国内最大手の補聴器メーカーであるリオンが、グループ企業のネットワークを刷新した。併せて、セキュリティ対策を見直してサイバー攻撃にも対応したレベルに引き上げることを決断した。
ただし、セキュリティの専門家がいない同社にとって、この実現は容易ではなかった。この課題を解決したのが、ソフォスの次世代型エンドポイントツールである。

CUSTOMER-AT-A-GLANCE

リオン株式会社

リオン株式会社
東京都国分寺市東元町
3-20-41

社員数
886名（2019年3月31日現在・連結）

Webサイト
https://www.rion.co.jp/

ソフォスソリューション
Sophos Intercept X

実際にソフォスのソリューションを導入して使ってみたところ、
脅威を検知する機能はもちろんですが、
運用管理が容易な点も高く評価しています。
IT推進室における作業の負担を大きく削減できました。

リオン株式会社
経営企画本部　IT推進室
課長　大川 佳洋 氏

国内最大手の補聴器メーカーであるリオン。同社は、理学・音響学の研究を行う小林理学研究所（現・一般財団法人）の研究成果を製品化することで社会に貢献することを目的として、1944年に東京都国分寺市で創業。現在は、21世紀のキーワードともいえる「医療」と「環境」をテーマとして、補聴器、医用検査機器、音響・振動計測器、微粒子計測器という4製品群を軸とした事業を展開している。
同社は2018年、本社を含めて合計で7社あるグループ企業のネットワークを刷新した。これまで、それぞれの企業が独自に構築していたネットワークを統合。この際に大きな課題となったのがセキュリティ対策だった。

ビジネスチャレンジ

ネットワークを統合する以前は、グループ企業ごとのセキュリティレベルに大きな格差があったという。グループ企業には、IT専任者が本社ともう1社のみに在籍しており、他グループ企業には在籍していない。総務部などの社員が兼任しているので、万全なセキュリティ対策が講じられていたわけではなかった。万が一、セキュリティレベルが低いグループ企業が攻撃者の標的にされれば、そこから様々な機密情報が盗まれる恐れもある。本社でも、ファイアウォールやアンチウイルスソフト、クラウド型のメール・セキュリティ・ツールなどのセキュリティツールを導入していたが、改善策が見つかっていない脆弱性を突くゼロデイ攻撃や、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）への対策は不十分だった。

そこでネットワークの刷新を機に、セキュリティ対策

社員のセキュリティ意識が高いがために、これまでは現場からの問い合わせ対応が大きな負担になっていました。Intercept Xを導入したら問い合わせが激減し、新たに創出できた時間を付加価値の高い作業に振り向けられるようになりました。

リオン株式会社
経営企画本部　IT推進室
嶋津 孝一 氏

も統合することを決断。本社のIT推進室で課長を務める大川佳洋氏は「グループ全体のセキュリティレベルを引き上げるという目標を立てました」と語る。

ただし、この実現には大きなハードルが立ちはだかっていた。セキュリティ対策のために導入するツールの運用の負荷が高くなると、防御体制にほころびが生じる恐れがあったのだ。グループのIT投資を管理しているのは、少数の本社IT推進室課員のみ。この少数の人員でITに関わる企画・開発・運用の全てを担っているため、セキュリティ対策に振り向けられる人的リソースはそれほど大きくない。実際、ネットワークを刷新する以前でも、セキュリティに関する現場からの問い合わせが大きな負担となっていた。

同社では、古くから教育・啓蒙活動に力を入れていたため、現場の社員のセキュリティ意識が高いという。それだけに、見慣れないポップアップ画面が開くなど、少しでもおかしな挙動をするとIT推進室に問い合わせが来るのだ。その都度、IT推進室のメンバーが対応しているのだが操作ミスであることが多く、結果的に何の障害もないケースがほとんどだった。IT推進室の嶋津孝一氏は「現状よりも、私たちIT推進室の負荷を下げるとともに、現場の社員の利便性を上げることが必要だと考えました」と語る。本社だけでも、これだけ負担が大きいのだから、現状の体制ではグループ全体をサポートするのは困難だと考えた。そこで未知のマルウエアにも対応できるような防御機能を備えているとともに、運用管理の負担が小さなセキュリティツールを新たに導入することを決断した。

テクノロジーソリューション

いくつかのツールが候補に上がったが、以前から取引のあったリコージャパンの推薦もあって、最終的にエンドポイント防御ツールである「Sophos Intercept X」を選定した。

Intercept Xは、クラウドと連携してさまざまな脅威を検知してエンドポイントを防御するソリューション。マルウエア対策、エクスプロイト対策、EDR（Endpoint Detection and Response）対応などの機能を提供する。

マルウエア対策では、シグネチャ（マルウエア定義ファイル）ではなく、ディープラーニング（深層学習）技術でマルウエアを検知することが大きな特徴だ。Intercept Xは、世界に5拠点あるソフォスの研究所「SophosLabs」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（人工知能）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。

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未知の脅威にも対応できるのだ。

ランサムウエア対策機能である「CryptoGuard」も搭載する。これは、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のバックアップを実行する機能。暗号化が正規のソフトやユーザーの意図によるものであれば、そのまま暗号化を継続させる。もしも、悪意あるプロセスによる暗号化であれば、この処理を自動的にブロックするとともに、バックアップからファイルを自動的に復元する。

大川氏は、Intercept Xを選んだ決め手を「信頼性です。セキュリティ専業で常に最新のテクノロジーを追究しているので、ソフォスのツールなら安心だと考えました」と語る。リコージャパンで同社を担当する荒木一夫氏は、このツールを推薦した理由を次のように評する。

「検知の精度が高いのにシステムへの負荷が小さい点と、設定や運用が容易な点を評価しました。次世代型のエンドポイントツールの多くは価格が高いのですが、お手頃な価格であるところもお薦めしやすい理由です。リコーでは他のベンダーのセキュリティツールも扱っていますが、リオン様にはIntercept Xが最適な製品だと考えました」

導入した結果

リオンでは2019年5月から約1カ月でグループ企業への導入を完了。合計で約2000台のPCにIntercept Xをインストールした。嶋津氏は、導入後の感想を「運用が飛躍的に楽になりました」と語る。Intercept Xには、管理者が許可したアプリケーション以外を実行できないようにする機能があり、操作ミスによる問い合わせが激減したからだ。

導入直後に、この機能の検知精度の高さを実感したエピソードがあるという。Intercept Xを導入したところ、自社で開発したシステムのある機能が停止したという。調べてみると、この機能がサイバー攻撃のある手口に似た挙動を示していた。Intercept Xがサイバー攻撃の脅威の可能性があると判断して、この機能のジョブのみを停止させていたのだ。このジョブをホワイトリストに登録することで、現在でもこのシステムを業務で活用中だ。

大川氏は、こうした運用の容易さも「Intercept Xを導入したメリット」だという。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、ホワイトリストの登録をはじめとして、運用管理を一元化できるからだ。同氏は「現場の社員と私たちIT推進室の双方で、セキュリティ対策に関する作業の生産性を大きく向上することができました」と語る。

SOPHOS