経済産業省

資料5

事務局説明資料

2025年6月19日

商務情報政策局 サイバーセキュリティ課・情報産業課

目次

Ⅰ．第2回SWG振り返り

Ⅱ．作業部会での検討状況

Ⅲ．　OTセキュリティガイドライン（案）の概要

Ⅳ．今後の予定

Ⅴ．ご議論いただきたい点

Ⅰ．第2回SWG振り返り

第2回SWG開催概要

日時　　：2025年3月31日（月）13:00-14:45

アジェンダ：SEAJ様講演

IPA様講演

事務局説明

Ⅰ. 第1回SWG振返り

Ⅱ. 作業部会での検討状況

Ⅲ. NIST CSF 2.0半導体プロファイル

Ⅳ. 半導体産業におけるセキュリティ対策基準

Ⅴ. OTガイドライン（検討中）の概要

Ⅵ. 今後の予定

Ⅶ. ご議論いただきたい点

第2回SWGのご意見取りまとめ（1/2）

項目	委員のご意見	SWGでの対応	OTガイドラインでの対応
具体的対策事例	① サイバーセキュリティにおける対策事例を取りまとめていただきたい	• 本SWGの講演等にて対策事例を紹介予定	• 第4章『具体的対策事例』に半導体業界における対策事例を記載
	② 工場向けのFSIRTと製造装置向けのPSIRT間の連携について、記載していただきたい	ー	• 第4章『4.3 FSIRTによる運用』に、FSIRTとPSIRT間の連携・協力体制について記載
マチュリティ（成熟度）	③ Tierのようなマチュリティの整理を導入する予定はあるか	ー	• 将来的な課題として、2026年度以降にガイドラインを改訂する際には、マチュリティ（成熟度）の考え方を取り込むことを検討
グローバルとの整合	④ グローバルからみた際のOTガイドラインの地位や認識を高める取り組みを考えているか	ー	• NIST CSF 2.0 半導体製造プロファイル等と整合性を取りつつ作成しており、今後グローバルな認証の取組が進む場合にも整合性を確保予定
	⑤ 各国でSMCCとの連携が進められており、同様に連携することでグローバルな基準とすることにフォーカスしてはどうか	• 共同で会合を開催する等、SMCCとの協力的な活動について協議中	ー

第2回SWGのご意見取りまとめ（2/2）

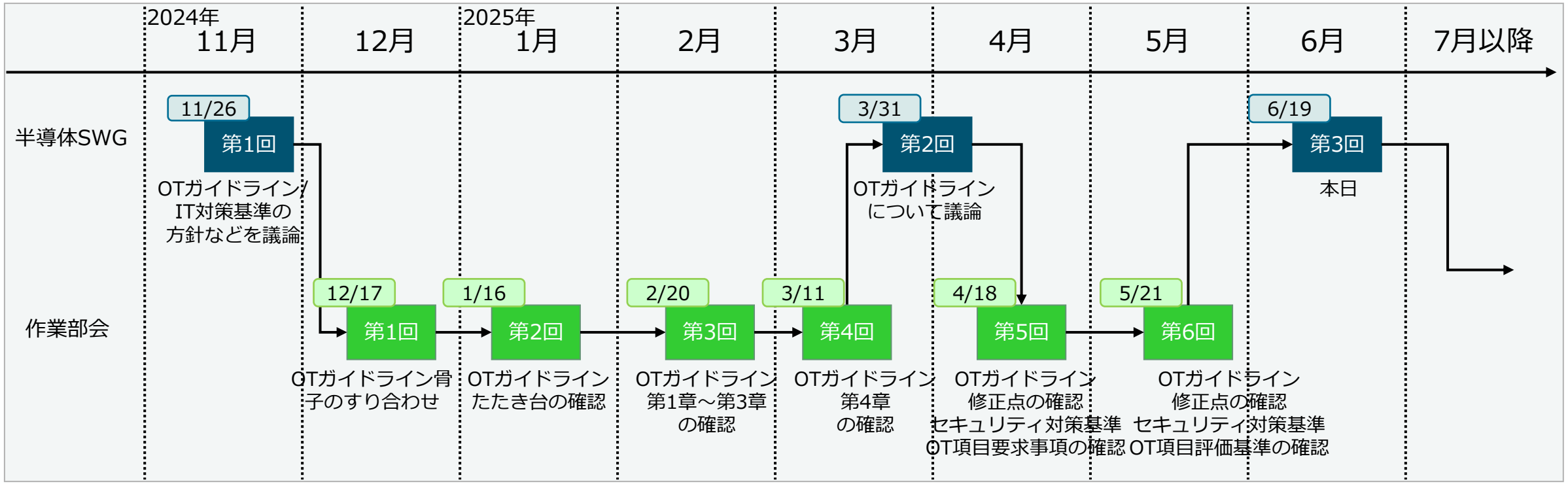
項目	委員のご意見	SWGでの対応	OTガイドラインでの対応
レガシー機器	⑥ レガシー機器について支援を検討していただきたい	• レガシー機器のセキュリティ対策の課題の１つとしてOT制御系人材の不足があるところ、ICSCoEの人材育成カリキュラムを紹介	• 第4章『4.2 装置ツールの被害と極小化と早期復旧を備えた追加防御対策』にレガシー機器に対する技術的対策事例を記載
OTガイドラインの普及	⑦ どのようにOTガイドラインをサプライヤー全体に広げることを検討しているか	• サプライチェーン強化に向けたセキュリティ対策評価制度（検討中）における実証等を通じて、コストや実現可能性を検討	ー

Ⅱ．作業部会での検討状況

作業部会の開催実績

- 引き続き作業部会を開催し、OTガイドラインの修正やセキュリティ対策基準の検討を実施

	開催日時	アジェンダ
第5回作業部会	2025年4月18日（金）13:00～15:00	• OTガイドライン第4章具体的対策事例の修正点を中心に確認 • セキュリティ対策基準（OT項目：要求事項）の確認
第6回作業部会	2025年5月21日（水）13:00～15:00	• OTガイドライン修正点の確認 • セキュリティ対策基準（OT項目：評価基準）の確認



Ⅲ．OTセキュリティガイドライン（案）の概要

半導体デバイス工場におけるOTセキュリティガイドライン～全体概要～

ガイドラインの背景と目的

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

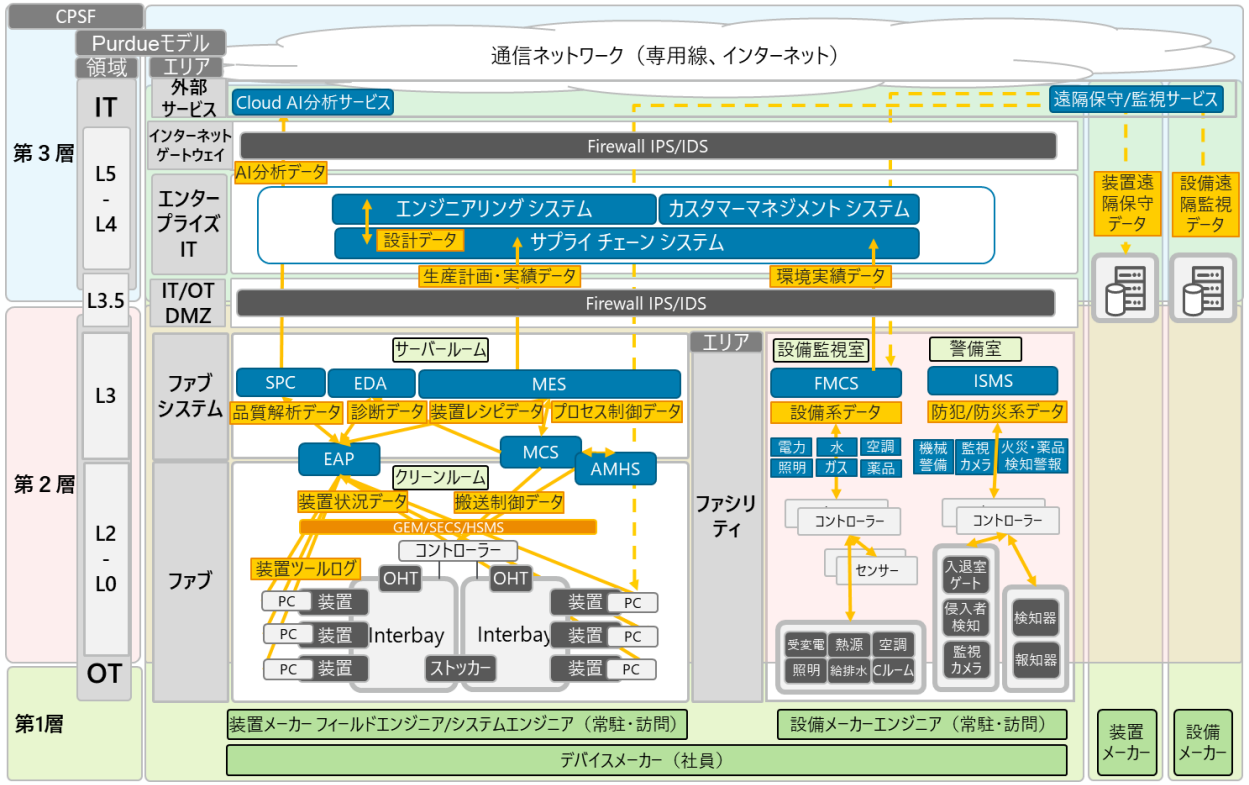
本ガイドラインの活用方法

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

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

本ガイドラインで示す対策項目

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



半導体デバイス工場のリファレンスアーキテクチャ

ガイドラインの構成　1. 本ガイドライン作成の背景と目的①

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

ガイドラインの背景と目的

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

想定読者

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

想定する攻撃主体

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

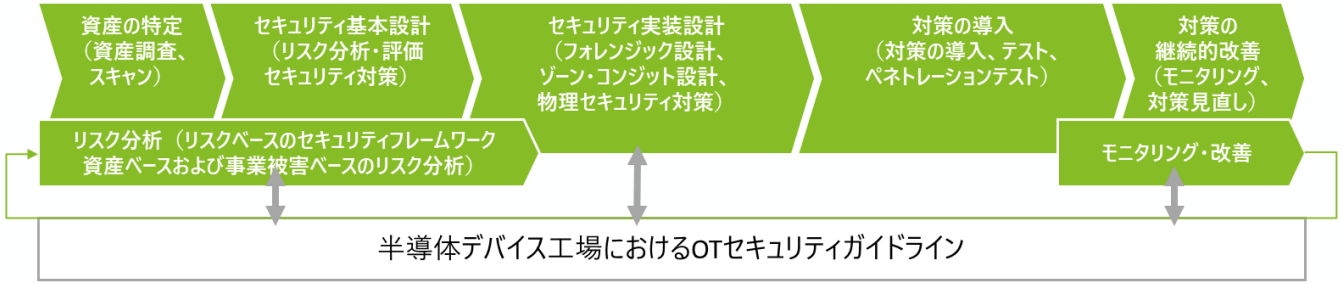
守るべき対象

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

ガイドラインの構成　1. 本ガイドライン作成の背景と目的②

本ガイドラインの利活用

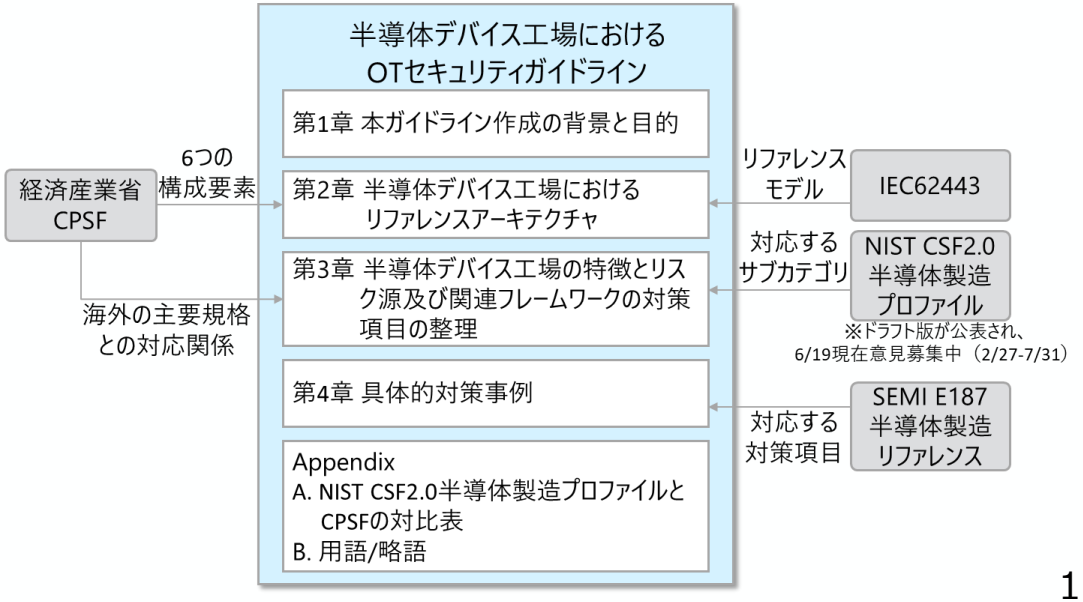
- 半導体サプライチェーンの保護という目的を達成するためには、構成する各企業が供給責任を果たせるサイバーセキュリティ対策を実現する必要があり、供給責任・事業継続計画と整合する必要がある。
- 供給責任及びその説明責任を果たすためには、**リスクの評価を行い、その結果を踏まえた適切な対策を検討・設計・実装する必要がある。**
- 本ガイドラインは、**工場のセキュリティ対策を進めるための一般的なプロセスにおいて、リスクベースのサイバーセキュリティフレームワーク（CPSF*1、NIST CSF2.0 *2）を活用したリスク分析、及び具体的な対策を検討する際などに活用することが想定される。**また、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



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

本ガイドラインの構成

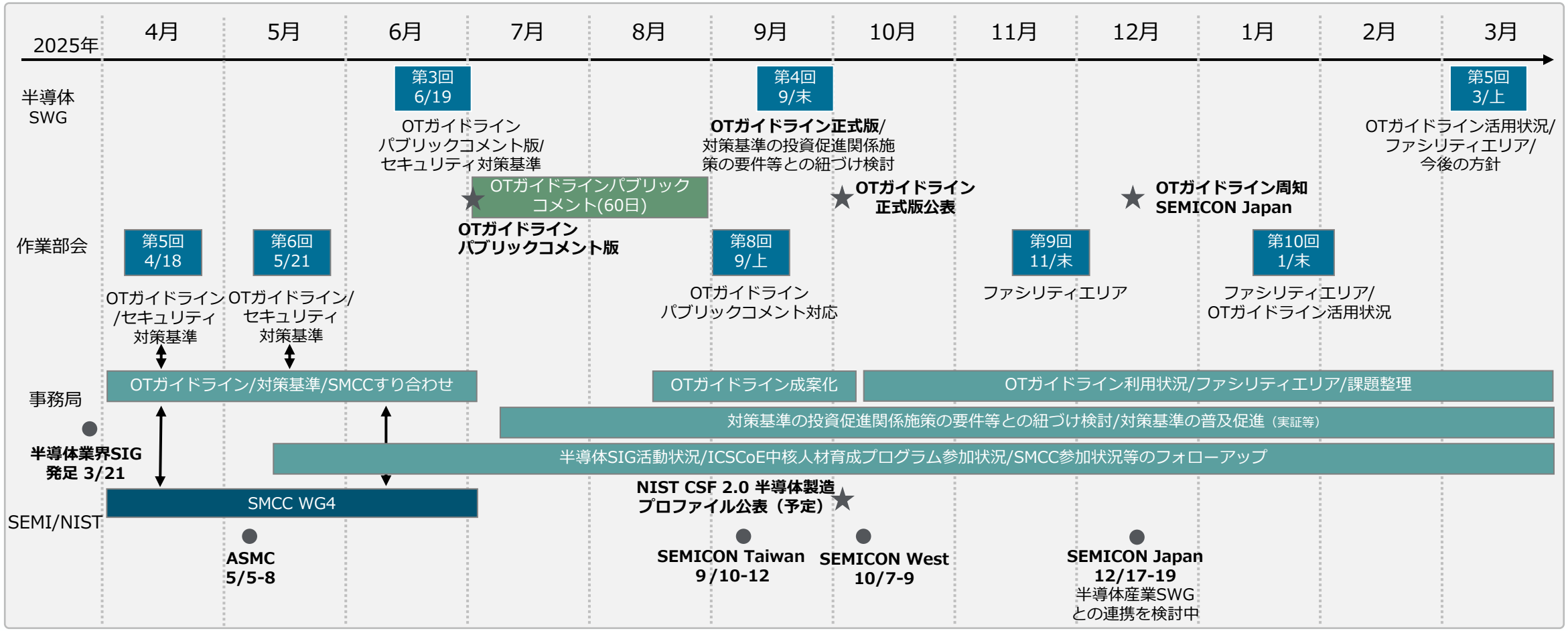
- 第2章：IEC62443のPurdueモデルを活用し半導体デバイス工場を領域・エリアに分割し、各エリアにおける CPSFの6つの構成要素を洗い出した。
- 第3章：前述CPSFの6つの構成要素に関連する半導体デバイス工場における特徴を整理し、 CPSFを活用しこれら特徴に起因するリスク源の洗い出し、及びNIST CSF2.0半導体製造プロファイルとの紐づけを行った。
- 第4章：マイクロセグメンテーション等、半導体デバイス工場において特に重要となる取り組みに関しては、より詳細な対策方法の例を示した。



Ⅳ．今後の予定

スケジュール（案）

- 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については、７月頃から60日間のパブリックコメントを経て2025年の秋頃に策定予定（英訳版も作成）
- セキュリティ対策基準については、投資促進関連施策の要件等との紐づけを検討予定



Ⅴ．ご議論いただきたい点

ご議論いただきたい点

【資料６・７・８】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

1. 特に、修正や追記を行った第4章 具体的対策事例について、ご意見をいただきたい。

2. パブリックコメントを開始するにあたり、業界団体への周知方法など積極的にご意見をいただくための方策について、ご助言いただきたい。

3. 普及に向けた取組について、ご意見をいただきたい。

【資料９】半導体産業におけるセキュリティ対策基準

1. OT評価項目の候補（案）について、ご意見をいただきたい。

2. OT評価基準（案）について、ご意見をいただきたい。

METI

Ministry of Economy, Trade and Industry