# 制御系サイバーセキュリティ－その実践対策と効果を考える

【セキュリティ対策ソリューション：導入法と効果】

# ICSサイバーセキュリティ実態の把握「ありもの調査」の必要性と効果的な対策

日本ダイレックス　松尾　義司

## 1. はじめに

2020年の東京オリンピック・パラリンピックを控え，政府，業界団体を中心にサイバーセキュリティ対策の強化が提唱されている。また，重要インフラ事業者に対しては，サイバーセキュリティ基本法に基づきサイバーセキュリティ戦略本部より，2018年4月4日に「重要インフラにおける情報セキュリティ確保係安全基準等策定指針（第5版）」が発行され，情報セキュリティに係るリスクへの必要な備えや，有事の際の適切な対処等を実現することなどが示されている。さらに，「制御システムのセキュリティリスク分析ガイド第2版」が2018年10月に独立行政法人情報処理推進機構セキュリティセンター（以下「IPA」）より発行され，セキュリティ対策におけるリスクアセスメントの実施と活用が推奨されている。

セキュリティ対策は，利便性を阻害する場合が多く，セキュリティと利便性という二律背反の関係をいかに最適化するかということが重要となる。また，セキュリティ対策は経営層，IT部門，OT部門，ユーザ部門の各部門が統一したセキュリティポリシーに従って「全員参加のセキュリティ対策」を実施しないと実効性の乏しい対策となってしまう。

この「全員参加のセキュリティ対策」を進める上では，各部門の意思疎通を円滑にするための用語の統一と図面（階層化され全体と部分が鳥瞰できる図面）が重要となるが，現場サイドでは，どのような機器がどのように配置，接続され，どのような通信を行っているかを継続的にトレースし，実態を把握することに苦慮している現状がある。

弊社では，多数のユーザにヒヤリングを行い，機器の台数，接続構成，配線，通信プロトコルなどの実態把握ができていないという回答を得ている。このような状態で，セキュリティ対策の強化を計画するには，まず，実態の把握が重要で，資産ベースのリスク分析の第一歩として，セキュリティ資産の棚卸（以下「ありもの調査」と表記）の実施を推奨する。

本稿ではリスクアセスメントの第一歩として実施するセキュリティ資産の棚卸（「ありもの調査」）の必要性とその手法，ツール等について解説する。

## 2. 産業用制御システムのリスクアセスメントについて

IPA発行の「制御システムのセキュリティリスク分析ガイド第2版」にも示されている通り，サイバーセキュリティ確保のためのリスクマネジメント強化の中で，リスクアセスメントが注目されている。国際標準規格IEC62443に加えてNIST（アメリカ国立標準技術研究所）やNISC（内閣サイバーセキュリティセンター）等が公開する各種セキュリティガイドライン等において，リスクアセスメントまたはリスク分析の実施が求められている。

**表1**に，IPA発行の「制御システムのセキュリティリスク分析ガイド第2版」に示されているリスクアセスメントまたはリスク分析の実施を要求するガイドライン等の例を示す。

**表1　リスクアセスメントまたはリスク分析の実施を要求するガイドライン等の例**（出典：IPA「制御システムのセキュリティリスク分析ガイド第2版」）

| 発行元 | ガイドライン等の名称 |
|---|---|
| IEC | IEC 62443-2-1:2010, Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program |
| ISO/IEC | ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems -- Requirements |
| NIST | Cybersecurity Framework Version 1.1 (April 2018) |
| NISC | 重要インフラにおける情報セキュリティ確保係る安全基準等策定指針（第5版） |
| 経済産業省 | 情報セキュリティ管理基準（平成28年改正版） |
| 日本電気協会 | JESC Z0004(2016) 電力制御システムセキュリティガイドライン 初版 |
| 厚生労働省 | 医療情報システムの安全管理に関するガイドライン 第5版 |
| 国土交通省 | 航空分野における情報セキュリティ確保に係る安全ガイドライン 第4版 |

リスクアセスメントは，ISO/IEC27000：2014で以下の3つのプロセスに規定されている。

①リスク特定

②リスク分析

③リスク評価

この3つのプロセスのうち，リスク分析は3段階のプロセスの中心に位置づけられており，その後のリスク対応を実効的にするために，非常に重要である。

経営課題であるセキュリティ対策を実施する上で，重要な観点は経営資源である「人，物，金，情報，時間，場所」をいかに効果的に配分するかである。そのためには，リスクを発見，認識および記述する「リスクの特定」とリスクの特質を理解し，リスクレベルを決定する「リスク分析」を経てリスクの大きさが受容可能か，または許容可能かをリスク基準に基づいて比較評価する「リスク評価」が求められる。

リスク分析には，定量化，数値化が重要である。リスク分析を実施することにより保護すべきシステムや事業を明確化し，それに対して想定される脅威を明確化し，その脅威に対する対策を明確化し，限られたコスト(予算)の中でリスク低減に効果的な対策を優先順位付けして実施する計画を立案・決定することが可能となる。

このアプローチは品質改善活動と同じPDCA(Plan・Do・Check・Action) サイクルであり，継続的に実施することが重要である。また，品質活動と同じく経営部門，IT部門，OT部門，ユーザ部門の全員が参加することが効果的な対策の実現に不可欠である。

## 3. ICSのセキュリティ資産の棚卸(「ありもの調査」)の必要性

2章でリスクアセスメントの重要性を述べたが，そもそもリスクを発見，認識および記述するリスクの特定を実施するためには，自社のICS (産業用制御システム)ネットワークについてどのような端末，デバイスがどのように接続され，どのような通信を行っているかを知る必要がある。

弊社の調査では，ICSネットワークは，構築時の接続構成図はあっても，その後のアップデートなどはきちんと実施されていないことが多く，時間の経過とともに個々の担当部門が接続した機器などが把握されていない。これは，OT部門では基本的にベンダが構築したネットワークは単独で運用されることが多く，他のネットワークとの接続が考えられていない，またはベンダの管理対象外として無視されるためだと推測される。

このような状況では，まずICSネットワークの実態調査が必要でセキュリティ資産の棚卸として「ありもの調査」を実施する必要がある。

「ありもの調査」では，どのような端末，通信ノード，制御装置(PLC，DCS等)がどのような接続構成で，どのような通信を行っているか，ネットワークセグメント(セキュリティゾーン)の詳細，地理的配置，論理アドレス(IPアドレス，MACアドレス等)などを調査し，情報の整理と図面の作成を実施する。ありもの調査は，リスクアセスメントの中のリスク分析プロセスに必要な情報を調査するための第一歩の工程として位置づけられる。

ICSネットワークは，ITネットワークに比較して可用性，安全性を特に重視するため，ありもの調査もICSネットワークの性質(業種，業態に関係する可用性，安全性の要求度)に応じて調査方式が異なる。「ありもの調査」の調査方式について次項で解説する。

## 4. 「ありもの調査」の方式について

ありもの調査の方式としては，既存のディジタル資産台帳，図面などのドキュメントを基に調査する机上調査と実際の現地で実施する実地調査の2つがあり，実際は問診などにより机上調査をしたうえで現地調査を実施することになる。

現地調査については，既存機器に一切の影響を与えないようにする「パッシブ調査」と既存機器に調査ツールからパケットを送信し，その応答により確認していく「アクティブ調査」がある。

また，電源が落とされている端末やネットワークに接続されていない低頻度使用端末などについての調査や配線確認，地理地番確認のための目視調査や聞き取り調査などがある。

ありもの調査分類を**表2**に示す。

### 4.1 パッシブ調査

パッシブ調査は，既存の機器に一切影響を与えないように制御システムネットワークに使用されているL2またはL3スイッチのミラーポートを介してパケットをキャプチャし分析する方式である。

この方式は，既存の機器に影響を与えないため，可用性を重視する制御システムネットワークには採用しやすい。しかし，通信している機器のパケット情報に依存するため，電源が入っていない端末や何ヵ月に1度しか使わないような低頻度使用端末の発見がで

**表2「ありもの調査」分類**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| ありもの調査 | 1 | 机上調査 | | | | | |
| | 2 | 現地調査 | 2.1 | 目視，聞き取り調査 | | | |
| | | | 2.2 | ツールによる調査 | 2.2.1 | パッシブ調査 | 2.2.1.1 パケットキャプチャ＋解析ツールによる調査 |
| | | | | | | | 2.2.1.2 セキュリティプラットフォームによる調査 |
| | | | | | 2.2.2 | アクティブ調査 | 2.2.2.1 脆弱性スキャンツールによる調査 |
| | | | | | | | 2.2.2.2 ネットワーク監視ツールによる調査 |
| | | | | | | | 2.2.2.3 ネットワーク調査，スキャンツールによる調査 |

きない場合がある。

パッシブ調査の接続構成図を**図1**に示す。

パッシブ調査に使用する計測ツールは，①パケットキャプチャツールと②セキュリティプラットフォームがある。

①パケットキャプチャツール

パケットキャプチャによる調査は，Wiresharkなどのフリーのツールを使用してパケットをキャプチャし分析できるため，ある程度スキルのある技術者であればすぐに実施できるメリットがある。しかし，複数の計測ポイントで長期間キャプチャして分析する場合は，パケット記録装置の設定，データ加工などに専門性が要求され，データ加工に膨大な工数が発生する。

弊社は，複数拠点のパケットキャプチャによるデータ加工・分析を中心とした「ITクリニックサービス」を提供している経験上，計測計画，データ加工計画など計測を実施する上での事前準備，計測時の設定，分析方針などを明確にして実施している。パケットキャプチャによる計測では，他の方式に比較して通信の詳細分析をオフラインでできるため，要求に応じて詳細分析を実施できるメリットがある。

②セキュリティプラットフォーム

セキュリティプラットフォームは，BAD(Behavioral Anomaly Detection 異常ふるまい分析装置)とも呼ばれ，NIST(アメリカ国立標準技術研究所)では，CyberXなどのベンダ数社の装置を使用した評価レポートをNISTIR 8219で公開している。セキュリティプラットフォームは，ありもの調査以外に脆弱性分析・対策，脅威の検知，フォレンジック分析，攻撃経路の発見など継続的にセキュリティ監視を行うツールとしても有用である。

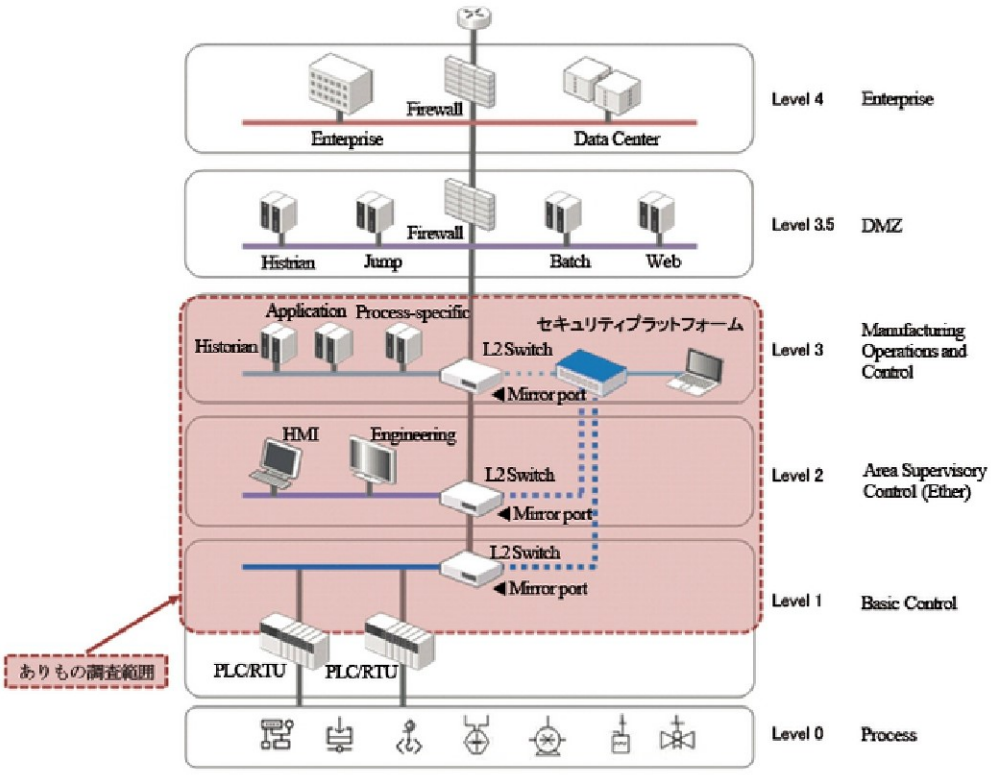


**図1 ありもの調査：パッシブ調査接続構成図**(Purdue Enterprise Reference Architecture(PERA)を参考に作成)

### 4.2 アクティブ調査

アクティブ調査は，明示的に指定したIPアドレスの範囲に対してPingなどのパケットを送信し，その応答パケットで端末，制御装置などの存在を確認する方式である。したがって，対象となる制御装置などがPingなどのパケットを受け付ける必要がある。重要インフラの設備に使用される機器などでは，このようなパケットを受信することで不安定な動作をするものがあるため，敬遠されてきたが，最近の制御ネットワークでは，Pingによる死活監視をしているものも多く，見直されてきている。

また，LinuxやWindowsなどの汎用OSを使用しているHMIなどの端末も多くなり，セキュリティ対策として脆弱性試験をするためにもアクティブスキャンを認める制御ネットワークも増えてきている。

アクティブ調査の接続構成図を**図2**に示す。

アクティブ調査に使用するツールとしては，①脆弱性調査ツール，②ネットワーク監視ツール，③ネットワーク調査・スキャンツールの3種類がある。

①脆弱性調査ツール

脆弱性調査ツールには，Tenable社の「NESSUS」やRapid7社の「Nexpose」などがあるが，ありもの調査としてスキャンを実施することで調査対象機器の存在を確認できる。機器の脆弱性情報の確認ができるメリットがあり，スケジュールを決めて定期的な脆弱性管理を実施することもできる。

②ネットワーク監視ツール

ネットワーク監視ツールには，SNMPやPingを利用した死活監視の機能を持つものがあり，ありもの調査として利用できる。この場合，死活監視をするIPアドレスを指定し，応答の有無で機器の存在を確認する。

ありもの調査と合わせてネットワークの正常性管理ができるメリットがある。特に制御システムでは，工場の敷地が広大で機器の接続状態を常時監視する意義は大きい。ICS用のネットワーク監視ツールとしては，Panduit社の「IntraVUE」がある。

③ネットワーク調査・スキャンツール

ネットワーク調査・スキャンツールには，「nmap」というフリーのツールがあり，セキュリティのスキャンツールとしては最も知られている。Nmapにはpingでの応答確認だけでなく，TCP, UDPのどのポートがオープンにされているかを確認するTCPスキャン，UDPスキャンなど多数のスキャン方法を選択できる機能がある。

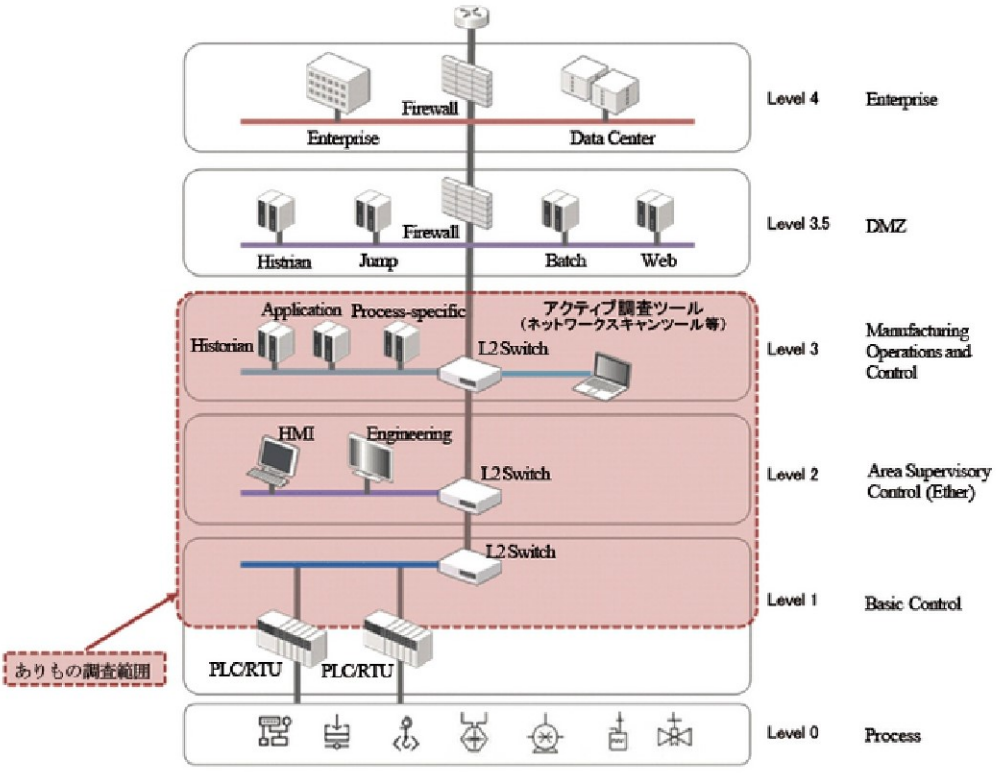


**図2　ありもの調査：アクティブ調査接続構成図**（Purdue Enterprise Reference Architecture（PERA）を参考に作成）

**表 3 ツールによるありもの調査方式の比較表(1)**

| 項番 | ツールの種類 | ツールの代表的な製品 | ツールの特徴 | メリット | デメリット |
|---|---|---|---|---|---|
| 1 | パケットキャプチャ+解析ツール | Wireshark | 一般のPCに簡単に搭載できるパケットキャプチャ，分析ツール。フリーのツールではWiresharkが有名である。 | 既存の制御システムトラフィックに影響を与えない。フリーのツールを使用すれば，安価に計測が可能。オフラインで分析可能。フォレンジックデータとしても利用できる。通信実態を把握可能。 | データ加工，分析に工数がかかる。データの加工，分析には，専門的なスキルが必要。低頻度使用機器については発見できない可能性がある。 |
| 2 | セキュリティプラットフォーム | CyberXプラットフォーム | セキュリティベンダ各社が提供している有償のセキュリティ分析装置。ネットワークの可視化機能に加え，AI(人工知能)やML(機械学習)を利用した異常振る舞い検知機能などを装備している。 | ありもの調査以外に脆弱性分析・対策，脅威の検知，フォレンジック分析，攻撃経路の発見など継続的にセキュリティ監視を行うツールとしても有用である。制御機器の通信に影響を与えない。 | 有償の製品で他の方式に比べてコスト面では，高価である。低頻度使用機器については発見できない可能性がある。 |
| 3 | 脆弱性スキャンツール | NESSUS, Nexpose | セキュリティベンダ各社が有償で提供している脆弱性診断ツール。一部フリーのツールも存在する。CVEと連携した提供ベンダーの脆弱性データベースを基に，ネットワークの機器をスキャンして機器の発見と脆弱性を調査する。 | ありもの調査の他に既知の脆弱性を保有している機器がないか，その深刻度はどうかなど数値化して脆弱性診断ができる。定期的に試験を実施することで継続的な脆弱性管理が可能。 | アクティブ調査方式であるため，制御装置によっては影響を受ける可能性がある。通信実態は，計測できない。 |
| 4 | ネットワーク監視ツール | IntraVUE | 有償または無償のネットワーク監視ツールで，Pingなどのパケットを送信し，その応答の有無でありもの調査を行う。ありもの調査以外にネットワークの健全性確認の機能を持つ。 | ありもの調査の他にケーブルを含めた通信ネットワークの常時監視が可能。ネットワーク作図機能と組み合わせたネットワークの可視化と常時監視ができる。 | アクティブ調査方式であるため，制御装置によっては影響を受ける可能性がある。通信実態は，計測できない。 |
| 5 | ネットワーク調査，スキャンツール | nmap | 脆弱性スキャンツールに組み込まれているものも多いが，無償のネットワーク調査，スキャンツールも存在する。ポートスキャン機能だけでなく，OSやバージョンの検出機能，サービスおよびそのバージョンの検出機能など，多くの機能を持つ。 | ありもの調査の他に，各機器のTCP/UDPのポート番号のオープン/クローズ状態の確認やOS，バージョンの検出機能など，多くの機能を持つ。 | アクティブ調査方式であるため，制御装置によっては影響を受ける可能性がある。スキャンの内容によっては，長時間を要する。通信実態は，計測できない。 |

しかし，スキャンの種類によっては，多数のパケットがネットワーク上に流れることがある。そのため，制御システムが使用しているネットワークトラフィックに影響を与えないように注意する必要がある。また，調査対象のIPアドレスの範囲を大きくしたり，UDPスキャンなどを全端末に実施したりすると，膨大な時間が必要になるので，スキャン内容を事前に絞り込むことが重要である。

## 5. 「ありもの調査方式」の比較

ありもの調査ツールには，前章に挙げた，①パケットキャプチャツール，②セキュリティプラットフォーム，③脆弱性調査ツール，④ネットワーク監視ツール，⑤ネットワーク調査・スキャンツールの5つのタイプがあるが，それぞれのツールを使用した場合のメリット，デメリットおよび必要要件に対する対応度を**表3**および**表4**にまとめた。

**表 4 ツールによるありもの調査方式の比較表(2)**

| 項番 | ツールの種類 | 制御装置間通信への影響 | 通信実態の把握 | セキュリティ常時監視 | ネットワーク常時監視 | 脆弱性診断 | セキュリティ脅威の検知 | フォレンジック分析 | 攻撃経路の発見 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | パケットキャプチャ+解析ツール | ◎ | ◎ | × | △ | × | × | ○ | × |
| 2 | セキュリティプラットフォーム | ◎ | ○ | ◎ | △ | ◎ | ◎ | ◎ | ◎ |
| 3 | 脆弱性スキャンツール | △ | × | △ | × | ◎ | × | × | △ |
| 4 | ネットワーク監視ツール | △ | × | × | ◎ | × | × | × | × |
| 5 | ネットワーク調査，スキャンツール | △ | × | × | × | △ | × | × | × |

コスト的にはセキュリティプラットフォームが最も高額になると考えられるが，セキュリティ要件に対する対応度，網羅性においては一番優れている。また，測定ツールでは確認できない低頻度使用機器や電源が入っていない機器などについては，目視，聞き取り調査も重要である。機器管理台帳，ネットワーク接続構成図の作成，更新と物理的な配置を記録した環境配置図などのドキュメントとともに，機器の構成情報管理も重要である。上記ドキュメントと「ありもの調査」の結果を基に，リスク分析，リスク評価を実施する必要がある。

## 6. 今後の動向

弊社（日本ダイレックス）は，既にクリニックサービスという名称で顧客ネットワークの実態調査，問題解決サービスを提供しているが，ITネットワークに加えOTネットワークでの実態調査，ありもの調査サービスの提供を開始した。ユーザの要求に応じて調査方式を選択でき，最適な調査ツールを選択して，ありもの調査に加え，リスクアセスメントサービスも提供する。

調査結果に基づいた対策についても，セキュリティプラットフォーム，データダイオード，セキュリティスイッチ，エンドポイント型ファイアウォールなど「ICS　水平・垂直多層防御ソリューション」の考え方を基に最適な対策を提供する予定である。

マツオ・ヨシジ
日本ダイレックス㈱
ネットワーク技術グループ　取締役
〒101-0047・東京都千代田区内神田2-5-5
電話（03）5207-7146
E-mail：sales@direx.com