経済産業省　御中

令和3年度サイバー・フィジカル・セキュリティ対策促進事業
工場等の製造現場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

三菱総合研究所

デジタル・イノベーション本部
サイバーセキュリティ戦略グループ

2022年3月31日

目次

1. 調査の背景・目的

経済産業省では、「Society5．0」の実現へ向けて様々なデータの「つながり」から新たな付加価値を創出していく「Connected Industries」という概念を提唱し、その実現に向けた取組を推進している。「Society5．0」の実現へ向けた歩みの中で、産業構造、社会環境の変化に伴う形で、サイバー攻撃の脅威も増大し、これまでとは異なる脅威も発生する。このような脅威の増大、新たな脅威の出現に対する準備が必要である。

このような背景の下、経済産業省では、平成30年2月7日に「産業サイバーセキュリティ研究会ワーキンググループ1（WG1）（制度・技術・標準化）」を設置し、「Society5．0」、「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保を目的としたサイバー・フィジカル・セキュリティ対策についての議論を進め、『サイバー・フィジカル・セキュリティ対策フレームワーク』（以下、「CPSF」という。）を平成31年4月18日に取りまとめた。さらに、CPSFの実装に向け、令和元年8月2日より『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォースを開催し、IoT機器等のフィジカル空間とサイバー空間をつなぐ機器・システムに対するセキュリティの検討を行っている。

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、個別の機械やデバイスの稼働データの利活用の可能性が広がる中で、工場等のネットワークがインターネットにつなぐ必要性や機会が増加しており、新たなセキュリティ上のリスク源になり得る。特に、工場等の製造現場においては、下記のような特徴があり、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。

- IT セキュリティ分野で一般的なデータの保護だけでなく、機器稼働等の維持が目的となる。
- 古い設備が運用されている場合があるなど、既存システムに対する段階的なセキュリティ対策の導入が必要になる。
- 工場等の規模がさまざまであり、規模や工場の性質によってとるべき対策が異なる。

本事業では、工場等の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、国内外の動向調査や有識者検討会の開催を通じて、結果をとりまとめた原案を策定することを目的とする。

2. 工場等の製造現場におけるサイバーセキュリティ対策の検討

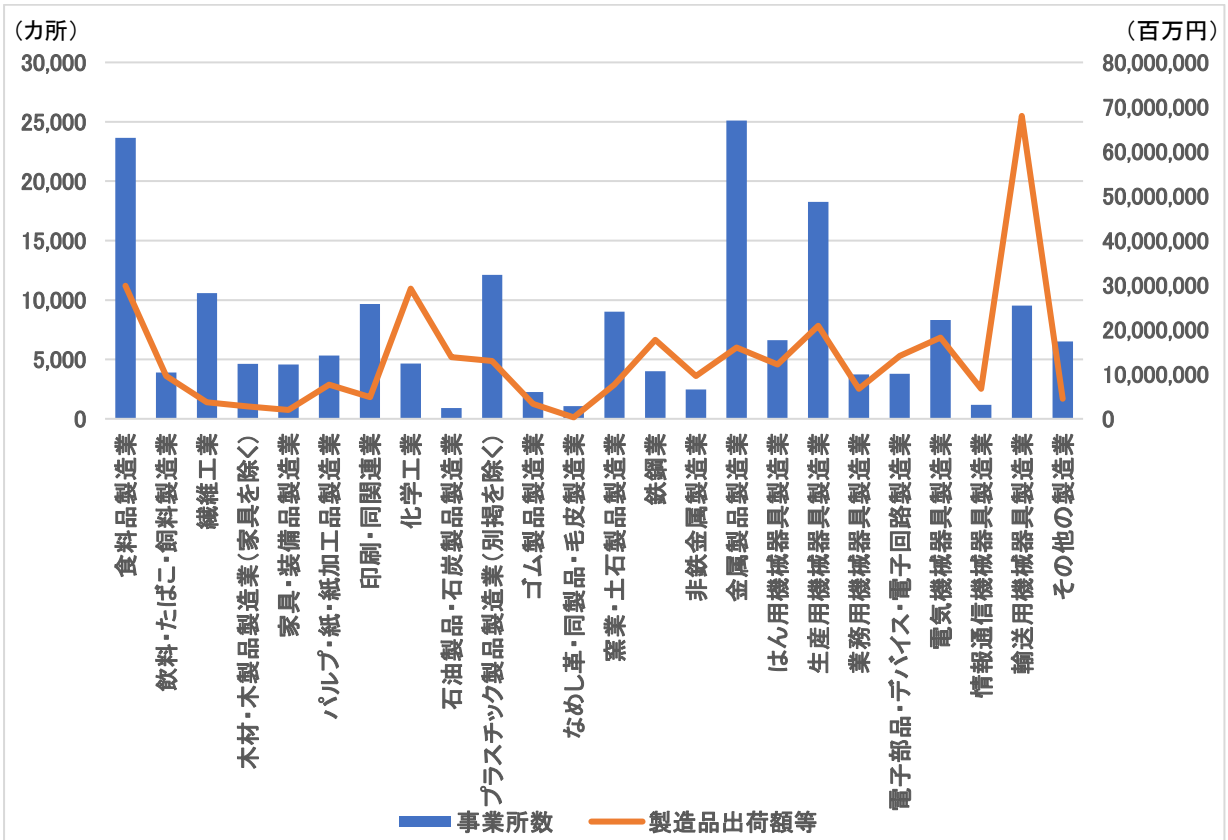
国内外の動向等の調査を通じて、工場等の製造現場におけるサイバーセキュリティのリスクを明らかにしたうえで、工場等の製造現場におけるサイバーセキュリティ確保に関わる各ステークホルダーが実施すべき対策をまとめたガイドライン原案のとりまとめを行った。

2.1 工場等の製造現場におけるサイバーセキュリティの動向

2.1.1 現状の工場等の製造現場におけるサイバーセキュリティ対策の課題と対策

(1) 日本の製造業におけるサイバーセキュリティの状況

セキュリティガイドラインの対象は、製造する製品や業種で限定するのではなく、セキュリティ対策が求められる工場において幅広く活用されることが望ましい。日本においては様々な製品を対象とした製造業があり、高いレベルでのセキュリティが要求される自動車、半導体、医療機器等を製造する工場はもちろん、IoT や AI 等の技術を採り入れ生産性や品質管理の向上等を目指す製造業においても、セキュリティリスクが高まっているといえる。そのため、様々な業種やデータの利活用状況を考慮した上で、セキュリティガイドラインを策定することが必要である。



出所)経済産業省工業統計調査(2020 年確報)を元に作成

図 2-1 製造業における事業所数・製造品出荷額等(2019 年)

セキュリティインシデント発生状況を見ると、2019 年 4 月～2020 年 3 月末の自組織で何らかのセキュリティインシデントが発生した組織は全業種で見ると 8 割弱、そのうち製造業は 8 割を少し上回る結果であった。これらのインシデントの多くはフィッシングメールの受信やビジネスメール詐欺のメール受信であるが、標的型攻撃（22.2%）やランサムウェア感染（17.7%）との回答もあり、これらの攻撃は深刻な被害を引き起こす可能性があることから、セキュリティ対策の必要性が高まっていると言える。

出所）トレンドマイクロ「2020 年度法人組織のセキュリティ動向調査」（2020 年 6 月）

図 2-2 法人組織におけるセキュリティインシデント発生率（業種別）

表 2-1 製造業における主なインシデント事例

タイトル	内容
自動車メーカー取引先のマルウェア感染（2022 年、日本）	・ 自動車メーカーの主要取引先の1つがマルウェア感染 ・ 自動車メーカーは国内全工場の稼働を停止、翌日に再開 ・ 約 1 万 3000 台の生産に影響 ・ 後日、この余波で部品調達に影響、一部工場のラインを 2 日間停止、3,000 台の生産に影響
パイプラインのランサムウェア被害（2021 年、米国）	・ パイプラインがランサムウェア被害 ・ 被害は情報系システムだったが、パイプラインは予防保全的に停止 ・ パイプラインが 6 日間停止、ガソリンが売切になる等、市民生活にも大きな影響
自動車メーカーのランサムウェア感染（2020 年、日本）	・ 自動車メーカーがランサムウェアに感染 ・ 工場の生産や出荷が一時停止、一部は 3 日間の生産停止 ・ 全社員の PC 利用停止等、オフィス系システムにも影響
アルミニウム工場のマルウェア感染（2019 年、ノルウェー）	・ アルミニウム製造大手で大規模なマルウェア感染 ・ 「LockerGoga」と呼ばれるランサムウェアに感染 ・ 発生直後、プレス加工等の一部生産、オフィス業務に影響 ・ プラントは影響拡散防止のためシステムから分離 ・ 被害は、最初 1 週間で 3 億～3 億 5000 万ノルウェークロネ（4000 万ドル相当）と推定
半導体工場のマルウェア感染（2017 年、台湾）	・ 台湾の大手半導体製造企業の社内ネットワークでマルウェア感染 ・ 社内のパッチが未適用の 1 万台以上の Windows7 が WannaCry の変種に感染 ・ 3 拠点の生産施設に影響 ・ 影響額は売上高で最大 190 億円程度
石油化学プラントの安全計装システムを狙ったマルウェア（2017 年、中東）	・ 中東の石油化学プラントで使用されていた Schneider Electric 社製の SIS コントローラー（Triconex）がマルウェア感染 ・ SIS のエンジニアリング・ワークステーションへのリモートアクセスを取得、SIS システムのゼロデイ脆弱性を利用して改ざん ・ プラントが緊急停止
光学機器メーカーのマルウェア感染（2019 年、日本）	・ 日本メーカーのタイ工場の多数のパソコンがマルウェアに感染 ・ 仮想通貨を不正取得するウイルスを送り込むための ID、PW を盗むマルウェアに 100 台程度が感染 ・ 受注生産管理ソフトが利用できず、生産ラインの一部が 3 日間ダウン
自動車工場のマルウェア感染（2017 年、日本）	・ 大手自動車メーカーの工場でコンピュータが WannaCry に感染 ・ 工場に据え付けの設備に付属するパソコンが感染 ・ 生産ラインの制御システムに影響が発生し、一時的にラインを停止 ・ 約 1 千台の車両生産に影響
自動車工場のウイルス感染（2008 年、日本）	・ ベンダのエンジニアリング端末からウイルス感染 ・ 工場の製造ラインの応答が遅くなり、生産が遅延 ・ 解決まで 1 か月間かかった
自動車工場のマルウェア感染（2005 年、米国）	・ マルウェア感染 ・ 外部から持ち込まれた PC による ・ 13 の工場で生産ラインが 50 分停止した ・ 1400 万ドルの損害

（2）製造業における制御方式

製造業においては、大きくセル生産・組立やライン生産・組立といったディスクリート製造（FA：Factory Automation）とプラントのようなプロセス製造（PA：Process Automation）に分ける考え方がある。もちろん、1つの生産拠点で両方の要素が混在する場合もあるが、概念としてこれらの制御方式について、サイバーセキュリティに関わる可能性がある点について対比した。

表 2-2 FA と PA の対比

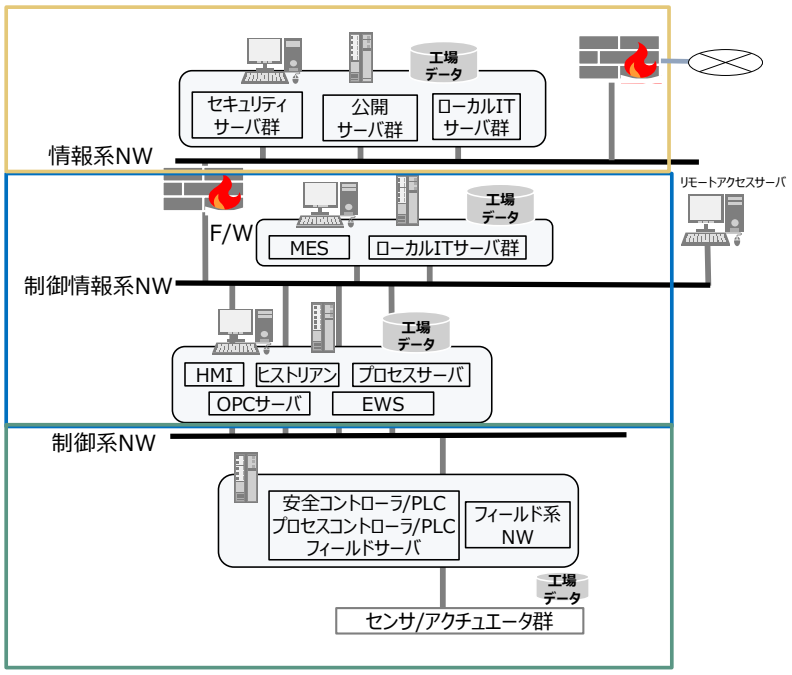
対比の視点	加工・組立工場（FA）	プラント工場（PA）	備考
生産対象	自動車、電機・電子部品等	鉄鋼、石油、食品等	
代表的な制御方式	シーケンス制御 PLC	プロセス制御 PCS	
主な生産方式	個別生産、ロット生産	連続生産、ロット生産	
工程	個別工程、フレキシブル生産 工程間の在庫を持つ	連続工程、一貫生産 工程間在庫を持たない	工程への割り込みの有無
機器・装置構成	変更は比較的容易 構成管理が重要	変更は困難	IoTの導入でセンサ機器の管理が必要
工場に関与するベンダー	装置毎に複数のベンダーが関与	一つのエンジニアリング会社の場合が多い	
制御の特性	集中制御 時定数系の制御	分散制御 無駄時間系が入る制御	
制御精度	加工精度 ロボットの活用	環境からの外乱の影響 統計的制御	
レスポンス性能	数ミリSEC～100ミリSEC リアルタイムに近づける	100ミリSEC～数秒	

対比の視点	加工・組立工場（FA）	プラント工場（PA）	備考
外部調達	部品の調達 加工品の調達	原材料の調達	
生産ステータスの把握	目視、画像、形態で把握	温度、圧力等の視認できない状態量をセンサで把握	
製品の組成	分解可能 リバースエンジニアリング	成分の分離は困難	
生産ステータスの把握	目視、画像、形態で把握	温度、圧力等の視認できない状態量をセンサで把握	
工場の稼働	中断可能	24時間稼働もある	

制御の特性や精度、レスポンス性能の違いにより、利用可能なセキュリティ対策が異なり、結果的にセキュリティ対策を行う箇所がシステム内において異なる場合や、工場の稼働継続に求められる要件の違いにより、システム停止リスクの許容範囲が異なる場合等が考えられる。

制御方式の違いとは異なる視点となるが、大規模プラントと組立工場という違いで見ると、立地による物理的な保護の容易さの違いや、取扱製品による規制や安全にかかわるリスクの違い（化学物質を扱うことによる爆発の危険性等）等は考えられる。

システム構成面では、制御システムの基本的な考え方を踏襲したモデルにおいて、利用されるプロトコル等の違いはあるものの、大きな差異はないと言える。



※ 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 2-3 工場におけるシステムモデル

PA と FA の共通の工場等の生産現場における課題として、以下のように整理できる。

- 可用性が重視され、システムの稼働停止を避ける。
  ただし、PA の方が複数の工程を連続的に制御し、中間生成物として在庫を持てないことから、停止した場合の影響範囲が広くなる可能性が高い。
- センサノイズ、データ遅延の影響を軽減する。
- 専用ネットワークと汎用ネットワークが混在している。
- 古い装置や機器が混在したシステム環境である。
- 品質の安定化が求められる。
- 安全性が重視される。
- 環境影響への配慮が求められる。

2.1.2 データの利活用が進んだ工場等の製造現場のサイバーセキュリティ

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、より高度にデータの利活用が進んだ場合に想定されるサイバーセキュリティリスクやその対策に係る論点を整理した。

（1） 高度なデータ利活用事例

高度なデータ利活用を行うスマートファクトリーの事例を調査し、目的や分類等について整理した。

ローカル（プライベート）5G の実用化に伴い、センサー情報等を高速で取得・分析し、アクチュエータに即座に指示を伝えることが可能となってきている。遠隔のサーバで情報を集約分析する事例も出ている。ただし、工作機械やロボットの加工動作制御（モーションコントロール）については、極めて高い低遅延性が求められることから、本格的な実現段階は先の可能性がある。

GAIA-X 等の活動を中心として、サプライチェーンにおける情報共有やコラボレーションの実装に向けた事例が見られる。環境コンプライアンスやサプライチェーンに係る法規制に対応するための取組みも見受けられる。

表 2-3 工場等の製造現場におけるデータ利活用の事例

事例	目的	分類	実用化段階	主な技術キーワード
①マシンビジョン（画像処理）による品質検査	品質の向上	データ分析による異常検出	実用またはそれに近い段階	マシンビジョン、5G、AI
②AR（拡張現実）による遠距離製品チェック、機器の正確な位置情報の測位	品質の向上	データ分析による異常検出		AR、5G、位置情報
③自動溶接、高精度な組立、重量物の無人搬送、ロボットと人間の協調	作業の効率化 品質の向上 技能の継承	機器の最適制御		マシンビジョン、5G、AI、AGV、ロボット、マン・マシン・コラボレーション
④ネットワークスライシングによるネットワーク分離、遠隔検査	作業の効率化 品質の向上	データ分析による異常検出		5G、AI、ネットワークスライシング
⑤接触を自動的に回避可能な自動搬送ロボット	作業の効率化	機器の最適制御		5G、AGV、ロボット
⑥デジタルツイン（仮想空間による現実空間の再現）を活用した生産プロセスの可視化とシミュレーション	作業の効率化	生産の最適化		デジタルツイン、シミュレーション、5G、ロボット
⑦高速高信頼データ通信による自動車製造の生産性、柔軟性向上	作業の効率化	生産の最適化		5G、AGV
⑧低遅延通信による人間とロボットの接触を回避する安全システム	作業の効率化	機器の最適制御		5G、ロボット
⑨グローバルサプライチェーンにおける CO2 や廃棄物の排出量の可視化	コンプライアンス	複数事業者の協調	実用前段階	サプライチェーン、IDS（GAIA-X）
⑩シェアード・プロダクション（工場や会社をまたいだ生産）	作業の効率化	複数事業者の協調		サプライチェーン、コラボレーション
⑪航空機の共同開発のためのプラットフォーム	作業の効率化	複数事業者の協調		サプライチェーン、コラボレーション、AR、シミュレーション

⑫製品・部品・原材料等のトレーサビリティ、リサイクル	コンプライアンス	複数事業者の協調		サプライチェーン
⑬工作機械やロボットの遠隔動作制御	作業の効率化	機器の最適制御	検討段階	ロボット、モーションコントロール

表 2-4 工場等の製造現場におけるデータ利活用の事例(詳細)

事例	内容	参考 URL 等
①マシンビジョン(画像処理)による品質検査	家電メーカーのハイアール(海尔集团)は、通信機器メーカーのファーウェイ(華為技術)、通信事業者のチャイナモバイル(中国移動)と共同開発したスマートファクトリー向けソリューションを工場に導入。AI を組み合わせた 5G モバイル・エッジ・コンピューティングを構築。工場内に高解像度カメラや AI モジュールを配備し、遠隔地の学習用サーバと低遅延通信を行うことで、高性能マシンビジョンを実現。	http://www.5gaia.org.cn/achievement/detail/167
②AR(拡張現実)による遠距離製品チェック、機器の正確な位置情報の測位	家電メーカーのミデア(美的集团)は、5G 全結合型スマート製造モデル工場をオープン。前年、ミデアとチャイナ・ユニコム(中国聯通)、ファーウェイ(華為技術)が協業し、工場生産製造プロセスを統合。スマート倉庫、スマート車両管理、AI スマートモニタリングなどを含む 19 件の応用と 600 件を超える 5G 接続の実施ソリューションを計画。	https://www.softbank.jp/biz/blog/business/articles/202104/lighthouse-midea/
③自動溶接、高精度な組立、重量物の無人搬送、ロボットと人間の協調	中国の建設機械大手であるサニー(三一重工)で主力製品回転式掘削リグなどを生産する北京工場は、重工業として世界で初めてライトハウス工場に認定された。5G、クラウドコンピューティング、人工知能などの技術を駆使することにより、労働生産性を 85%向上し、生産サイクルを 30 日から 7 日に短縮。	https://www.softbank.jp/biz/future_stride/entry/techblog/sbc/china/20211028/
④ネットワークスライシングによるネットワーク分離、遠隔検査	中国の空調メーカー大手であるグリー・エレクトリック(格力電器)は、チャイナ・ユニコム(中国聯通)と協力して、中国のインテリジェント製造の分野でモバイル・エッジ・コンピューティング、エッジクラウド、5G スタンドアローン及びネットワークスライシングに基づく最初のプライベートネットワークを実現。	http://www.5gaia.org.cn/achievement/detail/167
⑤接触を自動的に回避可能な自動搬送ロボット	自動車部品・電動工具メーカーのボッシュは、フォイエルバッハ工場にローカル 5G を導入し、自動搬送ロボット「ActiveShuttle」を運用。最大で 260Kg の重量の資材を運搬することが可能な「ActiveShuttle」は、レーザーセンサーで周囲の状況を検知し、ローカル 5G で互いに通信することで、モノや人に当たることなくスムーズに運行できる。	https://www.youtube.com/c/boschrexrothag
⑥デジタルツイン(仮想空間による現実空間の再現)を活用した生産プロセスの可視化とシミュレーション	MW は、工場の生産ラインを変更する際に、デジタルツインを活用してシミュレーションを行うことで、計画プロセスの効率化を実現。BMW には 40 種類以上のモデルがあり、車両ごとに選択できるオプションも 100 種類以上ある。多彩な生産要件に対応するため、デジタルツインを活用し、製造ラインあたり最大 10 種類の車種を生産可能にした。	https://www.youtube.com/c/NVIDIA
⑦高速高信頼データ通信による自動車製造の生産性、柔軟性向上	ドイツ自動車大手フォルクスワーゲン(VW)はヴォルフスブルクの本社工場で、ローカル 5G の「キャンパスネットワーク(5G Campusnetz)」が稼働したと発表。	https://www.volkswagenag.com/de/news/2021/10/volkswagen-tests-5g-for-production-on-its-way-to-smart-factories.html
⑧低遅延通信による人間とロボットの接触を回避する安全システム	アウディとエリクソンは、産業用ロボットを 5G で運用するパイロットプロジェクトを実施した。エアバッグモジュールをアウディ車のステアリングホイールに取り付ける作業を行う産業用ロボットに安全センサーをとりつけ、人間の手を検知した際に自動で停止する仕組みを検証した。	https://www.audi-mediacenter.com/en/press-releases/5g-in-production-audi-and-ericsson-take-the-next-step-together-12578

⑨グローバルサプライチェーンにおける CO2 や廃棄物の排出量の可視化	NTT コミュニケーションズは、欧州 GAIA-X を構成する技術標準 IDS のコア技術 IDS コネクターとの相互接続を実現するプラットフォームのプロトタイプを開発することに成功。IDS と企業間の安全なデータ流通を実現するトラストデータ基盤 withTrust を連携させるセキュアな国際データ流通プラットフォームのプロトタイプを新たに開発し、日欧の共同トライアルを 2021 年 10 月より開始。	https://www.ntt.com/about-us/press-releases/news/article/2021/1014.html
⑩シェアード・プロダクション（工場や会社をまたいだ生産）	スマートファクトリーKL では、「ビジョン 2025-プロダクションレベル 4」を目標に掲げ、工場や会社をまたいだ生産「シェアード・プロダクション」の実現に取り組んでいる。	https://www.bmwi.de/Redaktion/EN/Artikel/Digital-World/GAIA-X-Use-Cases/shared-production.htm
⑪航空機の共同開発のためのプラットフォーム	航空機、衛星、着陸機などの製品ライフサイクル全体を通じた作業プロセスをよりデジタル化し、長期的な競争力を高めるため、既存のプロセスをバーチャルリアリティ（AR/VR）技術やリアルタイムシミュレーションと連携させ、安全なバーチャル環境で航空宇宙工学のオプションを最短時間で表示・評価する。	https://dasclab.eu
⑫製品・部品・原材料等のトレーサビリティ、リサイクル	Catena-X は、オープン性と中立性を確保するために、ドイツに本拠を置く協会として組織された。自動車メーカーやサプライヤ、ディーラー、アプリケーション、プラットフォーム、インフラストラクチャのプロバイダを含むシステムサプライヤーが参加できる。Catena-X の目的は、自動車のバリューチェーン全体で情報とデータを共有するために、統一された業界標準を構築することにあり、GAIA-X と密接に連携している。	https://catena-x.net/fileadmin/user_upload/intro_praesenationen/catena-x_overview_eng_v2.2.pdf
⑬工作機械やロボットの遠隔動作制御	FA を構成する工作機械やロボットの動作制御（モーションコントロール）には、極めてシビアな低遅延性が求められる。製造業への 5G 適用を目指してドイツ電気電子工業連盟（ZVEI）が設立した業界団体 5G-ACI では、製造 IoT における 5G のユースケース検討と要求条件の洗い出しを行っている。	https://www.zvei.org/en/press-media/publications/5g-for-connected-industries-and-automation-white-paper-second-editon

（2） セキュリティリスクの検討

1）新たなネットワーク技術の利用によるセキュリティリスク

ローカル（プライベート）5G の実用化に伴い、センサーデータ等を高速で取得・収集・分析し、アクチュエータに指示を伝えることが可能となっている。従来、有線や Wi-Fi 等のネットワークを経由してセンサーデータを収集し、工場内ネットワーク内のサーバ群で分析を行うシステムが想定されていた。それに対して、より高速でリアルタイム性の高い情報処理を、ローカル 5G 基地局やエッジコンピューティングの資源を組み合わせて実現するようなシステムモデルが想定される。

そのため、5G 技術のセキュリティリスクや、ローカル 5G ネットワークを構築・運用する場合のセキュリティリスクが想定される。

2）クラウド利用・連携によるセキュリティリスク

組織間でのデータ共有のために、工場に蓄積されたデータをクラウドサービスにアップロードして活用する形態が進展することが想定される。クラウドサービスは、自社が利用するクラウドサービスと他組織が利用するクラウドサービスが異なる場合もある。クラウドへのデータ蓄積や交換に伴うセキュリティリスクや、他組織とデータを共有する際のセキュリティリスクが想定される。また、データ主権を脅かすセキュ

リティリスクに配慮する必要がある。

表 2-5 データ利活用が進展した工場等の製造現場におけるセキュリティ脅威と対策例

想定脅威	必要なセキュリティ対策例
無線ネットワークに対する不正アクセスによる 通信傍受、通信妨害、データ改ざん、データ窃取等	無線通信の暗号化 PoC 段階での十分なセキュリティ検証 早期に異常検知できる体制構築
SIM カードの窃取によるシステムへの侵入	物理的な盗難防止対策、eSIM の利用 アカウント保護対策 デバイスの真正性・セキュリティ状態の確認・制御
基地局への侵入、権限の窃取	基地局が有する脆弱性の十分な検証・確認
クラウドサービスへの不正アクセスによる データ窃取、不正利用等	クラウドサービスにおける適切なアクセスコントロール

（3）ガイドライン策定にあたり検討すべき視点

調査結果で得られた情報から、工場等の製造現場においてデータ利活用が進んだ場合のセキュリティガイドライン策定にあたり検討すべき視点を整理した。

表 2-6 データ利活用が進んだ工場等製造現場におけるセキュリティ検討の視点

検討の視点	従来の工場セキュリティの考え方	データ活用の利活用が進展した際に考慮すべき事項
システム/ ネットワーク	制御系／情報制御系のネットワークが有線ネットワーク主体で構成され、ネットワークの境界で防護。	無線基地局（ローカル 5G、B5G）やエッジコンピューティングの資源を組み合わせて実現する、境界が曖昧な環境での防護が必要。
ステークホルダー	自社に閉じた形で、自社工場内に関わるステークホルダーにおいてセキュリティを確保。	サプライチェーン全体のステークホルダーにおけるセキュリティの確保が必要。
技術	従来の ICT 及びそれに基づくセキュリティ対策の導入・運用を行うセキュリティマネジメントシステムの構築。	最新の技術を踏まえたセキュリティ対策の導入・運用、設計・開発の段階からのセキュリティの組み込み。
要件	有線ネットワークを利用した FA に求められるレベルの低遅延通信を要件とする環境におけるセキュリティ確保。	無線接続を含むネットワークや、処理能力が向上したエッジを活用した環境において、多くの工作機械やロボット等が同期した動作制御が可能なことを要件とする環境におけるセキュリティ確保。
データ	主に自社が保有するデータを対象として保護。	データを他組織と共有することを想定したデータの取り扱い、クラウドを利用したデータ蓄積・交換に伴うセキュリティの留意。

2.1.3 国内外の関連規格

（1） 調査対象

1）国際規格等との関係

工場等の製造現場におけるサイバーセキュリティに必要な要件を整理するにあたり、国内外の関連規格やガイドライン等について調査を実施した。調査対象を以下に示す。

表 2-7 工場等の製造現場のセキュリティに関連する国内外の規格等

国	名称	概要、出所
日本	サイバー・フィジカル・セキュリティ対策フレームワーク	日本の産業におけるサプライチェーン全体のサイバーセキュリティの確保へ向けたフレームワーク
		経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク Ver1.0」 https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf
共通	IEC62443	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。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1つ
		出所）International Electrotechnical Commission（IEC）「IEC62443 Series」
米国	Cybersecurity Framework Version 1.1 Manufacturing Profile（NIST、2020/10）	製造環境向け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 の実装の詳細（NISTIR - 8183 Rev 1 を参照）
		National Institute of Standard and Technology（NIST）「Cybersecurity Framework Version 1.1 Manufacturing Profile」 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf
	Industrial Internet Security Framework（IIC、2016/9）	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
		Industrial Internet Consortium（IIC）「Industrial Internet of Things Volume G4: Security Framework」 https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf
欧州	Guidelines for Securing the Internet of Things（ENISA、2020/11）	IoT のサプライチェーンを保護するための、要件と設計から最終用途の配送と保守、廃棄まで、ライフスパン全体のセキュリティガイドライン。IoT メーカー、開発者、インテグレーター、および IoT のサプライチェーンに関与するすべての利害関係者が対象
		The European Union Agency for Cybersecurity（ENISA）「Guidelines for Securing the Internet of Things」 https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things（2022 年3月 1 日）
	Industry 4.0 Cybersecurity : Challenges & Recommendations（ENISA、2019/5）	インダストリー4.0 とインダストリアル IoT のセキュリティ対策とセキュリティの採用に対する主な課題、推奨事項のリスト
		The European Union Agency for Cybersecurity（ENISA）「Industry 4.0 Cybersecurity : Challenges & Recommendations」 https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations（2022 年3月 1 日） 独立行政法人 情報処理推進機構（IPA）「インダストリー4.0 サイバーセキュリティ：課題と提言」 https://www.ipa.go.jp/files/000074696.pdf

	Good Practices for Security of Internet of Things in the context of Smart Manufacturing（ENISA、2018/11）	セキュリティとプライバシーの課題、脅威、リスク、攻撃のシナリオをマッピングしながら、インダストリー4.0 /スマートマニュファクチャリングにおいて IoT セキュリティを確保するためのグッドプラクティス
		The European Union Agency for Cybersecurity（ENISA）「Good practices for security of IoT」 https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1（2022 年3月 1 日） 独立行政法人 情報処理推進機構（IPA）「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」 https://www.ipa.go.jp/files/000073490.pdf
	Baseline Security Recommendations for IoT（ENISA、2017/11）	重要産業保護の点から定めた IoT セキュリティのベースライン
		The European Union Agency for Cybersecurity（ENISA）「Baseline Security Recommendations for IoT」 https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/（2022 年3月 1 日） 独立行政法人 情報処理推進機構（IPA）「IoT のベースラインセキュリティに関する提言」概要 https://www.ipa.go.jp/files/000063605.pdf
ドイツ	Recommendations for implementing the strategic initiative INDUSTRIE 4.0（acatech）	インダストリー4.0 実現に向けた戦略的なイニシアティブ。安全とセキュリティの考え方について具体的に言及
		Deutsche Akademie der Technikwissenschaften（acatech）「Recommendations for implementing the strategic initiative INDUSTRIE 4.0」 https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/download-pdf
	Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0（Plattform 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ついて記載
		Bundesverband Informationswirtschaft, Telekommunikation und neue Medien（BITKOM）, Verband Deutscher Maschinen- und Anlagenbau（VDMA）, Zentralverband Elektrotechnik- und Elektronikindustrie（ZVEI）「Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0 」 https://www.bitkom.org/sites/default/files/file/import/150410-Umsetzungsstrategie-0.pdf

（2）調査結果

1）サイバー・フィジカル・セキュリティ対策フレームワーク

a. 概要

サイバー・フィジカル・セキュリティ対策フレームワークの概要は以下の通り。

表 2-8 サイバー・フィジカル・セキュリティ対策フレームワークの概要

機関・タイトル	サイバー・フィジカル・セキュリティ対策フレームワーク（経済産業省）
発行年	2019 年 4 月
概要	サイバー空間とフィジカル空間が高度に融合した「Society5.0」において、新たな形のサプライチェーンである「価値創造プロセス（バリュークリエイションプロセス）」におけるセキュリティ対策を整理したフレームワーク
対象読者	CISO、サプライチェーンマネジメントに関わる戦略・企画部門の担当者、バリュークリエイションプロセスに関わる企業・団体等のセキュリティ担当者、情報関連機器、制御系機器の開発・品質保証、システム設計・構築・検証担当者、データマネジメントの担当者、各産業分野におけるセキュリティ対策のガイドライン等を策定する業界団体等の担当者
記載事項（脅威や対策）	「Society5.0」における新たな形のサプライチェーンにおいて全産業にほぼ共通して求められるセキュリティ対策をわかりやすく示すために、サイバー空間とフィジカル空間が高度に融合した産業社会を 3 つの切り口（「企業間のつながり」、「フィジカル空間とサイバー空間のつながり」、「サイバー空間におけるつながり」）から捉え、サプライチェーンの信頼性（trustworthiness）を確保する観点から、それぞれの切り口において守るべきもの、直面するリスク源、対応の方針等を整理している。

b. セキュリティ要件の整理

セキュリティ対策要件として、20 のカテゴリーを定義している。各カテゴリーは NIST の Cybersecurity Framework と整合している。

表 2-9 サイバー・フィジカル・セキュリティ対策フレームワークにおけるセキュリティ要件

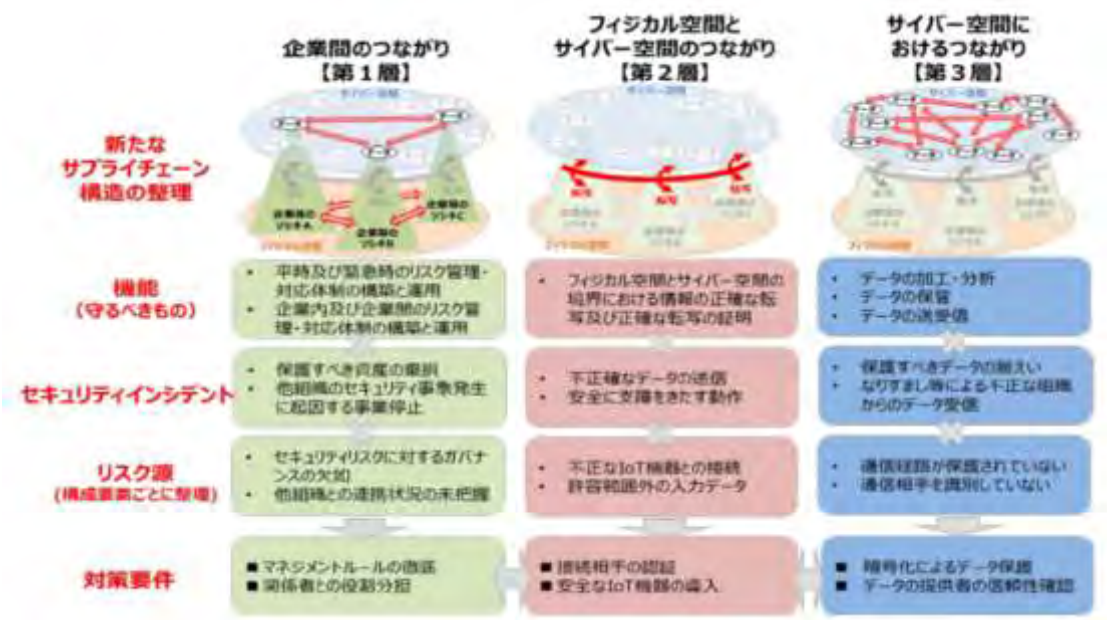
要件	概要
資産管理	企業等が事業目的を達成することを可能にするデータ、ヒト、モノ、システム、それらが管理される場所等を特定し、自組織のリスク戦略とその目的における重要性に応じた管理をする。
ビジネス環境	自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行う。この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。
ガバナンス	自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解し、サイバーセキュリティリスクの管理者に伝達する。
リスク評価	企業等は自組織の業務（ミッション、機能、イメージ、評判を含む）、資産、個人に対するサイバーセキュリティリスクを把握する。
リスク管理戦略	自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用する。

サプライチェーンリスク管理	企業等の優先順位、制約、リスク許容値及び想定が、サプライチェーンリスク管理に関連するリスクの決定を支援するために確立され、利用される。企業等は、サプライチェーンのリスクを特定、評価、管理するプロセスを確立し、実施する。
アイデンティティ管理、認証及びアクセス制御	資産及びそれが管理される場所への論理的・物理的アクセスを、承認されたソシキ、ヒト、モノ、プロシージャに限定し、承認された活動及びトランザクションに対する不正アクセスのリスクの大きさに合うよう管理する。
意識向上及びトレーニング	自組織の職員及びパートナーに対して、関連するポリシー、手順、契約に基づいた、サイバーセキュリティに関連する義務と責任を果たすために、サイバーセキュリティの意識向上教育と、訓練を実施する。
データセキュリティ	情報を、その機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理する。
情報を保護するためのプロセス及び手順	(目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う)セキュリティポリシー、プロセス、手順を維持し、システムと資産の保護の管理に使用する。
保守	産業用制御システムと情報システムの構成要素の保守と修理をポリシーと手順に従って実施する。
保護技術	関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティとレジリエンス、セーフティを確保するための、技術的なソリューションを管理する。
異変とイベント	異変を検知し、事象がもたらす可能性のある影響を把握する。
セキュリティの継続的なモニタリング	セキュリティ事象を検知し、保護対策の有効性を検証するために、システムと資産をモニタリングする。
検知プロセス	異常なセキュリティ事象を正確に検知するための検知プロセス及び手順を維持し、テストする。
対応計画	検知したセキュリティインシデントに対応し、適切に自組織の事業を継続しつつ、影響を受ける資産やシステムを復元できるよう、対応・復旧のプロセス及び手順を実施し、維持する。
伝達	セキュリティインシデントがもたらす自組織、及び社会全体への影響を低減し、法執行機関のような組織からの支援を得られるよう、内外の利害関係者(例えば、取引先、JPCERT/CC、他組織の CSIRT、ベンダ)との間で対応・復旧活動を調整する。
分析	効率的な対応を確実にし、復旧活動を支援するために、分析を実施する。
低減	セキュリティ事象の拡大を防ぎ、その影響を低減し、セキュリティインシデントを解決するための活動を実施する。
改善	現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応・復旧活動を改善する。

出所)サイバー・フィジカル・セキュリティ対策フレームワーク
(https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf)

c. 提示されているフレームワークやアーキテクチャ

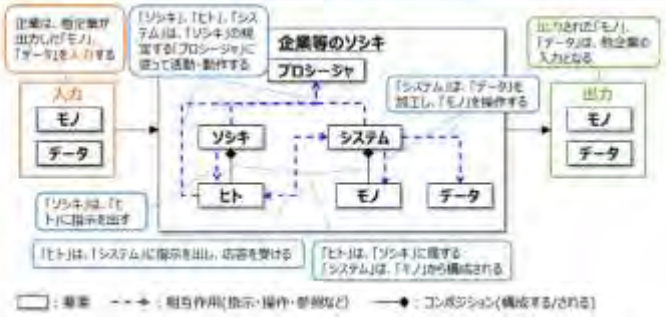
サイバー空間とフィジカル空間が一体化した産業社会における付加価値を創造するための一連の活動(サプライチェーン)において、「企業間のつながり(第1層)」「フィジカル空間とサイバー空間のつながり(第2層)」「サイバー空間におけるつながり(第3層)」の3つの層で整理し、信頼性の基点を的確に設定している。また、サプライチェーンがより柔軟で動的なものに変化した価値創造過程(バリュークリエイションプロセス)に関与する構成要素を、セキュリティ対策を講じる上で最適な最小単位として「ソシキ」「ヒト」「モノ」「データ」「プロシージャ」「システム」の 6 つに整理している。



出所）サイバー・フィジカル・セキュリティ対策フレームワーク
（https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf）

図 2-4 サイバー・フィジカル・セキュリティ対策フレームワークの3層モデル

構成要素	定義	構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・ソシキ	データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人	プロシージャ	• 定義された目的を達成するために一連の活動を定めたもの
モノ	• ハードウェア、ソフトウェア及びそれらの部品操作する機器を含む	システム	• 目的を実現するためにモノで構成される仕組み・インフラ



出所）サイバー・フィジカル・セキュリティ対策フレームワーク
（https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf）

図 2-5 サイバー・フィジカル・セキュリティ対策フレームワークの 6 つの構成要素

d. ガイドライン策定にあたり検討すべき視点

「サイバー・フィジカル・セキュリティ対策フレームワーク」において導出されているリスク源や対策要件を活用し、工場等の製造現場におけるサイバーセキュリティ対策の要件を整理することが考えられる。

また、セキュリティ対策要件において「ビジネス戦略」と「リスク管理戦略」という戦略面のカテゴリーがある。経営目標や組織としての戦略があり、それを基点としてセキュリティ戦略を展開していけるよう一連のプロセスを整理することが求められる。さらには、「サプライチェーンリスク管理」が明示されており、サプライチェーンのリスクを特定、評価、管理するプロセスを通じて、工場等の製造現場に関わる取引先等の関係者それぞれが実施すべきセキュリティ対策を明確化し、セキュリティを確保することが必要となる。

2)IEC62443

a. 概要

IEC62443 シリーズの概要は以下の通り。

表 2-10 IEC62443 シリーズの概要

機関・タイトル	IEC624443 シリーズ （IEC62443：IEC/TC65/W10、ANSI/ISA-62443：ISA99 WG）
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	産業用制御システムのセキュリティ確保に関わる責任者、担当者 （アセットオーナ、サービス提供者、システムまたはコンポーネント提供者）
記載事項 （脅威や対策）	対象を、「全般」「オーナ」「システム」「コンポーネント」に分類している。主な内容は以下の通り。 ・全般（62443-1） - 62443-1-1：62443 シリーズに共通するコンセプトやモデルの説明 - 62443-1-2：62443 シリーズで用いられる用語や略語集 ・オーナ（62443-2） - 62443-2-1：アセットオーナ向けのセキュリティプログラムの要件 - 62443-2-4：アセットオーナへのサービス提供者のセキュリティプログラムの要件（調達仕様作成時に参照可） ・システム（62443-3） - 62443-3-3：セキュリティレベル基準とシステムのセキュリティ機能要件 ・コンポーネント（62443-4） - 62443-4-1：コンポーネントベンダのセキュリティ開発プロセス要件 - 62443-4-2：コンポーネントのセキュリティ機能要件 本シリーズに関連する認証制度として、ISASecure 認証制度、CSA 認証、IECEE 認証制度、CSMS 認証制度、ISA/IEC 62443Cybersecurity Certificate Program 等がある。

b. セキュリティ要件の整理

7 つの基本的な要件（Foundational Requirements: FR）を定めている。

また、FR に対応する技術的なシステム要件（System Requirements: SR） と、それを満たす強化策（Requirement Enhancements:RE）を規定している。セキュリティレベル（Security Level:SL）は、各要件を満足した場合にどのような攻撃からシステムを保護できるかを示している。

表 2-11 IEC62443-1-1 で定められる 7 つの基本的な要件

FR の要件	概要
1. 認証	すべてのユーザー(人／ソフトウェアプロセス／デバイス)を識別し、認証する。
2. アクセス権制御	認証されたユーザに与える権限を限定し、システムやリソースに対して制限された実行がなされるようコントロールする。
3. データの完全性	データの改ざんや破損・喪失がなされないようにする。
4. データの機密性	開示されていない情報が漏洩されないようにする。
5. データフローの制約	不要なデータフローを制限するため、ゾーンや経路を適切に分割する。
6. イベントへのタイムリーな応答	セキュリティ違反に対し、関係者への通知、レポートの作成、各種調整などタイムリーな対応を行う。
7. リソースの可用性	サービスが使用不能にならないよう、システムやリソースの可用性を保証する。

出所)IEC62443-1-1

出所)日立製作所「制御システムセキュリティの標準化動向～IEC 62443 の最新状況と認証制度の紹介～」(https://www.jpcert.or.jp/present/2020/ICSR2020_04_HITACHI.pdf)

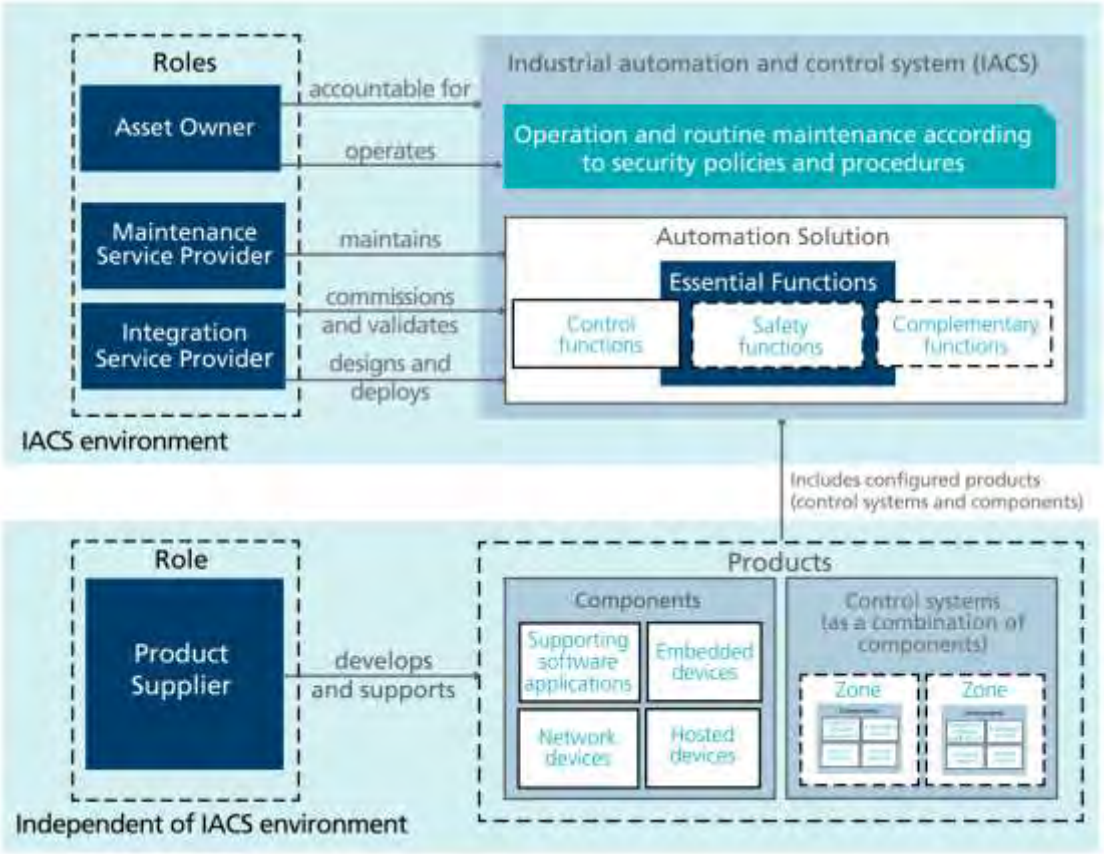
図 2-6 ISA/IEC 62443 シリーズの一覧

c. 提示されているフレームワークやアーキテクチャ

Purdue Enterprise Reference Architecture(PERA)を採用している。

62443 では、役割とシステムの関係を以下のように整理している。役割としては「アセットオーナ」と「メンテナンスサービスプロバイダ」「インテグレーションサービスプロバイダ」「プロダクトサプライヤ」に分類している。また、システムとしては「IACS コンポーネント」「IACS システム(制御システム)」「自動化ソ

リューション」「IACS（自動化ソリューションを含む）」と定義している。



出所）ISA「Quick Start Guide: An Overview of ISA/IEC 62443 Standards Security of Industrial Automation and Control Systems」

図 2-7 役割、製品、自動化ソリューション及び IACS

d. ガイドライン策定にあたり検討すべき視点

コンポーネントやシステム、それを提供するサプライヤにおいて必要なセキュリティについて整理する必要がある。コンポーネントやシステムに対しては、すでにグローバルな認証制度も立ち上がっていることから、整合性を図っていくことが求められる。また、コンポーネントやシステムのサプライヤの立場から、セキュアな製品を生産するためにどのようなプロセスを踏んで設計・実装するか、どのようなセキュリティを実装した製品を納品するか、納品後にどのようなサポートを行えばよいかといった点を考慮する必要がある。

3）Industrial Internet Security Framework

a. 概要

Industrial Internet Security Framework の概要は以下の通り。

表 2-12 Industrial Internet Security Framework

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 （脅威や対策）	エンドポイントにおけるセキュリティの脅威と脆弱性として以下の記載がある。 ・ ハードウェア構成の変更 ・ 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 ・ 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 ・ アプリケーションまたは API の不正な変更(ベアメタル／ネイティブ OS／ランタイム環境／コンテナ) ・ ディプロイ処理の脆弱性 ・ エンドポイントデータの意図せぬ変更 ・ 監視・分析システムの侵害 ・ 構成管理の脆弱性 ・ セキュリティモデル＆ポリシーの制御されない変更 ・ 開発環境の脆弱性

b. セキュリティ要件の整理

セキュリティフレームワークの機能的視点として、最上位層に 4 つのコア・セキュリティ機能を規定している。

表 2-13 Industrial Internet Security Framework におけるコア・セキュリティ機能

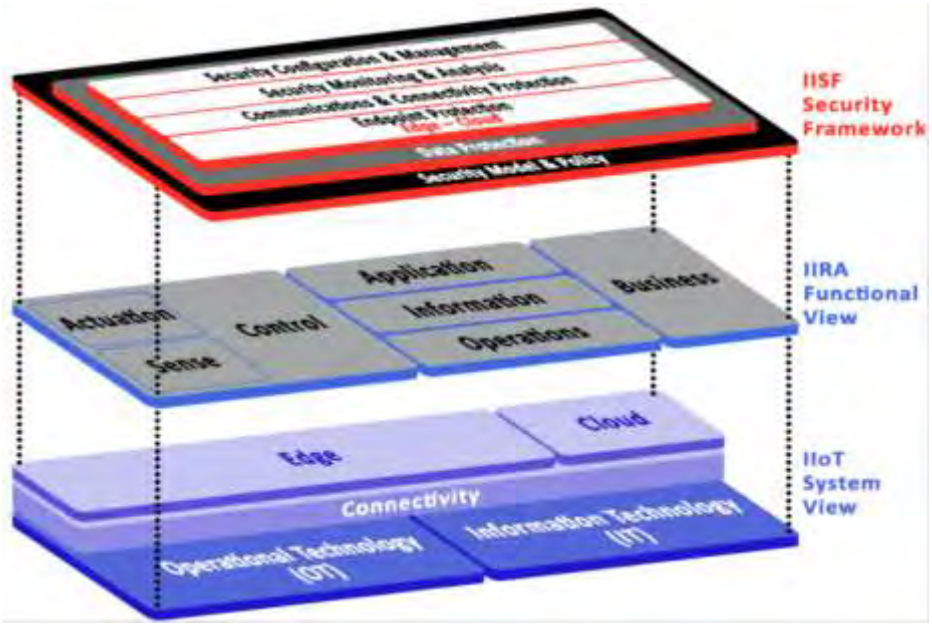
機能の項目	概要	機能内訳
1. エンドポイント保護	エンドポイント保護は、エンドポイントが実行する機能の可用性、機密性、完全性を保証する。	エンドポイント・物理セキュリティ エンドポイント・信頼の基点 エンドポイント・ID エンドポイント・完全性保護 エンドポイント・アクセス制御 エンドポイント・セキュア設定・管理 エンドポイント・監視・分析 エンドポイント・データ保護 エンドポイント・セキュリティモデル・ポリシー
2. 通信・接続保護	通信と接続性の保護では、エンドポイントのネットワークへの接続性を物理的に保護し、ネットワーク内の情報フローを保護し、エンドポイント間の通信を暗号的に保護する。	接続の物理的セキュリティ 通信のエンドポイント保護 暗号保護 情報フロー保護 ネットワーク設定・管理 ネットワーク監視・分析 ストリームデータの保護 通信と接続性の保護に関するセキュリティポリシー
3. セキュリティ監視・分析	セキュリティの監視と分析は、エンドポイントや接続トラフィックからシステム全体の状態に関するデータを取得し、それを分析してセキュリティ違反の可能性や潜在的なシステム脅	監視(エンドポイント・通信、セキュアな遠隔データロギング、サプライチェーン) 分析(振る舞い分析、ルールベース分析) アクション(先見・予測、反応・復旧、原因分析)

	威を検出する役割を担っている。	
4. セキュリティ設定・管理	セキュリティ設定・管理は、システムの運用機能（信頼性や安全性の動作を含む）と、その保護を確保するセキュリティ・コントロールの両方に対する変更のコントロールを担当する。	セキュアな運用管理 セキュリティ管理 エンドポイント ID 管理 エンドポイント設定・管理 通信設定・管理 セキュリティモデルの変更管理 設定・管理データ保護 変更管理のためのセキュリティモデルとポリシー

出所）Industrial Internet of Things Volume G4: Security Framework
（https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf）

c. 提示されているフレームワークやアーキテクチャ

セキュリティフレームワークの機能的視点は、相互に作用する 6 つのビルディングブロックで構成される。これらは３つの層に分かれており、最上位の層は、エンドポイント保護、通信・接続保護、セキュリティ監視・分析、セキュリティ構成管理の４つのコア・セキュリティ機能で構成される。この４つの機能を支えるのが、データ保護層とシステム全体のセキュリティモデルおよびポリシー層となる。

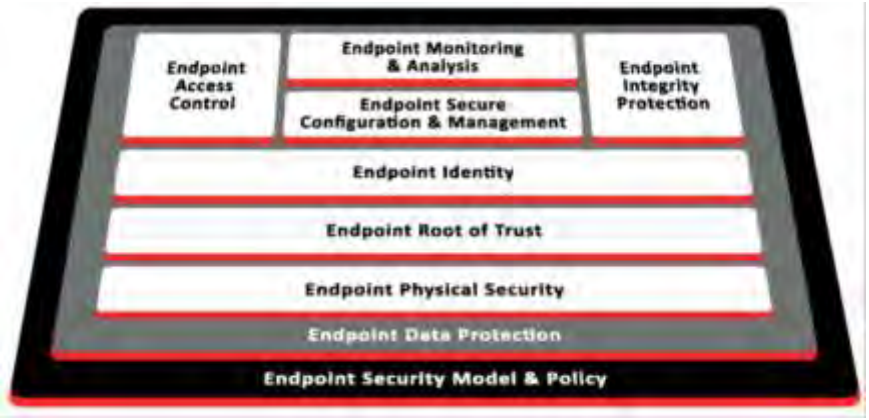


出所）Industrial Internet of Things Volume G4: Security Framework
（https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf）

d. ガイドライン策定にあたり検討すべき視点

「エンドポイント保護」では、「エンドポイント・認証の基点（Endpoint Root of Trust）」を機能の柱の一つとして取り上げている。Endpoint Root of Trust の考え方では、従来のセキュリティの考え方である境界型セキュリティによる対策の限界を踏まえ、いわゆるゼロトラストの概念により、ネットワークに接続されるすべてのデバイスが個々にセキュリティ対策を行い、多層的に防御することを想定する。こ

こでは、末端の IoT 機器等が信頼性を確保する根幹（信頼の起点）となることが求められる。機器におけるセキュリティ対策として、このような新しいセキュリティの概念について検討することが求められる。



出所）Industrial Internet of Things Volume G4: Security Framework
（https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf）

4）Cybersecurity Framework Version 1.1 Manufacturing Profile

a. 概要

Cybersecurity Framework Version 1.1 Manufacturing Profile の概要は以下の通り。

表 2-14 Cybersecurity Framework Version 1.1 Manufacturing Profile の概要

機関・タイトル	Cybersecurity Framework Version 1.1 Manufacturing Profile（NIST）
発行年	2020 年 10 月
概要	製造業向け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 の実装詳細を提供する。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。
対象読者	制御エンジニア、システム管理者、研究者など、製造システムのセキュリティに関わる様々な読者
記載事項 （脅威や対策）	CSF の製造業プロファイルは、製造者に次のような情報を提供する。 ・ 製造システムの現在のサイバーセキュリティ体制を改善する機会を特定する方法 ・ 統制環境を許容リスクレベルで運用する能力の評価 ・ 製造システムのセキュリティを継続的に保証するためのサイバーセキュリティ計画を作成するための標準的な手法 このプロファイルは、サイバーセキュリティ活動の最も基本的な機能を列挙した Cybersecurity Framework の主要機能分野を中心に構築されている。以下の 5 つの主要機能領域を定めている。 ・ 識別（Identify） ・ 保護（Protect） ・ 検知（Detect） ・ 対応（Respond） ・ 復旧（Recover） これらの主要機能分野は、定義されたリスクレベルである「低」、「中」、「高」において、メーカー固有またはセクター固有のプロファイルを作成するための出発点となる。

b. セキュリティ要件の整理

製造業に向けて、重要インフラで必須とされるサイバーセキュリティ活動と望ましい成果のセットであるフレームワーク・コアを定義している。フレームワーク・コアは、5 つの機能とそれぞれ対応するカテゴリーから構成される。

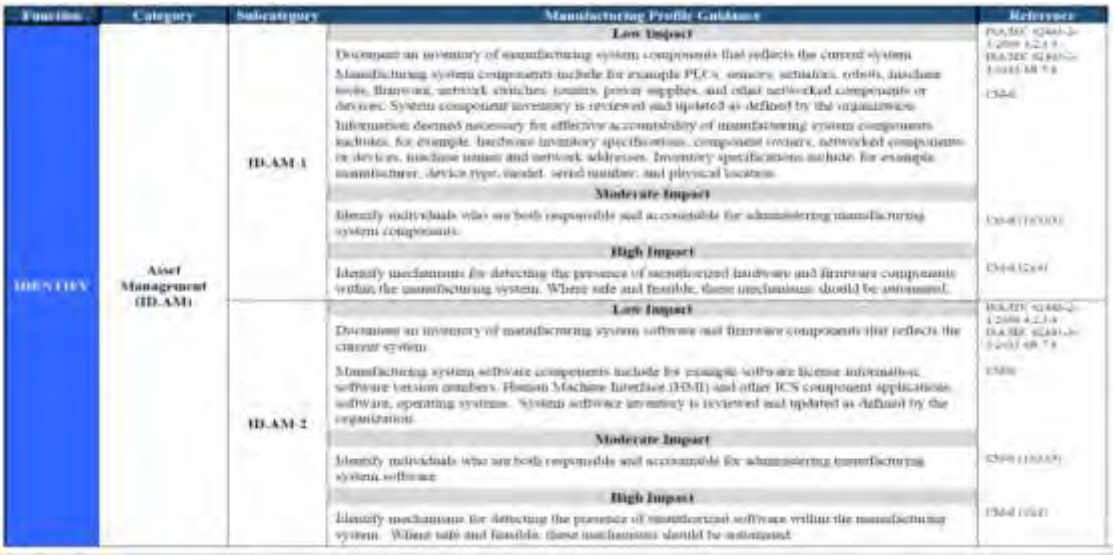
表 2-15 Cybersecurity Framework Version 1.1 Manufacturing Profile の 5 つの機能と対応カテゴリー

機能の項目	概要	カテゴリー
1. 識別	システム、資産、データ、能力に対するサイバーセキュリティリスクを管理するための組織的理解を深める。ビジネスコンテキスト、重要な機能をサポートするリソース、および関連するサイバーセキュリティリスクを理解することで、組織は、リスク管理戦略とビジネスニーズに沿って、その取り組みに焦点を当て、優先順位をつけることができる。	資産管理 ビジネス環境 ガバナンス リスク評価 リスク管理戦略 サプライチェーン管理
2. 防護	重要なインフラサービスを確実に提供するために、適切な保護手段を開発し、実施する。保護機能の活動は、潜在的なサイバーセキュリティイベントの影響を制限または抑制する能力をサポートするものである。	ID 管理・認証・アクセス制御 啓発・訓練 データセキュリティ 情報防護プロセス・手順 保守 防護技術
3. 検知	サイバーセキュリティイベントの発生を特定するための適切な活動を開発し、実施する。検出機能の活動は、サイバーセキュリティイベントのタイムリーな発見を可能にする。	異常な現象・イベント セキュリティの継続的なモニタリング 検知プロセス
4. 対応	検知されたサイバーセキュリティイベントに関して行動を起こすための適切な活動を策定し、実施する。潜在的なサイバーセキュリティイベントの影響を抑制する能力をサポートするものである。	対応計画 コミュニケーション 分析 軽減 改善
5. 復旧	復旧のための計画を維持し、サイバーセキュリティイベントによって損なわれた能力やサービスを回復するために、適切な活動を展開し、実施する。サイバーセキュリティイベントからの影響を軽減するために、通常のオペレーションへのタイムリーな復旧をサポートするものである。	復旧計画 改善 コミュニケーション

出所）Cybersecurity Framework Version 1.1 Manufacturing Profile
（https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf）

c. 提示されているフレームワークやアーキテクチャ

サイバーセキュリティフレームワークでは、5 つの機能（Funtion）と対応する 23 のカテゴリー、さらにサブカテゴリーに分類し、セキュリティリスクが及ぼすインパクトの大きさ（Low/Moderate/High）に応じて必要な対応策を定めている。



Function	Category	Subcategory	Manufacturing Profile Guidance	Reference
IDENTIFY	Asset Management (ID.AM)	ID.AM-1	**Low Impact** Document an inventory of manufacturing system components that reflects the current system. Manufacturing system components include for example PLCs, sensors, actuators, robots, machine tools, firmware, network switches, routers, power supplies, and other networked components or devices. System component inventory is reviewed and updated as defined by the organization. Information deemed necessary for effective accountability of manufacturing system components includes, for example, hardware inventory specifications, component owners, networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location. **Moderate Impact** Identify individuals who are both responsible and accountable for administering manufacturing system components. **High Impact** Identify mechanisms for detecting the presence of unauthorized hardware and firmware components within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	
		ID.AM-2	**Low Impact** Document an inventory of manufacturing system software and firmware components that reflects the current system. Manufacturing system software components include for example software license information, software version numbers, Human Machine Interfaces (HMI) and other ICS component applications software, operating systems. System software inventory is reviewed and updated as defined by the organization. **Moderate Impact** Identify individuals who are both responsible and accountable for administering manufacturing system software. **High Impact** Identify mechanisms for detecting the presence of unauthorized software within the manufacturing system. Where safe and feasible, these mechanisms should be automated.	

出所）Cybersecurity Framework Version 1.1 Manufacturing Profile
（https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf）

d. ガイドライン策定にあたり検討すべき視点

5 つの機能と対応する 23 のカテゴリー及びそれ以下のサブカテゴリーに分類し、セキュリティリスクが及ぼすインパクトの大きさに応じて必要な対応策を定めている。また、潜在的なインパクトについていくつかの例示も行っている。マニュファクチュアリングを対象としたプロファイルであるため、インパクトや対策の検討に際し参照可能と考えられる。

Table 7 Manufacturing System Impact Levels [3]

Impact Category	Low Impact	Moderate Impact	High Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization	Loss of life or limb
Financial Loss ($)	Tens of thousands	Hundreds of thousands	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Production	Temporary reductions without impacting quarterly production	Temporary reductions requiring additional shifts or overtime to meet quarterly production	Significant reduction and impact to meet quarterly production
Public Image	Temporary damage	Lasting damage	Permanent damage

出所）Cybersecurity Framework Version 1.1 Manufacturing Profile
（https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf）

5）Guidelines for Securing the Internet of Things

Guidelines for Securing the Internet of Things の概要は以下の通り。

a. 概要

表 2-16 Guidelines for Securing the Internet of Things

機関・タイトル	Guidelines for Securing the Internet of Things（ENISA）
発行年	2020 年 11 月
概要	IoT 製品やサービスのサプライチェーンの全体を俯瞰して、IoT 専門家の意見を取り入れ要件や設計から最終用途やメンテンナスさらに廃棄に至るライフスパン全体に関するサイバーセキュリティのガイドラインを作成する。セキュリティ上の考慮事項とグッドプラクティスも特定する。
対象読者	IoT の専門家、ソフトウェア開発者、製造者、情報セキュリティの専門家、IT／セキュリティソリューションアーキテクト、最高情報セキュリティ責任者（CISO）,重要情報インフラ保護（CIIP）の専門家、プロジェクトマネージャ、調達チーム
記載事項 （脅威や対策）	本調査の範囲は、IoT サプライチェーンのすべての段階を含み、あらゆる IoT 製品やサービスの全ライフスパン（構想から最終顧客への供給、製品ライフサイクルの終了まで）に関わる組織、人、技術、プロセス、情報、その他の物理および仮想リソースの全体的システムとして定義されている。 以下のリストには、スコープ内で検討された IoT サプライチェーンのステージが含まれている。 1. 製品設計 2. 半導体製造 3. 部品製造 4. IoT プラットフォーム開発 5. 部品組立・組込ソフトウェア 6. デバイスプログラミング 7. 流通・ロジスティクス 8. サービス提供、エンドユーザーによる運用 9. 技術サポート・保守 10. デバイスの回収と再利用

b. セキュリティ要件の整理

IoT のサプライチェーンの文脈で最も関連性が高いと考えられる一連の脅威を示す。

表 2-17 Guidelines for Securing the Internet of Things で示される脅威

	物理的攻撃（故意・計画的）	説明
1.1	妨害行為	悪意を持った攻撃は、問題を引き起こす可能性のある欠陥を挿入することができ、後工程で製品の全停止や故障が発生
1.2	グレーマーケット	正規の流通経路ではないところで、信頼性の低い不良製品が厳格なセキュリティと品質管理に問題を起こす可能性
1.3	不適切な物理的改ざんによる悪用	物理的破壊や使用しないメンテンスポートの悪用する可能性
	知的財産の損失	説明
2.1	知的財産の盗難	知財の機密情報の不正な取得・悪用。隠ぺいによるセキュリティ戦略
2.2	リバースエンジニアリング	悪意を持ったリバースエンジニアリングによる脆弱性等の暴露
2.3	契約外生産とクローン製品	正規製品に見えるが、安全性に欠けサプライチェーンへの脅威

	不正行為	説明
3.1	電磁波攻撃	ユニットに電磁波で干渉しメモリの破壊や情報漏洩の可能性
3.2	マルウェアの挿入	IoT ゲートウェイ介してデバイスに悪意あるソフトウェアを挿入
3.3	デバッグインターフェースの利用	開発・デバッグポートから IoT デバイスのプログラムを書き換えられるとメンテナンスにとって重要だがセキュリティの綻びの可能性
3.4	改ざん、偽造品(模造品)	不正改造ボードや不正チップ等の非正規サプライヤの製品の利用
	法的事項	説明
4.1	規格・規制への不適合による影響	サプライチェーンのセキュリティ面は、それぞれ異なる理解を持っているので、すべてのデバイスは、各業界で義務付けられているセキュリティガイドラインに準拠の必要性。
	意図しない情報の損傷または損失	説明
5.1	ネットワークの危殆化	適切な QoS やファイアウォールのポリシー設定の必要性
5.2	工場出荷時の認証設定の使用	固定したグローバルなデフォルト認証情報での出荷を回避
5.3	デバイスの予期せぬ障害	ハード、ソフトの問題の早期発見の広範囲な監視の必要性
5.4	ユーザのエラー	意図的でないヒューマンエラーによるセキュリティリスク
5.5	デバイスのライフサイクルにおける技術進化	ライフサイクルの長期化と技術進化による脆弱性の発見
5.6	パッチ未適用の機器・システムの使用	初期の段階で考慮されなかった脆弱性による脅威
5.7	クラウドサービスの中断	サービスベンダーの倒産等によるサービスの停止
5.8	復旧手順の失敗	IoT デバイスの復旧は、複数の資産の更新が必要になる場合があるので、どのプロセスに従うかの定義が必要
5.9	登録手続きへの攻撃	登録手順の不備や安全でない場合、攻撃者が不正なデバイスの登録や真正なデバイスの登録の阻止をする攻撃
5.10	回収・再利用部品の使用	廃棄部品をコスト最適化の理由で再投入すると検証がされない部品は、脅威となり、システムの汚染する可能性
5.11	製造工程への攻撃	製造工程は機密性が高く、アクセスを規制・監視する適切な対策を実施しないことによる深刻な脆弱性

出所)The European Union Agency for Cybersecurity(ENISA)「Guidelines for Securing the Internet of Things 」
(https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things(2022 年3月 1 日))

表 2-18 Guidelines for Securing the Internet of Things で示される脅威と該当する対応の例示

	脅威の整理軸	該当する対応の例示
1	物理的攻撃(故意・計画的)	物理的な破壊や物理的な改ざんを伴う脅威 信頼性の劣化した不良品の使用 使用していないメンテナンスポートの悪用
2	知的財産の損失	重要なデータの漏洩 リバースエンジニアリング ノウハウの流出
3	脅威の整理軸	悪意を持ったネットワークへの侵入 マルウェアの挿入 電磁波による攻撃
4	法的事項	規格・規制との不整合から生じる障害
5	意図しない情報の損傷または損失	ヒューマンエラー クラウドサービスの中断 リカバリー手順のミス 工場出荷時の設定の脆弱性

c. 提示されているフレームワークやアーキテクチャ

IoT のサプライチェーンを物理的側面と論理的側面の2面から捉えている。物理的側面は、サプライチェーンの各フェーズを移動する全ての物理オブジェクトと関連する手動のプロセスが関連し、論理的側面は、ソフトウェアの開発と展開、ネットワーク通信、IoT のオブジェクトとサプライチェーン関係者の仮想的な相互作用が含まれる。

出所)The European Union Agency for Cybersecurity(ENISA)「Guidelines for Securing the Internet of Things」(https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things(2022 年3月 1 日))

図 2-8 IoT サプライチェーンにおけるリファレンスモデル

d. ガイドライン策定にあたり検討すべき視点

IoT のライフサイクル全般にわたる過程のセキュリティに対するガイドラインとして整理されている。工場等の製造現場では IoT 機器も利用されており、想定される脅威の整理や、ライフサイクルを考慮した対策を検討するために参照可能である。

6)Industry 4.0 Cybersecurity : Challenges & Recommendations

a. 概要

Industry 4.0 Cybersecurity : Challenges & Recommendations の概要は以下の通り。

表 2-19 Industry 4.0 Cybersecurity : Challenges & Recommendations の概要

機関・タイトル	Industry 4.0 Cybersecurity : Challenges & Recommendations（ENISA）
発行年	2019年5月
概要	インダストリー4.0 および産業用 IoT のセキュリティやセキュリティ対策の採用における主な課題を特定するために実施されたギャップ分析の結果を提供している。さらにインダストリー4.0 のサイバーセキュリティの課題をステークホルダーに対する提言として整理している。
対象読者	IoT オペレータ、OT（運用・制御技術）および IT セキュリティ専門家、規制機関、国際組織および標準化コミュニティのメンバー、学術研究開発期機関
記載事項 （脅威や対策）	インダストリー4.0 のサイバーセキュリティを促進し、関連するイノベーションをセキュアな方法で幅広く普及させるために、様々な利害関係者グループへの概念レベルの提言を記している。 ENISA の調査「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」に基づき、インダストリー4.0 および産業用 IoT のセキュリティやセキュリティ対策の採用における主な課題を特定するために実施されたギャップ分析の結果を提供している。 さらに、インダストリー4.0 のサイバーセキュリティ及び関連するイノベーションを普及するために、ステークホルダーへの提言を記載している。

b. セキュリティ要件の整理

インダストリー4.0 のサイバーセキュリティに関連する問題へ全体的かつ包括的にアプローチで「課題」と「提言」を、「人」、「プロセス」および「技術」のカテゴリー毎に関連付を整理している。

表 2-20 「人」「プロセス」「技術」の課題と提言

	人の課題	提言
A1	IT/OT セキュリティの専門知識・意識を醸成、連携する必要がある	IT および OT セキュリティの分野横断的（cross-functional）な知識の習得を促進する
A2	組織のポリシーが不完全で、セキュリティへの投資に消極的である	インダストリー4.0 セキュリティの経済的および経営上のインセンティブを促進する
	プロセスの課題	提言
B1	インダストリー4.0 製品のライフサイクルに対する法的責任が十分定義されていない	インダストリー4.0 の当事者間の法的責任を明確にする
B2	インダストリー4.0 技術標準の分断化	インダストリー4.0 のセキュリティ標準類の取り組みを統合させる
B3	サプライチェーン管理の複雑さ	サプライチェーン管理プロセスをセキュアにする
	技術の課題	提言
C1	インダストリー4.0 機器、プラットフォーム、およびフレームワークの相互運用性	セキュリティの相互運用性のためのインダストリー4.0 のベースラインを確立する
C2	インダストリー4.0 とスマートマニュファクチャリングを妨げている技術的な制約	インダストリー4.0 セキュリティの確保のための技術的対策の適用

出所）The European Union Agency for Cybersecurity（ENISA）「Good practices for security of IoT」（https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1（2022 年3月 1 日））

出所）独立行政法人 情報処理推進機構（IPA）「インダストリー4.0 サイバーセキュリティ：課題と提言」
（https://www.ipa.go.jp/files/000074696.pdf）

表 2-21 インダストリー4.0 のサイバーセキュリティに関連する「提言」とステークホルダーとの関係

	提言	OT および IT セキュリティ専門家	IoT オペレータ	規制機関	国際組織および標準化コミュニティのメンバー	学術研究開発機関
A1	IT および OT セキュリティの分野横断的な知識の習得を促進する	○	○			○
A2	セキュリティの経済的および経営上のインセンティブを促進する		○	○		
B1	インダストリー4.0 の当事者間の法的責任を明確にする		○	○		
B2	インダストリー4.0 のセキュリティ標準類の取り組みを統合させる		○		○	
B3	サプライチェーン管理プロセスをセキュアにする	○	○			
C1	セキュリティの相互運用性のためベースラインを確立する	○	○	○	○	○
C2	セキュリティの確保のための技術的対策の適用	○	○			

出所）The European Union Agency for Cybersecurity（ENISA）「Industry 4.0 Cybersecurity : Challenges & Recommendations」
（https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations（2022 年3月 1 日））

c. 提示されているフレームワークやアーキテクチャ

フレームワークやモデルは示されていない。

d. ガイドライン策定にあたり検討すべき視点

対策を推進する当事者となるステークホルダーに対して、対策を紐づけている点が特徴的である。対策を整理する際に、対象を明確化することで、より具体的な取組みが推進されると考えられる。

また、ステークホルダーとして、規制機関、標準化コミュニティ、学術研究開発機関等が考慮されており、ガイドラインの普及・活用を念頭に置くと、工場等の製造現場のシステムに限らず、幅広いステークホルダーを考慮することも有効である。

7)Good Practices for Security of Internet of Things in the context of Smart Manufacturing

a. 概要

Good Practices for Security of Internet of Things in the context of Smart Manufacturing の概要は以下の通り。

表 2-22 Good Practices for Security of Internet of Things in the context of Smart Manufacturing の概要

<table>
<tr><td>機関・タイトル</td><td>Good Practices for Security of Internet of Things in the context of Smart Manufacturing（ENISA）</td></tr>
<tr><td>発行年</td><td>2018年 11 月</td></tr>
<tr><td>概要</td><td>産業用システムとサービスの進化に関連するセキュリティとプライバシーの課題に取り組むもの。セキュリティとプライバシーの課題、脅威、リスク、および攻撃のシナリオをマッピングし、インダストリー4.0/スマートマニュファクチャリングにおける IoT のセキュリティ確保のためのグッドプラクティスを収集したもの。</td></tr>
<tr><td>対象読者</td><td>・IIoT の専門家、ソフトウェア開発、機器メーカー
・IIoT オペレータとユーザ
・OT（運用・制御技術）、IT セキュリティ専門家、ソリューションアーキテクト
・最高情報セキュリティ責任者（CISO）
・国際組織およびセキュリティコミュニティのメンバー
・学術研究開発機関</td></tr>
<tr><td>記載事項
（脅威や対策）</td><td>方法論的なアプローチによって、インダストリー4.0 とスマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティスに関する調査を実施。以下の章から構成されている。
- 第 1 章：調査の目的、範囲、背景、対象読者、方法論、文書の構成に関する序論的情報
- 第 2 章：インダストリー4.0 とそのコンポーネントの定義。概念と関連するセキュリティ上の課題。
- 第 3 章：脅威の分類とインダストリー4.0 /スマートマニュファクチャリングの攻撃シナリオの例を含む脅威とリスクの分析。
- 第 4 章：脅威、セキュリティドメイン、標準、その他の関連文書にマッピングされたセキュリティ対策とグッドプラクティスの説明。

<table><tr><td colspan="2">セキュリティ上の課題</td></tr><tr><td>1. 脆弱なコンポーネント</td><td>7. セキュアでないプロトコル</td></tr><tr><td>2. プロセス管理</td><td>8. ヒューマンファクタ</td></tr><tr><td>3. 接続性の向上</td><td>9. 未使用の機能</td></tr><tr><td>4. IT／OT の融合</td><td>10. セーフティ</td></tr><tr><td>5. サプライチェーンの複雑さ</td><td>11. セキュリティの更新</td></tr><tr><td>6. レガシーな ICS</td><td>12. セキュアな製品ライフサイクル</td></tr></table></td></tr>
</table>

b. セキュリティ要件の整理

スマートマニュファクチャリングにおける IoT セキュリティにおける資産分類を行った上で、インダストリー4.0 環境における脅威の分類を提示している。その上で、12 の IIoT の攻撃のシナリオを提示し、想定される影響を示している。

スマートマニュファクチャリングにおける IoT セキュリティの対策については、広範囲の机上リサーチ

及び利害関係者とのインタビューに基づき 20 の領域のリストを作成し、そのセキュリティ対策／グッドプラクティスを「ポリシー」、「組織的対策」、「技術敵対策」の 3 つのグループで整理している。

表 2-23 「ポリシー」「組織的対策」「技術」毎のセキュリティ対策／グッドプラクティス

ポリシー	説明
セキュリティ・バイ・デザイン	製品開発の最初から適用されるべきセキュリティ対策。
プライバシー・バイ・デザイン	プライバシーと個人データの保護に関連するセキュリティ対策。
資産管理	資産の発見、管理、監視および保守に関するセキュリティ対策。
リスクと脅威の管理	リスクおよび脅威管理のプロセスへの推奨アプローチに関するセキュリティ対策。
組織的対策	説明
エンドポイントライフサイクル	製品（エンド機器およびインフラを含む）ライフサイクルのさまざまな段階におけるセキュリティに関連する対策
セキュリティアーキテクチャ	アーキテクチャベースのアプローチでセキュリティアーキテクチャ確立に関するセキュリティ対策。
インシデント処理	発生する可能性のあるインシデントの検出と対応に関するセキュリティ対策。
脆弱性管理	脆弱性管理プロセスおよび脆弱性の開示に関するセキュリティ対策。
トレーニングと意識向上	従業員の意識向上に関する推奨アプローチに関するセキュリティ対策
第三者組織の管理	第三者組織の管理および第三者組織のアクセス制御に関連するセキュリティ対策。
技術的対策	説明
信頼性と完全性の管理	データと機器の完全性と信頼性を保証するのに役立つセキュリティ対策
クラウドのセキュリティ	クラウドサービスのさまざまなセキュリティの側面に関するセキュリティ対策
事業継続および復旧	レジリエンスと業務の継続性を確保するための企業の計画の策定、テストおよびレビューに関するセキュリティ対策
機械間セキュリティ	機械間通信セキュリティにおけるキーストレージ、暗号化、入力検証、および保護に関するセキュリティ対策
データ保護	組織のさまざまなレベルにおける守秘データの保護およびデータへのアクセスの管理に関するセキュリティ対策
ソフトウェア/ファームウェアのアップデート	パッチの検証、テスト、および実行に関するセキュリティ対策
アクセス制御	リモートアクセス、認証、特権、アカウント、および物理アクセスの制御に関するセキュリティ対策。
ネットワーク、プロトコル、暗号化	適切なプロトコルの実装、暗号化、およびネットワークセグメンテーションを通じて、通信のセキュリティを確保
モニタリングと監査	ネットワークトラフィックと可用性の監視、ログ収集とレビューに関するセキュリティ対策。
構成管理	セキュリティ構成、構成の変更管理、機器の強化、およびバックアップ検証に関するセキュリティ対策。

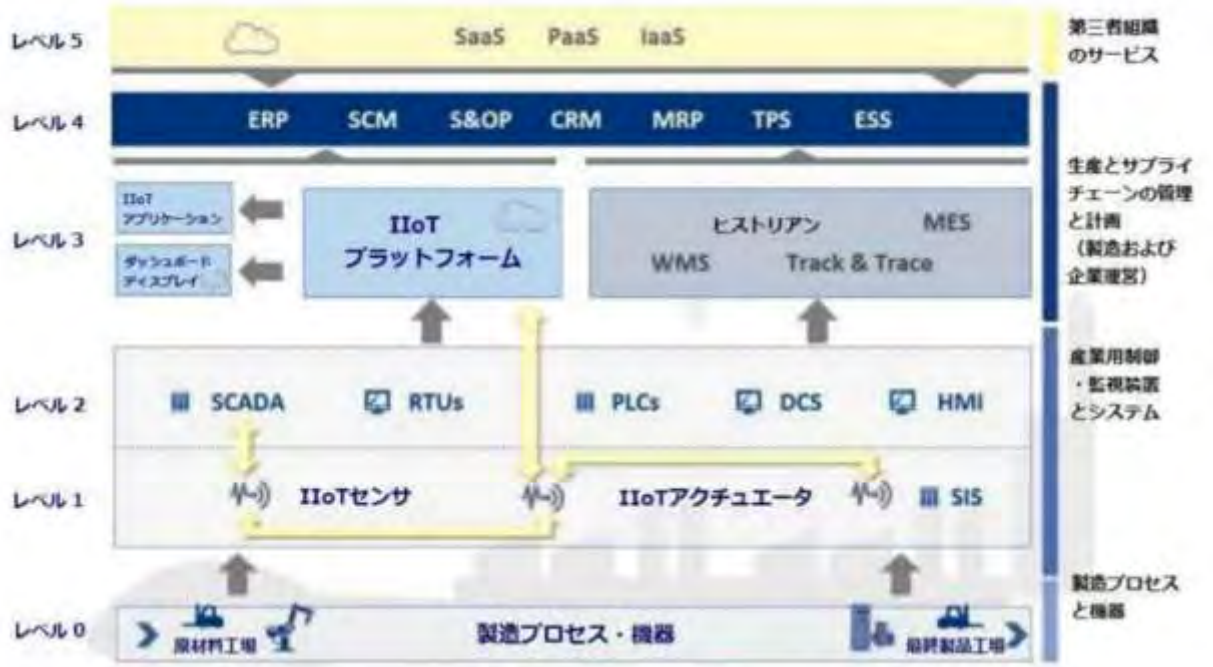
出所）The European Union Agency for Cybersecurity（ENISA）「Good practices for security of IoT」（https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1（2022 年3月 1 日））

出所）独立行政法人 情報処理推進機構（IPA）「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」（https://www.ipa.go.jp/files/000073490.pdf）

c. 提示されているフレームワークやアーキテクチャ

パデューモデル（パデュー大学コンソーシアムによって開発されたパデュー・エンタープライズリファレンスアーキテクチャ、ISA-95 で参照）に基づくリファレンスモデルが示されている。

このモデルは、スマートマニュファクチャリング環境を 6 つの階層に分けており、最も重要な資産とコンポーネントの関係を説明している。灰色の矢印がグループ間の通信経路を表しており、インダストリー4.0 で可能となった新しい通信経路（IIoT 機器間の通信、IIoT 機器と IIoT プラットフォームへの接続）が黄色の矢印で示されている。



出所）独立行政法人 情報処理推進機構（IPA）「スマートマニュファクチャリングにおける IoT セキュリティのグッドプラクティス」（https://www.ipa.go.jp/files/000073490.pdf）

図 2-9 リファレンスモデル

d. ガイドライン策定にあたり検討すべき視点

本ドキュメントで示されているセキュリティ対策/グッドプラクティスを参照することはもちろん、脅威の分類に基づき、スマートファクトリーにおける攻撃シナリオを整理し、脅威の重要度や影響を示していることから、工場等の製造現場において考慮すべきリスクの検討に際し、参考になると考えられる。

8）Baseline Security Recommendations for IoT

a. 概要

Baseline Security Recommendations for IoT の概要は以下の通り。

表 2-24 Baseline Security Recommendations for IoT の概要

<table>
<tr><td>機関・タイトル</td><td>Baseline Security Recommendations for IoT（ENISA）</td></tr>
<tr><td>発行年</td><td>2017 年 11月</td></tr>
<tr><td>概要</td><td>IoT のセキュリティ要件として、IoT 資産の分類、脅威とリスクの分析に基づき、「ポリシー」「組織的、人的、運用的対策」「技術的対策」を整理。</td></tr>
<tr><td>対象読者</td><td>・IoT のソフトウェア開発者、製造者
・IoT の専門家
・情報セキュリティの専門家
・IT／セキュリティソリューションアーキテクチャ
・最高情報セキュリティ責任者（CISO）
・重要情報インフラ保護（CIIP）の専門家</td></tr>
<tr><td>記載事項
（脅威や対策）</td><td>IoT に必要となる一連のベースラインセキュリティを提言するもの。
IoT 資産に対する主な脅威及びリストアップをリストアップし、脅威と影響する資産を対応付けている。また、IoT 資産に対する主な攻撃シナリオを抽出し、関係者や専門家へのヒアリングにより、優先すべきシナリオを詳細に解説している。
以上の検討を元に、IoT のセキュリティ対策/グッドプラクティスを 83 要件にまとめており、現状とあるべき姿のギャップ（6 点）及び IoT セキュリティ改善のための提言（7 点）を提示している。

<table>
<tr><th>推奨する提言</th><th>推奨内容</th></tr>
<tr><td>1. IoT セキュリティの取り組みと規制の調和の推進</td><td>IoT に関する欧州共通のガイドラインやセキュリティ基準を確立し、関係者間の調和・調整を行う。また、ガイドラインや基準の導入を促進する。</td></tr>
<tr><td>2. IoT セキュリティの必要性の啓発</td><td>開発者、産業界、ユーザ等、それぞれの関係者ごとに、IoT に対する脅威とリスク、セキュリティを確保する方法について教育を行う。</td></tr>
<tr><td>3. セキュアなソフトウェア／ハードウェアの開発ライフサイクルに関するガイドラインの策定</td><td>セキュリティおよびプライバシーを考慮した製品・サービスの開発ライフサイクルを定義し、開発者およびメーカーの IoT 開発プロセスへの組込みを促進する。</td></tr>
<tr><td>4. IoT エコシステムの相互運用性に関するコンセンサスの確立</td><td>IoT デバイス、プラットフォーム、フレームワークの相互運用性を確保し、準拠するオープン且つ利用しやすい相互運用性の検証機関やテストヘッドを増やす。</td></tr>
<tr><td>5. IoT セキュリティを促進するための経済的・経営的インセンティブの提供</td><td>セキュリティとプライバシーを確保したうえで市場展開が推奨される。セキュリティフレームワークの策定と認証を利用するには、この方向性を進めることになります。</td></tr>
<tr><td>6. セキュアな IoT 製品／サービスのライフサイクルマネジメントの確立</td><td>メーカーは、設計・開発から製造終了、サポート終了まで、セキュリティを組み込んだ IoT 製品／サービスのライフサイクルマネジメントを確立する。</td></tr>
<tr><td>7. IoT 関係者の責任分界点の明確化</td><td>責任分界点について議論し、EU レベルおよび各加盟国の法規において明確化</td></tr>
</table>
</td></tr>
</table>

b. セキュリティ要件の整理

IoT のセキュリティ対策／グッドプラクティスを「ポリシー」、「組織、人、プロセス」、「技術」のカテゴリーで整理している。

表 2-25 「ポリシー」「組織、人、プロセス」「技術」毎のセキュリティ対策／グッドプラクティス

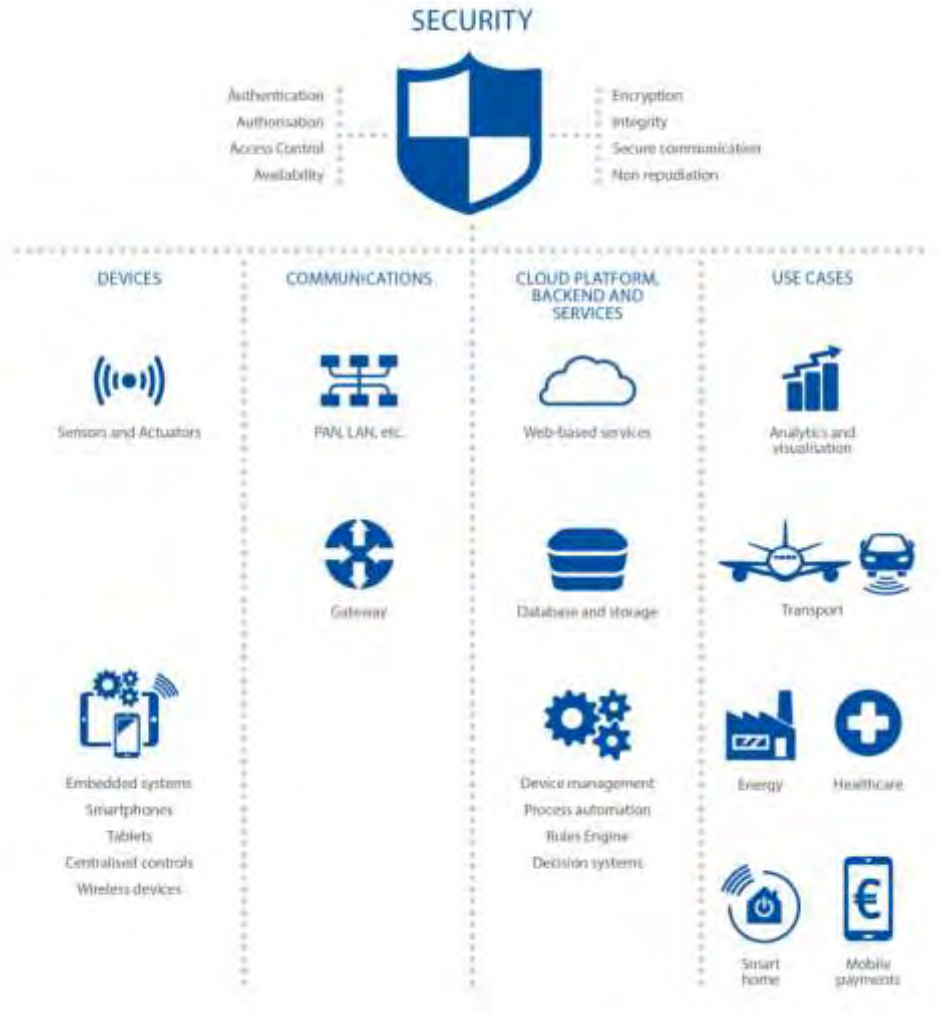
ポリシー(12要件)		主要な要件の概要
	セキュリティ・バイ・デザイン(7)	設計と開発のすべてのレベルにわたって、そのライフサイクル全体で、一貫したアプローチから IoT システム全体のセキュリティを考慮し、開発、製造、展開を通じてセキュリティを統合すること。 異なるセキュリティポリシーと技術を統合する能力を確保し、 IoT 開発者は、製品が期待した性能を検証するためのテスト計画を実施する。
	プライバシー・バイ・デザイン(2)	プライバシーをシステムの不可欠な部分。新しいアプリケーションを組み入れる前に、プライバシーへの影響評価を行う。
	資産管理(1)	ネットワーク及び情報システムの資産管理の手順と構成の確立・維持。
	リスクおよび脅威の特定と評価(2)	多層防御により、重大なリスクを特定する。IoT デバイスの使用目的及び環境を特定する。
組織的、人的、運用的対策(14要件)		主要な要件の概要
	製品ライフサイクルを通じたサポート(3)	IoT 製品の製品寿命の期間と終了時期を開示して戦略を策定。「サポート終了」時期まで、性能を監視し、既知の脆弱性にパッチを適用する。
	有効性が確認されているセキュリティ対策の利用(1)	実績と信頼がある通信プロトコルや暗号アルゴリズムなどを使用する。
	セキュリティ脆弱性／インシデント管理(4)	インシデントを分析し、処理するための手順を確立。脆弱性の報告と官民からサイバー脅威と脆弱性に関するタイムリーで重要な情報を受け取る。
	セキュリティ教育(3)	プライバシーとセキュリティの好事例を従業員に教育し、教育活動を文書化して、監視する。役割と責任を確立し人員の配置をおこなう。
	第三者組織とのセキュリティに関する取り決め(3)	第三者が処理するデータは、データ処理契約によって保護する。 IoT 開発者は、サイバーサプライチェーンリスク管理ポリシーを採用し、サプライヤ及びパートナーにサイバーセキュリティ要件を伝達する。
技術的対策(57要件)		主要な要件の概要
	ハードウェアセキュリティ(2)	機器の保護と完全性を強化するために、セキュリティ機能を組み込んだハードウェアを使用する。静止時および使用時の鍵の保護、セキュリティに敏感なコードへの非特権者のアクセスの防止。
	信頼性／完全性管理(5)	ブート環境での信頼は、他のいかなるソフトウェアやソフトウェアに対する信頼よりも先に確立する必要がある。安全なコードとして署名した後、改ざんされていないことを保証するために暗号的に署名する。
	堅牢なデフォルトセキュリティ／プライバシー設定(2)	適用可能なセキュリティ機能はすべてデフォルトで有効にし、未使用または安全でないものについては 機能はデフォルトで無効にする。
	データ保護／法規へのコンプライアンス(5)	個人情報は公正かつ合法的に収集・処理され、データ主体の同意なしに収集・処理されることがあってはならない。EU 一般データ保護規則(GDPR)に準拠する必要がある。
	システムの安全性／信頼性(3)	システムおよび運用が混乱した場合を考慮した設計を行い、システムは、人身事故や物理的な損害という許容できないリスクが生じることを防止する必要がある。
	セキュアなソフトウェア／ファームウェアアップデート(3)	デバイスのソフトウェア／ファームウェア、およびそのアプリケーションは、OTA(Over-The-Air)アップデート機能をする。アップデートサーバーは安全で、アップデートファイルは安全な接続を介して送信される。アップデートパッケージは、デバイスによって検証されたデジタル署名、署名証明書を持っている。
	認証(6)	初期設定時にデフォルトパスワードやデフォルトユーザ名が変更され、弱いパスワードや空白のパスワードが許可されないようにすること。 認証には強力なパスワードまたは個人識別番号(PIN)を使用し、二要素認証(2FA)または多要素認証(MFA)の使用を検討する必要。
	認可(2)	システムに最小特権の原則(PoLP)の認証メカニズムを実装し、許可さ

		れるアクションに制限をかける。デバイス・ファームウェアは、アクセスする必要の部分から分離するように設計されなければならない。
	アクセス制御(5)	特定のプロセスへのアクセスは、アクセス制御によって定義されたセキュリティポリシーを実施する必要がある。物理ポートをロックダウンして、信頼できる接続のみにする。
	暗号化(4)	データ及び情報の機密性、完全性を保護するために、暗号を適切に使用すること。標準的かつ強力な暗号化アルゴリズムと強力な鍵を適切に選択し、実装の堅牢性を検証する。暗号鍵は安全に管理する必要がある。
	セキュアで信頼のおける通信(9)	通信のセキュリティには、最先端の標準化されたセキュリティプロトコルを使用していることを確認する。内部または外部のネットワークトラフィックで認証情報が露出しないようにする。
	セキュアなインターフェース／ネットワークサービス(7)	ネットワーク要素を別々のコンポーネントに分割することで、セキュリティ侵害を分離し、全体的なリスクを最小化することができる。 製品群全体で同じ秘密鍵は避ける。必要なポートだけを公開する。
	セキュアな入力／出力処理(1)	データ入力の検証(使用前のデータの安全性確保)と出力フィルタリング。
	ログの取得(1)	ユーザ認証、アカウントやアクセス権の管理、セキュリティルールの変更、システムの機能に関するイベントを記録するログシステムを導入。
	監視／監査(2)	定期的な監視を実施し、機器の動作確認、マルウェアの検出、および 整合性エラーを発見する。セキュリティ管理の定期的な監査とレビューを実施し、管理が有効であることを確認する

出所)The European Union Agency for Cybersecurity(ENISA)「Baseline Security Recommendations for IoT」(https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/(2022 年3月 1 日))

c. 提示されているフレームワークやアーキテクチャ

既存の複数の IoT アーキテクチャから、コアとなる要素を抽出してリファレンスアーキテクチャを提示している。



出所）The European Union Agency for Cybersecurity（ENISA）「Baseline Security Recommendations for IoT」（https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/（2022 年3月 1 日））

図 2-10 リファレンスアーキテクチャ

d. ガイドライン策定にあたり検討すべき視点

「Good Practices for Security of Internet of Things in the context of Smart Manufacturing」の基礎となったドキュメントである。セキュリティ対策/グッドプラクティスや、IoT における攻撃シナリオ、脅威の重要度や影響について、リスクの検討に際して参考になる。

IoT は消費者向け製品を含む広い概念だが、IIoT は特に OT 環境で使用される。セーフティよりもユーザビリティに重点を置く IoT システムは、IIoT において OT 環境に固有のセキュリティ要件を満たす必要があることに留意が必要である。

表 2-26 IoT セキュリティにおける現状とあるべき姿のギャップ

	GAP の種類	主な GAP の理由
1	断片的なセキュリティアプローチや規制	関係者の責任分界が不明確であること等から、多くの企業やメーカーが独自のアプローチで IoT セキュリティに取り組む状況が生まれている。
2	セキュリティ意識の低さ	脅威が理解されておらず、セキュリティの必要性に対する認識が低いので、ユーザ、開発者、メーカー等に対しリスクおよび対策について教育する必要がある。
3	設計・開発におけるセキュリティの欠如	セキュリティ・バイ・デザイン、通信セキュリティの欠如や、既知の脆弱性へ未対応、不要なポート／サービスの開放、弱いパスワードの使用等がみられる。
4	IoT 機器、プラットフォーム、フレームワーク間の相互運用性の欠如	規制に対する意識の欠如から、多くの企業やメーカーが独自に開発を進め、相互運用性の問題が発生している。
5	経済的インセンティブの欠如	企業やメーカーはセキュリティよりも機能性やユーザビリティを重視しており、セキュリティに予算を掛けていない。
6	適切な製品ライフサイクルマネジメントの欠如	市場投入後の脆弱性対応や問題を早期に検知する仕掛けを含め、製品の適切なライフサイクルマネジメントが為されていない。

出所）The European Union Agency for Cybersecurity（ENISA）「Baseline Security Recommendations for IoT」（https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/（2022 年3月 1 日））

9）Recommendations for implementing the strategic initiative INDUSTRIE 4.0

a. 概要

Recommendations for implementing the strategic initiative INDUSTRIE 4.0 の概要は以下の通り。

表 2-27 Recommendations for implementing the strategic initiative INDUSTRIE 4.0 の概要

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
対象読者	インダストリー4.0 に関心を持つ人
記載事項 （脅威や対策）	CPS の戦略を実現するために以下 3 点が重要としている。 ・ バリューネットワークを通じての水平統合 ・ 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 ・ 垂直統合とネットワーク化された製造システム 特に優先して解決する 8 分野として以下を設定している。 ① 標準化と参照アーキテクチャ ② 複雑なシステムの管理 ③ 産業界のための包括的なブロードバンドインフラ

	④　安全とセキュリティ ⑤　業務組織と業務設計 ⑥　研修と継続的な専門家の育成 ⑦　制度的フレームワーク ⑧　資源効率 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として進めていく。

b. セキュリティ要件の整理

安全とセキュリティの分野で行動すべき 8 つの優先分野のリストを提示している。

表 2-28 安全とセキュリティの分野で行動すべき事項

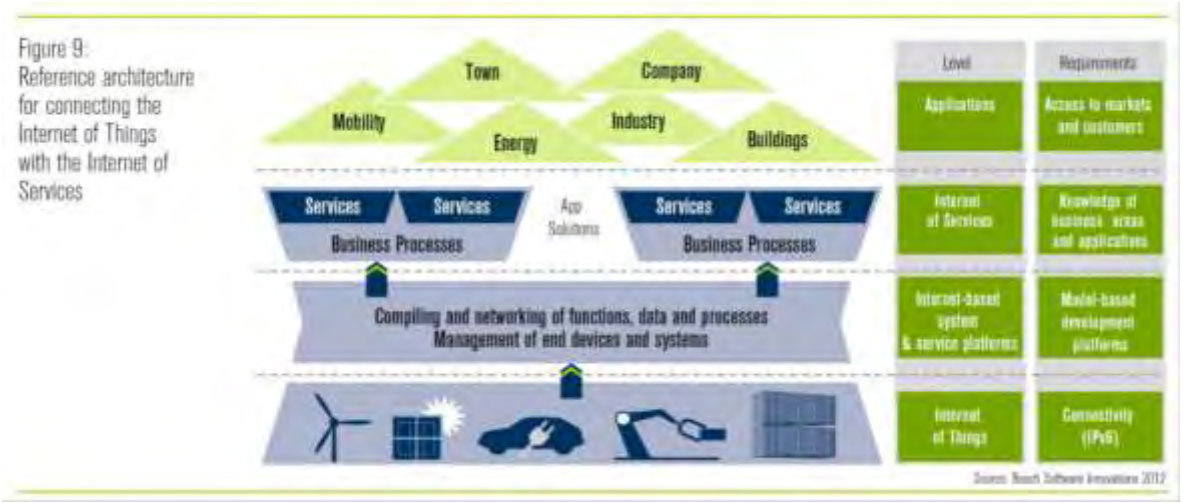
項目	概要
1. 統合された安全とセキュリティの戦略、アーキテクチャ、標準	システムのライフサイクル全体を通して、関連する原則や手法を体系的に適用するとともに、安全性とセキュリティの戦略を変更する必要がある。このアプローチの基礎として、共通の「知識プール」を開発する必要がある。
2. 製品、プロセス、機械のためのユニークで安全な ID	製造プロセス全体での安全な情報交換が鍵となる。これは、機械、そのコンポーネント、交換されるデータ、影響を受けるプロセス、関係する組織単位に適用される。この交換を可能にするためには、個々の機械、プロセス、製品、コンポーネント、材料が固有の電子 ID を持つことが必要である。
3. Industrie3.0 から Industrie4.0 への移行戦略	移行戦略では、既存設備の現状評価に加えて、個々のセキュリティソリューションを迅速かつ実用的に、そしてコスト効率よく導入できる標準化されたプロセス・モデルの開発が必要となる。このプロセスは、個々のセキュリティ目標の定義、弱点と脅威を特定するための状況分析、その後に実施される対策のリストの確立に基づいて、既存の(一般的な)IT セキュリティプロセスを適応することによって到達することができる。
4. ユーザーフレンドリーな安全・セキュリティのソリューション	ユーザのニーズに合った、ユーザーフレンドリーなインターフェースを持ち、アプリケーションの実行を保証する安全・セキュリティソリューションを開発する必要がある。これらの要素は、初期の設計段階から、エンジニアリング、運用、そしてメンテナンスに至るまで考慮されなければならない。
5. 企業経営面からの安全・セキュリティ	機械が故障すると、直接的な影響だけでなく、間接的な影響(損害賠償請求、企業イメージの低下など)も生じる。しかし、IT トラブルによる損害を補償する保険に加入しているメーカーはほとんどなかった。リスクを明確に算出し、IT 脅威が発生した場合やその疑いがある場合に製造施設を停止するという選択肢と比較して、関連するセキュリティソリューションの費用対効果を明確に算出できる方法を開発する必要がある。
6. 製品の違法コピーに対するセキュリティ防護	インダバリューネットワークにおけるさまざまなパートナー間の協力関係がより高度になることから、製品の海賊版に対する保護がさらに重要になる。そのため、技術的なレベル、特に会社法や競争法のレベルで、プラットフォーム内の信頼性と透明性を保証すると同時に、重要なビジネスノウハウを保護するためのソリューションを見つけることが必要である。
7. 訓練と社内教育	IT セキュリティに関する知識は、組織を構成するすべての人にとって不可欠なものであり、生産に関わるすべての人の意識を高めることが重要である。企業にセキュリティソリューションを導入する場合、単に技術的な製品を導入するだけでは十分ではなく、たとえそれが使いやすいものであったとしても、従業員は関連するセキュリティ要件に関して適切なトレーニングを受ける必要がある。
8. データ保護のためのコミュニティ形成	例えば、スマートファクトリーの機械やスマートアシスタンスシステムを介して、従業員の健康に関する情報を記録・分析することが技術的に可能になるため、産業界ではより厳しいデータ保護の取り決めが必要になる。個人情報の利用は、情報

	の自己決定権を重視するドイツでは、特にデリケートな問題である。

出所）Recommendations for implementing the strategic initiative INDUSTRIE 4.0
（https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/download-pdf）

c. 提示されているフレームワークやアーキテクチャ

IoT とインターネットサービスを接続する際のリファレンスアーキテクチャ挙げている。



出所）Recommendations for implementing the strategic initiative INDUSTRIE 4.0
（https://en.acatech.de/publication/recommendations-for-implementing-the-strategic-initiative-industrie-4-0-final-report-of-the-industrie-4-0-working-group/download-pdf）

図 2-11 リファレンスアーキテクチャ

d. ガイドライン策定にあたり検討すべき視点

安全とセキュリティの分野で行動すべき 8 つの優先分野として、いくつかの視点を提示している。両者は密接に関わる部分もあることから、ガイドライン策定において安全面についても配慮することや、安全と一体となったセキュリティ設計やセキュリティ対策を検討することが有効と考えられる。

上述の優先分野の一つに「ユーザーフレンドリーな安全・セキュリティのソリューション」が挙げられている。初期の設計段階から、セキュリティ・バイ・デザインの一環として、ユーザーフレンドリーな形でのソリューション設計を志向することが有効であると考えられる。また、「企業経営面からの安全・セキュリティ」が挙げられている。ここでは、セキュリティ上の脅威とその対策について、定量的に評価した上で経営を行う必要があることを示唆している。

10） Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0（Plattform Industrie 4.0）

a. 概要

Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0 (Plattform Industrie 4.0)の概要は以下の通り。

表 2-29　Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0 の概要

機関・タイトル	Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0 （BITKOM 、VDMA、ZVEI）
発行年	2015 年 4 月
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 （脅威や対策）	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。 ■　研究と革新 ・　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） ・　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） ・　垂直統合とネットワーキング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） ・　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） ・　分野横断的技術の継続的開発 ■　リファレンスアーキテクチャ、標準化、規格化 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） ■　ネットワーキングされたシステムの安全性 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。 以下に模範的なセキュリティ対策案を示す。 ・　セキュリティアーキテクチャ ・　アイデンティティ管理 ・　暗号-機密性の保護 ・　暗号-整合性の保護 ・　安全な遠隔アクセスと頻繁な更新 ・　プロセスと組織的措置 ・　企業全体を網羅

b. セキュリティ要件の整理

インダストリー4.0 の安全目標とセキュリティ要件を定めている。

表 2-30　安全目標とセキュリティ要件

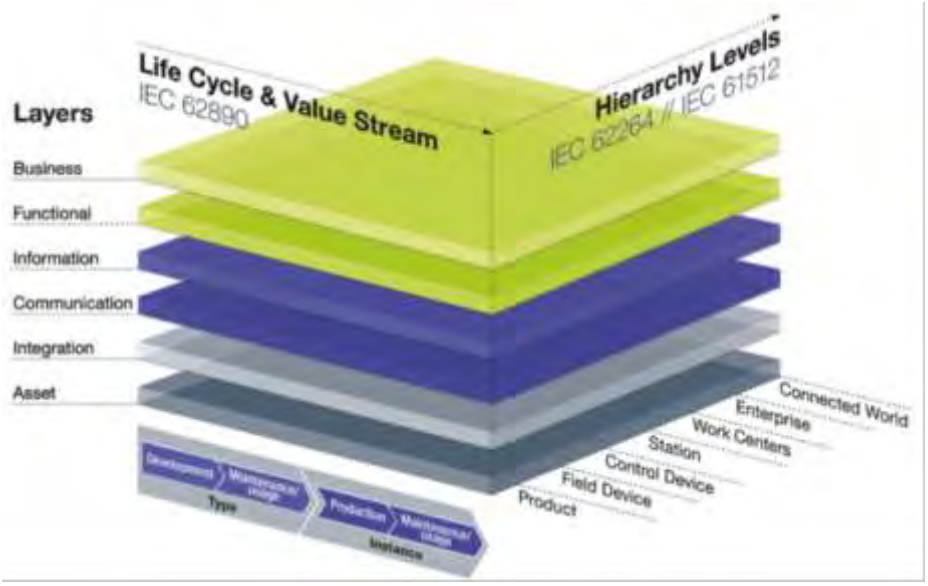
項目	概要
1.　一般的な目標	可用性／完全性／ノウハウ保護・機密性／真正性／バリューチェーンでのトレーサビリティ／法的安定性

2. インダストリー4.0 のセキュリティ・バイ・デザイン	技術的メカニズムを後からセキュリティに組み込むのではなく、製品開発およびプロセスにおける装置・インフラ保護のための統合的アプローチが必要となる。必要なセキュリティ機能を製品ないしソリューションに一体化した形で実装する。
3. ID 管理	機械／ユーザ／製品がバリューネットワークに参加するために必要なのが、ユニークで改ざん不可能な ID であり、それは電子証明書によって表現される。電子証明書には認証用の鍵のほか，暗号化と復号に必要な情報が含まれている。
4. バリューネットワークの動的構成	効率的なバリューネットワークには，システムの動的な構成／再構成が必要となる。コンポーネントのセキュリティ特性（セキュリティプロファイル）を標準化された言語を用いて記述する必要がある。その中には通信インターフェース／通信プロトコルとそのセキュリティ特性の記述も含まれる。セキュリティプロファイルは、動的に変化するバリューネットワークに求められる柔軟性を、適切な保護機能でサポートできるものでなければならない。
5. 仮想インスタンス用のセキュリティ	製品の「仮想インスタンス」が重要な役割を果たすため、仮想イメージのセキュリティも必要となる。「仮想インスタンス」の配置（オフィスプラットフォームまたはクラウド）によっては、セキュリティ環境条件が物理的な実装と異なってくる。従来のセキュリティの境界線をそのまま「仮想モデル」 にマッピングすることはできなくなる。エンドツーエンドのセキュリティが重要な項目となる。
6. 予防と対応	予防的な保護対策に加え、対応のメカニズムも必要である（監視／イベント処理／インシデント管理）。脅威の状況は、潜在的な攻撃者の新たな技術的可能性や、標準的な製品やコンポーネントの脆弱性の発見・公開によって、継続的に変化する。メーカーやオペレータは、パッチやアップデートでこれに対応できなければならない。
7. 啓発、教育、訓練	セキュリティ対策とその必要性についての認識を高めるために、関係者を対象とした意識向上トレーニングを、関係するすべての組織で行わなければならない。
8. ハンドリング性	豊富な予備知識がなくても、産業用セキュリティ機能を操作できること。Plug & Operate は、特にセキュリティソリューションにおいて目指すべきものである。
9. 規格、仕様	国際規格 IEC62443 では、4 つのセキュリティレベルに基づいて産業用セキュリティの評価基準を定めたフレームワークを提供している。VDI ガイドライン 2182 で知られる産業オートメーションにおける情報セキュリティの手順モデルは、部品メーカー、機械メーカー、オペレータの活動を相互に結びつけている。

出所）Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0（https://www.bitkom.org/sites/default/files/file/import/150410-Umsetzungsstrategie-0.pdf）

c. 提示されているフレームワークやアーキテクチャ

インダストリー4.0 リファレンスアーキテクチャモデル（RAMI4.0）を示している。縦軸には、データイメージ、機能、通信、資産、ビジネスプロセスなどの異なる視点を表すためにレイヤーを用いている。横軸には、製品ライフサイクルとその中に含まれる各種の価値連鎖の状況を表している。第三の軸は工場/装置内の機能および責任のマッピングである。



出所）Umsetzungsstrategie Industrie 4.0 Ergebnisbericht der Plattform Industrie 4.0」 https://www.bitkom.org/sites/default/files/file/import/150410-Umsetzungsstrategie-0.pdf

d. ガイドライン策定にあたり検討すべき視点

インダストリー4.0 リファレンスアーキテクチャモデル（RAMI4.0）は、それ自体がセキュリティを表している訳ではない。階層構造に整理されたアーキテクチャにより、ライフサイクルやバリューチェーン、工場におけるエンタープライズ制御システムの構成をわかりやすく可視化している。

インダストリー4.0 の安全目標とセキュリティ要件の一つに「インダストリー4.0 のセキュリティ・バイ・デザイン」が挙げられており、技術的メカニズムを後からセキュリティに組み込むのではなく、製品開発およびプロセスにおける装置・インフラ保護のための統合的アプローチが必要となるとしている。工場等の製造現場においては新旧の機器が混在することから、採用が難しい観点はあるが、製品やソリューション、あるいは新規のシステムにおいては、セキュリティ・バイ・デザインの考え方を取り入れ、必要なセキュリティ機能を一体化した形で実装することを考慮する必要があると考えられる。

2.2 工場システムにおけるサイバーセキュリティガイドライン原案のとりまとめ

前節で示した、工場等の製造現場におけるサイバーセキュリティ対策の調査、及び次章に示す検討会の審議、東京大学グリーン ICT プロジェクト・Edgecross コンソーシアム合同・工場セキュリティ WG における検討事項、及び「工場セキュリティガイドライン 概要編」の内容を参考に、工場システムにおけるサイバーセキュリティガイドライン原案の取りまとめを実施した。

ガイドライン原案の構成は以下の通りである。

【工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案） 第1版】

本ガイドラインは、特定の業界・業種や製品という観点で対象を限定せず、広く活用いただけるよう、業界団体や個社が自ら対策を進めるに当たり参照すべき考え方やステップ示すと共に、必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記した。

また、製造業／工場において重視される価値である事業／生産継続（BC：Business Continuity）、安全確保（S：Safety）、品質確保（Q：Quality）、納期遵守・遅延防止（D：Delivery）、コスト低減（C：Cost）を重視し、内容を取りまとめた。

3. 検討会の運営

調査の実施及び取りまとめにあたっては、専門的な見地からの検討、分析、助言を得ることを目的に、工場等の製造現場のサイバーセキュリティに係る有識者等からなる検討会を開催した。

3.1 工場 SWG の設置

（1） 設置目的

経済産業省は、産業・社会の変化に伴うサイバー攻撃の増大に対し、リスク源を適切に捉え、検討すべき対策を漏れなく提示するための新たなモデルとして「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」を提示した。この CPSF を実現するため、フィジカル空間とサイバー空間を繋ぐ機器・システムに対するセキュリティについても検討を行っている。

従来の工場内システムは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が、IoT 化の流れの中で、フィジカル空間に存する個別の機械やデバイスやその関連センサーといった末端部分が直接サイバー空間のインターネットに接することにより、知らない間にセキュリティホールが生じるなど、新たなセキュリティリスク源が増加しつつある。

今後、データの見える化や、遠隔制御、自動化等の進展に伴い、IP アドレスを保有するデバイス・機器がサプライチェーンの一層広域にまで広がることに鑑み、足元でのリソースや危機意識に乏しい中小企業も含め、工場におけるセキュリティリスク対策は一層重要になってくるものの、ステークホルダー間の相互信頼の土台となる考え方が整理できているとは言い難い状況である。

このため、今年度、工場のサイバーセキュリティ対策の推進に向けたガイドラインを取りまとめることを目標とし、産業サイバーセキュリティ研究会WG1に紐づける形で、工場のサイバーセキュリティ関係者により構成する「工場SWG」を設置した。

（2） 設置期間

2022 年 1 月～

（3）委員

座長	江崎 浩	東京大学大学院 情報理工学系研究科教授
委員	岩﨑 章彦	一般社団法人電子情報技術産業協会 セキュリティ専任部長
	榎本 健男	一般社団法人日本工作機械工業会 技術委員会標準化部会電気・安全規格専門委員会委員 （三菱電機株式会社名古屋製作所ドライブシステム部 専任）
	桑田 雅彦	日本電気株式会社 デジタルネットワーク事業部 兼 サイバーセキュリティ事業部 兼 デジタルプラットフォーム事業部 シニアエキスパート ソフトウェアアドバンストテクノロジスト（サイバーセキュリティ） （Edgecross・GUTP 合同工場セキュリティ WG リーダー）
	斉田 浩一	ファナック株式会社 IT 本部情報システム部五課 課長
	佐々木 弘志	フォーティネットジャパン合同会社 OT ビジネス開発部 部長 （IPA ICSCoE 専門委員）
	斯波 万恵	株式会社東芝 サイバーセキュリティ技術センター 参事 （ロボット革命イニシアティブ（RRI）産業セキュリティ AG）
	高橋 弘宰	トレンドマイクロ株式会社 OT セキュリティ事業部 OT プロダクトマネジメントグループ シニアマネージャー
	中野 利彦	株式会社日立製作所 制御プラットフォーム統括本部 大みか事業所 セキュリティエバンジェリスト
	西雪 弘	三菱電機株式会社 FA ソリューションシステム部 部長
	藤原 剛	ビー・ユー・ジーDMG 森精機株式会社 制御開発本部コネクティビティー部 副部長
	松原 豊	名古屋大学大学院 情報学研究科准教授
	村瀬 一郎	技術研究組合制御システムセキュリティセンター 事務局長
	渡辺 研司	名古屋工業大学大学院 社会工学専攻教授

（2022/3/23 時点、委員五十音順、敬称略）

（4） 開催概要

1）第１回

表 3-1 産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）工場 SWG 第 1 回会合

日時	2022 年 1 月 6 日（火） 14:00 ～ 16:00
場所	オンライン開催（WebEX）
議題	1. 産業サイバーセキュリティ研究会 WG1工場 SWG の議事運営について 2. 産業サイバーセキュリティ研究会 WG1 工場 SWG の設置について 3. 経済産業省委託調査「令和2年度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」結果概要の紹介 4. 東大グリーン ICT プロジェクト・Edgecross「工場セキュリティガイドライン(案)概要編」の紹介 5. 自由討議

2）第２回

表 3-2 産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）工場 SWG 第 2 回会合

日時	2022 年 2 月 28 日（月） 16:00 ～ 19:00
場所	オンライン開催（WebEX）
議題	1. 開会 2. 製造業における DX について 3. 工場セキュリティに関する取組みについて 4. 工場セキュリティに関する動向について 5. 東大グリーン ICT プロジェクト・Edgecross「工場セキュリティガイドライン(案)概要編」について 6. 自由討議 7. 閉会

3）第３回

表 3-3 産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）工場 SWG 第 3 回会合

日時	2022 年 3 月 23 日（水） 18:00 ～ 19:00
場所	オンライン開催（WebEX）
議題	1. 開会 2.「工場セキュリティガイドライン(案)」について 3. 自由討議 4. 閉会

3.2 工場 SWG における議論

3回開催した SWG 会合において得られた委員からの意見に対して、以下のように対応を行った。

表 3-4 工場 SWG における委員意見と対応一覧

No.	会合	ご意見	対応方針
1-1	第１回	標準に関して、ISO/IEC JTC 1 でスマートマニュファクチャリングに関するリファレンスモデルやフレームワークアーキテクチャの検討が進められている。この検討との関係はどのように考えているのか。	今後検討する上でのご意見として受け止め。
1-2	第１回	今回のセキュリティガイドラインの概要は準備編ないし計画導入編の位置づけと理解している。全体像を広く浅く見据えるのか、準備・導入を深く記載するのかによって、タイトルも検討できると良い。	ご指摘を踏まえて修正した。（ガイドライン案 タイトル） ※ 全体像を示すものとし、サブタイトルは記載せず。
1-3	第１回	ステークホルダーでもある本社との関係、戦略・ポリシーの兼ね合いについて、次バージョン以降では、事業継続の観点から運用保守やレスポンス、リカバリーの部分を掘り下げていただきたい。	今後検討する上でのご意見として受け止め。
1-4	第１回	中小・零細企業のセキュリティ対策については、広い意味のセキュリティとして部屋の施錠などの物理的対策も必要であり、それらを実施した上でネットワークやサイバーセキュリティの必要性に訴求する方が良いのではないか。	ご指摘を踏まえて修正した。 （ガイドライン案 「3.2.2(2)物理面での対策」）
1-5	第１回	物理的対策について、水道に関する記載が不足している。水の循環が止まるとエアコンなど様々なものが停止することが、最近意識されている。	ご指摘を踏まえて修正した。 （ガイドライン案「3.2.2(2)物理面での対策 ④水道設備に関わる対策」）
1-6	第１回	概要編にしてはボリュームが多い。最初に要求事項を記載し、次に対象のシステム、共通的なセキュリティ実施事項、運用面での対策、組織面での対策等を書けると良いのではないか。	ご指摘を踏まえて修正した。（全体の構成や書きぶりをわかりやすい形に修正）
1-7	第１回	RRI でも調達時のチェックリストを作っているので参考にしていただきたい。	ご指摘を踏まえて修正した。 （ガイドライン案 3.3(2)サプライチェーン対策）
1-8	第１回	対策には物理セキュリティとサイバーセキュリティの両方が含まれているが、資産や保護対象はサイバーセキュリティに寄っていると感じた。物理的な脅威と対策をどこまで考えるかをもう少し明確にできると良い。	ご指摘を踏まえて修正した。 （ガイドライン案「3.2.2(2)物理面での対策」） ※ 物理セキュリティはサイバー攻撃が関係する対策に焦点
1-9	第１回	これまであまりセキュリティを必要としなかった中小企業の方や専門家でない方が読んだ時に、事例が無いと理解が困難ではないかと感じた。	ご指摘を踏まえて修正した。（全体の構成や書きぶりをわかりやすい形に修正。また想定工場を明記しているほか、コラム1中に被害事例を掲載）
1-10	第１回	工場のライフサイクルマネジメントは製品のライフサイクルと一緒に動くことになるのではないか。同じ工場の敷地内であっても、製造するものの変更や人の入れ替えが生じる。	今後検討する上でのご意見として受け止め。
No.	会合	ご意見	対応方針
1-11	第１回	今回のガイドラインは、中小企業を含めたセキュリティの底上げが目的と理解した。高度な標的型攻撃	ご指摘を踏まえて修正した。 （ガイドライン案【参考】攻撃者の動機）

		もあるがそれはごく一部であり、むしろ人為的ミスでウイルスが混入してしまうことなどを前提にして書けると良い。攻撃者のレベルやその対策のレベルの意識合わせをし、それを前提としてガイドラインが書けると良い。	
1-12	第１回	昨年度の委託調査結果の中でレベル 0～レベル 4 と記載されていたように、工場の置かれている状況によって、やるべきことや対策方法は異なってくる。来年度以降、このレベルに応じて求められる対策や考慮すべき事項を検討する活動ができると良い。	ご指摘を踏まえて修正した。 （ガイドライン案 2.1 想定企業脚注にレベルに応じたセキュリティ対策に関する記述を記載）
1-13	第１回	詳細版も含めてかもしれないが、欧州等の諸外国と相互に認証し合うなどのレベルまでいくと、中小企業もカバーできるような形に持っていけるのではないか。	今後検討する上でのご意見として受け止め。
1-14	第１回	日本では小さい規模の企業がまだ多く、セキュリティ担当がいない企業もある。そのような企業もスムーズに理解できるようなガイドラインになると良い。	ご指摘を踏まえて修正した。（全体の構成や書きぶりをわかりやすい形に修正。また想定工場を明記しているほか、コラム1中に被害事例を掲載）
2-1	第２回	例えば食品、医薬品なども今回のガイドラインのスコープに入ると考えており、これらの業界では、サイバー攻撃が消費者の健康に影響する可能性がある。全業種を対象とすることでご検討いただきたい。	ご指摘を踏まえて修正した。（ガイドライン案 1.1 工場セキュリティガイドラインの目的）
2-2	第２回	排水、排気など、工場の周りの環境に影響する要因は、ガイドラインで共通に扱えるのではないか。	ご指摘を踏まえて修正した。 （ガイドライン案「3.2.2(2)物理面での対策 ④水道設備に関わる対策」）
2-3	第２回	全社的には工場の稼働を能動的に止めなければ事業継続性に影響を与えるという判断を行うことがありうる。P.74 表 6.1 の「安全」に関わる辺りに、安全上の問題発生回避のために能動的停止・安全停止（Active Defense）する選択肢も BCP の観点からあり得るとことを表記いただいてもよい。判断に必要な情報を本社に工場から能動的にエスカレーションして、本社経営陣に判断を求めるような役割を工場は担うべきだと考える。	ご指摘を踏まえて修正した。（ガイドライン案 P2 脚注）
2-4	第２回	最低限やらなければならないことを明確にすべきではないか。	ネットワークにおけるセキュリティ対策（例）においては、対策項目ごとに最低限のセキュリティ対策について明示しているものの、それ以外の部分については今後検討する上でのご意見として受け止め。
2-5	第２回	解説書があると現場にもわかりやすいという意見や、セキュリティの心得を作成している団体もあったので、良い点は、本ガイドラインにも取り入れていただきたい。	今後、ガイドライン本文案のパブリックコメント等の作業と並行して、わかりやすい形の資料を作成する予定。

No.	会合	ご意見	対応方針
2-6	第 2 回	必要最低限、何をすればよいかという勧告事項と、推奨事項に分けたものを作成した方がよい。	今後検討する上でのご意見として受け止めるものの、基本的には、今後、業界・業種の事情に応じたガイドラインの作成がなされる際に検討すべきご意見と受け止め。
3-1	第3回	資料 4　p.5-6 は資料 3 に同様の説明がある。文章で書かれているより、資料 4 のような図がある方が読みやすい。	ガイドライン本体も図で記載する。
3-2	第3回	最新版のガイドラインはコンパクトで読みやすいが、複数回出る図や、冗長な箇所がある。	冗長な箇所については改善を図る。
3-3	第3回	資料 3 の p.6「セキュリティ対策企画・導入の進め方」について、ステップ 1～3 とあるが、ステップ 3 以降、ステップ 1 に戻るのか、あるいは他のステップが増える等はあるのか。	ステップ 3 で得られた情報が、ステップ 1 に反映されるということもあると思うので、ステップ 3 の次はステップ 1 に戻ると考えている。
3-4	第3回	今後の改訂の頻度や読者のコメントをどうやって反映していくのかを伺いたい。これを工場内でどのように使われているのかは非常に気になるところであるが、その吸い上げをどうするのか。	今回のガイドラインは様々な業界・企業に使っていただくことを想定しているので、どのように使われていくかは注視したい。 どのように改訂するかについては、CPSF の改訂スキームについて、WG1・分野横断 SWG 合同会議で議論したいと考えている。例えば意見を受け付ける窓口を HP 等に設け、技術的な修正についてクイックに対応できる仕組みを作っていけないかと考えている。
3-5	第3回	また、注目されるガイドラインとなると思うので、パブコメにて様々な意見が上がってくると思う。対応するもの、今後の参考とするもの、記載はあるが勘違いしているもの、対象外となるものに分けられると思うが、その中でも勘違いをしたコメントが非常に重要である。つまりこちら側の意図が伝わっていない点であるので、最終版を策定する際には、そのような意見を SWG の検討の俎上に載せていただきたい。	パブコメについては、ご意見を頂ける貴重な機会であるので、頂いた意見と対応方針の一覧表を作成するなどして、どう対応していくか改めて議論させていただきたい。
3-6	第3回	ステップ 1～3 が繰り返される想定とのことだが、ループを回すという記載がなかった。前後いずれかに追記した方がよい。	ステップはループを回す旨を追記する。
3-7	第3回	細かい点だが、Edgecross でのレビューが進んでいるため、整合の確認を取った方が混乱を招かないと思う。	Edgecross の改訂内容について、必要な箇所を反映する。
3-8	第3回	「参考」にも有用な情報が記載されているため、目次で鳥瞰できるとよい。	目次(本来の目次とは別)に一覧化する。
3-9	第3回	また、表番号などは最後に更新することでよいか。	表番号、図番号、語尾など編集的なところは、パブコメにかけるまでに一括して見直す。
3-10	第3回	図中に図番号が埋め込まれてしまっているところがある。	矛盾の無いように番号を整理する。

No.	会合	ご意見	対応方針
3-11	第3回後	(ステップ1)情報収集・整理 (ステップ2)セキュリティ対策の立案 (ステップ3)セキュリティ対策の実行・管理体制の構築の文言を以下に変更した方がいい。 (ステップ1)経営陣の関与と情報収集・整理 (ステップ2)管理体制の確立と セキュリティ対策の立案 (ステップ3)セキュリティ対策の実行およびPDCAサイクル管理体制の実施構築 (理由1)情報収集・整理だけだとステップ1が軽く見える。ステップ3で初めて管理体制が登場し、経営陣の参加はステップ3で行われるように読める(誤解される) (理由2)管理体制ができないとステップ1, 2は無意味 (理由3)現ガイドラインのステップ1に「【参考】経営層による取組みの宣言[6.1.2]」はある。”	文言を修正する。

注:第3回で得られた意見への対応は、報告書作成時点のものであり、方針が変更される可能性がある。

4. 考察

本調査では、工場等の製造現場におけるサイバーセキュリティ対策の現状と課題、データの利活用が進んだ工場等の製造現場におけるサイバーセキュリティ、国内外における関連規格等について調査を行った。

また、産業サイバーセキュリティ研究会ワーキンググループ1（制度・技術・標準化）工場 SWG を立ち上げ、「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（案）」を取りまとめた。本ガイドラインの目的は、各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、工場システムのセキュリティレベルの底上げを図ることとし、各業界・業種において活用できるような、工場等の製造現場のセキュリティ確保に関する基本的な考え方を示した。

一方、ガイドライン策定の過程において、工場 SWG 委員や工場システムのユーザとなる業界団体から得られた意見において、今後の検討課題として整理された点は以下のとおりである。

- 国際標準において検討されているファレンスモデルやフレームワークアーキテクチャ、関連規格等との関係を整理すべき。
- 欧州等の諸外国と相互認証等も念頭に置き、中小企業もカバーできるような仕組みを構築できるとよい。
- 事業継続の観点から運用保守やレスポンス、リカバリーの部分を掘り下げてほしい。
- 最低限やらなければならないことを明確にすべき。
- 脅威レベルと対策が紐づけられるとよい。
- 成熟度アップのための施策レベルや手順があるとよい。
- ガイドラインの背景や実施例を提示する解説書が必要である。
- サイバーセキュリティ経営ガイドラインとリンクした形で、実務者が対策すべきことが書かれているとよい。

これらの点について、次年度以降、優先順位をつけて対応方針を策定し、検討結果についてガイドラインに反映することで、ガイドラインがより多くの工場システムに関わる部分で活用され、工場システムのセキュリティレベルの向上につながることが望ましい。

工場等の製造現場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

2022 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
サイバーセキュリティ戦略グループ
TEL 03-6858-3578