SOPHOS
Security made simple.

CUSTOMER CASE STUDY

Customer-at-a-Glance

ビジュアルテクノロジー株式会社
東京都台東区柳橋2-1-10 第2東商センター

業種
ハイパフォーマンスコンピューティング(HPC)
機器製造

社員数
25名

Webサイト
https://www.v-t.co.jp/

ソフォスソリューション
Sophos XG Firewall
Sophos Central Endpoint Protection Advanced
Sophos Intercept X

ソフォスカスタマー
ソフォス製品導入年数：3年

ハイパフォーマンスコンピューティング(HPC)機器を取り扱うビジュアルテクノロジー。顧客のセキュリティニーズの高まりを受け、まずは自社で最新のソフォスソリューションを導入した。それによって安全性が向上し、セキュリティビジネスを推進する環境が整った。

“ソフォスソリューションの導入によって、高度な脅威に対するセキュリティ環境を構築できただけでなく、運用管理の手間も省けました。このソリューションのメリットを多くの企業に知ってもらいたいですね。”

鬼澤慎氏
執行役員 HPC/エンタープライズ事業本部 本部長（写真左）

“「Sophos XG Firewall」は
ネットワーク状況をモニタリングし、
ネットワークとセキュリティを
オールインワンで管理できる製品です。
製品に対する信頼に加え、
ソフォスのテクニカルサポートが
力強くバックアップしてくれることも
今後の運用で安心できるポイントに
なりました。”

鷲尾浩伸氏
HPC事業本部 生産技術統括部 生産サポート部 部長

「The Personal Supercomputing Company」という経営ビジョンを掲げるビジュアルテクノロジー。HPCの拡大と普及を目指し、HPC を多く利用する大学や研究機関（民間含む）だけでなく、様々な企業にも製品を提供している。大学や研究機関ではLinux や UNIX などのシステムが数多く稼働しており、それらに対応するウイルス対策製品のラインナップをそろえるセキュリティ企業としてソフォスの存在を知った。顧客からの薦めもあり、その後、ソフォスの集中管理サーバ「Sophos Enterprise Console」とアンチウイルスソフト「Sophos Endpoint Protection」を利用し始めた。

ビジネスチャレンジ

ネットワーク機器ベンダーのファイアウォールルータを利用していたが、ビジネスの拡大に向け、ネットワークセキュリティのレベル向上とリモートアクセス環境の整備が必要だと考えた。また、未知の脅威や新種のランサムウェアウェアへの対策として、エンドポイントの強化も検討した。

▶セキュリティレベルの向上とリモートアクセスの実現
▶簡単なセキュリティ管理とコスト削減
▶未知の脅威や新種のランサムウェアウェアへの対策として
　エンドポイントの強化
▶ファイアウォールとエンドポイントの自動連携による管理工数の削減

ビジュアルテクノロジーは、すでにソフォスの集中管理サーバ「Sophos Enterprise Console」とアンチウイルスソフト「Sophos Endpoint Protection」を利用していたが、ランサムウェア対策やエクスプロイト対策などをより強固に、より管理しやすくしたいと考えた。通常、ファイアウォールで脅威を検知した場合、IT管理者が対象のエンドポイントを特定し、ネットワークから切り離す。エンドポイントで脅威を削除した後、ネットワークに接続させるが、脅威が多くなるにつれ、IT管理者がこれらの作業に費やす時間が多くなる。そのため、IT管理者に掛かる負荷が少ないソリューションを探した。

テクノロジーソリューション

ネットワークセキュリティの向上のため、ソフォスの次世代ファイアウォール「Sophos XG Firewall」を導入した。同製品はネットワーク機能とセキュリティ機能を搭載し、Web管理コンソールから簡単に管理できる。
未知の脅威や新種のランサムウェアウェアへの対策として、クラウド管理型エンドポイント保護ソリューション「Sophos Central Endpoint Protection　Advanced」と、クラウド管理型シグネチャーレスマル

ウェア対策ソリューション「Sophos Intercept X」も導入。「Sophos Intercept X」はランサムウェア対策機能の「CryptoGuard」を搭載する。
「Sophos XG Firewall」と「Sophos Intercept X」を連係させた。それによって、ソフォスが提唱するネットワークとエンドポイントの自動インシデント対応である「Synchronized Security」で管理工数を削減し、IT管理者に掛かる負荷の軽減を図った。

▶Sophos XG Firewall

次世代ファイアウォール。基本的なネットワーク機能だけでなく、他社製品ではオプションとなることが多いSSL-VPN機能も標準搭載する。ウイルス対策やIPS、Webフィルタ、リバースプロキシ、WAF、クラウド型サンドボックス(Sophos Sandstorm)、C&Cサーバの通信の検知、メールのDLP（データ流出防止）といったセキュリティ機能も搭載。クラウド型の管理コンソール「Sophos Central Admin」で簡単に管理できる。また、「Sophos XG Firewall」をHA 構成にし、冗長化することでトラブル発生時の対応も可能になる。

▶Sophos Central Endpoint Protection Advanced

クラウド管理型エンドポイント保護ソリューション。「Sophos XG Firewall」と連係することで、ソフォスが提唱するネットワークとエンドポイントの自動インシデント対応である「Synchronized Security」で管理工数を削減できる。

▶Sophos Intercept X

クラウド管理型シグネチャーレスマルウェア対策ソリューション。搭載するランサムウェア対策機能の「CryptoGuard」は、ファイルやフォルダの暗号化が始まると同時にファイルをバックアップ。その暗号化が正規のソフトやユーザの意図によるものであればそのまま暗号化するが、悪意あるプロセスによる暗号化は自動的にブロックし、バックアップからファイルを自動的に復元する。

「Sophos Intercept X」は、すべてのソフォス製品を管理する直感的なクラウド型の管理コンソールである「Sophos Central」に統合されている。サーバは不要で、ログインしてエージェントをダウンロードし、一カ所からすべてのエージェントを設定できる。また、社外にいてもクラウド型の管理コンソールで管理できるため、管理工数の削減につながる。なお、「Sophos Central Endpoint Protection Advanced」と同様に「Sophos XG Firewall」と連携し、「Synchronized Security」の機能も利用できる。

導入した結果

次世代ファイアウォール「Sophos XG Firewall」の導入により、既存のファイアウォールルータに比べてセキュリティレベルが向上。また、「Sophos Central Admin」を利用していつでもどこでも「Sophos XG Firewall」を管理できるため、管理工数削減につながった。さらに、「Sophos Intercept X」と「Sophos Endpoint Protection」とのシームレスな連動によって、マルウェアやランサムウェア、エクスプロイトなどへの対策が強化された。

“「Sophos XG Firewall」はとても使いやすく、サイズも小さいので、研究室や企業の部署・部門だけでなく、SOHOなどで利用するのに最適だと思います。事業所の規模に合わせて選択ができるのもいい。もし私がネットカフェを運営するなら、Wi-Fi機能つきの製品を選びますね。”

笠間康次氏
HPC/エンタープライズ事業本部 テクニカルSE部 副部長

▶ネットワークセキュリティの強化

「Sophos XG Firewall」の導入により、ネットワークの分割を行うとともに、ウイルス対策やIPS、C&Cサーバの通信の検知などができることによって、既存のファイアウォールルータに比べてセキュリティレベルが大幅に向上した。

また、「Sophos XG Firewall」が搭載するSSL-VPN機能によって、従業員がセキュアにリモートアクセスを行うこともできる。

「Sophos XG Firewall」のHA構成による技術的な安心だけでなく、ソフォスのテクニカルサポートのバックアップによってスムーズに導入できたことも今後の運用で安心できるポイントとなった。

▶増大する脅威に対応

「Sophos Central Endpoint Protection Advanced」と「Sophos Intercept X」をシームレスに連動でき、次世代型のディープラーニングを活用したマルウェア対策やランサムウェア対策、エクスプロイト対策を行えるようになった。

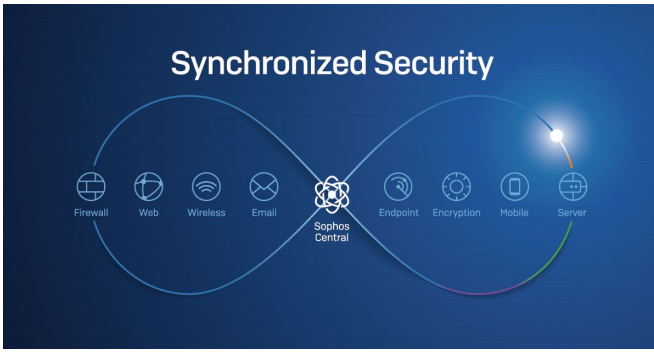
「Sophos Intercept X」に組み込まれた人工知能（AI）は、高度な機械学習システムによりマルウェア定義ファイルに依存せず、既知および未知のマルウェアを検出する。従来の機械学習やシグネチャベースのみを使用するセキュリティソリューションと比較して、より高い精度の検出が可能となった。

▶Synchronized Security

「Sophos Central Admin」を利用することで、管理者が社外にいてもアラートを受け取ったり、管理コンソールにログオンできたりする。いつでもどこからでもリモートで「Sophos XG Firewall」の管理ができる。

また、ファイアウォールとエンドポイントが連係するため、今までは、ファイアウォールで怪しい通信を見つけると、管理者がエンドポイントを隔離し、マルウェアの駆除、ネットワークへの復旧を管理者が手動で行っていたが、Synchronized Security により、これらのインシデント対応がすべて自動化されるため、今まで、1時間以上かかっていた対応が、数分で完了するようになった。これにより、管理者に掛かる負荷が、著しく軽減した。

鬼澤慎氏



ソフォス株式会社 営業部
Tel: 03-3568-7550
Email: sales@sophos.co.jp

Year-Month-Day Suffix-Language [Jo.No.-Intials]