2022/10/11

工場セキュリティガイドライン

概要編

1.00 版

2022 年 10 月 11 日

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

ECD-TE4-0009-01-JA

改版履歴

版	発行日	改版概要
1.00	2022 年 10 月 11 日	初版

読者の皆様へのメッセージ

東京大学 グリーン ICT プロジェクト 代表 江崎 浩

Industry 4.0[1]、Society 5.0[2]において、IT／ICT(情報通信技術)システムだけではなく、OT(産業制御・運用技術)システムと呼ばれる工場、交通インフラ、あるいは電力インフラなど、これまでデジタル化さらにはオンライン化が推進されていなかった産業領域におけるシステムのデジタル化・オンライン化の必要性が提言されてきましたが、実ビジネス領域における実展開は、そのサイバーセキュリティ対策を含め、なかなか進展していませんでした。しかし、近年は、それまでの売名行為的なサイバー攻撃が、商業行為的なサイバー攻撃に変化し、さらにテロ行為や、リアルとサイバーのハイブリッドのシステム破壊を含む戦闘行為へと進展、ロシアのウクライナ侵攻はこれを急加速させることになっています。その結果、海外展開している日本企業の工場施設等におけるサイバー被害のみならず、国内の工場施設等におけるサイバーインシデント(事件・事故)が急増・激増するに至っています。このような、世界の経済活動だけではなく、日本の経済活動を停滞・減速、さらには崩壊させる可能性をもつサイバーセキュリティ攻撃への対応策は、経済安全保障における重要な国家施策の位置づけとなりつつあります。従来の IT／ICT 領域ではない OT 領域におけるサイバーセキュリティ対策の重要性は経済産業省において強く認識されており、「産業サイバーセキュリティ研究会」が産業構造審議会に設置され、工場施設などに関するサイバーセキュリティ施策の議論が行われてきました。

---

[1] Industry 4.0 とは、ドイツが 2011 年に打ち出した「第 4 次産業革命」を意味する技術概念で、水力・蒸気機関を活用した機械製造設備が導入された第 1 次産業革命、石油と電力を活用した大量生産が始まった第 2 次産業革命、IT 技術を活用した生産自動化が始まった第 3 次産業革命に続く歴史的な変化として位置付けられている。AI(人工知能)や IoT(モノのインターネット接続)といった高度な IT 技術を活用し、生産自動化のさらなる自律的な最適化が可能になることで、製造業の変革を目指すもの。

[2] Society 5.0 とは、日本が提唱している未来社会の概念で、サイバー空間(仮想空間)とフィジカル空間(現実空間)を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会(Society)を意味するもの。

[参照：https://www8.cao.go.jp/cstp/society5_0/]

Edgecross コンソーシアムおよび GUTP(東京大学グリーン ICT プロジェクト)は、スマートビルやスマート工場の実現を推進するために設立された産官学のコンソーシアムであり、当然、スマートビルやスマート工場のデジタル化とオンライン化よる生産性向上の推進が主目的ですが、スマートシステムの実現には、その構成要素のデジタル化・オンライン化が行われることになり、必然的に十分なサイバーセキュリティ対策が必要となります。Edgecross コンソーシアムと GUTP が連携して、スマート工場におけるサイバーセキュリティ対策にかかわる最低限のガイドライン策定の必要性が関係者で認識され、ガイドライン作成の活動が 2020 年 9 月に始動しました。本活動は、経済産業省 産業サイバーセキュリティ研究会において、その必要性が認識され、経済産業省としてのガイドラインの重要参照ドキュメントと位置づけられ、公的位置づけをもった工場におけるサイバーセキュリティ対策のガイドラインとして公開されるに至りました。本ガイドラインは、組み立て工場を参照工場としており、今後は、本ガイドラインを参照しつつ、PA(Plant Automation)、自動車産業、半導体工場など、重要産業の工場施設に関するサイバーセキュリティ対策ガイドラインが策定される方向にあります。

本ガイドラインが、皆様の施設のデジタル化・オンラン化による生産性の向上と進化を、安全・安心に実現することに貢献することを期待しています。

Edgecross コンソーシアム テクニカル部会 会長 市岡 裕嗣

昔はクローズシステムであった工場内の FA(Factory Automation)システムは、近年では、オープン化、IT システム連携、IoT 技術活用が進み、セキュリティリスクが高まってきています。現に、FA システムへのサイバー攻撃により、生産に多大な影響を与えるようなニュースを頻繁に聞くようになってきており、FA システムのセキュリティに対する関心が高まってきています。

こうしたリスク(脅威)から FA システムを含めた工場全体を守るためには、物理面、システム面、運用管理面、維持改善面などで、多重・多面的なセキュリティ対策によりサイバー攻撃を受けにくくし、仮に攻撃を受けたとしても影響を低減する必要があります。

このような考えの下、工場セキュリティ WG に参画いただいた有識者の方々の知験を持ち寄って本ガイドラインを作成しました。本書が皆様の FA システムのセキュリティ対策の考え方を理解する助けとなることを期待いたします。

目次

1. はじめに

本セキュリティガイドラインは、工場におけるファクトリー・オートメーション(FA)など産業制御システム(ICS/OT)向けのセキュリティ対策が、製造業／工場の価値観から必要であり重要であることを説明するとともに、セキュリティ対策をどのように検討し実施するのが良いかを整理したものです。

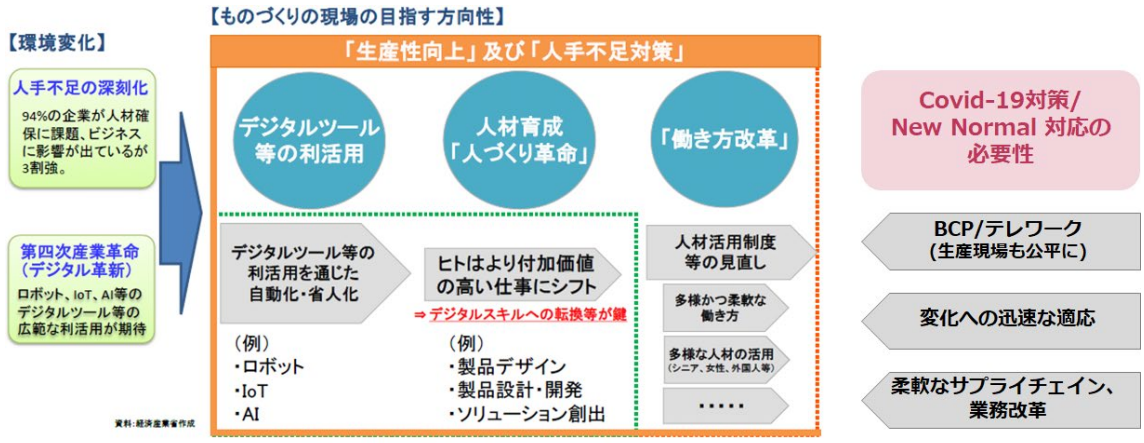
本章では、まず本ガイドラインの背景と目的、想定読者、対象範囲と位置付け、全体の構成と概要、読み方、基本的な方針と考え方を示します。

1.1. 背景、目的

本節では、本ガイドラインの背景と目的を示します。

1.1.1. 製造業／工場を取り巻く環境動向

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す。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ます。



出典：経済産業省「2018年版ものづくり白書」

図 1-1 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ます。

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、様々な目的があります。

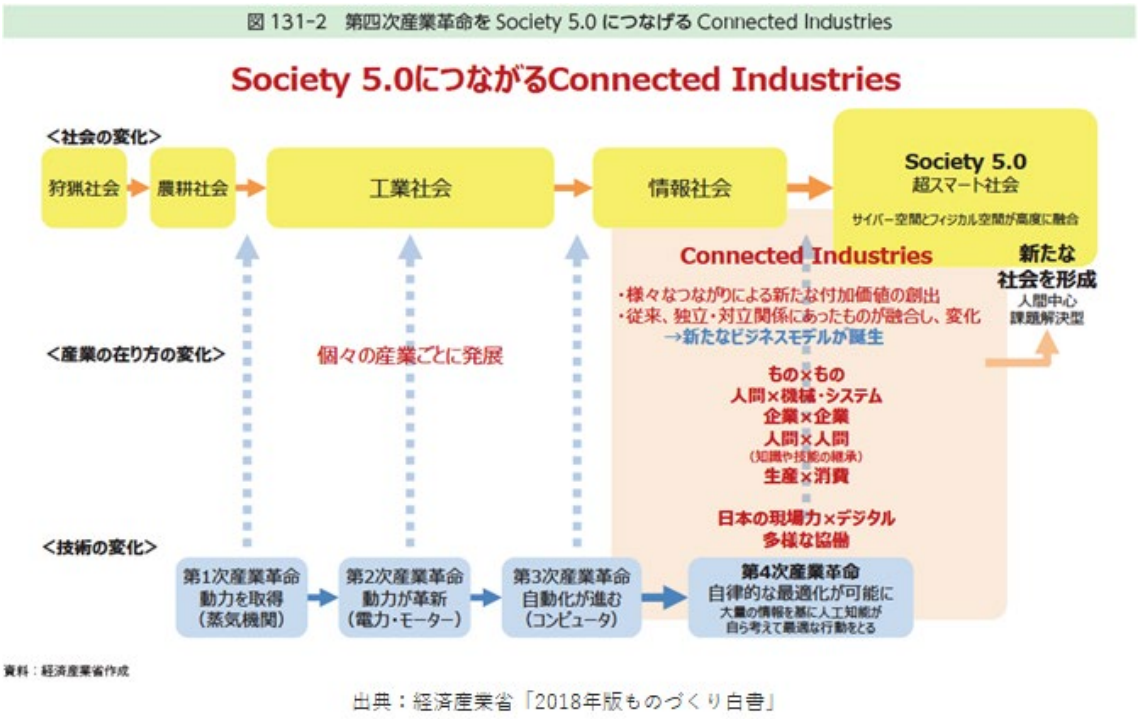


図 1-2 製造業／工場を取り巻く環境動向(2/4)

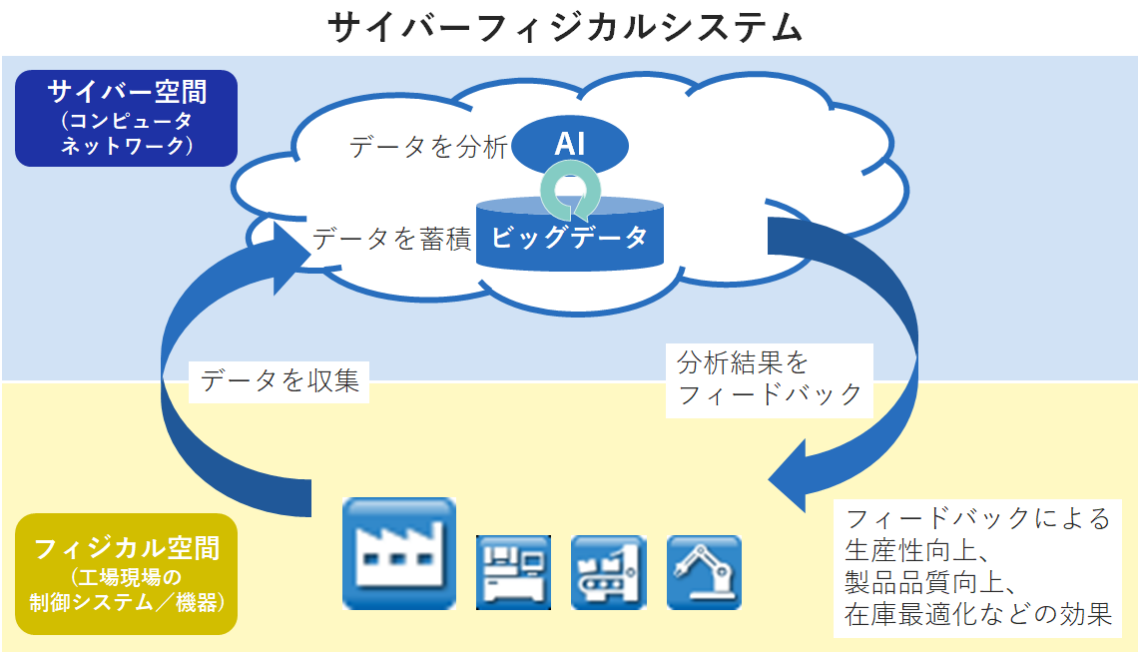


図 1-3 製造業／工場を取り巻く環境動向(3/4)

このサイバー・フィジカル融合の推進は、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します。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ます。

サイバー・フィジカル融合／DX 推進の対象・目的

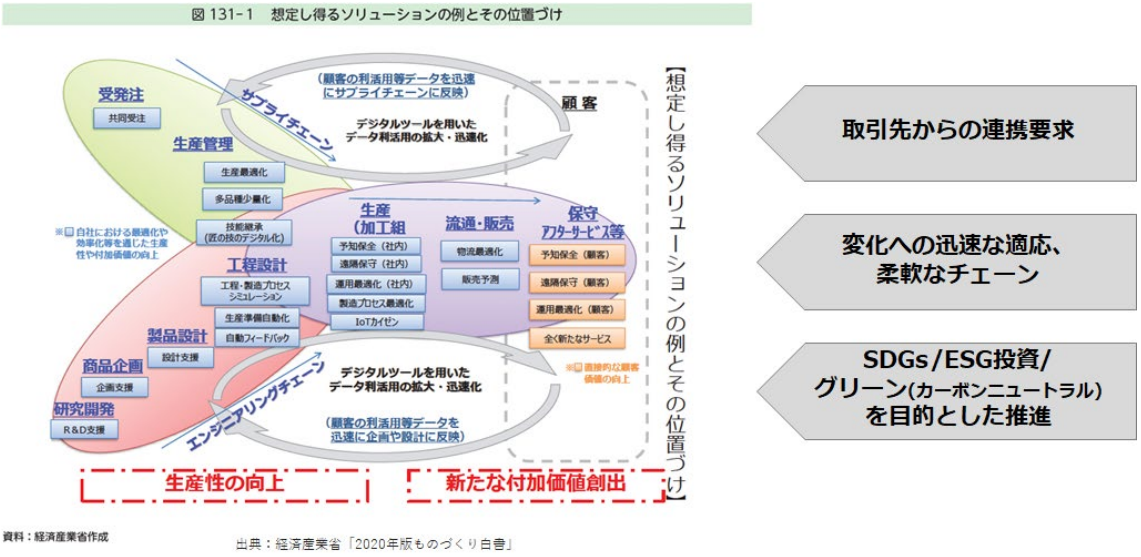


図 1-4 製造業／工場を取り巻く環境動向(4/4)

1.1.2. 工場における産業制御システムのセキュリティ確保の重要性

前節で述べた、工場の産業制御システムに対する CPS 実現や DX を推進するためには、併せてセキュリティを確保することも重要です。セキュリティを確保できていなければ、工場の産業制御システムの完全性(正常性)や可用性が損なわれるリスクが高くなり、ひいては、その安全確保(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)、及び事業／生産継続(BC: Business Continuity)といった、工場にとって極めて重要な価値を損なうことに繋がるからです。また他にも、製品や生産(ノウハウ)にかかわる情報やデータなど、営業秘密の漏えいを招くリスクも高くなり、競争優位性を損なうことにも繋がります。

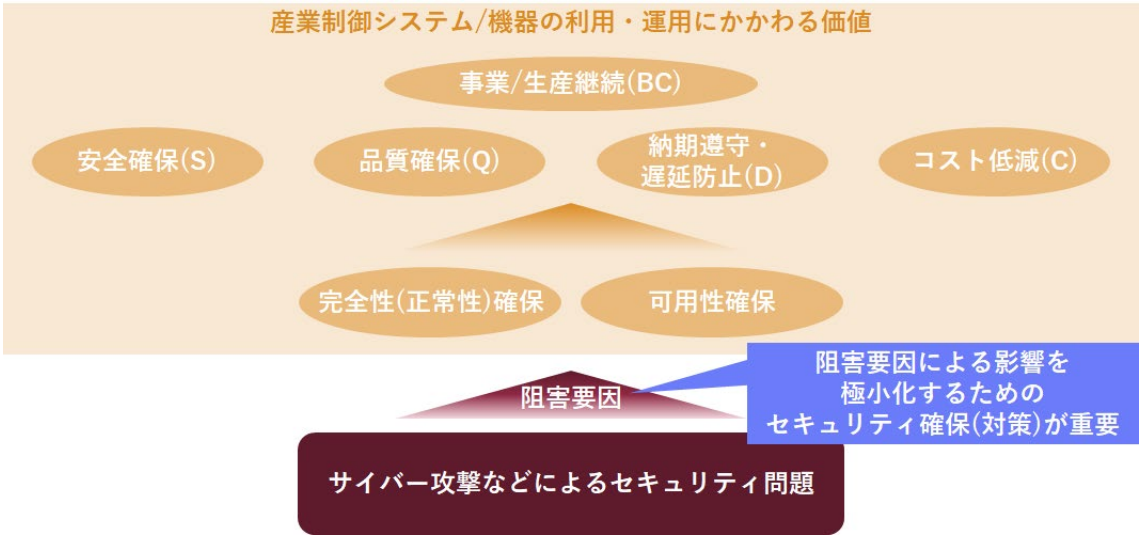


図 1-5 産業制御システム／機器のセキュリティ確保の主な目的

1.1.3. 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

工場の産業制御システムのセキュリティ確保が重要な一方で、残念ながら、そのセキュリティリスクは 2010 年頃から増大しており、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[3]です。

なぜ、このような状況になっているのでしょうか？その要因は大きく 2 つの切り口に分けられます。1 つは、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こと。もう 1 つは、攻撃者の動機が工場の産業制御システム／機器に向いていることです。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易くなる訳ですが、これらが両立するのが工場の産業制御システム／機器ということです。

---

[3] 産業制御システムに対するサイバー攻撃による被害事例は、IPA「制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ」を参照。

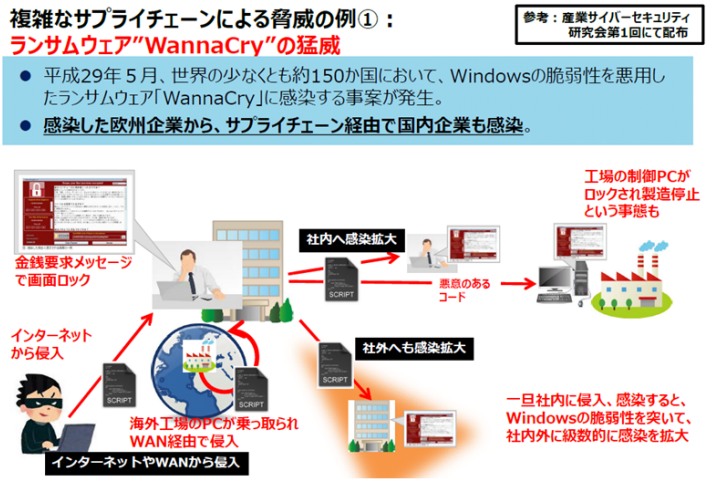
https://www.ipa.go.jp/security/controlsystem/incident.html

ここで、読者の中には、「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だ」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だ」と思っている方もいるのではないでしょうか？本当に大丈夫でしょうか？　残念ながら、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が媒介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す。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ます。

また、工場の産業制御システムの脆弱性を捉えるときには、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含め捉えることが必要な場合があります。昨今の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・侵入する事例も増えており、注意が必要です。

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	標的型攻撃による機密情報の窃取
3	テレワーク等の ニューノーマルな働き方を狙った攻撃
4	サプライチェーンの弱点を悪用した攻撃
5	ビジネスメール詐欺による金銭被害
6	内部不正による情報漏えい
7	予期せぬIT基盤の障害に伴う業務停止
8	インターネット上のサービスへの不正ログイン
9	不注意による情報漏えい等の被害
10	脆弱性対策情報の公開に伴う悪用増加

出典：IPA「情報セキュリティ10大脅威2021」



出典：経済産業省　産業サイバーセキュリティ研究会資料

図 1-6　サプライチェーンの連携先を踏み台にしたサイバー攻撃の増大

このように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セキュリティガイドラインが整備されつつあります。今後、日本の製造業／工場も海外の取引先やユーザを始めとする要求に応じることが必須となり、国内でも法規制や業界標準などの要求が定められていくと見られます。

1.1.4. 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

前節で述べた環境動向に応じて、日本の製造業／工場における産業制御システム／機器のセキュリティ対策は十分に実施できているのでしょうか？　残念ながら未だ甚だ不足しており、サイバー攻撃による重大な被害が多発しているのが実状です。

なぜ、セキュリティ対策の実施は進んでいないのでしょうか？　経済産業省「2018 年版ものづくり白書」によると、その要因は大きく 4 つの段階の課題を抱えていることによるものです。1 つ目は、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ことです。2 つ目は、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ことです。3 つ目は、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段階の企業が多いことです。4 つ目は、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遭った場合にどうすれば良いのかが分からない段階です。

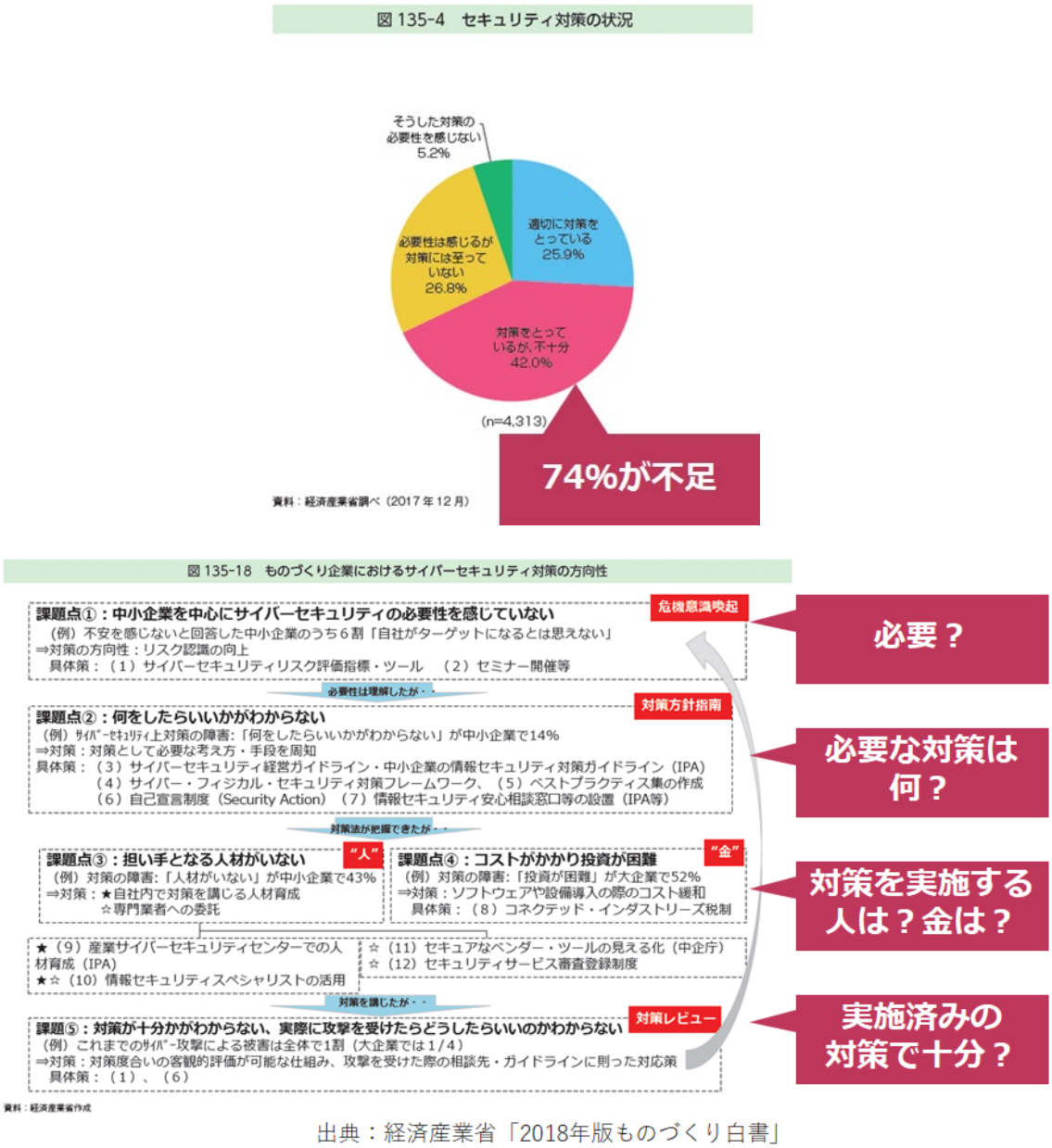


図 1-7 製造業／工場におけるセキュリティ対策の状況

また、製造業／工場が重視する価値は、事業／生産継続(BC)が第一であり、それを支える安全確保(S)、品質確保(Q)、納期遵守・遅延防止(D)、コスト低減(C)という価値の優先度が高いため、これらを損なうリスクを招くことは積極的に実施できないということも、忘れてはいけない点です。セキュリティ対策の導入・適用は、このリスクを招くものとして捉えられており、この点もセキュリティ対策実施の障壁となっています。

このような日本の製造業／工場の状況・課題や価値観を踏まえ、セキュリティ対策実施を無理なく促進していく必要があります。

1.1.5. 工場セキュリティガイドラインの目的

本セキュリティガイドラインは、前述のような諸々の動向や、工場における産業制御システムのセキュリティ確保の重要性を踏まえ、**製造業／工場における産業制御システム／機器のセキュリティ対策実施を促進**する一助となることを目指し、**①セキュリティ対策の必要性や危機意識の啓発、②対策方法の解説、③アウトソースという選択肢の提示**といった目的で、内容を検討／整理したものです。

①セキュリティ対策の必要性や危機意識の啓発の中では、製造業／工場の価値観から必要であり重要であることを説明します。

また、②対策方法の解説の中では、製造業／工場の価値観を踏まえ、セキュリティ対策実施を無理なく推進するために、どのような進め方が合っているかも提示します。

また、③アウトソースという選択肢の提示の中では、セキュリティ専門ベンダが提供する、対策実施を支援するサービスや対策実現に必要な製品として、どのようなものがあるかを紹介します。

さらに、工場の産業制御システム／機器及びセキュリティの調達要件を作成する人にとって、**調達要件モデルとして活用**できるものになることを目指しています。

1.2. 想定読者

本ガイドラインの読者としては、以下に挙げる方々を想定しています。

- 産業制御システム利用者
  - 生産技術部門、生産管理部門、工作部門など
- 同システム利用者の経営層(投資承認者)
- 同システム及びセキュリティの調達要件を作成する人
  - 調達対象機器に対する要件を含む
- 同システムのセキュリティ／リスク管理の関係者
  - 全社のリスク管理部門、情報システム部門など
- 同システムの構築者、管理者、運用者、保守者
- 同システム提供ベンダ、機器ベンダ／メーカ

1.3. 対象範囲、位置付け

本節では、本ガイドラインの対象範囲と位置付けを示します。

本ガイドラインは、**工場におけるファクトリー・オートメーション(FA)などの産業制御システム(ICS/OT)を対象とし、そのセキュリティ対策が製造業／工場の価値観から必要であり重要であることを説明**するとともに、**セキュリティ要件及び対策にかかわる推奨を提示**するガイドラインの基本・概要編です。必要最低限の要件や一般的な要件に焦点を当てた内容を提示しています。

新設システム／機器だけを対象にするのではなく、既存システム／機器のセキュリティ対策を向上させるためにはどうすれば良いかを含め、提示します。また、セキュリティ対策を適用できない既存の古い機器から、新しい機器へ置き換える動機付けとなる内容や、古い機器を継続利用せざるをえない場合に、どのように対処すれば良いかを併せて提示します。

既存の一般的なセキュリティガイドラインの内容を参照／流用しながら、**FA などの産業制御システムに特有の部分に焦点を当てた内容**としています。

なお、2 章以降では FA システムの場合を例に論じていますが、FA システム以外の産業制御システムが対象の場合は、適宜読み替えてください。

因みに、本ガイドラインの内容は、経済産業省の「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」(2022 年 11 月に第 1 版発行予定)の主要な構成内容として採用されています。経済産業省のガイドライン側では、本ガイドラインの 5.1～5.2 節で提示するセキュリティ対策の内容に焦点を絞った構成となっています。今後は必要に応じて随時、両書の内容の整合を取っていく予定です。

1.4. 全体構成、概要、読み方

本節では、本ガイドラインの全体構成と概要、及び読み方ガイドを示します。

本ガイドラインの全体構成は、以下に示すとおりです。

- 1 章：はじめに
- 2 章：工場 FA システムのセキュリティ対策の考え方
- 3 章：対象とする FA システムの全体像／基本構成
- 4 章：対象 FA システムのセキュリティ保護対象と脅威・影響
- 5 章：セキュリティ対策の全体像
- 6 章：中小企業の工場におけるセキュリティ対策の考え方
- 7 章：参考
- 付録 1：チェックリスト
- 付録 2：調達仕様書テンプレート(記載例)
- 付録 3：関連／参考資料
- 付録 4：用語／略語
- 別冊：取り組み事例

1 章にて、まず、本ガイドラインの背景と目的、対象範囲と位置付け、基本的な方針と考え方などを示します。

2 章にて、産業制御システムの代表例として工場 FA システムを取り上げ、そのセキュリティ対策をどのように考えれば良いのか、その考え方や論理全体の流れを先に把握してもらう位置づけで、製造業／工場が重視する価値軸：BC／SQDC などの視点と対応づけながら、セキュリティ対策の目的・機能を示し、3～5 章で提示する、対策検討・企画に必要な要素が何か、及び各種要素に基づき対策を考え出す方法(論理)を説明します。

セキュリティ対策の目的としては、BC／SQDC の確保に加え、法規制・標準規格・ガイドライン準拠への対応や各種ステークホルダからの要求といった環境要件、社会的セキュリティ要件も整理しています。

3 章にて、典型的な工場 FA システムのモデル／ユースケースを設定し、4 章にて、保護対象、想定脅威、リスク／影響度を整理します。製造業／工場の事業／業務にとって重要な価値軸：BC／SQDC に対して、セキュリティリスクがどのような影響を及ぼすのかを結びつけ、リスク対応の優先度を整理します。

5 章にて、工場 FA システムのセキュリティ対策の全体像を提示します。物理面、システム構成面の技術的防御策(ネットワーク、機器)、運用・管理面(OODA)、維持・改善面(PDCA)、サプライチェーン面に分け、FA システムのライフサイクル全体にわたるセキュリティ対策の概要を整理します。また、必要最低限の基本的な対策から始め、FA システムの DX 推進に応じ段階的にレベルを向上させていく進め方を提示します。

その際に、FA システムを利用する企業／工場だけで、必要なセキュリティ対策を実現するのは困難な場合があり、FA システム及び機器の提供ベンダ／メーカに対して、必要なセキュリティ対策を要求すべきであることを指摘します。また、必要なセキュリティ対策を実施するためのスキルを有する人財や体制を確保できない場合には、対策実施を支援するサービスや対策実現に必要な製品を提供するセキュリティベンダへアウトソーシングするという選択肢があることを紹介します。

6 章にて、中小企業の工場におけるセキュリティ対策の考え方の補足を提示します。

7 章にて、参考として、業界／製品分野ごとのセキュリティ法規制、セキュリティの標準規格／ガイドライン、各種ステークホルダからのセキュリティ要求、セキュリティ対策レベル、インシデント対応ガイドなどにかかわる補足を提示します。

末尾に付録として、ガイドラインの内容に基づくチェックシート、及び調達仕様書のテンプレート(記載例)、関連／参考資料、用語／略語の説明、図表目次を提供します。

また、別冊として、取り組み事例を提示します。

本ガイドラインの読み方

想定読者ごと、あるいは目的ごとの参照推奨箇所を示します。

想定読者それぞれの立場で**特に**読んでいただきたい部分は、以下の表に示すとおりです。

表 1-1 想定読者ごとの参照推奨箇所

想定読者 / 参照推奨箇所	産業制御システムの**利用者、セキュリティ／リスク管理者**	同利用者の**経営層**(投資承認者)	同システム及びセキュリティの**調達要件作成者**	同システムの**構築者**	同システムの**管理者、運用者、保守者**	同システムの**提供ベンダ、機器ベンダ／メーカ**	**中小企業**工場の同システム利用者、及び経営層
1 章	○		○				
1.1 節		◎					◎
2 章	◎		◎	○	○	○	
2.1 節		◎					◎
3 章	○		○	○	○		
4 章	◎		◎	○	○	○	
5 章	○		○	○	○		
5.1 節	◎						
5.1.2 節		◎					◎
5.2.1 節	◎		◎	◎	◎	◎	◎
5.2.2 節				◎			
5.2.3 節				◎		○	
5.2.3.2 節						◎	
5.2.4 節					◎		
5.2.5 節			◎				
5.3.3 節	◎		◎				◎
5.4 節	◎		◎	◎			◎
5.5 節	◎		◎	◎	◎	◎	◎

想定読者 / 参照推奨箇所	産業制御システムの**利用者、セキュリティ／リスク管理者**	同利用者の**経営層**(投資承認者)	同システム及びセキュリティの**調達要件作成者**	同システムの**構築者**	同システムの**管理者、運用者、保守者**	同システムの**提供ベンダ、機器ベンダ／メーカ**	**中小企業**工場の同システム利用者、及び経営層
6 章							◎
7 章	○		○				
7.1 節	◎	○	◎				○
7.2 節			◎				
7.3 節	◎	○	◎				○
7.5 節					○		
8.1 節	◎		◎				○
8.2 節			◎				

また、読者が本ガイドラインを参照する目的がどのような場合に、どの部分を読めば良いかを以下の表に整理します。

表 1-2 目的ごとの参照推奨箇所

目的（知りたいこと、課題）	参照推奨箇所
[why] なぜセキュリティ対策が必要なのか？重要なのか？	
● 製造業／工場を取り巻く**環境動向** [生産性向上、労働力不足／働き方改革、Covid-19 対策／New Normal 対応、第 4 次産業革命、サイバーフィジカルシステム実現など]	1.1.1
● 製造業／工場の価値から観た**セキュリティ対策の必要性・重要性** [事業／生産継続(BC)、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)など]	1.1.2, 2.1.1,
● **セキュリティ脅威・影響**の状況	1.1.3, 2.1.2.1, 4.2
● 工場や製品のセキュリティにかかわる**法規制** [国内、海外]	2.1.2.2, 7.1
● 工場や製品の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** [国際標準、海外、国内、業界]	2.1.2.3, 7.2
● **各種ステークホルダ**からのセキュリティにかかわる**要求** [国・自治体、業界、市場・顧客、取引先、出資者など]	2.1.2.4, 7.3
[what] どのようなセキュリティ対策が必要なのか？	
● 工場や製品のセキュリティにかかわる**標準規格／ガイドライン** [国際標準、海外、国内、業界]	2.1.2.3, 7.2
● 工場におけるセキュリティの**保護対象**及び**重要度**	3 章, 4.1
● 想定される**セキュリティ脅威・影響**	4.2
● **想定脅威ごと**の具体的なセキュリティ**対策**	5.2.1

目的（知りたいこと、課題）	参照推奨箇所
● **物理面**での具体的なセキュリティ**対策**	5.2.2
● **システム構成面**での具体的なセキュリティ**対策**	5.2.3
● **運用・管理面**での具体的なセキュリティ**対策** [プロセス、組織体制・要員を含む]	5.2.4.1
● **維持・改善面**での具体的なセキュリティ**対策** [プロセス、組織体制・要員を含む]	5.2.4.2
● **サプライチェーン面**での具体的なセキュリティ**対策**	5.2.5
● **必要最低限のセキュリティ対策**としては、 どのような対策から実施すれば良いのか？	5.3.3
● **実施済みのセキュリティ対策で不足は無いのか？** [セキュリティ対策・リスク状況のアセスメントや脆弱性診断を実施する アウトソースサービスの活用という選択肢を含む]	2 章, 4 章, 5 章, 5.5 節
[how] どのようにセキュリティ対策の企画・導入を進めれば良いのか？	
● **対策検討・企画の考え方** [目的・機能、必要性、リスクアセスメントの考え方／進め方を含む]	2 章
● **対策企画・導入の進め方**の全体概要 [経営層による取り組みの宣言を含む]	5.1
● **スマート工場の実現に向けた**セキュリティ対策導入の**進め方**	5.3
● **対策の段階的な向上の進め方** [どのような対策から始めれば良いのか？]	5.3.3
● **FA システム及び機器の提供ベンダ／メーカへの対策要求** [FA システム及び機器のセキュリティ対策は、利用者による実現が困難…]	5.4
● **セキュリティベンダが提供するサービス／製品の活用** (アウトソースという選択肢) [セキュリティ対策を実施するためのスキルを有する人財や体制を 確保できない…]	5.5

目的（知りたいこと、課題）	参照推奨箇所
その他の便利な資料・情報	
● **中小企業の工場**におけるセキュリティ対策の考え方	6 章
● セキュリティ対策レベルにかかわる補足 [①IEC 62443、②NIST サイバーセキュリティフレームワーク、 ③IoT セキュリティ・セーフティ・フレームワークなど]	7.4
● **インシデント対応ガイドライン**にかかわる補足 [セキュリティの問題が発生した場合に、どのように対応すれば良いのか？ 事前にどのような準備をしておく必要があるのか？]	7.5
● **チェックリスト**	8.1
● **調達仕様書テンプレート(記載例)**	8.2
● **取り組み事例**	別冊
● 関連／参考資料	8.3
● 用語／略語	8.4
● 図表目次	8.5

1.5. 基本的な方針、考え方

本節では、本ガイドラインの基本的な方針と考え方を示します。

前述のとおり、製造業／工場が重視する価値は、事業／生産継続(BC)が第一であり、それを支える安全確保(S)、品質確保(Q)、納期遵守・遅延防止(D)、コスト低減(C)という価値の優先度が高いため、これらを損なうリスクを招くことは積極的に実施できない状況に置かれています。セキュリティ対策の導入・適用は、このリスクを招くものとして捉えられており、この点を踏まえてセキュリティ対策の必要性、内容、進め方を論じることが肝要です。

そこで、製造業／工場の事業／業務にとって重要な価値軸：BC／SQDC に対して、セキュリティリスクがどのような影響を及ぼすのかを結びつけ、リスク対応の優先度を整理した上で、必要最低限あるいは一般的なセキュリティ対策の基本は何か、及び BC／SQDC へ影響を及ぼすリスクを避けることを配慮した対策導入・適用の進め方を論じています。

また、システム構成面の技術的防御策(ネットワーク、機器における対策)だけではなく、物理面、運用・管理面(OODA)、維持・改善面(PDCA)、サプライチェーン面も併せ、ライフサイクル全体やプロセス全体にわたる対策を実施する必要があることや、必要最低限の基本的な対策から始め、産業制御システムの DX 推進に応じ段階的にレベルを向上させていく進め方を推奨しています。

2. 工場 FA システムのセキュリティ対策の考え方

本章では、工場における産業制御システムの代表例として工場 FA システムを取り上げ、そのセキュリティ対策を検討・企画するにあたり、まず、FA システムのセキュリティ対策がどのような目的・機能を果たすのかを示します。そして、セキュリティ対策の検討・企画に必要な要素が何かを示し、これらの要素に基づきセキュリティ対策を考え出す方法(論理)を説明します。

2.1. セキュリティ対策の目的・機能、必要性

FA システムのセキュリティ対策は、どのような目的・機能を果たすものなのでしょうか？それを定義するためには、まず、FA システム自体の目的・機能が何か、及び製造業／工場が重視する価値が何かに立ち返る必要があります。

2.1.1. FA 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

FA 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

FA 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ます。つまり、システム及び構成要素の可用性(Availability)確保が求められるわけです。これは、納期遵守・遅延防止(D: Delivery)のためにも必要です。

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す。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す。

工場の安全確保、製品の品質確保から観たセキュリティ

また、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、FA 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ます。つまり、システム及び機器の機能・制御の完全性(Integrity)[すなわち正常性]を確保することが求められるわけです。

セキュリティ脅威には機能・制御の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す。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す。

FA 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

また、FA 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ます。つまり、システム及び機器の機能・制御にかかわる設定・指示データの完全性[正常性]確保が求められるわけです。

また、FA 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きています。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ます。つまり、システム及び機器から収集するデータの完全性[正常性]確保が求められるわけです。

セキュリティ脅威にはデータの完全性[正常性]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す。言い換えると、セキュリティ脅威により、FA 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す。

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

さらに、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ます。つまり、製品や生産にかかわる情報やデータの機密性(Confidentiality)確保が求められるわけです。

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す。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す。

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

そのうえ最近は、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しています。

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ます。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、部品の完全性[正常性]確保や真正性(Authenticity)確保が求められるわけです。

セキュリティ脅威には製品及び部品の完全性[正常性]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す。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す。

2.1.2. 外部からのセキュリティにかかわる社会的な要求

前節では、FA システム自体の目的・機能や、製造業／工場自らの重視する価値である製品事業伸張・継続、及び SQDC という視点から、FA システムのセキュリティ対策の必要性・重要性を述べてきましたが、FA システムのセキュリティ対策の目的を定義するときには、それに関して、製造業／工場の外部(外部環境、社会、各種ステークホルダ)からどのような要求があるかを併せて考慮に入れる必要があります。

本節では、FA システムを取り巻く外部からの社会的なセキュリティ要求として、どのようなものがあるかを示します。

FA システムが置かれている厳しいセキュリティ環境を認識するとともに、セキュリティにかかわる法規制・標準規格・ガイドライン準拠や、各種ステークホルダからの要求などを想定する必要があります。

2.1.2.1 セキュリティ脅威・影響の拡大

まず、外部環境の面では、1.1.3 節でも述べたとおり、工場の FA 産業制御システムのセキュリティリスクは増大しており、産業制御システムを狙ったサイバー攻撃や、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[4]です。

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ます。2018 年 8 月、台湾半導体製造大手の TSMC 社では、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ました。

また、2019 年 3 月、ノルウェーのアルミニウム製造大手のノルスク・ハイドロ社では、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りました。

---

[4] 産業制御システムに対するサイバー攻撃による被害事例は、IPA「制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ」を参照。

https://www.ipa.go.jp/security/controlsystem/incident.html

このように、FA 産業制御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す。

2.1.2.2 法規制によるセキュリティ対策の要求

セキュリティリスクの増大による製造業／工場や製品への影響の重大さを踏まえ、製造業／工場や製品に対して、セキュリティ対策を要求する社会的な動向も増えてきています。その一つとして、グローバルに法規制への対応が求められるようになってきています。

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** [5]や**忠実義務** [6]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** [7]や第三者に対する**損害賠償責任** [8]を問われる可能性があります。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ります。

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」が発生しています。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します。

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ます。

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ます。

---

[5] 会社法 330 条、民法 644 条
[6] 会社法 355 条
[7] 会社法 423 条 1 項
[8] 会社法 429 条 1 項

2022 年 6 月に新たに決定された「**重要インフラのサイバーセキュリティ対策に係る行動計画**」では、組織統治の一部としてサイバーセキュリティを組み入れ、経営層を含む組織全体での取り組みを推進すること、及び経営陣主導の体制整備や対処計画づくりを求めるとともに、サプライチェーンで使用する機器／サービスの安全確保も求めることが明記されています。また、重要インフラ関連事業者がサプライチェーン全体としてサイバーセキュリティの確保に努める責務を有する旨や、重要インフラサービス障害等に対する経営層の責任が明記されています。

また、工場で生産する製品のセキュリティにかかわる法規制として、インターネットに接続する端末などの機器(IoT 機器)に対しては、「**電気通信事業法** [9]及び**端末設備等規則** [10]」により、技術基準として満たすべきセキュリティ対策要件が規定されており、技術基準適合認定(いわゆる「**技適**」)を受けていることが電気通信事業者から義務付けられています。

国際的にも、業界／製品分野別にセキュリティ対策にかかわる法規制が進んでいます。業界／製品分野ごとのセキュリティにかかわる法規制の詳細な内容は、7.1 節に整理してありますので、参照してください。

[9] 電気通信事業法 52 条 1 項

[10] 端末設備等規則 34 条の 10

2.1.2.3 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

製造業／工場や製品に対してセキュリティ対策を要求する社会的な動向として、グローバルにセキュリティの標準規格／ガイドラインへの準拠も求められるようになってきています。

前節で述べたような法規制の基準として活用されたり、通常必要と考えられるセキュリティ対策の水準を示したりするものが、セキュリティ対策にかかわる標準規格やガイドラインです。

FA 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れば良いのかを検討する必要があります。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などがあり、さらに取引先が規定している要件などもあります。

これらのガイドラインの多くは、次の視点で記載されています。

・経営者の責任

・セキュリティマネジメントに基づく安全・安心な状態の維持

・セキュリティ攻撃や被害にあった場合の的確な行動

工場のセキュリティにかかわる代表的な標準規格／ガイドラインとして、とりわけ以下に挙げるようなものがよく参照されています。

（1）国際標準規格

・**IEC 62443**：産業自動化・制御システムの運用・管理プロセス面から、システムおよび構成要素の技術面まで、全体のサイバー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／電子システム及び製品の機能安全を規定

（2）海外の規格・ガイドライン

A) 米国

・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す。

「識別－防御－検知－対応－復旧」のプロセスに分類して提示しています。

・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ります。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ります。

B) 欧州(EU)

・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す。

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ます。

（3）国内の方針・ガイドライン

日本国内でも、政府や業界などから、各種の方針やガイドラインが発行されています。

・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

・経済産業省

－サイバーセキュリティ経営ガイドライン

－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)

－IoT セキュリティ・セーフティ・フレームワーク（IoT-SSF)

－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]

－制御システム　セーフティ・セキュリティ要件検討ガイド [同上]

なお、上記以外のものを含め、セキュリティにかかわる代表的な標準規格／ガイドラインは、7.2 節に詳しく整理してありますので、参照してください。

2.1.2.4 各種ステークホルダからのセキュリティ対策の要求

FA システムのセキュリティ対策を検討・企画するときに、製造業／工場を取り巻く各種ステークホルダ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ります。ステークホルダとしては、国・自治体、業界、市場・顧客、取引先、出資者などが想定されます。

要求される内容は、各種ステークホルダごとに異なりますが、前節で紹介した法規制、標準規格、ガイドライン準拠にかかわる内容に加え、国家・経済安全保障の一環としての対策、業界として連携したセキュリティ情報収集・分析・共有の促進、顧客からの調達要件、サプライチェーンリスク対策、有価証券報告書などにおけるリスク情報／セキュリティ対策情報の開示など、様々な側面で要求されることが増えています。

また、経営課題と捉え、経営層を始めとした企業全体としての取り組みが求められる内容となっています。

各種ステークホルダごとのセキュリティ要求にかかわる、より詳細な内容は、7.3 節に整理してありますので、参照していただき、企業の価値や対応能力を高めるための経営課題として取り組んでいただく必要があります。

2.1.3. セキュリティ対策の目的・機能のまとめ

上記をまとめると、FA システムのセキュリティ対策の目的・機能は、製造業／工場の経営にとって重要な、産業制御システムのセキュリティにかかわる諸々の社会的なセキュリティ要求に応えるとともに、セキュリティ脅威により生じる、以下に挙げる問題を防止／抑制することです。

- 製品事業の伸張や事業／生産の継続(BC: Business Continuity)を妨げられることの防止／抑制
- 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) を妨げられることの防止／抑制
- FA 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を妨げられることの防止／抑制
- 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の防止／抑制
- 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拡大の防止／抑制
- 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の防止／抑制
- 製品の製造責任を問われることを防止／抑制

これらを実現するためには、FA 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)、完全性(Integrity)[すなわち正常性]、真正性(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す。[11]

[11] これらのセキュリティ要素を確保するためには、さらに、システムの信頼性(Reliability)、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(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ります。

製造業／工場の経営にとって重要な、FA 産業制御システムのセキュリティにかかわる諸々の社会的なセキュリティ要求に応えるという目的とともに、FA システムにおける上記 SQDC の確保及び製品事業の伸張・継続を阻害し、生産業務停止・遅延を発生させる要因の一つとして、セキュリティ脅威を位置付け、セキュリティ対策を検討する必要があります。

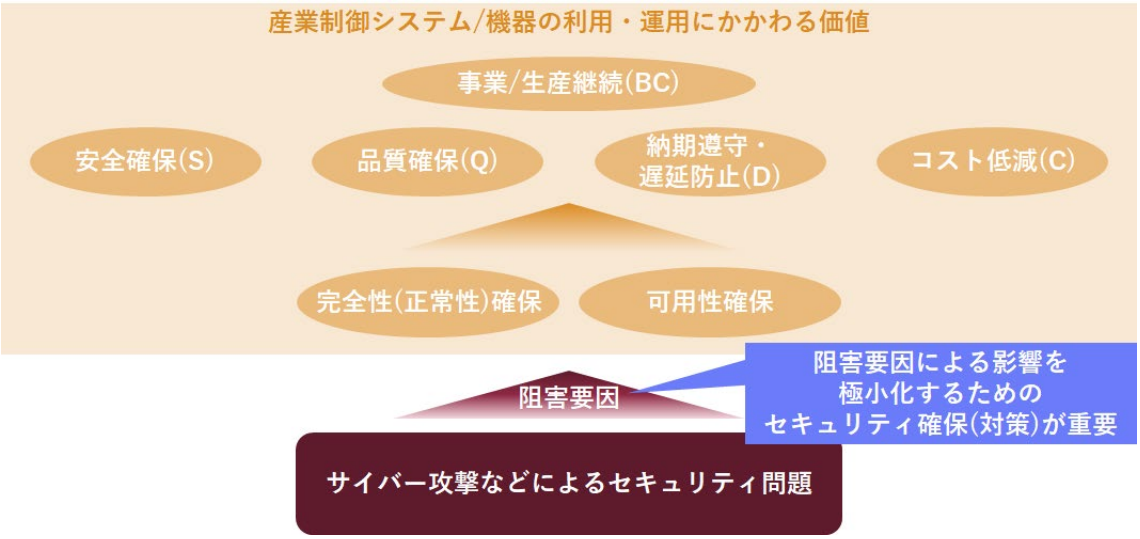


図 2-1 産業制御システム／機器のセキュリティ確保の主な目的（再掲）

2.2. セキュリティ対策検討・企画に必要な要素

本節では、セキュリティ対策の検討・企画に必要な要素が何かを示します。

①社会的なセキュリティ要件

セキュリティ対策を検討・企画するためには、第一に、社会的にどのようなセキュリティ対策を要求されているのかを考慮する必要があります。セキュリティにかかわる法規制・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、出資者からの要求などが想定されます。

②企業内部のセキュリティ要件

第二に、企業内部の要件や状況を考慮する必要があります。企業方針(ポリシ／ルール)、事業伸張・継続(BC)や投資対効果の視点、リスクマネジメントの視点、セキュリティ対策を運用・管理する体制・能力の視点などから、必要性や優先度、対策導入の順序や段階を考慮する必要があります。

③セキュリティ保護対象、及びその重要度／優先度

第三に、対象とする FA システムにおけるセキュリティの保護対象が何かを特定する必要があります。これはまず、セキュリティ対策を強化すべき業務と、当該業務を支援／実施する FA システムの構成要素(ネットワーク、機器、機能・プログラム、データ)を洗い出すことから始まります。[12]

[12] より細かくは、前節で述べたとおり、構成要素それぞれの可用性(Availability)、完全性(Integrity)、機密性(Confidentiality)、真正性(Authenticity)、信頼性(Reliability)、責任追跡性(Accountability)、否認防止(Non-Repudiation)といったセキュリティ要素のうち、どの要素を確保する必要があるのかを明確にします。

さらに、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／優先度を明確にする必要があります。

この際に、保護対象をゾーンやセグメントという単位にまとめ、その単位で重要度／優先度を大まかに整理するやり方もあるでしょう。

④セキュリティ脅威、及びそれを受ける可能性［脅威レベル］

第四に、保護対象それぞれに対して、どのようなセキュリティ脅威が想定されるのかを洗い出す必要があります。脅威の種別としては、以下に挙げるようなものがあります。[13]

- 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

なお、これらの脅威は、保護対象それぞれがどのような環境に置かれているか、そして、どのようなセキュリティ対策が既に施されているかにより、脅威を受ける可能性が変わるため、保護対象の状態に応じた脅威受難の可能性の高低を併せて想定しておく必要があります。なお、本ガイドラインでは、この想定脅威を受ける可能性(高低)のことを、「脅威レベル」と呼びます。

---

[13] 脅威の種別をより細かく挙げると、保護対象それぞれ(システムを構成する機器、機能・プログラム、データ)の可用性(Availability)、完全性(Integrity)、機密性(Confidentiality)、真正性(Authenticity)、信頼性(Reliability)、責任追跡性(Accountability)、否認防止(Non-Repudiation)というセキュリティ要素を損なうものがあり、主な種別としては、なりすまし(Spoofing)、改ざん(Tampering)、否認(Repudiation)、情報漏えい(Information Disclosure)、サービス妨害(Denial of Service)、権限昇格(Elevation of Privilege)、不正アクセス、踏み台攻撃利用などの種別があります。

⑤セキュリティ脅威による影響(影響度)、及びその発現の可能性

[セキュリティリスク]

第五に、保護対象それぞれにおいて、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を明確にする必要があります。そして、その影響が発現する可能性を併せて想定しておく必要があります。これにより、対象とする FA システムの保護対象それぞれの「セキュリティリスク」を想定できることになります。

2.3. セキュリティ対策検討・企画の考え方

本節では、前節で示した五つの要素に基づき、対象とする FA システムのセキュリティ対策を検討・企画するときの考え方(論理)を説明します。

アプローチの仕方は幾つかあり、これが正しい考え方だと一つに決まっているわけではありませんが、企業や工場の状況に応じた選択肢として、主なものを以下に提示します。

アプローチ例 1：外部からのセキュリティ対策にかかわる要求から入る考え方

工場の FA システムのセキュリティ対策に関して、企業／工場の外部(外部環境、社会、各種ステークホルダ)からどのような要求があるかを、第一に意識する入り方のアプローチを採る場合があります。

外部からの要求がセキュリティ対策要件として明確かつ具体的に示されている場合は、このアプローチを採る方が、必要なセキュリティ対策の企画・検討を効率的に進められるかもしれません。

このアプローチでは、まず、2.2 節で示した要素①「社会的要件」として、セキュリティにかかわるどのような法規制・標準規格・ガイドラインに準拠する必要があるのか、及び国・自治体、業界、市場・顧客、取引先、出資者などの各種ステークホルダからのどのような要求を満たす必要があるのかを、明確かつできるだけ具体的に整理し、それを満たすセキュリティ対策を企画・検討することになります。

それと併せて、要素②「企業内部要件」として、企業方針(ポリシ／ルール)、事業伸張・継続(BC)や投資対効果の視点、リスクマネジメントの視点、セキュリティ対策を運用・管理する体制・能力の視点などから、セキュリティ対策にかかわるどのような要件を満たす必要があるのかを整理します。これらの要件に基づき、各種セキュリティ対策の必要性や優先度、対策導入の順序や段階などを検討することになります。

これら要素①「社会的要件」及び要素②「企業内部要件」による、セキュリティ対策にかかわる“環境要件”を踏まえた上で、その要件を意識しながら、2.2 節で示した要素③「保護対象及びその重要度／優先度」の洗い出し・特定を進め、保護対象のゾーンやセグメントに対して、あるいはその構成要素それぞれに対して、要素④「脅威及びそれを受ける可能性[脅威レベル]」を想定します。

そして、これら要素③と要素④とを掛け合わせることにより、要素⑤「保護対象が被る脅威による影響(影響度)及びその発現の可能性」(すなわち「セキュリティリスク」)を導出することができます。

この要素⑤が、対象とする FA システムのどの保護対象において、どのような脅威に対するセキュリティ対策が必要なのかの基本的な必要度／優先度を示していることになりますが、それに応じて必要なセキュリティ対策を実際に導入するか否か、そして導入の順序や段階をどうするかの決定は、あらためて上記の“環境要件”を踏まえ、総合的に判断することになります。

アプローチ例 2：企業や工場の重視する価値軸の重要度／優先度から入る考え方

工場の FA システム自体の目的・機能や、企業／工場自らの重視する価値である製品事業伸張・継続、SQDC の視点を第一に意識する入り方のアプローチを採る場合があります。

2.2 節で示した要素①「社会的要件」及び要素②「企業内部要件」といった、セキュリティ対策にかかわる“環境要件”が不明確である(具体的ではない)場合は、このアプローチを採るのが良いでしょう。

あるいは、工場の FA システム自体の目的・機能、製品事業伸張・継続、SQDC という価値軸をとりわけ重視し、その視点から、セキュリティ対策の保護対象となる FA システムの構成要素それぞれの重要度／優先度を分類し、それに応じ、導入するセキュリティ対策のメリハリを付けることを優先させたい場合は、このアプローチを採るのが良いでしょう。

このアプローチでは、まず、2.2 節で示した要素③「保護対象及びその重要度／優先度」の洗い出し・特定を進めることになります。その中で、工場の FA システム自体の目的・機能、製品事業伸張・継続、SQDC という価値軸の視点、及びそれに応じた業務の重要性という視点から、FA システムの構成要素(保護対象)を、業務の重要度／優先度に応じたゾーンやセグメントに分けて整理します。場合によっては、必要に応じ、より細かく保護対象の構成要素それぞれの重要度／優先度を明確にします。

この保護対象のゾーンやセグメントに対して、あるいはその構成要素それぞれに対して、要素④「脅威及びそれを受ける可能性［脅威レベル］」を想定します。

そして、これら要素③と要素④「脅威及びそれを受ける可能性［脅威レベル］」を掛け合わせることにより、要素⑤「保護対象が被る脅威による影響(影響度)及びその発現の可能性」(すなわち「セキュリティリスク」)を導出することができます。

この要素⑤が、対象とする FA システムのどの保護対象において、どのような脅威に対するセキュリティ対策が必要なのかの基本的な必要度／優先度を示していることになりますが、それに応じて必要なセキュリティ対策を実際に導入するか否か、そして導入の順序や段階をどうするかの決定は、要素①「社会的要件」及び要素②「企業内部要件」を踏まえ、総合的に判断することになります。

アプローチ例 3：工場全体のセキュリティ対策レベルの底上げから入る考え方

工場の FA システム全体が以下のような状況である場合は、FA システム全体をひとまとまりに捉え、まずは全体として最低限必要なセキュリティ対策を実施することで、全体の底上げを図る入り方をするアプローチを採る場合があります。

- FA システム全体として、セキュリティ対策があまり実施できておらず、まずは全体の底上げが必要な状況である場合、
- 企業／工場が重視する価値軸の視点から、FA システム全体を重要度／優先度に応じたゾーンやセグメントに分けられていない、分けることが難しい、あるいは分ける必要が無く、FA システム全体を分け隔てなくひとまとまりに捉えられる状況である場合

この場合、2.2 節で示した、要素③「保護対象及びその重要度／優先度」の洗い出し・特定を実施する手間は省け、業務の重要度／優先度に応じたゾーン分けやセグメント分割の実施は省けますが、重要度／優先度に応じたメリハリを付けられなくなる点は認識しておく必要があります。

このアプローチでは、FA システム全体をひとまとまりの保護対象として、要素④「脅威及びそれを受ける可能性 [脅威レベル]」を想定し、要素⑤「保護対象が被る脅威による影響(影響度)及びその発現の可能性」(すなわち「セキュリティリスク」)を導出することになります。

このセキュリティリスクを踏まえ、FA システム全体として最低限必要なセキュリティ対策を検討・企画することになりますが、その一方で、最低限必要なセキュリティ対策は、要素①「社会的要件」及び要素②「企業内部要件」から観ても不足していないものにする必要があります。要素①「社会的要件」及び要素②「企業内部要件」から、セキュリティ対策にかかわる最低限の要件を明確にし、それを併せて満たすレベルのセキュリティ対策を企画・検討することが必要です。

工場 FA システムの状況(局面)に応じた考え方

上記三つのアプローチとは異なる切り口になりますが、対象とする工場の FA システムが「稼働中」、「更新間際」、「新設計画中」のどの状況(局面)にあるのかに応じた考え方で、セキュリティ対策導入の仕方を検討・企画する必要があります。

（1） 稼働中である場合

セキュリティ対策導入によるシステム改修に伴う影響を考慮し、セキュリティ対策を検討･企画する必要があります。稼働中の FA システムへ影響の無い対策を優先し、影響のある対策が必要な場合には、FA システムの定期的なシステム停止期間(メンテナンス期間など)に導入することを検討します。また、物理面や、教育など運用面の対策に注力することで補うことも検討します。

（2） 更新間際である場合

FA システムのうち更新対象部分と継続利用する既存部分との間で、セキュリティ対策の強度に差が生じないように考慮する必要があります。既存部分への対策導入が難しい場合には、既存部分が攻撃や不正の抜け穴とならないように、物理面や運用面の対策などにより、どのように補うかを検討する必要があります。

（3） 新設計画中である場合

新設の場合、稼働中や既存の FA システムに比べ、セキュリティ対策導入はし易い利点があります。一方で、FA システムは長期間(10 年以上)利用することが多くあり、その間に新たな機器の導入や初期導入機器の保守期限切れなどが発生します。このため、セキュリティ対策を検討・企画する際に、将来の変化をできるだけ想定する必要があります。

3. 対象とするFAシステムの全体像／基本構成

一般にFA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ります。そこで本章では、これからFAシステムのセキュリティ対策を論じていくにあたり、典型的な工場のFAシステムのユースケース例を設定することにします。

3.1. 想定企業

本ガイドラインのユースケース例では、FAシステムを所有する企業として、次の条件を想定します。

- 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
- 規模の大きな電子機器メーカ
- 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

上記のように規模の大きな電子機器メーカを想定しましたが、規模が中／小規模のシステムも包含しており、読者の対象システムの規模に応じて適宜読み替えてください。

3.2. 想定組織構成

想定するFAシステムに関連する組織として、次の5部門を想定します。

- 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
- 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(以下、情シ部門と称する)：
  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

実際の企業における関連組織はより多い場合もあるでしょうが、議論の発散を避けるために、上記の 5 部門としました。以降の章節において、本ユースケースを題材に論じている内容を参照する際には、各企業の実情に照らして読み替えてください。

3.3. 想定生産ライン

想定する生産ラインの特徴は、次に示すとおりです。

- 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。
  段取り替え、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)は設備ベンダから導入し、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 FA システムの例と、その構成要素の説明を示します。なお、本ガイドラインでは、この FA システム例を用いてセキュリティ対策を解説します。

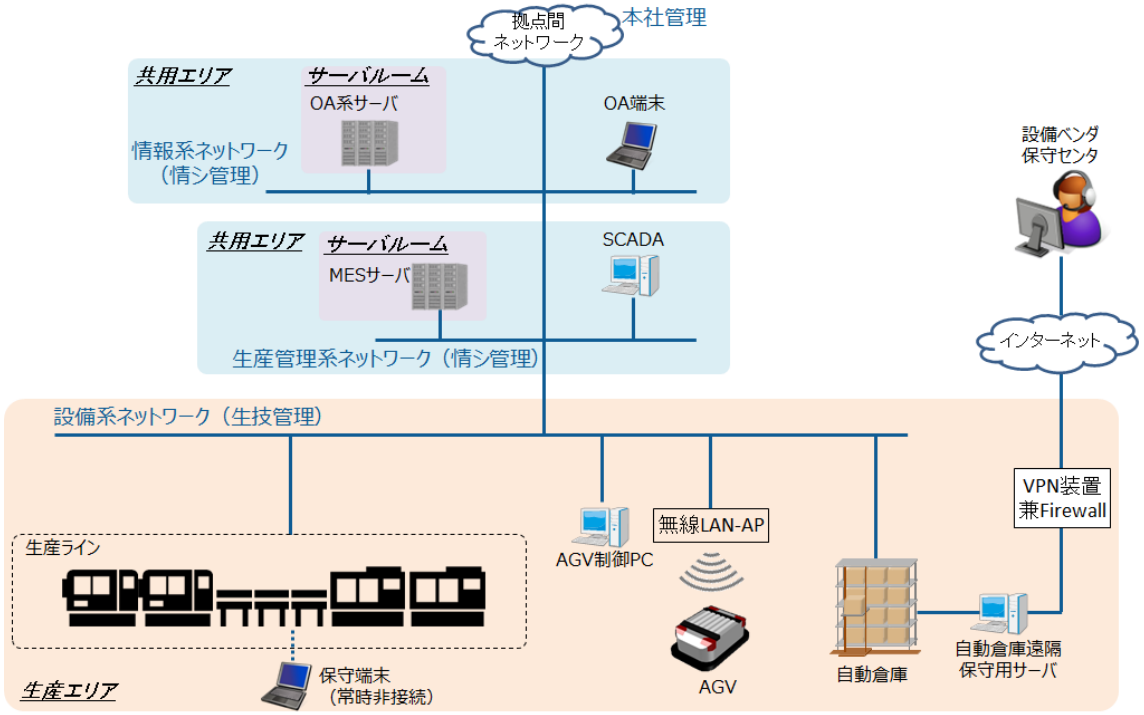


図 3-1 FA システムの例

表 3-1 主な構成要素

	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 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 制御 PC	AGV の運転計画を立案し、AGV を制御する PC

	種類	設備	概要
11		AGV	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

3.4. 想定業務

(1) 業務の重要度

FA システムにおいては、安定した品質の製品を計画どおりに生産することが重要となりますが、工場には FA システムにかかわる様々な業務があり、業務に応じた重要度が異なってくると考えられます。

業務の重要度は、セキュリティ対策の優先度を決定する判断材料となるため、ここで業務の重要度を定義します。

表 3-2 業務の重要度定義（例）

業務重要度レベル	定義
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。 もしくは、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。 もしくは、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。

(2) 業務の種類と重要度の例

FA システムが日々の業務でどのように使われているか、その業務を例示します。

表 3-3 業務と重要度（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	中
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	大
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	中
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	大
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	中
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	小
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	小
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)	小
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	小

3.5. 想定データ

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ますが、保管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てくることが想定されます。

消失、改ざん、漏えい、ファイル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につながるデータとしては、例えば以下に示すようなデータがあります。

- **生産計画データ**：
  生産当日に利用する生産計画に関する情報
- **生産レシピデータ**：
  生産設備が参照するレシピデータなどのパラメタ情報
- **部材ストックデータ**：
  生産に利用する部材がどの棚にストックされているかなどを管理する情報

3.6. ゾーンの定義

FA システムは業務内容や業務重要度などを加味して、幾つかのゾーンに論理的に区切ることができます。本ユースケース例では、下記のようにゾーンを区切ることにします。

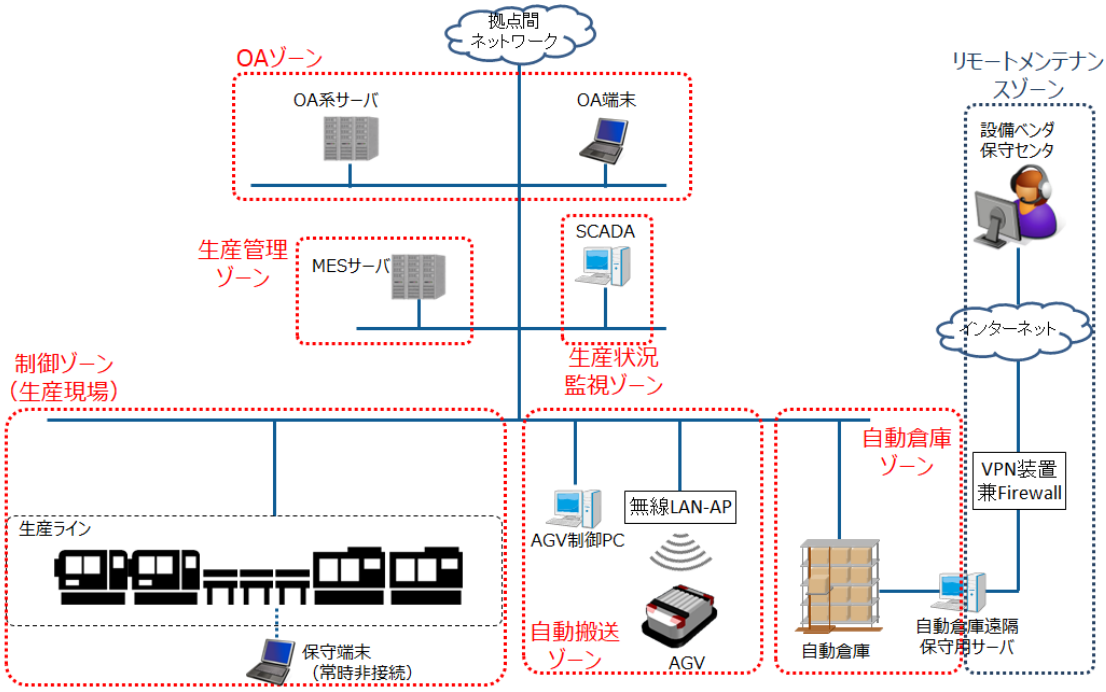


図 3-2 ゾーンの定義例

以下に各ゾーンの概要、関係する業務や重要度の例を示します。なお、ゾーンの重要度は、関連する業務の重要度のうち最大のものを設定しています。

表 3-4 ゾーンの概要と重要度（例）

	名称	概要	関連する業務	重要度
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	大
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)	大
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)	大

	名称	概要	関連する業務	重要度
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	大
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	中
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	中
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	小

なお、リモートメンテナンスゾーンは、本ユースケース例では設備ベンダの管理領域であると想定しました。そのため、以降の章節において本ユースケース例を題材に論じる際には、リモートメンテナンスゾーンは自社管理ではないとみなし、自社管理のゾーンに対するセキュリティ検討結果を示します。

4. 対象 FA システムのセキュリティ保護対象と脅威・影響

本章では、前章で示した対象 FA システムにおけるセキュリティの保護対象を示すとともに、それに対して想定される脅威及び影響を示します。

4.1. 想定保護対象

本節では、3 章で示した対象 FA システムの想定生産ラインにおける想定業務内容に基づき、セキュリティの保護対象をネットワーク、機器(機能・プログラム)、データの観点で整理します。

表 4-1 保護すべき対象（例）

	種類	保護対象	セキュリティ要素	用途	重要度
1	ネットワーク	設備系ネットワーク	可用性、完全性、責任追跡性	生産設備や各種サーバ間のデータ交換	高
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	高
3	装置・機器（機能・プログラム）	MES サーバ	可用性、完全性、真正性、責任追跡性	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	高
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	高
5		生産ライン上の設備		製品の生産	高
6		SCADA		生産ラインの生産状況の監視	中
7		保守用 PC		生産設備のメンテナンス	低
8		AGV 制御 PC		AGV の運転計画立案と、AGV 制御	高
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	高
10		AGV		部材を運ぶ装置	高
11		自動倉庫		部材の保管と入出庫を行う装置	高
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	高
13		遠隔保守用 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	低

	種類	保護対象	セキュリティ要素	用途	重要度
14	データ	生産計画	可用性、完全性、真正性、機密性、責任追跡性	月次・週次・日次の生産計画	高
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	高
16		生産レシピ		生産機種ごとの詳細情報(パラメタ等)	高
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	低
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	低
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	高
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	高
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	中

4.2. 想定される脅威・影響

本節では、前節で整理した保護対象に対して想定される脅威及び影響を示します。

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ます。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、多様になっています。

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と考えます。

そこで始めに、攻撃者の動機として考えられる例を整理します。

表 4-2 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

上記のいずれかの動機を持ち、FA 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ます。

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、管理懈怠などの想定も併せて必要です。

以下に、想定される脅威と生産への影響を例示します。

表 4-3 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 ・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)
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	

	脅威種別	脅威内容	生産・事業への影響
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
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	
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)

	脅威種別	脅威内容	生産・事業への影響
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

5. セキュリティ対策の全体像

本章では、3 章の対象 FA システムや 4 章の想定保護対象を例に採りながら、どのような進め方で、どのようなセキュリティ対策を企画・導入すれば良いのか、その全体像を説明します。

5.1. セキュリティ対策企画・導入の進め方

本節では、FA システムのセキュリティ対策を企画・導入する手順の概略を示します。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」が重要です。

ステップ 1：情報収集・整理

FA システムのセキュリティを検討するうえで、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、整理します。

・経営目標との関連整理：

経営目標を実現するために必要となる、システム導入・改修を整理

・外部要求事項(社会的セキュリティ要件)の考慮：

準拠すべき社会的ルールや、取引先等からの要求事項を整理

・内部要件／状況の把握：

企業内部のセキュリティ要件や、

現状のシステム構成（ネットワーク、機器、機能、データ等）・運用を整理

ステップ 2：経営層による取り組みの宣言

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シップが必要となります。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します。

ステップ 3：戦略立案

・セキュリティ対策の企画：

FA システムに対して、企業の事業方針と整合したセキュリティ対策を企画します。

・ロードマップの策定：

セキュリティ対策導入の実施計画を策定します。

ステップ 4：戦略の実行管理

実施状況と、ステップ 1 で収集した情報に変化が無いかを定期的に確認します。

以下に、3 章の例をもとに、このステップに沿った進め方の内容を説明します。

5.1.1. ステップ 1：情報収集・整理

（1）経営目標との関連整理

セキュリティ対策を検討・企画するに際し、事業伸張や事業継続の視点から、どのような経営目標にかかわる事項を考慮する必要があるのかを整理します。

表 5-1 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の例

区分	内容	例（3 章）
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／不調による事業上の損失防止	生産／出荷の遅延防止、規格外製品の製造防止
	安全上の問題の発生防止	生産設備、自動倉庫、AGV の誤動作防止

（2）外部要求事項(社会的セキュリティ要件)の考慮

セキュリティ対策を妥当な(過不足の無い)内容にするためには、外部からのセキュリティにかかわる要求事項(社会的セキュリティ要件)を考慮する必要があります。

表 5-2 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の例

区分	内容	例（3 章）
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	業界ガイドライン・国際標準規格	IEC 62443 ほか

（3）内部要件／状況の把握

対象 FA システムのセキュリティ対策(システム面、運用・管理面、維持・改善面)にかかわる要件や現状を確認します。

表 5-3 内部要件／状況把握の例

区分	内容	例（3 章）
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

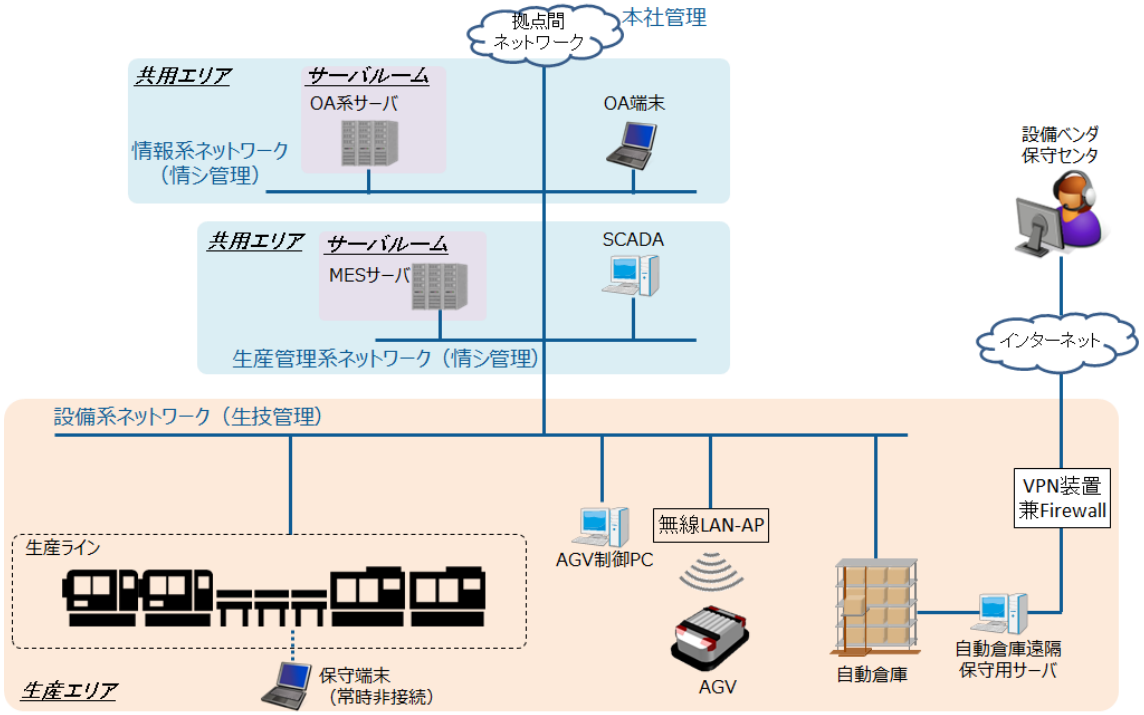


図 5-1　3 章の FA システム構成例(再掲)

5.1.2.　ステップ２：経営層による取り組みの宣言

セキュリティ対策を実施・推進するためには、経営層のリーダシップが重要となります。このため、経営層がセキュリティ対策推進の意志を組織として明文化し宣言します。

経営層が認識すべき事柄として、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」が発行されています。この内容などを参考にしながら、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します。

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。

5.1.3. ステップ３：戦略立案

ステップ１で収集・整理した情報に基づき、FA システムのセキュリティ対策を「セキュリティ戦略」として策定します。具体的には以下の項目を策定します。

・全体方針の策定：

セキュリティ対策の優先度・目標を策定します。

・物理面、システム面の対策：

セキュリティリスクアセスメントの結果に基づき、FA システムとして具備するセキュリティ対策を策定します。(⇒5.2.2 節、5.2.3 節を参照)

・運用・管理面の対策：

FA システムのセキュリティ攻撃に対する運用・管理面の対応方法を策定します。(⇒5.2.4.1 節を参照)

・維持・改善面の対策：

人財育成を含め、継続的にセキュリティを維持・改善する施策を策定します。(⇒5.2.4.2 節を参照)

全体方針の策定

FA 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決めます。
具体的には、「セキュリティ要求レベル」を定義します。

セキュリティ要求レベルの定義

FA 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ります。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)を検討します。

本ガイドラインでは、この重要度を「セキュリティ要求レベル」として整理します。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ります。本ガイドラインでのセキュリティ要求レベルは、下記として定義しています。(レベル決めの方法は、各社で最適なものとしてください。)

・「業務の重要度」×「脅威レベル」＝「セキュリティ要求レベル」

表 5-4 業務の重要度

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、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
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 5-5 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 • 物理的／論理的アクセスが容易 • 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 • 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 • 物理的／論理的アクセスに一般的な制限を掛けている • 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 • 攻撃や不正の実施にはそれなりの時間を要する

脅威レベル	定義
1	脅威を受ける可能性が低い • 物理的／論理的アクセスに強い制限が掛かっている • 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 • 攻撃や不正の実施には長い時間を要する

「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)が脅威を受ける可能性(高低)を表すものです。保護対象におけるセキュリティ対策が不足しており、攻撃や不正を実現する方法が容易で(あるいはパターン化／ツール化されインターネット上で入手でき)、スキルや知識を要さない場合には、脅威レベルは高：3 になります。一方で、保護対象におけるセキュリティ対策が充実しており、攻撃や不正を実現する方法が困難で(あるいは対象に応じた個別の探索や試行錯誤が必要で)、高度なスキルや知識を要する場合には、脅威レベルは低：1 になります。

保護対象(あるいはゾーン)それぞれにかかわる「脅威レベル」の評価を単純／容易にするために、保護対象における(物理的／論理的アクセスに制限を掛けるなどの)セキュリティ対策が実施できているか否かだけに着目し、「脅威レベル」を評価するのも良いでしょう。

「脅威レベル」を評価するのが難しいと感じる場合は、セキュリティ専門家／ベンダのリスクアセスメントサービスを活用しましょう。

なお、「脅威レベル」やその評価方法に関しては、IPA「制御システムのセキュリティリスク分析ガイド」[14]に詳しい解説が記載されていますので、参考にしてください。

[14] IPA「制御システムのセキュリティリスク分析ガイド」:
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
https://www.ipa.go.jp/files/000080712.pdf

表 5-6 セキュリティ要求レベルの例

		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

※レベル決めの方法は、各社で最適なものとしてください。

「セキュリティ要求レベル」（＝「業務の重要度」×「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

・その影響が発現する可能性の大小

を表すものになります。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ります。

表 5-7　3 章のシステムでの例

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(5.2 節を参照)を実施する必要があります。

5.1.4. ステップ４：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します。

（１） 実施計画の策定

前節で策定した全体方針に基づき、「6.2. 多面的なセキュリティ対策の全体像」にて整理されている対策の実施計画を明確にします。

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します。

1．目的
…

2．方針
…

3．体制
…

4．計画

施策目標	完了時期	実施計画				
		AA/1Q	AA/2Q	AA/3Q	AA/4Q	…
Aaライン堅牢	XX/YY	XX導入	○○改修	△△移行	切り替え	…
Bbサービス連携	XX/YY	－	××評価	×△運用見直し	◇◇開始	…
費用	－	○○	○○	○○	○○	…
人員	－	△△	△△	△△	△△	…

図 5-2 実施計画書の例

（２） 進捗確認

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します。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、PDCA サイクルを回し継続的かつ適応的に実行を進めていくことになります。

5.2. 多面的なセキュリティ対策の全体像

本節では、4 章で整理した保護対象、想定脅威／影響に対して、どのようなセキュリティ対策を取れば良いのか、多面的な全体像の概要を示します。ここで示した対策のうち、前節までに説明した方針や検討の進め方に沿い、重要度・優先度の高い対策を選定し適用することになります。

5.2.1. 想定脅威に対するセキュリティ対策の対応づけ

まず本節で、4.2 節で挙げた想定脅威に対して、どのようなセキュリティ対策が対応付けられるのか、その全体像を示します。

以下の表に整理するように、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対応づけられます。また、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対応づけられます。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、主にシステム構成面での機器における対策が対応づけられます。

さらに、前述のような事前防御的な物理面／システム構成面での対策に加え、運用を開始したあとのセキュリティ問題や環境の変化へ対応していくために必要な、ライフサイクル全体にわたる日常的な運用・管理面、維持・改善面の対策、及びプロセス全体にわたるサプライチェーン面での対策も、併せて実施することになります。

表 5-8 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､洪水などによる浸水・漏水	5.2.2. 物理面での対策	5.2.2.1. 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		5.2.2.5. 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	5.2.2. 物理面での対策	5.2.2.2. 電源／電気設備にかかわる対策
			5.2.3. システム構成面での対策	5.2.3.2. 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	5.2.2. 物理面での対策	5.2.2.6. 物理アクセス制御／管理にかかわる対策
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	5.2.2. 物理面での対策	5.2.2.5. 機器にかかわる対策
			5.2.3. システム構成面での対策	5.2.3.2. 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	5.2.3. システム構成面での対策	5.2.3.1. ネットワークにおける対策

No.	脅威種別	脅威内容	対策種別	対策内容
8	データ盗難・漏えい	USB などへの不正コピー	5.2.2. 物理面での対策	5.2.2.5. 機器にかかわる対策
			5.2.3. システム構成面での対策	5.2.3.2. 機器における対策
9		不正なサーバへのアップロード	5.2.3. システム構成面での対策	5.2.3.1. ネットワークにおける対策
				5.2.3.2. 機器における対策
10		パケットの盗聴	5.2.3. システム構成面での対策	5.2.3.1. ネットワークにおける対策
				5.2.3.2. 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	5.2.3. システム構成面での対策	5.2.3.2. 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	5.2.3. システム構成面での対策	5.2.3.1. ネットワークにおける対策
				5.2.3.2. 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	5.2.3. システム構成面での対策	5.2.3.1. 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		
16		設備の安全制御の機能停止		5.2.3.2. 機器における対策
17	可用性低下	ネットワーク停止	5.2.3. システム構成面での対策	5.2.3.1. 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		5.2.3.2. 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	5.2.3. システム構成面での対策	5.2.3.1. ネットワークにおける対策
				5.2.3.2. 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
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	5.2.2. 物理面での対策	5.2.2.2. 電源／電気設備にかかわる対策
			5.2.3. システム構成面での対策	5.2.3.2. 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	5.2.3. システム構成面での対策	5.2.3.2. 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	5.2.2. 物理面での対策	5.2.2.5. 機器にかかわる対策
			5.2.3. システム構成面での対策	5.2.3.2. 機器における対策
27		設定／操作ミス	5.2.3. システム構成面での対策	5.2.3.2. 機器における対策

5.2.2. 物理面での対策

工場の物理面でのセキュリティ対策とは、外部からの侵入、盗難等の防犯対策や、水害、地震等の天災から生産設備・制御システム等を保護し、その可用性や信頼性を確保するためのものです。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ります。

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ります。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」を参考にしてください。

5.2.2.1. 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重要です。

本節では、運用時にも必要となる「防水対策」、「有害物生物の侵入対策」を例示します。

（1） 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ます。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ります。注意する箇所や対策例を参考にしながら、必要な対策を実施してください。

- 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、フリーアクセスフロアなどには、
  漏水検知の仕組みを備えること

（2） 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ます。有害生物の対策としては、例えば以下のようなものが挙げられます。これらを参考に、有害生物の侵入対策を検討してください。

- 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

5.2.2.2. 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・機器の故障などのときにも、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ります。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や、信頼度の高い電源設備構成の実現などが求められます。

加えて、近年の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おり、サイバーセキュリティ対策がますます重要となっています。

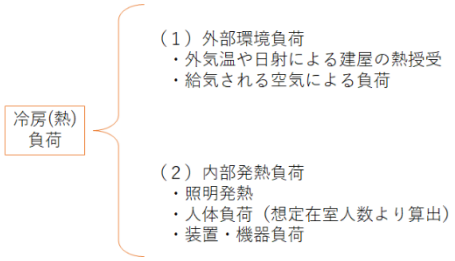
生産設備やラインの重要度などから給電停止が許容できない設備の場合には、それにかかわる電気設備の構成は、生産ラインのトラブルやサイバー攻撃による設備停止・故障時だけでなく、定期点検時においても、給電の継続が可能となるように冗長性を持たせた設備構成が必要です。

5.2.2.3. 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、空調による冷却を実施したり、諸室条件(湿度、静電気抑制、空気清浄度など)を確保したりする必要があります。

このような空調が停止する、あるいは異常を来たすことの無いように、対策を取る必要がありますが、設備の停止や異常が発生する要因として、設備の故障や不調だけではなく、サイバー攻撃や不正操作などの脅威も想定した対策が必要です。

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す。空調の冷却方式や仕様の選定は、装置の熱負荷計算を行い、これに加え、外部環境からの負荷や内部発熱による負荷を算定し、冷房負荷計算を行います。季節の条件にもよりますが、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します。



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 5-3 空調設備の熱負荷計算の方法

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します。

なお、外部への排気により自然環境に対する悪影響を招くことの無いように、排気や空気清浄などの制御に異常が発生した場合の対策も併せて必要です。

5.2.2.4. 水道設備にかかわる対策

工場では、水が生産原料に用いられる場合や、水が継続的かつ安定的に供給されないと稼働しない機器が存在する場合があります。生産機器やサーバ室など設備の冷却水や、製品の洗浄用水などがそれに当たります。

このような給水が停止する、あるいは異常を来たすことの無いように、対策を取る必要がありますが、設備の停止や異常が発生する要因として、設備の故障や不調だけではなく、サイバー攻撃や不正操作などの脅威も想定した対策が必要です。

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設備停止に至ることもあることから、対策として冷却水配管の冗長化、ポンプの冗長化、台数制御により停止時間を短くする等の対策が必要となります。冬には凍結することもあるため、凍結防止対策も実施する必要があります。

また、給水設備停止時の対策も必要です。異常による停止・故障時だけではなく、ポンプ整備などの設備保全時にも停止できるような対策が必要となります。対策例を以下に挙げます。

・ポンプなど給水／循環設備の停止により、工場の操業に及ぼす影響が大きい場合には、予備の設備・配管系統を待機系として設け、停止時に迅速に切り替えられるようにする。

・給水や循環水の流量を制御する自動弁の停止や整備の必要性を考慮し、バイパスラインを設ける。

なお、上水道だけではなく、下水道に関しても環境汚染を招くことの無いように、排水や浄水にかかわる水流などの制御に異常が発生した場合の対策も併せて必要です。

5.2.2.5. 機器にかかわる対策

FA システムに用いる機器としては、ネットワークに接続される計算機(サーバ、PC)や工作機器があります。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ります。

これらの機器には、設置場所や利用業務の重要性に応じた物理対策が必要となります。

機器にかかわる物理面のセキュリティ対策を考慮する主な視点として、下記があります。

（1）転倒・落下防止

地震などによる機器の転倒・落下を防止する対策が必要です。

（2）盗難防止

不正侵入者や内部不正者による機器の盗難を防止する対策が必要です。

・固定可能な計算機や工作機器：

必要な固定を実施する必要があります。特に重要な業務に関係する装置・機器は、設置場所も考慮する必要があります。

・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を検討する必要があります。

さらに定期的な監査の実施も必要となります。

（3）不正利用防止

盗難防止策を実施しても盗難される場合があります。盗難されても、業務に支障をきたすことなく、また、企業信頼が損なわれることのないように、対策を検討する必要があります。

・悪用の防止：

盗難された機器により、FA システムに侵入し攻撃されることを防止する対策が必要となります。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が必要となります。

また、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が必要となります。

・情報窃取の防止：

盗難された記憶デバイスは、内部に保存された情報を利用できないようにする必要があり、データ暗号化などの仕組みを利用する必要があります。

（4）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に、不要なインタフェース／ポート(LAN、USB など)を物理的に閉塞しておく必要があります。

いずれにしても、FA システムが設置されている物理的環境や、運用も考慮に入れ、必要な対策を検討する必要があります。

なお、装置・機器に対する技術的な対策は、5.2.3.2 節を参照してください。

5.2.2.6. 物理アクセス制御／管理にかかわる対策

物理アクセス制御／管理は、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します。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、及び管理・監視体制の構築が挙げられます。

中でも、物理アクセス制御／管理の基本は入退管理です。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す。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ですが、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うえで、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)を設置することも必要です。

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します。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す。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してください。

表 5-9　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 5-10　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

5.2.2.7. 物理セキュリティの運用・管理

前節までに示してきた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ります。たとえば、以下に挙げるような運用・管理の事項が考えられます。

・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、
・工場からの機器の不要／不正な持ち出し禁止、
・工場や生産ラインなどへのデバイスの不要／不正な持ち込み禁止、など

運用・管理を遠隔から一元的・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りますので、併せて検討するのが良いでしょう。

なお、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ります。

・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・管理する必要があります。

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ります。

5.2.3. システム構成面での対策

システム面のセキュリティ対策は、次の 3 つの視点で実施します。

・侵入防止：FA システムへの不正侵入の防止

・活動抑止：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：FA 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 5-11 システム構成面のセキュリティ対策の目的と説明

	目的		説明
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、FA 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ります。

それぞれの対策の内容を以下に説明します。

5.2.3.1. ネットワークにおけるセキュリティ対策

FA 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ります。

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)の設定や、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)の導入を行います。

また、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)も行います。

さらに、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も利用します。

以下の表に対策例を示します。保護対象のネットワーク及び通信のセキュリティ要求レベルに応じた強度の対策を選定する際の参考としてください。

なお、技術や攻撃手法は日々進化しています。各社の要件に応じて最適かつ最新の対策を検討・導入してください。

表 5-12 ネットワークにおけるセキュリティ対策例

対策カテゴリ	セキュリティ対策強度			目的		
	最低限	一般的	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細分	＋物理ドメイン分割	○	○	
接続機器制限	－	IP、MAC アドレス制限	＋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	○		

対策カテゴリ	セキュリティ対策強度			目的		
	最低限	一般的	高	侵入防止	活動抑止	運用支援
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・異常検知(IDS)	＋電文内容解析・異常通信遮断(IPS)	○	○	
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(IDS)	＋異常通信遮断(IPS)	○	○	○
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	＋ソフトウェア更新(セキュリティパッチ適用)[or 仮想的な対策(IPS、仮想パッチ等)]	○	○	
ログ取得	－	機器内ログ取得	＋IDS ログ連携			○

5.2.3.2. 機器におけるセキュリティ対策

FA システムにおいて生産設備や計算機などの機器(以降、機器)には、サーバ、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ります。本ガイドラインで提示する対策は、汎用 OS／ソフトウェアを利用する機器を想定しています。

機器における対策として、「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、機器の設定や、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などを行います。

また、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も利用します。

以下の表に対策例を示します。保護対象の機器(機器上の機能／プログラム／データ／インタフェースを含む)のセキュリティ要求レベルに応じた強度の対策を選定する際の参考としてください。

なお、技術や攻撃手法は日々進化しています。各社の要件に応じて最適かつ最新の対策を検討・導入してください。

表 5-13 機器におけるセキュリティ対策例

対策カテゴリ	セキュリティ対策強度			目的		
	最低限	一般的	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	○	○	
利用ポート	－	媒体検査	＋内容検査	○	○	

対策カテゴリ	セキュリティ対策強度			目的		
	最低限	一般的	高	侵入防止	活動抑止	運用支援
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			○

対策カテゴリ	セキュリティ対策強度			目的		
	最低限	一般的	高	侵入防止	活動抑止	運用支援
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査	＋ソフトウェア更新(セキュリティパッチ適用)[or 仮想的な対策（IPS、仮想パッチ等)]	○	○	
ログ取得	－	システムログ取得	＋業務ログ取得			○
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			○

5.2.3.3. 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

FA 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、必要な機能を実現します。

これらのセキュリティ対策は､統一的な対策内容の提示が難しいため､考慮すべきポイントを幾つか以下に記載します。各システムを構築するときに参考にしてください。

（1） 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て、自社の方針に合致しているか？

・セキュリティに関する設定項目の設定値が、自社の方針に合致しているか？

・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て、自社の方針に合致しているか？

（2） 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、実施・検証されているか？

（3） 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て、自社の方針に合致しているか？

・セキュリティに関する設定項目の設定値が、自社の方針に合致しているか？

・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て、自社の方針に合致しているか？

5.2.3.4. 対策の適用例

本節では、前節までに示してきた物理面、及びシステム構成面でのセキュリティ対策を、3 章の FA システム例に対して適用した例を紹介します。まずは対策方針を検討したうえで、ゾーンごとのレベルに応じたセキュリティ対策案を立案した内容を紹介します。

（1）対策方針の検討

5.1 節で示した手順による情報収集・分析結果に基づき、組織の事業方針や、対象となる FA システムの特性、生産製品の特徴などを加味し、工場ネットワークにどのようなセキュリティ対策を実施するかの方針を検討します。

現実的な考え方としては、業務内容や重要度を加味してゾーンを区切り、ゾーンの入口・出口対策や、ネットワークレベルでのセキュリティ対策を実施します。その理由は、制御系設備の機器には、利用者側で勝手にソフトウェアのインストールができないことが多く、ネットワークにおける対策を中心に導入するのが現実的と考えるからです。

例えば、ファイアウォールをゾーン境界に設置し、業務上必要なゾーン間通信のみを許可するように、IP アドレスやポート番号などを用いて制限を行います。また、重要なゾーンに対しては、ネットワーク上を流れる通信を監視し、攻撃や異常を検知・遮断する IDS/IPS などの導入も考えられます。

ここでは 3 章で示した FA システムを例に、対策方針を検討した例を示します。

- 生産に必要な情報は、生産管理ゾーンに置かれた MES サーバに集約します。
  各ゾーン間でデータ共有が必要になる場合は、基本的にはゾーン間での直接通信は行わずに、MES サーバを介してデータ共有を行います。
  また、MES サーバのコンソールへのログオンは、限られた管理者のみ許可するように制限し、多要素認証を導入して管理者へのなりすましリスクを低減します。

- 生産現場では、生産時に必要な情報は MES サーバから取得し、生産状況に関する情報は MES サーバや SCADA に保管します。その他のゾーンへの通信は、基本的には行わないようにします。

- 工員が操作する SCADA、営業担当などが操作する OA 端末(生産計画入力用)などの一般ユーザが操作する端末は、生産管理ゾーンとは独立したゾーンを設け、そのゾーンに端末を設置します。必要に応じて、各種サーバへのアクセス時には多要素認証を導入し、なりすましリスクへの対策を行います。

（2）ゾーンごとのレベルに応じたセキュリティ対策立案

検討したセキュリティ対策方針に応じて、ゾーンごとの重要度に応じた対策を立案します。このとき、生産現場のゾーンをレベル分け(重要度高・中・低など)し、対策方針とゾーンのレベルに応じて実施すべき対策を決めます。同じレベルのゾーンには同じ対策を当てはめることで、同一重要度のゾーンでセキュリティ対策レベルが異なることの無いようにする狙いがあります。

表 5-14 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		ゾ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

	区分	要件	低	中	高
3	活動抑止	不要通信の遮断	・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、3 章に示した FA システムの例に対し、対策を行った状態を図示します。

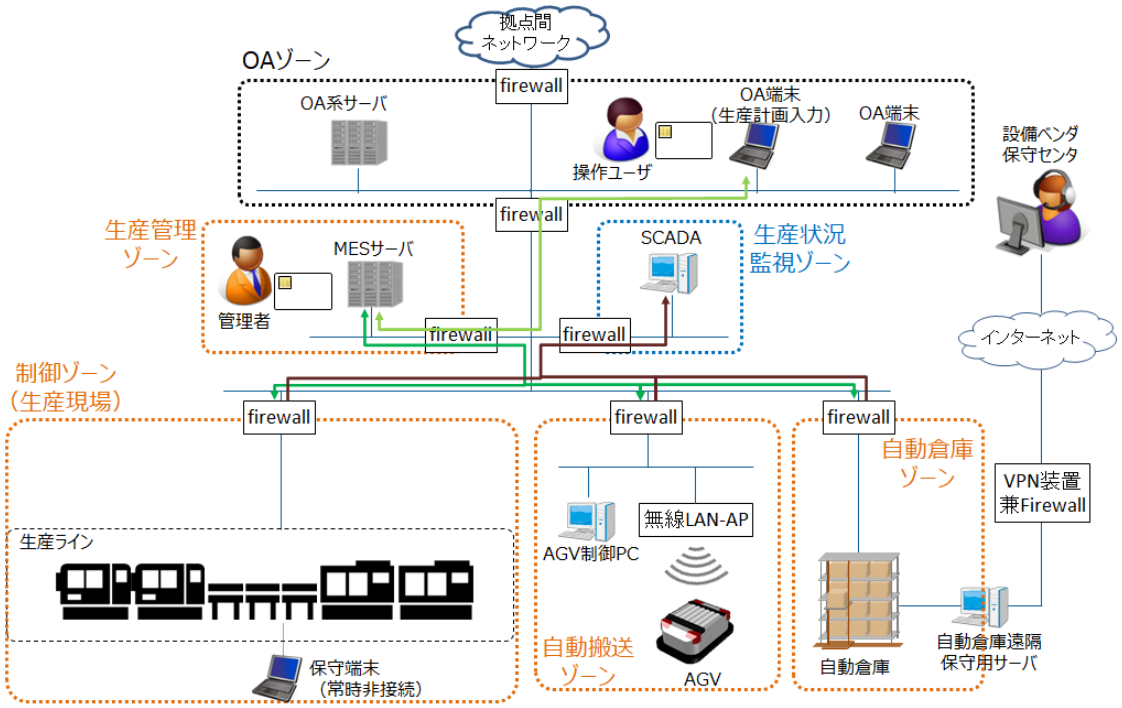


図 5-4 要件に対する各ゾーンでの対策例

なお、本書スペースの都合上、表 5-14 では主要な対策例のみを例示するに留めています。ここに記載したものを実施すれば十分という訳ではなく、実際には 5.1 節に記載の手順に従い、自社の置かれた状況を整理し、網羅的にセキュリティ対策を検討してください。また、7.2 節に挙げた各種ガイドラインや、セキュリティベンダが発行しているホワイトペーパ等も参考にしてください。

5.2.4. ライフサイクル面での対策

本節では、FA システムのシステム面でのセキュリティ対策を導入し、運用を開始したあとのライフサイクル面の対策として、運用・管理面の対策と、維持・改善面の対策として必要な内容を説明します。

5.2.4.1. 運用・管理面のセキュリティ対策

運用・管理面のセキュリティ対策には、２つの視点があります。

・サイバー攻撃の早期認識と対処

・セキュリティ対策の運用上必要な管理作業(ID/PW 管理、機器の設定変更など)

以下にそれぞれを説明します。また、運用・管理の体制例を示します。

5.2.4.1.1. サイバー攻撃の早期認識と対処

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ます。このため、侵入や攻撃活動が発生した場合に被害を最小化することを目指し、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を検討します。

具体的には、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対して、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になります。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必要です。

以降に、この一連の取り組みを、“監視(Observe)－分析(Orient)－判断(Decide)－行動(Act)”[OODA プロセス]に分解して説明します。

（1）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必要があります。

・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

・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

それぞれを監視するうえでの要件を以下に記載します。

(a) 従来のアラートからの類推

従来からのアラートが発生する要因の一つとして、セキュリティ攻撃が考えられます。このため、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ります。

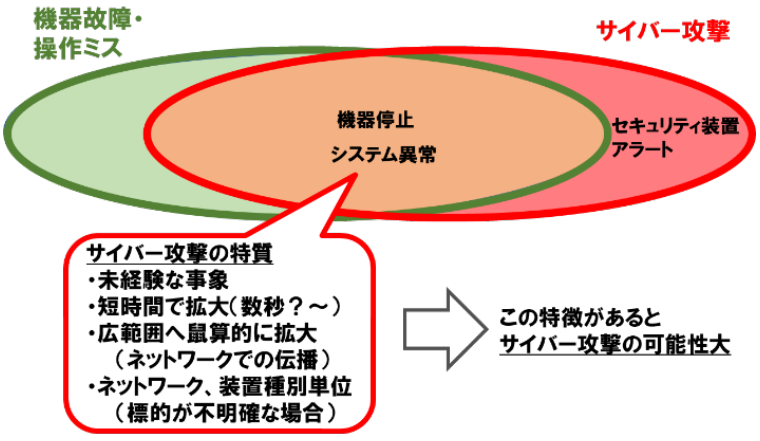


図 5-5 アラート発生要因の調査・整理

表 5-15 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	○

(b) セキュリティアラート

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することが必要です。

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)するかを明らかにします。

表 5-16 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の確認

もし、企業／工場の中に、FW や IDS などからのアラートを監視するためのスキルを有する人財や体制を確保できない場合には、それを支援するセキュリティ専門ベンダの監視サービスを活用してください。

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す。

（２）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ります。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ります。

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不可欠となります。セキュリティ専門家との連携方法を予め確立しておくことが必要です。もし、企業／工場の中に、分析するためのスキルを有する人財や体制を確保できない場合には、それを支援するセキュリティ専門ベンダの監視・分析サービスを活用してください。

分析の内容を以下に示します。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、分析する内容が異なります。

(a) 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

(b) 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

・影響波及の推定、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

（３）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ります。的確で迅速な判断ができる体制、方針・判断基準、連絡先・手段を予め確立しておく必要があります。

判断の内容を以下に示します。「兆候段階」か「被害発生段階」かにより、判断する内容が異なります。

(a)兆候段階

・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

(b)被害発生段階

・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）

・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

この意思決定を迅速にするためには、FA 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の影響度・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す。

（4）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ります。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す。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仕掛けが不可欠です。

なお、上述のような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り組みのことを「セキュリティインシデント対応」と呼びます。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、7.5 節に挙げる既存のガイドラインにて詳しく整理されていますので、そちらを参照してください。

5.2.4.1.2. 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、関係者への徹底が必要となります。

表 5-17 セキュリティ管理作業の例

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 (最終的にはツールで 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

管理対象		目的	運用ルール	管理が必要な情報
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

5.2.4.1.3. 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ります。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ります。

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ります。この体制整備の例を幾つか参考に提示します。

・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す。

・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 FA システムのセキュリティ運用・管理も実施する形態です。

・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。
FA 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す。

・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、FA 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

FA 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す。

・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

いずれかの方法がベストという訳ではありませんが、上記を参考にしていただき、生産現場や組織、システムの状況等を考慮したうえで、セキュリティ運用・管理を行える体制を確保する必要があります。

5.2.4.2. 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、FA 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、事業伸張／継続の視点及び SQDC 確保の視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(体制を含む)のセキュリティ対策を更新することです。

攻撃手法は日々進化し、FA システムや機器におけるセキュリティ上の弱点(脆弱性)が新たに顕在化します。攻撃が受ける前に、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、FA システムへの攻撃及び被害を未然に防ぐことができます。

さらに、セキュリティ対策を維持・継続するうえで、組織・人財のスキル向上として、FA 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ります。

維持・改善のプロセスは、一般的に PDCA(Plan-Do-Check-Act)となります。本節では、この PDCA プロセスを着実に回すために必要な活動のポイントと体制例を示します。

5.2.4.2.1. 維持・改善のために必要な活動

・変化するセキュリティ脅威・攻撃手法、脆弱性、技術にかかわる情報の入手
・利用機器、及びソフトウェアの脆弱性情報の入手
・人財のスキル向上、育成

（1）変化するセキュリティ脅威・攻撃手法、脆弱性、技術にかかわる情報の入手

脅威／脆弱性情報、セキュリティ技術情報などは、下記のサイトで公開されています。

・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（IPA）
https://www.ipa.go.jp/security/index.html

また、社内では IT 部門とも情報連携をする必要がありますし、社外のセキュリティ情報共有組織として、IPA のサイバー情報共有イニシアティブ(J-CSIP)[15]、日本 CSIRT 協議会[16]、業界ごとに設立・運営されている ISAC[17]などがありますので、積極的に活用してください。

（2）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脆弱性情報は、上記(1)のサイトでも公開されていますが、汎用製品以外の情報は公開されていません。このため、利用している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ります。

（3）人財のスキル向上、育成

FA 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、FA 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ります。

また、人の定期異動により、スキル自体も喪失される可能性があります。このため、実際の FA システムを前提にした、セキュリティスキルの維持・改善が不可欠となります。そこで、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により、FA 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・改善することが重要です。

---

15 サイバー情報共有イニシアティブ(J-CSIP)：公的機関である IPA を情報ハブ(集約点)の役割として、参加組織間でサイバーセキュリティに関する情報共有を行い、高度なサイバー攻撃対策に繋げていく取り組み。

https://www.ipa.go.jp/security/J-CSIP/

16 日本 CSIRT 協議会(NCA)：CSIRT 間の情報共有のための緊密な連携を図り、組織内 CSIRT 構築を促進・支援するなど、CSIRT 間の共通課題の解決に貢献するためのコミュニティ。https://www.nca.gr.jp/

17 ISAC (Information Sharing and Analysis Center)：サイバーセキュリティの脅威や脆弱性に関する情報を収集・調査・分析し、共有を促進したり、共同対処したりすることで、セキュリティ対策レベルの向上に寄与するための非営利組織で、業界ごとに設立・運営されている。(たとえば、金融、情報通信、電力、自動車、医療、貿易、交通など)

5.2.4.2.2. 維持・改善のための体制（例）

サイバー攻撃のリスクに対して早期に対処することは、事業継続や企業信頼を維持する上で重要となります。この活動を推進する体制整備の例を幾つか参考に提示します。

・FA 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）
・IT 管理部門で実施
・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）
・セキュリティ統括組織で実施

(a)FA 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）

FA 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す。

・メリット：FA 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

(b)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す。

・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：FA 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

(c)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す。

・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：FA 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

(d)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す。

・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

5.2.5. サプライチェーン面での対策

サプライチェーン面でのセキュリティ対策は、次の４つ視点で検討が必要です。

・購入製品／部品
・業務委託
・システム開発委託
・連携システム

それぞれに関して考慮すべき主なポイントを以下に記載します。
各社の状況に応じて補強するようにしてください。

（1）購入製品／部品

製品／部品購入時に下記の点を確認する必要があります。

・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、及び検証が実施されているか？
－「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

（2）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必要があります。

・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？

（3）システム開発委託

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ります。

・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？

（4）連携システム

FA 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必要があります。

・システムに対して必要なセキュリティ対策は導入されているか？
また、対策は自社と同等、もしくは、最低限必要な内容となっているか？

・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？

また、サプライチェーンを構成し連携する他社の工場やシステムにおいて、サイバー攻撃などによるセキュリティ問題が発生し、その生産や受発注などに支障が生じた場合に、自社の工場やシステムにまで影響が拡がり事業継続に支障が生じることの無いように、そのような事態を想定したシステム間の連携の仕方や、事業継続を実現するための備えをしておくことが重要です。

逆に言うと、自社のセキュリティ問題が、サプライチェーンを構成し連携する他社の工場やシステム、及びその事業継続に影響を与えることの無いように、セキュリティ対策の導入及び連携が必要だということです。

5.3. スマート工場の実現に向けた段階的な実現レベル向上

FA システムにおいてもスマート工場を目指し、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ニーズが高まっており、FA 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ます。

本節では、FA システムの今後の拡がり全体を概観するとともに、新たに発生するリスクを示します。

5.3.1. スマート工場への流れ

FA 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が進んできています。

ここでは利用形態の 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します。

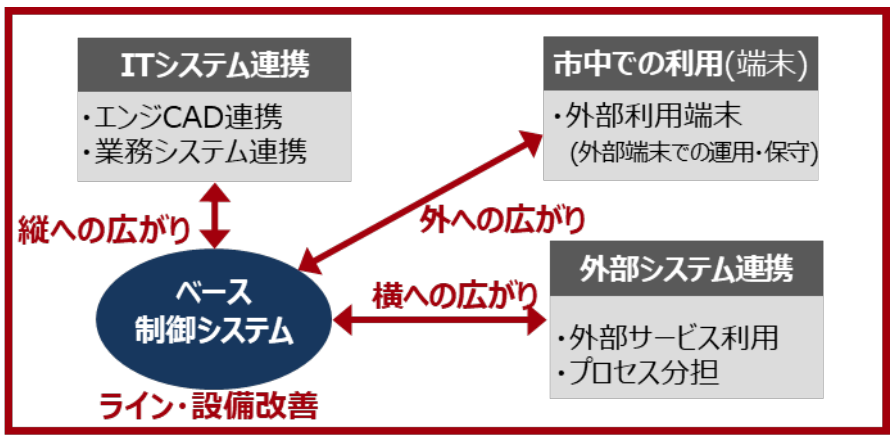


図 5-6 FA 制御システム利用形態の拡がり

（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います。

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ます。

表 5-18 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です。また、分析結果に基づき、FA システムの改善を行います。

この形態への拡がりにおいて、考慮すべきリスクの例を示します。

表 5-19 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、FA システムの監視・制御や保守を実施する形態です。

この形態への拡がりにおいて、考慮すべきリスクの例を示します。

表 5-20 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 FA システムの構築・連携を行います。

この形態への拡がりにおいて、考慮すべきリスクの例を示します。

表 5-21 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

5.3.2. 新たなセキュリティ対策の動向

スマート工場の実現へ向け、FA システムと外部の各種システムとの連携を実現するためには、従来は外部と接続していなかった製造現場のネットワークと、外部の組織(他部門、他社)が管理するネットワークやシステムとの接続を、進めていくことが必要になります。このため、新たなセキュリティ脅威を受けるリスクが増える可能性があります。

本節では、FA システムの各種システムとの連携による拡がりを支えるための組織面及び導入技術・対策面の新たな動向を示します。

(1) 組織

工場 SIRT (FSIRT)／PSIRT

セキュリティの脅威、脆弱性にかかわる情報を相互に連携し対応する組織として、「SIRT(Security Incident Response Team)」の導入が進んでいます。製造現場におけるセキュリティインシデントへ対応する組織として、「工場 SIRT(FSIRT)」があります。また、ソフトウェア製品の提供者がインシデント対応を実施するための組織として、「PSIRT(Product Security Incident Response Team : 製品脆弱性対応体制)」があります。

昨今セキュリティインシデントが増加し、製品を提供している各社で PSIRT 設置と運営が検討され、インシデント発生による被害拡大を抑えるための活動が始められています。PSIRT 運営では具体的な業務の例として、セキュリティにかかわるリモート監視やリモート保守などがあります。今後の FA システムにおいては、FA システムを構成する機器の外部接続によるリモート監視やリモート保守を想定しておく必要があります。

(2) 導入技術・対策

システム構成(ネットワーク、接続機器)の可視化・管理

外部のネットワークやシステムと接続するにあたり、まずは工場の FA システム内部のネットワーク及び接続機器の構成を正しく把握し、不正な機器が接続されていないことを管理できるようにする必要があります。

これを実現するための技術・対策製品として、ネットワークを流れる通信パケットに含まれる情報に基づき、ネットワーク及び接続機器の構成を可視化し、管理することを可能にするものがあります。

ネットワーク通信の監視・異常検知・遮断(IDS/IPS)

次に、内部のネットワーク上でやり取りされる通信が正常な状況であることを監視し、異常な通信を検知できるようにする必要があります。そして、万一異常な通信を検知した場合には、異常な通信を遮断できるようにする必要があります。

これを実現するための技術・対策製品として、ネットワークを流れる通信パケットを解析し、通信の状況を可視化したり、不正な送信先に対する通信を検知したり、異常な内容の通信を検知したりすることを可能にするものがあります。さらに、検知した異常な通信を遮断することを可能にするものがあります。

機器の真正性確保・認証

上記のセキュリティ対策をより安全に実現するために、内部のネットワークに接続する機器が正当な機器であることや、通信相手の機器が正しい相手であることを認証でき、機器の真正性を保証できるようにする必要があります。

これを実現するための技術・対策製品として、電子証明書や暗号技術を用いた通信相手の厳密な相互認証を可能にするものがあります。また、多数の機器に設定される認証情報(デバイス ID、電子証明書、暗号鍵など)の管理の簡易／省力／自動化を可能にする技術・対策製品があります。さらに、その際に用いる秘密鍵を安全に保護するためのハードウェアセキュリティモジュールやメモリアクセス制御機構を実現する技術・対策製品もあります。

機器のデータ保護、プログラム保護(マルウェア対策)、不正デバイス接続防止

さらに、機器内部のセキュリティ対策として、データの漏えい・改ざんを防ぐための暗号化を実現する技術・対策製品や、機器上で不正なプログラムの実行やプログラムの改ざんを防ぐためのマルウェア対策を実現する技術・対策製品や、機器に対する不正なデバイス接続を防ぐためのアクセス制御を実現する技術・対策製品などがあります。

5.3.3. FA システムセキュリティ対策の段階的な向上

5.3.1 節で示した新たなトレンドを実現するためには、FA システムが、組織内の情報システムやインターネット及び社外システムとの接続を行うことになります。しかし、現状のほとんどの FA システムは、制限された用途でしか接続していないことを理由に、十分なセキュリティ対策を実施できていない場合が多くあります。このような状態で、新たな状況への急激な変化及び対応を進めようとすると、ラインの安定・連続稼働や SQDC の担保などに影響する新たなセキュリティ課題が発生します。

本節では、このセキュリティ課題への対策を導入するステップを参考に紹介します。

情報システム・インターネット接続を進める際のセキュリティ課題

既存の FA システムは、閉域環境を前提に設計されているものが多いのと、可用性を重視するため、古いシステムが残りやすく、現状変更となるようなセキュリティ対策の導入は難しい状況です。

既存 FA システムでのセキュリティ課題として、大きくは以下の 5 点があります。

- ネットワークに接続されている機器(制御機器、PC 端末、ネットワーク機器など)が不特定で、何がどのように接続されているかの全容を把握できていない。
- ネットワークがフラットで階層化や分割／分離が為されていない。
- マルウェア(ウイルス)対策未導入の PC 端末が多く存在する。
- セキュリティ対策を想定していない脆弱な制御機器が用いられている。
- セキュリティ対策を想定していない脆弱な通信プロトコルが用いられている。

FA システムの外部接続・連携を拡げていくためには、セキュリティ対策を適用できず、上記課題を有する既存の古いシステム／機器から、セキュリティ対策を適用できる新しいシステム／機器へ置き換えられることが望ましいのですが、実現機能面やコスト面などの制約により古いシステム／機器を継続利用せざるをえない場合も未だ多いのが実情です。このような場合には、その制約を前提として、セキュリティ対策をどのように進めていけば良いかを工夫する必要があります。それを以下に説明します。

FA システムのセキュリティ課題への対策の段階的な導入

FA システムの段階的なセキュリティ向上の具体例として、外部との接続の度合いを 3 段階に分けて、順にセキュリティ対策を強化していく方法を示します。それぞれの段階で、どのようなセキュリティ対策が必要となるかを、「運用・管理」及び「システム」の面から整理しました。

① Step1：運用・管理を重視した対策

Step1 は、FA システムが情報システムやインターネットと接続していない、あるいは制限付きの接続を行っている状態です。FA システムの現状変更を伴うような対策は難しいため、ネットワーク構成には手を入れず、FA セキュリティの責任組織構築や運用・管理の改善など、組織と運用・管理を重視したセキュリティ対策を中心に実施します。管理を実現する一環で、物理面の対策だけでもまずは実施できるのが良いでしょう。

なお、運用・管理面のセキュリティ対策として、どのような対策を実施すれば良いのかは、5.2.4 節に記載されている対策内容を参考にしてください。(維持・改善面の対策を含む)

また、可能であれば、ネットワーク及び接続機器の構成可視化・管理を実現する対策や、PC 端末のセキュリティ対策を実施します。

② Step2：FA システムの境界やネットワークにおけるセキュリティ強化

この段階は、実験的に情報システムやインターネットとの接続を始めた段階です。この段階でも大きなシステム変更は難しいので、システム面の技術的な対策としては、ネットワーク及び接続機器の構成可視化・管理を実現する対策に加え、FA ネットワークと情報ネットワーク／外部ネットワークとの境界防御、及び FA ネットワーク内で異常な通信を検知する制御ネットワーク向けの IDS のような監視機器を導入します。これらの対策は、既存の FA システムへの影響が少ない対策となります。また、運用・管理面の対策もバランス良く実施することが必要です。

なお、ネットワークにおけるセキュリティ対策として、どのような対策から実施すれば良いのかは、5.2.3.1 節の表 5-12 にて、セキュリティ対策強度が最低限／一般的として記載されている対策内容を参考にしてください。

③ Step3：FA システム／機器におけるセキュリティ戦略の実現

この段階では、サプライチェーンによる FA ネットワーク統合が実施され、複数の外部システムと FA システムとを統合したセキュリティ対策を実現します。この段階で、「セキュリティ戦略」に基づき計画した対策(システム面、運用・管理面、維持・改善面、サプライチェーン面)を実現します。

なお、機器におけるセキュリティ対策として、どのような対策から実施すれば良いのかは、5.2.3.2 節の表 5-13 にて、セキュリティ対策強度が最低限／一般的として記載されている対策内容を参考にしてください。

上記のように、セキュリティリスクを段階的に縮小させていくことが必要です。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安全・安心を確保するためには、システム面の技術的な対策だけに頼るのではなく、体制や教育といった組織面、セキュリティポリシや事故対応手順といった運用・管理面の対策をバランスよく、段階的に実施していくことが重要となります。また、セキュリティ対策レベルを継続的に維持・改善していくことも必要です。

5.4. FA システム及び機器の提供ベンダ／メーカへの対策要求

5.2 節で説明したようなセキュリティ対策を実現するためには、FA システムを利用する企業／工場だけで実現するのは困難な場合があります。FA システムや機器を提供するベンダ／メーカが、システムや機器に対してセキュリティ対策を導入することにより、システムや機器の本来の機能／動作に影響を及ぼすことを恐れ、保証外の行為として扱っている場合があるからです。

このような場合は、FA システム及び機器を提供するベンダ／メーカに対して、必要なセキュリティ対策を要求する必要があります。FA システム及び機器のセキュリティ対策実装を促進するためには、利用者側から要求することが大きな影響力をもち、極めて重要であり、積極的に要求するようにしましょう。

5.5. セキュリティベンダが提供するサービス／製品の活用

セキュリティ対策の検討・企画、導入、管理・運用を実行しようとしたとき、企業／工場の中には、必要なセキュリティ対策を実施するためのスキルを有する人財や体制を確保できない場合があります。その場合には、対策実施を支援するサービスや対策実現に必要な製品を提供するセキュリティ専門ベンダへアウトソーシングするという選択肢があることを紹介します。セキュリティ対策を進めるためには、すべて自力で実行することにこだわらずに、積極的にセキュリティ専門ベンダの製品／サービスを活用するのが良いでしょう。

セキュリティ対策検討・企画支援

まず、2.3 節や 5.1 節で説明したように、必要なセキュリティ対策を検討・企画する必要がありますが、それを支援するサービスとして、セキュリティポリシ策定支援、セキュリティリスクアセスメント支援、セキュリティ要件定義支援などのサービスを提供しているセキュリティベンダがあります。

セキュリティ対策設計・導入支援

次に、5.2 節で説明したようなセキュリティ対策を導入する際には、それを支援するサービスとして、セキュリティ設計支援、セキュリティ導入支援などのサービスを提供しているセキュリティベンダがあります。また、必要なセキュリティ対策の機能を実現するセキュリティ製品を提供しているセキュリティベンダがあります。

セキュリティ管理・運用支援

さらに、5.2.4.1 節で説明したようなセキュリティ対策にかかわる管理・運用を実施する際には、それを支援するサービスとして、リモートから管理・運用を代行したりセキュリティ問題の監視・検知・対処を実施したりするサービスを提供しているセキュリティベンダがあります。また、管理・運用に必要なセキュリティ対策の機能を実現するセキュリティ製品を提供しているセキュリティベンダがあります。

セキュリティ維持・改善支援

同様に、5.2.4.2 節で説明したようなセキュリティ対策にかかわる維持・改善を実施する際には、それを支援するサービスとして、脆弱性／脅威情報の提供や、セキュリティ対策・リスク状況のアセスメントや脆弱性診断を実施するサービスを提供しているセキュリティベンダがあります。また、維持・改善に必要なセキュリティ対策の機能を実現するセキュリティ製品を提供しているセキュリティベンダがあります。

6. 中小企業の工場におけるセキュリティ対策の考え方

日本の製造業の 99%が中小企業であり、日本の製造業／工場をサイバー攻撃から守るためには、中小企業の工場にもセキュリティ対策導入を拡げることが、極めて重要です。また、サプライチェーンでつながっている中小企業を含め、セキュリティ対策導入を進めなければ、大企業の工場を守ることもできません。

昨今、サイバー攻撃に無防備な(あるいは対策が不足し脆弱な)中小企業の工場がサイバー攻撃に狙われる頻度が増加しています。そして、そこからサプライチェーンでつながっている大企業の工場へ攻撃が拡がり、影響が拡大する事態も数多く発生しています。この状況を踏まえ、取引先の大企業やグローバルから日本の中小企業に対して、サプライチェーンリスク対策として、セキュリティ対策が要求される場合も増えてきています。

中小企業の工場は、自らを守るために、そして取引先の大企業を守るためにも、セキュリティ対策の早急な導入・強化を迫られている状況です。

また、サプライチェーンの一翼を担う中小企業の工場において、自らの提供価値・競争力を向上させる目的に加え、取引先の大企業と連携するためにも、デジタル・トランスフォーメーション(DX)の推進が今後必須の要件になっていくことは確実であり、DX を進めるにあたり、サイバーセキュリティ対策は欠かすことのできない課題です。

一方で、中小企業は財務や人員に余力のない場合が多く、また、サイバーセキュリティにかかわる知識やスキルも有しておらず、セキュリティ対策は後回しにされていることが多い状況であるのも事実です。

そこで、国・自治体や業界団体がセキュリティ対策導入を支援する施策を打ち出しています。たとえば、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、経営者編で、経営者が自らの責任で対応しなければならない事項として、「サイバーセキュリティ経営ガイドライン」の内容を中小企業向けに編集し解説しています。また、管理実践編で、重要な情報に対する管理責任がある立場の方が実施する事項を、企業のレベルに合わせて段階的にステップアップできるような構成で解説しています。さらに、経済産業省と情報処理推進機構(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**」という支援を後押ししています。

5.3.3 節で説明したように、少しずつ段階的にセキュリティ対策を導入し、対策の強度を向上させる進め方を取ることも可能ですし、取引先の大企業からの要求を受け、5.4 節で指摘したように、FA システム及び機器の提供ベンダ／メーカに対してセキュリティ対策を要求するというアクションを取ることも良いでしょう。また、5.5 節で説明したように、アウトソーシングという選択肢を取り、上記「サイバーセキュリティお助け隊サービス」を活用したり、セキュリティベンダの製品／サービスを活用したりするのも良いでしょう。さらに、最低限必要なセキュリティ対策を導入したうえで、一部のリスクを移転するために、損害保険会社が提供する「**サイバーセキュリティ保険**」を活用するのも良いでしょう。

その際に、賢い買い物をするためのノウハウを身に付けておくことが肝要になります。あるいは、取引先や顧客の企業からセキュリティ対策を強く要求されるときに備えて、セキュリティにかかわる知識／見識を身に付けておくことが重要になります。

その日のために、本ガイドラインを参考にしていただければ幸いです。

7. 参考

7.1. 業界／製品分野ごとのセキュリティ法規制にかかわる補足

本節では、2.1.2.2 節で言及した、製造業／工場の FA システム及び製品のセキュリティにかかわる業界／製品分野ごとの法規制の内容を、より詳しく紹介しておきます。

業界／製品分野として、電力、自動車、医療機器、重要インフラを取り上げ、それぞれにおける法規制の内容を示します。

7.1.1. 電力分野におけるセキュリティにかかわる法規制

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ます。

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ます。

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ます。

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ます。

7.1.2. 自動車分野におけるセキュリティにかかわる法規制

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 が規定されました[18]。この規則及び規格は、まずは 2022 年 7 月以降に発売される OTA(無線データ送受信)対応の新型車に対して、次いで 2024 年 7 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ます。

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、仕組み、管理・運用、維持・改善)が求められます。

7.1.3. 医療機器分野におけるセキュリティにかかわる法規制

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ます。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ます。

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ます。

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りました。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ります。

[18] 車両のソフトウェア更新にかかわる国際標準規格として、ISO/DIS 24089 が 2022 年 1 月に発行されています。未だ国際標準のドラフト(草案)段階のものですが、今後、国際標準規格として改訂・発行されることが想定されます。

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ます。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す。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、米国が主導しています。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 が参照されています。

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)が求められます。

7.1.4. 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

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ます。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す。

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・施行されています。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ます。

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ます。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 分野を指します。

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ます。

7.2. セキュリティの標準規格／ガイドラインにかかわる補足

本節では、2.1.2.3 節で言及した、製造業／工場の FA システム及び製品のセキュリティにかかわる代表的な標準規格／ガイドラインを紹介しておきます。

7.2.1. 国際標準規格

国際標準を制定することを目的に設立された国際的な団体 ISO(International Organization for Standardization)や IEC(International Electrotechnical Commission)により規定された規格です。サイバーセキュリティに関しては、IEC の規格として規定されることが多いですが、IT 関連などの一部は、IEC と ISO が連携して規定されるものもあります。

(a) 共通的で代表的な規格

- **IEC 62443**：産業自動化・制御システムの運用・管理プロセス面から、システムおよび構成要素の技術面まで、全体のサイバーセキュリティを規定
- **ISO/IEC 27000 シリーズ(ファミリー)**：情報セキュリティのマネジメントを規定
- **IEC 61508**：電気／電子システム及び製品の機能安全を規定

(b) 分野ごとの規格

- **ISO/SAE 21434**：自動車のサイバーセキュリティリスク管理を規定
- **ISO 14971**：医療機器のリスク管理及びセキュリティを規定
- **IEC 62278**：鉄道システムの信頼性、可用性、保全性、及び安全性を確保するためのマネジメントを規定。RAMS 規格とも呼ばれる
  (RAMS: Reliability, Availability, Maintainability, Safety)

7.2.2. 海外の規格・ガイドライン

日本国内で参照されることが多いものとして、米国の規格と、EU(欧州)として規定されているものがあります。さらに、国ごとに独自の規格があります。

ここでは、米国と EU について代表的なものを示します。

A) 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ります。

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

・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す。

「識別－防御－検知－対応－復旧」に分類して提示しています。

・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ります。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ります。下記に代表的なものを記載します。

・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

B) 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ます。

・**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す。

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ます。EU 各国はこの指令を基に、自国の規則を作成します。なお、2020 年 12 月に改訂が提案され、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)が強化される予定です。

・**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す。

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ます。なお、EU 圏で共通の規則となります。

7.2.3. 国内の方針・ガイドライン

日本国内でも、政府や業界などから、方針やガイドラインが発行されています。

(a) 政府・省庁

表 7-1 国の方針・ガイドライン

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	日本国のサイバーセキュリティに関する基本的な理念、及び諸施策の目標と実施方針を示すもの。 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	サイバー攻撃から企業を守る観点で、経営者が認識すべき「3 原則」、及び経営者が情報セキュリティ対策の責任者となる担当幹部(CISO 等)に指示すべき「重要 10 項目」をまとめたもの。
	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)	サイバー空間とフィジカル空間を融合させ実現される「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したもの。
	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にかかわる考え方を整理したもの。

発行者	文書名	概要
	「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」 「【別冊３】検証人材の育成に向けた手引き」	機器のセキュリティを検証する際に検証サービス事業者及び検証依頼者が実施すべき事項や留意すべき事項等を整理したもの。 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し、検証サービス事業者が実施すべき脅威分析の手法、検証項目、検証の流れを示す。 別冊２は、機器メーカの開発者の観点から、代表的な検証手法を解説するとともに、機器メーカが実施すべき事項や用意すべき情報等を示す。 別冊３は、検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取り組みを示す。
	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)	制御システムのセキュリティ リスク分析を実施するための手順や手引きを示すもの。
	制御システム　セーフティ・セキュリティ要件検討ガイド (IPA：情報処理推進機構)	制御システムの開発者が検討すべき「安全性を確保しつつ、セキュリティ対策を講じるための検討ポイント」を整理し、その検討手順を示すもの。

発行者	文書名	概要
	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 製品の開発者が考慮すべきリスクや対策を指針として明確化したもの。
	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したもの。
	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 指針を提示するもの。
	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するもの。
総務省	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するもの。

(b) 業界

表 7-2 業界の方針・ガイドライン

発行者	文書名	概要
経団連	経団連サイバーセキュリティ経営宣言	サイバーセキュリティ対策の強化に積極的に取り組むことが経営の最重要課題と捉え、経営層の理解を促進するとともに、自ら変革を促す取り組みの一環として、サイバーセキュリティ対策に取り組む覚悟を表明したもの。
	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	米国インターネット・セキュリティ・アライアンスと全米取締役協会が発行した「企業の取締役向けサイバーリスクハンドブック(Cyber Risk Oversight Director's Handbook)」及びその英国版を基に、日本版として作成したもの。サイバーリスクの影響を管理・軽減するために、取締役が取り組むべき5つの原則を提示している。
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	ビルシステムにおけるサイバーセキュリティ対策の着眼点や具体的対策要件を整理したもの。
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を規定したもの。

発行者	文書名	概要
	スマートメーターシステム 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、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を規定したもの。
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示すもの。
	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	小売電気事業者がサイバーセキュリティ対策を実践していくための指針として、「サイバーセキュリティ経営ガイドライン」における 10 項目の実践規範を中心に、小売電気事業者における、より具体的な解釈及び実践ポイントを整理したもの。
一般社団法人 日本自動車工業会	自工会／部工会・サイバー セキュリティガイドライン	自動車メーカやサプライチェーンを構成する各社に求められる自動車産業固有のサイバーセキュリティリスクを考慮した、対策フレームワークや業界共通の自己評価基準を明示したもの。
一般社団法人 重要生活機器連携 セキュリティ 協議会	CCDS 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。

発行者	文書名	概要
(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、具体的なセキュリティ対策指針と要件を定義したもの。
経済産業省	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が考慮すべき最低限の対策を整理したもの。
国土交通省	鉄道分野における 情報セキュリティ確保に係る 安全ガイドライン	鉄道分野の特性に応じ、必要な又は望ましい情報セキュリティ対策の水準を明示し、個々の鉄道関連事業者が自主的に取り組む PDCA サイクルに沿った対策の実施や検証に当たっての目標を定めたもの。
Edgecross コンソーシアム	Edgecross ユーザ向け セキュリティガイドライン	エッジコンピューティング領域のソフトウェアプラットフォーム「Edgecross」を利用する FA システム、Edgecross 搭載 PC、及びこれらを繋ぐネットワークにおけるセキュリティ対策の推奨を提示するもの。

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)	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。
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。

7.3. 各種ステークホルダからのセキュリティ要求にかかわる補足

本節では、2.1.2.4 節で言及した、製造業／工場の FA システム及び製品のセキュリティにかかわる各種ステークホルダからの要求内容を、より詳しく紹介しておきます。

ステークホルダとして、国・自治体、業界、市場・顧客、取引先、出資者を取り上げ、それぞれの要求内容を示します。

7.3.1. 国・自治体からの要求

FA システムのセキュリティ対策を検討・企画するときに、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ります。

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ります。

また、経済産業省「**サイバーセキュリティ経営ガイドライン**」には、「セキュリティ投資は必要不可欠かつ経営者としての責務である」と明記されており、「経営者が認識すべき 3 原則」と「サイバーセキュリティ経営の重要 10 項目」がまとめられています。

さらに、**国家・経済安全保障**の観点から、重要インフラにおいては、セキュリティ対策が義務付けられる方向となっており、重要インフラを構成する製品にかかわるセキュリティ対策も義務付けられることになる見通しです。その際に、経営陣主導の体制整備や対処計画づくりを求めるとともに、サプライチェーンで使用する機器の安全確保も要請することが明記される見通しとなっています。

一方で、国や自治体と、FA 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ります。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ようになってきています。

また、グローバルで要求されている環境保護やカーボンニュートラルを実現するために、国や自治体が工場の DX を促進させる動きが加速しており、工場 DX を実現するためには、セキュリティ対策は欠かせないものとなっています。

なお、要求ではありませんが、セキュリティ攻撃を受けた場合の連絡先(警察、関係省庁など)、及び連絡ルールを確認しておく必要があります。

7.3.2. 業界からの要求

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 原則を示しています。

東京商工会議所や大阪商工会議所などでは、会員企業のサイバーセキュリティ対策を支援し、企業の経営課題としてセキュリティにかかわる取り組みを求めています。

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するなど、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・要求されています。

自動車業界では、自工会(日本自動車工業会)や部工会(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が策定されたり、J-Auto-ISAC(Japan Automotive ISAC)によりセキュリティ情報収集・分析・共有が促進されたりするなど、自工会／部工会を中心にセキュリティにかかわる取り組みが推進・要求されています。

また、国際的には、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 が規定されており、適合が要求されています。

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ます。

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ます。

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ます。

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・要求されています。

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ます。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 が管理しています。

今後、**重要インフラ分野**などでも、同様に業界／分野向けのセキュリティガイドラインが策定されたり、ISAC によりセキュリティ情報収集・分析・共有が促進されたりするなど、セキュリティにかかわる取り組みが推進・要求されていくことは間違いないでしょう。

なお、日本で重要インフラとは、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 分野を指します。

7.3.3. 市場・顧客からの要求

FA 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ります。

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、セキュリティリスクが増大している環境の中、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ます。

産業制御システムのセキュリティにかかわる標準規格の面では、「IEC62443」が、産業制御システムを利用する事業者向け、構築するインテグレータ向け、コンポーネントを製造する機器ベンダ向けに、それぞれのセキュリティにかかわる要件を規定しています。

産業制御システムのセキュリティにかかわるガイドラインの面では、経済産業省が産業サイバーセキュリティ研究会の WG1(制度・技術・標準化)において、サプライチェーン全体のセキュリティ確保を目的とした「**サイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)**」を策定・発行するとともに、WG1 配下の産業分野別 SWG にて、産業分野別のセキュリティ対策ガイドラインを策定・公開しています。

近年の例では、外部からの利用者を認証する手段として、所有物・知識・生体識別情報のうちの 2 要素以上を組み合わせた多要素認証を求められますし、ネットワークに接続する製品においては、デフォルトの ID やパスワードを変更する運用を必須とすることなど、取引先からの調達要件にセキュリティ関連要件の記載が含まれる場合があります。

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できます。

・FA 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、具備すべき要件を示される場合があります。

・情報管理など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 FA 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があります。

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ります。

・製品に関するセキュリティ

製品として、世の中で一般的な水準のセキュリティ機能を具備している必要があります。また、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を担保する必要があります。

いずれも、製品の企画段階から、設計、製造、検査、出荷・配送、導入、運用、保守、廃棄までのライフサイクル全般にわたり、セキュリティ要件を確認し実現する必要があります。

7.3.4. 取引先からの要求

FA 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ります。

サプライチェーンリスク対策の面では、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含め繋がっており、影響を及ぼすと捉え、チェーン全体としてセキュリティを確保することが求められるようになってきています。昨今の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・侵入する事例も増えているからです。

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ことが増えています。

また、グローバルで要求されている環境保護やカーボンニュートラルを実現するために、取引先が工場の DX を推進する動きが加速しており、取引先自らの工場だけでなく、エンジニアリングチェーン、サプライチェーン、バリューチェーンを連携させた工場 DX の実現に協力することを要求されることが増えています。工場 DX を実現するためには、セキュリティ対策は欠かせないものとなっています。

7.3.5. 出資者からの要求

FA 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ります。

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るようになっています。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・公表しています。

また、グローバルで要求されている環境保護やカーボンニュートラルを実現するために、出資者が工場の DX を要求する動きが加速しており、工場 DX を実現するためには、セキュリティ対策は欠かせないものとなっています。

7.4. セキュリティ対策レベルにかかわる補足

本節では、セキュリティ対策レベルにかかわる補足的な内容を紹介しておきます。

まず、代表的なセキュリティ対策レベル評価基準を紹介します。次に、これらの評価基準を参考にしたセキュリティ対策レベルの定義例を示します。

7.4.1. 代表的なセキュリティ対策レベル評価基準

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、①IEC 62443 におけるセキュリティレベル、②NIST の「サイバーセキュリティフレームワーク(Cyber Security Framework)」における評価基準、及び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)」における評価基準を説明します。

①IEC 62443

5.1.3 節では「セキュリティ要求レベル」を「業務の重要度」×「現状の脅威レベル」として表現しましたが、IEC 62443 におけるセキュリティレベルは「脅威レベル」だけに着目します。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、脅威レベルを評価します。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として評価します。

表 7-3 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します。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します。

②NIST サイバーセキュリティフレームワーク(Cyber Security Framework)

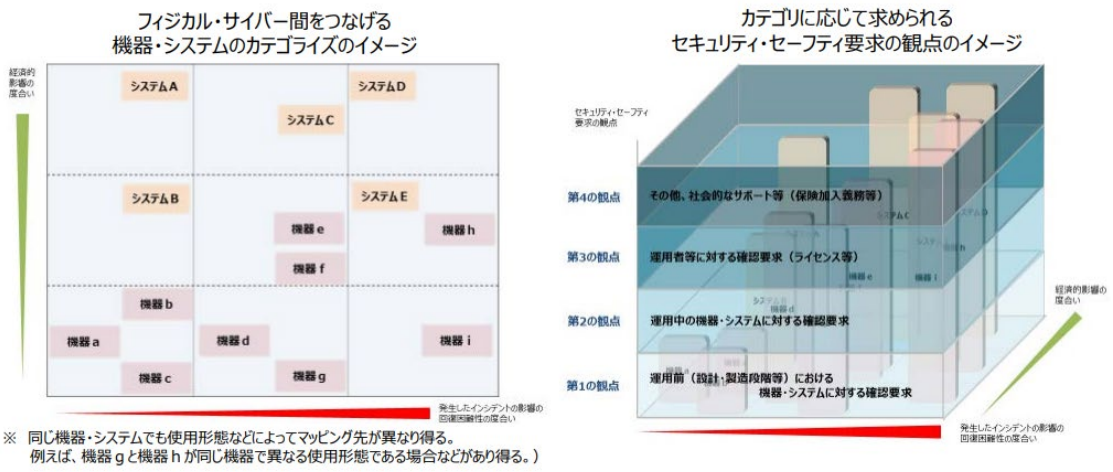
米国 NIST(National Institute of Standards and Technology)のサイバーセキュリティフレームワークでは、マネジメントの成熟度を軸にしたレベル評価となります。低いレベルは、個々人(あるいは個別組織やプロジェクト)の裁量をベースに実施している状態を表しています。高いレベルは、PDCA のマネジメントサイクルを適時実施し、サイクルの見直しを実施していることを表しています。

表 7-4 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

④ 経済産業省 IoT セキュリティ・セーフティ・フレームワーク

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、「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)」で表現します。



出典：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 7-1 IoT セキュリティ・セーフティ・フレームワークにおける
セキュリティ・セーフティ要求レベルのカテゴライズ

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 レベルで表現します。

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 レベルで表現します。

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ます。さらに、技術的対策ばかりではなく、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みを提供します。

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

7.4.2. セキュリティ対策レベルの定義例

セキュリティ対策レベルは、これらの基準などを参考に、各事業者がセキュリティ対策を実施・維持するために有用となるレベル定義を検討します。このセキュリティ対策レベルは、事業者にとって対策を推進するうえでの指標ともなります。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、実施マネジメントができるようなレベルを定義することがポイントとなります。

ここでは、セキュリティ施策の 3 つの実施先である「システム」「運用」「マネジメント」ごとに整理をすることにします。

（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ります。以下に、設定するレベルの例を示します。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ください。

表 7-5 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 7-6 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ります。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、レベルを設定します。

表 7-7 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 7-8 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ります。以下に、設定するレベルの例を示します。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ください。

表 7-9 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 7-10　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

7.5. インシデント対応ガイドラインにかかわる補足

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り組みのことを「セキュリティインシデント対応」と呼びます。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、以下に挙げる既存のガイドラインにて詳しく整理されていますので、そちらを参照してください。

表 7-11 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

No.	発行者	文書名	概要、参照先
4		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		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

No.	発行者	文書名	概要、参照先
6		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

No.	発行者	文書名	概要、参照先
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

8. 付録

8.1. チェックリスト

本節では、本ガイドラインの実施状況を確認するためのチェック項目を示します。

これらの項目を、以下の達成度に応じて評価することで、工場セキュリティの現状を把握することができます。

・達成度１：「未実施」

・達成度２：「一部実施」

・達成度３：「実施済み」

・達成度４：「実施済みで、管理手順を文書化・自動化し、定期的に対策を見直し」

・達成度５：「実施済みで、管理手順を文書化・自動化し、随時見直し」

表 8-1 チェックリスト

カテゴリ	番号	確認項目	参照
組織的対策	1-1	工場システムのセキュリティについて、決裁者（工場長、カンパニー長等）または経営層が脅威や必要性の認識をもっており、十分な予算・人員配置などの協力を得られる状態にある。	5.1.1 5.1.2
	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との協力・連携態勢が取られている。	5.1.4 (1) 5.2.4.1.3 5.2.4.2.2
	1-3	工場システムのセキュリティ検討組織があり、担当者がアサインされており、責任と業務内容が明確化されている。	5.1.4 (1) 5.2.4.2.2
	1-4	工場のセキュリティ事故発生時の担当者がアサインされていて、責任と業務内容が明確化されている。	5.1.4(1) 5.2.4.2.2

カテゴリ	番号	確認項目	参照
	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現場教育を行っている。	5.1.1 5.1.4(1) 5.2.4.2.1
運用的対策	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定量的に検討している。（リスクアセスメント実施）	5.2.1 表 5-8 5.2.4.1
	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。	5.2.4.1.2 表 5-17
	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。	5.2.4.1.2 表 5-17
	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。	5.2.4.1.1
	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。	5.2.4.1.1
	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、システム構成図が存在し、変更管理を実施している。	5.2.4.1.2 表 5-17 [接続機器]
	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。	5.2.4.1.2 表 5-17 [接続機器]
	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。	5.2.4.1.1

カテゴリ	番号	確認項目	参照
	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。	5.2.4.1.2 表 5-17 [媒体]
	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）	5.2.3.1 5.2.3.2 表 5-13 [利用者制限]
	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。	5.2.4.1.2 表 5-17 [利用者]
	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。	5.2.4.1.2 表 5-17 [媒体] 5.2.5(2)
	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。	5.2.3.2 表 5-13 [バックアップ(データ、機器)] 5.2.4.1.1 5.2.4.1.2 表 5-17 [装置・機器バックアップ]
技術的対策	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許可リスト(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。	5.2.3.2 表 5-12 [実行プログラム制御], [脆弱性対策] 5.2.4.1.1

カテゴリ	番号	確認項目	参照
	3-2	アプリケーション/オペレーティングシステム（OS）にはセキュリティパッチを適用している。もしくは代替策でリスクを低減させている。	5.2.3.2 表 5-12 [脆弱性対策]
	3-3	制御端末のオペレーティングシステムの使用サービス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。	5.2.3.2 表 5-13 [通信制限], [不要ポート], [利用ポート], [利用者制限], [実行プログラム制御]
	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）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補完してもよい。	5.2.2.6 表 5-9,10 5.2.2.7 5.2.4.1.2 表 5-17 [入退場者・入退室者]
	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）	5.2.3.1 表 5-12 [構成分割], [内部秘匿]
	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 要素認証が望ましい）やネットワーク侵入防護などの保護対策を行っている。	5.2.3.2 表 5-13 [利用者制限], [通信/接続機器認証]

カテゴリ	番号	確認項目	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。	5.2.3.1 表 5-12 [通信データ制限], [通信監視・制御], [脆弱性対策]
	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。	5.2.3.1 表 5-12 [ログ取得] 5.2.3.2 表 5-13 [ログ取得]
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の制御システムベンダー・構築事業者との連絡・連携態勢が取られている。	5.2.5(1),(4)
	4-2	工場システムのメンテナンス等にかかわる外部事業者向けのセキュリティ教育を実施している。	5.2.5(2),(4)
	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・構築業者との関係を維持している。	5.2.5(1)
	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。	5.2.5(2),(3)
	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みたしているかを判定するプロセス、または受け入れ検査がある。	5.2.3.3 5.2.5(3)

カテゴリ	番号	確認項目	参照
	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。	5.2.3.3 5.2.5(3)

8.2. 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す。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つに分けられます。

(ア)サプライヤのセキュリティマネジメント体制

(イ)製品・サービスのセキュリティ対策

(ウ)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す。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ます。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（IPA）」、「サイバーセキュリティ経営ガイドライン（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）」などを活用できます。

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（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す。②は、製品・サービスが備えるべきセキュリティ要件です。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ります。このような機能の列挙に、本ガイドラインを活用すると、調達仕様書を簡潔に記すことができます。

例２：PLC の調達仕様書のセキュリティ要件指定の例

X.X　PLC が備えるべきセキュリティ要件
「工場セキュリティガイドライン（経済産業省)」の Y.Y.Y に記載のセキュリティ要件を充たすこと。機器単体で充たせない項目は、必要な追加対策を明示すること。

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、ガイドライン記載の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ります。その場合、サプライヤから情報を取得して、調達する機器がみたしている要件と、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す。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ます。

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す。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す。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りますが、本ガイドラインでは、考慮すべき観点を示しますので、必要に応じて取捨選択してください。

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　製造時のセキュリティ

「工場 FA セキュリティガイドライン（経済産業省）」に準じた

セキュリティ対策を実施すること。

X.X.2　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

製品調達にかかわるセキュリティ要件は、ロボット革命・産業 IoT イニシアティブ協議会(RRI: Robot Revolution & Industrial IoT Initiative)の作成した「RRI サプライチェーン質問票」[19]が参考になります。

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

8.3. 関連／参考資料

欧州連合(EU) 欧州議会および欧州理事会

「EU 一般データ保護規則（GDPR: General Data Protection Regulation)」:

【概要】

欧州連合(EU)を含む欧州経済領域(EEA)内の全ての個人のために、基本的人権である個人データやプライバシの保護を強化し統合することを意図した、個人データの処理および移転に関する規則。EEA 域外への個人情報の輸出も対象としている。

【参照先】

JETRO「EU 一般データ保護規則(GDPR)について」:

https://www.jetro.go.jp/world/europe/eu/gdpr/

個人情報保護委員会「GDPR（General Data Protection Regulation：一般データ保護規則）」:

https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

EUR-Lex“Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32016R0679

欧州連合(EU) 欧州委員会

「EU NIS 指令（Directive on Security of Network and Information systems)」:

【概要】

欧州連合(EU)全体にわたり適用される、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。2016 年 8 月 8 日に発効され、各加盟国は 2018 年 5 月 9 日までに法制化している。

基幹サービス運営者(産業システムを含む)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。2020 年 12 月に改訂が提案され、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)が強化される予定。

【参照先】

JETRO「EU デジタル政策の最新概要」(2021 年 10 月) Ⅱ-4-(3):

https://www.jetro.go.jp/ext_images/_Reports/01/0a88cad7cdac3e5a/20210038.pdf

国立国会図書館「ネットワーク・情報システムの安全に関する指令(NIS 指令)

―EU のサイバーセキュリティ対策立法―」:

https://dl.ndl.go.jp/view/download/digidepo_11152345_po_02770001.pdf?contentNo=1

ENISA“NIS Directive”:

https://www.enisa.europa.eu/topics/nis-directive

European Parliament“The NIS2 Directive: A high common level of cybersecurity in the EU”:

https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

EUR-Lex “Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”:

https://eur-lex.europa.eu/eli/dir/2016/1148/oj

EUR-Lex “Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148”:

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020PC0823

国際電気標準会議(IEC: International Electrotechnical Commission)

“IEC 61508”:

【概要】

電気／電子／プログラム可能な電子システム及び製品のライフサイクルにわたる機能安全を確保するための要件を規定した国際標準規格。

【参照先】

JQA「安全規格の紹介 機能安全とは(IEC 61508 の場合)」:

https://www.jqa.jp/service_list/fs/file/techdata_61508.pdf

JEMIMA「機能安全規格の技術解説」:

https://www.jemima.or.jp/activities/file/func_safety_201311.pdf

IPA「組込みシステムの安全性向上の勧め(機能安全編)」:

https://www.ipa.go.jp/files/000005118.pdf

IEC“Safety and functional safety”:

https://www.iec.ch/functional-safety

IEC“IEC 61508-1:2010”:

https://webstore.iec.ch/publication/5515

“IEC 62278”:

【概要】

鉄道システムのライフサイクルにわたる信頼性、可用性、保全性、及び安全性を確保するための管理プロセスにかかわる要件及び評価手法を規定した国際標準規格。RAMS 規格とも呼ばれる。(RAMS: Reliability, Availability, Maintainability, Safety)

関連規格として、IEC 62279, 62280, 62425 などがある。

【参照先】

(株)三菱総合研究所 石原嘉一「鉄道等の大規模システムにおける安全性の示し方」

(安全工学 Vol.49 No.3 (2010)):

https://www.jstage.jst.go.jp/article/safety/49/3/49_160/_pdf/-char/ja

IEC“IEC 62278:2002”:

https://webstore.iec.ch/publication/6747

“IEC 62443”:

【概要】

産業自動化・制御システム(IACS)のセキュリティをライフサイクルにわたり確保するための要件を規定した国際標準規格。運用・管理プロセス面から、システムおよび構成要素の技術面まで、全体のサイバーセキュリティ要件を規定している。

【参照先】

IPA「制御システムセキュリティへの対応」:

https://www.ipa.go.jp/files/000066496.pdf

IEC“Understanding IEC 62443”:

https://www.iec.ch/blog/understanding-iec-62443

IEC System Committee Smart Energy“IEC 62443”:

https://syc-se.iec.ch/deliveries/cybersecurity-guidelines/security-standards-and-best-practices/iec-62443/

IEC“IEC TS 62443-1-1:2009”:

https://webstore.iec.ch/publication/7029

国際標準化機構(ISO: International Organization for Standardization)

“ISO 14971”:

【概要】

医療機器(医療機器として機能するソフトウェアや体外診断用医療機器を含む)のライフサイクルにわたるリスク管理及びセキュリティの要件を規定した国際標準規格。

【参照先】

JETRO ビジネス短信“ISO、医療機器製造業者向けの規格をウェブで紹介”:

https://www.jetro.go.jp/biznews/2020/07/fc3b777a901bc8fa.html

JIRA“医療機器のリスクマネジメント規格について”:

https://www.pref.kyoto.jp/yakumu/documents/kouen4.pdf

ISO“ISO 14971:2019”:

https://www.iso.org/standard/72704.html

“ISO/SAE 21434”:

【概要】

自動車(路上走行車両)の電気／電子システム(コンポーネントやインタフェースを含む)のライフサイクルにわたるサイバーセキュリティリスク管理のための要件を規定した国際標準規格。

因みに、“SAE(Society of Automotive Engineers) International”は、航空宇宙や自動車などモビリティ産業の専門家を会員とする米国の非営利団体で、同領域に関する標準化や教育の活動を推進している。

【参照先】

JETRO ビジネス短信「ISO、自動車サイバーセキュリティの国際規格発行」:

https://www.jetro.go.jp/biznews/2021/09/3e7758d46c78058a.html

ISO“ISO/SAE 21434:2021”

https://www.iso.org/standard/70918.html

“ISO/IEC 27000 シリーズ(ファミリー)”：

【概要】

情報セキュリティマネジメントシステム(ISMS)にかかわる要件及びガイドラインを規定した国際標準規格群。

【参照先】

JIPDEC“ISO/IEC 27000 ファミリーについて ～ISO/IEC JTC1/SC27/WG1 における検討状況～”：

https://www.jipdec.or.jp/project/smpo/u71kba000000jjgv-att/27000family_20191220.pdf

ISO“ISO/IEC 27001 Information Security Management”：

https://www.iso.org/isoiec-27001-information-security.html

“ISO/IEC 30147”：

【概要】

IoT 製品やサービスにおける信頼性(trustworthiness)の実装・保守のためのシステムライフサイクルプロセスを規定した国際標準規格。「IoT セキュリティガイドライン」や「つながる世界の開発指針」の内容に基づいている。

【参照先】

経済産業省「IoT 製品・システムを安全に実装するための国際規格が発行されました」：

https://www.meti.go.jp/press/2021/06/20210621004/20210621004.html

IPA「IoT 製品・サービスにセーフティ・セキュリティ等を実装するプロセスが国際標準として出版 ～日本提案の規格が国際標準化団体 ISO/IEC にて出版～」：

https://www.ipa.go.jp/ikc/info/20210621.html

IEC“ISO/IEC 30147:2021 Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes”：

https://webstore.iec.ch/publication/62644

NIST(米国国立標準技術研究所)“Cyber Security Framework (CSF): Framework for Improving Critical Infrastructure Cybersecurity”:

【概要】

産業(とりわけ重要インフラ関連産業)におけるサイバーセキュリティリスク管理・低減のための推奨手法を纏めたもの。組織の自発的な取り組みを促す位置づけのものだが、グローバルデファクト標準として広く参照されている。

識別(Identify)、防御(Protect)、検知(Detect)、対処(Respond)、復旧(Recover)という 5 つの機能に分け整理している。また、4 段階(部分的、リスクを認識、繰り返し可能、適応)の成熟度評価基準を定義している。

【参照先】

IPA「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」:

https://www.ipa.go.jp/files/000071204.pdf

NIST“Cybersecurity Framework”:

https://www.nist.gov/cyberframework

NIST“Framework for Improving Critical Infrastructure Cybersecurity”:

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST“NISTIR 8183 Rev.1: Cybersecurity Framework Version 1.1 Manufacturing Profile”:

【概要】

NIST CSF を製造環境に適用するときの実装の詳細を提供するもの。製造業の目標やベストプラクティスと整合した、サイバーセキュリティリスク低減のためのロードマップとして用いることができる。

製造業共通の目標として、環境安全、人的安全、生産目標、製品品質、及び機密情報の維持を挙げている。

【参照先】

NIST“NISTIR 8183 Revision 1: Cybersecurity Framework Version 1.1 Manufacturing Profile”:

https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf

NIST“NISTIR 8183A Volume 1:

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 1 – General Implementation Guidance”:

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8183A-1.pdf

NIST“NISTIR 8183A Volume 2:

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 2 – Process-based Manufacturing System Use Case”:

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8183A-2.pdf

NIST“NISTIR 8183A Volume 3:

Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: Volume 3 – Discrete-based Manufacturing System Use Case”:

https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8183A-3.pdf

NIST **“SP 800 シリーズ”**:

【概要】

コンピュータセキュリティに関するガイドライン、推奨、技術仕様、活動報告などを提供するもので、当初は米国連邦政府関連の情報及び情報システムのセキュリティやプライバシにかかわる要件を提示するために整備されたが、現在では米国連邦政府関連以外でも自発的なグローバルデファクト標準として広く参照されている。

【参照先】

IPA「セキュリティ関連 NIST 文書　翻訳文書　SP800 シリーズ」:

https://www.ipa.go.jp/security/publications/nist/index.html

NIST Computer Security Resource Center“SP(Special Publications) 800 series”:

https://csrc.nist.gov/publications/sp800

内閣サイバーセキュリティセンター(NISC)

「**サイバーセキュリティ戦略**」:

【概要】

サイバーセキュリティ基本法 第 12 条の規定に基づき定められた、日本国のサイバーセキュリティに関する基本的な理念、及び諸施策の目標と実施方針を示すもの。

【参照先】

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の概要」:

https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-gaiyou.pdf

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のパンフレット」:

https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-c.pdf

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」:

https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf

内閣サイバーセキュリティセンター(NISC) サイバーセキュリティ戦略本部

「**重要インフラの情報セキュリティ対策に係る行動計画**」:

【概要】

「サイバーセキュリティ戦略」を踏まえ、サイバーセキュリティ基本法 第 14 条及び第 26 条第 1 項第 5 号の規定に基づき策定された、日本国の重要インフラサービスの安全かつ持続的な提供を実現するためのセキュリティ対策の実施方針や具体的な取り組み内容を示すもの。

なお、2020 年 1 月に決定・公表された第 4 次行動計画を改訂する第 5 次行動計画(案)に関する意見募集が 2022 年 2 月末まで実施され、近く決定・公表される見込み。

【参照先】

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本部

「重要インフラの情報セキュリティ対策に係る第 4 次行動計画の概要」:

https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_abst_r1.pdf

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本部

「重要インフラの情報セキュリティ対策に係る第 4 次行動計画」:

https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_r2.pdf

内閣サイバーセキュリティセンター 重要インフラグループ

「「重要インフラのサイバーセキュリティに係る行動計画(案)」に関する意見の募集について」:

https://www.nisc.go.jp/policy/group/infra/pubcom_aprev.html

総務省

「**サイバーセキュリティ対策情報開示の手引き**」:

【概要】

企業が各種ステークホルダからの信頼を得るための重要な取り組みの一つとなっている、サイバーセキュリティ対策の実施状況に関する情報開示の在り方の参考になることを目的に、開示書類におけるサイバーセキュリティ対策の開示項目の例を示すとともに、既に公開されている開示書類の事例集を掲載したもの。

【参照先】

総務省 サイバーセキュリティ統括官「サイバーセキュリティ対策情報開示の手引き」:

https://www.soumu.go.jp/main_content/000630516.pdf

経済産業省、厚生労働省、文部科学省

「**製造基盤白書(ものづくり白書)**」:

【概要】

ものづくり基盤技術振興基本法 第 8 条に基づき作成・公表されている、政府がものづくり基盤技術の振興に関して講じた施策に関する年次報告書。

【参照先】

経済産業省「製造基盤白書(ものづくり白書)」:

https://www.meti.go.jp/report/whitepaper/index_mono.html

経済産業省「2018 年版 ものづくり白書」:

https://www.meti.go.jp/report/whitepaper/mono/2018/index.html

経済産業省「2020 年版 ものづくり白書」:

https://www.meti.go.jp/report/whitepaper/mono/2020/index.html

経済産業省「2021 年版 ものづくり白書」:

https://www.meti.go.jp/report/whitepaper/mono/2021/index.html

経済産業省

「サイバーセキュリティ経営ガイドライン」:

【概要】

大企業及び中小企業(小規模事業者を除く)の経営者を対象に、経営者のリーダ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に、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3 原則」、及び経営者が情報セキュリティ対策を実施する上で責任者となる担当幹部(CISO 等)に指示すべき「重要 10 項目」をまとめたもの。

【参照先】

経済産業省「サイバーセキュリティ経営ガイドライン」:

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

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（CPSF)」:

【概要】

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実現される「Society5.0」、様々なつながりによって新たな付加価値を創出する「Connected Industries」における新たなサプライチェーン(バリュークリエイションプロセス)全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したもの。

【参照先】

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」:

https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

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)
～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～」:

【概要】

IoT や AI によって実現される「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にかかわる考え方を整理したもの。

フィジカル空間とサイバー空間をつなげる機器・システムに潜むリスクを、発生したイ

ンシデントによる「影響の回復困難性の度合い」と「経済的影響の度合い」の 2 軸で整理し、それに対して求められるセキュリティ・セーフティ要求を、「運用前(設計・製造段階等)における機器・システムに対する確認要求」、「運用中の機器・システムに対する確認要求」、「運用者等に対する確認要求」、「その他、社会的なサポート等」の 4 つの観点から整理する考え方を提示している。

【参照先】

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～」:

https://www.meti.go.jp/press/2020/11/20201105003/20201105003-1.pdf

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】脅威分析及びセキュリティ検証の詳細解説書」、

「【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」、

「【別冊 3】検証人材の育成に向けた手引き」:

【概要】

セキュリティ検証サービスの高度化を目的とし、機器のセキュリティを検証する際に検証サービス事業者及び検証依頼者が実施すべき事項や、二者間のコミュニケーションにおいて留意すべき事項等を整理したもの。信頼できる検証サービス事業者を判断するための基準も提示している。

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脅威分析の手法や実施すべき検証項目、検証の流れを網羅的かつ詳細に示したもの。

別冊 2 は、機器メーカの開発者の観点から、検証フェーズを中心に「検証依頼前に実施しておくべき内容」、「検証依頼時に知っておきたい内容」、「検証完了後に実施する内容」の三つに分類し、代表的な検証手法を解説するとともに、機器メーカが実施すべき事項や用意すべき情報等、意図した検証を依頼するために必要な事項を詳細に示したもの。攻撃手法への対策例や、検証結果を踏まえたリスク評価等の対応方針も示している。

別冊 3 は、検証人材に求められるスキル・知識を示し、それらのスキル・知識を獲得するために望まれる取り組みを示したもの。検証人材のキャリアを構想・設計する上で考慮すべき観点を示し、検証人材のキャリアの可能性も示している。

【参照先】

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」:

https://www.meti.go.jp/press/2021/04/20210419003/20210419003-1.pdf

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】脅威分析及びセキュリティ検証の詳細解説書」:

https://www.meti.go.jp/press/2021/04/20210419003/20210419003-2.pdf

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 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」:

https://www.meti.go.jp/press/2021/04/20210419003/20210419003-3.pdf

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 3】検証人材の育成に向けた手引き」:

https://www.meti.go.jp/press/2021/04/20210419003/20210419003-4.pdf

経済産業省 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) ビルサブワーキンググループ

「**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**」:

【概要】

エレベータや空調など多くの制御系機器を有するビルシステムにおけるサイバーセキュリティの確保を目的に、サイバーセキュリティ対策の着眼点や具体的対策要件を体系的に整理したもの。

ビルシステムを構成するサブシステムに共通的なセキュリティ対策を整理した共通編の位置づけだが、ビルシステム全体管理にかかわる要素に加え、ビル内の場所ごと、機器ごとに想定されるセキュリティインシデント、リスク源、セキュリティ対策要件(ポリシ)を整理し提示している。さらに、ビルの設計、建設、竣工検査、運用、改修・廃棄というライフサイクルのフェーズごとに取るべき対策をより具体化し提示している。

【参照先】

経済産業省 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) ビルサブワーキンググループ

「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 第 1 版」:

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html

経済産業省、情報処理推進機構(IPA)

「**サイバーセキュリティお助け隊サービス制度**」:

【概要】

相談窓口、システムの異常監視、緊急時の対応支援、簡易サイバー保険など、中小企業に対するサイバー攻撃への対処を支援するサービスに不可欠な要件を纏めた「サイバーセキュリティお助け隊サービス基準」を IPA が 2021 年 2 月に策定。サービス審査登録機関の審査により当該基準を満たすと判定されたサービスには「サイバーセキュリティお助け隊マーク」の利用を許諾し、支援サービス事業の展開を後押しするとともに、SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)等を通して、産業界全体におけるサイバーセキュリティの取組みの一環として普及を促進する制度。

「サイバーセキュリティお助け隊サービス」として登録されたサービスのリストは、以下に示す参照先の IPA サイトに掲載されている。

【参照先】

情報処理推進機構(IPA)「サイバーセキュリティお助け隊サービス ユーザ向けサイト」:

https://www.ipa.go.jp/security/otasuketai-pr/

情報処理推進機構(IPA)「サイバーセキュリティお助け隊サービス制度」:

https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html

情報処理推進機構（IPA）

「情報セキュリティ 10 大脅威」：

【概要】

社会的に影響が大きかったと考えられる情報セキュリティにかかわる事案から、IPA が脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約 150 名のメンバからなる「10 大脅威選考会」が脅威候補に対して審議・投票を行い、決定したもので、解説書や簡易説明資料が提供されている。

【参照先】

情報処理推進機構(IPA)「情報セキュリティ 10 大脅威 2022」：

https://www.ipa.go.jp/security/vuln/10threats2022.html

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～」：

【概要】

重要インフラや産業システムの基盤となっている制御システムのセキュリティを抜本的に向上させるのに重要な位置付けとなるセキュリティリスク分析を、事業者が実施できるようにすることを目的に、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ともに、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。

併せて、リスク分析を補助する素材(ツール)として、リスク分析シート、脅威(攻撃方法)一覧、セキュリティ対策項目一覧、セキュリティ対策チェックリストも提供している。また、別冊として、ガイドを用いたリスク分析の実施例も提供している。

【参照先】

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 第 2 版

～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～」を公開」：

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

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 第 2 版

～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～」：

https://www.ipa.go.jp/files/000080712.pdf

情報処理推進機構(IPA)「制御システムに対するリスク分析の実施例 第 2 版
～制御システムのセキュリティリスク分析ガイド 別冊～」:
https://www.ipa.go.jp/files/000080715.pdf

情報処理推進機構（IPA）

「**制御システム　セーフティ・セキュリティ要件検討ガイド**」:

【概要】

制御システムの安全関連システムのセキュリティ向上を目的として、制御システムの設計・開発・運用に携わる開発者が検討すべき「安全性を確保しつつ、セキュリティ対策を講じるための検討ポイント」を整理し、その検討手順を具体的に示したもの。

併せて、ケーススタディによる解説も掲載し、脅威分析を実施する際の分析シートのテンプレートも添付している。

【参照先】

情報処理推進機構(IPA)「「制御システム セーフティ・セキュリティ要件検討ガイド」を公開
～安全関連システムのセキュリティ向上にむけて～」:
https://www.ipa.go.jp/sec/reports/20180319.html

情報処理推進機構(IPA)「制御システム セーフティ・セキュリティ要件検討ガイド 基本編」:
https://www.ipa.go.jp/files/000064728.pdf

情報処理推進機構(IPA)「制御システム セーフティ・セキュリティ要件検討ガイド ケーススタディ編」:
https://www.ipa.go.jp/files/000064729.pdf

情報処理推進機構（IPA）

「**つながる世界の開発指針**」:

【概要】

IoT 製品があらゆるモノとつながることを想定し、IoT 製品の開発者が開発時に考慮すべきリスクや対策を指針として明確化したもの。

IoT 製品を開発する企業全体の「方針」の策定、つながる場合のリスクの「分析」、リスクへの対策を行うための「設計」、製品導入後の「保守」や「運用」といった製品の開発ライフサイクル全体において考慮すべきポイントを全 17 の指針として明示し、指針ごとに取り組むための背景や目的、具体的なリスクと対策の例を解説している。

併せて、開発指針の実施状況を自己チェックできるように、指針とポイントを具体的な内容に落とし込んだチェックリスト(ひな形)を提供している。

【参照先】

情報処理推進機構(IPA)「「つながる世界の開発指針」を公開」:

https://www.ipa.go.jp/sec/reports/20160324.html

情報処理推進機構(IPA)「利用時の品質の観点を盛り込んだ「つながる世界の開発指針(第 2 版)」を発行」:

https://www.ipa.go.jp/sec/reports/20170630.html

情報処理推進機構(IPA)「つながる世界の開発指針～安全安心な IoT の実現に向けて開発者に認識してほしい重要ポイント～ 第 2 版」:

https://www.ipa.go.jp/sec/publish/tn16-002.html

情報処理推進機構 (IPA)

「「つながる世界の開発指針」の実践に向けた手引き [IoT 高信頼化機能編]」:

【概要】

「つながる世界の開発指針」にて明確化した指針のうち、技術面での対策が必要になる部分をさらに具体化し、IoT 機器・システム開発時のセーフティ要件とセキュリティ要件、そしてそれらを実現する機能を解説したもの。

【参照先】

情報処理推進機構(IPA)「開発者向け、安全安心な IoT 機器・システム開発のための「『つながる世界の開発指針』の実践に向けた手引き［IoT 高信頼化機能編］」の公開」:

https://www.ipa.go.jp/sec/reports/20170508.html

情報処理推進機構(IPA)「「つながる世界の開発指針」の実践に向けた手引き［IoT 高信頼化機能編］」:

https://www.ipa.go.jp/sec/publish/tn17-002.html

情報処理推進機構（IPA）

「つながる世界の品質確保に向けた手引き

～IoT 開発・運用における妥当性確認・検証の重要ポイント～」:

【概要】

「つながる世界の開発指針」の品質確保に関する事項を具体化したもの。開発者、保守者、品質保証者、運用者など、品質に携わるすべての担当者を読者対象とし、13 の品質確保の視点として検証に関する考慮事項をまとめている。

併せて、品質確保に向けた手引きの実施状況を自己チェックできるように、視点とポイントを具体的な内容に落とし込んだチェックリスト(ひな形)を提供している。

【参照先】

情報処理推進機構(IPA)「IoT 機器・システムの安全安心に向けた品質確保の手引きを公開

～検証の立場から考慮すべき重要事項を 13 の視点として提示～」:

https://www.ipa.go.jp/sec/reports/20180322.html

情報処理推進機構(IPA)「つながる世界の品質確保に向けた手引き

～IoT 開発・運用における妥当性確認・検証の重要ポイント～」:

https://www.ipa.go.jp/sec/publish/tn18-001.html

情報処理推進機構（IPA）

「自動車の情報セキュリティへの取組みガイド」:

【概要】

自動車システムで考えられる脅威と、それに対するセキュリティ対策を具体的に示すとともに、自動車本体や車載機器のライフサイクルの各段階(企画から廃棄まで)において、検討すべき情報セキュリティ上の取組み事項を纏めたもの。自動車セキュリティの確保に向けた自社の取組むべき内容を把握するとともに、情報セキュリティの取組みを強化するための指針を示している。

【参照先】

情報処理推進機構(IPA)「“セキュアな自動車”に向けて

「自動車の情報セキュリティへの取組みガイド」等を公開」:

https://www.ipa.go.jp/security/fy24/reports/emb_car/index.html

情報処理推進機構(IPA)「「自動車の情報セキュリティへの取組みガイド」第 2 版を公開」:

https://www.ipa.go.jp/security/iot/emb_car2.html

情報処理推進機構(IPA)「自動車の情報セキュリティへの取組みガイド 第 2 版」:

https://www.ipa.go.jp/files/000058198.pdf

情報処理推進機構（IPA）

「**中小企業の情報セキュリティ対策ガイドライン**」:

【概要】

中小企業および小規模事業者の経営者や情報管理の実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したもの。情報セキュリティ対策に取り組む際の、(1)経営者が認識し実施すべき指針、(2)社内において対策を実践する際の手順や手法をまとめている。

経営者編と実践編から構成されており、経営者編では、経営者が認識すべき「3 原則」と、経営者がやらなければならない「重要 7 項目の取組み」を示している。実践編では、すぐにできるところから始め、段階的にステップアップする進め方を示している。

併せて付録として、すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」などのひな形を提供している。

【参照先】

情報処理推進機構(IPA)「中小企業の情報セキュリティ対策ガイドライン」:

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

https://www.ipa.go.jp/files/000062413.pdf

https://www.ipa.go.jp/files/000055520.pdf

IoT 推進コンソーシアム、総務省、経済産業省

「IoT セキュリティガイドライン」:

【概要】

IoT 機器、システム、サービスの供給者及び利用者を対象として、サイバー攻撃などによる新たなリスクが、モノやその利用者の安全、個人情報・技術情報など重要情報の保護に影響を与える可能性があることを認識した上で、IoT 機器、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まとめたもの。IoT セキュリティ対策の 5 つの指針及び 21 の要点、ならびに利用者のためのルール 4 つを示している。

【参照先】

IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン ver1.0 概要」:
http://www.iotac.jp/wp-content/uploads/2016/01/04-IoT%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3ver1.0%E6%A6%82%E8%A6%81%EF%BC%88%E5%88%A5%E7%B4%99%EF%BC%92.pdf

IoT 推進コンソーシアム、総務省、経済産業省「IoT セキュリティガイドライン」:
https://www.soumu.go.jp/main_content/000428393.pdf

日本経済団体連合会(経団連)

「Society 5.0 実現に向けたサイバーセキュリティの強化を求める」提言:

【概要】

あらゆる産業のデジタル化によりモノ・ヒト・コトがデータでつながる社会「Society 5.0」の実現による価値創造と、危機管理(リスクマネジメント)の両面から、サイバーセキュリティ対策の強化に積極的に取り組むことが経営の最重要課題と捉え、社会的責任として、あらゆる企業や組織が、あらゆるステークホルダの連携のもとで、より具体的な対策の取り組みを進めるために、あらためて提言したもの。

経済界が全員参加で、自助・共助・公助・国際連携の視点で取り組むべき事項として、「①意識改革」、「②リソース確保(人材育成、情報共有、技術対策、投資促進)」、「③推進体制の整備」、「④法制度・規範の整備」を示している。

また、経団連自ら変革を促すアクションプランとして、「①経営層の理解促進」、「②広報・周知活動」、「③国際連携」の具体的な取り組みを推進することを示している。

【参照先】

日本経済団体連合会「Society 5.0 実現に向けたサイバーセキュリティの強化を求める」提言：

https://www.keidanren.or.jp/policy/2017/103.html

日本経済団体連合会(経団連)

「**経団連サイバーセキュリティ経営宣言**」：

【概要】

あらゆる産業のデジタル化によりモノ・ヒト・コトがデータでつながる社会「Society 5.0」の実現による価値創造と、危機管理(リスクマネジメント)の両面から、サイバーセキュリティ対策の強化に積極的に取り組むことが経営の最重要課題と捉え、経営層の理解を促進するとともに、自ら変革を促す取り組みの一環として、経済界が一丸となってサイバーセキュリティ対策に取り組む覚悟を表明したもの。

経済界が全員参加で取り組むべき事項として、「1. 経営課題としての認識」、「2. 経営方針の策定と意思表明」、「3. 社内外体制の構築・対策の実施」、「4. 対策を講じた製品・システムやサービスの社会への普及」、「5. 安心・安全なエコシステムの構築への貢献」の実践に努めることを宣言している。

【参照先】

日本経済団体連合会「経団連サイバーセキュリティ経営宣言」：

https://www.keidanren.or.jp/policy/2018/018.html

日本経済団体連合会(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 日本版)**」：

【概要】

米国インターネット・セキュリティ・アライアンスと全米取締役協会が発行した「企業の取締役向けサイバーリスクハンドブック(Cyber Risk Oversight Director's Handbook)」及びその英国版を基に、日本の法律や制度に応じて一部改変し、日本版として作成したもの。サイバーリスクの影響を管理・軽減するために、取締役が取り組むべき 5 つの原則を提示している。

【参照先】

日本経済団体連合会「サイバーリスクハンドブック」:

https://www.keidanren.or.jp/policy/cybersecurity/CyberRiskHandbook.html

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**」:

【概要】

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、及び普及啓発を推進する業界団体である CCDS が発行した、各種 IoT 機器や IoT サービスに共通に適用可能な、最低限守るべきセキュリティ要件を定義したもの。

【参照先】

CCDS「IoT 機器セキュリティ要件ガイドライン 2021 年版 Ver.2.0」:

https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021_v2.0_jpn.pdf

CCDS「IoT 機器セキュリティ要件ガイドライン 別冊 12 要件における解説編 2021 年版 Ver.2.0」:

https://www.ccds.or.jp/public/document/other/CCDS_SecGuide-IoTReq_2021-extra_v2.0_jpn.pdf

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 対策方針チェックリスト**」:

【概要】

「IoT 機器セキュリティ要件ガイドライン」の要件準拠を確認するために用いる、セキュリティ対策方針のチェックリスト。

【参照先】

CCDS「IoT 機器セキュリティ要件 2021 年版 対策方針チェックリスト v1.0」:

https://www.ccds.or.jp/public/document/other/CCDS_IoTReq_2021-checklist_v1.0_jpn.xlsx

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 システム調達のためのセキュリティ要件フレームワーク」:

【概要】

IoT セキュリティガイドラインの要点のうち、IoT 機器の製造や調達などを行う者にとって必要と考えられるセキュリティ要件を取り纏めたもの。

IoT システムを構成するコンポーネントごとに想定されるリスクを分類し、リスクごとに、部品調達時、製造時、流通販売時、運用開始～終了時に製造者や調達者などが考慮すべき一連のセキュリティ対策を、セキュリティの専門家で無くとも把握・理解し対策を実施できるように、分かり易く纏めている。

【参照先】

CCDS「IoT システム調達のためのセキュリティ要件フレームワーク」:

https://www.ccds.or.jp/public/document/other/CCDS_IoT%E3%82%B7%E3%82%B9%E3%83%86%E3%83%A0%E8%AA%BF%E9%81%94%E3%81%AE%E3%81%9F%E3%82%81%E3%81%AE%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E8%A6%81%E4%BB%B6%E3%83%95%E3%83%AC%E3%83%BC%E3%83%A0%E3%83%AF%E3%83%BC%E3%82%AF.pdf

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 機器セキュリティ実装ガイドライン(ソフトウェア更新機能)」:

【概要】

IoT 機器の製造者がセキュアな IoT 機器を設計するうえでの指針となることを目指し、IoT 機器における「ソフトウェア更新」機能の実装に求められる具体的なセキュリティ要件を提示したもの。

【参照先】

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 第 1.0 版」:

https://www.ccds.or.jp/public/document/other/CCDS_IoT%E6%A9%9F%E5%99%A8%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E5%AE%9F%E8%A3%85%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3(%E3%82%BD%E3%83%95%E3%83%88%E3%82%A6%E3%82%A7%E3%82%A2%E6%9B%B4%E6%96%B0%E6%A9%9F%E8%83%BD)_v1.0.pdf

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)

「**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**」:

【概要】

IPA「つながる世界の開発指針」、IoT 推進コンソーシアム「IoT セキュリティガイドライン」、および経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」を基本的な考え方として参照し、スマートホーム分野において対象となるシステム構成、および脅威(狙われるポイント)とリスク(被害)を踏まえ、スマートホーム分野の視点でライフサイクルのフェーズに応じて取り組むべき、具体的なセキュリティ対策の指針と要件を定義したもの。

【参照先】

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 概要説明資料 Ver.1.0」:

https://www.ccds.or.jp/public/document/other/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3-%E6%A6%82%E8%A6%81%E8%AA%AC%E6%98%8E%E8%B3%87%E6%96%99_%E3%82%B9%E3%83%9E%E3%83%BC%E3%83%88%E3%83%9B%E3%83%BC%E3%83%A0%E7%B7%A8_Ver.1.0_2.pdf

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 Ver.1.0」:

https://www.ccds.or.jp/public/document/other/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E3%82%B9%E3%83%9E%E3%83%BC%E3%83%88%E3%83%9B%E3%83%BC%E3%83%A0%E7%B7%A8_Ver.1.0_2.pdf

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 Appendix Ver.1.0」:

https://www.ccds.or.jp/public/document/other/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E3%82%B9%E3%83%9E%E3%83%BC%E3%83%88%E3%83%9B%E3%83%BC%E3%83%A0%E7%B7%A8_Appendix_Ver.1.0_2.pdf

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)

「**製品分野別セキュリティガイドライン 車載器編**」:

【概要】

IPA「つながる世界の開発指針」、IPA「自動車の情報セキュリティへの取組みガイド」、および IoT 推進コンソーシアム「IoT セキュリティガイドライン」を基本的な考え方として参照し、自動車の車載器分野において対象となるシステム構成、および想定される脅威と被害を踏まえ、車載器のライフサイクルのフェーズにおいて、セキュリティ対策のためにどのような取り組みをすべきかの指針と内容を示したもの。

【参照先】

CCDS「製品分野別セキュリティガイドライン 車載器編 概要説明資料 Ver.2.0」:

https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3%E6%A6%82%E8%A6%81_%E8%BB%8A%E8%BC%89%E5%99%A8%E7%B7%A8_Ver2.0.pdf

CCDS「製品分野別セキュリティガイドライン 車載器編 Ver.2.0」:

https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E8%BB%8A%E8%BC%89%E5%99%A8%E7%B7%A8_Ver2.0.pdf

Edgecross コンソーシアム

「Edgecross **ユーザ向けセキュリティガイドライン**」:

【概要】

企業・産業の枠を超え、コンソーシアム会員が共に構築し、FA と IT との協調を実現する、オープンな日本発のエッジコンピューティング領域のソフトウェアプラットフォーム「Edgecross」を利用する FA システム、Edgecross 搭載 PC、及びこれらを繋ぐネットワークにおけるセキュリティ対策の推奨を提示するもの。

【参照先】

Edgecross コンソーシアム「Edgecross セキュリティガイドライン 概要版」:

https://www.edgecross.org/ja/data-download/pdf/ECD-TE4-0004-01-JA.pdf

Edgecross コンソーシアム「Edgecross ユーザ向けセキュリティガイドライン 詳細版」:

https://www.edgecross.org/ja/data-download/pdf/ECD-TE4-0006-01-JA.pdf

ロボット革命・産業 IoT イニシアティブ協議会

(RRI: Robot Revolution & Industrial IoT Initiative)

「**RRI サプライチェーン質問票**」:

【概要】

ドイツ Plattform Industrie 4.0 の産業セキュリティを担う Security of networked systems(WG3)と共同で公表しているホワイトペーパ「IIoT Value Chain Security - The Role of Trustworthiness」で説明している、trustworthiness を保証するメカニズムの trustworthiness プロファイルに適用可能なもので、組織のセキュリティレベル(trustworthiness)や、セキュリティ状態の成熟度(マチュリティレベル)の評価を可能にする質問票。経済産業省が策定したサイバー・フィジカル・セキュリティ対策フレームワーク(CPSF)などをベースに作成している。

【参照先】

ロボット革命・産業 IoT イニシアティブ協議会「産業セキュリティ RRI サプライチェーン質問票」:

https://www.jmfrri.gr.jp/document/library/1890.html

8.4. 用語／略語

表 8-2 用語／略語の一覧及び説明

用語／略語	説明 [20]
AGV	《Automated Guided Vehicle》 工場や倉庫などで使用される「無人搬送車」。
CISO	《Chief Information Security Officer》 企業などの組織における情報セキュリティを統括する「最高情報セキュリティ責任者」。
CMMI	《Capability Maturity Model Integration》 企業などの組織のプロセスにかかわる能力を評価／改善するための指標を体系化したモデルで、プロセス能力の成熟度を 5 段階のレベルとして定義したもの。 レベルは低いものから、“1：初期状態(場当たり的な状態)”、“2：管理された状態(反復できる状態)”、“3：定義された状態(制度化された状態)”、“4：定量的に管理された状態(制御できる状態)”、“5：最適化している状態”。 [参考：Carnegie Mellon University Software Engineering Institute “Japanese Language Translation of CMMI for Development, V1.3” https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28776]

[20] Wikipedia などの公開情報を参考に作成。

Wikipedia:

https://ja.wikipedia.org/wiki/%E3%83%A1%E3%82%A4%E3%83%B3%E3%83%9A%E3%83%BC%E3%82%B8

それ以外の出典がある場合は、個別に付記。

用語／略語	説明 [20]
CPS	《Cyber Physical System： サイバーフィジカルシステム》 実世界(フィジカル空間)にある多様なデータをセンサーネットワーク等で収集し、サイバー空間で大規模データ処理技術等を駆使して分析／知識化を行い、そこで創出した情報／価値によって、産業の活性化や社会問題の解決を図っていくもの。 [出典：JEITA「CPS とは」https://www.jeita.or.jp/cps/about/]
CPU	《Central Processing Unit》 コンピュータの中心的な構成要素で、データの演算や、他の構成要素の制御などを行う「中央(演算)処理装置」。
CSR 報告書	《Corporate Social Responsibility》 企業は社会にとって望ましい組織として行動し、持続可能な社会の実現への貢献など、自発的に社会へ貢献し、倫理的な責任を果たすべきという考え方に基づく、「企業の社会的責任」にかかわる取組み内容を纏めた報告書。
FA システム	《Factory Automation》 センサ、制御／情報システム、産業用ロボット、無人搬送車(AGV)などを用いて工場の生産などの工程を無人化し、「工場の自動化」を実現するシステム。
FW	《Firewall： ファイアウォール》 コンピュータネットワークのゾーン(インターネット、LAN、ネットワークセグメントなど)の境界に設置し、通信のアクセス制御を実施することで、外部ネットワークからのサイバー攻撃に対して、内部ネットワークを保護する仕組み／機器。

用語／略語	説明 [20]
ICS	《Industrial Control System： 産業制御システム》 電力、ガス、水道、鉄道等の社会インフラや、石油、化学、金属、自動車・輸送機器、機械、食品、製薬、ビル管理等の工場・プラントにおける、設備監視・制御や生産・加工処理を実現するシステム。 [参考：IPA「制御システムのセキュリティ」 https://www.ipa.go.jp/security/controlsystem/index.html]
IDS	《Intrusion Detection System： 侵入検知システム》 コンピュータやネットワーク上で発生するイベント(各種アクセス／処理実行、ログ出力、通信データなど)を監視・分析することで、偵察行為や不正侵入と考えられる兆候を検知・通知する仕組み。
IP アドレス	《Internet Protocol： インターネットプロトコル》 コンピュータネットワークで標準的に用いられる「インターネットプロトコル」と呼ばれる通信手順において、「相互に接続・通信する機器を識別する、通信の送信元および宛先を示す番号」。
IPS	《Intrusion Prevention System： 侵入防止システム》 IDS(侵入検知システム)の検知機能に加え、アクセスを遮断することで、不正侵入を防止する仕組み。
ISMS	《Information Security Management System： 情報セキュリティマネジメントシステム》 組織の情報セキュリティを確保・向上するための管理策の実施、及び改善を継続的に図っていく仕組み。

用語／略語	説明 [20]
LAN	《Local Area Network： ローカルエリアネットワーク》 企業内や工場内など、特定の限られた範囲内で接続できるコンピュータネットワーク。
無線 LAN	電波による無線通信で接続・送受信する LAN。
無線 LAN AP (アクセス ポイント)	無線 LAN を構成するネットワーク機器の一種で、 無線 LAN に接続する端末間の無線通信の中継や、無線通信と有線通信の相互接続・変換を実現するもの。
NIST	《National Institute of Standards and Technology： 米国国立標準技術研究所》 米国商務省に属する連邦政府機関で、科学技術分野における計測と標準化に関する研究を幅広く行っている。 任務は、計測科学、標準、及び技術を前進させ、経済安全保障の強化や生活の質の向上に資することにより、米国の革新と産業競争力を促進させること。
OA システム	《Office Automation》 「オフィスにおける事務作業の効率化、省力化、自動化」を実現する情報システム。
OODA	Observe (観察)、Orient (状況判断、方向づけ)、Decide (意思決定)、Act (行動) の頭文字をとったもので、変化する状況に応じた的確な意思決定および行動を迅速に実現するプロセスの枠組み。4 段階のプロセスを素早く繰り返しループさせる(途中で観察からやり直しを含む)ことで、状況変化への迅速かつ臨機応変な適応を図る。
OT	《Operational Technology》 工場の生産システムなどの産業制御システム／機器を制御・運用するための技術のこと。

用語／略語	説明 [20]
PDCA	Plan (計画)、Do (実行)、Check (確認)、Act (改善) の頭文字をとったもので、品質管理などの管理業務において、4 段階を繰り返し、継続的に改善するプロセスの枠組み。
SIRT	《Security Incident Response Team： セキュリティインシデント対応チーム》 コンピュータシステム(産業制御システムなどを含む)やネットワークにおいて、セキュリティインシデント(問題)に繋がる事象が発生した際に対応する組織。平時は、それに備えたり、予防したりするための活動も担う。
SOC	《Security Operation Center： セキュリティ運用監視センタ》 ネットワークや機器に対するサイバー攻撃を監視し、サイバー攻撃の(兆候)検知や分析、対応策の助言を行う組織。
SSD	《Solid State Drive》 半導体メモリ(主にフラッシュメモリ)を用いた補助記憶装置。
VPN	《Virtual Private Network》 公衆インターネット回線を利用し、送受信データの暗号化により実現する、あるいは、通信事業者の閉域 IP ネットワークを利用し実現する、仮想的なプライベート(専用)ネットワーク。
アクセス制御 (Access Control)	コンピュータ、ネットワーク、データ、プログラムなどに対するアクセス可否を判断し実施する機能。
暗号鍵	データの暗号化や復号の処理をするために必要な、暗号アルゴリズム(計算手順)に入力する数値の一つ。 同じデータを同じ暗号アルゴリズムで暗号化する場合、異なる暗号鍵を用い計算することで、異なる暗号が出力される。また、暗号化に用いた暗号鍵に対応する暗号鍵(復号鍵)を用いなければ、暗号化されたデータを元のデータへ正しく復号することができない。

用語／略語	説明 [20]
アンドン	工場の生産ラインを効率的に管理するための道具で、工程で異常が発生した場合に、即時に関係者へ状況を知らせ、作業や処置を促す情報を表示する電光表示盤。トヨタ生産方式の要素の一つ。
インタフェース	異なる機器やプログラムを接続する境界面・接続口。
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一連の業務プロセスの連鎖。研究開発、商品企画、製品設計、工程設計、生産準備、生産、保守保全といった業務プロセスから構成される。
オンライン化	業務システムをネットワークへ接続し、ネットワークを介してオンライン上で業務を遂行可能な状態にすること。
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、稼働させ続け、その利用が継続できること、またはその指標のこと。
完全性 (Integrity)	データ、プログラム、機能、機器、ネットワーク、システムの構成や構成要素が不正に改ざんされたり、破壊されたりしておらず、正しく完全で整合が取れていること。
機密性 (Confidentiality)	許可されていない主体が、データ、プログラム、機能、機器、ネットワーク、システムに対し、許可されていないアクセスを実行できないこと。
許可リスト (ホワイトリスト)	不正なプログラムの実行、不正な通信、不正な操作をさせないことにより、サイバー攻撃などの異常を検知し防ぐ手法で用いられる、許可されるアクセス制御対象の一覧定義のこと。
クライアント	クライアント・サーバ形態のシステムにおいて、サーバに対してサービスを要求し、その提供を受ける位置づけのコンピュータやアプリケーションプログラムのこと。
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間でデータをやり取りするときに、中継や通信プロトコル(手順)／データ形式変換などの役割を担う、ルータのような機能を備えた通信機器・プログラム。

用語／略語	説明 [20]
権限昇格	利用者やプログラムの ID に割り当てられているアクセス権限を不正に昇格させ、本来は許可されていない不正なアクセス(プログラムの実行など)が可能な状態になること。
コーキング	建築物において、気密性や防水性を高めることを目的として、目地材などで隙間を充填し塞ぐこと。
コマンド	人間からコンピュータへ送信される、あるいは機器間、プログラム間などで送受信される、実行すべき処理の指示。
サプライチェーン	製品の原材料・部品の調達から、生産、物流、販売に至るまでの一連の製品供給プロセスの連鎖。
システム構成情報	生産設備などのシステムを構成する要素として、どのような計算機や機器などが接続され使われているかの情報。場合によっては、機器の OS や導入されているプログラムの種別・バージョンといった情報も含む。
真正性 (Authenticity)	利用者、データ、プログラム、機器、システムがなりすまされた偽物ではなく、真正な本物であること。
信頼性 (Reliability)	障害の発生のし難さのこと、またはその指標のこと。
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。
責任追跡性 (Accountability)	データの参照や変更、プログラムの実行などのアクセスにかかわる事実履歴情報(アクセス主体、アクセス対象、アクセス内容、時刻、アクセス元、アクセス方法など)を、後から過去に遡り追跡できるようにすること。
(ネットワーク) セグメント	ネットワークのうち、ルータやファイアウォールなどのアクセス制御機能により分割された、特定の部分的なネットワーク。
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。

用語／略語	説明 [20]
ソフトウェア	コンピュータを動作させるための命令やプログラム、及びデータのこと。ハードウェアと対比される用語。
段取り替え	生産ラインで生産する製品の種別や工程の変更に応じた、金型や治工具の取り替え、生産設備の設定変更・調整、部品や部材の切り替え、事前の作業内容確認、清掃など、段取りの切り替え作業のこと。
ディスク	ハードディスクや CD / DVD / BD(Blu-ray Disc)などの薄い円盤状のデータ記憶媒体、及び補助記憶装置のこと。
デジタル化	デジタル(情報通信)技術を活用し、業務プロセスの効率化やサービス・製品の高付加価値化、新たなビジネスモデルの実現を図ること。
デジタル トランス フォーメーション (DX)	高度なデジタル技術(第 3 のプラットフォームと呼ばれるクラウド、モビリティ、ビッグデータ・アナリティクス、ソーシャル技術)を活用したデジタル化により、業務プロセス、サービス・製品、ビジネスモデルの変革とともに、社会や組織の制度・文化などの変革も引き起こすこと。
デバイス ID	機器を一意に特定するための識別子で、英数字から成る文字列の形式で表現される。
電子認証	アクセスの主体や対象がなりすまされた偽物ではなく、真正な本物であることを、電子的に確認する仕組み。
トレーサビリティ	「個々の製品がいつ、どこで、誰によって、どのように、生産・流通・販売されたのか」をサプライチェーンにわたり追跡可能にすること。
内部統制報告書	金融商品取引法に基づき、企業の財務報告にかかわる内部統制の整備状況や、内部統制が有効に機能しているかを経営者自らが評価し、結果を記載した報告書のこと。
ハードウェア	コンピュータなどのシステムを構成する物理的な機器のこと。ソフトウェアと対比される用語。

用語／略語	説明 [20]
バリューチェーン	調達・購買した原材料・部品に対して、サプライチェーンやエンジニアリングチェーン、それを支援する間接業務など、一連の企業活動の各プロセスにて、価値を付加していく連鎖のこと。 元々は、競争戦略に関する研究の第一人者であるマイケル・ポーターが著書『競争優位の戦略』の中で最初に用いた言葉で、企業の競争優位性及び事業戦略の評価や改善策の検討のために、最終的に製品やサービスが提供されるまでに、どのプロセスで、どのような価値が付加されているかを分析する考え方。
否認防止 (Non-Repudiation)	データ、プログラム、機能、機器、ネットワーク、システムに対するアクセス(利用、参照、変更など)の事実を事後に否認できないように、証拠となるアクセスログを改ざんできない形態で記録し、証明を可能にすること。
ファイアウォール	コンピュータネットワークのゾーン(インターネット、LAN、ネットワークセグメントなど)の境界に設置し、通信のアクセス制御を実施する仕組みのこと。 信頼できない外部ネットワークからの攻撃に対する内部ネットワークの保護や、内部ネットワークから外部ネットワークへの不正／危険な通信の防止のために用いる。
フィードバック制御	制御システムにおいて、制御の実際の出力結果を出力目標と比較し、差分に応じて入力を調整することにより、出力目標に近づけ、それを保つ制御手法のこと。
踏み台攻撃	攻撃者がサーバ、PC などのコンピュータや機器に不正に侵入し、それを踏み台にして、別のコンピュータや機器、及びネットワークやサービスを対象に攻撃すること。
フリーアクセスフロア	床下に電源／通信用の配線や、空調設備などの機器を収納するための空間を設けた構造の床のこと。
(コンピュータ)プログラム	コンピュータに対する一連の処理命令を記述したもの。

用語／略語	説明 [20]
ペネトレーションテスト	コンピュータなどのシステムに対して、既知の攻撃手法を用いて実際に疑似的な攻撃を仕掛け、侵入を試みることで、システムにセキュリティ上の脆弱性(欠陥)が無いかを検査・検証する手法。
ポート	コンピュータなどの機器やプログラムが、外部の別の機器やプログラムと接続・通信するための入出力口。
ポート番号	コンピュータネットワークで標準的に用いられる「インターネットプロトコル」と呼ばれる通信手順において、相互に接続・通信する機器内の「サービスやプログラムを識別する番号」。
メモリ	コンピュータにおけるプログラムやデータを記憶する装置。特に、RAM や ROM などの半導体記憶装置を指す。
モルタル	砂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、仕上材や目地材、躯体の調整などに多く用いられる。
有価証券報告書	金融商品取引法に基づき、株式を発行する上場企業などが事業年度ごとに企業情報を開示する報告書。企業の概況、事業の状況、財務諸表などが含まれる。
ランサムウェア	サーバや PC などの機器内のデータを不正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暗号鍵(復号鍵)を渡すのと引き換えに、身代金を要求するマルウェア。
レシピ	工場における生産手順にかかわる情報。 たとえば、生産設備で製品を製造するための原材料の調合手順などのプロセスレシピや、生産設備のコントローラの設定値(マシンレシピ)など。

8.5. 図表目次

図目次

表目次

ガイドライン検討・作成メンバ紹介

※主要メンバ／執筆者は太字で表記し、氏名の右側に[主な役割]を付記してあります。

東京大学　グリーン ICT プロジェクト(GUTP)

代表：東京大学　江崎 浩 教授　[監修]

工場セキュリティ WG

メンバ：**株式会社シムックスイニシアティブ　中島 高英 代表取締役 CEO**、濱野

株式会社 竹中工務店　西園 健吾　[主要執筆者]

株式会社 GUTP コンサルティング　常田 光一

Edgecross コンソーシアム(ECC)

テクニカル部会長：三菱電機株式会社　西雪 弘、市岡 裕嗣(後任)

工場セキュリティ WG

リーダ：日本電気株式会社　桑田 雅彦　[全体編集者, 主要執筆者]

メンバ：**三菱電機株式会社　松田 規　[主要執筆者]**

株式会社 日立製作所　中野 利彦　[主要執筆者]、勝田

オムロン株式会社　岡村 弘太郎　[主要執筆者]、廣部、田原、芹川

株式会社 PFU　伴仲 輝大

トレンドマイクロ株式会社　高橋 弘宰、喜多 裕良

日本電気株式会社　石井 大二

その他

工場セキュリティ WG

メンバ：**日立チャネルソリューションズ株式会社　緒方** 日佐男　**(CCDS メンバ)**

ファナック株式会社　西 浩次、斉田

フォーティネットジャパン合同会社　佐々木 弘志　[主要執筆者]

以上