株式会社セブン&アイ・ホールディングス

セキュリティ基盤を刷新し サイバーリスク対応を迅速・高度化

背景	事業会社がECサイトや業務系システムで利用するグループ共通インフラの刷新に合わせて、柔軟かつ迅速にサイバーリスクに対応できるセキュリティ基盤の構築が求められた。
ソリューション	セキュリティ基盤の中核ツールとして、ログデータ管理・分析プラットフォームの「Splunk」を採用。多種・多量のログを自動的に集約、相関させることで多層的な分析ができる環境を整備した。
成果	高度なログ分析が実現し、サイバー攻撃などへの対応が迅速になった。従来なら攻撃の調査に数日かかっていたような複雑なケースでも即時の調査対応が可能になるなど、オペレーションが大幅に効率化した。

コアテクノロジー

サイバーセキュリティの知見、統合ログ管理・分析プラットフォーム「Splunk」の導入・活用ノウハウ

システム概要

●統合ログ管理・分析プラットフォーム：Splunk

関連 SDGs

地域コミュニティとともに住みやすい社会をつくる

株式会社セブン&アイ・ホールディングス
本社：東京都千代田区二番町8番地8
設立：2005年
資本金：500億円（2022年2月末現在）
グループ売上高：14兆2432億7000万円（2022年2月期）
従業員数：連結17万757名（2022年2月末現在）

※グループ売上高は、セブン-イレブン・ジャパン、セブン-イレブン・沖縄および7-Eleven, Inc.における加盟店売上高を含む。従業員数は、月間163時間換算の臨時従業員を含む。

変化するサイバーリスクに対応

大手流通グループの持ち株会社であるセブン&アイ・ホールディングスは、2019年から事業会社が共通して利用するITインフラの刷新に取り組んでいた。

このグループ共通インフラの刷新において、セブン&アイ・ホールディングスが重視したポイントの一つは、セキュリティ対策だ。

グループDX推進本部セキュリティ基盤部シニアオフィサーの廣畑順也氏は、「サイバーリスクが一層高まり、リスクトレンドも変化しているなかで、最新のリスクにも柔軟に対応できるセキュリティ対策をグループ共通インフラに導入する必要がありました。この共通インフラには、例えばセブン&アイグループの各種サービスで使える共通アカウント『7iD』の管理システムがあり、登録会員数は2400万人以上に上ります。この大規模なグループ共通インフラやその上で稼働するさまざまなアプリケーションを、よりセキュアに運用することが重要な要件となっていました」と語る。

強固なセキュリティ対策を導入するにあたり、セブン&アイ・ホールディングスは、すでにグループ共通インフラの構築に携わっていた日鉄ソリューションズ（以下、NSSOL）に支援を依頼した。

サイバーリスクの分析に注力する

セブン&アイ・ホールディングスが目指したのは、分散したサーバーやネットワーク機器などから多種・多量のログを集約し、多層的な分析によってサイバー攻撃などに対処できるセキュリティ基盤の構築である。同社はその中心に、ログデータ管理・分析プラットフォームの「Splunk（スプランク）」を据えた。

グループDX推進本部セキュリティ基盤部オフィサーの井上裕司氏は、Splunkの導入についてこう話す。

「セブン&アイグループ全体のセキュリティを向上させるため、私たちはサイバーリスクの監視や分析に注力しなければなりません。そのためには、ログ収集などの作業から解放される必要があり、そのうえで高度な分析ができる環境を求めていました。Splunkは、各所からログを自動で集約し、サイバーリスクをリアルタイムに可視化できるツールとして導

株式会社セブン＆アイ・ホールディングス
グループDX推進本部
セキュリティ基盤部
シニアオフィサー
廣畑 順也氏

株式会社セブン＆アイ・ホールディングス
グループDX推進本部
セキュリティ基盤部
オフィサー
井上 裕司氏

株式会社セブン＆アイ・ホールディングス
グループDX推進本部
セキュリティ基盤部
美濃 圭佑氏

入しました」。

新しいセキュリティ基盤の構築作業は、NSSOLの支援によって順調に進んだ。

グループDX推進本部セキュリティ基盤部の美濃圭佑氏は、「システムオーナーから、各システムのニーズに合わせてログの収集方法などを変えたい、といった柔軟性を求める声が強かったのですが、NSSOLは、私たちが望んでいるタイミングで、望んでいることを実現してくれました。技術的に難しい要件変更などにも柔軟に対応してくれています。NSSOLはプロジェクトマネジメントがうまく、現場のシステムエンジニア一人ひとりの技術力も高かった」と振り返る。

より深いインサイトを得られた

新しいセキュリティ基盤により、サイバーリスクへの対応スピードは大幅に向上した。

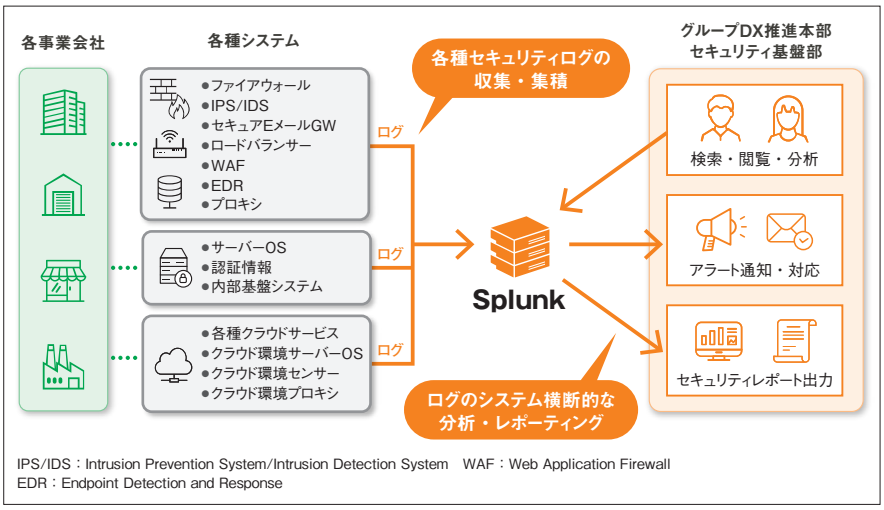
「従来と比べ、監視しているログの量は段違いに増えていますが、それらをSplunkで高速に収集・処理して、より高度な分析を短時間で実現しています。また、Splunkが持つ、さまざまな機能の組み合わせにより、システムオーナーが必要としているセキュリティ情報を非常に簡単かつ定期的に報告できるようになりました」と美濃氏は評価する。

廣畑氏は、サイバー攻撃を受けた際に、これまでよりも深いインサイトを得られるようになった点が大きいと語る。

「メールセキュリティだけとか、エンドポイントセキュリティだけを見ていても、表面的なことしか分かりません。しかし、新しいセキュリティ基盤では、これらのログを統合して相関的に分析することで、攻撃者がどのような手口を使い、どの程度の影響が実際に出ているのかなど、従来なら調査に数日かかるような複雑なケースでも即時に調査を開始して、その日のうちに関係者に報告し、迅速に対策を推進できるようになりました」。

セブン＆アイ・ホールディングスは今後、グループ共通インフラだけでなく、各事業会社が独自に運用しているシステムも含めて、サイバーセキュリティ対策を支援していく考えである。

■セブン＆アイ・ホールディングスのセキュリティ基盤に「Splunk」を導入



IPS/IDS：Intrusion Prevention System/Intrusion Detection System　WAF：Web Application Firewall
EDR：Endpoint Detection and Response

お問い合わせ

NS Solutions

日鉄ソリューションズ株式会社
東京都港区虎ノ門一丁目17番1号 虎ノ門ヒルズビジネスタワー

Printed in Japan