経済産業省

資料5

事務局説明資料

「半導体デバイスにおけるOTセキュリティガイドライン（案）」に対するパブリックコメントへの対応について

2025年10月2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3回SWG振り返り

Ⅱ．OTセキュリティガイドライン（案）に関するパブリックコメント

Ⅲ．御議論いただきたい点

Ⅰ．第3回SWG振り返り

第3回SWG開催概要

日時　　：2025年6月19日（木）10:30-12:30

アジェンダ：ローム様講演

日本電子様講演

事務局説明

Ⅰ. 第2回SWG振返り

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

OTセキュリティガイドラインについて

セキュリティ対策基準について

第3回SWGの御意見取りまとめ（1/2）

項目	委員の御意見	SWGでの対応	OTガイドライン（案）での対応
OTセキュリティガイドラインについて	① 業界団体で説明会を開催しOTセキュリティガイドラインの周知をしていく必要があると考えており、どのように説明していくべきか	• 概要資料を用いて説明する予定である。複数の業界団体に対してまとめて説明会を実施する、説明を録画し配布する等も検討する	―
	② 英語版のOTセキュリティガイドラインの対象読者はどのような方々であるか	• 主な対象読者は、海外の主要な半導体関連事業者や業界団体である。国内半導体関連事業者はグローバルでビジネスを実施していることが多く、OTセキュリティガイドラインのグローバルでの認知度を向上させることを目的としている	―
	③ 英訳版ガイドラインについて、1.1の最初二つのパラグラフ及び1.2の想定読者については、記載内容が日本に偏りすぎているため修正した方がよいのではないか	―	• 第1.1節の「半導体産業の発展と国内投資の促進」等の日本に偏った内容を、英語版OTセキュリティガイドライン（案）から削除させていただく
	④ リファレンスアーキテクチャ―のクラウドAI分析サービスとの記載について、生成AIなど取扱いが難しいものもある。AIと書かない方がよいのではないか。	―	• 生成AIの活用との誤解を招く可能性があるため、御指摘のとおり修正させていただく

第3回SWGの御意見取りまとめ（2/2）

項目	委員の御意見	SWGでの対応	セキュリティ対策基準での対応
セキュリティ対策基準について	⑤ セキュリティ対策基準のタイムラインはどのように考えているか	ー	• IT基準は検討中の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から抽出しており、同評価制度の正式な運用開始は来年度になる予定のため、セキュリティ対策基準もそれに整合したタイムラインとなることを想定している
	⑥投資関連施策との紐づけとはどのようなイメージで考えているか	ー	• 安全保障の補助金など特定の半導体企業の皆様に対して様々な支援策を用意させていただいているが、その中でセキュリティ対策基準に準拠していただくことを考えている
	⑦ 項目内容によっては行うことが難しいものもあるという印象を受けた。例えば、4-4の「不要サービスを無効化すること」という項目は、OT資産全てに対して不要かどうかを判断して無効化するのはかなり難しいと思う	ー	• 評価基準（案）はITとOTに分けている。OT資産に対して不要サービスを無効化することまでを求めることは想定していない

Ⅱ．OTセキュリティガイドライン（案）に関するパブリックコメント

パブリックコメントの実施概要・主な御意見

- 「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（案）」について、パブリックコメントを実施し、日本語版・英語版合わせて、71件の御意見を受領。
- 頂いた御意見を踏まえ、記載内容の補足や具体化、誤解を招く可能性がある表現の修正等の観点から記載の内容の修正を行った。

実施期間	2025年6月27日（金）～2025年8月26日（火）
意見数	71件（14者）
頂いた御意見のカテゴリ	①脅威・脆弱性・リスクの表記について ②無線デバイスについて ③装置ツールの調達と導入について ④ローカル・リモートアクセスについて ⑤装置のデータ保全について ⑥外部サービス通信について ⑦エッジ対策について ⑧ガバナンスについて ⑨OTセキュリティ人材の育成について ⑩法規制・国際標準への対応について ⑪生産機密情報の保護について ⑫装置ツールの管理と脆弱性評価について ⑬セグメンテーション手法について ⑭IT/OT領域の横断的監視について ⑮物理アクセス制限について

パブリックコメントで頂いた主な御意見に対する考え方（1/3）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方
①脅威・脆弱性・リスクの表記について	第3.2節 第3.3節	• 脅威・脆弱性・リスクを取り違えたような記述が散見される【No.41】	• 全体的に記載を見直し、想定されるセキュリティインシデント・脅威・脆弱性に分けて修正
②無線デバイスについて	第3.2.1節 ②-3	• 電波妨害や不正無線デバイス対策にRF監視やWIDSの活用が不可欠であることを記載すべき【No.28】	• ファブエリア内の無線に対する対応について追記
③装置ツールの調達と導入について	第3.2.1節 ③	• FW設置やNW分離等が購買仕様書に明記されず、情報も未開示のため記載すべき【No.54】	• 調達において、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の確認の必要性を追記
④ローカル・リモートアクセスについて	第3.2.1節 ⑥ 第3.2.3節 ②	• デバイスメーカーによるアクセス監視、セキュアなリモートアクセスのプロセスについて記載すべき【No.57】	• アカウント管理でのデバイスメーカーによるアクセス監視について追記 • 遠隔診断サービスのソリューションとプロセスの導入について追記
⑤装置のデータ保全について	第3.2.2節 ③	• データ保全として、製造装置内にあるデータ（構成情報、校正値、セキュリティログ等）のバックアップについて記載すべき【No.13】	• 製造装置内にあるデータのバックアップについて追記

パブリックコメントで頂いた主な御意見に対する考え方（2/3）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方
⑥外部サービス通信について	第3.2.3節②	• 持ち込み制限の実効性確保のために、不正無線デバイスの継続的監視の必要性を記載すべき【No.25】 • クラウド分析サービスとリモート診断機能の統合し、ゼロトラストフレームワークの活用について記載すべき【No.37】	• 外部サービスとの通信での継続的なセキュリティ監視の必要性を追記 • 外部サービス（遠隔診断サービス利用）では、「IT領域で行われるリモートアクセス対策」を実施する必要性を追記
⑦エッジ対策について	第3.2.3節③	• エッジ環境のセキュリティとネットワーク分離の検証を要件として記載すべき【No.33】	• 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おいて、定期的な監査と継続的な見直しの必要性を追記
⑧ガバナンスについて	第3.3節①	• 経営層のコミットメントと組織文化の醸成について記載すべき【No.6】	• 経営層のコミットメント確保の必要性を追記
⑨OTセキュリティ人材の育成について	第3.3節① 第3.3節⑦	• 製造プロセスを理解したOTセキュリティ専門家を育成し、インシデント対応能力の向上について記載すべき【No.6】 • 現場力強化と属人化の防止のために、Tabletop演習やスキルマップ整備を記載すべき【No.8】	• 半導体製造プロセスを理解した人材を育成し、インシデント対応能力向上の必要性を追記 • スキルマップを整理するによる継続的な現場力強化と属人化の防止について追記
⑩法規制・国際標準への対応について	第3.3節②	• 国内外の法規制・国際標準の動向を監視し、ガイドラインや対策へ柔軟な適応について記載すべき【No.6】	• 国内外の法規制や国際標準の動向を継続的に確認し、組織内のルールを策定・運用する必要性を追記

パブリックコメントで頂いた主な御意見に対する考え方（3/3）

頂いた御意見のカテゴリ	該当箇所	頂いた主な御意見	御意見への対応の考え方
⑪生産機密情報の保護について	第3.3節④	• 内部不正対策として、既存基盤への振る舞い分析の統合による効率化を記載すべき【No.17】	• 生産機密情報の保護として、保護プロセスを設けて監視・監査を行う運用の必要性を追記
⑫装置ツールの管理と脆弱性評価について	第4.1節	• 製造環境におけるデバイス発見と継続的構成管理について記載すべき【No.34】 • コンプライアンスについてSEMI E187を参照し、SCAPに代わる脆弱性管理手法の推奨も記載すべき【No.62】 • SMCC WG5は既に解散している可能性があり、記載を見直すべき【No.63】 • 環境変化に応じてリスクアセスメントを動的に実施し、対策の最適化について記載すべき【No.6】	• 装置ツールに対する、継続的な構成管理の見直しの必要性を追記 • 『SEMI E187 COMPLIANCE GUIDANCE』による脆弱性スキャナーの推奨を追記 • 業界向け脅威情報収集方法として記載していたSMCC WG5は既に解散しているため、記載から削除 • 新たな脅威や環境変化に応じて、既存資産と脆弱性の評価を動的に見直し、最新のリスク状況に基づいた対応判断が求められることを追記
⑬セグメンテーション手法について	第4.2節	• VLANなど設定変更なくセグメンテーションする手法と、OTプロトコル可視化の重要性を記載すべき【No.18】	• VLANに関する記述を追記
⑭IT/OT領域の横断的監視について	第4.3節	• IT/OT統合SOCによる横断的な監視を記載すべき【No.16】	• ネットワーク経由の侵入に対して、横断的な監視・分析が有効であることを追記
⑮物理アクセス制限について	第4.4節	• 不正無線デバイス対策として、無線侵入検知システムによる継続的監視を記載すべき【No.24】	• 装置ツールへの不正デバイス接続について追記

（参考）意見の概要と新旧の対照（1/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
①脅威・脆弱性・リスクの表記について	42	脅威・脆弱性・リスクを取り違えたような記述が散見される	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 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 ※修正箇所多数のため、第3.2.1節①のみ記載	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ることで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IoT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

（参考）意見の概要と新旧の対照（2/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
②無線デバイスについて	28	電波妨害や不正無線デバイス対策にRF監視やWIDSの活用が不可欠であることを記載すべき	＜記載なし＞	• 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。
③装置ツールの調達と導入について	54	FW設置やNW分離等が購買仕様書に明記されず、情報も未開示のため記載すべき	• 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、ファイア・ウォールの実装有無、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。	• 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。

（参考）意見の概要と新旧の対照（3/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
④ローカル・リモートアクセスについて	57	デバイスメーカーによるアクセス監視、セキュアなリモートアクセスのプロセスについて記載すべき	• 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）を適切な承認プロセスや監査プロセスを導入することを含む。 • 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、なりすましの防止を含めた管理や生産機密情報の漏洩対策を確認する必要がある。 • 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行う必要がある。	• 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。 • 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。 • 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。

（参考）意見の概要と新旧の対照（4/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
⑤装置のデータ保全について	13	データ保全として、製造装置内にあるデータ（構成情報、校正値、セキュリティログ等）のバックアップについて記載すべき	＜記載なし＞	• 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。
⑥外部サービス通信について	25	持ち込み制限の実効性確保のために、不正無線デバイスの継続的監視の必要性を記載すべき	• リモートからのネットワーク接続は、インターネット網を通じたVPN接続だけではなく、携帯電話通信網を通じた接続（モバイルルーター）等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。	• 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。
	37	クラウド分析サービスとリモート診断機能の統合し、ゼロトラストフレームワークの活用について記載すべき	【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	【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
⑦エッジ対策について	33	エッジ環境のセキュリティとネットワーク分離の検証を要件として記載すべき	• 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う必要がある。	• 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。

（参考）意見の概要と新旧の対照（5/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
⑧ガバナンスについて	6	経営層のコミットメントと組織文化の醸成について記載すべき	＜記載なし＞	• 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。
⑨OTセキュリティ人材の育成について	6	製造プロセスを理解したOTセキュリティ専門家を育成し、インシデント対応能力の向上について記載すべき	＜記載なし＞	• 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。 • 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俗人化の防止が可能となる。
	8	現場力強化と属人化の防止のために、Tabletop演習やスキルマップ整備を記載すべき		
⑩法規制・国際標準への対応について	6	国内外の法規制・国際標準の動向を監視し、ガイドラインや対策へ柔軟な適応について記載すべき	• 遵守すべき法制度に準拠した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。	• 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。
⑪生産機密情報の保護について	17	内部不正対策として、既存基盤への振る舞い分析の統合による効率化を記載すべき	• 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等になるため、工場内の入室者許可制限や撮影規制の実施、装置ツールの保守・入替時における機密データ保護や撤去時の完全消去が必要である。	• 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。

（参考）意見の概要と新旧の対照（6/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
⑫装置ツールの管理と脆弱性評価について	34	製造環境におけるデバイス発見と継続的構成管理について記載すべき	• 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、それに応じた構成管理の変更を実施する必要がある。	• 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。
	62	コンプライアンスについてSEMI E187を参照し、SCAPに代わる脆弱性管理手法の推奨も記載すべき	• また、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 E188』の「9.4 NIST Security Content Automation Protocol (SCAP)」）	• また、SEMI E187 COMPLIANCE GUIDANCE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)」）
	63	SMCC WG5は既に解散している可能性があり、記載を見直すべき	• 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 • 2024年1月から始まったSEMI SMCC-WG5においても、業界向けの脅威情報の収集対応について検討が進んでおり、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、活動を開始した状況である。	• 業界の脅威情報共有であるIT-ISAC Semiconductor Industry SIG 、J-CSIP半導体産業SIGからの情報収集 • 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。
	6	環境変化に応じてリスクアセスメントを動的に実施し、対策の最適化について記載すべき	＜記載なし＞	• 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。

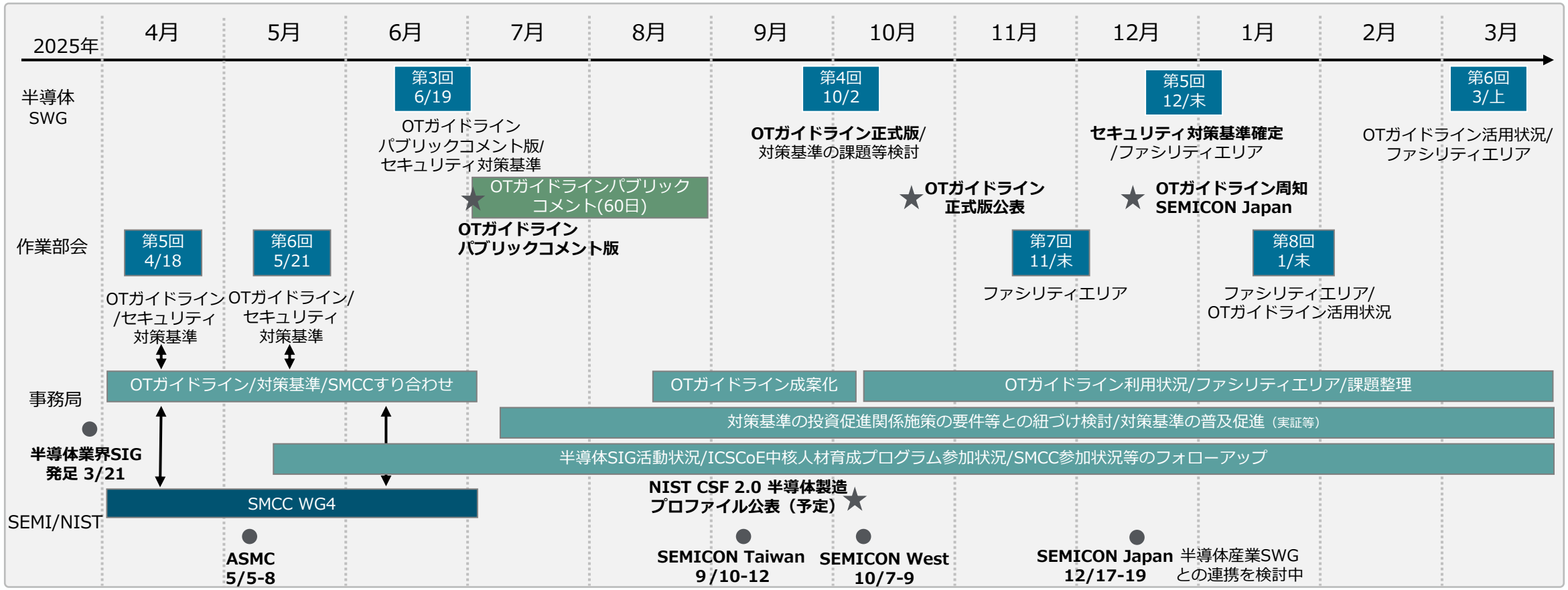
（参考）意見の概要と新旧の対照（7/7）

カテゴリ	No.	意見の概要	修正箇所	
			旧	新
⑬セグメンテーション手法について	18	VLANなど設定変更なくセグメンテーションする手法と、OTプロトコル可視化の重要性を記載すべき	• その際、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。	• 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。
⑭IT/OT領域の横断的監視について	16	IT/OT統合SOCによる横断的な監視を記載すべき	＜記載なし＞	• 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。
⑮物理アクセス制限について	24	不正無線デバイス対策として、無線侵入検知システムによる継続的監視を記載すべき	• 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必要がある。 • 表4-6 不正媒体の装置ツール接続	• 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。 • 表4-6 装置ツールへの不正デバイス接続

Ⅲ．御議論いただきたい点

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、10月中旬ごろ公表予定
- 次回、セキュリティ対策基準（デバイスメーカー部分）を確定予定。また、ファシリティエリアの論点整理について、議論予定



御議論いただきたい点

●半導体産業におけるセキュリティ対策基準（案）について（参考資料５－６参照）

1. 我が国の重要技術を守るために、必要十分な範囲はどのようなものか。
2. 様々なプレイヤー（デバイスメーカー、装置メーカー）が存在する中、各プレイヤーにとって過度な要求になっていないか。

– デバイスメーカーについて。大企業と中小企業に対して異なる基準を設ける等の必要性はあるか。ある場合、どのように分けるのがよいか。

– 装置メーカーにとって、デバイスメーカーと同じOT・IT基準を求められた場合、過度な要求になっていないか。

３．各プレイヤー（デバイスメーカー、装置メーカー）にとって、活用しやすいものになっているか。

– 例えば、自社が基準を満たしているか否かを明瞭に判断することはできるか。

半導体産業におけるセキュリティ対策基準の対象範囲（案）

半導体産業における
セキュリティ対策基準（案）

セキュリティガバナンス

対象システム
IT基盤・外部NW境界

対象システム
製造環境等の制御（OT）システム

半導体産業 メーカー種別	IT項目要求事項	OT項目要求事項
デバイスメーカー	**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★４取得※**	**６項目**
装置メーカー	今回議論	今回議論
部素材メーカー	今後検討	今後検討

※★４取得について同制度を開始してからとする。それまでの間は★４の一部項目に相当する旨についての自主宣言等が適当か。

METI

Ministry of Economy, Trade and Industry