トーヨーカネツ株式会社 様

エンドポイントツール導入で、運用管理の負担を軽減。
月に50～100件のマルウェアを侵入前に駆除。

CEC
Computer Engineering & Consulting

トータルセキュリティソリューション
CyberNEXT®

導入事例

未知の脅威に備えるために EDR 製品を導入

トーヨーカネツがセキュリティ対策を強化した。
未知の脅威であるサイバー攻撃にも対応できる防御体制を築くためだ。
ただし、人的リソースが限られるので、運用管理の負担を増やすことはできない。
この課題を解決したのが、シーイーシーが提案したエンドポイントツールである。

導入ポイント 導入効果

1. 1ヵ月に50～100件のマルウェアを侵入前に駆除
2. セキュリティ対策が不十分な端末の把握が容易
3. クライアントの状況をレポート形式で見える化

導入の背景

ゼロデイやAPT攻撃の防御に向けセキュリティ対策を強化

1941年に工業窯炉の製造・販売事業者として創業したトーヨーカネツ（当時の社名は東洋火熱工業）。「優れた技術、製品、サービスを裏付けとして持続的に成長・発展するグループ」を経営ビジョンに掲げる同社は、顧客や社会の要請に基づいて事業を拡大してきた。現在は、仕分け・ピッキングシステムや情報化技術に関して顧客から高い評価を受けている物流ソリューション事業と、原油や液化天然ガスなどの貯蔵タンクを世界各地に5700基以上納入している機械・プラント事業を経営の柱としている。

2019年に同社は、セキュリティ対策の強化に乗り出す。未知の脅威に備えることが大きな狙いだ。

これまで同社は、世界的に大きなシェアを持つセキュリティベンダーのアンチウイルスソフトを利用していた。シグネチャ（マルウェアの特徴的なパターン）でマルウェアを検知する仕組みのツールだ。

同社のIT投資を統括する情報システムグループは、セキュリティ対策を見直し、強化が必要だと判断したという。手口が巧妙化するサイバー攻撃を防御するためだ。ファイアウォールなど他のセキュリティツールも導入しているが、修正プログラムが提供される前に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して攻撃するAPT攻撃（Advanced Persistent Threat：持続的標的型攻撃）などはシグネチャベースのツールでは検知できない。攻撃者が社内に侵入していても、全く気づかないという恐れもあるのだ。

実害は被らなかったものの、サイバー攻撃が対岸の火事ではないと感じるような出来事もあった。ビジネスを装って金銭をだまし取る「ビジネスメール詐欺（BEC：Business E-mail Compromise）」が横行した2～3年前に、同社にも攻撃者からのメールが届いたという。

情報システムグループでは自社のセキュリティ対策を見直すため、2018年に外部のコンサルティング会社の診断を受けた。この診断結果を踏まえ、経営層に向けてセキュリティ対策強化の必要性を訴えた結果、投資に向けた意思決定が下された。

コーポレート本部 経営企画部 経営企画グループ 兼 総務部
情報システムグループ 主査 情報処理安全確保支援士 宮川 嘉正 氏

コーポレート本部 総務部 情報システムグループ 堀 聖彦 氏

トーヨーカネツ株式会社 様

エンドポイントツール導入で、運用管理の負担を軽減。
月に50～100件のマルウェアを侵入前に駆除。

CEC
Computer Engineering & Consulting

トータルセキュリティソリューション
CyberNEXT®

導入事例

選定の決め手

エンドポイントを防御するために EDR製品が選定の対象に

新たなソリューションを検討するに当たって、情報システムグループは付き合いのあったベンダーに相談を持ちかけて、次のような要件を固めていった。

大前提となるのが、シグネチャに頼らずに未知の脅威にも対応できることだ。これに加えて、社内のネットワークに接続された端末だけでなく、社外からアクセスする端末を防御できることも要件の一つに掲げた。情報システムグループでセキュリティ対策の中核を担っている堀聖彦氏は「ネットワークの境界を防御するだけではなく、端末やサーバーなどのエンドポイントそのものを守りたいと考えました」と語る。この要件に当てはまるのが、次世代のセキュリティ対策とも呼ばれる「EDR（Endpoint Detection and Response）」に分類されるソリューションだ。

運用管理が容易であることも重要な要件だった。対象となるPCは合計で約1000台。情報システムグループに属する11人の社員のうち、セキュリティ対策を担当しているのは堀氏を含めて2～3人しかいない。どんなに高機能なソリューションであっても、日常の運用に大きな手間がかかるのではセキュリティ対策が破たんする恐れがある。

この要件で絞り込んだところ、6種のEDR製品が選定対象に残った。情報システムグループが最終的に選んだのが、シーイーシーが提案した「Sophos Intercept X」である。最新のテクノロジーが搭載されたEDR製品であることに加え、圧倒的にコストパフォーマンスが優れていた点が決め手になったという。

防御機能と運用性を評価して シーイーシーの提案を採用

シーイーシーがIntercept Xを提案した大きな理由は、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機能を高く評価したからだ。マルウェア対策では、シグネチャを使わずにディープラーニング（深層学習）技術でマルウェアを検知することが大きな特徴だ。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ェ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ェ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。

運用管理が容易な点も、Intercept Xを提案した理由の一つ。ソフォスのソリューションにはベストプラクティスのポリシー設定がビルトインされている。設定変更も「Sophos Central」というクラウドベースの管理コンソールから一元的に実行できる。シーイーシーでは、搭載する機能だけでなく、将来の運用性を見据えてソリューションを提案している。

導入の効果

1ヵ月に50～100件の マルウェアを侵入前に駆除

トーヨーカネツは、シーイーシーとソフォスの協力の下で2019年9月からの約1ヵ月で全社への導入を完了。シーイーシーは、導入を進める中、トーヨーカネツの課題でもある「運用者の負担」をいかに極小化できるかを検討し、いくつかの機能改善案をまとめた。ソフォスとシーイーシーが協議した結果、これに対する改善要望をソフォスの英国本社へ上申した。現在、いくつかの機能を実装することを計画中だという。この案件に携わったシーイーシーの担当者は、グローバル企業にも関わらず小回りが利くことに驚いたという。一方でソフォスの担当者は、シーイーシーがユーザー目線で顧客の要望を上げてくる点を高く評価している。

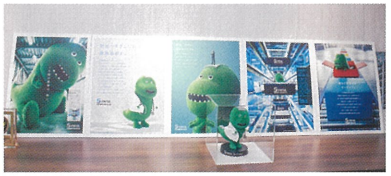
トーヨーカネツは3ヵ月の準備期間を経て2019年9月からの約1ヵ月で全社への導入を完了。導入後には月に50件から100件のマルウェアを侵入前に駆除しているという。駆除されたマルウェアの経路をたどれることに加え、最新のセキュリティパッチが適用されていない端末も容易に把握できるようになった。さらに、クライアントの状況をレポート化して経営層へ定期的に報告できるようになったので、経営層のセキュリティへの関心の高まりにもつながっているという。宮川氏は「将来的にはゼロトラストモデルとDLP（Data Loss Prevention：情報漏えい対策）を実現したいと考えています」と抱負を語る。

お客様プロフィール

トーヨーカネツ株式会社

本　社	〒136-8666　東京都江東区南砂二丁目11番
代表者	代表取締役社長　柳川 徹
従業員数	996名（2019年3月期、連結）
事業内容	物流ソリューション事業および機械・プラント事業
URL	https://www.toyokanetsu.co.jp/

トーヨーカネツ株式会社



■写真
オリジナルキャラクター「プツリューくん」。
主力事業の内容をより解りやすく伝えるため、カタログや各種広告など販売促進活動の場を中心に活躍。

お問い合わせ

CEC 株式会社シーイーシー
Computer Engineering & Consulting

〒150-0022　東京都渋谷区恵比寿南1-5-5　JR恵比寿ビル
TEL：03-5789-2442 FAX：03-5789-2585
Email：marketing@cec-ltd.co.jp
URL：https://www.cec-ltd.co.jp/

販売代理店

202003-003-010CI