経済産業省　内閣官房

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に関する 制度構築方針（案）

丸山満彦
2026.01.26

本日は

「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に関する制度構築方針（案）」の概要について経緯を踏まえて説明します。

“

発注者・受注者双方にとって、適切なセキュリティ対策の決定や対策状況の説明が容易・適切となる

発注企業のサプライチェーン・リスクの低減や、経済・社会全体でのサイバーレジリエンスの強化を図る

経済産業省　内閣官房
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に関する制度構築方針（案）

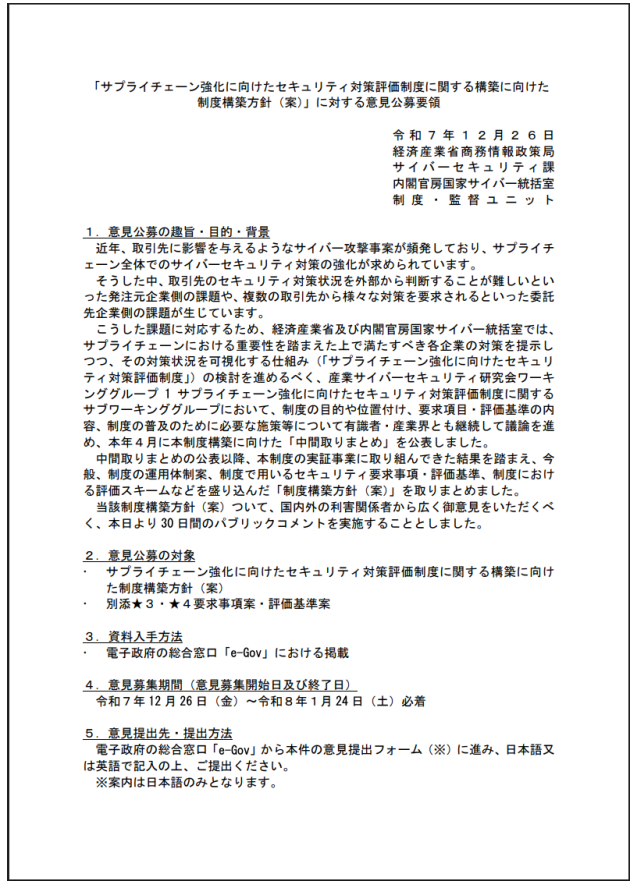
“

セキュリティ対策状況の可視化をする制度である

セキュリティ対策を競わせる格付け制度ではない

経済産業省　内閣官房
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に関する制度構築方針（案）

経済産業省、内閣官房が、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）に関する制度構築方針（案）とその評価基準案についての意見募集をした（2025.12.26）



「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に関する構築に向けた制度構築方針（案）」に対する意見公募要領

令和７年１２月２６日
経済産業省商務情報政策局
サイバーセキュリティ課
内閣官房国家サイバー統括室
制度・監督ユニット

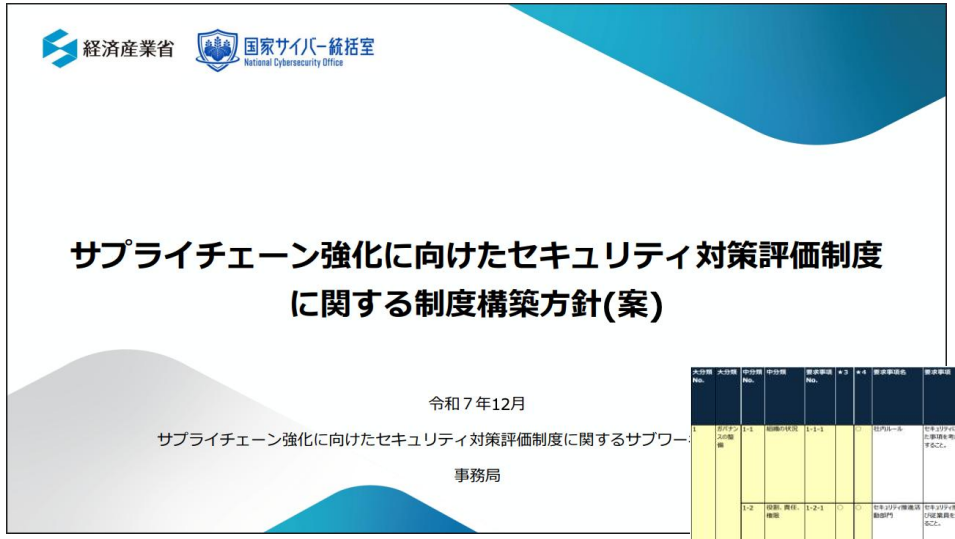
1．意見公募の趣旨・目的・背景
近年、取引先に影響を与えるようなサイバー攻撃事案が頻発しており、サプライチェーン全体でのサイバーセキュリティ対策の強化が求められています。
そうした中、取引先のセキュリティ対策状況を外部から判断することが難しいといった発注元企業側の課題や、複数の取引先から様々な対策を要求されるといった委託先企業側の課題が生じています。
こうした課題に対応するため、経済産業省及び内閣官房国家サイバー統括室では、サプライチェーンにおける重要性を踏まえた上で満たすべき各企業の対策を提示しつつ、その対策状況を可視化する仕組み（「サプライチェーン強化に向けたセキュリティ対策評価制度」）の検討を進めるべく、産業サイバーセキュリティ研究会ワーキンググループ１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に関するサプワーキンググループにおいて、制度の目的や位置付け、要求項目・評価基準の内容、制度の普及のために必要な施策等について有識者・産業界とも継続して議論を進め、本年４月に本制度構築に向けた「中間取りまとめ」を公表しました。
中間取りまとめの公表以降、本制度の実証事業に取り組んできた結果を踏まえ、今般、制度の運用体制案、制度で用いるセキュリティ要求事項・評価基準、制度における評価スキームなどを盛り込んだ「制度構築方針（案）」を取りまとめました。
当該制度構築方針（案）ついて、国内外の利害関係者から広く御意見をいただくべく、本日より 30 日間のパブリックコメントを実施することとしました。

2．意見公募の対象
・ 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に関する構築に向けた制度構築方針（案）
・ 別添★３・★４要求事項案・評価基準案

3．資料入手方法
・ 電子政府の総合窓口「e-Gov」における掲載

4．意見募集期間（意見募集開始日及び終了日）
令和７年 12 月 26 日（金）～令和８年１月 24 日（土）必着

5．意見提出先・提出方法
電子政府の総合窓口「e-Gov」から本件の意見提出フォーム（※）に進み、日本語又は英語で記入の上、ご提出ください。
※案内は日本語のみとなります。



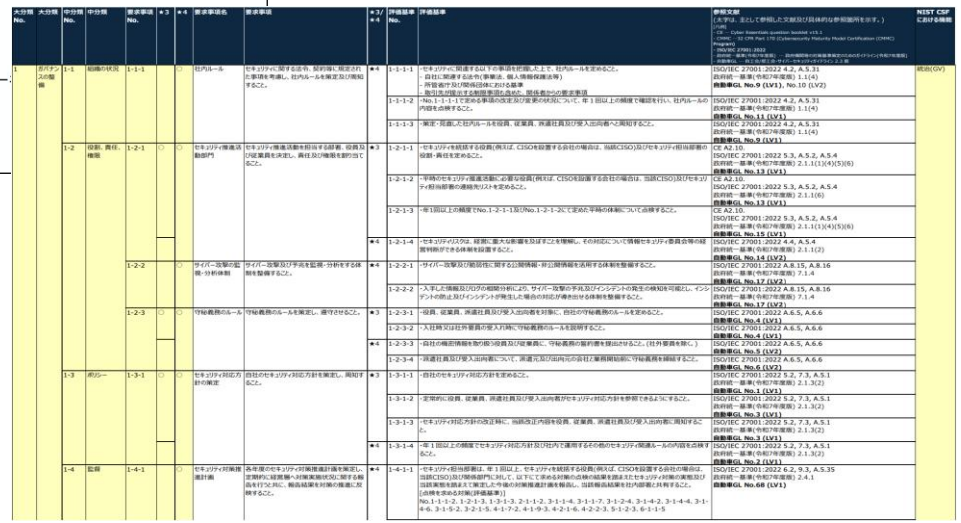
経済産業省　国家サイバー統括室
National Cybersecurity Office

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
に関する制度構築方針(案)

令和７年12月

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に関するサプワー

事務局



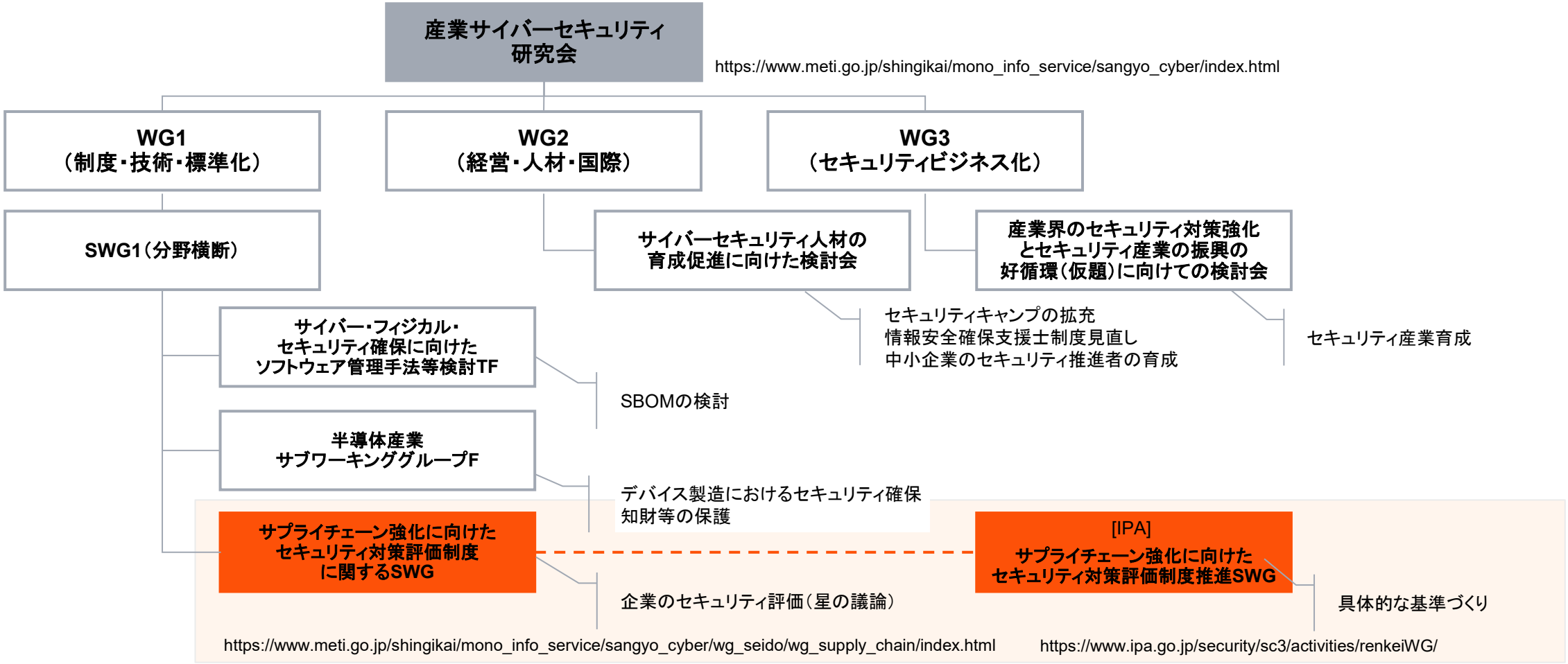
大分類 No.	大分類	中分類 No.	中分類	要求事項 No.	★3	★4	要求事項名	要求事項	★3/★4	評価基準 No.	評価基準	参照文献（主要3法、並びに参照した文献及び具体的な参照箇所を示す。）	NIST CSF 2.0における機能
1	ガバナンスの整備	1-1	組織の状況	1-1-1		○	社内ルール	セキュリティに関する法令、契約等に規定された事項を準拠し、社内ルールを策定及び周知すること。	★4	1-1-1-1	・セキュリティに関連する以下の事項を把握した上で、社内ルールを定めること。 ・自社に関連する法令（例：個人情報保護法等） ・所管省庁及び関係団体における基準 ・取引先の提示する制度要求に含まれ、関係者からの要求事項	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和7年度版) 1.1(4) **自動車GL No.9 (LV1)**, No.10 (LV2)	統治(GV)
										1-1-1-2	・No.1-1-1-1で定める事項の改定及び変更の状況について、年１回以上の頻度で確認を行い、社内ルールの内容を点検すること。	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和7年度版) 1.1(4) **自動車GL No.11 (LV1)**	
										1-1-1-3	・策定・見直した社内ルールを役員、従業員、派遣社員及び受入出向者へと周知すること。	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和7年度版) 1.1(4) **自動車GL No.9 (LV1)**	
		1-2	役割、責任、権限	1-2-1	○	○	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	★3	1-2-1-1	・セキュリティを統括する役員（例えば、CISOを設置する会社の場合は、当該CISO）及びセキュリティ担当部署の役割・責任を定めること。	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(1)(4)(5)(6) **自動車GL No.13 (LV1)**	
										1-2-1-2	・平時のセキュリティ推進活動に必要な役員（例えば、CISOを設置する会社の場合は、当該CISO）及びセキュリティ担当部署の連絡先リストを定めること。	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(6) **自動車GL No.13 (LV1)**	
										1-2-1-3	・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(1)(4)(5)(6) **自動車GL No.15 (LV1)**	
									★4	1-2-1-4	・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、その対応について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すること。	ISO/IEC 27001:2022 4.4, A.5.4 政府統一基準(令和7年度版) 2.1.1(2) **自動車GL No.14 (LV2)**	
				1-2-2	○		サイバー攻撃の監視・分析体制	サイバー攻撃及び予兆を監視・分析をする体制を整備すること。	★4	1-2-2-1	・サイバー攻撃及び脆弱性に関する公開情報・非公開情報を活用する体制を整備すること。	ISO/IEC 27001:2022 A.8.15, A.8.16 政府統一基準(令和7年度版) 7.1.4 **自動車GL No.17 (LV2)**	
										1-2-2-2	・入手した情報及び以下の観点分析により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が停止せる体制を整備すること。	ISO/IEC 27001:2022 A.8.15, A.8.16 政府統一基準(令和7年度版) 7.1.4 **自動車GL No.17 (LV2)**	
		1-2-3	○	○	守秘義務のルール	守秘義務のルールを策定し、徹守させること。	★3	1-2-3-1	・役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.4 (LV1)**	
										1-2-3-2	・入社時又は社外重責の受入れ時に守秘義務のルールを説明すること。	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.4 (LV1)**	
									★4	1-2-3-3	・自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。（社外重責を除く。）	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.5 (LV2)**	
										1-2-3-4	・派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結すること。	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.6 (LV2)**	
		1-3	約ポシー	1-3-1	○	○	セキュリティ対応方針の策定	自社のセキュリティ対応方針を策定し、周知すること。	★3	1-3-1-1	・自社のセキュリティ対応方針を定めること。	ISO/IEC 27001:2022 5.2, 7.3, A.5.1 政府統一基準(令和7年度版) 2.1.3(2) **自動車GL No.1 (LV1)**	
										1-3-1-2	・定期的に役員、従業員、派遣社員及び受入出向者がセキュリティ対応方針を参照できるようにすること。	ISO/IEC 27001:2022 5.2, 7.3, A.5.1 政府統一基準(令和7年度版) 2.1.3(2) **自動車GL No.3 (LV1)**	
										1-3-1-3	・セキュリティ対応方針の改定時に、当該改定内容を役員、従業員、派遣社員及び受入出向者に周知すること。	ISO/IEC 27001:2022 5.2, 7.3, A.5.1 政府統一基準(令和7年度版) 2.1.3(2) **自動車GL No.3 (LV1)**	
									★4	1-3-1-4	・年１回以上の頻度でセキュリティ対応方針及び付内で運用するその他のセキュリティ関連ルールの内容を点検すること。	ISO/IEC 27001:2022 5.2, 7.3, A.5.1 政府統一基準(令和7年度版) 2.1.3(2) **自動車GL No.2 (LV1)**	
		1-4	監査	1-4-1		○	セキュリティ対策推進計画	各年度のセキュリティ対策推進計画を策定し、定期的に経営層へ対策実施状況に関する報告を行うなど、報告結果を対策の機能に反映すること。	★4	1-4-1-1	・セキュリティ担当部署は、年１回以上、セキュリティを統括する役員（例えば、CISOを設置する会社の場合は、当該CISO）及び関係部門に対して、以下にて定める対策の点検の結果を踏まえたセキュリティ対策の実施及び当該実施を踏まえた策定した年度の対策推進計画を報告し、当該報告結果を社内部署と共有すること。 点検を定める対策（評価基準） No.1-1-1-2, 1-2-1-3, 1-3-1-3, 2-1-1-2, 3-1-1-4, 3-1-1-7, 3-1-2-4, 3-1-4-2, 3-1-4-4, 3-1-4-6, 3-1-5-2, 3-2-1-5, 4-1-7-2, 4-1-9-3, 4-2-1-6, 4-2-2-3, 5-1-2-3, 6-1-1-5	ISO/IEC 27001:2022 6.2, 9.3, A.5.35 政府統一基準(令和7年度版) 2.4.1 **自動車GL No.68 (LV1)**	

経済産業省：https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html
内閣官房：https://www.cyber.go.jp/policy/group/kihon-2/pubcom-scs2026.html

制度設計に関わっているSWG

経済産業省：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に関するSWG

IPA：SC3 業界連携WG 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推進SWG



何を目指しているのか？

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

背景（課題）

サプライチェーンを通じたセキュリティインシデントが頻発

企業の取引においてサイバーセキュリティ対策の担保が求められる

目指す制度

マークの取得を通じて、

- ビジネス・ITサービスサプライチェーンにおける適切なセキュリティ対策の実施を促す
- サプライチェーン全体でのセキュリティ対策水準の向上を図る。

★3	Basic	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的なシステム防御策と体制整備を中心に実施
★4	Standard	サプライチェーン企業等が標準的に目指すべきセキュリティ対策として、組織ガバナンス・取引先管理、システム防御・検知、インシデント対応等包括的な対策を実施
★5	Advanced	サプライチェーン企業等が到達点として目指すべき対策として、国際規格等におけるリスクベースの考え方に基づき、自組織に必要な改善プロセスを整備した上で、システムに対しては現時点でのベストプラクティスに基づく対策を実施

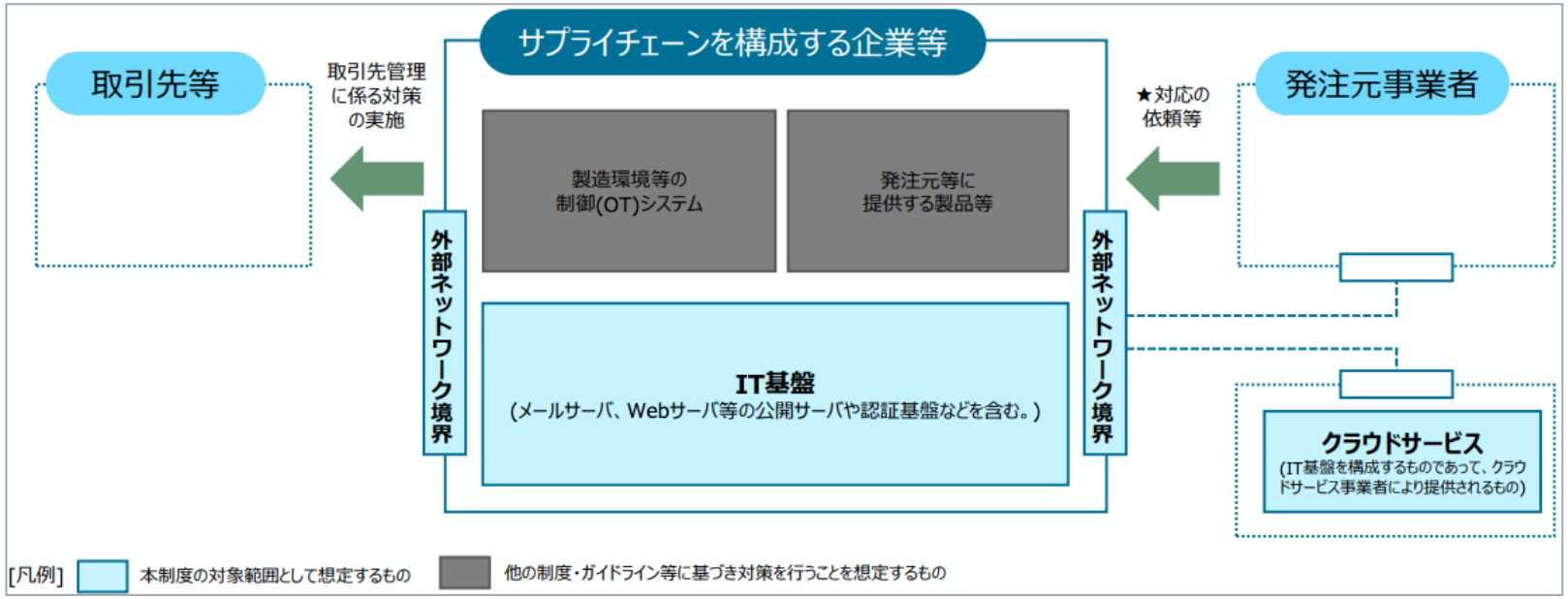
今回は★3, 4だけ

制度の対象範囲

サプライチェーンを構成する企業等の**IT基盤(クラウド環境で運用するものも含む)**が対象

製造環境等の制御(OT)システム、発注元等に提供する製品等は対象外

インターネット公開サーバ(Webサーバ、メールサーバ等)は適用範囲に必ず含める



◆適用範囲に含めないもの
- 製造環境等の制御(OT)システム (例:一方向セキュリティゲートウェイで外部ネットワークと区切られた製造拠点の制御システム)
- 発注元等に提供する製品等、自社のIT基盤に係るネットワークに接続していない機器

◆原則として適用範囲に含めるが、例外的に適用範囲に含めないことが許容され得るもの
- 本制度の要求事項を満たすことが困難なIT機器やソフトウェア(例:サポート期限切れのソフトウェア等)

※本事由により適用範囲から除外する場合は、具体的に除外理由を明記し、セキュリティ専門家(★3)又は評価機関(★4)は妥当性を評価すること。

要求事項・評価基準（案）の概要

★3は26の要求事項、83の評価項目
★4は44の要求事項、157の評価項目

大分類	★3	★4	NIST CSFにおける機能
ガバナンスの整備	**企業として最低限のリスク管理体制の構築** • 自社のセキュリティ担当の明確化 [No.1-2-1] • セキュリティ対応方針の策定 [No.1-3-1]	**継続的改善に資するリスク管理体制の構築** • 定期的な経営層への報告、不備の是正等 [No.1-4-1]	統治(GV)
取引先管理	**取引先に課す最低限のルール明確化** • 他社との機密情報の取扱い明確化 [No.2-1-2] • 接続している外部情報サービスの把握 [No.3-1-3]	**取引先の管理・把握及び取引先との役割・責任の明確化** • 機密情報共有先の把握 [No.2-1-1] • 重要な取引先等の対策状況把握 [No.2-1-3] • インシデント発生時の他社との役割等の明確化 [No.2-1-4]	
リスクの特定	**自社IT基盤や資産の現状把握** • 情報資産やネットワークの把握 [No.3-1-1,3-1-2] • 外部情報サービスの管理 [No.3-1-3]	**脆弱性など最新状況の把握と反映** • 脆弱性管理体制、管理プロセスの明確化 [No.3-2-1]	識別(ID)
攻撃等の防御	**不正アクセスに対する基礎的な防御** • ID管理手続、アクセス権限の設定[No.4-1-1,4-1-2] • パスワードの安全な設定及び管理 [No.4-1-4,4-1-5] • 内外ネットワーク境界の分離・保護 [No.4-5-1] **端末やサーバーの基礎的な保護** • 適時のアップデート適用、不要ソフトウェアの削除[No.4-4-1,4-4-4] • 端末等へのマルウェア対策 [No.4-4-1,4-4-4]	**多層防御による侵入リスクの低減** • 重要な保管データの暗号化 [No.4-3-1,4-3-2] • ログの収集・定期的な分析の実施 [No.4-4-3] • 社内システムにおける適切なネットワーク分離 [No.4-5-1] • 社外への不正通信の遮断(出口対策) [No.4-5-2]	防御(PR)
攻撃等の検知	**ネットワーク上の基礎的な監視等** • ネットワーク接続・データの監視[No.5-1-1]	**迅速な異常の検知** • 情報機器等の状態、挙動の監視・対応や分析[No.5-1-1,5-1-2]	検知(DE)
インシデントへの対応	**インシデント発生に備えた対応手順の整備** • インシデント対応手順の作成 [No.6-1-1]	*大分類「インシデントへの対応」において、★４での追加項目はなし	対応(RS)
インシデントからの復旧	**インシデント発生から復旧するための対策の整備** • インシデント発生から復旧するための対策の整備[No.7-1-1]	**インシデントからの復旧手順等の整備** • 復旧ポイント、復旧時間を満たす手順等の整備[No.7-1-1]	復旧(RC)

★3、★4の要求事項・評価基準（案）

詳細は、今年度確定する

大分類No.	大分類	中分類No.	中分類	要求事項No.	★3	★4	要求事項名	要求事項	★3/★4	評価基準No.	評価基準	参照文献 (太字は、主として参照した文献及び具体的な参照 [凡例] - CE … Cyber Essentials question booklet v15.1 - CMMC …32 CFR Part 170 (Cybersecurity Maturity Mode Program) - ISO/IEC 27001:2022 - 政府統一基準(令和7年度版) … 政府機関等の対策基準策定の - 自動車GL … 自工会/部工会-サイバーセキュリティガイドライン 2.3
1	ガバナンスの整備	1-1	組織の状況	1-1-1		○	社内ルール	セキュリティに関する法令、契約等に規定された事項を考慮し、社内ルールを策定及び周知すること。	★4	1-1-1-1	・セキュリティに関連する以下の事項を把握した上で、社内ルールを定めること。 - 自社に関連する法令(事業法、個人情報保護法等) - 所管省庁及び関係団体における基準 - 取引先が提示する制限事項も含めた、関係者からの要求事項	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和7年度版) 1.1(4) **自動車GL No.9 (LV1)**, No.10 (LV2)
										1-1-1-2	・No.1-1-1-1で定める事項の改定及び変更の状況について、年１回以上の頻度で確認を行い、社内ルールの内容を点検すること。	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和7年度版) 1.1(4) **自動車GL No.11 (LV1)**
										1-1-1-3	・策定・見直した社内ルールを役員、従業員、派遣社員及び受入出向者へと周知すること。	ISO/IEC 27001:2022 4.2, A.5.31 政府統一基準(令和7年度版) 1.1(4) **自動車GL No.9 (LV1)**
		1-2	役割、責任、権限	1-2-1	○	○	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。	★3	1-2-1-1	・セキュリティを統括する役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の役割・責任を定めること。	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(1)(4)(5) **自動車GL No.13 (LV1)**
										1-2-1-2	・平時のセキュリティ推進活動に必要な役員(例えば、CISOを設置する会社の場合は、当該CISO)及びセキュリティ担当部署の連絡先リストを定めること。	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(6) **自動車GL No.13 (LV1)**
										1-2-1-3	・年1回以上の頻度でNo.1-2-1-1及びNo.1-2-1-2にて定めた平時の体制について点検すること。	CE A2.10. ISO/IEC 27001:2022 5.3, A.5.2, A.5.4 政府統一基準(令和7年度版) 2.1.1(1)(4)(5) **自動車GL No.15 (LV1)**
									★4	1-2-1-4	・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、その対応について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すること。	ISO/IEC 27001:2022 4.4, A.5.4 政府統一基準(令和7年度版) 2.1.1(2) **自動車GL No.14 (LV2)**
				1-2-2		○	サイバー攻撃の監視・分析体制	サイバー攻撃及び予兆を監視・分析をする体制を整備すること。	★4	1-2-2-1	・サイバー攻撃及び脆弱性に関する公開情報・非公開情報を活用する体制を整備すること。	ISO/IEC 27001:2022 A.8.15, A.8.16 政府統一基準(令和7年度版) 7.1.4 **自動車GL No.17 (LV2)**
										1-2-2-2	・入手した情報及びログの相関分析により、サイバー攻撃の予兆及びインシデントの発生の検知を可能とし、インシデントの防止及びインシデントが発生した場合の対応が導き出せる体制を整備すること。	ISO/IEC 27001:2022 A.8.15, A.8.16 政府統一基準(令和7年度版) 7.1.4 **自動車GL No.17 (LV2)**
				1-2-3	○	○	守秘義務のルール	守秘義務のルールを策定し、遵守させること。	★3	1-2-3-1	・役員、従業員、派遣社員及び受入出向者を対象に、自社の守秘義務のルールを定めること。	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.4 (LV1)**
										1-2-3-2	・入社時又は社外要員の受入れ時に守秘義務のルールを説明すること。	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.4 (LV1)**
									★4	1-2-3-3	・自社の機密情報を取り扱う役員及び従業員に、守秘義務の誓約書を提出させること。(社外要員を除く。)	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.5 (LV2)**
										1-2-3-4	・派遣社員及び受入出向者について、派遣元及び出向元の会社と業務開始前に守秘義務を締結すること。	ISO/IEC 27001:2022 A.6.5, A.6.6 **自動車GL No.6 (LV2)**

★3案、26項目の具体的内容

No.	大分類	No.	中分類	No.	要求事項名	要求事項
1	ガバナンスの整備	1-2	役割、責任、権限	1-2-1	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。
				1-2-3	守秘義務のルール	守秘義務のルールを策定し、遵守させること。
		1-3	ポリシー	1-3-1	セキュリティ対応方針の策定	自社のセキュリティ対応方針を策定し、周知すること。
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	2-1-1	取引先とのビジネス又はシステム上の関係	取引先と自社とのビジネス又はシステム上の関係を把握すること。
				2-1-2	機密情報の取扱い	他社との間で、機密情報の取扱い方法を明確にすること。
				2-1-4	セキュリティインシデント発生時の役割・責任	セキュリティインシデント発生時の他社との役割及び責任を明確にすること。
3	リスクの特定	3-1	資産管理	3-1-1	ハードウェア、OS及びソフトウェアの把握	ハードウェア、OS及びソフトウェアに関する情報を把握すること。
				3-1-2	ネットワークの一覧作成	ネットワークの情報に関する一覧を作成すること。
				3-1-3	外部情報サービスの管理	自社の機密情報を扱う外部情報サービスを管理すること。
				3-1-4	機密区分に応じた情報の管理	機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。
				4-1-2	管理者IDの管理手続	管理者IDの発行・変更・削除の手続を定め、適切に運用すること。
				4-1-3	認証の強度・実装方法の決定	システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。
				4-1-4	アカウントロック制御	社内システムを構成する端末にアカウントロック制御を行うこと。
				4-1-5	パスワード設定ルール	パスワード設定に関するルールを定め、周知すること。
				4-1-6	パスワード管理ルール	パスワードの管理に関するルールを定め、周知すること。
				4-1-7	アクセス権の管理ルール	アクセス権の管理ルールを定めて、運用すること。
		4-2	意識向上とトレーニング	4-2-2	セキュリティインシデント発生時の教育・訓練	セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。
		4-3	データセキュリティ	4-3-4	適切なバックアップ	適切なバックアップを行うこと。
		4-4	プラットフォームセキュリティ	4-4-1	ハードウェア、OS及びソフトウェアの安全な構成	ハードウェア、OS及びソフトウェアの安全な構成を確立し、維持すること。
				4-4-4	セキュリティパッチ・アップデートの手続	ハードウェア、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を策定し、実行すること。
				4-4-5	マルウェア感染からの保護	システムをマルウェア感染から保護すること。
		4-5	技術インフラのレジリエンス	4-5-1	ネットワーク境界防護	内外のネットワークを適切に分離し、境界部分を防護すること。
5	攻撃等の検知	5-1	継続的監視	5-1-1	ネットワーク接続・データの監視	ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。
6	インシデントへの対応	6-1	インシデント管理	6-1-1	インシデント対応手順	セキュリティインシデントへの対応手順、対応体制等を定めること。
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	7-1-1	事業継続要件に沿った復旧準備	事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。

★4案、44項目の具体的内容 (1)

No.	大分類	No.	中分類	No.	要求事項名	要求事項
1	ガバナンスの整備	1-1	組織の状況	1-1-1	社内ルール	セキュリティに関する法令、契約等に規定された事項を考慮し、社内ルールを策定及び周知すること。
		1-2	役割、責任、権限	1-2-1	セキュリティ推進活動部門	セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。
				1-2-2	サイバー攻撃の監視・分析体制	サイバー攻撃及び予兆を監視・分析をする体制を整備すること。
				1-2-3	守秘義務のルール	守秘義務のルールを策定し、遵守させること。
		1-3	ポリシー	1-3-1	セキュリティ対応方針の策定	自社のセキュリティ対応方針を策定し、周知すること。
		1-4	監督	1-4-1	セキュリティ対策推進計画	各年度のセキュリティ対策推進計画を策定し、定期的に経営層へ対策実施状況に関する報告を行うと共に、報告結果を対策の推進に反映すること。
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	2-1-1	取引先とのビジネス又はシステム上の関係	取引先と自社とのビジネス又はシステム上の関係を把握すること。
				2-1-2	機密情報の取扱い	他社との間で、機密情報の取扱い方法を明確にすること。
				2-1-3	取引先のセキュリティ対策状況	重要な機密情報を取り扱う取引先のセキュリティ対策状況を把握すること。
				2-1-4	セキュリティインシデント発生時の役割・責任	セキュリティインシデント発生時の他社との役割及び責任を明確にすること。
				2-1-5	機密情報の回収・破棄	取引先との契約終了時に機密情報及びアクセス権を回収又は破棄すること。
3	リスクの特定	3-1	資産管理	3-1-1	ハードウェア、OS及びソフトウェアの把握	ハードウェア、OS及びソフトウェアに関する情報を把握すること。
				3-1-2	ネットワークの一覧作成	ネットワークの情報に関する一覧を作成すること。
				3-1-3	外部情報サービスの管理	自社の機密情報を扱う外部情報サービスを管理すること。
				3-1-4	機密区分に応じた情報の管理	機密区分に応じた情報の管理ルールを定め、それに基づく管理を行うこと。
				3-1-5	リモートワークにおけるルール	リモートワークで使用する情報機器及び機密情報の条件についてのルールを定め、運用していること。
		3-2	リスクアセスメント	3-2-1	脆弱性の管理体制	脆弱性の管理体制、管理プロセスを定め、それに基づく管理を行うこと。
4	攻撃等の防御	4-1	アイデンティティ管理、認証、アクセス制御	4-1-1	ユーザIDの管理手続	ユーザID の発行・変更・削除の手続を定め、適切に運用すること。
				4-1-2	管理者IDの管理手続	管理者IDの発行・変更・削除の手続を定め、適切に運用すること。
				4-1-3	認証の強度・実装方法の決定	システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。
				4-1-4	アカウントロック制御	社内システムを構成する端末にアカウントロック制御を行うこと。
				4-1-5	パスワード設定ルール	パスワード設定に関するルールを定め、周知すること。
				4-1-6	パスワード管理ルール	パスワードの管理に関するルールを定め、周知すること。
				4-1-7	アクセス権の管理ルール	アクセス権の管理ルールを定めて、運用すること。
				4-1-8	サーバ設置エリアへの入退室管理	サーバの設置エリアへの入退室を管理し、記録すること。
				4-1-9	可搬媒体の制限	可搬媒体の持込み・持出しを制限すること。
		4-2	意識向上とトレーニング	4-2-1	セキュリティの意識向上教育	経営層を含むすべての要員に対して、セキュリティの意識向上のための教育・研修を実施すること。
				4-2-2	セキュリティインシデント発生時の教育・訓練	セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。

★4案の44項目の具体的内容 (2)

No.	大分類	No.	中分類	No.	要求事項名	要求事項
		4-3	**データセキュリティ**	4-3-1	データの暗号化	情報機器及び情報システムの保管データを適切に暗号化するようルールを定め、周知すること。
				4-3-2	重要データの保管ルール	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。
				4-3-3	取引先との情報共有ルール	取引先との情報共有及び情報送信に関するルールを定め、周知すること。
				4-3-4	適切なバックアップ	適切なバックアップを行うこと。
		4-4	**プラットフォームセキュリティ**	4-4-1	ハードウェア、OS及びソフトウェアの安全な構成	ハードウェア、OS及びソフトウェアの安全な構成を確立し、維持すること。
				4-4-2	サポート期限の切れたOS及びソフトウェアへの対策	サポート期限の切れたOS及びソフトウェアの利用停止及び更改を実施すること。
				4-4-3	ログの取得	情報機器及びシステムに関するログを取得し、異常を検知するため、定期的にレビューを行うこと。
				4-4-4	セキュリティパッチ・アップデートの手続	ハードウェア、OS及びソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を策定し、実行すること。
				4-4-5	マルウェア感染からの保護	システムをマルウェア感染から保護すること。
		4-5	**技術インフラのレジリエンス**	4-5-1	ネットワーク境界防護	内外のネットワークを適切に分離し、境界部分を防護すること。
				4-5-2	社外への不正な通信の遮断	社内から社外への不正な通信を遮断する対策を実施すること。

No.	大分類	No.	中分類	No.	要求事項名	要求事項
5	**攻撃等の検知**	5-1	**継続的監視**	5-1-1	ネットワーク接続・データの監視	ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。
				5-1-2	ハードウェア及びソフトウェアの挙動監視	ハードウェア及びソフトウェアの状態及び挙動を監視すること。
		5-2	**有害事象の分析**	5-2-1	セキュリティインシデントの対象範囲	セキュリティインシデントとして扱う対象範囲を明確にし、運用していること。
6	**インシデントへの対応**	6-1	**インシデント管理**	6-1-1	インシデント対応手順	セキュリティインシデントへの対応手順、対応体制等を定めること。
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**	7-1-1	事業継続要件に沿った復旧準備	事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。

（参考）★3から始まっているのはなぜか？

★1、★2は中小企業のための**Security Action制度**

サプライチェーン用ではなく、自社向けの評価制度

★1

情報セキュリティ5か条

1. **OSやソフトウェアは常に最新の状態にしよう！**
2. **ウイルス対策ソフトを導入しよう！**
3. **パスワードを強化しよう！**
4. **共有設定を見直そう！**
5. **脅威や攻撃の手口を知ろう！**

★2

基本的対策

1. パソコンやスマホなど情報機器の OSやソフトウェアは常に最新の状態にしていますか？
2. パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1は最新の状態にしていますか？
3. パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
4. 重要情報※2に対する適切なアクセス制限を行っていますか？
5. 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？

従業員としての対策

1. 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
2. 電子メールやFAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
3. 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
4. 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
5. インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？
6. パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？
7. 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
8. 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
9. 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
10. 関係者以外の事務所への立ち入りを制限していますか？
11. 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
12. 事務所が無人になる時の施錠忘れ対策を実施していますか？
13. 重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？

組織としての対策

1. 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
2. 従業員にセキュリティに関する教育や注意喚起を行なっていますか？
3. 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
4. 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
5. クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・頼性を把握して選定していますか？
6. セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
7. 情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？

評価スキーム

★3：専門家確認付き自己評価
（有効期間1年）

① **取得希望組織は**、★3要求事項に基づき自己評価を記入(必要に応じて社内外のセキュリティ専門家からの支援を得ることも可)

② **社内外のセキュリティ専門家**は、取得希望組織が記入した内容を確認するとともに、必要に応じて評価結果の修正を含む助言を行い、最終的に制度事務 局へ提出する内容に関して了承した場合に署名を実施

③ **取得希望組織**は、経営層による自己適合宣誓を含め、登録機関に評価結果(セキュリティ専門家による署名を含むもの)を提出

④ **制度事務局**は、申請内容に問題が認められない場合には台帳に登録し、必要に応じて公開

自己評価とは、**経営層による自己適合宣言**を経た取得希望組織として実施する評価
（組織内のセキュリティを担当する担当者や部門が独自に実施する評価は含まない）

セキュリティ専門家とは、一定の**セキュリティ関連資格**を有し、かつ制度側で指定した**研修を受講**したもの
（情報処理安全確保支援し、公認情報セキュリティ監査人、CISSP、CISM、CISA、ISO27001 主任審査員）

★4：技術検証付き第三者評価
（有効期間3年、1年毎に自己評価結果を評価機関に提出）

① **指定委員会**は、評価機関・技術検証事業者を指定

② **取得希望組織**は、★4要求事項・評価基準に基づき自己評価を実施する。

③ **取得希望組織**は、評価機関に、検証・評価を依頼

④ **評価機関**は、検証・評価を実施(検証は必要に応じて他の技術検証事業 者が実施する場合もある)

⑤ **評価機関**は、評価結果を取得希望組織に通知し、制度事務局に提出

⑥ **制度事務局**は、「合格」とされた組織を台帳に登録し、必要に応じて公開

⑦ **評価機関**は、取得希望組織の求めに応じて証書を発行

評価の実施内容

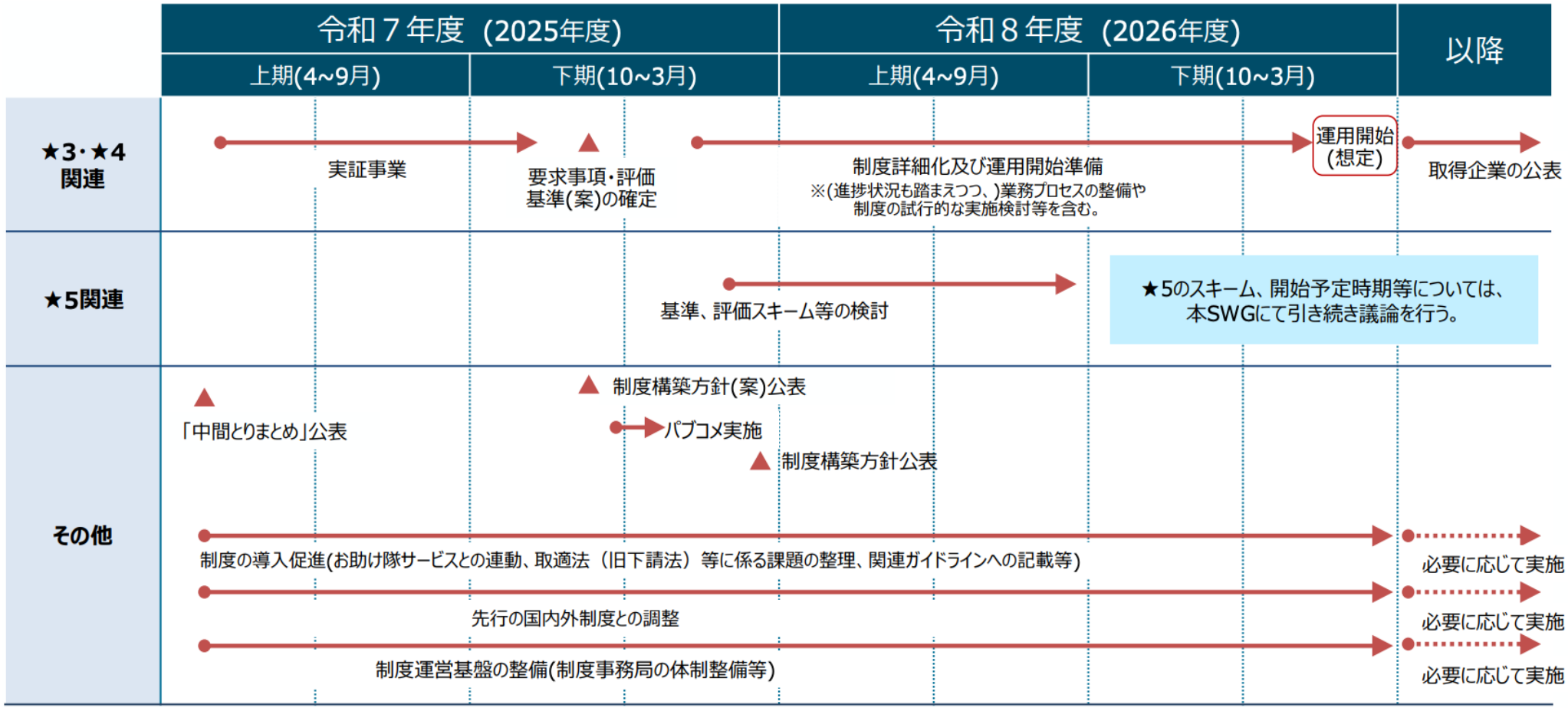
★3：セキュリティ専門家が、取得希望組織が作成した書類の確認を行う。

★4：評価機関・技術検証事業者が、文書確認に加え、実地審査及び技術検証(脆弱性検査等)を行う。

評価プロセス	所要期間(想定)	実施内容等	
		★3	★4
文書確認 (提出書類の確認)	1日~2日程度	• 取得希望組織が作成した自己評価の結果を確認 (主に、記載内容に矛盾がないか、評価基準から見て十分な事項が記されているかの確認) • 文書確認の結果、記載内容に明らかな不適合が認められない場合 ✓ ★3では、取得希望組織は登録機関に申請を行い、申請内容に問題等がなければ★3を取得することができる ✓ ★4では、実地審査及び技術検証に進む	
実地審査 (取得希望企業へのヒアリング、規程、操作画面等の確認による評価) ※リモートでの実施も可	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 相対的に重要性が高いと考えられる対策事項について証跡確認を含めた評価を実施 [実地審査で確認すべき事項(例)] ✓ 法令や契約等に規定された事項を考慮した社内ルールの策定 ✓ 脆弱性の管理体制、管理プロセス ✓ セキュリティインシデント対応手順 ✓ 事業継続要件に沿った復旧準備
技術検証 (取得希望企業の管理する対象機器に対して既知脆弱性の悪用等の一般的な攻撃パターンを試行)	1日~2日程度 ※ 事前準備、報告書作成は除く	(実施なし)	• 取得希望組織がインターネットに公開している機器のうち、脆弱性を悪用等された場合に組織内部に侵入されるリスクが高い機器(例：VPN装置、ルータ)を対象として、 ✓ 脆弱性検査を含む技術的な検証を実施する又は ✓ 当該検証の実施結果に相当する証跡(例：直近における対象機器への脆弱性検査の実施結果)を確認する
合格基準	-	• ★3・★4ともに、原則として、全ての評価基準への適合を求める。	
不適合の指摘及び改善	-	• 評価結果に不適合が発見された場合であっても、適切に是正対処し、セキュリティ専門家から当該是正について了承を得られれば★3を取得可能	• 不適合事項の是正報告を、指摘時から一定期間内(例：評価機関による実地審査等実施日から1か月以内)に提出し、内容について了承を得られれば★4を取得可能

今後のスケジュール

令和8年度下期の制度開始を目指し、制度運営基盤の整備や利用促進等を進めていく



みんな気になる疑問点（私見です…）

ISMSと何が違うのですか？

ISMSは**マネジメントシステム**の認証であるのに対して、本制度は、セキュリティ**対策**の実施状況の確認です。

なお、ISMSを取得しているサイトは現在8,000超です。

★の取り消しはありえるのか？

内部通報等により、取得組織において虚偽報告、情報隠蔽等の不正行為が確認された場合、評価機関又は制度事務局から★の一時停止又は取消しを行うことが想定されています。

星の取得単位は会社単位ですか？

取得は**会社（法人）単位**を考えています。ただ、大企業の場合、事業部単位、場所単位等も考えるべきという意見は大企業の委員からでていました。

評価コスト負担はどのくらいですか？

現在のPマークの取得と同程度の金額を想定。

詳細は今後詰めていく予定

国際的相互認証を考えていますか？

サプライチェーンは国際的に広がっていることもあり、国際的な相互認証も**視野にいれています**。ただし、詳細についてはまだ**今後の検討**となります。

質問など…

Thank you