

社内LAN不正接続をブロック!

AAM-2000



社内ネットワークセキュリティ対策+業務管理
社内WiFi・社内PC、管理できていますか？

社内のネットワーク保護。 社内WiFi・PC放置のリスク知っていますか？

1

社員が個人端末(PCやスマホ)でWiFi接続したときのリスク

セキュリティが万全でないかもしれない個人端末で、社内ネットワークにアクセスする事は危険をとまねいます。もしその個人端末がウイルスに感染していたら、どうなると思いますか？
AAM-2000では、WiFiに接続できる端末の設定ができるだけでなく、接続許可していない端末を検知した場合は、管理者にメール通知するとともに、不正接続した端末の通信をブロックしてネットワークを保護します。また、ネットワーク利用の一時停止など、細かい設定も可能です。

2

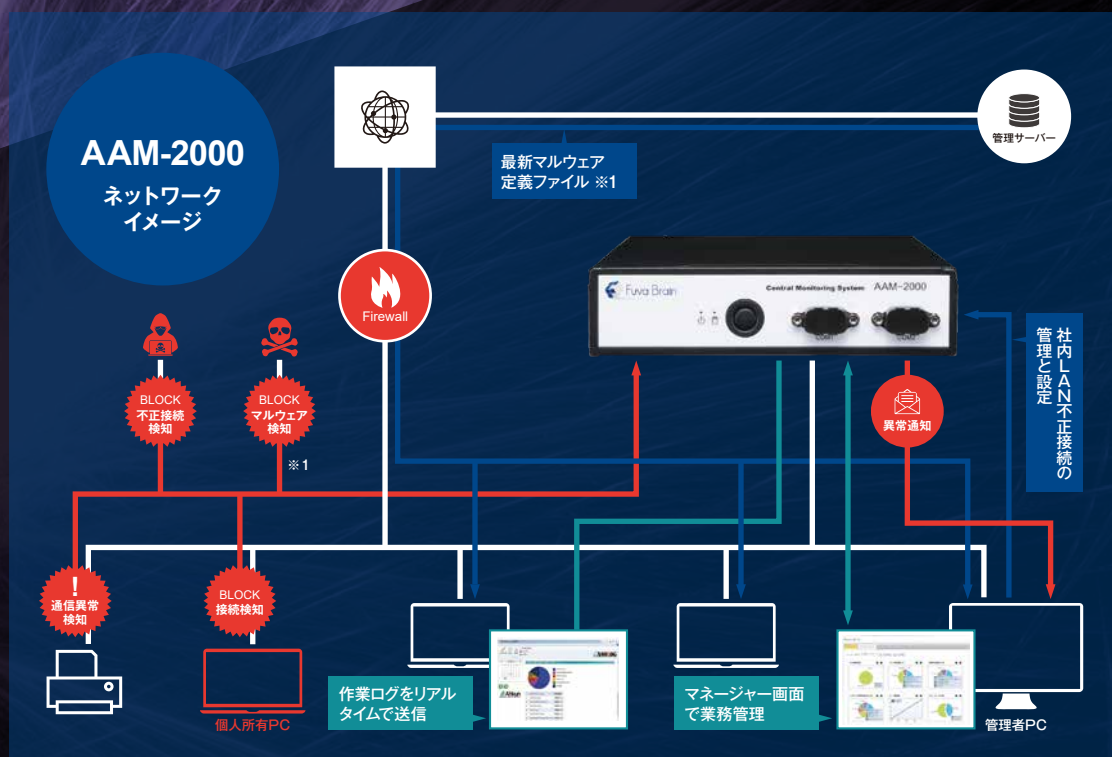
外部から不正接続されるリスク

例えばWiFiのパスワードを頻繁に変えていたとしても、それだけでは安全とはいえません。数々のハッキングツールが出回っている昨今、PCの不正接続による危険度は、非常に高くなってきています。そして一度ネットワークの中に侵入されてしまうと、そこからの情報搾取や攻撃は、簡単なものになってしまうのです。
AAM-2000では、WiFiハッキングや、LANに直接接続して引き起こすウイルス感染・情報漏えい・悪意のある攻撃から貴方のネットワークを守ります。

3

社内PCの持つリスク

許可された社内PCであっても、内部の人間が意図的に情報持ち出しを行おうとした場合は、言うまでもなく脅威となります。
AAM-2000では、各PCに対して、USBメモリやスマートフォン接続、アプリケーションの使用を細かく設定・管理することが可能なだけでなく、社員が今何をしているか、リアルタイムで確認することもできるので、情報漏えいに対する大きな抑止力となります。
また、ウイルス感染のリスクに対しても、自動で最新のセキュリティ情報にアップデートを行い、各PCをしっかりと守ります。※1



※1 EX AntiMalware v7バンドルモデルに限ります。

社内LAN不正接続をブロック！ 社内ネットワークセキュリティ対策＋業務管理

社内ネットワークセキュリティ対策＋業務管理



AAM-2000でこんな心配にも対応できる！



社内ネットワークの無断利用を心配しなくてよかった。

社内WiFiの無断利用を防ぐことで、ネットワークが重くなることや、情報持ち出しのリスクを少なくします。また、外部からの悪意あるネットワーク接続も防ぎます。



複合機やネットワーク監視カメラの異常にすぐ気づける

各機器の接続状況も監視しているので、異常があると管理者にメール通知します。「プリンターがずっとおかしい」「肝心な時に監視カメラが止まっていた。」といったリスクを少なくします。



USBメモリやスマホ接続、利用ソフトの制限

使用できるUSBメモリやソフトを制限できるので、「業務に必要なもののみ許可」といったことが可能となります。また、危険なフリーソフト利用のリスクも少なくします。



従業員のPC作業状況が把握でき、業務効率アップ。

PCの日々の作業内容を記録、本体に自動で送信されます。誰がどのような作業を行っていたかを見える化し、内部不正の抑止にも繋がります。



遠隔地や持ち出し中のPCのセキュリティ状況まで一括管理・把握 ※1

管理画面から、管理している全てのPCの状況を把握できます。また、どこにいても最新のセキュリティレベルを保ち、マルウェアの検知履歴も一括管理可能です。



PCやUSBがマルウェアに感染しても迅速に検知・隔離し、重大被害を阻止 ※1

2種類のマルウェアデータベースが、独自の高度監視強度を誇るスキャンエンジンと連携し、マルウェア実行前にその挙動を感知しアクティブにブロックします。

攻撃・内部不正のリスクから守る！ PC業務もしっかり管理！AAM-2000でネットワークもPCも、 しっかり防御、しっかり管理。UTMでは防御出来ない社内LANへの裏口侵入もブロック！

AAM-2000 はネットワークと PC を外部攻撃から守るだけでなく、管理をしっかりと行う事で内部からの情報漏えいも防ぎます。

また、PC 作業や状態の可視化により業務効率の向上も見込めます。あまりセキュリティを意識してこなかったお客様にも、UTM 等を既に導入済みのお客様にも、嬉しい機能が満載で社内の抜け穴をしっかり守ります。

ハッキングから ネットワークを守る！

WiFiハッキングを防ぐ

悪意ある人物が無線LANに不正接続してきた場合、UTMでは防げませんが、AAM-2000なら、接続許可していないPCを検知すると、管理者にメール通知し、不正PCの通信をブロックしてネットワークを保護します。

マルウェア侵入を防ぐ！ 瞬時に検知・隔離 ※1

マルウェアは検知して隔離

もしPCがマルウェアに感染しても、最新の情報で挙動を検知。マルウェア実行前に隔離します。感染したUSBをPCに接続した場合でも、瞬時に検知・隔離します。

Fuva Brain 管理サーバ 常に最新セキュリティ！ ※1

自動情報更新で常に最新

世界中の脅威情報を共有しており、最新のセキュリティレベルを保ちます。クラウドでのPC集中管理にて、オフィス外にいても、最新のセキュリティレベルを共有します。

何かあったら アラート通知！

不正検知でメール通知

不正接続や通信異常の検知など、何かあったらすぐにメールで通知します。

社内LAN 不正接続をブロック

社内ネットワークセキュリティ対策+業務管理

INTERNET
OFFICE NETWORK

プライベート端末の 接続を禁止！

サボり目的から情報持ち出しまで

会社で管理していない、個人PCやスマートフォンの接続を検知すると、管理者にメール通知しブロックします。サボり目的のネットワーク利用や、社内ネットワークからの情報持ち出し阻止に役立ちます。

USBメモリやスマホの 接続を制限！

許可デバイスを細かく設定

社内PCへの、USBメモリやスマートフォンの接続禁止や許可を、個人単位や部署単位で細かく設定することが可能です。

複合機等の異常 を発見！

複合機や監視カメラの状態監視

社内ネットワーク内の各機器の接続状況を監視しているので、複合機や監視カメラなどの通信が切断した場合、管理者にメール通知します。また、管理PCで社内ネットワーク内の接続状況も簡単に確認できます。

個人や全体の動きがわかる！ 資産管理も簡単に！

分析機能で一発確認

PCごとや社内全体の、作業内容や作業時間、ソフト使用率の分析集計結果を簡単に確認できます。また、PCの各種スペックやインストール済み。ソフトもわかるので、資産管理も楽に行えます。



業務に不要な アプリケーションを禁止！

危険アプリやサボリアプリは排除

「メッセージソフト」や「IP電話ソフト」といったカテゴリ別の設定や、個別設定での利用禁止が可能です。



リアルタイムで 社員PCを監視！

各種不正の抑止効果に

社内PCの作業内容ログをリアルタイムでサーバに送信。各PCのデスクトップ画面まで見えるので、業務外作業や情報漏えい防止に役立ちます。



管理者PC

企業には企業のための最新セキュリティ！



情報セキュリティ対策を支援

開発・発売元



株式会社フーバーブレイン

ソリューション営業部

本社

〒102-0094
東京都千代田区紀尾井町4-1 ニューオータニガーデンコート22F
TEL 03-5210-3061 FAX 03-5210-3062

お問い合わせ・ご購入は下記販売店まで

1_2018.10

www.fuva-brain.co.jp

型番

シリーズ	型番	CL数	ライセンス期間
	AAM-15	~15	5年
	AAM-15L		6年
	AAM-25	~25	5年
	AAM-25L		6年
	AAM-50	~50	5年
	AAM-50L		6年

※EX AntiMalware v7 / バンドルモデルもございます。詳細はお問合せください。

ハードウェアスペック

動作環境条件	温度5~40℃、湿度0~95% (結露しないこと)
電源	AC100V (50/60Hz)
最大消費電力	16W
搭載ストレージ	SSD128GB
外形寸法	W39.5×D200×H165mm
質量	1.43kg
アクセスウォール	
主な機能	○未登録機器の不正接続検知、通信ブロック、アラート通知メール ○登録機器の通信異常監視、アラート通知メール
通知メール登録数	最大3メールアドレス
許可ネット機器登録数	最大50台
管理設定	ブラウザベース (GoogleChrome、FireFox推奨)

ソフトウェア動作環境



PasoLogクライアントプログラム	
対応OS	Windows 10 / 8.1 / 8 / 7 / Vista (32 / 64 ビット版)
対応OS言語	日本語 / 英語
CPU	1.5GHz以上 (推奨2GHz以上)
メモリ	2GB以上 (推奨4GB以上)
ハードディスク	インストール時に500MB以上の空き容量
PasoLog Manager	
Webブラウザ	Google Chrome (推奨)、Internet Explorer 9 以降
画面解像度	1024×768以上 (1280×1024推奨)
サーバーエージェント	
対応OS	Windows Server 2016 / 2012R2 / 2012 Windows Storage Server 2016 / 2012R2 / 2012 (64ビット版)
対応OS言語	日本語
CPU	1.5GHz以上 (推奨2GHz以上)
メモリ	512MB以上
ハードディスク	インストール時に1GB以上の空き容量



EX AntiMalware v7 クライアントプログラム	
対応OS	Windows 10 / 8.1 / 8 / 7 Windows Server 2016 / 2012R2 / 2012 / 2008R2 Windows Storage Server 2016 / 2012R2 / 2012 / 2008R2 (32/64ビット版)
対応OS言語	日本語 / 英語
CPU	1.5GHz以上 (推奨2GHz以上)
メモリ	2GB以上 (推奨4GB以上)
ハードディスク	インストール時に1GB以上の空き容量
EX AntiMalware v7 Manager	
Webブラウザ	Google Chrome (推奨)、Internet Explorer 11.0 以降
画面解像度	1024×768以上 (1280×1024 推奨)

※本製品の設置・ご使用に関しましては、製品に添付しております安全上の注意をよくご確認の上、必ずお守りください。※本製品は日本国外での使用については一切のサポート、保証をしておりません。※記載内容は2018年10月現在のものです。※仕様は予告なく変更する場合がありますので、予めご了承ください。※記載されている製品名は各社の商標・登録商標です。