制御システム向け セキュリティ監視サービスの高度化

Advancement of SOC Services for OT Systems to Further Enhance Cybersecurity

大矢　章晴 OYA Toshiharu　　原田　崇 HARADA Takashi　　村田　仁 MURATA Jin

東芝グループは，制御システムへの増大するサイバーセキュリティリスクに迅速に対応可能なSOC（Security Operation Center）サービスを提供している。SOCサービスの品質向上に向け，監視対象のセキュリティセンサーから発せられたアラートの原因分析及びリスク判定の精度を高めることで，システムオーナーが対応するべきアラートを絞り込み，サイバー攻撃に効率的に対応できる監視技術を開発している。また，発電・変電システムの設計シミュレーターを用いた検証環境を構築し，実運用を想定した技術検証を行っている。

In order to protect operational technology (OT) systems from increasing cybersecurity risks, the Toshiba Group is continuing its efforts to offer security operation center (SOC) services for OT systems.

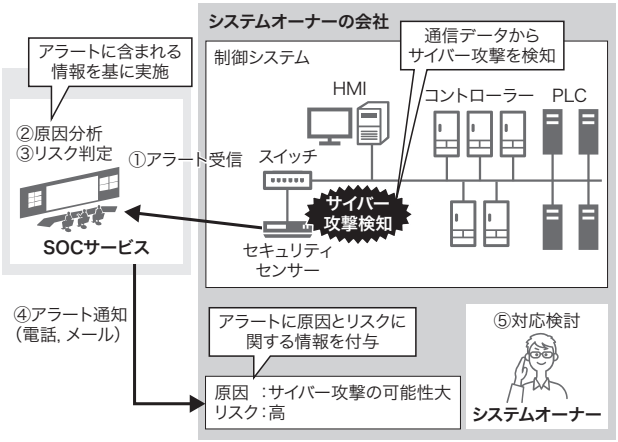
We have been actively focusing on improving the quality of these SOC services through the development of monitoring technologies to efficiently provide system owners with measures against cyberattacks. These technologies include a security monitoring platform to investigate and narrow down the causes of alerts from security sensors installed in the OT system, and a risk assessment method to evaluate the resultant impact on the OT system. In addition, we have constructed a verification environment assuming cyberattacks on various OT systems in operation using design simulators for power generation and transformation systems.

1. まえがき

昨今，社会インフラや工場などで稼働する制御システムのサイバーセキュリティリスクが増大しており，東芝グループは，制御システム向けのSOC サービスを24時間365日で提供している。SOCサービスの概要を，**図1**に示す。SOCは，通信内容からサイバー攻撃を検知するIDS（Intrusion Detection System：不正侵入検知システム）[(1)]などのセキュリティセンサーから①アラート受信し，②原因分析と③リスク判定を行う。原因分析では，そのアラートの発生原因がサイバー攻撃によるものか否かを判断する。サイバー攻撃だった場合には，それがどの程度制御システムの稼働に影響を与えるかをリスク判定により評価する。次に，その結果をシステムオーナーに④アラート通知する。システムオーナーは⑤対応検討を行い，アラートの重要度に応じて優先度を判断する。しかし従来は，原因がサイバー攻撃以外の場合も通知されることがあって（偽陽性アラート）通知回数が多くなったり，アラートによるシステムへの影響度が分かりにくかったりして，システムオーナーによる適切な対応の検討が難しかった。

これらを解決するために，東芝グループは，監視技術[(2)]の高度化に取り組んでいる。原因分析及びリスク判定の精度を高めることで，システムオーナーへの通知回数の削減とアラートに対する対応優先度の提示が可能になり，SOCサービスの品質向上につながる。

ここでは，原因分析の高度化に向けたセキュリティ監視基盤の開発と，リスク判定の精度を向上させる制御システムへの影響度評価について述べる。更に，発電・変電システムのシミュレーター環境を用いて構築した検証環境とその活用



HMI：ヒューマンマシンインターフェース　　PLC：Programmable Logic Controller

図1. SOCサービスの概要

セキュリティセンサーから発報されたアラート情報を監視し，システムオーナーに通知する。

Overview of SOC service for OT system

方法について述べる。

2. 原因分析の高度化

セキュリティセンサーの検知手法は，大別すると2種類ある。一つ目は，許可リストを用いた検知手法である。この手法では，事前に正常なパターンを許可リストとしてセキュリティセンサーに登録する。システム稼働時には，通信データを取得・分析して許可リストから外れた通信パターンを，異常な動作として検知する。二つ目は，脅威リストを用いた検知手法である。サイバー攻撃の通信パターンを脅威リストとしてセキュリティセンサーに登録し，これと一致する通信をサイバー攻撃として検知する。

制御システムは，情報システムと比較してシステム構成が固定的であり，通信パターンが変化しにくいため，許可リストを用いた検知手法が有効とされる。

2.1 許可リストを用いた検知手法の課題

許可リストは，システムの通信仕様から作成することや，システムが正常に稼働しているときの通信パターン（通信元と宛先のIP（Internet Protocol）アドレスや通信プロトコルの組み合わせ）を観測して作成することが多い。しかし，通信仕様から許可リストを作成する場合，OS（基本ソフトウェア）の標準通信などが明示的でないことや，複数ベンダーの機器が混在するために通信仕様の把握が困難なことがある。また，正常な通信データから作成する場合，観測期間に発生しない通信パターンは，許可リスト登録漏れとなるケースがある。例えば，保守メンテナンス作業などの非定常作業が観測期間中に発生しない場合や，冗長化された機器で，待機状態にある機器の通信が発生しない場合などである。

正確な許可リストが作成できないと，正常な通信が異常な通信として検知されることがある。これを防ぐため，セキュリティセンサーのアラート以外の情報（制御システムの構成やメンテナンス作業の情報など）と組み合わせた原因分析が必要になる。これには，サイバーセキュリティの知見だけでなく，監視対象の制御システムに関する知見も必要となる。しかし，SOC運用担当者は監視対象の制御システムを熟知していないため，原因分析のためには制御システムのエンジニアの協力が必要となる。

2.2 セキュリティ監視基盤の開発

そこで，制御システムエンジニアの分析作業を自動化し，SOC運用担当者による原因分析を可能にするセキュリティ監視基盤を開発した。**図2**に，プラントを監視対象制御システムとしたセキュリティ監視基盤の構成とアラートの調査フローを示す。セキュリティ監視基盤は，プラント情報管理システムなどから情報連携で入手したプラント情報（メンテナンスや，冗長系の待機状態機器への切り替え，システム構成などの情報）を保存するプラント情報DB（データベース），セキュリティセンサーからのアラート情報を受信して分析ロジックに従って原因分析を行う分析基盤，過去の分析情報を記録するナレッジDB，及び分析結果などを表示する監視ダッシュボードから構成される。この構成の特長を，次に述べる。

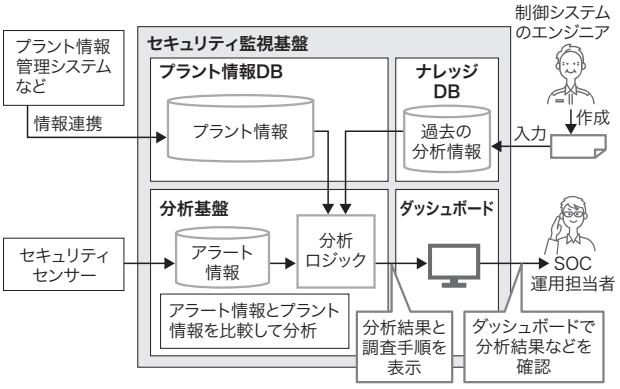


図2. セキュリティ監視基盤の構成とアラートの調査フロー

アラート情報，プラント情報，及び過去の分析情報を突き合わせて原因分析し，制御システムのエンジニアが行っていた作業を自動化する。

Configuration of security monitoring platform and flow of investigation of security alert

(1) アラート情報と，プラント情報DBの情報を分析基盤上で組み合わせることで，プラントの動作状態に由来する誤検知を排除する。例えば，アラート発生時刻にメンテナンス作業などがあったか否かを確認し，あった場合は，例外的に発生した正常な通信とみなすなどである。

(2) プラント情報DBにあるシステム構成情報を用いて，誤検知を排除する。例えば，システムに冗長構成がある場合，許可リストの中から冗長系の一方のネットワークに同様の通信パターンがないかを確認し，ある場合は，待機状態の冗長構成で通信パターンの登録漏れがあったと考えられる。このとき，ナレッジDBにある過去の分析情報が，分析精度の向上に役立つ。

(3) 原因分析した結果を，過去の分析情報としてナレッジDBに記録し，以後の分析に活用できるようにしている。セキュリティ監視基盤での分析結果のほかに，制御システムエンジニアが様々な知見を基に作成した調査手順も記録している。これにより，同様の事象が発生した場合に，SOC運用担当者が原因分析できる。

(4) SOC運用担当者が見るべき情報を集約し，分析作業を効率化するため，分析結果や調査手順をダッシュボードに表示する構成としている。

このように，セキュリティ監視基盤で原因分析を高度化して誤検出を減らすことで，システムオーナーへの通知件数を絞り込み，効率的に運用できる。

2.3　今後の取り組み

許可リストを用いた検知手法では，正常な通信パターンではないことを検知できるが，サイバー攻撃の内容は把握できない。そこで，許可リストと脅威リストをそれぞれ用いた二つの検知手法を組み合わせることで，サイバー攻撃の内容を特定する手法を開発している。具体的には，許可リストで検知したアラート情報に関連する情報，例えばアラートの発信元となった機器でのサイバー攻撃のパターンに該当する事象の発生有無を分析することで，サイバー攻撃内容を把握する。

3. リスク判定の精度向上

従来のアラートは，異常内容と通信に関するIPアドレス情報などが通知されるだけだったので，システムオーナーがこれに基づいて影響度を判断するのは難しかった。そこで，想定されるアラートに対して，事前にリスクアセスメントを実施して結果を記録しておき，監視時にはこの結果とアラート情報を比較することで影響度を評価し，リスク判定結果として提供して優先度の検討に役立てる。

3.1　リスクアセスメントの実施

サイバー攻撃が制御システムにどのような影響を与えるかの評価を，システム設計時にリスクアセスメントとして実施する。

制御システムに対する攻撃では，不正な制御コマンドを送信して制御システムの稼働に影響を与える攻撃が行われることが多いため，制御コマンドに着目したリスクアセスメントを実施する。例えば，攻撃者は不正にWriteコマンドを発行し，PLC（Programmable Logic Controller）の動作に影響を与えるなどの攻撃を行う。一方で，Readコマンドのように制御システムに直接影響を及ぼさないコマンドもある。

このように，攻撃者が発行するコマンドの種類によって異なる制御システムへの影響度を，評価する。

3.2　アラートの影響度評価

監視時の影響度評価フローを，**図3**に示す。3.1節に示したリスクアセスメント結果は，セキュリティ監視基盤のプラント情報DBに保存しておく。その結果とアラート情報をマッチングさせることで，システムへの影響度を評価する。

セキュリティセンサーは，IPアドレスやポート番号などの情報を基に，許可リストを用いた検知をしていることが多い。異常な通信を検知した際に，その通信に含まれる制御コマンドを，事前に実施したリスクアセスメント結果と突き合わせることで，アラートの影響度評価を行う。

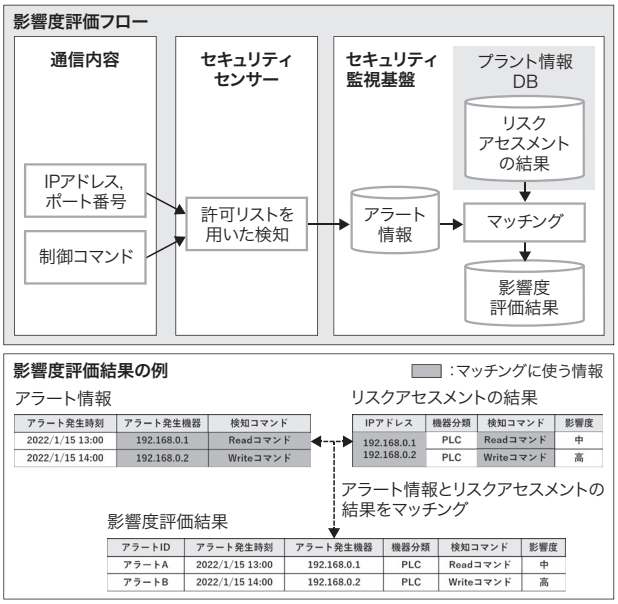


図3. 影響度評価フローと影響度評価結果の例
アラート情報とリスクアセスメント結果に含まれる，機器のIPアドレスや制御コマンドをマッチングして，制御プロセスへ与える影響度評価を行う。
Flow of impact evaluation and examples of risk judgment results

アラート情報に加えて，その影響度を付与しリスク判定結果としてシステムオーナーに通知することで，サイバー攻撃への対応優先度の提示が可能になる。

今後は，制御コマンド以外の情報についても影響度評価への有効性を検証するなど，リスク判定の更なる精度向上を図っていく。

4. 発電・変電システムのシミュレーターを用いた検証環境

2章，3章で述べた監視技術を開発するために，次の2点が重要である。

(1) 内容の把握・熟知　　制御システムの定常稼働状態や，運用操作などによる状態変化，定常稼働ではない異常状態，サイバー攻撃後の状態など，実際に発生し得る状態を再現し，動作を熟知することが重要である。

(2) ログの記録・収集　　原因分析では，制御システムの状態変化を検知するために，ログを記録し，1か所に集めて統合する必要がある。実稼働に近い動作をしている機器のログで原因分析することにより，分析精度を向上させることができる。

これらを実施するための検証環境の候補として，実稼働しているシステムや，稼働前に機能確認を行う事前環境などが挙げられる。実稼働しているシステムでの検証は，サイ

バー攻撃を行うなど定常稼働状態以外の状態を作り出すと稼働に影響があるため，避けられることが多い。また事前環境は，機能確認を主な目的としており，制御システムの一部の機能だけを再現するにとどまるため，実稼働時とはシステム状態及びログの内容が異なる。

そこで，想定する状態を自由に作り出すことができ，ログ取得が可能であり，かつ実稼働に近い，シミュレーターを用いた環境を活用する。

4.1 検証環境の概要

発電・変電システムの設計・構築に利用しているシミュレーターを基に，そこに攻撃ツール，分析のためのセキュリティセンサー，セキュリティ監視基盤を導入し，検証環境を構築した（**図4**）。

サイバー攻撃の手口を再現するために，発電・変電システムと接続している業務システム，リモートアクセス拠点のシステムを模擬して構築できるよう考慮した。また，今後の制御システムの進化も見据え，クラウドシステムと連携した制御システムが構築できるよう拡張性を持たせた。

発電・変電システムのシミュレーターには，定常運転時の通信，定常運用操作，非定型作業操作による通信状態を再現できる機能があり，偽陽性判定の検証や，制御コマンドの把握，サイバー攻撃に対する分析ができる。

4.2 検証環境での実証効果

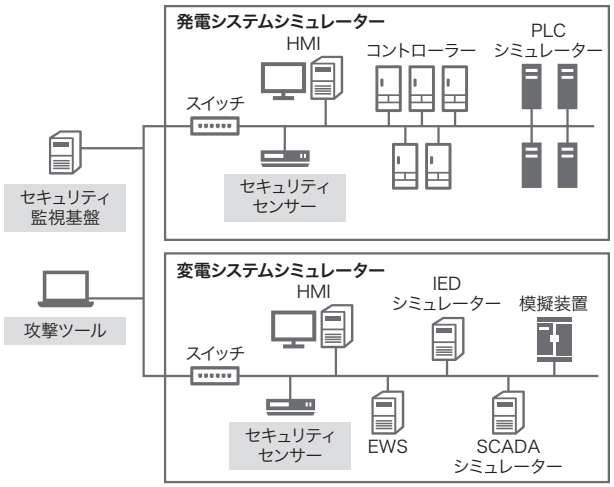
検証環境で得られる具体的な効果を，次に述べる。

⑴ サイバー攻撃に対するシミュレーション　　検証環境に攻撃ツールを導入してサイバー攻撃を模擬することで，実システムがサイバー攻撃を受けた状態に近いデータを使用した検証が可能になった。

⑵ 分析手法の継続更新　　攻撃手法は日々更新されており，それに追従するために分析手法も更新が必要である。検証環境で，攻撃手段の更新と攻撃手順の自動化，検知・防御製品の能力及び使用方法の評価，分析手法の更新のサイクルを継続していくことで，攻撃への追従と，セキュリティ対策の進化を続けていくことができる。

4.3 今後の取り組み

現状の検証環境は発電・変電システムであるが，今後は様々な分野に対するSOCサービス高度化の検証を行うため，スマートファクトリーなどのクラウドシステムと連係した制御システムや，別分野の制御システムについて，検証環境のバリエーションを増やしていく。



IED：Intelligent Electronic Device　EWS：Engineering Workstation
SCADA：Supervisory Control and Data Acquisition
：シミュレーターに追加したもの

図4. 検証環境の概要
実際のシステムに近い検証環境で実証を行い，開発の効率化と精度向上を図っている。
Overview of verification environment capable of simulating cyberattacks

5. あとがき

SOCサービスの監視技術を高度化する二つの取り組みについて述べた。今後，構築した検証環境を活用し，より実環境に近い形での原因分析及びリスク判定の精度を高める技術開発に取り組んでいく。

文　献

⑴ 東芝ITサービス．“制御システム向けサイバーセキュリティ・プラットフォームCyberX（Defender for IoT）の「リモートセキュリティ監視サービス」を提供開始のご案内”．<https://www.it-serve.co.jp/topics/20210616.htm>，（参照 2022-03-02）．

⑵ 東芝デジタルソリューションズ．“産業インフラをサイバー攻撃から守る東芝の「制御システムセキュリティ運用監視サービス」”．DiGiTAL T-SOUL．<https://www.global.toshiba/jp/company/digitalsolution/articles/tsoul/36/003.html>，（参照 2022-03-02）．


大矢　章晴　OYA Toshiharu
研究開発センター サイバーセキュリティ技術センター
セキュリティ技術部
Security Technology Dept.


原田　　崇　HARADA Takashi
東芝デジタルソリューションズ（株）
ICT ソリューション事業部 制御セキュリティ事業推進部
Managed Security Dept.


村田　　仁　MURATA Jin
東芝エネルギーシステムズ（株）
パワーシステム事業部 火力電気システム事業部
Toshiba Energy Systems & Solutions Corp.