令和７年３月31日

令和6年度中小企業対外経済政策推進事業

（半導体産業分野におけるセキュリティガイドラインの整備等に関する調査）

報告書

目次

改訂履歴

1. エグゼクティブサマリ

- 我が国では、半導体関連産業の国内投資の促進が強力に進められているところ、特定重要物資である半導体の安定的な供給を確保する観点や、製造技術等の機微情報を適切に管理し競争力を維持向上する観点からも、サイバーセキュリティ対策を進めることが極めて重要である。
- 海外では半導体製造装置のセキュリティ規格の策定や調達要件化等、サプライチェーンにおける取引先へのセキュリティ対策が要請されている一方、国内ではそのような基準も存在せず、業界としての蓄積もないため、個々の企業による取組に依存している状態である。
- 本事業では、我が国の半導体関連産業（半導体デバイス、半導体製造装置、部素材等）におけるセキュリティの確保に向けて、国際的なセキュリティ検討の動向、企業のセキュリティ対策状況や製品セキュリティへの取組の実態を把握しつつ、半導体関連企業がセキュリティ対策を行う上で、留意すべき点や具体的な対策をまとめたガイドラインの策定を目的に、調査や検討会の運営、資料作成等を実施した。
- 事業内容（1）「国際動向調査」では、半導体工場に対するサイバー攻撃事例や規格等を含めた国際的なセキュリティ検討の動向の調査及び半導体関連企業のセキュリティ対策状況や製品セキュリティへの取組の実態に関する調査を行った。
- 規格等の調査ではインターネットの公開情報を調査したり会議体に参加して情報収集を行ったり、E187、CPSF 及び NIST CSF 2.0 半導体製造プロファイル等複数の規格を分析し、関係性を整理した。取組実態調査においては、半導体デバイスメーカに対してヒアリングを行い、調査結果を取りまとめた。
- 事業内容（2）「半導体デバイス工場における OT ガイドライン素案の作成」では、上記の調査結果を踏まえ、知財等重要情報流出の防止を目的とした「半導体産業におけるセキュリティ対策基準」及びサイバー攻撃による事業継続リスクへの対策を目的とした「半導体デバイス工場における OT ガイドライン」素案を作成した。
- 事業内容（3）「検討会の運営」では、上記の調査の実施、半導体デバイス工場における OT ガイドライン素案の作成、取りまとめをする過程で、専門的な見地からの検討、分析、助言を得ることを目的に、半導体関連産業の関係者やサイバーセキュリティに関する有識者等からなる検討会（「半導体産業 SWG」、「半導体産業 SWG 作業部会」）を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 配下に設置し、会議の開催、運営を行った。
- 「半導体産業 SWG」では方向性を検討し、その下に設置された「半導体産業 SWG 作業部会」ではガイドラインの具体的な検討を行った。

2. 本事業の概要

2.1 目的

我が国では、半導体関連産業の国内投資の促進が強力に進められているところ、特定重要物資である半導体の安定的な供給を確保する観点や、製造技術等の機微情報を適切に管理し競争力を維持向上する観点からも、サイバーセキュリティ対策を進めることが極めて重要である。

しかしながら、海外では半導体製造装置のセキュリティ規格の策定や調達要件化等、サプライチェーンにおける取引先へのセキュリティ対策が要請されている一方、国内ではそのような基準も存在せず、業界としての蓄積もないため、個々の企業による取組に依存している状態である。

本事業では、我が国の半導体関連産業(半導体デバイス、半導体製造装置、部素材等)におけるセキュリティの確保に向けて、国際的なセキュリティ検討の動向、企業のセキュリティ対策状況や製品セキュリティへの取組の実態を把握しつつ、半導体関連企業がセキュリティ対策を行う上で、留意すべき点や具体的な対策をまとめたガイドラインの策定を目的に、調査や検討会の運営、資料作成等を実施した。

2.2 事業内容

上記の事業目的を達成するために、以下(1)～(3)事業を実施し、調査結果を調査報告書として取りまとめる。

(1)国際動向調査

本事業では、知財等重要情報流出の防止を目的とした半導体産業におけるセキュリティ対策基準及びサイバー攻撃による事業継続リスクへの対策を目的とした「半導体デバイス工場における OT ガイドライン」を作成するため、半導体関連産業の工場に対する国際的なセキュリティ対策の検討の動向、半導体関連企業のセキュリティ対策状況や製品セキュリティへの取組の実態を調査した。調査対象とした主な規格や会議体等を以下に示す。

1) 国際的なセキュリティ検討の動向

- SEMI[1](Semiconductor Equipment and Materials International)
- SMCC[2](Semiconductor Manufacturing Cybersecurity Consortium)
- NIST[3](National Institute of Standards and Technology)

[1] 国際半導体製造装置材料協会(SEMI): https://www.semi.org/jp
[2] 半導体製造サイバーセキュリティコンソーシアム(SMCC)
[3] 米国国立標準技術研究所(NIST)

- 経済産業省 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
  サプライチェーン強化に向けたセキュリティ対策評価制度に関する SWG

2） 国際規格、基準、ガイドライン等

- NIST IR 8546, Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile （Initial Public Draft)[4]
  （以下、NIST CSF2.0 半導体製造プロファイル）
- NIST Cybersecurity Framework（CSF）2.0[5]（以下、NIST CSF2.0）
- SEMI E187 - Specification for Cybersecurity of Fab Equipment[6]（以下、E187）
- SEMI E187 Cybersecurity Reference Architecture for Semiconductor Manufacturing Environments[7]（以下、E187 製造リファレンス）
- SEMI E189 Specification for Equipment Management of Consumables and Durables（EMCD)[8]（以下、E189）
- サイバー・フィジカル・セキュリティ対策フレームワーク[9]（以下、CPSF）
- 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[10]
  （以下、工場ガイドライン）

（2)半導体デバイス工場におけるOTガイドライン素案の作成

上記の調査結果を踏まえ、知財等重要情報流出の防止を目的とした半導体産業におけるセキュリティ対策基準及びサイバー攻撃による事業継続リスクへの対策を目的とした「半導体デバイス工場における OT ガイドライン」素案を作成した。半導体デバイス工場における OT ガイドライン素案の作成に当たっては以下の資料を参照した。

- NIST CSF2.0 半導体製造プロファイル
- NIST CSF2.0

---

[4] NIST CSF2.0 半導体製造プロファイル(NIST IR 8546, Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile):https://csrc.nist.gov/pubs/ir/8546/ipd
[5] NIST CSF2.0): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
[6] E187: https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment
[7] E187 製造リファレンス: https://www.txone.com/blog/unveiling-semi-innovative-cybersecurity-architecture/
[8] E189:https://store-us.semi.org/products/e18900-semi-e189-specification-for-equipment-management-of-consumables-and-durables-emcd
[9] CPSF: https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
[10] 工場ガイドライン:
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_ver1.0.pdf

- E187
- E187 製造リファレンス
- E189
- CPSF
- 工場ガイドライン(別冊含む)

(3)検討会の運営

上記の調査の実施、半導体デバイス工場における OT ガイドライン素案の作成、取りまとめにあたっては、専門的な見地からの検討、分析、助言を得ることを目的に、半導体関連産業の関係者やサイバーセキュリティに係る有識者等からなる以下の検討会を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 配下に設置し、会議の開催、運営を行った。

- 半導体産業サブワーキンググループ(以下、半導体産業 SWG)
- 半導体産業 SWG 作業部会(以下、作業部会)

本事業期間中の検討会等の運営を滞りなく実施するため、必要な検討材料の提供、意見の集約、調査の実施等を行った。検討会等の運営にあたっては、担当者と相談の上、方針を決定し実施した。なお、本事業期間中に、半導体産業 SWG は計 2 回、作業部会は計 4 回開催した。

2.3 実施スケジュール

本事業は、2024 年 11 月上旬より開始し、国際動向調査、半導体デバイスメーカへのヒアリングを実施したあと、NIST CSF2.0、E187 製造リファレンス、CPSF 等を参照し半導体デバイス工場における OT ガイドライン事務局案を 2 月中旬に策定し、作業部会からの意見を踏まえ修正し、3 月末に半導体産業 SWG に諮問した。また、本事業期間内に半導体産業 SWG を計 2 回、作業部会を計 4 回実施し、主に半導体デバイス工場における OT ガイドラインに対する意見を収集した。具体的なスケジュールを図 2.3-1 に示す。

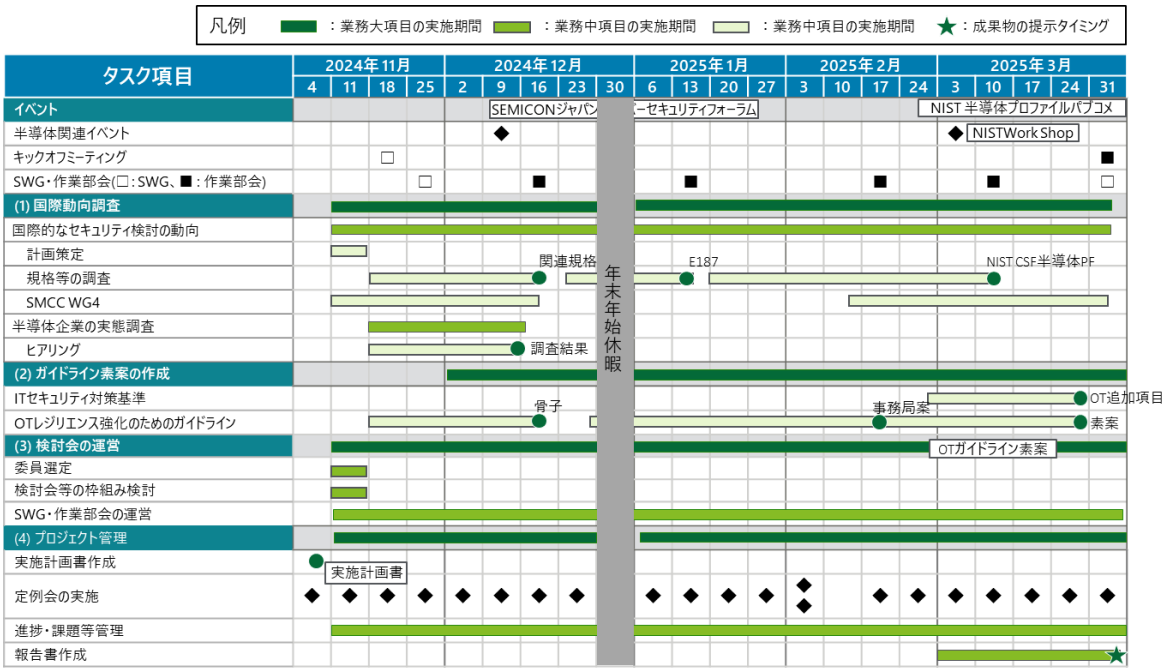


図　2.3-1　実施スケジュール

2.4　実施体制

本事業では短納期で検討会における意見を集約し、半導体デバイス工場における OT ガイドライン素案をまとめる必要があったため、半導体工場における OT セキュリティ対策の経験を持つメンバーをリーダに配置し、かつ、OT セキュリティのアドバイザリ業務の経験の豊富なメンバーを SME（Subject Matter Expert）としてアサインして実施した。

2.5　本調査報告書の構成

本調査報告書では、以下（1）～（3）事業の調査結果を調査報告書として以下の構成で取りまとめている。

（1）国際動向調査

半導体デバイス工場における OT ガイドライン素案及び半導体産業におけるセキュリティ対策基準を検討するにあたり必要となる、「国際的セキュリティ検討の動向」と「半導体関連企業のセキュリティ対策状況や製品セキュリティへの取組の実態」について、それぞれ目的、調査内容及び調査結果を報告する。

（2）ガイドライン素案の作成

本事業で検討した「半導体産業におけるセキュリティ対策基準」と「半導体デバイス工場における OT ガイドライン素案」の作成業務に関して、目的、考え方、検討の進め方及び半導体産業におけるセキュリティ対策基準、半導体デバイス工場における OT ガイドラインの概要について報告する。

（3）検討会の運営

本事業で設置、開催した半導体産業 SWG 及び作業部会の概要、各回のアジェンダ、主要な説明資料及び主要な意見について報告する。併せて、半導体産業 SWG 及び作業部会の運営業務についても報告する。

3. 国際動向調査等

知財等重要情報流出の防止を目的とした半導体産業におけるセキュリティ対策基準及びサイバー攻撃による事業継続リスクへの対策を目的とした半導体デバイス工場における OT ガイドラインを作成するために調査を行った。

本事業では主に以下の 2 つの調査を行った。

- 半導体工場に対するサイバー攻撃事例や規格等を含めた、国際的なセキュリティ検討の動向の調査
- 半導体関連企業のセキュリティ対策状況や製品セキュリティへの取組の実態に関する調査

ガイドライン作成においては、日本独自の規格を新たに作るのではなく、国際的な規格と整合が取るとの方針で進めた。かつ、半導体デバイス工場における OT ガイドラインは半導体デバイスメーカを対象として作成した。したがって、本調査もこれらガイドラインの基礎となる情報を収集することをポイントとして行った。

3.1 国際的なセキュリティ検討の動向

3.1.1サイバー攻撃の事例

（1）調査方法

外国政府や国際標準化団体の報告資料、国内外の専門誌、国内外のニュース記事、商用データベース等を対象に、インターネットの公開情報を元に調査を行った。検索する対象として、まずランサムウェアの被害の全体感を把握したうえで、半導体関連企業の被害について検索した。具体的には、Chainalysis、IPA、Recorded Future 等のサイト及び各社のホームページに掲載されているインシデント発表内容等を調査し結果をまとめた。

（2）調査結果

半導体産業においては世界中で多数のサイバー攻撃事例がある。Chainalysis の調査によると、図 3.1.1-1 のとおり、2023 年の全世界におけるランサムウェアによる身代金支払い額は、過去最高の 11 億ドル（約 1,595 億円）に到達している[11]。また、被害の業種別では、半導体産業を含む製造業が 2 位である。[12]

[11] Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline：https://www.chainalysis.com/blog/ransomware-2024/

[12] IC3 “Internet Crime Report 2023”をもとに IPA が作成したものが「IPA セキュリティ白書 2024」に掲載されている。

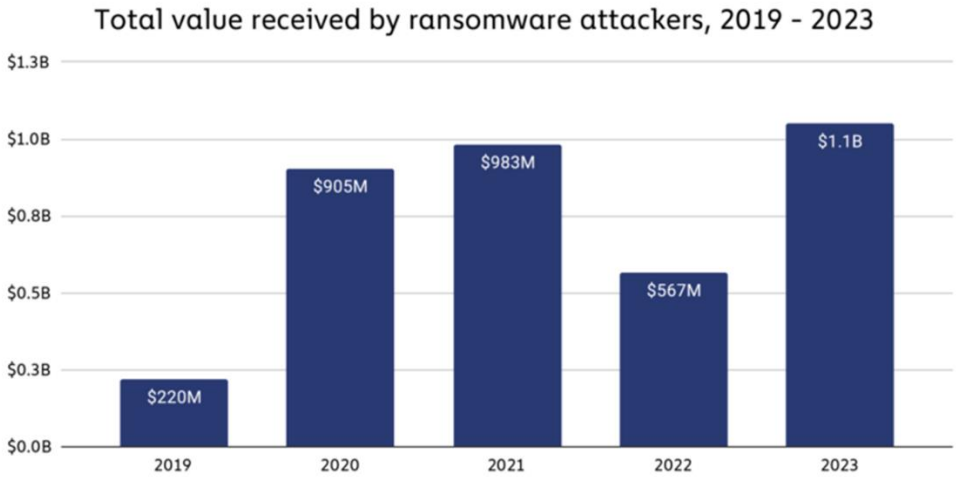


図　3.1.1-1　ランサムウェアによる被害額
出典：Chainalysis「Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline」より

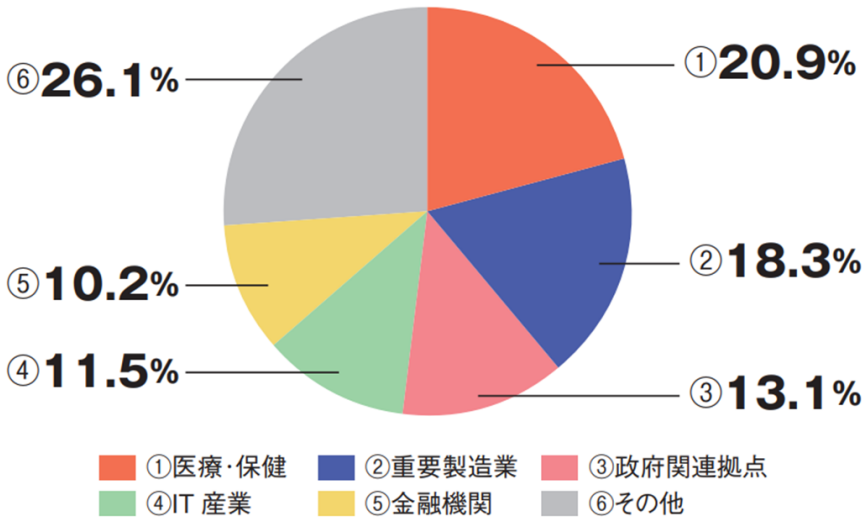


図　3.1.1-2　ランサムウェア被害の業種別構成比（2023 年）
出典：IPA「IPA セキュリティ白書 2024」より

半導体は、電子機器の心臓部として機能するため、コンピュータ、スマートフォン、テレビなど、日常生活で使われるさまざまなデバイスに不可欠な部品であり、半導体の供給が途絶えると多くの産業に影響を及ぼす。このため、半導体産業はサイバー攻撃のターゲットになりやすいと考えられる。半導体産業に対する主なサイバー攻撃の状況を表 3.1.1-1 に示す。以下の表のとおり、半導体産業に対するサイバー攻撃によるインシデントはグローバルに発生しており、そ

の数は年々増えているのが実情である。事例は海外の事案が多いが、これは公開されている情報を調査した結果であり、日本の半導体企業に対するサイバー攻撃も発生している。半導体関連企業に対するサイバー攻撃により工場を停止したインシデントも発生しており、ひとたびインシデントが発生すると他産業へも大きな影響を及ぼす。加えて、半導体の設計情報や製造にかかる生産情報は各企業の競争力の根幹となる機密情報でもあることから、産業スパイを含めた国家型 APT 攻撃の対象になりやすいことが調査の結果から推測される。

表 3.1.1-1 半導体工場に対する主なサイバー攻撃事例

#	年度	企業	被害内容
1	2018/2	TSMC(台湾)	• 先端半導体工場の製造設備 10,000 台以上に障害が発生し、複数工場を閉鎖、Apple や Qualcomm 向けチップ生産が遅延した可能性
2	2018-2019	台湾 新竹サイエンスパーク 複数の半導体ベンダー	• Chimera APT Group(中国拠点)による半導体業界に対する大規模 APT 攻撃が発生(IC 開発ソースコードや SDK 等機密情報や知的財産の搾取目的と考えられる)(CyCraft)
3	2022/2	NVIDIA(米国)	• NVIDIA の内部システムが 2 日間停止 • ハッキングされたデータの WEB 上での公開
4	2022/3	Samsung(韓国)	• ハッキングされたデータの第三者への公開
5	2022/5	AMD(米国)	• ハッキングされた一部データの WEB 上での公開 • ランサム組織による WEB 上での AMD データ脆弱性の流布
6	2022/6	Diodes(米国)	• ハッキングされたデータの WEB 上での公開
7	2022/6	Etron Technology(台湾)	• ハッキングされたデータの WEB 上での公開
8	2022/6	SilTerra(マレーシア)	• ハッキングされたデータの WEB 上での公開

9	2022/8	Semikron（ドイツ）	• ハッキングされたデータうち約10%のWEB上での公開
10	2023/2	MKS Instruments（米国）	• 生産関連システムに影響し、一部施設での運用停止 • AMATサプライチェーンとして影響
11	2023/6	Kinmax Technology（台湾）	• 内部固有のテスト環境が侵害 • TSMCの取引先として報道（被害なし）
12	2023/12-2024/2	韓国の半導体装置メーカ２社	• 北朝鮮ハッキング組織により、構成管理サーバーとセキュリティポリシーサーバーにハッキングされ、製品設計図面や施設現場の写真を搾取（韓国：国家情報院（NIS）注意喚起）
13	2023/12-2024/2	台湾の半導体ベンダー	• 中国の国家支援グループである可能性が高いRedJulietが、主に台湾の政府、学術、技術、外交組織を標的としたサイバースパイ活動を実施（Recorded Future Insikt Group）
14	2024/8	Microchip Technology（米国）	• 製造及び注文処理への影響

出典：Recorded Future「Semiconductor Companies Targeted by Ransomware」、各社インシデント発表内容[13]

※水色はAPT攻撃

3.1.2 半導体惨状におけるOTセキュリティの国際規格・基準・ガイドライン等の状況

（1）半導体産業におけるOTセキュリティの国際規格・基準等の整理

1） 調査方法

半導体デバイス工場におけるOTガイドラインを作成するにあたり、これまで国際的に普及している半導体関連のOTセキュリティ関連規格等について内容を精査し関係性を整理した。

[13] 2022年までは、Recorded Futureの「Semiconductor Companies Targeted by Ransomware」内容、2023年以降は各社のインシデント発表内容を抜粋した。

調査の対象とした規格等を以下に示す。

- NIST CSF2.0 半導体製造プロファイル
- NIST CSF2.0
- CPSF
- E187
- E188
- ISA/IEC 62443
- 工場ガイドライン

調査方法としては、まず、NIST CSF2.0 半導体製造プロファイル及び E187/E188 を精査し、各規格等の中で参照されている規格等について調査を実施、これを繰り返すことで各規格間の相互関係を整理した。調査結果は次項に示す。

2） 調査結果

半導体関連の装置ツールに対するセキュリティ要件については SEMI にて策定された E187 及び製造工場におけるセキュリティ要件を整理した E187 製造リファレンスを参照した。これら規格については、いずれも ISA/IEC62443 をベースに作成されている。

次に、NIST CSF2.0 半導体製造プロファイルに関して調査を実施した。情報に関しては、SEMI SMCC の WG4 に参加し収集した。NIST CSF2.0 半導体製造プロファイルは NIST CSF2.0 の組織プロファイルとして検討されているものであり、NIST IR 8183r1 Cybersecurity Framework Version 1.1 Manufacturing Profile Rev. 1（以下、NIST CSF1.1 製造プロファイル）をベースに、半導体工場の特徴を踏まえ特に留意すべき事項について、エコシステム、ファブ、装置ツール、エンタープライズ IT の 4 つの側面より整理されている。なお、NIST CSF2.0 半導体製造プロファイルの中では、E187/E187 製造リファレンスについても参照している。

更に、CPSF と NIST CSF2.0 半導体製造プロファイルの関係性についても整理を行った。CSPF の対策要件 ID は NIST CSF1.1 との関係性が整理されており、一方、NIST CSF2.0 の中で NIST CSF1.1 との関係が整理されている。これらを組み合わせることにより、CPSF と NIST CSF2.0 半導体製造プロファイルの関連を整理した。

なお、NIST CSF2.0 半導体製造プロファイルは、現在、パブリックコメントを募集しており、本年 6 月にファイナライズされる予定である。また、E187/E187 製造リファレンスは、現在、Ver2.0 への改版が検討されており、年末までには新たなバージョンが発行される予定である。これらの動向を踏まえながら半導体デバイス工場における OT ガイドラインについても修正していく必要がある。

セキュリティ要求事項に半導体関連の OT セキュリティ関連規格等の関係性は以下のとおりである。

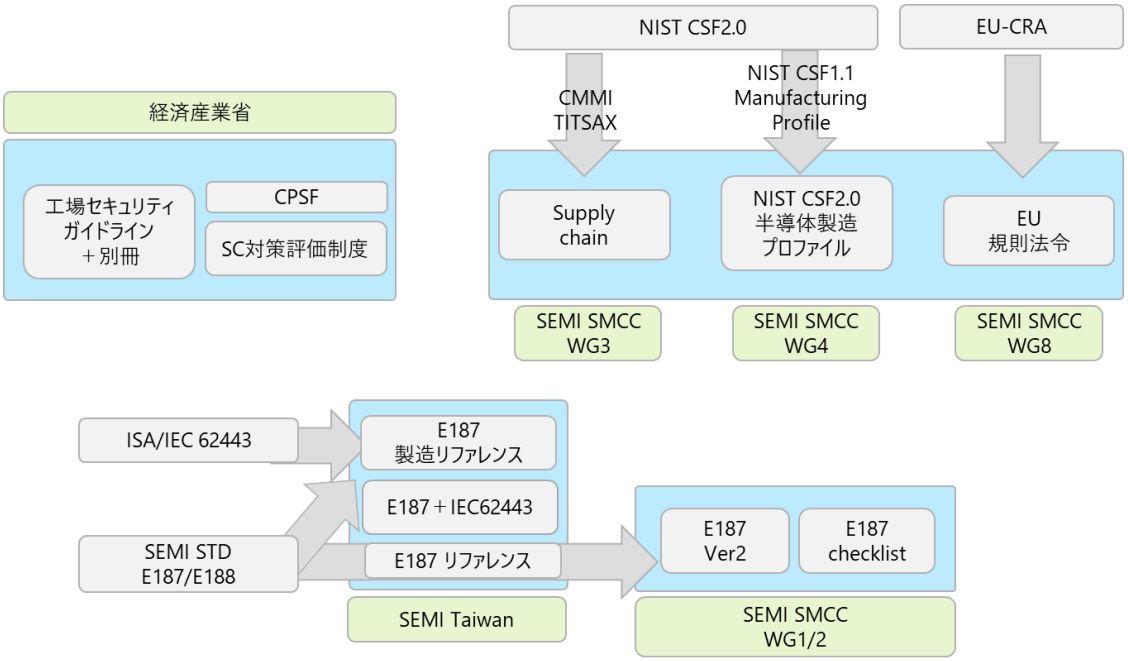


図　3.1.2-1　半導体関連の OT セキュリティ関連規格等の関係性

参考までに、経済産業省、SEMI、NIST、IPA が発行しているそれぞれの規格等の概要や特徴、URL 等に関する情報を以下の表に示す。

表　3.1.2-1　経済産業省が公表している関連フレームワーク・ガイドライン等

CPSF（サイバー・フィジカル・セキュリティ対策フレームワーク） https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html • 産業に求められるセキュリティ対策の全体像を整理した対応指針 • サイバー空間とフィジカル空間を高度に融合させることにより実現される「Society5.0」、「Connected Industries」における新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的に策定 • リスク源を整理するためのモデル（三層構造と 6 つの構成要素）を整理した「コンセプト」、モデルを活用したリスク源の整理と、リスク源に対応する対策要件を提示した「ポリシー」、対策要件に対応するセキュリティ対策例を提示した「メソッド」で構成	WG1 2019 年 04 月
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 factorysystems_guideline_ver1.0.pdf • 製造業における工場の OT セキュリティ対策を策定することを目的として策定されたガイドライン	工場 SWG

• 自社の工場におけるセキュリティ対策を企画、実行するにあたり、参照すべき考え方やステップについて記載 • 工場セキュリティで実施すべきセキュリティ対策に関するチェックリストも掲載	2022年11月
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【別冊：スマート化を進める上でのポイント】 factorysystems_guideline_appendix.pdf • 先進的な企業が工場のスマート化を進め、工場の価値創造を促進することを後押しすることを目的に策定されたガイドライン • スマート工場の概要を示すとともに、スマート化を進めるに当たってのセキュリティ対策に関する留意点や具体例について本編ステップに合わせて記載	工場SWG 2024年04月
ビル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第２版 https://www.meti.go.jp/policy/netsecurity/wg1/bill_gideline_2.pdf • ビルシステムのサイバーセキュリティに関して、その確保のためのガイダンス • ビルシステムの脅威対策について、設計、建設、竣工検査、運用、改修・廃棄のライフサイクル各段階において整理、さらに実際に脅威に遭遇した際に取るべき対応についても整理 • 追加構成、外部接続、図面管理、コスト、損害賠償・免責条件、データセンターJDCCリファレンスとの差異についても記載	ビルSWG 2023年03月
サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ（SC 対策評価制度） https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/002.html • 企業間のサプライチェーンにおける取引に着目し、企業において実施すべきセキュリティ対策を評価する制度を検討するサブワーキンググループ • セキュリティ対策要求の共通化を通じたサプライチェーン対策の重複排除、対策状況の可視化による確認の効率化を目的に、★3-★5までを評価する枠組みを検討	SC強化SWG 作成中

表 3.1.2-2 SEMI：Standard E187, E188, E169, E191 / Reference

E187	Specification for Cybersecurity of Fab Equipment（ファブ装置のサイバーセキュリティ仕様） https://store-us.semi.org/products/e18700-semi-e187-specification-for-cybersecurity-of-fab-equipment • 装置やツールの提供における安全設計（SecureDesign）に関する仕様 • 4カテゴリー（OS、NW セキュリティ、エンドポイント保護、セキュリティ監視）から 12 項目の要求事項を定義	2022 年 01 月
E188	Specification for Malware Free Equipment Integration（マルウェアに感染しない装置組み込みのための仕様） https://store-us.semi.org/products/e18800-semi-e188-specification-for-malware-free-equipment-integration • 装置やツールの導入・運用・保守のライフサイクルにおいて、デバイスメーカへマルウェアを感染させないための仕様について整理	2022 年 2 月
E169	Guide for Equipment Information System Security（装置情報システムセキュリティのためのガイド） https://store-us.semi.org/products/e16900-semi-e169-guide-for-equipment-information-system-security • 装置の情報セキュリティ運用に関する手引き目標、設備情報システムの役割、セキュリティ要件等	2014 年 4 月初版
E191 E191.1	Specification for Computing Device Cybersecurity Status Reporting（コンピューティングデバイスのサイバーセキュリティ・ステータスレポートに関する仕様）	2024 年 10 月

	https://store-us.semi.org/products/e19000-semi-e191-specification-for-computing-device-cybersecurity-status-reporting • 工場ネットワークに接続される機器(装置、搬送機、PLCS など)のサイバーセキュリティのステータスレポートに関する仕様。5つの基本項目(CDI、OS メーカ、OS 名、バージョン、ビルド)を整理 • E191.1 は、装置既存の SECS-II インターフェース経由で取得するための仕様 • 北米 CSD(Fab & Equipment Computer and Device Security)タスクフォースが、SMCC メンバーの意見を取り入れ作成	
E187 Reference Practice	• E187 の各要求事項(OS、NW セキュリティ、エンドポイント保護、セキュリティ監視の 4 カテゴリー12 項目)に対しての、解説とセキュリティ対策実装に関する Q&A 及び実践例を紹介	2022 年 10 月
Cybersecurity Reference Architecture for Semiconductor Manufacturing Environments	• 半導体製造環境を守るために、SEMI E187 及び ISC/IEC62443 シリーズに基づいた、半導体製造工場におけるセキュリティ対策リファレンスアーキテクチャ • IEC62443 の Purdue モデルにて、半導体製造環境の標準的なシステムや装置機能などを表し、10 項目の対策方法を記載	2023 年 10 月

表 3.1.2-3 NIST 関連規格

The NIST Cybersecurity Framework（CSF）2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/begoj9000000d400.pdf • 産業界、政府機関及びその他の組織が、サイバーセキュリティリスクを体系的に管理するためのガイダンス	2024 年 2 月

• あらゆる組織が CSF をもとに、セキュリティ対策状況を評価し、優先順位を付け、伝達するために使用することが可能 • 2024 年 2 月に Ver1.1 から Ver2.0 へ改版（ガバナンス、サプライチェーンリスク管理の強化等）	
NIST IR 8546 Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile. https://www.nccoe.nist.gov/projects/cybersecurity-framework-profile-semiconductor-manufacturing • 半導体業界の目標とベストプラクティスを盛り込んだ、NIST CSF2.0 の組織プロファイル • 半導体業界のサイバーセキュリティリスクを軽減するためのリスクベースのアプローチを提供 • NIST CSF1.1 製造プロファイルを参考に作成 • SEMI SMCC WG4 と連携しながら作成しており、2025 年 2 月よりパブリックコメントを募集中 • 2025 年 6 月頃に発行予定	作成中
NIST IR 8183r1 Cybersecurity Framework Version 1.1 Manufacturing Profile Rev. 1 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8183r1.pdf • NIST CSF 1.1 の製造業界の目標とベストプラクティスを盛り込んだ業界プロファイル（コミュニティ プロファイル） • 製造業界のサイバーセキュリティリスクを軽減するためのリスクベースのアプローチを提供	2020 年 10 月
NIST SP 800-82 Rev. 3 Guide to Operational Technology（OT）Security https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf • OT 環境の性能、信頼性、安全性の要件を満たしセキュリティを確保するためのガイダンス • OT トポロジーを示し、脅威と脆弱性を特定しリスクを軽減するための推奨セキュリティ対策を提供	2023 年 9 月

表 3.1.2-4 IPA（情報処理推進機構）J-CSIP/J-CRAT/ICSCoE

サイバー情報共有イニシアティブ（J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan）	2011 年 10 月～

https://www.ipa.go.jp/security/j-csip/about.html • 公的機関である IPA を情報ハブ（集約点）の役割として、参加組織間でサイバーセキュリティの脅威情報等の共有を行い、高度なサイバー攻撃対策に繋げていく取組 • 13 の SIG（Special Interest Group）に 279 の組織が参加 • 現在、半導体業界 SIG を準備中	
サイバーレスキュー隊（J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan） https://www.ipa.go.jp/security/j-crat/about.html • ウイルス不正アクセス届出制度の一環「標的型サイバー攻撃特別相談窓口」にて、広く一般から標的型サイバー攻撃（APT）に関わる相談や情報提供を受け付け、提供された情報を分析して調査結果による助言を実施 • 国家支援型と推定される標的型サイバー攻撃（APT）の被害拡大防止のため相談を受けた組織の被害の低減と攻撃の連鎖の遮断も支援	2014 年 7 月～
産業サイバーセキュリティセンター（ICSCoE：Industrial Cyber Security Center of Excellence） https://www.ipa.go.jp/icscoe/index.html • 我が国の経済・社会を支える重要インフラや産業基盤のサイバー攻撃に対する防御力を抜本的に強化 • 社会インフラ産業基盤事業者において、自社システムのリスクを認識しつつ必要なセキュリティ対策を判断できる将来人材を育成するプログラムを提供 • 情報系システムから制御系システムまでを想定した模擬プラントを設置し、専門家と共に安全性・信頼性の検証や早期復旧の演習を実施	2017 年 4 月～

（2）SEMI SMCC WG4

1）調査方法

SMCC は SEMI が主催しており、8 つのワーキンググループが存在する。[14]

- WG1（Factory cybersecurity implementation）
  半導体製造装置に関する既存の SEMI 規格（E187 及び E188）において、サイバーセキュリティ防御を運用する方法など、解釈や必要なアクションについて特

[14] https://www.semi.org/en/industry-groups/semiconductor-cybersecurity/working-groups

定している。

- WG2（compliance readiness）
  装置メーカ、デバイス製造メーカ、第三者認証機関が使用できるようなチェックリストを作る等、既存の SEMI サイバーセキュリティ規格に対する装置の適合性を検証するための基準を開発している。
- WG3（supply chain cybersecurity）
  サイバーセキュリティに大きく影響するサプライチェーンのメンバー企業を評価するためのチェックリストを作成している。
- WG4（international regulation and specs）
  半導体製造に関する SEMI サイバーセキュリティ規格を他の規格等と統合し、理解と順守を目指す。例えば、NIST CSF2.0、EU サイバーセキュリティ法、DFARS、ISA/IEC62443 等と比較する取組を行う。
- WG5（threat sharing）
  悪意のある攻撃者はサプライチェーンの重複部分を効率的に狙っている状況を鑑み、信頼できる業界参加者間で脅威情報を共有して防御装置の迅速な展開と攻撃の緩和を目指す。
- WG6（cybersecurity pre-standards engineering）
  半導体サプライチェーン全体のサイバーセキュリティを確保するため、プロセスガイダンス文書や事例を作成し、全ての SEMI 規格の品質を向上させる。
- WG7（outreach, communications, and events）
  サプライチェーン内の企業が活用できる教育リソースとツールを提供している。これにより、会員企業におけるサイバーセキュリティへの影響を軽減することを目指している。また、主要な業界におけるイベントへの参加についても調整している。
- WG8（EU regulation and CRA）
  欧州サイバーレジリエンス法（CRA）等の半導体エコシステムへの影響を解釈し、CRA 標準化グループにて半導体業界を代表してギャップ分析等を実施している。また、SEMI 規格をソリューションとして欧州に普及させる活動も実施している。

今回の調査では、NIST CSF2.0 半導体製造プロファイルに関する情報を収集するため、国際規格や仕様について扱う WG4 の会議に参加した。

WG4 は 2024 年 1 月に法規制の整理をする WG として発足し、活動を開始した。米国にて、同年 5 月に半導体業界のセキュリティ確保に関する国家サイバーセキュリティ戦略実施計画[15]が出されたことを受け、NIST で半導体製造プロファイルの策定が開始された以降は、

[15] 半導体は経済安全保障および国家安全保障に不可欠であり、業界を保護するために、5 月 7 日に米国の

NIST と連携し NIST CSF2.0 半導体製造プロファイルの内容について検討を行っている。8 月、9 月からは集中的に内容を作成するために毎週開催された。

なお、2025 年 3 月 5 日時点で SMCC に参加している企業を以下に示す。[16]

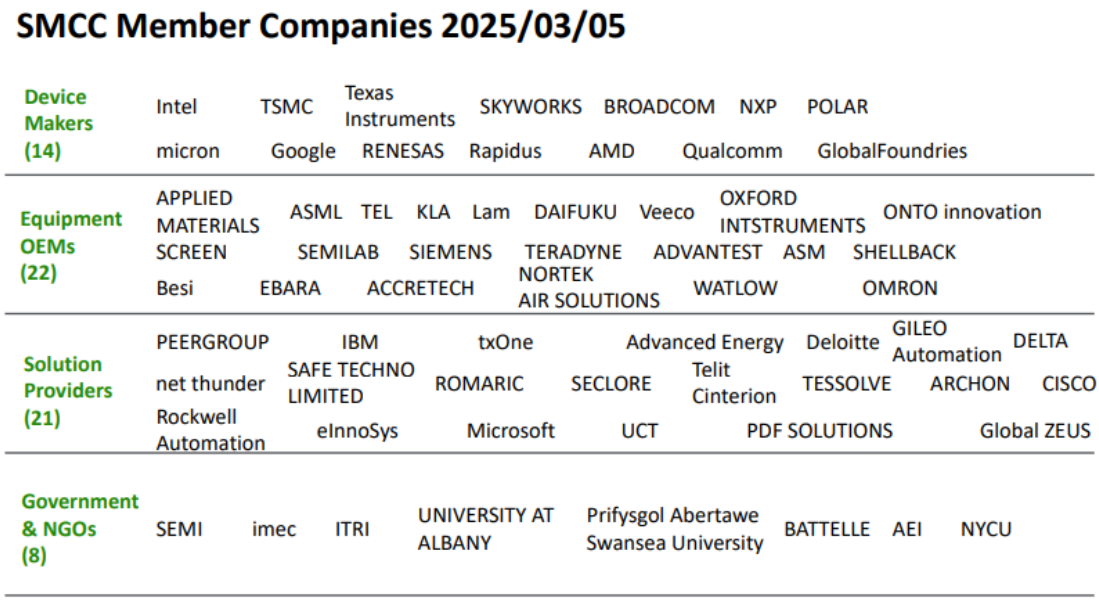


図 3.1.2-2 SEMI-SMCC 参加企業

SMCC WG4 に参加した実績を以下に示す。

表 3.1.2-5 SMCC WG4 開催実績(日本標準時)

2024 年 11 月 8 日 金曜日 2:00-4:00
2024 年 11 月 15 日 金曜日 2:00-4:00
2024 年 11 月 22 日 金曜日 2:00-4:00
2024 年 12 月 13 日 金曜日 2:00-4:00
2025 年 2 月 14 日 金曜日 2:00-3:00
2025 年 2 月 21 日 金曜日 2:00-3:00
2025 年 2 月 28 日 金曜日 2:00-3:00
2025 年 3 月 7 日 金曜日 2:00-3:00
2025 年 3 月 21 日 金曜日 1:00-2:00
2025 年 3 月 28 日 金曜日 1:00-2:00

国家サイバーセキュリティ戦略実施計画(NISIP)にて、半導体業界用途に合わせた NIST CSF の作成が盛り込まれました(Initiative Number: 5.5.5)

[16] Semiconductor Manufacturing Cybersecurity Consortium Participating Companies: https://www.semi.org/en/industry-groups/semiconductor-cybersecurity/participating-companies

上記の WG4 への参加に加え、2024 年 10 月 30 日-31 日に行われた NIST CSF2.0 半導体製造プロファイルの確認や修正作業のためのワークショップ（SEMI 主催）及び 3 月 13 日に行われたパブリックコメント版のドラフトについてのワークショップ（NIST 主催）にも参加し、情報を収集した。なお、WG4 及び 10 月のワークショップでは NIST CSF2.0 半導体製造プロファイルの内容が会員企業に対して提供されていたため、早い段階より NIST CSF2.0 半導体製造プロファイルを参照する半導体デバイス工場における OT ガイドラインについて検討することが可能となった。

表 3.1.2-6 SMCC WG4 F2F Workshop

	Agenda Item
Day 1 **（Oct 30）**	Authorship Discussions
	Preamble/ Deep Dive: Review Draft for overall profile and Final tables
	Readiness for Public Review: IDENTIFY and PROTECT
	Deep Dive- GOVERN
	Wrap up Day 1
Day 2 **（Oct 31）**	Review Day 1
	Deep Dive- GOVERN/ RECOVER
	NCCoE Tour
	Deep Dive- GOVERN/ RECOVER based on Parking Lot
	What's Next? After the Profile Publication, what is the next project for WG4? JL to list out the different activities that might be of interest to the group NIST Profile Public Workshop NCCoE- SMCC Profile Workshop（Day 2）
	Feedback and Retrospective

表 3.1.2-7 Cybersecurity Framework Profile for Semiconductor Manufacturing Public Workshop

Activity
Overview of NISTIR 8546 Cybersecurity Framework 2.0 Semiconductor Manufacturing Community Profile, Public Comment Review and Feedback
Objectives & Key Results Exercise
Working Exercises ・Assumption Collection Exercises ・Impact Effort Mapping
Working Exercises ・Expectation Alignment ・Adoption of Profile
Next Steps & Wrap Up

2）調査結果

＜NIST CSF2.0 半導体製造プロファイルの検討経緯＞

- 米国では、半導体は経済安全保障及び国家安全保障に不可欠であり、業界を保護するために、2024 年 5 月 7 日に米国の国家サイバーセキュリティ戦略実施計画（NISIP）にて、半導体業界用途に合わせた NIST CSF2.0 業界プロファイルの作成が盛り込まれた。（Initiative Number: 5.5.5）
- 2024 年 6 月より、NIST が SEMI SMCC と提携して、NIST CSF2.0 半導体製造プロファイルについて検討を開始し、同年 9 月 30 日に NIST CSF 2.0 半導体製造プロファイルの作成がプレスリリースされた。
- WG4 では 2024 年 12 月下旬まで NIST CSF2.0 半導体製造プロファイルの作成と確認が行われ、以降 2025 年 2 月中旬まではメールベースでプロファイルの修正を実施、2025 年 2 月からはパブリックコメントの実施や NIST ワークショップの内容について議論された。
- 2025 年 2 月 27 日より 44 日間のパブリックコメントが開始され、3 月 13 日には NIST 主催のワークショップにて NIST CSF2.0 半導体製造プロファイルの内容について説明され、意見交換が行われた。
- 今後は、収集したパブリックコメントを考慮し、NIST CSF2.0 半導体製造プロファイルを修正したうえで、2025 年 6 月末に正式に公表される予定である。

＜NIST CSF2.0 の概要＞

- NIST CSF は、重要インフラ（例：エネルギー、金融、通信など）の保護を目的として、米国の大統領令 13636「重要インフラのサイバーセキュリティの向上」に基づいて 2014 年に開発され、発行された。その後、2018 年に NIST CSF1.1 へ改定、2024 年 2 月に NIST CSF2.0 へと改定された。今では重要インフラにとどまらず、企業の IT システムとその管理態勢におけるセキュリティ指針として、全世界のあらゆる業種で活用されている。
- NIST CSF2.0 は、情報セキュリティの ISO 規格である ISO27001 と比較すると、外部脅威に対する侵入後の管理策まで網羅し、組織面及び技術面の双方から俯瞰したフレームワークとして構成されているところが特徴である。

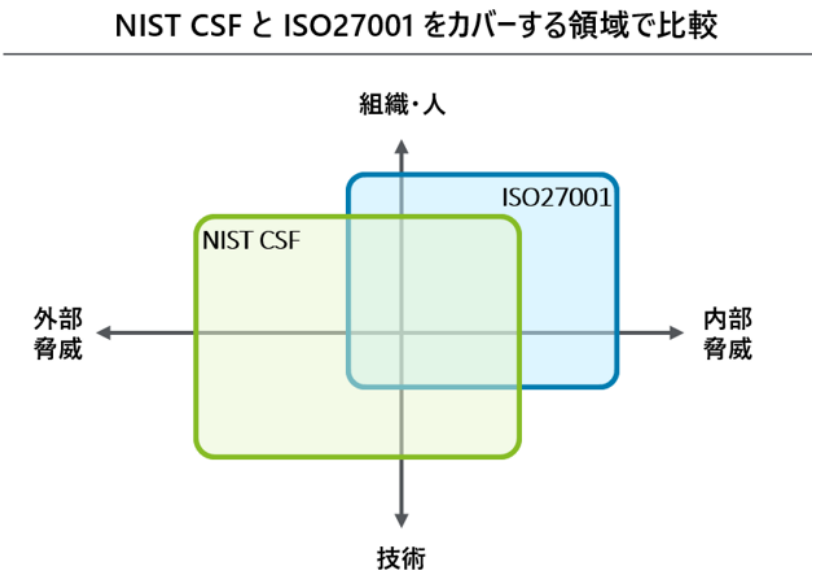


図 3.1.2-3 NIST CSF と ISO27001 のカバー領域

- NIST CSF2.0 では必要なサイバーセキュリティレベルの維持・向上のため、『あるべき組織構造』と『求められる能力』が示されている。
- 求められる能力は、組織のサイバーセキュリティリスク管理の土台となるガバナンス機能及び組織を取り巻くリスク全体を考慮する5つの機能（識別、防御、検知、対応、復旧）の合計 6 機能（Function）から 106 の詳細項目（Subcategory）で構成される。

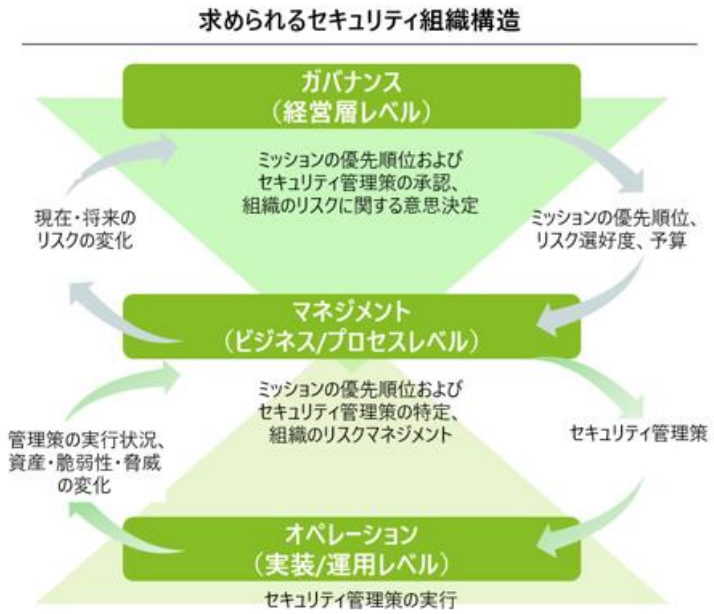


図　3.1.2-4 求められるセキュリティ構造

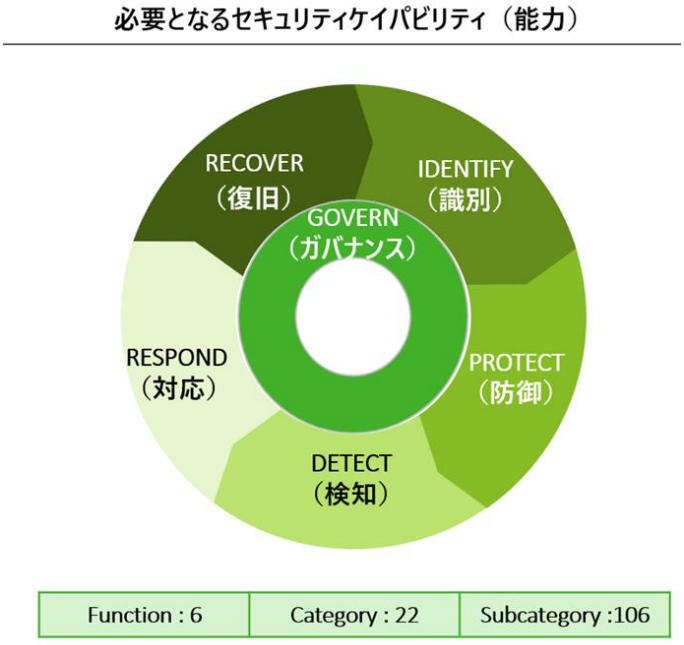


図　3.1.2-5 必要となるセキュリティケイパビリティ（能力）

＜NIST CSF2.0 半導体製造プロファイルの概要＞

- NIST CSF2.0 半導体製造プロファイルは、NIST CSF2.0 の 6 つの機能（Function）の各項目に対して、半導体業界の目標とベストプラクティスに沿っ

て、先に発行されている NIST CSF1.1 製造プロファイルを参考に、優先順位付けや対策アプローチの開発が進められている。これにより、次のような利点がある。

- 体制強化：改善領域を特定し、対処するための構造化された方法が示されている
- リスク管理：リスクレベルの評価を促進し、サイバーセキュリティの脅威を特定することが可能
- 標準化：計画を策定、維持するための方法論を確立し、ライフサイクル全体での継続性を検討することが可能

- 半導体業界の各企業は、NIST CSF2.0 半導体製造プロファイルを利用することにより、自社におけるリスクレベル（成熟度）を確認し、目指すべき水準に向けた内容を特定して優先順位を付け、実用的なセキュリティプラクティスを効果的に実装することが可能となる。

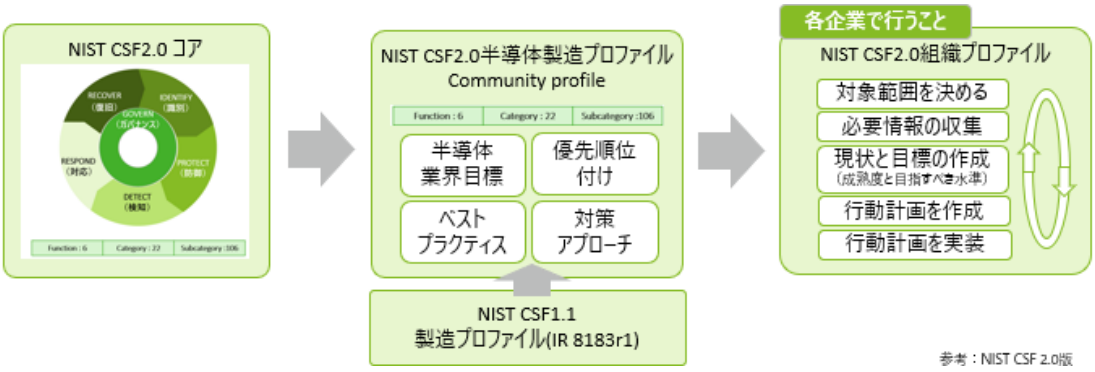


図 3.1.2-6 NIST CSF2.0 半導体製造プロファイルの概要

また、NIST CSF2.0 半導体製造プロファイルのパブリックコメント版は日本語の仮訳を作成した。

（3）E187/ CPSF/NIST CSF2.0/NIST CSF2.0 半導体製造プロファイルの関係

1）調査方法

国際的な半導体関連の規格である E187/E187 製造リファレンス、NIST CSF2.0/NIST CSF2.0 半導体製造プロファイル、CPSF の 3 つの規格等の関係性の整理を行った。具体的な調査方法について以下に示す。

- E187 製造リファレンスの第 3 章に記載されている 10 の対策について、CPSF のリスク源の洗い出しを実施し、リスク源に対する対策要件 ID を整理。リスク源の洗い出しについては、E187 製造リファレンスに記載されている内容を分析し、

CPSF の 6 つの構成要素(ソシキ・ヒト・モノ・データ・プロシージャ・システム)を特定

- CPSF の「添付 D 海外の主要規格との対応関係」から、CPSF の対策要件 ID と NIST CSF1.1 との関係性を整理
- NIST CSF2.0 Informative References より NIST CSF1.1 と NIST CSF2.0 の関係性を整理

2) 調査結果

E187/ CPSF/NIST CSF2.0/NIST CSF2.0 半導体製造プロファイルの関係性について、以下のとおり E187 製造リファレンスに関連する CPSF リスク源、CPSF 対策要件 ID、NIST CSF2.0 半導体製造プロファイル(Ecosystem、Fab、Enterprise IT、Equipment & Tools)を Excel で取りまとめた。

E187製造リファレンス			CPSF リスク源 脆弱性ID		CPSF 対策要件ID	
領域	エリア	領域・エリアにおける特徴				

CPSF 対策要件ID		NIST CSF2.0半導体プロファイル					
		識別	記述概要	EcoSystems	Fab	Enterprise IT	Equipment & Tools

図 3.1.2-7 E187 製造プロファイル・CPSF・NIST CSF2.0 半導体製造プロファイルの関係性整理

(4) E187 製造リファレンス

1) 調査方法

SEMI Taiwan が作成し 2023 年 10 月 1 日に公開された E187 製造リファレンスに関して、具体的なセキュリティ対策が記述されている第 3 章の内容を精査して要点をまとめた。

また、SEMI Taiwan に参加するメンバーに、2025 年の春公開を目指して作成中の E187 Ver2.0 について、改変するポイントや方向性をヒアリングした。加えて、SEMI Taiwan と政府の位置づけや協力の方法についてもヒアリングを実施し、半導体産業全体でセキュリティを確保する体制の特徴について整理した。

2) 調査結果

<E187 製造リファレンスの要点>

表 3.1.2-8 E187 製造リファレンスの要点

3.1 Secure by Design	【要点】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	【要点】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。
3.3 Move-in/Move-Out/Transfer	【要点】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	【要点】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。
3.5 Tool Network and Application Integration	【要点】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。
3.6 Local & Remote Accesses	【要点】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。
3.7 Secure data exchange	【要点】ファブエリアへのデータを転送する際に、マルウェア等の不正ソフトウェアのデータ侵入から保護するためのアクセス制御について記載。
3.8 Prevent, Detect and Response	【要点】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。
3.9 User Awareness Training	【要点】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。
3.10 Security Key Performance Indicators	【要点】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。

＜E187 Ver2.0 への改定のポイント＞

SEMI Taiwan における E187 Ver2.0 への改定に向けた検討のポイントを以下に示す。

- セキュリティレベル(SL)の設定

E187 Ver2.0 より新たにセキュリティレベルの設定を検討
SL-1 は全てのデバイスに適用されるレベル、SL-2 は装置ツール向けに適用されるレベル、SL-3 はクリティカルな装置ツール向けに適用されるレベル

- 対象エリアの拡大
  対象範囲をこれまでのファブエリアからファシリティエリアまで拡大することを検討。ファシリティの各設備に対するセキュリティ対策を記載。
- 対象装置ツール及び OS の拡大
  より多くの装置ツールや OS タイプをカバーすることに加え、装置ツールの中のすべてのインターナルコンピュータもスコープとすることを検討。
- セキュリティ対策の記載の拡充
  脆弱性とパッチ管理、ネットワークセキュリティ、エンドポイントプロテクション、IAM、ログ監視等の記述を拡充
- ISC/IEC62443 との整合

＜台湾における半導体産業に対するセキュリティの検討体制＞

SEMI Taiwan のサイバーセキュリティコミティの下には WG が 4 つ設けられているが、コミティと WG の間にサポート役の事務局がある。台湾政府は、半導体産業のグローバルな競争力強化を目的に、半導体産業におけるサイバーセキュリティ対策の実装に対する経済的な支援、サイバーセキュリティ対策を検討する会議体の設置や会議運営の支援等を実施している。

3.2 半導体関連企業のセキュリティ対策状況や製品セキュリティへの取組の実態調査

3.2.1 目的

半導体関連企業が抱える工場セキュリティにおける課題を明らかにし、それらの課題の解決に資する半導体デバイス工場における OT ガイドラインを作成することを目的とし、3.1 項の動向調査に加え、半導体関連企業のセキュリティ対策状況や製品セキュリティへの取組の実態を調査した。

3.2.2 調査対象

今回の実態調査（ヒアリング）では、国内デバイスメーカ 6 社を対象に、半導体製造工場におけるセキュリティ対策の実態や課題等についてヒアリングを実施した。また、第1回半導体産業 SWG では JEITA より半導体製造メーカにおける工場セキュリティに対する問題意識や課題についてご講演を頂き、その内容を含め、取りまとめを行った。

3.2.3 ヒアリング項目

3.2.2 の各デバイスメーカに対し、下記に示すヒアリング項目を事前送付した上で、オンラインにてヒアリング項目への回答を聴取した。

表 3.2.3-1 ヒアリング項目

項目		質問内容
サプライチェーン	工場に要求されるセキュリティ要件	取引先や法規制等により求められるセキュリティ基準・チェックリストの内容、対応状況、課題についてお聞かせください。
	サプライヤーに対するセキュリティ要件	部素材、装置メーカ、業務委託先等のサプライヤーに対するセキュリティ活動に関する取組状況、今後の予定、課題についてお聞かせください。
規定等	IT/OT セキュリティ規定	製造(OT)エリアを含む、IT/OT セキュリティに関連する社内の規定やガイドライン、ルールの運用状況、課題についてお聞かせください。
工場セキュリティ	装置に対するセキュリティ対策	装置の調達/導入/運用保守時におけるセキュリティ対策や確認方法等についてお聞かせください。
	ファシリティ設備のセキュリティ対策	各ファシリティサービス業者に対するセキュリティ含めた継続性の確認、機器構成管理方法、脆弱性対応、リモート保守のリスク確認等に関する対応状況、課題についてお聞かせください。
	製造エリアの外部ネットワーク接続	製造システムエリア(MES/SPC/EDA 等)におけるセキュリティ対応状況、課題についてお聞かせください。
機密	機密情報の取扱い	機密情報の取扱いに関して、作業部会で議論すべき課題等があればお聞かせください。
運用	インシデント対応	有事対応(異常検知・トリアージ・インシデント対応等)、SOC、CSIRT/FSIRT/PSIRT 等の体制・運用面の対応状況、課題についてお聞かせください。
	脅威・脆弱性情報収集・分析	脅威・脆弱性情報収集・分析に対する対応状況、課題についてお聞かせください。
	ビジネス復旧計画・訓練	ビジネス復旧計画・訓練に対する、対応状況、課題についてお聞かせください。
	人材の確保・育成	IT、OT、製品、サプライチェーンマネージメント等のセキュリティ対策に関する人材の確保の状況、外部サービス等の利用状況、課題について

		お聞かせください。
	成熟度評価	国内外工場のサイバーセキュリティに関する成熟度（対策レベル）評価について、取組状況、今後の予定等があればお聞かせください。
ガイドライン	半導体デバイス工場における OT ガイドラインについて	前述質問項目に関して、優先度の高い課題、半導体デバイス工場における OT ガイドラインで取組むべきテーマについてお聞かせください。

3.2.4 調査結果

調査結果については、ヒアリングした結果を課題ごとのインサイト（示唆）という形で整理し、国内デバイスメーカ 6 社からのヒアリング結果に加え、第 1 回 SWG の JEITA 講演で共有された工場セキュリティの課題について整理した結果も併せて整理を行った。

3.2.3 のヒアリング項目に対する調査結果を下記に示す。

表 3.2.4-1 調査結果

項目		質問内容
サプライチェーン	工場に要求されるセキュリティ要件	発注者からの**セキュリティチェックリストの対応負荷**が大きい（1-3 件/月）、**統一化**できないか
	サプライヤーに対するセキュリティ要件	• 数百以上のサプライヤーに対してセキュリティチェックリストへの回答を要請しており、管理工数が大きい • 発注者によっては、ティア 2 以降のサプライヤーのリスクアセスメントに関する要求も来ている
規定等	IT/OT セキュリティ規定	• IT セキュリティ規定をベースに OT セキュリティを運用しているケースや OT 固有の規定を作成しているケースがある • ISMS の 20 項目を社内に展開し周知させるために説明会を行っている
工場セキュリティ	装置に対するセキュリティ対策	装置や PC の管理する台数が 1 万台規模と多く**OS のバージョンアップやセキュリティ対策ソフトの導入が難しい**
	ファシリティ設備のセキュリティ対策	水/電気/薬品等装置毎にセキュリティ対策が異なり、かつ、脆弱。**ファシリティ設備のセキュリティ対策強化が課題**
	製造エリアの外部ネットワ	リモートメンテナンスへの要求が高まり、新たに

	ーク接続	セキュリティガイドラインと審議プロセスを構築する必要がある
機密	機密情報の取扱い	先端半導体に加え**レガシー半導体の製造、設計情報の保護も重要**である
運用	インシデント対応	• SOC、CSIRT、PSIRT 体制はあるが、**FSIRT 体制は無い企業が多い**（検討中の企業は多いがリソースが課題） • 脆弱性が破られた際の PSIRT、CSIRT 等の対処を検討するべきである
	脅威・脆弱性情報収集・分析	**半導体分野の脅威情報の収集は未実施、業界で共有する仕組み**が必要
	ビジネス復旧計画・訓練	BCP/BCM は策定済み、一部では訓練もしているが**装置を停止できないため工夫が必要**（入替え時等）
	人材の確保・育成	• セキュリティ人材は全般的に不足、工場は地方にあり人材確保が困難、OT セキュリティ人材の育成が課題 • 国内でのセキュリティ人材の確保は難しく、海外から人材を集めている
	成熟度評価	一部企業では工場セキュリティの成熟度評価を実施
ガイドライン	半導体デバイス工場における OT ガイドラインについて	• 国際標準は初歩的なレベルのものであるため、**半導体デバイス工場における OT ガイドラインでは実装レベル**まで意識を合わせてほしい • 攻撃アクターとして国家背景のアクターを含めることで、E187 に追加事項を加えてほしい • 国際的な標準化の議論の中に日本企業も参加すべき

半導体デバイス工場における OT ガイドラインでは、上記の調査結果のうち特に太字下線部を中心に検討を行う。（詳細は 4.2 項「半導体デバイス工場における OT ガイドライン素案作成」参照）

4. ガイドライン素案の作成

4.1 半導体産業におけるセキュリティ対策基準

4.1.1目的

本事業では、半導体産業における企業や組織の知財等重要情報流出の防止することを目的とし、包括的かつ実効性のある半導体産業におけるセキュリティ対策基準の策定を目的の一つに掲げている。昨年 4 月に開催された「産業サイバーセキュリティ研究会」の事務局資料では「半導体関連産業において求められるセキュリティ対策を具体化していくとともに、その内容を経済産業省の投資促進関係施策の要件等とも紐付けること等を検討し、その実効性を強化していく。」と記されており、現在検討している半導体産業におけるセキュリティ対策基準については、今後、投資促進関係施策の要件等との紐づけを検討する。

4.1.2 半導体産業におけるセキュリティ対策基準の考え方

半導体産業におけるセキュリティ対策基準については、知財等重要情報流出の防止や半導体工場における OT セキュリティの対策強化を目的にしていることから、IT 領域及び OT 領域のセキュリティ対策要件を組み合わせて策定する。具体的な考え方を以下に示す。

- IT 領域及び OT 領域のセキュリティ対策要件を組み合わせて策定する
- IT 領域におけるセキュリティ対策要件については、すでに「サプライチェーン強化に向けたセキュリティ対策評価制度に関するサブワーキンググループ」において検討が進められているセキュリティ対策評価制度を活用する（★3 及び★4）
- OT 領域のセキュリティ対策要件については、OT ガイドラインの第 3 章「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」及び第 4 章「半導体デバイス工場における具体的な対策事例」の中で、工場ガイドラインのチェックリストに同様の内容が記載されているなど、特に重要であると考えられる項目を選択する

4.1.3 半導体産業におけるセキュリティ対策基準作成の進め方

半導体産業におけるセキュリティ対策については、前述考え方に従い、OT 領域のセキュリティ対策要件の洗い出しを実施したうえで、半導体産業 SWG に諮問し、ご意見を頂いたうえで要件を確定させる。

次に、確定したセキュリティ対策要件について、評価基準を作業部会にて議論を行ったうえで基準案を作成し、半導体産業 SWG に諮問し、成案化させる。

4.1.4 半導体産業におけるセキュリティ対策基準の概要

現在検討している OT ガイドラインの第 3 章及び第 4 章に記載している内容から 15 件、要

件の候補を抽出した。

4.2 半導体デバイス工場における OT ガイドライン素案作成

4.2.1 目的

本事業では、サイバー攻撃による事業継続リスクへの対策を目的とし、半導体デバイス工場における OT ガイドライン素案を作成した。

半導体は経済安全保障法の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。半導体産業の、経済及び安全保障上の重要性に鑑みると、今後高度なサイバー攻撃を受けることを想定し、対策を進めていく必要がある。国際的には、SEMI により SEMI E187/E188 規格が策定され、米国 NIST により NIST CSF2.0 半導体製造プロファイルの策定が進められているが、国内の半導体産業全体でセキュリティ対策を進める枠組みは存在しないため、国内の半導体産業におけるセキュリティ対策状況等を踏まえた工場セキュリティ対策の指針を示すことが求められている。

また、経済産業省では、汎用的な組立型の工場向けに『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン』を策定し公表しているが、半導体工場は一般的にプロセスオートメーション（PA）型の工場であり、工場の規模が大きく、汎用 OS を用いた製造装置の台数が多い等の特徴があることから、既存の工場向けのガイドラインでは対応が難しいため、半導体デバイス工場向けに半導体デバイス工場における OT ガイドラインを策定した。

半導体製造は素材、設計、製造（前工程・後工程）など複雑なサプライチェーンによって成り立っており、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り、半導体関連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。半導体デバイス工場における OT ガイドラインではその最初の段階として半導体デバイスメーカの工場を対象としているが、将来的には装置メーカや部素材メーカなどサプライチェーン全体への拡大を目指す。

4.2.2 半導体デバイス工場における OT ガイドラインの考え方

半導体デバイス工場における OT ガイドラインは以下の考え方に基づき作成した。

- NIST CSF2.0 半導体製造プロファイルや SEMI E187 など半導体産業における国際的な規格等を参考として関係性を整理し、活用方法やユースケースを加え国際標準との整合性を踏まえ、日本独自の規格としない。
- 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、チェックリスト形式の確認ではなく、工場のセキュリティ対策を進めるための一般的なプロセスにおいて、リスクベースのサイバーセキュリティフレームワーク（CPSF、NIST CSF2.0）を活用したリスク分析及び具体的な対策を検討する際などに活用されるガイドラインとする。
- 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領域

とエリアで分類し、特に重要なエリアにフォーカスし優先順位をつけて作成する。

- 国際標準化動向や業界における課題を踏まえて継続的に更新していく。

4.2.3 半導体デバイス工場における OT ガイドライン作成の進め方

以下の進め方で半導体デバイス工場における OT ガイドラインを作成した。

- NIST CSF2.0 半導体製造プロファイルや E187 半導体製造リファレンス、IEC62443 等の国際規格や CSPF や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等の国内のガイドラインの関係性を整理する。
- 第 2 回工場 SWG における JEITA 半導体部会発表資料にて共有された工場セキュリティへの要求事項を参考にしつつ、デバイスメーカへのヒアリングを行い、工場セキュリティ対策の課題等を取りまとめる。
- SWG 委員からの意見を取りまとめ、半導体デバイス工場における OT ガイドライン素案を作成する。
- 半導体デバイス工場における OT ガイドライン素案に対する作業部会メンバーの意見を踏まえ半導体デバイス工場における OT ガイドライン素案を修正する。
- 半導体デバイス工場における OT ガイドライン素案を SWG 委員に諮問する。

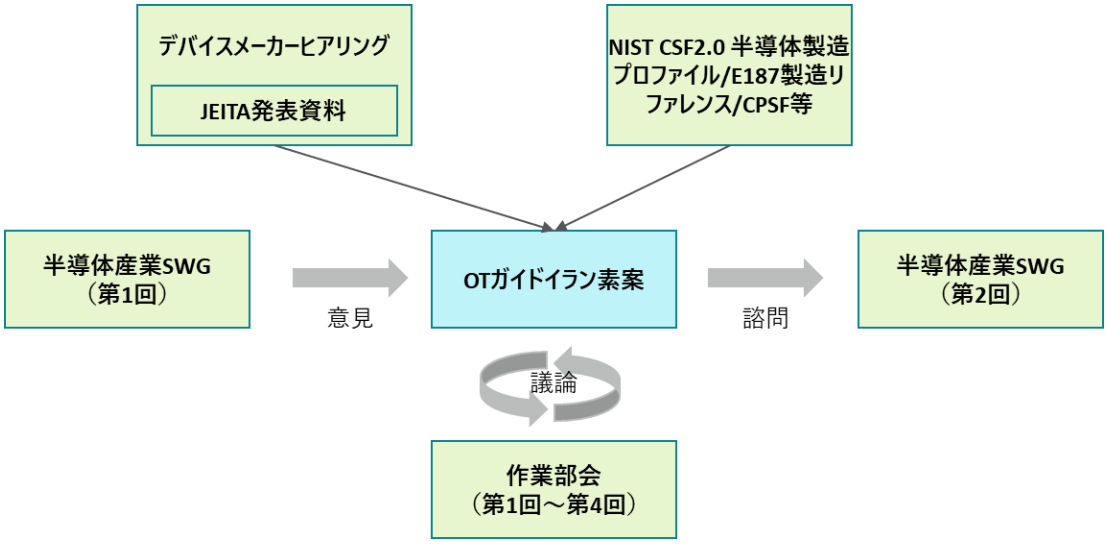


図 4.2.3-1 半導体デバイス工場における OT ガイドライン作成の進め方

また、以下のポイントを工夫し半導体デバイス工場における OT ガイドラインを作成した。

- 半導体デバイス工場における OT ガイドラインは、CPSF や NIST CSF2.0

等リスクベースのフレームワークを活用したリスク分析及びセキュリティ対策の検討をする際の参考文献とするために、CPSF と NIST CSF2.0 半導体製造プロファイルの関係性を取りまとめた。

4.2.4 半導体デバイス工場における OT ガイドラインの概要

(1) 半導体デバイス工場における OT ガイドラインの構成

半導体デバイス工場における OT ガイドラインは、第１章 背景と目的、第２章 半導体デバイス工場のリファレンスアーキティチャ、第 3 章 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、第 4 章 半導体デバイス工場における具体的対策事例及び Appendix で構成する。各節の記載概要を以下に示す。

表 4.2.4-1 半導体デバイス工場における OT ガイドラインの構成と記載概要

半導体デバイス工場における OT ガイドライン構成		**記載概要**
第１章 本ガイドライン作成の背景と目的	1.1 背景と目的	半導体産業の重要性、半導体企業に対するサイバー攻撃の現状、工場セキュリティ規格の国際動向、半導体工場向けの半導体デバイス工場における OT ガイドラインの必要性等について記載
	1.2 ガイドラインの対象者(想定読者)	半導体産業全体の OT セキュリティ対策の底上げを目指しつつ、当面の対象は半導体デバイス工場に設定
	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	サイバー攻撃から守るべき 5 つの対象を記載
	1.4 半導体製造工程における脅威とリスク	半導体工場の生産プロセスにおける在庫、機密情報、品質向上の重要性を記載
	1.5 想定する攻撃主体	攻撃主体の種別とこれに対応した目指すべきセキュリティレベルについて記載
	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	半導体工場における BCP と連動したリスク分析の重要性及び本ガイドラインの活用方法について記載

	イドラインの利活用	
	1.7 ガイドラインの構成	ガイドラインが参照している国内外の規格・ガイドライン等について整理
第 2 章 半導体デバイス工場の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	半導体デバイス工場におけるリスク源の洗い出し及びリスク対策を整理する基本となるリファレンスアーキテクチャについて、CPSF 及び Purdue モデルの組合せにより整理(アーキテクチャの図及び CPSF の構成要素を整理した表)
	2.2 Purdue モデルの適用	2.1 節で定義した半導体工場のリファレンスアーキテクチャにおける Purdue モデルの領域及びエリアについて説明
	2.3 CPSF の三層構造の適用	2.1 節で定義した半導体工場のリファレンスアーキテクチャにおける CPSF の三層構造について説明
第 3 章 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	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リスクの洗い出しを行い、関連フレームワークの対策項目の整理を行う
	3.2 半導体デバイス工場の技術・物理側面における OT 領域各エリア別のリスク分析のための情報	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、技術・物理側面から OT 領域の各エリア別にまとめる
	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ハーを加工製造する装置ツール群となる「ファブエリア」についてまとめる
	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」についてまとめる

	3.2.3 OT 領域の外部サービス活用及び IT/OT DMZ 分離制御のリスク分析のための情報	OT 領域に対する「外部サービス」の活用及び「IT/OT DMZ」の分離制御についてまとめる
	3.3 半導体デバイス工場の組織・人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・人の側面からまとめる
第 4 章 半導体デバイス工場における具体的対策事例	4.1 装置ツールの資産管理と脆弱性評価	「3.2.1 - ① 装置ツールの資産管理と脆弱性」について具体的対策事例を示す
	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 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」について具体的対策事例を示す
	4.3 運用(監視・対応・復旧・改善) - FSIRT による運用	「3.2.3 - ⑥ 運用(監視・対応・復旧・改善)」について具体的対策事例を示す
	4.4 物理アクセスの制限(入室・持ち込み・接続) - ファブエリアにおける物理的対策	「3.2.1 - ⑤ 物理アクセスの制限(入室・持ち込み・接続)」について具体的対策事例を示す
Appendix A	NIST CSF2.0 と経産省 CPSF の対比表	CPSF の対策 ID と NIST CSF2.0 のサブカテゴリの対比表
Appendix B	用語/略語	半導体デバイス工場における OT ガイドラインにおける用語・略語の一覧

（2）半導体デバイス工場における OT ガイドラインのポイント

半導体デバイス工場における OT ガイドラインは、半導体デバイス工場に対して CPSF/NIST CSF 等リスクベースのセキュリティ対策を立案する際の手引書として利用することを企図して作成した。

第 2 章では、半導体デバイス工場を Purdue モデルでエリア分けし、CPSF の 6 つの構成要素をマッピングした半導体デバイス工場リファレンスアーキテクチャについて説明している。第 3 章では、前述リファレンスアーキテクチャの主要なエリアにおける半導体デバイス工場における特徴、考慮すべきセキュリティ要求事項、リスク源をまとめ、これに対応する NIST CSF2.0 半導体製造プロファイルのサブカテゴリ及び CPSF の対策 ID を整理している。また、第 4 章では、半導体デバイス工場における具体的なセキュリティ対策事例を掲載している。

半導体デバイス工場における OT ガイドラインの各章におけるポイントを以下に示す。

ガイドラインの構成　1. 本ガイドライン作成の背景と目的①

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

ガイドラインの背景と目的

- サイバー攻撃はますます多様化・高度化しており、多くの制御装置等が攻撃され、工場における生産が停止する等の被害が発生している。また各種の開発機密（知的財産）がサイバー攻撃によって流出する危険も増している。半導体産業の、経済及び安全保障上の重要性に鑑みると、今後高度なサイバー攻撃を受けることを想定し、対策を進めていく必要がある。**海外ではSEMI E187/E188規格が策定され、米国NISTによりNIST CSF2.0半導体製造プロファイルの策定が進められている。**
- 一方、国内の半導体産業全体でセキュリティ対策を進める枠組みは存在しないため、**国際的な半導体産業における各種セキュリティ規格と整合しつつ、国内の半導体産業におけるセキュリティ対策状況等を踏まえた工場セキュリティ対策の指針を示すことが喫緊の課題**である。
- 経済産業省では、汎用的な組立型の工場向けに「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」を策定し公表しているが、**半導体工場は一般的にプロセスオートメーション（PA）型の工場であり、工場の規模が大きく、汎用OSを用いた製造装置の台数が多い等の特徴があることから、新たに半導体デバイス工場向けに本ガイドラインを策定した。**

想定読者

- 半導体デバイスメーカーの製造部門の方々
（製造装置メーカー、素材メーカーの方々）

想定する攻撃主体

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

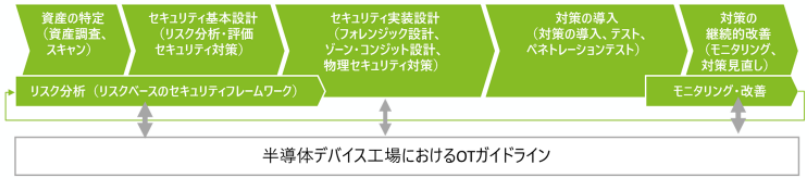
守るべき対象

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

ガイドラインの構成　1. 本ガイドライン作成の背景と目的②

本ガイドラインの利活用

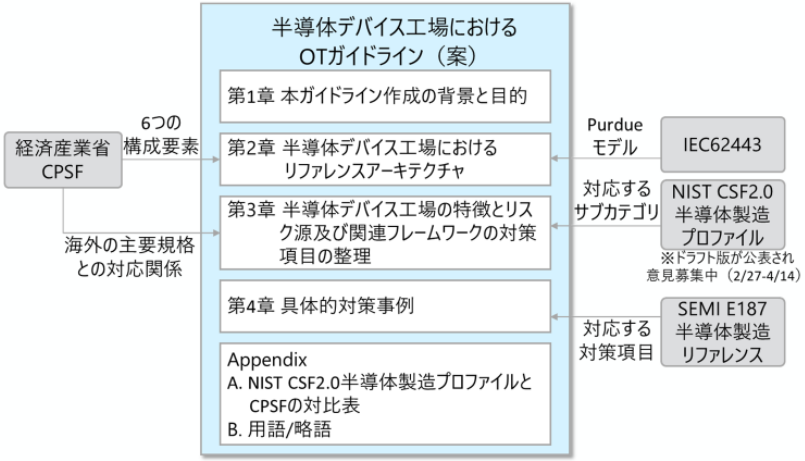
- 半導体サプライチェーンの保護という目的を達成するためには、構成する各企業が供給責任を果たせるサイバーセキュリティ対策を実現する必要があり、事業継続計画と整合する必要がある。
- 供給責任及び、その説明責任を果たせる対策を行うためには、**リスク評価を行った上で、その結果を踏まえた適切な対策の検討・設計・実装を行う必要がある。**
- 本ガイドラインは、**工場のセキュリティ対策を進めるための一般的なプロセスにおいて、リスクベースのサイバーセキュリティフレームワーク（CPSF*1、NIST CSF2.0 *2）を活用したリスク分析、及び具体的な対策を検討する際などに活用することが想定される。**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



*1：https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html
*2：https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
*3：https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

本ガイドラインの構成

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



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

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

半導体デバイス工場のリファレンスアーキテクチャの特徴

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

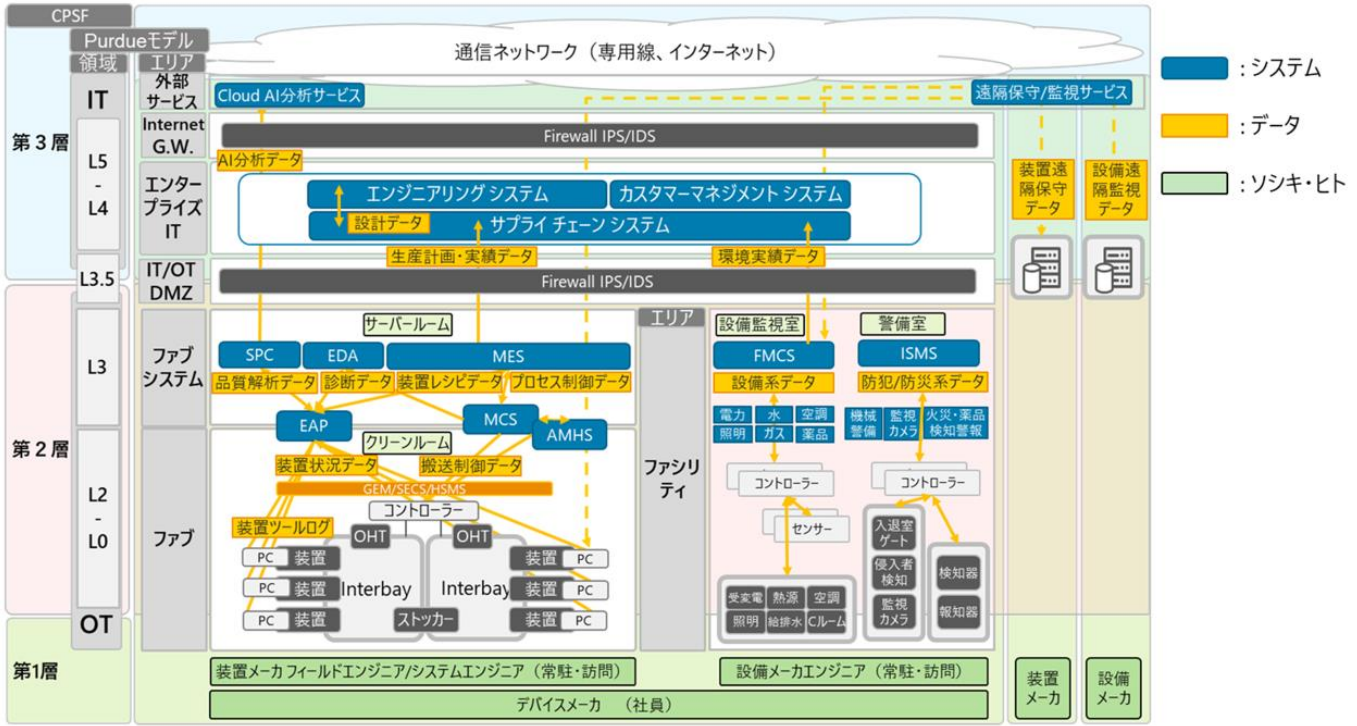
Purdueモデル

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

CPSF三層構造

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

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



半導体デバイス工場のリファレンスアーキテクチャ

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

Purdueモデル		CPSFによる6つの構成要素					
領域		システム	データ	モノ	プロシージャ	ソシキ及びヒト	
						デバイスメーカー	協力会社
外部サービス		AIデータ分析サービス 遠隔監視保守サービス	AIデータ分析データ 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、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
Internet G.W.		Internet G.W.（RAS）	組織外通信制御データ	FW、IPS/IDS等	Internet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	FW、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 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
	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、製造レシピ【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
	ファシリティ（L0-3）	FMCS ISMS	設備データ、環境データ 防犯データ、防災データ	各設備、コントローラ、センサ	半導体製造のクリ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

PurdueモデルとCPSFによる6つの構成要素

・　第３章　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

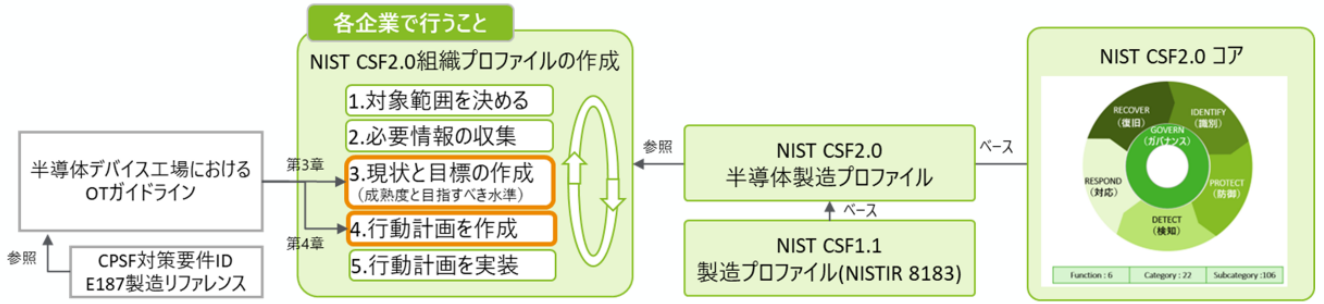
ガイドラインの構成

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

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

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

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



ガイドラインの構成

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

リファレンスアーキテクチャを活用したセキュリティ対策項目への整理

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

「リスク分析のための情報」の活用方法

現状と目標の作成

特徴の把握及び関連箇所の確認

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

組織プロファイルの目標設定

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

行動計画の作成

具体的対策例の活用

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

ガイドラインの構成

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

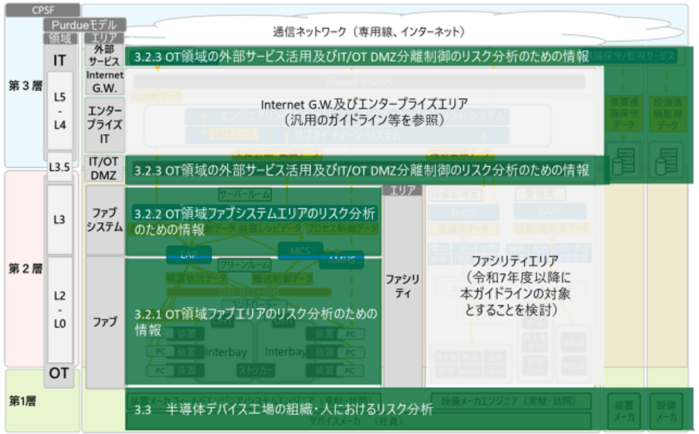
リファレンスアーキテクチャを活用したセキュリティ対策項目への整理

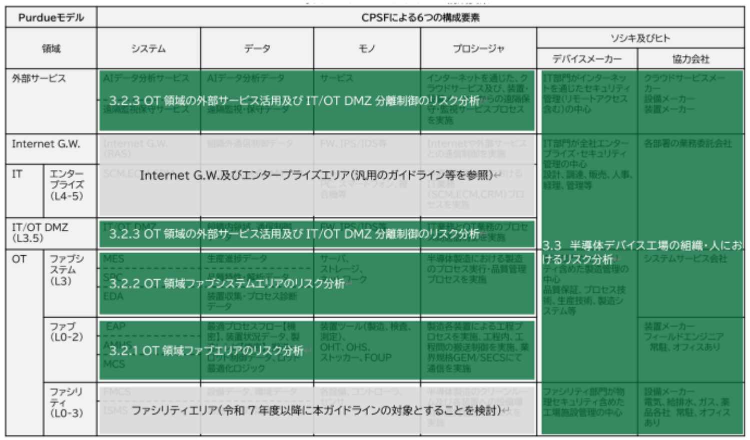
リファレンスアーキテクチャを活用し、半導体デバイス工場における特徴を踏まえたリスク源（脅威、脆弱性）の洗い出しを行い、対応するリスク対策フレームワーク（CPSF及びNIST CSF2.0）のセキュリティ対策項目について取りまとめている。

対策項目の整理の対象範囲については、Purdueモデルで分類したファブエリア、ファブシステムエリア、IT/OT DMZ、外部システム及び組織・人的側面とする。

Internet G.W.及びエンタープライズエリアは、通常のIT領域におけるセキュリティ対策と差異がないことから、第3章の対象外とする。

OT領域のファシリティエリアについては、現在検討が進められている国際的な規格との連携を考慮し、令和7年度以降に本ガイドラインの対象とすることを検討する。





ガイドラインの構成

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

リファレンスアーキテクチャを活用したセキュリティ対策項目への整理

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

技術・物理的側面

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

組織・人的側面

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

ガイドラインの構成

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

リ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（例：装置ツールの資産管理と脆弱性評価①）

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

ガイドラインの構成

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

リ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（例：装置ツールの資産管理と脆弱性評価①）

CPSF 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　及び　CPSF
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 **脆弱性**： • モノのセキュリティ状況やネットワーク接続状況が適切に管理されていない • 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IoT機器のセキュリティ対策状況(ソフトウェア構成情報、パッチ適用状況等)を把握できていない • 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	**【NIST CSF2.0 半導体製造プロファイル】** • ID.AM-01 • ID.AM-02 • ID.AM-04 • ID.AM-05 • ID.AM-08 • ID.RA-01 • ID.RA-02 • ID.RA-03 • ID.RA-04 • ID.RA-05 • ID.RA-06 • ID.RA-07 • ID.RA-08 ※半導体プロファイルはサブカテゴリをさらにファブ、装置ツール、エンタープライズIT、エコシステムの4つに分類しており、関連性の高いものを今後抜粋し記載する予定である 例）ID.AM-01 　　ファブ：現行システムを反映した製造システムコンポーネントのインベントリを文書化する **【CPSF対策要件ID】** • CPS.AM-1 • CPS.AM-5 • CPS.AM-6 • CPS.RA全て **【SEMI E187製造リファレンス】** 3.4 Vulnerability/Threat Assessment and Patch Management 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

・　第４章　半導体デバイス工場における具体的対策例

ガイドラインの構成　４．半導体デバイス工場における具体的対策事例

半導体デバイス工場における具体的対策例

半導体デバイス工場で対策検討を進めるうえで、参考となる以下の４つ具体的な事例を示す

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

ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価①

- 半導体デバイス工場におけるOT領域ファブエリアは、1工場で2千台以上と非常に多くの装置ツールが、クリーンルーム環境の中でシステム・装置間を自動連携しながら連続生産を行っている。
  工場で守るべき生産目標、半導体品質の維持、生産機密情報の保護、人命・環境の維持を実現するには、このファブエリアにある大量の装置ツールの資産管理を漏れなく洗い出しを行う。効果的な対策を行えるように、被害想定から重要度の重みづけを行う。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。

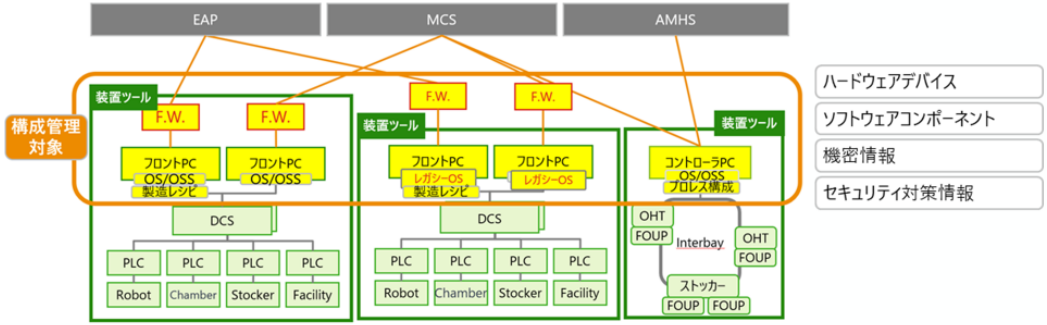
- 装置ツール資産の内部は、複数のハードウェアデバイス、ソフトウェアコンポーネントで構成され複雑である。一方で発見される脆弱性は年間4万件を超える中で、装置ツールにおける効果的な資産管理と脆弱性評価について、以下の5つに分けて具体的な対策事例を示す。

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

ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価②

資産（装置ツール）の洗い出し・構成管理の決め方

- ハードウェアデバイスは、装置ツール内のFab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Fabネットワークに接続されるファイア・ウォール等が管理対象となる。
- 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を管理範囲とする。SEMI E187：7 コンピュータオペレーティングシステムのセキュリティ要件により装置メーカーから提供されるソフトウェアの互換性、ソフトウェアパッケージの依存関係の情報を管理対象とする。
- 機密情報は、装置ツール内に保管される生産機密情報を対象とする。設計回路情報や製造レシピ、プロセス構成等が管理対象となる。
- セキュリティ対策情報は、装置ツール本体に対してSEMI E187のベースライン要件の適用状況を対象とする。SEMI E187のベースライン要件では、パッチ適用条件、マルウェア対策、アクセス制御、ネットワーク管理、セキュリティモニター等、脆弱性の評価を効率的に行うための要件項目を管理対象とする。



ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価③

資産（装置ツール）の重要度の決め方

- ファブエリアにあるすべての装置ツール資産の管理構成に対して、サイバー攻撃により資産が損なわれた場合の被害の大きさから重要度を定めていく。半導体産業では国家支援型APT攻撃も発生しており、攻撃者は必ず狙いをもってアタックを仕掛けてくる。
  守るべき資産に対してサイバー被害が発生した場合、どのようなビジネスダメージがどの程度発生するのかを吟味して重要度を予め定め、適切に見直し管理する必要がある。

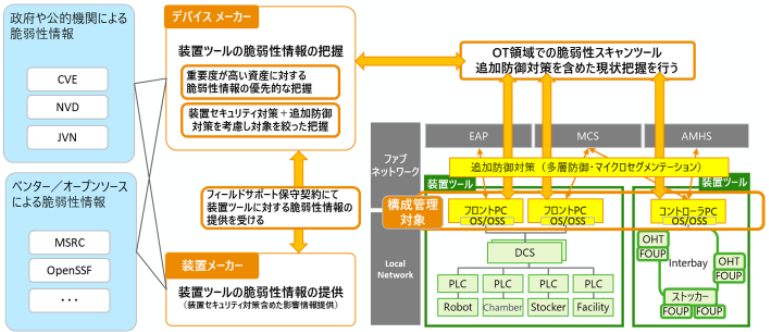
カテゴリー	システム資産としての価値		その資産がサイバー攻撃を受けることによって想定される事業被害・事業継続性の影響						
	財務影響	情報漏洩（機密性）	事業継続性（可用性）		半導体品質（完全性）		産業活動の安全性（HES）		法規制等の遵守
	装置ツールの破損	生産機密情報の漏洩	生産停止	供給影響	歩留まり影響	市場品質影響	労災事故	環境被害	
A（高）	収益の5%以上の損失		1日以上	7日以上	歩留まり率50%を下回る影響	市場品質不良影響あり・PL法影響あり	死亡	重大な地域のインシデント	政府の規制や業界の標準に重大な違反による厳重な監視や制約
B（中）	競争優位性に影響を与える収益の１～５%の損失		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
C（低）	影響はなし収益上の影響はない		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	法令厳守に影響を及ぼす可能性はない

ガイドラインの構成　4-1. 装置ツールの資産管理と脆弱性評価④

装置ツールの脆弱性の把握方法

脆弱情報の入手先

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



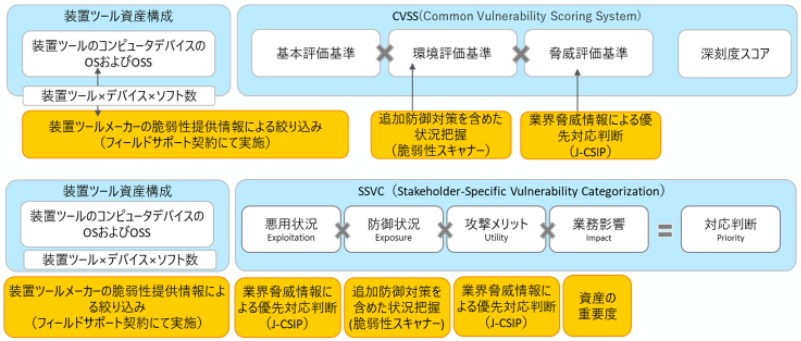
装置ツールに対する脅威情報の収集方法

脅威情報の入手先

- 政府や公的機関であるNISC、JPCERT/CC、IPA、CISA、CUS-CERT、ENISAからの情報収集
- 業界の脅威情報共有であるSEMI-SMCC-WG5, IT-ISAC Semiconductor Industry SIG、J-CSIP半導体産業SIGからの情報収集
- 自社のアタック・インシデント情報の分析結果からの情報収集

装置ツールに対する脆弱性評価と対応優先度の決め方

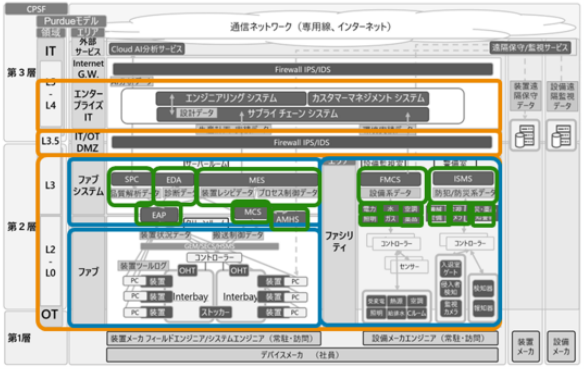
装置ツールの脆弱性の評価は、装置ツールの弱点となる脆弱性を把握し、攻撃者の脅威の可能性を含め、装置ツールに対する深刻度を把握し、対応判断（方法：軽減・回避・保有、時期）するための評価を行う。

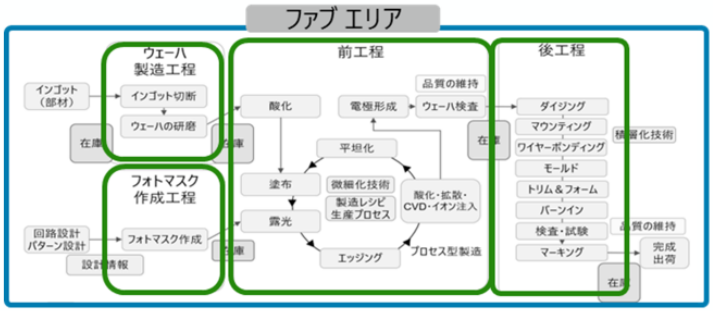


ガイドラインの構成　4-2. 装置ツールの被害の極小化と早期復旧を備えた追加防御策①

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

ネットワークによる多層防御、マイクロセグメンテーションとセキュリティ監視	
1	**OT領域の分離と通信制限** 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)　左下図のオレンジ枠箇所
2	**エリア毎のゾーン分割と通信制限** 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を分割したうえ通信制限を行う 左下図の青色枠箇所
3	**エリア内でのゾーン分割と通信制限** ファブエリアについては、生産計画を行う工程単位でネットワークを分割して通信制限を行う（同じ工程でも、建屋、フロアー等にて生産計画が違う場合は分離）　右下図の緑色箇所 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 右下図の緑色枠箇所

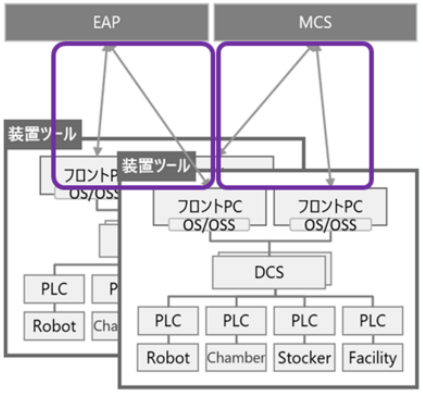


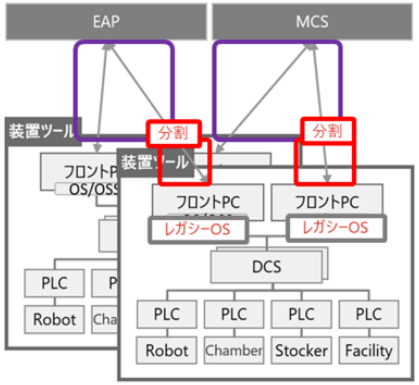


ガイドラインの構成　4-2. 装置ツールの被害の極小化と早期復旧を備えた追加防御策②

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

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

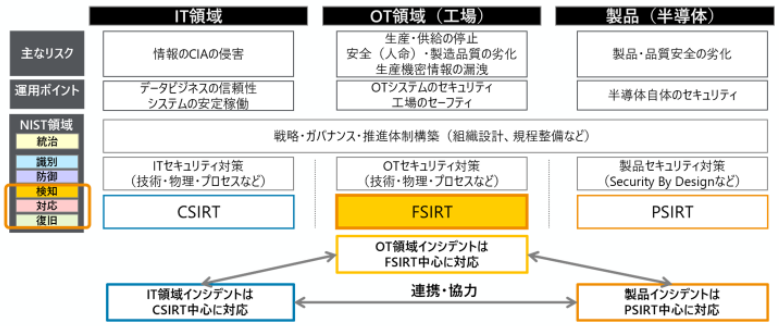




ガイドラインの構成　4-3. 運用（監視・対応・復旧・改善） - FSIRTによる運用①

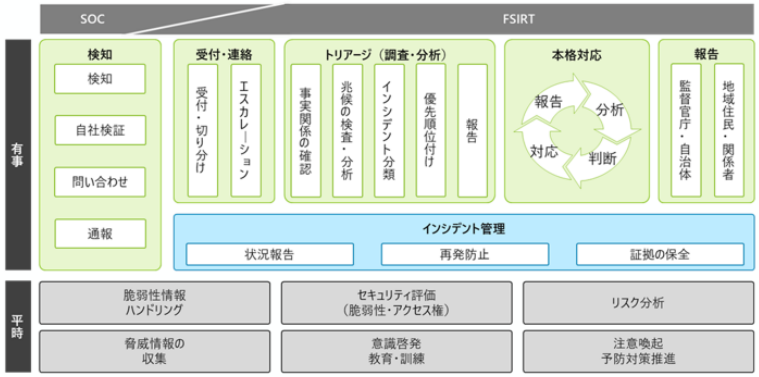
半導体デバイス工場でのFSIRTの事例

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



FSIRTの有事および平時の対応

- **FSIRTでは、サイバー攻撃の検知における有事の対応を行える体制と運用を整えるとともに、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では早期に拡大防止を図る対応を行う。被害の発生が確認された場合、エスカレーションを行い、通常生産稼働できる状態に早期復旧を行う。



ガイドラインの構成

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

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

ファブエリアの特徴	攻撃のポイント	対策例
大フロアーレイアウトの中に、重要な資産に区分される装置ツールが数多く存在する 装置ツールの故障修理・不具合改善にて、保守用デバイスの接続、ソフトウェアコンポーネントの入替、装置ツールストレージ交換を行う	装置ツールの不正操作 不正媒体の装置ルール接続 →不正プログラム実行 →マルウェア感染	装置ツールでのコンソールログイン認証、USBポート物理・論理保護 ストレージ保有デバイスの持ち込み制限
プロセス工程編成、装置ツールの機種や台数規模などレイアウトの視覚情報も生産機密情報とする工程が多い	持込機器の不正録画 →情報搾取	録画機能デバイスの持ち込み制限
自動搬送機が無線制御されており、利用無線周波数が管理制御されている	持込機器の妨害電波発信 →機能停止	無線電波発信デバイスの持ち込み制限
装置ーシステム間、装置間のファブネットワーク通信は業界標準の平文／未認証プロトコルを利用している	持込機器の不正NW接続 →高負荷攻撃（DoS）NW攻撃 MITM、Replay、FDLA等	コンピュータデバイスの持ち込み制限
非常に多くの人員が出入りする（顔見知りではない） • 装置ツールを管理する社員とともに、様々な装置メーカーと保守員が入室する。 • 24時間／7日間の連続稼働のため交代勤務者含めた人数登録となる • 保守員は、常駐者・訪問者が混在する • クリールームのため全身クリーンスーツを着用しており、視覚情報による個人識別が困難である	工場およびファブエリアへの不正侵入	入室許可制限（社員、常駐者、訪問者） 位置情報等での個人識別・追跡記録

4.2.5　今後の改定に向けて

デバイス工場における OT 領域のファシリティエリアについては現在検討されている国際的な規格との連携を考慮し、半導体デバイス工場における OT ガイドラインの対象外としているが、来年度以降の改定にて対象とする。

また、半導体デバイス工場における OT ガイドラインではサプライチェーン全体の保護の最初の段階として半導体デバイスメーカの工場を対象としているが、将来的には装置メーカや部素材メーカなどサプライチェーン全体への拡大を目指して改定を想定している。

5. 検討会等の運営

本事業では、専門的な見地からの検討、分析、助言を得ることを目的に、半導体関連産業の関係者やサイバーセキュリティに係る有識者等からなる検討会（産業サイバーセキュリティ研究会 WG1 の下に新設する半導体産業 SWG 及び半導体産業 SWG の下で開催するガイドライン作成のための作業部会）を開催した。

5.1 検討会の構成

（1）半導体産業 SWG

半導体産業 SWG の概要を以下に示す。

表 5.1-1 半導体産業 SWG の概要

（敬称略）

会議体名	半導体産業サブワーキンググループ
目的	• 半導体産業において求められる取組の整理 • デバイス製造におけるセキュリティ確保のための取組を整理したガイドラインの整備 • IT セキュリティ向上のための IT 対策基準の整備 • 国際規格策定等サイバーセキュリティ関連活動への参画（SMCC への参加推進等）
座長	江崎 浩（東京大学 大学院情報理工学系研究科 教授）
委員	秋山 裕明（マイクロンメモリジャパン株式会社） 飯嶋 織行（東京エレクトロン株式会社） 高橋 清文（株式会社ニコン） 高原 正裕（株式会社ダイフク） 中川 昭一（一般社団法人電子情報技術産業協会） 長野 茂樹（株式会社 SCREEN） 浜島 雅彦（SEMI ジャパン） 東 健介（株式会社アドバンテスト） 藤井 俊郎（Rapidus 株式会社） 三井 豊興（一般社団法人電子情報技術産業協会） 渡部 潔（一般社団法人日本半導体製造装置協会）
事務局	経済産業省 サイバーセキュリティ課 デロイト トーマツ サイバー合同会社

（2）半導体産業 SWG 作業部会

半導体産業 SWG 作業部会の概要を以下に示す。

表 5.1-2 半導体産業 SWG 作業部会の概要

会議体名	半導体産業サブワーキンググループ 作業部会
目的	• 専門的な見地から、デバイス製造におけるセキュリティ確保のための取組を整理した半導体デバイス工場における OT ガイドライン等の内容を検討
メンバー企業	キオクシア株式会社、 サンケン電気株式会社、 株式会社 SCREEN セミコンダクタソリューションズ、 株式会社 SCREEN ホールディングス、 ソニーセミコンダクタソリューションズ株式会社、 ソニーセミコンダクタマニュファクチュアリング株式会社、 株式会社ダイフク、 一般社団法人電子情報技術産業協会 半導体部会、 東京エレクトロン株式会社、 東芝デバイス＆ストレージ株式会社、 株式会社ニコン、 一般社団法人日本半導体製造装置協会、 ヌヴォトンテクノロジージャパン株式会社、 株式会社ベリサーブ、 マイクロンメモリジャパン株式会社、 三菱電機株式会社、 Rapidus 株式会社、 ルネサスエレクトロニクス株式会社、 ローム株式会社 ※上記メンバー企業は第 4 回作業部会実施時点（3/11）
事務局	経済産業省 サイバーセキュリティ課 デロイト トーマツ サイバー合同会社

5.2 全体スケジュール

本事業では、計 2 回の SWG と計 4 回の作業部会を開催した。各回の開催日時・場所を下記に示す。

表 5.2-1 検討会等の開催日時・場所

イベント名	開催日時	開催場所
第 1 回 SWG	令和 6 年 11 月 26 日（火）	新東京ビル 7 階セミナール

	13 時 00 分～14 時 45 分	ーム S(ハイブリッド)
第 1 回作業部会	令和 6 年 12 月 17 日(火) 15 時 00 分～17 時 00 分	オンライン(Teams)
第 2 回作業部会	令和 7 年 1 月 16 日(木)15 時 00 分～17 時 00 分	新東京ビル 7 階セミナール ーム M(ハイブリッド)
第 3 回作業部会	令和 7 年 2 月 20 日(木) 9 時 30 分～11 時 30 分	オンライン(Teams)
第 4 回作業部会	令和 7 年 3 月 11 日(火)13 時 30 分-15 時 30 分	新東京ビル 7 階セミナール ーム D(ハイブリッド)
第 2 回 SWG(予定)	令和 7 年 3 月 31 日(月)13 時 00 分～15 時 00 分	新東京ビル 7 階セミナール ーム A(ハイブリッド)

5.3 第 1 回 SWG

5.3.1 開催概要

第 1 回 SWG では、以下の議事次第と資料で議論が行われた。

日時:
令和 6 年 11 月 26 日(火)13 時 00 分～14 時 45 分

議事次第:
1. 開会
2. 事務局説明
3. 自由討議
4. 閉会

配付資料:
資料 1 議事次第・配布資料一覧
資料 2 委員等名簿
資料 3 本サブワーキンググループの議事運営について(案)
資料 4 事務局説明資料
資料 5 JEITA 半導体部会講演資料
資料 6 SEMI 講演資料

5.3.2 議事内容

下記に会議中の主な発言内容を示す。

＜守るべき対象について＞

- 材料メーカやコンポーネントメーカも検討の対象に含めても良いのではないか。
- 知財や情報の流出については、半導体産業におけるセキュリティ対策基準の作成で対応したいと考えており、半導体デバイス工場における OT ガイドラインの検討から始め、後半にかけて半導体産業におけるセキュリティ対策基準の中身を検討していく。
- サプライチェーンのセキュリティ対策評価制度 SWG 等他 SWG の成果を本 SWG に展開できる。検討において他業界の取組を参考にする必要があれば、他の SWG からエキスパートを呼んで話をしてもらいたい。
- レガシー半導体について、メーカ内に閉じた製造ノウハウだけでなく、顧客とのすり合わせ等も含め様々なノウハウがあると認識。サイバーセキュリティの観点から、先端半導体とレガシー半導体との違いも含めて、様々なご意見をいただきたい。
- 検討の進め方に関して、資料 6 に記載の SMCC プログラムカレンダーに作業部会のスケジュールを整合させてはどうか。これにより、日本で検討した内容をグローバルに発信し、グローバルの検討内容を国内に展開することが可能になる。半導体デバイス工場における OT ガイドラインは来年の夏頃に公表との説明があったが、これを SEMICON West で発信するなど、良いトラクション（牽引力）が作れると思う。
- 情報を守るため自社で情報のラベリングを行うことが大切であり、このベースがないと、守るべきものが何か優先順位が付けられないので、情報管理のガイドラインなども今回の検討に必要と思う。

＜ガイドラインについて＞

- E187 は初歩的なレベルであるが、台湾においても守られていない企業があり、次のステップが大事である。日本から E187 の実装を前提に次はインプルメンタブルなステップを示すことで、日本が国際的な標準化のリーダーシップの中に入っていく構造にすることが重要であり、本 SWG はその良い機会である。
- 半導体工場ではかなりのロボットオペレーションが導入されており、ソフトウェアロボットとハードウェアロボットの両方が工場に入ってくると、それに対するプロテクション、調達条件を調達側が持っておくというのは重要なことになる。調達の際にこれら条件を要求しやすくするため、国として基準を作っており、政府調達の条件とすることが考えられ、このような枠組みを適用するのが一番効率的である。
- 一番重要なのは、企業のオペレーション上のクリティカルな点を把握して対策の優先度を上げていく議論である。他の SWG と違う点があるはずで、そこを明確

化するのが非常に重要である。

- サイバーセキュリティ対策に関しては E187 をベースするのが一番わかりやすいと思うが、各社の E187 への準拠状況を評価したうえで、半年間のフィージブルな目標を設定するのが良いと思う。E187 自体は非常にベーシックな内容であるが、結構な数の日本企業が対応できていないと認識している。
- NIST の CMMC 等の認証取得を考えているが、米国基準の認証取得となるため、日本国内で認知されるかという課題はある。国際的な基準の中に日本の意見をうまく入れ込み、日本で同様の認証を取得するとNISTの基準にも合致している状態になると非常にありがたい。

＜検討スコープについて＞

- 台湾が企業に要求している対策にはコーポレートガバナンスまで含まれており、脆弱性が破られた際の PSIRT、CSIRT 等のインシデントレスポンスの体制もチェックリストに入っている。しかしながら、大企業と中小企業で体制や人的リソースが違うので、業界として中小企業をどのようにサポートするも重要な論点になる。サプライチェーンの中でこれがビジネスとして動けばエコシステムとして回っていく認識である。
- ガイドラインを活用する際に、どの製品を選べばよいかという課題があるが、国のガイドラインにおいて特定のプロダクトを推奨することはできない。しかし、方法論を実装するプロダクト、ソリューションとの記述はできる。公正取引の観点に注意しながら書く必要はあるが、プラティカルな情報をガイドラインに添付していくことは、業界として実際にやっていることであり、適合していないのではないかという場合に修正箇所をフィードバックすることで対応できる。買う側がベンダーに対して実装すべき要件を言うことも可能であり、業界としてどうしていくかが重要である。

＜人材育成について＞

- 米国では退役軍人等様々なサイバーセキュリティ人材がいるが、日本人に比べて給料が 3-4 倍と高額なため、雇用することは非現実的である。日本では、聞いている限り人材がそろっている会社はゼロである。したがって、人材をいかに育成するかが一番重要であり、今いるサイバーセキュリティ人材をいかに取られないということを意識する必要がある。また、高専を活用する取組は九州の方で既に始まっている。人材への投資をしっかり行うべきと経営者に対してメッセージすることも重要である。
- 人材育成については WG2 で検討しており連携しながら IT・OT 人材、製品セキュリティ人材について検討できればと考えている。OT セキュリティについては紹

介させていただいた IPA の中核人材育成プログラム等あり、この場を活用して色々な取組を実施する必要があると認識している。

- SOCレベルのテクニカルな部分を判断できる専門家については、現在アウトソースでサービスを買える状態にあり、AI を使って振る舞い検知を行うプロダクトを提供する企業もある。半導体業界としてサービス事業者を選定し情報を共有するとよい。しかしすべてアウトソーシングすることは難しく、企業内でログデータ等を判断できるエンジニアが必要となる。このようなエンジニアを育成する際に、IPA の ICSCoE が実施している取組が活用できる。新しいものを作るのではなく、既存のカリキュラムに半導体業界として戦略的に人材を投入して育成するのが良い。

5.3.3 運営業務

半導体産業SWGの運営業務として、日程調整、出欠確認、会場／リモート会議環境の確保、会議運営に必要な備品等準備、資料作成、資料準備／印刷、会場設営、受付、会議運営支援、議事録作成、委員に対する謝金の支払い等を実施した。

5.4 第 1 回作業部会

5.4.1 開催概要

第 1 回作業部会では、以下の議事次第と資料で議論が行われた。

日時：
令和 6 年 12 月 17 日(火)15 時 00 分～17 時 00 分

議事次第：
1. 開会
2. 第 1 回作業部会について
3. 半導体デバイス工場における OT ガイドライン作成の進め方
4. 半導体デバイス工場における OT ガイドラインの骨子(案)について
5. 自由討議
6. 閉会

配付資料：
資料 1 議事次第・配布資料一覧
資料 2 作業部会構成員名簿 ※会議後配布
資料 3 半導体デバイス工場における OT ガイドラインの作成について

5.4.2　議事内容

OT ガイドラインの骨子のすり合わせが行われた。自由討議では、規格の標準化、具体的な対策やツールの提示、社内体制等のトピックが挙げられた。

5.4.3　運営業務

半導体産業 SWG 作業部会の運営業務として、日程調整、開催案内、出欠確認、リモート会議環境の確保、会議運営に必要な備品等準備、資料作成、資料準備、会議運営、議事録作成等を実施した。

5.5　第 2 回作業部会

5.5.1　開催概要

第2回作業部会では、以下の議事次第と資料で議論が行われた。

日時：
令和 7 年 1 月 16 日(木)15 時 00 分～17 時 00 分

議事次第：
1. 開会
2. 第1回作業部会振り返り
3. 半導体デバイス工場における OT ガイドライン(案)について
4. 自由討議
5. 閉会

配付資料：
資料 1　議事次第・配布資料一覧
資料 2　作業部会構成員名簿
資料 3　第 1 回作業部会振り返り
資料 4　半導体デバイス工場における OT ガイドライン(案)説明資料

5.5.2　議事内容

OT ガイドラインのたたき台の記述内容の確認が行われた。自由討議では、対策の優先順位やスコープ等のトピックが挙げられた。

5.5.3　運営業務

半導体産業 SWG 作業部会の運営業務として、日程調整、開催案内、出欠確認、会場／リモート会議環境の確保、会議運営に必要な備品等準備、資料作成、資料準備／印刷、会場設営、

受付、会議運営、議事録作成等を実施した。

5.6 第 3 回作業部会

5.6.1 開催概要

第 3 回作業部会では、以下の議事次第と資料で議論が行われた。

日時：
令和 7 年 2 月 20 日(木) 9 時 30 分～11 時 30 分

議事次第：
1. 開会
2. 第 2 回作業部会振り返り
3. 半導体デバイス工場における OT ガイドライン(案)の方針について
4. 半導体デバイス工場における OT ガイドライン(案)について
5. 自由討議
6. 閉会

配付資料：
資料 1 議事次第・配布資料一覧
資料 2 作業部会構成員名簿
資料 3 第 1 回作業部会振り返り
資料 4 半導体デバイス工場における OT ガイドライン(案)の方針
資料 5 半導体デバイス工場における OT ガイドライン(案)
資料 6 第 1 回作業部会議事録
資料 7 第 2 回作業部会議事録

5.6.2 議事内容

OT ガイドライン第 1 章～第 3 章の記述内容の確認が行われた。自由討議では、物理的対策やリスク分析、脆弱性評価等のトピックが挙げられた。

5.6.3 運営業務

半導体産業 SWG 作業部会の運営業務として、日程調整、開催案内、出欠確認、リモート会議環境の確保、会議運営に必要な備品等準備、資料作成、資料準備、会議運営、議事録作成等を実施した。

5.7 第 4 回作業部会

5.7.1 開催概要

第 4 回作業部会では、以下の議事次第と資料で議論が行われた。

日時：
令和 7 年 3 月 11 日(火)13 時 30 分-15 時 30 分

議事次第：
1. 開会
2. 第 3 回作業部会振り返り
3. SC 対策評価制度(検討中)について
4. 半導体デバイス工場における OT ガイドライン(案)について
5. NIST CSF2.0 半導体製造プロファイル パブコメについて
6. 自由討議
7. 閉会

配付資料：
資料 1 議事次第・配布資料一覧
資料 2 作業部会構成員名簿
資料 3 第 3 回作業部会振り返り
資料 4 サプライチェーン強化に向けたセキュリティ対策評価制度(検討中)
資料 5 半導体デバイス工場における OT ガイドライン(案)説明資料
資料 6 半導体デバイス工場における OT ガイドライン(案)
資料 7 NIST CSF2.0 半導体製造プロファイルパブコメについて

5.7.2 議事内容

OT ガイドライン第 4 章「半導体デバイス工場における具体的対策例」確認が行われた。自由討議では、推奨と要求の書き分け、半導体業界特有の記載等のトピックが挙げられた。

5.7.3 運営業務

半導体産業 SWG 作業部会の運営業務として、日程調整、開催案内、出欠確認、会場／リモート会議環境の確保、会議運営に必要な備品等準備、資料作成、資料準備／印刷、会場設営、受付、会議運営、議事録作成等を実施した。

5.8 第 2 回 SWG

5.8.1 開催概要

第 2 回 SWG では、以下の議事次第と資料で議論が行われた。。

日時：
令和 7 年 3 月 31 日(月)13 時 00 分～15 時 00 分

議事次第：
1. 開会
2. SEAJ 講演
3. IPA 講演
4. 事務局説明
5. 半導体デバイス工場における OT ガイドラインについて
6. 自由討議
7. 閉会

配付資料：
資料 1 議事次第・配布資料一覧
資料 2 作業部会構成員名簿
資料 3 SEAJ 講演資料
資料 4 IPA 講演資料① J-CSIP 半導体業界 SIG について
資料 5 IPA 講演資料② ICSCoE の事業説明
資料 6 事務局説明資料
資料 7 サプライチェーン強化に向けたセキュリティ対策評価制度(検討中)
参考資料 1 半導体デバイス工場における OT ガイドライン(案)概要資料
参考資料 2 半導体デバイス工場における OT ガイドライン(案)

5.8.2 議事概要

OT ガイドライン(案)について確認・検討が行われ、サプライチェーン対策評価制度、人材育成や攻撃情報共有等のトピックが挙げられた。

5.8.3 運営業務

半導体産業 SWG の運営業務として、日程調整、出欠確認、会場／リモート会議環境の確保、会議運営に必要な備品等準備、資料作成、資料準備／印刷、会場設営、受付、会議運営支援、議事録作成、委員に対する謝金の支払い等を実施した。

以上