SUCCESS STORY | 南総通運株式会社

opentext™

EPP/EDR、MDR、バックアップでセキュリティを強化
サイバー攻撃からの防御体制を確立しながら、管理コストも軽減

千葉県を拠点に、総合物流サービス事業を展開する南総通運株式会社。同社はデスクトップPCからモバイルPCへの移行を契機に、端末のセキュリティを強化するためエンドポイントセキュリティ（EPP/EDR）のOpenText™ Core Endpoint Protection、運用サービスのOpenText™ Core MDR、自動バックアップのOpenText™ Core Endpoint Backupを導入。近年増加するランサムウェアや、サプライチェーン攻撃に対する防御体制を整備すると同時に、管理コストの軽減を図っています。

営業力強化に向けたモバイル活用を進め エンドポイントセキュリティも強化

千葉県・東金市に本社を構える南総通運。総合物流事業者として、基幹事業の輸送に加え、倉庫での保管、荷役、包装・梱包、流通加工、情報処理など幅広いサービスを展開しています。

同社は2024～2026年度の中期経営計画で「創造と挑戦による企業価値の向上」を掲げ、複数の重点施策を推進しています。その1つである営業力・営業企画力の強化による事業拡大に向けて、デスクトップPC中心の環境をモバイルPCに切り替えました。管理部 情報システム課 主幹の林 儀雄氏は次のように語ります。

「従来の営業スタイルでは、紙の資料提供や口頭での説明が中心で、PC作業は社に持ち帰る形でした。現在は、お客様先にモバイルPCを持参してその場で提案ができるようになり、場所にとらわれない業務スタイルを確立しています。2～3年かけて徐々に切り替え、現在は8～9割がモバイルPCです」

モバイル活用に伴い、新たな課題として浮上したのがセキュリティ強化でした。PCを社外に持ち出して仕事ができるようになると、エンドポイントのリスクは拡大します。加えて、増加するランサムウェアやサプライチェーン攻撃、監査対応の厳格化を背景に、より高度な対策が必須でした。

同社はこれまでもEPPやEDRを導入し、セキュリティを強化してきました。しかし、バックアップはファイルサーバーのみでクライアント側は未整備だったため、故障や盗難、近年増加するランサムウェア攻撃などに対する不安がありました。そこで、既存のEPP/EDRを見直し、新たなソリューション導入を検討しました。

「近年、日本の大手企業でもランサムウェアによる被害が深刻化しています。報道を受けて経営層の意識も“何か起きてからでは遅い”と高まりつつあります」（林氏）

コストと機能のバランス、 SOCによる24時間監視体制を評価

EPP/EDRの更新やバックアップの強化にあたり、南総通運はOpenText Core Endpoint Protection、Core MDR、Core Endpoint Backupを採用。複数のソリューションを検討した中で、必要な機能を備えながら低コストで導入できる点を評価したと林氏は語ります。

「OpenTextの営業担当者が当社を継続的に訪問し、機能やコストメリットについて詳しく説明してくれました。導入後のサポートにも期待し、採用を決めました」

導入・運用のしやすさも決め手となりました。選定段階では林氏自身が検証環境でテストを実施し、エージェントの入れ替えや、全社展開の手順を確認しています。

「実際に試してみたところ、手間なくスムーズに移行できました。当社で管理している300台程

事業内容

自動車運送事業、倉庫事業、附帯事業、その他事業

企業名

南総通運株式会社

ビジネス課題

- モバイルPCの拡充に伴う端末セキュリティの強化
- 増加するランサムウェアやサプライチェーン攻撃への対策
- クライアントPCのデータバックアップ

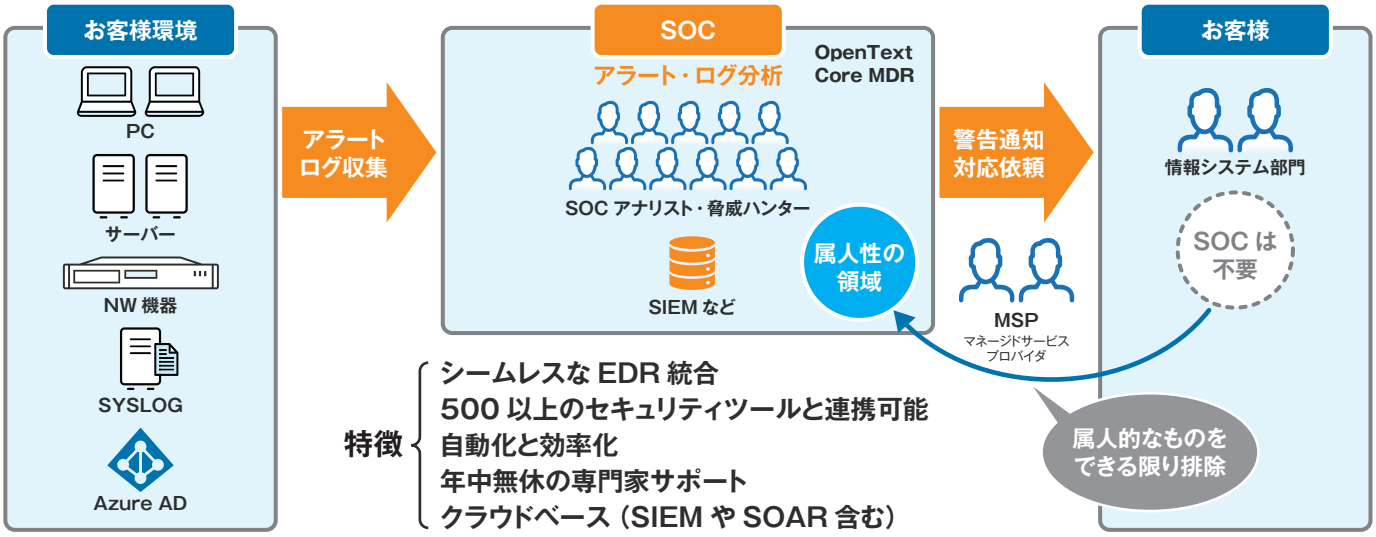
ビジネスソリューション

- OpenText™ Core Endpoint Protection
- OpenText™ Core MDR
- OpenText™ Core Endpoint Backup

ビジネスメリット

- エンドポイントセキュリティの強化
- SOCによる運用負荷の軽減と日本語による対応
- インシデント発生時のリカバリー体制の強化
- 取引先企業からの信頼獲得
- コストの最適化

図：OpenText™ Core MDR の概要



度のPCであれば、私1人でも十分に対応可能と判断しました」（林氏）

24時間365日稼働のセキュリティオペレーションセンター（SOC）がリアルタイム監視からインシデント対応までをサポートするOpenText Core MDRについては、OpenTextのパートナー企業である株式会社アクトの日本語対応も安心材料となりました。

「検討段階でアクト社から直接、インシデントが発生した際の対応について詳しく伺いました。『困ったことがあれば何でも言ってください』という言葉をいただき、密にコミュニケーションが取れる距離の近さも選定の後押しとなりました」（林氏）

さらに、OpenText Core Endpoint Backupによるバックアップ機能により、ランサムウェア対策やPCの故障・盗難対策に加え、遠隔からのデータ消去機能など情報漏洩対策に寄与する点もポイントになりました。

南総通運は、2025年10月から3つのソリューションの運用を開始。約300台のモバイルPCに対して、既存のエージェントを削除して新規エージェントを導入する作業は、クライアント運用管理ソフトを使ってリモートで実施し、大きなトラブルもなく短期間で完了。EPP/EDRの導入時に課題となりやすい誤検知・過検知のチューニングもほぼ不要で、円滑に移行できました。

「元々、当社独自の特殊な業務アプリケーションは少なく、ほとんどがクラウドベースのWebアプリケーションです。そのため、特別なチューニングをすることなく切り替えることができました」（林氏）

サプライチェーン全体での信頼性向上 物流事業者として取引先への責任を担保

OpenTextソリューション導入後、運用面ではOpenText Core MDRのSOCによる監視体制とアクト社による日本語サポート体制が整備され、日常的な監視業務の負担が軽減されています。

「対処が必要な場合のみ、アクト社経由で当社に通知が届く仕組みです。現在のところ軽微な通知を1件受け取った程度で、大きな問題は発生していません。メールでのサイバー攻撃が増えていますが、ほとんどをSOC側で確認いただけるため、セキュリティ担当者が1人体制の当社でも、無理なく運用ができています」（林氏）

導入の成果は、セキュリティレベルの底上げにも表れています。EPP/EDRのエンドポイントセキュリティの強化、MDRによる脅威検知と対応に加え、バックアップの整備により、インシデント発生時のリカバリー体制が強化されました。

「これまでファイルサーバーだけだったデータのバックアップが、クライアント端末のデータまでカバーでき、万一の際も対処が可能になりました。これまで別製品で対応していたリモート消去機能を、OpenText Core Endpoint Backupに統合できたことで、コストの圧縮にもつながっています」（林氏）

サプライチェーン全体で高いセキュリティ意識が求められる中、南総通運の取り組みを対外的にアピールできることは、信頼性の獲得という側面でも重要な価値となると、林氏は強調します。

「社会インフラを支える物流事業者として、取引先に迷惑をかけることは避けなければなりません。今回のセキュリティ強化で信頼性が一段と高まり、サプライチェーンの中で責任を果たせる体制が整いました」

多層防御による全体最適を目指し NDRやSASEの導入を検討

林氏は今後のさらなるセキュリティ強化に向けて、クライアントからサーバー、ネットワークまでを網羅する多層防御を目指す考えを明らかにしています。具体的には、ネットワーク領域での対策として、NDRやSASEの導入を2027年度に向けて検討中で、エンドポイントにとどまらない全体最適のセキュリティ基盤を構築する方針です。

一方、セキュリティ面以外でも、高度化するIT環境への対応や運用負荷の軽減が重要になっています。そのため林氏は、そのほかのOpenTextの豊富なソリューション群にも関心を寄せています。

「IT部門は現場を支える裏方として、現場が使いやすく、トラブルを起こさない環境を整えることが重要です。OpenTextのイベントに参加し、さまざまな製品を扱っていることを知りました。今後も当社のIT課題にどのような提案をいただけるか楽しみにしています」

80年以上の歴史に新しい価値観とテクノロジーを融合し、社会への貢献を続ける南総通運。セキュリティ強化やIT環境整備の取り組みは、次のステージへと進み始めています。

オープンテキスト株式会社
Tel: 03-4560-7704
Email: jpmkt-group@opentext.com
https://www.opentext.com/jp