SOPHOS

CUSTOMER CASE STUDY　**生活協同組合コープさっぽろ**

札幌市民生協として1965年に創立された生活協同組合コープさっぽろ。同組合は、北海道全域に108店舗を展開し、北海道に暮らす人々の生活に寄り添う事業を提供している。また、「つなぐ」を新たな経営の主テーマに設定し、過去の常識にとらわれず革新的な事業も展開している。同組合の情報システムも、デジタル推進本部が中心となり「コープさっぽろ版DX」を強力に推し進めている。

CUSTOMER-AT-A-GLANCE

つなぐ
COOP
SAPPORO

生活協同組合コープさっぽろ

本社所在地　札幌市西区発寒11条5丁目10番1号
会社設立　1965年に創立
（当時は札幌市民生協）
理事長　大見英明
出資金　80,370,632千円
（2021年3月20日現在）
事業内容　店舗事業、宅配事業、共済事業ほか

職員数　正規職員:2,405名
契約職員:2,228名
パート・アルバイト職員:10,110名
※従業員数は子会社含む数値
（2021年3月20日現在）
事業高　合計3,043億円(合計)
（2020年3月21日~2021年3月20日）
webサイト　https://www.sapporo.coop/
ソフォスソリューションズ　Intercept X Advanced Server with EDR

何らかの脅威が発生したとしても、Intercept X Advanced Server with EDR※がしっかりと守ってくれることに期待しています。

※Intercept X Advanced Server with XDRに改称

生活協同組合コープさっぽろ
デジタル推進本部 システム部 インフラチームリーダー
若松 剛志氏

生活協同組合コープさっぽろのデジタル推進本部では、2019年からオンプレミスで稼働してきたサーバー環境をAWSにすべて移行する（AWS All in）プロジェクトを推進してきた。運用するシステムは約190で、サーバーは約650に及ぶ。そのすべてをAWSへ移行するにあたり、サーバーセキュリティの強化と統合が課題となっていた。そこで、2020年からプロジェクトに参加したAWSに精通したエキスパートエンジニアである若松氏と山崎氏が中心となって、セキュリティ対策を強化するために、ソフォスのIntercept X Advanced Server with EDRが採用された。

ビジネスチャレンジ

「約650台のサーバーを安全に守り移行する取り組み」

Intercept X Advanced Server with EDRを採用した背景について、デジタル推進本部 システム部 インフラチームリーダーの若松剛志氏は、次のように振り返る。

「レガシーなシステムが多く、古いOSも数多く動いていました。組織が縦割りだったため、基盤も乱立していました。一部のシステムはAWS上で運用されていたものの、中核となるオンプレミスのシステムは、3つのデータセンターで稼働し、ルーターはコープさっぽろの本部内にありました。本部内に設置された巨大なルーターに、インターネットやデータセンター、工場、店舗がすべて接続されている複雑なネットワーク環境でした。そうした環境に、約190のシステムが、約650台のサーバー上で稼働していました。」

乱立するサーバー環境には、もうひとつ大きな課題があった。その課題について、若松氏は「サーバーごとに導入されているセキュリティ対策ソフトがバラバラで、統合的に管理されていませんでした。システムが構築された時期や部門によって、対応もそれぞれ

だったので、一元的なセキュリティ管理が困難な状況にありました」と説明する。
複雑なネットワーク環境と柔軟性に欠けるサーバー構成を改善するために、デジタル推進本部では全サーバーをAWSに移行する（AWS All in）プロジェクトをスタートした。そして「サーバーのAWS移行に合わせて、オンプレミスでもクラウドでも利用できるサーバー用のセキュリティ対策ソフトを選定し、すべて統合することにしました」と若松氏は導入の経緯を語る。

より安全に運用していくためには、
自動修復やSOC対応は、重要なポイントでした。

生活協同組合コープさっぽろ
デジタル推進本部 システム部 インフラチーム エンジニア
山﨑 奈緒美氏

テクノロジーソリューション

「3社の製品を比較検討してIntercept X Advanced with EDRを採用」

セキュリティ対策ソフトの選定にあたり、デジタル推進本部 システム部 インフラチーム エンジニアの山﨑奈緒美氏は、次の点に注目しました。

「検討段階では、3社の製品を比較検討しました。その過程で、まずは、スケールできるかどうかの性能を検討しました。auto scalingなど、管理者の手間を省いて自動でスケーリングできるか、といった機能に注目しました。以前に、AWS上のサーバーに導入したセキュリティ対策ソフトは、サーバーのスケーリングに追随できなかったので、苦労した経験がありました。そこで、クラウドで利用する上では、スケーリングへの対応が重要だと考えました。また、ディープラーニングによるファイル分析など、AIを活用した先進的な検知や解析機能も求めました。セキュリティ対策に関する運用負荷を軽減するためには、高度な検知性能をAIなどで自動化してくれる性能に期待したのです。そして、特に重視したのが、国内で信頼できるSOC（Security Operation

Center）を利用できるかでした。スタッフに負担をかけずに、安全に継続してサーバーを守っていくためには、国内で信頼できるSOCに依頼できる製品が必要でした。」
検知性能やスケーリングにSOC対応といった項目に加えて、山崎氏が判断したのは「自動修復の機能です。デジタル推進本部には、セキュリティの専任者がいないので、これまでは何かアラートがあがったときには、個別に調べて対処していました。そうした労力を省いて、より安全に運用していくためには、自動修復も、重要なポイントでした」と説明する。
こうした総合的な評価を経て、デジタル推進本部ではIntercept X Advanced Server with EDRを採用した。

導入の成果

「約60台のAWS上のサーバーに適用」

AWSへ移行する全サーバー数を想定し、コープさっぽろのデジタル推進本部では、2021年4月に650台分のライセンスを契約した。その後、AWSに移行したサーバーは、すべてIntercept X Advanced Server with EDRによるセキュリティ対策を実施している。現状の取り組みについて、若松氏は「2021年10月の時点で、約60台のサーバーをAWSに移行しました。移行後は、順調に稼働しています。Intercept X Advanced Server with EDRからのアラートは、ほとんどあがってこないので、滞りなくセキュリティ対策が機能していると判断しています」と導入の成果を語る。
そして「最初から全サーバー分のライセンスを契約しているので、AWS向けだけではなく、まだオンプレミスで稼働しているサーバーにも、順次Intercept X Advanced with EDRを導入していく計画です。今は、AWS All inが最優先事項なので、実際に取り掛かってはいませんが、セキュリティ対策の強化も急務だと捉えています」と若松氏は補足する。

今後の展望

「AWS対応のソフォス製品への期待とセキュリティの強化」

今後に向けた取り組みについて、若松氏は「AWSの管理ルールの中に、ソフォスの製品もラインナップされているので、そちらは将来的に利用するかも知れません。また、Sophos Cloud Optixというクラウドセキュリティポスチャ管理にも、興味はありますが、検討には至っていません。今は、サーバーのAWS移行に伴って、Intercept X Advanced Server with EDR対応の推進が急務です」と話す。
さらに「現在はまだ、台数が少ないので、アラートも少ないのかも知れません。今後、すべてのサーバーをAWSに移行し終えたときに、何らかの脅威が発生したとしても、Intercept X Advanced Server with EDRがしっかりと守ってくれることに期待しています」と若松氏は語った。

SOPHOS