SOPHOS
Cybersecurity made simple.

CUSTOMER CASE STUDY

JCS
Japan Computer Services Inc.

Customer-at-a-Glance

株式会社ジャパンコンピューターサービス
〒101-0025
東京都千代田区神田佐久間町1丁目11番地
産報佐久間ビル 7階

業種
独立系の総合IT企業

社員数
約240名

Webサイト
https://www.japacom.co.jp/

ソフォスソリューション
Sophos XG Firewall
Sophos Intercept X

ソフォスカスタマー
ソフォス製品導入年数：2年

総合IT企業であるジャパンコンピューターサービス(JCS)が、ソフォスのソリューションを導入した。自社運用での導入効果が大きかったため、2018年から顧客企業向けのセキュリティビジネスに参入した。

“ゼロデイ攻撃やAPT攻撃のような高度なサイバー攻撃に備えるためにソフォスのソリューションを導入しました。ファイヤウオールとエンドポイント製品が連携してマルウエアの検知から隔離・復旧までを処理してくれる点が大きな魅力です。”

加藤 弘隆 氏
事業統括本部 PA事業本部 PA1部

“実際に運用してみたら
セキュリティ対策に関する
オペレーションが
ほぼゼロになりました。
SIEMやSOCと異なって、
特別なスキルを備えた要員を
必要としないため、
どのようなお客様にも提供できます。”

加藤 弘隆 氏
事業統括本部 PA事業本部 PA1部

独立系のIT企業として、最新の技術に基づくシステムおよびネットワークの構築や高品質の運用サービス、システム資源のライフサイクル管理コンサルティングなどを手がけるJCS。ITシステムの構築・運用をワンストップで請け負う総合IT企業だ。そんな同社が高度化・複雑化するサイバー攻撃を防御するために、従来のセキュリティツールに代えて、新たにソフォスのソリューションを導入。自社運用での導入効果が大きかったため、2018年から顧客企業向けにセキュリティソリューションの販売とサポートに乗り出した。

ビジネスチャレンジ

同社は、これまでセキュリティツールとして、世界的に大きなシェアを誇るファイアウオール製品と、エンドポイント（PCやサーバーなど）向けのアンチウイルスソフトを導入していた。しかし、サイバー攻撃の高度化・複雑化に伴って、セキュリティ対策を強化することが必要だと考えていた。同社の加藤弘隆氏は、この背景を次のように語る。

「一昔前までは、シグネチャ（ファイルや通信の定型パターン）でマルウエアを検知するセキュリティツールでもサイバー攻撃を防御することが可能でした。しかし、これでは脆弱性を解消する手段が見つかっていないゼロデイ攻撃や、長期間にわたってターゲットを分析するAPT攻撃（持続的標的型攻撃）を防ぐことができません。総合IT企業の当社にとって、こうした最新の脅威にも対応できるような防御体制が不可欠だと考えたのです」

ITシステムやネットワークの構築・運用を主力事業としている同社では、新たにセキュリティビジネスへ乗り出すことを検討していた。そこで、顧客企業にも提供できるようなソリューションを探していた。具体的には、導入コストが安価で、セキュリティに関する専門知識を備えていないスタッフでも運用できるようなソリューションである。2017年夏ころから、さまざまな製品の比較検討を開始。最終的に選定したのがソフォスのソリューションだった。2018年2月から社内への展開を開始した。現在は、ソフォスのエンドポイントの防御ツール「Sophos Intercept X」と、ファイアウオール製品「Sophos XG」（2台のXG230によるクラスター構成）を運用中だ。

テクノロジーソリューション

ソフォスが提供するソリューションの大きな特徴は、エンドポイント向けのツールとファイアウオールが連携してセキュリティ対策に関わる作業を自動化することだ。マルウエアの検知から隔離・復旧までの作業を自動化することが可能だ。

一般的には、ネットワークを守るファイアウオールとエンドポイントのそれぞれで別のベンダーの製品を導入しているので、両者を直接連携さ

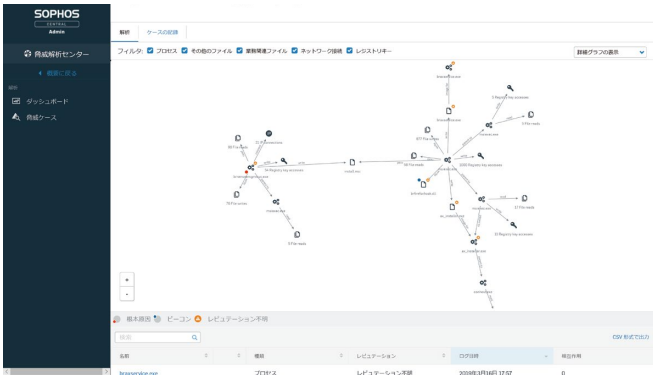
せることは不可能。最近は、組織内に導入したセキュリティツールのログの集約と分析を行う「SIEM（セキュリティ情報イベント管理）」というソリューションも登場しているが、マルウエアの侵入を特定した後の隔離や復旧などの処理は、専門知識を備えたスタッフの手作業に頼ることになる。運用担当者には、少なくともそれぞれのセキュリティツールが出力するログの意味を理解できるようなスキルが求められる。JCSでも、SIEMを導入することも検討したが「初期導入費用が高い上に専門家による手作業が必要になるので、中堅・中小のお客様が導入・運用するのは困難だと判断しました」（加藤氏）という。

ソフォスの製品の場合は「セキュリティハートビート（Security Heartbeat）」という独自技術が、さまざまな作業の自動化を実現している。エンドポイントのIntercept Xとファイアウオールがリアルタイムでセキュリティ情報を共有することで、マルウエアを検知した場合に処理を連携する仕組みだ。

例えば、エンドポイントがマルウエアに感染すると、Intercept Xがそれをファイアウオールに通知。この通知を受けたファイアウオールは、感染したエンドポイントを隔離する。エンドポイントではIntercept Xがマルウエアの削除した後に、ファイアウオールと連携して自動的に復旧させる。マルウエアの感染から無害化までを自動で処理するため、エンドポイントを復旧させるまでの手間暇を最小限に抑えられる。

ゼロデイ攻撃やAPT攻撃など、シグネチャでは検知できないような脅威にも対応できる。AI（人工知能）技術の一種である「ディープラーニング（深層学習）」を駆使することによって、未知の脅威を検知する仕組みだ。Intercept Xは、世界に5拠点あるソフォスの研究所「Sophos Labs」が持つ100万件以上のマルウエアサンプルを教師データとして学習したAIエンジンを搭載。このエンジンが、エンドポイントで実行されるマルウエアの特徴を自動的に検知する。学習データは常に更新されるため、最新の脅威にも対応できる。

加藤氏によると、ソフォスのソリューションが、世界で150超の国・地域で1億人超、国内でも3500社超の顧客に利用されている実績があるということも選定を後押ししたという。



導入した結果

ソフォスのソリューションを自社で導入・運用した結果について、加藤氏は次のように評する。

「実際に運用してみたら、セキュリティ対策に関する日常のオペレーションがほぼゼロになりました。従来は必要だった専門家の手作業が不要になりました。これなら、ITやセキュリティの専門知識を備えた要員抱えることができないような企業でも、導入と運用が可能です」

脅威を検知する機能も高く評価しているという。加藤氏は「マルウエアを検出するスピードと精度が高いとは聞いていましたが、想定したよりもはるかに優れているので驚きました」と語る。

JCSでは「ソフォスのソリューションであれば、ITやセキュリティの専門家がいないような中小・中堅のお客様でも運用が可能」（加藤氏）と判断し、これを駆使したセキュリティビジネスに乗り出すことを決断した。ファイアウオールの「XG　Firewall」とエンドポイント向けツール

の「Intercept X」を顧客企業の組織内に導入し、これらの運用をJCSが請け負うという形態のサービスを2018年から提供開始した。組織内における脅威の監視と侵入後の対応を担うSOC（セキュリティ・オペレーション・センター）を顧客企業がJCSにアウトソースするようなイメージだ。

ソフォスのソリューションには、同社のツールを単一のユーザー・インタフェースから統合管理する「Sophos Central」というクラウドベースの管理コンソールがあり、これを利用することで、このような形態のサービスを実現できた。このコンソールが備えている「Central Partner」という機能を使うことによって、顧客企業における脅威を監視・対応が可能になるからだ。顧客企業がJCSの新サービスを導入すれば、SIEMやSOCを独自に構築するよりもTCO（総所有コスト）を大きく引き下げることが可能になる。

加藤氏は、ソフォスのソリューションを活用したサービスがJCSの業績にも貢献すると期待して、次のように説明する。

「現在、JCSではパブリッククラウドやIoT（インターネット・オブ・シングス）などを活用する新たな形態のシステムの構築に注力しています。こうした案件に乗り出す競合も多いのですが、ソフォスのソリューションを駆使したセキュリティサービスが大きな差異化要因になると考えています」

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

2019-04-18 JAPAN (Jo.No.-CHU01)

SOPHOS