FLEXIBLE FACTORY
PARTNER ALLIANCE

フレキシブルファクトリ
セキュリティガイドライン

工場ネットワークで無線通信を安心して利用するために

執筆者：

株式会社 FFRI research-feedback@ffri.jp	松木　隆宏
株式会社カスペルスキー jp-sis@kaspersky.com	松岡　正人
日本電気株式会社 iot-sec-pr@ioth.jp.nec.com	勝倉辰之助 河合　亮佑 桑田　雅彦 岡山　義光
エヌ・ティ・ティ・コミュニケーションズ株式会社 iot-td@ntt.com	田良島周平 野村　啓仁 太田　和彦

協力パートナー：
Flexible Factory Project（国立研究開発法人 情報通信研究機構 共同研究プロジェクト）

発行者：
フレキシブルファクトリパートナーアライアンス
info@ffp-a.org

巻頭言

製造現場では情報通信技術（ICT）の活用が進んでいます。このトレンドは、労働人口および熟練者の減少、顧客ニーズの多様化、国際競争の激化などの問題を背景として、今後も続いていくと想定されます。ICTは、生産効率の向上だけではなく、オンデマンド・マニュファクチャリングによる付加価値を生み出すためにも必要とされています。人とモノが密接に協調する製造現場では、柔軟な運用やプロセスが大変重要になります。製造機械とロボットや自動搬送機などの移動体の間でのデータ交換をするためには、とりわけ無線通信が多く使われることになります。

フレキシブルファクトリセキュリティガイドラインは、無線通信が導入された工場ネットワークにおいて、サイバーセキュリティをどう考えるべきかの指針を提示します。また、セキュリティの専門家ではない工場のスタッフに対して、セキュリティベンダーの協力のもとでセキュリティに関する計画や対策を実施するための知識を提供します。

このような目的のため、フレキシブルファクトリセキュリティガイドラインは、フレキシブルファクトリパートナーアライアンスのコーディネーションのもとで、セキュリティベンダー、ITベンダーのボランティアによって策定されました。また策定にあたっては、国立研究開発法人情報通信研究機構の共同プロジェクトFlexible Factory Projectの協力を得ています。

2019年9月
フレキシブルファクトリパートナーアライアンス

目次

1. はじめに 5
1.1. ガイドライン策定の背景 5
1.2. ガイドラインの位置付け 5
1.3. ガイドラインの構成 6
1.4. ガイドラインの使い方 6
1.5. 用語の定義 6

2. サイバーセキュリティのフレームワーク 8
2.1. IEC 62443参照モデル 8
2.2. ゾーンとコンジットのモデル 10

3. 工場ネットワークの典型モデルとセキュリティリスク 12
3.1. 工場ネットワークの典型モデル 12
3.2. 守るべき資産 13
3.3. 想定される脅威とリスク 14
3.4. 無線通信特有の脅威 16

4. セキュリティ対策 18
4.1. 技術的な対策 18
4.2. 物理的な対策 21
4.3. 運用的な対策 23
4.4. 管理的な対策 24

5. 工場におけるセキュリティアセスメント 27

参考文献 **34**
略号 **35**

1. はじめに

1.1. ガイドライン策定の背景

製造現場での無線利用が拡大しています。それに伴いサイバーセキュリティのリスクも増大しています。サイバーセキュリティのインシデント（事象）は工場の物理的な安全にも脅威を与えることがあります。

一例を挙げると、2017年に製造業を含む多くの企業がランサムウェア「WannaCry」によるサイバー攻撃を受けました。代表的な日本の自動車会社のヨーロッパ子会社では、テスト装置を介して、サーバーがウイルスに感染し、企業内ネットワーク内で感染が広がっていきました。被害の範囲は、ビジネス用サーバーやPCに留まらず、工場の製造・生産システム、制御機器、物流倉庫システム、受入れ管理システムにも広がりました。別の日本の自動車工場や台湾の半導体工場もウイルス感染により一時操業がストップしました。

これらの事例は、無線ネットワークに起因するものではありません。しかしながら、無線ネットワークにおけるセキュリティには、有線ネットワークに比べサイバー攻撃を受けるポイントが多いため、過分に注意する必要があります。

このガイドラインは、無線ネットワークが組み込まれた工場ネットワークを対象とした実用的なセキュリティ対策を普及させるために策定されました。

1.2. ガイドラインの位置付け

このガイドラインは、情報システム、生産技術、生産設備、設備保全の部門、および左記に相当する部門で、セキュリティ対策の責任者向けに書かれています。図1には、生産技術の観点から対象となる部門を組織図で表していますが、生産技術部門に限定するものではありません。

対象となる製造現場は、有線/無線ネットワークが混在する環境です。無線通信の視点でのセキュリティ対策が記載されています。有線通信の一般的なセキュリティ対策は既存のガイドラインも参照してください。

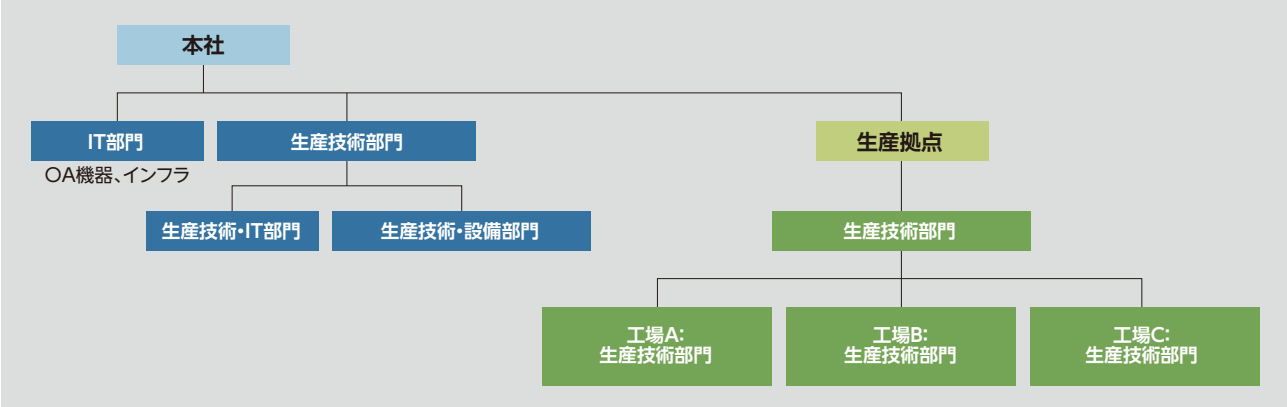


図1　このガイドラインを読むべき人が所属する部門（ファクトリオートメーションの例）。関連する運用・保守部門の人も対象。企業によって組織構造は異なるが、その場合は読み替える

1.3. ガイドラインの構成

このガイドラインは、５つの章で構成されています。

第１章では、ガイドライン策定の背景やポジショニングを記しています。また用語の定義を記載しています。第２章では、工場ネットワークのセキュリティフレームワークとして、IEC 62443 参照モデルを記述しています。第３章では、製造現場のネットワークにおける守るべき資産を考慮し、典型的なセキュリティリスクと、想定される脅威を示しています。第２章に示したフレームワークとの関係も説明しています。第４章では、技術的、物理的、運用的、管理的という4つの視点で、具体的なセキュリティ対策を提示しています。第５章では、製造現場でのセキュリティアセスメントの準備と考察を記述しています。

1.4. ガイドラインの使い方

このガイドラインは、以下の２つの目的で策定されています。

- 工場ネットワークに無線通信で接続されるデバイス、機器、システムのセキュアな管理を行うためのネットワークセキュリティや、その対策に関する基本的なフレームワークを理解する。

- 工場におけるセキュリティ対策の責任者が、セキュリティベンダーやセキュリティ監査人とコミュニケーションをするときにツールして使用する。

本ガイドラインは、すべての種類の工場のシステム構成、資産、サイバーセキュリティの脅威やリスクを記載しているわけではないので、実際のケースでは、ここでの記載を参考として扱ってください。

1.5. 用語の定義

改竄：機器、データ、またはプロセスを一部消去または変更を実行することで、正確ではない状態にすること

脅威：セキュリティ違反の可能性。セキュリティに違反して害を及ぼす可能性のある状況、機能、行動、またはイベントがある場合に存在する

コンジット：通信の資産を論理的にグループ化したものを接続する通信路。通信チャネルに含まれる資産のセキュリティを保護する

資産：ハードウェア、ソフトウェア、機能、インフラストラクチャなど、工場ネットワークを構成するものすべて

ジャミング : 通信やレーダーに必要な電波の適切な利用を不可能にする電波妨害

脆弱性 : システムの整合性またはセキュリティポリシーに違反し悪用される可能性がある、システムの設計、実装、運用または管理における欠陥または弱点

セキュリティリスク : 特定の脅威が特定の脆弱性を悪用する可能性があり、製造における通常の動作に損害を与える可能性があるという被害の発生または被害の見込み

ゾーン : 共通のセキュリティ要件を共有する論理的または物理的資産をグループ化したもの

多層防御アーキテクチャ : 単一層だけでなく複数層のセキュリティ規定でセキュリティリスクを軽減する手法

盗聴 : 会話、通信またはデジタル伝送を不正に傍受すること

なりすまし : 許可されたユーザーであることを装って、許可されていないアクションを実行すること

フィールドデバイス : アクチュエータ (ポジショニング機器、バルブおよび衝撃吸収ドライブ、周波数変換器など) およびセンサ (測定トランスデューサー、プローブ、モニタなど)

プロセス : 製品または材料の製造、処理または輸送において行われる一連の作業

物理デバイス : 製造、加工、輸送、医療などの活動に使用されるハードウェア。これには、(a) センサおよびアクチュエータ、機器、および制御下の機械、(b) 分散制御システム、プログラマブルロジックコントローラ、SCADAシステム、オペレーターが操作するコンソールなどの制御機器、ならびに管理および管理に使用される現場検知および制御装置、(c) 通信サブネットワークまたはネットワーク間に接続され、接続された他のシステムとデータを交換するためにネットワークによって提供されるサービスを使用することができるコンピュータおよびネットワーク機器、が含まれる

DMZ (DeMilitarized Zone) : 非武装地帯。物理的または論理的サブネットワークで、信頼できないネットワークにさらされ、組織の外部向けサービスを担う

DoS攻撃 (Denial of Service attack) : サービスを停止するための攻撃の1種。広く知られている方法の1つは、膨大な数のパケット (トラフィック) を特定のサーバーまたはサイトに送信すること。広義には、少量のパケットの送信、およびサービスを停止するための物理的な攻撃 (デバイスの破壊、ワイヤレス干渉など) も含まれる。複数の送信元からパケットを送信する攻撃は、(DDoS攻撃) と呼ばれる

IACS (産業用オートメーションおよび制御システム) : 産業プロセスの安全、安心、および信頼性のある操作に影響を与える、または影響を与える可能性のある人、ハードウェア、およびソフトウェアで構成されるシステムまたはその集合

2. サイバーセキュリティのフレームワーク

製造現場のサイバーセキュリティを理解するために、守るべき資産、脅威とリスク、対策とアセスメントを記述した工場ネットワークのための共通フレームワークが必要になります。このガイドラインで用いるフレームワークは、国際電気標準会議 (IEC) の技術仕様IEC/TS 62443-1-1 [1] (以下、IEC 62443) に記載されたサイバーセキュリティフレームワークに基づいています。

工場ネットワークでは、MES (Manufacturing Execution System) やERP (Enterprise Resource Planning) の下に、産業用オートメーションおよび制御システム (IACS : Industrial Automation and Control System) として、フィールドデバイス、コントローラ、SCADA (Supervisory Control and Data Acquisition) が構成されています。このIACSのネットワークは、管理権限、統一されたポリシーと信頼レベル、機能上の重要性、およびネットワーク領域の境界を超える通信トラフィック量を考慮しつつ、他のネットワークから慎重に分離されるべきものです。

2.1. IEC 62443参照モデル

図2は、IEC 62443参照モデルと、想定読者の関係を示しています。また、このモデルでは、デバイスやシステムを5つの階層 (レベル) で分類しています。詳細は、IEC 62443 (Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models IEC/TS 62443-1-1, pages 63-65, Edition 1.0 2009-07を参照してください。

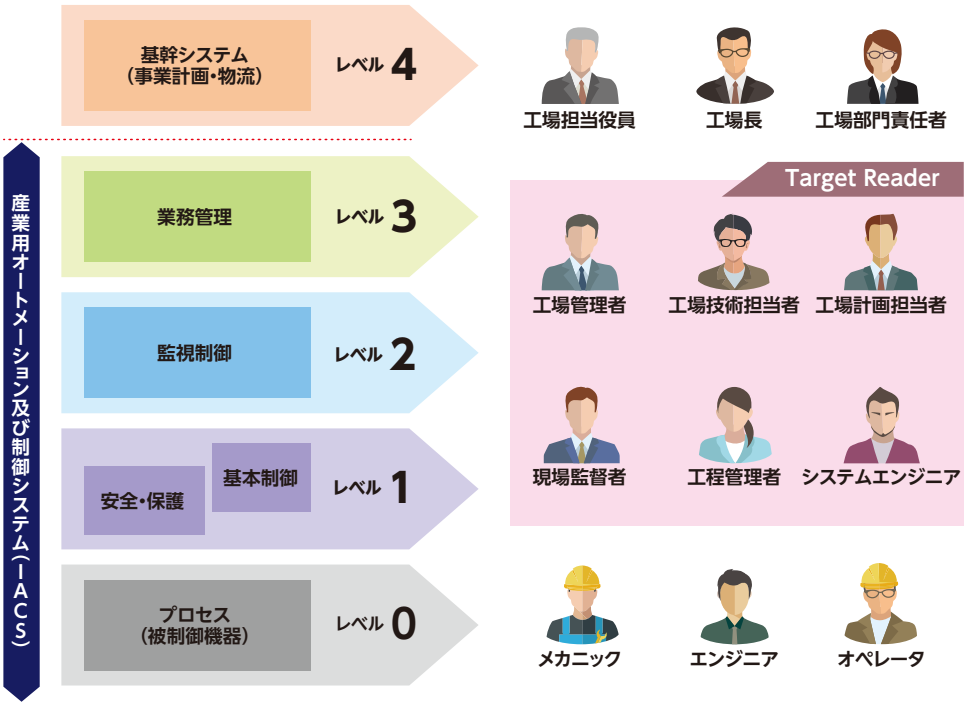


図2　IEC 62443の参照モデルと想定読者

IEC 62443の参照モデルは、5つの論理的な階層（レベル）で構成された製造または生産の統合システムに対する一般的な見方を定義しています。

レベル4　基幹システム

このレベルは、IEC 62264-1 [2]で事業計画および物流と説明されていますが、製造組織の管理に必要なビジネス関連活動に関する機能を含むものとして定義されています。企業または地域の金融システム、および企業内の個々の工場またはサイトの生産計画、運用管理、および保守管理などの他の企業インフラストラクチャの構成要素が含まれます。

レベル3　業務管理

レベル3には、最終製品を生産するためのワークフローの管理に関わる機能が含まれています。例としては、生産指示、詳細な生産計画、信頼性保証、および製造現場全体での管理の最適化などがあります。

レベル2　監視制御

レベル2には、プロセス（作業）の監視と制御に関わる機能が含まれています。プラント内には通常複合生産エリアがあり、蒸留、転化、製油場またはタービンデッキ内での混合、および発電所内の石炭処理などのプロセスがあります。

レベル1　ローカルおよび基本制御

レベル1には、プロセスの検知と操作に関わる機能が含まれています[1]。プロセス監視機器は、センサからデータを読み取り、必要に応じてプログラムを実行し、プロセス履歴を維持します。レベル1のコントローラは、連続制御、シーケンス制御、バッチ制御、およびディスクリート制御用の各プロセスにおけるセンサおよびアクチュエータに直接接続されています。最近では、多くのコントローラは、すべての種類の制御を含むようになっています。

レベル1には、プロセスを監視し、安全制限を超えた場合に自動的にプロセスを安全な状態に戻すため、安全および保護システムが含まれています。プロセスを監視し、差し迫った危険な状況についてオペレーターに警告するシステムも含まれます。

レベル1の機器には、DCS（分散制御システム）、PLC（プログラマブル・ロジック・コントローラ）、RTU（遠隔端末装置）などが含まれます。

レベル0　プロセス

このレベルには、実際の物理的なプロセス 、例えばプロセス（機器）に直接接続されているセンサおよびアクチュエータが含まれます。物理プロセスには、すべての分野における多くの異なる種類の製造設備が含まれており、その分野はディスクリート部品製造、炭化水素加工、製品流通、医薬品、パルプおよび製紙、電力など広範に渡ります。

セキュリティ対策の観点で、設計と運用のために参照モデルを実際のIACS構成にあてはめることは有用です。各レベルの機器、機器、およびシステムは、守るべき資産と見なすことができます。ハードウェアとソフトウェアのリソース、データ、機能、ネットワークインターフェースなど、各レベルの資産のさまざまな側面を考慮する必要もあります。

---

[1] IEC 62443では、プロセスはIACSシステムで制御される機器として記載されている。

2.2. ゾーンとコンジットのモデル

IEC 62443に記載されたゾーンとコンジットは、工場内の資産の論理的なグループ分けを行うために使用されます。資産をグループ化することで、各ゾーンのすべての資産に対して共通のセキュリティポリシーを定義できます。コンジットは、ゾーン間を結ぶ通信路、またはゾーン内の通信に使用される通信路と見なされます。資産間を接続する通信チャネルを保護し、通信の両端で安全なプロセスを保証します。

ゾーンおよびコンジットを対応させたネットワーク構成の例を図3に示します。資産を保護するための適切なセキュリティ対策では、各ゾーンに対し、セキュリティポリシーに従って予想される脅威およびリスクを評価します。

IACS保護のためには、多層防御アーキテクチャも必要です。第3章、第4章に示すように、IACSはさまざまな要素で構成され、さまざまな脅威にさらされているため、一般的にはセキュリティ対策を1つだけで実装するのは不十分です。図4のモデルで示されているように、さまざまなセキュリティ対策を組み合わせることでセキュリティリスクを最小限に抑えることができます。

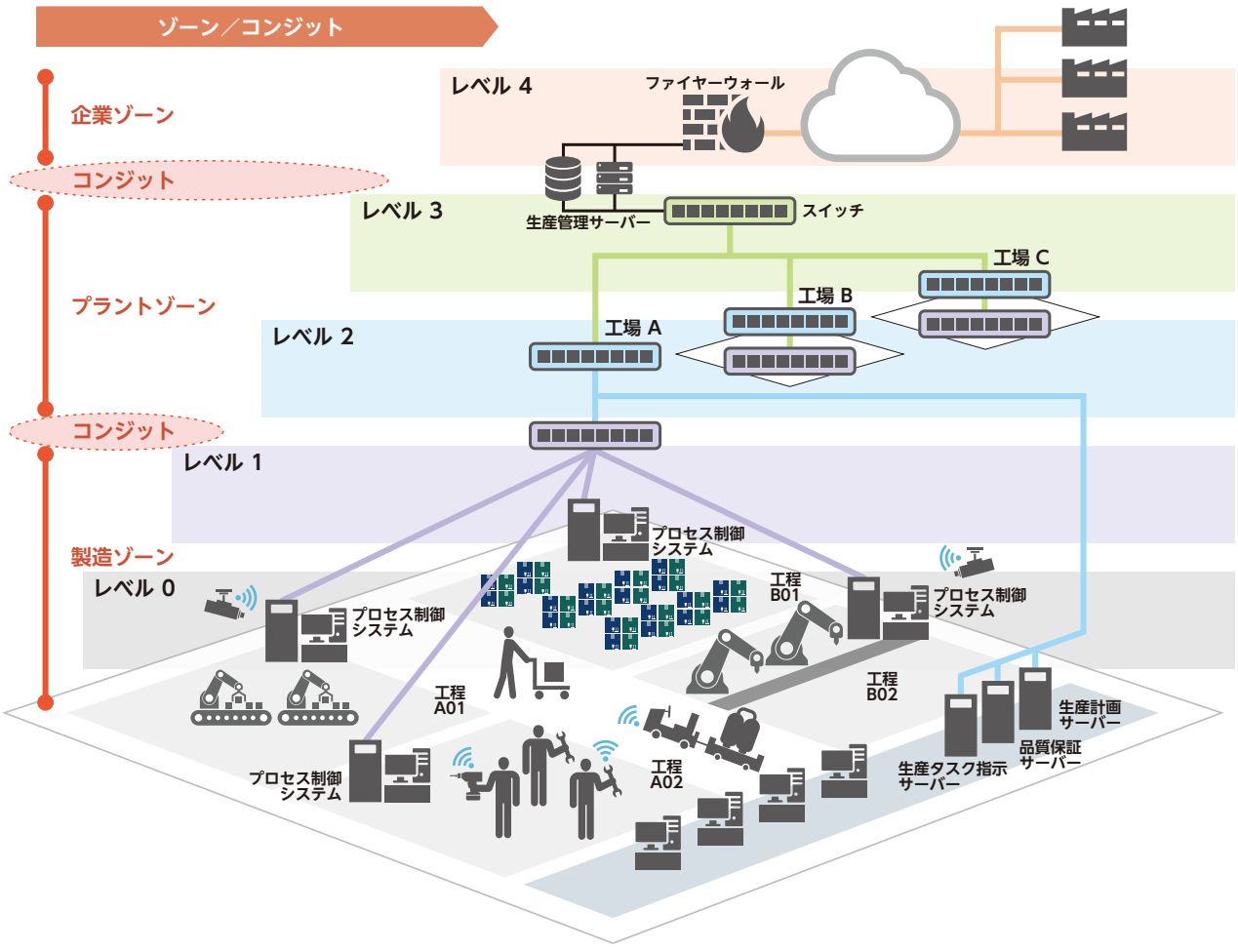


図3　ゾーンおよびコンジットを対応させたネットワーク構成の例

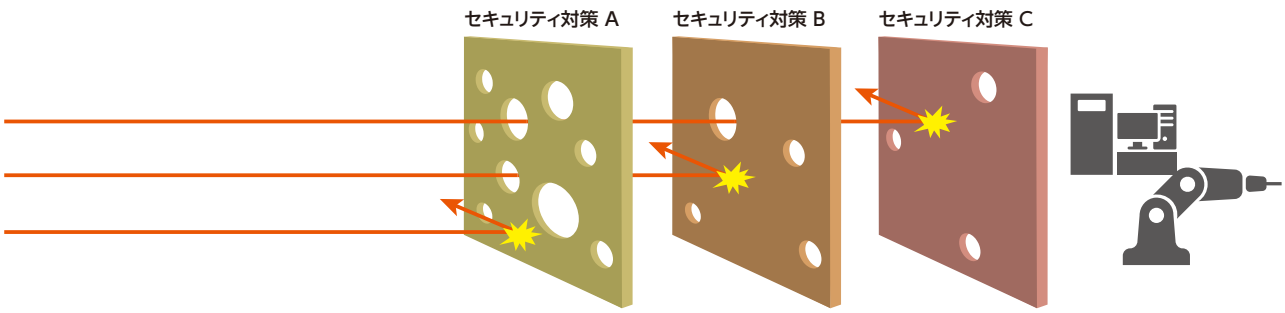


図4　多層防御アーキテクチャのイメージ（スイスチーズモデル）

3. 工場ネットワークの典型モデルとセキュリティリスク

この章では、守るべき資産と予想される脅威を理解するために、自動車工場のネットワークシステムの例を典型的なモデルとして説明します。他のプラントや工場向けには、資産や脅威を特定するための参考としてください。

3.1. 工場ネットワークの典型モデル

自動車工場におけるネットワークシステムの典型的な構成モデルを図５に示します。この例では、生産管理システムがプレス、溶接、塗装、および組立の各現場の管理システムに接続されています。各組立現場の管理システムには、作業指示、詳細な生産計画、信頼性保証などの機能があります。プロセス制御および監視システムは、現場の管理システムとネットワークで接続されています。製造プロセスを実行するために、フィールドデバイスの状態を監視しながら、コマンドをフィールドデバイスに送信します。フィールドデバイスには、自動搬送機（AGV）やインパクトレンチなど、ネットワークに接続するための無線インターフェースを備えたデバイスが含まれます。

現場の管理システムは、生産スケジュールに従って、情報および制御ネットワークを介してプロセ

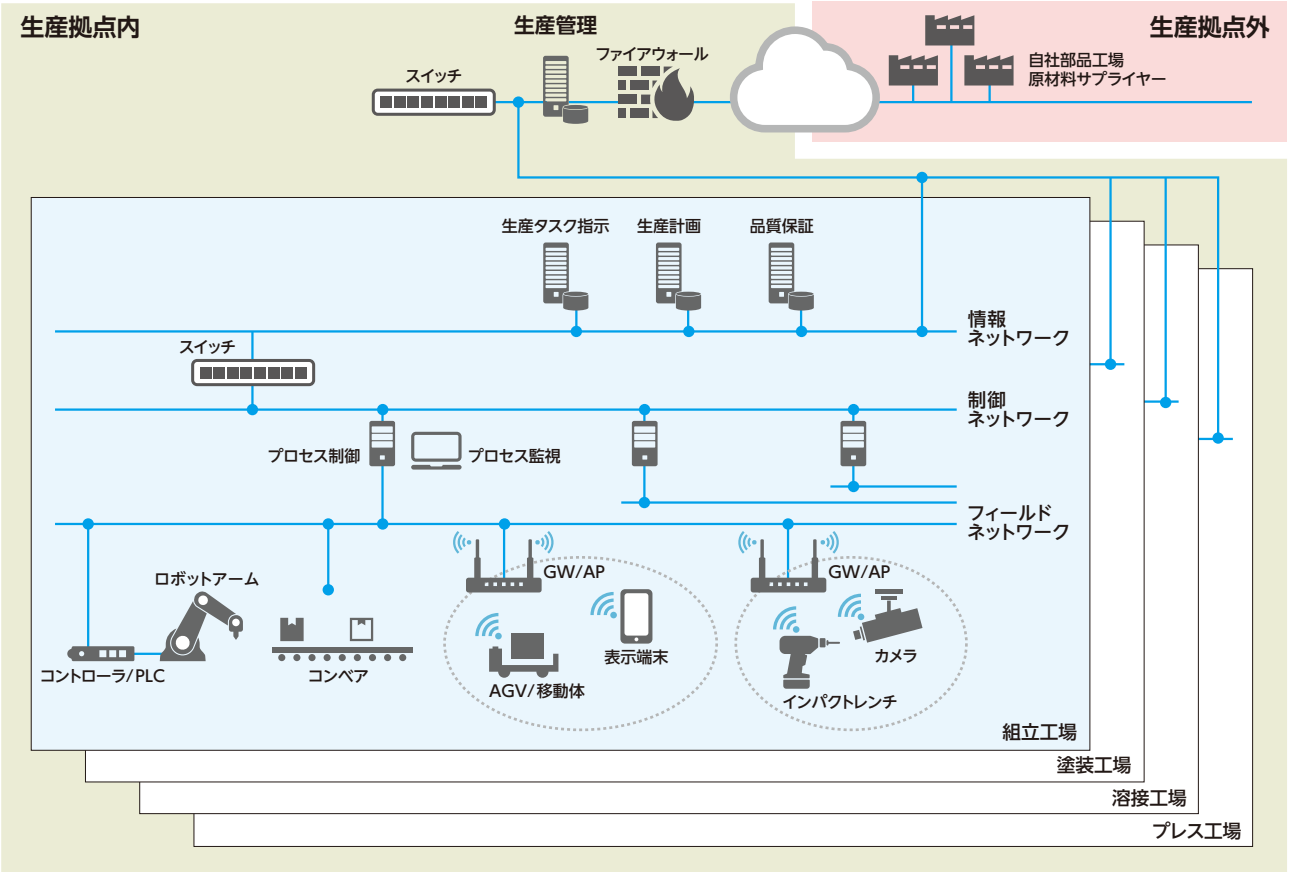


図5　自動車工場における典型的なシステム構成

ス制御システムにタスクを送り、コンベアを起動します。プロセス制御システムは、フィールドネットワークを介してコンベアにコマンドを送信します。ロボットアームのPLCは、フィールドネットワークを介してプロセス制御およびプロセス監視システムにステータス情報を送信します。信頼性を保証するために、プロセス監視システムは、制御ネットワークおよび情報ネットワークを介して現場の管理システムに情報を中継します。図5には示されていませんが、制御ネットワークと情報ネットワークの間にDMZを設定することが望ましいです。DMZを含む構成の例は他の文献に示されています[3]。

この典型モデルでは、ほとんどのネットワークのインターフェースは有線通信を使用していますが、生産設備や機器によっては無線通信を使用するものもあります。以下には、このモデルに基づいて保護される資産と想定される脅威の例を示します。工場の種類や規模によって、設備と装置、生産のための管理と運用は各工場現場で異なりますので、それぞれのモデルに応じて柔軟に適用してください。

3.2. 守るべき資産

表1には、図5のモデルで守るべき資産の例を示しています。ここでのレベルは、IEC 62443で定義されているデバイスおよびシステムのレベルに対応しています。各行は、セキュリティに関して管理される固有のシステムまたはネットワークの資産を表します。各列の項目は、セキュリティ

表1　守るべき資産

レベル	リソース	データ	機能	インターフェース
4	生産管理サーバー　(HW/SW) 例:ERP	財務、人的資源、物流、製造、 サプライチェーン、 認証などの各種データ	製造計画・実行、調達、製造などのデータ、 データの送受信、認証の管理機能	LAN(有線)
	内部・外部の調達システム　(HW/SW)	調達データ、認証データ	調達データ、データの送受信、 認証の管理機能	
	ネットワーク (HW/SW)	上記データ	データの送受信機能	
3	生産タスク指示、詳細な生産計画、 信頼性保証、 拠点内指示最適化のためのサーバー 例:MES	運用情報、指示記録、 製品品質などのデータ、認証データ	プロセス計画、生産プロセス管理、 プロセス・製品の品質管理、 拠点在庫管理、生産トレース、 設備メンテナンス、データ、 データの送受信、認証の機能	LAN(有線)
	ネットワーク (HW/SW)	上記データ	データの送受信機能	
2	フィールドデバイスの監視・制御のための上位コントローラ 例:SCADA[2], オペレータ用HMI	プロセスフロー、レシピ、プロセス状態、 認証などのデータ	プロセス制御、プロセス監視、データ、 データの送受信、認証の機能	LAN(有線)、 フィールドバス
	ネットワーク (HW/SW)	上記データ	データの送受信機能	
1	フィールドデバイスのセンシング、操作に関わるローカル又は基本コントローラ 例:DCS、PLC、RTU	フィールドデバイスへのコマンド、 フィールドデバイスの状態、 監視・作動プログラム、認証などのデータ	フィールドデバイスのセンシング・操作、 データの送受信、認証の機能	LAN(有線/無線)、 フィールドバス、 シリアルインターフェース (有線)
0	フィールドデバイス(HW/SW) 例:センサ、アクチュエータ	プロセスステップ、センシング、 認証などのデータ	センシング、操作、データの送受信、 認証の機能	LAN(有線/無線)、 シリアルインターフェース /USB(有線) BT/BLE/ZigBee(無線)

[2] IEC 62443には、上位コントローラがレベル3となっているSCADAのリファレンスモデルが記述されている

に関して識別および管理できる資産の要素、すなわち「リソース」、「データ」、「機能」および「インターフェース」を示し、資産のさまざまな側面を表します。リソースには、ハードウェア（HW）とソフトウェア（SW）の両方が含まれます。データには、ソフトウェアとは別に評価する必要があるデータが含まれています。機能には、資産によって、または資産を使用して実行される機能が含まれます。インターフェースは、資産とネットワークとのインターフェースです。

表2には、レベル0、1の機器やデバイスに相当する資産の例を記しています。　センサ、カメラ、計測ツール、ロボット、AGVなど、さまざまな種類の機器やデバイスがあります。表2に記載したインターフェースは、無線通信装置の種別／規格を示していますが、工場現場では、イーサネット、シリアルバスなど有線通信も使用されています。

3.3. 想定される脅威とリスク

前節に記載した資産の要素に対応する脅威とリスクの例を図6に示します。脅威の例には、不正アクセス、盗聴、およびDoS攻撃が含まれます。リスクの例には、ハードウェアまたはソフトウェアの動作停止または違法な操作、データの損失、機密データの漏洩、データ伝送の中断、およびネットワークインターフェースの障害が含まれます。

資産の要素に対する脅威とリスクの具体例を以下に示します。

リソース

ハードウェア資産に対する潜在的な脅威には、物的破壊、盗難、または不正アクセスが含まれます。これらの脅威によるリスクには、ハードウェアが物理的に破壊しているか無効になっている、または不正な操作に使用されている可能性があります。ソフトウェア資産に対する潜在的な脅威は、消去、不正なコピー、不正な変更です。これらの脅威からのリスクには、ソフトウェアが使用不能になったり、誤動作したり、または許可されていない操作に使用されたりする可能性があります。

データ

データ資産に対する潜在的な脅威には、不正コピー、消去、および改ざんが含まれます。データ資産のリスクには、データの損失、機密データの許可されていない漏洩などがあります。このような脅威やリスクは、プロセス管理、品質管理、生産管理、調達システムに必要な情報を含む、さまざまな種類のデータ資産に及ぶ可能性があります。

機能

データの送受信などの機器や機器のさまざまな機能、および認証機能は、運用の中断や改ざんなどのリスクを考慮する必要があります。関連する脅威として、不正なリモートアクセス、不正なデバイスや機器の接続、DoS攻撃などがあります。

インターフェース

インターフェースの主なリスクは、ネットワークへの接続の失敗と通信途絶です。これらのリスクの原因となっている脅威には、不正なネットワークアクセスやDoS攻撃などがあります。次節には、無線通信のインターフェースに特有の無線伝搬の性質による脅威を説明します。

表2　レベル0、1の機器やデバイスに相当する資産

リソース	データ	機能	無線インターフェース
リモコン	操作情報	遠隔操作	IEEE802.15.4g, その他
移動機器(スタッカクレーン, AGV, シャトル, コンベア, 各種搭載機/注入器)	制御情報、監視情報	移動体制御	IEEE 802.11
動線分析機器	ビーコン、地磁気、加速度、方位、 画像(バーコード)、映像	動線分析	IEEE 802.11/ 802.15.4g, BLE
PLC (上位コントローラへの状態情報通知)	PLCの稼働状況	稼動状況計測	IEEE 802.11/ 802.15.4g
保全作業支援機器	画像、音声、画像通話表示	保全支援	IEEE 802.11, BT, ZigBee
測位機器(生産管理)	人やモノのリアルアイム位置、 みずすましの位置・ルート	測位(生産管理)	IEEE 802.11/ 802.15.4g, BLE, UWB
測位機器(資産管理)	設備や資材の位置	測位(資産管理)	BLE
警光灯/回転灯	設備状態情報	設備状態表示	IEEE 802.15.4g
作業指示機器	作業指示情報 (段取り、手順、搬送)	作業指示	IEEE 802.11
ピッキング指示機器	ピッキング指示情報(選別、分別)	ピッキング指示	その他
安全確認機器(人)	安全確認情報、バイタル情報、 安全設備装着確認情報、危険アラーム	安全情報収集(人)	IEEE 802.15.4g, BLE
安全確認機器(環境)	有毒ガス、酸素濃度、放射線被爆	安全情報収集(環境)	その他
カメラ(ポカヨケ)	画像	ポカヨケ監視	IEEE 802.11
トルクレンチ(ポカヨケ)	ネジ締め付け情報	締め付け計測・確認	IEEE 802.11, BT, BLE
部品在庫監視機器	在庫情報	在庫管理	RFID using Sub-1GHz
検査機器	画像(寸法、歪・へこみ)、音響(駆動部の音)、X線、動画(不良状態、異物混入)	製品検査	IEEE 802.11
電力計測機器	電力量、電流波形	電力計測、電力消費計測	IEEE 802.11/ 802.15.4g, BT
流量測定機器	水量	流量計測	IEEE 802.11
空調測定機器	気流	空調計測	IEEE 802.11/ 802.15.4g, BT
温湿度測定機器	周囲温湿度、機器／ツール温度	温度計測、湿度計測	IEEE 802.11/ 802.15.4g, BT, LPWA
トルク測定機器	トルクチェック(規定値)、トルク波形、 トルク設定	トルク計測	IEEE 802.11, BT
設備・環境監視機器	画像、音響、匂い	設備・環境監視	IEEE 802.11
衛生監視機器	細菌数	衛生監視	IEEE 802.11
空気監視機器	塵埃量(パーティクル)、CO2濃度、 VOC(揮発性有機化合物)濃度	空気監視	IEEE 802.11/ 802.15.4g, BT
照度管理機器	照度	照度管理	IEEE 802.15.4g
持ち込み物監視機器	電波、熱	電子機器持ち込み監視	IEEE 802.15.4g
監視カメラ	画像	セキュリティ(侵入検知)	IEEE 802.11
生産状態表示機器	滞留、生産/非生産	生産状態表示	IEEE 802.11/ 802.15.4g
作業記録機器	作業証明、作業ログ、作業ミス記録	作業記録	IEEE 802.11
計数機器	カウンター情報	計数	IEEE 802.11/ 802.15.4g

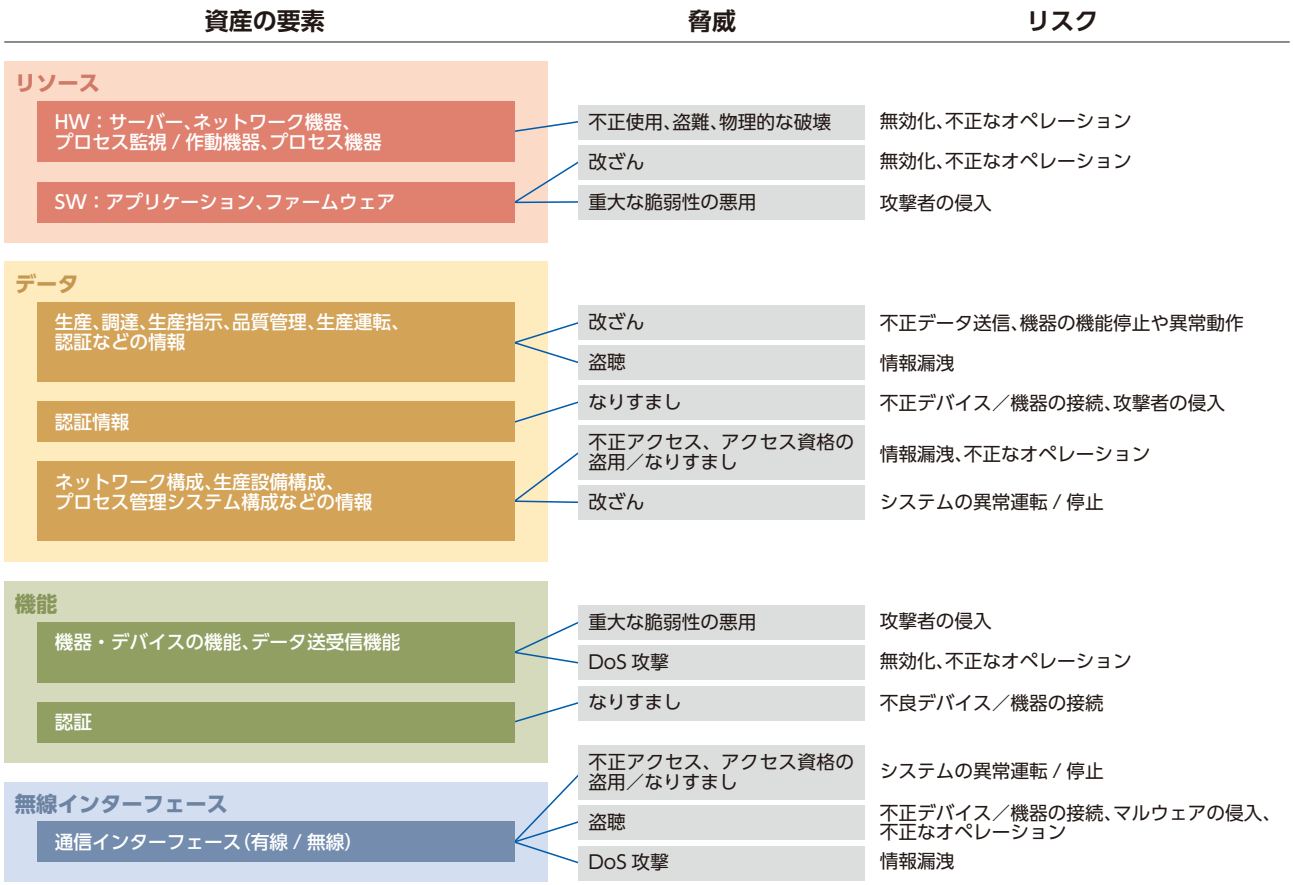


図6　資産の要素に対応する脅威とリスクの例

3.4. 無線通信特有の脅威

無線通信は、有線接続と比較して大きな利点を備えており、現代の工場では、広く使用されています。無線インターフェースを備えた機器や装置は、設置や移動が簡単で、設置コストを削減し、運用開始までの時間を短縮します。物理的なコネクタやケーブルがないため、物理的な接点不良や作業ミスや経年劣化等によるケーブル切断が問題になりません。また、AGV やロボットなどの移動体、作業員を支援するウェアラブル端末には、無線通信は不可欠です。

無線ネットワークを安全に利用するために、無線伝搬の特徴で決まる無線通信の重要な性質を以下のように理解すべきです。

工場内のモノによる影響：電波伝搬は、反射、透過、吸収、回折、遮蔽の影響を受ける特性を持っています。送信機端末と受信機端末との間の電波伝搬は、パイプ、柱、壁、セル、機械、製品、搬送機械、人々などを含む、施設のレイアウトによって変わってきます。信頼性のある無線通信を確立することができないリスクを減らすために、特定の物理的空間に適した無線端末の種類および設置場所の選択が重要となります。リスクを軽減するための対策を実施するためには、運用中の無線通信の状態を継続的に監視することも重要です。

空間を介した影響： 悪意のある電波放射は、無線の送受信を劣化させ、無線通信を妨害する可能性があります。近隣の住宅地の無線LANシステムなど、同じ周波数帯を使用する工場外の無線システムが工場内で干渉を引き起こす可能性があります。また、工場内で使用されている無線システムは、意図せずに互いに干渉する可能性があります。Wi-FiやBluetoothを搭載したスマートフォンや音楽プレーヤーなど、作業者が工場に持ち込むモバイル機器が、同じ周波数帯を使用する工場の無線システムにとって脅威となる可能性があります。無線デバイスとシステムの協調管理、および無線通信の利用状況の継続的な監視は重要です。

空間を介したアクセス： 電波は工場敷地内外に広がるため、無線インターフェースには有線通信にはないリスクがあります。物理的なコネクタがなく、接続プロトコルはソフトウェア設定で変更できるため、脆弱なシステムの無線端末による不正アクセスは重大な脅威となります。SSIDのなりすまし、およびAPのなりすましは、不正アクセスを許すと同時に、正常な通信に障害を与える可能性があります。不正アクセスは、盗聴による情報漏えい、システムの異常動作、またはネットワーク動作の改ざんによる停止の原因となります。無線インターフェースは、WEPなどの不適切な暗号プロトコルや、複数のユーザー間でパスワードを共有するなどの不適切な認証の使用を回避する必要があります。

セキュリティに関する無線通信の特性と脅威を、図7に示します。無線リンクは見えないため、いつ、どこで問題が発生したのかを知ることは困難です。したがって、有線通信を使用する場合と比較して、より多くの注意が必要です。

性質	脅威
工場内のモノによる影響	周囲を取り囲む壁や天井、工場内の機械、製品、搬送機械、人などの物体に影響される通信品質、およびそれらの移動による通信品質の動的変化
空間を介した影響	(悪意のある) 意図的な電波放射、意図しない電波放射に干渉による通信リンクの品質劣化または途絶
空間を介したアクセス	盗聴、改ざん、SSID/APのなりすまし。目に見える接続がないため発見が困難

図7　無線通信の特性と脅威

4. セキュリティ対策

この章では、技術的、物理的、運用的および管理的という４つの視点で、セキュリティ対策を説明します。この章で説明されているセキュリティ対策を図８に示します。第５章では、これらの対策と第３章で説明した資産と脅威との対応を示しています。

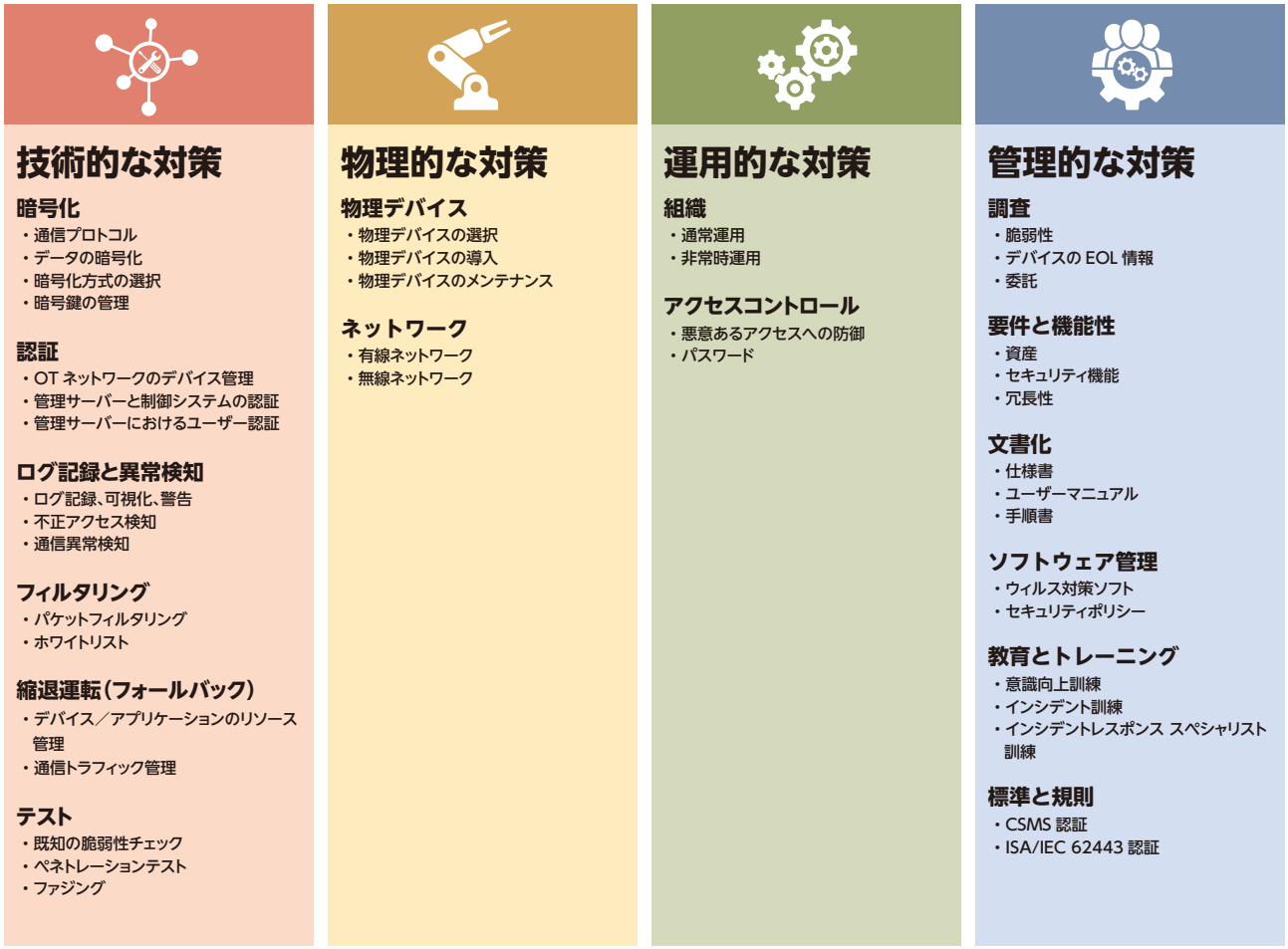


図8　セキュリティ対策の一覧

4.1. 技術的な対策

4.1.1. 暗号化

4.1.1.1. 通信プロトコル

M2M (Machine-to-Machine) 通信は、盗聴を防ぐために安全に暗号化する必要があります。安全な通信プロトコルの典型はSSL / TLS です。デバイス、機器、およびシステムが古く、安全な暗号化機能を持たない場合は、トンネリング技術を適用して外部アクセスをブロックすることが強く推奨されます。

4.1.1.2. データの暗号化

盗聴や盗聴を防ぐために、保存データの暗号化が推奨されます。持続的標的型攻撃(APT: Advanced Persistent Threat)を考慮すると、改ざんのリスクを軽減するために、データの暗号化は効果的です。プロセスレシピと関連データを暗号化することで、どのデータが重要かを難読化することもできます。

4.1.1.3. 暗号化方式の選択

最先端の暗号化方法を選択する際には、その暗号化のメリット・デメリット[4]を適切に考慮する必要があります。暗号化強度は、セキュリティ要件とハードウェアリソースの両方を考慮して慎重に選択する必要があります。

4.1.1.4. 暗号鍵の管理

暗号が解読可能であれば、システムは脆弱です。暗号鍵は適切な方法またはツールで保護する必要があります。最も一般的な方法は、アクセスパスワードを使用して暗号鍵を管理する暗号化アプリケーション・ソフトウェアを利用し、暗号鍵の使用を制御することです。ハードウェア暗号化モジュール(HSM)などの物理的なツールも解決策になります。

4.1.2. 認証

4.1.2.1. OTネットワークのデバイス管理

運用・制御技術(OT:Operational Technology)を担うネットワークでは、悪意のあるハッカーの攻撃を防ぐために、集中型のデバイス管理が強く推奨されます。一般的な方法は、デバイス認証にMACアドレスを使用することです。デバイスのMACアドレスが管理サーバーに登録されていない場合、デバイスの通信はネットワークで拒否されます。MACアドレスによる管理は有効ですが、MACアドレスは容易になりすましが可能であるため、他のセキュリティ対策と組み合わせて使用することが、より望ましい方法です。IEEE 802.1Xもよく知られている認証規格ですが、現時点では一部のIoT / OTデバイスでこの規格は利用できません。

4.1.2.2. 管理サーバーと制御システムの認証

管理サーバーと制御システム間の通信は、それらの間のほとんどのプロトコルが公に知られているため、典型的な攻撃の標的です。したがって、パスワード認証などのセキュリティ機能を適用して、それらを保護する必要があります。また、例えばOPC-UA(Open Process Control-Unified Architecture)で用いられるOLE(Object Linking and Embedding)などの産業用機器間のプロセス制御の規格に準拠した機器を用いることも有効です。

4.1.2.3. 管理サーバーにおけるユーザー認証

任意のユーザーが任意の場所から管理サーバーにアクセスできる場合、システムは脆弱です。アクセスは、管理された場所からに制限するべきであり、パスワード認証も登録された個人だけに配布されるパスワードを使って実行されるべきです。

4.1.3. ログ記録と異常検知

4.1.3.1. ログ記録、可視化、警告

システムで発生した異常の早期発見と予測のために、設備、機器、サーバーのログを取得し、状態

分析のためのデータを集約するログ記録の機能を実装する必要があります。システム内のコンポーネントが異常に動作した場合には、自動警告システムが必要です。異常動作には、頻度、量、パケットのヘッダー情報、予期しない停止などが含まれます。いくつかの異常はルールとして定義するのが難しいことに注意してください。そのような場合、自動異常検出の実現は難しいかもしれません。そのため、人間にとってのログの可読性を向上させることや、操作ログを可視化する方法も重要です。各セキュリティツール（4.1.3.3を参照）、サーバーアクセスログ、およびウイルス対策ソフトウェア（4.4.4.1を参照）からの情報を収集し、サイバーセキュリティの観点から分析する必要があります。取集したログの分析は、悪意のあるサイバー活動を検出するのに効果的です。

4.1.3.2. 不正アクセス検知

USBポートへのアクセスなど、重要な資産への不正アクセスはログに記録する必要があります。さらに、そのようなアクセスが予定されていない場合、これは自動的に警告を発し、システムへの論理接続はSNMP(Simple Network Management Protocol）などの機能を使用して自動的に遮断するようにします。

4.1.3.3. 通信異常検知

通信異常を検出するためのセキュリティツールは、異常な動作（頻度、通信量、送信元/宛先デバイスなど）および異常な内容（パケットのIPヘッダー、コマンド、パラメータなど）を含む通信を検出および識別することを目的としています。侵入検知システム（IDS）と侵入防止システム（IPS）は、マルウェアからの悪用パケットやマルウェアの拡散など、悪意のある通信や活動を監視および検出します。通信が改ざんされる可能性があるため、これを検知して処理対象から除外する機能（例えば、生産管理サーバーや工程監視制御装置から送信された情報のチェック）も用意する必要があります。

4.1.4. フィルタリング

4.1.4.1. パケットフィルタリング

許可されていないパケットは、そのようなパケットがシステム内のサーバー、機器、およびデバイスに転送されないように、ゲートウェイ（GW）、スイッチ、およびルータによってフィルタリングされる必要があります。

4.1.4.2. ホワイトリスト

例えば、送信元と宛先のペア、プロトコル、アプリケーションなどによって識別される不正な通信は、GW、スイッチ、およびルータなどのネットワークデバイスによってブロックされる必要があります。

4.1.5. 縮退運転（フォールバック）

4.1.5.1. デバイス／アプリケーションのリソース管理

管理サーバー、監視サーバー、制御サーバー、要求サーバー等のサーバーが利用するリソースが、常に使用可能であることを確認します。また、システム内で通信が確実に行われるように、RAMやCPUなどのアプリケーションが使用するリソース、およびアプリケーションの使用を適切に制限する必要があります。

4.1.5.2. 通信トラフィック管理

重要な制御プロトコルの通信が妨げられないように、通信トラフィックは制限されるべきです。トラフィックシェーパなど通信帯域幅の制御デバイスは、管理サーバー、要求サーバー、制御サーバー、および監視/制御機器の近くに導入する必要があります。

4.1.6. テスト

4.1.6.1. 既知の脆弱性チェック

システムコンポーネント（物理デバイス）と通信プロトコルに対し、既知の脆弱性をチェックする必要があります（4.2.1.1を参照）。そのような脆弱性が見つかった場合は、最新のプロトコルを使用する（4.1.1.1を参照）、デバイスのファームウェアを最新バージョンに更新する、リリース時にセキュリティパッチを適用するなどの適切な対策を講じる必要があります。

4.1.6.2. ペネトレーションテスト

ペネトレーションテスト（またはペンテスト）では、攻撃者がネットワークシステム内の管理サーバー、要求サーバー、監視サーバー、制御サーバーなどのサーバーに侵入できるかどうかを確認します。具体的には、ペネトレーションテストには、脆弱性の確認と計画の不備の特定が含まれます。

4.1.6.3. ファジング

ファジング（またはファジングテスト）では、予期しないサイズ、時間間隔、メタデータ、またはフォーマットなどのデータがシステムを入力し、予測不可能な脆弱性を発見します[5]。ファジングは、システムのセキュリティをテストするだけでなく、機器の予期しない動作を発見するためにも使用でき、システムの安全性の向上に役立ちます。

4.2. 物理的な対策

4.2.1. 物理デバイス

4.2.1.1. 物理デバイスの選択

第三者によって認定されている物理デバイスを選択することは、システム全体を保護するための信頼性の高いアプローチです。典型的な認証システムは、国際規格IEC 62443-4 [6]に基づいているEDSA認証です。IEC 62443-4では、単一の制御装置のセキュリティ要件が規定されています。また、一部の物理デバイスについては、製造およびサポートの終了が製造元によって事前に発表されています。このような物理デバイスが故障すると、交換が困難になるため、システム操作に影響を与える可能性が非常に高くなります。したがって、物理デバイスのサポート終了（EOL）情報を確認する必要があります（4.4.1.2を参照）。

4.2.1.2 物理デバイスの導入

物理デバイスが盗まれる可能性があるので、そのようなリスクを最小化して導入するべきです。選択肢はいくつかあります。例えば（1）物理デバイスから数メートル以内に人が近づけないように機器を配置する、（2）物理デバイスを囲む、（3）物理デバイスをケーブルロックで固定する、（4）防犯カメラを取り付ける、（5）物理デバイスが設置されている部屋に入る権限を制限する、（6）設

置場所を必要最小限の利害関係者にだけ通知する、(7) 物理デバイスが元の場所から移動したときに警報を発するセンサを導入する、などが挙げられます。また写真を撮って定期的に物理デバイスが存在する証拠を保管しておくことも重要です。さらに、物理デバイスに、アクセス可能な物理的なポートがあると、誤操作や悪意のあるアクセスにより、物理デバイス内の情報が盗まれたり改ざんされたりする危険性があります (4.3.2を参照)。これらの問題に対処するには、未使用の物理ポートを物理的にアクセス不能にするか、論理的にアクセスを無効にする必要があります。また、不正な接続が検出されたときに管理者に警告するために、管理者への警告機能も実装する必要があります。

4.2.1.3 物理デバイスのメンテナンス

物理デバイスのメンテナンスは、それらが正しく機能し続けるために重要です。メンテナンスは、故障、障害、またはその他の理由によって引き起こされる異常な動作などの予期しないリスクを軽減します。このような物理デバイスの状態を特定するために、人による、または他の独立したシステムによる検査を行う必要があります。メンテナンスはデバイスと機器の品質とパフォーマンスを維持するために常に重要です。具体的な方法やアクションは機器依存性が高いため、各デバイスのマニュアル等を参照してください。

4.2.2. ネットワーク

4.2.2.1. 有線ネットワーク

制御プロトコルと情報プロトコルの通信経路は物理的に分離する必要があります。また、ネットワークにおいて、制御メッセージを送受信するデバイスおよび産業用スイッチのインターフェースは、優先度制御 (VLANやQoSなど)、安全プロトコル (CIP Safetyなど)、および動作制御 (CIP Syncなど) に適合させる必要があります。

4.2.2.2. 無線ネットワーク

無線通信は第3章で議論された性質のために、いくつかの特定の脅威を持っています。「工場内のモノによる影響」および「空間を介した影響」を受ける性質に関しては、通信途絶が大きなリスクです。最も一般的な対策は、サイトサーベイ (現地調査) を実行することです。サイトサーベイの目的には、(1) 現場の無線伝送の品質を調査することによって、対象のデバイスまたは機器に到達するために使用できる周波数帯を見つけること、(2) サイト内の伝送品質を調査することによって適切なデバイス配置を推定すること、(3) 無線干渉を防ぐことができるファラデーケージなどの物理的シールドを取り付ける必要性を判断すること、および (4) システム内の電波が互いに干渉しないように無線チャネルを設計すること、が含まれます。

「空間を介したアクセス」という性質に関しては、データの盗難や改ざんが一般的な問題となります。データの盗難を防ぐため、通信は脆弱性のない最新の方法で暗号化され (4.1.1を参照)、アクセス用のパスワードは適切に設定されなければなりません (4.3.2.2を参照)。データの改ざんを防ぐために、不正な機器がシステムに接続しないように適切な認証 (4.1.2を参照) を採用する必要があります。さらに、ユーザー機器 (UE) の観点からは、SSID/APのなりすましが、データ盗難および改ざんの潜在的なリスクを伴う脅威となります。この問題に対処するには、SSIDを隠蔽する設定(ステルス機能)を使用する必要があります。また、可能であれば、WIPS (Wireless Intrusion Prevention System) などの偽装を検出する機能をシステムに導入する必要があります。

4.3. 運用的な対策

4.3.1. 組織

4.3.1.1. 通常運用

システム内のデバイスと機器を構成する手順は、事前に規定しておく必要があります。オペレーターのミスや悪意のある行為を防ぐために、人間が入力した値をシステムのユーザーマニュアルに従ってチェックすることによって、動作設定を二重にチェックし、絶対に安全にする必要があります（4.4.3.2 参照）。管理端末を他の目的に使用したり、他のサービスネットワークに接続したりすることは避けるべきです。構成情報などの機密情報の管理に関する規則を明確にし、関連当事者やサプライヤー／ベンダーを厳格に管理するように注意を払うことが重要です。認証アクセスログは、早い段階で、繰り返しの認証エラーによって示される不正なログインを検出するためにチェックする必要があります。ヒューマンエラーが発生する可能性がある手順では、自動化を採用することも重要です。

また、脆弱性が発見された場合のバグ修正パッチの配布手順を明確にすることが重要です。検証とソフトウェアの更新を実施するための手順は、マニュアルに明確に記載されていなければなりません [7]。

4.3.1.2. 非常時運用

システムの障害とシステムダウンを処理するためにチームを編成することは、不規則な状況に迅速に対応するために必要です。緊急事態が異なればリスクのレベルも異なるため、リスクレベルに応じていくつかのタスクフォースを編成する必要があります。

4.3.2. アクセスコントロール

4.3.2.1. 悪意あるアクセスへの防御

オペレーターのミスを防ぎ、インサイダーがシステムを攻撃するのを防ぐために、動作設定は二重にチェックし、確実なものにします。たとえば、人間が入力した値のチェックは、オペレーターのミスや悪意のある行動を避けるために実装されるべきです。

4.3.2.2. パスワード

不正なログインを防ぐために、管理サーバーなどのユーザーインターフェースで適切な認証を提供する必要があります。ID とパスワードを各ユーザーに提供し、それらを複数のユーザーで共有しないようにします。認証アクセスはログに記録する必要があります。これにより、繰り返しの認証エラーなどの不正ログインの兆候を早期に検出できるようになります。初期パスワードは、ユーザーがより強力なものに変更する必要があります。管理サーバーへのリモートアクセスが必要な場合は、双方向認証と IP アドレス制限を使用してアクセスを適切に制限する必要があります。

4.4. 管理的な対策

4.4.1. 調査

4.4.1.1. 脆弱性

ソフトウェアとハードウェアに関する既知の脆弱性情報を収集します。もし、そのような脆弱性がシステムに見つかった場合は、それらを修正し、対応する問題を解決する必要があります。バグ修正パッチが存在する場合は、正規のウェブサイトからダウンロードしたものを使用します。

4.4.1.2. デバイスのEOL情報

一部の機器では、製造業者はサポートまたは生産の終了を事前に発表します。そのような機器は故障時に交換することは不可能であるため、システム動作の保守に問題が生じる可能性があります。そのため、機器を設置する際には、EOL (End-of-Life) 情報を確認する必要があります。インストール後も、EOL情報を定期的に確認する必要があります。後継機および代替機に関する情報を収集することも重要です。さらに、機器のサプライチェーンをチェックし、機器不足のリスクを減らすために複数のサプライヤーから調達することが望ましいです。理想的には、システムは特定の機器または製造業者から独立するように設計されるべきです。製造の終了や製造者の倒産などの理由で装置のEOLが判明した場合、開発、検証、設置、労務費などの交換計画をEOLの前に確立して完了する必要があります。

4.4.1.3. 委託

システムの設計や開発を外部委託する場合は、インテグレーターを適切に選択、管理、検査する必要があります。そのためには、選定、管理、検査の基準を設定し、それらにコミットすることが望まれます。

4.4.2. 要件と機能性

4.4.2.1. 資産

システム内で守るべき資産 (第3章を参照) を最初に規定しなければなりません。次に、それらを保護するために適切な方法を選択する必要があります。そのような方法の例には、(1) メモリの保護、(2) 保存データの暗号化 (例えばPostgreSQLのpgcryptoモジュール)、(3) 通信の暗号化 (例えばセキュアプロトコル)、(4) データの監査 (例えばpg_auditモジュール)、(5) 情報アクセス制限、および (6) 物理的アクセス (例えば、物理的な鍵および設置場所へのアクセス制限) への警報の設置が挙げられます。このような機能や資産をデータベースで管理する場合は、SQLインジェクション対策も用意する必要があります (たとえば、sql_firewallモジュール)。さらに、システム内の資産を自動的に検出する機能もそれらを保護するのに効果的です。

4.4.2.2. セキュリティ機能

潜在的な脅威に対処するためのセキュリティ要件を明確にする必要があります。セキュリティ要件を満たすために、技術的および物理的手順 (4.1および4.2を参照) を実行する必要があります。また、対応するセキュリティ機能を動作させるのに十分なリソースをシステムに用意する必要があります[8]。たとえば、組み込みソフトウェアの場合、セキュリティ要件には、(1) 耐タンパー性に関する要件、および (2) 第三者製アプリケーションとの通信に関するポリシーが含まれます。一般に、

第三者のアプリケーションへの通信は許可されるべきではありません。

セキュリティ機能には、(1) 異常の兆候を検出するための手段 [7]、(2) 暗号鍵の情報登録、ユーザーマニュアルおよび自動設定の規制などの操作ミスおよび悪意のある操作を防ぐための手段、および (3) 生産設備の電磁波ノイズに対する耐性、が必要です。また、異常発生時の機器の復旧優先順位も明確にする必要があります。

4.4.2.3. 冗長性

システム全体の運用に影響を与える重要機器については、問題発生時にシステムが停止しないように冗長性を担保する機器を導入する必要があります。冗長性は、システムの緊急停止への対応、および重要なデータの保存に大変重要です。

また、サービスプロバイダーに障害を通知する仕組みや、冗長化された機器に自動で切り替える機能、例えばホットスタンバイも有効です。

4.4.3. 文書化

4.4.3.1. 仕様書

4.4.2 で明確にされたセキュリティ要件、機能およびシステム構成は、仕様書に規定します。

4.4.3.2. ユーザーマニュアル

4.4.3.1 に記載の仕様書に加えて、事業者が使用するマニュアルも作成する必要があります。マニュアルでは、オペレーターが間違えないように手順を明確に示す必要があります。

4.4.3.3. 手順書

デバイス、機器、および操作に関連する間違いが操作中に発生しないように、手順はマニュアル (4.4.3.2 を参照) に明確に記述する必要があります。

4.4.4. ソフトウェア管理

4.4.4.1. ウイルス対策ソフト

ウイルス対策ソフトウェアはできるだけ広範囲にインストールする必要があります。また、通常のマルウェアスキャン、指定された形式以外の形式で保存されたファイルの検出、および定期的なソフトウェアの更新をデフォルトとして設定する必要があります。

4.4.4.2. セキュリティポリシー

機器内での不必要なアプリケーションの実行を検出し、見つかった場合は自動的に停止する必要があります。各アプリケーションがアクセス可能なディスク領域は、許可されていないアクセスによる情報の盗難や改ざんのリスクを減らすために、ディスクパーティションによって制限されるべきです。さらに、各アプリケーションの信頼性をチェックするためのポリシーを事前に定義する必要があります。このようなポリシーには、アプリケーション開発者の確認、改ざん、脆弱性、疑わしい操作と通信、およびバックドアが含まれます。

4.4.5. 教育とトレーニング

4.4.5.1. 意識向上訓練

サイバーセキュリティの意識が低い組織は、意識が高い組織よりもセキュリティレベルは弱くなります。なぜなら、個人がインシデントの兆候を見たとしても、インシデントが発生していることに気づかない可能性があるためです。

4.4.5.2. インシデント訓練

人や組織が、さまざまなインシデントをシミュレーションするプログラムで訓練を行うことは、工場ではこれまで発生しなかったサイバーセキュリティのインシデントに対する復旧力を向上させるために非常に重要です。また、人々が被害の明確なイメージと特定のケースにおける効果的な対策を持つことができるようになります。

4.4.5.3. インシデント対応スペシャリスト訓練

インシデント対応スペシャリスト訓練は、インシデントに対応するときに問題を解決するためにインシデントレスポンス (IR) エンジニアを教育する技術トレーニングです。また、インシデント対応作業中に問題を解決するのに役立つ可能性がある第三者のスペシャリストとコミュニケーションをとるのに役立ちます。

4.4.6. 標準と規則

4.4.6.1. CSMS認証

CSMS 認証は、工場におけるサイバーセキュリティのリスクに対し、サイバーセキュリティ管理を改善するためのものです。

4.4.6.2. ISA/IEC 62443認証

ISA / IEC 62443認定は、工場でサイバーセキュリティを担当する個人を支援するためのものです。証明書のカテゴリごとに、それぞれの組織における責任者が明示されます。

5. 工場におけるセキュリティアセスメント

IEC 62433 [1]では、セキュリティアセスメントは、潜在的なリスクを減らすために工場内のリソースに対する脆弱性と脅威を特定する「リスクアセスメント」として記述されています。「セキュリティ監査」の目的は、適切な対策、つまり工場を保護するための「セキュリティ管理」を把握することです。「リスクアセスメント」および「セキュリティ監査」は、通常十分な知識とスキルを持った第三者、すなわちサイバーセキュリティリスクアセスメント担当者および監査人によって行われます。その結果、たとえサイバー攻撃が発生したとしても、工場が止まることのないようにすることが重要です。セキュティベンダーと一緒に管理をするために、作業の完全なスケジュールとマイルストーンと、発行されるレポートの種類を、アセスメント担当者／監査人に尋ねることが重要です。

工場スタッフは、専門的なITやサイバーセキュリティの用語に関心を持つ必要はありませんが、通常サイバーセキュリティリスクアセスメント担当者および監査人とは、工場のスタッフにはなじみのない専門用語を使ってやりとりをすることがあります。アセスメントや監査サービスの前後に、「工場および生産システムにとって何を意味するのか」などの質問をして、工場スタッフがコミュニケーションのギャップを埋めるように努める必要があります。

表3～5は、工場の構成要素と典型的なリスクおよび対策を表しています。表中の脅威は、次のような状況の例を示しています。

ユーザー認証情報の盗難/改ざん：攻撃者はリモートで情報を入手しようとします。

データ/ファイルの改ざん：攻撃者は、データとファイルをリモートで改ざんすることにより、製造工程で何かの問題を起こそうとします。

データ/コマンドの盗聴：攻撃者はプロセスのレシピと指示をリモートで取得しようとします。

不正なオペレーション：デバイスが悪意のあることをするために攻撃者にさらされます。

生産プロセスの改ざん/情報漏洩：攻撃者は生産ラインのデバイスを介してプロセスのレシピと指示を改ざん/情報漏洩させようとしています。

DoS攻撃：攻撃者は製造プロセスを妨害するつもりです。

これらの表は、工場スタッフがサイバーセキュリティリスクアセスメント担当者および監査担当者とのコミュニケーションを改善し、また推奨する対策の背後にある理由を理解するために役立ちます。

表３　工場における守るべき資産の構成要素と典型的なリスクとその対策（レベル 2-4）

レベル	リソース	データ	機能	インターフェース （無線通信で記載されていても、有線通信となる場合がある）
4	生産管理サーバー (HW/SW)	財務、人的資源、物流、製造、サプライチェーン、認証などの各種データ	製造などのデータ、データの送受信、認証の管理機能	LAN (有線)
	内部・外部の調達システム (HW/SW)	調達データ、認証データなど	調達データ、データの送受信、認証の管理機能	–
	ネットワーク (HW/SW)	上記データ	データの送受信機能	–
3	生産タスク指示、詳細な生産計画、信頼性保証、拠点内指示最適化のためのサーバー (HW/SW, 例：SCADA サーバー)	運用情報、指示記録、製品品質などのデータ、認証データ	プロセス計画、生産プロセス管理、プロセス・製品の品質管理、拠点在庫管理、生産トレース、設備メンテナンス、データ、データの送受信、認証の機能	LAN (有線)
	ネットワーク (HW/SW)	上記データ	データの送受信機能	–
2	フィールドデバイスの監視・制御のためのサーバー (HW/SW)	フィールドデバイスへのコマンド、フィールドデバイスの状態、監視・作動プログラム、認証などのデータ	フィールドデバイスのセンシング・操作、データの送受信、認証の機能	LAN (有線)、フィールドバス
	ネットワーク (HW/SW)	上記データ	データの送受信機能	–

リスク	脅威	対策																	
		技術的						物理的		運用的		管理的							
		4.1.1. 暗号化	4.1.2. 認証	4.1.3. ログ記録と異常検知	4.1.4. フィルタリング	4.1.5. 縮退運転（フォールバック）	4.1.6. テスト	4.2.1. 物理デバイス	4.2.2. ネットワーク	4.3.1. 組織	4.3.2. アクセス制御	4.4.1. 調査	4.4.2. 要件と機能	4.4.3. 文書化	4.4.4. ソフトウェア管理	4.4.5. 教育と訓練	4.4.6. 標準と規制
生産データの改ざん、漏洩	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●	すべてに適用	●		●				●	●		すべてに適用	●	すべてに適用	すべてに適用
	データやファイルの改ざん	●	●		●		●				●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●		●		
	不正なオペレーション	●	●					●	●	●							
	生産プロセルの改ざん、情報漏洩	●	●		●		●	●		●	●	●	●				
調達データの改ざん、漏洩	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●		●		●				●	●			●		
	データやファイルの改ざん	●	●		●		●				●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●		●		
	不正なオペレーション	●	●					●	●	●							
ネットワークの停止、生産データの漏洩.	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●		●		●				●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●		●		
	DoS攻撃				●	●			●				●				
生産管理の不良、生産プロセス情報の漏洩	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●		●		●				●	●			●		
	データやコマンドの改ざん	●	●		●		●		●		●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●		●		
	不正なオペレーション	●	●		●			●	●	●							
	生産プロセルの改ざん、情報漏洩	●	●					●		●	●	●	●				
	DoS攻撃				●	●			●				●				
ネットワークの停止、生産データの漏洩.	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●		●		●				●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●		●		
	DoS攻撃				●	●			●				●				
プロセス管理の不良、プロセス情報の漏洩	データやコマンドの改ざん	●	●		●		●		●		●	●			●		
	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●		●		●				●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●				
	不正なオペレーション	●	●					●	●	●							
	生産プロセルの改ざん、情報漏洩	●	●					●		●	●	●	●		●		
	DoS攻撃				●	●			●				●		●		
ネットワークの停止、生産データの漏洩.	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●		●		●				●	●			●		
	データやコマンドの盗聴	●	●		●		●		●			●	●		●		
	DoS攻撃				●	●			●				●		●		

表４　工場における守るべき資産の構成要素と典型的なリスクとその対策（レベル 0-1）

レベル	リソース	データ	機能	インターフェース （無線通信で記載されていても、有線通信となる場合がある）
1	フィールドデバイスのセンシング、操作に関わるローカル又は基本コントローラ（HW/SW） 例：DCS、PLC、RTU	フィールドデバイスへのコマンド、フィールドデバイスの状態、監視・作動プログラム、認証などのデータ	フィールドデバイスのセンシング・操作、データの送受信、認証の機能	LAN（有線/無線）、フィールドバス、シリアルインターフェース（有線）
	リモコン	操作情報	遠隔操作	IEEE 802.15.4g, その他
	移動機器（スタッカクレーン, AGV, シャトル, コンベア, 各種搭載機/注入器）	制御情報、監視情報	移動体制御	IEEE 802.11
0	動線分析機器	ビーコン、地磁気、加速度、方位、画像（バーコード）、映像	動線分析	IEEE 802.11/802.15.4g, BLE
	PLC（上位コントローラへの状態情報通知）	PLCの稼働状況	稼動状況計測	IEEE 802.11/802.15.4g
	保全作業支援機器	画像、音声、画像通話表示	保全支援	IEEE 802.11, BT
	測位機器（生産管理）	人やモノのリアルアイム位置、みずすましの位置・ルート	測位（生産管理）	IEEE 802.11/802.15.4g, BLE, UWB
	測位機器（資産管理）	設備や資材の位置	測位（資産管理）	BLE
	警光灯/回転灯	設備状態情報	設備状態表示	IEEE 802.15.4g
	作業指示機器	作業指示情報（段取り、手順、搬送）	作業指示	IEEE 802.11
	ピッキング指示機器	ピッキング指示情報（選別、分別）	ピッキング指示	Others (using specific frequency)
	安全確認機器（人）	安全確認情報、バイタル情報、安全設備装着確認情報、危険アラーム	安全情報収集（人）	IEEE 802.15.4g, BLE
	安全確認機器（環境）	有毒ガス、酸素濃度、放射線被爆	安全情報収集（環境）	Others (using specific frequency)
	カメラ（ポカヨケ）	画像	ポカヨケ監視	IEEE 802.11
	トルクレンチ（ポカヨケ）	ネジ締め付け情報	締め付け計測・確認	IEEE 802.11, BT, BLE
	部品在庫監視機器	在庫情報	在庫管理	RFIC using Sub-1GHz

リスク	脅威	対策																
		技術的						物理的		運用的		管理的						
		4.1.1. 暗号化	4.1.2. 認証	4.1.3. ログ記録と異常検知	4.1.4. フィルタリング	4.1.5. 縮退運転（フォールバック）	4.1.6. テスト	4.2.1. 物理デバイス	4.2.2. ネットワーク	4.3.1. 組織	4.3.2. アクセス制御	4.4.1. 調査	4.4.2. 要件と機能	4.4.3. 文書化	4.4.4. ソフトウェア管理	4.4.5. 教育と訓練	4.4.6. 標準と規制
プロセスの不良、プロセスデータの漏洩	データやコマンドの改ざん	●	●	●	●		●		○		◎	◎		◎	◎	◎	◎
	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●	●	●		●				◎	◎		◎	◎	◎	◎
	データやコマンドの盗聴	●	●	●	●		●		○			◎	◎	◎	◎	◎	◎
	不正なオペレーション	●	●	●	●			○	○	◎				◎		◎	◎
	生産プロセルの改ざん、情報漏洩	●	●	●				○		◎	◎	◎	◎	◎		◎	◎
	DoS攻撃			●	●	●			○				◎	◎	◎	◎	◎
生産停止、機能不良	生産プロセルの改ざん、情報漏洩	●	●	●			●		○		◎				◎	◎	◎
生産停止、機能不良																	
機能不良	DoS攻撃				●	●			○				◎		◎	◎	◎
制御不良	ユーザー認証情報（ID、パスワード等）の盗難、改ざん		●	●			●				◎				◎	◎	◎
生産停止、機能不良																	
機能不良	データやコマンドの改ざん	●	●	●			●		○		◎				◎	◎	◎
機材、材料の紛失、機能不良																	
機能不良																	
生産停止、機能不良																	
生産停止、機能不良																	
作業者のケガ、生産停止	DoS攻撃				●	●			○				◎		◎	◎	◎
不良品の増加（歩留まり低下）、作業者の健康被害、生産停止																	
不良品の増加（歩留まり低下）、生産停止																	
不良品の増加（歩留まり低下）、生産停止																	
生産停止、機能不良																	

表５　工場における守るべき資産の構成要素と典型的なリスクとその対策（レベル 0）

レベル	リソース	データ	機能	インターフェース （無線通信で記載されていても、有線通信となる場合がある）
0	検査機器	画像（寸法、歪・へこみ）、音響（駆動部の音）、X線、動画（不良状態、異物混入）	製品検査	IEEE 802.11
	電力計測機器	電力量、電流波形	電力計測、電力消費計測	IEEE 802.11/802.15.4g, BT
	流量測定機器	水量	流量計測	IEEE 802.11
	空調測定機器	気流	空調計測	IEEE 802.11/802.15.4g, BT
	温湿度測定機器	周囲温湿度、機器／ツール温度	温度計測、湿度計測	IEEE 802.11/802.15.4g, BT, LPWA
	トルク測定機器	トルクチェック（規定値）、トルク波形、トルク設定	トルク計測	IEEE 802.11, BT
	設備・環境監視機器	画像、音響、匂い	設備・環境監視	IEEE 802.11
	衛生監視機器	細菌数	衛生監視	IEEE 802.11
	空気監視機器	塵埃量（パーティクル）、CO2 濃度、VOC（揮発性有機化合物）濃度	空気監視	IEEE 802.11/802.15.4g, BT
	照度管理機器	照度	照度管理	IEEE 802.15.4g
	持ち込み物監視機器	電波、熱	電子機器持ち込み監視	IEEE 802.15.4g
	監視カメラ	画像	セキュリティ（侵入検知）	IEEE 802.11
	生産状態表示機器	滞留、生産／非生産	生産状態表示	IEEE 802.11/802.15.4g
	作業記録機器	作業証明、作業ログ、作業ミス記録	作業記録	IEEE 802.11
	計数機器	カウンター情報	計数	IEEE 802.11/802.15.4g

	リスク	脅威	対策															
			技術的						物理的		運用的		管理的					
			4.1.1. 暗号化	4.1.2. 認証	4.1.3. ログ記録と異常検知	4.1.4. フィルタリング	4.1.5. 縮退運転（フォールバック）	4.1.6. テスト	4.2.1. 物理デバイス	4.2.2. ネットワーク	4.3.1. 組織	4.3.2. アクセス制御	4.4.1. 調査	4.4.2. 要件と機能	4.4.3. 文書化	4.4.4. ソフトウェア管理	4.4.5. 教育と訓練	4.4.6. 標準と規制
	不良品の増加（歩留まり低下）																	
	不良品の増加（歩留まり低下）																	
	不良品の増加（歩留まり低下）																	
	不良品の増加（歩留まり低下）																	
	不良品の増加（歩留まり低下）																	
	不良品の増加（歩留まり低下）																	
	不良品の増加（歩留まり低下）、作業者の健康被害																	
	作業者の健康被害	データやコマンドの改ざん	●	●	●			●		●		●				●	●	●
	不良品の増加（歩留まり低下）、作業者の健康被害																	
	作業者の健康被害																	
	不良品の増加（歩留まり低下）																	
	侵入検知の失敗																	
	生産収量の過不足																	
	記録のない作業の発生																	
	不良品の増加（歩留まり低下）、生産収量の過不足、生産停止																	

参考文献

[1] Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models, IEC/TS 62443-1-1, Edition 1.0 2009-07, International Electrotechnical Commission (IEC).

[2] Enterprise - Control System Integration - Part 1: Models and terminology, IEC 62264-1, Edition 2.0, 2013-05, International Electrotechnical Commission (IEC).

[3] Secure Architecture Design, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), https://ics-cert.us-cert.gov/Secure-Architecture-Design

[4] CRYPTREC Encryption, https://www.cryptrec.go.jp/english/list.html

[5] Fuzzing, The Open Web Application Security Project (OWASP), https://www.owasp.org/index.php/Fuzzing

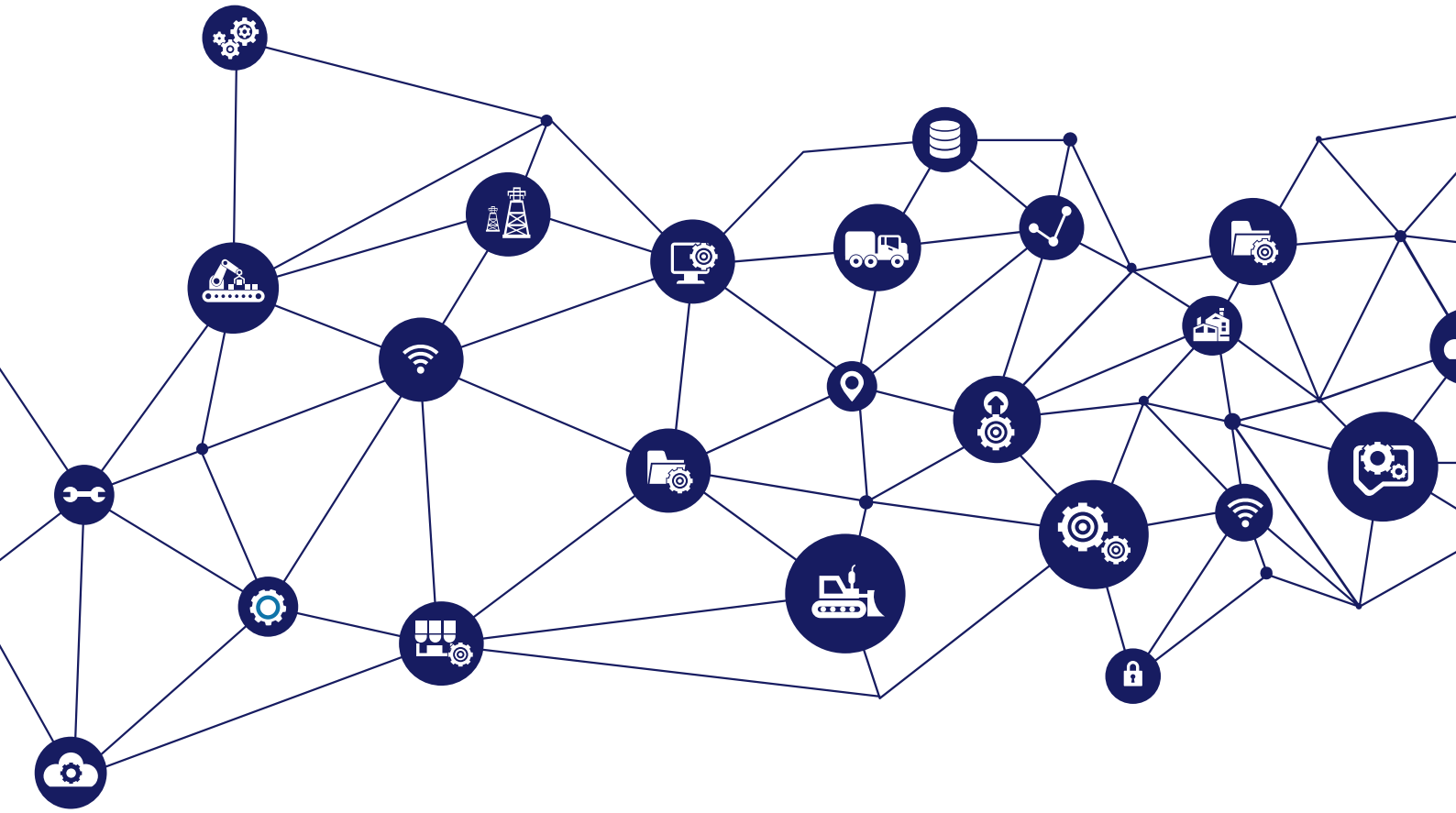
[6] Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1, Edition 1.0 2018-01, International Electrotechnical Commission (IEC).

[7] Guidance for Practice Regarding "IoT Safety/Security Development Guidelines," Information-technology Promotion Agency (IPA), https://www.ipa.go.jp/files/000063228.pdf
日本語版 「IoT 開発におけるセキュリティ設計の手引き」
https://www.ipa.go.jp/security/iot/iotguide.html

[8] C. H. Gebotys, "Security in Embedded Devices", Springer, 2010.

略号

AGV	Automated Guided Vehicle
AP	Access Point
APT	Advanced Persistent Threat
BLE	Bluetooth Low Energy
BT	Bluetooth
CIP	Critical Infrastructure Protection
CPU	Central Processing Unit
CSMS	Certified Software Measurement Specialist
DCS	Distributed Control Systems
DDoS	Distributed Denial of Service attack
DMZ	Demilitarized Zone
DoS	Denial of Service
EDSA	Embedded Device Security Assurance
EOL	End of Life
ERP	Enterprise Resource Planning
GW	Gateway
HMI	Human Machine Interface
HSM	Hardware Encryption Module
IACS	Industrial Automation and Control System
ID	Identifier (or Identification)
IDS	Intrusion Detection System
IEC	The International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IR	Incident Response
ISA	The International Society of Automation
IT	Information Technology
LAN	Local Area Network
LPWA	Low Power Wide Area
M2M	Machine to Machine
MAC	Media Access Control
MES	Manufacturing Execution Systems
OLE	Object Linking and Embedding
OPC-UA	OLE for Process Control-Unified Architecture
OT	Operational Technology
PC	Personal Computer
PLC	Programmable Logic Controller
QoS	Quality of Service
RAM	Random Access Memory
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UE	User Equipment
USB	Universal Serial Bus
UWB	Ultra-WideBand
VLAN	Virtual LAN
WEP	Wired Equivalent Privacy
WIPS	Wireless Intrusion Prevention System



FLEXIBLE FACTORY
PARTNER ALLIANCE

Contact:
https://www.ffp-a.org/
info@ffp-a.org