提出No.	No.	提出者	提出意見	御意見に対する考え方
1	1	匿名	1．以下の用語の定義についても解説をお願いしたい。 (1) サイバーセキュリティ (2) インシデント	頂いた御意見を参考に、追記いたします。 修正箇所：Appendix B（P.101、P103）
1	2	匿名	2．ガイドラインの整理 個別分野ごとに部分的に重複するサイバーセキュリティに関するガイドラインを個別に出すのではなく、例えば政府統一基準のガイドラインをベースに、個別の分野に必要な対策を追加で上乗せするなどガイドラインの体系を整理するべきではないか。「重要インフラのサイバーセキュリティに係る安全基準等策定指針」を含め、類似するガイドラインが乱立しており、不合理であると感じる。	類似ガイドラインの乱立は避けるべきという指摘は今後の検討の参考とさせていただきます。他方、半導体工場のOTセキュリティについては、指摘されているような政府や重要インフラ向けのガイドラインでもカバーされておらず、半導体工場の特殊性から考慮すべき観点が異なるため、本ガイドライン（案）の作成は必要と考えており、頂いた御意見については、原案の通りとさせていただきます。
2	3	匿名	半導体産業が我が国の経済成長と安全保障の基盤であり、サイバー攻撃からそのOT（Operational Technology）環境を守ることが極めて重要であるとの認識のもと、本ガイドラインが策定されたことに深く敬意を表します。 本ガイドラインは、国家の経済安全保障に直結する半導体サプライチェーンの強靭化を目指すものと理解しており、この極めて重要な視点に鑑み、さらなる強化策として、特に「サプライチェーンの信頼性確保と国際連携の原則」、そして「継続的なセキュリティ強化と適応」について、以下の観点からの明記と施策強化を提案いたします。	本ガイドライン（案）に対する肯定的な御意見として承ります。
2	4	匿名	1. サプライチェーンにおける外国資本への依存度低減と信頼性原則の明確化 本ガイドラインが対象とする半導体デバイス工場は、多数の製造装置、素材、システム、サービスによって構成される複雑なサプライチェーンの上に成り立っています。このサプライチェーンにおける潜在的なリスクとして、特定の外国資本への過度な依存が挙げられます。サイバーセキュリティの観点からは、悪意のあるバックドアの仕込み、サプライチェーン攻撃による機密情報の窃取、あるいは有事の際の供給停止リスクなどが懸念されます。 したがって、ガイドラインにおいて、以下の点を追記・強化することを提案します。 ・重要機器・サービスの調達における信頼性基準の明記： ファブ内の重要製造装置、制御システム、基幹ソフトウェア、およびそれらの保守サービスを提供するベンダー選定において、単なる技術的性能やコストだけでなく、サプライヤー企業の資本構成、技術開発体制、過去のセキュリティ実績、特定の外国政府からの影響度などの「信頼性」を評価する基準を設けることを推奨します。 ・リスクの高いサプライヤーへの依存度低減策の推進： 特定の国や地域に偏ったサプライヤー構成を見直し、国内または信頼できる同盟国からの調達比率を高めるための具体的な指針やインセンティブ制度の検討を促すべきです。また、重要なコンポーネントの複数ベンダー化（マルチソース化）や代替手段の確保を促す記述を追加すべきです。 ・サプライヤーへのセキュリティ監査の強化： 既存のサプライヤーに対しても、ガイドラインで示されるセキュリティ基準への準拠状況を定期的に監査する仕組みを強化し、脆弱性管理やインシデント対応能力の向上を義務付ける条項を設けることを検討すべきです。	・重要機器・サービスの調達における信頼性基準の明記 本ガイドライン（案）においては、重要機器の調達におけるグローバル標準のE187の準拠を推奨しています。半導体産業においては、国際スタンダードにアラインすることが重要であり、そのようなポリシーの基、本ガイドライン（案）を作成しているため、頂いた御意見については、原案の通りとさせていただきます。 ・リスクの高いサプライヤーへの依存度低減策の推進、サプライヤーへのセキュリティ監査の強化 本ガイドライン（案）では第3章にてNIST CSF2.0 半導体製造プロファイルの該当箇所との紐づけがされており、サプライヤー構成についてはGV.SC-02、サプライヤーへのセキュリティ監査の強化についてはGV.SC-05、GV.SC-06、GV.SC-07等に記載されているため、頂いた御意見については、原案の通りとさせていただきます。
2	5	匿名	2. 同盟国・友好国との連携強化によるサイバーセキュリティ協力の深化 半導体産業におけるサイバー脅威は国境を越えるため、国際的な連携は不可欠です。本ガイドラインでも国際規格との整合性が述べられていますが、さらに踏み込んで、特に「安全保障上の信頼関係に基づいた同盟国・友好国」との連携を強化する視点を加えるべきです。 具体的には、以下の連携強化策を提案します。 ・情報共有体制の構築： 半導体産業を狙うサイバー攻撃に関する脅威インテリジェンスを、同盟国・友好国の関連機関や企業とタイムリーに共有する枠組みを構築・強化することを促します。これにより、攻撃の予兆や最新の手口を早期に把握し、共同で防御策を講じることが可能になります。 ・共同演習・訓練の実施： 国際的なサイバーセキュリティ共同演習や訓練に積極的に参加・主催し、有事の際の連携体制を確認・強化します。これにより、実戦的な対応能力を高めることができます。 ・技術協力と標準化への貢献： 半導体OTセキュリティに関する技術開発や、国際的な標準策定プロセスにおいて、同盟国・友好国と連携し、我が国が主導的な役割を果たすことを目指す記述を加えるべきです。	国際連携の重要性はご指摘の通りで、今後の施策の参考とさせていただきます。他方、国際連携は本ガイドライン（案）のスコープを超えるため、頂いた御意見については、原案の通りとさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
2	6	匿名	3. 継続的なセキュリティ強化と適応 本ガイドラインで示された対策に加え、変化し続ける脅威環境に対応し、半導体OTセキュリティを継続的に強化し適応させていくための以下の視点を追記することを提案します。 リスクベースアプローチの深化と継続的な最適化： ・脅威インテリジェンスの活用強化： 最新のサイバー攻撃手法、攻撃者の動機、ターゲットとなる脆弱性に関する情報を継続的に収集・分析する仕組みを強化し、予測的な防御策を講じることが可能にする。 ・リスクアセスメントの定期的・動的な実施： 新たな脅威や環境変化（例：新しい装置の導入、サプライヤーの変更）に合わせて、既存の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策の優先順位付けと最適化を図る。 高度な技術的対策の導入と適応： ・ゼロトラストモデルの導入推進： ネットワーク内部の信頼を前提とせず、全てのアクセス要求を検証するゼロトラストの概念をOT環境にも適用を推進する。特にファブエリアのような高セキュリティを要する環境では、このアプローチが効果的である。 ・AI/機械学習を活用した異常検知： 膨大なOTデータの監視において、AIや機械学習を活用することで、従来のルールベースでは見つけにくい異常や潜在的な脅威を早期に検知する能力を強化する。 ・サイバーレジリエンスの強化（回復力の向上）： 攻撃を受けた際に、システムがダウンしても事業を継続できるような回復力（レジリエンス）の向上に焦点を当てる。これには、堅牢なバックアップ・リカバリー計画、代替システムの準備、オフラインでの運用継続能力などが含まれる。 人材育成と組織文化の醸成： ・OTセキュリティ専門人材の育成： ITセキュリティの専門知識に加え、半導体製造プロセスの深い理解を持つOTセキュリティ専門家を育成・確保する。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向上させる。 ・経営層のコミットメントと組織文化の浸透： セキュリティ対策が単なる技術的課題ではなく、経営戦略の一部として位置づけられるよう、経営層の強いコミットメントを確保する。従業員一人ひとりがセキュリティ意識を持ち、ガイドラインに基づいた行動を実践する文化を醸成するための継続的な啓発活動を強化する。 ・法規制・国際標準への継続的な追随： 半導体産業のセキュリティに関する国内外の法規制や国際標準は常に変化している。これらの動向を継続的に監視し、ガイドラインや自社の対策を適応させる柔軟性を持つことが重要である。	リスクベースアプローチの深化と継続的な最適化： ・脅威インテリジェンスの活用強化 最新の脅威情報収集及び対策の必要性とその情報収集方法については第4.1.4節に記載しているため、頂いた御意見については、原案の通りとさせていただきます。 ・リスクアセスメントの定期的・動的な実施 頂いた御意見を参考に、修正いたします。 修正箇所：第4章 4.1.5（P.64） 高度な技術的対策の導入と適応： ・ゼロトラストモデルの導入推進 頂いた御意見については、今後の検討の参考とさせていただきます。 ・AI/機械学習を活用した異常検知 早期の異常検知の必要性については第 3.2.1節 ②に記載しているため、頂いた御意見については、原案の通りとさせていただきます。 ・サイバーレジリエンスの強化（回復力の向上） 早期復旧のためのバックアップ等の必要性については第 3.2.2節 ②に記載しているため、頂いた御意見については、原案の通りとさせていただきます。 人材育成と組織文化の醸成： ・OTセキュリティ専門人材の育成 頂いた御意見を参考に、修正いたします。 修正箇所：第3章 3.3 1①、⑦（P.51 表3-10「特徴及び考慮すべき観点」） ・経営層のコミットメントと組織文化の浸透 頂いた御意見を参考に、修正いたします。 修正箇所：第3章 3.3 ①（P.45 表3-10「特徴及び考慮すべき観点」） ・法規制・国際標準への継続的な追随 頂いた御意見を参考に、修正いたします。 ・法規制・国際標準への継続的な追随 頂いた御意見を参考に、修正いたします。 修正箇所：第3章 3.3 ②（P.45-46 表3-10「特徴及び考慮すべき観点」）
3	7	企業	（1）㊒語版ガイドラインの恒常的な位置付けの明記（第1.6節への追記） 外資系装置ベンダーとの信頼構築やセキュリティ要件共有の観点から、「英語版の継続的公開と同時更新」を制度上明記いただきたく提案いたします。 【理由】 本ガイドライン案には英語版が付属していますが、将来的な更新においても「英語版の継続的な公開・同時更新」が制度設計上、明記されることで、日本のサプライチェーンに関与する外資系装置メーカーや海外ベンダーとの信頼関係構築がより円滑になります。これは、製造現場における“設備導入時のセキュリティ要件共有”を支援し、国際標準と連動する日本の対策の可視化に寄与するものです。英語版の恒常的な位置付けは、「利活用（1.6）」の深化と整合する施策と考えます。	本ガイドライン（案）は各社がセキュリティ対策の検討をする際の参考資料であり、その頒布形態や更新タイミングについて本文中で規定することは趣旨と異なるため、頂いた御意見については、原案の通りとさせていただきます。
3	8	企業	（2）人材・訓練・ベンダー連携の成熟指標導入（第3.3節の補完） Tabletop演習（年1回以上）やスキルマップ整備（ENISA ECSF、NIST NICE準拠）を明記することで、現場力強化と属人化の防止が期待されます。 【理由】 「3.3 組織・ヒト側面のリスク分析」では、組織体制や人材に関する説明がありますが、より実践的に工場現場の対応力を高めるためには、次のような項目の明記が有効です。 ①サプライヤーや保守業者との情報共有フローの確立 ②年1回以上の机上演習（Tabletop Exercise）の導入 ③OT/ITのハイブリッド人材像とスキルマップ（ENISA ECSFやNIST NICE Frameworkを参考） これらはすでにシンガポールCSA（The Cyber Security Agency of Singapore）やST Engineering等の先進事例において制度化されています。 ・参照：ENISA CSIRT Maturity Framework https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity ・参照：NIST NICE Framework　Workforce Framework for Cybersecurity https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf ・参照：The Singapore Cybersecurity Strategy 2021 https://www.csa.gov.sg/resources/publications/the-singapore-cybersecurity-strategy-2021 ・参照：TRUSTED INDUSTRIAL CYBERSECURITY SOLUTION https://www.stengg.com/getmedia/c97c148d-d51a-4fce-9202-c7b9f873e860/industrial-cybersecurity-solutions-brochure.pdf	頂いた御意見を踏まえ、追記いたします。 修正箇所：第3章 3.3 ⑦（P.51 表3-10「特徴及び考慮すべき観点」）

提出No.	No.	提出者	提出意見	御意見に対する考え方
3	9	企業	（3）FSIRTの成熟度評価手法導入（第4.3節の補完） ENISAのSIM3を活用し、FSIRTの運用水準を「見える化」することで、工場内での自己評価と改善活動が可能になります。ただし、FSIRTならではの取り組みとして、機能面で十分化を評価するというのではなく、文書化などによる成熟度評価になります。 【理由】 現行ガイドラインではFSIRTの役割や運用フロー（監視、対応、復旧）が記載されていますが、その能力・成熟度の「見える化」手法については記述がありません。 ENISA（欧州連合サイバーセキュリティ庁）がEU域内産業CSIRTに対して実施しているSIM3（Security Incident Management Maturity Model）を参考に、以下のような成熟度指標（例：対応の文書化レベル、訓練実施頻度、社内外連携体制の整備度）を導入することにより、工場内でのFSIRT能力の現状把握と改善ロードマップ策定が可能になります。但し、FSIRTならではの取り組みとして、機能面で十分化を評価するというのではなく、文書化などによる成熟度評価になります。 ●参照：ENISA CSIRT Maturity Framework https://www.enisa.europa.eu/topics/incident-response/csirt-capabilities/csirt-maturity ●参照：FIRST CSIRT Services Framework https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2-1 ●参照：SIM3 Model & References https://opencsirt.org/maturity/sim3/ ●参照：SIM3　v2 interim https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf これにより、現場対応力の属人化を防ぎ、PDCAサイクル型でのセキュリティ運用が促進されます。	FSIRTとCSIRTでは求めるスキルも異なり、また、FSIRTの成熟度モデルを提示することは時期尚早であると考えるため、頂いた御意見については、原案の通りとさせていただきます。
4	10	企業	1,「製造装置メーカー、素材メーカーが多数存在することから、そうした各社に求められる要件や対策も想定できるようなガイドライン」をとにかく早期に策定して頂くことを希望する。☒ 【理由】 製造装置をセキュアにするためには構成部品のセキュリティ対応も必要だが、部品メーカーの認識が十分に高まっていない。また、サプライチェーン全体を対象としたガイドラインは海外にも無いと思われるので、先駆けて作成できれば価値が高い。	頂いた御意見については、今後の検討における参考とさせていただきます。
4	11	企業	2,「半導体装置の安全化」とあるが、「セキュア化」の方が良くないか。 【理由】 「安全」だとsafetyとsecurityのどちらを指すかが分からないため。機械規則にサイバーセキュリティ要件が加わったため、同じ文脈でsafetyとsecurityの両方に言及する可能性も高くなっており、混同の可能性は避けたい。	頂いた御意見を参考に、修正いたします。 修正箇所：第1.2節 図1-1（P.2）
4	12	企業	3.「最も高度な攻撃者（下記1）を想定した対策レベルを実現する必要がある」に関し、製造装置が単体で目指すべきセキュリティレベルの目安を提示できないか。☒ 【理由】 EU CRAは要件の抽象度が高く、対応のレベルにはメーカーごとにかなりの幅が出る可能性がある。業界としての共通認識があれば、装置メーカーの対応レベルを揃えることができ、デバイスメーカー側の対策が行いやすかったり、双方のコストの最適化が図れたりするのではないか。	本ガイドライン（案）はデバイスメーカー向けであるため、頂いた御意見については、今後の検討における参考とさせていただきます。
4	13	企業	4. データ保全の観点として、製造装置内にあるデータ（構成情報、校正値、セキュリティログなど）のバックアップについて述べることはできないか。 【理由】 製造装置単体では、ランサムウェア被害を想定したバックアップのオフライン保管やWORMによる解決は難しい。また、ログの改ざんを防ぐ高度なセキュリティの実現にも難しさがある。何らかの指針があると、製造装置側の対応を考えやすい。	頂いた御意見を参考に、修正いたします。 修正箇所：第3.2.2節 ③（P.36 表3-6「特徴及び考慮すべき観点」）
4	14	企業	5.『ソフトウェア管理に向けたSBOM の導入に関する手引 ver2.0』の拡張として、多数のハードウェア部品から構成される製造装置のような大規模組み込み製品でのSBOMのガイドラインを作成できないか。 【理由】 ハードウェア部品のSBOMはそれぞれの製造者のノウハウを含むため、製造者が開示を望まないケースが多いと思われる。製造装置のような多数のハードウェア部品からなる製品において、SBOMをどのような範囲で収集し活用するか、ガイドラインがあるとデバイスメーカー／製造装置メーカー／部品メーカーで一貫した対応が進めやすくなる。	頂いた御意見については、今後の検討における参考とさせていただきます。
5	15	企業	経済産業省が策定された「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）」は、半導体産業のサプライチェーン全体を保護し、高度化・多様化するサイバー攻撃から日本の重要な産業を守るための、非常に重要な指針であると認識しております。特に、国際的な規格（NIST CSF 2.0、SEMI E187/E188等）との整合性を図りつつ、半導体工場の特性を踏まえた詳細なリスク分析や具体的な対策例を提示されている点は、現場でのセキュリティ対策を促進する上で大変有用です。 このガイドラインをさらに実効性の高いものとし、将来的な脅威にも対応可能な強固なセキュリティ体制を構築するため、以下の4点について追記・修正のご意見を提出いたします。	本ガイドライン（案）に対する肯定的な御意見として承ります。

提出No.	No.	提出者	提出意見	御意見に対する考え方
5	16	企業	1．IT/OT統合SOCによるセキュリティ対策の強化 ・本意見は、第1章「本ガイドライン作成の背景と目的」および第4章「半導体デバイス工場における具体的対策例」の運用（監視・対応・復旧・改善）に対するものです。半導体工場へのサイバー攻撃は、OT領域の脆弱性を直接狙うだけでなく、IT領域を経由してOT領域へ侵入するケースが多々あります。パロアルトネットワークスの調査によると、OT環境におけるインシデントの72%はIT環境が起点となって発生しています。(必要に応じて、エビデンスを提出致しますので私までコンタクトください。) ・現在のガイドラインではIT領域とOT領域を「分離し、通信を制御する」という記述が中心ですが、OTへの攻撃経路がIT側に大きく偏っている現状を踏まえ、ITとOTの双方を横断的に監視・分析し、インシデントの全体像（コンテキスト）を把握するためのIT/OT統合SOCの重要性を追記すべきです。 ・IT、OT、クラウド環境からのログやアラートを一元的に管理し、AIを活用した高度な脅威分析を行うことで、インシデントの早期発見と迅速な対応を可能にする統合SOCの導入を推奨します。	頂いた御意見を参考に、修正いたします。 修正箇所：第4.3節（P.72-73）
5	17	企業	2．OTセキュリティ対策における内部不正対策の明確化と統合運用の重要性 ・本意見は、第1章「半導体製造においてサイバー攻撃から守るべき対象」および第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」における生産機密情報の保護に関する記述に対するものです。ガイドラインの「半導体製造として守るべき対象」には、知的財産（生産機密情報）の保護が含まれています。しかし、その脅威として、外部からのサイバー攻撃だけでなく、内部関係者による不正な情報持ち出しも重要なリスクです。 ・特に半導体工場では、多数の従業員や外部の保守要員がファブエリアに出入りするため、物理的なセキュリティ対策だけでなく、論理的なアクセス制御やログの監視を組み合わせた、内部不正対策の具体的な指針を強化すべきです。 内部不正対策のためだけの個別ソリューションは、運用が煩雑になり、セキュリティチームの負担を増大させ、見落としや形骸化（shelfware化）のリスクを伴います。 ・したがって、サイバーセキュリティインシデントと同様に、内部不正の兆候を検知・分析するには、ネットワークやエンドポイントにおけるユーザーの振る舞いを常時監視し、不審な行動を可視化する振る舞い分析機能を、既存のサイバーセキュリティ対策ソリューションと連携または統合したプラットフォーム上で実現することが不可欠です。これにより、サイバー攻撃と内部不正の両方のコンテキストを統合的に把握し、より効率的かつ実効性の高い運用が可能となります。	頂いた御意見を参考に、修正いたします。 修正箇所：第3.3節④（P.48 表4-10「特徴及び考慮すべき観点」）
5	18	企業	3．IT/OT間の通信制御、セグメンテーションの実現方法の多様化とOTプロトコルの可視化の重要性 ・本意見は、第2章「半導体デバイス工場におけるリファレンスアーキテクチャ」および第4章「半導体デバイス工場における具体的対策例」における多層防御・マイクロセグメンテーションに関する記述に対するものです。ガイドラインでは、OT領域を守るための対策として、IT/OT DMZを通過する通信の制御や、ファブエリア内での多層防御・マイクロセグメンテーションの重要性が示されています。 ・OT環境では、多くの装置ツールのIPアドレスやデフォルトゲートウェイ等のネットワーク設定を安易に変更できないという運用上の制約が存在するため、セグメンテーションの実施が困難となる場合があります。例えば、「このPLCはDCS1とだけ通信できればよいが、セグメント的にはDCS2とも通信できてしまう」という状況は、不必要にラテラルムーブメントの範囲を広げていると言えます。このような状況でもセグメントを分割しようとすると、各デバイスのIPアドレスやデフォルトゲートウェイを変更しなくてはならないため、実現が難しいことが課題です。 ・そこで、VLAN挿入（VLAN insertion）など、既存のネットワーク設定を変更することなく、論理的なセグメンテーションを可能にする技術があることも補足し、より多様な実現方法を検討できるよう促すべきです。 ・また、OTプロトコル（例：GEM/SECS/HSMS）は暗号機能や認証機能を持たない場合が多く、攻撃に悪用されるリスクがあることから、単なるポート番号やIPアドレスによる制御だけでなく、通信内容やアプリケーション、プロトコルを可視化し、正規の通信か不正な通信かを判断することが不可欠である点も強調すべきです。	頂いた御意見を参考に、修正いたします。 修正箇所：第4.2節（P.70）
5	19	企業	4．CSIRT、PSIRT、FSIRTを統合・横断的に管轄する組織の必要性 ・本意見は、第4章「半導体デバイス工場における具体的対策例」の運用（監視・対応・復旧・改善）に対するものです。ガイドラインでは、IT、OT、製品それぞれのセキュリティインシデント対応組織として、CSIRT、FSIRT、PSIRTが個別に定義されています。しかし、サイバー攻撃がIT、OT、製品を横断して発生する現実を踏まえると、これらの個別組織を連携させるだけでは、インシデント対応の迅速性や全体像の把握に課題が生じる可能性があります。 ・したがって、IT、OT、製品のセキュリティを統合的に管轄し、戦略策定から運用、インシデント対応までを一元的に指揮する組織や機能の必要性を追記すべきです。この統合された組織は、各専門チーム（CSIRT, FSIRT, PSIRT）を束ねる司令塔として機能し、平時からの情報共有、技術的な知見の統合、共通のセキュリティポリシー策定を推進し、有事には迅速かつ統一的な意思決定と対応を可能とします。 ・このような統合的な組織体制を構築することで、サイバー攻撃の複雑なコンテキストを包括的に理解し、サプライチェーン全体のリスクをより効果的に管理できるようになります。	4.3 図4-14.　中段『戦略、ガバナンス、推進体制構築（組織設計、規程整備など）』はご提案の通り分離せず記載しているため、頂いた御意見については、原案の通りとさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
6	20	企業	1. ガイドラインの位置づけと運用に関する懸念 1.1 ガイドラインの活用方針の明確化 意見： このガイドラインの具体的な活用方針について明確化を求めます。 提案： •☒イドラインの位置づけ（推奨・必須・調達基準等）を明記 •☒階的導入スケジュールの提示 •☒存の公共調達基準との整合性確保 理由： •☒達基準として活用される場合、海外メーカーの対応可否が日本企業の競争力に直接影響する •☒ベル1の汎用ガイドラインで検討されていた公共調達基準との関係性が不明確 1.2 国際的な相互運用性の確保 意見： 各国で類似ガイドラインが策定される際の重複対応コスト軽減策を求めます。 提案： •☒C62443やNIST準拠製品の同等性認定制度の導入 •☒要国（米国、EU、韓国、台湾等）との相互認証協定推進 •☒ローバル標準への収束を前提とした制度設計 理由： •☒本市場規模を考慮すると、海外半導体メーカーが日本独自要件への対応を見送るリスク •☒果として日本企業の調達選択肢減少と競争力低下が懸念	1,1 ガイドラインの活用方針の明確化 本ガイドライン（案）は調達基準として活用するチェックリスト型ではなく、リスクベースの参考書として作成させていただいているため、頂いた御意見については、原案の通りとさせていただきます。 1.2 国際的な相互運用性の確保 本ガイドライン（案）は、国際標準と整合性を取ったうえで、日本における参考書として作成されているため、重複とならないよう作成が進められています。また、相互運用に関しては、以降の検討会にて検討を進めていく予定であり、頂いた御意見については、原案の通りとさせていただきます。
6	21	企業	2. 参照規格・基準に関する懸念 2.1 参照規格の選定根拠と国際的認知度 意見： CPSFおよびSEMI E187/E188規格の選定根拠と国際的実績の開示を求めます。 提案： •☒参照規格の選定基準と国際的認定実績の詳細開示 •☒要国での採用状況と相互運用実績の公表 •☒期的な参照規格見直しメカニズムの構築 理由： •☒導体は国際商品であり、グローバルに認知された基準での対応が必要 •☒照規格の妥当性が国際競争力に直接影響 2.2 他国基準との整合性確保 意見： NIST CSF2.0半導体製造プロファイルおよび他国基準との相互運用性確保を求めます。 提案： •☒ST CSF2.0との相互運用性の明確化 •☒U CRA（Cyber Resilience Act）等、主要市場の規制との整合性確認 •☒際標準化団体での日本提案の積極的推進 理由： •☒数国への輸出を前提とする企業の負担軽減 •☒際サプライチェーンでの円滑な連携確保	2.1 参照規格の選定根拠と国際的認知度 米にてSEMIと共同で作成されたNIST CSF2.0半導体プロファイルをリスクベースのアプローチとして選定いたしました。CPSFは国内における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として作成されており、現在国際規格化が進められています。そのため、頂いた御意見については、原案の通りとさせていただきます。 2.2 他国基準との整合性確保 本ガイドライン（案）は、NIST CSF2.0半導体製造プロファイルやSEMI E187半導体製造リファレンスなどの国際標準との整合性を取って作成されているため、頂いた御意見については、原案の通りとさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
6	22	企業	3. 技術的内容に関する改善提案 3.1 IEC62443参照箇所の具体化 意見： 「IEC62443の」という曖昧な表記の具体化を求めます。 提案： •IEC62443-X の Y.Z節」形式での具体的記述 •照個所一覧表の添付 •装ガイダンス文書の提供 理由： •み手による解釈の差異を防止 •装時の混乱回避と効率的対応の実現 3.2 セキュリティレベル要求の適正化 意見： 1.5節「想定する攻撃主体」におけるSL-4要求の見直しを求めます。 提案： •スクベースアプローチによる段階的要求レベル設定 •造環境向け（IEC62443-2系）と装置・コンポーネント向け（IEC62443-4系）の明確な区分 •スト・ベネフィット分析に基づく現実的要求水準 理由： •製造環境へのSL-4要求は過剰で実装コストが膨大 •造プロセスの特性に応じた段階的要求が妥当 3.3 リスク評価手法の国際整合性 意見： CPSF中心のリスク評価手法の妥当性について検討を求めます。 提案： •C62443-3のPurdueモデルを主軸とした領域・エリア分割 •PSFを補完手法として位置づけ •ST等、国際的に確立された手法との併用 理由： •際的通用性の確保が半導体製品の競争力に直結 •ローバル標準との乖離リスク	3.1 IEC62443参照箇所の具体化 本ガイドライン（案）では、第3章にNIST CSF2.0のサブカテゴリを記載しています。NIST CSF2.0にそのサブカテゴリに関連するIEC62443の節が記載されているため、頂いた御意見については、原案の通りとさせていただきます。 3.2 セキュリティレベル要求の適正化 各企業の状況に合わせてリスクベースで行っていただくことを想定し作成しているため、頂いた御意見については、原案の通りとさせていただきます。 3.3 リスク評価手法の国際整合性 本ガイドライン（案）は、リスク源についてはCPSFで業界の特徴に合わせて落とし込み、リスク評価についてはNIST CSF2.0を活用して作成しているため、頂いた御意見については、原案の通りとさせていただきます。
7	23	団体	サイバー攻撃が激化して、これまでクローズと考えられてきたOT系システムにもその被害が及ぶ状況となっている中、我が国のICTを支える半導体デバイス工場に対するセキュリティガイドラインを策定されるのは大変時宜を得たものであり、賛同いたします。 JSSECでは、OT系の開発者が必ずしもサイバーセキュリティに関する知見が高いとは限らないことから、IoTセキュリティに関してOT系とIT系の共通認識が持てるようにIoTセキュリティチェックシート（以下、本チェックシート）を作成しております。本チェックシートでは、IT系とOT系のどちらが検討主体になるか、一目でわかるように整理しており、タブレット等工場装置以外のIoTデバイスの利用にあたって有効と考えますので、活用いただけましたら幸いです。なお、本チェックシートはNIST　CSF1.0を参照しておりますが、2.0に合わせて見直す予定です。 【理由】 IoTセキュリティチェックシート（シートそのもののほか解説が載っています） https://www.jssec.org/iot	今後の検討における参考とさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
8	24	企業	翻訳） 【該当箇所】 第4.4節「物理アクセスの制限（入室・持込み・接続） - ファブエリアにおける物理的対策」　表4-6. ファブエリアにおける物理対策 【コメント】 「表4-6. ファブエリアにおける物理的対策」への追加提案（追加箇所は緑色でハイライトされています） ・持込機器の不正ネットワーク接続：無線侵入検知システムなど記録機能を有する~~コンピュータ~~デバイスの持込み制限を検知・防止するための対策 ・持込機器の妨害電波発信：無線侵入検知システムなど、無線電波発信デバイスの持込み制限を検知・防止するための対策 ・持込機器の不正録画：録画機能デバイスの持込み制限を検知・防止するための対策 【理由】 このドラフトでは、物理的なファブ環境における複数の脆弱性に対する予防的統制として「持ち込み制限」を規定しています。しかし実際には、半導体クリーンルームに出入りする多数の協力会社、装置、消耗品を対象にこのポリシーを徹底することは、追加的な診断・監視ツールなしでは現実的に困難です。 パッシブ型・広帯域の無線侵入検知システム（WIDS）を活用すれば、組織管理ネットワークに接続されていない段階でも、設定した周波数帯域で発信を開始したあらゆるデバイスを自動的に検知・位置特定し、多くの場合は分類まで行うことが可能です。これには、不正な携帯電話、SDR（ソフトウェア無線）、無線妨害装置（ジャマー）、ホットスポット、悪意あるアクセスポイント等が含まれます。 WIDSは100%受動的に動作するため、電磁波干渉やシステム停止リスクを新たに生じさせることなく、EDRソフトウェアを導入できない無線資産に対する異常な接続の監視も可能です。こうした対策は、他のミッションクリティカルな産業分野でも同様の目的で既に導入されています。 このようなプロアクティブかつ継続的な監視要件を追加することは、NIST CSF Version 2.0 Semiconductor Manufacturing Profileガイドラインにも合致します。 ・「製造システムに対し、不正な人員、接続、デバイス、アクセスポイント、ソフトウェアについて継続的なセキュリティ状態監視を実施すること。」（IR 8183r1: DE.CM-7） ・「不正なローカル、ネットワーク、リモート接続を検知し、製造システムの不正利用を特定すること。」（IR 8183r1: DE.CM-1） ・「製造システム内に監視デバイスを戦略的に配置し、特定のイベント検知に必要な情報を収集すること。」（IR 8183r1: DE.CM-7） さらに、NIST SP 800-53 SI-4 (14)「無線侵入検知」でも次のように規定されています。 【統制文】「不正な無線デバイスを特定し、システムへの攻撃試行や潜在的な侵害・漏洩を検知するために、無線侵入検知システムを導入すること。」【補足ガイダンス】「無線信号は組織の施設外へも放射される可能性があるため、組織は不正な無線接続を積極的に探索し、施設内外を問わず不正な無線アクセスポイントの有無を徹底的にスキャンする必要がある。これには、システムを含むエリアだけでなく、施設の外部も対象とし、組織システムに不正なアクセスポイントが接続されていないことを確認する。」	頂いた御意見を参考に、追記いたします。 修正箇所：第4.3節（P.74 図4-17）、第4.4節（P.81 表4-6、P82 図4-22）
8	25	企業	翻訳） 【該当箇所】 第3.2.3節　表3-8. OT領域の外部サービス及びIT/OT DMZ分離制御のリスク分析のための情報　②外部サービス（遠隔診断サービス） 【コメント】 追加提案箇所は緑色でハイライトされています 「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。ファブ内の装置・機器に組み込まれた無線通信ネットワーク（例：モバイルルーター）の有無を確認するためには、無線周波数検知ツールの活用が有効です。」 【理由】 米国の太陽光発電パネルやバッテリーにおいて、隠されたリモート通信デバイスが発見されたという最近の事例は、皆様ご存知かもしれません。従来型のネットワーク監視手法では、モバイルルーターのようなサードパーティ製ハードウェア部品に組み込まれた、隠蔽または未申告の無線アウトオブバンドチャネルを検知・警告することは非常に困難です。しかし、WIDS（無線侵入検知システム）のようなRFスキャン手法であれば、こうした異常を即座に検知・通報することが容易です。 この方法は、ガイドライン該当箇所の要求事項を製造事業者が最適に満たす手段であり、半導体工場向けOTセキュリティガイドラインの目的である「未知の無線通信経路の排除と監視強化」に直接合致します。よって、具体的なアプローチ例として明記することで、当該セクションの意図したセキュリティ要件の達成に資するものと考えます。	頂いた御意見を参考に、追記いたします。 修正箇所：第3.2.3節 ②（P.41　表3-8「特徴及び考慮すべき観点」）

提出No.	No.	提出者	提出意見	御意見に対する考え方
8	26	企業	翻訳） 【該当箇所】 第3.2.1節　表3-4. OT領域ファブエリアのリスク分析のための情報　②-1 装置ツール（エンドポイント）の考慮するべき観点 【コメント】 追加提案箇所は緑色でハイライトされています。 装置・ツールのセキュリティ対策は、SEMI E187/E188に準拠して検討する必要があります。具体的には、装置の性能保証を前提としたうえで、セキュリティエージェントの導入、マルウェア対策の実施、ハードニング（不要なI/Oポートの制限や、不要なサービス・コンポーネント・ネットワークプロトコル・ポートの無効化）、異常検知ツール（例：EDRやWIDS）の導入などの対策を検討してください。 一部の既存装置やツールでは、性能保証仕様の都合により新たなソフトウェアのインストールや設定変更ができない場合があります。そのため、特に無線機能を有する重要機器・ツールに対しては、WIDS等による追加的な異常検知対策の検討が必要です。また、EDRによる監視が困難かつ無線機能を有しない装置・ツールについては、ネットワークを利用した多層防御（ディフェンス・イン・デプスやマイクロセグメンテーション等）、他の対策手法の導入も検討してください。 【理由】 ご指摘の通り、一部のファブ装置・ツールでは、ハードウェア仕様や運用効率の観点からEDRやソフトウェアベースのセキュリティ対策を導入できない場合があります。特に無線機能を有する資産については、対象となるプロトコルによっては、マイクロセグメンテーションやネットワーク制限による無線デバイス間の通信遮断も現実的でないケースが存在します。 このような場合、EDR等の導入が困難な無線対応資産に対しては、パッシブ型WIDS（ワイヤレス侵入検知システム）による異常検知が有効です。パッシブWIDSは、無線周波数の発信や資産との直接的な相互作用を伴わないため、スキャンによる運用上のリスクを生じません。メーカーは、他の十分なセキュリティ対策が実装できない重要な無線対応資産について、パッシブWIDSの導入を検討することが望まれます。	該当箇所の「既存装置ツールにおいては、性能保証上の仕様により新たなソフトウェアツールの導入や設定変更が行えないものも存在するため、ネットワークによる追加対策（多層防御やマイクロセグメンテーション等）を検討する必要がある。」における、「既存装置ツール」には「無線機能を有する資産」も含まれているため、頂いた御意見については、原案の通りとさせていただきます。
8	27	企業	翻訳） 【該当箇所】 第3.2.1節　表3-4. OT領域ファブエリアのリスク分析のための情報　②-2 ネットワークの考慮するべき観点 【コメント】 追加提案箇所は緑色でハイライトされています。 5. 重要な箇所にはネットワークの異常検知の仕組みを導入する。特に、無線機能を有する重要資産については、無線侵入検知システム（WIDS）などの適切なネットワーク異常検知機構により、無線データフローを監視する必要があります。 【理由】 (2)-2 で指摘されている通り、多くのファブ資産はソフトウェアベースのセキュリティ対策を導入できないため、ネットワークベースの異常検知機構などのアプローチが必要です。本セクションは、プロセス遅延やハードウェア／プロトコル上の制約から利用可能なセキュリティ対策が限られる資産を対象としています。そのため、プロセス遅延を発生させずに導入・運用でき、マイクロセグメンテーションやネットワーク制限が困難な状況でも無線通信を監視できる異常検知ツール（例：WIDS）の具体例を示すことで、メーカーの対策検討を支援できます。 また、WIDSの活用は本ガイドが本セクションで挙げている複数の脅威・脆弱性への直接的な対策となります。メーカーは、下記のような本セクションの主要な懸念をカバーする手段を知っておくべきです： 【このセクションに記載の脅威例】 組織が保護すべきデータの漏えい（例：通信経路上のデータ改ざん等のMITM攻撃） 【このセクションに記載の脆弱性例】 外部への不正通信を適切に検知・遮断する仕組みが不十分 セキュリティ異常（例：なりすまし・メッセージ改ざん等）を迅速に検知し早期対応できる仕組みが未整備	該当箇所の「重要な箇所にはネットワークの異常検知の仕組みを導入する。」は、無線異常検知（WLAN）も含んでいるため、頂いた御意見については、原案の通りとさせていただきます。
8	28	企業	翻訳） 【該当箇所】 第3.2.1節　表3-4. OT領域ファブエリアのリスク分析のための情報　②-3 物理的な制約の考慮すべき観点 【コメント】 追加提案箇所は緑色でハイライトされています。 例：ファブエリア内のネットワーク機器は、施錠管理可能なラックやボックスの中で管理を行う。未使用のファブネットワークの接続口が通常アクセス可能な範囲にある場合は、物理的なポートロック対策を行う。WIDSを導入することで、電波妨害機器の存在や、スマートフォンやSDR（ソフトウェア無線機）などの不正デバイスがファブ資産に無線接続することを監視・防止する。 【理由】 本セクションで挙げられている脆弱性の一つである「ファブ施設内での電波妨害（ジャミング）攻撃リスク」への対応には、継続的なRF（無線周波数）モニタリング手法が不可欠です。また、同じく本セクションで記載されている「ネットワークに接続された不正デバイスの検知対策」についても、EDRやその他のソフトウェアベース監視が困難な無線資産を運用する場合にはWIDSの活用を検討すべきです。	頂いた御意見を参考に、追記いたします。 修正箇所：第3.2.1 ②-3（P.27　表3-4「特徴及び考慮すべき観点」）

提出No.	No.	提出者	提出意見	御意見に対する考え方
9	29	企業	当該意見募集に際し、特段反対の意見はございません。以下、弊社として賛同の意見を申し上げます。 半導体製造におけるサイバーセキュリティ対策を促進するには、現下の状況を現場から経営層までしっかりと理解していただくことが重要であり、サプライチェーンを含めた対策（最も高度な攻撃者を想定）をNISTが示した守るべき5つの対象に沿って、経産省からガイドライン案として具体的に提示されることについては、大変重要なものと考えます。 弊社といたしましては、「たしかなテクノロジーで「信じられる社会」を築く。」をパーパスとして掲げており、わが国、関係する諸外国で活躍する企業等におけるサイバーセキュリティ対策の重要性が、関係各所により浸透していくことが肝要と認識しており、本ガイドラインに賛同いたします。	本ガイドライン（案）に対する肯定的な御意見として承ります。
10	30	団体	総論 JICSSは、半導体デバイス工場のための包括的なOTセキュリティガイドラインの策定を強く支持いたします。本ガイドラインは、半導体製造環境の独特な特性を適切に認識し、国家支援型APTグループを含む高度なサイバー脅威から日本の半導体サプライチェーンを保護することの重要性を明確に示しています。 SEMI E187/E188規格やNISTサイバーセキュリティフレームワーク2.0などの国際的枠組みと整合したリスクベースアプローチの採用を高く評価いたします。この整合性により、日本がグローバル半導体市場における競争力を維持しながら国際協力を促進することが可能になります。 半導体製造工場内のセキュリティ確保は、OT技術、IT技術が混合される環境を考慮せねばならず、要求条件は用途によっては設置後20年以上の稼働が求められることも考慮する必要があります。その結果、当該環境を安全に保つためには、長期的な視点にたった対策を、1）工場所有者および運用者、2）工場内機器納入業者、3）前述の機器を構成するための要素を提供する事業者など複数の階層に渡るサプライチェーン全体を考慮した施策が必要であり、そのためのガイドラインやベストプラクティスは産業界および日本産業界の世界的地位保全、向上に有効に機能すると想定されます。具体的には、現在すでに納入されている機材の安全確保の手段、手順、そして今後開発される機材やシステムの安全運用、更新の手順は異なる階層として捉え、ガイドラインやベストプラクティスをまとめていくことが適切と考えます。そして、ITの世界では一般的に考慮され始めたAIや将来の量子技術への対応なども上記の対策と並行して行うべきでありますが、最重要なのは現在稼働しているシステムを安定的に運用しつつ保全することであり、優先順位をつけた対策が重要と考えます。	本ガイドライン（案）に対する肯定的な御意見として承ります。
10	31	団体	1. 製品ライフサイクルセキュリティの統合 ガイドラインに包括的な製品ライフサイクルセキュリティアプローチを組み込み、ISO/IEC TR 6114「製品ライフサイクル全体にわたるセキュリティ考慮事項」を単なる参照ではなく、SEMIおよびNIST CSF規格と並ぶ基盤的ライフサイクル管理要件として位置づけることを推奨いたします。このセキュリティ考慮事項は、半導体製造に典型的な長期装置ライフサイクル（25年以上）にわたるセキュリティ管理のための重要なガイダンスを提供します。 【理由】 半導体ファブは他のほとんどのOT環境と異なり、数十年にわたって装置を運用します。ライフサイクルセキュリティを中核設計原則として組み込まなければ、ガイドラインは持続可能な回復力ではなく短期的なパッチとして見られるリスクがあります。経済産業省は、ライフサイクル管理をTier-1セキュリティ制御カテゴリに正式に格上げすることでリーダーシップを示すことができます。ISO/IEC TR 6114は半導体ファブセキュリティ課題に対処するために特別に開発され、デバイス識別、構成管理、ライフサイクルセキュリティ制御のための体系的アプローチを提供します。これらの長期運用期間を通じた機器真正性、構成完全性、ライフサイクル追跡のためのデジタル署名メカニズムは、半導体製造における基本的なデバイス管理課題に対処します。	製品ライフサイクルセキュリティアプローチ（ISO/IEC TR 6114）については、グローバル業界標準と照らし合わせ、今後予定するファシリティエリアへの対策と共に検討を行う予定であり、頂いた御意見は今後の検討における参考とさせていただきます。
10	32	団体	2. 長期装置ライフサイクル管理 ガイドラインにおいて、デバイスが25年以上稼働し、容易に更新や交換ができないレガシーシステムを管理するための体系的アプローチを含む、半導体製造における長期装置運用の現実に特化して対処することを推奨いたします。 【理由】 半導体製造装置は他の産業と比較して独特に長い運用ライフサイクルを持ちます。現在の運用環境には、装置保証、性能保証、または運用要件のために更新できないWindows XPやその他のレガシープラットフォームを実行するシステムが含まれています。ガイドラインは、分離戦略、補償統制、切断または部分的に接続されたレガシー装置を特定・管理するための体系的アプローチを含む、これらのシステムを管理するための実践的アプローチを提供すべきです。	本ガイドライン（案）は、ご指摘のレガシーシステム問題も念頭に置いた国際標準SEMI E187/188を参照しており、同規格が推奨するリスクベースのアプローチは本ガイドラインにも反映しております。御意見の趣旨はガイドラインの基本的な考え方に含まれていると整理しており、頂いた御意見については、原案の通りとさせていただきます。
10	33	団体	3. 強化されたエッジコンピューティング統合 ガイドラインにおいて、製造フロアデバイスから中間エッジデータセンターを経てクラウドサービスまでにわたる進化するエッジ（分散）コンピューティングリソースの重要性を認識することを推奨いたします。既存のクラウドサービスとリモート診断フレームワークを基盤として、このエッジコンピューティング環境のセキュリティ考慮事項に対処すべきです。さらに、多くの分離されていると信じられているネットワークが実際には分離されていないため、ネットワーク分離テストと検証の包括的要件を含めることを推奨いたします。 【理由】 現代の半導体製造では、製造装置への組み込み処理、ローカル分析のための中間エッジデータセンター、高度処理のためのクラウドベースリソースを含むエッジコンピューティング機能をますます利用しています。このコンピューティングの中央集約型から分散型アーキテクチャへの進化には、適切なOT/IT分離とデータ保護要件を維持しながら動的ワークロード分散に対応できるセキュリティの枠組みが必要です。製造業界では、装置メーカーが独自の診断デバイスを持ち込み、不適切なVPN構成やDNSなどの認識されていないプロトコルアクセシビリティを通じてネットワーク分離を妨げる可能性があるという重要なセキュリティギャップが存在します。多くの認識されていない経路が分離ネットワークを公開ネットワークに接続する可能性があります。例えば、分離ネットワークデバイスがHDMI 1.4（2009年）以降の規格を使用して接続デバイスと共有ディスプレイに接続される場合などです。産業環境では、KVMスイッチは一般的ですが、ネットワーク接続も伝送できることが認識されていません。分離の一度きりのテストは不適切です。24時間年中無休の継続的テストが不可欠です。一部のシステムは、製造装置プロバイダーに定期的にテレメトリをアップロードし、予測可能なスケジュールで不適切なトンネリング構成により分離ネットワークを公開インターネットに露出させる可能性があるためです。	頂いた御意見を参考に、追記いたします。 修正箇所：第3.2.3節 ③（P.42　表3-8「特徴及び考慮すべき観点」）

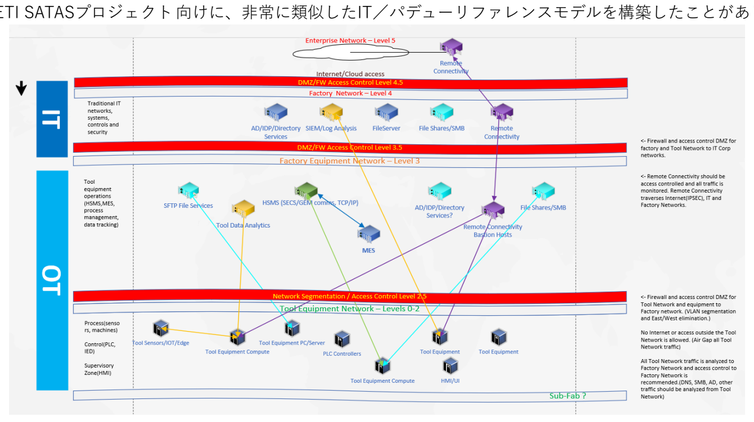
提出No.	No.	提出者	提出意見	御意見に対する考え方
10	34	団体	4. デバイス識別と構成管理 ガイドラインにおいて、長期運用期間にわたって数千のデバイスが展開される可能性がある複雑な製造環境におけるデバイス発見と構成管理のための体系的アプローチを強調することを推奨いたします。これらのアプローチは、デジタル署名、不変ベースライン、自動監視を使用した必須のデバイス発見と継続的構成管理を要求すべきです。 【理由】 資産可視性は今日のファブにおける重要な課題です。これを明示的かつ規範的にすることで、ガイドラインがこの運用ギャップに対処することが保証されます。半導体OTセキュリティの基本的な課題は、工場環境でのデバイスの発見と管理です。装置が数十年間稼働し、時間の経過とともに構成変更が発生する中で、正確な資産在庫一覧表の維持はますます困難になります。デジタル署名メカニズムと体系的な構成管理アプローチは、長期装置ライフサイクル全体でセキュリティと運用の完全性を維持するための重要な能力を提供します。	頂いた御意見を参考に、追記いたします。 修正箇所：第4.1節（P.56）
10	35	団体	5. 国際標準との整合 ガイドラインにおいて国際標準との調和・整合への言及を強化し、既存のSEMI E187/E188およびNIST CSF 2.0参照と並んでISO/IEC TR 6114を明示的に認識し、半導体固有のセキュリティ考慮事項の包括的なカバレッジを確保することを推奨いたします。 【理由】 SEMI E187/E188標準は重要な基盤要件を提供しますが、業界からのフィードバックによると、サプライヤーの実装課題により初期要件レベルは保守的に設定されました。ISO/IEC TR6114は半導体製造環境向けに特別に開発された補完的ガイダンスを提供し、他の標準では完全にカバーされていない重要なライフサイクルセキュリティの考慮すべき事項に対処します。	頂いた御意見については、今後の検討における参考とさせていただきます。
10	36	団体	6. 実践的実装考慮事項 ガイドラインにおいて、長期装置ライフサイクル、ベンダー制限、運用継続性要件を含む半導体製造環境の実践的制約を認識しながら、現実的で達成可能なセキュリティ対策に焦点を維持することを推奨いたします。 【理由】 日本の装置メーカーは、グローバルベストプラクティスと比較して高度なセキュリティメカニズムの実装において大きな課題に直面しています。ガイドラインは、現在の業界能力と実装タイムラインを認識しながら、段階的なセキュリティ改善のための実践的な道筋を提供すべきです。包括的なデジタル署名などの高度なセキュリティ機能については、加速された展開スケジュールよりも現実的な10年実装タイムラインがより適切である可能性があります。	本ガイドライン（案）は、国内業界の要望をもとにデバイスメーカーの実践的な意見を交え、第4章に具体的対策例を記載させていただいています。頂いた御意見については、今後の検討における参考とさせていただきます。
10	37	団体	7. クラウドセキュリティと外部サービス ガイドラインにおいて、適切なOT/IT分離とデータ主権性考慮事項を維持しながら、クラウドベース分析サービスとリモート診断機能の安全な統合に関するガイダンスを提供し、ゼロトラストフレームワークを活用することを推奨いたします。 【理由】 クラウドサービスとリモート診断（e-Diagnostics）は、半導体製造最適化と予知保全にますます重要になっています。ガイドラインは、製造システムの完全性を保持し、機密運用データを保護しながら、これらの機能を可能にするグローバルに認識された安全な実装パターンに対処すべきです。	頂いた御意見を参考に、修正いたします。 修正箇所：第3.2.3節 ②（P.41　表3-8「関連するNIST CSF2.0半導体製造プロファイル、CPSF、SEMI E187製造リファレンス」）
10	38	団体	今後の発展への提言 1. スマート製造とAI対応準備 AI技術は現在、半導体製造フロアには大きく展開されていませんが、将来のガイドライン更新においてスマート製造、製造DXイニシアチブ、適応的製造の進化に向けたAI対応に対処する専用セクションを含めることを推奨いたします。現在の運用環境は主に従来の制御システム（サーボ制御、SCADA、PLC）を利用していますが、今後5-10年にわたるスマート製造進化への準備は、日本の競争力維持にとって重要です。さらに、包括的なセキュリティカバレッジを確保するため、継続的なファームウェアセキュリティテストと検証に関するセクションが有益です。 将来開発の重要領域： ● AIoTセキュリティモデル： 適応的製造プロセスとリアルタイム最適化を可能にするAI対応IoTデバイスのセキュリティフレームワーク開発 ● スマート製造セキュリティ： リアルタイムデータ分析と予測アルゴリズムに基づいてプロセスを適応させることができるAI駆動製造システムのセキュリティ考慮事項 ● 製造DX統合： 機密製造データと知的財産を保護しながらデジタル変革イニシアチブを支援するセキュリティフレームワーク ● 適応的製造セキュリティ： AIと機械学習技術によって可能になる動的製造プロセスに対応でき、重要な知的財産インプットを保護するセキュリティ対策 ● ファームウェアセキュリティ： 運用ライフサイクル全体を通じて装置完全性を確保するための継続的なファームウェアセキュリティテストと検証プログラム 2. 強化されたエッジ・ツー・クラウドコンピューティングフレームワーク 半導体製造が製造フロアのデバイスからエッジデータセンターを経てクラウドサービスまでにいたる分散コンピューティングアーキテクチャに向けて進化するにつれ、将来のガイドラインはOT環境分離要件を維持しながら包括的な継続的セキュリティ研究から洞察を得るべきです。我々は、エッジ・ツー・クラウドアーキテクチャにより、従来想定されていたネットワーク分離の境界を超えて、新たなセキュリティリスクが発生する可能性があることを認識しています。別のネットワーク化されたコンピューティング環境に終端されるトンネリングは、追加の脆弱性ポイントを作り出す可能性があります。例えば、脆弱性研究では、コンテナ化の現在のパラダイムが内部（仮想/SDN）ネットワーキングに依存する悪用を露出し、分離されていると信じられているネットワークを露出する複数の潜在的リークポイントを持つことが実証されています。 開発領域： ● 分散コンピューティングセキュリティ： エッジデバイス、中間データセンター、クラウドリソースに分散された処理能力を利用する製造環境向けに特別設計されたセキュリティフレームワーク ● 動的ワークロードセキュリティ： 要件とネットワーク条件に基づいて計算ワークロードが動的に移動する際に適応できるセキュリティポリシー	本ガイドライン（案）に対する肯定的な御意見として承ります。

提出No.	No.	提出者	提出意見	御意見に対する考え方
			● ハイブリッドコンピューティング統合： リソース制約のある製造デバイス、ローカルで利用可能な「エッジ」リソース、強力なクラウドベース分析プラットフォームの統合に対応するセキュリティ対策 ● コンテナセキュリティ： 分散製造環境におけるコンテナ化ワークロードと仮想ネットワーキングを保護するための包括的フレームワーク 3. サイバーセキュリティ脆弱性テストと軽減プログラム 将来のガイドラインは、長期装置ライフサイクルと運用継続性要件の独特な課題を認識し、半導体製造環境向けに特別設計された包括的な脆弱性テストと軽減フレームワークを確立すべきです。ITシステムとOTシステムのテストにおける主要な違いの一つは、ITシステムでは侵入テストが外部侵入（「外部から内部に入ることができるか」）に焦点を当てるのに対し、OTシステムでは、テストは双方向—外部侵入と内部流出の両方（「大脱走は可能か」）であるべきことです。 プログラム要素： ● 製造固有脆弱性評価： 半導体製造装置の運用制約と長期ライフサイクルを考慮したテスト手法。変更管理プロセスとの密接な統合は、これをより簡単にすることができますが、簡単ではありません。この課題は、メンテナンスサイクルが2-3年と長く、デバイスライフサイクルが時に50年に近づく発電OT環境に存在します。 ● 継続的セキュリティ検証： セキュリティ効果を維持しながら運用中断を最小化する継続的セキュリティ評価のフレームワーク。安全なサプライチェーン管理、常に最新のSBOM、ゴールドスタンダード画像に対するジャストインタイムファームウェア/ソフトウェアバージョン/コンテンツ検証は、この検証を達成するのに価値があります。 ● 補償統制開発： 装置制約により直接的な脆弱性パッチが実現不可能な場合のセキュリティ対策実装のための体系的アプローチ ● 双方向テスト： OT環境における外部侵入ベクトルと内部データ流出可能性の両方を評価するテスト手法 4. 人的資本開発と産学連携 半導体製造サイバーセキュリティの効果的な実装には、製造プロセス、運用技術、サイバーセキュリティ原則の理解を組み合わせた専門知識が必要です。さらに、内部者リスクは専門的注意を必要とする重要な脅威ベクトルを表します。半導体製造は、チップの早期故障を引き起こすプロセスに不純物を導入する検出困難な妨害行為を含む多くのタイプの攻撃に脆弱であり、これらの攻撃は実際に発生しています。AI行動分析の使用は、人間から発生する脅威を追跡し、行動の変化や変装下で活動する偽装者を検出するために使用できます。 開発イニシアチブ： ● 専門訓練プログラム： 半導体製造環境の独特なサイバーセキュリティ課題に対処する教育カリキュラム ● 産学パートナーシップ： 製造サイバーセキュリティの理論的理解と実践的実装の両方を進歩させる共同研究・教育プログラム ● 専門職能開発フレームワーク： 半導体製造で働くサイバーセキュリティ専門家のための認定および継続教育プログラム ● 機能横断的専門知識開発： 製造専門家がサイバーセキュリティの含意を理解し、サイバーセキュリティ専門家が製造要件を理解できるようにする訓練プログラム ● 内部者脅威管理： 行動分析、アクセス制御、AI対応脅威検出を通じて内部者リスクに対処する包括的プログラム ● 行動分析： 製造環境における異常な人間行動と潜在的内部者脅威を検出するAI駆動システムの開発 5. 高度サプライチェーンセキュリティ 現在のSEMI標準整合に基づき、将来の発展では半導体装置サプライチェーン全体でのソフトウェア部品表（SBOM）要件と強化されたベンダーサイバーセキュリティ透明性、特にAI対応製造装置の進化する状況への対応を含めて対処すべきです。SBOM要件とベンダーサイバー成熟度開示を調達および装置認証標準に組み込むことを推奨します。半導体装置は高度にグローバル化されており、サプライチェーンの可視性なしに、日本はサードパーティソフトウェアやファームウェアの奥深くに隠された脆弱性への系統的露出のリスクを負います。SBOMはグローバルベストプラクティスになりつつあり、日本をリーダーとして位置づけます。 SBOM実装は2つのアプローチに従うべきです：ベンダー宣言インベントリと自動リバースエンジニアリングを通じてソフトウェア画像（バイナリ）から構築されたSBOM。他の産業セグメントでは、ベンダー自己宣言SBOMはバイナリで実際に見つかるソフトウェアの10%-20%しか含まない可能性があり、ベンダー自身が理解していない可能性のあるライブラリなどのソフトウェアを含むことが示されています。経済安全保障、二重用途、グローバル産業協調は、デジタル半導体サプライチェーン統合から恩恵を受ける可能性があります。 6. 量子安全暗号計画 半導体製造装置の長期ライフサイクルを考慮し、将来のガイドラインは、ポスト量子時代まで延長される可能性がある装置運用ライフスパン全体にわたって長期投資と機密製造データを保護するためのポスト量子暗号標準への準備戦略を含めるべきです。 結論 JICSSは、日本の半導体産業におけるサイバーセキュリティ課題に対する経済産業省の思慮深いアプローチを高く評価いたします。これらのガイドラインは、運用効率と国際競争力を維持しながら重要な製造インフラを保護するための重要な基盤を提供しています。 長期装置ライフサイクルと複雑な運用要件を含む半導体製造環境の独特な特性を認識した、実践的で実装可能なセキュリティ対策への重点を特に支持いたします。ISO/IEC TR 6114ガイダンスの統合により、半導体製造に重要なライフサイクルセキュリティ考慮事項のガイドラインカバレッジが大幅に強化されます。 半導体産業は、エッジコンピューティング機能の統合により急速に進化し、スマート製造プロセスに向けて発展し、AIに適応した製造形態への準備を進めています。日本が安全な半導体製造の最前線に留まり、次世代スマート製造能力の基盤を構築することを確保するため、将来のガイドライン更新においてこれらの新興トレンドを考慮することを経済産業省に奨励いたします。 経済産業省の半導体セキュリティにおける日本のリーダーシップの継続的な支援を期待しております。JICSSは、これらの重要なガイドラインの成功的な実施、特に製品ライフサイクルセキュリティ、長期装置管理、スマート製造進化への準備領域において、追加的な技術専門知識と政策研究を提供する準備ができています。 これらのガイドラインが確定・実装される際の継続的な対話の機会を謹んでお願いするとともに、現在の運用卓越性と将来の製造イノベーションの両方を可能にする現実的で	
11	39	企業	1. 以下は誤記と思われます。（計3か所） ×「通信系路上」 〇「通信経路上」	頂いた御意見の通り、修正いたします。 修正箇所：第3.2.1節 ②-2（P.26　表3-4「CPSFリスク源（脅威、脆弱性、脆弱性ID）」）

提出No.	No.	提出者	提出意見	御意見に対する考え方
11	40	企業	2. 以下は文章がおかしいと思われます。 「ファブシステムエリアでは、ファブエリアの装置ツール類の生産プロセス・品質管理を MES、SPC、EDA のシステムを、サーバ・ストレージ・ネットワーク等で構成する。」	頂いた御意見を参考に、修正いたします。 修正箇所：第3.2.2節 ①（P.35　表3-6「特徴及び考慮すべき観点」）
11	41	企業	3. 表3-4から表3-10において、「CPSFリスク源」として脅威や脆弱性が記載されていますが、脅威・脆弱性・リスクを取り違えたような記述が散見されます。 以下に例をあげます。 ・表 3-4. OT 領域ファブエリアのリスク分析のための情報 P.25 「通信系路上でデータを改ざんする中間者攻撃等自組織の保護すべきデータが漏洩する」は、脅威ではなくリスクです。また、完全性（改ざん）と機密性（漏洩）のどちらを問題にしているのかが不明です。 ・表 3-8. OT 領域の外部サービス及び IT/OT DMZ 分離制御のリスク分析のための情報 P.37 「脅威」として挙げられている3点は脆弱性であり、「脆弱性」として挙げられている3点はリスクです。 ・表 3-10. 半導体デバイス工場の組織・ヒト側面におけるリスク分析のための情報 P.42 「セキュリティインシデントにより適切に事業継続できない」は、脅威ではなくリスクです。 P.44 「セキュリティ事象による被害を受けたモノ(製品)・サービスが生じる」は、脆弱性ではなくリスクです。 P.44 「自組織が保護すべきデータが漏洩する」は、脅威ではなくリスクです。 P.45 「セキュリティインシデントにより自組織が適切に事業継続できない」は、脅威ではなくリスクです。 P.46 同上 P.47 同上	頂いた御意見を参考に、追記いたします。 修正箇所：第3章 表3-4、表3-6、表3-8、表3-10（各表「CPSFリスク源（脅威、脆弱性、脆弱性ID）」）
11	42	企業	4.「7 向上とトレーニング」の「脆弱性」に、「自組織の保護すべきデータのセキュリティ上の扱いについて、関係者が十分に認識していない」という項目が重複して2回書かれています。	頂いた御意見の通り、修正いたします。 修正箇所：第3.3節 ⑦（P.51　表3-10「CPSFリスク源（脅威、脆弱性、脆弱性ID）」）
11	43	企業	5. 以下は誤記と思われます。（計3か所） ×「パッチ適応」 〇「パッチ適用」	頂いた御意見の通り、修正いたします。 修正箇所：第4.1.5節（P.65）
11	44	企業	6. 以下は誤記と思われます。 ×「ファブエリアへの入室・持込み・接続の制限する物理的アクセス防御」 〇「ファブエリアへの入室・持込み・接続を制限する物理的アクセス防御」	頂いた御意見の通り、修正いたします。 修正箇所：第4.3節（P.73）
12	45	企業	1.「経済産業省の投資促進関連施策の要件等に対する当該ガイドラインで示すセキュリティ対策基準の紐付け等について検討していく予定」とあるが、ガイドラインのどこを確認すれば準拠・対応していると判断できるのか現状のガイドラインではわからないため、判断するためのチェックリストを別紙等に添付していただきたい。 【理由】 https://www.meti.go.jp/press/2025/06/20250627009/20250627009.html 4.　今後の見通し 今後、パブリックコメントでいただく御意見を踏まえて本年秋頃を目途として当該ガイドラインを成案化し、経済産業省の投資促進関連施策の要件等に対する当該ガイドラインで示すセキュリティ対策基準の紐付け等について検討していく予定です。	投資促進関連施策の要件等に対する当該ガイドラインで示すセキュリティ対策基準の紐付け等について検討は、本ガイドライン（案）とは別に進められており、紐づけのセキュリティ対策基準（チェックリスト）は、本ガイドライン（案）には含まれておりません。頂いた御意見については、今後の検討における参考とさせていただきます。
12	46	企業	2. ガイドラインでは、装置ツールの構成管理情報の例としてSBOM、ファブネットワークに接続される装置ツールのサイバーセキュリティのステータスレポート情報を取得するフレームワークとしてSEMI E191の２つの記載がある。今後、半導体工場は、装置メーカーからSBOMを提出してもらい構成情報の更新を行うこと、ステータスレポート情報の管理をする必要があるという2点が求められることになる。という理解でよろしいでしょうか。	本ガイドライン（案）は、各社がリスクベースで対策を検討する際の参考情報を提供するものであり、記載されている対策（SBOMやSEMI E191の活用を含む）を一律に義務付けるものではありません。ご指摘の点は、サプライチェーンセキュリティにおける有効な対策の参考事例として記載しており、各事業者の判断で活用を検討いただくことを想定しております。
12	47	企業	3. 装置ツールの脆弱性情報の把握のために、装置メーカーからの脆弱性情報の提供がガイドライン準拠には必要となってくるのでしょうか。	本ガイドライン（案）は、各社がリスクベースで対策を検討する際の参考情報を提供するものであり、記載されている対策を一律に義務付けるものではありません。ご指摘の点は、サプライチェーンセキュリティにおける有効な対策の参考事例として記載しており、各事業者の判断で活用を検討いただくことを想定しております。
12	48	企業	4. 装置ツールの脆弱性情報の把握のために、脆弱性スキャンツールを利用する場合は、半導体工場の製造部門が実施するという理解でよろしいでしょうか。	本ガイドライン（案）は、各社がリスクベースで対策を検討する際の参考情報を提供するものであり、記載されている対策を一律に義務付けるものではありません。ご指摘の点は、サプライチェーンセキュリティにおける有効な対策の参考事例として記載しており、各事業者の判断で活用を検討いただくことを想定しております。

提出No.	No.	提出者	提出意見	御意見に対する考え方
13	49	企業	翻訳） Comment： 半導体プロファイルに紐付けられていますが、次回改訂時に新たなコメントによって現状のまま維持されるか、変更されるかは不明です。 Description： NIST CSF 2.0 半導体製造プロファイル	本ガイドライン（案）は、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への紐づけを行っており、頂いた御意見については、原案の通りとさせていただきます。
13	50	企業	翻訳） Comment： 脆弱性管理やパッチ管理は有効なセキュリティ対策ですが、OEMメーカーによって広く採用されているとは言えません。そのため、デバイスメーカー（DM）やファウンドリーは、OEM側がパッチ適用や脆弱性管理を十分に実施していない場合でも、ネットワークセキュリティの代替的な統制（コンペンセーティングコントロール）を構築する責務があります。 Description： 【SEMI E187 - 製造リファレンス】 3.4 脆弱性／脅威評価	第3.2.1節 ①『装置ツールの資産管理と脆弱性評価』にて同等の内容を記載しているため、頂いた御意見については、原案の通りとさせていただきます。
13	51	企業	翻訳） Comment： 3.5 この記述は内容が不明確なので、「階層的」という表現について明確化が必要です。「階層的」は、ネットワーク全体のセキュリティを指している可能性がありますが、具体的に何を意味するのか判断できません。 Description： 階層的ネットワークセキュリティ対策	頂いた御意見を参考に、修正いたします。 修正箇所：英語版 第3.2.1節 ②-2、第3.2.1節 ②-3
13	52	企業	翻訳） Comment： これは有効なアイデアだと考えますが、具体的な実施方法や主要なKPIについては不明確です。 Description： セキュリティ重要業績評価指標（KPI） 概要：持続可能なセキュリティ運用・管理を達成するためのセキュリティKPIを概説する。	本ガイドライン（案）に対する肯定的な御意見として承ります。
13	53	企業	翻訳） Comment： 現在、当社の購買仕様書にはSEMI E187の12項目要件への準拠のみが記載されています。 Description： 3.1 装置ベンダーと事前に確認すべき調達要件の重要ポイント	頂いた御意見は、今後の検討における参考とさせていただきます。
13	54	企業	翻訳） Comment： ファイアウォールの設置やネットワークの分離はデバイスメーカー（DM）の責務ですが、これらは購買仕様書には明記されていません。また、ファイアウォールの詳細情報はOEMやサプライヤーには開示されていません。 Description： 3.2 半導体デバイスメーカーが装置やツールを調達する際に考慮すべき仕様（例：ファイアウォールの設置やネットワーク分離 など）	頂いた御意見を参考に、追記いたします。 修正箇所：第3.2.1節 ③（P.30 表3-4「特徴及び考慮すべき観点」）
13	55	企業	翻訳） Comment： 3.3および3.7の両方に同意します。両領域について、適切なプロセスとソリューションが整備されている必要があります。 Description： 3.3 搬入・搬出（Move-in/out）、3.7 セキュアなデータ交換（Secure Data Exchange）	本ガイドライン（案）に対する肯定的な御意見として承ります。

提出No.	No.	提出者	提出意見	御意見に対する考え方
13	56	企業	翻訳） Comment： Vulnerability managementやPatch managementは重要なセキュリティ対策ですが、OEM（装置メーカー）側では必ずしも広く導入されていません。そのため、OEMが脆弱性管理やパッチ管理を十分実施していない場合でも、デバイスメーカー（DM）やファウンドリー側がネットワークセキュリティの補完的なコントロール（Compensating Controls）を構築する責任があります。 Description： 3.4 脆弱性・脅威評価およびパッチ管理（Vulnerability/Threat Assessment and Patch Management）	第3.2.1節 ⑤『物理アクセスの制限（入室、持込み、接続）』への御意見として頂いておりますが、御意見の内容としては脆弱性評価であると認識しております。第3.2.1節 ①『装置ツールの資産管理と脆弱性評価』にて同等の内容を記載済みであるため、頂いた御意見については、原案の通りとさせていただきます。
13	57	企業	翻訳） Comment： ローカルアクセスはOEMおよびDM／ファウンドリーによって定義され、個別アカウントによる管理と、適切なアクセスプロセスの確立が必要です。また、DMはすべてのアクセスを監視する責任があります。 リモートアクセスは、DM／ファウンドリーのみによって定義されるべきであり、DM／ファウンドリーが監視・ログ取得・暗号化を行うセキュアなソリューションとプロセスが確立されている必要があります。リモートアクセスを有効化するための明確なプロセスも整備されるべきです。 Description： 3.6 ローカルおよびリモートアクセスの概要：不正アクセス防止のためのアカウント管理および特権権限管理の主要ポイントを整理します。 3.7 ローカルおよびリモートアクセスの概要：不正アクセスを防止するため、アカウント管理および特権権限管理の主要ポイントを整理します。	頂いた御意見を参考に、追記いたします。 修正箇所：第3.2.1節 ⑥（P.33 表3-4「特徴及び考慮すべき観点」）、第3.2.3節 ②（P.42 表3-8「特徴及び考慮すべき観点」）
13	58	企業	翻訳） Comment： 私たちはこれは良い提案だと考えますが、実装方法や主要なKPIについては不明瞭です。 Description： 3.10 セキュリティKPI（重要業績評価指標）の概要：持続可能なセキュリティ運用・管理を実現するためのセキュリティKPIを整理します。	本ガイドライン（案）に対する肯定的な御意見として承ります。
13	59	企業	翻訳） Comment： これに同意します。 Description： 3.8 予防・検知・対応の概要：ファブエリアを保護するための主要ポイントを整理します。これには、セキュリティ監視、サイバー攻撃の検知、封じ込め、復旧などが含まれます。	本ガイドライン（案）に対する肯定的な御意見として承ります。
13	60	企業	翻訳） Comment： これに同意します。OEMの技術者・エンジニア、DM／ファウンドリーのツール所有者、技術者およびエンジニアは、すべてサイバーセキュリティトレーニングの対象とすべきです。ツール設備へアクセスするすべての要員は、サイバーセキュリティ意識向上およびトレーニングに含める必要があります。 Description： 3.9 ユーザー意識向上トレーニングの概要：新たな脅威に適切に対応できるよう、ユーザー教育およびトレーニングの主要ポイントを整理します。	本ガイドライン（案）に対する肯定的な御意見として承ります。
13	61	企業	翻訳） Comment： 現時点では、E187の対象範囲は工場向けおよび内部のPC／コンピュータのみです。PLCや内部コントローラはE187およびセキュリティ検討の対象外となっています。しかし、OEMはPLCや内部コントローラと連携するソフトウェアに対してセキュアコーディングを実施し、これらの機器を出荷前に可能な限りセキュアにするよう十分な配慮が必要です。 Description： 図4-2. ファブエリア資産の構成	本ガイドライン（案）はE188およびE187による構成管理範囲に照らし併せて作成しているため、頂いた御意見については、原案の通りとさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
13	62	企業	翻訳） Comment： これに同意します。コンプライアンスについてはSEMI SMCC E187ガイダンスドキュメントを参照してください。脆弱性管理はE187の一部ですが、OEMによるツール機器への導入は遅れています。 SCAPについても言及されていますが、今後の継続性が不透明であり、定期的なサポートやアップデートも行われていません。SEMI SMCCでは、コンソーシアムからのフィードバックを基に、代替となる脆弱性スキャナや手法の推奨も検討しています。例として、CISベンチマーク（CIS Benchmarks ）、OWASPリスト（OWASP Vulnerability Scanning Tools ）、Gartnerリスト（Gartner Vulnerability Assessment ）などがあります。 Description： 半導体デバイス工場向けの具体的な対策例として、設備メーカーとのフィールドサポートや保守契約に、SEMI E187およびSEMI E188で推奨されている設備・ツールの脆弱性対応に関する基本要件を参照し、脆弱性管理要件を含めることが可能です。この方法により、運用体制や脆弱性の特定フレームワークを効率的に確立することができます（SEMI E187「脆弱性緩和」第9.2章およびSEMI E188「製造装置の脆弱性確認」第9.2章を参照）。 設備・ツールや部品の数が多い場合、有効な方法の一つとして、脆弱性スキャニングツール（例：SCAPスキャナ）を用いて、現在どのように脆弱性が扱われているか（追加防御策の有無も含め）を特定することが挙げられます。また、SEMI E188の基本要件に従い残存する脆弱性を特定する方法も有効です（SEMI E188第9.4章「NIST Security Content Automation Protocol (SCAP)」参照）。 なお、脆弱性スキャンツールを利用する場合、アクティブスキャン方式のツールでは一部の設備・ツールで性能低下や停止が発生する可能性があるため、工場はスキャン実施前に、使用するスキャン方式の選定やスキャン日時の調整など、運用面の詳細を検討・決定する必要があります。	頂いた御意見を参考に、追記いたします。 修正箇所：第4.1.3節（P.63）
13	63	企業	翻訳） Comment： SMCC WG5による脆弱性管理分野での活動状況については把握していません。WG5はすでに解散している可能性もあります。SEMIに現状について確認をお願いします。	頂いた御意見を参考に、修正いたします。 修正箇所：第4.1.4節（P.64）
13	64	企業	翻訳） Comment： 下記のMETIリファレンスアーキテクチャ図について、原則として同意します。OT領域のパデューモデルおよびITモデルは正しい構成に見えます。 以前、SEMI SMCCおよびMETI SATASプロジェクト向けに、非常に類似したIT／パデューリファレンスモデルを構築したことがあります。下記をご参照ください。  Description： 表2-1. パデューモデルとCPSFの6要素	本ガイドライン（案）に対する肯定的な御意見として承ります。
14	65	個人	必須の国際規格と通報・統治・KPIが抜けています。 投資条件とガイドライン適合を直結し、“デジタル・バイ・デフォルト”と“レガシー一掃”を国家投資のゲートにしてください。 これで初めて「2030年15兆円」の実行可能性に近づきます。 ガイドライン全体：セキュリティの基本不在。セキュリティの 4 領域の技術のみ重視されている印象であり、人・組織・物理が薄い。ISO 27001セキュリティのCIAおよび4つ、真正性・責任追跡性・否認防止・信頼性も重視すべき。 理由 •本ガイドライン案はネットワーク中心で人的・物理的要因への記述が薄く、国際規格や現場実情との乖離が大きい。国際規格マッピング、NIST SP 800-82 Rev.3適用、IEC 62443の人的資源要件、国際制度との整合（SBOM含む）、職場文化改革を同時に進めることで、実効性あるOTセキュリティ基盤が構築できる。 本ガイドラインはNIST CSF 2.0のみに依拠せず、NIST SP 800-82 Rev. 3（Guide to OT Security）の適用を明記し、今後の“potential updates”を踏まえて実装ガイドを継続更新すべき •サイバー攻撃など、人為的な脅威は工場や企業の安全に関わる問題であり、組織的な対応が求められるはずです。技術だけでは防げません。	本ガイドライン（案）は各社がセキュリティ対策の検討をする際の参考資料として作成しており、ご指摘いただいた国際規格との詳細な整合性の明記等については、本ガイドライン（案）が主眼とする範囲とは異なるため、頂いた御意見については、原案の通りとさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
14	66	個人	第1章「背景・目的」、図1-6「国内外の標準規格との関係」、3.3「組織・ヒト側面」共通：OTセキュリティに必須な国際規格の欠如：ISA/IEC 62443／NIS2／NIST SP 800-82 Rev.3を必須にすべき。	本ガイドライン（案）は、NIST CSF2.0半導体製造プロファイル、E187、IEC62443等のグローバル業界セキュリティ規格と整合させて作成しているため、頂いた御意見については、原案の通りとさせていただきます。
14	67	個人	第1章：過去の延長線上の発想ではなく、現状の国際競争構造を踏まえた課題設定に改めるべき 理由 第1章では、日本半導体産業は素材・装置で優位性を持つ一方、設計・量産は米中韓依存という構造にあり、「黄金期の再来」ではなく「高速で寿命の短い国際競争期」にあります。この現実を背景に置かない限り、適切なリスク分析・対策設計はできません。	本ガイドライン（案）は、半導体デバイス工場におけるサイバーセキュリティのリスクベースのガイドラインであり、検討会にて半導体関連企業や主要な半導体関連企業に参加いただき、現状から課題を抽出し作成したものです。そのため、頂いた御意見については、原案の通りとさせていただきます。
14	68	個人	第2章：CPSFを前提とする記述が多いが、多様性、多文化環境におけるセキュリティ運用の具体策が必要 理由 第2章のCPSFは経産省内の用語に留まっており、部外者が理解しづらいです。海外委託・コミュニケーション不足などの人的・組織的要因こそがOT運用のボトルネックであり、これを前提に対策を策定すべき。 2.1.セキュリティ意識向上の欠落 　現案はアクセス制御・脅威検知・脆弱性管理は述べても、従業員のセキュリティ意識向上策が不足しています。教育・研修はIEC 62443-2-1にも明記される必須項目であり、特に非正規雇用や多国籍労働環境では標準化教育が欠かせません。 2.2.依存しない設計の必要性 　OS依存を避けたISA-95（IEC 62264）モデル準拠のシステム設計、日本語依存を避けるISO 7010準拠の安全表示、ヒトに依存しない自動化・リモート対応が不可欠。	頂いた御意見を参考に、追記いたします。 修正箇所：第3.3節 ①（P.45 表3-10「特徴及び考慮すべき観点」）
14	69	個人	第4章：資産・人的要因の定義拡張が必要。資産を「設備・金銭・機密情報」に限定せず、「人材能力・安全・職場環境・ブランド価値」等の無形資産も管理対象に含めること。BCPにおいては、人的移動の削減や自動化による人的リスク低減策を明記すべき。 理由 •組織崩壊および旧3K（きつい、汚い、危険）をなくし、透明性を上げてください。 •中小企業の割合は99.7%です。ほぼ中小企業なので、大企業ほど潤沢な金も高度な人材も足りません。レガシー環境がのこり、セキュリティリスクの元です。 •国際規格未整備、セキュリティの偏り、人・組織・物理の欠落では、現場も委託先も動けません。	第4章は、半導体デバイス工場におけるOTセキュリティの具体的対策事例を記載しています。OTセキュリティの基準として資産（装置ツール）の重要度は、「表4-2. 装置ツールの重要度」にリスク領域と経営資源について明記しているため、頂いた御意見については、原案の通りとさせていただきます。
14	70	個人	第3章（リスクの例示：有害化学物質や高電圧・高温機器等の人身・環境リスク） 「安全（SIS/ISD）×セキュリティ（62443）」の二階建てを本文に明記し、ヒヤリハットの“未然阻止KPI”（例：SIS有効性、誤動作率、検知→隔離までの中央値）を年次開示してください。 理由 ・本案は危害源を列挙する一方、未然防止の体系（SIS/ISD）の実装・監査指標が不十分。 ・事故・ヒヤリハットは継続発生。現実の安全実効性を指標化し、開示すべき •組織崩壊および旧3K（きつい、汚い、危険）をなくし、透明性と生産性を上げてください。 •中小企業の割合は99.7%です。ほぼ中小企業なので、大企業ほど潤沢な金も高度な人材も足りません。レガシー環境がのこり、セキュリティリスクの元です。 •国際規格未整備、セキュリティの偏り、人・組織・物理の欠落では、現場も委託先も動けません。 •横串の効いたMECE運用は、無駄・ムラを無くし、迅速な経営判断とセキュリティ向上を両立させます。 •多くの産学連携により、高度な人材が結集するなら、内閣府の目標は前倒しで達成可能なはずです。 •高度人材の活用で製造工程の人員はより安全な業務へ移行でき、生産性と人の生活の両立が可能です。	第3章は、半導体デバイス工場のリファレンスアーキテクチャを基に、各領域の特徴と考慮点を踏まえ、各社のOTセキュリティのリスクベースの確認を行うことを想定して作成しています。工場全体のリスク視点を目的としたものではなく、個別の領域に焦点を当てております。そのため、頂いた御意見については、原案の通りとさせていただきます。

提出No.	No.	提出者	提出意見	御意見に対する考え方
14	71	個人	補足回答：対象工場は日本でどれだけ？ 単一の公的台帳はありません。総務省e-Statの「日本標準産業分類」に基づき、2813（半導体素子）／2814（集積回路）等の“事業所数”を経済センサスで集計するのが公式に近い積み上げ手順です（SEAJ統計は工場数を直接は出していません）。本ガイドラインにはこの集計手順と年次更新を付録化することを提案します。 サイバー攻撃など、人為的な脅威は工場や企業の安全に関わる問題であり、組織的な対応が求められるはずです。技術だけでは防げません。 第1章では、日本半導体産業は素材・装置で優位性を持つ一方、設計・量産は米中韓依存という構造にあり、「黄金期の再来」ではなく「高速で寿命の短い国際競争期」にあります。この現実を背景に置かない限り、適切なリスク分析・対策設計はできません。 第2章のCPSFは経産省内の用語に留まっており、部外者が理解しづらいです。海外委託・コミュニケーション不足などの人的・組織的要因こそがOT運用のボトルネックであり、これを前提に対策を策定すべき。 2.1.セキュリティ意識向上の欠落 　現案はアクセス制御・脅威検知・脆弱性管理は述べても、従業員のセキュリティ意識向上策が不足しています。教育・研修はIEC 62443-2-1にも明記される必須項目であり、特に非正規雇用や多国籍労働環境では標準化教育が欠かせません。 2.2.依存しない設計の必要性 　OS依存を避けたISA-95（IEC 62264）モデル準拠のシステム設計、日本語依存を避けるISO 7010準拠の安全表示、ヒトに依存しない自動化・リモート対応が不可欠。 第4章では、資産価値を金銭・設備・機密情報に限定していますが、実際には「人材の健康・安全」「職場環境」「ブランド価値」等も損害対象。特に安全面では、自動化や人的移動削減で災害・事故・離職を減らす施策を優先すべき。 •組織崩壊および旧3K（きつい、汚い、危険）をなくし、透明性を上げてください。 •中小企業の割合は99.7%です。ほぼ中小企業なので、大企業ほど潤沢な金も高度な人材も足りません。レガシー環境がのこり、セキュリティリスクの元です。 •国際規格未整備、セキュリティの偏り、人・組織・物理の欠落では、現場も委託先も動けません。 現時点で「日本の半導体デバイス工場数」の公的な一元台帳が存在しません。母集団推計は、経済センサス（2021）や工業統計（2020など）の日本標準産業分類の細分類（例：2813「半導体素子製造業」、2814「集積回路製造業」）に基づく事業所数で上限・下限をとる形で可能ですが、本ガイドラインの「対象（例：製造ウェハ/アッセンブリ/後工程、クリーンルーム保有等）」と完全一致しません。したがって、適用対象の定義と台帳の整備・年次公表を本案に組み込み、監査サンプリングの枠組みと併せて制度化することを強く要望します。 「計画どおりの稼働＋人材・電力・水・ESGの詰まり解消」できれば可能では。組織崩壊、カジュアルに言えばブラック企業＋旧３K（きつい、汚い、危険）とレガシー環境が揃っては発展しません。 政府は「AI・半導体産業基盤強化フレーム」で2030年度までに10兆円超の公的支援と官民50兆円超投資を掲げていますが、これを規格適合・レガシー撤去・人材安全KPIと連動させ、NIS2型の通報・IFRS開示まで接合しない場合、遅延・コスト超過・事故で未達リスクが高まります。 （いただいたリンクは省略させていただきます）	本ガイドライン（案）は、半導体サプライチェーン全体のサイバーセキュリティ対策の基本指針を示すことを目的としており、台帳整備や監査手法の制度化、教育研修の具体策など、個別の課題に踏み込むことはその範囲を超えるものと考えます。これらの課題は、別の政策や取り組みの中で検討されるべき事項と判断し、頂いた御意見については、原案の通りとさせていただきます。