関西を中心に、港湾や一般土木、道路、河川橋梁などを建設しているヤマト工業株式会社。同社の総務部では、国内の事業所や建設現場で社員が使うPCのセキュリティ対策を強化するために、パターンマッチング方式のアンチウィルスソフトから、Sophos Intercept X Advancedへ更新し安全性の向上と運用負担の軽減を実現した。

株式会社ハイパー大阪支店
一課　課長　平 潤偉氏

株式会社ハイパー大阪支店
支店長　飯名 良太氏

CUSTOMER-AT-A-GLANCE

ヤマト工業株式会社

ヤマト工業株式会社

本 社 所 在 地　〒552-0012 大阪市港区市岡1丁目2番19号

ＷＥＢサイト　https://www.yamato-gc.co.jp/

ソフォスソリューションズ　Sophos Intercept X Advanced

ソフォスが世界で1億以上のデバイスを保護している中で、ランサムウェアの攻撃に対する圧倒的な防御力を持つという実績を高く評価しました。

ヤマト工業株式会社
総務部 総務課長
谷口 英生 氏

昭和9年に山戸商店として創業し、昭和22年に法人化されたヤマト工業株式会社は、総合建設業をはじめとして、港湾工事や浚渫工事、建設資材販売に海陸運送業など、社会資本の建設に携わる事業を国内で展開している。大阪市の本社を中心に、東京、神戸、九州に支店や営業所を構え、男性・女性がいきいき働ける環境整備にも取り組んでいる。同社の総務部では、全社の情報システムの運用管理を担い、セキュリティ対策も推進してきた。そして、国内で急増するサイバー攻撃やランサムウェア被害から、社員のPCを守るために、旧世代のアンチウィルス製品からSophos Intercept X Advancedへ更新した。

ビジネスチャレンジ

「旧世代のアンチウィルスソフトの限界を実感」

ヤマト工業株式会社の総務部で、社員が利用するPCのセキュリティ対策を担ってきた谷口英生総務課長は、以前に抱えていた課題を次のように振り返る。
「約10年ほど前から、全社で利用するアンチウイルスソフトは統一していました。しかし、報道などでサイバー攻撃の被害が増えていると実感していたので、昔から使っていたパターンマッチング方式のアンチウイルスソフトでは、新たな脅威に対応できないのではないかと限界を感じていました」。
同じ総務部で、PCの運用管理やセキュリティ対策に携わってきた濱貴之係長も、旧世代のアンチウイルスソフトの限界に触れる。
「以前のソフトは、社員が手動でアップデートを実行しないと、パターンファイルが更新されない仕様でした。そのため、工事や建設現場で使われているPCは、更新が遅れてしまい、セキュリティ面での不安がありました。幸いにも、マルウェアへの感染やラン

サムウェア被害などは発生していませんでしたが、運用管理の面からも、何らかの対策が必要だと考えるようになりました」。

ヤマト工業株式会社
総務部 総務係長
濱 貴之 氏

テクノロジーソリューション

「ランサムウェア被害ゼロの実績を高く評価」

セキュリティ対策に不安を感じていた総務部では、長い取引の実績があるITパートナーで、Rising Star of the Year Award 2022を受賞した株式会社ハイパーから新たな提案を受けた。谷口氏は「ハイパーからSophos Intercept Xを紹介されたときには、マルウェアに対する高い検知率に加えて、ソフトウェアの脆弱性やセキュリティ上の欠陥を狙うエクスプロイト攻撃も防げると聞きました。また、ランサムウェアに感染しても、正常な状態に自動復旧してくれるCryptoGuard機能があり、ソフォスが世界で1億以上のデバイスを保護している中で、ランサムウェアの攻撃に対する圧倒的な防御力を持つという実績も信頼できました」と更新のきっかけに触れる。

濱氏も「Sophos Intercept Xはインターネットに接続しているだけで、最新のアップデートが自動で実行される点に注目しました。また、管理コンソールの画面も直感的で使いやすそうだったので、運用管理の効率も改善できると思いました」と補足する。

Sophos Intercept Xの性能を高く評価した総務部では、2023年2月から評価版による検証を開始した。その過程で「一部のPCで利用している土木積算ソフトが、定期的に大量のデータを書き換えるため、Sophos Intercept Xによるアラートが出ました。そこで、ハイパーとソフォスのサポートに協力してもらい、ホワイトリストを作成して対応しました。その他には、特に気になる点はなかったので、2023年5月から正式な導入を開始しました」と谷口氏は検証の経緯を振り返る。

ビジネスインパクト

「セキュリティ対策の運用負担を軽減し安全性も大幅に向上」

Sophos Intercept X導入後の効果について、濱氏は「運用管理の負担が大きく軽減されました。導入当初は、毎日ソフォスの管理コンソールをチェックしていましたが、現在はメールによるアラートが送られてこなければ、月単位でチェックするようにしています。また、管理コンソールからは各PCが最新の状態かどうかをチェックできるだけではなく、インストールされているソフトも確認できるので、誰かが不用意に危険なソフ

トを使っていないかどうかも分かるようになりました。さらに、危険なサイトを閲覧しないようにSophos Intercept Xの標準設定に加えて、ハイパーと相談して怪しいサイトもブロックするようにしています」と対応を語る。
谷口氏も「これまでにインシデントが発生した経験がないので、Sophos Intercept Xによって安全性が向上したという実感はないのですが、コストの低減と運用負担の軽減という面では、導入した価値があったと評価しています。また、ランサムウェア被害ゼロという信頼性の高さや、エクスプロイト攻撃も防げるという面からも、安心感は大きく得られたと思います」と補足する。

フューチャービジョン

「UTMの更新を計画し将来的にはEDRも検討」

Sophos Intercept Xによりセキュリティ対策の安全性を向上させた総務部では、今後に向けた対策の強化も検討している。谷口氏は「UTMをソフォス製に更新したいと考えています。エンドポイントとUTMを連携させたSynchronized Securityを運用できれば、サイバーリスクを低減しインシデントの自動対応も実現できると期待しています。セキュリティ対策の自動化を推進できれば、総務部としての業務に注力できるようになります」と話す。
また、運用面でも濱氏は「もしも、サイバー攻撃の被害にあったときに、SOC（Security Operation Center）のように対応してもらえるSophos MDRサービスにも注目しています。膨大なログデータの解析や専門家でなければ発見できないシステムの脆弱性なども調査してもらえるようになるとハイパーから紹介を受けているので、今後の検討を考えています」と補足する。
さらに、谷口氏は「サイバー攻撃の脅威は、非常に速いスピードで発生しているので、セキュリティ対策にも同等かそれを上回るスピード感が求められています。それだけに、ハイパーのように新しい対策を提案してくれるパートナーの存在は重要です。これからも、優れたセキュリティ対策の提案と最新の情報提供に期待しています」と語る。

SOPHOS