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（概要）

２０２５年4月１４日

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ブワーキンググループ

事務局

サプライチェーン企業のセキュリティ対策評価制度の構築

- **サプライチェーンに起因するインシデントを背景**に、**企業の取引においてもセキュリティ対策の担保が求められる中**、受注企業が**異なる取引先から様々な対策水準を要求される**、発注企業は**外部から各企業等の対策状況を判断することが難しい**といった課題が存在。
- こうした課題に対応するため、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の検討**を進めており、本年４月に**制度の概要を整理した中間とりまとめを公表**。今後、実証事業等を通じた**評価スキームの具体化**や制度の**利用促進のための施策の検討**等を進め、**2026年度中の制度開始**を目指す。

構築する評価制度（現時点案）

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）※
想定される脅威	• 広く認知された脆弱性等を悪用する一般的なサイバー攻撃	• 供給停止等によりサプライチェーンに大きな影響をもたらす企業への攻撃 • 機密情報等、情報漏えいにより大きな影響をもたらす資産への攻撃	• 未知の攻撃も含めた、高度なサイバー攻撃
対策の基本的な考え方	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： • 基礎的な組織的対策とシステム防御策を中心に実施	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： • 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	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： • 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
評価スキーム	自己評価	第三者評価	第三者評価

※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

政府調達や重要インフラ事業者等での活用推進

取引先からの対策要請による活用促進

利害関係者への情報開示による対話の促進

※サプライチェーン間の結び付きが強固・複雑な自動車、半導体、主要製造業等において、優先的に本制度の利用を促進。

制度実現に向けた検討課題（例）

- **国内外の関連制度・評価制度との整合性確保、相互認証**
- 対策推進のための企業への支援の在り方（**専門家の活用促進**、**中小企業支援策との連動**、**評価機関の支援**）
- 下請法や価格転嫁に関する課題の整理
- 実効性の強化に向けた取組（政府機関や重要インフラ事業者等における活用推進、サプライチェーン上の取引先や投資家等の**ステークホルダとの対話での活用**等の促進）

サプライチェーン対策評価制度に関する現状整理（案）①

- 2024年4月に制度構想を示して以降、これまで本SWGを4回開催。また、IPAがSC3の下に「サプライチェーンサイバーセキュリティ成熟度モデル検討SWG」を立ち上げ、これまで6回検討会を開催。これまでの議論を通じて、以下の通り制度の概要を整理。

【現状認識（制度検討の背景）】

- 中小企業含めて多数の企業は取引先への製品・サービスの提供等を通じて、サプライチェーンを構成している。近年、**サプライチェーンを通じた情報漏えい・事業継続に関するインシデントが頻発**。その対策として、政府や重要インフラ企業のみならずその取引先についても、自主的なセキュリティ対策を基本としつつ、適切なセキュリティ対策を課す必要があるが、**複雑なサプライチェーン下で、様々な取引先から様々な要求事項を求められている**状況。**発注企業にとっては、正しいセキュリティ対策が取引先でなされているか不明確／受注企業にとっては（特に中小企業を中心に）過度な負担につながっている**。結果として、**サプライチェーン全体のセキュリティ底上げにつながっていない**。

【制度趣旨】

- **本制度に基づく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、**取引先へのサイバー攻撃を起因とした情報セキュリティリスク／製品・サービスの提供途絶や取引ネットワークを通じた不正侵入等のリスクに対する適切なセキュリティ対策の実施を促し、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**（※１）。
- **具体的には、2社間の取引契約等において発注企業が、受注側に適切な段階（★）を提示し、示された対策を促すとともに実施状況を確認することを想定**（※２）（**再委託先は発注者から見た直接の管理対象にはならないが、委託先を通じて必要に応じて管理**することを想定（※３））。

（※１）本制度で対象としているのは、あくまでサプライチェーンを構成する企業等のIT基盤におけるセキュリティ対策であり、組織のガバナンス・取引先管理、自社IT基盤への検知・防御等、組織全体に影響が及ぶ範囲を対象としている。ソフトウェア開発やIoT機器、データ等その他のセキュリティ・信頼性確保等については様々な観点から評価制度・取組が行われているが、これらとは目的が異なっており、**求められる対策内容や効果も基本的に異なる**（制度・取組の重複を避ける観点からも、本制度ではあくまで企業等のIT基盤における対策を対象とする）。

（※２）なお、取引先からの要請が無くても、各企業が自らのサイバーセキュリティ対策状況を可視化するためにマークを自主的に取得することも考えられる。

（※３）対策基準の項目において、「重要な取引先におけるセキュリティ対策状況の把握」を求めることを想定

【目指す効果】

- **サプライチェーンにおけるリスクを対象**にした上で（※）、その中での立ち位置に応じて必要な対策を提示することで、**企業の対策決定を容易・適切なものにする**。すべてのサプライチェーン企業が対象となるが、特に**サプライチェーンを構成する中小企業は、セキュリティ対策におけるリソースが限られていること／自社のリスクを踏まえてセキュリティ対策を行うことはハードルが高いことから、活用による効果が大きい。**

（※）**本来は各企業が自社のリスクを特定して必要なセキュリティ対策を個別に検討・実施することが望ましい**が、リソースに限りのある**中小企業を中心にただちにこれを実現できていない企業が一定数存在**する。本制度は、**包括的なリスク分析に基づき共通して求められる対策を示す**もの。将来的には、こうした企業も**より自社のリスク分析に基づいたさらなる対策の強化をしていくことが望ましい**。

サプライチェーン対策評価制度に関する現状整理（案）②

【基準の考え方】

- 求められるセキュリティ対策について、**各企業のサプライチェーンにおける重要性や影響度を踏まえた上で、複数区分（★3～5）に分ける**ことを想定。具体的には、**①ビジネス観点（データ保護・事業継続における重要度）②システム観点（接続の有無）の二点で整理**。
- これらの考え方や、**海外での類似制度（英Cyber Essentials）や各産業のガイドライン（自工会・部工会ガイドライン、他分野別ガイドライン等）の内容**を踏まえつつ、NISTの「サイバーセキュリティフレームワーク2.0」等にも基づき、「ガバナンス整備、取引先管理、リスクの特定、システムの防御、攻撃等の検知、インシデントの対応・復旧」の観点から、**★3・4の考え方、対策事項・要求項目について整理**を行った。
- **★3は基礎的なシステム防御策と体制整備を中心に構成**。**★4はガバナンスから防御・検知・対応まで包括的な対策**とすることを想定。

（※） ★5については、より高いレベルの対策としては、前述の通り自社やサプライチェーンに対するリスクアセスメントの考え方が求められるため、**各企業におけるリスクに応じて対策を講じることを求めるISMS適合性評価制度との制度的整合性も含めて、位置付け・基準を引き続き検討。**

【国内外の関連制度等との連携・整合】

- 先行する自己評価の仕組みである**「SECURITY ACTION」（★１、★２）、「自工会・部工会ガイドライン」**や前述した国際標準である**「ISMS適合性評価制度」等**とは、**相互補完的な制度として発展することを目指す**。
- 具体的には、**現在の★3・4の要求項目案は自工会・部工会ガイドラインの内容とも整合性を一定程度確保**しており、同ガイドラインに基づく自己評価に際しての本制度での活用等、**連携のあり方については、運営団体とも議論を進めていく**。また、**海外の類似制度**についても、**将来的な相互認証の可能性も念頭に、引き続き調査・意見交換を実施**する。

サプライチェーン対策評価制度に関する現状整理（案）③

【制度において設ける段階の考え方】

- 先行する海外制度等の分析を通じて、★３については、一般的なサイバー脅威に対処しうる水準を目指すものとして規定。
  ★４は、初期侵入の防御に留まらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合した事業継続を推進している点を改めて明確化。
- ★５については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定（★3・4の精査も踏まえ、今後さらに具体化）。
- 上位の段階はそれ以下の段階で求められる事項を包括するため、例えば、★3を事前に取得していなければ★4を取得できないという関係とはならない。

	★3	★4	★5（※）
想定される脅威	• 広く認知された脆弱性等を悪用する**一般的なサイバー攻撃**	• **供給停止**等によりサプライチェーンに**大きな影響**をもたらす企業への攻撃 • 機密情報等、**情報漏えい**により**大きな影響**をもたらす資産への攻撃	• **未知の攻撃**も含めた、**高度なサイバー攻撃**
対策の基本的な考え方	• 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、**基礎的な組織的対策とシステム防御策**を中心に実施	• 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	• 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
脅威に対する達成水準（イメージ）	• **組織内の役割と責任が定義**されている。 • 一般的なサイバー脅威への対処を念頭に、自社**IT基盤**への初期侵入、侵害拡大等への対策が講じられている。 • インシデント発生時に、**取引先を含む社内外関係各所への報告・共有に必要な最低限の手順が定義、実施**されている。	• セキュリティ対策が**組織的な仕組みに基づいて実施され、継続的に改善**している。 • **取引先のシステムやデータを含む内外**への被害拡大や攻撃者による目的遂行のリスクを低減する対策が講じられている。 • **事業継続に向けた取組や取引先の対策状況の把握**など、自社の位置づけに適合した**サプライチェーン強靭化策が講じられている**。	• 組織において**国際規格等に基づくマネジメントシステム**が確立されている。 • **リスクを適宜適切に把握**した上で、インシデントに対して迅速に検知・対応するなど、**ベストプラクティスに基づくサイバーレジリエンス確保策**が講じられている。 • 取引先等への指導や共同での訓練の実施など、**自社サプライチェーン全体のセキュリティ水準向上に資する対策**が講じられている。
評価スキーム	**自己評価** （※）社内等の専門家による評価を想定	**第三者評価** ※第三者評価を原則とするが、評価コストの負担を抑える観点から詳細は今後検討	**第三者評価**
ベンチマーク （対象企業やリスクが同様であり、対策項目を検討する上で参考）	• 自工会・部工会ガイドLv1 • Cyber Essentials ⇒★3で対処する脅威等に照らして精査し、対策事項（案）を抽出	• 自工会・部工会ガイドLv2～3 • 分野別ガイドライン 等 ⇒★4で対処する脅威等に照らして精査し、対策事項（案）を抽出	• ISO/IEC27001 • 自工会・部工会ガイドLv3 等 （※）ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

制度で用いるセキュリティ要求事項・評価基準

- レベルごと達成すべき「経営の責任」、「サプライチェーンの防御」、「IT基盤の防御」に資する対策を以下にて提示

※1 以下は必ずしも全要求を網羅しているわけではない点に留意。

※2 資料2の大分類のうち、ガバナンスの整備、リスクの特定、インシデントへの対応、インシデントからの復旧は「経営の責任」に、取引先管理は「サプライチェーンの防御」に、攻撃等の防御、攻撃等の検知は「IT基盤の防御」に該当

	★3（Basic）	★4（Standard）
経営の責任	**企業として最低限のリスク管理体制構築** • 自社のセキュリティ担当の明確化 [No.1] • セキュリティ対応方針の策定 [No.3] **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.25] **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一覧化 [No.7,8] • 取引先等とのネットワーク接続の管理 [No.9]	**継続的改善に資するリスク管理体制の構築** • 定期的な見直しの実施 [No.6] • 定期的な経営層への報告、不備の是正等 [No.7] **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.44] **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.17] • 定期的な見直しの実施「No.6」（再掲）
サプライチェーンの防御	**取引先等に課す最低限のルールの明確化** • 接続している外部情報システムの一覧化 [No.5] • 他社との機密情報の取扱い明確化 [No.6]	**サプライチェーンにおける対策状況の把握** • 機密情報共有先の一覧化 [No.8] • 重要な取引先等の対策状況把握 [No.10] **取引先等との役割と責任の明確化** • インシデント発生時の他社との役割等の明確化 [No.11]
IT基盤の防御	**不正アクセスに対する基礎的な防御** • 基礎的なID管理手続き、アクセス権限の設定 [No.11,12,17] • パスワードの安全な設定及び管理 [No.15,16] • 内外ネットワーク境界の分離・保護 [No.23] **端末やサーバーの基礎的な保護** • ソフトウェアの適時のアップデート適用、不要なソフトウェアの削除 [No.20,21] • 端末等へのマルウェア対策 [No.22]	**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.29] • 社内システムにおける適切なネットワーク分離 [No.38] • 社外への不正通信の遮断(出口対策) [No.39] • 情報機器等の状態や挙動の監視・対応 [No.41] **迅速な異常の検知** • ログの収集・定期的な分析の実施 [No.35] • ネットワーク接続やデータ転送の監視 [No.40] • 情報機器等の状態や挙動の監視・対応 [No.41]（再掲） • 監視活動で検知された事象の分析 [No.42]

制度の導入促進に向けた取組

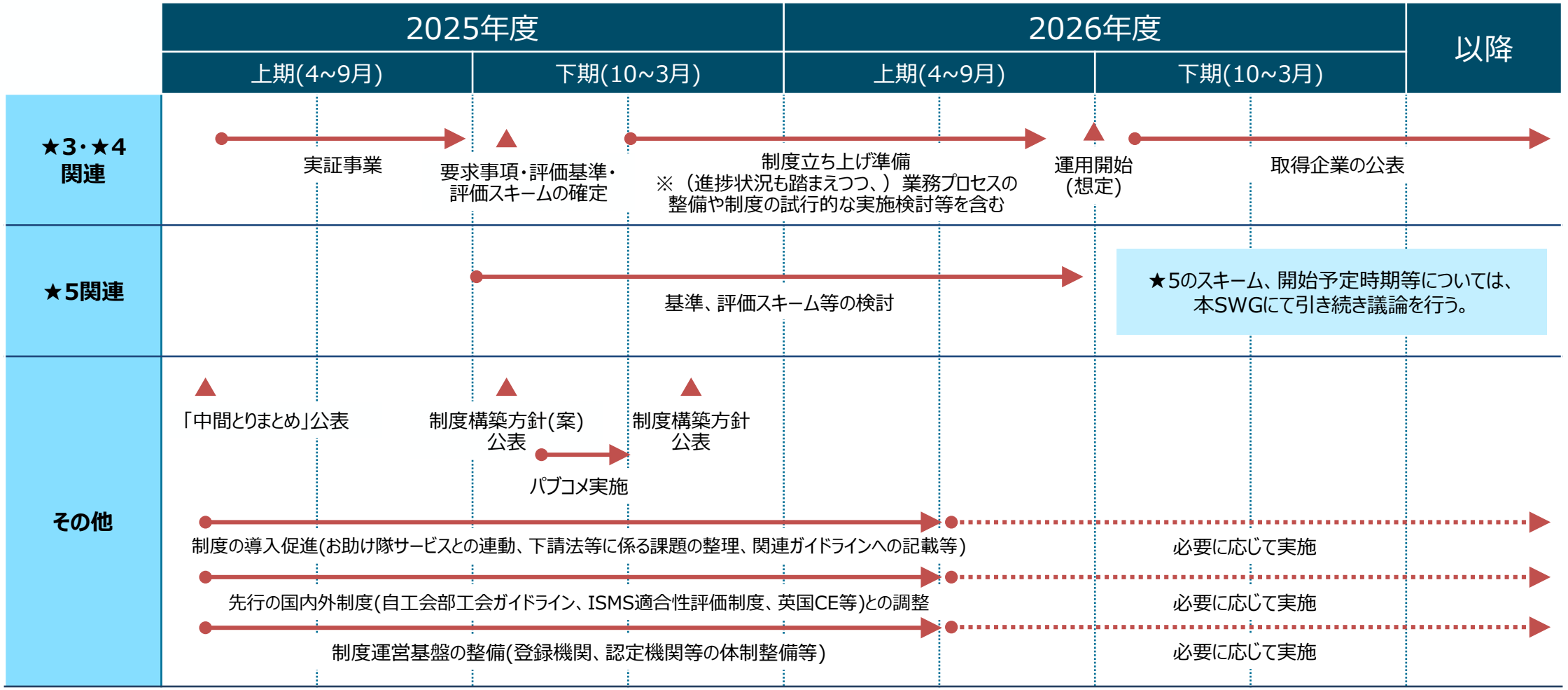
- 各業界に対するヒアリングの中では、制度を活用する上で下記の施策を求める声が見受けられており、これらも踏まえて導入促進に向けた取組の具体化を進めていく。

①発注者層、②中間者層、③エンド層、④評価機関・専門家

課題	導入促進策（案）	①	②	③	④
①対策推進のための企業への支援	● **専門家の活用促進** 専門家の確保・育成を行うと共に、主に中小企業と専門家のマッチングの仕組みを構築する。専門家の確保にあたっては、情報処理安全確保支援士（登録セキスペ）に加え、セキュリティ・プレゼンターやITコーディネータ（セキュリティ関連資格保有者）等の活用も検討する。専門家による支援内容の明確化のため、過去IPAが実施した「中小企業の情報セキュリティマネジメント指導業務」等の成果を活用し、支援プロセスやアウトプットを明確にした指導要領の作成、支援ツール（企業へのヒアリングシート、作成文書雛形等）を準備する。			○	
	● **中小企業セキュリティ普及促進策との連動** SA宣言事業者に対する推奨、★取得とお助け隊サービス、情報セキュリティサービス審査登録制度、その他業界団体が提供するサービスリストなど中小企業が導入可能な具体的なサービスとセットでの普及啓発を行う。また、中小企業セキュリティ対策普及啓発コンテンツに本制度、及び★取得推奨に関して追記する。			○	
②下請法や価格転嫁への対応	● **取引先への対策の要請等に係る考え方の整理** 取引先へのセキュリティ対策の支援や要請に係る独占禁止法等との明確な整理を行う。それを踏まえつつ、民民の契約において本制度の要求基準や★取得の推奨等を盛り込む際のひな型の作成、提供を行う。	○	○	○	
③国としての推進、業界の巻き込み	● **中小企業の情報セキュリティガイドラインへの追記** 中小企業の情報セキュリティガイドライン、及び付録サンプル規程において、本制度の要求基準等の記載、★取得の推奨を行う。			○	
	● **業界毎の特性を踏まえた導入促進** 各業界のセキュリティガイドライン等における委託先へのセキュリティ対策として、本制度の要求基準等の記載、★取得確認の推奨を推進する。また、政府の施策等との連動等により、各業界への適用に向けた検討を進める。	○	○		
	● **政府機関や重要インフラ事業者等における活用の推進** 政府調達での参照や重要インフラ事業者等での活用推奨等について検討を進める。	○	○		
	● **本制度の継続的な広報、周知** 国や制度オーナーが連携し、本制度の効果や取得のメリット、発注者・受注者それぞれに期待される役割等について分かりやすく発信し、制度に対する活用意欲を向上させる広報や周知活動を継続的に行う。	○	○	○	○
④評価機関の支援・育成	● **評価機関の支援** 評価基準や評価手法を明確化し、評価の品質を保つとともに、企業における対応を容易なものとするため、評価者に向けた評価ガイドとして、標準的なレビュープロセス、実施事項を明確化する。				○
	● **セキュリティ評価・対策支援人材の育成** セキュリティ人材不足の解消、及び評価及び対策支援をシームレスに行うため、本制度に関わる人材育成のための、コンテンツや研修機会を設ける。				○
⑤他制度との連携推進	● **他のガイドラインや国内外の関連制度との整合性確保** 「SECURITY ACTION」「自工会・部工会ガイドライン」や、国際標準であるISMS適合性評価制度等との整合性の確保や、評価結果の本制度での活用などの連携方策の検討を進める。また、将来的な相互認証の可能性を念頭に、グローバルな評価制度との連携・意見交換を継続する。 サプライチェーン対策全体を俯瞰し、各制度の位置づけを明確にする利用者目線での他のガイドライン等との関係整理を行う。	○	○	○	○

今後のスケジュール

- 2026年度の制度開始を目指し、実証事業による制度案の検討と並行して、制度運営基盤の整備や利用促進等を進めていく。



（参考）制度が効果的と想定される業界等

- 下記の観点から、制度が効果的と想定される業界等については、優先的に制度活用を促進していく。
  - ✓ 発注者層では、重要な機密情報を有し、高いセキュリティレベルが求められる業界、セキュリティ要求への対応が困難な取引先が含まれる業界、サプライチェーン間の結びつきが強い業界、サプライチェーンが複雑な業界
  - ✓ 中間層では、重要な機密情報・重要な業務の委託を受け、様々な業界からセキュリティ要請を受けている業界・事業者
  - ✓ エンド層では、情報管理や事業継続において重要な役割を果たす業界・事業者

	該当する業界等	業界等におけるニーズ
① サプライチェーン発注者層	・政府機関等 ・重要インフラ事業者 ・主要製造業　等	・**重要な機密情報を有し、高いセキュリティレベルが求められる業界**：顧客情報等、重要な機密情報を委託する取引先のセキュリティ管理の実効性に課題あり。厳密な第三者評価、評価結果の開示、技術検証を制度に組み込むことにより、★4以上の活用が期待できる。（例：金融　等） ・**セキュリティ要求への対応が困難な取引先が含まれる業界**：重要な機密情報を委託しているものの、取引先・再委託先企業の人材・予算が十分でなく、自己評価の実効性にも課題を抱えており、取引先への支援策とセットで★3活用が期待できる。（例：金融等） ・**サプライチェーン間の結びつきが強い業界**：サプライチェーンを構成する事業者の事業停止がサプライチェーン全体に波及するリスクのある業界については、★3～4の活用が期待できる。（例：自動車、半導体等） ・**サプライチェーンが複雑な業界**：取引先・再委託の管理や対策状況の確認に多大なコストが生じるため、取引内容・取引先に応じて★3～4の活用が期待できる。（例：主要製造業）
② 多様な業界から業務を受ける中間層	・BPO事業者 ・製品・部品製造業等	・**重要な機密情報・重要な業務の委託を受け、様々な業界からセキュリティ要請を受けている業界・事業者**：様々な要請や現地審査に対応するための負担あり。BPOでは、業種・業界問わず統一的に活用されることで★3～4の活用が見込める。ISMS等を既に取得する事業者もあり、既存の取組との整合性が必要。製造業は対応負荷軽減につながれば★4の活用が期待できる。大手事業者の★取得のコスト負担の影響は少ないが、取引先が海外を含む場合は海外制度との整合性が必要。
③ サプライチェーンを下支えするエンド層	・中小企業全般（BtoB）	・**情報管理や事業継続において重要な役割を果たす業界・事業者**：特に、比較的規模の大きな事業者（101人以上）、インシデントを経験した事業者、既に対策に取り組んでいる事業者（SA宣言者）等において、セキュリティ対策を進めるために、★3～4の活用が期待できる。エンド層にとっては、費用や人材、経営者のリテラシー等が課題となり、導入促進策とセットの展開が必要である。

※　重要な機密情報：機密情報のうち、当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの

（参考）実証事業の推進計画　― 実証の類型及び関係主体の役割分担等

- 実証においては類型1（★3）、類型2（★4）の2タイプを設けるとともに、調達者を対象としたヒアリング等を実施することを予定。
- 類型ごとの関係主体、それぞれの役割は以下の通りと想定。
  - 類型1（★3）：事務局、ユーザー事業者、外部専門家（必要な場合）
  - 類型2（★4）：事務局、ユーザー事業者、評価機関、検証事業者
  - ヒアリング等：事務局、調達者