資料４

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

令和４年３月２４日

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）

工場サブワーキンググループ

変更履歴

発行日	版	概要

内容

1. はじめに [1] 3
1.1. 工場セキュリティガイドラインの目的 [1.1.5] 3
1.2. ガイドラインの適用範囲 [1.2] 6
2. 本ガイドラインの想定工場 [3] 7
2.1. 想定企業 [3.1] 7
2.2. 想定組織構成 [3.2] 8
2.3. 想定生産ライン [3.3] 8
2.4. 想定業務 [3.4] 10
2.5. 想定データ [3.5] 11
2.6. 想定ゾーン [3.6] 11
3. セキュリティ対策企画・導入の進め方 [6.1] 13
3.1. ステップ 1 ：情報収集・整理 [6.1.1] 14
3.1.1. ステップ 1-1：セキュリティ対策検討・企画に必要な要件の整理 [2.2] 14
3.1.2. ステップ 1-2：業務の整理 [2.2] 16
3.1.3. ステップ 1-3：業務の重要度の設定 [2.2] 16
3.1.4. ステップ 1-4：保護対象の整理 [2.2] 18
3.1.5. ステップ 1-5：保護対象の重要度の整理 [2.2] 21
3.1.6. ステップ 1-6：ゾーンの整理と、ゾーンと業務、保護対象の結びつけ 23
3.1.7. ステップ 1-7：ゾーンと、セキュリティ脅威による影響の整理 [2.2.2] 25
【参考】経営層による取組みの宣言 [6.1.2] 30
3.2. ステップ 2：セキュリティ対策の立案 [6.1.3] 31
3.2.1. ステップ 2-1：全体方針の策定 31
3.2.2. ステップ 2-2：想定脅威に対するセキュリティ対策の対応づけ 38
(1)システム構成面での対策
(2)物理面での対策
3.3. ステップ 3：セキュリティ対策の実行・管理体制の構築 [6.1.4･5] 55
(1)ライフサイクルでの対策
(2)サプライチェーン対策
付録 A 用語／略語 69
付録 B 工場システムを取り巻く社会的セキュリティ要件 76
3.1. 法規制、標準規格、ガイドライン準拠にかかわる要件 [6.1] 76
3.1.1. 法規制によるセキュリティ対策の要求 [6.1.1] 76
【参考：業界毎のセキュリティにかかわる法規制】 77

●電力分野におけるセキュリティにかかわる法規制　[6.1.2] 77
●自動車分野におけるセキュリティにかかわる法規制　[6.1.3] 77
●医療機器分野におけるセキュリティにかかわる法規制　[6.1.4] 77
●重要インフラ分野におけるセキュリティにかかわる法規制　[6.1.5] 78
3.1.2.　セキュリティにかかわる標準規格・ガイドライン準拠の要求　[6.1.6] 79
3.2.　国・自治体からの要求　[6.2] 86
3.3.　産業界からの要求　[6.3] 87
3.4.　市場・顧客からの要求　[6.4] 88
3.5.　取引先からの要求　[6.5] 89
3.6.　出資者からの要求　[6.6] 89
付録 C　関係文書におけるセキュリティ対策レベルの考え方 90
3.1.　セキュリティ対策レベル　[8.1] 90
3.1.1.　代表的なセキュリティ対策レベル評価基準　[8.1.1] 90
3.1.2.　セキュリティ対策レベルの定義例　[8.1.2] 92
付録 D　関連／参考資料 95
付録 E　チェックリスト 98
付録 F　調達仕様書テンプレート(記載例) 102
コラム 1：工場セキュリティを巡る動向　[2] 104
3.1.　製造業／工場を取り巻く環境動向[1.1.1] 104
3.2.　工場における産業制御システムのセキュリティにかかわる環境動向　[1.1.3] .. 107
3.3.　工場における産業制御システムのセキュリティ対策実施の動向　[1.1.4] 108
コラム 2：工場システムの目的や製造業／工場の価値から観たセキュリティ [2.1.1] 110
コラム 3：スマート工場への流れ 112
本ガイドラインの検討体制 114
謝辞 115

	工場セキュリティについて知りたいこと	本ガイドラインの 記載箇所
	工場のセキュリティ対策はどのような流れで進めていけばいいか知りたい。	3. セキュリティ対策企画・導入の進め方 （P13-P70）
	工場のセキュリティ対策にはどのようなものがあるか知りたい。	3.2. ステップ 2: セキュリティ対策の立案 （P31-P56） 3.3. ステップ 3: セキュリティ対策の実行・管理体制の構築 （P57-P70）
	工場のセキュリティを考えていく際に考慮しなければいけない要件について知りたい。	付録 B 工場システムを取り巻く社会的 セキュリティ要件 （P78-P91）
	工場のセキュリティをどのように管理していけばいいか知りたい。	3.3. ステップ 3: セキュリティ対策の実行・管理体制の構築 （P57-70）
	保護対象や業務、セキュリティ対策の優先順位を付けていくにあたり、どのような考え方があるか知りたい。	付録 C セキュリティ 要求レベル （P92-P96）
	工場を取り巻くサイバーセキュリティ環境はどのようなものか知りたい。工場へのサイバー攻撃によりどのような被害が過去にあったのか知りたい。	コラム 1 工場セキュリティを巡る動向 （P106-111）
	関連する業界標準・国際標準規格を知りたい。工場を運用している際にどのような者からどのような要求をされることがあるのか知りたい。	付録 B 工場システムを取り巻く社会的 セキュリティ要件 （P78-P91） 付録 D 関連／参考資料 （P97-P99）
	具体的にどこまで対策ができているかイメージしたい。	付録 E チェックリスト （P100-P103）
	製品調達の際に具体的にどのようなことを調達仕様に落とし込めばいいかイメージしたい。	付録 F 調達仕様書 テンプレート（記載例） （P104-P105）

1. はじめに［1］

1.1. 工場セキュリティガイドラインの目的［1.1.5］

工場システム（産業制御システム(ICS/OT)やこれらを構成する機器、及び接続されるシステム・機器）[1]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。しかし、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り、新たな付加価値が生み出される取組が進められる一方で、工場等のネットワークをインターネットにつなぐ必要性や機会が増加することによる、新たなセキュリティ上のリスク源も増加している。特に、工場等の製造現場においては、以下のような特徴があるため、こうした特徴に即したサイバーセキュリティ対策が必要となる。

- 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、機器稼働等の維持や安全の確保が求められる。
- 古い設備が運用されている場合など、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。
- 工場等の規模や性質によって行うべき対策が異なる。

また、一般的に、製造業／工場では、

・ 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)

という価値が重視されている[2]。

工場と言ってもその規模や機器・システムは千差万別であるため、業界・業種ごとに実施すべき事項は異なることから、本ガイドラインは特定の業界・業種や製造する製品という観点で対象を限定したものではない。

---

[1] FA（Factory Automation）システムのほか、PA（Process Automation）システムにおいても参照可能な内容も含んでおり、適宜読み替えることを期待する。

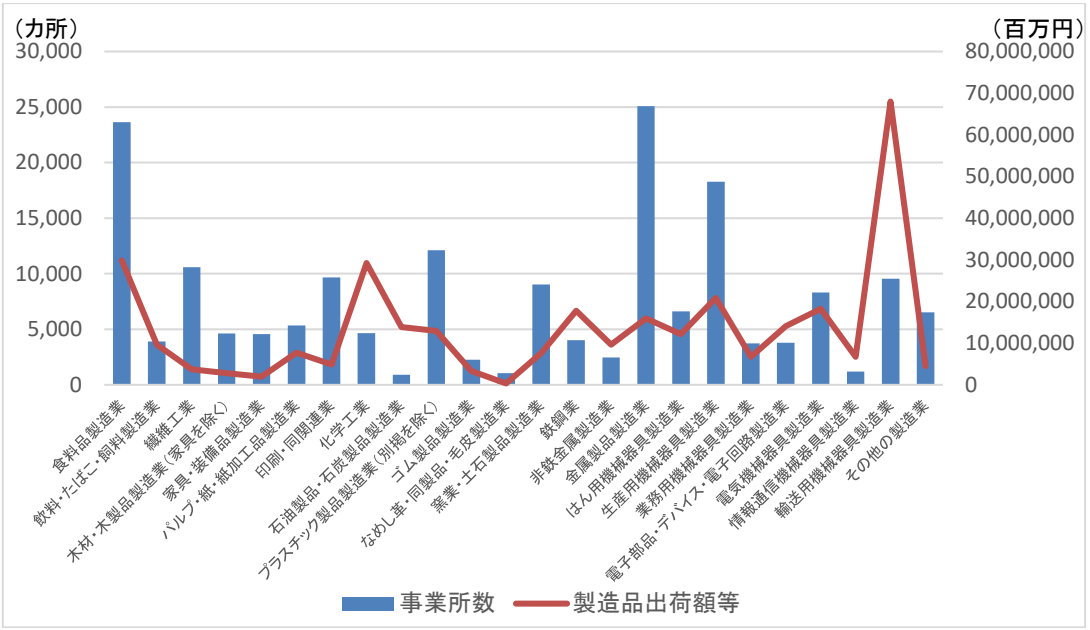
[2] 工場では、事業／生産継続（BC）のための事業継続計画が策定することが一般的であるが、必ずしも工場の稼働維持を目指すものではなく、サイバー攻撃により工場システムの制御権が奪われる等の場合は、安全確保（S）のために能動的に工場システムを停止するという選択を行うこともありうる。

また、本ガイドラインは、業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを「手引き」として示し[3]、また、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ている。

重要なことは、業界団体や個社が、自らの工場を取り巻く業界・業種の環境を整理し、当該環境と業界・業種が重要視する価値観を比較考量し、当該価値観を維持・発展させていくために必要な工場のセキュリティとは何かを考え、本ガイドラインに示した考え方やステップ、対策を参照しつつ、業界・業種の事情に応じたガイドラインを作成するなどしながら工場へのセキュリティ対策を進めていく、といった行動に移すことである。

本ガイドラインは、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、とりわけ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を目的としている。

その結果、BC／SQDC の価値がサイバー攻撃により棄損されることを防止し、更にはセキュリティが担保されることで IoT 化や自動化が進み、多くの工場の現場から新たな付加価値が生み出されていくことを期待している。



出所）経済産業省工業統計調査（2020 年確報）を元に作成

[3] セキュリティ対策の導入に伴う製品原価への影響や工程変更に伴う稼働や品質への影響など、セキュリティ対策が BC/SQDC に影響を及ぼすことへの影響にもなるべく配慮した考え方を示している。

図 1-1 製造業における事業所数・製造品出荷額等（2019 年）

【参考】工場システムにおいてセキュリティ脅威により生じる影響[4]の例

- 製品事業の伸張や事業／生産の継続(BC: Business Continuity)への影響
- 工場の安全確保(S: Safety)、製品の品質確保(Q: Quality)、納期遵守・遅延防止(D: Delivery)、コスト低減(C: Cost) への影響
- 工場システム及び機器の正常動作確保、適正なフィードバック制御の実現の妨害
- 製品や生産(ノウハウ)にかかわる情報やデータの外部漏えい
- 自社工場の機器を踏み台にした、エンジニアリングチェーン、サプライチェーン、バリューチェーンの連携先へのセキュリティ問題の拡大
- 意図せず製品に内包された不正な部品や悪意のある機能(マルウェア)による、外部からの不正な利用・制御や、製品の稼働の妨害、製品利用者の情報の外部漏えい

[4] これらの影響を緩和するためには、工場システム及び構成要素(ネットワーク、機器・部品、機能・プログラム、データ)の可用性(Availability)、正常性[完全性](Integrity)、真正性確保(Authenticity)、機密性(Confidentiality)といったセキュリティ要素を確保することが必要である。これらのセキュリティ要素を確保するためには、システム利用者やシステムを構成する機器・部品、機能・プログラム、データそれぞれのアクセス制御(Access Control)、そして事後の責任追跡性確保(Accountability)、否認防止(Non-Repudiation)を実現するための各種セキュリティ機能が必要になる。

1.2. ガイドラインの適用範囲 [1.2]

本ガイドラインの想定読者は、例えば以下を想定している[5]が、IT システム担当や生産関係部門の間で、部門間・担当間の立場や価値観の違い[6]を認識しつつ、セキュリティ対策の企画・実施に向けたコミュニケーションを行っていくことが重要である。

- IT システム部門
- 生産関係部門(生産技術部門、生産管理部門、工作部門　等)[7]
- 戦略マネジメント部門(経営企画等)
- 監査部門
- 機器システム提供ベンダ、機器メーカ(サプライチェーンを構成する調達先を含む)

本ガイドラインの適用範囲となる機器・システムは以下を想定している。

- 本ガイドラインの対象となる機器・システムは、新設・既設によらず、工場における産業制御システム(ICS/OT)としており、事務系の情報システム(IT)は対象としていない。

[5] 本ガイドラインは主に想定読者を中心とした実務層向けのものであるが、セキュリティの考え方が適切に経営層（CTO、CISO 等）に浸透していないと考えられる場合には、本ガイドラインを参照しつつ、想定読者が経営層（CTO、CISO 等）を始めとした意思決定を行う者と適切なコミュニケーションを行うことを期待する。

[6] 例えば、IT システム部門は工場のシステムのみならず自社が有するシステム全体の性能を重視し、生産現場は製品製造の遅延防止や稼働の維持、安全の確保等を重視するなど、各者・各部門が置かれた環境や価値観は様々である。

[7] 当該部門で中心となる者については、例えば、機器・システム及びセキュリティの調達要件の作成者や機器・システムの構築者、管理者、運用者、保守者が考えられる。

2. 本ガイドラインの想定工場 [3]

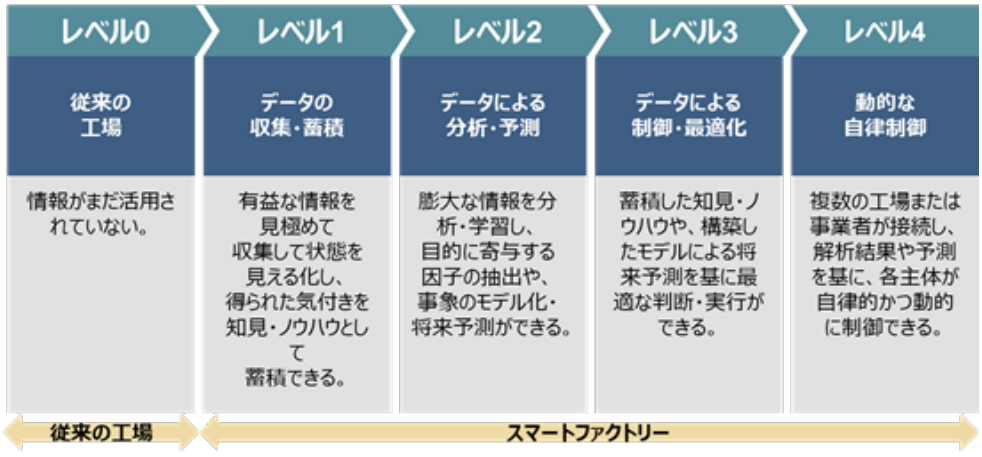
一般に工場システムと言っても、規模の大小や、製造する製品に応じて、それを構成する機器類や接続するシステムには差異がある。そこで本章では、工場システムのセキュリティ対策を提示するにあたり、わかりやすさの観点からある工場を想定工場として設定する。

なお、読者の置かれた環境と想定工場とが必ずしも一致しない部分もあると考えられるため、適宜読み替えることを期待する。

2.1. 想定企業 [3.1]

- 経営者によって DX(デジタルトランスフォーメーション)が求められている
- 電子機器メーカ
- 複数の拠点に工場が存在し、それぞれの拠点で製品を生産
- 本社が管理する拠点間ネットワークで拠点同士は接続されるが、拠点内ネットワークは拠点ごとに管理
- 工場における有益な情報を見極めて収集し、状態を見える化し、得られた気付きを知見・ノウハウとして蓄積できている [8]。

[8] このような場合は、経済産業省の「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」に照らせば、スマートファクトリーの段階のレベル１に相当する。スマートファクトリーとは、データ活用・分析により製造管理の高度化を実現する工場を指す。一般的に、レベルが上がるにつれてサイバー空間との結びつきが強くなり、その結果セキュリティリスクも上がると考えられることから、レベルに応じたセキュリティ対策を行うことが重要である。



出所）経済産業省「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」(2021 年 3 月)

2.2. 想定組織構成 [3.2]

- **生産技術・管理部門:**
  生産ライン設備の構築、管理を実施
- **工作部門:**
  生産ラインを運用し、生産計画に基づき実際の生産を実施
- **営業部門:**
  製品の営業管理、顧客管理を実施
- **資材部門:**
  生産に必要な資材の調達、管理を実施
- **品質管理部門:**
  製品及び部品・部材の品質を確保するための検査、管理を実施
- **情報システム部門:**
  OA(Office Automation)系を中心に、ネットワーク、サーバ、端末の管理を実施

なお、実際の企業における関連組織はこれより多い場合もあるが、各組織の役割を分かりやすくするために、上記の6部門とした。

2.3. 想定生産ライン [3.3]

- 生産ラインでは電子機器に組み込まれるプリント基板を生産
- 生産自体は自動化されており、生産指示に基づいて複数機種を生産可能。
- 段取り掛け、部品の補充などは工場の従業員が実施
- 工場内には複数の生産ラインが存在し、それぞれ独立して異なる機種を生産可能
- 生産設備(装置・機器)は設備メーカから導入し、生産技術・管理部門が生産ラインを構築・管理
- 設備の保守は設備ベンダが実施
- 自動倉庫は、設備ベンダが保守に備えてリモートで状態監視、及び現地での保守を実施

以下に、想定生産ラインを含む工場システムの例と、その構成要素を示す。本ガイドラインでは、この工場システム例を用いてセキュリティ対策を提示する。

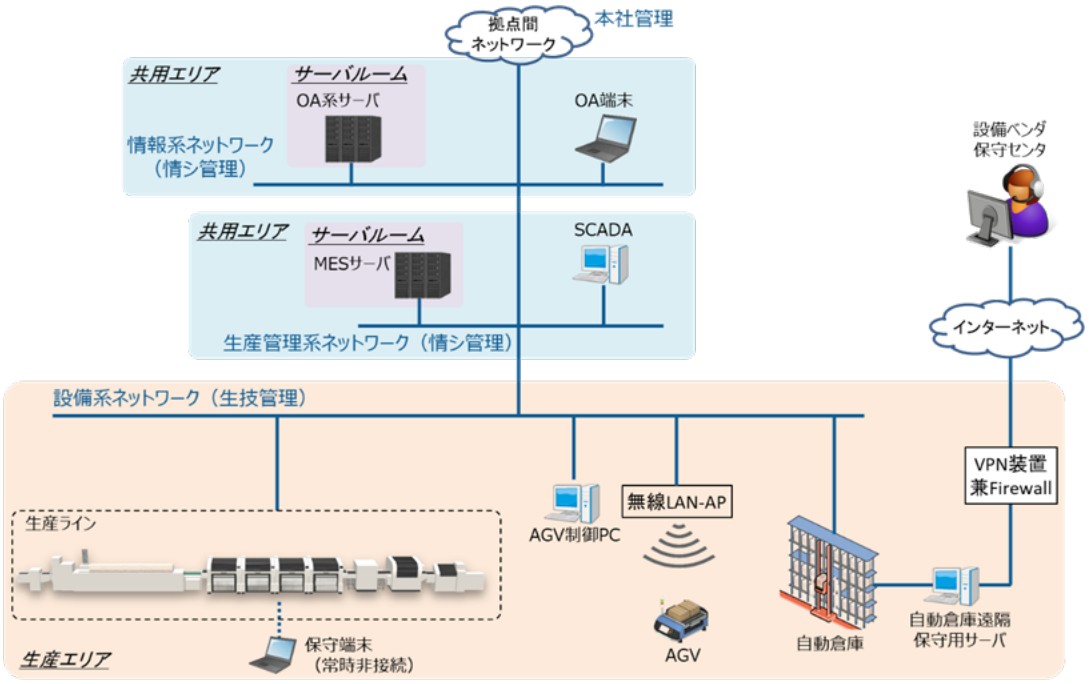


図 2-1　工場システムの例

- ネットワーク[9]
  - **設備系ネットワーク**:
    生産設備が接続されるネットワーク
  - **生産管理系ネットワーク**:
    生産管理を行うサーバなどが接続されるネットワーク
  - **情報系ネットワーク**:
    OA 業務、製品設計用の端末が接続されるネットワーク

- 装置・機器（機能・プログラム）[10]
  - **VPN 機器**:
    設備ベンダがリモートでアクセスする際に利用する、セキュアな通信を実現するための機器。設備ベンダの保守センタ以外からのアクセスは許可しないようにファイアウォール(アクセス制御)機能を内蔵
  - **無線 LAN アクセスポイント（無線 LAN-AP）**:
    AGV（無人搬送車）との通信を行うためのネットワーク機器
  - **ルータ（設備系-生産管理系）**　:
    設備系ネットワークと生産管理系ネットワーク間のネットワーク機器

9 セキュリティ要素としては、可用性、完全性、責任追跡性が考えられる。
10 セキュリティ要素としては、可用性、完全性、真正性、責任追跡性が考えられる。

- MES サーバ:
  生産計画、生産実績のデータ管理、及び生産ラインに対しての生産指示を行うサーバ
- 生産ライン:
  製品の生産を行うために用いる設備
- SCADA:
  生産ラインの生産状況の監視を行う PC
- 保守用 PC:
  生産設備のメンテナンスに用いる PC
- AGV(無人搬送車)制御 PC:
  AGV(無人搬送車)の運転計画を立案し、AGV を制御する PC
- AGV(無人搬送車):
  部材を運ぶ装置
- 自動倉庫:
  部材の保管と入出庫を行う装置
- 自動倉庫遠隔保守用サーバ:
  設備ベンダ保守センターが自動倉庫をリモートから保守する際に利用するサーバ
- OA 系サーバ:
  事務用途で利用するサーバ。営業管理ツール、社内ワークフローシステム、ファイルサーバなどを想定
- OA 端末:
  事務用途で利用する PC

2.4. 想定業務 [3.4]

- 生産計画設定
- 生産(＋検査)
- 生産状況監視(現場)
- 部材補充(現場へ)
- 部材購入(倉庫へ)
- 生産性分析
- トレーサビリティデータ参照
- メンテナンス
- リモートメンテナンス

なお、工場システムにおいては、安全に配慮の上、安定した品質の製品を計画どおりに生産し続けることが重要となるが、業務に応じて重要度は異なる。

2.5. 想定データ [3.5]

生産設備やネットワークの停止・故障などにより業務が影響を受けるが、保存されているデータの消失、改ざん、漏えいによっても業務に影響が出ることが想定される。

データの消失、改ざん、漏えい、あるいはデータアクセスの一時的なサービス停止によって、生産ラインの停止や生産ノウハウの漏えいなど BC/SQDC を脅かすことにつながるデータを例示する。

- 生産計画
- 生産指示(生産機種・量)
- 生産レシピ
- 生産実績(トレサビデータ)
- 設備状態
- 設備プログラム・パラメタ・図面
- 部材在庫量(現場)
- 部材在庫量(倉庫)

2.6. 想定ゾーン [3.6]

工場システムは業務内容や業務重要度などを考慮し、以下のゾーン[11]を想定する。

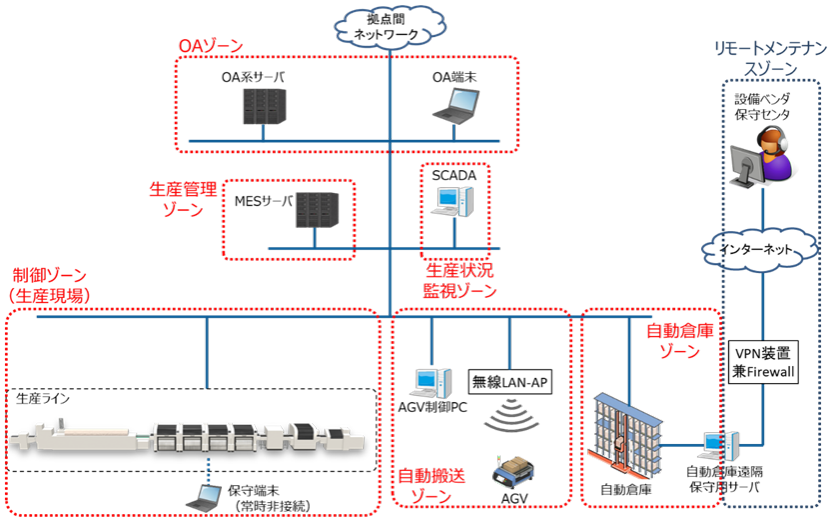


図 2-2 ゾーンの定義例

11 ゾーンとは、共通のセキュリティレベルを持つ領域であると定義する。

以下に各ゾーンの概要、関係する業務の例を示す。

表 2-1 ゾーンの概要

	名称	概要	関連する業務
1	制御ゾーン (生産現場)	製品を生産するための生産ライン。制御装置・機器などで構成されるゾーン	・生産(＋検査) ・生産状況監視(現場) ・部材補充(現場へ) ・メンテナンス
2	自動搬送 ゾーン	部材や完成品の運搬を行う AGV を運用するゾーン	・部材補充(現場へ)
3	自動倉庫 ゾーン	部材を保管しつつ、自動で入出庫する装置を運用するゾーン	・部材補充(現場へ) ・部材補充(倉庫へ)
4	生産管理 ゾーン	生産計画の管理、トレーサビリティデータの管理などを行うサーバ群からなるゾーン	・生産計画設定 ・生産(＋検査) ・生産状況監視(現場) ・生産性分析 ・トレーサビリティ データ参照
5	生産状況 監視ゾーン	生産状況や設備情報の取得・見える化を行う設備からなるゾーン	・生産状況監視(現場) ・生産性分析 ・トレーサビリティ データ参照
6	OA ゾーン	生産に直接関係ない業務を行うゾーン	・生産計画設定 ・部材補充(倉庫へ) ・生産性分析
7	リモート メンテナンス ゾーン	設備ベンダの保守センタが、自動倉庫をリモートで監視するためのゾーン	・リモートメンテナンス

なお、リモートメンテナンスゾーンは、設備ベンダの管理領域であると想定した。

3. セキュリティ対策企画・導入の進め方 [6.1]

本節では、工場システムのセキュリティ対策を企画・導入するステップの概略を示す[12]。

ただし、各ステップにおける表などの記載内容は、全て2章で定義した想定工場に基づき考えられることを例示しているものである。

個社や業界ごとに置かれた環境は異なることから、各ステップにおいて、個社や業界ごとに適した整理や考え方の定義を行うことが必要である。

ステップ 1:情報収集・整理 【3.1】

工場システムのセキュリティを検討する上で、実施する内容を妥当なものとするために必要な情報を収集、整理する。

- ステップ 1-1 セキュリティ対策検討・企画に必要な要件の整理 【3.1.1】
  - (1) 経営目標との関連整理
  - (2) 外部要求事項(社会的セキュリティ要件)の考慮:
  - (3) 内部要件／状況の把握
- ステップ 1-2 業務の整理 【3.1.2】
- ステップ 1-3 業務の重要度の設定 【3.1.3】
- ステップ 1-4 保護対象の整理 【3.1.4】
- ステップ 1-5 保護対象の重要度の設定 【3.1.5】
- ステップ 1-6 ゾーンの整理と、ゾーンと業務、保護対象の結びつけ
- ステップ 1-7 ゾーンと、セキュリティ脅威の影響の整理 【3.1.6】

(参考)経営層による取組の宣言

ステップ1において明らかにした個社の置かれた環境や、業務や保護対象の重要度から、個社において必要となるセキュリティ対策を整理する必要があるが、セキュリティ対策を実現するためには、経営層の強いリーダーシップが必要となることから、必要な体制を構築するとともに、推進するうえで必要な権限を明確にし、関係者に向けてメッセージを発信する。

ステップ 2:セキュリティ対策の立案 【3.2】

ステップ 1 で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。

12 セキュリティ対策は、「事業視点で必要性を明確にし、組織全体で統一的な考え方に基づき計画的に実施すること」が重要である。

3.1. ステップ1：情報収集・整理 [6.1.1]

「情報収集・整理」においては以下の事項を実施する。

3.1.1. ステップ 1-1：セキュリティ対策検討・企画に必要な要件の整理 [2.2]

本節では、セキュリティ対策の検討・企画に必要な要素を示す。

(1) 経営目標とセキュリティ目標の関連整理

自社の工場システムのセキュリティ対策に関わる経営目標（事業伸張、事業継続、等）はどのようになっているか整理する。

表 3-1 セキュリティ対策を検討・企画する際に考慮すべき経営目標事項（想定工場における例）

経営目標	内容	例
事業伸張の視点	フレキシブルな製造ライン構築	AGV 導入
	スマート工場に向けた新たなシステムの構築	自動倉庫の導入
	サプライチェーン下流の取引先・顧客価値向上	製品納入先との連携
事業継続の視点	設備停止による事業上の損失	納期遅延
	安全上の問題の発生	生産設備、自動倉庫、AGVの

(2) 外部要求事項（社会的セキュリティ要件）の洗い出し [2.2.4]

自社の工場システムセキュリティ対策に関わる外部要求事項（セキュリティ法規制・標準規格・ガイドライン準拠、国・自治体からの要求、業界からの要求、市場・顧客からの要求、取引先からの要求、出資者からの要求等）はどのようになっているか整理する。

表 3-2 セキュリティ対策を検討・企画する際に考慮すべき外部要求事項（想定工場における例）

外部要求事項	内容	例
ビジネス上の要求	取引上の要求条件	製品納入先からの要求事項
	国や業界からの経済安全保障にかかわる要請	製品供給の持続・安定化の要求
	他社サービスを利用する要件	自動倉庫保守ベンダからの要件
標準規格対応[13]	業界ガイドライン・国際標準規格	IEC 62443 ほか

(3) 企業内部のセキュリティ要件の洗い出し [2.2.5]

自社の工場セキュリティに関わる内部要求事項（システム面、運用・管理面、維持・改善面、等）や現状がどのようになっているか整理する。

表 3-3 内部要件／状況把握（想定工場における例）

セキュリティ対策	内容	例
方針	全社セキュリティルール	本社セキュリティガイドライン
システム面	ネットワーク、装置・機器の構成	複数の生産ラインを集中管理・自動化、AGV や自動倉庫を導入
	現状のセキュリティ対策	拠点間ファイアウォールのみ
運用・管理面	セキュリティ監視	未実施
	ソフトウェアの更新	情報システム部門管理分のみ実施
維持・改善面	セキュリティ体制整備	未実施
	セキュリティ教育	情報システム(OA ゾーン)に関するセキュリティ教育のみ
	継続的なリスク対応	未実施

[13] 適宜「付録 D 関連／参考資料」を参照のこと。

3.1.2. ステップ 1-2：業務の整理 [2.2]

工場システムが日々の業務でどのように使われているか、その業務の洗い出しを行う。

表 3-4 業務（想定工場における例）

	業務	実施者	業務内容
1	生産計画設定	生産技術・管理部門	・OA 端末から MES サーバに対して、月次・週次・日次の生産計画を入力する
2	生産(＋検査)	工作部門	・MES サーバから生産ラインに対する生産機種・生産量などの指示をトリガとして、現場で段取り替えを実施し、生産ライン上の設備は MES サーバよりレシピを取得し、生産を開始する ・生産設備で生産を実施するとともに、ワークや部材の ID、品質検査情報などのトレーサビリティデータを MES サーバに保管する
3	生産状況監視(現場)	工作部門	・SCADA や現場のアンドンは、MES サーバに上げられた生産状況を取得し画面に表示する
4	部材補充(現場へ)	工作部門	・現場の部品在庫量を収集し、部材切れが近い場合は自動倉庫に保管された部材を AGV で生産現場に輸送する
5	部材購入(倉庫へ)	資材部門	・自動倉庫に保管された部材量を把握し、生産計画と照らし合わせたうえで部材切れが近い場合は、部材の発注を行う
6	生産性分析	生産技術・管理部門	・OA 端末から、MES サーバに保管された過去の生産量・生産不具合などの生産実績情報を取得し、データ分析を実施して要改善箇所を特定する
7	トレーサビリティデータ参照	品質管理部門	・OA 端末から MES サーバに対して、生産 ID に対応する部材情報や品質検査情報を取得する
8	メンテナンス	生産技術・管理部門、設備ベンダ	・生産ラインにて物理的に保守端末を接続し、生産ラインのパラメタ調整、また設備のプログラムバージョンアップやパラメタ設定などを実施する(物理的な部品交換も実施する)
9	リモートメンテナンス	設備ベンダ	・インターネット経由で自動倉庫等に接続し、装置(部品等)の劣化度合いを取得する。必要に応じてパラメタ調整などを実施する

3.1.3. ステップ 1-3：業務の重要度の設定 [2.2]

洗い出した工場システムが使われる業務について、それぞれの業務の重要度を定める。業務の重要度は、セキュリティ対策の重要度／優先度を決定する判断材料となる。

ただし、個社や業界ごとに置かれた環境は異なることから、個社や業界ごとに適した業務の重要度の定義を行うことが必要である。

【参考】業務の重要度（想定工場における例）

表 3-5 業務の重要度（想定工場における例）

業務重要度レベル	内容
大	・ 製品の安定生産に直結する業務で、本業務が実施できなくなると、その日のうちに生産に支障が出る。 ・ 許されない範囲の品質劣化が大規模に生じる。
中	・ 製品の安定生産に間接的に関連する業務で、本業務が実施できなくなると、2～3 日のうちに生産に支障が出る。 ・ 許されない範囲の品質劣化が小規模に生じる。
小	・ 製品の安定生産に関連が薄い業務で、本業務が実施できなくなっても、生産に支障が出るリスクは低い。 ・ 製品としては問題ないレベルの品質劣化が生じる。

また、重要度については、個社・業界の置かれた環境により様々であることから以下の表では重要度レベルについて記載しておらず、個社や業界ごとに適した重要度付けを行うことが重要である。

なお、重要度付けの考え方については、付録 C に記載のとおり国際規格等においても考え方が示されていることから、こうした考え方も参照することが有効である。

表 3-6 業務と重要度(想定工場における例)

	業務	実施者	業務内容	重要度
1	生産計画設定	生産技術・管理部門	・OA 端末から MES サーバに対して、月次・週次・日次の生産計画を入力する	
2	生産(＋検査)	工作部門	・MES サーバから生産ラインに対する生産機種・生産量などの指示をトリガとして、現場で段取り替えを実施し、生産ライン上の設備は MES サーバよりレシピを取得し、生産を開始する ・生産設備で生産を実施するとともに、ワークや部材の ID、品質検査情報などのトレーサビリティデータを MES サーバに保管する	
3	生産状況監視(現場)	工作部門	・SCADA や現場のアンドンは、MES サーバに上げられた生産状況を取得し画面に表示する	
4	部材補充(現場へ)	工作部門	・現場の部品在庫量を収集し、部材切れが近い場合は自動倉庫に保管された部材を AGV で生産現場に輸送する	
5	部材購入(倉庫へ)	資材部門	・自動倉庫に保管された部材量を把握し、生産計画と照らし合わせたうえで部材切れが近い場合は、部材の発注を行う	
6	生産性分析	生産技術・管理部門	・OA 端末から、MES サーバに保管された過去の生産量・生産不具合などの生産実績情報を取得し、データ分析を実施して要改善箇所を特定する	
7	トレーサビリティデータ参照	品質管理部門	・OA 端末から MES サーバに対して、生産 ID に対応する部材情報や品質検査情報を取得する	
8	メンテナンス	生産技術・管理部門、設備ベンダ	・生産ラインにて物理的に保守端末を接続し、生産ラインのパラメタ調整、また設備のプログラムバージョンアップやパラメタ設定などを実施する(物理的な部品交換も実施する)	
9	リモートメンテナンス	設備ベンダ	・インターネット経由で自動倉庫等に接続し、装置(部品等)の劣化度合いを取得する。必要に応じてパラメタ調整などを実施する	

3.1.4. ステップ 1-4:保護対象の整理 [2.2]

セキュリティ対策を強化すべき業務に対して、当該業務を支援／実施する工場システムの構成要素(ネットワーク、装置・機器(機能・プログラム)・データ)を洗い出し、システム構成図の模式図を整理する。

表 3-7 主な構成要素（想定工場における例）

	種類	設備	概要
1	ネットワーク機器、及びネットワーク	VPN 機器	設備ベンダがリモートでアクセスする際に利用する、セキュアな通信を実現するための機器。設備ベンダの保守センタ以外からのアクセスは許可しないようにファイアウォール(アクセス制御)機能を内蔵
2		無線 LAN-AP (アクセスポイント)	AGV（無人搬送車）との通信を行うためのネットワーク機器
3		設備系ネットワーク	生産設備が接続されるネットワーク
4		生産管理系ネットワーク	生産管理を行うサーバなどが接続されるネットワーク
5		情報系ネットワーク	OA 業務、製品設計用の端末が接続されるネットワーク
6	装置・機器	MES サーバ	生産計画、生産実績のデータ管理、及び生産ラインに対しての生産指示を行うサーバ
7		生産ライン	製品の生産を行うために用いる設備
8		保守端末	生産設備のメンテナンスに用いる PC
9		SCADA	生産ラインの生産状況の監視を行う PC
10		AGV（無人搬送車）制御 PC	AGV（無人搬送車）の運転計画を立案し、AGV を制御する PC
11		AGV（無人搬送車）	部材を運ぶ装置
12		自動倉庫	部材の保管と入出庫を行う装置
13		自動倉庫遠隔保守用サーバ	設備ベンダ保守センターが自動倉庫をリモートから保守する際に利用するサーバ
14		OA 系サーバ	事務用途で利用するサーバ。営業管理ツール、社内ワークフローシステム、ファイルサーバなどを想定
15		OA 端末	事務用途で利用する PC
16	データ	生産計画	月次・週次・日次の生産計画
17		生産指示 (生産機種・量)	生産ラインで何を生産するかの指示。生産機種、生産量、対応するレシピなどの情報
18		生産レシピ	生産機種ごとの詳細情報(パラメタ等)
19		生産実績 (トレサビデータ)	過去の生産実績。生産計画に対する現在の生産台数などの生産状況、ワークや部材の ID、品質検査情報などのトレサビデータ等を含む
20		設備状態	生産設備(装置)の状態情報。治具の累積使用時間、最終メンテナンス日時、等を含む
21		設備プログラム・パラメタ・図面	生産設備(装置)に設定されたプログラム、及び動作をカスタマイズするパラメタなど
22		部材在庫量(現場)	生産現場及び装置に補充されている部品の型番と残量など
23		部材在庫量(倉庫)	自動倉庫内に保管されている部品の残量、型番、棚情報など

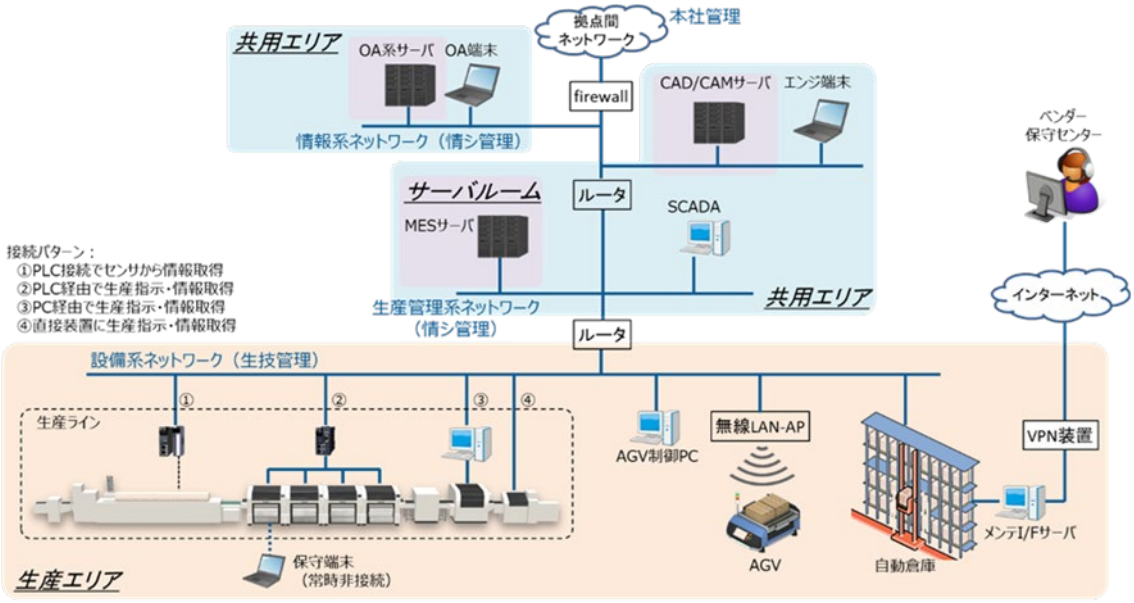


図 3-1 3 章の工場システム構成例(再掲)

3.1.5. ステップ 1-5：保護対象の重要度の整理 [2.2]

製造業／工場が重視する価値軸である事業伸張・継続(BC)の視点、安全確保(S)、品質確保(Q)、納期遵守・遅延防止(D)、コスト低減(C)の視点、それによる業務の重要性の視点から、洗い出した保護対象それぞれの重要度を明確にする。保護対象の重要度は、セキュリティ対策の優先度を決定する判断材料となる。

重要度については、個社・業界の置かれた環境により様々であることから以下の表では重要度レベルについて記載しておらず、個社や業界ごとに適した重要度付けを行うことが重要である。

なお、重要度付けの考え方については、付録 C に記載のとおり国際規格等においても考え方が示されていることから、こうした考え方も参照することが有効である。

表 3-8 保護すべき対象と重要度（想定工場における例）

	種類	保護対象	用途	重要度
1	ネットワーク	設備系 ネットワーク	生産設備や各種サーバ間の データ交換	
2		生産管理系 ネットワーク	生産設備や各種サーバ間の データ交換	
3	装置・機器 （機能・プログラム）	MES サーバ	生産計画、生産実績のデータ管理、及び生産ラインに対する生産指示	
4		ルータ (設備系−生産管理系)	設備系ネットワークと生産管理系 ネットワーク間のデータ交換	
5		生産ライン	製品の生産	
6		SCADA	生産ラインの生産状況の監視	
7		保守用 PC	生産設備のメンテナンス	
8		AGV 制御 PC	AGV の運転計画立案と、AGV 制御	
9		無線 LAN アクセスポイント	AGV と通信を行うための ネットワーク機器	
10		AGV	部材を運ぶ装置	
11		自動倉庫	部材の保管と入出庫を行う装置	
12		自動倉庫 遠隔保守用サーバ	設備のリモートメンテナンス用のリモートアクセス・管理サーバ	
13		VPN 機器	設備のリモートメンテナンスを 行うためのネットワーク機器	
14	データ	生産計画	月次・週次・日次の生産計画	
15		生産指示 (生産機種・量)	生産ラインで何を生産するかの 指示。生産機種、生産量、対応するレシピなどの情報	
16		生産レシピ	生産機種ごとの詳細情報 (パラメタ等)	
17		生産実績 (トレサビデータ)	過去の生産実績。生産計画に対する現在の生産台数などの生産状況、ワーク	

	種類	保護対象	用途	重要度
			や部材の ID、品質検査情報などのトレサビデータ等を含む	
18		設備状態	生産設備(装置)の状態情報。 治具の累積使用時間、最終メンテナンス日時、等を含む	
19		設備プログラム・ パラメタ・図面	生産設備(装置)に設定されたプログラム、及び動作をカスタマイズするパラメタなど	
20		部材在庫量(現場)	生産現場及び装置に補充されている部品の型番と残量など	
21		部材在庫量(倉庫)	自動倉庫内に保管されている部品の残量、型番、棚情報など	

3.1.6. ステップ 1-6：ゾーンの整理と、ゾーンと業務、保護対象の結びつけ

工場システムは業務内容や業務重要度などを考慮しつつ、共通のセキュリティレベルを持つ領域として、ゾーンを設定する。また、ゾーンごとに、これまでに整理した業務、保護対象を結びつける。

ただし、個社・業界の置かれた環境によっては、保護対象や業務を厳密に定義しようとすれば膨大な量になることも考えられる。これは、かえって整理のための業務量が膨大になることや、ミスが生じ得ること、時間がかかりすぎること、といったデメリットが考えられることから、個社・業界の置かれた環境に応じ、整理するゾーンと保護対象、業務の粒度や整理方法については柔軟な対応を行っていただきたい。

以降のステップにおいても、必要に応じ、同様の対応を行っていただきたい。

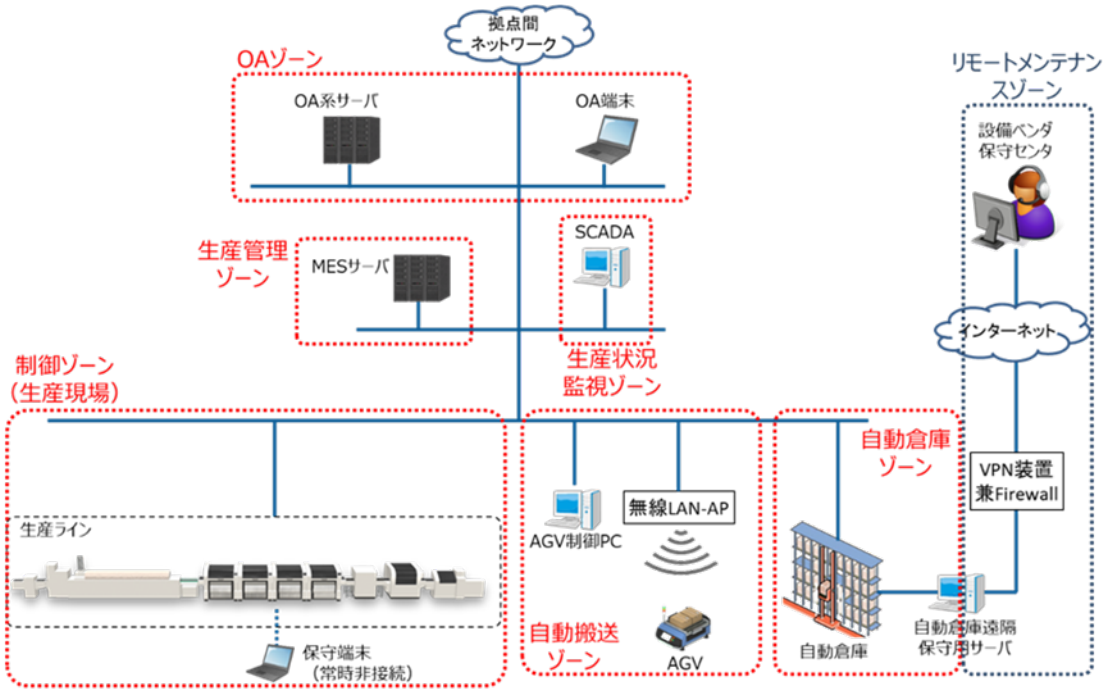


図 3-2 ゾーンの定義例（再掲）

表 3-9 ゾーンの概要と重要度（想定工場における例）

	関連する保護対象	関連する業務	名称	概要
1	・生産ライン ・保守端末 ・ルータ	・生産(＋検査) ・生産状況監視(現場) ・部材補充(現場へ) ・メンテナンス	制御ゾーン ・(生産現場)	・製品を生産するための生産ライン。制御装置・機器などで構成されるゾーン
2	・AGV 制御 PC ・無線 LAN-AP ・AGV	・部材補充(現場へ)	自動搬送 ・ゾーン	・部材や完成品の運搬を行う AGV を運用するゾーン
3	・自動倉庫遠隔保守用サーバ ・自動倉庫	・部材補充(現場へ) ・部材補充(倉庫へ)	自動倉庫 ・ゾーン	・部材を保管しつつ、自動で入出庫する装置を運用するゾーン
4	・MES サーバ	・生産計画設定 ・生産(＋検査) ・生産状況監視(現場) ・生産性分析 ・トレーサビリティデータ参照	生産管理 ・ゾーン	・生産計画の管理、トレーサビリティデータの管理などを行うサーバ群からなるゾーン
5	・SCADA	・生産状況監視(現場) ・生産性分析 ・トレーサビリティデータ参照	・生産状況監視ゾーン	・生産状況や設備情報の取得・見える化を行う設備からなるゾーン
6	・OA 系サーバ ・OA 端末	・生産計画設定 ・部材補充(倉庫へ) ・生産性分析	・OA ゾーン	・生産に直接関係ない業務を行うゾーン
7	・保守センタ ・VPN 装置兼 Firewall	・リモートメンテナンス	・リモートメンテナンスゾーン	・設備ベンダの保守センタが、自動倉庫をリモートで監視するためのゾーン

※リモートメンテナンスゾーンは、設備ベンダの管理領域であると想定。

3.1.7. ステップ 1-7:ゾーンと、セキュリティ脅威による影響の整理 [2.2.2]

脅威の種別の例としては、以下が挙げられる。

- 不正な物理的侵入、物理的窃盗、
- 不正アクセス、不正デバイス接続、
- マルウェア感染、不正プログラム実行、
- 不正なデータ送信、不正な指示／命令送信、過失送信、
- 情報窃取・漏えい、情報改ざん／破壊、不正な設定変更、過失設定、
- 不正な操作・制御、過失操作、機器停止、機器破壊、
- 高負荷攻撃、通信妨害、など

また、脅威と生産・事業への影響は以下のような関係があると考えられる。

表 3-10 一般的な脅威と生産への影響(例)

	脅威種別	脅威内容	生産・事業への影響
1	不正侵入	ゾーン外からの物理的侵入	・機器の盗難 ・システム、機材に対する破壊行為(による生産停止等)
2		ゾーン内での機器に対する直接的な不正接続／アクセス	
3		ゾーン外からのネットワークを介した不正アクセス	
4	設備の異常な制御や破壊	設備の不正な制御や停止	・品質不良や、それに伴うブランド毀損 ・生産性低下による納期遅れや原価上昇 ・設備の誤動作による人身事故や災害の発生 ・設備故障による損害
5		設備へ異常負荷をかけての破壊	
6		設備の安全制御の機能停止	
7	データ盗難・漏えい	USB などへの不正コピー	・生産情報や品質保証ノウハウの流出 ・顧客情報の流出と、それに伴うブランド毀損
8		不正なサーバへのアップロード	
9		パケットの盗聴	
10	データ改ざん・破壊	データやプログラムの改ざん・消去	・品質不良や、 それに伴うブランド毀損 ・生産性低下による 納期遅れや原価上昇 ・設備の誤動作による 人身事故や災害の発生 ・設備故障による損害
11		設備設定値の悪意ある変更	
12		パケットの改ざん	
13	可用性低下	ネットワーク停止	・生産性低下による納期遅れや原価上昇 ・設備制御不能による人身事故や災害の発生 ・品質不良や、それに伴うブランド毀損
14		設備・サーバ・PC の停止	
15		リソースの不足	
16		ネットワーク停止・容量オーバ	

	脅威種別	脅威内容	生産・事業への影響
17	外部への攻撃の踏み台として利用	外部のサーバ／ネットワークへの攻撃	・ブランド毀損 ・捜査中のライン停止に伴う納期遅れの発生
18	自然環境の脅威	大雨、洪水などによる漏水	・事業／生産停止による損害 ・生産性低下による納期遅れや原価上昇 ・設備制御不能による人身事故や災害の発生 ・設備故障による損害 ・品質不良や、それに伴うブランド毀損
19		有害生物の侵入	
20		地震などによる機器の転倒・落下	
21		落雷、洪水、地震などによる停電・瞬断・電圧変動	
22	システム／機器の障害・故障	電源の停電・瞬断・電圧変動、電源設備・機器の障害・故障	・生産性低下による納期遅れや原価上昇 ・設備制御不能による人身事故や災害の発生 ・設備故障による損害 ・品質不良や、それに伴うブランド毀損
23		空調の障害・故障による温度、湿度、静電気、空気清浄度などの異常	
24		通信機器の障害・故障	
25		設備・サーバ・PC の障害・故障	
26	従業員の過失	異常な(マルウェアに感染した)機器の接続	・生産情報や品質保証ノウハウの流出 ・顧客情報の流出と、それに伴うブランド毀損 ・システム、機材に対する破壊行為(による生産停止等)
27	従業員の過失	設定／操作ミス	・品質不良や、それに伴うブランド毀損 ・設備の誤動作による人身事故や災害の発生 ・設備故障による損害

こうした脅威と生産・事業への影響を勘案し、それぞれのゾーンに対して、どのようなセキュリティ脅威が想定されるのか、それによりどのような影響があるかを整理する。

表 3-11 保護対象と関連する業務、脅威、影響の関係（例）

	関連する保護対象	関連する業務	脅威	影響	名称
1	□生産ライン	・□生産(＋検査) ・□生産状況監視(現場) ・□部材補充(現場へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産(＋検査) 不可 ・□生産状況監視(現場) 不可 ・□部材補充(現場へ) 不可	制御ゾーン (生産現場)
	□保守端末	・□メンテナンス	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□メンテナンス不可	
	□ロータ	・□生産(＋検査) ・□生産状況監視(現場) ・□部材補充(現場へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産(＋検査) 不可 ・□生産状況監視(現場) 不可 ・□部材補充(現場へ) 不可	
2	□AGV制御PC	・□部材補充(現場へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□部材補充(現場へ)不可	自動搬送 ゾーン
	□無線LAN-AP	・□部材補充(現場へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□部材補充(現場へ)不可	
	□AGV	・□部材補充(現場へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□部材補充(現場へ)不可	
3	□自動倉庫遠隔保守用サーバ	・□部材補充(現場へ) ・□部材補充(倉庫へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障	・□部材補充(現場へ)不可 ・□部材補充(倉庫へ)不可	自動倉庫 ゾーン
	□自動倉庫	・□部材補充(現場へ) ・□部材補充(倉庫へ)	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障	・□部材補充(現場へ)不可 ・□部材補充(倉庫へ)不可	

	関連する保護対象	関連する業務	脅威	影響	名称
4	□MESサーバ	□生産計画設定 □生産(＋検査) □生産状況監視(現場) □生産性分析 □トレーサビリティデータ参照	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 □従業員の過失	・□生産計画設定不可 ・□生産(＋検査) 不可 ・□生産状況監視(現場) 不可 ・□生産性分析トレーサビリティデータ参照不可	生産管理ゾーン
5	□SCADA	・□生産状況監視(現場) ・□生産性分析 ・□トレーサビリティデータ参照	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産状況監視(現場) 不可 ・□生産性分析トレーサビリティデータ参照不可	生産状況監視ゾーン
6	□OA系サーバ	・□生産計画設定 ・□部材補充(倉庫へ) ・□生産性分析	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産計画設定 ・□部材補充(倉庫へ)不可 ・□生産性分析不可	OAゾーン
	□OA端末	・□生産計画設定 ・□部材補充(倉庫へ) ・□生産性分析	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産計画設定 ・□部材補充(倉庫へ)不可 ・□生産性分析不可	
7	□保守センタ	・□リモートメンテナンス	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□リモートメンテナンス不可	リモートメンテナンスゾーン
	□VPN装置兼Firewall	・□リモートメンテナンス	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□リモートメンテナンス不可	

【参考】攻撃者の動機

最近のサイバー攻撃は、攻撃の目的が明確で、かつ、目的達成まで執拗に攻撃が繰り返される傾向が認められる。また、攻撃者の種別も、情報収集や破壊工作を目的とした軍隊や諜報機関といった国家レベルの組織、身代金目的の犯罪集団、内部不正を犯す関係者など、多様になっている。

そのため、事前に攻撃者の動機を想定し、万一サイバー攻撃を受けたときに、生産にどのような影響が起こりうるかを想定しておくことが重要である。

工場における脅威を想定する場合、攻撃者が動機を持ち、工場システムへサイバー攻撃を行った場合、生産現場で何らかの異常事象や影響が発生すると予想される。

一方、工場においては、犯罪組織によるランサムウェアなど金銭を目的とした攻撃もあるが、目的が不明瞭な場合もある。攻撃者は意図的に工場を狙ったわけではなく、たまたま攻撃した先が工場という場合もある。自社は犯罪組織等に狙われることはないと考えるのではなく、流れ弾に当たるということも想定しておくべきである。

また、サイバー攻撃以外にも、自然環境の脅威、システム／機器の障害・故障、従業員の過失、管理不備などの想定も併せて必要である。

以下に、攻撃者の動機として考えられる例を整理する。

表 3-12 攻撃者の動機(例)

	目的	説明	想定される攻撃者
1	社会混乱	当該工場の生産物が重要品であり、供給不足や品質不安を引き起こすことで社会混乱を誘発	・国家的組織(軍隊、諜報機関等) ・犯罪組織、テロ組織
2	情報窃取	当該工場の高付加価値生産物や高度な生産プロセスに関する、企業機密を盗む	・ライバル企業 ・犯罪組織(金銭目当て)
3	企業価値棄損	当該工場の生産物に不正な機能を仕込み、当該製品の品質低下を招き、企業価値を棄損する	・ライバル企業 ・犯罪組織
4	二次被害	生産ラインの事故を誘発させ、人的・物的被害を発生させる、薬品等の漏出を引き起こさせ環境汚染を誘発させる、製品に細工を行い利用者からの情報窃取等、二次被害を狙う	・国家的組織(軍隊、諜報機関等) ・犯罪組織、テロ組織 ・ライバル企業
5	踏み台	生産ラインを踏み台として、当該企業の IT システムへ侵入したり、サービスを妨害したりする(情報窃取や営業妨害などにつながる)	・国家的組織(軍隊、諜報機関等) ・犯罪組織、テロ組織 ・ライバル企業
6	金銭	ランサムウェア等に感染させ、金銭を要求	・犯罪組織、テロ組織
7	嫌がらせ	怨恨等による嫌がらせ(内部不正)	・現在／以前の従業員、取引先等
8	営業妨害	営業妨害(風評被害狙いや、ライバル企業の株価つり上げなど)	・ライバル企業 ・犯罪組織

【参考】経営層による取組みの宣言 [6.1.2]

セキュリティ対策を実施・推進するためには、経営層のリーダーシップが重要となる。このため、経営層がセキュリティ対策推進の意志が明らかでない場合には、組織として明文化し宣言することが重要である[14]。

例えば、推進組織の設置、権限の付与、目的、方針などを明らかにし、組織内に宣言を表明することが必要である。

経営層によるセキュリティ取り組み宣言の例:

X 社は、電子機器メーカとして安定した製品供給が重要である。このため、生産ライン及び製品に対するセキュリティ確保が重要であり、組織的な対策推進を実施する。

- 目的:セキュリティ視点でのリスク評価に基づき実施目標を設定し、確実な実施と継続的な改善を図ることを目的とする。
- 方針:目的を実現するため、推進体制を整備するとともに必要な権限を委譲する。
- 体制:CEO 直下に推進組織を設置し、戦略的かつ全社統一的な視点で推進する。
- リスク評価:セキュリティ、業務継続、リスク対応の視点から総合的に実施する。
- 周知と教育・訓練:サプライチェーンの関係者に周知し順守を徹底する。

[14] 経営層に向けては、経済産業省より「サイバーセキュリティ経営ガイドライン」が発行されており、経営層が認識すべき 3 原則及び CISO 等に対して指示すべき 10 項目が記されている。「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティリスクの管理体制構築、サイバーセキュリティリスクの特定と対策の実装、インシデント発生に備えて体制構築について、経営者がリーダーシップをとったセキュリティ対策の推進を求めている。

3.2. ステップ 2：セキュリティ対策の立案 [6.1.3]

ステップ1で収集・整理した情報に基づき、工場システムのセキュリティ対策方針を策定する。

ステップ 2-1 全体方針の策定【3.2.1】

ステップ1で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。

ステップ 2-2 想定脅威に対するセキュリティ対策の対応づけ【3.2.2】

どのようなセキュリティ対策が対応付けられるのか整理する。脅威に対応するためには物理面、システム構成面どちらか一方でなく双方の対策が重要となるため、参照されたい。

(1)システム構成面での対策
①ネットワークにおけるセキュリティ対策
②機器におけるセキュリティ対策
③業務プログラム・利用サービスにおけるセキュリティ対策

(2)物理面での対策
①建屋にかかわる対策
②電源／電気設備にかかわる対策
③環境(空調など)にかかわる対策
④水道設備にかかわる対策
⑤機器にかかわる対策
⑥物理アクセス制御にかかわる対策

3.2.1. ステップ 2-1：全体方針の策定

工場システムのセキュリティ対策を実施する上での全体方針を策定する。ステップ1で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。

重要度については、個社・業界の置かれた環境により様々であることから以下の表では重要度レベルについて記載しておらず、個社や業界ごとに適した重要度付けを行うことが重要である。

なお、重要度付けの考え方については、付録 C に記載のとおり国際規格等においても考え方が示されていることから、こうした考え方も参照することが有効である。

表 3-13 保護対象、関連する業務、脅威、影響、ゾーン、重要度／優先度の関係（例）

	関連する保護対象	関連する業務	脅威	影響	名称	重要度／優先度
4	□MES サーバ	□生産計画設定 □生産（＋検査） □生産状況監視（現場） □生産性分析 □トレーサビリティデータ参照	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 □従業員の過失	・□生産計画設定不可 ・□生産（＋検査）不可 ・□生産状況監視（現場）不可 ・□生産性分析トレーサビリティデータ参照不可	生産管理ゾーン	
5	□SCADA	・□生産状況監視（現場） ・□生産性分析 ・□トレーサビリティデータ参照	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産状況監視（現場）不可 ・□生産性分析トレーサビリティデータ参照不可	生産状況監視ゾーン	
6	□OA 系サーバ	・□生産計画設定 ・□部材補充（倉庫へ） ・□生産性分析	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産計画設定 ・□部材補充（倉庫へ）不可 ・□生産性分析不可	OAゾーン	
	□OA 端末	・□生産計画設定 ・□部材補充（倉庫へ） ・□生産性分析	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□生産計画設定 ・□部材補充（倉庫へ）不可 ・□生産性分析不可		
7	□保守センタ	・□リモートメンテナンス	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□リモートメンテナンス不可	リモートメンテナンスゾーン	
	□VPN 装置兼 Firewall	・□リモートメンテナンス	・□自然環境の脅威 ・□不正侵入 ・□データ盗難・漏えい ・□データ改ざん・破壊 ・□設備の異常な制御や破壊 ・□可用性低下 ・□システム／機器の障害・故障 ・□従業員の過失	・□リモートメンテナンス不可		

【参考】セキュリティ要求レベルの考え方の例

工場システムのセキュリティ対策は、投資コストや運用コストの視点から現実的である必要がある。このため、保護対象システムが担う役割の重要度に応じた、セキュリティ対策の重要度(優先度)を定める必要がある。

この重要度を「セキュリティ要求レベル」とすると、要求レベルが高いほど、強度の高いセキュリティ対策が必要となる。セキュリティ要求レベルとして、以下を例示するが、レベル設定の方法は、各社で最適なものを設定することが望ましい。

「業務の重要度」×「現状の脅威レベル」＝「セキュリティ要求レベル」

＜例＞2 章の工場システムでの例

表 3-14 業務の重要度(例)

業務重要度	定義
大	システムが誤動作や停止すると、製品供給に支障、 システムの暴走・爆発、休業労災
中	システムが誤動作や停止すると、業務停止(供給支障なし)、 不休労災、不適切な排水による環境汚染
小	システムが誤動作や停止すると、業務混乱(供給支障なし)

表 3-15 脅威レベル[＝脅威を受ける可能性(高低)]

脅威レベル	定義
3	脅威を受ける可能性が高い • 高い攻撃スキルや知識を保有していない者でも、攻撃や不正を実施可能 • 物理的／論理的アクセスが容易 • 極めて短時間で攻撃や不正を実施可能
2	脅威を受ける可能性が中程度はある • 一定レベルの攻撃スキルや知識を保有している者であれば、攻撃や不正を実施可能 • 物理的／論理的アクセスに一般的な制限を掛けている • 攻撃や不正の実施にはそれなりの時間を要する
1	脅威を受ける可能性が低い • 極めて高い攻撃スキルや高度な知識を保有していなければ、攻撃や不正の実施は不可能 • 物理的／論理的アクセスに強い制限が掛かっている • 攻撃や不正の実施には長い時間を要する

表 3-16 セキュリティ要求レベル(例)

		脅威レベル		
		1	2	3
業務重要度	大	高	高	高
	中	中	中	高
	小	低	低	低

「セキュリティ要求レベル」(=「業務の重要度」×「現状の脅威レベル」)は、業務にかかわる保護対象(システム及びその構成要素)それぞれにおいて、想定されるセキュリティ脅威を受けた場合に、保護対象の重要度/優先度の視点から、

- どのような影響(及び影響度の大小)を被る可能性があるのか、及び
- その影響が発生する可能性の大小

を表すものになる。これはすなわち、保護対象それぞれの「セキュリティリスク」を表していることになる。

表 3-17 業務重要度、脅威レベル、セキュリティ要求レベル(例)

ゾーン	関係する業務	業務重要度	脅威レベル	セキュリティ要求レベル
制御/生産ライン	生産、検査	大	2	高
制御/保守端末	生産プログラム作成	大	1	高
自動搬送	部品・部材補充	大	2	高
自動倉庫	部品・部材補充	大	2	高
生産管理	生産計画設定、生産指示	大	2	高
生産状況監視	生産状況監視	大	1	高
リモートメンテ	リモートメンテナンス	大	1	高
OA	生産性分析	中	2	中

各ゾーンにある保護対象(ネットワークや装置・機器など)に対して、セキュリティ要求レベルに応じた強度のセキュリティ対策(6.2 節を参照)を実施する必要がある。

【参考】対策の深さ

ゾーンごとに対策を行うに当たり、どこまでの対策を行うかといった対応の深さはそれぞれであることから、この深さの考え方と対策内容の一例を示す。

表 3-18 各ゾーンのレベルに応じたセキュリティ対策例（主要対策のみを抜粋）

	区分	要件	低	中	高
1	侵入防止	外部ネットワークからの侵入防止	・他のゾーンからの通信、及び他のゾーンへの通信に対して、予め許される通信のみを通過させる(IP アドレス、アクセスポートなどで制御)	・他のゾーンからの通信、及び他のゾーンへの通信に対して、予め許される通信のみを通過させる(IP アドレス、アクセスポートなどで制御) ・当該ゾーン利用者の認証を行う	・他のゾーンからの通信、及び他のゾーンへの通信に対して、予め許される通信のみを通過させる(IP アドレス、アクセスポートなどで制御) ・当該ゾーン利用者の認証は多要素認証を導入し、厳格に行う
2		ソーン内部への直接侵入防止	・ゾーン内への入室者を制限する ・ゾーン内 LAN へ接続する機器を管理する	・入退管理が行われた区画に設備を設置 ・ゾーン内への入室者を制限する ・ゾーン内 LAN へ接続する機器を管理する	・入退管理が行われた区画に設備を設置 ・ゾーン内への入室者を厳しく制限する ・ゾーン内 LAN へ接続する機器は機器認証で制限する
3	活動抑止	許可通信のみの通過	・他のゾーンからの通信、及び他のゾーンへの通信に対して、予め許される通信のみを通過させる(IP アドレス、アクセスポートなどで制御)	・他のゾーンからの通信、及び他のゾーンへの通信に対して、予め許される通信のみを通過させる(IP アドレス、アクセスポートなどで制御) ・当該ゾーン利用者の認証を行う	・他のゾーンからの通信、及び他のゾーンへの通信に対して、予め許される通信のみを通過させる(IP アドレス、アクセスポートなどで制御) ・当該ゾーン利用者の認証は多要素認証を導入し、厳格に行う

4		不正行為の抑止	・操作ユーザのログオンを認証し、アクセス制御により操作を限定 ・業務に従事する者に対し、操作を監視することを周知し、不正行為の抑止を図る ・不要ポートに端子キャップを付ける	低レベルの対策に加えて ・サーバコンソールへのログオンは、管理者に限定する ・当該ゾーン利用者の認証は多要素認証を導入し、厳格に行う ・重要操作は管理者一人では実施させず、ワークフローにより承認、もしくは権限分離を実施 ・IDS による不正な通信パケットの監視を実施 ・不要ポートをソフト閉塞する	中レベルの対策に加えて ・ネットワークを流れるパケットに対して、許可リスト型監視により、定常でないパケットの出現を監視 ・実行制御ツールにより、事前に許可したプログラム以外の起動を防止 ・不要ポートをハード閉塞する
5	運用支援	ログ管理	・監視端末のログを収集・管理	低レベルの対策に加えて ・設備のアラートやファイアウォールなどの多種にわたるログを収集・管理	中レベルの対策に加えて ・収集したログの定期的な分析を実施
6		アラート監視	・監視端末のログを SOC にて集中監視し異常を検出	低レベルの対策に加えて ・各種サーバやセキュリティ機器(ファイアウォールや IDS などを指す)のログを SOC にて集中監視し異常を検出	中レベルの対策に加えて ・設備のアラートを SOC にて集中監視し異常を検出

以下に、2 章に示した工場システムの例に対し、対策を行った状態を図示する。

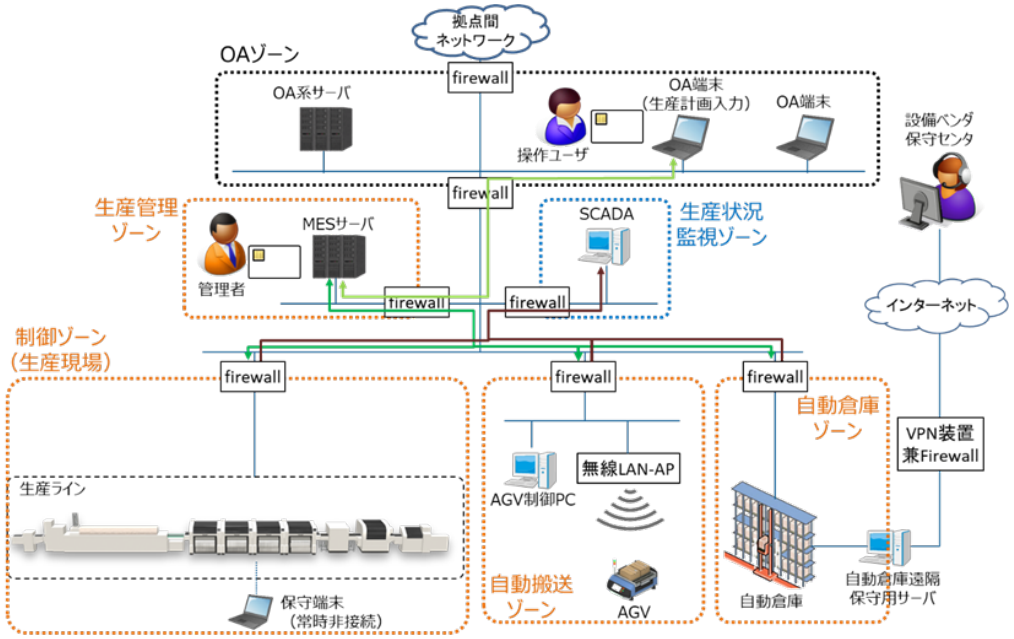


図 3-3 要件に対する各ゾーンでの対策(例)

3.2.2. ステップ 2-2：想定脅威に対するセキュリティ対策の対応づけ

表 3-16 に示した脅威と対策の全体像も参考にし、これまでに整理した、ゾーン、保護対象、業務、脅威、影響と対策を結びつける。

表 3-19 保護対象、関連する業務、脅威、影響、ゾーン、重要度／優先度、対策（生産ラインのみを抜粋）

	関連する保護対象	関連する業務	脅威	影響	名称	重要度／優先度	対策	
1	□生産ライン	□生産(＋検査) □生産状況監視(現場) □部材補充(現場へ)	□自然環境の脅威	□生産(＋検査) 不可 □生産状況監視(現場) 不可 □部材補充(現場へ) 不可	制御ゾーン(生産現場)		① 物理面での対策	① A) 建屋にかかわる対策 ① B) 電源／電気設備にかかわる対策 ① E) 機器にかかわる対策
							② システム構成面での対策	② B) 機器における対策
			□不正侵入				① 物理面での対策	① E) 機器にかかわる対策 ① F) 物理アクセス制御にかかわる対策
							② システム構成面での対策	② A) ネットワークにおける対策 ② B) 機器における対策
			・□データ盗難・漏えい				① 物理面での対策	① ⑤ 機器にかかわる対策
							② システム構成面での対策	② A) ネットワークにおける対策 ② B) 機器における対策
			・□データ改ざん・破壊				② システム構成面での対策	② A) ネットワークにおける対策 ② B) 機器における対策
			・□設備の異常な制御や破壊				② システム構成面での対策	② A) ネットワークにおける対策 ② B) 機器における対策
			・□可用性低下				② システム構成面での対策	② A) ネットワークにおける対策 ② B) 機器における対策
			・□システム／機器の障害・故障				① 物理面での対策	① B) 電源／電気設備にかかわる対策 ① E) 機器にかかわる対策
							② システム構成面での対策	② A) ネットワークにおける対策 ② B) 機器における対策
			・□従業員の過失				① 物理面での対策	① E) 機器にかかわる対策
							② システム構成面での対策	② B) 機器における対策

個別の対策については、以降の記載を参照の上、それぞれの環境等に応じて検討することが望ましい。

表 3-20 想定脅威に対応するセキュリティ対策(例)の全体像

No.	脅威種別	脅威内容	対策種別	対策内容
1	自然環境の脅威	大雨、洪水などによる漏水	(2) 物理面での対策	(2)① 建屋にかかわる対策
2		有害生物の侵入		
3		地震などによる機器の転倒・落下		(2)⑤ 機器にかかわる対策
4		落雷、洪水、地震などによる停電・瞬断・電圧変動	(2) 物理面での対策	(1)② 電源／電気設備にかかわる対策
			(1) システム構成面での対策	(1)② 機器における対策
5	不正侵入	ゾーン外からの物理的侵入	(2) 物理面での対策	(2)⑥ 物理アクセス制御にかかわる対策
6		ゾーン内での機器に対する直接的な不正接続／アクセス	(2) 物理面での対策	(2)⑤ 機器にかかわる対策
			(1) システム構成面での対策	(1)② 機器における対策
7		ゾーン外からのネットワークを介した不正アクセス	(1) システム構成面での対策	(1)① ネットワークにおける対策
8	データ盗難・漏えい	USB などへの不正コピー	(2) 物理面での対策	(2)⑤ 機器にかかわる対策
			(1) システム構成面での対策	(1)② 機器における対策
9		不正なサーバへのアップロード	(1) システム構成面での対策	(1)① ネットワークにおける対策
				(1)② 機器における対策
10		パケットの盗聴	(1) システム構成面での対策	(1)① ネットワークにおける対策
				(1)② 機器における対策
11	データ改ざん・破壊	データやプログラムの改ざん・消去	(1) システム構成面での対策	(1)② 機器における対策
12		設備設定値の悪意ある変更		
13		パケットの改ざん	(1) システム構成面での対策	(1)① ネットワークにおける対策
				(1)② 機器における対策

No.	脅威種別	脅威内容	対策種別	対策内容
14	設備の異常な制御や破壊	設備の不正な制御や停止	(1) システム構成面での対策	(1)① ネットワークにおける対策
15		設備へ異常負荷をかけての破壊		(1)② 機器における対策
16		設備の安全制御の機能停止		
17	可用性低下	ネットワーク停止	(1) システム構成面での対策	(1)① ネットワークにおける対策
18		ネットワーク容量オーバ		
19		設備・サーバ・PC の停止		(1)② 機器における対策
20		リソースの不足		
21	外部への攻撃の踏み台として利用	外部のサーバ／ネットワークへの攻撃	(1) システム構成面での対策	(1)① ネットワークにおける対策
				(1)② 機器における対策
22	システム／機器の障害・故障	電源の停電・瞬断・電圧変動、電源設備・機器の障害・故障	(2) 物理面での対策	(2)② 電源／電気設備にかかわる対策
			(1) システム構成面での対策	(1)② 機器における対策
23		空調の障害・故障による温度、湿度、静電気、空気清浄度などの異常	(1) システム構成面での対策	(1)② 機器における対策
24		通信機器の障害・故障		
25		設備・サーバ・PC の障害・故障		
26	従業員の過失	異常な(マルウェアに感染した)機器の接続	(2) 物理面での対策	(2)⑤ 機器にかかわる対策
			(1) システム構成面での対策	(1)② 機器における対策
27		設定／操作ミス	(1) システム構成面での対策	(1)② 機器における対策

以下に、想定される具体的なセキュリティ対策について示す。脅威に対応するためには物理面、システム構成面どちらか一方でなく双方の対策が重要となるため、参照されたい。

なお、中小企業においては、情報系の領域と工場系の領域の切り分けがなされていない場合もあることから、そうした固有の状況に応じ、適宜中小企業向けのセキュリティ情報[15]も参照しつつ、固有の状況に応じた対策を行っていただきたい。

(1) システム構成面での対策
- ① ネットワークにおけるセキュリティ対策
- ② 機器におけるセキュリティ対策
- ③ 業務プログラム・利用サービスにおけるセキュリティ対策

(2) 物理面での対策
- ① 建屋にかかわる対策
- ② 電源／電気設備にかかわる対策
- ③ 環境(空調など)にかかわる対策
- ④ 水道設備にかかわる対策
- ⑤ 機器に関わる物理的対策
- ⑥ 物理アクセス制御にかかわる対策

15 例えば、情報処理推進機構(IPA)は、「中小企業の情報セキュリティ対策ガイドライン」を公開している。また、経済産業省及び情報処理推進機構(IPA)は、地域の業界団体(商工会議所など)や企業等と連携し、登録された民間事業者による「サイバーセキュリティお助け隊サービス」を実施している。

(1) システム構成面での対策 [6.2.3]

ネットワークを介した不正侵入やデータ漏えいなどの脅威に対しては、主にシステム構成面でのネットワークにおける対策が必要となる。また、機器上での不正接続／アクセス、データ改ざん、機器の異常な設定／制御などの脅威に対しては、主にシステム面での機器における対策が必要となる。

システム面のセキュリティ対策は、次の 3 つの観点を考慮する。

- **侵入防止:**
  工場システムへの不正侵入の防止
- **構成分割:**
  侵入を防ぎきれず侵入された場合であっても、攻撃活動を抑止
- **運用支援:**
  工場システムへの侵入や攻撃などの活動を早期に検知・対処するための運用を支援

表 3-21 システム構成面のセキュリティ対策の目的概要

	目的		概要
1	侵入防止	ネットワークへの侵入防止	外部ネットワークからの侵入、内部ネットワークへの不正機器接続などを防止
2		装置・機器への侵入防止	外部媒体やネットワークを介しての侵入、不正者による侵入を防止
3	活動抑止	ネットワーク内の不要通信遮断	設計仕様外の通信を抑止
4		装置・機器での不正なプログラム実行、不正なファイル操作の抑止	決められたプログラム以外の実行、ファイルへの書き込みや参照を抑止
5		装置・機器の不正利用の抑止	決められた利用者以外の装置・機器の利用を抑止（装置・機器の機能／プログラム／データ／インタフェースを含む）
6	運用支援	特定・可視化	保護対象を特定、構成を管理、状況を可視化
7		検知	不正な侵入や不正な活動を検知したときにアラートを通報
8		分析	障害が発生した場合の原因分析のために、ログを記録・収集・分析
9		回復	マルウェア感染などによる業務障害状態から正常状態への復旧

これらの対策は、工場システムを構成する「ネットワーク」、「設備や計算機などの装置・機器」、及び「業務プログラム・利用サービス」に対して実施することになる。

それぞれの対策の内容を以下に説明する。

① ネットワークにおけるシステム構成面でのセキュリティ対策

工場システムは、制御装置・機器を中心に、システム全体を統合的に制御するために、ネットワークを介して周辺機能と連携する構成となっていることが多く、セキュリティ対策においてもこの特質を考慮する必要がある。

ネットワークにおける対策として、「不正な装置・機器が接続されないこと」、「他のネットワークから不正なデータやプログラムが流入してこないこと」を目的に、

- ネットワーク機器(スイッチ、ルータ)の設定
- セキュリティ機器(ファイアウォール(FW)
- 侵入検知システム(IDS)
- ゲートウェイ機器)の導入
- ネットワーク機器やセキュリティ機器に対するセキュリティ関連の設定(ID／パスワード設定、アクセス制御ポリシ設定など)
- ネットワークへの侵入行為を運用で早期に発見するための機能の利用

等を行うことが考えられる。

表 3-22 に、想定工場において、具体的な対策として考えられる項目と、当該項目ごとのセキュリティ強度ごとの対策及びシステム構成面のセキュリティ対策の目的との整合関係について例示している。

個社や業界の置かれた環境によっては、必ずしもセキュリティ強度と対策が表 3-22 の内容が整合しない場合もあると考えられるが、いずれにせよ個社や業界の置かれた環境に応じ、対策の費用対効果等も勘案しながら、必要な対策を企画・実行することが重要である。

表 3-22 ネットワークにおけるセキュリティ対策（例）

対策項目	セキュリティ強度ごとの対策			目的		
	最低限	中	高	侵入防止	活動抑止	運用支援
構成分割	－	VLAN 等による論理ドメイン構築	物理ドメイン分割	○	○	
接続機器制限	－	IP、MAC 制限	＋接続機器の論理証明	○	○	
内部秘匿	－	NAT、ステルス	ゲート機器設置	○		
通信データ制限	送信元／宛先制限(FW)	＋通信電文種別制限	＋電文内容解析(IDS/IPS)	○	○	

対策項目	セキュリティ強度ごとの対策			目的		
	最低限	中	高	侵入防止	活動抑止	運用支援
利用者制限	不要ユーザ削除、パスワード(定期)変更	＋個人 ID 認証(1 要素認証)	＋多要素認証	○	○	
通信監視・制御	－	通信状況可視化・監視、異常検知	＋異常通信遮断	○	○	○
構成管理	－	接続機器管理・可視化	＋機器内の構成管理・可視化			○
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査、[＋仮想対策(IPS、仮想パッチ等)]	＋ソフトウェア更新(セキュリティパッチ適用)	○	○	
ログ取得	－	機器内ログ取得	IDS ログ連携			○

② 機器におけるシステム構成面でのセキュリティ対策

機器におけるシステム構成面での対策[16]として、「機器に不正なプログラムなどを設置・導入させないこと」、「機器内で不正なプログラムやコマンドの実行をさせないこと」を目的に、

- 機器の設定
- セキュリティソフトウェアの実装
- 外付けのセキュリティ機器の導入
- ネットワークへの侵入行為を運用で早期に発見するための機能の利用

等を行うことが考えられる。

表 3-23 に、具体的な対策として考えられる項目と、当該項目ごとのセキュリティ強度ごとの対策及びシステム構成面のセキュリティ対策の目的との整合関係について例示している。

個社や業界の置かれた環境によっては、必ずしもセキュリティ強度と対策が表 3-23 の内容が整合しない場合もあると考えられるが、いずれにせよ個社や業界の置かれた

16 工場における生産設備や計算機などの機器には、サーバ、操作端末 PC、プリンタ、高機能な機器など汎用 OS／ソフトウェアを利用している機器や、独自の OS／ソフトウェアを用いて構築している装置などがあるが、ここでは汎用 OS／ソフトウェアを利用する機器を想定している。

環境に応じ、対策の費用対効果等も勘案しながら、必要な対策を企画・実行することが重要である。

表 3-23 機器におけるセキュリティ対策例

対策項目	セキュリティ対策強度			目的		
	最低限	中	高	侵入防止	活動抑止	運用支援
通信制限	不要サービス閉塞	＋通信先制限	＋FW の導入	○	○	
不要ポート	端子キャップ	＋ソフト閉塞(サービスの停止、USB クラス制限等)	＋ハード閉塞(完全に利用不可)	○	○	
利用ポート	－	媒体検査	＋内容検査	○	○	
通信／接続機器認証	－	IP、MAC、デバイス ID 認証	＋相手機器の論理証明(暗号による)	○	○	
送受信データ保護	－	暗号化、暗号鍵の管理	＋暗号鍵の厳密な保護	○	○	
利用者制限	不要ユーザ削除、パスワード(定期)変更	＋個人 ID 認証(1 要素認証)	＋多要素認証	○	○	
実行プログラム保護	－	プログラム改ざん対策	＋保護ツール活用	○	○	
実行プログラム制御	不要プログラム停止・削除	ユーザグループ管理、グループ実行権限付与、ユーザ権限動作	実行制御ツール活用	○	○	
ファイル保護	ユーザグループ管理	＋暗号化	＋保護ツール活用		○	
資源保護(CPU，メモリ，ディスク)	－	定期確認	保護ツール活用		○	
構成管理	－	機器内の構成管理・可視化	＋設定情報管理・可視化			○
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査、[＋仮想対策(IPS、仮想パッチ等)]	＋ソフトウェア更新(セキュリティパッチ適用)	○	○	
ログ取得	－	システムログ取得	＋業務ログ取得			○

対策項目	セキュリティ対策強度			目的		
	最低限	中	高	侵入防止	活動抑止	運用支援
バックアップ（データ、機器）	－	定期オフラインデータバックアップ	＋切替え機器の確保			○
電源可用性確保	－	UPS の導入	＋自家発電設備の導入			○

③ 業務プログラム・利用サービスにおけるセキュリティ対策

工場システムでは、各種パッケージソフトウェアの利用や独自プログラムによる機能構築、さらには外部ベンダが提供するサービスの利用により、必要な機能が実現されていることがあるが、こうしたサービスを利用する場合には、例えば以下の観点で確認を行うことが考えられる。

表 3-24 業務プログラム・利用サービスにおける確認事項（例）

パッケージソフトウェア	• セキュリティに関する機能仕様が記載されているか • セキュリティに関する設定項目の設定値が記載されているか • セキュリティ上の不具合が発生した場合の対応が記載されているか
独自プログラム	• セキュリティを考慮した機能仕様となっているか • プログラム構築時のセキュリティルールが整備されているか
外部サービス	• セキュリティに関する仕様が提示されているか • セキュリティに関する設定項目の設定値が記載されているか • セキュリティ被害の影響に関する取り決めが記載されているか

(2)　物理面での対策 [6.2.2]

自然環境の脅威や物理的な侵入などの脅威に対しては、主に物理面での対策が必要となる。主な対策は、生産設備・制御システム等を物理的に守るもので、建物の構造、防火・防水の強化や、電源設備・制御システムの施錠管理、入退室管理、バックアップなどになる[17]。

① 建屋にかかわる対策

工場建屋は、生産現場を中心に生産設備、自動搬送・倉庫設備、建物設備などを各室に配置した建物であり、その中でも、生産に不可欠な生産システム、自動搬送・倉庫システム、システム間ネットワーク、及びそれらを構成する装置・機器などを、安定的かつ継続的に運用するのに最適な環境及び基盤を提供することが必要となる。

17 工場のサイバーセキュリティ対策は、生産設備・制御システム自体にとどまらず、建築施設ファシリティ面の対策まで考えておく必要がある。ファシリティ面の対策に関しては、「ビル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」が参考となる。

【参考】建屋にかかわる対策（例）

表 3-25 建屋にかかわる対策（例）

防水対策	工場建屋は、大雨や洪水などにより、壁やダクトの隙間から浸水することが想定される。工場の運用開始後、経年劣化により、止水処理能力が低下することも考える必要がある。 例えば、以下の例を参考にして、必要な対策を実施することが望ましい。 • 建屋の外壁を配管やケーブル等が貫通する箇所は、コーキング・モルタル等による止水処理を行うこと • サーバ室の天井裏や隣接室には、水を扱う部屋(トイレ等)や配管を設置しないこと • 行政が公開しているハザードマップや近年の気象条件から、水害時の想定水没レベルより低い位置には、貫通部を設けないこと • 漏水により水が滞留しやすい埋設ダクトや、フリーアクセスなどには、漏水検知の仕組みを備えること
有害生物の侵入対策	建屋のケーブルダクトや配管ラックの開口部は、鼠などの有害生物が入りこみ、電気ケーブルとの接触による漏電や、短絡の発生などにより、生産ラインの停止や工場全体の操業停止に陥ることも想定される。 例えば以下の例を参考にして、有害生物の侵入対策を検討することが望ましい。 • 隔壁等により汚水槽、動物飼育場等の不潔な場所から完全に隔てられていること • 鼠等の小動物の侵入を防止するため、外部に開放される窓や吸・排気口等には、網戸や金網等の覆いを設置すること • 外部に開放される出入口には、自動開閉式の扉等や前室を設けること

② 電源／電気設備にかかわる対策

工場・生産設備は、電源の停電・瞬断・電圧変動だけでなく、法定点検、機器の増設・撤去、電源設備・機器の故障などの時にも、製品の生産・品質に影響を与えない、高信頼な電気設備の構築が必要となる。このため、

- 生産設備、自動搬送・倉庫設備などとBAS(ビルディング・オートメーション・システム)とを連動させた設備監視体制の構築
- 信頼度の高い電源設備構成の構築

などが求められる。

なお、サイバー攻撃により、電源／電気設備が攻撃を受け、生産ラインのみならず、生産管理・監視システムや情報系(OA)システムも稼働停止に至る被害の発生も増えてきているが、こうした事態に対応する際に、生産設備やラインの重要度などから給電停止が許容できない設備の場合には、それにかかわる電気設備の構成は、生産ラインのトラブルやサイバー攻撃による設備停止・故障時だけでなく、定期点検時においても、給電の継続が可能となるように冗長性を持たせた設備構成とすることが必要である。

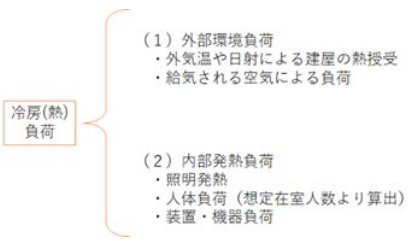
③ 環境(空調など)にかかわる対策

工場の生産ライン、自動搬送・倉庫設備などの環境や、各種システム及びネットワークを構成する機器を設置するサーバ室(計算機室、電算室等)の環境は、

- 空調による冷却 [18]
- 湿度、静電気抑制、空気清浄度

などの諸条件を考慮する必要がある。

この際、空調の冷却方式や仕様の選定については、装置の熱負荷計算を行うことや、外部環境からの負荷や内部発熱による負荷を算定し、冷房負荷計算を行うといった方法がある [19]。算定後、空調機の仕様や台数を確定し、熱負荷に合う冷却方式が選定されたサーバ室を構築する。



負荷計算種別	算定内容
冷房(熱)負荷計算	外部環境負荷と内部発熱負荷を対象に算定
加湿負荷計算	加湿設備を設ける場合、冬季の冷房負荷計算温湿度条件の下限値加湿負荷を算定
除湿負荷計算	除湿設備を設ける場合、夏季の冷房負荷計算温湿度条件の上限値で除湿負荷を算定

図 3-4 空調設備の熱負荷計算の方法

18 主にサーバ室の冷却には空調設備を設置し、冷却を行うことが一般的である。
19 季節の条件にもよるが、加湿が必要な寒冷地や、除湿が必要な高温多湿の地域では、それぞれ加湿負荷、除湿負荷も併せて算定する。

④ 水道設備に関わる対策

工場には、水道がないと稼働しない機器がある。設備に使用する冷却水は、循環式が多く循環が停止すると冷却効率の低下や最悪設備停止に至ることもあることから、例えば、

- 冷却水配管の冗長化
- ポンプの冗長化
- 台数制御にて停止時間を少なくする

等の対策を行うことが考えられる[20]。

また、水道設備停止時への対策も必要であり、異常による停止・故障だけでなくポンプ整備などの設備保全時にも停止できるような設計とすることが考えられる。

[20] 冬は凍結することもあるため、凍結防止対策を実施することも考えられる。

⑤ 機器に関わる物理的対策

工場システムに用いる機器[21]に対する、設置場所や利用業務の重要性に応じ、また運用面も考慮した上で、セキュリティ対策を行うことが考えられる。

表 3-26 機器にかかわる対策（例）

転倒・落下防止	地震などによる機器の転倒・落下防止対策
盗難防止[22]	不正侵入者や内部不正者による機器の盗難防止対策 ・固定可能な計算機や工作機器: 必要な固定の実施。特に重要な業務に関係する装置・機器は、設置場所も考慮。 ・モバイル機器や可搬型の記憶デバイス: 物品管理方法として、保管方法及び利用方法の設定。定期的な監査の実施。
悪用の防止	盗難された機器により、FA 工場システムに侵入し攻撃されることを防止する対策。 ・盗難された機器がネットワークに接続されても、不正な機器として検知し、通信やデータのやり取りを防ぐような仕組みの構築 ・盗難された外部記憶デバイスも同様に、機器に接続されても、不正なデバイスとして検知し、通信やデータのやり取りを防ぐような仕組みの構築。
情報窃取の防止	盗難された記憶デバイスにより、内部に保存された情報を利用されないための、データ暗号化などの仕組みの構築。
内部不正／過失の防止	工場内部で、故意に、あるいは過失により、機器に対して不正なネットワークやデバイスが接続され、マルウェアに感染したり、サイバー攻撃を受ける入り口が増えたりすることを防ぐための、不要なインタフェース／ポート(LAN、USB など)の物理的な閉塞。

21 例えば、ネットワークに接続される計算機(サーバ、PC)や工作機器がある。さらに、無線や携帯電話網を活用するモバイル機器や、ネットワークには接続せず単独で設置し、データを可搬型の記憶デバイス(USB メモリや SSD メモリなど)により連携する機器がある。

22 盗難防止策を実施してもなお盗難される場合があることから、盗難されても、業務や企業信頼に影響が出ることのないよう不正利用防止策を講ずることも考えられる。

⑥ 物理アクセス制御にかかわる対策

物理アクセス制御は、生産設備・計算機などの産業制御システム／機器や、それらに付随する情報システムなどへの物理的なアクセスに対する保護を指す。具体的には、

- 産業制御システム／機器の専用室(サーバ室・計算機室)の設置
- 入退管理システムの導入
- 監視カメラの設置
- 管理・監視体制の構築

といった対策が挙げられる。

【参考】入退管理の考え方

物理アクセス制御の基本は入退管理である。入場・入室権限を持たない人の入場・入室を拒否し、正当な権限を持つ人だけに入場・入室を許可する機能と、入場・入室後、適切な時に確実に退場・退室したかどうかを確認できる機能に基づいた入退管理が必要である。不正な侵入の防止を主目的に行われる、訪問者の管理のみであれば、受付に人を配置し管理するだけでも良いが、工場内の部屋を用途に応じたアクセスレベルに分けて、社員も対象に「部屋レベル」の入退管理を実施する必要がある場合や、高度な機密性を確保する必要のある部屋に対しては、必要に応じて施錠できるようにした上で、人の認証を実施する装置・機器(ID カードや生体情報による認証装置・機器等)を設置することも考えられる。

一括で集中管理するためには、入退管理システムの導入や、適切なアクセスレベルの区分けの検討を実施する。以下の表は、アクセスレベルに応じた部屋・エリアの分け方・アクセス制御・管理方法の参考例である。必要に応じて、これを参考に、アクセスレベルによるエリアと対象者の細分化、及びアクセス制御・管理の方法を各社にて検討することが考えられる。

表 3-27 アクセスレベルに応じたエリア区分け(例)

低 ↓ 高

アクセスレベル	エリア名称	エリア概要	対象者
1	一般・来客エリア	敷地周辺から敷地内・工場棟内に入ったエリア(受付・応接室など)	来客者・社内関係者
2	執務・生産エリア	社内関係者が常勤し、業務を生産を行うエリア(生産エリア・執務室・社内会議室など)	社内関係者
3	高セキュリティエリア	重要度の高いシステムや情報・データを保管・取り扱うエリア(集中監視室、サーバー室など)	社内関係者(製造管理者・保守に携わる社員)

表 3-28 アクセスレベルにより細分化したエリアと対象者のアクセス制御・管理方法

エリア名称	管理・アクセス制御方法	使用する扉	認証方法
一般・来客エリア	・工場に入場する者は常に名札を着用 ・社内関係者の名札は顔写真付きとする ・ストラップの色正社員/正社員以外を区別 ・来訪者は来訪者用の名札を着用	・ゲートタイプの開閉扉(一人が通過するごとに開閉)	各個人に配布したICカードによって個人認証
執務・生産エリア	・常時施錠し、入室を許可するものを特定する ・管理者を定め、入室者を管理する) ・入室者は常に名札を付ける	・一般的な開閉扉(扉閉鎖時に電気錠にて施錠)	・各個人に配布したICカードによって個人認証 ・暗証番号による認証
高セキュリティエリア	・一般・来客エリアと隣接させない ・常時施錠し、入室及び退室の記録をとる ・出入口付近には監視官根らを設置し、常時監視と監視記録を一定期間保存する	・堅固な開閉扉(扉閉鎖時に電気錠にて施錠)	・各個人に配布したICカードによって個人認証 ・指紋などの生体情報による認証

(a) その他、日常的な運用・管理が必要なもの

物理セキュリティ対策の中には、日常的な運用・管理が必要なものがある。例えば、以下に挙げるような運用・管理の事項[23]が考えられる。

- 実物の状態や、目的とする対策の機能が維持できているかの管理・確認
- 運用状況や異常有無の監視・確認
- 運用・管理状況や各種設定の定期的な監査
- 工場からの不要／不正な機器の持ち出し禁止
- 工場や生産ラインなどへの不要／不正なデバイスの持ち込み禁止 など

【参考】物理セキュリティ運用・管理の担当部署

物理セキュリティの運用・管理は、その対象により、扱う部門が異なる場合が多くある。

- 建屋の入退管理(扉開閉、監視カメラ、持ち出し管理):総務部や保安部門など
- 工場内の対策導入・設置:生産技術・管理部門など
- 工場内の対策運用:工作部門など

企業としてセキュリティを確実に実施するためには、これらの組織が独立で活動するのではなく、連携して企画・設計・導入・運用・管理する必要がある。
特に運用・管理は、各種設定登録／変更～監視～異常(不正)兆候の検知・把握～分析～対処のライフサイクル全体で、それぞれの組織の役割と連携策を明確にしておく必要がある。

[23] 遠隔から一元的・集中的に実施したり、省力化・自動化したりする仕組みを活用できる場合もある。

3.3. ステップ 3：セキュリティ対策の実行・管理体制の構築 ［6.1.4・5］

(1) ライフサイクルでの対策 ［6.2.4］

物理面／システム構成面でのセキュリティ対策を導入したとしても、システムへの攻撃手法の進化により、システムへの攻撃を 100%除去する防御は難しいと言える。このため、業界や個社の状況によっては、物理面／システム構成面での対策に加え、侵入や攻撃活動が発生した場合に被害を最小化するための取組として、早期に発見するための対策や、迅速に対処し攻撃活動を抑止するための対策といったライフサイクルにわたる対策を行うことが重要となる。

運用を開始した後のライフサイクル面の対策として、

(1)運用・管理面の対策

(2)維持・改善面の対策

を示す。

① 運用・管理面のセキュリティ対策

運用・管理面で必要な対策として、3 つの観点を想定し、それぞれの例を示す。

- A) サイバー攻撃の早期認識と対処
- B) セキュリティ対策管理(ID/PW 管理、機器の設定変更など)
- C) サイバー攻撃に関する情報共有 [24]

A) サイバー攻撃の早期認識と対処

セキュリティ攻撃に起因するシステムの異常を早期に検知・把握するために、機器からのアラート、計測値、指示値の挙動などから、通常と異なる兆候に気づき対処する一連の運用業務にサイバーセキュリティ攻撃の視点での監視を加えることが考えられる。また、迅速な対処を実現するために、異常の兆候や問題・被害の発生を想定し、予め役割・体制や手順を整備しておくことが考えられる。

なお、工場システムに障害が発生した場合、その原因がサイバー攻撃であることがすぐ判明するわけではない。工場システムの障害の状況に応じて、どのような場合にセキュリティ部門と連携するのか、連携する条件・基準や手順を定めておくことが重要である。

[24] サイバー攻撃に関する情報共有組織として、ISAC（Information Sharing and Analysis Center）がある。電力、金融、ICT、交通、自動車等、いくつかの産業分野において ISAC が設置されている。

例えば、サイバー攻撃の認識と対処の一連の取り組みを整理したモデルとして“監視(Observe)－分析(Orient)－判断(Decide)－行動(Act)”[OODA プロセス]がある。

表 3-29　OODA プロセス

監視(Observe)	セキュリティにかかわる監視として、次の 2 種類の監視を実施することが考えられる。 • **従来のアラートからの類推：** 機器故障(停止、誤動作)やアラートが、セキュリティ攻撃に関連しないかを監視。アラートが発生した場合に、要因が従来の故障などだけでなく、サイバー攻撃である可能性も調査・整理し、運用者(組織)で共有する必要がある。 • **セキュリティアラート：** セキュリティ機器やセキュリティ対策ソフトウェアからのセキュリティアラートが発生していないかを監視。ウイルス(マルウェア)対策ソフトウェアの導入、ネットワークへのファイアウォール(FW)や侵入検知システム(IDS)などの導入を行った場合に、それぞれからのアラートなどのメッセージを運用者が認識できることが重要。具体策として、“見つけることができるサイバーセキュリティ攻撃が何か”を明らかにし、これらのセキュリティ対策から発報されるメッセージを、誰がいつ確認(認識)するかを明らかにする。 なお、アラートが発生し検知した段階から、事業継続の観点で企業全体として早期の対応を図るために、全社のリスク管理部門へ連絡・共有し、企業全体で連携し対応していくことが重要である。
分析(Orient)	セキュリティにかかわる分析として、監視によって得られた情報から、サイバー攻撃である場合を想定した「業務・事業への影響」と、異常や問題の「原因」及び「対策方法」を分析する必要がある。分析に必要な情報として、業務とシステムの関連や、システム構成(機器、プログラム、データ、ネットワーク)にかかわる情報を予め整理・把握しておく必要がある。この分析を行うためには、サイバー攻撃の知識を有する専門家との連携が重要であると考えられることから、必要に応じ、セキュリティ専門家との連携方法を予め確立しておく。
判断(Decide)	セキュリティにかかわる判断として、監視で得られた情報及び分析の結果に基づき、対策案を立案し、何を実施すべきかの意思決定を行う必要がある。的確で迅速な判断ができる体制や、方針・判断基準[25]、連絡先・手段を予め確立しておく必要がある。

25　工場の事業継続計画において定められている目標復旧時間、目標復旧時点（復旧ポイント、バックアップ）、最大許容時間等の要求事項を踏まえ、工場システムの復旧方法や

	この意思決定を迅速にするためには、工場システムにおいて、「業務」と「システム(機器・ネットワーク)」との関係、「業務」や「システム」が被害を受けたとき影響度・影響先といった情報を予め整理・把握し、何を優先させるべきかの方針・判断基準を設けておくことが重要である。
行動(Act)	セキュリティにかかわる行動として、判断で決定した対策内容に従い、関連する各部門(全社のリスク管理、情報システム、総務、法務、財務、広報などを含む)に連絡・指示を出すとともに、対策を確実に実施し、想定した効果が得られるかを検証する必要がある。そのためには、サイバーセキュリティ攻撃が発生し対策を実施するときの体制、役割、手順、連絡先・手段を、予め明確に規定しておくことが重要である。また、連絡・指示を出すためのフォーマット、及び対策状況を管理するための準備を行っておくことが望ましい。

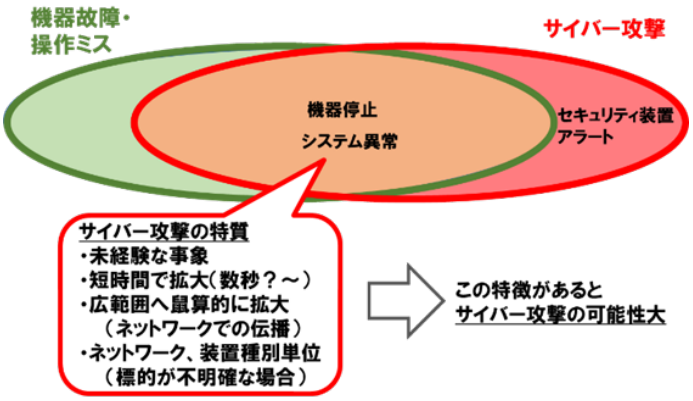


図 3-5 アラート発生要因の調査・整理

表 3-30 アラート発生要因としてセキュリティ関連の可能性を想定

発生事象		発生要因		
機器	内容	対象	推定要因	セキュリティ関連
監視システム	XX 機器停止アラート	XX 機器	機器故障	
			不正指示による機器停止	○
		ネットワーク	誤信号	○

人的対応・他の生産拠点の活用を含めた代替手段の利用等についての、方針・判断基準の設定などが考えられる。

表 3-31 セキュリティアラートの分類と対応内容

機器	メッセージ種別		
	種別	発報タイミング	対応内容
FW	通信拒否	認識時	対象機器の確認
IDS	不正通信	解析時	対象機器及び通信内容確認

分析(Orient)における分析内容、及び判断(Decide)における判断内容を以下に示す。情報が得られるタイミングが「兆候段階」か「被害発生段階」かにより、分析する内容及び判断内容が異なる[26]。

表 3-32 分析(Orient)における分析内容及び判断(Decide)における判断内容

	分析(Orient)における分析内容	判断(Decide)における判断内容
兆候段階	• 業務・事業への影響が無い段階で発見された事象なので、予防保全を中心に分析 • 発生する可能性がある事業被害の推定、原因の推定、影響防止方法(予防保全対策)の検討	• 稼働している生産ラインへの影響を考慮しながら、予防保全対策を決定
被害発生段階	• 業務・事業への影響が発生している段階なので、早期収束を中心に分析 • 原因の推定、影響極小化方法(被害発生対象への対策、被害拡大防止策)、システム／業務／事業回復方法の検討	• システム／業務／事業回復と連携し、被害発生対象への対策、及び被害拡大防止策を決定(封じ込め対策に加え、最終的には根絶対策も併せて実施) • 影響が及ぶ可能性のある各種ステークホルダ(顧客、取引先など)の連絡先

[26] セキュリティにかかわる異常や被害へ対応するための取組みのことを「セキュリティインシデント対応」と呼ぶ。インシデント対応のために必要な機能、役割、体制、方針、手順の整備に関しては、既存のガイドラインにおいても整理されており、詳しくは付録〇を参照。

B） セキュリティ管理

セキュリティ対策を運用する上で必要な管理作業として、下記に挙げるような運用ルールの作成・実施と、関係者への徹底を行うことが考えられる。

これらの管理を実施していくため、利用者等に対して、機器や媒体の利用や入退室等に関わる運用ルールに関して、周知・教育を定期的に行うことが望ましい。

表 3-33 セキュリティ管理作業（例）

管理対象		目的	運用ルール	管理が必要な情報
1	利用者	不正な者の装置・機器へのアクセス防止	利用者変更依頼に基づき登録/削除、利用状況により確認/削除	装置・機器別の利用者一覧(ID、権限)
2	接続機器	不正な装置・機器のネットワーク接続防止	接続変更依頼に基づき登録/削除、利用状況により確認/削除	ネットワーク別の登録機器一覧 (項目は台帳による)
3	実行プログラム	計算機内で実行を許可するプログラムを統制	構成管理ルールと連携したルール	装置・機器ごとの実行プログラム(ツールで対応)
4	媒体	不正媒体の接続防止、 媒体情報の漏えい防止	媒体の購入～廃棄までを一元管理し、利用状況を管理(クリア化やウイルス検査を含む)	媒体一覧 媒体別利用管理 (項目は台帳による)
5	装置・機器バックアップ	セキュリティインシデントで感染後、未感染な状態に復旧	装置・機器ごとにリカバリを考慮したバックアップ基準	バックアップ履歴
6	入退場者・入退室者	不正な者の管理エリアへの立ち入り防止	入場者変更依頼に基づき登録/削除、利用状況により確認/削除	エリア別の入室者許可一覧
7	図書	設計書や、システム構成図等のシステム情報を保護	ISMS 等の情報管理ルール活用	図書

C) 情報共有

サイバー攻撃に関する情報の入手を適時に行うことは、個社の適切な備えや効果的なセキュリティ対応に繋がり、個社が入手したサイバー攻撃に関する情報を業界や政府に提供することは、業界や社会全体でサイバー攻撃から防御することに繋がる。

具体的には、

- 業界団体や CSIRT 間における情報共有と適宜の業界標準への反映
- 脆弱性情報を情報処理推進機構(IPA)や JPCERT コーディネーションセンター等から入手して自社のセキュリティ対策に導入
- 日本シーサート協議会等のコミュニティ活動への参加により情報を入手し、自社のセキュリティ対策に導入

すること等が考えられる。

【参考:運用管理体制(例)】

サイバー攻撃を早期に発見し対処することは、事業継続や企業信頼を維持する上で重要となる。しかし、セキュリティの運用・管理を実施するためには、体制整備、人員確保、支援ツール整備などが必要となる。

このため、運用・管理体制をどの程度のレベルで整備するかを検討する必要がある。この体制整備の例を提示する。

- 既存システム運用・保守組織での運用
- IT 部門の運用組織での運用
- 外部委託での運用
- 独自組織での運用

(1) 既存システム運用・保守組織での運用

既存システムを運用・保守している現組織において、サイバーセキュリティに関する運用・管理も実施する形態である。各事業部・工場の OT 部門を中心とした組織も該当する。

- メリット:
  従来の障害と併せて対応が可能
- デメリット:
  セキュリティの専門家が不在。通常勤務時間外の場合の即応が困難

(2) IT 部門の運用組織での運用・管理

IT 部門において既に OA システム等のセキュリティ運用・管理を実施してい

る場合に、IT 部門において工場システムのセキュリティ運用・管理も実施する形態である。

- メリット:
  IT 部門のセキュリティ専門家を活用可能。
  24 時間監視を実施している場合は、即応が可能
- デメリット:
  通常発生する従来の障害関連のイベントも発生。
  工場システムの知識がないため、業務への影響を含めた分析が困難

(3) 外部委託での運用・管理
セキュリティ運用・管理全体もしくは一部を社外組織に委託する形態である。

- メリット:
  セキュリティの専門家が社内に不要
- デメリット:
  契約内容のみの委託となり、工場システムの運用・管理との連携が必要

(4) 独自組織での運用・管理
工場システムのセキュリティを運用・管理するための組織を新たに設置する形態である。各事業部・工場の OT 部門と IT 部門(またはセキュリティ部門)のメンバーから構築される委員会のような構成もありうる。

- メリット:全てを総合的に運用・管理可能
- デメリット:専門家の育成が必要。運用・管理要員が必要

② 維持・改善面のセキュリティ対策

維持・改善面のセキュリティ対策とは、工場システムを取り巻く環境の変化にかかわる情報を収集・評価し、BC/SQDC 確保の観点からセキュリティ対策を再検討し、物理面、システム面、運用・管理面のセキュリティ対策を更新することである。

攻撃手法は日々進化し、工場システムや機器におけるセキュリティ上の弱点が新たに顕在化する中、新たな攻撃手法や脆弱性にかかわる情報を収集・把握し、対応することにより、工場システムへの攻撃及び被害を未然に防ぐことができる。

さらに、セキュリティ対策を維持・継続するうえで、組織・人材のスキル向上として、工場システムに携わる人たちが、それぞれの立場に応じたセキュリティスキルを持つことが重要となる。

表 3-34 維持・改善のために必要な活動（例）

変化するセキュリティ脅威・攻撃手法や技術にかかわる情報の入手	脅威情報、セキュリティ技術情報などは、例えば、下記の組織が公開している。 • 一般社団法人 JPCERT コーディネーションセンター https://www.jpcert.or.jp/ • 独立行政法人 情報処理推進機構 https://www.ipa.go.jp/security/index.html
利用機器、及びソフトウェアの脆弱性情報の入手	機器やソフトウェアの汎用品の脆弱性情報は、上記で公開されているが、汎用品以外の機器やソフトウェアの脆弱性情報の取り扱いを、各製品ベンダに確認する必要がある。
人材のスキル向上、育成	工場システムに従事する人へのセキュリティ教育は、OA 関連のセキュリティ教育(メールによる周知など)以外には実施していない場合も多く、さらにこれまでは、工場システムでのセキュリティ攻撃の発生頻度は高くなく、実際に発生した場合に的確に行動することが難しい状況にある。 また、人の定期異動により、スキル自体も衰退する可能性がある。このため、実際の工場システムを前提にした、セキュリティスキルの維持・改善が不可欠となる。 例えば、セキュリティの基礎教育だけではなく、セキュリティ攻撃を発生させることによる模擬訓練を繰り返し実施することが考えられ、これにより工場システムにかかわる人たちが、それぞれの立場で必要なスキルを蓄積・維持・改善することが考えられる。

表 3-35 維持・改善のための体制(例)

工場システムの計画・構築・管理組織で実施（生産技術・管理部門、工作部門など）	工場システムの計画、構築を主に担っている組織において、セキュリティにかかわる維持・改善も併せて実施する形態である。 • メリット: 工場システムの現状に即した検討が可能 • デメリット: セキュリティに関する人財育成、ノウハウ蓄積が必要
IT 管理部門で実施	IT システムにおけるリスク管理を実施している部門で実施する形態である。 • メリット: IT 部門のセキュリティ専門家を活用可能 • デメリット: 工場システムの知識が無いため、業務への影響を含めた分析が困難。現場との連携が不可欠
企業全体のリスク管理部門で実施（リスク管理部、総務部など）	企業のリスク管理を統括する部門で実施する形態である。 • メリット: 組織全体での包括的なリスク管理の一環として実施が可能。 組織間にまたがる施策展開が実施しやすい • デメリット: 工場システムの知識が無いため、業務への影響を含めた分析が困難。 現場との連携が不可欠
セキュリティ統括組織で実施	CISO(Chief Information Security Officer)配下に、セキュリティ問題対応を統括する組織(SIRT: Security Incident Response Team)などを設置し実施する形態である。 • メリット: セキュリティの専門的な視点での判断が可能。 セキュリティの視点で全社横断的な維持・改善が可能 • デメリット: 兼務者中心となりがちで、専門家の確保が困難となる場合がある

(2)　サプライチェーン対策 [6.2.5]

サプライチェーンにおけるセキュリティリスク[27]は、一つの工場内に閉じずに、エンジニアリングチェーン、サプライチェーン、バリューチェーンの連携先まで影響を及ぼし得る[28]ことから、サプライチェーン全体でのセキュリティ対策を検討することが重要である。

本ガイドラインでは、

- 購入製品／部品
- 業務委託
- システム開発委託
- 連携システム

の観点で、それぞれに関して考慮すべき主なポイントを例示する。

なお、サプライチェーンの構造や取り巻く環境は、業界や個社の状況に応じて様々であることから、項目の精査や、各項目の具体化等について適宜検討を行い、必要に応じ、取引先や調達先に対するセキュリティ対策の要請や対策状況の確認[29]を行うことが望ましい。

---

27 工場を狙ったサイバー攻撃では、より脆弱な中小企業や海外の工場をまず攻撃・侵入してから、そこを踏み台にして、その連携先の大企業の工場を攻撃・侵入するケースがある。

28 「情報セキュリティ 10 大脅威 2021」（独立行政法人情報処理推進機構）によると、セキュリティ対策の強固な企業を直接攻撃するのではなく、サプライチェーンのセキュリティが脆弱な取引先等を標的とする「サプライチェーンの弱点を悪用した攻撃」は組織における脅威の第 4 位。

29 ロボット革命・産業 IoT イニシアティブ協議会では、調達元が調達時にサプライヤに期待するセキュリティレベルを満たしているかどうかを簡易的に評価するために「RRI サプライチェーン質問票　Ver.1.0」を策定している。この調査票は、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」をベースにした 25 個の設問から構成され、企業の規模、業種を問わず、利用可能である。

RRI サプライチェーン質問票　https://www.jmfrri.gr.jp/document/library/1890.html

表 3-36 取引先や調達先への主な確認ポイント（例）

購入製品／部品	製品／部品購入時に下記の点を確認する。 • 保守範囲として、セキュリティに関する脆弱性情報や修正プログラムの提供が含められているか • セキュリティ脅威が発生した場合に、対応できる体制ができているか また、依頼時に即応が可能な契約形態となっているか • 当該製品／部品のセキュリティ視点での機能実装、及び検証[30]が実施されているか
業務委託	システムにかかわる業務の一部を委託する場合に、下記の点を確認する。 • 従事者に対するセキュリティ要件が明記されているか また、要件は自社と同等、もしくは、より厳しい内容となっているか • 従事者に対するセキュリティ教育が実施されているか また、実施する教育内容は自社と同等、もしくは、より厳しい内容となっているか
システム開発受託	システム開発の一部を委託する場合に、下記の点を確認する必要がある。 • 開発プロセスの各フェーズにおいて、セキュリティを考慮する要件が記載されているか • 成果物の検収時に、セキュリティ仕様及び実装状況の確認が記載されているか • 取扱い情報の守秘義務に関する要件が記載されているか • 委託終了時に、情報を破棄することが記載されているか • 開発環境に関するセキュリティ要件が記載されているか • 監査に関する要件が記載されているか
連携システム	工場システムを他のシステムやクラウドサービスと連携する場合に、下記の点を確認する。 • 連携システムを管理する部門と、セキュリティに関する情報を連携することが記載されているか • セキュリティ障害が発生した場合の責任範囲が記載されているか • セキュリティ障害が発生した場合に、問題解決に向けた協力内容が記載されているか • セキュリティ訓練の共同実施が記載されているか

30 「セキュリティ機能の具備」、「セキュリティ検査・診断」、「製品セキュリティ認証」など

【参考】下請振興基準

中小企業庁が、下請中小企業の振興を図るため、下請事業者及び親事業者のよるべき一般的な基準として下請中小企業振興法第 3 条第 1 項の規定に基づき、定めた下請振興基準において、情報化への対応に際し、以下の事項が記載されている。

第３　下請事業者の施設又は設備の導入、技術の向上及び事業の共同化に関する事項

５）　情報化への積極的対応

(1) 下請事業者は、管理能力の向上、事務量軽減、事務の迅速化等の業務工程の見直しによる効率性の向上のため、必要なセキュリティ対策と併せて、次の事項に積極的に対応していくものとする。

① 情報化に係る責任者の配備及び企業内システムの改善（業務のデジタル化推進を含む）

② 中小企業共通ＥＤＩ（電子データ交換）などによる電子受発注

③ 電子的な決済等（インターネットバンキング、電子記録債権、全銀ＥＤＩシステムなどの活用）

(2)親事業者は、前号の下請事業者による取組の支援のため、下請事業者の要請に応じ、管理能力の向上についての指導、標準的なコンピュータやソフトウェア、データベースの提供、オペレータの研修、セキュリティ対策の助言・支援及び国・地方自治体による情報化支援策の情報提供等の協力を行うものとする。また、サプライチェーン全体の業務工程の見直しによる効率性向上を図る観点から、次号の配慮を行いつつ、電子受発注及び電子的な決済等の導入を積極的に働きかけていくとともに、自らも共通化された電子受発注又は電子的な決済等に係るシステムへの接続に努めるものとする。

（出典：中小企業庁 HP）

https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun.htm#zenbun

【参考】稼働中の工場と新設の工場における対策の考慮

工場システムにセキュリティ対策を行う場合、対象とする工場システムが「稼働中なのか」「更新間際」「新設を計画中」のものか、状況を考慮した対策が必要となる。

(1) 稼働中の工場システムへの対策

システム改修に伴うインパクトを考慮し、工場システムへの実装を検討する。この場合、既存の工場システムへ与える影響がない対策を優先し、影響がある対策については、工場システムのメンテナンス期間など定期的なシステム停止期間での対応を検討する。また、教育や運用での対策も併用することで工場システムのセキュリティリスクを低減することを検討する。

(2) 更新間際の工場システムへの対策

更新間際の工場システムに対しては、更新対象の部分と、継続して利用する部分においてセキュリティ対策に対して差が内容に考慮する。既存システムへの対策が難しい場合は、更新部分と既存部分がセキュリティの観点で悪影響を与えない対策についても検討する。

(3) 新設を計画している工場システムへの対策

工場システムは、10 年以上利用することが多くある。この間に新たなインテリジェント機器の導入や初期導入機器のサポート切れなどが発生する。このため、新設を計画している工場システムでは、今だけでなく将来の変化を想定したセキュリティ対策が必要となる。

それ以外は、リスク分析の結果リスクが高い脅威に対応するものから順に実施する。

ただし、実施する対策はシステムの各装置の対策のみでは限界があり、必要に応じて業務プログラムや、教育・訓練、運用支援などを組み合わせる必要がある。

【参考】戦略の実行管理

策定した戦略を確実に実現するための管理策を明確にする。

策定した全体方針に基づき、今後実施すべき計画を明確にする。

計画策定時には、意図した効果を得るために、目的、方針、計画推進に責任を持つ体制を明確にするとともに、狙う効果ごとに実施計画、費用及び人員計画を明確にする。

進捗確認は、実施計画に対する進捗状況を確認するとともに、実施計画の前提となったステップ 1 で収集・整理した情報「経営目標との関連整理」、「外部要求事項の考慮」、「内部要件／状況の把握」に変化が無いかを確認する。

＜観点の例＞

経営目標との関連整理:

・製品のラインナップの増強、フレキシブルなライン構築
・別のスマート工場との新たな接続
・工場のエネルギー効率の向上
・環境上のより強い配慮　等

外部要求事項の考慮:

・経済安全保障上の要求
・新たな国際規格の策定　等

内部要件／状況の把握:

・全社セキュリティルールの見直し
・ネットワーク構成、装置・機器構成の変更、セキュリティ対策の変更
・セキュリティ監視範囲の変更、ソフトウェアの更新
・セキュリティ体制の変更、セキュリティ教育の充実　等

これらの変化に伴い、保護資産や業務の重要度の見直しが必要となる可能性がある。

また、組織の周りのサイバー攻撃が進化していること、攻撃も高度化しているため、脅威は常に変化している。対策においても、技術進歩で今まで実施できなかった対策が、安価にあるいは低負荷で実現できるようになる場合がある。

この結果に基づき、必要であれば計画を見直し、経営者の了承を得ながら、継続的かつ適応的に実行を進めていくことになる。

付録 A　用語／略語

AGV《Automatic Guided Vehicle》

CISO《Chief Information Security Officer》

CMMI《Capability Maturity Model Integration》

CPS《Cyber Physical System：サイバーフィジカルシステム》

CPU《Central Processing Unit：中央演算装置》

CSR 報告書《Corporate Social Responsibility》

DCS《Distributed Control System：　分散制御システム》

FA システム《Factory Automation》

FW《FireWall》

ICS《Industrial Control System：産業制御システム》

IDS《Intrusion Detection System：侵入検知システム》

IP アドレス《Internet Protocol Address》

IPS《Intrusion Prevention System：侵入防止システム》

ISMS《Information Security Management System》

LAN《Local Area Network：ローカルエリアネットワーク》

NIST《National Institute of Standards and Technology：米国国立標準技術研究所》

OA システム《Office Automation》

OODA《Observe、Orient、 Decide、Act：観察、状況判断・方向づけ、意思決定、行動》

OT《Operational Technology》

SIRT《Security Incident Response Team》

SOC《Security Operation Center》

SSD《Solid State Drive》

VPN《Virtual Private Network》

アクセス制御(Access Control)
コンピュータやネットワークにアクセスできるユーザを制限する機能のこと。

暗号鍵
データの暗号化や復号を行う際、計算手順に与える短い符号のこと。 同じデータを同じ暗号方式で暗号化しても、異なる暗号鍵を用いて計算することで異なる暗号を得ることができる。

アンドン
必要な情報を、必要な人に、タイミングよく知らせるための「目で見る管理のためのツール」のこと。

インタフェース
「境界面」「接点」などという意味を持つ言葉で、IT の分野では、2 者間の情報のやり取りを仲介する規格や機能のこと。

エンジニアリングチェーン
製造プロセスにおける設計部門を中心とした業務で、企画構想から始まり、製品設計、工程・設備設計、生産準備、アフターサービスまでの一連業務のプロセスのこと。商品企画あるいは受注から始まり、設計・生産準備・製造・調達という一連の業務を技術や情報という観点で結びつける。

エンジニアリングツール

コントローラの制御プログラミングや、設定を行うツールのこと。

オンライン操作
稼働中の設備に対する操作のこと。コントローラにエンジニアリングツールから生産設備が動作中でもシステム情報や動作設定データを変更できる機能を指すこともある。

可用性(Availability)
障害（機器の故障、災害、事故など)、サイバー攻撃、設定／操作ミスなどにより、システムを停止させることなく稼働し続けること、またはその指標のこと。

完全性(Integrity)
正確さ及び完全さの特性。[JIS Q 27000:2014]

機密性(Confidentiality)
認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性。[JIS Q 27000:2014]

クライアント
クライアント・サーバシステムにおいて、サーバ（英: server）に対してサービスの依頼を行いその提供を受けるような、コンピュータまたはアプリケーションやプロセスのこと。

ゲートウェイ
コンピュータネットワークにおいて、異なるネットワーク同士がデータをやり取りする際、中継する役割を担うルータのような機能を備えた機器やそれに関するソフトウェア。

権限昇格攻撃
ソフトウェアや操作者の ID が持つ実行権限を昇格させてあらゆる攻撃を実行させること。

コーキング
建築物において目地剤などで隙間を塞ぐ作業を指し、気密性や防水性を高めることを目的として行う作業のこと。

コマンド
人間からコンピュータへ、あるいは機器間、ソフトウェア間などで交わされる、実行すべき処理の指示や依頼などのこと。

サプライチェーン
製品の原材料・部品の調達から販売に至るまでの一連の流れのこと。あるいは、それを実現する目的で、他社のシステムを含めた複数のシステムが相互に連携すること。

システム構成情報
生産設備などのシステムにどのような計算機や機器などが使われているかの情報のこと。
場合によっては、計算機の OS や導入されているソフトウェア群の情報も含むことがある。

実行モジュール
ユーザプグラムをコントローラが処理できるような形に変換したもの。

真正性(Authenticity)
エンティティは、それが主張するとおりのものであるという特性。[JIS Q 27000:2014]

脆弱性
コンピュータのハードウェアやプログラムにおける不具合や設計上のミスによるセキュリティ上の欠陥のこと。
一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JISQ 27000:2014]

責任追跡性(Accountability)
情報の閲覧や編集などの動作、または情報を取り扱っている人を追跡できるようにすること。

セグメント
ネットワークを構成する個々のネットワーク環境や、コンピュータのメモリで一度にアクセスできる領域のこと。

操作用表示端末
機器やシステムを監視・操作するための端末のこと。HMI《Human Machine Interface》とも言われている。

ゾーン
システムの設定などによりネットワーク上に設けられた論理的な区画のこと。

ソフトウェア

コンピュータを動作させるためのプログラムや命令を記述したデータのまとまりのこと。

段取り替え
生産ラインに流す製品に合わせて、加工機や治具・装置の設定を変更する作業のこと。

通信妨害
通信信号に対する妨害（ECM）のこと。無線の場合、正規の電波通信と同一の周波数または周波数帯の電波を送出し、混信もしくは電波障害を引き起こすことで、正規の通信を妨害する。

ディスク
ハードディスクや CD/DVD/Blu-ray Disc などの薄い円盤状のデータ記憶媒体（メディア）や、そのような媒体を利用した外部記憶装置（ストレージ）のこと。

デバイス ID
機器を特定するための識別子で、数字や文字から成る文字配列で規定されることが多い。

電子認証
対象がなりすまし等の虚偽のものではないことを電子的に確認する仕組み。

トレーサビリティ
「その製品がいつ、どこで、だれによって作られたのか」を明らかにすべく、原材料の調達から生産、そして消費または廃棄まで追跡可能な状態にすること。

内部統制報告書
企業の財務報告に関する内部統制が有効に機能しているかどうかを経営者自身が評価し、その結果を記載した報告書のこと。

ハードウェア
コンピュータのシステム全体を構成する機器の総称で、コンピュータ本体、ディスプレイ、プリンタ、キーボードなど、目に見えるものを示す。

バリューチェーン
製品の製造や販売、それを支える開発や労務管理など、すべての活動を価値の連鎖として捉える考え方のことで、競合と比較して強み、弱みを分析して事業戦略の改善策を探るフレームワークのこと。

否認防止(Non-Repudiation)
主張された事象（3.21）又は処置の発生，及びそれらを引き起こしたエンティティを証明する能力。

ファイアウォール
あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のこと。

フィードバック制御
制御系において、出力（制御量）を入力（目標値）側へフィードバックすることにより制御品質をあげる制御方法のこと。

フリーアクセス
フリーアクセスフロアとは、床下に電源や通信用の配線、さらに空調設備などの機器を収納することのできるフロアのこと。

踏み台攻撃
攻撃者が攻撃対象とするコンピュータ以外のコンピュータに侵入し、このコンピュータを介して、攻撃対象のコンピュータを攻撃すること。

ペネトレーションテスト
侵入可否の検査。システム全体の観点でサイバー攻撃耐性がどのくらいあるかを試す為に、悪意のある攻撃者が実行するような方法に基づき、検証ツールもしくは専門家によりシステムに侵入することができるかを確認すること。

ポート
機器やソフトウェアが外部の別の主体と接続・通信するための末端部分のこと。

ポート番号
インターネットで標準的に用いられるプロトコル（通信規約）である TCP/IP において、同じコンピュータ内で動作する複数のソフトウェアのどれが通信するかを指定するための番号のこと。

ホワイトリスト
不正なプログラムの実行、通信、操作をさせないことによりサイバー攻撃を防ぐ手法で用い

られる、「安全な対象」のリスト定義のこと。

メモリ
コンピュータにおいて、プログラムやデータを記憶する装置のことである。 特に、RAM や ROM などの半導体記憶装置のこと。

モルタル
砂（細骨材）とセメントと水とを練り混ぜて作る建築材料ペースト状で施工性が良く、仕上げ材や目地材、躯体の調整などに多く用いられるもの。

ランサムウェア
PC 内のデータを勝手に暗号化することで利用できない状態にして、暗号化されたデータの復号に必要な鍵を渡すのと引き換えに身代金を要求するタイプのマルウェア。

有価証券報告書
株式を発行する上場企業などが開示する企業情報で、企業の概況、事業の状況、財務諸表などが開示される。

ユーザプログラム
計算機内のプログラムの種別で、利用者が独自に作成したプログラムのこと。

レシピ情報
生産設備で製品を製造するための調合などのプロセスレシピや、複数のコントローラで成り立つ生産設備の各コントローラの設定値（マシンレシピ）。

付録 B　工場システムを取り巻く社会的セキュリティ要件

3.4. 法規制、標準規格、ガイドライン準拠にかかわる要件 [6.1]

3.4.1. 法規制によるセキュリティ対策の要求 [6.1.1]

法規制の面では、取締役がサイバーセキュリティに関する体制整備を怠ったことが原因で企業に損害が発生した場合には、善管注意義務[31]や忠実義務[32]に対する違反を理由に、取締役個人が会社に対する任務懈怠責任[33]や第三者に対する損害賠償責任[34]を問われる可能性がある。また、サイバーセキュリティ攻撃に対して企業及びシステムとして迅速かつ的確な対処を怠った場合にも、同様に不法行為として問われる場合がある。

上記に該当する損害賠償請求に関する過去の裁判例では、企業として「その当時の技術水準」を満たすセキュリティ対策実装が為されていない場合、経営者の「善管注意義務違反」として「任務懈怠責任」が発生している。この「その当時の技術水準」は、政府系のガイドラインを中心にセキュリティ対策ガイドラインに記載されている内容が該当する。

また、日本のサイバーセキュリティに関する基本的な法律として「サイバーセキュリティ基本法」があり、サイバーセキュリティに関する施策を総合的かつ効率的に推進するため、基本理念を定め、国の責務等を明らかにし、サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を規定している。

この法律に基づき、政府は「サイバーセキュリティに関する基本的な計画」である「サイバーセキュリティ戦略」を定めることになっており、また、国は基本的施策として、重要インフラ事業者等におけるサイバーセキュリティの確保を推進しなければならないことになっている。

---

31 会社法 330 条、民法 644 条
32 会社法 355 条
33 会社法 423 条 1 項
34 会社法 429 条 1 項

【参考：業界毎のセキュリティにかかわる法規制】

●電力分野におけるセキュリティにかかわる法規制 [6.1.2]

電力分野では、米国で、北米の大規模発電施設と送電関連施設を保有する事業者に対して、NERC(North American Electric Reliability Corporation)により策定されたCIP(重要インフラ保護)標準への準拠が義務付けられている。

欧州でも同様に、重要インフラ事業者のセキュリティ対策を義務付ける法規制として、NIS 指令(EU2016/1148)が規定・施行されています。電力分野では、発電／送電事業者に加え、(スマートメータなどの設置責任者を想定し、)小売事業者も対象となっている。

日本でも、電気事業法 第 39 条、及び電気設備に関する技術基準を定める省令により、一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供する電気工作物の運転を管理する電子計算機に係るサイバーセキュリティの確保が規定され、技術基準への適合維持が義務付けられている。

これら発電／送配電事業者からの要求として、発電設備や送配電設備を構成する製品を生産する企業／工場においても、製品のセキュリティを確保するために必要な対策が求められる。

●自動車分野におけるセキュリティにかかわる法規制 [6.1.3]

自動車分野では、国連の自動車基準調和世界フォーラム(WP29)において、車両のサイバーセキュリティやソフトウェア更新にかかわる規則が規定され、それに基づく国際標準規格 ISO/SAE 21434 が規定された。この規則は、国内においてまずは 2022 年 7 月以降に発売される OTA(無線により車載プログラムを改変する機能)対応の新型車に対して、最終的には 2026 年 5 月以降は全ての車両に対して適用・義務化されることになっている。

自動車を生産する企業／工場に対しても、規定された CSMS(サイバーセキュリティマネジメントシステム)に準拠した、セキュリティを確保するためのプロセス(体制、管理・運用、維持・改善)が求められる。

●医療機器分野におけるセキュリティにかかわる法規制 [6.1.4]

医療機器分野では、米国で、医療機器を販売するために必要な市販前認可を受けるための FDA(アメリカ食品医薬品局) 510(k)申請の審査において、サイバーセキュリティ対策の確認が必要とされている。その基準として、「医療機器のサイバーセキュリティ管理のための市販前申請内容(“Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”)」などのガイダンス文書が規定されている。

欧州でも同様に、医療機器のセキュリティ対策を義務付ける法規制として、セキュリティ要件を盛り込んだ EU 医療機器規則(MDR)の適用が開始されている。

日本でも、薬機法により、医療機器は JIS T14971(ISO 14971 相当)に基づくリスクマネジメントが要求されており、JIS T14971 の 2020 年改訂により、セキュリティ対策も要求されるようになった。経過措置が終了する 2023 年 9 月 30 日以降には、JIS T14971:2020 への適合が義務付けられることになった。

また、厚生労働省 医薬・生活衛生局から、「国際医療機器規制当局フォーラム(IMDRF)による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について(周知依頼)」という文書が発行されており、2023 年を目途に、医療機器製造販売業者に対して IMDRF ガイダンスを導入することが示されている。早ければ 2022 年度から当ガイダンスに基づく審査が開始され、医療機器のサイバーセキュリティ対策が求められるようになる見込みである。因みに、IMDRF の医療機器サイバーセキュリティ WG の議長は、米国 FDA の医療機器サイバーセキュリティガイダンス発行責任者が務めており、米国が主導している。また、IMDRF ガイダンスの中で、医療機器のリスクマネジメント原則として上記 ISO 14971 が参照されている。

医療機器を生産する企業／工場に対しても、規定に準拠した、医療機器のセキュリティを確保するために必要な、製品ライフサイクル全体にわたるリスクマネジメントプロセス(体制、仕組み、管理・運用、維持・改善)が求められる。

●重要インフラ分野におけるセキュリティにかかわる法規制 [6.1.5]

重要インフラ分野では、米国で、DHS(米国国土安全保障省)が主導し、エネルギー(電力、ガス、石油)分野をはじめ、原子力施設、防衛産業基盤、政府施設、農業・食料、医療・公共衛生、金融、上下水道、化学、商業施設、重要製造業、ダム、情報技術、通信、緊急サービス、交通・物流の各分野におけるセキュリティ確保のための計画が策定され、政府と業界が共同でセキュリティ対策導入を推進している。法規制としては、まだ一部の分野に限定されている状況である。

欧州では、重要インフラ事業者のセキュリティ対策を義務付ける法規制として、NIS 指令(EU2016/1148)が規定・施行されている。適用対象分野として、重大(essential)エンティティ:エネルギー(電力、石油、ガス)、輸送、医療、上下水道、宇宙などが挙げられ、重要(important)エンティティ:郵便・配送、廃棄物処理、化学品、食品、製造(医療機器、コンピュータ及び電気電子製品、電気設備、機械設備、自動車、その他の輸送機器)などが挙げられている。

日本でも、国家・経済安全保障の観点から、重要インフラのサイバーセキュリティ対策がますます重視されてきており、重要インフラ事業者に対して 2022 年度から重

要インフラにかかわるシステム及び機器のセキュリティ対策が義務付けられる見通しとなっている。

重要インフラとは、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む)、医療、水道、物流、化学、クレジット、石油の 14 分野を指す。

重要インフラを構成する産業制御機器などの製品を生産する企業／工場においても、製品のセキュリティを確保するために必要な対策が求められる。

3.4.2. セキュリティにかかわる標準規格・ガイドライン準拠の要求 [6.1.6]

工場システムにおいてセキュリティ対策を実現するためには、何をどの程度実施すべきかを検討する必要がある。この検討を行うための参照情報として、国内外の規格やガイドラインさらに法規などがあり、さらに取引先が規定している要件などもある。

以下に代表的なものを示す。

(1) 国際標準規格

① 共通的で代表的な規格

- IEC 62443:
  制御システムのマネジメントからシステム、コンポーネントまで、全体のセキュリティを規定
- ISO/IEC 27000 シリーズ:
  サイバーセキュリティのマネジメントを規定
- IEC 61508:
  電気・電子・プログラマブル電子(装置・システム)の機能安全規格

② 分野ごとの規格

- ISO/SAE 21434:
  自動車に関するセキュリティを規定
- ISO 14971:
  医療機器に関するリスクマネジメント及びセキュリティを規定
- IEC 62278:
  鉄道分野における安全に関する規定
  (RAMS: Reliability, Availability, Maintainability, Safety)
- IEC 62351:
  電源系統マネジメント及び関連情報交換データおよび通信セキュリティ

(2) 海外の規格・ガイドライン

① 米国

アメリカ国立標準技術研究所(NIST: National Institute of Standards and Technology)が制定し発行するガイドラインを活用することが多くある。

代表的なものとして「NIST CSF」と「NIST SP800 シリーズ」がある。

- NIST CSF(Cyber Security Framework):
  サイバー攻撃への対策・対応を中心に規定したガイドラインである。
  「識別－防御－検知－対応－復旧」に分類して提示している。
- NIST SP800 シリーズ:
  政府調達システムのためのガイドラインで、その中にセキュリティ要件が規定されたものがある。これらのガイドラインは、政府調達だけでなく、一般のシステムにおいても参照されることが多くある。下記に代表的なものを記載する。
  - SP800-30:リスクアセスメント実施の手引きを提示
  - SP800-53:政府系システム及び組織のセキュリティ管理及びプライバシ管理
  - SP800-82:SP800-53 をベースに、産業用制御システム(ICS)の管理策を提示
  - SP800-115:情報セキュリティを評価するための基本的な技術ガイドを提示
  - SP800-161:SP800-53 をベースに、サプライチェーンの管理策を提示
  - SP800-171:SP800-53 ベースに、政府情報を扱う委託先への管理策を提示

② 欧州(EU)

EU は、加盟国における IT/OT システムや取り扱う情報を保護するために必要となる、セキュリティ要件を規定している。

- NIS 指令(Directive on Security of Network and Information Systems):
  ネットワーク及び情報システムのセキュリティに関する指令である。
  基幹サービス運営者(産業システムも含む)及びデジタルサービス事業者を対象に、システムへのサイバーセキュリティ要件を規定している。EU 各国はこの指令を基に、自国の規則を作成している。なお、2020 年 12 月に改訂され、IoT や DX によるサプライチェーンを見据えた対応(認証製品の利用など)が強化された。

- **一般データ保護規則(GDPR: General Data Protection Regulation):**
  EU 域内の個人データ及びプライバシの保護を規定した規則である。
  EU 圏の人に対する規定のため、EU 圏以外でも同様の取り扱いを要求している。EU 圏で共通の規則。

(3) 国内のガイドライン

① 国内の全般的なセキュリティ関連方針・ガイドライン等

表 3-37 国内の全般的なセキュリティ関連方針・ガイドライン等

発行者	文書名	概要
内閣サイバーセキュリティセンター	サイバーセキュリティ戦略	政府としての全体方針。 2021 年 9 月に改訂
経済産業省	サイバーセキュリティ経営ガイドライン	経営者の役割と行うべき内容を提示
	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)	サイバー・フィジカル空間を融合させた「 Society5.0 」、「 Connected Industries」におけるサプライチェーン全体のセキュリティ対策像を整理
	IoT セキュリティ・セーフティ・フレームワーク ～フィジカル空間とサイバー空間のつながりの信頼性の確保～(IoT-SSF)	「Society5.0」、「Connected Industries」における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の考え方を整理
	「機器のサイバーセキュリティ確保のための セキュリティ検証の手引き」 「【別冊1】機器メーカに向けた脅威分析及びセキュリティ検証の解説書」 「【別冊2】機器メーカに向けた脅威分析及びセキュリティ検証の解説書」	機器のセキュリティを検証するセキュリティ検証における、検証サービス事業者が実施すべき事項を示したもの。 別冊1は、脅威分析の具体例や効果的な検証手法等の考え方を整理するとともに、検証サービス 事業者が実施すべき事項や手法等を網羅的かつ詳細に示す。 別冊2は、IoT 機器等を開発、生産、販売するメーカを対象に、メーカが検証依頼者になる場合に、事前対策含めて検証の知識を提供する。

発行者	文書名	概要
	制御システムのセキュリティ リスク分析ガイド (IPA:情報処理推進機構)	セキュリティリスク導出方法を提示
	制御システム　セーフティ・セキュリティ要件定義ガイド (IPA:情報処理推進機構)	制御システムの安全性確保と セキュリティ対策のための 検討ポイント・手順を提示
	つながる世界のセーフティ& セキュリティ設計入門 (IPA:情報処理推進機構)	IoT 製品／サービスに必要な「セーフティ設計」、 「セキュリティ設計」、 「見える化」のガイドブック
	つながる世界の開発指針 (IPA:情報処理推進機構)	IoT 製品の開発時に 考慮すべきリスクや対策に かかわる指針を提示
	IoT 開発におけるセキュリティ設計の手引き (IPA:情報処理推進機構)	IoT 機器及びその使用環境で想定されるセキュリティ脅威と対策を整理
	組込みシステムのセキュリティ への取組みガイド (IPA:情報処理推進機構)	ネットワークに接続される 組込みシステムのライフ サイクルの各フェーズで 考慮すべき、セキュリティ 取組みの具体的な指針を提示
	組込みソフトウェアを用いた機器におけるセキュリティ (IPA:情報処理推進機構)	組込み機器が抱えるセキュリティリスクを回避するための取組みを提示
経団連	経団連サイバーセキュリティ 経営宣言	経済界が全員参加でサイバーセキュリティ対策を推進することで、安全・安心なサイバー空間の構築に貢献することを表明
	サイバーリスクハンドブック　取締役向けハンドブック 日本版	取締役がセキュリティ脅威による企業経営リスクへの対処策を検討・議論する際に考慮すべき事項を整理し、サイバーリスク管理の 5 原則を提示

A) 業界、製品毎のセキュリティ関連方針、ガイドライン等

表 3-38 民間、業界、製品毎のセキュリティ関連方針・ガイドライン等

発行者	文書名	概要
経済産業省（産業サイバーセキュリティ研究会 WG1（制度・技術・標準化)ビル SWG)	ビル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	ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策を整理したもの。
一般社団法人 日本電気協会	電力制御システムセキュリティガイドライン	電力制御システム等のサイバーセキュリティ確保を目的として、電気事業者が実施すべきセキュリティ対策の要求事項について規定を提示
	スマートメータシステム セキュリティガイドライン	スマートメーターシステムのセキュリティ確保を目的として、一般送配電事業者が実施すべきセキュリティ対策の要求事項について規定
経済産業省	ERAB (Energy Resource Aggregation Business) に関する サイバーセキュリティ ガイドライン	ERAB に参画する事業者が取り組むべきサイバーセキュリティ対策の指針を提示
	小売電気事業者のための サイバーセキュリティ対策 ガイドライン	小売電気事業者が各々の事業モデルに適したサイバーセキュリティ対策を実践していくための指針を提示
一般社団法人 日本自動車工業会・一般社団法人 日本自動車部品工業会	自工会／部工会・サイバー セキュリティガイドライン	自動車産業全体のサイバーセキュリティ対策のレベルアップや対策レベルの効率的な点検を推進することを目的としたガイドライン

発行者	文書名	概要
一般社団法人 重要生活機器 連携 セキュリティ 協議会 （CCDS: Connected Consumer Device Security Council）	CCDS 製品分野別セキュリティガイドライン 車載器編	車載機器において適切なセキュリティ対策を実施するための、設計から製品リリース後までに考慮すべき設計・開発プロセスをガイドラインとしてまとめたもの。
	CCDS 製品分野別セキュリティガイドライン スマートホーム編	スマートホームホーム分野における構成要素・ライフサイクルを踏まえた具体的な対策指針とセキュリティ要件を定義する。
	IoT 機器セキュリティ要件ガイドライン	日常生活で利用する重要生活機器のセキュリティ技術に関する調査研究、ガイドラインの策定や認証制度の提供、標準化の検討を行う業界団体が発行し、IoT 機器に共通に適用可能なセキュリティ要件ガイドライン。
	IoT 機器セキュリティ要件 対策方針チェックリスト	セキュリティ要件ガイドライン要件準拠のための対策方針チェックリスト。
	CCDS IoT 機器セキュリティ 実装ガイドライン(ソフトウェア更新機能)	「ソフトウェア更新」の実装に具体的なセキュリティ要件を提示し、製造者がセキュアな IoT 機器を設計するうえでの指針を提供するガイドライン。
経済産業省（産業サイバーセキュリティ研究会 WG１（制度・技術・標準化）スマートホーム SWG	スマートホームの安心・安全に 向けたサイバー・フィジカル・ セキュリティ対策ガイドライン	スマートホームにおけるサイバー・フィジカル・セキュリティ対策の考え方や各ステークホルダーが考慮すべき最低限の対策について整理したもの。
IoT 推進コンソーシアム	IoT セキュリティガイドライン	IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめたもの。
総務省	スマートシティ セキュリティガイドライン（第 2.0 版）	スマートシティのセキュリティの考え方やスマートシティを実現する上で実施することが推奨されるセキュリティ対策等について整理したもの。

発行者	文書名	概要
	テレワークセキュリティガイドライン	テレワーク実現方法とセキュリティ対策を提示

【参考】セキュリティインシデント対応に関する主なガイドライン

表 3-39 セキュリティインシデント対応に関する主なガイドライン

No.	発行者	文書名	概要、参照先
1	NIST	SP800-61: “Computer Security Incident Handling Guide” Revision 2	セキュリティインシデント対応のために必要な方針、計画、手順、情報共有、体制、機能・サービスを整理し、手順(検知、分析、封じ込め、根絶、復旧、事後活動)と組織間連携・情報共有の内容を提示。 https://www.nist.gov/privacy-framework/nist-sp-800-61
2	情報処理推進機構(IPA)、NRI セキュアテクノロジーズ	コンピュータセキュリティインシデント対応ガイド	NIST SP800-61: “Computer Security Incident Handling Guide” Revision 1 の日本語翻訳。 https://www.ipa.go.jp/files/000025341.pdf
3	JPCERT/CC (Coordination Center)	CSIRT ガイド	CSIRT(コンピュータセキュリティインシデント対応チーム)の概念、役割、体制、組織間連携、準備内容、インシデント対応作業の概要を提示。 https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20211130.pdf
4	JPCERT/CC (Coordination Center)	インシデントハンドリングマニュアル	セキュリティインシデント対応の基本的な流れを整理し、代表的なインシデント種別に応じた対応内容を提示。 https://www.jpcert.or.jp/csirt_material/files/manual_ver1.0_20211130.pdf
5	JPCERT/CC (Coordination Center)	組織内 CSIRT 構築支援マテリアル	組織内 CSIRT を企画・構築するために必要な情報を提供する目的で、インシデント対応体制設置の意義やメリット、事前のインシデント対応計画立案の重要性を説明。また、組織内 CSIRT の役割モデルを纏め、組織内 CSIRT 活動の定義と範囲、組織内 CSIRT の形態分類と特徴を提示。さらに、組織内 CSIRT 構築プロセスを提示。 https://www.jpcert.or.jp/csirt_material/build_phase.html

6	JPCERT/CC (Coordination Center)	コンピュータセキュリティインシデント対応チーム(CSIRT)のためのハンドブック	Carnegie Mellon University / Software Engineering Institute (CMU/SEI) “Handbook for Computer Security Incident Response Teams (CSIRTs)” の日本語翻訳。 CSIRT の基本的な枠組み(任務、顧客、位置付け)、機能・サービス、やり取りする情報、方針策定方法、品質保証方法を整理し、インシデント対応サービスの内容、組織運営の内容を提示。 https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf
7	日本ネットワークセキュリティ協会(JNSA)、日本セキュリティオペレーション事業者協議会 (ISOG-J)	セキュリティ対応組織(SOC/CSIRT)の教科書	セキュリティ対応組織の存在意義、機能、役割、体制、成熟度、及び必要な人財スキルと育成方法を提示。 https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1.pdf
8	日本セキュリティオペレーション事業者協議会 (ISOG-J)	セキュリティ対応組織(SOC/CSIRT)の教科書 ハンドブック	「セキュリティ対応組織(SOC/CSIRT)の教科書」の内容のうち、セキュリティ対応組織の役割やその成熟度モデルに関する部分を取り上げ、分かり易く纏めたもの。 https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0.pdf

3.5. 国・自治体からの要求 [6.2]

工場システムのセキュリティ対策を検討・企画する際、国・自治体からのセキュリティにかかわる要求を考慮することが必要な場合もある。

セキュリティ対策を検討するうえで、従来から前提となっている法令(労働安全基準法、環境基本法など) やガイドラインにかかわる問題が無いかを確認する必要がある。

国や自治体と、工場システムを介して情報をやり取りする場合など、相互のシステムを連携する場合に、セキュリティ要件が規定されている場合がある。

また、国や自治体が導入する製品の調達基準の中に、製品自体のセキュリティ対策要件や、製品の生産システム／工程におけるセキュリティ確保を目的とした要件が明示される場合がある。

3.6. 産業界からの要求 [6.3]

経団連は「経団連サイバーセキュリティ経営宣言」を公表し、経済界が全員参加でサイバーセキュリティ対策を推進することで、安全・安心なサイバー空間の構築に貢献することを表明するとともに、経団連「サイバーリスクハンドブック(取締役向けハンドブック)」として、取締役がセキュリティ脅威による企業経営リスクへの対処策を検討・議論する際に考慮すべき事項を整理し、サイバーリスク管理の 5 原則を示している。

【参考:業界毎の要求】

●電力業界

電力業界では、日本電気技術規格委員会(JESC)や、経済産業省の産業サイバーセキュリティ研究会 WG1 電力 SWG、ERAB(Energy Resource Aggregation Business)検討会において、電力制御システム向け、スマートメータ向け、電力小売事業者向け、ERAB(Energy Resource Aggregation Business)向けのセキュリティガイドラインが策定されたり、電力事業者から構成される電力 ISAC(Information Sharing and Analysis Center)によりセキュリティ情報収集・分析・共有が促進されたりなど、資源エネルギー庁や電気事業連合会を中心にセキュリティにかかわる取り組みが推進・要求されている。

●自動車業界

自動車業界では、自工会(日本自動車工業会)及び部工会(日本自動車部品工業会)において、自動車産業向けのセキュリティガイドラインの策定や、J-Auto-ISAC(Japan Automotive ISAC)によるセキュリティ情報収集・分析・共有の促進など、自工会/部工会を中心にセキュリティにかかわる取組みが推進・要求されている。

また、国際的には、3.4 で述べたとおり、国連の自動車基準調和世界フォーラム(WP29)において、車両のサイバーセキュリティやソフトウェア更新にかかわる規則が規定され、これらに準拠した各国の法令に従って認可を受ける必要がある。

また、CCDS(一般社団法人 重要生活機器連携セキュリティ協議会)において、車載器向けのセキュリティガイドラインが策定されている。

●医療機器業界

医療機器業界では、、国際的に、国際医療機器規制当局フォーラム(IMDRF)において、医療機器向けのサイバーセキュリティガイダンスが策定され、日本でも厚生労働省 医薬・生活衛生局から適合が要求されている。

また、、薬機法により、医療機器は JIS T14971(ISO 14971 相当)に基づくリスクマネジメントやセキュリティ対策への適合が要求されている。

●住宅業界

住宅業界では、JEITA(電子情報技術産業協会)のスマートホーム部会と、経済産業省の産業サイバーセキュリティ研究会 WG1 スマートホーム SWG において、スマートホーム向けのセキュリティガイドラインが策定され、セキュリティにかかわる取り組みが推進・要求されている。

また、CCDS(一般社団法人 重要生活機器連携セキュリティ協議会)において、スマートホーム向けのセキュリティガイドラインが策定され、スマートホーム向けガイドライン適合を検査し、認証マークを発行するプログラムの運用が開始されている。本プログラムは自己検査もしくは第三者による適合検査を求めており、適合検査結果は CCDS が管理している。

3.7. 市場・顧客からの要求 [6.4]

工場システムのセキュリティ対策を検討・企画するときに、市場・顧客からのセキュリティにかかわる要求を考慮することが必要な場合もある。

産業制御システムのセキュリティ要件にかかわる標準規格やガイドラインの規定・策定が進んでおり、このような環境の中、市場・顧客から、標準規格「IEC62443」や、サイバーセキュリティにかかわるグローバルなデファクト標準となっている米国「NIST SP800 シリーズ」、経済産業省の産業分野別セキュリティ対策ガイドラインなどへの対応が要求される場合も増えている。

このような市場・顧客からの要求は、次の3つの視点で捉えることが考えられる。

- **工場のラインに関するセキュリティ**
  取引先の製品を製造するラインや、取引先と連携するシステムに対して、具備すべきセキュリティ要件を示される場合がある。
- **情報管理や工場システムのセキュリティ管理等、企業行動に関するセキュリティ**
  企業価値を評価するポイントの一つとして、情報管理や工場システムにおけるセキュリティマネジメントが確立されているか[35]確認される場合がある。
- **製品に関するセキュリティ**
  製品内で使われているソフトウェアや部品に、セキュリティ上の問題が無いことが担保されているか確認される場合がある。

[35] 企業間の取引評価において、必要なセキュリティマネジメントが確立されていることが重要となる場合がある。

3.8. 取引先からの要求 [6.5]

工場システムのセキュリティ対策を検討・企画するときに、取引先からセキュリティ対策要求を求められる場合がある。

また、取引先から、供給する製品・部品に不正なハードウェアやソフトウェア(プログラム)が含まれることの無いように、工場の製品生産過程におけるセキュリティ対策を要求される場合もある。

3.9. 出資者からの要求 [6.6]

工場システムのセキュリティ対策を検討・企画するときに、出資者[36]からセキュリティ対策要求を求められる場合がある。

[36] 出資者からも、サイバーセキュリティリスクは企業の経営リスクのひとつとして捉えられるようになっており、有価証券報告書、内部統制報告書、CSR 報告書などに、リスク開示としてセキュリティ対策情報を記載することが要求されている。このような社会的な要請を踏まえ、総務省も、民間企業のサイバーセキュリティ対策にかかわる情報開示を促進するために、「サイバーセキュリティ対策情報開示の手引き」を策定・公表している。

付録 C　関係文書におけるセキュリティ対策レベルの考え方

3.10. セキュリティ対策レベル　[8.1]

3.10.1. 代表的なセキュリティ対策レベル評価基準　[8.1.1]

セキュリティ対策レベル評価基準の代表的なものとして、
(1)IEC 62443 におけるセキュリティレベル、
(2)NIST の「サイバーセキュリティフレームワーク」における評価基準
(3)経済産業省の「IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)」
がある。

(1)　IEC 62443

脅威がどの程度のスキルを持つ攻撃者によるものかを示す 5 つの観点から、脅威レベルを評価する。具体的には、攻撃者の悪意、攻撃手段、使用リソース、スキルレベル、動機の観点で定性的にレベル1～4として評価する。

表 3-40　IEC 62443 におけるセキュリティレベル（脅威レベル）

レベル	悪意	手段	リソース	スキル	動機
1	なし	―	―	―	―
2	あり	単純	低	汎用	低
3	あり	複雑	中	固有	中
4	あり	複雑	高	固有	高

セキュリティレベルが低い攻撃者を想定する場合は、多くの攻撃者が公知な技術を活用する、シンプルな攻撃を想定した対策とする。一方、セキュリティレベルが高い攻撃者を想定する場合は、限られた人や組織が、内部犯行も含め、高度で複雑な攻撃手法を活用する攻撃を想定した対策とする。

(2)　NIST サイバーセキュリティフレームワーク

米国 NIST(National Institute of Standards and Technology)のサイバーセキュリティフレームワークでは、マネジメントの成熟度を軸にしたレベル評価となる。低いレベルは、個々人(あるいは個別組織やプロジェクト)の裁量をベースに実施している状態を表している。高いレベルは、PDCA のマネジメントサイクルを適時実施し、サイクルの見直しを実施していることを表している。

表 3-41　NIST サイバーセキュリティフレームワークにおけるセキュリティレベル

レベル	内容	実施例
ティア1	Partial	部分的実施
ティア2	Risk Informed	リスク評価に基づき実施
ティア3	Repeatable	定期的な見直しを実施
ティア4	Adaptable	事象ごとに見直しを実施

(3)　経済産業省 IoT セキュリティ・セーフティ・フレームワーク(IoT-SSF)

経済産業省の IoT セキュリティ・セーフティ・フレームワークでは、IoT 機器・システムにおける「セキュリティ・セーフティ要求レベル」(リスク)を 2 つの軸、すなわち、「第 1 軸:発生したインシデントの影響の回復困難性の度合い」、「第 2 軸:発生したインシデントの経済的影響の度合い(金銭的価値への換算)」で表現する。

第 1 軸では、「限定的なダメージ(リカバリが容易)」「重大なダメージ(リカバリが容易ではない)」「致命的なダメージ(リカバリが困難)」の 3 レベルで表現する。

第 2 軸では、「限定的な経済影響」「重大な経済影響」「壊滅的な経済影響」の 3 レベルで表現する。

上記 2 軸を 2 次元の表にマッピングすることで、システムや機器のセキュリティ・セーフティ要求レベルを整理することができる。さらに、3次元目の軸として、社会的サポートも含めた 4 つの観点で、対策を検討する枠組を設定している。

出所)経済産業省「IoT セキュリティ・セーフティ・フレームワーク」

図 3-6 カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ

第 1 の観点:運用前(設計・製造段階等)におけるフィジカル・サイバー間をつなぐ機器・システムのセキュリティ・セーフティ確認要求

第 2 の観点:運用中のフィジカル・サイバー間をつなぐ機器・システムのセキュリティ・セーフティ確認要求

第 3 の観点:機器・システムの運用・管理を行う者の能力に関する確認要求

第 4 の観点:その他、社会的なサポート等の仕組みの要求

3.10.2. セキュリティ対策レベルの定義例 [8.1.2]

セキュリティ対策レベルは、これらの基準などを参考に、業界・個社の置かれた状況に応じ、各者にて定義することが必要である。現在の状況と、世の中の規格やガイドラインなどの状況との差を考慮しながら、実施できるようなレベルを定義することがポイントとなる。

一例として、セキュリティ施策の 3 つの観点である「システム」「運用」「マネジメント」ごとにセキュリティ対策レベルを整理をする。

(1) システムのレベル例

システムのレベルは、「どの程度のセキュリティ脅威からシステムを守ることができるか」を評価することが目的となる。以下に、設定するレベルの例を示す。各事業者で、内部での活用を想定し、最適なレベル構成としていただきたい。

表 3-42 セキュリティ要求レベルと対比し、IEC 62443 のレベルを利用した設定の例

レベル	対応する要求レベル	対策内容
1	低	セキュリティレベル 1
2	中	セキュリティレベル 2
3	高	セキュリティレベル 3

表 3-43 対象とする脅威を段階的に拡げる場合の設定例

レベル	内容
1	OA 系からの侵入を想定した対策
2	制御システムに対して外部攻撃を想定した対策
3	制御システムに関与する内部犯行を想定した対策

(2) 運用のレベル例

運用のレベルは、「OODA プロセスを円滑に実施できる状況にあるか」を評価

することが目的となる。セキュリティ攻撃が発生した時に、「いかに早く認識し的確に対処できるか」の視点で、レベルを設定する。

表 3-44 運用者のレベルに着目した設定例

問題が発生した時に対応できる能力での例

レベル	監視	判断	決定	行動
1	即時検知 (セキュリティ機器)	規定なし	規定なし	規定なし
2	即時検知 (セキュリティ機器)	運用者の教育・訓練	部門内体制整備	部門内連携整備
3	即時検知 (＋業務ふるまい異常)	判断知識蓄積・活用	意思決定体制整備	BCP 連携整備

表 3-45 複合的な項目を組み合わせた設定例

運用者のスキル、組織が持つ知識、運用者へ与える情報、運用者を支える仕掛け／仕組みの整備を複合的に組み合わせた例

レベル	スキル	知識	情報		仕掛け／仕組み	イメージ
			システム	脅威		
1	－	－	－	－	－	運用者スキルに依存
2	教育	－	障害情報	－	手順あり	手順を整理
3	訓練	訓練	セキュリティ情報	－	分析ツール整備	組織内での目標
4	総合訓練	蓄積	セキュリティ情報	入手	外部組織連携整備	国際規格準拠

(3) マネジメントのレベル例

マネジメントのレベルは、「各種情報をもとに最適な見直しを行っているか」を評価することが目的となる。以下に、設定するレベルの例を示す。各事業者で、内部での活用を想定し、最適なレベル構成としていただきたい。

表 3-46　NIST のサイバーセキュリティフレームワークのレベルを活用する例

レベル	内容
1	個人に依存し部分的に実施
2	リスク評価に基づき実施
3	定期的にリスクの変化を確認し、システム・運用等の見直しを実施
4	社内外からの情報ごとにリスクの変化を確認し、システム・運用等の 見直しを実施

表 3-47 マネジメントの成熟度を活用する例

マネジメントの成熟度として認知されている、CMMI(Capability Maturity Model Integration)を活用

レベル	内容
1	個人に依存
2	組織ごとに実施
3	組織としてルールが整備されている
4	社内外からの情報ごとにリスクの変化を確認し、システム・運用等の 見直しを実施
5	4を繰り返し実施

付録D　関連／参考資料

Edgecross コンソーシアム ／ ユーザ向けセキュリティガイドライン
FA システムを構築する際に考慮すべきセキュリティのポイントを示し、安全・安心を確保するためのガイドライン

EU NIS 指令
EU のサイバーセキュリティの水準を高めることを目的としたネットワークと情報システムのセキュリティに関するルール

EU GDPR
EU 一般データ保護規則（General Data Protection Regulation：GDPR）
欧州連合（EU）の個人情報（データ）保護という基本的人権の確保を目的とした規則

IEC 62443
IEC（国際電気標準会議、The International Electrotechnical Commission）
制御システムに関するセキュリティ標準の体系。複数のサブ標準からでき上がっており、現在も検討、標準策定が続いている。
IEC TS 62443-1-1:2009 https://webstore.iec.ch/publication/7029
IEC 62443-2-1:2010 https://webstore.iec.ch/publication/7030
IEC TR 62443-2-3:2015 https://webstore.iec.ch/publication/22811
IEC 62443-2-4:2015 https://webstore.iec.ch/publication/61335
IEC TR 62443-3-1:2009 https://webstore.iec.ch/publication/7031
IEC 62443-3-3:2013 https://webstore.iec.ch/publication/7033
IEC 62443-4-1:2018 https://webstore.iec.ch/publication/33615
IEC 62443-4-2:2019 https://webstore.iec.ch/publication/34421

ISO/SAE 21434
(自動車向け)
車のライフサイクル全般に渡るサイバーセキュリティ要件を定めたエンジニアリング規格。

NIST Cyber Security Framework (CSF)
重要インフラのサイバーセキュリティを改善するためのフレームワーク

NIST CSF （Manufacturing Profile） IR8183(？)
サイバーセキュリティ活動を管理し、製造システムに対するサイバーリスクを軽減するた

めのリスクベースのアプローチを提供

NIST SP800 シリーズ
CSD が発行するコンピュータセキュリティ関係のレポート。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書

経済産業省 ／ サイバーセキュリティ経営ガイドライン
大企業及び中小企業（小規模事業者を除く）を対象に、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するためのガイドライン

経済産業省 ／ サイバー・フィジカル・セキュリティフレームワーク
「Society 5.0」、「Connected Industries」によって拡張したサプライチェーンに求められるセキュリティへの対応指針を整理したもの

経済産業省 ／ IoT セキュリティ・セーフティ・フレームワーク ～フィジカル空間とサイバー空間のつながりの信頼性の確保～
「Society 5.0」、「Connected Industries」における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の考え方を整理したもの。

経済産業省 ／ ビル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
ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策を整理したもの。マンション等の共用スペースに対するセキュリティ対策の参考となる。

経済産業省 ／ ものづくり白書
製造基盤白書（ものづくり白書）
「ものづくり基盤技術振興基本法」第 8 条に基づく年次報告書のこと。

経済産業省 ／「機器のサイバーセキュリティ確保のための セキュリティ検証の手引き」「【別冊１】機器メーカに向けた脅威分析及びセキュリティ検証の解説書」「【別冊２】機器メーカに向けた脅威分析及びセキュリティ検証の解説書」
機器のセキュリティを検証するセキュリティ検証における、検証サービス事業者が実施すべき事項を示したもの。
別冊１は、脅威分析の具体例や効果的な検証手法等の考え方を整理するとともに、検証サービス 事業者が実施すべき事項や手法等を網羅的かつ詳細に示す。
別冊２は、IoT 機器等を開発、生産、販売するメーカを対象に、メーカが検証依頼者になる

場合に、事前対策含めて検証の知識を提供する。

情報処理推進機構（IPA）／「制御システムのセキュリティリスク分析ガイド ～セキュリティ対策におけるリスクアセスメントの実施と活用～」
リスク分析の全体像の理解を深め、リスク分析を具体的に実施するための手順や手引きを示すと共に、IPA において実践したリスク分析のノウハウを提供するもの。

一般社団法人 重要生活機器連携セキュリティ協議会（CCDS: Connected Consumer Device Security Council）／ IoT 機器セキュリティ要件ガイドライン
日常生活で利用する重要生活機器のセキュリティ技術に関する調査研究、ガイドラインの策定や認証制度の提供、標準化の検討を行う業界団体が発行し、IoT 機器に共通に適用可能なセキュリティ要件ガイドライン。

IoT 機器セキュリティ要件 対策方針チェックリスト
セキュリティ要件ガイドラインの要件準拠のための対策方針チェックリスト。

一般社団法人 重要生活機器連携セキュリティ協議会（CCDS: Connected Consumer Device Security Council）／ CCDS IoT 機器セキュリティ実装ガイドライン(ソフトウェア更新機能)
「ソフトウェア更新」の実装に具体的なセキュリティ要件を提示し、製造者がセキュアな IoT 機器を設計するうえでの指針を提供するガイドライン。

一般社団法人 重要生活機器連携セキュリティ協議会(CCDS: Connected Consumer Device Security Council）／ CCDS 製品分野別セキュリティガイドライン スマートホーム編
スマートホームホーム分野における構成要素・ライフサイクルを踏まえた具体的な対策指針とセキュリティ要件を定義するもの。

一般社団法人 重要生活機器連携セキュリティ協議会(CCDS: Connected Consumer Device Security Council）／ CCDS 製品分野別セキュリティガイドライン 車載器編
車載機器において適切なセキュリティ対策を実施するための、設計から製品リリース後までに考慮すべき設計・開発プロセスをガイドラインとしてまとめたもの。

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 ／ 工場セキュリティガイドライン 概要編
工場における FA など産業制御システム（ICS/OT）向けのセキュリティ対策の検討・実施について、製造業／工場の価値観を踏まえて整理したもの

付録Ｅ　チェックリスト

本ガイドラインに示す対策の具体化が実施できているかをイメージしていただくためのチェックリストを以下に示す。

これらの項目の達成度を「1：未実施・一部実施」、「2：実施済だが未文書化」、「3：文書化済」、「4：文書化済で適宜、改善」に応じて評価するなどして、工場セキュリティの現状をチェックしていただきたい。

付録 E-1　チェックリスト

カテゴリ	番号	確認項目	達成度	参照
組織的対策	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）または経営層が認識をもっており、十分な予算・人員配置などの協力を得られる状態にある。		3.1.1 3.1.7（参考）
	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。		3.1
	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。		3.1
	1-4	工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。		3.1
	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの情報収集を行っている。		3.1
システム関連対策	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している		3.2.2(1)
	2-2	工場システムにおける専用のセキュリティポリシが規定されていて、認知されている。		3.2.2(1)

カテゴリ	番号	確認項目	達成度	参照
	2-3	工場システムからの電子メールやインターネットアクセスはポリシによって禁止している。		3.2.2(1)
	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。		3.2.2(1)
	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。		3.2.2(1)
	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器(サーバ、クライアント端末、ネットワーク機器、設備等)の台帳を作成し、システム構成図が作成している。		3.2.2(1)
	2-7	工場内に無線 LAN を導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。		3.2.2(1)
	2-8	定期的な脆弱性診断やペネトレーションテスト(侵入可否検査)を実施して、システムへの侵入を成功させるために使用できる攻撃手法や脆弱性を特定している。		3.2.2(1)
	2-9	工場内に外部記録媒体(USB メモリ、フラッシュカード)やポータルメディアの利用・持ち込みを制限している。		3.2.2(1)
	2-10	工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。(安全に関わる緊急対応を必要とする表示器などの端末は除く)		3.2.2(1)
	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント(退職者・異動者など)を削除している。		3.2.2(1)

カテゴリ	番号	確認項目	達成度	参照
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウイルスに感染していないことを確認する手順がある。		3.2.2(1)
	2-13	システム機能の完全な復旧を想定したバックアップを行い、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。		3.2.2(1)
物理的対策	3-1	ウイルス対策がインストールできる端末にはアンチウィルスソフトまたはアプリケーションホワイトリストを導入し、インストール不可能な端末では何らかの代替策（USB 型のアンチウィルスなど）を導入している。		3.2.2(2)
	3-2	アプリケーション/オペレーティングシステム（OS）にセキュリティパッチを適用している。もしくは代替策を講じている。		3.2.2(2)
	3-3	制御端末のオペレーティングシステムやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。		3.2.2(2)
	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）。または、入退室管理、外部の入室者への関係者の付き添いなど運用面での代替策を講じている。		3.2.2
	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN 等）。		3.2.2(1)
	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（2要素認証等）やネットワーク侵入防護などの保護対策を行っている。		3.2.2(1)

カテゴリ	番号	確認項目	達成度	参照
	3-7	工場内のネットワーク(情報システムとの境界含む)の不審な通信を特定するためのネットワーク検知/防護システムを導入している。		3.2.2(1)
	3-8	工場内システムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析するか必要日数保存している。		3.2.2(1)
工場システムサプライチェーン管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダー・構築事業者と連絡・連携体制を構築している。		3.3(2)
	4-2	工場システムセキュリティのメンテナンス等、協力会社向けのセキュリティ教育を実施している。		3.3(2)
	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダー・構築業者との連絡・連携体制を構築している。		3.3(2)
	4-4	サプライチェーン(協力会社、生産子会社など)における工場システムの脅威、影響度、対応状況(監査実施など)を把握できている。		3.3(2)
	4-5	納入する工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある。		3.3(2)
	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。		3.3(2)

付録Ｆ　調達仕様書テンプレート（記載例）

セキュアな工場を構築するためには、工場で使用する製品・サービスを調達する際に、予めセキュリティに関する要件をサプライヤに提示し、そのうえで調達契約を締結することが重要である。製品・サービスの調達時に考慮すべきセキュリティ要件のカテゴリは、大きく3つに分けられる。

(1) サプライヤのセキュリティマネジメント体制
(2) 製品・サービスのセキュリティ対策
(3) 製品・サービスのライフサイクルに関わるセキュリティ対策
    ① エンジニアリング・開発時のセキュリティ対策
    ② サプライヤのサプライチェーンに関するセキュリティ対策
    ③ 製造・流通時のセキュリティ対策
    ④ 保守・サービス・廃棄に関するセキュリティ対策

このうち、(1)については、購買のベンダ登録時の審査項目として加えるような内容であり、個別の製品・サービスの調達とは別に、取引先として信用できるのかという観点である。購買で管理している与信審査の一部としてみなすことができる。この評価指標として、対象のサプライヤの規模や求める製品の重要度に応じて、「中小企業の情報セキュリティ対策ガイドライン第 3 版（IPA）」、「サイバーセキュリティ経営ガイドライン Ver2.0（経済産業省、IPA）」、「ISO/IEC 27001（情報セキュリティマネジメントシステム）」などを活用できる。

例1：制御機器サプライヤへのセキュリティ要件指定の例

X.X　サプライヤが備えるべきセキュリティ要件
「中小企業の情報セキュリティ対策ガイドライン第 3 版（IPA）」を自己評価し、SECURITY ACTION の二つ星を宣言していること。

また、(2)、(3)については、サプライヤから調達する製品・サービスの個別のセキュリティ要件である。(2)は、製品・サービスが備えるべきセキュリティ要件である。例えば、工場内で用いられる機器であれば、権限に応じたアクセス管理、ログイン認証等、達成したいセキュリティ強度に応じて、機器に必要なセキュリティ機能を列挙することになる。

例2：PLC の調達仕様書のセキュリティ要件指定の例

X.X　ペネトレーションテストの実施

　　公開されている脆弱性や攻撃手法を用いたペネトレーションテストを実施し、セキュリティリスクを低減するための対策を行うこと。

PLC のような制御機器は、セキュリティ機能を実装するだけの物理的なリソースがない場合がある。その場合、サプライヤから情報を取得して、調達する機器が満たしている要件と、追加対策が必要な要件と実装方法を明確にすることが重要である。そうすることで、リスクを把握したうえで、一時的にリスク受容するなど、柔軟な選択を行うことができる。

次に、(3)は、製品・サービスのライフサイクル関するセキュリティ要件である。これらの要件は、製品・サービスの開発、製造、流通、運用、廃棄といったライフサイクル上で発生するセキュリティリスクを低減するための要件である。調達する機器によっては、ここまでの要件を求めない場合もあるため、必要に応じて取捨選択していただきたい。

例3：PLC の製品ライフサイクルに関するセキュリティ要件指定の例

X.X　開発時のセキュリティ要件

　X.X.1　開発環境

　　X.X.1.1　開発人員の管理

　　X.X.1.2　開発環境の物理的なセキュリティ

　　X.X.1.3　開発環境のセキュリティ対策

　　X.X.1.4　開発ソフトウェア管理

X.X　使用する OSS に関するセキュリティ要件

　X.X.1　ライセンス管理の実施

　X.X.2　脆弱性管理の実施

X.X　製造・流通時のセキュリティ要件

　X.X.1　流通時のセキュリティ

　　製造拠点からどのような流通経路で納品されたかの記録を保持すること。

　　開封シールなど機器の改ざん防止の措置をとること。

X.X　保守・メンテナンス・廃棄時のセキュリティ要件

　X.X.1　バージョン変更時のファームウェア更新

　X.X.2　脆弱性発見時の対応

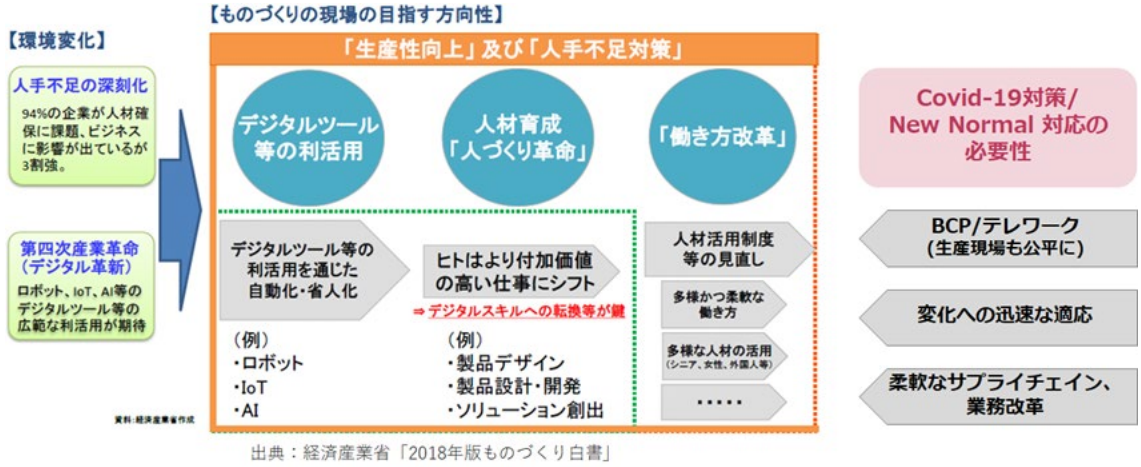
　　X.X.2.1　報告

　　X.X.2.2　対処

コラム１：工場セキュリティを巡る動向　[2]

3.11. 製造業／工場を取り巻く環境動向　[1.1.1]

製造業／工場は、常日頃から生産性向上を求められており、また、昨今の労働力不足／働き方改革への対策にも迫られている状況である。さらに、Covid-19(新型コロナウイルス感染症)対策及び New Normal (新しい常態／生活様式)への対応の必要性から、その流れが強まり、事業継続のための生産現場を含むテレワーク実現、環境変化への迅速な適応、柔軟なサプライチェーンの実現、業務改革などが求められている。



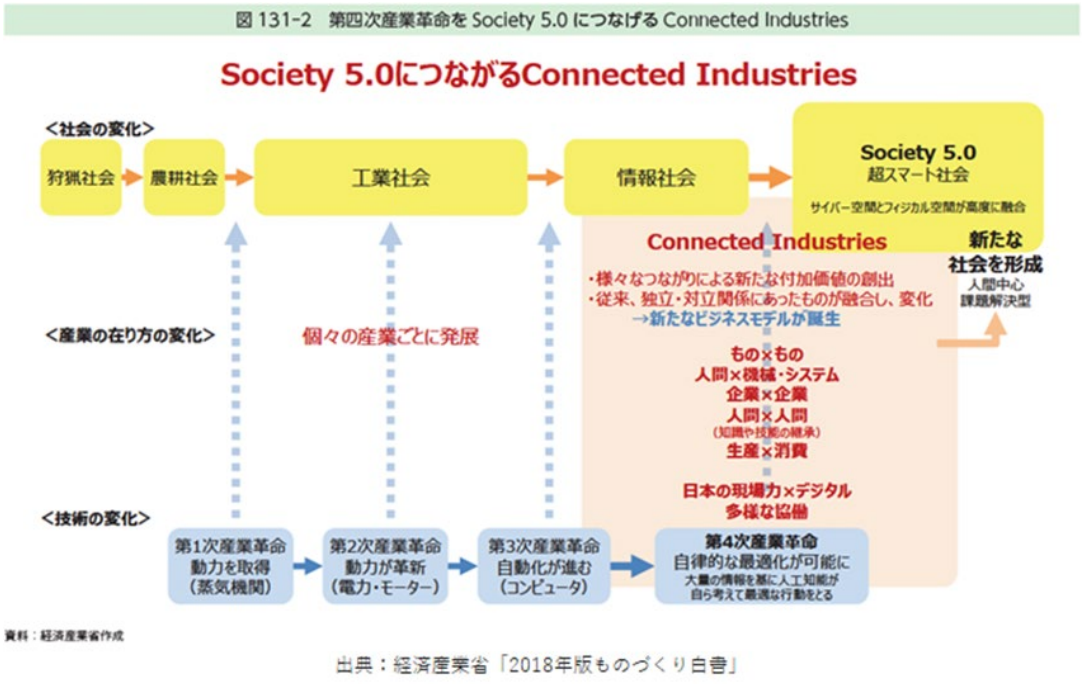
出典：経済産業省「2018年版ものづくり白書」

出所）経済産業省「2018 年版ものづくり白書」を元に作成

図 0-1　製造業／工場を取り巻く環境動向(1/4)

一方で、グローバルに第 4 次産業革命の時代となり、サイバー空間(コンピュータネットワーク)とフィジカル空間(工場現場の制御システム／機器)を融合させ、フィジカル空間から収集したビッグデータを人工知能(AI)により分析し、結果をフィジカル空間へフィードバックする、サイバーフィジカルシステム(CPS)実現の推進が、グローバル競争の視点からも必要となってきている。

サイバーフィジカルシステム(CPS)実現の例としては、生産性向上のための生産工程の自動化、製品品質向上のための検査データ分析結果フィードバックのリアルタイム化、販売／保守／アフターサービスから製品企画／設計／生産への顧客ニーズフィードバックの直接化・迅速化・精度向上、在庫最適化のための販売－生産間、生産－部材購買間での需給調整の遅延解消など、様々な目的がある。

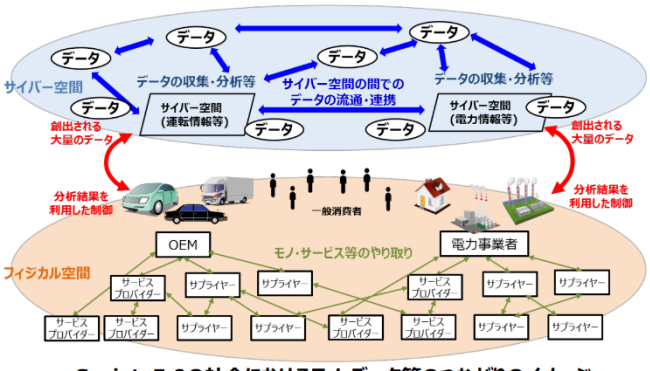


出典：経済産業省「2018年版ものづくり白書」

図　0-2　製造業／工場を取り巻く環境動向(2/4)

サイバー空間とフィジカル空間が高度に融合した「Society5.0」の到来

- 我が国では、**サイバー空間とフィジカル空間を高度に融合**させることにより、多様なニーズにきめ細かに対応したモノやサービスを提供し、経済的発展と社会的課題の解決を両立する超スマート社会**「Society5.0」**の実現を提唱。
- **「Society5.0」では、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） の形態が、より柔軟で動的なものに変化。**この**新たな形のサプライチェーンを価値創造過程（バリュークリエイションプロセス）**と定義。
- 一方で、**サイバー空間とフィジカル空間の融合により、サイバー攻撃の脅威が増大。**



Society5.0の社会におけるモノ・データ等のつながりのイメージ

大量のデータの流通・連携 ⇒データの性質に応じた管理の重要性が増大

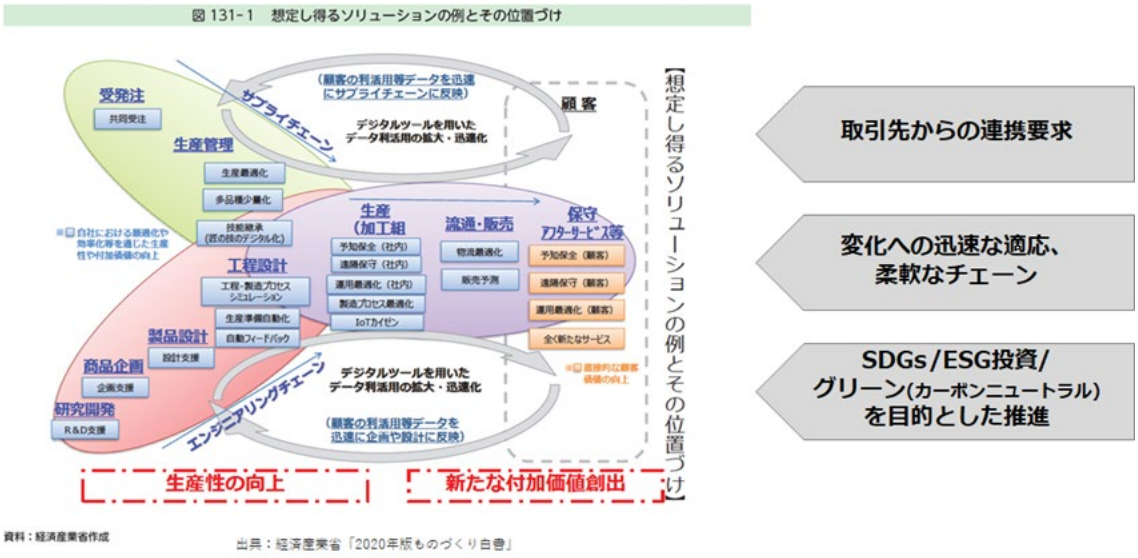
フィジカル空間とサイバー空間の融合 ⇒フィジカル空間までサイバー攻撃が到達

複雑につながるサプライチェーン ⇒影響範囲が拡大

出所）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」

図　0-3　製造業／工場を取り巻く環境動向(3/4)

このサイバー・フィジカル融合は、一つの工場内に閉じることではなく、エンジニアリングチェーン、サプライチェーン、バリューチェーンの連携まで対象とするものであり、取引先から連携が要求されたり、動的で柔軟なチェーンの実現が求められたりする。さらには、SDGs／ESG 投資／グリーン(カーボンニュートラル)を目的とした、CPS 実現やデジタルトランスフォーメーション(DX)の推進も重要になってきている。



出所）経済産業省「2018 年版ものづくり白書」を元に作成

図 0-4　製造業／工場を取り巻く環境動向(4/4)

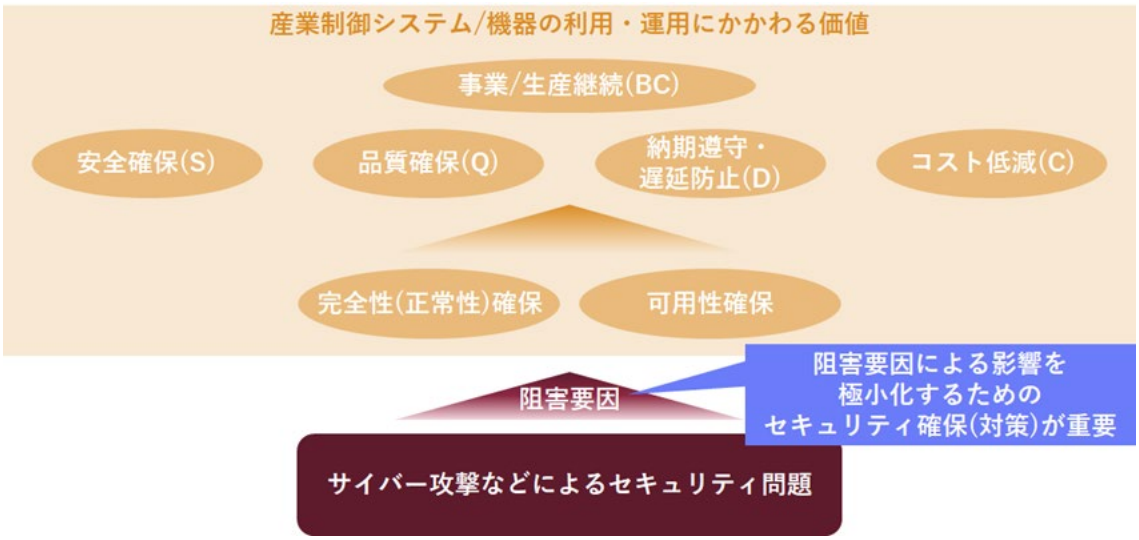
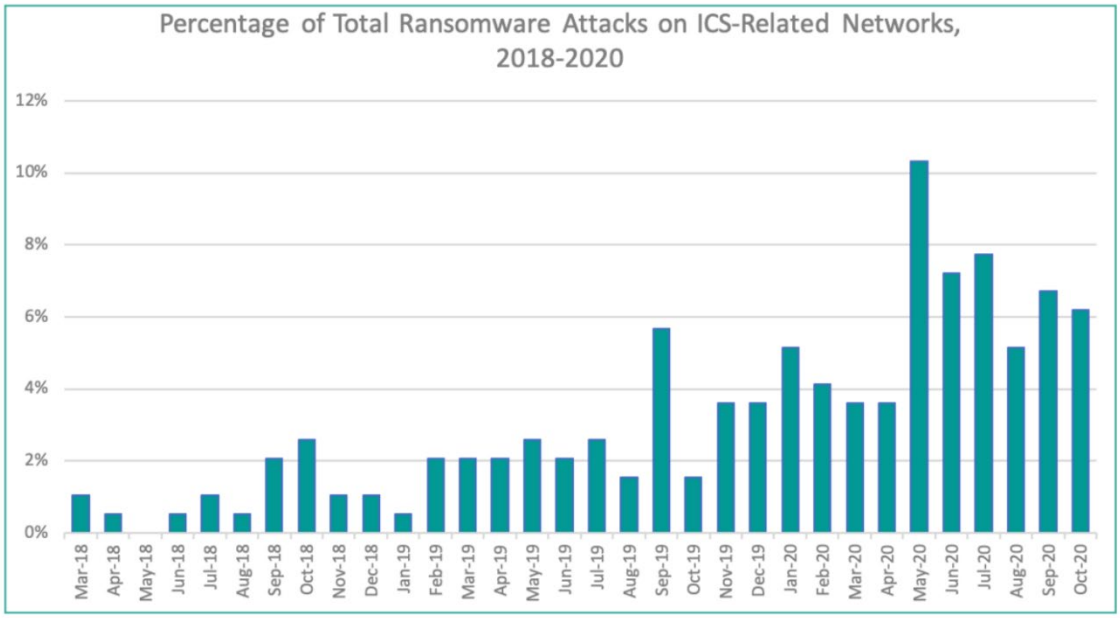


図 0-5　産業制御システム／機器のセキュリティ確保の目的（再掲）

3.12. 工場における産業制御システムのセキュリティにかかわる環境動向 [1.1.3]

工場システムのセキュリティリスクは右肩上がりに増大しており、産業制御システムを狙ったサイバー攻撃(システムのセキュリティを損なう攻撃)や、それによる生産停止／設備損壊といった重大な被害が多発している状況である。



出所）「Ransomware in ICS Environments – Dragos 2020」

図 0-6 ランサムウェアにおける制御システム関連のネットワークに対する攻撃の割合

例えば、近年流行しているランサムウェア(不正ソフトウェアの一種)により、工場の稼働停止などの被害を受けるケースが増えている。2018 年 8 月、海外の半導体製造大手企業では、工場内の PC 約 1 万台がマルウェアに感染し、操業停止に陥るとともに、約 190 億円の機会損失が発生した[37]。また、2019 年 3 月、海外のアルミニウム製造大手企業では、情報システム内にあった生産管理システムなどがランサムウェアに感染し、海外拠点を含む製造拠点が一時的に操業停止に陥り、その財務的被害は数十億円に上った[38]。このように、工場システムと情報システムの連携が深まるにつれて、サイバー攻撃の影響が工場の稼働にまで及んでいるのが実態である。

このような状況になっている要因は大きく 2 つあると考えられる。

① 工場の産業制御システム／機器が脆弱でセキュリティ対策が不足しており、サイバー攻撃を受けやすい状態になっている。

37 「制御システム関連のサイバーインシデント事例 6 ～2018 年 半導体製造企業のランサムウェアによる操業停止」（独立行政法人情報処理推進機構） https://www.ipa.go.jp/files/000085317.pdf

38 「制御システム関連のサイバーインシデント事例 5 ～2019 年 ランサムウェアによる操業停止」（独立行政法人情報処理推進機構） https://www.ipa.go.jp/files/000080702.pdf

② 攻撃者の動機が工場の産業制御システム／機器に向いている。

攻撃者は、被害者にとって攻撃による影響が重大に受けとめられるほど攻撃効果が高いと捉え、攻撃対象が脆弱なほど容易に攻撃を成功させることができ狙いやすくなるが、これらが両立するのが工場の産業制御システム／機器であると考えられる。

多くの工場では「自社の工場の産業制御システム／機器は、インターネットや社内LAN(ネットワーク)には繋がっていないから大丈夫」あるいは「外部ネットワークとは通信していないから大丈夫」と思われている。しかし、インターネットや社内 LAN などの外部ネットワークに物理的に直接繋がっていないシステム／機器であっても(あるいは外部ネットワークと通信していないシステム／機器であっても)、工場従業員やシステム／機器ベンダの保守担当者などの人間が介在することで間接的に繋がり、サイバー攻撃を受け被害が発生しているのが現実である。また、工場従業員による不正な操作や過失がセキュリティ問題を招く場合も増えている。

前述した半導体製造大手企業のランサムウェア感染の事例でも、内部の過失により持ち込んだツールのウィルススキャンがなされないまま、工場内のネットワークに接続したことにより、感染が拡大している[39]。

このように工場においてセキュリティリスクが増大している状況を踏まえ、米国や欧州を始めとして、工場の製品や製造プロセスにかかわるセキュリティ対策を要求する取引先や製品ユーザが増えてきており、その基準となる標準規格やガイドライン等が整備されつつある。

3.13. 工場における産業制御システムのセキュリティ対策実施の動向 [1.1.4]

経済産業省「2018 年版ものづくり白書」によると、工場においてセキュリティ対策の実施が進んでいない理由は、大きく 4 つの段階に分けられる。

① 中小企業を中心に、工場の産業制御システム／機器に対するセキュリティ対策の必要性を正しく認識／理解できていない段階の企業が多い。
② どのような対策が必要なのかが分からない段階の企業が多い。
③ 必要な対策を実施するためのスキルを有する人財や予算を確保できていない。
④ 実施した対策で十分なのかが分からない段階や、対策が不足していてサイバー攻撃の被害にあった場合にどうすれば良いのかが分からない。

[39] 制御システム関連のサイバーインシデント事例 6 ～2018 年 半導体製造企業のランサムウェアによる操業停止」（独立行政法人情報処理推進機構） https://www.ipa.go.jp/files/000085317.pdf

図 0-7　製造業／工場におけるセキュリティ対策の状況

コラム 2：工場システムの目的や製造業／工場の価値から観たセキュリティ [2.1.1]

(1) 工場システム自体の目的・機能、製品事業の伸張・継続、納期遵守から観たセキュリティ

工場システムは、製品事業の伸張や事業／生産の継続(BC: Business Continuity)を実現するために、生産性をより高め、コスト低減(C: Cost)を図るとともに、安定的かつ継続的に製品を生産するためのシステムであり、その安定・連続稼働が求められる。つまり、システム及び構成要素の可用性確保(Availability)が求められる。これは、納期遵守・遅延防止(D: Delivery)のためにも必要である。セキュリティ脅威には可用性を損なうものがあり、それを防止／抑制するためのセキュリティ対策が必要である。言い換えると、セキュリティ脅威により、製品事業の伸張・継続(BC)や、納期遵守・遅延防止(D)、コスト低減(C)が妨げられることを防止／抑制するために、セキュリティ対策が必要ということである。

(2) 工場の安全確保、製品の品質確保から観たセキュリティ

工場の安全確保(S: Safety)や、製品の品質確保(Q: Quality)を実現するために、工場システム及び機器が正常に動作する状態を保つことが求められる。つまり、システム及び機器の機能・制御の正常性[完全性]確保(Integrity)が求められる。セキュリティ脅威には機能・制御の正常性[完全性]を損なうものがあり、それを防止／抑制するためのセキュリティ対策が必要である。言い換えると、セキュリティ脅威により、工場の安全確保(S)や、製品の品質確保(Q)が妨げられることを防止／抑制するために、セキュリティ対策が必要ということである。

(3) 工場システムの正常動作確保や適正なフィードバック制御から観たセキュリティ

工場システム及び機器が正常に動作する状態を保つためには、システム及び機器の機能・制御の仕方を設定・指示するデータが正しいこと、すなわちデータが壊れたり改ざんされたりしていないことが求められる。つまり、システム及び機器の機能・制御にかかわる設定・指示データの正常性[完全性]確保が求められる。また、工場システム及び機器の制御・稼働・運用の最適化・自動化・自律化を図る目的で、システム及び機器の稼働状態に応じたフィードバック制御を実現するために、システム及び機器の稼働状態にかかわるデータを収集・分析・監視し、その時点の状態に基づき、システム及び機器の機能・制御の仕方にかかわる設定・指示を変更していく運用の実現が必要になっている。このループを正しく回すためには、システム及び機器から収集するデータが正しいこと、すなわちデータが壊れたり改ざんされたりしていないことが求められ

る。つまり、システム及び機器から収集するデータの正常性[完全性]確保が求められる。セキュリティ脅威にはデータの正常性[完全性]を損なうものがあり、それを防止／抑制するためのセキュリティ対策が必要である。言い換えると、セキュリティ脅威により、工場システム及び機器の正常動作確保や、適正なフィードバック制御の実現を妨げられることを防止／抑制するために、セキュリティ対策が必要ということである。

(4)　製品や生産にかかわる情報やデータの保護から観たセキュリティ

製品事業にとって、競合他社による自社製品の優位点の模倣を防ぎ、差異及び競争優位性を確保することは重要であり、製品や生産(ノウハウ)にかかわる情報やデータが外部に漏えいしないようにすることが求められる。

つまり、製品や生産にかかわる情報やデータの機密性確保(Confidentiality)が求められる。セキュリティ脅威にはデータの機密性を損なうものがあり、それを防止／抑制するためのセキュリティ対策が必要である。

言い換えると、セキュリティ脅威による、製品や生産(ノウハウ)にかかわる情報やデータの外部漏えいを防止／抑制するために、セキュリティ対策が必要ということである。

(5)　製品のセキュリティ品質確保や製造責任から観たセキュリティ

最近は、工場における製品の生産過程で、製品の部品として用いられるハードウェアやソフトウェア(プログラム)の中に、セキュリティ脅威を内包する不正なものが意図せず含まれてしまうことがあり、製品出荷後に製品内包のセキュリティ脅威により、製品が外部から不正に利用・制御されたり、製品の稼働を妨害されたり、製品利用者の情報を外部へ漏えいさせたりする問題を引き起こすことが発生する。製品の製造責任を問われることの無いように、製品の品質確保(Q)の位置づけで、このような不正なハードウェアやソフトウェア(プログラム)の部品が含まれることの無いように、工場の製品生産過程でセキュリティ対策を取ることが求められる。つまり、製品の部品に悪意のある機能(マルウェア)が含まれていないことや、部品の正常性[完全性]確保や真正性確保(Authenticity)が求められる。セキュリティ脅威には製品及び部品の正常性[完全性]や真正性を損なうものがあり、それを防止／抑制するためのセキュリティ対策が必要である。言い換えると、意図せず製品の部品に内包されたセキュリティ脅威により、製品が外部から不正に利用・制御されたり、製品の稼働を妨害されたり、製品利用者の情報を外部へ漏えいされたりすることで、製品の製造責任を問われることを防止／抑制するために、セキュリティ対策が必要ということである。

コラム 3：スマート工場への流れ

工場システムは今後さらなる進展を目指し、最新の ICT(情報通信)技術やロボットなどの自動化技術を活用した、ライン・設備の改善や各種システムとの連携や、機器に対するリモート監視・制御や生産管理システムとの連携するニーズが高まっており、工場システムが情報システムやインターネットと接続する機会が増えている一方で、リスクも新たに発生している。

そこで、利用形態の 4 つの流れと、それぞれのセキュリティリスクにかかわる考慮すべき点を説明する。

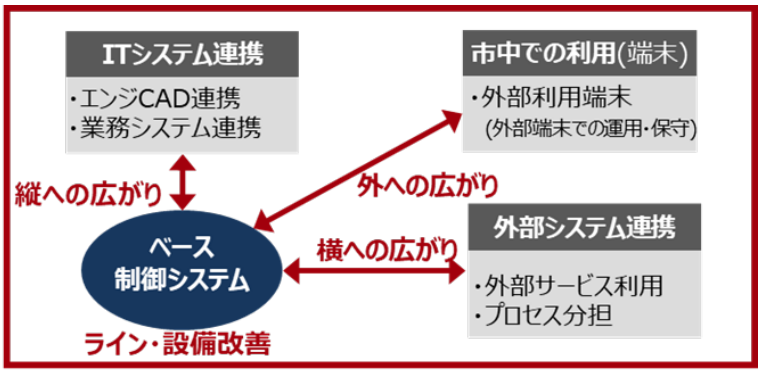


図 0-8　FA 制御システム利用形態の拡がり

(1)　ライン・設備改善

ラインの自由度向上や生産改革のために、ロボットや自動装置の導入を行う。

ロボットや自動装置は、装置内に計算機が内蔵されていることが多く、さらに、無線 LAN などのオープンな無線通信技術を活用し外部接続することが多くなり、新たなリスクが考えられる。

表 0-1　ライン・設備改善に伴うリスクの例

考慮が必要な事象	リスク
装置内に計算機を内蔵	・計算機と同等のリスクあり
無線 LAN などを利用し外部と連携	・外部ネットワーク接続のリスク拡大

(2)　IT システム連携（縦への拡がり）

現場データに基づく生産改革などを目的に、エンジニアリング部門の分析システムと連携する形態。また、分析結果に基づき、工場システムの改善を行う。

表 0-2　IT システム連携に伴うリスクの例

考慮が必要な事象	リスク
FA システムと OA システムのネットワークが接続	・OA システムと FA システムの間のセキュリティ対策の差異による相互リスク拡大
FA システムのデータが OA システムに存在	・システム利用者管理が異なることによる、情報改ざん／漏えいリスク拡大

(3)　市中での利用（外への拡がり）

リモートアクセスやモバイル端末により現場機器に接続し、工場システムの監視・制御や保守を実施する形態。

表 0-3 市中での利用に伴うリスクの例

考慮が必要な事象	リスク
外部ネットワークを介した接続	・外部ネットワークからの攻撃
外部にある機器の利用	・利用機器の管理が不十分 ・利用者管理が不十分

(4)　外部システム連携（横への拡がり）

他社(他事業所)の生産ラインと連携を取り、他社を含めた統合的な工場システムの構築・連携を行う。

表 0-4 外部システム連携に伴うリスクの例

考慮が必要な事象	リスク
異なるセキュリティポリシ	・許容リスクが異なることによる攻撃等の可能性
セキュリティ攻撃による影響があった場合の対応	・セキュリティ運用(OODA プロセス)の円滑な連携が困難 ・責任範囲が不明確

本ガイドラインの検討体制

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)
工場サブワーキンググループ　構成員一覧

※敬称略、五十音順

	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
座長	江崎 浩	東京大学大学院 情報理工学系研究科教授
	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株式会社　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

謝辞

本ガイドラインは、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、および「工場セキュリティガイドライン 概要編」の内容を参考に作成しました。多大なるご協力に感謝いたします。