YOKOGAWA

横河電機株式会社：Elastic CloudでDX戦略を支えるグローバルSOC基盤を構築

ベンダーが異なる多種多様な機器・システムからの大量のログをリアルタイムに分析

お客様企業
横河電機株式会社

所在地
東京都

業種
製造業

製品
Elastic Cloud

ユースケース
グローバルSOC基盤を構築

サブスクリプション
プラチナ

15
ヶ所
分散する拠点のセキュリティ監視を実現

500~600
万件／日
イベント情報をElastic Cloudに集約しリアルタイムに分析

3
万台
PCと重要サーバ、ネットワークのセキュリティ監視

横河電機 株式会社について

創設 100 余年の歴史を持つ横河電機株式会社（以下、横河電機）は、プラント制御のシステムを中心に年間 4,000 億円強（2019 年度／連結）を売り上げる製造企業だ。世界 62 カ国に拠点を展開し、海外売上比率が約 80%に上る、文字通りのグローバルカンパニーでもある。

デジタル戦略の推進でセキュリティ監視の強化が不可欠に

横河電機では現在、デジタルトランスフォーメーション（DX）を経営戦略の柱に据えて、強力に推進している。同社における DX の主たる方向性は、制御システムなどのオペレーショナルテクノロジー（OT）と情報技術（IT）とを融合させ、インテリジェントな工場を支えるサポートサービスを提供していくというものだ。顧客の工場内設備から IoT センサーを通じて収集した膨大なデータをクラウド上の AI（人工知能）によって解析し、工場のシミュレーターを作り上げ、機器の障害予測やそれに基づくプロアクティブな部品・機器の交換、さらにはエネルギーマネジメントなどのサービスを提供していくという（図 1）。

その戦略をまとめれば、クラウド、コンテナ、データアナリティクス、AI/ML、IIoT などのテクノロジーを駆使しながら、機器のサービス化を図り、ハードウェアの「販売＋保守サービス」のビジネスモデルを、リカーリングモデルへと転換（トランスフォーム）することを目指している。

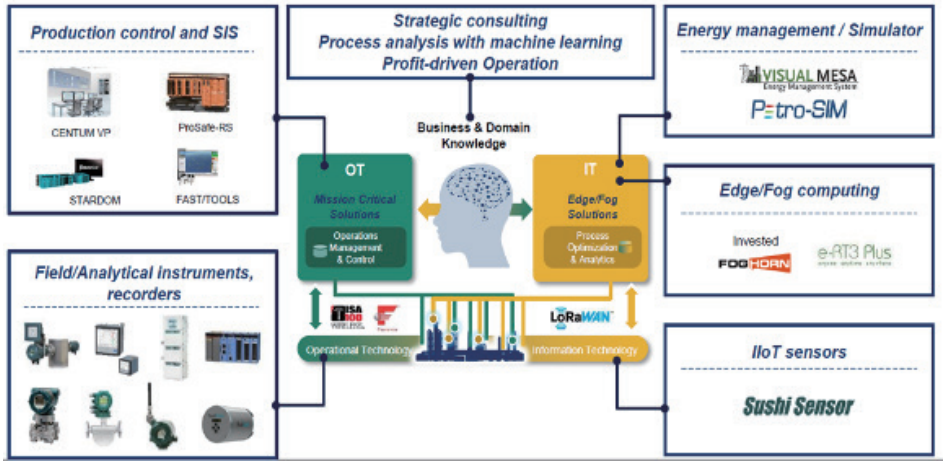

図 1：横河電機が構想する AI による次世代サポートサービスのイメージ

elastic

また、同社では社内的にも DX を推進しており、例えば、多種多様な情報ソースから収集したデータによってデータレイクを形成し、データ駆動型の経営やシステム運用管理のさらなる効率化に役立てる取り組みを進めている。

「こうした DX 戦略を推進していくうえで、非常に重要になるのがセキュリティの強化です」と、横河電機 デジタル戦略本部 副本部長の塩崎哲夫氏は指摘する。

例えば、OT 環境は、インターネットなどの外部ネットワークから切り離されたクローズドな環境に置かれてきたために、サイバー攻撃にさらされるリスクが低く、攻撃に対する防御が手薄なケースが間々ある。その OT と IT との融合を進めて、クラウドによる工場のインテリジェント化を推進するとなれば、OT 環境はもとより、IT 環境の守りを固めて、IT 環境から OT 環境への脅威の侵入を防いだり、OT 環境への脅威の侵入を早期に検知したりする仕組みづくりや体制づくりが強く求められることになる。

「そうした課題に対応するには、OT と IT のセキュリティに関するノウハウを社内に蓄積していくことが必須であり、そうしなければ、社内はもとより、社外に向けた DX 戦略を安心して推進することはできないと考えました。当社では従来、社内システムに対するセキュリティ監視を社外の IT 企業に委託していたのですが、その体制を見直し、社外の IT 企業と連携しながらも自社で SOC を立ち上げ、自力でセキュリティ監視を行うことにしたのです」（塩崎氏）。

製品非依存のオープン性を重視し、Elastic Cloud を選択

塩崎氏が属するデジタル戦略本部は、情報システム部門（IT 部門）が母体となって創設された組織であり、今日では、社内における DX の推進と、社外（顧客）向けの DX 戦略を支える仕組みづくりを一手に担っている。

また、世界各国の拠点にもリージョンごとに IT 部門が置かれているが、最近、日本のデジタル戦略本部が中心となり、グローバル IT シェアードサービス化を行い、グローバルなアプリケーション・インフラ環境の共用化・最適化を進めている。その取り組みは、セキュリティ製品についても同様に進められ、SOC の立ち上げに向けても、「2018 年秋ごろから、グローバルな SOC 基盤の構築に向けた共通ソリューションの選定に乗り出しました」と、塩崎氏は明かす。

> DX戦略を支えるグローバルなSOC基盤を立ち上げるには、多種多様なログを収集し、分析するための有効なソリューションが必要でした。そのニーズをElastic Cloudはしっかりと満たしてくれたと評価しています。
>
> デジタル戦略本部 副本部長
> 塩崎 哲夫 氏

このソリューション選定の結果として、同社が採用を決めたのが、SIEM をはじめ、エンドポイントセキュリティや脅威ハンティング、クラウド監視など、広範な用途に使えるクラウドソリューション「Elastic Cloud」である。

言うまでもなく、同社が Elastic Cloud を採用した理由は、このクラウドサービスが、グローバル SOC 基盤の構築に求められる要件を満たしていたためである。

その要件の一つは、特定のセキュリティ製品に依存しないかたちで、広範な機器・システムからのログの収集・分析を可能にすることである。例えば、先に触れたとおり、同社ではセキュリティ監視を外部の IT 企業に委託していたが、その監視は IDS（不正侵入検知システム）を使

用したものだった。

塩崎氏によれば、IDS による監視だけでは、今日の高度で複雑なサイバー攻撃の動きを捉えることが難しく、誤検知も多く発生させていたという。ゆえに、SOC の基盤構築にあたっては、多様なセキュリティ機器・システムのログ収集・分析を可能にするソリューションが必要とされた。

しかも、監視ツールの選定を進めていた 2018 年当時は、グローバル拠点でのセキュリティ製品の共通化・標準化が進んでおらず、拠点ごとに多種多様なセキュリティ製品が導入されていた。そうした多種多様な製品からログを収集し、分析するためにも、監視のソリューションには、特定の製品に依存しないオープン性が求められたのである。

以上のような要件の下、導入ソリューションの有力候補として同社は Elastic Cloud を選び、2019 年 1 月から 3 カ月にわたって PoC（概念検証）を行った。検証の内容は、東京の本社とシンガポールの拠点で IDS や認証サーバ（AD サーバ）、DHCP ／ DNS サーバなどのログを収集して、Elastic Cloud に転送し、「ログの収集から分析までにどの程度の時間を要するか」を点検するというものだ。その結果として、Elastic Cloud を使ったセキュリティ監視の仕組みが、グローバル SOC の基盤として有効に機能しうると判断され、2019 年 4 月に同社は Elastic Cloud の採用を正式に決めた。そして、PoC で使用したシステムを、リソースを増強して、そのまま本番環境へと移行させ、SOC の立ち上げに向けたセキュリティ監視基盤の開発作業を始動させたのである。

世界 15 カ所に分散する約 3 万台の PC、重要サーバ、ネットワークを集中監視

Elastic Cloud を使った SOC 基盤の開発に当たり、横河電機がまず着手したのは、Elastic に精通した技術者の雇用だ。具体的には、インド バンガロールに展開しているエンジニアリングセンターを通じて Elastic 技術者を募集、採用した技術者を中心に SOC 基盤の立ち上げを進めた。

ちなみに、その際には、技術者のスキルアップを目的に、Elastic の共通スキーマ「Elastic Common Scheme（ECS）」定義や「Logstash」サーバのログフィルタリング設定に関するエラスティックの教育サービス／コンサルティングサービスも活用したという。

「当社の場合、ログ収集の対象が多種多様なセキュリティ製品になりますので、共通スキーマを定義しておかないと、検索のスピードが上げられません。ですので、技術者に ECS を学ばせることはとても重要でしたし、かなり有効だったと言えます」（塩崎氏）。

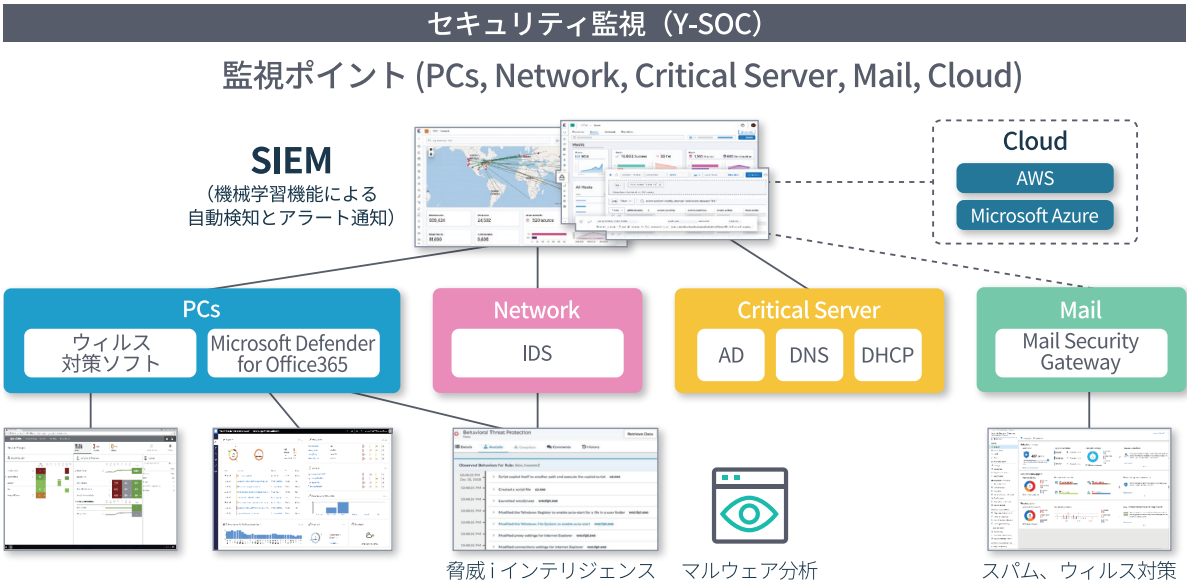

図 2：Elastic セキュリティを活用した横河電機の SOC 基盤のイメージ

こうして SOC の基盤作りとデータ分析の体制作りを進めた同社では、2019 年度に主要拠点（日本・欧州・北米・シンガポール・中東・インド）に対するセキュリティ監視を始動させた。また、それと並行して監視・検知アプリケーションの改善にも力を注いでいる。これは、Elastic Cloud と他社の脅威インテリジェンスや「IOC（Indicator Of Compromise：サイバー攻撃によるセキュリティ侵害の指標／痕跡情報）」とを連携させ、脅威監視・検知の的確性を増す取り組みだ。

さらに、2020 年には、監視の範囲を中国、ロシア、南米、台湾、フィリピン、インドネシアなどの各拠点へと広げている。

これにより、世界 15 カ所の拠点で使われている PC（のウイルス対策ソフトや EDR）や重要サーバ（AD サーバ、DHCP/DNS サーバ、など）、IDS、さらには Microsoft Azure ／ AWS の WAF（Web Application Firewall）などが監視対象となり、それらの機器・システムから収集されたログ、イベント情報が Elastic Cloud が稼働する クラウド環境に集約されるようになった。そのデータをリアルタイムに分析しながら、サイバー攻撃の予兆やセキュリティ侵害を検知するセキュリティ監視が日々展開されている（図 2）。

ちなみに、この監視対象になる機器／システムの数は、PC だけで世界約 3 万台に上り、1 日に収集されるイベント情報の件数は 500~600 万件、容量にして 1 日に 250 ～ 300GB に達しているという。これは、まさに、多種多様な機器のセキュリティログを集めたセキュリティデータレイクと位置づけられる。

Elastic SIEM と機械学習を組み合わせた高度な検知プログラムの開発も推進

以上のように、横河電機では、Elastic Cloud によってグローバル SOC の基盤を立ち上げ、セキュリティ監視の対象を着実に拡大させてきた。その取り組みを振り返りつつ、塩崎氏は Elastic Cloud の導入効果について改めてこうまとめる。

「Elastic Cloud 導入の大きな効果は、やはり、多種多様なログを可視化して、リアルタイムに分析することが可能になったことです。また、Elastic Cloud というクラウドサービスを採用したことで、グローバルでの SOC 基盤の立ち上げが早期化されました。それも当社にとっては意義の大きな効果だったと言えます」

同社では今後も、Elastic Cloud を使ったセキュリティ監視の強化を図っていく計画であり、すでに Elastic Cloud の Elastic SIEM を採用し、機械学習を組み合わせた高度な検知プログラムの開発や「MITRE ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge：脆弱性攻撃を戦術や技術、手法の観点から分類した知識ベース）」の活用を推し進めている。

また、SOC の基盤を IT サービス管理（ITSM ツール）ツールの「ServiceNow」と連携させ、SOC が発したインシデントアラートに関連コメントや対処方法を付加して、各担当者に自動的に通知する仕組みもすでに構築し、運用を始めている。

さらに、SOC 基盤の構築で培った Elastic によるセキュリティ監視のノウハウは、顧客向けにセキュリティ監視のサービスを提供している横河電機の事業部門と共有され、そのサービス強化にも活かされているという。

Elastic Cloud は、横河電機の DX 戦略を今、この瞬間も支えている。

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

