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

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

目次

これまでいただいた主なご意見

1. 制度の目的と位置づけ

◆ 制度化の要否について

- ある程度政府が前に出てメッセージを出すべきものと理解している。**業界に任せるより国として制度化を目指すべき**ではないか

◆ 制度の目的について

- 中小企業の状況を改善することで社会全体がよくなるという位置づけを示して**ブランディングすべき**ではないか
- 業界でも発注者や受注者だけでなく業界全体として取り組みを進めているところ、**本制度についても日本全体のため、というメリットで説明**いただきたい

◆ 制度の位置づけについて

- サプライチェーンは製造業の他、業務委託やサービスの利用等も含む。モノの供給や情報漏えいという観点からも、**サプライチェーンの定義を明確にすべき**ではないか
- サプライチェーンに属する企業だけではなく、**属してない企業も取得すべき**でないか。サプライチェーンという用語を前に出すと、**自社は関係ないという考える企業も多い**。委託先は広義のサプライチェーンであり、メッセージの出し方が重要。
- ★３を上場企業の取引上の最低条件とする世界観を目指してはどうか

◆ 他の制度等との関係について

- **「サイバーインフラ事業者に求められる役割等の検討会」との棲み分けを明確**にすべき
- 現状、既存制度等がサプライチェーン全体に対して求める対策に俯瞰性と網羅性がない。全体のなかでの本制度の位置付けを明確にするガイドを示すことはできるのではないか

これまでいただいた主なご意見

2. 構築する評価制度

◆ 対策の適用範囲について

- **取得のスコープをどう設定するか明確化**いただきたい。また、**適用範囲としてどこまで評価されたか情報開示**して欲しい
- 中小、中堅、大企業でも、**★３★４★５が組織内で混在してるが、どう対応すればいいのか明確化**されたい
- 適用対象を整理すべき。HD化した企業も多いので、**法人単位、企業グループ単位としていただいた方がわかりやすいが、大きな企業では事業部単位で対応が異なっている可能性**がある。**引き続き検討をいただきたい。**
- クラウドの活用が広く進む中で、中小企業ですべてのITシステムを丸投げしている会社もある。その場合どうすべきか実証等も通じて明確化されたい

◆ 制度で設ける段階について

- サプライチェーンの重要性や業界の立場、重視するリスクの種類（情報漏えい、業務継続に係るリスク等）に応じて実施すべき対策という観点で、**制度の各段階で求める対策のレベル分けをすべき**ではないか
- 対象事業者を判断する際に、ビジネス観点（データ保護及び事業継続）及びシステム観点について、「取引先がサイバー攻撃を受けたと想定した際の自社ビジネスへの影響」が「想定されない、または影響範囲小」のときに★3とすると、**現実的に★3に該当する企業はなくなるのではないか**
- 調達元が委託先へ★5を要求する場合に、再委託先等に対しても同等の対策レベルを求めるのか、あるいは下げてもよいかなど、どう判断するのか明確化されたい

◆ 要求事項・評価基準について

＜★3★4共通＞

- 対策の方向性がずれうるため、どのレベルにおいて何を求めるかは注意が必要ではないか
- セキュリティ対策は導入して終わりではない。**パッチの適用等、運用面でのセキュリティ対策も補記すべき**ではないか
- 既存ガイドラインを引用するならば、引用時の考え方は明示すべきではないか
- 中小企業を対象とする場合、セキュリティベンダーにおいても各段階の対策を運用する仕組みや、対策の内容に一定の責任を持たせるなど、中小企業が責任をもって自社の対策を把握し、★3や★4を運用できる形式とする必要があるのではないか
- **★3★4の要求事項、評価基準は、ANDで見るのか、ORで見るのか、明確**にしてほしい
- 技術や攻撃パターンも更新されていく。**制度として更新をしていくべき**である。取得した企業も★を取得して満足するのではなく、常に対策を続けていくことが重要なのではないか

これまでいただいた主なご意見

2. 構築する評価制度 (前頁の続き)

◆ 要求事項・評価基準について

＜★3について＞

- **★3の対策事項群には、アタックサーフェスマネジメントの導入方法についても盛り込むべき**ではないか
- 現状の対応や復旧に係る対策事項の記載が簡素。★3が基本的な対策ならば、復旧プロセスは詳細に示すべきではないか。

＜より詳細なガイド等の必要性について＞

- 現状の案では中小企業の担当者は何をすればよいかわからず踏み込んだことをしない可能性があるため、**より具体的な内容を記載**してはどうか
- **★3や★4について、よりブレイクダウンしてガイドを作成**いただけるとありがたい。
- 対策要件で、機能を求めるだけではわかりにくいため、特定の製品を推奨するなど例示をするほうが理解しやすいのではないか

◆ 認証スキームについて

＜★3★4共通＞

- ★を一度取得してそのままでよいのか。**定期的な更新の方法について決めておくべき**ではないか
- ★3をとってから★4なのかという点について、★3取得からとなるとレベルダウンしたところから始まるので、ぜひ★4から取得できるように検討されたい
- **依頼主の希望により詳細な情報をサプライチェーン構成企業から開示**いただけるよう仕組みを検討されたい
- ★4、★5等を取得された事業者はどのようにそれをアピールできるか、英国CEの事例等も参考に検討されたい

＜★4における第三者評価について＞

- **自己評価だけでは発注者側にとって担保が不足**する。第三者評価は発注者サイドにとっては頼りになるのではないか
- **第三者評価を採用すれば費用が増す**。取引先や業種や業態に応じて選択できるように、第三者評価を切り離すべきではないか
- 第三者認証においては、**認証機関を認定する機関を設ける必要**がある。また、**認証機関は複数設けるべき**ではないか
- **評価機関や検証事業者の具体的な資格要件を検討**すべき
- 実運用する際、評価制度機関について他省庁の制度との関係性や連携等を整理すべきではないか
- **評価を実施する工数や費用の検証や、取得組織が対策する際の負担感についても実証で検証**されたい

これまでいただいた主なご意見

2. 構築する評価制度 (前頁の続き)

◆ **国内外の関連制度等との連携・整合について**

- サプライチェーンの下流に位置する企業には、様々な業界から要求事項が来る。本制度を策定する際は、米国におけるNIST SP 800や、自工会のガイドラインのように、**上位のガイドライン（CPSF等）と整合性を取るようにすべき**ではないか
- 例えば、国交省ガイドラインは任務保証の考えのもとで必要な事項についてまとめられている。異なる考えに基づいて対策が記されている既存ガイドラインが本制度のどのレベル(★3～5)に該当するのか、**整合性を確保すべき**ではないか
- 自工会で既に自己評価を行っている中で本制度に対応する場合、本評価制度の認証と他の認証との関係性が理解できなければ、サプライヤーにとって二重の対応が必要となる**既存のガイドラインと本制度との関係性を、事業者に対し明確に提示すべき**ではないか。**中長期的には統合するのがよい**のではないか
- **業界によってはグローバルにビジネス**をしていることから、一歩踏み込んで**相互認証まで検討すべき**ではないか

3. 制度整備に向けた道筋

◆ **制度が効果的と想定される業界等について**

- 業界毎の導入とあるが、サプライヤが業界横断である。**業界内での制度適用をすすめるだけでなく、業界横断で進めていく必要**がある
- 製品の製造は国内で完結せず、資本の入っていない国外（台湾、アジア等）メーカーと工程が跨る。本制度は、国外メーカーに対して、どう対応すれば良いのか明確化されたい

◆ **具体的な制度運営体制等について**

- **制度の運営機関はどこになるのか**。制度オーナーの具体的なイメージをお伝えすると、ユーザー企業の苦情対応等を持ち込むところである
- 評価者のスキルを高めていくため、**お助け隊の活用**も含め、**様々な教育施策を並行して行うことが重要**

これまでいただいた主なご意見

3. 制度整備に向けた道筋 (前頁の続き)

◆ **制度の導入促進**

＜専門家の活用促進、中小企業セキュリティ普及促進策との連動＞

- ★4企業は価格面でお助け隊サービス1類の対象外、2類の利用には1類の利用経験が必要。この点は**お助け隊サービスとの連携を考えるうえで課題**ではないか
- セキュリティ人材は不足している。大学、高専とタイアップしながら取組みを進めているが、**人材育成施策を明確化**されたい
- 運用をうまく回すためには、**取引関係における手順をドキュメントに示すことが有益**なのではないか

＜下請法や価格転嫁への対応＞

- **取引先にセキュリティ対策を要求する際に、下請けいじめと取られない様に、企業にとって必要な対策であることを、国から強いメッセージを出してほしい。**

＜本制度の継続的な広報、周知＞

- **取得企業の目標（★３を１万社など）を決めた上で、省庁が一体となり普及啓発をすすめてほしい**
- 中小企業中心の施策が多いが、**大企業、中堅企業も対象**なので、**そこに向けたメッセージも必要**
- 取引先から、セキュリティ対策をどうして良いか判らないといわれ困っている。**具体的なやり方と、その支援策がセットになった情報を提供して欲しい**
- セキュリティ対策やり方のノウハウを必要としてる企業は多い。業界も努力するが、**丁寧な説明、ドキュメント提供を、国、IPAで考えてほしい**
- **本制度の目標(取得企業数)**をどこかで示すべきではないか
- サプライチェーンには大企業、中小企業等が含まれるところ、**経済団体とタッグを組んで課題等を一緒に解決するようなスキーム等を作るべき**

＜中小企業等に対する対策資金等の支援＞

- サイバー保険は、有事対応や復旧支援に利用されることが多く、事業継続対策としての「適切な資金の確保」にもなる
- サプライチェーン上流になるほど特定の企業に集中し、そこには対策余力のない中小企業もいる。**コスト等の支援を検討すべき**ではないか
- 制度疲労を起こさないよう、実態は民間主導で推進するという方針のもと、補助金支給よりも、**税制優遇やルールメイキングの施策が重要**ではないか
- 来年度は制度単体ではなく、例えば税制などをパッケージとして考えるなど、**コストを払えるための総合的なパッケージとして検討を進めるべき**

[参考] 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の実施状況

- 本日を含め、これまで以下のような日程及び議題にて、5回に渡るSWGを実施。

SWG	日程	議題
第1回	2024年7月12日 10:00～12:00	• 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構築について • 今後の論点について • 自由討議
第2回	2024年9月9日 10:00～12:00	• サプライチェーン対策評価制度の基本構想（案）について • 委員からのプレゼンテーション • 自由討議
第3回	2024年12月24日 10:00～12:00	• 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これまでの議論の整理（案）について • 自由討議
第4回	2025年2月28日 9:00～11:00	• サプライチェーン対策評価制度の構築について - 要求事項案・評価基準案 - 制度普及に向けた考え方・取組 - 今後の進め方 • 自由討議
第5回	2025年4月7日 13:00～15:00	• 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中間とりまとめ（案）について • 自由討議

[参考] SC３成熟度モデル検討SWGの実施状況

- SC3においても、本SWGと並行する形で、これまで以下のような日程及び議題にて、6回に渡るSWGを実施。

SWG	日程	議題
第1回	2024年4月24日 10:00～12:00	• 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構築について • 自由討議
第2回	2024年8月19日 13:00～15:00	• 制度全体について（制度の目的、想定する対象事業者、想定するサプライチェーンリスクの範囲） • 各段階（★３～★５）について（各段階の定義、対策の対象範囲（事業者、システム）、対策の基本的な考え方） • 自由討議
第3回	2024年10月18日 13:00～15:00	• サイバーインフラ事業者に求められる役割等の検討の方向性について • サプライチェーン対策評価制度の基本構想(案) について • 自由討議
第4回	2024年12月11日 15:00～17:00	• 海外制度調査報告について • SC 対策評価制度の構想について • 普及策について • 自由討議
第5回	2025年1月27日 13:00～15:00	• 海外制度調査（英国現地調査）の報告について • SC対策評価制度の普及策について • 自由討議
第6回	2025年3月3日 13:00～15:00	• 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―中間整理（案）―について • 中小企業実態調査報告について • 自由討議

1. 制度の目的と位置づけ

1.1 制度の目的

【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。**

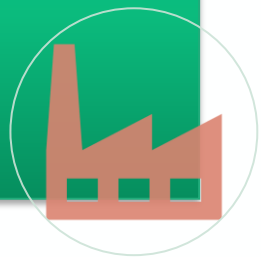
（※）**本来は各企業が自社のリスクを特定して必要なセキュリティ対策を個別に検討・実施することが望ましい**が、リソースに限りのある**中小企業を中心にただちにこれを実現できていない企業が一定数存在**する。本制度は、**包括的なリスク分析に基づき共通して求められる対策を示す**もの。将来的には、こうした企業も**より自社のリスク分析に基づいたさらなる対策の強化をしていくことが望ましい**。

1.1 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、また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

1.2 制度の位置づけ　— 対象とするリスクの範囲

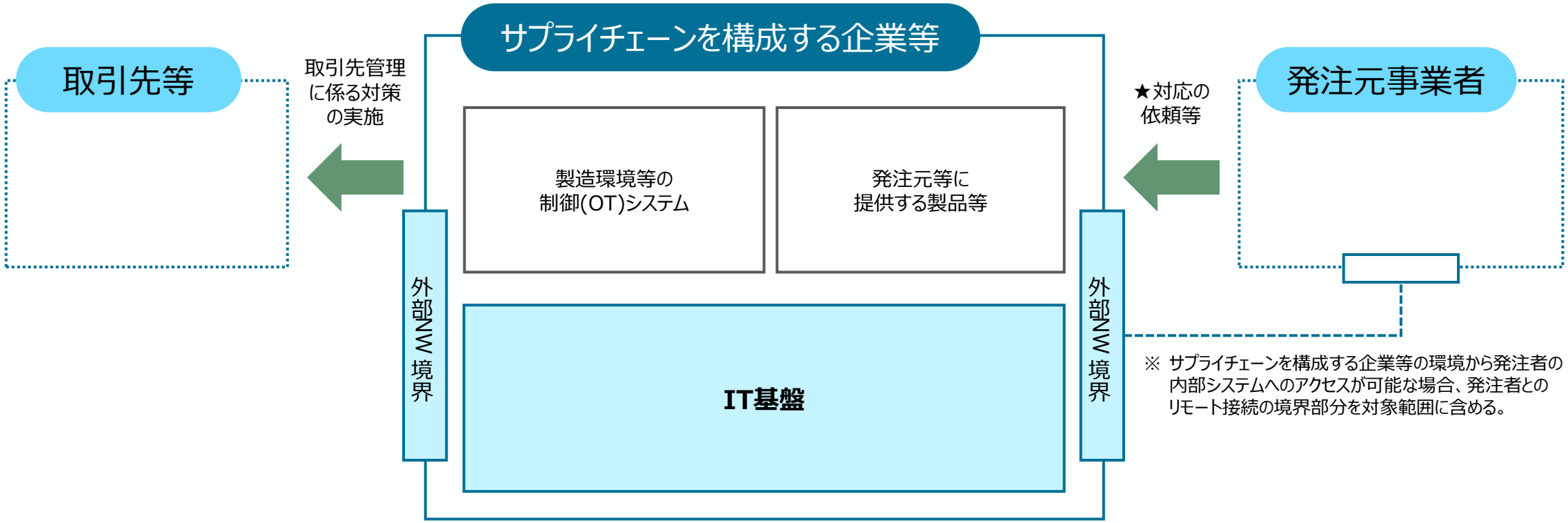
- 本制度では、取引先へのサイバー攻撃等を起因とした情報セキュリティリスク（機密性・可用性・完全性への影響）に加えて、製品・サービスの提供途絶リスク（事業継続性への影響）、及び取引ネットワークを通じた不正侵入等リスクを、対象とするサプライチェーンリスクとして想定。

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・役務の調達、業務提携、API連携など（他の類型に含まれるものを除く））
	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（MSP*、クラウドサービス等を含む）　* Managed Service Provider
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。

1.2 制度の位置づけ　― 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（オンプレミス環境で運用されるものに加え、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。



[凡例] 本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

1.3 「サイバーインフラ事業者に求められる役割等の検討会」との役割分担

- 本検討は、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靱性（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。

	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（本検討）	サイバーインフラ事業者に求められる役割等の検討会	両者の関係性（右図参照）
対象範囲・事業者	• ビジネスサプライチェーン(物資・役務の調達等) • ITサービスサプライチェーン(MSP*、クラウドサービス等を含む)に係る事業者	• ソフトウェア（クラウド上のもの含む）のサプライチェーン(開発・供給・運用)に係る事業者（＝サイバーインフラ事業者）	• ITサービスサプライチェーンに係る事業者は、双方の対象範囲に含まれる
検討目的・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	• ソフトウェアを利用する顧客等の保護を目的に、 • ソフトウェアの提供（開発・運用・供給）において、**事業者が果たすべき具体的な役割**(セキュア・バイ・デザイン／デフォルト等)の整理	• 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
アウトプット	• 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等の段階的評価制度を整備	• 「サイバーインフラ事業者に求められる役割等に関するガイドライン」に基づき、サイバーインフラ事業者による自己適合宣言を促進	-

＊ Managed Service Provider

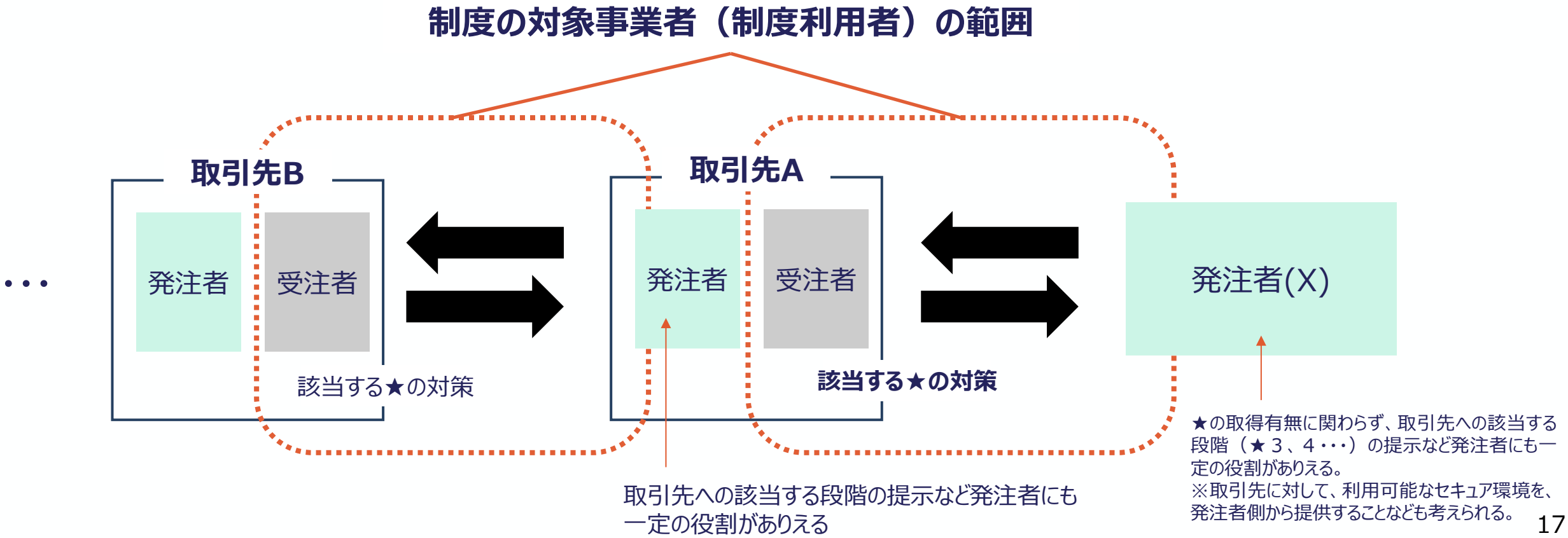
例えば、以下の業務を行うITサービスサプライチェーン構成企業は、顧客からの要請に応じて、双方の対応が必要となる場合がある

- 情報システムの開発及び構築業務・運用業務を受託する場合（自社IT基盤等のセキュリティ対策についてSC対策評価 / 開発・運用するシステムについてガイドラインに基づく対応）
- クラウドサービス事業者(IaaS/PaaS/SaaS)によるサービス提供（自社IT基盤等のセキュリティ対策についてSC対策評価制度/ 提供するクラウドサービスについてガイドラインに基づく対応）

2. 構築する評価制度

2.1 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又は企業グループ単位）を想定しているが、今後具体化を進めていく。



2.2 制度において設ける段階

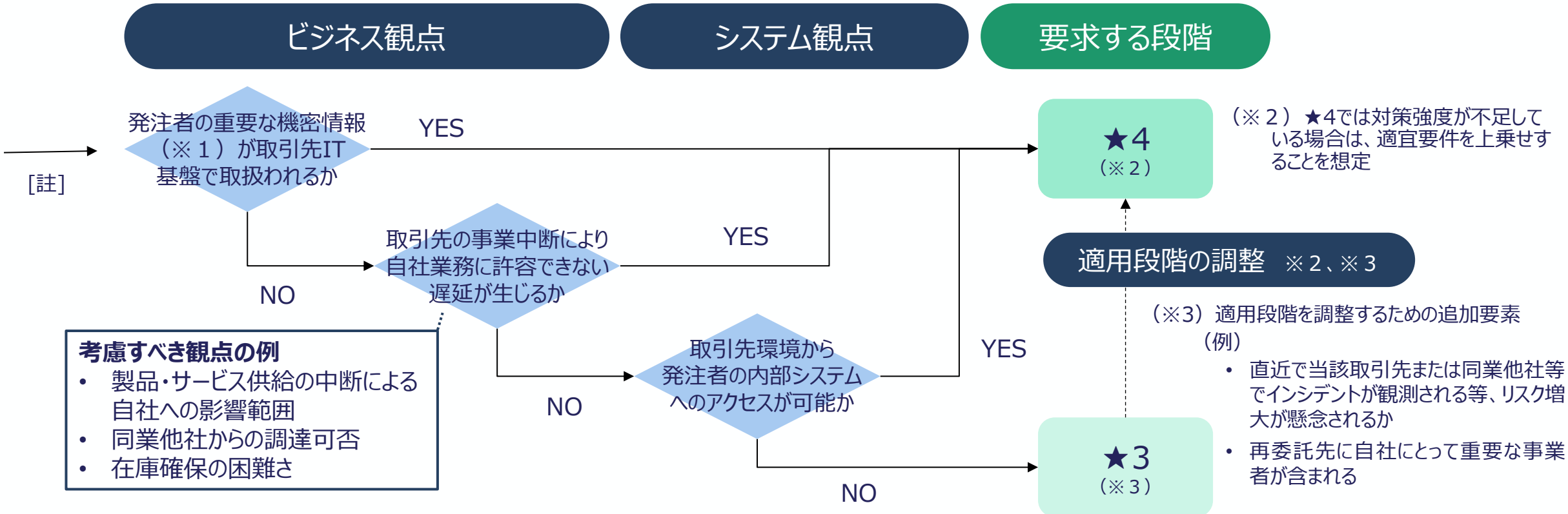
- 先行する海外制度等の分析を通じて、★３については、一般的なサイバー脅威に対処しうる水準を目指すものとして規定。
  ★４は、初期侵入の防御に留まらず、内外への被害拡大防止・目的遂行のリスク低減によって取引先のデータやシステム保護に寄与する点や、サプライチェーンにおける自社の役割に適合した事業継続を推進している点を改めて明確化。
- ★５については、より高度なサイバー攻撃への対応として、自組織のリスクを適切に把握・マネジメントした上で、システムに対する具体的な対策としては既存のガイドライン等も踏まえた上で現時点でのベストプラクティスに基づく対策を実行する形を想定（★3・4の精査も踏まえ、今後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

2.2 制度において設ける段階　― サプライヤー企業への適用の考え方

- サプライヤー企業への適用にあたっては、 ３つのサプライチェーン・リスクに照らして取引先を★4または★3の段階を割り当てる考え方を、制度の想定する使い方（モデル分岐図）として提示。
- 3つのリスクに照らして★３/４に振り分けたのち、直近のインシデント発生状況等に照らしての段階調整や、対策要件自体の上乗せなどは発注者の判断で実施されることを想定

（※）★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、2025年度以降に具体化を進める予定。

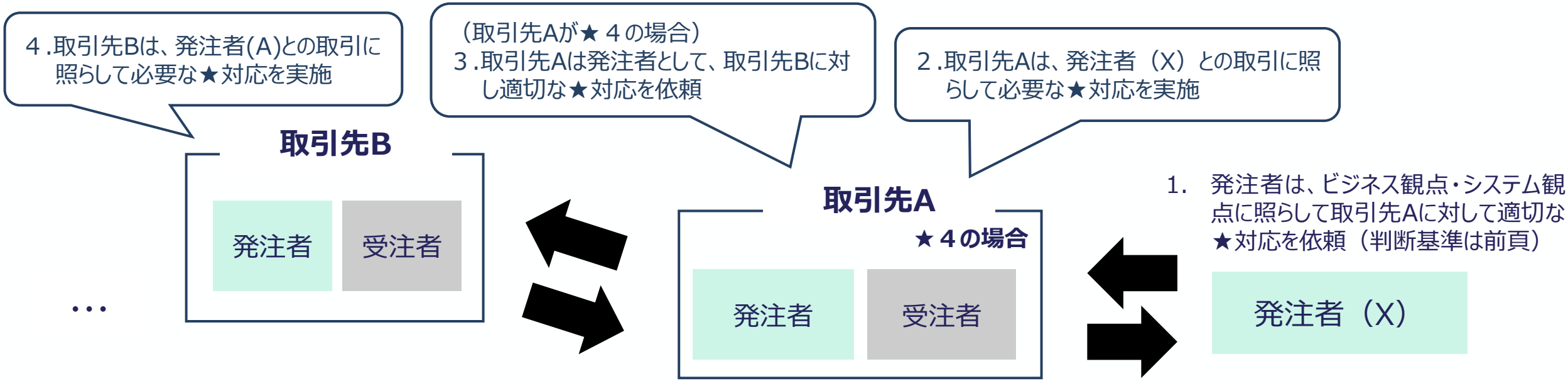


（※１）当該情報を漏洩した場合における、社会的信用低下や損害賠償等の訴訟リスクなどビジネスへの影響が大きいもの

（※４）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

2.2 制度において設ける段階　― 再委託先への適用の考え方

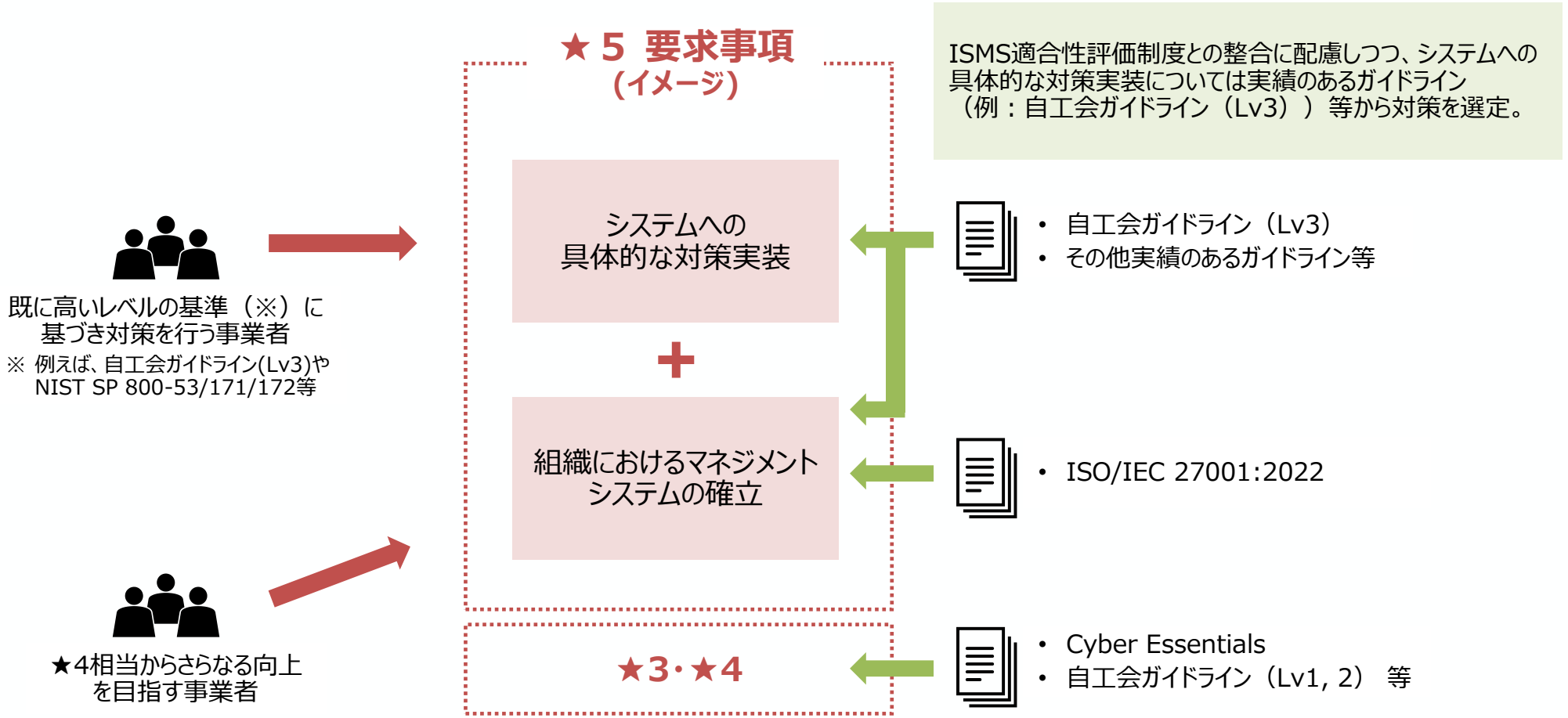
- 再委託先へのサプライチェーン対策評価制度の適用は、元の発注者ではなく直接の取引先（委託先）による判断で実施
- 直接の取引先（委託先）が★４対象の場合、★４要求事項に「重要な取引先におけるセキュリティ対策状況の把握」があるため、重要な機密情報が提供されている再委託先等にも一定の適用が期待される



★４要求事項（案）	★４評価基準（案）
10　重要な機密情報等を取扱うパートナー企業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又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

2.2 制度において設ける段階　― ★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。
- 2025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適合性評価制度とサプライチェーン対策評価制度の比較

- サプライチェーン対策評価（★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、2025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）	SC対策評価制度（★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）

2.3 制度で用いるセキュリティ要求事項・評価基準　― 各段階のベンチマーク

- 基本的な考え方に基づき、ベンチマークとする関連制度・ガイドラインを設定。★３/★４の対策事項案を具体化。

米　CMMC	英　Cyber Essentials	日本　自工会・部工会ガイドライン
Lv3 Expert 110項目＋24項目（SP800-172）	–	Lv3　：24類型153項目
Lv2 Advanced 110項目（SP800-171）	–	Lv2　：24類型124項目
Lv1 Foundational 15項目　（SP800-171より選ばれた対策）	防御、検知に特化した５つの分野の対策 ＋　前提としてIT資産管理	Lv1　：20類型50項目

★3のベンチマークを設定
- 米CMMC LV1
- 英Cyber Essentials
- 自工会・部工会ガイドライン Lv1

★4のベンチマークを設定
- 自工会・部工会ガイドライン LV1～3
- 重要インフラ分野別ガイドライン（金融、航空、電力、通信）
- ISO27001

★5のベンチマーク（候補）
- ISO/IEC 27001:2022
- 自工会・部工会ガイドライン LV3　等

- 対策を抽出、重複を整理
- ★３で対処する脅威等に照らして精査
- ★３対策事項（案）25項目を抽出

- 対策を抽出、重複を整理
- ★４で対処する脅威等に照らして精査
- ★３ベンチマーク中★３で除外した事項を考慮
- ★４対策事項（案）44項目を抽出

うち11項目は★３と同一内容

2.3 制度で用いるセキュリティ要求事項・評価基準

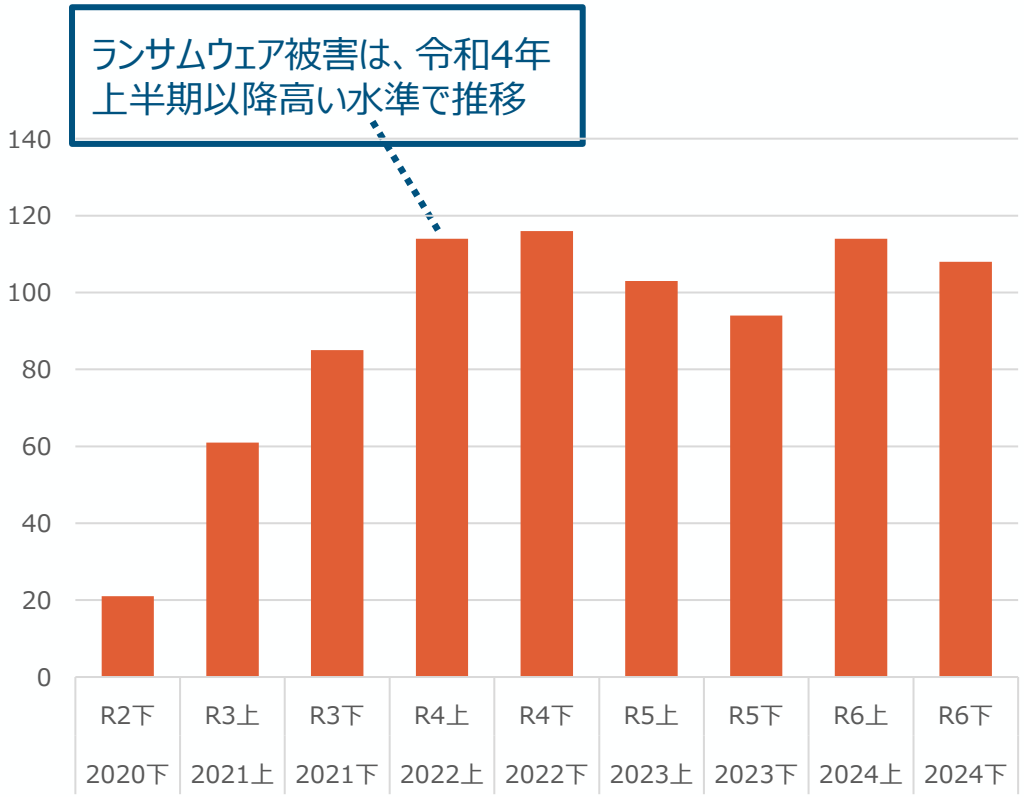
- レベルごと達成すべき「経営の責任」、「サプライチェーンの防御」、「IT基盤の防御」に資する対策を以下にて提示（詳細は参考資料１を参照）。

※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 参考資料１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

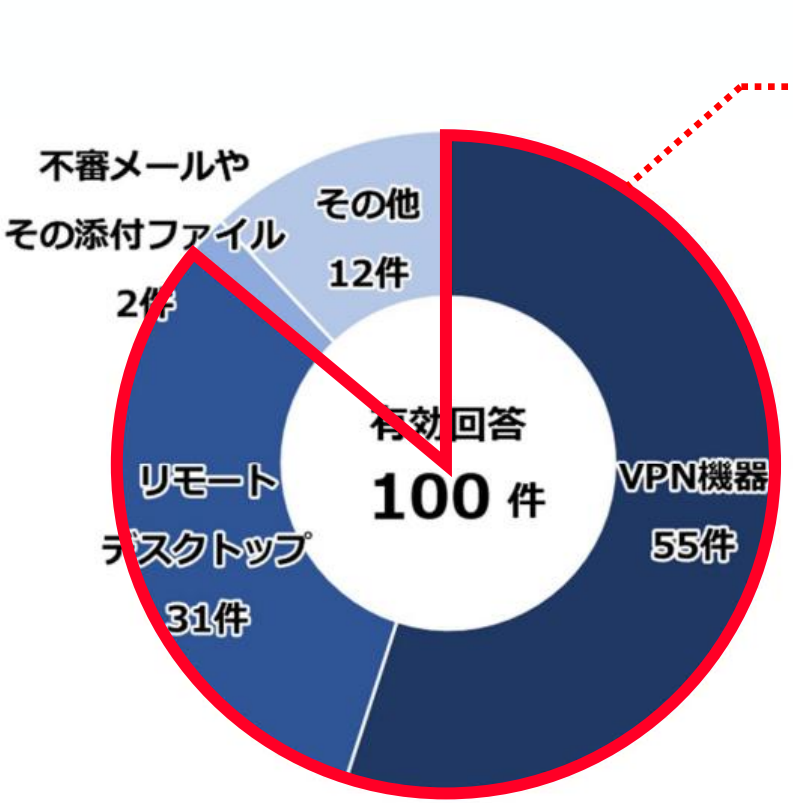
	★3（Basic）	★4（Standard）
経営の責任	**企業として最低限のリスク管理体制構築** • 自社のセキュリティ担当の明確化 [No.1] • セキュリティ対応方針の策定 [No.3] **インシデント発生に備えた対応手順の整備** • インシデント対応手順の作成 [No.25] **自社IT基盤や資産の現状把握** • 情報資産やネットワークの一覧化 [No.7,8] • 取引先等とのネットワーク接続の管理 [No.9]	**継続的改善に資するリスク管理体制の構築** • 定期的な見直しの実施 [No.6] • 定期的な経営層への報告、不備の是正等 [No.7] **インシデン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]

2.3 制度で用いるセキュリティ要求事項・評価基準　― ★3 対策による効果

- 業種・企業規模を問わず、昨今多くの被害が出ているランサムウェア感染は、ネットワーク経由が大半を占めている（86%）　。
- ★３要求事項の「ネットワークの把握と境界の防護（No.5,23）」、「アイデンティティ・アクセス管理（No.11～17）」、「ソフトウェア脆弱性へのパッチ適用（No.21,22）」を適切に実装することで、ネットワーク経由での代表的なランサムウェア攻撃を緩和できる。



ランサムウェア被害の報告件数（推移）



ランサムウェア感染の経路（令和6年）

代表的な手口である

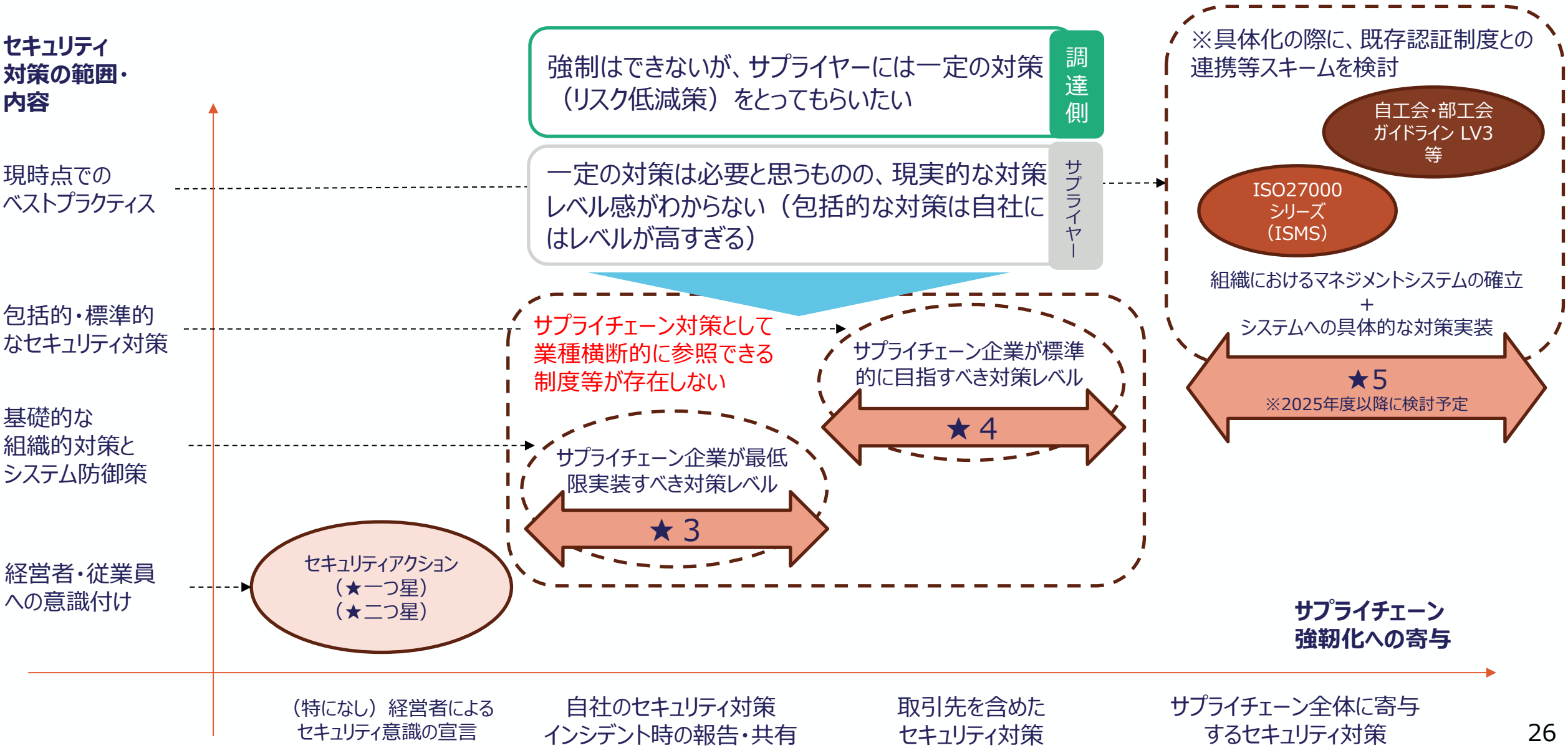
- **既知のソフトウェア脆弱性を悪用した侵入**
- **脆弱な認証(例：容易に推測可能なIDパスワード）を突破する侵入**

への防御策として★３は有効

※ゼロデイまたは公開後間もない脆弱性を悪用した攻撃に対しては★３対策レベルでは不十分

[参考] 警察庁「サイバー空間をめぐる脅威の情勢等」
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

2.3 制度で用いるセキュリティ要求事項・評価基準　― まとめ

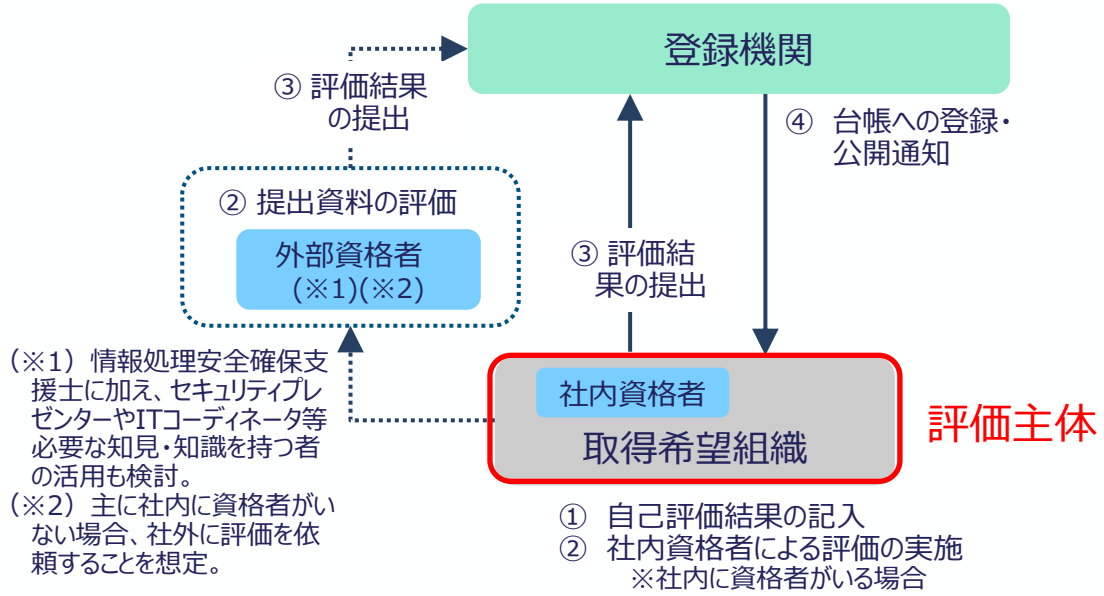


2.4 制度における評価スキーム

- 英国CEや米国CMMCを参考に、★3は自己評価（ただし専門家の助言プロセスを要する）、★4は第三者評価（技術要件を中心に、一部要求事項について第三者評価を実施）スキームを想定。
- ★４を自己評価型と第三者評価型の双方とする案（★４,★4plus）や、審査品質の確保方策（評価者に求める要件、第三者評価時の対象項目・評価観点等）は、今後の実証事業、海外制度調査や想定される評価機関の状況等も踏まえつつ、引き続き精査。

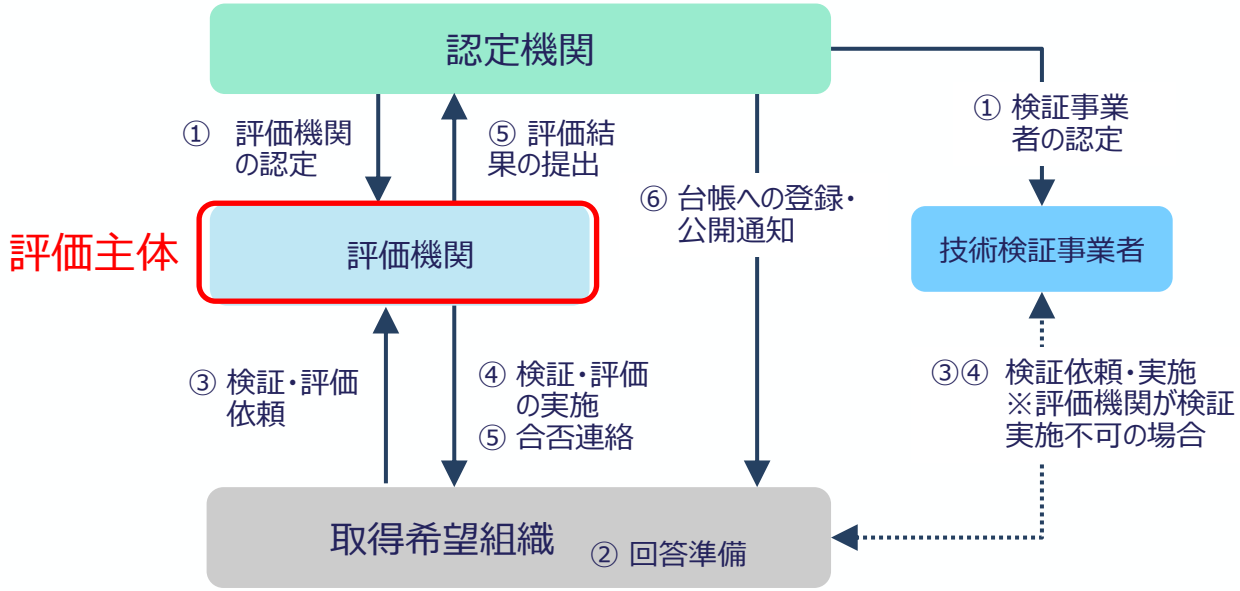
自己評価：★3

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、社内外の資格者の助言を得る）
② 社内外の資格者は、記入内容を評価、要求事項に対する合否を判断
③ 取得希望組織または社内外の資格者は、登録機関に評価結果を提出
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・公開



第三者評価：★4

① 認定機関は、評価機関・技術検証事業者を認定
② 取得希望組織は、★4要求事項に基づき回答を準備
③ 取得希望組織は、評価機関または技術検証事業者に、検証・評価を依頼
④ 評価機関または技術検証事業者は、検証・評価を実施
⑤ 評価結果を取得希望組織に通知し、認定機関に提出
⑥ 認定機関は、「合格」とされた組織を台帳に登録し、公開



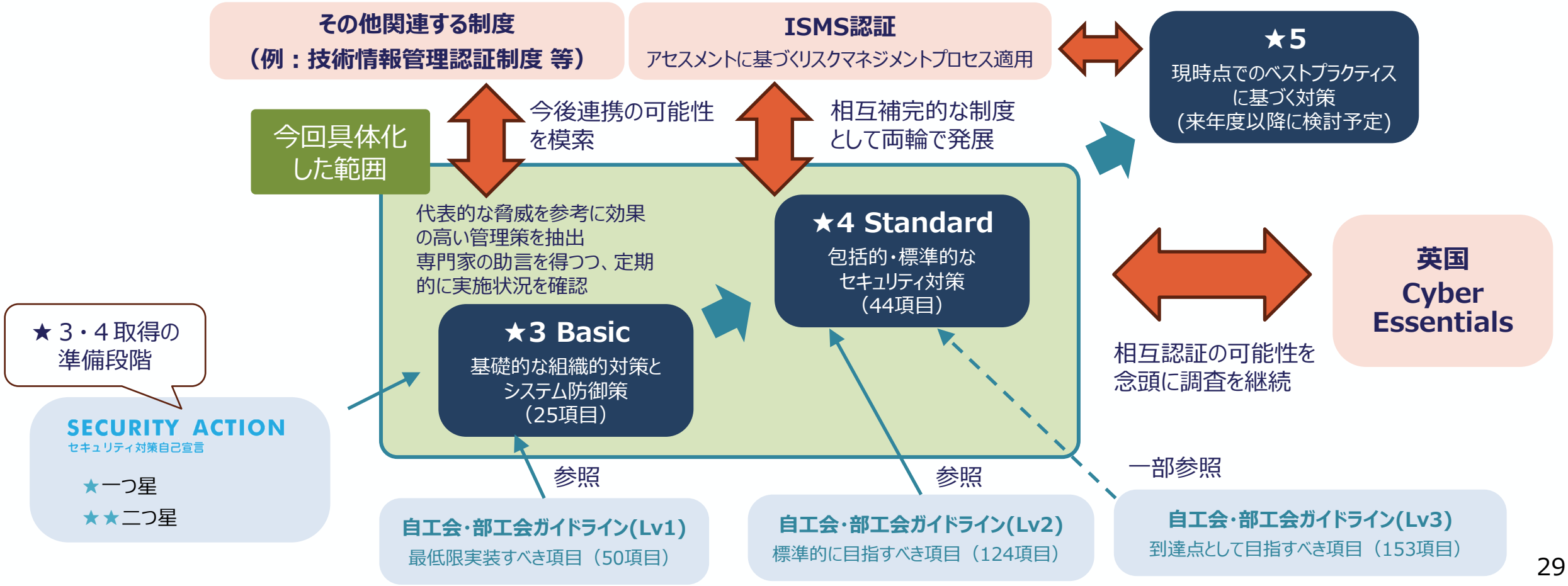
2.4 制度における評価スキーム

- ★３については有効期間を１年とし、対策状況について年次で点検することをもって更新可能とする。★４については複数年の有効期間とし、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案として想定。
- これらについては、今後の実証事業や想定される評価機関の状況等も踏まえつつ、引き続き精査。

	★３（自己評価）	★４（第三者評価）	★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）	認定機関から認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自己評価（専門家の助言プロセス有り）	・有効期間内は、1年ごとに自己評価を実施（評価機関に提出） ・有効期限を更新する際（３年に1回）は第三者評価が必要	
資格の取消し等	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、評価機関または認定機関から資格の一時停止または取消しを行う場合がある		

2.5 国内外の関連制度等との連携・整合

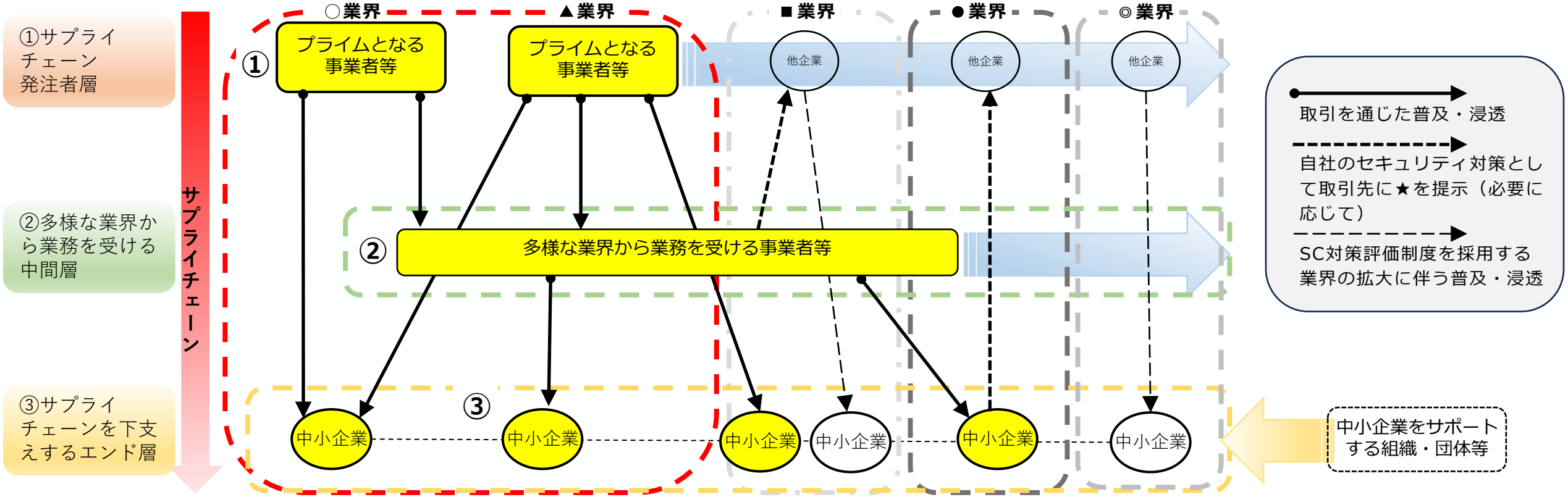
- サプライチェーン対策評価制度（★３/４）は、先行する自己評価の仕組みである「SECURITY ACTION」「自工会・部工会ガイドライン」や、国際標準であるISMS適合性評価制度等と相互補完的な制度として発展することを目指す。
- ★３/4は、自工会・部工会ガイドラインのLv1、Lv2に対応。自工会・部工会ガイドラインに基づく自己評価結果の本制度での活用などの連携方策を引き続き検討。また、英国CEとは、将来的な相互認証の可能性も念頭に、引き続き調査・意見交換を継続。



3. 制度整備に向けた道筋

3.1 制度が効果的と想定される業界等 - 複雑なサプライチェーンの構造

- サプライチェーンは多層構造、複雑性（N×N）を有するため、特定の企業や業界への普及策だけではサプライチェーン全体の強靭性に繋がらない可能性が存在する。
- こうした点を踏まえ、**①日本経済を牽引し市場への影響の大きいサプライチェーンの発注者側②多様な業界から業務を受ける中間層③中小企業を中心にサプライチェーンを下支えするエンド層**に分けた上で制度普及について検討していく。



3.1 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）各業界へのヒアリングから得られた意見

	業界	ヒアリング結果
①サプライチェーン 発注者層	金融、クレジット	● 金融業界やクレジット業界では、高いセキュリティが求められることから、取引先のセキュリティ対策確認の実効性を高めるために、評価制度の活用ニーズはあると考えられる。 ● 金融業界として、委託先へのセキュリティに関する確認事項を標準化予定であることから、本制度と連携して検討を進めていくことが望ましい。
	金融（保険）、建設	● 保険業界では、代理店におけるセキュリティ対策状況の底上げのために、★3制度に対する期待があると考えられる。 ● 建設業においては、協力会社を対象としたセキュリティガイドラインが既にあり、業界のピラミッド構造を踏まえた各層への要求レベルを明確化することで、制度の活用が期待できる。ただし、小規模な企業も含まれることから、費用面での支援や相談窓口の設置等、導入促進策とセットでの展開が求められる。
	自動車、半導体	● 自動車産業や半導体産業のような、サプライチェーンの事業上の連接が強い業界においては、取引先に対するセキュリティ対策のニーズがあると考えられる。 ● 特に、自動車産業においては、セキュリティガイドラインが存在し活用されていることから、本制度と連携していくことが望ましい。
	主要製造業	● 多数の製品・取引先を抱える製造業においては、取引先のセキュリティ対策状況をチェックリストで確認している場合も多いが、実効性には課題があり、また取引先数も多く全件の確認が困難であることから、本制度に対する期待がある。
②多様な業界から業務を受ける中間層	BPO事業者	● BPO業界においては、業界・業種問わず項目を統一することで対策要請への対応の効率化が図れることから、★取得希望がある。取引条件や調達における資格審査要件となれば、希望度合いは上がる。 ● 自身が取得するだけではなく、取引先にも本制度の取得を求めるニーズがあることから、取得事業者の広がりが期待できる。
	製品・部品製造業	● 一般製品等の製造業では、様々な取引先からセキュリティ対策要請を受けており、今後も増えていくことが想定される。評価基準が統一され、一つの基準を達成することで様々な業界・業種と取引が容易になることが期待されている。 ● ただし、制御系や工作機器等、グローバルでの取引が中心となる業界は、海外制度との整合性を図ることが必要である。
③サプライチェーンを 下支えするエンド層		● セキュリティ対策に対する必要性が高い中小企業はあるが、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。 ● 中小事業者の中でも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）であれば、本制度を円滑に活用できる可能性がある。

3.2 制度の導入促進

- 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。

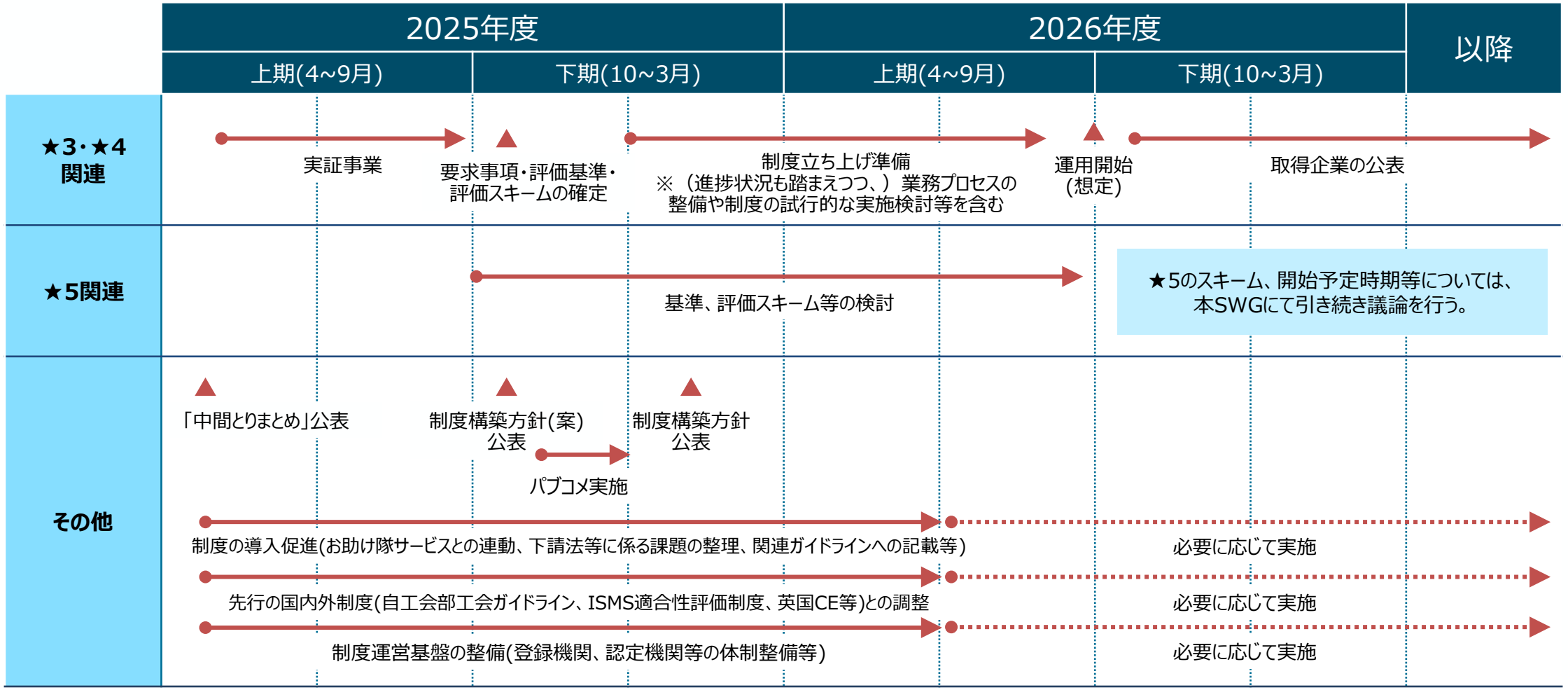
①発注者層、②中間者層、③エンド層、④評価機関・専門家

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）等必要な知見・知識を持つ者の活用も検討する。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。	○	○	○	○

4. 今後の検討の進め方及びスケジュール

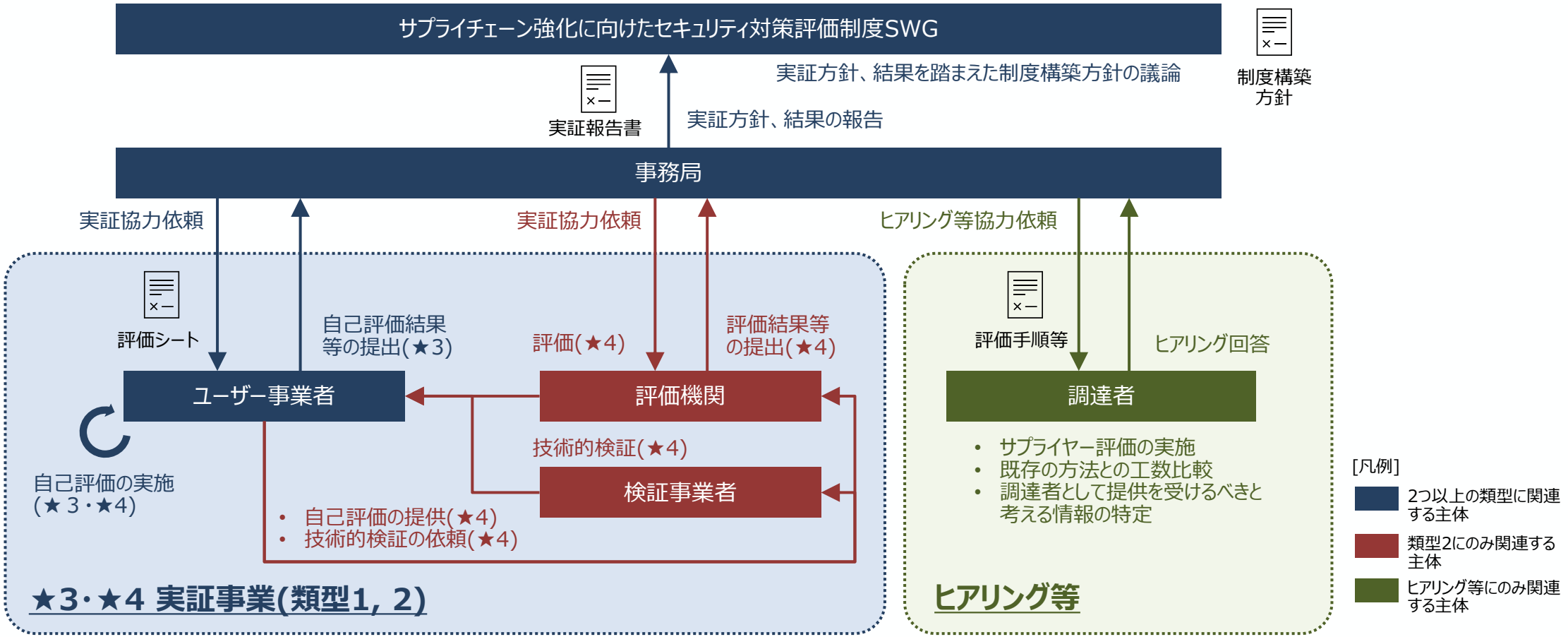
25年度以降のスケジュール

- 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。



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



付録：諸外国における関連する取組

1. 英国サイバー・エッセンシャルズ（Cyber Essentials）

- 英国サイバー・エッセンシャルズは、代表的なサイバー攻撃への普遍的な防御策として、英国セキュリティ機関NCSCが提供するフレームワーク。企業の規模によらず、一般的なサイバー攻撃全般から組織を保護するのに役立つとされている。
- 自己診断で取得可能な「Cyber Essentials」と、第三者による技術検証が必要な「Cyber Essentials Plus」の二段階が存在。
- 英国の公的機関の調達において必須要件として課される場合が多い。また、鉄道など一部民間分野でも取引要件として一般的に活用されつつある。（2023年3月段階で、12万以上の者がCEを取得）

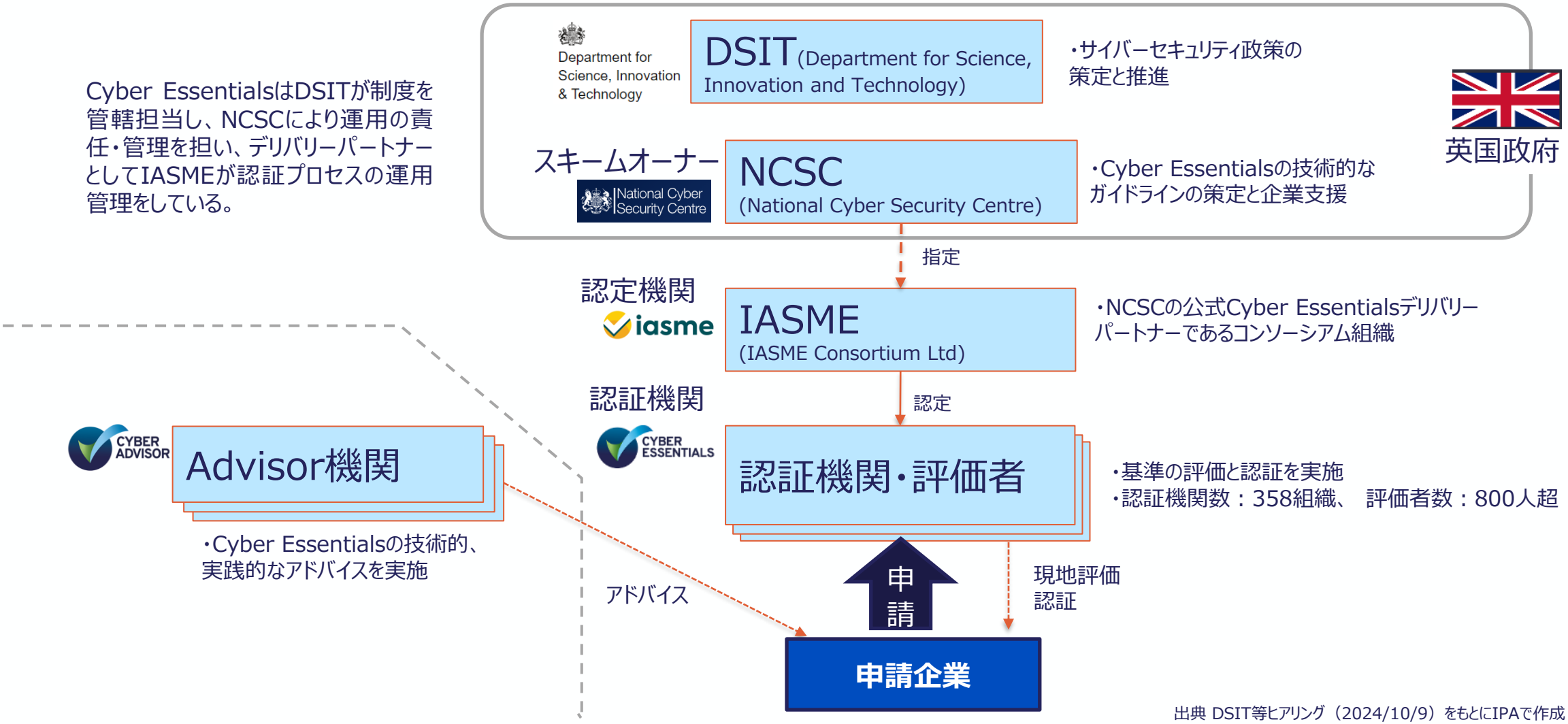
	セキュリティ要件（共通）	アセスメント要件
CYBER ESSENTIALS PLUS	• ファイアーウォール • セキュアな構成 • セキュリティアップデート管理 • ユーザアクセス制御 • マルウェア対策 の５つのカテゴリで要求事項を提示 ※認証の適用範囲の評価を行う際に、対象資産に関する設問があり、資産管理についても間接的に要求していると解釈できる	• Cyber Essentialsの取得を前提として、実地検査として認定機関による技術検証を受けることが必要（脆弱性診断、権限管理など具体的なテスト項目と仕様を提示）
CYBER ESSENTIALS		• インターネット上でのオンライン審査にて自己診断を行い、認定機関に所属する有資格の審査員が回答内容を評価。 • 合格した場合は認定証が授与され、不合格の場合は今後の助言等が示される。

参考 https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf
https://assets.publishing.service.gov.uk/media/652d2b6ad86b1b000d3a4fbe/2023-10-11_Updated_PPN_09_23_Cyber_Essentials_eg.pdf

1. 英国サイバー・エッセンシャルズ　― 認証スキーム

- Cyber EssentialsはDSITが制度を管轄担当し、NCSCにより運用の責任・管理を担い、デリバリーパートナーとしてIASMEが認証プロセスの運用管理をしている。

Cyber EssentialsはDSITが制度を管轄担当し、NCSCにより運用の責任・管理を担い、デリバリーパートナーとしてIASMEが認証プロセスの運用管理をしている。



出典 DSIT等ヒアリング（2024/10/9）をもとにIPAで作成

1. 英国サイバー・エッセンシャルズ　― 制度の効果検証

- 英国政府は2013年にサイバー攻撃事例を分析、組織がシステムを適切に保護するために「最低限必要な5つのコントロール」を抽出しCEの要件とした。最新の攻撃動向に照らしても、5つのコントロールは有効との見解。

サイバーエッセンシャルズ効果検証※（2024年10月）のポイント

- **CE利用者の80%**が、CEのセキュリティ要件は**一般的なサイバー脅威に対して有効でありリスク低減につながっている**と回答
- **CEの利用者は、サイバー攻撃の被害に遭う可能性を5.8点/10点と評価**（未取得組織は3.7点）。**CE利用者のサイバー脅威に対するリスク意識の高まり**が見られた
- **CE利用者の76%**が、CE要件以外の**追加的な予防措置を講じた**と報告
- **CE利用者の約半数（48%）**が、**サプライヤーへのCE取得義務**あるいは将来的な義務化を検討。
- NCSCの年次レビューによると、**CE取得組織は、同じ保険契約を結んでいるCE未取得の組織と比べてサイバー保険の請求が80%減少**（2022年請求データ）

※CE取得組織(606)と未取得組織(516)をサンプルとして比較、取得効果を検証

NCSC公式サイト（サイバーエッセンシャルズ解説ページ）

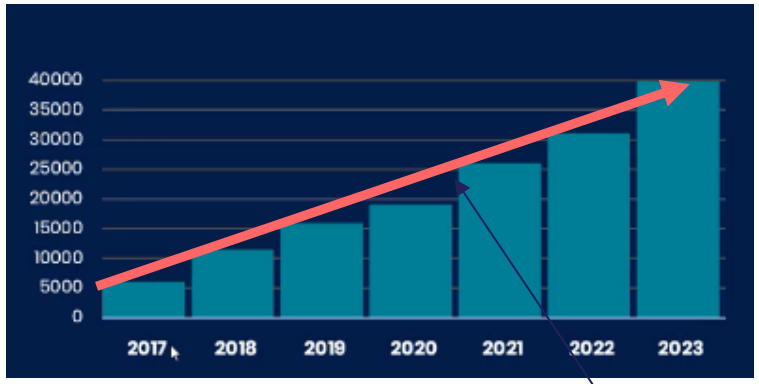
参考　https://www.gov.uk/government/publications/cyber-essentials-scheme-impact-evaluation
https://www.ncsc.gov.uk/cyberessentials/overview

1. 英国サイバー・エッセンシャルズ　― 申請費用と実績数

- Cyber Essentialsの申請費用は、企業規模に応じたものとしてIASMEで定めている（下表）。なお、コンサル経由で申請する場合などにおいては、市場原理に応じた柔軟な価格設定される場合もある。
- Cyber Essentials Plusは申請企業の規模と複雑さにより差異が大きいため、標準価格は定めず認証機関の見積による。
- Cyber Essentialsの審査の実績情報は、経年とともに増加している。
- 直近の年間認証数は約47,500件。うちCyber Essentials がその75%を占める。認証取得組織の規模は、小規模以下の組織が68%（小規模、零細ともに34%）を占める。

表．Cyber Essentialsの申請費用

企業規模	費用
零細（0-9名）	$420（約60千円）
小規模（10-49名）	$570（約81千円）
中規模（50-249名）	$650（約93千円）
大規模（250名以上）	$780（約112千円）



図．Cyber Essentials 認証件数の経年変化

出典　DSITヒアリング2024/10/9より

表．企業規模ごとのCE認証件数

制度の種類	大規模（250以上）	中規模（50-249）	小規模（10-49）	零細（0-9）	合計	割合
Cyber Essentials	3,595	7,254	12,544	12,420	35,813	75%
Cyber Essentials Plus	1,715	2,735	3,479	3,741	11,670	25%
合計	5,310	9,989	16,023	16,161	47,483	100%
割合	11%	21%	34%	34%	100%	

小規模以下の組織で68%

Cyber Essentialsが75%

出典　英国政府サイト（2024年1月～2024年12月の集計結果）をもとにIPAにて加工
https://www.gov.uk/government/statistical-data-sets/cyber-essentials-management-information

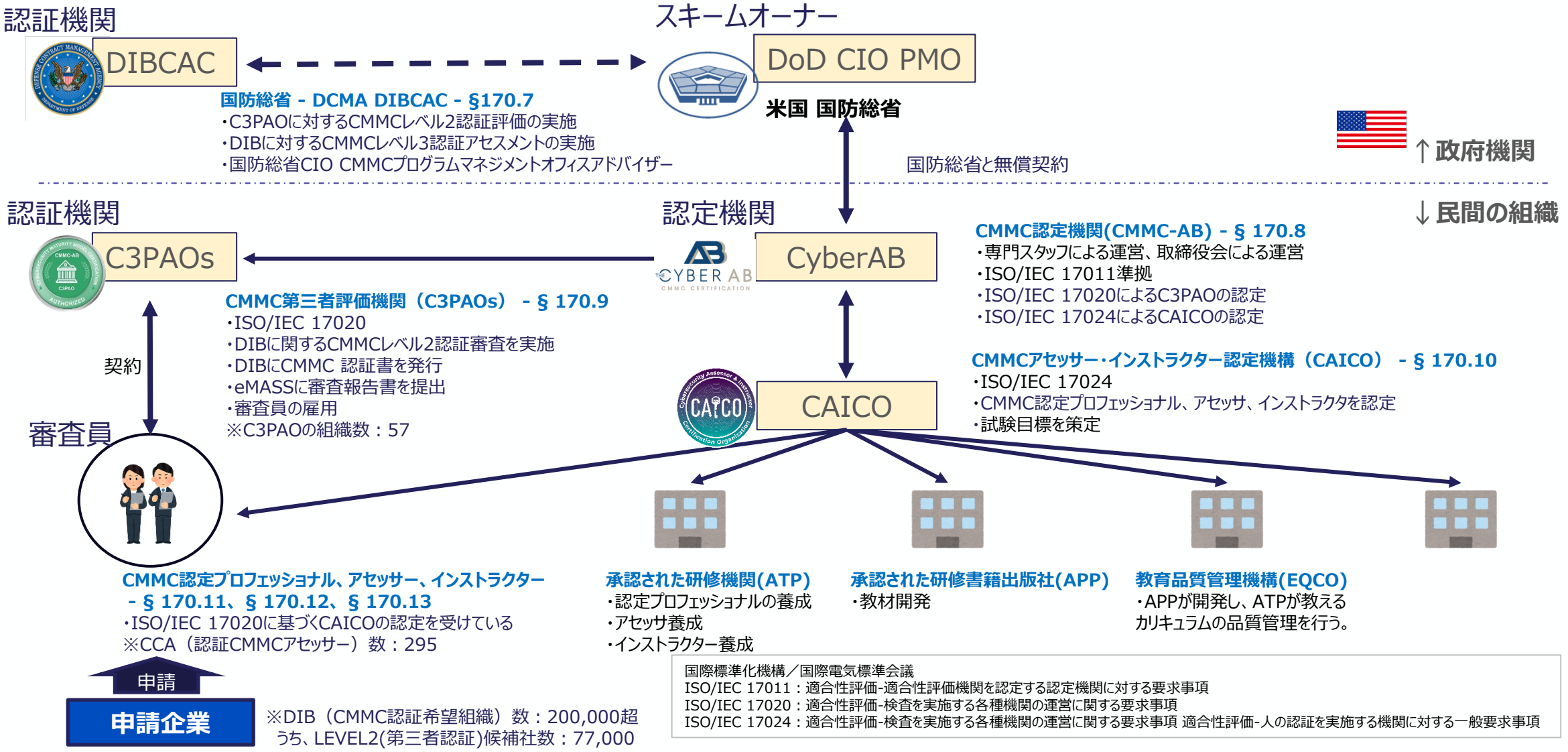
2. 米国 CMMC 2.0　― 概要

- 米国CMMC 2.0は、国防総省から発注を受ける防衛産業基盤（DIB：Defense Industrial Base）企業が「連邦契約情報(FCI)」及び「管理された非格付け情報(CUI)」を適切に保護させるための米国防総省(DoD)のプログラム。
- 2021年12月CMMC2.0を発表（CMMC 1.0と比較して基準を簡素化、レベル区分も3段階に見直し）。2024年12月にCMMC 2.0が発効。下位レベルから順次段階的に採用して数年を掛けて完全実施を予定。
- CUIの取扱い要件は、国防総省の調達ルール(DFARS)でのみ規定されたものであるが、全ての米国政府機関の調達契約に適用すべく、連邦政府の管理ルール(FAR)での規定案が2025年1月に公開され、2025年3月までパブコメを実施。*1

	セキュリティ要件 (Security Requirements)	アセスメント要件 (Assessment Requirements)	確認要件 (Affirmation Requirements)
LEVEL 3	• DFARS 252.204-7012の要求 • NIST SP800-171 R2の110項目 • NIST SP800-172 Feb2021から選択された24項目	• **DoD評価**（DIBCAC）により、要件すべての実装を検証 • 未達の要件は、評価後180日以内に終了しなければならない行動計画(POA&M)を設定することが認められる	• 請負業者の幹部職員は、POA&Mへの対応を含む毎回の審査後及びその後毎年、セキュリティ要件の継続的な遵守を確認 • 確約は SPRS に入力
LEVEL 2	• DFARS 252.204-7012の要求 • NIST SP800-171 R2*1の110項目	• **自己評価または第三者評価**により、要件すべて実施されていることを検証 • 未達の要件は、評価後180日以内に終了しなければならない行動計画(POA&M)を設定することが認められる	• 請負業者の幹部職員は、POA&Mへの対応を含む毎回の審査後及びその後毎年、セキュリティ要件の継続的な遵守を確認 • 確約は SPRS に入力
LEVEL 1	• FAR Clause 52.204-21で既に要求 • 15項目	• **自己評価**により確認 • 評価結果をサプライヤー・パフォーマンス・リスク・システム(SPRS)に入力	• 請負業者は、毎年、セキュリティ要件の継続的な遵守を確認 • 確約は SPRS に入力

参考　https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program
*1　https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information

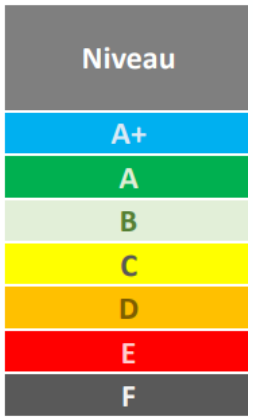
2. 米国 CMMC 2.0　— 認証スキーム



出典 米国のサプライチェーン企業におけるサイバーセキュリティ制度の調査報告書（2024年 エヴァアビエーション）をもとにIPAで加工

3. フランス　サイバースコア法（CYBERSCORE）　― 概要

- フランスでは、Webサイトを対象に、サイバーセキュリティに係るスコアリングの実施を法律により義務付け。
- 消費者の個人情報保護の観点から、Webサイトにおけるセキュリティ確保とデータ保護に係る信頼性を消費者に通知することを目的とするもの。
- 対象は、2024年時点でフランス領土からの月間ユニークビジター数が2,500万人以上（2025年以降は月間1,500万人以上へと基準の引下げ予定）のサイト。対象サイトの運営者等に対して、サイバーセキュリティ監査の実施及び監査結果から算出されたスコアの提示を義務化。
- スコアの算出は、ANSSIによって指定されたプロバイダーによる監査を通じて行われる。

	スコア算出上考慮される主な基準	段階分け
Cyber Score	「組織とガバナンス」 「データ保護」 「デジタルサービスに対する知識と習熟」 「アウトソーシングのレベル」 「インターネット上での露出度」 「セキュリティインシデント対処体制」 「セキュリティ監査の実施」 等の９つのカテゴリで監査基準を提示	 スコアはFからA+の7段階で定義される （現状、それぞれの段階の定義は公表されていない）

参考URL https://www.vie-publique.fr/loi/282626-loi-3-mars-2022-cyberscore-securite-des-plateformes-numeriques
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045294275

4. オーストラリア　エッセンシャル・エイト（Essential Eight）　― 概要

- エッセンシャル・エイトは、豪州のセキュリティ機関ACSC(Australian Cyber Security Center）が策定した基準。
- 4段階の成熟度を定義し、攻撃者の手口や脅威のレベルに応じて、組織が段階的に実施できるよう設計。
- 豪州内のすべての組織を対象として想定。なお成熟度２は、パブリックガバナンス・パフォーマンス・アクト（PGPA Act）の対象となる豪州の中央政府及びその他の公的団体等では必須要件とされている。
- 組織がサイバーセキュリティインシデントを軽減するため８分類の重要な対策を提示。
  （パッチ適用、パッチ運用システム、多要素認証、特権の制限、アプリケーション管理、Microsoft Officeマクロの制限、ユーザーアプリケーションの堅牢化、定期的なバックアップ）

Essential Eight

組織の成熟度	定義	セキュリティ要件 （レベル毎に詳細な対策を提示）
レベル３	より適応力が高く、公開ツールやテクニックへの依存度がはるかに低い攻撃者への対応を念頭に置く	8分類 149項目（＝全項目）
レベル２	レベル1より高度な攻撃者で、ツールの有効性に対してより多くの時間の投下を厭わない者への対応を念頭に置く	8分類 107項目
レベル１	広く入手可能で汎用的な技術の活用で満足する攻撃者への対応を念頭に置く	8分類　48項目
レベル０	組織の全体的なサイバーセキュリティ態勢に弱点がある	ー　（求められるセキュリティ要件無し）

参考URL　https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model

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