経済産業省

資料５－１

工場システムにおけるサイバーセキュリティ対策の検討状況について

経済産業省

サイバーセキュリティ課

目次

目次

高度化・巧妙化するサイバー攻撃の現状

- **昨今のサイバー攻撃は、**企業等の情報を暗号化して金銭をゆすり取る「ランサムウェア攻撃」や、国家支援型の攻撃集団等が特定の企業を執拗に狙う「標的型攻撃」など、**多種多様**。
- 加えて、**サイバー攻撃が高度化・巧妙化**するとともに、あらゆるものがネットワークにつながり、**攻撃の起点が増加**したことで、**サイバー攻撃が社会や産業に「広く」、「深く」影響を及ぼすように**なっている。

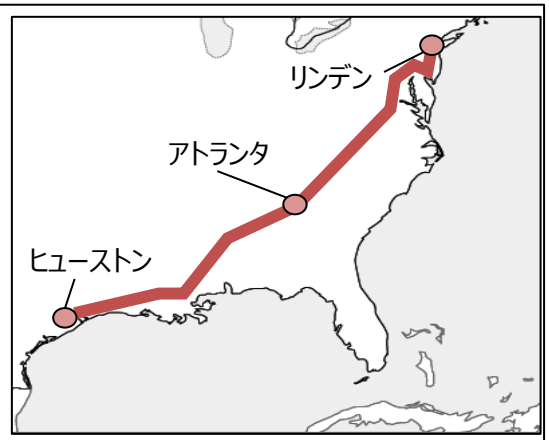
情報セキュリティ10大脅威 2022

順　位	組織向け脅威
1位	ランサムウェアによる被害
2位	標的型攻撃による機密情報窃取
3位	サプライチェーンの弱点を悪用した攻撃
4位	テレワーク等のニューノーマルな働き方を狙った攻撃
5位	内部不正による情報漏えい
6位	脆弱性対策情報の公開に伴う悪用増加
7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
8位	詐欺による金銭被害
9位	予期せぬIT基盤の障害に伴う業務停止
10位	不注意による情報漏えい等の被害

<出典：(独)情報処理推進機構(IPA)、2022.1.27>

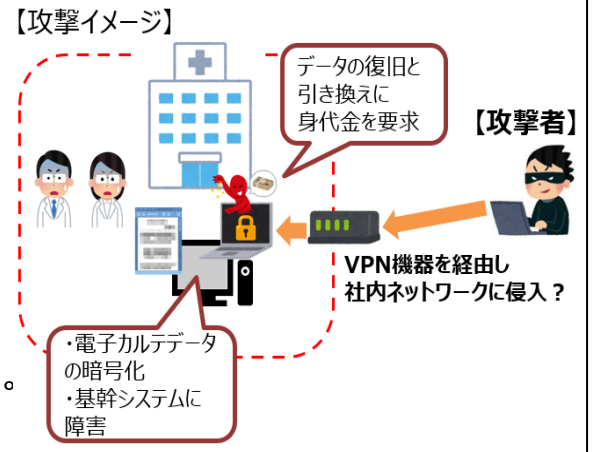
事例（海外）

- 米国の専門機関によれば、米国における重要インフラ事業者等への攻撃のうち、**約1割は制御系システムまで影響を及ぼした**。
- 一例として、2021年5月には、米石油パイプライン大手がランサムウェア攻撃を受け、**全てのパイプラインを一時停止**。米運輸省が燃料輸送に関する緊急措置の導入を宣言する事態に陥った。



事例（国内）

- 2021年10月末、**国内の公立病院がランサムウェア攻撃を受け、電子カルテが暗号化され閲覧不可**になったほか、**診療報酬計算や電子カルテ閲覧に使用する基幹システムが使用不能**になったため、**新規患者の受け入れを停止**。
- 病院は、**身代金要求には応じず**、同年12月29日にサーバーを復旧させ、2022年1月４日から通常診療を再開。



工場におけるサイバー攻撃事例

- アルミニウム工場のマルウェア感染（2019年、ノルウェー）

事象

- ✓ ノルウェーのアルミニウム製造大手で大規模なマルウェア感染
- ✓ 「LockerGoga」と呼ばれるランサムウェアに感染
- ✓ 発生直後、プレス加工等の一部生産、オフィス業務に影響
- ✓ プラントは影響拡散防止のためシステムから分離
- ✓ 被害は、最初1週間で3億～3億5000万ノルウェークロネ（4000万ドル相当）と推定

- 石油化学プラントの安全計装システムを狙ったマルウェア（2017年、中東）

事象

- ✓ 中東の石油化学プラントで使用されていた Schneider Electric 社製の SIS コントローラー(Triconex)がマルウェア感染
- ✓ SISのエンジニアリング・ワークステーションへのリモートアクセスを取得、SISシステムのゼロデイ脆弱性を利用して改ざん
- ✓ プラントが緊急停止

- 自動車工場のマルウェア感染（2017年、日本）

事象

- ✓ 大手自動車メーカーの工場でコンピュータがWannaCryに感染
- ✓ 工場に据え付けの設備に付属するパソコンが感染
- ✓ 生産ラインの制御システムに影響が発生し、一時的にラインを停止
- ✓ 約1千台の車両生産に影響

目次

（１）事例

（２）産業サイバーセキュリティ研究会　～工場SWG～

（３）工場システムセキュリティガイドライン（案）の概要

分野別SWGにおけるサイバー・フィジカルセキュリティ対策フレームワーク（CPSF）の具体化 とテーマ別TFにおける検討

- **7つの産業分野別サブワーキンググループ（SWG）**を設置し、CPSFに基づくセキュリティ対策の具体化・実装を推進
- 分野横断の共通課題を検討するために、**3つのタスクフォース（TF）を設置**

産業サイバーセキュリティ研究会ＷＧ１（制度・技術・標準化）

標準モデル（CPSF）

Industry by Industryで検討
(分野ごとに検討するためのSWGを設置)

ビルSWG
- ガイドライン第1版の策定(2019.6)

電力SWG
- 小売電気事業者ガイドライン策定(2021.2)

防衛産業SWG
- 防衛産業サイバーセキュリティ基準の改訂を公表(2022.4)

自動車産業SWG
- ガイドライン2.0版を公表(2022.4)

スマートホームSWG
- ガイドライン1.0版を公表(2021.4)

宇宙産業SWG
- 2022年2月に第4回を開催

工場SWG
- 2022年夏を目途にガイドライン案を作成予定

・・・

分野横断SWG

『第3層』TF：『サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
データの信頼性確保に向け「データによる価値創造（Value Creation）を促進するための新たなデータマネジメントの在り方とそれを実現するためのフレームワーク（仮）」案のパブリックコメント（2回目：22年2月～3月）を実施。

ソフトウェアTF：サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース

検討事項：
OSSの管理手法に関するプラクティス集を策定、SBOM活用促進に向けた実証事業（PoC）を実施。

『第2層』TF：『フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース

検討事項：
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するための「IoTセキュリティ・セーフティ・フレームワーク(IoT-SSF)」を公開。このIoT-SSFをわかりやすく理解するためのユースケースを策定（公開準備中）。

工場SWG （座長：江崎 浩　東京大学 教授）

- 2022年1月6日に工場SWGを設置し、これまでに計3回開催。委員、オブザーバー、ヒアリング対象など、主な関係団体・企業も広く参画し、工場セキュリティガイドラインの策定に向けて活動。
- 3月23日の第3回SWGでは、パブコメ実施に向けたガイドライン案を審議した。現在、パブコメ結果を取りまとめ中。

開催実績

第１回　工場SWG設置について

第２回　主な産業界団体・企業からのヒアリング
- 日本自動車工業会
- 電子情報技術産業協会半導体部会
- NEC プラットフォームズ
- パナソニック
- 日本鉄鋼連盟
- 日本医療機器産業連合会
- 日本工作機械工業会

第３回　パブコメに向けたガイドライン案の審議

委員名簿

江崎 浩（座長）	東京大学 教授
岩﨑 章彦	電子情報技術産業協会
榎本 健男	日本工作機械工業会
桑田 雅彦	日本電気株式会社
斉田 浩一	ファナック株式会社
佐々木 弘志	フォーティネットジャパン株式会社
斯波 万恵	株式会社東芝
高橋 弘宰	トレンドマイクロ株式会社
中野 利彦	株式会社日立製作所
西雪 弘	三菱電機株式会社
藤原 剛	ビー・ユー・ジーDMG森精機株式会社
松原 豊	名古屋大学　准教授
村瀬 一郎	技術研究組合制御ｼｽﾃﾑｾｷｭﾘﾃｨｾﾝﾀｰ
渡辺 研司	名古屋工業大学　教授

Panasonic Cyber Security Team　7

工場(制御システム)のセキュリティ課題

- 長期運用と可用性重視のため、ITシステム同等の対応が困難
  ⇒ **脆弱な状態が前提**と考え、侵入されることを前提とした対策が必要
- 制御システムの物理症状からサイバー攻撃の特定は困難
  ⇒ 迅速な対策・復旧には専門家による**サイバー空間での監視が不可欠**

問題点	ITシステム（OA用PC）	制御システム（製造システム）	
機器・システムのライフサイクル	3-5年	10年以上	・長期運用 ・OSサポート終了後も稼働
サポート切れOS・ソフトの使用	禁止	禁止できない	・誤動作の可能性あり ・ベンダの保証対象外となる
ウィルス検査ソフト導入	導入必須	導入不可	・誤動作の可能性あり ・専用装置は導入方法無し
セキュリティパッチ適用	適用必須	適用不可	・誤動作の可能性あり ・設備メーカ保証外

JSIA　JEITA 一般社団法人 電子情報技術産業協会 半導体部会

③各社における工場セキュリティを取り巻く課題（1）

➢ 各社ともさまざまな課題を抱えている

- 製造装置は、導入時のシステムのまま使われることが多く、バージョンアップなどセキュリティ対策が実質できない。
- セキュリティ対策ソフトは、装置動作の保証ができないとの装置ベンダーからの回答があり、導入が困難。そのため直接的な保護、検疫ができない。
- 製造装置の保守時に装置や関係するベンダーによるコンピュータウィルスの持ち込みリスクがある。
- 製造装置の修理のためハードディスクなどの記憶媒体を修理に出した際、コンピュータウィルスの混入リスクがある。
- リモート診断・支援などが進む場合、社外からのアクセスに伴うセキュリティ対策をユーザー単独として対策することに限度がある。また、様々なツール、方式が乱立することにより、対応がより複雑になる。
- 導入したセキュリティソリューションにより工場システムへ予期しない影響が発生することがある。
- Cloudベースのセキュリティソリューションでは、自社でコントロールできない問題が発生して、工場のオペレーションに影響を及ぼす。
- 新たな技術/デバイスの登場に対するセキュリティ対策が追い付かない(IoT、Cloud、Mobile etc)。

第2回 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　資料4-2,4-4より抜粋
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/002.html

目次

（１）事例

（２）産業サイバーセキュリティ研究会　～工場SWG～

（３）工場システムセキュリティガイドライン（案）の概要

※パブコメにかけたものを元に作成しており、今後修正の可能性あり。

ガイドラインの目次

- イメージしやすさの観点から、想定工場を想定し、参照すべき考え方やステップを「手引き」として示しつつ、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。
- また、付録にて、関連する基準や、工場セキュリティ対策のチェックリスト等、読者の参考になると考えられる情報を載せている。

目次（検討中）

ガイドラインの構成（読み進め方）

- ガイドライン冒頭に、工場セキュリティについて読者が知りたいと思われる事項とガイドラインにおける記載箇所を一覧化し、アクセスしやすい工夫を行った。

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

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】

● 一般的に、製造業／工場では、

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

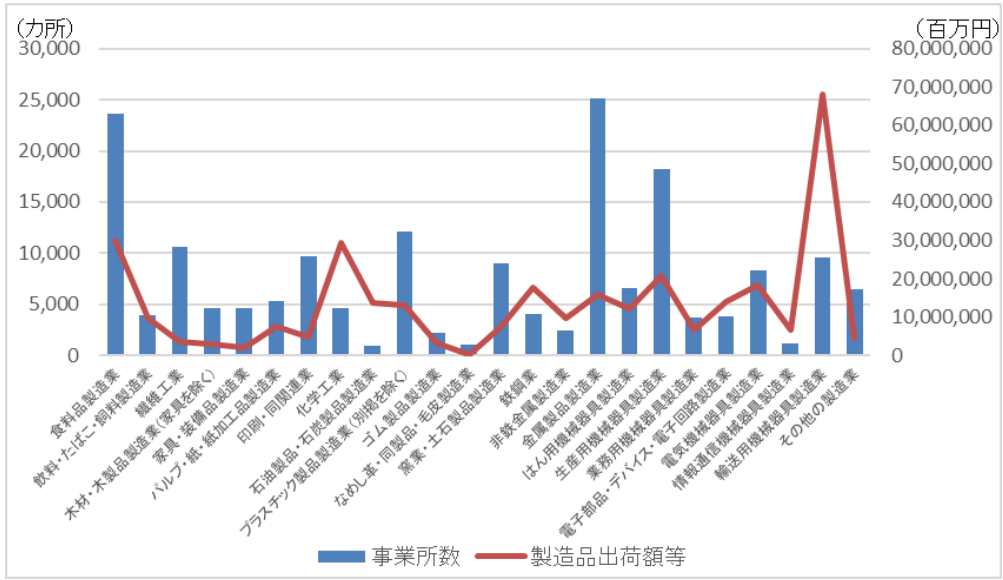
という価値が重視されている 。

● 工場と言っても、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** 、また、**必要最小限と考えられる対策事項として脅威に対する技術的な対策から運用・管理面の対策までを明記**している。

● 重要なことは、**業界団体や個社が、本ガイドラインに示した考え方やステップ、対策を参照**しつつ、**業界・業種の事情に応じたガイドラインを作成するなどしながら工場へのセキュリティ対策を進めていく**、といった行動に移すことである。

● 本ガイドラインは、**各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティレベルの底上げを図ることを目的**としている。



出所）経済産業省工業統計調査（2020年確報）を元に作成
図１１　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である。

- ✓ ITシステム部門
- ✓ 生産関係部門（生産技術部門、生産管理部門、工作部門　等）
- ✓ 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。

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を提示するにあたり、わかりやすさの観点からある工場を想定工場として設定（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：

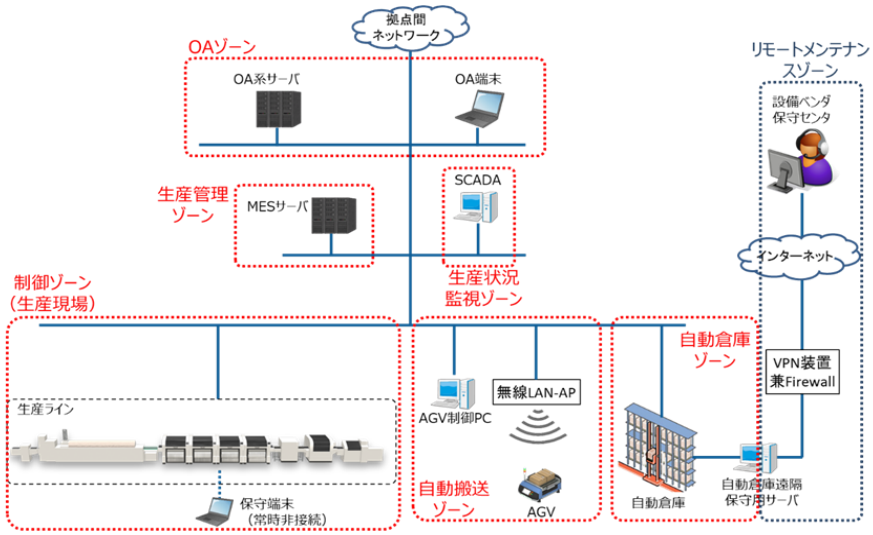
【想定生産ライン】

- 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

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を提示するにあたり、わかりやすさの観点からある工場を想定工場として設定（読者の置かれた環境に応じ適宜読み替え）。

【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機器
  - 無線LANアクセスポイント（無線LAN-AP）
  - ルータ（設備系-生産管理系）
  - MESサーバ
  - 生産ライン
  - SCADA
  - 保守用PC
  - AGV（無人搬送車）制御PC
  - AGV（無人搬送車）
  - 自動倉庫
  - 自動倉庫遠隔保守用サーバ
  - OA系サーバ
  - OA端末

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①全体）

- 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)経営目標との関連整理
  - (2)外部要求事項（社会的セキュリティ要件）の考慮
  - (3)内部要件／状況の把握
- **ステップ1-2** 業務の整理
- **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サイクルの構築）

- 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
B) セキュリティ対策管理(ID/PW管理、機器の設定変更など)
C) サイバー攻撃に関する情報共有

②維持・改善面のセキュリティ対策

(2) サプライチェーン対策

事業や環境、技術の変化に応じて見直し

※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、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。

（参考）サプライチェーン対策：取引先や調達先への主な確認ポイント（例）

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

ガイドラインの構成（付録　チェックリスト（例））

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

カテゴリ	番号	確認項目	達成度	参照
組織的対策	1-1	工場システムのセキュリティの必要性について、決裁者（工場長、カンパニー長等）または経営層が認識をもっており、十分な予算・人員配置などの協力を得られる状態にある。		3.1.1 3.1.7（参考）
	1-2	工場システムのセキュリティ対応について情報システム部門や生産関係部門等の関係する部署・部門との間で協力・連係態勢が取られている。		3.1
	1-3	工場システムのセキュリティ検討組織や、担当者が準備されており、責任と業務内容が明確化されている。		3.1
	1-4	工場のセキュリティ事故発生時の担当者が準備されていて、責任と業務内容が明確化されている。		3.1
	1-5	工場セキュリティに関する脅威の動向などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの情報収集を行っている。		3.1
システム関連対策	2-1	システムが侵害・停止した場合の事業に対するリスクを検討している		3.2.2(1)
	2-2	工場システムにおける専用のセキュリティポリシが規定されていて、認知されている。		3.2.2(1)
	2-3	工場システムからの電子メールやインターネットアクセスはポリシによって禁止している。		3.2.2(1)
	2-4	工場システムにおけるセキュリティの異常発生時の責任者の対応が明確化されている。		3.2.2(1)
	2-5	工場システムにおけるセキュリティの異常発生時の対応方法を現場作業者が理解し、訓練を実施している。		3.2.2(1)
	2-6	情報資産の検出ツールを利用するなど、工場ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器、設備等）の台帳を作成し、システム構成図が作成している。		3.2.2(1)
	2-7	工場内に無線LANを導入している場合、ネットワークへの接続を許可された機器の台帳を作成し、無許可の機器を拒否する仕組みがある。		3.2.2(1)
	2-8	定期的な脆弱性診断やペネトレーションテスト（侵入可否検査）を実施して、システムへの侵入を成功させるために使用できる攻撃手法や脆弱性を特定している。		3.2.2(1)
	2-9	工場内に外部記録媒体（USBメモリ、フラッシュカード）やポータルメディアの利用・持ち込みを制限している。		3.2.2(1)
	2-10	工場内のシステムのパスワードの強度と有効期限を含むパスワードルールがある。（安全に関わる緊急対応を必要とする表示器などの端末は除く）		3.2.2(1)
	2-11	工場内のシステムへのアクセス権で使用していない古いアカウント（退職者・異動者など）を削除している。		3.2.2(1)
	2-12	工場ネットワーク内の接続機器について、事前にそれらがウイルスに感染していないことを確認する手順がある。		3.2.2(1)
	2-13	システム機能の完全な復旧を想定したバックアップを行い、定期的にバックアップデータからの復旧テストを行っている また、その手順が明確化されている。		3.2.2(1)

ガイドラインの構成（付録　チェックリスト）

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

カテゴリ	番号	確認項目	達成度	参照
物理的対策	3-1	ウイルス対策がインストールできる端末にはアンチウィルスソフトまたはアプリケーションホワイトリストを導入し、インストール不可能な端末では何らかの代替策（USB型のアンチウィルスなど）を導入している。		3.2.2(2)
	3-2	アプリケーション/オペレーティングシステム（OS）にセキュリティパッチを適用している。もしくは代替策を講じている。		3.2.2(2)
	3-3	制御端末のオペレーティングシステムやアプリケーションは必要最小限とし、未使用のサービスやポートは停止・無効化している。		3.2.2(2)
	3-4	工場の重要設備への物理的なアクセスについてレベル分けなどの十分な対策を行っている（例：監視カメラ、警報装置）。または、入退室管理、外部の入室者への関係者の付き添いなど運用面での代替策を講じている。		3.2.2
	3-5	工場ネットワーク内において、セキュリティレベルに応じたネットワークセグメント管理を行っている（VLAN等）。		3.2.2(1)
	3-6	工場システムのリモートメンテナンスなどを目的とした外部からのインターネットアクセスが可能な場合、認証（２要素認証等）やネットワーク侵入防護などの保護対策を行っている。		3.2.2(1)
	3-7	工場内のネットワーク（情報システムとの境界含む）の不審な通信を特定するためのネットワーク検知/防護システムを導入している。		3.2.2(1)
	3-8	工場内システムのログイン、操作履歴などのイベントログを取得している。それらのログは定期的に分析するか必要日数保存している。		3.2.2(1)
工場システムサプライチェーン管理	4-1	工場システムのセキュリティ事故発生時に対応ができるよう、制御システムベンダー・構築事業者と連絡・連携体制を構築している。		3.3(2)
	4-2	工場システムセキュリティのメンテナンス等、協力会社向けのセキュリティ教育を実施している。		3.3（2）
	4-3	納品された工場システムに関するセキュリティの脆弱性が発見された場合、その情報が速やかに共有されるように、制御システムベンダー・構築業者との連絡・連携体制を構築している。		3.3(2)
	4-4	サプライチェーン（協力会社、生産子会社など）における工場システムの脅威、影響度、対応状況（監査実施など）を把握できている。		3.3(2)
	4-5	納入する工場システム機器に対して、一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査がある。		3.3(2)
	4-6	新規システム導入時の設計仕様要件にセキュリティに関する要求仕様が明確化されている。		3.3(2)