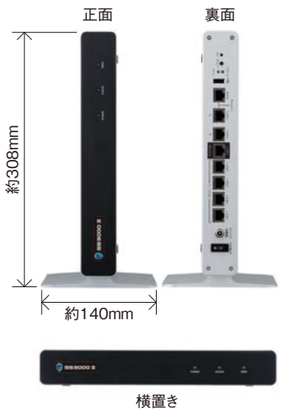
システム構成

※Wi-Fi機能はProのみ搭載

SS3000Ⅱの主な仕様

	Std	Pro
本体寸法	約290（W）×43（H）×180（D）mm　※突起物およびアンテナを除く	
質量	約2kg	
環境温度	0～40℃	
相対湿度	20～80%（結露しないこと）	
電源／周波数	AC100V　50／60Hz	
最大消費電力	40W	
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：1Gbps／アンチウイルス：150Mbps／IPS：300Mbps	
インターフェース	USB2.0×1　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	—	IEEE802.11a／IEEE802.11g／ IEEE802.11b／IEEE802.11n 周波数帯域：5GHz帯、2.4GHz帯
付属品	ACアダプタ　DC12V／3.3A	
オプション品	据置用品（スタンド）／壁掛用品（Wall）	



αScan エンドポイントセキュリティ動作環境

クライアントプログラム動作環境

OS	Windows 10／8.1／8／7／Vista、Windows Server 2012／2008（32／64ビット版）
CPU	Intel Pentium4　1.3GHz相当以上
メモリ空き容量	256MB以上
ディスク空き容量	インストール時に300MB以上
Web環境	Internet Explorer 9以上［注意事項］マシンへのログオン時のみ、すべての機能が利用可能です。マシン速度、環境により十分なパフォーマンスが発揮できない場合があります。

管理マネージャー動作環境

Web環境	Internet Explorer 9以上
画面解像度	1,024×768以上

※αScanエンドポイントセキュリティのライセンス数：Std（α）は15、Pro（α）は30

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SS3000Ⅱ Std／SS3000Ⅱ Pro／SS3000Ⅱ Std（α）／SS3000Ⅱ Pro（α）は5年間、SS3000Ⅱ Std Plus／SS3000Ⅱ Pro Plus／SS3000Ⅱ Std（α）Plus／SS3000Ⅱ Pro（α）Plusは6年間、SS3000Ⅱ Std Plus＋／SS3000Ⅱ Pro Plus＋／SS3000Ⅱ Std（α）Plus＋／SS3000Ⅱ 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。●本製品はフレッツ光ネクスト、Bフレッツ、フレッツADSLで提供しているIPv6サービスには対応しておりません。●ウイルスブロック／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は、米国マイクロソフトコーポレーションの米国およびその他の国における登録商標です。●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 Lab ZAO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。

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

■オフィス営業本部
ネットワーク営業部　☎(03)5791-3931

●営業拠点

東北支社	☎(022)297-5835	札幌営業所	☎(011)281-1035
東京支社	☎(03)5791-5530	大宮営業所	☎(048)650-9311
中部支社	☎(052)220-3930	静岡営業所	☎(054)653-7711
関西支社	☎(06)6367-0393	金沢営業所	☎(076)255-0393
九州支社	☎(092)473-1511	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　http://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2017年9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-0454

サクサ UTM（統合脅威管理アプライアンス）

SS3000 II

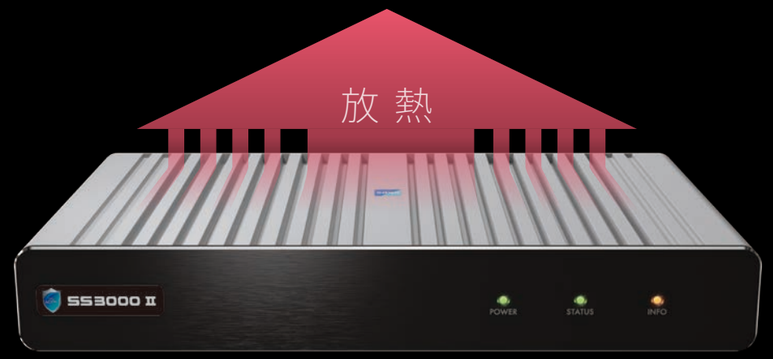
強固なセキュリティで、
あなたのオフィスを守ります。

Office AGENT
オフィスエージェントシリーズ

オフィスを静かに、美しく守る。

サクサのUTMは一般的なUTMとは違い、アルミファンレス筐体を採用しています。
高い放熱性と静音性を備えながら、エレガントにオフィスを守ります。

高い放熱性と静音設計



UTMが外部からの攻撃をシャットアウトするときに、多くの熱が発生します。
SS3000Ⅱは、ヒートシンク型のアルミファンレス筐体により、堅牢な防御を長期間安定して提供します。

アルミ製パネル

筐体はすべてアルミ製＋アルマイト加工で作られているため、樹脂筐体と比べ美しく堅牢です。
また、鉄板筐体と比べ軽量のため、壁掛け設置も可能になっています。

機能性・信頼性を極めた美しいデザイン

素材を一から見直し、ヒートシンク型アルミ筐体を採用しました。アルミの質感を活かした高級感あるデザインとともに、高い放熱性・堅牢性を実現。
また、ファンレス設計により、騒音の発生や機器内への埃の侵入も防いでいます。

多様なバリエーションと柔軟な設置形態

サクサのUTMは、お客様のご要望に合わせて、多様なバリエーションをラインアップしています。Wi-Fi搭載のProに加え、さまざまな設置形態に対応する縦置きスタンド、壁掛けブラケットを用意しています。

ビジネスに安心をもたらす
強固なネットワークセキュリティを。

Office AGENT
オフィスエージェントシリーズ

オフィスのネットワークセキュリティに必要な機能を1台に集約。
外部からの攻撃や内部からの情報漏えいを防ぎます。

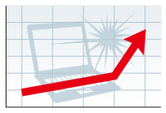
■ウイルス定義ファイルの5年間自動更新
（Plusは6年間、Plus＋は7年間）

- ■世界トップクラスのエンジン（カスペルスキー）搭載
- ■カテゴリ選択による簡単URLフィルタリング機能
- ■対策パッチが公開される前の攻撃も検知（ゼロデイ攻撃対策）
  ※詳細はP6をご参照ください。
- ■メール添付ファイル自動暗号化機能

SS3000 II

Office AGENTシリーズ

クライアントのオフィス業務に関する
「困った」をトータルにサポート！



ウイルス対策ソフトだけではセキュリティは不十分です。

あなたのPCをおびやかす脅威は今も増え続けています。

情報漏えい

インターネットの情報（データ）は、第三者に盗み見られる可能性があります。

・オンラインショッピングでクレジットカード番号が盗まれる。
・電子メールが盗み見られる。

不正アクセス

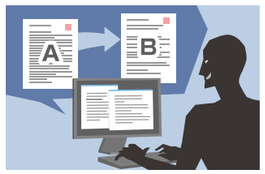
インターネットに接続したサーバは悪意ある人から侵入の標的になる場合があります。

・機密情報や顧客情報などの重要データが漏えい。
・Webページが改ざんされる。
・社内カメラが閲覧される。

なりすまし

銀行や有名企業を騙ったなりすましメールで偽サイトへ誘導し、IDやパスワードをだまし取られる可能性があります。

・不正にシステムにアクセスされる。
・詐欺の被害にあう。



改ざん

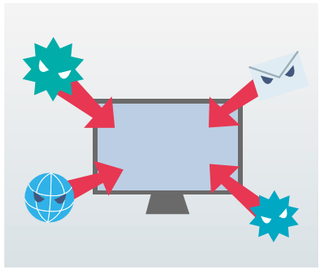
電子データは紙に書いた情報と違い、不正にアクセスされ、改ざんされる可能性があります。

・品物を発注する際に、情報が改ざんされて相手に届く。

基本機能強化

情報漏えいには万全の対策を取っておきたい。

UTMのセキュリティ機能をさらに強化。世界トップクラスのエンジン（カスペルスキー）を搭載しています。



ウイルスや迷惑メールなど、ネットワークは日々攻撃を受けています。

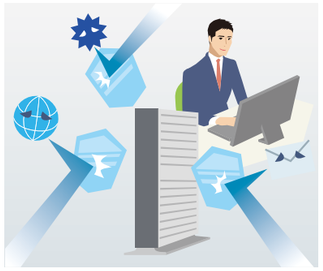
SS3000IIにおまかせください。ネットワークの入り口に設置するだけ。

1台で、さまざまな攻撃から大切なデータや情報機器を守ります。

PLATIAII（ビジネスホン）/SB2100（サーバ）連携

ウイルスの防御状況を確認できると安心なのだが…。

ウイルスの防御状況や迷惑メールを遮断した内容を、手元の電話機で確認できます。



ウイルス防御、迷惑メール検知など、日々活躍するSS3000II。

防御状況を、SB2100を通して電話機に通知。

電話機の液晶ディスプレイに表示されるので、防御状況を確認できます。

リモート保守

導入した後もスピーディーにサポートしてくれるの？

障害時など、サポートセンタへのお問い合わせに対して、リモートで迅速に対処します。

問題発生などの際は、サポートセンタに問い合わせ。

※すべての障害や設定変更をリモートで対応できるわけではありません。

リモートで状況確認や障害の切り分けを行います。

お客様に承諾をいただいた上で設定変更を行い、解決します。

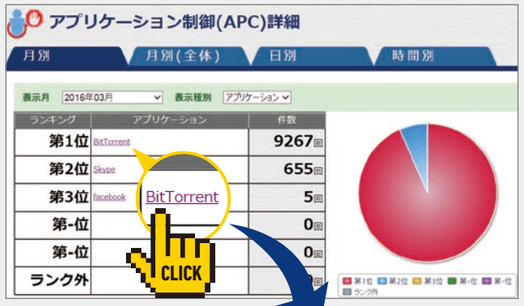
■ サクサUTM見える化ツール

お客様専用のWebページをご用意し、「脅威からの防御状況」を分かりやすく表示。
導入効果を簡単・手軽、しかも視覚的に把握できます。

■SS3000Ⅱご購入のお客様には追加費用なしでご利用いただけます。
■Webで確認ができるので、タブレットなどでも利用できます。
■特別なツールのインストールなどは不要です。

さまざまな脅威からの防御状況を、ランキング形式で表示

見える化ツールでは、全体の防御状況以外にも、種別ごとのランキング形式で表示できます。また、「詳細」ボタンクリックで、各脅威の詳細情報も表示可能です。例えば、アプリケーション制御の詳細画面では、「表示種別」をアプリケーション単位で表示させたり、そのアプリケーションの使用者単位で表示することで、状況を把握し、的確な対策を立てることができます。



どのPCがアプリケーションを使用しているか、一目で分かります。

確認できる防御項目

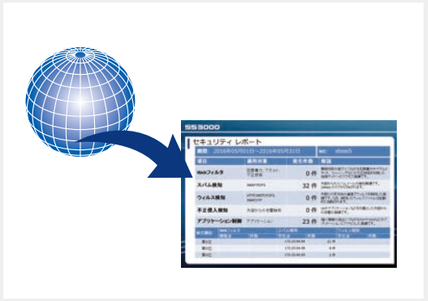
- アンチウイルス……ウイルス名
- アンチスパム……送信元メールアドレス
- IPS攻撃(不正侵入防御)…攻撃対象ソフトウェア名
- DoS攻撃(攻撃防御)……自社への攻撃回数
- URLフィルタリング……アクセス制限したサイトのURL
- アプリケーション制御 ……通信制限したアプリケーション

＜その他、以下項目も表示＞
- 脅威の全体傾向確認：同サービスご利用のお客様の統計情報から全体の傾向を把握
- セキュリティニュースの表示

詳細レポートファイル出力で、ブロック状況を毎月把握

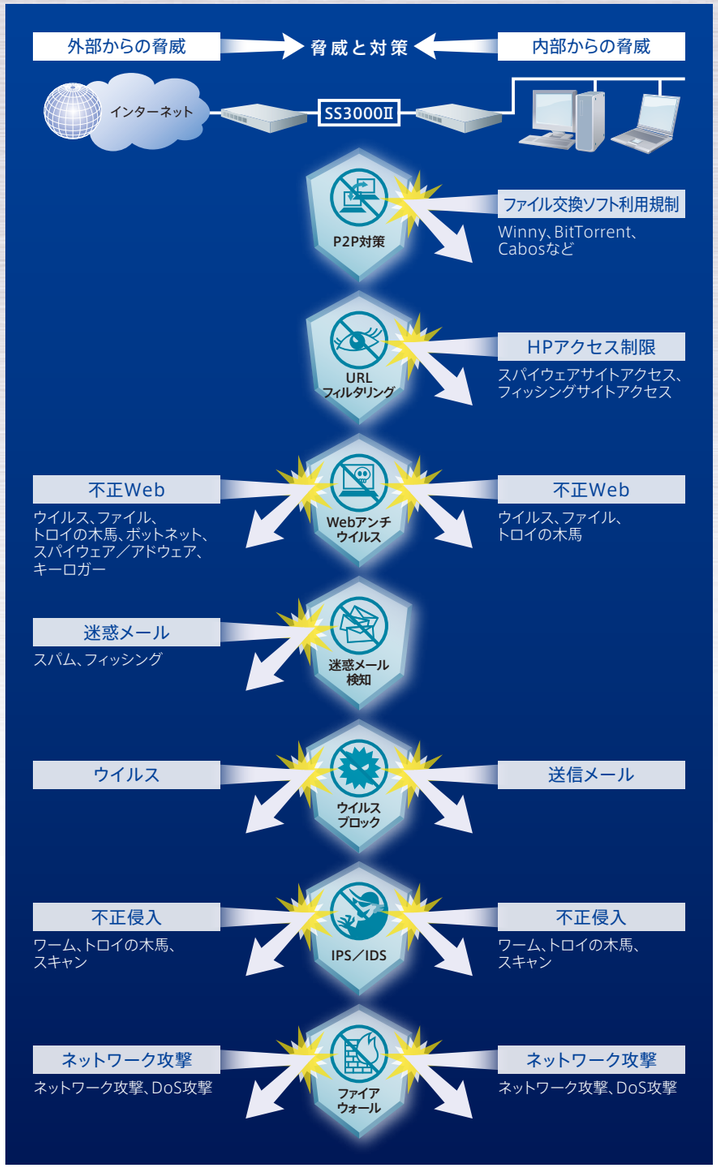
見える化ツールから、詳細レポート(PDF形式)をダウンロードできます。また、指定したメールアドレスに対して、セキュリティ結果を毎月送信することも可能です。資料化することで、Webアクセスの必要がなく、社内会議などで使用できるので便利です。

毎月メールで、セキュリティ結果を通知。



見える化ツールから、詳細レポートファイルをダウンロード。

SS3000Ⅱがさまざまな脅威からブロック！



P2P*、メッセンジャーアプリの防御

P2P通信を遮断することができるので、セキュリティ対策を行っていない相手や悪意のある相手からのウイルス感染を防ぐことができます。
＊P2Pとはインターネットを介して相手のパソコンと1対1で通信を行い、画像などのファイル交換を行うソフトウェア。

URLフィルタリング機能

あらかじめ指定したホームページカテゴリを選択することにより、ホームページへのアクセスを禁止できるので、業務効率の低下を抑えることができます。ギャンブルウェブサイト、アダルトサイト、麻薬関連など、50以上のカテゴリにてURLフィルタリングが可能です。

Webアンチウイルス機能

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チェックします。

迷惑メール検知機能

不要な広告やウイルスが添付されたメールを検知。業務効率の低下や偽造ホームページなどでのIDやパスワードの盗難を防ぎます。

IPS／IDS機能

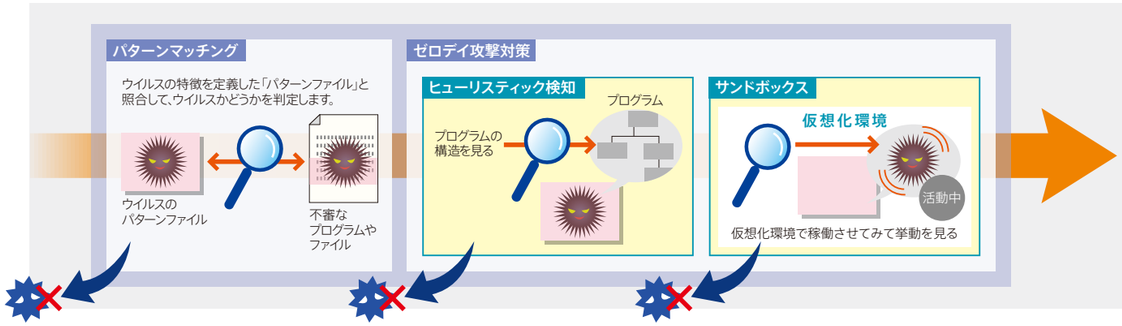
IPSとは、Intrusion【侵入】Prevention【防止】System【システム】の略。IDSとは、Intrusion【侵入】Detection【検知】System【システム】の略。インターネット上からのさまざまな攻撃から守ります。

ファイアウォール機能

データ通信の状況や利用するソフトウェアなどにより、社内ネットワークにデータを通過させるか否かを判断し、不正なアクセスを防ぎます。

対策パッチが公開される前の攻撃も検知(ゼロデイ攻撃対策)

- ヒューリスティック検知
  「パターンファイル」を使わずに、プログラムの構造や動作(ふるまい)を解析することで、ウイルスかどうかを判定します。
- サンドボックス(仮想環境)
  仮想環境内で、不審なプログラムを動作させることで、ウイルスかどうかを判定します。



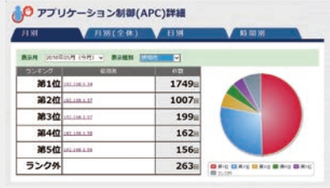
機能UP

見える化ツールの情報表示拡張

より詳細な内容を確認できます。現状の脅威を把握することで、迅速な対策を立てることができます。

ウイルス検出結果から、受信者の特定が可能です。

脅威サイトへアクセスしたPCの特定が可能です。



アプリケーション制御の結果を新たに追加しました。

機能UP

ホワイトリスト登録の簡略化

URLアクセス／メール受信時に、誤って規制･スパム判定された場合は、その場で管理者権限による規制解除が可能です。

URLフィルタ：ブロックイメージ図

SPAMメール検知イメージ図

管理者は、表示されたURLをクリックするだけで、ホワイトリスト登録を行い、ブロック、検知を解除することができます。

機能追加

メール添付ファイル自動暗号化機能追加

添付ファイルを暗号化して、メール送信が可能です。その後、パスワードメールを送信します※。

※自動設定の場合：受信者にパスワードが通知されます。手動設定の場合：送信者にパスワードが通知されます。

SS3000Ⅱラインアップ

	Std						Pro					
	標準	Plus	Plus+	(α)	(α)Plus	(α)Plus+	標準	Plus	Plus+	(α)	(α)Plus	(α)Plus+
PC同時接続推奨台数	15						60					
Wi-Fi搭載	–						○					
ウイルス定義ファイル自動更新年数	5	6	7	5	6	7	5	6	7	5	6	7
αScanソフトウェアライセンス	–	–	–	15	15	15	–	–	–	30 60*	30 60*	30 60*

＊オプションで追加30ライセンスあり。
※SS3000Ⅱ本体とαScanの自動更新数は同じです。※オプションで先出しセンドバック保守契約あり。

αScan（クライアントPC用セキュリティ管理ツール）

エンドポイントセキュリティ

マルウェア（Malicious Software）とは、ウイルスはもちろん、不正侵入や情報漏えいにつながるスパイウェアなどの不正プログラムやファイル交換ソフトなどです。これにより、迷惑メールの発信源にされたり大量のデータを送出して、プロバイダから契約解除になる事例も増加しています。

ウイルス対策	高い検知力で、ネットワーク内のあらゆる侵入経路から、ウイルスの侵入を防ぎ、駆除します。
不正プログラム対策	ウイルス対策製品では見つかりにくい、スパイウェアなどのプログラムを検知、駆除します。
危険なプログラム対策	ファイル交換ソフトによる情報漏えい事件が後を絶ちません。8,000種以上のファイル交換ソフトを隔離します。

集中監視セキュリティ

パソコン集中管理機能

更新期日が過ぎていないか、最新のウイルス対策データをアップデートしているか、検知したウイルスをきちんと処理しているかなどの煩わしい作業を管理者に代わってすべて自動で実行し、各クライアントパソコンを常に最新のセキュリティレベルに保ちます。

USBセキュリティ

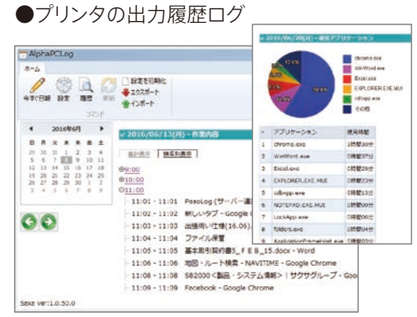
挿入時オートスキャン機能

USBメモリは手軽で便利なツールである反面、マルウェアを媒介させる危険なツールにもなります。ARCは、USBメモリの実行時に自動でスキャンし、問題があれば警告します。

内部統制セキュリティ

パソコンの業務内容を日報形式で管理者へメール送信

業務に無関係な操作を監視･抑止することがコンプライアンス上とても大切です。
●パソコンの利用時間統計
●パソコンの利用アプリケーション統計
●インターネットの閲覧履歴ログ
●プリントへの透かし印刷、利用制限
●プリンタの出力履歴ログ



ウイルス感染PCヘルプサポート［登録不要］

［1］ウイルス駆除サービス

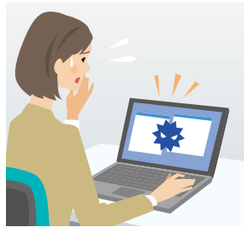
SS3000ⅡとαScanでガードしていますが、それでも万が一ウイルスに感染した場合には、PCに対しリモートでウイルス駆除をサポートします。

※SS3000Ⅱαシリーズのみのサポートです。

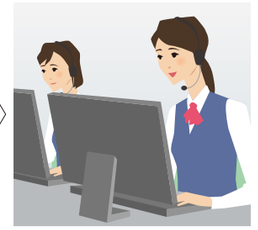
［2］ウイルス感染義援金サービス UTM業界初!*

［1］でウイルス駆除ができなかった場合、義援金をユーザ様へお支払いします。

※1台の「SS3000Ⅱ」においてライセンス年数にかかわらず1回までの給付となります。義援金は一律20万円です。
※義援金給付には条件がありますので、規定を確認してください。
※SS3000Ⅱαシリーズのみのサポートです。



お使いのPCがウイルスに感染。



ウイルス感染PCヘルプサポートセンタへ販売店様を通じ障害連絡。

リモートでウイルスの駆除を行います。

それでもウイルスを駆除できなかった場合は、義援金を給付します。

＊無償のサービスとして、UTMとエンドポイントの組合わせ商品でUTM業界初（当社調べ）