経済産業省

参考資料２

「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」 概要資料

経済産業省

サイバーセキュリティ課

産業機械課

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　～全体概要～

ガイドラインの背景・目的

- 工場のIoT化によるネットワーク接続機会の増加に伴いサイバー攻撃リスクが増加。また、ネットワークの接続に乏しい工場であっても不正侵入者等による攻撃の可能性あり。
- 意図的な攻撃の場合もあれば、たまたま攻撃される場合もある。

→**いかなる工場でもサイバー攻撃のリスクあり**。

- 本ガイドは業界団体や個社が自ら対策を企画・実行するに当たり、参照すべき考え方やステップを示した「手引き」。

→**各業界・業種が自ら工場のセキュリティ対策を立案・実行**することで、**工場のセキュリティの底上げを図ることが目的**。

想定する読者の方

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

※想定読者が経営層（CTO、CIO、CISO）をはじめとした意思決定層と適切なコミュニケーションを行うことが重要。

対策に取り組む効果

- **工場のBC／SQDC※の価値がサイバー攻撃により毀損されることを防止**。
- セキュリティが担保されることでIoT化や自動化が進み、多くの工場から新たな付加価値が生み出されていくことを期待。

※ 安全確保(S：Safety)、
事業／生産継続(BC：Business Continuity)
品質確保(Q：Quality)
納期遵守・遅延防止(D：Delivery)
コスト低減(C：Cost)

セキュリティ対策企画・導入の進め方

ステップ 1　内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2**　業務の整理
- **ステップ1-3**　業務の重要度の設定
- **ステップ1-4**　保護対象の整理
- **ステップ1-5**　保護対象の重要度の設定
- **ステップ1-6**　ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7**　ゾーンと、セキュリティ脅威の影響の整理

ステップ 2　セキュリティ対策の立案

- **ステップ2-1**　セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ

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

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

ステップ 3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策

(1)ライフサイクルでの対策
① 運用・管理面のセキュリティ対策
A) サイバー攻撃の早期認識と対処（OODAプロセス）
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) 情報共有

②維持・改善面のセキュリティ対策
・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
・組織・人材のスキル向上（教育、模擬訓練等

(2) サプライチェーン対策
・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

経営者の皆様へ ～ 工場のサイバーセキュリティ対策の推進に向けて ～

工場にサイバーセキュリティ対策が求められる背景

- 工場のIoT化や自動化に伴い工場をインターネット等のネットワークに接続する機会が増加する結果、サイバーセキュリティ上のリスクが増大。また、インターネット接続の機会に乏しい工場であっても不正侵入者等による攻撃を受ける場合もあり。
- **サイバー攻撃は、意図的に狙われる場合もあれば、たまたま攻撃される場合もある**。

- **いかなる工場においてもサイバー攻撃を受ける可能性あり**。
- 特に、一般的に製造業／工場では、**安全確保**(S：Safety)、**事業／生産継続**(BC：Business Continuity)、**品質確保**(Q：Quality)、**納期遵守・遅延防止**(D：Delivery)、**コスト低減**(C：Cost)という価値が重視されているが、**サイバー攻撃はこれらを脅かすおそれがある**。

- **セキュリティの推進は経営層等の意思決定を行う者による体制の構築や適切な指示が重要**。本ガイドラインは、対策を行う実務層向けのものであり、工場のセキュリティ対策を行うにあたり参照すべき考え方や対策のステップを「手引き」として示している。

本ガイドラインの目的

- 各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的。

想定読者

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

(2) ガイドラインの構成（１．はじめに）

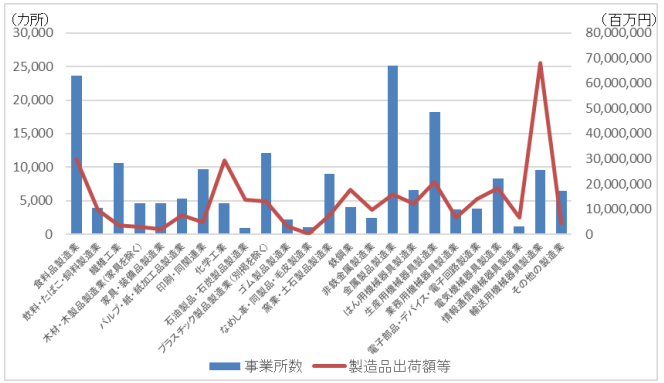
● 「１．はじめに」において、本ガイドラインの目的や想定読者、想定機器・システムを記載。

【ガイドラインの目的】

- 工場をインターネット等のネットワークにつなぐことによるセキュリティリスクが増加。
- 工場DXに伴い、クラウドやサプライチェーンのシステムと直接接続された工場におけるセキュリティも考慮する必要。
- インターネット接続の機会に乏しい工場についても不正侵入者等による攻撃を受ける場合もある。
- 攻撃の態様により、特定の工場が狙われる場合もあれば、たまたま攻撃した先が工場である場合もある。

したがって、いかなる工場においても、サイバー攻撃を受ける可能性があることを認識する必要がある。

- 一般的に、製造業／工場では、「安全確保(S：Safety)」「事業／生産継続(BC：Business Continuity)」「品質確保(Q：Quality)」「納期遵守・遅延防止(D：Delivery)」「コスト低減(C：Cost)」という価値を重視。
- 工場といっても、業界・業種ごとに実施すべき事項は異なることから、本ガイドラインは**特定の業界・業種や製造する製品という観点で対象を限定したものではない。**
- 業界団体や個社が**自ら対策を企画・実行するに当たり、参照すべき考え方やステップを「手引き」として示し、必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記**している。
- 重要なことは、業界団体や個社が、本ガイドラインに示した考え方やステップ、対策を参照しつつ、業界・業種の事情に応じたガイドラインを作成するなどしながら工場へのセキュリティ対策を進めていく、といった行動に移すことである。
- 本ガイドラインは、**各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティの底上げを図ることを目的**としている。



出所）経済産業省工業統計調査（2020年確報）を元に作成
図 1-1 製造業における事業所数・製造品出荷額等（2019年）

【ガイドラインの適用範囲】

- 本ガイドラインの想定読者は以下を想定。**部門間・担当間の立場や価値観の違いを認識しつつ、コミュニケーション**を行っていくことが重要。
  セキュリティの考え方が経営層（CTO、CIO、CISO等）を始めとした意思決定を行う者に浸透していない場合には、想定読者が適切なコミュニケーションを行うことが重要。
  - ✓ ITシステム部門
  - ✓ 生産関係部門（生産技術部門、生産管理部門、工作部門 等）
  - ✓ 戦略マネジメント部門（経営企画等）
  - ✓ 監査部門
  - ✓ 機器システム提供ベンダ、機器メーカ（サプライチェーンを構成する調達先を含む）
- 本ガイドラインの対象機器・システムは、**新設・既設によらず、工場における産業制御システム(ICS/OT)**としており、事務系の情報システム（IT）は対象としない。

(2) ガイドラインの構成（２．本ガイドラインの想定工場）

- 工場システムのセキュリティ対策のステップを提示するにあたり、わかりやすさの観点から具体例の1つとしてある工場を想定工場として設定。

※読者の置かれた環境と想定工場とが必ずしも一致しない部分もあると考えられるため、読者の置かれた環境に応じ適宜読み替え。

【想定企業】

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

【想定組織構成】

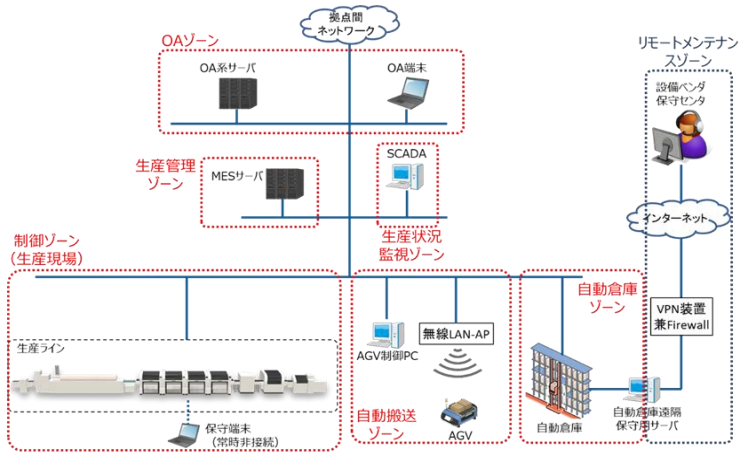
- 生産技術・管理部門
- 工作部門
- 営業部門
- 資材部門
- 品質管理部門
- 情報システム部門

【想定生産ライン】

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

(2) ガイドラインの構成（２．本ガイドラインの想定工場）

【想定システム、ゾーン※】



【想定業務】

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

【想定データ】

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

【工場システム例における構成要素】

- ネットワーク
  - 設備系ネットワーク※
  - 生産管理系ネットワーク※
  - 情報系ネットワーク
- 装置・機器（機能・プログラム）
  - VPN装置兼ファイアウォール
  - 無線LAN-AP
  - MESサーバ
  - 生産ライン
  - SCADA
  - 保守端末（常時非接続）
  - AGV制御PC
  - AGV
  - 自動倉庫
  - 自動倉庫遠隔保守用サーバ
  - OA系サーバ
  - OA端末

※近年、設備系ネットワークや生産情報系ネットワークから情報系ネットワークを経由することなく、直接インターネットに接続できる経路も増えているが、そのような場合でも、本ガイドラインに示したステップや対策は活用可能。

※工場といってもその分類や規模は様々であり、機器やシステムも千差万別である。そこで、現場感と矛盾しない効果的な対策が立案できるよう、ある抽象的なモデルから具体的な対策を立案するアプローチではなく、現場の業務から立脚し、工場の機器やシステムを大きな括りの概念として俯瞰的に捉えるためのゾーンを設定し、セキュリティ対策を立案するアプローチを提示している。

(2) ガイドラインの構成（３．セキュリティ対策企画・導入の進め方）

- 工場システムのセキュリティ対策を企画・導入するステップや対策の概略を提示。
- 想定工場に基づき考えられることを例示したものであり、各ステップにおいて、個社や業界ごとに適した整理や考え方の定義を行うことが必要である旨明記。

ステップ 1

内外要件（経営層の取組や法令等）や業務、保護対象等の整理

- **ステップ1-1**
  セキュリティ対策検討・企画に必要な要件の整理
  (1)経営目標等の整理
  (2)外部要件の整理
  (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **ステップ1-3** 業務の重要度の設定
- **ステップ1-4** 保護対象の整理
- **ステップ1-5** 保護対象の重要度の設定
- **ステップ1-6** ゾーンの整理とゾーンと業務、保護対象の結びつけ
- **ステップ1-7** ゾーンと、セキュリティ脅威の影響の整理

ステップ 2

セキュリティ対策の立案

- **ステップ2-1** セキュリティ対策方針の策定
- **ステップ2-2**
  想定脅威に対するセキュリティ対策の対応づけ
  (1)システム構成面での対策
  ① ネットワークにおけるセキュリティ対策
  ② 機器におけるセキュリティ対策
  ③ 業務プログラム・利用サービスにおけるセキュリティ対策
  (2)物理面での対策
  ① 建屋にかかわる対策
  ② 電源／電気設備にかかわる対策
  ③ 環境(空調など)にかかわる対策
  ④ 水道設備にかかわる対策
  ⑤ 機器にかかわる対策
  ⑥ 物理アクセス制御にかかわる対策

ステップ 3

セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施）

- **ライフサイクルでの対策**
  サプライチェーンを考慮した対策
  (1)ライフサイクルでの対策
  ① 運用・管理面のセキュリティ対策
  A) サイバー攻撃の早期認識と対処（OODAプロセス）
  B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
  C) 情報共有
  ②維持・改善面のセキュリティ対策
  ・セキュリティ対策状況と効果の確認・評価、環境変化に関する情報収集、対策の見直し・更新
  ・組織・人材のスキル向上（教育、模擬訓練等
  (2) サプライチェーン対策
  ・取引先や調達先に対するセキュリティ対策の要請、対策状況の確認

事業や環境、技術の変化に応じて各ステップについて不断の見直しを行いながらステップのサイクルを回す

※重要度については、個社・業界の置かれた環境により様々であることから、重要度レベルについて記載しておらず、個社や業界ごとに適した重要度付けを 行うことが重要である。
※なお、重要度付けの考え方については、国際規格等（IEC62443規格群、NIST サイバーセキュリティフレームワーク、IoT-SSF）においても考え方が示されていることから、こうした考え方も参照することが有効である。

(2) ガイドラインの構成（3-ステップ1　内外要件や業務、保護対象等の整理）

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

ステップ1-1　セキュリティ対策検討・企画に必要な要件の整理 【3.1.1】	**（１）経営目標等の整理** 工場のセキュリティ対策に関わる経営目標（事業伸張、事業継続等）を整理する。特に、事業継続の観点では、事業継続計画（BCP）が策定されているかが重要であるため、その内容を確認する。BCPが整備されていなければ、必要に応じて担当部署とともに策定の検討を実施する 。 **（２）外部要件の整理** 工場のセキュリティ対策に関わる外部要件（セキュリティ法規制・標準規格・ガイドライン準拠、国・自治体／業界／市場・顧客／取引先／出資者からの要求等）を整理する。 **（３）内部要件／状況の整理** 自社の工場セキュリティに関わる内部要件（システム面、運用・管理面、維持・改善面、等）や体制を整理する。体制等が不明確である場合は、セキュリティ対策を推進するための体制やルール・手順等を整備し実施計画を立案し周知・教育等を実施する 。
ステップ1-2　業務の整理 【3.1.2】	工場システムが使われている日々の業務の洗い出しを行う。
ステップ1-3　業務の重要度の設定 【3.1.3】	洗い出した業務について、それぞれの業務の重要度を定める。
ステップ1-4　保護対象の整理 【3.1.4】	セキュリティ対策を強化すべき業務を支援／実施する工場システムの構成要素(ネットワーク、装置・機器（機能・プログラム）・データ)を洗い出し、システム構成図の模式図を整理する 。
ステップ1-5　保護対象の重要度の設定 【3.1.5】	事業伸張・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)、それによる業務の重要性の視点から、洗い出した保護対象それぞれの重要度を明確にする。
ステップ1-6　ゾーンの整理と、ゾーンと業務、保護対象の結びつけ【3.1.6】	業務の重要度が同等であり、同等の水準のセキュリティ対策が求められる領域として、ゾーンを設定する。ゾーンごとに、これまでに整理した業務、保護対象を結びつける。 ※ゾーンを設定することにより、工場の機器やシステムを大きな括りの概念として俯瞰的に見ることが可能となり、あるゾーン内の保護対象がサイバー攻撃を受けた際、別のゾーンへ影響が及ぶことを抑止し、被害を極小化することを検討することが可能となる。
ステップ1-7　ゾーンと、セキュリティ脅威の影響の整理 【3.1.7】	最新の脅威について認識した上で、こうした脅威と生産・事業への影響を勘案し、それぞれのゾーンに対するセキュリティ脅威と影響を整理する。

【参考】整理すべき事項の観点の例

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

経営目標	内容
事業伸張の視点	製造設備の増強・高度化
	工場におけるカーボンニュートラル推進
	調達先の分散や標準化・共通化の推進等サプライチェーン強靭化
事業継続の視点	製造設備停止・不調、製品の品質低下、サービス停止・遅延等による事業上の損失防止
	製品等の機密情報や顧客情報の窃取・漏えいによる社会からの信頼低下の防止
	製造に必要なデータの改ざん・破壊による事業停止の防止
	製造設備の不具合や暴走等による従業員や近隣住民の安全・健康、有害物質の排出等環境面の被害の防止
	工場システムの機能不全や製品の品質不備による製品利用者の安全・健康、製品廃棄後の環境面への被害の防止

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

外部要求事項	内容
ビジネス上の要求	取引先からの要求
	法規制への対応　（国・自治体）
	国からの要求
	産業界、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
標準規格対応	ガイドライン・標準規格への準拠

セキュリティ対策を検討・企画する際に考慮すべき内部要求事項

セキュリティ対策	内容
方針・体制	セキュリティポリシー
	事業継続計画（BCP）
	セキュリティ推進体制
	セキュリティ関連ルール、手順　等
	セキュリティ対策実施計画　等
システム面	ネットワーク
	装置、機器
	業務プログラム、利用サービス
運用・管理面	セキュリティ監視・異常検知
	セキュリティ管理
	情報共有
維持・改善面	セキュリティ教育
	継続的なリスク対応（確認、改善・見直し）

【参考】一般的な脅威と生産への影響の例

	脅威種別	脅威内容	生産・事業への影響
1	機器の盗難、システム・機器に対する破壊・不正操作	物理的な侵入による、システム・機器に対する直接的な破壊・盗難・不正操作	• 生産性低下による納期遅れや原価上昇 • 設備故障、盗難による損害システム・機器材に対する破壊行為による生産停止等
2		直接的な不正接続によるシステム・機器の破壊・不正操作	
3		ネットワーク経由の侵入、または内部からの不正通信（バックドアやコネクトバック通信）を利用したシステム・機器の破壊、不正操作	
4	設備の異常な制御や停止	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停止	
6		設備の安全制御の機能停止	
7	データ盗難・漏えい	USBなどへの不正コピー	• 生産情報や品質保証ノウハウの流出 • 顧客情報の流出と、それに伴うブランド毀損
8		不正なサーバへのアップロード	
9		パケットの盗聴（通信データの盗聴）	
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・消去	
12		パケットの改ざん（通信データの改ざん）	
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		ネットワーク停止・容量オーバ	
15		設備・サーバ・PCの停止	
16		リソースの不足	
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 • 操作中のライン停止に伴う納期遅れの発生
18	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
19		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	
20		通信機器の障害・故障	
21		設備・サーバ・PCの障害・故障	
22	従業員、保守要員（設備ベンダ）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)
23		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
24	施設や作業環境の脅威	漏電、火気不始末等による火災、近隣からの延焼	• 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
25		積載した資材等の崩落	
26		化学薬品などによる爆発	
27		電磁波による電子機器の損傷	
28	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
29		有害生物の侵入	
30		地震などによる機器の転倒・落下	
31		落雷、洪水、地震などによる停電・瞬断・電圧変動	

【参考】攻撃者の動機

- 最近のサイバー攻撃は、攻撃の目的が明確で、かつ、目的達成まで執拗に攻撃が繰り返される傾向が認められる。また、攻撃者の種別も、情報収集や破壊工作を目的とした軍隊や諜報機関といった国家レベルの組織、身代金目的の犯罪集団、内部不正を犯す関係者など、多様になっている。そのため、事前に攻撃者の動機を想定し、万一サイバー攻撃を受けたときに、生産にどのような影響が起こりうるかを想定しておくことが重要である。
- 一方、攻撃者は意図的に工場を狙ったわけではなく、たまたま攻撃した先が工場という場合もある。自社は犯罪組織等に狙われることはないと考えるのではなく、流れ弾に当たるということも想定しておく必要がある。

	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	企業価値毀損	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、企業価値を毀損する	・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

(2) ガイドラインの構成（3-ステップ2　セキュリティ対策の立案）

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

- **ステップ2-1　セキュリティ対策方針の策定【3.2.1】**
  - ステップ１で整理したゾーンとこれに紐づく業務、保護対象、想定脅威に対して、業界や個社の置かれた環境に応じ、重要度・優先度を設定する。
- **ステップ2-2　想定脅威に対するセキュリティ対策の対応づけ【3.2.2】**
  - どのようなセキュリティ対策が対応づけられるのか整理する。脅威に対応するためには物理面、システム構成面どちらか一方でなく双方の対策が重要となるため、参照されたい。

(1)システム構成面での対策

①ネットワークにおけるセキュリティ対策（例）

対策項目	セキュリティ強度ごとの対策		
	最低限	中	高
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制限	＋接続機器の論理証明 ＋接続機器の信頼性確保
内部秘匿	－	NAT、ステルス	不正通信防止（ゲートウェイ）
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、 パスワードポリシー策定	＋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（NDR）、 異常検知（IDS）	＋異常通信遮断 （IPS、フィルタリング）
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 ＋回避策	＋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 （処理負荷への影響を考慮）	＋IDSログ連携	＋ログ分析の仕組み整備

※ 表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。

②機器におけるセキュリティ対策（例）

※ 表は例示であり、内容について個社や業界に応じて精査が必要な場合がある。

対策項目	セキュリティ対策強度		
	最低限	中	高
通信制限	不要サービス閉塞	＋通信先制限	＋FWの導入
不要ポート	端子キャップ	＋ソフト閉塞 (サービスの停止、USBクラス制限等)	＋ハード閉塞（完全に利用不可）
利用ポート	－	持込媒体の検査（目視や管理票等で外形的に検査）	＋持込媒体のシステムチェック等（ウイルスチェック等でコンテンツやプログラムまでを検査）
通信／接続機器認証	－	IP、MAC、デバイスID認証	＋相手機器の論理証明(暗号による)
送受信データ保護	－	暗号化、暗号鍵の管理	＋暗号鍵の厳密な保護
利用者制限	不要ユーザ削除、 パスワードポリシー策定	＋個人ID認証(1要素認証)	＋多要素認証
実行プログラム保護	－	プログラム改ざん対策	＋保護ツール活用
実行プログラム制御	不要プログラム停止・削除、 ユーザグループ管理	＋グループ実行権限付与、 ユーザ権限動作	＋実行制御ツール活用
ファイル保護	ユーザグループ管理	＋暗号化	＋保護ツール活用
資源保護 (CPU、メモリ、 ディスク)	－	定期確認	＋保護ツール活用
構成管理	－	機器内の構成管理・可視化	＋設定情報管理・可視化
脆弱性対策	脆弱性情報収集	＋脆弱性診断、侵入可否検査、緩和策の適用	＋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 （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
バックアップ (データ、機器)	－	定期オフライン データバックアップ	＋切替え機器の確保
電源可用性確保	－	UPSの導入	＋自家発電設備の導入

③業務プログラム・利用サービスにおけるセキュリティ対策（例）

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

(2) ガイドラインの構成（3-ステップ2　セキュリティ対策の立案）

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

(2)物理面での対策

①建屋に関わる対策	● 工場建屋は、生産現場を中心に生産設備、自動搬送・倉庫設備、建物設備などを各室に配置した建物であり、その中でも、生産に不可欠な生産システム、自動搬送・倉庫システム、システム間ネットワーク、及びそれらを構成する装置・機器などを、安定的かつ継続的に運用するのに最適な環境及び基盤を提供することが必要となる。
②電源／電気設備に関わる対策	● 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る。このため、生産設備、自動搬送・倉庫設備などとBAS(ビルディング・オートメーション・システム)とを連動させた設備監視体制の構築、信頼度の高い電源設備構成の構築などが求められる。
③環境(空調など)に関わる対策	● 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、湿度、静電気抑制、空気清浄度などの諸条件を考慮する必要がある。
④水道設備に関わる対策	● 工場には、水道がないと稼働しない機器がある。設備に使用する冷却水は、循環式が多く循環が停止すると冷却効率の低下や最悪設備停止に至ることもあることから、例えば、冷却水配管の冗長化、ポンプの冗長化、台数制御にて停止時間を少なくする等の対策を行うことが考えられる 。 ● また、水道設備停止時への対策も必要であり、異常による停止・故障だけでなくポンプ整備などの設備保全時にも停止できるような設計とすることが考えられる。
⑤機器に関わる対策	● 工場システムに用いる機器 に対する、設置場所や利用業務の重要性に応じ、また運用面も考慮した上で、セキュリティ対策を行うことが考えられる。
⑥物理アクセス制御に関わる対策	● 物理アクセス制御は、生産設備・計算機などの産業制御システム／機器や、それらに付随する情報システムなどへの物理的なアクセスに対する保護を指す。具体的には、産業制御システム／機器の専用室(サーバ室・計算機室)の設置、入退管理システムの導入、監視カメラの設置、管理・監視体制の構築、といった対策が挙げられる。

(2) ガイドラインの構成（3-ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施））

- ステップ3ではライフサイクルでの対策、及びサプライチェーンを考慮した対策を実施する。
- これらの取組により得られた情報により、ステップ3の後は、事業や環境、技術の変化等に応じて計画・対策・運用状況の見直しを行い、必要に応じてステップ1から改めて取組を進めるなどのサイクルを回すことが重要である。

(1)ライフサイクルでの対策

①運用・管理面のセキュリティ対策

A）サイバー攻撃の早期認識と対処（OODAプロセス）

サイバー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付き対処する一連の運用業務にサイバー攻撃の視点での監視を加えることが考えられる。また、迅速な対処を実現するために、異常の兆候や問題・被害の発生を想定し、あらかじめ役割・体制や手順を整備しておくことが考えられる。

B）セキュリティ管理(ID/PW管理、機器の設定変更など)

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やそれに基づく標準的な手順の作成・実施と、関係者への徹底を行うことが考えられる。

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

なお、ヒューマンエラーへの対策として、セキュリティに関する業務に対する過失や疲労への対策、及びセキュリティに関するルールや意識付け・教育の不備等への対策についても考慮することが望ましい。

C）情報共有

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

※業種や対象によって入手可能な情報に差があることに留意。こうした状況にあって可能な限り情報を入手・共有するためには、脅威情報や効果的な対策等、各社の対策に資する情報について、業界やコミュニティ等を通じて情報共有を行うことが望ましい。

②維持・改善面のセキュリティ対策

セキュリティ対策の実施・運用状況とその効果を確認した上で、工場システムを取り巻く環境の変化に関わる情報を収集し、BC／SQDC確保の観点も踏まえて、セキュリティ対策を評価し、必要に応じて物理面、システム面、運用・管理面のセキュリティ対策を見直し、更新する。

(2) ガイドラインの構成（3-ステップ3　セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し（PDCAサイクルの実施））

(2)サプライチェーン対策

- サプライチェーンの広がりとともに、大企業から中小企業までが関わるサプライチェーンの中でも、セキュリティ対策が進んでいない企業がサイバー攻撃によって狙われる事例が増加。
- 対策予算や人材に限りがある中小企業においても、自分たちの事業を守るために工場におけるセキュリティ対策を進める必要。
- グローバル化の進展の中で、サプライチェーンもグローバル化しているため、グローバルなビジネスを行っている企業は、世界情勢の考慮や、各国の法制度あるいは標準規格やガイドライン等に準拠した対策を進める必要。

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

取引先や調達先への主な確認ポイント（例）

購入製品／部品	● 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 ● 廃棄時の情報漏えいリスクを考慮した取決めを実施しているか
業務委託	● 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 ● 再委託が許可されている場合、再委託先のセキュリティ管理を行っているか。また、セキュリティ管理内容は、自社と同等、もしくはより厳しい内容となっているか
システム開発受託	● 開発プロセスの各フェーズにおいて、セキュリティを考慮する要件が記載されているか ● 成果物の検収時に、セキュリティ仕様及び実装状況の確認が記載されているか ● 取扱い情報の守秘義務に関する要件が記載されているか ● 委託終了時に、情報を破棄することが記載されているか ● 開発環境に関するセキュリティ要件が記載されているか ● 監査に関する要件が記載されているか
連携システム	● 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 ● 共有する情報の取扱いや保護に関する規約や取り決めを定めているか

【参考】稼働中の工場と新設の工場における対策の考慮

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

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る。システム構成面の対策については、稼働中の工場システムへ影響のない対策を優先しつつ、影響がある対策が必要な場合には、工場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する。
- また、物理面での対策やライフサイクルでの対策を充実させることで補うことも検討する。

更新間際である場合

- システム構成面の対策については、工場システムのうち更新対象部分と、継続利用する部分との間で、対策の強度に差が生じないように考慮する必要がある。
- 既存部分へのシステム構成面の対策導入が難しい場合は、既存部分が攻撃や不正の抜け穴とならないように、物理面での対策やライフサイクルでの対策を充実させることで補うことも検討する。

新設計画中である場合

- 新設の場合、稼働中や既存の工場システムに比べ、セキュリティ対策導入はしやすい利点がある。一方で、工場システムは、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する。
- 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る。

【参考】付録B　工場システムを取り巻く社会的要件

- 工場システムを取り巻く社会的要件や要求を、法規則や標準規格・ガイドライン準拠、国・自治体産業界など、さまざまな視点から整理する。

B-1　法規制、標準規格、ガイドライン準拠に関わる要件	**B-1.1　法規制によるセキュリティ対策の要求** ● 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 や忠実義務　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（けたい）責任 や第三者に対する損害賠償責任　を問われる可能性がある。また、サイバーセキュリティ攻撃に対して迅速かつ的確な対処を怠った場合にも、同様に不法行為として問われる場合がある。 **B-1.2　セキュリティに関わる標準規格・ガイドライン準拠の要求** ● 何をどの程度実施すべきかの参照情報として、国内外の規格やガイドライン更に法規などがあり、更に取引先が規定している要件などもある。
B-2　国・自治体からの要求	● 法令(労働安全基準法、環境基本法など) やガイドラインに関わる問題がないかを確認する必要がある。 ● 国や自治体と工場システムを介する場合など、相互のシステムを連携する場合に、セキュリティ要件が規定されている場合がある。 ● 国や自治体が導入する製品の調達基準の中に、製品自体のセキュリティ対策要件や、製品の生産システム／工程におけるセキュリティ確保を目的とした要件が明示される場合がある。
B-3　産業界からの要求	● 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原則を示している。
B-4　市場・顧客からの要求	● 標準規格「IEC62443」や、サイバーセキュリティに関わるグローバルに参照されている米国「NIST SP 800シリーズ」、経済産業省の産業分野別セキュリティ対策ガイドラインなどへの対応が要求される場合も増えている。
B-5　取引先からの要求	● 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)が含まれることのないように、工場の製品生産過程におけるセキュリティ対策を要求される場合もある。
B-6　出資者からの要求	● 工場システムのセキュリティ対策を検討・企画するときに、出資者からセキュリティ対策要求を求められる場合がある。

【参考】付録C　関係文書におけるセキュリティ対策レベルの考え方

- 代表的なセキュリティ対策レベル評価基準「IEC 62443」、「NIST サイバーセキュリティフレームワーク」、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)」における評価基準とセキュリティ対策レベル定義例の概略を提示。

C-1　代表的なセキュリティ対策評価基準

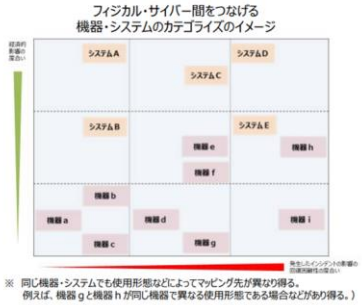
(1)IEC 62443規格群
脅威がどの程度のスキルを持つ攻撃者によるものかを示す5つの観点から脅威レベルを評価。

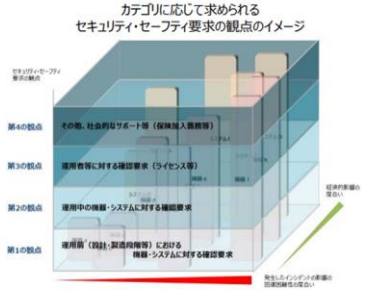
レベル	悪意	手段	リソース	スキル	動機
1	なし	－	－	－	－
2	あり	単純	低	汎用	低
3	あり	複雑	中	固有	中
4	あり	複雑	高	固有	高

(2)NIST サイバーセキュリティフレームワーク
マネジメントの成熟度を軸にしたレベル評価。

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

(3)経済産業省「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」
IoT機器・システムにおける「セキュリティ・セーフティ要求レベル」(リスク)を2つの軸「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。





C-2　セキュリティ対策を行う度合いの定義例

(1)システムに関する対策の度合い例
「どの程度のセキュリティ脅威からシステムを守ることができるか」を評価することが目的となる。
(2)運用に関する対策の度合い例
「OODAプロセスを円滑に実施できる状況にあるか」を評価することが目的となる。サイバー攻撃が発生したときに、「いかに早く認識し的確に対処できるか」の視点で、レベルを設定する。
(3)マネジメントに関する対策の度合い例
「各種情報を元に最適な見直しを行っているか」を評価することが目的となる。

【参考】付録E　チェックリスト

- 特に実施いただきたい対策について、具体的な実施内容をイメージし、対策ができているか確認いただくためのチェックリストを5カテゴリ、5段階の達成度で提示。

カテゴリ

- 準備
- 組織的対策
- 運用的対策（システム関連等）
- 技術的対策
- 工場システムサプライチェーン管理

なお、チェックリストの確認項目は例示であり、読者の状況に応じて、項目の追加・削除や、内容の修正を行っても構わない。

達成度

各カテゴリに示した対策の達成度を以下の５段階で評価し、工場セキュリティの現状をチェックしていただきたい。

- １：未実施
- ２：一部実施
- ３：実施済み
- 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
- ５：実施済みで、管理手順を文書化・自動化し、随時見直し

なお、達成度の基準については、読者の状況に合わせて簡素化して用いても構わない。

付録 E-1 チェックリスト

カテゴリ	番号	確認項目	達成度	参照
準備	0-1	工場システムにおけるセキュリティ対策の検討・企画に必要な経営目標、外部要件、内部要件/状況を整理する。		3.1.1 ステップ 1-1
	0-2	工場システムにおける業務・保護対象の整理及び重要度の設定を行う。この結果を踏まえてゾーンを設定し、業務・保護対象を結びつけ、セキュリティ脅威との影響の整理を行う。		3.1.1 ステップ 1-2 ～ステップ 1-7
	0-3	工場システムに関する内外の要件や、業務・保護対象・ゾーン等の情報の収集・整理結果に基づき、工場システムのセキュリティ対策方針を策定し、想定脅威に対する対策の対応づけを行う。		3.2 ステップ 2-1 ステップ 2-2
組織的対策	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）又は経営層が認識を持っており、十分な予算・人員配置などの協力を得られる状態にある。		3.1.1(4) 内部要件／状況の整理
	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。		3.1.1(4) 内部要件／状況の整理
	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。		3.1.1(4) 内部要件／状況の整理
	1-4	事業継続計画（BCP）が策定されており、工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。		3.1.1(2) 経営目標等の整理 3.1.1(4) 内部要件／状況の整理

【参考】付録E　チェックリスト

カテゴリ	番号	確認項目	達成度	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。		3.3(1) ライフサイクルでの対策
運用的対策（システム関連等）	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している		3.1.1(2) 経営目標等の整理
	2-2	工場システムにおける専用のセキュリティポリシーが規定されていて、認知されている。		3.1.1(4) 内部要件／状況の整理
	2-3	工場内のシステムからの電子メールやインターネットアクセスはポリシによって禁止している。		3.1.1(4) 内部要件／状況の整理
	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。		3.1.1(4) 内部要件／状況の整理
	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。		3.3(1) ライフサイクルでの対策
	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、システム構成図を作成している。		3.1.4 保護対象の整理
	2-7	工場内に無線 LAN を導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。		3.1.4 保護対象の整理 3.2.2(1) システム構成面での対策
	2-8	システムへの侵入を可能とする攻撃手法や脆弱性を特定し、脆弱性へ対応している、又は緩和策を講じている。（脆弱性を特定する手法の例：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）、組込機器（PLC や IoT 機器など）のモデル情報やファームウェア情報の把握及び脆弱性情報の定期的な確認等(※1)）		3.2.2(1) システム構成面での対策
	2-9	工場内に外部記録媒体（USB メモリ、フラッシュデバイス）やポータルメディアの利用・持込みに関するルールを定め、運用している。		3.3(1) ライフサイクルでの対策
	2-10	工場内のシステムのパスワードの強度や有効期限等のパスワード設定の考え方を定めたルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）		3.2.2(1) システム構成面での対策
	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）を速やかに削除している。		3.2.2(1) システム構成面での対策
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウィルスに感染していないことを確認する手順がある。		3.2.2(1) システム構成面での対策
	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、バックアップデータは保護された場所に格納するとともに、定期的にバックアップデータからの復旧テストを行っている。また、その手順が明確化されている。		3.2.2(1) システム構成面での対策
技術的対策	3-1	インストールできる端末にはアンチウィルスソフト又はアプリケーションホワイトリスト（許可リスト）を導入し、インストール不可能な端末では何らかの代替策（USB 型のアンチウィルスなど）を導入している。		3.2.2(1) システム構成面での対策
	3-2	アプリケーション／オペレーティングシステム（OS）の重大な脆弱性については可能な限り速やかにセキュリティパッチを適用している。もしくは代替策を講		3.2.2(1) システム構成面での対策

【参考】付録E　チェックリスト

カテゴリ	番号	確認項目	達成度	参照
		じている。		
	3-3	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。		3.2.2(1) システム構成面での対策
	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）。又は、入退室管理、外部の入室者への関係者の付添いなど運用面での代替策を講じている。		3.2.2(2) 物理面での対策
	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN 等）。		3.2.2(1) システム構成面での対策
	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（2要素認証等）やリモートユーザ毎の接続対象機器(※2)の制限、接続可能時間の制限、メンテナンス期間外の機器接続等の異常検知、ネットワーク侵入防護などの保護対策を行っている。		3.2.2(1) システム構成面での対策
	3-7	工場内のネットワーク（情報システムとの境界やリモートアクセスを含む）の不審な通信を特定するためのネットワーク検知／防護システムを導入している。		3.2.2(1) システム構成面での対策
	3-8	工場内の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し、必要日数保存している。		3.2.2(1) システム構成面での対策
工場システムサプライチェーン管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダ・構築事業者と連絡・連携体制を構築している。		3.3(2) サプライチェーン対策
	4-2	工場システムのメンテナンス等に関わる協力会社向けのセキュリティ教育を契約開始時及び定期的に実施している。		3.3(2) サプライチェーン対策
	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・構築業者との連絡・連携体制を構築している。		3.3(2) サプライチェーン対策
	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（内部及び/または外部監査実施など）を把握できている。		3.3(2) サプライチェーン対策
	4-5	納入される工場システム機器に対して、一定のセキュリティ基準[53]を満たしているかを判定するプロセスや受入検査がある。		3.3(2) サプライチェーン対策
	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。		3.3(2) サプライチェーン対策

（※1）テレワークの普及に伴い、VPN を利用して外部から内部ネットワークに接続するケースが増えているが、近年、VPN 装置の脆弱性を突いたサイバー攻撃が継続的に見られている。多くは過去に明らかになった脆弱性であり、ベンダからの対策状況も公表されているにも関わらず、多数の被害が出ていることから、自らが利用している工場の機器・システムにおける脆弱性情報の収集・特定を行い、適時に対応することは重要である。

（※2）接続機器の健全性が確保されているか確認した上で、アクセスを許可することが望ましい。

【参考】付録F　調達仕様書テンプレート（記載例）

● 製品・サービスの調達時に考慮すべきセキュリティ要件を、調達仕様書の記載例を提示。

- 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、あらかじめセキュリティに関する要件をサプライヤに提示し、その上で調達契約を締結することが重要である。

- 調達時に考慮すべきセキュリティ要件のカテゴリは、大きく３つに分けられる。
  (1)サプライヤのセキュリティマネジメント体制
  (2)製品・サービスのセキュリティ対策
  (3)製品・サービスのライフサイクルに関わるセキュリティ対策
  ①エンジニアリング・開発時のセキュリティ対策
  ②サプライヤのサプライチェーンに関するセキュリティ対策
  ③製造・流通時のセキュリティ対策
  ④保守・サービス・廃棄に関するセキュリティ対策

例1：制御機器サプライヤへのセキュリティ要件指定の例

X.X　サプライヤが備えるべきセキュリティ要件

「中小企業の情報セキュリティ対策ガイドライン第 3 版（IPA）」を自己評価し、SECURITY ACTION の二つ星を宣言していること。

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

例2：PLC の調達仕様書のセキュリティ要件指定の例

X.X　ペネトレーションテストの実施

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

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

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

例3：PLC の製品ライフサイクルに関するセキュリティ要件指定の例

X.X　開発時のセキュリティ要件
　X.X.1　開発環境
　　X.X.1.1　開発人員の管理
　　X.X.1.2　開発環境の物理的なセキュリティ
　　X.X.1.3　開発環境のセキュリティ対策
　　X.X.1.4　開発ソフトウェア管理
X.X　使用するOSS に関するセキュリティ要件
　X.X.1　ライセンス管理の実施
　X.X.2　脆弱性管理の実施
X.X　製造・流通時のセキュリティ要件
　X.X.1　流通時のセキュリティ
　製造拠点からどのような流通経路で納品されたかの記録を保持すること。
　開封シールなど機器の改ざん防止の措置をとること。
X.X　保守・メンテナンス・廃棄時のセキュリティ要件
　X.X.1　バージョン変更時のファームウェア更新
　X.X.2　脆弱性発見時の対応
　　X.X.2.1　報告
　　X.X.2.2　対処

【参考】コラム１　工場セキュリティをめぐる動向

- 工場システムのセキュリティに関して理解を深められるよう、「コラム1　工場セキュリティをめぐる動向」を掲載。

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ある。
- 新型コロナウィ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、事業継続のための生産現場を含むテレワーク実現、環境変化への迅速な適応、柔軟なサプライチェーンの実現、業務改革などが求められている。
- サイバー・フィジカル融合により、取引先から連携が要求されたり、動的で柔軟なチェーンの実現が求められたりする。さらには、SDGs／ESG投資／グリーン(カーボンニュートラル)を目的とした、CPS実現やデジタルトランスフォーメーション(DX)の推進も重要になってきている。

工場における産業制御システムのセキュリティに関わる環境動向

- 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つながっていないシステム／機器であっても、工場従業員やシステム／機器ベンダの保守担当者などの人間が介在することで間接的につながり、サイバー攻撃を受け被害が発生しているのが現実である。また、工場従業員による不正な操作や過失がセキュリティ問題を招く場合も増えている。
- このように工場においてセキュリティリスクが増大している状況を踏まえ、米国や欧州を始めとして、工場の製品や製造プロセスに関わるセキュリティ対策を要求する取引先や製品ユーザが増えてきており、その基準となる標準規格やガイドライン等が整備されつつある。

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

- 経済産業省「2018年版ものづくり白書」によると、工場においてセキュリティ対策の実施が進んでいない理由は、大きく4つの段階に分けられる。
- ①中小企業を中心に、工場の産業制御システム／機器に対するセキュリティ対策の必要性を正しく認識／理解できていない段階の企業が多い。
- ②どのような対策が必要なのかが分からない段階の企業が多い。
- ③必要な対策を実施するためのスキルを有する人財や予算を確保できていない。
- ④実施した対策で十分なのかが分からない段階や、対策が不足していてサイバー攻撃の被害にあった場合にどうすれば良いのかが分からない。

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

- 「コラム2　工場システムの目的や製造業/工場の価値から観たセキュリティ」を掲載。

(1) 工場システム自体の目的・機能、製品事業の伸張・継続、納期遵守	● 工場システムは、製品事業の伸張や事業／生産の継続(BC：Business Continuity)を実現するために、生産性をより高め、コスト低減(C: Cost)を図るとともに、安定的かつ継続的に製品を生産するためのシステムであり、その安定・連続稼働が求められる。 ● 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／抑制する必要がある。
(2) 工場の安全確保、製品の品質確保	● 工場の安全確保(S: Safety)や、製品の品質確保(Q: Quality)を実現するために、工場システム及び機器が正常に動作する状態を保つことが求められる。 ● 工場の安全確保(S)や、製品の品質確保(Q) のために、工場システム及び機器が正常に動作する状態を保つ必要がある。
(3) 工場システムの正常動作確保や適正なフィードバック制御	● 工場システム及び機器が正常に動作する状態を保つためには、システム及び機器の機能・制御の仕方を設定・指示するデータが正しいこと、すなわちデータが壊れたり改ざんされたりしていないことが求められる。 ● 工場システム及び機器の正常動作のために、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を保つ必要がある。
(4) 製品や生産に関わる情報やデータの保護	● 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)に関わる情報やデータが外部に漏えいしないようにすることが求められる。 ● 製品や生産(ノウハウ)に関わる情報やデータが漏えいしないようにする必要がある。
(5) 製品のセキュリティ品質確保や製造責任	● 最近は、工場における製品の生産過程で、製品の部品として用いられるハードウェアやソフトウェア(プログラム)の中に、セキュリティ脅威を内包する不正なものが意図せず含まれてしまうことがあり、製品出荷後に製品内包のセキュリティ脅威により、製品が外部から不正に利用・制御されたり、製品の稼働を妨害されたり、製品利用者の情報を外部へ漏えいさせたりする問題を引き起こすことが発生する。製品の製造責任を問われることのないように、製品の品質確保(Q)の位置付けで、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ないように、工場の製品生産過程でセキュリティ対策を取ることが求められる。 ● 製品の品質確保(Q)のために、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を防止

【参考】コラム3　スマート工場への流れ

- 制御システムからスマート工場への動きがある中、セキュリティリスクとして考慮すべき点として「コラム3　スマート工場への流れ」を掲載。

【コラム3　スマート工場への流れ】

- 工場システムは最新のICTや自動化技術を活用し、情報システムやインターネットと接続する機会が増。
- 利用形態の4つの流れと、セキュリティリスクに関わる考慮すべき点を説明。

● ライン・設備改善

➢ ラインの自由度向上や生産改革のために、ロボットや自動装置の導入を行う。

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

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

● ITシステム連携

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

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

● 市中での利用（端末）

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

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

● 外部システム連携

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

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