SS6000Ⅱの主な仕様

	SS6000Ⅱ Std	SS6000Ⅱ Pro
本体寸法	約291(W)×43(H)×178(D)mm ※突起物およびアンテナを除く	
質量	約2.3kg	
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	15W	18W
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:2.95Gbps／IPS:500Mbps／アンチウイルス:340Mbps	
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は10/100Mbpsのみ対応。※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 8.1 / Windows 8.1 Pro / Windows 8.1 Enterprise / Windows 10 Home / Windows 10 Pro / Windows 10 Enterprise / Windows 11 Home / Windows 11 Pro	macOS Sierra 10.12 / macOS High Sierra 10.13 / macOS Mojave 10.14 / macOS Catalina 10.15 / macOS Big Sur 11 / macOS Monterey 12
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 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 Windows 11の場合:4GB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／ Windows 11	macOS Catalina 10.15／ macOS Big Sur 11／ macOS Monterey 12	iOS 13／iOS 14／iOS 15 iPadOS 13／iPadOS 14／ iPadOS 15	Android 10／Android 11／ Android 12
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	–	–	–

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は有効期限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低下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。●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。

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
ＩＣＴ営業部　パートナー営業Ｇ　☎(03)5791-5524

●オフィス営業部
東京第一支社　☎(03)5791-3931　札幌営業所　☎(011)281-1035
東京第二支社　☎(03)5791-5530　大宮営業所　☎(048)650-9311
東北支社　☎(022)297-5835　静岡営業所　☎(054)653-7711
中部支社　☎(052)220-3930　金沢営業所　☎(076)255-0393
関西支社　☎(06)6367-0393　高松営業所　☎(087)861-7450
九州支社　☎(092)473-1511　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2022年5月現在のものです。

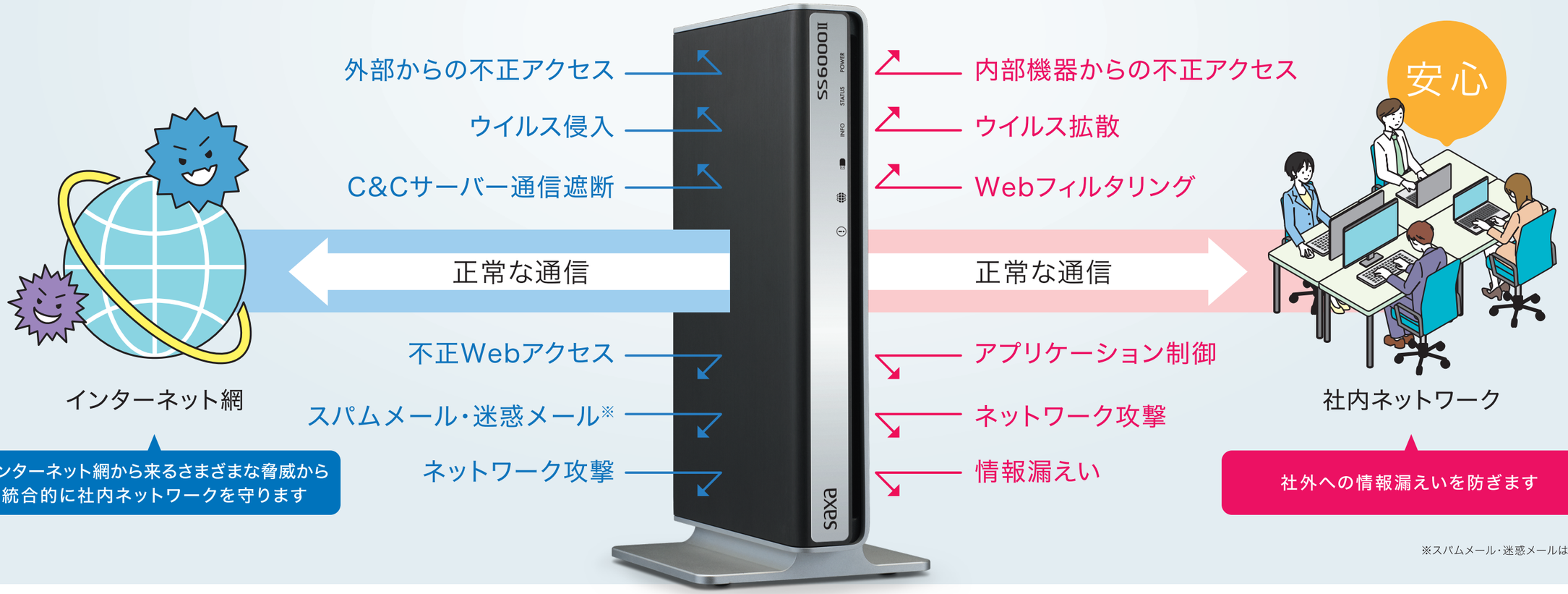
このカタログは再生紙を使用しております。　このカタログは植物油インキを使用しています。　SA-0638

SS6000Ⅱ

サクサUTM(統合脅威管理アプライアンス)

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。

SS6000Ⅱがさまざまなセキュリ ティリスクから御社を守ります



※スパムメール・迷惑メールは件名にタグを付与。

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 SS6000Ⅱ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。

SS6000Ⅱで課題解決

課題1〜5 会社の価値・信用を向上させるには？ P04〜P05

課題6 万が一の時も安心なサポート体制とは？ P06〜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 リモートワークでのウイルス感染を防ぐには？ P09

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

安心1 高評価のエンジン搭載だから、安心できる

18年連続シェア No.1

大手携帯キャリアほか 1,500万 端末以上の導入実績

国内最大級 144 カテゴリ

既知ウイルス検出テストVB100アワード 通算100回以上受賞

Webフィルタリング ALSI

登録コンテンツ 43億 以上

Webアクセス網羅率 98% で国内最高水準

エンドポイントセキュリティ eset ※αシリーズにバンドル

P08へ

安心2 高速通信だから、いつものように作業がはかどる

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。

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。新たにサイバー保険サービスもご用意しています。

P06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］

シグネチャ（ウイルス定義ファイル）を定期的に更新し最新のセキュアなネットワーク環境を実現します。

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

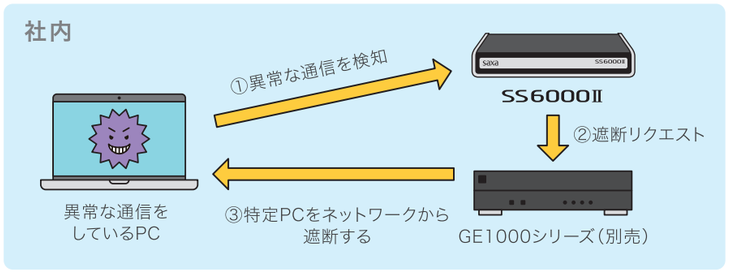
PCのウイルス感染対策も大事だけど、感染後の対策も必要

社外で会社のPCがウイルス感染した場合、
社内ネットワークへ接続すると、社内でウイルス拡散してしまい、被害が拡大します。

解決 SOLUTION

［情報セキュリティゲートウェイ連携］

異常な通信をしているPCを検知しネットワークから遮断して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

PROBLEM 課題 3

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

［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します。

［ボタン電話装置との連携］

ボタン電話装置のLCDにSS6000Ⅱのウイルス検知数等を表示します。

［警告ランプ］（USB信号灯）（別売）

SS6000Ⅱの状態を光で表現します。

※株式会社パトライトの製品です

セキュリティ状態を視覚的に把握できる

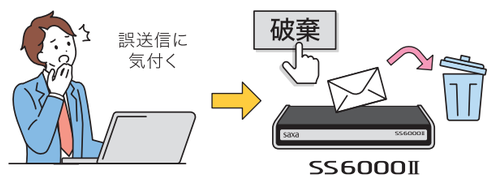
PROBLEM 課題 4

メールの誤送信が不安

解決 SOLUTION

［メール誤送信防止］

送信メールを一定時間（30秒～10分）保留でき、キャンセルすることができます。



メールによる情報漏えいを防ぐことができる

※本機能は、IPv6と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。

PROBLEM 課題 5

VPN構築したい

解決 SOLUTION

［簡単VPN構築］

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。

SS6000ⅡだけでVPN構築できる

迅速丁寧なサポート体制で更なる安心

PROBLEM
課題 6

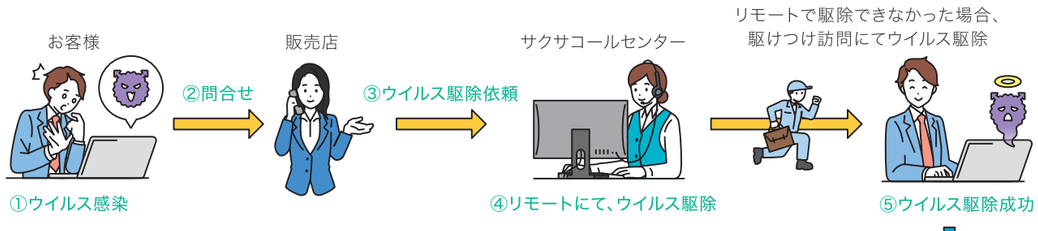
セキュリティに詳しくないから、UTM導入後も不安だな

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

[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。



[サイバー保険サービス] (無料) NEW!

SS6000Ⅱにはサイバー保険サービスが標準で付帯されています。サイバー攻撃等でSS6000Ⅱを通過して侵入したウイルスに対し、PCウイルス駆除サービスで駆除できなかった場合、ウイルス感染による情報漏えいの損害賠償や、システムの復旧費用として、最大50万円を補償します。

加入条件	SS6000Ⅱシリーズ設置のお客様 (標準付帯)		
補償金額	最大 **50万円**／年		
補償対象装置	デスクトップPC	ノートPC	サーバーPC
補償対象作業	●再インストール ●買い替えによる復旧 ●データ復旧	●再インストール ●データ復旧	●再インストール ●買い替えによる復旧 ●データ復旧

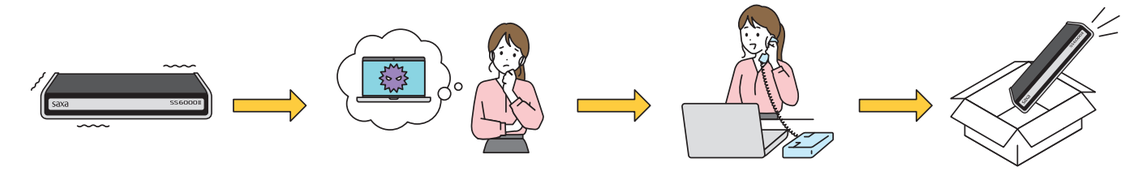
※本サービスの詳細は、サクサHPに記載の規定をご確認ください。
※補償対象装置のOSは、Microsoft社がサポートしているWindows OSとなります。

MS&AD 三井住友海上

解決 SOLUTION

[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。

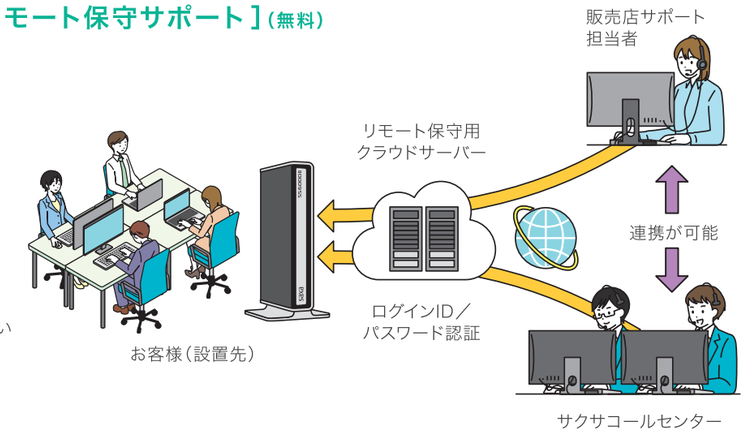


[サクサコールセンターでのリモート保守サポート] (無料)

お客様のSS6000Ⅱ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。
※リモート設定変更は、有償となります。



[C&Cサーバー通信検知 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。

万が一の時も安心なサービス

SS6000Ⅱ（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？

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］

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します。

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）

数多くの企業が導入している「ESET」を採用

ESETが選ばれる理由

新種・亜種のマルウェ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の負荷を軽減することで軽快な動作を実現し、第三者機関において高い評価を獲得しています。

フィッシング対策

フィッシングサイトへ誘導する有害なメールを検出し、フィッシングサイトへのアクセスを防止します。

デバイスコントロール

USBメモリやCD／DVDなどの光学式メディアからのマルウェア感染防止として、各種外部デバイスへのアクセスを制御します。

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。

ESETの詳細についてはこちら！

SS6000Ⅱ＋ESETのダブルガードについて動画公開中！

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、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。

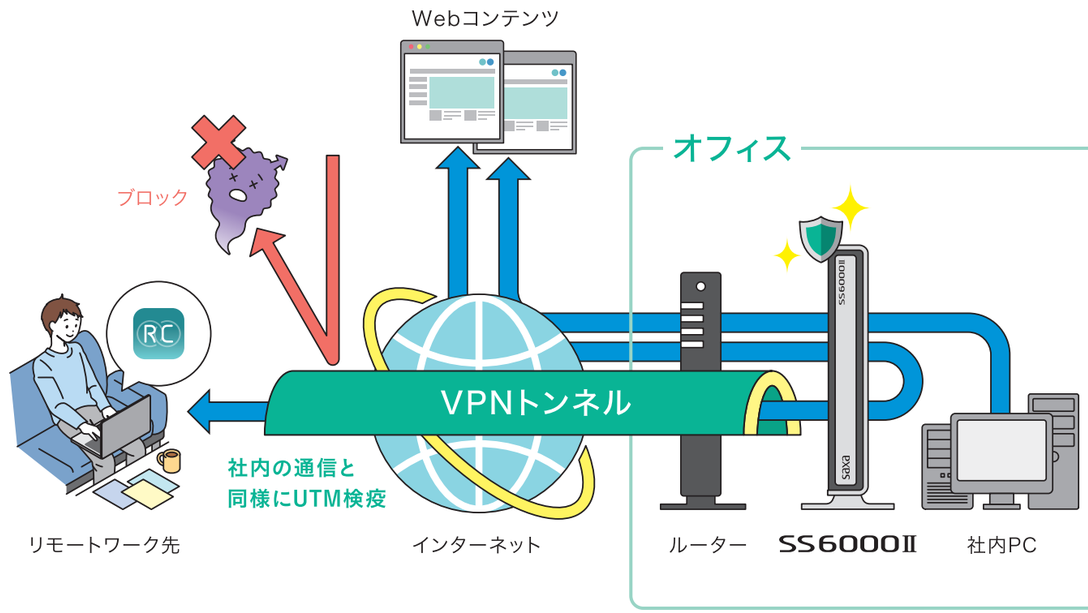
解決 SOLUTION

［リモートコネクト］

社内ネットワークに直接接続し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検疫も可能になります。

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



リモートコネクトの詳細について動画公開中！

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

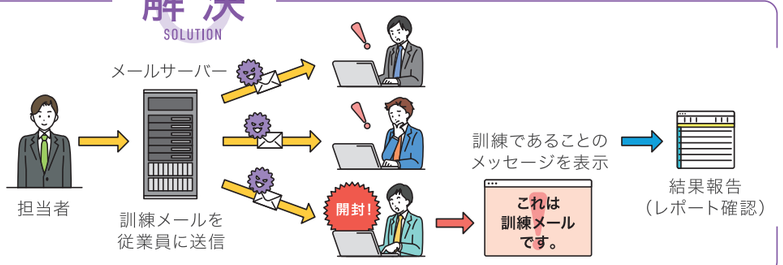
社員があやしいメールを開かないよう、どう教育するか

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。

SOLUTION
解決

［標的型攻撃メール訓練］

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。

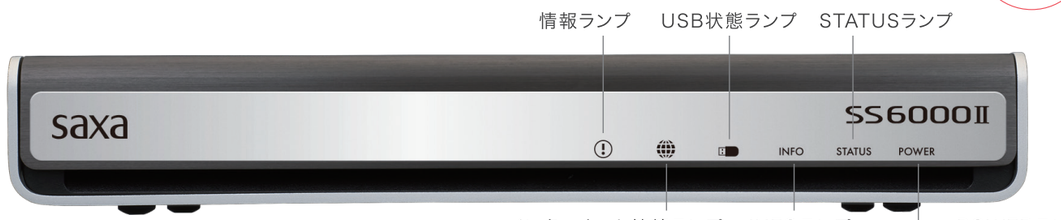


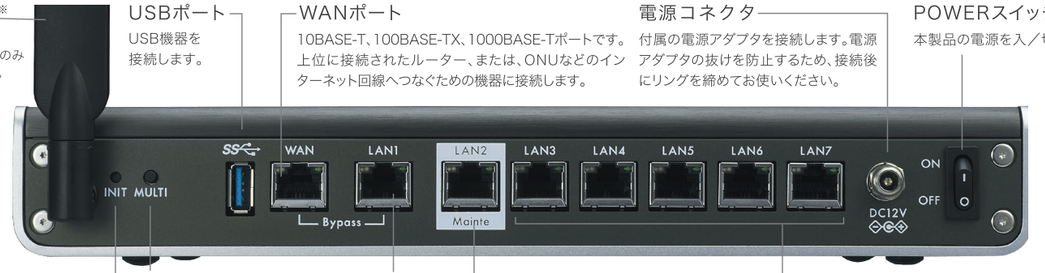
個々のセキュリティ意識を高められる

信頼の日本製

［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

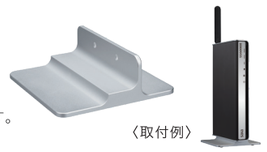




［オプション］

据置用品

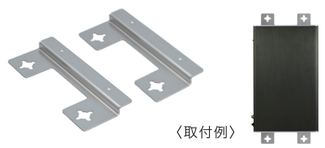
空いたスペースにスッと収まる、場所を取らない縦置きが可能になります。



〈取付例〉

壁掛用品

壁に掛けて設置できるので、設置場所を選びません。



〈取付例〉

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

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

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

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。

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

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/禁止が可能

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

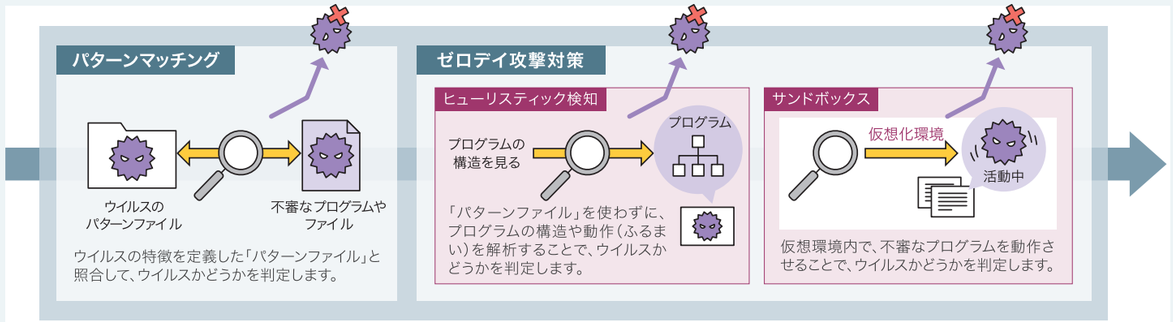
ネットワーク攻撃

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