Fuva Brain

AI×AIで中小企業を守る！最強セキュリティ対策製品

FB SATMail 標的型攻撃メール訓練サービス FB SATMail付属

Eye“247” Safety Zone USAV V 社内ネットワーク・エンドポイントを、外部・内部の脅威・人的セキュリティリスクから総合的に守る

CHECK POINT UTM

UTM（ネットワークのセキュリティ）
社内ネットワークを外部・内部の脅威から守ることができるアプライアンスです。
P.3～P.4

NETWORK SECURITY
ネットワークセキュリティ

ルーター

● UTM
外部からの攻撃・不正なアクセスをブロック

● UTM
内部からの脅威をブロック

ハブ

サーバー

Eye 24.7 Safety Zone

エンドポイントセキュリティ
PC端末を外部・内部の脅威から総合的に守ることができるソフトウェアです。P.5～P.8

社内 PC

● UTM（サポート）
・機器の状態確認
・設定の追加・変更実施
・ファームウェアアップデート実施
・障害時のリモート調査

● UTM（サポート）
故障時センドバック対応・代替機貸出

SUPPORT
カスタマーサポート

Fuva Brain

カスタマーサポート
専任のサポートスタッフが導入後もあらゆる面からサポートします。P.10

● UTM
社内ネットワークのセキュリティを管理・運用

ENDPOINT SECURITY
エンドポイントセキュリティ

● エンドポイントセキュリティ
外部からの端末への攻撃をブロック

● エンドポイントセキュリティ
端末からの情報漏洩をブロック

● エンドポイントセキュリティ
社内端末のセキュリティを集中管理

● 情報漏洩対策ツール
端末の情報漏洩リスクを一元管理

● エンドポイントセキュリティ（サポート）
インストール手順の案内
設定の追加・変更をリモートで実施
リモートでのウイルス駆除支援

INTERNET
インターネット

Eye 24.7 Work Smart Agent

情報漏洩対策ツール
内部不正対策と業務の可視化をし、情報漏洩リスクを減らします。 P.9

● 情報漏洩対策ツール
情報漏洩のリスクを可視化

MANAGER
管理者

Fuva Brain Security Awareness Training シリーズ FB SAT Mail

標的型攻撃メール訓練サービス
攻撃メールの体験を行い、社員のリテラシーの向上に繋げることができます。 P.9

● 標的型攻撃メール訓練サービス
メール訓練の実施

● 標的型攻撃メール訓練サービス
標的型攻撃メールのリテラシー向上による被害の減少

CYBER ATTACKERS
攻撃者

USER
ユーザ

CHECK POINT UTM ● UTM
ネットワークセキュリティ

Eye 24.7 Safety Zone ● エンドポイントセキュリティ
PC端末のセキュリティ

Eye 24.7 Work Smart Agent ● 情報漏洩対策ツール
内部不正対策・情報漏洩リスク可視化

FB SAT Mail ● 標的型攻撃メール訓練サービス
標的型攻撃メール教育

Fuva Brain ● カスタマーサポート
製品ごとのサポート

UTM・エンドポイントセキュリティのトリプルガード

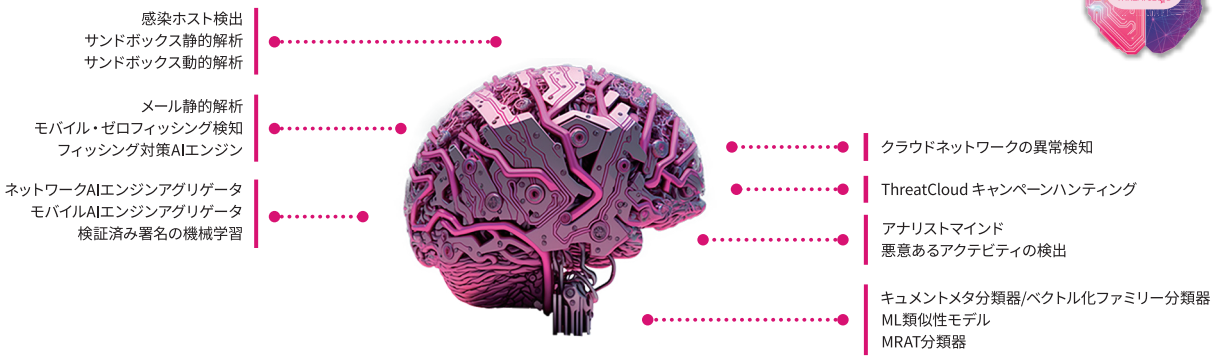
Eye“247”Safety Zone USAVVは、世界最高水準のセキュリティを誇る「CheckPoint」UTM と Fuva Brain の提供するエンドポイントセキュリティ「Eye“247”Safety Zone」、業務可視化ソフトウェア「Eye“247”WorkSmart Agent」3つのセキュリティで、従来型のセキュリティでは不可能だった多層防御型のセキュリティを実現し、企業の情報資産を外部・内部の脅威から守ります。

CheckPoint UTMのココが他社よりすごい！

CHECK POINT

■ ThreatCloudで使用されるAIベースのテクノロジー

様々なセキュリティ機能に関する75の脅威対策エンジン



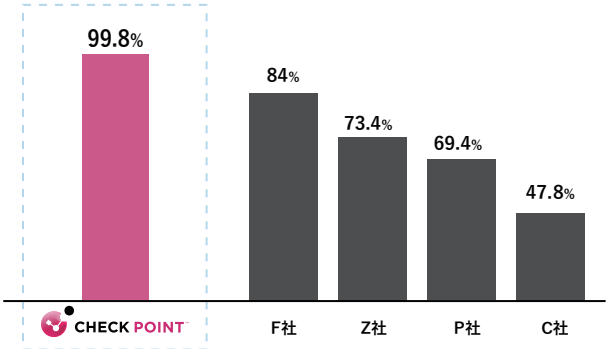
■ リアルタイムの最高レベルの脅威防御

Miercom
2024 セキュリティ ベンチマーク　第1位（2年連続）

CHECK POINT は
企業にとって最もリスクの高い
新種のマルウェアによるゼロデイ+1攻撃を

99.8% 阻止

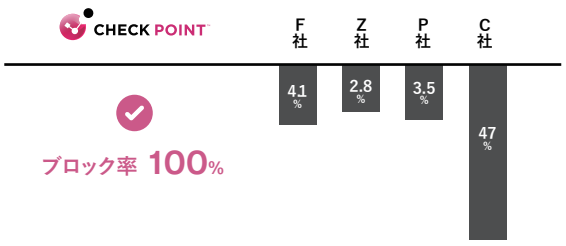
2024年セキュリティベンチマーク レポート
ゼロデイ+1に対するマルウェア防御率



■ フィッシングについての第三者機関検証

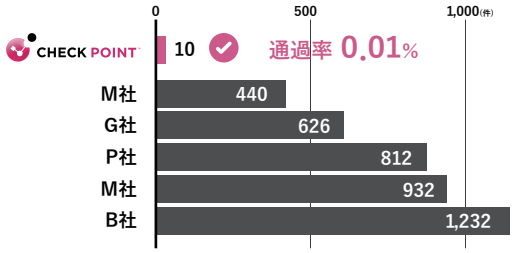
フィッシングリンクの見逃し、フィッシングEメールの通過数、ともに他社に負けない防御を実現しています。

フィッシングリンクの見逃し
（WEBブラウジング） Miercom

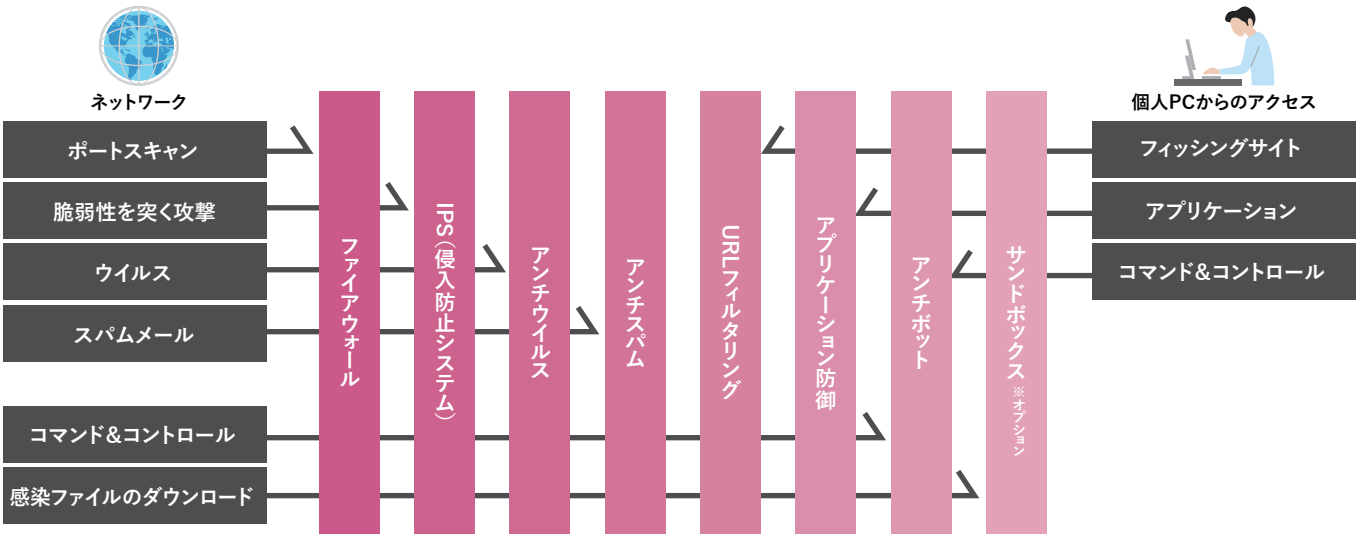


ブロック率 100%

10万件フィッシングメールを送付して
通過した数



多層防御で、様々な脅威からブロック



機能名	機能説明
ファイアウォール	アクセス防御・ユーザー認証・ネットワークアドレス変換（NAT）等のサービスを提供します。
侵入防御システム（IPS）	外部からの侵入や攻撃の前段階となる不審な通信を検知して遮断する機能です。
アンチウイルス	マルウェアなどの脅威となる通信を検知、評価し、自動的に遮断するなどの処理を行います。
アンチスパム	メールの送信元や内容を検査し、迷惑メールを検知、遮断します。
URLフィルタリング	接続先のURLを検査し、セキュリティ上危険なサイトや管理者が禁止したサイトへの接続を遮断します。
アプリケーション防御	通信を検査し、セキュリティ上危険なアプリケーションや管理者が禁止したアプリケーションを遮断します。
アンチボット	社内から発生した攻撃者（C&Cサーバー）への通信を検知し、自動的に遮断するなどの処理を行います。
サンドボックス※オプション	不審な動作を行おうとするプログラムをクラウド上の検査システムで評価し、未知のマルウェア感染から未然に防御します。

レポート機能でひと目で確認

シンプルで直感的なレポートを標準で提供。追加のライセンスやアプライアンスは不要。
通信量や検出したセキュリティ脅威等の情報を確認することが可能です。

1

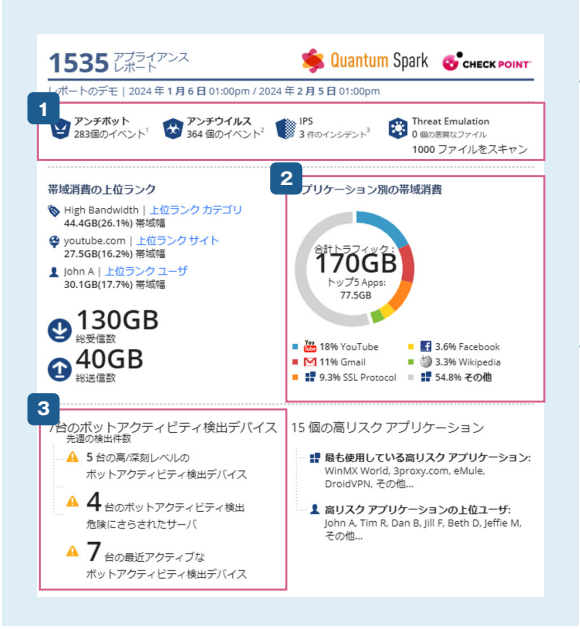
検出した脅威数がわかる

検知したボットウイルス数、マルウェア数、攻撃件数を表示します。

2

インターネットトラフィックの合計とアプリケーション毎の利用割合がわかる

インターネットトラフィックの合計と、アプリケーションごとの利用割合をグラフ表示します。



3

ウイルス感染している PC台数がわかる

以降のページで
感染したPCのIPアドレスがわかる

万が一ウイルス感染した PC やサーバがあった場合には、感染した PC 台数を表示。以降のページで感染した PC の IP アドレスを確認できます。

最高評価のBitdefenderエンジンによる総合的な防御

Eye“247” Safety Zone は世界 170 カ国 5 億台のネットワークを持つ Bitdefender 社のエンジンを採用。
Bitdefender 社は毎分 400 もの新しい脅威を発見しており、その高い防御技術は第三者機関でも常に高評価を得ています。

EDR（Endpoint Detection and Response）

エンドポイントにおける不審な挙動を検知し、迅速な対応を支援。

マルウェアなどの侵入を検知
管理者へアラートメール通知も可能

インシデントの詳細画面から
検知したモジュールやファイルの動作を表示

人工知能と機械学習をもとに迅速に脅威を検知するハイパーディテクト

Eye“247” Safety Zone は、ハイパーディテクトを搭載。既存のスキャン機能にさらなるセキュリティレイヤーが追加され、人工知能と機械学習に基づく強力なヒューリスティックを用いて新世代のサイバー攻撃に対抗します。
標的型攻撃を予測し、実行前の段階でマルウェアを検出する能力を持ち、シグネチャーベースや挙動スキャン技術よりも迅速に脅威を検出することが可能です。

01. 標的型攻撃

特定の個人や組織を狙ったサイバー攻撃のことで、攻撃者はターゲットの弱点を突くために綿密な情報収集を行い、カスタマイズされた手法を用います。

02. 不審なファイルや通信

マルウェアを含む可能性のあるファイルやフィッシング詐欺に関連する不審なメールやメッセージが含まれます。これらは主にユーザーの情報を盗んだり、システムに損害を与えることを目的としています。

03. エクスプロイト

ソフトウェアの脆弱性を悪用して不正なコードを実行するための手法です。これによって攻撃者がシステムやネットワークにアクセスし、データを盗むかシステムをコントロールすることが可能となります。

04. ランサムウェア

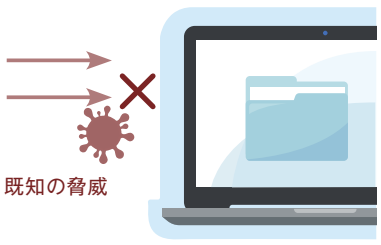
このマルウェアは、被害者のファイルやシステムを暗号化し、複合カギを提供する代わりに身代金を要求します。ランサムウェアは重要なデータやシステムを人質に、企業や個人に深刻な影響を与えることがあります。

05. グレーウェア

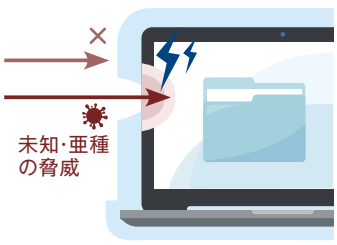
この種のソフトウェアは、明確な意思はないものの、望ましくない言動や迷惑を引き起こす可能性があります。アドウェアやスパイウェアなどがこれに含まれ、これらはユーザーのプライバシーやパフォーマンスに影響を与えることがあります。

ランサムウェアの動きを監視し、自動でファイルをバックアップ

アプリケーションが行うすべての動作を常時監視し、不審な兆候・異常な動作を検知します。
万が一の時は、ランサムウェアの動きより前に自動でファイルをバックアップします。



ランサムウェアをブロック



アプリケーションの動きを常に監視し
万が一の時も異常・不審な動きを検知

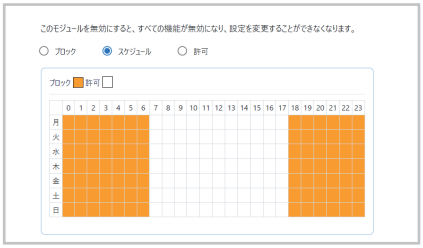
ランサムウェアの動きより前に
自動でバックアップ・保護

ネットワーク保護機能

フィッシング詐欺やランサムウェアの被害は近年増加を続けています。
Eye“247” Safety Zone は、HTTP(S) トラフィックをスキャンすることでフィッシングサイトや詐欺サイト、その他の悪意のある Web サイトを自動的にブロックします。
また、時間帯やカテゴリーを指定して、Web アクセスに制限を設けることもできます。

Webアクセスコントロール

時間帯を指定して Web アクセスに対して許可やブロックなど制限を設けることができます。



Webプロテクション

フィッシングサイトや悪意ある Web サイトを自動的にブロックし、不用意にオンラインで個人情報や機密情報を開示することを防ぎます。

ネットワーク攻撃検出

HTTP アプリケーションなど Web ブラウザを介さないネットワークアクセスに対しても攻撃を検出し、ブロックします。

レポート機能

期間中に Eye“247” Safety Zone で検知した内容を、日次 / 週次 / 月次 レポートとして、指定メールアドレスへ送信します。
※メールアドレスは最大 5 件まで登録できます。

マルウェア検知件数トップ10

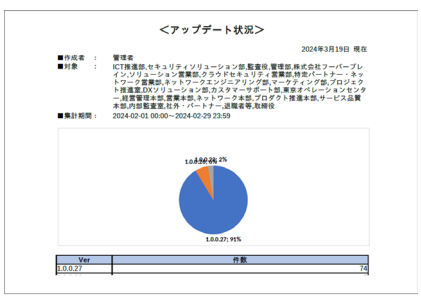
Eye“247”Safety Zone をインストールしている PC で検知されたマルウェアを 10 位までランキングにしたレポート

アンチフィッシング検知内容

Eye“247”Safety Zone をインストールしている PC で検知されたフィッシングサイトの URL を一覧にしたレポート

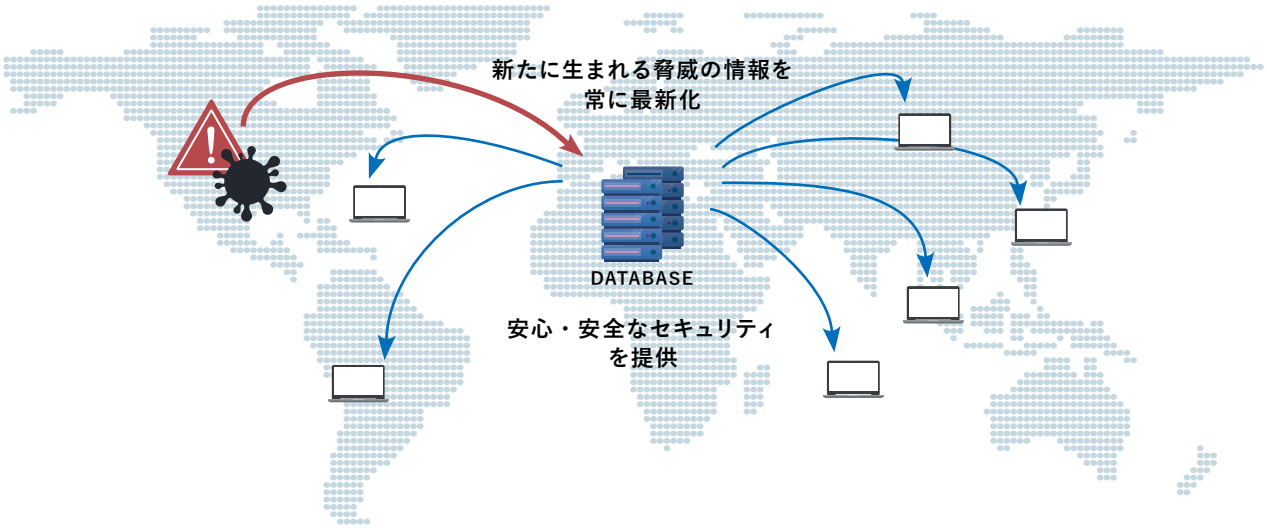
プログラムアップデート状況

インストールしている Eye“247”Safety Zone のバージョンを一覧にしたレポート



常に最高の検出力で端末を保護

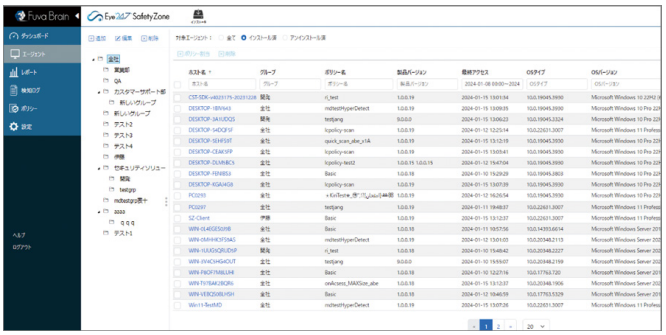
世界各地のユーザから集められる脅威情報をもとに、常にデータベースを更新しています。
テレワークや離れた拠点の PC 端末も、インターネットにつながっている限り、
世界最高クラスの安心・安全を実現できます。



集中管理

一目で社内の PC 状況がわかり、何かあった時もすぐに対応可能です。
操作しやすい管理画面で、レポートの確認も簡単にでき、運用者の負担を軽減します。

管理画面



PC やサーバーの機器情報や Safety Zone の更新状況、マルウェアの検知状況を一元管理することができます。
また、管理 Manager から全端末に対してセキュリティ設定（ポリシー）を一括変更することが可能です。

ダッシュボード

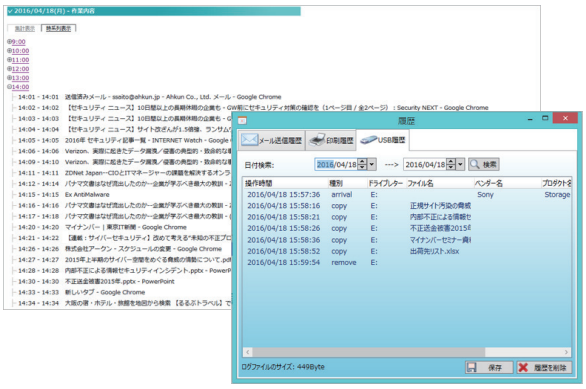
エージェントの適用状況や、検知数などをグラフでの可視化やランキング形式で表示します。
ダッシュボードを見ることで一目で自社のセキュリティ状況が分かります。

Eye“247” WorkSmart Agent

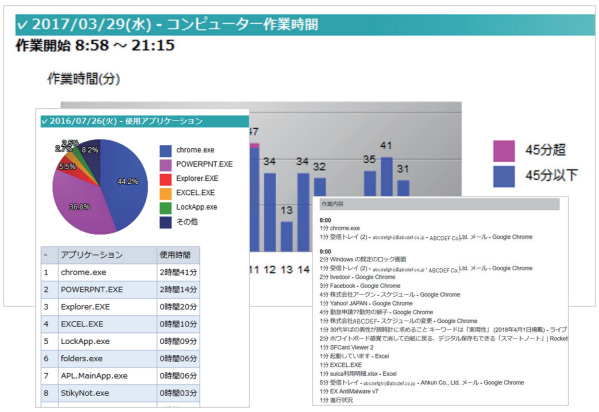
内部不正を未然に防ぎ、情報漏洩リスク・勤務実態を可視化

Eye“247” Work Smart Agent は、PC に常駐し、日々の作業内容を記録、任意設定した管理者に日報形式で業務報告を自動で行います。
「誰が、いつ、どのような作業を行っていたのか。」
これらの情報を把握することにより、社内での不正行為を抑止するだけでなく、日々の業務効率の改善にヒントを提供します。

情報漏洩対策



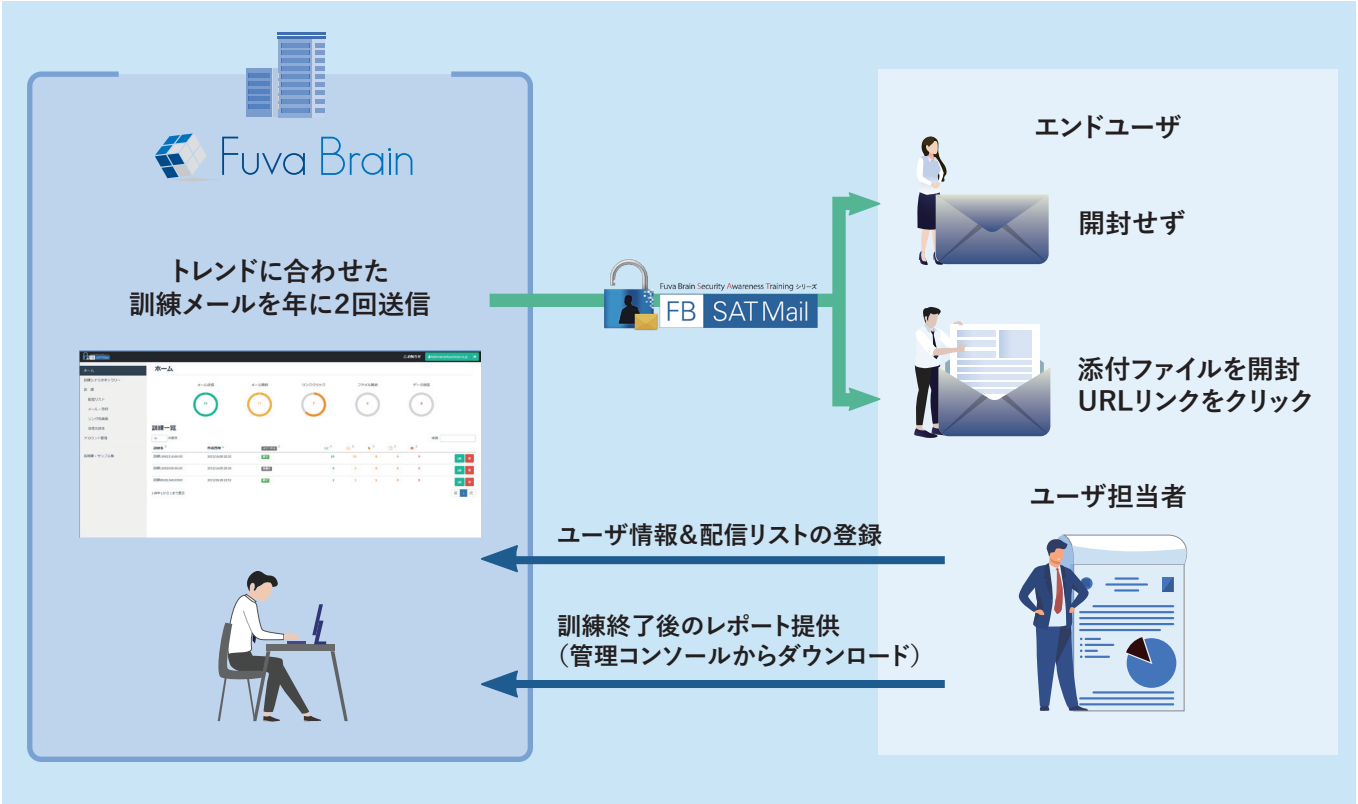
業務可視化



FB SATMail

標的型攻撃メール訓練でセキュリティ教育を支援

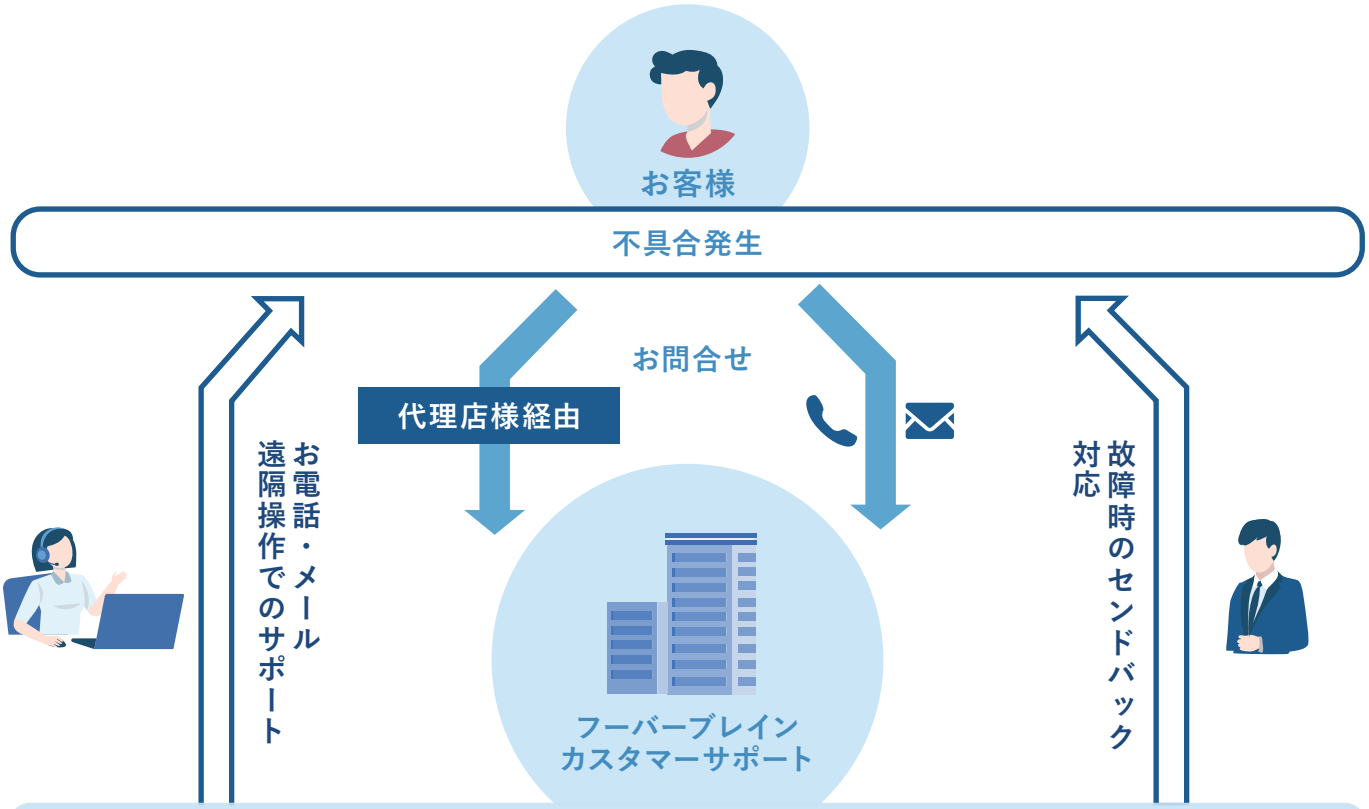
ユーザ様は、ユーザ情報と配信リストを登録するだけ。シナリオ選定・配信設定等の面倒な運用をフーバーブレインが対応します。
従業員向けに訓練用メールを年に２回自動で配信し、訓練終了後は管理コンソールから訓練結果レポートがダウンロードできます。
（メール配信は５年ライセンスの場合、最大１０回）



導入後もあらゆる面からサポート

ライセンス期間中は、専任のサポートスタッフによるサポートをご用意。
サポートサービスは初期費用に含まれているので安心してご利用いただけます。

フーバーブレイン　サポート体制

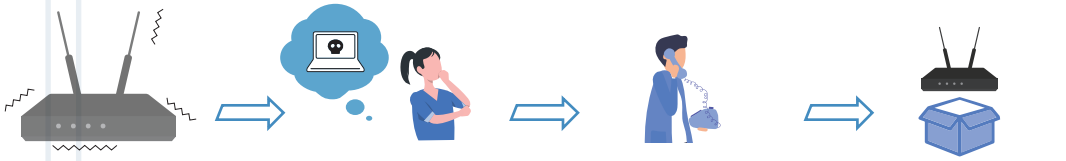


UTM へのサポート

- お電話口でのサポート
- 遠隔操作でのリモートサポート
  - 機器の状態の確認
  - 設定の追加・変更
  - ファームウェアアップデートの実施
- メールによるセキュリティレポートを定期配信

故障時も安心！代替機発送サービス

故障時は新品同等の代替機をお送りします。故障期間を最小限にし、安心して業務を継続していただけます。



ソフトウェアへのサポート※SafetyZone/WorkSmart Agent

- インストール手順のご案内
- 遠隔操作でのリモートサポート
  - 設定の追加・変更
  - ウイルス駆除支援
  - ※SafetyZone がインストールされている端末に限る

情報セキュリティ対策を支援

開発・発売元

Fuva Brain
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

5_2024.11

www.fuva-brain.co.jp

型番

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

200CL以上のモデルもございます。担当営業までお問い合わせください。

ソフトウェア動作環境

Eye247 Safety Zone

Eye"247" Safety Zone エージェントプログラム		
	Windows OS	Mac OS
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 / 10Sは非対応です。	Sonoma (14.0以上) Ventura (13.0以上)
CPU	クロック周波数1.5GHz以上（推奨 2GHz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	4GB以上（推奨8GB以上） ※EDR機能を有効にする場合　8GB以上（推奨16GB 以上）	4GB以上（推奨8GB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	

Eye"247" Safety Zone Manager	
Webブラウザ	Google Chrome（推奨）、Microsoft Edge
画面解像度	1680×1050以上(1920×1080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	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行われています。
※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2024年11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。