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ブワーキンググループ

事務局

目次

１．はじめに

1. はじめに

現状認識 ～制度検討の背景～

- 近年、**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。** 取引先等、**サプライチェーン全体のセキュリティ対策が求められる**中、以下の課題が表面化しつつある。
  - 発注企業：取引先における**セキュリティ対策が可視化しづらく、要求事項（チェックリスト等）の適正性の担保も難しい**
  - 委託先企業：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、**過度な負担**につながっている(特に中小企業を中心に)

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) 本制度は、サプライチェーンにおける企業の位置づけや想定リスク等を踏まえて求められるセキュリティ対策の水準を定め、企業の対応状況を可視化するものであり、事業者のセキュリティ対策レベルを競わせることを目的としたもの**(格付け制度等)ではない**。

(※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**。全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直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更なる対策の強化をしていくことが望ましい。

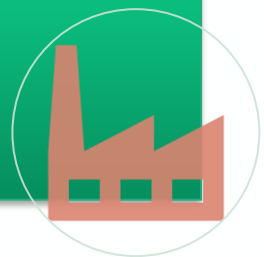
2. 構築すべき評価制度の目的と位置づけ

2.1 制度の目的

- 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・適切となることが期待される。
- また、取引先のセキュリティ対策が適切に実装されることで、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が期待される。

受注企業への効果

- 自社がどの程度のセキュリティ対策を実施するべきか明確になる。
- 発注企業等に対して、セキュリティ対策に係る説明が容易になる。
- 対策に要する費用や効果の可視化
- セキュリティサービスの標準化による選択肢拡大やコスト低減(中長期)



発注企業への効果

- 取引先に求めるセキュリティ対策の内容や水準の決定や、実施状況の把握が容易・適切になる
- 取引先におけるセキュリティ対策の適切な実装により、サプライチェーンに起因する自社セキュリティリスクの低減

社会全体での効果

- サプライチェーン全体での底上げを通じた経済・社会全体のサイバーレジリエンス※の強化
- サイバー攻撃への備えのある企業等への適切な評価
- セキュリティ製品やサービスの市場拡大・競争力向上(中長期)

※サイバーレジリエンス(Cyber resiliency)
サイバー資源を使用する又はサイバー資源によって実現するシステムに対する不利な状況、ストレス、攻撃、侵害を予測し、それらに耐え、回復し、適応する能力 https://csrc.nist.gov/glossary/term/cyber_resiliency

2.2 制度の位置づけ　2.2.1 対象とするリスクの範囲

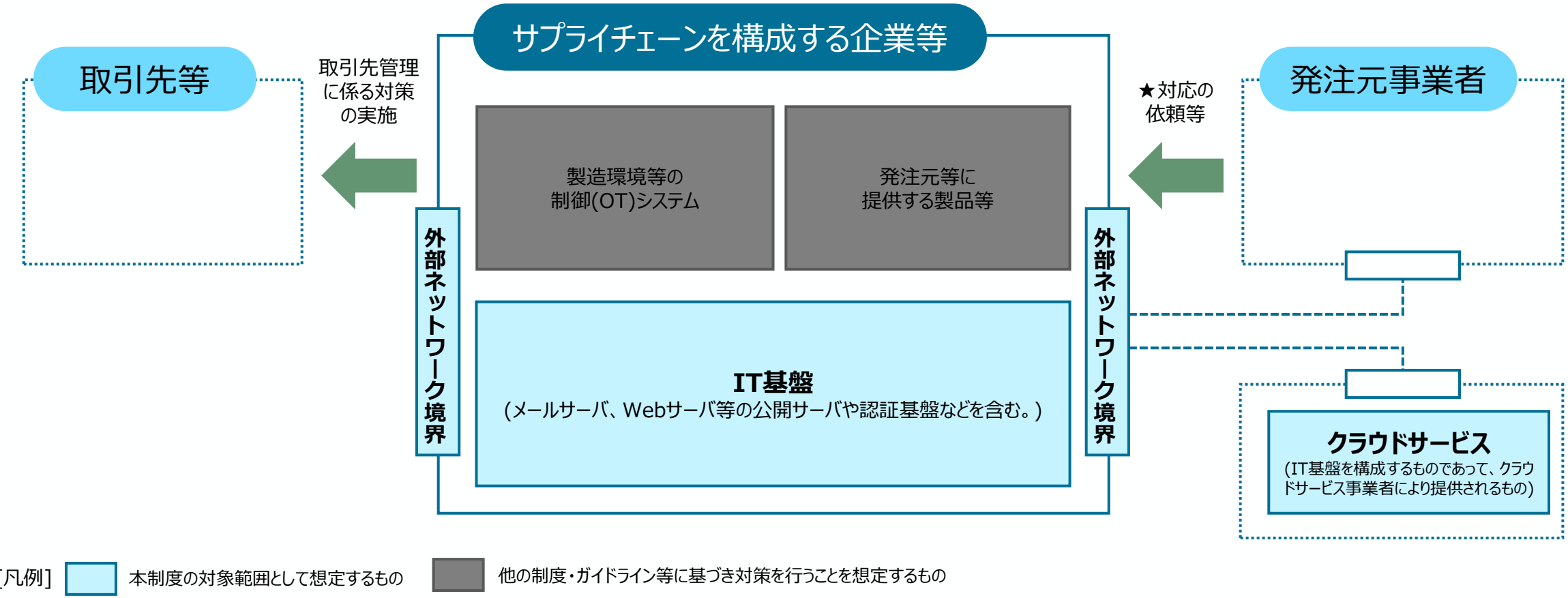
- 本制度では、取引先へのサイバー攻撃等を起因とした情報セキュリティリスク(機密性・可用性・完全性への影響)に加えて、製品・サービスの提供途絶リスク(事業継続性への影響)及び取引ネットワークを通じた不正侵入等リスクを対象とするサプライチェーンリスクとして想定。

分類	想定するサプライチェーンリスク	インシデント事例	影響を受けるサプライチェーン
自社事業・サービスの提供途絶 事業継続	サプライチェーン企業へのサイバー攻撃等に起因する、調達部品の供給遅延・停止	• 自動車部品メーカー • 半導体事業者	⇒ ビジネスサプライチェーン (物品調達及び業務委託(IT機器又はシステムの設計・構築・運用に係るものも含む。)に加え、業務提携、API連携など(他の類型に含まれるものを除く。)を含む。)
	調達したクラウドサービスへのサイバー攻撃等に起因する、クラウドサービスの停止	• クラウド事業者	⇒ ITサービスサプライチェーン (外部情報サービス(例えばクラウドサービス、ホスティングサービス等、自組織内で情報機器を保有しない形態の情報サービス。)の調達を含む。)
機密情報の漏えい、改ざん データ保護	サプライチェーン企業へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	• BPO事業者	⇒ ビジネスサプライチェーン
	マネージドサービス等へのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	• ITベンダー	⇒ ITサービスサプライチェーン
	調達したクラウドサービスへのサイバー攻撃等に起因する、機密情報の漏えい・改ざん	• クラウド事業者	⇒ ITサービスサプライチェーン
取引先等を踏み台とした不正侵入 不正アクセス	サプイチェーン企業の環境を踏み台とした、発注者側システム環境への不正侵入	• 医療機関	⇒ ビジネスサプライチェーン
	マネージドサービス等の環境を踏み台とした、発注者側システム環境への不正侵入	• ITベンダー	⇒ ITサービスサプライチェーン

※ 本制度の対象は、企業体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機器のセキュリティを対象にした評価制度・取組とは目的が異なるため、求められる対策内容や効果も基本的に異なる。

2.2 制度の位置づけ　2.2.2 制度の対象範囲

- 本制度は、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。)を対象とする。
- 一般的にIT基盤には該当しないと考えられる製造環境等の制御(OT)システム、発注元等に提供する製品等については求められる対応が基本的に異なることから直接の対象とはせず、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。



2.2 制度の位置づけ　2.2.2 制度の対象範囲

■ 適用範囲の考え方

◆適用範囲に含むもの

1. IT基盤

- 特定の業務領域によらず全体の業務に共通するIT基盤を構成するサーバ群のうち、「適用範囲に含めないもの」に該当しないもの
  [註] 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。
- エンドポイント機器(パソコン、スマートデバイス等、人が使用するインターフェースを持つもの)
- ★取得希望企業のIT基盤を構成するが、他社との間で対策に係る責任を共有するもの(例：クラウドサービス、親会社の提供するグループ共通のネットワーク等)
  [註] これらのサービス等においては、責任共有モデル(※)に基づき、自社における対策実装又はサービス提供者等における対策状況の確認等(例:ISMAP登録の有無やSOC2レポートの確認等)を行う必要がある。
  (※) 責任共有モデルとは、サービスを提供する事業者とサービス利用者との間で、サービスのセキュリティに関する責任を共有し合うための考え方のことを指す。

2. 外部ネットワーク境界

- 適用範囲の境界を定義するネットワーク機器(ファイアウォール、ルータ、VPN装置等) * 他組織の内部システムへ接続する際の境界を構成する機器を含む。

3. その他

- 企業は個社/(国内又は海外を含む)企業グループ/事業部等と★の取得範囲を柔軟に定めることができる。
- 適用範囲とするIT基盤等に接続等するが適用範囲には含めないという判断をしたものについて、ネットワーク機器等(例：VLAN、ファイアウォール)により、適用範囲との境界を技術的に分離すること。(例：取得単位を国内の事業所とする場合、海外事業所との間の通信をネットワーク機器等により必要最小限にする)

◆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

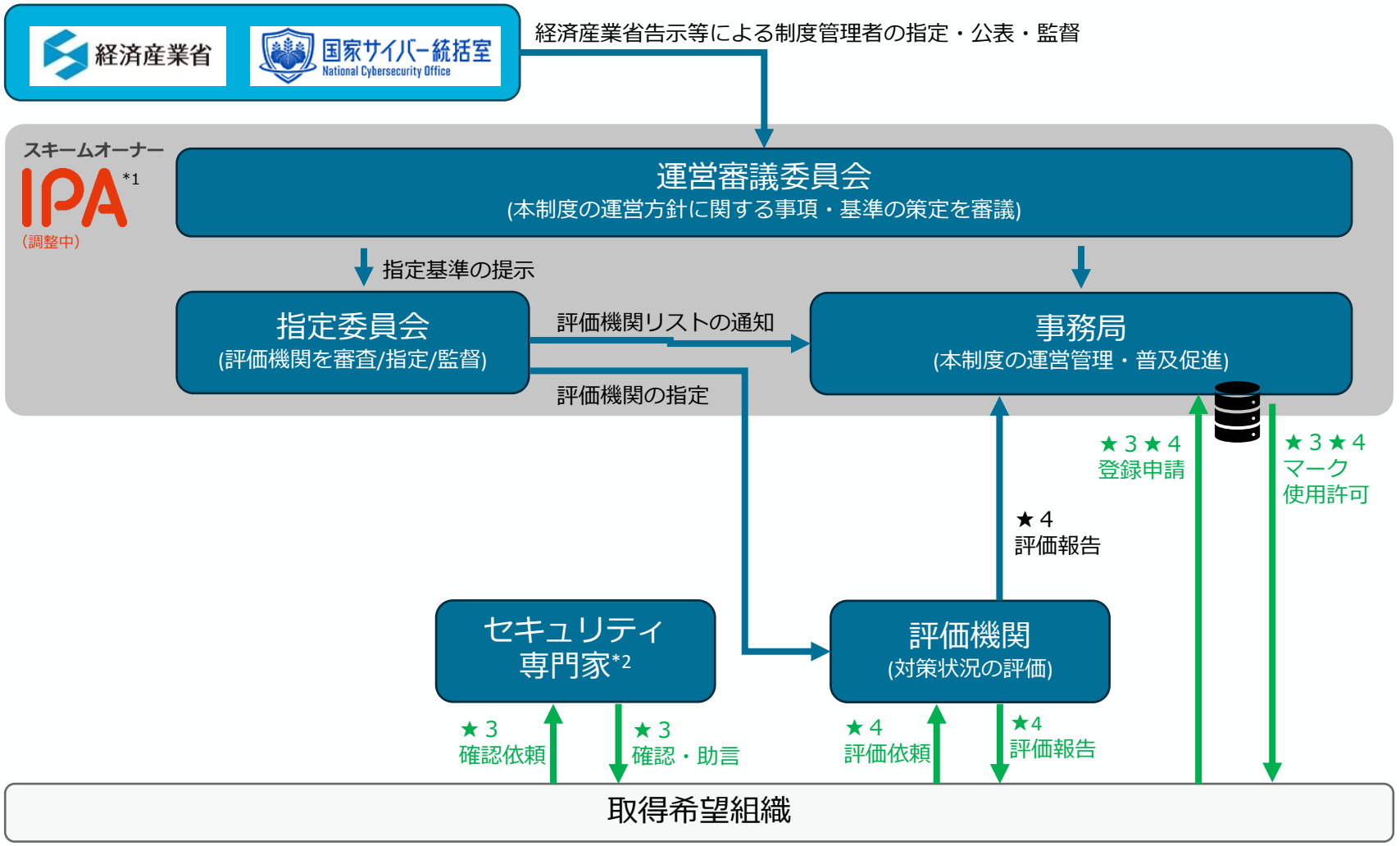
◆原則として適用範囲に含めるが、例外的に適用範囲に含めないことが許容され得るもの

- 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。

3. 構築する評価制度

3.1 制度の運用体制案

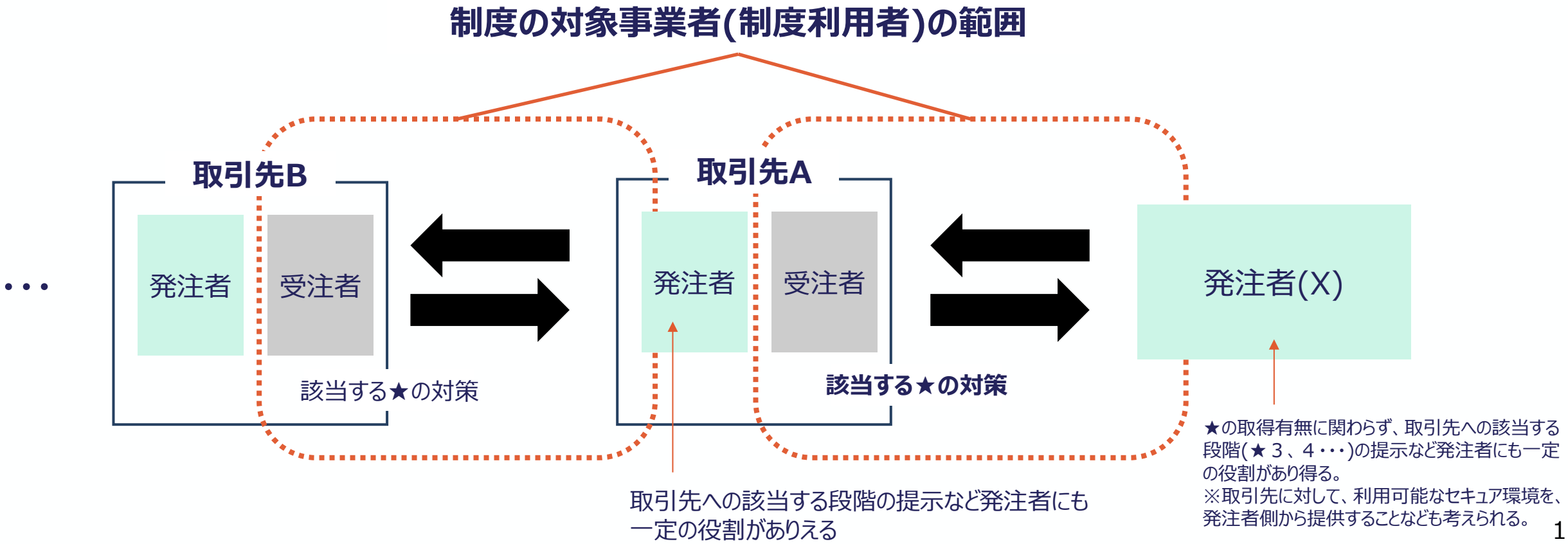
- 制度の運用にあたっては、以下のような運用体制を想定。



*1　IPA：独立行政法人情報処理推進機構
*2　20ページにて示すセキュリティ専門家向けの研修に係るスキームは今後検討予定

3.2 制度の対象とする組織

- 本制度で定めるセキュリティ対策の実施主体として想定するのは、サプライチェーン企業(2 社間の契約における受注者側)。サプライチェーン企業が対策を実施するに当たって、発注者による協力が必要な場合があることから、制度が想定する対象事業者(制度利用者)の範囲は、赤枠囲いとする。なおサプライチェーン企業は、取引によっては発注者にもなりえる。
- 評価取得の申請主体は、自社IT基盤を中心とした自社のセキュリティ対策の向上に責任を有する単位(基本的には法人単位、企業グループ単位又は事業部単位)とする。



3.3 制度において設ける段階（★３・★４）　3.3.1 段階別評価の概要

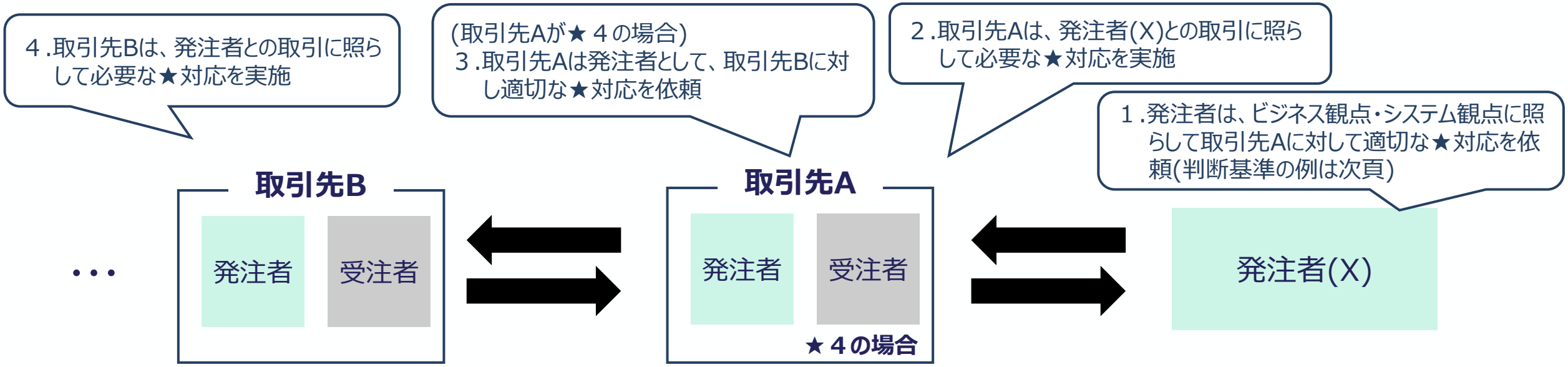
- ★３については、一般的なサイバー脅威に対処しうる水準を目指すものとして規定。
- ★４は、初期侵入の防御にとどまらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合したサプライチェーン強靭化策が講じられていることを水準として想定。
- ★５については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定(★3・4の精査も踏まえ、今後更に具体化)。
- 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[*1]	★４	★５[*4]
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（**実地審査及び技術検証を含む評価**によって対策実施状況の確認を行う。）	• 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。	• **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	**専門家確認付き自己評価**[*2]	**第三者評価**[*3]	**第三者評価**[*3]
有効期間	1年	3年	TBD
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(Lv3については一部の項目) • 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

*1　★１・★２については、IPAが運営する「SECURITY ACTION」を参照されたい。
*2　★取得希望組織が自ら実施した評価の結果について、セキュリティ専門家による確認及び助言を経て、取得希望組織の評価結果として確定させることをいう。
*3　★取得希望組織が自ら実施した評価の結果について、★取得希望組織以外の組織(評価機関)による評価等を経て、評価結果として確定させることをいう。
*4　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、今後対策事項を検討

3.3 制度において設ける段階（★３・★４）　3.3.2 再委託先への適用の考え方(例)

- 再委託先への本制度の適用は、元の発注者ではなく直接の取引先(委託先)による判断で実施。
- 直接の取引先(委託先)が★４対象の場合、★４要求事項に「重要な取引先におけるセキュリティ対策状況の把握」があるため、重要な機密情報が提供されている再委託先等にも一定の適用が期待される。

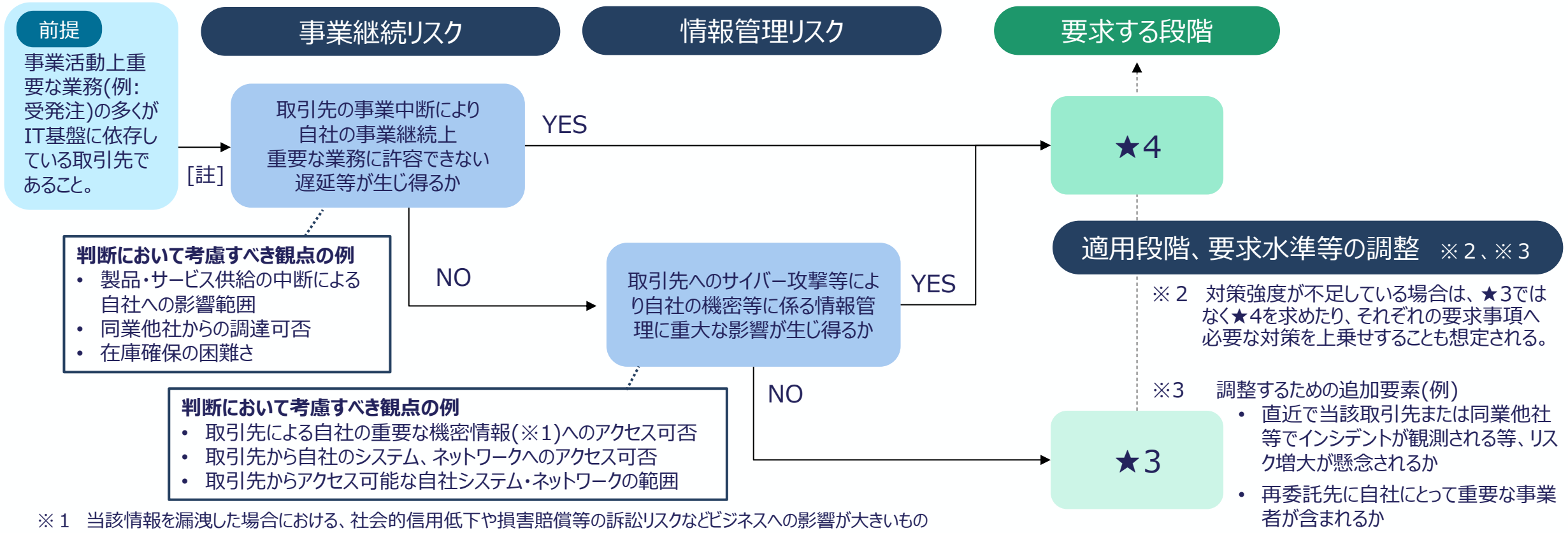


★４要求事項(案)	★４評価基準(案)
2-1-3　重要な機密情報を取り扱う取引先のセキュリティ対策状況を把握すること。	・以下に示す条件のいずれか若しくは複数に該当する子会社又は取引先を対象に、年１回以上の頻度で、以下の例を参考にセキュリティ対策状況を把握すること。 [対策状況把握の対象とする子会社又は取引先の条件] - 自社の重要な機密情報を提供・共有する - 自社の事業継続にとって重要な位置づけを持つ - 当該取引先の環境から発注者の内部システムへのアクセスが可能 [対策状況の把握方法(例)] - 本制度が定める★の取得状況について取引先から回答を受領する、又は本制度の運用主体が管理するWebサイト等で確認する - 取引先に訪問し点検を実施する - セキュリティ対策チェックシートを作成して回答を受領する

3.3 制度において設ける段階（★３・★４）　3.3.3 ★3・★4適用の考え方(例)

- サプライヤー企業への適用に当たっては、例えば以下のように、事業継続リスクと情報管理リスクという２つの主要なリスクに着目し、取引先を★４又は★３の段階に割り当てたり、必要に応じて適用段階、要求水準等を調整することが考えられる。
  (※)★５適用の考え方については、対策基準や評価スキームの具体的なあり方等と同様、令和８年度以降に具体化を進める予定。

■　★3・★4適用の考え方(例)



※１　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

[註]　単発・一過性の調達や、市販品など市場で容易に代替可能な製品・サービスの調達等のうち、重要度が相対的に高いとは言えないものについては、本フローの対象から外すことも考えられる。

3.4 制度で用いるセキュリティ要求事項・評価基準　3.4.1 要求事項・評価基準

- NIST Cyber Security Framework(CSF)の機能に対応した６つの分類に、取引先管理に重点を置いた分類を加えた７つの分類において、それぞれレベルごと達成すべき対策を提案。詳細は別添を参照。要求事項・評価基準は、サイバーセキュリティの動向等を踏まえ今後定期的な見直しを想定。

[註] 以下は必ずしも全要求事項を網羅しているわけではない点に留意されたい。　[註] []内は要求事項No.を指す

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 制度で用いるセキュリティ要求事項・評価基準　3.4.2 ガイダンス資料の整備

- ★３・★４要求事項・評価基準に加え、★取得希望組織による自己評価及び評価機関による第三者評価等を支援する観点から、具体的な評価手法やガイダンス情報を提示するためのガイダンス資料を今後策定する予定。
  ※　下記の図はあくまで本方針作成時点におけるイメージであり、完成後の文書とは異なる場合がある。

★３・★４要求事項・評価基準

要求事項

1-2-1 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。

評価基準

1-2-1-1 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・責任を定めること
1-2-1-2 平時のセキュリティ推進活動に必要な連絡先リストを定めること
1-2-1-3 年1回以上の頻度及び必要に応じて、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を行うこと
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していること

具体的事項や手法について補足

★３・★４ 自己評価ガイド(仮称)

【1-2-1-1の解説・評価方法】

・・・

【1-2-1-4の解説・評価方法】

- 情報セキュリティ委員会のような特別な体制を設置している場合、体制の代表者は、必ずしも役員である必要はなく、部門長クラスの就任でもよい。
- 情報セキュリティ委員会のような特別な体制がない場合、経営会議や取締役会等のより上位の会議体の議題として年1回以上の頻度で取り上げられることが定められているか、又はそれに相当する記録があるかを確認する。

★４ 第三者評価ガイド(仮称)

【1-2-1-1の評価方法】

- 面談：「CISO 等やセキュリティ担当部署の役割・責任」(1-2-1-1)について社内規程等に定められているか確認を行う。

【1-2-1-2の評価方法】

- 閲覧：「平時のセキュリティ推進活動に必要な連絡先リスト」(1-2-1-2)について現物確認を行う。

★４ 技術検証ガイド(仮称)

・・・

実施手順

① 特定されたIPアドレスを、推奨されるTCP/UDPポートとセットでスキャンすること。
② インターネットにアクセス可能なサービスのうち、脆弱性等悪用時に内部への不正アクセスのリスクが高いものについて、以下の事項の確認を実施すること。

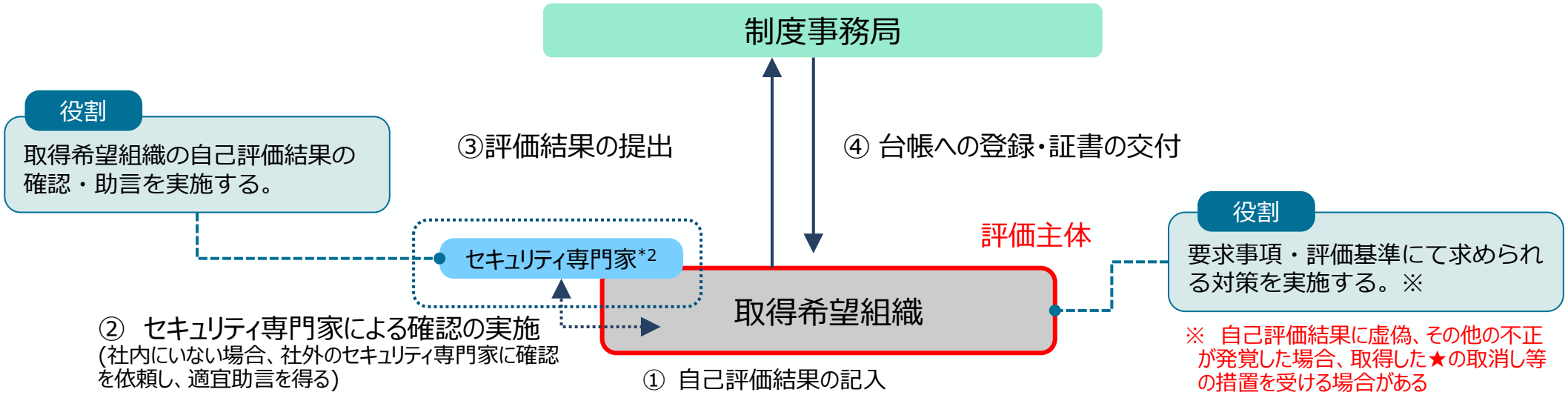
- CVSS 7.0以上の脆弱性の有無
- 多要素認証の実装有無
- 初期パスワードの変更有無

3.5 制度における評価スキーム　3.5.1 各段階の評価スキームの概要 - ★3

- ★３は、セキュリティ専門家による確認を経た取得希望組織による自己評価*1(専門家確認付き自己評価)を求めるスキームとする。

専門家確認付き自己評価：★3

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 登録機関は、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



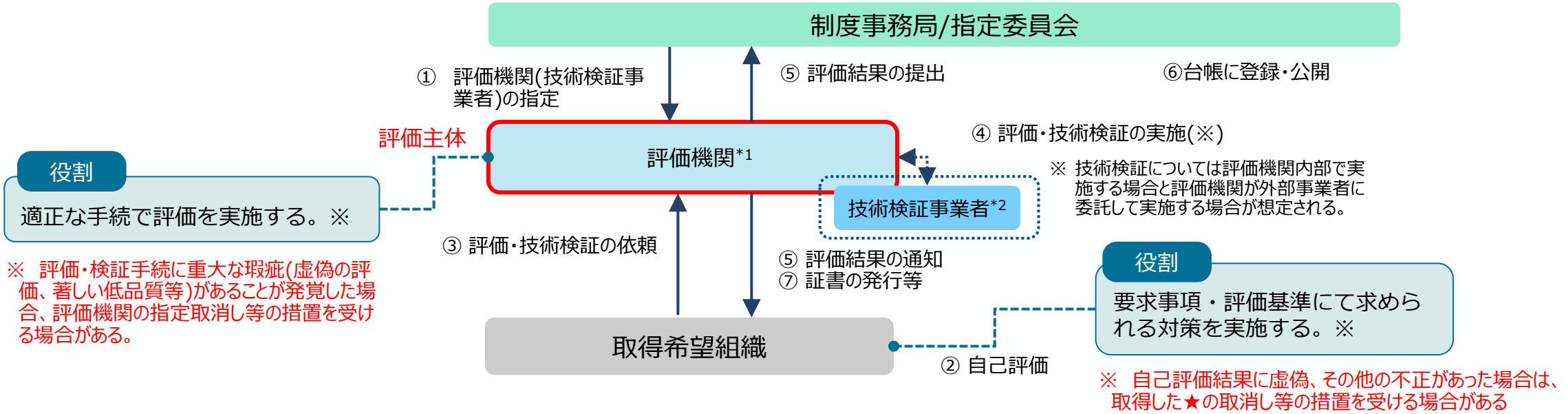
*1　経営層による自己適合宣言を経た取得希望組織として実施する評価のことを指し、組織内のセキュリティを担当する担当者や部門が独自に実施する評価は含まれない。
*2　取得希望組織が実施した自己評価結果に対してその内容の確認・助言を実施する者であって、一定のセキュリティ関連資格を有し、かつ、制度側で指定した研修を受講したものをいう。確認・助言に係る作業については、制度側で指定した研修を受講した作業従事者に実施させることができる。(20ページ参照)

3.5 制度における評価スキーム　3.5.1 各段階の評価スキームの概要 - ★4

- ★４は第三者評価(要求事項について評価機関による審査(取得希望組織へのヒアリング、規程の確認等)）及び技術検証(後述)の実施を求めるスキームとする。

第三者評価：★4

① 指定委員会は、評価機関・技術検証事業者を指定する。
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 取得希望組織の求めに応じて評価機関から証書を発行



*1 指定委員会による指定を受けた組織であって、取得希望組織外の立場で★4取得希望組織に対する第三者評価を実施するものをいう。
*2 指定委員会による指定を受けた組織であって、取得希望組織外の立場で★4取得希望組織のIT基盤等に対して制度側が指定した方法による技術的な検証を実施するものをいう。

3.5 制度における評価スキーム

3.5.2 セキュリティ専門家、評価機関及び技術検証事業者の要件 - セキュリティ専門家の要件

- 「力量の保有/維持」及び「研修の受講」の観点から、セキュリティ専門家の要件を設定することとする。当該セキュリティ専門家による管理のもとで別に要員に確認等の作業を行わせる場合、当該作業の従事者(作業従事者)には制度が定める研修の受講を求める。
- 情報処理安全確保支援士、公認情報セキュリティ監査人、CISSP、CISM、CISA、ISO27001主任審査員をセキュリティ専門家の資格として設定する。

セキュリティ専門家及び作業従事者の要件

- セキュリティ専門家には力量の保持/維持と研修の受講に係る要件を課す。
- 当該セキュリティ専門家による管理の下、別の要員に作業を担わせる場合、当該作業従事者には制度が定める研修の受講を求める。

	役割	力量の保持/維持	研修の受講
セキュリティ専門家 *自らの監督の下で確認の実務を作業従事者に担わせることが可能	確認過程全般を統括し、確認を行った上で、自らの責任において確認結果に対する署名を行う。	• IT・セキュリティに関する高度な知見(ITSSレベル4以上又はそれに相当する力量)を保持していること • 上記に加え、力量を維持するために保持している知識を更新していること	★3専門家として制度が定める研修を受講していること
(セキュリティ専門家が実際の作業を作業者に担わせる場合) **作業従事者**	セキュリティ専門家の監督下で、確認を行う。	(不要)	同上

セキュリティ専門家の力量の保持/維持要件を満たす資格

項目	力量の保有	力量の維持
情報処理安全確保支援士	• ITSSレベル4に位置づけられる	• 年次でオンライン講習を受けるとともに、3年間のうち1回実践講習を受ける。
公認情報セキュリティ監査人	• ITSSレベル4に相当する力量を有すると考えられる	• 監査業務等を通じて更新に必要な資格維持ポイントを取得する。
CISSP		• 講習受講、業務経験、書籍通読等を通じて更新に必要なCPEポイントを取得する。
CISM		
CISA		
ISO27001　主任審査員		• 審査実績の提出 • 15hの継続的専門能力開発(CPD)実績の提出

セキュリティ専門家及び作業従事者を対象とした研修

目的	• ★3の評価者として、本制度に関する概要や専門家業務を行うにあたっての注意事項を理解することで、円滑に助言・確認できるようになる。
研修項目	• 本制度に関する知見 • 専門家業務を行うに当たっての注意事項　等

※　上記研修の内容や実施スキーム等については、今後具体化していく予定

3.5 制度における評価スキーム

3.5.2 セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関及び技術検証事業者の要件

- ★4 第三者評価及び技術検証を行う資格を得るためには、所定要件に関して指定委員会の審査を受ける必要がある。
- 第三者評価を行うために満たすべき要件及び技術検証を行うために満たすべき要件を満たす場合、当該機関は双方の評価を行うことができる。

※ ★4 第三者評価及び★取得に向けたその他の技術的支援(第三者評価の実施を除く、コンサルティング、製品・サービスの提供等)について、それら双方を同一の法人等が実施することは必ずしも否定されるものではないと考えられる。その際、当該機関等が満たすべき中立性や公平性に関する要件等は今後詳細化する予定。

分類	評価機関及び技術検証に課す要件*1
★4 第三者評価を行うために満たすべき要件(評価機関の要件)	• 前頁に示すセキュリティ専門家の資格を満たすものを1名以上雇用し、当該セキュリティ専門家を自社が行う第三者評価における責任者として配置し、評価に従事する者及び成果物に対する監督等を行わせること • 評価に従事する者(第三者評価実施における責任者以外の従事者を含む)には制度が定める研修を受講させること • 情報保護マニュアルの整備や情報保護の維持・向上に関する手続きの導入を行っており、情報保護管理者を割り当てていること • 品質管理マニュアルの整備や品質の維持・向上に関する手続等の導入を行っており、品質管理者を割り当てていること
★4 技術検証を行うために満たすべき要件(技術検証事業者の要件)	• 以下に示す「情報セキュリティサービス基準適合サービスリスト」(脆弱性診断サービス)登録要件*2を満たすこと ✓ 専門性を有する者の在籍 ✓ サービス仕様の明示 ✓ 品質管理者の割当 ✓ 品質管理マニュアルの整備 ✓ 品質の維持・向上に関する手続等の導入 • 技術検証に従事する者(技術検証における責任者以外の従事者を含む)には制度が定める研修を受講させること

*1 第三者評価を行うために満たすべき要件及び技術検証を行うために満たすべき要件を双方満たす場合、双方の評価を行うことができる。
また、本要件は、制度構築方針における大枠を示したものであるため、今後初回の評価機関募集までの間に具体化を図る。

*2 「情報セキュリティサービス基準第 4.1 版」(https://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun4_1.pdf)

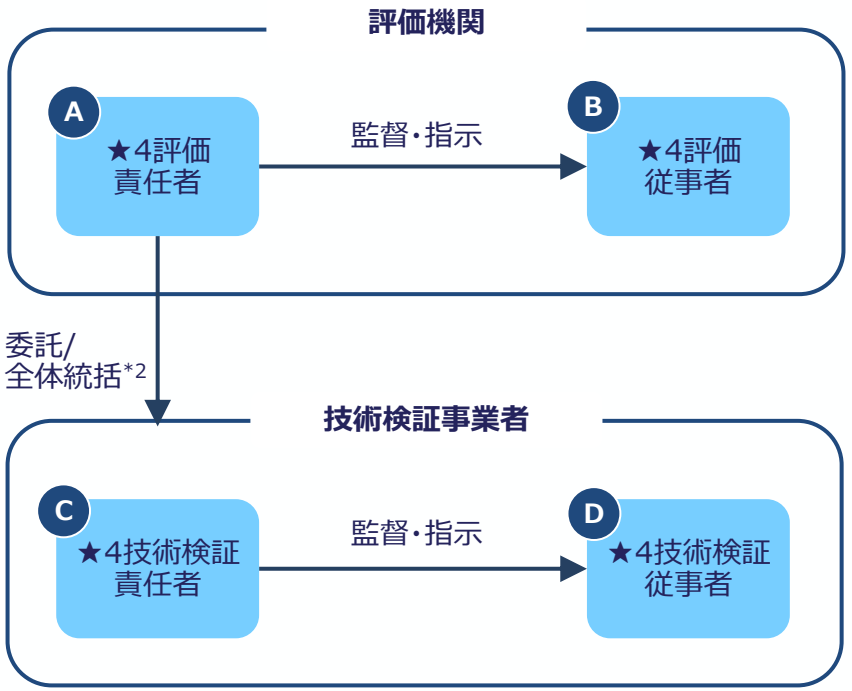
3.5 制度における評価スキーム

3.5.2 セキュリティ専門家、評価機関及び技術検証事業者の要件 - 評価機関の要件

- ★4 第三者評価における評価責任者は、セキュリティ専門家の条件(20ページ)を満たす必要がある。
- ★4 技術検証責任者は、原則として、「情報セキュリティサービス基準適合サービスリスト」(脆弱性診断サービス)における技術責任者を想定する。第三者評価及び技術検証における従事者に対しては、研修の受講は求めるものの所定の力量保持は必ずしも求めない。

分類		役割	前提	力量の保持/維持	研修の受講
第三者評価	A **★4評価責任者**	評価過程全般を統括し、自らの責任において評価を行う。	セキュリティ専門家の条件を満たすこと	(セキュリティ専門家として一定の要件を満たすため、追加の要件は課さない)	(セキュリティ専門家であり、既に研修を受講しているため、新たに要件を課さない)
	B (★4評価責任者が実際の作業を★4評価従事者に担わせる場合) **★4評価従事者**	★4評価責任者の監督下で、第三者評価に係る作業を行う。	なし	(不要)	以下に係る研修を受講していること(*1) - 本制度に関する知見 - セキュリティ専門家業務を行うにあたっての注意事項(評価活動実務、利害関係の注意等を含む)
技術検証	C **★4技術検証責任者**	技術検証過程全般を統括し、自らの責任において技術検証を行う。	原則として、「情報セキュリティサービス基準適合サービスリスト」(脆弱性診断サービス)における技術責任者を指す。	(情報セキュリティサービス基準適合サービスリスト」(脆弱性診断サービス)における技術責任者であり、既に力量を保持しているため、新たに要件を課さない)	以下に係る研修を受講していること - 本制度に関する知見 - セキュリティ専門家業務を行うにあたっての注意事項(評価活動実務、利害関係の注意等を含む)
	D (★4技術検証責任者が実際の作業を★4技術検証従事者に担わせる場合) **★4技術検証従事者**	★4技術検証責任者の監督下で、技術検証に係る作業を行う。	なし	(不要)	以下に係る研修を受講していること(*1) - 本制度に関する知見 - セキュリティ専門家業務を行うにあたっての注意事項(評価活動実務、利害関係の注意等を含む)

■イメージ図



*1 既に★3作業従事者として別途研修を受講している場合、新たに受講する必要はない。
*2 技術検証については評価機関内部で実施する場合と評価機関が外部事業者に委託して実施する場合が想定される。

3.5 制度における評価スキーム　3.5.3 評価の考え方 – 評価の実施内容

- ★3では、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では、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。
  ※ 以下の評価プロセスでは、各取得希望組織で決定した適用範囲の中から対象をサンプリングの上、評価等を実施することを想定。
  ※ より具体な実施内容を、本方針に基づき、令和８年度に検討・詳細化予定。

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

3.5 制度における評価スキーム　3.5.3 評価の考え方 – 評価の有効期間等

- ★３は有効期間を１年とし、対策状況を年次で点検し、基準全体の遵守を改めて確認している場合に更新可能とする。
- ★４は３年の有効期間とし、有効期間内は年次での自己評価(結果は評価機関に提出)をもって更新可能とすることを想定。
- ★３・★４のいずれにおいても、前回取得時に設定した適用範囲や要求事項・評価基準の遵守状況に影響を及ぼす変更*がある場合は、再度セキュリティ専門家又は評価機関の確認・評価を受ける。

	★3	★4	★5
評価実施主体	適合性評価の対象となる組織自身(自己評価)	指定委員会から指定を受けた評価機関(第三者評価)	TBD
有効期間	１年	３年	
維持に必要な手続き	• 有効期限を更新するため、要求事項の遵守状況について、年次でセキュリティ専門家の確認・助言を経た自己評価の更新版を登録機関へ提出する	• 有効期間内は、１年ごとに自己評価を実施し、結果を評価機関に提出 • 自己評価の更新に当たって、前回取得時に設定した適用範囲の変更又は要求事項・評価基準の達成に顕著な影響を及ぼす変更*がある場合は、再度評価機関の評価を受ける。 • 上記以外の軽微な変更がある場合は、変更後も要求事項に適合していることを表明するための自己適合宣誓書を提出する。 • 有効期限を更新する際(３年に１回)は第三者評価を受ける。	
合格基準	• 原則として、全ての評価基準への適合を求める。		
★の取消し等	• 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場合がある。		

＊ 以下のような変更が発生した場合を想定する。ただし、規程・手順書等における誤字脱字・体裁の修正や、要求事項・評価基準の達成に顕著な影響のない軽微な設定・運用上の変更を除く。
- 要求事項・評価基準に関連する社内規程・手順書等の大幅な変更
- 要求事項・評価基準の達成方法や運用方法の大幅な変更(IT基盤を構成する端末やサーバ等の大規模なリプレイス、クラウド基盤への大規模な移行、ネットワーク構成の顕著な変更 等)

3.6 評価結果の登録等

- ★３又は★４を取得した企業について、取得企業名及び所在地、更新回数、適用範囲等を含む情報を台帳に登録し、制度事務局のwebページ等で検索の上開示する仕組みを構築する予定。

※　下記の図はあくまで本方針作成時点におけるイメージであり、台帳の項目や開示の仕組みについては、今後具体化を図る。

台帳項目のイメージ

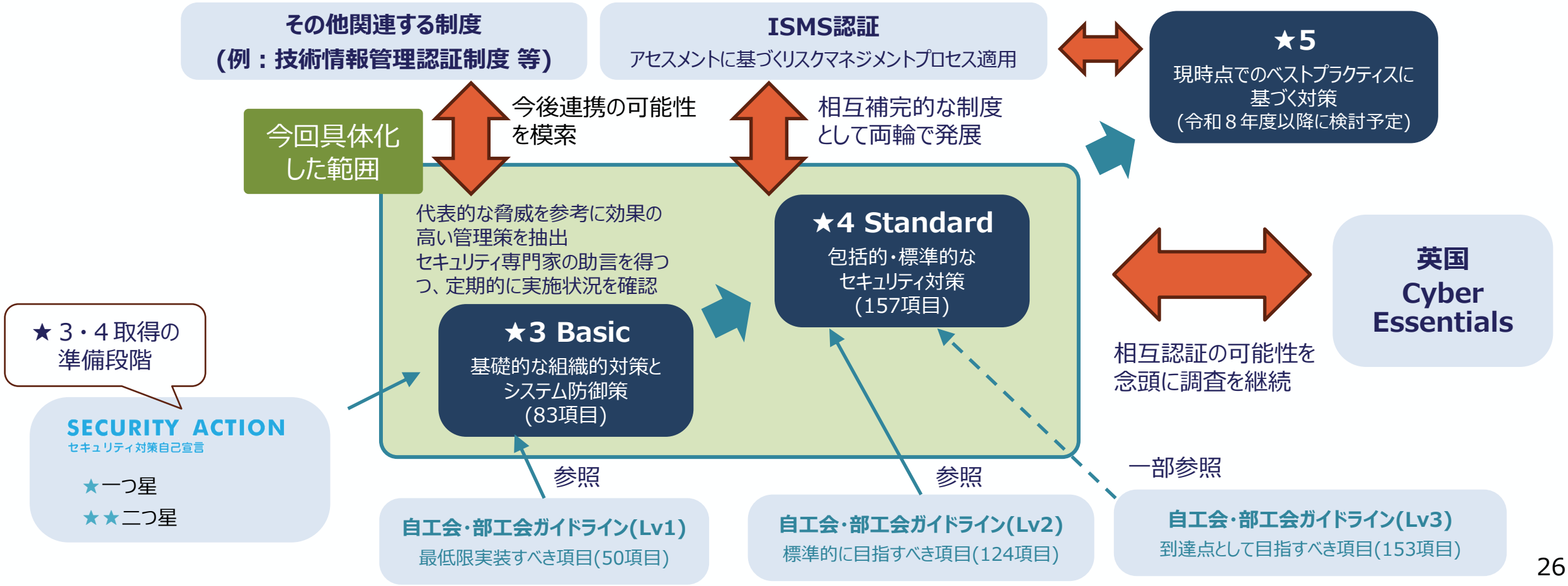
		区分	ID	名称	屋号	法人番号	所在地	評価取得日	有効期限	更新回数	適用範囲	評価機関名	技術検証事業者名
★3	法人の場合	○	○	○	－	○	○	○	○	○	○	－	－
	個人事業主の場合	○	○	○	(※任意)	－	(※任意)	○	○	○	○	－	－
★4	法人の場合	○	○	○	－	○	○	○	○	○	○	○	○
	個人事業主の場合	○	○	○	(※任意)	－	(※任意)	○	○	○	○	○	○

台帳のサンプル

		区分	ID	名称	屋号	法人番号	所在地	評価取得日	有効期限	更新回数	適用範囲	評価機関名	技術検証事業者名
★3	法人の場合	★3	000001	株式会社XX	－	0000000000…	東京都千代田区…	202X/10/1	202X/9/30	0	XXに限る。	－	－
	個人事業主の場合	★3	000002	霞が関太郎	(※任意で記載)	－	(※任意で記載)	202X/11/1	202X/10/31	2	全てのネットワーク	－	－
★4	法人の場合	★4	000003	株式会社XX	－	0000000000…	東京都千代田区…	202X/10/1	202X/9/30	3	全てのネットワーク	一般社団法人xxx	一般社団法人xxx
	個人事業主の場合	★4	000004	霞が関太郎	(※任意で記載)	－	(※任意で記載)	202X/11/1	202X/10/31	1	全てのネットワーク	一般社団法人xxx	株式会社xxx

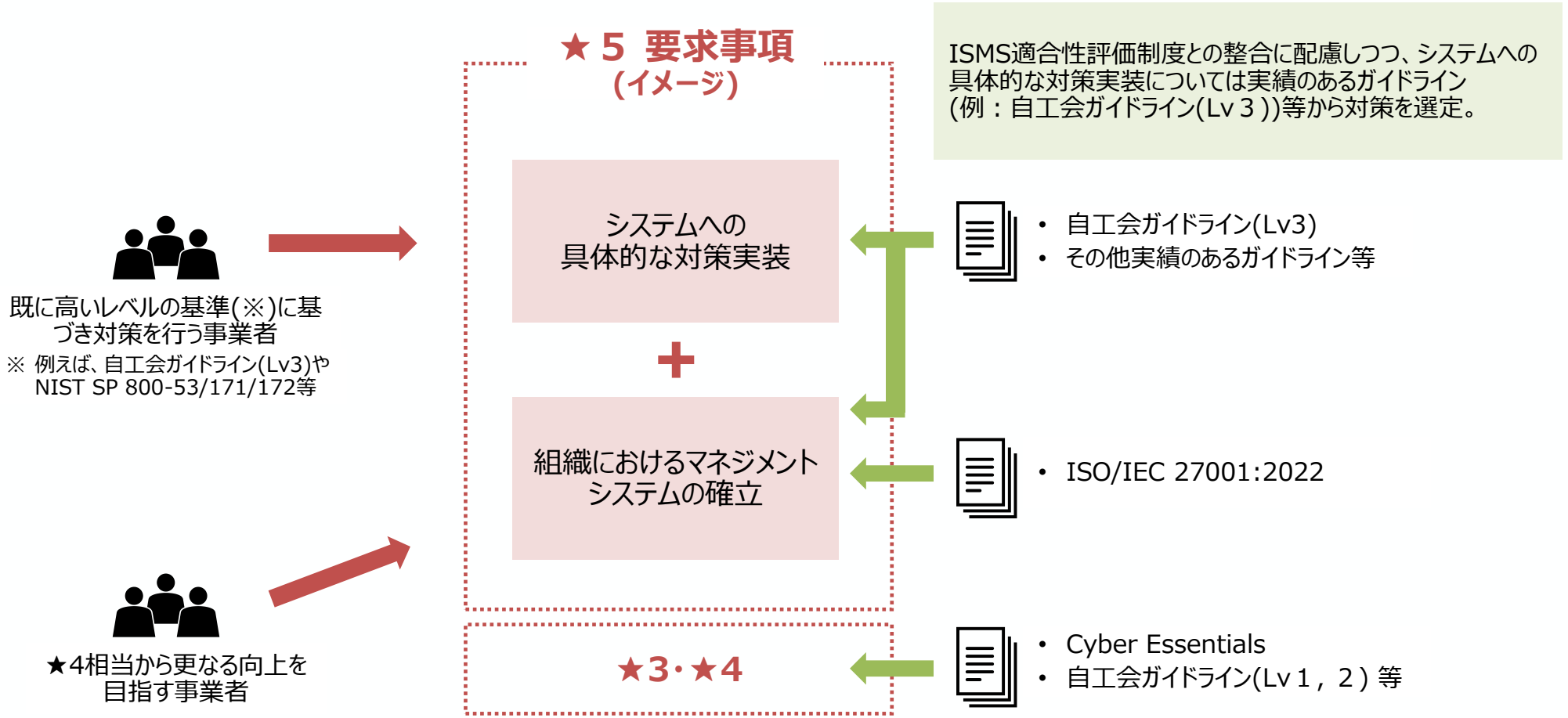
3.7 国内外の関連制度等との連携・整合

- 本制度(★３・★４)は、先行する仕組みである「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相互補完的な制度として発展することを目指す。
- ★３・★４は、自工会・部工会ガイドラインのLv１、Lv２に対応。自工会・部工会とは、本制度との連携を引き続き検討。英国CEとは、将来的な相互認証等の可能性も念頭に、引き続き調査・意見交換を継続。



3.8 制度において設ける段階（★５）　3.8.1 ★５の位置づけ

- ★５では、ISMS適合性評価制度との整合に配慮しつつ、システムへの具体的な対策実装については実績のあるガイドライン(例：自工会ガイドライン(Lv３))等から対策を選定することを想定。
- 令和８年度以降、対策基準や評価スキームの具体的なあり方等を検討する予定。(再掲)



[参考] ISMS適合性評価制度と本制度の比較

- 本制度(★３・★４)は、代表的な脅威を参考に効果の高い管理策を抽出先行するベースラインアプローチを採用。
- ★５段階では、組織におけるリスクベースの改善プロセスを整備した上で、システムへの具体的な対策実装が必要であり、ISMS適合性評価制度との整合に配慮しつつ、令和８年度以降具体的なあり方等を検討する予定。

	ISMS適合性評価制度	★５ 要求事項（イメージ）	本制度(★３・★４)
目的	・組織が運用する情報セキュリティマネジメントシステム(ISMS)が、国際規格に基づいて適切に運用管理されていることを第三者が公平な立場から審査し証明するための、国際的に整合の取れた枠組みを確保・維持すること		・サプライチェーン全体でのサイバーレジリエンスの向上 ・部品供給、業務委託等のビジネスサプライチェーンを通じたサイバーリスク(※)への対応を重視 (※)事業・サービスの供給途絶リスク、機密情報の漏えい改ざんリスク、取引先等を踏み台とした不正侵入リスク等
取得範囲	・ISMSを運用する「組織」が対象 (組織の単位は、管理する情報に応じて、認証取得を希望する組織が対象範囲を決定する。一企業内の特定部門のほか、グループ企業全体を認証範囲とすることもある。)	システムへの具体的な対策実装 ＋ 組織におけるマネジメントシステムの確立	・「インターネットに接続している自社IT基盤」が対象(一般的に、IT基盤が外部からの不正侵入やNW横展開の足掛かりとなるため、リスクの高いシステムとして制度側で指定) ・取引先管理の観点を盛り込み
採用する管理策	・リスクアセスメント結果に基づいて、リスク対策のために必要な情報セキュリティ管理策を組織が決定する。 ・ISO/IEC27001(JISQ27001)附属書Aを参照し、情報セキュリティ管理策(組織的・人的・物理的・技術的)に漏れがないかどうかを確認する。		・代表的な脅威や国内外制度を参考に、効果の高い管理策を業界横断的なコンセンサスとして設定することを目指す。 ★３：取引上の要請に応えるために最低限必要な対策 ★４：侵害の早期発見・拡大防止等に必要な対策
審査の観点	・ISO/IEC 27001で規定されている要求事項に適合したISMSが構築・運用できているか		・各段階(★３・★４)で求める具体的なセキュリティ対策が実装されているか
特徴	■ リスクアセスメント結果に基づき、組織自らが適切な管理策を決定 ■ 認証により、組織的に対策を維持・向上させる仕組み(マネジメントシステム)が構築できていることを証明	ISMS取得後SCを取得 相互補完的な制度として両輪で発展 SC取得後ISMSを取得	■ 代表的な脅威・リスクを前提に、具体的な対策や範囲が決められているため、何をするか迷うことが少ない ■ システムへの対策実装を、第三者評価で確認(★４)

3.8 制度において設ける段階（★５）　3.8.2 ★５の具体化に係る今後の進め方

- 実証事業を通じて、各参画企業から★５に対する意見、要望等を収集。
- 令和８年度以降、これらの意見、要望等も踏まえ、★５の要求事項・評価基準や評価スキームを具体化していく予定。

令和７年度(2025年度)　実証事業を通じた意見収集

- 実証事業を通じて、参画企業から★５に対する意見、要望等を収集

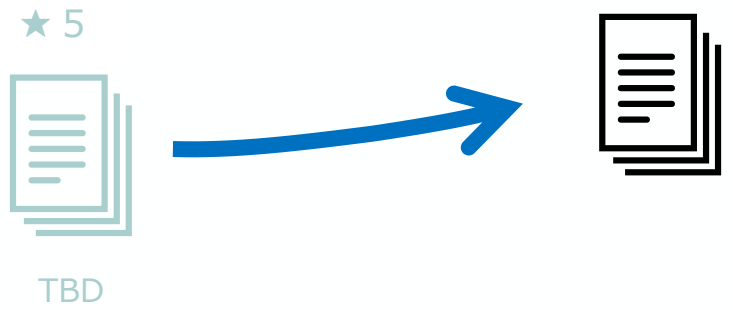
実証参画企業からの★５に対する主な意見・要望

＜要求事項・評価基準に関する意見＞
- 経営層の関与や内部不正対策など、**組織ガバナンスに係る項目をさらに充実させる**べき。
- 復旧ポイントや復旧時間を含めた復旧計画の策定や、復旧中の業務代替手段の確保など、**インシデントからの復旧に係る項目をさらに充実させる**べき。
- 技術的対策については、**先端技術や高度なセキュリティ施策(例：自動車業界ガイドラインにおけるLv3の内容)を厳選して定める**べき。
- インシデント対応演習等の**より実践的な対策**を含めてはどうか。

＜評価スキーム等に関する意見＞
- 経営層の関与をより確実なものとするため、**経営層へのインタビュー**を評価手法として取り入れたり、**経営層を含めて報告会等を行う**等を検討してはどうか。
- ★５では、**評価を受ける範囲をさらに広げつつ**(例えば、データセンターの訪問を含める等)、**より高度な技術検証**を含めるとよい。

令和８年度(2026年度)～　意見等を踏まえ具体化

- 実証参画企業等からの意見も踏まえ、★５の要求事項・評価基準や評価スキームを具体化していく予定



[参考] 関連する制度等との関係性 – JC-STARとの関係性

- 本制度は、サプライチェーン構成企業による自社IT基盤を中心とした自社のセキュリティ対策の向上を通じて、サプライチェーン全体の強靭性(事業継続性、機微情報の保護、取引先等を通じた不正侵入の抑制)の確保を目指すものである。

	本制度	IoT製品に対するセキュリティラベリング制度(JC-STAR)
対象範囲	• ビジネスサプライチェーンを構成する企業等 (物資・役務の調達等) • ITサービスサプライチェーンを構成する企業等 (MSP*、クラウドサービス等を含む。)	• インターネットに接続可能な機器：IP を使用してインターネット上でデータを送受信する機能を持つ機器 • ネットワークに接続可能な機器：他の「インターネットに接続可能な製品」や「ネットワークに接続可能な製品」に接続し、IP を使用してデータを送受信する機能を持つ機器
目的・内容	• サプライチェーン全体でのセキュリティリスクの低減を目的に、発注者(顧客)から受注者に求めるセキュリティ要件(自社IT基盤等、**サプライチェーン企業自身のセキュリティ対策**)の整理	• 共通的な物差しによる製品に具備されているセキュリティ機能の評価・可視化を目的に、**適切なセキュリティ対策が講じられているIoT製品**に求められるセキュリティ要件等の整理
制度の整備	• 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として、★３・★４の段階的評価制度を整備	• IoT製品に対するセキュリティラベリング制度(JC-STAR)として、★1から段階的に評価制度を整備

* Managed Service Provider

例えば、IoT製品の供給を行うサプライチェーン構成企業は、顧客からの要請に応じて、JC-STARによる製品ごとの評価に加えて、企業として本制度への対応が必要となる場合がある。

[参考] 関連する制度等との関係性 - 技術情報管理認証(TICS)との関係性

- TICSでは産業競争力強化法に基づき企業等における情報セキュリティ体制を審査・認証することで、技術情報の管理体制を強化し、漏えい等リスクを低減するとともに、産業基盤やサプライチェーンの安定性を維持することを主な目的としているが、本制度は組織面やサイバー攻撃を受けた際の事業継続も含めたセキュリティ対策全般を対象とし、かつ基準統一やコストの低廉な評価方法の採用等による社会的コスト削減を主体たる目的としている。

	本制度	技術情報管理認証(TICS)	両者の関係性等
目的・内容	✓ サプライチェーン全体でのセキュリティリスク(情報漏えい等に加え、事業継続リスクを含む)低減 ✓ 様々な取引先から様々な要求事項を求められる状況下における基準統一による企業の負担軽減	✓ 組織の「強み」となる技術情報の漏えい等リスクを低減し、産業基盤やサプライチェーンの安定性を維持 ✓ 適切な情報管理が行われることで、企業間のオープンイノベーションや研究開発連携を促進	✓ TICSが産業競争力強化法に基づき企業等における情報セキュリティ体制を審査・認証することで、技術情報の管理体制を強化し、漏えい等リスクを低減するとともに、産業基盤やサプライチェーンの安定性を維持することが目的であるのに対して、本制度は組織面も含めたセキュリティ対策全般(情報漏えい等への対策に加え、サイバー攻撃を受けた際の事業継続に係る対策を含む)を対象としつつ、かつ基準統一による社会的コスト削減を主体たる目的としている。 ✓ 本制度★3及びTICSは、いずれも自工会/部工会ガイドラインのレベル1の項目をベンチマークとする。 ※★3では一部の技術的対策においてより詳細な管理を求める。 ✓ 本制度★4では、さらに、自工会/部工会ガイドラインのレベル2の項目をベンチマークとしている。
要求事項の概要	✓ ガバナンスの整備 ✓ 取引先管理 ✓ リスクの特定 ✓ 攻撃等の防御 ✓ 攻撃等の検知 ✓ インシデントへの対応 ✓ インシデントからの復旧	✓ 守る情報の決定 ✓ 守る情報の識別・対策整理 ✓ 管理責任者選任 ✓ 情報管理プロセスの設定 ✓ 従業員への対策周知や教育 ✓ 情報漏えい等の事故発生時の報告ルールの設定 ✓ 管理対象情報へのアクセス権の設定 ✓ 金庫等による物理的情報の管理 ✓ ID設定等による電子情報の管理	
評価スキーム	★3： 専門家確認付き自己評価 ★4、★5：第三者評価 ※★1及び★2については「SECURITY ACTION」を参照	第三者認証 ※認証機関として7機関が認定されている。	✓ 取得段階が複数又は単一か、取得時に第三者評価を求めるかが異なっている。

発注元企業及びサプライチェーン構成企業は、個社の事情を勘案しつつ、これらの制度を柔軟に使い分けることも想定される

- 製品の企画・設計・製造等において顧客の重要な技術情報等の提供を受ける場合は、TICS又は本制度★4の取得を進める。
- 第三者認証の取得が必要ない場合は、本制度★3の取得を推奨する。 等

[参考] 関連する制度等との関係性 – 海外諸制度との関係性

- 本制度は各業界共通でサプライチェーン強化のためのセキュリティ対策を示すことで、サプライチェーンにおけるセキュリティリスクの低減や、サプライヤー企業の負担軽減を目的とした制度である。

	本制度	Cyber Essentials/ Cyber Essentials Plus	CMMC 2.0	TISAX
制度所管	• 経済産業省/ 内閣官房国家サイバー統括室	• 英国 国家サイバーセキュリティセンター(NCSC)	• 米国 国防総省(DoD)	• ドイツ自動車工業会(VDA)
目的	• サプライチェーン全体でのセキュリティリスク(情報漏えい、事業の停止等)の低減 • 様々な取引先から様々な要求事項を求められる状況下における基準統一による企業の負担軽減	• 企業の規模によらず一般的に想定されるサイバー攻撃全般からの組織の保護	• 国防サプライチェーン全体のサイバーセキュリティ強化 • 管理対象非機密情報(CUI)、連邦契約情報(FCI)の保護	• 自動車業界のサプライチェーンにおけるサイバーセキュリティ強化 • 各自動車メーカー(OEM)等における基準統一による企業の負担軽減
主な対象	• ビジネスサプライチェーンを構成する企業等(物資・役務の調達等) • ITサービスサプライチェーンを構成する企業等(MSP[*1]、クラウドサービス等を含む。) *1 Managed Service Provider	• 英国内に拠点を置く全ての企業	• 国防総省から発注を受ける防衛産業基盤(DIB：Defense Industrial Base)企業	• 自動車メーカー(OEM)及びそのサプライヤー等
要件・要求事項	• 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」等に資する要求事項を提示	• 「ファイアーウォール」、「セキュアな構成」、「セキュリティアップデート管理」、「ユーザアクセス制御」、「マルウェア対策」の５つのカテゴリで要求事項を提示	• NIST SP800-171等から抽出された要求事項	• ISO/IEC 27001等をベースとした要求事項に加え、「試作品保護」、「データ保護」に係る要求事項
評価スキーム	• ★3:専門家確認付き自己評価 • ★4、★5:第三者評価	• CE：自己診断後、認証機関が回答を評価 • CE+：評価機関による技術検証(CE取得が前提)	• LV1:自己評価 • LV2:取り扱う情報の種類に応じて、第三者評価又は自己評価 • LV3: 防衛産業基盤サイバーセキュリティ評価センター(DIBCAC)による評価(LV2取得が前提)	• 審査機関による審査

4. 制度の導入促進策

導入促進策の全体像

- ★取得のための各プロセスにおいて推進している支援策について、以下のとおり整理。

発注元企業	★の取得を求める				
サプライヤー企業		制度について知る	必要な対策を講じる	★を取得する	★を更新等する
実施事項	■ ★の取得をサプライヤー企業に求めることを通じてサプライチェーン全体のサイバーレジリエンスを向上させる。	■ 制度についてインターネット等で情報収集する。 ■ セミナーや講習等に参加する。	■ 必要に応じてベンダーやセキュリティ専門家からの協力を得つつ、★取得に必要なセキュリティ対策を講じる。	■ セキュリティ専門家からの確認(★3)、又は評価機関等からの第三者評価(★4)を受け、★を取得する。	■ ★の有効期限に基づき、適宜更新及びそれに必要な手続き等を行う。
導入促進策	✓ **取引先への要請等に係る考え方の整理** サプライヤー企業への要請に係る独占禁止法等との考え方整理	✓ **本制度の継続的な広報、周知** 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実施	✓ **中小企業セキュリティ普及促進** ★3・★4に対応した、新しいお助け隊サービスの開発を検討	✓ **取引先への要請等に係る考え方の整理** 発注元企業は、★取得による価格交渉に積極的に対応する必要がありかつ委託先にこれを周知する必要がある等	
	✓ **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いて、本制度の要求基準等の活用や★取得確認の推奨を推進	✓ **「中小企業の情報セキュリティ対策ガイドライン」の整備** 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★の取得を支援		✓ **セキュリティ評価・対策支援人材の育成** 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整備	
	✓ **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	✓ **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」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を検討	✓ **専門家の活用促進** 「中小企業向けサイバーセキュリティ専門家リスト」を整備し、主に中小企業と専門家とのマッチングの仕組みを構築		

[参考] サイバーセキュリティお助け隊サービス（新類型）について

- 本制度の**★３・★４の取得支援**を目的とする。具体的には、★３・★４の対策項目のうち**未達成の項目について、お助け隊サービス(新たな類型)の導入により全部又は一部の対策項目を達成させる**ものとする。
- STEP１として、サービス提供に当たって**本制度の★取得及び更新時に中小企業の対策状況を評価**することをサービスに含める。
- STEP２として、本制度の対策項目の中には、ITツールの導入により達成できる項目や、人的支援により達成できる項目があるため、お助け隊サービス（新類型）は「**ITツールによる支援**」のほか「**ITツール以外の支援**」を組み合わせて提供することをサービス内容とする。

お助け隊サービス（新類型）のイメージ

STEP1：課題の可視化

✓本制度の要件項目毎に中小企業の**対策状況を診断**

✓本制度の**更新時に、各対策項目の対策状況を評価**

STEP２：対象サービスの選定と対応実施

✓診断結果に基づき、以下の支援を実施

✓ITツールによる支援
★３・★４取得に推奨されるITツールを導入

✓ITツール以外の支援
セキュリティポリシーやインシデント手順書の整備、セキュリティ教育など、中小企業が自助努力で達成しづらい項目を支援

【サービス例】

★4＋	★４要件に駆付け支援がプラスされたサービス
★4	★４要件を最低限満たすサービス
★3＋	★３要件に駆付け支援がプラスされたサービス
★3	★３要件を最低限満たすサービス

STEP1・STEP2の支援サービスを一定の価格要件の下で提供

STEP3：★取得

✓ 本制度の★3もしくは★４の**項目要件をすべて充足することで★を取得**

[参考] サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説（概要）

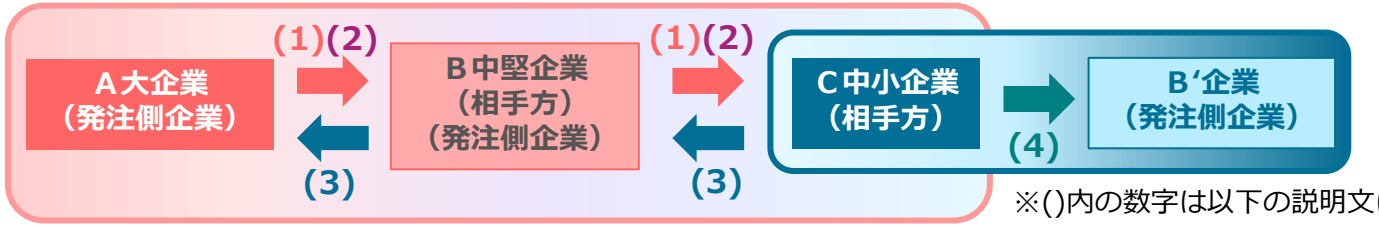
経済産業省・公正取引委員会

○　経済産業省及び公正取引委員会では、「サプライチェーン全体のサイバーセキュリティの向上のための取引先とのパートナーシップの構築に向けて」を補足するため、**発注者・相手方双方を対象とした、独占禁止法・取適法上「問題とならない」想定事例及びその解説文書を作成。**

○　想定事例は、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基づく対策要請を円滑に行い、発注者側・相手方がパートナーシップを構築してセキュリティ対策と価格交渉を実施し、円満に合意するものとしている。

【想定事例】

【サプライチェーンのイメージと想定事例の各場面】



※()内の数字は以下の説明文に対応

(1) セキュリティ対策実施の要請

A（大企業）は、相手方であるB（中堅企業）に対し、①組織ガバナンス・取引先管理、システム防御・検知、事案対応等の対策の実施(＊)、②Bの相手方であるC（中小企業）に対し①と同様の対策を講ずることを要請

(＊)**「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）」中の「★４」に相当**

(2) 要請に当たってのパートナーシップの構築

Aは、自社の対応方針を定め、B・Cに対する説明会を定期的に開催（講ずべきセキュリティ対策の内容や国の支援策等を説明）。また、AからB、BからCに対し、費用負担の考え方、セキュリティ対策が価格交渉の対象になる旨、価格交渉に積極的に対応する旨を周知。

(3) 要請への対応と価格交渉の実施

B・Cは、それぞれ発注者側から受けた説明により対策の必要性を理解し、国の支援策を活用することで要請された対策を安価に実現。対策に要したコストに関し、発注者側による説明に基づき価格交渉を実施し、円満に合意。結果を双方が書面に記録して保存。

(4) 要請を行っていない発注者側企業への対応

Cは、要請を受けていないB'（中堅企業）とも価格交渉を行うため、取引かけこみ寺などの支援機関へ相談。得られた助言に基づき、Bとの交渉で用いた費用負担の考え方等を整理した上でB'に対し価格交渉を申し入れ、対策の必要性や同社との取引割合などを勘案した費用負担の考え方等を説明。交渉は円満に合意に達し、結果を双方が書面に記録して保存。

【想定事例解説】

想定事例を補足するため、以下の点について解説を作成。

① SCS評価制度に基づいたセキュリティ対策要請が合理的範囲を超えた負担を課すものではないこと。
② 発注者・相手方双方でパートナーシップを構築することの必要性や重要性。
③ セキュリティの経費が物件費や人件費などの間接経費として計上されること。
④ 価格交渉の考え方や、要請をしていない発注者側企業に対する価格交渉に当たって支援機関を活用すること。
⑤ 取引かけこみ寺や公正取引委員会の事前相談制度・一般相談・事例集の紹介。

【今後の取組】

本文書について、経済団体や中小企業支援機関等に協力いただきつつ、大企業・中小企業等の双方に対して、普及展開を進めていく。

[参考]中小企業向けサイバーセキュリティ対策支援者リストについて

- 「中小企業向けサイバーセキュリティ専門家リスト」を整備し、主に**中小企業と専門家とのマッチングの仕組みを構築**する。
- 2025年7月からリストを試行公開するとともに専門家による中小企業指導の支援ツール（5テーマの実施要領）を公表。今後、**本制度におけるセキュリティ専門家の確認・助言に資する支援ツールを追加**する予定。

中小企業向けサイバーセキュリティ対策支援者リスト

- 国家資格「**情報処理安全確保支援士（登録セキスペ）**※」の資格者のうち、**中小企業向けのサイバーセキュリティ対策支援**が実施できる専門家の**得意分野・専門領域を可視化**したリスト（支援対象地域別）
- 現段階の情報を試行公開（PDF）。今後、整備・拡充する予定
- URL：https://www.ipa.go.jp/security/sme/shien/list.html

※サイバーセキュリティ対策を推進する人材の国家資格。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、セキュリティの確保を支援する。国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務を有する。 https://www.ipa.go.jp/jinzai/riss/index.html

- 掲載専門家の**支援対象地域別**にリスト化
  支援対象地域：北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄
- 掲載専門家が支援可能な**指導テーマ**、支援**実績**、得意とする**業界**、支援可能**形態**、支援**料金**、保有**資格**、保有**スキル**等を記載

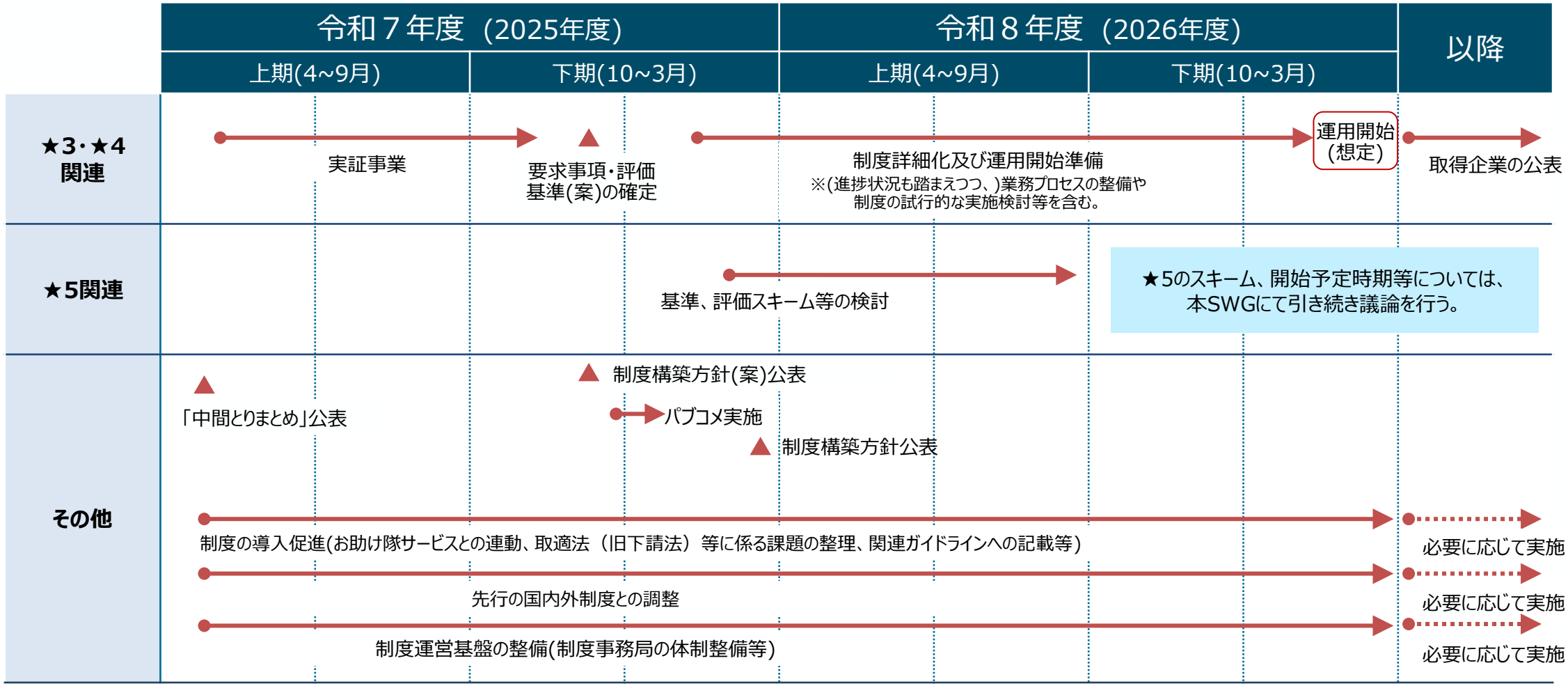
- 専門家による中小企業指導の支援ツール（5テーマの実施要領）を整備・公表
  - テーマ(1) 情報セキュリティ規程の整備
  - テーマ(2) 情報資産の洗い出しとリスク分析
  - テーマ(3) クラウドサービスの安全利用
  - テーマ(4) セキュリティインシデント対応
  - テーマ(5) 従業員向け情報セキュリティ教育

※支援ツールは今後も拡充予定

5. 今後の検討の進め方及びスケジュール

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。



METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html