\Orchestrating a brighter world NEC

セキュリティアプライアンス

Aterm® SA3500G

製品概要ご説明資料 2ndエンハンス対応版（Rev 5.1）

日本電気株式会社
NECプラットフォームズ株式会社

目次

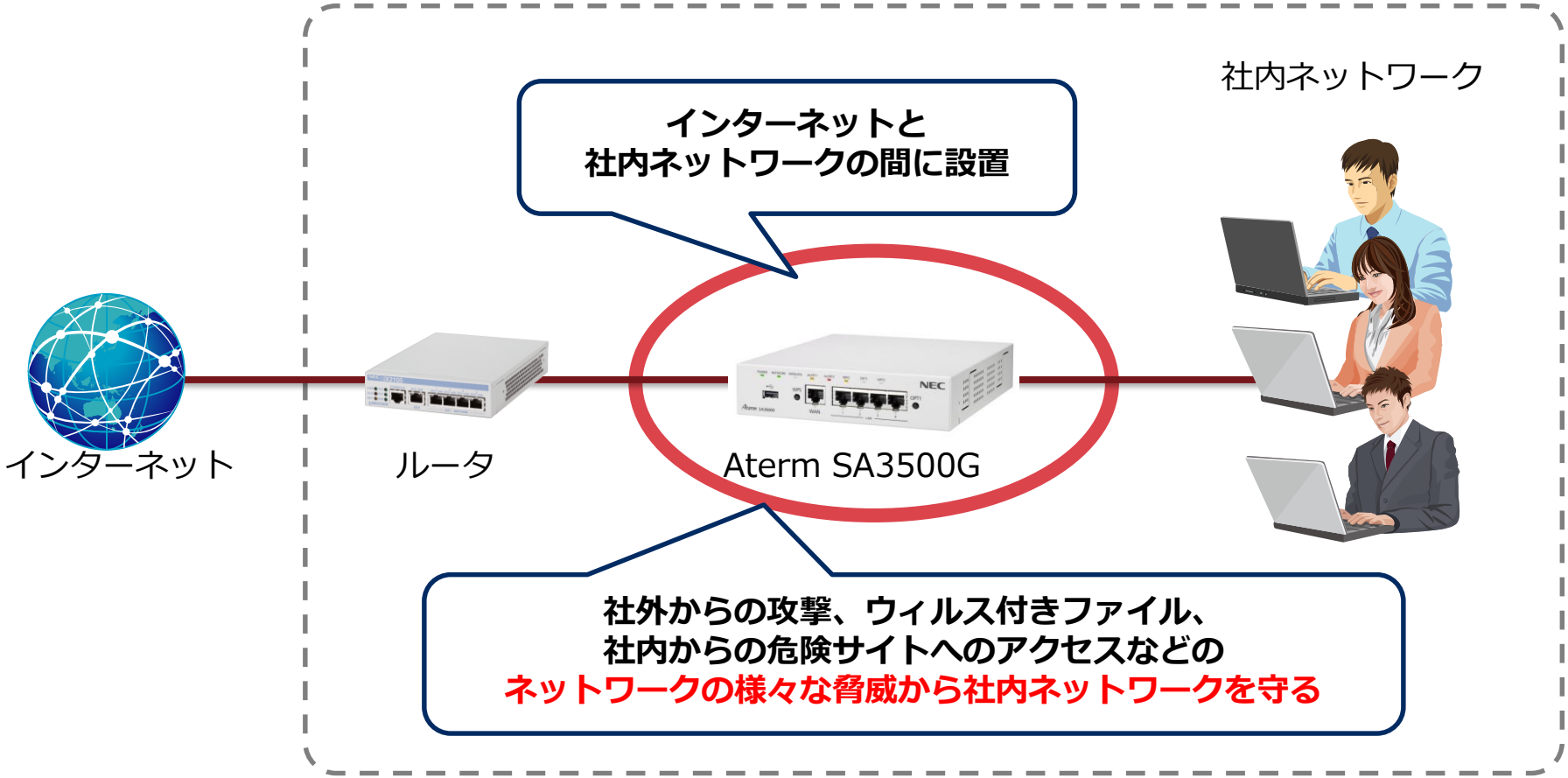
① はじめに
② 特長
③ ラインナップ
④ 機能概要
- セキュリティ機能
- お知らせ機能
- 管理機能
- メンテナンス機能
- ネットワーク機能

⑤ サポート情報

①はじめに

セキュリティアプライアンス　SA3500Gとは？

ネットワークの出入り口に設置することで、ネットワークの脅威から社内ネットワークを守るいわゆるUTMカテゴリの製品です。



本製品のおすすめ先

マイナンバーの個人番号・
特定個人情報を扱う上で
セキュリティ対策が必要！

しかしセキュリティ対策
を行う専任の情報システム
の担当者・部門がない！

このような悩みをお持ちの中小企業様にぜひご紹介したい製品です。

Aterm Biz シリーズ

セキュリティアプライアンス

Aterm® SA3500G

②特長

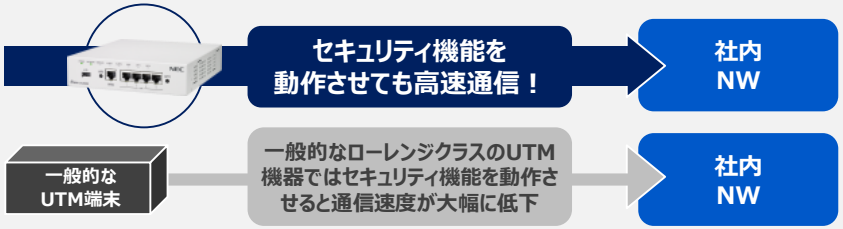
特長

1 カンタンに導入

ブリッジタイプで既存ネットワーク構成を変えず**「ポン付け」**が可能。
設定もシンプルで簡単です。

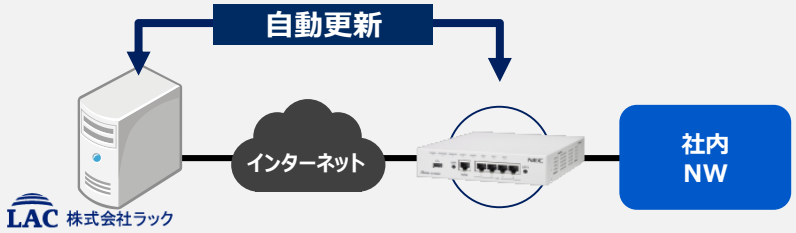
2 ハイコストパフォーマンス

高速セキュリティエンジンを採用することでセキュリティ機能がONの状態でも **約700Mbps**※の高スループットを実現。
※当社、試験環境による測定



3 安心の自動更新

サイバーセキュリティ分野で評価の高い**ラック社との協業**により、
ラック社が大企業向けのハイエンドなセキュリティ対策機器に提供
している攻撃分析情報「JSIG」（ジェイシグ）を本製品に提供。

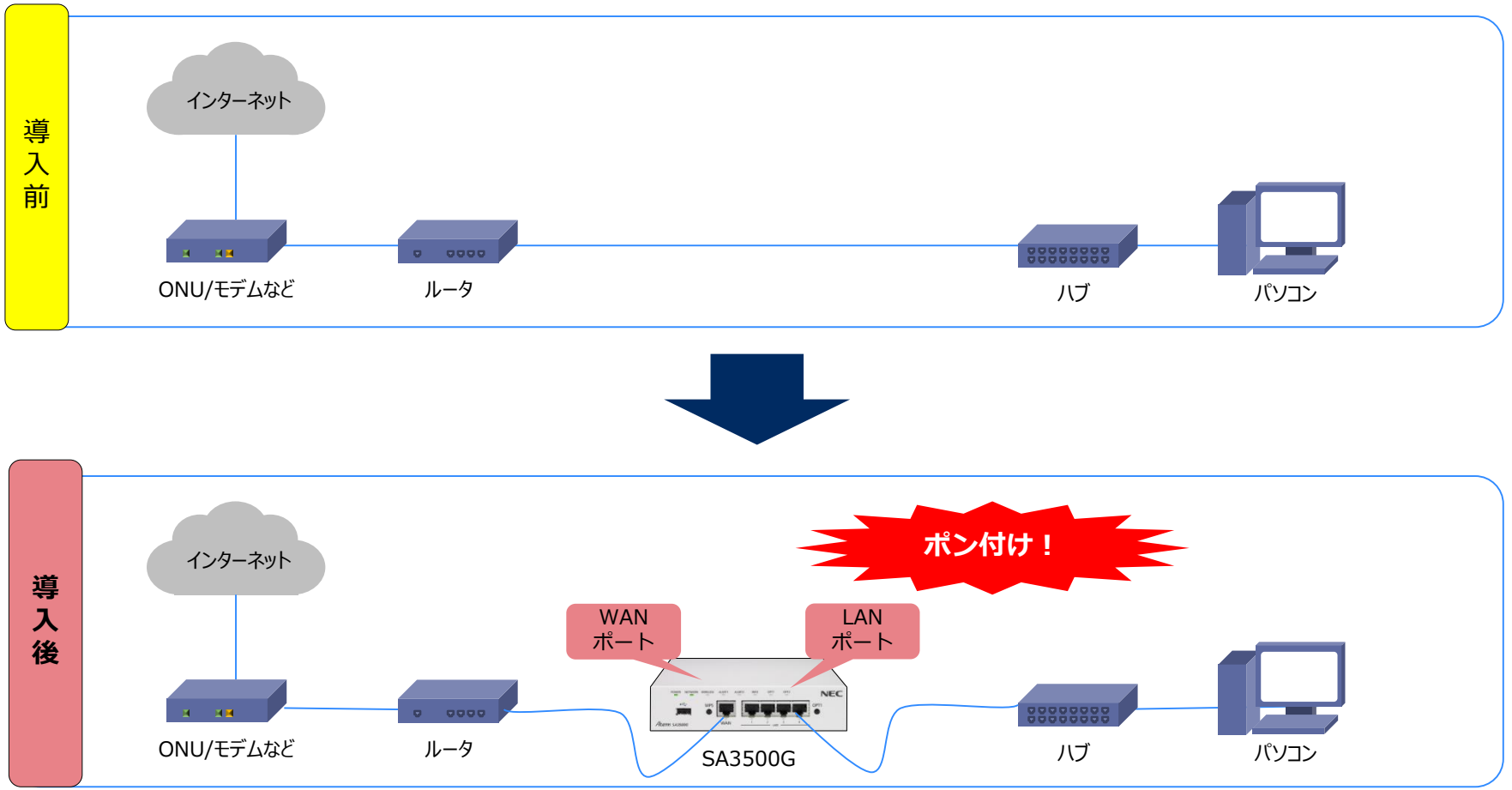


さらに！ Aspire UX連携機能も搭載

UNIVERGE Aspire UXとSA3500Gを連携し、脅威検
出時に、機能ボタンで**ランプ表示**できます。

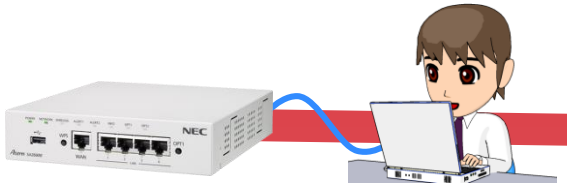
1．カンタンに導入

ブリッジタイプ※で、既存のネットワーク構成を大きく変えず、ポン付け可能なセキュリティソリューションです。

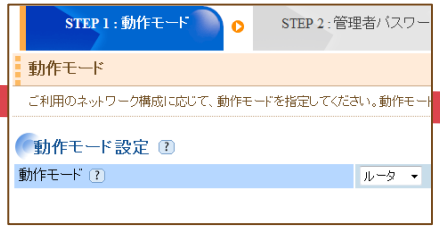


※モード設定切替によりルータとしての動作も可能です。

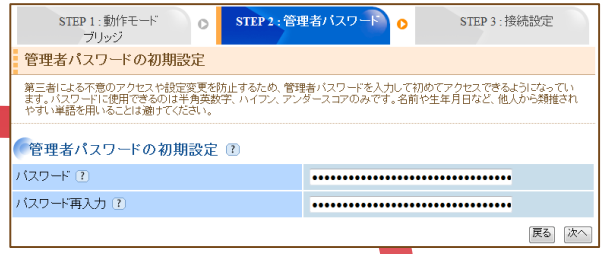
初期設定の概要



①ブラウザでアクセス

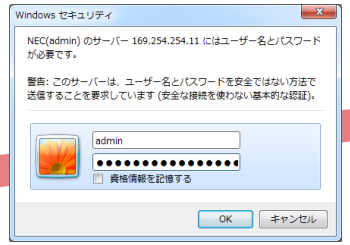


②動作モードの設定



③管理者パスワードの設定

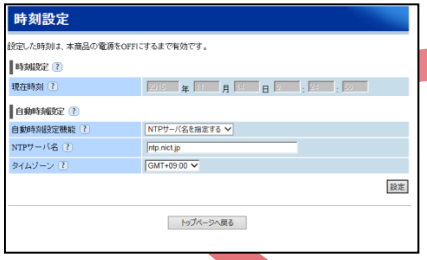
④IPアドレスの設定



⑤設定したパスワードで再ログイン

⑥ファームウェアの更新設定

基本的にはデフォルトのままで動作OK



⑦時刻の設定（NTPの設定）

基本的にはデフォルトのままで動作OK（DHCP設定）

デフォルトのままで動作OK（NICT参照）

⑧セキュリティ機能の設定

⑨アクティベーションの実施

運用開始

NICT・情報通信研究機構

https://youtu.be/9F4w3rYZBB0

本ページで掲載している設定手順は動画でもご紹介しております。

2．ハイコストパフォーマンス

ミドルエンドの価格帯ながら、高速なセキュリティエンジンの採用により、セキュリティ機能を動作させた際の**スループットはハイエンドクラス**

		NECPF SA3500G	A社 ローエンド	A社 ハイエンド	B社 ローエンド	C社 ローエンド	C社 ミドルエンド
UTM機能	ファイアウォール	○（ルータ時）	○	○	○	○	○
	アプリケーション制御	○	○	○	○	△(P2Pアプリの検出)	△(P2Pアプリの検出)
	IDS/IPS（侵入検知/侵入防止）	○	○	○	○	○	○
	アンチウイルス	○	○	○	○	○	○
	Webフィルタリング	○	○	○	○	○	○
	状況確認（パソコン）	○	○	○	○	○	○
	状況確認（キーテレ連携）	○	–	–	–	△（要サーバ）	△（要サーバ）
ルータ機能	ルーティング機能	○（ルータ時）	○	○	○	○	○
	VPN	○（ルータ時）	○	○	○	–	–
性能	FW スループット(1500バイト)	1.0Gbps ※	1.5Gbps	2.5Gbps	500Mps	1000Mbps	1000Mbps
	Anti Virus	**700Mbps**	50Mbps	**650Mbps**	60Mbps	150Mbps	150Mbps
	IPS（侵入防止）	**700Mbps**	200Mpps	**950Mbps**	80Mbps	300Mbps	300Mbps
	GbE WAN	1	2	2	1	1	1
	GbE LAN	4	7	14(FE)	4	6	6
	シリアルコンソール	-	1	1	1	メンテナンス専用Etherポート	
	USB	1	Device1/Host1	Device2/Host1	1	1	1
	無線LAN	802.11bgn （ルータ時）	802.11abgn	-	802.11bgn	-	802.1111abgn

※ショートパケットでも同等のスループット

3．安心の自動更新

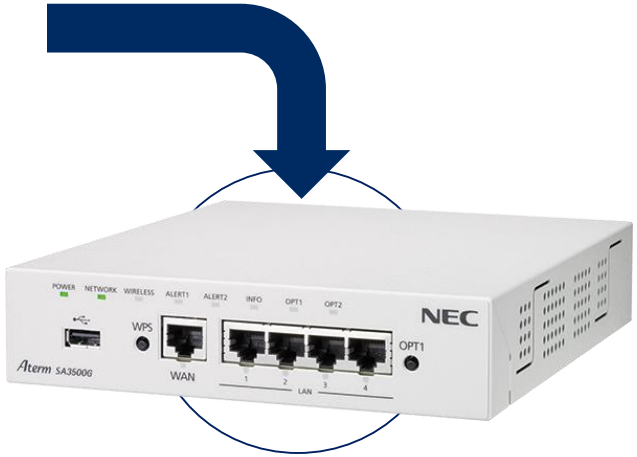
日本企業には日本のUTMを。

サイバー攻撃をする者は、市販されているウイルス対策ソフトやIDS/IPS機器では発見されないように巧妙に攻撃手法を変化させています。
そのため、一般的なメーカが提供しているシグネチャだけでは、攻撃行動を捉える事ができないケースがあります。特に日本特有のものやマイナーな脆弱性を狙った攻撃、発見されたばかりの脆弱性、脆弱性以外の問題を狙った攻撃には対応が間に合わない場合が多々あります。

Aterm SA3500Gは、こういった攻撃に対応すべく、**ラック社との協業**によりラック社が大企業向けのハイエンドなセキュリティ対策機器に提供している攻撃分析情報「JSIG」（ジェイシグ）を提供いただいております。

ラック社の運営する日本最大級のセキュリティ監視センター「JSOC」により生成・配信される攻撃分析情報「JSIG」

JSOC（ジェイソック）は、最前線でセキュリティ事故の対応やセキュリティ運用監視という活動を実施している。
ここで発見された情報を取り込み攻撃分析情報「JSIG（JSIG）」を生成し、大企業向けのハイエンドなセキュリティ対策機器に提供している。



SMB市場向けの製品でJSIGの配信を受けているのはAterm SA3500Gだけ！

ご参考：株式会社ラックについて

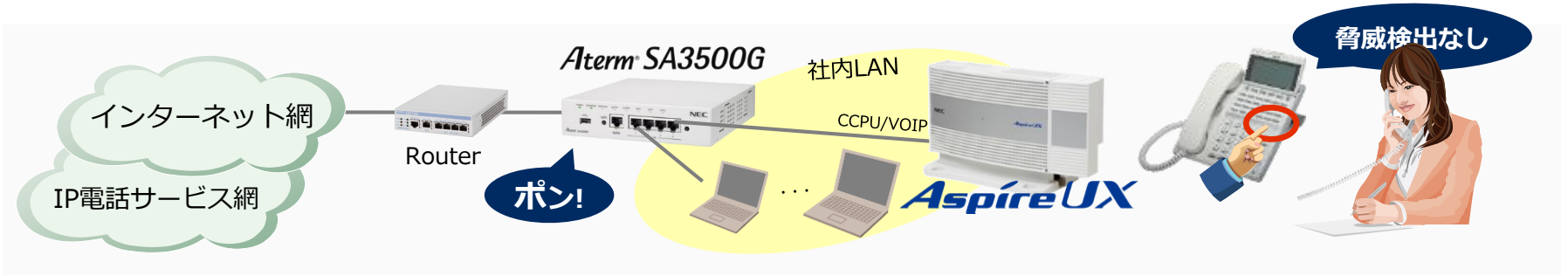
LAC 株式会社ラック

JSIG

- ラックは、1986年にシステム開発事業で創業、社会の基盤システムの開発を行ってきた。1995年にはいち早く情報セキュリティ事業を開始し、現在では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、官公庁・企業・団体等のお客様に業界屈指のセキュリティ技術を駆使した、先端のITトータルソリューションサービスを提供。
- 2015年には、米フロスト＆サリバンより、「セキュリティ監視」「脆弱性診断」「セキュリティ事故対応」「セキュリティコンサルティング」などが高く評価され、**「日本市場マネージドセキュリティーサービス プロバイダー最優秀賞」受賞**。
- **JSOC（Japan Security Operation Center）**
  - 2000年に不正アクセス監視のための監視センターを設立。2002年より名称をJapan Security Operation Center「JSOC」を変更。
  - 2014年4月時点において契約顧客は、官公庁や大手企業を中心に、850団体以上、1,500センサー以上。
- **JSIG**
  - JSOCが侵入検知システム（IDS）や侵入防御システム（IPS）に配信し高く評価を受けている攻撃分析情報「JSIG（ジェイシグ）」です。国内大企業向けのハイエンドなセキュリティ対策機器に提供しているこの情報を、中小規模事業者向けのセキュリティアプライアンス（UTM）に提供。また、国内約850社のセキュリティ監視や、緊急対応サービス「サイバー119」の調査などから得られた不正なURLの情報についても提供を行う。
- 2009年10月よりサイバー事件の緊急対応に特化した専門組織「サイバー救急センター」を新設
- 2014年に顧客情報流出事件のあった、ベネッセコーポレーションは、その後ラックと高セキュリティのDB保守・運用会社「株式会社ベネッセインフォシェル」を設立(2015年1月）。
- **中小規模事業者向けUTMに攻撃分析情報「JSIG」を提供（ラック、NECプラットフォームズ）（2015/12）http://scan.netsecurity.ne.jp/article/2016/02/01/38039.html**

さらに！　「UNIVERGE Aspire UX」との連携機能

UNIVERGE Aspire UXとSA3500Gを連携し、脅威検出/ファームウェアアップデート/ライセンスの付加情報を機能ボタンにランプ表示できます。また、機能ボタン押下で付加情報の内容をディスプレイ表示することができます。



① 脅威検出の有無

脅威検出の有無を情報表示します。
［5分間隔で情報取得します］

- **機能ボタンランプ表示**
  消灯：脅威検出なし
  赤点灯：脅威検出あり

- **機能ボタン押下時の情報表示**
  脅威検出の有無と検出時の種類（WebGuard機能もしくはAntiVirus機能）を表示します。消灯も本体と連携します。

検出なし
ｾｷｭﾘﾃｨｱﾌﾟﾗｲｱﾝｽ Alarm
脅威検出情報はありません

検出あり
2015/12/21 15:42:00
WebGuard Block

② ファームウェアアップデート情報

F/Wアップデートの有無を情報表示します。
［1日1回（AM2:00）情報取得します］

- **機能ボタンランプ表示**
  消灯：アップデートなし
  赤点灯：アップデートあり

- **機能ボタン押下時の情報表示**
  F/Wアップデート情報の有無を表示します。

更新なし
ｾｷｭﾘﾃｨｱﾌﾟﾗｲｱﾝｽ F/W
F/Wは最新の状態です

更新あり
ｾｷｭﾘﾃｨｱﾌﾟﾗｲｱﾝｽ F/W
更新F/Wがあります

③ ライセンス情報

ライセンスを情報表示します。
［1日1回（AM2:00）情報取得します］

- **機能ボタンランプ表示**
  消灯：ライセンスが有効
  赤点灯：ライセンスの期限切れ間近(1ヶ月)など
  赤点滅：ライセンスが無効

- **機能ボタン押下時の情報表示**
  ライセンス有効期限を表示します。

ライセンス有効
ｾｷｭﾘﾃｨｱﾌﾟﾗｲｱﾝｽ License
License 有効期限[2021/12/10]

ライセンス無効
ｾｷｭﾘﾃｨｱﾌﾟﾗｲｱﾝｽ License
License 無効です

③ラインナップ

ラインナップ

ライセンス期間分の「シグネチャ更新」と「先出しセンドバック保守」
コミコミでわかりやすい価格設定

ラインナップ	希望小売価格
Aterm SA3500G（1年ライセンス付き）	198,000円
Aterm SA3500G（5年ライセンス付き）	738,000円
Aterm SA3500G（6年ライセンス付き）	848,000円
Aterm SA3500G（7年ライセンス付き）	958,000円

ライセンス期間は延長もできて安心

Aterm SA3500G追加ライセンス(1年)※	150,000円

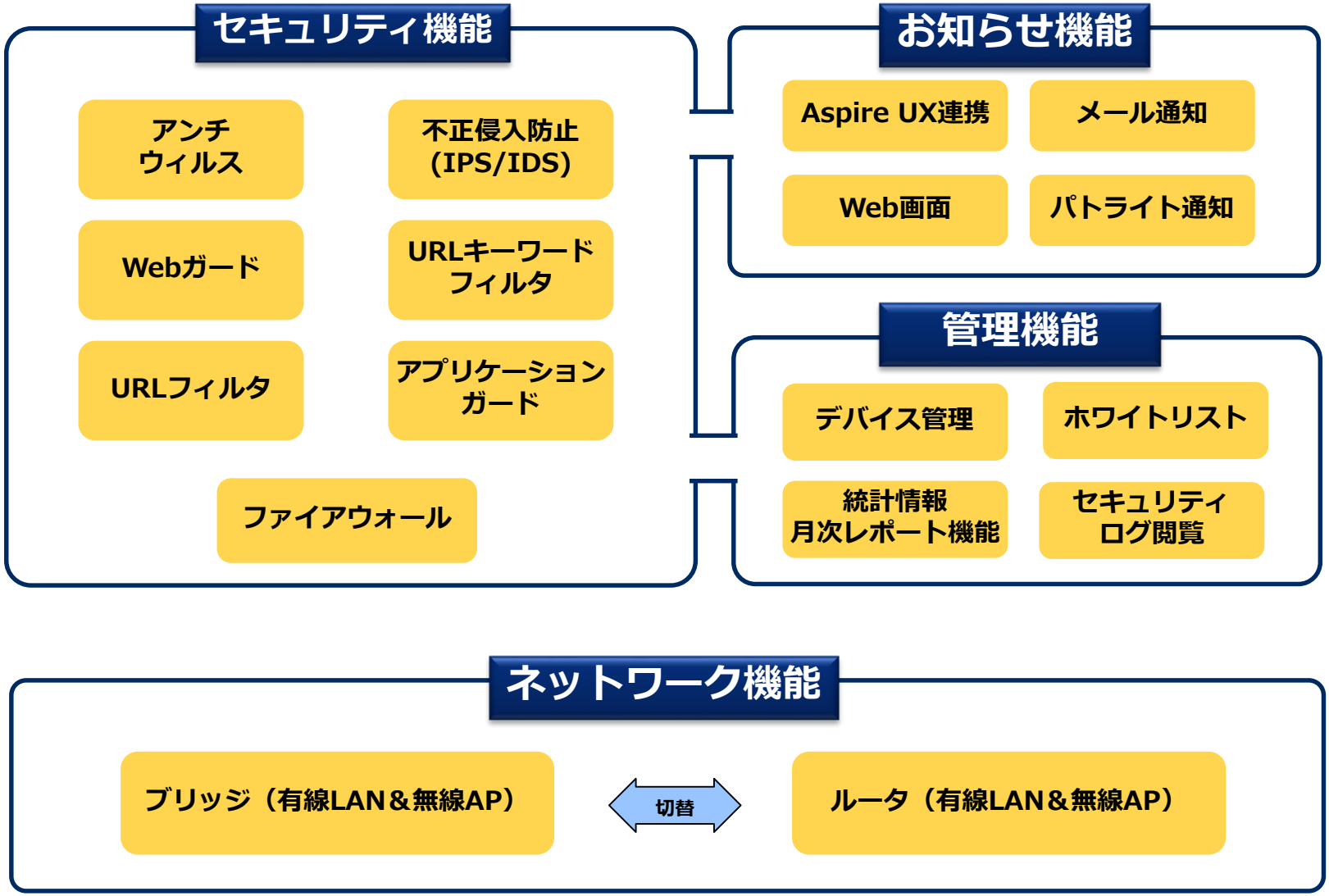
※ライセンス付き製品に対して、基本保守を含むライセンスを1年(365日)追加します。
製品のライセンス期間と合わせて7年まで追加ライセンスを購入できます。

④機能概要

本章で掲載している機能のうち、主な機能を動画で紹介しています。
是非こちらもご参照ください。

https://youtu.be/0hDT3YqAmRQ

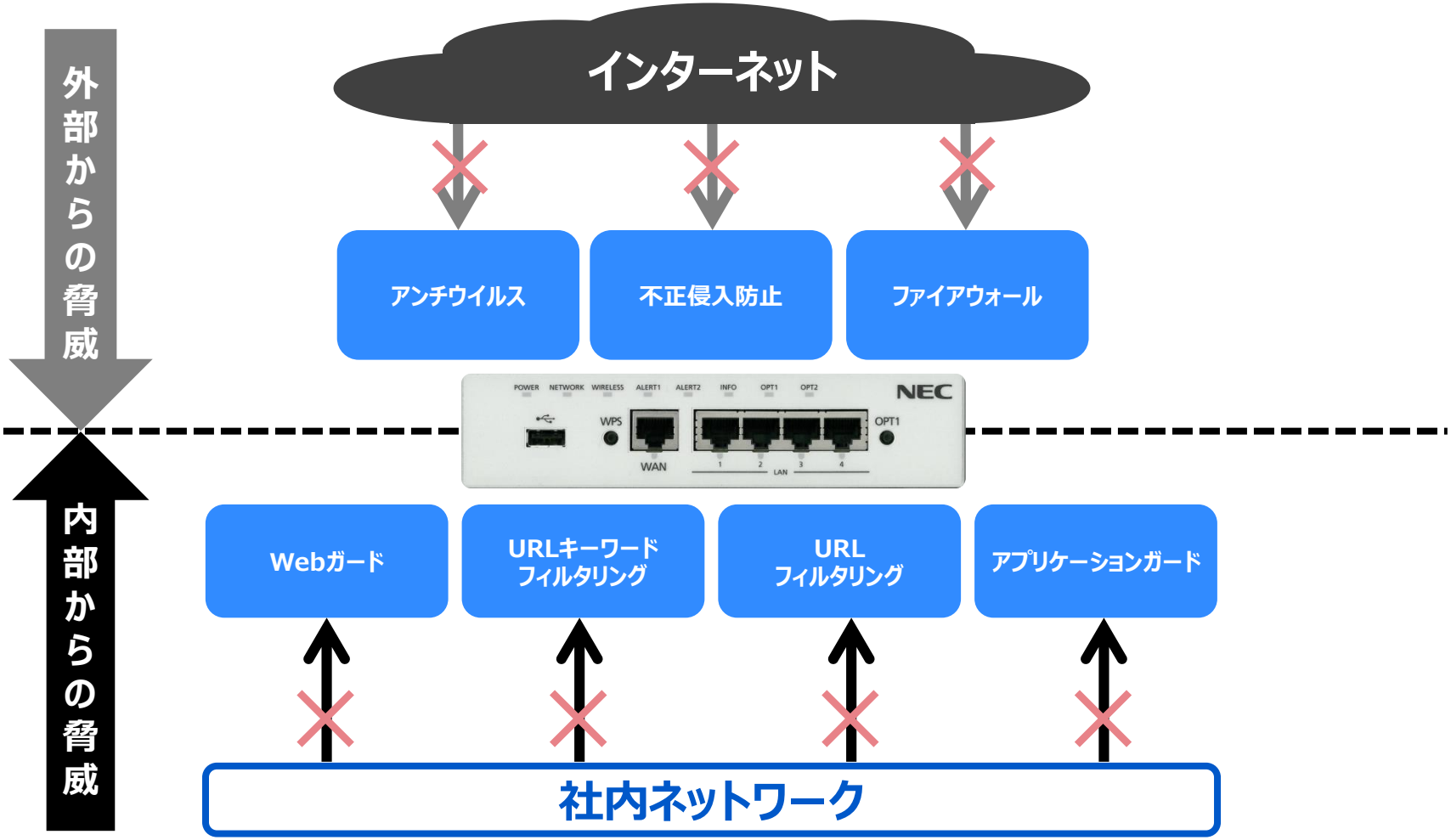
SA3500G機能マップ



セキュリティ機能

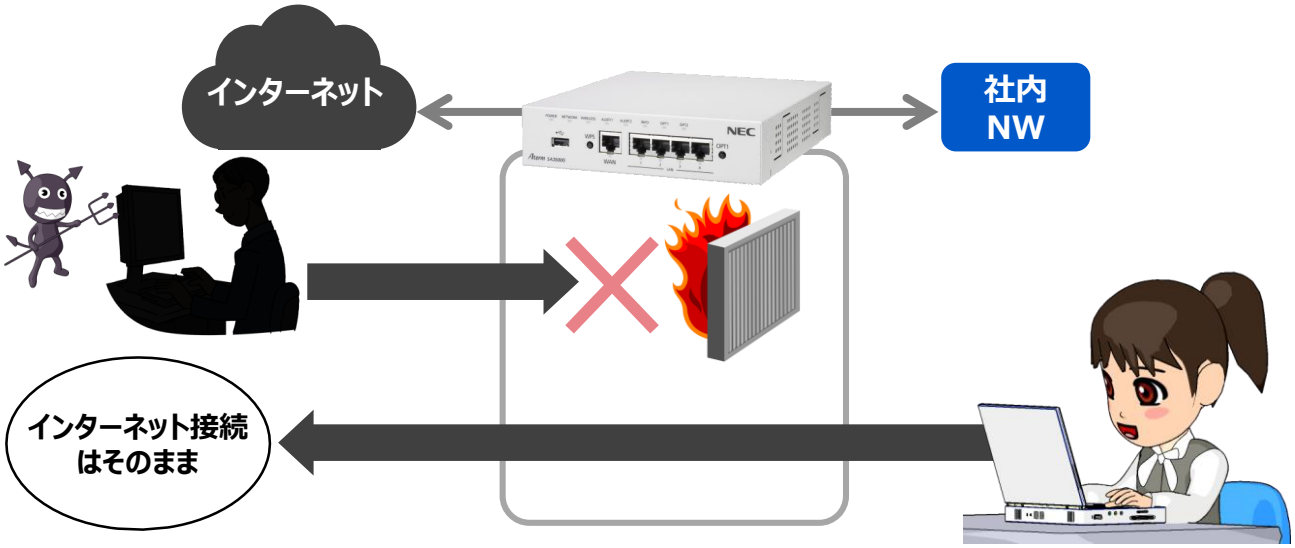
Aterm SA3500Gの7つのセキュリティー機能

以下7種類のガード機能により、「外部から」「内部から」の
双方からの脅威からお客様のネットワークを守ります。

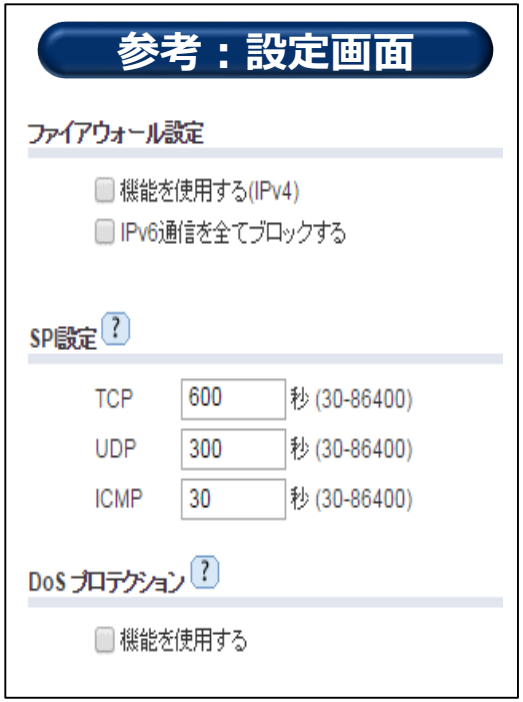


ファイアウォール

社外との通信をポート制御することで、社内ネットワークからのインターネット通信を損なわず、社外から社内ネットワークへのアクセスを制限



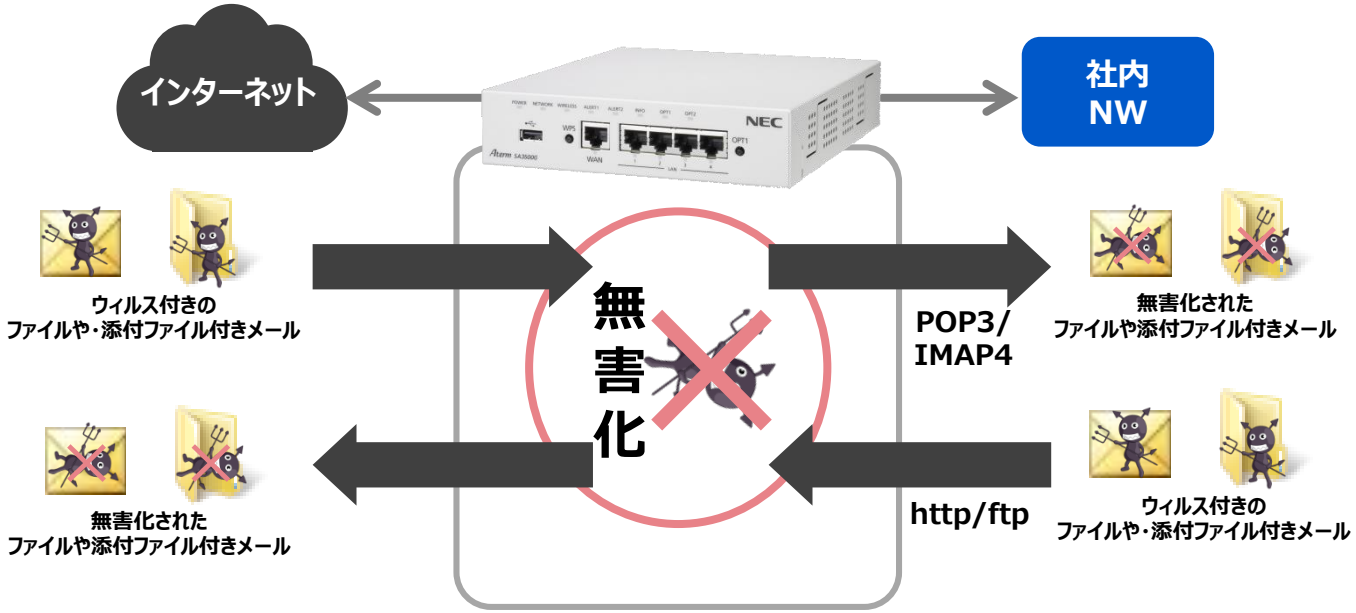
参考：設定画面



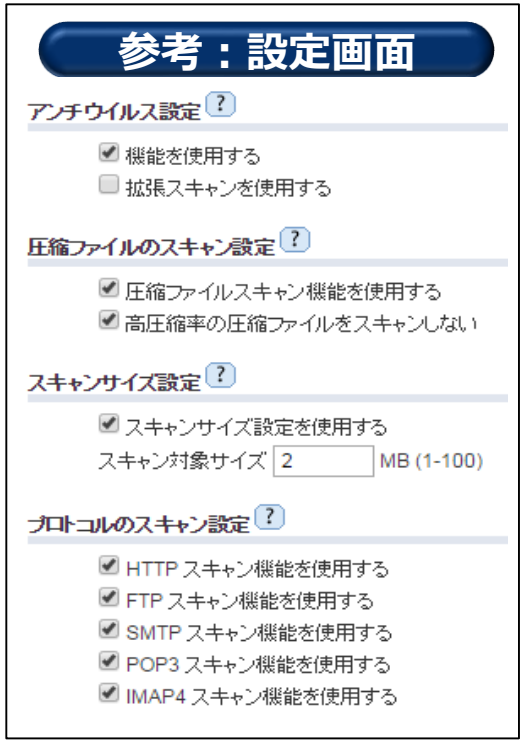
社外との通信をポート制御することで、社内ネットワークからのインターネット通信を損なわず、社外から社内ネットワークへのアクセスを制限仕組みです。
ルータモード/ブリッジモードのどちらでもご利用いただけます。

アンチウイルス

ホームページ閲覧時やメール受信、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、発見時には無害化



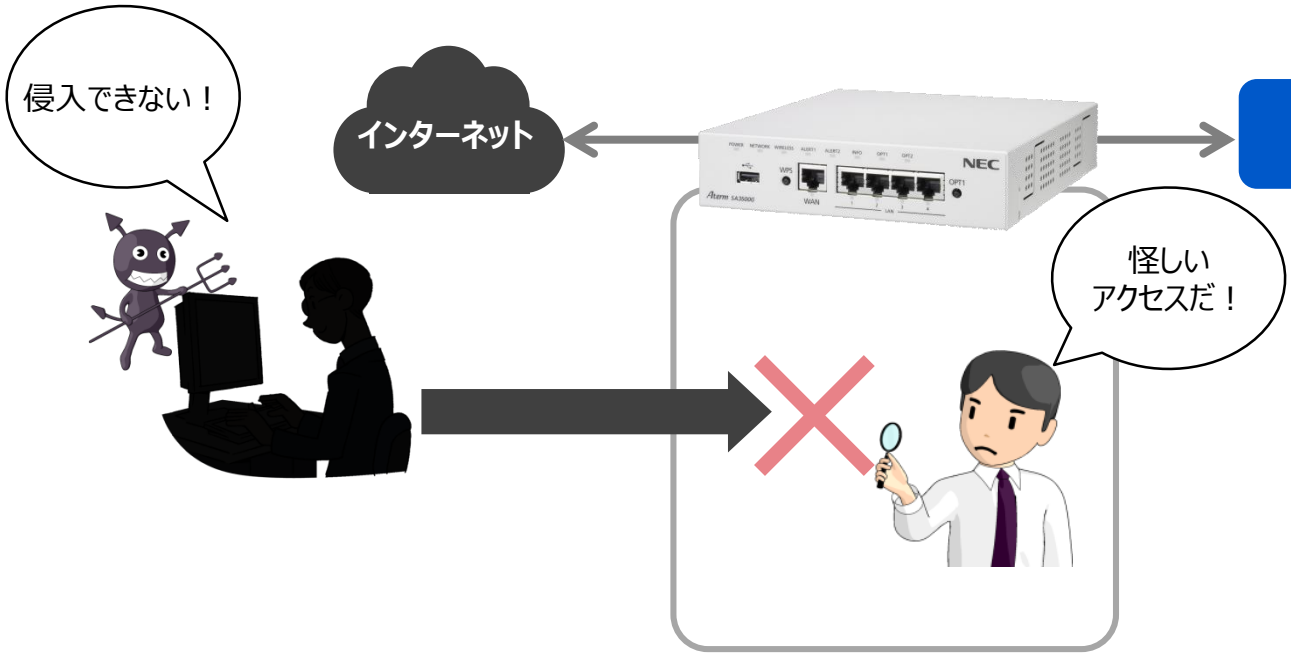
参考：設定画面

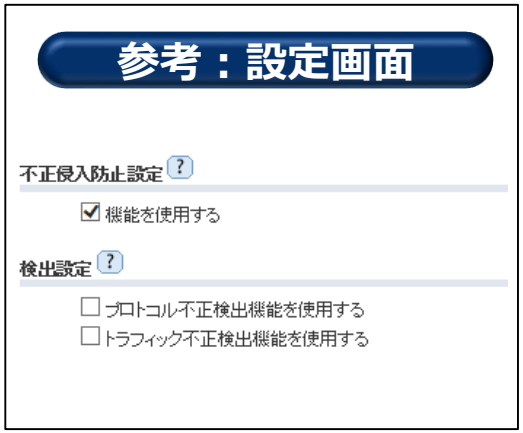


知っている人からのメールファイルや、著名なサイトにあるフリーソフトだからといってウィルスが無いとは限りません。本製品はファイルの内容を見て判断し、無害化します。この無害化されたファイルは社員が不用意に実行したり、ファイルを開こうとしてもウィルスにかかることはありません。

不正侵入防止

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／防止し、社内ネットワークへの不正なアクセスを防御する機能

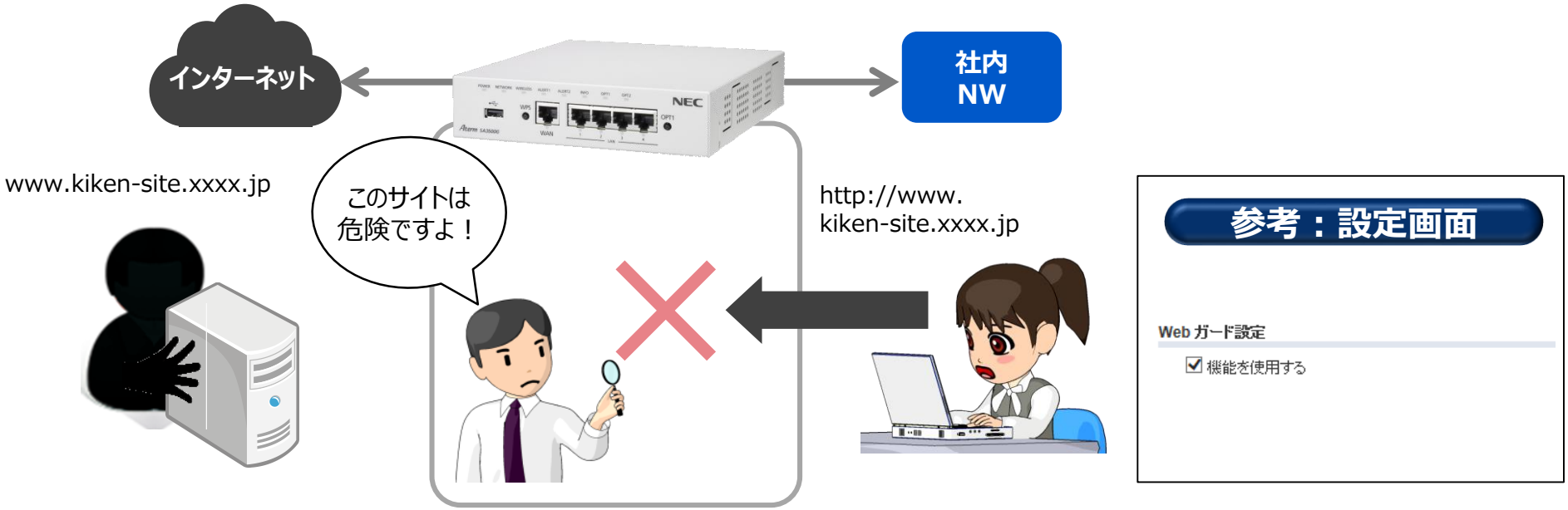




不正侵入の攻撃パターンをシグネチャ情報と比較してチェックすることで、不正侵入の攻撃を防ぎます。

Webガード

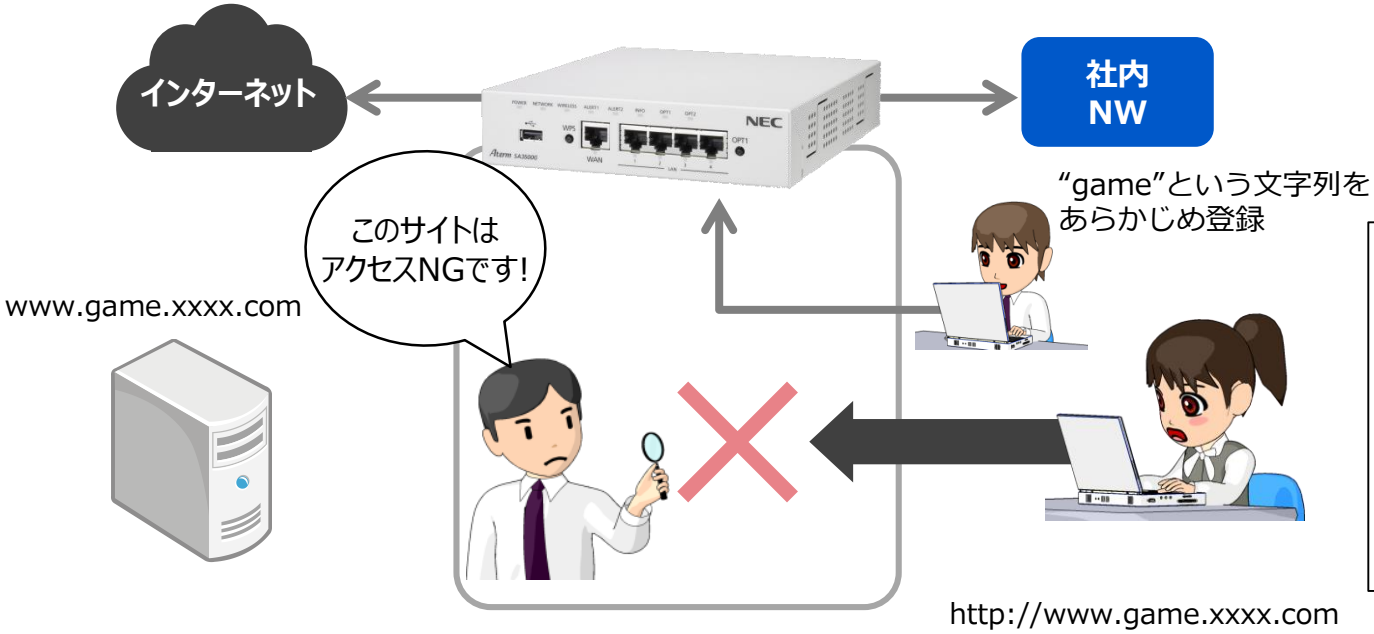
フィッシングサイトなどの詐欺サイトや、閲覧によりウィルス感染の可能性がある危険なサイトへのアクセスをガード

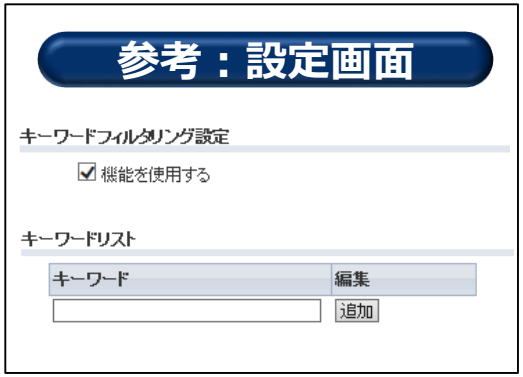


最新の危険サイトの情報により、社内からのアクセスを防御し、悪意のあるサイトからの被害を未然に防ぎます。

URLキーワードフィルタリング

Web閲覧において、あらかじめユーザが設定した特定の文字列をURLに含むページのアクセスをブロック

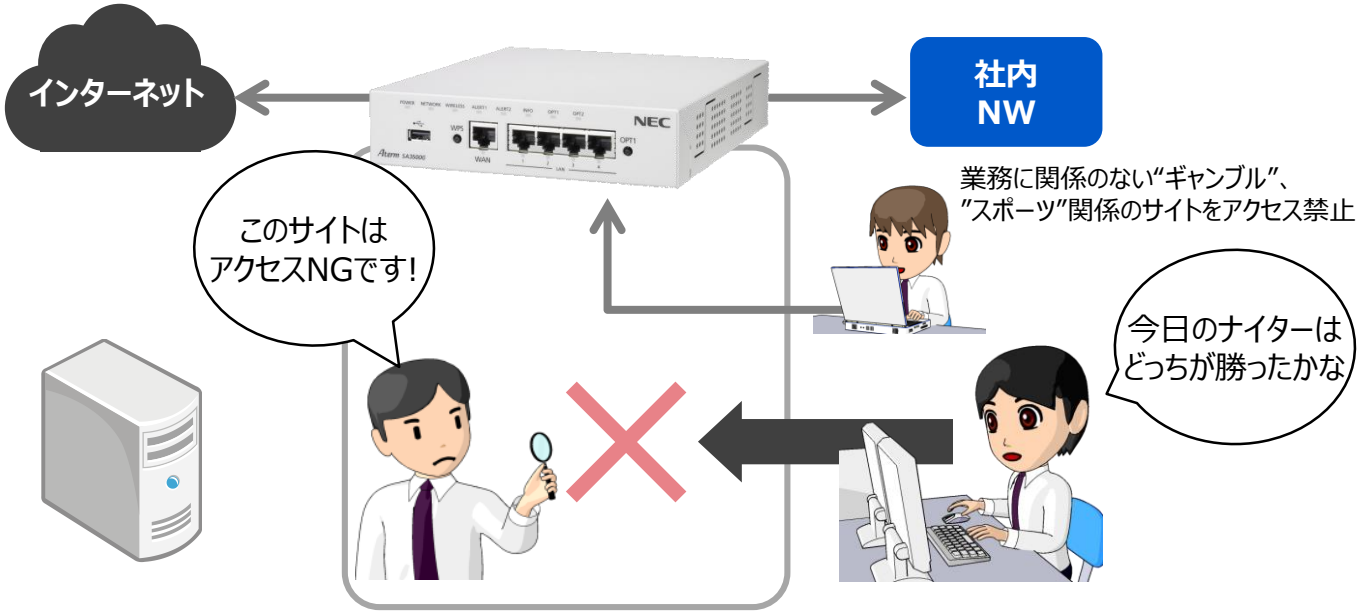




設定可能なURLのキーワードは最大100個です。

URLフィルタリング

多くの著名なサイトのURLをカテゴリごとに分類
分類されたカテゴリに対してアクセス禁止などの動作をユーザが設定可能



参考：設定画面

URL フィルタリング設定

☑ 機能を使用する

スタンダード設定

全てのカテゴリ	ブロックする	許可する
アダルトサイトカテゴリ	ブロックする	許可する
危険サイトカテゴリ	ブロックする	許可する

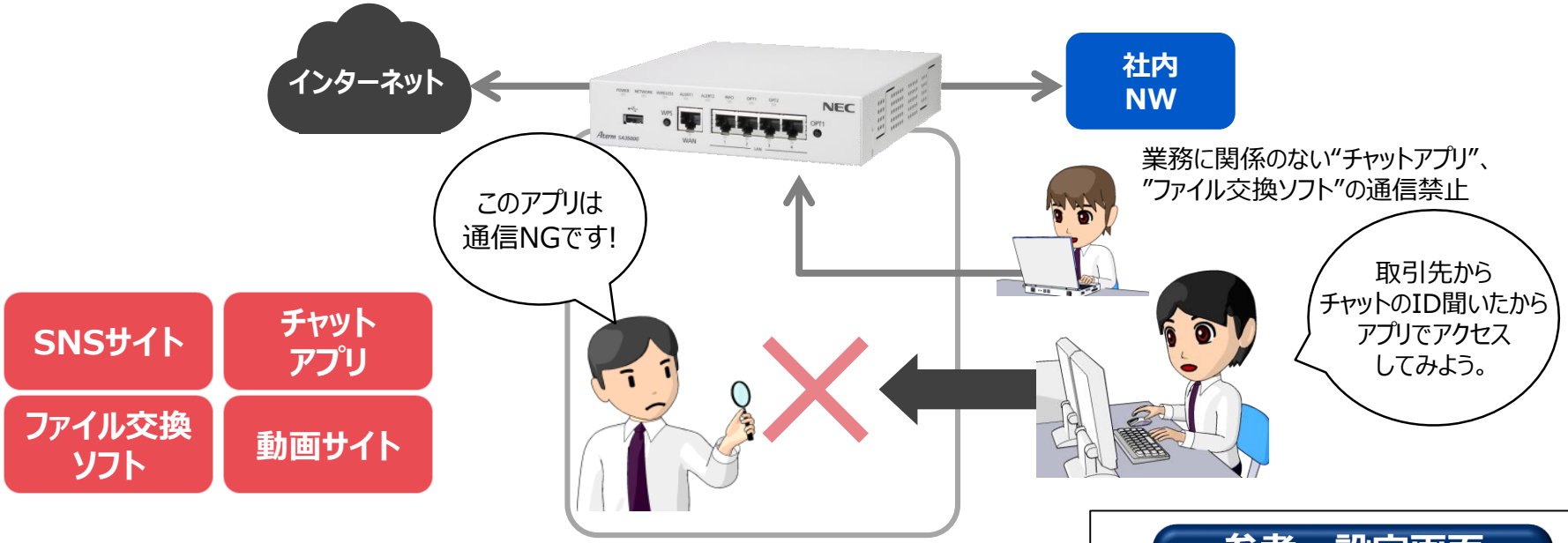
ブロックカテゴリ設定

カテゴリ	ブロック	許可
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	○	●

カテゴリの例：
ギャンブル、スポーツ、旅行、ニュース、求人情報、カジュアルライフ、アートと文化、飲み物と食物、ペット、ソーシャルネットワーク、ショッピングとオークション、ゲーム、コミック、漫画およびアニメ、ダウンロードサイト、P2P

アプリケーションガード

チャットアプリ、ファイル交換ソフト、SNSサイト、動画サイトなど、業務に関係ないアプリケーションの通信を検出し、制御することが可能



通信内容から、アプリケーションを検出・判別し、その通信を遮断することができます
各アプリの通信可否は設定可能です
チャットアプリ(Skype、Lineなど)・ファイル交換ソフト(BitTorrentなど)・ SNSサイト(Facebook、mixiなど)・動画サイト(YouTube、ニコニコ動画など)

参考：設定画面

アプリケーション制御設定

☑ 機能を使用する

ブロックアプリケーション設定

全てブロックする　全て許可する

#	アプリケーションID	アプリケーション名	カテゴリ	ブロック	許可
1	0229_01	Baidu Hi (Login)	IM	○	◉
2	0238_06	Baidu Space (DataFlow)	Social web site	○	◉
3	0238_07	Baidu Space (Protocol Detect)	Social web site	○	◉
4	3180_01	BBM (Login)	IM	○	◉
5	3179_03	BeeTalk (File Transfer)	IM	○	◉
6	3179_01	BeeTalk (Login)	IM	○	◉
7	0219_06	Gadu-Gadu (DataFlow)	IM	○	◉
8	1069_04	Google Hangouts (Audio)	IM	○	◉
9	1208_04	ICQ (Audio)	IM	○	◉

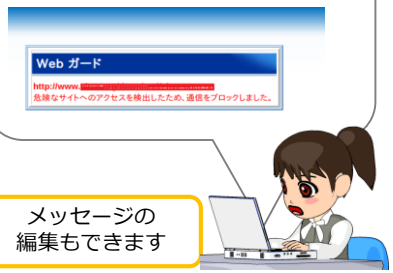
お知らせ機能

お知らせ機能

脅威を検出時、新しいファームウェア検知時などのお知らせ方法として、
メールや連携機種のAspireUX、パトライトによってお知らせします。

ブラウザでお知らせ

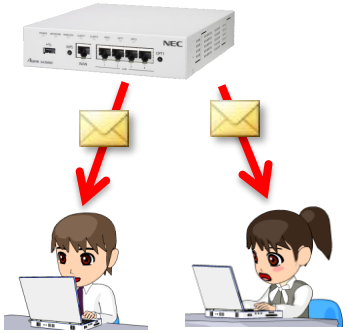
<ブラウザ画面の
通知イメージ>



メッセージの
編集もできます

※Webガードで検出された場合の例です。

メールでお知らせ



管理者　　端末利用者

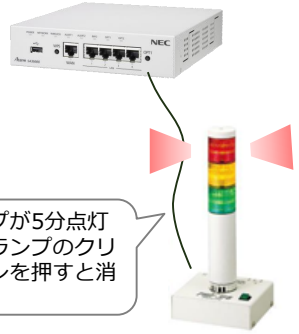
メッセージの編集もできます

Aspire UX連携機能でお知らせ

多機能電話機の
機能ボタンが点灯

本体と連携して消灯操作できます

パトライトでお知らせ



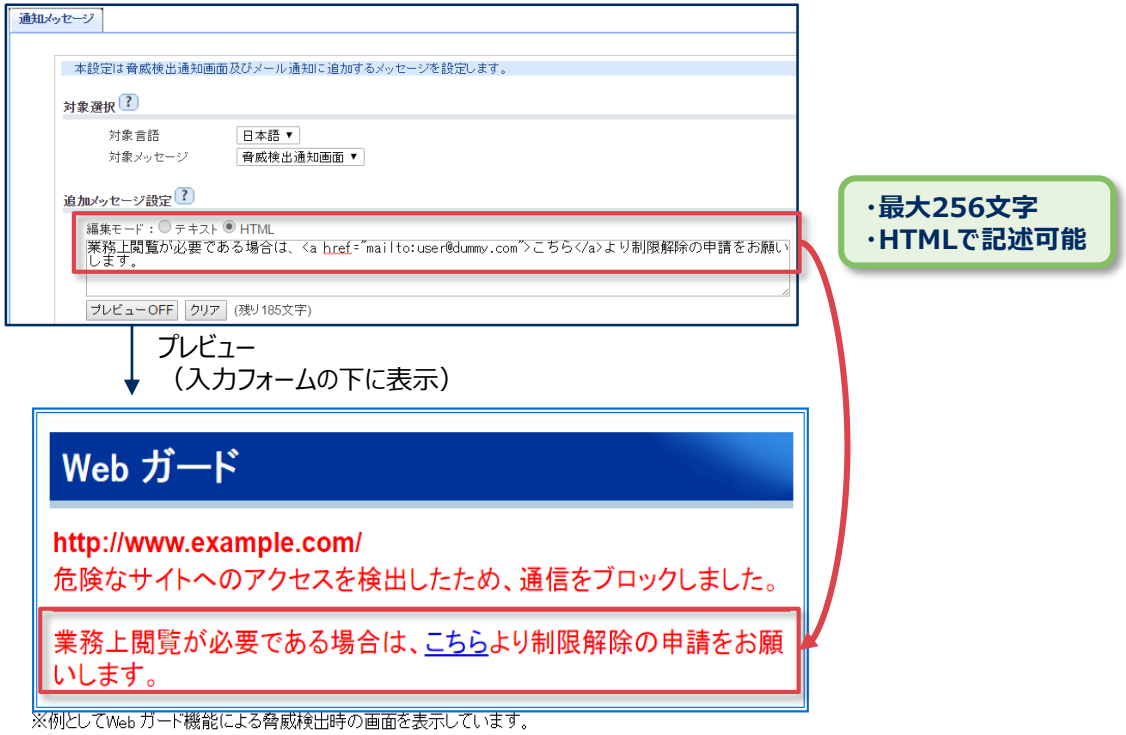
赤ランプが5分点灯
（パトランプのクリアボタンを押すと消えます）

ブラウザでお知らせ機能（通知メッセージのカスタマイズ）

脅威検出時にPCの使用者にお知らせする通知メッセージのカスタマイズができます。

- 案内文や問合せ先などの任意のメッセージを表示させることができ、検知時の業務効率化に活用できます。

■リダイレクト画面変更設定画面



※例としてWeb ガード機能による脅威検出時の画面を表示しています。

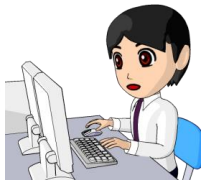
メールでお知らせ機能

脅威を検出した際に、メールの管理者と脅威対象となった端末（PC）使用者宛てにメールを発信できます。

管理者宛てには
常に送信

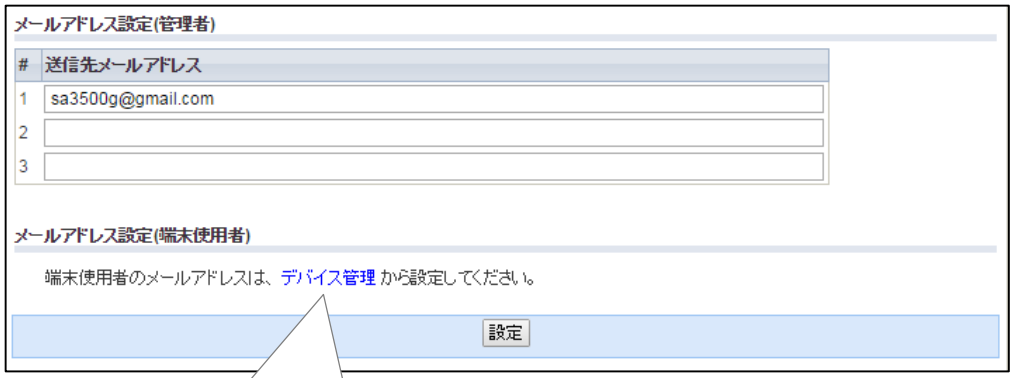
管理者

該当者のみに送信



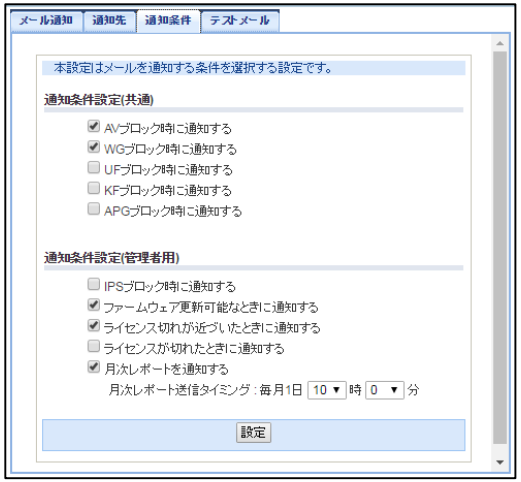
端末使用者

メール宛先の設定



脅威検出したPCのメールアドレスと紐づけるため、デバイス管理画面から登録します。

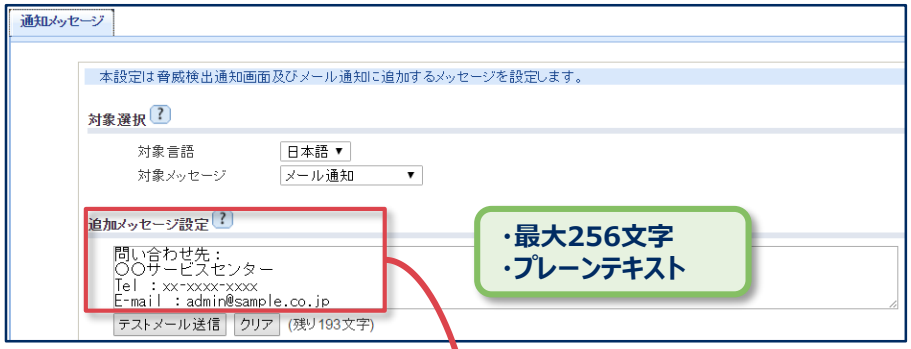
通知対象の設定



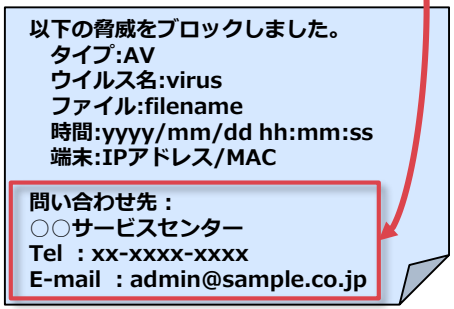
メールでお知らせ機能（通知メッセージのカスタマイズ）

- 脅威を検出した際に、管理者と使用者宛てに発信されるメールの通知メッセージをカスタマイズできます。
  案内文や問合せ先などの任意のメッセージを付加して、検知時の業務効率化に活用できます。

メール宛先の設定



通知メール例



「メールでお知らせ」の仕様

- お知らせ先のメールアドレスとして、管理者３件、端末使用者50件の登録ができます。

- 端末使用者宛てには、脅威の検出した際に、脅威を検出した端末をMACアドレスで識別して送信を行います。端末のMACアドレスと通知されるメールアドレスは、デバイス管理画面で登録することにより自動的に関連付けて送信されます。
- 通知内容とタイミングとそれぞれの通知先は以下のような対応となっております。

通知内容	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でガードしたとき		○	○
	IPSでガードしたとき		○	–
ライセンス情報	ライセンス切れ間近(30日前)のとき	1)動作中、ライセンス切れ間近になったとき 2)装置起動時、ライセンス切れ間近のとき 3)以降、24時間毎	○	–
	ライセンスが切れたとき	1)動作中、ライセンスが切れたとき 2)装置起動時、ライセンスが切れていたとき	○	–
FWアップデート	更新可能なFWを検出したとき		○	–

<ご留意事項>

本機能はSA3500Gがメール送信クライアント機能として動作し、メール送信を行うことで実現しています。このため、送信用のメールアカウントも、お客様側でご用意いただき、メール送信の設定が必要となります。

パトライトでお知らせ

脅威を検出時にＬＡＮ接続タイプのパトライトを点灯させることができます。

赤ランプが5分点灯
（パトランプのクリアボタンを押すと消えます）

動作検証済みのパトライト

パトライト社製の以下の機種

PHN-3FBE1

NHS-□FV1
NHP-□FV1
NHL-□FV1
NHS-□FB1
NHP-□FB1
NHL-□FB1

＜パトライト関連の設定画面＞

管理機能

デバイス管理機能

ネットワークに接続されたデバイス情報を管理することができます。

①接続されているパソコンや、スマホなどのデバイス情報・状態が確認できます。（最大100件）

②メール通知や統計情報の対象デバイスを指定できます。（最大50件）

③デバイス管理画面からデバイス毎の統計情報表示と連携します。

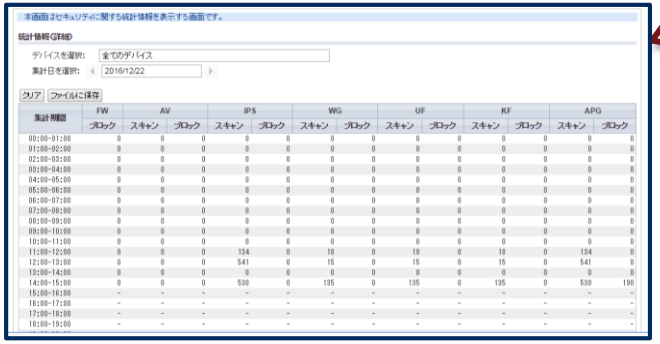
識別しやすい名前を任意に登録できます。

ここをチェックすることで、脅威等のメール通知や、デバイス毎の個別統計の対象にすることができます。（各50個まで）

デバイス一覧

#	MACアドレス	IPアドレス	情報	コメント	メールアドレス	接続	メール	統計情報		クリア
1	00:0D:5E:EE:B0:0F	169.254.254.1	Windows 7	事務PC(畑さん)	hata@aaa.bb.jp	有線	通知	収集	参照	クリア
2	48:43:7C:5C:23:DA	192.168.11.9	iPhone	iPhone（佐藤さん携帯	sato@aaa.bb.jp	無線	通知	収集	参照	クリア
3	C0:25:A2:8B:00:1B	192.168.11.11	Windows 7	事務PC(細田さん)	hosoda@aaa.bb.jp	有線	通知	収集	参照	クリア
4	C4:9A:02:40:72:3C	192.168.11.12	Nexus 5	スマホ(坂口さん)	akaguchi@aaa.bb.jp	無線	通知	収集	参照	クリア
5	FC:61:98:7A:40:80	192.168.11.10	Windows 7	事務PC(畑さん)	hata@aaa.bb.jp	有線	通知	収集	参照	クリア

機器から自動認識されたOS等の情報を表示します。

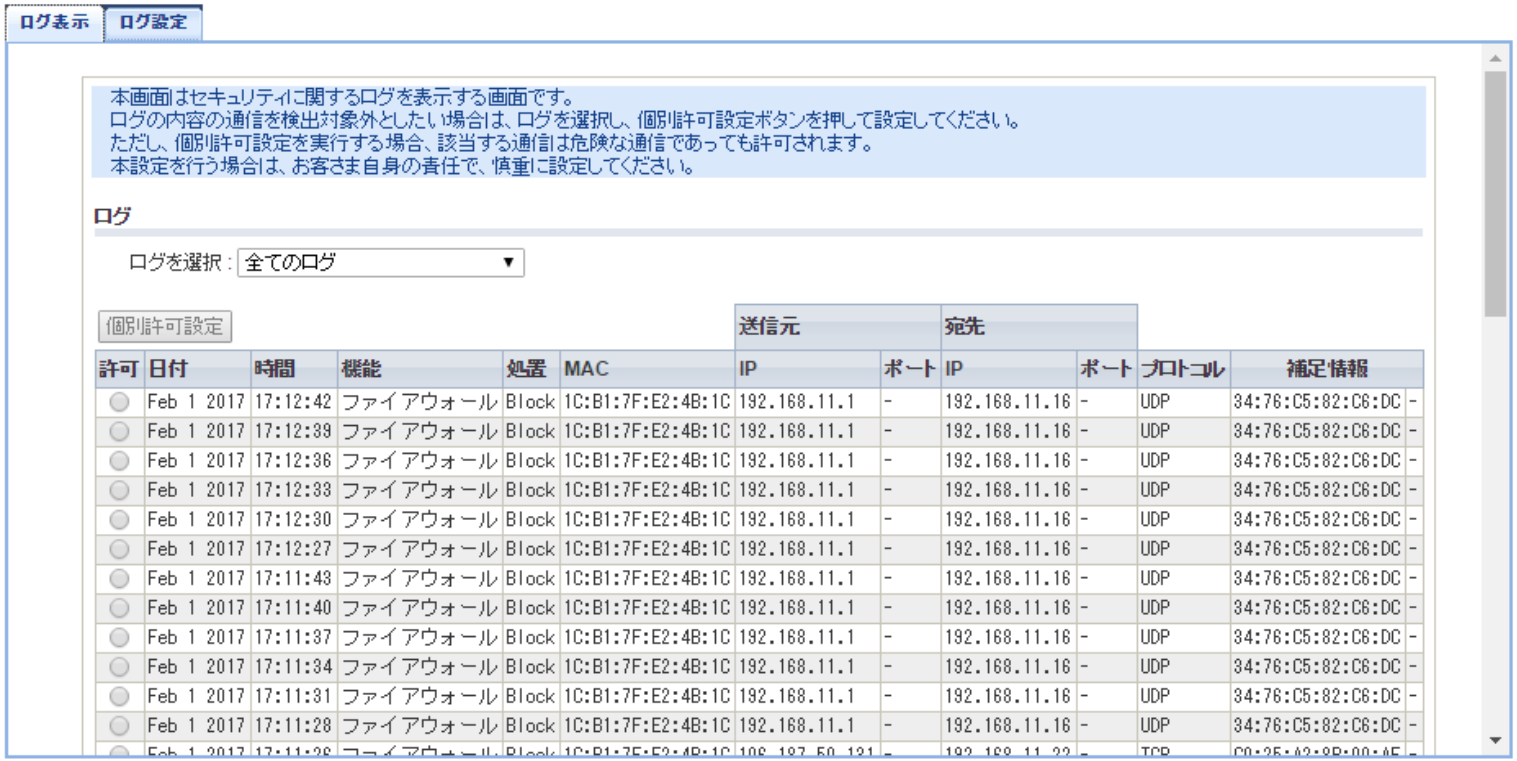


「参照」の押下で選択デバイス個別の統計情報画面を表示します。

セキュリティログ機能

直近1000件までのログを設定Web画面から閲覧できます。

- ログ保存容量は最大約500MBで、ファイルに出力することが可能です。
  - 件数換算で約72万件の蓄積が可能（内、直近1000件を閲覧できます）



統計情報機能

各セキュリティ機能毎に、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集計情報として表示します。

- 表示の単位は、集計期間の単位は日/週/月から選択できます。

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 1 / 1 | 情報表示件数 50 件 | 最新状態に更新 | クリア | ファイルに保存

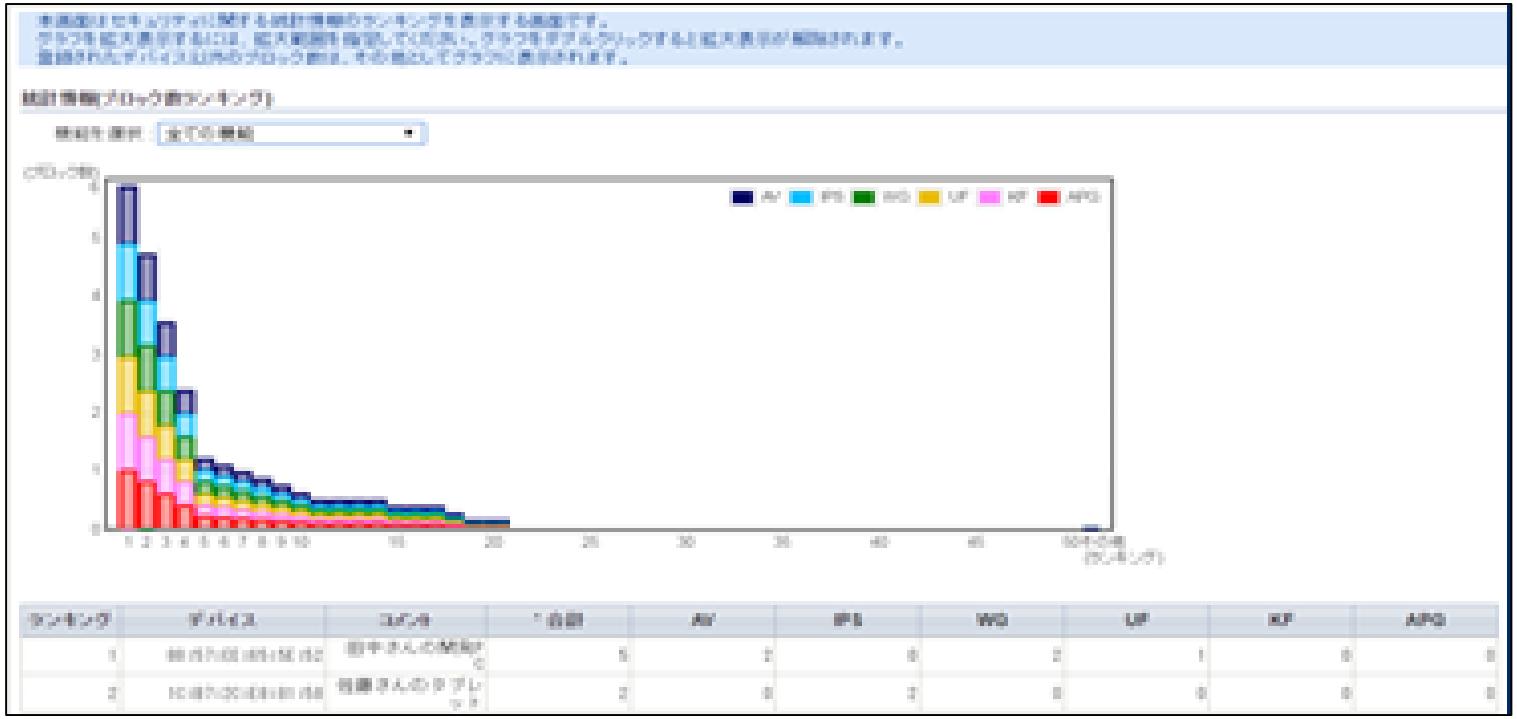
集計された期間を示します。
日表示の場合は、文字色で土日を示します。

補足情報：
・スキャンされ、かつ、ブロックされなかった通信は、脅威が検出されなかった通信です。

ブロック数グラフ機能

統計情報からデバイス毎のブロック数が多い順にグラフ表示できます。

- これによりデバイス毎の脅威に対するリスクを判断するのに役立てることができます。



月次レポート機能

毎月１日に、管理者宛てに統計情報、ファームウェア更新情報、ライセンス有効期限のレポートを作成して管理者宛てにメールで送信します。

- 本機能は、「メールでお知らせ」のメール送信機能の一部となっており、メール送信のための設定は共通となっております。

「メールでお知らせ」の設定の後、以下の画面にて、チェックを入れることで動作します。

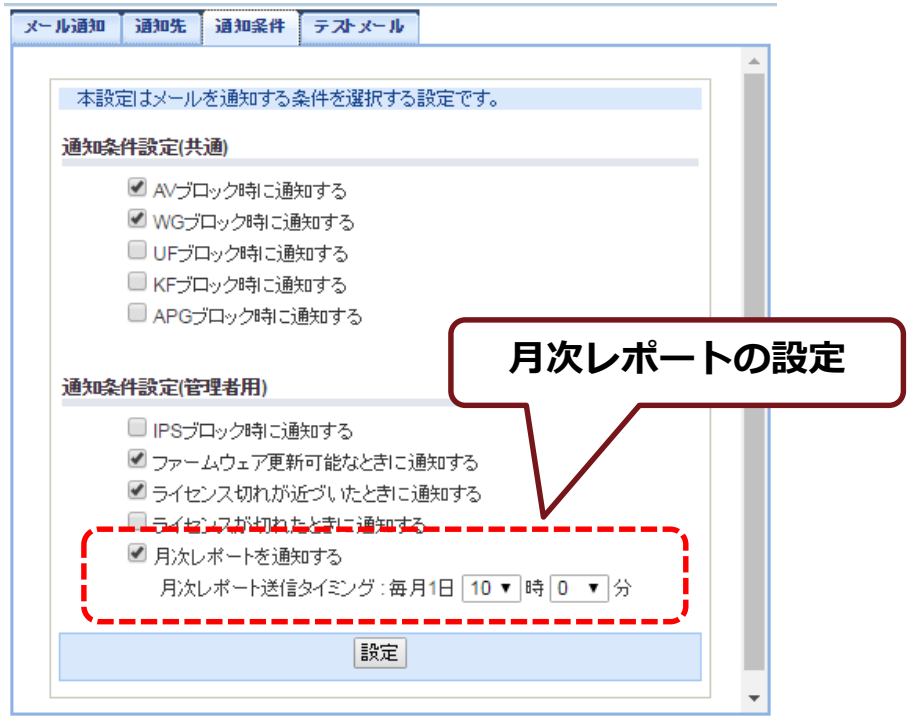
<送信されるレポートの記載内容イメージ>

件名：　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)

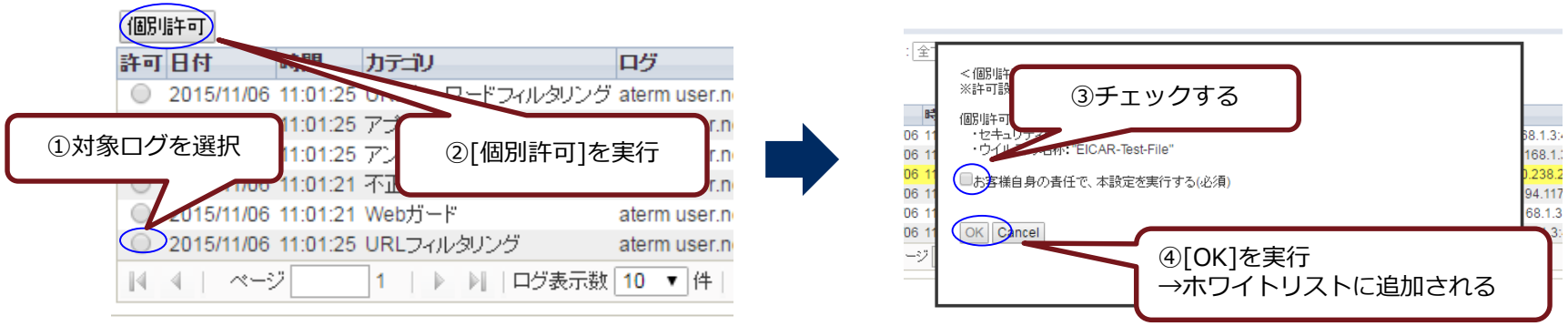
[ライセンス有効期限]
yyyy:mm:dd hh:mm:ss



ホワイトリスト機能

セキュリティログから、特定の対象に「個別許可設定」を行うことでホワイトリストに登録することが可能です。

- 例えば、URLフィルタで「アルコール飲料」のカテゴリをブロックに設定したが、一部のメーカのページ「だけ」は許可したいといった場合に、この画面からブロック対象外にすることができます。



- ホワイトリストとして登録できる対象は、URLフィルタ、アンチウィルス、Webガードで検出されたものとなります。
- 登録件数は以下の通りとなります。
  - URLフィルタ　：MAX　100件
  - アンチウィルス：MAX　10件
  - Ｗｅｂガード　：MAX　10件
- 登録したホワイトリストは各機能の「個別許可設定」画面にて編集可能です。

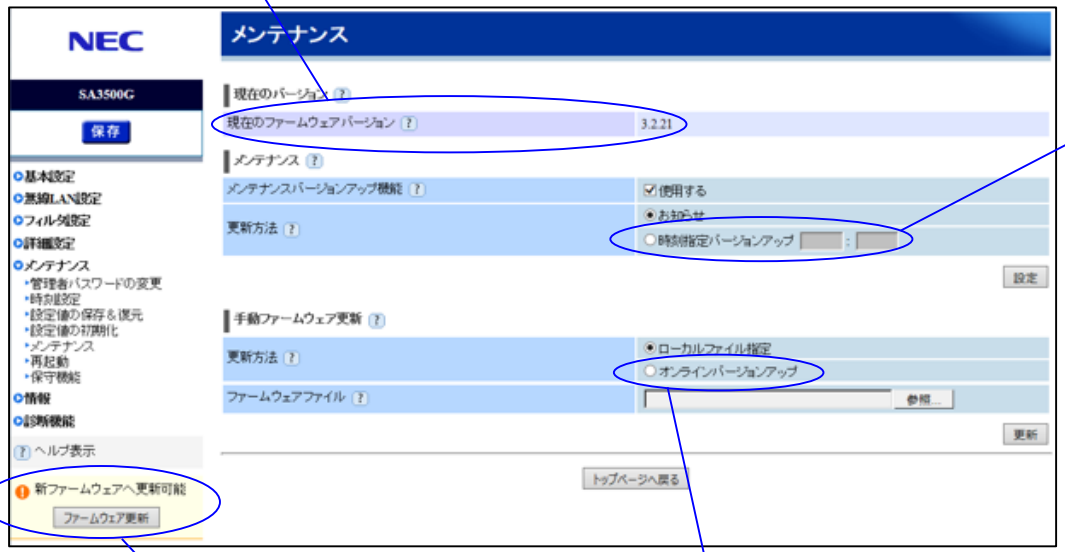
メンテナンス機能

メンテナンスバージョンアップ機能

- 設定Web画面から新しいファームウェアの確認やファームウェアの更新を行う事ができます。

①FWのバージョン情報が表示される

②「メンテナンスバージョンアップ機能」の「使用する」を選択
③「時刻指定バージョンアップ」を選択した場合は、指定時刻に自動的に[最新バージョン]のファームウェアに更新を行います。

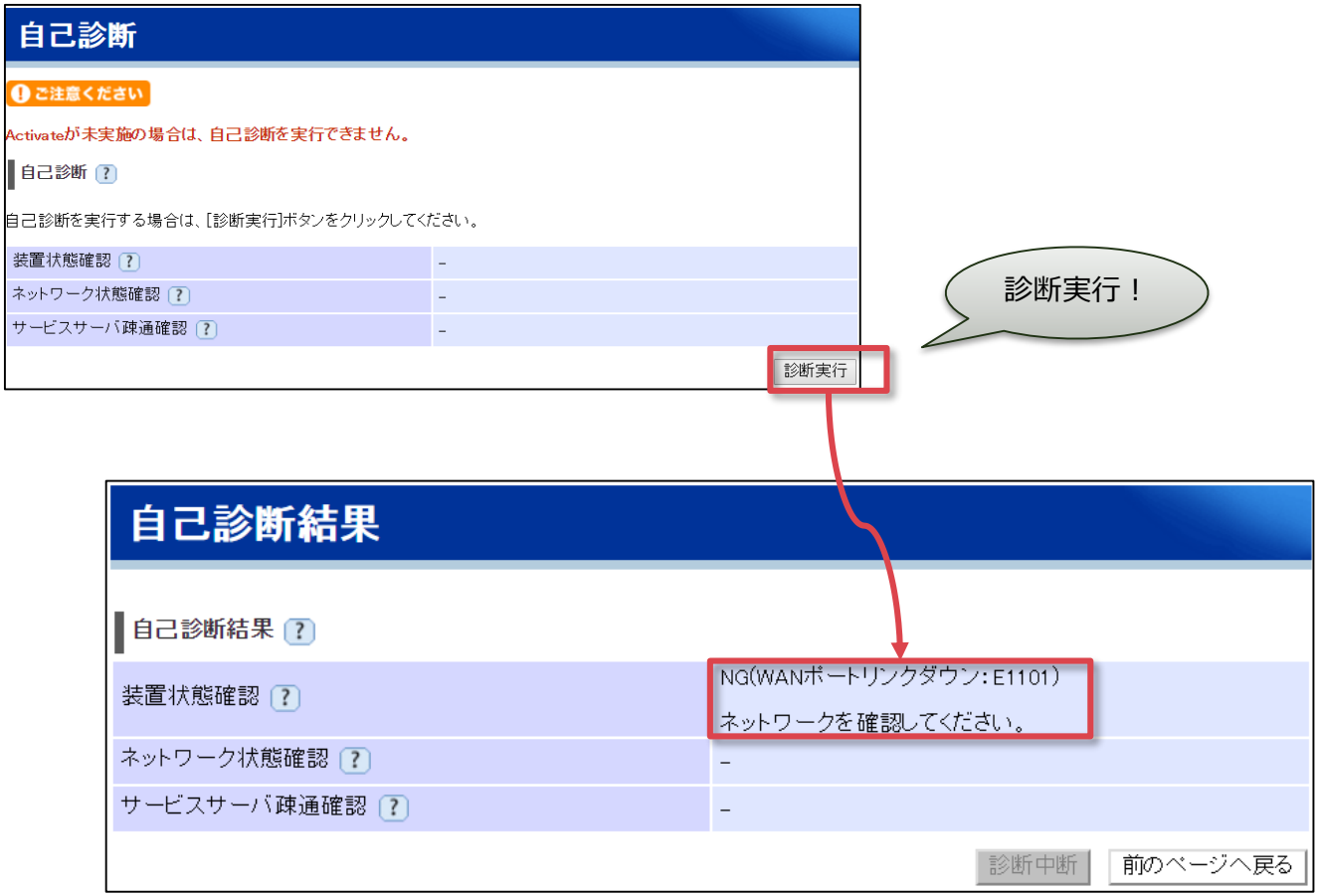


④「メンテナンスバージョンアップ機能」で「お知らせ」を選択してあると[最新バージョン]があるときにトップページやメンテナンスページの設定画面選択ウィンドウに更新のお知らせをします。

⑤オンラインバージョンアップを選択した場合は、手動で[最新バージョン]のファームウェアに更新することができます。

ネットワーク診断機能

- Etherポートのリンク状況など装置の状態、ネットワークの状態、サービスサーバとの接続状態の自己診断が可能です。



パケットフィルタ機能

- 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。
  本機能はブリッジモードとルータモード共通の機能です。

IPv4パケットフィルタエントリ

1~10 | 11~20 | 21~30 | 31~40 | 41~50

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	廃棄	out	UDP	any	any	any	137-139	編集	削除
2	廃棄	out	TCP	any	any	any	137-139	編集	削除
3	廃棄	out	UDP	any	any	any	445-445	編集	削除
4	廃棄	out	TCP	any	any	any	445	編集	削除
5	廃棄	out	TCP	any	any	any	2049	編集	削除
6	廃棄	out	UDP	any	any	any	2049	編集	削除
7	廃棄	out	TCP	any	any	any	1243	編集	削除
8	廃棄	out	TCP	any	any	any	12345	編集	削除
9	廃棄	out	TCP	any	any	any	27374	編集	削除
10	廃棄	out	TCP	any	any	any	31785	編集	削除

1~10 | 11~20 | 21~30 | 31~40 | 41~50

パケットフィルタエントリ編集

Entry No.	1
種別	通過 廃棄 拒否
フィルタタイプ	転送 送受信
方向	in out
プロトコル	IPすべて プロトコル番号 TCP FLAG 指定なし ack fin psh rst syn urg ICMP MESSAGE 指定なし TYPE CODE
送信元IPアドレス	any /
送信元ポート番号	any -
宛先IPアドレス	any /
宛先ポート番号	any -

設定 前のページへ戻る

MACアドレスフィルタリング機能

ＭＡＣアドレスフィルタリング

- ホワイトリスト形式で登録したMACアドレス以外の端末から、有線でのWAN側への転送及び、無線でのSA3500G（無線AP）への帰属を禁止することができます。

- MACアドレスフィルタリングは、有線LAN/無線LANそれぞれ個別にON/OFFが可能です。
- 登録可能なMACアドレスは、有線LAN/無線LANそれぞれ60個となります。

ポート通信速度固定設定機能

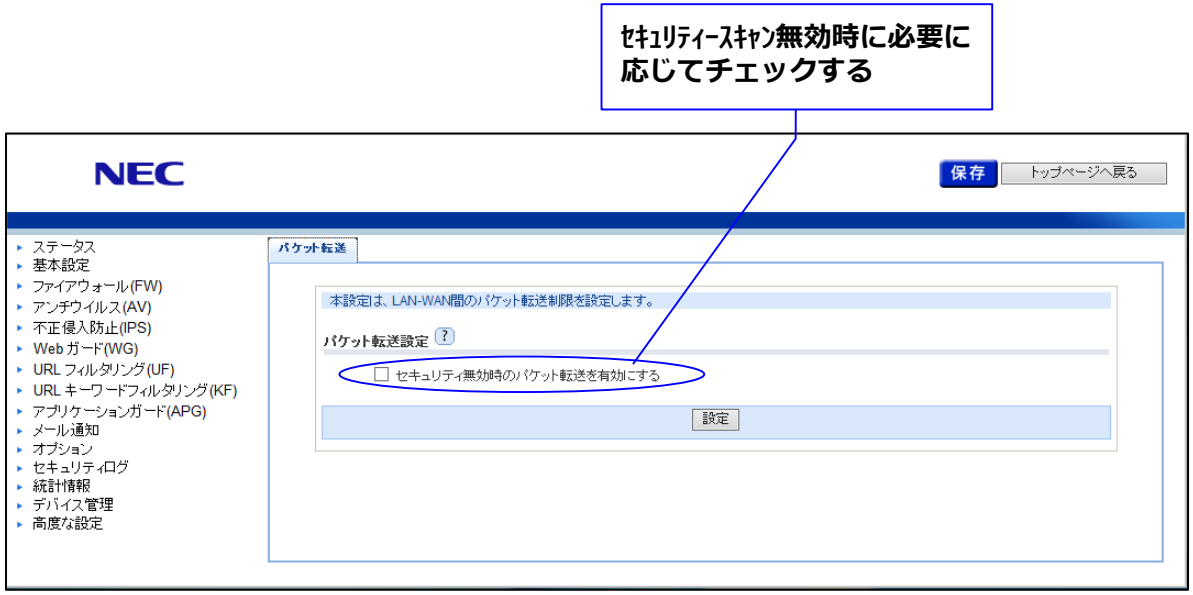
- Ethernetポートの通信速度/モードを固定できるように対応しました。

パケットスルー設定機能

ライセンス期間終了後などセキュリティースキャン無効時にLAN-WAN間のパケット転送を行う設定ができます。（デフォルトはOFFです）

(注)ライセンス期間中に本設定を有効にした場合、ライセンス期間終了時点でセキュリティースキャンが無効になった状態でもパケット転送を行います。

セキュリティー機能が無効になった事を知らずにご使用を続けることが無いよう、本機能のご利用時はライセンス終了日時を十分認識された上で自己責任でご利用ください。
(ライセンス終了後に自己責任でご利用されることを推奨します)



ネットワーク機能

ブリッジモード/ルータモード

本製品では、ブリッジモードとルータモードがあります。
それぞれのモードの仕様は下表のとおりです。

ブリッジモード

ブリッジ機能	トランスペアレントブリッジ

ルータモード

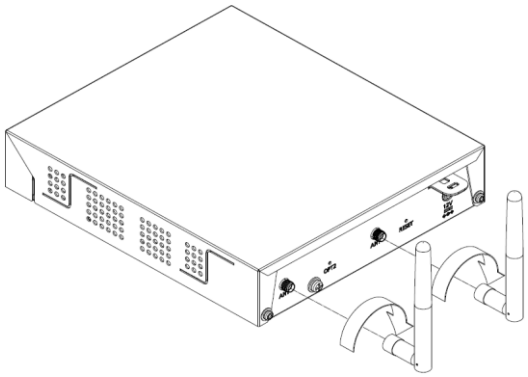
リンクレイヤ機能	PPPoEクライアント	：	セッション ※WANインタフェースは、PPPoEとIPoEで排他設定
ルーティング機能	IPv4	：	静的ルーティング(最大50件)
拡張機能	IPv4	：	DHCPサーバ（IPアドレスの払い出し：最大250件） DHCPクライアント プロキシDNS NAPT(無効設定可) IPsecパススルー NTPクライアント ポートマッピング(最大50件) ICMP Redirect, ホストルート ホームIPロケーション(Aterm独自機能)
IPsec/IKE	IPv4	：	IPsec(ESP), トンネルモード, post-fragment, IKEv1 IKEv2
	暗号化アルゴリズム	：	3DES, AES(128,192,256bit)
	認証アルゴリズム	：	MD5, SHA-1, SHA-2(256bit)
	対地数	：	1
SNMP	IPv4	：	SNMPv1, SNMPv2c (エージェント)
	標準MIB	：	MIB Ⅱ(RFC1213) ※PrivateMIBには対応していません。

無線LAN アクセスポイント機能

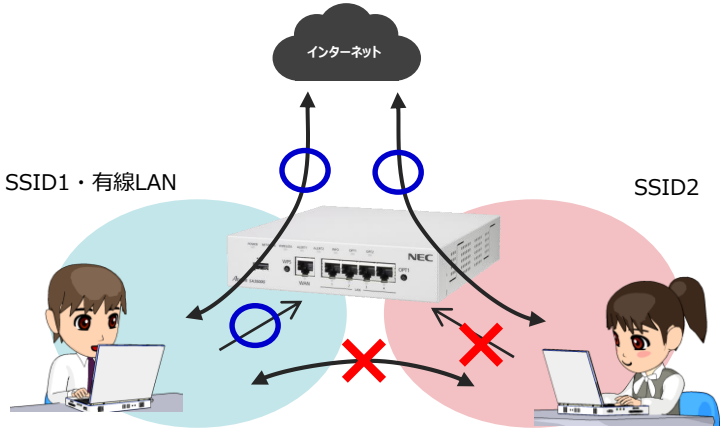
ルータモード/ブリッジモードでAP(アクセスポイント)として動作します。

- 仕様は下記のとおりです。

機能	詳細
802.11b/g/n	・2.4HGzサポート (5GHzは未サポート)
接続数	・max32台
SSID	・マルチSSID対応：2つ ・ステルス機能 ・ネットワーク分離機能 (※下記参照)
暗号化	・WPA(AES-PSK, TKIP-PSK) ・WPA2(AES-PSK, TKIP-PSK)
アンテナ切り替え	設定Webから、内蔵アンテナ、外付けアンテナで切り替え可能(初期は内蔵アンテナ)



外付けアンテナの取り付けイメージ

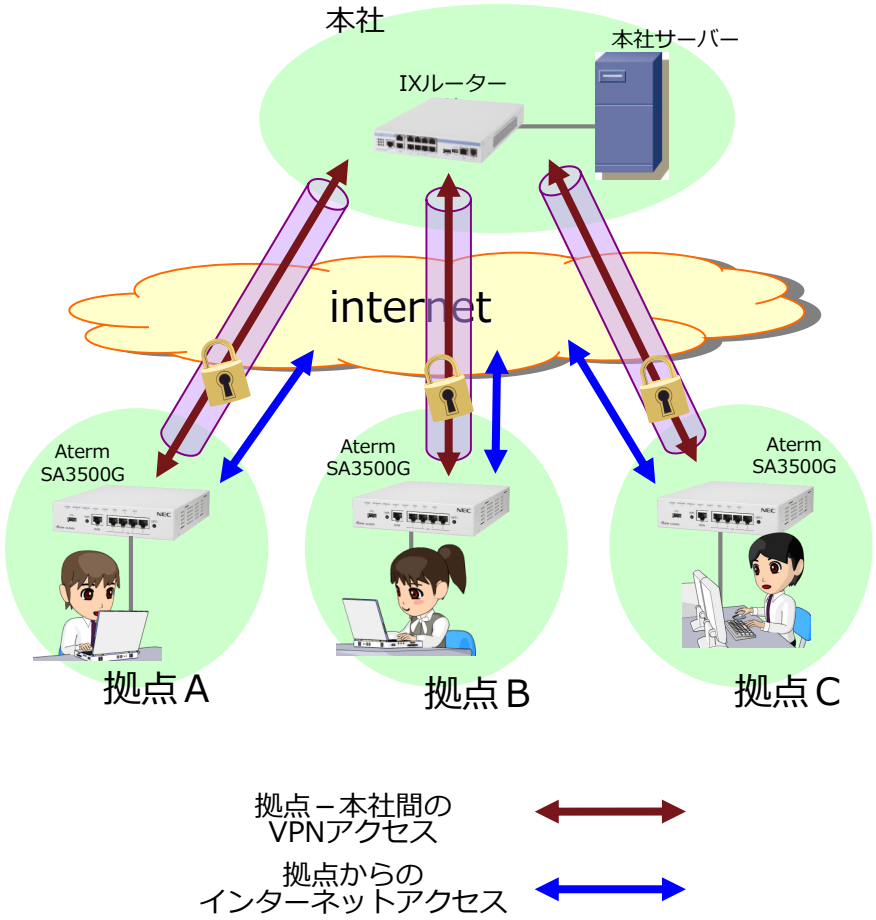


ネットワーク分離機能有効時の動作イメージ
(SSID2を分離した場合)

VPN機能

ルータモードにて1対地のIPsec通信のVPNを構成する事ができます。

- 本社側でIXシリーズのように複数のIPSec通信のできる装置を設置することで、本社-拠点間をスター型のＶＰＮ構成をとることが可能です。



機能		
IPSec	スループット	約20Mbps
	モード	Tunnel Mode
	セキュリティプロトコル	ESP
	暗号化アルゴリズム	3DES, AES-128, AES-192, AES-256
	認証アルゴリズム	HMAC-MD5-96, HMAC-SHA-1-96, HMAC-SHA2-256-128
	PFS (Perfect Forward Secrecy)	DHグループ1(768), DHグループ2(1024), DHグループ5(1536), DHグループ14(2048)
	フラグメント方式	post-fragment
	SA	認証：local-id, remote-id設定ライフタイム、リキータイミング
IKE	鍵交換方式	自動鍵 (鍵交換プロトコル)　IKEv1/IKEv2
	交換タイプ	IKEv1:Main／Aggressive／Quick Mode
	ISKMP SA – IPsec SAの依存関係	IKEv1:Continuous-channel SA
	認証方式	Pre-Shared Key,IKEv2:電子証明書(EAP-MD5)
	暗号化アルゴリズム	3DES, AES-128, AES-192, AES-256
	認証アルゴリズム	HMAC-MD5, HMAC-SHA-1, HMAC-SHA2-256
	DHグループ (Diffie-Hellman)	DHグループ1(768), DHグループ2(1024), DHグループ5(1536), DHグループ14(2048)
	SA	認証：local-id, remote-id設定 , ライフタイム、リキータイミング
	ソースアドレス指定	固定設定
	対地数	1

⑤サポート情報

サポート窓口

お客様・販売店様からのお問い合わせについて

- 本製品の機能・操作・設定・故障診断などのお問い合わせを以下にて受け付けております。

Aterm Biz(エータームビズ)インフォメーションセンター

ナビダイヤル：0570-025225　（携帯電話からも同一番号）

受付時間： 9:00～12:00、13:00～17:00
（月～金曜日のみ　祝日、年末年始、当社の休日、システムメンテナンス時を除く）

※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。
※通話料はお客様のご負担となります。

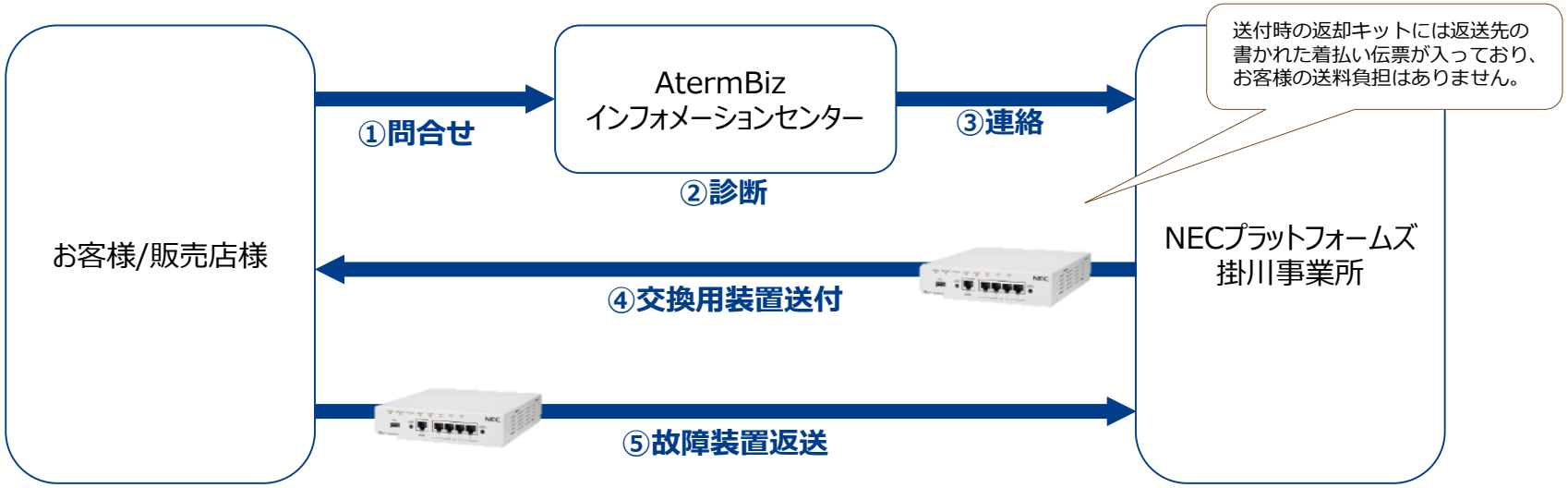
製品添付の取扱説明書や、カタログ、Webなどで案内されています。

- 基本保守（先出しセンドバッグ）の対応もこちらで行っております。

基本保守のご紹介

故障については、基本保守対象期間中、先出しセンドバッグの基本保守サービスを提供します。このサービス費用は製品価格に含まれています。（追加ライセンスにも適用されます）

- 実際の手続きは、NECプラットフォームズが運営するコールセンター「AtermBizインフォメーションセンター」にお電話いただき、下記のようなフローで行ないます。



基本保守対象期間について

- 使用開始から、ライセンス分の年数の期間受けられます。
  追加ライセンスによりライセンスを追加した場合は、その期間分も基本保守の対象となります。
- 使用開始とは本製品をアクティベーションした時点もしくは、納入後31日経過した時点の早い日を示します。
  故障交換で本製品が交換された場合は、交換前の製品の使用開始情報が引き継がれます。
- お客様が本製品のご利用を中止した場合、ライセンス期間満了以前であっても、お支払いいただいた料金は返金いたしません。


Orchestrating a brighter world
NEC