IT/OT 統合環境におけるセキュリティへの取り組み

Yokogawa's Approach to Cybersecurity in the IT/OT Convergence Environment

塩崎 哲夫 *1
Tetsuo Shiozaki

横河電機（YOKOGAWA）では，2019 年から社内システムのセキュリティ監視の内製化を推進し，さらには社外向けモノのインターネット（IoT: Internet of Things）サービスのセキュリティ監視も始めている。セキュリティ監視センター（SOC: Security Operation Center）の社内開発については，その技術的な難しさや運営体制の問題から自社開発を躊躇する企業も多い。本稿では，SoC を社内開発した経緯，その技術的なポイント，運用体制について説明し，YOKOGAWA のサイバーセキュリティに対する方向性を紹介する。

Many companies hesitate to develop a security operation center (SOC) on their own due to its technical and operational difficulties. In 2019, Yokogawa started to develop a cybersecurity monitoring system for its corporate system and is now using it. For customers, Yokogawa has also been developing a security monitoring system for Internet of Things (IoT) services. This paper explains Yokogawa's in-house development of the SOC, key technical points, and operation system, as well as the company's approach to cybersecurity.

1. はじめに

デジタルトランスフォーメーション（Digital Transformation: DX）の流れの中でクラウドサービスの利用が進み，オペレーショナルテクノロジー（Operational Technology: OT）と情報テクノロジー（Information Technology: IT）の統合が進んでいる。一方で，IDC Japan の調査によると，３割を超える製造業企業が，産業分野向けのモノのインターネット（Industrial Internet of Things: IIoT）や OT のシステムでセキュリティ事故の経験がある [1] と答えており，セキュリティ監視の重要性が増している。**図 1** は，横河電機（YOKOGAWA）の DX インフラアーキテクチャを示したものである。本稿では，この中からセキュリティ管理サービスについて説明する。

2. セキュリティ監視センター開発の背景

DX 推進のためにはセキュリティの強化が必須であるが，YOKOGAWA では次の課題を抱えていた。

- 不正アクセス監視装置（Intrusion Detection System: IDS）によるセキュリティ監視を外部 IT 会社に委託していたが，IDS 監視だけではサイバー攻撃の特定やタイムリーな検知，その影響範囲の特定が難しく，多様なログを相関的に分析する必要があった。

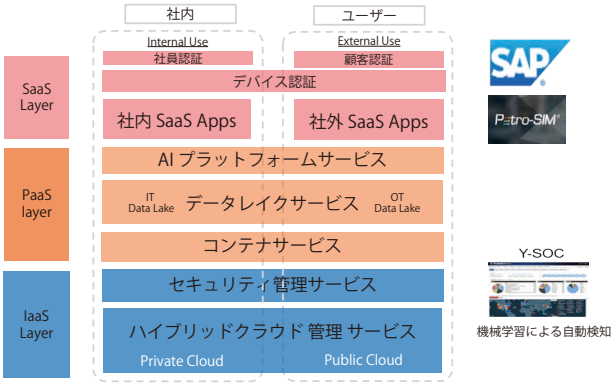

図 1 YOKOGAWA の DX インフラアーキテクチャ

- グローバルに IT システムを展開しており，拠点毎に IT 部門が存在する。しかし，IT についてのガバナンスが不十分なため，様々なセキュリティ製品が導入され，監視体制も統一されていなかった。
- セキュリティの強度が地域毎に異なり，脆弱性を持つ地域から侵入され，グローバルなシステム全体に影響を与えていた。
- 多様なログを分析するためには，自社でセキュリティ監視基盤（Security Information and Event Management: SIEM）を開発・運用する必要があるが，そのための IT 要員が不足していた。

このような背景から，セキュリティ監視センター（Security Operation Center: SOC）の開発にあたって

*1 デジタル戦略本部 グローバルインフラ・セキュリティセンター

は，IT および OT の様々なデータソースからログやイベントを収集・加工・分析し，タイムリーに対応できるソリューションが必要である。また，将来の外部向けのサービス提供も考慮し，特定の製品に依存しないオープン性や，Microsoft Azure や Amazon AWS などのパブリッククラウドにも対応できる監視ソリューションが必要であった。そこで，クラウドの Software as a Service（SaaS）型の SIEM を採用することで，その開発工数を削減し，早期立ち上げを目指すこととした。

3. SOC 開発の歩みと概要

監視の方法には，地域毎に監視する分散型監視（Distributed SOC）と，どこかでまとめて監視する集中型監視（Centralized SOC）のパターンがある。我々は，YOKOGAWA のシステム規模から集中型を選択し，日本（東京）とシンガポールでリファレンスモデルを作成して，そのモデルを各国に展開することとした。その歩みは次の通りである。

- 2019 年 1 月～ 3 月：
  東京とシンガポールを対象に，SaaS 型 SIEM として Elasticsearch（オープンソースの分散処理マルチテナント対応の検索エンジン）の PoC（概念検証）を実施した。IDS や Active Directory（AD），Dynamic Host Configuration Protocol（DHCP）/Domain Name System（DNS）の各サーバ等のログを収集した。PoC では，ログの収集方式や転送時間さらに不正アクセスの検知，分析方法，ダッシュボードの設計など SOC の要件整理と Elastic Cloud の有効性を検証した。
- 2019 年 4 月～ 12 月：
  インド（ベンガルール）で SOC 開発体制を整え，主要 6 拠点（日本, 欧州, 北米, シンガポール, 中東, インド）のセキュリティ監視を立ち上げた。
- 2020 年 1 月～ 6 月：
  監視地域を 15 箇所に拡大した（中国，ロシア，南米，台湾，フィリピン，インドネシア等）。また，各国の IT 部門と Computer Security Incident Response Team（CSIRT）体制の見直しを行った。
- 2020 年 7 月～ 12 月：
  社内での監視機能が十分であることが確認できたため，外部委託による監視をやめ，社内監視体制に切り替えた。また，O365 関係（Defender ATP，MCAS）やクラウドの WAF（Web Application Firewall）による監視を開始した。さらに，IT サービスの各種ワークフローを提供する ServiceNow ITSM と連携を行った。
- 2021 年 1 月～：
  日本，ベンガルール，ルーマニアの 3 極ローテーションによる 24 時間監視体制を確立した。

このような経緯を辿り，現在，YOKOGAWA セキュリティ監視センター（Y-SOC）では，次の機能を実現している。

(a) YOKOGAWA の IT インフラで発生するイベントやセキュリティログを収集する（PCs, IDS, AD / DHCP / DNS, Mail Gateway, Cloud Service）。
(b) Python スクリプト，Watcher（Elasticsearch のアラート検知プラグイン），そして Cyber Threat Intelligence（CTI：サイバー攻撃の証跡や検知方法をまとめたもの）を利用して，疑わしい通信やイベントを検知し，自動的にアラートを通知する。
(c) 各地域のセキュリティ担当者と ServiceNow を利用し，インシデントへの対応ワークフローを自動化する。

Y-SOC の全体概要図を**図 2** に示す。監視対象の PC は約 30,000 台，全世界に配備された IDS は 83 台，AD は 111 台，DNS は 100 台に及ぶ。

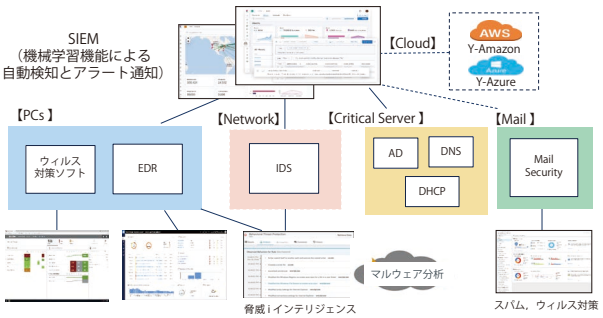

図 2 Y-SOC 全体概要図

現在 Y-SOC で扱っているイベント数，ログ容量，保存期間，ホットノードなどのシステム規模を**表 1** に示す。

グローバルに収集される一日のログサイズは 200 ～ 300 GB，イベント数は 5 億件 / 日である。一週間分のデータを直近の分析対象にし，3 カ月分のデータ保持し，同様の手口や関連する脆弱性の有無を調査している。

表 1 Y-SOC システム規模

Item	Size/Rate/Period
Data Ingestion rate	~ (500–600 million) logs/day
Data Ingestion size	~ (250-300) GB/day
Frequently accessed data	Last 7days
Infrequently accessed	Last 90 days
Uptime SLA	99.95%
Data replication	2 (1 Primary & 1 Replica)
Hot Retention Period	30 days or 40 GB/index (whichever is earlier)
Warm Retention Period	60 days (with potential to increase)

4. SOC 開発の技術的ポイント

SOC の開発においては，各種ログの収集方法からそのデータ構造の設計，効率的な検索インフラの準備，さらには不正アクセス検知プログラムの開発やダッシュボードの設計等，様々な要素が絡む。ここでは，各段階における技術的なポイントについて説明する。

4.1 監視対象のログの調査

最初に，セキュリティ監視の対象となるログやイベント情報を選定し，その容量を見積もる。例えば，企業にとって認証システムは非常に重要であり，AD のログは必須である。また，ハッカーが不正アクセスに使用する Command and Control（C&C）サーバの通信を検知するためには，IDS と DNS のログが必要となる。さらに，各端末でのマルウエアの状況も監視する必要がある。このような背景から，**表 2** に示す機器のログやイベント情報を監視の対象とした。

表 2 ログ・イベント情報を収集する対象

Device category	Devices
ネットワーク	Firewalls / IDS & IPS Proxy servers VPN servers
社内 server	DNS & DHCP servers, etc.
ユーザ認証	Active Directory
クライアント PC	Endpoint protection (Anti-virus)
Cloud サービス	Web Application Firewalls (WAF)

4.2 SIEM 基盤のデザイン

次に，上述のログを処理するために必要となるクラスタ構成とノードタイプを設計し，ディスク容量を見積もる。今回は，ログやメトリックの時系列データを扱う場合に多く採用される Hot-Warm アーキテクチャを採用した。このアーキテクチャは，データ全体が Immutable（不変）であり，時系列でインデックスができるという原則に基づいている。そのため，各インデックスに特定の時期のデータを持たせることで，保持するか，削除するかというインデックス全体のライフサイクルを管理することができる。また，30 分毎にクラスタ内のすべてのインデックスのスナップショットを作成し，それを 48 時間保持することにより，障害からの回復や偶発的な削除に対する高可用性を実現している。Elasticsearch を利用した SIEM 基盤の設計項目は次の通りである。

- クラスタの配置
- ノードタイプ（マスター，データ，機械学習など）
- ノード数とストレージ容量
- ログ保存期間

4.3 ログ・イベントの収集

Elasticsearch では，監視対象となるサーバやノードに応じて様々なログ収集エージェント（Beats）が用意されている。Y-SOC では次の Agent を使っている。また，SaaS 型のサービス（Cisco WSA / Cloud の WAF / O365 等）では，Application Programming Interface（API）連携やクラウドストレージ（AWS S3 等）経由でのログ収集を行っている。

- Filebeat：システムからファイルを読み取る。
- Winlogbeat：Windows イベントを収集する。
- Metricbeat：サーバからメトリックを収集する。
- Packetbeat：ネットワークの遅延，エラー，応答時間を監視する。

4.4 共通的なスキマー名の定義

様々なセキュリティ製品やシステムにおいては，同じ種類の製品（例えば，ファイアウォール等）でもそれぞれの製品のログのフィールド名やフォーマットは同じではない（ソースアドレスを示すフィールドの例：src, client_ip, source_ip, src_ip）。しかし，SIEM では，様々なログやイベント情報を関連付けて検索する必要があるため，すべてのフィールドを標準化して正規化する必要がある。

Y-SOC では，Elastic Common Schema（ECS）[2] を基にインデックステンプレート（yokogawa_ecs_template）を独自に用意し，各フィールド名を ECS の標準的な命名規則に沿った名前で定義し，インデックス化している。これにより，異なるデータソースを自動的に関連付けることができるようになった。

4.5 データの動的変換と Enrichment

収集されたデータは，格納する前に分析データに適するように動的に変換・統合・正規化し，さらに Enrichment（付加的な属性情報を付与）する必要がある。Y-SOC では Logstash を使用し，統一的なデータフォーマットに変換している。Logstash は，リアルタイムのパイプライン機能を備えたオープンソースのデータ収集エンジンで，入力，フィルター，出力の 3 つのステージで構成されており，様々な機能を持つプラグインを使用することができる（**図 3**）。

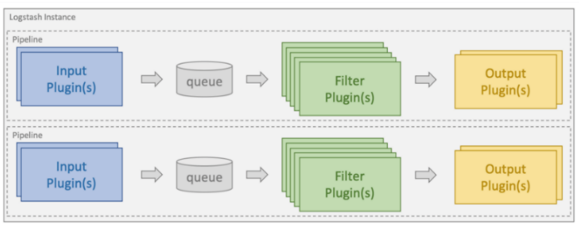

図 3 Logstash の構造

各プラグインの構成と機能は次の通りである。Y-SOCでは，マルチパイプライン処理を採用してパフォーマンスを上げている。

■ 入力プラグインは，各種イベントを Logstash に取り込む。
- File：File からイベントをストリーミングする。
- Beats：様々な Beats Agent からログを収集する。
- TCP：TCP ソケットを介してイベントを読み込む。
- JDBC：トランザクションを Logstash のイベントに変換する。

■ Filter プラグインは，イベントを変更，操作する。
- Grok：非構造化データ構造化形式に変換する。
- Mutate：イベントのフィールドの名前変更，削除，置換，変更等を実行する。
- GEOIP：IP アドレスを検索し，地理的位置情報をログに追加する。
- KV：メッセージを自動的に解析し，キーと値のペアに分解する。

■ 出力プラグインは，イベントデータを特定の宛先に送信する。出力はイベントパイプラインの最終段階である。

4.6 標準化されたダッシュボードの設計

Y-SOC では，世界各地域のセキュリティ状況が一括で見える（Top level dashboard），各地域の状況が見える（Region wise alert dashboard），デバイス毎の 3 階層のダッシュボード（Detailed dashboard）を開発した（**図 4**）。

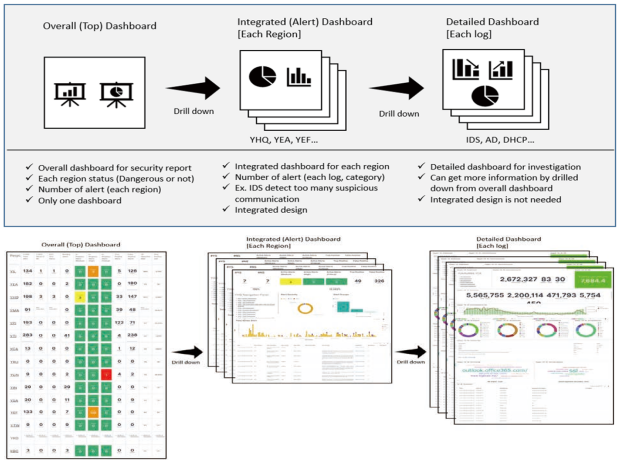

図 4 セキュリティダッシュボード

Top level dashboard からは，各地域の IDS/AD/PC の不正アクセスやマルウエアの検知状況とその対処・未対処件数が分かる。また，Region wise alert dashboard では，IDS/AD/DNS/PC などの時系列の動きが分かるようになっている。各デバイスのログについてさらにドリルダウンすることにより，全体のデータを細分化しながら異常の原因を突き止められるように，階層化構造として設計されている。

4.7 SOC ユーザルールの設計

SOC を運用するためには，様々な役割を持つメンバーが必要である。全体責任者，SOC 開発者，セキュリティ分析者，インフラ運用者，各地域のセキュリティ担当者等である。SOC システムの認証やダッシュボードの認証には，PingFederate（クラウド環境のアプリケーション認証と社内システムの認証基盤を連携できる SSO 製品）を採用し，各担当の役割に応じたアクセス権を付与している。

5. ログ・イベントの収集と検知ロジックの開発

サイバーセキュリティの防御には，サイバー攻撃の侵入の予備段階からの検知が必要であり，また，侵入後はその被害の拡大を阻止することが重要である。そこで，サイバー攻撃の証跡や検知方法をまとめた各種サイバー脅威インテリジェンス（Cyber Threat Intelligence: CTI）と連携し，不正アクセスで使われた IP アドレスや URL，ドメイン情報と検知ログとの突き合わせを自動化している。

各デバイスの不正ログの検知にあたっては，一般社団法人 JPCERT/CC[3] 等の資料を参照して検知ルールを開発した（**表 3**）。

表 3 不正アクセス検知プログラム例

PC	・mimikatz.exe，pwddump.exe などクレデンシャルダンプ実行可能ファイルの検出 ・未対応のスクリプトの実行検知など
IDS	・スパイウェア，ウイルス，脆弱性に関連する脅威イベントの検知 ・疑わしい DNS Query やネットワークスキャンニング
DNS	・悪意のある Tor（TCP/IP 接続経路の匿名化）/ダークウェブアクセスの検知 ・DNS 閾値を超える疑わしいドメイン，ホスト名，またはエンコードされた FQDN（完全修飾ドメイン名）の検出

AD の監視イベントに関しては，JPCERT/CC[4] やマイクロソフト社から推奨されているイベントを監視している。例えば，特権権限で AD を操作した時は，その監査ログと操作履歴を突き合わせている。また，短時間での大量な成功・不成功のログインは挙動不審としてアラートを挙げ，利用者に確認している。

イベントの検知では，Elasticsearch の持つ機械学習（ML）機能を利用して挙動を検知している。分析アプリは主に Python で開発されており，Jenkins によって定期的に実行され，各種 CTI のセキュリティ侵害インジケー

ター（Indicator of Compromise: IOC）の情報とのマッチング分析を行っている（**図 5**）。また，教師なしの機械学習機能により，時系列モデリングから閾値や異常値を自動設定できる。この機能を使って，通信先，ログイン数，データアップロード，疑わしい DNS Query などの行動特性から発見できるインシデントにつながる動きも検知している。その分析結果は，アラートインデックスに保存され，Y-SOC のセキュリティ分析者に通知される。これらの検知プログラムは，新しい脅威が報告される度に継続的に改善している。

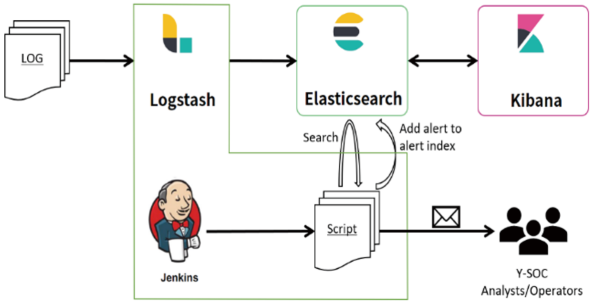

図 5 Python Script 実行環境

6. インシデントレスポンス管理（CSIRT）

SOC でのアラート検知後は，速やかな現地調査と対処が必要である。そこで，インシデントレスポンスのワークフローを確立し，各地域のセキュリティ担当者との連携を図っている。その流れは次の通りである（**図 6**）。

(1) 分析エンジンが異常を自動的に検知し，脅威カテゴリと脅威レベルから構成されるマトリクスから各アラートの重要度を自動判定する。

(2) アラート情報は Alert Index に収集され，Y-SOC チームに自動的に通知される（一日平均約 50 ～ 70 件）。

(3) Y-SOC チームのセキュリティ分析官が，個々のアラートから true-positive（実際の攻撃）か false-positive（誤検知）かの判断をする。その判断は次の手順で行っている。

- 様々なログのソースを分析し，相互に関連付けを行い，真偽性を判断する。
- 内部トラフィックの通信を調査する。
- 様々なサイバー脅威インテリジェンス（Virus Total, MineMeld, Online threat intelligence platform, online sand box）を使用して，外部通信 / ファイルを分析する。

(4) 連絡が必要なインシデントを特定した後，各地域の担当者にインシデント内容，現場での調査方法，IoC および緩和策を付記して通知する。

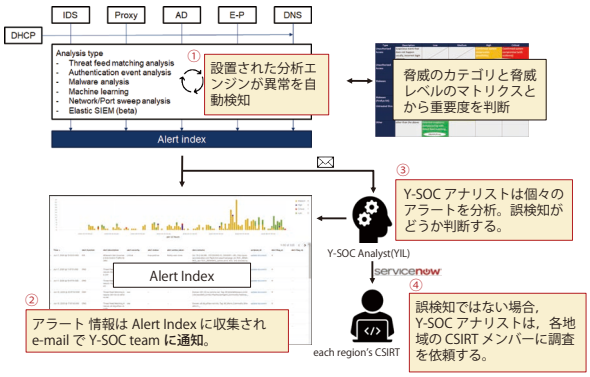

図 6 インシデントワークフロー

サイバー攻撃の分析には，サイバー攻撃の戦術やテクニックなどを，攻撃のライフサイクル別に整理・体系化したフレームワークである MITRE ATT&CK[5] を採用している。このフレームワークを使用して攻撃手法や利用ソフトの分析を行い，攻撃グループの推測や検知方法の見直し，緩和策の立案を行っている。さらに，MITRE ATT&CK Navigator などを使い，サイバー攻撃の戦術予測を試みている。

各インシデントは，ServiceNow ITSM を利用してチケット化し，そのステータス（発生数，対処済数，未対処数，対処時間）を管理している。さらに，四半期毎に世界各地域のインシデント数の変動や Attack Vector（不正アクセスの経路や方法）の分析を行い，検知ルールの改善や IT インフラのセキュリティの改善を行っている（**図 7**）。

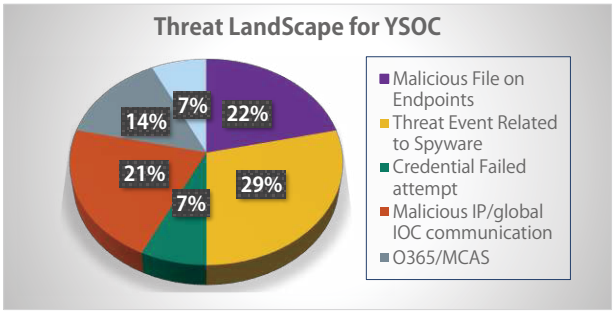

図 7 Y-SOC Threat Landscape

7. クラウドサービスのセキュリティ監視

YOKOGAWA では，社内システムおよび社外サービスの DX 化において Amazon AWS や Microsoft Azure などのパブリッククラウドサービスの利用を促進している。そこで，外部公開サーバに対しては，WAF のログを収集し，Web アプリケーションセキュリティのオープン・コミュニティである OWASP のコアルールセット（CRS）に照らし合わせて，WAF のポリシーをカスタマイズしている。これにより，過検知による通信ブロックを防いでいる。

また，外部向け DX サービスとして Sushi Sensor とクラウドの IoT Hub を利用してコンテナアプリケーションを開発し，Cloud Native の IoT サービスを始めた。そのセキュリティに関しては，Azure Security Center を利用し，セキュリティスコアが常に 75% 以上になるように維持している。

8. 今後の展開

今後の展開として，ServiceNow SecOps のインシデント管理と，脆弱性対応および脅威情報との連携を進めている（**図 8**）。

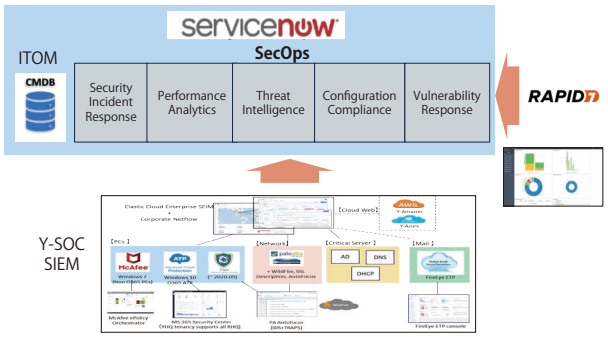

図 8 ServiceNow の連携

インシデント管理では，SIEM と各セキュリティ製品を統合することにより，インシデントの発見から調査，影響範囲の特定，封じ込め，回復などのワークフローを自動化できる（SOAR: セキュリティのオーケストレーション）。

脆弱性診断については，脆弱性診断ソフト Rapid 7 Insight VM で診断したレポートを読み込み，ServiceNow の構成管理データベース（CMDB）と突き合わせて，Patch 対応の担当者のアサインと対応状況の管理，サイバー攻撃に対する脆弱性の有無の確認を進めている。

脅威情報の連携では，サイバー脅威インテリジェンスの情報を自動的に参照できるようにしていく。

また，外部向け IoT のクラウドサービスでは Azure Security Center と ServiceNow との連携を図り，インシデントのワークフローの改善とセキュリティ状況の把握を進める予定である。さらに e-RT3（PLC）など制御機器のログの収集も検証中である。

9. おわりに

本稿では，クラウドサービスの SIEM や ML の利用，さらに CTI との連携により，SOC の開発・運用を効率よく実現できることを説明した。YOKOGAWA では，今後 IT と OT の統合において，顧客側に配置される Edge サーバとクラウドサービスとを連携して強化し，外部向け OT SOC サービスへと展開していく計画である。

その実現に向けて，監視技術の強化だけでなく，脅威及び検知情報の交換規約（STIX/TAXII）[6] などにより，米国国土安全保障庁の Cybersecurity & Infrastructure Security Agency（CISA）[7] や政府・専門機関とのサイバー脅威情報の共有体制の確立や，ATT&CK for ICS 等の制御系システムの脅威ナレッジにも貢献してゆく予定である。

参考文献

(1) IDC Japan, “2020 年国内企業の IIoT/OT セキュリティ対策実態調査を発表”, 2020, https://www.idc.com/getdoc.jsp?containerId=prJPJ46173120（参照 2021-04-30）
(2) Elastic Common Schema (ECS), https://github.com/elastic/ecs (accessed 2021-04-30)
(3) JPCERT/CC, “高度サイバー攻撃への対処におけるログの活用と分析方法”, 2016, https://www.jpcert.or.jp/research/apt-loganalysis.html（参照 2021-04-30）
(4) JPCERT/CC, “ログを活用した Active Directory に対する攻撃の検知と対策”, 2017, https://www.jpcert.or.jp/research/AD.html（参照 2021-04-30）
(5) MITRE ATT&CK, https://attack.mitre.org/ (accessed 2021-04-30)
(6) STIX/TAXII, https://oasis-open.github.io/cti-documentation/ (accessed 2021-04-30)
(7) CISA, Automated Indicator Sharing, https://www.cisa.gov/ais (accessed 2021-04-30)