経済産業省

# 「半導体デバイス工場における OTセキュリティガイドライン」概要資料

商務情報政策局 サイバーセキュリティ課・情報産業課

# 半導体デバイス工場におけるOTセキュリティガイドライン~全体概要~

## ガイドラインの背景と目的

- 半導体産業の経済及び安全保障上の重要性や足下でのサイバー脅威/リスクの高まりを踏まえると、高度なサイバー攻撃への対応を含めたセキュリティ対策を進めていく必要がある。
- 海外では、国際的な半導体関連の業界団体であるSEMIにより、半導体製造装置に係るE187/E188規格が策定され、米国立標準技術研究所（NIST）においてもCybersecurity Framework 2.0（以下、NIST CSF 2.0）について、半導体製造プロファイルの策定が進んでいる。
→**国際的な半導体産業における各種セキュリティ規格と整合しつつ、生産目標の維持・機密情報保護・半導体品質の維持のための工場セキュリティ対策の指針を示す**。

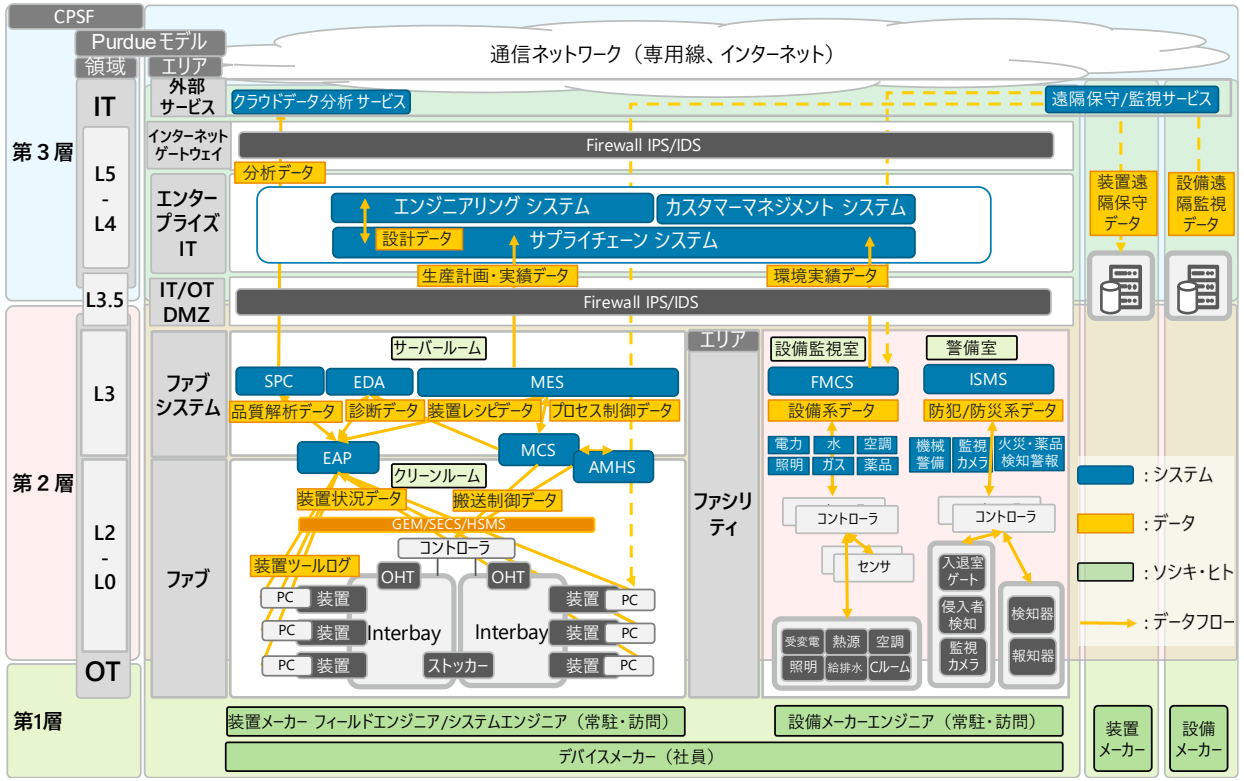
## 本ガイドラインの活用方法

- 本ガイドラインは、主に**半導体デバイスメーカーの製造部門（実務者レベル）**を対象としており、サイバー空間とフィジカル空間を統合的に保護するための基本原則と具体的な指針を定めた**サイバー・フィジカル・セキュリティ対策フレームワーク（以下、CPSF）やNIST CSF2.0等リスクベースのフレームワークを活用したリスク分析、セキュリティ対策の検討をする際の参考資料として活用**することができる。

- **組織プロファイルの作成**
本ガイドラインの第3章の特徴及び考慮すべき観点に記載されている内容を参考に、サブカテゴリ毎の現状の把握と目標の設定
- **行動計画を策定**
組織プロファイルの現状と目標のギャップ分析から行動計画を策定するにあたり、本ガイドラインの第3章に記載されているCPSFの対策要件IDやE187製造リファレンス、及び第4章に記載されている対策例を参照

## 本ガイドラインで示す対策項目

- 半導体デバイス工場のリファレンスアーキテクチャに基づき、リスク対策フレームワーク（CPSF及びNIST CSF2.0）を活用し、**半導体デバイス工場の特徴を踏まえたリスク源（脅威、脆弱性）の洗い出しを行うとともに対応するセキュリティ対策項目**について取りまとめた。
- Purdueモデルで分類した**ファブエリア、ファブシステムエリア、外部サービス及びIT/OT DMZ、組織・ヒト側面**について対策項目を整理した。




半導体デバイス工場のリファレンスアーキテクチャ

# ガイドラインの構成　1. 本ガイドライン作成の背景と目的①

- 「1. 本ガイドライン作成の背景と目的」において、本ガイドラインの背景と目的や想定読者、守るべき対象、想定する攻撃主体、本ガイドラインの利活用、本ガイドラインの構成について記載

## ガイドラインの背景と目的

- サイバー攻撃はますます多様化・高度化しており、多くの制御装置等が攻撃され、工場における生産が停止する等の被害が発生している。また各種の開発機密（知的財産）がサイバー攻撃によって流出する危険も増している。半導体産業の経済及び安全保障上の重要性や足下でのサイバー脅威/リスクの高まりを踏まえると、高度なサイバー攻撃への対応を含めたセキュリティ対策を進めていく必要がある。海外では**国際的な半導体関連の業界団体であるSEMIにより、半導体製造装置に係るE187/E188規格が策定され、米国立標準技術研究所（NIST）においてもCybersecurity Framework 2.0（以下、NIST CSF 2.0）について、半導体製造プロファイルの策定が進んでいる。**
- 一方、国内の半導体産業全体でセキュリティ対策を進める枠組みは存在しないため、**国際的な半導体産業における各種セキュリティ規格と整合しつつ、国内の半導体産業におけるセキュリティ対策状況等を踏まえた工場セキュリティ対策の指針を示すことが喫緊の課題**である。
- 経済産業省では、汎用的な組立型の工場向けに「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」を策定し公表しているが、**半導体工場は一般的にプロセスオートメーション（PA）型の工場であり、工場の規模が大きく、汎用OSを用いた製造装置の台数が多い等の特徴があることから、新たに半導体デバイス工場向けに本ガイドラインを策定した。**

## 想定読者

- 半導体デバイスメーカーの製造部門（実務者レベル）
（製造装置メーカー、素材メーカーの製造部門）

## 想定する攻撃主体

- 半導体製造のサプライチェーンは安全保障上の重要性から、**最も高度な攻撃者（国家の支援を受けたグループ（APT））を想定した対策レベルを実現する必要がある。**（IEC62443ではSL4）

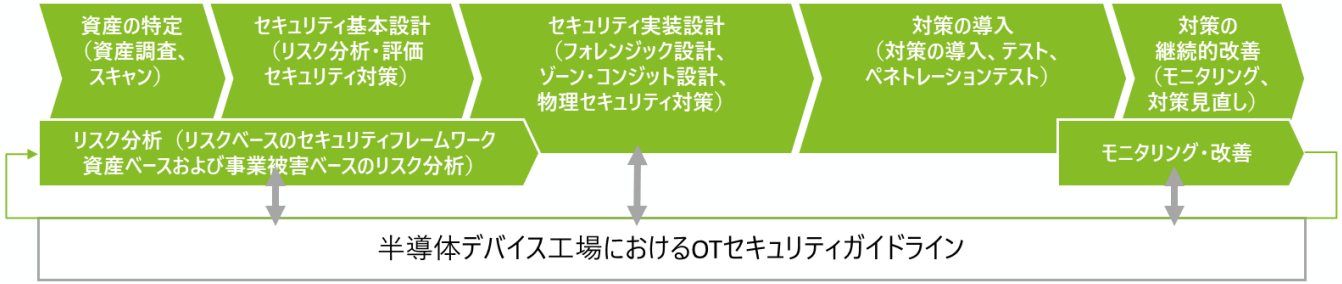
## 守るべき対象

- 「生産目標の維持（供給責任）」「機密情報の保護」「半導体の品質の維持」「環境安全の維持」「人間の安全の維持」の5つの項目がNIST CSF2.0 半導体製造プロファイルで守るべき項目として挙げられている。
- 本ガイドラインでは特に**「生産目標の維持（供給責任）」「機密情報の保護」「半導体の品質の維持」**に焦点をあてる

# ガイドラインの構成　1. 本ガイドライン作成の背景と目的②

## 本ガイドラインの利活用

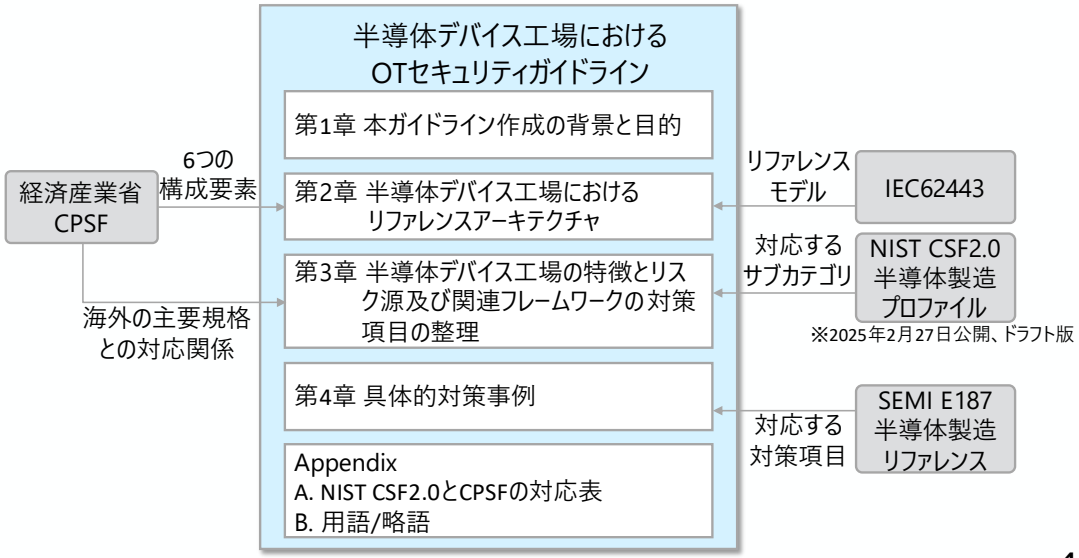
- 半導体サプライチェーンの保護という目的を達成するためには、構成する各企業が供給責任を果たせるサイバーセキュリティ対策を実現する必要があり、供給責任・事業継続計画と整合する必要がある。
- 供給責任及びその説明責任を果たすためには、**リスクの評価を行い、その結果を踏まえた適切な対策を検討・設計・実装する必要がある。**
- 本ガイドラインは、**工場のセキュリティ対策を進めるための一般的なプロセスにおいて、リスクベースのサイバーセキュリティフレームワーク（CPSF*1、NIST CSF2.0 *2）を活用したリスク分析、及び具体的な対策を検討する際などに活用することが想定される。**また、工場における制御系システムの具体的なリスク分析の方法については、IPA『制御システムのセキュリティリスク分析ガイド』 *3が参考になる。




*1：https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
サイバー・フィジカル・セキュリティ対策フレームワーク：サイバー空間とフィジカル空間を統合的に保護するための基本原則と具体的な指針を定めたフレームワーク
*2：https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
*3：https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

## 本ガイドラインの構成

- 第2章：IEC62443のPurdueモデルを活用し半導体デバイス工場を領域・エリアに分割し、各エリアにおける CPSFの6つの構成要素を洗い出した。
- 第3章：前述CPSFの6つの構成要素に関連する半導体デバイス工場における特徴を整理し、 CPSFを活用しこれら特徴に起因するリスク源の洗い出し、及びNIST CSF2.0半導体製造プロファイルとの紐づけを行った。
- 第4章：マイクロセグメンテーション等、半導体デバイス工場において特に重要となる取り組みに関しては、より詳細な対策方法の例を示した。



# ガイドラインの構成　2. 半導体デバイス工場におけるリファレンスアーキテクチャ①

- 「2. 半導体デバイス工場におけるリファレンスアーキテクチャ」において、サイバー攻撃から守るべき対象「生産目標の維持（供給責任）」「機密情報の保護」「半導体の品質の維持」に対してセキュリティ対策を検討しやすくすることを目的とした整理した半導体デバイス工場のリファレンスアーキテクチャについて記載

**半導体デバイス工場のリファレンスアーキテクチャの特徴**

- **産業制御システム（ICS）向けのアーキテクチャであるPurdueモデルを汎用的な半導体デバイス工場に適用**
  工場における主要なエリアを「IT領域」「OT領域」「IT/OT DMZ」に分割し、各エリアに対してレベル（L）0ー4/5の関連付けした。
- **半導体デバイス工場における特徴を考慮したリスクの抽出及びこれに対するセキュリティ対策を整理するため、CPSFを適用**
  半導体デバイス工場をCPSFの三層構造に分割するとともに、CPSFの6つの構成要素（ソシキ、ヒト、システム、プロシージャ、モノ、データ）を抽出した。

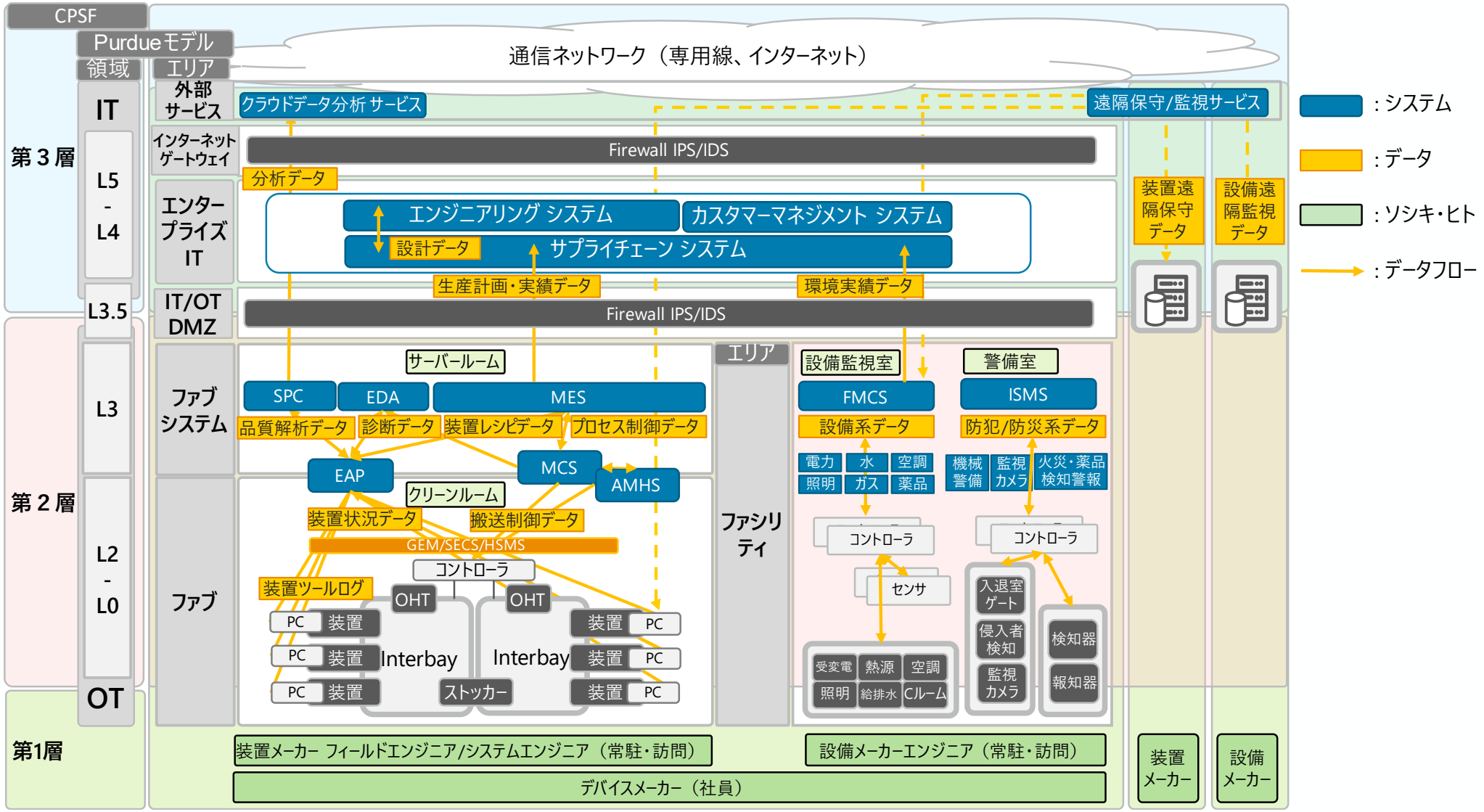
## Purdueモデル

- IT領域（レベル 4-5）
  - インターネットゲートウェイ（レベル 5）
  - エンタープライズITエリア（レベル 4-5）
- OT領域（レベル 0-3）
  - ファブシステムエリア（レベル 3）
  - ファブエリア（レベル 0-2）
  - ファシリティエリア（レベル 0-3）
- IT/OT DMZ（レベル 3.5）

## CPSF三層構造

- 第1層
  半導体デバイス工場を中心とした、企業間（ソシキ・ヒト）のつながり
- 第2層
  半導体デバイス工場内のフィジカル空間とサイバー空間のつながり
- 第3層
  半導体デバイス工場から外のサイバー空間でのサービス利用のつながり

# ガイドラインの構成　2. 半導体デバイス工場におけるリファレンスアーキテクチャ②




半導体デバイス工場のリファレンスアーキテクチャ

# ガイドラインの構成　2. 半導体デバイス工場におけるリファレンスアーキテクチャ③

| Purdueモデル | | CPSFによる6つの構成要素 | | | | | |
|---|---|---|---|---|---|---|---|
| 領域 | | システム | データ | モノ | プロシージャ | ソシキ及びヒト | |
| | | | | | | デバイスメーカー | 協力会社 |
| 外部サービス | | クラウドデータ分析サービス<br>遠隔監視保守サービス | クラウド分析データ<br>遠隔監視・保守データ | サービス | インターネットを通じたクラウドサービス及び、装置・設備メーカーからの遠隔保守・監視サービスプロセスを実施 | IT部門がインターネットを通じたセキュリティ管理(リモートアクセス含む)の中心 | クラウドサービスメーカー、設備メーカー、装置メーカー |
| インターネット<br>ゲートウェイ | | インターネット<br>ゲートウェイ(RAS) | 組織外通信制御データ | ファイア・ウォール、IPS/IDS等 | インターネットや外部サービスとの通信制御を実施 | IT部門が全社エンタープライズ・セキュリティ管理の中心<br>(設計、調達、販売、人事、経理、管理等) | 各部署の業務委託会社 |
| IT | エンタープライズ<br>(L4-5) | SCM、ECM、CRM | SCM、ECM、CRMデータ | サーバ、ネットワーク、<br>PC、スマートフォン、複合機等 | 半導体製造企業におけるIT業務(SCM、ECM、CRM)プロセスを実施 | | |
| IT/OT DMZ<br>(L3.5) | | IT/OT DMZ | 組織内領域、通信制御データ | ファイア・ウォール、IPS/IDS等 | IT業務とOT業務のプロセス間通信制御を実施 | | |
| OT | ファブシステム<br>(L3) | MES<br>SPC<br>EDA | 生産進捗データ<br>品質特性・解析データ<br>装置収集・プロセス診断データ | サーバ、<br>ストレージ、<br>ネットワーク | 半導体製造における製造のプロセス実行・品質管理プロセスを実施 | 製造部門がセキュリティ含めた製造管理の中心<br>(品質保証、プロセス技術、生産技術、製造システム等) | システムサービス会社 |
| | ファブ<br>(L0-2) | EAP<br>AMHS<br>MCS | 最適プロセスフロー【機密】、装置状況データ、レシピ【機密】、搬送・ロット制御データ、ロット最適化ロジック | 装置ツール(製造、検査、測定)、<br>OHT、OHS、<br>ストッカー、FOUP | 製造各装置による工程プロセスを実施、工程内、工程間の搬送制御を実施、業界規格GEM/SECSにて通信を実施 | | 装置メーカー<br>(フィールドエンジニア<br>常駐、オフィスあり) |
| | ファシリティ<br>(L0-3) | FMCS<br>ISMS | 設備データ、環境データ<br>防犯データ、防災データ | 各設備、コントローラ、<br>センサ | 半導体製造のクリーンルーム及び各装置への設備環境の運営管理プロセスを実施 | ファシリティ部門が物理セキュリティ含めた工場施設管理の中心 | 設備メーカー<br>(電気、給排水、ガス、薬品各社　常駐、オフィスあり) |

PurdueモデルとCPSFによる6つの構成要素

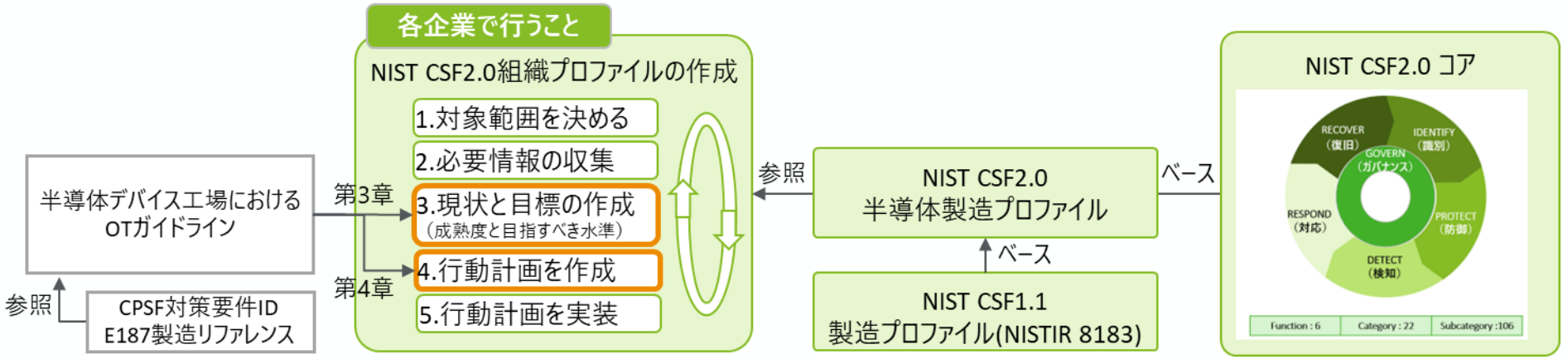
# ガイドラインの構成

## 3. 半導体デバイス工場の特徴とリスク源及び関連フレームワークの対策項目の整理①

### NIST CSF2.0、NIST CSF2.0半導体製造プロファイル等を活用して自組織のリスク分析を行うケース

**本ガイドラインは、CPSFやNIST CSF2.0等リスクベースのフレームワークを活用したリスク分析を行ったり、セキュリティ対策の検討をする際の参考資料として活用することができる。**
具体的には以下のような活用方法を想定している。

- **組織プロファイルの作成**
  本ガイドラインの第3章の特徴及び考慮すべき観点に記載されている内容を参考に、サブカテゴリ毎の現状の把握と目標の設定
- **行動計画を策定**
  組織プロファイルの現状と目標のギャップ分析から行動計画を策定するにあたり、本ガイドラインの第3章に記載されているCPSFの対策要件IDやE187製造リファレンス、及び第4章に記載されている対策例を参照



# ガイドラインの構成

## 3. 半導体デバイス工場の特徴とリスク源及び関連フレームワークの対策項目の整理②

### リファレンスアーキテクチャを活用したセキュリティ対策項目への整理

本ガイドラインは、工場のセキュリティ対策を進めるための一般的なプロセスにおいて、リスクベースのサイバーセキュリティフレームワーク（CPSF、NIST CSF2.0 半導体製造プロファイル）を活用したリスク分析、及び具体的な対策を検討する際などに活用することが想定し作成されている。以下に**本ガイドライン（第3章、第4章）とNIST CSF2.0 半導体製造プロファイル、CPSF等を活用した組織プロファイルの現状分析や目標設定の流れを示す。**

**「リスク分析のための情報」（本資料P.12、13）の活用方法**

**現状と目標の作成**

**特徴の把握及び関連箇所の確認**

第3章にて各領域・エリアの「特徴」を読んだ上で、「関連するNIST CSF2.0 半導体製造プロファイル 及び CPSF」に記載されているサブカテゴリ 及び 対策要件IDの内容を確認する

**組織プロファイルの目標設定**

NIST CSF2.0 半導体製造プロファイル、CPSF等を用いて組織プロファイルの現状分析や目標設定をする際に、「セキュリティ対策を行う上で考慮するべき観点」を参考としつつ行う

**行動計画の作成**

**具体的対策例の活用**

第4章「半導体デバイス工場における具体的対策例」及びE187 製造リファレンス等を参考とし、対策検討を進める

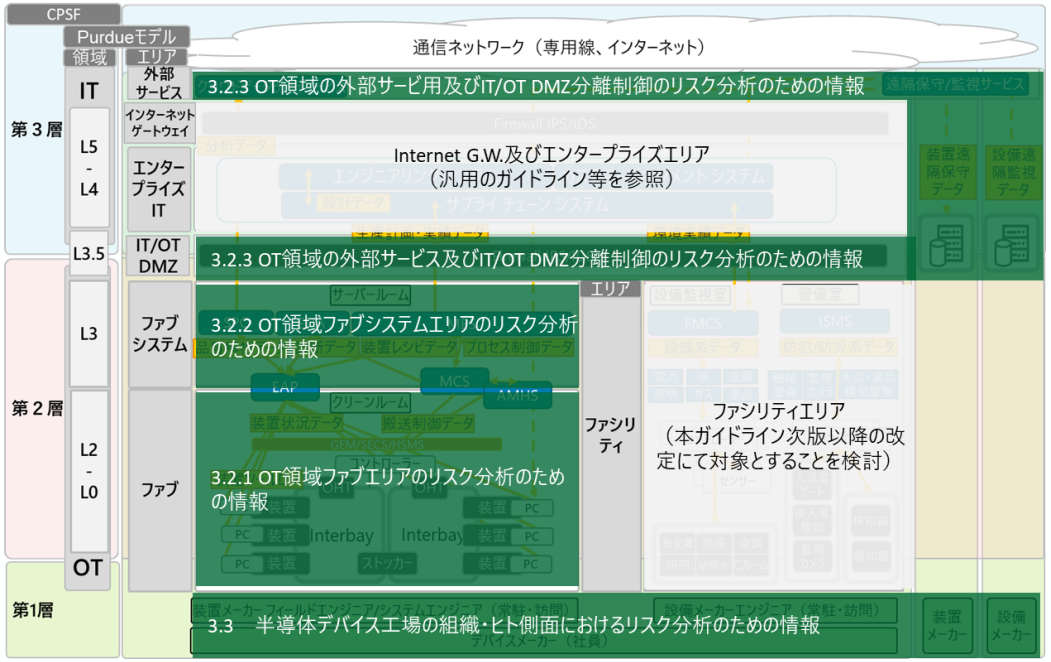
# ガイドラインの構成

## 3. 半導体デバイス工場の特徴とリスク源及び関連フレームワークの対策項目の整理③

### リファレンスアーキテクチャを活用したセキュリティ対策項目への整理

**リファレンスアーキテクチャを活用し、半導体デバイス工場における特徴を踏まえたリスク源（脅威、脆弱性）の洗い出しを行い、対応するリスク対策フレームワーク（CPSF及びNIST CSF2.0）のセキュリティ対策項目について取りまとめている。**

対策項目の整理の対象範囲については、Purdueモデルで分類したファブエリア、ファブシステムエリア、IT/OT DMZ、外部システム及び組織・ヒト側面とする。
インターネットゲートウェイ及びエンタープライズエリアは、通常のIT領域におけるセキュリティ対策と差異がないことから、第3章の対象外とする。
OT領域のファシリティエリアについては、現在検討が進められている国際的な規格との連携を考慮し、本ガイドライン次版以降の対象とする予定である。




| Purdueモデル | | CPSFによる6つの構成要素 | | | | | |
|---|---|---|---|---|---|---|---|
| 領域 | | システム | データ | モノ | プロシージャ | ソシキ及びヒト | |
| | | | | | | デバイスメーカー | 協力会社 |
| 外部サービス | | クラウドデータ分析サービス | クラウド分析データ | サービス | インターネットを通じたメーカーからの遠隔保守・監視サービスプロセスを実施 | IT部門がインターネットを通じたセキュリティ管理(リモートアクセス含む)の中心 | クラウドサービスメーカー、設備メーカー、装置メーカー |
| インターネットゲートウェイ | | インターネットゲートウェイ(RAS) | 組織外通信制御データ | ファイア・ウォール、IPS/IDS等 | インターネット/外部サービスとの通信制御を実施 | IT部門が全社エンタープライズ・セキュリティ管理の中心（設計、調達、販売、人事、経理、管理等） | 各部署の業務委託会社 |
| IT | エンタープライズ(L4-5) | SCM, ECM, CRM | | 複合機等 | 半導体製造企業におけるIT業務(SCM, ECM, CRM)プロセスを実施 | | |
| IT/OT DMZ (L3.5) | | | | IPS/IDS等 | 通信制御を実施 | | |
| OT | ファブシステム(L3) | MES<br>SPC<br>EDA | 生産進捗データ<br>品質特性・解析データ<br>装置収集・プロセス診断データ | サーバ、ストレージ、ネットワーク | 半導体製造における製造のプロセス実行・品質管理プロセスを実施 | 製造システム部門が品質保証、プロセス技術、生産技術、製造システム等） | |
| | ファブ(L0-2) | EAP<br>AMHS<br>MCS | 最適プロセスフロー【機密】、装置状況【機密】、装置状況診断データ、ロット最適化ロジック | 装置ツール(製造、検査、測定)、 | 製造各装置による工程プロセスを実施、工程間の搬送を実施、業界規格GEM/SECSにて通信を実施 | | 装置メーカー（フィールドエンジニア 常駐、オフィスあり） |
| | ファシリティ(L0-3) | FMCS<br>ISMS | 設備データ、環境データ | 各装置、コントローラー | 半導体製造のクリーンルーム及び各装置を実施 | ファシリティ部門が物理セキュリティ含めた工場施設管理の中心 | 設備メーカー（電気、給排水、ガス、薬品各社 常駐、オフィスあり） |

3.2.3 OT領域の外部サービス用及びIT/OT DMZ分離制御のリスク分析のための情報
Internet G.W.及びエンタープライズエリア（汎用のガイドライン等を参照）
3.2.3 OT領域の外部サービス及びIT/OT DMZ分離制御のリスク分析のための情報
3.2.2 OT領域ファブシステムエリアのリスク分析のための情報
3.2.1 OT領域ファブエリアのリスク分析のための情報
ファシリティエリア（本ガイドライン次版以降の改定にて対象とすることを検討）
3.3　半導体デバイス工場の組織・ヒト側面におけるリスク分析のための情報

# ガイドラインの構成

## 3. 半導体デバイス工場の特徴とリスク源及び関連フレームワークの対策項目の整理④

### リスク分析のための情報

リファレンスアーキテクチャで整理したPurdueモデルに基づき、**技術・物理的側面及び組織・ヒト側面から特徴と考慮すべき観点を洗い出し、脅威や脆弱性をリスク源の視点からまとめる。**さらに、**業界グローバルでの対策フレームワークやリファレンス（NIST CSF2.0 半導体製造プロファイル、SEMI E187製造リファレンス）及びCPSFとの関係を整理**して示す。

**技術・物理的側面**

| 3.2　半導体デバイス工場の技術・物理的側面におけるOT領域各エリア別のリスク分析のための情報 |
|---|
| **3.2.1　OT領域ファブエリアのリスク分析のための情報** |
| ① 装置ツールの資産管理と脆弱性評価 |
| ② 装置ツールの被害の極小化と早期復旧を備えた追加防御対策 |
| ③ 安全な装置ツールの調達と導入 |
| ④ 生産機密情報の把握とデータ管理 |
| ⑤ 物理アクセスの制限（入室・持込み・接続） |
| ⑥ 論理的アクセスの制限（ID管理、認証及びアクセス制御） |
| **3.2.2　OT領域ファブシステムエリアのリスク分析のための情報** |
| ①システム可用性 |
| ②データ保全 |
| ③サーバルームの物理的対策 |
| **3.2.3　OT領域の外部サービス活用及びIT/OT DMZ分離制御のリスク分析のための情報** |
| ① 外部サービス活用（クラウドサービス） |
| ② 外部サービス活用（遠隔診断サービス利用） |
| ③ IT/OT DMZ |

**組織・ヒト側面**

| 3.3　半導体デバイス工場の組織・ヒト側面におけるリスク分析のための情報 |
|---|
| ① ガバナンス（ビジネス環境の理解、役割・責任・権限の確立） |
| ② 法規制・業界標準対応（人命の確保及び環境安全の維持） |
| ③ 供給責任・サプライチェーン対応（生産目標・製品品質の維持） |
| ④ 生産機密情報の保護 |
| ⑤ リスクマネジメント・ポリシー・レジリエンス |
| ⑥ 運用（監視・対応・復旧・改善） |
| ⑦ 意識向上とトレーニング |

# ガイドラインの構成

## 3. 半導体デバイス工場の特徴とリスク源及び関連フレームワークの対策項目の整理⑤

### リスク分析のための情報（例：装置ツールの資産管理と脆弱性評価①）

<table>
<tr><th colspan="2">領域・エリア</th><th>特徴　及び　セキュリティ対策を行う上で考慮すべき観点</th></tr>
<tr><td>OT</td><td>ファブ<br>エリア</td><td>
①装置ツールの資産管理と脆弱性評価<br>
特徴<br>
半導体デバイス工場の製造工程であるファブエリアは、クリーンルーム環境内において異メーカー装置ツールをシームレスにシステム連携を用いてプロセスを形成し、自動連動生産を行っている。これらの装置ツールは、ウェハーへのナノ単位の加工精度を求める技術が求められるため非常に高額であり、利用期間が平均的に20年以上と長期間にわたる。装置ツールは、定期的なハードウェアの保守とともにOSやアプリケーションソフトウェアへのアップデートを行うことを基本とするが、装置ツールの中には、性能保証のためOSおよびアプリケーションソフトウェアの変更が制限されるもの、セキュリティパッチ適用対応ができないもの、連続稼働により適用タイミングが難しいものがある。<br>
ファブ内には新旧様々な装置ツールが混在し、以下のような特徴がある。
<table>
<tr><th colspan="4">装置ツールの特徴</th></tr>
<tr><td>1</td><td>管理台数が多い　１工場当たり数千台、現場のデジタルツイン化により今後も増加</td><td>6</td><td>装置ツールの性能上アクティブスキャンでシステム停止するものがある<br>アクティブスキャンでの脆弱性評価が難しい</td></tr>
<tr><td>2</td><td>装置ツール内のハード・ソフトウェア構成が複雑である<br>複数のフロントPC、DCS、PLC等のハードウェア構成と制御するソフトウェア構成がある</td><td>7</td><td>装置ツールの性能上ソフトウェアの追加ができないものがある（EPP/EDR）</td></tr>
<tr><td>3</td><td>１台の装置ツールから複数用途のネットワーク接続がある</td><td>8</td><td>装置ツールの性能上パッチ適用できないものがある</td></tr>
<tr><td>4</td><td>装置内のフロントPCには汎用OSが利用される（Windows/Linux）</td><td>9</td><td>装置ツールがレガシーOSとなりパッチ適用できできないものがある</td></tr>
<tr><td>5</td><td>装置システム間・装置間の通信には業界通信プロトコル（平文/未認証）が使われる<br>（GEM/SECS/HSMS）</td><td>10</td><td>パッチ適用作業時間が限られる（ライン停止時間が限定）</td></tr>
</table>
セキュリティ対策を行う上で考慮すべき観点<br>
ファブエリアの資産管理においては、管理対象台数となる装置ツール台数が大変多く、かつ個々の装置ツール内の構成は複数のハードウェアとソフトウェアが混在し複雑なため、脆弱性評価の視点での構成管理の対象範囲や収集・管理方法を定め、把握しモニタリングする必要がある。<br>
また、各資産への脆弱性評価およびセキュリティ対策を効果的に進めるためには、資産の重要度を分類し優先順位を付けることが必要である。<br>
例えば、半導体製品の品質や歩留まりに大きく影響を与える検査工程の装置ツールの重要性や、各工程の装置ツール内に保管される生産レシピなどの生産機密情報の漏洩影響の大きさなどより資産の重要度を予め分類し、優先度をつけた脆弱性評価やセキュリティ対策に繋げることが効果的である。<br>
脆弱性評価では、装置ツールの性能や運用における制約をもとに実施された追加対策（多層防御やマイクロセグメンテーション）をふくめ、生産の可用性に対して行う必要がある。生産の可用性に対する脆弱性評価の手法としては、CVSSによる定量評価だけではなく、SSVC等の生産可用性に対する対応優先を用いた評価についても検討を行う必要がある。<br>
具体的な対策事例<br>
対策検討を進めるうえで、参考となる具体的な事例を4.1に示す
</td></tr>
</table>

# ガイドラインの構成

## 3. 半導体デバイス工場の特徴とリスク源及び関連フレームワークの対策項目の整理⑥

### リスク分析のための情報（例：装置ツールの資産管理と脆弱性評価②）

| CPSF 想定されるセキュリティインシデント/リスク源<br>（脅威・脆弱性・脆弱性ID） | 関連する NIST CSF2.0 半導体製造プロファイル　及び　CPSF |
|---|---|
| **想定されるセキュリティインシデント**：<br>• 自組織で管理している領域において保護すべきデータが改ざんされる<br>• 遠隔から機器を管理するシステムに不正アクセスされ、機器に不正な入力をされることで事前に想定されていない動作をする<br><br>**脅威**：<br>• セキュリティ上の脆弱性を利用したマルウェア感染<br>• 機器を管理するシステムからIoT機器への不正なコマンド送信<br><br>**脆弱性**：<br>• 自組織の情報システムや産業用制御システムに接続している機器の状態を把握できていない<br>• 脆弱性情報、脅威情報を収集・分析し、適切に対応していない。<br>• 情報システムや産業用制御システムに接続している自組織のIoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない<br>• 自組織のシステムにおいて、対処すべき脆弱性が放置されている<br>• システムにおいて対処すべき脆弱性が適切に対処されていない<br><br>**対象となる構成要素**<br>•　モノ：装置ツール<br><br>**【CPSF脆弱性ID】**<br>•　L1_1_a_SYS<br>•　L1_1_b_COM<br>•　L2_1_a_ORG<br>•　L2_1_b_ORG<br>•　L2_1_c_SYS<br>•　L2_1_c_ORG<br>•　L3_1_a_SYS | **【NIST CSF2.0 半導体製造プロファイル】**<br>• ID.AM-01　ハードウェア管理　Fab：攻撃対象インタフェースの資産を抽出<br>• ID.AM-02　ソフトウェア管理<br>• ID.AM-04　サービス管理<br>• ID.AM-05　資産の重要度　Fab：ビジネス影響を及ぼす重要資産の判断<br>• ID.AM-08　資産のライフサイクル管理　Fab：レガシー資産と最新資産の融合運用<br>• ID.RA-01　脆弱性評価　Fab：大量・複雑な資産の脆弱性評価<br>• ID.RA-02　脅威インテリジェンス収集　Fab：OT脅威インテリジェンスの収集<br>• ID.RA-03　脅威識別<br>• ID.RA-04　脅威の発生可能性と影響　Fab：連続稼働におけるビジネス影響判断<br>• ID.RA-05　脅威の優先順位付け　Fab：リスク評価の実施<br>• ID.RA-06　リスク対応の計画と実施　Fab：リスク対応の計画と実施<br>• ID.RA-07　変更管理　Fab：変更管理<br>• ID.RA-08　脆弱性開示プロセス　Fab：脆弱性開示プロセスの確立<br><br>**【CPSF対策要件ID】**<br>•CPS.AM-1<br>•CPS.AM-5<br>•CPS.AM-6<br>•CPS.RA全て<br><br>**【SEMI E187製造リファレンス】**<br>3.4 Vulnerability/Threat Assessment and Patch Management<br><br>ファブネットワークに接続されるアセットに対して、リアルタイムな不正な動きの検知、パッチ適用等、セキュリティ脅威を低減する方法について記載 |

# ガイドラインの構成　４．半導体デバイス工場における具体的対策事例

## 半導体デバイス工場における具体的対策例

半導体デバイス工場で対策検討を進める上で、参考となる以下の４つの具体的対策事例を示す

| 具体的対策事例 | |
|---|---|
| 4.1 | 装置ツールの資産管理と脆弱性評価（3.2.1 - ①） |
| 4.2 | 装置ツールの被害の極小化と早期復旧を備えた追加防御対策（3.2.1 - ②） |
| 4.3 | 運用（監視・対応・復旧・改善） - FSIRTによる運用（3.2.3 - ⑥） |
| 4.4 | 物理アクセスの制限（入室・持ち込み・接続） - ファブエリアにおける物理的対策（3.2.1 - ⑤） |

# ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価①

- 半導体デバイス工場におけるOT領域ファブエリアは、1工場で2千台以上と非常に多くの装置ツールが、クリーンルーム環境の中でシステム・装置間を自動連携しながら連続生産を行っている。
  **工場で守るべき生産目標、半導体品質の維持、生産機密情報の保護、人命・環境の維持を実現するには、このファブエリアにある大量の装置ツールの資産を漏れなく洗い出し、管理する必要がある。想定被害から重要度を設定することで、効率的な対策を行うことができる。資産に対する脆弱性と脅威情報の把握を行い、評価と対応優先度を決める必要がある。**

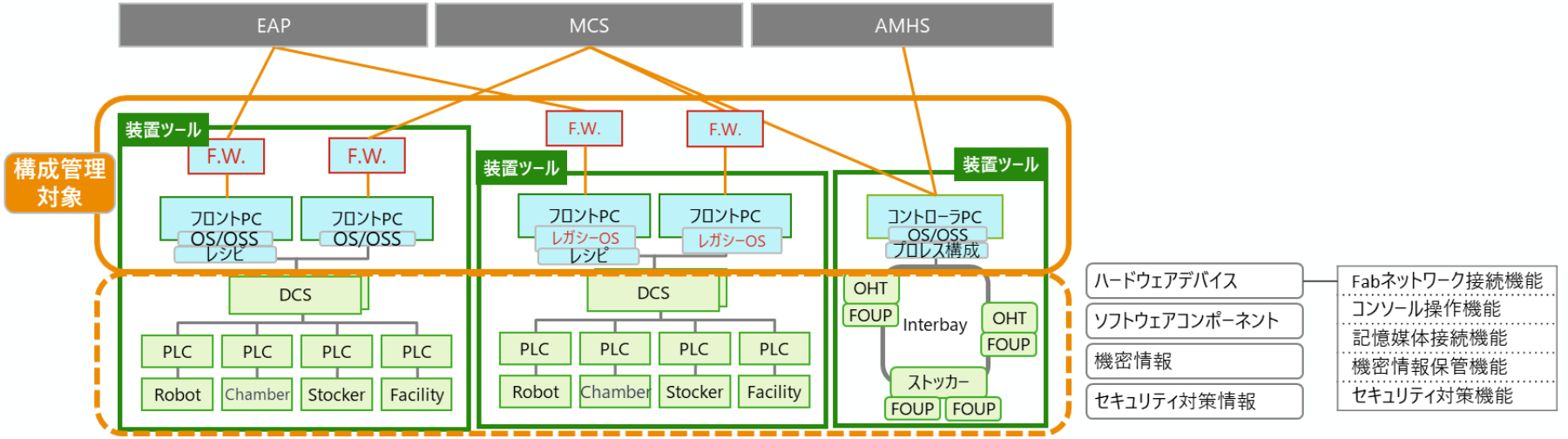
- 装置ツールの資産は、複数のハードウェアデバイス、ソフトウェアコンポーネントで構成され複雑である。一方で発見される脆弱性は年間4万件を超えるため、装置ツールにおける資産管理と脆弱性評価は効率的に行う必要がある。
  以下の5つに分けて具体的な対策事例を示す。

| | | |
|---|---|---|
| 資産管理 | 資産（装置ツール）の洗い出し･構成管理の定め方 | 全自動プロセス型連続生産のため工場で管理する資産数が多く構成も複雑、重要度による重みづけで分類 |
| | 資産（装置ツール）の重要度の決め方 | |
| 脆弱性評価 | 装置ツールの脆弱性の把握方法 | 大量の資産に対する、脆弱性の状況把握を行い評価を実施する<br>脆弱性の発見件数も年々増加しているため、効果的な評価方法と対応優先度の決め方を示す |
| | 装置ツールに対する脅威情報の収集方法 | |
| | 装置ツールに対する脆弱性評価と対応優先度の決め方 | |

# ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価②

## 資産（装置ツール）の洗い出し・構成管理の定め方

- ハードウェアデバイスは、装置ツール内のファブネットワークへの接続機能、コンソール操作機能、記憶媒体接続機能、機密情報保管機能、セキュリティ対策機能のいずれかの機能をもつハードウェアデバイスを対象とする。装置ツール内のフロントPCやコントローラPC、装置内のファブネットワークに接続されるファイア・ウォール等が基本的な管理対象となるが、上記の機能をもつDCS、PLC等のハードウェアも保守メンテナンスによるサイバーリスクを考慮し管理対象とする。
- ソフトウェアコンポーネントは、装置ツール内で対象としたハードウェアデバイスのOSやOSSを管理範囲とする。『SEMI E187』の「7 Computer Operation System Security Requirement」のセキュリティ要件により装置メーカーから提供されるソフトウェアの互換性、ソフトウェアパッケージの依存関係の情報を管理対象とする。
- 機密情報は、装置ツール内に保管される生産機密情報を対象とする。設計回路情報や製造レシピ、プロセス構成等が管理対象となる。
- セキュリティ対策情報は、装置ツール本体に対してSEMI E187のベースライン要件の適用状況を対象とする。SEMI E187のベースライン要件では、パッチ適用条件、マルウェア対策、アクセス制御、ネットワーク管理、セキュリティモニター等、脆弱性の評価を効率的に行うための要件項目を管理対象とする。



# ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価③

## 資産（装置ツール）の重要度の決め方

- 半導体デバイス工場がサイバー攻撃の被害に備えるためには、守るべき資産を明確にし、被害が発生した場合に事業にどのような影響が発生し、どれほど深刻な事態になるのかを吟味した上で、資産の重要度をあらかじめ定める必要がある。
  **定めた資産の重要度を優先順位として活用することで、効率的なリスク評価や防御対策、脆弱性評価、さらには運用対応の実施が可能となる。**

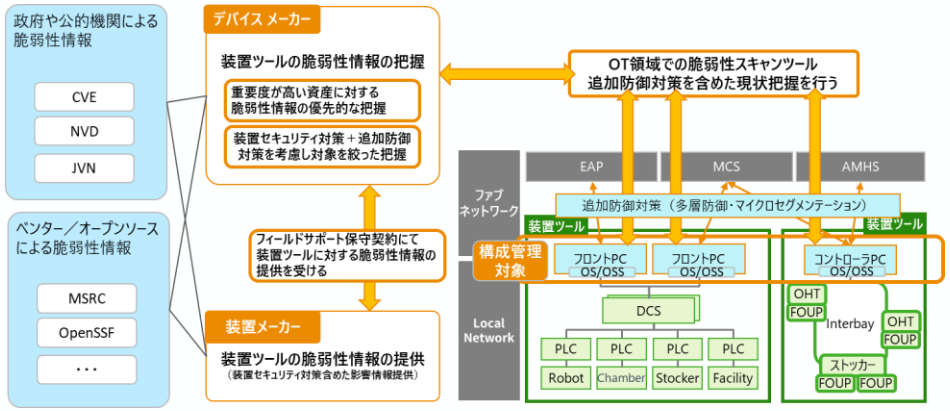
| リスク領域 | その資産がサイバー攻撃を受けることによって想定される事業被害・事業継続性の影響 | | | | | | | システム資産としての価値 | |
|---|---|---|---|---|---|---|---|---|---|
| | 事業継続性（可用性） | | 半導体品質（完全性） | | 産業活動の安全性（HES） | | 法規制等の遵守 | 情報漏洩（機密性） | 財務影響 |
| 重要度 | 生産停止 | 供給影響 | 歩留まり影響 | 市場品質影響 | 労災事故 | 環境被害 | | 生産機密情報の漏洩 | 装置ツールの破損 |
| 高 | 1日以上 | 7日以上 | 歩留まり率50%を下回る影響 | 市場品質不良影響あり・PL法影響あり | 死亡 | 重大な地域のインシデント | 政府の規制や業界の標準に重大な違反による厳重な監視や制約 | 競争優位性に影響を与える収益の5%以上の損失 | |
| 中 | 1時間以上 | 2日以上 | 歩留まり率50～70%となる影響 | 市場品質不良影響あり・PL法影響なし | 休職または重傷 | 苦情または地域社会への影響 | 政府の規制や業界の標準に重大な違反による監視 | 競争優位性に影響を与える収益の1～5%の損失 | |
| 低 | 1時間未満 | 1日未満 | 歩留まり率70%以上 | 市場品質不良影響なし | 応急手当または記録すべき怪我 | 苦情なし | 法令順守に影響を及ぼす可能性はない | 競争優位性の影響はなし収益上の影響はない | |

# ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価④

## 装置ツールの脆弱性の把握方法

### 脆弱情報の入手先

- 政府や公的機関であるCVE、NVD、JVN等の脆弱性公表情報からの把握
- セキュリティベンダー情報（MSRC等）、オープンソース情報（OpenSSF等）からの把握
- 装置メーカーからの脆弱性提供情報による把握
- 脆弱性スキャンツール（SCAPスキャナー）を利用した把握



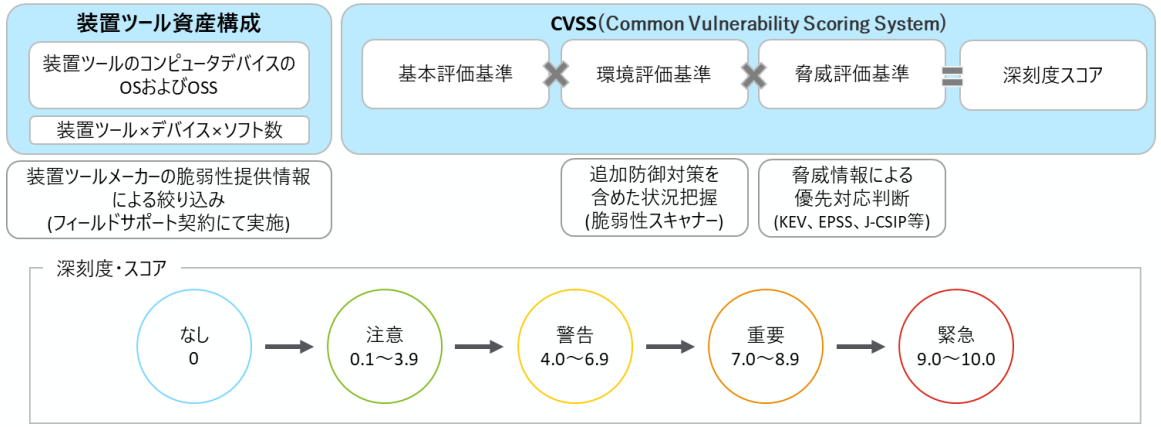

## 装置ツールに対する脅威情報の収集方法

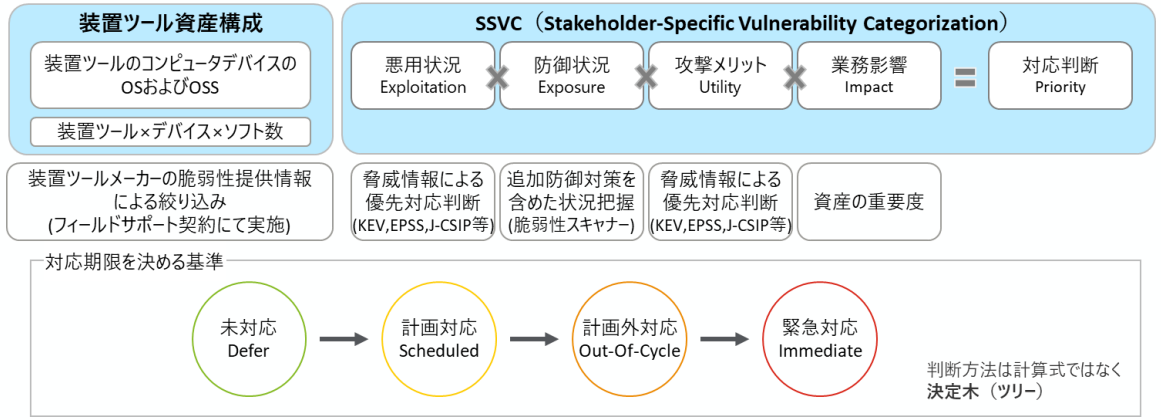
### 脅威情報の収集方法

- 政府や公的機関であるNISC、JPCERT/CC、IPA、CISA、NISA、CERT-EUからの情報収集
- CISAの悪用が確認された脆弱性リストであるKEV、FIRSTの脆弱性の悪用確率の推測であるEPSSからの情報収集及び、KEVとEPSSを組み合わせたLEVの活用
- 業界の脅威情報共有であるIT-ISAC Semiconductor Industry SIG、J-CSIP半導体産業SIGからの情報収集
- 自社のアタック・インシデント情報の分析結果からの情報収集

## 装置ツールに対する脆弱性評価と対応優先度の決め方

装置ツールの脆弱性情報を入手した際には、弱点となる脆弱性の詳細を把握し、攻撃者による脅威を想定した上で、装置ツールに対する深刻度を把握し、対応方針（軽減・回避・保有）、対応時期等を判断することが求められる。
また、新たな脅威や環境変化（例：装置ツールの導入や変更）に応じて、既存資産と脆弱性の評価を動的に見直し、常に最新のリスク状況に基づいた対応判断を行うことが求められる。

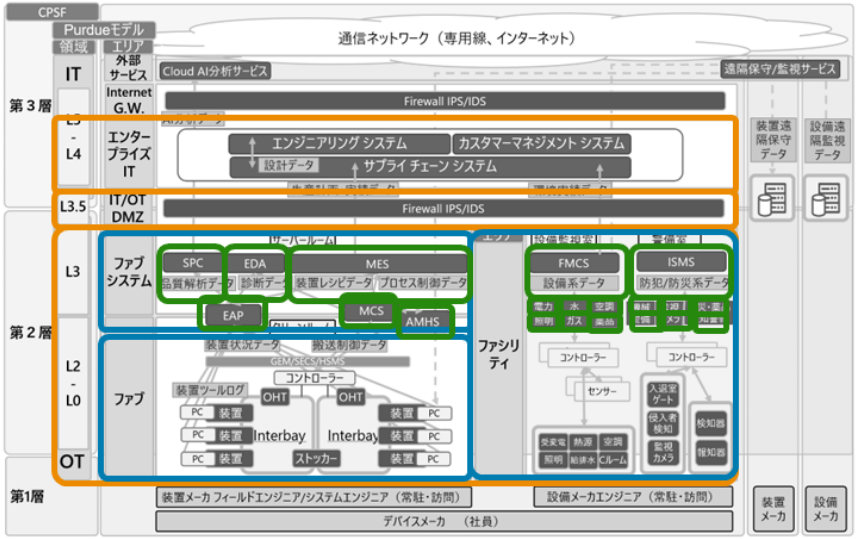


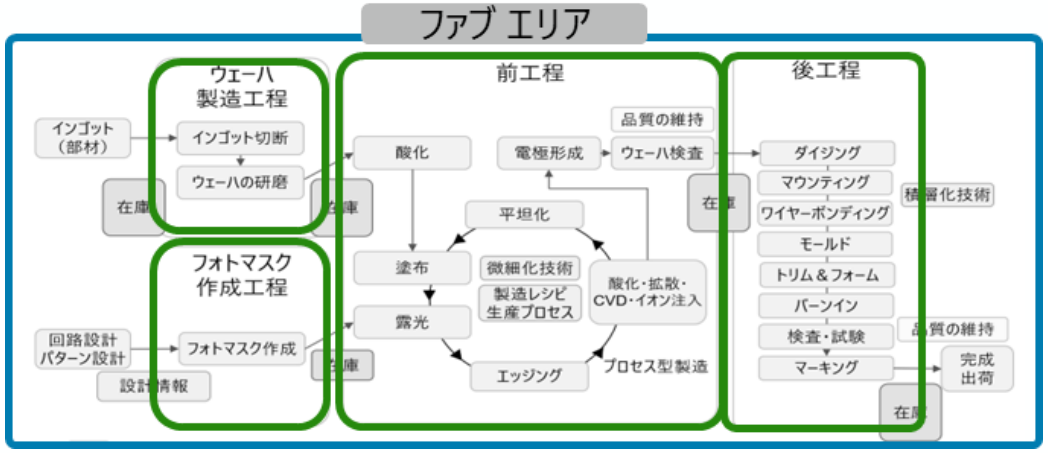



# ガイドラインの構成　4-2. 装置ツールの被害の極小化と早期復旧を備えた追加防御策①

- **生産継続に重要となる装置ツールおよびファブネットワークを安全に運用するために追加の防御対策が必要。**
  **安全に運用するための追加防御対策である多層防御、マイクロセグメンテーション、ネットワークによるセキュリティ監視について示す。**

| ネットワークによる多層防御、マイクロセグメンテーションとセキュリティ監視 | |
|---|---|
| 1 | **<u>OT領域の分離と通信制限</u>**<br>OT領域ネットワークは、IT領域のネットワークからファイアウォール等を用いてDMZを設けてネットワークを分離し通信制御を行う (OT領域はIT領域のネットワークやインターネットから分離された状態とする)　左下図のオレンジ枠箇所 |
| 2 | **<u>エリア毎のゾーン分割と通信制限</u>**<br>OT領域ネットワーク内では、ファブシステムエリア、ファブエリア、ファシリティエリアはエリアをネットワークを分割したうえ通信制限を行う<br>左下図の青色枠箇所 |
| 3 | **<u>エリア内でのゾーン分割と通信制限</u>**<br>ファブエリアについては、生産計画を行う工程単位でネットワークを分割して通信制限を行う（同じ工程でも、建屋、フロアー等にて生産計画が違う場合は分離）　右下図の緑色箇所<br>ファブシステムエリア内においてはシステム単位、ファシリティエリア内においては設備サービス単位でネットワークを分割して通信制限を行う<br>右下図の緑色枠箇所 |

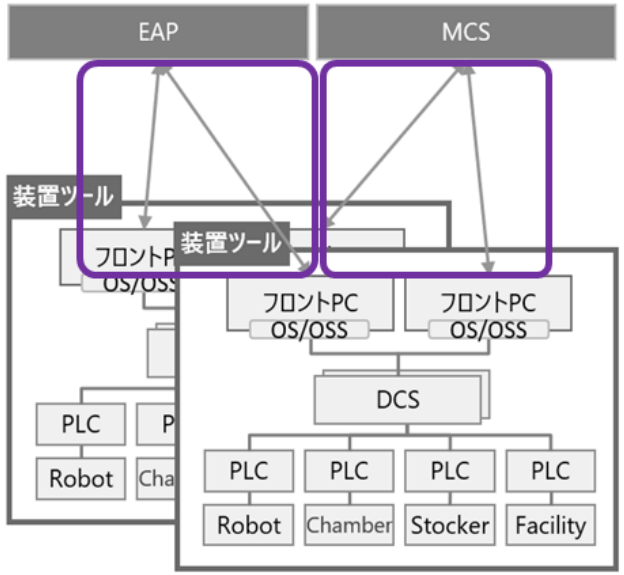


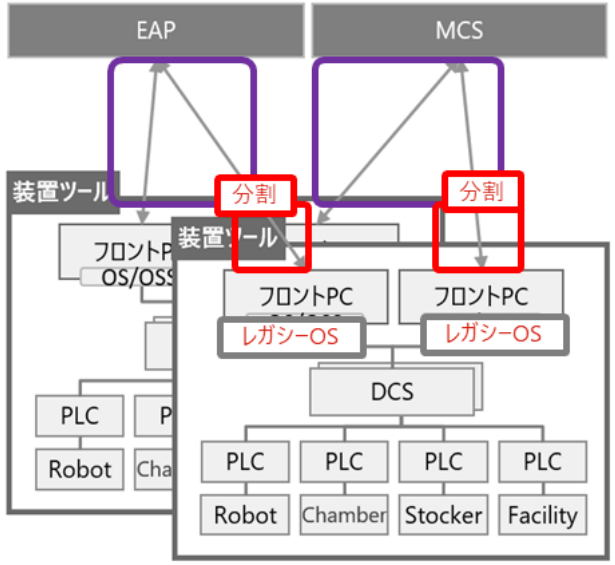



# ガイドラインの構成　4-2. 装置ツールの被害の極小化と早期復旧を備えた追加防御策②

- **生産継続に重要となる装置ツールおよびファブネットワークを安全に運用するために追加の防御対策が必要。**
  **安全に運用するための追加防御対策である多層防御、マイクロセグメンテーション、ネットワークによるセキュリティ監視について示す。**

| ネットワークによる多層防御、マイクロセグメンテーションとセキュリティ監視 | |
|---|---|
| 4 | **ファブエリア内システム用途別のゾーン分離と通信制限**<br>ファブエリア内で生産計画単位で分けられた中で、装置システム間のプロセス制御用途や、製品品質確認のための画像映像記録用途、故障予測検知用途などシステム用途別にネットワークをゾーン分割し通信制御を行う　左下図の紫枠箇所 |
| 5 | **装置ツールを守るマイクロセグメンテーション**<br>装置ツールにてレガシーOSの利用やパッチ適用できない等セキュリティ対策が行えないデバイスには、マイクロセグメンテーションによるゾーン分割を行う　右下図の赤枠箇所<br>さらに重要な装置ツールについては、仮想パッチ適用の検討を行う |
| 6 | **ネットワークによるセキュリティ監視**<br>分割した各ネットワークへは異常検知ツール（NDR）を導入し、異常アラートのログの記録保管および監視検知を行う |

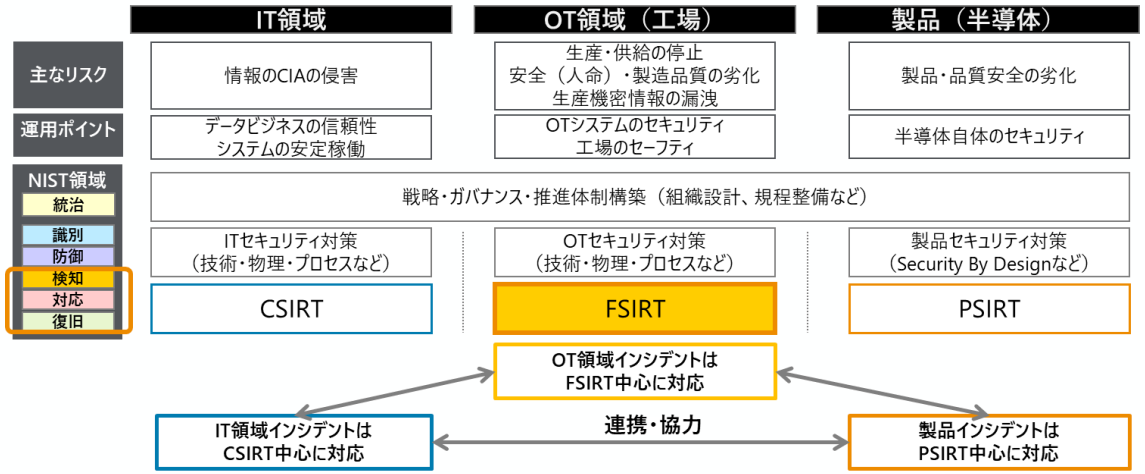


# ガイドラインの構成　4-3. 運用（監視・対応・復旧・改善）　- FSIRTによる運用①

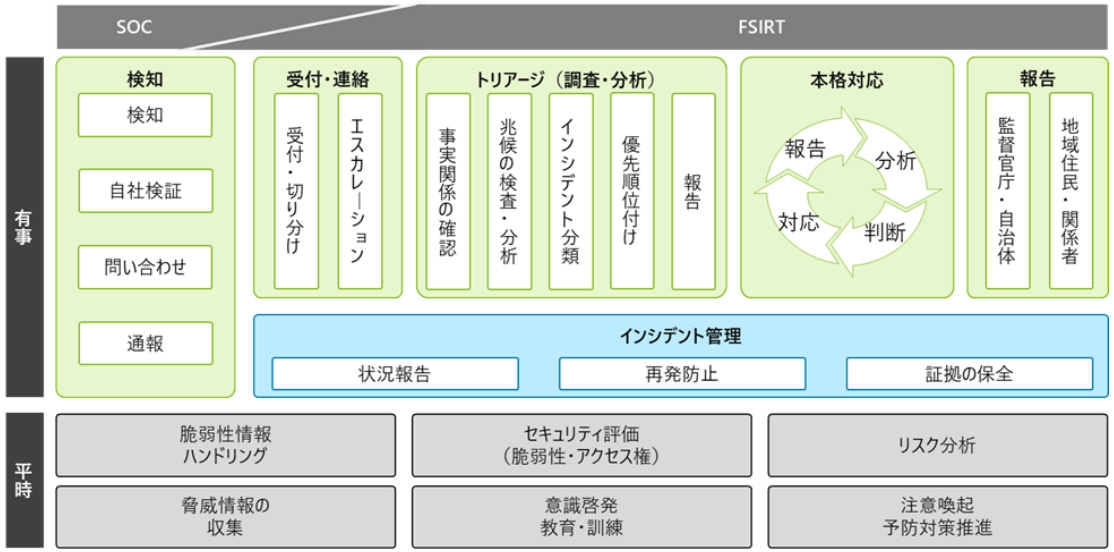
## 半導体デバイス工場でのFSIRTの事例

- **半導体デバイス工場を安全に運営し、半導体を安定的に供給するためには、自社のリスクを明確化し、計画的に対策を進めるとともに、サイバー攻撃の有事の対応を想定して、安全管理に必要な体制の構築が必要である。**
  工場OT領域においてサイバー攻撃の検知・対応・復旧を担う、半導体デバイス工場でのFSIRTの事例を示す。




## FSIRTの有事および平時の対応

- **FSIRTでは、サイバー攻撃の検知をした際の有事対応を行える体制と運用を整備するとともに、平時からの備えも準備しておく必要がある。**
  工場で発生するインシデントに対して、FSIRTでは早期に対応し、被害の拡大を防止するための措置を講じる。被害の発生が確認された場合、エスカレーションを行い、顧客や取引先等のサプライチェーン関係者が通常生産稼働できる状態に早期復旧を図る必要がある。



# ガイドラインの構成

## 4-4. 物理アクセスの制限（入室・持ち込み・継続） - ファブエリアにおける物理対策

- **半導体デバイス工場の生産現場であるファブエリアは、クリーンルームとして分離されているが、攻撃者にとって物理的な侵入口として狙われやすい。ファブエリアの特徴を改めて示して整理するとともに、物理セキュリティ対策の事例を示す。**

| 物理的侵入攻撃のポイント | ファブエリアの特徴 | 対策例 |
|---|---|---|
| • OT領域への不正侵入 | • ファブエリアであるクリーンルームには、顔見知りではなく識別が困難である多くの人員が出入りする<br>• 装置ツールを管理する社員とともに、様々な装置メーカーの業務委託の保守員が入室する<br>• 24時間／7日間の連続稼働のため、交代勤務者含めた社員および業務委託の保守員が対象者となる<br>• 装置メーカーの業務委託による保守員は、常駐者・訪問者が混在する<br>• クリールーム内作業のため全身クリーンスーツを着用しており、視覚情報（目視・映像記録）による個人識別が困難である | • 工場への入門・訪問管理<br>• ファブエリアへの入退室許可制限（社員、常駐者、訪問者）<br>• 訪問者への常時付き添い |
| • 装置ツールへの不正操作 | • ファブエリア内は、大フロアーで同一レイアウトの中に、多くの人員が出入りし重要資産に区分される装置ツールが数多く混在しコンソールへのアクセスが容易である | • 装置ツールでのコンソールログイン認証強化<br>• 訪問者の常時付き添い |
| • 装置ツールへの不正デバイス接続 | • 装置ツールの故障修理・不具合改善を行う保守業務にて、ファブエリアへデバイスの持ち込みが発生する<br>• 装置ツールに対して、保守用外部記憶媒体デバイスや保守用PCの接続、ソフトウェアコンポーネントの入替、装置ツール内のストレージ部品含めた保守交換を実施する | • コンピュータデバイスの持ち込み制限<br>• ストレージ保有デバイスの持ち込み制限<br>• 装置ツールでのインターフェイスポートの物理・論理的保護（ポートロック） |
| • 持込機器の不正ネットワーク接続 | • ファブエリア内のネットワーク通信プロトコルは、業界標準で定められた平文／未認証プロトコルを利用しており、容易な通信解読・改ざんが可能である | • コンピュータデバイスの持ち込み制限<br>• ネットワークケーブル、ネットワーク機器接続ポート、無線アクセス接続の物理・論理的保護 |
| • 持込機器の妨害電波発信 | • 自動搬送機は無線通信による制御が行われており、利用する無線周波数が管理されている | • 無線電波発信デバイスの持ち込み制限 |
| • 持込機器の不正録画 | • ファブエリア内のプロセスの工程編成、装置ツールの機種情報や台数規模などのファブエリア内レイアウトの視覚情報も生産機密情報である | • 録画機能デバイスの持ち込み制限 |
| • 装置ツールの破壊・窃盗 | • 装置ツールのストレージには、製造レシピ情報等の生産機密情報が含まれる | • 装置ツールの保守交換、撤去時における生産機密情報の確実な消去確認 |


METI
Ministry of Economy, Trade and Industry