

経済産業省 御中

**スマートファクトリーにおける  
サイバーセキュリティ確保に向けた調査  
報告書**

---

2021 年 3 月 26 日

 **株式会社三菱総合研究所**

デジタル・イノベーション本部

## 目次

|                                                    |           |
|----------------------------------------------------|-----------|
| <b>1. 背景・目的 .....</b>                              | <b>2</b>  |
| 1.1 背景 .....                                       | 2         |
| 1.2 目的 .....                                       | 2         |
| <b>2. 国内外の製造現場におけるサイバーセキュリティ動向に関する調査.....</b>      | <b>3</b>  |
| 2.1 調査方法 .....                                     | 3         |
| 2.2 調査結果.....                                      | 3         |
| <b>3. スマートファクトリーにおけるサイバーセキュリティガイドライン策定に向けた調査..</b> | <b>30</b> |
| 3.1 調査方法.....                                      | 30        |
| 3.2 ヒアリング結果まとめ .....                               | 30        |

## 図目次

|       |                                 |    |
|-------|---------------------------------|----|
| 図 2-1 | 調査フロー .....                     | 3  |
| 図 2-2 | スマートファクトリーの分類 .....             | 4  |
| 図 2-3 | データ利活用の目的とユースケース分類 .....        | 4  |
| 図 2-4 | スマートファクトリーにおけるシステムモデル.....      | 12 |
| 図 2-5 | データの接続に着目したシステムモデル .....        | 13 |
| 図 2-6 | データ分析に着目したシステムモデル .....         | 13 |
| 図 2-7 | 制御システムに対するアクセスに着目したシステムモデル..... | 14 |
| 図 2-8 | スマートファクトリーにおけるステークホルダー.....     | 19 |
| 図 2-9 | スマートファクトリーにおけるセキュリティの特徴.....    | 29 |

## 表 目 次

|        |                                                                                                                 |    |
|--------|-----------------------------------------------------------------------------------------------------------------|----|
| 表 2-1  | スマートファクトリー事例とユースケース分類の対応.....                                                                                   | 5  |
| 表 2-2  | スマートファクトリー事例 .....                                                                                              | 6  |
| 表 2-3  | スマートファクトリーで利活用されるデータ分類.....                                                                                     | 9  |
| 表 2-4  | スマートファクトリー事例とデータ分類の対応.....                                                                                      | 9  |
| 表 2-5  | スマートファクトリーで利活用されるデータごとのリスク .....                                                                                | 10 |
| 表 2-6  | 脅威とセキュリティ対策 .....                                                                                               | 14 |
| 表 2-7  | セキュリティ対策事例 .....                                                                                                | 15 |
| 表 2-8  | システムモデルにおいて必要なセキュリティ対策例と期待される技術.....                                                                            | 17 |
| 表 2-9  | サイバーセキュリティ確保に向けてニーズが高まる技術例.....                                                                                 | 18 |
| 表 2-10 | 調査対象規格 .....                                                                                                    | 21 |
| 表 2-11 | Industrial Internet Security Framework (IIC).....                                                               | 22 |
| 表 2-12 | NIST (NIST IR 8183 Revision1) .....                                                                             | 22 |
| 表 2-13 | Report: AIOTI Working Group 4-Policy(AIOTI).....                                                                | 23 |
| 表 2-14 | Baseline Security Recommendations for IoT (ENISA) .....                                                         | 24 |
| 表 2-15 | ENISA Good Practices for Security of Internet of Things in the<br>context of Smart Manufacturing.....           | 24 |
| 表 2-16 | Recommendations for implementing the strategic initiative INDUSTRIE<br>4.0 .....                                | 25 |
| 表 2-17 | Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform<br>Industrie 4.0 BITKOM、VDMA、ZVEI.....          | 26 |
| 表 2-18 | Security in Automation -Profilierung von IT-Sicherheitsstandards für<br>den Maschinen- und Anlagenbau VDMA..... | 27 |
| 表 2-19 | Industrie 4.0 : Industrial Security 4.0 als gemeinschaftliche Aufgabe<br>ZVEI .....                             | 27 |
| 表 2-20 | IEC62443 シリーズ .....                                                                                             | 28 |
| 表 3-1  | ヒアリング対象者 .....                                                                                                  | 30 |

## 用語集・略語集

本報告書では、以下のとおり用語を定義する。

| 用語     | 概要                                                                |
|--------|-------------------------------------------------------------------|
| EWS    | Engineering WorkStation エンジニアリング機能を搭載したワークステーション                  |
| FW     | Firewall 異なるネットワークの境界に設置し、通過すべき通信とそうでない通信を分ける機器                   |
| HMI    | Human Machine Interface 人と機械が情報をやりとりするための手段                       |
| LAN    | Local Area Network 施設内で用いられるネットワーク                                |
| MES    | Manufacturing Execution System 製造実行システム<br>工場の生産ラインと情報システムを連携するもの |
| OPC    | 産業オートメーション分野等における、安全で信頼性あるデータ交換を目的とした相互運用を行うための標準規格               |
| PLC    | Programmable Logic Control シーケンス制御を行う機器                           |
| SCADA  | Supervisory Control And Data Acquisition システム監視及びプロセス制御           |
| インシデント | 事業運営に影響を与えたり、セキュリティを脅かしたりする事件や事故                                  |
| マルウェア  | 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコード                            |
| 脆弱性    | ソフトウェア等におけるセキュリティ上の弱点                                             |

## 1. 背景・目的

### 1.1 背景

我が国では、サイバー空間とフィジカル空間を高度に融合させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的发展と社会的課題の解決を両立する超スマート社会「Society5.0」の実現を提唱している。

「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを構成することが可能である一方、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要となる。

工場分野の制御システムは、内部ネットワークとして、インターネットには曝されないことを前提に設計されてきた。他方、IoT化や自動化の流れの中でスマートファクトリーへの注目が高まり、個別の機械やデバイスの稼働データを取るために、末端の機器がネットワークにつながることで、新たなセキュリティ上のリスク源になり得る。そのため、サイバーセキュリティ対策について特別な対応が求められると考えられる。

### 1.2 目的

本事業では、製造現場でのサイバーセキュリティ対策を検討するために、国内外の工場セキュリティ対策の動向について調査を行うとともに、工場に必要なサイバーセキュリティ対策を実際に実施していくために有用なガイドラインの策定に向け、国内の企業や業界団体、有識者にヒアリングを行い、その結果をとりまとめることを目的とする。

## 2. 国内外の製造現場におけるサイバーセキュリティ動向に関する調査

### 2.1 調査方法

スマートファクトリーに関する製品・サービスを提供するベンダー、及びユーザー企業の事例に関する資料や、政府・業界団体等のスマートファクトリーが目指す姿等に関する資料を元に、国内外におけるスマートファクトリーの事例におけるシステム構成及びデータ利活用のシナリオを調査した。

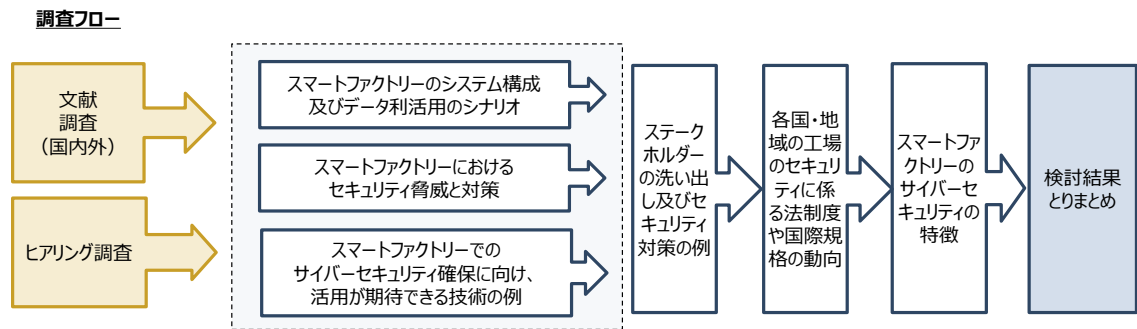


図 2-1 調査フロー

### 2.2 調査結果

国内外におけるスマートファクトリーの事例におけるシステム構成及びデータ利活用のシナリオを調査した。

#### 2.2.1 スマートファクトリーにおけるデータ利活用のシナリオやセキュリティ対策に関する調査

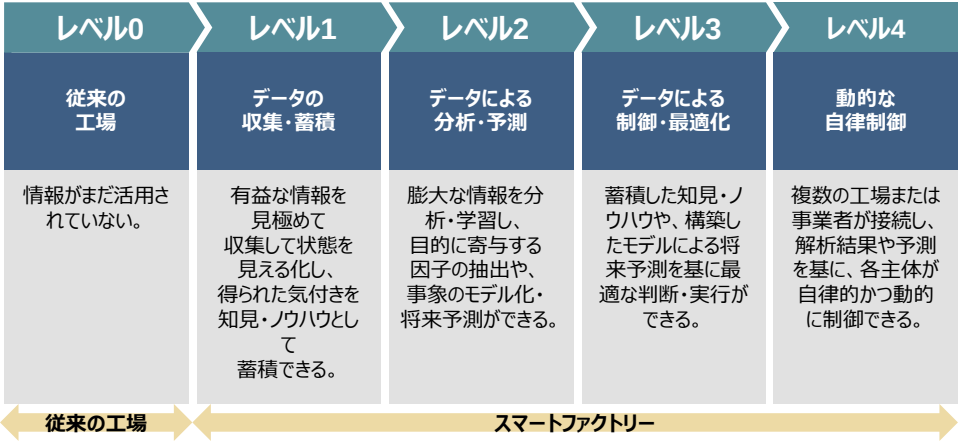
##### (1) データ利活用の目的とユースケース分類

はじめに、本調査では、スマートファクトリーを以下のような範囲で考える。

ドイツの「インダストリー4.0 実現戦略」では、インダストリー4.0 は「製品のライフサイクルを通じて価値連鎖全体の組織と制御が新たなる段階に入ることを意味する。このサイクルは個別化の進む顧客の要望に対応するもので、アイデア段階から開発および製造の指示、製品の末端顧客への納品、果てはリサイクリングまですべての段階を指し、それに関連するサービスも含む。」とされている。

しかし、「インダストリー4.0」はまだ実現されておらず、特に日本においては多くの製造業においてようやくデータの利活用が始まりつつある状況である。スマートファクトリーのセキュリティを検討するにあたり、将来的に目指す姿を念頭に置くことは重要であるが、データの利活用を開始したばかりの工場から、ある程度活用が進む工場まで考慮する必要がある。

そこで、データの活用度合いに応じて、複数の段階があることを想定した上で、スマートファクトリーのセキュリティを検討した。



資料：経済産業省中部経済産業局「スマートファクトリーロードマップ」（2017年5月）を基に作成

図 2-2 スマートファクトリーの分類

次に、スマートファクトリーの事例を調査し、スマートファクトリーにおけるデータ利活用の目的と、それぞれの目的に対応するユースケースを以下の7種類に分類した。

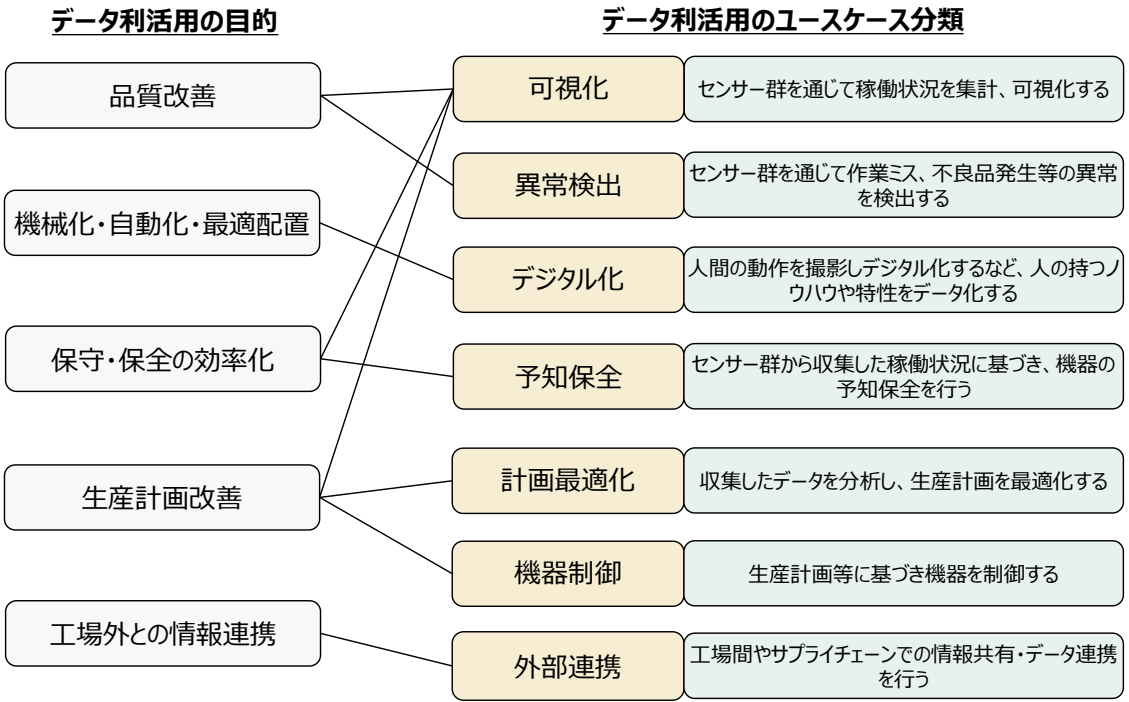


図 2-3 データ利活用の目的とユースケース分類

スマートファクトリーの事例とユースケース分類との対応を以下に示す。

表 2-1 スマートファクトリー事例とユースケース分類の対応

| 項番 | 事例タイトル                               | ユースケース分類 |      |       |      |      |      |      |
|----|--------------------------------------|----------|------|-------|------|------|------|------|
|    |                                      | 可視化      | 異常検出 | デジタル化 | 予知保全 | 生産計画 | 機器制御 | 外部連携 |
| 1  | 工場内 IoT プラットフォームの構築によるデータの集約と生産最適化   | ○        |      |       |      | ○    |      |      |
| 2  | パブリッククラウドによる工場間ネットワーク                |          |      |       |      |      |      | ○    |
| 3  | クラウドからの産業機器・制御機器の遠隔診断保守              |          |      |       | ○    |      |      |      |
| 4  | 産業機器・制御機器のインテリジェント化                  |          |      |       |      |      | ○    |      |
| 5  | FA 機器と IT の融合                        |          |      |       |      |      |      | ○    |
| 6  | 工場内のネットワーク化                          | ○        |      |       |      |      |      |      |
| 7  | 工場ネットワークの階層                          |          |      |       |      |      |      | ○    |
| 8  | Windows 環境と EtherCAT                 |          |      |       | ○    | ○    |      |      |
| 9  | 産業機器・制御機器のインテリジェント化                  | ○        |      |       | ○    | ○    |      |      |
| 10 | 製造現場のデータ収集と仮想でのビッグデータ解析の融合           |          |      |       | ○    |      |      |      |
| 11 | スマートファクトリーを実現                        | ○        |      |       |      |      |      |      |
| 12 | Lumada（進捗・稼働監視システム）                  | ○        |      |       |      | ○    |      |      |
| 13 | 工場インフラの課題を解決                         |          |      |       |      |      |      | ○    |
| 14 | データ収集、フォグコンピューティング、クラウドソリューションまでサポート | ○        |      |       |      |      |      |      |
| 15 | 課題の早期解決に向けて、より最適な見える化・分析をクイックにサポート   | ○        |      |       |      |      |      |      |
| 16 | 作業状況データの利活用                          | ○        | ○    |       |      |      |      |      |
| 17 | 製造機器エネルギー使用データの利活用                   | ○        | ○    |       |      |      |      |      |
| 18 | 生産設備動作データの利活用                        |          |      | ○     |      |      |      |      |
| 19 | 従業員データの利活用                           |          |      | ○     |      |      |      |      |
| 20 | 工作機械稼働データの利活用                        |          |      |       |      |      | ○    |      |
| 21 | 工作機械稼働データの利活用                        | ○        |      |       |      |      |      |      |
| 22 | 生産設備稼働データの利活用                        | ○        |      |       | ○    |      |      |      |
| 23 | 工作機械の実稼働データの利活用                      | ○        |      |       |      |      |      |      |
| 24 | 工作機械の実稼働データの利活用                      | ○        |      |       | ○    |      |      |      |

## (2) スマートファクトリー事例

スマートファクトリーの実例の詳細は以下の通りに整理した。

表 2-2 スマートファクトリー事例

| 項番 | 事例タイトル                             | 内容                                                                                                                                                                           | 参考 URL 等                                                                                                                                            |
|----|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 工場内 IoT プラットフォームの構築によるデータの集約と生産最適化 | 富士フイルムテクノプロダクツは、作業員から得られる生産データを中心として、AGV を用いた搬送システムや設備データなどを 1 つのプラットフォームに集約して活用するための体制を構築した。                                                                                | <a href="https://monoist.atmarkit.co.jp/mn/articles/2001/21/news002.html">https://monoist.atmarkit.co.jp/mn/articles/2001/21/news002.html</a>       |
| 2  | パブリッククラウドによる工場間ネットワーク              | デンソーは、同社が世界に展開する約 130 の工場を IT と IoT でつなぐ「Factory-IoT プラットフォーム」を開発したと発表した。Factory-IoT プラットフォームにより、工場のさまざまな機器から収集したデータを 1 つのクラウドに蓄積し、自由な活用を目指す。                                | <a href="https://www.denso.co.jp/ja/news/newsroom/2020/20201005-01/">https://www.denso.co.jp/ja/news/newsroom/2020/20201005-01/</a>                 |
| 3  | クラウドからの産業機器・制御機器の遠隔診断保守            | ヤマザキマザックは、ビフォアサービスからアフターサービスまでのすべてを「Mazak iCONNECT」として統合、さらに最新の IoT を活用して、お客さまと工作機械、そしてマザックのサポートセンタとをつなぐコネクティッドサービスを進化・拡充させて提供開始した。                                          | <a href="https://www.denso.co.jp/ja/news/newsroom/2020/20201005-01/">https://www.denso.co.jp/ja/news/newsroom/2020/20201005-01/</a>                 |
| 4  | 産業機器・制御機器のインテリジェント化                | DMG 森精機は、工作機械の加工中に発生する切りくずを AI を用いて自動で除去する「AI チップリムーバル」を開発した。横形マシニングセンタに搭載し、AI を用いて切りくずの堆積状況进行分析し、切りくずを自動で効率的に除去する。                                                          | <a href="https://www.dmgmori.co.jp/corporate/news/pdf/20201026_aichip.pdf">https://www.dmgmori.co.jp/corporate/news/pdf/20201026_aichip.pdf</a>     |
| 5  | FA 機器と IT の融合                      | 三菱電機は、産業用オープンネットワーク「CC-Link IE TSN」に対応する FA 製品を開発する。CC-Link IE TSN 対応の FA 製品により、リアルタイム性が必要な制御通信と、上位 IT システムとの情報通信が、同一の Ethernet ケーブル上で混在しても定時性を確保し、自由度の高いシステムを容易に構築できるようになる。 | <a href="https://iot.aperza.com/2018/12/2882/">https://iot.aperza.com/2018/12/2882/</a>                                                             |
| 6  | 工場内のネットワーク化                        | 生産部門のための工場ネットワークの管理を支援するのが、産業ネットワーク専用可視化管理ツール「Cisco IND」である。製造設備ネットワーク管理を直感的にする。                                                                                             | <a href="https://monoist.atmarkit.co.jp/mn/articles/1904/01/news007.html">https://monoist.atmarkit.co.jp/mn/articles/1904/01/news007.html</a>       |
| 7  | 工場ネットワークの階層                        | 工場の製造ラインや設備で利用するネットワークは、大きく 3 つの階層に分けられる。上から「制御情報ネットワーク」、「コントローラー間ネットワーク」、「フィールドネットワーク」に分けて考えている。                                                                            | <a href="https://businessnetwork.jp/Detail/tabid/65/artid/5543/Default.aspx">https://businessnetwork.jp/Detail/tabid/65/artid/5543/Default.aspx</a> |
| 8  | Windows 環境と EtherCAT               | windows 環境で、情報システムから設備までシームレスに接続し、データ解析し、生産効率向上、予兆検知を実現する。                                                                                                                   | <a href="https://www.sbbt.jp/article/cont1/33221">https://www.sbbt.jp/article/cont1/33221</a>                                                       |
| 9  | 産業機器・制御機器のインテリジェント化                | IBM Cognitive Manufacturing ソリューションは 4 つに分類される。第一が生産管理システムを、IoT によるリアルタイムデータ収集で、生産プロ                                                                                         | <a href="https://www.ibm.com/jp-ja/industries/indus">https://www.ibm.com/jp-ja/industries/indus</a>                                                 |

| 項番 | 事例タイトル                               | 内容                                                                                                                                                                    | 参考 URL 等                                                                                                                                                                            |
|----|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                      | セスを効果的に支援する仕組み。第二は、システム上に、仮想の工場オペレーションを見える化し、製品品質や設備保全の予知を行う仕組み。第三は AI で、音声や画像を分析し生産現場の作業を支援する仕組み。そして、第四が現実の生産現場の作業情報をリアルタイムにデータを収集する IT 基盤。                          | <a href="http://trial/industry-4-0">trial/industry-4-0</a>                                                                                                                          |
| 10 | 製造現場のデータ収集と仮想でのビッグデータ解析の融合           | 日立産業制御ソリューションズは、現場データの解析ツール/解析手法の適用と産業システム SE による解析エンジニアリングサービスを提供する。ビッグデータ解析により得られた品質影響パラメータ（診断モデル）を、実行システムとして開発し、設備予兆診断/品質兆候検知システムを構築する。                            | <a href="https://info.hitachi-ics.co.jp/product/sigma/index.html">https://info.hitachi-ics.co.jp/product/sigma/index.html</a>                                                       |
| 11 | スマートファクトリーを実現                        | ヤマザキマザックは、工場内の IoT 化を図る上で重要な機械間のデータ取得の共通化やサイバーセキュリティの問題を解決するために、製造業向けオープン通信規格「MTConnect®(MT コネクト)」を採用したネットワーク接続装置を開発した。付属のセンサーを用いて設備機の状態を感知し、収集したデータを SMARTBOX に転送する。 | <a href="https://www.mazak.jp/machines/technology/factory-network/ismart-factory/#sensorbox">https://www.mazak.jp/machines/technology/factory-network/ismart-factory/#sensorbox</a> |
| 12 | Lumada（進捗・稼働監視システム）                  | 日立製作所は、製造実績情報から各作業の能力過不足や進捗をひと目で分かるよう可視化し、工程遅延を防止する。人員を含めた生産リソースの最適配置など、納期遅延へのタイムリーな対策・改善を促進する。                                                                       | <a href="http://www.hitachi.co.jp/products/it/lumada/solution/lumada_s_010036.html">http://www.hitachi.co.jp/products/it/lumada/solution/lumada_s_010036.html</a>                   |
| 13 | 工場インフラの課題を解決                         | 富士通は、工場ネットワークの現状課題を踏まえ、お客様の考えるネットワーク実現に向けて、要件にあった機器選定やネットワーク設計および構築する。場内ネットワークを理解した専任者によるリスクの把握、迅速な異常検知・対処など、ネットワーク安定稼働の実現に向けた運用サービスを提供する。                            | <a href="https://www.fujitsu.com/jp/solutions/business-technology/iot/factory-iot/">https://www.fujitsu.com/jp/solutions/business-technology/iot/factory-iot/</a>                   |
| 14 | データ収集、フォグコンピューティング、クラウドソリューションまでサポート | マクニカは、データの収集、クレンジング、蓄積・活用・分析をすべてデジタル化する支援を行う。必要な部分だけをカスタムして利用することも、スマートファクトリー実現の土台となるシステムすべての導入も支援する。                                                                 | <a href="https://www.macnica.co.jp/business/ai-iot/solutions/datavisualization/">https://www.macnica.co.jp/business/ai-iot/solutions/datavisualization/</a>                         |
| 15 | 課題の早期解決に向けて、より最適な見える化・分析をクイックにサポート   | オムロンは、生産現場の様々な情報を時間同期して収集、現場と紐づけて見える化によって、早期の課題発見を支援する。課題解決のために、独自のノウハウで導き出したセンサーの取り付け位置を提案する。                                                                        | <a href="https://www.fa.omron.co.jp/solution/ibelt/service02/">https://www.fa.omron.co.jp/solution/ibelt/service02/</a>                                                             |
| 16 | 作業状況データの利活用                          | 日立アプライアンスは、3 人一组で組み立てを行うセル生産で、各作業者の動きや部品の流れをセンサーでつかむ。作業手順にミスがあると、センサーが感知して、リアルタイムに警告音とモニターで作業者に知らせる。また、センサーで作業スピードを計測し、作業者の作業スピードが近い人を同じ組に配置することで、1 日の総生産台数を増やしている。   | <a href="https://www.youtube.com/watch?v=hETltJHFneo">https://www.youtube.com/watch?v=hETltJHFneo</a>                                                                               |
| 17 | 製造機器エネルギー使用データの利活用                   | ハリマ化成グループは、攪拌機や冷却ポンプ等の製造機器でどれくらいのエネルギー（電力量や排水 ph 等）が使われているかをリアルタイムに吸い上げて、シーケンサーで収集し、表示器（ダッ                                                                            | <a href="https://www.mitsubishielectric.co.jp/faq/compass/casestudies/custom/ccase40/i">https://www.mitsubishielectric.co.jp/faq/compass/casestudies/custom/ccase40/i</a>           |

| 項番 | 事例タイトル          | 内容                                                                                                                                                                                                                                   | 参考 URL 等                                                                                                                                                                                |
|----|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                 | シュボード) で確認する。これらにより、エネルギーの削減と共に設備異常の早期発見にもつながり、設備保全や安全にも繋がっている。                                                                                                                                                                      | <a href="#">ndex.html</a>                                                                                                                                                               |
| 18 | 生産設備動作データの利活用   | 長島鋳物は、シーケンサー等から取得できる各生産設備の動作データ等を生産管理上の注文情報等と紐付けることで、情報を一元管理する仕組みを開発した。蓄積したデータを分析することで、例えば、「この製品であれば、この温度で製造しなければならない」等の熟練作業者の経験知をデータから導くことができるようになった。これにより、製造の自動化をしても、継続的な製品品質を確保することができている。                                        | <a href="https://www.meti.go.jp/meti_lib/report/H28FY/000279.pdf">https://www.meti.go.jp/meti_lib/report/H28FY/000279.pdf</a>                                                           |
| 19 | 従業員データの利活用      | 今橋製作所は、従業員の思考力やストレス耐性等のパーソナルデータに基づいて、適材適所に配置して、モチベーションと生産性を高めている。<br>(配置の例)<br><ul style="list-style-type: none"> <li>ロジック系が苦手な社員はルーチン系の仕事に就いて成果を挙げてもらおう。</li> <li>成功体験が少ない若手社員にはなるべく得意分野を担当させ、成功体験を積み重ねて自信を持たせる。</li> </ul>         | <a href="https://www.meti.go.jp/report/whitepaper/mono/2018/honbun_pdf/pdf/honbun01_01_02.pdf">https://www.meti.go.jp/report/whitepaper/mono/2018/honbun_pdf/pdf/honbun01_01_02.pdf</a> |
| 20 | 工作機械稼働データの利活用   | 小松製作所は、工作機械や溶接ロボットからデータを収集・分析し、機械の稼働時間を適正化したり、動作を効率化したりして生産性を高めている。例えば、切削プロセスのデータを集めると、切削スピードを上げられる部分があると分かり、工作機械を制御するプログラムを改善した。                                                                                                    | <a href="https://www.itmedia.co.jp/news/articles/1904/09/news001.html">https://www.itmedia.co.jp/news/articles/1904/09/news001.html</a>                                                 |
| 21 | 工作機械稼働データの利活用   | 大矢製作所は、摩擦圧接加工機から設定条件データ（製品No、名称、回転数、圧力制御条件）と一定間隔で収集した加工機実測データ（回転数、ヘッド位置、圧力、摩擦熱温度）を収集し、生産実績の見える化を実現した。                                                                                                                                | <a href="https://esg.teldevi.co.jp/iot/azure/case/case04.html">https://esg.teldevi.co.jp/iot/azure/case/case04.html</a>                                                                 |
| 22 | 生産設備稼働データの利活用   | オムロンは、生産設備の様々なデータやイベントログを取得し、生産設備の稼働状況を可視化している。可視化することで、生産設備の稼働におけるロスを発見している。                                                                                                                                                        | <a href="https://www.fa.omron.co.jp/product/special/sysmac/technology/kusatsu-report-1.html">https://www.fa.omron.co.jp/product/special/sysmac/technology/kusatsu-report-1.html</a>     |
| 23 | 工作機械の実稼働データの利活用 | 飯山精器株式会社は、Edgecross を用いたマルチベンダー環境（ファナック、三菱電機 NC 搭載加工機他）での実稼働データの収集を行っている。既存の稼働管理システムおよび生産管理システムとの連携により段取り替えなどの効率化や先回り準備効率化を実現している。                                                                                                   | <a href="https://www.edgecross.org/ja/case/">https://www.edgecross.org/ja/case/</a>                                                                                                     |
| 24 | 工作機械の実稼働データの利活用 | 名張ホールディングスは、設備の任意の箇所に IoT センサーを設置することで、振動、温度、電流、気圧、湿度などのデータを収集できる。収集したデータは LAN ケーブル経由でデータの記録、蓄積用デバイスに送信し、JIP が開発したデータ分析アプリ「ParaReco Visualizer Lite」で処理を行う。データの内容から故障の予兆を検知した場合には、すぐに使用者に知らせる仕組みとなっており、大きな手間をかけずに生産設備の適切なメンテナンスが行える。 | <a href="https://silson.jp/product/pararecollectar/">https://silson.jp/product/pararecollectar/</a>                                                                                     |

### (3) データ分類

スマートファクトリーの事例を調査し、スマートファクトリーにおいて、利活用されるデータについて、一次データ及び各種加工データを以下の8種類に分類した。

表 2-3 スマートファクトリーで利活用されるデータ分類

| データ分類                      | データ概要                                    | 典型的なデータの流れ                                                                     |
|----------------------------|------------------------------------------|--------------------------------------------------------------------------------|
| センサーデータ<br>(センサー)          | 機器や組立等のリアルタイムの状態を各種センサーで取得したデータ。         | フィールド内のセンサーで取得され、フィールド系 NW、制御系 NW またはそれ以外のネットワーク経路を通じて情報系 NW やクラウド等に送られる。      |
| 静止画データ<br>(静止画)            | 機器や組立等の状況を静止画で取得したデータ。                   | フィールド内のカメラで撮影され、フィールド系 NW、制御系 NW 以外のネットワーク経路あるいは記憶媒体を通じて情報系 NW やクラウド等に送られる。    |
| 動画データ<br>(動画)              | 機器や組立等の状況を動画で取得したデータ。                    | フィールド内のビデオカメラで撮影され、フィールド系 NW、制御系 NW 以外のネットワーク経路あるいは記憶媒体を通じて情報系 NW やクラウド等に送られる。 |
| 制御コマンド<br>(制御 CMD)         | 制御の状態を変更するために、送られる命令や指示値。                | HMI から入力され、または MES からゲートウェイを通じて PLC 等のコントローラーに送られる。                            |
| エンジニアリング<br>設定<br>(ENG 設定) | 制御のためのレシピ等各種の制御値を調整するためのプログラムやデータ。       | EWS で作成され、PLC 等のコントローラーに送られる。                                                  |
| 機器状態値<br>(機器状態)            | 機器や組立等のリアルタイムの内部状態を表すデータ。                | フィールド内の機器で生成され、インターネットや専用線等を通じて保守サービスプロバイダ等に送られる。                              |
| 生産計画値<br>(生産計画)            | 生産計画を表す日程、生産能力、在庫等の諸データ。                 | MES で作成され、保持される。                                                               |
| 集計分析データ<br>(集計分析)          | 収集したデータを人間が理解しやすいよう集計・加工・分析・可視化するなどしたもの。 | 制御情報系 NW、情報系 NW、クラウド等で生成され、各種端末で参照される。                                         |

スマートファクトリーの事例とデータ分類との対応を以下に示す。

表 2-4 スマートファクトリー事例とデータ分類の対応

| 項番 | 事例タイトル                             | データ分類 |     |    |        |        |      |      |      |     |
|----|------------------------------------|-------|-----|----|--------|--------|------|------|------|-----|
|    |                                    | センサー  | 静止画 | 動画 | 制御 CMD | ENG 設定 | 機器状態 | 生産計画 | 集計分析 | その他 |
| 1  | 工場内 IoT プラットフォームの構築によるデータの集約と生産最適化 | ○     |     |    |        |        |      | ○    | ○    |     |
| 2  | パブリッククラウドによる工場間ネットワーク              | ○     |     |    |        |        |      |      | ○    |     |
| 3  | クラウドからの産業機器・制御機器の遠隔診断保守            |       |     |    |        |        | ○    |      |      |     |

| 項番 | 事例タイトル                                   | データ分類 |     |    |       |       |      |      |      |     |
|----|------------------------------------------|-------|-----|----|-------|-------|------|------|------|-----|
|    |                                          | センサー  | 静止画 | 動画 | 制御CMD | PLC設定 | 機器状態 | 生産計画 | 集計分析 | その他 |
| 4  | 産業機器・制御機器のインテリジェント化                      |       | ○   | ○  |       |       |      |      |      |     |
| 5  | FA 機器と IT の融合                            |       |     |    |       |       |      |      |      | ○   |
| 6  | 工場内のネットワーク化                              |       |     |    |       |       |      |      | ○    |     |
| 7  | 工場ネットワークの階層                              |       |     |    |       |       |      |      |      | ○   |
| 8  | Windows 環境と EtherCAT                     |       |     |    |       |       |      | ○    | ○    |     |
| 9  | 産業機器・制御機器のインテリジェント化                      | ○     |     |    | ○     |       |      | ○    | ○    |     |
| 10 | 製造現場のデータ収集と<br>仮想でのビッグデータ解析の融合           | ○     |     | ○  |       |       |      | ○    | ○    |     |
| 11 | スマートファクトリーを実現                            | ○     |     |    |       |       |      |      | ○    |     |
| 12 | Lumada（進捗・稼働監視システム）                      | ○     |     | ○  |       |       |      | ○    | ○    |     |
| 13 | 工場インフラの課題を解決                             | ○     |     |    |       |       |      |      |      | ○   |
| 14 | データ収集、フォグコンピューティング、ク<br>ラウドソリューションまでサポート | ○     |     |    |       |       |      |      | ○    |     |
| 15 | 課題の早期解決に向けて、より最適な見える<br>化・分析をクイックにサポート   | ○     | ○   | ○  |       |       |      |      | ○    |     |
| 16 | 作業状況データの利活用                              | ○     |     |    |       |       |      |      | ○    |     |
| 17 | 製造機器エネルギー使用データの利活用                       | ○     |     |    |       |       |      |      | ○    |     |
| 18 | 生産設備動作データの利活用                            | ○     |     |    |       |       | ○    |      | ○    |     |
| 19 | 従業員データの利活用                               |       |     |    |       |       |      |      |      | ○   |
| 20 | 工作機械稼働データの利活用                            | ○     |     |    |       | ○     | ○    |      |      |     |
| 21 | 工作機械稼働データの利活用                            | ○     |     |    |       |       | ○    |      | ○    |     |
| 22 | 生産設備稼働データの利活用                            |       |     |    |       |       | ○    |      | ○    |     |
| 23 | 工作機械の実稼働データの利活用                          |       |     |    |       |       | ○    |      | ○    |     |
| 24 | 工作機械の実稼働データの利活用                          | ○     |     |    |       |       |      |      | ○    |     |

#### (4) リスク

利活用されるデータ分類ごとに、データの窃取や改ざん等に伴うリスクを検討した。画像データについては、フィールド内の機器や組立等の機密が視覚的に漏洩するため、データを窃取されたときのリスクが比較的高いと考えられる。制御コマンドやエンジニアリング設定については、機器の正常な動作に支障をきたし可用性に影響を及ぼすおそれがあるため、データを改ざんされたときのリスクが比較的高いと考えられる。集計分析データ等についても、データの性質等によっては機密性がありリスクが高くなる場合もあり得る。データ分類ごとのリスクは以下の通りに整理した。

表 2-5 スマートファクトリーで利活用されるデータごとのリスク

| 利活用データ分類 | データの窃取・改ざん等のリスク                                                                 |
|----------|---------------------------------------------------------------------------------|
| センサーデータ  | 部分的な窃取ではフィールド内からの具体的な機密漏洩に至る可能性は低い。改ざんされた場合、情報が攪乱されるリスクはあるが、正常稼働に直接影響するおそれは少ない。 |
| 静止画データ   | 窃取された場合、フィールド内の機器や組立等の機密が（静止画情報という形                                             |

| 利活用データ分類       | データの窃取・改ざん等のリスク                                               |
|----------------|---------------------------------------------------------------|
|                | で) 漏洩する。                                                      |
| 動画データ          | 窃取された場合、フィールド内の機器や組立等の機密が（動画情報という形で）漏洩する。                     |
| 制御コマンド         | 改ざんされた場合、誤った制御情報により正常稼働できなくあるおそれがある。                          |
| エンジニアリング<br>設定 | 投入するプログラムへのマルウェア混入等により正常稼働できなくあるおそれがある。                       |
| 機器状態値          | 部分的な窃取ではフィールド内からの具体的な機密漏洩に至る可能性は低い<br>ため、リスクは比較的低い。           |
| 生産計画値          | 窃取された場合、生産計画という内部情報が漏洩するおそれがある。改ざん<br>された場合、情報の解釈を誤るおそれがある。   |
| 集計分析データ        | 窃取された場合、（情報処理後の）非公開情報が漏洩するおそれがある。改ざ<br>んされた場合、情報の解釈を誤るおそれがある。 |

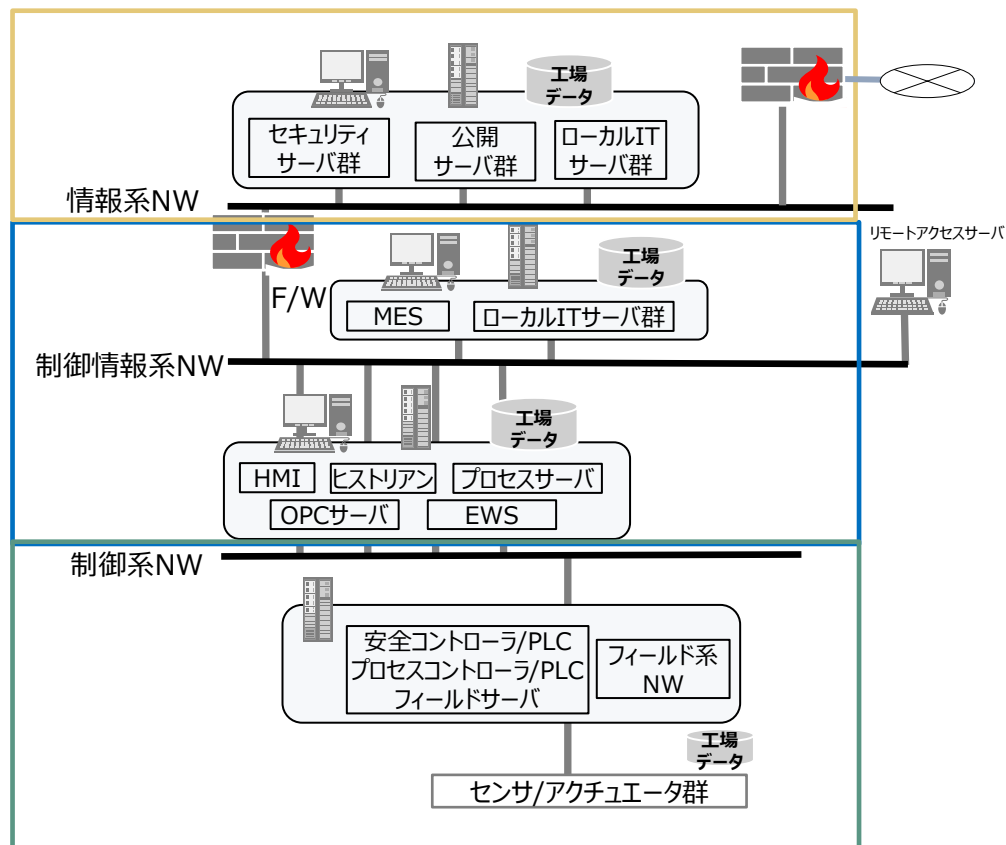
## 2.2.2 スマートファクトリーにおける主なシステムモデルの設定

スマートファクトリーの事例調査結果を踏まえて、スマートファクトリーにおける主なシステムモデルを設定した。

データの接続に着目した場合、「制御系 NW データ（工場内部データ）」「制御情報系 NW データ」「情報系 NW データ」が、それぞれ従来のクローズな工場システムでは接続していなかった、新たな接続先に接続することによるシステムモデルが設定できる。

データ分析に着目した場合、データ分析が「制御情報系 NW」「情報系 NW」に接続された機器、または「外部」のどこで分析されるかという観点でシステムモデルが設定できる。

制御システムに対するアクセスに着目した場合、コントローラー/PLC に接続する「制御情報系 NW」の EWS 等にインターネットで接続するモデルが設定できる。



※ 経済産業省・NEDO・三菱総合研究所  
「IoTセキュリティ対応マニュアル産業保安版（第2版）」を基にMRI作成

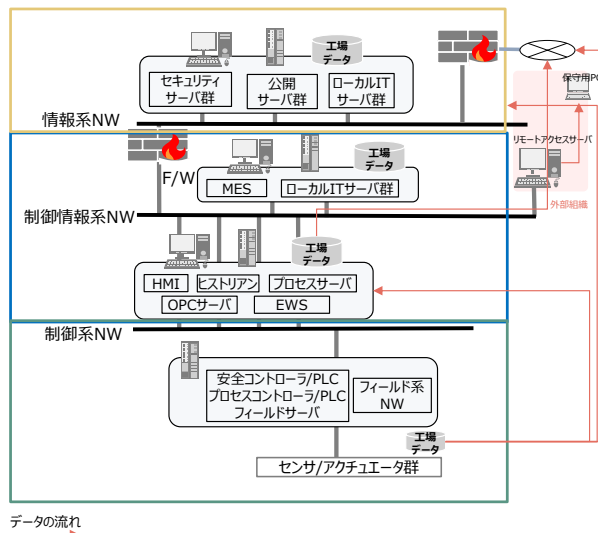
図 2-4 スマートファクトリーにおけるシステムモデル

### (1) 工場内部データの工場内外への接続

データの接続に着目した場合、スマートファクトリーは、特に工場現場にある「制御系NWデータ（工場内部データ）」の活用が進んでいる。

従来の工場では「制御系NW」「制御情報系NW」「情報系NW」が三層に分かれていたが、無線通信などにより、これらのネットワーク接続以外の経路により工場データが送受信される場合がある。

従来はそれぞれの境界で守ることができたが、このような接続の場合、ネットワーク境界だけで守るだけではなく、新たな接続点や接続回線におけるセキュリティ等に留意が必要となる。



<本システムモデルにおける利用シーンと接続形態>

【制御系NWデータ（工場内部データ）】

- センサーデータ  
機器のセンタデータが、Wi-Fiを通じて（有線も利用して）制御情報系NW、情報系NWに送信される。
- センサーデータ  
機器のセンタデータが、広域無線を通じて（有線も利用して）制御情報系NW、情報系NW、外部に送信される。
- 静止画データ  
タブレット等で撮影された静止画データが、Wi-Fiを通じて（有線も利用して）制御情報系NW、情報系NW、外部に送信される。
- 動画データ  
監視カメラ等で撮影された動画データが、有線NW（工場NWとは別NW）を通じて情報系NW、外部に送信される。

【制御情報系NWデータ（工場内部データ）】

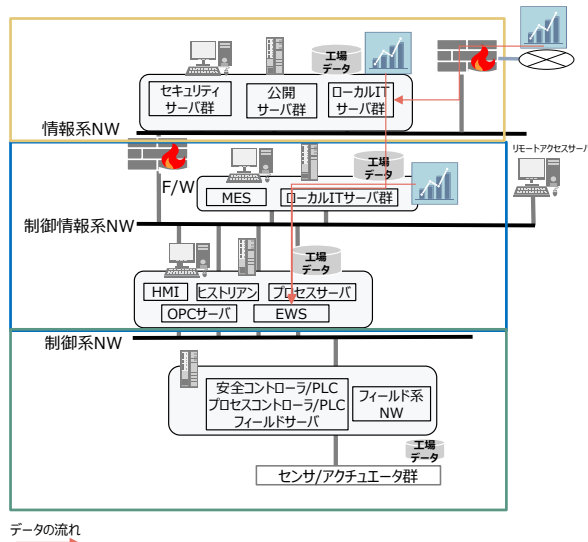
- センサーデータ  
制御情報系NWの機器に存在するセンタデータが、リモートアクセスサーバと専用線を通じて、外部（クラウド）に送信される。
- センサーデータ  
制御情報系NWの機器に存在するセンタデータが、リモートアクセスサーバに接続された保守用PCに送信される。

図 2-5 データの接続に着目したシステムモデル

## (2) 集計分析データの工場における活用

データ分析に着目した場合、データ分析が「制御情報系 NW」「情報系 NW」に接続された機器、または「外部」のどこで分析されるかという観点でシステムモデルが設定できる。

データ分析において外部を利用する場合は、外部接続及び外部保存（クラウド）のセキュリティに留意が必要である。AI 等の技術が用いられる場合、分析を行う機器において正しい分析がなされるか、制御に関係するデータが正しいか等のセキュリティ等に留意が必要となる。（ただし、リアルタイムかつ自動で制御を行うケースは見られない）



<本システムモデルにおける利用シーンと接続形態>

【外部】

- 集計分析データ  
集計分析データが生成され、情報系NWに送信される。  
情報系NWのサーバ等において、様々な分析に活用される。

【情報系NW】

- 集計分析データ  
集計分析データが生成され、集計分析データが利用された制御に関わるデータが、情報系NWを通じて、制御情報系の機器で利用される。  
（制御情報系NWの機器から、制御コマンドが制御系NWに送信される。）

【制御情報系NW】

- 集計分析データ  
集計分析データが生成され、集計分析データが利用された制御に関わるデータが、制御情報系NWの機器で利用される。  
（制御情報系NWの機器から、制御コマンドが制御系NWに送信される。）

図 2-6 データ分析に着目したシステムモデル

(3) リモートメンテナンス

制御システムに対するアクセスに着目した場合、コントローラ/PLC に接続する「制御情報系 NW」の EWS 等に、リモートメンテナンスのために外部から接続するモデルが設定できる。

リモートメンテナンスの接続先、リモートメンテナンス回線のセキュリティ等に配慮が必要となる。

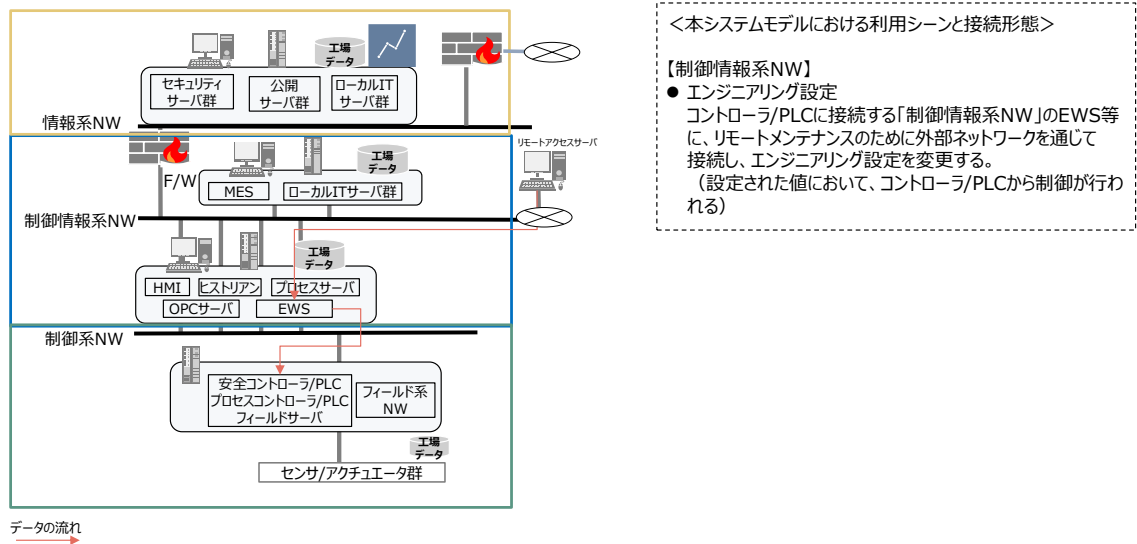


図 2-7 制御システムに対するアクセスに着目したシステムモデル

2.2.3 脅威とセキュリティ対策

(1) 脅威と対策

システムモデルにおいて想定される脅威と必要なセキュリティ対策例を以下の通り整理した。

表 2-6 脅威とセキュリティ対策

|                  | 想定される脅威                                                                                                                                                                                                                              | 必要なセキュリティ対策                                                                                                                                                    |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 工場内部データの工場内外への送信 | <ul style="list-style-type: none"><li>データを送受信するネットワークへの不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li><li>データを集約する機器への不正アクセスに基づくデータ改ざん、データ窃取等</li><li>クラウドに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li><li>外部事業者のなりすましによるデータ改ざん、データ窃取等</li></ul> | <ul style="list-style-type: none"><li>ネットワークへの不正侵入防止</li><li>機器の認証</li><li>リモートアクセスサーバや保守用PCの不正侵入防止</li><li>無線通信の認証、暗号化</li><li>セキュリティが確保されたクラウドサービス</li></ul> |

|                              | 想定される脅威                                                                                                                          | 必要なセキュリティ対策                                                                               |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
|                              |                                                                                                                                  | の利用<br>・ 接続先（人）の認証<br>・ データの妥当性検証                                                         |
| 集計分析<br>データの<br>工場にお<br>ける利用 | ・ 情報系ネットワークに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等<br>・ クラウドに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等<br>・ 外部事業者のなりすましによるデータ改ざん、データ窃取等 | ・ ネットワークへの不正侵入防止<br>・ セキュリティが確保されたクラウドサービスの利用<br>・ 接続先（人）の認証<br>・ データの妥当性検証<br>・ 分析の妥当性検証 |
| リモート<br>メンテナ<br>ンス           | ・ 外部ネットワークに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等<br>・ 外部事業者のなりすましによるデータ改ざん、データ窃取等                                                 | ・ ネットワークへの不正侵入防止<br>・ セキュリティが確保されたクラウドサービスの利用<br>・ 接続先（人）の認証<br>・ データの妥当性検証               |
| 全般                           | ・ デジタルデータ化・蓄積・集計等を行う各種サーバ（IT サーバ）のマルウェア感染<br>・ MES のマルウェア感染<br>・ EWS のマルウェア感染<br>・ OPC サーバーのマルウェア感染<br>・ 入力・表示するモバイル端末のマルウェア感染   | ・ 各種機器のマルウェア対策<br>・ データの妥当性検証<br>・ セキュリティを考慮した標準規格への準拠<br>・ 各種機器の脆弱性管理                    |

## (2) セキュリティ対策事例

スマートファクトリーに関する脅威に対する、主なセキュリティ対策事例を以下に示す。

表 2-7 セキュリティ対策事例

| 項番 | 事例タイトル                                      | 内容                                                                                                                                                                               | 参考 URL 等                                                                                                                                                                                                                    |
|----|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | 制御システムにおける NW への不正侵入防止（IT/OT を分離する DMZ を構築） | 日立 Astemo は、Industrial DMZ を構築、国内主要工場で稼働を開始した。工場ネットワークと OA 用ネットワーク を直接接続せず、その境界に IDMZ を配備して 2 つのネットワークを分離する。基盤には拡張性の高いハイパーコンバージドインフラストラクチャ（HCI）を採用し、IDMZ を構成するアセットは仮想アプライアンス化する。 | <a href="https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2177-hitachi-automotive.html">https://www.cisco.com/c/ja_jp/about/case-studies-customer-success-stories/2177-hitachi-automotive.html</a> |
| 2  | 制御システムにおける NW への不正侵入防止（IT/OT の統合監視）         | NTT コミュニケーションズは、機能別のネットワークの境界に SOC、OT-IDS を導入することで IT/OT の統合監視を行い、IT 領域のナレッジを OT 領域に適用することで、マルウェアの早期検出や、各層で脅威の検出を行う仕組みを提供している。                                                   | IT/OT 統合セキュリティソリューションご説明資料                                                                                                                                                                                                  |
| 3  | 制御システムにおける NW への不正侵入防止（サイバー攻撃をリアルタイム検知）     | 東京電力パワーグリッド株式会社は社会インフラの 1 つである電力供給を行う会社であるため、テロやサイバー攻撃を防ぐためのセキュリティ対策は最優先事項の一つとなっている。そのため、ネットワーク層からアプリケーション層までネットワークトラフィックを分析して、データを送信し                                           | <a href="https://www.macnica.net/forescout/case_01.html/">https://www.macnica.net/forescout/case_01.html/</a>                                                                                                               |

| 項番 | 事例タイトル                                     | 内容                                                                                                                                                                                                                                                                                                                        | 参考 URL 等                                                                                                                                                                                              |
|----|--------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                            | たアプリケーションの種類を検出し、監視することができる DPI (Deep Packet Inspection) 製品である、eyeInspect を採用した。                                                                                                                                                                                                                                          |                                                                                                                                                                                                       |
| 4  | 制御システムにおける NW への不正侵入防止 (ACL 設定機能を搭載したスイッチ) | ヤマハはスイッチにより、ACL (Access Control List) の設定を行うことができる機器を開発している。特定の端末以外からの通信をすべて遮断する、ホワイトリスト型のセキュリティ対策である。スイッチによる ACL の設定を行うことができるため、データリンク層で動作し、上位プロトコルに依存しないアクセス制御が可能となる。                                                                                                                                                   | <a href="https://www.mcafee.com/enterprise/ja-jp/assets/case-studies/cs-makino.pdf">https://www.mcafee.com/enterprise/ja-jp/assets/case-studies/cs-makino.pdf</a>                                     |
| 5  | 制御システムにおける NW への不正侵入防止 (不正侵入検知システムによる対策)   | Nozomi Networks 社は産業用制御システムの監視と評価を行うことができる、SCADAguardian を開発した。以下の特徴を持っている。 <ul style="list-style-type: none"> <li>・ 既知の脅威を検出</li> <li>・ 各デバイスの状態を時系列で監視</li> <li>・ ホワイトリスト/ブラックリストのハイブリット方式による脅威の検出と防止</li> </ul>                                                                                                        | リアルタイムサイバーセキュリティと ICS ネットワークの可視化に！Nozomi Networks 社 “SCADAguardian” シリーズ                                                                                                                              |
| 6  | マルウェア対策 (OT のホワイトリスト型ウイルス対策)               | 東武鉄道では、OT 領域でのセキュリティ強化を重要な経営課題と判断し、自社の運行管理システムにホワイトリスト型のウイルス対策を導入。 <ul style="list-style-type: none"> <li>・ あらかじめ許可リストに登録したアプリケーション (実行ファイル) のみの実行を許可。システムを特定用途化 (ロックダウン) することで、脆弱性攻撃などによる不正侵入や不正実行を防止する。</li> <li>・ USB メモリなどのリムーバブルメディアを利用できる端末を最小限に絞り込み、それらの端末で可用性に影響がないことを確認しつつ、Safe Lock の導入を路線ごとに段階的に導入。</li> </ul> | <a href="https://www.trendmicro.com/ja-jp/about/customer-stories/2019/tobu-201909-01.html">https://www.trendmicro.com/ja-jp/about/customer-stories/2019/tobu-201909-01.html</a>                       |
| 7  | マルウェア対策 (装置ごとにセキュリティソフトを導入)                | McAfee は組込み向けアプリケーションのセキュリティ対策として、McAfee Embedded Control を提供している。IPC (産業用コンピュータ) ごとに導入でき、許可されていないアクセスをブロックし、メモリ保護機能により実行中のプロセスの乗っ取りを防止する。                                                                                                                                                                                | <a href="https://esg.teldevi ce.co.jp/iot/mcafee/product/device/embedded_control.html#anchor-merit-4">https://esg.teldevi ce.co.jp/iot/mcafee/product/device/embedded_control.html#anchor-merit-4</a> |
| 8  | セキュリティを考慮した標準規格への準拠 (OPC UA 規格)            | OPC UA の規格を採用することにより、工場の装置、エッジコンピューティング、OT、IT とのリアルタイムでの情報連携が可能になる。セキュリティ対策として、一般的な認証、権限、信頼性、完全性、監視、可用性などに対して行うことができる。                                                                                                                                                                                                    | <a href="https://monoist.atmarkit.co.jp/mn/articles/1906/19/news002_2.html">https://monoist.atmarkit.co.jp/mn/articles/1906/19/news002_2.html</a>                                                     |

## 2.2.4 サイバーセキュリティ確保に向けてニーズが高まる技術

### (1) 想定される脅威と対策

スマートファクトリーでのサイバーセキュリティ確保に向け、活用が期待できる技術の例について調査した。

主なシステムモデルにおいて想定されるセキュリティリスクに対応するセキュリティ対

策の例を踏まえて、近年の対策技術について文献調査及びヒアリング調査を用いて調査を実施した。

表 2-8 システムモデルにおいて必要なセキュリティ対策例と期待される技術

| 想定される脅威                                                                                                                                                                                                                                   | 必要なセキュリティ対策<br>(例)                                                                                                                                                                                                | 期待される技術 (例)                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>データを送受信するネットワークへの不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li> <li>データを集約する機器への不正アクセスに基づくデータ改ざん、データ窃取等</li> <li>クラウドに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li> <li>外部事業者のなりすましによるデータ改ざん、データ窃取等</li> </ul> | <ul style="list-style-type: none"> <li>ネットワークへの不正侵入防止</li> <li>機器の認証</li> <li>リモートアクセスサーバや保守用 PC の不正侵入防止</li> <li>無線通信の認証、暗号化</li> <li>セキュリティが確保されたクラウドサービスの利用</li> <li>接続先 (人) の認証</li> <li>データの妥当性検証</li> </ul> | <ul style="list-style-type: none"> <li>不正侵入防止技術</li> <li>データ改ざん防止技術</li> <li>IoT 機器認証技術</li> <li>脅威検出技術</li> <li>エッジ仮想化技術</li> <li>片方向通信技術</li> <li>機能安全とサイバーセキュリティの融合技術</li> </ul> |
| <ul style="list-style-type: none"> <li>情報系ネットワークに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li> <li>クラウドに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li> <li>外部事業者のなりすましによるデータ改ざん、データ窃取等</li> </ul>                                                  | <ul style="list-style-type: none"> <li>ネットワークへの不正侵入防止</li> <li>セキュリティが確保されたクラウドサービスの利用</li> <li>接続先 (人) の認証</li> <li>データの妥当性検証</li> <li>分析の妥当性検証</li> </ul>                                                       | <ul style="list-style-type: none"> <li>不正侵入防止技術</li> <li>データ改ざん防止技術</li> <li>脅威検出技術</li> <li>機能安全とサイバーセキュリティの融合技術</li> </ul>                                                        |
| <ul style="list-style-type: none"> <li>外部ネットワークに対する不正アクセスに基づく通信傍受、通信妨害、データ改ざん、データ窃取等</li> <li>外部事業者のなりすましによるデータ改ざん、データ窃取等</li> </ul>                                                                                                      | <ul style="list-style-type: none"> <li>ネットワークへの不正侵入防止</li> <li>セキュリティが確保されたクラウドサービスの利用</li> <li>接続先 (人) の認証</li> <li>データの妥当性検証</li> </ul>                                                                         | <ul style="list-style-type: none"> <li>不正侵入防止技術</li> <li>脅威検出技術</li> <li>機能安全とサイバーセキュリティの融合技術</li> </ul>                                                                            |
| <ul style="list-style-type: none"> <li>デジタルデータ化・蓄積・集計等を行う各種サーバ (IT サーバ) のマルウェア感染</li> <li>MES のマルウェア感染</li> <li>EWS のマルウェア感染</li> <li>OPC サーバのマルウェア感染</li> <li>入力・表示するモバイル端末のマルウェア感染</li> </ul>                                           | <ul style="list-style-type: none"> <li>各種機器のマルウェア対策</li> <li>データの妥当性検証</li> <li>セキュリティを考慮した標準規格への準拠</li> <li>各種機器の脆弱性管理</li> </ul>                                                                                | <ul style="list-style-type: none"> <li>IoT 機器認証技術</li> <li>脅威検出技術</li> <li>エッジ仮想化技術</li> <li>片方向通信技術</li> <li>機能安全とサイバーセキュリティの融合技術</li> </ul>                                       |

## (2) サイバーセキュリティ確保に向けてニーズが高まる技術例

スマートファクトリーのサイバーセキュリティ確保に向けて、ニーズが高まると想定されるセキュリティ技術例を以下に示す。

表 2-9 サイバーセキュリティ確保に向けてニーズが高まる技術例

| 項番 | 事例タイトル                               | 内容                                                                                                                                                                                                                                                                     | 参考 URL 等                                                                                                                                                                                                    |
|----|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | データ改ざん防止技術（軽量暗号技術によるメッセージ認証）         | NTT は、ルーベンカトリック大学、デンマーク工科大学と共同で開発した IoT 向け軽量暗号技術「LightMAC」が ISO 標準に採択されたと発表した。LightMAC は演算リソースの限られている IoT デバイスにおいても動作でき、IoT プラットフォーム全体の安全性を向上させるとしている。また、ブロック暗号を独自の手法で繰り返し適用することが特徴。これにより、既存の軽量ブロック暗号の実装を有効活用しつつ、必要な安全性を確保できる。                                         | <a href="https://monoist.arkit.co.jp/mn/articles/1910/07/news045.html">https://monoist.arkit.co.jp/mn/articles/1910/07/news045.html</a>                                                                     |
| 2  | データ改ざん防止技術（ブロックチェーン技術の活用）            | Xage Security 社はブロックチェーンを活用し、エネルギーや電気通信、公益事業、建物管理、製造現場といった分野で、インフラとデバイス間で改ざん防止のコミュニケーションを可能にする技術を開発。                                                                                                                                                                   | <a href="https://www.smartcape.co.jp/top/products/xage/">https://www.smartcape.co.jp/top/products/xage/</a>                                                                                                 |
| 3  | データ改ざん防止技術（ネットワーク経由によるファームウェア更新時の認証） | 東芝デバイス&ストレージ株式会社は IoT デバイスを遠隔地からネットワークを介して、FW 更新などを行うことを想定し、“セキュアファームウェアローテーション”技術の開発を行った。セキュアファームウェアローテーションとは、マイコンの FW を格納領域に冗長性を持たせ、起動用と更新用に FW を分けることで、FW が更新されたときに、FW の信頼性をマイコンが判断し、正しいデジタル署名付きの FW であるときに、起動用と更新用 FW を切り替えて動作させる技術である。                            | 東芝デバイス&ストレージ株式会社 東芝マイコン新技術セキュアファームウェアローテーションの紹介                                                                                                                                                             |
| 4  | IoT 機器認証技術（ローカル 5G の SIM 認証）         | 大日本印刷はローカル 5G 向けの加入者識別 SIM「DNP SIM for ローカル 5G」を開発、2020 年 3 月より販売。移動通信用加入者識別機能のほか、無線 LAN の EAP-SIM 認証機能やペアリング（特定移動機への利用制限）機能対応などの特徴を備える。                                                                                                                               | <a href="https://www.dnp.co.jp/biz/solution/products/detail/10157626_1567.html">https://www.dnp.co.jp/biz/solution/products/detail/10157626_1567.html</a>                                                   |
| 5  | IoT 機器認証技術（接続された機器の真贋認証）             | 東芝デバイス&ストレージ株式会社はネットワークで接続された機器が本物であることを認証することができるルートオブトラストに対応したマイコンを開発した。物理層の暗号化システムが正常に動作することを保証することで、サイバー攻撃の足がかりに使われるリスクのある不正デバイスの混入や悪意のあるプログラムのインストールといった脅威からデバイスを守ることが可能となる。                                                                                      | <a href="https://toshiba.semicon-storage.com/jp/comp/any/news/news-topics/2019/10/micro-20191023-1.html">https://toshiba.semicon-storage.com/jp/comp/any/news/news-topics/2019/10/micro-20191023-1.html</a> |
| 6  | 片方向通信技術（データダイオードを搭載した集積回路）           | 富士通は 2020 年 8 月、産業用制御システムへのサイバー攻撃を物理的に遮断するネットワーク機器「FUJITSU Manufacturing Industry Solution COLMINA Data Diode (COLMINA Data Diode)」を発売。製造業や社会インフラを担う企業向けに提供を開始。<br>産業用制御システムや電力、ガス、水道など社会インフラ設備向けの OT (Operational Technology) 環境と業務環境をつなぐネットワーク間に設置することで、サイバー攻撃を遮断する。 | <a href="https://pr.fujitsu.com/jp/news/2020/08/18.html">https://pr.fujitsu.com/jp/news/2020/08/18.html</a>                                                                                                 |

| 項番 | 事例タイトル                            | 内容                                                                                                                                                                                                 | 参考 URL 等                                                                                                                                                                                                                              |
|----|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7  | 企業間認証技術（データ流通プラットフォームにおける汎用的な枠組み） | 汎欧州型データインフラ構築プロジェクト GAIA-X では、IDS(International Data Spaces の略)と呼ばれるインタフェースを使って、欧州の企業や行政機関、市民の権利を守るためのデータ保護やオープン性、信頼性、データ主権などの機能を持つ相互運用性、相互接続性を保ったデータ流通プラットフォームの社会実装を目指す。                          | <a href="https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf">https://www.internationaldataspaces.org/wp-content/uploads/2019/03/IDS-Reference-Architecture-Model-3.0.pdf</a> |
| 8  | エッジ仮想化技術（SDN による不正アクセス対策）         | NEC は SDN (Software-Defined Networking) による通信の仮想化技術をエッジコンピューティングに適用した製品を開発した。<br>SDN を実現するために、Open Flow 技術をホワイトリスト型セキュリティに適用することで、抽象化によりユーザーが簡単に設定可能な通信ホワイトリストと、システムが想定していない異常な通信のリアルタイム検知を実現している。 | <a href="https://jp.n.nec.com/techrep/journal/g17/n01/170105.html">https://jp.n.nec.com/techrep/journal/g17/n01/170105.html</a><br><a href="https://jpn.nec.com/sdn/sol08.html">https://jpn.nec.com/sdn/sol08.html</a>                |

## 2.2.5 ステークホルダーの洗い出し

スマートファクトリーにおけるステークホルダーの洗い出し及びセキュリティ対策の例について調査した。

スマートファクトリーにおける主なシステムモデルを考慮し、システムオーナー/ユーザー、ベンダー（ハードウェア、ソフトウェア、ネットワーク）の観点を元に、設計～製造～構築～運用～廃棄/利用終了までのライフサイクルを踏まえて、スマートファクトリーに関わるステークホルダーを洗い出した。

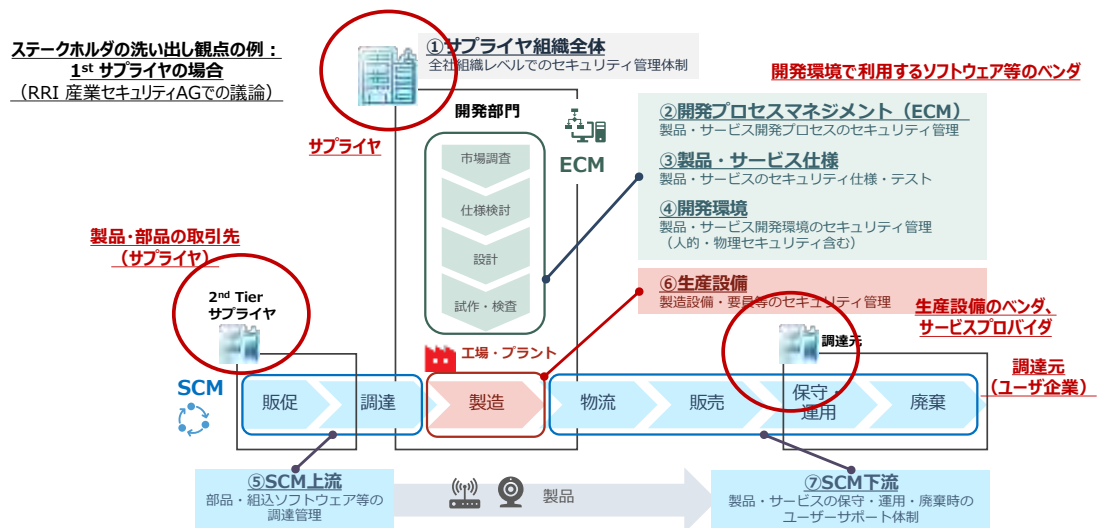


図 2-8 スマートファクトリーにおけるステークホルダー

### (1) ユーザー企業

スマートファクトリーのセキュリティ確保において最も重要な役割を果たすのが、ユーザー企業である。セキュリティを推進する主体となり、セキュリティ要件の策定や予算の確

保等を行う役割を果たす。ユーザー企業の中でも、経営者、IT 部門、OT 部門（生産技術等）等、役職や部門によりそれぞれの役割は異なる。

## **(2) 部品・製品サプライヤー**

スマートファクトリーにおいて製造される製品のセキュリティ確保のためには、その製品を構成する部品や製品のサプライヤーも、部品・製品のセキュリティ確保が求められる。そのため、部品や製品のサプライヤーは重要な役割を果たす。部品や製品の性質や納品先との契約によっては、納品後の利用・運用時においても、脆弱性管理などのセキュリティ面でのサポートが求められる。

## **(3) 生産設備のサプライヤー**

スマートファクトリーの工場システムを構成する生産設備に対してもセキュリティ確保が求められることから、生産設備のサプライヤーも重要な役割を果たす。生産設備自体がスマート化することで、機器そのものにおいて必要なセキュリティ要件を備えていく必要がある。また、生産設備においても利用・運用時において、脆弱性管理などのセキュリティ面でのサポートが求められる。

## **(4) システムインテグレーター、販売会社**

スマートファクトリーの工場システムを構成する生産設備や各種機器においては、単体でのセキュリティ確保は必要であるものの、最終的に複数の機器を接続してシステムとして納めるシステムインテグレーターや販売会社等の果たす役割も大きい。ユーザー企業とのニーズや要件を把握できる立場にあり、システム全体としてのセキュリティを検討し、実装する役割を果たす。

## **(5) 製品開発環境ソフトウェア等ベンダー**

製品のセキュリティを確保するためには、製品開発環境のセキュリティも必要となる。そのため、製品開発環境において利用されるソフトウェア等を提供するベンダーが関わる。

## **(6) ネットワークベンダー、クラウドベンダー**

スマートファクトリーにおいて、情報系ネットワークとの接続や外部との接続が増えることでネットワークベンダーの関わりが増えてくる。工場システムでのセキュリティ対策が難しい場合、ネットワークセキュリティの確保が果たす役割も大きくなる。ネットワークベンダーには、今後ローカル 5G の提供事業者も加わることが想定される。

また、スマートファクトリーによってクラウドサービスの利用が増えることから、クラウドベンダーの関わりが重要となる。

## (7) セキュリティベンダー

スマートファクトリーにおいてもセキュリティベンダーが提供する製品・サービスが活用されることから、セキュリティベンダーが関わる。制御システム向けのセキュリティを提供するベンダーも増えてつつある。

## (8) 利用時の関連事業者

製品・サービスの利用時には、物流事業者、販売・構築の部分でシステムインテグレーターや販売会社、部品提供者、保守・運用事業者、廃棄事業者と別々の事業者が関わる。

### 2.2.6 ガイドラインに活用可能なスマートファクトリー規格

#### (1) 調査対象規格

我が国を含む各国・地域の工場のセキュリティに係る法制度や国際規格の動向について調査した。

既存のセキュリティガイドラインや規格、法制度等から、スマートファクトリーにおける脅威と必要な対策を抽出・整理した。

表 2-10 調査対象規格

| 国   | 名称                                                                                            | 選定理由                                                                                                                   |
|-----|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 米国  | Industrial Internet Security Framework (IIC)                                                  | 米国において産業 IoT (IIoT) を実現するために設立されたコンソーシアム (IIC) によりまとめられたセキュリティフレームワークであり分野に関わらず広く参照される可能性が高いため                         |
| 米国  | NIST (NIST IR 8183 Revision1)                                                                 | 製造業環境のために開発されたサイバーセキュリティフレームワーク (CSF) バージョン 1.1 の実装のための詳細な内容を提供しているため                                                  |
| 欧州  | Report: AIOTI Working Group 4- Policy (AIOTI)                                                 | AIOTI (Alliance for IoT Innovation) は、欧州の産業界が加盟する IoT 推進団体であり、ポリシーを検討する WG4 が IoT におけるプライバシー、セキュリティ、信頼性に関する考えを公表しているため |
| 欧州  | Baseline Security Recommendations for IoT (ENISA)                                             | 重要産業保護の点から IoT セキュリティのベースラインを定めており、欧州各国が参照する可能性も高いため                                                                   |
| 欧州  | ENISA Good Practices for Security of Internet of Things in the context of Smart Manufacturing | スマートマニュファクチャリングに必要とされる IIoT のセキュリティを確保するための推奨策を収集し、関連するセキュリティおよびプライバシーの脅威、リスク、攻撃シナリオを明らかにしているため                        |
| ドイツ | Recommendations for implementing the strategic initiative INDUSTRIE 4.0 (acatech)             | インダストリー4.0 実現に向けて戦略的なイニシアティブをまとめてあり、安全とセキュリティの考え方について具体的に言及しているため                                                      |

| 国   | 名称                                                                                                                   | 選定理由                                                                                       |
|-----|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| ドイツ | Umsetzungsstrategie Industrie 4.0<br>Ergebnisbericht der Plattform<br>Industrie 4.0 (Plattform<br>Industrie 4.0)     | インダストリー4.0を実現するための戦略として、セキュリティ要求条件、セキュリティバイデザイン、セキュリティ対策、セキュリティアーキテクチャに関してまとめているため         |
| ドイツ | Security in Automation -<br>Profilierung von IT-<br>Sicherheitsstandards für den<br>Maschinen- und Anlagenbau (VDMA) | インダストリー4.0において必要となるオートメーションと製造装置のエンジニアリングに関するセキュリティガイドラインであり、国際標準である IEC62443 を参照しているため    |
| ドイツ | Industrie 4.0: Industrial<br>Security 4.0 als<br>gemeinschaftliche Aufgabe<br>(ZVEI)                                 | インダストリー4.0に対して必要となるインダストリーセキュリティ 4.0に関する包括的なセキュリティアーキテクチャのコンセプトについて検討しているため                |
| 国際  | IEC62443 シリーズ                                                                                                        | IEC62443 シリーズは国際的に認知された電気安全規格として開発された規格であり、欧州や北米で開発されている産業向けセキュリティ規格の開発時に参照される規格のうちのひとつのため |

## (2) 規格詳細

調査した規格の詳細を以下に示す。

表 2-11 Industrial Internet Security Framework (IIC)

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | Industrial Internet Security Framework(IIC)                                                                                                                                                                                                                                                                                                                                                                        |
| 発行年             | 2016 年 9 月                                                                                                                                                                                                                                                                                                                                                                                                         |
| 概要              | Industrial Internet of Things(IIoT)システムにおけるセキュリティ関連のアーキテクチャ、設計、技術及びシステムの信頼性に係る手続きについて記載。                                                                                                                                                                                                                                                                                                                           |
| 対象読者            | セキュリティ及びそれに関連する主要なシステム特性に関心を有するあらゆるステークホルダー                                                                                                                                                                                                                                                                                                                                                                        |
| 記載事項<br>(脅威や対策) | 8.1 エンドポイントにおけるセキュリティの脅威と脆弱性 <ul style="list-style-type: none"> <li>・ ハードウェア構成の変更</li> <li>・ BIOS/ファームウェアまたはシステムブート処理の妨害または乗っ取り</li> <li>・ ゲスト OS またはハイパーバイザー/分離カーネルへの脅威</li> <li>・ アプリケーションまたは API の不正な変更<br/>(バスメタル/ネイティブ OS/ランタイム環境/コンテナ)</li> <li>・ ディプロイ処理の脆弱性</li> <li>・ エンドポイントデータの意図せぬ変更</li> <li>・ 監視・分析システムの侵害</li> <li>・ 構成管理の脆弱性</li> <li>・ セキュリティモデル&amp;ポリシーの制御されない変更</li> <li>・ 開発環境の脆弱性</li> </ul> |

表 2-12 NIST (NIST IR 8183 Revision1)

|         |                                          |
|---------|------------------------------------------|
| 機関・タイトル | NIST (NIST IR 8183 Revision1)            |
| 発行年     | 2020 年 10 月                              |
| 概要      | サイバーセキュリティフレームワーク (CSF) バージョン 1.1 の実装の要件 |

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 対象読者            | 製造業者                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 記載事項<br>(脅威や対策) | <p>NISTIR 8183 Revision1 は、製造業環境のために開発されたサイバーセキュリティフレームワーク（CSF）バージョン 1.1 の実装のための詳細を提供している。CSF の「製造業プロファイル」は、製造業セクターの目標と業界のベストプラクティスに沿った、製造業者のサイバーセキュリティリスクを低減するためのロードマップとして使用することができる。サイバーセキュリティ活動を管理し、製造システムに対するサイバーリスクを低減するための、リスクベースの自主的なアプローチを提供する。</p> <p>適用可能なサイバーセキュリティのリスク軽減策を検討し、特定し、管理するためにビジネス・ミッション目標との関係を意識する必要がある。製造業セクターに共通のビジネス／ミッションにおける目標を 5 つに設定している。</p> <p>技術的対策では、IIoT デバイスに実装する必要がある技術的なセキュリティ対策の概要やその実装方法、またインフラストラクチャの回復力や継続性を確保するための要求事項を定めている。</p> <p>製造業プロファイルは、製造業者が採用している現行のサイバーセキュリティ基準や業界ガイドラインを強化することを目的としていますが、それにとって代わるものではありません。製造業プロファイルは、製造業者が採用している現行のサイバーセキュリティ基準や業界ガイドラインを強化することを目的とする。</p> |

表 2-13 Report: AIOTI Working Group 4-Policy(AIOTI)

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | Report: AIOTI Working Group 4-Policy(AIOTI)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 発行年             | 2015 年 10 月                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 概要              | プライバシー、セキュリティ、責任、ネット中立性の 4 つの観点からポリシーを提言。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 対象読者            | IoT に関係する広範なステークホルダー                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 記載事項<br>(脅威や対策) | <p>3 プライバシー</p> <p>プライバシーに係る 10 の課題に対するポリシー提言</p> <ul style="list-style-type: none"> <li>・ 「プライバシーエンジニアリング」がエンジニアリングコミュニティに組み込まれていない</li> <li>・ エンジニアリングの目標に置き換えられるような、一般的なプライバシーリスク評価のフレームワークが存在しない</li> <li>・ 広く認められたプライバシーエンジニアリングの取り組みが存在しない</li> <li>・ IoT アプリケーションの設計開発にあたり、匿名化・仮名化されたデータの利用が不十分</li> <li>・ プライバシー問題に対する、文書に基づく一般的に知られた知識ベースの欠如</li> <li>・ 「プライバシー・バイ・デザイン」の技術ガイドラインや標準が存在しない</li> <li>・ データ主体およびユーザーが、権利を行使できず個人の IoT データを「コントロール」できない可能性</li> <li>・ IoT アプリケーションに関連付けられたデータが、転用されることで新たなプライバシーリスクを生じる</li> <li>・ 規則が適用されていない</li> <li>・ すべての企業がプライバシーを重視している訳ではない</li> </ul> <p>4 セキュリティ</p> <ul style="list-style-type: none"> <li>・ 多様なステークホルダー</li> </ul> <p>多様な IoT エコシステムにまたがるベストプラクティスになり得る、工場での事例が存在する。一つは GSMA が行っている、IoT のセキュリティガイドライン群の策定である。もう一つは OneM2M プロジェクトである。</p> |

|  |                                                                                                                                                                                                                                                                |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <ul style="list-style-type: none"> <li>・ 技術面<br/>あらゆるレベルでのデバイス／アプリケーションのセキュリティ設計・開発・実装を通じて、「安全でセキュアなソフトウェア」の設計・開発方法論をそのライフサイクルに組み込む。</li> <li>・ 社会的<br/>IoTに係る社会的関心。プライバシーに係る 10 の提言の考え方をセキュリティにも適用。特に、工場は設計フレームワークによりプライバシー／セキュリティの利用を促進しなければならない。</li> </ul> |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

表 2-14 Baseline Security Recommendations for IoT (ENISA)

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | Baseline Security Recommendations for IoT (ENISA)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 発行年             | 2017 年 11 月                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 概要              | 設備、ネットワーク、サービス、情報処理装置等を含む重要情報インフラストラクチャに焦点を当て、IoT の基準サイバーセキュリティ推について詳述。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 対象読者            | IoT を適用する組織、IoT の製造・運用を行う企業、IoT 技術者、情報セキュリティ技術者、IT／セキュリティアーキテクト、最高情報セキュリティ責任者、重要情報インフラストラクチャ保護の専門家等を含む個人                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 記載事項<br>(脅威や対策) | <p>3 脅威とリスク分析</p> <p>3.2 脅威の分類</p> <ul style="list-style-type: none"> <li>・ 不正な活動<br/>マルウェア／エクスプロイトキット／標的型攻撃／DDoS／悪意あるデバイスによる偽造／プライバシーへの攻撃／情報の改変</li> <li>・ 盗聴、傍受、乗っ取り<br/>中間者攻撃／IoT 通信プロトコル乗っ取り／情報の傍受／ネットワーク偵察／セッション乗っ取り／情報収集／メッセージの繰り返し</li> <li>・ 停止<br/>ネットワーク停止／デバイスの故障／システムの故障／サポートサービスの喪失</li> <li>・ IT 資産の損害／損失データ・機密情報の漏洩</li> <li>・ 故障<br/>ソフトウェア脆弱性／サードパーティーの故障</li> <li>・ 災害<br/>自然災害／環境災害</li> <li>・ 物理攻撃<br/>デバイス変更／デバイス破壊</li> </ul> <p>3.4 クリティカルな攻撃シナリオ</p> <ul style="list-style-type: none"> <li>・ IoT 管理システムへの攻撃</li> <li>・ センサーデバイスの数値操作</li> <li>・ コマンドインジェクション</li> </ul> |

表 2-15 ENISA Good Practices for Security of Internet of Things in the context of Smart Manufacturing

|         |                                                                                               |
|---------|-----------------------------------------------------------------------------------------------|
| 機関・タイトル | ENISA Good Practices for Security of Internet of Things in the context of Smart Manufacturing |
| 発行年     | 2018 年 10 月                                                                                   |
| 概要      | スマートマニュファクチャリングに必要とされる IIoT のセキュリティを確保のための要件                                                  |

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 対象読者            | 製造業者                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 記載事項<br>(脅威や対策) | <p>ENISA は、インダストリー4.0 を「IoT などの新しいサイバーフィジカル技術を取り入れることで、生産における分散型意思決定を可能にする、デジタル化され統合されたスマートバリューチェーンへのパラダイムシフト」と定義している。設計から製造、運用、サプライチェーン、そしてサービスの保守に至る産業オペレーションの全フェーズを自動化するインテリジェントな、相互接続されたサイバーフィジカルシステムを利用するインダストリー4.0 は、急速に現実のものとなりつつある。スマートマニュファクチャリングに必要とされる IIoT のセキュリティを確保するための推奨策を収集し、関連するセキュリティおよびプライバシーの脅威、リスク、攻撃シナリオを明らかにすることにより、それらに対するセキュリティ意識を高めることを目的としている。本書の 4.1 セキュリティ対策の分類では、論理的に領域を整理するために 3 つの主要グループに分類しており、ポリシー（24 要件）、組織的対策（27 要件）、技術的対策（59 要件）となる。技術的対策では、セキュリティ対策集として 110 件のセキュリティ要件を定義している。</p> <ul style="list-style-type: none"> <li>・ 信頼性および完全性</li> <li>・ クラウドセキュリティ</li> <li>・ 事業継続と復旧</li> <li>・ M2M セキュリティ</li> <li>・ データ保護</li> <li>・ ソフトウェア/ファームウェアの更新</li> <li>・ アクセス制御</li> <li>・ ネットワーク、プロトコル、暗号化</li> <li>・ 監視と監査</li> <li>・ 構成管理</li> </ul> |

表 2-16 Recommendations for implementing the strategic initiative INDUSTRIE 4.0 acatech(German Academy of Science and Engineering )

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | Recommendations for implementing the strategic initiative INDUSTRIE 4.0 acatech(German Academy of Science and Engineering )                                                                                                                                                                                                                                                                                              |
| 発行年             | 2013 年 4 月                                                                                                                                                                                                                                                                                                                                                                                                               |
| 概要              | インダストリー4.0 の実現のために、主軸となる CPS(Cyber Physical System)を普及させるための施策について記載する。                                                                                                                                                                                                                                                                                                                                                  |
| 対象読者            | インダストリー4.0 への関心者                                                                                                                                                                                                                                                                                                                                                                                                         |
| 記載事項<br>(脅威や対策) | <p>CPS の戦略を実現するために以下 3 点が重要になる。</p> <ul style="list-style-type: none"> <li>・ バリューネットワークを通じての水平統合</li> <li>・ 全バリューチェーンを横断するエンジニアリングについてエンドツーエンドのデジタル統合</li> <li>・ 垂直統合とネットワーク化された製造システム</li> </ul> <p>特に、優先して解決する 8 分野についてはワーキンググループ内でアクションを検討する。</p> <ol style="list-style-type: none"> <li>① 標準化と参照アーキテクチャ</li> <li>② 複雑なシステムの管理</li> <li>③ 産業界のための包括的なブロードバンドインフラ</li> <li>④ 安全とセキュリティ</li> <li>⑤ 業務組織と業務設計</li> </ol> |

|  |                                                                                                                                                                                                          |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | ⑥ 研修と継続的な専門家の育成<br>⑦ 制度的フレームワーク<br>⑧ 資源効率<br><br>また、スマート生産、スマートロジスティックス、スマートグリッド、スマート製品、製造業のIoTとIOSを活用し、新たなビジネスモデルを導き、インダストリアル4.0を普及させるための戦略としてドイツの製造業間でリーディング市場を創造することと、ドイツ製造設備産業をリーディングサプライヤーとして進めていく。 |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

表 2-17 Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0 BITKOM、VDMA、ZVEI

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0 BITKOM、VDMA、ZVEI                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 発行年             | 2015/4                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 概要              | インダストリー4.0を実現することで新たな価値連鎖バリューチェーンやバリューネットワーク、デジタル化の進行に伴うことで中心となるプラットフォーム・インダストリー4.0について記載する。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 対象読者            | 経営幹部、専門人材などインダストリー4.0に関心を持つ人                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 記載事項<br>(脅威や対策) | <p>プラットフォーム・インダストリー4.0は3項目が中心となる。</p> <p>■研究と革新</p> <ul style="list-style-type: none"> <li>・ バリューネットワークを横断する水平統合(企業内外の統合を目指す)</li> <li>・ ライフサイクル全体を通じて終始一貫したエンジニアリング(対象商品の開発→生産→保守の情報を一貫して収集する)</li> <li>・ 垂直統合とネットワーク化された生産システム(工場内のアクチュエータ、センサー、生産システム、事業計画など縦割りの流れをまとめて管理する)</li> <li>・ 職場環境に配慮した新たな労働インフラ(機械中心ではなく人間中心に成り立つようにインフラを整備する)</li> <li>・ 分野横断的技術の継続的開発</li> </ul> <p>■リファレンスアーキテクチャ、標準化、規格化</p> <p>インダストリー4.0は訳15業種に適用できるように検討する必要があるため、各業種のプロセス、タスクを分解し、それぞれ標準化、規格化を行うことで、ソリューションに制約を与えることがないアーキテクチャを作成し確率することを目指す。(オブジェクト指向の発想で各タスク、コンポーネントに分けて、責務を明確にしてソリューションを作成する)</p> <p>■ネットワーク化されたシステムの安全性</p> <p>水平方向、垂直方向のネットワーク内における確実なセキュリティを保証するための理論的な考察を行い、セキュリティの仮説、必要条件を整理し定義する。</p> <p>以下に模範的なセキュリティ対策案を示す。</p> <ul style="list-style-type: none"> <li>・ セキュリティアーキテクチャ</li> <li>・ アイデンティティ管理</li> <li>・ 暗号-機密性の保護</li> <li>・ 暗号-整合性の保護</li> <li>・ 安全な遠隔アクセスと頻繁な更新</li> <li>・ プロセスと組織的措置</li> <li>・ 企業全体を網羅</li> </ul> |

表 2-18 Security in Automation -Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau VDMA

| 機関・タイトル                      | Security in Automation -Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau VDMA                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                    |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|-----------------------|--------------------|------------------------------|------------------------------------------------------------------------------------|-----------------------------|--------------------------|------------------|--------------------------------------------|-------------|---------------------------------------------------------------------------|-------------------------------------------|----------------|-------------------------------------------------------------------------|--------------------------------------------------------------------|------------------------|------------------|--------------------------------------------|-----------------------|-----------------|
| 発行年                          | 2016/11                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                    |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| 概要                           | 装置システムのオペレーティングなどの IT システムのセキュリティの要件について IEC6244 シリーズに従ってセキュリティガイドラインについて記載している。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                    |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| 対象読者                         | 業種に関係なく、VDMA メンバー全員                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                    |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| 記載事項<br>(脅威や対策)              | IEC62443 の要件を整理し、以下のように体系的にアプローチする。(表 1)<br>また、実際のシステムを実装するときのセキュリティ基準の要件を IEC62443 の Functional Requirements(FR)と System Requirements(SR)と Requirement Enhancements(RE)に従って実装可能な要件を提示している。(5 章)<br>ゾーン、コンポジット設計時に適用させる要件やデータの信頼、保守についての要件を提示している。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                    |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
|                              | <p>表1</p> <table><tr><th>Security-Ziel</th><th>Aktivitäten/Maßnahmen</th><th>Kapitel (Standard)</th></tr><tr><td>Produkt &amp; dessen Integration</td><td>Festlegen des gewünschten Security-Levels<br/>Systemanforderungen (Maschine/Anlage)</td><td>3.4<br/>3.5.1 IEC 62443-3-3)</td></tr><tr><td>Betrieb<br/>Maschinenpark</td><td>Sicherer Betrieb</td><td>3.5.2 IEC 62443-2-1<br/>oder IEC 62443-2-4)</td></tr><tr><td>Komponenten</td><td>Beschaffung sicherer Komponenten bzw.<br/>Herstellung sicherer Komponenten</td><td>3.5.4 IEC 62443-4-1<br/>und IEC 62443-4-2)</td></tr><tr><td>Inbetriebnahme</td><td>Systemanforderungen (Maschine/Anlage)<sup>1)</sup><br/>Sicherer Betrieb</td><td>3.5.1 IEC 62443-3-3)<br/>3.5.2 IEC 62443-2-1<br/>oder IEC 62443-2-4)</td></tr><tr><td>Dauerhafter<br/>Betrieb</td><td>Sicherer Betrieb</td><td>3.5.2 IEC 62443-2-1<br/>oder IEC 62443-2-4)</td></tr><tr><td>Wartung<sup>2)</sup></td><td>Sichere Wartung</td><td>3.5.3 IEC 62443-2-4)</td></tr></table> <p>Tabelle 5: Security-Aktivitäten</p> | Security-Ziel                                                      | Aktivitäten/Maßnahmen | Kapitel (Standard) | Produkt & dessen Integration | Festlegen des gewünschten Security-Levels<br>Systemanforderungen (Maschine/Anlage) | 3.4<br>3.5.1 IEC 62443-3-3) | Betrieb<br>Maschinenpark | Sicherer Betrieb | 3.5.2 IEC 62443-2-1<br>oder IEC 62443-2-4) | Komponenten | Beschaffung sicherer Komponenten bzw.<br>Herstellung sicherer Komponenten | 3.5.4 IEC 62443-4-1<br>und IEC 62443-4-2) | Inbetriebnahme | Systemanforderungen (Maschine/Anlage) <sup>1)</sup><br>Sicherer Betrieb | 3.5.1 IEC 62443-3-3)<br>3.5.2 IEC 62443-2-1<br>oder IEC 62443-2-4) | Dauerhafter<br>Betrieb | Sicherer Betrieb | 3.5.2 IEC 62443-2-1<br>oder IEC 62443-2-4) | Wartung <sup>2)</sup> | Sichere Wartung |
| Security-Ziel                | Aktivitäten/Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Kapitel (Standard)                                                 |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| Produkt & dessen Integration | Festlegen des gewünschten Security-Levels<br>Systemanforderungen (Maschine/Anlage)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 3.4<br>3.5.1 IEC 62443-3-3)                                        |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| Betrieb<br>Maschinenpark     | Sicherer Betrieb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 3.5.2 IEC 62443-2-1<br>oder IEC 62443-2-4)                         |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| Komponenten                  | Beschaffung sicherer Komponenten bzw.<br>Herstellung sicherer Komponenten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | 3.5.4 IEC 62443-4-1<br>und IEC 62443-4-2)                          |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| Inbetriebnahme               | Systemanforderungen (Maschine/Anlage) <sup>1)</sup><br>Sicherer Betrieb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 3.5.1 IEC 62443-3-3)<br>3.5.2 IEC 62443-2-1<br>oder IEC 62443-2-4) |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| Dauerhafter<br>Betrieb       | Sicherer Betrieb                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | 3.5.2 IEC 62443-2-1<br>oder IEC 62443-2-4)                         |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |
| Wartung <sup>2)</sup>        | Sichere Wartung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 3.5.3 IEC 62443-2-4)                                               |                       |                    |                              |                                                                                    |                             |                          |                  |                                            |             |                                                                           |                                           |                |                                                                         |                                                                    |                        |                  |                                            |                       |                 |

表 2-19 Industrie 4.0 : Industrial Security 4.0 als gemeinschaftliche Aufgabe ZVEI

|                 |                                                                                                                                                                                                                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | Industrie 4.0 :<br>Industrial Security 4.0 als gemeinschaftliche Aufgabe ZVEI                                                                                                                                                                                                                            |
| 発行年             | 2016/4                                                                                                                                                                                                                                                                                                   |
| 概要              | インダストリー4.0を実現するうえで、様々な装置を接続するネットワークの動<br>的变化について記載する。                                                                                                                                                                                                                                                    |
| 対象読者            | -                                                                                                                                                                                                                                                                                                        |
| 記載事項<br>(脅威や対策) | <p>現状と将来のネットワークセキュリティの比較を行い、ギャップを明確にし、方<br/>向性を示している。</p> <p>現状：自社ネットワーク<br/>将来：企業間のネットワーク</p> <p>重要項目としてシステムのアイデンティティ管理を挙げ、メーカー、インテグ<br/>レータ、オペレータなどのネットワークの信頼性を高めることの重要性を提言して<br/>いる。</p> <p>また、異なるネットワーク、異なる企業間で横断的に同じセキュリティレベル(通<br/>信システムの信頼、予防、検出)を合わせることで、セキュリティの脅威に対応で<br/>きる体制を整えていくことができる。</p> |

表 2-20 IEC62443 シリーズ

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 機関・タイトル         | IEC62443 シリーズ                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 発行年             | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 概要              | IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 対象読者            | -                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| 記載事項<br>(脅威や対策) | <p>IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書群である。</p> <p>62443-1-1 では、7つの基本要件を定義している。7つの基本要件（FR：Foundation Requirement）</p> <p>FR 1．識別および認証制御（IAC）</p> <p>FR 2．使用制御（UC）</p> <p>FR 3．システム整合性（SI）</p> <p>FR 4．データの機密性（DC）</p> <p>FR 5．制限されたデータフロー（RDF）</p> <p>FR 6．イベントへのタイムリーな応答（TRE）</p> <p>FR 7．リソースの可用性（RA）</p> <p>IEC 62443-2-4：Requirements for IACS service providers：産業用オートメーション及び制御システム（IACS）のための構築及び保守サービスのプロバイダに対するセキュリティ要求事項を含む IEC 62443 シリーズの部である。オートメーションソリューションの構築及び保守活動中に、アセットオーナーに提供される可能性のある IACS サービスプロバイダのセキュリティ能力に対する要求事項を規定している。</p> <p>62443-1-1 での7つの基本要件に関連する詳細な技術システム要件（SR）を提供する。7つの基本的要件に対応要件 IEC62443-3-3 に具体的な要件が示されている。</p> <p>IEC 62443-4-1 は、産業オートメーションおよび制御システムを構成する製品の開発プロセスを規定している。セキュアなコンポーネントを開発するための方法を規定しており、ISA Secure の EDSA（SDSA）をベースにしている。ソフトウェア開発のライフサイクルを12段階に分けて、それぞれのセキュリティに関する要求事項を記載している。（2018年2月23日発行）</p> <p>IEC 62443-4-2 は、産業オートメーションおよび制御システムのコンポーネントのセキュリティの技術要件を規定している。コンポーネントのセキュリティ要件を規定した国際標準（IS）であり、デバイスに搭載されるセキュリティ機能を規定している。ISA Secure の EDSA（FSA）をベースにしており、セキュリティ機能の実装評価に関する要求事項を記載している。（未発行）</p> |

## 2.2.7 スマートファクトリーのサイバーセキュリティの特徴

従来の工場や、本社機能におけるサイバーセキュリティと比較した、スマートファクトリーのサイバーセキュリティの特徴について以下の通り整理した。

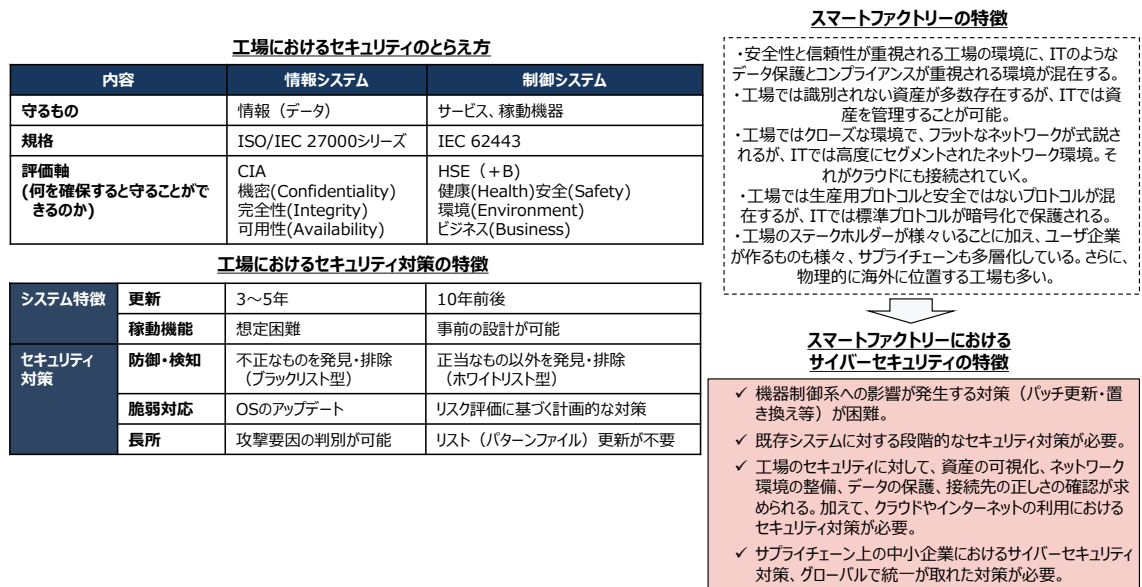


図 2-9 スマートファクトリーにおけるセキュリティの特徴

### 3. スマートファクトリーにおけるサイバーセキュリティガイドライン策定に向けた調査

#### 3.1 調査方法

国内外のステークホルダーに対してのヒアリング調査は、以下の有識者・専門家を対象とした。

ヒアリング対象者は、ロボット革命イニシアティブ協議会（RRI）IoT による製造ビジネス変革 WG 産業セキュリティ AG のメンバーや、スマートファクトリーのセキュリティに関連する取り組みを行う専門家、ステークホルダーに該当する方々とした。

表 3-1 ヒアリング対象者

| カテゴリー               | No. | 組織名                |
|---------------------|-----|--------------------|
| セキュリティ専門家           | 1   | マカフィー              |
|                     | 2   | NEC                |
| 工場生産設備・機器メーカー       | 3   | ジェイテクト             |
|                     | 4   | DMG 森精機            |
|                     | 5   | ソフィックス             |
| 制御システムベンダー          | 6   | 三菱電機               |
|                     | 7   | 東芝                 |
|                     | 8   | 日立製作所              |
| 工場運営主体<br>(サプライヤー含) | 9   | 東京エレクトロン           |
|                     | 10  | ソニーセミコンダクタソリューションズ |
| ネットワーククラウド          | 11  | NTT コミュニケーションズ     |

主なヒアリング項目は以下の通り。

- スマートファクトリーにおけるセキュリティについて
  - スマートファクトリーにおけるシステムモデル
  - スマートファクトリーに関わるステークホルダー
  - スマートファクトリーにおけるセキュリティ対策、ニーズが高まる技術等
- スマートファクトリーにおけるサイバーセキュリティガイドライン策定について
  - スマートファクトリーのセキュリティ確保・推進に向けた課題
  - 策定するガイドラインにおいて、今後議論を深めるべき内容  
(例：新設工場・既設工場、工場の規模等)

#### 3.2 ヒアリング結果まとめ

ガイドライン策定に関する検討を深めるべき議論対象として、ヒアリング調査より得られた意見は以下の通り。

### 3.2.1 ガイドラインの対象

スマートファクトリーにおいては、ユーザー企業（工場）が製造する製品にもバリエーションがあり、ステークホルダーも多様である。ガイドラインについては、想定読者と目的を明確にすべきであるという意見が得られた。対象とする工場を考える上でのポイントを以下に整理する。

#### <新設・既設>

- 工場の新設・既設により取り得る対策は異なる。
- また、新設の工場であっても、既設工場から古い設備を移動して利用するケースもある。
- 古い設備の場合は、レガシー機器のセキュリティ対策についての考慮が必要である。
  - 繋げた結果、ネットワークセキュリティが不完全だったり、プログラムに脆弱性のある古い端末が接続されていたりする。
  - 運用の手間を考慮すると、古い設備を活かすのがよいのか、作り替えるのがよいのか、セキュリティを考慮したコスト効果を考えてもよい。

#### <規模>

- 工場は大半が中小規模であり、どう巻き込んで対策を推進していくかが課題である。

#### <データ活用の進展度>

- データ活用や接続等のグレードに応じたスマートファクトリーの類型化があれば、このタイプのスマートファクトリーはこのくらいのセキュリティが必要、といった整理ができるのではないかと考えられる。類型化だけでも参照する価値のあるガイドラインになると考えられる。

#### <リスク>

- リスクによって取り得るセキュリティ対策は異なることから、同じような脅威、リスクが想定されるメンバーにより検討を進めてはどうか。

### 3.2.2 対応すべきリスク

基本的な考え方としては、リスクベースで検討した上でセキュリティガイドラインをまとめるべき、という意見であった。

- セキュリティの議論はリスクベースとする必要がある、
- セキュリティリスクはユースケースで議論を深めていく必要がある。そのため、スマートファクトリーで考えられるユースケースはこういうモデルで、リスクはこう考えられ、ステークホルダーは誰、脅威は何、だからこういう対策をすべきのように、シナリオを想定して整理する良い。ライフサイクル毎でもリスクが異なる。
- どこまでのリスクを許容して、どこからリスク対策を検討するのかの整理が必要である。また、どこまでの攻撃シナリオを想定するかも要検討である。

リスクに対する対策の考え方としては、海外動向と調和する形で、CPSF との確認を行いながら整理することが受け入れられやすいと考えられる。

- 議論を進める上では、国際規格（IEC62443、NIST CSF、NISTIR 8183）等の拠り所があることで、海外規格の整理に対する日本としての対応というストーリーが受け入れられやすいのではないかと。
- 海外の規制（特に EU）や業界毎の規制と整合性の取れたガイドラインとすることが必要である。

提供側としては、どこまでのセキュリティが求められるかを提示できると有効と考えられる。

- システム単位のセキュリティ、製品単位のセキュリティ、部品単位のセキュリティと考えられるが、部品に対してどこまでのセキュリティについて求められるかを示してほしい。

例) センサーというフィジカルからサイバーに切り出す部分で、どこまでセキュリティを考えるべきか。バックドアをしかけられていないか、製品として正しく作られているかどうかを証明する必要があるのではないかと。運用時に一部の部品を入れ替えるときに、それが本物であることの証明が必要かもしれない。

### 3.2.3 対策を進める主体

スマートファクトリーのステークホルダーは様々であり、各々がセキュリティについて実施すべきことを進める必要がある。各ステークホルダーが対策を推進する必要性等について以下に整理する。

- ユーザー企業（工場）：  
エンドユーザーがセキュリティ対策の必要性を認識し、予算を確保することが最も重要である。予算がなく、仕様としてセキュリティが示されない限り、提供側からセキュリティを強化する提案にはならない。また、工場内に複数のラインが存在し、様々なベンダーのシステムや機器が混在することから、システムの全体像を把握できるのはユーザー企業側のみとなる。工場側の設備について所管する生産技術部門の方々の意識を高め、セキュリティ対策を推進することが必要である。また、ユーザー企業側には、セキュリティ対策を推進する人材と、現場で実際に対策検討・導入・運用・評価する人材のいずれもが必要となる。
- ユーザー企業（工場・中小規模）：  
中小企業向けのセキュリティ対策を進めることが、サプライチェーン全体のセキュリティ確保に重要である。中小企業向けにガイドに記載する内容としては、啓発的な内容で、導入のしやすさやセキュリティがわからなくても容易にできる取り組みが求められる。
- 工作機器メーカー：  
欧米の工作機械メーカーが IEC62443-4-2 認証を取得する動向が見られた。工作機器メーカーの委託先への要求も想定されることから、委託先も含めて、工作機器メーカーに対して、欧米の規格に沿った形で対策を提示することは、工作機器におけるセキュ

リティ対策を推進する上で有効と考えられる。メーカー社内において、製品セキュリティを主管する部門が存在しない場合もあり、また、製品は企画・設計～開発～製造～運用～廃棄までライフサイクルがあるため、各ライフサイクルにおいてどの組織がどう対応するのか、全体のセキュリティをどう確認するか等、社内体制も考慮する必要がある。

- システムインテグレーター、販売会社：

工作機器メーカーや PLC メーカーにとって自社製品のセキュリティ確保は重要であるが、ユーザー企業の実環境や要件に合わせてシステムとして納めるシステムインテグレーターや販売会社が、システムとしての全体的なセキュリティ評価を行い、適切な箇所にセキュリティ対策を施して、納入できることは重要である。外部に接続しないことを前提とした古い設備が工場に残ることも多く、クラウドに繋ぐとことで問題が発生するリスクもある。

- ネットワークベンダー、セキュリティベンダー

ユーザー企業におけるデータ活用が限定的（OA 系の PC を通るのみ等）であれば、ネットワークセキュリティにより一定レベルの対策が可能となる。また、ユーザー企業において工場側の担当がセキュリティについて詳しくない場合、ネットワークに接続するタイミングの検討で IT 側の担当者からセキュリティが求められる場合がある。その際に、ネットワークベンダーとして適切にセキュリティ対策を提案できることは重要である。将来的にローカル 5G の提供事業者が加わった場合の安全性についても考慮が必要である。

### 3.2.4 現在推進されているスマートファクトリーのセキュリティに関する取り組み

- RRI 産業セキュリティ AG：

RRI 産業セキュリティ AG において作成した、サプライチェーンのオンラインコントラクトにおけるバイヤーからサプライヤーへのセキュリティ要求についてまとめた Questionnaire が参考にできると考えられる。これは、CPSF を参考にしつつ、工場の ECM プロセスの不足部分を IEC 62443 から採用したものであり、マチュリティレベルで整理されている。チェック項目をスマートファクトリー化して整理することで活用できると考えられる。

- GUTP（東大グリーン ICT プロジェクト）エッジクロス合同 工場セキュリティ WG：  
GUTP では、データセンターセキュリティやビルセキュリティのガイドラインを検討していた。日本の主要ベンダーやセキュリティベンダー等が参画。工場のサイバーセキュリティに関するガイドラインを策定しており、2021 年 6 月の公表を目指している。ユーザー企業が、機器を導入するときのチェックリストや、機器の調達仕様書テンプレート等を整理しようとしている。

- CSSC：

工場セキュリティに関してユーザーとベンダーが検討する場を設置している。

- ICT-ISAC：

通信系や通信機器メーカーにより、ローカル 5G の提供側として、工場に必要なセキュリティをまとめた簡単なガイドラインを作成予定。

### 3.2.5 その他ガイドラインに対する意見等

＜ガイドの普及促進に向けて＞

- セキュリティ対策を実際に進める上では、仕様を出す側が、具体的な要件（暗号化、ネットワーク、認証、アクセス権等）について明記する必要があることから、ガイドラインにおいて、ユーザーが発注時に利用可能な仕様が明記されればよい。
- IPA「制御システムのセキュリティリスク分析ガイド」のように標準的に参照されることで、周囲からそれを活用してほしいという要求が出てくることもある。  
包囲網的にガイドラインを使うという普及促進の方法もあり得る。
- スマートファクトリーにバリエーションがあるならば、全体像を v1 として示した後、v2 以降でさらに充実していくという方法もあるのではないかと。
- 様々な規格があって乱立するのは困るため、統一されたガイドラインやフレームワークがあると良い。業界団体等と連携した形も望ましい。
- ユーザー企業と話をする、自社ではネットワークに繋いでいないから関係ない、資金が無い、資金があってもスキルの的に使えないと言われるのが実態。  
対策を進めるには、金銭面や技術面での支援や、罰則や義務的なルール等、実効性を高めるための方策を考えていく必要がある。

＜ガイドラインへの記載が望ましい事項＞

- お客様に具体的に何をすべきかわからないと言われるため、何をすべきかわかるようなリファレンス的なものがあれば良い。
- 工場では安全という考え方に親和性があるので、安全の文脈の中にセキュリティという観点を含めた見せ方が意識を変えやすいのではないかと。安全規格に折り込んでいくことも有効と考える。
- BtoB の場合、サプライチェーンの BCP で工場の稼働を確保しようという動きはある。BtoB のお客様の事業継続の要求にセキュリティを入れていくとよいのではないかと。その要求に応えるために、ガイドラインを見たらわかるというのが理想である。



「令和2年度サイバー・フィジカル・セキュリティ対策促進事業  
（スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査）」  
報告書

2021年3月

株式会社三菱総合研究所  
デジタル・イノベーション本部  
TEL 03-6858-3578