経済産業省

資料７

「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」 拡充版（案）の概要と今後の方針

経済産業省

サイバーセキュリティ課

第5回SWG資料 再掲

スマートファクトリーにおけるセキュリティ検討の必要性

- 現行の「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」については、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作成。

・現行のFAシステムを例に、制御システムに対するセキュリティ施策を検討するプロセスおよび勘所を提示

・既存の制御システムを前提に、境界防御型のセキュリティを想定。

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**
- **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
  (2)物理面での対策

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
  (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

・スマートファクトリーに向けた制御システムにおけるシステムアーキテクチャの変化

・サプライチェーンによる脅威の増加

工場がクラウドやデジタルツインといったサイバー空間に密接に繋がっていく世界における
セキュリティのあり方を検討することが必要。

作業部会の概要

- スマート化を進める業界・企業におけるニーズ等のヒアリング調査結果を踏まえ、工場SWGの委員を中心に、工場のスマート化におけるセキュリティについて関心の高いメンバーによる作業部会を構成し、更なる課題の深堀や具体的な対策の検討を進めている。
- これまで、計3回の会合での議論と1回の書面レビューを行い、ガイドライン拡充版に関する内容を検討した。今後は、パブコメを経て、対応検討及びレビューを実施予定である。

作業部会概要

活動目的	• スマート化を進める企業等におけるセキュリティ課題や対策の実態等についての、「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」拡充版への反映
活動内容	• 「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」拡充版に関する検討・執筆支援、レビュー
メンバー	• 工場SWGの委員を中心とした、工場セキュリティについて関心の高いメンバー有志 • メンバー形態は以下の2形態 ✓ **コアメンバー**：会合における議論・原稿執筆支援が中心 ✓ **メンバー**：メール等を通じた原稿レビュー・確認が中心（会合参加は任意）
実績	• 会合開催（対面及びオンライン） ✓ 第1回：令和5年10月30日 ✓ 第2回：令和5年11月22日 ✓ 第3回：令和5年12月6日 • 書面レビュー：令和5年12月28日～令和6年1月12日
今後の予定	• パブコメ対応支援・レビュー：令和6年3月予定

メンバー

<コアメンバー>

- 名古屋工業大学　渡辺研司委員【作業部会長】
- 技術研究組合制御システムセキュリティセンター　村瀬一郎委員
- 株式会社東芝　斯波万恵委員
- トレンドマイクロ株式会社　高橋弘宰委員
- 日本電気株式会社　桑田雅彦委員
  岡山大河様、大林克成様、小川陽平様
- 日立製作所　中野利彦委員
- ファナック株式会社　斉田浩一委員
- フォーティネットジャパン合同会社　佐々木弘志委員
- 三菱電機株式会社　柴田陽一様、松田規様

<メンバー>

- JFEスチール株式会社
- シスコシステムズ合同会社
- 東京エレクトロン株式会社
- 東京電力パワーグリッド株式会社
- 株式会社日立製作所
- 三井化学株式会社
- 三菱ガス化学株式会社
- 三菱電機株式会社
- 独立行政法人情報処理推進機構

「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」拡充版（案）

- 工場のスマート化において検討すべきセキュリティについて、昨年度公表した「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」拡充版として整備した。
- 「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」に記載した実施事項（ステップ1・2・3）と整合を取り、各ステップにおいてスマート化の際に留意すべき点や対策のポイント等について、別冊で整理した。

「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」本編　目次

目次構成を整合

「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」拡充版（案）　目次

本編の基本的な実施事項を確認しながら、拡充版でスマート化のポイントを参照可能とする。

ガイドライン拡充版（案）：1. はじめに

- 「１． はじめに」において、本ドキュメントの目的、読者、読み方を記載する。
- スマート工場のセキュリティを進めるにあたって、ステークホルダーの責任分界と役割分担、ゾーンの考え方を考慮する。

ドキュメントの目的

- 工場のスマート化において、サイバー空間との密接な繋がりが進んでいくと想定。
- 制御システムにおけるシステムアーキテクチャの変化や、サプライチェーンによる脅威の増加により、工場がサイバー空間に密接に繋がっていく世界におけるセキュリティのあり方を検討することが必要。

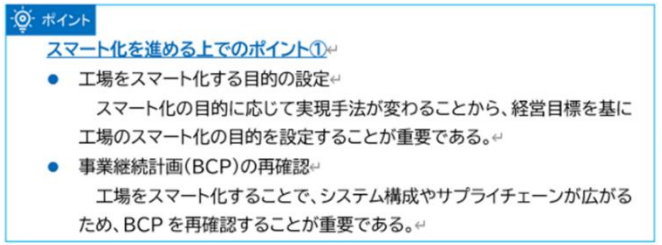
→ **先進的な事業者が臆することなく工場のスマート化を進め、工場の価値創造を促進することを後押しする。**

- 工場のスマート化を先進的に進める業界（例：半導体業界等）では、サプライチェーンにおいて取引先に対するセキュリティ対策を要請
- 海外では、機器に対するセキュリティ確保の取組が推進（例：米国U.S. Cybersecurity Labeling Program for Smart Devices、EU Cyber Resilience Act 等）

→ **業界としてのセキュリティ向上の取組や、海外におけるセキュリティ対策推進の具体的な事例を提示し、近年さらに強まっているセキュリティの必要性を訴える。**

本ドキュメントの読み方

- 別冊の読者としては、主に工場のスマート化を進めている、もしくは検討している企業を想定している。企業内は、ガイドライン本編と同様の読者を想定している。
- 「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」では、3章において、工場システムのセキュリティ対策を企画・導入するステップの概略を示している。
- 別冊では、**スマート工場の概要を示すとともに、ガイドライン本編3章に示した各ステップの対策におけるスマート化を進めるにあたっての留意点や具体例を示す**。
- 各ステップの**青枠にポイントを示すとともに、緑枠にガイドライン本編の記載内容の概要**を示す。



スマート化を進める上でのポイント

ガイドライン本編上の記載

ガイドライン拡充版（案）：2. 本ドキュメントのスマート工場

- 「２． 本ドキュメントのスマート工場」において、工場のスマート化の解説と想定セキュリティリスクとスマート化のセキュリティ対策のポイントを記載する。

工場のスマート化

- **スマート工場は、デジタル技術を活用してビジネス競争力の強化を目指している。**目指す上で、品質の向上やコストの削減を目的として、工場の各種状況の見える化、各種データに応じた作業指示・支援、データ連携と協調製造などを実現する。
- 実現事項によっては、フィジカル空間とサイバー空間との結びつきが強くなり、その結果セキュリティリスクも上がると考えられる。そのため、リスクに応じて適切なセキュリティ対策を行うことが重要である。

スマート工場で想定されるセキュリティリスク

- 工場をスマート化する上では、デジタル技術を活用してスマート化の目的や実現事項によって様々な取り組みが進められる。特にスマート工場では、以下のような点においてセキュリティリスクが増加することが想定される。
  - **外部ネットワーク接続の増加**
    スマート化を進める上で、制御システムが情報システムや外部サービス・クラウドと連携され、外部ネットワーク接続が増える可能性が高い。そのため、攻撃者が侵入できる経路が増え、工場システムが攻撃を受けるリスクが増加する。
  - **サプライチェーンの広がり**
    スマート化を進める上で、外部機器やサービスの導入が検討され、自社で管理できない内容が増える可能性が高く、外部の状況に応じて自社の工場システムが停止するおそれがある。

スマート工場でのセキュリティ対策のポイント

- スマート工場におけるセキュリティ対策では、サイバー空間とフィジカル空間が密接に関連するため、品質管理の観点での対策も記載する。特に以下の点を考慮する。
  - **ゾーン設定の考え方**
    スマート化では、目的に応じて業務 の追加・高度化を行うため、業務視点での詳細なゾーン設定がより重要である。また、スマート化では、フィジカル空間で接続されていないが、サイバー空間では接続されているケースがあるため、よりサイバーフィジカルが融合したゾーンとなる。ガイドライン本編では、ゾーンの重要性を示していたが、別冊では、業務視点に基づいたゾーン設定における考え方と留意点を記載する。
  - **サプライチェーンの広がりに伴う責任分界や役割分担の考え方**
    スマート化を進める上で、外部機器やサービスの導入、自社の工場間や自社・他社間でのデータ流通が促進され、自社のみで管理できない対象が増える可能性が高いため、対策の責任分界や役割分担がより重要である。ガイドライン本編では、サプライチェーン対策を進める上でのポイントを示していたが、別冊では、取引先・調達先に求めるセキュリティ要件における考え方を具体的に例示する。

ガイドライン拡充版（案）：3. セキュリティ対策企画・導入におけるスマート化のポイント

- 「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」で示した各ステップにおいてスマート化における留意点を示す。
- 各ステップでスマート化を進める上でのポイントを示すとともに、ガイドライン本編の記載内容の概要を示す。

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
    - 工場をスマート化する目的の設定
    - 事業継続計画（BCP）の再確認
  - (2)外部要件の整理
    - 国内外の規格や法制度の動向
    - 業界動向
  - (3)内部要件／状況の把握
    - 国内外の規格や法制度の動向
    - 関連部署の拡大、ガバナンス体制の変更
    - インシデントが与える影響の範囲拡大
- **ステップ1-2**　業務の整理
  - スマート化の目的に照らした業務の広がり
  - 業務の広がりに応じたシステム範囲の拡大
- **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
  - スマート化におけるゾーンごとのセキュリティ要件の考え方
  - スマート化により考慮すべき脅威と影響の考え方

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
      - ネットワーク接続における対策
      - クラウド利用時の対策
    - ②機器におけるセキュリティ対策
      - 汎用品のセキュリティ対策
    - 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
      - データ活用・連携における対策
  - (2)物理面での対策

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**
  - (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
      - スマート化におけるサイバー攻撃の早期認識と対処プロセスの実現
    - ②維持・改善面のセキュリティ対策
      - スマート化におけるPDCAサイクルの実現
  - (2) サプライチェーン対策
    - 汎用品利用時の留意事項
    - クラウド利用時の留意事項
    - ソフトウェア利用時の留意事項

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

ガイドライン拡充版（案）：3-ステップ1. 内外要件や業務、保護対象等の整理①

- ステップ1では、スマート化を進めるにあたって内外要件・業務・保護対象等を再整理する際の留意事項、ゾーン設定の具体的な考え方を記載する。

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** • **工場をスマート化する目的の設定** スマート化の目的に応じてスマート化の実現手法が様々であり、必要となるセキュリティ対策も変わるため、経営目標を基に工場のスマート化の目的を設定することが重要である。 • **事業継続計画（BCP）の再確認** 工場をスマート化することで、システム構成やサプライチェーンが追加・拡大するため、BCPを再確認することが重要である。 **（2）外部要件の整理** • **国内外の規格や法制度の動向** スマート化によって新たな技術や設備を利用するため、関係する海外の規格や法制度を再確認することが重要である。 • **業界動向** スマート化によって新たな技術や設備を利用するため、自社の業界独自の規格やガイドラインを再確認することが重要である。 **（3）内部要件／状況の整理** • **内外ステークホルダーの拡大** スマート化によって外部機器やサービスの利用が増える可能性があるため、内外ステークホルダーを再確認することが重要である。 • **関連部署の拡大、ガバナンス体制の変更** スマート化によって、新規サービス導入や外部ネットワーク接続が増えるため、関連部署やガバナンス体制を再確認・変更することが重要である。 • **インシデント発生時の影響の広がり** スマート化によってステークホルダーや社内関係者が増えるため、インシデント発生時の影響の広がりを再確認することが重要である。
ステップ1-2	**業務の整理**【3.1.2】	• **スマート化の目的に照らした業務の広がり** スマート化に応じたセキュリティ対策を検討するために、スマート化により広がる業務を確認することが重要である。 • **業務の広がりに応じたシステム範囲の拡大** スマート化によって新たな業務が増えるため、増えた業務に応じたシステム範囲の拡大を確認することが重要である。

ガイドライン拡充版（案）：3-ステップ1. 内外要件や業務、保護対象等の整理②

- ステップ1では、スマート化の目的から業務の洗い出しを行い、ゾーン設定とセキュリティ脅威を整理するまでの流れを記載する。

ステップ1-3	**業務の重要度の設定**【3.1.3】	• **業務の広がりに伴う業務の重要度の見直し** スマート化によって、新たに増えた業務に対して重要度の見直しを行うことが重要である。
ステップ1-4	**保護対象の整理**【3.1.4】	• **システムの拡大に伴う保護対象の見直し** スマート化によって、拡大したシステムに応じて保護対象を見直すことが重要である。
ステップ1-5	**保護対象の重要度の設定**【3.1.5】	• **ステップ1-3、ステップ1-4を踏まえた、各保護対象の重要度の見直し** スマート化により改めて洗い出した保護対象それぞれの重要度を見直すことが重要である。
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】	• **技術の進化を踏まえ、スマート化を進める際の内外の接続の考え方の整理** スマート化によって、新たに増えた業務を考慮して、セキュリティ対策を実施するために必要なゾーン設定を改めて行うことが重要である。
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】	• **スマート化におけるゾーンごとのセキュリティ要件の考え方** スマート化によって、新たに設定されたゾーン毎に、必要なセキュリティ要件を検討することが重要である。 • **スマート化により考慮すべき脅威と影響の考え方** スマート化によって、外部サービスの連携や外部ネットワークの接続等の特に注意すべき脅威と影響について検討することが重要である。

ゾーン設定の進め方

スマート工場の目的の設定	目的に応じた実現事項の確認	実現事項に応じた業務の確認	業務を基にゾーンを設定
以下の目的のカテゴリを参考に、工場をスマート化する具体な目的を設定 • 品質の向上 • コストの低減 • 生産性の向上 • 製品化・量産化の期間短縮 • 人材不足・育成への対応 • 新たな付加価値の提供	スマート工場の目的を達成するための実現事項を、下記のカテゴリを参考に複数設定 • 機能の追加・改善 工場における機能を追加・改善する事項（例：工場の各種状況の見える化、各種データに応じた作業指示・支援） • 構成要素の追加・改善 工場の構成要素を追加・改善する事項（例：製造装置配備の多様化、汎用品の利活用）	実現事項に応じて、工場に関わる実施対象毎に業務を洗い出し（下記は実施対象の例） • 現場 • 工場システム（装置・機器やソフトウェア等） • 外部サービス • 組織	洗い出された業務の重要度を設定し、下記の様々な視点でゾーンを設定 • 業務の視点 • BCP・業務重要度の視点 • 設置環境（物理、サイバー空間）の視点 • 既存環境の制約の視点

ガイドライン拡充版（案）：3-ステップ2. セキュリティ対策の立案①

- ステップ2では、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。
- 工場のスマート化では外部システムや汎用品の利用拡大が想定され、ステップ3の運用・マネジメントの対策がより重要である。

ステップ2-1	**セキュリティ対策方針の策定**【3.2.1】	**・ スマート化を踏まえたセキュリティ対策の方針を策定** スマート化によって、設定した各ゾーンにおけるセキュリティ要件に基づいてセキュリティ対策の方針を策定することが重要である。
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】	**・ スマート化におけるシステム構成面・物理面での対策について** スマート化によって、外部機器・サービスの利用などが増えるため、スマート化の特徴に応じてセキュリティ対策を見直すことが重要である。 **(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** スマート化におけるネットワーク接続の対策としては、安全な接続を確立することに加えて、データの機密性・完全性・可用性を確保するために、他社・他事業所・他拠点との連携を取りつつ、統合的にシステム構成面でのセキュリティ対策を検討する必要がある。 また、工場においてスマート化を進める際には、クラウドサービスを利用することが考えられ、適切なクラウドサービスを選定する必要がある。 **②機器におけるセキュリティ対策** 工場においてスマート化を進める際には、セキュリティ機能を指定できない汎用品を用いる場合も増える。汎用品の活用により、利便性の向上やコスト低減を見込めるが、利用形態や目的毎に必要なセキュリティを確保することが必要である。 **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** スマート化された工場システムにおいては、プログラム・サービス内の不具合などによって、正しくデータが活用されず、本来意図していないフィードバックが行われる可能性があり、データ活用・連携の際には、自社内または自社と外部事業者間で詳細に条件を確認する必要がある。

ガイドライン拡充版（案）：3-ステップ2. セキュリティ対策の立案②

- ステップ2で示した対策例が、どのような脅威と対応するか、ガイドライン本編と同様の枠組みで整理する。

スマート化の想定脅威に対応するセキュリティ対策例

	脅威種別	脅威内容	対策種別	対策内容
1	機器の盗難、システム・機器に対する破壊・不正操作	外部ネットワークからのシステムへの不正アクセス	(1) システム構成面での対策	(1)① ネットワークにおける対策
2		ソフトウェアの不具合を利用した設備の不正制御	(1) システム構成面での対策	(1)② 機器における対策
3	設備の異常な制御や破壊	脆弱性を利用した設備への不正アクセス	(1) システム構成面での対策	(1)② 機器における対策
4	データ盗難・漏えい	外部サービスに保存されているデータの漏えい	(1) システム構成面での対策	(1)② 機器における対策
			(1) システム構成面での対策	(1)③ 業務プログラム・利用サービスにおける対策
5	データ改ざん・破壊	プログラム内でのデータの欠損	(1) システム構成面での対策	(1)② 機器における対策
6		不正なデータ入力による不適切なフィードバック	(1) システム構成面での対策	(1)① ネットワークにおける対策
7	可用性低下	データベースの容量不足によるデータ欠損	(1) システム構成面での対策	(1)③ 業務プログラム・利用サービスにおける対策
8	従業員、保守要員（設備ベンダ）の過失	ソフトウェアのライセンス不備による利用停止	(1) システム構成面での対策	(1)② 機器における対策
9		データの取扱不備による外部へのデータ漏えい	(1) システム構成面での対策	(1)③ 業務プログラム・利用サービスにおける対策

ガイドライン拡充版（案）：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） ①

- 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。
- ライフサイクルの対策では、サイバー攻撃の早期認識と対処の重要性と、スマート化においてPDCAサイクルを回す際に検討すべき事項を記載する。
- サプライチェーン対策では、スマート化に伴い拡大するクラウド・汎用品・ソフトウェア利用時の留意事項を記載する。

ステップ3【3.3】	**・ スマート化におけるライフサイクル対策** スマート化によって、関係部署の広がりや外部ネットワーク接続の増加するため、ライフサイクル対策を見直すことが重要である。 **①運用・管理面の対策** スマート化において、外部ネットワークの接続の増加などによりセキュリティリスクが増加していることより、サイバー攻撃の早期認識と対処（OODAプロセス）を実現することが重要である。 スマート化によって増加した外部との接続に対するセキュリティ対策を検討する上で、OTセキュリティとITセキュリティの融合化がより必要となるため、サイバー攻撃の早期認識と対処を実践するためには、各プロセスにおける担当部署と意思決定者を明確化し、情報連携の体制を構築することが重要である。 **②維持・改善面のセキュリティ対策** 工場のスマート化においては、外部ネットワーク接続の増加、外部機器利用の増加、機器ベンダなどの関係者の増加などの可能性が高く、セキュリティリスクが増えることが想定される。スマート化による変化に応じて、セキュリティ対策を評価し、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PDCAサイクルを回す必要がある。 **・ スマート化におけるサプライチェーン対策** スマート化によって、外部機器・サービスの利用などが増えるため、サプライチェーン対策を見直すことが重要である。 **①クラウド利用時の留意事項** スマート化において、外部クラウドサービスの利用が検討されるが多くのクラウドサービスは利用者側でセキュリティ対策を管理することが難しい。そのため、クラウドサービスの調達、契約、運用・保守の3段階で、インシデントが発生したりした場合の対応の責任や対応方針について確認する必要がある。 **②汎用品利用時の留意事項** スマート化によって、一般に流通している汎用品の利用も増えることが想定される。汎用品については、セキュリティ対策を調達側が実施することが難しいため、製品に対してセキュリティ対策がきちんと行われているか、また納品後に脆弱性が検出されたり、インシデントが発生したりした場合の対応の責任や対応方針について確認する必要がある。 **②ソフトウェア利用時の留意事項** スマート化によって、工場内でのソフトウェアの利用も検討される。ソフトウェアは、外部開発・内製ともに検討され、調達、契約、運用・保守に加えて、開発時においても、ステップ2で示したようにOSSの活用や構成要素の管理、脆弱性管理・対応などをソフトウェア利用時に注意する必要がある。

ガイドライン拡充版（案）：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

- ライフサイクルの対策では、サイバー攻撃の早期認識と対処における役割分担の重要性を記載するとともに、役割分担の例を示す。

サイバー攻撃の早期認識と対処における役割分担例（予防保全段階）

	主な担当部署	意思決定者	実施内容の例
監視（Observe）	ベンダ	-	・導入している機器の脆弱性情報に関する連絡
分析（Orient）	セキュリティ担当部署	・セキュリティ担当部署の責任者	・脆弱性の悪用可能性 ・脆弱性を悪用された場合、工場に与える影響度合い
決定（Decision）	セキュリティ担当部署	・経営者（重要度に応じて） ・セキュリティ担当部署の責任者 ・現場部門長	・脆弱性に対する対策 ・対策を実施した場合の稼働への影響 ・対策実施の決定
行動（Action）	製造現場	・現場部門長	・対策の内容に応じて、現場に対策を指示 ・現場に指示された内容に応じて実施

サイバー攻撃の早期認識と対処における役割分担例（被害発生段階）

	主な担当部署	意思決定者	実施内容の例
監視（Observe）	製造現場	・現場部門長	・通常の現場との違和感とその理由について都度報告 ・工場システムの構成要素の把握と更新
分析（Orient）	報告内容に応じて適切な部署	・BCP担当部署の責任者 ・セキュリティ部署の責任者	・報告事象が工場に与える影響度合い ・報告事象の原因がセキュリティによるものかの分析
決定（Decision）	セキュリティ担当部署	・経営者（重要度に応じて） ・セキュリティ部署の責任者 ・現場部門長	・報告事象に対する対策 ・対策を実施した場合の稼働への影響 ・対策を実施の決定
行動（Action）	製造現場	・現場部門長	・対策の内容に応じて、現場に対策を指示 ・現場に指示された内容に応じて実施

ガイドライン拡充版（案）：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） ③

- サプライチェーン対策では、調達・契約・開発・運用保守の4つの観点で、クラウド・汎用品・ソフトウェアを利用する際の留意事項を記載する。

クラウド利用時の留意事項

	確認すべきポイント
調達	・クラウドサービス事業者の信頼性が高いか ・クラウドサービス利用時のサポートは提供されているか ・自社とクラウドサービスのセキュリティポリシーに矛盾がないか ・クラウドサービスに付随して機器・サービスが導入されるか
契約	・サービスの稼働率、障害発生頻度、回復目標時間などのサービスレベルが示されているか ・仮にサービスが終了した場合のデータの取り扱い条件は設定されているか
運用・保守	・クラウドサービスと業務の切り分けや運用ルールを明確化しているか ・クラウドサービスで取り扱う情報の機密性は確認しているか ・クラウドサービスの利用方法を理解している担当者がいるか ・クラウドサービスのユーザを適切に管理しているか ・クラウドサービスが停止した際のバックアッププランを準備しているか ・クラウドサービスを介して調達先や他社のネットワークと接続されているか

汎用品利用時の留意事項

	確認すべきポイント
調達	・製品セキュリティポリシーが策定・開示されているか ・製品セキュリティサポート方針が明示されているか ・製品セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか ・製品セキュリティを確保するための機能（アップデート機能、初期化機能等）があるか ・基準に則ったセキュリティチェックや検証が行われているか ・製品及び構成要素の脆弱性情報が収集されているか ・製品のセキュリティ機能や設定に関する情報が確認できるか ・製品以外に付随して機器・サービスが導入されるか
運用・保守	・導入されている製品を管理できているか ・製品が利用されている業務の重要性に応じて、追加でセキュリティ対策を実施しているか ・製品の脆弱性情報を逐次確認し、必要に応じて対応しているか ・脆弱性の確認・対応できる体制は構築できているか ・製品のサポート切れや販売中止となった場合のバックアッププランは準備しているか

ソフトウェア利用時の留意事項

	確認すべきポイント
調達	・ソフトウェアに関するセキュリティポリシーを確認できるか ・セキュリティを維持するための体制（サポート窓口、脆弱性報告の受付窓口、インシデントへの対応体制等）が整備されているか ・ソフトウェアのセキュリティを確保するための機能（アップデート機能、初期化機能等）があるか ・基準に則ったセキュリティチェックや検証が行われているか ・ソフトウェア及び構成要素の脆弱性情報が収集されているか ・ソフトウェアのセキュリティ機能や設定に関する情報を確認できるか ・ソフトウェアに付随して機器・サービスが導入されるか
契約	・セキュリティサポート方針が明示されているか ・ソフトウェアに不具合が発生した場合のサポートについて明示されているか ・ソフトウェアの構成要素の開示について明示されているか ・ソフトウェアのライセンス情報について明示されているか
開発	・ソフトウェアで使用するOSS含めた構成要素を管理できているか ・ソフトウェアの構成要素のライセンスを管理できているか ・日々の脆弱性管理、必要なセキュリティ対策の実施が実施できる体制が構築できているか
運用・保守	・導入されているソフトウェアを管理できているか ・ソフトウェアが利用されている業務の重要性に応じて、追加でセキュリティ対策を実施しているか ・ソフトウェアの脆弱性情報を逐次確認し、必要に応じて対応しているか ・脆弱性の確認・対応できる体制は構築できているか ・ソフトウェアがサポート切れとなった場合のバックアッププランは準備しているか

スケジュール

- 本日の工場SWGでの意見を反映した上で、令和5年度内にパブコメを行い、公表を目指す。

スケジュール（案）