生活協同組合コープさっぽろ 様

サーバーのセキュリティ対策にIntercept X Advanced with EDRを導入
CEC SOCがコープさっぽろのDX推進をセキュリティ面で支える

CEC
Computer Engineering & Consulting

Intercept X Advanced with EDR & CEC SOC

導入事例

インフラのモダナイゼーションに取り組むなかで、Intercept X Advanced with EDRとCEC SOCでセキュリティを強化。シーイーシーの手厚いサポートにより、DX推進に注力。

課 題

- インフラ基盤ごとに縦割りのセキュリティ対策で統一化されていなかったため、運用状況やコストなどを把握できない
- オンプレミスからクラウドへの移行作業でリソースがなく、セキュリティ脅威の対処に携わる専任者がいなかった
- 脅威の監視およびアラートが発生した場合の対策としてSOCの導入が必要だった

効 果

- Intercept X Advanced with EDRにより、セキュリティの運用状況を一元的に把握
- Intercept X Advanced with EDRの自動検知・駆除により、人的リソース不足の解消
- 実績と経験豊富なCEC SOCの導入により、24時間365日の強固なセキュリティを実現

導入の背景・課題

デジタル化でクラウド移行が急加速

1965年に設立された生活協同組合コープさっぽろ（以下、コープさっぽろ）は、北海道全域で事業を展開する歴史の長い生活協同組合。従業員はパート・アルバイトを含めて約15,000人、事業規模は全国の生協のなかで最大級を誇る。そのコープさっぽろが近年、急速に推し進めているのがデジタル化だ。

「もっと使いやすく、買い物しやすく、職員が働きやすい環境の構築を目指し、ここまで大規模な組織に成長してきましたが、実際のところは建て増し構築や外部ベンダー任せのシステム開発がほとんど。今後、組織の規模に見合ったサービスを組合員様に届けるには、これまでのようなやり方では通用しません。情報共有とスピード感をベースに組織内のコミュニケーションを高め、業務の進め方を変革していく必要があります。そこで、システム部と広報部とシステムサポート部という3つの部門から成るデジタル推進本部を立ち上げ、デジタル化に向けてレガシーなインフラのモダナイゼーションに取り組んでいます。」と語るのは、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。

そのデジタル化の大きな柱となっているのが、内製によるオンプレミスからクラウドへの移行だ。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 奈緒美氏は次のように話す。「長年にわたって構築・運用されてきたオンプレミスのシステムを、丸ごとクラウドへ移行している最中。紆余曲折はありましたが、今のところ移行は軌道に乗っていると思います。」

課題と感じていたセキュリティ対策

クラウド移行するにあたって、コープさっぽろが課題と感じていたのはセキュリティだった。それぞれのインフラ基盤ごとに縦割りのセキュリティ対策が取られていたこと、端末のセキュリティ対策ソフトに複数の製品が採用されてことなど、運用を統一できていなかった。なかには保守切れの製品もあったという。これについて若松氏は「そもそもレガシーなところにメスを入れていくのがモダナイゼーションのテーマでしたから、このセキュリティ対策状況に驚きはありませんでした。まずは、端末をすべて入れ替えることでセキュリティ対策ソフトの統一化を図り、クラウド側は移行が終わったサーバーから順にセキュリティ対策を施そうと考えました。」と語る。

ベンダーの選定

決め手はお任せ運用とCEC SOC

サーバー側のセキュリティ対策として比較・検討したのは、ソフォスのIntercept X Advanced with EDR（以下、ソフォス）をはじめとする3製品。その中からソフォスを選定した理由について、山﨑氏は以下のように語っている。

＜お任せで運用できる＞

「我々はクラウド移行作業で手が離せません。かといって、セキュリティの専任チームを立ち上げるほどリソースに余裕はなく、これがセキュリティに関する大きな課題でした。そこで求めたのは自動化です。ソフォスなら高性能なAIのディープラーニングによって自動的に処理してくれま

生活協同組合コープさっぽろ 様

サーバーのセキュリティ対策にIntercept X Advanced with EDRを導入
CEC SOCがコープさっぽろのDX推進をセキュリティ面で支える

CEC
Computer Engineering & Consulting

Intercept X Advanced with EDR & CEC SOC

導入事例

す。我々は定期的に管理コンソール画面をチェックするだけの運用方法に期待しました。」

＜CEC SOCが利用できる＞

「ソフォスには脅威を検出した場合、その脅威がどこから侵入して、何をしようとしたのかをグラフィカルに表示する根本原因解析（RCA）機能がありますが、ソフォスが非自動である影響範囲の特定や、そもそもの原因究明、およびCSIRTからみた恒久的な対策の3点については、専門家にアドバイスを求めたいと考えていました。その点について、ソフォスはベンダーであるシーイーシーのCEC SOCを利用できるとのこと。ソフォスのJapan Next Gen Partner of the Year Awardを受賞しているシーイーシーに任せることができれば、脅威を検知したときでも安心です。我々はクラウド移行に専念できます。」

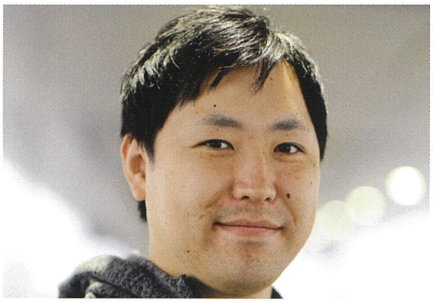
＜スケールがしやすい＞

「企業の成長にともなうサーバー増強などを想定すると、スケールのしやすさも欠かせない要件。追加サーバーを自動的に保護の対象に入れるオートスケーリングも構想に入れており、そうした場合の選択肢はソフォスでした。」

導入の進捗と効果

守られている安心感を獲得

コープさっぽろが購入したソフォスのライセンスはサーバープロテクションに必要な541台分。2021年2月から順次導入を開始し、4月から本格的な運用も始まっている。年度内までにはすべてのサーバーに入れる体制で動いているという。



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

そうした現状のソフォスおよびCEC SOCの運用状況について、若松氏は次のように語った。「アラートと呼べるものは出ていないため、ソフォスおよびCEC SOCの実力に触れる機会は今のところありません。とはいえ、何もないのがベストなわけですから、ソフォスおよびCEC SOCに守られている安心感を得たまま、平穏無事に作業を進められることを願っています。」

また、CEC SOCに満足しているという山崎氏は「CEC SOCはサービスをカスタマイズできる点、運用ごとにある程度の運用設計のひな型を持っている点にメリットを感じました。さまざまな運用スタイルのお見積りを何度も出していただき、大変感謝しています。若松が言ったように、現在のところ気になるインシデントはなく、CEC SOCからいただく月1回のレポートを見ても、重大なものは報告されていません。」と語る。

これに対し、CEC SOCのセンター長 古山は「CEC SOCとしては、怪しい兆候には漏らさず対応します。アラートが発生した場合の方針は、影響範囲を隔離するのが第一段階。その後、原因を究明し、再発防止に向けて最善の解決方法を提案させていただきます。」と話す。

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

今後の展望

ソフォス製品およびCEC SOCに期待

コープさっぽろは引き続きセキュリティ対策を続けていく予定で、基本的にはクラウド側が提供するセキュリティサービスを中心に固めていく形になるという。「今後、導入する予定があるのはWAFですが、我々でシグネチャーを設定するのはハードルが高い作業だと思っています。そういう意味では、ソフォス製品のマネージドルールに期待する部分はあります。」（若松氏）

また、コープさっぽろが考えるDXについて伺ったところ、若松氏は「DXに形はなく、我々が答えるものでもないと思いますが、現場の立場から言わせていただきます。オンプレミスからクラウドに移行する流れのなか、わずか1～2年でコミュニケーション手法が変わり、働き方も大きく変わりました。コープさっぽろ全組織的に、インターネット上で仕事をしていくスタイルが顕著になってきたと思います。我々はクラウド移行で下支えしつつ、コープさっぽろのDXに貢献できればと考えています。」と語った。

お客様プロフィール

生活協同組合コープさっぽろ 様

つなぐ COOP SAPPORO

1965年創立の札幌市民生活協同組合を母体した生活協同組合。北海道28市20町にかけ107店舗（2021年3月20日現在）を展開。2006年10月には、コープこだわりの商品を組合員の自宅まで届ける宅配サービス、「コープ宅配システム トドック」を開始。毎週月～金、決まった曜日・時間に、20市17町にわたる39センター10デポ（2021年6月25日現在）の地域担当が商品を配送する。このほか、夕食宅配サービス、CO・OP共済、保険、ファイナンシャルプランナー、エネコープ、トドック電力など、幅広いサービスを提供。組合員数は180万人以上。北海道で生きることを誇りと喜びにするために「人と食をつなぐ」「人と人をつなぐ」「人と未来をつなぐ」をテーマに事業を展開している。

本　社　〒063-8501
札幌市西区発寒11条5丁目10番1号

代表者　理事長　大見 英明

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（2021年3月20日現在）

事業高　3,043億円
（合計 2020年3月21日～2021年3月20日）

URL　https://www.sapporo.coop/

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

202111-003-026CI