

半導体デバイスメーカーに対するセキュリティ要求事項

商務情報政策局 サイバーセキュリティ課・情報産業課

半導体デバイスメーカーに対するセキュリティ要求事項

- 半導体デバイスメーカーに対するセキュリティ要求事項について、IT項目は「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（SCS評価制度）」における★4項目（43項目）を要件とし、OT項目は「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」を参照し作成した項目（6項目）を要件とする。
- なお、SCS評価制度の開始（2027年3月予定）以降は★4取得が要件となるが、制度開始までは、SCS評価制度の★4項目に相当するセキュリティ対策を実施することを要件とする。

IT項目（43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制度構築方針における★4項目^{*1}を参照）

- ガバナンスの整備：6項目
 - 継続的改善に資するリスク管理体制の構築
- 取引先管理：5項目
 - 取引先の管理・把握及び取引先との役割・責任の明確化
- リスクの特定：6項目
 - 脆弱性など最新状況の把握と反映
- 攻撃等の防御：21項目
 - 多層防御による侵入リスクの低減
- 攻撃等の検知：3項目
 - 迅速な異常の検知
- インシデントへの対応：1項目
 - インシデント発生に備えた対応手順の整備
- インシデントからの復旧：1項目
 - インシデントからの復旧手順等の整備

OT項目（6項目）

（※本資料の第3-4頁を参照）

- ガバナンスの整備：1項目
 - セキュリティ担当部署・担当者への権限等割り当て
- リスクの特定：2項目
 - ハードウェア、OS、ソフトウェアの情報一覧作成
 - 脆弱性の管理体制、管理プロセスの策定
- 攻撃等の防御：2項目
 - 重要データの保管ルールの策定・周知
 - ハードウェア・ソフトウェア等の安全な構成確立・維持
- インシデントへの対応：1項目
 - あらかじめ定めた手順に沿ってインシデントへ対応

*1 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/20260327_report.html

より、エクセルファイル「★3★4要求事項及び評価基準」をダウンロードして参照してください。

OT項目 要求事項・要求項目（1/2）

大分類	中分類	OT項目 要求事項	OT項目 要求項目	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。	<ul style="list-style-type: none"> □ 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 □ 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 □ 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 1-4
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。	<ul style="list-style-type: none"> □ 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 □ 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 □ 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。	<ul style="list-style-type: none"> □ 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 □ 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 □ 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 □ 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項目 要求事項・要求項目（2/2）

大分類	中分類	OT項目 要求事項	OT項目 要求項目	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。	<ul style="list-style-type: none"> □ 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）の対象を明確化すること □ 工場で取り扱う機密情報（同上）の保管場所や通信経路（データフロー）を把握し、情報流出を防ぐための適切なデータ保護ルールを定めること □ 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、機密情報を取り扱う対象者へ周知すること 	3.2.1.④ 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。	<ul style="list-style-type: none"> □ OT領域の資産に対するセキュリティ対策状況を把握し、重要度に応じた防御対策を行うこと（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） □ 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レベル分けなど十分な対策を行うこと（入退館・入退室、持ち込み接続等） 	3.2.1.② 3.2.1.⑤	0-3 3-4
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。	<ul style="list-style-type: none"> □ 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 □ 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 □ 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 □ 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 □ 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 □ 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