# グローバルな脅威に対応した管理・運用を実現する制御システム向け統合セキュリティ管理ソリューション

**Integrated Security Management Solutions to Protect Operational Technology Systems from Global Security Threats**

外山　春彦 TOYAMA Haruhiko　　森田　昌 MORITA Akira　　長嶺　友樹 NAGAMINE Tomoki

社会インフラや産業システムなどの制御システムでは，インターネット技術の活用が進むにつれて，グローバルなサイバー攻撃などの脅威が顕在化しており，一般の情報システム向けセキュリティ対策の適用が難しいことから，制御システムに対応したセキュリティ管理・運用が求められている。

東芝デジタルソリューションズ（株）は，各国で整備が進む制御システム関連のガイドラインや最前線で実績を重ねる対策技術などの動向を踏まえ，制御システム向けの保有資産・通信・脆弱（ぜいじゃく）性の可視化機能や，異常検知機能，物理的な一方向通信による境界防御機能などを採用することで，国内の制御システムやその運用環境に適応したセキュリティ管理・運用を実現する制御システム向け統合セキュリティ管理ソリューションを提供している。

Operational technology (OT) systems for critical social and industrial infrastructures in Japan have been facing global security threats including cyberattacks as a consequence of the increasingly widespread utilization of Internet technologies in these areas. In particular, as it is difficult to generally apply security measures for information technology (IT) systems to such OT systems, demand has been rising for security management and operations dedicated to OT systems.

In keeping with the worldwide trend toward the development of guidelines and leading-edge cybersecurity technologies for OT systems, Toshiba Digital Solutions Corporation is offering various solutions for the realization of security management and operations adapted to both OT systems and their operational environments in Japan by integrating the following functions: (1) visualization of assets, protocols, and vulnerabilities; (2) abnormality detection; and (3) network boundary protection using a physical unidirectional communication method.

## 1. まえがき

2021年，ランサムウェアによるサイバー攻撃の影響で，米国最大手の石油パイプラインが数日間にわたり燃料供給を停止した。また，不正侵入により，米国フロリダ州の水処理システムで，飲料水への薬品添加が人命に危険な濃度に設定されるなど，社会インフラへのサイバー攻撃が社会・生活・人命を脅かすことを顕在化する事例が起こっている。

社会インフラや産業システムなどの制御システムに対するサイバー攻撃への対策は，被害に遭ったときの深刻さから国の重要課題の一つになり，政府や業種横断の連携組織・体制作りや，法律・ガイドラインなどの整備，それらに基づく各社会インフラ事業体での対応などが進められている。

重要インフラは，停止の影響が深刻なことや設備機器の更新周期が長くて変更が困難なことなど，情報システム向けのセキュリティ対策や技術を，そのまま適用することが難しい。そこで，制御システム関連のガイドラインでは，情報セキュリティのベストプラクティスや対策技術を基にして，制御システムの特性や固有のポイントに応じた対応を行っている。

一方，国内では，制御ベンダー独自の制御ソフトウェアや制御プロトコルがまだ多く使われている。グローバルな脅威への防波堤になる面もあるが，実績のある対策技術を導入する際の課題にもなっている。

ここでは，制御システムのセキュリティの特性とガイドラインの要件を踏まえ，安全なCPS（サイバーフィジカルシステム）の実現に向けた，制御システムの統合セキュリティ管理ソリューションについて述べる。

## 2. 制御システムのセキュリティの特性と考え方

制御システムのセキュリティは，情報システムと比較して，**表1**に示すような違いがある。情報システムで培われ，日々改良が加えられているサイバーセキュリティ技術やセキュリティ管理のベストプラクティスを基に検討することが重要で，次のような問題がある。

(1) 機器の更新周期が長く，追加対策が困難

(2) 被害の深刻さによる，侵入前提対策の適用が困難

**表1. 制御システムと情報システムの主な違い**
Salient differences between OT and IT systems

| 項　目 | 制御システム | 情報システム |
|---|---|---|
| セキュリティ保護対象 | 設備，事業 | 情報 |
| セキュリティ優先順位 | 可用性重視 | 機密性重視 |
| 稼働時間 | 24時間365日連続 | 通常業務時間 |
| 被害の影響 | 社会・人命への深刻な影響 | 金銭的損失・プライバシー侵害 |
| システム利用期間 | 10～20年 | 3～5年 |
| パッチ提供 | 少ない頻度 | 頻繁・定期的 |
| 運用部門 | 設備保安部門 | 情報システム部門 |
| 通信プロトコル | 制御システム固有 | 情報通信プロトコル |

⑶　事例の少なさと現場の知見不足
⑷　設備保安部門と情報システム部門の壁
⑸　制御機器のセキュリティ観点での状況把握不足

このような特性の違いや問題に対し，米国の原子力・電力分野において規制・ガイドラインが先行して整備され，汎用的な制御システムセキュリティの国際標準としてIEC 62443（国際電気標準会議規格 62443）シリーズや各国の業界ガイドラインの整備が進められている。

### 2.1　ガイドライン

事業分野などで細かな違いはあるが，以下に示すようなベストプラクティスを基本とした要件に整理されている。

⑴　体制面では，情報セキュリティと同様に，経営層から制御システムの運用現場までの横断的な体制作りを求めている。
⑵　管理面では，制御システムの管理運用までのPDCA（Plan-Do-Check-Act）を基本としたセキュリティマネジメントシステムの適用を求めている。情報資産の特定と管理に加え，制御システムの資産管理，各機器のログの管理を基本事項として求めている。
⑶　運用面では，制御システムの長いライフサイクルにわたる対応，サプライチェーンリスクへの対応，セキュリティ監視を求めている。
⑷　システム面では，誤検知による制御システムの停止を避けることや，機器へのソフトウェアの追加・変更が難しいこと，長期間にわたり利用され構成が固定的であることなどの特徴に配慮している。ネットワークを分割して外部との境界を最小化し，監視防御や，接続機器への制限・不正接続検知など，管理と監視ができるシステムを求めている。

### 2.2　制御システムへの攻撃傾向とその対応方針

従来は，イランの核施設やウクライナの送配電網への攻撃など，国家紛争・テロなどを背景とした標的を絞った攻撃が注目されていたが，近年は，米国の石油パイプラインへのランサムウェア攻撃など，対策に漏れがある対象を見付けて攻撃してくる事例が増加している。これらに対しては，アプローチの特徴を踏まえた対策方針がある。

標的型攻撃は，狙った攻撃相手に対し手段を変えながら，潜入・潜伏・探索し，機会を見て攻撃する。新たな手段を繰り出すため，一般に事前対処は難しいが，潜伏中の探索行動などの予兆を発見して対応することが重要である。

一方，あらかじめ決めた標的はなく，攻撃手段が有効な対象を見付けて攻撃する手法に対しては，脆弱性対応などの事前の対策が有効であり，その対策が想定どおりに確実に実施されていることが重要である。

いずれも高度な攻撃なので，見落としや対策漏れが重大な被害につながる。一方，制御セキュリティの現場では予兆や脅威の情報量が少なく，運用担当者だけで脅威情報を基に適切に対処することは難しいので，セキュリティ部門や専門家との連携が重要になる。

## 3.　制御システム向けのセキュリティ管理運用

ガイドラインや，攻撃の動向，対処方法に加え，先端ソリューションの動向も合わせた，制御システムのセキュリティ管理での対策ポイントを**図1**に示す。

グローバルな最新の脅威に備えるために，今回，最前線で活用され，その知見を生かし続けている制御システム向けの統合セキュリティ管理ソリューションを取り込んだ。

情報システムのセキュリティ管理ソリューションは，管理対象の機器にソフトウェアのインストールが必要であり，制御システムに適用することは難しかった。

取り込んだソリューションは，ネットワークパケットを収集してプロトコルを解析，分析・可視化し，資産管理，脅威・脆弱性管理，セキュリティ監視，インシデント対応といったセキュリティ管理・運用を支援する機能を提供する（**図2**）。また，この機能を国内事業者に適用するにあたり，独自プロトコルの利用など，国内独自の要件に対応した。

これらにより，制御システムに影響を与えずに，現状把握，事前対策，監視と検知，対応と復旧といったセキュリティ管理全体を統合的に対応できるようなった。

また，ログ管理と連携することで，全体を俯瞰（ふかん）した監視や監視アラートからインシデントに対応し，更に，物理的に侵入不可能な境界防御である一方向通信を併用することで，監視の簡素化を実現した。

これらの各機能により，セキュリティ管理・運用をどのように実現できたかについて，以下に述べる。

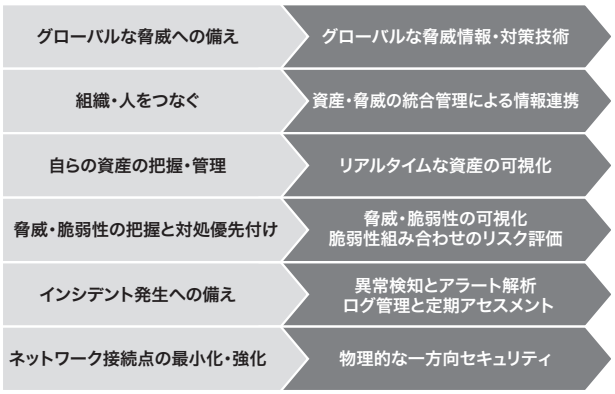


**図1. 制御システムのセキュリティ対策の要点と解決策**

社会・産業のインフラを支える制御システムには，様々なセキュリティ対策の要点がある。

Important issues concerning security of OT systems and their solutions

### 3.1 リアルタイムな資産・通信の可視化と把握

セキュリティの管理では，まず保有している資産を把握することが重要である。台帳管理されている情報が，ネットワーク接続されている機器やその通信プロトコルと整合していることを確認する必要がある。

資産管理機能では，ネットワークパケットを収集分析して資産と通信を識別し，リアルタイムに可視化できる。

制御プロトコルを解析することで，接続された機器が，例えば，PLC（Programmable Logic Controller）なのか，HMI（Human Machine Interface）なのかを識別できる。

制御システムの資産台帳とネットワーク上で識別した機器とその振る舞いを比較することで，設備運用部門とセキュリティ部門での情報共有が可能になり，連携して異常が起こっていないかを確認できるようになった。

国内提供では，独自のプロトコルに対応することが必要であった。そこで，国内標準プロトコルと制御ベンダー固有のプロトコルに対応するプラグインを試作検証し，対応できることを確認した。これにより国内独自プロトコルを利用しているシステムでも，資産管理機能の提供が可能になった。

### 3.2 脅威・脆弱性の可視化

ネットワークパケットを分析し，資産や通信を識別した情報をCVE（Common Vulnerabilities and Exposures）などの脆弱性情報やベンダー独自の脅威情報と照合した結果を提示する機能により，制御システムの運用者が保有する資産の脅威・脆弱性を把握できるようになった。また，資産情報と脅威情報を結び付けることで，セキュリティ担当と連携した脅威への対応を実現した。

更に，複数の脆弱性を用いた攻撃経路を分析する機能を活用し，単独では重要度が高くないが，組み合わせでリスクのある脆弱性にも対応可能になった。

### 3.3 異常検知とアラート解析・ログ管理

インシデント発生への備えとして，監視が必要である。制御機器は，通信の内容や頻度などの通信パターンが比較的固定的なので，資産や通信状況から正常であるかどうかが判断しやすいため，次の4種類の監視が有効である。

⑴ 通常と異なる機器の接続
⑵ 通常と異なるリスクとなり得る通信
⑶ 既知の脅威の特徴がある通信
⑷ 制御装置への危険な操作コマンド通信

これらを機械学習などによる分析で検知してリスクを判定し，アラートとして通知する異常検知機能により，監視できるようになった。

一般に，セキュリティ監視では大量のアラートへの対応が課題である。特に社会インフラでのアラート対応では，その影響度から組織的で大きな動きを伴うため，日々の監視では，重要度・緊急度が高いものに絞って対応することが必要である。その際，以下の観点が重要である。

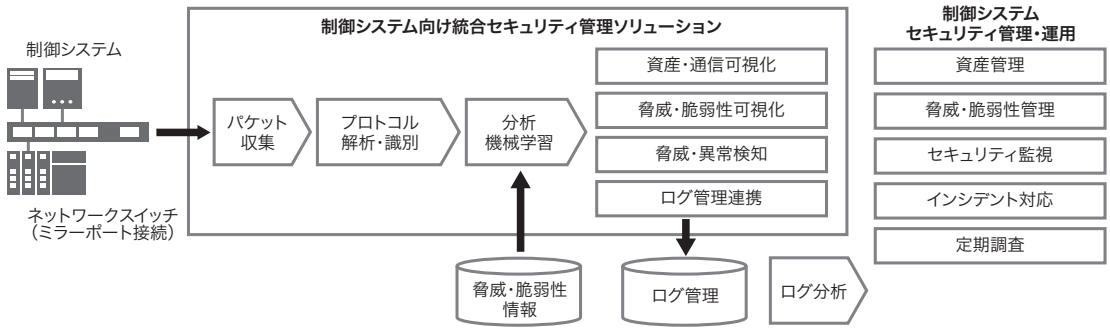


**図2. 制御システム向け統合セキュリティ管理ソリューションの概要**

ミラーポートによってネットワークパケットを複製・収集し，プロトコル解析や，分析・可視化などの機能で，セキュリティ管理・運用を統合的に支援する。

Outline of integrated security management solution for OT systems

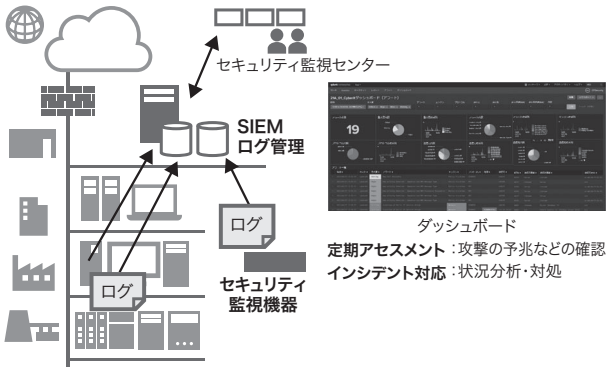


**図3. ログ管理と連携した定期アセスメントとインシデントへの対応**

ログをSIEMに集め，ログ全体の俯瞰や個々のログの詳細分析で，対策が必要なポイントやインシデントの状況を確認できる。

Periodic assessment and response to incidents in conjunction with log management system

⑴　リスクのあるアラートを見逃していないか

⑵　標的型攻撃の予兆が含まれていないか

これらに対処するには，重要なアラート通知に加え，全体を俯瞰して関連性で分析する定期的な分析が有用である。このような分析は，設備運用現場とセキュリティ部門の最新脅威への知見を高める機会にもなる。

このような分析に対しては，ログ管理を高度化するSIEM（Security Information and Event Management）が有用である[1]。各種セキュリティ機器からのログを集め，アラートの発生状況全体を俯瞰して分析することで，見逃しているアラートや攻撃の予兆を把握することが可能になる（**図3**）。更に，定期的な調査に加え，インシデントが発生したときに，アラートを起点にして複数の事象を深掘りしていくドリルダウン分析にも有用である。

このような俯瞰的な状況把握とドリルダウン分析を行うSIEMを活用したダッシュボードを開発し，検知・状況把握・ドリルダウン分析を統合した対応が可能になった。

### 3.4　物理的な一方向セキュリティ

制御システムのセキュリティ管理と運用を簡素化する，物理的な一方向通信による境界防御を採用した（**図4**）。

従来，物理的に外部ネットワークから分離されていた制御システムも，情報活用のために外部接続されることが増えている。ファイアウォールなどで論理的に進入禁止に設定できるが，設定ミスなどのリスクがあるため，異常通信がないか，常に監視が必要になる。

一方，光通信を用いて物理的に一方向通信に制限すると，逆方向に侵入されるリスクがなく監視が不要になる。制御システムの安全性を高めると同時に，セキュリティ管理を大幅に簡素化できる。例えば，北米電力信頼度協議会の

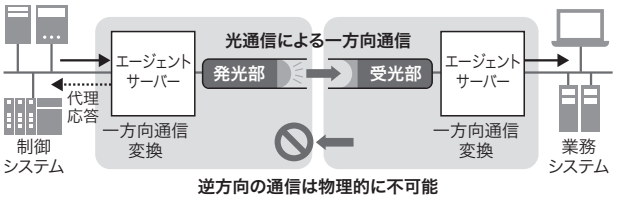


**図4. 物理的な一方向通信を用いた境界防御の概要**

光通信による一方向のデータ伝送で，制御システムに侵入する通信が物理的に不可能になり，制御システムのセキュリティ管理が簡素化される。

Overview of network boundary protection using physical unidirectional communication

重要インフラ保護基準 NERC CIP V5における要求事項の35％以上が免除されることが分かっている。

一方向セキュリティでは，実績のある多くのプロトコルをサポートする一方，国内独自のプロトコルへの対応や互換性の確認が課題であった。そこで，検証ラボを立ち上げ，構成検討や事前検証により，適用を可能にした。

## 4. あとがき

社会・産業インフラの制御システムがグローバルなサイバー脅威に対応するために，ガイドラインでの推奨事項を踏まえた，制御システム向けの統合セキュリティ管理ソリューションについて，資産管理と脅威の可視化機能や，一方向境界防御の国内制御システムの状況に適合させた展開などを述べた。

サイバー脅威は，世界中で日々変化しており，その最前線での対策を取り込み提供し続けていくことで，安全なCPSの実現に貢献していく。

## 文　献

⑴　小島健司，外山春彦．制御システム向けセキュリティ監視技術．東芝レビュー．2014，**69**，1，p.6–9.

外山　春彦　TOYAMA Haruhiko
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 マネージドサービス推進部
Toshiba Digital Solutions Corp.

森田　　昌　MORITA Akira
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
Toshiba Digital Solutions Corp.

長嶺　友樹　NAGAMINE Tomoki
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
Toshiba Digital Solutions Corp.