主要諸元

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 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)		管理画面からのアンテナ切り替え選択 WPSは有効 / 無効設定可能
	IEEE802.11n	周波数帯域 / チャネル	2.4GHz(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(2400～2484MHz)/1～13ch	
		伝送速度	54/48/36/24/18/12/9/6Mbps	
	IEEE802.11b	周波数帯域 / チャネル	2.4GHz(2400～2484MHz)/1～13ch	
		伝送速度	11/5.5/2/1Mbps	
USB インタフェース ・バージョンアップにより対応(無償)※	物理インタフェース	タイプ A コネクタ		
	ポート数	1 ポート		
	タイプ	USB 2.0		
電源		AC100V ±10% 50/60Hz±5% (AC アダプタ)		
動作保証環境		温度：0 ～ 40℃、湿度：10 ～ 90%		結露しないこと
保管条件		温度：-20℃～ 60℃、湿度：90%以下		結露しないこと
消費電力		35VA (21W) 以下		
発熱量		75.9kJ/h=18.1kcal/h 以下		
外形寸法		約 174 (W) ×195 (D) ×40 (H) mm		突起部／スタンド除く
EMI		VCCI Class B		
本体質量		0.9kg 以下		スタンド、ネジ、ゴム足を除く
冷却方式		自然空冷 (ファンレス)		
添付品		取扱説明書／ Ethernet ケーブル／ AC アダプタ／電源コード／スタンド／ゴム足 (4 個)／スタンド固定ネジ (1 個)		
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) が必要です

※2018 年 4 月時点では非対応です。

	品名	希望小売価格(税別)
本体	Aterm SA3500G(1年ライセンス付)	198,000円
	Aterm SA3500G(5年ライセンス付)	738,000円
	Aterm SA3500G(6年ライセンス付)	848,000円
	Aterm SA3500G(7年ライセンス付)	958,000円

	品名	希望小売価格(税別)
ライセンスパック	Aterm SA3500G追加ライセンス(1年)	150,000円

※本製品は 1 年、5 年、6 年のライセンス付き製品に対して 1 年間 (365日) のライセンスを追加するものです。
(製品本体のライセンスと合計して7年まで 1 年ごとに追加可能ですが、ライセンスが切れる前に追加が必要です)

	品名	希望小売価格(税別)
オプション	壁掛けキット	8,000円
	外付けアンテナ(2本1組)	10,000円

環境配慮基準

RoHS指令 準拠

EU加盟国で2011 年6月に公布された環境基準「改正RoHS指令」。本製品は鉛、水銀、カドミウム、六価クロム、ポリ臭化ビフェニール、ポリ臭化ジフェニルエーテルの使用を禁止する改正RoHS指令 (Restriction of the use of certain Hazardous Substances in electrical and electronic equipment) に適合しています。

■無線LAN製品ご使用時におけるセキュリティに関するご注意

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

●通信内容を盗み見られる：悪意ある第三者が、電波を故意に傍受し、IDやパスワードまたはクレジットカード番号等の個人情報、メールの内容等の通信内容を盗み見られる可能性があります。
●不正に侵入される：悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、個人情報や機密情報を取り出す (情報漏洩)、特定の人物になりすまして通信し、不正な情報を流す (なりすまし)、傍受した通信内容を書き換えて発信する (改ざん)、コンピュータウィルス等を流しデータやシステムを破壊する (破壊) などの行為をされてしまう可能性があります。
◎本来、無線LANカードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線LAN 製品のセキュリティに関する設定を行って製品を使用することで、その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十分理解したうえで、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勧めします。
◎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いっさい負いかねますのであらかじめご了承ください。

■無線LAN製品の使用環境に関するご注意

・電話機やテレビ、ラジオ、BS/CSチューナー等無線機器の近くで使用すると、双方に影響が出たり、正常に動作しない場合があります。・自動ドアや火災報知器など自動制御機器の周辺、および病院内や航空機内など電子機器、無線機器の使用が禁止されている区域では使用しないでください。機器の電子回路に影響を与え、誤作動や事故の原因となる恐れがあります。・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。・補聴器を装着されている方は、補聴器にノイズなどを引き起こす可能性がありますのでご注意ください。・第三者により故意に通信内容を傍受されることがあります。・障害物などの陰で電波の弱い場所や電波の届かない場所ではご使用になれません。・使用中に電波状態が悪い場所へ移動した場合に通信が途切れたり、伝送エラーになる場合があります。・本製品と同じ無線周波数を使用する他の無線機器を同時に使用すると、転送速度の低下や伝送エラーが発生し、正常に動作しないことがあります。・無線機器を搭載した装置の内部を改造することは法律で禁止されています。・本製品は、電波法に基づく小電力データ通信システムの無線局の無線設備として技術基準適合証明を受けています。したがって、本製品を使用するときに無線局の免許は必要ありません。

■電波に関する注意事項

●本製品は、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等の産業・科学・医療機器のほか、他の同種無線局、工場の製造ライン等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、アマチュア無線局等 (以下「他の無線局」と略す) が運用されています。

2.4DS/0F4

(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 (電波の発射を停止) 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、Aterm Biz (エーターム ビズ) インフォメーションセンターまでお問い合わせください。

■メンテナンスバージョンアップ機能に関するご注意

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が発生したり、パケット通信量超過による速度制限が発生する場合があります。本機能に関して許諾いただけない場合は、機能を無効にすることができます。ただし、本機能を無効にした場合、セキュリティ上の不具合を改善するような重要なソフトウェアの更新であっても、自動的にバージョンアップは行いません。改善前のソフトウェアをそのまま使用し続ける場合、悪意のある第三者から不正なアクセスをされる危険が残る可能性があります。

⚠ 安全上のご注意

● 正しく安全にお使いいただくために、ご利用の前には必ず取扱説明書をよくお読みください。
● 水、湿気、湯気、ほこり、油煙等の多い場所に設置しないでください。火災、感電、故障などの原因となります。

●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装置ですが、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。●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。●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、工場出荷初期値ではインターネットへの接続はできなくなります。●本製品に多くのトラフィック負荷がかかると、回線速度が低下する場合がありますのでご注意ください。●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。また、米国再輸出規制 (Export Administration Regulations) の適用を受ける場合があります。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には、本製品の販売元にご相談ください。●本製品の故障・誤動作または不具合により、通信などにおいて利用の機会を逸したために発生した損害、および通信料金等付随の損害について、当社は一切その責任を負いかねますのでご了承ください。●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等は行っておりません。

製品の最新情報を下記で提供しています。

製品情報サイト：
www.necplatforms.co.jp/product/security_ap/

お問い合わせは、下記へ

本製品の機能、操作、設定、故障診断などのお問い合わせ
本製品専用窓口 **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です) 通話料はお客様ご負担です。

受付時間 9:00～12:00、13:00～17:00 (月～金曜日のみ)
※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。
※土・日曜日、祝日、年末年始、当社の休日、システムメンテナンス時はお休みさせていただきます。
※本紙に掲載された製品の専用窓口です。

UD FONT 見やすいユニバーサルデザインフォントを採用しています。

VEGETABLE OIL INK 環境にやさしい植物油インキを使用しています。

NECプラットフォームズ株式会社 〒101-8532 東京都千代田区神田司町二丁目3

2018年4月現在

Cat.No. PAB001 180420004MM

2018年4月
Aterm Biz シリーズ

\Orchestrating a brighter world NEC

社内ネットワークとインターネット間のトラフィックを監視してセキュリティ対策に貢献
セキュリティアプライアンス

Aterm® SA3500G

優れたコストパフォーマンスで、安心できるネットワーク環境を構築。導入・運用が簡単に行えるSOHO/SMB向けセキュリティアプライアンス

ネットワークのセキュリティ対策はお済みですか？

最近のサイバー攻撃は高度化しており、もはや会社の情報資産はパソコンのウイルス対策ソフトや既存のファイアウォールだけでは守れません。
また近年は、無差別で金銭搾取を目的とした「ばらまき型」のメール攻撃が手段としてあらわれ、企業の規模に関係なくサイバー攻撃の標的になり得ます。

ネットワークの脅威はサイバー攻撃だけではありません。会社のインターネット環境は、業務を遂行するために必須であったり、アライアンス先や顧客とのコミュニケーションに活用する、様々な調べものを行うなど、現代の会社にはなくてはならないものとなっています。
一方、業務に関係ないサイトへのアクセスや、SNSサイトへの書き込みやストレージサービスの利用などは会社にとっては必ずしも有益とは限りません。適切に利用しないと、モラルや生産性の低下だけではなく、情報の漏えいによる社会的信用の喪失など会社の存続さえ脅かすリスクがあります。

このような背景から複数のセキュリティ対策機能を搭載した、統合セキュリティアプライアンスが注目されています。

Aterm SA3500Gとは

Aterm SA3500Gは、ネットワークの入口に設置するだけで、インターネットからの不正侵入防止や社員が誤って危険なサイトにアクセスすることを防止、送受信するメールに添付されたファイルやWebからのダウンロードファイルに含まれたウイルスなどを検知・無害化する等、複数のセキュリティ機能を1つにまとめ、様々なサイバー攻撃の脅威から自社のネットワークを守る、統合セキュリティアプライアンスです。

Aterm SA3500Gの特長

簡単設置（ブリッジモード）

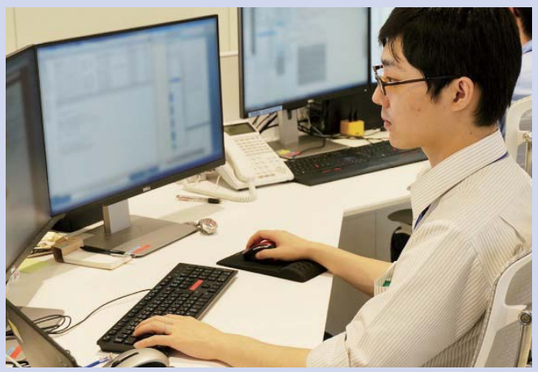
Aterm SA3500Gは、ブリッジモード(初期設定)が利用でき、既存の社内ネットワークの構成を変えることなく、導入することができます。また設定もWebブラウザを用いたシンプルでわかりやすいGUIで行うことができます。

高速セキュリティエンジン

Aterm SA3500Gは、高速セキュリティエンジンを採用することで、セキュリティ機能が有効な状態でも、約700Mbps*の高スループットを実現しています。 ＊当社の試験環境にて測定した結果です。

日本に合った安全対策を提供

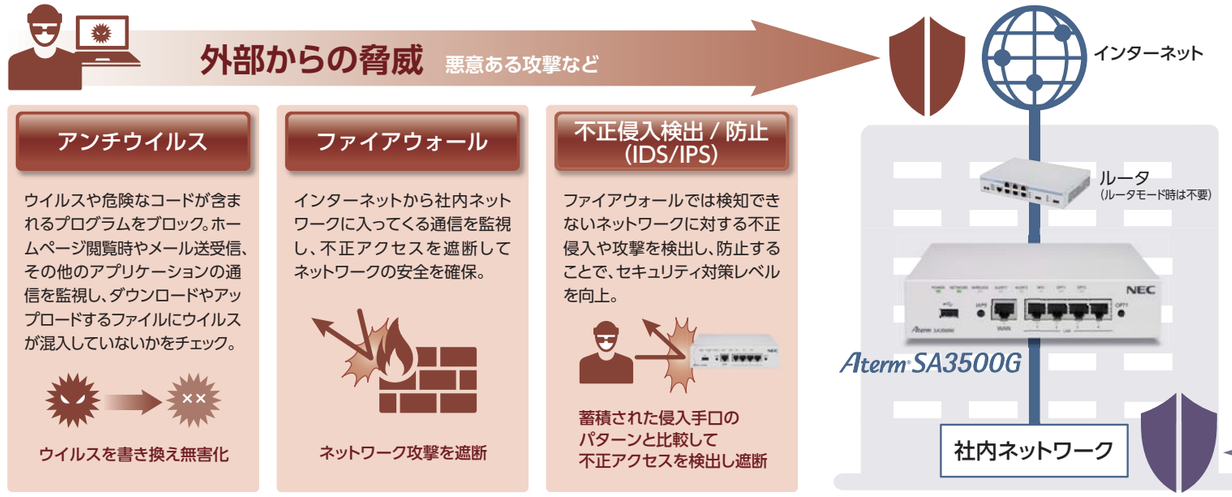
株式会社ラックとパートナー契約を締結し、同社が提供するシグネチャ（攻撃を識別するための情報）を採用しています。 同社は、グローバルなサイバー攻撃情報を収集するだけでなく、日本の最新情報も加えて解析を行うことで、より日本のネットワーク環境に合ったシグネチャを提供しています。
SA3500Gは、この最新のシグネチャをライセンス期間中（1年間/5年間/6年間/7年間）、定期的に自動更新して提供しており、安全にネットワークを利用できる環境を実現しています。 このシグネチャは、「JSIG」と呼ばれ、ラック社のセキュリティアナリスト・セキュリティエンジニアが24時間365日の監視・運用体制で運営されている「JSOC」にて収集・解析された情報に基づき作成されています。



株式会社ラックについて

サイバーセキュリティ分野のリーディングカンパニーとして、業界屈指のセキュリティ技術を駆使し、セキュリティ対策に必要な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。　https://www.lac.co.jp

セキュリティ機能



※これらの機能をご利用される場合は、設置後に設定が必要です。

Web ガード

最新のシグネチャによりフィッシングやウイルス感染を起こすなどの危険なサイトへのアクセスをガード。

危険なWebサイトへのアクセスをブロック

URLキーワードフィルタリング※

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

キーワードが入ったURLをを検出するとアクセスをブロック

URLフィルタリング※

あらかじめ用意されているWebサイトのカテゴリーを指定することで閲覧の制限が可能です。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。

指定されたカテゴリに属するWebサイトへのアクセスをブロック

アプリケーションガード※

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、社外の人との情報交換可能なアプリケーションの利用を制限可能。

制限したいアプリケーションを事前に設定することで通信をブロック

うっかりミスやコンプライアンス違反など **内部からの脅威**

運用が容易なユーザインターフェース

簡単初期設定ウィザード

初期設定はウィザード形式で画面の指示に従い、わずかなステップの設定を行うだけで完了します。脅威防御のためのセキュリティ機能は初期状態で有効になっています。

わかりやすい設定画面

機能毎に設定項目をまとめており、目的の設定まで直観的にたどり着けます。わかりにくい項目は補足説明をヘルプ表示できる親切設計で、日々の運用管理にも専門知識は不要です。複雑なコマンドラインによる設定は一切なく、全ての機能を左記の管理画面上で設定できます。

豊富なお知らせ機能

お知らせ機能

脅威を検出した場合や処置が必要な場合には、いろいろな方法でお知らせできます。

- Webアクセス系の脅威防止時はブラウザ上に表示(警告メッセージはカスタマイズ可能)
- 本体ランプでの表示
- 外部機器(別売)での表示:Aspire UXの多機能電話機、パトライト社対応機器でランプ表示
- メールでの通知:管理者向け通知(最大3宛先)、利用者向け通知(最大50宛先)

対応パトライト型番
・NHS-FV1/NHP-FV1/NHL-FV1
・NHS-FB1/NHP-FB1/NHL-FB1
・PHN-3FBE1

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)との連携により、脅威検出状態・新しいファームウェアの有無・ライセンスの有効期限をお手元の電話機で確認することができます。

- 脅威検出の有無を情報表示します。
- 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(Webガード機能もしくはアンチウイルス機能)を表示します。

※UNIVERGE Aspire UX 連携機能のご利用には 5th エンハンス以降のファームウェアを搭載した Aspire UX 本体が必要です。
特別なオプションは必要ありません。

ネットワークセキュリティの見える化

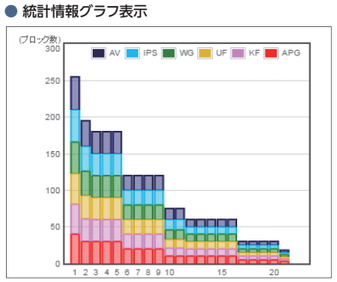
統計機能

Aterm SA3500G では、セキュリティ機能毎にスキャンした通信の件数、脅威を検出してブロックした件数を統計情報として確認することができます。脅威検出の件数を、自社の脅威リスクの大きさを捉えるひとつの指標としてご活用いただけます。

● 統計情報(日/週/月で表示可能)

集計期間	AV		IPS		
	スキャン	ブロック	スキャン	ブロック	スキ
2018/03/30	16	0	7,921	1	2
2018/03/29	1,175	464	9,288	1	2
2018/03/28	0	0	7,196	0	
2018/03/27	87	1	5,277	0	1
2018/03/26	0	0	2,826	0	
2018/03/25	0	0	3,851	0	
2018/03/24	0	0	4,308	0	1
2018/03/23	0	0	4,005	0	1
2018/03/22	0	0	3,471	0	1
2018/03/21	0	0	1,952	0	

● 統計情報グラフ表示



月次レポート(メール通知)

毎月1日に前月分の統計情報を管理者メールアドレス宛に発信することができます。

```
[ 統計情報]
 AV:0/100
 IPS:0/100
 WG:0/100
 UF:50/100
 KF:20/100
 APG:10/100

[ アクセス情報]
<UFカテゴリ( 上位5カテゴリ)>
No  カテゴリ                    アクセス数  過去平均  ブロック数
--  --------------------------  ----------  --------  ----------
1   ニュース、メディア                1000       800           0
2   ブログ、個人サイト                 900       300           0
3   スポーツ                           400       500         400
4   コンピューター、IT                 300       600           0
5   ギャンブル、宝くじ                 200        20           0

<アプリケーション( 上位5アプリケーション)>
No  アプリケーション            アクセス数  過去平均  ブロック数
--  --------------------------  ----------  --------  ----------
1   xxxxx Drive ( FileTransfer )      1000       800           0
2   xxxxx.com ( DataFlow )             900       300         900
3   xxxxx for Buisiness ( Login/Me     400       500           0
4   ○○アプリ                          300       600         300
5   ○○乗換案内                        200        20           0
```

インターネットアクセスの見える化

各セキュリティ・スキャン機能※で“ログのみ”とすることで、インターネットのアクセス利用を可視化できます。 ※ファイアウォール機能を除く

カテゴリ	ブロック	ログのみ	許可
ポルノ / Pornography	○	●	○
アダルトサイト / Nudity and Potentially Adult Content	○	●	○
ギャンブル、宝くじ / Gambling and Lottery	○	●	○

#	アプリケーションID	アプリケーション名	カテゴリ	ブロック	ログのみ	許可
1	1070_06	Google Mail (DataFlow)	Mail	○	●	○
228	1467_22	LINE (Audio/Video)	IM	○	●	○
229	2359_06	Skype (DataFlow)	IM	○	●	○
292	0131_06	Amazon Shopping (DataFlow)	Shopping	○	●	○
293	0156_06	ヤフオク! (DataFlow)	Shopping	○	●	○
294	0711_06	eBay (DataFlow)	Shopping	○	●	○

URLフィルタリングの各Webカテゴリ、アプリケーションリスト毎のアクセス数の月間累計値を確認できます。

No.	カテゴリ	アクセス数	過去平均	ブロック数
1	コンピューター、IT / Computers and Information Technology	11,915	0	0
2	エンターテインメント、芸術 / Entertainment and Arts	4,878	0	0
3	ポータル、検索サイト / Portals and Search Engines	4,298	0	0
4	広告 / Advertisments and Pop-Ups	1,887	0	0
5	コンテンツ配信サーバー / Content Delivery Network	1,617	0	0
6	ポルノ / Pornography	1,286	0	1,286
7	ショッピング、オークション / Shopping and Auction	780	0	0
8	飲食物 / Food and Drink	739	0	0

Step 1 見える化機能で現状把握
業務に関係ないサイトのアクセスが多い、ファイル共有系のアプリが利用されている、といったことが把握できます。

Step 2 “ブロック”指定で内部統制
- 明らかに業務に関係ないWebカテゴリのサイトアクセスを防止
- 情報漏えいリスクのあるアプリケーションの通信をブロック

ネットワークの見える化

デバイス管理機能

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

#	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	00:00:00:00:00:01	192.168.10.250	Windows 7	事務PC(畑さん)	hata@aa.bb.jp		通知	収集	参照	クリア
2	00:00:00:00:00:02	192.168.10.20	iPhone	iPhone(佐藤携帯	sato@mobile.bb.jp		通知	収集	参照	クリア
3	00:00:00:00:00:03	192.168.10.12	Windows 10	事務PC(細田さん)	Hosoda@aa.bb.jp		通知	収集	参照	クリア
4	00:00:00:00:00:04	192.168.10.5	Windows 10	開発PC(坂口さん)	Sakaguchi@aa.bb.j		通知	収集	参照	クリア

<確認できる情報>
- MACアドレス/IPアドレス
- OS等の情報
- 接続方法(有線または無線)

<各端末に設定できる情報>
- 端末ごとのコメント(名称など)
- メール通知先のアドレスと通知有無
- 個別統計情報の収集(最大50台)

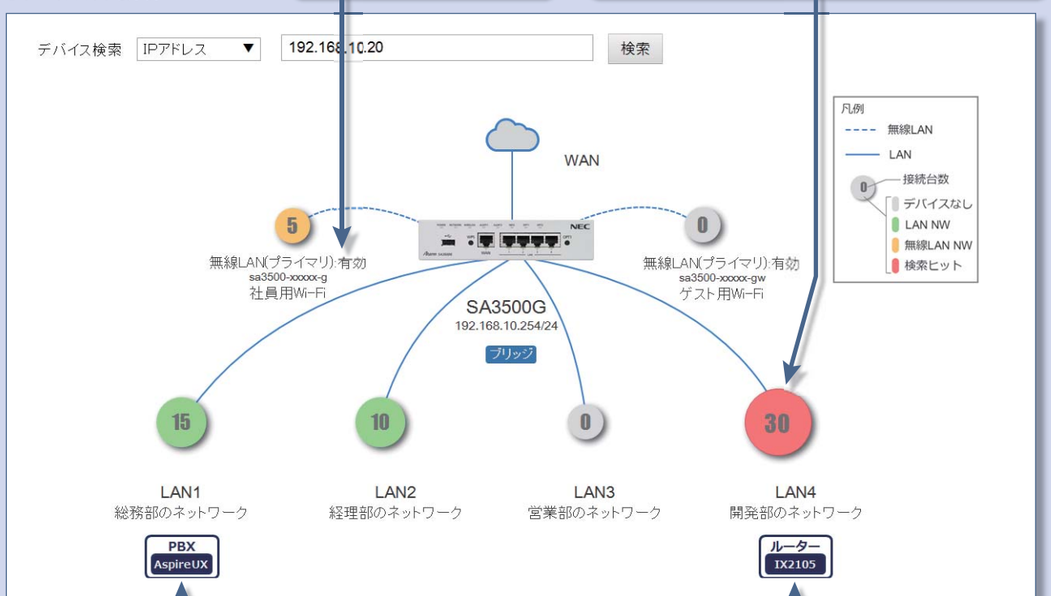
デバイスマップ機能

Aterm SA3500G に接続されたデバイスを
視覚的に管理できます。

各サークルは接続されたデバイスの数を示しています。
クリックすると接続されたデバイスの一覧を表示します。

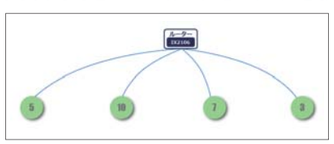
各インタフェースごとに
名前をつけることが可能です。

● デバイスマップ表示例



【Aspire UX 連携】
Aspire UXの主装置を検出すると、アイコン表示。
クリックで収容されているIP電話機の一覧を表示します。

【UNIVERGE IX/WAシリーズ連携】
IX/WAシリーズを検出するとアイコン表示。
クリックするとIX/WAルータ配下の階層を展開して表示します。



※本機能でアイコン表示が可能な機種は製品情報サイトをご覧ください。

Point ▶

社内ネットワークの構成を見える化

社内のネットワーク内のPCやスマートデバイスなどをAterm SA3500Gの管理画面上で確認することができるため、今まで把握できていなかった社内ネットワークの機器構成が見える化します。専任管理者がいない場合や、追加投資の検討の際にも活用でき、管理効率の向上や負担の軽減が期待できます。

安心の接続環境構築

簡易RADIUS機能

IEEE802.1X認証で必要な認証サーバとして、Aterm SA3500Gをご活用頂けます。
無線LANデバイスの接続に際し、認証を設けることで、不正なデバイスの接続を防ぐことが可能になります。

- SA3500Gの内蔵無線LANは、この簡易RADIUS機能と連携するIEEE802.1X認証に対応しています。
- ユーザーIDとパスワードによる認証・クライアント証明書による認証をサポート。
- クライアント証明書の発行は、1ユーザにつき、最大2つまでの発行が可能です。
- 登録可能なユーザ数は200、接続可能なIEEE802.1X認証機器は20台までとなります。

ネットワーク機能

Aterm SA3500Gは動作モードとしてブリッジモードとルータモードがあり、それぞれのモードの仕様は以下の通りです。

ブリッジモード

項 目	仕 様	
ブリッジ機能	トランスペアレントブリッジ	
無線LAN アクセスポイント 機能	規格	IEEE802.11b/g/n(2.4GHz)
	SSID	マルチSSID(2つ)、ステルス機能
	暗号化	WPA(AES-PSK、TKIP-PSK)、WPA2(AES-PSK、TKIP-PSK)、WPA/WPA2-PSK(AES、TKIP)、IEEE802.1X(EAP)
	アンテナ	内蔵アンテナ、外付けアンテナ(オプション)

ルータモード

項 目	仕 様	
リンクレイヤ機能	PPPoEクライアント	1セッション※1
拡張機能	IPv4	DHCPサーバ※2、DHCPクライアント、プロキシDNS、NAPT、SNTPクライアント、ポートマッピング(最大50件)、ICMP Redirect、静的ルーティング(最大50件)、ホームIPロケーション※3
無線LAN アクセスポイント 機能	規格	IEEE802.11b/g/n(2.4GHz)
	SSID	マルチSSID(2つ)、ステルス機能
	暗号化	WPA(AES-PSK、TKIP-PSK)、WPA2(AES-PSK、TKIP-PSK)、WPA/WPA2-PSK(AES、TKIP)、IEEE802.1X(EAP)
	アンテナ	内蔵アンテナ、外付けアンテナ(オプション)
IPsec/IKE	IPv4	IPsec(ESP)、トンネルモード、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
	対地数	1
SNMP	IPv4	SNMPv1、SNMPv2c(エージェント)
	標準MIB	MIB Ⅱ(RFC1213)※4

※1：WANインタフェースは、PPPoEとIPoEで排他設定。
※2：ルータモードでのDHCPのIPアドレス払出し数は最大250件です。
※3：Aterm 独自機能（本装置でグローバルIPを取得時、DNSサーバに本装置のFQDNを登録する機能）
※4：PrivateMIBはありません。

クラウドサービス接続

クラウドサービスへの接続を容易に行える専用の設定画面をご用意。
接続するクラウドサービスを選択することで、対象サービスへの接続に必要な設定項目のみが表示され、カンタンに情報を入力できます。

以下のクラウドサービスに対応しています。
- Amazon Web Services(AWS)
- Microsoft Azure

※AWS、Amazon Web Servicesは、米国その他の諸国における、Amazon.com, Inc.またはその関連会社の商標です。
※Microsoft Azureは、米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。

MACアドレスフィルタリング機能

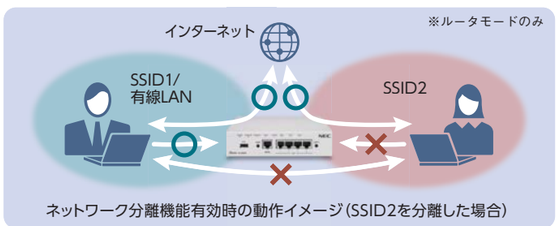
ホワイトリスト形式で登録したMACアドレス以外の端末から、有線でWAN側への転送及び、無線でのAterm SA3500G(無線LAN機能)への帰属を禁止できます。

- 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それぞれ最大60個です。

無線LAN機能

無線LANアクセスポイントとしても同時に動作可能です。

無線LAN機能ではマルチSSIDによりネットワークの分離機能を有しています。



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)