SS7000の主な仕様

	SS7000 Std	SS7000 Pro
本体寸法	約292(W)×43(H)×178(D)mm ※突起物およびアンテナを除く	
質量	約2.1kg	約2.2kg
環境温度	0～40℃	
相対湿度	30～80%(結露しないこと)	
電源／周波数	AC100V ±10% 50／60Hz	
最大消費電力	20W	23W
EMI／認証	日本:VCCI-A、JATE、電波法	
PC同時接続推奨台数	15台	60台
スループット	ファイアウォール:3.0Gbps／IPS:1.36Gbps／アンチウイルス:560Mbps	
インターフェース	USB 3.0×1　WAN:10／100／1000Mbps×1　LAN:10／100／1000Mbps×7(メンテナンス専用ポート×1含む) ※メンテナンス専用ポートにはお客様のネットワーク機器を接続できません。	
無線LAN規格	–	IEEE802.11 a／b／g／n／ac
付属品	ACアダプタ DC12V／4A	
オプション品	据置用品／壁掛用品	

ESET 動作環境※

	Windows	Mac
OS	Windows 7 Starter / Windows 7 Home Premium / Windows 7 Professional / Windows 7 Enterprise / Windows 7 Ultimate / Windows 8 / Windows 8 Pro / Windows 8 Enterprise / Windows 8.1 / Windows 8.1 Pro / Windows 8.1 Enterprise / Windows 10 Home / Windows 10 Pro / Windows 10 Enterprise	macOS Sierra 10.12 / macOS High Sierra 10.13 / macOS Mojave 10.14 / macOS Catalina 10.15 / macOS Big Sur 11
CPU	1GHz以上の32bitプロセッサ または 64bitプロセッサ (インテル Itanium および ARM プロセッサーを除く)	インテル プロセッサ (32bitまたは64bit) / Apple M1チップ (Rosetta2経由) ※PowerPCは非対応。
メモリ	Windows 7 / Windows 8 / Windows 8.1 の場合:1GB以上 Windows 10の場合:32ビット版 1GB以上 / 64ビット版 2GB以上	512MB以上
ハードディスク	1GB以上の空き容量	200MB以上の空き容量
ディスプレイ	Super VGA (1024×768) 以上	–

※Linux、Android、WindowsServerの動作環境は、ESETホームページを参照ください。

リモートコネクト動作環境

	Windows	MacOS	iOS/iPadOS	Android
OS	Windows 8.1／Windows 10	MacOS 10.14 Mojave／MacOS 10.15 Catalina／MacOS 11 Big Sur	iOS 12／iOS 13／iOS 14 iPadOS 13／iPadOS 14	Android 9／Android 10 ／Android 11
CPU	1GHz以上のプロセッサ またはシステム・オン・チップ(SoC)	–	–	–
メモリ	32bit版OS:1GB以上 64bit版OS:2GB以上	2GB以上	–	–
必須アプリケーション	Microsoft .NET Framework 4.0以上	–	–	–

サクサエコ商品

安全に関するご注意

●本商品ご購入後は、添付の「取扱説明書」をよくお読みの上、正しくお使いください。「取扱説明書」には、本商品をご購入されたお客様や他の方々への危害や財産の損害を未然に防ぎ、本商品を安全にお使いいただくために守っていただきたい事項を記載しています。
●水、湿気、湯気、ほこり、油煙などの多い場所には設置しないでください。火災、感電、故障などの原因となることがあります。

〔本体について〕●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。本製品を導入することによりその脅威を完全に取り除くことを保証するものではありません。●お客様の環境により別途HUBが必要な場合があります。●各種セキュリティ機能の有効期限は使用開始からSS7000 Std／SS7000 Pro／SS7000 Std(α)／SS7000 Pro(α)は5年間、SS7000 Std Plus／SS7000 Pro Plus／SS7000 Std(α) Plus／SS7000 Pro(α) Plusは6年間、SS7000 Std Plus+／SS7000 Pro Plus+／SS7000 Std(α) Plus+／SS7000 Pro(α) Plus+は7年間となります。有効期間が経過すると機能が停止したり、定義ファイルが更新されないなど、脅威の防御効果が著しく減少してしまいますのでご注意ください。●本製品に多くのトラフィック負荷がかかると、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。●ウイルス侵入防御／スパムメール・迷惑メール検知は本製品を経由するWeb、またはメール送受信に対して実施をいたします。●本製品は、外国為替および外国貿易法で定める規制対象貨物・技術に該当する製品です。この製品を輸出する場合または国外に持ち出す場合は、日本国政府の輸出許可が必要です。●本製品の補修用性能部品の最低保有期間は、販売終息後7年です。●Windows、Microsoft Outlook、Exchange Online、Internet Explorer、Microsoft Edgeは米国Microsoft Corporationの米国およびその他の国における登録商標または商標です。●Mac および Safari は、米国およびその他の国々で登録されたApple Inc.の商標です。●ESETは、ESET, spol.s r.o.の商標です。●Intel、Pentiumは、アメリカ合衆国およびその他の国におけるIntel Corporationの商標です。●カスペルスキー、Kasperskyは、Kasperskyの商標または登録商標です。●ALSIはアルプスシステムインテグレーション株式会社の商標または登録商標です。●PATLITEおよびパトライトは、株式会社パトライトの商標または登録商標です。●その他の製品名および社名などは各社の商標または登録商標です。●仕様は予告なく変更する場合があります。●カラーは印刷の都合上、実際とは異なる場合があります。

saxa

サクサ株式会社

本社/〒108-8050　東京都港区白金1-17-3　NBFプラチナタワー

■営業本部
オフィス営業部　ネットワーク営業G　☎(03)5791-3931
パートナー営業部　パートナー営業G　☎(03)5791-5524

●営業拠点
東北支社　☎(022)297-5835
東京支社　☎(03)5791-5530
中部支社　☎(052)220-3930
関西支社　☎(06)6367-0393
九州支社　☎(092)473-1511
札幌営業所　☎(011)281-1035
大宮営業所　☎(048)650-9311
静岡営業所　☎(054)653-7711
金沢営業所　☎(076)255-0393
高松営業所　☎(087)861-7450
広島営業所　☎(082)511-7555

●お客様相談室:0570-001-393　☎(050)5507-8039
URL　https://www.saxa.co.jp/　E-mail　customer@saxa-as.co.jp

●お問い合わせ・ご用命は

このカタログの記載内容は2021年6月現在のものです。

このカタログは再生紙を使用しております。　VEGETABLE OIL INK　このカタログは植物油インキを使用しています。　SA-0594

saxa

SS7000

さまざまなネットワークセキュリティの課題に応える、この一台を。

日々、多様化・巧妙化するネットワークの脅威。
今、どんなセキュリティ対策が必要だろうか。

大企業のみならず中小企業においても、さまざまなサイバー攻撃が急増。
ランサムウェアやリモートワークを狙った不正アクセスなど、多様化・巧妙化が進んでいます。
しかし、これらの脅威から守るためには、膨大な手間とコストがかかります。
このような課題に、高いセキュリティと低コストを実現した国産のサクサ UTM SS7000が応えます。
時代に必要とされるセキュリティ強化に、この一台を。

課題1〜4
会社の価値・信用を向上させるには？
P04〜05

課題5
安心・安全なネットワークを構築するには？
P06

課題6
社員のセキュリティ意識を高めるには？
P06

SS7000 7つの課題解決

課題7
万が一の時も安心なサポート体制とは？
P07

オプション
外出時のPCのセキュリティを強化するには？
P08

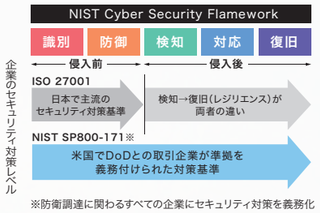
オプション
攻撃メールに備えた社内体制を構築するには？
P10

オプション
リモートワークでのウイルス感染を防ぐには？
P09

■企業を取り巻くセキュリティ環境の変化

世界的に発展するセキュリティ標準化

米国、EUをはじめ世界的にセキュリティ標準化の流れは急速に進んでいます。2019年より日本の防衛省もNIST SP800-171相当のセキュリティ要求事項を調達基準に盛り込んでいます。



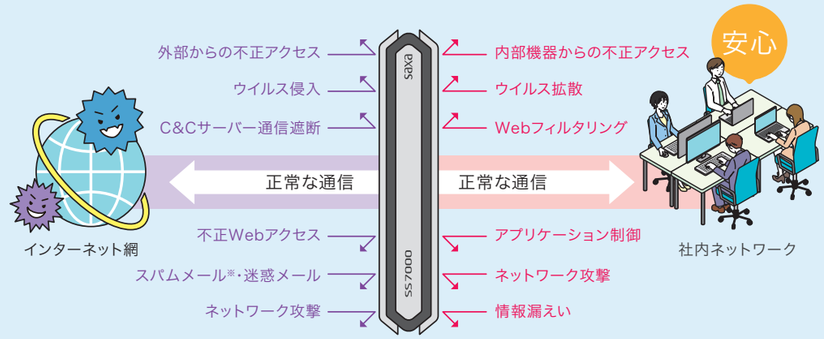
※防衛調達に関わるすべての企業にセキュリティ対策を義務化

働き方改革によるセキュリティリスク

働き方改革として推奨されている「リモートワーク」では、社外の業務は既存のセキュリティ環境の外であるため、情報漏えいなどのリスクが高まります。安心・安全なセキュリティは、企業の信頼向上、経営目標の達成に貢献します。

SS7000がさまざまなセキュリティリスクから御社を守ります

サクサUTM SS7000とは？ 外部からの脅威と内部からの脅威、どちらにも対応できます



インターネット網から来るさまざまな脅威から統合的に社内ネットワークを守ります

社外への情報漏えいを防ぎます

※スパムメールは件名にタグを付与。

安心1 高評価のエンジン搭載だから、安心できる

年間最優秀製品賞
(Product of the Year 2020)を受賞

既知ウイルス検出テストVB100アワード
通算100回以上受賞

アンチウイルス
kaspersky
AV comparatives Product of the Year 2020

エンドポイントセキュリティ
eset ※αシリーズにバンドル
VB100 AWARDS

P08へ

17年連続シェアNo.1
WEBフィルタリング ALSI

大手携帯キャリアほか	国内最大級	登録コンテンツ	Webアクセス網羅率
1,500万	147	43億	98%
端末以上の導入実績	カテゴリ	以上	で国内最高水準

安心2 高速通信だから、いつものように作業がはかどる

前機種（SS5000Ⅱ）と比べ、通信速度は大幅アップ。高速スループット（高速通信）のままセキュリティを確保でき、業務の生産性を落としません。

スループット	SS7000
ファイアウォール	3.0Gbps
IPS	1.36Gbps
アンチウイルス	560Mbps

通信速度大幅アップ

安心3 信頼の日本製、迅速丁寧なサポート体制

わからないこと、困ったことがあれば、サクサコールセンターへ。
PCウイルス駆除サービスやリモート保守サポートを行っています。有償のセキュリティサービスもご用意しています。

P07へ

さまざまなセキュリティリスクに対応。会社の信頼性向上に貢献

PROBLEM 課題 1

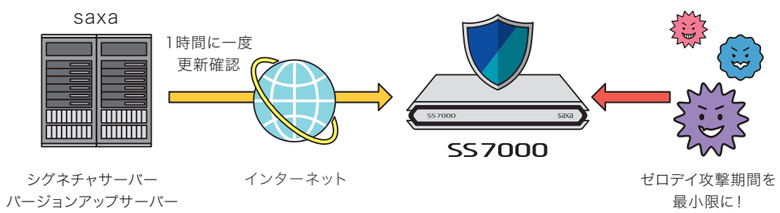
最新のネットワークウイルスに対応しているか気になる

新しいマルウェアは、毎日100万個作られていると言われているため、非常に危険です。
感染した場合、データの破損や、機密情報、個人情報の漏えいにつながる恐れがあります。

解決 SOLUTION

［ウイルスのデータパターンを自動更新］

1時間に一度、サーバーと通信し、シグネチャ（ウイルス検知ファイル）を更新。最新のセキュアなネットワーク環境を実現します。バージョンアップによる新セキュリティ機能も随時公開します。



常に最新のセキュアなネットワーク環境を実現

PROBLEM 課題 2

取引先からUSBメモリを渡されたけど、社内のPCに差し込むのは不安

USBメモリから感染するリスクは非常に高く「警視庁からのお知らせ」でもリモートワークで
使用したUSBメモリは、社内ネットワーク接続前のウイルススキャンを要請しています。

解決 SOLUTION

［USBメモリスキャン］

業務上やむを得ずUSBメモリを使用する際は、SS7000本体にUSBメモリを差し込むことで、ファイルをカスペルスキーエンジンで検疫することができます。

簡単2ステップ！メモリ検疫

STEP. 1
SS7000背面にある「USBポート」に、スキャンしたいUSBメモリを挿入

STEP. 2
PCからSS7000にブラウザでアクセス。必要なファイルを選んで、ダウンロードするだけで完了

PCへのウイルス感染を防ぐことができる

PROBLEM 課題 3

メールを送ったあとで、違う添付ファイルだったことに気づいた

情報漏えいは宛先間違いや添付ファイルの誤りなどによるものが非常に多いです。※
人の注意力には限界があり、必ずミスは発生してしまうものと想定すべきです。

※IPA「情報セキュリティ10大脅威（組織）」より、メール誤送信を含む「不注意による情報漏洩」は第7位

解決 SOLUTION

［メール誤送信防止］
［メール添付ファイル自動暗号化］

メール送信を一定時間（30秒～10分）保留でき、時間内でキャンセルが可能。また、添付ファイルの自動暗号化で誤送信による情報漏えいを防ぎます。

※本機能は、IPv6、Exchange Online、Microsoft Outlookにおけるリッチテキスト形式には未対応となります。

メールによる情報漏えいを防ぐことができる

PROBLEM 課題 4

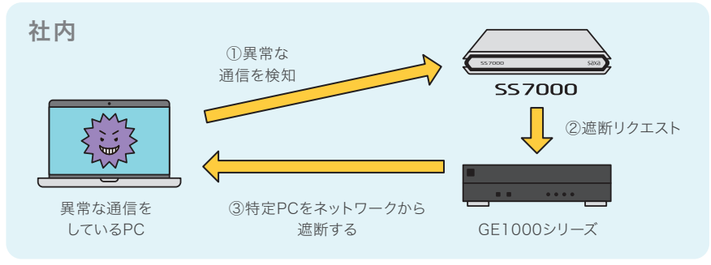
PCのウイルス感染対策も大事だけど、感染後の対策も必要だよな

社外で会社のPCが感染した場合、
社内ネットワークへ接続すると、社内で拡散してしまいます。

解決 SOLUTION

［情報セキュリティゲートウェイ連携］

サクサGE1000シリーズ（別売）との連携で、異常な通信をしているPCを検知、ネットワークからの遮断が可能です。社内でのウイルス拡散を防ぎます。



ウイルス感染後の拡散を食い止められる

さまざまなビジネス環境で
安心・安全なネットワークを構築

PROBLEM 課題5

UTMを買っても、VPNルーターが必要だったり、設定変更したりと大変

拠点間VPNを構築する場合、VPNルーターが必要です。さらに拠点が増えた場合、
設置済のルーターの設定をすべて変更する必要があり、設置工事費用が負担となります。

解決 SOLUTION

［簡単VPN構築］

SS7000はルーターでも動作が可能です。また、管理サーバー上で接続したい拠点を選択するだけで簡単に拠点間VPN接続が可能です。いろいろな機器を用意しなくても良いので、経費削減につながります。

SS7000だけで簡単にVPNを構築できる

脅威の「見える化」で
社員のセキュリティ意識向上に貢献

PROBLEM 課題6

UTMの動作状態って、どうやって確認するの？

見えない場所に置いている場合も多いため、UTMの動作状態がわかりにくく、
セキュリティ状態をすぐに確認できていないのが現状です。

解決 SOLUTION

オフィスに馴染むデザインとわかりやすい表示で、攻撃・検疫状況をタイムリーに確認可能

［見える化サイト］

お客様専用のWebページで
状況をわかりやすく表示

［視認性パネル］ アイコンでSS7000の状態をわかりやすく

［ボタン電話装置との連携］

ボタン電話装置のLCDにSS7000の
ウイルス検知数等を表示

［警告ランプ］
（USBパトライト）（別売）

パトライトでSS7000の
状態を光で表現

PHE-3FB3N-RYG

※株式会社パトライトの製品です。
※本製品はオプションとなります。

セキュリティ状態を視覚的に把握できる

迅速丁寧なサポート体制で更なる安心

PROBLEM 課題7

UTMが故障した場合、修理中のウイルス感染が怖いな

万が一UTMが故障した場合、修理中にウイルス感染リスクが発生してしまいます。
また、ウイルス感染時はお客様だけで対処できません。

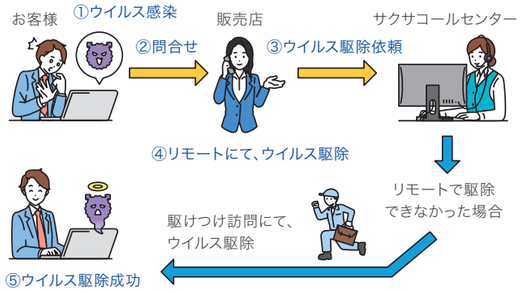
解決 SOLUTION

さまざまなサポートで、万全の態勢を構築できます

［PCウイルス駆除サービス］（無料）

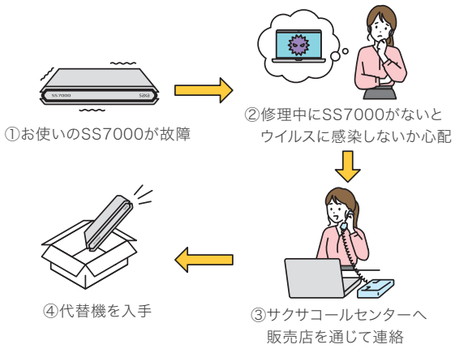
PCのウイルス感染時には、リモートまたは現地訪問（離島を除く）にてウイルス駆除をサポートします。

※ウイルスがデータ破損した場合の復旧を保証するわけではございません。



［代替機発送サービス］（有償サポート／要登録）

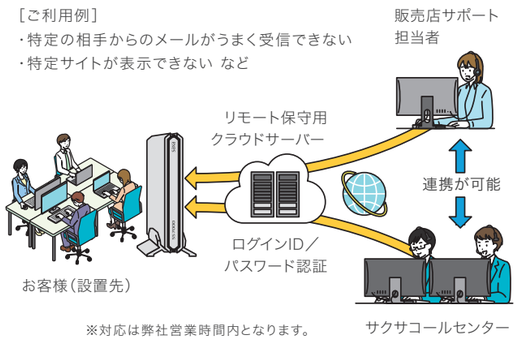
故障時は新品同等の代替機をお送りします。故障期間を最小限に止め、安心して業務の継続が可能です。



［サクサコールセンターでのリモート保守サポート］（無料）

お客様のSS7000にリモートで直接接続するため、ルーターの設定変更は不要です。サクサコールセンターと連携し解決にあたります。さまざまなご相談に迅速丁寧に対応いたします。

［ご利用例］
・特定の相手からのメールがうまく受信できない
・特定サイトが表示できない など

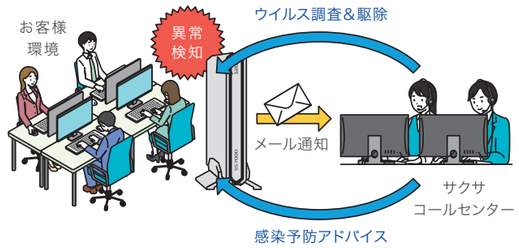


※対応は弊社営業時間内となります。

［C&C検知サーバー通信 監視・駆除サービス］（有償サポート／要登録）

社内の異常な機器は、解決しない限り攻撃は続きます。そのため通信状況をセキュリティのプロが監視。ウイルスの拡散、C&Cサーバー通信※を検知した場合、遠隔で駆除を行い、感染予防のアドバイスをします。

※C&Cサーバーとは、不正なソフトウェアが仕込まれたPCに対し、攻撃の命令を行うサーバーのことです。



万が一の時も安心して作業ができる

SS7000(α)シリーズ オプション 「ESET」「リモートコネクト」を同梱

社外でも安心
場所を選ばない働き方をサポート

PROBLEM 課題

最近PCを持ち出すことが多いけど、ウイルスに感染したらどうしよう

社外でのPC作業時はセキュリティ環境が整っていないため、感染する可能性があります。
また、UTMだけでは、社内ネットワークでウイルスが拡散するリスクが残っています。

解決 SOLUTION

[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」の追加で、社外PCをさまざまなウイルスやフィッシングサイトなどからダブルガード。セキュリティ対策が飛躍的に向上します。

エンドポイントセキュリティとは？

PCやサーバー、スマートフォンなどIT端末に対し、サイバー攻撃や内部不正を想定したセキュリティ対策を施すことを指します。

数多くの企業が導入している「ESET」を採用

導入実績 391,000※社！
※2018年12月31日時点。法人向け製品（スクールパックを除く）

ESETが選ばれる理由

新種・亜種のマルウエアまで高確率で検出・駆除

独自の検出技術により多くの未知のウイルスを既知・早期検出し駆除します。

低負荷設計でスキャン中の作業も軽快

PCへの低負荷でBCNセキュリティユーザー調査でも高評価を獲得しました。

フィッシング対策

フィッシングコンテンツを配布していることが判明しているWebページをブロックします。

Webカメラアクセス制御

望ましくないアプリケーションがPCのカメラにアクセスするのを禁止できます。

技術力のあるサポートで、購入後の対応も万全

技術力のあるスタッフが迅速丁寧に対応します。

https://eset-info.canon-its.jp/business/

PCのセキュリティをより強固に

リモートワークや外出中でもセキュアな環境を実現
生産性向上に貢献

PROBLEM 課題

リモートワークでのウイルス感染が話題だけど、このPCは大丈夫かな

リモートワークのニーズが増加していますが、個人のPCやネットワーク環境は、
オフィスに比べてセキュリティが不十分なため、ウイルス感染リスクが高まります。

解決 SOLUTION

[リモートコネクト]

社内ネットワークに直接接続できる「リモートコネクト」を用意。VPN環境を簡単に構築できます。オフィス同様に社内のIT資産をそのまま使用でき、UTM検疫を可能に。社内の資産を無駄なく活用できます。

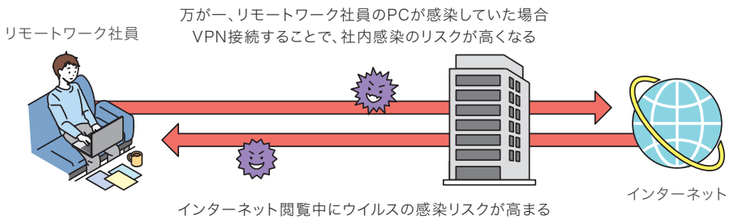
リモートコネクトの特長

- ブリッジ／ルーターモードで使用可能
- Windows／Mac Android／iOSで提供
- UTM検疫が可能

従来のVPN接続 <Before>

リモートワークは、オフィスと比べセキュリティレベルが低くウイルス感染リスクが高くなります。
また感染した場合、VPNを通じて社内感染のリスクが高いです。

オフィスのネットワークは、セキュリティ対策をしているけど、自宅や公衆Wi-Fiのセキュリティ対策は？



リモートコネクトを使った、新しいVPN接続 <After>

リモートワークの通信も、オフィスに接続したSS7000で検疫可能！
「オフィス」と「リモートワーク」のセキュリティ対策を一括し、無駄なくIT資産活用できます！

SS7000のみで、セキュアなVPN環境を構築可能。社内感染を未然に防止。

社外でも会社と同様のセキュリティ環境に

定期的なメール訓練で
社内のセキュリティ意識向上に貢献 オプション

PROBLEM
課題

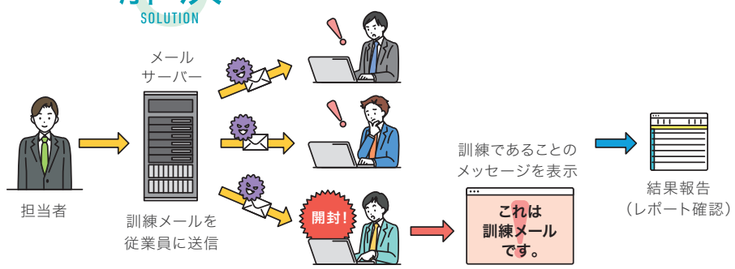
社員があやしいメールを開かないようにしたい。どう教育したらいいのかな

標的型攻撃メールは添付ファイルの開封でウイルスに感染します。そのためメールの予防訓練を行うことが大切ですが、業務の中で継続して訓練メールを実施していくのは大変です。

解決 SOLUTION

［標的型攻撃メール訓練］

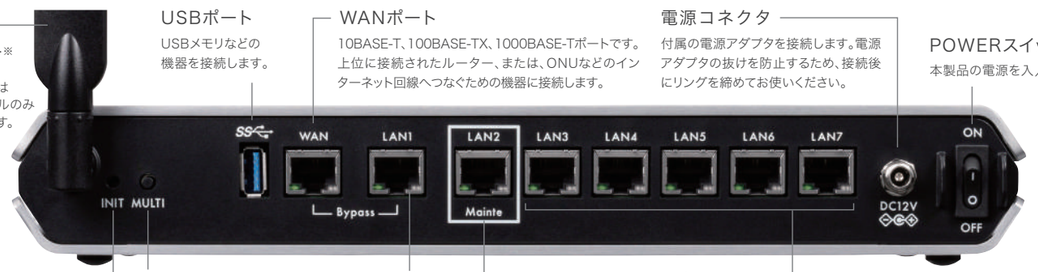
標的型攻撃を模した訓練用メールを従業員に送信。訓練により、社員の意識が向上し、メールからの感染を減らすことができます。



個々のセキュリティ意識を高められる

［ハードウェア仕様］ アルミ筐体による放熱性を高めてファンレス化を実現

信頼の日本製



基本機能一覧

外部からの脅威

外部からの不正アクセス

ファイアウォール機能・IPS/IDS機能で、外部からのデータ通信を監視し、社内ネットワークへの不正アクセスを防ぎます。

ウイルス侵入 kaspersky

ファイルダウンロードやメール受信時に、AI分析した定義ファイルを使用しウイルスを検知駆除します。

C&Cサーバー通信遮断

不正なプログラムが仕込まれたPCに対して攻撃の命令を行うサーバーとの通信を検知し、ブロックします。また、指定したメールアドレスに対して該当PC情報を通知します。

不正Webアクセス kaspersky

ホームページを閲覧するときの通信を監視。閲覧している画像やダウンロードするファイルにウイルスが混入していないか検知駆除します。

スパムメール・迷惑メール kaspersky

スパム、フィッシングメール等を検知し、偽造ホームページ等によるIDやパスワードの盗難を防ぎます。また、メール本文内の不正Webサイトへのリンクも検知します。

ネットワーク攻撃

外部からのDoS攻撃など、ネットワーク攻撃を防ぎます。

内部からの脅威

内部機器からの不正アクセス

パソコンが乗っ取られ、外部のWebサーバーなどへの攻撃や迷惑メール送信の踏み台などに悪用されることを防ぎます。

ウイルス拡散 kaspersky

ファイルアップロードやメール送信時に、ウイルスを検知駆除します。

Webフィルタリング ALSI

アダルトサイトや薬物、犯罪に関する業務上不適切なWebサイトへのアクセスをブロックします。

※カテゴリー単位でWebアクセスの許可/禁止
※Webページ本文中の特定単語が含まれていた場合、Webアクセスをブロック

アプリケーション制御

通信内容からアプリケーションを特定し使用を制限します。
例：Winny、BitTorrentなどP2Pアプリ、メッセンジャーアプリ

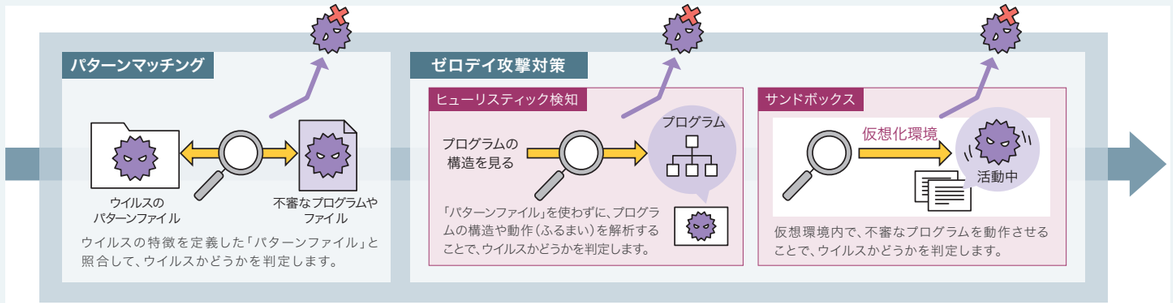
ネットワーク攻撃

内部機器からのDoS攻撃など、ネットワーク攻撃の拡散を防ぎます。

情報漏えい対策

メールによる情報漏えいを防ぎます。

対策パッチが公開される前の攻撃を検知（ゼロデイ攻撃対策）



システム構成