ものづくりの現場における制御システムのセキュリティ対策

Security Measures for Industrial Control Systems of MONOZUKURI Sites

● 岩田洋一　● 平尾直也　● 鈴木智良

あらまし

ものづくりの現場では，IoT(Internet of Things)，Industrie 4.0などのキーワードに代表されるように，高度なロボット制御技術などを駆使したデジタル化が急速に進んでいる。一方，近年高度化するサイバー攻撃の対象は，情報システム分野のみならず，ものづくりの現場や重要インフラで稼働し続ける制御システム分野にまで広がっている。制御システムは，連続稼働およびリアルタイム制御・処理が求められるため，情報システムで培われた最善のセキュリティ対策が必ずしも適用できるわけではない。また，制御システムが稼働するものづくりの現場において，セキュリティの脅威が把握されておらず,具体的に何をどこまで実施すれば良いのかを決められないという課題がある。更に，制御システムをサイバー攻撃から守り，現場がサイバー攻撃を受けた場合の対処をリードできる人材が不足していることも問題である。

本稿では，ものづくりの現場におけるセキュリティリスクを可視化する手法，および制御システム分野のセキュリティ人材の育成について紹介し，今後の展望について述べる。

Abstract

As the terms the Internet of Things and Industrie 4.0 imply, *MONOZUKURI* (manufacturing) is rapidly undergoing digitization, leveraging highly developed technologies for controlling robots. Meanwhile, cyberattacks continue to become more tactical, targeting not only information systems but also industrial control systems that are in non-stop operation at *MONOZUKURI* sites and critical infrastructure. The fact that the industrial control systems require perpetual operation and real-time control/processing, makes it difficult to ensure that the best security measures developed for information systems always apply to them. Many *MONOZUKURI* sites where industrial control systems are deployed are unaware of their security threats, and thus they are unable to determine specific actions and the extent to which they need to be implemented. There is also a shortage of personnel who have the knowledge and skills to defend the industrial control systems from cyberattacks, and who can lead an incident response team when their site comes under attack. This paper presents a method to visualize security risks at *MONOZUKURI* sites, and describes the training for security engineers in the industrial control systems field, followed by a discussion on the future prospects.

ま え が き

ものづくりの現場では，品質向上および効率化を目的としたデジタル化が急速に進んでいる。製造工場における各種センサー，センサーを制御するPLC（Programmable Logic Controller），システム監視とプロセス制御を行うSCADA（Supervisory Control And Data Acquisition）などで構成される自動運転システムは「制御システム」と呼ばれており，オフィス環境における情報システムとは区別されている。従来の制御システムは，外部ネットワークとの接点を持たず，専用OS，専用プロトコルが使われていたため，第三者に狙われるリスクが低く，セキュリティ対策はほとんど実施されていなかった。

しかし，近年の制御システムは，パソコンやタブレットなどをはじめとする汎用的なICTの利用が加速しており，かつ情報システムと密にネットワークでつながるようになったため，マルウェアに感染するなどのセキュリティリスクが高まっている。公表はされていないものの，マルウェア感染による製造工場のライン停止は日本の多くの製造業が経験していると言われており，製品に対するバックドア（外部から侵入するための裏口）の仕掛けや，製品設計の情報漏えいなどのリスクも存在する。

日本では，制御システムに対するサイバー攻撃への対処のため，経済産業省の指導のもとに2012年3月に技術研究組合システムセキュリティセンター（CSSC：Control System Security Center）[(1)]が設立された。ここでは，高セキュア化技術などの研究開発などが進められており，富士通も2013年から参画している。

一方，ものづくりの現場においては，セキュリティ対策として何をどこまで実施すれば良いのか決められない，という声がよく聞かれる。その背景として，以下の2点が挙げられる。

(1) 制御システムを管理・監督する現場部門において，セキュリティに対する知見が不足している。
(2) セキュリティに精通している情報システム部門は，制御システムの現状を理解しきれていないため，セキュリティ対策が進んでいない。

富士通では，制御システムにおけるセキュリティ強化の考え方として，マネジメント，フィジカル，システムの3点を挙げている（**図-1**）。その中でも，

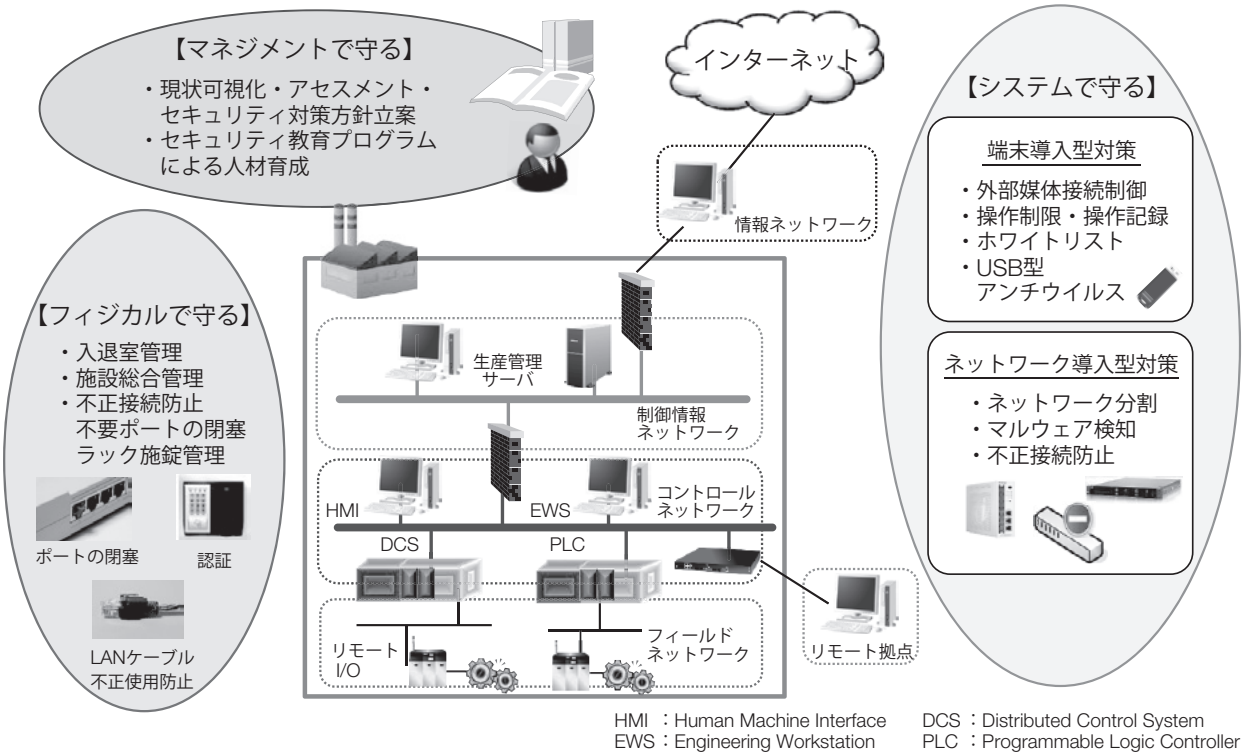


図-1　制御システムにおける三つのセキュリティ対策の考え方

マネジメントに関しては，制御システムの特性を理解した専門家によるセキュリティコンサルティング「制御システム　アセスメント/ポリシー策定支援」の提供を2014年5月から開始し，お客様の制御システムにおけるセキュリティ施策を支援している。

本稿では，制御システムのセキュリティリスクを把握し，セキュリティ対策の優先度を決定するために使われる，セキュリティリスクを可視化する手法について述べる。また，制御システムセキュリティと情報システムセキュリティの両面を理解する人材の育成についても併せて紹介する。

制御システムにおけるセキュリティ対策事情

近年のものづくりの現場における制御システムは，コストダウンやシームレスなデータ連携を目的として，情報システムで培った技術が使われるようになり，情報システムとネットワークを介してつながることが増えてきている。そのため，セキュリティリスクが情報システムと制御システムの間で相互に影響し合う関係となっている（**図-2**）。つまり，情報システムからネットワーク経由で侵入したマルウェアが制御システムに感染するリスクだけではなく，逆に制御システムに蔓延（まんえん）したマルウェアが情報システムにも拡散してしまう可能性がある。

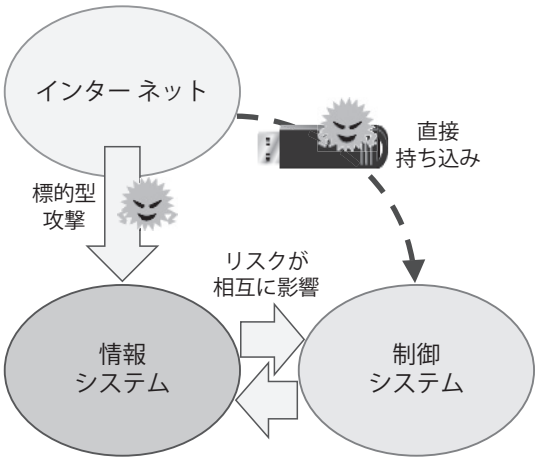


図-2　制御システムと情報システムとの関係性

制御システムにおいて，セキュリティ対策が遅れているのは，次のような制御システム導入時・運用時の背景によるものと考えている。

(1) 連続稼働し続ける必要があり，停止できない。また，リアルタイム処理に必要な性能が求められるため，リソースを消費するセキュリティパッチの適用やアンチウイルスソフトウェアなどの導入が難しい。
(2) 操業開始時の状態のまま使われ続けるため，その後発見されたセキュリティの脆弱性が未対策のまま残る。
(3) 制御システムにおけるセキュリティ標準化の取り組みは始まったばかりであり，ベストプラクティスが確立されていない。

上記のような制御システム特有の制限があるとはいえ，セキュリティ対策の基本的な考え方は情報システムと同じであると考えている。すなわち，情報システムとは異なる制御システムに内在するセキュリティリスクを明らかにし，セキュリティ対策基準を策定する。その上で，順次セキュリティレベルを向上していくマネジメントシステムを確立することが，制御システムでも重要である（**図-3**）。

セキュリティ基準とのFit & Gap分析の工夫

制御システムにおけるセキュリティリスクを把握するためには，理想像となる基準を定め，理想

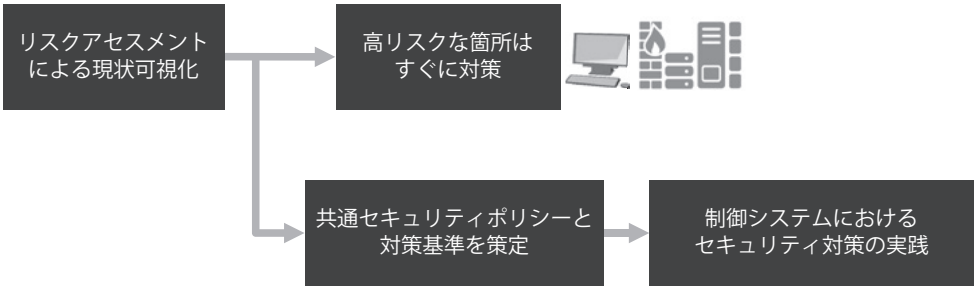


図-3　制御システムにおけるセキュリティ強化の進め方

と現状がどの程度一致し，あるいは乖離（かいり）しているかを確認するFit & Gap分析を行う手法が考えられる。制御システムセキュリティの基準となり得るものとして，国際標準であるIEC62443-2-1[(2)]がある。これは，情報システムを対象とした国際セキュリティ基準であるISO/IEC 27001との互換性が高く，情報システムセキュリティマネジメント（ISMS）を構築した経験があるエンジニアにとっては扱いやすい基準と言える。しかし，IEC62443-2-1に含まれる126件の要求事項は，内容が抽象的な表現にとどまるため，要求事項を満たしているかどうかの判定が曖昧となり，リスクを把握するための基準としては使いづらい側面もある。

そこで，富士通はIEC62443-2-1をベースとして，以下のようにカスタマイズすることで，製造工場の現場になじむリスクアセスメントを実践している。

（1）要求事項の絞り込み（30 ～ 35項目）
（2）分かりやすい表現への置き換え
（3）選択式回答の採用

具体例として，IEC62443-2-1の要求事項の一つである「接続の保護」においては，「全ての接続は適切に保護すべき」というレベルの記述にとどまっているが，富士通のリスクアセスメントにおいては，以下のような質問事項・選択肢に変換される。

（1）質問事項

工場から許可されたUSBメモリ（可搬媒体）のみ利用していますか？

（2）回答選択肢

・制御端末にUSBメモリの管理ソフトをインストールして利用制限している。
・利用許可されたUSBメモリにシールを貼るなどして識別できるようにしている。
・ルールで個人所有など許可を受けていないUSBメモリの利用を禁じており，社員・委託先に周知できている。
・利用するUSBメモリについては，特に制限していない。

選択式回答とすることで，各製造工場の調査結果を集計しやすくなるとともに，継続的な改善に使用できる。

リスクアセスメント実施のステップ

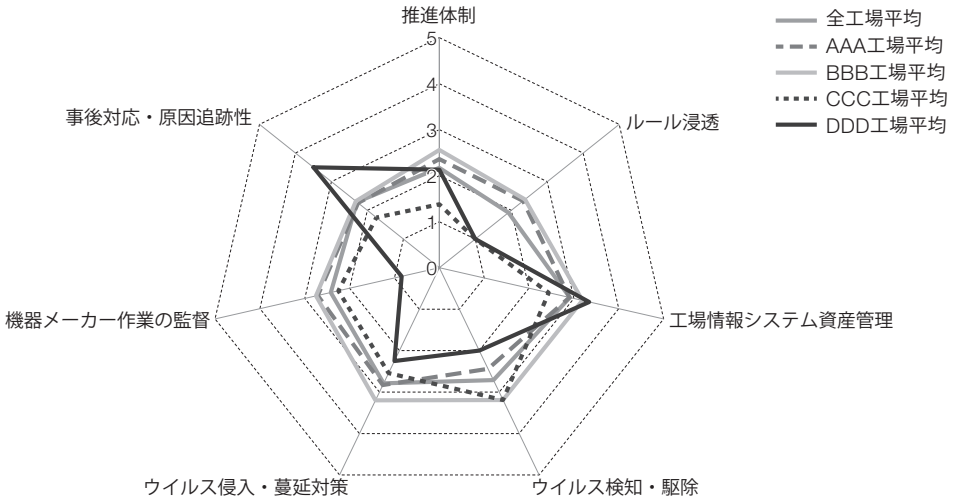
前章で述べた質問方式に則り，製造工場のアセスメントを実施する前に，製造工場の全体業務・システム概要を把握する目的でモデル工場における視察を行うとともに，質問事項が現場部門に受け入れられる表現となっているかの妥当性を評価することが重要である。製造工場の現場にとって，セキュリティ関係の質問に答えることは通常の業務にはなく不慣れである。このため，アセスメントの趣旨説明とともに，できるだけ回答の負荷を軽減することが回答率の向上と正しい回答を得ることにつながる。したがって，富士通が製造工場のアセスメントを実施する際は，以下の四つのステップを実践している。

（1）現場への趣旨説明資料とアンケートシートの作成
（2）モデル工場におけるアンケートシート妥当性評価と強み・課題の整理
（3）アンケートシートによる全工場の調査
（4）結果分析と改善提言

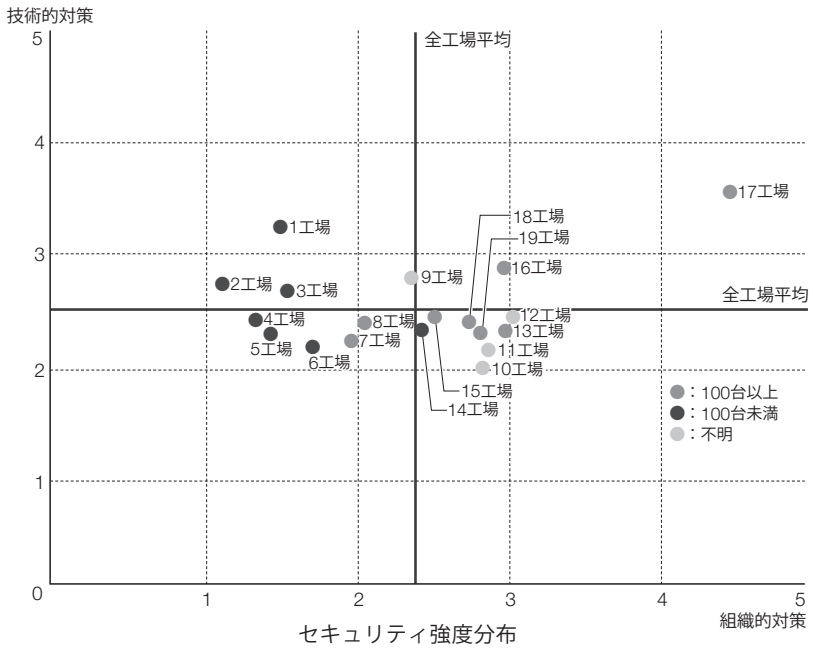
リスクアセスメントのアウトプットとしては，セキュリティ対策状況が分かるレーダーチャート，全工場のアンケート結果を色分けすることで傾向分析を行うバランスマップ，工場の規模や製品の種別ごとのセキュリティ強度分布図などがある（**図-4**）。その結果を基に改善計画を策定し，現場に提示する。しかし，現状実施できないことを優先度順に行うだけではなく，実施できている好事例をほかの工場に水平展開していく施策も重要となる。

制御システム分野のセキュリティ人材育成

制御システムにおけるセキュリティリスクアセスメントや，その後のセキュリティ施策の遂行，また万が一制御システムにおいてセキュリティインシデントが発生した場合，制御システムの特性を理解し，かつセキュリティ対策を実施できるだけの知見を持つ人材が求められている。国際的に見ると，制御システムセキュリティの資格制度であるGICSP（Global Industry Cyber Security Professional）[(3)]の運用が2013年から開始されており，全世界で775名（2015年末）がGICSPとし



セキュリティ対策状況レーダーチャート



セキュリティ強度分布

図-4　制御システムリスクアセスメントのアウトプット例

て認定され，富士通ではGICSPの認証取得を推進（1名取得済み）している。また，米国のSANS Instituteやアイダホ国立研究所が提供する制御システム分野のサイバーセキュリティ演習にも継続的に参加し，同分野の人材育成に力を入れている。

更に，ものづくりの現場におけるセキュリティ意識改革を目的に，ものづくりに携わる社員に対して制御システムセキュリティトレーニングを2015年9月に初めて実施した。トレーニングは，PLC，HMI（Human Machine Interface）などから構成される制御システムシミュレーターを用いて，制御システムで発生したマルウェア感染によるセキュリティインシデントの原因分析を行う演習形式とした。実機を用いた演習を受講者に体験してもらうことで，制御システムにおけるセキュリティインシデントが与えるインパクト，および制御システムセキュリティの重要性の理解につなげている。

今後の課題

制御システムにおけるセキュリティ対策は，情報システムと同様に継続的に取り組む必要がある。

本稿では，マネジメントの中のリスクアセスメントと人材育成について述べてきた。

今後は，情報システムのセキュリティ対策と同様に，ファイアーウォールなどの境界防御に加え，サイバー攻撃によって制御システム内に侵入されることを想定した監視・検知・インシデント対応などのセキュリティ対策が求められると考えている。すなわち，制御システム向けのセキュリティ運用のために，SOC（Security Operation Center）やCSIRT（Computer Security Incident Response Team）の機能が求められることを意味する。富士通は，2015年11月に情報システムにおけるセキュリティ運用の知見を基に，お客様のセキュリティ運用をトータルでサポートする「FUJITSU Security Solutionグローバルマネージドセキュリティサービス」[4]を発表した。今後は，本サービスのエンハンスとして，ものづくりの現場で使われるプロトコルやログ，特性を理解した上での分析を行い，情報システム・制御システム双方のセキュリティ運用をサポートする予定である。

む　す　び

本稿では，ものづくりの現場におけるセキュリティ対策立案に有効な制御システムにおけるリスクアセスメント手法，および制御システムセキュリティ分野の人材育成について述べた。

制御システムにおけるセキュリティ対策はまだ途上ではあるが，大規模なサイバー攻撃が発生してから対策を講じても手遅れである。ものづくりの現場においても，スマートなものづくりにより，品質向上・効率化というメリットがある一方，つながるリスクがあることも併せて認識しなければならない。

富士通は，情報システムに限定することなく，ICTが利活用される全てのシーンにおいて，安心・安全を提供することにより，お客様の事業の発展を支えていく所存である。

参考文献

(1) 技術研究組合制御システムセキュリティセンター（CSSC：Control System Security Center）.
http://www.css-center.or.jp/

(2) IEC 62443-2-1 Industrial communication networks - Network and system security - Part 2-1：Establishing an industrial automation and control system security program.

(3) GICSP（Global Industry Cyber Security Professional）.
http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp

(4) 富士通：FUJITSU Security Solutionグローバルマネージドセキュリティサービス.
http://www.fujitsu.com/jp/solutions/business-technology/security/secure/global-managed-security/globalmanaged-securityservice/

著者紹介

岩田洋一（いわた　よういち）
セキュリティマネジメントサービス事業本部
マネージドセキュリティ事業部
マネージドセキュリティサービスの企画・開発に従事。

平尾直也（ひらお　なおや）
セキュリティマネジメントサービス事業本部
マネージドセキュリティ事業部
制御システム分野におけるセキュリティサービスの企画・開発に従事。

鈴木智良（すずき　ともよし）
セキュリティマネジメントサービス事業本部
マネージドセキュリティ事業部
サイバーセキュリティインテリジェンスの開発に従事。