経済産業省

資料9

# 半導体産業における
# セキュリティ対策基準について

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

# 半導体産業におけるセキュリティ対策基準の目的と方針

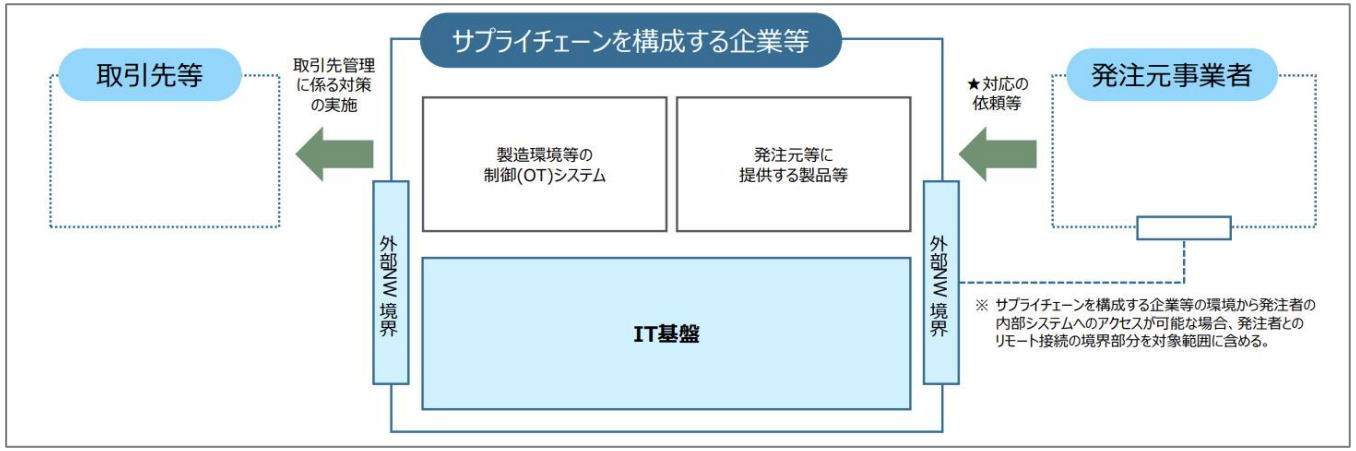
**目的**

- 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づ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以上のIT項目（基準）に加えて、半導体工場特有の工場におけるOT項目（基準）を加えることとしたい
  - 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を活用することとしたい
  - OT項目：作業部会にてOTセキュリティガイドライン（案）の第3章より重要な項目を数個程度で選定した

※本資料では、半導体デバイスメーカー向けの基準を想定している




【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対象範囲】

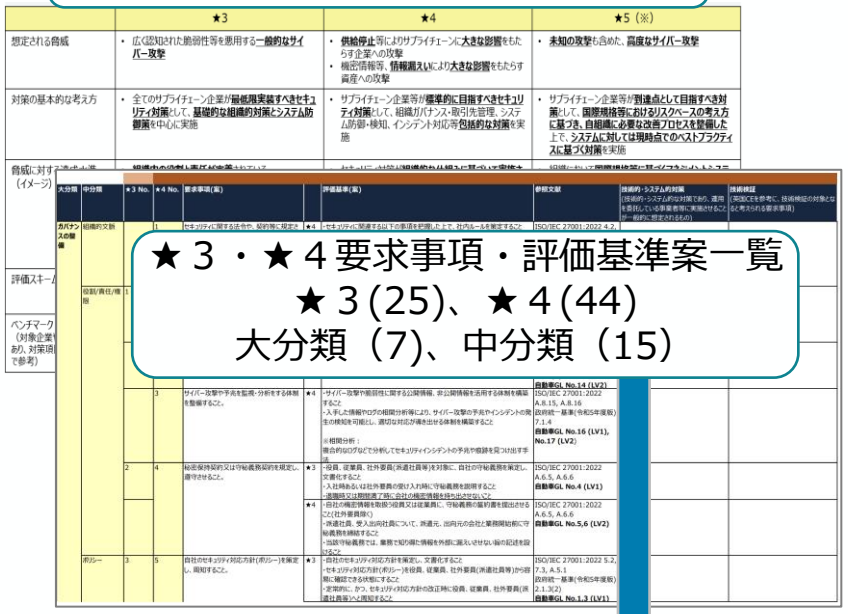
サプライチェーン強化に向けたセキュリティ対策評価制度制度の対象範囲として想定するもの

他の制度・ガイドライン等に基づき対策を行うことを想定するもの

「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構築に向けた中間取りまとめ」資料より

# IT、OT基準の選定方法

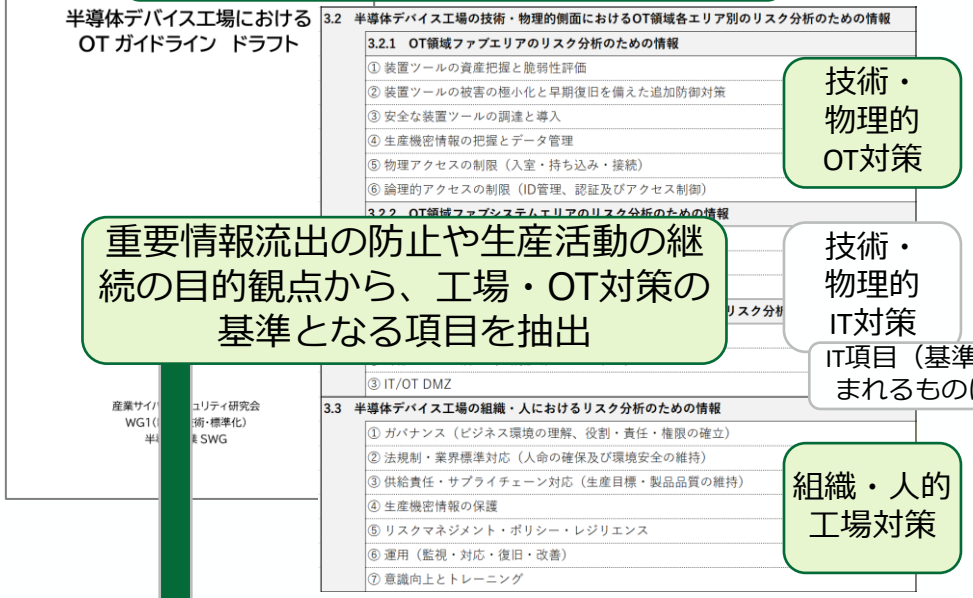
サプライチェーン強化に向けた
セキュリティ対策評価制度



★３・★４要求事項・評価基準案一覧
★３(25)、★４(44)
大分類（7)、中分類（15）

**44項目（=★4）**
※半導体デバイスメーカ向けを想定

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第3章



重要情報流出の防止や生産活動の継続の目的観点から、工場・OT対策の基準となる項目を抽出

技術・物理的 OT対策

技術・物理的 IT対策

IT項目（基準）に含まれるものは除外

組織・人的 工場対策

**数項目**
※半導体デバイスメーカ向けを想定

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

# 半導体産業におけるセキュリティ対策基準の対象範囲

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<br>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 | **★４（４４項目）** | **６項目** |
| 装置メーカー | 今後検討 | 今後検討 |
| 部素材メーカー | 今後検討 | 今後検討 |

# OT要求事項の項目（案）の抽出方法

| サプライチェーン対策評価制度 | | | | 半導体産業における対策評価制度 | | OTガイドライン３章 | 工場チェックリスト |
|---|---|---|---|---|---|---|---|
| 大分類 | | 中分類 | | 候補 | OT要求事項の項目（案） | | |
| 1 | ガバナンスの整備 | 1-1 | 組織的文脈 | | 工場のOT領域におけるセキュリティ対策の検討・企画に必要な**経営目標、外部要件、内部要件/状況を整理**すること。 | 3.3.①<br>3.3.② | 0-1 |
| | | 1-2 | 役割/責任/権限 | ● | 工場のOT領域におけるセキュリティ検討組織や、担当者が準備されており、**責任と業務内容が明確化**されていること。**事業継続計画（BCP）**が策定されており、セキュリティ事故発生時の体制が準備されていていること | 3.3.⑤ | 1-3<br>1-4 |
| | | 1-3 | ポリシー | | | | |
| | | 1-4 | 監督 | | | | |
| 2 | 取引先管理 | 2-1 | サイバーセキュリティサプライチェーンリスクマネジメント | | **サプライチェーン**（装置メーカー、部素材メーカー、設備メーカーなど）における工場のOT領域への**脅威、影響度、対応状況**（内部及び/または外部監査実施など）が把握できていること。 | 3.3.③ | 4-4 |
| | | | | | 工場のOT領域に導入する資産に対して、**一定のセキュリティ基準を満たしているかを判定するプロセスや受入検査**があること。 | 3.2.1.③ | 4-5 |
| 3 | リスクの特定 | 3-1 | 資産管理 | ● | 工場のOT領域における**業務・保護対象の資産の整理**を行い、管理すべき資産及び重要度の設定を行うこと。 | 3.2.1.① | 0-2 |
| | | 3-2 | リスクアセスメント | ● | 工場のOT資産に対する攻撃手法や脆弱性を特定し、追加防御隊対策含めた管理体制、管理プロセスを定めること。 | 3.2.1.① | 2-8 |
| 4 | 攻撃等の防御 | 4-1 | アイデンティティ管理とアクセス制御 | | 工場のOT領域各システムにおける**運用アカウントと保守用特権アカウントの運用ルール**を定めること。保守業者を含めた**人の異動に伴うアクセス権の管理ルール**を定めて、運用すること。 | 3.2.1.⑦ | 2-10<br>2-11 |
| | | 4-2 | 意識向上及びトレーニング | | 工場のOT領域に関する**脅威の動向**などについて、定期的に情報提供を受けたり、勉強会を開いたりするなどの**現場教育**を行っていること。 | 3.3.⑦ | 1-5 |
| | | 4-3 | データセキュリティ | ● | 工場で取り扱う機密情報（顧客の設計情報や生産に関するレシピ情報等）**の対象及び保管場所を把握を把握**し、情報漏洩を防ぐ適切なデータ保護を行うルールを定め、周知すること。 | 3.2.1.④<br>3.3.④ | 0-2 |
| | | | | | 工場のOT領域に対して完全で早期復旧を想定した**バックアップ**を行い、**バックアップデータは保護された場所に格納**するとともに、**復旧テスト**を行っている。また、その手順が明確化されていること。 | 3.2.2.② | 2-13 |
| | | 4-4 | プラットフォームセキュリティ | ● | 工場のOT領域を守るべき要件や、業務・保護対象の収集・整理結果に基づき、**想定脅威に対する防御対策（物理対策含めた多層防御、マイクロセグメンテーション、ふるまい検知等を含む）**を行うこと。<br>工場のOT領域における**物理的なアクセス（入退館・入退室、持ち込み、接続）**について重要度の高いエリアや資産への物理的なアクセスについてレベル分けなど十分な対策を行っていること。 | 3.2.1.②<br>3.2.1.⑤ | 0-3<br>3-4 |
| 5 | 攻撃等の検知 | 5-1 | 継続的モニタリング | ● | 工場のOT領域における、**ネットワークや物理的侵入の初期段階を捉えた検知**を行い、被害の封じ込め、早期復旧に対する体制の整備と管理ルールを定め運用すること。 | 3.3.⑥ | 3-8 |
| | | 5-2 | 有害イベントの分析 | | | | |
| 6 | インシデントへの対応 | 6-1 | インシデントマネジメント | | | | |
| 7 | インシデントからの復旧 | 7-1 | インシデント復旧計画の実行 | | | | |

※工場チェックリスト：経済産業省『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』チェックリスト

抽出方法

- サプライチェーン対策評価制度の大分類から、網羅性の観点から１つを候補として抽出
- OTガイドライン3章の中から、作業部会で要望をいただき具体的対策事項を記載（OTガイドライン4章）した項目について抽出
- 第4回作業部会のご意見、重要情報流出観点から 4-3データセキュリティの項目を追加
- 第5回作業部会のご意見、OT領域の対策観点から、2-1 サイバーセキュリティサプライチェーンリスクマネジメントの項目を削除

# OT評価基準（案）（1/4）

- 『OT項目 評価基準（案）』（薄緑塗りつぶし部分）をご確認いただきたい

| 大分類 | | 中分類 | | IT項目・OT項目<br>要求事項 | IT項目 評価基準(案)<br>OT項目 評価基準(案) | 候補 | OTガイドライン | 工場チェックリスト |
|---|---|---|---|---|---|---|---|---|
| 1 | ガバナンスの整備 | 1-2 | 役割/責任/権限 | セキュリティを担当する部署及び従業員を決定し、責任及び権限を割り当てること。 | □ セキュリティを統括する役員(CISO 等)やセキュリティ担当部署の役割・責任を明確化すること<br>□ 平時のセキュリティ推進活動に必要な連絡先リストを整備すること<br>□ セキュリティリスクは、経営に重大な影響を及ぼすことを理解し、情報セキュリティ委員会等の経営判断ができる体制を設置していること平時のセキュリティ推進活動に必要な連絡先リストを整備すること | | | |
| | | | | | □ **工場**を統括する**責任者**（役員、工場長 等）や**工場セキュリティ担当部署の役割・責任を明確化**すること<br>□ **工場セキュリティリスク**は、経営に重大な影響を及ぼすことを理解し、サイバーセキュリティのリスクを考慮した**事業継続計画（BCP）が策定**されていること<br>□ 工場セキュリティ**事故発生時**の**対応体制・連絡先リスト**を**整備**すること | ● | 3.3.⑤ | 1-3<br>1-4 |

# OT評価基準（案）（2/4）

| 大分類 | 中分類 | IT項目・OT項目<br>要求事項 | IT項目 評価基準(案)<br>OT項目 評価基準(案) | 候補 | OTガイドライン | 工場チェックリスト |
|---|---|---|---|---|---|---|
| 3 リスクの特定 | 3-1 資産管理 | ハードウェア、OS、ソフトウェアの情報に関する一覧を作成すること。 | □ 適用範囲内のパソコン、シンクライアントの製造元とOS及び台数を一覧化すること<br>□ 適用範囲内のサーバ、仮想サーバ、ハイパーバイザの製造元とOS及び台数を記入すること<br>□ 情報機器、OS、ソフトウェアについて、導入、設置、ネットワーク接続、セキュリティパッチ適用等のルールを含む管理ルールを定め、文書化していること<br>□ 適用範囲内のスマートデバイスの製造元とOS及び台数を一覧化すること<br>□ 重要なシステムを構成する機器について、設定情報を一覧に含めること | | | |
| | | | □ **OT領域の資産**について、情報機器、OS、ソフトウェアの**構成管理**方法を定め、**一覧化**していること<br>□ **OT領域の資産**について、導入、設置、ネットワーク接続、セキュリティパッチ適用等のルールを含む**管理ルールを定め、文書化**していること<br>□ **OT領域の資産**について、レジリエンスを考慮した**重要度**を定め、**一覧化**していること | ● | 3.2.1.① | 0-2 |
| | 3-2 リスクアセスメント | 脆弱性の管理体制、管理プロセスを定めること。 | □ 脆弱性情報の収集から対応まで担当部署の役割・責任を明確化すること<br>□ 脆弱性情報/脅威情報を収集する情報源、ツール、頻度を定めること<br>□ 収集した情報の対応要否判断基準・対応手順を定め、文書化すること<br>□ 管理対象の情報機器における脆弱性の残存状況を把握すること<br>□ 対応履歴を記録し、月次でチェックすること | | | |
| | | | □ **OT領域の資産**について、**脆弱性情報の収集から対応**まで担当部署の**役割・責任を明確化**すること<br>□ **OT領域の資産**について、**脆弱性情報/脅威情報**を収集する**情報源、ツール、頻度**を定めること<br>□ **OT領域の資産**について、収集した**情報の対応要否判断基準・対応手順を定め**、**文書化**すること<br>□ **OT領域の資産**について、脆弱性情報/脅威情報と実施している対策を比較・検討して、**生産ビジネス影響度**を**把握**すること | ● | 3.2.1.① | 2-8 |

# OT評価基準（案）（3/4）

| 大分類 | 中分類 | IT項目・OT項目<br>要求事項 | IT項目 評価基準(案)<br>OT項目 評価基準(案) | 候補 | OTガイドライン | 工場チェックリスト |
|---|---|---|---|---|---|---|
| 4 攻撃等の防御 | 4-3 データセキュリティ | 重要データを適切な場所に保管するようルールを定め、周知すること。 | □ マルウェアによる被害を受けた場合に業務に支障をきたす重要データはパソコン以外の社内ネットワーク上の相対的に安全な区域にあるサーバに保管するようルールを定め、役員、従業員、社外要員(派遣社員等)、受入出向者を対象に周知すること | | | |
| | | | □ 工場で取り扱う機密情報（顧客の設計情報や生産に関するレシピ情報など）**<u>の対象を明確化</u>**すること<br>□ 工場で取り扱う機密情報（同上）の**<u>保管場所や通信経路（データフロー）を把握</u>**し、情報流出を防ぐための適切な**<u>データ保護ルールを定める</u>**こと<br>□ 工場で取り扱う機密情報（同上）を守るために定めた保護ルールを、**<u>機密情報を取り扱う対象者へ周知する</u>**こと | ● | 3.2.1.④<br>3.3.④ | 0-2 |
| | 4-4 プラットフォームセキュリティ | ハードウェア・ソフトウェア等の安全な構成を確立し、維持すること。 | □ パソコン、サーバ、スマートデバイスで使用していないソフトウェアをすべて削除又は無効化すること<br>□ すべてのシステムで自動実行(auto-run)又は自動再生(auto-play)を無効にすること<br>□ サーバ及びネットワーク機器の設定変更を申請・承認制にすること<br>□ 不要サービスを無効化すること<br>□ デフォルトユーザ ID の利用を停止すること<br>□ 利用するOS及びソフトウェアについて、ベンダーによる推奨セキュリティ設定を参考に設定を行うこと | | | |
| | | | □ OT領域の**<u>資産に対する</u>**セキュリティ対策状況を把握し、**<u>重要度に応じた防御対策</u>**を**<u>行う</u>**こと（物理対策を含めた多層防御、マイクロセグメンテーション、ふるまい検知等）<br>□ OT領域における重要度の高いエリアや資産への物理的なアクセスについて**<u>レベル分けなど十分な対策を行う</u>**こと（入退館・入退室、持ち込み接続等） | ● | 3.2.1.②<br>3.2.1.⑤ | 0-3<br>3-4 |

# OT評価基準（案）（4/4）

| 大分類 | 中分類 | IT項目・OT項目<br>要求事項 | IT項目 評価基準(案)<br>OT項目 評価基準(案) | 候補 | OTガイドライン | 工場チェックリスト |
|---|---|---|---|---|---|---|
| 6 インシデントへの対応 | 6-1 インシデントマネジメント | あらかじめ定めた手順に沿ってセキュリティインシデントに対応すること。 | □ セキュリティインシデントへの対応手順を作成し、文書化すること<br>□ 対応手順には組織の必要に応じて以下の手順を含んでいること<br>①発見報告、 ②初動、③調査・対応、④復旧、⑤最終報告<br>□ セキュリティインシデントの基準や社内外組織との連絡先、ルートを明確化すること<br>□ セキュリティインシデント発生時におけるセキュリティを統括する役員(CISO 等)やセキュリティ担当部署の役割・責任を明確化し、文書化すること<br>□ セキュリティインシデントの報告フォーマットを整備すること<br>□ 年１回以上、若しくは、社内外で重大なセキュリティインシデントが発生した際に、インシデント事例やその対応策を社内部署へ共有していること | | | |
| | | | □ 工場における**セキュリティインシデントへの対応手順**を作成し、**文書化**すること<br>□ 対応手順には、**被害の最小化および早期復旧に対する体制の整備と管理ルール**を含んでいること<br>□ OT領域で検知されたアラートが、**セキュリティインシデントに該当する**か否かを判断する体制を整備すること<br>□ 工場セキュリティインシデントの**基準や社内外組織との連絡先、ルートを明確化**すること<br>□ 工場セキュリティインシデント発生時における、対応責任者（役員や工場長）やセキュリティ担当を含めた**関係各部署の役割・責任を明確化し、文書化**すること<br>□ インシデント対応手順及び報告は、**事業継続計画**に即したものとすること | ● | 3.3.⑥ | 3-8 |

METI

Ministry of Economy, Trade and Industry