株式会社QTnet：情報通信サービスの安心・安全を確保する独自のSIEM基盤をElastic Cloud Enterpriseで実現

QTnetでは、電気通信事業を支える事業用設備のセキュリティ監視を強化する目的でElastic Cloud Enterpriseを採用し、多種多様なソースから収集した膨大な数のログ情報を機械学習の機能などを使って分析し、サイバー攻撃の兆候をリアルタイムに検知するSIEM基盤を作り上げている。

40
万回線超
光ブロードバンドサービス
利用者40万回線超

3.6
億ドキュメント
Elasticによる処理ログ量
月間約3.6億ドキュメント

400
件
検知イベント
一日当たり約400件

お客様企業
株式会社QTnet

所在地
福岡県

業種
情報通信サービス

製品
Elastic Cloud Enterprise（Elastic Security）

ユースケース
事業設備のセキュリティ監視基盤の構築

サブスクリプション
プラチナ

QTnet について

株式会社 QTnet は、九州の個人・企業・自治体を対象に ISP（インターネットサービスプロバイダー）サービスなどの情報通信サービスを手掛ける企業だ。高品質な情報通信サービスによって、「未来を拓く新たな“光”を九州から。」をビジョンとして掲げ、自治体・企業向けサービス「QT PRO（キューティープロ）」では、ISP サービスはもとより、仮想化、リモートアクセス、Web 会議、IoT といった多彩な ICT ソリューションを提供している。また、一般家庭向けには九州域内40万回線超のユーザーベースを有する光ブロードバンドサービス「BBIQ（ビビック）」をはじめ、スマートフォンサービス「QT モバイル」や電力サービス「BBIQ 電力」などを展開している。
Web サイト　https://www.qtnet.co.jp/

「ゼロトラスト」のコンセプトに基づく脅威の可視化が急務に

QTnet にとって、電気通信事業を支える事業用設備（以下、事業用設備）のサイバーセキュリティリスクを低減させることは、文字どおりの経営命題である。ただし一方で、サイバー攻撃は高度化・複雑化の一途をたどっており、従来どおりにインターネットに対する出入口を集中的に守る「境界防御」だけでは、事業用設備がセキュリティ侵害の実害を被るリスクを回避したり、被害の拡大を阻止したりするのが困難になりつつあった。

「そこで必要とされたのが、従来の境界防御の対策に加えて、ゼロトラストの考え方に基づき、収集可能なあらゆる情報を一元的に管理・分析して、事業用設備に対するサイバー攻撃の兆候を早期に可視化・把握できる検知機能の開発です。セキュリティ対策上、それを行うことが急務となりました」と、QTnet 技術部 技術開発グループ長 兼 監視システムグループ長の忽那康郎氏は明かす。

Elasticの技術を使ったセキュリティ監視基盤によって、これまでとらえることができなかったサイバー攻撃の兆候がリアルタイムにとらえられるようになった意義は非常に大きいと感じています

技術部 技術開発グループ長 兼 監視システムグループ長
忽那 康郎 氏

Elastic セキュリティで SIEM 基盤の構築へ

QTnet では当初、「事業用設備から収集可能なあらゆる情報を一元的に管理・分析する」という目的を果たすために、既製の SIEM（Security Information and Event Management）製品の導入を検討した。しかし、既製の SIEM 製品はどれも企業の社内情報システムを対象にしたもので、情報通信サービス事業者の事業用設備から収集される多種多様で膨大なセキュリティログを管理・分析し、セキュリティ監視に役立てられるような製品は一つもなかった。そこで同社が構想したのが、Elasticsearch の機能を使い、事業用設備に最適化した SIEM 環境を独自に構築するというソリューションだった。

この構想の下、同社では以前から付き合いのあった株式会社インターネットイニシアティブ（IIJ）に SIEM 構築の協力を要請し、同社による協力の下、2019 年 6 月 からプロジェクトがスタートを切り、翌 2020 年 4 月から本番運用が開始されている。

Elasticsearch の本格導入に先立ち、QTnet では、Elasticsearch が SIEM として機能しうるかどうか点検すべく、Elastic Stack 環境を構築し PoC（概念検証）を実施したと、技術部監視システムグループの永江達也氏は言う。

その PoC を通じて、ElasticStack の機械学習（Machine Learning：ML）などの各種機能の活用によるログ分析の有効性、想定ログ量に対する処理能力、既存システムとの親和性などについての検証・評価を行い Elasticsearch の導入が本決まりになった。

ただし、Elasticsearch はオープンソースソフトウェア（OSS）であることから、バージョンアップのスピードが速く環境のバージョン管理を行うだけでも相応の工数がかかるうえに、スケールをコントロールする難度も高いという課題があった。そこで QTnet では、本番環境の構築用として、Elastic 社が商用のプロダクトとして提供しているオンプレミス型の「Elastic Cloud Enterprise（ECE）」を採用し、バージョン管理やスケールコントロールを巡る問題を解決した。

「運用開始以降、これまで数回のバージョンアップやスケール変更を行いましたが、ECE を採用したことにより、サービスのアベイラビリティを担保しつつ Elasticsearch の最新機能を利用できるため、その選択は正しかったと考えています」（永江氏）。

攻撃のタイプごとに脅威検知の機能を実装

QTnet が ECE を活用して構築した事業用設備のセキュリティ監視（SIEM）基盤の全体像は図 1 に示すとおりである。

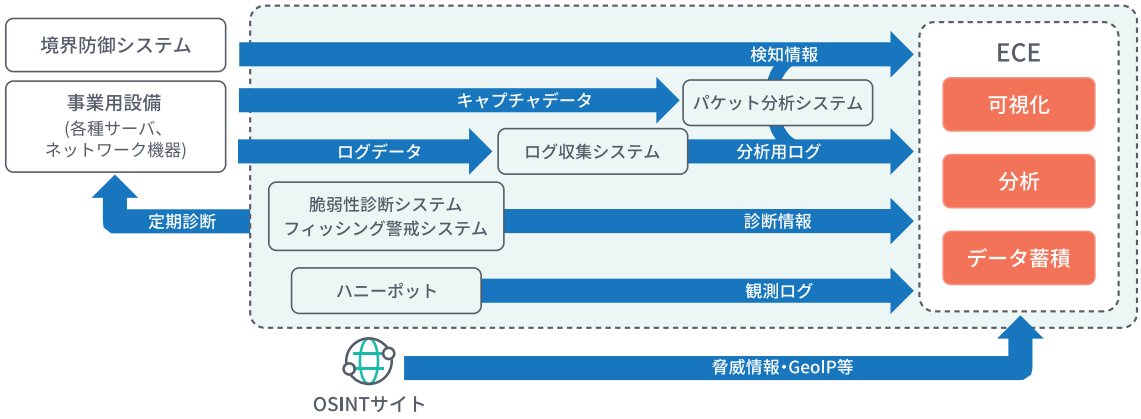

図 1：ECE を使い構築された QTnet のセキュリティ監視基盤

ECE（Elastic Security）の ML やアラート、さらには多様な情報ソースからデータを取り込み分析可能な形式に変換し、格納する Logstash の機能などを用いて構築されている。

その構築に際して、QTnet では、サイバー攻撃を「既知か」「未知か」という指標と、そのリスク（リスクが既知か未知か）の 2 軸によって分類し、それぞれに適した分析手法を検討・選択して、「シグネチャ検知」「振る舞い検知・差分比較」「アノマリ検知」の各検知機能を開発・実装していったという（図 2）。

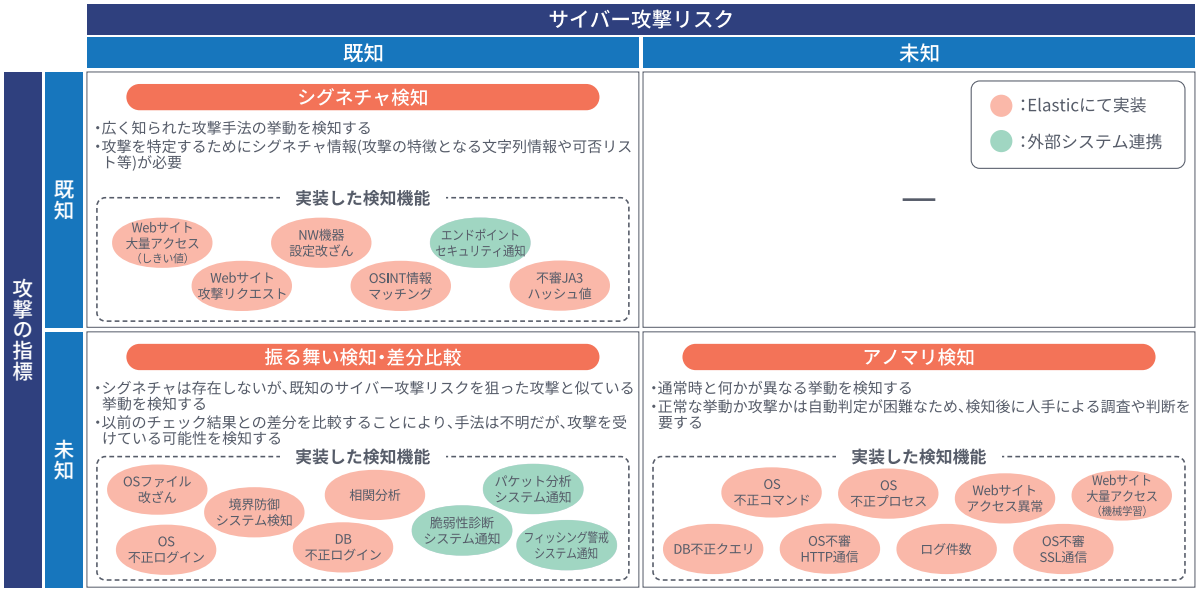

図 2：サイバー攻撃の分類と Elastic で実装した検知機能のマップ

「Elastic の技術は、ログ情報に対して横断的な検索・分析をかけるのに適したテクノロジーですが、特定の攻撃を分析するうえで、それに特化したセキュリティアプライアンスと Elastic を連携させたほうがよい場合があります。このように、サイバー攻撃のタイプに応じて最適な分析技術を組み合わせ、多角的な視点から検知を行い、精度を高めることを目指しました」と、忽那氏は説明を加える。

また、QTnet では、セキュリティ監視による脅威の検知から対処に至るプロセスの効率化と有効性の最大化を目指して、検知した脅威情報を運用者へ通知する段階で、内容に合わせてトリアージ情報（対処の優先順位を表す情報）を事前に付加するという一手も講じている。これにより、セキュリティ監視に不慣れな担当者でも、アラート（検知された情報）に対して、それが即座に対処すべきものかどうかを正しく判断することが可能になるという（画面）。

画面：QTnet のセキュリティ監視担当者向けダッシュボード

> 機械学習機能をはじめとするElasticの技術は、セキュリティ監視の基盤づくりに適した技術です。その活用によって日々変化し、複雑化するサイバー攻撃の脅威に十分対抗していけると考えています
>
> 技術部 監視システムグループ 兼 サイバーセキュリティ部
> 永江 達也 氏

ちなみに、事業用設備に対するセキュリティ監視では、セキュリティインシデント発生によるサービスへの影響を最小限に抑えることが大切であり、特に通信の遮断は可能な限り回避することが望ましいという。そのため、検知された脅威への対処は必ず人手を介して行うことが原則とされ、ECE を活用したセキュリティ監視基盤（SIEM 基盤）の守備範囲も、脅威の検知と見える化、深刻度の初期判断（トリアージ）に限定されている。また、検知した事象については、SIEM だけで確認するのではなく、従来から運用している通信事業用の統合監視システムに対して、SNMP トラップの方式で検知情報を送出し、よりマクロな視点での監視を実現しているという。

マネージドセキュリティサービスでの ECE の活用も始動

以上のようにセキュリティ監視基盤の構築に ECE を活用したことで、QTnet では数々の効果を手にしている。なかでも大きな効果は、サイバー攻撃の兆候をリアルタイムに観測することが可能になった点であるという。

「これまでは何らかのインシデント情報を入手したあとでしかサイバー攻撃の情報がつかめず、対処が後手に回る可能性がありました。その可能性を大幅に低減できたという点で ECE の導入効果は大きいと言えます」（忽那氏）。

また、インシデント発生時の調査に要する時間も短縮されていると、永江氏は指摘する。

「従来は各機器にログインして 1 ファイルずつログを確認する必要がありましたが、Elasticsearch を使用することで横断的かつ柔軟なログの検索が可能です。これにより、ログの調査時間はかなり短くなっています」

さらに、比較的経験の浅い担当者でも、トリアージによって脅威検知時の初動対応が適切に行えるようになった点も、大きなメリットであるという。

ちなみに、QTnet におけるセキュリティ監視基盤で Elastic が処理しているログの総量は月間約 3.6 億ドキュメントに上り、一日当たりに検知されるイベント数は「ログ分析＋外部システム」の総和で約 400 件、ログ分析に絞った場合で約 30 件であるという。これだけの数のイベントが検知され、全てにおいて均一の対応が求められるとすれば、担当者の負担はかなり大きくなる。そうした負荷を引き下げ、かつ、対応の適切さを担保するソリューションとしてトリアージが有効に機能しているということだ。

QTnet では今後も、検知された新たなインシデント情報を基に、新たなシグネチャや ML ジョブを追加し、検知機能をさらに強化・充実させ、変化し続けるサイバー攻撃に対抗していくという。さらに、同社が提供しているマネージドセキュリティサービスのログ分析機能も開発中であり、この開発を通じて、サイバー攻撃の業界別・地域別の傾向・状況を分析し、顧客への提案に生かすだけではなく、セキュリティ情報として広く発信していくという。Elastic の技術はこれからも、QTnet によるセキュリティ対策の進化・発展を支え続ける。

お問い合わせ
Email: elastic-japan@elastic.co

