	説明
アプリケーションガード	アプリケーションガード機能の使用有無を設定します。
アプリケーションリスト	ブロックするアプリケーション、プロトコルを選択します。 シグネチャ更新により追加されるアプリケーションの動作を設定します。

■アプリケーションガード



■アプリケーションリスト

①ブロックアプリケーションの設定



1. [TOP]-[セキュリティ]-[アプリケーションガード（APG）]画面を開きます。
2. [アプリケーションガード]タブをクリックし、[機能を使用する]をチェックし、「設定」ボタンを押下します。
3. [アプリケーションリスト]タブをクリックし、次ページの設定項目説明を参照の上で、アプリケーションガード機能をセキュリティポリシーにしたがって設定します。
   アプリケーションガード機能の詳細は 3.3.12 章を参照してください。

4. [アプリケーションリスト]タブの最下行の「設定」ボタンを押下します。
   ※「設定」ボタンを押し忘れると設定が有効になりませんので、ご注意ください。
5. 「保存」ボタンを押下して、設定値を保存します。

② シグネチャ更新により追加されるアプリケーションの設定

1. [TOP]-[セキュリティ]-[アプリケーションガード（APG）]画面を開きます。
2. [アプリケーションガード]タブをクリックし、[機能を使用する]をチェックし、「設定」ボタンを押下します。
3. [アプリケーションリスト]タブをクリックし、[カテゴリ選択]リストから「全て」以外の「カテゴリ」を選択しすると、[シグネチャ更新により追加されるアプリケーションの設定]欄が表示されます。
   ※画面は「Game」カテゴリを選択した表示例です。
4. 次ページの設定項目説明を参照の上で、セキュリティポリシーにしたがって「ブロック」または「ログのみ」に変更します。
5. [アプリケーションリスト]タブの最下行の「設定」ボタンを押下します。
   ※「設定」ボタンを押し忘れると設定が有効になりませんので、ご注意ください。
6. 「保存」ボタンを押下して、設定値を保存します。

設定項目	説明	初期値
アプリケーションガード設定	アプリケーション、プロトコルを監視し、対象のトラフィックを遮断する機能を使用する場合は、本項目をチェックします。 初期値はすべてのアプリケーション、プロトコルが「許可」（通過）に設定されています。「ブロックアプリケーション設定」で遮断するアプリケーション、プロトコルを「ブロック」に設定してください。	有効

項目	説明	初期値
カテゴリ選択	以下のリストから選択します。 全て COMMON File Hosting File Transfer Game IM Mail OTHER P2P Remote Controller Shopping Social web Site Streaming Tunnel Update VoIP Web Services	全て
シグネチャ更新により追加されるアプリケーションの設定	シグネチャ更新により追加されるアプリケーションの検出時の動作をカテゴリ毎に「ブロック」・「ログのみ」・「許可」に設定してください。 (ファームウェア Ver 3.6.9 以降) ブロック：アプリケーション、プロトコルの通信をブロックし、ログ出力を行います。 ログのみ：アプリケーション、プロトコルの通信を検出したことを示すログ出力のみを行いアプリケーション、プロトコルの通信はブロックしません。 許可　　：アプリケーション、プロトコルの通信を許可します。検出時のログ出力を行いません。 アプリケーションガード(APG)のブロック時のURLを登録すると、APG において過検知でブロックされた通信などを許可することができます。	許可

ブロックアプリケーション設定	遮断するアプリケーション、プロトコルの選択を行います。 遮断するアプリケーション、プロトコルの設定を「ブロック」に設定してください。 「全てブロックする」ボタンを押下するとアプリケーションリストに表示されたすべてのアプリケーション、プロトコルを「ブロック」します。 「全てブログのみにする」ボタンを押下するとアプリケーションリストに表示されたすべてのアプリケーション、プロトコルを検出したときにログに記録します。 「全て許可する」ボタンを押下すると、すべてのアプリケーション、プロトコルを「許可」します。	すべて許可
#	項目番号です。 ※シグネチャの更新で、アプリケーションの順序が変わります。	＊1
アプリケーション ID	サーバで管理している ID です。	＊1
アプリケーション名	アプリケーション名、プロトコル名です。	＊1
カテゴリ	アプリケーションやプロトコルをカテゴリ分けしています。 COMMON：一般的なプロトコル File Hosting：オンラインストレージ File Transfer：ファイルのダウンロード支援サービス Game：ゲーム IM：インスタントメッセージング Mail：メールサービス OTHER：その他 P2P：P2P アプリケーション Remote Controller：リモートアクセスのためのアプリケーション Shopping：オークションサイト Social web Site：SNS（Social Networking Service） Streming：ストリーミング Tunnel：VPN（Virtual Private Network） VoIP：Voice over IP Web Service：Web サービス Update：アップデート	＊1

＊1：対応アプリケーション、プロトコル、カテゴリ選択のリストは定期的に更新します。

5.8.10. **メール通知**

メール通知機能を運用ポリシーにしたがい、適切な内容に設定してください。

タブ	説明
メール通知	メール通知機能の使用有無、メールの言語、メール送信に使用するメールアカウントを設定します。
通知先	メール通知の宛先メールアドレスを設定します。
通知条件	メールを通知する条件を設定します。
テストメール	テストメールを送信します。

■メール通知タブ

1. [TOP]-[セキュリティ]-[メール通知]画面を開きます。
2. [メール通知]タブをクリックし、[機能を使用する]をチェックします。
3. 言語設定、メール送信に使用するメールアカウントを設定します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、設定値を保存します。

[メモ]

ここで設定する「SMTP サーバアドレス」や「ポート番号」、「SMTP 認証」、「TLS」については、お使いのメール設定環境に合わせて設定してください。もし、設定値が分らない場合は、社内の管理部門もしくはインターネットサービスプロバイダにお問い合わせください。

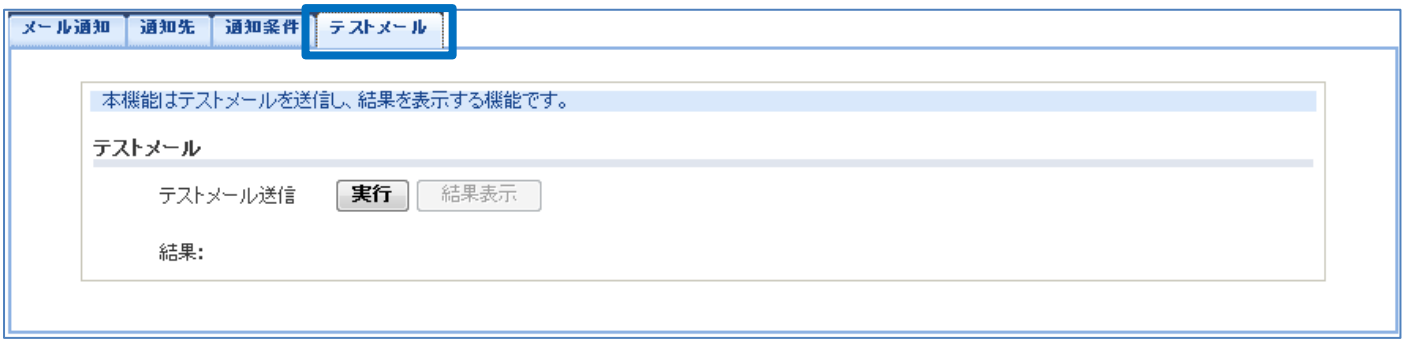
■通知先タブ

1. [TOP]-[セキュリティ]-[メール通知]画面を開きます。
2. [通知先]タブをクリックし、管理者用のメールアドレスを設定します。
   ※端末使用者にもメール通知することができます。端末使用者のメールアドレス設定は 5.9.3 章を参考に
   デバイス管理から行ってください。
   ※管理者、端末使用者のメール通知条件は、3.3.14 章を参照してください。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、設定値を保存します。

■通知条件タブ

1. [TOP]-[セキュリティ]-[メール通知]画面を開きます。
2. [通知条件]タブをクリックし、管理者用の通知条件、端末使用者用の通知条件を設定します。
   ※管理者、端末使用者のメール通知条件は、3.3.14 章を参照してください。
3.「設定」ボタンを押下します。
4.「保存」ボタンを押下して、設定値を保存します。

■テストメールタブ



1. [TOP]-[セキュリティ]-[メール通知]画面を開きます。
2. [テストメール]タブをクリックし、「実行」ボタンを押下します。
3. 画面内の「結果」欄にテスト結果が表示されます。
   ※テストメール送信が失敗した場合は、[通知先]タブ、および[メール通知]の設定値を確認してください。

設定項目	説明	初期値
メール通知設定	脅威検出などのイベント発生時にメールでお知らせする機能を使用する場合は、本項目をチェックします。	無効
言語設定	メールに記載する言語を設定します。	
メールの言語設定	メールの言語を変更する場合は、本設定を変更してください。	日本語
アカウント設定	本設定はメール通知に利用するアカウントを指定する設定です。 利用可能なメールアドレスのアカウント情報を設定してください。	
メールアドレス	メールアドレスを設定します。	未設定
SMTP サーバアドレス	SMTP サーバアドレスを設定します。	未設定
ポート番号	SMTP 通信に利用するポート番号を設定します。	未設定
SMTP 認証を使用する	SMTP 認証を使用する場合は、本項目にチェックします。	有効
認証用ユーザー名	SMTP 認証を使用する場合は、認証用のユーザー名を設定します。	未設定
認証用パスワード	SMTP 認証を使用する場合は、認証用のパスワードを設定します。	未設定
TLS	TLS、STARTTLS を使用する場合は、本設定を変更してください。	使用しない

設定項目	説明	初期値
メールアドレス設定(管理者)	管理者の宛先情報を設定します。 [通知先]タブで設定するすべてのイベントを通知します。	
#	項目番号です。	
送信先メールアドレス	管理者のメールアドレスを設定します。	未設定

設定項目	説明	初期値
通知条件設定(共通)	管理者と端末使用者宛てにメール送信を行いたい条件を設定します。	
AV ブロック時に通知する	アンチウイルスで通信をガードしたときにメールを通知する場合は、本項目にチェックします。 ※インターネットから受信したメールの添付ファイルに、ウイルスや危険なコードが含まれるプログラム検知して無害化した場合は、通知するメールに受信したメールの表題とメールの日付を付与します。	有効
WG ブロック時に通知する	Web ガードで通信をガードしたときにメールを通知する場合は、本項目にチェックします。	有効
UF ブロック時に通知する	URL フィルタリングで通信をガードしたときにメールを通知する場合は、本項目にチェックします。	無効
KF ブロック時に通知する	URL キーワードフィルタリングで通信をガードしたときにメールを通知する場合は、本項目にチェックします。	無効
APG ブロック時に通知する	アプリケーションガードで通信をガードしたときにメールを通知する場合は、本項目にチェックします。	無効
通知条件設定(管理者用)	管理者宛てにメール送信を行いたい条件を設定します。	
IPS ブロック時に通知する	不正侵入防止で通信をガードしたときにメールを通知する場合は、本項目にチェックします。	無効

ファームウェア更新可能なときに通知する	更新可能なファームウェアを検出したときにメール通知する場合は、本項目にチェックします。	有効
ライセンス満了が近づいたときに通知する	ライセンス期限満了間近（60 日前）となったときにメール通知する場合は、本項目にチェックします。	有効
ライセンスが満了したときに通知する	ライセンス期限満了となったときにメール通知する場合は、本項目にチェックします。	有効
月次レポートを通知する	毎月 1 日に、月次レポートを通知する場合は、本項目にチェックします。	無効
月次レポートタイミング	月次レポートを通知するタイミングを指定します。 通知するには、毎月 1 日の指定した時間に、本製品の電源が入っている必要があります。	10:00

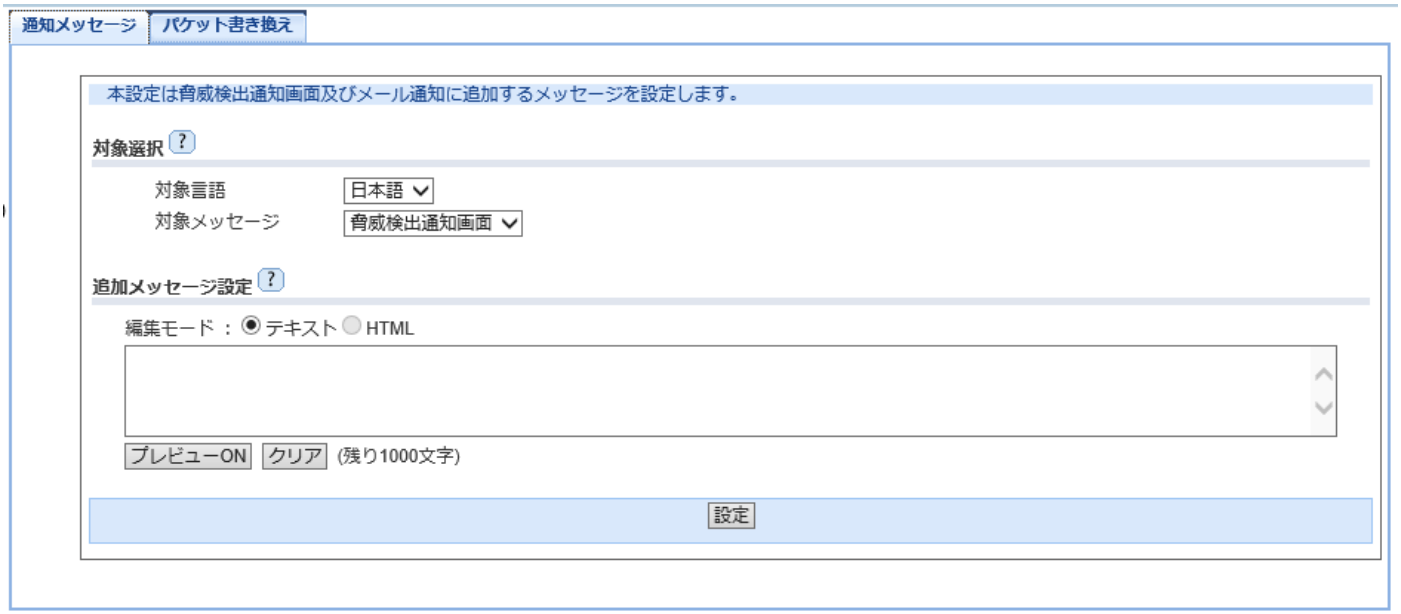
設定項目	説明	初期値
テストメール	管理者のメールアドレス宛てにメールを送信します。 テストメールを実行するには、事前にアカウント設定、メールアドレス設定(管理者)を行ってください。	
実行	「実行」ボタンを押下すると、管理者のメールアドレス宛てにメールを送信します。	–
結果表示	メール送信実行後に「結果表示」ボタンを押下すると、メール送信の結果を表示します。 ● 送信中：メール送信中です。しばらくしてから、再度「結果表示」ボタンを押下してください。 ● 送信完了：メールは正常に送信されました。管理者宛てにメールが届いたか確認してください。 ● 送信失敗：メールは正常に送信されませんでした。アカウント設定、メールアドレス設定(管理者)の内容を確認してください。	–

5.8.11. 高度な設定

脅威検出画面やメール通知に任意のメッセージを追加することができます。

5.8.11.1. 通知メッセージ

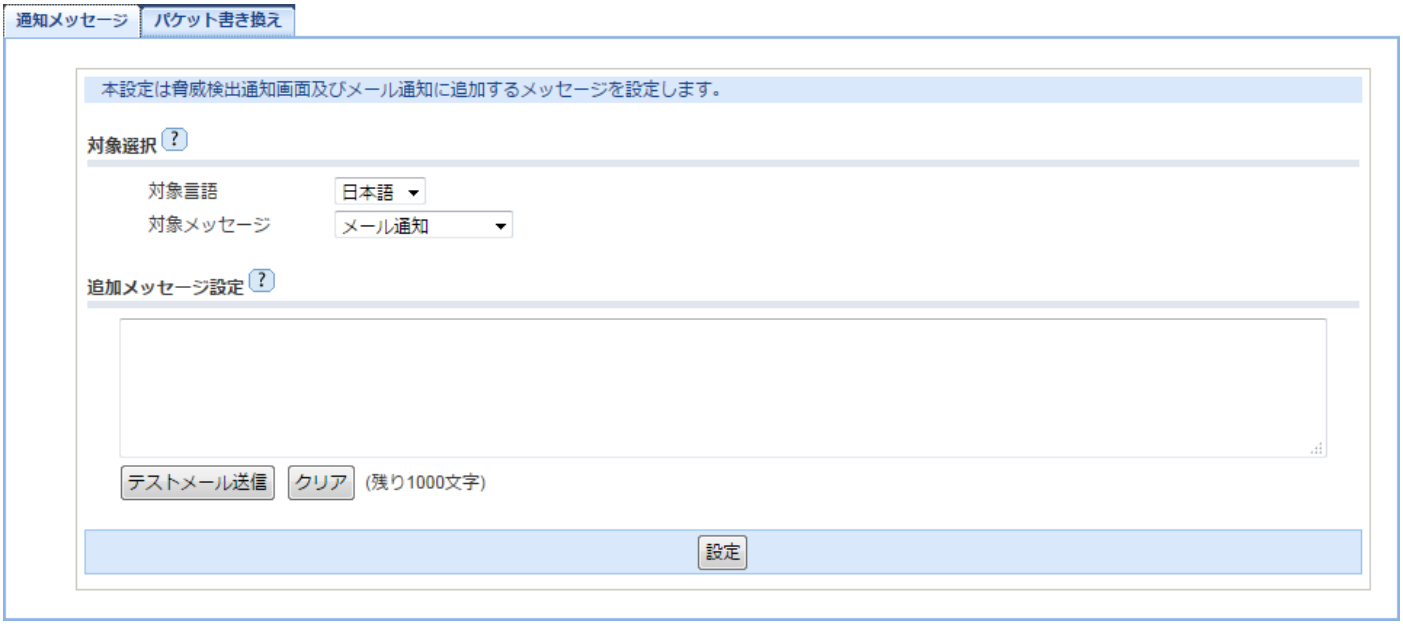
■脅威検出通知画面を選択の場合



1. [TOP]-[セキュリティ]-[高度な設定]画面を開きます。
2. 通知メッセージに設定する言語を変更する場合、[対象言語]を選択します。日本語か英語を選択できます。
3. [対象メッセージ]で「脅威検出通知画面」を選択します。
4. [追加メッセージ設定]に任意の追加メッセージを入力します。
5. 「プレビューON」ボタンをクリックして、通知イメージを確認します。
6. 「設定」ボタンを押下します。
7. 「保存」ボタンを押下して、本設定を保存します。

設定項目	説明	初期値
対象選択		
対象言語	言語を日本語もしくは英語を選択します。	日本語
対象メッセージ	編集を行う機能を脅威検出画面もしくはメール通知を選択します。	脅威検出画面
追加メッセージ設定		
編集モード	編集モードは「テキスト」形式のみ使用できます。 「HTML」形式はファームウェアバージョン 3.5.12 にて、使用不可に変更しました。3.5.12 への更新の前に「HTML」形式で設定していた場合には、ファームウェア更新の際にその設定は維持されます。	テキスト
追加メッセージ	任意の追加メッセージを入力します。 半角と全角文字を使って、1000 文字以内で入力してください。改行も 1 文字とみなします。HTML タグを使用できます。	未設定
プレビューON	編集したメッセージのプレビューを行う場合、クリックします。	
クリア	編集したメッセージをクリアする場合、クリックします。	

■通知メッセージ（メール通知を選択の場合）

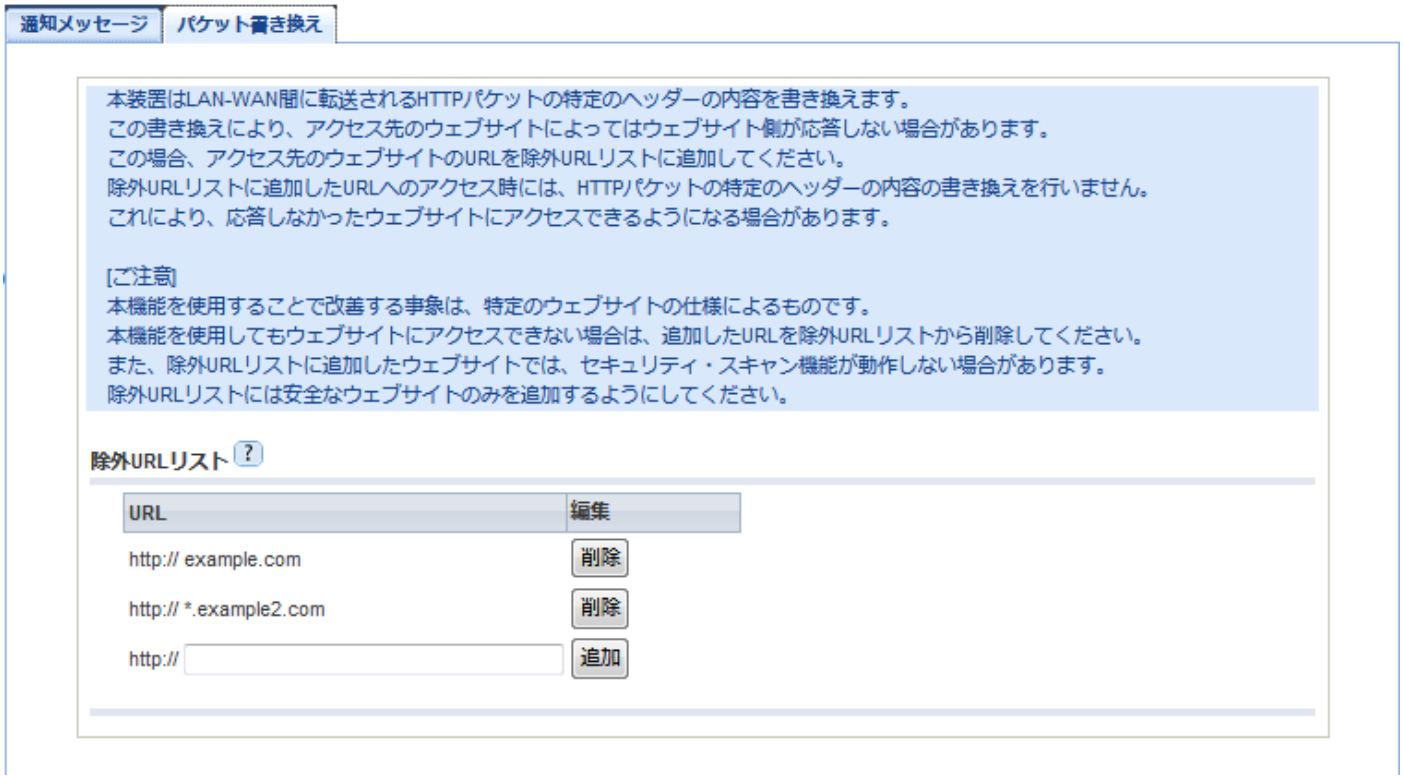


1. [TOP]-[セキュリティ]-[高度な設定]画面を開きます。
2. [対象言語]を選択します。
3. [対象メッセージ]で「メール通知」を選択します。
4. [追加メッセージ設定]に任意の追加メッセージを入力します。
5. 「テストメール送信」ボタンをクリックして、テストメールにて通知内容を確認します。
   メール送信に必要な情報の設定については、5.8.10 章を参照してください。
6. 「設定」ボタンを押下します。
7. 「保存」ボタンを押下して、本設定を保存します。

設定項目	説明	初期値
対象選択		
対象言語	言語を日本語もしくは英語を選択します。	日本語
対象メッセージ	編集を行う機能を脅威検出画面もしくはメール通知を選択します。	脅威検出画面
追加メッセージ設定		
追加メッセージ	任意の追加メッセージを入力します。 半角と全角文字を使って、1000 文字以内で入力してください。改行も 1 文字とみなします。HTML タグは使用できません。	未設定
テストメール送信	テストメールにて通知内容を確認する場合、クリックします。	
クリア	編集したメッセージをクリアする場合、クリックします。	

5.8.11.2. **パケット書き換え機能**

本製品がセキュリティ・スキャン機能使用時に行うパケット書き換え動作の対象から、指定した URL を除外することが出来ます。



設定項目	説明
除外 URL リスト	
URL	URL にはホスト名を入力します。 URL には「http://」または「https://」は含めません。 先頭文字（サブドメイン部分）に「*」を使用できます。 先頭文字（サブドメイン部分）に「*」を使用している場合は、URL のチェックはサブドメイン部分をワイルドカードとして判断します。 先頭文字（サブドメイン部分）に「*」を使用していない場合は、URL のチェックは完全一致で判断します。 パス部分の入力はできません。また、マルチバイト文字は使用できません。 使用可能文字　　：アスキーコードで 0x21-0x7e URL の最大サイズ　：127 文字（127 バイト） 登録可能件数　　：100 件
追加	入力した URL を除外 URL リストに登録する場合、クリックします。
削除	登録した URL を削除する場合、クリックします。

5.8.12. 簡易 RADIUS 機能

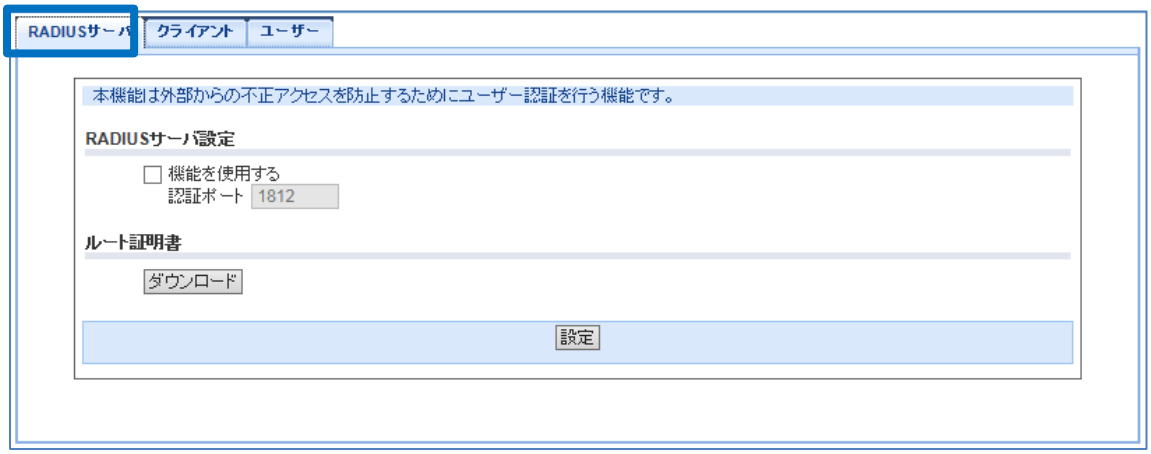
運用ポリシーにしたがい、適切な内容に設定してください。

5.8.12.1. 本製品を RADIUS サーバとして使用する場合

タブ	説明
RADIUS サーバ	簡易 RADIUS サーバ機能の設定とルート証明書のダウンロードを行います。
クライアント	認証を行う RADIUS クライアントの設定を行います。
ユーザー	認証を行う無線 LAN 端末のユーザー登録とクライアント証明書の発行を行います。

本製品はプライベート CA を搭載しています。このルート証明書はプライベートルート証明書になります。

■RADIUS サーバの設定



1. [TOP]-[セキュリティ]-[簡易 RADIUS 機能]画面を開きます。
2. [RADIUS サーバ]タブをクリックし、[機能を使用する]をチェックします。
3. 使用するポート番号を設定します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、設定値を保存します。
6. 本機能で使用するルート証明書を「ダウンロード」ボタンをクリックしてパソコンなどに一時保存した上で、認証を行うユーザー端末に登録してください。
   ※ユーザー端末へのルート証明書の登録方法は、ユーザー端末のマニュアルを参照してください。

設定項目	説明	初期値
RADIUS サーバ設定		
機能を使用する	RADIUS サーバ機能を使用する場合にチェックします。	無効
認証ポート	RADIUS 認証を行うポート番号を設定します。	未設定

[メモ]

ルート証明書は本製品が内部に保有しているサーバ証明書の正当性確認に利用します。Windows 端末ではサーバ認証のためにルート証明書の登録が必要です。他の OS では、ユーザー端末に登録しなくても認証可能な場合がありますが、ユーザー端末にセキュリティの警告が表示することがあります。

ルート証明書は「設定値の保存、復元」により保存、復元されます。(5.6.14 章参照)

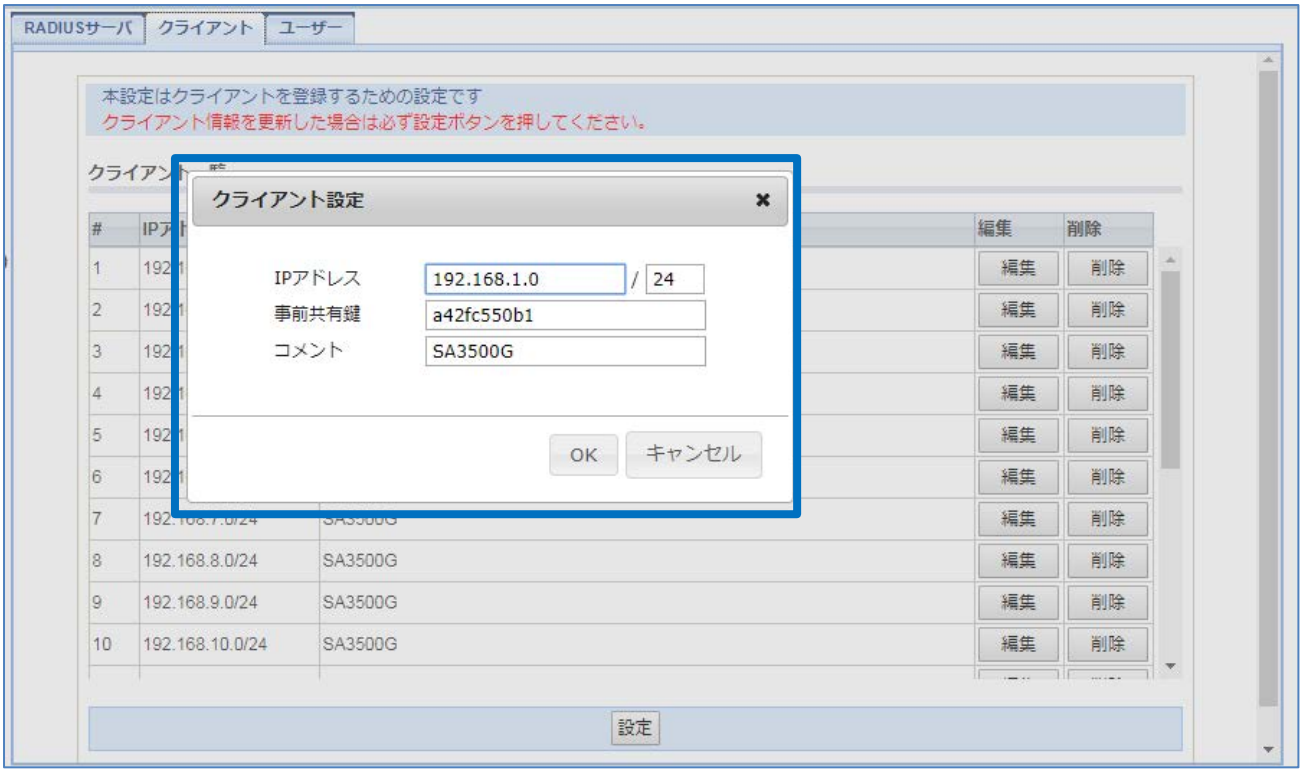
■外部の RADIUS クライアントの設定

※外部の RADIUS クライアントは最大 20 台登録できます。

1. [TOP]-[セキュリティ]-[簡易 RADIUS 機能]画面を開きます。
2. [クライアント]タブをクリックします。
3. [編集]をクリックして、クライアントとして登録する端末の IP アドレスとコメント、事前共有鍵を設定します。
4. 編集後に[OK]をクリックします。クライアント一覧がら消す場合は、[削除]をクリックします。
5. クライアントの設定が終わりましたら、「設定」ボタンを押下します。
6. 「保存」ボタンを押下して、設定値を保存します。

[メモ]

本製品の RADIUS クライアントを使用する場合は、クライアント一覧への登録は不要です。

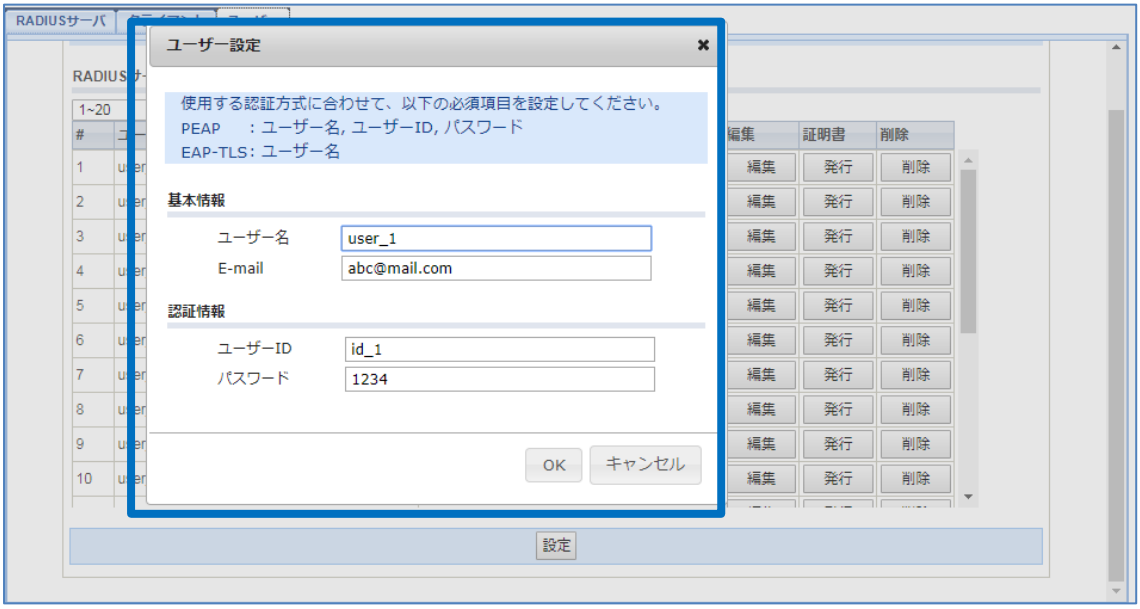


設定項目	説明	初期値
クライアント設定		
IP アドレス	RADIUS クライアントの IP アドレスとネットマスクを入力します。	未設定
事前共有鍵	認証に使用する事前共有鍵を入力します。	未設定
コメント	設定した RADIUS クライアントを識別するための任意コメントを入力します。	未設定

■ユーザーの設定

※ユーザーは最大 200 ユーザー登録できます。

1. [TOP]-[セキュリティ]-[簡易 RADIUS 機能]画面を開きます。
2. [ユーザー]タブをクリックします。
3. 「編集」ボタンをクリックして、ユーザー名、ユーザーのメールアドレス、認証用の ID とパスワードを設定します。
4. 編集後に「OK」ボタンをクリックします。ユーザー一覧から削除したい場合は、「削除」ボタンをクリックします。
5. ユーザーの設定が終わりましたら、「設定」ボタンを押下します。[設定]ボタンを押下しないと、ユーザー情報が更新されません。
6. 「保存」ボタンを押下して、設定値を保存します。



認証方式によって必須となるパラメータが異なります。お使いになる環境に合わせて設定してください。

PEAP　　：基本情報のユーザー名、認証情報のユーザーID, 認証情報のパスワード

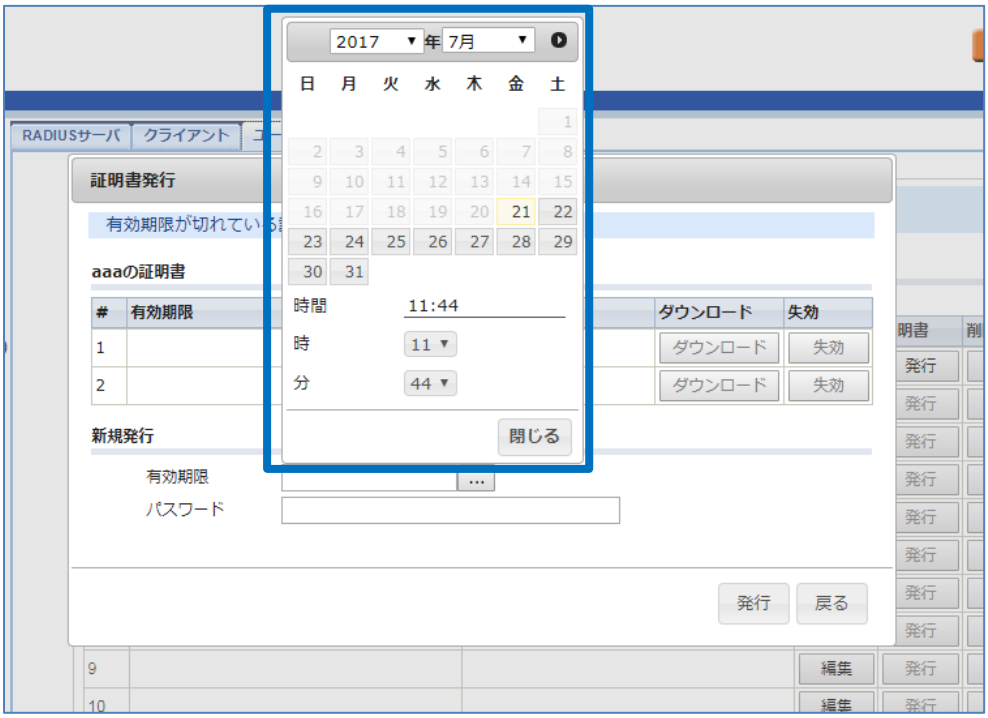
EAP-TLS　：基本情報のユーザー名

※基本情報の E-mail はクライアント証明書作成で使用します。

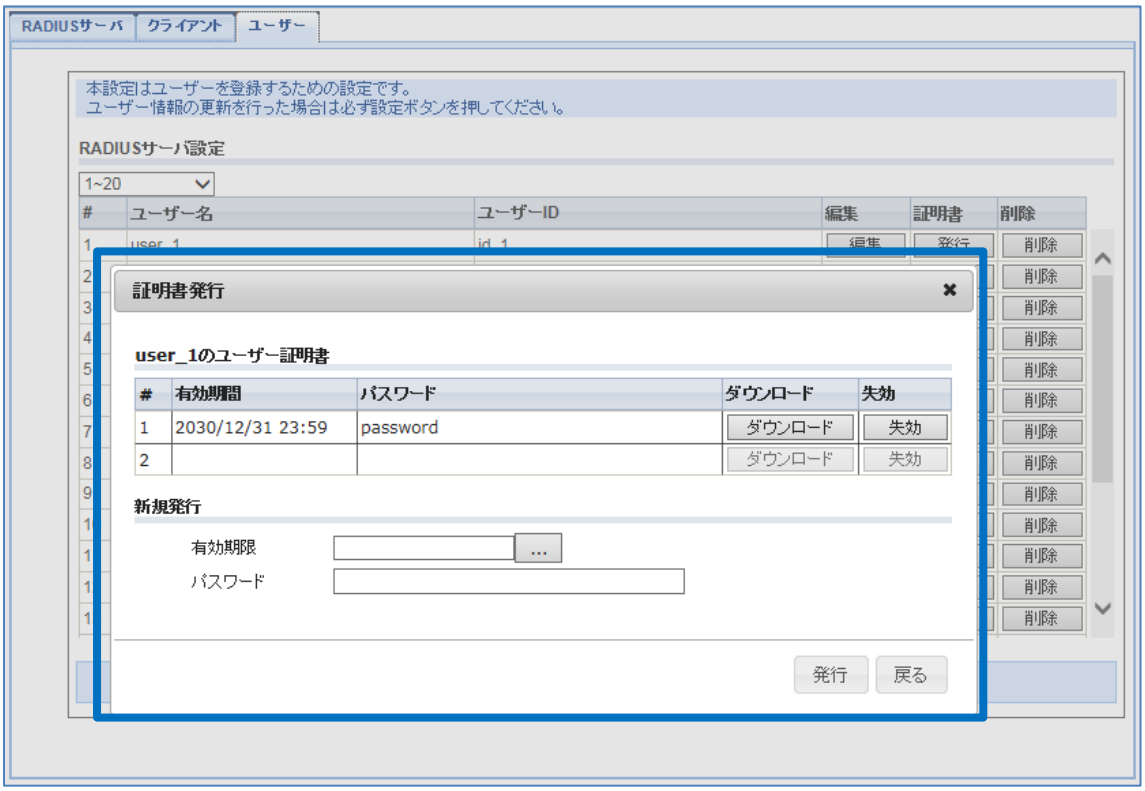
※PEAP をお使いになる場合は、クライアント証明書は必要ありません。

設定項目	説明	初期値
基本情報		
ユーザー名	接続を行うユーザー名を入力します。	未設定
E-mail	ユーザーのメールアドレスを入力します。	未設定
認証情報		
ユーザーID	認証に使用するユーザーID を入力します。	未設定
パスワード	認証に使用するパスワードを入力します。	未設定

■クライアント証明書発行



1. ユーザーを追加するとクライアント証明書の「発行」ボタンがクリックできるようになります。
2. 「発行」ボタンをクリックします。
3. カレンダーの画面が表示されますので、クライアント証明書の有効期限を設定して「閉じる」ボタンをクリックします。



4. 設定した有効期限が新規発行の有効期限の欄に反映されます。
5. 任意のパスワードを設定します。
6. [発行]ボタンを押下して、クライアント証明書を生成します。
7. [ダウンロード]ボタンを押下して、クライアント証明書をダウンロードします。

認証するユーザー端末に、ルート証明書とクライアント証明書を登録します。本書では登録手順は割愛します。ルート証明書は発行元不明と表示することがありますが、認証に影響はありません。
1 ユーザーに最大 2 つのクライアント証明書を発行可能です。
※ユーザー端末へのクライアント証明書の設定方法はユーザー端末のマニュアルを参照してください。

[メモ]
本製品の有線 LAN ポートに接続している無線アクセスポイントの再認証については、無線アクセスポイントの設定に依存します。無線アクセスポイントが再認証しない場合は、無線 LAN 端末が帰属した後にクライアント証明書の有効期限が満了したとしても、無線アクセスポイントとの接続中は無線の帰属が外れることはありません。
登録ユーザーの発行済みクライアント証明書を 2 つとも失効させて、新しくクライアント証明書を発行したい場合は、該当ユーザーを削除して、ユーザーを再登録してください。

5.8.12.2. **本製品を RADIUS クライアントとして使用する場合**

本製品を RADIUS クライアントとして使用する場合の設定は、無線 LAN の設定画面で行います。
設定方法は、5.7.8 章を参照してください。

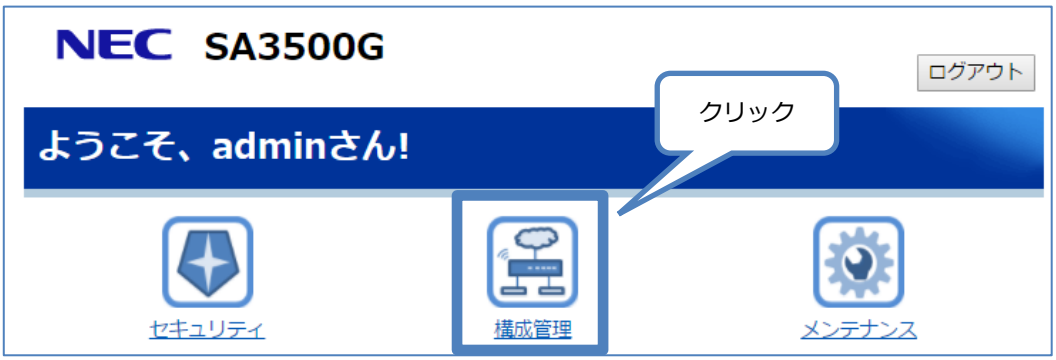
[接続確認済み OS]
・Windows 10/8.1/7
・macOS 10.12/10.14
・iOS 10.3.3/10.3.1
・Android 7.1.2/6.0.1
※本製品内部の RADIUS クライアントを使用した場合

[メモ]
本製品を RADIUS クライアントとして動作させる場合、RADIUS サーバと 1 時間ごとに再認証を行います。このときクライアント証明書の有効期限が満了している場合は無線の帰属が外れます。

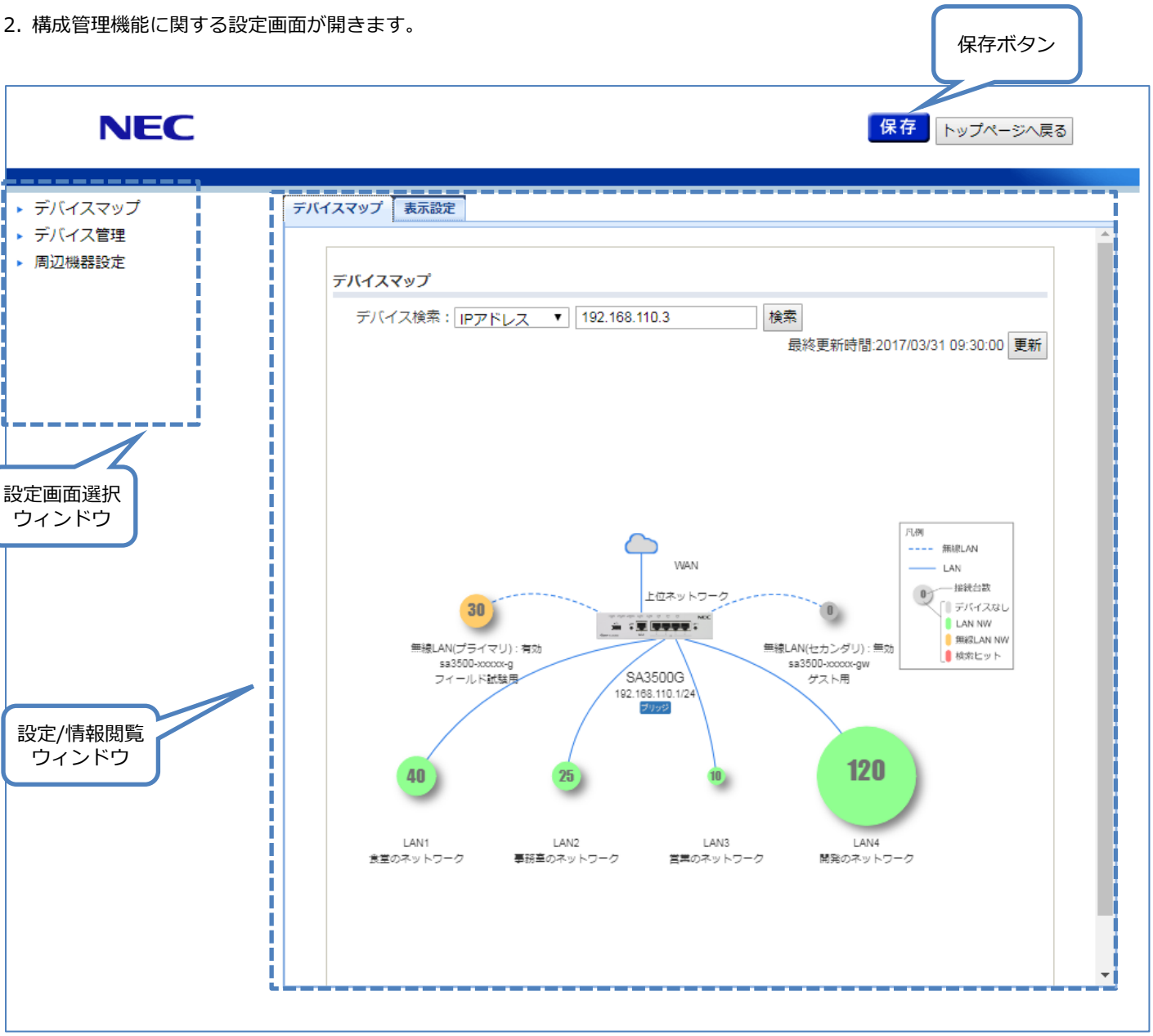
5.9. 構成管理機能に関する設定

構成管理機能は、ブリッジモード、ルータモードで共通です。

1. TOP 画面で「構成管理」アイコンをクリックします。



2. 構成管理機能に関する設定画面が開きます。



5.9.1. **設定画面構成**

構成管理に関する設定画面構成は次のとおりです。

項目		説明	操作の必要性の有無/備考
構成管理		構成管理機能に関する設定と参照	
	デバイスマップ	デバイスマップの表示、および設定	
	デバイス管理	デバイス管理の設定	
	周辺機器設定	Aspire 連携機能とパトライト連携機能の設定 パトライト連携機能の設定	

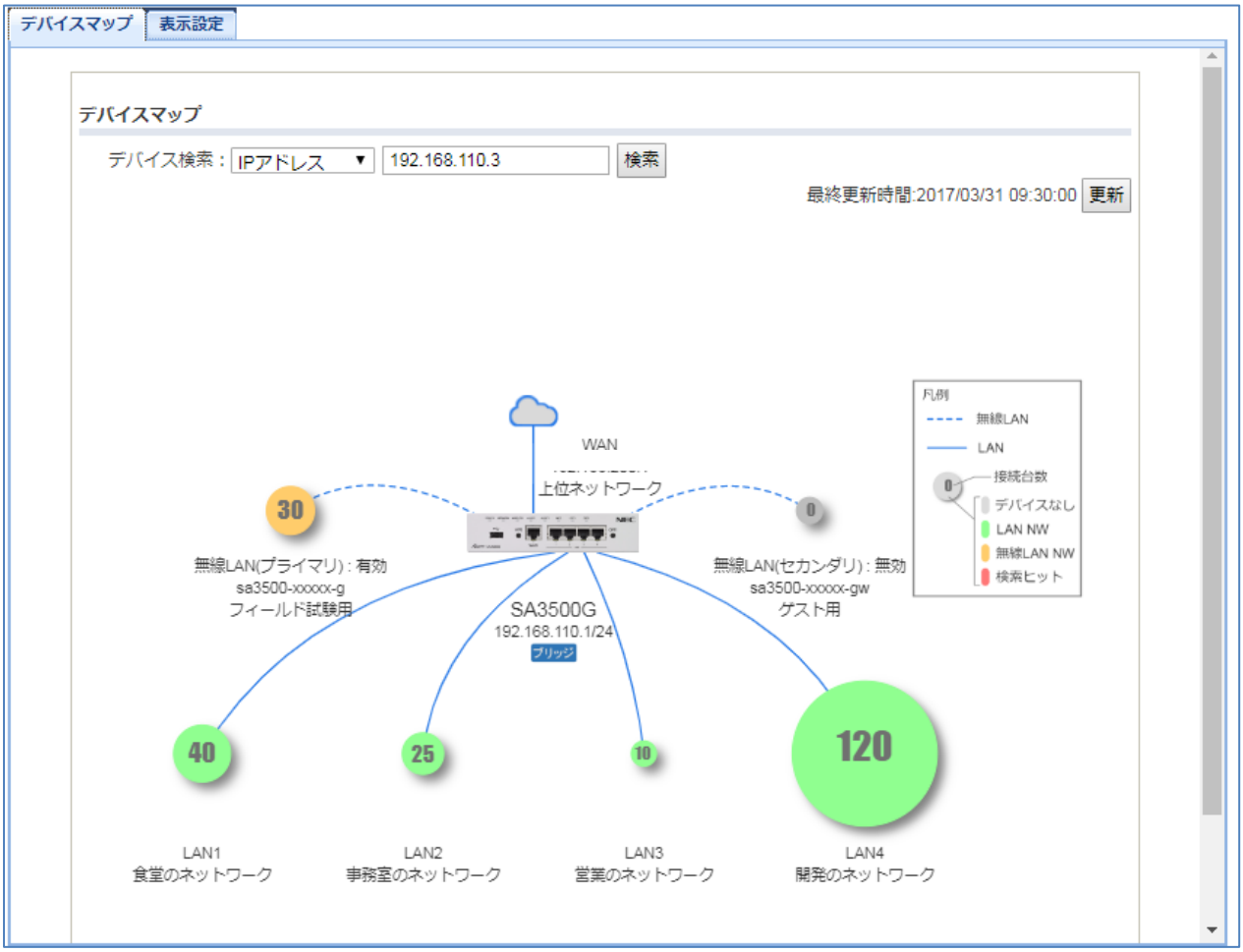
5.9.2. **デバイスマップ**

次の場合は設定 Web で設定を変更してください。

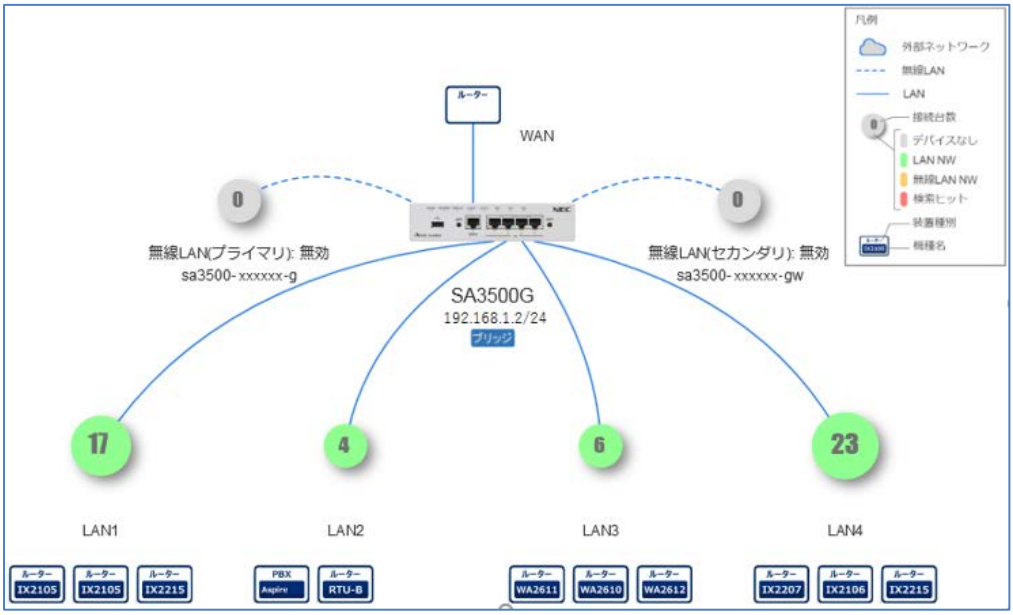
- 物理 LAN ポートごとに、ポート識別のための任意の名前を追加/変更したい
- デバイスマップ上に表示する、情報の更新間隔を設定したい

■デバイスマップによる端末検索方法

MAC モードの表示例

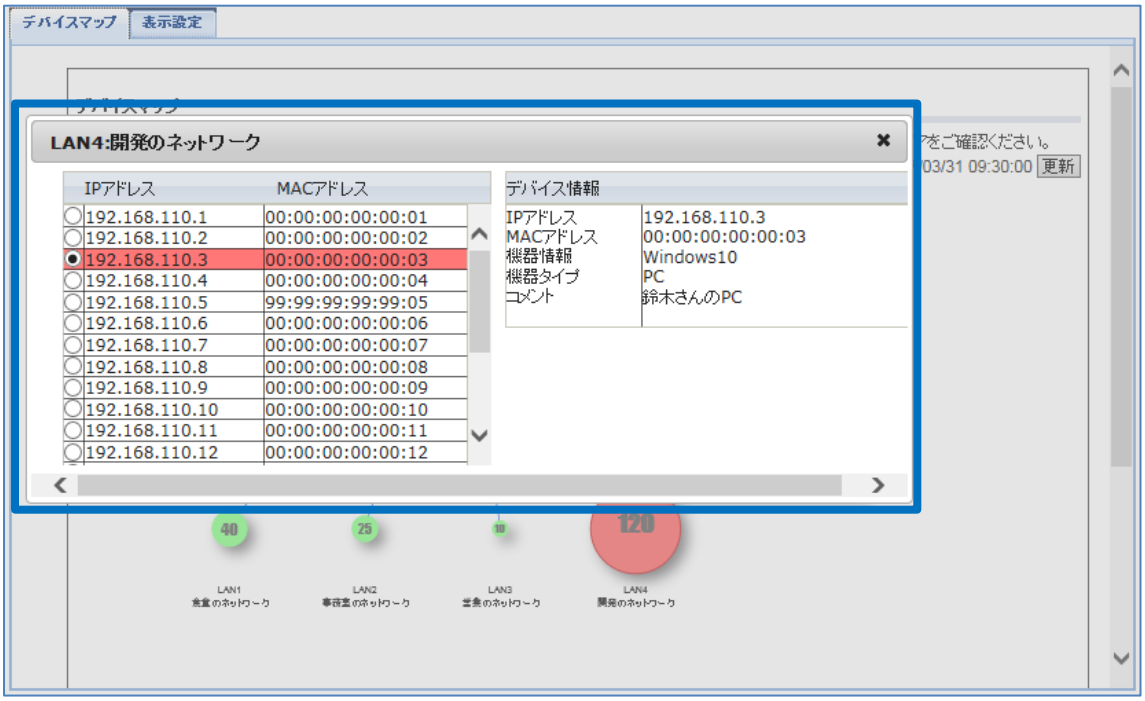


IP モードの表示例



※周辺機器設定で Aspire を登録している場合、デバイスマップ上に Aspire を示すアイコンを表示します。

1. [TOP]-[構成管理]-[デバイスマップ]画面を開いて、[デバイスマップ]タブをクリックします。
2. プルダウンメニューで検索キーとして「IP アドレス」もしくは「MAC アドレス」を選択します。
3. 「IP アドレス」もしくは「MAC アドレス」を入力し「検索」ボタンをクリックします。
4. 検索した端末の接続ポートの円マークが赤色に変わり接続場所を示します。
5. この接続ポートの円マークをクリックすることで、次のように検索した端末の詳細情報を確認することができます。



[メモ]

接続されている端末数が増えると、接続台数の円マークのサイズが大きくなります。

表示する接続台数は最大 250 台です。

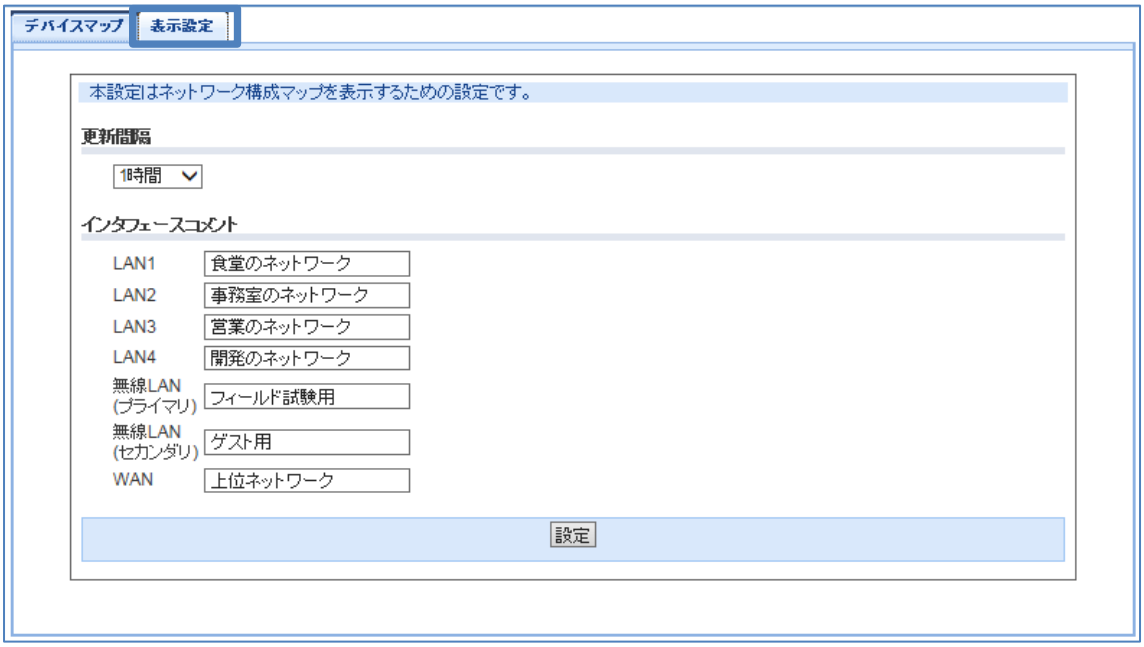
[ご注意]

デバイスマップは LAN-WAN 間の通信を行った端末を検出して表示します。LAN-LAN 間で行われる通信は検知しません。

本装置とデバイスの間にルータが接続されていた場合、デバイス情報が正しく表示されません。MAC アドレスはルータの WAN 側アドレス、機器情報、機器タイプがデバイスの情報と表示されます。

機器情報、機器タイプは、必ずしもデバイスの情報と一致するものではありません。デバイス上で動作するアプリケーションが、User-Agent を偽装して HTTP 通信しているときに、一致しない場合があります。

■デバイスマップの表示設定(MAC モード)

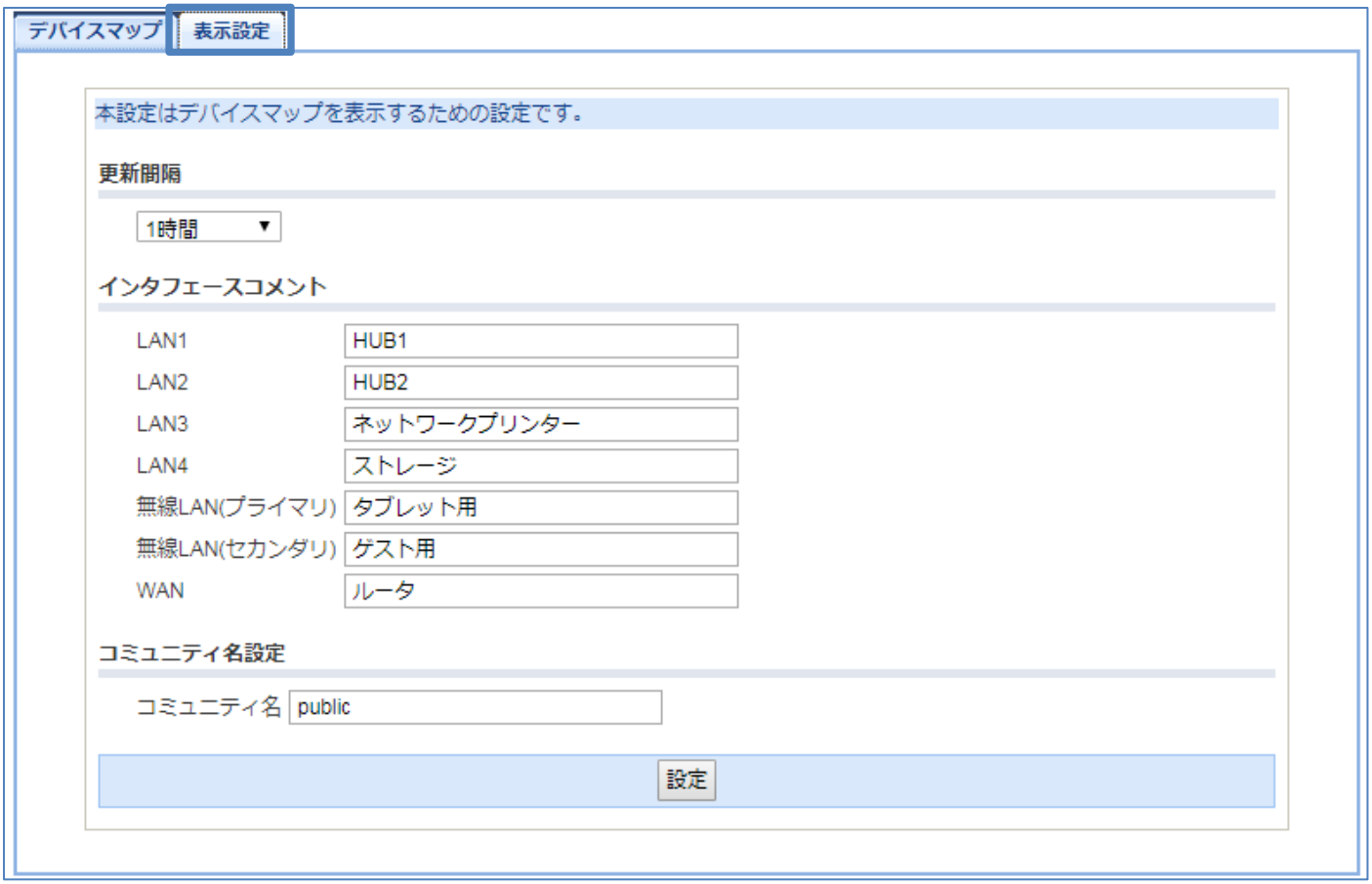


1. [TOP]-[構成管理]-[デバイスマップ]で[表示設定]のタブをクリックします。
2. 更新間隔をプルダウンメニューから選択します。
3. 各インタフェースのコメントを入力します。最大 32 文字です。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

設定項目	説明	初期値
更新間隔	表示するデバイス情報のバックグラウンドでの更新間隔をプルダウンで設定します。 1 時間、4 時間、8 時間、12 時間、24 時間、更新しないから選択します。	1 時間
インタフェースコメント	各物理インタフェースにコメントを付けることができます。	
LAN1	LAN ポート 1 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
LAN2	LAN ポート 2 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
LAN3	LAN ポート 3 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
LAN4	LAN ポート 4 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
無線 LAN (プライマリ)	プライマリ SSID を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定

	無線 LAN (セカンダリ)	セカンダリ SSID を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
	WAN	WAN ポートを識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定

■デバイスマップの表示設定(IP モード)



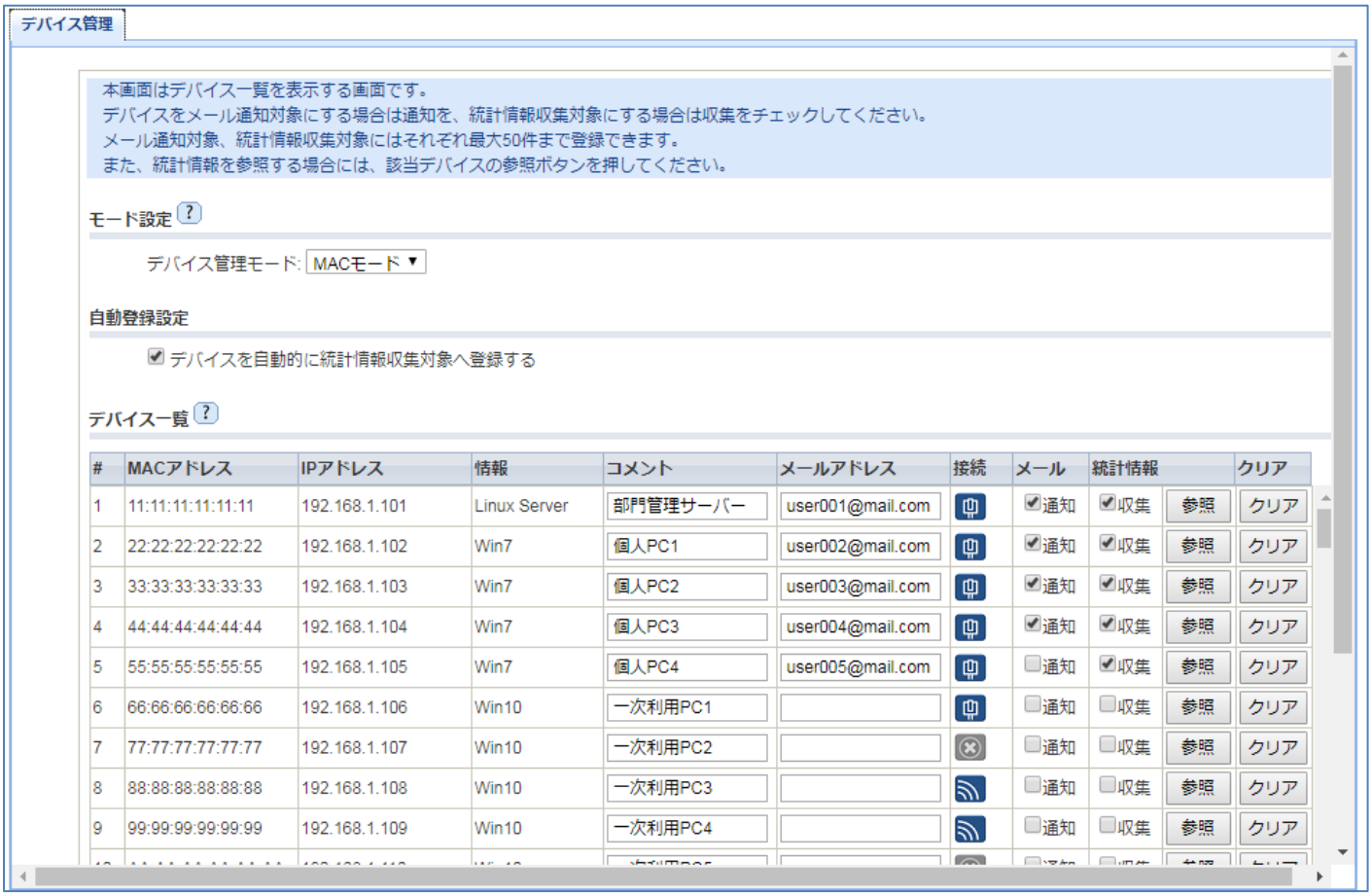
1. [TOP]-[構成管理]-[デバイスマップ]で[表示設定]のタブをクリックします。
2. 更新間隔をプルダウンメニューから選択します。
3. 各インタフェースのコメントを入力します。最大 32 文字です。
4. コミュニティ名を設定します。IX シリーズルータの本製品の連携機能をご使用になる場合は、連携機器の SNMP を有効にしていただき、連携機器の SNMP コミュニティ名と同じコミュニティ名を本設定にて設定してください。最大 30 文字です。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下して、本設定を保存します。

設定項目	説明	初期値
更新間隔	表示するデバイス情報のバックグラウンドでの更新間隔をプルダウンで設定します。 1 時間、4 時間、8 時間、12 時間、24 時間、更新しないから選択します。	1 時間
インタフェースコメント	各物理インタフェースにコメントを付けることができます。	
LAN1	LAN ポート 1 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
LAN2	LAN ポート 2 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
LAN3	LAN ポート 3 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
LAN4	LAN ポート 4 を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
無線 LAN (プライマリ)	プライマリ SSID を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
無線 LAN (セカンダリ)	セカンダリ SSID を識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
WAN	WAN ポートを識別するための名前などを入力してください。0 から 32 文字以内で設定できます。	未設定
コミュニティ名設定	ネットワークのコミュニティ名を設定します。	
コミュニティ名	本製品と連携するルータをお使いの場合は、ルータに設定した SNMP のコミュニティ名と同じコミュニティ名を設定してください。	public

5.9.3. デバイス管理

次の場合は設定 Web で設定を変更してください。

- 端末識別のための任意のコメントを追加、変更したい
- 端末使用者にメール通知を行いたい
- 端末ごとの統計情報収集対象に関する設定を変更したい
- 手動で端末を登録したい



※図は MAC モードの表示イメージです。IP モードでは表示順が IP アドレス、MAC アドレスの順になります。

1. [TOP]-[構成管理]-[デバイス管理]画面を開きます。
2. モード設定からデバイス管理モードを「MAC モード」もしくは「IP モード」から選択します。Ver3.3.26 以前のファームウェアは MAC モードです。Ver3.3.26 以前のファームウェアからバージョンアップされた場合は「MAC モード」でお使いください。
3. 検出した端末の端末ごとの統計情報を有効にしたい場合は自動検出設定の「デバイスを自動的に統計情報収集対象へ登録する」にチェックします。
4. 自動表示された MAC アドレスを確認するか、手動で MAC アドレスを入力します。
5. [コメント]に端末を識別するための名前などを入力します。
6. [メールアドレス]にメール通知を受けたい端末使用者のメールアドレスを入力します。
   ※メール通知の利用には、メールアカウントの設定が必要です。(5.8.10 章参照)
7. メール通知を行う場合は[メール]にチェックします。(このとき、メールアドレスは必ず入力してください。)
8. 端末ごとの統計情報の収集対象とする場合は[統計情報]にチェックします。
   ※「参照」ボタンを押下し、メッセージが表示されたあとに「OK」をクリックすると、「TOP」-「セキュリティ」-「統計情報」の画面に遷移します。(6.1.12 章参照)
9. [設定]ボタンを押下します。

10. [保存]ボタンを押下して、本設定を保存します。

[手動登録]

- 手動で端末を登録する場合は、登録する端末の MAC アドレスを用意してください。
  また、[コメント]、[メールアドレス]、[統計情報]のいずれかに値の入力が必須です

[デバイス一覧に既に 100 件表示されている場合]

- デバイス一覧から削除する端末の「クリア」ボタンを押下します。その後にアクセス履歴の「参照」ボタンを押下して、本製品にアクセスしたデバイスリストを表示します。リストから追加したい MAC アドレスを選択して、「追加」ボタンを押下します。
- デバイス一覧から削除する端末の「クリア」ボタンを押下します。空白になった行に、登録する端末の MAC アドレス、コメント、メールアドレス、統計情報を入力して、「設定」ボタンを押下します。

[デバイスの削除]

本製品はセキュリティ装置であるため、本製品の運用中に通信を検知したデバイスの情報を保持します。
このため、デバイス一覧からデバイスを削除するには、以下の手順で行います。

1．削除するデバイスと本製品の接続を遮断します。
2. [TOP]-[構成管理]-[デバイス管理]画面を表示します。
3.「デバイスを自動的に統計情報収集対象へ登録する」のチェックを外します。
4. 削除するデバイスの行の「クリア」ボタンを押します。
5. 画面下にある「設定」ボタンを押します。
6. 画面上にある「保存」ボタンを押します。
7. 本製品の電源 OFF/ON、または[TOP]-[メンテナンス]-[メンテナンス]-[再起動]画面で本製品を再起動します。

[メモ]

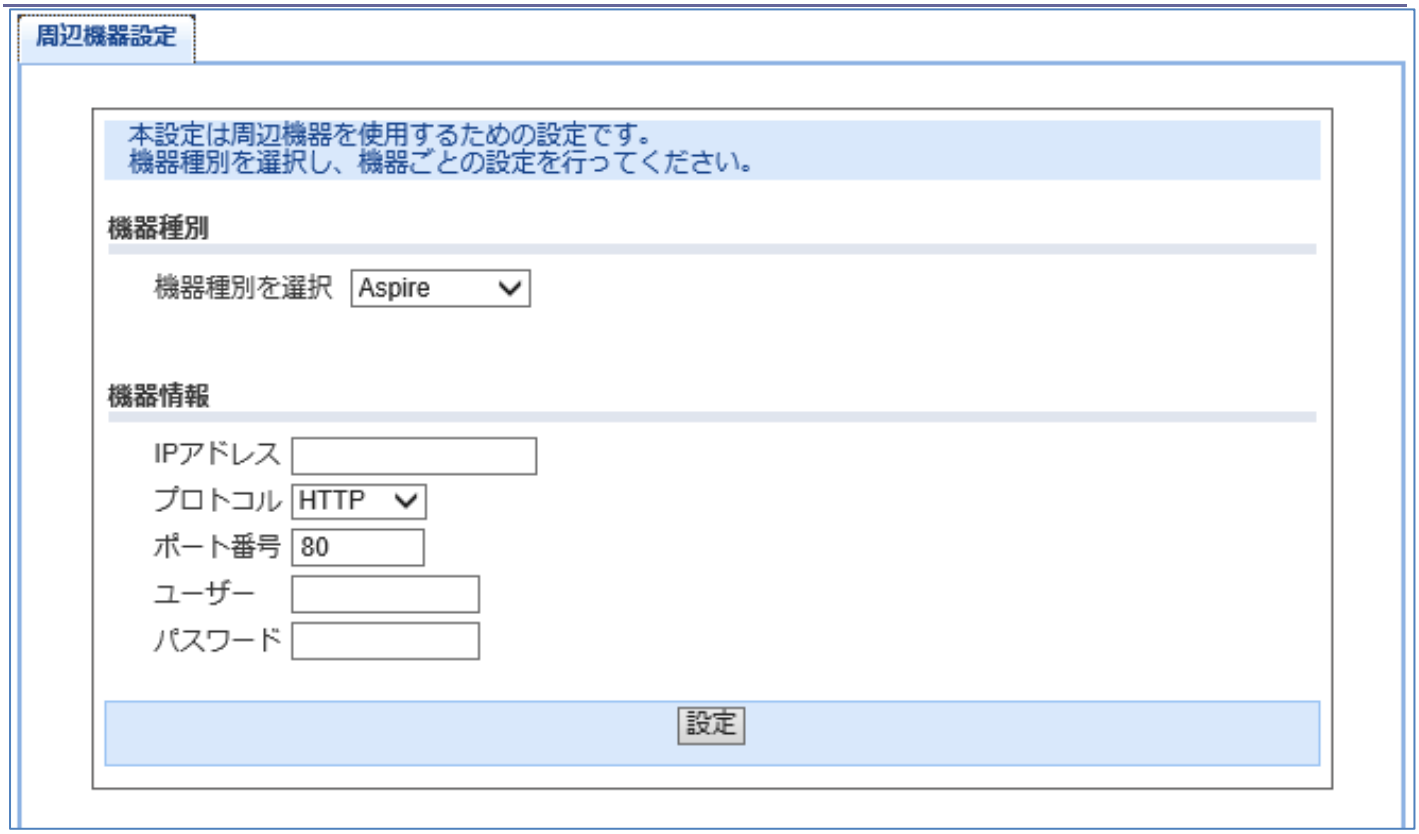
登録されている端末数が多い場合、表示に時間がかかる場合があります。

設定項目	説明	初期値
モード設定	デバイス管理のモードを MAC アドレス単位の MAC モードか IP アドレス単位の IP モードかを指定します。モードを変更すると、それまで本製品に保持していた統計情報がクリアされます。ご注意ください。	MAC モード
自動登録設定	端末ごとの統計情報を自動的に有効にしたい場合に本項目をチェックします。	有効
デバイス一覧	端末ごとに以下項目の表示と設定ができます。	
MAC アドレス	検出した端末の MAC アドレスを表示します。 MAC アドレスを手動で入力することもできます。	未設定
IP アドレス	検出した IP アドレスを表示します。	
情報	検出した端末の OS などの関連情報を表示します。 端末の通信内容から検出するため、ご利用のアプリケーションなどによっては、異なる情報が表示する場合があります。	
コメント	端末を識別するための名前などを入力してください。 「"、'、`、$、¥、<、>」は使用できません。	未設定
メールアドレス	メール通知を受けたい端末使用者のメールアドレスを入力してください。	未設定
接続	有線、無線、未接続をアイコンで表示します。 本製品から管理対象の端末を検知できない場合は、未接続の表示になります。	
メール通知	メール通知を有効にする場合はチェックを入れます。	無効
統計情報	端末ごとの統計情報の収集対象にする場合はチェックを入れます。 チェックを入れることができる端末数は最大 50 台です。 手動入力した端末は手動でチェックしてください。	無効
参照	選択している端末の統計情報を参照したいときにクリックします。	
クリア	該当行が空行となり、手動登録可能になります。 空行のまま設定を保存した場合、画面更新後に自動検出した端末情報が表示する場合があります。	
アクセス履歴		
参照	デバイス一覧に表示しきれない端末情報を参照するときにクリックします。	

5.9.4. **周辺機器設定**

本製品の Aspire 連携機能とパトライト連携機能を使用する場合は、本章を参考に設定してください。

5.9.4.1. **Aspire 連携機能の設定**



1. [TOP]-[構成管理]-[周辺機器設定]画面を開きます。
2. 「機器種別を選択」で「Aspire」を選択します。
3. 「IP アドレス」、「プロトコル」、「ポート番号」、「ユーザー」、「パスワード」を入力します。
   ※「ユーザー」と「パスワード」は、デバイスマップ機能において、Aspire の IP 電話の IP アドレス、内線番号の情報を取得するために使用します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

[Aspire 連携機能の解除方法]

1. [TOP]-[構成管理]-[周辺機器設定]画面を開きます。
2. 「機器種別を選択」で「Aspire」を選択します。
3. 「IP アドレス」に設定されている IP アドレスを削除し、空欄にします。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下して、本設定を保存します。

※[TOP]画面に表示されていた[Aspire]アイコンは削除されます。

設定項目	説明	初期値
機器種別	Aspire を選択します。	Aspire
	選択した機器ごとに以下項目の表示と設定ができます。	
IP アドレス	連携する Aspire の IP アドレスを入力します。	未設定
プロトコル	HTTP と HTTPS を選択します。	HTTP
ポート番号	設定可能な数値は以下です。 <HTTP の場合> 80, 1024-65535 <HTTPS の場合> 443, 1024-65535	<HTTP> 80 <HTTPS> 443
ユーザー	Aspire の Web プログラミングのログインユーザー名を設定します。	未設定
パスワード	Aspire の Web プログラミングのログインパスワードを設定します。	未設定

5.9.4.2. **パトライト連携機能の設定**

本製品のパトライト連携機能を使用する場合は、本章を参考に設定してください。

パトライトは別売（当社オプションではありません）です。お客様自身でご用意ください。

当社動作確認済みパトライト製品は 3.3.15 章を参照してください。

1. [TOP]-[構成管理]-[周辺機器設定]画面を開きます。
2. 機器種別を選択でパトライトを選択します。
3. パトライト設定で「機能を使用する」をチェックします。
4. [接続設定]にパトライトに設定されている情報を入力します。
5. [点灯条件]に点灯させる脅威検出条件をチェックします。
6.「設定」ボタンを押下します。
7.「保存」ボタンを押下して、本設定を保存します。

設定項目	説明	初期値
機器種別	パトライトを選択します。	Aspire
パトライト設定	パトライト連携機能を使用する場合に本項目をチェックします。	無効
接続設定		
IP アドレス	パトライトに設定しているユニット IP を指定します。	未設定
ポート番号	パトライトに設定しているユニットポートを指定します。	未設定
通信プロトコル	パトライトに設定している通信プロトコルを指定します。 「TCP」または「UDP」を選択します。	TCP
点灯条件		
AV ブロック時に点灯する	アンチウイルスで脅威を検出したときにパトライトを点灯する場合は、本項目をチェックします。	有効
IPS ブロック時に点灯する	不正侵入防止で脅威を検出したときにパトライトを点灯する場合は、本項目をチェックします。	無効
WG ブロック時に点灯する	Web ガードで脅威を検出したときにパトライトを点灯する場合は、本項目をチェックします。	有効
UF ブロック時に点灯する	URL フィルタリングで脅威を検出したときにパトライトを点灯する場合は、本項目をチェックします。	無効
KF ブロック時に点灯する	URL キーワードフィルタリングで脅威を検出したときにパトライトを点灯する場合は、本項目をチェックします。	無効
APG ブロック時に点灯する	アプリケーションガードで脅威を検出したときにパトライトを点灯する場合は、本項目をチェックします。	無効

5.10. **スイッチ操作**

本製品には 4 つのスイッチがあります。各スイッチの配置位置は 2.3.1 章の図を参照してください。

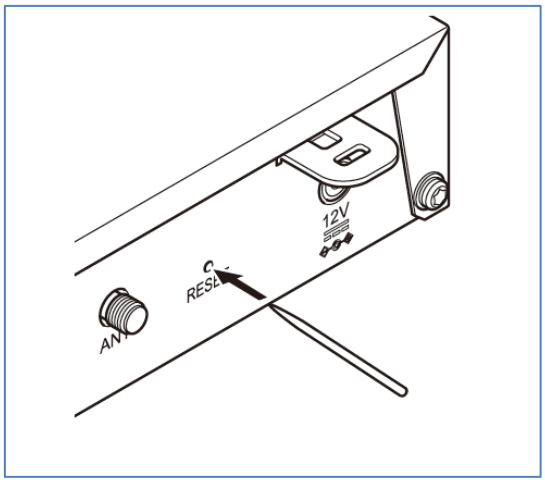
表示	機能	スイッチ位置	備考
RESET	本製品の初期化	製品背面右側	プッシュ型
OPT1	セキュリティ・スキャン機能用スイッチ ・アクティベーション ・脅威検出状態解除	製品前面右側	プッシュ型
OPT2	ファームウェアアップデート用	製品背面左側	プッシュ型
WPS	WPS スイッチ	製品前面左側	プッシュ型

5.10.1. **初期化**

本製品の RESET スイッチを使って初期化します。

1. 本製品の POWER ランプが緑点灯していることを確認します。
   電源を入れ直した場合や電源を入れた直後の場合は、約 140 秒お待ちください。

2. 本製品の背面にある RESET スイッチを細い棒状のもの(電気を通さない材質のもの、つまようじの先など)で押し続け、POWER ランプ、NETWORK ランプ、WIRELESS ランプが緑点滅を始めたら放します。
   POWER ランプ、NETWORK ランプ、WIRELESS ランプが緑点滅するまで約 6 秒～ 10 秒かかります。



以上で初期化は完了です。
初期化後、本製品は自動で再起動します。

各ランプがすべて緑点灯した後、POWER ランプ以外が一度消灯するまでお待ちください。
（その他のランプは、ご利用状況によって状態が変化します。）

[メモ]

設定 Web でも設定値を初期化できます。
初期化範囲は、設定 Web、RESET スイッチのどちらも同じです。
本製品再起動後、アクティベーション操作する必要はありません。

5.10.2. **アクティベーション**

初回設置時にアクティベーション操作が必要です。

5.2.3 章を参照してください。

5.10.3. **脅威検出状態の解除**

アンチウイルス機能でのウイルス検出、および、Web ガード機能でのトラフィック遮断で、「脅威検出状態」に移行します。

このとき、ALERT1 ランプが橙点滅、または橙点灯します。（脅威を検出したことをお知らせするための状態表示です。）

OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を数秒押し続けることで、ALERT1 ランプが消灯し脅威検出状態を解除できます。

なお、ランプが橙点灯/点滅していても脅威は既に除去されている状態です。

[メモ]

- 脅威検出状態の解除は、設定 Web でも操作できます。
  設定 Web でセキュリティログを閲覧することで、脅威検出状態を解除します。
- 脅威検出状態の際に、本製品を再起動した場合は、「脅威検出状態」は解除されます。

[メモ]

脅威検出状態（ALERT1 ランプの橙点滅/橙点灯）は、脅威を検出したことをお知らせする機能です。

脅威検出状態中でもセキュリティ・スキャン機能は動作します。

5.10.4. **スイッチ操作によるファームウェアの更新**

メンテナンスバージョンアップ機能を使用する場合、スイッチ操作で新しいファームウェアに更新できます。

動作仕様は次のとおりです。INFO ランプの状態で動作が異なります。

[INFO ランプが橙点灯している場合]

1. 本製品の背面にある OPT2 スイッチを細い棒状のもの（電気を通さない材質のもの、つまようじの先など）で 2 秒以上押し続けます。
2. ファームウェアの更新が始まると INFO ランプが橙点滅します。橙点滅したら、OPT2 スイッチを放します。本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

[INFO ランプが消灯している場合]

1. 本製品の背面にある OPT2 スイッチを細い棒状のもの（電気を通さない材質のもの、つまようじの先など）で INFO ランプが 0.5 秒周期で緑点滅するまで 2 秒以上押し続けます。緑点滅したら、OPT2 スイッチを放します。
2. 新しいファームウェアがあると INFO ランプは 3 秒後に橙点灯します。新しいファームウェアがない場合、INFO ランプは 3 秒後に消灯します。
3. INFO ランプが橙点灯した場合、本製品の背面にある OPT2 スイッチを細い棒状のもの（電気を通さない材質のもの、つまようじの先など）で INFO ランプが橙点滅するまで 2 秒以上押し続けます。橙点滅したら、OPT2 スイッチを放します。
4. ファームウェアの更新が始まります。本製品が再起動し、INFO ランプが消灯していれば、ファームウェアの更新は完了です。

[メモ]

- ファームウェア更新中は電源を OFF しないでください。故障の原因となります。
- メンテナンスバージョンアップ機能を有効にするには、5.6.16 章を参照してください。初期値は有効です。

5.10.5. **WPS スイッチによる Wi-Fi の自動設定**

本製品の WPS スイッチを使用して、WPS-PBC に対応した無線 LAN 端末と Wi-Fi の自動設定を行うことができます。

設定方法は下記のとおりです。

※ 設定の際は、本製品と無線 LAN 端末は近くに置いた状態で設定してください。(目安：1m 程度)

[ご注意]

以下の場合、WPS 機能が無効となります。

- 無線 LAN 機能が無効
- 無線の MAC アドレスフィルタリング機能が有効
- プライマリ SSID の無線暗号化モードを TKIP、または、802.1X(EAP)に設定
- プライマリ SSID の ESS-ID ステルス機能が有効

1. 無線 LAN 端末の WPS-PBC 機能を起動する
   ※起動方法は、無線 LAN 端末に添付の取扱説明書などを参照してください。
2. 本製品前面の WPS スイッチを押し続けて、本製品の WIRELESS ランプが橙点滅したら放す
3. 本製品の WIRELESS ランプが橙点灯することを確認する
   ※ WIRELESS ランプは WPS 処理が終わった後、緑点灯に戻ります。

失敗した場合は、WIRELESS ランプが約 10 秒間赤点滅します。

再度手順 1 からやり直しても失敗する場合は、無線 LAN 端末の取扱説明書などを参照して、本製品の SSID と暗号化キーにより手動設定してください。

※ 本製品の SSID と暗号化キーは、5.7.8 章「無線 LAN の設定」でお客様自身が設定したものです。設定値は設定 Web で確認してください。

6. 装置情報の確認

6.1. 装置情報の確認

本製品で確認できる装置情報は次のとおりです。

装置情報	確認画面
現在のファームウェアバージョン	TOP → メンテナンス → 情報 → デバイスの状態
ネットワーク情報	TOP → メンテナンス → 情報 → デバイスの状態
DHCP サーバアドレス払い出し情報、Wi-Fi 帰属情報、 ARP テーブル情報	TOP → メンテナンス → 情報 → 装置管理情報
ルーティングテーブル	TOP → メンテナンス → 情報 → ルーティングテーブル
BGP ピア状態	TOP → メンテナンス → 情報 → BGP ピア状態
IPsec SA 情報	TOP → メンテナンス → 情報 → VPN 接続状態
IPsec 証明書情報	TOP → メンテナンス → 情報 → VPN 接続状態
IPsec トンネルを通過するトラフィックの統計情報	TOP → メンテナンス → 情報 → VPN 統計情報
SNMP MIB 情報	TOP → メンテナンス → 情報 → MIB 情報
イベントログ	TOP → メンテナンス → 情報 → イベントログ
セキュリティ・スキャン機能のライセンス情報	TOP → セキュリティ → ステータス
セキュリティ・スキャン機能のログ情報	TOP → セキュリティ → セキュリティログ
セキュリティ・スキャン機能の統計情報	TOP → セキュリティ → 統計情報
ping 送信によるネットワーク到達確認	TOP → メンテナンス → 診断機能 → ping
traceroute によるネットワーク経路確認	TOP → メンテナンス → 診断機能 → traceroute
自己診断情報	TOP → メンテナンス → 診断機能 → 自己診断
パケットダンプ	TOP → メンテナンス → 診断機能 → パケットダンプ

6.1.1. ファームウェアバージョン、ネットワーク情報の確認（ブリッジモードの場合）

本製品のファームウェアのバージョン情報、ネットワーク情報を設定 Web で確認できます。

1. [TOP]-[メンテナンス]-[情報]-[デバイスの状態]画面を開きます。

■デバイスの状態（ブリッジモードの場合）

装置情報	説明
装置情報	本製品の装置情報を表示します
デバイス ID	本製品のデバイス ID を表示します
製造番号	本製品の製造番号を表示します
WAN MAC アドレス	本製品の WAN インタフェースの MAC アドレス情報を表示します
LAN MAC アドレス	本製品の LAN インタフェースの MAC アドレス情報を表示します
WLAN MAC アドレス	本製品の無線 LAN インタフェースの MAC アドレス情報を表示します
現在のファームウェアバージョン	システムファームウェアのバージョン情報を表示します
動作モード	ブリッジ … ブリッジモードで動作中 ルータ … ルータモードで動作中

無線情報 1	本製品のプライマリ SSID の無線情報を表示します
無線 LAN ネットワーク機能	プライマリ無線 LAN 機能の有効/無効の状態を表示します
ネットワーク名(SSID)	プライマリ無線 LAN 機能の SSID を表示します
使用チャネル	プライマリ無線 LAN 機能で使用しているチャネルを表示します
暗号化モード	プライマリ無線 LAN 機能で使用している暗号化モードを表示します
無線情報 2	本製品のセカンダリ SSID の無線情報を表示します
無線 LAN ネットワーク機能	セカンダリ無線 LAN 機能の有効/無効の状態を表示します
ネットワーク名(SSID)	セカンダリ無線 LAN 機能の SSID を表示します
使用チャネル	セカンダリ無線 LAN 機能で使用しているチャネルを表示します
暗号化モード	セカンダリ無線 LAN 機能で使用している暗号化モードを表示します
WAN 側 IPoE 状態	WAN 側 IPoE 状態を表示します
IPv4 接続状態	インターネット利用可能　… WAN ポートに IP アドレスが設定されている状態 インターネット未接続　　… WAN ポートに IP アドレスが未設定の状態
IPv4 アドレス/ネットマスク	WAN ポートの IP アドレス、ネットマスクを表示します
IPv4 ゲートウェイ	デフォルトゲートウェイアドレスを表示します
IPv4 プライマリ DNS	プライマリ DNS サーバアドレスを表示します
IPv4 セカンダリ DNS	セカンダリ DNS サーバアドレスを表示します
NetMeister 情報	NetMeister の情報を表示します
NetMeister 機能	NetMeister 機能の有効/無効の状態を表示します
状態	NetMeister 機能の更新結果（成功/失敗）と最終更新時刻を表示します
Ethernet ポート状態	Ethernet ポートの接続状態を表示します
WAN ポート	WAN ポートの接続状態を表示します
LAN ポート 1	LAN ポート 1 の接続状態を表示します
LAN ポート 2	LAN ポート 2 の接続状態を表示します
LAN ポート 3	LAN ポート 3 の接続状態を表示します
LAN ポート 4	LAN ポート 4 の接続状態を表示します
「最新状態に更新」ボタン	本画面の表示内容を最新の情報に更新します

6.1.2. ファームウェアバージョン、ネットワーク情報の確認（ルータモードの場合）

本製品のファームウェアのバージョン情報、ネットワーク情報を設定 Web で確認できます。

1. [TOP]-[メンテナンス]-[情報]-[デバイスの状態]画面を開きます。

■デバイスの状態（ルータモードの場合）

装置情報	説明
装置情報	
デバイス ID	本製品のデバイス ID を表示します
製造番号	本製品の製造番号を表示します
WAN MAC アドレス	本製品の WAN インタフェースの MAC アドレス情報を表示します
LAN MAC アドレス	本製品の LAN インタフェースの MAC アドレス情報を表示します

WLAN MAC アドレス	本製品の無線 LAN インタフェースの MAC アドレス情報を表示します
現在のファームウェアバージョン	システムファームウェアのバージョン情報を表示します
動作モード	
動作モード	ブリッジ … ブリッジモードで動作中 ルータ … ルータモードで動作中
無線情報 1	
無線 LAN ネットワーク機能	プライマリ無線 LAN 機能の有効/無効の状態を表示します
ネットワーク名（SSID）	プライマリ無線 LAN 機能の SSID を表示します
使用チャネル	プライマリ無線 LAN 機能で使用しているチャネルを表示します
暗号化モード	プライマリ無線 LAN 機能で使用している暗号化モードを表示します
無線情報 2	
無線 LAN ネットワーク機能	セカンダリ無線 LAN 機能の有効/無効の状態を表示します
ネットワーク名（SSID）	セカンダリ無線 LAN 機能の SSID を表示します
使用チャネル	セカンダリ無線 LAN 機能で使用しているチャネルを表示します
暗号化モード	セカンダリ無線 LAN 機能で使用している暗号化モードを表示します
LAN 側状態	
IPv4 アドレス/ネットマスク	LAN インタフェースの IP アドレス、サブネットマスクを表示します
DNS サーバ情報	
IPv4 プライマリ DNS	プライマリ DNS サーバアドレスを表示します
IPv4 セカンダリ DNS	セカンダリ DNS サーバアドレスを表示します
WAN 側 IPoE 状態	
IPv4 接続状態	インターネット利用可能　… WAN インタフェースに IP アドレスを設定している状態 インターネット未接続　　… WAN インタフェースに IP アドレスが未設定の状態
IPv4 アドレス/ネットマスク	WAN インタフェースの IP アドレス、サブネットマスクを表示します
IPv4 ゲートウェイ	デフォルトゲートウェイアドレスを表示します
WAN 側 PPPoE 状態	
IPv4 接続状態	インターネット利用可能　… WAN インタフェースに IP アドレスを設定している状態 インターネット未接続　　… WAN インタフェースに IP アドレスが未設定の状態
IPv4 アドレス	WAN インタフェースの IP アドレスを表示します
ホーム IP ロケーション	
ホーム IP ロケーション名	ホーム IP ロケーション名を表示します。
Ethernet ポート状態	Ethernet ポートの接続状態を表示します
WAN ポート	WAN ポートの接続状態を表示します
LAN ポート 1	LAN ポート 1 の接続状態を表示します
LAN ポート 2	LAN ポート 2 の接続状態を表示します
LAN ポート 3	LAN ポート 3 の接続状態を表示します
LAN ポート 4	LAN ポート 4 の接続状態を表示します
「最新状態に更新」ボタン	本画面の表示内容を最新の情報に更新します。

6.1.3. セキュリティ・スキャン機能のステータス

本製品のセキュリティ・スキャン機能のライセンス状況および各機能のシグネチャのバージョン情報を設定 Web で確認できます。
また、本製品のライセンス満了時刻（満了日時）を確認できます。

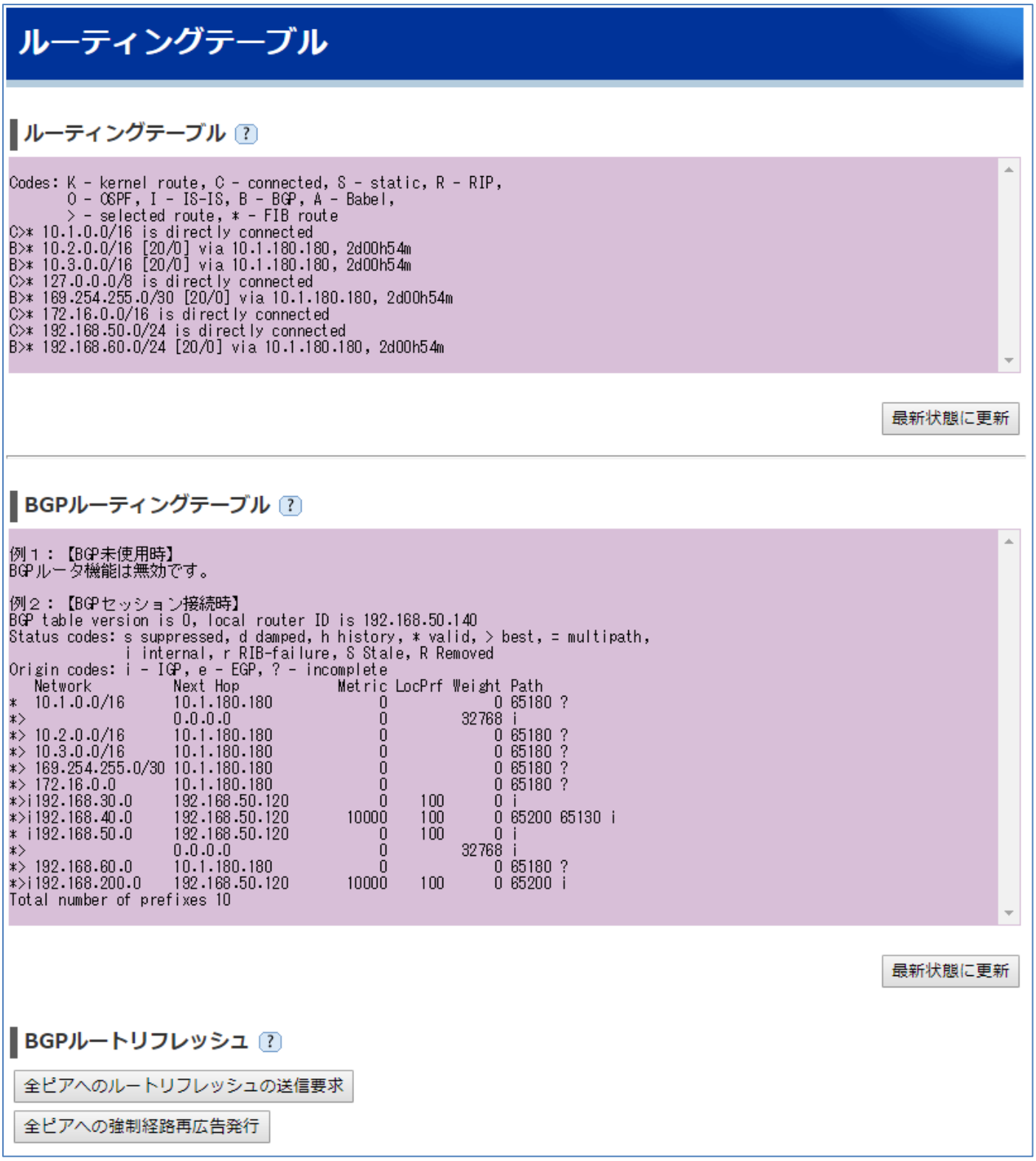
1. [TOP]-[セキュリティ]-[ステータス]画面を開きます。

装置情報	説明
ライセンス、シグネチャ情報	
ライセンス満了時刻	契約ライセンスの満了日時を表示します。
シグネチャ最終更新時刻	シグネチャの最終更新日時を表示します。
シグネチャ確認時刻	
機能動作状態	有効 … セキュリティ・スキャン機能が動作中の状態 無効 … セキュリティ・スキャン機能のライセンスが満了している状態、 アクティベーションが未実施の状態
「ライセンスを確認する」ボタン	ライセンスサーバにライセンス満了時刻を確認し、最新の満了時刻を表示します。 追加ライセンス(1 年)を購入したときに使用します。 ※ファームウェアバージョン 3.4.21 にて追加しました。
「シグネチャを更新する」ボタン	更新可能なシグネチャの有無を確認の上で、最新のシグネチャに更新します。
機能状態	
ファイアウォール（FW）	有効 … ファイアウォール機能が有効の状態 無効 … ファイアウォール機能が無効の状態 ※シグネチャを使用しない機能のため、シグネチャバージョンは“-”と表示されます。
アンチウイルス（AV）	有効 … アンチウイルス機能が有効の状態 無効 … アンチウイルス機能が無効の状態
不正侵入防止（IPS）	有効 …不正侵入防止機能が有効の状態 無効 …不正侵入防止機能が無効の状態
Web ガード	有効 … Web ガード機能が有効の状態 無効 … Web ガード機能が無効の状態
URL フィルタリング	有効 … URL フィルタリング機能が有効の状態 無効 … URL フィルタリング機能が無効の状態 ※シグネチャを使用しない機能のため、シグネチャバージョンは“-”と表示されます。
URL キーワードフィルタリング	有効 … URL キーワードフィルタリング機能が有効の状態 無効 … URL キーワードフィルタリング機能が無効の状態 ※シグネチャを使用しない機能のため、シグネチャバージョンは“-”と表示されます。
アプリケーションガード	有効 … アプリケーションガード機能が有効の状態 無効 … アプリケーションガード機能が無効の状態
簡易 RADIUS 機能	
機能動作状態	簡易 RADIUS 機能の動作状態を示します。 稼働中…簡易 RADIUS 機能が有効の状態 停止中…簡易 RADIUS 機能が無効の状態
登録クライアント数	本製品に登録されているクライアント数を示します。
登録ユーザー数	本製品に登録されているユーザー数を示します。

6.1.4. **ルーティングテーブル**

本製品のルーティングテーブルを設定 Web で確認できます。本情報はルータモードのときのみ表示されます。

1. [TOP]-[メンテナンス]-[情報]-[ルーティングテーブル]画面を開きます。



「最新情報に更新」ボタンを押下すると、表示画面を最新の情報に更新します。

[ルーティングテーブルの見かた]

項目	表示値	内容
Codes:	K - kernel route C – connected S – static R - RIP, O – OSPF I - IS-IS B – BGP A - Babel, > - selected route * - FIB route	ルーティングテーブルに追加するルートの情報源。
	10.1.0.0/16	宛先ルートとサブネットマスク
	is directly connected	直接本製品に接続されて、追加したテーブル
	[20/0]	20 はアドミニストレーティブディスタンスの値
		0 はメトリック。ダイナミックルーティングのときに使用する値。
	via 10.1.180.180	ネクストホップアドレス
	2d00h54m	ダイナミックルーティングにおいて、宛先ルートが追加されてからの経過時間 例では 2 日と 54 分経過しています。

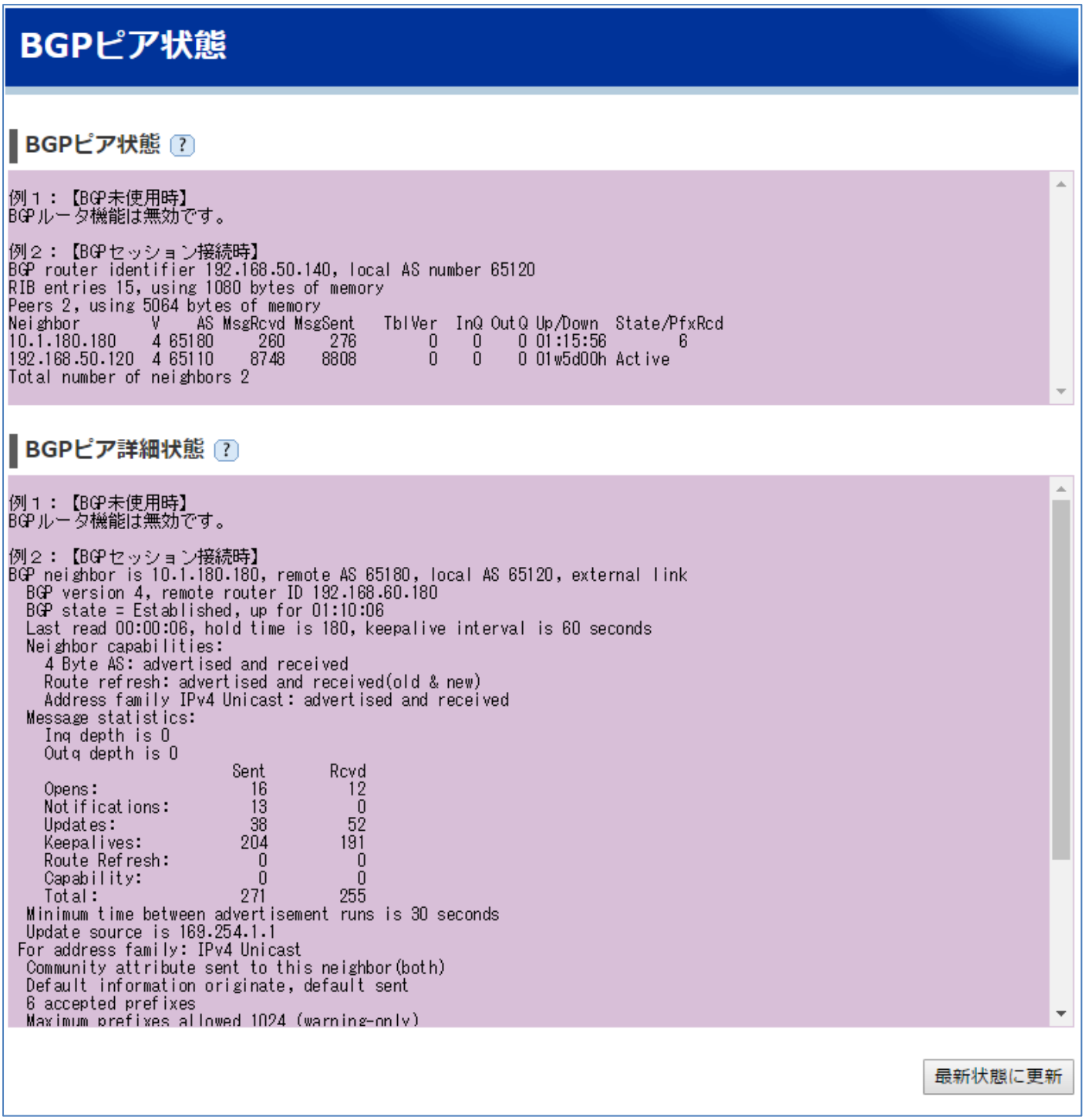
[BGP ルーティングテーブルの見かた]

項目	表示値	内容
左端の*などの記号	*	BGP テーブル上で有効なルート
	d	該当ルートの up/down が激しく、抑制されている状態
	r	RIB-Failure によりルーティングテーブルにインストールされていない状態
	s	aggregate-address コマンドの summary-only オプションで抑制されている状態
	>	ベストパスとして選択されたルート
	i	ベストパス（>）右側に「 i 」と表示する場合、そのルートは iBGP ルート, ベストパス（>）右側に、何も表示されない場合、そのルートは eBGP ルート, Next Hop が「0.0.0.0」とある場合はルートローカルで生成されたルート
Network	10.1.0.0/16	宛先ネットワークのプレフィックス/マスク長
Next Hop	10.1.180.180	ネクストホップの IP アドレス
Metric	0	MED アトリビュート デフォルト値は 0。隣接する AS 内でのみ有効な値です。
LocPrf		LOCAL_PREFERENCE アトリビュート デフォルト値は 100。eBGP ルートの場合は空欄で表示されます。
Weight	32768	WEIGHT アトリビュート デフォルト値は 32768。AS 内のローカルルート以外は 0 と表示されます。
Path	65180 ?	AS_PATH アトリビュート AS 番号がない場合、そのルートは AS 内のルートであることを意味します。右端から順に経由した AS 番号が表示されます。「i」は ORIGIN アトリビュートの IGP、「?」は Incomplete。

6.1.5. **BGP ピア状態**

本製品の BGP ピア状態を設定 Web で確認できます。本情報はルータモードのときのみ表示されます。

1. [TOP]-[メンテナンス]-[情報]-[BGP ピア状態]画面を開きます。



「最新情報に更新」ボタンを押下すると、表示画面を最新の情報に更新します。

[BGP ピア状態の見かた]

BGP 接続の状態と各 neighbor との接続状態を要約して表示します。

項目	表示値	内容
BGP router identifier	192.168.50.140	本製品の BGP ルータ ID
local AS number	65120	本製品の AS 番号
RIB entries	15	ルーティングテーブルのエントリ数

Neighbor	10.1.180.180	BGP ネイバーの IP アドレス
V	4	BGP のバージョン
AS	65180	BGP ネイバーの AS 番号
MsgRcvd	260	受信した BGP メッセージの数
MsgSent	276	送信した BGP メッセージの数
TblVer	0	送信した BGP テーブルの最新バージョン
InQ	0	未処理の受信した BGP メッセージの数
OutQ	0	未送信の BGP メッセージの数
Up/Down	01:15:56	BGP セッションが確立されてからの経過時間
State/PfxRcd	6	BGP セッションが確立するまでは BGP ステートを表示。確立後は BGP ネイバーから受信した経路数を表示。
Total number of neighbors	2	BGP ネイバーの数。BGP セッション未確立のネイバーも含みます。

[BGP ピア詳細状態の見かた]

BGP 接続の状態と各 neighbor との接続状態を要約して表示します。

項目	表示値	内容
BGP neighbor	10.1.180.180	ネイバーの IP アドレスを表示します。
remote AS	65180	ネイバーの AS 番号を表示します。
local AS	65120	自身の AS 番号を表示します。
internal link/ external link	external link	リンクの状態（internal or external）を表示します。
BGP version	4	BGP のバージョンを表示します。
remote router ID	192.168.60.180	ネイバーのルータ ID を表示します。
BGP state	Established	BGP の状態を表示します。
up for	01:10:06	セッションが有効になってからの経過時間（時:分:秒）
Last read	00:00:06	このネイバーから最後にメッセージを読んだ時間（時:分:秒）
hold time	180	セッションを維持する時間を表示します。
keepalive interval	60 seconds	keepalive を送信する間隔を表示します。
Neighbor capabilities	4 Byte AS: advertised and received Route refresh: advertised and received(old & new) Address family IPv4 Unicast: advertised and received	ネイバーの能力
Message statistics	Inq depth is 0	メッセージの統計情報

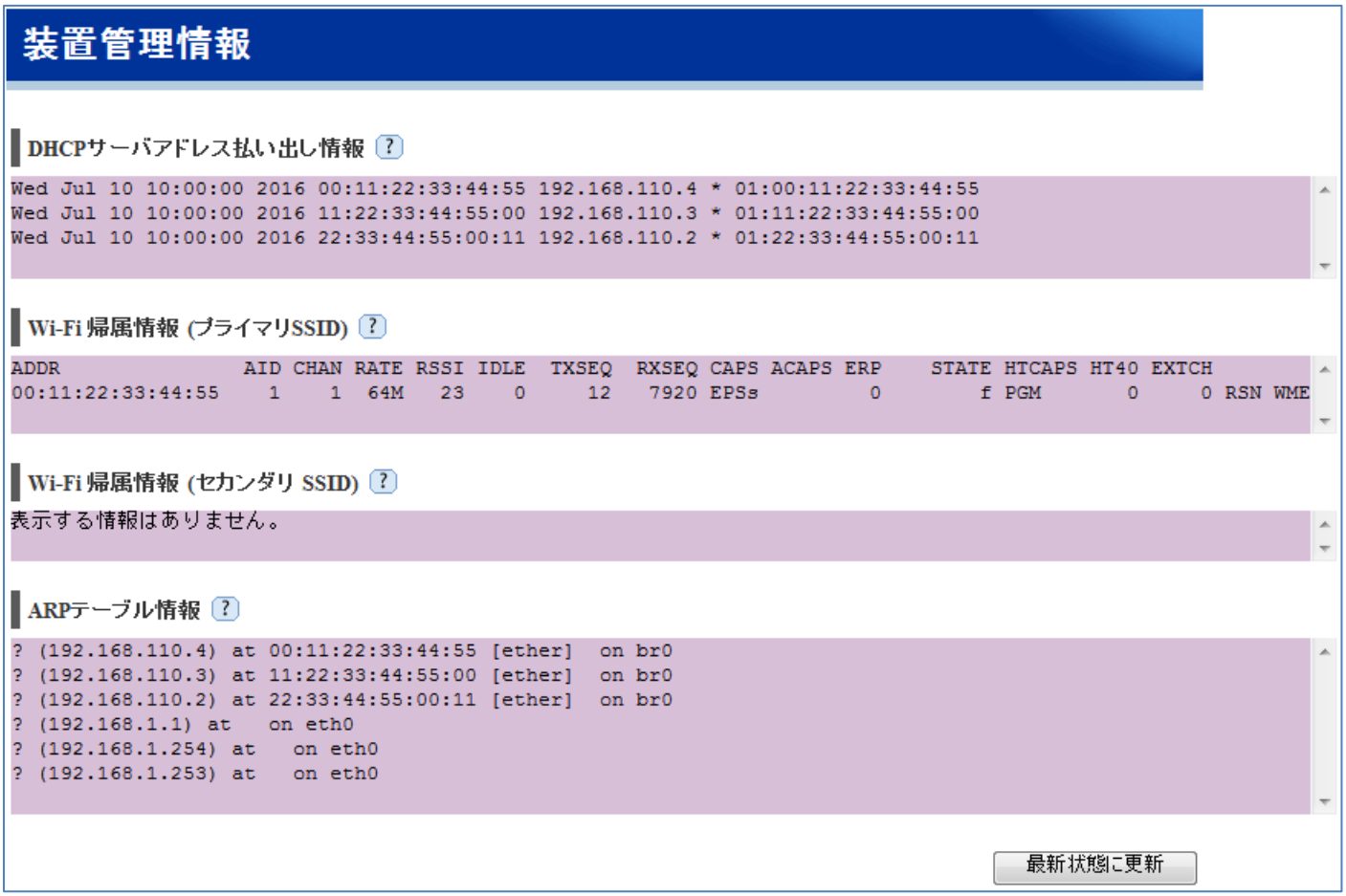
	Outq depth is 0 Sent Rcvd Opens: 16 12 Notifications: 13 0 Updates: 38 52 Keepalives: 204 191 Route Refresh: 0 0 Capability: 0 0 Total: 271 255 Minimum time between advertisement runs is 30 seconds Update source is 169.254.1.1	
For address family	IPv4 Unicast Community attribute sent to this neighbor(both) Default Information originate, default sent 6 accepted prefixes Maximum prefixes allowed 1024 (warning-only) Threshold for warning message 100% Connections established 13; dropped 12 Last reset 01:10:18, due to User reset	アドレスファミリの説明
Local host	10.1.1.1	ローカルホストの IP アドレス
Local port	49909	ローカルホストのポート番号
Foreign host	10.1.180.180	外部ホストの IP アドレス
Foreign port	179	外部ホストのポート番号
Nexthop	10.1.1.1	ネクストホップアドレス
Nexthop global	fe80::20c:29ff:fe0f:6b62	ネクストホップの IPv6 グローバルアドレス
Nexthop local	::	ネクストホップの IPv6 リンクローカルアドレス
BGP connection	non shared network	BGP コネクションの種類
Read thread	on	Read thread の状態
Write thread	off	Write thread の状態

6.1.6. DHCP サーバアドレス払い出し情報、Wi-Fi 帰属情報、ARP テーブル情報

本製品の DHCP サーバアドレス払い出し情報、Wi-Fi 帰属情報、ARP テーブル情報を設定 Web で確認できます。

DHCP サーバアドレス払い出し情報はルータモードのときに表示されます。

1.[TOP]-[メンテナンス]-[情報]-[装置管理情報]画面を開きます。



■装置管理情報

項目		説明
DHCP サーバアドレス払い出し情報[22]（ルータモードのときに表示）		本製品が DHCP サーバとして、アドレスを払い出した情報を確認できます。 1 件の IP アドレス払い出し情報が一行ごとに表示されます。 以下、表示内容の左側から項目の内容を説明します。
	リース満了時刻	本製品が払い出した IP アドレスのリース期間が満了する時刻です。
	クライアントの MAC アドレス	IP アドレスが払い出されたクライアントの MAC アドレスです。
	払い出した IP アドレス	クライアントに払い出した IP アドレスです。
	クライアントのホスト名	クライアントのホスト名です。
	クライアント ID	クライアントのクライアント ID です。
Wi-Fi 帰属情報(プライマリ SSID)		プライマリ SSID に帰属した無線 LAN 端末情報を確認できます。
	ADDR	無線 LAN 端末の MAC アドレスです。
	AID	無線 LAN 端末に割り当てられた帰属 ID です。
	CHAN	制御チャネルです。

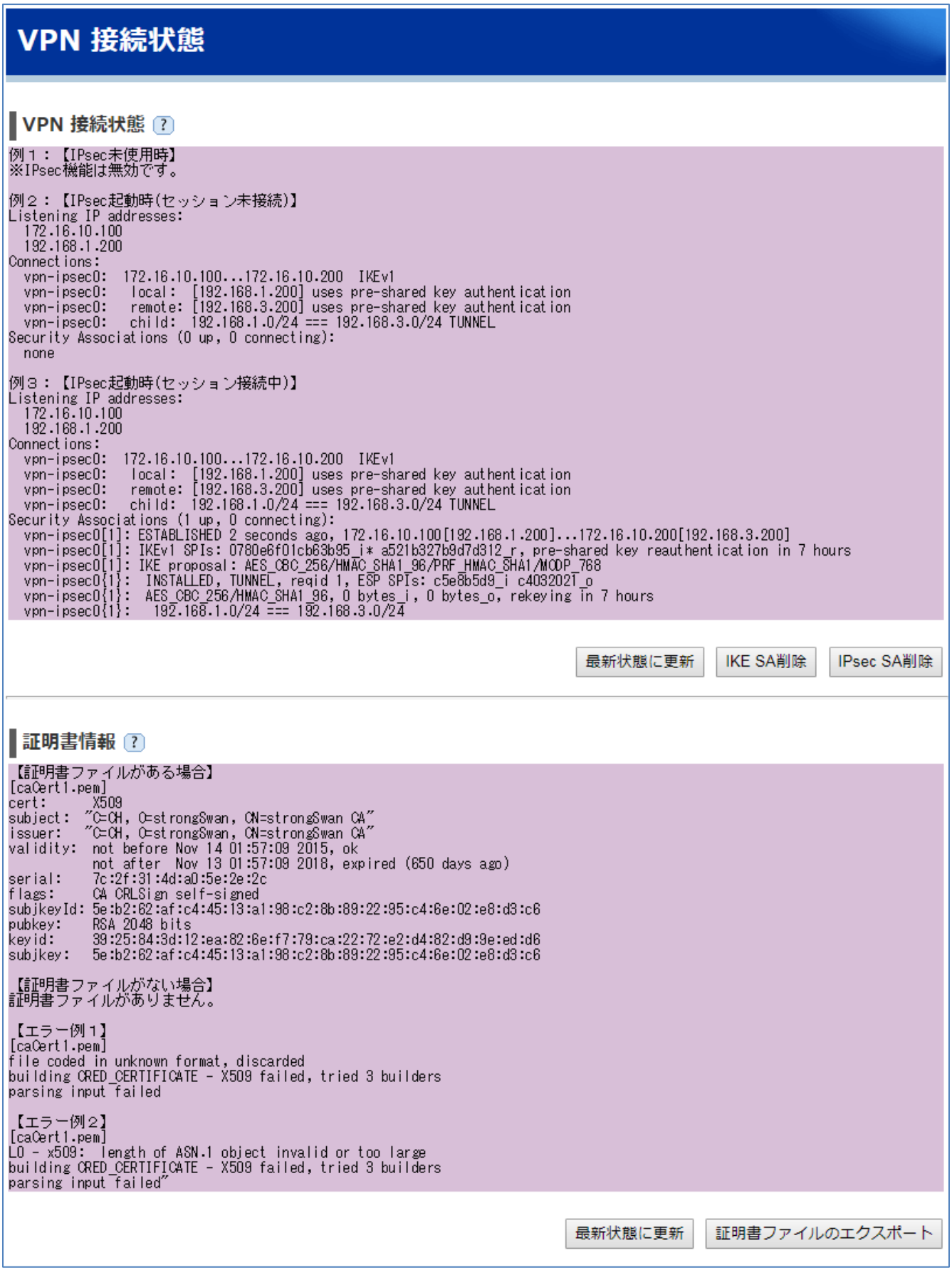
[22] 装置起動直後は正しく表示されない場合があります。

	RATE	通信レートです。
	RSSI	受信信号強度です。
	IDLE	無線 LAN 端末のアイドルタイム（15 秒単位）です。
	TXSEQ	TID0(BestEffort)の無線 LAN 端末への送信パケットシーケンスナンバーです。
	RXSEQ	TID0(BestEffort)の無線 LAN 端末からの受信パケットシーケンスナンバーです。
	CAPS	CAPS Capability Information です。
	ACAPS	情報非公開
	ERP	ERP Information です。
	STATE	無線 LAN 端末のステータスです。
	HTCAPS	HT Capabilities です。
	HT40	チャネルの接続状況です。 0:シングルチャネル、1:デュアルチャネル
	EXTCH	拡張チャネルの使用状況です。 0:拡張チャネルの使用なし -1: 拡張チャネルは制御チャネルより 4 チャネル下 1: 拡張チャネルは制御チャネルより 4 チャネル上
Wi-Fi 帰属情報(セカンダリ SSID)		セカンダリ SSID に帰属した無線 LAN 端末情報を確認できます。 詳細は Wi-Fi 帰属情報(プライマリ SSID)の説明を参照してください。
ARP テーブル情報		本製品の ARP テーブル情報を確認できます。 1 件のエントリ情報が一行ごとに表示されます。 以下、表示内容の左側から項目の内容を説明します。
	ホスト名、IP アドレス	ホスト名、IP アドレスが表示されます。 ホスト名が不明のときは、?と表示されます。
	MAC アドレス[HW タイプ]	エントリの MAC アドレス、ハードウェアタイプです。
	インタフェース	エントリが接続されているインタフェースです。

6.1.7. **IPsec SA 情報**

IPsec トンネルの状態を設定 Web で確認できます。本情報はルータモードのときのみ表示されます。

1. [TOP]-[メンテナンス]-[情報]-[VPN 接続状態]画面を開きます。



「最新情報に更新」ボタンを押下すると、表示画面を最新の情報に更新します。

[SA 情報の読み方]

項目	表示値	内容
Listening IP address	172.168.10.100	自装置対向装置の WAN 側 IP アドレス
	192.168.1.200	自装置の LAN 側 IP アドレス
	169.254.254.11	自装置の LINKLOCAL アドレス
Connections	vpn-ipsec： 0%any...172.16.20.200 IKEv1	自装置と対向装置 WAN（IP アドレス）を IKEv1 メインモードで設定していることを示します。アグレッシブモードのときは“IKEv1 Aggressive“と表示します。
	vpn-ipsec0: local: [172.16.10.100] uses pre-shared key authentication vpn-ipsec0: remote: [172.16.20.200] uses pre-shared key authentication	IKE フェーズ 1 のローカル ID/リモート ID 設定と事前共有鍵方式であることを示します。
	vpn-ipsec0: child: 192.168.1.0/24 === 192.168.3.0/24 TUNNEL	IKE フェーズ 2 のローカル ID/リモート ID 設定を示します。
Security Associations (1up,0connecting)	vpn-ipsec0[1]: ESTABLISHED 6 seconds ago, 172.16.10.100[172.16.10.100]...172.16.20.200[172.16.20.200] vpn-ipsec0[1]: IKEv1 SPIs: c2a243c70373cf6f_i* b53e19843e16ad53_r, pre-shared key reauthentication in 6 hours vpn-ipsec0[1]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_768	IKE SA 情報です。接続している WAN の IP アドレスと IKE フェーズ 1 のローカル ID/リモート ID を示します。SPI と IKE のリキー残り時間を示します。Proposal 情報を示します。
	vpn-ipsec0{2}: INSTALLED, TUNNEL, reqid 1, ESP SPIs: ccf8ac1a_i c156e9c2_o vpn-ipsec0{2}: AES_CBC_256/HMAC_SHA1_96, 0 bytes_i, 0 bytes_o, rekeying in 5 hours vpn-ipsec0{2}: 192.168.1.0/24 === 192.168.3.0/24	IPsec SA 情報です。SPI を示します。Proposal 情報と ESP の送受信パケット数。リキー残り時間を示します。

[証明書情報の読み方]

項目	内容
cert	証明書の形式を示します。
subject	証明する対象を示します。
issuer	証明書の発行者を示します。
validity	有効期限を示します。 本装置では時刻取得できなかった場合を考慮し、開始時刻のチェックはしません。
serial	シリアル番号を示します。
flags	CRL に関するフラグを示します。
subjkeyId	公開鍵の ID を示します。
pubkey	公開鍵長を示します。
keyid	keyid を示します。
subjkey	公開鍵を示します。

6.1.8. **IPsec トンネルを通過するトラフィックの統計情報**

IPsec トラフィックの統計情報を設定 Web で確認できます。本情報はルータモードのときのみ表示されます。

1. [TOP]-[メンテナンス]-[情報]-[VPN 統計情報]画面を開きます。

「最新情報に更新」ボタンを押下することで、表示画面を最新の情報に更新します。

「統計情報クリア」ボタンを押下すると、各種統計情報のカウンタを 0 クリアします。

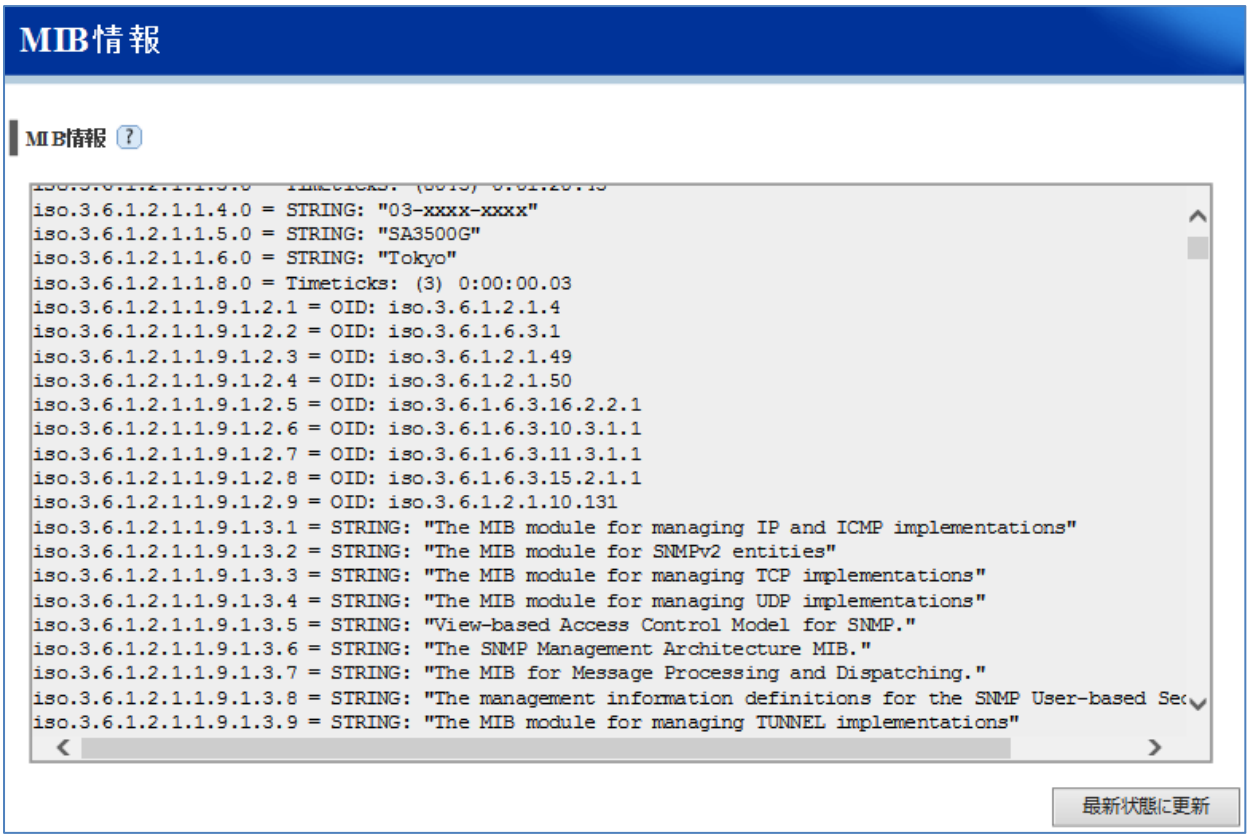
[統計情報の読み方]

項目	説明
ikeInitRekey	IKE SA リキー始動カウンタ
ikeRspRekey	IKE SA リキー応答カウンタ
ikeChildSaRekey	IPsec SA リキー成功カウンタ
ikeInInvalid	無効メッセージ受信カウンタ
ikeInInvalidSpi	無効 ID、SPI 受信カウンタ
ikeInInitReq	IKE SA 初期化要求受信カウンタ
ikeInInitRsp	IKE SA 初期化応答受信カウンタ
ikeOutInitReq	IKE SA 初期化要求送信カウンタ
ikeOutInitRsp	IKE SA 初期化応答送信カウンタ
ikeInAuthReq	IKE 認証要求受信カウンタ
ikeInAuthRsp	IKE 認証応答受信カウンタ
ikeOutAuthReq	IKE 認証要求送信カウンタ
ikeOutAuthRsp	IKE 認証応答送信カウンタ
ikeInCrChildReq	IPsec SA 作成要求受信カウンタ
ikeInCrChildRsp	IPsec SA 作成応答受信カウンタ
ikeOutCrChildReq	IPsec SA 作成要求送信カウンタ
ikeInInvalidSpi	無効 ID、SPI 受信カウンタ
ikeInInitReq	IKE SA 初期化要求受信カウンタ
ikeInInitRsp	IKE SA 初期化応答受信カウンタ
ikeOutCrChildRsp	IPsecSA 作成応答送信カウンタ
ikeInInfoReq	INFORMATIONAL 要求受信カウンタ
ikeInInfoRsp	INFORMATIONAL 応答受信カウンタ
ikeOutInfoReq	INFORMATIONAL 要求送信カウンタ
ikeOutInfoRsp	INFORMATIONAL 応答送信カウンタ

6.1.9. **SNMP MIB 情報**

SNMP MIB の情報を設定 Web で確認できます。

1. [TOP]-[メンテナンス]-[情報]-[MIB 情報]画面を開きます。



「最新情報に更新」ボタンの押下で、表示画面を最新の情報に更新します。

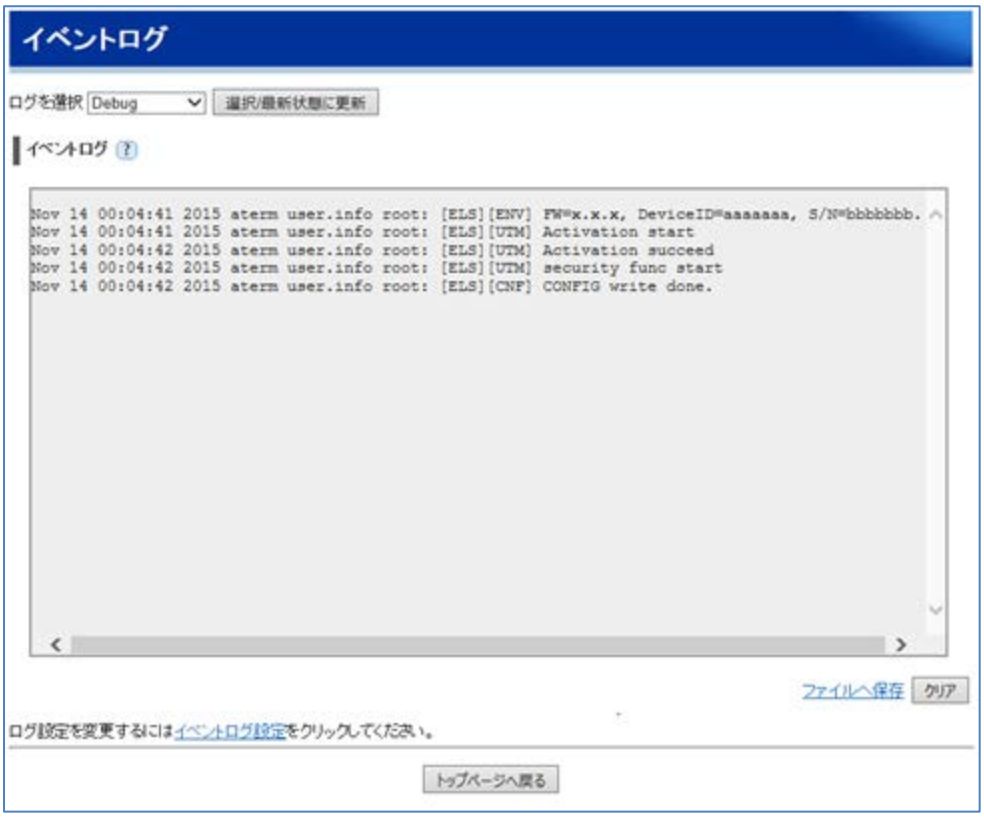
表示している MIB のうち、SNMP 統計情報は、iso.3.6.1.2.1.11.1.0　～　iso.3.6.1.2.1.11.32.0 が該当します。
SNMP 統計情報の各 MIB の内容は次ページ表のとおりです。
（表中では、iso.3.6.1.2.1.11.1.0 の OID は、1.3.6.1.2.1.11.1 と記しています）

OID	オブジェクト名	内容
1.3.6.1.2.1.11.1	snmpInPkts	受信した SNMP メッセージの総数
1.3.6.1.2.1.11.2	OutPkts	送信した SNMP メッセージの総数
1.3.6.1.2.1.11.3	InBadVersions	未サポートバージョンの SNMP メッセージが届いた総数
1.3.6.1.2.1.11.4	InBadCommunityNames	コミュニティ名が不正な SNMP メッセージの総数
1.3.6.1.2.1.11.5	InBadCommunityUses	Community に許可されていないオペレーションが指定された SNMP メッセージの総数
1.3.6.1.2.1.11.6	InASNParseErrs	OID の形式が間違っていた SNMP メッセージの総数
1.3.6.1.2.1.11.8	InTooBigs	「tooBig」エラーがあった受信 SNMP メッセージの総数
1.3.6.1.2.1.11.9	InNoSuchNames	「noSuchName」エラーがあった受信 SNMP メッセージの総数
1.3.6.1.2.1.11.10	InBadValues	「badValue」エラーがあった SNMP 受信メッセージの総数
1.3.6.1.2.1.11.11	InReadOnlys	「readOnly」エラーがあった SNMP 受信メッセージの総数
1.3.6.1.2.1.11.12	InGenErrs	「getErr」があった受信 SNMP メッセージの総数
1.3.6.1.2.1.11.13	InTotalReqVars	正常に読みだされた MIB オブジェクトの総数
1.3.6.1.2.1.11.14	InTotalSetVars	正常に変更された MIB オブジェクトの総数
1.3.6.1.2.1.11.15	InGetRequests	受信した Get-Request の総数
1.3.6.1.2.1.11.16	InGetNexts	受信した Get-Next の総数
1.3.6.1.2.1.11.17	InSetRequests	受信した Set-Request の総数
1.3.6.1.2.1.11.18	InGetResponses	受信した Get-Response の総数
1.3.6.1.2.1.11.19	InTraps	受信した Trap の総数
1.3.6.1.2.1.11.20	OutTooBigs	「tooBig」エラーがあった送信 SNMP メッセージの総数
1.3.6.1.2.1.11.21	OutNoSuchNames	「noSuchName」エラーがあった送信 SNMP メッセージの総数
1.3.6.1.2.1.11.22	OutBadValues	「badValue」エラーがあった送信 SNMP メッセージの総数
1.3.6.1.2.1.11.24	OutGenErrs	「getErr」があった送信 SNMP メッセージの総数
1.3.6.1.2.1.11.25	OutGetRequests	送信した Get-Request の総数
1.3.6.1.2.1.11.26	OutGetNexts	送信した Get-Next の総数
1.3.6.1.2.1.11.27	OutSetRequests	送信した Set-Request の総数
1.3.6.1.2.1.11.28	OutGetResponses	送信した GetResponse の総数
1.3.6.1.2.1.11.29	OutTraps	送信した Trap の総数
1.3.6.1.2.1.11.30	EnableAuthenTraps	認証失敗 Trap 発生の制御。1：TRAP を発生　2：TRAP を発生しない
1.3.6.1.2.1.11.31	SilentDrops	空の変数ブリッジ・フィールドがある代替 Response-PDU を含む応答のサイズが、 ローカル側の制約または要求の発信元に関連した最大メッセージ・サイズを超えているために通知もなく除去された、GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の総数
1.3.6.1.2.1.11.32	ProxyDrops	通知もなく除去された GetRequest-PDU、GetNextRequest-PDU、GetBulkRequest-PDU、SetRequest-PDU、および InformRequest-PDU の総数

※ SNMP の統計情報はクリアできません。

6.1.10. **イベントログ**

イベントログを設定 Web で確認できます。



1. [TOP]-[メンテナンス]-[情報]-[イベントログ]画面を開きます。
2. イベントログを表示するレベルを「ログを選択」から選択します。
3. 「選択/最新状態に更新」ボタンを押下します。

[イベントログのパソコンなどへの保存]

「ファイルへ保存」をクリックすると、パソコンなどにイベントログを保存できます。

設定項目	値	備考	初期値
ログを選択	Emergency … 緊急 Alert … 警戒 Critical … 危機的 Error … エラー Warning … 警告 Notice … 通知 Informational … 情報提供 Debug … デバッグ イベント量：小 ↓ イベント量：大	イベントログを表示するレベルを選択します。 Log Level で変更できるレベルは左記のとおりです。イベントログのレベルはイベントの重要度や緊急度にあわせて変更できます。 例えば、Emergency レベルに設定した場合、Emergency レベルに該当するイベントのみ表示しますが、 Informational レベルに設定すると上位全てのイベントを表示することができます。	Emergency

[メモ]

「イベントログ設定」をクリックすると、[イベントログ設定]画面が開いて、イベントログを保存するレベルを変更できます。

1. [TOP]-[メンテナンス]-[情報]-[イベントログ]-[イベントログ設定]画面を開きます。
2. イベントログを保存するレベルを「Log Level」から選択します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
イベントログ機能	• チェック有…イベントログ機能を使用する場合 • チェック無…イベントログ機能を使用しない場合		有効
Log Level	Emergency … 緊急 Alert … 警戒 Critical … 危機的 Error … エラー Warning … 警告 Notice … 通知 Informational … 情報提供 Debug … デバッグ イベント量：小 ↓ イベント量：大	イベントログを保存するレベルを設定します。	Informational

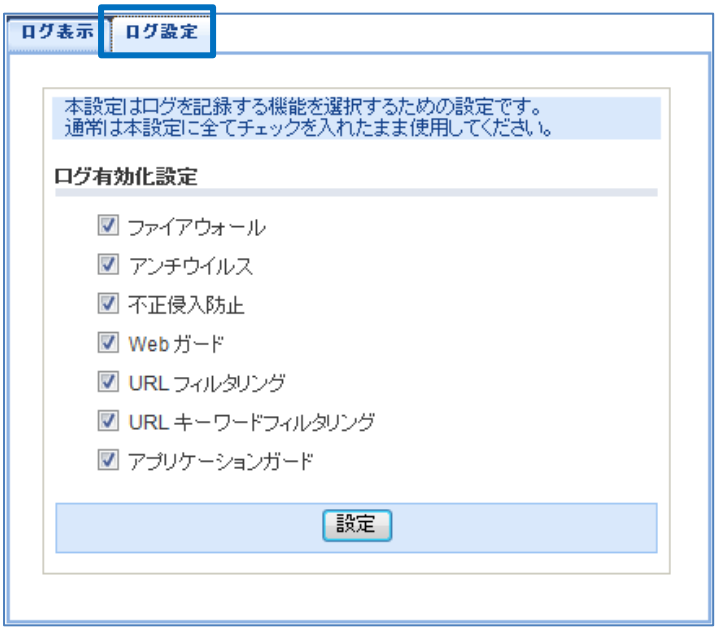
6.1.11. **セキュリティログ**

異常トラフィックが生じていないかなど定期的に確認してください。

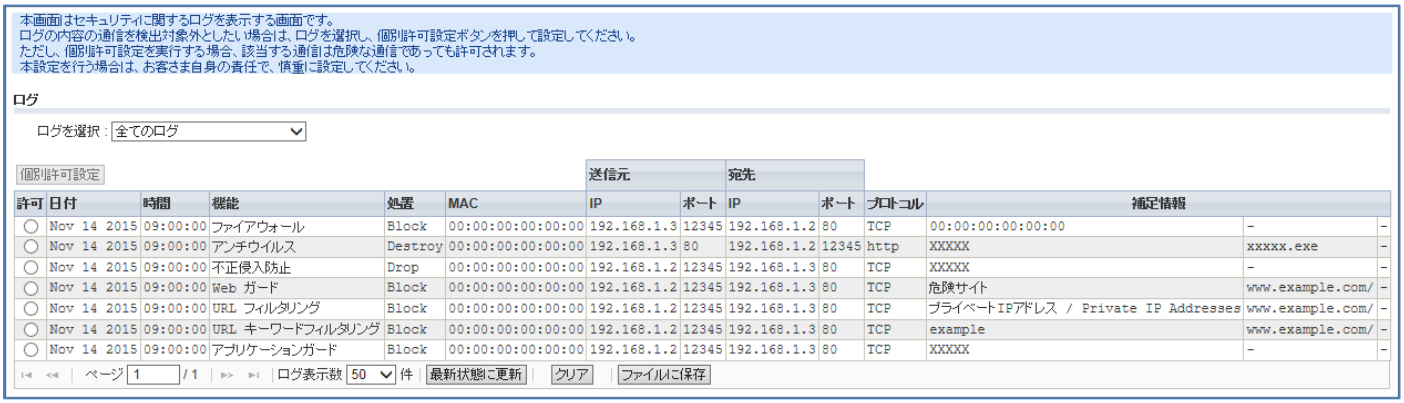
本製品のセキュリティ・スキャン機能の動作状況を設定 Web で確認できます。

タブ	説明
ログ表示	セキュリティ・スキャン機能のセキュリティログを表示します。 ブロックされた通信を検出対象外にしたい場合は、当画面から個別許可設定してください。
ログ設定	セキュリティ・スキャン機能の機能ごとにセキュリティログの表示有無を設定します。 セキュリティログへ出力をさせる機能にチェックを入れてください。

■ログ設定



■ログ表示



1. [TOP]-[セキュリティ]-[セキュリティログ]画面を開きます。
2. 「ログ設定」タブをクリックし、有効化する機能をチェックし、「設定」ボタンを押下します。
3. 「ログ表示」タブをクリックし、セキュリティログを確認し、検出された脅威の種類や脅威の対象となった端末をご確認ください。

[メモ]

「ログ設定」タブでログ機能を無効に設定すると、それまで出力していたセキュリティログを表示しません。

また、その後有効にしても、その間のセキュリティログを表示しません。

[ログメッセージのパソコンなどへの保存]

「ファイルに保存」ボタンを押下すると、パソコンなどにセキュリティログを保存できます。

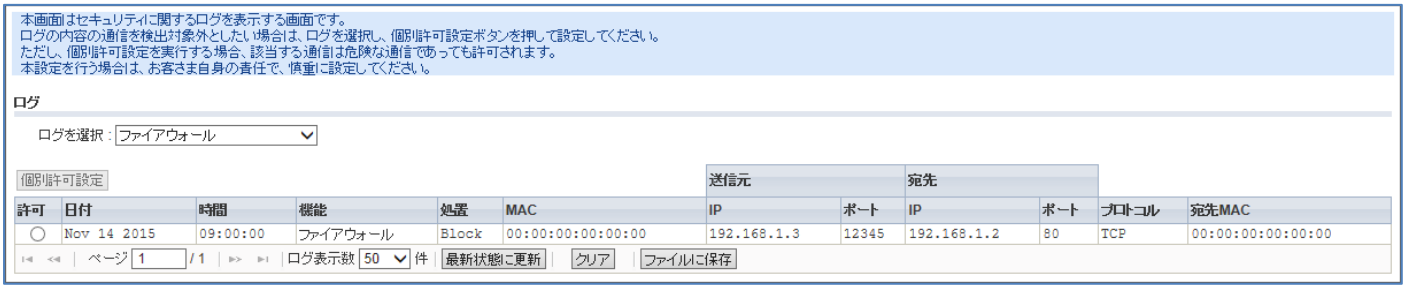
[個別許可]

セキュリティ・スキャン機能でブロックした通信を検出対象外にする場合は、該当のセキュリティログを選択し、個別許可ボタンをクリックしてください。

ただし、個別許可設定を実行する場合、該当する通信は危険な通信であっても許可されます。

本設定を行う場合は、お客様自身の責任で、慎重に設定してください。

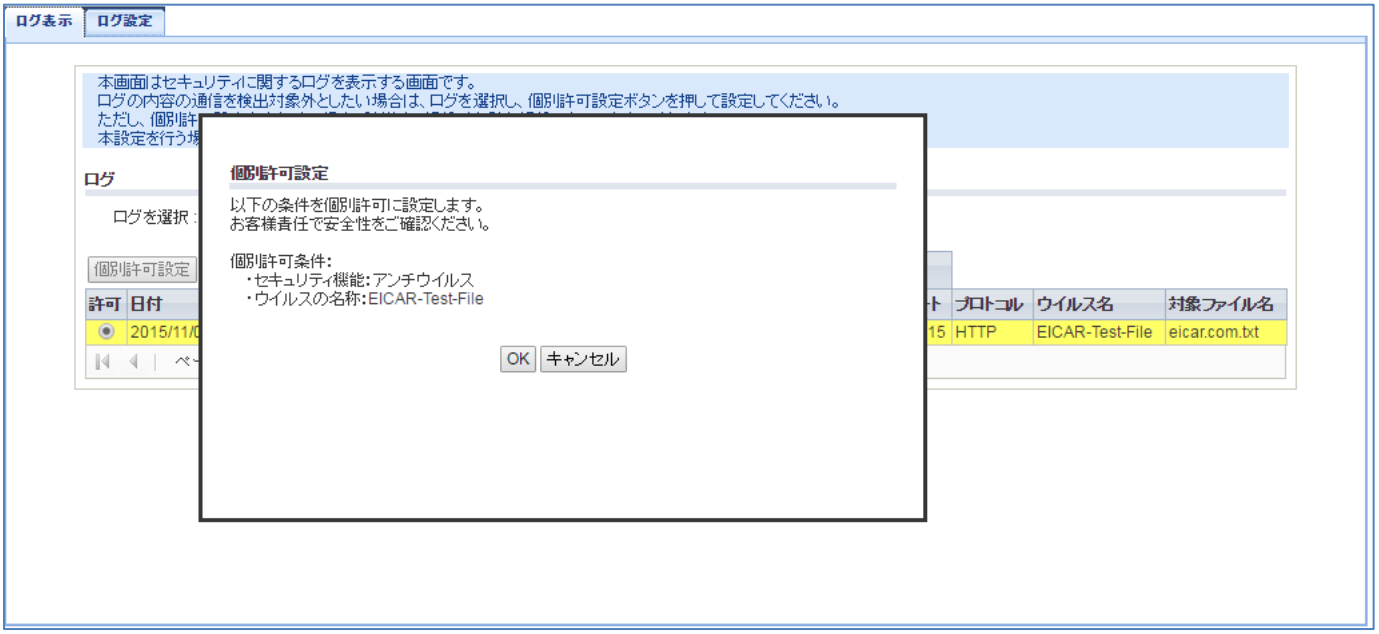
- ファイアウォール（FW）



- アンチウイルス（AV）

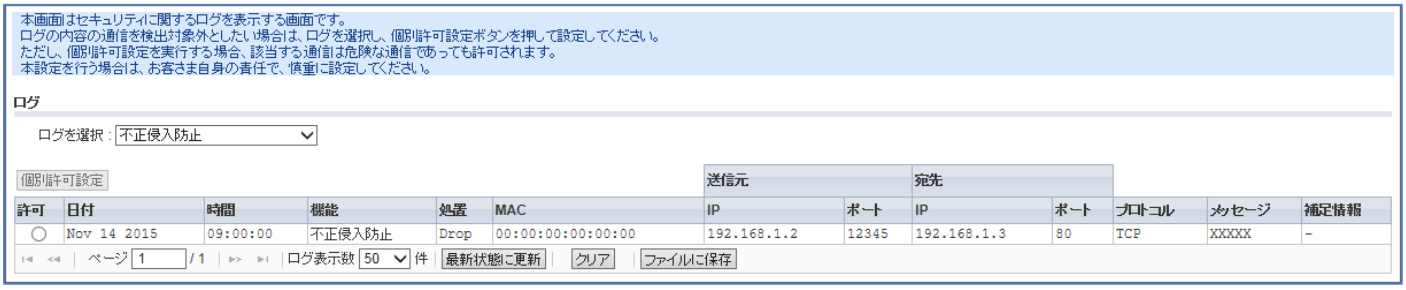
※メール送受信でのウイルス検出時に、メールの表題と日付をログに出力します。該当するメールの添付ファイルを無害化したことを示します。添付ファイルの送信元と送信内容をご確認いただく際にご利用ください。

リストから個別許可を設定する場合は、該当リストを選択し、「個別許可設定」ボタンを押下します。以下の画面がポップアップで表示されます。内容を確認の上、「OK」もしくは「キャンセル」ボタンを押下してください。「OK」を押下すると個別許可設定に反映されます。他のセキュリティ・スキャン機能でも個別許可設定の方法は同じです。

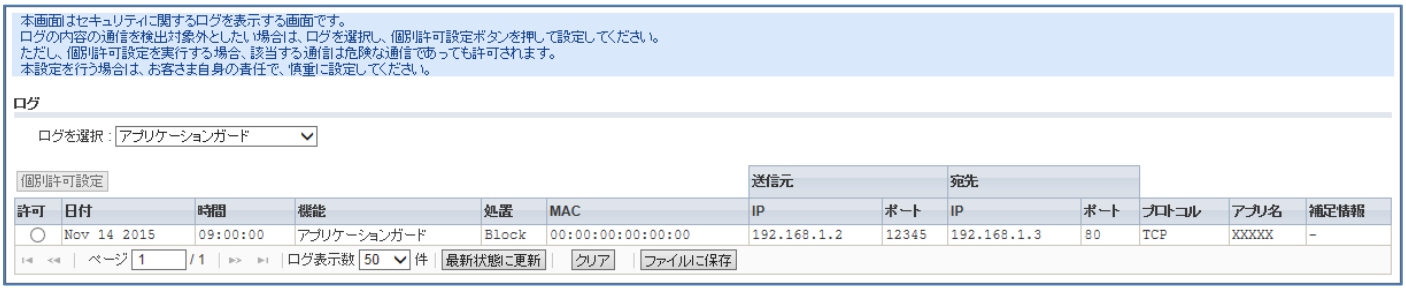


1. セキュリティログから個別許可する項目を選択し、「個別許可設定」ボタンを押下します。
2. Web ガードおよび URL フィルタリングの場合は個別許可設定ダイアログ上の URL を編集できます。
3. 「OK」ボタンを押下します。

- 不正侵入防止（IPS）



- アプリケーションガード（APG）

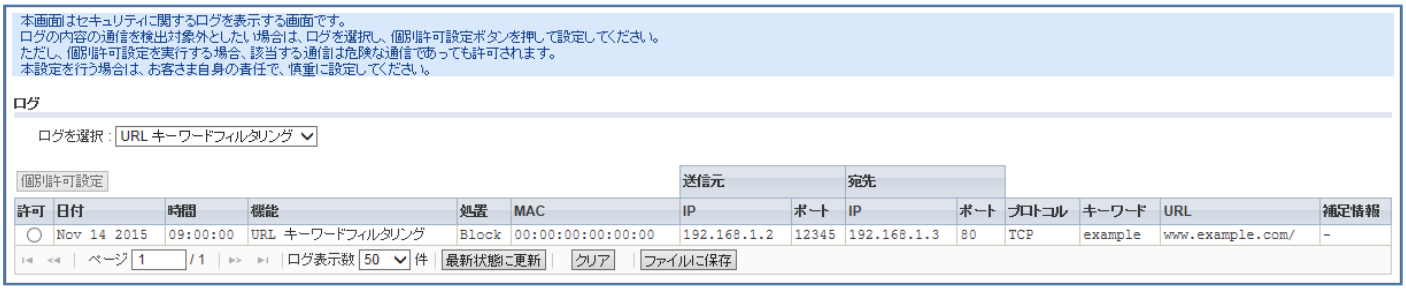


- Web ガード（WG）

※HTTP アクセスをブロックしたときに、セキュリティログに HTTP の“X-Forwarded-For”ヘッダー情報を出力します。プロキシサーバ経由で該当ページにアクセスした場合に、アクセス元を確認する際にご利用ください。

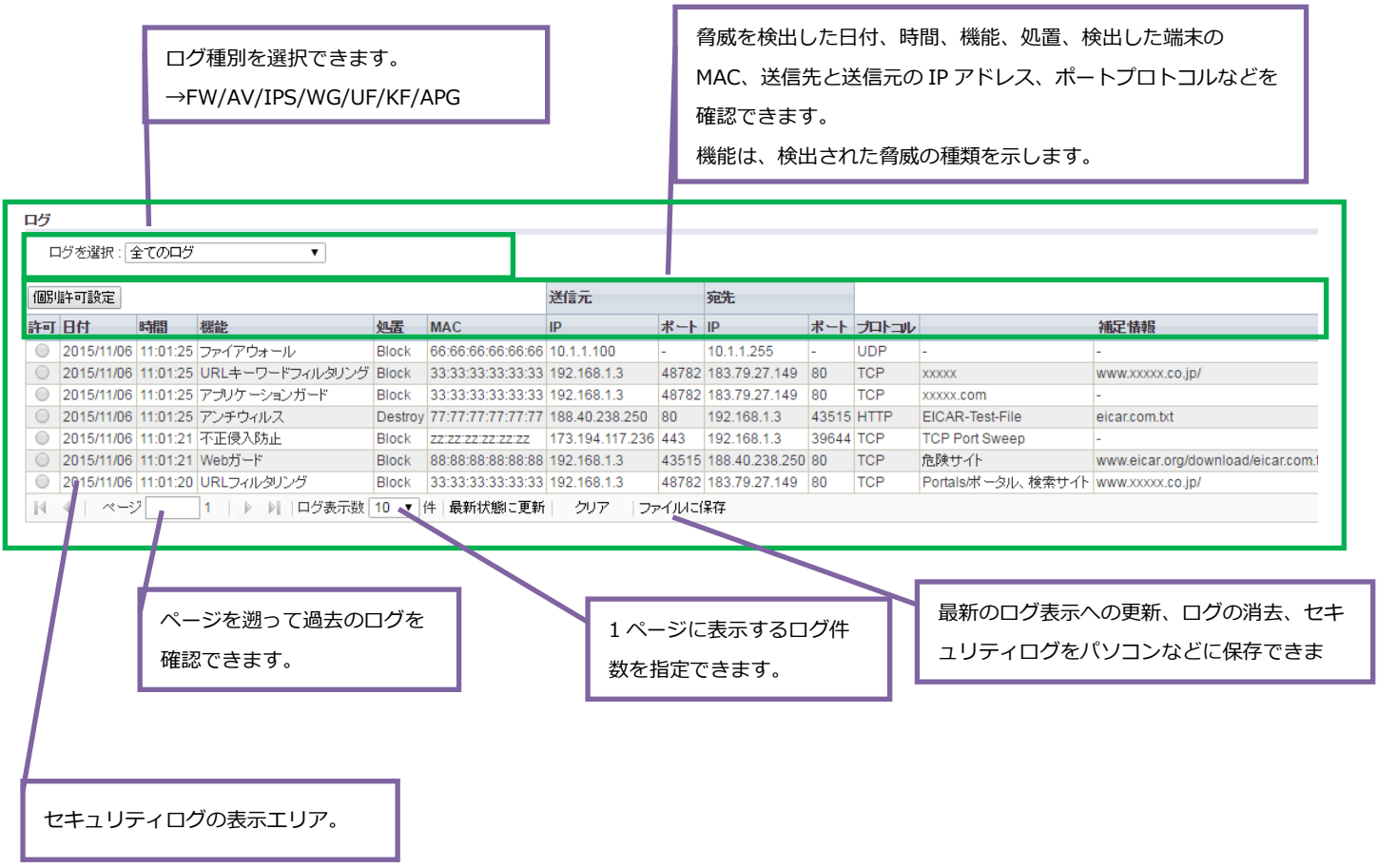
- URL フィルタリング（UF）

- URL キーワードフィルタリング（KF）



[ログ表示画面の説明]

ログ表示画面の構成について説明します。



6.1.12. 統計情報

異常トラフィックが生じていないかなど定期的に確認してください。

本製品のセキュリティ・スキャン機能の統計情報を設定 Web で確認できます。

端末ごとの統計情報やブロック数のグラフを確認することもできます。設定方法は 5.9.3 章デバイス管理を参照してください。

なお、本製品のセキュリティ・スキャン機能のライセンスが満了したとき、セキュリティ・スキャン機能が準備中のとき、および、各セキュリティ・スキャン機能の設定を無効にしたときは、統計情報は更新されません。

タブ	説明
日表示	日ごとの統計情報を表示します。
週表示	週ごとの統計情報を表示します。
月表示	月ごとの統計情報を表示します。 月ごとの通信情報を表示します。(UF、APG)
詳細	選択した日の時間ごとの統計情報を表示します。
グラフ	端末ごとのブロック数をグラフで表示します。表示対象の端末は[デバイス管理]画面で設定します。

■日表示

セキュリティ・スキャン機能ごとにブロック数とスキャン数を日ごとに表示します。

■週表示

セキュリティ・スキャン機能ごとにブロック数とスキャン数を週ごとに表示します。

■月表示 統計情報

セキュリティ・スキャン機能ごとにブロック数とスキャン数を月ごとに表示します。

UF と APG については項目名をクリックすると、UF では月ごとのカテゴリ、APG では月ごとのアプリケーションの通信情報を表示することができます。

■月表示 UF カテゴリの通信情報(画面例)

検出数の多いカテゴリ順に並びます。

[UF カテゴリの通信情報]

項目	説明
対象期間	通信情報の対象月を選択できます。 対象月の変更は前後にある矢印ボタンで行います。
No.	検出数の多いカテゴリ順に昇順で番号が与えられます。
カテゴリ	URL フィルタリング機能のカテゴリ名を表示します。 対象月に検知したものだけを表示します。
検出数	選択した「対象期間」中に本製品が通信を検知した総数を表示します。
過去平均	現在から過去 2 ヶ月分の平均数を表示します。 過去情報が 1 ヶ月分しかない場合は、過去 1 か月分の情報が表示されます。「対象期間」を過去月に選択したとしても、「過去平均」の値は変わらず、現在から見た過去平均数が表示されます。
ブロック数	選択した「対象期間」中に本製品がブロックした総数を表示します。

■月表示 アプリケーションの通信情報(画面例)

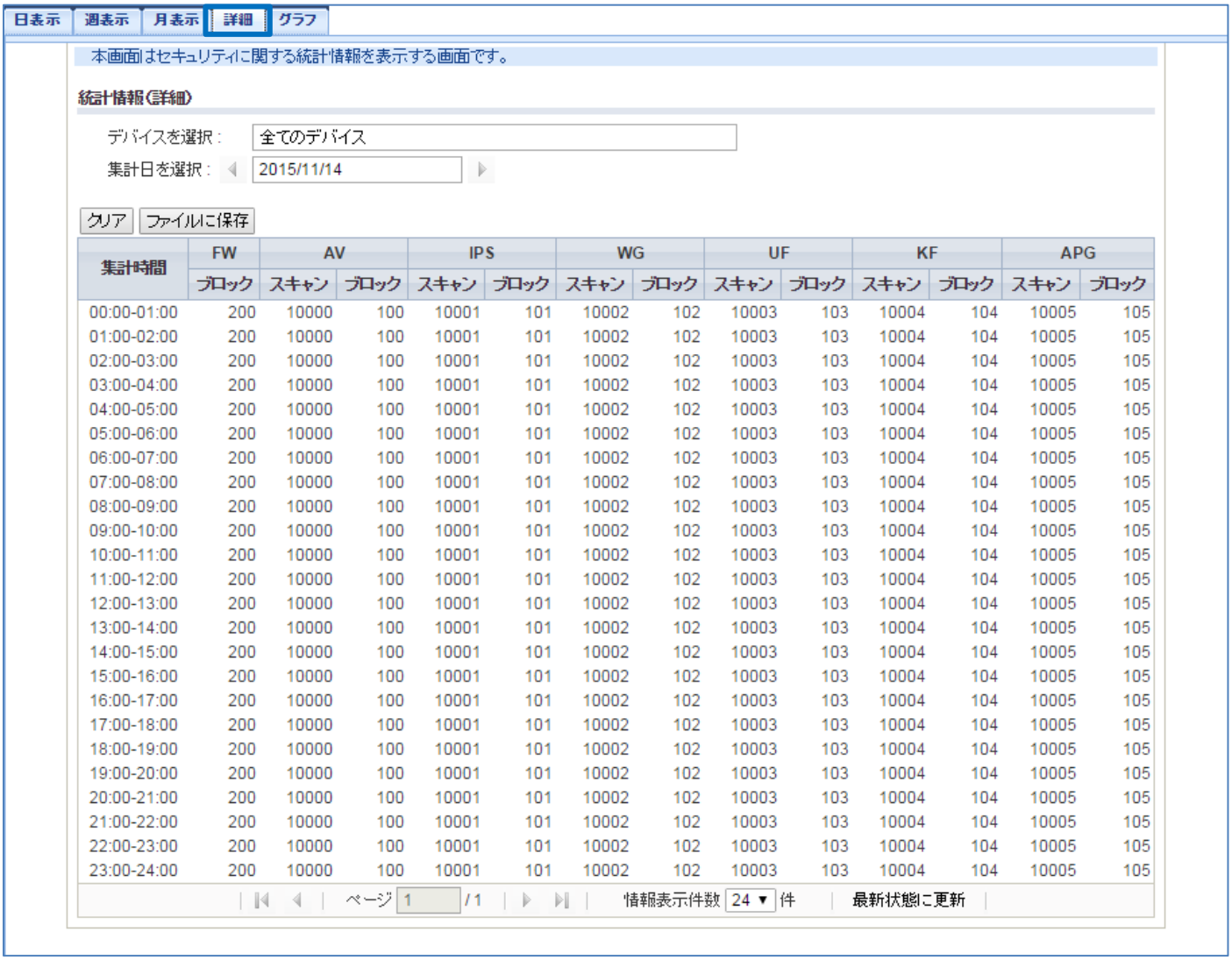
検出数の多いアプリケーション順に並びます。

[月表示 アプリケーションの通信情報]

項目	説明
対象期間	通信情報の対象月を選択できます。 対象月の変更は前後にある矢印ボタンで行います。
No.	検出数の多いアプリケーション順に昇順で番号が与えられます。
アプリケーション名	アプリケーションガード機能のアプリケーション名を表示します。 対象月に検知したものだけを表示します。
検出数	選択した「対象期間」中に本製品が通信を検知した総数を表示します。
過去平均	現在から過去 2 ヶ月分の平均数を表示します。 過去情報が 1 ヶ月分しかない場合は、過去 1 か月分の情報が表示されます。「対象期間」を過去月に選択したとしても、「過去平均」の値は変わらず、現在から見た過去平均数が表示されます。
ブロック数	選択した「対象期間」中に本製品がブロックした総数を表示します。

■詳細

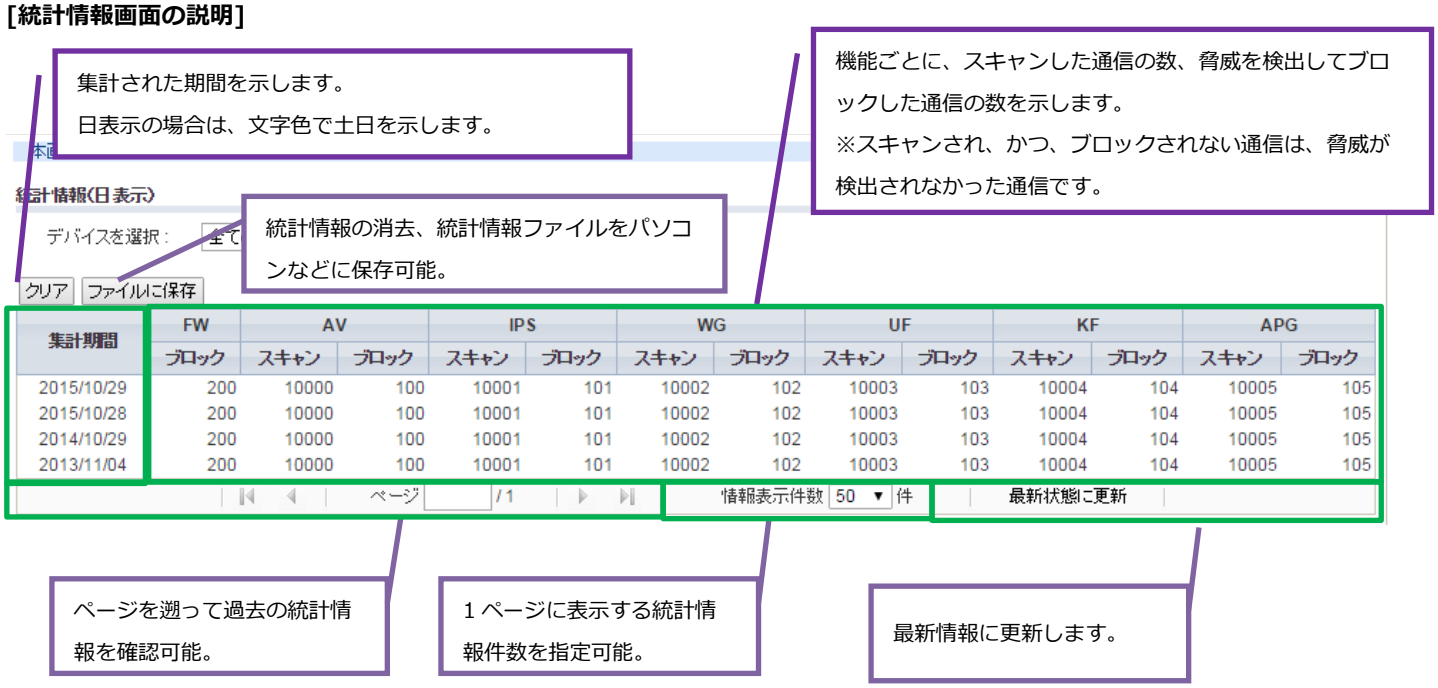
選択した集計日について、セキュリティ・スキャン機能ごとのスキャン数とブロック数を時間ごとに表示します。



集計時間	FW	AV		IPS		WG		UF		KF		APG	
	ブロック	スキャン	ブロック	スキャン	ブロック	スキャン	ブロック	スキャン	ブロック	スキャン	ブロック	スキャン	ブロック
00:00-01:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
01:00-02:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
02:00-03:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
03:00-04:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
04:00-05:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
05:00-06:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
06:00-07:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
07:00-08:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
08:00-09:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
09:00-10:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
10:00-11:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
11:00-12:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
12:00-13:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
13:00-14:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
14:00-15:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
15:00-16:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
16:00-17:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
17:00-18:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
18:00-19:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
19:00-20:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
20:00-21:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
21:00-22:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
22:00-23:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105
23:00-24:00	200	10000	100	10001	101	10002	102	10003	103	10004	104	10005	105

1. [TOP]-[セキュリティ]-[統計情報]画面を開きます。
2. 各項目の説明は以下の統計情報画面の説明を参照してください。

[統計情報画面の説明]



[統計情報]

項目		説明
集計期間		集計された期間を示す。 日表示の場合は、文字色で土日を示します。
FW	ブロック	ファイアウォール機能で遮断したパケット数
AV	スキャン	アンチウイルス機能でスキャンしたファイル数
	ブロック	アンチウイルス機能でウイルスを検出し、書き換えたファイル数
IPS	スキャン	不正侵入防止機能でスキャンしたパケット数
	ブロック	不正侵入防止機能で遮断したパケット数
WG	スキャン	Web ガード機能でスキャンしたトラフィック数（URL 数）
	ブロック	Web ガード機能で遮断したトラフィック数（URL 数）
UF	スキャン	URL フィルタリング機能でスキャンしたトラフィック数（URL 数）
	ブロック	URL フィルタリング機能で遮断したトラフィック数（URL 数）
KF	スキャン	URL キーワードフィルタリング機能でスキャンしたトラフィック数（URL 数）
	ブロック	URL キーワードフィルタリング機能で遮断したトラフィック数（URL 数）
APG	スキャン	アプリケーションガード機能でスキャンしたプロトコル、アプリケーション数
	ブロック	アプリケーションガード機能で遮断したプロトコル、アプリケーション数

[統計情報のパソコンなどへの保存]

「ファイルに保存」ボタンを押下すると、パソコンなどに統計情報を保存できます。

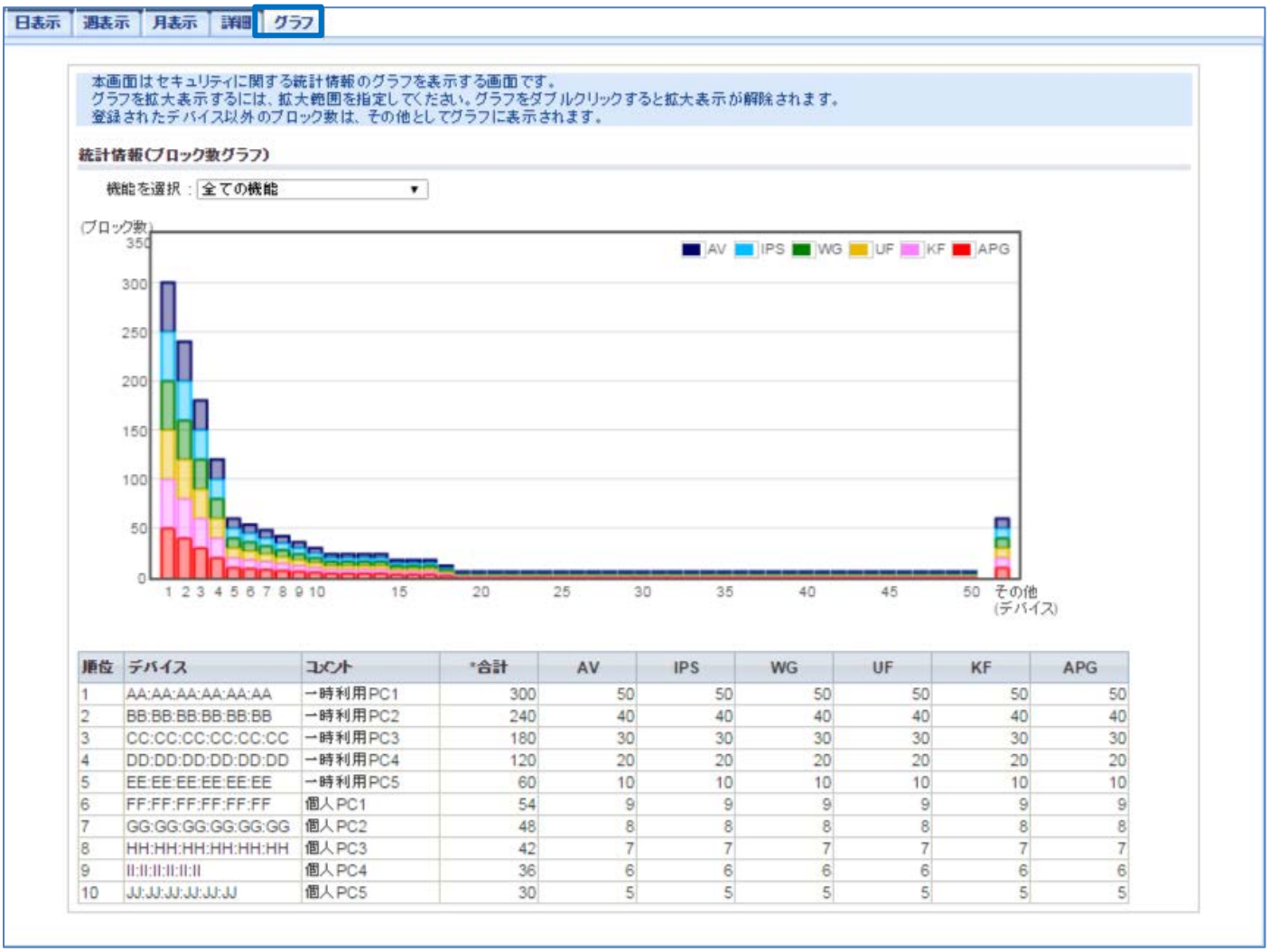
■グラフ

グラフ画面では、端末ごとのブロック数をグラフで表示します。表示対象の端末は 5.9.3 章デバイス管理で設定してください。左側からブロック数が多い順に表示します。これにより特定の端末にブロック発生が偏っていないかなどの傾向を把握しやすくなります。ブロック数は、対象端末を端末ごとの統計情報収集対象に設定した日から収集を開始し、最大 90 日間分の合計値で表示します。

[拡大表示について]

グラフが見えづらい場合は、ドラッグにより範囲を指定して拡大表示を活用してください。

グラフをダブルクリックすると拡大表示は解除されます。



順位	デバイス	コメント	*合計	AV	IPS	WG	UF	KF	APG
1	AA:AA:AA:AA:AA:AA	一時利用PC1	300	50	50	50	50	50	50
2	BB:BB:BB:BB:BB:BB	一時利用PC2	240	40	40	40	40	40	40
3	CC:CC:CC:CC:CC:CC	一時利用PC3	180	30	30	30	30	30	30
4	DD:DD:DD:DD:DD:DD	一時利用PC4	120	20	20	20	20	20	20
5	EE:EE:EE:EE:EE:EE	一時利用PC5	60	10	10	10	10	10	10
6	FF:FF:FF:FF:FF:FF	個人PC1	54	9	9	9	9	9	9
7	GG:GG:GG:GG:GG:GG	個人PC2	48	8	8	8	8	8	8
8	HH:HH:HH:HH:HH:HH	個人PC3	42	7	7	7	7	7	7
9	II:II:II:II:II:II	個人PC4	36	6	6	6	6	6	6
10	JJ:JJ:JJ:JJ:JJ:JJ	個人PC5	30	5	5	5	5	5	5

1. [TOP]-[セキュリティ]-[統計情報]画面を開きます。
2. [グラフ]タブをクリックし、ブロック数グラフからブロック数の発生状況を確認します。
3. [機能を選択]で表示するセキュリティ・スキャン機能を選択することもできます。
   表の項目欄の「*」印は選択されているセキュリティ・スキャン機能を示しています。

[メモ]

グラフ右側の「その他」は端末ごとの統計情報収集対象に設定されていない端末のブロック数の合計数を示します。

本グラフ未対応のファームウェア(Ver3.1.35 以前)で収集されたブロック数は「その他」にカウントされます。

また、ブロック数の偏りなどによりグラフが見えづらい場合は、拡大表示をご利用ください。

[メモ]

グラフ画面がうまく表示されない場合、以下の点をご確認ください。

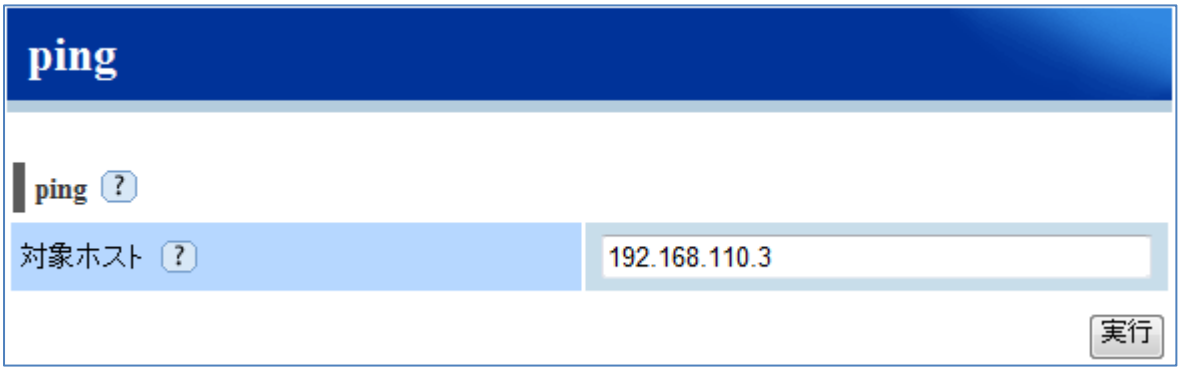
- Internet Explorer をお使いの場合は、バージョン 11 以降に更新する
- Internet Explorer の以下の設定を変更する

  「ツール」→「互換表示設定」→「イントラネットサイトを互換表示で表示する」のチェックを外す

  ※「イントラネットサイトを互換表示で表示する」を変更する場合、通常のブラウジングに影響する場合があります。
  この場合は「イントラネットサイトを互換表示で表示する」の設定を使い分けてください。

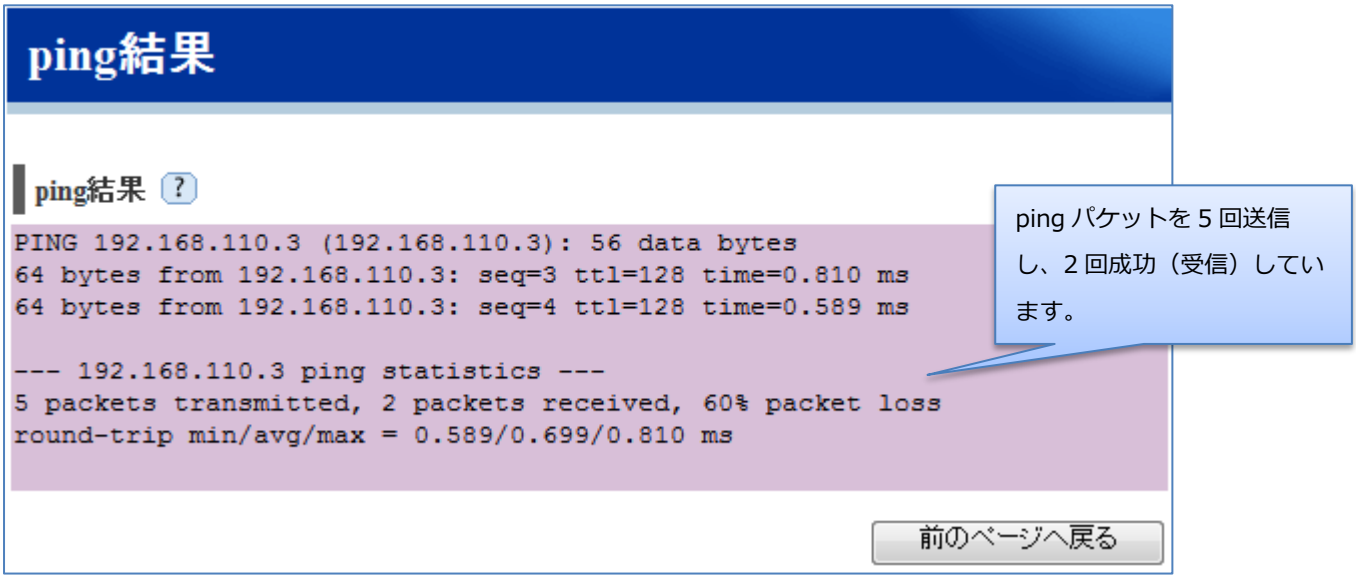
6.1.13. **ping 送信によるネットワーク到達確認**

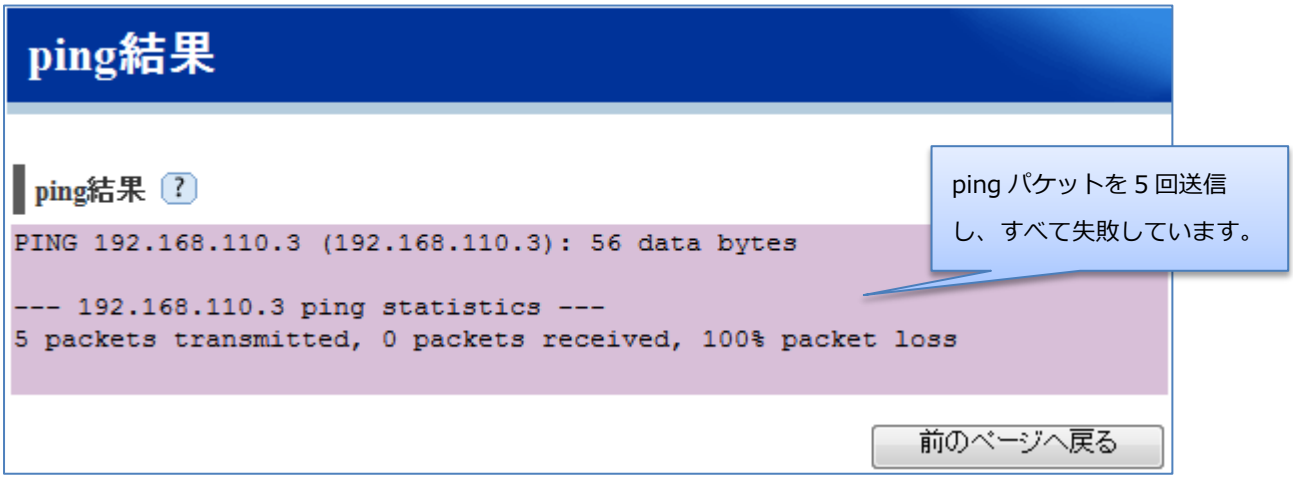
ネットワーク到達確認用途として、本製品から ping パケットを送信し、その到達を確認します。



1. [TOP]-[メンテナンス]-[診断機能]-[ping]画面を開きます。
2. 対象ホストに到達確認対象のノードのアドレス情報を設定します。
   到達確認対象ノードの IPv4 アドレス、または、ドメイン名を入力します。
3. 「実行」ボタンを押下します。

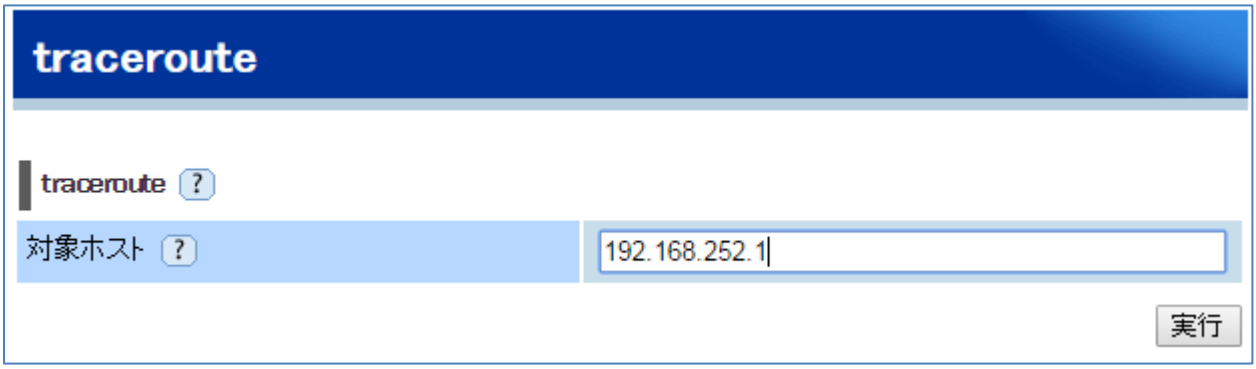
[結果の見かた]





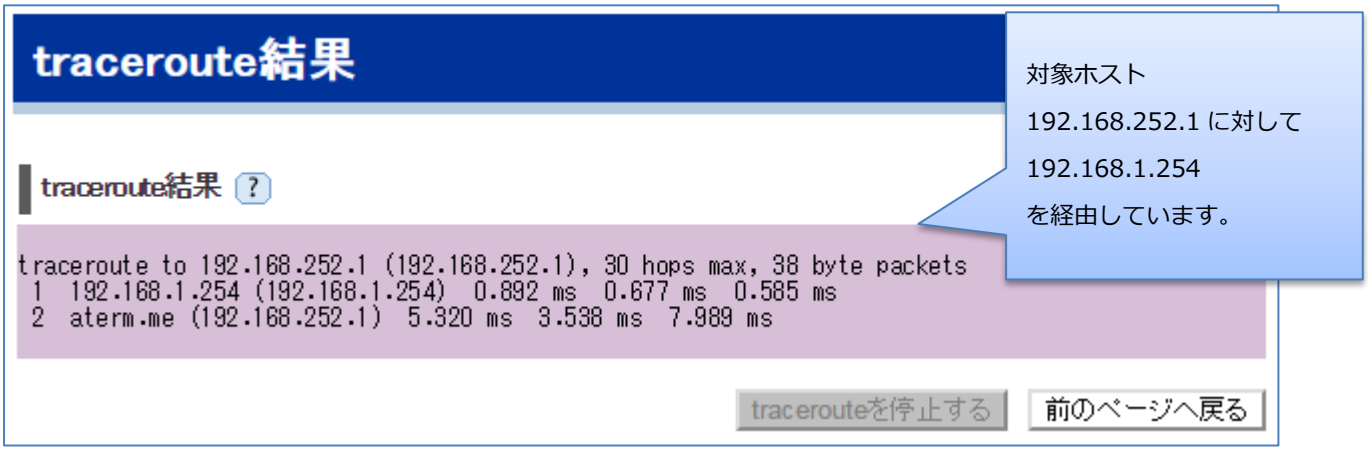
6.1.14. traceroute によるネットワーク経路確認

ネットワーク経路確認用途として、本製品から traceroute を送信し、対象ホストまでの到達経路を確認します。



1. [TOP]-[メンテナンス]-[診断機能]-[traceroute]画面を開きます。
2. 対象ホストに経路確認対象のノードのアドレス情報を設定します。
   経路確認対象ノードの IPv4 アドレス、または、ドメイン名を入力します。
3. 「実行」ボタンを押下します。

[結果の見かた]



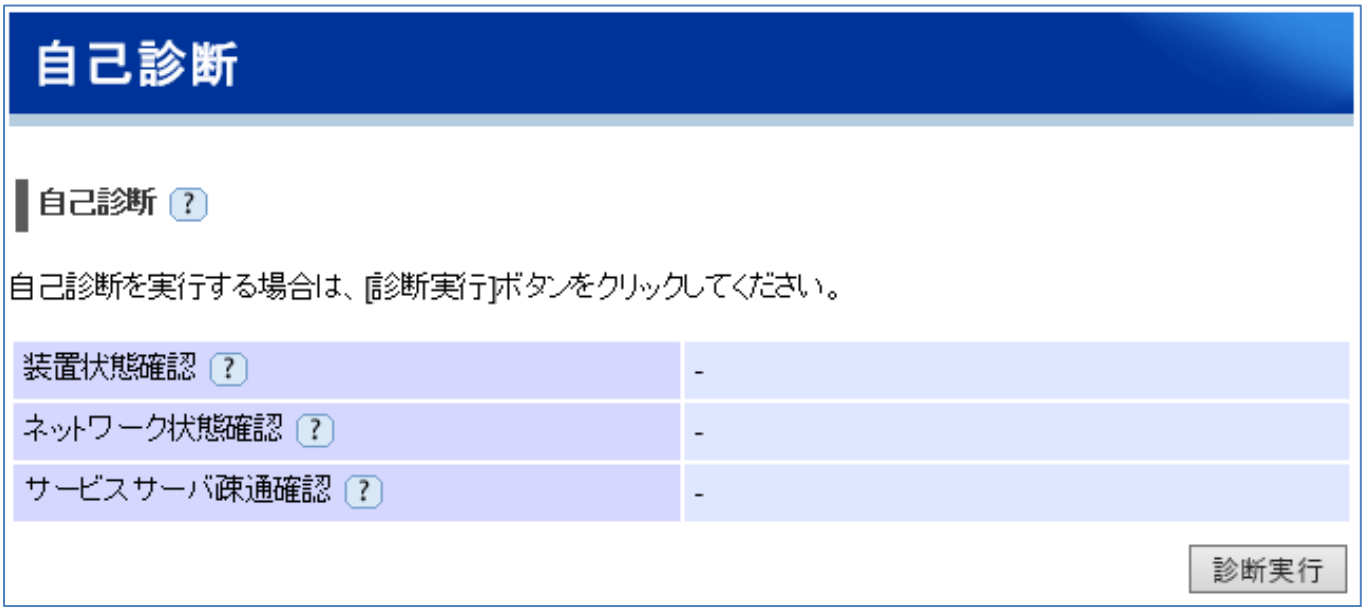
6.1.15. 自己診断機能

「診断実行」ボタンのクリックにより、本製品の設定情報の確認とサービスサーバへの疎通確認を実行します。

診断結果は、設定 Web 上に表示します。以下に表示例を示します。

自己診断の結果がすべて「OK」にもかかわらず、インターネットにアクセスできない場合は、7.1.5 章「インターネットにアクセスできない」を参照してください。

■自己診断（診断実行前）



1. [TOP]-[メンテナンス]-[診断機能]-[自己診断]画面を開きます。
2. 「診断実行」ボタンを押下します。

[結果の見かた]

■自己診断（診断実行後）

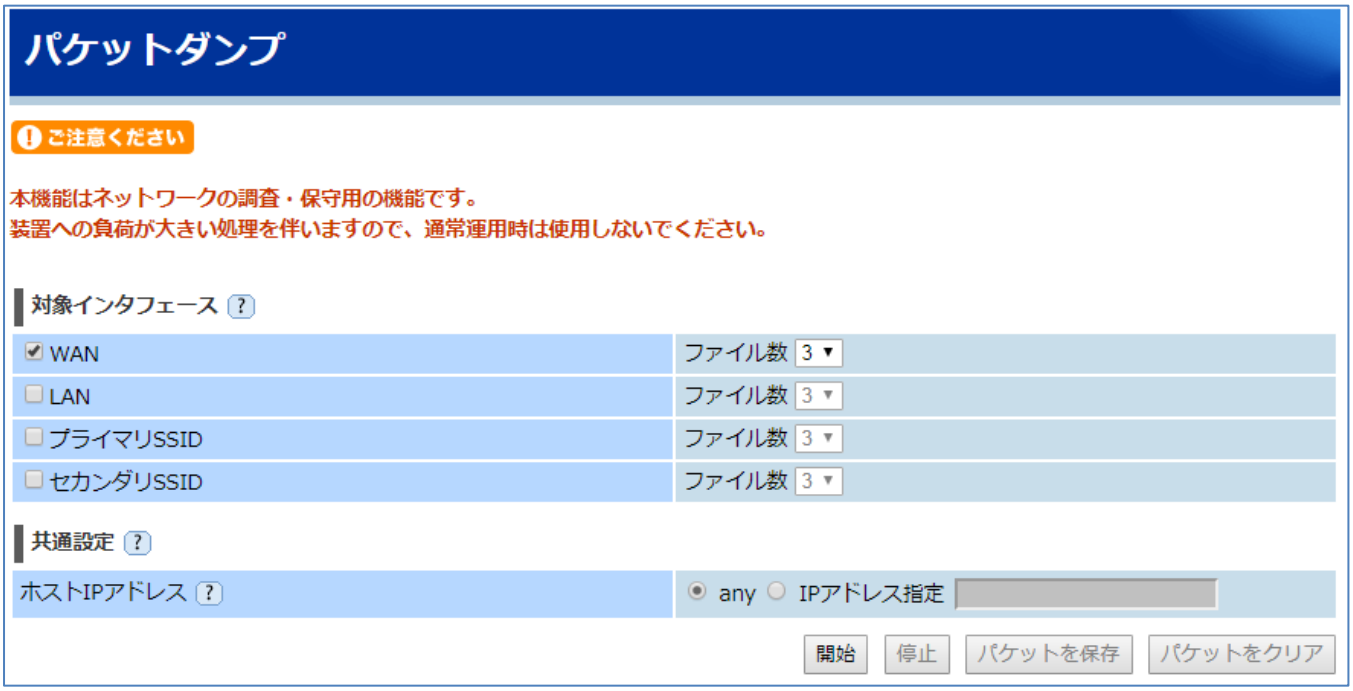
表示例は WAN ポートのケーブルが抜けている場合の例です。診断結果欄にガイドが表示されますので、ガイドにしたがって設定および接続などの見直しを行ってください。

6.1.16. パケットダンプ機能

本製品を通過するパケットをファイルに保存することができます。

1. [TOP]-[メンテナンス]-[診断機能]-[パケットダンプ]画面を開きます。
2. 対象インタフェースにチェックを入れ、保存するファイル数を設定します。
   共通設定でホスト IP アドレスを指定するか、any を設定します。
3. 「開始」ボタンを押下します。
4. パケット採取を停止する場合は「停止」ボタンを押下します。
5. 採取したパケットをパソコンなどに取得する場合、「パケットを保存」ボタンを押下します。
6. 本製品が保存しているパケットダンプ情報をクリアする場合、「パケットをクリア」ボタンを押下します。

※「パケットを保存」ボタンを押下した後にパケットダンプの再採取を行う場合は、「パケットをクリア」ボタンを押下する必要があります。



設定項目	値	備考	初期値
対象インタフェース			
WAN	• チェック有…WAN インタフェースのパケットダンプを採取する • チェック無…WAN インタフェースのパケットダンプを採取しない	保存するファイル数をプルダウンで選択します。	無効、 ファイル数 3
LAN	• チェック有…LAN インタフェースのパケットダンプを採取する • チェック無…LAN インタフェースのパケットダンプを採取しない	保存するファイル数をプルダウンで選択します。	無効、 ファイル数 3
プライマリ SSID	• チェック有…プライマリ SSID のパケットダンプを採取する • チェック無…プライマリ SSID のパケットダンプを採取しない	保存するファイル数をプルダウンで選択します。	無効、 ファイル数 3
セカンダリ SSID	• チェック有…セカンダリ SSID のパケ	保存するファイル数をプルダウンで選	無効、

		ットダンプを採取する • チェック無…セカンダリ SSID のパケットダンプを採取しない	択します。	ファイル数 3
共通設定				
	ホスト IP アドレス	パケットの宛先ホスト、送信元ホストを指定します。すべての IP アドレスを対象とする場合は「any」を選択してください。		any

各インタフェースの最大取得ファイル数は 12 個です。1 ファイルあたりのサイズは 10M バイトとなります。本装置は最大 120M バイトまで FlashROM に保存できますので、それを超えないように設定する必要があります。
例えば 4 つのインタフェースすべてキャプチャしたい場合は、4 つのインタフェースにチェックを入れ、各ファイル数を 3 に指定する必要があります。
（4 インタフェース x 3 ファイル x 10 M バイト = 120M バイト）
LAN、WAN だけ採取したい場合は、LAN と WAN にチェックを入れて、各ファイル数を 6 にすれば、それぞれ 60MB 分のキャプチャが採取できます。

[ご注意]

・無線 LAN 機能を無効のときにプライマリ SSID,セカンダリ SSID にチェックがされていてもキャプチャはされません。
・キャプチャデータは古いデータから上書き保存します。開始から停止するまでの間に設定された最大容量を超えるトラフィックがある場合はご注意ください。

7. こんな時には

7.1. こんな時には

7.1.1. 本製品を設置するネットワーク内で複数経路が存在する

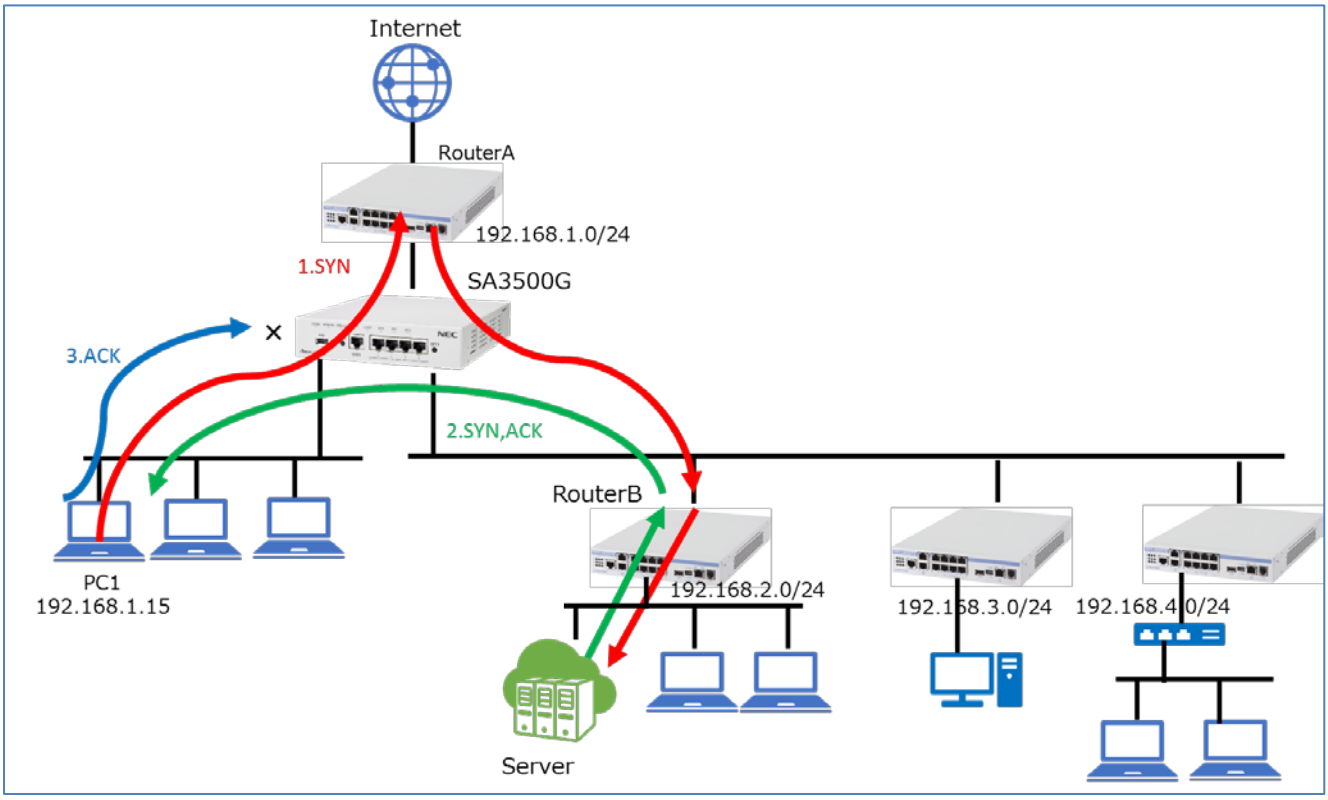
PC から見て複数経路が存在する場合の注意点についてご説明します。

本製品は TCP 通信において、行きと帰りのパケットの整合性をチェックしています。このため行きと帰りのパケットが揃っていない場合は TCP セッションを切断します。

下図に例を示します。動作モードはブリッジモードです。

本製品はパケットを検査して TCP のステートを確認しています。以下 1～4 の場合では、TCP SYN,ACK を本製品が検知していないため、不正なパケットとみなして、本製品が TCP ACK を破棄します。

このようなときには、Router のルーティング設定を変更して経路変更要求を出さなくする、もしくは各 PC のルーティングテーブルに、経路情報を追加していただく必要があります。



1．PC1 から Server への TCP SYN は異なるサブネットのため、デフォルトゲートウェイの RouterA に送られる。RouterA はルーティングテーブルにしたがって RouterB に転送する。

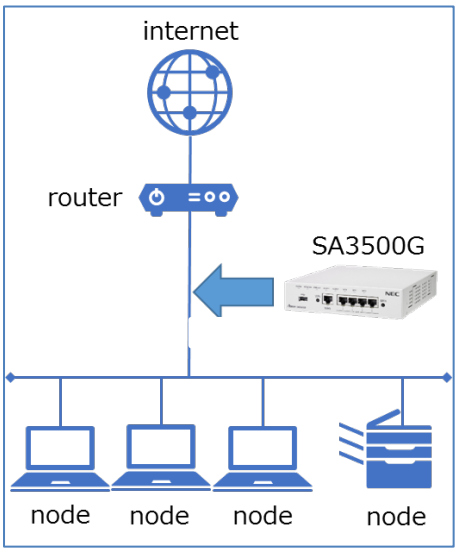
2．RouterA は PC1 と RouterB が同一サブネットのため、PC1 に対して経路変更要求を出す。

3．Server から PC1 への TCP SYN,ACK は RouterA を経由せずに PC1 に送られる。

4．PC1 から Server への TCP ACK を本製品は不正なパケットとみなして破棄する。

1）ブリッジモードでネットワーク変更せずに設置できるネットワーク構成

各 node からみて、出口が 1 つのネットワーク

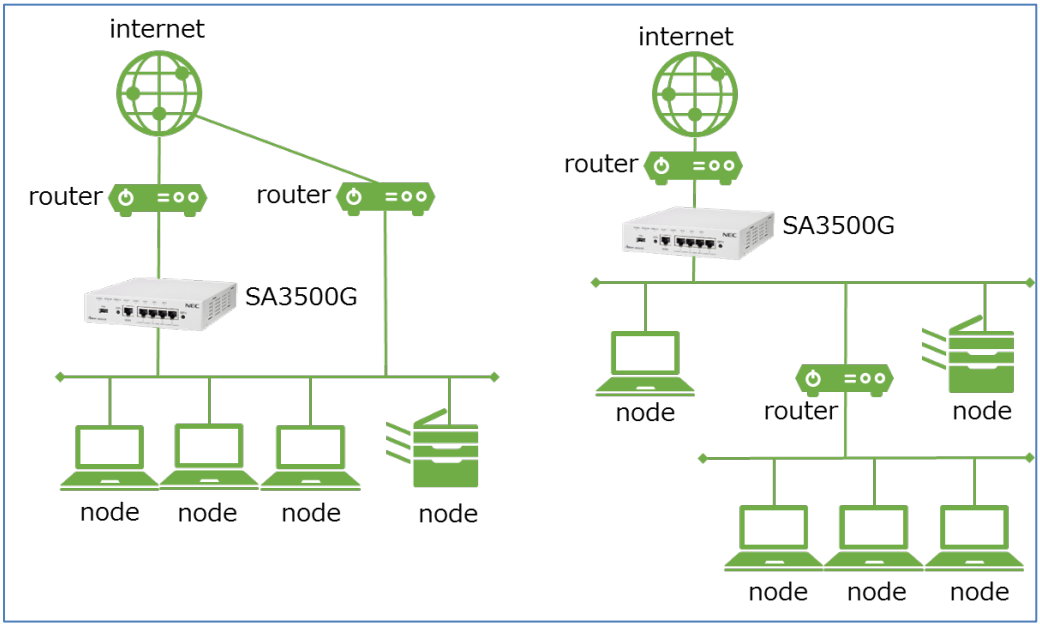


node（PC など）とインターネット間のすべてのパケットが SA3500G を通過するため、ご使用中のネットワークを変更せずに本製品を設置いただけます。

2) 設置に際して、ネットワーク構成の確認が必要なネットワーク

ネットワークによっては、他ネットワーク機器の設定変更が必要な場合があります。

各 node へのパケットの経路が複数存在するネットワーク



ノード間の行きと帰りのすべてのパケット（ノードからインターネットアクセスを含みます）が、本製品を通過しないことが想定するネットワーク構成の例です。

その場合、すべてのパケットが本製品を通過するようにネットワーク設計いただく必要があります。

7.1.2. **設定 Web にログインできない**

- ✓ パソコンの IP アドレスが 169.254.xxx.xxx/16 であることを確認してください。
  ※本製品のブリッジモードでは DHCP サーバ機能がありません。パソコンに固定で IP アドレスを設定してください。
  ※設定終了後、パソコンの IP アドレスの設定を元に戻してください。パソコンの IP アドレスが 169.254.xxx.xxx/16 の場合、インターネットにアクセスできません。
- ✓ パソコンの Web ブラウザのプロキシ設定が無効であることを確認してください。
- ✓ 本製品の LAN ポートとパソコンが Ethernet ケーブルで確実に接続できていることを確認してください。
  ※本製品の LAN ポートのランプが緑点灯していることを確認してください。
- ✓ 本製品のユーザー名は、"admin"（ダブルクオートを除きます）です。
- ✓ 簡易 RADIUS 機能の利用で、HTTPS で設定 Web へアクセスできない場合は、ルート証明書をパソコンなどへインポートしていないか確認してください。
  ※HTTPS のサーバ証明書は、本製品のルート証明書で署名されており、ルート証明書は、装置初期化で再生成されます。
  古いルート証明書を PC 等へインポートしている場合、装置初期化後の設定 Web に HTTPS でアクセスできません。
  新たに生成されたルート証明書を再インポートしてください。

7.1.3. **設定 Web のログインパスワードを忘れた**

本製品を初期化してください。
※本製品は、ログインパスワードのみを初期状態に戻すことができません。

[初期化方法]

本製品の RESET スイッチを使って初期化してください。
詳細は、5.10.1 章を参照してください。

[メモ]

本製品の初期化および再起動後、アクティベーション操作は必要ありません。

7.1.4. **アクティベーションできない**

OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を放してから 1 分以上経過しても ALERT2 ランプが消灯しない場合、アクティベーションが成功していません。アクティベーション操作しても ALERT2 ランプが消灯しない場合は、下記を実施/確認してください。

- ✓ 本製品がインターネット通信できる状態であることを確認してください。
  設定 Web の[TOP]-[メンテナンス]-[情報]-[デバイスの状態]画面で、下記表示になっていることを確認してください。
  ・「IPv4 接続状態」が"インターネット利用可能"と表示されていること
  ・「IPv4 アドレス/ネットマスク」「IPv4 ゲートウェイ」「IPv4 プライマリ DNS」に IPv4 アドレスが表示されていること
- ✓ プロキシサーバを経由したインターネット通信環境の場合は、本製品にプロキシサーバの設定を行ってください。
- ✓ 上記表示内容が問題ない場合、本製品以外の装置を使用して、本製品が接続しているネットワークがインターネット通信できることを確認してください。
- ✓ OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を ALERT2 ランプが緑点灯するまで約 4 秒間押し続けてください。
- ✓ ライセンス契約の状況をご確認ください。ライセンス契約状況の確認は、Aterm Biz インフォメーションセンターまでお願いします。

7.1.5. **インターネットにアクセスできない**

IP パケットが本製品を通過しない場合、下記を実施/確認してください。

- ✓ 本製品の設定に使用したパソコンの場合、パソコンの IP アドレスを元の設定に戻していることを確認してください。
  パソコンの IP アドレスが、169.254.xxx.xxx/16 の場合、インターネットにアクセスできません。
- ✓ 本製品のセキュリティ・スキャン機能が有効になっていることを確認してください。
- ✓ 原因が分らない場合は、自己診断機能をお試しください。詳細は 6.1.15 章を参照してください。

No	ランプ	状態	説明/対処方法	参照する章
1	POWER	緑点灯	正常です。 ※本製品の起動中は、すべてのランプが緑点灯します。	
2		赤点灯	本製品の起動に失敗しています。一度、電源を OFF にし、10 秒ほど経過後、電源を入れてください。これでも赤点灯する場合は、Aterm Biz インフォメーションセンターにお問い合わせください。	
3		消灯	本製品の電源を入れてください。緑点灯しない場合は、Aterm Biz インフォメーションセンターにお問い合わせください。	
4		上記以外	上記以外の状態が 10 分以上続いている場合、本製品に異常が生じている可能性があります。一度、電源を OFF にし、10 秒ほど経過後、電源を入れてください。これでも状態が継続する場合は、Aterm Biz インフォメーションセンターにお問い合わせください。 [注意] 橙点滅は、FlashROM、USB ストレージへの書き込みを表します。 この場合は、本製品の電源を OFF にしないでください。	
5	NETWORK[23]	橙点灯、または緑点灯	IP アドレスは正常です。DNS サーバ、ゲートウェイが正しく設定されているか確認してください。	
6		橙点滅、または緑点滅	IP アドレスを取得処理中です。しばらくしても点滅が終わらない場合は、ネットワークの環境を確認してください。	
7		消灯	本製品の WAN ポートと本製品の上位機器を Ethernet ケーブルで接続し、本製品の WAN ポートのランプが緑点灯することを確認してください。 これでも NETWORK ランプが緑点灯、または橙点灯しない場合、本製品に IP アドレスが設定されていることを確認(*)してください。 (*) 設定 Web の[TOP]-[メンテナンス]-[情報]-[デバイスの状態]画面で、「IPv4 接続状態」が"インターネット利用可能"と表示されていることを確認してください。 (*) ブリッジモードのときは LAN ポートにパソコンを接続している場合は消灯しません。	4.5 6.1.1 6.1.2
8	ALERT2	消灯	正常です。	

[23]本製品は本製品自身がインターネット通信できない状態の場合、セキュリティ・スキャン機能はご使用になれません。

9		赤点滅	正常です。 ※ライセンス期限が近づいています。ライセンス更新に関するお問い合わせはAterm Bizインフォメーションセンターにお願いします。	
10		橙点灯	アクティベーションしてください。	5.2.3
11		赤点灯	ライセンス期限が満了しています。 ご購入の販売店、または当社営業担当までご連絡ください。	
12		上記以外	上記以外の状態が 10 分以上続いている場合、本製品に異常があります。一度、電源を OFF にし、10 秒ほど経過後、電源を入れてください。これでも状態が継続する場合は、Aterm Biz インフォメーションセンターにお問い合わせください。	

7.1.6. **セキュリティ・スキャン機能が動作しない**

- 本製品のセキュリティ・スキャン機能は、検出対象のパケットを限定しています。
  暗号化パケット（IPsec などで暗号化されたパケット）には対応していません。
  本製品のセキュリティ・スキャン機能の検出対象パケットの詳細は、3.1 章を参照してください。
- URL フィルタリングなどのセキュリティ・スキャン機能が動作しない場合は、本製品の時刻が実際の時刻に合っているかを確認してください。時刻の確認方法は、5.6.13 章を参照してください。

7.1.7. **ファームウェアを更新できない**

本製品を一旦再起動してください。その後、ファームウェアの更新を再操作してください。
これでもファームウェア更新に失敗する場合は、Aterm Biz インフォメーションセンターにお問い合わせください。

7.1.8. **セキュリティ・スキャン機能を停止したい**

セキュリティ・スキャン機能は次の方法で停止することができます。

ただし、セキュリティ・スキャン機能の停止は、セキュリティリスクを増大させます。そのため、機能の停止はお客様の責任でご確認の上で実施してください。

機能	停止方法
ファイアウォール（FW）	[ファイアウォール（FW）]画面で「ファイアウォール設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.3 章参照）
アンチウイルス（AV）	[アンチウイルス（AV）]画面で「アンチウイルス設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.4 章参照）
不正侵入防止（IPS）	[不正侵入防止（IPS）]画面で「不正侵入防止設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.5 章参照）
Web ガード（WG）	[Web ガード（WG）]画面で「Web ガード設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.6 章参照）
URL フィルタリング（UF）	[URL フィルタリング（UF）]画面で「URL フィルタリング設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.7 章参照）
URL キーワードフィルタリング（KF）	[URL キーワードフィルタリング（KF）]画面で「URL キーワードフィルタリング設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.8 章参照）
アプリケーションガード（APG）	[アプリケーションガード（APG）]画面で「アプリケーションガード設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.9 章参照）

7.1.9. **設定値を変更した場合に行う作業**

本製品の設定値を変更した場合は、何らかの理由により本製品が立ち上がらなくなった場合を想定し、設定値をパソコンなどに保存しておくことをお願いします。設定 Web からの設定値はお客様の固有情報であり、保存されていない場合には再設定が必要となります。パソコンなどへの設定値の保存手順については、3.4.3 章を参照してください。

USB ポートに USB ストレージを接続して、設定値を保存することが出来ます。保存手順については、3.8.1 章を参照してください。

7.1.10. **本製品の電源を OFF にする前に行う作業**

本製品は、本製品のセキュリティ・スキャン機能のセキュリティログと統計情報、およびイベントログを毎時 1 回、FlashROM に定期保存します。（毎時 00 分に保存します）次の処理を行わずに本製品の電源を OFF にすると、データが消去することがありますのでご注意ください。

[電源を OFF にする前にセキュリティログと統計情報、およびイベントログを FlashROM に保存する方法]

- 設定 Web から再起動を行う（5.6.17 章参照）

7.1.11. 統計情報が正しく表示されない

例えば、「2015/11/14」などが表示される理由は、本製品が時刻を補正する前の統計情報が表示されるためです。
本製品は起動後から時刻補正までの情報を初期時刻の統計情報として扱います。初期時刻については 5.6.13 章を参照してください。

7.1.12. ネットワーク通信に関するエラーログ表示はありますか

イベントログで確認できます。イベントログは設定 Web の[メンテナンス]-[情報]-[イベントログ]画面で確認できます。
詳細は、3.4.11 章を参照してください。

7.1.13. IPsec で接続できない

本製品で IPsec 通信ができない場合は、以下の点をチェックしてください。

1. OPT 1 ランプが橙点灯のままの場合
   IPsec トンネルを構築できていません。設定が間違っている可能性があります。以下の設定値を再確認してください。
   ① 対向拠点宛先が正しいこと
   ② 事前共有鍵が対向装置の設定と一致していること
   ③ IKE フェーズ 1 のローカル ID とリモート ID が対向装置の設定と一致していること
      ※IKEv2 では IKE_SA_INIT 交換のローカル ID とリモート ID が対向装置の設定と一致していること
   ④ IKE フェーズ 2 のローカル ID とリモート ID が対向装置の設定と一致していること
      ※IKEv2 では IKE_AUTH 交換のローカルトラフィックセレクタとリモートトラフィックセレクタが
      対向装置の設定と一致していること
   ⑤ 暗号化アルゴリズムと認証アルゴリズムが対向装置の設定と一致していること

2. OPT 1 ランプが緑点灯なのに、データ通信ができない場合
   ① LAN 側に暗号化対象のサブネットワークがある場合は、静的ルーティング設定で LAN 側のサブネットワークを明示的に設定してください。
   ② ALERT2 ランプが橙点灯している場合はアクティベーションが完了していないため、LAN 側からのユーザーパケットを WAN 側に転送できません。アクティベーション操作をしてください。

7.1.14. **Wi-Fi 通信できない**

✓ 本製品の WIRELESS ランプが緑点滅または緑点灯していることを確認してください。

WIRELESS ランプの状態	対処方法
橙点滅	WPS 動作中ですので、特に問題ありません。 ただし、橙点滅が 2 分以上続く場合、本製品が異常な状態に陥っている可能性があります。本製品を再起動してください。
赤点滅	WPS 失敗です。5.10.5 章を参照してください。 ただし、赤点滅が 1 分以上続く場合、本製品が異常な状態に陥っている可能性があります。本製品を再起動してください。
消灯	本製品の無線 LAN 機能を有効にしてください。 設定方法は、5.7.8 章を参照してください。

✓ 周囲の電波状況を確認してください。

確認事項	対処方法
2.4GHz 帯域の電波干渉の有無	● 本製品の近くに同じチャネルを使用している無線 LAN アクセスポイントを設置していないことを確認してください。本製品のオートチャネル機能を使用している場合は、本製品の無線 LAN 機能を無効→有効、または本製品を再起動することで、電波状況の良いチャネルを自動選択します。 ● 本製品の近くに Bluetooth などを利用した電子機器を設置していないことを確認してください。
外付けアンテナの設置状況	外付けアンテナを利用している場合、外付けアンテナの取り付けが正しいことを確認してください。外付けアンテナの取り付け方法は、4.3 章を参照してください。 ※外付けアンテナの取り付け状態を定期的に確認してください。

7.1.15. **PPPoE セッションがつながらない**

PPPoEセッションがつながらない場合やつながったり切れたりする場合は以下を確認してください。

・ADSL モデム、ONU の回線側ポートがリンク確立しているかどうか確認してください。

・回線事業者の工事情報、故障情報を確認してください。

・PPP 認証情報（ユーザーID/パスワード）やに誤りがないか確認してください。

・回線側の品質に問題がある可能性があります。ADSL モデムやONU のログを確認し、セッションの異常切断が発生していないか確認してください。もしくは回線事業者に確認を依頼してください。

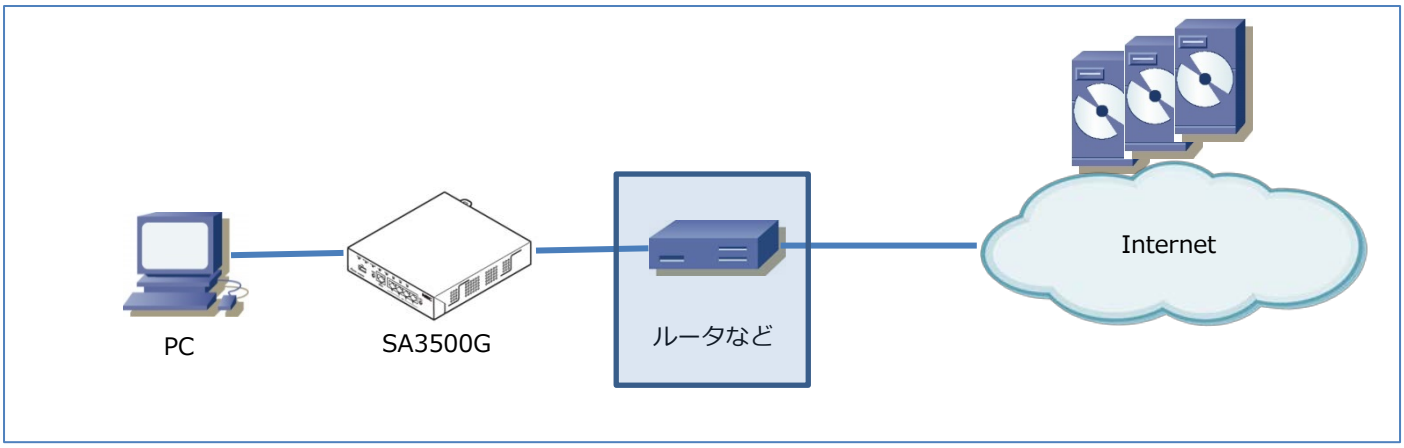
7.1.16. **「デバイス ID」、「製造番号」を設定 Web で確認したい**

[TOP]-[メンテナンス]-[情報]-[デバイスの状態]画面を開きます。「装置情報」欄に「デバイス ID」と「製造番号」が表示されていますので、ご確認ください。表示例は 6.1.1 章を参照してください。

7.1.17. ルータモードでインターネットにつながらない

[TOP]-[セキュリティ]-[ファイアウォール（FW）] 画面で「NAPT 有効インタフェース」を無効にした場合、SA3500G の上位に接続しているルータやネットワーク機器の設定の見直しが必要になる場合があります。
ルータやネットワーク機器の設定によっては、本製品の LAN 側に接続している端末からインターネットに接続できなくなる場合がありますので、SA3500G の上位に接続しているルータやネットワーク機器の静的ルーティング設定を見直してください。

・上位ルータの設定例
　宛先 IP アドレス：SA3500G の LAN サブネットアドレス
　転送先　　：SA3500G の WAN IP アドレス

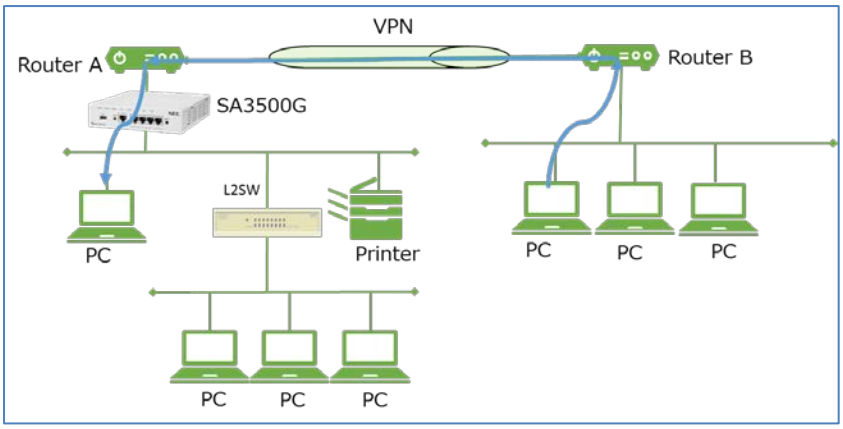


7.1.18. ブリッジモードで RIP の経路情報が転送されない

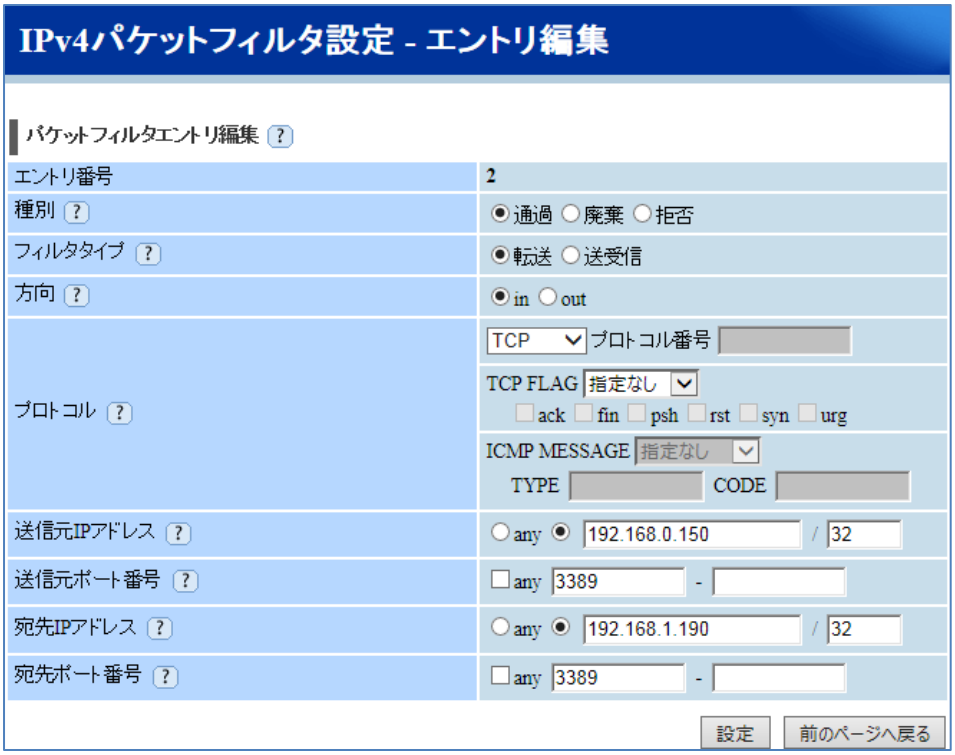
[TOP]-[セキュリティ]-[ファイアウォール（FW）] 画面で「ファイアウォール設定」を有効にしている場合、本製品の上位に接続しているルータやネットワーク機器からブロードキャストで送信される、RIP の経路情報は本製品で破棄します。
この場合、「ファイアウォール設定」を無効にしてご使用ください。

7.1.19. リモートデスクトップ接続ができない

ブリッジモードでファイアウォール機能を有効に設定しますと、VPN 接続先のリモート PC からローカル PC に対して、リモートデスクトップ接続ができません。この場合は、本製品の IPv4 パケットフィルタ設定で許可フィルタを設定する必要があります。



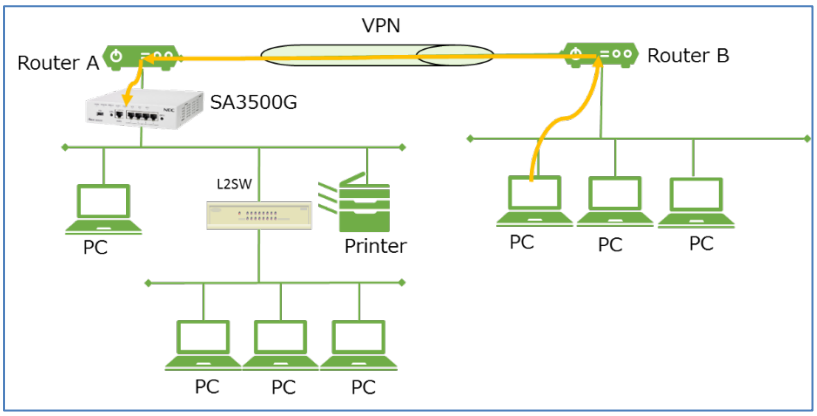
許可フィルタは設定 Web の[メンテナンス]-[IPv4 パケットフィルタ設定]-[編集]から、フィルタタイプ・プロトコル・宛先ポートの指定を行って、「設定」ボタンを押下してください。エントリ編集後に「保存」をクリックして、設定値を保存してください。



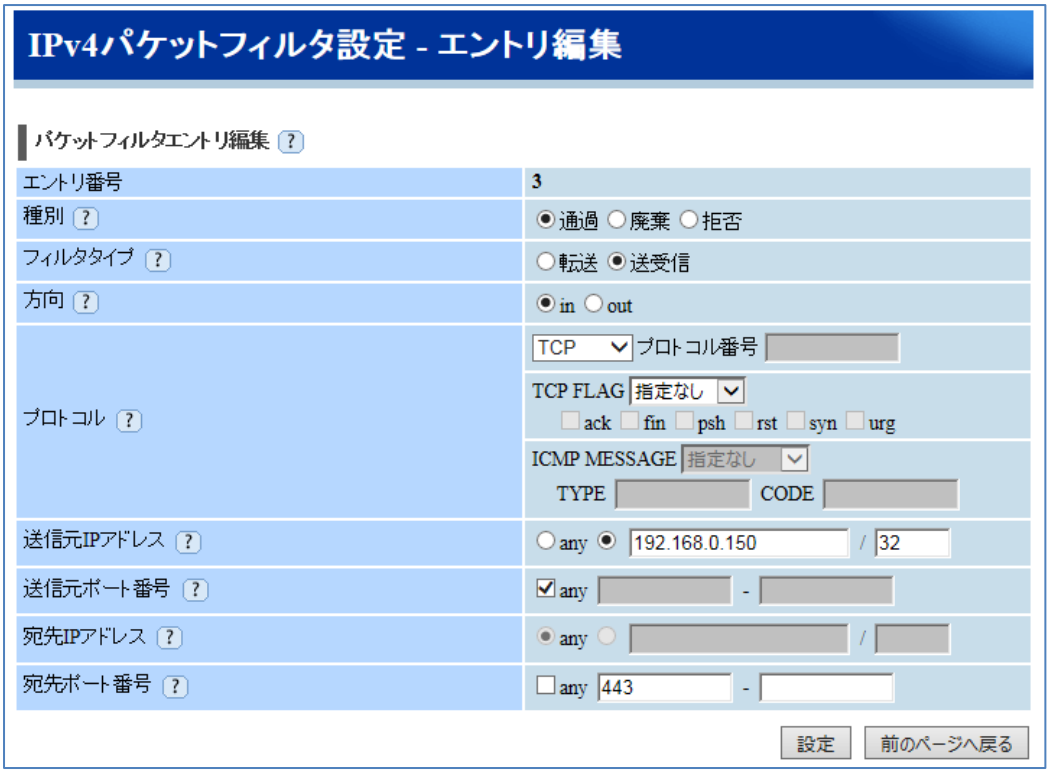
設定項目	設定値	備考
種別	通過	
フィルタタイプ	転送	
方向	in	
プロトコル	TCP	
送信元 IP アドレス	リモート PC の IP アドレス	ネットマスクは 32 を推奨します。
送信元ポート番号	3389	※ポート番号が固定の場合はそのポート番号を入力してください。不定の場合は any にチェックを入れてください。
宛先 IP アドレス	ローカル PC の IP アドレス	ネットマスクは 32 を推奨します。
宛先ポート番号	3389	※図は Windows を例に記載しています。お使いの環境に合わせてください。

7.1.20. リモート PC から本製品の設定 Web にアクセスしたい

VPN 環境を構築しているお客様において、下図のようにリモート PC から本製品の設定 Web を開くには、本製品の IPv4 パケットフィルタ設定で許可フィルタを設定する必要があります。



許可フィルタは設定 Web の[メンテナンス]-[IPv4 パケットフィルタ設定]-[編集]から、フィルタタイプ・プロトコル・宛先ポートの指定を行って、「設定」ボタンを押下してください。エントリ編集後に「保存」をクリックして、設定値を保存してください。



設定項目	設定値	備考
種別	通過	
フィルタタイプ	送受信	
方向	in	
プロトコル	TCP	
送信元 IP アドレス	リモート PC の IP アドレス	ネットマスクは 32 を推奨します。
送信元ポート番号	リモート PC のポート番号	ポート番号が固定の場合はそのポート番号を入力してください。 不定の場合は any にチェックを入れてください。
宛先ポート番号	443	設定 Web へのアクセスは、https://xxx.xxx.xxx.xxx/(本製品の IP アドレス)にて行ってください。

7.1.21. **特定のサイトにアクセスできない**

特定のサイトにアクセスできない場合は、URL フィルタリングでブロックされている可能性があります。その場合は該当するカテゴリを許可設定にするか、個別許可設定をご利用ください。設定方法は 5.8.7 章を参照してください。

7.1.22. **特定のアプリケーションが通信できない**

特定のアプリケーションが通信できない場合は、アプリケーションガードでブロックされている可能性があります。その場合は該当するアプリケーションを許可設定にしてご利用ください。設定方法は 5.8.9 章を参照してください。

7.1.23. **セキュリティログに不明なログが出力されている**

デバイスの多くはバックグラウンドで各種アプリケーションが動作していることがあります。その場合は、セキュリティログで出力する送信元 IP アドレスからデバイスを特定してください。その後に必要なアプリケーションかどうかを、本製品をお使いになっている環境のセキュリティポリシーを基に判断してください。
必要ではないアプリケーションの場合は、バックグラウンド処理を停止するなどの処置を行ってください。

7.1.24. **受信したメールの添付ファイルが開けない**

本製品がウイルスを検知してメールの添付ファイルの無害化を行った可能性があります。受信したメールの時間情報と本製品のセキュリティログで、アンチウイルスに「Destroy」(破壊)のログが残っていないかを確認してください。

7.1.25. **MAC アドレスでデバイス認証を行っている**

本製品を MAC アドレスでデバイスを認証しているネットワークに設置する場合は、本製品の MAC アドレスを許可設定する必要があります。動作モードによって、許可設定を行う MAC アドレスが異なりますのでご注意ください。

動作モード	許可設定する MAC アドレス
ブリッジモード	LAN MAC アドレス
ルータモード	WAN MAC アドレス

MAC アドレスは、設定 Web の[TOP]-[メンテナンス]-[デバイスの状態]で確認できます。

7.1.26. **Microsoft Azure(Route Based)設定時に通信ができない、遅い場合がある**

ご利用の回線の MRU(Maximum Receive Unit)値を確認してください。ご利用の環境において、MTU(Maximum Transmission Unit)が上記の値以上に設定されていると通信できない、または遅くなる可能があります。
MTU の設定手順は、5.7.6 章を参照してください。

7.1.27. **異常事象発生時、電源を OFF にする前に実施いただきたい作業**

不都合な事象が発生した場合に本製品の情報取得をお願いする場合があります。
5.6.18 章の[装置状態の一括取得]の項に装置情報の取得手順を載せています。

7.1.28. **NetMeister の状態が成功にならない**

NetMeister 設定画面で設定している親機が NetMeister Ver3.0 以降に対応していることをご確認ください。
NetMeister Ver1.0、NetMeister Ver2.0 に対応した親機とは接続できません。対応している親機については 3.4.15 章の[利用環境]を参照してください。

7.1.29. **装置の初期ウィザード設定を行う前に最新のファームウェアへ更新したい**

OPT2 ボタン操作により、設定 Web を操作することなく、オンラインバージョンアップによる最新のファームウェアへの更新が行えます。オンラインバージョンアップを行うには、本製品をインターネットに接続する必要があります。
本製品は DHCP クライアント機能の初期値が有効となっていますので、DHCP サーバがあるネットワークに本製品を接続することで、インターネット接続することができます。詳しい設定方法は 5.10.4 章を参照してください。

7.1.30. **メールの受信が中断される**

アンチウイルス機能の拡張スキャンを有効にしている場合、ウイルスファイルを検知した際に通信を途中でリセットさせることがあります。受信したメールの時間情報と本製品のセキュリティログで、アンチウイルスに「Destroy」(破壊)のログが残っていないかを確認してください。該当する場合は、再度同じ通信を行った際にファイルの無害化が行われますので、再度メールの受信を行ってください。
複数のウイルスファイルを受信した場合は複数回通信のやり直しを行う必要がある場合があります。

7.1.31. **サーバからの PING の応答がない**

本製品は TCP、ICMP の状態遷移を監視する「厳格チェック」を行っており、本製品上で正しい開始手続きが行われていないパケットを廃棄することがあります。
「TCP ストリームの厳格チェック設定」を「厳格チェックしない」にチェックすることで事象が改善される場合は、この機能により PING の reply パケットを廃棄していると考えられます。
設定方法については 5.8.2 章を参照してください。

「厳格チェック」によりパケットが廃棄されている場合、本製品が正しい経路上に設置されていない可能性があります。
厳格チェック時でも PING が通るように、通信の行きと戻りの両方が本製品を経由するネットワーク構成にして運用することを推奨します。

8. 設定事例

設置例や設定例をまとめています。

章	タイトル
8.1	こんなネットワークで使いたい
8.1.1	ルータの WAN 側は PPPoE で動作している
8.1.2	VPN を使っている
8.1.3	VLAN を使っている
8.1.4	端末を IEEE802.1X で認証している
8.1.5	Aspire と本製品の接続について
8.1.6	1 台の親機を使用して NetMeister と接続する
8.1.7	2 台の親機を使用して NetMeister と接続する

8.1. こんなネットワークで使いたい

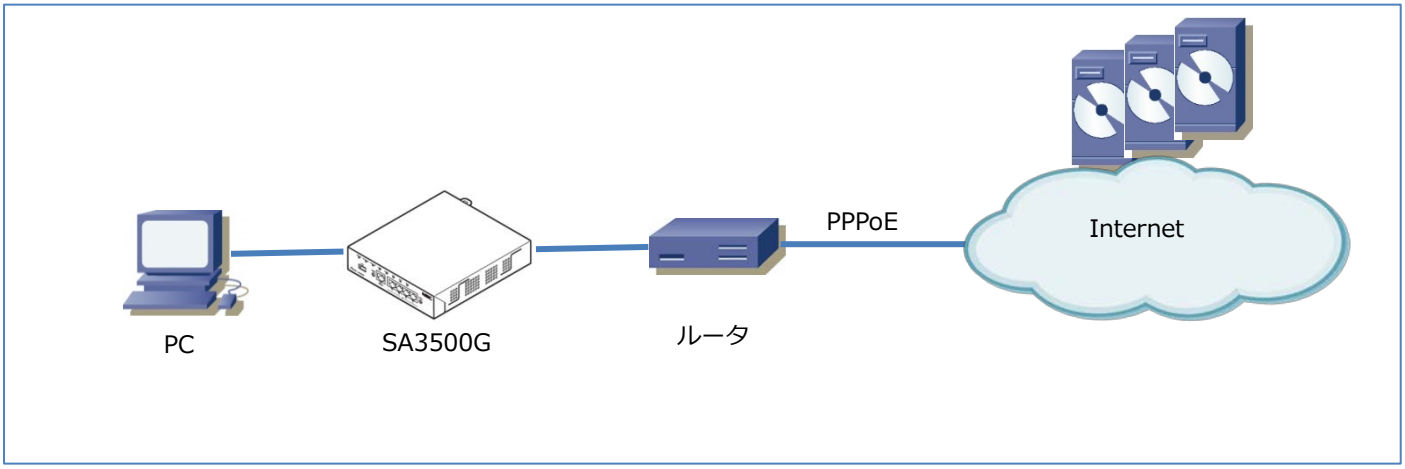
本章では、本製品の設置例を紹介しています。

8.1.1. ルータの WAN 側は PPPoE で動作している

※ルータは、ブロードバンドルータまたはホームゲートウェイを含みます

本製品をルータのローカルエリア側に設置してください。

設置場所



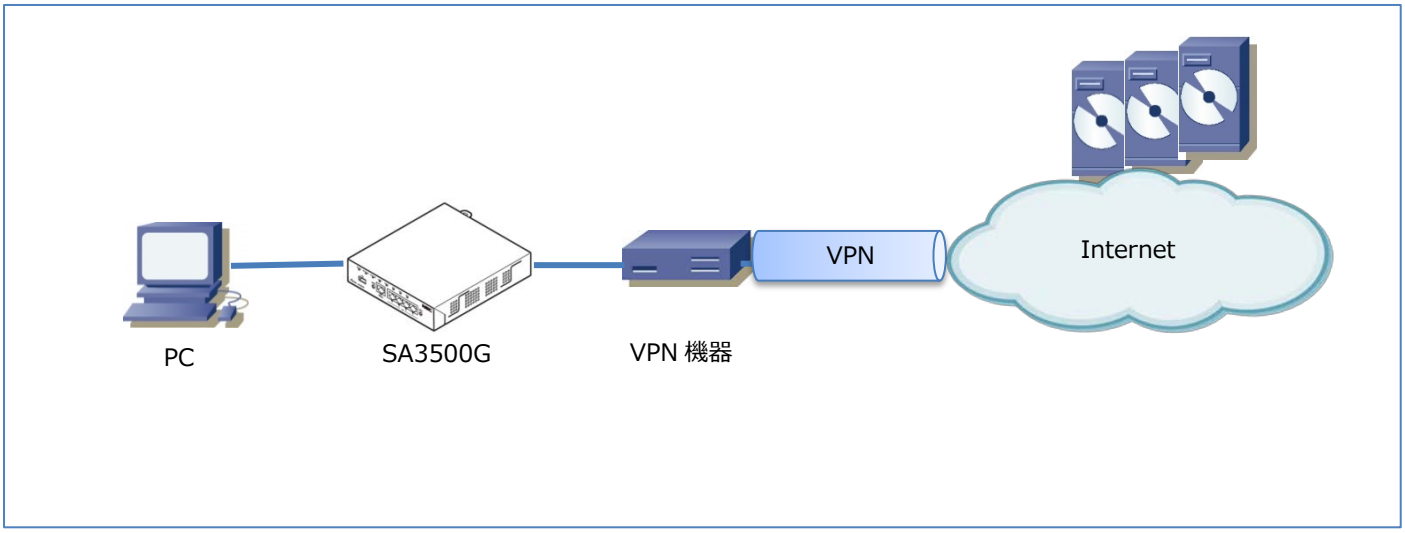
8.1.2. VPN を使っている

設置場所

本製品を VPN のネットワークの外側に設置してください。

説明

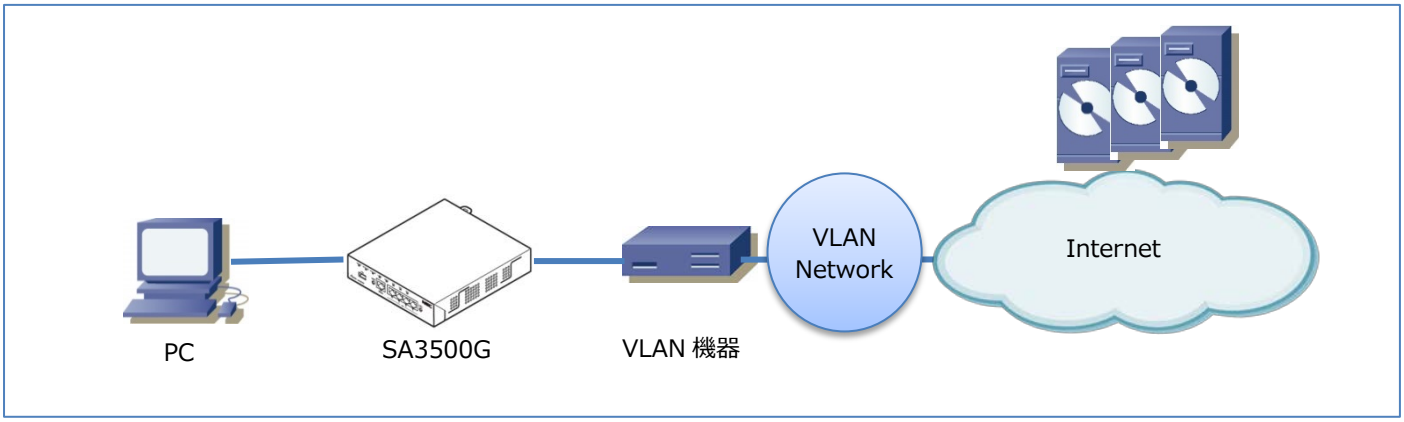
本製品のセキュリティ・スキャン機能は、VPN パケットに対応していないため、次の構成を推奨します。



8.1.3. **VLAN を使っている**

設置場所

本製品を VLAN のネットワークの外側に設置してください。



8.1.4. 端末を IEEE802.1X で認証している

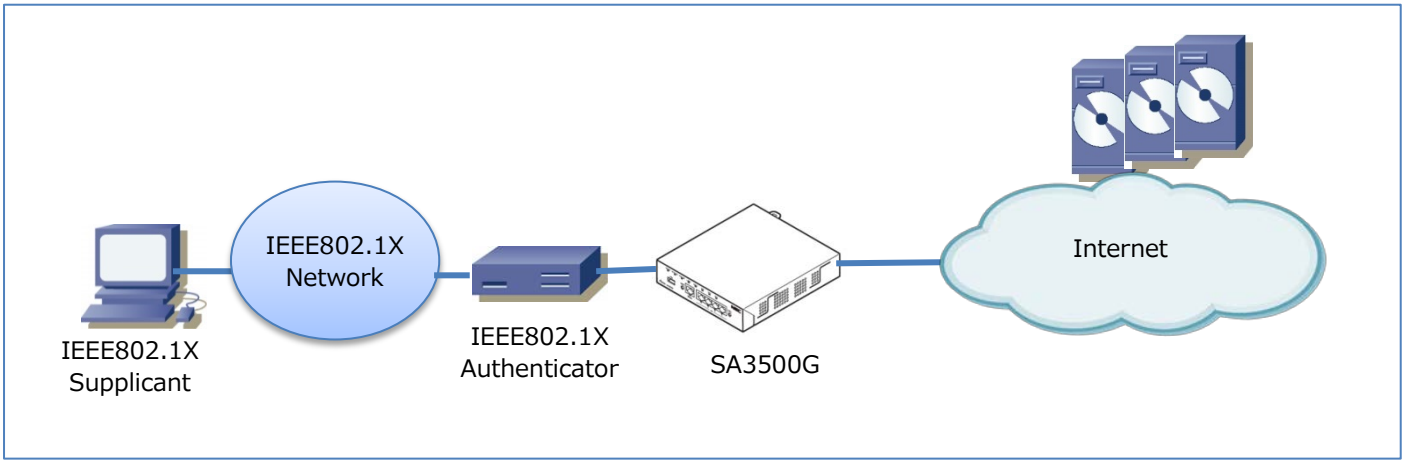
■有線 LAN の場合

設置場所

本製品を IEEE802.1X のネットワークの外側に設置してください。下図に示す構成にしてください。

説明

本製品は、EAPoL フレームおよびマルチキャストの EAP フレームを遮断します。

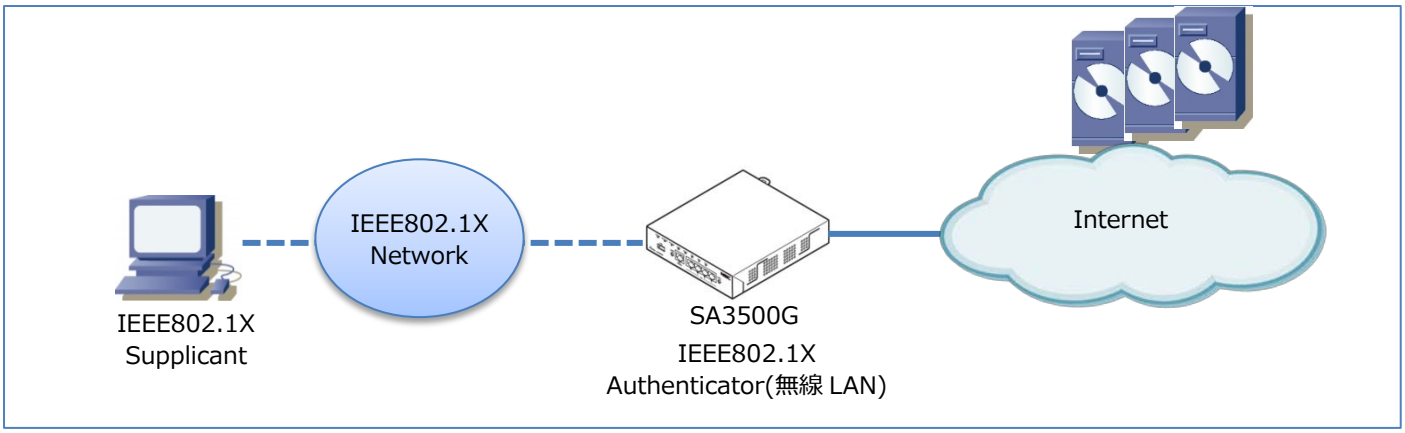


■無線 LAN の場合

本製品の簡易 RADIUS 機能を使って、以下の構成で設置することができます。

説明

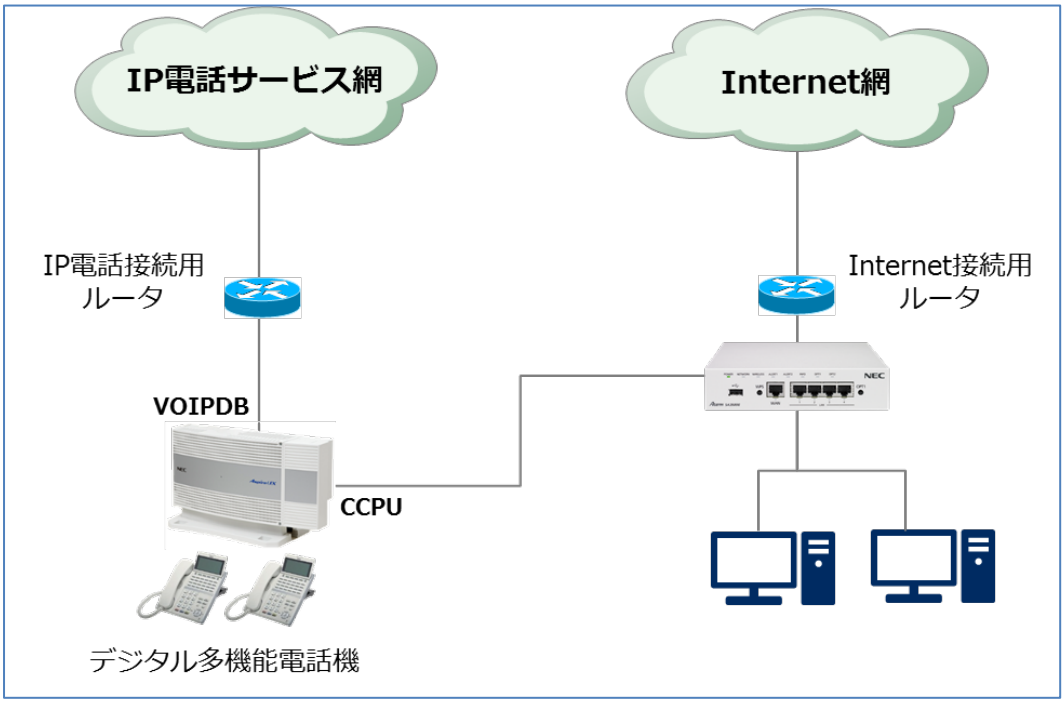
本製品は IEEE802.1X の無線 LAN の Authenticator として動作します。



8.1.5. **Aspire と本製品の接続について**

Aspire を本製品に接続する場合、本製品はブリッジモードで運用してください。Aspire が IP 電話のサーバに Aspire の IP アドレスや音声通信に利用するポート番号を登録するときに、Aspire に NAT 越えの機能が必要となります。本製品をルータモードで運用される場合には Aspire の設定によっては、本製品の NAT を越えられない場合があります。

また、本製品のセキュリティ・スキャン機能によって、音切れなどの IP 電話の通話に影響が出る場合があります。以下の図に示す構成のようにデータ通信を利用するポートと IP 電話を利用するポートは分けて接続してください。



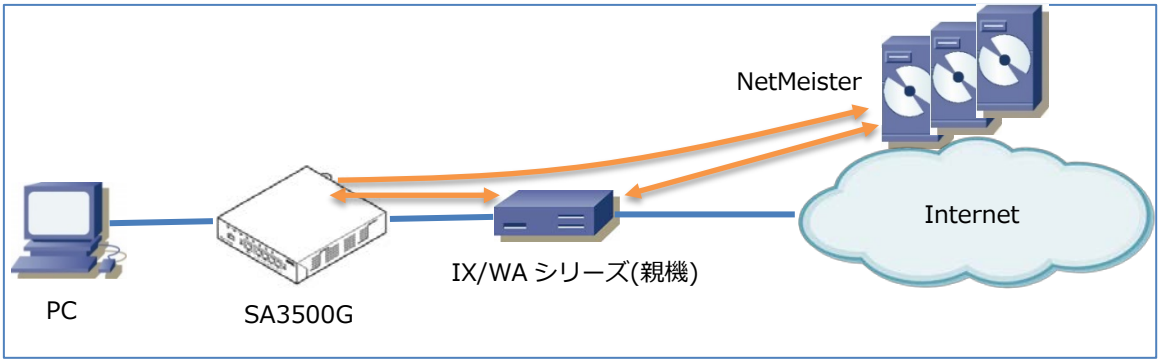
8.1.6. 1 台の親機を使用して NetMeister と接続する

設置場所

本製品を UNIVERGE IX シリーズや UNIVERGE WA シリーズの LAN 側に設置してください。

説明

UNIVERGE IX シリーズや UNIVERGE WA シリーズのルータを親機として NetMeister を使用します。



8.1.7. 2 台の親機を使用して NetMeister と接続する

本製品には NetMeister の親機を 2 台まで設定できます。

2 台の親機を設定することで NetMeister との接続を冗長化することができます。

設置場所

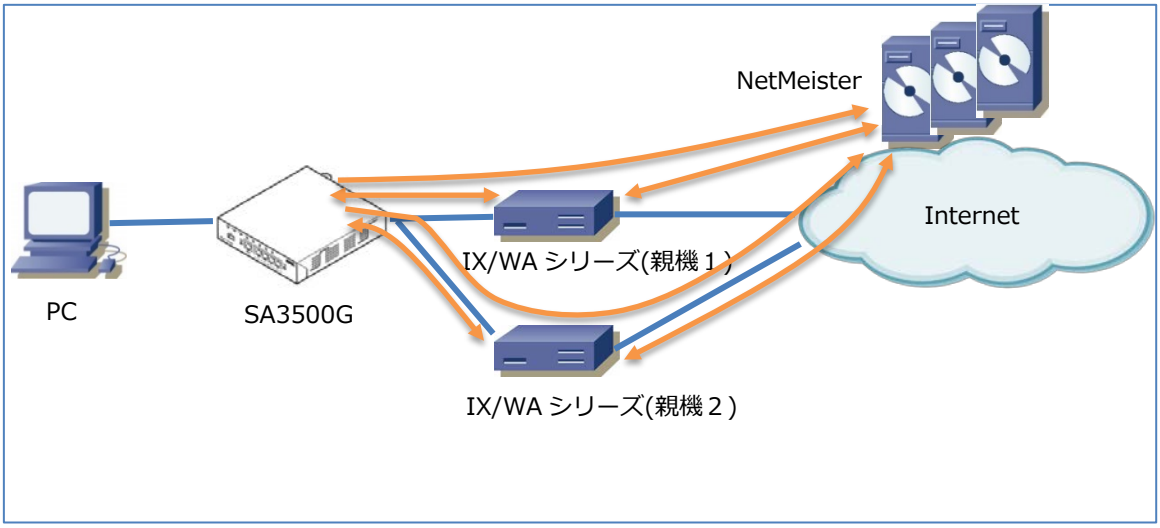
本製品を 2 台の UNIVERGE IX シリーズや UNIVERGE WA シリーズの LAN 側に設置してください。

説明

2 台の UNIVERGE IX シリーズや UNIVERGE WA シリーズのルータを親機として NetMeister を使用します。

2 台の親機の NetMeister に関する設定は、同一である必要があります。

NetMeister 上での操作によるアクション実行は、親機 1 または親機 2 のどちらかを経由して行います。



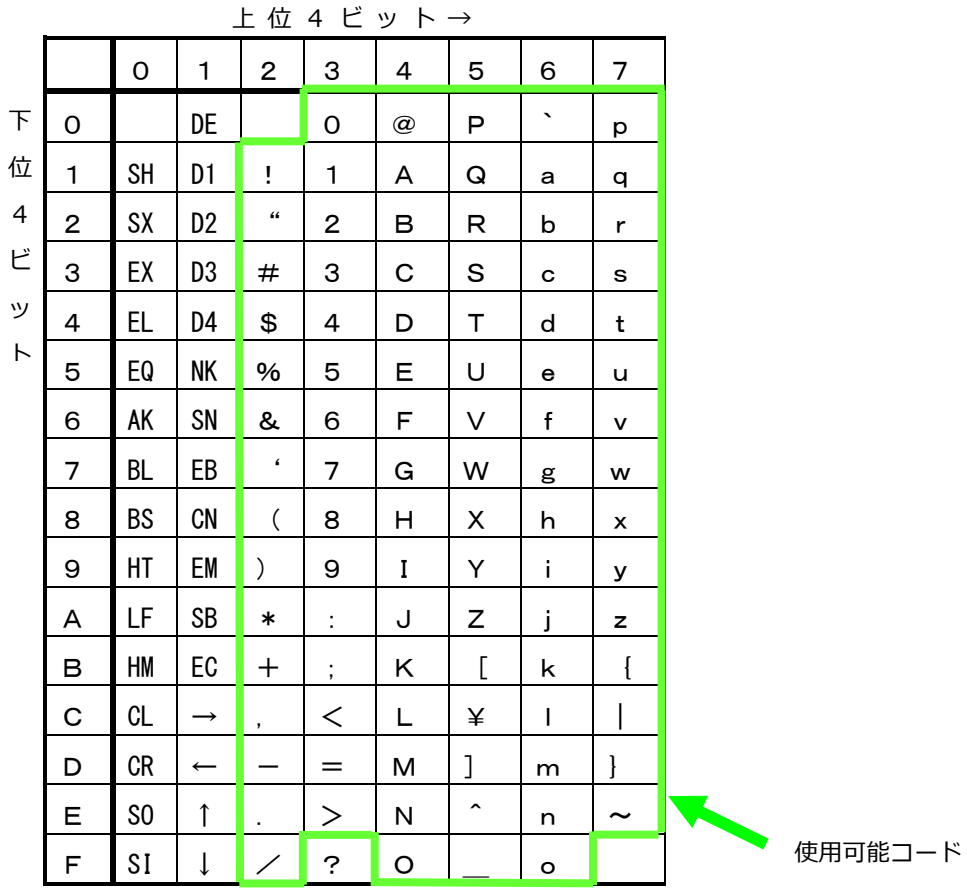
9. 用語集

9.1. 用語集

本製品や本マニュアルで、通常と異なる意味で使用している語句について説明します。

用語	説明
アクティベーション	本製品のセキュリティ・スキャン機能を有効にする処理です。 初回起動時、本製品のライセンスをライセンスサーバに通知することで本製品のセキュリティ・スキャン機能を使用できます。この一連の処理が終了した状態を「アクティベーション済み」と呼びます。 （ライセンスの利用開始日は、アクティベーションが成功した日または、本製品納入後 31 日を経過したいずれかの早い日です。）
個別許可	特定の通信を脅威検出対象外に設定する機能の名称です。 許可リストとして動作します。
シグネチャ	本製品が各種脅威を検出する際に使用するデータベース（ウイルスのリストや危険な Web サイトのリストなど）です。 本製品は、シグネチャを定期的に更新し、常に最新の情報を使用します。シグネチャは定義ファイルと呼ばれることがあります。 シグネチャは次の機能で使用します。 アンチウイルス（AV）、不正侵入防止（IPS）、Web ガード（WG）、アプリケーションガード（APG）
セキュリティ・スキャン機能	本製品のセキュリティ機能の名称です。 セキュリティ・スキャン機能として、次の機能を持ちます。 ファイアウォール（FW）、アンチウイルス（AV）、不正侵入防止（IPS）、Web ガード（WG）、URL フィルタリング（UF）、URL キーワードフィルタリング（KF）、アプリケーションガード（APG）
設定 Web	本製品の設定用画面の名称です。 パソコンなどの Web ブラウザで http://169.254.254.11 にアクセスすると、設定 Web が開きます。
トラフィック	本書では、フレーム、パケットの総称として使用しています。 一般的には PDU（パケット・データ・ユニット）と呼ばれます。
ノード	ネットワーク機器です。 パソコン、スマートフォン、スイッチ、ルータなどを指します。
パケット	本書では、OSI 参照モデルのレイヤ 3 のトラフィックの総称として使用しています。
フレーム	本書では、OSI 参照モデルのレイヤ 2 のトラフィックの総称として使用しています。
ライセンス	本製品のセキュリティ・スキャン機能を利用するためのライセンスです。
Aspire	本書では、UNIVERGE Aspire UX および UNIVERGE Aspire WX を総称し、Aspire の表記としています。

9.2. **ASCII コード表**



下位4ビット ＼ 上位4ビット →	0	1	2	3	4	5	6	7
0		DE		0	@	P	`	p
1	SH	D1	!	1	A	Q	a	q
2	SX	D2	“	2	B	R	b	r
3	EX	D3	#	3	C	S	c	s
4	EL	D4	$	4	D	T	d	t
5	EQ	NK	%	5	E	U	e	u
6	AK	SN	&	6	F	V	f	v
7	BL	EB	‘	7	G	W	g	w
8	BS	CN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SB	*	:	J	Z	j	z
B	HM	EC	+	;	K	[	k	{
C	CL	→	,	<	L	¥	l	|
D	CR	←	−	=	M	]	m	}
E	SO	↑	.	>	N	^	n	~
F	SI	↓	／	?	O	_	o	

例：0x35　→　5

0x21　→　!

0x0D　→　CR（復帰）

0x0A　→　LF（改行）

0x09　→　TAB（水平タブ）

0x03　→　CTL+C (コントロール+C)

0x1B　→　ESC (エスケープ)

0x20　→　SPC (スペース)

10. お問い合わせ窓口

Aterm Biz製品の機能、操作、設定、故障診断など一般的なご質問は、Aterm Bizインフォメーションセンターへお問い合わせください。

Aterm Biz インフォメーションセンター

製品情報サイト	https://www.necplatforms.co.jp/product/security_ap/
ナビダイヤル	TEL：0570-025225（携帯電話からも同一番号です。） ※通話料はお客様ご負担です。
お問い合わせ受付時間	午前9時～午前12時、午後1時～午後5時（月～金曜日） （土日、祝日、年末年始、当社の休日、システムメンテナンス時は休ませていただきます。）

※サービス内容などは予告なく変更させていただく場合があります。

※一部のIP 回線(050 番号) からはつながらない場合があります。つながらない場合は、携帯電話など、別の通信手段でおかけください。

本製品の機能や取り扱い方法などでご不明の点がありましたら、Web からお問い合わせいただくこともできます。

https://contact.nec.com/http-www.necplatforms.co.jp_tb_root_security_ap/index.html

から、手順にしたがってお問い合わせ内容を入力してください。

お問い合わせになるときには、次のことをお伝えください。

- ●お名前
- ●電話番号
- ●本製品の機種名：Aterm SA3500G
- ●製品型番　　：ZA-SA3500G/
- ●製造番号（15ケタ）
- ●デバイスID（16ケタ）
- ●詳しい症状、ランプの点灯状況や、メッセージが表示されていたらその内容など

※回線接続の条件などについては、各通信事業者又はプロバイダにお問い合わせください。

※添付品で不足しているものがありましたら、お買い上げの販売店にご連絡ください。

【個人情報のお取り扱いについて】

当社では、個人情報保護ポリシーを制定し、お客様の個人情報保護に努めております。お客様からご提供いただく情報に含まれるお客様の個人情報は、お客様への連絡やお問い合わせにお答えするために取得し、他の目的に利用することはありません。また、お客様の承諾なく第三者へ個人情報を提供することはありません。ただし、業務を委託するために業務委託先に個人情報を開示する場合があり、その場合には秘密保持条項などを含む契約を締結したうえで委託し、個人情報を適切に管理します。個人情報に関するお問い合わせやご相談がある場合は、ＮＥＣプラットフォームズ株式会社 Aterm Biz（エータームビズ）インフォメーションセンター（☛ 上記）までお願いいたします。

Aterm SA3500G 機能詳細マニュアル
AM1-002926-009

©2016-2020 NEC Platforms, Ltd

2020 年 10 月　第 9.0 版
ＮＥＣプラットフォームズ株式会社

ＮＥＣプラットフォームズ株式会社の許可なく
複製・改版、および複製物を配布することはできません。