経済産業省

資料6

事務局説明資料

2025年3月31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1回SWG振り返り

Ⅱ．作業部会での検討状況

Ⅲ．NIST CSF2.0 半導体製造ﾌﾟﾛﾌｧｲﾙ

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

Ⅷ．半導体政策関連（参考）

Ⅰ．第1回SWG振り返り

第1回SWG開催概要

日時　　：2024年11月26日（火）13:00-14:45

アジェンダ：事務局説明

Ⅰ. 半導体産業におけるサイバー攻撃の現状

Ⅱ.半導体産業における現状と課題

Ⅲ.検討の方向性

Ⅳ.本SWGの進め方

Ⅴ.ご議論いただきたい点

JEITA様講演

SEMI様講演

第1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
守るべき対象	① 装置メーカーや部素材メーカーも検討の対象に含めてよいのではないか	• OTガイドラインにて対応	• 第1章『1.2 ガイドラインの対象者（想定読者）』に装置メーカーや部素材メーカーをサプライチェーンとし、装置メーカーや部素材メーカーを次年度以降の取組とすることを記載
	② 先端半導体デバイスの技術情報や顧客からの開示された半導体設計情報はどう守るか	• IT対策基準にて、知財や情報の流出をOT項目として追加することを検討	• 第1章『1.4 半導体製造工程における脅威とリスク』に半導体製造工程における守るべき対象を記載
	③ レガシー半導体の製造や設計に関するノウハウも重要ではないか	• OTガイドラインにて対応	
具体的記述	④ E187やNIST CSF等の国際標準は初歩的なレベルのものであり、OTガイドラインでは実装のレベルまで意識合わせをしているものであると良い	• OTガイドラインにて対応	• 第4章『具体的対策例』に半導体デバイス工場で対策検討を進めるうえで、参考となる具体的な事例についての内容を記載
	⑤ 各領域の推奨するソリューションの情報を取りまとめて欲しい	• OTガイドラインにて対応	• 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が、第4章『具体的対策例』に実装するプロダクト、ソリューションの方法論を記載

第1回SWGのご意見取りまとめ（2/2）

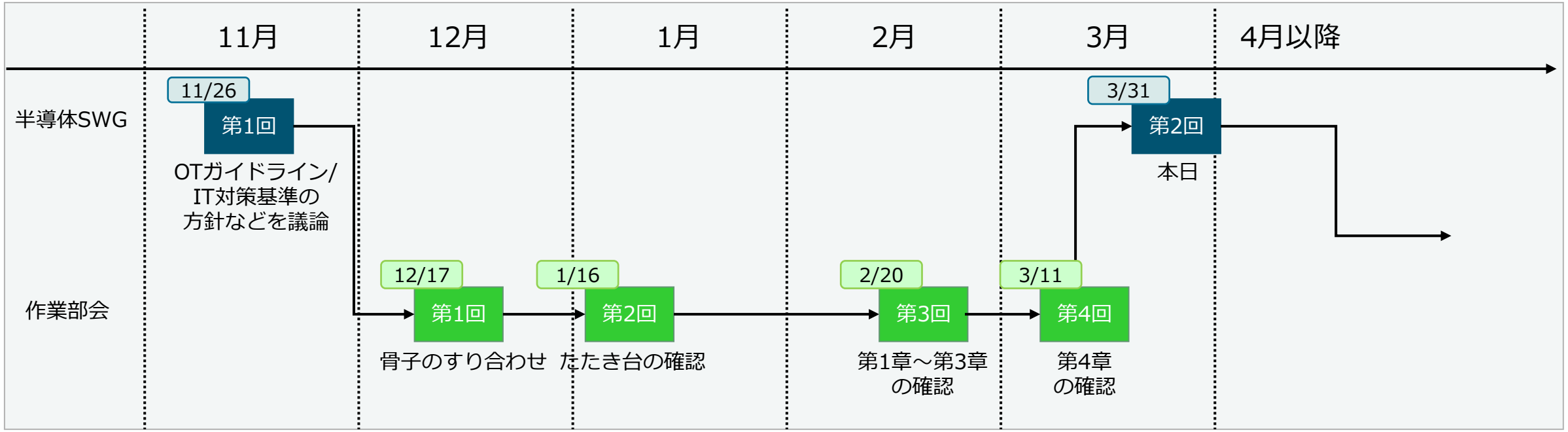
項目	委員のご意見	SWGでの対応	OTガイドラインでの対応
想定する攻撃アクターの範囲	⑥ 攻撃アクターについて国家背景のアクターも含め、E187に追加的な対策を検討する必要があるのではないか	• OTガイドラインにて対応	• 第1章『1.5 想定する攻撃主体』に国家の支援を受けたグループ（APT）を想定した対策レベルを実現する必要があることを記載
国際標準化	⑦ 国際基準の中に日本の意見を入れ込むことで、日本で同様の認証を取得すると、NISTの基準にも合致するようにして欲しい	• SWGを活用してNISTやSEMIと連携を検討 • NIST CSF2.0 半導体製造プロファイルへはパブコメを提出する予定	ー
人材育成	⑧ セキュリティ人材が不足しており、人材をいかに育成するかが重要である	• IT・OT人材、製品セキュリティ人材の育成について、ICSCoEの中核人材プログラムを活用することを推進	• 第4章『4.3 運用（監視・対応・復旧・改善） - FSIRTによる運用』に中核人材育成プログラムの活用について記載
スケジュール	⑨ 検討の進め方に関してSMCCと作業部会のスケジュールを整合させてはどうか	• SMCCと合わせた活動となるよう作業部会のスケジュールを整合	ー

Ⅱ．作業部会での検討状況

作業部会の開催実績

- 作業部会を設置し、集中的にOTガイドラインを作成

	開催日時	アジェンダ
第1回作業部会	2024年12月17日（火）15:00～17:00	• OTガイドラインの骨子のすり合わせ
第2回作業部会	2025年 1月16日（木）15:00～17:00	• OTガイドラインたたき台の記述内容の確認
第3回作業部会	2025年 2月20日（木） 9:30～11:30	• OTガイドライン第1章～第3章の記述内容の確認
第4回作業部会	2025年 3月11日（火）13:30～15:30	• OTガイドライン第4章「具体的対策例」の記述内容の確認



Ⅲ. NIST CSF2.0 半導体製造プロファイル

NIST CSF2.0 半導体製造プロファイルの意見公募について

NIST CSF2.0 半導体製造プロファイル概要

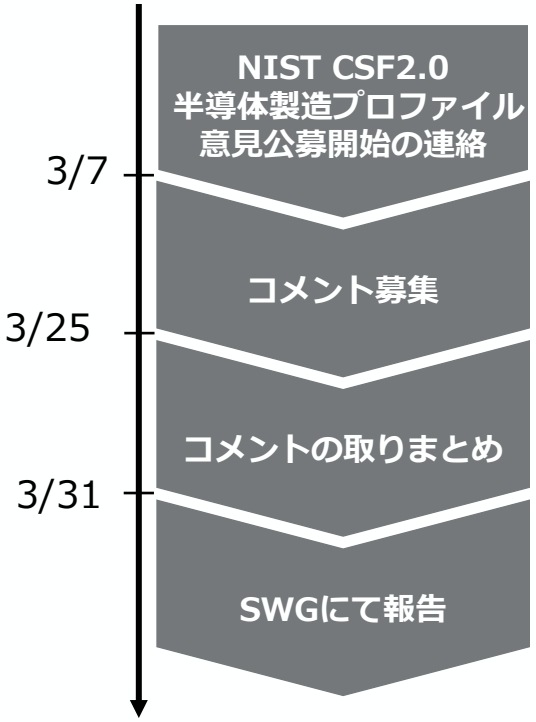
- NIST CSF2.0 半導体プロファイルは半導体製造業界がサイバーセキュリティ活動に優先順位をつけるのを支援するためのリスクベースのアプローチとして作成
- コメント期間：2/27-4/14（44日間）
- Cybersecurity Framework Version 2.0 Semiconductor Manufacturing Profile
  https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8546.ipd.pdf
- E-mail コメント提出先
  semiconductor-manufacturing-profile@nist.gov
  ※各社個別に直接意見を提出する場合

https://csrc.nist.gov/pubs/ir/8546/ipd

本SWGにおける意見公募の目的

- 国際的な規格の策定に我が国も積極的に参画することが重要と考えられるところ、半導体産業SWG 作業部会のメンバー企業よりコメントを募り、半導体産業SWGとして意見の提出を検討
  ※各社個別に意見を提出することを妨げるものではない

本SWGとしてのパブリックコメント提出の流れ



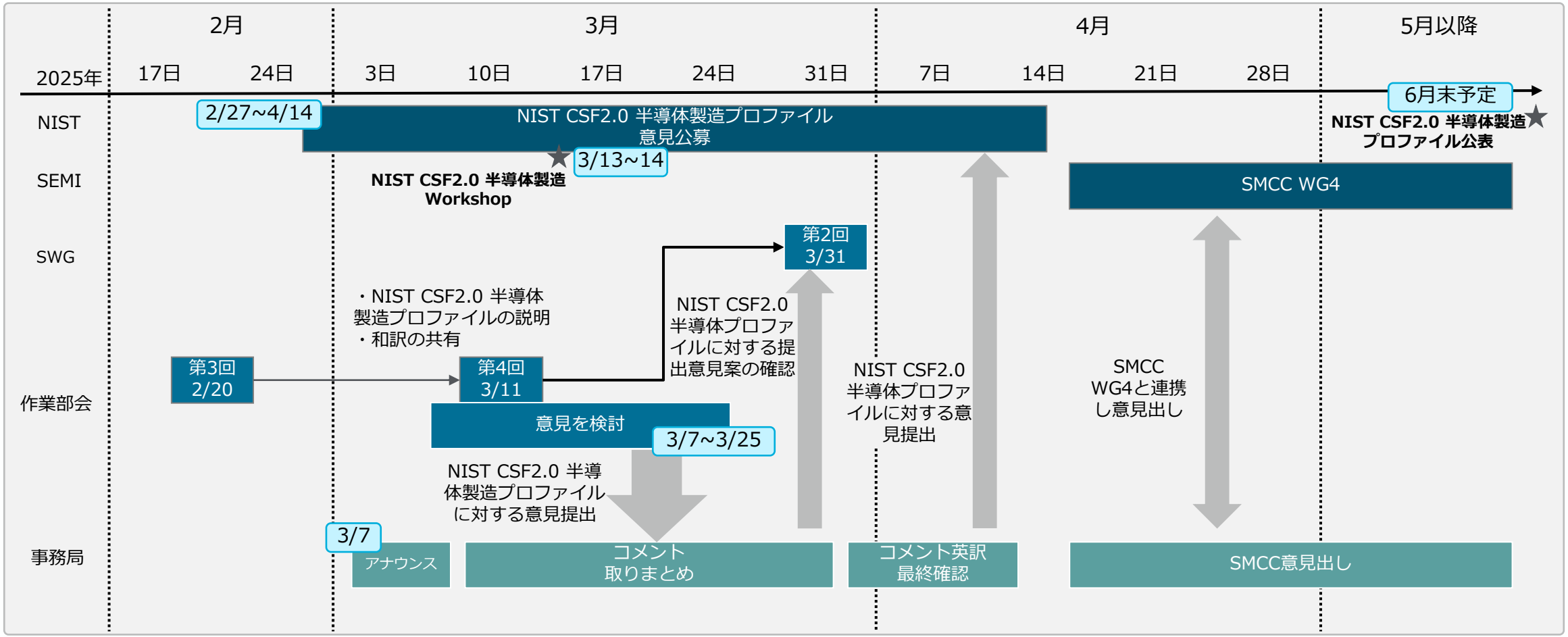
メールにて意見公募開始をアナウンス（3/7送付済）

SWG、作業部会メンバー企業よりコメントの募集
（コメント募集期間：3/7-3/25）

事務局にて構成員からの意見を取りまとめ

第2回SWG（3/31開催）にて報告後、コメントを提出

半導体産業SWGから意見提出に向けたスケジュール



半導体産業SWG作業部会メンバー企業からのコメント①

該当箇所	コメント
P.4　Figure2	「ベンダー」の意味が明確でないため、本文に「ベンダー」に関する説明を記載してほしい。
P.7　Figure3	製品ライフサイクルの矢印とツリー図の関係が明確になっていない。 これら 2 つの図が異なる概念を表している場合は、2 つの別個の図に分離した方がよい。
P.26　L870	レベル分けは３つで定義されることが多いが、あくまで例として記載いただくか、3つ以上が推奨としておいていただいた方がよい。
P.30　GV.OC-02 Ecosystem	「cyber supply chain risk」は、「Cybersecurity Supply Chain Risk」とした方がよいのではないか。
P.31　GV.OC-03 Ecosystem	第3者機関が顧客指定の機関だと機密情報が顧客に渡る可能性はないか。 また、第3者機関に依頼するのはサプライヤか。顧客はどのタイミングで結果をレビューするのか。
P.38　GV.RR-04 Fab	「元従業員のIDやアクセス権限をすぐに削除し、共通IDパスワードは更新する。」とあるが、共通IDのパスワード更新は半導体工場の運用及び半導体製造装置の運用上では難しい。
P.41　GV.SC-01 Equipment and Tooling	機器の「single points of failure」に対する想定される対策を具体的にしてほしい。機器で対処する必要のある例と対策があるとよい。
P.52　ID.AM-08 Equipment and Tooling	ガイダンスの「Equipment should provide logging capabilities.」がここに記載されている意図が不明である。
P.57　ID.RA-08 Equipment and Tooling	記載されているものは「進行中の製造業務への影響」に関連する問題ではなく、ゼロデイ攻撃に関連する懸念ではないか。

半導体産業SWG作業部会メンバー企業からのコメント②

該当箇所	コメント
P.65　PR.AA-02 Equipment and Tooling	考慮事項の「Embedding context-aware identity proofing capabilities provides a hardware-based foundation for secure authentication in end products.」が具体的にどのようなハードウェアベースの認証基盤を要求しているのかよくわからない。
P.67　PR.AA-04 Fab	クリーンルーム環境の固有の特性を考慮し、どのようなタイプの MFA が実行可能かを説明するとよい。たとえば、クリーンルーム環境には次のような特性がある： • ユーザーはゴーグル、マスク、手袋を着用する • 音響ノイズ • スマートフォンやトークンなどのデバイスの持ち込みは制限される
P.78　PR.PS-02	「ソフトはリスクに応じて保守され、交換され、削除されている。」とあるが、製造装置、ネットワークそのものがセキュアなハードウェア・ソフトウェアで構成されていないといけない。その点を別に明記した方がよいのではないか。
P.81　PR.PS-04 Equipment and Tooling	ログをどの程度の期間、装置に保存しておく必要があるのか追記してほしい。
P.110　RC.RP-06	「インシデントの経験を元に、改善策を作り、運用に反映されている。」のような ユースケースを記載してもよいのではないか。
ガイドライン全体	半導体工場には多くのレガシーシステムがあり、これらのシステムは今後も長期間稼働し続けると想定される。これは、半導体業界における最も重要な課題の 1 つである。より詳細なガイダンスを提供するために、レガシーシステムに関する専用のセクションを含めもらえるとよい。

Ⅳ.　半導体産業におけるセキュリティ対策基準

半導体産業におけるセキュリティ対策基準

目的

- 特定重要物資に位置づけられる半導体の知財等重要情報流出の防止及び生産活動の継続

方針

- 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を念頭にセキュリティの対策事項を作成
- 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の★4以上をベースに、半導体産業特有の工場におけるOTセキュリティ要件を追加し作成したい
  - IT項目：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の★４以上を活用予定
  - OT項目：作成中のOTガイドラインにおける第3章・第4章から重要な項目を数個程度で選定予定

Ｖ．OTガイドライン（検討中）の概要

半導体デバイス工場におけるOTガイドライン　～全体概要～

検討中

ガイドラインの背景と目的

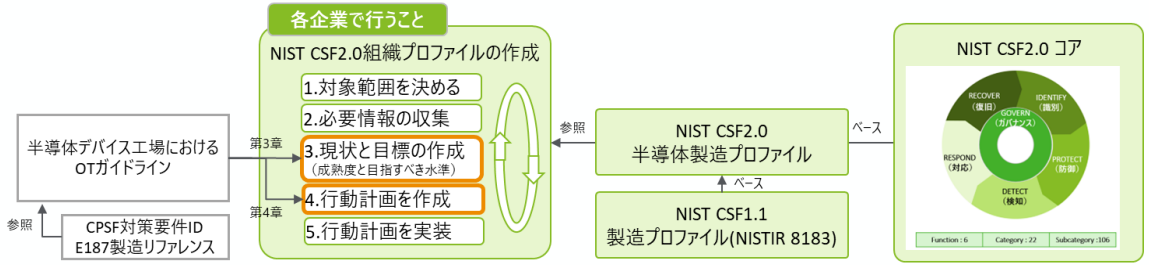
- 半導体産業の、経済及び安全保障上の重要性に鑑みると、今後高度なサイバー攻撃を受けることを想定し、対策を進めていく必要がある。
- 海外ではSEMI E187/E188規格が策定され、米国NISTによりNIST CSF2.0半導体製造プロファイルの策定が進められている。
  →**国際的な半導体産業における各種セキュリティ規格と整合しつつ、国内の半導体産業におけるセキュリティ対策状況等を踏まえた工場セキュリティ対策の指針を示すことが喫緊の課題。**

本ガイドラインの活用方法

- 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、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。

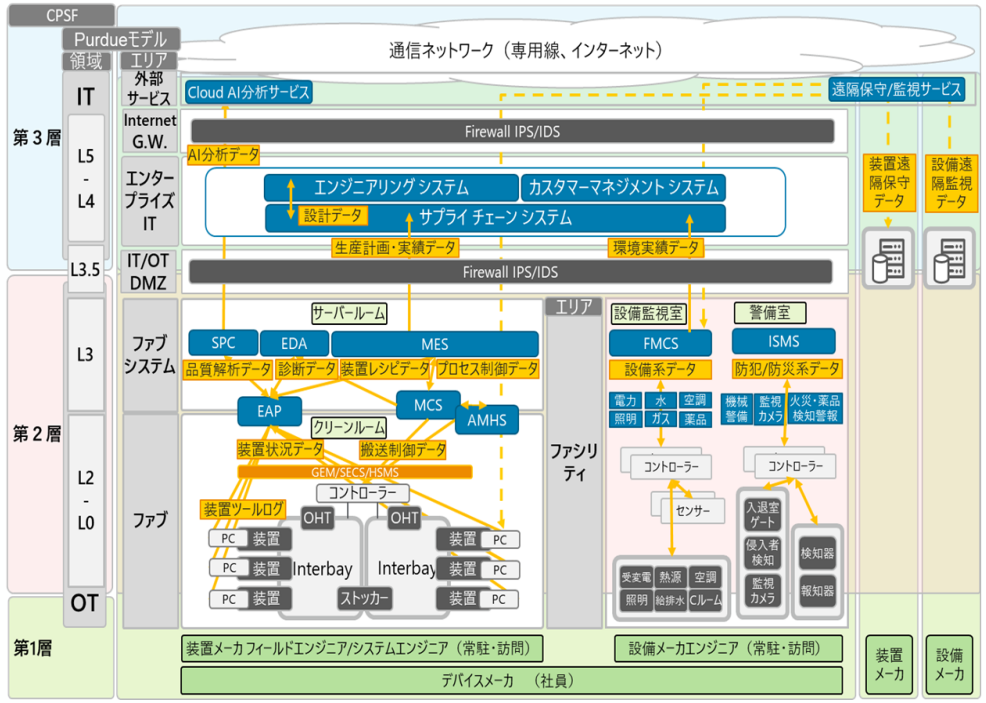
➢ **組織プロファイルの作成**
本ガイドラインの第3章の特徴及び考慮すべき観点に記載されている内容を参考に、サブカテゴリ毎の現状の把握と目標の設定

➢ **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



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。



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

検討中

- 「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

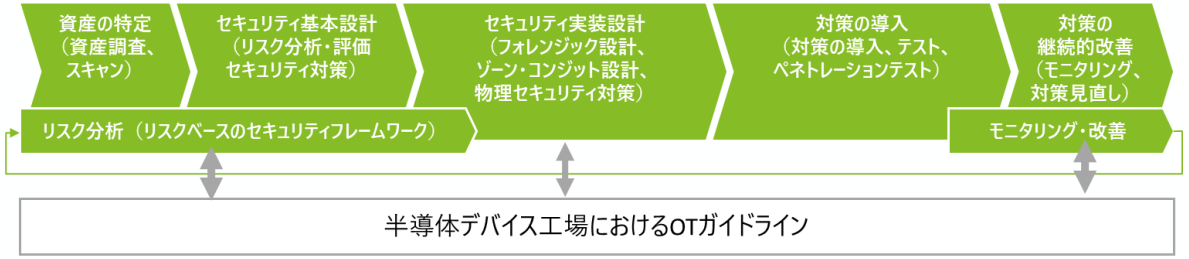
- 「生産目標の維持（供給責任）」「機密情報の保護」「半導体の品質の維持」「環境安全の維持」「人間の安全の維持」の5つの項目がNIST CSF2.0 半導体製造プロファイルで守るべき項目として挙げられている。
- 本ガイドラインでは特に**「生産目標の維持（供給責任）」「機密情報の保護」「半導体の品質の維持」**に焦点をあてる

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

検討中

本ガイドラインの利活用

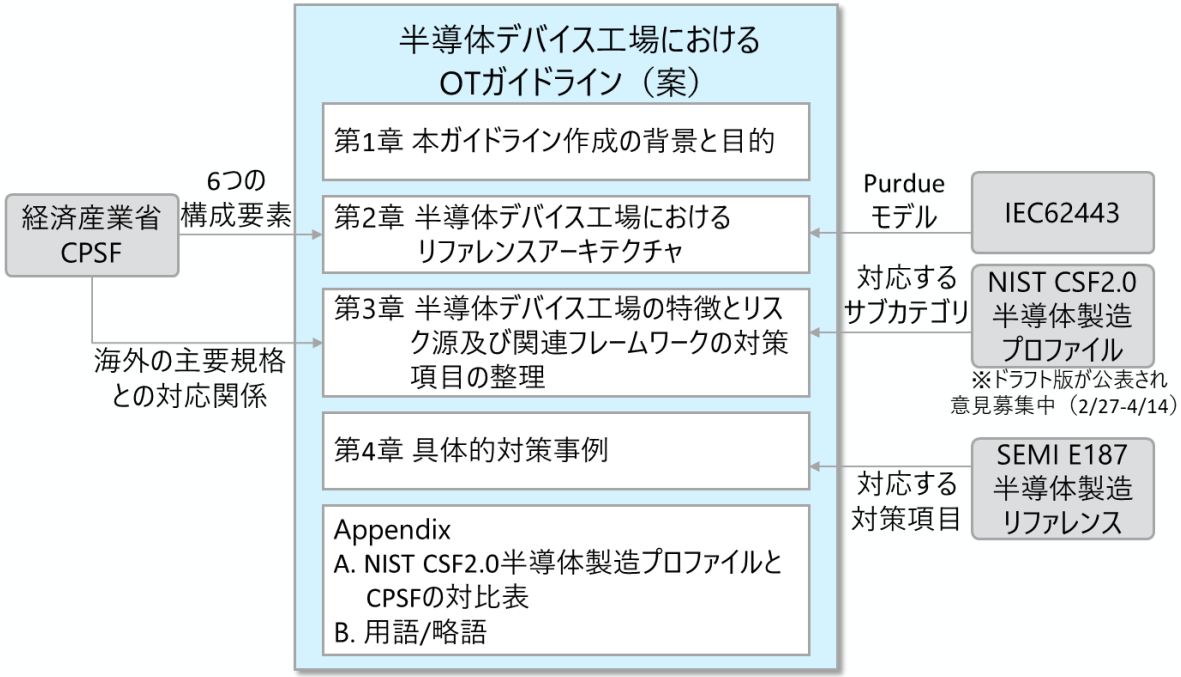
- 半導体サプライチェーンの保護という目的を達成するためには、構成する各企業が供給責任を果たせるサイバーセキュリティ対策を実現する必要があり、事業継続計画と整合する必要がある。
- 供給責任及び、その説明責任を果たせる対策を行うためには、**リスク評価を行った上で、その結果を踏まえた適切な対策の検討・設計・実装を行う必要がある。**
- 本ガイドラインは、**工場のセキュリティ対策を進めるための一般的なプロセスにおいて、リスクベースのサイバーセキュリティフレームワーク（CPSF*1、NIST CSF2.0 *2）を活用したリスク分析、及び具体的な対策を検討する際などに活用することが想定される。**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

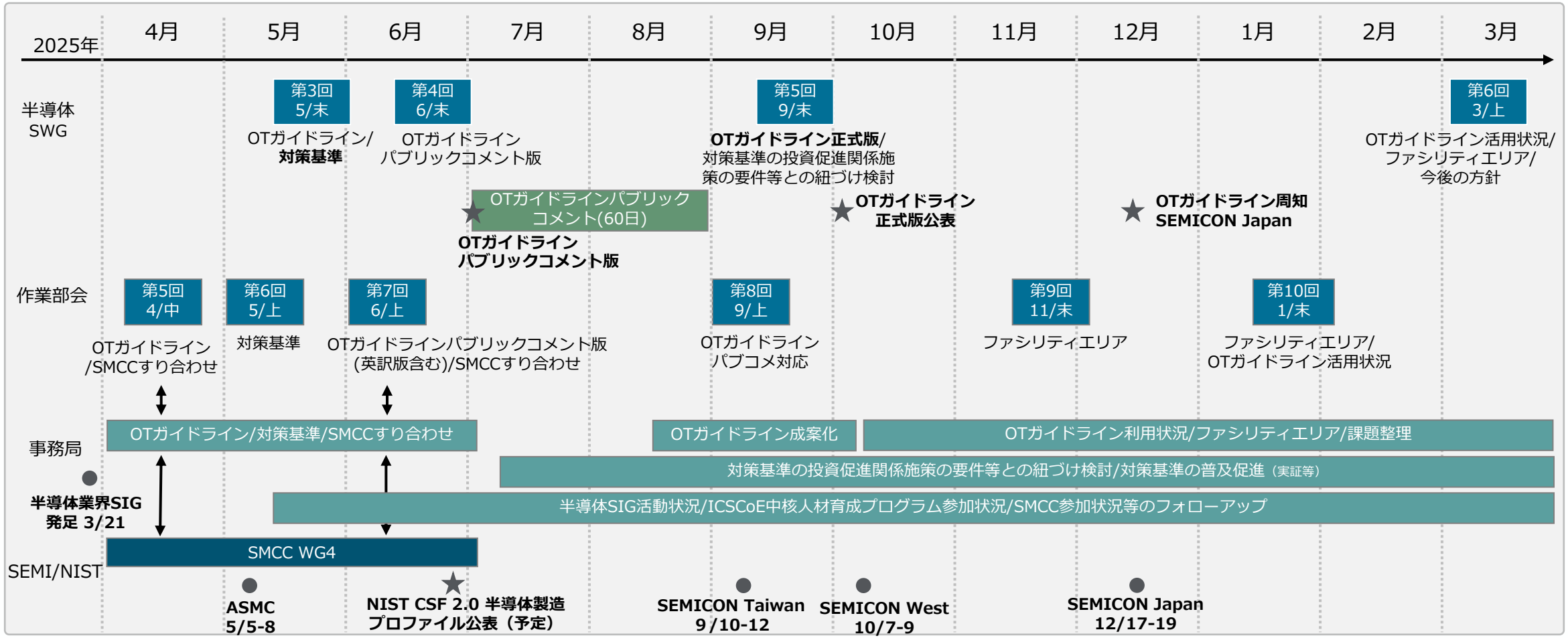
- 第2章：IEC62443のPurdueモデルを活用し半導体デバイス工場を領域・エリアに分割し、各エリアにおける CPSFの6つの構成要素を洗い出した。
- 第3章：前述CPSFの6つの構成要素に関連する半導体デバイス工場における特徴を整理し、 CPSFを活用しこれら特徴に起因するリスク源の洗い出し、及びNIST CSF2.0半導体製造プロファイルとの紐づけを行った。
- 第4章：マイクロセグメンテーション等、半導体デバイス工場において特に重要となる取組に関しては、より詳細な対策方法の例を示した。



Ⅵ．今後の予定

スケジュール（案）

- OTガイドラインについては作成を継続し10月頃公表予定
- ７月上旬頃から60日間のパブリックコメントを予定（英訳版も作成）



Ⅶ. ご議論いただきたい点

ご議論いただきたい点

1. 半導体デバイス工場におけるOTガイドラインの内容に関して、ご意見をいただきたい。

2. OTガイドラインの普及と実効性を高めるための取組についてアイディアをいただきたい。

3. 半導体産業におけるセキュリティ対策基準の作成にあたり、選定すべきOT項目についてご意見をいただきたい。

4. セキュリティ対策基準の普及に向けた取組についてご意見をいただきたい。

Ⅷ. 半導体政策関連（参考）

半導体関連産業におけるセキュリティの確保に向けた検討の開始

参考

- 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、**安定的な供給を確保する観点からも、サイバーセキュリティ対策を進めることが重要**。
- 2024年11月、産業サイバーセキュリティ研究会の下に半導体産業SWGを設置。デバイスメーカーや製造装置メーカーを含めた様々な企業・団体等が参加し、**我が国の半導体産業におけるサイバーセキュリティのあり方や守るべき対象技術などを議論する**とともに、**サイバーセキュリティ対策への取組、問題意識や事例等、相互に情報共有を行う**。
- こうした議論の中で、国際的な枠組みとの整合も念頭に置きつつ、**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。

半導体セキュリティの直近の動向

海外の動向

- TSMCは、2018年に主力工場がランサムウェアの被害に遭い生産停止を余儀なくされ、影響額は最大190億円に及んだ。
- 2023年に半導体装置のセキュリティ規格であるSEMI E187を調達要件化。SEMI E187の要件を満たしていることを、認証機関によって証明されたサプライヤーも出現。

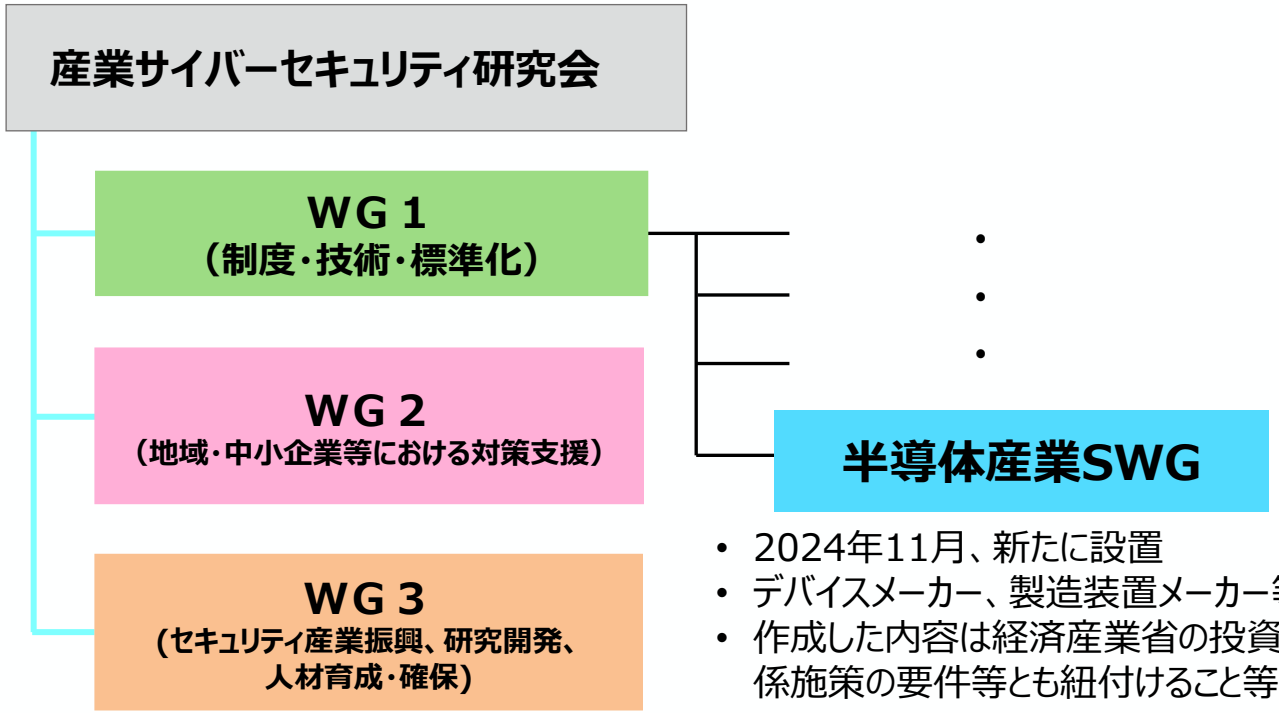
出所：日本経済新聞、TSMC社プレスリリース

国内の動向

- 半導体向けの研磨材を扱うフジミインコーポレーテッドは、サーバへの不正アクセスがあったことから公式Webサイトを含む社内システムを全面停止し、一部製品の生産と出荷を見合わせた。
- シリコンウェハを扱うグローバルウェーハズ・ジャパンは、社内サーバーに不正アクセスを受けたことから、ネットワークから社内システムを切り離す措置を実施し、シリコンウェハの製造および出荷が不能となった。

出所：フジミインコーポレーテッド社プレスリリース、グローバルウェーハズ・ジャパン社プレスリリース

国内の安定供給確保のためサイバーセキュリティ対策を進めていく



- 2024年11月、新たに設置
- デバイスメーカー、製造装置メーカー等が参加。
- 作成した内容は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。

経済産業省　半導体関係補正予算事業

参考

令和３年度補正予算　7,740億円

◆先端半導体基金：6,170億円
◆半導体生産設備刷新補助金：470億円
◆ポスト５Ｇ基金：1,100億円

令和４年度補正予算　1兆3,036億円

◆先端半導体基金：4,500億円
◆経済安全保障基金：3,686億円
◆ポスト５Ｇ基金：4,850億円

令和５年度補正予算　1兆9,867億円

◆先端半導体基金：7,652億円　※既存基金残金含む
◆経済安全保障基金：5,754億円
◆ポスト５Ｇ基金等：6,461億円

AI・半導体関係　令和６年度補正予算の概要

参考

AI･半導体関係の予算は、既存基金の活用とあわせて計1.6兆円。

＜補正予算案に計上されている主要予算＞

◆ ポスト５Ｇ情報通信システム基盤強化研究開発事業等（AI･半導体関係）【9,916億円】

先端半導体等の設計・製造技術や、ロボティクス分野の生成AIに関する基盤モデル等の開発、実証に取り組む。

◆ 先端半導体の国内生産拠点の確保【4,714億円】

産業基盤の強靭化や戦略的自律性・不可欠性の向上の観点から、先端半導体の国内生産拠点整備を支援し、事業者による投資判断を促すことで、安定供給の確保等を目指す。

※2030年度までの７年間で10兆円以上の公的支援を行う「ＡＩ・半導体産業基盤強化フレーム」を創設。

情報処理の促進に関する法律及び特別会計に関する法律の一部を改正する法律案の概要

参考

背景・法律案の概要

- ✓ **生成AIの利活用の急速な拡大**に伴い、**電子計算機に求められる計算量は大幅に増加**していることから、今後情報処理の更なる促進を図るためには、**先端的な半導体の確保**、生成AIの**計算需要を十分に満たせるだけのサーバーの導入等**を併せて進める必要がある。
- ✓ また、**半導体・AIの成長需要を取り込み、各産業の国際競争力の強化につなげていく**ため、**半導体・AI分野の公的支援**に係る**民間事業者の予見可能性を高め大規模な官民投資を誘発**していく必要がある。
- ✓ こうした背景を踏まえ、**情報処理の高度化を推進するための環境の整備を図る**ため、
  （１）指定高速情報処理用半導体※１の生産を安定的に行うために必要な取組の支援、
  （２）高度な情報処理の性能を有する設備の導入※２の支援、
  （３）デジタル人材の育成、
  （４）（１）～（３）の**措置に係る独立行政法人情報処理推進機構（IPA）の業務の追加**、
  （５）半導体・AI施策に係る必要な財源を確保するための新たな公債※３の発行・償還等に関する措置を**情報処理の促進に関する法律**（情促法）において定め、**（５）に係る経理を明確にするための新たな勘定の創設等の措置**について**特別会計に関する法律**（特会法）において定める。

※１　我が国において生産及び供給が安定的に行われていない、極めて大量の情報を極めて高速度で処理することを可能とする半導体であって、情報処理の高度化のために特に必要なもの

※２　大規模なサーバーや冷却設備等の導入

※３　半導体の性能の向上等の措置等に充てるために必要な財源を確保するためのつなぎ国債

指定高速情報処理用半導体に関する支援【情促法】

① 支援対象（公募により選定）

- 経済産業大臣が指定した**指定高速情報処理用半導体の生産を安定的に行うために必要な取組**を**最も適切に実施することができる者**

② IPAへの追加業務

- 当該取組※に必要な**資金の出資**若しくは**施設・設備の現物出資**、**当該資金に係る社債又は借入れに係る債務の保証**等

※　生産施設の設置、需要の開拓等

高度な情報処理の性能を有する設備に関する支援【情促法】

① 支援対象

- **高度な情報処理の性能を有する設備の導入**を行おうとする**情報処理サービス業を営む会社**

② IPAへの追加業務

- **高度な情報処理の性能を有する設備の導入**に必要な資金に係る社債又は借入れに係る**債務の保証**

デジタル人材の育成【情促法】

○ IPAへの追加業務

- デジタル人材の養成や、その資質の向上に係る業務を追加する。

必要な財源の確保【情促法・特会法】

- **「AI・半導体産業基盤強化フレーム」**として、**2030年度**までに合計**10兆円以上の半導体・AI分野への公的支援（補助・委託等：６兆円程度、金融支援：４兆円以上）**を行うところ、こうした支援には一度に多額の資金が必要と想定されることから、**エネルギー対策特別会計**の負担において、**公債を発行**できることとする。
- ①新たな公債の償還及び半導体・AI施策に要する費用の財源に充てるため、**財政投融資特別会計の投資勘定から新たな勘定へ繰り入れることができる**旨、
  ②半導体・AI施策に要する費用の財源に充てるため、**エネルギー対策特別会計のエネルギー需給勘定から新たな勘定へ繰り入れることができる**旨及び
  ③半導体・AI施策に要する費用の財源に充てるため、**一般会計（経済産業省が所管する基金からの国庫返納金）から新たな勘定へ繰り入れることができる**旨
  を規定する。
- 上記に係る経理を明確にするため、**エネルギー対策特別会計に新たな勘定及び対策を設置し、歳入歳出項目等を規定**する。

METI

Ministry of Economy, Trade and Industry