Digital communications
株式会社デジタル・コミュニケーションズ

中小企業に最適な多層防御型情報漏えい対策

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。

Cloud
Mobile
IoT

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 -

Internet

攻撃者

進化する脅威に対抗する

既知の脅威
亜種の脅威
未知の脅威

ATC
先進型振る舞い検知
Advanced Threat Control

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。

※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。

DATA SHIELD

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。

万が一、ランサムウェアなどの
被害が発生した場合

RESTORE

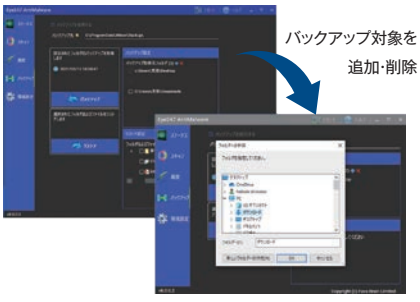
感染対応後、
バックアップフォルダから
ファイルの復旧が可能です。

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

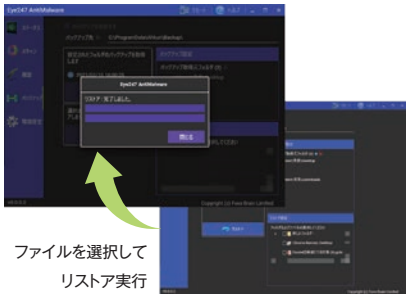
管理Managerでバックアップ対象のファイルパスを指定することで、全端末共通の領域に対してバックアップを取ることができます。

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

CHECK POINT YOU DESERVE THE BEST SECURITY

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

Eye247 AntiMalware

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

Eye247 Work Smart Agent

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！

Internet

CHECK POINT YOU DESERVE THE BEST SECURITY

Eye247 AntiMalware

Eye247 Work Smart Agent

UTM（統合脅威管理）

ポートスキャン

脆弱性攻撃

ウイルス

スパムメール

未知の脅威

Firewall
高度な技術と性能を有する、実績と信頼性の高いファイアウォール。

IPS
数千種類に及ぶ外部からの攻撃に対する防御機能を提供。

アンチウイルス
パターンファイルを自動配信。PCのウィルス感染を防止。

スパムメールフィルタ
コンテンツやIPレピュテーションに基づく高度なアンチスパム機能。

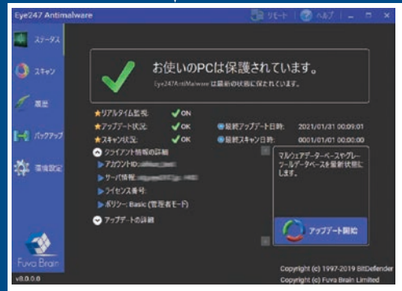
サンドボックス
ファイルを仮想空間で実行させ、安全かどうかを判定。
※オプション

アプリケーションコントロール
30万以上のWebアプリケーションの利用を禁止または制限。

URLフィルタリング
URLのカテゴリ毎にアクセスコントロール、アプリケーション毎に許可・禁止。

アンチボット
ボットウィルスに感染したPCとC&Cサーバ間の通信検知・遮断。

安全な社内ネットワーク



わかりやすいクライアント画面！
一目で自分のPC状況がわかり、何かあった時もすぐに対応可能に。

USB、プリンタ利用履歴記録
いつ、どのPCで、どのファイルをコピーしたかの管理が可能に。
USB

禁止アプリ

未知のマルウェア検知・隔離
ATC機能が未知のマルウェアを検知し、自動で隔離。

作業日報自動報告
毎日の作業内容を管理者に自動でメール送信。

フィッシングサイト

マルウェア検知・隔離
世界最高レベルの検知能力で、マルウェア実行前に挙動を検知し隔離。

USB・WPD利用制限
「使用禁止」「書き込みのみ禁止」といった設定が可能。

C&C不正通信

バックアップリストア機能
保護領域に重要情報をバックアップ。万が一の時は、バックアップデータからリストア（復旧）。

ウェブ閲覧、利用アプリ記録
ウェブの閲覧履歴から利用したアプリまでしっかり記録。

店舗・倉庫

外出先

Fuva Brain

UPDATE

Check Point

UPDATE

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 D-Guard UTM シリーズは、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

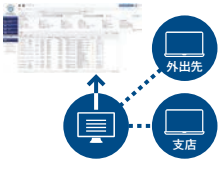
USBメモリやスマホ接続、利用ソフトの制限がかけられるようになって助かっている。

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。

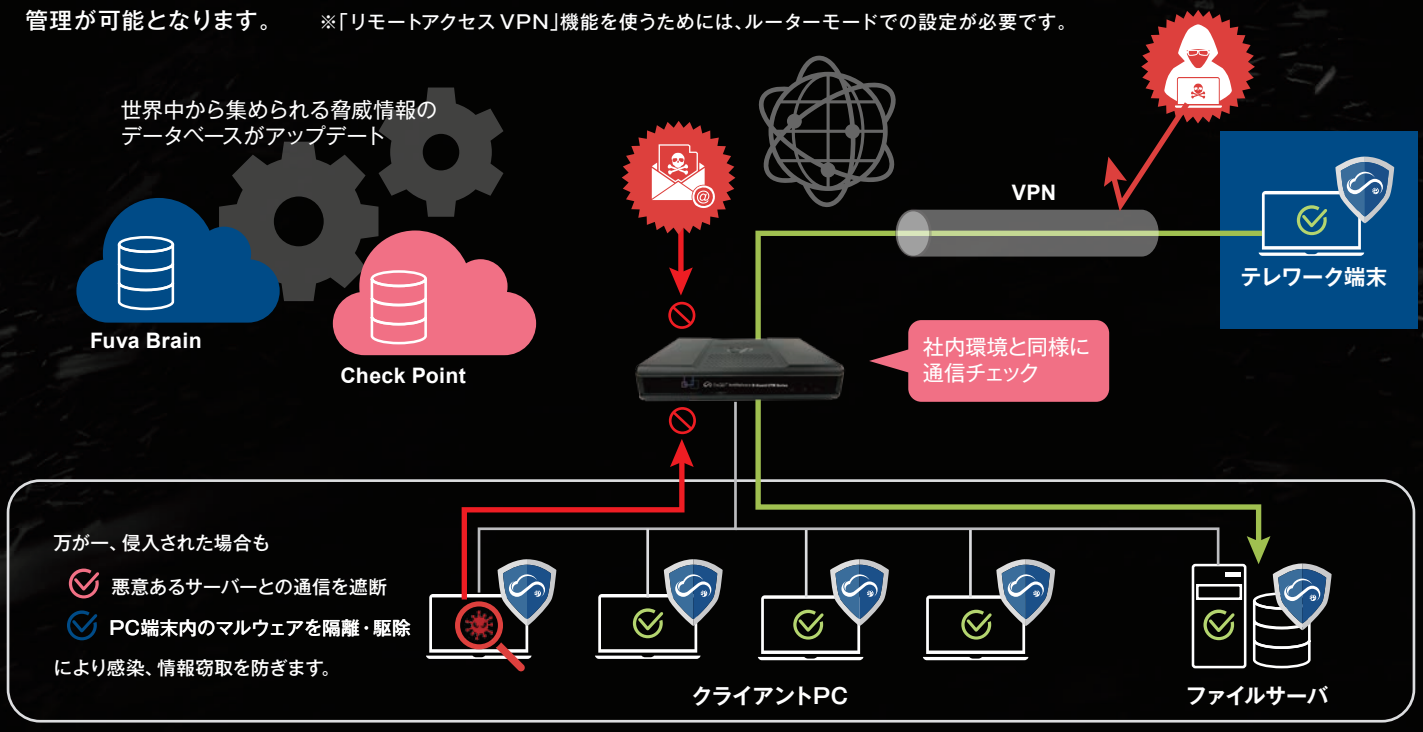
PCの日々の作業内容を記録し、管理者にメールで自動送信することが可能です。誰がどのような作業を行っていたのかを見える化し、内部不正も抑止します。

サポート

テレワークのセキュリティ面の課題をD-Guard UTM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。

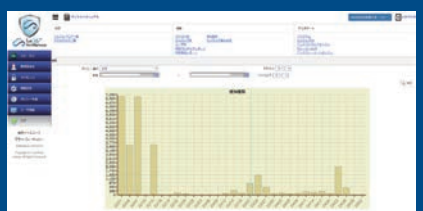
テレワーク端末にも社内と同じセキュリティを提供

D-Guard UTM Series 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D-Guard UTMシリーズのみの機能です

Eye “247” AntiMalware 管理Manager



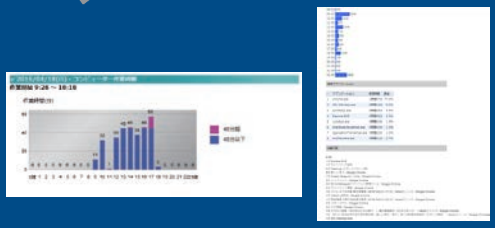
マルウェアの検知状況をリアルタイムに把握できる他、PC・サーバの機器情報（OS やユーザ名等）、ソフトウェア情報の一元管理が可能です。

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

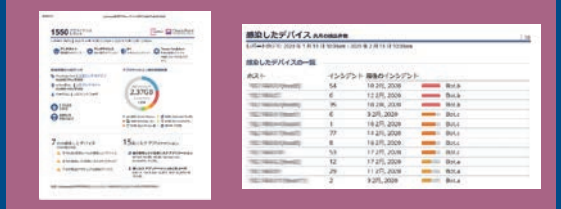
管理者端末

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

発売元

Digital communications
株式会社デジタル・コミュニケーションズ

本社 〒103-0014
東京都中央区日本橋蛎殻町1-29-9 ネオテック水天宮ビルM1階
TEL 03-6231-1855 FAX 03-6231-1880

お問い合わせ･ご購入はこちらの窓口まで

1_2023.02

www.dcoms.co.jp

型番

シリーズ		CL数	ライセンス期間
Eye“247”AntiMalware D-Guard UTM Series		~10	5年 / 6年 / 7年
		~20	
		~50	
		~70	
		~100	
		~150	
		~200	
Eye“247”AntiMalware D-Guard UTM Series Wi-Fiモデル		~10	
		~20	
		~50	

ソフトウェア動作環境

Eye247 AntiMalware

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 / 2012R2 / 2012 Windows Storage Server 2016 / 2012R2 / 2012 Windows Server IoT 2019 for storage ※本製品は、Microsoft .NET Framework4.5.2以上が必要です。 ※Windows11S/10Sは非対応です。	下記OSをサポートします。 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おりません。	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)

Eye247 Work Smart Agent

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	340	450	550	660
	VPNスループット(Mbps)	970	1,300	1,800	2,000
	接続数/秒	10,500	14,000	15,000	21,000
	同時接続数	500,000			
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 （Wi-Fi モデルのみ）	802.11 b/g/n/ac 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行われています。
※2 10/100/1000Base-T RJ-45 ポート
※3 1000Base-F SFP ポート