

中小企業に最適な多層防御型情報漏えい対策



Eye^{“24/7”}

AntiMalware

USAV



標的型攻撃も。顧客情報流出も。機密情報の持ち出しも。
情報漏えいリスクをまとめて減らすヒント、教えます。

ZERO TRUST

日々、増大するマルウェアの新種・亜種群。
従来のシグネチャベースでは
検知は追いつけない。

進化する脅威に対抗する



01 取り巻く環境の変化 内部への侵入リスクが拡大

クラウドサービスやモバイルデバイスの普及 -
働き方改革の推進によるテレワーク需要 -
IoT (モノのインターネット) の増加 -

Cloud
Mobile IoT

Internet

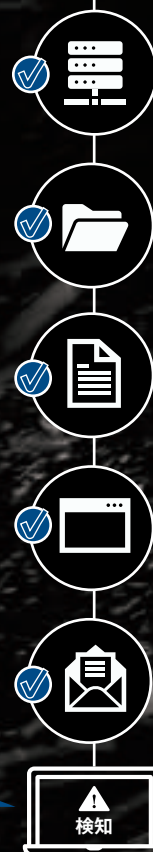


02 攻撃者の組織化 ランサムウェアの産業化

サイバー攻撃のビジネス化で金銭目的が顕著に -
ランサムウェア攻撃の頻度は3倍に上昇 -

03 マルウェアの増大と 攻撃手法の高度化・複雑化

毎月1200万を超える新しい亜種のマルウェアの出現 -
1秒に11.6個生成される新種のマルウェア -



ゼロトラストを前提としたリアルタイム監視。
進化する脅威を一貫して検出。

ATC (Advanced Threat Control: 先進型振る舞い検知) は、パソコンやサーバ内のアプリケーションの動きを常時監視し、不正な動きを検知。既知、亜種、未知の脅威から保護します。



高度なヒューリスティック手法に基づく
動的テクノロジーを採用。



アプリケーションが行うすべての動作
を監視し、未知の脅威を逃さず検出。

検知 不正な挙動を検知



※ATC 機能は Windows OS に対応

BACKUP

データ消失によるビジネスへの影響を最小限に抑え、
万が一の時の業務復旧時間を短縮。 ※バックアップ機能はWindowsOSに対応



定期的に自動実行



安全な領域でデータ保護



容易に復旧



指定フォルダを自動バックアップ
(更新データのみ)

差分バックアップにより、
バックアップ時間を短縮。



スケジュールスキャン実施

スケジュールスキャンとバックアップ機能
との連携により、重要情報を定期的に負
荷なくバックアップ。



バックアップフォルダを
Eye'247' AntiMalware が保護。



感染対応後、
バックアップフォルダから
ファイルの復旧が可能です。

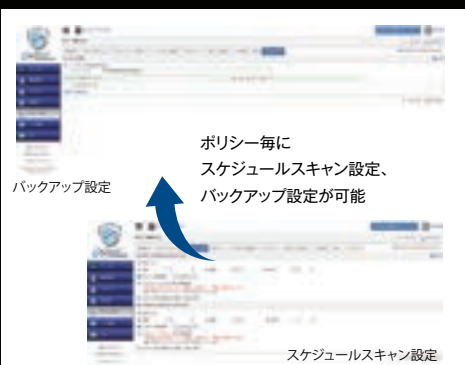


万が一、ランサムウェアなどの
被害が発生した場合



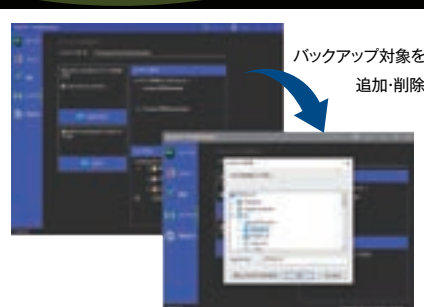
バックアップフォルダを
Eye'247' AntiMalware が保護。
不正な書き換え、暗号化など
の被害を受けません。

管理Managerで
全端末共通のバックアップ設定



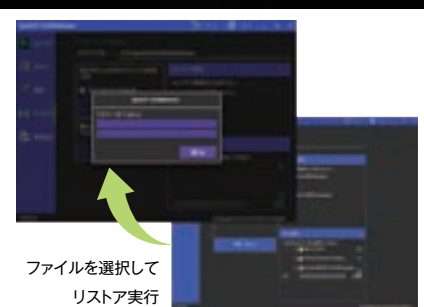
管理Managerでバックアップ対象のファイルパスを指定することで、全端末共通の領域に対してバックアップを取ることができます。

クライアントで
個別にバックアップ設定も可能



日々、使用しているファイルの保存場所は利用者毎に異なるものです。Eye'247' AntiMalwareでは管理Managerで指定したファイルパスの他にPC毎に任意のファイルパスを指定できます。

クライアントで
データのリストアを簡単に実行



万が一、ランサムウェアに感染した場合でも、クライアントで簡単に直近のバックアップデータからリストア(復旧)できます。

「常に最新のセキュリティ」トリプルガードで情報漏えいリスクを減らす！ 従来型では不可能だった多層防御型で、企業の情報資産を外部・内部の脅威から守ります。

世界中の脅威情報を共有し、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することが可能です。

1 ネットワークで守る



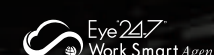
世界最高水準の「CheckPoint」のUTMで、入口対策・出口対策を行います。ポートスキャン、脆弱性攻撃はもちろん、標的型攻撃メールなどによるC&C不正通信も防ぎます。

2 各PCで守る



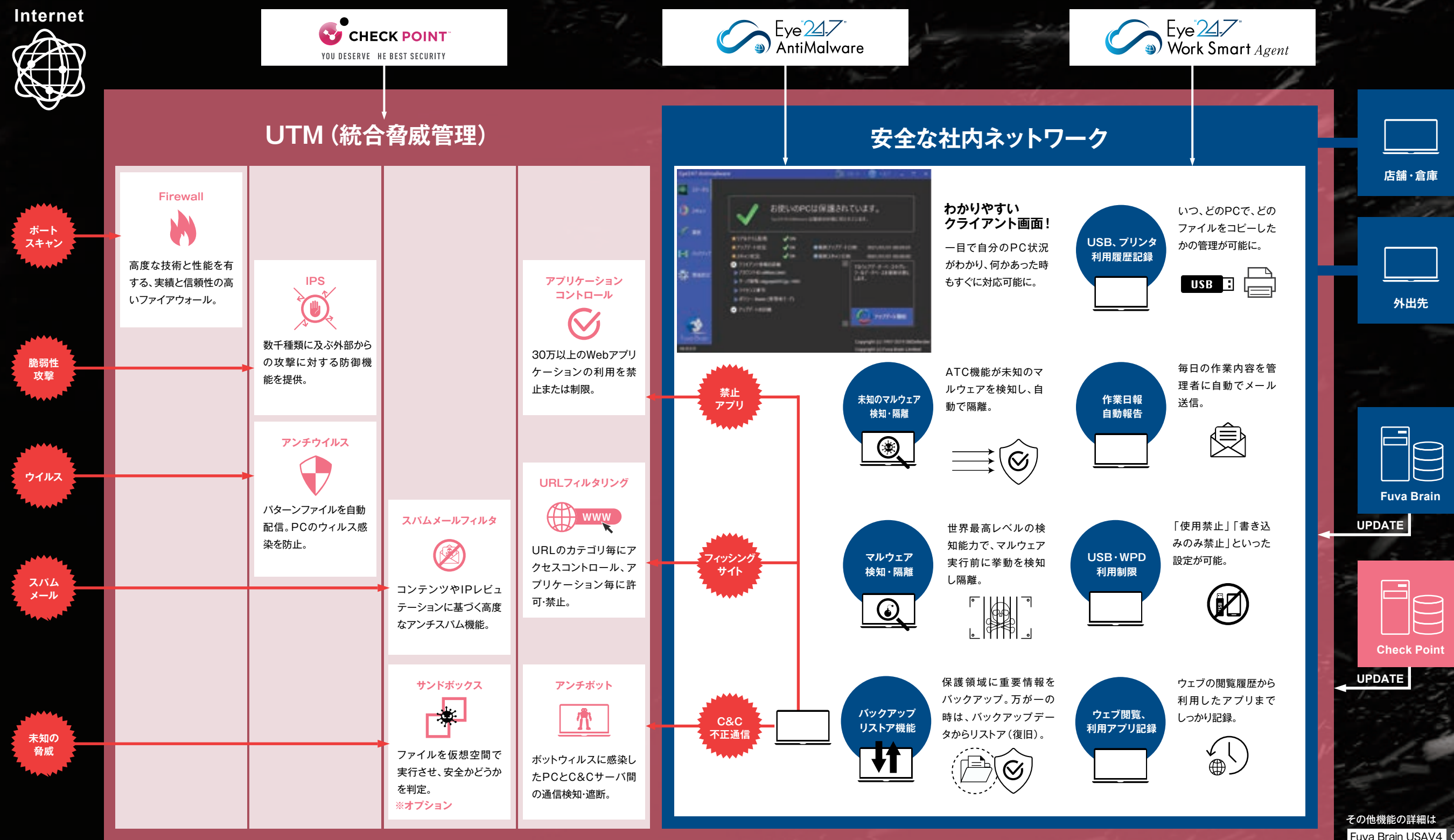
エンドポイントセキュリティ「Eye"247" AntiMalware」でウイルス検知時隔離、USB接続時の自動スキャンなどを行い、各PCを守ります。PCの一元管理や、持出し用PCのセキュリティにも使えます。

3 業務可視化で守る



業務可視化ソフトウェア「Eye"247" WorkSmart Agent」にてウェブ閲覧履歴、USBやプリンタの利用履歴の確認が可能。USB・WPDの利用制限もでき、意図的な情報持ち出しの抑止にもなります。PC作業内容のメール自動送信機能も。

企業には企業のための最新セキュリティ！



UTM・エンドポイントセキュリティ・業務可視化のトリプルガードで企業の情報資産を守ります。

Eye“247”AntiMalware USAV IV は、世界最高水準のセキュリティを誇る「CheckPoint」UTM と Fuva Brain の提供するエンドポイントセキュリティ「Eye“247”AntiMalware」、業務可視化ソフトウェア「Eye“247”Work Smart Agent」3つのセキュリティで、従来型のセキュリティでは不可能だった多層防御型のセキュリティを実現し、企業の情報資産を外部・内部の脅威から守ります。

導入後はセキュリティ情報を自動更新！ 内部統制機能まで付いているから、こんなに嬉しい！

セキュリティ製品を組み合わせたソリューション



管理者
A社さま

サイバー攻撃をされて
いたらしい。でも防げ
たみたい。



サイバー攻撃をされても、ネットワークの入口と
出口・各PCで防ぎます。また、検知したボット
ウイルス数、マルウェア数、攻撃件数は、セキュ
リティレポートで確認できます。

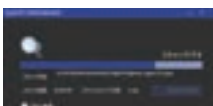


サポート



管理者
C社さま

USBメモリがマルウェ
ア感染していたらし
い。でもPCには感染し
なかった。



感染USBはリアルタイム検知機能にて瞬時に検
知可能です。他のPCやネットワークに被害を拡散
させることなく、マルウェアを確実に隔離します。



サポート



管理者
D社さま

PCがマルウェアに感
染する前にすぐに検
知・隔離できたので、
大きな被害にはならな
かった。



ATC（先進型振る舞い検知）機能や2種類の
マルウェアデータベースによる検知機能が連携
し、マルウェア実行前にその挙動を感知してア
クティブにブロックします。



サポート



管理者
B社さま

USBメモリやスマホ接
続、利用ソフトの制限
がかけられるように
なって助かっている。



使用できるUSBメモリやWPD、ソフトを制限でき
るので、「業務に必要な物のみ許可」といったこと
が可能となります。また、無断使用の危険なフリー
ソフトなどからのマルウェア感染を予防できます。



サポート



管理者
Y社さま

遠隔地や持ち出し中の
PCのセキュリティ状況
も一括管理・把握出来
て安心できる。



管理Managerから、管理している全てのPCの
状況を把握できます。また、どこにいてもクラ
ウドから最新のデータを提供し、マルウェアの
検知履歴も一括管理可能です。

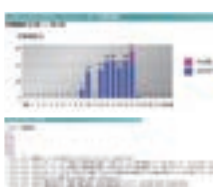


サポート



管理者
S社さま

従業員のPC作業状
況の把握ができて、全
体の業務効率アップ
に繋がった。



PCの日々の作業内容を記録し、管理者にメー
ルで自動送信することが可能です。誰がどのよ
うな作業を行っていたのかを見える化し、内部
不正も抑止します。

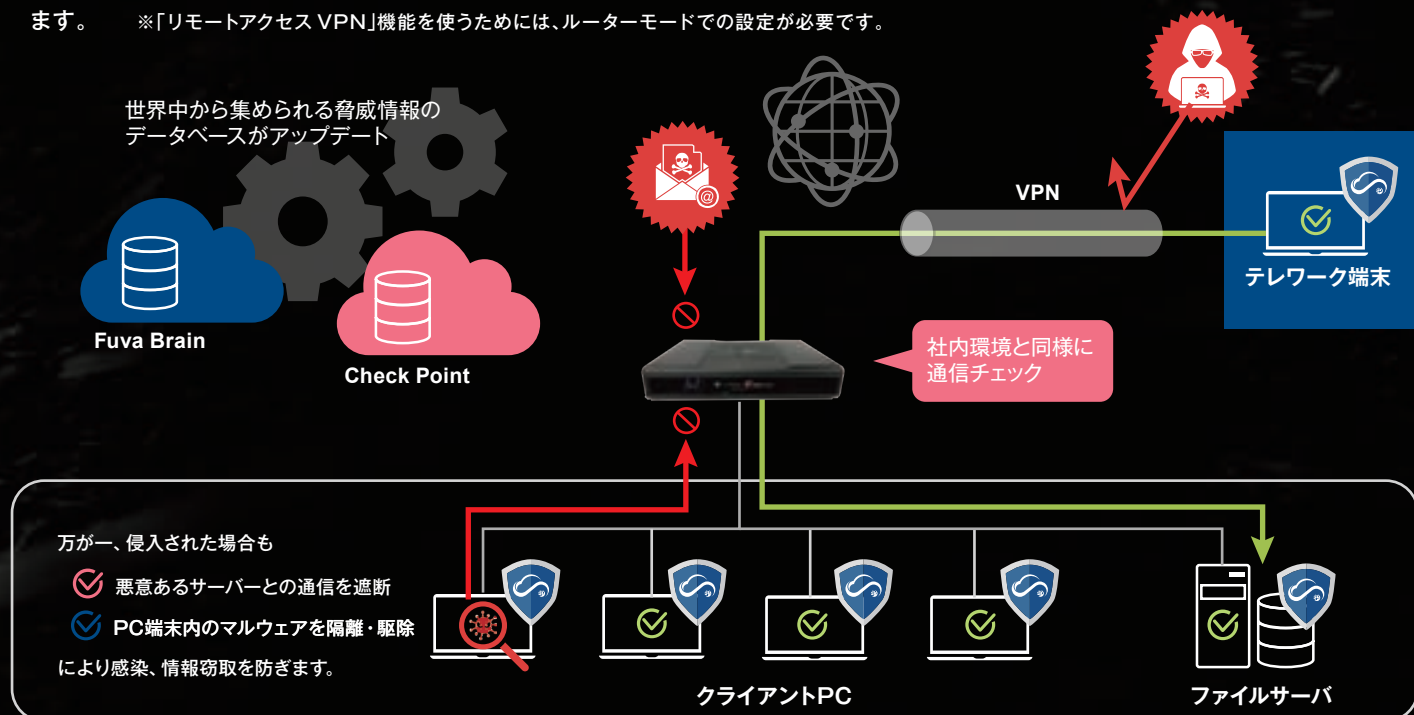


サポート

テレワークのセキュリティ面の課題をUSAV IVが解決！ 管理者は全ての端末を管理Managerと業務日報で一元管理。

テレワーク端末にも社内と同じセキュリティを提供

USAV IVに標準搭載されている「リモートアクセス VPN」機能を利用すれば、社外でも社内環境と同様の通信チェックが可能になります。テレワーク中でも、エンドポイントセキュリティと業務可視化によるトリプルガードで、社内にいるのと同様のセキュリティ環境で業務が行えます。管理者は管理 Manager でセキュリティ状況とメール送信される業務日報をチェックすることで一元管理が可能となります。 ※「リモートアクセス VPN」機能を使うためには、ルーターモードでの設定が必要です。



管理 Manager では、UTM レポート連携機能を搭載。「CheckPoint」UTM と Eye” 247” AntiMalware が検知したセキュリティ脅威状況を管理画面上でレポート表示させます。 ※UTMレポート連携機能はUSAV IVシリーズのみの機能です

Eye” 247” AntiMalware 管理Manager

マルウェアの検知状況をリアルタイムに把握できる他、PC・サーバの機器情報(OSやユーザ名等)、ソフトウェア情報の一元管理が可能です。

ユーザー情報

- マルウェアの検知状況の把握、自動レポート
- OSのバージョンや利用状況、アップデート状況の把握
- スケジュールスキャンの実施状況の把握



Eye” 247” WorkSmartAgent 業務日報

毎日のPCの作業内容が翌営業日に管理者にメールで送信されます。

UTMレポート連携

- アンチウイルス、アンチボット機能等で検知した件数
- ウイルスに感染していると思われるPCの台数やIPアドレス
- 悪意あるサーバーとの疑わしい通信を検知した端末の特定
- 業務に関係ないアプリケーション利用やウェブサイト閲覧の把握

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

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

9_2023.10

www.fuva-brain.co.jp

型番

シリーズ		CL数	ライセンス期間
Eye "247" AntiMalware USAV IV		~10	5年 / 6年 / 7年
		~20	
		~50	
		~70	
		~100	
		~150	
Eye "247" AntiMalware USAV IV Wi-Fiモデル		~200	
		~10	
		~20	
		~50	

ソフトウェア動作環境



Eye "247" AntiMalware クライアントプログラム		
対応OS (日本語/英語)	下記OSの32ビット、64ビット(×64)をサポートします。 Windows 11 / 10 Windows Server 2022 / 2019 / 2016 Windows Storage Server 2016 Windows Server IoT 2019 for Storage ※本製品は、Microsoft .NET Framework4.5.2以上が必要です。 ※Windows 11S / 10Siは非対応です。	下記OSをサポートします。 macOS Ventura (13.0以上) macOS Monterey(12.0以上) macOS Big Sur(11.0以上) macOS Catalina(10.15以上) macOS Mojave(10.14以上) macOS High Sierra(10.13以上)
CPU	クロック周波数1.5GHz以上(推奨 2GHz以上) ※Windows11 は、1.5GHz(推奨2GHz以上)で2コア以上 ※IntelまたはAMDプロセッサに対応しています。 ※ARMプロセッサには対応していません。	クロック周波数 2GHz以上 ※Apple M1チップ Intelプロセッサに対応しています。
メモリ	2GB以上(推奨4GB以上) ※Windows11は、4GB以上(推奨8GB以上)	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	インストール時に1GB以上の空き容量
Eye "247" AntiMalware Manager		
Webブラウザ	Google Chrome(推奨)、Microsoft Edge	
画面解像度	1024×768以上(1280×1024推奨)	



Eye "247" WorkSmart Agent	
対応OS	Windows 11 / 10 (32/64ビット版)
対応OS言語	日本語 / 英語
メモリ	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

ハードウェアスペック

		10CL / 20CL	50CL	70CL / 100CL	150CL / 200CL
パフォーマンス	脅威対策スループット(Mbps)※1	440	600	650	900
	VPNスループット(Mbps)	970	1,300	1,950	2,600
ハードウェア	WAN	1ポート※2			
	DMZ	-		1ポート※2 1ポート※3	
	LAN	5ポート※2		8ポート※2	
	Wi-Fi	802.11 a/b/g/n/ac/ax ※Wi-Fi 6 対応 MIMO 3×3		-	
	無線対応電波帯域	2.4/5Ghz ※バンド同時利用不可		-	
	コンソールポート	1ポート USB-C			
	USB ポート	1ポート USB 3.0			
寸法	外形寸法 (W×H×D)	210×37.5×160mm		210×42×170mm	
	重量	0.43kg		0.87kg	
使用環境	動作時	温度：0～40℃			
	非動作時	温度：-45～60℃ 湿度：5～95%（結露なきこと）			
電源	AC入力電圧	110 - 240V、50 - 60 Hz			
	電源仕様	12V/3.3A 40W デスクトップ・アダプタ			
	消費電力（最大）	17.92W 21.95W [Wi-Fi 有]		26.01W	
	熱出力	61.11BTU/h 74.85BTU/h [Wi-Fi 有]		88.70BTU/h	
適合規格	安全性	UL / c-UL / IEC 62368-1 CB			
	エミッション	EMC：EMI EN55024,EN55032 ClassB,VCCI,AS, NZS CISPR 32,IC ICES 03,RSS247 FCC：Part 15 Class B,C,E			
	環境対応	RoHS,REACH,WEEE			

※1 SMBの実環境に近づけた(HTTPを含む) 基本的なルール、NAT、ロギングや最新の脅威対策機能をオンにした状態で実行されています。

※2 10/100/1000Base-T RJ-45ポート

※3 1000Base-F SFPポート

※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2023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。