スマートマニュファクチャリングを支える製造システムセキュリティ

Manufacturing System Security to Protect Smart-Manufacturing Systems

小 野 正 浩* 坂 田 祐 二*
Masahiro Ono Yuji Sakata

近年，サプライチェーンの仕組みは，データの流通・活用を含み，柔軟で動的になっている．それに伴い，工場では，データを活用することでQCDを向上させる，スマートマニュファクチャリング化が進んでいる．このような情報化に伴い，サイバーリスクは増大し，製造に影響するサイバー攻撃による障害も増えてきている．生産を継続するために，製造部門のネットワークと装置・機器をサイバー攻撃から守り，それによってサイバーリスクを低減するための製造システムセキュリティは不可欠になっている．

Recently, the supply chain system has become flexible and dynamic, including the distribution and utilization of data. Along with that, smart manufacturing is progressing in factories, which uses data to improve QCD. With such computerization, cyber risks are increasing, and obstacles due to cyber-attacks affecting manufacturing are also increasing. In order to continue production, manufacturing system security is indispensable to protect the network and equipment/devices of the manufacturing department and to respond to cyber-attacks and cyber risks.

1. 当社のモノづくり

当社の工場は，国内に122拠点 海外には中国・アジアを中心に190拠点，合わせて312の工場がある．そこでは，大物から小型デバイスまで，また大量生産から多品種少量生産までさまざまな生産形態を持っている．事業セグメント別では従来の家電アプライアンス中心の姿から，家電アプライアンスが約1/4，それ以外の住宅や車載，部品，システムが3/4を占めており，大きく姿を変えてきている．地域別売り上げでは日本国内と海外がほぼ半々となっている．

当社は，情報技術を使い『スマートマニュファクチャリング』を構築することを目指しており，既にトレーサビリティや工場の見える化などの情報通信技術を活用した取り組みが始まっている．加えてさらなるQCD（Quality，Cost，Delivery）の総称の飛躍的向上を目指してIoT，ビッグデータ，AIを活用してマスカスタマイゼーションやゼロディフェクトモノづくりの実現を目指している．

2. 製造システムセキュリティの位置づけ

当社のモノづくりの活動基盤の強化の一環として，モノづくりの基礎体力と筆者らが呼んでいる現場力・人材育成・製造情報基盤の強化が必要である．特に工場に展開するIoT，ビッグデータ，AIを活用したアプリケーションやソリューションでは他の機器やサーバとネットワークを通して連携した，デジタライゼーションによる進化において，個々の構成要素間の通信を維持することは，必須の課題である．製造システムセキュリティの取り組みもこの考えで進めている．

* マニュファクチャリングイノベーション本部
全社モノづくり統括室
Corporate Manufacturing Management Office,
Manufacturing Innovation Div.

3. 製造システムセキュリティの取り組み

工場がサイバー攻撃を受けると生産の停止や品質・歩留まりの低下など経営に影響する障害が発生する．

BCPの視点からは，サイバー攻撃を受けても生産稼動・品質確保が必要である．

また，お客様要請として，情報通信技術を活用した生産性･信頼性向上の取り組みを積極的に実施していくことが必要である．

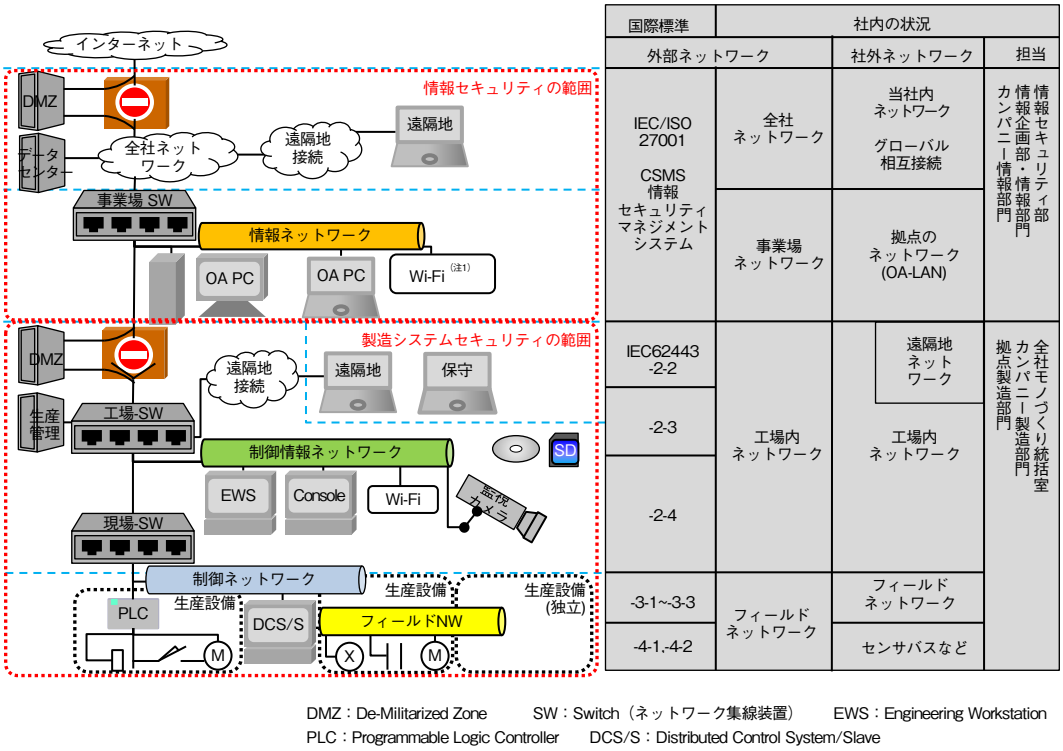
結果として，お客様から信頼される会社であるために，安定したモノづくりを支える製造システムのサイバーセキュリティ対策は不可欠である．

3.1 具体的取り組み

当社は情報セキュリティには，積極的に取り組んでおり，既に全社体制が確立され，製品そのもののセキュリティの確保の取り組みも進んでいる．

そこで，製造システムセキュリティとして他の取り組みで対象となっていないイントラネットと工場の接点，インターネットと工場の接点から内側の工場ネットワークおよびそれに接続されているアプリケーション・システム・機器・働いている人を対象とする．**第1図**に工場でのサイバーセキュリティの取り組み範囲を産業用自動制御システム（IACS: Industrial Automated Control System）の汎用国際標準であるIEC62443の枠組みで示す．

ここでは，工場内情報，制御ネットワークからフィールドネットワークまでのマネジメントレベルからセンサや測定器などのフィールドレベルまでを対象としている．



DMZ：De-Militarized Zone　SW：Switch（ネットワーク集線装置）　EWS：Engineering Workstation
PLC：Programmable Logic Controller　DCS/S：Distributed Control System/Slave

第1図　取り組み範囲
Fig. 1　Scope of activity

まず，工場に適した製造システムセキュリティ対策を確立し，それを，工場として必要なベースラインとして以下のガイドラインにまとめた．

1. 侵入防止ガイドライン
2. 異常検知ガイドライン
3. インシデント対応ガイドライン

推進人材の教育・訓練を行いつつグローバル全拠点へ製造セキュリティの取り組みの推進を行い全拠点で必要なBCPを策定する．これについては，ガイドラインに沿い，3つのステップで進めている．

第1ステップは，工場へのウイルスやマルウェアの侵入・持ち込み防止を徹底する．

第2ステップは，異常検知システムの開発．人手に頼る，手順やガイドラインでは，抜け漏れがあることを前提とし，多重防御すべく，工場で発生した異常を検知できる仕組みを導入する．

第3ステップは，異常検知後，速やかにインシデント対応ができる手順の作成，体制の構築と人材の育成を行う．

ウイルス・マルウェアの侵入防止に関しては，既存の技術情報の漏洩（ろうえい）防止のガイドラインをもとに，スマート工場としての変化点を踏まえて，新たなネットワーク接続や機器に対応すべく進化させた．異常を検知できる仕組みは，工場に適したものがなく，2016年から社内の8製造拠点で工場内ネットワークの通信を収集し，異常検知の仕組みを検証し，異常検知システムの開発に着手した．

3.2　異常検知システムの開発

本開発にあたり，2つの機能が必要であった．

1つは，端末情報の取得対応である．工場では物理構成や配線・機器配置・製造システムなど，多くの装置が工場内ネットワークに接続されていている．これを情報基盤全体として整理し対応する必要があった．

2つ目に，異常検知機能である．工場のネットワーク内の通信データから通信状況を監視することにより，異常が検知できるかを開発，検証する必要があった．

〔1〕端末情報の取得

実際にネットワークへ接続されている端末の情報や　ネットワークの接続構成はインシデントに対応する場合，最新かつ正確な情報が不可欠である．特定の検知対象セグメントの端末の基本情報と接続情報を定期的に収集して，ネットワークや機器の見える化を行った．

〔2〕異常検知機能

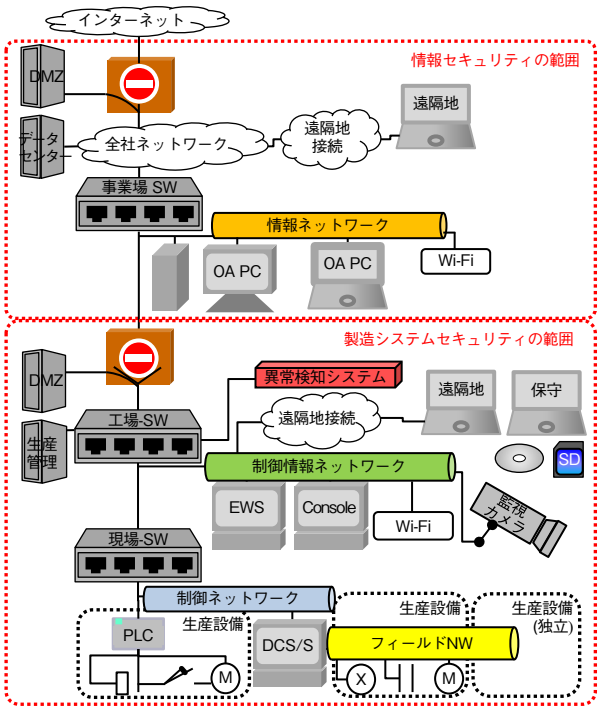
スイッチングハブを流れる通信をハブのミラー機能で取得・分析する仕組みを構築した．

（注1）Wi-Fi Allianceの登録商標．

ほとんどの場合，ウイルス・マルウェアは情報ネットワークから侵入してくる．そこで**第2図**に示すように工場-SWのミラー信号を異常検知システムで監視する．

特に，既存の製造装置，ネットワークの変更，影響を最小化し，異常検知システムを導入できるようにした．

サイバー攻撃を検知した場合，検知内容だけでなく，時間をさかのぼって，前後の通信を詳細に分析できるように，日常の通信の生データを蓄積する仕組みも併せて提供する．**第2図**は一般的な工場のネットワークにおける異常検知システムの位置づけである．



第2図　異常検知システムの位置づけ
Fig. 2　Location of the anomaly detection system

ネットワーク分析装置は，侵入検知システム(IDS: Intrusion Detection System)，通信データ蓄積機能，通信分析機能で構成する．

侵入検知システムは，ネットワーク内の通信から既知のマルウェアの攻撃パターンに一致した場合に異常として検知する．従来のアンチウイルスでは検知しにくい，侵入の兆しであるネットワーク走査や脆弱（ぜいじゃく）性チェックも検出しており，有効な予兆保全策であることも検証できた．

また，IEC62443などの新しい標準化に取り組むなかで，脆弱性を検知・定量化する仕組みが必要であることがわかった．そのため，脆弱性を定量化し，複数の対策を提示，対策実施後，再度定量化することにより，リスクの低減を見える化している．この予防保全により，事前管理ができ製造拠点を強化できる．

定常監視機能は，これらの機能により検知したアラートを関係者へ通知し現場確認や判断を通知する．そのとき，異常検知装置は常時稼働監視している．

4. 製造システムセキュリティの応用と今後

製造システムセキュリティは，情報セキュリティ，製品セキュリティとも密接に関係している．また，これは，種々の製造装置やセンサ，端末など複雑なネットワークのなかでのサイバー攻撃に備えたシステムを構築しており，他の分野にも応用展開が可能である．ISO/SAE 21434は，情報セキュリティ，製品セキュリティ，製造システムセキュリティが関わる規格になっており，これを満足することが必要な商品，システムには，広く展開されるものと期待する．

参 考 文 献

[1] 藤井俊郎, “製造システムセキュリティの取り組み,” 富士通フォーラム, 東京, May 18, 2018 .
[2] Toshio. Fujii, “Manufacturing System Security at Panasonic,” Digital Manufacturing Summit 2018, Seoul, May 30, 2018.
[3] 平本琢士, “パナソニックが取り組む工場セキュリティ対策,” 制御システムセキュリティーセミナー, 大阪, Jan. 24, 2020.
[4] 寺澤弘泰, “パナソニックの工場セキュリティソリューション,” 制御システムセキュリティーセミナー, 大阪, Jan. 24, 2020.