株式会社ラック　CloudFalcon®

サイバー攻撃自動分析システムをAWS上に構築

経済産業省が公開した「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティリスクは経営課題であると定義されているように、多くの企業が情報システムと情報の保護に取り組んでいる。
サイバー攻撃から情報システムを保護する最前線は境界防御だ。だが、侵入検知 / 防御システムやファイアウォールなどのセキュリティ対策機器を導入していても、正しく運用できていない企業が多い。
ラックは、すべての企業が境界防御システムを最大限に活用するためのサービス「CloudFalcon」を Amazon Web Service（AWS）に構築した。

ネットワーク境界防御の現状

今や、ほぼすべての企業が情報システムを活用し、企業経営と事業展開を行う時代となった。生産管理や在庫管理、サプライチェーンなどあらゆる業務はデータ化され、それらの情報をBIツールで活用し経営者が直接閲覧し、スピーディーな経営に向け取り組んでいる。

経済産業省と独立行政法人情報処理推進機構（IPA）は、2015年12月に「サイバーセキュリティ経営ガイドライン」の初版を公開した。このガイドラインでは、「サイバーセキュリティは経営問題」と宣言し、情報とシステムの保護は経営者の責任と指摘している。これに呼応し、多くの企業が情報システムの保護に積極的に取り組み、多層防御と呼ばれる複数のセキュリティ対策を組み合わせ、巧妙化するサイバー攻撃への対応を行っている。
ウイルス対策製品や次世代ファイアウォールなど、セキュリティ対策製品の導入率は高まっているが、それらが的確に運用されているかというと課題が残るのが現状である。

セキュリティ事業推進部 テクノセンター北九州 センター長 井原 康博は、「大手企業を中心にCSIRT（シーサート：サイバー攻撃による事故対応組織）を組織化する企業が増えていますがまだ少数です。多くの企業は、設置されているセキュリティ対策機器が発する警告に気が付いていない場合が見受けられます。」と語る。

ラックのサイバー救急センター®が対応したインシデント（事故）でも、セキュリティ対策機器の警告からサイバー攻撃の痕跡がありながらも、それらに気が付かず被害を拡大した事例を確認している。

セキュリティ事業推進部 セキュリティシステム開発室 新倉 康弘は、「私はJSOC® マネージドセキュリティサービス（MSS）のシステム開発を担当していますが、セキュリティ技術者が複数のデータソースを相関分析しなければ、サイバー攻撃の発見は難しいと考えています。」と、データ分析の重要性を語る。

CloudFalconの開発

MSSは、セキュリティ機器の保守運用と、機器が発する警告からサイバー攻撃を見分けるサービスだ。世界中から行われるサイバー攻撃を、24時間365日休むことなく監視する、高いサービス品質を要求される。

JSOCは日本最大規模の施設と、100名を超えるセキュリティ技術者がローテーションを組んで800を超える組織へセキュリティ監視サービスを提供しているが、最高クラスのサービスのため料金は高額となる。また、セキュリティ監視の対象となる機器は、ハイエンドモデルに限られている。

セキュリティ事業推進部
テクノセンター北九州
センター長 井原 康博

セキュリティ事業推進部
セキュリティシステム開発室
グループリーダ 新倉 康弘

しかし、高額なセキュリティ対策費用を支払える企業は限られており、多くの企業は導入しやすい価格帯のセキュリティ対策機器を、監視・運用サービスを導入せずに運用している。

ラックのセキュリティ事業部では、セキュリティ監視・運用サービスの価格を抑えることでこの状況を改善できると考え、「CloudFalcon」を開発した。

CloudFalconは、クラウド上に構築されたサイバー攻撃自動分析システムである。セキュリティ対策機器から発せられる警告情報を収集し、サイバー攻撃の痕跡を発見する機能を提供する。対象となるセキュリティ対策機器は低価格のものにも対応しているとともに、セキュリティ技術者が常時監視するのではなく、CloudFalconが自動的に分析を行う。

CloudFalconの特長としては、JSOC MSSが政府機関や大手企業のセキュリティ監視で得られた知見を、最新の脅威分析に活用している点が挙げられる。

CloudFalcon ダッシュボード

CloudFalconの販路は、パートナー専売モデルを取っている。パートナー企業の独自サービスに仕立てることで、よりきめ細やかな顧客対応と低価格化を実現し、より多くの企業を支援することを目指している。

新倉は「ITシステムの安心と安全のためにJSOCの導入を検討しても、どうしても費用面で折り合わない場合が多いですが、CloudFalconであればご納得いただけるでしょう。」と語る。

クラウドプラットフォームはAWSを選定

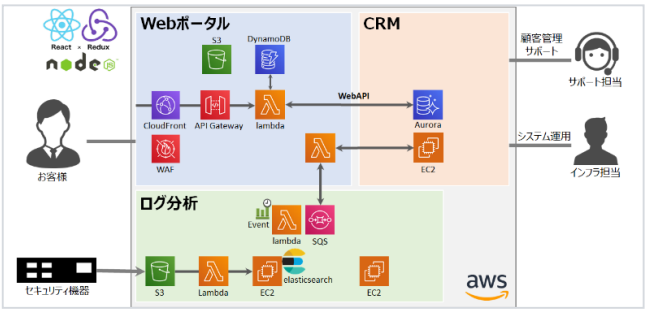
CloudFalconは、名前の通りクラウド環境に構築されたSaaSとして提供されていますが、クラウド上にシステムを構築した理由について井原は次のように語る。

「新しいサービスの企画で問題になるのは、初期投資と運用の手間、そして競争力のあるサービスにできるかということですが、まだ契約顧客が少ない状況で初期投資を抑えられたり、ハードウェアの故障対応を考慮しなくても良く、お客様が増えたときのリソース強化が簡単に行える点がすぐれています。CloudFalconが実現できたのは、クラウドのおかげと言えます。」

また数あるクラウドプラットフォームのなかでAWSを選んだ理由として「AWSは開発者向けのツールや事例が豊富にあるのが決め手でした。私自身、AWSのユーザーコミュニティに参加していることもありますが、大規模なサーバーレスアーキテクチャの事例を聴いたのです。セキュリティイベントの分析は大量なデータを扱うという点で考え方が近く、API-GatewayとAWS Lambdaを使用したサーバーレスアーキテクチャを採用することを決めました。」という。

IaaSなど、従来のオンプレミス環境をクラウドにリフトしたシステムの場合、マネジメント画面やWebサーバー、データベースのセキュリティ対策など、管理負担は大きく変わらないが、サーバーレスアーキテクチャに関しては、基盤レベルの懸念は全くなくなるという。

井原は、「AWSは、開発者がお客様の課題解決のために、新しい技術を習得し、使いこなしたくなるプラットフォームだと思う。」と語る。



CloudFalconのこれから

CloudFalconは、ラックの知見の粋を集めたシステムだが、今後の展開について、新倉は次のように語った。

「CloudFalconにより、今まで対応できなかった中小企業の情報が集まることで、日本全体のサイバー攻撃の傾向把握と、JSOC MSSへのフィードバックが期待できます。また、AIによる分析も取り込み、分析能力を高めます。そして、AWSの優れた機能を使いつくし、お客様の不安を解消できるシステムに成長させたいと思っています。」

CloudFalconが、パートナーとのタッグにより日本全体のセキュリティ対策を前進させることを期待する。

株式会社ラック
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー　E-MAIL：sales@lac.co.jp　https://www.lac.co.jp