sumo logic

CASE STUDY

SaaS型SIEMソリューションでログのモニタリング体制を最短で整備

Coincheck

課題

コインチェック株式会社は、2018年1月の仮想通貨NEM不正流出事故を受け、仮想通貨取引所サービスのシステムをインフラから再構築し、セキュリティの強化に取り組んでいる。その1つとして、ログのモニタリングの強化を行った。クラウドサービスサーバやネットワークセキュリティ機器、端末類のログを一元管理し、不正アクセスなどのログをいち早く検出して対処することで、セキュリティ事故を未然に防ぐことが狙いで、可能な限り短期間での導入が求められていた。

導入経緯

モニタリングのシステムには、「Sumo Logic」を採用。SaaS型ゆえに短期導入が可能な点、優れたユーザインターフェース、充実したサポートが決め手となった。クラウドサービスのサーバ、オンプレミスのネットワークセキュリティ機器、エンドポイントの端末類のログをSumo Logicに集約。あらゆる事態を想定し、セキュリティ事故の原因になり得る事象が検出されれば、アラートをあげる仕組みを構築した。

導入効果

システムすべてを横断的にログ管理し、膨大なログの中から不正アクセスの予兆などを検出でき、迅速な対処が可能となった。そのため、高いレベルでのセキュリティの担保だけでなく、さらにコンプライアンスやガバナンスを強化できた。Sumo LogicはSaaS型であるため、狙い通りの短期導入も実現した。今後は分析機能をより活用しつつ、パフォーマンス監視などセキュリティ以外へのSumo Logicの活用を検討していく。

SaaS型による導入の容易さと優れたUIを評価し、Sumo Logicを採用

仮想通貨取引所サービスを柱に事業展開するコインチェック株式会社。同社は2018年1月に発生した約580億円相当の仮想通貨「NEM」の不正流出事故を受け、部分的にサービスを停止し、経営管理態勢や内部管理態勢の改善を実施した。それとともに、システムをインフラから再構築し、セキュリティの強化に取り組んだ。

具体的な施策の柱の1つがログのモニタリングである。システムのログを一元的に監視・分析を行い、不正アクセスなど重大なセキュリティ事故につながりかねないログがあれば、迅速に対処することでセキュリティを強化する。その中心となる仕組みとして、SIEM（Security Information and Event Management）を導入することにした。

業種

金融

所在地

東京都渋谷区渋谷3-28-13 渋谷新南口ビル3F

従業員数

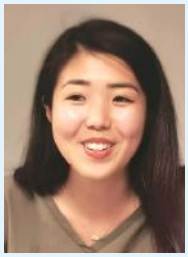
168名（2019年3月末時点）

導入ソリューション

Sumo Logic

コインチェック株式会社
サイバーセキュリティ
推進部長
大浦 秀昭氏

コインチェック株式会社
サイバーセキュリティ
推進部
喜屋武 慶大氏



コインチェック株式会社
サイバーセキュリティ
推進部
中井 祐季氏

複数のSIEMソリューションを比較検討した末に採用したのが、Sumo Logic社の「Sumo Logic」である。Sumo LogicはSaaS型のSIEMソリューションであり、世界約1600社で導入されている実績を持つ。

コインチェック株式会社 サイバーセキュリティ推進部長 大浦秀昭氏は、その採用理由を次のように語る。

「何と言ってもSaaS型であるがゆえに、スピーディに導入できる点が大きな魅力でした。当時、当社は可能な限り短期間でモニタリング体制を再整備することが必須でした。Sumo Logicの充実したサポートや豊富なドキュメントも、短期導入の大きな助けになりました」(大浦氏)

優れたユーザインターフェース(UI)も採用のポイントとなった。コインチェック株式会社 サイバーセキュリティ推進部 喜屋武 慶大氏は「他社ソリューションに比べて、Sumo LogicはシンプルでわかりやすいUIであり、より直感的に操作できる点を高く評価しました」と話す。

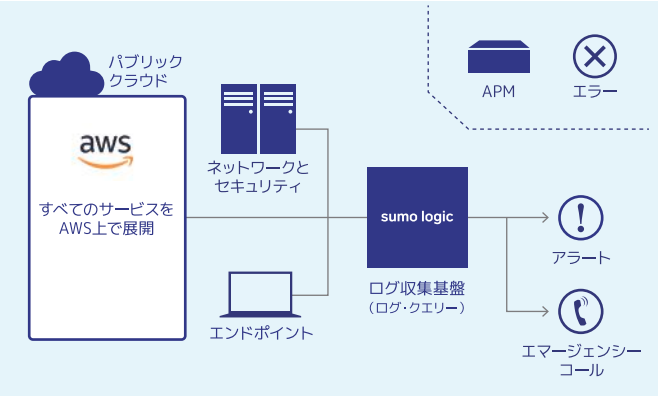
クラウド、オンプレミス、エンドポイントを包括的にモニタリング

コインチェックの新システムでは、サービスサーバ類はすべてAWS上に構築し、一部のネットワークセキュリティ機器のみをデータセンター内にオンプレミスで設置。それらに加えて、エンドポイントも含めたすべてのシステムのログをSumo Logicに集約してモニタリングできる構成とした。

「想定し得る限りのあらゆる事態やリスクをログから検出できるよう、必要なクエリーを用意しておきます。もし該当するログを1件でも検出したら、ビジネスチャットツールなどによるアラート、または電話によって自動通知する仕組みを構築しました」(喜屋武氏)

そのようなモニタリングシステムの構築は、期待通り短期間で行うことができた。Sumo LogicはSaaS型であることに加え、定番の分析が用意され、AWSをはじめ主要クラウドサービスやOSSも含めた主要製品に対応したモニタリングのテンプレートが約160種類揃っており、短期間で容易な導入を可能としている。

コインチェック株式会社 サイバーセキュリティ推進部 中井 祐



コインチェック様 システム概要

季氏は「当社の要件やシステムに合わせてテンプレートを選び、ログを取り込むだけで、すぐにモニタリングを始められました。また、クエリーに関しても、Sumo Logicが書き方など手厚くサポートしてくれたので、スムーズに作成できました」と振り返る。

モニタリング体制を最短で整備し、セキュリティ強化を実現

コインチェックはSumo Logicの導入によって、当初の狙い通りにモニタリング体制を整備できた。

「システムすべてを横断的にログ管理・モニタリングが可能となりました。Sumo Logicは、まさに当社SOCシステムの要と言うべき存在でしょう」(喜屋武氏)

必須であった短期間での導入についても、「当社が必要とする機能と品質を備えたモニタリング体制を最短で整備できました。セキュリティを強化できただけでなく、コンプライアンスやガバナンスも確保できて、大変満足しています」と大浦氏は語る。

同社は今後、Sumo Logicのさらなる活用を図っていく予定だ。

「Sumo Logicにはまだ我々が活用できていない豊富な機能が用意されています。Sumo logicを当社の監視・分析プラットフォームとしてさらに活用していくことで、セキュリティをより強固にするだけでなく、サービス内容やシステムの改善にもつなげていきたいと考えています」(大浦氏)

コインチェックについて

2012年8月設立。仮想通貨販売所・取引所サービス「Coincheck」を提供。Bitcoinに加え、NEMやRippleなど9種類の仮想通貨を取り扱う。2018年4月にマネックスグループ株式会社の100%子会社となり、2019年1月に仮想通貨交換業者登録完了。他に、貸仮想通貨サービス「Coincheck Lending」や「Coincheckでんき」なども提供している。

Sumo Logic ジャパンについて

Sumo Logicは2010年に米国で設立。SaaS型SIEMソリューション「Sumo Logic」は、アプリケーションごとに分散したログを一元管理・分析する。大量のログデータをパターンマッチングで圧縮して人が把握しやすい量にする「LogReduce」、任意の時間、データソースを比較する「LogCompare」など、高度な機械学習分析も提供。ユーザは世界で約1600社にのぼる。2018年10月、日本法人となるSumo Logicジャパン株式会社を設立した。

sumo logic

Sumo Logic ジャパン株式会社
Email: info-jp@sumologic.com

sumologic.jp