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 Appendix

Ver 1.0

【工場セキュリティの重要性と始め方】

令和７年４月11日

産業サイバーセキュリティ研究会
ワーキンググループ１（制度・技術・標準化）
工場サブワーキンググループ

変更履歴

発行日	版	概要
2025 年 4 月 11 日	Ver1.0	Ver1.0 発行

目次

1 はじめに

1.1 本ドキュメントの目的

近年、工場の IoT 化等に伴うサイバー攻撃のリスクが増加しており、特に、取引先まで被害が波及するなど、サプライチェーンを介したサイバー攻撃のリスクが高まっている。そのため、製造業全体を守るためには、工場の規模を問わずサプライチェーンを構成する全ての企業においてセキュリティ対策を実施する必要がある。

本書は「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[1]」(以下、ガイドライン本編)の解説書として、主に工場を有する中小規模の製造事業者の経営層や、工場のセキュリティ担当者として選任された方を対象に、工場セキュリティ[2]の重要性を解説し、取組の始め方を解説したものである。

1.2 想定読者・活用方法

本書の各章では、以下の読者を想定している。

- 第 2 章 工場セキュリティの重要性
  - 経営層
  - IT 関係部門(情報システム部門、セキュリティ部門等)の責任者
  - 生産関係部門(生産技術部門、生産管理部門、工作部門等)[3]の責任者(例:工場長、所長、製造部長)
- 第 3 章 工場セキュリティの始め方
  - 生産関係部門において工場セキュリティの担当者に選任された方
  - IT 関係部門における工場セキュリティの担当者

本書は、想定読者に対してガイドライン本編の内容をより分かりやすく解説し、具体的な事例・手順を示した解説書であり、以下の活用も想定している。

- 工場セキュリティの必要性を経営層に説明する際の参考として
- 取引先に工場セキュリティを求める際の参考として

---

[1] https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html
[2] 本書における「工場セキュリティ」は、工場システムにおけるサイバーセキュリティ対策を意味している。
[3] 生産関係部門において中心的な役割を果たす者として、機器・システムやセキュリティ製品の調達者や、機器・システムの構築者、管理者、運用者、保守者等を想定している。

2 工場セキュリティの重要性

2.1 なぜ工場セキュリティが重要なのか

2.1.1 工場がサイバー攻撃を受けた時の影響とは

近年、工場の IoT 化等に伴うサイバー攻撃のリスクが増加しており、その理由の一つとして工場のセキュリティ対策が十分でないことが考えられる。

例えば、工場はネットワークから切り離されているために安全と考えている経営者もいるが、意図せずに工場がインターネットなどの外部と繋がっていたためにサイバー攻撃の被害を受けることもある。

また、サイバー攻撃による被害として、システム停止、生産停止、生産効率低下、不良品出荷、機密情報漏えい、環境汚染などが知られているが、これらのほか、発注元企業と自社がネットワークで接続されている場合に、自社が発注元企業への攻撃の踏み台にされた事例も確認されており、以下のような被害が生じることがある(このようなセキュリティの事故・出来事を“インシデント”という)。

- 取引の停止
  自社へのサイバー攻撃が、発注元企業に対しても被害を及ぼした場合に、契約を解除される可能性がある。
- 賠償金の支払い
  自社へのサイバー攻撃により、発注元企業に金銭的な被害が発生した場合に、賠償金の支払いを求められる可能性がある。
- 新規取引機会への影響
  取引先を選ぶ際に、サイバーセキュリティ対策の実施状況を問われ、対策が不十分とみなされた場合に新規取引の機会を失う可能性がある。

以上のことから、サイバー攻撃により、自社に限らず顧客にまで被害が及ぶ可能性があることについて、しっかりと認識する必要がある。

図 2-1 サイバー攻撃による自社への影響のイメージ

2.1.2 製品の提供が滞ることによる他社への影響について

製造業においては、1つの製品を製造するために様々な部品が必要となることが一般的である。そのため、特定の部品を製造する企業が、サイバー攻撃により生産停止や生産効率低下などの被害を受けた場合に、その部品を使用する製品の製造や出荷にまで影響を及ぼす。

また、自覚はなくとも自社の製品や部品が他社の提供する製品やサービスに不可欠な場合があり、提供ができなくなることで他社に甚大な影響を及ぼすおそれがある。そのため、日頃から自社の製品や部品の生産停止が他社にどのような影響を与えるかについて把握しておくことが大切である。

2.1.3 工場セキュリティに関連する制度等について

工場セキュリティの必要性が高まっていることを背景に、国内外の工場セキュリティに関連して様々な法律・規制・ガイドライン等が整備され始めている。

特に、我が国では IoT 製品に対するセキュリティ対策基準を定めた「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」[4]、欧州では製品を販売する際に求められるセキュリティ対策を定めた「EU サイバーレジリエンス法」において、製品へのセキュリティ対策（製品セキュリティ）が求められ始めている。

その他にも、サプライチェーンを構成する企業が一定のセキュリティ対策を行うための基準としての「サプライチェーン強化に向けたセキュリティ対策評価制度」[5]の検討も行われており、さらには、経済安全保障の観点で取引先から工場セキュリティを求められることも十分に考えられる。

[4] https://www.ipa.go.jp/security/jc-star/index.html
[5] https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain

2.2 サイバー攻撃による被害事例を学ぶ

2.2.1 製造業に対するサイバー攻撃の現状について

近年、サイバー攻撃における最大の脅威の一つとしてランサムウェア攻撃(データを暗号化し、その解除と引き換えに金銭を要求する攻撃)がある。

警察庁の公開資料[6]では、2024 年のランサムウェア被害件数のうち、規模別では中小企業が 63%、業種別では製造業が 29%を占めている。製造停止による影響が大きいため、製造業は、攻撃者に狙われやすいとも考えられる。

さらには、サプライチェーンを介したサイバー攻撃も確認されており、発注元企業の取引先を標的としてサイバー攻撃が行われ、その取引先を足がかりとして発注元企業に攻撃を仕掛けるなどの事例が報告されている[7]。

自社がサプライチェーン上の他企業とネットワークで接続されている場合には、自社が他企業への攻撃の踏み台となる可能性があることを認識しておく必要がある。

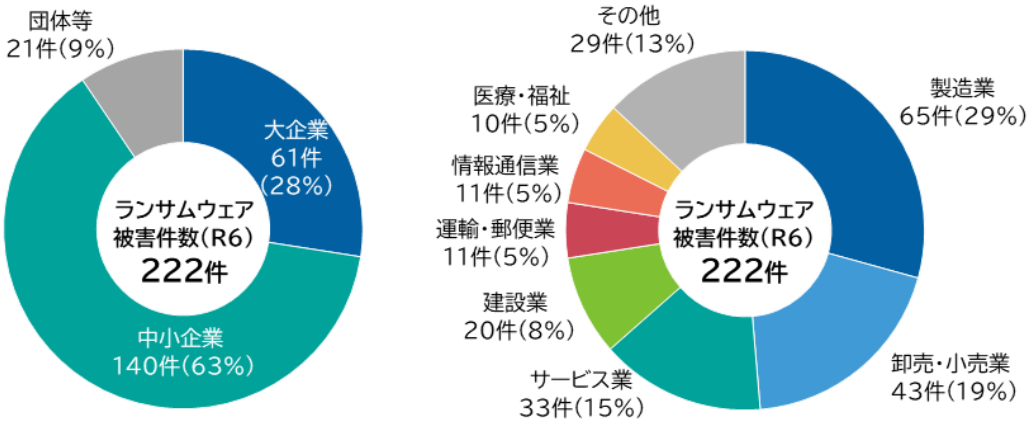

図 2-2 2024 年のランサムウェアの被害件数の規模別・業種別件数

2.2.2 製造業等に対するサイバー攻撃の事例について

ここでは、サイバー攻撃の被害事例として、生産停止、機微情報の漏えい、発注元企業への踏み台にされた事例について紹介する。しかしながら、これらの事例に限らず、全ての企業が様々なサイバー攻撃の標的にされる可能性があることに留意する必要がある。

---

[6] 「令和 6 年におけるサイバー空間をめぐる脅威の情勢などについて」(2025 年 3 月 13 日 警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf

[7] 「サイバーセキュリティに関する調査」(2022 年7月1日 トレンドマイクロ)
https://www.trendmicro.com/ja_jp/about/press-release/2022/pr-20220701-01.html

（1） 生産停止に至った被害事例

2022 年 3 月、自動車の内外装部品を生産する事業者（従業員約 1,500 名）において、ランサムウェア攻撃により全てのサーバが停止した。この被害により、部品供給の一部が止まった結果、大手の自動車メーカーにおける国内 14 か所の工場における計 28 の生産ラインが停止し、約 1 万 3,000 台の自動車の生産に影響を及ぼした。

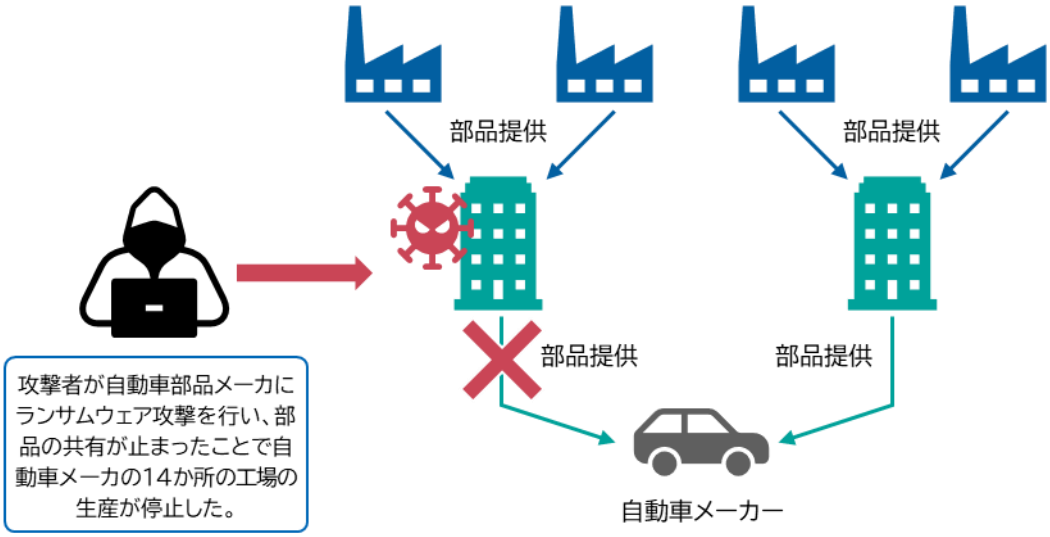

図 2-3 生産停止事例の一例

（2） 機微情報の漏えいに至った被害事例

2023 年 11 月、自動車の部品を生産する事業者（従業員約 600 名）において、不正アクセスにより取引先情報を含む 1,000 件以上の情報が漏えいした。

この漏えいした情報には、自社の従業員の情報だけではなく、取引先の担当者氏名などの情報も含まれていた。

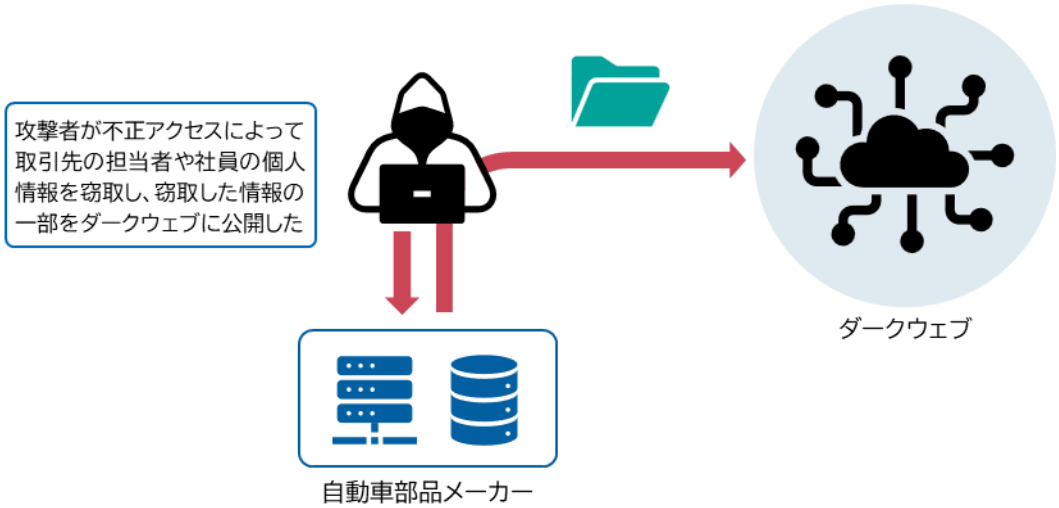

図 2-4 機微情報漏えい事例の一例

（3） 意図せず発注元企業への攻撃者になった事例

2022 年 10 月、攻撃者は、給食センター（従業員約 140 名）へ侵入後、更に給食センターを介して医療機関へランサムウェア攻撃を行い（このように攻撃者に利用されることを“踏み台にされる”という）、給食センターは医療機関への攻撃者となってしまった。医療機関では電子カルテを含む総合情報システムが全て停止し、復旧には約 2 か月を要した。被害額は、診療制限による影響や調査・復旧等のための費用として十数億円以上と見込まれている。

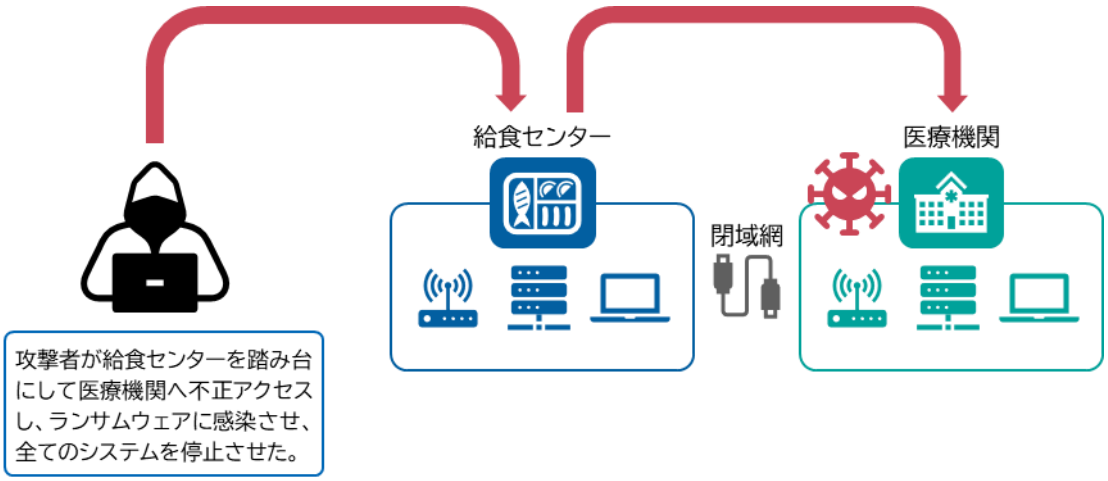

図 2-5 踏み台にされた事例の一例

【参考】発注元への踏み台になった事例における問題点

上記事例では、一定のセキュリティ対策を実施していたにもかかわらず、期待していた効果が十分に得られていなかったために被害が発生してしまった。

本事例のインシデント調査報告書[8]では、以下の問題点が指摘されている。

- 利便性を優先し、サイバー攻撃を想定した作りになっていなかった。
  - ✓ 給食センターと医療機関は閉域網で接続しており、双方ともに不要なネットワーク通信を遮断するファイアウォールを設置してネットワークを分離していたが、ベンダが遠隔保守をするための機能（リモートデスクトップ）が常時利用可能であった。そのため、外部から給食センターへ侵入し、給食センターから医療機関のサーバに直接アクセスできる状態になっていた。そのサーバが院内ネットワークにも同時に接続しており、マルウェア感染が広がった。
  - ✓ 全てのユーザが管理者権限でログインできる状態になっており、ウィルス対策ソフトウェアを削除できる設定になっていた。
- ファイアウォール設置後のメンテナンスができておらず、設置後の役割分担が明確でなかったために、ファームウェア（基本的なソフトウェア）のアップデートが行われていなかった。

[8] https://www.gh.opho.jp/incident/1.html

2.3 工場セキュリティによってサイバー攻撃の被害を低減する

2.3.1 工場セキュリティによるサイバー攻撃の被害低減について

サイバー攻撃による被害を減らすためには、適切に工場のセキュリティ対策を導入し、適切に運用することが重要である。正しく実施することで、以下の効果が得られるため被害を低減することができる。

- 工場へのサイバー攻撃による被害リスクを低減できる
- サイバー攻撃を受けた場合の被害を軽減し、早期に回復できる

2.3.2 コストをかけずとも実施できる対策について

多大なコストをかけてセキュリティ対策を導入するのではなく、製造工程における重要な設備や機器を特定し、リスクに応じた必要かつ十分なセキュリティ対策を実施することが大切である。

特に、サイバー攻撃の被害を軽減する観点からは、サイバー攻撃を受けても業務を継続できるよう、事前に準備をしておくことが大切である。その準備としては、以下に示すような平常時の対策とサイバー攻撃を想定した対策がある。これらの対策では、新たな設備や機器を導入する必要がないため、コストをかけずとも実施することができる。一度に多くの対策を実施するよりも、コストをかけずとも実施できる対策から優先的に始めるべきである。

- 平常時の対策
  - 社内のセキュリティに対する意識向上を図る
    （例：SECURITY ACTION[9]の活用）
  - サイバー攻撃の原因と影響について理解を促すことを目的として、生産現場の担当者に対してセキュリティ教育や注意喚起を行う
    （例：IPA や警視庁が公開している工場セキュリティ教育コンテンツ[10]の活用）
  - 情報システムと工場システムの分離や工場セキュリティの導入を見据えて、IT 関係部門と生産関係部門の連携体制を構築する

[9] SECURITY ACTION は中小企業自らが、情報セキュリティ対策に取り組むことを自己宣言する制度である。一つ星と二つ星があり、一部の補助金の申請要件としても使われている。
https://www.ipa.go.jp/security/security-action/sa/

[10] 情報処理推進機構「現場向け制御セキュリティ教育：セキュリティ道場」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2021/security-dojo.html
警視庁「Counter Cyber Attack～誰もが狙われる時代～」CASE3『制御システムに対する攻撃』
https://www.keishicho.metro.tokyo.lg.jp/about_mpd/joho/movie/cyber/cca/220.html

- サイバー攻撃を想定した対策
  - サイバー攻撃を受けた際の対応を明確にするために、あらかじめ被害発生時の役割分担を決めておく
  - サイバー攻撃を受けた際に速やかに支援を求めることができるよう、あらかじめ外部の連携先を確認しておく
    （例：サイバーセキュリティお助け隊サービス制度[11]におけるサービス提供事業者、サイバーインシデント緊急対応企業[12]、専門家（登録セキスペ[13]など）、情報システム・工場システムを委託しているベンダ）
  - 被害の内容や状況に応じた報告先をあらかじめ整理しておく
    （例：警察[14]（犯罪が疑われる場合）・個人情報保護委員会[15]（個人情報が漏えいした場合）・IPA[16]や JPCERT/CC[17]（サイバー攻撃が疑われる場合））
  - 一部の設備・機器が停止しても製造は完全に停止しないためのバックアッププランを準備し、訓練を行う
    （例：一時的に手作業による代替運用が可能な体制の構築、予備の設備・機器の準備、危険予知訓練（KYT）にサイバー攻撃を含めること）

これらの対策を、セキュリティ関連の認証・マーク取得するための活動として推進し、認証・マークの取得により外部からの信頼を得ることも可能である。

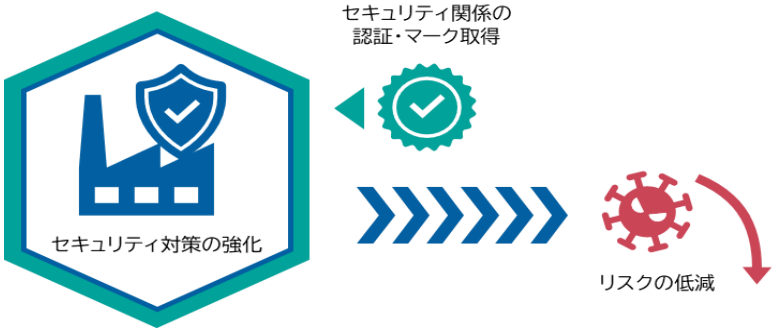

図 2-6　工場セキュリティによるリスクの低減のイメージ

---

[11] サイバーセキュリティお助け隊サービス制度とは、中小企業に対するサイバー攻撃への対処として不可欠なワンパッケージのサービスを要件としてまとめ、これを満たすことが所定の審査機関により確認された民間サービスを IPA が登録・公表する制度である。
https://www.ipa.go.jp/security/otasuketai-pr/
[12] サイバーインシデント緊急対応企業とは、日本ネットワークセキュリティ協会（JNSA）が紹介しているサイバーインシデント時に相談できる企業である。
https://www.jnsa.org/emergency response/
[13] 登録セキスペは、サイバーセキュリティ対策を推進する人材の国家資格である。以下の URL から登録セキスペの人材を検索することが可能である。
https://riss.ipa.go.jp/
[14] 警察庁におけるサイバー事案に関する相談窓口は以下のとおりである。
https://www.npa.go.jp/bureau/cyber/soudan.html
[15] 個人情報保護委員会における相談窓口は以下のとおりである。
https://www.ppc.go.jp/
[16] IPA におけるコンピュータウイルス・不正アクセスに関する届出については以下のとおりである。
https://www.ipa.go.jp/security/todokede/crack-virus/about.html
[17] JPCERT/CC におけるインシデントの報告は以下のとおりである。
https://form.jpcert.or.jp/

3 工場セキュリティの始め方

3.1 工場セキュリティを始める上で重要となる考え方

工場セキュリティの担当者は、サイバー攻撃により製品の供給を止めないようにすることを考えなければならない。

前章の 2.3.2 項においては、コストをかけずとも実施できるセキュリティ対策を紹介したが、一定のコストをかけてセキュリティ対策を導入することも、また大切である。

ただし、多大なコストをかける必要はなく、製品の供給を止めないために必須の設備に絞って適切なセキュリティ対策を導入することが肝要であり、本節では、これら検討をする上で重要となる 2 つの考え方を紹介する。

3.1.1 守るべき対象を決定するために

工場セキュリティを検討する際には、最初に製造工程上の重要な設備・機器を特定する必要があり、抜け漏れがないかしっかり確認することが求められる。特に、製造の手順を把握した上で、各手順に関わる設備・機器を網羅的に整理することが重要である。

製造工程上の重要な設備・機器の特定については、サイバー攻撃の影響を考慮しながら進める必要がある。このため自社の工場を詳細に理解している従業員が、信頼できるセキュリティ専門家（例えば、情報システム・工場システムを委託しているベンダ）と協力・連携して実施することが望ましい。

また、網羅的な整理には、設備・機器が停止した際の工場への影響が把握しやすくなる効果や、インシデント発生時に必要な対応を明確化する効果などもあるため、追加対策の導入まで至らなくとも十分に意義がある。

3.1.2 対策の効果を組織全体で共有しチームで推進する

セキュリティ対策を導入する際に、工場セキュリティの担当者のみで新たな機器を設置して正しい設定を行うことは難しい。したがって、自社の情報システム部門や情報システム・工場システムを委託しているベンダと連携することが多いと想定される。

その際、関係者に対し、目的や効果や運用含めずに手段（求める装置や機能）のみを伝えてしまうと、得たい効果を発揮しないファイアウォールが設置されて

しまうなど、意図しない状態の機器が導入されることが発生し得る。

このような事態を避けるためには、SQDC（安全、品質、工程、コスト）の視点を考慮し、どのようなサイバー攻撃から、設備や機器への影響をどの程度低減するかについて、“セキュリティ対策の目標と実施条件”として決める必要がある。この目標と実施条件を工場へセキュリティ導入する関係者（工場関係者、情報システム部門など）及び経営者との間で合意し、この合意した目標と条件を、ベンダを含め関係者へ正しく伝えることが大切である。

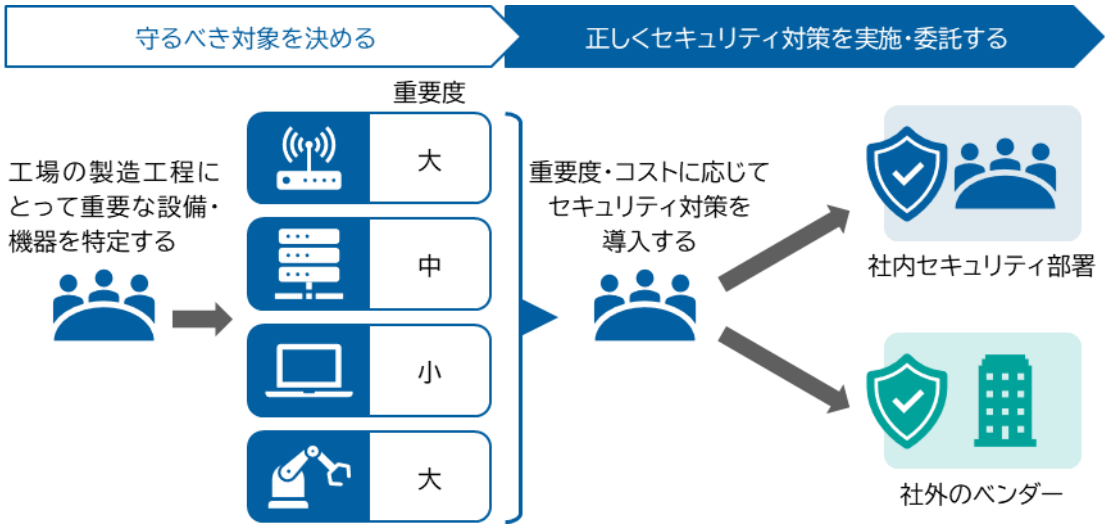

図 3-1 工場セキュリティにおける重要な考え方

【参考】適切でない設定がなされていたケース①

ファイアウォール（通信を監視・制御する機器）を導入していたにもかかわらず効果を発揮していなかったケースを紹介する。

ファイアウォールを導入したものの、設定条件や保守分担が曖昧なため以下のような状態を誘発し、内部ネットワークへの不正侵入を許してしまいサイバー攻撃を受けた。

- ✓ 通信遮断の設定がデフォルトのままで、不要な通信が通過可能な状態
- ✓ リモートデスクトップ通信が許可されており、任意の PC 操作ができてしまう状態
- ✓ ファイアウォール自体の脆弱性対策（装置のソフトウェア更新）が実施されていない状態

ファイアウォールを導入する際には、設定内容や運用について導入したベンダとの間で、確認・合意することが大切である。

3.2 守るべき対象の決め方について

3.2.1 業務の整理・重要度の決定

最初に、工場における製造に関わる全ての業務を洗い出し、表 3-1 の基準を例として、それぞれの業務の重要度を決定する。

表 3-1 業務の重要度の一例

業務の重要度	内容
大	• 製品の安定生産に直結する業務であり、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をきたす。 • 許容できない範囲の品質劣化が大規模に発生する。
中	• 製品の安定生産に間接的に関連する業務であり、本業務が実施できなくなると、2～3 日のうちに生産をきたす。 • 許容できない範囲の品質劣化が小規模に発生する。
小	• 製品の安定生産への影響が小さい業務であり、本業務が実施できなくとも、生産に支障をきたす可能性は低い。 • 許容できる範囲の品質劣化が発生する。

3.2.2 資産の整理・重要度の決定

次に、工場で使用している全ての設備・機器・データを洗い出し、表 3-2 に示す主な資産の種別を例として、それぞれの資産が、重要度を決定したそれぞれの業務に使用されているかどうかを確認する。

そして、設備・機器・データといった資産が稼動できない場合における業務への影響を踏まえて、資産の重要度を決定する。

表 3-2 資産の種別の例

種別	内容
ネットワーク機器	• スイッチ、ルータ、ファイアウォールなど
装置・機器	• MES サーバ、SCADA、PC、PLC、工作機械など
データ	• 生産計画、生産レシピ、生産状況など

3.2.3 業務・資産に応じた守るべき対象の整理

最後に、以下の手順で業務・資産に応じて守るべき対象の整理を行う。

1. 整理した業務・資産に基づき、工場のネットワーク構成図を作成する。
2. 製品が製造されるまでの流れに沿って、3.2.1 項で洗出した業務に基づいて、業務間のつながりを確認する。
   （業務間のつながりの例：A 業務のアウトプットを B 業務に利用する、A 業務のデータを C 業務で監視する）
3. 業務間のつながりと業務の重要度に応じて、業務をグループ化する。グループ化した業務内で使用する設備・機器・データを守るべき対象として整理する。

3.2.4 守るべき対象の決め方の実施例

3.2.1 項～3.2.3 項の実施例として、中小規模の加工組立の工場を想定し、守るべき対象を決定するまでの手順を詳細に説明する。想定工場のネットワーク構成図は図 3-2 のとおりである。

この工場では、工作機械による自動生産が行われており、生産指示データに基づいて2つ製品（製品①、製品②）を生産している。また、図中の標準ルータは、インターネット回線の契約に併せて貸与されるルータや、標準設定のままで使用している市販の汎用ルータを意図している。

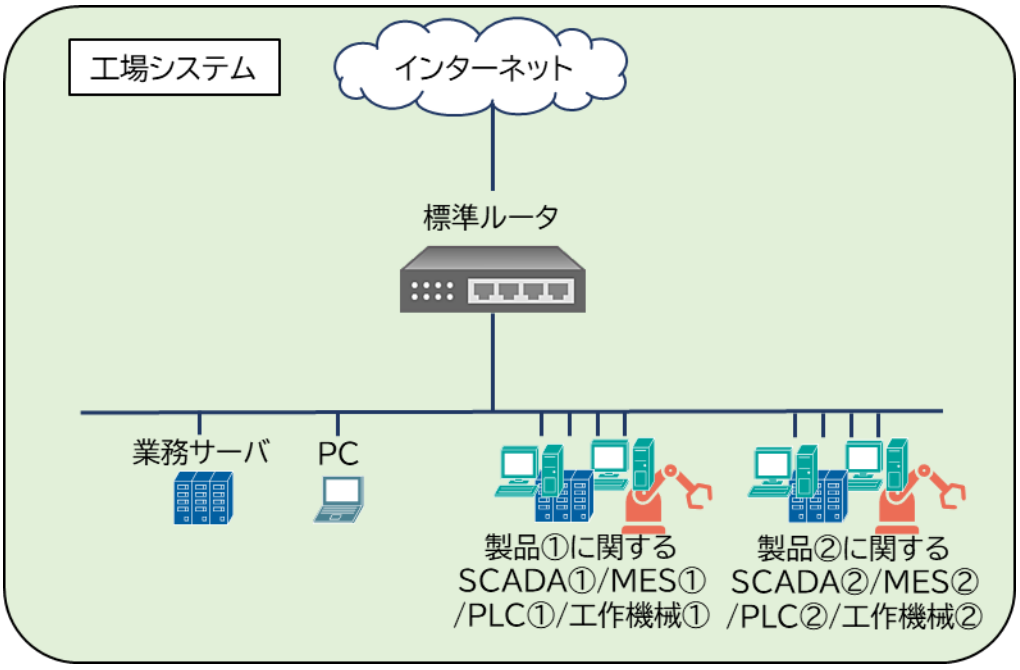

図 3-2 想定工場のネットワーク構成図

（1） 業務の整理・重要度の決定

表 3-3 は想定工場における業務と重要度の例を示している。ここで、重要度の決定には表 3-1 の基準を用いている。

表 3-3 想定工場における業務の重要度の例

	業務	業務内容	重要度（判断理由）
1	製品①の生産計画設定	• PC から月次・週次・日次の生産計画を MES サーバ①に入力する。 • MES サーバ①に加え、紙媒体でも生産計画を管理している。	小 （MES サーバの他に紙でも生産計画を管理しており、バックアップがあるため、生産への影響は小さい。）
2	製品①の生産指示	• MES サーバ①から PLC①への生産機種・生産量・生産レシピなどの指示をトリガとして生産を開始する。 • 上記と同様に、手動でも PLC①に直接生産指示を入れることができる。	中 （MES サーバ経由だけでなく、手動でも PLC に生産指示を送れるため、直ちに生産への影響はない。）
3	製品①の生産状況監視	• PLC①は自身の生産状況を MES サーバ①に送信する。 • SCADA①は、MES サーバ①から生産状況を取得して画面に表示する。	中 （生産状況が監視できない場合も、ある程度の監視は手動で行うことができるため、直ちに生産への影響はない。）
4	製品①の生産	• PLC①から工作機械に指示を出す。	大 （PLC や工作機械が停止した場合、代替手段がなく、直ちに生産へ影響する。）
5	製品②の生産計画設定	• PC から MES サーバ②に対して、月次・週次・日次の生産計画を入力する。 • MES サーバ②に加え、紙媒体でも生産計画を管理している。	小 （MES サーバの他に紙でも生産計画を管理しており、バックアップがあるため、生産への影響は小さい。）
6	製品②の生産指示	• MES サーバ②から PLC②への生産機種・生産量・生産レシピなどの指示をトリガとして、生産を開始する。 • 上記と同様に、手動でも PLC②に生産指示を直接入れることができる。	中 （MES サーバだけでなく、手動でも PLC に生産指示を送れるため、直ちに生産への影響はない。）
7	製品②の生産状況監視	• PLC②は自身の生産状況を MES サーバ②に送信する。 • SCADA②は、MES サーバ②から生産状況を取得し画面に表示する。	中 （生産状況が監視できない場合も、ある程度の監視は手動で行うことができるため、直ちに生産への影響はない。）
8	製品②の生産	• PLC②から工作機械に指示を出す。	大 （PLC や工作機械が停止した場合、代替手段がなく、直ちに生産へ影響する。）

	業務	業務内容	重要度(判断理由)
9	部材補充	• SCADA と MES サーバからの情報に基づいて各生産ラインに部材を補充する。	中 (目視で部材を補充できるため、直ちに生産への影響はない。)

(2) 資産の整理・重要度の決定

表 3-4 は想定工場における資産と重要度の例を示している。ここで、重要度の決定には表 3-1 の基準を用いている。なお、本例では情報漏えいの観点を考慮していないため、データ資産に対しての重要度は示していない。また、ネットワーク機器はセキュリティ対策の設定を行う機器自体であるため除外している。

表 3-4 想定工場における資産の重要度の例

	資産	関連業務	重要度(判断理由)
1	業務サーバ	• 生産関連業務への影響なし	小 (生産業務と関係がなく、生産に影響しないため)
2	PC	• 製品①、製品②の生産計画策定	小 (重要度が小さい業務としか関係がないため)
3	SCADA①	• 製品①の生産状況監視 • 部材補充	中 (重要度が中程度の業務と関係あるため)
4	MES サーバ①	• 製品①の生産計画策定 • 製品①の生産指示 • 部材補充	中 (重要度が中程度の業務と関係あるため)
5	SCADA②	• 製品②の生産状況監視 • 部材補充	中 (重要度が中程度の業務と関係あるため)
6	MES サーバ②	• 製品②の生産計画策定 • 製品②の生産指示 • 部材補充	中 (重要度が中程度の業務と関係あるため)
7	PLC①	• 製品①の生産指示 • 製品①の生産状況監視 • 製品①の生産	大 (重要度が大きい業務と関係あるため)
8	工作機械①	• 製品①の生産 • メンテナンス	大 (重要度が大きい業務と関係あるため)
9	PLC②	• 製品②の生産指示 • 製品②の生産状況監視 • 製品②の生産	大 (重要度が大きい業務と関係あるため)
10	工作機械②	• 製品②の生産 • メンテナンス	大 (重要度が大きい業務と関係あるため)

（3）業務・資産に応じた守るべき対象の整理

表 3-4 の重要度を踏まえ、守るべき対象をまとめてゾーンとして整理したものが図 3-3 と表 3-5 である。ここでは、重要度が小の機器は、生産への影響が少ないため OA ゾーンとし、製品を生産する設備が、製品①と製品②で異なるため、製品①の生産に影響があり重要度が中・大の機器群を制御ゾーン①、製品②の生産に影響があり重要度が中・大の機器群を制御ゾーン②とした。

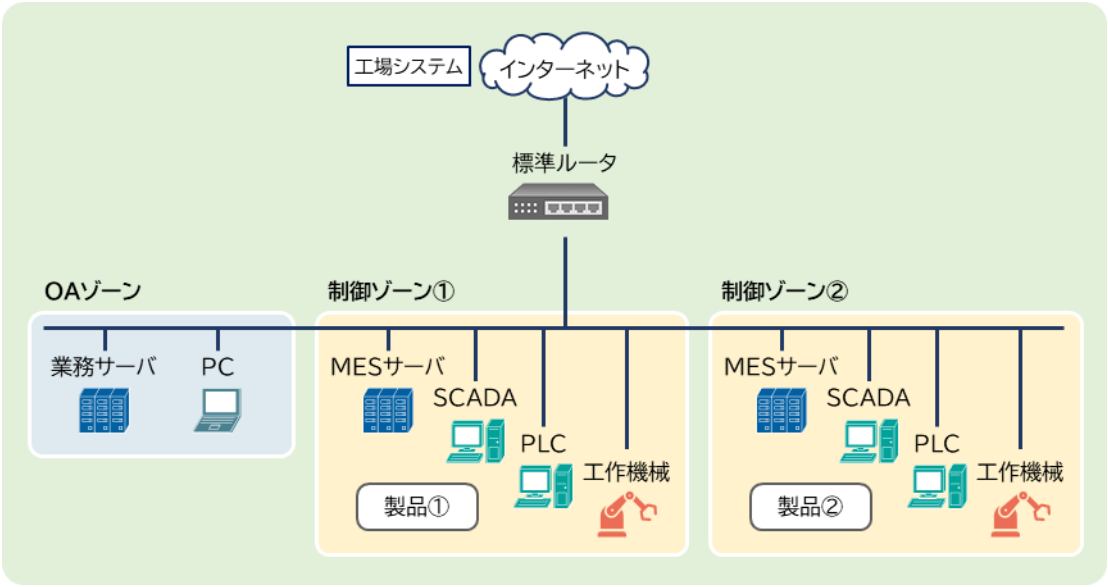

図 3-3 想定工場において守るべき対象を整理した例

表 3-5 守るべき対象をゾーンに整理した概要

ゾーンの名称	ゾーンとしてまとめた機器群
OA ゾーン	生産への影響が少ない機器群
制御ゾーン①	製品①の生産に影響がある機器群
制御ゾーン②	製品②の生産に影響がある機器群

3.3 ネットワーク分割とセキュリティ対策の実装例

3.3.1 ゾーンごとの分割

サイバー攻撃を受けた際の影響を最小化するためには、ゾーンごとにネットワークの分割が可能なルータを導入する必要がある。

図 3-4 には、3.2.4 項の想定工場においてゾーンの分割を行ったネットワーク構成図を示している。ここでは、ネットワークを、生産計画の策定や一般業務を担う OA ゾーン、製品①の製造を担う制御ゾーン①、製品②の製造を担う制御ゾーン②の 3 つに分割している。また、表 3-6 に各ルータの概要をまとめている。

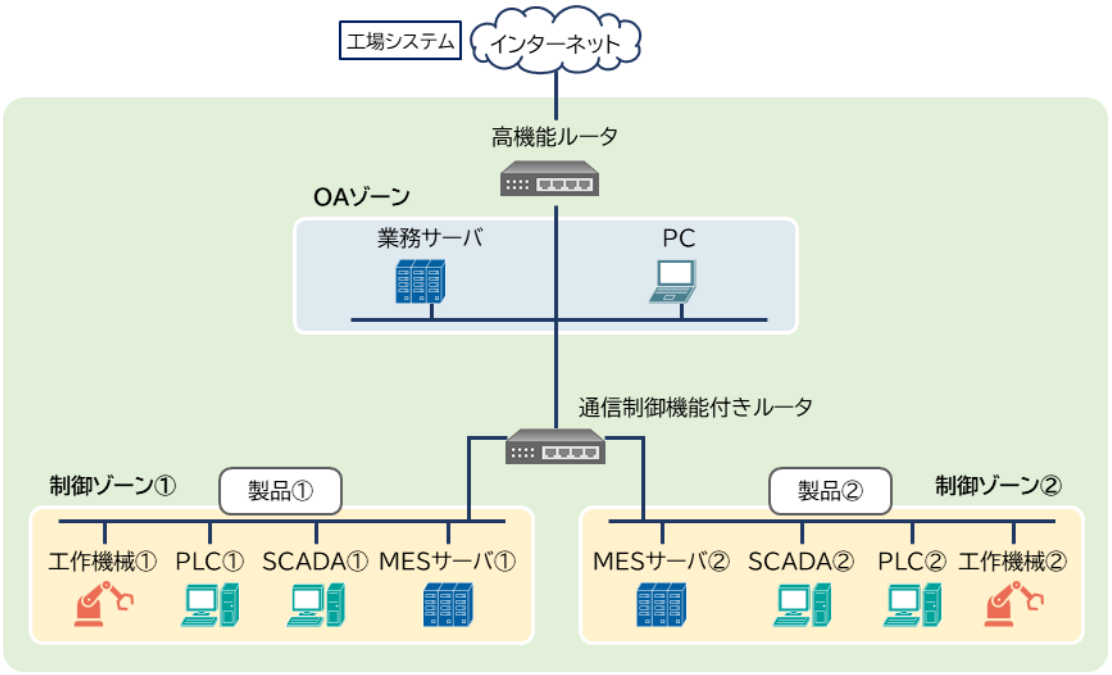

図 3-4 想定工場における守るべき対象の分割イメージ

表 3-6 各ルータの概要

ルータ名	概要	セキュリティ上の効果
標準ルータ	インターネット回線の契約に合わせて貸与されるルータや、標準設定のままで使用している市販の汎用ルータ	有害な通信を通過させてしまう場合があり、効果が限定的
通信制御機能付きルータ	通信制御のための設定を適切に行ったルータ	通信の宛先や送信元に基づいて通信を制御するため、一定の効果がある
高機能ルータ	ファイアウォールや侵入検知・防御（IPS・IDS）の機能を有するルータ	通信の宛先や送信元に加えて通信の内容も確認して通信を制御するため、大きな効果が見込める

【参考】適切でない設定がなされていたケース②

ファイアウォールの導入後の運用において、適切でない設定がなされていたケースを紹介する。

工場のライン変更や合理化に伴い、新たな機器・機能を工場に追加する際には、機器間の通信も変更となるため、ファイアウォールの設定を変更・修正する必要がある。その際に、追加する機器・機能が正常に動作することを優先して、ファイアウォールの設定の見直しが後回しになることがある。例として、構築フェーズにおいて全ての通信を許可する状態にし、そのまま放置されるケースも確認されている。

そのため、新たな機器・機能を工場に追加する際には、セキュリティ関連の設計・実装・検証を併せて実施する必要があり、ベンダへ依頼する場合において、それらを明確に指示することが重要である。

3.3.2 ゾーン内における追加的セキュリティ対策

ゾーン内における追加的なセキュリティ対策については、資産の重要度に応じて必要な強度の対策を実施することが望ましい。より詳細については、ガイドライン本編を参照いただきたい。また、表 3-7 は、各機器等が停止した場合の影響に応じたセキュリティ対策の例である。

表 3-7 各機器等に対するセキュリティ対策（例）

対策項目	最低限	各機器等が停止した場合の影響（「＋」は、左欄の対策に加えて実施する対策を意味する）	
		中	大
通信制限	不要サービス閉塞	＋通信先制限	＋FW の導入
不要ポート	端子キャップ	＋ソフト閉塞（サービスの停止、USB クラス制限等）	＋ハード閉塞（完全に利用不可）
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、パスワードポリシー策定	＋個人 ID 認証（1 要素認証）	＋多要素認証
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
資源保護（CPU、メモリ、ディスク）	－	定期確認	＋保護ツール活用
ログ取得	システムログ取得（処理負荷への影響を考慮）	＋操作ログ取得・ログ連携	＋ログ分析の仕組み整備

【参考】工場に導入している機器や機能の洗出しに問題があったケース

コストをかけてセキュリティ対策を導入したにもかかわらず、工場に導入している機器や機能の洗出しに問題があったため、製造に影響を及ぼしたケースを紹介する。

セキュリティ対策としては、通信などを制御できる機器(ファイアウォール、ルータなど)を導入する場合が多い。

このため、工場に導入している機器や機能の洗出しが不十分である場合には、誤った通信の制御により既存機器の通信を遮断してしまい、既存機器の動作不安定や動作不良を起こして工場が停止する可能性がある。

セキュリティ対策を導入する場合は、工場に導入している機器や機能について十分に洗い出して整理した情報に基づき、通信制御の設定を行う必要がある。

なお、洗出しが困難な場合は、段階的に通信制御を実施する方法もある。

これらを、セキュリティ対策を実施する部門やベンダと共有する必要がある。

4 まとめ

本書では、ガイドライン本編の解説書として、主に工場を有する中小規模の製造事業者の経営層と工場セキュリティの担当者に選任された方に向けて、工場セキュリティの重要性とその取組の始め方を説明した。

また、2 章では、工場の経営層に向けて、工場がサイバー攻撃を受けた際の影響やサイバー攻撃による工場の被害事例を紹介し、コストをかけずとも実施できるセキュリティ対策について記載した。さらに、3 章では、主に工場セキュリティの担当者に向けて、工場セキュリティを検討する際の重要な考え方と、具体的な手順に沿った対策の実施例について解説を行った。

本書では、工場セキュリティの始め方を紹介したが、ガイドライン本編においても説明されているように、セキュリティ対策の実施後も定期的に見直しを行うことが重要である。

本書を契機として、中小規模の製造事業者における工場セキュリティの意識が啓発され、製造業全体のセキュリティが向上することを期待している。

謝辞

本書の作成に当たり、一般社団法人電子情報技術産業協会（JEITA）サイバー・フィジカル・セキュリティ専門委員会、特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）西日本支部 工場セキュリティ WG、一般社団法人サイバーリスク情報センター 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（SC3）業界連携 WG 工場セキュリティ共創 SWG の皆様に御協力をいただきました。皆様の多大なる御協力に感謝いたします。