NEC

Aterm Biz シリーズ

Aterm SA3500G 機能詳細マニュアル

第 3.0 版　2016 年 11 月
ＮＥＣプラットフォームズ株式会社

※ファームウェア Ver 3.1.35 に基づいて説明しています。

目次

1. はじめに

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、当社では一切責任も負いかねますので、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、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 もしくは 100BASE-TX、100Mbps 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。このため、インターネットへ接続できなくなります。

無線 LAN に関する免責事項

- 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。
- 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。
- 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」とします）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 情報技術装置です。この装置は、家庭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）を有償にて、回収／再資源化しています。
詳細については、こちらのページ
http://jpn.nec.com/eco/ja/recycle/method/it/ (2016 年 11 月現在)
をご覧ください。
（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。）

本製品を廃棄する前に、本製品の初期化を行い、お客様により設定された設定値、および、セキュリティ・スキャン機能のログメッセージ、統計情報を消去してください。(5.6.8 章参照)

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「重要なお知らせ」にてご案内します。

通信中にメンテナンスバージョンアップ機能が動作し始めると、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の発生やパケット通信量超過による速度制限が生じます。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ーへ通知します。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。

本機能の初期値は有効です。本機能に関して許諾いただけない場合は、次ページの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実施しません。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受ける危険性があります。

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について処理します。

- セキュリティ・スキャン機能で使用するシグネチャ（ウイルス情報などの定義ファイル）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の発生したパケット通信量超過による速度制限が生じます。
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をサーバーへ通知します。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、適切に管理します。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に管理します。

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

やむを得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について

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（11 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**

- **RoHS 指令準拠**：RoHS（Restriction of Hazardous Substances）指令とは、電気・電子機器の特定有害物質〔鉛、水銀、カドミウム、六価クロム、ポリ臭化ビフェニル（PBB)、ポリ臭化ジフェニルエーテル（PBDE)〕の使用制限に関する 欧州議会および理事会指令です。
- **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**

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。
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。
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、各社の登録商標、または商標です。

1.12. 安全にお使いいただくために

製品を安全に正しくお使いいただき、お客様や他の人々への危害や、財産への損害を未然に防止するために、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とおりです。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

使用している表示と図記号の意味は次のとおりです。内容をよく理解してから、本文をお読みください。


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


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

 警　告

電源

- 日本国内 AC100V 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。

こんなときには

- 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。

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。

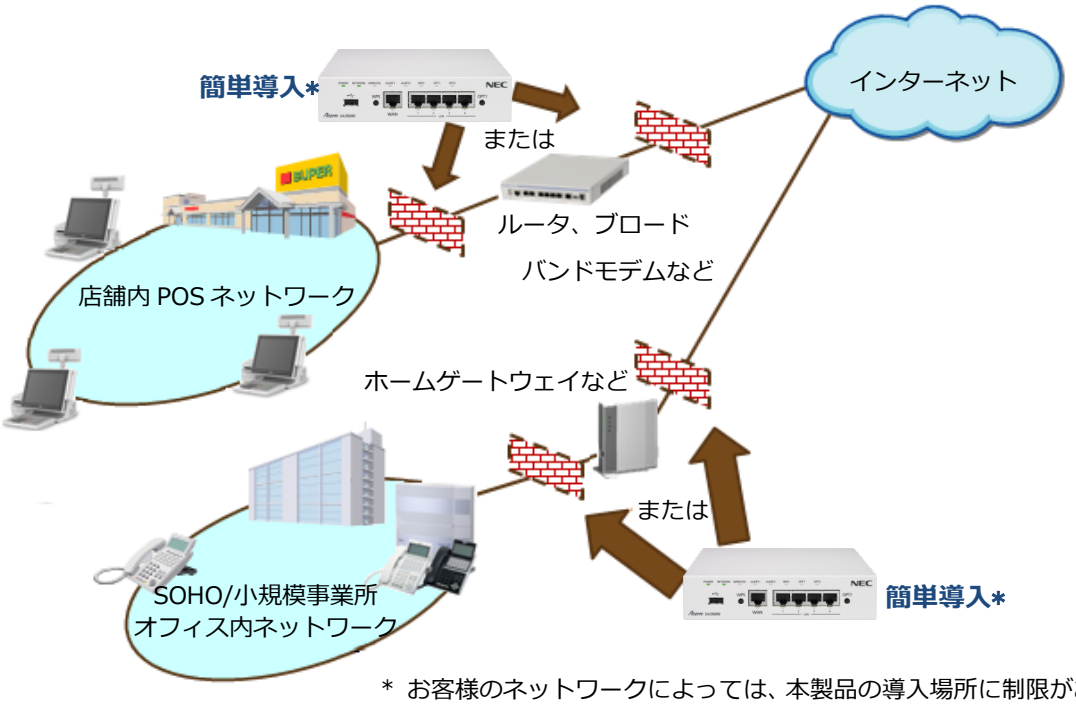
セキュリティ対策をほどこさず、あるいは、無線 LAN の仕様上やむをえない事情によりセキュリティの問題が発生してしまった場合、当社はこれによって生じた損害に対する責任は一切負いかねますのであらかじめご了承ください。

2. 製品について

本製品は、アンチウイルス機能、不正侵入防止（IPS）機能などを搭載した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（~50 名程度のネットワーク）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。



* お客様のネットワークによっては、本製品の導入場所に制限があります。
詳細は、3.2 章を参照してください。

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（ブリッジモード）

ブリッジモードでは、本装置は既存の社内ネットワーク構成を変えることなく、簡単に設置できます。

本製品の設定は Web ブラウザを用いたシンプルな 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のない方でも、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。本装置は高速セキュリティエンジンを採用することで約 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 を組み込んだシグネチャ（ウイルス等定義ファイル）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。

✓ お知らせ機能

脅威を検出した場合やライセンス切れ警告、ファームウェアアップデートなどの処置が必要な場合には、Web ブラウザ利用時はブラウザ上に表示、本体ランプでの表示、メールでの通知などができます。

✓ UNIVERGE Aspire UX 連携

オフィスコミュニケーションゲートウェイ UNIVERGE Aspire UX（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・ライセンスの有効状態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

設定ウィザード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）でセキュリティログの閲覧やホワイトリスト作成ができます。

脅威をブロックした件数などを月別、週別、日別のセキュリティ統計として閲覧することができます。

---

[1]当社の試験環境にて測定した結果です。

[2]株式会社ラック社について

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全ての支援を先端の 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。

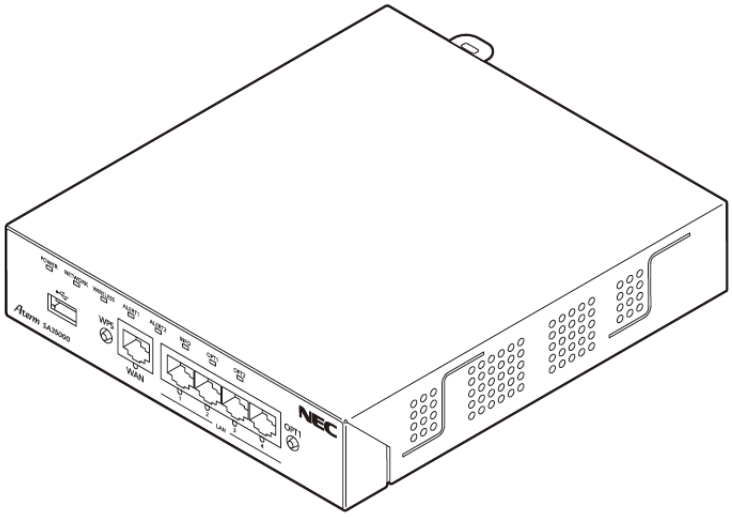
詳細は株式会社ラックの HP でご確認ください。（http://www.lac.co.jp/）

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

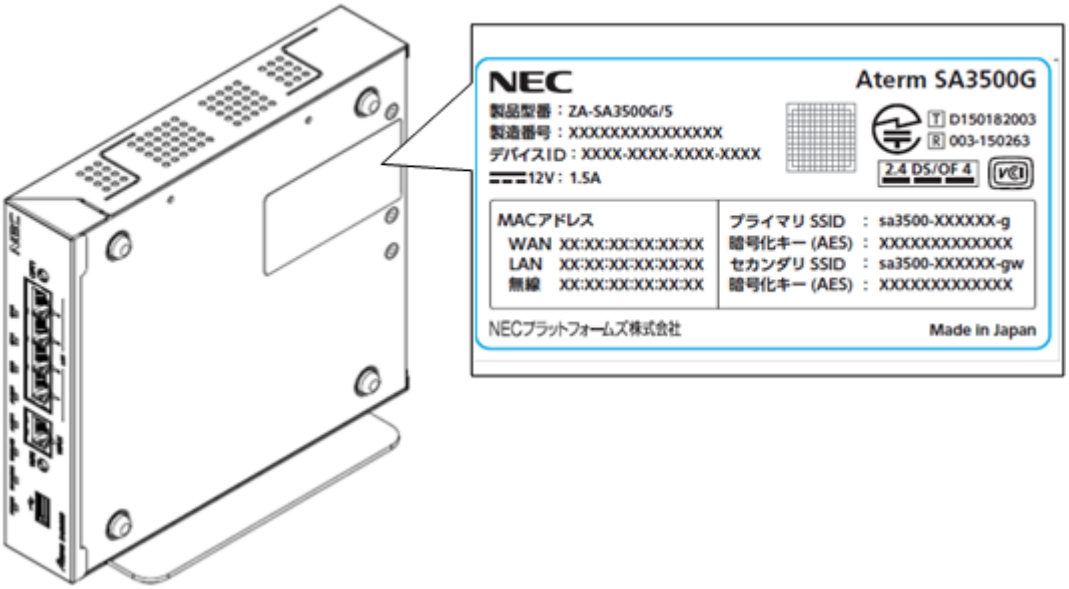
2.3. 製品仕様

2.3.1. 製品外観

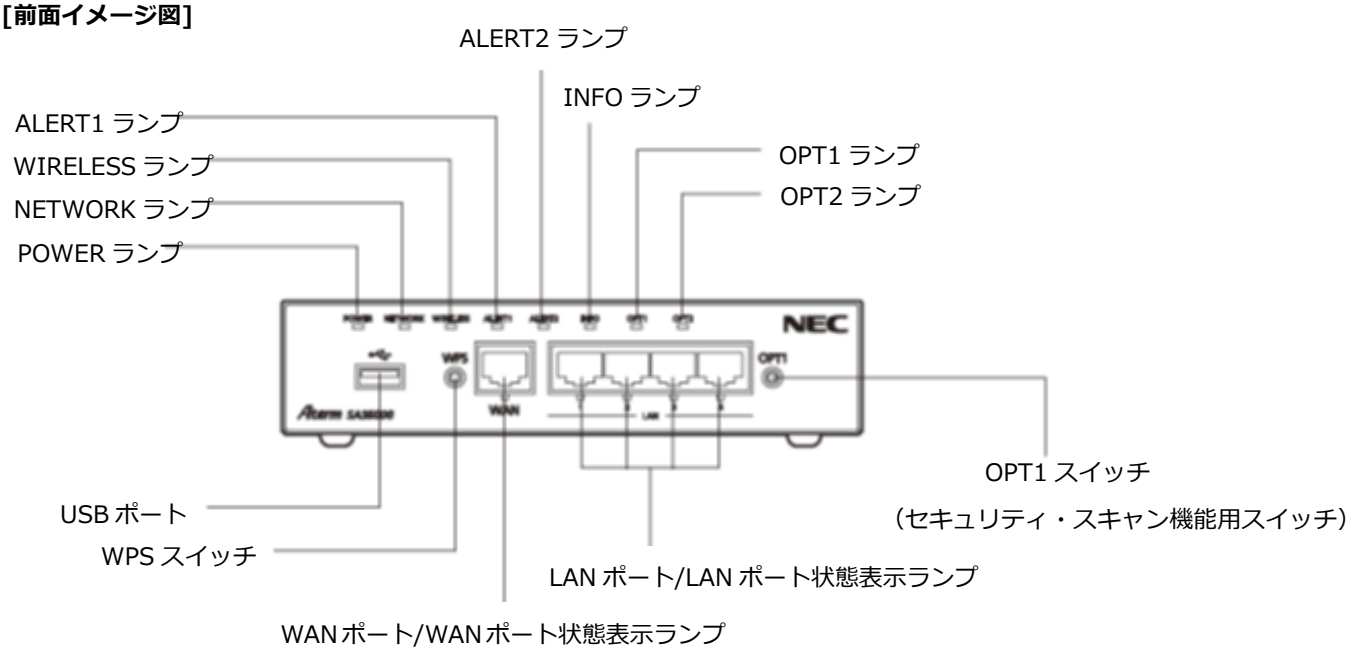
[斜視イメージ図]



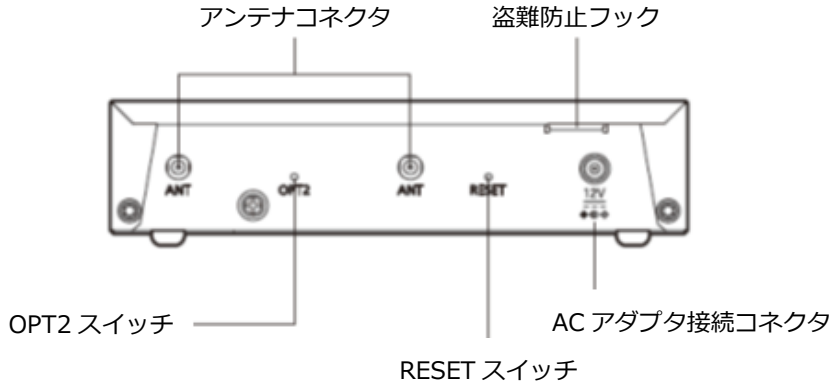
[底面イメージ図（スタンド取り付け時）]



[前面イメージ図]



[背面イメージ図]



2.3.2. **基本仕様**

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		ログファイル保存などに使用 ※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）		
PC 同時接続台数		50 台以下推奨 ※3		
動作保証環境		温度：0~40℃ 湿度：10~90%		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：AC100V ± 10% 50Hz/60Hz 出力：DC12V/2.0A AC インレットタイプ		添付品
消費電力		最大 21W		
本体質量		約 1Kg		AC アダプタを除く
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		
		J60950 準拠		
		鉛フリー		
		RoHS 対応		

※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 将来サポート予定です。

※3 ルータモードでの DHCP の IP アドレス払出し数が最大 50 個、お知らせ機能のユーザーへの脅威検出通知宛先登録が最大 50 宛先です。

2.3.3. **ランプ表示**

表示名称	ランプ表示	機能	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 メモリ書き込み中の状態	装置の電源を OFF 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 ※1 （ブリッジ モード時）	橙点灯	IP アドレス取得済の状態	
	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 ※2	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 ※3	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 ※3	
	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
	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切れの状態	
	赤点滅	セキュリティ・スキャン機能のライセンス期限切れまで 30 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	正常終了後は再起動する 失敗した場合は橙点灯に戻る
	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 ※4	緑点灯	IPsec 通信可能な状態	IPsec SA 確立済み
	橙点灯	IPsec 接続処理中の状態	IPsec SA 未確立
	消灯	IPsec を使用していない状態	
OPT2		未使用	
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	
	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	
	消灯	LAN ポートのリンクが確立していない状態	

※1 ファームウェアバージョン 3.0.1 をご利用の場合、NETWORK ランプ（ブリッジモード時）は、橙点灯は緑点灯に、橙点滅は緑点滅に読み替えてください。

※2 無線 LAN はルータモード時の機能です。

※3 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のでご安心ください。

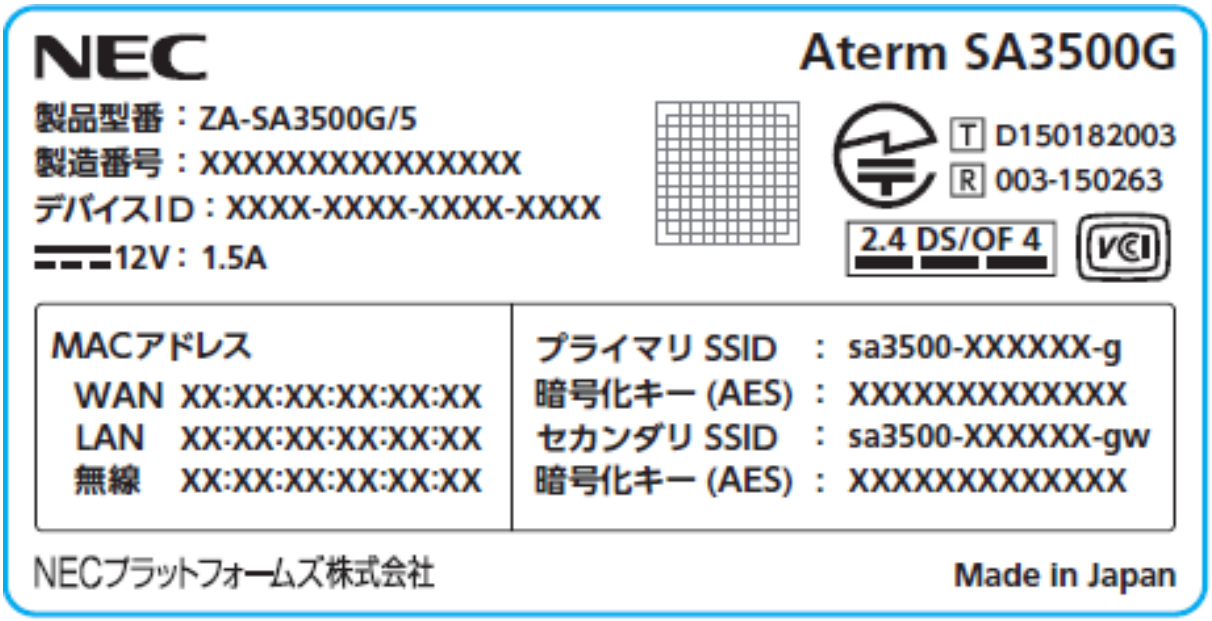
※4 IPsec はルータモード時の機能です。

[メモ]

電源投入~システム起動前は、すべてのランプが緑点灯します。

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

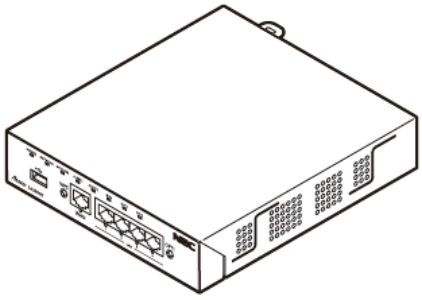
ZA-SA3500G/7　：7 年ライセンス付き製品

2.4. **構成品**

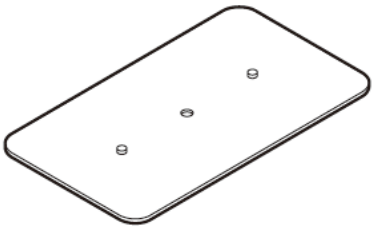
構成品が揃っていることを確認してください。

■構成品

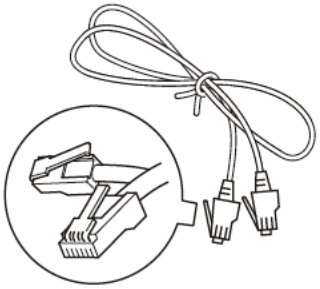
□SA3500G



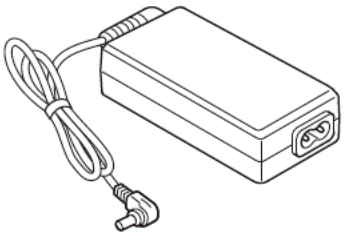
□スタンド



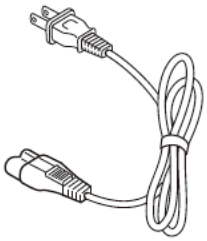
□Ethernet ケーブル（ストレート）
（約 2m）



□AC アダプタ

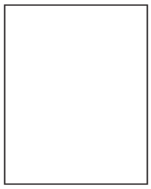


□電源コード

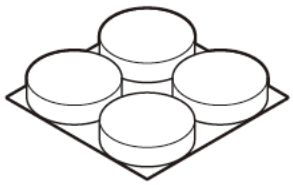


□取扱説明書

□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

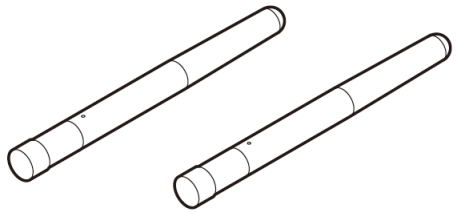
AC アダプタおよび電源コードは必ず本製品に添付のものをお使いください。また、添付の AC アダプタは、他の製品に使用しないでください。

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。

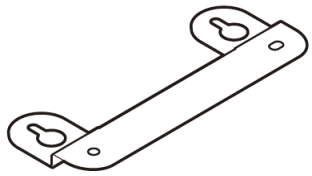
■オプション

□外付けアンテナ（2 本 1 組）（品番：ZA-SA/AN1）

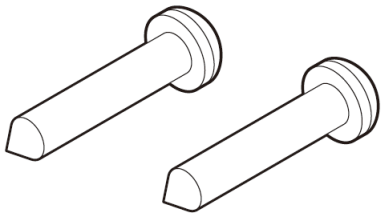


□壁掛けキット（品番：ZA-SA/MK1）

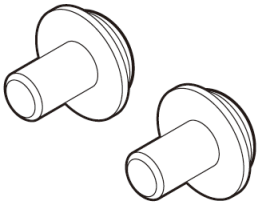
・壁掛け金具（1 個）



・木ネジ（2 本）

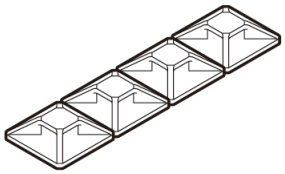


・壁掛け金具固定ネジ（2 本）

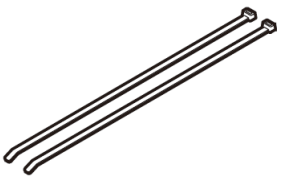


□USB クランプキット（品番：ZA-SA/UC1）

・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（Ver3.1.26 以降） ● Aspire UX との連携 ● パトライトとの連携（Ver3.1.26 以降） ● セキュリティ情報の自動アップデート
ブリッジ機能	● トランスペアレントブリッジ機能
IPv4 ルータ機能 （Ver3.1.26 以降）	● ルータ機能 ● NAT/NAPT ● DHCP クライアント/DHCP サーバー ● PPPoE ● IP パケットフィルタリング ● IPsec/IKEv1
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 プロキシサーバー（Ver3.1.26 以降） ● SNMPv1/SNMPv2c（Ver3.1.26 以降）
無線 LAN 機能 （Ver3.1.26 以降）	● IEEE802.11b/g/n(2.4G) ● WPS
USB 機能	（将来サポート予定）

※ブリッジ機能とルータ機能は、同時動作しません。

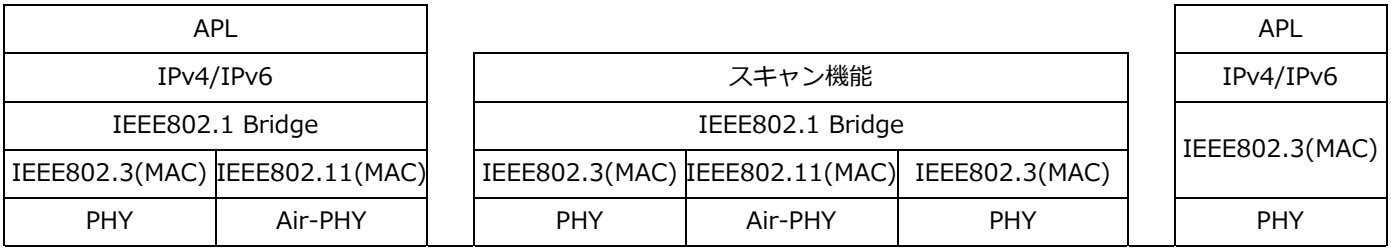
※ファイアウォール（FW）機能、SNMP 機能、および、無線 LAN 機能は、ルータモードでのみ動作します。（Ver3.1.26 以降）

3.1. プロトコルスタック

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。

※ PPPoE（PPP）フレームに対応しています。

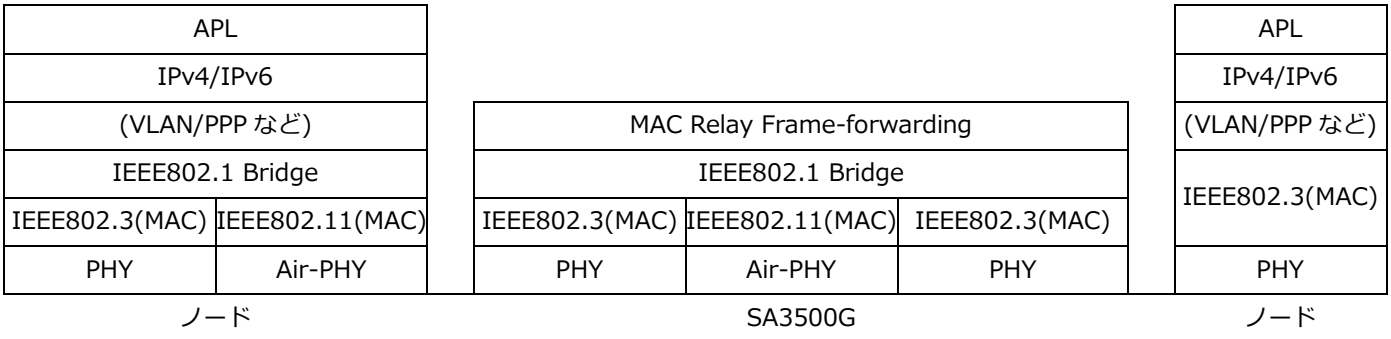
※ VLAN フレームに対応しています。

※ 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]

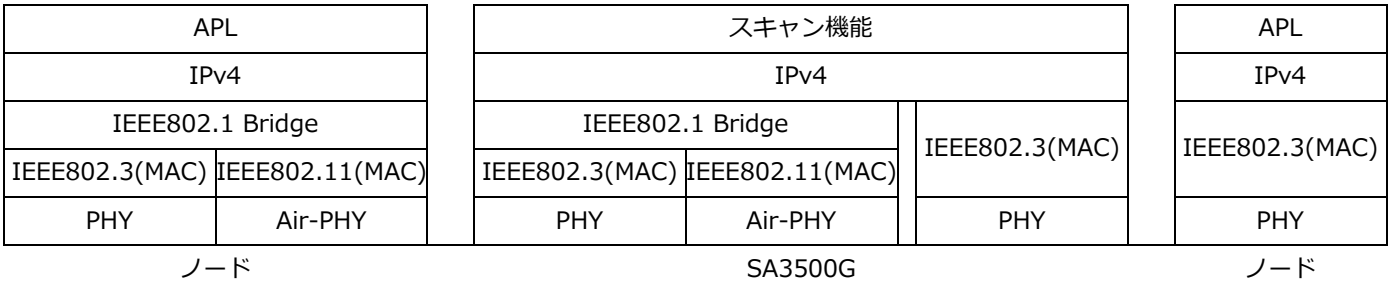


※ 下記 MAC フレームは透過しません。

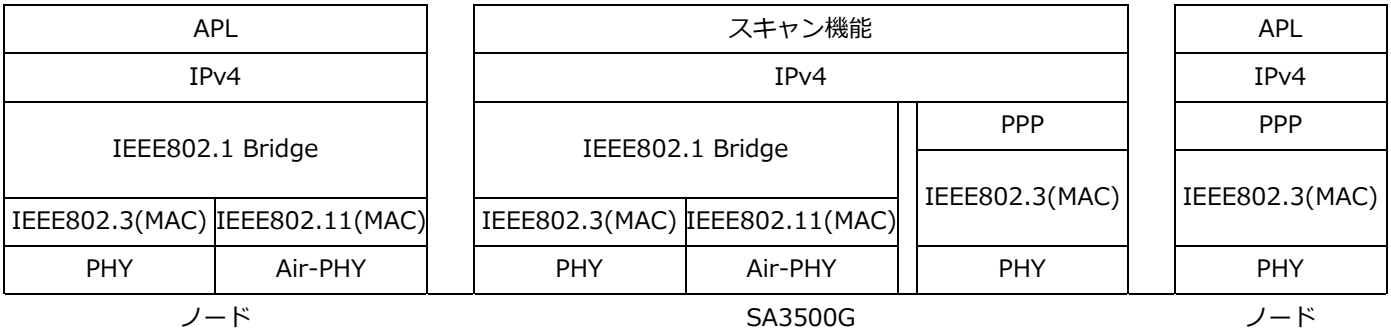
01-80-C2-00-00-03 IEEE802.1X EAPoL Frame

3.1.2. **ルータモード**

[DHCP、または固定 IP で WAN IP を設定の場合]



[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. **動作可能なネットワーク**

本製品を使用するは、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。
  - ・本製品が送出する IP パケットは次のとおりです。[5]
    必須トラフィック：TCP port=80（HTTP）、TCP port=443（HTTPS）、TCP port=8080、UDP port=53（DNS）
    他のトラフィック：UDP port=67（DHCP）、UDP port=123（NTP）
- 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。

3.2.1. **ブリッジモード**

ネットワーク例（ここでは、本製品のアップリンク側を WAN 側、本製品のダウンリンク側を LAN 側と呼びます）

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 IPv4 プロトコルが必要です。
IEEE802.1X でノードを認証している	○＊	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 IEEE802.1X 機能をサポートしていません。 ・本製品は EAPoL/EAP フレームを透過しません。

＊8.1 章にネットワーク接続構成例を載せています。

[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。

3.2.2. **ルータモード**

ネットワーク例（ここでは、本製品のアップリンク側を WAN 側、本製品のダウンリンク側を LAN 側と呼びます）

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 IPv4 プロトコルが必要です。
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 でノードを認証している	○＊	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 IEEE802.1X 機能をサポートしていません。 ・本製品は EAPoL/EAP フレームを透過しません。
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 章にネットワーク接続構成例を載せています。

3.3. **セキュリティ・スキャン機能**

[Ver3.1.26 での追加機能]

- ファイアウォール（FW）

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
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
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

*1 ファイアウォール（FW）は、ルータモード時の機能です。

*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）、WRL 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。

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、IPv4 または IPv6 のパケットです。 ● PPPoE（PPP）フレームに対応しています。 ● VLAN 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
ルータモード	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。

3.3.3. **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、ノード（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、ノードごとのトラフィックを監視します。このため、ノード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. **サーバーとの連携**

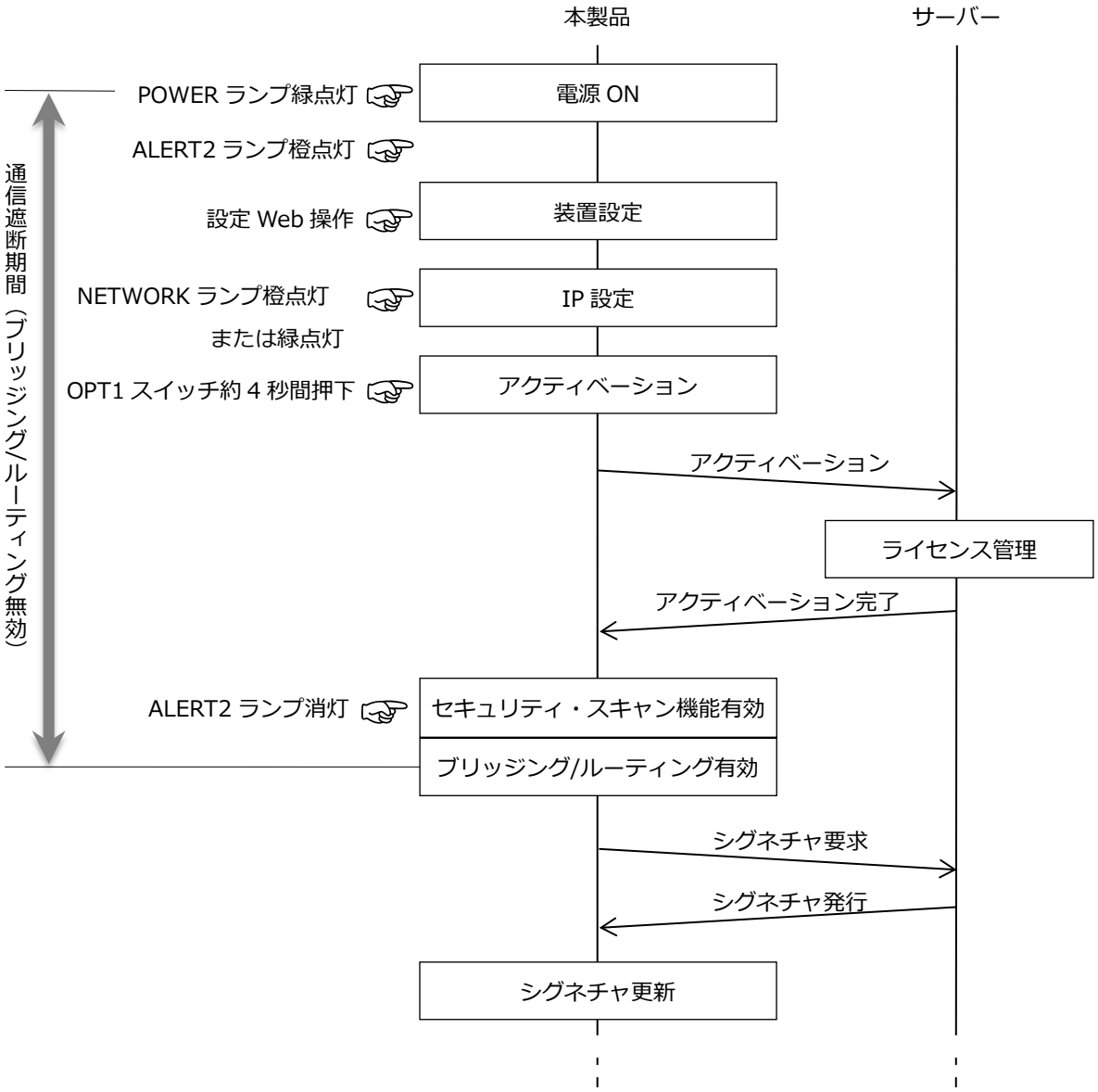
本製品は、サーバーと連携して以下を行います。

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。 ライセンス契約期間は、1 年、および複数年契約の製品を用意しています。 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ーにアクセスします。これにより、ライセンスサーバーが本製品の管理を開始します。（アクティベーション） ライセンスサーバー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ー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 ランプで確認できます。	
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]

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 秒間押下したら、放します。
   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すると、本製品のセキュリティ・スキャン機能を起動します。
5. セキュリティ・スキャン機能の起動が完了[7]すると 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。[8]

※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。

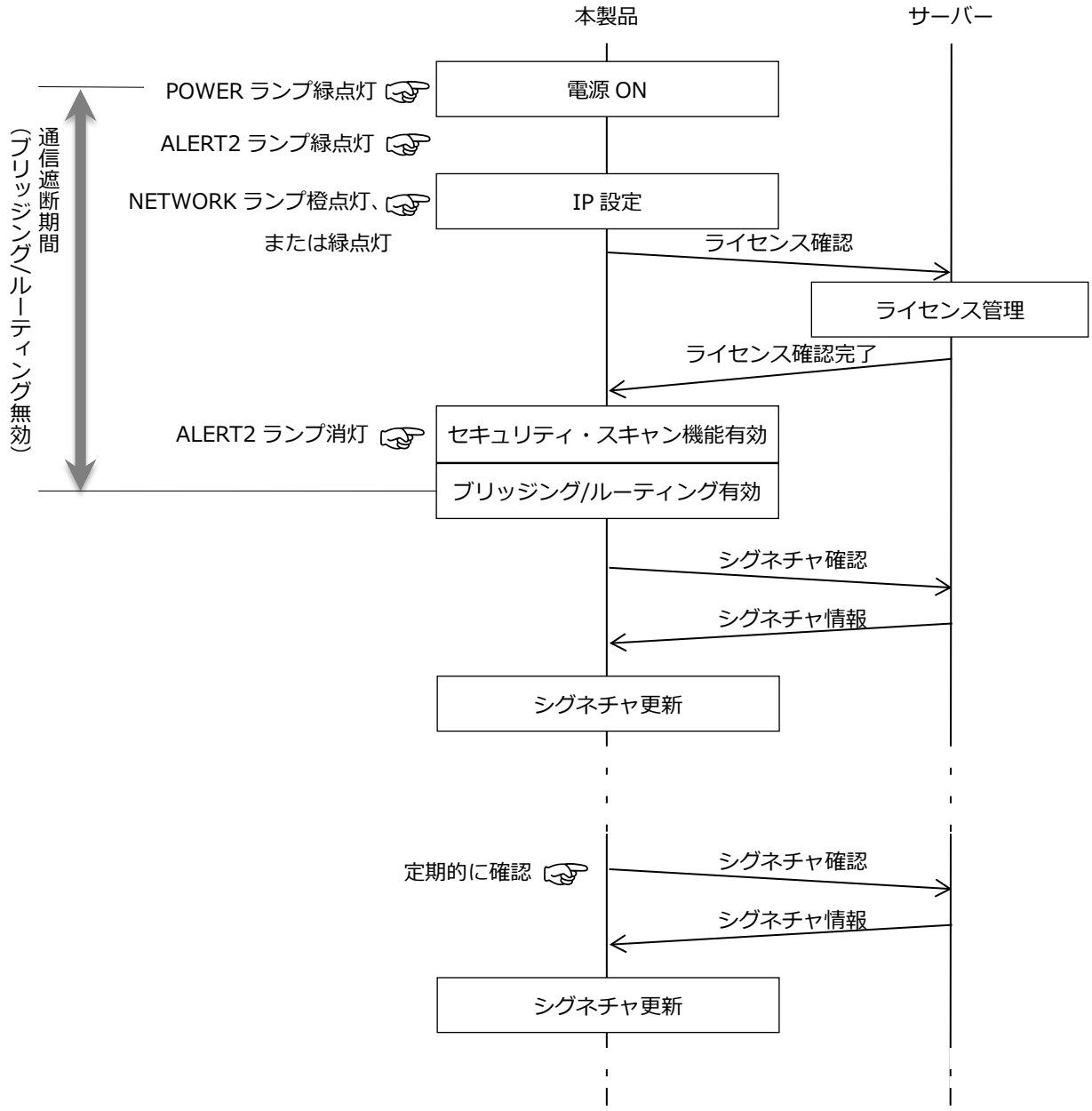
[6] ALERT2 ランプの橙点灯は、アクティベーション処理が終わっていないことを表します。

[7] 数分かかることがあります。

[8] 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。

[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。サーバー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[9]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。
   このタイミングで、セキュリティ・スキャン機能を起動します。
   同時にライセンスの確認処理を実施します。
3. セキュリティ・スキャン機能の起動が完了[10]すると 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。

[9] 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。

[10] 数分かかることがあります。

[ライセンス切れ時の動作]

- ライセンスが切れると、本製品のブリッジング機能/ルーティング機能を無効にします。
  (セキュリティ確保のために WAN⇔LAN 間の通信を遮断します)

[ライセンス切れの判定について]

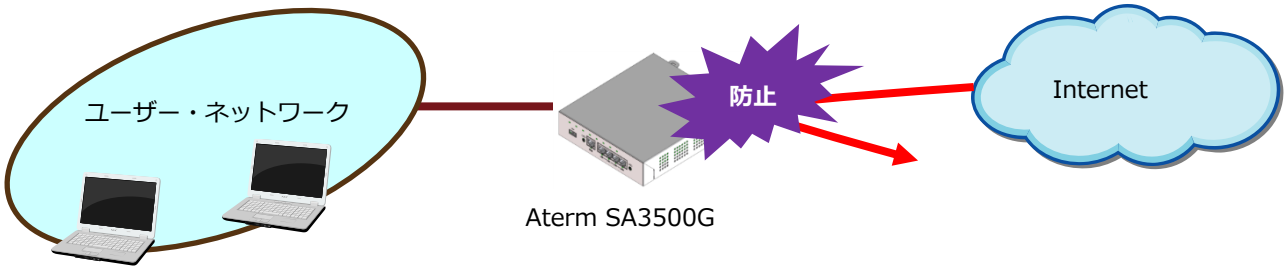
- 次のどちらかの場合にライセンス切れと判定します。
  ・本製品に設定された時刻がライセンス期限を過ぎた場合。
  ・本製品がサーバーにライセンス確認を行った結果、ライセンス期限切れと判定された場合。
  □ライセンス切れ、およびライセンス切れの 30 日前の時刻判定は、本製品に設定された時刻を基準にしています。正しく時刻判定するために、本製品の時刻は実際の時刻に合わせてお使いください。
- ライセンスが切れる 30 日前から、ALERT2 ランプが赤点滅します。
- ライセンスが切れると ALERT2 ランプが赤点灯します。

3.3.5. **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。

また、NAPT 機能により、外部からのアクセスパケットを廃棄します。

※ファイアウォール機能は、ルータモード時のみ動作します。



[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
NAPT により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]

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
ルータモード時にはファイアウォール機能は常時有効です。 Smurf 攻撃、IP スプーフィング攻撃 は以下で停止できます。 「DoS プロテクション」の「機能を使用する」のチェックを外す。（5.8.2 章参照）	

3.3.6. **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。[11]

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。

[検出対象]

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

[検出対象のファイルタイプ]

exe, dll, com, elf, scr, js

[検出対象の圧縮ファイル]

gz, zip, rar, jar, apk

[11] 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）

[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]

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 UX 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 スイッチ押下 ・設定 Web でセキュリティログを閲覧

*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：設定 Web で設定が必要です。

*3：Aspire UX 側の設定が必要です。

[セキュリティ機能の停止方法]

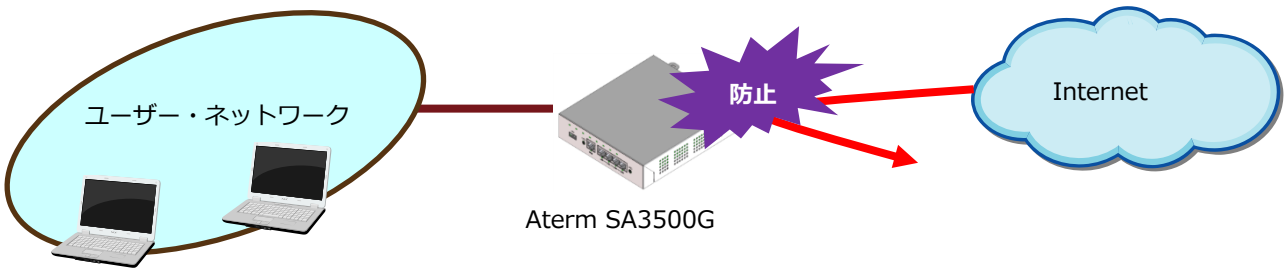
正常なファイルを脅威と誤検出する際は、次の方法により一時的に機能を停止してください。

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（5.8.3 章参照）	無効に変更した場合、アンチウイルス機能は停止します

3.3.7. **不正侵入防止（IPS）**

DoS 攻撃などのネットワーク異常を検知し、異常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]

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。

[セキュリティ機能の停止方法]

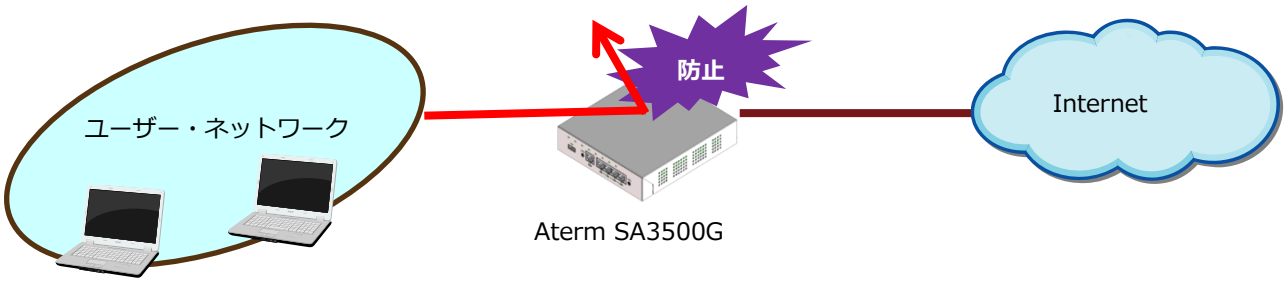
外部からの正常なアクセスを脅威と誤検出する際は、次の方法により一時的に機能を停止してください。

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。（5.8.4 章参照）	無効に変更した場合、不正侵入防止機能は停止します。

3.3.8. **Web ガード（WG）**

最新のシグネチャにより、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

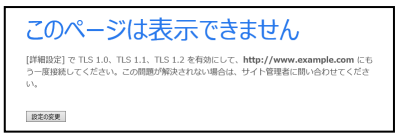
※HTTP1.0 は、検出できない場合があります。

※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]

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 UX 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 スイッチ押下 ●設定 Web でセキュリティログを閲覧 ・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。
*4：Aspire UX 側の設定が必要です。

[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。

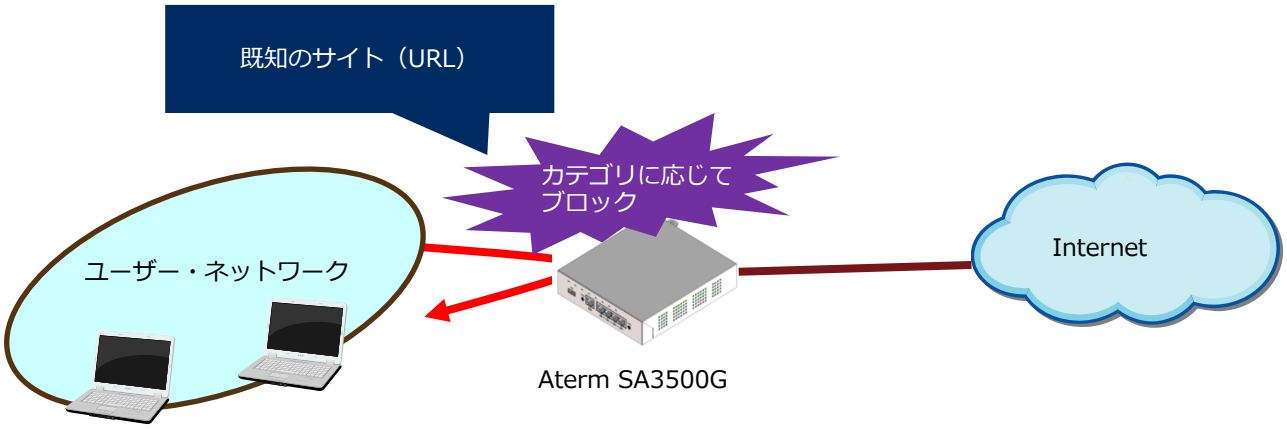
停止方法	備考
「Web ガード設定」の「機能を使用する」のチェックを外し、無効に変更する。（5.8.5 章参照）	無効に変更した場合、Web ガード機能は停止します。

[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。

3.3.9. 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。
初期値は、すべてのカテゴリで「許可」（ブロックしない）に設定しています。

※TCP port＝8080 が通信できる環境が必須です。

[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]

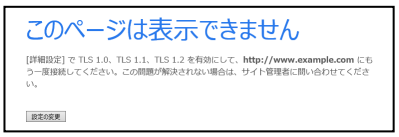
プロトコル	説明
HTTP	検出対象のポート番号　　：80 検出対象の HTTP メソッド　：GET, POST
HTTPS	検出対象のポート番号　　：443 検出対象の HTTP メソッド　：GET, POST

※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]

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) *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。

[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（5.8.6 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。（5.8.6 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。 ・機能を無効に変更した場合、URL フィルタリング機能は停止します。

[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。

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.79 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.16 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.37～No.43 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.17～No.20 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.21～No.23 と No.27～No.32 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 Porn	[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	児童ポルノ Child 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。
3	性教育 Sex Education	[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	アダルトサイト Adult Others	[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	ギャンブル Gambling	[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	公営ギャンブル Official Gambling Business	[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	暴力的なサイト Violent 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。
8	残忍なスポーツ(ハンティング等) Brutal Sports	[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	アルコール飲料 Alcohol Drinks	[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	たばこ 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。
11	マリファナ Marijuana	[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。
12	ドラッグ 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。

13	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。
14	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。
15	違法行為 Other Illegal 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。
16	学業不正 School Cheating	[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。
17	チャットルーム Chat Room and Dating	[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。
18	ニュースグループ、フォーラム、掲示板 Newsgroup, Forums and Bulletin Boards	[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。
19	ブログと個人サイト Blog and Personal Web	[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。
20	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。
21	クラブ Club	[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。
22	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。
23	クーポン Coupons and Money-saving	[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。
24	教育機関 Education	
25	wiki、辞書 Reference	
26	オンライン教育 Streaming Education	
27	エンターテインメント General Entertainment	[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。
28	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。
29	コミック、アニメ Comics, Cartoons 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。
30	ダウンロードサイト Download Sites	[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。
31	P2P P2P	[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。
32	ストリーミングメディア Streaming Media	[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。

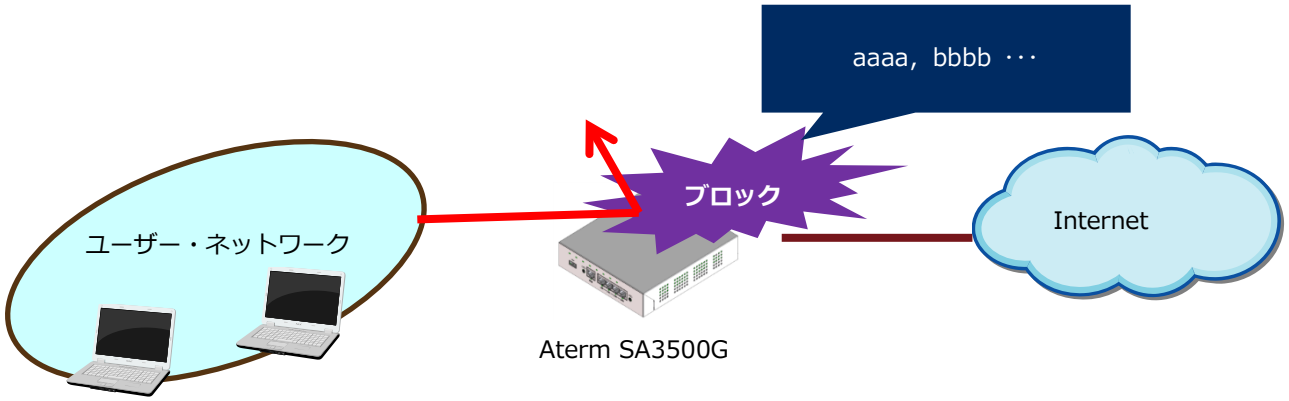
33	Web メール Web Mail	
34	オンライン共有、ストレージ Online Sharing and Storage	
35	プロキシ、アノニマイザー Proxy and Anonymizers	
36	コンテンツサーバー Content Server	
37	フィッシング詐欺 Phishing and Fraud	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
38	マルウェア Malware	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
39	BlackHat SEO サイト BlackHat SEO Sites	[危険サイトカテゴリ]を[ブロックする]設定時に自動選択されます。
40	ハッキング Hacking Websites	[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。
41	ボットネット Botnets	[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。
42	その他の危険サイト Other Malicious Web	[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。
43	危険アプリケーション 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。
44	広告 Advertising and Popup	
45	リダイレクトページ URL Translation	
46	ビジネス Business	
47	金融、保険 Finance and Insurance	
48	建築 Construction and Building	
49	農業、放牧 Agriculture and Pasturage	
50	ロジスティクス Freight and Logistics	
51	電子マネーシステム Electronic Money Systems	
52	政治組織 Politics	
53	軍隊関連 Military	

53	政府 Government	
55	IT General IT	
56	健康、医学 Health and Medicine	
57	宗教 Global Religion	
58	数秘術 Numerology	
59	スポーツ Sport	
60	旅行 Travel	
61	ファッション、ビューティー Fashion and Beauty	
62	自動車 Automobile and Vehicle	
63	ニュース News	
64	天気 Weather	
65	求人情報 Job Boards	
66	カジュアルライフ Casual Life	
67	芸術、文化 Arts and Culture	
68	飲食物 Drink and Food	
69	イスラムフード Islamic Food	
70	ベビー、妊娠 Baby and Pregnancy	
71	ペット Pets	
72	書籍 Book and Magazine	
73	フィットネス、ジム、スパ Fitness and Recreation	
74	交通情報 Transportation Info	

75	コレクション Collection and Habit	
76	レンタル Rental	
77	ポータル、検索サイト Portals	
78	不明なサイト Misc	
79	プライベート IP アドレス Private IP Address	

3.3.10. **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。
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。[12]

※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]

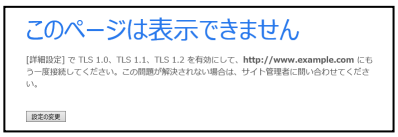
使用可能文字　　：アスキーコードで 0x21-0x7e、マルチバイト文字（ただし、"'`$¥<> を除く）

キーワードの最大サイズ　：128 文字

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。

[脅威を検出した際の動作・通知などの振る舞い]

検出時の動作	検出時の通知方法	検出状態の解除方法
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  ・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	・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：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。

[12] 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。

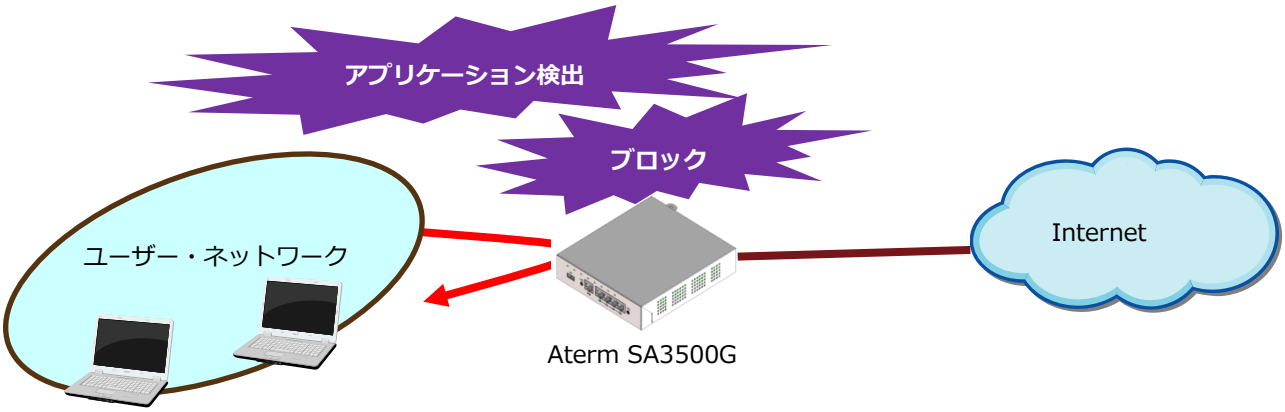
[意図しない検出の停止方法]

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（5.8.7 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。（5.8.7 章参照）	・機能を無効に変更した場合、URL キーワードフィルタリング機能は停止します。

3.3.11. 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、5.8.8 章を参照してください。

[脅威を検出した際の動作・通知などの振る舞い]

検出時の動作	検出時の通知方法	検出状態の解除方法
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。

[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（5.8.8 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。（5.8.8 章参照）	・機能を無効に変更した場合、アプリケーションガード機能は停止します。

3.3.12. **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（インターネット側からのパケットの場合は、送信元 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 バイトです。
    1 M 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 720 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。

セキュリティ機能	個別許可の設定可能件数
アンチウイルス（AV）	10 件
Web ガード（WG）	10 件
URL フィルタリング（UF）	100 件

[USB ストレージへの保存]

（将来サポート予定）

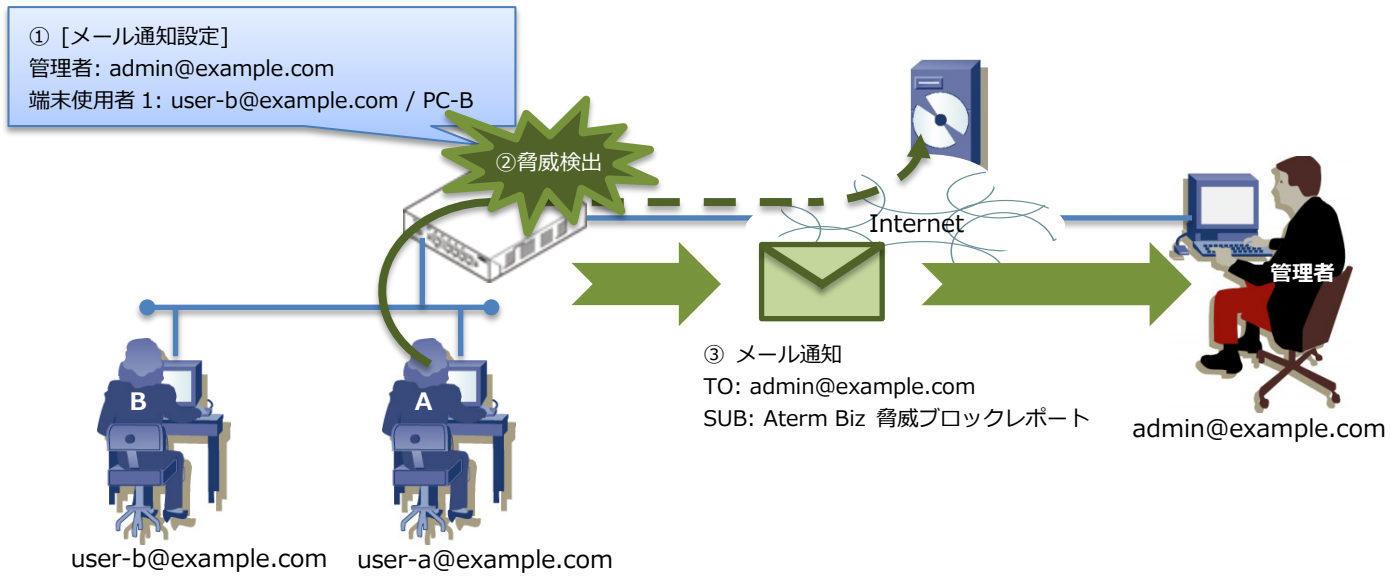
[その他の仕様]

- 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。

3.3.13. **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。



[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『脅威を検出！』しました。

③ メール通知で管理者に「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
- ライセンス期限切れ間近になったとき（ライセンス期限切れの 30 日前）
- ライセンス期限が切れたとき
- 月次レポートの送信時刻がきたとき

[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	ノード情報（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	登録済みのノードからのパケット、または、ノード宛てのパケットで脅威を検出した場合、当該ノード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	ライセンス期限切れ間近（30 日前）	(1) 装置動作中にライセンス期限切れ間近となったとき (2) 装置起動時、ライセンス期限切れ間近のとき (3) 上記(1)または(2)を実行した後、ライセンス期限が切れるまで 24 時間ごと	○	×
	ライセンス期限切れ	・装置動作中にライセンス期限切れとなったとき ・装置起動時、ライセンス期限切れのとき	○	×
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	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（日本語）]

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* 時間: *yyyy/mm/dd hh:mm:ss* 端末:*IP* アドレス/*MAC*	・通知先によらず共通 ・端末=LAN 側端末
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*	・タイプ=WG/KF ・端末=LAN 側端末
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*	・端末=LAN 側端末
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*	・端末=LAN 側端末
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*	
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。 満了時刻: *yyyy/mm/dd hh:mm:ss*	
ライセンス情報 (有効期限切れ)	Aterm Biz 情報通知	ライセンスの有効期限が満了しました。	
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。 Ver:*x.x.x*	
月次レポート	Aterm Biz 月次レポート	*yyyy/mm* レポート [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* [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*	
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。	テストメール送信時

[メール通知内容（英語）]

通知内容	メール件名	メール内容	補足
脅威検出 (AV)	Aterm Biz Blocking Report	Blocking the following threat. Type:AV Virus:*virus* File:*filename* Time: *yyyy/mm/dd hh:mm:ss* Device: *IP* アドレス/*MAC*	・通知先によらず共通 ・Device=LAN 側端末
脅威検出 (WG, KF)	Aterm Biz Blocking Report	Blocking the following threat. Type:*Function* URL:*url* Time: *yyyy/mm/dd hh:mm:ss* Device: *IP* アドレス/*MAC*	・Type=WG/KF ・Device=LAN 側端末
脅威検出 (UF)	Aterm Biz Blocking Report	Blocking the following threat. Type:UF URL:*url* Category:*category* Time: *yyyy/mm/dd hh:mm:ss* Device:*IP* アドレス/*MAC*	・Device=LAN 側端末
脅威検出 (APG)	Aterm Biz Blocking Report	Blocking the following threat. Type:APG Application:*application* Time: *yyyy/mm/dd hh:mm:ss* Device: *IP* アドレス/*MAC*	・Device=LAN 側端末
脅威検出 (IPS)	Aterm Biz Blocking Report	Blocking the following threat. Type: IPS attacker IP:*IP* アドレス Details:*msg* Time: *yyyy/mm/dd hh:mm:ss* Device: *IP* アドレス/*MAC*	・attacker IP=送信元 IP アドレス
ライセンス情報 (有効期限間近)	Aterm Biz　Information	License will expire soon. License expiration: *yyyy/mm/dd hh:mm:ss*	
ライセンス情報 (有効期限切れ)	Aterm Biz　Information	License expired.	

ファームウェアアップデート	Aterm Biz　Information	Release new firmware. 　Ver:*x.x.x*	
月次レポート	Aterm Biz Monthly Report	*yyyy/mm reports* [Statistics] 　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* [Firmware Information] 　Release new version (or No information) [License expiration] 　*yyyy/mm/dd hh:mm:ss*	
テストメール	Aterm Biz Test Mail	Sending this test mail.	テストメール送信時

［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 時間:2016/08/01 12:00:00 端末:192.168.110.2/FF:FF:FF:FF:FF:FF

- 月次レポートの表示例

件名	**Aterm Biz 月次レポート**
本文	2016/07 レポート [統計情報] AV:0/100 IPS:0/100 WG:0/100 UF:50/100 KF:20/100 APG:10/100 [ファームウェア更新情報] なし [ライセンス有効期限] 2023/08/01 12:00:00

3.3.14. **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 分間点滅(※)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。

※赤が点滅します。
　5 色表示に対応したパトライト製品の場合でも点滅するのは赤色です。

[当社動作確認済みパトライト製品][13]

- PHN-3FBE1 (株式会社パトライト製)
- NHP-5FV1（株式会社パトライト製）

[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、5.8.10 章を参照してください。

[13] 2016 年 7 月現在

3.3.15. **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]

- 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。
- 日、週、月ごとに閲覧できます。

セキュリティ・スキャン機能	統計情報	説明
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
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

[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、月ごとに閲覧できます。
- 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。

[USB ストレージへの保存]

（将来サポート予定）

[その他の仕様]

- 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。

3.3.16. **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、この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）押下
- 設定 Web でセキュリティログを閲覧

[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。

3.4. メンテナンス機能

[Ver3.1.26 での追加機能]

- SNMP
- ping 送信

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手順は、次の 3 つの方法があります。

[更新方法 1]

1. INFO ランプが橙点灯していることを確認
2. OPT2 スイッチ押下、または、設定 Web でファームウェア更新ボタンを押下

※本製品は最新のファームウェアの有無を定期的にチェックし、最新のファームウェアがある場合、INFO ランプが橙点灯します。

[更新方法 2]

1. パソコンなどに新しいファームウェアを保存
2. 設定 Web でファイルを指定してファームウェアを更新

[更新方法 3]

1. 本製品の WAN ポートをインターネットに接続
2. 設定 Web で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

※他に緊急でファームウェアを更新することがあります。[14]

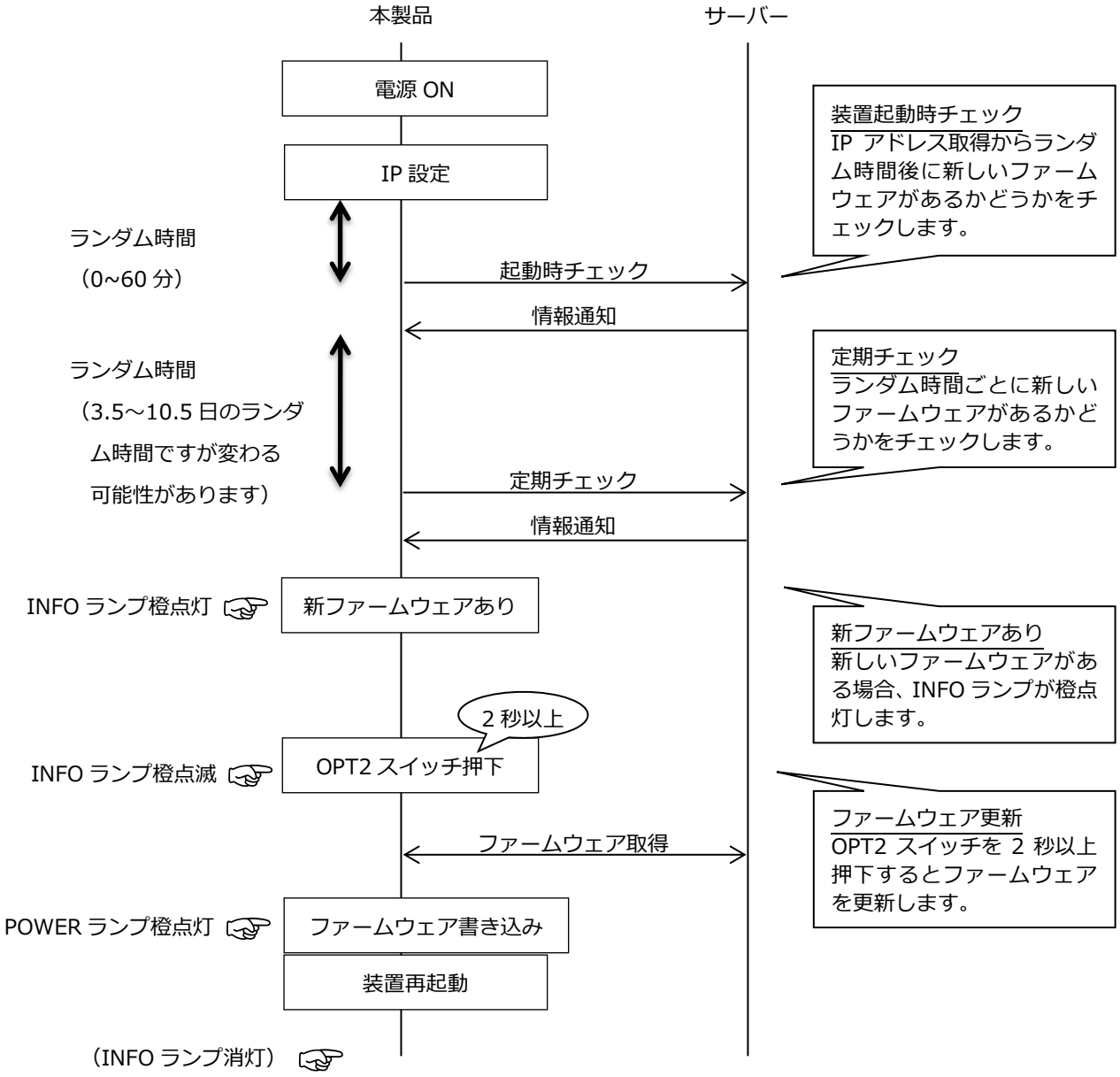
[メモ]

- 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。
- ファームウェアのバージョンダウンでは、設定値を初期化します。

[14] 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（5.6.5 章参照）。

[メモ]

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。



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。

[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 5.6.8 章を参照してください）
- RESET スイッチ（操作手順は 5.9.1 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（5.6.11 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（5.6.5 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

保存方法は 3.4.3 章を参照してください。

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

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。5.6.7 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。（6.1.8 章、6.1.9 章参照）

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
- ファームウェア更新後

初期化を伴わない再起動には、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 JST です。
本製品の時刻設定手順は、5.6.4 章を参照してください。

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 サーバーの指定が必要になります。

[NTP サーバーの設定]
設定 Web で、NTP サーバーのアドレスを変更できます。初期値は、NICT 公開 NTP サービスの NTP サーバーを指定しています。
NTP サーバーは 1 台のみ指定できます。

[タイムゾーン]

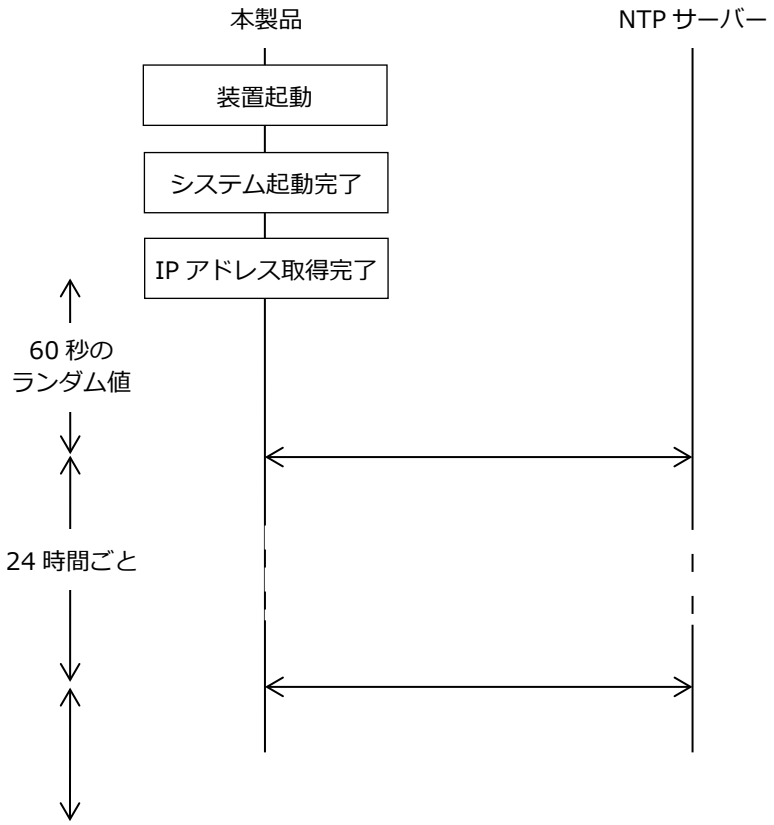
タイムゾーンを設定 Web で変更できます。初期値は（GMT+09:00）を指定しています。

サマータイムには対応していません。

時間	都市（例）
(GMT-12:00)	Enewetak, Kwajalein
(GMT-11:00)	Midway Island
(GMT-10:00)	Hawaii
(GMT-09:00)	Alaska
(GMT-08:00)	Pacific Time (US, Canada)
(GMT-07:00)	Mountain Time (US, Canada)
(GMT-06:00)	Central Time (US, Canada), Mexico City, Saskatchewan
(GMT-05:00)	Eastern Time (US, Canada), Indiana (East)
(GMT-04:00)	Atlantic Time (Canada), La Paz
(GMT-03:00)	Brasilia, Buenos Aires, Georgetown
(GMT-02:00)	Mid-Atlantic
(GMT-01:00)	Azores, Cape Verde Islands
(GMT 00:00)	Greenwich Mean Time：Dublin, Edinburgh, Lisbon, London
(GMT+01:00)	Berlin, Stockholm, Rome, Bern, Brussels, Vienna
(GMT+02:00)	Athens, Helsinki, Istanbul, Cairo, Eastern Europe, Israel
(GMT+03:00)	Baghdad, Kuwait, Nairobi, Riyadh, Moscow
(GMT+04:00)	Abu Dhabi, Muscat, Tblisi, Kazon, Volgograd
(GMT+04:30)	Kabul
(GMT+05:00)	Islamabad, Karachi, Ekaterinburg, Tashkent
(GMT+05:30)	New Delhi
(GMT+06:00)	Almaty, Dhaka
(GMT+06:30)	Yangon (Rangoon)
(GMT+07:00)	Bangkok, Jakarta, Hanoi
(GMT+08:00)	Beijing, Hong Kong, Perth, Singapore, Taipei
(GMT+09:00)	Tokyo, Osaka, Sapporo, Seoul, Yakutsk
(GMT+09:30)	Adelaide, Darwin
(GMT+10:00)	Brisbane, Canberra, Melbourne, Sydney, Hobart
(GMT+11:00)	Magadan, Solomon Islands, New Caledonia
(GMT+12:00)	Fiji, Kamchatka, Marshall Islands, Wellington, Auckland

[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 サーバーから応答がない場合などにより、NTP サーバーとの通信に失敗した場合、次のように再送します。

- NTP サーバー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 プロキシサーバー対応**

お客様のネットワークが HTTP プロキシサーバー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 プロキシサーバーを設定してください。
→ 本製品のセキュリティ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、ネットワークの到達を確認に使用します。

[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

3.5. **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 フレームを透過しません。
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。[15]

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。

[15] 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。[16]
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 メッセージ
送信	DISCOVER, REQUEST, RELEASE, DECLINE
受信	OFFER, ACK

[16] 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。

3.5.3. **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。
- プロキシ DNS 経由で動作します。
- DNS サーバーの IP アドレスを最大 2 アドレス管理します。

  DNS サーバーの 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**

[Ver 3.1.26 での追加機能]

- ルータ機能
- IPsec 機能
- SNMP 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ー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 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。

本製品は、本製品のルーティングテーブルを動的に生成し、スタティックルーティングにも対応しています。

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

[スタティックルーティングエントリ]

スタティックルーティングエントリを 50 エントリ設定できます。[17]

[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。

設定については、5.7.11 章を参照してください。

[17] IPv4 静的ルーティングエントリで設定できます。

3.6.4. **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。

[注意] Ver3.1.26 以降では、NAPT 機能は常時有効です。

[注意] Ver3.1.26 以降では、IPsec トンネルに流れるパケットに対して、NAPT しません。

[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 Addresss（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、5.8.2 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 IPsec を使用している場合や 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。

3.6.5. **PPPoE**

[動作インタフェース]

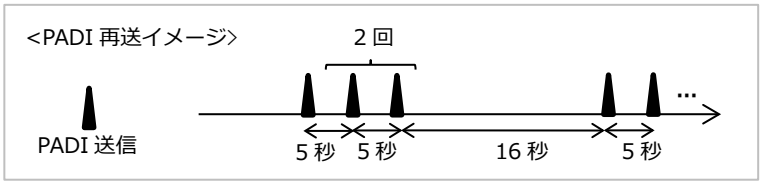
WAN インタフェース

[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。

3.6.6. **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 サーバーからの 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 サーバーから配布された 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。

3.6.7. **DHCP サーバー**

[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 50 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。

3.6.8. **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 サーバー動作します。
  LAN/無線 LAN インタフェースに接続しているノードから DNS query パケットを受信すると、DNS サーバーに送信します。
  また、DNS サーバーからの DNS response パケットを受信すると、ノードに送信します。
- DNS サーバーの IP アドレスを最大 2 アドレス管理します。
  DNS サーバーの 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。

3.6.9. **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。

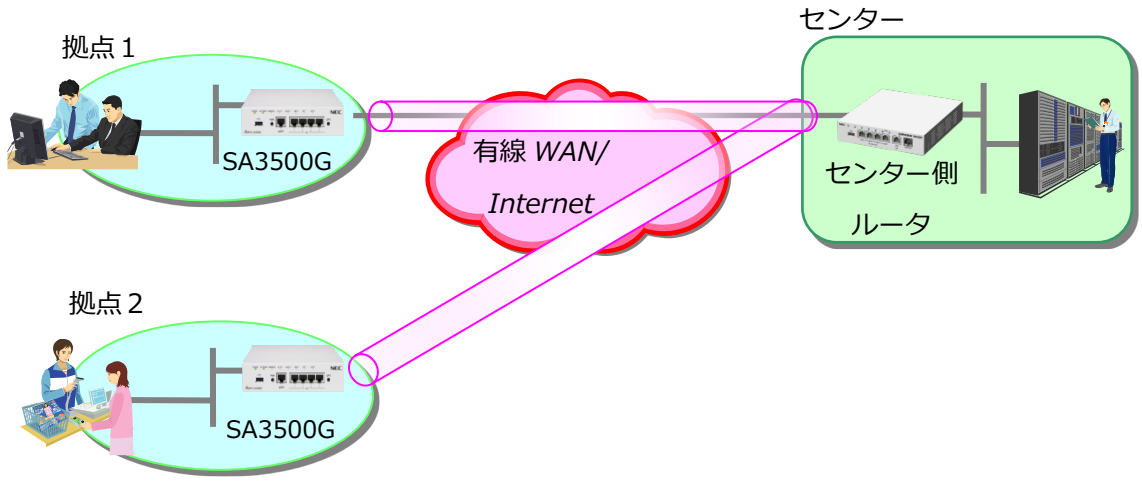
フィルタ対象パケット	対象ｲﾝﾀﾌｪｰｽ	フィルタタイプ	方向
IPoE→LAN	IPoE	転送 (転送パケット)	in
LAN→IPoE			out
IPoE→本製品		送受信 (本製品送受信パケット)	in
本製品→IPoE			out
PPPoE→LAN	PPPoE	転送 (転送パケット)	in
LAN→PPPoE			out
PPPoE→本製品		送受信 (本製品送受信パケット)	in
本製品→PPPoE			out
LAN→WAN (IPoE・PPPoE)	LAN	転送 (転送パケット)	in
WAN (IPoE・PPPoE)→LAN			out
LAN→本製品		送受信 (本製品送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

3.6.10. **IPsec**

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 は、以下の機能をサポートしています。

[暗号化]

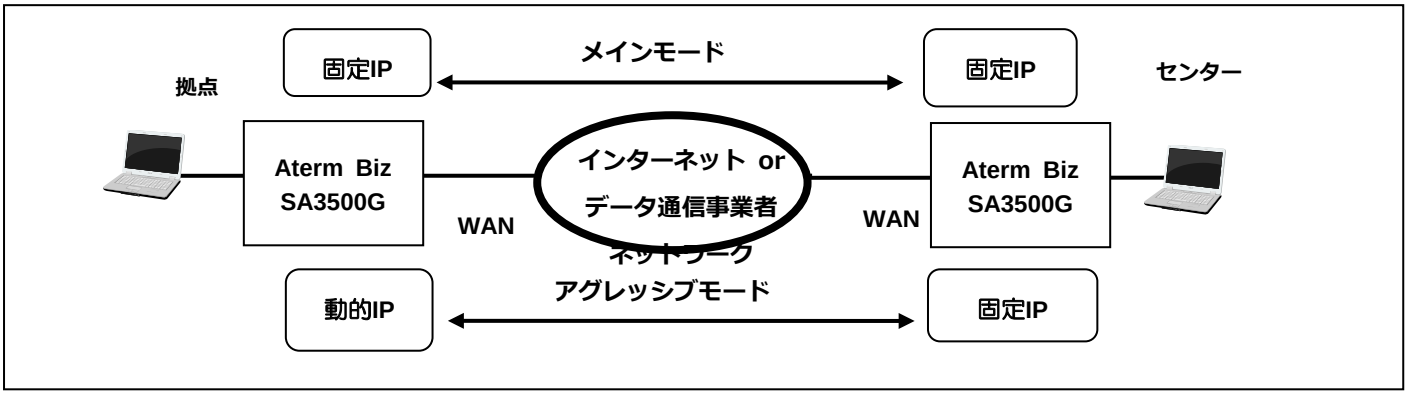
ESP（Encapsulated Security Payload）を使用した IP パケット全体を暗号化するトンネルモードをサポートしています。

[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



[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。

[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

[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。

[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します。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。本製品は、「post-fragment」方式のみサポートしています。

[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時には 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 を消失したものと見なし、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。

[その他連携機能]

- NAT/NAPT 同時動作（Sprit 動作）

  物理インタフェースでは暗号化パケットと暗号化されないパケットを併用して送信できます。

[IPsec 諸元一覧]

項目			機能
IKE	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)
		ライフタイム	時間設定
	ソースアドレス指定		固定設定
	対地数		1 対地
IKE 拡張	IKE SA 削除		delete payload 受信時、IKE SA 削除時の delete payload 送信
	IPsec SA/IKE SA のリキー拡張		・常時接続の場合 - ユーザートラフィックなしでもリキーする ・オンデマンド接続の場合 - ユーザートラフィックありでリキーする - ユーザートラフィック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)
	Keep-Alive		DPD 方式(IPsec SA があるときに送信)
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
		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		暗号化後にフラグメント(post-fragment)
	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
IPsec 拡張	IPsec SA 削除		delete payload 受信時、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		AUTO
	アンチリプレイ防御		可能
その他連携機能	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、通常のスタティック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。

[制限事項]

・IPsec は、中継路に NAT/NAPT がないネットワーク環境で使用してください。

・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。

3.6.11. **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、重要なイベントが発生した際に、トラップ情報を SNMP マネージャに送信することでイベント情報を管理者に通知できます。

[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。
[注意] 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

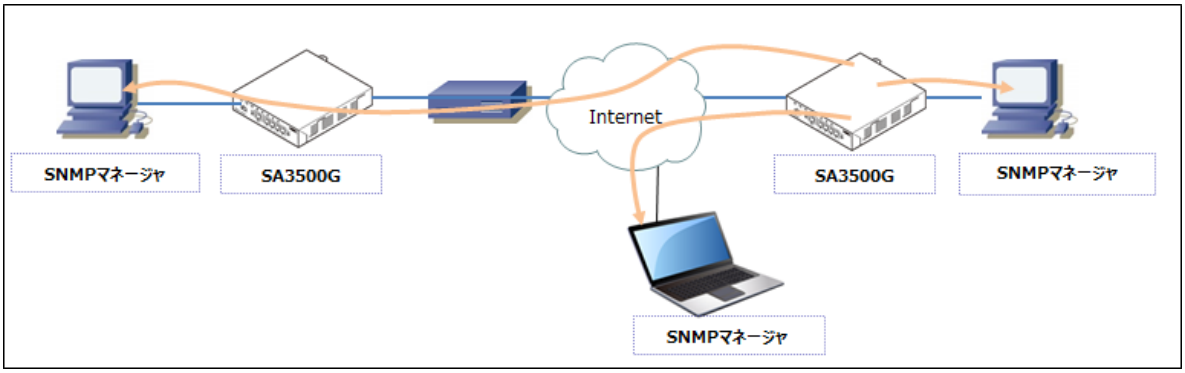
MIB グループ	管理している情報
System	システム情報
Interface	保有するハードのウェアインタフェース情報
Address Translation	IP アドレスと物理的なアドレスとの変換テーブル
IP	プロトコルの使用に関する情報
ICMP	ICMP の動作に関する情報
TCP	TCP の動作に関する情報
UDP	UDP の動作に関する情報
Transmission(dot3)	データ転送(イーサネットライクインタフェース)に関する情報
SNMP	SNMP に関する情報
ifMIB	インタフェース拡張情報

[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」ボタンを押すと、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。

3.6.12. **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。(5.7.15 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。

3.7. **無線 LAN 機能**

[Ver 3.1.26 での追加機能]

- 無線 LAN 機能

  [メモ] 無線 LAN 機能は、ルータモード時に動作します。

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)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。
外付けアンテナはオプション品です。

3.7.1. **無線 LAN**

無線主要機能一覧

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）	
ネットワーク分離	有効/無効切り替え	
無線 LAN 端末接続台数	最大 32 台	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]

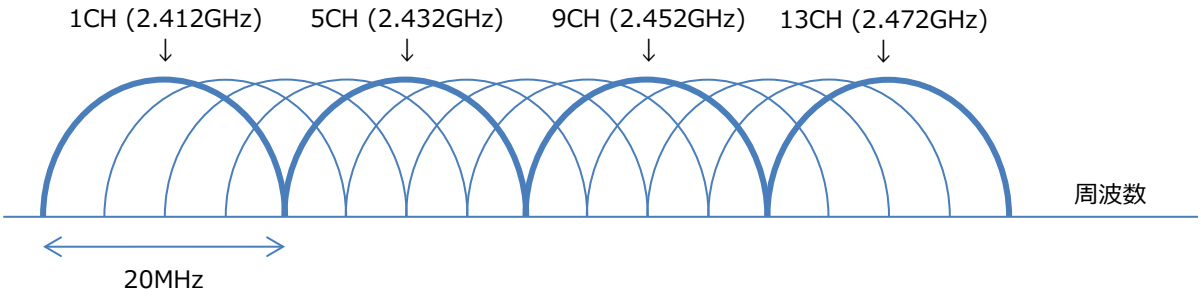
プライマリ SSID、セカンダリ SSID の 2 つの SSID を利用できます。

- SSID 名を設定 Web で変更できます。
- ESS-ID ステルス機能と呼ぶ、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を有しています。

[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

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)

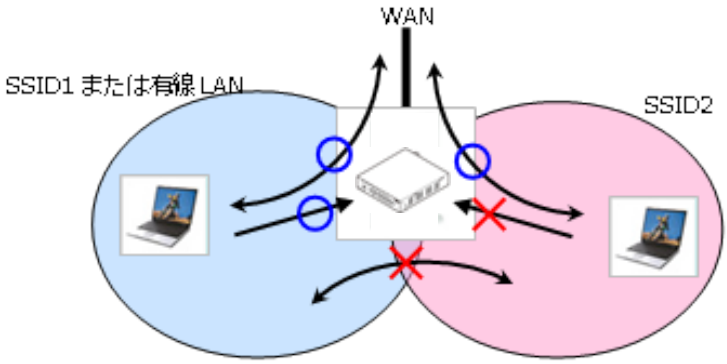
他に「暗号化無効」を選択できます。

[ネットワーク分離]

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 に接続しているノードから、インターネットアクセスおよび本製品の設定 Web にアクセス可能。

・SSID2 から SSID1、有線 LAN のノードにアクセスでません。SSID2 から本製品の設定 Web にもアクセスできません。



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 ボタンを使用して、WPS-PBC に対応した無線 LAN 端末と WiFi の自動設定を行うことができます。

3.8. **USB 機能**

（将来サポート予定）

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済み
- ライセンス確認済み [18]

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はできません。

[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

[18] 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

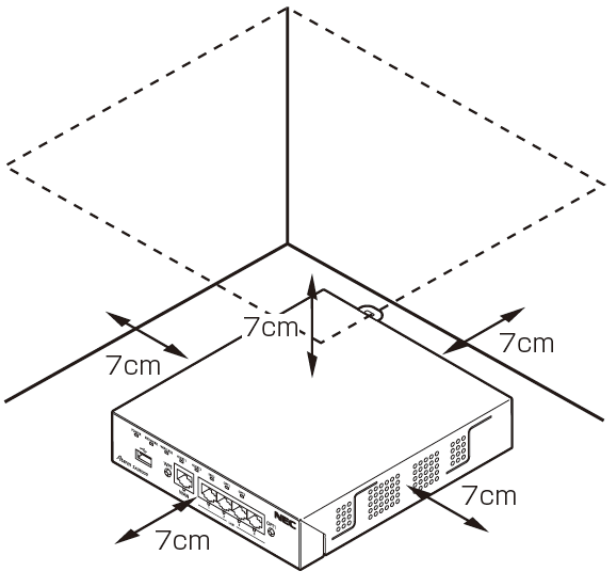
設置する前に以下の章の警告事項、注意事項を必ずお読みください。

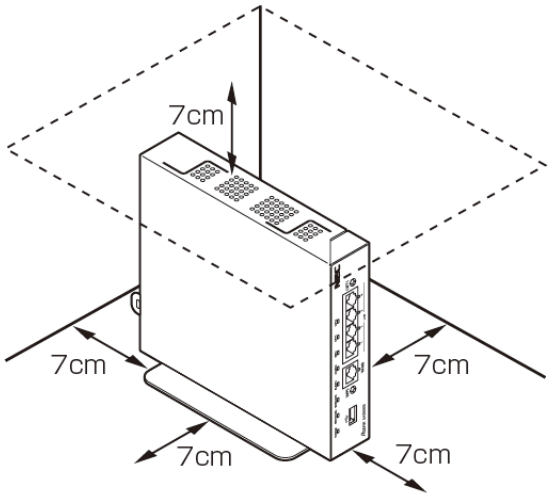
- 1.12 章 安全にお使いいただくために
- 1.13 章 本製品の故障を防ぐために

設置スペース

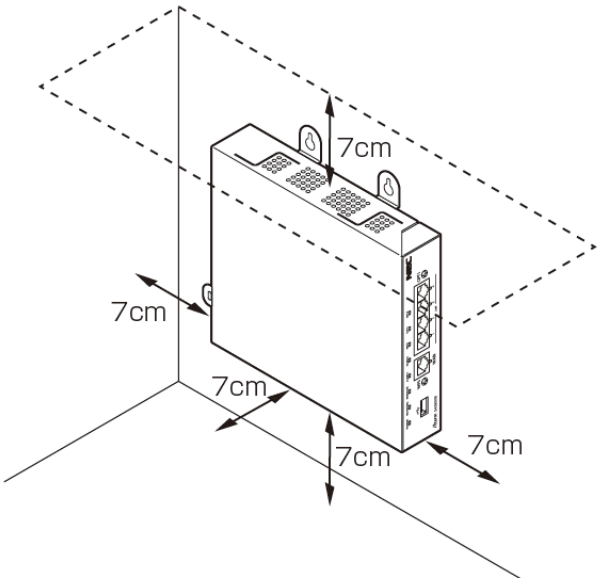
本製品は、本製品の周囲約 7cm 以内にパソコンや壁などのものがない場所に設置してください。

（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。）





（壁掛けの場合）



[注意]

- 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、破損や火災の原因となることがあります。
- 本製品の上にものをのせることや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。

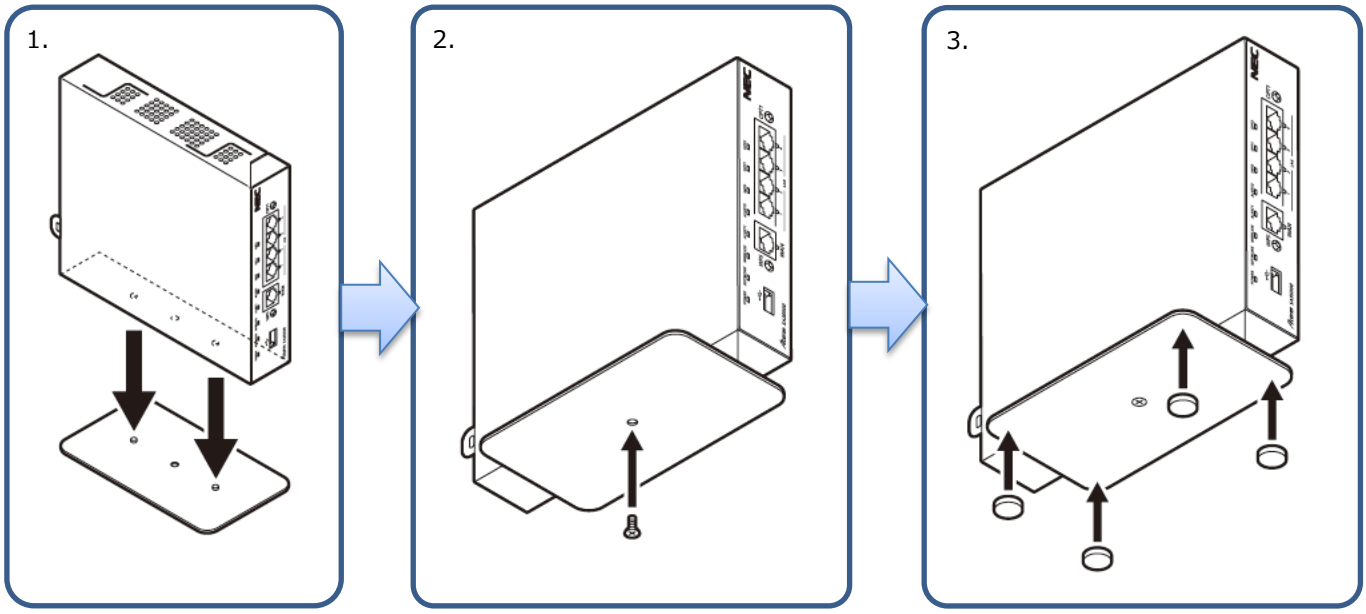
[設置手順]

■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。

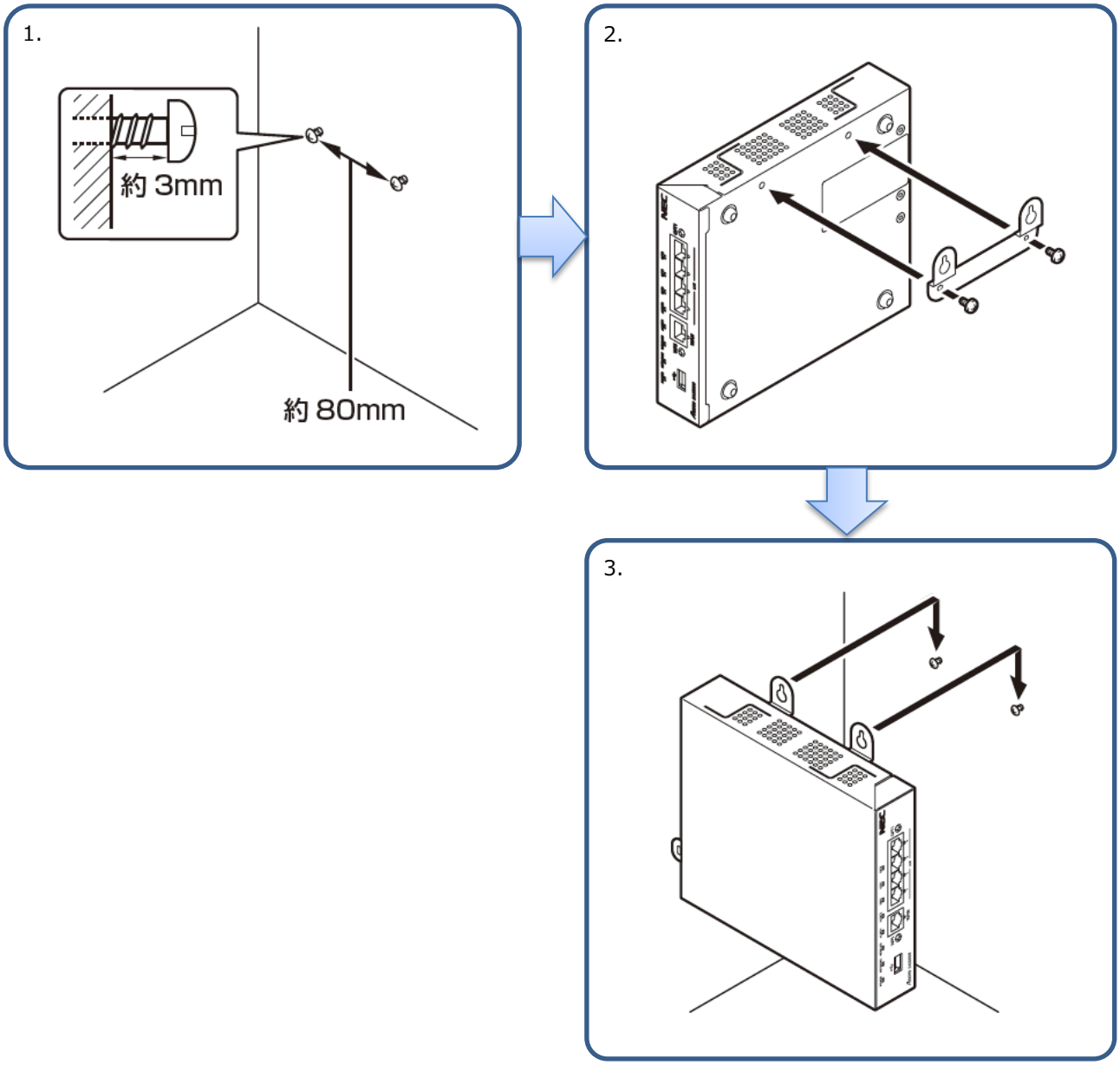


[注意]

- 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。

■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。



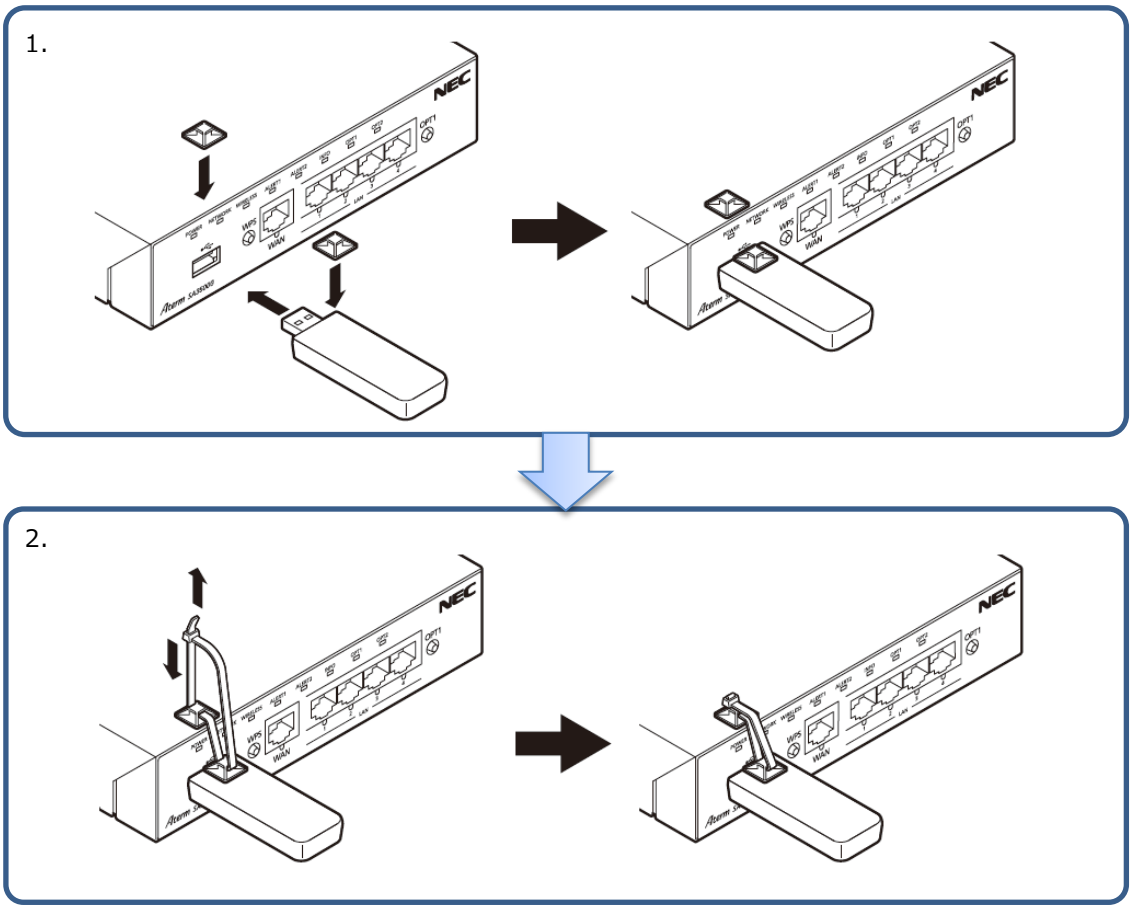
[注意]

- 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 デバイスの固定**

本製品の USB ポートから USB デバイス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。

1. USB 抜け防止用固定具を USB デバイスと本製品天面にそれぞれ貼り付けます。
   ※USB デバイスに貼り付ける USB 抜け防止用固定具の向きに注意してください。
   ※USB デバイスの形状によっては、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 デバイスを取り外す際は、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 デバイスを取り外してください。

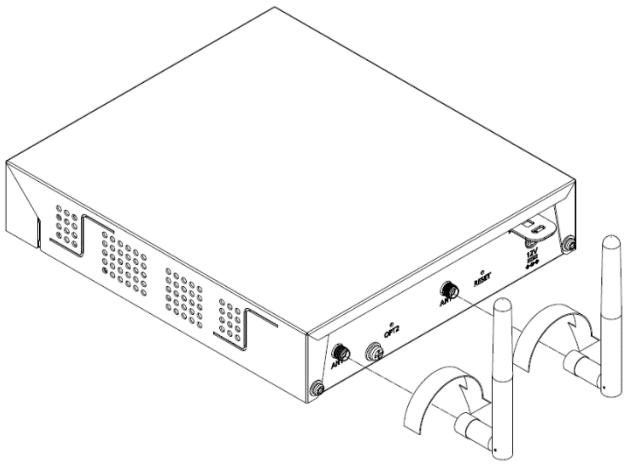
4.3. **アンテナの取り付け**

本製品の無縁 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）を本体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体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体に取り付け後、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体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（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み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。

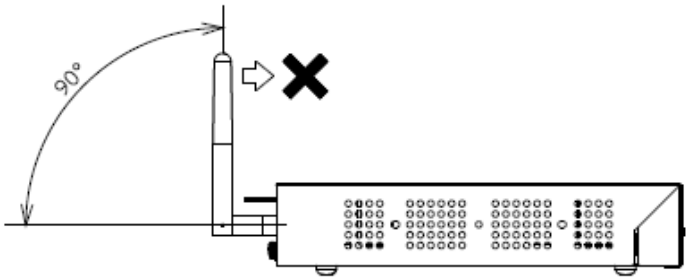
※ 落下などで外付けアンテナが破損した場合、速やかに外付けアンテナを交換するか、外付けアンテナを外して、アンテナの設定を“内蔵アンテナ”に切り替えてください

アンテナの取り付け



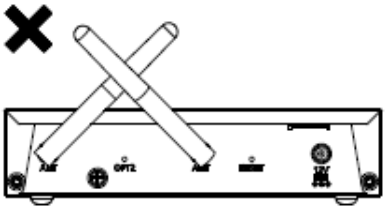
禁止事項 1.

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。*

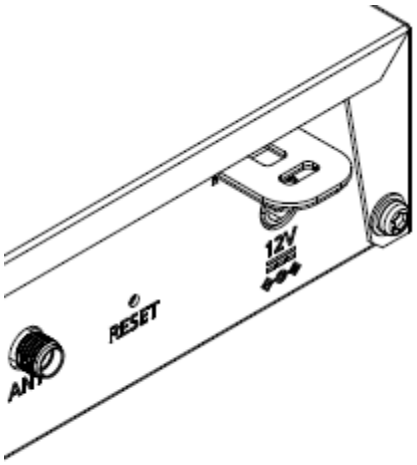


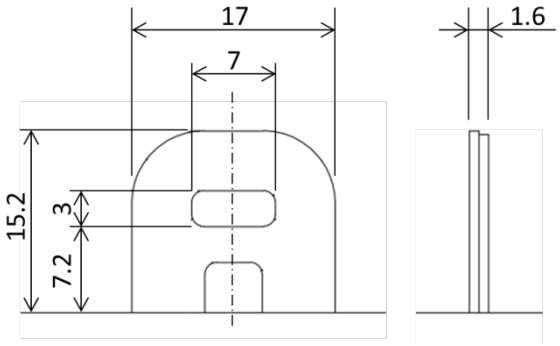
4.4. 盗難防止フックの使用方法

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



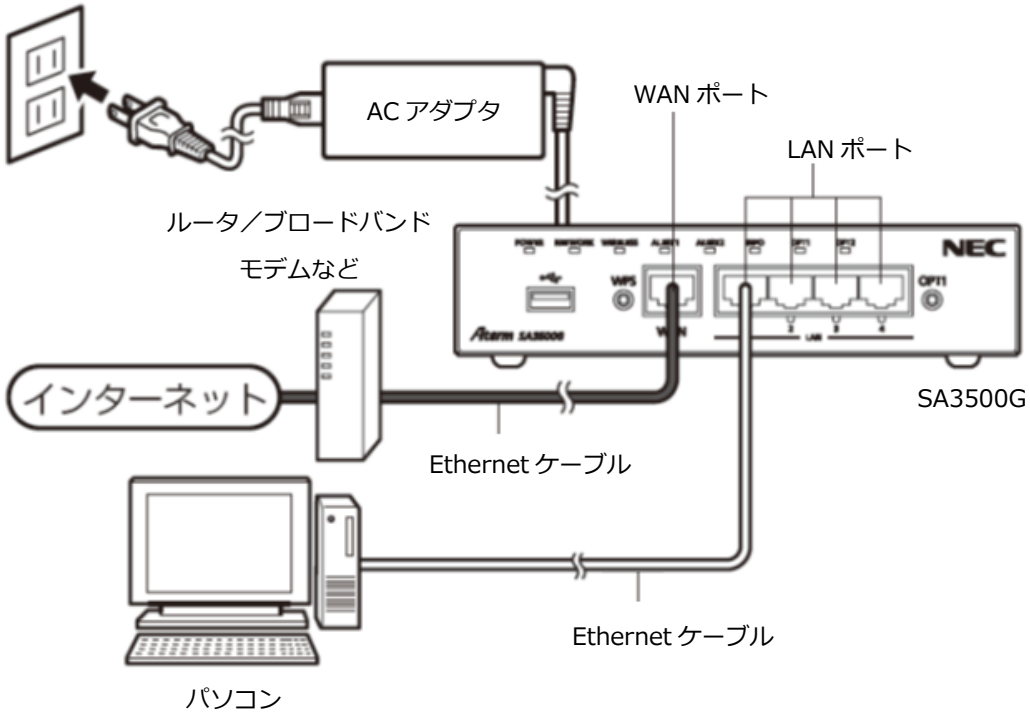


4.5. **ケーブルの接続**

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 アダプタを本体の 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、大きくわけて 2 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

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 10/8.1/7	Internet Explorer 11 Google Chrome 51	
Windows 8	Internet Explorer 10	
OS X v10.11/v10.10	Safari 9	

[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 章参照）

設定終了後は、元の設定に戻してください。

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

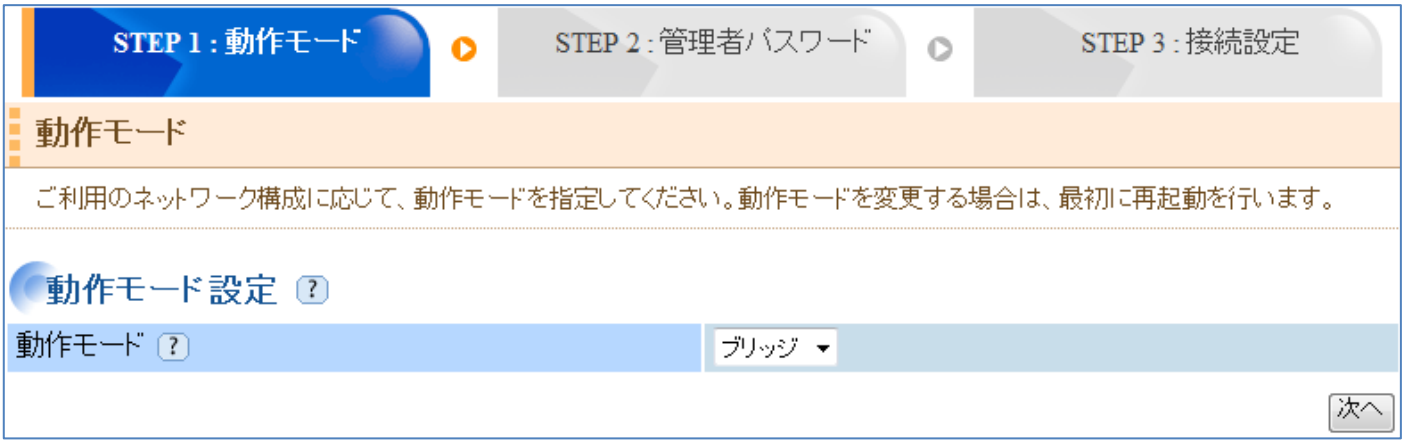
初回装置起動時は、次の操作が必要です。

- 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）

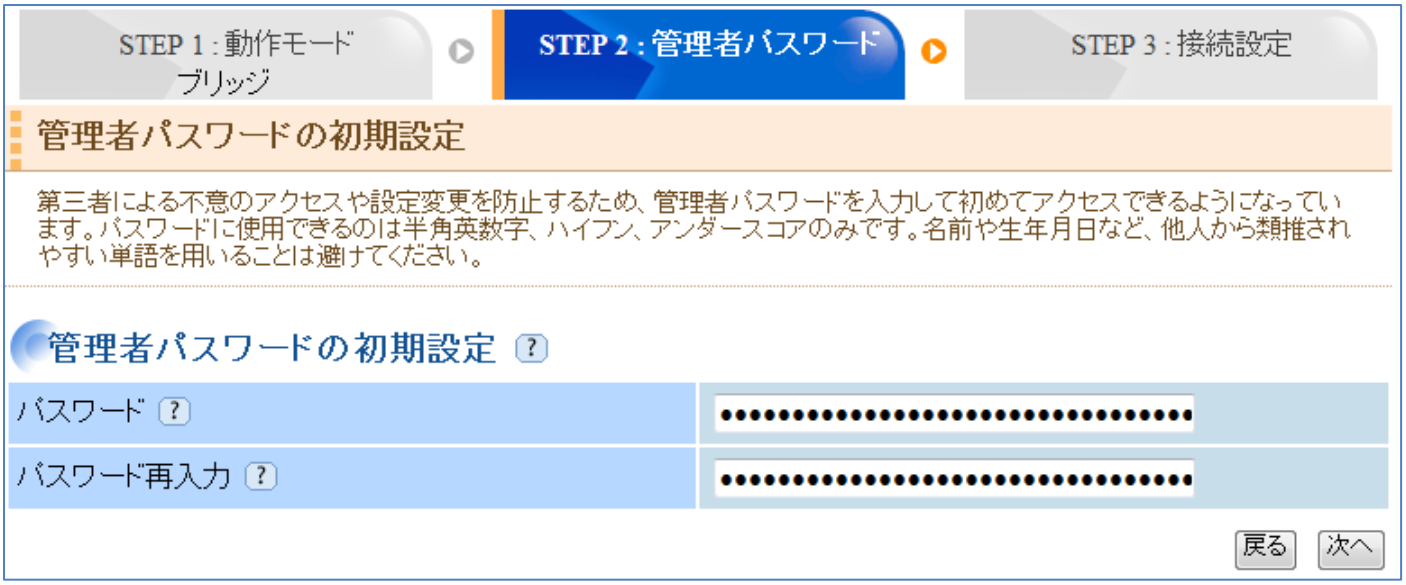
5.2.1. ブリッジモードで動作させる場合

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/にアクセスします。
4. 設定ウィザードが開きます。
   STEP1 → STEP2 → STEP3 の順で設定してください。
5. **STEP1:** 動作モードを選択します
   ブリッジモードを選択します。

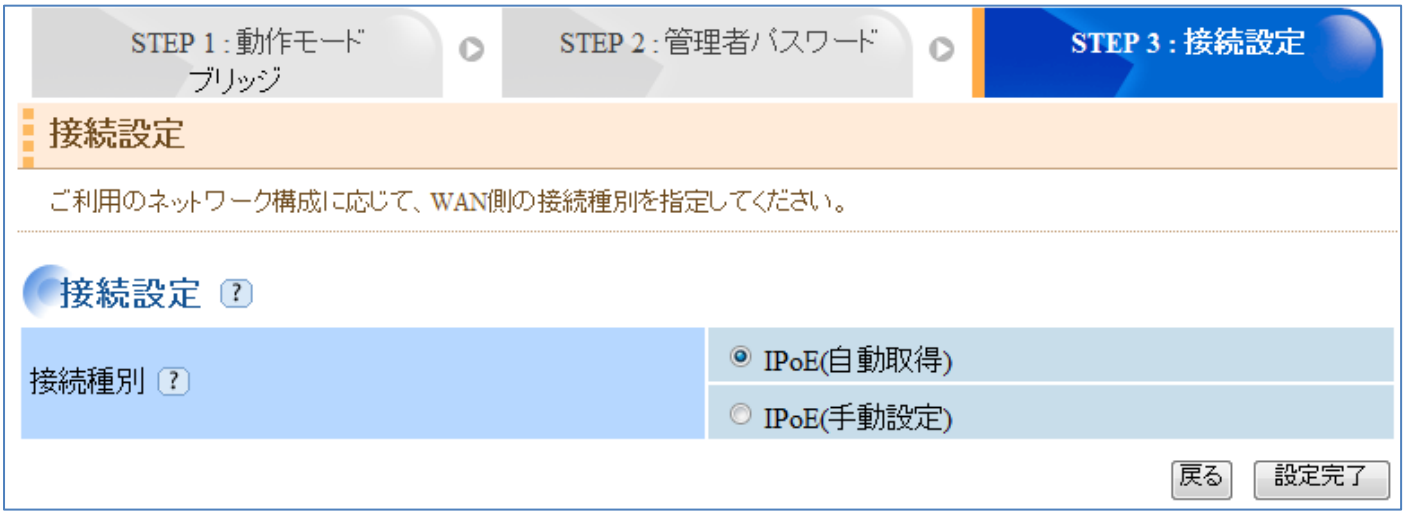


6. **STEP2:** 管理者パスワードを設定します
   パスワードに使用できる文字は、半角文字 0～9,a～z,A～Z,-(ハイフン),_(アンダースコア)です。
   入力可能文字数は、1～64 です。
   ※管理者パスワードとは、本製品の設定 Web へのログインパスワードです
   ※ここで設定したパスワードは、STEP3 の「設定完了」ボタン押下で FlashROM に保存します



7. **STEP3：** 装置用 IP アドレスに関して設定します

選択項目	説明
IPoE（自動取得）	本製品の IP アドレス [19]を DHCP で取得する場合に選択します。
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）

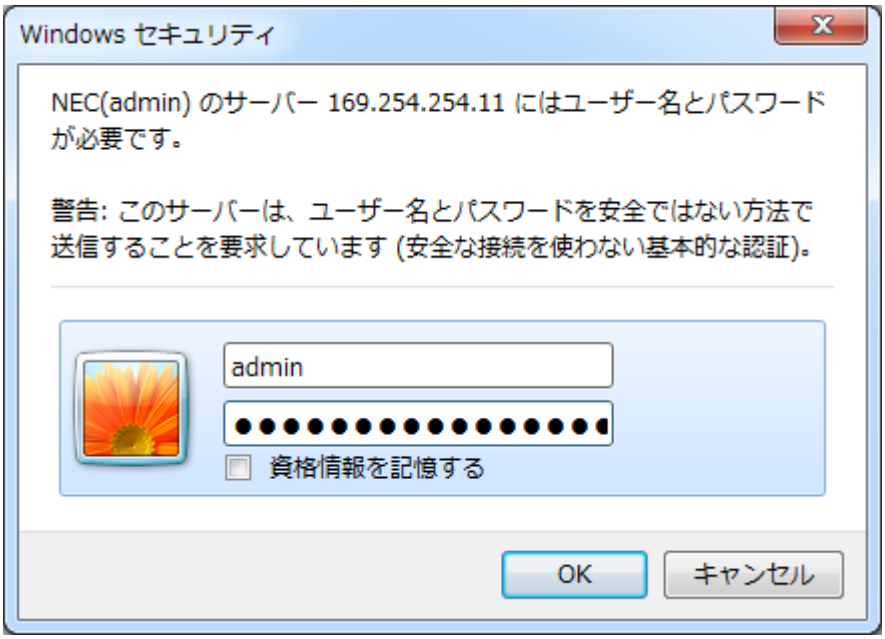


[19]本製品のセキュリティ・スキャン機能を使用するには、本製品に IPv4 アドレスが必要です

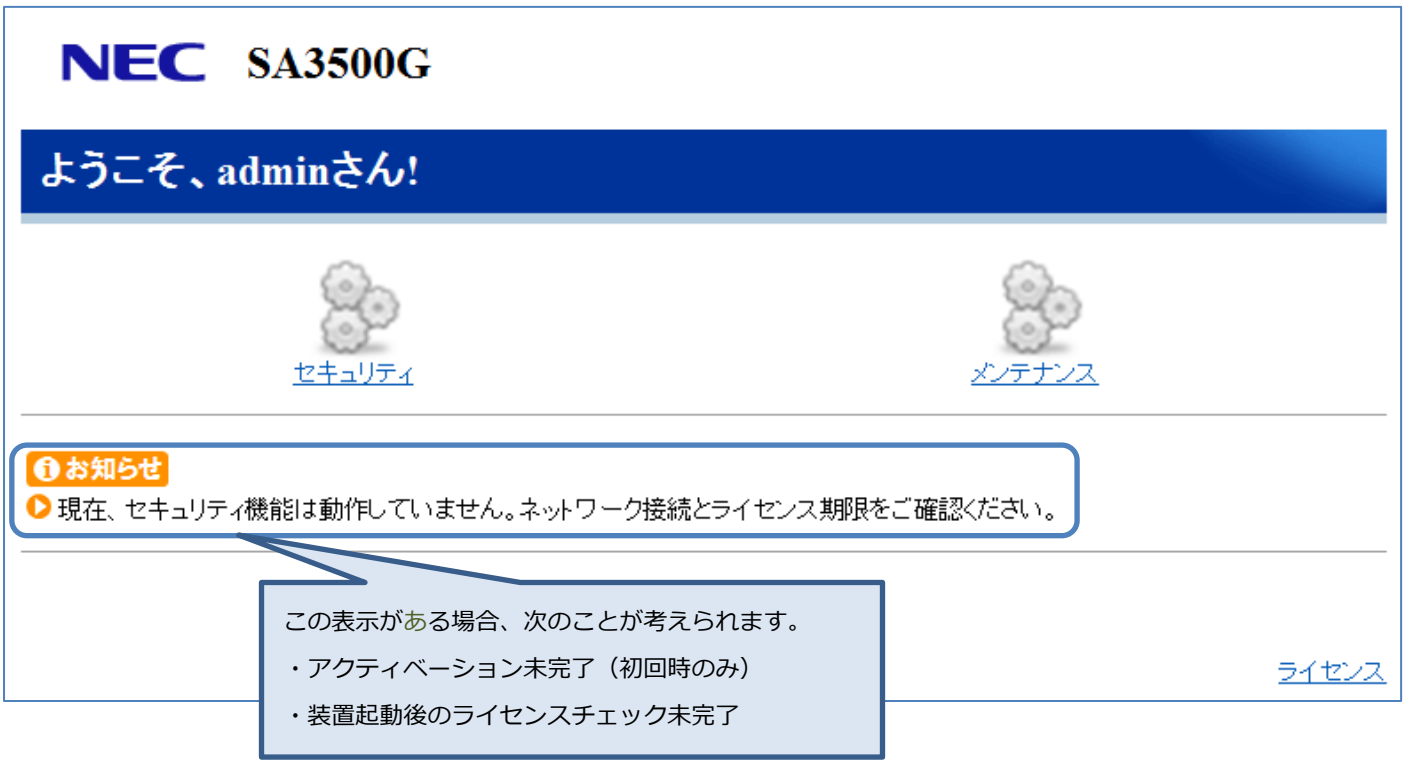
8. 本製品の設定 Web のログイン画面が開きますので、ユーザー名/パスワードを入力します。

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



9. 上記手順が完了すると TOP 画面に移動します。



10.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。

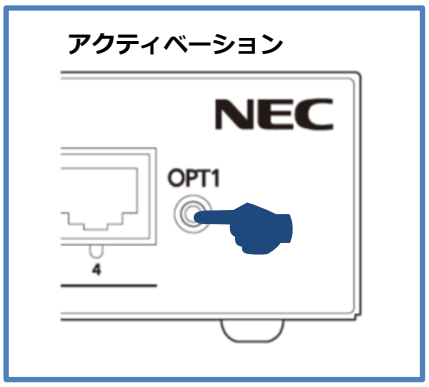
11.セキュリティ・スキャン機能に関して設定します。（5.8 章を参照してください。）

12.設定を保存します。（5.5 章を参照してください。）

13.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。（5.6.5 章を参照してください）

14.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。

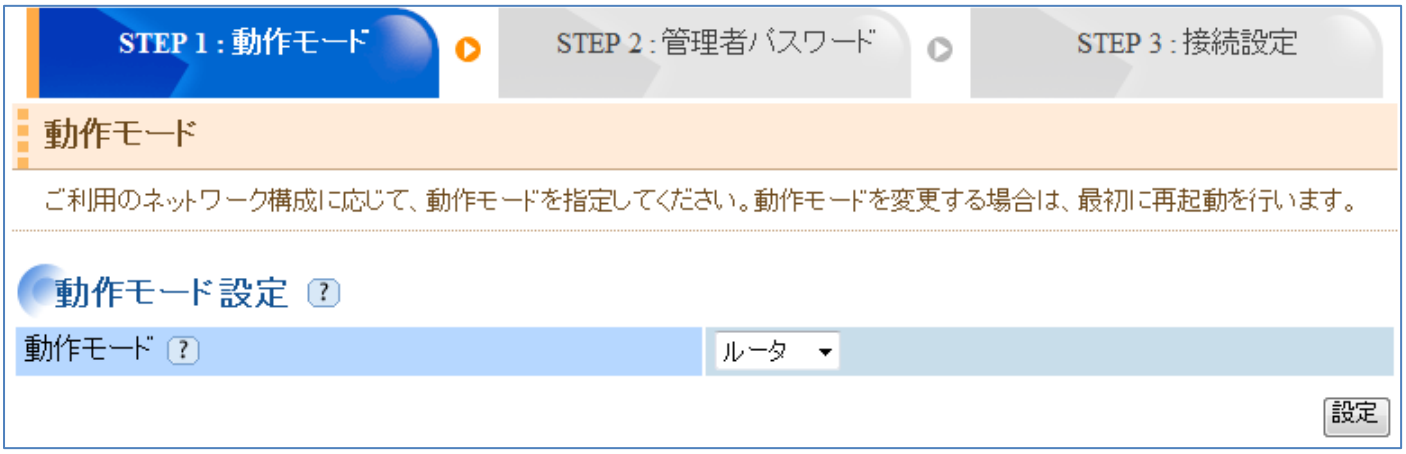
15.パソコンの IP アドレスを元に戻します。
※もともとお使いの設定に戻してください。



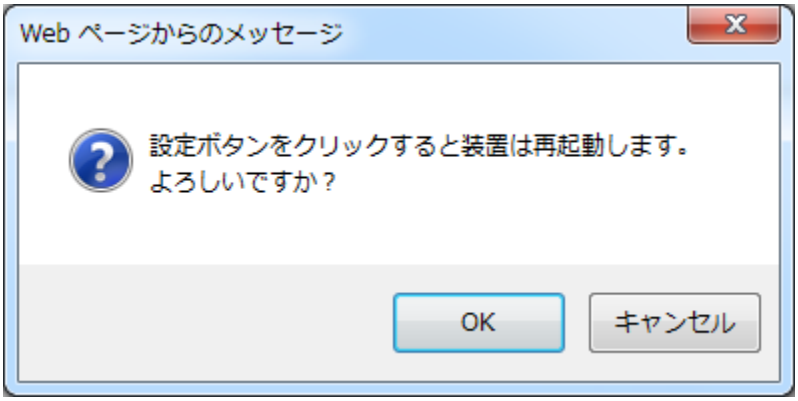
5.2.2. **ルータモードで動作させる場合**

次の手順で設定します。

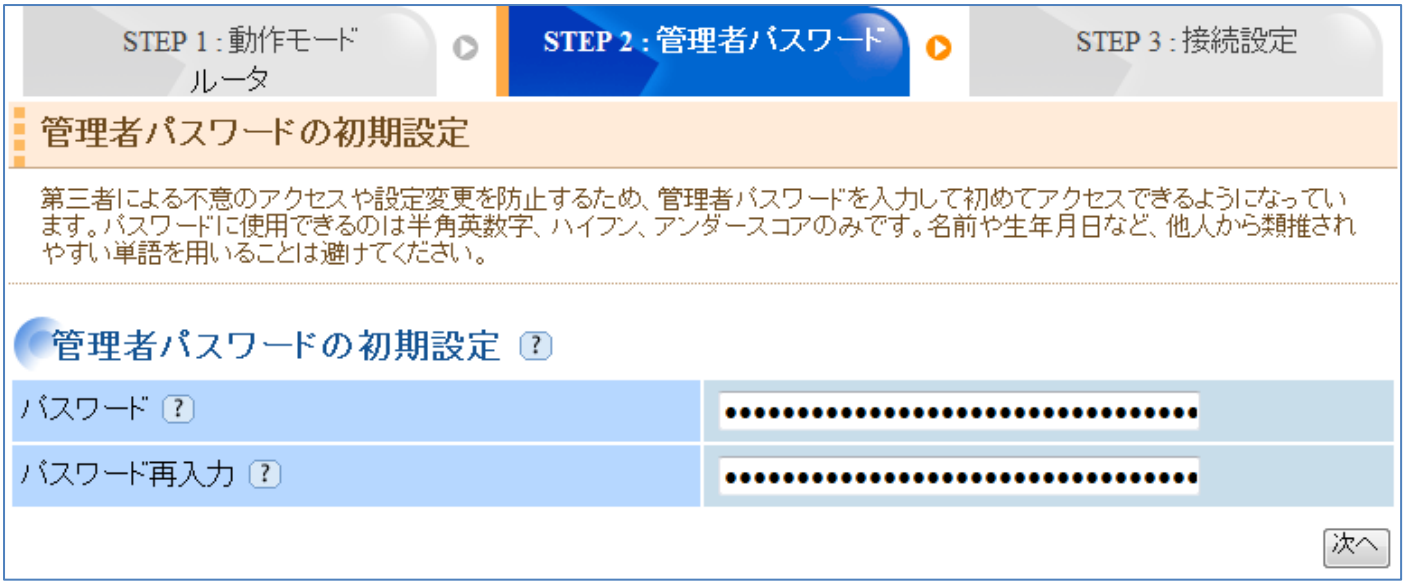
1. 本製品に各種ケーブルを接続します。(4.5 章を参照してください。)
2. 本製品を設定するパソコンの IP アドレスを 169.254.xxx.xxx/16 に設定します。
   (xxx は 1~254 の任意の整数です。169.254.254.11 以外の IP アドレスを設定してください。)
3. パソコンの Web ブラウザを開き、http://169.254.254.11/にアクセスします。
4. 設定ウィザードが開きます。
   STEP1 → STEP2 → STEP3 の順で設定してください。
5. **STEP1:** 動作モードを選択します
   ルータモードを選択します。



※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。

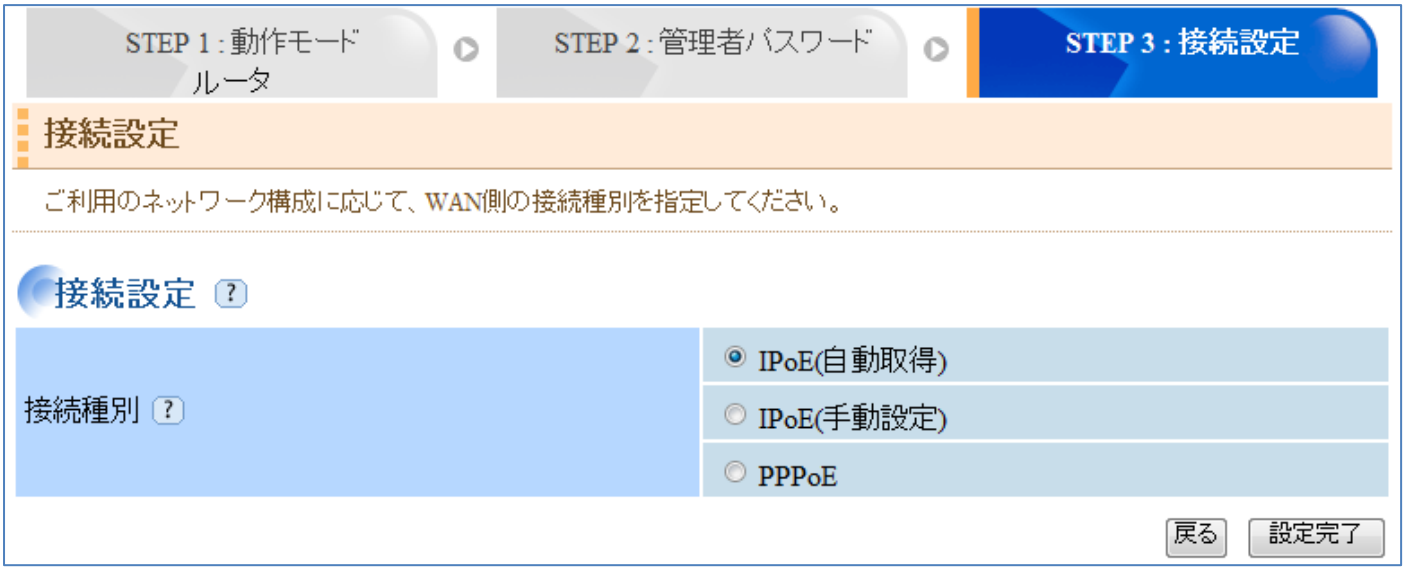


6. **STEP2:** 管理者パスワードを設定します
   パスワードに使用できる文字は、半角文字 0~9,a~z,A~Z,-(ハイフン),_(アンダースコア)です。
   入力可能文字数は、1~64 です。
   ※管理者パスワードとは、本製品の設定 Web へのログインパスワードです
   ※ここで設定したパスワードは、STEP3 の「設定完了」ボタン押下で FlashROM に保存します



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

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 [20]を DHCP で取得する場合に選択します。
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）
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。 ● 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。



[20]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


STEP 1 : 動作モード
ルータ
STEP 2 : 管理者パスワード
STEP 3 : 接続設定
接続設定
ご利用のネットワーク構成に応じて、WAN側の接続種別を指定してください。
接続設定
接続種別
IPoE(自動取得)
IPoE(手動設定)
PPPoE
IPv4アドレス/ネットマスク
IPv4アドレス/ネットマスク(ビット指定)
192.168.1.2
/
24
ゲートウェイ
ゲートウェイアドレス
192.168.1.1
DNSv4サーバアドレス
IPv4プライマリDNS
192.168.1.253
IPv4セカンダリDNS
192.168.1.254
戻る
設定完了

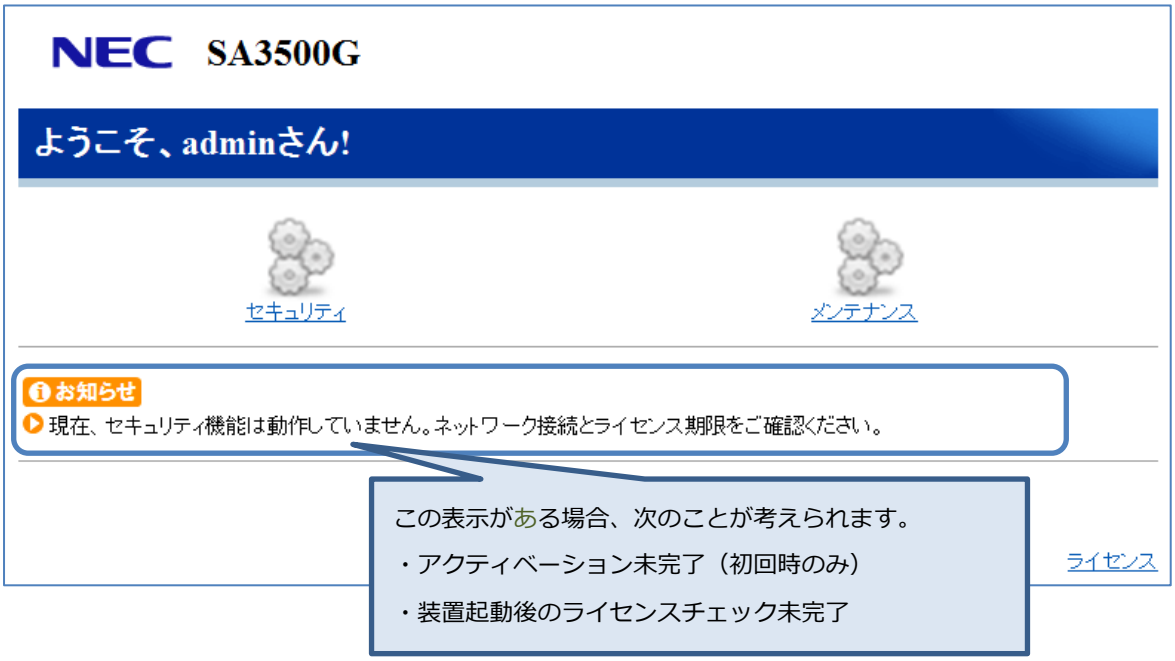

STEP 1 : 動作モード
ルータ
STEP 2 : 管理者パスワード
STEP 3 : 接続設定
接続設定
ご利用のネットワーク構成に応じて、WAN側の接続種別を指定してください。
接続設定
接続種別
IPoE(自動取得)
IPoE(手動設定)
PPPoE
PPPoE 設定
ユーザー名
sample@example.com
パスワード
戻る
設定完了

8. 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

9. 上記手順が完了すると TOP 画面に移動します。



10.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。）

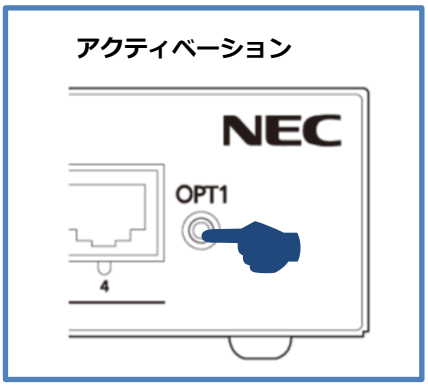
11.セキュリティ・スキャン機能に関して設定します。（5.8 章を参照してください。）

12.設定を保存します。（5.5 章を参照してください。）

13.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。
（5.6.5 章を参照してください）

14.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。

15.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。

[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]

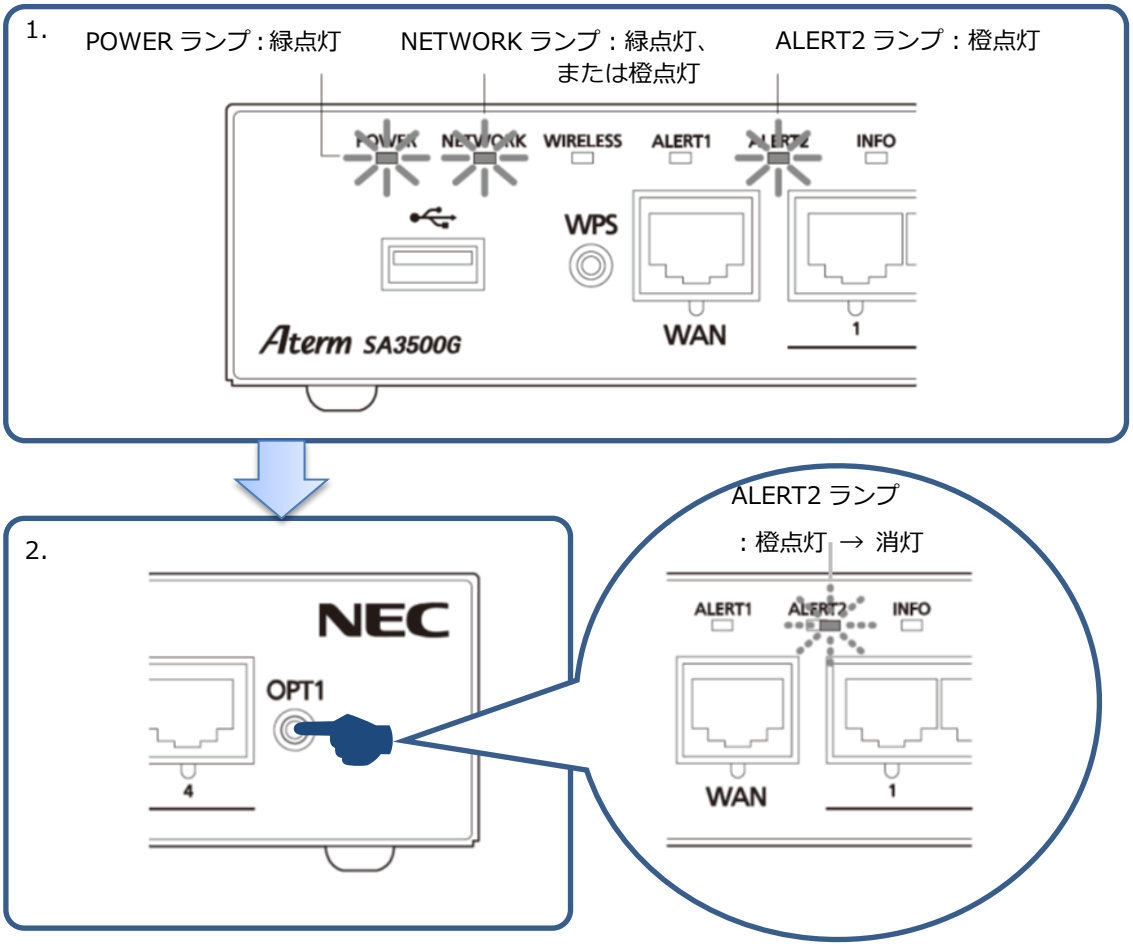
本製品がインターネット通信できる状態にしてください。

（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。

[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 秒間押下したら放します。
   (ALERT2 ランプが橙点滅するときがあります)
3. 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。



[アクティベーションが成功しない場合は...]

OPT1 スイッチ（セキュリティ・スキャン機能用スイッチ）を押下して 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。

この場合は、ネットワーク環境を確認したのち、再度アクティベーション操作してください。詳細は 7.1.3 章を参照してください。

[メモ]

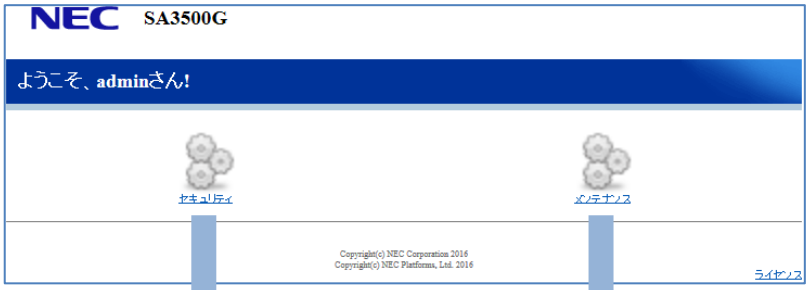
ライセンスの利用開始日は、アクティベーションが成功した日または、本製品納入後 31 日を経過したいずれかの早い日です。

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。

5.3. 設定画面構成

本製品の設定手順は次のとおりです。

ログイン



TOP ページ

セキュリティ設定

メンテナンス設定

※画面の表示内容は動作モードにより異なります。

※画面の表示内容は動作モードにより異なります。

「セキュリティ」「メンテナンス」の各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	
ファイアウォール（FW）	ファイアウォールに関する設定 ※ルータモード時に動作します	
アンチウイルス（AV）	ウイルススキャン対象に関する設定	
不正侵入防止（IPS）	IPS の有効無効に関する設定	
Web ガード（WG）	特に危険な Web サイトへのアクセス可否に関する設定	
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	
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	
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	
メール通知	イベントを通知するメールアドレスの設定	※Ver3.1.26 で追加
オプション	パトライト機能の設定	※Ver3.1.26 で追加
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出力の設定、および、表示	定期的な確認を推奨します
統計情報	セキュリティ・スキャン機能に関する統計情報の表示	
メンテナンス（ブリッジモード）	ブリッジ、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	お客様の環境に合わせて変更してください
接続設定	モード切り替え	
ネットワーク	本製品の IP アドレスや HTTP プロキシサーバーなどの設定	
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	
管理者パスワードの変更	設定画面のパスワードの設定	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	設定値の保存、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	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	
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	バージョン情報、および、動作状況の表示	
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	
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	※Ver3.1.26 で追加
基本設定	本製品のネットワークに関する設定	お客様の環境に合わせて変更してください
接続設定	モード切り替え、IPoE/PPP 切り替え	
PPP 設定	PPPoE に関する設定	
IPv4 WAN 設定（IPoE）	DHCP クライアントに関する設定	
IPv4 LAN 設定	DHCP サーバーに関する設定	

無線 LAN 設定	無線 LAN に関する設定	
無線 LAN 設定	無線 LAN に関する設定	
ネットワーク設定	本製品の NAPT 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追加、削除	
DNS 設定	本製品の DNS 機能に関する設定	
IPv4 静的ルーティング設定	静的ルーティングエントリの追加、削除	
その他の設定	ICMP redirect 応答有無の設定	
VPN 設定	VPN 接続に関する設定	
IPsec 設定	IPsec/IKEv1 に関する設定	
セキュリティ設定	IPv4 パケットフィルタリングに関する設定	
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追加、削除	
管理設定	管理プロトコルに関する設定	
SNMP 設定	SNMPv1, SNMPv2c に関する設定	
メンテナンス	メンテナンスに関する設定	
管理者パスワードの変更	設定画面のパスワードの設定	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	設定値の保存、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	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	
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	バージョン情報、および、動作状況の表示	
装置管理情報	Wi-Fi 帰属情報や ARP テーブルの表示	
VPN 接続状態	IKE SA, IPsec SA などの表示	
VPN 統計情報	IPsec 統計情報の表示	
MIB 情報	MIB 情報の表示	
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	
ライセンス	OSS ライセンス情報の表示	

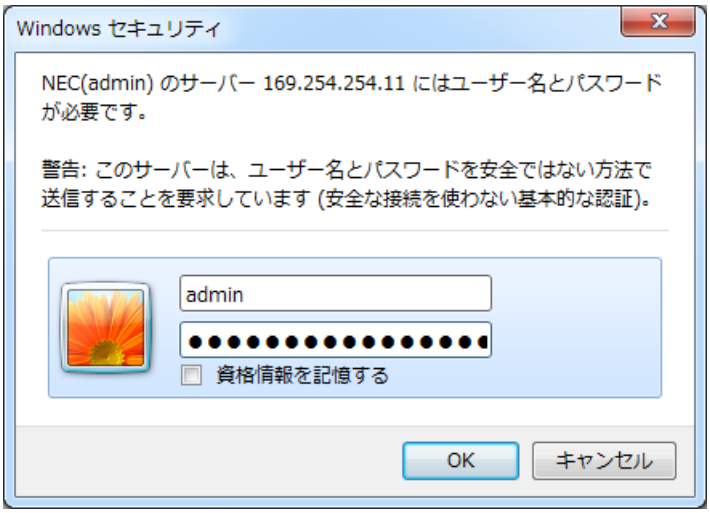
5.4. 本製品へのログイン

ここでは、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。

   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。
3. ログイン用ユーザー名/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。

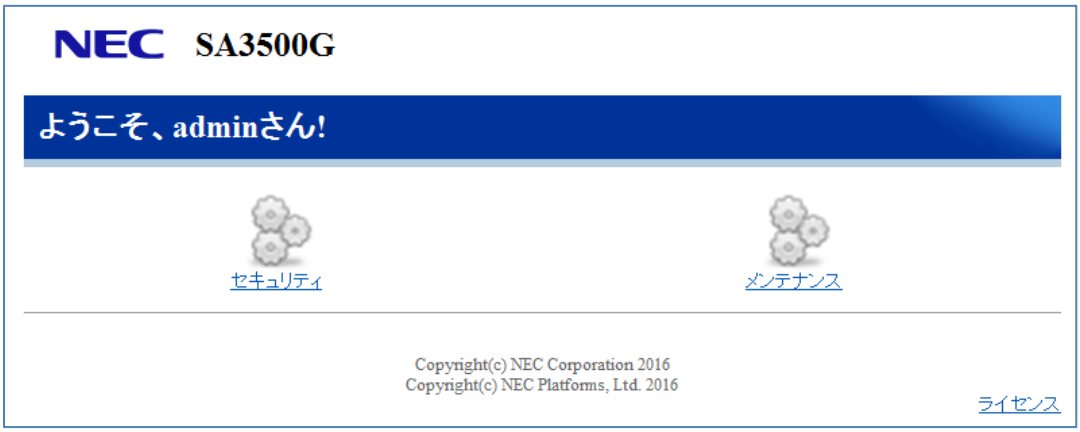


（左図はブリッジモードの場合）

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、5.6.6 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時は、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。

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。

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 ●印は設定項目の内容です。 ○印は表示項目の内容です。	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	お客様の環境に合わせて変更してください
接続設定	●ルータモードへの切り替え ※ルータモードへの切り替えは、本製品の再起動が必要です。	※Ver3.1.26 で追加
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 サーバー情報 ●HTTP プロキシサーバー	※Ver3.1.26 で HTTP プロキシサーバー機能を追加
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	
管理者パスワードの変更	●設定画面のパスワードの設定	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	
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 ○製品の IP アドレス	
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	※Ver3.1.26 で追加

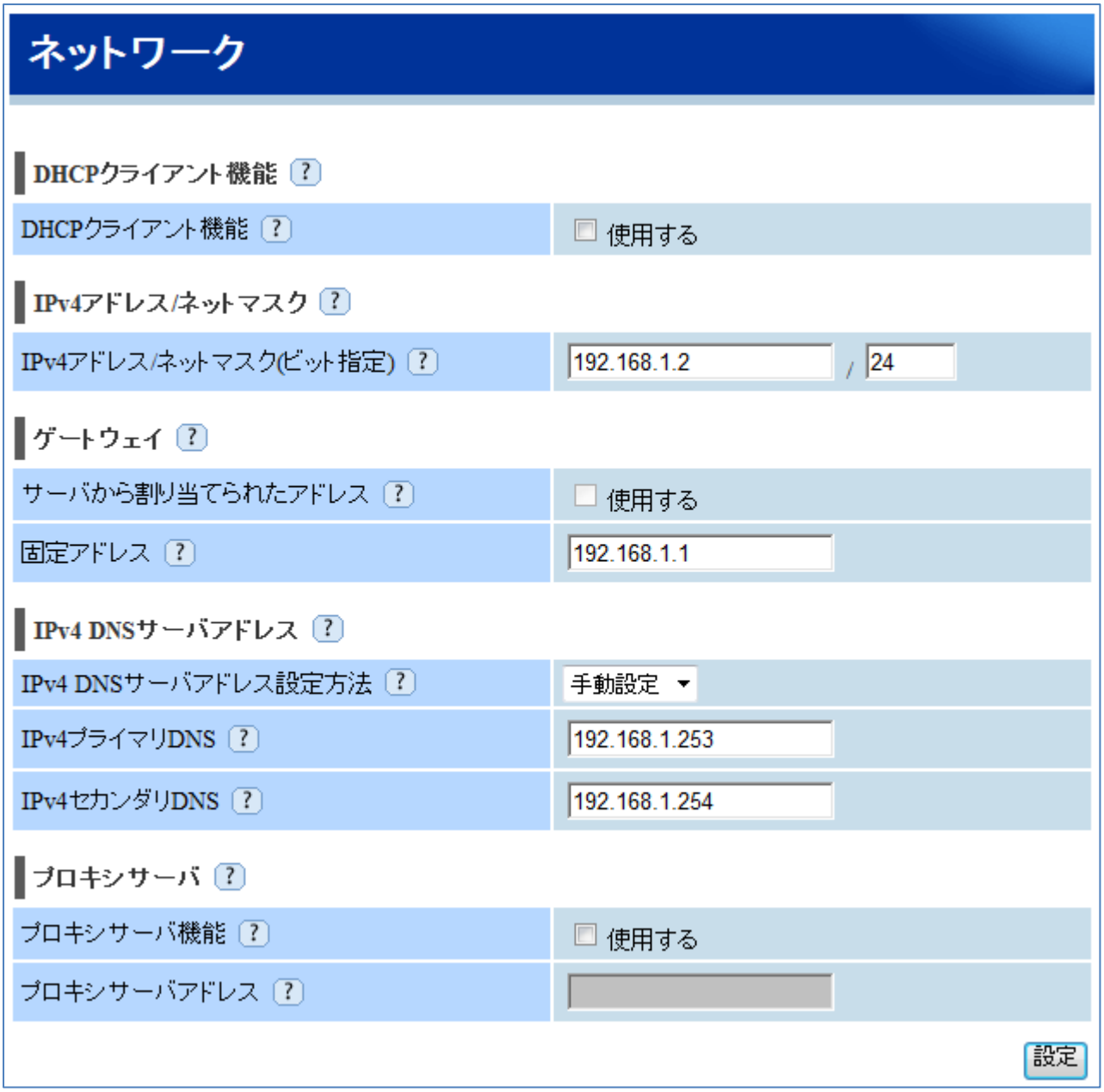
5.6.2. **本製品の IP アドレスの設定**

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、本製品に管理用の 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。



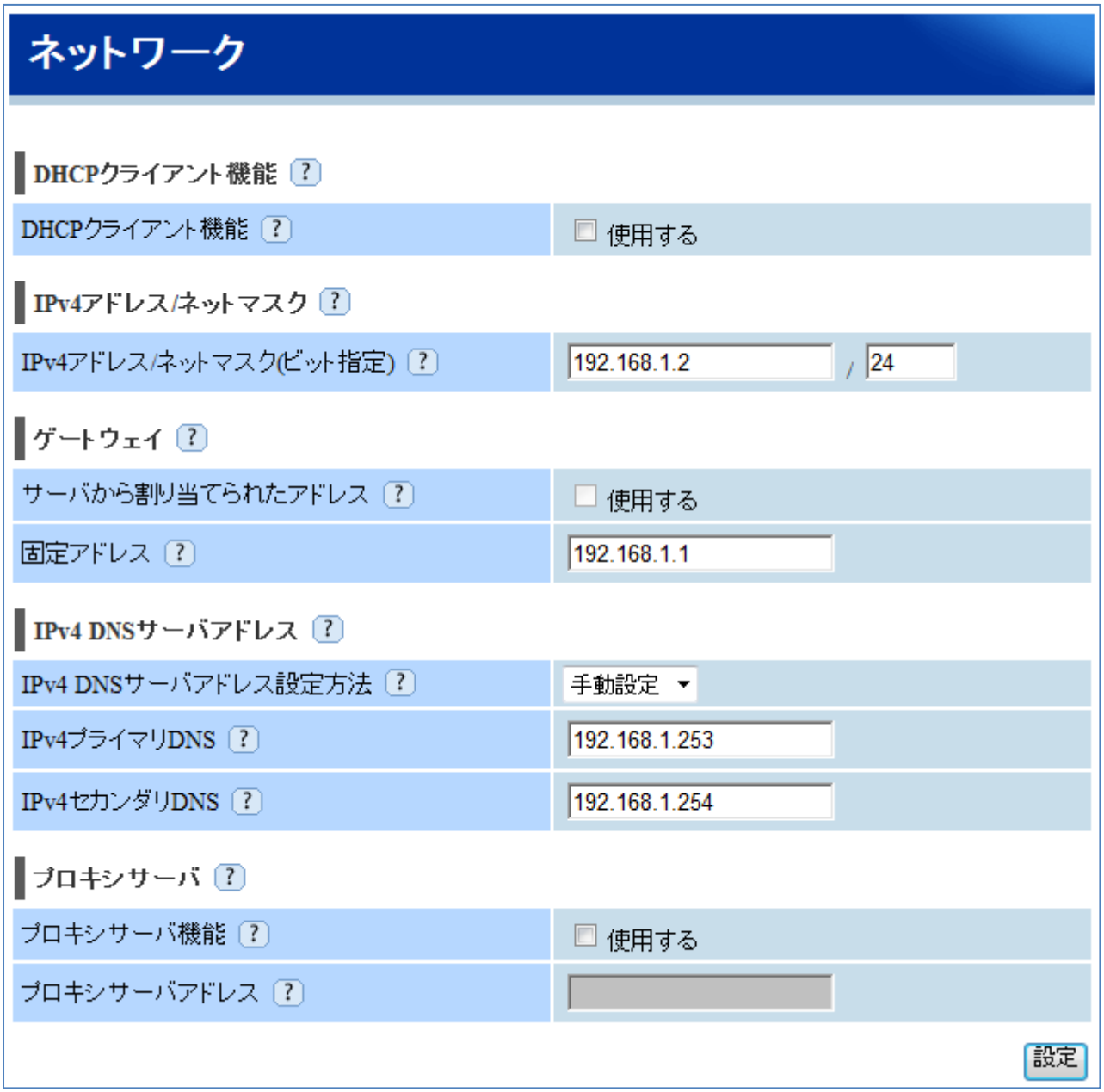
1. [TOP]-[メンテナンス]-[基本設定]-[ネットワーク]画面を開きます。
2. 本製品のネットワーク情報を入力します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、本設定を保存します。

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		
サーバー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
IPv4DNS サーバアドレス	DNS サーバーアドレス情報の設定		
IPv4 DNS サーバーアドレス設定方法	• **自動設定**…本製品がアクセスする DNS サーバーアドレスを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 サーバー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 サーバーアドレスを入力		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 サーバーアドレスを入力	本設定項目は省略可能です。	未設定

5.6.3. HTTP プロキシサーバーの設定

お客様のインターネット接続ネットワークが、プロキシサーバー経由の場合、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. プロキシサーバ機能の「使用する」をチェックします。
3. プロキシサーバアドレスに HTTP プロキシサーバー情報を入力します。
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。

設定項目	値	備考	初期値
プロキシサーバ	HTTP プロキシサーバー情報の設定		
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ーを設置している場合 • **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ーを設置していない	お客様のネットワークに合わせて設定してください。	無効
プロキシサーバアドレス	HTTP プロキシサーバー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]/ • 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]/	お客様の HTTP プロキシサーバー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

[制限事項]

HTTP プロキシサーバーを使用する場合、URL フィルタリング機能を使用できません。

5.6.4. **時刻の設定**

本製品の時刻に関する設定を変更したい場合は、実施してください。

本製品の時刻は、NTP サーバーから時刻を取得します。

- お客様で NTP サーバーを指定する場合は、本章を参考に設定してください。
  NTP サーバー情報を 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 サーバーの変更

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 サーバー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 サーバーを使用しない場合

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 JST）に戻ります。

NTP サーバーを使用せず、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。

5.6.5. ファームウェアの更新

必ず確認してください。

本製品のファームウェアは、次の方法で更新できます。

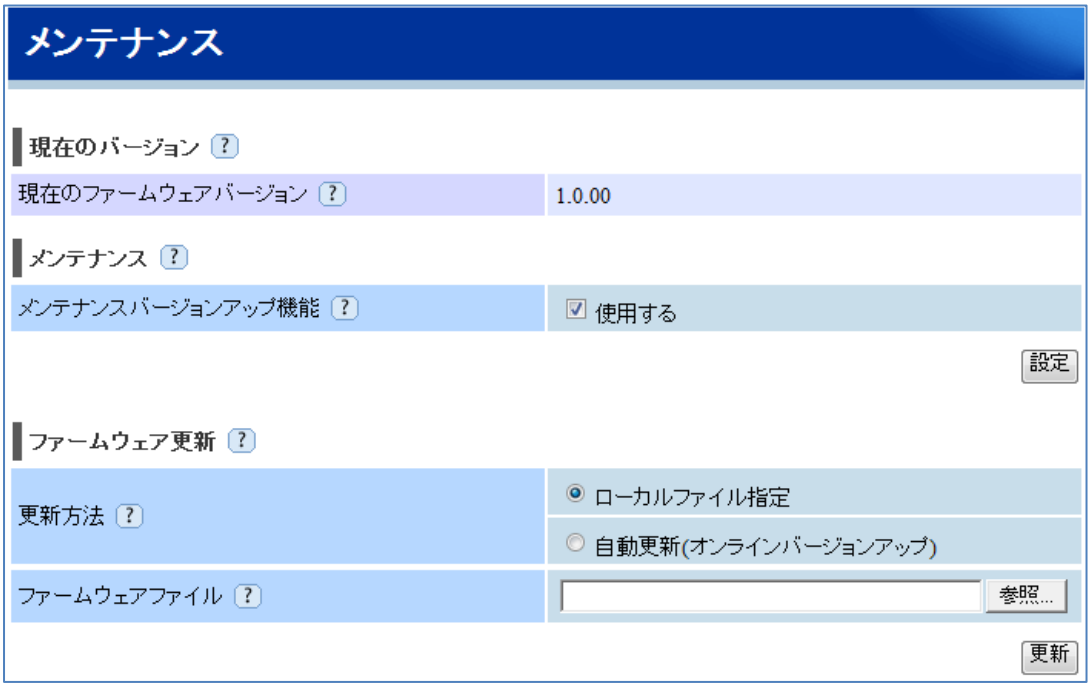
本製品の運用ポリシーにしたがい、どちらの方法でファームウェア更新するかを決めてください。

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ー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 OPT2 スイッチを押下する方法 ● 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 本機能の初期値は有効です。
設定 Web を使用して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。 ● ローカルファイルを指定してファームウェアを更新 ● 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

[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ーに通知します。[21]
- 特定事由により、OPT2 スイッチを押下せずに（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。



[21] 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. 「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。

[ファームウェアの更新①]

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 秒以上押下します。
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。

※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（本製品は再起動しません）。

[ファームウェアの更新②]

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。

[ファームウェアの更新③]

緊急を要する場合など、自動で（お客様の操作なしに）ファームウェアを更新する場合があります。

この場合も本製品を再起動します。

■設定 Web を使用する場合（ローカルファイル指定）

[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「参照」などのボタン（ブラウザにより異なる場合があります）を押下し、パソコンに保存された新しいファームウェアファイルを選択します。
3.「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。

[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。
- ファームウェアのバージョンダウンでは、設定値を初期化します。

■設定 Web を使用する場合（オンラインバージョンアップ）

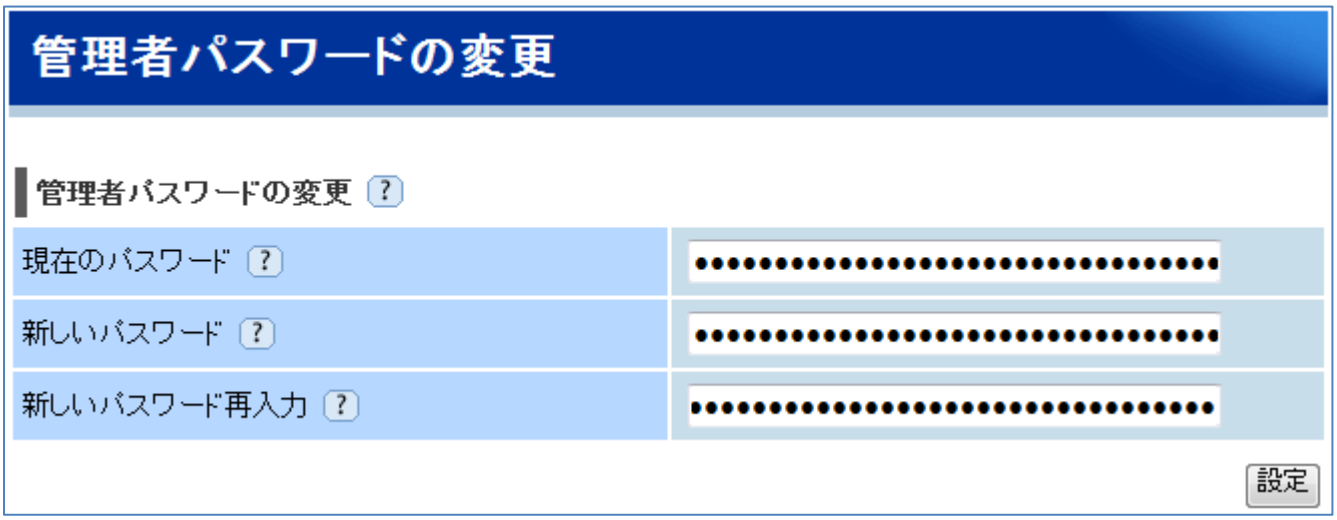
[設定]

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「自動更新（オンラインバージョンアップ）」を選択します。
3. 「更新」ボタンを押下します。
4.「最新のバージョン」が表示されるまで、そのまましばらく待ちます。
5.「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。
6.「OK」ボタンを押下します。
7. 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。
8. 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。

5.6.6. **パスワードの再設定**

定期的に変更することを推奨します。

本製品にログインする際のパスワードを設定（変更）します。



1. [TOP]-[メンテナンス]-[メンテナンス]-[管理者パスワードの変更]画面を開きます。
2. 管理者パスワードを変更します。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、新しいパスワードを保存します。

※ 手順 4 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
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。
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。
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。

5.6.7. **設定値の保存、復元**

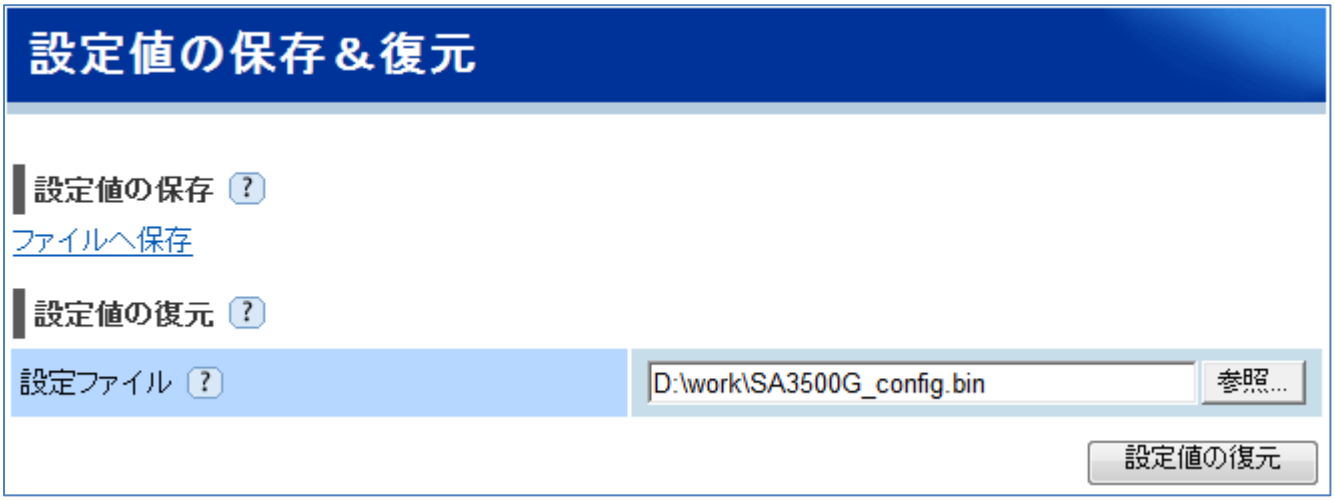
設定 Web で設定した設定値をパソコンなどに保存できます。

保存した設定値を本製品に復元することができます。

[メモ]

セキュリティ・スキャン機能は、シグネチャが更新されることによって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。



■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

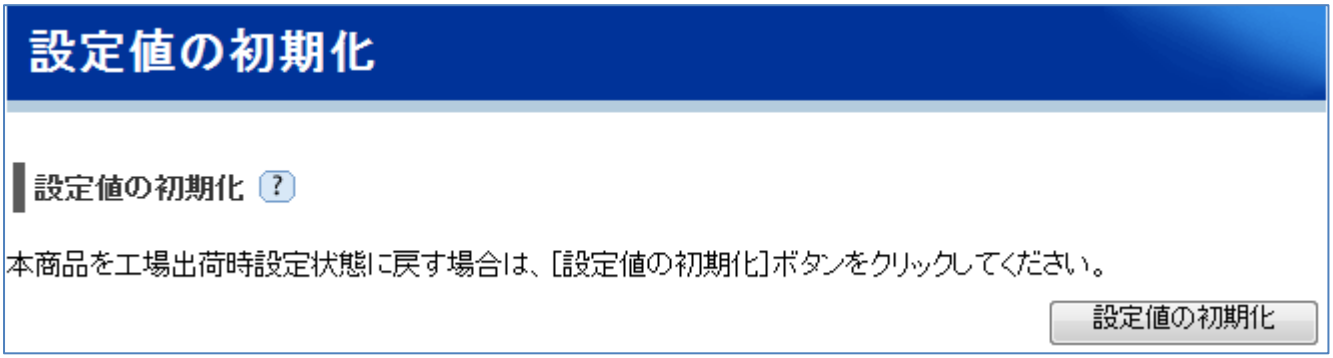
1. [TOP]-[メンテナンス]-[設定値の保存＆復元]画面を開きます。
2. 「設定ファイル」に 設定値の保存 で保存した設定値（bin ファイル）を入力し、「設定値の復元」ボタンを押下します。
3. 設定値を復元した後、本製品は再起動します。再起動完了で設定値の復元は完了です。

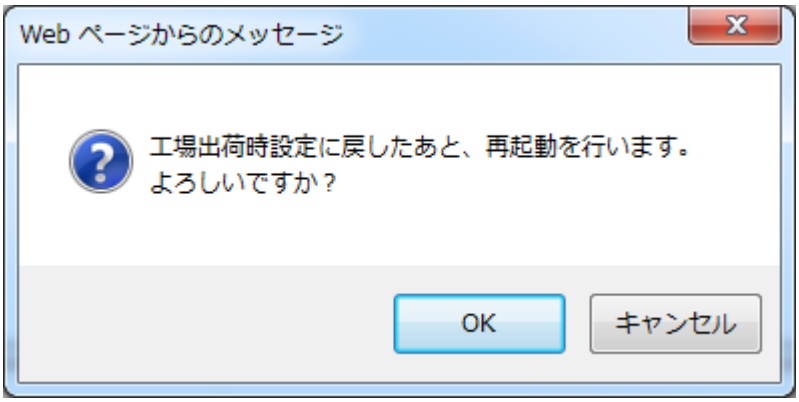
5.6.8. **設定値の初期化**

設定 Web で、設定値を初期状態に戻すことができます。

[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、統計情報は削除されます。





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。[22]
4. 本製品は自動的に再起動します。

[メモ]

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 5.9.1 章を参照してください。

[22] 「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。

5.6.9. **再起動**

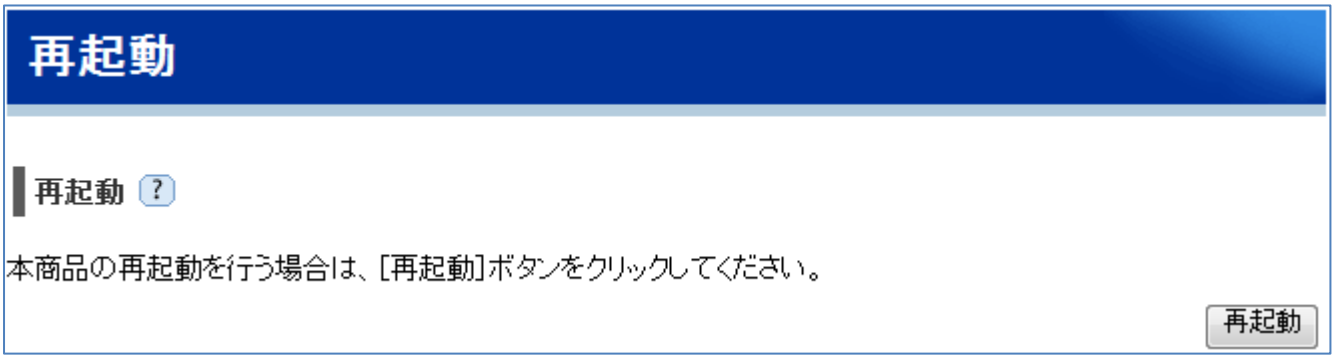
設定 Web で、本製品を再起動することができます。

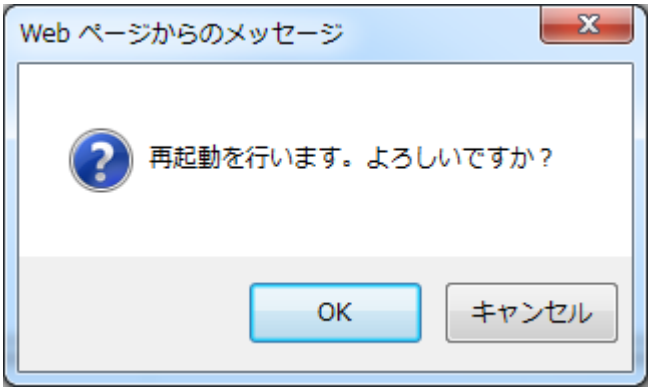
FlashROM に保存していない設定値がある場合、設定値の保存を促すメッセージを表示します。必要に応じて「保存」ボタンを押下し、設定値を FlashROM に保存してください。

[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

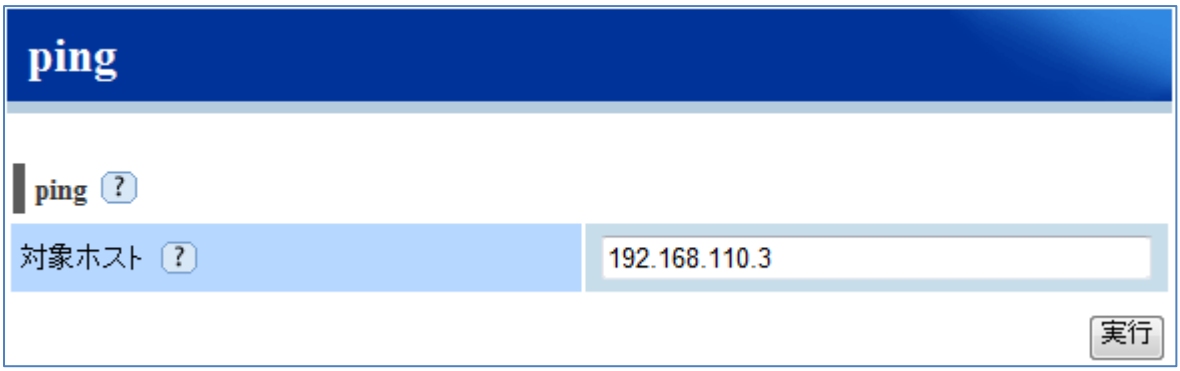




1. [TOP]-[メンテナンス]-[メンテナンス]-[再起動]画面を開きます。
2. 「再起動」ボタンを押下します。
3. 再起動する旨のメッセージウィンドウを表示しますので、「OK」ボタンを押下します。
4. 本製品が再起動します。
5. 「再起動が完了しました」画面がポップアップしたら、「OK」ボタンを押下します。
6. 再起動は完了です。

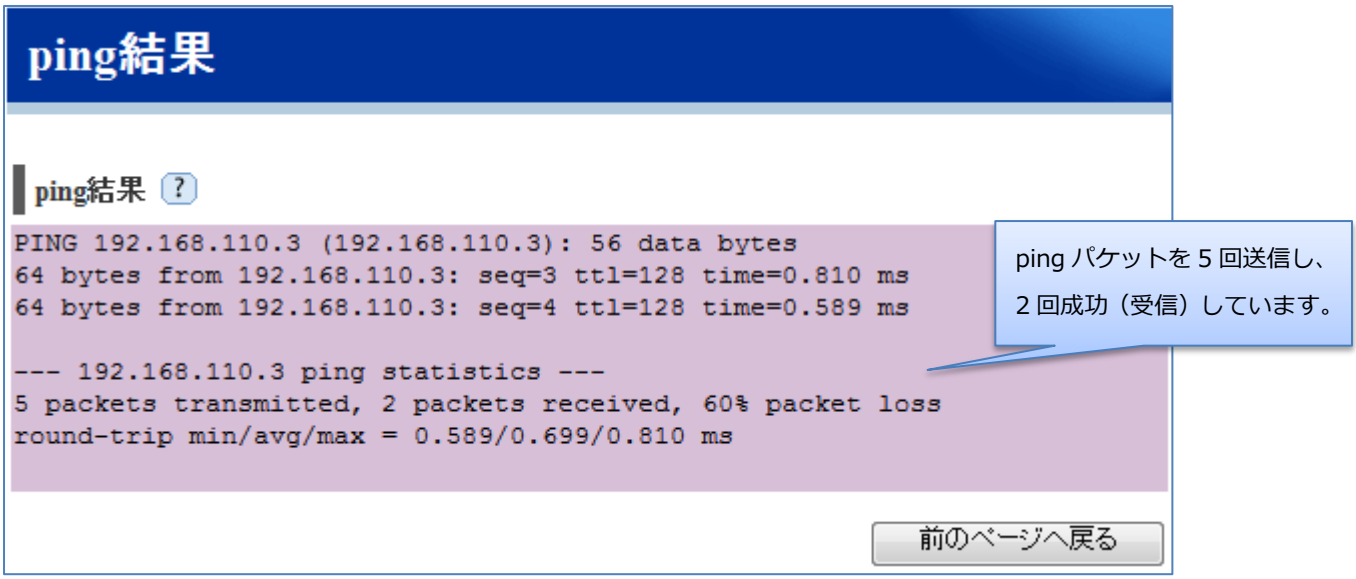
5.6.10. **ping 送信によるネットワーク到達確認**

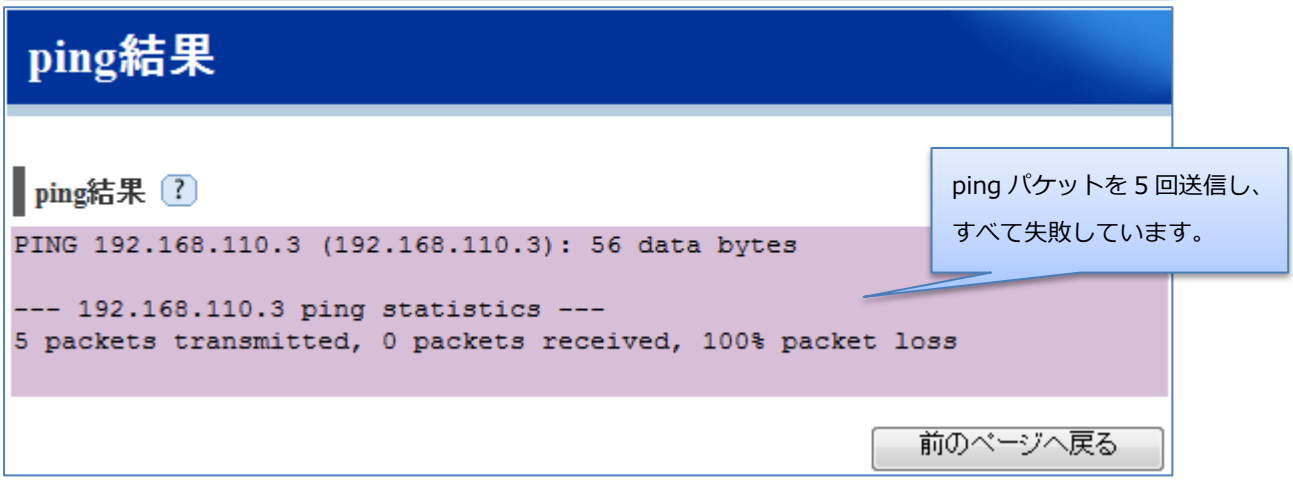
ネットワーク到達確認用途として、本製品から ping パケットを送信し、その到達を確認します。



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]

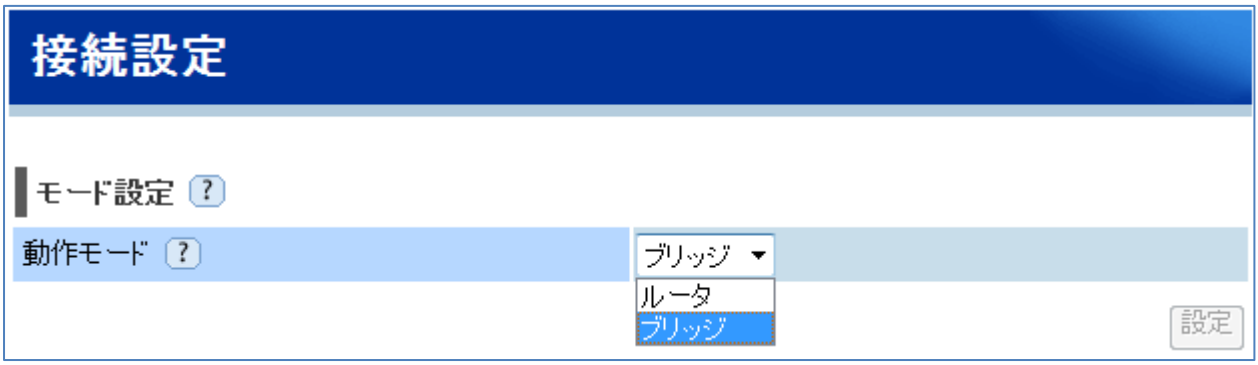


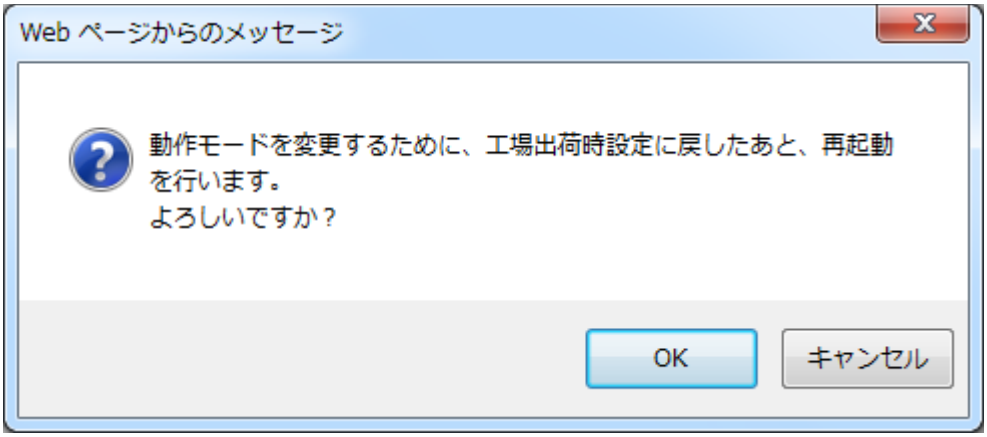


5.6.11. ルータモードへの切り替え

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。





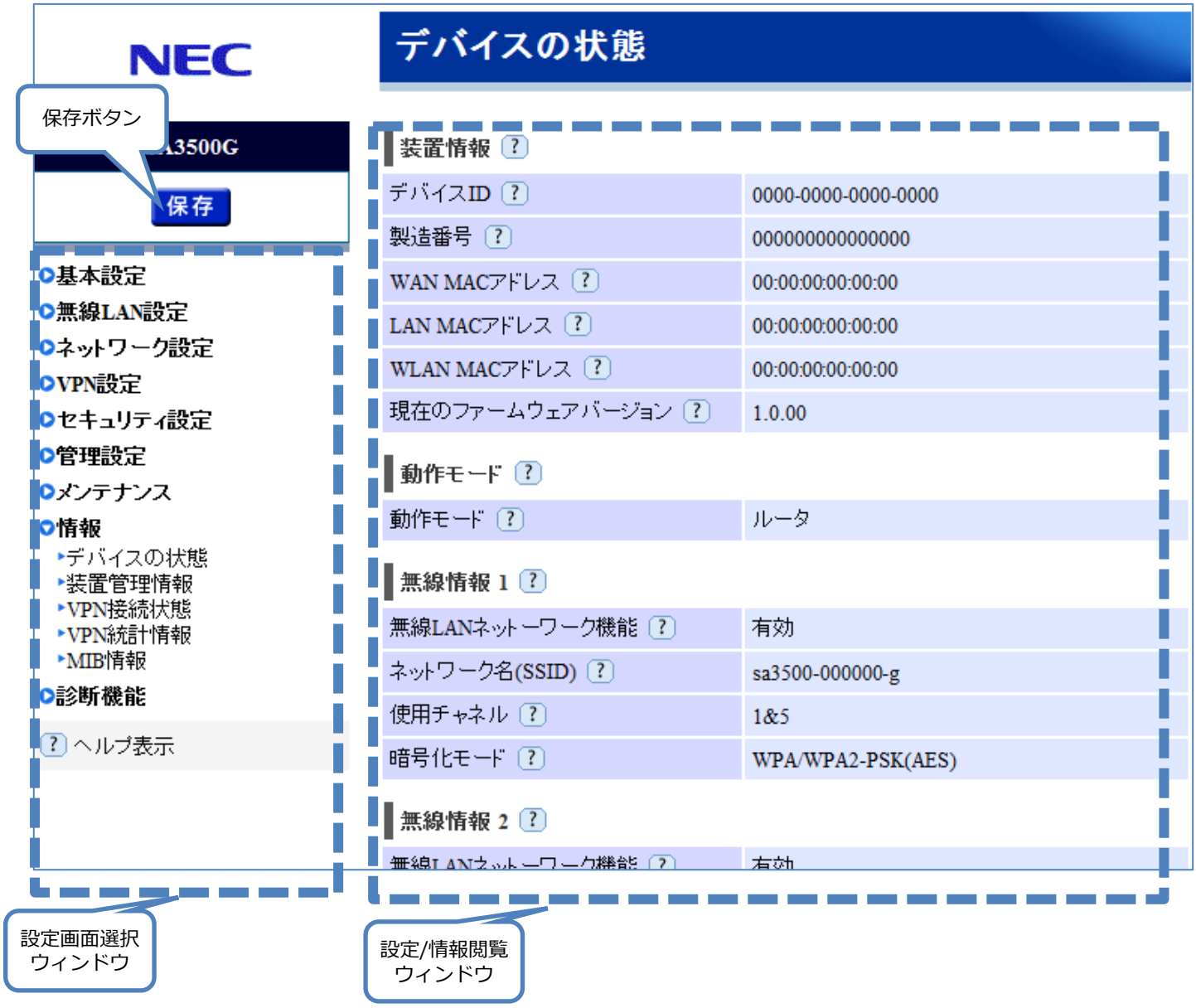
1. [TOP]-[メンテナンス]-[基本設定]-[接続設定]画面を開きます。
2. モード設定で「ルータ」を選択します。
3. 「設定」ボタンを押下します。
4. 再起動する旨のメッセージウィンドウを表示しますので、OK ボタンを押下します。
5. 再起動後、設定ウィザードの STEP2（管理者パスワード）が実行されます。5.2.2 章を参照し、設定してください。

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 ●印は設定項目の内容です。 ○印は表示項目の内容です。	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	※Ver3.1.26 で追加
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。	お客様の環境に合わせて設定してください
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	お客様の環境に合わせて設定してください
IPv4 WAN 設定（IPoE）	●DHCP クライアントの設定 ●HTTP プロキシサーバーの設定	お客様の環境に合わせて設定してください
IPv4 LAN 設定	●LAN インタフェースの IP アドレスの設定 ●DHCP サーバーの設定	お客様の環境に合わせて設定してください
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	お客様の環境に合わせて設定してください
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	お客様の環境に合わせて設定してください
DNS 設定	●DNS 機能の設定	お客様の環境に合わせて設定してください
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	お客様の環境に合わせて設定してください
その他の設定	●ICMP redirect パケット送信有無の設定	お客様の環境に合わせて設定してください
VPN 設定	VPN 接続に関する設定	
IPsec 設定	●IPsec/IKEv1 の設定	お客様の環境に合わせて設定してください
セキュリティ設定	IPv4 パケットフィルタリングに関する設定	
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	お客様の環境に合わせて設定してください
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	本製品を SNMP で管理する場合は設定してください
メンテナンス	メンテナンスに関する設定	
管理者パスワードの変更	●設定画面のパスワードの設定	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	
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	
	VPN 接続状態	○IPsec SA、IKE SA の状態	
	VPN 統計情報	○IPsec トラフィックの統計情報	
	MIB 情報	○SNMP MIB 情報	
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	

5.7.2. LAN インタフェースの IP アドレス設定

お客様のネットワークに合わせて設定してください。

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。 （5.7.6 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**

お客様のネットワークに合わせて設定してください。

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

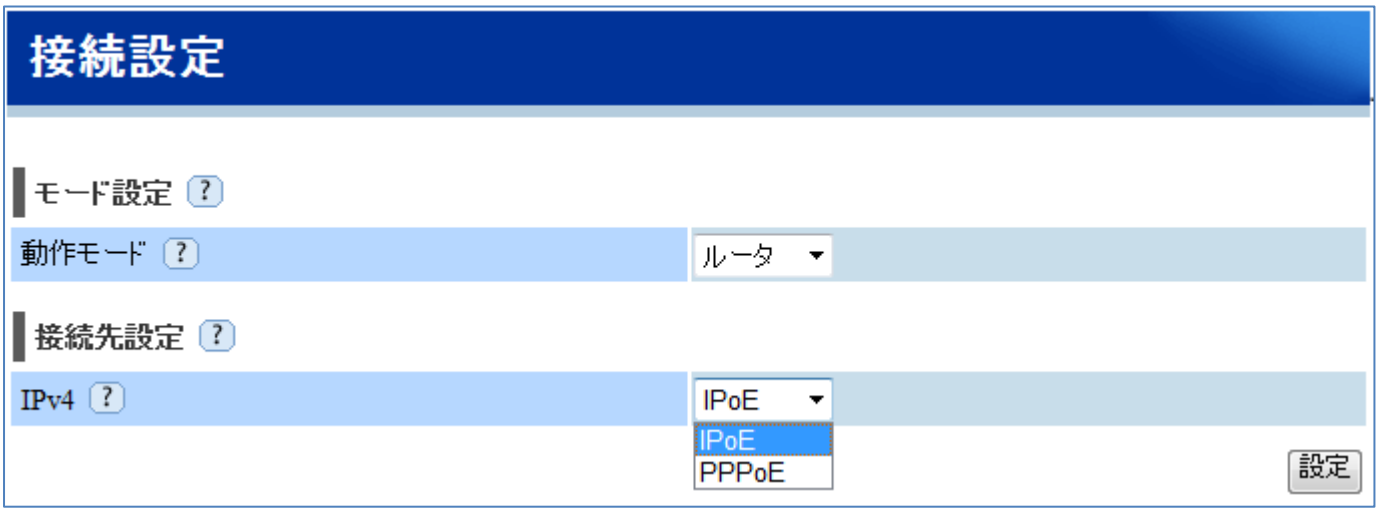
次の手順で設定します。

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	5.7.4 章を参照してください
(c)	PPP 機能を使用して設定	5.7.5 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 サーバーアドレスの設定が必要です。(5.7.7 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 サーバーアドレス	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 サーバー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 サーバーから取得する場合 • **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 サーバーアドレスの設定

5.7.7 章を参照してください。

5.7.4. DHCP クライアントの設定

お客様のネットワークに合わせて設定してください。

本製品の WAN インタフェースの IP アドレスを 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。

5.7.5. PPP/PPPoE の設定

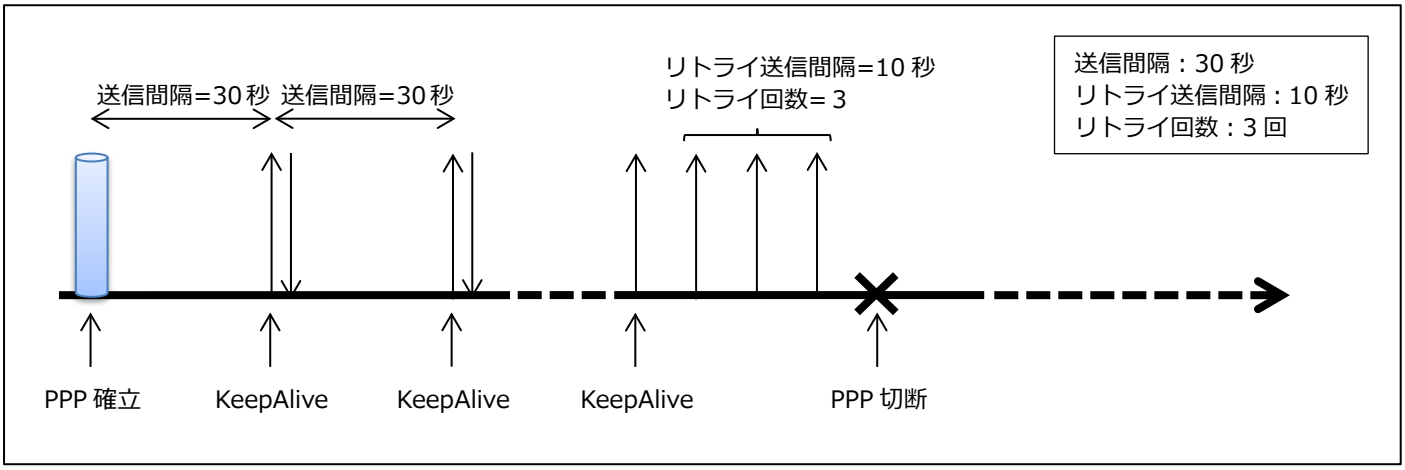
お客様のネットワークに合わせて設定してください。

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	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（サーバー）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（サーバー）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（サーバー）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



5.7.6. **DHCP サーバー**

お客様のネットワークに合わせて設定してください。

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 サーバー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
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。	192.168.110.1/24
DHCP サーバ	本製品の DHCP サーバーアドレスの設定		
DHCP サーバ機能	• **チェック有**…DHCP サーバー機能を使用する場合 • **チェック無**…DHCP サーバー機能を使用しない場合		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 サーバーが配布可能な 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 50 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 50 です。	192.168.110.51
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 サーバーの IP アドレスを設定してください。	DHCP の option44 の値です。	無効

5.7.7. DNS サーバーの設定

お客様のネットワークに合わせて設定してください。

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 サーバーの取得ができない場合、DNS サーバー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 サーバー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 サーバー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 サーバーアドレスの設定を DHCP クライアントまたは PPP で取得する場合 • **手動設定**…DNS サーバー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 サーバーの 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 サーバーの 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

5.7.8. スタティックルーティング

スタティック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。

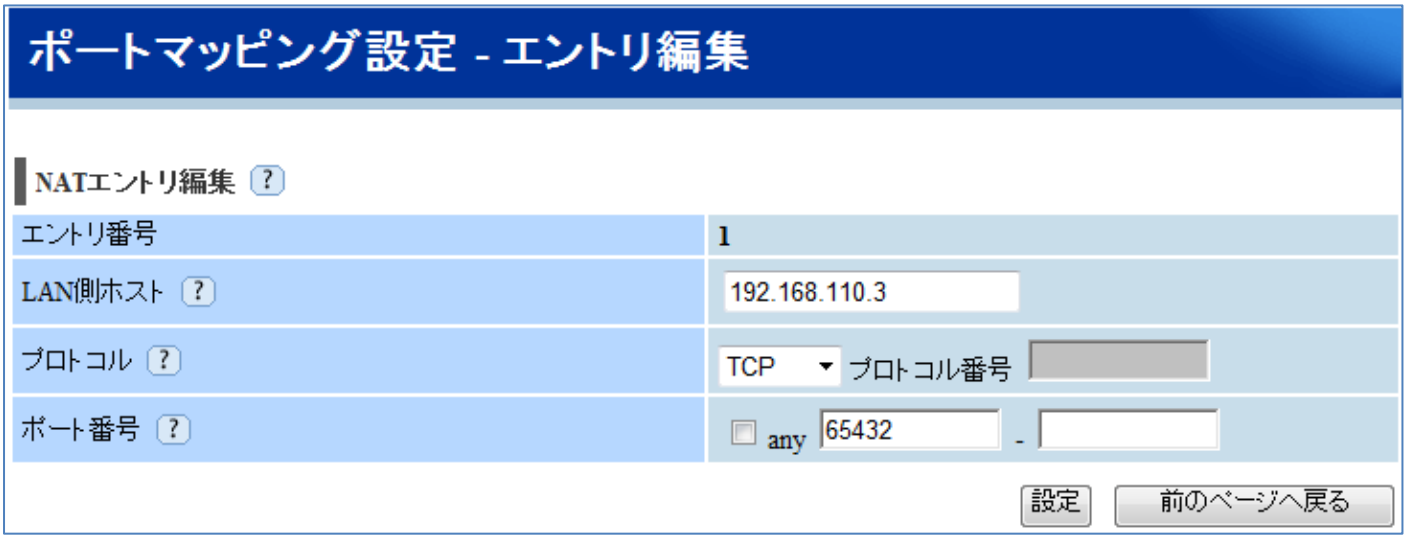
設定項目		**値**	備考	初期値
IPv4 静的ルーティングエントリ編集			50 エントリ設定できます。	
	エントリ番号	エントリの番号が入ります。		未設定
	宛先 IP アドレス	ルーティングエントリの宛先ネットワークを指定してください。		未設定
	指定方法	• **インタフェース**…ルーティング先をインタフェースで指定する場合 • **ゲートウェイ**…ルーティング先を IPv4 アドレスで指定する場合		未設定
	インタフェース	• PPPoE が入ります。		未設定
	ゲートウェイ	ゲートウェイの IPv4 アドレスを設定してください。		未設定
	メトリック	メトリック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

5.7.9. **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指定します。 • **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

5.7.10. **パケットフィルタエントリに関する設定**

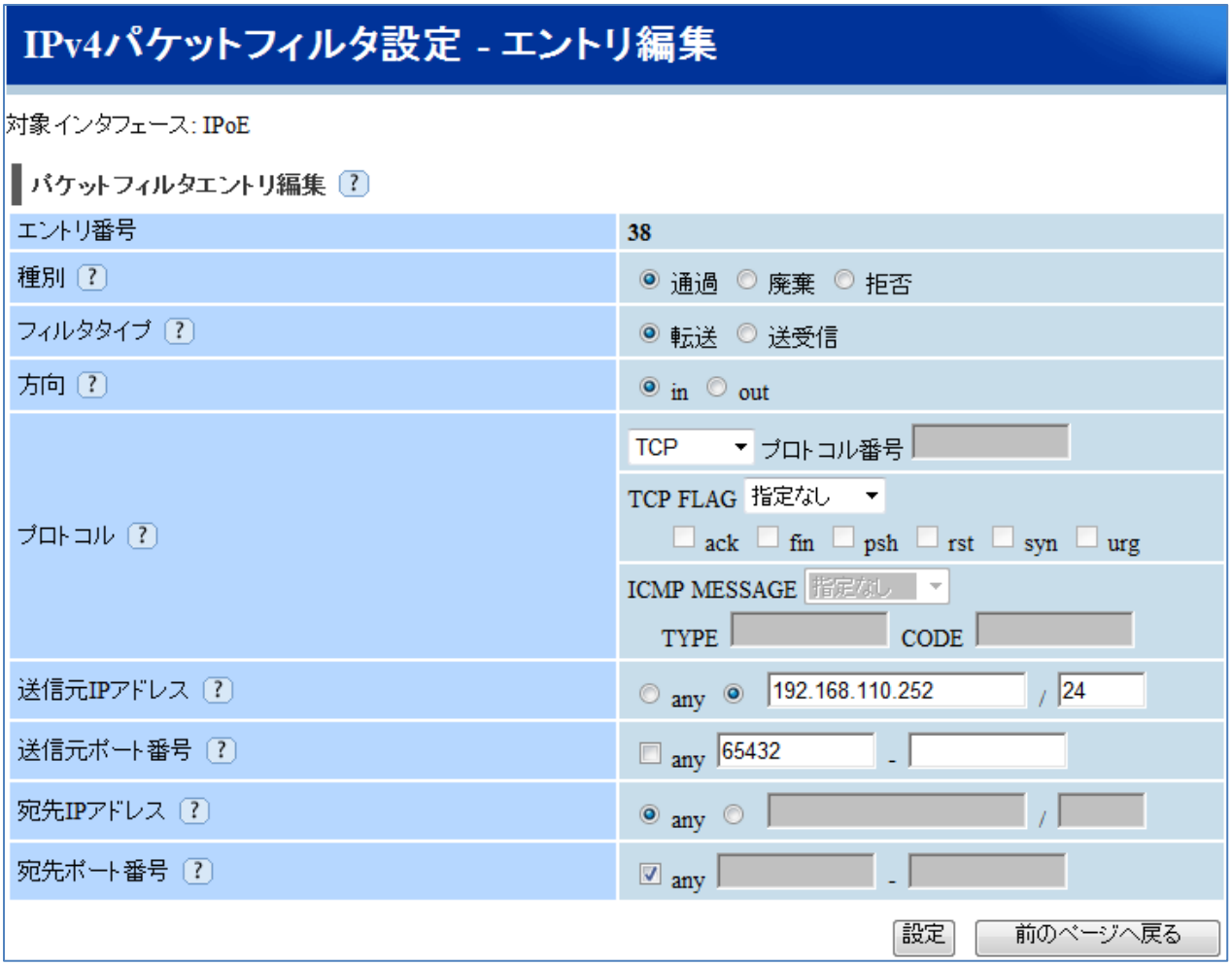
特定の条件を満たすパケットの通過や廃棄を設定できます。[23]

エントリ番号	種別	方向	プロトコル	送信元	送信元ポート	宛先	宛先ポート	編集	削除
1	drop	out	UDP	any	any	any	137-139	編集	削除
2	drop	out	TCP	any	any	any	137-139	編集	削除
3	drop	out	UDP	any	any	any	445-445	編集	削除
4	drop	out	TCP	any	any	any	445	編集	削除
5	drop	out	TCP	any	any	any	2049	編集	削除
6	drop	out	UDP	any	any	any	2049	編集	削除
7	drop	out	TCP	any	any	any	1243	編集	削除
8	drop	out	TCP	any	any	any	12345	編集	削除
9	drop	out	TCP	any	any	any	27374	編集	削除
10	drop	out	TCP	any	any	any	31785	編集	削除

1～10 | 11～20 | 21～30 | 31～40 | 41～50

1. [TOP]-[メンテナンス]-[セキュリティ設定]- [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」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。

[23] 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。



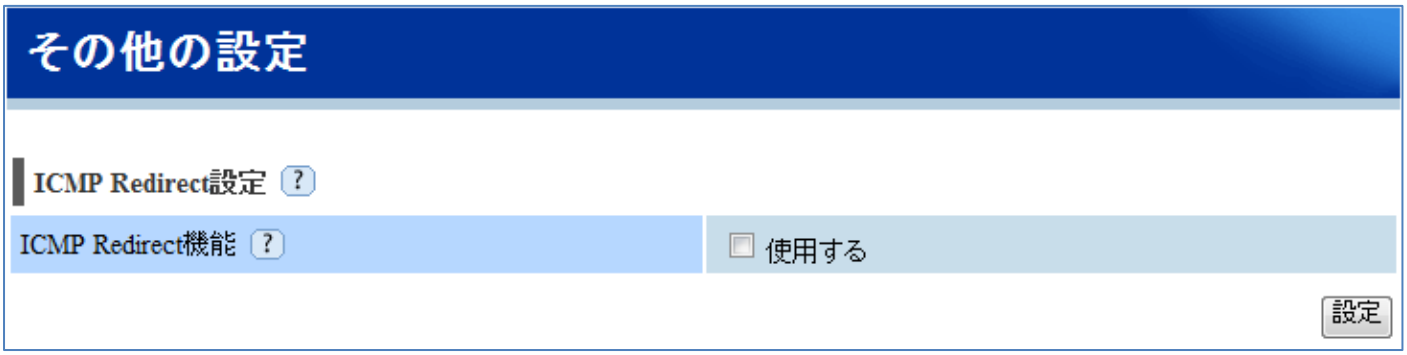
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

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（silentry 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		未設定
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		未設定

	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		未設定
	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		未設定
	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		未設定
	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		未設定
	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

5.7.11. **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か否かを設定します。
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
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

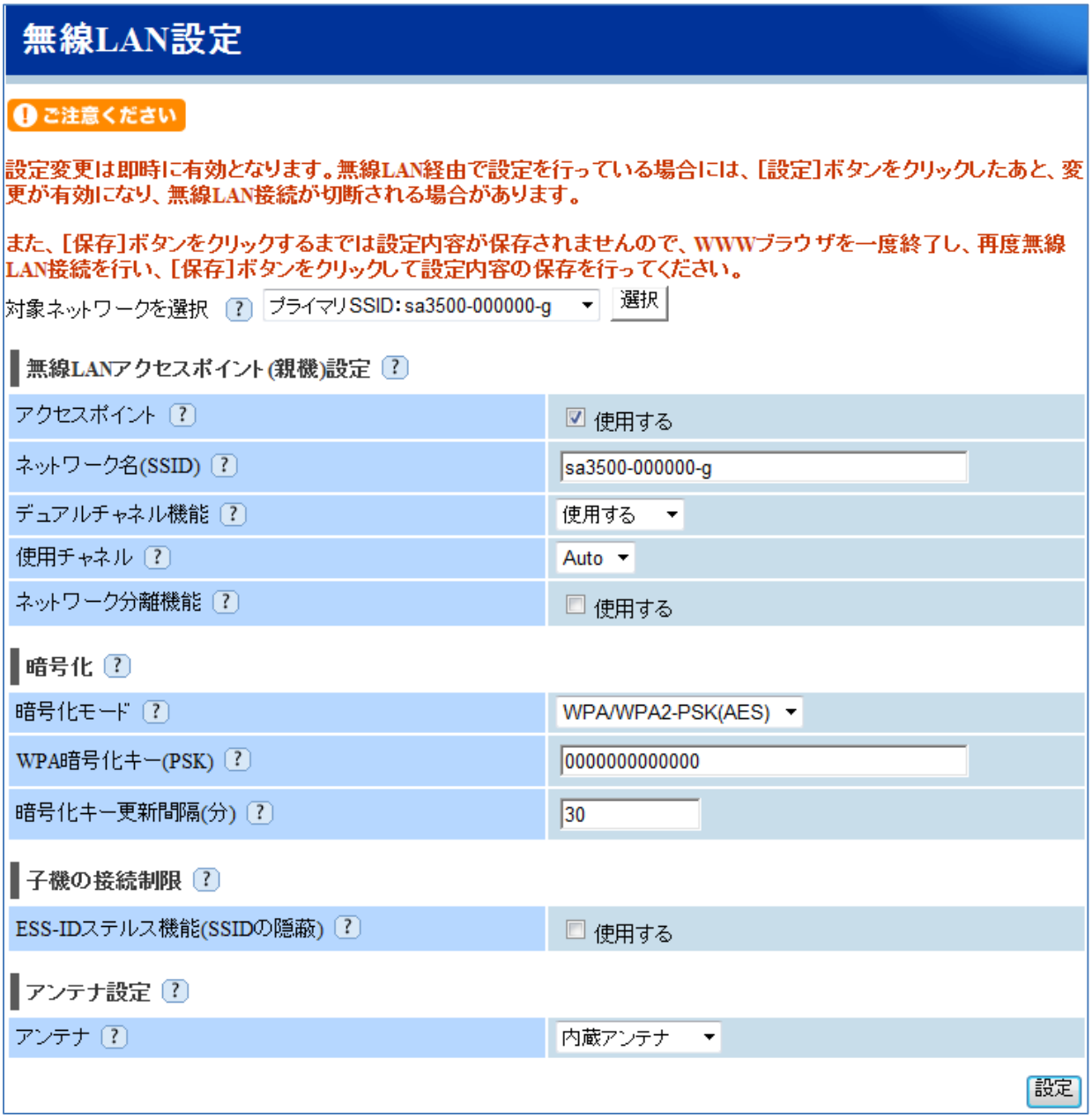
5.7.12. 無線 LAN の設定

本製品は、アクセスポイントとして動作します。

WPS 操作については、5.9.5 章を参照してください。

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。

外付けアンテナはオプション品です。



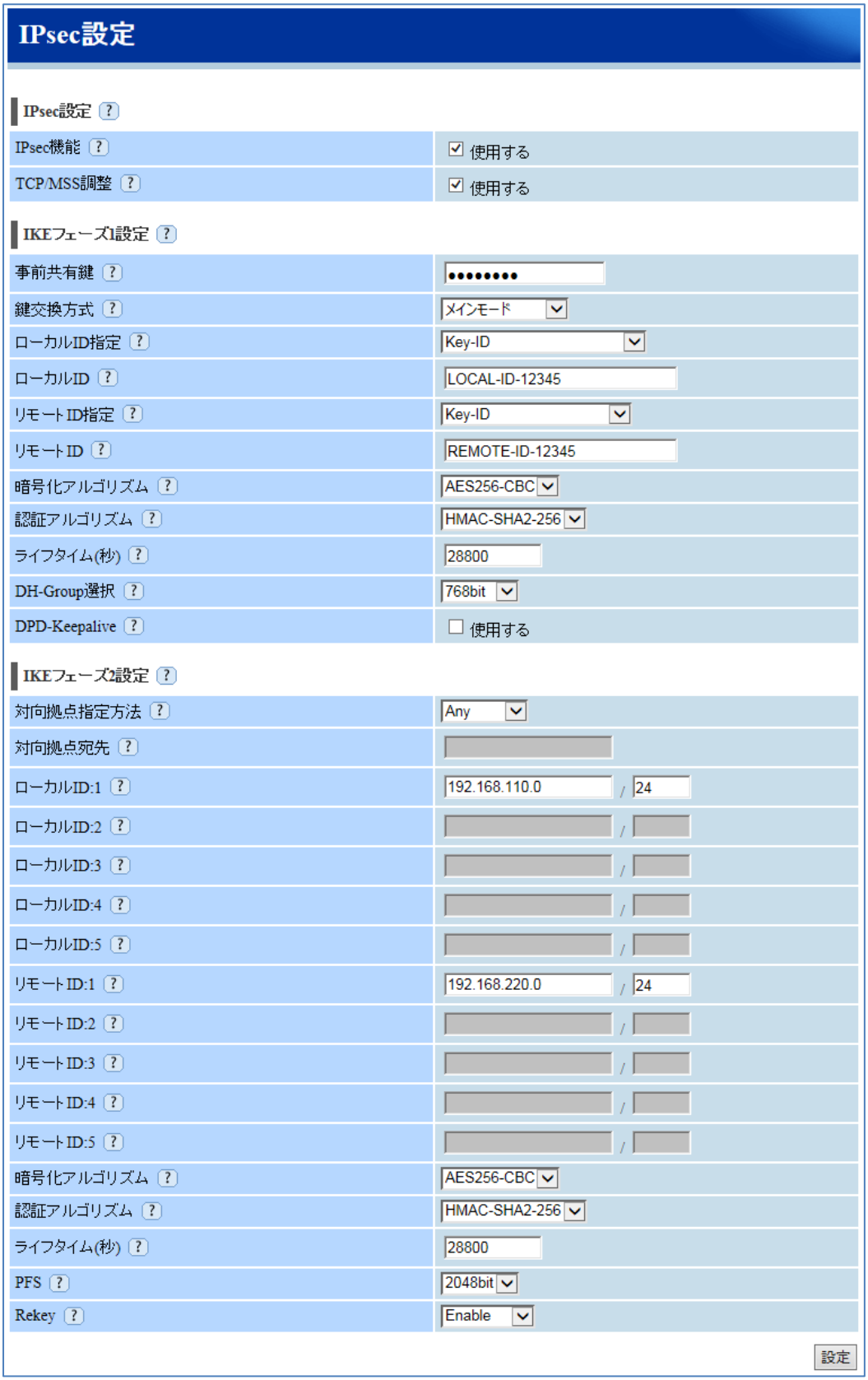
1. [TOP]-[メンテナンス]-[無線 LAN 設定]-[無線 LAN 設定]画面を開きます。
2. 「アクセスポイント」の「使用する」をチェックします。
3. 外付けアンテナを使用している場合は、「アンテナ」を「外付けアンテナ」に変更します。
4. 「設定」ボタンを押下します。
5. 「保存」ボタンを押下します。

設定項目	値	備考	初期値
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。	入力可能文字列は、半角英数字、-(ハイフン)、_(アンダースコア) 入力可能文字数は最大 32 文字	プライマリ：sa3500-XXXXXX-g セカンダリ：sa3500-XXXXXX-gw XXXXXX は装置ごとに異なる値が入ります。
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	• **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）**		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、記号)で 8～63 ケタまたは、16 進数(0～9、a～f、A～F)で 64 ケタ	プライマリ、セカンダリともに装置ごとに異なる値が入ります
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

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		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）

5.7.13. **IPsec の設定**

本製品は、IPsec/IKEv1 をサポートしています。



1. [TOP]-[メンテナンス]-[VPN 設定]-IPsec 設定]画面を開きます。
2. IPsec に関する設定を入力します。
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
TCP MSS 調整	• **チェック有**…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 (「"、'、`、#、¥、$、スペース、?」を除く)	事前鍵共有方式のみサポートしています	未設定
鍵交換方式	• **メインモード**…本製品と対向の IPsec 機器のどちらも IPsec トンネルの IP アドレスが固定値の場合に選択します **アグレッシブモード**…本製品または対向の IPsec 機器のどちらか、またはいずれも IPsec トンネルの IP アドレスが不定値の場合に選択します	固定鍵方式をサポートしていません	メインモード
ローカル ID 指定	IKE フェーズ 1 で送信する自装置の ID ペイロードの入力形式を設定します。 • **指定しない(送信元 IP アドレス)**…本製品の WAN インタフェースの IP アドレスを使用します • **IP アドレス**…IP アドレス • **FQDN**…ドメイン名 • **Key-ID**…任意の文字列 • **User-FQDN**…ユーザー名付きドメイン名		指定しない（送信元 IP アドレス）
ローカル ID	「ローカル ID 指定」で選択した入力形式にしたがって ID を設定します。 • **IP アドレス**…IP アドレスの形式で設定してください • **FQDN**…ドメイン名の形式で設定してください。入力可能文字列は、英数半角 1～64 文字です。 • **Key-ID**…入力可能文字列は、英数半角 1～47 文字です。 • **User-FQDN**…"ユーザー名@ドメイン名”の形式で設定してください。入力可能文字列は、英数半角 3～160 文字です。 ※「FQDN」,「Key-ID」,「User-FQDN」では ASCII 記号 0x21~0x7e(「"、'、`、#、¥、$、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	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** • **AES192-CBC** • **AES128-CBC** • **3DES-CBC**		AES256-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 秒間隔で送信します。	無効
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。また、静的ルーティング設定が必要です。	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。（静的ルーティング設定は必要ありません）	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**		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
	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

[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、通常のスタティック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。

■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は次のとおりです。

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, 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は次のとおりです。

・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

接続形態	LAN-WAN 接続パターン	ローカル ID	リモート ID
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。

[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]

■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。

[IPsec の設定例]

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。

SA3500G IP アドレス

LAN ：192.168.110.1/24

WAN：192.168.100.2/24

IX2215 IP アドレス

LAN ：10.0.0.254/24

WAN：192.168.100.10/24

■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。

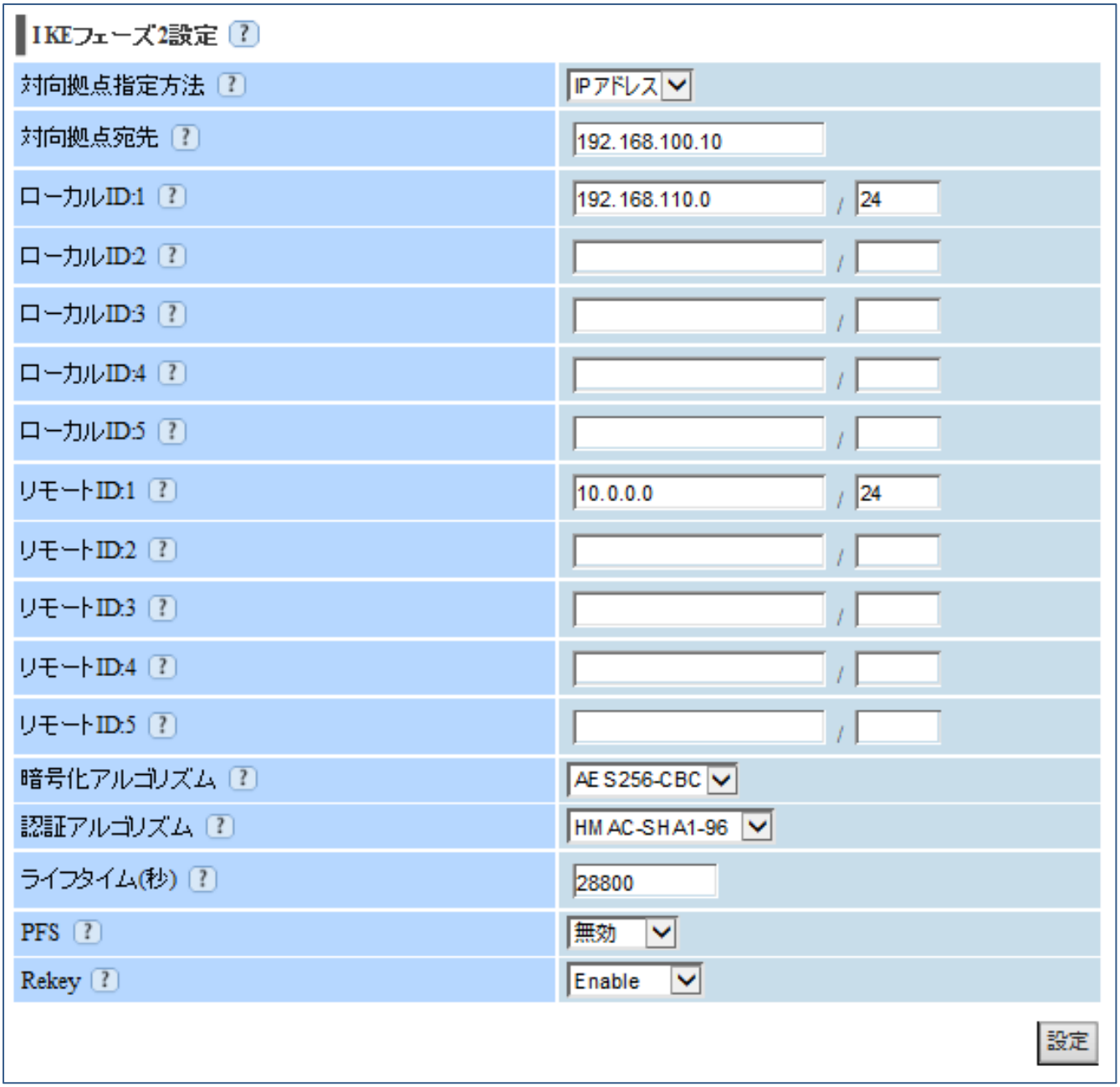
IPsec設定

IPsec設定

IPsec機能	☑ 使用する
TCP/MSS調整	☑ 使用する

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


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
10.0.0.0
24
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
PFS
無効
Rekey
Enable
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。

■かんたん設定
かんたん設定
■詳細設定
詳細設定
装置
パスワードの設定
装置名の設定
時刻の設定
LAN
LANアドレスの設定
DHCPサーバの設定
WAN
プロバイダの設定
静的NAPTの設定
WANフィルタの設定
VPN
VPNの設定
リモート保守
SSH/Telnetの設定
デバイス
デバイスの設定
■保守管理
保守管理
■外部リンク
製品ページ

VPNの設定

設定を変更する場合は [反映] を押してください。

接続種別の選択

接続種別の変更はできません。

	現在の設定	設定の変更
接続種別	IPsec	◉ IPsec
接続元アドレス契約	固定IPアドレス	◉ 固定IPアドレス
接続先アドレス契約	固定IPアドレス	◉ 固定IPアドレス

IPsecの詳細設定 (メインモード)

		現在の設定	設定の変更
接続名		SA3500G_1	接続を識別するための任意の名称を設定してください。 SA3500G_1
接続先 (相手装置)	WAN側 IPアドレス	192.168.100.2	接続先のIPアドレスを入力してください。 192.168.100.2
	LAN側 ネットワーク	192.168.110.0/24	接続先のLAN側のネットワークアドレスを入力してください。 192.168.110.0 / 24
ルーティング			接続先のLAN側ネットワークアドレス以外にも接続するネットワークアドレスがある場合に入力してください。 / 24 / 24 / 24 / 24

暗号/認証の詳細設定

設定は全て接続先の装置と一致させてください。

		現在の設定	設定の変更
IKE	事前共有鍵	hogehoge	接続先と共通のパスワードを設定してください。 hogehoge
	アルゴリズム	AES(256bit) SHA1	暗号 AES(256bit) / 認証 SHA1
	DHグループ	DH group 1(768bit)	DH group 1(768bit)
	ID	設定なし	メインモードでは設定しません。
IPsec	アルゴリズム	AES(256bit) SHA1	暗号 AES(256bit) / 認証 SHA1

戻る 反映

5.7.14. **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） **cold-start**：電源 OFF から電源 ON の場合に送信		ALL

		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

5.7.15. 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。

5.7.16. **HTTP プロキシサーバーの設定**

メンテナンス（ブリッジモード）の設定と同じです。5.6.3 章を参照してください。

5.7.17. **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。5.6.4 章を参照してください。

5.7.18. **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。5.6.5 章を参照してください。

5.7.19. **パスワードの再設定**

メンテナンス（ブリッジモード）の設定と同じです。5.6.6 章を参照してください。

5.7.20. **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。5.6.7 章を参照してください。

5.7.21. **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。5.6.8 章を参照してください。

5.7.22. **再起動**

メンテナンス（ブリッジモード）の設定と同じです。5.6.9 章を参照してください。

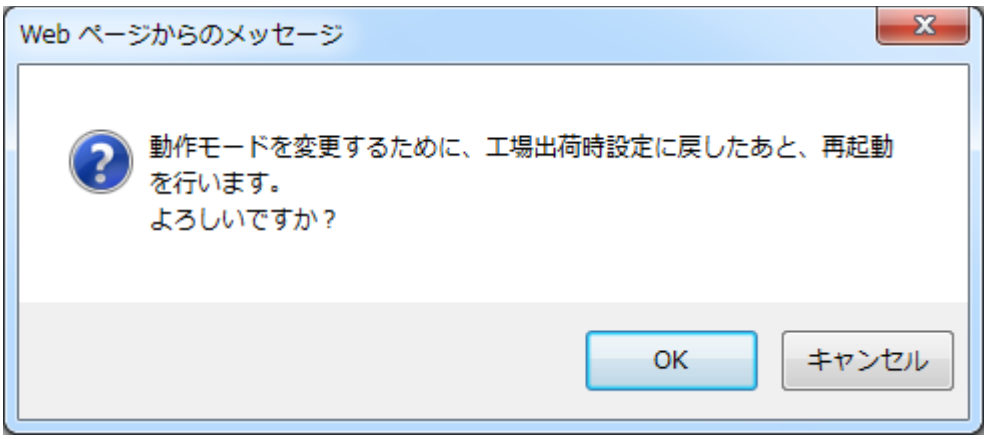
5.7.23. **ping 送信によるネットワーク到達確認**

メンテナンス（ブリッジモード）の設定と同じです。5.6.10 章を参照してください。

5.7.24. 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、ルーターモードで共通です。

（一部の機能は、いずれかのモードのみ使用します。）

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。

※画面の表示内容は動作モードにより異なります。

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 ●印は設定項目の内容です。 ○印は表示項目の内容です。	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	
ファイアウォール（FW）	●DoS アタックに関する設定 ●NAPT セッションタイマの設定	※Ver3.1.26 で追加（ルータモードのみ動作します）
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	※Ver3.1.26 で個別許可の設定機能を追加
不正侵入防止（IPS）	●IPS に関する設定	
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	※Ver3.1.26 で個別許可の設定機能を追加
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	※Ver3.1.26 で個別許可の設定機能を追加
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	※Ver3.1.26 で追加
オプション	●パトライトとの連携に関する設定	※Ver3.1.26 で追加
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 ※Ver3.1.26 で個別許可の設定機能を追加
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

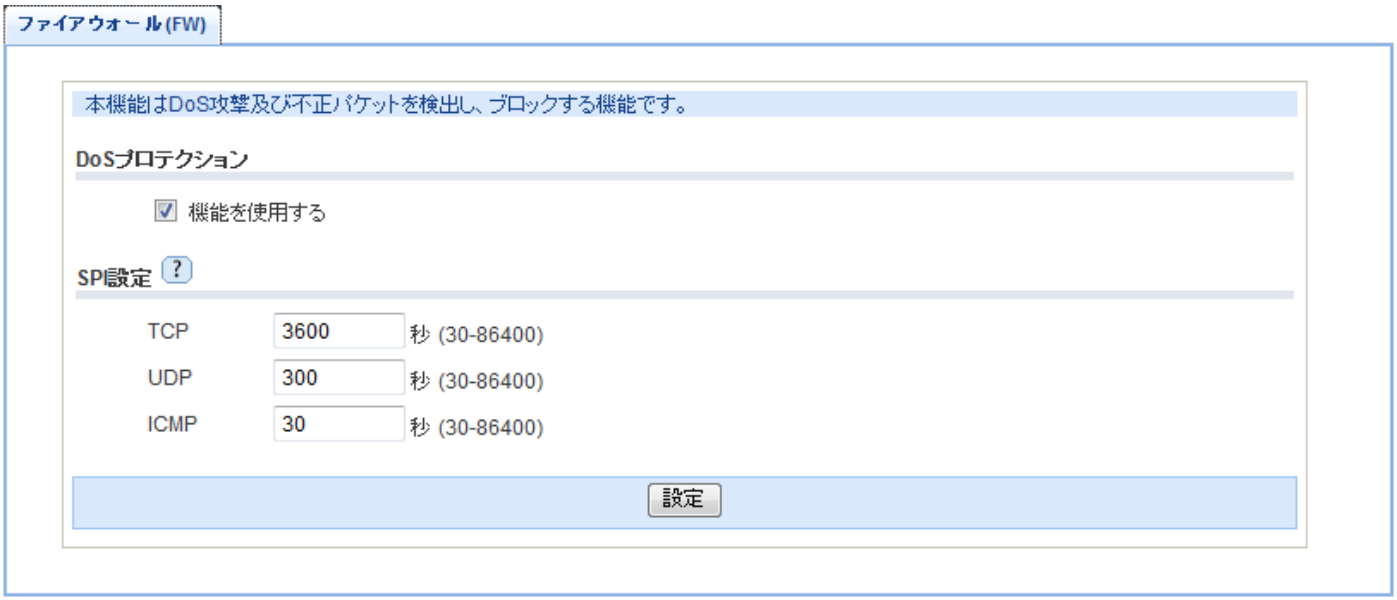
5.8.2. ファイアウォール（FW）

必ず確認してください。

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。

本機能は、ルータモード時に動作します。ルータモード時、SPI 設定は常時有効となります。

■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. 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。
3. 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。
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。

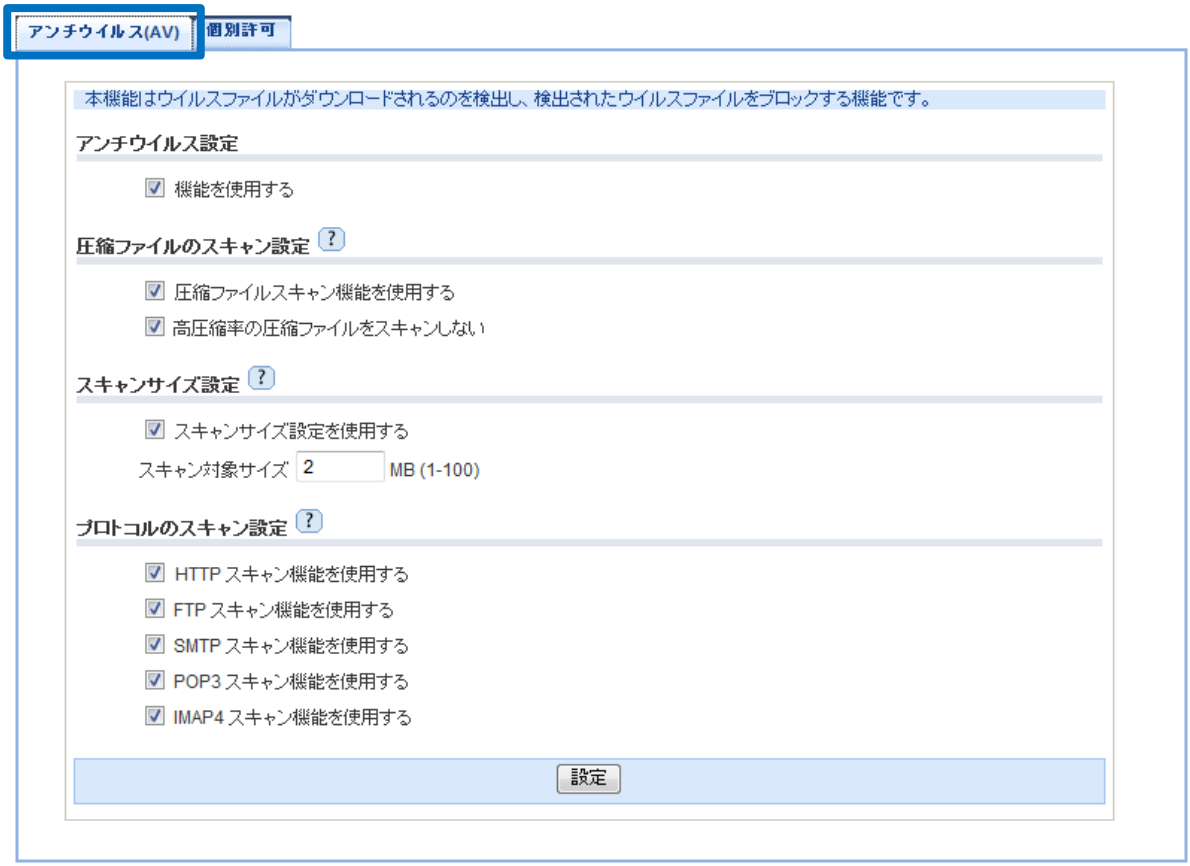
設定項目	説明	初期値
DoS プロテクション	DoS 攻撃（Smurf 攻撃、IP スプーフィング攻撃）を検出し、これらのアクセスを廃棄する場合は、本項目をチェックします。 本機能を無効化した場合、Smurf 攻撃、IP スプーフィング攻撃のパケットを検出対象から外します。	有効
SPI 設定	NAPT セッションタイマに関する設定項目です。	
TCP	TCP establish の NAPT セッションタイマを設定します。 設定範囲は、30~86,400 秒です。	3,600
UDP	UDP の NAPT セッションタイマを設定します。 設定範囲は、30~86,400 秒です。	300
ICMP	ICMP の NAPT セッションタイマを設定します。 設定範囲は、30~86,400 秒です。	30

5.8.3. **アンチウイルス（AV）**

必ず確認してください。

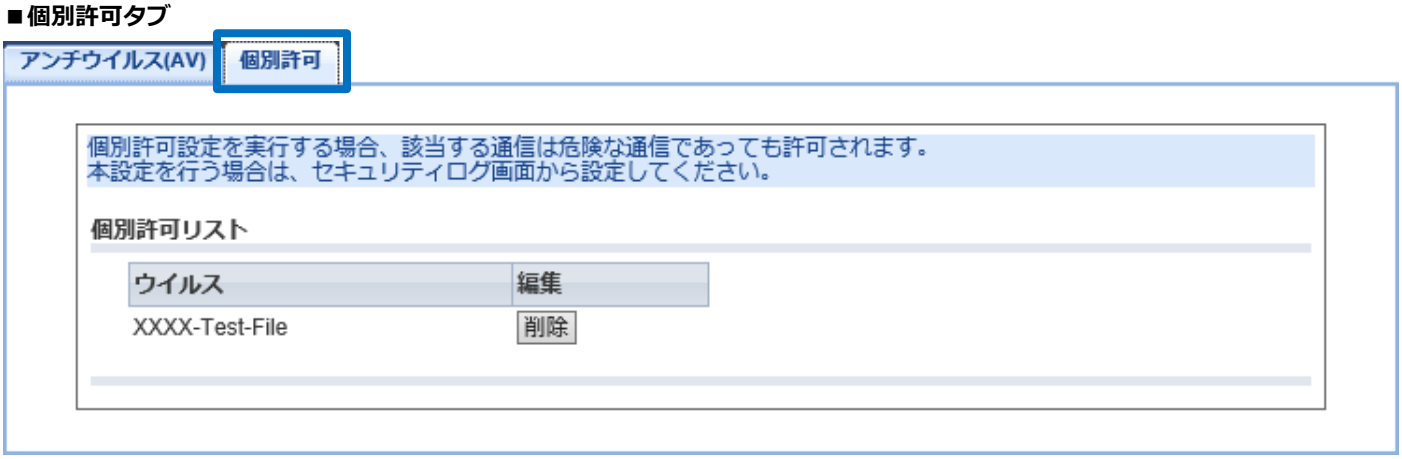
アンチウイルス機能を運用ポリシーにしたがい、適切な内容に設定してください。

■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 6.1.8 章を参照してください。

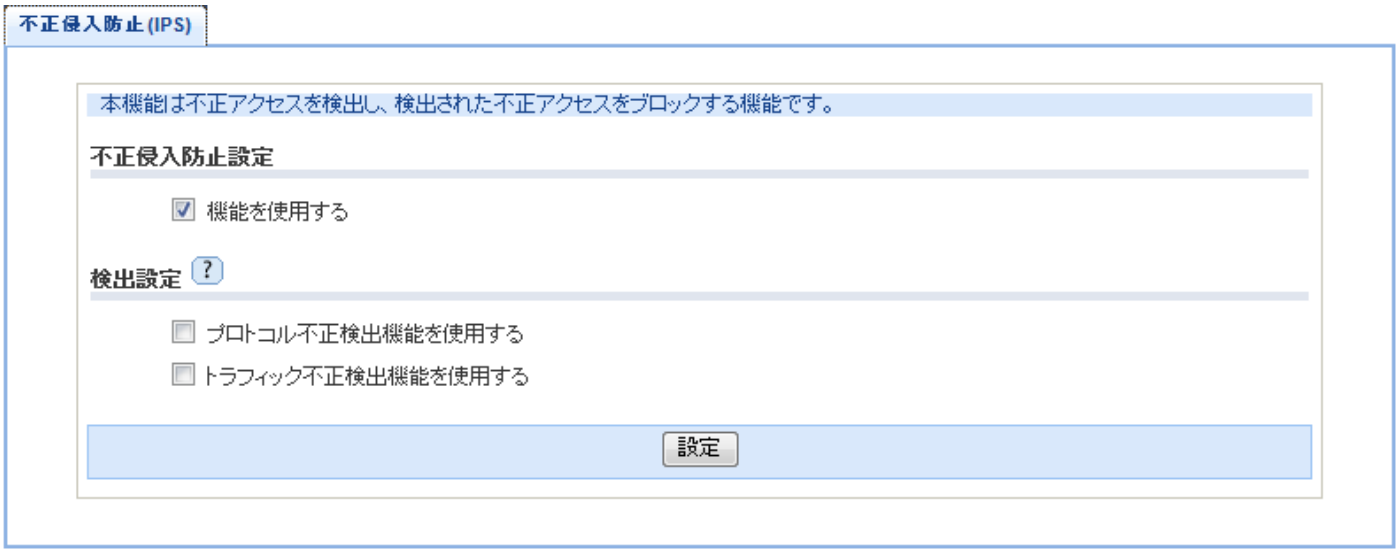
設定項目	説明	初期値
アンチウイルス設定	ウイルスや危険なコードが含まれるプログラムを検出した場合にプログラムを書き換え無害化する機能を使用する場合は、本項目をチェックします。	有効
圧縮ファイルのスキャン設定	圧縮ファイルをスキャンする場合、本製品内で一度解凍してからスキャンします。このため、本処理中は一時的に処理速度が低下します。 ● 次の圧縮ファイルに対応しています。 gz, zip, rar, jar, apk ● パスワードを設定した ZIP ファイルなどはスキャンできません。	
圧縮ファイルスキャン機能を使用する	圧縮ファイルをスキャンする場合は、本項目をチェックします。	有効
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。	–

5.8.4. **不正侵入防止（IPS）**

必ず確認してください。

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
検出設定		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	不正な TCP トラフィックを検出した場合、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。[24]	無効
	トラフィック不正検出機能を使用する	TCP パケットのポートスキャンを検出した場合、そのトラフィックを遮断する場合は、本項目をチェックします。	無効

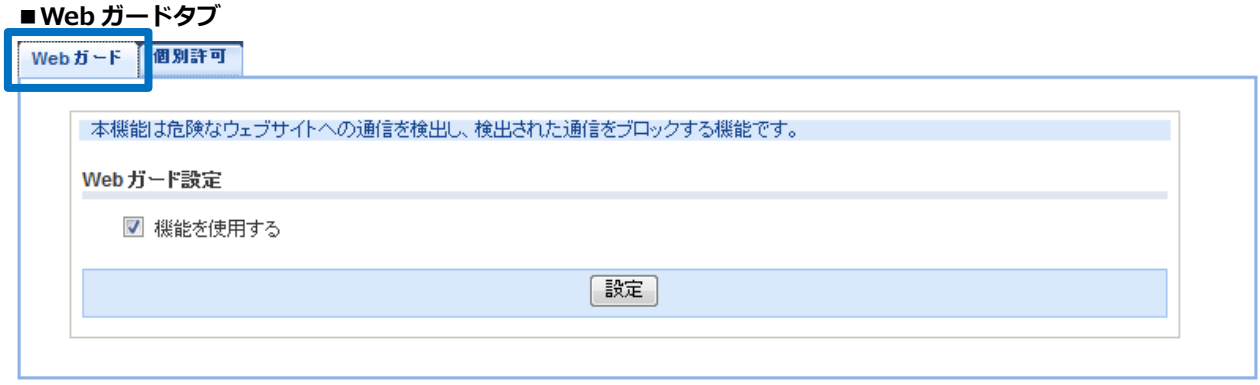
[24] 正常なトラフィックを不正なトラフィックと検出する可能性があるため、トラフィックを遮断しません。

5.8.5. Web ガード（WG）

必ず確認してください。

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。

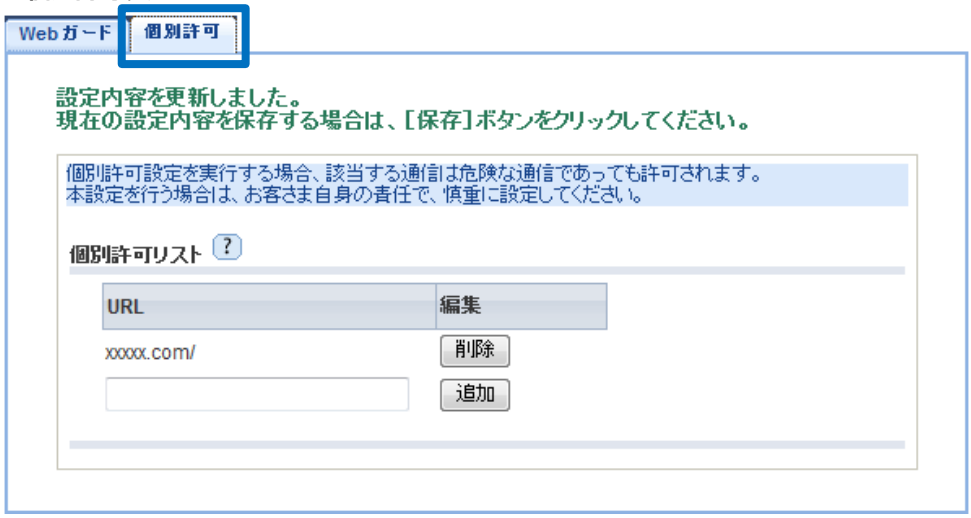
■Web ガードタブ



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

■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　：256 文字 登録可能件数　　：10 件	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。	－

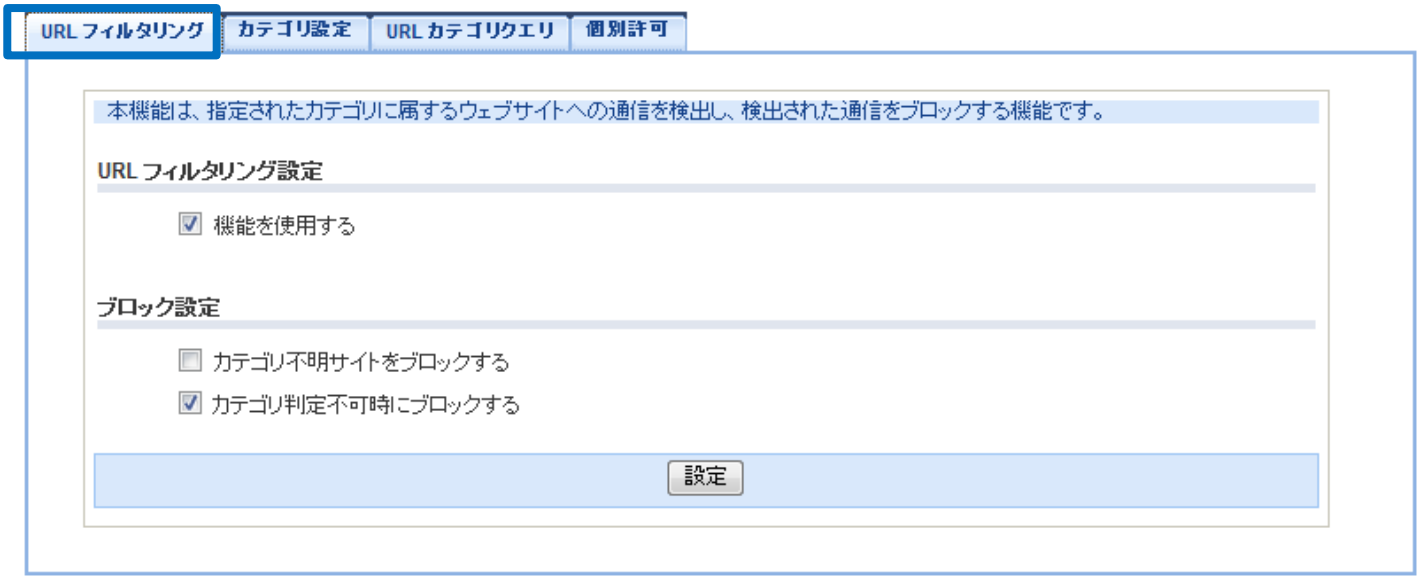
5.8.6. URL フィルタリング（UF）

必ず確認してください。

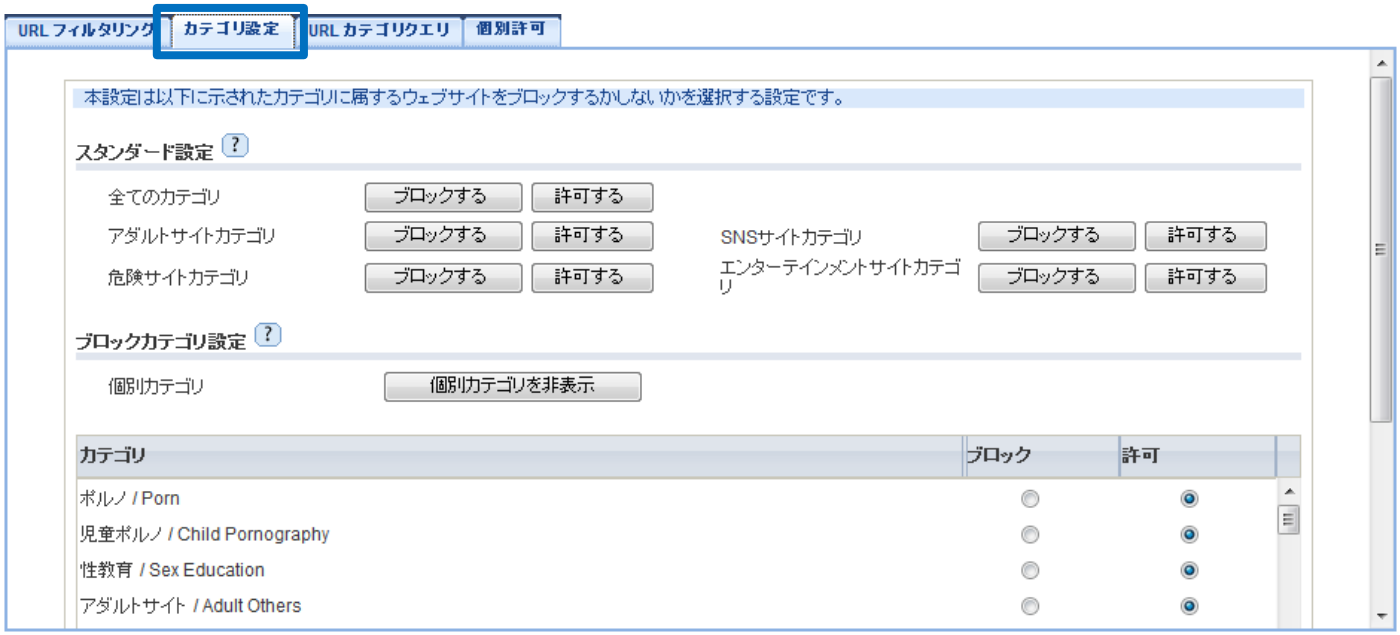
URL フィルタリング機能を運用ポリシーにしたがい、適切な内容に設定してください。

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



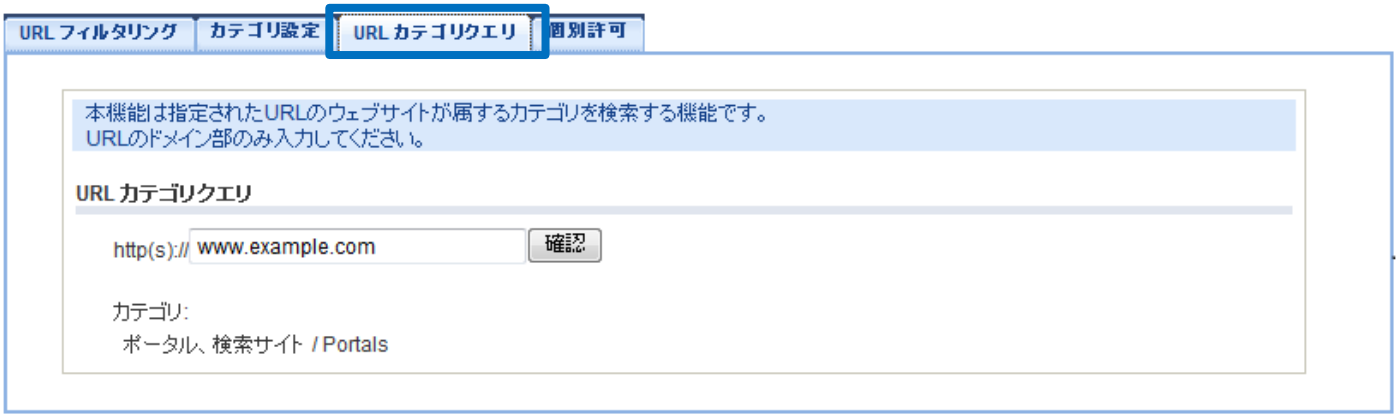
■カテゴリ設定タブ



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 1.1.1 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。

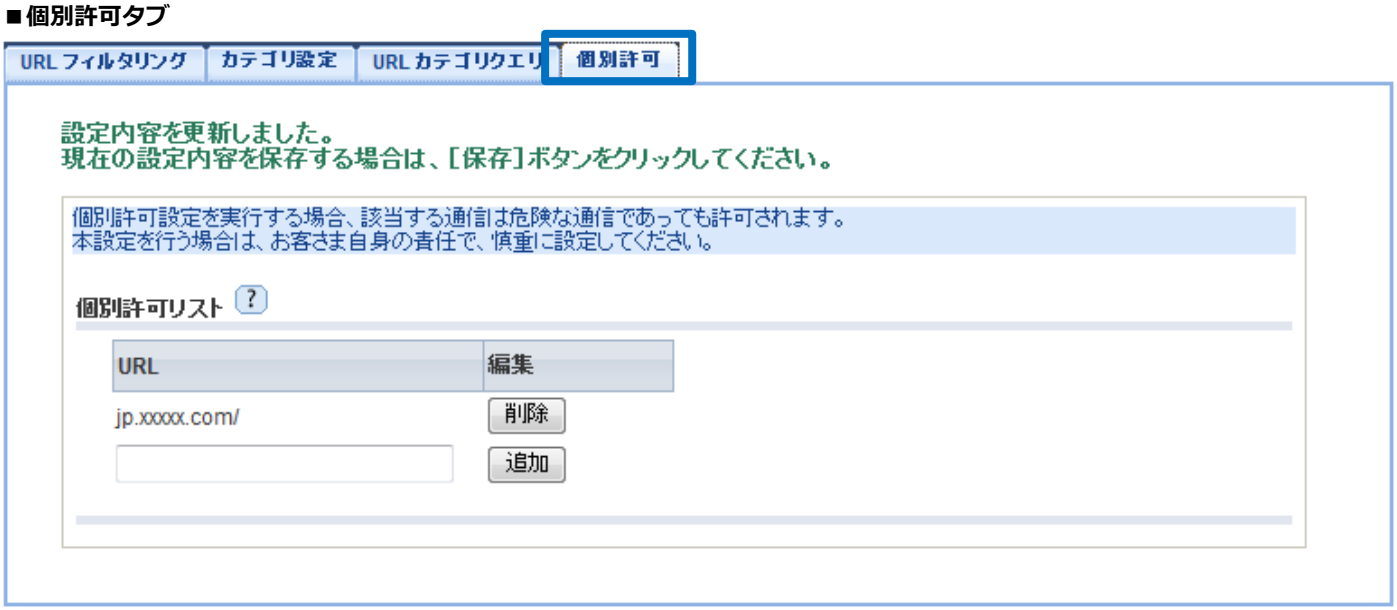
■URL カテゴリクエリタブ



※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”jp.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
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。	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。	有効

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。	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 / Porn 児童ポルノ / Child Pornography 性教育 / Sex Education アダルトサイト / Adult Others ギャンブル / Gambling 公営ギャンブル / Official Gambling Business 暴力的なサイト / Violent and Bloody 残忍なスポーツ(ハンティング等) / Brutal Sports アルコール飲料 / Alcohol Drinks たばこ / Tobacco マリファナ / Marijuana ドラッグ / Drug 中絶 / Abortion 過激論、人種差別 / Ultraism 違法行為 / Other Illegal Actions 学業不正 / School Cheating	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 ハッキング / Hacking Websites ボットネット / Botnets その他の危険サイト / Other Malicious Web 危険アプリケーション / Malicious APP	許可

SNS サイトカテゴリ	下記のカテゴリが該当します。 チャットルーム / Chat Room and Dating ニュースグループ、フォーラム、掲示板 / Newsgroup, Forums and Bulletin Boadrs ブログと個人サイト / Blog and Personal Web ソーシャルネットワーク / Social Network	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。 クラブ / Club ショッピング、オークション / Shopping and Auction クーポン / Coupons and Money-saving エンターテインメント / General Entertainment ゲーム / Game コミック、アニメ / Comics, Cartoons and Anime ダウンロードサイト / Download Sites P2P / P2P ストリーミングメディア / Streaming Media	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、1.1.1 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　：256 文字 登録可能件数　　：100 件	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。	−

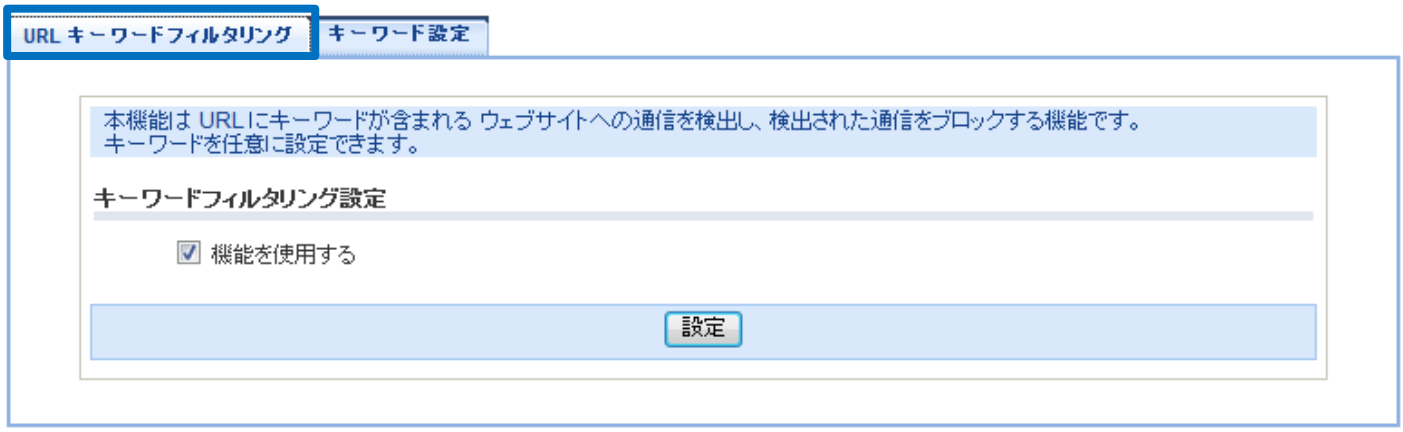
5.8.7. URL キーワードフィルタリング（KF）

必要に応じて設定してください。

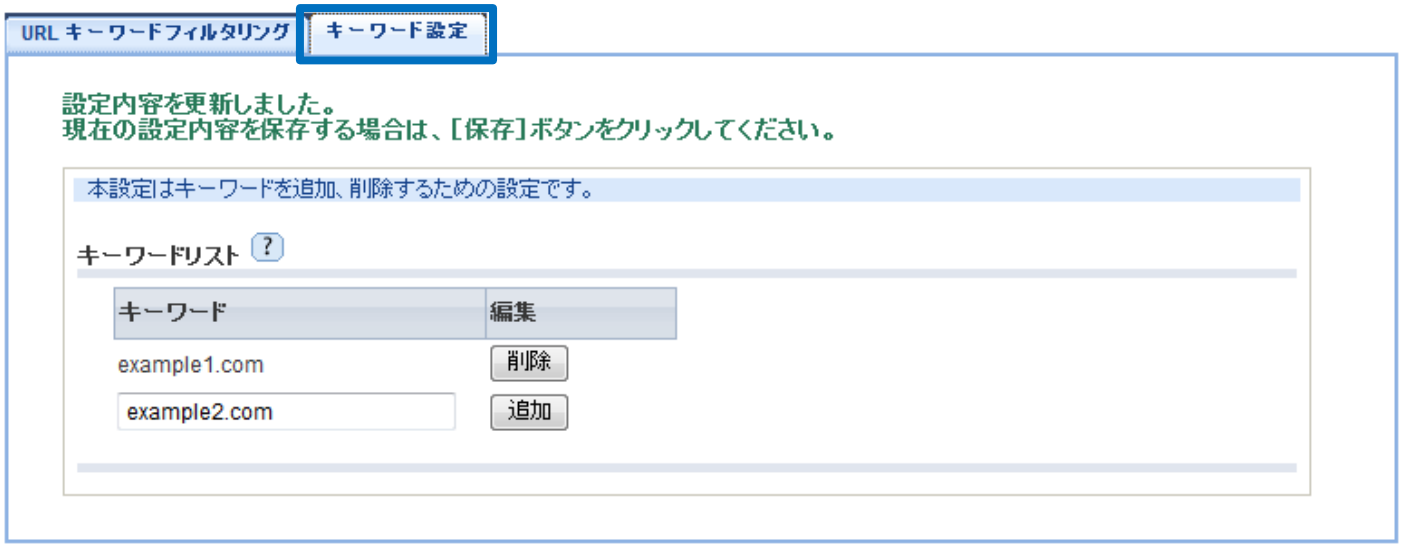
URL キーワードフィルタリング機能を運用ポリシーにしたがい、適切な内容に設定してください。

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	ブロック対象とする「キーワード」の追加、削除を設定します。

■URL キーワードフィルタリング



■キーワード設定



※画面は”example1.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 3.3.10 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 3.3.10 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　：128 文字 キーワードの登録可能数　：100 件	未設定
	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。	－

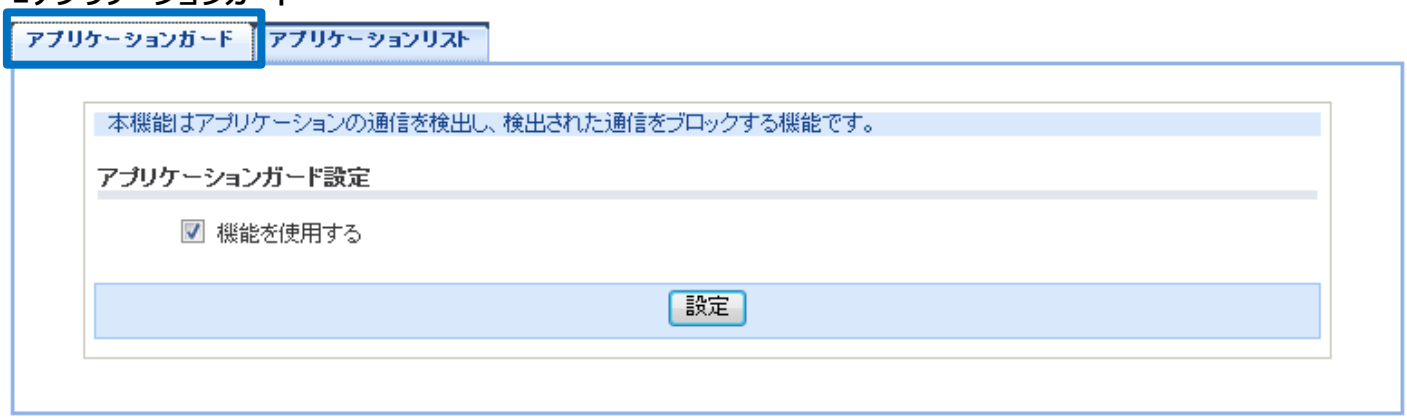
5.8.8. **アプリケーションガード（APG）**

必ず確認してください。

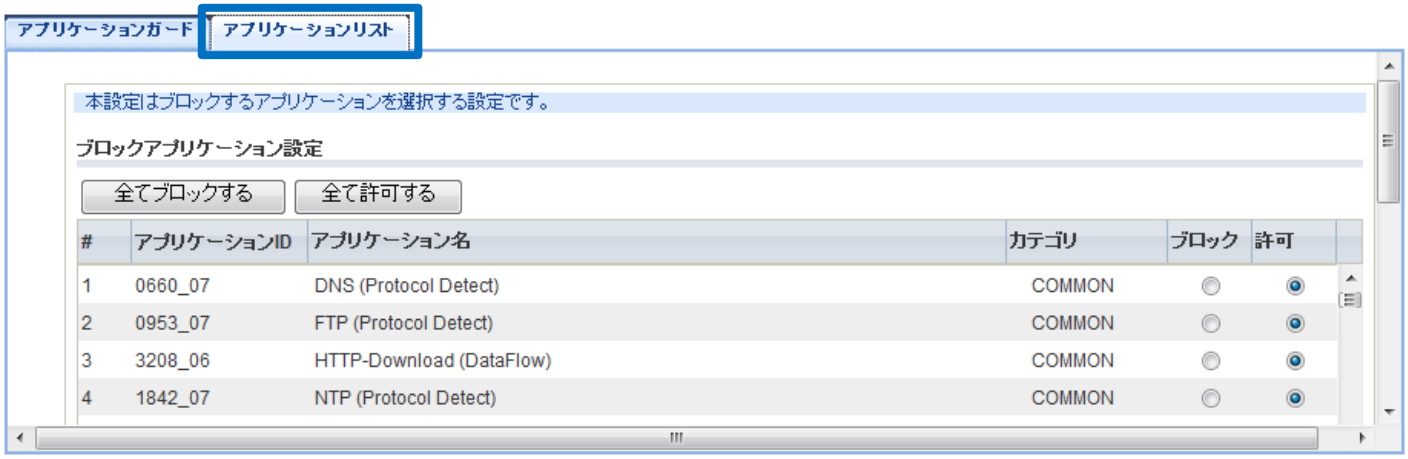
アプリケーションガード機能を運用ポリシーにしたがい、適切な内容に設定してください。

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。

■アプリケーションガード



■アプリケーションリスト



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 3.3.11 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。

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
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	サーバーで管理している 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、プロトコルは定期的に更新します。

5.8.9. **メール通知**

必ず確認してください。

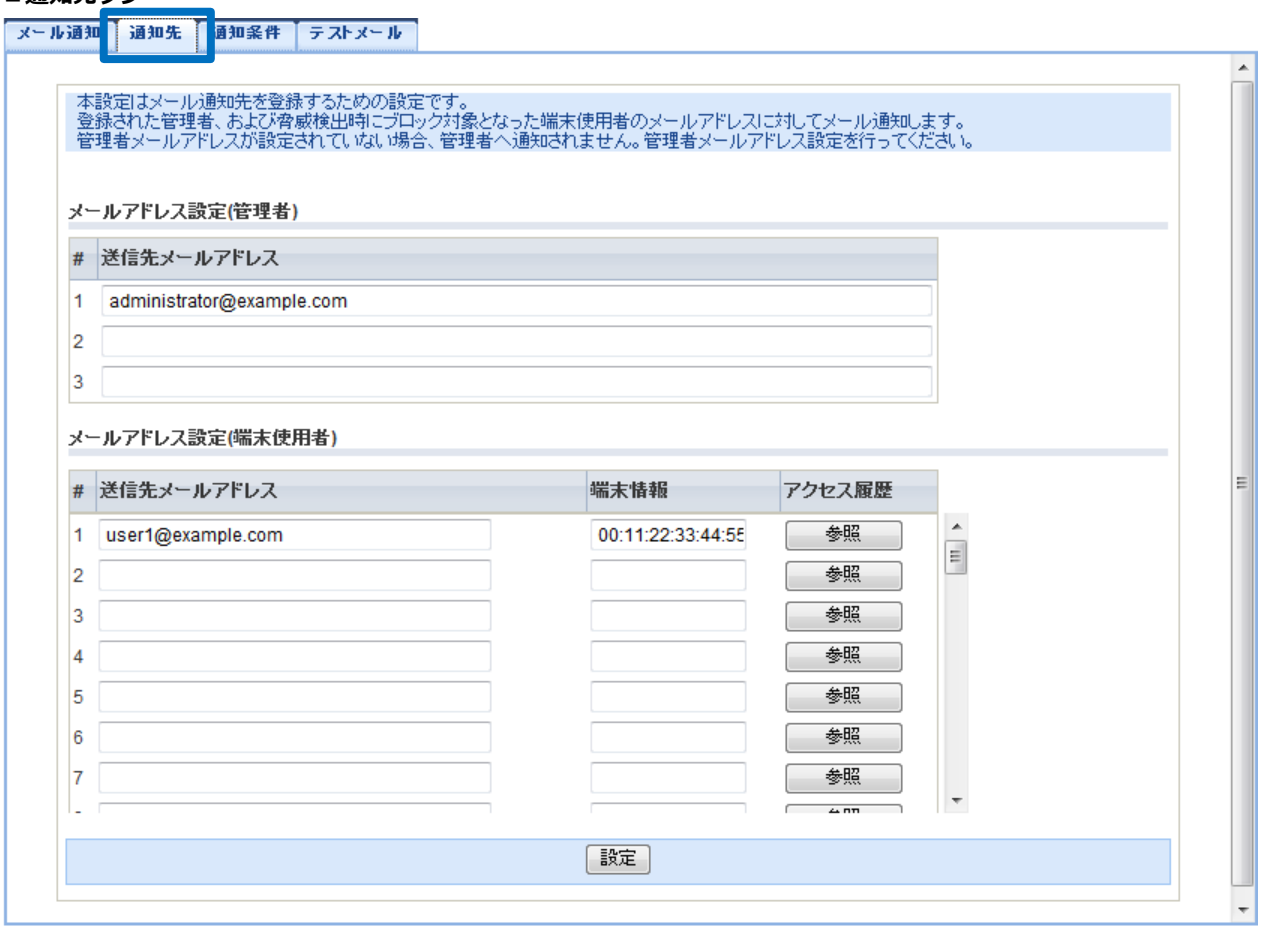
メール通知機能を運用ポリシーにしたがい、適切な内容に設定してください。

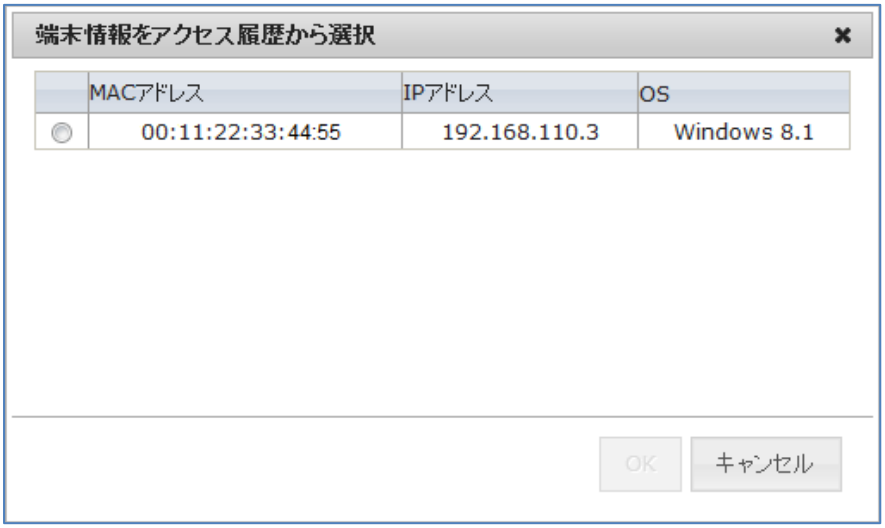
タブ	説明
メール通知	メール通知機能の使用有無、メールの言語、メール送信に使用するメールアカウントを設定します。
通知先	メール通知の宛先メールアドレスを設定します。
通知条件	メールを通知する条件を設定します。
テストメール	テストメールを送信します。

■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。

■通知先タブ



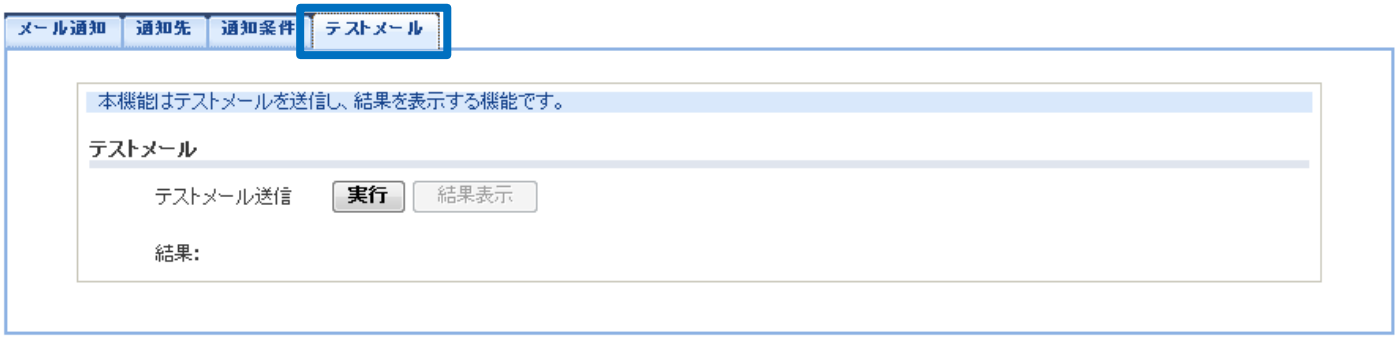


1. [TOP]-[セキュリティ]-[メール通知]画面を開きます。
2. [通知先]タブをクリックし、管理者用のメールアドレス、端末使用者用のメールアドレスを設定します。
   ※管理者、端末使用者のメール通知条件は、3.3.13 章を参照してください。
   ※端末使用者の端末情報には、MAC アドレスを FF:FF:FF:FF:FF:FF の形式で入力してください。
   その際、「参照」ボタンを押下すると、本製品に接続されている端末のリストから選択することができます。
3. 「設定」ボタンを押下します。
4. 「保存」ボタンを押下して、設定値を保存します。

■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、3.3.13 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 サーバー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
メールアドレス設定(端末使用者)		端末使用者の宛先情報を設定します。 登録済みのノードからのパケット、または、ノード宛てのパケットで脅威を検出した場合、当該ノードに登録しているメールアドレス宛てに通知します。	
	#	項目番号です。	
	送信先メールアドレス	端末使用者のメールアドレスを設定します。	未設定
	端末情報	端末使用者が使用する端末の MAC アドレスを設定します。 FF:FF:FF:FF:FF:FF 形式で入力してください。	未設定
	アクセス履歴	「参照」ボタンを押すと、リストから選択して簡単に端末情報を設定できます。 リストに表示される端末は、本製品が通信を検出した端末の情報です。	–

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。	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
	ライセンス切れが近づいたときに通知する	ライセンス期限切れ間近（30 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
	ライセンスが切れたときに通知する	ライセンス期限切れ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

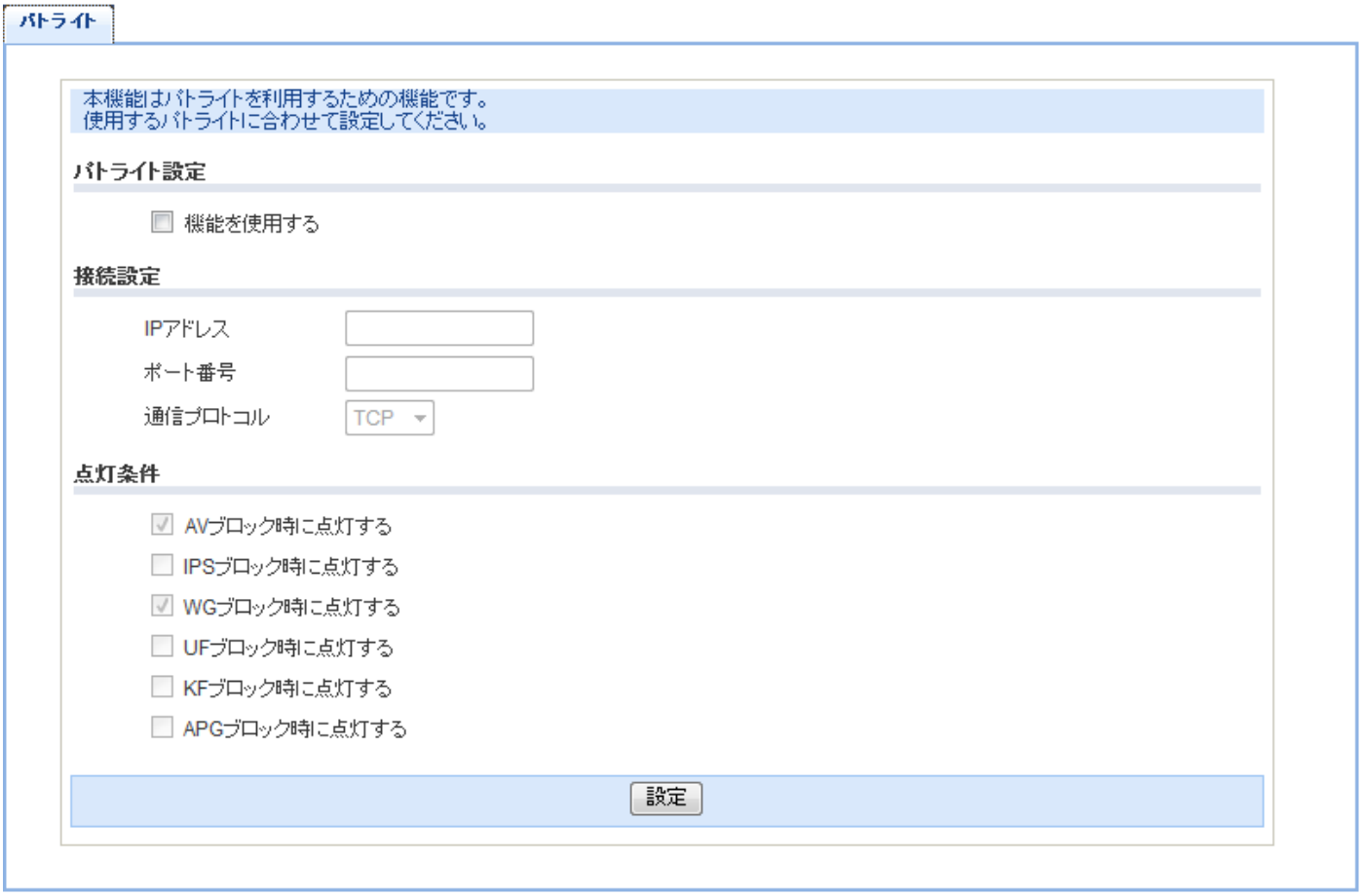
設定項目		説明	初期値
テストメール		管理者のメールアドレス宛てにメールを送信します。 テストメールを実行するには、事前にアカウント設定、メールアドレス設定(管理者)を行ってください。	
	実行	「実行」ボタンを押すと、管理者のメールアドレス宛てにメールを送信します。	−
	結果表示	メール送信実行後に「結果表示」ボタンを押下すると、メール送信の結果を表示します。 ● 送信中：メール送信中です。しばらくしてから、再度「結果表示」ボタンを押下してください。 ● 送信完了：メールは正常に送信されました。管理者宛てにメールが届いたか確認してください。 ● 送信失敗：メールは正常に送信されませんでした。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。	−

5.8.10. **パトライト連携**

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 3.3.14 章を参照してください。



1. [TOP]-[セキュリティ]-[オプション]画面を開きます。
2. [パトライト]タブの「機能を使用する」をチェックします。
3. [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。
4. [点灯条件]に点灯させる脅威検出条件をチェックします。
5. 「設定」ボタンを押下します。
6. 「保存」ボタンを押下して、本設定を保存します。

設定項目	説明	初期値
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」を選択できます。	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

5.9. **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。

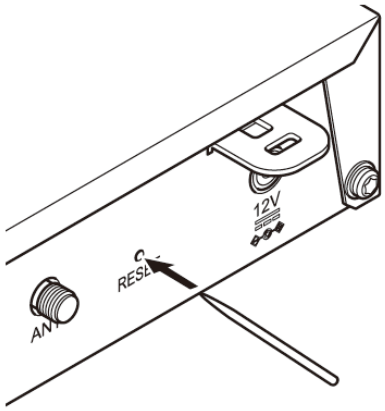
表示	機能	スイッチ位置	備考
RESET	本製品の初期化	製品背面右側	プッシュ型
OPT1	セキュリティ・スキャン機能用スイッチ ・アクティベーション ・脅威検出状態解除	製品前面右側	プッシュ型
OPT2	ファームウェアアップデート用	製品背面左側	プッシュ型
WPS	WPS スイッチ	製品前面左側	プッシュ型

5.9.1. **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。

5.9.2. **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。

5.9.3. **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。
この時、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）を数秒押下することで、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ので、ご安心ください。

[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。
  ※ファームウェアバージョン 3.0.1 をご利用の場合、本製品を再起動しても解除されません。

[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。

5.9.4. **ファームウェアアップデート**

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。

1. 新しいファームウェアの有無を定期的に確認します。
2. 新しいファームウェアがあると INFO ランプが橙点灯します。
3. 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）で押し続け、2 秒以上押下します（INFO ランプが橙点滅します）
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]
メンテナンスバージョンアップ機能を有効にするには、5.6.5 章を参照してください。
初期状態は有効です。

5.9.5. **WPS**

本製品の WPS ボタンを使用して、WPS-PBC に対応した無線 LAN 端末と WiFi 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）

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 ボタンを長押しし、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、本製品底面の装置ラベル、または設定 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-F i 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
IPsec SA 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
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

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。

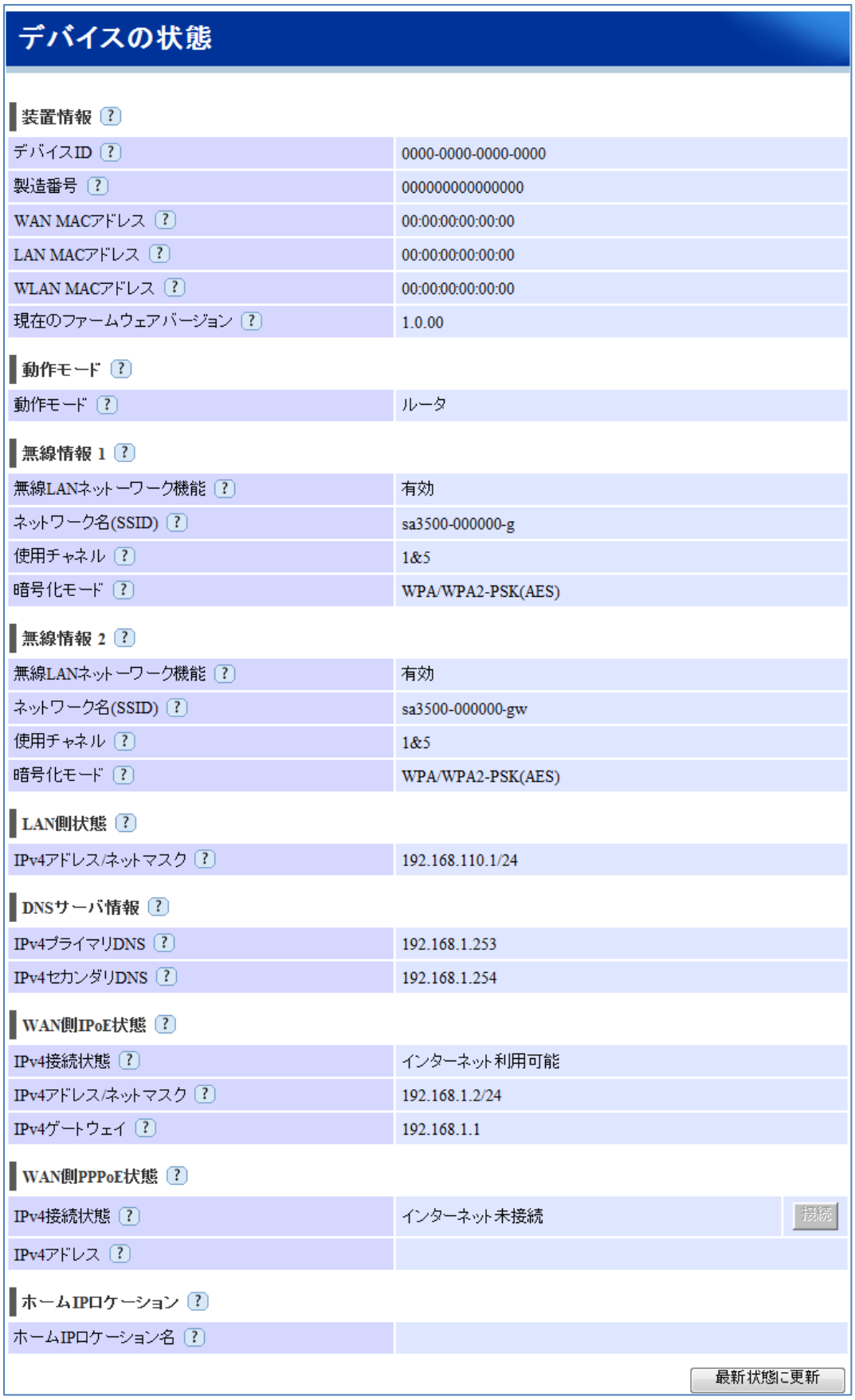
装置情報	説明
装置情報	本製品の装置情報を表示します。
デバイス ID	本製品のデバイス ID を表示します。
製造番号	本製品の製造番号を表示します。
WAN MAC アドレス	本製品の WAN インタフェースの MAC アドレス情報を表示します。
LAN MAC アドレス	本製品の LAN インタフェースの MAC アドレス情報を表示します。
WLAN MAC アドレス	本製品の無線 LAN インタフェースの MAC アドレス情報を表示します。
現在のファームウェアバージョン	システムファームウェアのバージョン情報を表示します。
動作モード	ブリッジ … ブリッジモードで動作中 ルータ　… ルータモードで動作中
WAN 側 IPoE 状態	
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
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
IPv4 プライマリ DNS	プライマリ DNS サーバーアドレスを表示
IPv4 セカンダリ DNS	セカンダリ DNS サーバーアドレスを表示
「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。



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 サーバーアドレスを表示します。
IPv4 セカンダリ DNS	セカンダリ DNS サーバー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/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。
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。
「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**

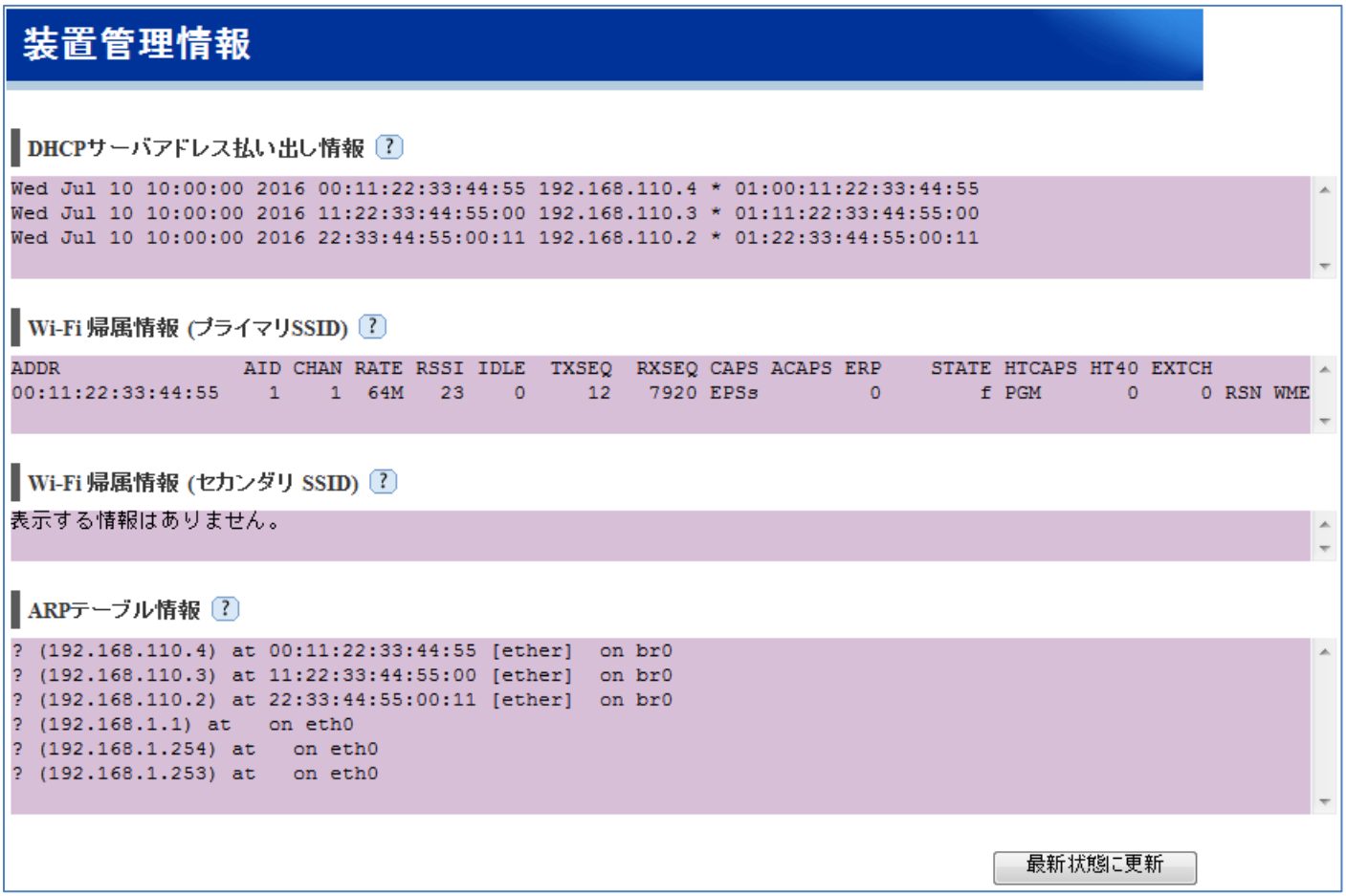
本製品のセキュリティ・スキャン機能のライセンス状況および各機能のシグネチャのバージョン情報を設定 Web で確認できます。

1. [TOP]-[セキュリティ]-[ステータス]画面を開きます。

6.1.4. 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-F i 帰属情報、ARP テーブル情報を設定 Web で確認できます。

1.[TOP]-[メンテナンス]-[情報]-[装置管理情報]画面を開きます。



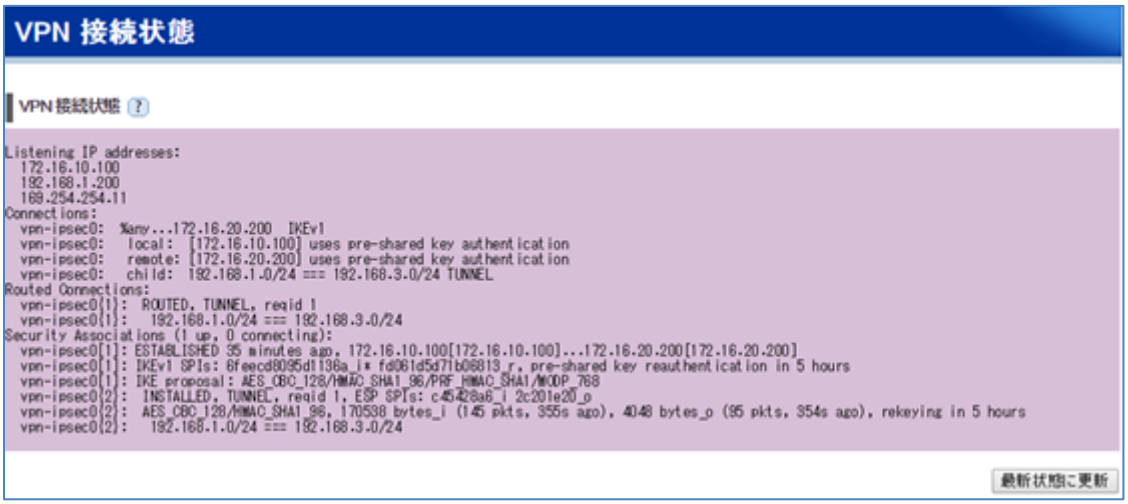
項目		説明
DHCP サーバアドレス払い出し情報		本製品が DHCP サーバーとして、アドレスを払い出した情報を確認できます。 1 件の IP アドレス払い出し情報が一行ごとに表示されます。 以下、表示内容の左側から項目の内容を説明します。
	リース満了時刻	本製品が払い出した IP アドレスのリース期間が満了する時刻です。
	クライアントの MAC アドレス	IP アドレスが払い出されたクライアントの MAC アドレスです。
	払い出した IP アドレス	クライアントに払い出した IP アドレスです。
	クライアントのホスト名	クライアントのホスト名です。
	クライアント ID	クライア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。
	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ーフェースです。

6.1.5. **IPsec SA 情報**

IPsec トンネルの状態を設定 Web で確認できます。

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。

6.1.6. **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。

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]

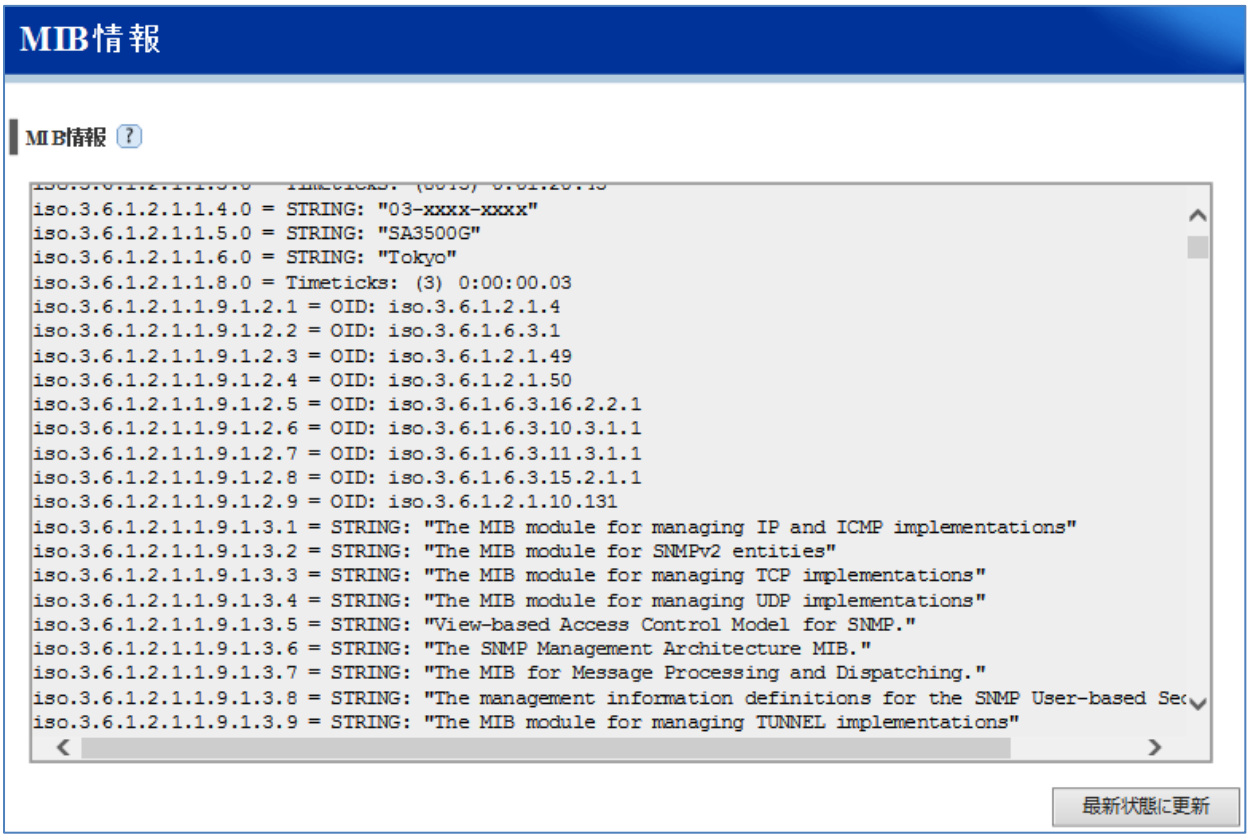
項目	説明
ikeInitRekey	IKE SA リキー始動カウンタ
ikeRspRekey	IKE SA リキー応答カウンタ
ikeChildSaRekey	IPsec SA リキー成功カウンタ
ikeInInvalid	無効メッセージ受信カウンタ
ikeInInvalidSpi	無効 ID、SPI 受信カウンタ
ikeInInitReq	IKE SA 初期化要求受信カウンタ
ikeInInitRsp	IKE SA 初期化応答受信カウンタ
ikeOutInitReq	IKE SA 初期化要求送信カウンタ
ikeOutInitRsp	IKE SA 初期化応答送信カウンタ
ikeInAuthReq	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

6.1.7. **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。

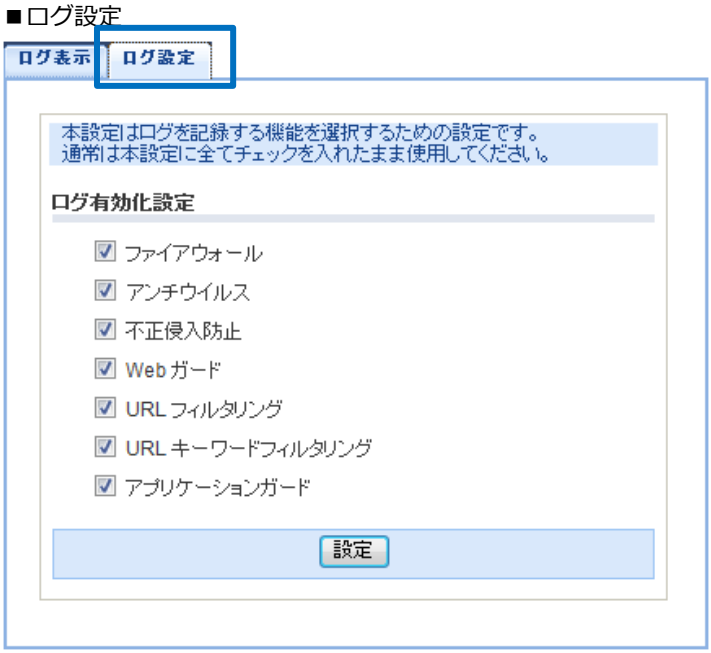
6.1.8. セキュリティ・スキャン機能のログメッセージ

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。

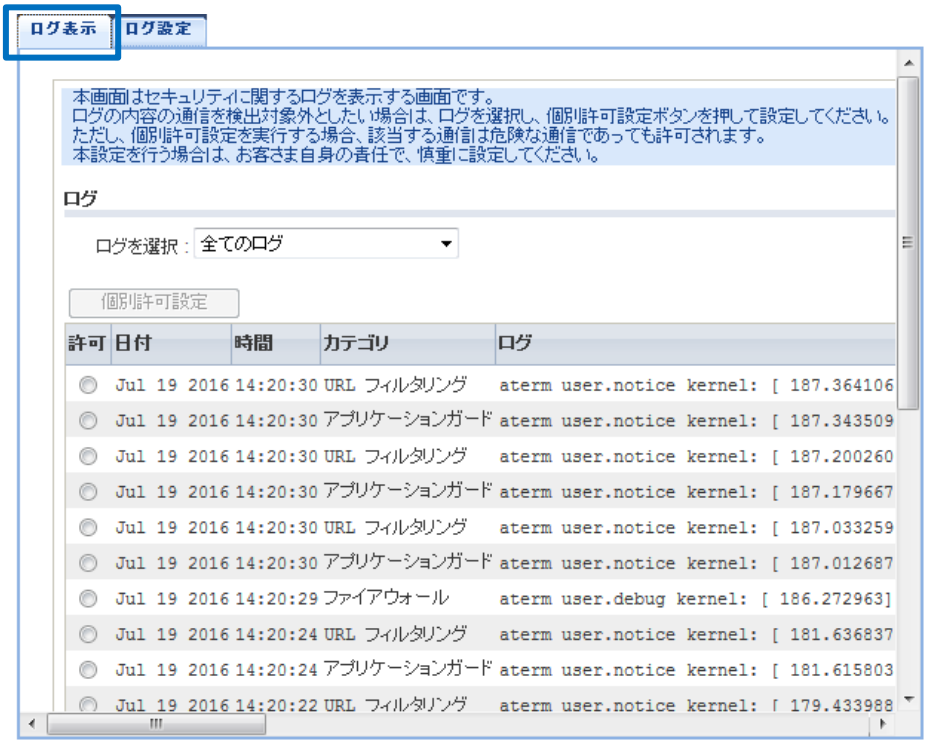
本製品のセキュリティ・スキャン機能の動作状況を設定 Web で確認できます。

タブ	説明
ログ表示	セキュリティ・スキャン機能のログメッセージを表示します。 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ログメッセージの表示有無を設定します。 ログメッセージが必要ない機能は、チェックを外してください。

■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、ログメッセージを確認し、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ログメッセージを表示しません。
また、その後有効にしても、その間のログメッセージを表示しません。

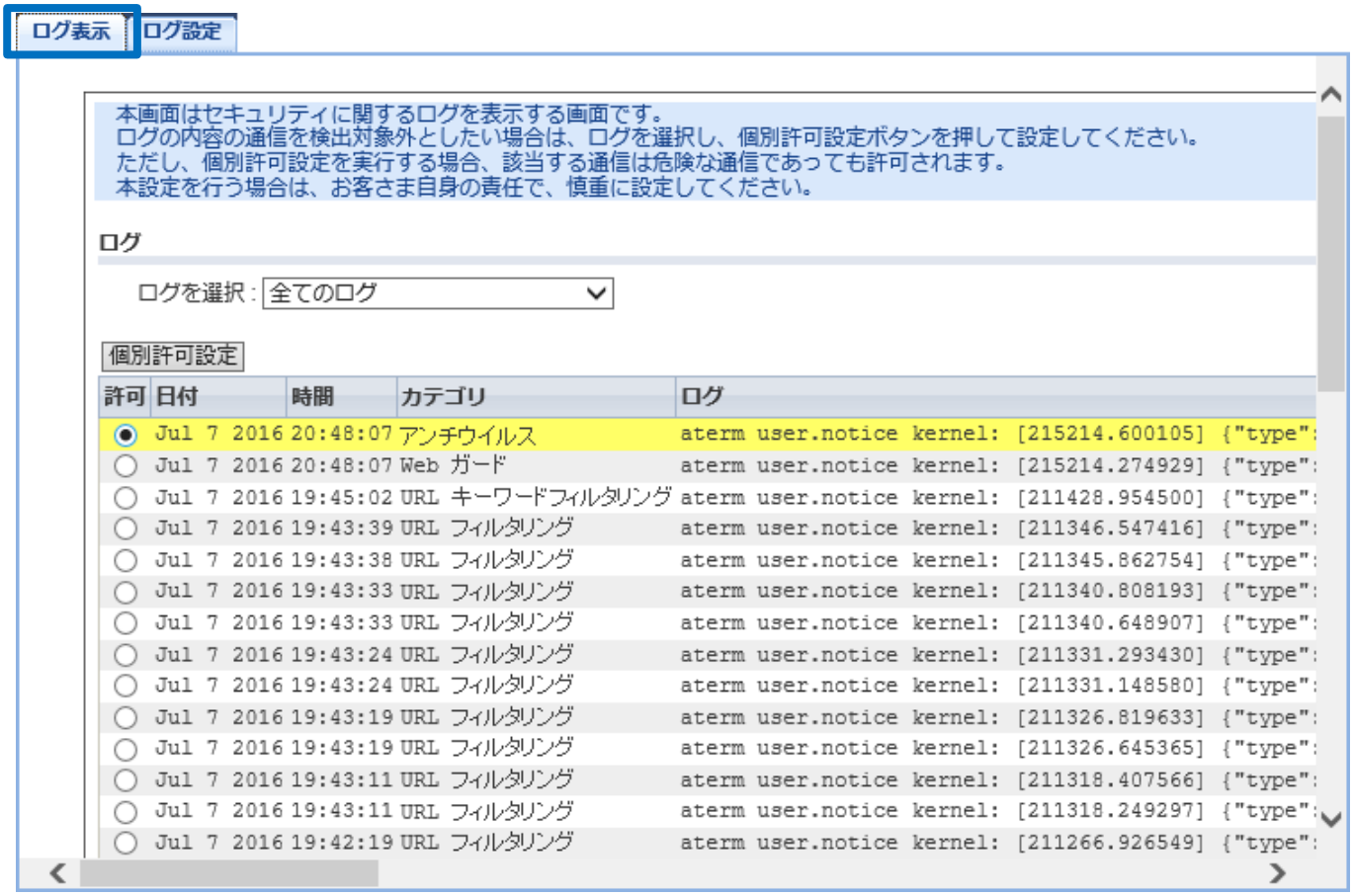
[ログメッセージのパソコンなどへの保存]

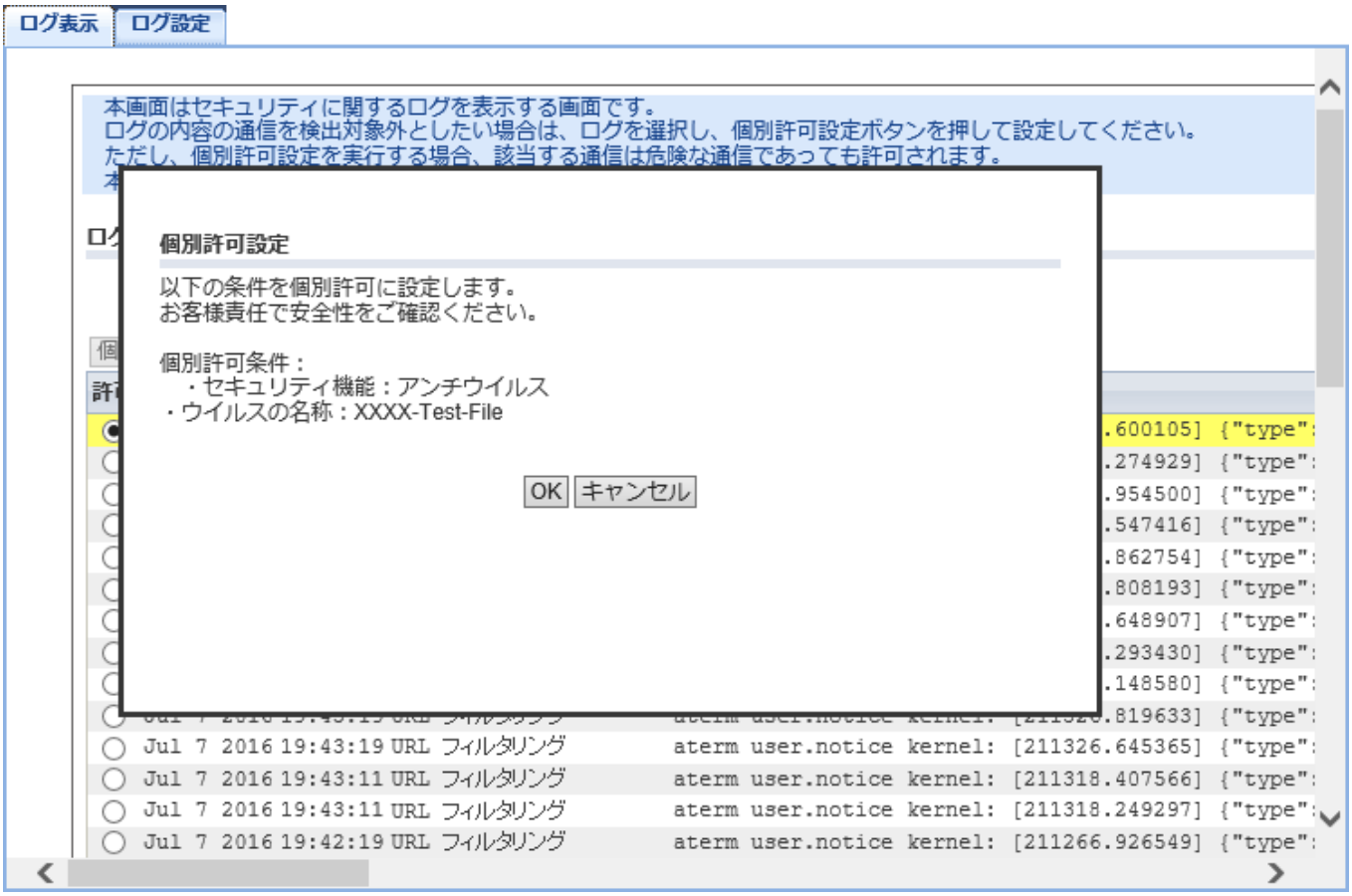
「ファイルに保存」ボタンを押下すると、パソコンなどにログメッセージを保存できます。

[個別許可]

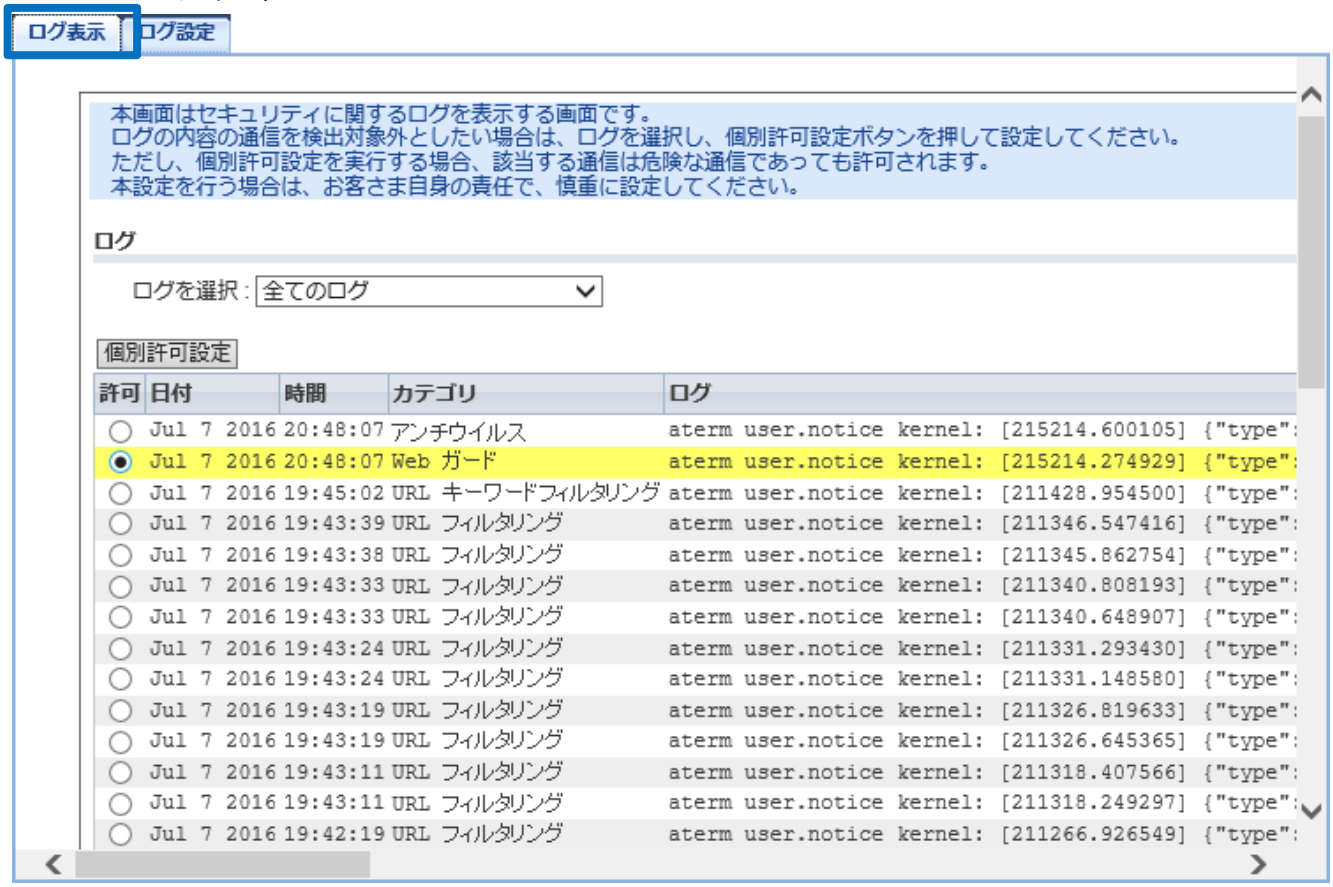
ログの内容の通信を検出対象外にしたい場合は、ログを選択し、個別許可ボタンを押して設定してください。
ただし、個別許可設定を実行する場合、該当する通信は危険な通信であっても許可されます。
本設定を行う場合は、お客さま自身の責任で、慎重に設定してください。

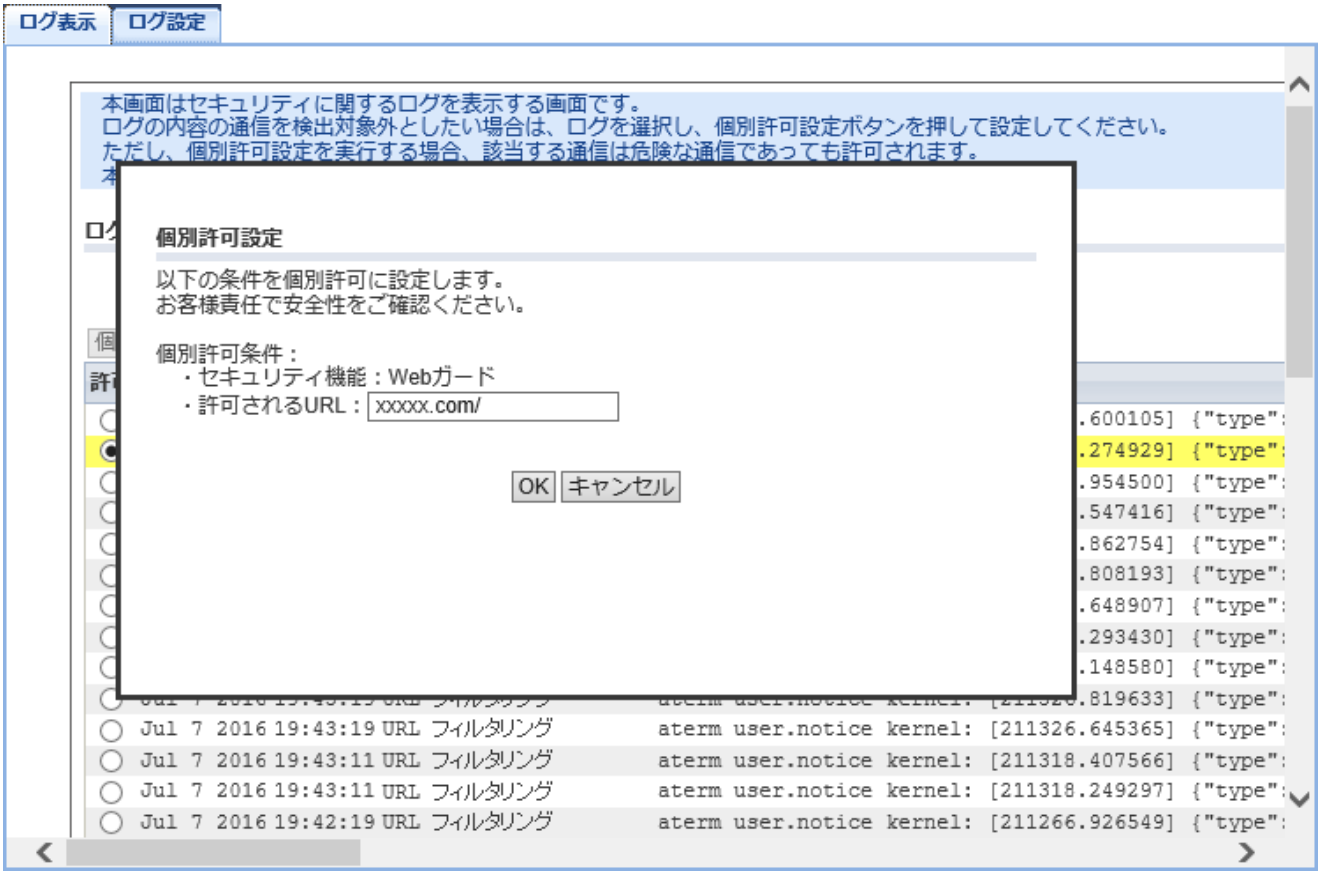
- アンチウイルス（AV）


ログ表示
ログ設定
本画面はセキュリティに関するログを表示する画面です。
ログの内容の通信を検出対象外としたい場合は、ログを選択し、個別許可設定ボタンを押して設定してください。
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、お客さま自身の責任で、慎重に設定してください。
ログ
ログを選択：全てのログ
個別許可設定
許可 日付 時間 カテゴリ ログ
Jul 7 2016 20:48:07 アンチウイルス aterm user.notice kernel: [215214.600105] {"type":
Jul 7 2016 20:48:07 Web ガード aterm user.notice kernel: [215214.274929] {"type":
Jul 7 2016 19:45:02 URL キーワードフィルタリング aterm user.notice kernel: [211428.954500] {"type":
Jul 7 2016 19:43:39 URL フィルタリング aterm user.notice kernel: [211346.547416] {"type":
Jul 7 2016 19:43:38 URL フィルタリング aterm user.notice kernel: [211345.862754] {"type":
Jul 7 2016 19:43:33 URL フィルタリング aterm user.notice kernel: [211340.808193] {"type":
Jul 7 2016 19:43:33 URL フィルタリング aterm user.notice kernel: [211340.648907] {"type":
Jul 7 2016 19:43:24 URL フィルタリング aterm user.notice kernel: [211331.293430] {"type":
Jul 7 2016 19:43:24 URL フィルタリング aterm user.notice kernel: [211331.148580] {"type":
Jul 7 2016 19:43:19 URL フィルタリング aterm user.notice kernel: [211326.819633] {"type":
Jul 7 2016 19:43:19 URL フィルタリング aterm user.notice kernel: [211326.645365] {"type":
Jul 7 2016 19:43:11 URL フィルタリング aterm user.notice kernel: [211318.407566] {"type":
Jul 7 2016 19:43:11 URL フィルタリング aterm user.notice kernel: [211318.249297] {"type":
Jul 7 2016 19:42:19 URL フィルタリング aterm user.notice kernel: [211266.926549] {"type":

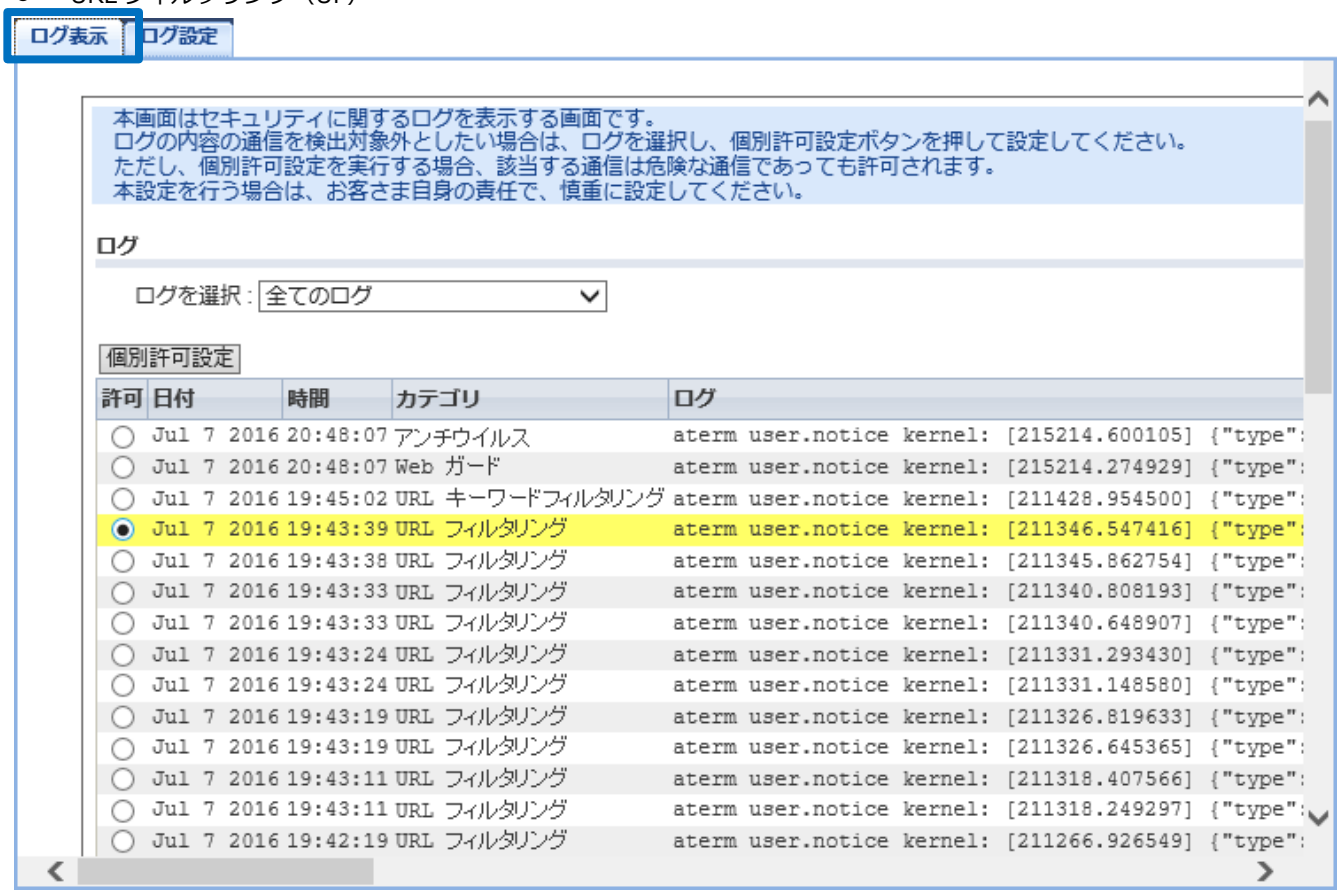

ログ表示
ログ設定
本画面はセキュリティに関するログを表示する画面です。
ログの内容の通信を検出対象外としたい場合は、ログを選択し、個別許可設定ボタンを押して設定してください。
ただし、個別許可設定を実行する場合、該当する通信は危険な通信であっても許可されます。
個別許可設定
以下の条件を個別許可に設定します。
お客様責任で安全性をご確認ください。
個別許可条件：
・セキュリティ機能：アンチウイルス
・ウイルスの名称：XXXX-Test-File
OK
キャンセル
Jul 7 2016 19:43:19 URL フィルタリング aterm user.notice kernel: [211326.645365] {"type":
Jul 7 2016 19:43:11 URL フィルタリング aterm user.notice kernel: [211318.407566] {"type":
Jul 7 2016 19:43:11 URL フィルタリング aterm user.notice kernel: [211318.249297] {"type":
Jul 7 2016 19:42:19 URL フィルタリング aterm user.notice kernel: [211266.926549] {"type":

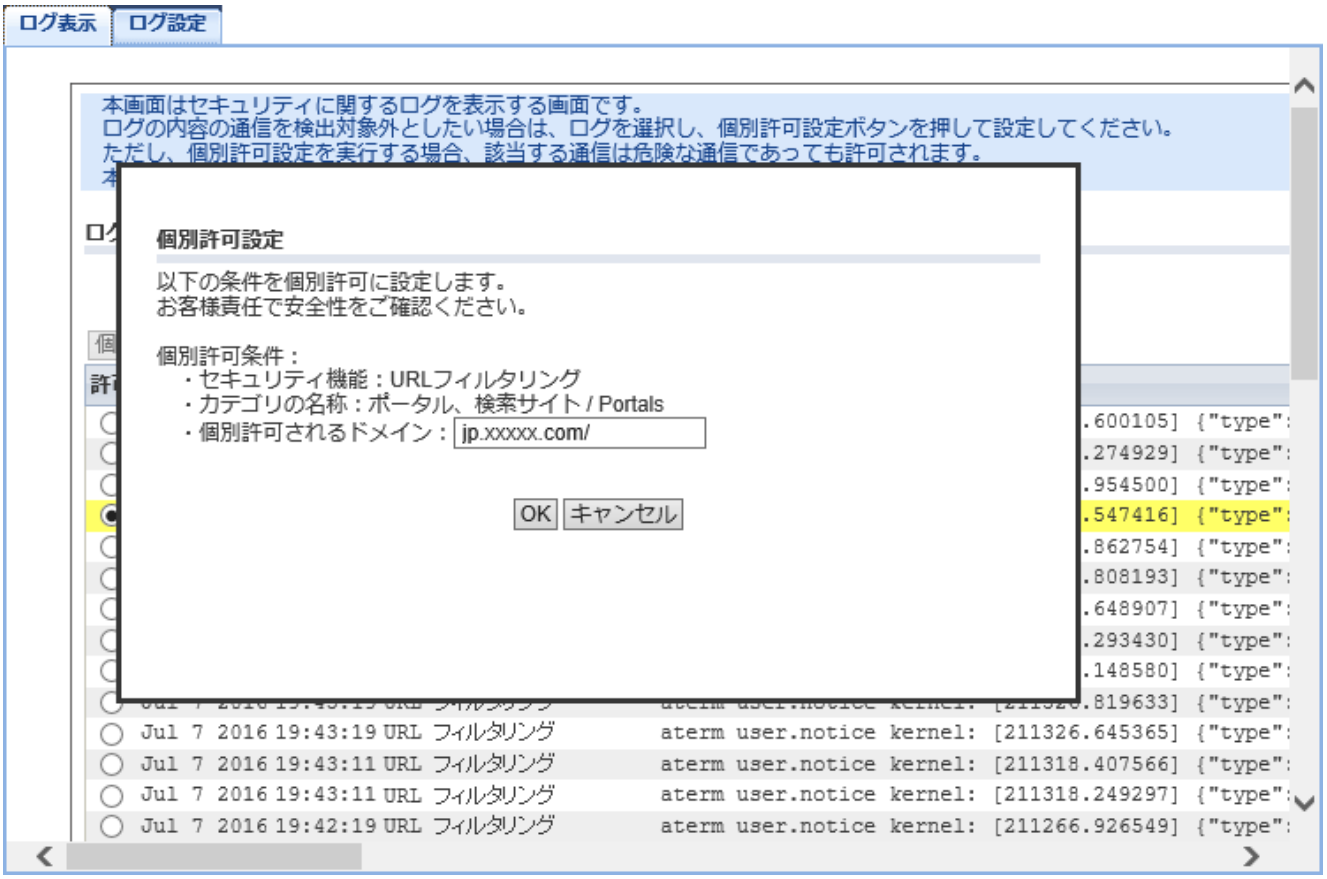
- Web ガード（WG）


ログ表示
ログ設定
本画面はセキュリティに関するログを表示する画面です。
ログの内容の通信を検出対象外としたい場合は、ログを選択し、個別許可設定ボタンを押して設定してください。
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、お客さま自身の責任で、慎重に設定してください。
ログ
ログを選択：全てのログ
個別許可設定
許可 日付 時間 カテゴリ ログ
Jul 7 2016 20:48:07 アンチウイルス aterm user.notice kernel: [215214.600105] {"type":
Jul 7 2016 20:48:07 Web ガード aterm user.notice kernel: [215214.274929] {"type":
Jul 7 2016 19:45:02 URL キーワードフィルタリング aterm user.notice kernel: [211428.954500] {"type":
Jul 7 2016 19:43:39 URL フィルタリング aterm user.notice kernel: [211346.547416] {"type":
Jul 7 2016 19:43:38 URL フィルタリング aterm user.notice kernel: [211345.862754] {"type":
Jul 7 2016 19:43:33 URL フィルタリング aterm user.notice kernel: [211340.808193] {"type":
Jul 7 2016 19:43:33 URL フィルタリング aterm user.notice kernel: [211340.648907] {"type":
Jul 7 2016 19:43:24 URL フィルタリング aterm user.notice kernel: [211331.293430] {"type":
Jul 7 2016 19:43:24 URL フィルタリング aterm user.notice kernel: [211331.148580] {"type":
Jul 7 2016 19:43:19 URL フィルタリング aterm user.notice kernel: [211326.819633] {"type":
Jul 7 2016 19:43:19 URL フィルタリング aterm user.notice kernel: [211326.645365] {"type":
Jul 7 2016 19:43:11 URL フィルタリング aterm user.notice kernel: [211318.407566] {"type":
Jul 7 2016 19:43:11 URL フィルタリング aterm user.notice kernel: [211318.249297] {"type":
Jul 7 2016 19:42:19 URL フィルタリング aterm user.notice kernel: [211266.926549] {"type":


ログ表示
ログ設定
本画面はセキュリティに関するログを表示する画面です。
ログの内容の通信を検出対象外としたい場合は、ログを選択し、個別許可設定ボタンを押して設定してください。
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。
個別許可設定
以下の条件を個別許可に設定します。
お客様責任で安全性をご確認ください。
個別許可条件：
・セキュリティ機能：Webガード
・許可されるURL：xxxxx.com/
OK
キャンセル

- URL フィルタリング（UF）

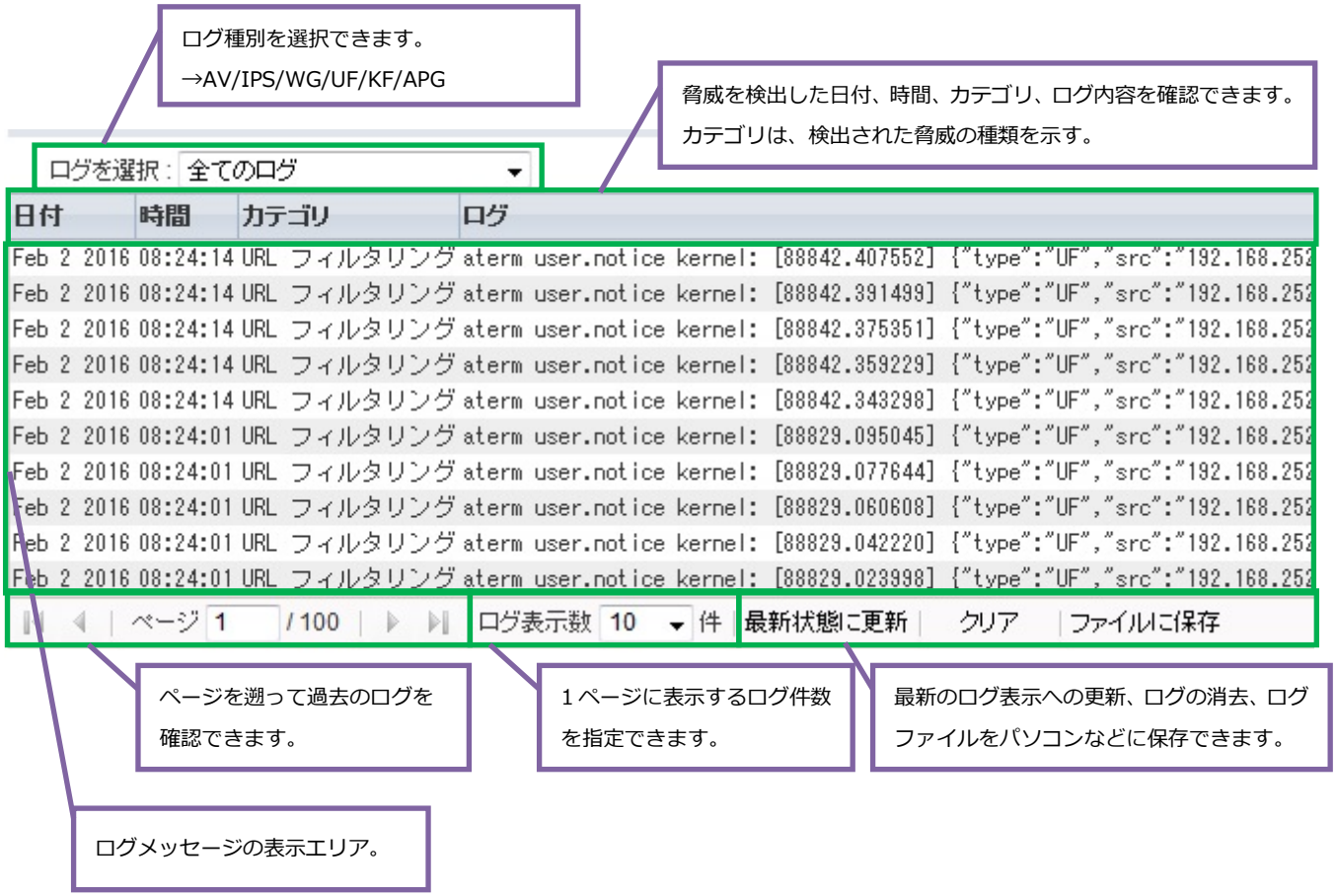




1. セキュリティログから個別許可する項目を選択し、「個別許可設定」ボタンを押下します。
2. Web ガードおよび URL フィルタリングの場合は個別許可設定ダイアログ上の URL を編集できます。
3. 「OK」ボタンを押下します。

[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。



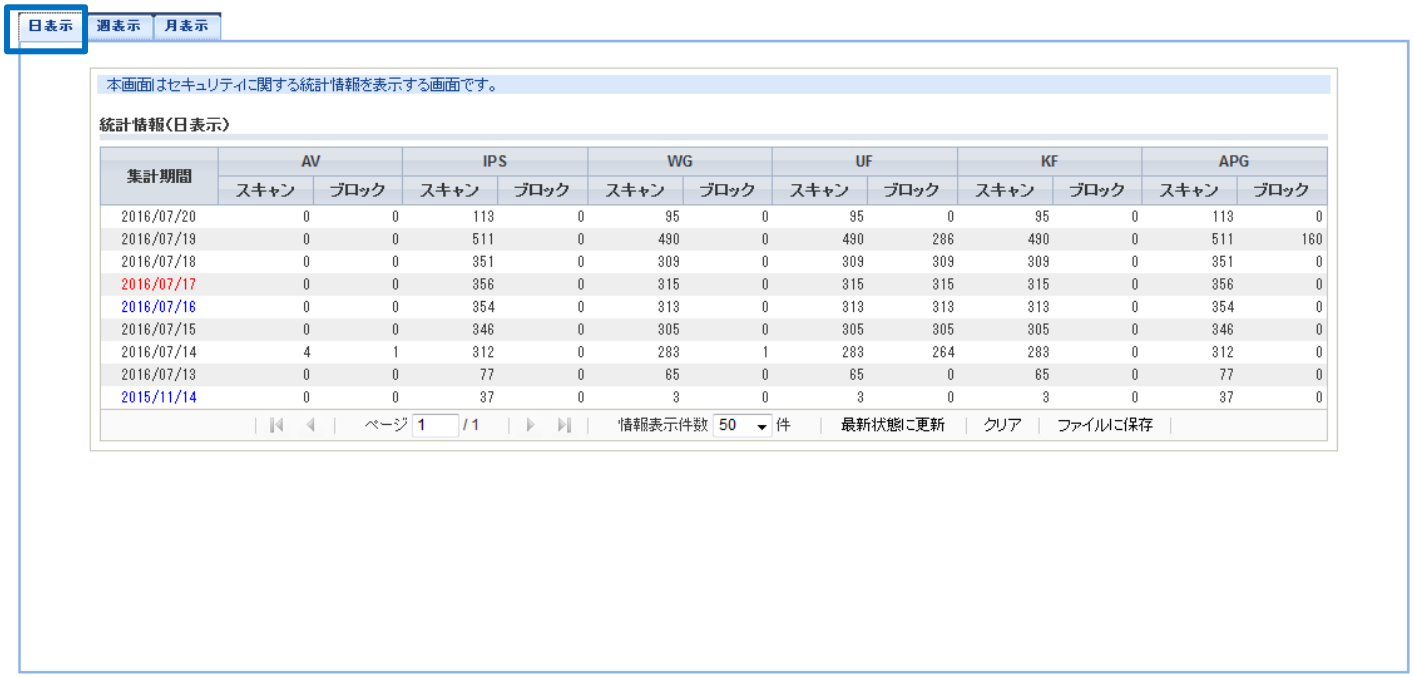
6.1.9. セキュリティ・スキャン機能の統計情報

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。

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。

■日表示



■週表示

■月表示

1. [TOP]-[セキュリティ]-[統計情報]画面を開きます。
2. 各項目の説明は次ページを参照してください。

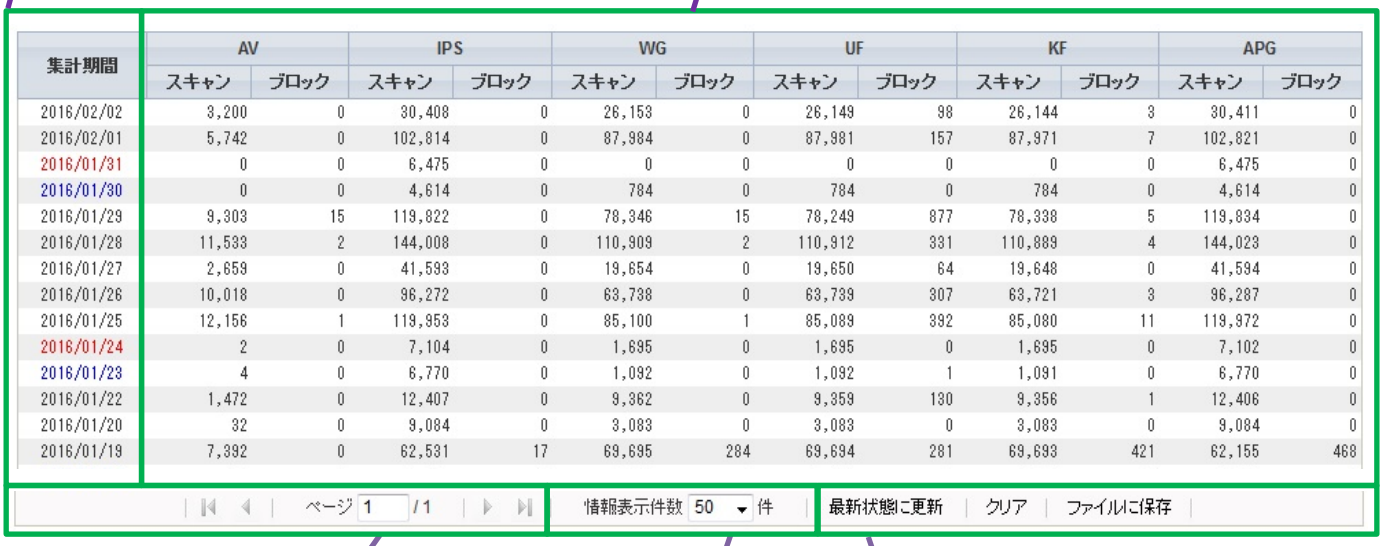
[統計情報のパソコンなどへの保存]

「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。

[統計情報画面の説明]

集計された期間を示します。
日表示の場合は、文字色で土日を示します。

機能ごとに、スキャンした通信の数、脅威を検出してブロックした通信の数を示します。
※スキャンされ、かつ、ブロックされない通信は、脅威が検出されなかった通信です。



集計期間	AV		IPS		WG		UF		KF		APG	
	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
2016/02/02	3,200	0	30,408	0	26,153	0	26,149	98	26,144	3	30,411	0
2016/02/01	5,742	0	102,814	0	87,984	0	87,981	157	87,971	7	102,821	0
2016/01/31	0	0	6,475	0	0	0	0	0	0	0	6,475	0
2016/01/30	0	0	4,614	0	784	0	784	0	784	0	4,614	0
2016/01/29	9,303	15	119,822	0	78,346	15	78,249	877	78,338	5	119,834	0
2016/01/28	11,533	2	144,008	0	110,909	2	110,912	331	110,889	4	144,023	0
2016/01/27	2,659	0	41,593	0	19,654	0	19,650	64	19,648	0	41,594	0
2016/01/26	10,018	0	96,272	0	63,738	0	63,739	307	63,721	3	96,287	0
2016/01/25	12,156	1	119,953	0	85,100	1	85,089	392	85,080	11	119,972	0
2016/01/24	2	0	7,104	0	1,695	0	1,695	0	1,695	0	7,102	0
2016/01/23	4	0	6,770	0	1,092	0	1,092	1	1,091	0	6,770	0
2016/01/22	1,472	0	12,407	0	9,362	0	9,359	130	9,356	1	12,406	0
2016/01/20	32	0	9,084	0	3,083	0	3,083	0	3,083	0	9,084	0
2016/01/19	7,392	0	62,531	17	69,695	284	69,694	281	69,693	421	62,155	468

ページを遡って過去の統計情報を確認可能。

1ページに表示する統計情報件数を指定可能。

最新状態の表示、統計情報の消去、統計情報ファイルをパソコンなどに保存可能。

[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。
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

7. こんな時には

7.1. こんな時には

7.1.1. 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 サーバー機能がありません。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。

7.1.2. 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、5.9.1 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。

7.1.3. アクティベーションできない

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
- ✓ 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）を約 4 秒間押下してください。
- ✓ 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。

7.1.4. **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。

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 メモリへの書き込みを表します。USB メモリへ連続して書き込み（消去を含む）している場合は橙点滅が続きます。この場合は、本製品の電源を OFF にしないでください。	
5	NETWORK[25]	橙点灯、または緑点灯	IP アドレスは正常です。DNS サーバー、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。 (*) ブリッジモードの時は 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

[25] 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、およびブリッジング/ルーティング機能を無効にします。

8	ALERT2	消灯	正常です。	
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	ライセンス期限切れです。 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。	

7.1.5. **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。

7.1.6. **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。

7.1.7. **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）	ルータモード時、ファイアウォール機能（SPI）は常時有効です。 Smurf 攻撃、IP スプーフィング攻撃 は以下で停止できます。 「DoS プロテクション」の「機能を使用する」のチェックを外す。（5.8.2 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。（5.8.3 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。（5.8.4 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。（5.8.5 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。（5.8.6 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。（5.8.7 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。（5.8.8 章参照）

7.1.8. **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、5.6.7 章を参照してください。

7.1.9. **本製品の電源を OFF する前に行う作業**

本製品は、本製品のセキュリティ・スキャン機能のログメッセージと統計情報を 1 日に 1 回、FlashROM に定期保存します。（当日の情報を翌日の AM0:00 に保存します）次の処理を行わずに本製品の電源を OFF すると、データが消去されることがありますのでご注意ください。

[電源を OFF する前にログメッセージと統計情報を FlashROM に保存する方法]

- 設定 Web から再起動を行う（5.6.9 章参照）

7.1.10. **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、本製品の時刻が補正され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 5.6.4 章を参照してください。

7.1.11. **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**

エラーログ表示はありません。

7.1.12. **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
   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
   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 ALERT1 ランプが緑点灯していない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。

7.1.13. **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。5.9.5 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、5.7.12 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 親機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。

7.1.14. **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。

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	ノードを IEEE802.1X で認証している

8.1. こんなネットワークで使いたい

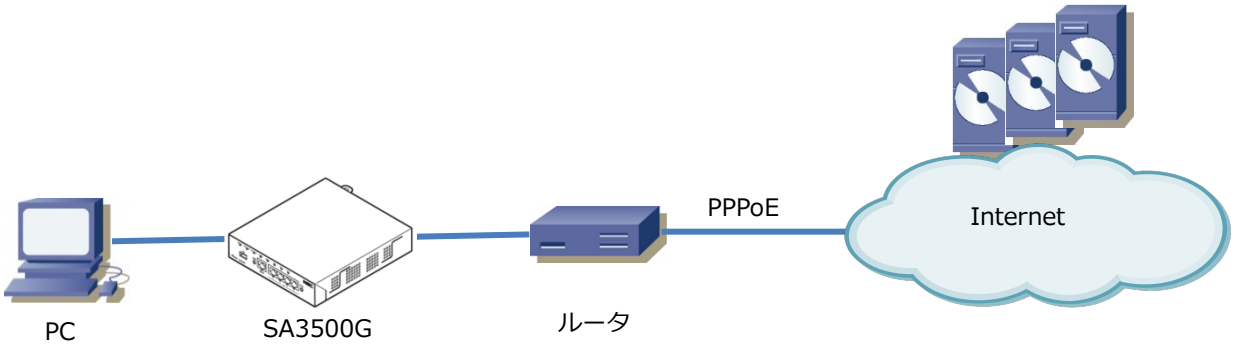
本章では、本製品の設置例を紹介しています。

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

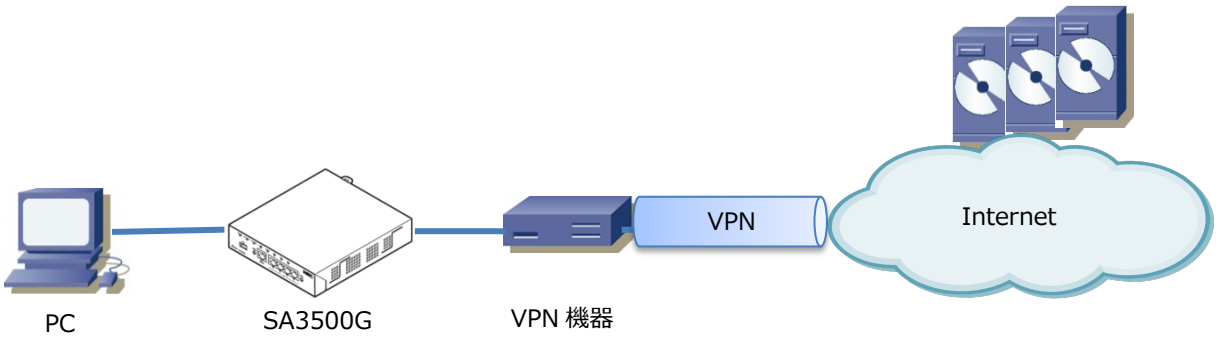
事例

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

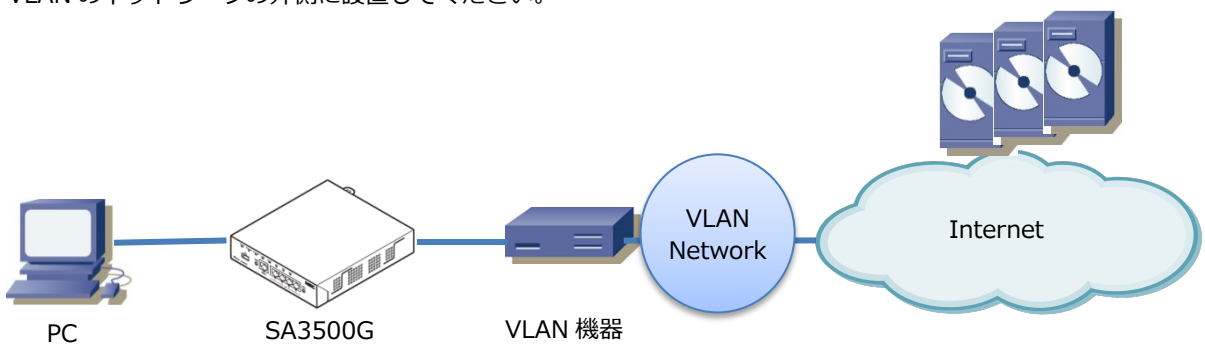
本製品のセキュリティ・スキャン機能は、VPN パケットに対応していないため、次の構成を推奨します。



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。



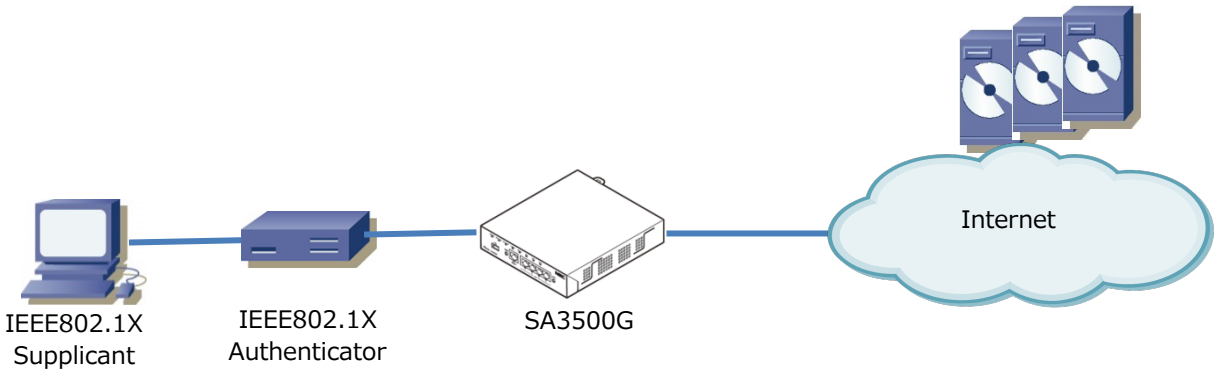
8.1.4. **ノードを IEEE802.1X で認証している**

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。

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。



9. 機能一覧

ファームウェアバージョン		3.0.1	3.1.26 / 3.1.34 /3.1.35		備考
対応動作モード		ブリッジ	ブリッジ	ルータ	
セキュリティ・スキャン機能		○	○	○	
	ファイアウォール（FW）	×	×	○	
	アンチウイルス機能（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）	○	○	○	
	Aspire 連携	○	○	○	
	メール通知	×	○	○	
	パトライト連携	×	○	○	
	セキュリティログ	○	○	○	
	統計情報	○	○	○	
ルータ機能		×	×	○	
	IPsec/IKE v1	×	×	○	
パケット中継機能（IPv4）		○	○	○	
	IPv4 ルーティング（NAT/NAPT）	×	×	○	
	DHCP クライアント	○	○	○	
	DHCP サーバ	×	×	○	
	PPPoE クライアント	×	×	○	
	ポートマッピング	×	×	○	
	静的ルーティング	×	×	○	
	パケットフィルタ	×	×	○	
	ICMP redirect 機能	×	×	○	
プロキシ DNS		×	×	○	
DNS リゾルバ機能		○	○	○	
無線 LAN 機能		×	×	○	
	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	×	×	○	
管理機能		×	×	○	
	SNMPv1, SNMPv2c	×	×	○	
設定 Web 機能		○	○	○	
メンテナンス機能		○	○	○	

	パスワード変更	○	○	○	
	時刻設定	○	○	○	
	設定値の保存＆復元	○	○	○	
	設定値の初期化	○	○	○	
	メンテナンスバージョンアップ	○	○	○	
	オンラインバージョンアップ	×	○	○	
	ローカルバージョンアップ	○	○	○	
	ホーム IP ロケーション機能	×	×	○	
情報表示機能		○	○	○	
	デバイスの状態	○	○	○	
	装置管理情報	×	×	○	
	VPN 接続状態	×	×	○	
	VPN 統計情報	×	×	○	
	MIB 情報	×	×	○	
診断機能		×	○	○	
	ping	×	○	○	

10. 用語集

10.1. 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ー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。 ホワイト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、ルーターなどを指します。
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。

10.2. **ASCII コード表**

上 位 4 ビ ッ ト →

下位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	

使用可能コード

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)

11. お問い合わせ窓口

Aterm Biz製品の機能、操作、設定、故障診断、保守、修理、オプションのご購入などのご質問は、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	http://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。

Aterm Biz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、メールにて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時には、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
AM1-002926-003

2016 年 11 月 第 3.0 版
ＮＥＣプラットフォームズ株式会社