注目度の割に活用が進まない SIEM

工数とコスト　クラウド SIEM はどこまで課題を解決できるか

sumo logic®

x

NIKKEI XTECH

考え方の有効性は認識。しかし現実は違う

セキュリティ被害が後を絶たず、多くの企業が効果的な対策を模索する中、近年「SIEM（Security Information Event Management：セキュリティ情報イベント管理）」に注目が集まっている。SIEM を活用すれば、各種セキュリティ製品をはじめ、ネットワーク機器や OS、ミドルウエア、各種アプリケーションといったシステムのログを収集して統合的に管理可能。さらに、それらログの相関分析を行うことで脅威の侵入や活動の状況を明らかにすることができるという期待からだ。

たしかに、SIEM が標榜している通りの効果を発揮できれば、セキュリティを向上できる。だが、現実はそう簡単ではない。

課題の 1 つは多くの企業のシステムは、まだ部門ごとに個別最適化されており、全社的に SIEM を適用しようとすると膨大な工数がかかってしまうという点だ。クラウドサービスの普及によって、オンプレミス、プライベートクラウド、パブリッククラウドとシステム環境も多様化しており、そのこともこの課題に拍車をかけている。

例えば金融分野では、一般的にオンプレミスに基幹システムが設置され、Windows、Linux、そして UNIX やメインフレームなど、ヘテロな環境となっていることが多い。同時に、FinTech への取り組みを背景にクラウドを活用したオンライン金融サービスの開発なども進んでおり、この環境下で SIEM を適用するには膨大な手間を要してしまう。

もう 1 つ問題となっているのがコストだ。一因となっているのが変動するログの量である。

分かりやすいのがゲーム業界だ。次々に新タイトルが投入されるゲーム業界において、いつサービスがヒットしてアクセスが急増するかは予測が困難だ。結果、SIEM を導入する際には、最初から多めに余剰リソースを見込んでおく必要がある。そうした余剰のリソースは、当然、平時にはムダなコストとなってしまう。

このような課題によって、SIEM は有効性を認識されつつも、実際には導入に至っていない、あるいは十分に活用できていないというケースが多い。だが、これらの課題をクリアして SIEM を有効活用している企業も実際にはある。カギはクラウドだ。具体的に成功企業は、どのようなサービスを選定し、どう課題をクリアしているのか。それを見ていこう。

クラウドとの組み合わせで SIEM が変わる

Sumo Logic ジャパン立ち上げメンバー：
左から *Sumo Logic* ジャパン セールス・ディレクター 古根川 哲也氏、
カントリー・マネージャー ロバート・スチーブンソン氏、
マーケティング・ディレクター 若色 亨昌氏

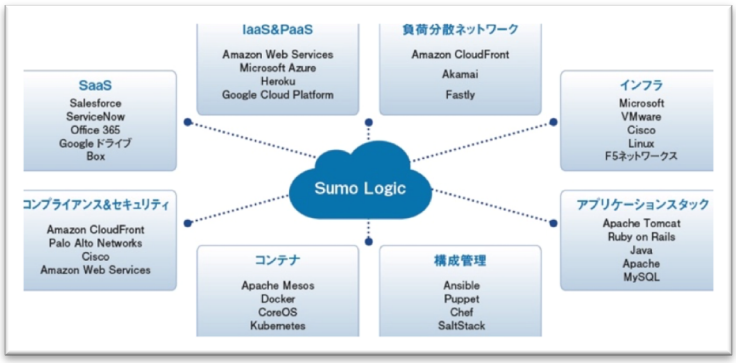
既存の SIEM の課題を解決するサービスとして、グローバルに高い評価を得ているサービスがある。「Sumo Logic」だ。

提供元である Sumo Logic 社は、2010 年に米国で設立。現在では、世界で約 1600 社のユーザーを獲得している。2018 年 10 月には、日本法人となる Sumo Logic ジャパンが設立され、サービスのローカライズや日本語によるサポート体制が急加速で進められている。

「Sumo Logic の最大の特徴は、クラウドサービスであること」と Sumo Logic ジャパンのロバート・スチーブンソン氏は紹介す

る。クラウドやオンプレミス環境で運用している多種多様な機器やアプリケーションなどが生成するログの収集・統合・分析をクラウド上で実現するのである。

具体的に Sumo Logic は、セキュリティ、ネットワーク機器、仮想化基盤など、標準で 200 を超えるアプリケーションに対応し、多様なログ、メトリクスを収集し、統合管理することが可能（図）。さらにクラウドサービスならではの強みとして、AWS（Amazon Web Services）や Microsoft Azure、Google Cloud Platform をはじめとするメジャーパブリッククラウドともネイティブに連携可能。この特徴により、Sumo Logic は SIEM の大きな課題である、連携時の工数を大きく削減する。



図●Sumo Logic の連携アプリケーション例：主要なベンダーのアプリケーションとはほぼ連携可能な上、独自アプリケーションにも対応可能

加えて、急激なログの増大といった課題についても、クラウドの強みが生きる。

「ログを格納するストレージリソースは、企業規模やサービスレベルなどのニーズに合わせてヨタバイトレベルまで柔軟に拡張可能です。当然、スモールスタートしてスケールアウトしていくことも容易。ログデータは月単位の容量課金ですが、仮に契約の 10 倍以上のデータを取り込んでもサービスはすぐには停止せず、翌月以降に契約を見直しさせていただきます」と同社の古根川 哲也氏は言う。

膨大なログの中から問題のありそうな箇所を瞬時に抽出

Sumo Logic は、ログの分析機能にも定評がある。

まず「LogReduce」という機能は、蓄積された膨大なログの中から、問題のありそうな箇所の抽出を支援するもの。「AI／機械学習を使ったパターン分析を行っており、ボタンクリック 1 つで対象となるログ全体から例外的なパターンを瞬時に探し出して、分析者が着目すべき部分として示します」とスチーブンソン氏は説明する。

また、抽出結果の表示画面には「いいね！」ボタンが付されており、Sumo Logic の提示結果が適切だと考えれば、そのボタンをクリックすることで AI がそれを学習。継続的な利用の中で分析精度を高めていくことができる。

クラウドと *SIEM* の親和性の高さ、*Sumo Logic* の優位性を強調するスチーブンソン氏

「LogCompare」と呼ばれる機能もある。こちらは、現在のログを過去の任意の時間のログと比較するためのもの。

例えば、システムをリリースしたタイミングで、リリース前のある時点と現状を比較すれば、アプリケーションがシステムの稼働に悪影響を及ぼしていないかなどを把握することが可能。ほかにもサーバーの稼働状況を別のサーバーと比較したり、セキュリティインシデントの発生前と後で影響範囲を調査したり、様々な用途で有効となる。

ほかにもメトリクスなどの数値が任意のしきい値を逸脱した際に異常値として通知する「Outlier Detection」、問題発生時

の状況をベースに時系列データから将来、同様の問題が発生するタイミングを予測する「Predictive Analytics」などの機能がある上、グローバルにビジネスを展開する主要セキュリティベンダー数社が提供するスレートインテリジェンスとも標準で連動しており、最新かつ精度の高い脅威情報を基に分析を行うことができる。

「なお、そうした主要セキュリティベンダーのほとんどが Sumo Logic のユーザーでもあります。ベンダーとしての脅威分析に我々のツールを活用しているのです」と同社の若色 亨昌氏は続ける。

金融、ゲーム関連企業をはじめ多くの企業が高く評価

Sumo Logic のダッシュボードは、直感的に理解しやすいインタフェースデザインとなっており、使い勝手のよさを評価する声も多い（画面例）。「専門のオペレータやエンジニアでなくとも、誰もが使いこなせることから、お客様のログ領域における『データ民主化』にも寄与するものと考えています」とスチーブンソン氏は言う。

画面例●Sumo Logic 画面イメージ
オンプレミス、クラウドを問わず、あらゆるログを収集して、ビジュアルと数値で 1 画面に表示。機械学習による分析を通じて検知した「驚異」や「違和感」の本質を瞬時に把握できる

例えば、収集したメトリクスをダッシュボードで可視化し、システムの稼働状況をグラフで確認しながら、気になる箇所があれば、関連のありそうなログカテゴリを指定。すると、グラフと同じ時系列で出力されているログの量がヒートマップで示される。仮に予約機能のあるオンラインサービスで、予約失敗のメトリクスとログ出力が同じタイミングで急増していれば、エラーログだと推察することができる。そこから、メトリクスグラフをクリックして、その時点のログを一斉に抽出した上で、特定のインスタンス、特定のサーバーというようにログを絞り込み、原因を究明。これらの操作をほぼクリック操作だけで行える。

既に述べた通り、Sumo Logic はグローバルで約 1600 社のユーザーに導入されている。英国を本拠に銀行業を核とした多彩なビジネスを展開するヴァージン・マネー（Virgin Money UK）は、デジタルトランスフォーメーションの推進に向け、IT 環境のモダナイゼーションに取り組んだ。特に金融サービスにおけるセキュリティについては、誰が、いつ、どんな取引を行ったかを正確に把握することが求められることから、AWS をインフラとしたシステム再構築に際し、同社は Sumo Logic を採用している。

また、国内では、ソーシャルゲームプラットフォームの展開で知られるグリーも Sumo Logic のユーザーだ。同社をはじめ、サービスを常に最適な状態で稼働させるために、数多くのゲーム関連企業が Sumo Logic を採用している。

データ連係と大量ログデータの収集という SIEM の機能を考えると、SIEM とクラウドは明らかに親和性が高い。クラウド SIEM の先駆的存在として既に豊富な実績を持つ Sumo Logic の存在感は、今後さらに高まりそうだ。

sumo logic®
Sumo Logic ジャパン株式会社
info-jp@sumologic.com
https://www.sumologic.jp/