今後のIoT時代を見据えた制御システムのセキュリティ

宇野 東平　杉浦 昌

要 旨

情報通信技術（ICT）が企業の情報システムの域を超えて、生産やサービスなどの事業基盤、社会インフラに至る隅々で活用されていくなか、制御システムの重要性が増してきている一方で、特に民間企業における制御システム、工場、プラントのセキュリティ対策は十分とはいえない状況です。企業へのインタビューを通じて、セキュリティ対策の必要性の背景、制御システムの特徴、セキュリティ対策に当たっての課題を整理し、対策の方向性について論じます。

KeyWords　制御システム／サイバーセキュリティ／CSMS／EDSA／SDN

1. はじめに

社会のデジタル化の流れのなかで、情報通信技術（ICT）がこれまでの業務システム、情報システムのオフィス内での活用の域を超えて工場や現場、製品への組み込み、家庭、社会インフラなど幅広く普及し、多大な利便性と効率性の恩恵を受けています。その一方で、悪意を持ったサイバー攻撃や内部の利用者の誤謬や犯行などによって、情報や資産の保護、事業継続性や社会の安全、安心を脅かすリスクも高まっています。

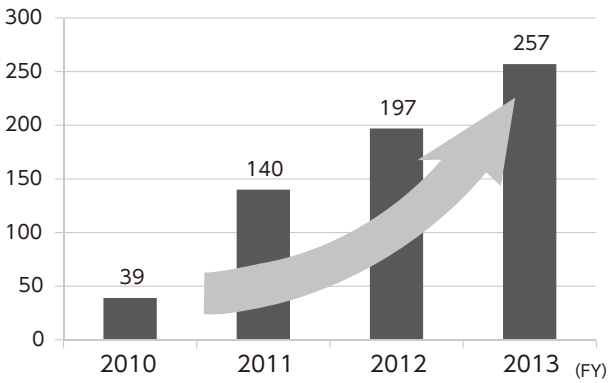
これまで、企業の情報システムやコミュニケーションにおけるセキュリティ対策は、ある程度注視され行われてきています。一方で、事業を支える制御システム領域のセキュリティ対策については、十分とはいえない状況です。

本稿では、特に企業の制御システム領域の対応状況と対応の方向性について論じます。

2. 制御システムセキュリティの背景

2010年にイランの核施設に対してStuxnetというマルウェアを使用して行われたサイバー攻撃の出現以降、海外では特にエネルギー・プラントや重要機器製造業などへのサイバー攻撃が急増しており（図1）、2014年には新たに2種類のマルウェアも検出され、更なる増加の兆しが現れています。米国自動車会社の工場では、持ち込まれたPCから制御システムがウイルス感染し、生産ラインが停止して約17億円の損害が発生、サイバー攻撃による石油パイプラインの爆発、2014年ではドイツ製鉄所がマルウェア感染し溶鉱炉を正常停止できず、設備破損で多大な被害を受けるなどの事象が起きています。

これは海外だけのことではなく、日本国内においても情



FY：財政年度（10/1 ～ 9/30）
※ICS - CERT「Year in Review 2012」及び「Year in Review 2013」をもとに作成

図1　米国ICS-CERTサイバーインシデント対応件数

報処理推進機構（IPA）に届けられる制御システムにおける脆弱性情報で、リモートからシステムを完全に制御されるような場合や、大部分の情報が漏えいするような深刻な脅威に関する届け出件数が増加しています（図2）。

制御システムにかかわるこれらセキュリティインシデントの増加の現象に対して、実際に企業がどのように捉えていて、どのように対応していこうとしているのかを、ヒアリングに基づく実地調査を踏まえて論じます。

制御システムセキュリティが求められている背景として以下3つ挙げられます。

1つ目は、M&Aなどを活用して事業のグローバル化を加速し、生産拠点はもとより研究拠点をも海外に進出していくなかで、操業ノウハウ、レシピ情報、設計情報などの機密情報も海外拠点に展開され、機密情報の漏えいのリスクが高まってきているという課題認識があります。

2つ目は、工場の自動化やネットワーク化が進むなか、情報セキュリティ事故が社会インフラや工場、プラントの安全、環境保全を脅かす事態に発展するリスクが高まってきているという課題認識です。2014年11月に成立したサイバーセキュリティ基本法にみられるように、政府が主体となり、社会インフラを支え、社会環境に甚大な影響を及ぼす可能性のある13業種を指定し、各業界でセキュリティに関する安全基準を設けて対策を講じるとともに、インシデントの報告、情報共有などを求めています。

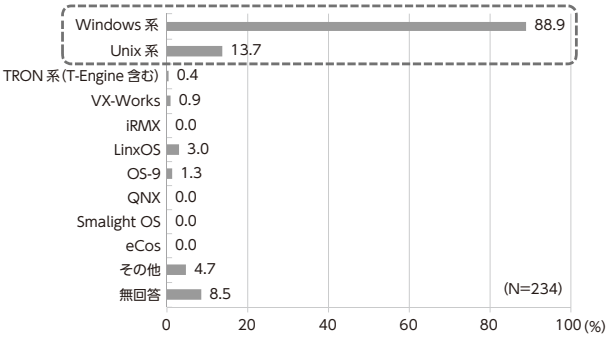
このように、官民一体となってサイバーセキュリティ対策を行っていく環境作りがなされてきています。

従来のセキュリティ対策とは様相を変え、事業継続や企業の社会的責任といった経営課題の1つとなっているという背景があります。

3つ目は制御システムそのものに起因する背景として、工場、プラントのオープン化とネットワーク化です。「工場は制御システムベンダー独自の技術、プロトコルで構成されており、セキュリティのリスクはあまりない。工場は外部との接続はなく安全だ」という声が以前は聞こえていました。

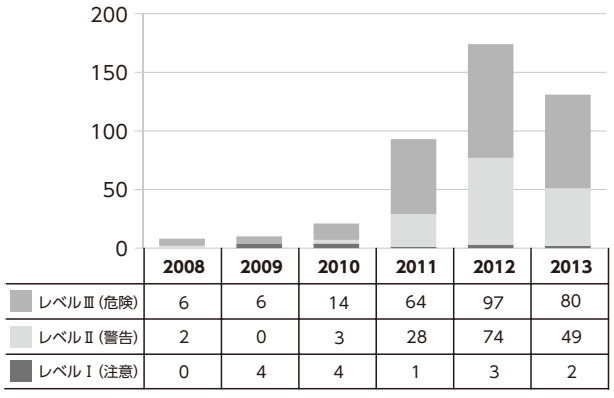
図3は、2009年時点で既にプラント設備の約9割が汎用的なOSを利用しているという、経済産業省の調査結果です。また、図4は同じ調査で、約4割のプラント設備は外部との接続がなされているという結果です。ほかに、7割のプラント設備でUSBデバイスを利用してデータの入出力、保守を行っているという回答もあります。

最近では更に、無線LANやタブレット端末の利用、インダストリー4.0やインダストリアル・IoTといった“つながる工



※経済産業省「工業用装置等における汎用IT技術応用に起因する脅威と対策に関する実態調査事業 報告書（平成21年3月）」をもとに作成

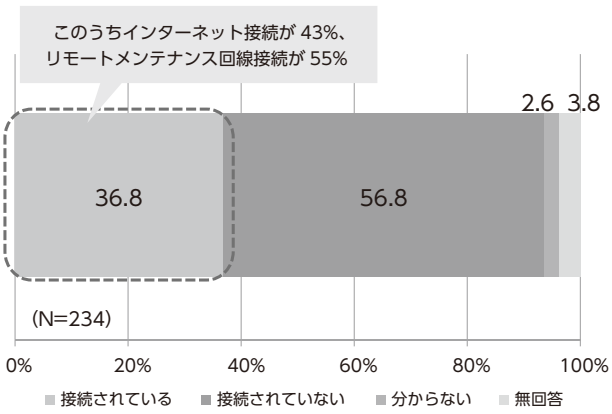
図3　プラント整備でのOSの利用状況（端末）



	2008	2009	2010	2011	2012	2013
レベルⅢ（危険）	6	6	14	64	97	80
レベルⅡ（警告）	2	0	3	28	74	49
レベルⅠ（注意）	0	4	4	1	3	2

※IPA「脆弱性対策情報データベース JVN iPedia の登録状況［2013年第4四半期（10月～12月）］」をもとに作成

図2　産業用制御システムに関するソフトウェアの脆弱性の深刻度別件数



※経済産業省「工業用装置等における汎用IT技術応用に起因する脅威と対策に関する実態調査事業報告書（平成21年3月）」をもとに作成

図4　外部ネットワークとの接続

場、つながる製品”といったコンセプトに向けて、グローバルでの工場の見える化、ネットワーク化など、新たなビジネスニーズへの対応が迫られてきています。

3. 制御システムの特徴

次に、制御システムにかかわる代表的な特徴について整理し、制御システムセキュリティの課題を考察します。

図5は代表的な制御システムの構成イメージです。

オフィス系のネットワークとは別の、制御情報ネットワーク、制御システムネットワーク、フィールドネットワークの3層で構成されています。

図中に点線で囲んだ範囲を制御システムと捉えて、その特徴を挙げます。

- **可用性重視のシステム**
  リアルタイムでの制御動作が最優先で、システムとしてはシンプルに、セキュリティ対策など講じられているケースは少ない。また、制御動作への影響を排除するため、パッチをあてるなどのシステム更新をすることが少ない。
- **接続性重視のシステム**
  さまざまなフィールド機器と接続するため、インタフェースやプロトコルは一般に公開されているオープンなものが多い。
- **長い使用年数**
  10～20年使用するため、サポート切れのOSやアプリケーションが組み込まれていたり、利用されている場合が多い。
- **ベンダー依存度の高さ**
  システムの可用性を最優先するため、制御システムの維持、運用、保守は制御システムベンダーに依存している場合が多い。
- **組織の役割分担**
  図5での制御システムネットワーク以上が情報システム部門の管理、以下がエンジニアリング部門、生産技術部門などの管理という役割分担が多く、情報セキュリティという観点での連携や、情報システムと制御システム双方を理解した人材が不足している場合が多い。

つまり、制御システムは、オープン・ネットワーク化されている一方で、システムとしてのセキュリティ対策は行われていない、あるいは行うことができない状態で、脆弱性が多く、非常にセキュリティリスクの高い状態であるといえます。

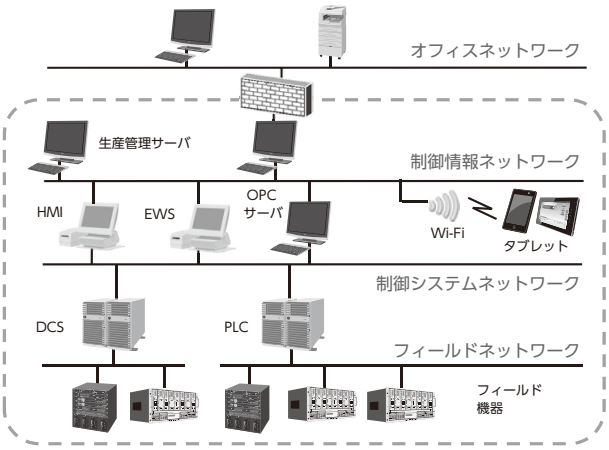


図5　制御システム構成イメージ

以上から、制御システムセキュリティに関する主要な課題を以下の3つにまとめます。

(1)　制御システムにおける情報セキュリティ意識の醸成
(2)　制御システムの特徴に応じた対策施策の導入
(3)　サプライヤーと連携した対応

4. 制御システムセキュリティの対応施策案

ここで、第3章で挙げた3つの課題に対する施策案をそれぞれ紹介します。

4.1 制御システムにおける情報セキュリティ意識の醸成

制御システムセキュリティとして何に取り組まなければならないか、そのフレームとして国際規格IEC 62443-2に基づくCSMS（Cyber Security Management System）というマネジメント認証があります。情報システムセキュリティにおけるISMS（Information Security Management System）の制御システム版に当たります。認証取得は別として、認証の要求事項をリファレンスとして取り組むことは有益であるといえます。

4.2 制御システムの特徴に応じた対策施策の導入

- **ネットワークのセグメント化の利用**
  セキュリティレベルに応じてネットワークを分割し、マルウェアの侵入、拡大を防止するとともに、サポート切れ端末の活用環境をセキュアにします。
  具体的には、ファイアウォールなどでオフィス系ネット

ワークと制御系ネットワークを分離することはもちろん、SDN（Software-Defined Networking）技術を活用し、サポート切れ端末のネットワーク接続や不審な動きをするパケットを捉えた場合、よりセキュアなネットワークに迂回させたりしてセキュリティを確保します。

- **個人認証管理の導入**

  工場、プラント内で作業従事する人が社員のみに限定されず、かつ流動性が高いなかで、ID・パスワードによる個人認証を運用することには困難があります。その場合、物理的なセキュリティとサイバーセキュリティの複合的な対策を講じることができます。

  例えば、監視の効く執務室でのみ制御システムの操作が可能になるようにする、監視カメラでの顔認証を活用して個人認証を行うなどです。また、個人認証と前述のSDNを組み合わせることで、個人単位にアクセスできるネットワークを動的に限定することも可能になります。

その他、ホワイトリスト型のアプリケーション制御やUSBなどのデバイス制御など、オフィス領域でのセキュリティ対策を十分に活用できます。

4.3 サプライヤーと連携した対応

情報システムにおいては、調達時、運用時に非機能要件としてセキュリティ要件を明確にすることは一般的ですが、制御システムについてもセキュア開発、運用の要件定義の必要性が高まってきています。更には、先に示したCSMS認証の関連として、EDSA認証（Embedded Device Security Assurance）という製品認証制度があります。そのフレームを活用して、導入する制御システムのセキュリティ機能を確認する方法もあります。

5. むすび

制御システムセキュリティという領域では、その影響の重要性を認識しながらも対策が不十分と感じている企業が大半です。また、制御システム、工場となると海外現地法人を含めたグローバルセキュリティ管理と切り離せない難易度の高い管理になってきます。

オフィスと工場、本社とグループ会社、国内と海外といった壁を越えて、情報システム部門がそのノウハウを生かして経営に近い立場からリードしていくことが強く求められていると感じています。

参考文献

1）サイバーセキュリティ戦略本部：重要インフラの情報セキュリティ対策に係る第3次行動計画（改訂版），2015.5
2）日本情報経済社会推進協会（JIPDEC）：制御システムセキュリティにおけるサイバーセキュリティマネジメントシステム（CSMS）認定・認証制度に関する文書の公表について，2014.4
3）日本情報経済社会推進協会（JIPDEC）：CSMSサイバーセキュリティマネジメントシステム 適合性評価制度の概要，2015.2
4）経済産業省：工業用装置等における汎用IT技術応用に起因する脅威と対策に関する実態調査事業 報告書，2009.3
5）情報処理推進機構（IPA）：脆弱性対策情報データベースJVN iPediaの登録状況［2013年第4四半期（10月～12月）］，2014.1
6）情報処理推進機構（IPA）：制御システム利用者のための脆弱性対応ガイド，2015.3

執筆者プロフィール

宇野 東平
コンサルティング事業部
シニアマネージャー

杉浦 昌
サイバーセキュリティ戦略本部
シニアエキスパート

NEC 技報のご案内

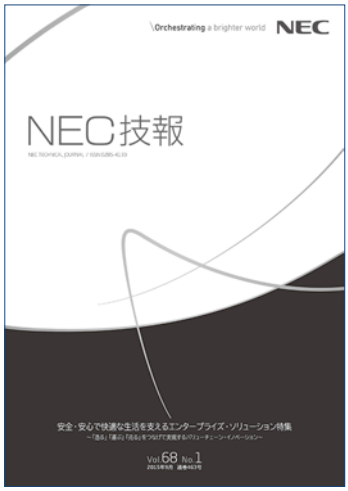
NEC技報の論文をご覧いただきありがとうございます。
ご興味がありましたら、関連する他の論文もご一読ください。

NEC技報WEBサイトはこちら

NEC技報(日本語)　　NEC Technical Journal(英語)

Vol.68 No.1　安全・安心で快適な生活を支えるエンタープライズ・ソリューション特集
～「造る」「運ぶ」「売る」をつなげて実現するバリューチェーン・イノベーション～

安全・安心で快適な生活を支えるエンタープライズ・ソリューション特集によせて
NECが考えるバリューチェーン・イノベーション
～バリューチェーン・イノベーションが実現する安全・安心で快適な生活～



Vol.68 No.1
(2015年9月)

特集TOP

◇ 特集論文

バリューチェーン・イノベーション「造る」
製造業を元気に！ NECものづくり共創プログラム
IoTを活用した次世代ものづくり ～NEC Industrial IoT～
インダストリー4.0と自動車業界におけるものづくり改革の最新動向

バリューチェーン・イノベーション「運ぶ」
アジア新興国における物流可視化クラウドサービス

バリューチェーン・イノベーション「売る」
小売業の方向性とICTの貢献 ～Consumer-Centric Retailingの追求～
サービスの高度化を支える電子決済
オムニチャネル時代のポイントとECソリューション「NeoSarf/DM」
「おもてなし」をグローバルに展開するNEC Smart Hospitality Solutions

豊かな生活/豊かな暮らし
公共交通ICカードソリューションの取り組みと今後の展望
スマートモビリティへの取り組み
EV充電事業の商用化を支えるEV充電インフラシステム
IoTを活用した端末・サービス基盤と業際ビジネス実現に向けた取り組み

エンタープライズ領域を支える先進のICT/SIへの取り組み
新たな価値を創出するビッグデータ活用
補修用部品の在庫最適化に貢献する需要予測ソリューション
異種混合学習技術を活用した日配品需要予測ソリューション
プラント故障予兆検知サービスのグローバル展開
食品メーカーの商品需要予測へのビッグデータ技術活用
事業貢献を実現するマルチクラウド活用法と移行技術
SDNを活用したグループ統合ネットワーク ～東洋製罐グループホールディングス株式会社様～
企業を狙う標的型攻撃の動向とサイバーセキュリティ対策ソリューション
深刻化するサイバー攻撃対策を「確実な実践」に導くセキュリティアセスメント
今後のIoT時代を見据えた制御システムのセキュリティ
画像識別・認識技術を活用したVCAソリューションへの取り組み
短納期・低コストを実現する現場SEから生まれたWeb開発フレームワーク
IoT時代に新たな社会価値創造を実現する組込みシステムソリューション
NECにおけるSAPプロジェクトの先進的な取り組み