経済産業省

資料５

# 「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」 拡充版と検討体制

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。**

# 「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

- 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」拡充版として整備する。
- 「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」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、別冊で整理する。

## 「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」本編　目次

**1．はじめに**
**2．本ガイドラインの想定工場**
**3．セキュリティ対策企画・導入の進め方**
3.1　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
3.2　ステップ2
セキュリティ対策の立案
3.3　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）

付録A　用語／略語
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
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
付録D　関連／参考資料
付録E　チェックリスト
付録F　調達仕様書テンプレート（記載例）

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　目次（案）

**1．はじめに**
**2．本ドキュメントのスマート工場**
**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**
3.1　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
3.2　ステップ2
セキュリティ対策の立案
3.3　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）

**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。**

# 拡充版の構成（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や読み方を記載する。
- 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。

・セキュリティを考慮したDX、スマート化の推進のためのガイドである点について記載する。【A1-3】

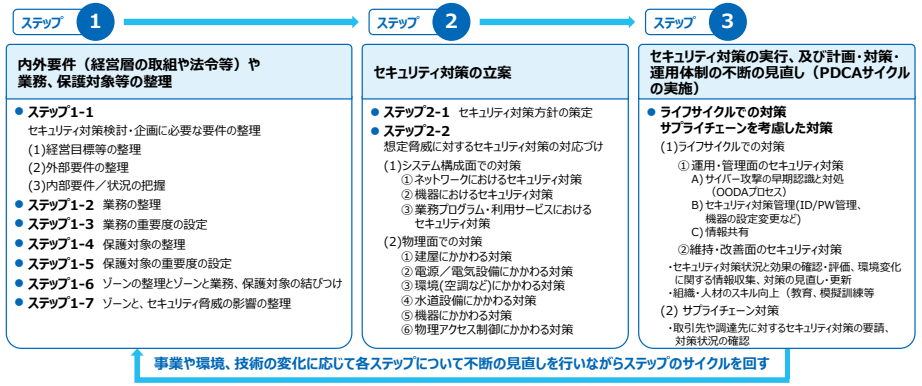
- 工場のスマート化を先進的に進める業界（例：半導体業界等）では、サプライチェーンにおいて取引先に対するセキュリティ対策を要請
- 海外では、機器に対するセキュリティ確保の取組が推進（例：米国U.S. Cybersecurity Labeling Program for Smart Devices、EU Cyber Resilience Act 等）

→ 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

- 「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。
- スマート工場のセキュリティにおいては、以下の点を特に考慮することが必要である。
  - 責任分界、役割分担
  - 業務の作り方、ゾーン※の考え方

    ※ ゾーンとは、業務の内容や重要度が同等である領域。
    同じゾーンに存在する保護資産に対しては、同等の水準のセキュリティ対策が必要である。
- これらを踏まえ、スマート化を進めるに当たっての「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」で示した各ステップでの留意点を示す。




※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。

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

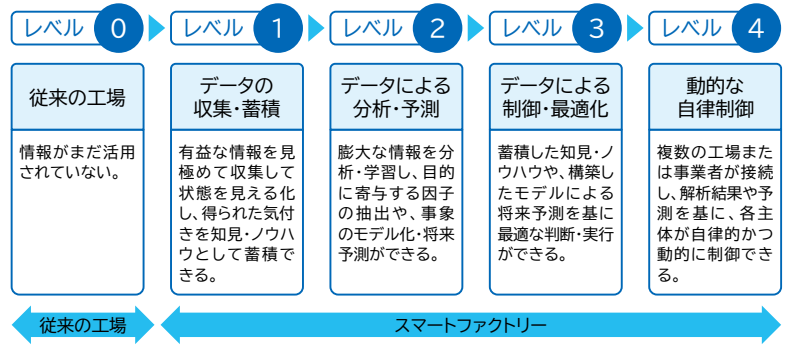
# 拡充版の構成（案）：2. 本ドキュメントのスマート工場

- 「２．本ドキュメントのスマート工場」において、スマート工場の定義と想定リスクを記載する。

## スマート工場とは

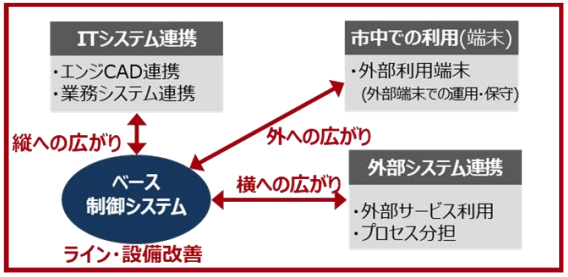
- **製造業におけるスマート化の背景**
  - 技術的革新
  - 国際経済とのつながりの深化
- **スマート化を目指す上で検討すべき課題**
  - グローバルガバナンスの実現
  - 業務標準化・デジタル化（基幹系／IT）
  - スマートマニュファクチュアリングの実現／現場データの活用（OT、IT×OT）
  - 効率的なサプライチェーンマネジメント／デジタルケイレツの実現
- **スマート化によりもたらされる効果**
  - 製造業におけるDXは、付加価値のQCD向上（①エンジニアリングチェーン/ECの最適化、②サプライチェーン/SCの最適化）と事業機会の拡大（③N倍による規模拡大と④サービス化・プラットフォーム化）を可能にする。

- スマートファクトリーとは、データ活用・分析により製造管理の高度化を実現する工場を指す。一般的に、レベルが上がるにつれて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ことから、レベルに応じたセキュリティ対策を行うことが重要である。




## 想定されるセキュリティリスク

- 工場システムが情報システムやインターネットと接続したり、他社や他事業所・他拠点と連携したりする機会が増えている一方で、リスクも新たに発生している。




| | 考慮が必要な事象 | セキュリティリスク |
|---|---|---|
| **ライン・設備改善** | 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** | 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** | 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** | 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 |
| | サイバー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<br>責任範囲が不明確 |

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

# 拡充版の構成（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

- スマート化を進めるに当たっての「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」で示した各ステップでの留意点を示す。
- スマート化の目的を達成するための実現事項（見える化、データ連携等）に合わせ、セキュリティに対する考え方と対策を示す。

## セキュリティにおけるポイント

### 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

- **業務やスマートファクトリーシステムに関する内外要件等の整理**
  - ✓ 業務やシステム範囲の拡大
  - ✓ 内外ステークホルダーの拡大
  - ✓ 関連部署の拡大、ガバナンス体制の変更
  - ✓ 脅威やセキュリティリスクの変化、インシデント発生時の影響の広がり
- **スマート化を進める際の内外の接続の考え方　（現状～将来）**
  - ✓ データ連携
  - ✓ システム・機器接続
- **スマート化を進める際のゾーンの考え方**
  - ✓ 利用サービスや他システムとの間での役割分担
  - • プラットフォームやパッケージとのセキュリティ分担
  - • サービスを利用するうえでのセキュリティ条件の確認と実装
  - • 業務システムのセキュリティ重要度、SQDC要件の確認と実装

### ステップ 2　セキュリティ対策の立案

- **スマート化の目的を踏まえたセキュリティ対策例の整理**
  - ✓ 内外の接続の考え方に応じたセキュリティ対策例
  - ✓ ゾーンの分け方に応じたセキュリティ対策例

※　共通の考え方に加え、FA／PAの事例を記載

※　スマート化の観点を含めて具体的に記載

### 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）

- **スマート化におけるライフサイクルでの対策の留意点**
- **運用・管理面のセキュリティ対策**
  - ✓ 日々の運用における留意点
  - • インシデント対応
  - • 利用するサービスや他システムでインシデント発生（兆候、被害）が発生した場合の保護
  - • 利用するものに脆弱性が発見された場合のアップデート
  - • 利用するものが感染の起点となった場合の対応
  - ✓ スマート化による環境変化を踏まえた見直し
- **維持・改善面のセキュリティ対策**
  - ✓ BCP、レジリエンスへの対応
  - ✓ 未知な事象への対応人材（ノンテクニカルスキル）
- **サプライチェーン対策**
  - ✓ クラウド・汎用品等の調達・契約の留意事項 ※検証関連文書も参照
  - ✓ 外部連携に係る契約先との留意事項
  - ✓ ソフトウェア開発時の留意事項　※主にSBOM関連文書の参照

※　接続形態（拠点内OT/IT接続～拠点間～他社）を考慮した記載を行う。
※　新たな制御モデルやデジタルツイン等のスマート化の将来形と必要なセキュリティについては、ステップ2または3でコラムとして記載する。

# 拡充版の構成（案）：3-ステップ1. 内外要件や業務、保護対象等の整理

- 「3-ステップ1. 内外要件や業務、保護対象等の整理」では、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。
- ゾーン設定の方針やセキュリティ要件の整理等について、既存のフレームワーク（IoT-SSF、データマネジメントフレームワーク）を活用しつつ示す。

| | | |
|---|---|---|
| **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**<br>・スマート工場の目的（生産性向上、品質向上、設備故障予測、技術の継承　等）<br>・BCPとの関係<br>**（2）外部要件の整理**<br>・海外規格の動向　　・業界動向<br>**（3）内部要件／状況の整理**<br>・内外ステークホルダーの拡大<br>・関連部署の拡大、ガバナンス体制の変更<br>・工場、本社生産技術、情報システム部門、セキュリティ担当部門等の洗い出し<br>・インシデント発生時の影響の広がり |
| **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<br>・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**【3.1.3】 | ・スマート化による業務の広がりに伴う、生産業務（S、BC、Q、D、C）に照らした業務の重要度の見直し |
| **ステップ1-4** | **保護対象の整理**【3.1.4】 | ・スマート化によるシステムや接続範囲の拡大に伴う、保護対象の見直し |
| **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た、スマート化を進める際の内外の接続の考え方の整理（現状の整理、現状を踏まえてどのような将来形を描くか　例：ネットワーク環境のオープン/クローズ、AIのクラウド利用/エッジ）<br>・スマート化を進める際のゾーンの設定の方針<br>・ゾーン設定の一例 |
| **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】 | ・ゾーン設定時に検討すべきセキュリティ要件の整理（データマネジメントフレームワーク・IoT-SSFの活用） |

・経営者が実施すべき組織体制の構築に関する事例等について記載する。【A8-3】

・責任分界の考え方や、主なケース毎の対応について記載する。【A7-1】
・制御側・情報側の役割分担について記載する。【A7-3】

・スマートファクトリーの現状を踏まえつつ将来像を示すとともに、技術の進展と合わせBC/SQDC/セキュリティの観点も踏まえて、システム全体のデザインを行い、その中で内部/外部の判断、ゾーンの考え方を記載する。【A1-1】【A1-4】

・クラウド利用時のゾーンの考え方を示す。【A3-2】

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

# 拡充版の構成（案）：3-ステップ2. セキュリティ対策の立案①

- 「3-ステップ2. セキュリティ対策の立案」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。
- スマート化の目的に応じたセキュリティの考え方と対策について、主にシステム構成面を中心にポイントを示す。

| | | |
|---|---|---|
| **ステップ2-1** | **セキュリティ対策方針の策定**【3.2.1】 | 工場システムのセキュリティ対策を実施する上での方針を策定する際に、スマート化を踏まえて、重要度・優先度の見直しを行う。 |
| **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】 | 内外の接続の考え方に応じたセキュリティ対策例を示す。<br>ゾーンの分け方に応じたセキュリティ対策例を示す。<br>・システム、業務の観点でのセキュリティに対する考え方、実現方法<br>※ スマート化の観点を含めて具体的に記載<br>※ 共通の考え方に加え、FA／PAの事例について記載<br>※ 工場の価値であるSQDCの観点を考慮する点を提示 |

・スマート化の目的（課題の把握・対策等）に応じた対策の考え方を示す。【A1-2】【A1-5】

・SQDCの観点はガイドでも取り込んでいるが、改めて脅威と対策の検討においては、セーフティに留意して記載する。【A8-1】
・特定の製品の推奨はできないが、有効な対策や機能等、可能な内容を記載する。【A8-2】

(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
a. ネットワーク接続における対策
・接続形態毎の対策（OT（ライン）内部での接続、OTとITの接続、市中との接続、外部システムとの連携）
例：システム・ネットワーク構成・ネットワーク機器設置の考え方、回線の選択・利用（ワイヤレス／有線、L5G/5G ）等

・OTとIT等、異なるセキュリティが求められるゾーン間の接続における留意点について記載する。【A2-1】【A2-2】【A2-3】【A2-4】
・ワイヤレス利用の際のセキュリティの考え方を示す。【A2-6】

・利用形態・目的毎の対策（データ収集・蓄積（監視）、データ分析・予測（制御への間接的な反映・リアルタイム性低）、制御・高度化（制御への間接的な反映・リアルタイム性高）、メンテナンス（制御への直接的な影響））

・外部から制御を行う場合のセキュリティの考え方を示す。【A2-5】

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

# 拡充版の構成（案）：3-ステップ2. セキュリティ対策の立案②

（続き）

(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（続き）
b. クラウド利用時の対策
・クラウドの利用形態・目的毎の、接続形態、通信経路、データに関するセキュリティの考え方

・クラウド連携の際の留意点

・クラウド利用時のセキュリティに関する確認事項について記載する。【A3-1】
・クラウド利用の際のデータに関するセキュリティの考え方を示す。【A3-3】

②機器におけるセキュリティ対策
a. 汎用品のセキュリティ対策
・汎用品の利用形態・目的毎、利用箇所を考慮したセキュリティの考え方

・汎用品を利用する際のセキュリティ対策の考え方を示す。【A4-1】
・汎用品のセキュリティ対策については、外部接続との関係においても記載する。【A4-2】

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
a. データ活用・連携における対策
・データの利用形態・目的毎のセキュリティの考え方　（例：収集・蓄積（監視）、分析・予測、制御・高度化、メンテナンス）

・フィードバックの際のデータ品質の確保について記載する。【A5-1】

(2)物理面での対策
※ スマート化に関する大きな変更点無し

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

# 拡充版の構成（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

- 「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）」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。
- 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。
- ライフサイクルでの対策のうち、運用・管理面では様々な機器・システムが接続された環境における、インシデント対応や利用するものに脆弱性が発見された場合の対応等について示す。維持・改善面では、現場における工場システムの停止/稼働継続の判断等、事業継続に係る対応や、人材について示す。

### （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**

・ゾーンの分け方に応じたセキュリティ対策例

- インシデント対応、利用するサービスや他システムでインシデント発生（兆候、被害）が発生した場合の保護

・運用時のインシデント対応の考え方や留意点等を記載する。【A6-3】

- 利用するものに脆弱性が発見された場合のアップデート、利用するものが感染の起点となった場合の対応

・インシデント発生時のメーカーに求める対応や、保守契約内容について記載する。【A6-2】
・運用時のパッチ対応の考え方や留意点等を記載する。【A8-4】

・インシデント発生時の対応体制

・インシデント対応の際の、制御側・情報側の役割分担について記載する。【A6-1】

・スマート化による環境変化を踏まえた見直し

**② 維持・改善面のセキュリティ対策**

・BCP、レジリエンスへの対応

- 工場現場における工場システムの停止/稼働継続判断の権限
- 社内における関係部署間の役割分担、外部との連携

・未知な事象への対応人材（ノンテクニカルスキル）

- 変化に対応できる知識の獲得、多様なインシデントの経験

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

# 拡充版の構成（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

- スマート化が進展することにより、サプライチェーン対策がより重要となることから、ステークホルダー間の責任分界の考え方、契約における記載事項等のポイントを示す。

### （2）サプライチェーン対策

・スマート化におけるステークホルダーの広がり、サプライチェーン対策の必要性
　→ 責任分界を行い、契約に落とし込むことが最も重要

・取引先におけるセキュリティの重要性を記載し、責任分界に関する考え方を記載し、契約条項として記載する。【A7-5】【A7-7】【A7-8】
・顧客システムと機器の責任分担の考え方について記載する。【A7-6】

・クラウド・汎用品等の調達・契約の留意事項
　※ セキュリティ検証関連文書も参照

・ベンダとの契約条件や留意点について記載する。【A7-2】

・外部連携に係る契約先との留意事項

・メンテナンスのためのデータ利用時のセキュリティに関して、契約時の確認事項を記載する。【A5-2】
・外部委託の対象に警備会社も想定する。【A7-4】

・ソフトウェア開発時の留意事項
　※ SBOM関連文書も参照

※ 緑枠は、ヒアリングにおいて得られた意見への対応方針を記載

# 検討体制

- 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<br>• メンバー形態は以下の2形態<br>✓ **コアメンバー**：会合における議論・原稿執筆支援が中心<br>✓ **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） |
| **進め方** | • 令和5年10月～12月<br>拡充版内容に関する議論・執筆支援、レビュー<br>（会合3回程度予定、オンライン想定）<br>• 令和6年1月～3月<br>拡充版パブコメ対応支援、レビュー |

※　年度内は随時メンバー募集中。
ご関心のある方は、経済産業省サイバーセキュリティ課までお気軽にお問合せください。

## メンバー（2023/10/17時点）

**<コアメンバー>**

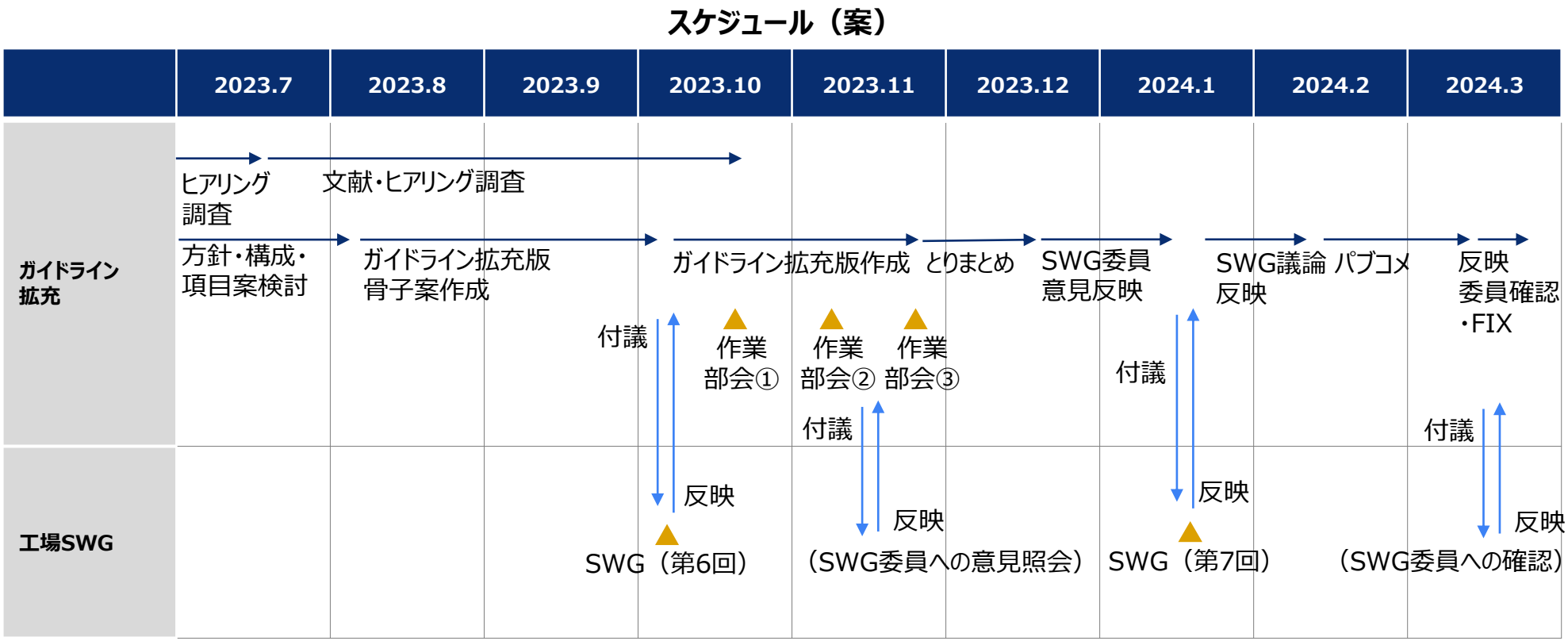
- 名古屋工業大学　渡辺研司委員【作業部会長】
- 技術研究組合制御システムセキュリティセンター　村瀬一郎委員
- 株式会社東芝　斯波万恵委員
- トレンドマイクロ株式会社　高橋弘宰委員
- 日本電気株式会社　桑田雅彦委員
  岡山大河様、大林克成様、小川陽平様
- 日立製作所　中野利彦委員
- ファナック株式会社　斉田浩一委員
- フォーティネットジャパン合同会社　佐々木弘志委員
- 三菱電機株式会社　柴田陽一様、松田規様

**<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
- 三井化学株式会社
- 三菱ガス化学株式会社　※2023年11月～
- 三菱電機株式会社
- 独立行政法人情報処理推進機構

# スケジュール（案）

- 作業部会は、年内に開催する会合（3回程度予定）及び適宜レビューを実施する。検討結果は、適宜工場SWGに付議・報告する形でガイドライン拡充版の策定を進める。
- ガイドライン拡充版は、令和5年度内にパブコメを経た上で、公表を目指す。



# 参考
# 「工場のスマート化におけるセキュリティに関するヒアリング」結果

# 「工場のスマート化におけるセキュリティに関するヒアリング」概要

- 工場のスマート化の取組を進める企業や業界団体に対してヒアリングを実施した。
- 企業または業界団体における工場のスマート化の状況、工場のスマート化に伴うリスクを管理していくための考え方等について調査を行った。

**「工場のスマート化におけるセキュリティに関するヒアリング」概要**

| | |
|---|---|
| 調査対象 | 工場のスマート化の取組を進める企業や業界団体 |
| ヒアリング件数 | 11件 |
| 調査項目数 | 6項目 |
| 調査項目 | 1．工場のスマート化に向けた対応（仮説）について<br>・貴業界（主要な企業）／貴社における工場のスマート化の状況<br>・「工場のスマート化に伴うリスクを管理していくための考え方の仮説」についてのご意見<br>- スマート化に関する状況、及びセキュリティに関する懸念の有無・対応<br>- スマート化（自動化）が進む中でのセキュリティインシデント対応の想定（人材、組織、ルール等）<br>- クラウドサービス事業者・調達先等、外部連携先との責任分界や役割分担　　等<br>・上記以外の工場のスマート化におけるセキュリティに関する課題・ニーズ<br>・スマート化の観点から、「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」への記載が望ましい事項<br><br>2．デジタルツイン・制御の高度化に関する現状とセキュリティ課題について<br><br>3．ガイドライン拡充に関する検討を行う作業部会（工場SWGの下に設置）へのご参画や意見出しについて |
| 調査期間 | 2023年6月～2023年7月 |

# 工場セキュリティガイドライン拡充に関するヒアリング結果①

| ヒアリング項目 | カテゴリ | 【No】 | ご意見 | 対応方針（案） |
|---|---|---|---|---|
| 工場のスマート化に向けた対応（仮説）について | 【A1】全般 | 【1】 | • スマートファクトリーについては、この先こうなるという絵姿を入れて欲しい。例えば、クラウドに載せなくてもエッジで処理できることが増えている中、どのような処理を内部で実施し、どこを外部に出すかをそれぞれで判断し、その上で、ゼロトラストやゾーンを考えていくことになるのではないか。 | ➢ スマートファクトリーの現状を踏まえつつ将来像を示すとともに、技術の進展と合わせBC/SQDC/セキュリティの観点も踏まえて、システム全体のデザインを行い、その中で内部/外部の判断、ゾーンの考え方を記載する。 |
| | | 【2】 | • 現場でAIを活用したいニーズがあれば、そのヒントになるような情報があるとよい。 | ➢ スマート化の目的（課題の把握・対策等）に応じた対策の考え方を示す。 |
| | | 【3】 | • 国がガイドラインをどのように活用してほしいのかを書けると良い。日本の製造業に何を求めているかを明らかにしてほしい。 | ➢ セキュリティを考慮したDX、スマート化の推進のためのガイドである点について記載する。 |
| | | 【4】 | • スマート化を目指す上で、工場側のシステムの構築思想を整理したい。安全に外部と繋げていく前提で、システムの中身をどう構築するべきかを検討している。 | ➢ 【A1-1】と同様。 |
| | | 【5】 | • 設備に応じたガイドラインがあれば事業者はガイドラインを使うイメージを持ちやすくなると考える。 | ➢ 設備は個社毎に様々であるので、スマート化の目的に応じた対策の考え方を示す。 |
| | 【A2】接続 | 【1】 | • DXと言われる部分は相当進めている。社内では、OTとITをどのようにつなげるかが主な検討内容である。 | ➢ OTとIT等、異なるセキュリティが求められるゾーン間の接続における留意点について記載する。 |
| | | 【2】 | • インダストリアルDMZやマイクロセグメンテーションを社内向けガイドラインの中で記載しており、まさにこれから具現化するところである。 | ➢ ゾーン設計の考え方と、異なるセキュリティが求められるゾーン間の接続における留意点について記載する。 |
| | | 【3】 | • 工場のライン上で自動化を進めているが、繋ぐ区間のセキュリティはどのように担保するか。 | ➢ 【A2-1】と同様。 |
| | | 【4】 | • 外部と繋げる場合、セキュリティ確保に向けてどのような回線を使うのか検討を行う。ソリューションはゼロトラスト関連のものが多く、最新のものを導入すべきなのか、限定して利用するか、メーカーが提供するソリューションも複数あり、どれが良いのか判断が難しい。 | ➢ 【A2-1】と同様。 |

# 工場セキュリティガイドライン拡充に関するヒアリング結果②

| ヒアリング項目 | カテゴリ | 【No】 | ご意見 | 対応方針（案） |
|---|---|---|---|---|
| 工場のスマート化に向けた対応（仮説）について | 【A2】接続（続き） | 【5】 | • 外から制御側が操作する場合のセキュリティをどう進めるかが今後の検討課題である。 | ➢ 外部から制御を行う場合のセキュリティの考え方を示す。 |
| | | 【6】 | • AGV、自動搬送機、ワイヤレスで繋がっており、どのようなセキュリティ対策が実際にできるか、今後勉強しながら導入したいと考えている。 | ➢ ワイヤレス利用の際のセキュリティの考え方を示す。 |
| | 【A3】クラウド | 【1】 | • 出口自体がクラウドということも多く、クラウド側にどのようにデータを持って行くのか、またクラウド上の情報をどのように取り込むかが課題となる。 | ➢ クラウド利用時のセキュリティに関する確認事項について記載する。 |
| | | 【2】 | • 現場からまだニーズはないが、クラウドに情報を出すならどういうルートで出すか、クラウドから情報を装置に戻すのであれば、どのように行えるかが今後の検討課題である。 | ➢ クラウド利用時のゾーンの考え方を示す。 |
| | | 【3】 | • 制御系、情報系のネットワークとは別に、無線センターと無線センサー用の別の通信手段、外部のクラウドを使用できるよう環境を整備している。情報の一部が外部のクラウド上に保管されているが、設備の状態に関するデータは、運転・制御に係る情報ではなく機微情報ではないので、クラウドに載せたとしてもセキュリティ上の懸念はしていない。 | ➢ クラウド利用の際のデータに関するセキュリティの考え方を示す。 |
| | 【A4】汎用品 | 【1】 | • 汎用品において、コストとセキュリティの確保はトレードオフであり、今後の検討課題と認識している。 | ➢ 汎用品を利用する際のセキュリティ対策の考え方を示す。 |
| | | 【2】 | • 業務効率化を目的としたタブレットの導入や、設備管理を目的としたセンサを試験的に導入している。これらは市販品でありブラックボックス状態ではあるが、外部とつなげていないため、特にセキュリティ上の懸念は抱いていない。 | ➢ 汎用品のセキュリティ対策については、外部接続との関係においても記載する。 |
| | 【A5】データ | 【1】 | • トレーサビリティを確保する必要性がある。IT側からOT側へのフィードバックループの信頼性を確保するために、データの品質、改ざんされていないか等も、今後の検討課題として認識している。 | ➢ フィードバックの際のデータ品質の確保について記載する。 |
| | | 【2】 | • メンテナンスの際、どこまでデータを見られているか、データを取られているかは懸念している。確認すればよいのだろうが、セットで導入されるケースもある。 | ➢ メンテナンスのためのデータ利用時のセキュリティに関して、契約時の確認事項を記載する。 |

# 工場セキュリティガイドライン拡充に関するヒアリング結果③

| ヒアリング項目 | カテゴリ | 【No】 | ご意見 | 対応方針（案） |
|---|---|---|---|---|
| 工場のスマート化に向けた対応（仮説）について | 【A6】インシデント対応 | 【1】 | • インシデント対応として、CSIRT規則を作った。会社の危機管理対策規定では、サイバー攻撃があった場合、情報系の対応は従来から含まれていたが、制御系について、工場の生産や安全の確保を優先し、工場側が手動で止める権限を有することを規定した。 | ➢ インシデント対応の際の、制御側・情報側の役割分担について記載する。 |
| | | 【2】 | • インシデントが起きた場合、社内の情報系に連絡を行うが、メーカーにも報告する。デバイスや制御装置を作っているメーカーに対しても指導が必要である。 | ➢ インシデント発生時のメーカーに求める対応や、保守契約内容について記載する。 |
| | | 【3】 | • 現状、方法を模索しながらサイバーセキュリティ対策の訓練を行っている。ケーススタディを例示していただけるとありがたい。 | ➢ 運用時のインシデント対応の考え方や留意点等を記載する。 |
| | 【A7】役割分担 | 【1】 | • 責任分界について、検討することは非常に重要である。スマート化により、社内外のプレーヤーが増えたり変わったりすることが予想される。その際、責任範囲や責任を取る主体を切れ目なく検討することは難しい。 | ➢ 責任分界の考え方や、主なケース毎の対応について記載する。 |
| | | 【2】 | • 情報システム、生産技術、工場現場で新たな組織を立ち上げた。ベンダとの利用条件等を含んだ契約時においては、新設組織と外部のベンダが協力し、システムの導入やどの機器にどうつなぐか等を協議している。 | ➢ ベンダとの契約条件や留意点について記載する。 |
| | | 【3】 | • 制御系の部門と情報システム系の部門があり、社内規則によってハード系とソフト系で社内の役割分担を行っている。<br>• 制御系と情報系はFWで介しており、役割分担もそれに準じている。制御システムについては、クラウドサービスを現在利用していないため、制御システムに関する管理は、現場の担当者が管轄している。 | ➢ 制御側・情報側の役割分担について記載する。 |
| | | 【4】 | • さまざまな箇所に監視カメラを導入している。カメラは工場内にあり、ローカルネットワークに繋いでいる。カメラは警備会社が監視しており、警備会社のネットワークと繋いでいる。 | ➢ 外部委託の対象に警備会社も想定する。 |
| | | 【5】 | • サプライチェーン上のつながりから、取引先におけるセキュリティ対策の重要性の強調をお願いしたい。（取引先に要請する際に活用できる） | ➢ 取引先におけるセキュリティの重要性を記載し、責任分界に関する考え方を記載し、契約条項として記載する。 |
| | | 【6】 | • 納品機器はIEC62443がベースで作るものは変わらないが、周辺のロボット・搬送装置・プログラムなどのソフトウェアを構築するにあたって、顧客システムと自社のインターフェースの責任をどのように分けるかが課題である。 | ➢ 顧客システムと機器の責任分担の考え方について記載する。 |

# 工場セキュリティガイドライン拡充に関するヒアリング結果④

| ヒアリング項目 | カテゴリ | 【No】 | ご意見 | 対応方針（案） |
|---|---|---|---|---|
| 工場のスマート化に向けた対応（仮説）について | 【A7】役割分担（続き） | 【7】 | • 特に中小企業とのコミュニケーションにおいては苦労することも多く、責任分界に関する基準を提示してもらえるとコミュニケーションを取りやすくなると考える。 | ➢ 【A7-5】と同様。 |
| | | 【8】 | • IEC62443の考え方、すなわちセキュリティ対策は誰か一者だけで進めるものではなく、使う側も調達する側も含めそれぞれが実施するものである点について普及してほしい。 | ➢ 【A7-5】と同様。 |
| | 【A8】その他 | 【1】 | • セーフティの観点が抜け落ちてしまうおそれがある。セーフティ機能があるところをバイパスしてしまうことが懸念される。 | ➢ SQDCの観点はガイドでも取り込んでいるが、改めて脅威と対策の検討においては、セーフティに留意して記載する。 |
| | | 【2】 | • セキュリティ製品に関する情報が氾濫している。どの製品を使うのが良いかを判断することが難しい。適切な判断を後押しすることができるような書きぶりがあることが望ましい。 | ➢ 特定の製品の推奨はできないが、有効な対策や機能等、可能な内容を記載する。 |
| | | 【3】 | • 経営者が社内にセキュリティ対策に関する組織体制を検討する際に、検討を後押しできるような取り組みを具体的に示してもらえると良い。 | ➢ 経営者が実施すべき組織体制の構築に関する事例等について記載する。 |
| | | 【4】 | • ユーザー側がラインの停止を懸念してパッチを当てないことがある。実験実証用のラインを持てるような業界は持つよう推奨し、そうではない場合、仮想で検証してパッチを当てることを推奨する書きぶりにすると良いか。 | ➢ 運用時のパッチ対応の考え方や留意点等を記載する。 |
| 【B】その他 | | 【1】 | • 中国でPLCのセキュリティ認証が始まる等、各国の規制にそれぞれ対応しなければならない状況において、メーカーの負担を軽減するような国の施策があると望ましい。経済安全保障の関係でも、製品の保護のために必要なのではないか。 | ➢ 今後の工場セキュリティに関連する政策の検討において参考とする。 |
| | | 【2】 | • メーカーの製品や技術の見極めが困難である。ガイドラインや決められた規格に準拠しているなどがあると工場側は導入しやすくなる。 | ➢ 今後の工場セキュリティに関連する政策の検討において参考とする。 |
| | | 【3】 | • ある程度の企業になると、自社でガイドラインを作成している。IEC 62443を参照にしながら、自社でガイドラインを作成した。まだ取り組みが進んでいない中小企業などに対しては、ガイドラインの普及を通じて、セキュリティ確保の取り組みを推奨する必要があると考える。 | ➢ 引き続き、ガイドラインの普及啓発を進めていく。 |