

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)
	ポート数	1 ポート
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)
	ポート数	4 ポート
無線 LAN インタフェース	タイプ	1000BASE-T/100BASE-TX Auto MDI/MDI-X
	アンテナ	内蔵アンテナ、外付けアンテナ (オプション)
	IEEE802.11n	周波数帯域 / チャンネル 2.4GHz (2400~2484MHz) / 1~13ch 伝送速度 最大 300Mbps (HT40 の場合)
	IEEE802.11g	周波数帯域 / チャンネル 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 / チャンネル 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 ポート数 タイプ
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	
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、壁掛けキットが必要です

※2017 年 2 月時点では非対応です。

品名	型番	希望小売価格 (税別)	品名	型番	希望小売価格 (税別)
Aterm SA3500G(1年ライセンス付)	ZA-SA3500G/1	198,000円	Aterm SA3500G追加ライセンス(1年)	ZA-SA/LA1	150,000円
Aterm SA3500G(5年ライセンス付)	ZA-SA3500G/5	738,000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)		
Aterm SA3500G(6年ライセンス付)	ZA-SA3500G/6	848,000円	壁掛けキット	ZA-SA/MK1	8,000円
Aterm SA3500G(7年ライセンス付)	ZA-SA3500G/7	958,000円	外付けアンテナ(2本1組)	ZA-SA/ANT1	10,000円
			USBケーブルキット (この製品は無線LANアダプタ無しUSB接続はできません)	ZA-SA/UC1	500円

■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）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、誤動作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が届かない場所ではご使用にならないでください。・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、この周波数帯域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。

- (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ンネルを変更するか、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排除することはできません。●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ません。●本製品は多くのトラフィック負荷がかかるため、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（非居住者への役員提供等をむ）に関しては、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、本製品の販売店にご相談ください。●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、および通信料金等随時的損害について、当社は一切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/](http://www.necplatforms.co.jp/product/security_ap/)

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。

●Atermは日本電気株式会社の登録商標です。  
●本紙に掲載された社名、製品名は各社の商標または登録商標です。  
●本紙に掲載された製品の色は、印刷の都合上、実際のものとは多少異なることがあります。また、改良のため予告なく形状、仕様を変更することがあります。

機能一覧

項目	プリッ モード	ル モード	仕様	
ネットワーク セキュリティ 機能	アンチ ウイルス	○	○	シグネチャファイルに基づき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、検出時は当該プログラムの書き換えにより無害化する。
	ファイアウォール機能	○	○	社内ネットワークに入ってくる通信を監視し、不正アクセス/パケットを遮断する。
	不正侵入検出/防止 (IDS/IPS)	○	○	あらかじめ登録された侵入手口/シグネチャファイルとのパターン マッチングにより不正侵入を検出し、当該通信を遮断する。
	Web ガード	○	○	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シグネ チャファイルとのパターンマッチングにより検出し、当該通信を遮断する。
	URL フィルタリング	○	○	クラウドサーバへの問い合わせによりURLがどのカテゴリのWebサイトに属する か検出し、あらかじめ設定されたカテゴリに該当する場合は当該通信を遮断する。
	URLフィルタリング	○	○	あらかじめユーザが設定した文字列がURLに含まれる場合に当該通信を遮断する。
	アプリケーション ガード	○	○	あらかじめ登録された通信プロトコルなどをシグネチャファイルと のパターンマッチングにより検出し、当該通信を遮断する。
	IMC フィルタリング	○	○	あらかじめ登録されたMACアドレス以外の通信をブロックする。
	検査対象/パケット	○	○	ブリッジモード/IPv4、IPv6 /パケット ルータモード/IPv4 /パケット
	デバイス管理 機能	○	○	接続されたデバイスのMACアドレス/IPアドレス/OS情報/有線無線種別を自動検出し、PC名などのコ メント付与、メール送附時のメールアドレスとの紐付け、統計情報収集の対象選択/最大50台が可能。
統計情報	○	○	デバイス管理機能で選択されたデバイス(最大50台)の身元検出状況、URLフィル タリング/アプリケーションガードなどでの遮断状況を表とグラフにて表示。	
ブリッジ機能 (ブリッジモード)	○	○	トランスベラレントブリッジ	
リンクレイバ機能	PPPoEクライアント	○	IPCP 1 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	○	動的ルーティング(最大50台)、NAT、IPsec/VPN、ポート転送(最大50台)、ICMP Redirect、ホストルー ティング	
拡張機能	IPv4	○	DHCPサーバ(アドレス払い出し数最大250個)、DHCPクライアント、 プロキシDNS、NTPクライアント、ホームIPローケーション*、自己診断	
無線 LAN アクセスポイント 機能	規格	○	○	IEEE802.11b、IEEE802.11g、IEEE802.11n (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)
アンテナ 機能	アンテナ	○	○	内蔵アンテナ、外付けアンテナ (オプション)
	IPv4	○	○	対地数 1
IPsec	IKEv1	○	○	IPsec (ESP、トンネルモード、post-fragment、IKEv1 (メインモード、アグリゲーションモード)、暗号化 モード(DES、AES(128、192、256bit))、認証アルゴリズム(MD5、SHA-1、SHA-2(256bit))
	IKEv2	○	○	IPsec (ESP)、トンネルモード、post-fragment、IKEv2、暗号化モード(3DES、 AES(128、192、256bit))、認証アルゴリズム(MD5、SHA-1、SHA-2(256bit))
SNMP	IPv4	○	○	SNMPv1、SNMPv2c (エージェント)
	標準 MIB	○	○	MIB II (RFC1213) (Private MIB には対応していません)

※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)

**環境配慮基準** 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。

**RoHS指令  
準拠**



# 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？

セキュリティに関する専門部署や専任SEがない場合のネットワークのセキュリティはウイルス対策ソフトだけになっていませんか。電子メールの添付ファイル監視や迷惑メールへの対策だけでは十分とはいえません。不正アクセスやなりすまし、改ざんなど意図しない情報漏えいに対しても対策が必要になります。



### Aterm SA3500Gとは

Aterm SA3500Gは、ネットワークの入口に設置するだけで、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・無害化したり、インターネットからの不正侵入の防止、社員が誤って危険なサイトにアクセスすることを防止する等、複数の機能を1つにまとめ、様々なサイバー攻撃の脅威から自社のネットワークを防御するセキュリティ端末です。



### 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しています。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/>

### Aterm SA3500Gの特長

#### 簡単設置(ブリッジモード)

SA3500Gは、ブリッジモードが利用でき、既存の社内ネットワークの構成を変えずに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

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。SA3500Gは、この最新のシグネチャをライセンス期間(1年間/5年間/6年間/7年間)に合わせて定期的に自動更新して提供します。

## セキュリティ機能

### 外部からの脅威

悪意ある攻撃など

#### アンチウイルス

ウイルスや危険なコードが含まれるプログラムをブロック。ホームページ閲覧時やメール送受信、その他のアプリケーションの通信を監視し、ダウンロードやアップロードするファイルにウイルスが混入していないかチェック。

ウイルスを書き換え無害化

#### ファイアウォール

インターネットから社内ネットワークに入ってくる通信を監視し、不正アクセスを遮断してネットワークの安全を確保。

ネットワーク攻撃を遮断

#### 不正侵入検出 / 防止 (IDS/IPS)

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不正侵入や攻撃を検出し、防止することで、セキュリティ対策レベルを向上。

蓄積された侵入手口のパターンと比較して不正アクセスを検出し遮断

インターネット

社内ネットワーク

#### 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。

サイトA (OK) / サイトB (NG)

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。

NGワード xyz

http://abc...xyz/

キーワードが入ったURL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。

違法行為 / 違法薬物

指定されたカテゴリーに属する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、メッセージアプリなど、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。

ファイル交換 / 動画共有

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

\*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。

## 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
- 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のランプ表示可能
- メールでの通知  
ユーザー(最大50宛先)への脅威検出通知、管理者(最大3宛先)への脅威検出通知・ライセンス切れ警告・ファームウェアアップデート通知が可能

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

ブラウザ上に表示する脅威ブロック画面のメッセージは、案内文や問合せ先などの任意のメッセージを追加するといったカスタマイズが可能です。また、メール通知にて記載されるメッセージも同様にメッセージの追加が可能です。

<標準> Web ガード  
http://www.example.com/  
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。

<カスタマイズ後> Web ガード  
http://www.example.com/  
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。  
※事前に設定が必要である場合は、こちらより制限解除の申請をお願いします。

## 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)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。(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(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。

2017/01/23 13:30:00  
WebGuard Block

※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。

## 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。

- <確認できる情報>  
●MACアドレス/IPアドレス ●機器の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)

#	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	00:00:00:00:00:00	192.168.11.16	Windows 7	事務PC(佐藤さん)	hata@aaa.bb.jp	有線	通知	収集	参照
2	00:00:00:00:00:00	192.168.11.9	iPhone	iPhone(佐藤さん)	sato@aaa.bb.jp	無線	通知	収集	参照
3	00:00:00:00:00:00	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
4	00:00:00:00:00:00	192.168.11.12	Nexus 5	スマホ(細田さん)	waguchi@aaa.bb.jp	無線	通知	収集	参照
5	00:00:00:00:00:00	192.168.11.10	Windows 7	事務PC(佐藤さん)	hata@aaa.bb.jp	有線	通知	収集	参照

## 1年ライセンス付きモデルおよび追加ライセンス

従来の5年間/6年間/7年間のライセンス付きモデルに加えて、お求めやすい価格の1年間のライセンス付きモデルを追加しました。1年間/5年間/6年間モデルは追加ライセンス(1年)のご購入により最大7年間までご利用可能となります。

統計情報(ブロック数グラフ)

機能を選択: 全ての機能

順位	デバイス	コメント	合計	AV	IPS	WG	UF	APG
1	00:00:00:00:00:00	事務PC(佐藤さん)	255	45	44	43	42	
2	00:00:00:00:00:00	iPhone(佐藤さん)	185	85	84	83	82	
3	00:00:00:00:00:00	事務PC(細田さん)	180	80	80	80	80	