セキュリティマネジメント指導（テーマ別）実施要領

テーマ⑥｜セキュリティアセスメント

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

IPA Better Life with IT

本資料の位置づけ（指導の全体像）

本資料は、セキュリティ専門家が中小企業に対して行う個別訪問指導「**セキュリティマネジメント指導（セキュリティアセスメント）**」の説明資料です。

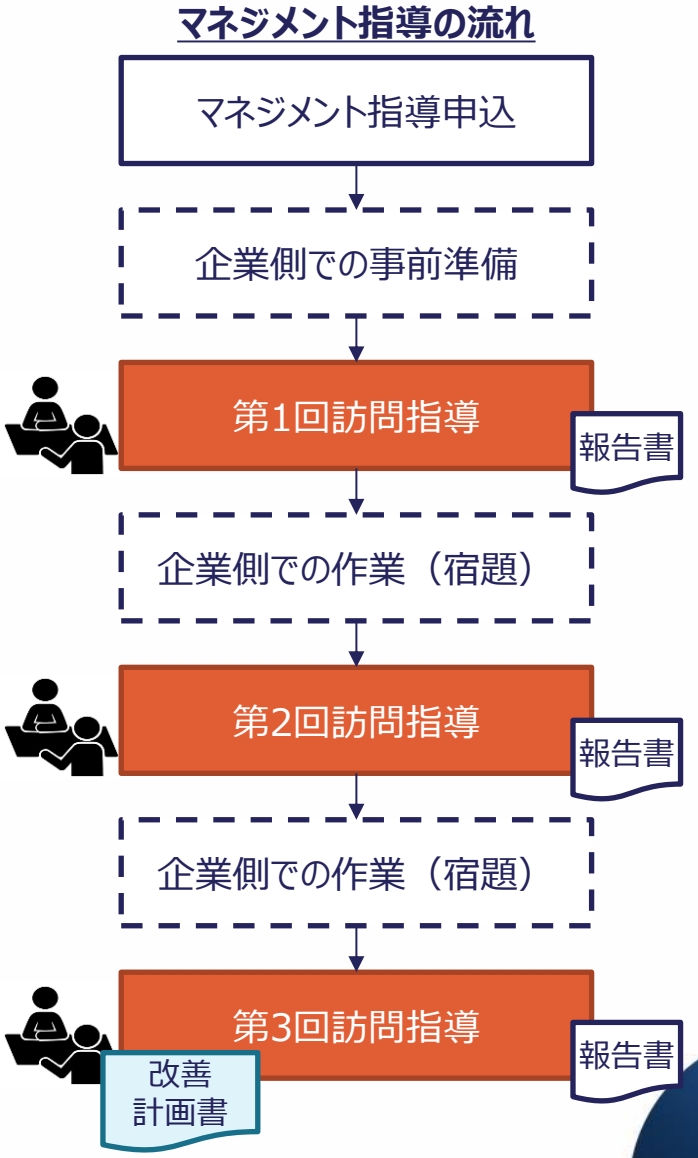
中小企業は経営資源の制約から、限られたリソースの中で情報セキュリティ対策を行う必要がありますが、どの部分に対策の重点を置くべきかの判断が、必ずしも明確でないケースが多くあります。また、中小企業が自社の取組の妥当性を専門家の第三者的な視点から確認したいというニーズもあります。

この点、セキュリティマネジメント指導（テーマ別）では、そのような中小企業に対してセキュリティ専門家が訪問指導する際の基本的なフレームワークとして、①情報セキュリティ規程の整備、②情報資産の洗い出しとリスク分析、③クラウドサービスの安全利用、④セキュリティインシデント対応、⑤従業員向けのセキュリティ教育の5つの主要なテーマを設定しています。本資料は、これらの対策を行った中小企業、またはそのレベルに達した中小企業が、**自社のセキュリティ対応状況評価（セキュリティアセスメント）**を行うことを想定し、これをセキュリティ専門家が客観的な評価を行い、改善点を助言するための具体的な方法と手順をセキュリティマネジメント指導ツールとして提供しています。

セキュリティアセスメントの実施に際しては、「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[注]」（以下「SCS評価制度」という）の中で、全ての企業が最低限実装すべきセキュリティ対策とされる、★３の要求事項・評価基準に基づくフレームワークで構成した、セキュリティアセスメントシートを用いて行います。これにより、本セキュリティマネジメント指導（セキュリティアセスメント）を実施した企業は、SCS評価制度の★３申請を行うために実施すべき対策（改善事項）が明らかになり、自律的なセキュリティ対策の強化が期待できます。

セキュリティ専門家の皆さまにおかれましては、本資料の趣旨をご理解の上、中小企業へのセキュリティマネジメント指導にご活用ください。

注：「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）」公表
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html



マネジメント指導のテーマと狙い

- 本資料は、企業の情報セキュリティ対策全体の現状評価（セキュリティアセスメント）をテーマとします。
- セキュリティアセスメントシートを用いた評価と助言においては、セキュリティマネジメント指導（５テーマ）も、個別の対策に活用することができます。

指導テーマ	1 情報セキュリティ規程の整備	2 情報資産の洗い出しとリスク分析	3 クラウドサービスの安全利用	4 セキュリティインシデント対応	5 従業員向け情報セキュリティ教育	6 セキュリティアセスメント
どういった企業に受けてもらいたいか	**サイバー攻撃の増加や法令遵守の必要性に直面しつつも、情報セキュリティ規程が未整備な中小企業**。特に、従業員が多様なITツールを使って業務を行っているが、具体的な指針がなく、責任範囲が曖昧な企業に必要である。	**デジタル化が進み、膨大な情報を管理しているが、どの情報が重要か、リスクがどこにあるかが把握できていない企業**。特に、製造業やサービス業など、顧客情報や技術情報を大量に扱う企業に必要である。	**業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な企業**。特に、情報管理の外部委託が進んでいるが、適切な安全対策ができていない中小企業に必要である。	**セキュリティインシデントが発生した際の対応が曖昧で、事後対応に時間がかかり、被害が拡大するリスクがある企業**。特に、**サプライチェーンの一部として他社との連携が多い企業**に必要である。	**従業員のセキュリティ意識が低く、パスワード管理やフィッシング攻撃に対する対応が不十分な企業**。特に、ITリテラシーの差が大きい企業や、非専門職の従業員が多く、日常的なセキュリティ対策が徹底できていない企業に必要である。	**自社の情報セキュリティ対策への取組みの妥当性を、専門家の第三者的な視点から確認したい企業**。特に、サプライチェーンに絡んだ取引先が多く、顧客からもセキュリティ対策の評価や強化を要望されている企業に必要である。
マネジメント指導を受けたことによる効果	不足していた情報セキュリティ規程が整備され、社内での運用・周知方法まで確立されることで、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。	企業が保有する情報資産が洗い出され、リスク分析シートとして整備することで、自律的な運用が図れるとともに、リスク低減策等の検討の題材にもなる。	当該支援先企業における「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用に伴うリスクを理解できるようになる。	インシデント対応プロセスを整備し、必要に応じ、従業員の演習を実施することで、セキュリティインシデント発生時に迅速かつ効果的に対応できる体制が構築できる。	セキュリティ教育プログラムを策定するとともに、定期的に見直しと更新を行う体制を構築。実際に従業員に対するセキュリティ教育を実施することで、社内の意識向上にもつなげられる。	アセスメントの基準に対して適合の評価を得ることにより、顧客や取引先の信頼を高めることができる。また更なるレベルアップが望まれる対策分野についても、具体的な検討を推進できる。

本書の構成

- 指導テーマであるセキュリティアセスメントを行うに当たって、「**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）」を念頭に、3回の標準的な訪問指導内容（**標準シラバス**）と、指導に用いる各種ツール類や留意点を説明する「**実施要領**」を作成しました。
- 「実施要領」には、各回ごとの指導の内容（標準的な進め方）に加えて、指導に当たっての留意点を記載し、使用するツール/資料の活用方法を記載した、実践的なノウハウを提供する内容としています。
- セキュリティアセスメントで使用する「**セキュリティアセスメントシート**」は、SCS評価制度の要求事項・評価基準に基づくフレームワークで構成し、その記入例や留意事項を記載しています。

具体的支援の進め方	**標準シラバス**	**指導全体の構成と留意事項** ・専門家指導の全体構成 ・各回ごとの指導の内容（標準的な進め方） ・指導に当たっての留意点
	ツール解説編	**各種ツールの活用方法** ・使用するツール/資料 ・参考資料

テーマ⑥｜セキュリティアセスメント

【標準シラバス】
専門家指導全体の構成と留意事項

指導業務の達成目標と成果物

➢「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）」★３の要求事項・評価基準を基に作成したセキュリティアセスメントシートを用いて、指導先企業のセキュリティ対策状況を評価し、★３申請を行うために実施すべき対策（改善事項）について、必要な助言を行います。

マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

【達成目標１】現状における自社のセキュリティ対策状況の洗い出し
【達成目標２】セキュリティアセスメントシートによるセキュリティ対策状況の評価
【達成目標３】実施すべきセキュリティ対策の改善計画書策定

注：成果物

取組みスタート

達成目標1

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状の対策状況の洗い出し結果

達成目標2

セキュリティアセスメントシート
SCS評価制度
★３認証ベース

セキュリティアセスメントシートによる自社のセキュリティ対策状況の評価

達成目標3

改善計画書

★３申請を行うために実施すべき対策を改善計画書として取りまとめ

専門家：評価と助言

改善活動

SC評価制度
★３ 申請
（自己評価）

★３申請シート

専門家：確認と助言

【参考】アセスメントと監査との違い

- セキュリティアセスメントの実施に当たっては、監査に関する知識やスキルを活用することが有効です。
  ※監査の基礎知識については、後述の「ツール解説編｜2．参考資料」を参照
- セキュリティアセスメントとセキュリティ監査では、実施者や用いる基準に違いがあるものの、「一定の基準に基づいて、客観かつ公正な視点で妥当性を評価する」という点は同じであり、監査実施の手続き（方法）や進め方がアセスメントにも参考になります。

項目	セキュリティマネジメント指導におけるアセスメント	セキュリティ監査
目的	自社の取組の妥当性を専門家の視点から確認	定められた認証・認可・法的要求への対応
実施内容	制度の基準への適合可否を評価する	求められる基準への適合可否判定を行う
実施者	セキュリティ関連の資格や経験を有する専門家 （★３では第三者性は必須ではない）	独立した監査人 （第三者性が重視される）
用いる基準	SCS評価制度 ★３の要求事項・評価基準	明確に定められた基準に基づく （法令、規格、社内規程など）
報告書	改善計画書 （適合可否、助言、改善計画案）	監査報告書 （適合可否、指摘事項、改善提案）

専門家指導の全体構成

1～2週間

事前準備#1

*「5分でできる自社診断」(Excel版)の実施依頼
*「セキュリティアセスメントシート」の確認依頼

第１回

規程類の整備状況の確認とセキュリティアセスメントシート要求事項の解説

指導先企業のビジネス内容や組織概要等を聞き取った上で、情報セキュリティ関連規程類の整備状況を確認します。また、セキュリティアセスメントシートにおける要求事項・評価基準について説明するとともに、回答記入のポイントを説明し、指導先企業に記入を依頼します。

2～3週間

事前準備#２

*前回の指導を通じて得た情報をもとにした改善領域の見極め
*事前に受領したセキュリティアセスメントシートについて、確認・ヒアリングポイントの整理

第２回

セキュリティアセスメントシートの記入内容の評価と改善点についての指南

指導先企業が記入したセキュリティアセスメントシートについて評価を行います。企業側が策定時に苦労した点や、疑問に思った点等について質問を受け付け、アドバイスします。また、不十分な点があれば指摘し、改善計画書に反映するように指導します。

2～3週間

事前準備#３

*前回結果に加え、経営施策に対する情報セキュリティリスクの検討
*事前に受領した改善計画書について、内容確認、追加対策の検討

第3回

改善計画書の作成

指導先企業が作成した改善計画書について、優先度・実効性の観点を踏まえて検討を行い、適切なアドバイスを行います。作成に際し企業側で生じた疑問や質問等に回答・アドバイスします。また、継続的なレベルアップの観点から今後の取り組みのついての検討を行います。

計2.0ヶ月程度

「標準的な進め方」の詳細（１）

第1回　規程類の整備状況の確認とセキュリティアセスメントシート要求事項の解説

		企業	専門家	成果物/提供ツールなど
事前準備	1	提供可能な社内資料の準備 (企業紹介のパンフレット等)	ホームページなどによる企業の情報収集　(企業・事業の理解)	–
	2	「5分でできる！自社診断（Excel版）」による自己診断の実施	（事前配布）	【提供】5分でできる！自社診断チェックシート（Excel版）
	3	「セキュリティアセスメントシート」内容確認	（事前配布）	【提供】セキュリティアセスメントシート
	4	出席メンバー選定 (経営者/従業員等、半日x3回)	専門家指導の作業内容、全体スケジュール案の作成、初回訪問日程の事前確認	初回のスケジュール調整
当日	1	説明事項に対するディスカッション(確認・了解)	今回の訪問指導の目標、作業内容、全体スケジュール、成果物等の説明と合意	–
	2	ビジネス内容、組織概要、規程類の整備状況についての説明	情報資産に関する確認および情報セキュリティ関連規程類の整備状況（ドキュメント一覧）の確認	–
	3	セキュリティアセスメントシートの要求事項についての理解	セキュリティアセスメントシートにおける要求事項、記入のポイントについて説明	【参考】★３評価 要求事項と評価基準
	4	依頼事項についての確認と了解	アセスメントに必要な関係書類の準備依頼 ・規程類、実施記録など 次回のスケジュール調整、依頼事項の確認	（終了後） 実施報告書の作成

実施のポイント

- 第1回の指導では、ヒアリングによって、企業側での情報セキュリティ関連規程の現時点での整備状況（ドキュメント体系レベル）について把握します。
- 「5分でできる！情報セキュリティ自社診断」は参考資料として扱い、深堀は行いません。
- 企業側で記入したセキュリティアセスメントシートは、第2回実施の前に送付いただくよう依頼します。

「標準的な進め方」の詳細（２）

第2回　セキュリティアセスメントシートの記入内容の評価と改善点についての指南

		企業	専門家	成果物/提供ツールなど
事前準備	1	依頼された必要情報の準備	前回訪問で得た情報の整理・分析 (理解に齟齬が無いか訪問時に確認する)	－
	2	セキュリティアセスメントシートへの記入および事前送付	セキュリティアセスメントシートの事前受領と内容確認 ・確認、ヒアリングポイントの整理 ・重点改善領域の見極め	－
当日	1	依頼された必要情報の提供・説明	提供された情報の確認・質疑応答	－
	2	セキュリティアセスメントシート記入内容の説明と関係書類の提示	セキュリティアセスメントシート記入内容の評価、関係書類確認	【成果物】 ・セキュリティアセスメントシート
	3	改善要項目に対する改善計画に関するディスカッション	重点改善領域を踏まえた改善計画に関するディスカッション ・緊急度、重要度、難易度による絞り込み	【提供】改善計画書（ひな形）
	4	改善計画書の作成了解	改善計画書の作成依頼	（終了後） 改善計画書の「2.評価結果（専門家記入）」欄の記入と送付 実施報告書の作成

実施のポイント

- 事前に受領したセキュリティアセスメントシートを基に、規程類のドキュメント体系を踏まえて評価方法を整理しておきます。
- 評価基準に沿って、企業側の記入内容を確認して評価します（「適合」の評価は、全評価項目への適合が必要となります。）。
- 企業側が作成した改善計画書は、第3回実施の前に送付いただくよう依頼します。

「標準的な進め方」の詳細（３）

第3回　改善計画書の作成

		企業	専門家	成果物/提供ツールなど
事前準備	1	改善計画書の策定	前回訪問結果の整理と、改善計画の検討結果の整理	–
	2	改善計画書の事前送付	改善計画書の内容確認、追加対策の要否検討	–
当日	1	作成した改善計画案の説明と実現性検討 ・必要とされるリソース：人・物・金	改善計画案のレビューと、これまでの指導を踏まえた具体的改善計画の検討	–
	2	改善計画書の合意	改善計画書の合意	【成果物】改善計画書
	3	継続的レベルアップのための今後の取り組みについてのディスカッション	継続的レベルアップのための今後の取り組みについてのディスカッション	–
		専門家指導についての評価	指導結果のまとめと評価	（終了後）指導結果のまとめと評価を行う実施報告書の作成

実施のポイント

- 今後の取り組みを改善計画書としてまとめ、企業側と合意します。改善計画は実現可能なレベルでまとめ、結果が計測できる内容とします。
- 要求事項に適合している項目についても、今後の継続的レベルアップの観点から改善ポイントについてディスカッションを行います。
- 計画される情報セキュリティ対策は、経営者が自分事として取り組める実効性と納得感のあるものとします。

当日タイムスケジュールの提示

- 訪問指導当日の具体的な進行は、指導先企業の状況を踏まえて進めます。
  ⇒ 対面でのQ&A方式、ワークショップ方式、グループ討議方式等、状況に即した方式を設定します。
  ⇒ 状況によっては、訪問をせずにWeb会議で指導を行うこともあり得ます。
- 各回とも半日（２～３時間程度）の限られた時間ですので、効率的に進行します。
  ⇒ 可能な限り事前に、当日のタイムスケジュールをセキュリティ専門家から提示します。

＜当日タイムスケジュール（例）＞

初回の例	時間	項目	考慮点
13:30-13:40	10分	*自己紹介と当事業内容全体の説明/確認 *当日の進め方と準備資料についての説明と合意 *情報の取り扱い	セキュリティマネジメント指導の目的と、目標とする成果物を明確に伝える
13:40-14:40	60分	*企業の事業（業務）内容と情報システム環境の理解	企業ホームページ等での事前確認を踏まえて、効率的にヒアリングを進める
14:40-14:50	10分	休憩	
14:50-15:30	20分	*情報セキュリティ規定類の整備状況の確認	セキュリティアセスメントシートの評価の際に関係書類として利用できるドキュメントの一覧を確認する
15:30-16:10	60分	*セキュリティアセスメントシートの要求事項についての説明	企業側がセキュリティアセスメントシート記入に際して留意するポイントについて説明する
16:10-16:20	10分	*追加で必要となる情報の提供依頼	第2回の準備作業に間に合うように、できる限り早めの対応を依頼する
16:20-16:30	10分	*全体を通してのQ&A *次回以降の日程と準備事項の確認	第2回目の冒頭で前回の振り返りを行う

指導先企業への依頼や調整事項

- 指導を円滑に進めるため、指導先企業へ依頼する事項を予め伝えておき、調整が必要な事項の有無を明らかにしておきます。

＜指導先企業への確認・調整依頼事項＞

	確認・調整事項	依頼のポイント
1	企業の検討体制(参加メンバー)等の調整	✓ 経営層に加え、以下の現場のリーダー層～課長クラスに参加いただくことを推奨します。 ・事業や業務のプロセスに詳しい方 ・ITシステムの運用管理を担っている方
2	打ち合わせ場所や環境の確認/準備	✓ 会議室/プロジェクター等の環境確認/準備をお願いします。 ・映像コンテンツの投影や、ディスカッションの効率に大きな影響があります。
3	指導環境の調整（コミュニケーション環境）	✓ 原則として訪問による現地指導を行いますが、初回を除く2回目以降で訪問と同等の指導がオンラインでも可能であることが見込まれ、かつ指導企業が合意した場合に、オンラインによる指導を行う場合もあります。
4	提供を受ける情報の取り扱い	✓ 指導企業にいただいた情報は、専門家において取り扱いに留意します。

【ツール解説編】
各種ツールの活用方法

5分でできる！情報セキュリティ自社診断

- IPAが提供する「**5分でできる！情報セキュリティ自社診断**」を使用します。
- 第１回目の事前準備として、指導先企業へ自社診断の実施を依頼の上、訪問前に返送してもらいます。
- 専門家は、第１回目の訪問前の事前情報として、企業の現状を把握し、アセスメントに役立てます。

  ※結果についての掘り下げは行いませんが、アセスメント結果と共に、重点改善領域と思われる項目についての助言に役立てます。

自社診断のための25項目

- **基本的対策（5項目）**
  脆弱性対策、ウイルス対策、
  パスワード強化など
- **従業員としての対策（13項目）**
  標的型攻撃メール、電子メール、ウェブ利用、
  持ち出し、廃棄など
- **組織としての対策（7項目）**
  守秘義務、教育、委託先管理、ルール化など

※　Excelファイルをそのまま、または印刷して実施してください。Excelファイルは、IPA Webサイトからダウンロードが可能です。
https://www.ipa.go.jp/security/guide/sme/5minutes.html

セキュリティアセスメントシート（記入例）

- セキュリティアセスメントシートは、「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」★３ の要求事項・評価基準をもとに作成したものであり、中分類の括りで企業のセキュリティ対策内容を評価します。

大分類	中分類	★3 要求事項 No.	要求事項	企業が記入する欄		評価手続き（実施したものに〇印）				評価結果（専門家が記入）	専門家コメント
				確認結果	結果に関するコメント	文書類	システム機能	現場視察	ヒアリング		
ガバナンスの整備	役割、責任、権限	1-2-1 1-2-3	・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。 ・守秘義務のルールを策定し、遵守させること。	対応	・IT担当責任者、担当者を明示し、従業員から誓約書提出済。	○			○		組織図、誓約書の内容等を確認に運用されていることを確
	ポリシー	1-3-1	・自社のセキュリティ対応方針(ポリシー)を策定し、周知すること。		と社内ポータルやWebにも盛り込んでいる。	○	○		○		での掲載状況や就業規されていることを確認し
取引先管理	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 2-1-2 2-1-4	・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。 ・他社との間で、機密情報の取扱い方法を明確にすること。 ・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。		先とは秘密保持契約取り扱いや、障害発生明確にしている。	○			○		の経緯や事情があるも取引先との秘密保持契約まれる。
リスクの特定	資産管理	3-1-1 3-1-2 3-1-3 3-1-4	・ハードウェア、OS及びソフトウェアの情報に関する一覧を作成すること。 ・ネットワークの情報に関する一覧を作成すること。 ・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。 ・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。		レの手順書をもとに、ステムの各種機能でいる。	○	○	○	○	適合	・手順書と運用管理システムの機能を確認し、適切に管理されている。
攻撃等の防御	アイデンティティ管理、認証、アクセス制御	4-1-1 4-1-2 4-1-3 4-1-4 4-1-5 4-1-6 4-1-7	・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。 ・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。 ・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。 ・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。 ・パスワード設定に関するルールを定め、周知すること。 ・パスワードの管理に関するルールを定め、周知すること。 ・アクセス権の管理ルールを定めて、運用すること。	対応済	・管理ルールの運用管理システム対応できている。						
	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対応に関する教育・訓練を行うこと。	未対応	・従業員へのセキュリティ教育は実施しているが、インシデント発生時の訓練は未実施。	○	○		○	改善要	・現在の社内ポータルでのセキュリティ教育に加え、インシデント発生時の訓練が必須と考える。
	データセキュリティ	4-3-4	・適切なバックアップを行うこと。	対応済	・重要データは、社内サーバ、クラウド共に、日次でバックアップしている。		○	○	○	改善要	・ネットワークから切り離したバックアップ保管ができていないことが判明し、早急に検討が必要。
	プラットフォームセキュリティ	4-4-1 4-4-4 4-4-5	・ハードウェア・ソフトウェアの安全な構成を確立し、維持すること。 ・ハードウェア・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。 ・システムをマルウェア感染から保護すること。	対応済	・管理ルールの手順書をもとに、運用管理システムの各種機能で対応できている。	○	○	○	○	適合	・手順書と運用管理システムの機能を確認し、適切に管理されている。
	技術インフラのレジリエンス	4-5-1	・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。	対応済	・UTMを導入し、境界防御を行っている。		○	○	○	適合	・UTMの設定も、購入業者のSEと定期的に確認するなど、適切に運用されている。
攻撃等の検知	継続的監視	5-1-1	・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。	一部対応済	・UTMでの監視に加え、リモートワーク用PCについて、来期以降にEDRの導入を検討する予定。		○	○	○	改善要	・当企業のシステム環境において、EDRの導入は有効な対策であり、ぜひ実施いただきたい。
インシデントへの対応	インシデント管理	6-1-1	・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。	対応準備中	・連絡先一覧表は作成済。 ・手順書は来月完成予定。	○			○	改善要	・手順書の作成が準備中であるが、従業員への周知に十分留意して実装することが望まれる。
インシデントからの復旧	インシデント復旧計画の実行	7-1-1	・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。	未対応	・現在ある地震対応のBCPを、セキュリティインシデント対応の観点から見直す。				○	改善要	・セキュリティインシデントへの対応手順書をもとに、BCPへの対策整備を進めていただきたい。

【選択肢】
対応済
一部対応済
対応準備中
未対応
対象外

【選択肢】
適合
改善要
対象外

SCS評価制度は、現在立ち上げ検討中であり、「要求事項・評価基準」についても確定に向けて適宜修正されることに留意が必要です。

【参考】★３評価の要求事項と評価基準

- 「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）」★３は、中分類12項目、要求事項26項目、評価基準83項目から構成されます（一つの要求事項に対して複数の評価基準が設定されている項目もあり）。

＜ ★３ 要求事項と評価基準（抜粋）＞

大分類No.	大分類	中分類No.	中分類	要求事項No.	要求事項名	要求事項	評価基準No.	評価基準
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。	1-2-1-1	・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。
							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。
				1-2-3	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。	1-2-3-1	・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。
							1-2-3-2	・入社時又は社外要員の受入れ時に守秘義務を説明すること。
		1-3	ポリシー	1-3-1	セキュリティポリシーの策定	自社のセキュリティ対応方針(ポリシー)を策定し、周知すること。	1-3-1-1	・自社のセキュリティ対応方針(ポリシー)を定めること。
							1-3-1-2	・定常的に、かつ、セキュリティ対応方針の改正時に役員、従業員、派遣社員及び受入出向者へと周知すること。
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。	2-1-1-1	・自社以外の組織(顧客・子会社・関係会社・クラウドサービス提供者を含む取引先)が管理・提供し、自組織の資産が接続している情報システムを把握するための仕組みを整備すること。
							2-1-1-2	・年1回以上の頻度及び必要に応じて、上記において把握すべき情報の内容を点検をしていること。
				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。	2-1-2-1	・自社の機密情報を共有する取引先との間で、業務開始前に機密情報の取扱いについて、以下の事項の取り交わしを行うこと。 - 機密情報の定義 - 機密情報の取扱い (表示、保管方法、複製可否及び第三者への提供可否) - 機密情報の返還又は廃棄
				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。	2-1-4-1	・機密情報を共有する子会社又は取引先との間で、セキュリティインシデント発生時の自社及び子会社又は取引先の役割及び責任について、以下の事項を定めること。 - セキュリティインシデント発生時の相手方への通知義務 - セキュリティインシデント発生時の連絡先 - 再発防止策の協議方法

セキュリティアセスメントシート　（実施に当たっての留意点）

- 要求事項や評価基準に対する企業のセキュリティ対策には幅があり、どの程度の対策レベルであれば適合とするか、判断に迷うことが想定されます。
- SCS評価制度の具体的な運用ルールが未確定のため、現時点では確たるガイドが難しい状況ですが、専門家が適合可否の評価や助言を行うに当たっては、以下の視点に留意が必要です。
  - ① 企業の事業内容や特有の環境などを踏まえた、実効性のある対策か。
  - ② 対策は、漏れなく（例外なく、忖度なく）実施・運用されているか。
  - ③ 企業体力等から見て、継続的に実施可能なレベルか。
  - ④ 準備中の対策は、数ヶ月以内に実現できるか。
  - ⑤ 検討に挙がっている対策は、「緊急度、重要度、難易度」からみた優先度が明確か。
  - ⑥ 成熟度モデル（後述）の考え方から見て、対策の継続的なレベルアップが期待できるか。
  - ⑦上記の視点について、経営層の理解とリーダーシップが得られているか。

セキュリティアセスメントシート（ヒアリングの留意点）

- ヒアリングでは、初対面の相手先に対しても円滑なコミュニケーションが求められます。
- 効率的、且つ実効性の高いものにしていくために心掛けるポイントや留意点を、以下に整理しました。注

項目	心掛けるポイント・留意点
アセスメントに対する悪いイメージの払しょく	✓ 粗捜しではないことや、効率的に進めるために理解と協力が不可欠であることを十分に説明する ✓ ヒアリングを通じての改善目標の共有化や、事前の準備や情報提供を依頼する
周囲の観察	✓ サイバーセキュリティ以外の対策についても、訪問先の建物周辺、受付の対応、施設内の状況などを観察することで、ヒアリングの内容と事実認識とのズレを確認する
相手への問いかけ	✓ 相手を否定せず、日常の仕事やその手順など、身近なことに関係づけた質問で理解しやすくする ✓ 質問を繋げて聞いていきながら、内容を少しづつ深堀りし、相手に気付きを与える
質問・評価の流れ	✓ 「計画の有無は？⇒手順書等の文書化の有無は？⇒責任者は誰か、その役割は？⇒規程・ルールと実態とのギャップの有無は？」等の流れで、質問を掘り下げながら評価していく
相手の話を聞く	✓ 指示・命令ではなく、対等な関係で傾聴する
不具合の指摘	✓ 証拠を慎重に検証し、思い込みで判断しない ✓ 説明の矛盾点、手順書や用いる基準との差異について、直ぐに指摘するのではなく、不具合の背景（要因）を掘り下げた後に指摘事項として表明する

注：情報システム監査実践マニュアル 第３版（日本システム監査人協会編）を参考に作成

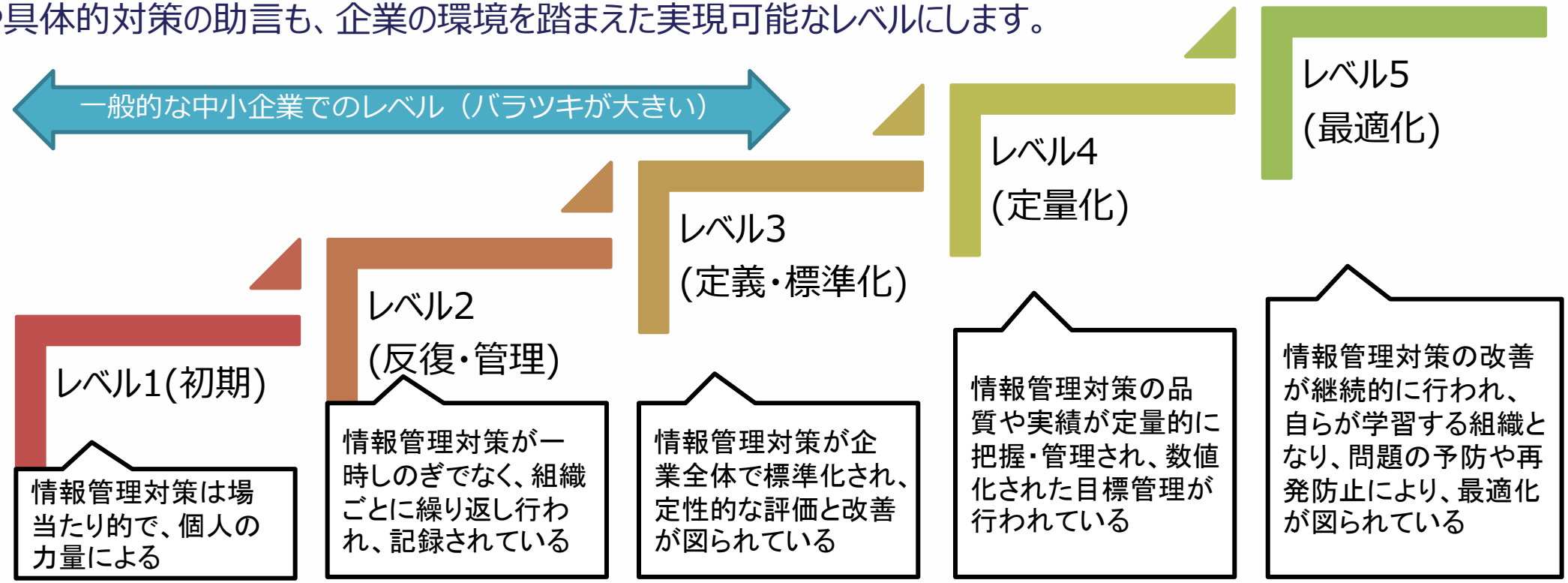
セキュリティアセスメントシート（効果的なコミュニケーション）

- 効果的なコミュニケーションには、「クローズド・クエスチョン」 と「オープン・クエスチョン」を組み合わせると良いと言われます。
- ヒアリングでは、Yes, Noの回答を求める「クローズド・クエスチョン」 になりがちですが、さらに要因を掘り下げていくために、「オープン・クエスチョン」を織り交ぜていくことが効果的です。

	クローズド・クエスチョン	オープン・クエスチョン
特徴	相手から回答を引き出す質問（回答は一言になりやすい）	相手に気づきを与える質問
	YES/NOで答えられる(一言になりやすい)	YES/NOで答えられない(説明になりやすい)
	具体的な事象や数値などを確認する質問	WHAT（なに）・WHY（なぜ）・HOW（どうやって）・WHO（だれ）など５W1Hの質問
	答える側の自由度が低く、会話は広がりづらい	答えの自由度が高いので、会話が盛り上がりやすい
	答える側は考える要素が少ないので、信頼関係が成立していない相手にも答えやすい	信頼関係がない相手にオープンクエスチョンをされると、情報をさらけ出すことに警戒心を覚えたりする
質問の例	＊パスワードは設定してますか？ ＊ウイルスに感染したことはありますか？ ＊毎年セキュリティ教育は行ってますか？ ＊社外でパソコンを使用していますか？	＊パスワードの設定にはどんな制限をかけてますか？ ＊ウイルスに感染した場合の対応は、どうなっていますか？ ＊セキュリティの啓発活動は、どんなことを行ってますか？ ＊リモートワークの手続きや環境はどのようなものですか？

【参考】アセスメントにおける成熟度モデルの考え方

- 企業が置かれた環境を踏まえて取り組みレベルを評価し、認識の共有化を図ることが必要です。
- 今後の目標や具体的対策の助言も、企業の環境を踏まえた実現可能なレベルにします。



顧客や取引先企業からの見え方	運用は担当者任せだが、規程・計画はあるので、単発の発注は可能な水準	規程の理解・運用が個人や部署により、ばらつきが見える水準	安心して仕事の発注や取引ができる水準	トレーサビリティがあり、信頼できる水準	ベストプラクティス企業として手本にしたい水準
企業の取り組みの特徴	規程や計画の仕組みができた状態	規程や計画に基づき活動しているが、改善の余地がある	PDCAの仕組みが定着している	活動の実績を分析し、問題発生の予兆を予測している	新技術を導入した革新的な試みを重視し、企業に変革を起こしている

※能力成熟度モデル：CMMI（Capability Maturity Model Integration）

改善計画書（記入例）

- 改善計画書は、セキュリティアセスメントの結果、「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）」★３申請を行うために実施すべき対策を取りまとめます。

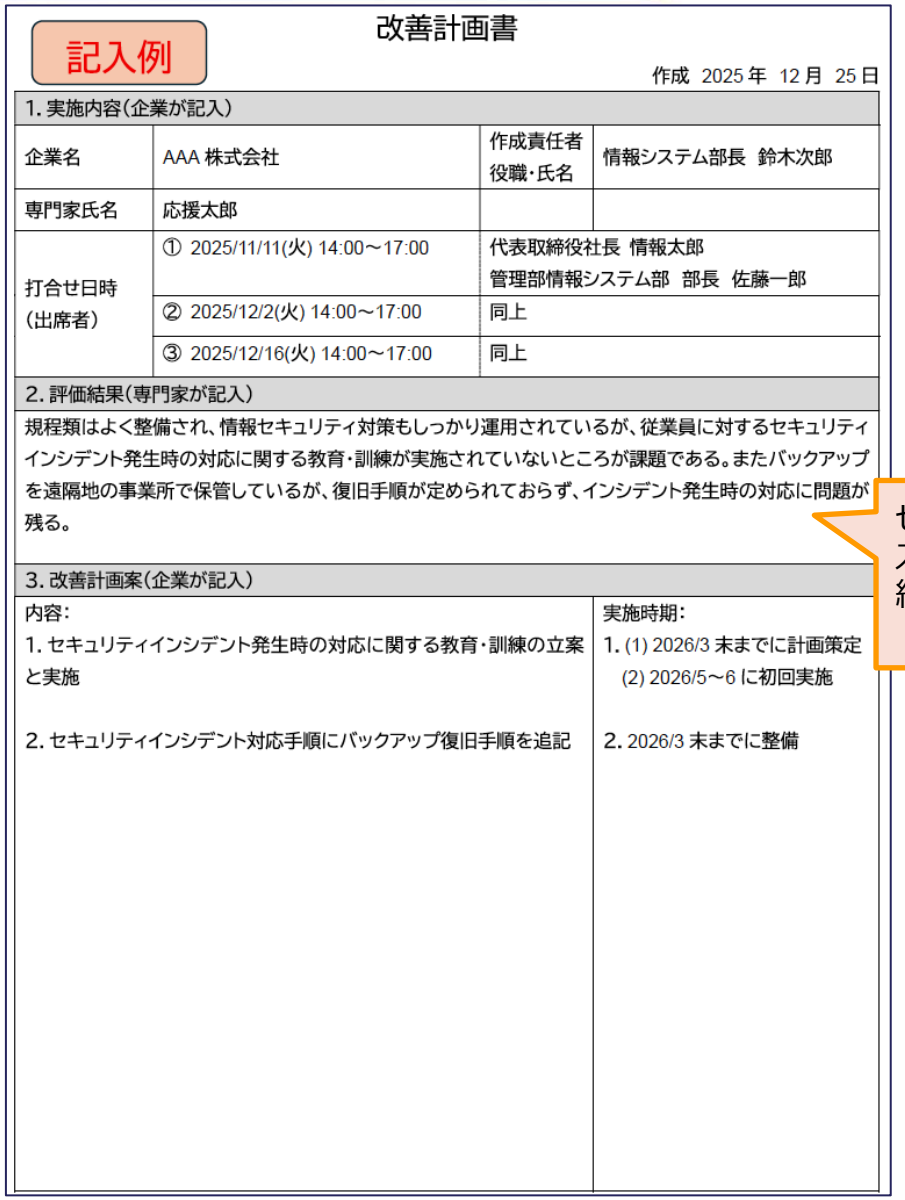
【作成手順】

（第2回指導）

- セキュリティアセスメントの結果、対策が不十分な項目の改善に関するディスカッションを行い、第3回までに指導先企業が改善計画書に対策を反映します。
- セキュリティ専門家は、第2回指導終了後、改善計画書の「2.評価結果（専門家記入）」欄にセキュリティアセスメントの評価結果を記入し、指導先企業へと送付しておきます。

（第3回指導）

- 指導先企業が作成した改善計画書について、優先度・実効性の観点を踏まえて検討を行い、作成に際し企業側で生じた疑問や質問等に回答・助言して、改善計画書を合意します。



記入例

改善計画書

作成 2025 年 12 月 25 日

1. 実施内容（企業が記入）			
企業名	AAA 株式会社	作成責任者 役職・氏名	情報システム部長 鈴木次郎
専門家氏名	応援太郎		
打合せ日時 （出席者）	① 2025/11/11(火) 14:00～17:00	代表取締役社長 情報太郎 管理部情報システム部 部長 佐藤一郎	
	② 2025/12/2(火) 14:00～17:00	同上	
	③ 2025/12/16(火) 14:00～17:00	同上	

2. 評価結果（専門家が記入）

規程類はよく整備され、情報セキュリティ対策もしっかり運用されているが、従業員に対するセキュリティインシデント発生時の対応に関する教育・訓練が実施されていないところが課題である。またバックアップを遠隔地の事業所で保管しているが、復旧手順が定められておらず、インシデント発生時の対応に問題が残る。

セキュリティアセスメントの評価結果を記載（専門家）

3. 改善計画案（企業が記入）

内容：	実施時期：
1. セキュリティインシデント発生時の対応に関する教育・訓練の立案と実施	1. (1) 2026/3 までに計画策定 (2) 2026/5～6 に初回実施
2. セキュリティインシデント対応手順にバックアップ復旧手順を追記	2. 2026/3 までに整備

監査の主な分類と特徴

- 監査はいくつかの視点により分類されますが、主なものを以下に示します。
- 監査の目的による分類では、企業などの組織体において、経営や業務活動が適切に行われているかを、第三者の監査人が、法令や一定の基準に基づいて客観的に評価し、その結果が適切でなければ、正しい方向へ改善を促す【助言型監査】 と、会計監査に代表される評価結果が適切であることを外部へ保証する【保証型監査】があります。
- 監査主体（実施者）の視点では、セルフチェック、内部監査、外部監査に分類され、それぞれが以下の特徴を持ちます。

視点 （監査の目的）	被監査企業（被監査部門）	監査主体・実施者（監査人）	監査結果利用者 （経営者、ステークホルダー）
助言型監査	改善提案が得られるが、正式な保証としては弱い	改善提案が期待され、コンサル的要素を含む	企業（部門）の内部改善に期待
保証型監査（※）	外部への説明責任を果たせるが、改善支援は限定的	独立性・客観性が強く求められる	外部への信頼確保に有効

※「保証」といっても、絶対的な保証ではなく、一定の判断の尺度に従って監査手続きを行った範囲における合理的な保証となることに留意が必要

視点 （監査主体）	被監査企業（被監査部門）	監査主体・実施者（監査人）	監査結果利用者 （経営者、ステークホルダー）
セルフチェック （自己点検）	取り組みやすいが客観性は弱い	本人や部門が自己点検	各自、各部門の内部改善に期待
内部監査	一定の客観性あり、改善に直結	独立した内部部門	企業（部門）のリスク管理に活用
外部監査	独立性が最も高く、信頼性確保に有効	外部専門家や監査法人	外部説明責任の証明に活用

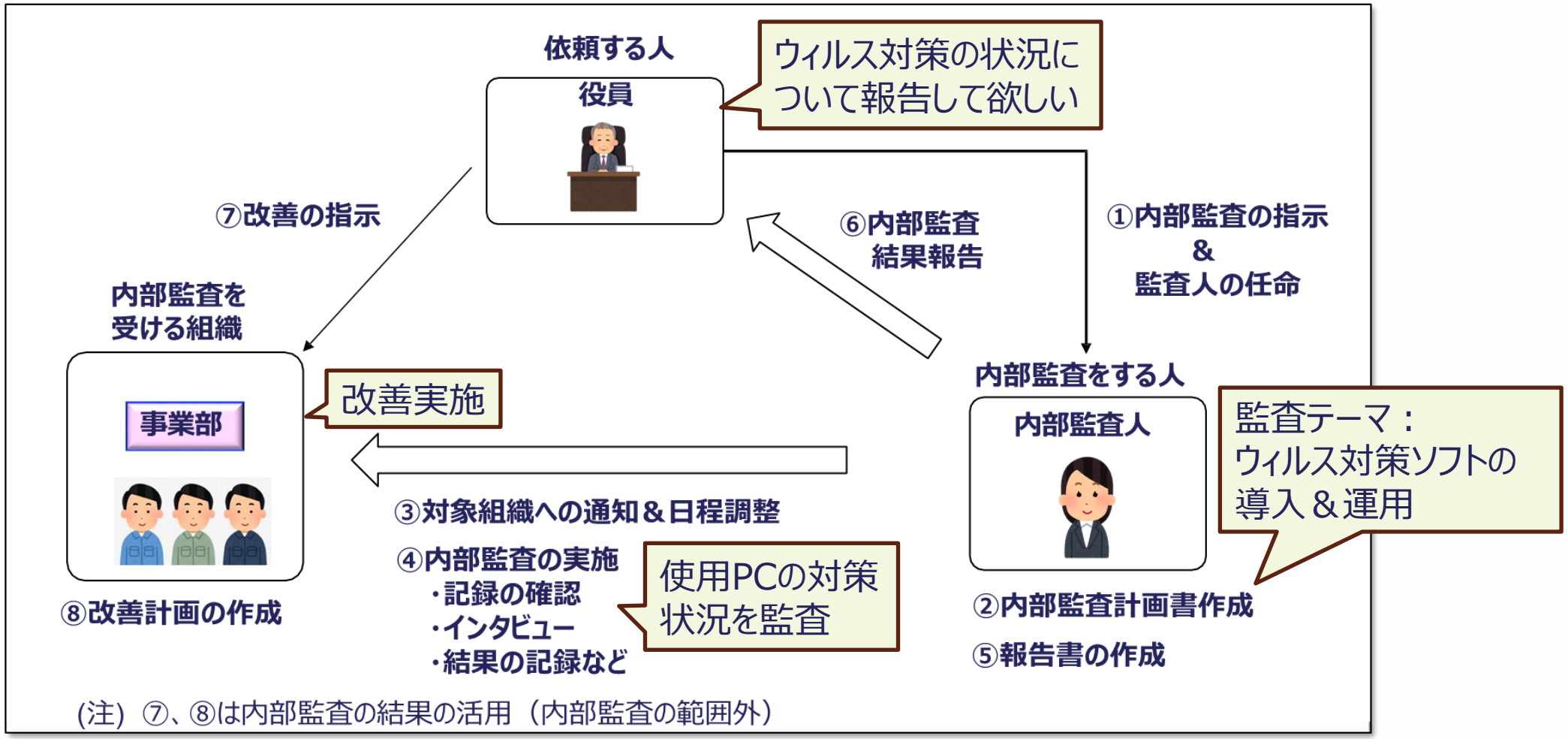
監査のプロセスと監査人の役割・責任

- 監査は、計画からフォローアップに至るプロセスで進められます。
- 以下に、各プロセスでの主な作業と、監査人が果たすべき役割と責任を整理しました。

監査プロセスの段階		主な作業項目	監査人の役割・責任
1	監査計画の策定	・監査目的、範囲、基準、方法を定義 ・監査チームと日程の調整 ・監査計画書の作成と承認	・監査計画書の作成責任を負う ・監査対象部門との調整・通知を行う ・独立性と客観性を確保する
2	予備調査（事前評価）	・関連文書や前回監査結果の確認 ・リスクや重点項目の特定	・監査重点を明確化し、効率的な監査を検討する ・必要に応じて監査計画を修正する
3	現地監査（実地審査）	・インタビュー、観察、記録の確認 ・証拠の収集と評価	・監査証拠を客観的に収集・記録する ・不適合や改善事項を明確に特定する ・監査チームをリードし、公正な判断を行う
4	監査結果の評価・結論	・証拠の整合性・妥当性を検証 ・基準との適合性を判定	・不適合の根拠を明確化する ・監査意見をまとめ、最終判断を下す
5	監査報告の作成	・監査結果を報告書に整理 ・是正要求や改善提案の提示	・報告書の正確性と透明性を確保する ・経営層や関係部門への説明責任を果たす
6	是正確認・フォローアップ	・是正処置の実施状況確認 ・再監査や改善確認の実施	・是正完了の妥当性を評価する ・必要に応じてフォローアップを実施する ・継続的改善を支援する

内部監査手続きの流れ（例：ウィルス対策ソフトの導入＆運用）

- 「ウィルス対策ソフトの導入＆運用」をテーマとした内部監査の例で、計画からフォローアップに至るプロセスを示します。
- また、次ページ以降で、監査人の視点や結果のまとめ方について例示します。



【出典】情報セキュリティ内部監査読本初学者向け（入門編）：・日本セキュリティ監査協会（JASA）、日本ネットワークセキュリティ協会（JNSA）より

内部監査の事例　（例：ウィルス対策ソフトの導入＆運用）

監査に用いる基準（情報セキュリティ管理基準など）

項目	内容
要求基準	✓ マルウェア対策として、以下の対策を実施すること
確認項目①	✓ 利用しているPCすべてにウィルス対策ソフトを導入（インストール）すること
確認項目②	✓ ウィルス対策ソフトの定義ファイルを最新化すること
確認項目③	✓ 毎週フルスキャンしてPCのHDDをすべて確認すること

【監査の視点】
規程や対策は、基準を満たしているか

社内ルール（規程、ガイド類）

項目	内容
規程	✓ マルウェア対策として、以下の対策を実施すること
対策①	✓ ネットワークに接続するPCにはすべて指定のウィルス対策ソフトをインストールする
対策②	✓ ウィルス対策ソフトのウィルス定義ファイルは常に最新のものを使用する
対策③	✓ 原則、毎週金曜日にフルスキャンを行う

【監査の視点】
現場の運用は、社内ルールを遵守しているか

チェックリストやヒアリングによる運用状況の確認結果

項目	PC #1	PC #2	PC #3	PC #4
対策①	○	X	○	○
対策②	○	X	○	○
対策③	X	X	○	X

監査結果	内容
発見事項①	✓ PC #02はウィルス対策ソフト自体がインストールされていなかった
発見事項②	✓ フルスキャンされていなかったPCが2台存在（PC #01、PC #04）

【監査の視点】
要因はどこにあり、どんな是正対応や助言があるか

【出典】情報セキュリティ内部監査読本初学者向け（入門編）をもとに編集・作成

内部監査の事例　（例：ウィルス対策ソフトの導入＆運用）

発見事項と要因分析＆是正対応

発見事項	指摘事項	ルール逸脱の要因（ヒアリング結果）	是正対応　（例示）
発見1： PC#02はウィルス対策ソフト自体がインストールされていなかった	ウィルス対策ソフトのインストールの実施＆フルスキャンの実施	PCを新機種に交換したタイミングで、ウィルス対策ソフトのインストールをしない状態で利用していた	機種交換時の設定マニュアルにウィルス対策ソフト等のインストールチェックリストを用意すると共にインストール結果＆設定状況のエビデンスの提出を行うプロセスとする
発見2： フルスキャンされていなかったPCが2台存在（PC#01、PC#04）	フルスキャンの実施	フルスキャンのタイミングが金曜日に設定されており、実行すると終了するまで30分～1時間程度を要することと、PCの反応が鈍くなることから業務優先で実行しなかった 特に金曜日は休み前のためにバタバタしていて他の曜日よりも余裕がない	フルスキャンのタイミングについて金曜日から水曜日に変更すると共に、設定で昼休み等に実行するように設定を行う

【出典】情報セキュリティ内部監査読本初学者向け（入門編）：・日本セキュリティ監査協会（JASA）、日本ネットワークセキュリティ協会（JNSA）より

監査における留意点　（基準、会社のルール、運用実態の整合性）

- 用いる基準や会社のルールに照らし合わせて、現場の対策状況を確認し、会社のレベルに合わせた是正や助言を行います。

用いる基準、会社のルール、現場の運用実態の対策レベルの差	評価・改善のポイント、留意点
求める対策レベル：用いる基準 ＝ 会社のルール ＝ 運用実態	✓ 基準、会社のルール、運用実態が合致 ✓ 更に対策の質的レベルを上げていくための助言があるか
用いる基準 ＞ 基準を満たしていない：会社のルール ＝ 運用実態	✓ 会社のルール（規程やガイド）の見直し ✓ 基準が高すぎて、これ以上対策レベルを上げることが難しいのか
用いる基準 ＝ 会社のルール ＞ ルールが遵守されていない：運用実態	✓ 現場に対策の必要性の理解を徹底 ✓ 基準や会社のルールが、現場とかけ離れたものになっていないか
過度な会社のルール：用いる基準 ＜ 会社のルール ＝ 運用実態	✓ 過度な対策の要求・実施が、現場の負担となり、生産性を阻害していないか

【出典】情報セキュリティ内部監査読本初学者向け（入門編）をもとに編集・作成

監査における留意点　（監査人として心掛けること）

- 監査人には、情報資産の保護と相手先との信頼性の確保において、以下に示すような高い職業倫理が求められますが、この点はアセスメントを担当する専門家においても、十分に心掛ける必要があります。

項目	監査人が心掛けるポイント（情報システム・情報セキュリティ監査の例）
誠実性	✓ 脆弱性や不正行為を発見した場合、適切に報告し、経営層にも率直にリスクを伝える ✓ 利害関係や圧力に屈せず、虚偽や隠蔽を行わない
客観性	✓ 特定の製品・技術への偏りを排除し、自らが関与したシステムやプロジェクトは監査しない ✓ 感情的判断ではなく、証拠とリスクに基づいて評価する
独立性	✓ 被監査部門・ベンダーから独立した立場を保持する ✓ 経済的・人的利害関係を排除し、外部からの影響を受けずに独自の判断を行う
公正性・透明性	✓ 監査範囲に対して手続きを公正に実施し、判定理由を明確に文書化する ✓ 技術的内容を非技術者にも分かりやすく説明する
守秘義務	✓ 入手した情報は厳重に管理し、保存・廃棄も定められた基準に従う ✓ 機密情報の私的利用や漏洩を行わない

SCS評価制度の概要

サプライチェーンセキュリティ対策評価制度

- **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、受注企業は**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しています。
- こうした課題に対応するため、国家サイバー統括室（NCO）、経済産業省、IPA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の検討**を進めており、2025年４月に制度の概要を整理した中間とりまとめを公表。現在、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**を目指しています。

SCS評価制度の評価スキーム

（2025年12月時点）

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制度構築方針（案）」公表
https://www.meti.go.jp/press/2025/12/20251226001/20251226001.html

	★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セキュリティ対策**として、**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	**専門家確認付き自己評価**	**第三者評価**	**第三者評価**
有効期間	1年	3年	TBD

セキュリティマネジメント指導（セキュリティアセスメント）の評価項目

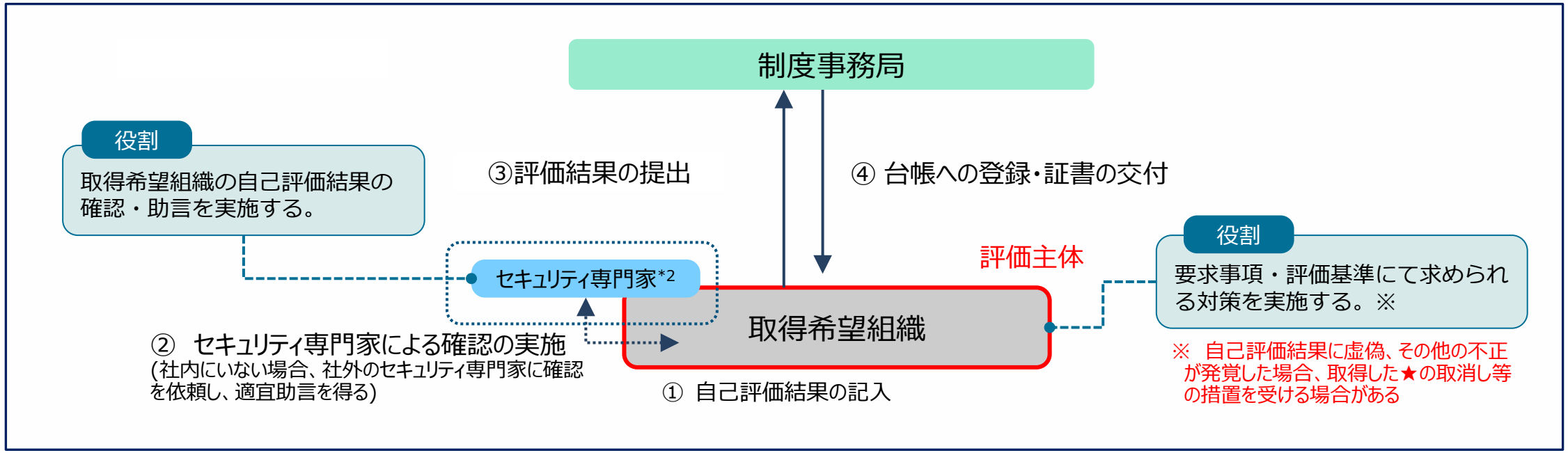
※ISMS適合性評価制度との制度的整合性、★3・4との整合性も踏まえ、対策事項を検討

- 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

★３における評価スキーム

専門家確認付き自己評価*1：★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

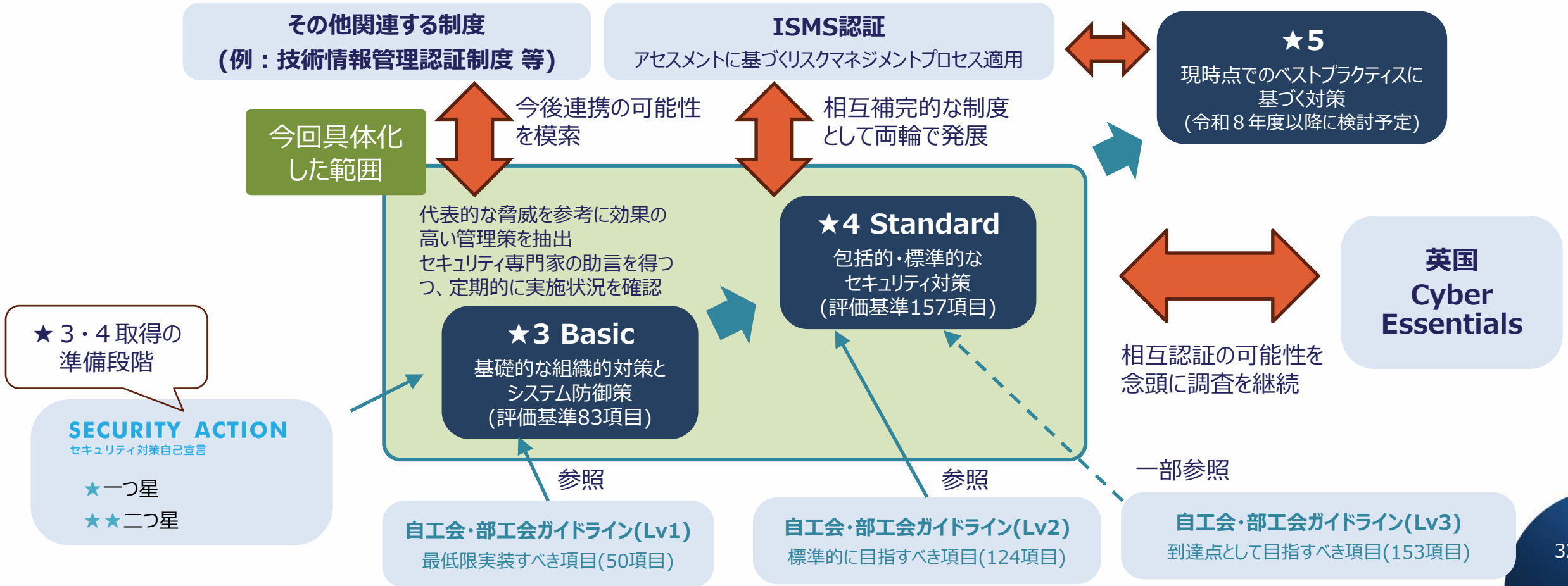


*1　経営層による自己適合宣言を経た取得希望組織として実施する評価のことを指し、組織内のセキュリティを担当する担当者や部門が独自に実施する評価は含まれない。
*2　取得希望組織が実施した自己評価結果に対してその内容の確認・助言を実施する者であって、一定のセキュリティ関連資格を有し、かつ、制度側で指定した研修を受講したものをいう。確認・助言に係る作業については、制度側で指定した研修を受講した作業従事者に実施させることができる。

SCS評価制度の概要

【参考】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。



参考情報一覧　（IPA関連）

- 中小企業の情報セキュリティ対策支援サイト
  https://www.ipa.go.jp/security/sme/isec-portal.html
  - 5分でできる！情報セキュリティ自社診断
    https://www.ipa.go.jp/security/guide/sme/5minutes.html
  - 情報セキュリティ対策ベンチマーク
    https://www.ipa.go.jp/security/sec-tools/benchmark.html
  - ５分でできる！ポイント学習
    https://www.ipa.go.jp/security/sec-tools/5mins_point.html
- セキュリティプレゼンター向け資料ダウンロード
  https://www.ipa.go.jp/security/sme/presenter/presenter-materials.html
- 中小企業の情報セキュリティ対策ガイドライン
  https://www.ipa.go.jp/security/guide/sme/about.html
- SECURITY ACTION セキュリティ対策自己宣言
  https://www.ipa.go.jp/security/security-action/
- 映像で知る情報セキュリティ ～映像コンテンツ一覧～
  https://www.ipa.go.jp/security/videos/list.html
- YouTube「IPAチャンネル」内の 情報セキュリティ普及啓発映像コンテンツ
  https://www.youtube.com/playlist?list=PLF9FCB56776EBCABB

参考情報一覧　（監査・アセスメント関連）

【監査関連】

- 情報セキュリティ内部監査読本初学者向け（入門編）
  ・日本セキュリティ監査協会（JASA）、日本ネットワークセキュリティ協会（JNSA）
  https://www.jasa.jp/wp-content/uploads/docs/情報セキュリティ内部監査読本%E3%80%80初学者向け（入門編）.pdf

- システム監査を知るための小冊子（改定第４版）　　日本システム監査人協会（SAAJ）
  https://www.saaj.or.jp/csa/CSAShiryo/CSA_Booklet2025.pdf

- 政府機関等のサイバーセキュリティ対策のための統一基準群に基づく情報セキュリティ監査の実施手引書
  ・政府機関等のサイバーセキュリティ対策のための統一基準群（国家サイバー統括室）
  https://www.nisc.go.jp/policy/group/general/kijun.html

【アセスメント関連】

- 自動車産業サイバーセキュリティガイドライン第2.3版　、同解説書、同チェックシート
  https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

- 技術情報管理認証制度 自己チェックリスト
  https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page03.html#checklist