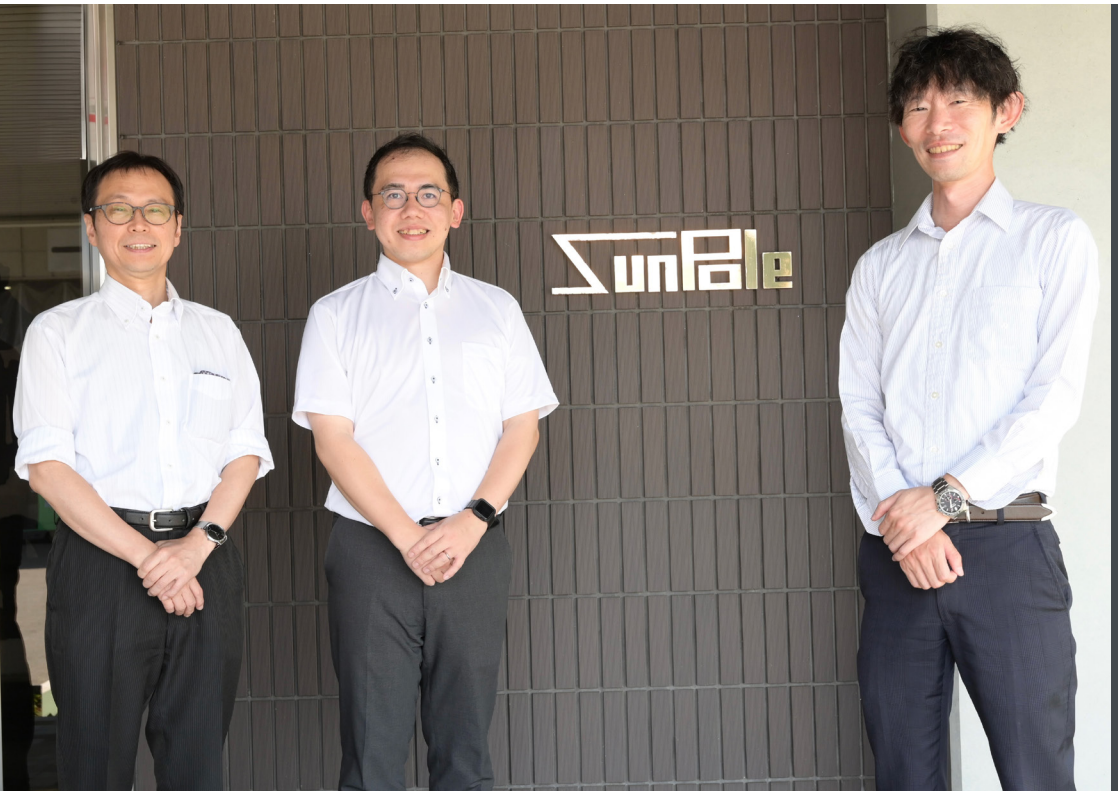


「外部空間を豊かにクリエイトする演出者」として笑顔あふれる街づくりに貢献することを企業理念に掲げる株式会社サンポール。同社は、1970年の創立から「旗ポール」と「車止め」の製造販売で事業を拡大してきた。同社のITを推進している管理部　管理課では、広島県や中国地方の企業でサイバー攻撃の被害が相次いでいることから、感染をいち早く検知し、迅速に対処できる仕組みが必要だと判断して、クライアントPCとサーバーにSophos MDR Complete を採用した。

CUSTOMER-AT-A-GLANCE

SunPole

株式会社サンポール

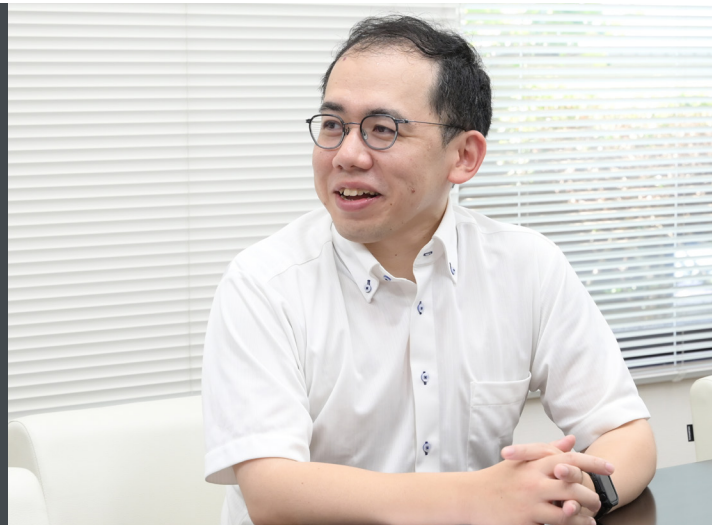
本 社 所 在 地　730-8667 広島市中区南吉島2丁目4-5
TEL:082-244-4655　FAX:082-243-5914

W E B サ イ ト　https://www.sunpole.co.jp/

ソフォスソリューションズ　Sophos MDR Complete

EDRを導入して自社で運用管理するには、人員や経験が不足していると諦めていましたが、Sophos MDR Completeならば当社の事業規模でも24時間365日の監視と対策を実現できる本格的なEDRを導入できました。

株式会社サンポールホールディングス
管理部 管理課
熊野 翔一 氏



1970年に創業しアルミ製ハンドル型旗ポールの製造販売を開始した株式会社サンポール。旗ポール、車止めを通して、街の景観にかかわる製品を製造してきた同社は、日本各地の学校、会社、公共施設やスポーツ施設などに納入実績がある。笑顔あふれる街づくりを念頭に、誠実で心のこもった製品づくりを行ってきた同社は、サイバーセキュリティ対策にも積極的に取り組んできた。そして、広島県をはじめ中国地方でもサイバー攻撃の脅威が増している現状を危惧して、ITパートナーからの提案を受け2025年にSophos MDR Completeを採用した。

ビジネスチャレンジ

「EDR導入を阻んでいたライセンス数とナレッジの不足」

Sophos MDR Completeの採用に至る背景について、管理部　管理課の熊野　翔一氏は、次のように振り返ります。

「以前は、AI型のアンチウイルスを導入していました。侵入検知と防御性能に関しては、特に不満はなかったのですが、運用面での課題がありました。課題のひとつは、正常なプログラムもブロックしてしまうので、その都度ホワイトリストを更新する手間がかかっていました。また、パターンファイルのアップデートが手動だったので、利用頻度の低いPCへの適用が遅れがちで苦慮していました。それに加えて、最新のパターンファイルが必ずしも日本語版に適応しているとは限らなかったので、アップデートにも注意が必要でした。こうした不便さを感じていたころに『広島県内でも有名な企業がサイバー攻撃の被害を受けた』というニュースを目にしました。こうした背景から、アンチウイルス対策よりも強力なセキュリティ対策を導入する必要があると考えて、EDR（Endpoint Detection and Response）の検討を始めました」。

EDR導入の調査を開始した熊野氏は、その段階で2つの課題に直面する。それは「EDRの導入には、最低ライセンス数を設定しているサービスが多く、当社の事業規模では契約できないと分かったのです。また、EDRを自社で運用してサイバー攻撃に対処するには知識や経験が必要で、対応できるスタッフの数が限られている情報システム部では、マネジメントし切れないという課題もありました」と熊野氏は補足する。

テクノロジーソリューション

「事業規模に影響されずに導入できるSophos MDR Completeに注目」

サイバー攻撃の脅威が増す中で、事業規模が小さな企業では本格的なEDRを導入するのは不可能だと思っていた熊野氏は「当社の規模でも導入できるEDRがないか、ITパートナーに相談しました。その時点では、3社のサービスを提案してもらいました。1社は最低ライセンス数が、当社の契約数を上回っていたので、検討を見送りました。もう1社は、問い合わせがチケット制で海外から時差のあるサポートになるため、タイムリーな回答が受けられない心配がありました。最終的に、外部機関による評価の高さと、契約ライセンス数が当社の規模でも対応してもらえる点を評価して、Sophos MDR Completeのトライアルを開始しました」と検討の経緯を話す。

トライアル期間の印象について、熊野氏は「初めは検証用のPCにインストールしました。その後、当部署で動作検証を行いました。その時点では、トラブルもなく円滑に試験ができました。その後、展開するPCを増やしていく中で、既存のソフトと競合してCPUの使用率が100%になる、といった事象も発生しました。しかし、ITパートナーとソフォスからの助言で解決できました。ITパートナーは、当社のPCやサーバーの情報を正確に把握しているので、その構成情報をソフォスのシステムエンジニアと共有して、問題の特定と解決方法を的確に指示してもらいました」と振り返ります。

ビジネスインパクト

「Sophos MDR Completeの導入で運用負担が軽減し安心感は増大」

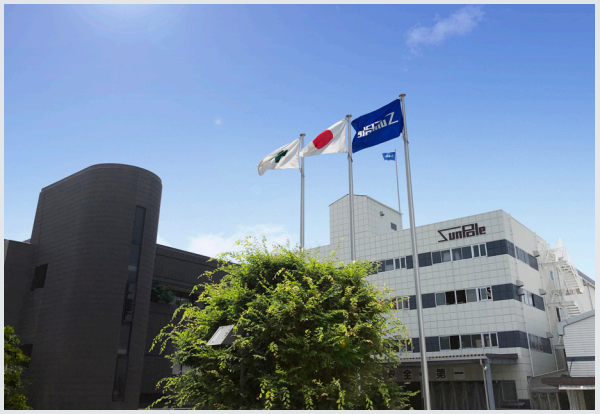
2025年から本格的な運用を開始したSophos MDR Completeの効果について、熊野氏は「検証期間に細かい問題は洗い出していたので、本番稼働はスムーズでした。導入直後には、疑わしいソフトやWebサイトがブロックされたという表示に関して、社員からの問い合わせもありましたが、その警告メッセージも、結果的には社員のセキュリティ意識を高める効果につながったと思います。また、Sophos MDR CompleteはPCやサーバーに対し、常に最新のエンドポイントセキュリティを自動的に適用してくれるので、パターンファイル更新が抱えていた課題も解決しました」と導入の効果に触れ、「運用管理に関しては、24時間365日で監視してくれるMDRにより、管理部の負担や不安も軽減されました。以前は、休日でもサイバー攻撃がないか気になっていましたが、もし攻撃されて

も、Sophos MDR Completeがリモートで対応してくれるので、安心して休めるようになりました。それに加えて、毎月届くレポートで、どれだけのサイバー攻撃がブロックされたのか、どのような対策を施したのか、といった詳しい情報が得られるので、これまで気が付いていなかった脅威も意識できるようになりました」と評価する。

フューチャービジョン

「Sophos Firewallへの更新やクラウドサービスとの連携も検討していく」

今後に向けたセキュリティ対策の強化について、熊野氏は「UTMの更新時期が近いので、そのタイミングでSophos Firewallへの切り替えを検討しています。UTMもソフォスで統一できれば、より安心感も増すと思っています。また、Sophos MDR CompleteとMicrosoft 365の連携によるセキュリティの強化も考えています。Microsoft 365対応アクションを利用すると、ユーザーサインインのブロックや有効化、現在のユーザーセッションの終了、不審な受信トレイルールの無効化など、Microsoft 365への攻撃にも対応できるようになります。クラウドサービスを安全に使うためにも、Sophos MDR Completeを活用していきたいと思います。これからも、ITパートナーとソフォスには、当社のセキュリティを強化するアドバイスをいただけたらと願っています」と話す。



SOPHOS