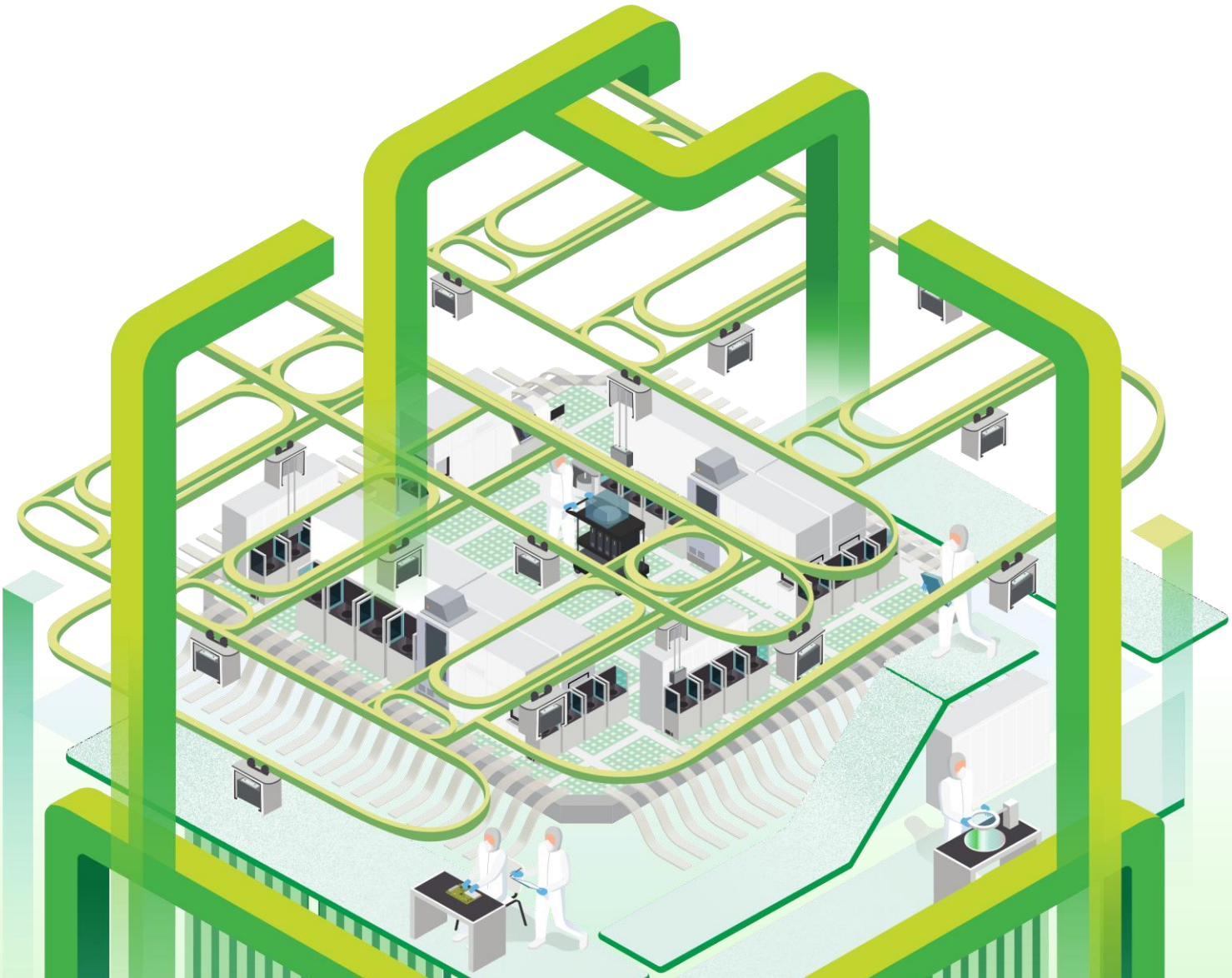
半導体デバイス工場における
OT セキュリティガイドライン

Ver 1.0



令和 7 年 10 月 24 日

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（実効性強化・国際連携）
半導体産業サブワーキンググループ

変更履歴

発行日	版	概要
2025年10月24日	Ver1.0	Ver1.0 発行

目次

1　本ガイドライン作成の背景と目的 1

1.1　背景と目的 1
1.2　ガイドラインの対象者(想定読者) 2
1.3　半導体製造においてサイバー攻撃から守るべき対象 3
1.4　半導体製造工程における脅威とリスク 5
1.5　想定する攻撃主体 6
1.6　半導体デバイス工場におけるセキュリティ対策と本ガイドラインの利活用 7
1.7　ガイドラインの構成 7

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 9

2.1　半導体デバイス工場のリファレンスアーキテクチャ 9
2.2　Purdue モデルの活用 12
2.3　CPSF 三層構造の活用 14

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 15

3.1　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 15
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 19

3.2.1　OT 領域ファブエリアのリスク分析のための情報 21
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 35
3.2.3　OT 領域の外部サービス及び IT/OT DMZ 分類制御のリスク分析のための情報 39

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 44

4　半導体デバイス工場における具体的対策例 53

4.1　装置ツールの資産管理と脆弱性評価 53

4.1.1　資産(装置ツール)の洗い出し・構成管理の定め方 54
4.1.2　資産(装置ツール)の重要度の決め方 56
4.1.3　装置ツールの脆弱性の把握方法 62
4.1.4　装置ツールに対する脅威情報の収集方法 63
4.1.5　装置ツールに対する脆弱性評価と対策優先度の決め方 65

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 66
4.3　運用(監視・対応・復旧・改善) - FSIRT による運用 71
4.4　物理アクセスの制限(入室・持込み・接続) - ファブエリアにおける物理的対策 80

Appendix A:NIST CSF2.0 と CPSF の対応表 83
Appendix B:用語/略語 100
本ガイドラインの検討体制 109

1 本ガイドライン作成の背景と目的

1.1 背景と目的

半導体産業の発展と国内投資の促進に向けて：

80 年代に世界シェア首位となり『日の丸半導体』と呼ばれた半導体産業の競争力を取り戻し、成長分野としていくことは最も重要な産業振興策の1つであり、それによって国内外からの投資を促進することが必要である。既に政府は 10 兆円規模の支援を行う意向を表明しており、高度なロジック半導体の開発を進めているところである。

安全保障の側面からみた半導体産業：

半導体は経済安全保障推進法の特定重要物資に指定された戦略物資の1つであり、高性能な半導体の安定供給は安全保障上の課題となっている。現代の兵器の製造や運用は半導体なしでは行えない。また、近年話題になっているハイブリッド戦争の観点では、実際の軍事行動以外の情報戦や認知戦と呼ばれる新しい領域において生成 AI を含む高度な IT システムが必須となり、大量のコンピュータリソースを必要とする。すなわち大量の半導体を必要とする。

サイバー攻撃の進化と半導体産業保護の重要性：

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。こうした動きは国内だけでなく海外でも始まっており、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[1]/E188[2]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）[3]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

[1] https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment
[2] https://store-us.semi.org/products/e18800-semi-e188-specification-for-malware-free-equipment-integration
[3] https://www.nist.gov/cyberframework

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、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、半導体デバイス工場は一般的にプロセスオートメーション（PA）型に近い特徴を持った工場であり、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。

1.2 ガイドラインの対象者（想定読者）

半導体製造は素材、設計、製造（前工程・後工程）等複雑なサプライチェーンによって成り立っているため、半導体の安定供給を維持するためにはこのサプライチェーン全体を保護する必要がある。従って半導体産業全体のサイバーセキュリティ対策の底上げを目指す必要がある。本ガイドラインでは、その最初の段階としてデバイスメーカーの工場を対象としたセキュリティ対策強化を目的とする。そのためまずデバイスメーカーの製造部門の方々を想定読者としているが、一方で我が国の半導体業界では製造装置メーカー、素材メーカーが多数存在することから、そうした各社に求められる要件や対策も想定できるようなガイドラインを目指している。

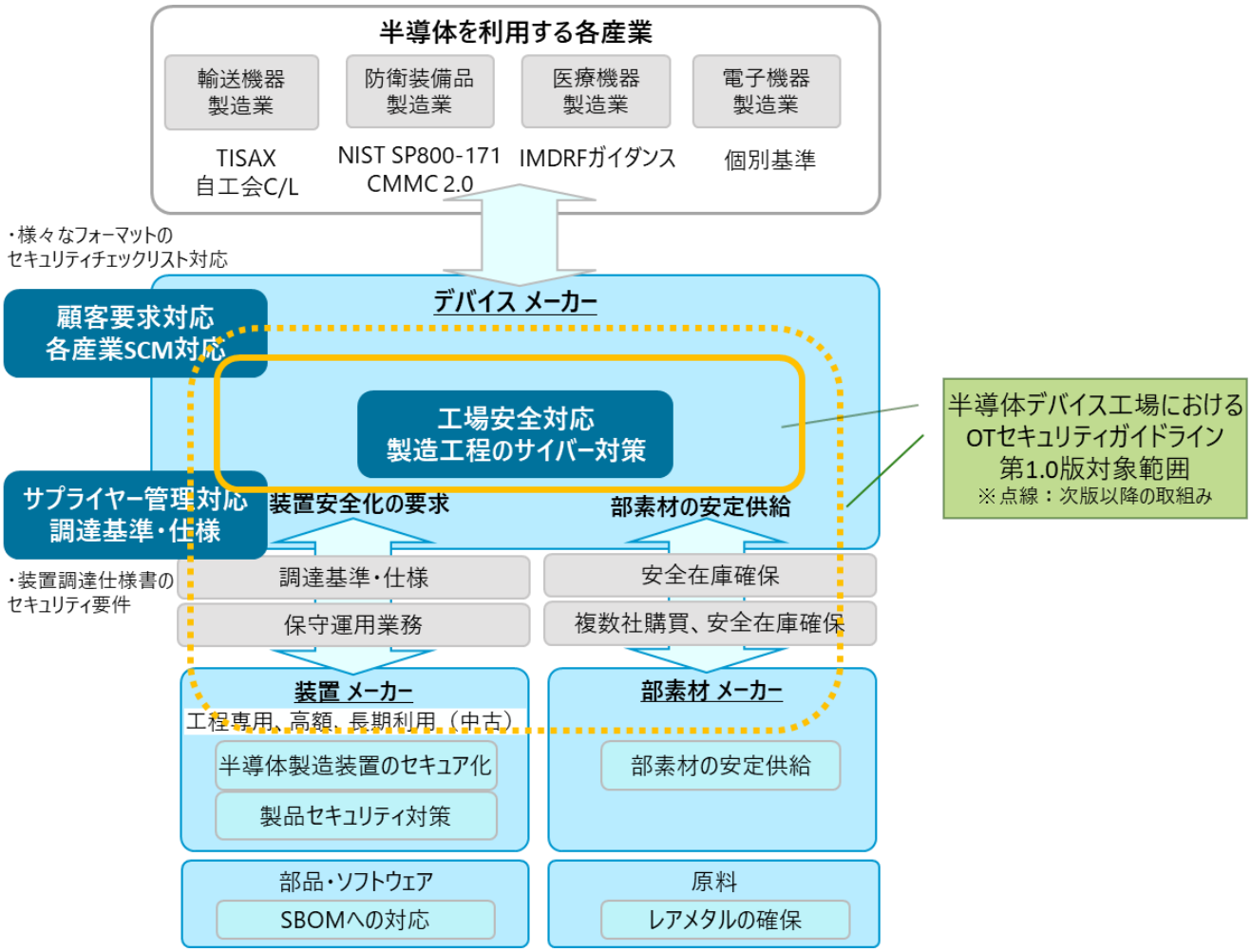


図 1-1. 半導体産業におけるサプライチェーン

1.3 半導体製造においてサイバー攻撃から守るべき対象

半導体の安定供給を実現するために守るべき対象として、NIST CSF2.0 半導体製造プロファイルでは以下の 5 つの項目が挙げられている。

- 生産目標の維持（供給責任）
  資産の損傷、ラインや装置の予定外の停止等、生産目標、スループット、歩留まりに悪影響を与える可能性のあるサイバーセキュリティリスクを管理する。サイバーセキュリティと本番環境の目標との間の相互依存性を理解する必要がある。
- 機密情報の保護
  組織の知的財産（IP）、半導体ファブ、OEM 機器、及びサプライチェーン全体の関連データ等、機密性の高いデータや規制対象のデータの損失や侵害につながる可能性のあるサイバーセキュリティ リスクを管理する。

- 半導体品質の維持
  製品やプロセスの品質に悪影響を与える可能性のあるサイバーセキュリティリスクを管理する。半導体製造プロセス、OEM 機器、及びサプライチェーン全体の関連データの整合性が維持されていることを確認する必要がある。
- 環境安全の維持
  偶発的または意図的な損害等、環境に悪影響を与える可能性のあるサイバーセキュリティリスクを管理する。サイバーセキュリティと環境安全性の相互依存性を理解する必要がある。
- 人間の安全の維持
  人間の安全に影響を与える可能性のあるサイバーセキュリティリスクを管理する。サイバーセキュリティと人間の安全との相互依存性を理解する必要がある。

本ガイドラインでは、経済安全保障を踏まえ、上記守るべき対象の中でも、特に、「生産目標の維持(供給責任)」「機密情報の保護」「半導体品質の維持」の 3 つに焦点をあてる。

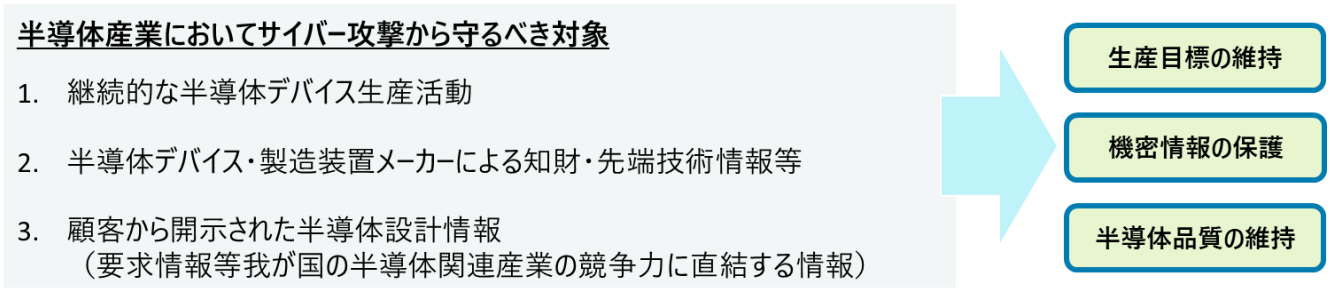


図 1-2. 半導体産業においてサイバー攻撃から守るべき対象

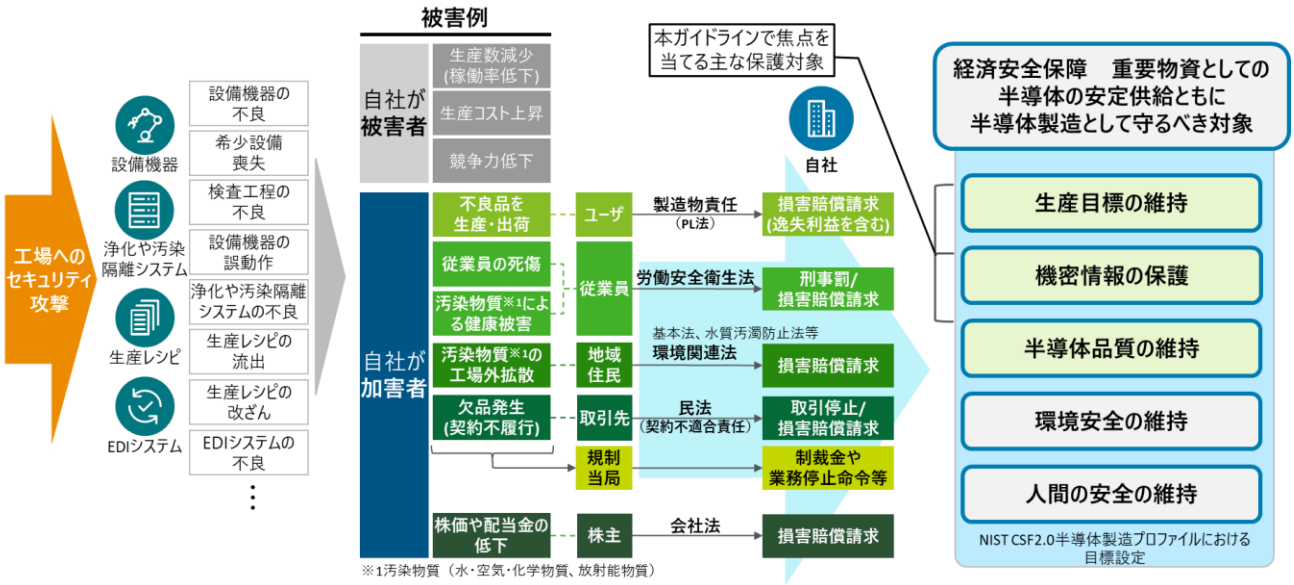


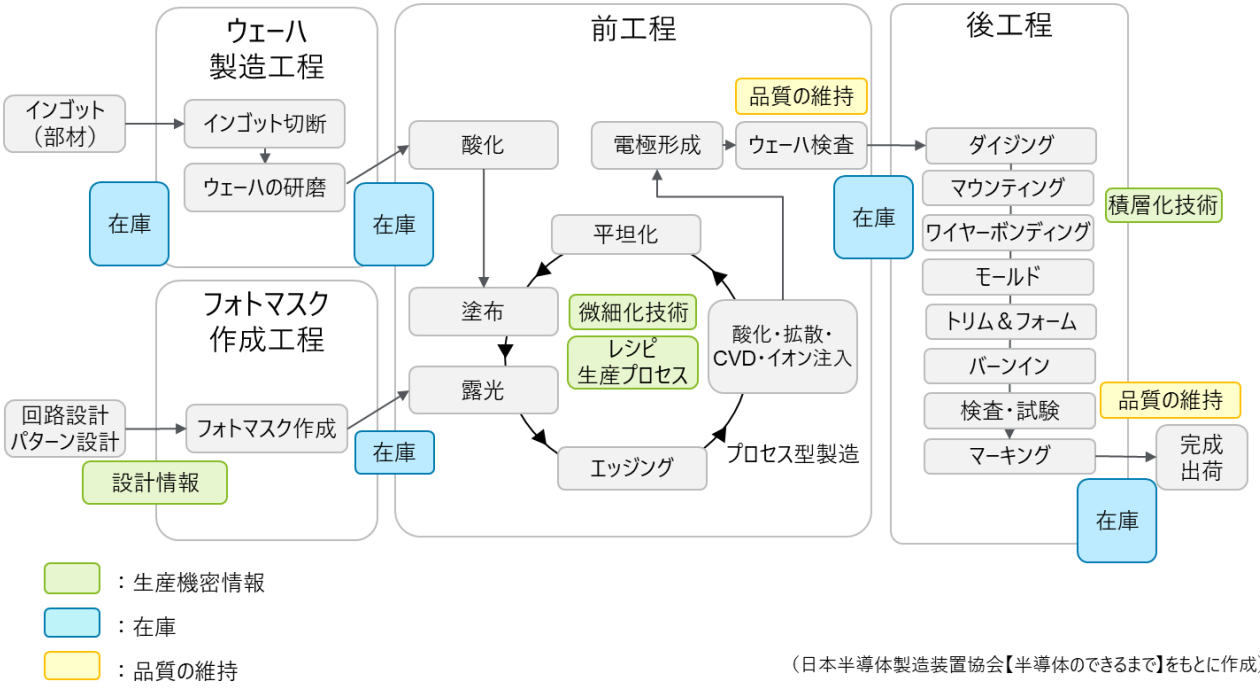
図 1-3. 半導体製造として守るべき対象

1.4 半導体製造工程における脅威とリスク

半導体デバイス工場における、製造工程は、「ウェーハ製造工程」「フォトマスク作成工程」「前工程」「後工程」と大きく 4 つに分けられる。各工程では、サイバー攻撃を受けて被害が発生すると、生産上の機密情報（以下、生産機密情報）の保護や供給責任を果たすうえでの大きなリスクとなる可能性がある。

生産機密情報としては、フォトマスク作成工程での設計情報、前工程での微細化技術、歩留まり向上に対するレシピ・生産プロセスの情報、後工程の積層化技術に対する生産技術情報等がある。これらの情報は機密性が非常に高く（図 1-4 緑色箇所「生産機密情報」）、侵害により知的財産が流出すると競合他社に対する開発競争等において不利な状況に陥るリスクがある。

通常、各工程の前後では各社が在庫を保有するなど、供給責任・事業継続計画（BCP）に基づいた安全在庫が考慮されている。サイバー攻撃による被害は各工程の安全在庫を超える生産停止を引き起こし、供給責任を果たせなくなるリスクがある（図 1-4 青色箇所「在庫」）。



（日本半導体製造装置協会【半導体のできるまで】をもとに作成）

図 1-4. 半導体製造工程

1.5 想定する攻撃主体

サイバー攻撃を行う主体は、一般的に以下の５つに分類され、攻撃者の種別により、攻撃技術のレベルが異なると考えられる。半導体産業全体のサプライチェーンはその安全保障上の重要性から、最も高度な攻撃者（下記①）を想定した対策レベルを実現する必要がある。（IEC62443 では SL4）

① 国家の支援を受けたグループ（APT（Advanced Persistent Threat）攻撃グループ）
執拗に高度で継続的な攻撃を行うことが特徴（ミッション達成優先でコスト度外視の攻撃集団）。

② サイバー犯罪組織（クライム系）
情報等を盗んで現金化するグループ。

③ ハクティビスト
「アクティビスト（社会活動家）」と「ハッカー」を掛け合わせた言葉で、サイバー攻撃を通じて社会的・政治的メッセージを発信していくことを主眼とした活動を行うグループ。

④ 悪意のある個人（愉快犯、腕試し等）
趣味や研究の延長として個人が行う攻撃で、子供が行っているケースも少なくない。

⑤ 産業スパイ
知的財産の窃取を目的とした攻撃グループ。

表 1-1. IEC62443 におけるセキュリティレベル（SL）

セキュリティ水準	定義
SL1	偶然または偶発的な侵害行為に対する保護
SL2	わずかな資源と一般的なスキルと低い動機を持ち、単純な方法を用いた意図的な侵害行為に対する保護
SL3	並みの資源と IACS※固有のスキルと並の動機を持ち、高度な方法を用いた意図的な侵害行為に対する保護
SL4	大規模な資源と、IACS 固有のスキルと高い動機を持ち、高度な方法を用いた意図的な侵害行為に対する保護

※IACS（Industrial Automation Control System：産業用自動制御システム）

1.6 半導体デバイス工場におけるセキュリティ対策と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、BCP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、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）[4]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。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』[5]が参考になる。

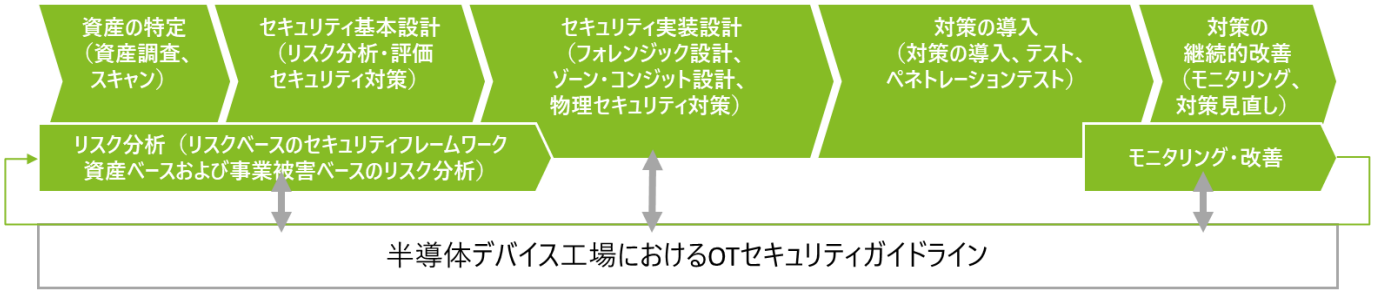


図 1-5. 半導体デバイス工場のセキュリティ構築プロセスにおける本ガイドラインの活用

1.7 ガイドラインの構成

本ガイドラインは、「CPSF」の考え方に基づいて半導体デバイス工場におけるリスク源を洗い出し、それらの対策について「NIST CSF2.0 半導体製造プロファイル（2025年2月27日公開、ドラフト版）」[6]及び「SEMI E187 半導体製造リファレンス」[7]の該当箇所を紐づける構成とする。

① IEC62443[8]のPurdueモデルを活用し半導体デバイス工場を領域・エ

[4] https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
[5] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
[6] https://csrc.nist.gov/pubs/ir/8546/ipd
[7] https://www.txone.com/blog/unveiling-semi-innovative-cybersecurity-architecture/
[8] https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards

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 2 章）。

② 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 3 章）。

③ 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（第 4 章）。

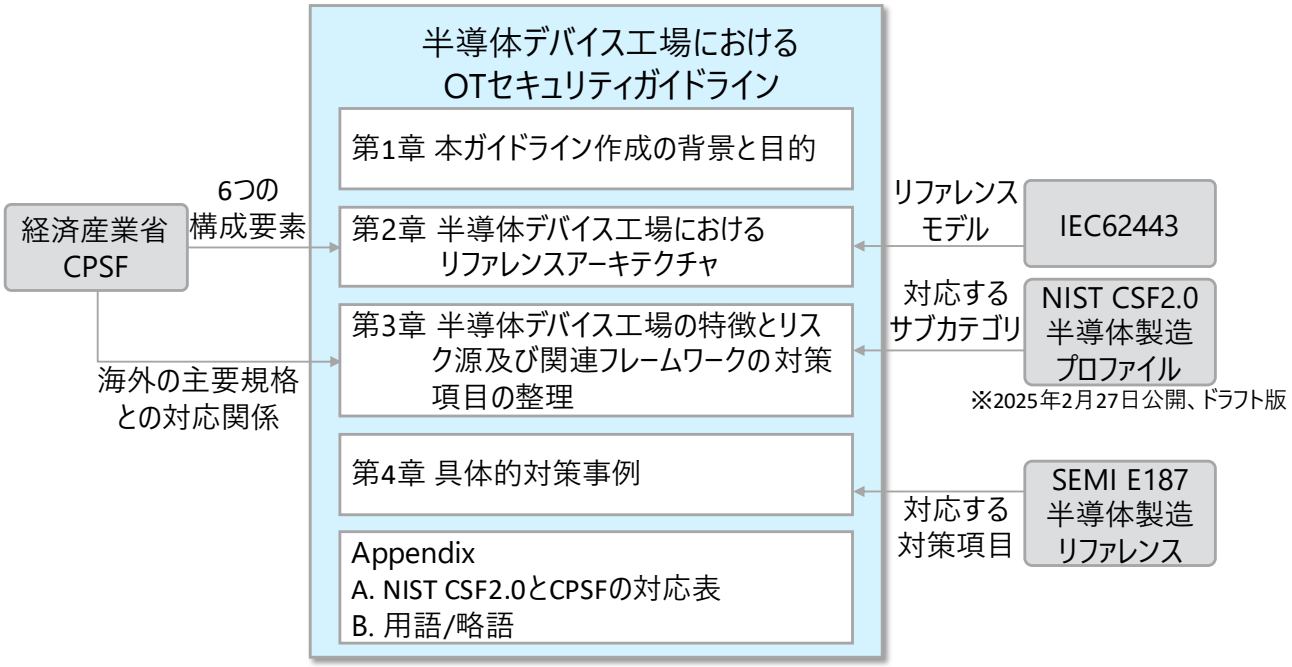


図 1-6. 本ガイドラインの構成及び国内外の標準規格との関係

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

2.1 半導体デバイス工場のリファレンスアーキテクチャ

第 2 章では、第 1.3 節にて整理した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、半導体デバイス工場のリファレンスアーキテクチャ（図 2-1、表 2-1）について説明する。

① 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した。具体的には、工場における主要なエリアを IT 領域、OT 領域及び IT/OT DMZ に分割し、各エリアに対してレベル（L）0ー4/5 の関連付けを行った。このセグメンテーションによりエリア毎のセキュリティ要件の整理がしやすくなる。

② 次に、半導体デバイス工場の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に CPSF を適用した。具体的には、半導体デバイス工場を CPSF の三層構造に分割し、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。

第 3 章では、この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基づき、半導体デバイス工場における特徴を踏まえた想定されるセキュリティインシデントとリスク源（脅威、脆弱性、脆弱性 ID）を洗い出し、それに対するセキュリティ対策として NIST CSF2.0 半導体製造プロファイルの該当項目を紐づけている。これにより、リスク源とその対策を NIST CSF2.0 半導体製造プロファイルに基づいて整理・検討することが可能となる。

なお、本リファレンスアーキテクチャは、代表的な半導体デバイス工場を想定した一例である。そのため、本ガイドラインを参考に、自社の工場におけるリファレンスアーキテクチャを整理し、工場における特徴やリスク源を明確にした上で、必要に応じて NIST CSF2.0 半導体製造プロファイルの該当項目の紐づけを実施する必要がある。

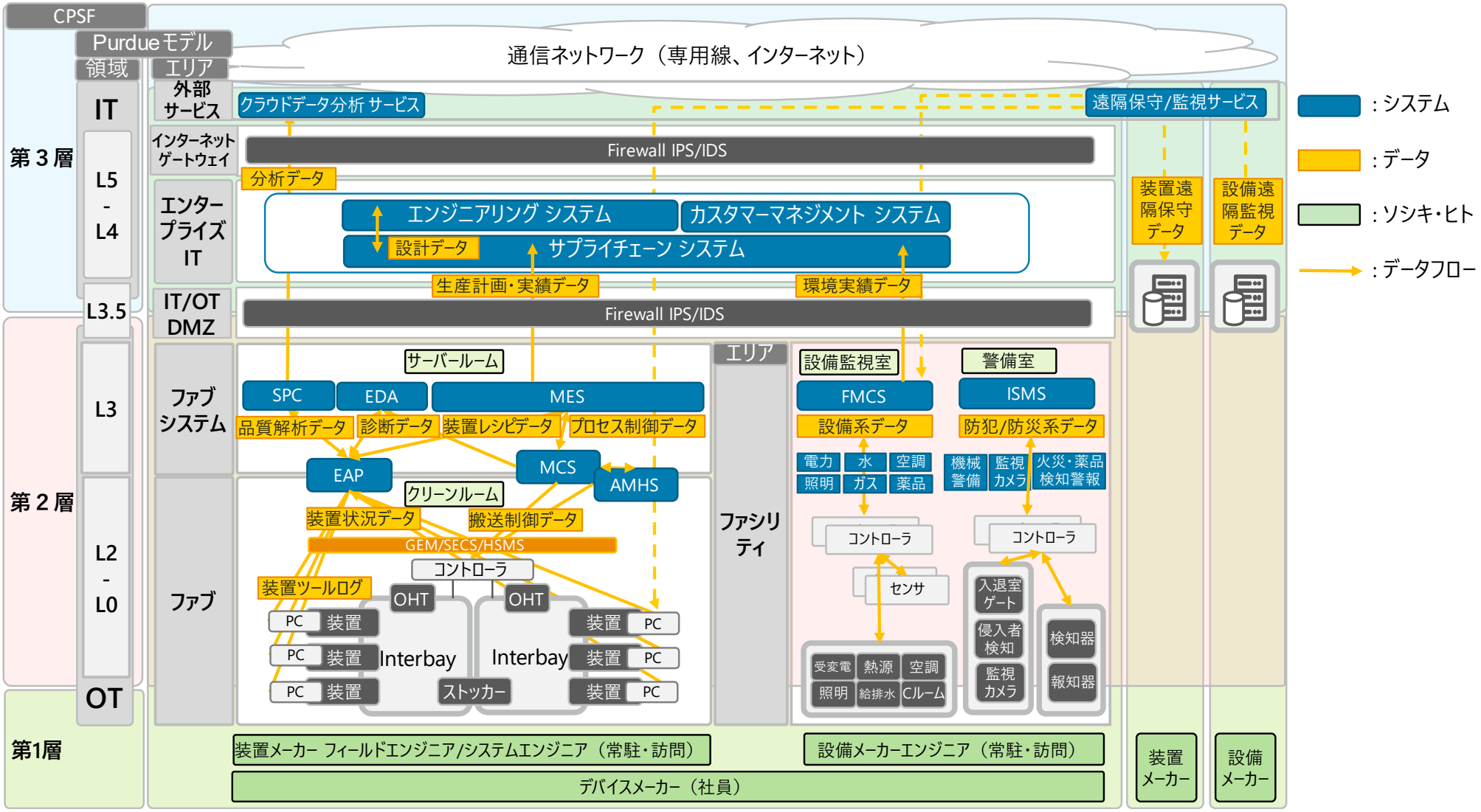


図 2-1. 半導体デバイス工場のリファレンスアーキテクチャ

表 2-1. Purdue モデルと CPSF による 6 つの構成要素

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
		遠隔監視保守サービス	遠隔監視保守データ				
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(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	SCM、ECM、CRM データ	サーバ、ネットワーク、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(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(L3)	MES	生産進捗データ	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	製造部門がセキュリティ含めた製造管理の中心(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
		SPC	品質特性・解析データ				
		EDA	装置収集・プロセス診断データ				
	ファブ(L0-2)	EAP	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)、OHT、OHS、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(フィールドエンジニア 常駐、オフィスあり)
		AMHS					
		MCS					
	ファシリティ(L0-3)	FMCS	設備データ、環境データ	各設備、コントローラ、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(電気、給排水、ガス、薬品各社 常駐、オフィスあり)
		ISMS	防犯データ、防災データ				

2.2 Purdue モデルの活用

Purdue モデルを用いて、半導体デバイス工場におけるセキュリティを以下の領域とエリアに分類する。

（1） 領域について

工場内は、エンタープライズ業務を行う IT 領域と生産業務を行う OT 領域に分けられる。また 2 つの領域間は DMZ で分離する。概要と機能は以下のとおりである。

- IT 領域(レベル 4-5)
  概要： オフィス業務として利用される機器(PC、スマホ、プリンター、サーバ等)が接続される領域。
  機能： 生産計画、調達、設計、販売、顧客管理等の基幹業務を行うシステムが含まれる。
  エリア：エンタープライズエリア、インターネットゲートウェイが IT 領域内に含まれる。
- OT 領域(レベル 0-3)
  概要： 装置ツールや製造・制御システム、ファシリティ設備等が接続される領域。
  機能： 装置ツールの制御、監視、データ収集、製造システムが含まれる。
  エリア：ファブシステムエリア(製造システム)、ファブエリア(装置ツール群)、ファシリティエリア(設備)の 3 つのエリアが OT 領域に含まれる。
- IT/OT DMZ(レベル 3.5)
  概要： IT 領域と OT 領域をファイア・ウォールで分離し、中継を行う領域。
  機能： セキュリティゲートウェイとして、両ゾーン間の通信を制御し、不正アクセスや攻撃から保護を行う。

（2） エリアについて

半導体デバイス工場における IT 領域、OT 領域を機能とセキュリティ要件に基づいて、以下のようにエリア分けを行った。OT 領域の各エリアについては、セキュリティ対策の特徴をあわせて記載している。

- IT 領域
  - インターネットゲートウェイ(レベル 5)
    概要：エンタープライズエリアとインターネット環境の通信制御を実施するゲートウェイ。

機能：クラウドデータ分析の通信許可、遠隔保守・支援のためのリモートアクセスの制御、インターネット側からの不正アクセスやサイバー攻撃の防御を行う。

- エンタープライズ IT エリア（レベル 4-5）

概要：従業者がオフィス業務を行うエリア。

機能：生産計画や調達のためのサプライチェーンシステム、回路設計を行うための EDA や CAD 等のエンジニアリングシステム、販売や顧客の管理等を行うカスタマーマネジメントシステム、等がある。

- OT 領域
  - ファブシステムエリア（レベル 3）

概要：製造全体のプロセスオートメーションを制御するシステムが属するエリア。

機能：MES はエンタープライズエリアにあるサプライチェーンシステムと生産計画・実績データ等を DMZ 経由で通信する。SPC はクラウド上のデータ分析を活用し、より速く正確な品質解析を行う。DX の進展に伴ってファブシステムエリアからインターネットへの通信が行われるケースも増加している。

セキュリティ対策：

IT 領域と同様のサーバ・システム対策を行うが、ファブシステムエリアの各システムは連続稼働を前提としているため、脆弱性評価やパッチ適用の運用が重要となる。

  - ファブエリア（レベル 0-2）

概要：高度に清浄なクリーンルーム環境内で、高度な技術を用いた装置ツール群が属するエリア。

機能：装置ツール群は EAP、MCS、AMHS 等の制御システムとリアルタイムな通信を行う。また、これらのシステムはファブシステムエリアにある MES、SPC、EDA とも通信を行う。

セキュリティ対策：

ファブエリアにある装置ツール群の特徴として、汎用 OS の長期間利用（開発元によるサポートが終了した後も使われ続ける）、暗号機能や認証機能を持たない通信プロトコルを業界規格として利用している、プロセスオートメーションによる装置ツール台数が多く、連続稼働するためパッチ適用の運用が容易ではない、等がある。

- ファシリティエリア(レベル 0-3)

  概要:工場ファシリティとして電気・水・ガス・薬剤等の各設備システム、監視カメラ・入退室管理等の防犯システムや火災検知等の防災システムが属するエリア。

  セキュリティ対策:

  一般的なビル管理システムと類似した課題(長期利用、マルチステークホルダー等)となり同様の対策が必要となる。

2.3 CPSF 三層構造の活用

半導体デバイス工場における CPSF の三層構造は、企業間、フィジカル・サイバー空間、及びサイバー空間におけるつながりを示している。

- 第 1 層(図 2-1 グリーン)

  半導体デバイス工場を中心とした、企業間(ソシキ・ヒト)のつながりを示している。

  デバイス工場のファブで使われる装置ツールやファシリティ設備を支える装置メーカーや設備メーカー、工場で常駐保守や訪問保守を行うフィールドエンジニアを記載している。
- 第 2 層(図 2-1 ピンク)

  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を示している。

  半導体デバイス工場の OT 領域ファブエリアに設置された各装置ツール群から MES 等ファブシステムへのつながり、ファシリティエリアにおける各設備内のセンサやコントローラのつながり、ファブシステムエリア及びファシリティエリアから IT/OT DMZ を通じた IT 領域へのシステム及びデータのつながりを記載している。
- 第 3 層(図 2-1 水色)

  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を示している。

  クラウドデータ分析サービスの利用や、装置メーカーによる e-Diagnostics 技術を用いた遠隔診断サービス等を記載している。

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

3.1 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

第 3 章では、第 2 章で定義した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想定されるセキュリティインシデントとリスク源（脅威、脆弱性、脆弱性 ID）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について取りまとめている。

第 3 章の内容は 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及び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。

① 半導体デバイス工場のリファレンスアーキテクチャで整理した CPSF の 6 つの構成要素に対して特徴を洗い出し、セキュリティ対策を検討する上で考慮する観点を整理

② CPSF のフレームワークを活用して、①で洗い出した考慮すべき観点より、想定されるセキュリティインシデントとリスク源（脅威、脆弱性、脆弱性 ID）を整理

③ CPSF の海外主要規格との対応関係等に基づき、②で整理した脆弱性から、関連する CPSF の対策要件 ID、NIST CSF2.0 半導体製造プロファイルのサブカテゴリ、及び SEMI E187 製造リファレンスの該当箇所を抽出

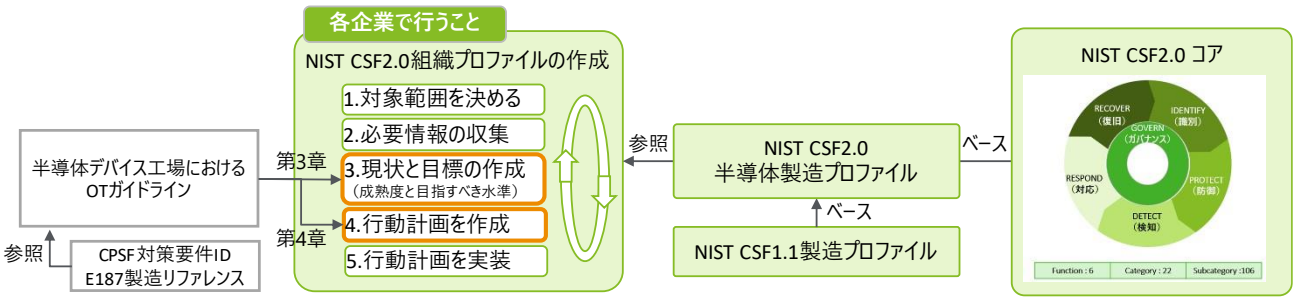


図 3-1. 本ガイドラインの活用方法

第 3 章で実施する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。

また、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改定にて対象とする予定である。

第 3.2 節「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」及び、第 3.3 節「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」に記載するリスク分析の詳細を図 3-2 に示す。

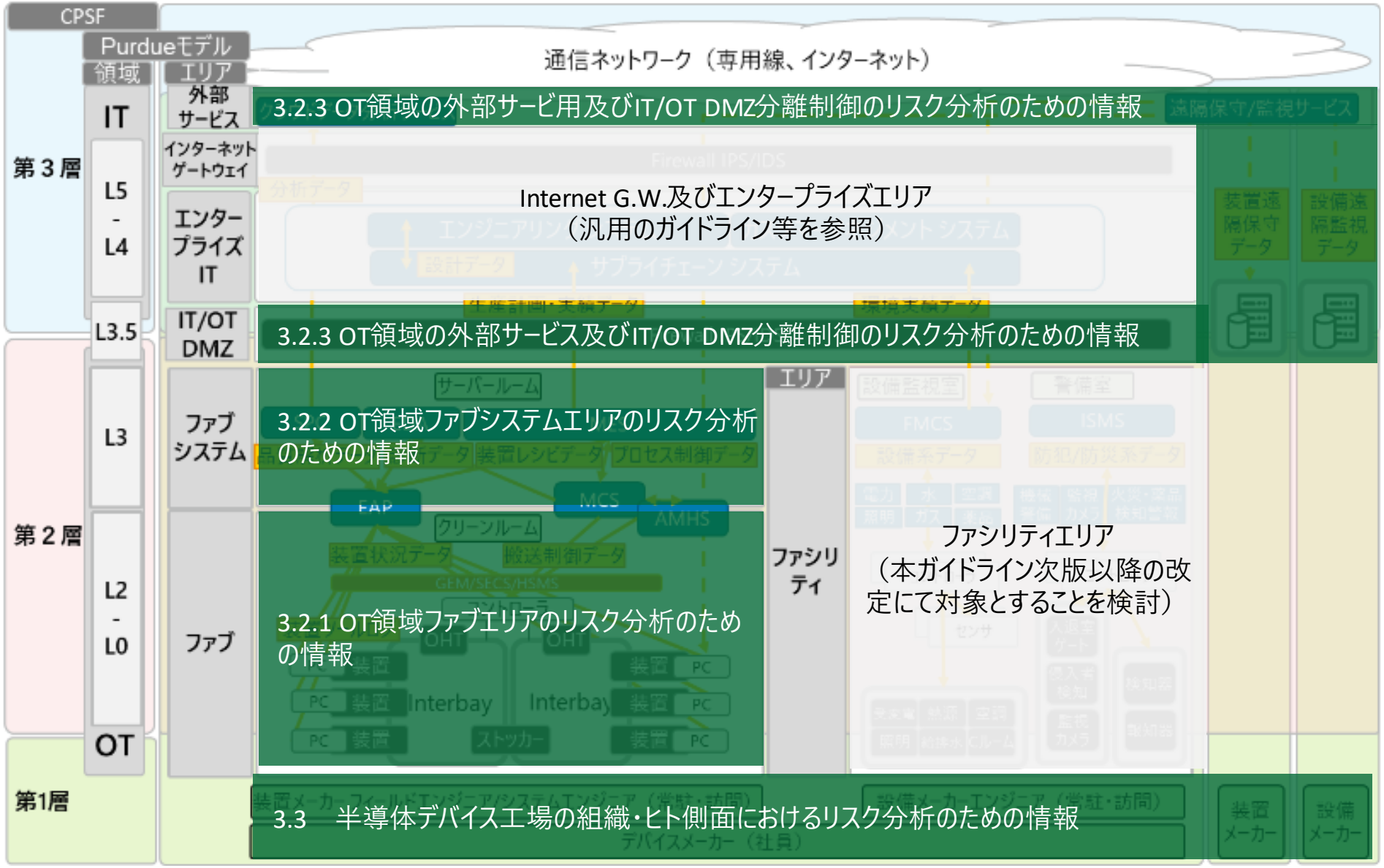


図 3-2. 第 3 章のリスク分析のための情報

表 3-1. CPSF による 6 つの構成要素

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 遠隔監視保守サービス	クラウド分析データ 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(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			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	プロセス間通信制御を実施		
OT	ファブシステム(L3)	MES SPC EDA	生産進捗データ 品質特性・解析データ 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	製造部門(ファブ)の中心(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(L0-2)	EAP AMHS MCS	最適プロセスフロー【機密】、装置状況データ、トレンド【機密】、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)、OHT、OHS	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(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 ISP	設備データ、運転データ	各設備、コントローラ、	半導体製造のクリーンルーム及び各装置の設備運転を	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

3.3 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

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)

3.2 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

第 2 章「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」で整理した Purdue モデルに基づき、OT 領域の各エリアに対して、技術・物理的側面から特徴と考慮すべき観点を洗い出し、想定されるセキュリティインシデントとリスク源の視点からまとめる。さらに、半導体業界のグローバルな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。

OT 領域は、デバイス製造の現場であり、ウェーハを加工・生産する装置ツール群のエリアである「ファブエリア」、製造の自動化を管理するシステム群のエリアである「ファブシステムエリア」、製造のための水、電気、ガス等の工場の稼働を支えるインフラ群である「ファシリティエリア」に分けて整理を行う。

また OT 領域と IT 領域を分離し制御する「IT/OT DMZ」及び OT 領域へ外部から通信接続がある「外部サービス」についても整理を行う。

なお、リファレンスアーキテクチャで整理した IT エンタープライズエリア、インターネットゲートウェイについては、IT 領域の対策となることから、本ガイドラインでは対象外とする。また、ファシリティエリアについては、半導体業界におけるグローバルな組織での検討が進行中である点踏まえ本版では対象外としている。

表 3-2. 領域・エリアにおける特徴

領域・エリア		領域・エリアにおける特徴
外部サービス		OT 領域内のファブシステムエリアでは、クラウド上でデータ解析を活用する外部サービスが利用される。クラウドの活用に際しては、ファブシステムエリアからの接続に対し、IT 領域で行うクラウドサービスセキュリティと同様の対策が必要である。 装置メーカーによるファブエリア内の装置ツールへの遠隔診断サービス（e-Diagnostics 等）や、設備メーカーによるファシリティエリア内の設備への遠隔保守サービスが利用されている。これらの各 OT 領域へのリモートアクセスサービスに対しては、IT 領域で行う対策と同様の対策が必要である。
インターネットゲートウェイ		IT 領域での対策を実施（本ガイドライン対象外）
IT	エンタープライズエリア（L4-5）	
IT/OT DMZ （L3.5）		半導体製造の OT 領域の制御システムの特性に応じた、IT/OT 領域の分離、通信の制御を行う。
OT	ファブシステムエリア（L3）	ファブシステムエリアでは、IT 領域と同様のサーバやシステムに対するサイバーセキュリティ対策が前提であるが、連続稼働を前提とした脆弱性評価やパッチ適用の運用、事業継続性を考慮したデータ保全（大量データのバックアップ及びリストア）、生産機密情報を保管するサーバルームの管理等も必要である。
	ファブエリア（L0-2）	ファブエリアのセキュリティ上の特徴として、プロセスオートメーションにより1つの工場あたりの装置ツール台数が数千台規模であるため、管理対象の台数が非常に多い点が挙げられる。また、連続稼働を前提としているため、セキュリティのパッチ適用が容易ではないという課題がある。さらに、装置ツールは平均して20年以上という長期間にわたり使用される一方で、装置ツール内に構成される PC には汎用 OS が採用されており、開発元によるサポートが終了した後も使用され続けるケースが多い。加えて、装置ツール間やファブシステムとの通信については、暗号機能や認証機能を持たない通信プロトコルが業界規格として利用されている場合が多い。 このためファブエリアでは、レシピや生産プロセス等の競合他社との差別化要因となる機密情報の保護や、装置ツールを介した不正アクセスや操作による供給・生産目標、半導体品質、人命や環境への影響（セーフティ）に対するリスクマネジメント、セキュリティ的に脆弱な環境においても可用性を高める運用の実現等が必要である。
	ファシリティエリア（L0-3）【本版対象外】	ファシリティエリアでは、データセンターやビル管理システムと類似したセキュリティ課題（機密情報の管理エリアとしての物理的対策、長期の設備運用、多種な設備メーカーのサービス管理等）があるため、同様の対策が必要である。

3.2.1 OT 領域ファブエリアのリスク分析のための情報

半導体デバイス製造の現場であり、ウェーハを加工製造する装置ツール群である「ファブエリア」では、生産目標・半導体品質の維持と生産機密情報の保護の 2 つの視点に基づき、特徴と考慮するべき観点を以下の6つに分け、それぞれ想定されるセキュリティインシデントとリスク源の視点からまとめる。さらに、グローバルな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。

表 3-4 から表 3-10 の最右列では、NIST CSF2.0 半導体製造プロファイルとして、NIST CSF2.0 におけるカテゴリ及びサブカテゴリ（GV.OC-01、ID.AM-01 等）と NIST CSF2.0 半導体製造プロファイルの 4 つのドメイン（Fab、Enterprise IT（以降、E-IT）、Ecosystem（以降、Eco）、Equipment and Tooling）を記載する。

また同様に、SEMI E187 製造リファレンスとして、第 3 章の節のタイトルを記載する。

表 3-3. OT 領域ファブエリアの分類

生産目標・半導体品質の維持のための装置ツール群のセキュリティ対策	生産機密情報の保護（ファブエリア全体、装置内データ）
①装置ツールの資産管理と脆弱性評価	④生産機密情報の把握とデータ管理
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	⑤物理アクセスの制限（入室・持込み・接続）
③安全な装置ツールの調達と導入	⑥論理的アクセスの制限（ID 管理、認証及びアクセス制御）

表 3-4. OT 領域ファブエリアのリスク分析のための情報

<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
（以下、考慮すべき観点）</th><th>CPSF 想定されるセキュリティインシデント/リスク源
（脅威、脆弱性、脆弱性 ID）</th><th>関連する NIST CSF2.0 半導体製造プロファイル/CPSF/SEMI E187 製造リファレンス</th></tr>
<tr><td>OT</td><td>ファブエリア</td><td>
①装置ツールの資産管理と脆弱性評価
特徴
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なるメーカーの装置ツールをシームレスにシステム連携し、プロセスを形成して自動連動生産を行っている。
これらの装置ツールは、ウェーハへのナノ単位の加工精度を実現する技術を盛り込んでおり非常に高額であり、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 及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。
ファブエリア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="2">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></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
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></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></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</td></tr>
</table>
</td><td>
想定されるセキュリティインシデント
• 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
• 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、事前に想定されていない動作をする

脅威
• セキュリティ上の脆弱性を利用したマルウェア感染
• 機器を管理するシステムから機器への不正なコマンド送信

脆弱性
• 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
• 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。
• 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機器のセキュリティ
</td><td>
【NIST CSF2.0 半導体製造プロファイル】
• 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
• ID.AM-02 ソフトウェア管理
• ID.AM-04 サービス管理
• ID.AM-05 資産の重要度
Fab：事業への影響を及ぼす重要資産の判断
• 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
• ID.RA-01 脆弱性評価
Fab：大量・複雑な資産の脆弱性評価
• 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
• ID.RA-03 脅威識別
• ID.RA-04 脅威の発生可能性と影響
Fab：連続稼働における事業への影響判断
• ID.RA-05 脅威の優先順位付け
Fab：リスク評価の実施
• 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
• ID.RA-07 変更管理
Fab：変更管理
• 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

【CPSF 対策要件 ID】
• CPS.AM-1
• CPS.AM-5
• CPS.AM-6
</td></tr>
</table>

		<table><tr><td></td><td>(Windows/Linux)</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(GEM/SECS/HSMS)</td></tr><tr><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 アクティブスキャンでの脆弱性評価が難しい</td></tr><tr><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>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>9</td><td>装置ツールがレガシーOS となりパッチ適用できないものがある</td></tr><tr><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> **考慮すべき観点** 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であるため、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をする必要がある。 また、各資産への脆弱性評価及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。 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レシピ等の生産機密情報の漏洩影響の大きさ等により、資産の重要度をあらかじめ分類し、優先度をつけた脆弱性評価やセキュリティ対策につなげることが有効である。	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 • 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 • 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 **対象となる構成要素** • モノ:装置ツール **【CPSF 脆弱性 ID】** • L1_1_a_SYS • L1_1_b_COM • L2_1_a_ORG • L2_1_b_ORG • L2_1_c_SYS • L2_1_c_ORG • L3_1_a_SYS	• CPS.RA 全て **【SEMI E187 製造リファレンス】** 3.4 Vulnerability/Threat Assessment and Patch Management 概要: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

		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基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）を含め、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。 **具体的対策事例** 対策検討を進める上で、参考となる具体的な事例を第 4.1 節に示す。		
		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 **特徴** 脆弱性対策が難しい装置ツールがあるファブエリアにおいては、攻撃者の侵入を防ぎ被害を極小化するためのネットワークや物理制約を組み合わせた多層防御やマイクロセグメンテーションの追加防御対策を行う特徴がある。 **考慮すべき観点** 装置ツールへの追加対策は、生産の可用性を守り高めるために行われ、ネットワークによる細分化では、被害発生時の極小化により製造の影響を限定し封じ込め、早期復旧や限定継続できる生産の可用性を踏まえた多層防御やマイクロセグメンテーションの対策に合わせ、異常検知の検討が必要である。 以下では多層防御を、以下の3つに分け、関連プロファイル、リファレンスとの整理を行う。 ②-1 装置ツール（エンドポイント）の考慮すべき観点 ③-2 ネットワークの考慮すべき観点 ②-3 物理的な制約の考慮すべき観点 **具体的対策事例** 対策検討を進める上で、参考となる具体的な事例を第 4.2 節に示す。		

		②-1 装置ツール(エンドポイント)の考慮すべき観点 装置ツールへのセキュリティ対策は、SEMI E187/188 に合わせたセキュリティ対策を検討する必要がある。具体的には、装置の性能保証の上で、セキュリティ対策エージェントの導入、マルウェア対策の有効化、ハードニング対策(不要な I/O ポートの制限、不要なサービス/コンポーネント/ネットワークプロトコル/ポートの無効化等)、異常検知ツールの導入(EDR)等を検討する必要がある。既存装置ツールにおいては、性能保証上の仕様により新たなソフトウェアツールの導入や設定変更が行えないものも存在するため、ネットワークによる追加対策(多層防御やマイクロセグメンテーション等)を検討する必要がある。	**想定されるセキュリティインシデント** • 脆弱性を悪用して機器内部に不正アクセスされ、事前に想定されていない動作をする • 正規のユーザーになりすまして機器内部に不正アクセスされ、事前に想定されていない動作をする **脅威** • 機器におけるセキュリティ上の脆弱性を利用したマルウェア感染 • 窃取した ID、パスワード等を利用した正規ユーザーへのなりすまし **脆弱性** • 利用している機器が十分なセキュリティ機能を実装していない • 自組織のリスクを踏まえた技術的対策が実装されていないか、実装を確認できない • 保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている • セキュリティの観点において強度が十分でない設定(パスワード、ポート等)が	**【NIST CSF2.0 半導体製造プロファイル】** • 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 • PR.DS-01 保存データのセキュリティ保護 Fab:データアクセスの複雑化 • PR.DS-10 使用データのセキュリティ保護 Fab:運用データの保護 • PR.DS-11 データのバックアップ Fab:機密運用データのバックアップ • PR.PS 全て プラットフォームセキュリティ • PR.IR-02 技術資産の環境脅威からの保護 Fab:クリーンルーム環境の管理 • PR.IR-03 レジリエンスの確保 Fab:レジリエンスの確保 • PR.IR-04 リソース容量の確保 Fab:リソース容量の確保 • DE.CM-03 人員・技術利用の監視 Fab:人員の活動の監視 • DE.CM-06 外部サービスプロバイダの監視 Fab:外部サービスプロバイダの監視 • DE.CM-09 コンピュータ・データの監視 **【CPSF 対策要件 ID】** • CPS.IP-2 • CPS.IP-3 • CPS.IP-7 • CPS.PT-2 • CPS.PT-3 • CPS.DS-10 • CPS.DS-13 • CPS.DS-15 **【SEMI E187 製造リファレンス】** 3.5

			なされている • 早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない **対象となる構成要素** • モノ:装置ツール **【CPSF 脆弱性 ID】** • L1_1_a_SYS • L1_1_c_SYS • L2_1_a_COM • L2_1_b_COM • L3_1_a_SYS • L3_3_a_SYS • L3_3_d_SYS	Tool Network and Application Integration **概要:**脆弱性評価やパッチ適用が制約される装置ツールに対する階層型のネットワークセキュリティ対策等について記載
		②-2 ネットワークの考慮すべき観点 装置ツールでは、パッチ適用やマルウェア対策等セキュリティ対策が行えないものや、運用制約上でパッチ適用に時間を要するものがあるため、ネットワークによる追加対策を検討する必要がある。 ネットワークの対策においては、生産の可用性を守り高めるために、被害発生時の極小化により製造の影響を限定し封じ込め、早期復旧や限定継続できることを意識した細分化と通信制限(ゾーン・コンジット)を行う必要がある。 具体的には第 2 章の半導体デバイス工場におけるセキュリティアーキテクチャ(Purdue モデル)に基づき、以下の検討を行う必要がある。	**想定されるセキュリティインシデント** • サービス拒否攻撃、ランサムウェアへの感染等により、自組織のデータを取り扱うシステムが停止する • 品質や信頼性の低い機器がネットワークに接続され、故障や正確でないデータの送信、想定していない通信先へのデータ通信等が発生する • 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	**【NIST CSF2.0 半導体製造プロファイル】** • ID.AM-03 ネットワークデータフロー管理 Fab:複雑なデータフローの管理 • PR.DS-02 伝送データのセキュリティ保護 Fab:M2M 通信データの保護 • PR.PS-04 ログ記録の管理 Fab:レガシー機器のログ管理 • PR.IR 全て 技術インフラのレジリエンス • DE.CM-01 ネットワーク監視 Fab:専門的な監視ソリューション • DE.CM-03 人員・技術利用の監視 Fab:人員の活動の監視 • DE.CM-06 外部サービスプロバイダの監視 Fab:外部サービスプロバイダの監視

		ネットワークの考慮すべき観点 1 OT ネットワークは、IT 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） 2 OT 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分割したうえ通信制限を行う。 3 ファブエリア内のファブネットワークにおいても、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用途、故障予測や検知用のセンサ連携用途等、装置ツール間や各ファブシステムとのデータフローを洗い出し、適切に分離のうえ通信制限を行う。 4 装置ツールへのセキュリティ対策が行えないものは、マイクロセグメンテーションによる被害や拡散防止のための対応を検討する。マイクロセグメンテーションの単位は、生産の可用性を意識し、被害発生時に極小化し封じ込めが可能な単位で検討を行う。 5 重要な箇所にはネットワークの異常検知の仕組みを導入する。	**脅威** • システムを構成するサーバ等の電算機器、通信機器等に対するサービス拒否攻撃 • 改ざんされた正規なモノ/システムからの適切でないデータの受信 • 通信経路上でデータを改ざんする中間者攻撃等 **脆弱性** • 通信開始時に、通信相手を識別・認証していない • サーバ等に対する通信を適切に制御していない • 通信経路上でデータが十分に保護されていない • 組織外部への不正な通信を適切に検知し、遮断する等の対応ができない • 通信経路が適切に保護されていない • 早期にネットワーク上での異常（例：なりすまし、メッセージの改ざん）を素早く検知し、対処するような仕組みがシステムに実装されていない **対象となる構成要素** • モノ：OT ネットワーク **【CPSF 脆弱性 ID】** • L1_1_b_DAT	**【CPSF 対策要件 ID】** • CPS.AM-4 • CPS.AM-5 • CPS.AC-3 • CPS.AC-7 • CPS.AC-8 • CPS.DS-6 • CPS.DS-9 • CPS.AE-1 **【SEMI E187 製造リファレンス】** 3.5 Tool Network and Application Integration 概要：脆弱性評価やパッチ適用が制約される装置ツールに対する階層型のネットワークセキュリティ対策等について記載 3.10 Security Key Performance Indicators **概要：**持続可能なセキュリティ運用管理を実現するためのセキュリティ KPI について記載

<table>
<tr><td></td><td></td><td></td><td>• L1_1_b_SYS
• L1_1_c_SYS
• L2_1_a_COM
• L3_2_b_DAT
• L3_3_a_SYS</td><td></td></tr>
<tr><td></td><td></td><td rowspan="2">②-3 物理的な制約の考慮すべき観点
セキュリティ対策が難しい装置ツールに対しては、物理的な操作や接続、通信窃取のアクセスを制限する対策を検討する必要がある。
複数の装置メーカーのフィールドサポート保守要員が常駐・訪問することから、入室エリアや操作ボックスを制限した物理的な対策を検討する必要がある。

例）
ファブエリア内のネットワーク機器は、施錠管理可能なラックやボックスの中で管理を行う。
未使用のファブネットワークの接続口が通常アクセス可能な範囲にある場合は、物理的なポートロック対策を行う。
ファブエリア内で利用する無線については、施設エリア内・外への放射範囲や、施設エリア外から届く電波を確認し、適切な対策を行う。</td><td>リスク（想定されるセキュリティインシデント）
• 物理的な不正行為により、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する
• 自組織で管理している領域から保護すべきデータが漏洩する</td><td rowspan="2">【NIST CSF2.0 半導体製造プロファイル】
• PR.AA-06 物理アクセスの管理
Fab：クリーンルームへのアクセス制御
• PR.PS-04 ログ記録の管理
Fab：レガシー機器のログ管理
• PR.IR-02 技術資産の環境脅威からの保護
Fab：クリーンルーム環境の管理
• DE.CM-02　物理環境の監視</td></tr>
<tr><td></td><td></td><td>脅威
• 保護が必要なエリアに対する不正なヒトの物理的な侵入
• 悪意を持った自組織内外のヒトによる不正改ざん
• センサの測定値、閾値、設定の改ざん

脆弱性
• 自組織内外のヒトによる機器に対する物理的な不正行為を防げない
• 設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない
• サーバ等に対する物理的な妨害（例:妨害電波）に対処できていない</td><td>【CPSF 対策要件 ID】
• CPS.AC-2
• CPS.IP-5
• CPS.CM-2</td></tr>
</table>

			• 不正な機器がネットワークに接続されたことを適切に検知できない **対象となる構成要素** • ファブエリア **【CPSF 脆弱性 ID】** • L1_1_a_SYS • L1_1_c_SYS • L2_3_b_SYS • L2_3_b_PEO • L2_3_c_SYS • L2_3_d_SYS • L3_1_a_SYS	
		③安全な装置ツールの調達と導入 **特徴** 装置ツールは非常に高額であり、平均的に 20 年以上の長期利用が行われるデバイスとなる。そのため、ファブ環境でのセキュリティ運用を見据えた安全設計(Security by design)を盛り込んだ仕様への反映、導入時の確認が必要である。 2021 年に、業界の装置ツールの安全化の標準として SEMI E187/ E188 が発行されている。 **考慮すべき観点** ファブエリアに安全な装置ツールを導入するためには、調達の際に、SEMI E187「ファブ装置のサイバーセキュリティ仕様」を基にしてファブ運用を考慮した OS のサポート状況やセキュリティアップデートの実施手順、脆弱性診断の実施状況、セキュアなプロトコル利用及び通信制限のための必要情報、アクセス制御機能、セキュリティログ機能等について装置ベンダー等に事前に確認することが必要である。	**想定されるセキュリティインシデント** • 製品・サービスの提供チャネルでセキュリティ事象が発生し、機器の破損等の意図しない品質劣化が生じる **脅威** • 機器におけるセキュリティ上の脆弱性を利用したマルウェア感染 • 悪意を持った自組織内外のヒトによる計測機能に対する不正行為 **脆弱性** • 製品・サービスを調達する際、それが信頼できるものか	**【NIST CSF2.0 半導体製造プロファイル】** • GV.SC-01 リスク管理枠組みの確立と同意 Fab:単一供給者への依存対策 • GV.SC-02 役割・責任の確立 • GV.SC-04 サプライヤの把握 • GV.SC-05 リスク要件の確立 Fab:購買仕様・SLA の定義 • GV.SC-06 リスク評価と計画実施 Fab:サプライヤ重要度の評価 • GV.SC-07 サプライヤリスク管理 • GV.SC-09 セキュリティプラクティスの監視 • GV.SC-10 合意後の活動規定 Fab:ベストプラクティス実現可能性評価 • ID.AM-04 サービス管理 • ID.RA-09 真正性・完全性のアセスメント Fab:コンポーネントの真正性の確保 • ID.RA-10 サプライヤのアセスメント Fab:専門のサプライヤのアセスメント

			を確認していない • 調達時に、適切なレベルのセキュリティ機能が実装されているかを確認するプロシージャがない • 自組織の調達に関わる要員が、調達に係るセキュリティリスクを十分に認識していない • 製品・サービスの調達時に、調達品の適格性を確認するプロシージャが存在しない • 機器を調達する際、安全性を実装しているか確認していない • 機器を調達する際、調達製品が計測セキュリティを考慮しているものかを確認していない **対象となる構成要素** • モノ:装置ツール **【CPSF 脆弱性 ID】** • L1_1_d_ORG • L1_1_d_PRO • L2_1_a_PRO • L2_2_a_ORG • L2_3_c_ORG • L2_3_c _PRO • L2_3_d_ORG	**【CPSF 対策要件 ID】** • CPS.SC-1 • CPS.SC-2 • CPS.SC-3 • CPS.SC-4 • CPS.SC-5 • CPS.SC-6 • CPS.AM-7 • CPS.DP-1 • CPS.PT-3 • CPS.DS-12 • CPS.CM-3 **【SEMI E187 製造リファレンス】** 3.1 Secure by Design 概要:ファブエリアに安全な装置ツールを導入するために、装置ベンダー等と事前に確認すべき調達要件のポイントについて記載 3.2 Tool Configurations 概要:ファイア・ウォールの設置、通信の分離等、半導体デバイスメーカーが装置ツールを調達する際に検討することが望ましい仕様について記載

		④生産機密情報の把握とデータ管理 **特徴** ファブエリアにおける生産機密情報は、フォトマスク作成工程としての設計情報、前工程での微細化技術、歩留まり向上に対するレシピ・生産プロセスの情報、後工程の積層化術に対する生産技術情報等がある。これらの情報は機密性が非常に高く、侵害が知財流出を引き起こすと競合他社に対する開発競争等において不利な状況を招く特徴がある。 **考慮すべき観点** OT 領域における生産機密情報は、主にファブシステムエリアで保管されるが、ファブエリアにおいてもファブエリア自身及び装置ツール内に生産機密情報が存在するため、機密データ管理が必要となる。 クリーンルーム内は、生産プロセス工程の編成、利用する装置ツールの機種や台数等視覚的情報を含めて生産機密情報の扱いとする工場も多い。そのため、ファブエリア内での画像・映像の録画、録音デバイスの持込み制約を検討する必要がある。 装置ツール内には、レシピや品質情報等生産機密情報が保存されている。各装置内に保管される生産機密情報についても情報資産として把握を行い、通常運用における生産機密情報へのアクセス制限を行うとともに、保守メンテナンス時においてもアクセス制限やデータ持ち出し制限を行う必要がある。 また、装置ツールの入替や撤去時においては、装置ツール内部のストレージに保管された機密データの確実な消去を行う必要がある。	**想定されるセキュリティインシデント** • 自組織が保護すべきデータが漏洩、改ざんされる **脅威** • 悪意あるエンティティによる保護すべきデータの持ち出し • 媒体の物理的な破壊 • 正規ユーザーへのなりすまし **脆弱性** • 機密区分に沿った情報の保護が実装されていない • 保護すべきデータが格納されたシステムにおいて、セキュアでない設定がなされている • 保護すべきデータの管理に関する組織内の責任が明確でない **対象となる構成要素** • データ:生産機密情報 • ヒト:ファブエリア入室者 • 装置ツールへのアクセス者 **【CPSF 脆弱性 ID】** • L1_1_a_DAT • L1_1_a_SYS • L1_1_b_SYS • L1_1_c_SYS • L3_1_a_DAT • L3_1_a_ORG • L3_4_a_ORG	**【NIST CSF2.0 半導体製造プロファイル】** • GV.OC-03 法的・規制上の要求事項の管理 • ID.AM-05 資産の重要度 Fab:事業への影響を及ぼす重要資産の判断 • ID.AM-07 メタデータの管理 Fab:プロセスレシピのメタデータの管理 • 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 • PR.DS 全て データセキュリティ • PR.IR-02 技術資産の環境脅威からの保護 Fab:クリーンルーム環境の管理 **【CPSF 対策要件 ID】** • CPS.DS-1 • CPS.DS-2 • CPS.DS-3 • CPS.DS-4 • CPS.DS-5 • CPS.DS-9 • CPS.DS-11 • CPS.DS-14 • CPS.AM-6 • CPS.GV-3 • CPS.IP-6 **【SEMI E187 製造リファレンス】** 3.3 Move-in/Move-Out/Transfer 概要:装置ツールの導入、撤去、移転の際に、特に生産機密情報を保護するための確認すべきポイントについて記載 3.7 Secure data exchange

			• L3_4_b_SYS	概要：装置ツールの導入、撤去、移転の際に、特に生産機密情報を保護するための確認すべきポイントについて記載
		⑤物理アクセスの制限（入室、持込み、接続） **特徴** ファブエリアであるクリーンルーム内は、生産プロセス工程の編成、利用装置ツール機種や台数等視覚的情報を含めて生産機密情報の扱いとする。また、装置ツール群については単体でのセキュリティ対策運用が困難であるため、ファブエリアへの入室許可、デバイスの持込み・接続含めた管理を行う必要がある。 また、ファブエリア内の生産工程は、異なるメーカーの専用装置ツールを用いて構成され、連続生産稼働されることから、多くの装置メーカーと保守契約が結ばれている。各装置メーカーのフィールドエンジニア要員の常駐や訪問含めた保守運用作業が頻繁に行われる特徴がある（台湾大手半導体企業にて、2018 年保守持込みデバイスからのマルウェア大規模感染被害の事例がある）。 **考慮すべき観点** 生産機密情報を扱うファブエリアへの入室者の制限は、デバイス工場への入門からクリーンルーム入室までの動線で行う必要がある。 また、デバイスの持込みに関しては、画像・映像の録画、録音デバイスの持込みの制約を検討する必要がある。 合わせて OHT 等自動搬送装置は無線通信で稼働するため、無線通信を妨害する可能性がある電波を発生するデバイスの持込みについても制約する必要がある。 保守作業で多く行われるデバイスの接続に関しては、ファブエリアへの新たな装置ツール類（センサ周辺デバイス機器を含む）の導入によるファブネットワークへの接続、及び装置ツール類への保守作業による持込みデバイスの装置ツールへの接続（USB、シリアルやネットワーク）が発生する。接続時には、決められたセキュリティ対策確認手順を得た上で接続する運用を行う必要がある。 保守作業におけるデバイス接続時のセキュリティ対策確認においては、マルウェア等不正プログラムの持込みだけではなく、装置ツール	**想定されるセキュリティインシデント** • 物理的な不正行為により、故障や正確でないデータの送信、想定していない通信先へのデータ送信等が発生する • 自組織で管理している領域から保護すべきデータが漏洩する **脅威** • 保護が必要なエリアに対する不正なヒトの物理的な侵入 • 悪意を持った自組織内外のヒトによる不正改ざん • センサの測定値、閾値、設定の改ざん **脆弱性** • 設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない • 不正な機器がネットワークに接続されたことを適切に検知できない • 不正な機器によるネットワーク接続（有線あるいは無線）を防止できない	**【NIST CSF2.0 半導体製造プロファイル】** • DE.CM-01 ネットワーク監視 Fab：専門的な監視ソリューション • DE.CM-02 物理環境の監視 • DE.CM-03 人員・技術利用の監視 Fab：人員の活動の監視 • DE.CM-09 コンピュータ・データの監視 **【CPSF 対策要件 ID】** • CPS.CM-2 • CPS.CM-6 • CPS.MA-2 **【SEMI E187 製造リファレンス】** 3.3 Move-in/Move-Out/Transfer 概要：装置ツールの導入、撤去、移転の際に、特に生産機密情報を保護するための確認すべきポイントについて記載 3.4 Vulnerability/Threat Assessment and Patch Management 概要：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

		内にあるレシピや品質情報等の生産機密情報の持ち出し確認も検討する必要がある。 **具体的対策事例** 対策検討を進める上で、参考となる具体的な事例を第 4.4 節に示す。	• 機器設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない **対象となる構成要素** • ヒト　:装置保守担当者 • データ:生産機密情報 • モノ　:持込みデバイス **【CPSF 脆弱性 ID】** • L1_1_a_SYS • L2_3_b_SYS • L2_3_c_SYS • L2_3_d_SYS • L3_1_a_SYS	
		⑥論理的アクセスの制限(ID 管理、認証及びアクセス制御) **特徴** 装置ツールにはレシピ等機密データが保管されているため、厳格なアイデンティティ管理、認証及びアクセス制御が必要となる。 アカウントは、通常運用時に利用されるアカウントとともに、保守メンテナンス時利用されるアカウントが存在する。 また、装置ツールは、装置メーカーと保守契約を行いフィールドサポート要員が常駐、訪問して対応を行う。さらに、装置メーカーから e-Diagnostics 技術を用いた遠隔診断サービスが提供される場合もある。装置ツールのアカウント管理は、装置メーカーの業務委託契約の保守員を含めた管理が行われる特徴がある。 **考慮すべき観点** 装置ツールへの不正アクセスは、生産の停止や生産機密情報の漏洩、レシピの改ざん等につながるため、適切な IAM(Identity and Access Management)としてアカウント管理と特権管理	**想定されるセキュリティインシデント** • 自組織で管理している領域から保護すべきデータが漏洩する **脅威** • 窃取した ID、パスワード等を利用した正規ユーザーへのなりすまし **脆弱性** • 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない	**【NIST CSF2.0 半導体製造プロファイル】** • GV.RR-04 人事プロセスのセキュリティ Fab:不許可アクセスの防止 • PR.AA-01 ID・認証情報の管理 Fab:産業制御・IT システムのアクセス制御 • PR.AA-02 相互作用の ID 認証 Fab:相互作用のコンテキスト • PR.AA-03 ユーザー認証 Fab:すべての機器へ認証メカニズムを実装 • PR.AA-04 ID アサーション Fab:ファブシステムと装置間の ID アサーション • PR.AA-05 最小特権・職務分離の原則 Fab:異なるエリアへのアクセス制御 • PR.AA-06 物理アクセスの管理 Fab:クリーンルームへのアクセス制御

		を行うことが重要である。アカウント管理は、そのアカウントのライフサイクル全体(生成・変更・廃棄)をデバイスメーカーによる適切な承認プロセスや、すべてのアクセスの監視、監査プロセスを導入することを含む。特に多くの権限を使用する保守時に利用する特権をもつアカウント(Privileged Account)については運用時の一般アカウントよりも厳密な管理を行う必要がある。 業界で開始されている e-Diagnostics 技術を用いた遠隔診断サービス等については、デバイスメーカーによるなりすましの防止や機密情報の漏洩対策を含めた監視、ログ取得、暗号化を含むセキュアなソリューションとプロセスの導入と運用を行う必要がある。	• 定められた機密区分に沿った情報の保護が実装されていない • 職務及び責任範囲(例:ユーザー/システム管理者)を適切に分離する **対象となる構成要素** • ヒト:装置ツールへのアクセス者 **【CPSF 脆弱性 ID】** • L1_1_a_SYS • L1_1_b_SYS • L1_1_a_DAT • L2_1_c_SYS • L3_1_a_DAT	**【CPSF 対策要件 ID】** • CPS.AC-1 • CPS.AC-4 • CPS.AC-5 • CPS.AC-6 • CPS.AC-9 • CPS.IP-1 • CPS.IP-9 **【SEMI E187 製造リファレンス】** 3.6 Local & Remote Accesses 概要:不正アクセスを防ぐため、アカウント管理と特権管理のポイントについて記載

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

半導体デバイス製造の自動化を管理するシステム群である「ファブシステムエリア」については、IT 領域と同様にサーバ・システムに対するサイバーセキュリティ対策が前提となる。その中でも、半導体デバイス工場での IT 領域対策とは異なり、特徴と考慮するべき観点として以下の3つを想定されるセキュリティインシデントとリスク源の視点からまとめる。さらに、グローバルな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。

表 3-5. OT 領域ファブシステムエリアの分類

分類	概要説明
①システム可用性	連続稼働におけるパッチ適用等を含めた運用考慮点
②データ保全	映像・画像を扱う大容量バックアップと事業継続を考慮した早期リストア
③サーバルームの物理的対策	機密データ保管エリアとしての物理対策管理

表 3-6. 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

領域・エリア		特徴及び考慮すべき観点	CPSF 想定されるセキュリティインシデント/リスク源（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/CPSF/SEMI E187 製造リファレンス
OT	ファブシステムエリア	**①システム可用性（連続稼働における運用）** **特徴** ファブシステムエリアでは、ファブエリアの装置ツール類の生産プロセス及び品質管理を MES、SPC、EDA の各システムによって行い、これらはサーバ・ストレージ・ネットワーク等で構成される。ファブシステムエリアのセキュリティ対策は、IT 領域と同様に脆弱性評価・パッチ適用管理の対策を行うが、連続稼働やシステム連携の確認を前提とした運用が必要である。 具体的な運用として、EC サイトと同様な連続サービス提供の中でのオンラインパッチ適用を求められる。しかし、ファブシステムへのパッチ適用の中には、システム連携の確認等によりオンライン適用が行えないものもある。そのため、年に限られたライン停止時のメンテナンス時間にて計画・実行するという特徴がある。 **考慮すべき観点** ファブシステムエリアの脆弱性評価とパッチ適用の実行には、タイムラグが発生する。（ライン停止のメンテナンスタイミングが数か月や 1 年単位となる） 具体的な対策として、IT 領域とファブシステムエリアの領域を、IT/OT DMZ で分離し、通信を制限した対応や、IPS/IDS を用いた異常検知や仮想パッチ適用を検討することが有効である。	**想定されるセキュリティインシデント** • システムや通信機器等の機能が停止する **脅威** • システムを構成する機器、通信機器等に対するサービス拒否攻撃 • 品質や信頼性の低いシステムによるサービス提供 **脆弱性** • 稼動するシステムとして、安全計装が考慮されていない • 品質や信頼性の低いシステムによるサービス提供、連続稼働を前提とした、十分なリソース（処理能力、通信帯域、ストレージ容量）が確保されていない **対象となる構成要素** • システム：MES、SPC、EDA 等 • モノ：サーバ、ストレージ、ネットワーク **【CPSF 脆弱性 ID】**	**【NIST CSF2.0 半導体製造プロファイル】** • PR.IR-03 レジリエンスの確保 Eco：回復メカニズムの実装 E-IT：ビジネスシステムのアクセスの維持 • PR.IR-04 リソース容量の確保 Eco：リソース容量の確保 E-IT：リソース容量の確保 **【CPSF 対策要件 ID】** • CPS.DS-7

			• L1_1_c_SYS • L2_1_d_SYS • L3_3_c_SYS	
		②データ保全(大容量バックアップ、リストア) **特徴** ファブのシステムは、プロセス型自動制御の指示を行うとともに、高画像・映像のデータ利用による品質判定と履歴保管を行うため、大容量のストレージを必要とする。 また、システムの停止や生産データの被害発生時には、供給責任を含めた早期復旧のために、バックアップデータからリストア時間を考慮したシステム構成を行う特徴がある。 **考慮すべき観点** ファブのシステムでは大容量のストレージのバックアップが必要となるが、早期復旧のためのリストア時間を考慮したバックアップ方法の選択が重要である。合わせて、ランサムウェアの被害が、バックアップデータに及ばないように、権限分離や改ざん防止(オフラインやWORM 機能)等のセキュリティ対策を検討する必要がある。 また、装置ツール内に保管されるデータ(構成情報、校正値、セキュリティログ等)についても、復旧を考慮したバックアップ方法を選択することが重要である。	**想定されるセキュリティインシデント** • 自組織のセキュリティインシデントにより自組織が適切に事業継続できない **脅威** • データを保管する機器に対する攻撃 • 品質や信頼性の低いシステムによるサービス提供 **脆弱性** • セキュリティインシデント発生時に事業を継続するために必要なデータが、適切に準備されていない、又は準備されているが適切に機能しない **対象となる構成要素** • システム:ファブシステムのバックアップシステム • モノ:バックアップサーバ、ストレージ、バックアップ媒体 【CPSF 脆弱性 ID】 • L1_3_a_DAT • L2_1_d_SYS	**【NIST CSF2.0 半導体製造プロファイル】** • PR.DS-11 データのバックアップ Eco:バックアップデータの検証 E-IT:重要データの定期的なバックアップ • PR.IR-03 レジリエンスの確保 Eco:回復メカニズムの実装 E-IT:ビジネスシステムのアクセスの維持 • PR.IR-04 リソース容量の確保 Eco:リソース容量の確保 E-IT:リソース容量の確保 • RC.RP-03 バックアップの整合性の検証 Eco:バックアップの整合性の検証 E-IT:バックアップの整合性の検証 **【CPSF 対策要件 ID】** • CPS.IP-4

			• L3_3_c_SYS	
		③サーバルームの物理的対策 **特徴** ファブのシステム群は、大容量のストレージを必要とするとともに、ファブエリアの装置ツールと MES 等ファブシステムは、距離的遅延を避けた高速なネットワークで接続される必要があるため、工場内にサーバルームを設ける必要がある。 工場内のサーバルームには、デバイス製造の連続稼働を支える冗長化されたサーバ、ストレージ等で構成されたファブシステムが導入され、社内運用を行う必要がある。 また、ファブシステム群のサーバ及びストレージ機器には、生産機密情報が保管されるため、管理するサーバルームは、機密データ保管エリアとしての運用管理される特徴がある。 **考慮すべき観点** サーバルームでは生産機密情報が保管されるため、機密データ保管エリアとしての対策が必要である。具体的には、入退室のアクセス制限(保守業者の作業ルール)や監視システム(CCD カメラによる監視や記録、センサ検知)、サーバルームへのデバイス持込み・持ち出し管理(バックアップ媒体含む)等を検討する必要がある。	**想定されるセキュリティインシデント** • 自組織で管理している領域から保護すべきデータが漏洩する **脅威** • 保護が必要なエリアに対する不正なヒトの物理的な侵入 • 不正なエンティティの物理的侵入 • 悪意あるエンティティによる保護すべきデータの持ち出し **脆弱性** • 設置エリアのアクセス制御や監視等の物理的セキュリティ対策を実施していない • 機密区分に沿った情報の保護が実装されていない **対象となる構成要素** • モノ:サーバルーム **【CPSF 脆弱性 ID】** • L1_1_a_SYS • L1_1_c_SYS • L2_3_b_PEO • L2_3_b_SYS • L2_3_c_SYS • L2_3_d_SYS • L3_1_a_SYS	**【NIST CSF2.0 半導体製造プロファイル】** • PR.AA-06 物理アクセスの管理 Eco:人員の出入りの監視 E-IT:開発環境の物理的セキュリティの確保 • PR.PS-04 ログ記録の管理 Eco: ログの継続的な監視 E-IT:システムログのフォーマットの統合 • PR.IR-02 技術資産の環境脅威からの保護 Eco:環境的脅威からの保護 E-IT:サーバの環境的脅威からの保護 • DE.CM-02 物理環境の監視 Eco:機密領域への不正アクセスの監視 E-IT:不正な物理アクセスからの保護 **【CPSF 対策要件 ID】** • CPS.AC-2 • CPS.IP-5 • CPS.CM-2

3.2.3 OT 領域の外部サービス及び IT/OT DMZ 分類制御のリスク分析のための情報

歩留まり品質の早期改善やコストダウンを進める上で、 OT 領域に対して「外部サービス」を活用した取り組みが検討されている。合わせて OT 領域を、IT 領域及びインターネットから分離制御して守る「IT/OT DMZ」の機能と合わせて運用が行われる。これらの特徴と考慮するべき観点を、以下の3つを想定されるセキュリティインシデントとリスク源の視点からまとめ、グローバルな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。

表 3-7. OT 領域の外部サービス及び IT/OT DMZ 分離制御の分類

分類	概要説明
①外部サービス活用（クラウドサービス）	OT ファブシステムにあるデータを、クラウドデータ分析サービスに活用
②外部サービス活用（遠隔診断サービス利用）	保守先の装置メーカーからファブエリアにある装置ツールへの遠隔診断サービス活用（e-Diagnostics 等）
③IT/OT DMZ	OT 領域を分離制御して守る IT/OT DMZ

表 3-8. 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

領域・エリア		特徴及び考慮すべき観点	CPSF 想定されるセキュリティインシデント/リスク源（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/CPSF/SEMI E187 製造リファレンス
OT	外部サービス	**①外部サービス活用（クラウドサービス）** **特徴** 歩留まり品質向上・コスト削減のため、OT ファブシステムにある品質データを用いて、クラウドデータ分析技術を用いたサービスと接続させた利用が進められている。 **考慮すべき観点** クラウドサービス利用時のサイバーセキュリティ対策は、IT 領域で行われる対策（CSPM、CWPP、CASB、CIEM、SSPM 等）と同様に実施する。クラウドサービスを利用する OT 領域のシステム管理者は、IT 領域のクラウド関連セキュリティ責任者と連携し、対策（ポリシーチェック等含む）を行う必要がある。 特に、生産機密情報となる品質データを用いたデータ解析のクラウド利用においては、データ保護（通信・保管上の暗号化）アクセス管理等に留意して、クラウドセキュリティ対策の検討を行う必要がある。	**想定されるセキュリティインシデント** • クラウドで管理しているデータ保管領域から自組織の保護すべきデータが漏洩する • サービスの提供チャネルでセキュリティ事象が発生し、意図しない品質劣化、停止が発生する **脅威** • セキュリティ上の脆弱性を利用したマルウェア感染 • 品質や信頼性の低いシステムによるサービス提供 **脆弱性** • 自組織のシステム/データのサイバー空間における他組織との連携状況を把握していない • 早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない • サービスサプライヤに対して、組織、システム等の信頼性を契約前、契約後に確認していない	**【NIST CSF2.0 半導体製造プロファイル】** *IT 領域で行われるクラウドセキュリティ対策を実施 **【CPSF 対策要件 ID】** *IT 領域で行われるクラウドセキュリティ対策を実施

			対象となる構成要素 • システム:クラウドサービス	
		②外部サービス(遠隔診断サービス利用) **特徴** 保守先の装置メーカーからファブエリアにある装置ツールへの遠隔診断/保守サービス利用(e-Diagnostics 等)が進められている。 **考慮すべき観点** ファブエリアや OT 領域へ外部からのネットワーク回線の接続が発生する場合は、接続業者や利用業者との契約事項を含め、回線の接続構成や利用方法、管理責任範囲等について情報セキュリティ責任者とリスク評価を行い、IT 領域と同等のセキュリティ対策を行う必要がある。 リモートからのネットワーク接続は、専用網、インターネット網、電話回線網などの一般的な有線通信網による接続だけではなく、モバイルルーター等が使う携帯電話通信網や WiFi 無線接続網、衛星通信網などの無線通信網も漏れなく対象として洗い出し、リスク評価を行う必要がある。 ファブエリアに設置された装置ツールへの遠隔保守に関しては、連続稼働する装置ツールに対するセキュリティ対策が不十分となるため、IT/OT DMZ エリア等に常に最新のセキュリティ対策が行われた JUMP サーバ環境を設け、遠隔操作内容の監視記録、ユーザーのなりすましを防ぐ認証強度の強化(多要素認証(MFA)等)、通信先と通信ポートを限定した接続環境を限定する等の対策を実施するとともに、機密情報の漏洩対策を含めた監視、ログ取得、暗号化を含むセキュアなソリューションとプロセスの導入と運用を行う必要がある。	**想定されるセキュリティインシデント** • 外部から自組織で管理している領域への悪意あるエンティティによる侵入により、保護すべきデータが漏洩し、データを取り扱うシステムが停止する **脅威** • システムにおけるセキュリティ上の脆弱性を利用した侵入攻撃 • 悪意あるエンティティによる保護すべきデータの持出し • 窃取した ID、パスワード等を利用した正規ユーザーへのなりすまし **脆弱性** • 自組織のシステム/データのサイバー空間における他組織との連携状況を把握していない • 早期にセキュリティ上の異常を素早く検知し、対処するような仕組みがシステムに実装されていない • サービスサプライヤに対して、組織、システム等の信	**【NIST CSF2.0 半導体製造プロファイル】** *IT 領域で行われるリモートアクセス対策を実施 **【CPSF 対策要件 ID】** *IT 領域で行われるリモートアクセス対策を実施 **【SEMI E187 製造リファレンス】** 3.6 Local & Remote Accesses 概要:不正アクセスを防ぐため、アカウント管理と特権管理のポイントについて記載

			頼性を契約前、契約後に確認していない **対象となる構成要素** • システム：遠隔診断サービス	
		③IT/OT DMZ による分離制御 **特徴** 連続稼働のなか数千台規模の装置ツールを製造システムと自動制御のうえ製造を行う OT 領域をサイバーセキュリティの脅威から守るために、IT 領域のネットワークやインターネットから DMZ を設けて分離を行う。 **考慮すべき観点** OT 領域と IT 領域及びインターネット等外部サービスとの通信について、データフローを明確にし、デフォルト拒否ポリシーと最小権限の原則に基づいた通信制御を行い、定期的な監査と継続的な見直しを実施する必要がある。 また、送受信されるトラフィックの中から異常な振る舞いを検知・防御する機能の検討を行う必要がある。	**想定されるセキュリティインシデント** • 故障や正確でないデータの送信、送信していない通信先へのデータ送信等が発生する **脅威** • 改ざん等された正規なモノ/システムからの適切でないデータの受信 **脆弱性** • 通信開始時に、通信相手を識別・認証していない • 通信経路上でデータが十分に保護されていない • 組織外部への不正な通信を適切に検知し、遮断する等の対応ができない **対象となる構成要素** • モノ：IT/OT DMZ 機器 **【CPSF 脆弱性 ID】** • L2_3_c_SYS • L3_2_b_DAT • L3_3_a_SYS	**【NIST CSF2.0 半導体製造プロファイル】** • ID.AM-03 ネットワークデータフロー管理 Fab：複雑なデータフローの管理 • PR.DS-02 伝送データのセキュリティ保護 Fab：M2M 通信データの保護 • PR.PS-04 ログ記録の管理 Fab：レガシー機器のログ管理 • PR.IR-01 無許可の論理アクセスからの保護 Fab：無許可の論理アクセスからの保護 • PR.IR-02 技術資産の環境脅威からの保護 Fab：クリーンルーム環境の管理 • PR.IR-03 レジリエンスの確保 Fab：レジリエンスの確保 • PR.IR-04 リソース容量の確保 Fab：リソース容量の確保 • DE.CM-01 ネットワーク監視 Fab：専門的な監視ソリューション • DE.CM-03 人員・技術利用の監視 Fab：人員の活動の監視 • DE.CM-06 外部サービスプロバイダの監視 Fab：外部サービスプロバイダの監視 **【CPSF 対策要件 ID】** • CPS.AM-4 • CPS.AM-5 • CPS.AC-3 • CPS.AC-7 • CPS.AC-8

				• CPS.DS-6 • CPS.DS-9 • CPS.AE-1
				【SEMI E187 製造リファレンス】 3.10 Security Key Performance Indicators 概要:持続可能なセキュリティ運用管理を実現するためのセキュリティ KPI について記載

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

半導体デバイス工場のビジネス目的に合わせたリスクマネジメントを達成するために、組織・人の側面による特徴と考慮すべき観点を、想定されるセキュリティインシデントとリスク源の視点から以下の7つにまとめ、グローバルな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。

表 3-9. 半導体デバイス工場の組織・ヒト側面の分類

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

表 3-10. 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

領域・エリア	特徴及び考慮すべき観点	CPSF 想定されるセキュリティインシデント/リスク源（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/CPSF/SEMI E187 製造リファレンス
組織的対応	**①ガバナンス（ビジネス環境の理解、役割・責任・権限の確立）** **特徴** 半導体デバイス工場は、生産の可用性・品質を守り供給責任を果たすとともに、生産機密情報（自社及び他社）の保護、人的被害や環境への影響を含めた法的対応のビジネス環境がある中で、産業スパイを含めた国家支援型 APT 攻撃等サイバーセキュリティの危険性が高い状況を理解した上で役割・責任・権限の確立が必要である。 **考慮すべき観点** 半導体デバイス工場は OT 領域（ファブ、ファブシステム、ファシリティ）のリスクがより高く、重要性が高いビジネス環境を理解し、OT 領域での役割・責任・権限の確立を行う必要がある。 OT セキュリティ対策が単なる技術的課題ではなく、事業リスクマネジメントとして位置づけられるように、経営層の強いコミットメントを確保する必要がある。また、OT セキュリティ専門家として、IT セキュリティの知識に加え、半導体製造プロセスに深い理解を持つ人材の確保・育成を行うことが求められる。	**想定されるセキュリティインシデント** • セキュリティインシデントにより適切に事業継続できない **脅威** All threats **脆弱性** • セキュリティ事象を的確に検知するための体制が構築されていない • 自組織と他組織（サプライヤ等）との連携状況及び責任分界を把握していない **対象となる構成要素** • ソシキ: デバイスメーカー **【CPSF 脆弱性 ID】** • L1_1_a_ORG • L1_3_a_ORG • L1_3_b_ORG • L1_3_c_ORG	**【NIST CSF2.0 半導体製造プロファイル】** • GV.OC-01 組織のミッションの理解 Eco:組織の目標・プロセスの理解 • GV.OC-02 ステークホルダーの理解 Eco:ステークホルターの要件の理解 • GV.OC-05 組織の成果・能力の理解 Eco:サプライチェーンの役割を定義・連携 • GV.RR-01 組織のサイバーセキュリティ責任 Eco:組織の方向性の明示とサポート • GV.RR-02 サイバーセキュリティマネジメント Eco:役割・責任・権限の明示 • GV.RR-03 リソースの割り当て Eco:サイバー戦略へのリソースの割り当て • GV.SC-02 役割・責任の確立 Eco:サプライヤの期待と組織の目標の一致 • RC.CO-03 復旧状況の伝達 Eco:復旧状況の伝達 **【CPSF 対策要件 ID】** • CPS.AM-7 • CPS.BE-1 • CPS.BE-2 • CPS.GV-1 • CPS.RM-1 • CPS.DP-1 • CPS.CO-3

	②法規制・業界標準対応（人命の確保及び環境安全の維持） **特徴** 半導体産業のセキュリティに関する国内外の法規制や国際標準は常に変化している。半導体デバイス工場においては、可燃性や毒性のあるガス、強酸、強アルカリ溶剤等の有害化学物質、X 線や紫外線等の放射線、高電圧、高温、稼働機器（巻き込み、挟み込み、衝突）等により、人命及び環境へのリスクが生じ、その影響に対して、法的（環境関連法や労働安全衛生法）準拠対応が必要である。 また、デジタルの要素をもつ製品をサイバーセキュリティの脅威から消費者を守る目的とした欧州サイバーレジリエンス法への対応についても今後準拠が必要となる。特にセキュリティ関連機能を備えるマイクロプロセッサ・コントローラ、耐タンパ性マイクロプロセッサ・コントローラ等、重要なデジタル製品としての対応が必要となる。 **考慮すべき観点** 半導体産業のセキュリティに関する国内外の法規制や国際標準の最新の動向を継続的に確認し、適切に組織内のルールを策定・運用する必要がある。合わせて、顧客となる業界標準（例：車業界 TISAX）も含めて対応する必要がある。	**想定されるセキュリティインシデント** • 法制度等で規定されている水準のセキュリティ対策を実装できない **脅威** All threats **脆弱性** • 遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを策定・運用していない • 遵守すべき法制度等を認識していないか、法制度に準拠した組織内のルールを遵守していない • 組織内で規定されているプロシージャが関連する法規制等を遵守するような内容となっていない **対象となる構成要素** • ソシキ：デバイスメーカー 【CPSF 脆弱性 ID】 • L1_1_a_SYS • L1_2_a_ORG • L1_2_a_COM • L1_2_a_SYS • L1_2_a_PRO • L1_2_a_DAT	**【NIST CSF2.0 半導体製造プロファイル】** • GV.OC-03 法的・規制上の要求事項の管理 Eco：業界フレームワークへの遵守 **【CPSF 対策要件 ID】** • CPS.GV-2 • CPS.GV-3 • CPS.DP-2

	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） **特徴** 半導体は、各産業に利用される経済安全保障上の重要物資である。また、顧客へ半導体チップの性能仕様や精度等の品質条件を満たすとともに、安全な環境で生産での説明を含めた供給責任を果たす必要がある（顧客から確認が求められる）。 半導体デバイス工場は、クリーンルーム・ファシリティ環境設備と全自動プロセス生産を構成する装置ツールや搬送機を利用し、工場当たりの建設費用が 100 億円以上と高額となるため業界生産能力が限られる。（容易な工場増減はない） 半導体の生産リードタイムは、3 か月～5 か月と比較的長いため、デバイス工場の生産ライン停止時の損失影響を踏まえた対策やリスク許容度の設定が必要となる。 **考慮すべき観点** 供給責任に対しては、生産ライン停止影響を踏まえた安全在庫の設定（例 20 日分等）のうえ、状況に合わせたサイバーセキュリティ対応を行う必要がある。 合わせて、インシデント発生時に生産に関わる被害範囲を極小化し、供給への影響を抑えるための対策や運用体制等の整備を行う必要がある。 供給責任が大きい場合には、ふるまいや異常検知等のモニタリングを強化し、影響範囲を極小化するマイクロセグメンテーションによる対応等のリスク対策強化を検討する必要がある。顧客から求められるサプライチェーンでの製品品質として、安全な製品設計とともに、安全な環境で製造がおこなわれていることを説明する必要がある（半導体に意図的に組み込まれる悪意のある機能や回路であるハードウェアトロージャンは、設計だけではなく、製造工程で行われる可能性も踏まえた対策や、検査工程での検出が必要である）。	**想定されるセキュリティインシデント** • 自組織のセキュリティインシデントにより自組織が適切に事業継続できない • 自組織のセキュリティインシデントにより関係する他組織が適切に事業継続できない • 関係する他組織のセキュリティインシデントにより自組織が適切に事業継続できない **脅威** All threats **脆弱性** • 必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない • セキュリティ事象による被害を受けたモノ（製品）・サービスが生じる • 自組織が提供する/されるモノ（製品）に関する記録が保持されていない **対象となる構成要素** • ソシキ：デバイスメーカー **【CPSF 脆弱性 ID】** • L1_1_a_ORG • L1_1_a_PRO • L1_1_b_ORG	**【NIST CSF2.0 半導体製造プロファイル】** • GV.OC-04 外部ステークホルダーの理解 Eco：組織の防御能力の向上 • GV.RM-05 コミュニケーションラインの確立 Eco：サプライチェーンリスク管理プロセス • GV.SC 全て サイバーサプライチェーンリスクマネジメント • ID.AM-04 サービス管理 Eco：インベントリの維持 • PR.IR-03 レジリエンスの確保 Eco：回復メカニズムの実装 **【CPSF 対策要件 ID】** • CPS.SC 全て • CPS.BE-3 • CPS.RP-4 • CPS.AM-2 • CPS.AM-3

		• L1_1_b_PRO	
	④生産機密情報の保護 **特徴** 半導体デバイス企業では、回路設計図、製品ロードマップ、顧客契約等の機密データとともに、半導体デバイス製造におけるレシピやプロセス編成（フローや条件等）等、生産における利益に関わる歩留まりや、製造の実現性による顧客獲得等、生産技術の競争力の重要な生産機密情報を扱っており、厳密な管理が行われる。 **考慮すべき観点** 生産機密情報は、クリーンルーム内に設置される装置ツール自身（メーカー型番）やその設置レイアウトの物理内容、装置内に含まれる設定データなどが該当する。そのため、工場内への入室者の許可制限や撮影規制の実施など、保護プロセスを設けて監視・監査を行う運用が必要である。 生産機密情報が含まれる装置ツールは、装置メーカーによる保守契約により、フィールドサポートメンバーによる常駐・訪問・遠隔から装置ツールへの保守メンテナンス権限でのアクセスが行われるため、厳密なアイデンティティ管理、認証及びアクセス制御が必要である。	**想定されるセキュリティインシデント** • 自組織の保護すべきデータが漏洩、改ざんされる **脅威** • 悪意あるエンティティによる保護すべきデータの持出し • 媒体の物理的な破壊 • 正規ユーザーへのなりすまし **脆弱性** • 定められた機密区分に沿った情報の保護が実装されていない • データを保管する組織、システム等の安全性を確認していない • 保管情報へのアクセスについて、情報の機密レベル等に合わせた方式でリクエスト元を識別・認証していない **対象となる構成要素** • ソシキ：デバイスメーカー • ソシキ：保守契約メーカー（装置、設備、部素材メーカー等） **【CPSF 脆弱性 ID】** • L1_1_a_DAT • L1_1_a_SYS	**【NIST CSF2.0 半導体製造プロファイル】** • ID.AM-05 資産の重要度 Eco：資産の重要度 • PR.IR-02 技術資産の環境脅威からの保護 Eco：環境的脅威からの保護 • RC.RP-04 運用規範の確立 Eco：運用規範の確立 **【CPSF 対策要件 ID】** • CPS.AM-6 • CPS.BE-3 • CPS.DS-8

		• L1_1_b_SYS • L3_1_a_DAT • L3_1_a_SYS • L3_1_c_ORG	
	⑤リスクマネジメント・ポリシー・レジリエンス **特徴** 半導体デバイス工場においては、特に OT 領域におけるサイバーセキュリティの影響度が高く、OT 領域の自社における状況を正しく把握するためのリスク評価、マネジメント、ポリシーの作成、BCP へのサイバーセキュリティ対策等の盛り込みが必要である。 **考慮すべき観点** 半導体デバイス工場の特徴や考慮すべき観点を踏まえ、自社のビジネス状況に合わせたリスクマネジメント、ポリシー、事業の継続計画を行うことが必要である。	**想定されるセキュリティインシデント** • セキュリティインシデントにより自組織が適切に事業継続できない **脅威** All threats **脆弱性** • セキュリティに関わるリスクマネジメントの適切な手順が確立していない • 適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない **対象となる構成要素** • ソシキ:デバイスメーカー **【CPSF 脆弱性 ID】** • L1_1_a_ORG • L1_1_a_PRO • L1_1_b_ORG • L1_1_b_PRO • L1_1_c_ORG • L1_1_c_PRO	**【NIST CSF2.0 半導体製造プロファイル】** • GV.RM 全て リスクマネジメント戦略 • GV.PO 全て ポリシー • GV.OV 全て 監督 • ID.IM 全て 改善 **【CPSF 対策要件 ID】** • CPS.GV 全て • CPS.RA-4 • CPS.RA-6 • CPS.GV-4 • CPS.RM 全て • CPS.SC-6 • CPS.SC-7 • CPS.SC-11 • CPS.IP-7 • CPS.DP-4 • CPS.RP-3 • CPS.CO-2 • CPS.CO-3 • CPS-IM 全て

	⑥運用(監視・対応・復旧・改善) **特徴** インシデント発生時の事業への影響を軽減することを目標に、ネットワークとシステムを監視してセキュリティ侵害の兆候を確認し、データ分析により脅威やインシデントの発生を判断する。また、適切なアクションを取ってインシデントを封じ込め、早期に修復を行う必要がある。 **考慮すべき観点** サイバー脅威の検出と対応の目標は、早期アラートに対応してデータ損失を防ぎ、影響を最小限に抑え、可能な限り迅速に業務を復旧させることである。なお、重要となる資産に対してインシデントの検知や追跡に関するログ取得の防御対策を行い、工場の OT 領域に特化したインシデント対応態勢(FSIRT)の構築を行う必要がある。 **具体的対策事例** 対策検討を進める上で、参考となる具体的な事例を第 4.3 節に示す。	**想定されるセキュリティインシデント** • セキュリティインシデントにより自組織が適切に事業継続できない **脅威** All threats **脆弱性** • セキュリティ事象を的確に検知するための体制が構築されていない • セキュリティインシデントに的確に対応するための体制が構築されていない • セキュリティインシデント発生時に適切なアクションを取ることができない • 自組織におけるセキュリティインシデントへの対応手順が策定されていない • BCP にセキュリティインシデントが位置づけられておらず、セキュリティインシデント発生時に自組織の事業継続に支障が生じる **対象となる構成要素** • ソシキ:デバイスメーカー **【CPSF 脆弱性 ID】** • L1_3_a_ORG • L1_3_a_PEO	**【NIST CSF2.0 半導体製造プロファイル】** • DE.AE 全て 有害事象の分析 • RS.MA 全て インシデント管理 • RS.AN 全て インシデント分析 • RS.CO 全て インシデント対応の報告とコミュニケーション • RS.MI 全て インシデントの軽減 • RC.RP 全て インシデント復旧計画の実行 • RC.CO 全て インシデント復旧のコミュニケーション **【CPSF 対策要件 ID】** • CPS.AE 全て • CPS.DP-2 • CPS.DP-3 • CPS.RP 全て • CPS.CO 全て • CPS.AN 全て • CPS.MI 全て **【SEMI E187 製造リファレンス】** 3.8 Prevent, Detect and Response 概要:ファブエリアを保護するためのセキュリティ監視、サイバー攻撃の検知、封じ込め、復旧のポイントについて記載

<table>
<tr><td></td><td></td><td>・L1_3_a_DAT
・L1_3_a_PRO
・L2_1_b_PRO
・L2_1_c_PRO
・L2_2_a_PRO</td><td></td></tr>
<tr><td></td><td>⑦意識向上とトレーニング
特徴
半導体デバイス工場は、工場停止時における事業への影響が大きく、ファブエリアでは、各企業の競争力につながる生産機密情報の取り扱いがあり、産業スパイを含めた国家支援型 APT 攻撃等危険性が高い状況である。半導体デバイス工場においては、生産プロセスを支える従業員及び装置メーカー設備メーカーの常駐者含めた業務委託者とともに非常に多くのヒトによって支えられている。

考慮すべき観点
BCP には、サイバーセキュリティのリスクが考慮されており、脆弱面を狙った攻撃に備え、OT 領域のすべての関係者（従業員・業務委託者等）へ OT 領域を含めたサイバーセキュリティ教育・訓練を実施する必要がある。
OT 領域のサイバーセキュリティ教育・訓練の内容は、事業を取り巻くサイバーセキュリティ脅威や脆弱性に応じて定期的に見直す必要がある。
OT セキュリティを担う人材への、定期的に実践的なトレーニングやシミュレーションを通じて、インシデント対応能力を定期的に向上させるとともに、スキルマップを整備することで継続的な現場力強化と属人化の防止が可能となる。</td><td>想定されるセキュリティインシデント
・セキュリティインシデントにより自組織が適切に事業継続できない

脅威
All threats

脆弱性
・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない
・自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない
・セキュリティインシデント発生時に適切なアクションを取ることができない

対象となる構成要素
・ソシキ：デバイスメーカー

【CPSF 脆弱性 ID】
・L1_1_a_PEO
・L1_1_b_PEO</td><td>【NIST CSF2.0 半導体製造プロファイル】
・PR.AT 全て 意識向上とトレーニング
・ID.IM-02 改善点の認識
Eco：サプライチェーン全体の改善点の認識

【CPSF 対策要件 ID】
・CPS.AT 全て
・CPS.SC-9

【SEMI E187 製造リファレンス】
3.9
User Awareness Training
概要：新たな脅威に適切に対応することを目的としたユーザー教育とトレーニングに関するポイントについて記載</td></tr>
</table>

		• L1_1_c_PEO • L3_3_a_PEO • L3_4_a_PEO • L3_4_b_PEO	

4 半導体デバイス工場における具体的対策例

第 4 章では、第 2 章で定義したリファレンスアーキテクチャと第 3 章で整理した関連フレームワークの対策項目を基に、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具体的対策事例について紹介する。

表 4-1. 具体的対策事例

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（3.3-⑥）
4.4	物理アクセスの制限（入室・持込み・接続） - ファブエリアにおける物理的対策（3.2.1-⑤）

4.1 装置ツールの資産管理と脆弱性評価

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。本章では以下の 5 つに分けて具体的な対策事例を紹介している。

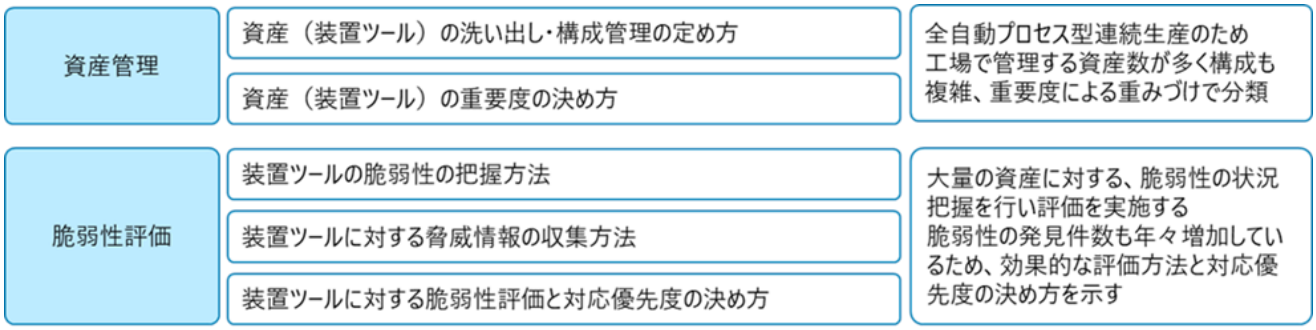


図 4-1. 装置ツールにおける効果的な資産管理と脆弱性評価

4.1.1 資産(装置ツール)の洗い出し・構成管理の定め方

半導体デバイス工場では、1 つの工場につき 400 を超える工程プロセスがあり、工程間の搬送を含めて(数千台に上る)非常に多くの装置ツールがシステムで連携制御され、製造が行われる。また、各装置ツールは各工程で必要な機能と性能の要件を満たすために、フロント PC や DCS、PLC、アクチュエーター、センサ等の多数のハードウェアデバイス(搬送装置は OHT、ストッカー、FOUP 等)と、複数システムとの連携や内部デバイスを制御するためのソフトウェアコンポーネントから構成されている。また、装置ツール内には、設計情報やレシピ等の生産機密情報が保管・管理されている。以下では、装置ツールにおける資産管理の洗い出し・構成管理の対策事例を示す。

ファブエリアの資産管理では、中心となる装置ツールは台数が多く、複雑な内部構成の中に生産機密情報を含んでいる。そのため、ハードウェアデバイス、ソフトウェアコンポーネント、機密情報、セキュリティ対策情報の側面から管理対象範囲を定める必要がある。セキュリティ対策に効果的な資産管理を行うためには、脆弱性評価が効率的に運用可能となる構成管理の対象を定めることが有効である。

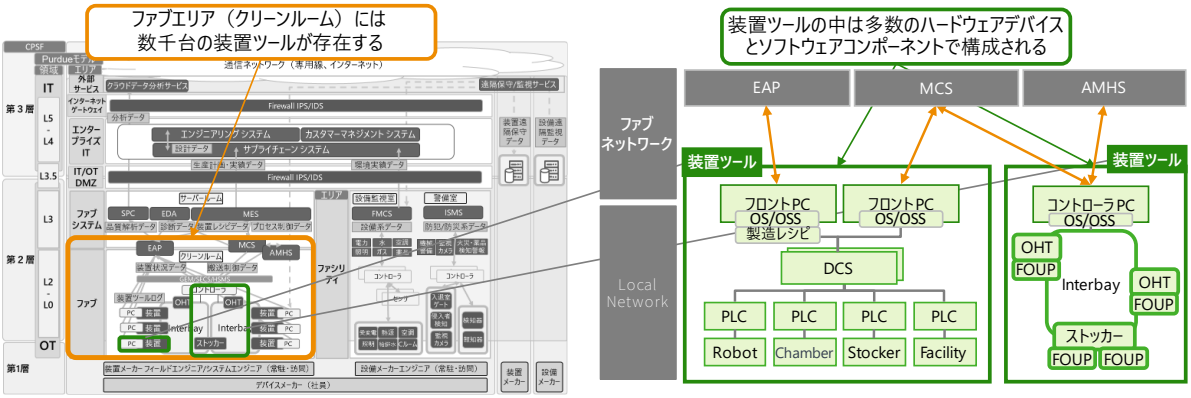


図 4-2. ファブエリアにおける資産構成

ファブエリアでは製造工程に関わるすべての装置ツールを対象に、資産の洗い出しを行うことが必要である。洗い出した装置ツールの資産に対して、脆弱性管理の視点から装置ツール内のハードウェアデバイス、ソフトウェアコンポーネント、機密情報、セキュリティ対策情報について構成把握及び管理を行うことが求められる。

- 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、上記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（Open Source Software）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（E187.00-RQ-00001-00 及び RQ-00002-00）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（EPP、ハードニング対策）、アクセス制御（特権分離管理）、ネットワーク管理（マイクロセグメンテーション、通信制御条件）、セキュリティモニター（イベントログ、EDR、NDR）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。

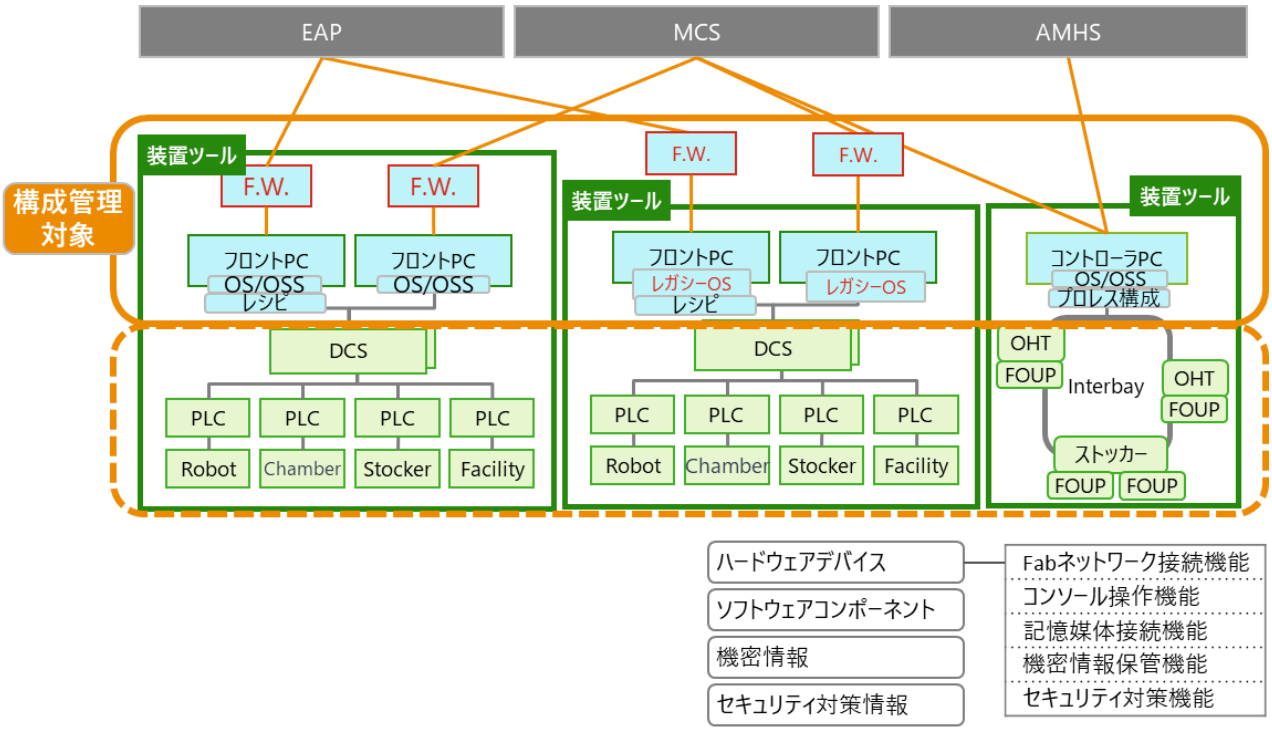


図 4-3. ファブエリアにおける構成管理対象

なお、装置ツールは平均的な利用期間が 20 年強であり長期間にわたり使用される。この期間中には、装置の機能改善や強化、セキュリティ対応等に伴い、ハードウェアデバイスやソフトウェアコンポーネントの変更が行われるため、それに

応じた継続的な構成管理の見直しを実施する必要がある。

装置ツールの構成管理対象は、効果的な資産管理と脆弱性管理を行うために、対象となるハードウェアデバイスやソフトウェアコンポーネントを絞り込んでいる。ただし、デバイスメーカーと装置メーカーとの間で締結されるフィールドサポート保守契約の中で、装置ツールのセキュリティ対策に関する構成管理方法（SBOM情報の提供、脆弱性の評価、セキュリティパッチ提供が行われる対象範囲）を確認し、運用することが望ましい。

参考情報として、業界団体 SEMI では、ファブネットワークに接続される装置ツール内のコンピュータデバイスに対して、OS 情報等サイバーセキュリティのステータスレポート情報を取得するフレームワークを 2024 年 10 月に標準化（SEMI E191[9]）した。今後、装置ツールの提供機能として実装が進むと考えられる。

また、装置ツールにおける構成管理の進め方については、経済産業省『ソフトウェア管理に向けた SBOM の導入に関する手引 ver2.0』[10]の第 4-1 節「SBOM 適用範囲の明確化」が参考となる。

4.1.2 資産（装置ツール）の重要度の決め方

半導体産業では国家支援型 APT 攻撃も発生しており、攻撃者は常に具体的な目的を持ってサイバー攻撃を仕掛けてくる。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。

工場における資産の重要度の決め方は、各企業のビジネスリスク要件に基づき行われるが、この対策事例では、半導体デバイス工場へのサイバー攻撃のリスクを踏まえ、守るべき資産の重要度の判断基準と、効率的な重要度の定め方を示す。

半導体デバイス工場における資産の重要度判断基準

重要度を決める基準は、半導体デバイス工場の守るべき生産目標、半導体品質の維持、生産機密情報の保護、人命・環境の維持に対して、以下のリスク領域に

[9] https://store-us.semi.org/products/e19000-semi-e191-specification-for-computing-device-cybersecurity-status-reporting
[10] https://www.meti.go.jp/press/2023/07/20230728004/20230728004.html

分けて重要度（高・中・低）の参考例を示す。なお、重要度の各基準値は業界の実態を基にした参考例であり、各工場のビジネス状況に応じて適切に設定する必要がある。

① **生産目標・供給責任に対する重要度判断**

半導体デバイス工場における生産は、生産リードタイムが長く（3～6 か月）、業界の生産キャパシティに余力が小さいため、安全在庫を上回る生産停止が発生した場合、半導体利用顧客への供給責任が果たせず、サプライチェーン全体にリスクが生じる。特に前工程においては、プロセス型製造で繰り返しシリコンウェーハに回路形成が行われる。この重要工程で利用される装置ツールにおいて、長時間の性能低下や停止を引き起こすインシデントが発生した場合、計画された生産数を確保できず、納期を守れなくなる等、事業に大きな影響を及ぼす可能性がある。さらに、一度生産が停止すると、再稼働までに多くの時間とコストがかかり、投入されたウェーハは全損・廃棄となる可能性がある。

対象となる資産が損なわれた場合、生産目標に関しては生産の停止日数、供給責任に関しては市場供給の停止日数を基にして重要度を決めることが有効である。

② **半導体品質の維持に対する重要度判断**

半導体製造の各工程で品質を検査するために利用される検査装置ツールは、製造物責任法（PL 法）を含む半導体の品質保証に加え、製品が正しく製造されるための信頼性（例：製造工程でチップに対してハードウェアトロージャン等の不正な侵入・改ざんが行われていないこと）を考慮する必要がある。

対象となる資産が損なわれた場合、歩留まりへの影響については歩留まり率、市場品質への影響については市場品質不良や PL 法の影響の有無を基にして重要度を決めることが有効である。

品質に関わる各国の法令として、製造物責任法（PL 法）や EU サイバーレジリエンス法（CRA）等があり、これらの法令違反による損害賠償請求や制裁措置のリスクも考慮する必要がある。

③ **人命・環境、法令順守に対する重要度判断**

半導体の生産工程における装置ツールでは、人体や環境に有害となる無機化合物や放射性物質の利用、ウェーハ洗浄後の水質汚染、プラズマ生成後の排ガスによる大気汚染等に対するセーフティ（安全）確認を行う必要がある。また、セキュリティインシデントが起きた場合の影響も併せて確認する必要がある。さらに、環境関連法や労働安全衛生法等、法的規制への

直接の影響についても確認する必要がある。
対象となる資産がセキュリティインシデントによって損なわれた場合、人命については障害の危険性、環境については地域社会への影響、法規制については環境関連法や労働安全衛生法への影響に照らして重要度を決めることが有効である。
なお、セーフティ(安全)については、IPA が公開している『制御システムセーフティ・セキュリティ要件検討ガイド』[11]が参考となる。

④ **生産機密情報の保護に対する重要度判断**
各装置ツールには、製品品質・歩留まりに影響するレシピ情報や設定パラメータ、競争力の源泉となる機密情報や設計情報を含む他社技術情報等の生産機密情報が保管されている。そのため、各装置ツールで管理する生産機密情報が競合他社へ漏洩した場合の、事業への影響や損失についても考慮する必要がある。
対象となる資産が損なわれた場合、生産機密情報の保護については、損失の想定金額を基に重要度を決めることが有効である。

⑤ **装置ツールによる財務上影響にする重要度判断**
装置ツールはナノテクノロジーを実現するための高度な技術が組み込まれているため、1 台当たりの資産価値が高額となる。そのため、資産の破壊や損傷を想定した上で、重要度を判断する必要がある(例:微細化が進む露光工程の装置ツールは、他の工程の装置ツールに比べ特に高額な資産価値を持つ)。

判断基準を具体化する際の参考情報として、『IEC 62443-2-1』の「Annex A.2.3.3.7(Table A.2 – Typical consequence scale)」及び、IPA『制御システムのセキュリティリスク分析ガイド』[12]の「4.2 資産の重要度」に示された、リスク分析のための典型的な結果の尺度例を、表 4-2 に示す。

本表は、資産が攻撃され被害が発生した際のリスク(被害の大きさ)を 3 段階で分類し、その値を基に資産の重要度を定義するための判断基準になる。

また、サイバーセキュリティ攻撃による、経営資源が被害を受ける内容も考慮する必要がある。

[11] https://www.ipa.go.jp/archive/digital/iot-en-ci/mieruka/20180319.html
[12] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

表 4-2. 装置ツールの重要度

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	

参考）サイバーセキュリティ攻撃によって、経営資源が被害を受ける内容

経営資源	被害内容
ヒト	装置ツール・ファシリティ設備の誤作動等による労働災害（従業員の死傷）の発生
モノ	装置ツール・ファシリティ設備の破損、シリコンウェーハの全損・廃棄、製品の品質（歩留まり）・安全性等の低下
カネ	収益機会の喪失、損害・費用の発生
データ	生産機密情報（レシピ等）や新工程・新技術に関する情報等、重要な情報資産の流出
レピュテーション	道義的責任、取引先との契約違反、信頼関係の毀損、ブランドイメージへの悪影響

半導体デバイス工場において、大量の資産を効率的に管理し重要度を定めるには、個々の資産に対して個別に判断を行なうのではなく、BCP と同様にビジネスリスクに基づいて業務単位で分け、その中の資産を同様の機能でまとめた資産グループ単位で重要度の判断を行うことが可能である。

特に資産の多いファブエリアの装置ツールに対しては、業務単位として供給責任に基づき生産ライン単位(ウェーハサイズ別ライン)で分け、さらに生産工程(酸化・塗布・露光・検査等)の機能単位で装置ツールを資産グループ単位としてまとめて重要度を設定するのが効率的である。

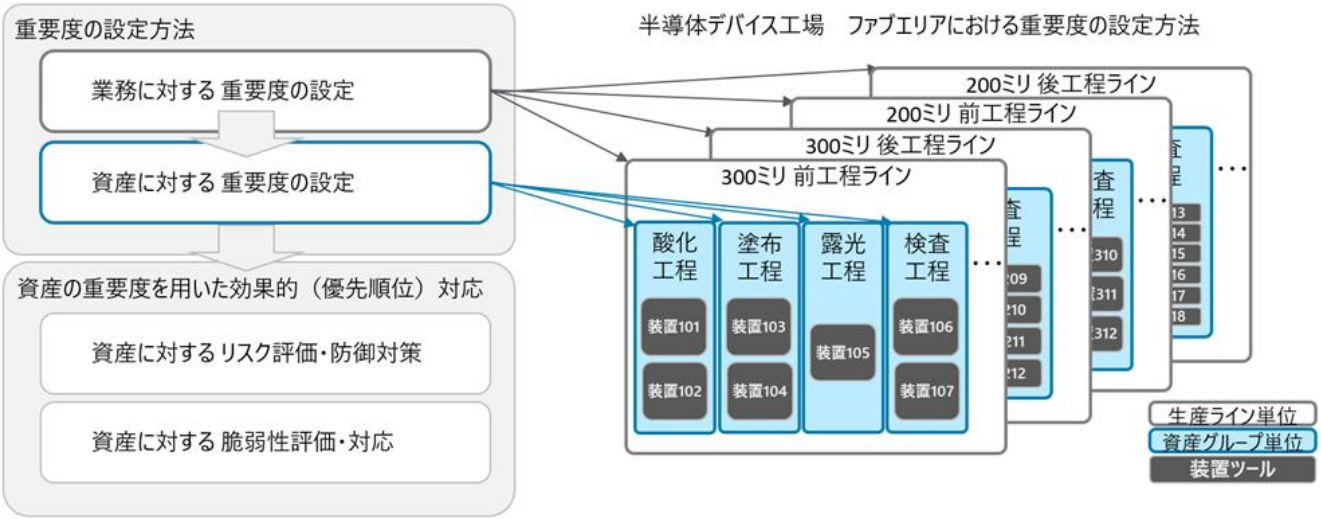


図 4-4. 重要度の効率的な設定

以下に、半導体デバイス工場のファブエリアにおける、装置ツールの資産の重要度の算出例を示す。

ファブエリアの装置ツールの資産は、業務単位である生産ライン、資産を機能別のグループとして分けた工程単位で装置ツールをまとめて、重要度の基準として定めた各リスク領域に対して、重要度の算出を行う。

なお、生産ライン、工程別にまとめた資産グループに対して、社内の既存運用である以下の情報を参考に重要度を判断することが効果的である。

- 事業継続性:事業継続計画情報
- 半導体品質及び産業活動の安全性:工程品質管理情報(工程 FMEA)
- 法規制等の厳守:工程品質管理情報及び機密管理情報
- 機密情報:機密管理情報
- 財務影響:固定資産情報

リスク領域				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（業務・資産）							資産価値の影響	
業務単位 生産ライン		資産グループ単位 工程		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
ウェーハ サイズ	ライン	工程 装置グループ	装置 数	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	資産の破損
300㎜	前工程	酸化	2	中	中	低	低	**高**	**高**	**高**	中	
		塗布	2	中	中	中	低	中	中	中	中	
		露光	1	**高**	**高**	中	低	中	中	中	**高**	
		検査	2	中	中	**高**	低	低	低	低	**高**	
	後工程	ダイジング	4	中	低	低	低	低	低	低	低	
		ボンディング	4	中	低	低	低	低	低	低	低	
		検査	4	中	低	**高**	**高**	低	低	低	中	
200㎜	前工程	酸化	3	低	低	低	低	**高**	**高**	**高**	低	
		塗布	3	低	低	中	低	中	中	中	低	
		露光	3	低	低	中	低	中	中	中	中	
		検査	3	低	低	**高**	低	低	低	低	中	
	後工程	ダイジング	6	低	低	低	低	低	低	低	低	
		ボンディング	6	低	低	低	低	低	低	低	低	
		検査	6	低	低	**高**	**高**	低	低	低	低	

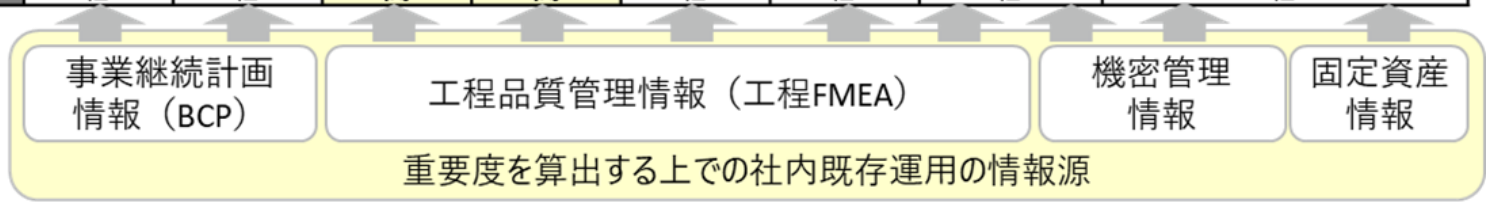


図 4-5. 装置ツールの資産の重要度算出例

経済産業省『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』[13]の「3 セキュリティ対策企画・導入の進め方」や「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」が重要度の設定方法の参考となる。

4.1.3 装置ツールの脆弱性の把握方法

装置ツールの脆弱性評価を行うための基礎情報として、装置ツールの構成管理で対象としたコンポーネントに対する脆弱性情報を正確に把握することが必要となる。脆弱性情報の入手先や、年間 4 万件を超える脆弱性発見情報から装置ツールに対する脆弱性の把握方法の事例を示す。

脆弱性情報の入手先としては以下がある。

- 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
- 装置メーカーから提供される脆弱性情報による把握
- 脆弱性スキャンツール（SCAP スキャナー）を利用した把握

装置ツールの脆弱性の把握においては、IT 領域で行われる脆弱性情報の把握を行うとともに、より効率的な情報入手として、装置メーカーから提供される脆弱性情報（装置ツールでのセキュリティ対策を考慮して提供される）や脆弱性スキャンツール（SCAP スキャナー）を利用した把握が有効である。

また、装置ツールの資産数が多いため、運用工数を考慮し効率的な対応を行う必要がある。そのためには以下のような検討が可能である。

① 重要度の高い資産に対する脆弱性の把握を行い、優先順位をつける。
② 装置ツールの資産管理で洗い出したセキュリティ対策情報（マイクロセグメンテーションやアプリケーション実行許可型対策等）を踏まえて脆弱性を把握する対象を絞り込む。
③ 脆弱性の把握を行う対象資産の絞り込みを行った脆弱性情報入手を行う。

装置メーカーから提供される脆弱性情報に基づき、SEMI E187 及び 188 が推奨する装置ツールの脆弱性対応方法に関する基本要件を参考にすることで、脆弱性管理の要件を装置メーカーとのフィールドサポート保守契約書に含めることが可能である。これにより、脆弱性の把握が可能とする運用と体制構築を

[13] https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

効率的に進めることができる。(参考:『SEMI E187』の「9.2 Vulnerability Mitigation」、及び『SEMI E188』の「9.2 Checking for Vulnerabilities on the Manufacturing Equipment」)

さらに、装置ツールの台数や構成要素が多いことから、現状の追加保護対策を含めた脆弱性状況を効率的に把握する(一定の対策を講じた後に残留している脆弱性の有無を把握する)ために、脆弱性スキャンツール(SCAP スキャナー)を用いて、残存する脆弱性を把握することが効果的である。また、SEMI E187 COMPLIANCE GUIDANCE[14]による脆弱性スキャナーの推奨や、SEMI E188 で定められた基本要件を基に把握することも有効である。(参考:『SEMI E187 COMPLIANCE GUIDANCE』の「E187.00-RQ-00005-00 E187.00-RQ-00008-00」、及び『SEMI E188』の「9.4 NIST Security Content Automation Protocol (SCAP)」)

なお、脆弱性スキャンツールの利用に際しては、アクティブスキャンを用いるシステムツールの場合、性能影響(停止・低下)が発生する装置ツールが存在するため、スキャン方式やスキャン運用日時の調整等、適切な運用計画を策定したうえで実施する必要がある。

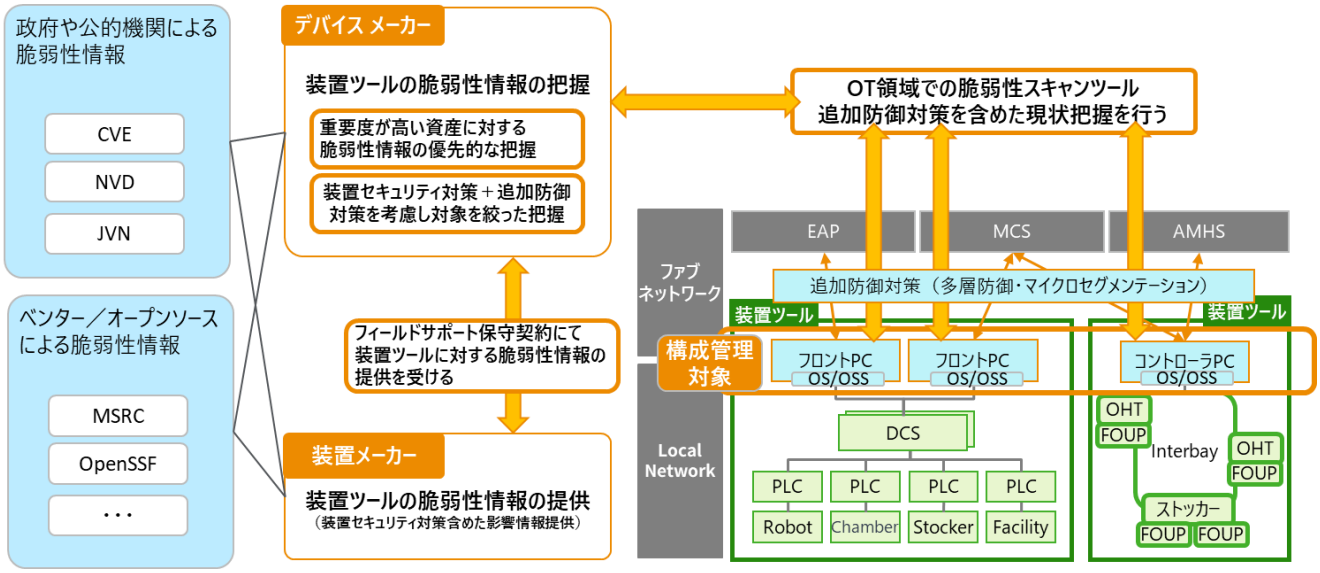


図 4-6. 装置ツールの脆弱性の把握方法

4.1.4 装置ツールに対する脅威情報の収集方法

半導体業界は、経済安全保障の視点から国家支援型 APT 攻撃等の高度な攻撃を受ける可能性が高い業界である。そのため、業界向けの脅威情報(深刻度の高い脆弱性に対する攻撃コードの作成・公開状況)やインシデントの発生情報(検

[14] https://www.semi.org/en/standards-watch-2025-aug/navigating-semi-e187-new-cybersecurity-white-paper

知された攻撃情報を含む）を収集し、出来る限り早期に対策を講じる必要がある。

脅威情報の収集方法として以下がある。

- 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[15]半導体産業 SIG からの情報収集
- 自社の攻撃・インシデント情報の分析結果からの情報収集

業界向けの脅威情報の収集対応については、米国では IT-ISAC Semiconductor Industry SIG が、国内においては、IPA の J-CSIP に半導体産業 SIG が設置され、活動を開始している状況である。

従来の政府や公的機関による公開情報、悪用が確認された脆弱性情報及び自社の攻撃・インシデント情報からの分析結果による情報収集にとどまらず、業界向けに共有された脅威情報を活用することで、OT 領域及びファブエリアの装置ツールに残存する脆弱性を狙った攻撃コード（エクスプロイトコード）の作成・公開状況の把握や、業界内の企業に対する攻撃状況（監視状況）の把握等について共有を行い、各種の対策を効率的に実施することが可能である。

脆弱性情報の把握に際しては、IPA が毎週月曜日に更新する『CISA が公開した制御システムの脆弱性情報（直近 1 ヶ月）』[16]を参考に、攻撃コード（エクスプロイトコード）の発生状況を確認することが有効である。

IPA J-CSIP（サイバー情報共有イニシアティブ）は、経済産業省協力のもと、2011 年から重要インフラ関連機器製造業者を中心に活動しており、サイバー攻撃の被害拡大防止を目的とした情報共有と早期対応の場を提供している。2025 年 4 月からは、半導体産業 SIG の活動も開始され、業界特化型の情報共有を推進している。

KEL、EPSS、LEV については、NIST のサイバーセキュリティホワイトペーパー『NIST CSWP 41 Likely Exploited Vulnerabilities』[17]が参考になる。

---

[15] https://www.ipa.go.jp/security/j-csip/about.html
[16] https://www.ipa.go.jp/security/controlsystem/icsadvisories.html
[17] https://csrc.nist.gov/pubs/cswp/41/likely-exploited-vulnerabilities-a-proposed-metric/final

4.1.5 装置ツールに対する脆弱性評価と対策優先度の決め方

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。IT 領域での脆弱性評価では、発見された脆弱性に対して CVSS の基本評価基準のスコアによる定量評価を行い、評価結果に応じたパッチ適用時期の調整、パッチ適用以前に講じる回避策の実施等の対応方法があるが、OT 領域の装置ツールへのパッチ適用に対しては性能への影響による制約や運用上の制約があるため、多くの場合、パッチ適用以外の回避策・低減策を含めた対応を検討する必要がある。

特に、半導体デバイス工場の OT 領域において、資産数の多い装置ツールの脆弱性評価を行う際には、効率的で実効性の高い評価方法を用いて、適切な判断を行う必要がある。

効果的な脆弱性評価を行うための対策事例:

脆弱性情報を把握するためには、装置メーカーと協力して対策が必要な脆弱性情報を特定することで、対応すべき優先順位を絞り込むことが可能となる。次に、脆弱性スキャナーを用いて対策実施後の残留する脆弱性を把握(シミュレーション含む)し、脆弱性の環境評価基準を加えた影響度を把握することが可能である。また、脅威情報の収集においては、J-CSIP 半導体産業 SIG や IT-ISAC Semiconductor Industry SIG が提供する業界脅威情報を活用することで、脅威評価基準を加味した影響度での判断を行い、対応すべき脆弱性をさらに絞り込むことができる。

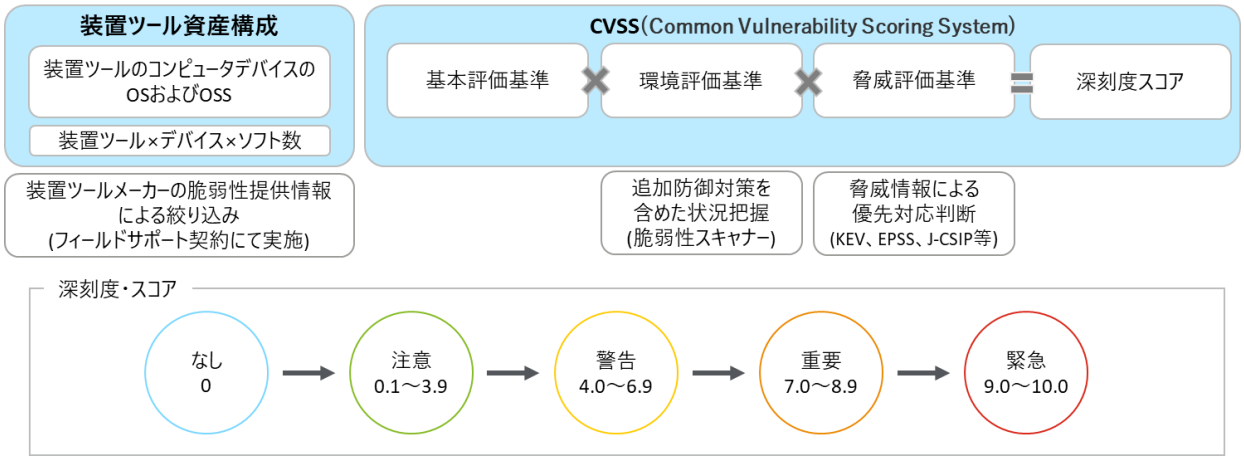


図 4-7. CVSS による脆弱性評価

【参考】装置ツールの資産の構成管理数は 1 万 8 千コンポーネントを管理
(装置ツール 2 千台×コンピュータデバイス数3台×ソフトウェアコンポーネント数×3個＝1 万 8 千)
2024 年の CVE データは 4 万件以上(前年 38%増)うち 10.0 (深刻度: Critical)も 231 件発生

SSVC では、環境特性を考慮し、対応判断を行うことが可能である。悪用状況(Exploitation)、防御状況(Exposure)、攻撃メリット(Utility)、業務影響(Impact)を基に、環境特性を考慮した対応判断(Priority)として緊急対応(Immediate)、計画外対応(Out-Of-Cycle)、計画対応(Scheduled)、未対応(Defer)が示される。

これにより、OT 環境での対応判断に迷う深刻度の高い脆弱性(攻撃コードが作成済みで攻撃をうける可能性があり、業務影響が大きいもの)について、客観的な対応判断を行うことが可能となる。実際の対応では、脆弱性の修正(パッチ適用)、回避(攻撃ルートの無効化)、低減(検知項目の追加、監視の強化)が行われる。

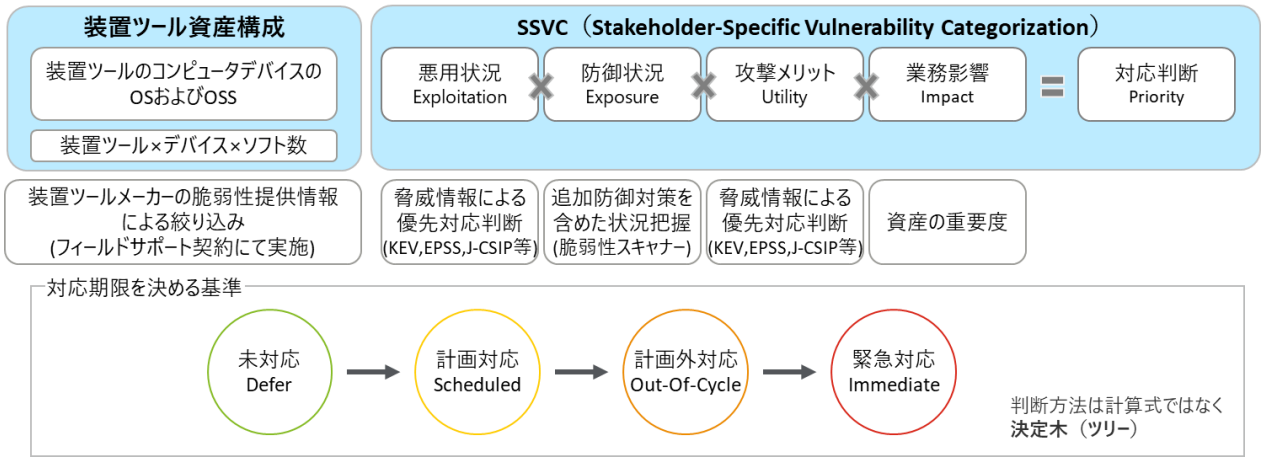


図 4-8. SSVC による脆弱性評価

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

OT 領域において、資産台数が多く脆弱性対応が難しい装置ツールは、長期利用によるサポートが終了した OS を利用している場合や機能・性能保証の観点からパッチ適用ができない、連続稼働によりパッチ適用日時が制限される等、多くの制約がある状況で運用される。さらに、装置ツールとファブシステム、あるいは

装置ツール間の通信は、暗号機能や認証機能を持たない業界通信プロトコルを利用して行われている。このため、生産継続において重要となる装置ツール及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である。

対策事例では、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。

- 多層防御は、サイバー攻撃の侵入口である入口対策だけではなく、攻撃侵入後の拡散経路や移動方向を考慮した用途や機能、セキュリティ対策状況に応じて細かくゾーンとコンジットに分けて守ることが重要である。これにより、インシデントが発生した場合のフォレンジック対象範囲の極小化や、ゾーン分割による影響範囲の封じ込め、早期復旧が可能になる。対策事例としては、第 2 章の半導体デバイス工場のリファレンスアーキテクチャにて定めた領域・エリアを基に 4 つの分離分割の例を示す。
- マイクロセグメンテーションは、パッチ適用が困難な装置ツールを、ゾーン分割とコンジット設定によって保護し、安全な利用を可能とする。
- ネットワークによるセキュリティ監視は、分割したゾーンのセキュリティ監視を行うことで、サイバー攻撃の初期段階を捉え、インシデント被害の発生を防止することが可能となる。

表 4-3. ネットワークセキュリティ対策概要

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	領域毎の分離と通信制限	多層防御: サイバー攻撃からの侵入容易性と被害拡大性を低減する	OT 領域の入口分離（IT 領域、インターネット領域から DMZ を設け分離する）
2	エリア毎の分離と通信制限		ファブシステム、ファブ（装置ツール）、ファシリティの機能
3	エリア内での分離と通信制限		ファブエリア内は、生産計画単位（建屋・フロアー毎の工程）
4	システム用途別の分離と通信制限		装置 I/F システム内（プロセス・搬送系、品質系、保全系等）
5	装置ツールを守るマイクロセグメンテーション	マイクロセグメンテーション	装置ツール自身の追加セキュリティ対策
6	ネットワークによるセキュリティ監視	セキュリティ監視	サイバー攻撃の初期段階を捉え、インシデント被害の発生を防止する検知

表 4-4. ネットワークセキュリティ対策詳細

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	**領域毎の分離と通信制限** 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）（図 4-9 のオレンジ枠箇所）
2	**エリア毎の分離と通信制限** 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で分割した上で通信制限を行う。（図 4-9 の青色枠箇所）
3	**エリア内での分離と通信制限** 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。図（4-9 の緑色箇所） 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。（図 4-10 の緑色枠箇所）
4	**システム用途別の分離と通信制限** ファブエリア内で工程別に分けられた中においても、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用途、故障予測や検知用のセンサ連携用途等、システム用途別にネットワークを分割し通信制御を行う。（図 4-11 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** 装置ツールにてレガシーOS の利用やパッチ適用ができない等、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。（図 4-12 の赤枠箇所） 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** 分割したネットワークに異常検知ツール（NDR）を導入し、異常アラートのログの記録と監視検知を行う。

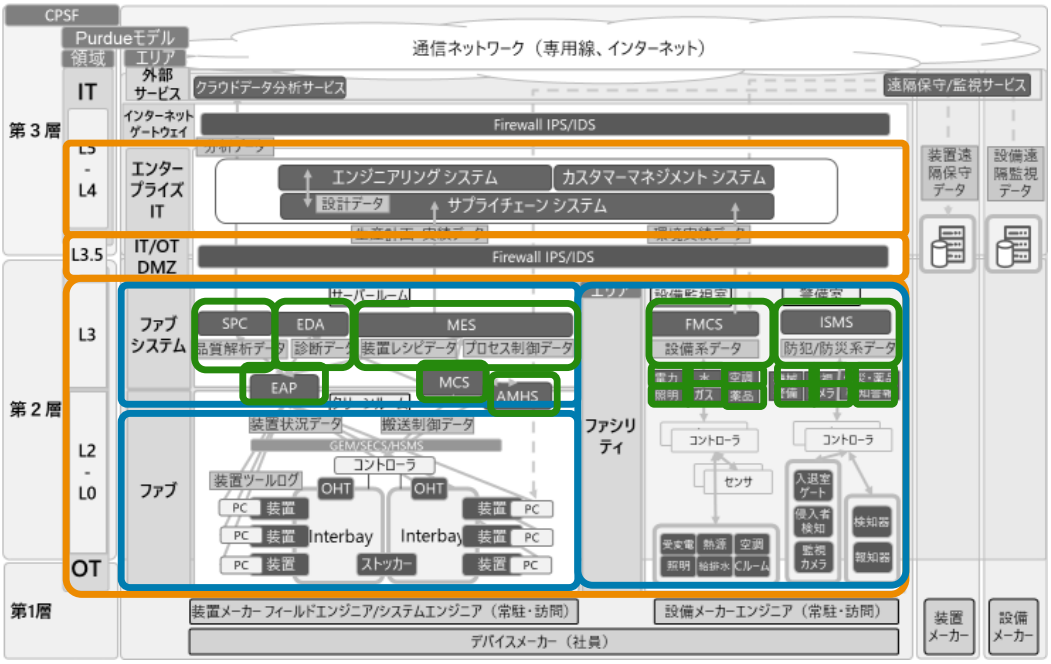


図 4-9. ネットワーク分離概要（領域・エリアレベル）

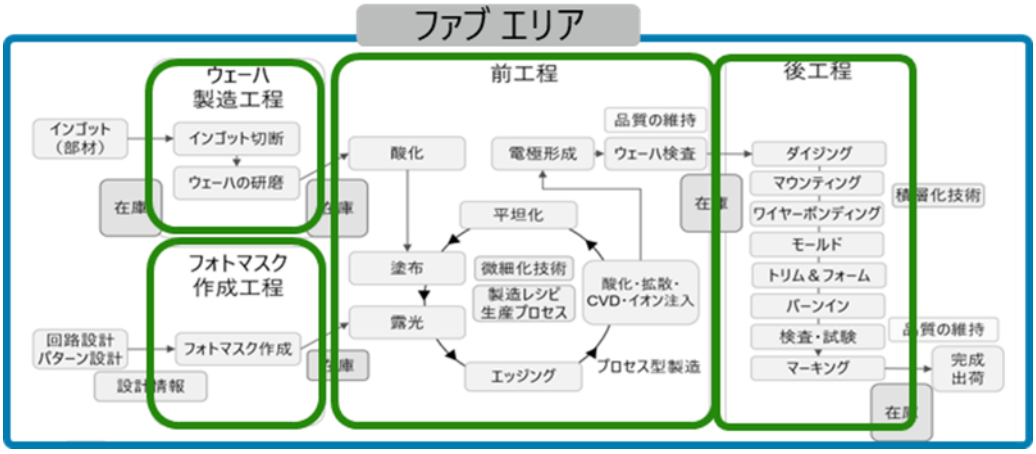


図 4-10. ファブエリアネットワーク分離詳細（工程レベル）

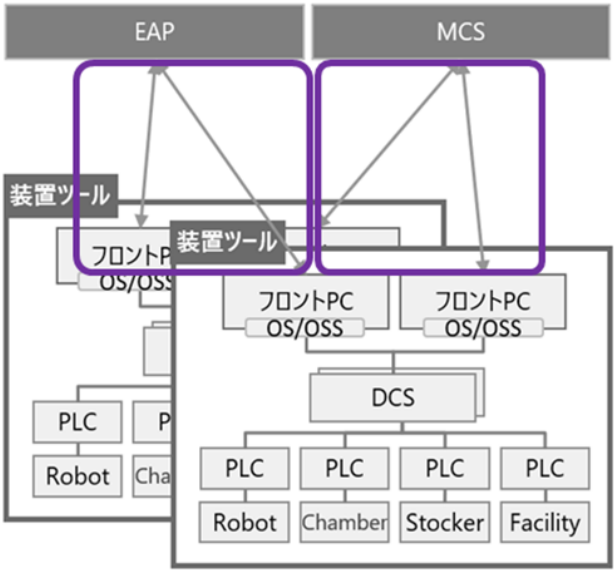


図 4-11. 装置システムネットワーク分離詳細

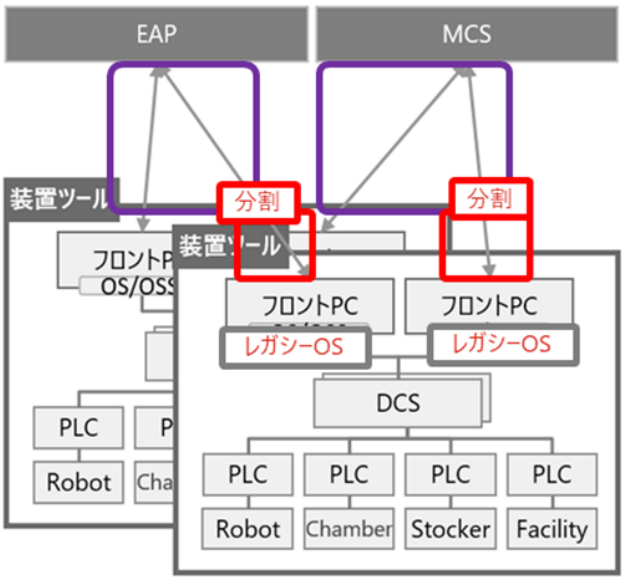
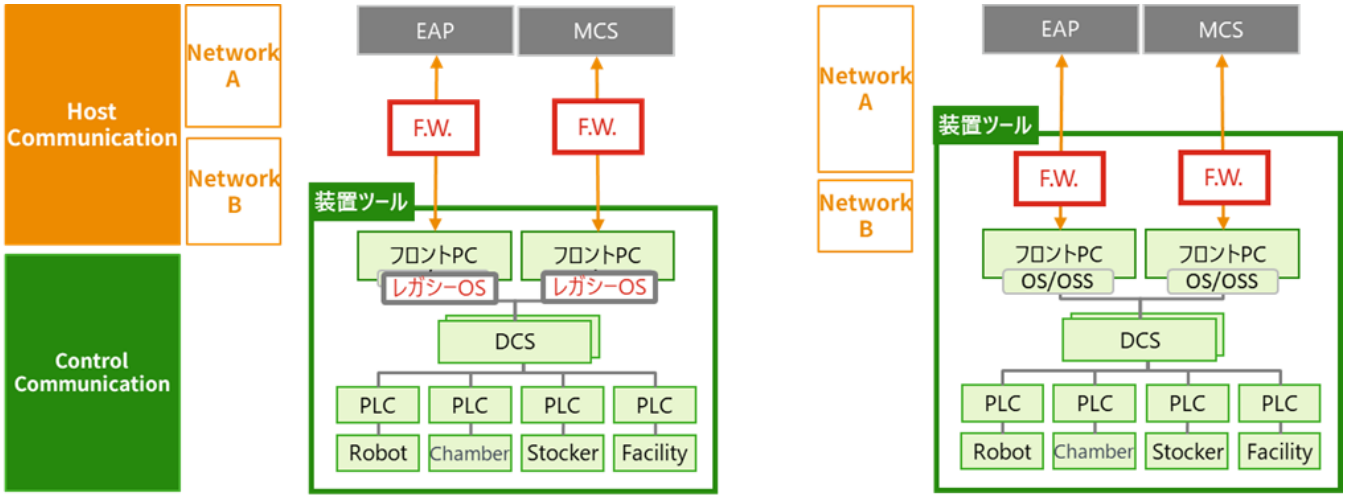


図 4-12. 装置ツールマイクロセグメンテーション構成例

サポート期間が終了した OS を搭載し運用している装置ツールや、セキュリティパッチを適用できない装置ツールについては、装置ツール内のフロント PC やコントロール PC 等のコンピュータデバイスごとに、1つのゾーンを設定したマイクロセグメンテーションで対策することが有効である。

なお、現在業界で対策規格が進む SEMI E187 及び 188 に基づく装置ツールのサイバーセキュリティ強化では、装置ツール内でマイクロセグメンテーションが対応可能となるセキュアな装置ツールへの対応が今後見込まれる。既存で稼働中の装置ツールに関する対応(装置外への設置等)を含め、装置メーカーと調達仕様書及びフィールドサポート保守契約等を通じて、セキュリティ対策と運用の確認(推奨する構成や設定内容、運用方法等)を行い、導入・運用を行うことが求められる。



F.W.を装置ツール外に設置する場合　　F.W.を装置ツール内に設置する場合

SEMI E187 製造リファレンス(Cybersecurity Reference Architecture for Semiconductor Manufacturing Environments)3.2 Tool Configurations を参照

図 4-13. マイクロセグメンテーション構成要素と選定ポイント

図 4-13 の F.W.箇所の選定では、装置ツールの重要度を踏まえ脅威からの保護の観点で、ファイア・ウォール、Router ACL、IPS、IDS、UTM 等から選択する。その際、VLAN、パケット制御、ステートフル、ペイロード、アノマリ、シグネチャ検知、仮想パッチ等の機能について、必要性を精査するとともに、コストも考慮して、調達仕様書や保守契約の範囲内で適切に選択する必要がある。

4.3 運用(監視・対応・復旧・改善) - FSIRT による運用

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、安全管理に必要な組織体制を構築する必要である。ここでは、工場の OT 領域においてサイバー攻撃の検知・対応・復旧を担うインシデント対応組織である、FSIRT(Factory Security Incident Response Team)の事例を示す(NIST CSF2.0 の 6 領域では検知、対応、復旧に該当する)。

工場の OT 領域を担う FSIRT は、IT 領域のセキュリティを担う CSIRT(Computer Security Incident Response Team)、製品セキュリティを担う PSIRT(Product Security Incident Response Team)と緊密な連携・協力を行い、サイバー攻撃からの有事の対応及び平時の備えを行う。

半導体デバイス工場は、非常に多くの装置ツール及びファシリティ設備を扱い、多くの保守要員にて運用が行われている。ひとたび事故が発生すると、自社の被害だけでなく、半導体利用産業への供給責任の影響も大きいため、攻撃の発生兆候を捉えた事前対応や、攻撃を早期に検知して被害拡大を極小化し、復旧する有事の対応、平時からの攻撃に対する備えを含めた FSIRT 運用が重要である。

有事の対応は、自然災害対策同様に、発生を想定した体制をあらかじめ整えておくとともに、運用を行うための手順策定及び教育・訓練が必要である。

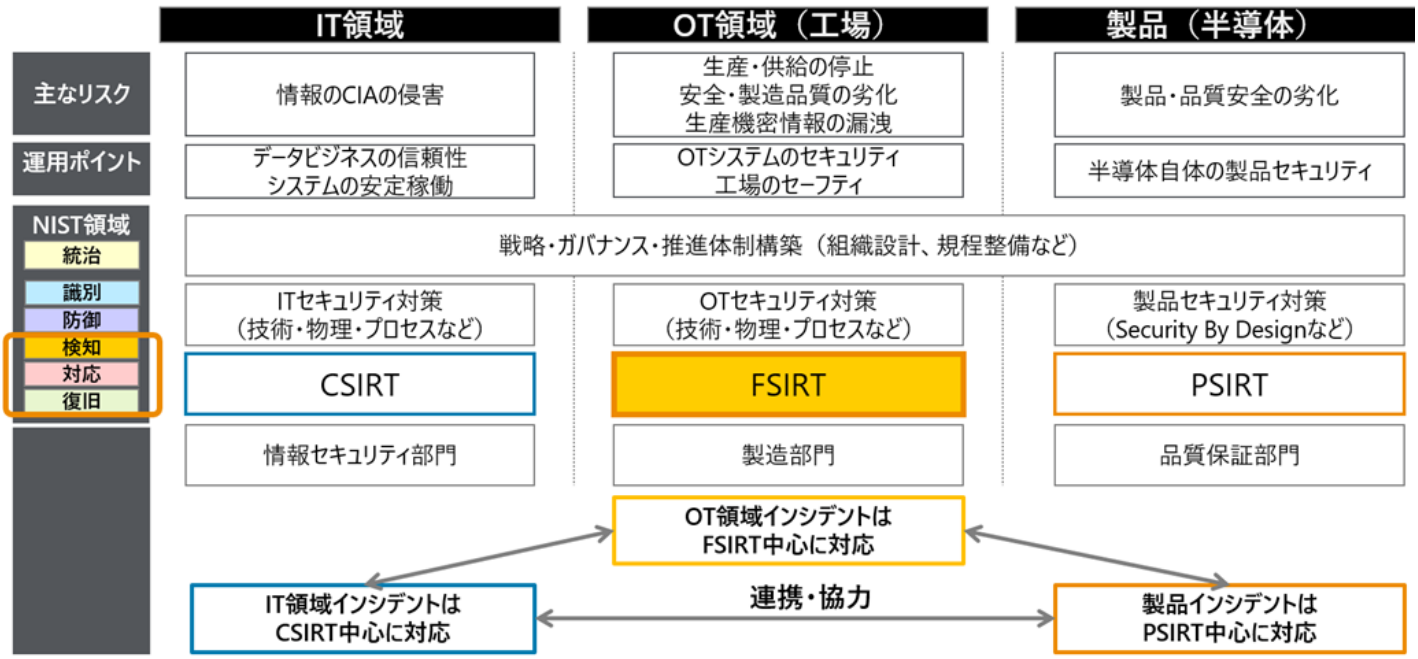


図 4-14. CSIRT、PSIRT、FSIRT の役割

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（有事におけるインシデント対応プロセスについては、「図 4-18. FSIRT インシデント対応プロセス」に記述する）。

FSIRT における平時の対応は、生産停止や情報漏洩等の発生を予防することを目的としている。工場の OT 領域の資産を保護するとともに、ヒト的・物理的セキュリティ運用ルールが適切に守られているかを確認する。また、現状の工場のセキュリティレベルを把握し、それに基づいて改善計画を立てるためのリスク分析も平時に実施する。

	有事の対応	平時の対応
	工場で発生したインシデントに対し早期発見し拡大防止を図るとともに、被害発生時は通常生産稼働できる状態に早期復旧を行う	工場の重要資産の安全化やセキュリティ運用ルールの徹底を行い、生産停止や情報漏洩等の発生を予防する
実施内容（例）	攻撃の初期段階を捉えた被害の拡大防止対応 被害発生時の封じ込めと早期復旧の対応 • 原因・被害内容等の調査（聞き取り、ログ調査等） • 被害の封じ込め（ネットワーク制限、認証強化等） • 原因の根絶（脆弱性に対するパッチ適用等） • 装置ツール・システム等の復旧（バックアップの適用等）	セキュリティ対策の危殆化確認と安全化対応 人的・物理セキュリティ運用状況の確認と是正対応 • ポリシー・運用ルール • リスク分析・評価 • 資産管理・セキュリティ監視（脆弱性管理等） • 意識啓発（教育・訓練）

図 4-15. FSIRT の平時・有事の実施内容

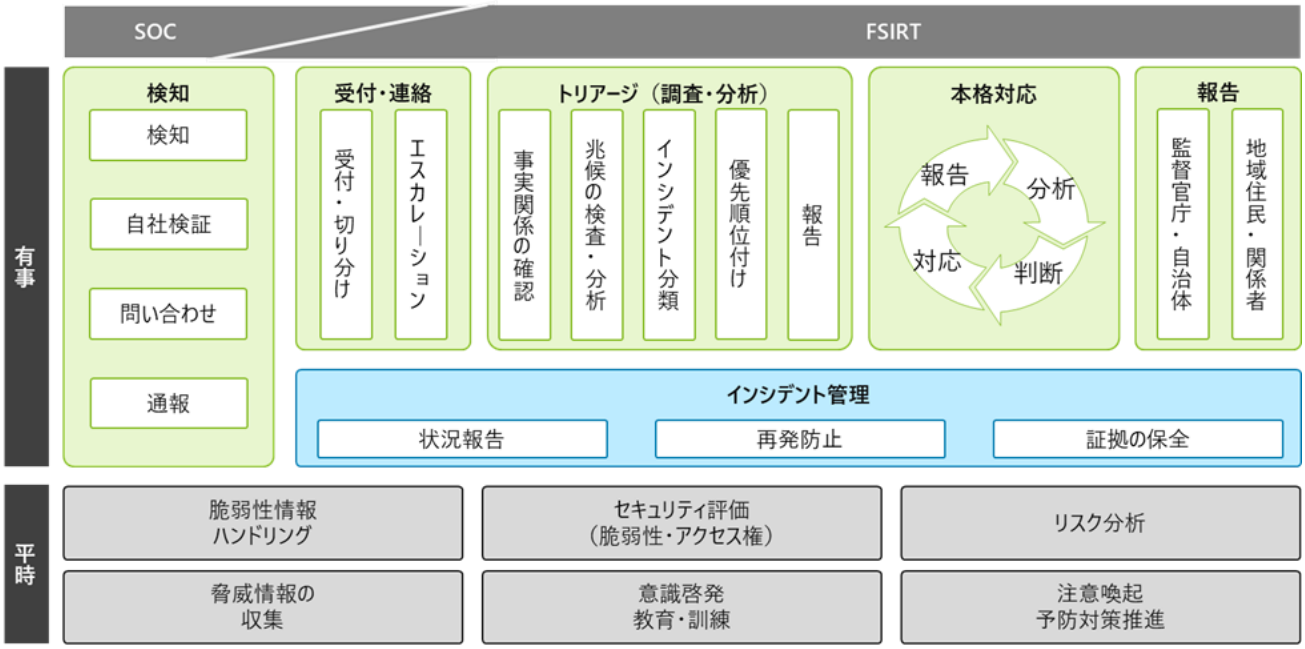


図 4-16. FSIRT の平時・有事の業務内容

サイバー攻撃は、侵入口を突破した後、いくつかの攻撃の段階を経て最終的な目的を達成するための攻撃が実行され、被害が表面化する。以下の事例では、半導体デバイス工場におけるネットワークの侵入や物理的侵入から目的実行に至るまでの流れを、サイバーキルチェーンモデルの形式で示している。

FSIRT の有事対応では、サイバーキルチェーンの中で侵入から目的達成に至るまでのサイバー攻撃の兆候（初期段階）を検知し、被害の発生を防ぐ対応が求められる。万が一被害が発生した場合は、その時点での影響範囲や損害を迅速に特定し、さらなる被害拡大を封じ込めるとともに、早期復旧のための対応が可能な体制を整えておく必要がある。

半導体デバイス工場では、被害発生時の事業への影響が大きいことから、より初期段階でサイバー攻撃の兆候を検知し、攻撃を防止するための防御施策が実施されている。ネットワーク経由の侵入では、IT 領域を起点として OT 領域へ侵入するリスクが高いため、IT 領域と OT 領域において横断的な監視・分析を行い、サイバー攻撃の初期段階で対応することが有効である。

また、生産機密情報や生産停止に関連する多くの重要資産がファブエリア（クリーンルーム）の装置ツールの中にあり、その保守作業のために、自社の装置ツール管理を担当する従業員に加え、装置メーカーや設備メーカー各社の多数の保守作業員がファブエリアに入室して運用作業を行うことが多い。そのため、ファブエリアの装置ツールでの保守作業はサイバー攻撃の物理的侵入口として悪用されるリスクが高い箇所である。

このようなリスクに対応するため、ファブエリアへの入室・持込み・接続を制限する物理的アクセス防御をルール化して運用するとともに、ネットワーク経由での侵入や移動を制限する多層防御、マイクロセグメンテーションによるセキュリティ監視を行い、初期段階での検知を強化している。FSIRT では、検知された攻撃の情報を警報（アラート）として受け取り、迅速に対応判断を行う必要がある。

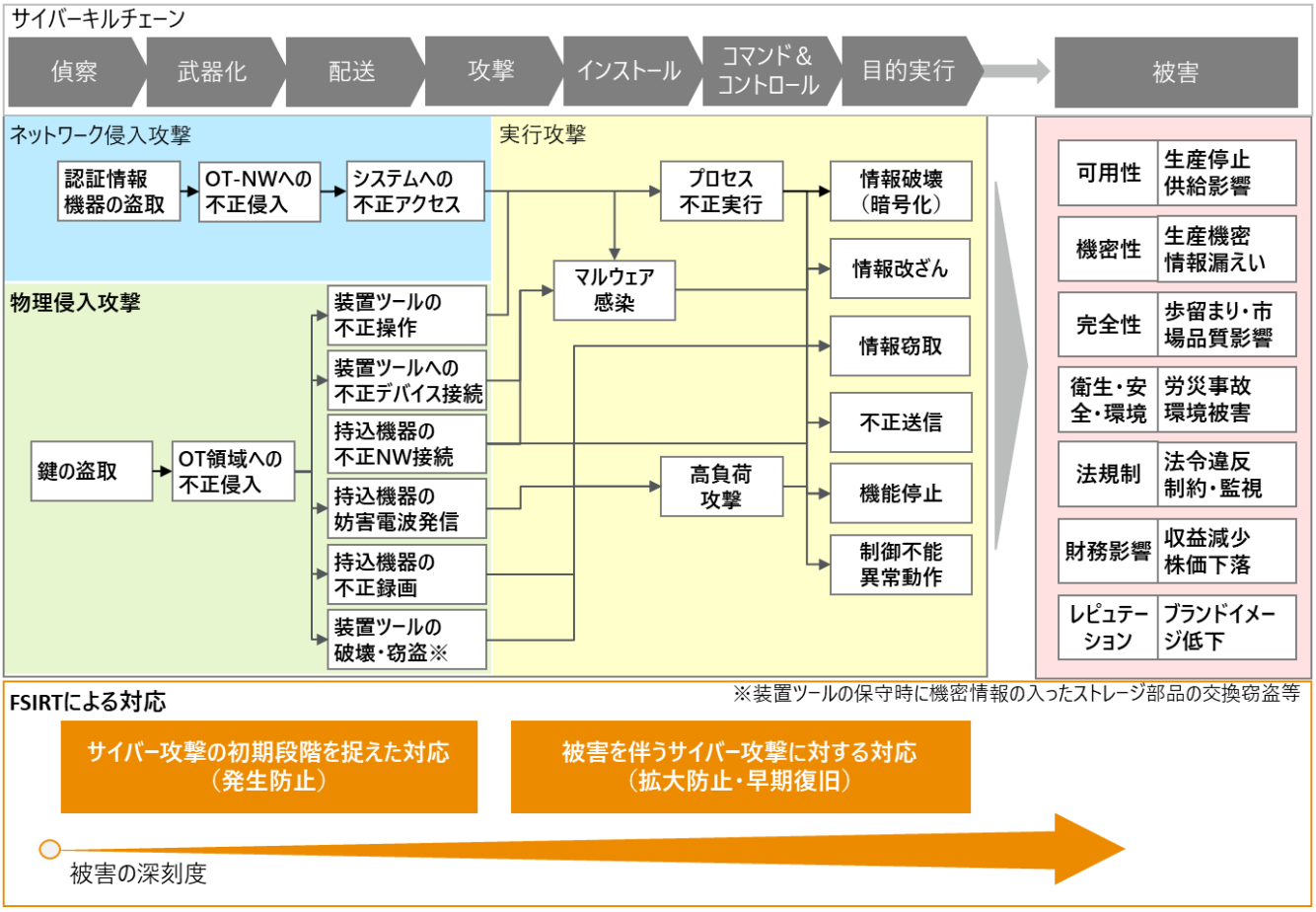


図 4-17. 工場におけるサイバーキルチェーン

FSIRT におけるインシデント対応プロセス及び体制の例を以下に示す（図 4-18、図 4-19）。

半導体デバイス工場では、対応プロセスの最初の段階である検知・受付の発生頻度が誤検知を含め非常に高くなる特徴がある。これはサイバー攻撃の初期段階である兆候を捉え検知するネットワーク対策機器の台数や、物理的対策での入室・持込み・接続の制限通知受付監視の対象人員が多いことから、検知件数が多くなるためである。

FSIRT では、この大量の検知を効率的に受付し、応急処置が迅速に実施できるよう、あらかじめ手順書（プレイブック等）を作成し、対応能力を高めるために訓練を行う。これにより、深刻なインシデントの発生を未然に防ぐ運用を実現するとともに、被害の発生内容や被害範囲を調査・分析し、深刻度に応じて対応方針を決定する。

事業に与える影響が非常に大きい場合は、工場の責任者と協議の上、生産の停止を判断することが求められる。また、事業継続のためのリスク管理対応として、緊急対策本部の立ち上げを要請することが必要である。生産停止を伴う規模のインシデントが発生した際には、経営層への状況報告を常に行いながら、インシ

デントの原因究明や封じ込め、根絶を進める。同時に、社内の各部署と協力して生産稼働の早期復旧を目指すとともに、サプライチェーンを構成する顧客や取引先を含む社外のステークホルダーへの報告を並行して進める必要がある。

これらの対応は、自然災害、特に大規模地震を想定した定期的な避難訓練や教育の実施と同様に、生産停止を伴う大規模なサイバー被害を具体的に想定した机上訓練及び教育を実施する必要がある。

なお、この一連のインシデント対応プロセスは「サイバー攻撃である」ことが認知れた時点から開始されている。しかし実際の工場では何らかの機器故障や不具合が発生した際、その原因が単なる機器故障なのか、サイバー攻撃によるものなのかを最初に切り分ける必要がある場合も想定される。そのためサイバー攻撃を対象とした訓練だけでなく、一般的な BCP の訓練の中にサイバー攻撃を組み込んでいくことが望まれる。

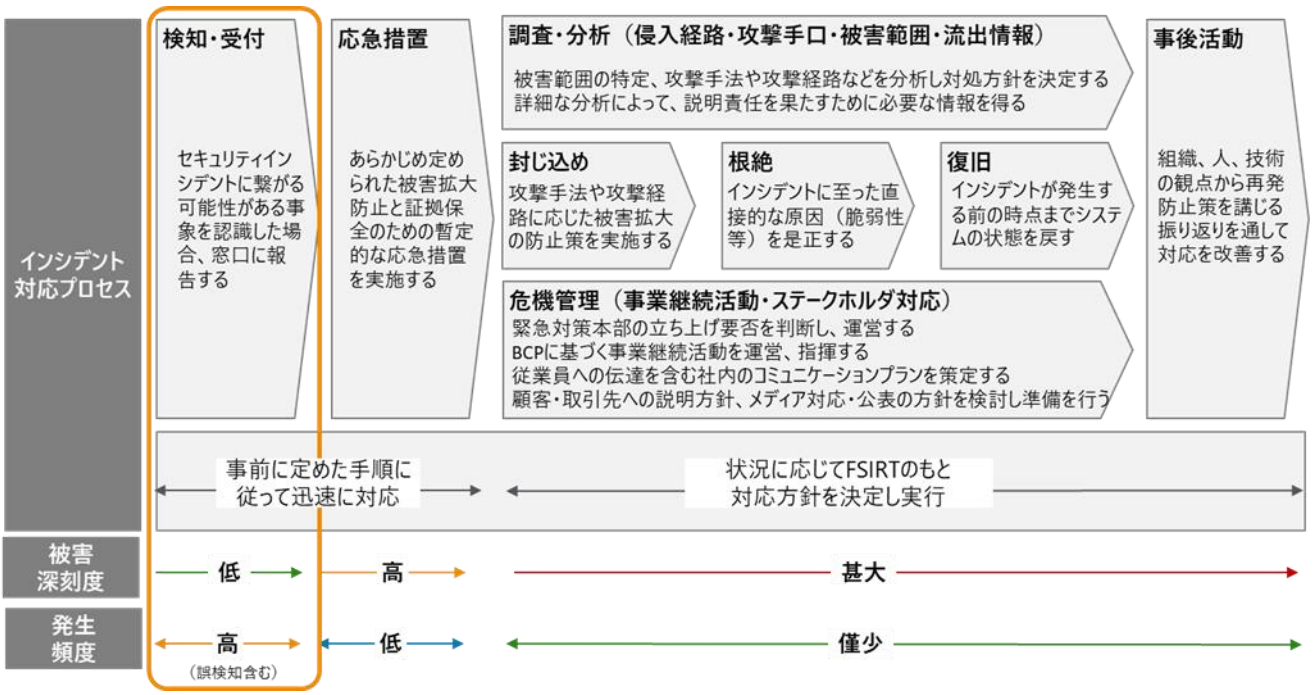


図 4-18. FSIRT インシデント対応プロセス

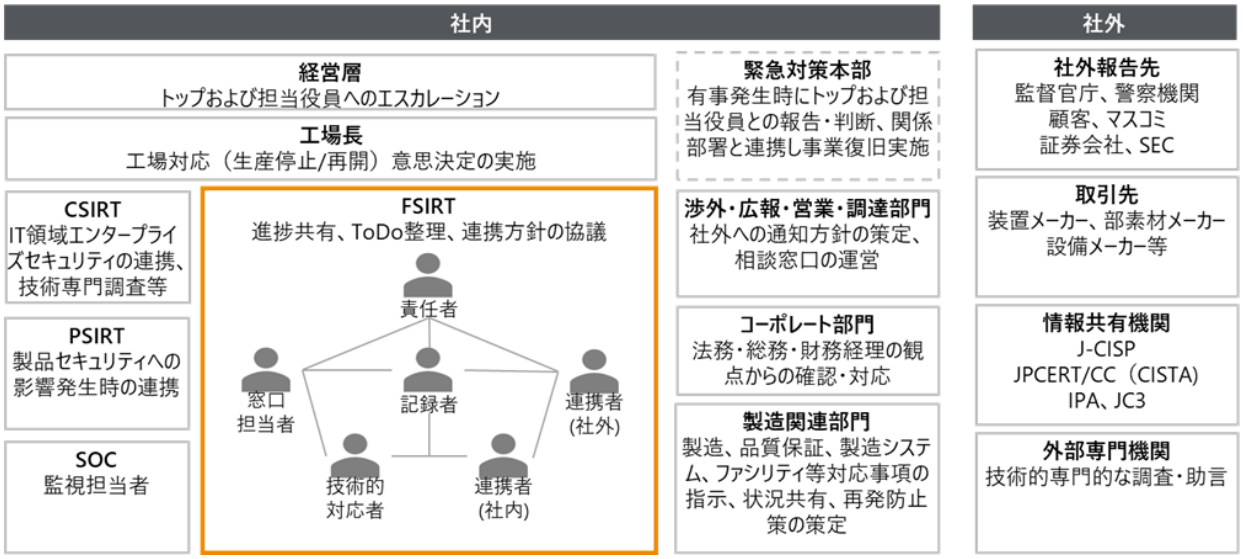


図 4-19. FSIRT 体制・社内外関係図

FSIRT の責任者や技術的担当者等、OT 領域のセキュリティ対策や運用を行う人材の育成には、IPA の「中核人材育成プログラム」[18]が活用できる。

このプログラムでは、現場から経営層までの幅広い視点から組織・サプライチェーン・業界全体を俯瞰しながら、セキュリティやビジネスについて総合的に学習し知見を深めることができる。また、製造現場におけるサイバーセキュリティリスクをより深く理解するための模擬システムを使った実践的演習の実施がされるほか、海外の関連機関との連携トレーニングによる国内外や業種を超えたトップレベルの人脈を形成することも可能である。

半導体デバイス工場は、第 2 章のリファレンスアーキテクチャで示した通り、連続稼働型の全自動プロセス工程として、非常に多くの装置ツールを組み合わせて半導体製造が行われている。日々の製造活動は、デバイス工場の従業員とともに、製造の主たる構成要素である各装置メーカーのフィールドサポートエンジニアによる保守サポートによって運用されている（半導体デバイス工場のリファレンスアーキテクチャの第 1 層）。

年々増加・高度化するサイバー攻撃から半導体デバイス工場を守るためには、半導体製造を支える重要な資産である装置ツールに対して、日々のセキュリティ対策を確実に運用する必要がある。

特に、数が多く、稼働を停止することができない装置ツールに対して、脅威情報や脆弱性情報に対する迅速な評価や対応、監視を基にした、サイバー攻撃の早期検知、被害発生に伴うインシデント対応等、デバイスメーカーの FSIRT と装置メーカーの PSIRT を含めた企業間での連携したセキュリティ対応強化が求められている。

[18] https://www.ipa.go.jp/jinzai/ics/core_human_resource/2025.html

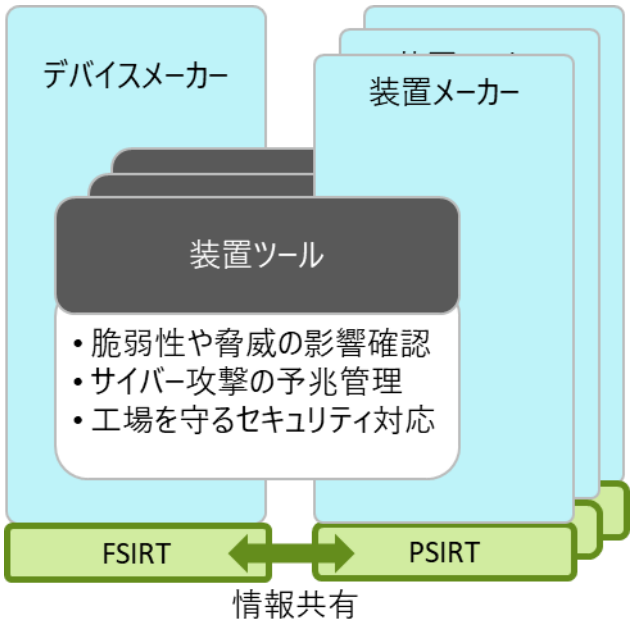


図 4-20. デバイスメーカーと装置メーカーの企業間連携

具体的なデバイスメーカーと装置メーカーのセキュリティ連携について、企業間の連携は契約を前提として成り立つため、既存の装置ツール調達プロセスにおける調達仕様書及び運用時の保守契約書に、セキュリティ要件（SEMI E187/188 Capability Requirements 等）を追加することが重要である。

また、連携を行う体制も重要であり、現状ではデバイスメーカーの装置ツール及びプロセス管理技術者と装置メーカーのフィールドサポートエンジニアが企業間連携の中心となっている。しかし、双方のセキュリティ責任者が連携し、セキュリティ対策やインシデント対応の要件や運用方法について定期的なコミュニケーションを行うことが望まれる。

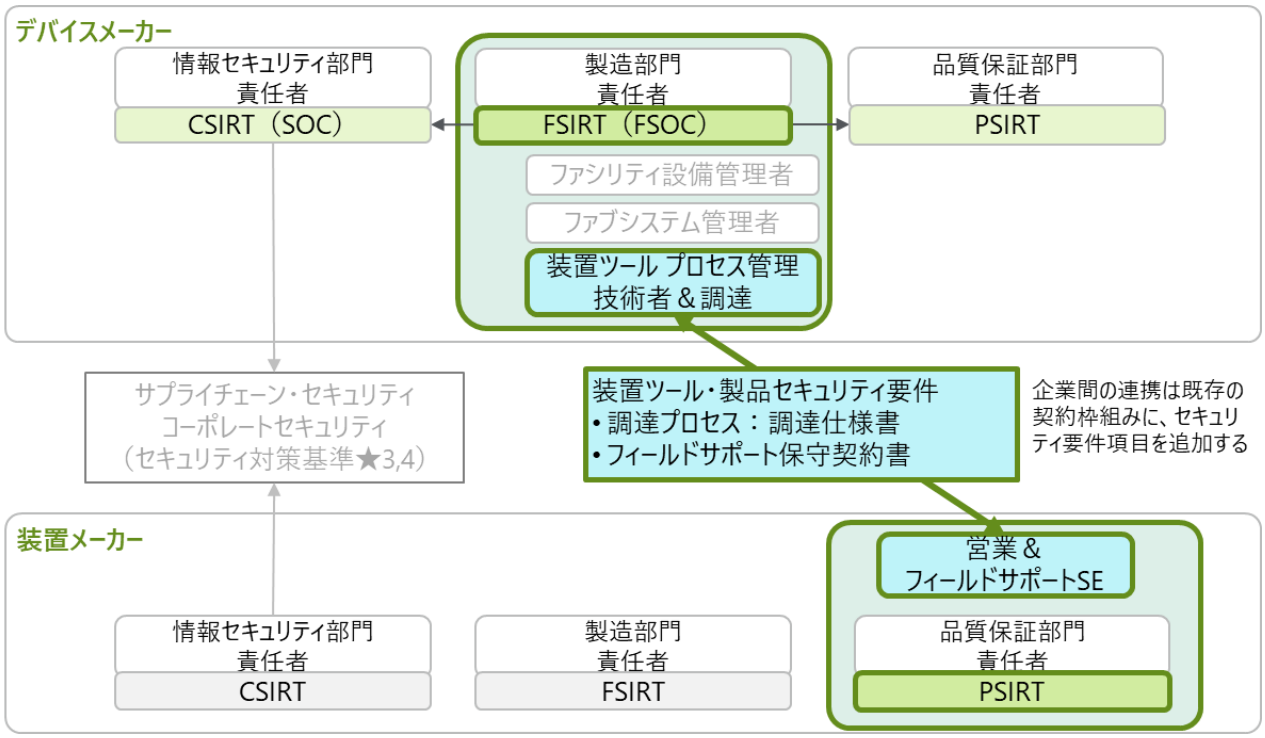


図 4-21. デバイスメーカー、装置メーカーのセキュリティ連携の具体的イメージ

装置ツールのセキュリティ対策を強化するために、デバイスメーカーと装置メーカーの連携ポイントは、調達時（調達仕様書から納品）と運用時（保守契約による平時・有事対応）の 2 つに分類される。 各連携ポイントにおける具体的な7つのセキュリティ連携イベントを表 4-5 に示す。

連携イベントごとに、デバイスメーカーと装置メーカーの双方でセキュリティ要件と提供内容を定め、運用の取り決めを行う。

なお、情報の提供にあたり、デバイスメーカー側の追加セキュリティ対策を含めた生産機密情報や、装置メーカーの製品のセキュリティ構成情報を含めた機密情報の取り扱いが発生するため、あらかじめ双方のセキュリティ関係者を含めた機密保持契約（NDA）を締結し、進める必要がある。

また、『SEMI E169』[19]の「9.3.3 Confidentiality Requirements of Equipment Design Information」及び「9.3.4 Requirement for Information Availability」にて、関連する機密情報の取り扱いに関する参考指針が示されている。

[19] https://store-us.semi.org/products/e16900-semi-e169-guide-for-equipment-information-system-security

表 4-5. デバイスメーカーと装置メーカー間のセキュリティ連携イベント

セキュリティ連携イベント		デバイスメーカー	装置メーカー
調達時（調達仕様書）	見積・注文時（仕様確認） ①見積時	装置ツールの調達仕様書にセキュリティ要件を盛り込み見積依頼 (SEMI E187/188 Capability Requirements 等)	見積仕様書にセキュリティ要件を含め作成・提出 （SEMI E187/188 Capability Requirements回答 ：C: 準拠、NC: 非準拠、WC:準拠予定、NA: 該当なし）
	決定・注文	注文→制作	
	納品前 ②設計時	注文した装置ツールのセキュリティ要件を確認し、設置環境のセキュリティ追加防御対策の設計を実施（多層防御／マイクロセグメンテーション、セキュリティ監視設定、不明点をデバイスメーカーから装置メーカーへ確認）	設置環境のセキュリティ追加防御対策の確認および回答
	納品時 ③納品時	装置ツールのセキュリティ要件のエビデンス確認	・装置ツールのセキュリティ要件 エビデンスの提出 （資産構成情報、マルウェア・脆弱性検査、ハードニング実施状況等）
	導入設置時 ④接続時	装置ツールのセキュリティ設定結果の確認および、ネットワークへの追加対策の実施、資産管理台帳への登録、運用開始	Fabネット接続前セキュリティ設定の実施 （デバイスメーカー指定のセキュリティツール導入、ネットワーク・ログ等の設定）
		装置ツールの導入テスト開始（従来）	
運用時（フィールドサポート）	平時対応 脆弱性評価 ⑤評価時	脆弱性情報・脅威情報の収集 装置ツールの脆弱性影響の確認 装置ツールの脆弱性評価の実施と共有 （対応判断：緊急実施、定期実施、現対策による許容）	脆弱性情報・脅威情報の収集 装置ツールの脆弱性影響情報の提供 装置ツールの脆弱性評価結果の共有
	脆弱性対応 ⑥変更時	装置ツールに対する脆弱性対応の決定 装置ツールに対する脆弱性対応計画の確認 装置ツールに対する脆弱性対応の周知（停止調整含む） 装置ツールに対する脆弱性対応実施結果の確認 変更記録管理の実施	装置ツールに対する脆弱性対応計画の作成 （リスク軽減・緩和策を含む） 装置ツールに対するセキュリティ対応の実施
	有事対応 ⑦異常時	インシデント対応（調査・分析）、状況共有・報告	装置ツールでの影響最小化（封じ込め）対策の実施 装置ツールの早期復旧対応

4.4 物理アクセスの制限(入室・持込み・接続) - ファブエリアにおける物理的対策

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。

半導体デバイス工場のファブエリアは、事業への影響度が高い重要資産を多く管理する高セキュリティエリアに該当する。このエリアには従業員や保守員を含め多くの人員の出入りがしており、クリーンルーム内ではクリーンスーツを着用しているため、個人の視覚的に識別することが難しいという特徴がある。このような点を踏まえ、ヒトの認証を実施する装置・機器(ID カードや生体情報による認証装置・機器等)での管理を行う等、物理侵入攻撃ルートを整理し物理的対策を行うとともに、継続的なセキュリティ状態監視を実施する必要がある。

物理セキュリティの対策例は、『IEC62443』 及び、経済産業省『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 Ver1.1』の「3.2 ステップ 2 セキュリティ対策の立案(2) 物理面での対策」の内容を参考として作成している。

表 4-6. ファブエリアにおける物理対策

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 • 装置ツールを管理する従業員とともに、様々な装置メーカーの業務委託の保守員が入室する • 24 時間／7 日間の連続稼働のため、交代勤務者含めた従業員及び業務委託の保守員が対象者となる • 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 • クリーン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 • ファブエリアへの入退室許可制限（従業員、常駐者、訪問者） • 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 • 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込みが発生する • 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込み制限 • ストレージ保有デバイスの持込み制限 • 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込み制限 • 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等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、レシピ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

攻撃ポイントについては、「図 4-22. 工場におけるサイバーキルチェーンの物理侵入攻撃」を参照

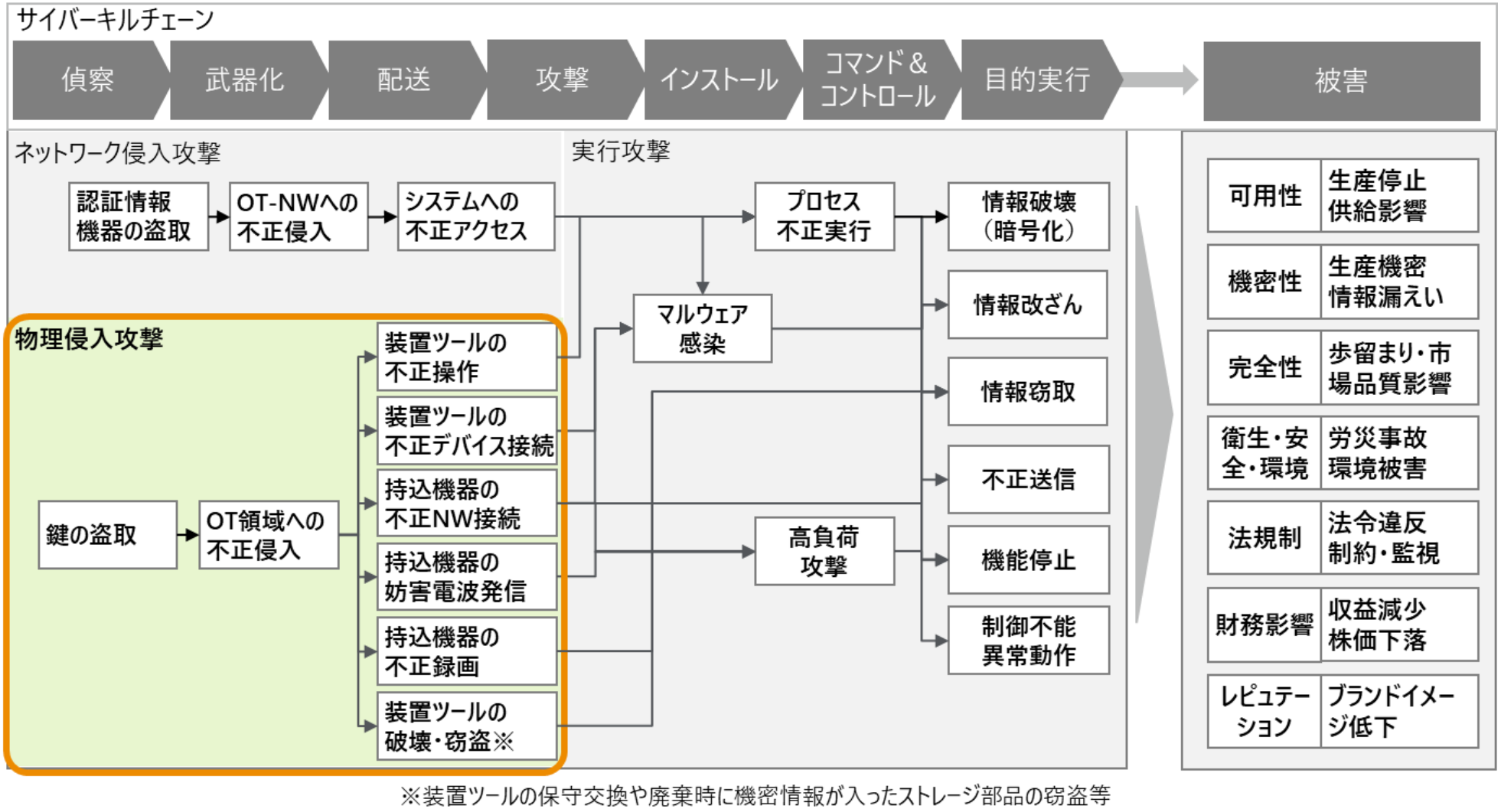


図 4-22. 工場におけるサイバーキルチェーンの物理侵入攻撃

Appendix A:NIST CSF2.0 と CPSF の対応表

表 A-1. CPSF を基準とする NIST CSF2.0 と CPSF の対応表

CPSF		NIST CSF2.0	
対策要件 ID	対策要件	Subcategory	
CPS.AM-1	システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	ID.AM-01	組織が管理するハードウェアのインベントリ（一覧）が維持されている。
		ID.AM-02	組織が管理するソフトウェア、サービス、及びシステムのインベントリ（一覧）が維持されている。
CPS.AM-2	自組織が生産したモノのサプライチェーン上の重要性に応じて、トレーサビリティ確保のための特定方法を定める。		
CPS.AM-3	重要性に応じて、生産日時やその状態等について記録を作成し、一定期間保管するために生産活動の記録に関する内部規則を整備し、運用する。		
CPS.AM-4	組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。	ID.AM-03	組織が認可したネットワーク通信及び内部と外部のネットワークのデータフローの描写が維持されている。
		ID.AM-07	指定されたデータタイプのデータ及び対応するメタデータのインベントリ（一覧）が維持されている。
CPS.AM-5	自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	ID.AM-04	サプライヤが提供するサービスのインベントリ（一覧）が維持されている。
CPS.AM-6	リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	ID.AM-05	資産は、分類、重要度、リソース、及びミッションへのインパクトに基づいて優先順位付けされている。
CPS.AM-7	自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。	GV.SC-02	サプライヤ、顧客、パートナーに対するサイバーセキュリティの役割と責任が確立され、伝達され、社内及び社外で調整されている。
		GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。
CPS.BE-1	サプライチェーンにおいて、自組織が担う役割を特定し共有する。	GV.OC-01	組織のミッションが理解され、サイバーセキュリティリスクマネジメントに情報を提供している。
		GV.OC-05	組織が依存する成果、ケイパビリティ（能力）、サービスを理解が理解され、伝達されている。
CPS.BE-2	あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤ、第三者プロバイダ等を含む）に共有する。	GV.OC-01	組織のミッションが理解され、サイバーセキュリティリスクマネジメントに情報を提供している。
CPS.BE-3	自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。
		GV.OC-05	組織が依存する成果、ケイパビリティ（能力）、サービスを理解が理解され、伝達されている。
CPS.GV-1	セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。	GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。
		GV.PO-01	サイバーセキュリティリスクマネジメントのポリシーが、組織の状況、サイバーセキュリティ戦略、優先順位に基づいて策定され、伝達され、実施されている。
		GV.PO-02	サイバーセキュリティリスクマネジメントのポリシーが、要件、脅威、技術、組織のミッションの変化を反映するようレビューされ、更新され、伝達され、実施されている。
		GV.OC-02	社内外のステークホルダーが理解され、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待が理解され、考慮されている。
		GV.SC-02	サプライヤ、顧客、パートナーに対するサイバーセキュリティの役割と責任が確立され、伝達され、社内及び社外で調整されている。
CPS.GV-2	個人情報保護法、不正競争防止法等の国内外の法令	GV.OC-03	サイバーセキュリティに関する法的要求事項、規制

	や、業界のガイドラインを考慮した社内ルールを策定する。		上の要件、及び契約上の要求事項（プライバシー及び市民的自由の義務を含む）が理解され、管理されている。
CPS.GV-3	各種法令や関係組織間だけで共有するデータの扱いに関する取決め等によって要求されるデータの保護の水準を的確に把握し、それぞれの要求を踏まえたデータの区分方法を整備し、ライフサイクル全体に渡って区分に応じた適切なデータの保護を行う。		
CPS.GV-4	セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。	GV.RM-03	サイバーセキュリティリスクマネジメントの活動及び成果が、事業体のリスクマネジメントプロセスに含まれている。
CPS.RA-1	自組織の資産の脆弱性を特定し、対応する資産とともに一覧を分書化する。	ID.RA-01	資産の脆弱性が識別され、妥当性が確認され、記録されている。
CPS.RA-2	セキュリティ対応組織（SOC/CSIRT）は、組織の内部及び外部の情報源（内部テスト、セキュリティ情報、セキュリティ研究者等）から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。	ID.RA-02	サイバー脅威インテリジェンスが、情報共有フォーラムや情報源から入手されている。
		ID.RA-08	脆弱性開示情報を受領し、分析し、対応するプロセスが確立されている。
CPS.RA-3	自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。	ID.RA-03	組織に対する内部及び外部の脅威が識別され、記録されている。
CPS.RA-4	構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。	ID.RA-04	脆弱性を悪用する脅威の潜在的インパクトと起こりやすさが識別され、記録されている。
		ID.RA-06	リスク対応が選択され、優先順位付けされ、計画され、追跡され、伝達されている。
CPS.RA-5	リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。	ID.RA-05	脅威、脆弱性、起こりやすさ、及びインパクトが、内在するリスクを理解し、リスク対応の優先順位付けに情報を提供するために使用されている。
CPS.RA-6	リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。	ID.RA-06	リスク対応が選択され、優先順位付けされ、計画され、追跡され、伝達されている。
CPS.RM-1	自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者（例：上級管理職）に伝達する。また、自組織の事業に関係する自組織及び他組織（例：業務委託先）の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。	GV.RM-01	リスクマネジメントの目的が確立され、組織のステークホルダーによって合意されている。
		GV.RM-06	サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立され、伝達されている。
		GV.RR-03	サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースが割り振られている。
CPS.RM-2	リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。	GV.RM-02	リスク選好度及びリスク許容度が確立され、伝達され、維持されている。
		GV.RM-04	適切なリスク対応のオプションを表す戦略的方向性が確立され、伝達されている。
CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化した上で、その内容について取引先と合意する。	GV.RM-05	サプライヤ及びその他の第三者によるリスクを含む、サイバーセキュリティリスクに関する組織全体にわたるコミュニケーション系統が確立されている。
		GV.SC-01	サイバーセキュリティサプライチェーンリスクマネジメントのプログラム、戦略、目的、ポリシー、及びプロセスが確立され、組織のステークホルダーによって合意されている。
		GV.SC-06	サプライヤまたはその他の第三者との正式な関係を結ぶ前に、リスクを低減するための計画と適正評価が実施されている。
		GV.SC-09	サプライチェーンのセキュリティプラクティスが、サイバーセキュリティ及び事業体のリスクマネジメントプログラムに統合され、その実行が、技術製品及びサービスのライフサイクルを通じて監視されている。
		GV.SC-10	サイバーセキュリティサプライチェーンリスクマネジメント計画に、パートナーシップまたはサービス合

			意の締結後に発生する活動に関する規定が含まれている。
CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	GV.OC-02	社内外のステークホルダーが理解され、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待が理解され、考慮されている。
		GV.SC-03	サイバーセキュリティサプライチェーンリスクマネジメントが、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合されている。
		GV.SC-04	サプライヤが把握され、重要度によって優先順位が付けられている。
		GV.SC-07	サプライヤ、その製品及びサービス、並びにその他の第三者によってもたらされるリスクが理解され、記録され、 優先順位が付けられ、アセスメントされ、対応され、その関係継続中に監視されている。
		ID.RA-10	取得前に重要なサプライヤがアセスメントされている。
CPS.SC-3	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。	GV.SC-05	サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件が確立され、優先順位が付けられ、サプライヤやその他の関連する第三者との契約やその他の種類の合意に統合されている。
CPS.SC-4	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織の提供する製品・サービスが適合していることを確認する。		
CPS.SC-5	取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。		
CPS.SC-6	取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。	GV.SC-07	サプライヤ、その製品及びサービス、並びにその他の第三者によってもたらされるリスクが理解され、記録され、 優先順位が付けられ、アセスメントされ、対応され、その関係継続中に監視されている。
		ID.RA-10	取得前に重要なサプライヤがアセスメントされている。
CPS.SC-7	取引先等の関係する他組織に対する監査、テストの結果、契約事項に対する不適合が発見された場合に実施すべきプロシージャを策定し、運用する。		
CPS.SC-8	自組織が、関係する他組織及び個人との契約上の義務を果たしていることを証明するための情報(データ)を収集、安全に保管し、必要に応じて適当な範囲で開示できるようにする。		
CPS.SC-9	サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。	GV.SC-08	関連するサプライヤ及びその他の第三者が、インシデントの計画、対応、及び復旧活動に含まれている。
		ID.IM-02	サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。
CPS.SC-10	取引先等の関係する他組織との契約が終了する際(例:契約期間の満了、サポートの終了)に実施すべきプロシージャを策定し、運用する。		
CPS.SC-11	サプライチェーンに係るセキュリティ対策基準及び関係するプロシージャ等を継続的に改善する。		
CPS.AC-1	承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。	PR.AA-01	認可されたユーザー、サービス、及びハードウェアの ID 及び認証情報が、組織によって管理されている。
		PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。
CPS.AC-2	IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。	PR.AA-06	資産への物理的なアクセスが、リスクに応じて管理され、監視され、実施されている。
CPS.AC-3	無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する。	PR.AA-03	ユーザー、サービス、及びハードウェアが認証されている。
		PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小

			特権と職務分離の原則が組み込まれている。
		PR.IR-01	ネットワーク及び環境が認可されていない論理アクセス及び使用から保護されている。
CPS.AC-4	一定回数以上のログイン認証失敗によるロックアウトや、安全性が確保できるまで再ログインの間隔をあける機能を実装する等により、IoT 機器、サーバ等に対する不正ログインを防ぐ。		
CPS.AC-5	職務及び責任範囲(例:ユーザー/システム管理者)を適切に分離する。	PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。
CPS.AC-6	特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式(例:二つ以上の認証機能を組み合わせた多要素認証)を採用する。	PR.AA-03	ユーザー、サービス、及びハードウェアが認証されている。
		PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。
CPS.AC-7	データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する(例:開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する。	PR.IR-01	ネットワーク及び環境が認可されていない論理アクセス及び使用から保護されている。
		PR.AA-06	資産への物理的なアクセスが、リスクに応じて管理され、監視され、実施されている。
CPS.AC-8	IoT 機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ(ヒト/モノ/システム等)との通信に限定する。	PR.AA-02	相互作用の文脈に基づいて ID が証明され、認証情報に結びつけられている。
CPS.AC-9	IoT 機器やユーザーによる構成要素(モノ/システム等)への論理的なアクセスを、取引のリスク(個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク)に見合う形で認証・認可する。	PR.AA-03	ユーザー、サービス、及びハードウェアが認証されている。
CPS.AT-1	自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ(能力)、及びサービスが理解され、伝達されている。
		PR.AT-01	サイバーセキュリティリスクを念頭に置いて一般的な職務を遂行するための知識とスキルを有するよう、人員に意識向上とトレーニングが提供されている。
		PR.AT-02	サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。
CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施し、その記録を管理する。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ(能力)、及びサービスが理解され、伝達されている。
		ID.IM-02	サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。
		ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセ キュリティ計画が策定され、伝達され、維持され、改善されている。
		PR.AT-01	サイバーセキュリティリスクを念頭に置いて一般的な職務を遂行するための知識とスキルを有するよう、人員に意識向上とトレーニングが提供されている。
		PR.AT-02	サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。
CPS.AT-3	自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。		
CPS.DS-1	組織間で保護すべき情報を交換する場合、当該情報の保護に係るセキュリティ要件について、事前に組織間で取り決める。		
CPS.DS-2	情報を適切な強度の方式で暗号化して保管する。	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。
CPS.DS-3	IoT 機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。	PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。
CPS.DS-4	情報を送受信する際に、情報そのものを暗号化して送受信する。	PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。

CPS.DS-5	送受信データ、保管データの暗号化等に用いる鍵を、ライフサイクルを通じて安全に管理する。		
CPS.DS-6	サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース(例:ヒト、モト、システム)を確保する。	PR.IR-04	可用性を確実にするために十分なリソース容量が維持されている。
CPS.DS-7	IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。	PR.IR-04	可用性を確実にするために十分なリソース容量が維持されている。
CPS.DS-8	保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。
		PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。
		PR.DS-10	使用中のデータの機密性、完全性、及び可用性が保護されている。
CPS.DS-9	自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。
		PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。
		PR.DS-10	使用中のデータの機密性、完全性、及び可用性が保護されている。
CPS.DS-10	IoT 機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。
		DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。
CPS.DS-11	送受信・保管する情報に完全性チェックメカニズムを使用する。	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。
CPS.DS-12	ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。	ID.RA-09	ハードウェア及びソフトウェアの真正性と完全性が、取得及び使用前にアセスメントされている。
		DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。
CPS.DS-13	IoT 機器やソフトウェアが正規品であることを定期的(起動時等)に確認する。		
CPS.DS-14	データの取得元、加工履歴等をライフサイクルの全体に渡って維持・更新・管理する。		
CPS.DS-15	計測の可用性、完全性保護によるセンシングデータの信頼性確保のために、計測セキュリティの観点が考慮された製品を利用する。		
CPS.IP-1	IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。	ID.RA-07	変更及び例外が管理され、リスクのインパクトがアセスメントされ、記録され、追跡されている。
		PR.PS-01	構成管理のプラクティスが確立され、適用されている。
CPS.IP-2	IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する。	PR.PS-01	構成管理のプラクティスが確立され、適用されている。
CPS.IP-3	システムを管理するためのシステム開発ライフサイクルを導入する。	PR.PS-06	セキュアなソフトウェア開発プラクティスが統合され、その実行がソフトウェア開発ライフサイクル全体を通じて監視されている。
		ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。
CPS.IP-4	構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストする。	PR.DS-11	データのバックアップが作成され、保護され、維持され、テストされている。
		RC.RP-03	バックアップ及びその他の復旧資産の完全性が、復旧に使用する前に検証されている。
CPS.IP-5	無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ(能力)、及びサービスが理解され、伝達されている。
		PR.IR-02	組織の技術資産が環境上の脅威から保護されている。
CPS.IP-6	IoT 機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規 IoT 機器、サーバ等を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする。	ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。
		PR.PS-03	ハードウェアはリスクに応じて保守され、交換さ

			れ、削除されている。
CPS.IP-7	セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、資産を保護するプロセスを改善する。	ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。
CPS.IP-8	保護技術の有効性について、適切なパートナーとの間で情報を共有する。	ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。
CPS.IP-9	人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項(例:アクセス権限の無効化、従業員に対する審査)を含める。	GV.RR-04	サイバーセキュリティが人事プラクティスに含まれている。
CPS.IP-10	脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。	ID.RA-01	資産の脆弱性が識別され、妥当性が確認され、記録されている。
		PR.PS-02	ソフトウェアはリスクに応じて保守され、交換され、削除されている。
CPS.MA-1	IoT 機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する。	ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。
		PR.PS-03	ハードウェアはリスクに応じて保守され、交換され、削除されている。
CPS.MA-2	自組織の IoT 機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。	ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。
		PR.PS-02	ソフトウェアはリスクに応じて保守され、交換され、削除されている。
CPS.PT-1	セキュリティインシデントを適切に検知するため、監査記録/ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。	PR.PS-04	ログ記録が生成され、継続的監視のために利用可能となっている。
CPS.PT-2	IoT 機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT機器、サーバ等の機能を必要最小限とする。	PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。
		PR.PS-01	構成管理のプラクティスが確立され、適用されている。
CPS.PT-3	ネットワークにつながることを踏まえた安全性を実装する IoT 機器を導入する。	PR.IR-03	通常時及び困難な状況でのレジリエンス要件を達成するためのメカニズムが実装されている。
CPS.AE-1	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。	ID.AM-03	組織が認可したネットワーク通信及び内部と外部のネットワークのデータフローの描写が維持されている。
CPS.AE-2	セキュリティ管理責任者を任命し、セキュリティ対応組織(SOC/CSIRT)を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。	DE.AE-02	関連する活動をよりよく理解するために、潜在的な有害事象が分析されている。
CPS.AE-3	セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。	DE.AE-03	情報は複数の情報源から相互に関連付けられている
		DE.AE-07	サイバー脅威インテリジェンス及びその他の文脈的情報が分析に統合されている。
		RS.MA-02	インシデント報告がトリアージされ、妥当性が確認されている。
CPS.AE-4	関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。	DE.AE-04	有害事象の推定されるインパクトと範囲が理解されている。
CPS.AE-5	セキュリティ事象の危険度の判定基準を定める。	DE.AE-08	有害事象が、定義されたインシデント基準を満たす場合に、インシデントが宣言される。
CPS.CM-1	組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。	DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。
CPS.CM-2	IoT機器、サーバ等の重要性を考慮し、適切な物理的アクセスの設定及び記録、監視を実施する。	DE.CM-02	潜在的な有害事象を発見するために、物理的環境が監視されている。
CPS.CM-3	指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。 サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。	DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。
		DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。
CPS.CM-4	サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。	DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。
		DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。
CPS.CM-5	セキュリティ事象を適切に検知できるよう、外部サービ	DE.CM-06	潜在的な有害事象を発見するために、外部サービ

	スプロバイダとの通信内容をモニタリングする。		スプロバイダの活動及びサービスが監視されている。
CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況（ネットワーク接続の有無、アクセス先等）及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。	DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。
		DE.CM-03	潜在的な有害事象を発見するために、人員の活動及び技術の利用が監視されている。
		DE.CM-06	潜在的な有害事象を発見するために、外部サービスプロバイダの活動及びサービスが監視されている。
		DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。
		PR.PS-05	認可されていないソフトウェアのインストール及び実行が防止されている。
CPS.CM-7	自組織の管理しているIoT機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。	ID.RA-01	資産の脆弱性が識別され、妥当性が確認され、記録されている。
CPS.DP-1	セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。	GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。
CPS.DP-2	監視業務では、地域毎に適用される法令、通達や業界標準等に準拠して、セキュリティ事象を検知する。		
CPS.DP-3	監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。	ID.IM-02	サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。
CPS.DP-4	セキュリティ事象の検知プロセスを継続的に改善する。	ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。
CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。
		ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセキュリティ計画が策定され、伝達され、維持され、改善されている。
		DE.AE-06	有害事象に関する情報が、認可されたスタッフ及びツールに提供されている。
		RS.MA-01	インシデントが宣言されると、関連する第三者と連携してインシデント対応計画が実行されている。
		RS.CO-02	社内外のステークホルダーにインシデントを通知する。
		RS.CO-03	指定された社内外のステークホルダーと情報を共有する。
		RC.CO-04	インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。
CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。
		ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセキュリティ計画が策定され、伝達され、維持され、改善されている。
		RS.MA-01	インシデントが宣言されると、関連する第三者と連携してインシデント対応計画が実行されている。
		RS.MA-04	インシデントは必要に応じてエスカレーションまたは昇格されている。
		RS.CO-03	指定された社内外のステークホルダーと情報を共有する。
CPS.RP-3	自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。	GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ（能力）、及びサービスが理解され、伝達されている。
		RS.MA-05	インシデントの復旧の開始基準が適用されている。
		RC.RP-01	インシデント対応計画の復旧に関する部分が、インシデント対応プロセスから取り組みが開始されると実行されている。
		RC.RP-02	復旧活動が選択され、範囲が設定され、優先順位が付けられ、実施されている。
CPS.RP-4	セキュリティインシデント発生時に被害を受けた設備に		

	て生産される等して、何らかの品質上の欠落が生じていることが予想されるモノ(製品)に対して適切な対応を行う。		
CPS.CO-1	セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。	RC.CO-04	インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。
CPS.CO-2	事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。	RC.CO-04	インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。
CPS.CO-3	復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。	RC.CO-03	復旧活動及び運用ケイパビリティ(能力)復旧の進捗状況が、指定された社内外のステークホルダーに伝達されている。
CPS.AN-1	セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。	RS.MA-02	インシデント報告がトリアージされ、妥当性が確認されている。
		RS.MA-03	インシデントが分類され、優先順位が付けられている。
		RS.MA-04	インシデントは必要に応じてエスカレーションまたは昇格されている。
		RS.AN-08	インシデントの規模が推定され、妥当性が確認されている。
CPS.AN-2	セキュリティインシデント発生後に、デジタルフォレンジックを実施する。	RS.AN-03	インシデント発生中に何が起こったのか、及びインシデントの根本原因を特定するための分析が実施されている。
		RS.AN-06	調査中に実施されたアクションが記録され、記録の完全性と来歴が保持されている。
CPS.AN-3	検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。	RS.MA-03	インシデントが分類され、優先順位が付けられている。
CPS.MI-1	セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。	RS.MI-01	インシデントが封じ込められている。
		RS.MI-02	インシデントが根絶されている。
CPS.IM-1	セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。	ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。
		ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセ キュリティ計画が策定され、伝達され、維持され、改善されている。
CPS.IM-2	セキュリティインシデントへの対応から教訓を導き出し、事業継続計画を継続的に改善する。	ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。
		ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセ キュリティ計画が策定され、伝達され、維持され、改善されている。

表 A-2. NIST CSF2.0 を基準とする CPSF と NIST CSF2.0 の対応表

NIST CSF2.0		CPSF	
Subcategory	対策要件	対策要件 ID	
GV.OC-01	組織のミッションが理解され、サイバーセキュリティリスクマネジメントに情報を提供している。	CPS.BE-1	サプライチェーンにおいて、自組織が担う役割を特定し共有する。
		CPS.BE-2	あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者(サプライヤ、第三者プロバイダ等を含む)に共有する。
GV.OC-02	社内外のステークホルダーが理解され、サイバーセキュリティリスクマネジメントに関する彼らのニーズと期待が理解され、考慮されている。	CPS.GV-1	セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
		CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。
GV.OC-03	サイバーセキュリティに関する法的要求事項、規制上の要件、及び契約上の要求事項(プライバシー及び市民的自由の義務を含む)が理解され、管理されている。	CPS.GV-2-	個人情報保護法、不正競争防止法等の国内外の法令や、業界のガイドラインを考慮した社内ルールを策定する。
GV.OC-04	外部ステークホルダーが組織に依存または期待する重要な目的、ケイパビリティ(能力)、及びサービスが理解され、伝達されている。	CPS.AT-1	自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。
		CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施し、その記録を管理する。
		CPS.IP-5	無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。
		CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順(セキュリティ運用プロセス)をあらかじめ定義し、実装する。
		CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
		CPS.RP-3	自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
		CPS.BE-3	自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。
GV.OC-05	組織が依存する成果、ケイパビリティ(能力)、サービスを理解が理解され、伝達されている。	CPS.BE-1	サプライチェーンにおいて、自組織が担う役割を特定し共有する。
		CPS.BE-3	自組織が事業を継続する上での自組織及び関係する他組織における依存関係と重要な機能を特定する。
GV.RM-01	リスクマネジメントの目的が確立され、組織のステークホルダーによって合意されている。	CPS.RM-1	自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者(例:上級管理職)に伝達する。また、自組織の事業に関係する自組織及び他組織(例:業務委託先)の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。
GV.RM-02	リスク選好度及びリスク許容度が確立され、伝達され、維持されている。	CPS.RM-2	リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。
GV.RM-03	サイバーセキュリティリスクマネジメントの活動及び成果が、事業体のリスクマネジメントプロセスに含まれている。	CPS.GV-4	セキュリティに関するリスク管理を適切に行うために戦略策定、リソース確保を行う。
GV.RM-04	適切なリスク対応のオプションを表す戦略的方向性が確立され、伝達されている。	CPS.RM-2	リスクアセスメント結果及びサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する。
GV.RM-05	サプライヤ及びその他の第三者によるリスクを含	CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーン

	む、サイバーセキュリティリスクに関する組織全体にわたるコミュニケーション系統が確立されている。		に係るセキュリティの対策基準を定め、責任範囲を明確化した上で、その内容について取引先と合意する。
GV.RM-06	サイバーセキュリティリスクの計算、文書化、分類、優先順位付けのための標準化された方法が確立され、伝達されている。	CPS.RM-1	自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者(例:上級管理職)に伝達する。また、自組織の事業に関係する自組織及び他組織(例:業務委託先)の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。
GV.RM-07	戦略的機会(すなわちプラスに働くリスク)が特徴付けられ、組織のサイバーセキュリティリスクに関する議論に含まれている。		
GV.RR-01	組織のリーダーシップが、サイバーセキュリティリスクに対する責任と説明責任を負い、リスクを認識し、倫理的で、継続的に改善する文化を育んでいる。		
GV.RR-02	サイバーセキュリティリスクマネジメントに関連する役割、責任、権限が確立され、伝達され、理解され、実施されている。	CPS.GV-1	セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
		CPS.AM-7	自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。
		CPS.DP-1	セキュリティ事象の説明責任を果たせるよう、セキュリティ事象検知における自組織とサービスプロバイダが担う役割と負う責任を明確にする。
GV.RR-03	サイバーセキュリティリスク戦略、役割、責任、ポリシーに見合った適切なリソースが割り振られている。	CPS.RM-1	自組織内におけるサイバーセキュリティリスクマネジメントの実施状況について確認し、組織内の適切な関係者(例:上級管理職)に伝達する。また、自組織の事業に関係する自組織及び他組織(例:業務委託先)の責任範囲を明確化し、関係する他組織によるセキュリティリスクマネジメントの実施状況を確認するプロセスを確立し、実施する。
GV.RR-04	サイバーセキュリティが人事プラクティスに含まれている。	CPS.IP-9	人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項(例:アクセス権限の無効化、従業員に対する審査)を含める。
GV.PO-01	サイバーセキュリティリスクマネジメントのポリシーが、組織の状況、サイバーセキュリティ戦略、優先順位に基づいて策定され、伝達され、実施されている。	CPS.GV-1	セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
GV.PO-02	サイバーセキュリティリスクマネジメントのポリシーが、要件、脅威、技術、組織のミッションの変化を反映するようレビューされ、更新され、伝達され、実施されている。	CPS.GV-1	セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
GV.OV-01	戦略と方向性に情報を与え調整するために、サイバーセキュリティリスクマネジメント戦略の成果がレビューされている。		
GV.OV-02	組織の要件とリスクを確実にカバーするために、サイバーセキュリティリスクマネジメント戦略がレビューされ、調整されている。		
GV.OV-03	組織のサイバーセキュリティリスクマネジメントの実績が、必要な調整のために評価され、レビューされている。		
GV.SC-01	サイバーセキュリティサプライチェーンリスクマネジメントのプログラム、戦略、目的、ポリシー、及びプロセスが確立され、組織のステークホルダーによって合意されている。	CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化した上で、その内容について取引先と合意する。
GV.SC-02	サプライヤ、顧客、パートナーに対するサイバーセキュリティの役割と責任が確立され、伝達され、社内及び社外で調整されている。	CPS.AM-7	自組織及び関係する他組織のサイバーセキュリティ上の役割と責任を定める。
		CPS.GV-1	セキュリティポリシーを策定し、自組織及び関係する他組織のセキュリティ上の役割と責任、情報の共有方法等を明確にする。
GV.SC-03	サイバーセキュリティサプライチェーンリスクマネジメントが、サイバーセキュリティ及び事業体のリスクマネジメント、リスクアセスメント、改善プロセスに統合されている。	CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。
GV.SC-04	サプライヤが把握され、重要度によって優先順位が	CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層に

	付けられている。		おいて重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。
GV.SC-05	サプライチェーンにおけるサイバーセキュリティリスクに対処するための要件が確立され、優先順位が付けられ、サプライヤやその他の関連する第三者との契約やその他の種類の合意に統合されている。	CPS.SC-3	外部の組織との契約を行う場合、目的及びリスクマネジメントの結果を考慮し、自組織のセキュリティに関する要求事項に対して関係する他組織のセキュリティマネジメントが適合していることを確認する。
GV.SC-06	サプライヤまたはその他の第三者との正式な関係を結ぶ前に、リスクを低減するための計画と適正評価が実施されている。	CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化した上で、その内容について取引先と合意する。
GV.SC-07	サプライヤ、その製品及びサービス、並びにその他の第三者によってもたらされるリスクが理解され、記録され、 優先順位が付けられ、アセスメントされ、対応され、その関係継続中に監視されている。	CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。
		CPS.SC-6	取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。
GV.SC-08	関連するサプライヤ及びその他の第三者が、インシデントの計画、対応、及び復旧活動に含まれている。	CPS.SC-9	サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。
GV.SC-09	サプライチェーンのセキュリティプラクティスが、サイバーセキュリティ及び事業体のリスクマネジメントプログラムに統合され、その実行が、技術製品及びサービスのライフサイクルを通じて監視されている。	CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化した上で、その内容について取引先と合意する。
GV.SC-10	サイバーセキュリティサプライチェーンリスクマネジメント計画に、パートナーシップまたはサービス合意の締結後に発生する活動に関する規定が含まれている。	CPS.SC-1	取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化した上で、その内容について取引先と合意する。
ID.AM-01	組織が管理するハードウェアのインベントリ(一覧)が維持されている。	CPS.AM-1	システムを構成するハードウェア、ソフトウェア及びその管理情報(例:名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報)の一覧を作成し、適切に管理する。
ID.AM-02	組織が管理するソフトウェア、サービス、及びシステムのインベントリ(一覧)が維持されている。	CPS.AM-1	システムを構成するハードウェア、ソフトウェア及びその管理情報(例:名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報)の一覧を作成し、適切に管理する。
ID.AM-03	組織が認可したネットワーク通信及び内部と外部のネットワークのデータフローの描写が維持されている。	CPS.AM-4	組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。
		CPS.AE-1	ネットワーク運用のベースラインと、ヒト、モノ、システム間の予測される情報の流れを特定し、管理するプロシージャを確立し、実施する。
ID.AM-04	サプライヤが提供するサービスのインベントリ(一覧)が維持されている。	CPS.AM-5	自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。
ID.AM-05	資産は、分類、重要度、リソース、及びミッションへのインパクトに基づいて優先順位付けされている。	CPS.AM-6	リソース(例:モノ、データ、システム)を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。
ID.AM-07	指定されたデータタイプのデータ及び対応するメタデータのインベントリ(一覧)が維持されている。	CPS.AM-4	組織内の通信ネットワーク構成図及び、データフロー図を作成し、適切に管理する。
ID.AM-08	システム、ハードウェア、ソフトウェア、サービス、及びデータが、ライフサイクル全体を通じて管理されている。	CPS.IP-3	システムを管理するためのシステム開発ライフサイクルを導入する。
		CPS.IP-6	IoT 機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規 IoT 機器、サーバ等を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする。
		CPS.MA-1	IoT 機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する。
		CPS.MA-2	自組織の IoT 機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。

ID.RA-01	資産の脆弱性が識別され、妥当性が確認され、記録されている。	CPS.RA-1	自組織の資産の脆弱性を特定し、対応する資産とともに一覧を分書化する。
		CPS.IP-10	脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。
		CPS.CM-7	自組織の管理している IoT 機器、サーバ等に対して、定期的に対処が必要な脆弱性の有無を確認する。
ID.RA-02	サイバー脅威インテリジェンスが、情報共有フォーラムや情報源から入手されている。	CPS.RA-2	セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源(内部テスト、セキュリティ情報、セキュリティ研究者等)から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。
ID.RA-03	組織に対する内部及び外部の脅威が識別され、記録されている。	CPS.RA-3	自組織の資産に対して想定されるセキュリティインシデントと影響及びその発生要因を特定し、文書化する。
ID.RA-04	脆弱性を悪用する脅威の潜在的インパクトと起こりやすさが識別され、記録されている。	CPS.RA-4	構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。
ID.RA-05	脅威、脆弱性、起こりやすさ、及びインパクトが、内在するリスクを理解し、リスク対応の優先順位付けに情報を提供するために使用されている。	CPS.RA-5	リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮する。
ID.RA-06	リスク対応が選択され、優先順位付けされ、計画され、追跡され、伝達されている。	CPS.RA-4	構成要素の管理におけるセキュリティルールが、実装方法を含めて有効かを確認するため、定期的にリスクアセスメントを実施する。 IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階から、受容できない既知のセキュリティリスクの有無を、セーフティに関するハザードの観点も踏まえて確認する。
		CPS.RA-6	リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。 IoT 機器及び IoT 機器を含んだシステムの企画・設計の段階におけるアセスメントにて判明したセキュリティ及び関連するセーフティのリスクに対して適宜対応する。
ID.RA-07	変更及び例外が管理され、リスクのインパクトがアセスメントされ、記録され、追跡されている。	CPS.IP-1	IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。
ID.RA-08	脆弱性開示情報を受領し、分析し、対応するプロセスが確立されている。	CPS.RA-2	セキュリティ対応組織(SOC/CSIRT)は、組織の内部及び外部の情報源(内部テスト、セキュリティ情報、セキュリティ研究者等)から脆弱性情報/脅威情報等を収集、分析し、対応及び活用するプロセスを確立する。
ID.RA-09	ハードウェア及びソフトウェアの真正性と完全性が、取得及び使用前にアセスメントされている。	CPS.DS-12	ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。
ID.RA-10	取得前に重要なサプライヤがアセスメントされている。	CPS.SC-2	自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。
		CPS.SC-6	取引先等の関係する他組織が、契約上の義務を果たしていることを確認するために、監査、テスト結果、または他の形式の評価を使用して定期的に評価する。
ID.IM-01	改善点が評価から識別されている。		
ID.IM-02	サプライヤ及び関連する第三者と協力して実施されるものを含め、セキュリティテスト及び演習から改善点が識別されている。	CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施し、その記録を管理する。
		CPS.SC-9	サプライチェーンにおけるインシデント対応活動を確実にするために、インシデント対応活動に関係する者の間で対応プロセスの整備と訓練を行う。
		CPS.DP-3	監視業務として、セキュリティ事象を検知する機能が意図したとおりに動作するかどうかを定期的にテストし、妥当性を検証する。
ID.IM-03	運用プロセス、手順、及び活動の実行から改善点が識別されている。	CPS.IP-7	セキュリティインシデントへの対応、内部及び外部からの攻撃に関する監視/測定/評価結果から教訓を導き出し、資産を保護するプロセスを改善する。
		CPS.IP-8	保護技術の有効性について、適切なパートナーとの間

			で情報を共有する。
		CPS.DP-4	セキュリティ事象の検知プロセスを継続的に改善する。
		CPS.IM-1	セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。
		CPS.IM-2	セキュリティインシデントへの対応から教訓を導き出し、事業継続計画を継続的に改善する。
ID.IM-04	運用に影響を及ぼすインシデント対応計画及びその他のサイバーセ キュリティ計画が策定され、伝達され、維持され、改善されている。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順(セキュリティ運用プロセス)をあらかじめ定義し、実装する。
		CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
		CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施し、その記録を管理する。
		CPS.IM-1	セキュリティインシデントへの対応から教訓を導き出し、セキュリティ運用プロセスを継続的に改善する。
		CPS.IM-2	セキュリティインシデントへの対応から教訓を導き出し、事業継続計画を継続的に改善する。
PR.AA-01	認可されたユーザー、サービス、及びハードウェアの ID 及び認証情報が、組織によって管理されている。	CPS.AC-1	承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。
PR.AA-02	相互作用の文脈に基づいて ID が証明され、認証情報に結びつけられている。	CPS.AC-8	IoT 機器、サーバ等が実施する通信は、適切な手順で識別されたエンティティ(ヒト/モノ/システム等)との通信に限定する。
PR.AA-03	ユーザー、サービス、及びハードウェアが認証されている。	CPS.AC-3	無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する。
		CPS.AC-6	特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式(例:二つ以上の認証機能を組み合わせた多要素認証)を採用する。
		CPS.AC-9	IoT 機器やユーザーによる構成要素(モノ/システム等)への論理的なアクセスを、取引のリスク(個人のセキュリティ、プライバシーのリスク及びその他の組織的なリスク)に見合う形で認証・認可する。
PR.AA-04	ID アサーションが保護され、伝達され、検証されている。		
PR.AA-05	アクセス許可、資格の付与、及び認可がポリシーで定義され、管理され、実施され、レビューされ、最小特権と職務分離の原則が組み込まれている。	CPS.AC-1	承認されたモノとヒト及びプロシージャの識別情報と認証情報を発効、管理、確認、取消、監査するプロシージャを確立し、実施する。
		CPS.AC-3	無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する。
		CPS.AC-5	職務及び責任範囲(例:ユーザー/システム管理者)を適切に分離する。
		CPS.AC-6	特権を持つユーザーのシステムへのネットワーク経由でのログインに対して、想定されるリスクも考慮して、信頼性の高い認証方式(例:二つ以上の認証機能を組み合わせた多要素認証)を採用する。
PR.AA-06	資産への物理的なアクセスが、リスクに応じて管理され、監視され、実施されている。	CPS.AC-2	IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の物理的セキュリティ対策を実施する。
		CPS.AC-7	データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する(例:開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する。
PR.AT-01	サイバーセキュリティリスクを念頭に置いて一般的な職務を遂行するための知識とスキルを有するよう、人員に意識向上とトレーニングが提供されている。	CPS.AT-1	自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。
		CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ

			教育を実施し、その記録を管理する。
PR.AT-02	サイバーセキュリティリスクを念頭に置いて関連職務を遂行するための知識とスキルを有するよう、専門的な役割を担う個人に意識向上とトレーニングが提供されている。	CPS.AT-1	自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。
		CPS.AT-2	自組織におけるセキュリティインシデントに関係し得る、セキュリティマネジメントにおいて重要度の高い関係他組織の担当者に対して、割り当てられた役割を遂行するための適切な訓練(トレーニング)、セキュリティ教育を実施し、その記録を管理する。
PR.DS-01	保存されているデータの機密性、完全性、及び可用性が保護されている。	CPS.DS-2	情報を適切な強度の方式で暗号化して保管する。
		CPS.DS-8	保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。
		CPS.DS-9	自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。
		CPS.DS-10	IoT 機器、サーバ等にて稼働するソフトウェアの完全性を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。
		CPS.DS-11	送受信・保管する情報に完全性チェックメカニズムを使用する。
		CPS.PT-2	IoT 機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバ等の機能を必要最小限とする。
PR.DS-02	伝送中のデータの機密性、完全性、及び可用性が保護されている。	CPS.DS-3	IoT 機器、サーバ等の間、サイバー空間で通信が行われる際、通信経路を暗号化する。
		CPS.DS-4	情報を送受信する際に、情報そのものを暗号化して送受信する。
		CPS.DS-8	保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。
		CPS.DS-9	自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。
PR.DS-10	使用中のデータの機密性、完全性、及び可用性が保護されている。	CPS.DS-8	保護すべき情報を扱う、あるいは自組織にとって重要な機能を有する機器を調達する場合、耐タンパーデバイスを利用する。
		CPS.DS-9	自組織外への不適切な通信を防ぐため、保護すべき情報を自組織外へ送信する通信を適切に制御する。
PR.DS-11	データのバックアップが作成され、保護され、維持され、テストされている。	CPS.IP-4	構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストする。
PR.PS-01	構成管理のプラクティスが確立され、適用されている。	CPS.IP-1	IoT 機器、サーバ等の初期設定手順(パスワード等)及び設定変更管理プロセスを導入し、運用する。
		CPS.IP-2	IoT 機器、サーバ等の導入後に、追加するソフトウェアを制限する。
		CPS.PT-2	IoT 機器、サーバ等の本体に対して、不要なネットワークポート、USB、シリアルポート等を物理的または論理的に閉塞することで、IoT 機器、サーバ等の機能を必要最小限とする。
PR.PS-02	ソフトウェアはリスクに応じて保守され、交換され、削除されている。	CPS.IP-10	脆弱性修正措置計画を作成し、計画に沿って構成要素の脆弱性を修正する。
		CPS.MA-2	自組織の IoT 機器、サーバ等に対する遠隔保守を、適用先のモノ、システムのオーナー部門による承認を得て、ログを記録し、不正アクセスを防げる形で実施する。
PR.PS-03	ハードウェアはリスクに応じて保守され、交換され、削除されている。	CPS.IP-6	IoT 機器、サーバ等の廃棄時には、内部に保存されているデータ及び、正規 IoT 機器、サーバ等を一意に識別する ID(識別子)や重要情報(秘密鍵、電子証明書等)を削除又は読み取りできない状態にする。
		CPS.MA-1	IoT 機器、サーバ等のセキュリティ上重要なアップデート等を、必要なタイミングに管理されたツールを利用して適切に履歴を記録しつつ実施する。 可能であれば、遠隔地からの操作によってソフトウェア(OS、ドライバ、アプリケーション)を一括して更新するリモートアップデートの仕組みを備えた IoT 機器を導入する。

PR.PS-04	ログ記録が生成され、継続的監視のために利用可能となっている。	CPS.PT-1	セキュリティインシデントを適切に検知するため、監査記録/ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューする。
PR.PS-05	認可されていないソフトウェアのインストール及び実行が防止されている。	CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
PR.PS-06	セキュアなソフトウェア開発プラクティスが統合され、その実行がソフトウェア開発ライフサイクル全体を通じて監視されている。	CPS.IP-3	システムを管理するためのシステム開発ライフサイクルを導入する。
PR.IR-01	ネットワーク及び環境が認可されていない論理アクセス及び使用から保護されている。	CPS.AC-3	無線接続先(ユーザーや IoT 機器、サーバ等)を正しく認証する。
		CPS.AC-7	データフロー制御ポリシーを定め、それに従って適宜ネットワークを分離する(例:開発・テスト環境と実運用環境、IoT 機器を含む環境と組織内の他の環境)等してネットワークの完全性を保護する。
PR.IR-02	組織の技術資産が環境上の脅威から保護されている。	CPS.IP-5	無停電電源装置、防火設備の確保、浸水からの保護等、自組織の IoT 機器、サーバ等の物理的な動作環境に関するポリシーや規則を満たすよう物理的な対策を実施する。
PR.IR-03	通常時及び困難な状況でのレジリエンス要件を達成するためのメカニズムが実装されている。	CPS.PT-3	ネットワークにつながることを踏まえた安全性を実装する IoT 機器を導入する。
PR.IR-04	可用性を確実にするために十分なリソース容量が維持されている。	CPS.DS-6	サービス拒否攻撃等のサイバー攻撃を受けた場合でも、資産を適切に保護し、攻撃による影響を最小限にできるよう、構成要素において十分なリソース(例:ヒト、モト、システム)を確保する。
		CPS.DS-7	IoT 機器、通信機器、回線等に対し、定期的な品質管理、予備機や無停電電源装置の確保、冗長化、故障の検知、交換作業、ソフトウェアの更新を行う。
DE.CM-01	潜在的な有害事象を発見するために、ネットワーク及びネットワークサービスが監視されている。	CPS.CM-1	組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。
		CPS.CM-3	指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。
		CPS.CM-4	サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。
		CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
DE.CM-02	潜在的な有害事象を発見するために、物理的環境が監視されている。	CPS.CM-2	組織内のネットワークと広域ネットワークの接点において、ネットワーク監視・制御、アクセス監視・制御を実施する。
DE.CM-03	潜在的な有害事象を発見するために、人員の活動及び技術の利用が監視されている。	CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
DE.CM-06	潜在的な有害事象を発見するために、外部サービスプロバイダの活動及びサービスが監視されている。	CPS.CM-5	セキュリティ事象を適切に検知できるよう、外部サービスプロバイダとの通信内容をモニタリングする。
		CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
DE.CM-09	潜在的な有害事象を発見するために、コンピューティングハードウェアとソフトウェア、ランタイム環境、及びそれらのデータが監視されている。	CPS.CM-3	指示された動作内容と実際の動作結果を比較して、異常の検知や動作の停止を行う IoT 機器を導入する。サイバー空間から受ける情報が悪質なコードを含んでおらず、許容範囲内であることを動作前に検証する。
		CPS.CM-4	サイバー空間から受ける情報の完全性及び真正性を動作前に確認する。
		CPS.CM-6	機器等の構成管理では、ソフトウェア構成情報、ネットワーク接続状況(ネットワーク接続の有無、アクセス先等)及び他のソシキ、ヒト、モノ、システムとの情報の送受信状況について、継続的に管理する。
		CPS.DS-10	IoT 機器、サーバ等にて稼働するソフトウェアの完全性

			を組織が定めるタイミングで検証し、不正なソフトウェアの起動を防止する。
		CPS.DS-12	ハードウェアの完全性を検証するために完全性チェックメカニズムを使用する。
DE.AE-02	関連する活動をよりよく理解するために、潜在的な有害事象が分析されている。	CPS.AE-2	セキュリティ管理責任者を任命し、セキュリティ対応組織（SOC/CSIRT）を立ち上げ、組織内でセキュリティ事象を検知・分析・対応する体制を整える。
DE.AE-03	情報は複数の情報源から相互に関連付けられている	CPS.AE-3	セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。
DE.AE-04	有害事象の推定されるインパクトと範囲が理解されている。	CPS.AE-4	関係する他組織への影響を含めてセキュリティ事象がもたらす影響を特定する。
DE.AE-06	有害事象に関する情報が、認可されたスタッフ及びツールに提供されている。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
DE.AE-07	サイバー脅威インテリジェンス及びその他の文脈的情報が分析に統合されている。	CPS.AE-3	セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。
DE.AE-08	有害事象が、定義されたインシデント基準を満たす場合に、インシデントが宣言される。	CPS.AE-5	セキュリティ事象の危険度の判定基準を定める。
RS.MA-01	インシデントが宣言されると、関連する第三者と連携してインシデント対応計画が実行されている。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
		CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
RS.MA-02	インシデント報告がトリアージされ、妥当性が確認されている。	CPS.AE-3	セキュリティ事象の相関の分析及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントを正確に特定する。
		CPS.AN-1	セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。
RS.MA-03	インシデントが分類され、優先順位が付けられている。	CPS.AN-1	セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。
		CPS.AN-3	検知されたセキュリティインシデントの情報は、セキュリティに関する影響度の大小や侵入経路等で分類し、保管する。
RS.MA-04	インシデントは必要に応じてエスカレーションまたは昇格されている。	CPS.AN-1	セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。
		CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
RS.MA-05	インシデントの復旧の開始基準が適用されている。	CPS.RP-3	自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
RS.AN-03	インシデント発生中に何が起こったのか、及びインシデントの根本原因を特定するための分析が実施されている。	CPS.AN-2	セキュリティインシデント発生後に、デジタルフォレンジックを実施する。
RS.AN-06	調査中に実施されたアクションが記録され、記録の完全性と来歴が保持されている。	CPS.AN-2	セキュリティインシデント発生後に、デジタルフォレンジックを実施する。
RS.AN-07	インシデントのデータ及びメタデータが収集され、その完全性と来歴が保持されている。		
RS.AN-08	インシデントの規模が推定され、妥当性が確認されている。	CPS.AN-1	セキュリティインシデントの全容と、推測される攻撃者の意図から、自組織及び関係する他組織を含む社会全体への影響を把握する。
RS.CO-02	社内外のステークホルダーにインシデントを通知する。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順（セキュリティ運用プロセス）をあらかじめ定義し、実装する。
RS.CO-03	指定された社内外のステークホルダーと情報を共有する。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順（セキュリテ

			ィ運用プロセス)をあらかじめ定義し、実装する。
		CPS.RP-2	セキュリティ運用プロセスにおいて、取引先等の関係する他組織との連携について手順と役割分担を定め、運用する。
RS.MI-01	インシデントが封じ込められている。	CPS.MI-1	セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。
RS.MI-02	インシデントが根絶されている。	CPS.MI-1	セキュリティインシデントによる被害の拡大を最小限に抑え、影響を低減する対応を行う。
RC.RP-01	インシデント対応計画の復旧に関する部分が、インシデント対応プロセスから取り組みが開始されると実行されている。	CPS.RP-3	自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
RC.RP-02	復旧活動が選択され、範囲が設定され、優先順位が付けられ、実施されている。	CPS.RP-3	自然災害時における対応方針及び対応手順を定めている事業継続計画又は緊急事対応計画の中にセキュリティインシデントを位置づける。
RC.RP-03	バックアップ及びその他の復旧資産の完全性が、復旧に使用する前に検証されている。	CPS.IP-4	構成要素(IoT 機器、通信機器、回線等)に対し、定期的なシステムバックアップを実施し、テストする。
RC.RP-04	重要なミッション機能とサイバーセキュリティリスクマネジメントが、インシデント後の運用規範を確立するために考慮されている。		
RC.RP-05	復旧した資産の完全性が検証され、システム及びサービスが復旧し、正常な運用状態が確認されている。		
RC.RP-06	基準に基づいてインシデント復旧の終了が宣言され、インシデント関連の文書の作成が完成している。		
RC.CO-03	復旧活動及び運用ケイパビリティ(能力)復旧の進捗状況が、指定された社内外のステークホルダーに伝達されている。	CPS.CO-3	復旧活動について内部及び外部の利害関係者と役員、そして経営陣に伝達する点を、事業継続計画又は緊急事対応計画の中に位置づける。
RC.CO-04	インシデント復旧に関する公開最新情報は、承認された方法及びメッセージングを使用して共有されている。	CPS.RP-1	セキュリティインシデント発生後の対応の内容や優先順位、対策範囲を明確にするため、インシデントを検知した後の組織/ヒト/モノ/システムの対応手順(セキュリティ運用プロセス)をあらかじめ定義し、実装する。
		CPS.CO-1	セキュリティインシデント発生後の情報公表時のルールを策定し、運用する。
		CPS.CO-2	事業継続計画又は緊急事対応計画の中に、セキュリティインシデントの発生後、組織に対する社会的評価の回復に取り組む点を位置づける。

Appendix B:用語/略語

AMHS ≪Automated Material Handling Systems:自動搬送システム≫

APT ≪Advanced Persistent Threat≫

CAD ≪Computer-Aided Design:コンピュータ支援設計≫

CASB ≪Cloud Access Security Broker≫

CCD ≪Charge Coupled Devices≫

CSPM ≪Cloud Security Posture Management:クラウドセキュリティ態勢管理≫

CSIRT ≪Computer Security Incident Response Team≫

CVE ≪Common Vulnerabilities and Exposures≫

CVSS ≪Common Vulnerability Scoring System:共通脆弱性評価システム≫

CWPP ≪Cloud Workload Protection Platform≫

DCS ≪Distributed Control System:分散制御システム≫

DMZ ≪DeMilitarized Zone:非武装地帯≫

EAP ≪Extensible Authentication Protocol:拡張認証プロトコル≫

EDA ≪Electronic Design Automation≫

EDR ≪Endpoint Detection and Response:エンドポイントの検知と対応≫

EOSL ≪End of Service Life≫

EPP ≪Endpoint Protection Platform:エンドポイント保護プラットフォーム≫

FOUP ≪Front Opening Unified Pod≫

FSIRT ≪Factory Security Incident Response Team≫

GEM ≪Generic Equipment Model:汎用機器モデル≫

HSMS ≪High Speed Message Service≫

IAM ≪Identity and Access Management≫

I/O ≪Input/Output:入出力≫

IDS ≪Intrusion Detection System:不正侵入検知システム≫

IPS ≪Intrusion Prevention System:不正侵入防止システム≫

JVN ≪Japan Vulnerability Note≫

MCS ≪Material Control System≫

MES ≪Manufacturing Execution System≫

MSRC ≪Microsoft Security Response Center≫

NDR ≪Network Detection and Response≫

NVD ≪National Vulnerability Database≫

OEM ≪Original Equipment Manufacturing:相手先ブランド製造≫

OHT ≪Overhead Hoist Transport:天井走行式無人搬送車≫

PLC ≪Programmable Logic Controller:プログラマブルロジックコントローラ≫

PSIRT ≪Product Security Incident Response Team≫

SBOM ≪Software Bill of Materials:ソフトウェア部品表≫

SECS ≪SEMI Equipment Communications Standard:SEMI 機器通信規格≫

SPC ≪Statistical Process Control:統計的工程管理≫

SSPM ≪SaaS Security Posture Management:SaaS セキュリティ態勢管理≫

SSVC ≪Stakeholder-Specific Vulnerability Categorization≫

VPN ≪Virtual Private Network:仮想専用通信網≫

WORM ≪Write Once Read Many≫

アクセス制御
情報及び関連情報処理サービスの取得及び使用、ならびに特定の物理施設(例:連邦政府の建物、軍事施設、国境検問所)への入場の具体的な要求を許可または拒否するプロセス。[NIST SP 800-53 Rev.5]

アクティブスキャン
ネットワークやシステムの脆弱性を積極的に探すために、パケットやプローブを送信するセキュリティ評価手法。ポートスキャン、脆弱性スキャン、侵入テスト等が含まれ、システムの設定ミスや既知の脆弱性を特定することで、セキュリティリスクを評価する。

異常検知
サイバーセキュリティ攻撃を検知するための多面的なアプローチを提供する仕組み。[NISTIR 8219]

インシデント
情報システム、またはそのシステムが処理、保存、送信する情報の機密性、完全性、可用性

を実際に、または潜在的に危険にさらす出来事、またはセキュリティポリシー、セキュリティ手順、許容利用ポリシーの違反、もしくは違反の差し迫った脅威を構成する出来事。[NIST SP 800-12 Rev. 1]

エンタープライズ
明確な使命/目標と明確な境界を持ち、その使命を実行するために情報システムを使用し、自身のリスクとパフォーマンスを管理する責任を持つ組織。企業は、調達、プログラム管理、財務管理(例:予算)、人事、セキュリティ、情報システム、情報及びミッション管理といったビジネス側面の全てまたは一部で構成される場合がある。[NIST SP 800-53 Rev.4]

エンドポイント
組織のネットワークに接続するコンピュータ、モバイルデバイス、IoT デバイス、その他の端末等、情報システムにアクセスまたはデータの送受信を行うあらゆるデバイス。

脅威
情報システムを介した不正アクセス、破壊、開示、情報の変更、またはサービス拒否を通じて、組織の運用(ミッション、機能、イメージ、評判を含む)、組織資産、個人、他の組織、または国家に悪影響を与える可能性のある状況や出来事。[NIST SP 800-30 Rev.1]

クラウド
設定可能なコンピューティングリソース(例:ネットワーク、サーバ、ストレージ、アプリケーション、サービス)の共有可能なリソース群に対し、遍在で便利なオンデマンドのネットワークアクセスを可能にするモデル。このリソースは、最小限の管理作業またはサービスプロバサーバとのやり取りで迅速にプロビジョニング及びリリースできる。[NIST SP 800-53 Rev.4]

ゲートウェイ
機能は似ているが実装が異なる 2 つ(またはそれ以上)のコンピュータネットワークに接続し、ネットワーク間の単方向または双方向の通信を可能にする中間システム(インタフェース、リレー)。[NIST SP 800-53 Rev.4]

権限分離
システムへのアクセスを制限し、最小権限の原則を適用することで、単一のユーザーやプ

ロセスが過剰な権限を持つことを防ぐためのセキュリティ対策。

構成管理
システム開発ライフサイクル全体にわたって、情報技術製品及びシステムの構成を初期化、変更、及び監視するプロセスを制御することにより、それらの製品及びシステムの整合性を確立及び維持することに焦点を当てた一連の活動。[NIST SP 800-53 Rev.5]

コンジット
産業オートメーション及び制御システム(IACS)環境内の異なるゾーン間で情報を伝達するために使用される通信チャネル。異なるセキュリティレベルのゾーン間の安全な通信を可能にする。

コンソール
計算リソースと対話するために使用される、視覚指向の入出力デバイス。[NIST SP 1800-27B]

コンポーネント
システムの構成要素を表す、個別に識別可能な情報技術資産。ハードウェア、ソフトウェア、ファームウェアを含む場合がある。[NIST SP 800-53 Rev.5]

サイバーセキュリティ
コンピュータ、電子通信システム、電子通信サービス、有線通信、及びそれらに含まれる情報を含む電子通信の損害防止、保護、及び復旧を行い、それらの可用性、完全性、認証、機密性、及び否認防止を確保すること。[NIST SP 800-53 Rev. 5]

サーバ
ネットワークリソースを管理する、ネットワーク上のコンピュータまたはデバイス。ファイルサーバ(ファイルを保存するため)、プリントサーバ(1 台以上のプリンターを管理するため)、ネットワークサーバ(ネットワークトラフィックを管理するため)、データベースサーバ(データベースクエリを処理するため)等がある。[NIST SP 800-175B Rev.1]

サプライチェーン
複数の階層の組織間で接続されたリソースとプロセスのセットであり、それぞれが取得者として、製品とサービスの調達から始まり、ライフサイクル全体に及ぶ。 [NIST SP 800-53 Rev.5]

産業制御システム(ICS)
製造、製品の出荷、生産、及び販売等の産業プロセスを制御するのに使用される情報システム。産業用制御システムには、地理的に分散している資産を管理する のに使用される監視制御データ収集システム(SCADA)、分散制御システム(DCS)、 及び前二者より小規模ながらローカルなプロセスをプログラマブル論理制御装 置(PLC)の利用を通じて制御するシステム等がある。[NIST SP 800-53 Rev.4]

システム
情報の収集、処理、維持、使用、共有、配布、または処分のために編成された、個別の情報資源の集合。[NIST SP 800-30 Rev.1]

脆弱性
脅威ソースによって悪用またはトリガーされる可能性のある、情報システム、システムセキュリティ手順、内部制御、または実装の弱点。[NIST SP 800-53 Rev.5]

セキュリティログ
システム上で行われたイベントの記録。セキュリティ関連のイベント(ログイン試行、ファイルアクセス、システム変更等)に関する情報を含む。

ソフトウェア
実行中に動的に書き込まれたり変更されたりする可能性のあるコンピュータプログラムと関連データ。[NIST SP 800-53 Rev.4]

ゾーン
共通のセキュリティレベルを持つ論理的なグループにまとめられた IACS システムの要素の集合。異なるセキュリティレベルのゾーン間の情報フローを制限することで、セキュリティリスクを軽減する。

多層防御
組織の複数のレイヤー及びミッションにわたって可変的なバリアを確立するために、人、技術、及び運用機能を統合する情報セキュリティ戦略。[NIST SP 800-53 Rev.4]

多要素認証(MFA)
認証を達成するために 2 つ以上の異なる要素を使用する認証。要素には、(i) 本人が知

っているもの(例:パスワード/PIN)、(ii) あなたが持っているもの(例:暗号識別デバイス、トークン)、または (iii) 自身(例:生体認証)が含まれる。[NIST SP 800-53 Rev.4]

認証
上級組織職員によって与えられる公式の管理決定であり、情報システムの運用を承認し、合意された一連のセキュリティ管理の実装に基づいて、組織の運用(ミッション、機能、イメージ、評判を含む)、組織資産、個人、他の組織、及び国家に対するリスクを明示的に受け入れることを指す。[NIST SP 800-53 Rev.4]

ネットワーク
相互接続されたコンポーネントの集合で実装された情報システム。このようなコンポーネントには、ルーター、ハブ、ケーブル、通信コントローラ、鍵配布センター、及び技術制御デバイスが含まれる場合がある。[NIST SP 800-53 Rev.4]

ネットワーク管理
ネットワークインフラストラクチャの運用、監視、保守、及び最適化のプロセス全体。

ハードウェア
情報システムの物理的なコンポーネント。[NIST SP 800-53 Rev.4]

ハードニング
脆弱性を修正し、不要なサービスをオフにすることによって、攻撃手段を排除することを目的としたプロセス。[NIST SP 800-152]

汎用 OS
特定の用途やハードウェアに特化しておらず、幅広い種類のコンピュータシステムやアプリケーションで使用可能な OS。

ファイア・ウォール
ローカルセキュリティポリシーに従ってネットワーク間のアクセスを制限するゲートウェイ。[NIST SP 800-53 Rev.4]

ファームウェア
ハードウェア(通常は読み取り専用メモリ(ROM)またはプログラム可能な読み取り専用

メモリ(PROM))に保存されたコンピュータプログラムとデータであり、プログラムの実行中にプログラムとデータを動的に書き込んだり変更したりできないもの。[NIST SP 800-53 Rev.4]

プロトコル
システム間のある種の関連付け(例えば、通信)を実装及び制御するための一連の規則(すなわち、形式と手順)。[NIST SP 800-53 Rev.4]

フロント PC
装置ツールを操作・制御するための、装置ツールに付属する PC。ファブネットワークへの接続機能を持ち、コンソール操作機能や記憶媒体接続機能等を提供する。

ポート
通信デバイスや周辺機器を接続するための、コンピュータへの入り口または出口地点。[NIST SP 800-82r3]

マルウェア
情報システムの機密性、完全性、または可用性に悪影響を与える不正なプロセスを実行することを意図したソフトウェアまたはファームウェア。ウイルス、ワーム、トロイの木馬、またはホストに感染するその他のコードベースのエンティティ。[NIST SP 800-53 Rev.5]

リスク
エンティティが潜在的な状況またはイベントによって脅かされる範囲の尺度であり、通常以下の要素によって決定される。(i) 状況またはイベントが発生した場合に発生する悪影響、及び (ii) 発生の可能性。[NIST SP 800-30 Rev.1]

リスク分析
システムの運用に起因する、組織の運用(ミッション、機能、イメージ、評判を含む)、組織の資産、個人、他の組織、及び国家に対するリスクを特定するプロセス。[NIST SP 800-30 Rev.1]

リスクマネジメント
組織の運用(ミッション、機能、イメージ、評判を含む)、組織の資産、個人、他の組織、及び国家に対する情報セキュリティリスクを管理するためのプログラムとサポートプロセスであり、以下が含まれる。(i) リスク関連活動のコンテキストの設定。(ii) リスクの評価。

（iii）リスクが特定された場合の対応。（iv）時間の経過に伴うリスクの監視。[NIST SP 800-30 Rev.1]

リファレンスアーキテクチャ
特定のドメインや業界におけるシステムやソリューションの構築・運用・管理に関するベストプラクティスや標準的な構成要素を示したテンプレートまたはフレームワーク。

レジリエンス
情報システムが以下を継続する能力。（i）悪条件または負荷がかかる状態でも、低下または衰弱した状態であっても、不可欠な運用能力を維持しながら運用すること。（ii）ミッションのニーズに合った時間枠で効果的な運用体制に回復すること。[NIST SP 800-39]

ログ
組織のシステム及びネットワーク内で発生するイベントの記録。[NIST SP 800-92]

本ガイドラインの検討体制

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（実効性強化・国際連携）
半導体産業サブワーキンググループ　構成員一覧
※敬称略、五十音順、2025 年 10 月 24 日時点

	秋山 裕明	マイクロンメモリジャパン株式会社　ディレクター
	飯嶋 織行	東京エレクトロン株式会社 製品セキュリティ戦略部　部長
座長	江崎 浩	東京大学大学院 情報理工学系研究科教授
	高橋 清文	株式会社ニコン 経営管理本部情報セキュリティ推進部長
	高原 正裕	株式会社ダイフク クリーンルーム事業部生産本部システム部 部長
	長野 茂樹	株式会社 SCREEN システムサービス 代表取締役社長
	二上哲也	Rapidus 株式会社　CIO（※2025 年 9 月～）
	（藤井 俊郎	Rapidus 株式会社　IT・デジタル本部 副部長/IT セキュリティ部長（※～2025 年 9 月））
	浜島 雅彦	SEMI ジャパン 代表取締役
	濱田 正紀	一般社団法人電子情報技術産業協会　半導体部会 半導体統括委員会 委員長（※2025 年 9 月～）
	（中川 昭一	一般社団法人電子情報技術産業協会　半導体部会 半導体統括委員会 委員長（※～2025 年 9 月））
	東 健介	株式会社アドバンテスト　法務知財コンプライアンス統括部長
	三井 豊興	一般社団法人電子情報技術産業協会　半導体部会 半導体統括委員会 副委員長/政策提言タスクフォース 主査
	渡部 潔	一般社団法人日本半導体製造装置協会 専務理事

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（実効性強化・国際連携）
半導体産業サブワーキンググループ　作業部会　構成員一覧
※敬称略、五十音順、2025 年 10 月 24 日時点

青木 敏	株式会社 SCREEN セミコンダクタソリューションズ 技術管理部 製品セキュリティプロジェクト
飯嶋 織行	東京エレクトロン株式会社 製品セキュリティ戦略部　部長
池田 秀正	三菱電機株式会社 パワーデバイス製作所製造管理部技術管理課 課長
今林 晃一	東芝デバイス＆ストレージ株式会社 半導体経営企画部
小野　治	サンケン電気株式会社 ものづくり本部ものづくり開発センター生産改革部システム開発課
門田 栄一	三菱電機株式会社 半導体・デバイス業務部 情報システム課 主任
金子 優美	ソニーセミコンダクタソリューションズ株式会社 企画管理部門情報セキュリティ部
河上 勇一	東芝デバイス＆ストレージ株式会社 IT 推進部
小林 知之	株式会社 SCREEN ホールディングス 経営戦略本部 IT 室 情報セキュリティ部
小林 仁	ヌヴォトンテクノロジージャパン株式会社 情報セキュリティ委員会
佐々木 慎介	キオクシア株式会社 サイバーセキュリティセンター
鈴木 雅大	株式会社ニコン 半導体事業開発統括部第四開発部
高橋 清文	株式会社ニコン 経営管理本部情報セキュリティ推進部長
高原 正裕	株式会社ダイフク クリーンルーム事業部生産本部システム部 部長
田中 暁	東京エレクトロン株式会社 情報セキュリティ部
椿田 収	株式会社ベリサーブ サイバーセキュリティ事業部
飛田 英恵	ルネサスエレクトロニクス株式会社 情報システム統括部 情報セキュリティ部 シニアマネージャー
中川 昭一	一般社団法人電子情報技術産業協会　半導体部会 半導体統括委員会 委員長
中西 博一	ソニーセミコンダクタマニュファクチャリング株式会社 企画管理部門情報システム部
長野 茂樹	株式会社 SCREEN システムサービス 代表取締役社長
中村 宏	Rapidus 株式会社　IT・デジタル本部　IT セキュリティ部 シニアマネージャー
西村 剛幸	株式会社 SCREEN セミコンダクタソリューションズ 技術管理部
萩尾 英二	東京エレクトロン株式会社 情報セキュリティ部

林 忠弘	ルネサスエレクトロニクス株式会社 情報システム統括部 情報セキュリティ部 部長
林 資泰	株式会社 SCREEN セミコンダクタソリューションズ 技術管理部 製品セキュリティプロジェクト
林 良太郎	キオクシア株式会社 サイバーセキュリティセンター セキュリティ企画・管理担当
福山 亮治	ソニーセミコンダクタマニュファクチャリング株式会社 企画管理部門情報セキュリティ部
堀江 純平	株式会社 SCREEN ホールディングス 経営戦略本部 IT 室 情報セキュリティ部
牧岡 孝則	サンケン電気株式会社 事業推進本部 DX 推進統括部 IT 推進部 業務アプリケーション課
真辺 雄一	ソニーセミコンダクタマニュファクチャリング株式会社 企画管理部門情報セキュリティ部
松尾 泰三	東芝デバイス&ストレージ株式会社 IT 推進部
松田 英克	東京エレクトロン株式会社 製品セキュリティ戦略部
三井 豊興	一般社団法人電子情報技術産業協会　半導体部会 半導体統括委員会 副委員長/政策提言タスクフォース 主査
森 隆久	ソニーセミコンダクタソリューションズ株式会社 企画管理部門情報セキュリティ部
吉田 秀二	ソニーセミコンダクタマニュファクチャリング株式会社 企画管理部門情報セキュリティ部
渡部 潔	一般社団法人日本半導体製造装置協会 専務理事
株式会社ダイフク	
マイクロンメモリジャパン株式会社	
ローム株式会社	