経済産業省

資料３

事務局説明資料

2025年2月

経済産業省 商務情報政策局

サイバーセキュリティ課

Ⅰ　議論の全体像

Ⅱ　第３回の議論の振り返り

Ⅲ　登録セキスペ
　○登録セキスペアクティブリストを活用した中小企業支援
　○みなし受講制度

Ⅳ　中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保
　○実践的方策ガイドの位置付け等
　○実践的方策ガイドβ版（案）

Ⅰ　議論の全体像①（第４回検討会のテーマ）

- サイバーセキュリティ人材不足への対応として、本検討会では、既存施策の拡充や改善などを基本として、①セキュリティ・キャンプの拡充、②登録セキスペの活用及び制度の見直し、③中堅・中小企業等の内部でセキュリティ対策を推進する者の確保に向けた新たな施策、の３つの論点にスコープを絞って議論。
- 第４回検討会では、**上記②（登録セキスペ）のうち特にアクティブリスト・資格更新時の講習の受講みなし制度、③（内部人材確保策）に係る実践的方策ガイド（β版）**について、第３回検討会以降の検討を踏まえて議論。

※①（セキュリティ・キャンプの拡充）については、セキュリティ・キャンプ協議会WG等で検討中。

第３回検討会・資料３（抄）　＊赤字は第３回検討会資料に対する加工

サイバーセキュリティ人材育成の現状

セキュリティに関する知識・スキル水準の程度

トップガン

例）大手セキュリティ企業に就職する者、ベンダーとして起業する者など

高度専門人材

例）規模が大きいユーザー企業のセキュリティ担当者、大手ベンダー実務担当者など

専門人材

例）中堅・中小企業のユーザーのセキュリティ担当者など

※プラス・セキュリティ人材については、セキュリティに関する知識・スキル水準の高低とは別軸であるため、対象外とする。

施策の空白地帯

各層の育成・確保に向けた主な施策

セキュリティ・キャンプ ①

中核人材育成プログラム

登録セキスペ制度 ②

③

政策的な課題

- １年間に**育成できる人数が限定的**であり、スケールしていない。
- 修了後の**状況を追跡できていない。**

- ①実態を伴う**登録セキスペの活躍イメージを提示できていない（活躍の場がない）**場合や、②人手不足の**中小企業と登録セキスペとのミスマッチ**が起きている場合がある。
- 結果として、**登録更新に係る費用を支払うだけの動機が失われ**、登録者数の大幅な増加には至っていない。

- 中堅・中小企業においてサイバーセキュリティ人材が不足している一方、**社内育成・確保は困難**。参考事例もほぼ無い。
- 中堅・中小企業といっても多様であり、必要なセキュリティ対策や体制・人材水準は**各々の状況により異なる。**

対応の方向性

- 単純拡大ではなく、裾野を広げる観点から、特定領域（AI等）の専門性と高度なサイバーセキュリティの知見の双方を兼ね備えた人材の育成を目的とする**新たなキャンプを実施。**
- 修了生の継続的な知見研鑽・社会還元・活躍状況共有等を目的とした**コミュニティを整備。**

- **登録セキスペの得意分野・専門領域を可視化したリスト（アクティブリスト）の整備**等を通じた**市場への働きかけ**や、各種制度における登録セキスペ配置の要件化等の**企業側への働きかけ**を多層的に実施。
- **所定の実務経験を有する者を対象に資格更新時の講習の受講みなし制度を導入**する等により、資格維持コストを低減。

- **中堅・中小企業が実施すべきセキュリティ対策に応じた人材確保・育成の実践的方策を示したガイド（実践的方策ガイド）を整理し、様々な媒体で広報。**
- **自社のセキュリティ対策における現在の立ち位置、目指すべき姿の参考となる事例、人材を「育成」する際に参照できる実際のセミナー・資格等も提示。**

とりまとめに向けた継続議論事項

- 登録セキスペアクティブリストの詳細設計（掲載項目、活用促進策等）、更新講習の「みなし受講」の対象とする実務経験の範囲・判断方法等
- 中堅・中小企業向け「実践的方策を示したガイド」（β版）の策定、来年度におけるβ版の改善活動等（取組事例の収集、有効性の確認、普及方法）

⇒ 引き続きこれらの点について議論を行い、**令和６年度末を目途に①～③に係る具体的政策対応をとりまとめることを目指す。**

Ⅰ　議論の全体像②（予算事業の結果等を踏まえた支援策）

令和５年度補正**予算事業**（セキュリティ人材活用促進実証等）や**支援機関等の意見から得られた課題を踏まえ**、中小企業等がサイバーセキュリティ対策を無理なく実施できる人材面の支援策として、 ①個社の状況に応じた個別相談・支援が可能な登録セキスペをリスト化した**「登録セキスペアクティブリスト」** 、②セキュリティ対策の内容・人材確保策のエッセンスを段階的に示す**「実践的方策ガイド(β版)」**を活用・普及。

予算事業等の結果と課題

(1) セキュリティ対策の必要性と実施内容

〔セキュリティ人材活用促進実証〕
- セキュリティに対する意識があるものの、**始め方が分からない**、**相談先が分からない**社が約８割。
- 各社のセキュリティ課題は、**成熟度・課題領域が非常に多様**。

〔中小企業実態調査〕
- 47%が「**対策の必要性を感じたことがない**」と回答。
- 対策内容は、ウィルス対策など**基本的なものにとどまる**。

〔支援機関等の意見〕
- 対策を記載したガイドラインは**長尺で読むことが困難**。
- サンプル規程も個社に**そのまま適用できない**。

(2) 対策実施のための社内人材の確保・育成

〔中小企業実態調査〕
- 70%が社内に対策の**体制（専門部署、兼務担当者の任命）がなく**、64%が従業員への**セキュリティ教育を実施していない**と回答。
- 41%が人材育成のための**適切な演習がない・わからない**と回答。
- 対策向上に必要な事項として、上位から「**経営者のリスク意識向上**」「従業員の意識向上」「企業内の体制整備」「従業員への実践教育」と回答。

(3) 対策実施のための外部リソースの確保

〔中小企業実態調査〕
- 51%の企業が「**困った際の相談先が特にない**」と回答。
- 対策の情報収集先として**社外の登録セキスペは2.4%**。

(3) 対策実施のための外部リソースの確保（続き）

〔セキュリティ人材活用促進実証〕
- 専門家選定の観点として、「**緊急時の対応力**」「提案内容の**具体性**」「**技術力・専門性**」「自社の**業界に対する理解度**」「**コスト**」が上位。
- 依頼したい支援内容として「セキュリティ**教育の実施**」「**規程作成・改訂**」等が上位。また、自社の取組の妥当性を**第三者の視点から確認したい**、**業界別の要求事項**を具体的な対策に**落とし込みたい**といったニーズが存在。
- 専門家の探索方法として、「**公的機関（IPA等）におけるリストの利用**」のほか「**商工会議所等の支援機関**による紹介・マッチング」「取引のある**ITベンダー**からの紹介」が上位。

〔支援機関等の意見〕
- 専門家の情報として、**業務形態**（インハウス/独立）、**指導形態**（訪問/オンライン）による**料金区分**、**他の保有資格**などがあると選びやすい。
- 支援機関への専門家の浸透策として、**専門家団体による組織的対応**が有効では。
- 支援機関の指導員に対する研修実施も有効では。

個社の状況に応じて、セキュリティに関する**課題を発見**し、**対策内容をカスタマイズ**する**個別相談・支援**が必要

→ 相談者のニーズに応じた登録セキスペを探索できる**「登録セキスペアクティブリスト」**

各所に散らばったセキュリティ対策や人材確保・育成策（教育コンテンツを含む）の**標準的なエッセンスを段階的かつコンパクトに示すガイド**が必要

→ セキュリティ対策・人材確保・育成策を凝縮した**人材確保の「実践的方策ガイド(β版)」**

（連携）

ユーザである中小企業の利便性、中小企業の**支援機関による活用利便性**を念頭に具体化

Ⅰ　議論の全体像③（予算事業の結果等を踏まえた支援策（続き））

予算事業の結果等を踏まえた支援策（概要イメージ）

	必要性	内 容	活用・普及策
登録セキスペアクティブリスト	• セキュリティ対策の「始め方が分からない」「相談先が分からない」企業が**自社の課題を特定**するために、また、ひな形や要求事項を**自社にカスタマイズ**して落とし込むために、**専門家と相談**できる機会を**探索コストをかけずに確保**する必要。	• 相談者のニーズに応じた登録セキスペを選定できるよう、実証事業での声を踏まえ、 **支援実績テーマ／得意な業界／所属形態／登録セキスペ以外の保有資格など** を記載メニュー化したリストを作成・公表。 • **定型的な支援テーマ**（規程整備・リスク分析・クラウドサービス・インシデント対応・従業員教育）について、引き続き**ニーズ把握しつつ拡充を検討**。	• 中小企業の**直接利用（プル型）**のみならず、支援機関やITベンダー等の中小企業の**相談先を介した活用（プッシュ型）**も想定。 • 支援機関の**指導員への周知・研修**、支援機関の**窓口・専門家派遣事業**における利用。 • **専門家団体との連携**も検討。
人材確保・育成策の実践的方策ガイド	• **長尺なガイドを読むのが難しい**、人材育成のための**適切な演習が分からない**などの声や企業の**セキュリティ課題**は成熟度・課題領域が**多様**であることを踏まえ、**各所に散らばった対策の内容**や**人材確保・育成策のエッセンス**を**段階的・コンパクト**に示す必要。	• 経営者の意識向上につながるよう、**経営者向けのメッセージ**も収録。 • 相談各社の**セキュリティ課題は多様**であることを踏まえ、実施すべきセキュリティ対策をSECURITY ACTION★１レベルから**段階的に提示**。 • 段階ごとに**提示したタスクを実施する人材の確保・育成策**を**具体的な教育コンテンツ**等とともに提示。	• 中小企業の**経営者・セキュリティ担当者**を読者とするだけでなく、**中小企業の支援機関による活用**も想定。 • 支援機関、業界団体、教育コンテンツ提供者等を通じた普及のほか、**読者に応じた**チラシの作成、セミナーコンテンツ、**映像コンテンツ**等による普及も検討。

（参考）令和５年度補正予算事業（セキュリティ人材活用促進実証の概要）

- 物価高や最低賃金引上げ等により中小企業等における資金的余力や人材確保が厳しい状況にある中、セキュリティ専任の部署（担当者）が置かれるケースは少なく、多くは兼務となっており、セキュリティ業務の外部委託も進んでいない。その要因の１つとして、**セキュリティ人材に関する需要と供給の適切なマッチングがされていない**ことが考えられる。
- 令和５年度補正予算事業において、**中小企業等と登録セキスペとのマッチング**を促す場を構築する実証事業を実施し、**登録セキスペの社外における活用**と、**中小企業等がセキュリティ人材を探索しやすくするための環境整備**を検討。
- 具体的には、**商工会議所と連携**した**サイバーセキュリティ相談会を実施**し、相談会参加企業106社のうち34社が登録セキスペとマッチング。**登録セキスペによる訪問指導（マネジメント指導）を実施。**

〔中小企業等と登録セキスペのマッチングフロー〕

商工会議所と連携したサイバーセキュリティ相談会
- 商工会議所と連携したサイバーセキュリティ相談会を開催。
- 専門家によるセキュリティ対策の必要性等を訴求する基調講演を実施。

登録セキスペによる個別相談
- 相談会参加者のうち希望者に対して登録セキスペによる個別相談を実施。
- 自社のセキュリティ対策の課題を特定・優先づけを実施。

登録セキスペによるマネジメント指導
- 個別相談参加者のうち希望者に対し、**５つのマネジメント指導テーマ**の中から選択したテーマについて伴奏支援（３回実施し、各回ごとに目標を設定）。

〔相談会・個別相談の実施結果〕

相談会参加者アンケート・個別相談の結果
- セキュリティに対する意識がある社の中で、**どこから始めたらよいか分からない、どこに相談したらよいか分からない社が約８割**存在した。
- **セキュリティ専門家を選定するときに重視する点**として、「**緊急時の対応力**」「**提案内容の具体性**」「セキュリティ専門家の**技術力・専門性**」「**自社の業界に対する理解度**」「**コスト**」が上位に挙がった。
- **支援を希望する内容**（個別相談の中で明らかになったものを含む）として、「従業員向け**セキュリティ教育の実施支援**」「取引先から／取引先への**要求事項への対応支援**」「情報セキュリティ**規程の作成・改訂支援**」「現在の社内の**セキュリティ対策状況の診断**」が上位に挙がった。
- **セキュリティ専門家の探索手法**として望ましいと考えるものとして、「**公的機関（IPA等）における専門家リストの利用**」のほか、「商工会議所等の**中小企業支援機関による紹介**・マッチング支援サービス」「取引のある**ITベンダーからの紹介**」が上位に挙がった。

個別相談における具体的な相談内容
- 各社におけるセキュリティ課題は、その**成熟度や課題領域において非常に多様**。
- 「**サンプル規程**があることは知っているが、それをどのように使用し、**自社用に作り直せばいいのかがわからない**」など**具体的なアドバイス**を求める相談が見られた。
- 「作成した規程の内容が本当に十分か、自社に合っているか」など、**自社の判断・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**というニーズも存在。
- **業界別の対策水準の要求等の確保**を目的としたセキュリティ対策の相談が多く、**要求事項を自社に即した具体的な対策として落とし込む方法**について、実践的な示唆を求める声が複数確認。

Ⅰ　議論の全体像

Ⅱ　第３回の議論の振り返り

Ⅲ　登録セキスペ
　○登録セキスペアクティブリストを活用した中小企業支援
　○みなし受講制度

Ⅳ　中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保
　○実践的方策ガイドの位置付け等
　○実践的方策ガイドβ版（案）

Ⅱ　議論の振り返り①

セキュリティ・キャンプの拡充

①新たなキャンプの実施（セキュリティ・キャンプ・コネクト）

- **新たなキャンプのコンセプト**（特定の専門領域における高度な知見・技能を有する者の中からサイバーセキュリティに関する一定の知見を有する者を発掘し、サイバーセキュリティに関する知見と、サイバーセキュリティ以外の特定の専門領域における知見をトップレベルで併有する人材を育成）**に賛同。**
- 対象テーマについては、汎用的な技術領域／特定事業領域／その他社会科学系の領域等、様々検討の余地あり。
- 活動を推進させていくために、国立高専機構やenPiT等の既存の取組との連携、セキュリティ・キャンプの講義自体を大学の単位とできないか。
- **講師の確保に向けた課題**があるのではないか。

②修了生コミュニティの整備

- **修了生コミュニティ整備の趣旨**（①修了生同士のつながりを強化し相互に知見・技能を研鑽する機会を継続的に提供すること、②講師の立場としてのキャンプへの参画や政府機関等での活動を含め、修了生の知見・技能を社会に還元していくこと、③修了生の活躍状況を対外的に広報・PRすることで、セキュリティ・キャンプの取組やサイバーセキュリティ人材の価値向上につなげること）**に賛同。**
- **コミュニティの運営コストに課題**があるのではないか。

登録セキスペの活用及び制度の見直し

①ユーザ企業における活用促進・活躍の場の拡大（アクティブリスト活用等）

- **ユーザ企業における活用促進・活躍の場の拡大のための施策の全体パッケージ**、企業支援ができるセキュリティコンサルを見える化する**アクティブリストの趣旨に賛同。**
- アクティブリストに掲載されるべき情報項目として、産業別の実務経歴等のナラティブデータ、保有している他資格があるとよい。

登録セキスペの活用及び制度の見直し（続き）

- アクティブリストが活用されるための方策・環境整備として、**企業内登録セキスペが多いこと**、アクティブリスト**登録のメリット**、**登録者自身が情報をアップデートするインセンティブ**について考慮・検討が必要。
- 今年度実施している登録セキスペマッチング事業の進捗報告と今後の展開戦略について示されたい。

②資格維持コストの低減（「みなし受講制度」等）

- **みなし受講制度の対象となる実務経験を特定するための基本的な考え方（軸）について賛同。**
- サイバーセキュリティ関連業務（実践的業務）の内容を評価する方策等については、実務経歴書による**実務活動の信憑性確認は非常に大変**であること、確認する**体制面についても配慮**が必要。また、確認手法として、実務経歴書に加え自己学習とセットで信憑性を確認するべきという意見がある一方で、**所属長の承認等のエビデンスで足りるのでは**ないかとの意見もあり。
- みなし受講制度の対象として、国際会議での役職・セキュリティ関係のシンポジウム参加についても認められないか。
- **アクティブリストへの実務経験の登録との連携**も必要ではないか。
- みなし受講制度について、**登録者のブランドイメージの低下**や、登録者のキャリアにとってマイナス**にならないよう**にすることが重要。

③情報処理安全確保支援士試験の在り方

- 情報処理安全確保支援士試験の**試験科目や試験区分について複雑にするべきではない。**
- （試験科目や試験区分は同一としつつも）**情報処理安全確保支援士試験におけるセキュリティマネジメントに関する出題の要素を増やす**（午後試験の選択問題として増やす 等）と良いのではないか。

Ⅱ　議論の振り返り②

中堅・中小企業等の内部でセキュリティ対策を推進する者の確保

- **実践的方策ガイド**（想定読者として経営層、セキュリティ人材本人、中堅・中小企業を支援する立場の人材を置き、実施すべきセキュリティ対策に応じて人材の確保・育成策についても合わせて提示するとともに、自社のセキュリティ対策における現在の立ち位置、目指すべき姿の参考となる事例等を提示したガイド）**の全体像に賛同**。
- 実践的方策ガイドにおいて参照しているSECURITY ACTION、中小企業の情報セキュリティ対策ガイドラインの改訂が必要ではないか。実践的方策ガイドと経営ガイドラインとその付属文書との関係性、現在検討中のサプライチェーン対策評価制度との関係性を含めた**体系的な整理が必要性**ではないか。
- 実践的方策ガイドの内容として、読者が自分事として捉えられる**事例の提示**が有効。
- 実践的方策ガイドの**普及方法**として、実践的方策ガイド文書にとどまらず、**セミナー**等での展開や**映像コンテンツ**を活用できないか。
- 来年度の**実証**について、**セキュリティ専門家等が伴走支援**をしながらの実践的方策ガイドの**有効性確認**や**事例の収集**を実施することに**賛同**。
- 実証に併せて、実践的方策ガイドを中堅・中小企業に**普及させるために有効な方法**等の調査を実施することに**賛同**。
- **事例の収集**については、大企業であれば当たり前に実施するような**平易な対策の実施事例**、**人材不足によってインシデント対応が遅れた事例**などが有効ではないか。

Ⅰ　議論の全体像

Ⅱ　第３回の議論の振り返り

Ⅲ　登録セキスペ
　○登録セキスペアクティブリストを活用した中小企業支援
　○みなし受講制度

Ⅳ　中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保
　○実践的方策ガイドの位置付け等
　○実践的方策ガイドβ版（案）

登録セキスペアクティブリストを活用した中小企業支援（趣旨）

- 令和５年度補正予算事業において、**中小企業と登録セキスペのマッチングを促す場を構築**し、予め設定した**マネジメント指導テーマに即して**、セキュリティの課題を抱える**中小企業と登録セキスペの効率的なマッチング**について検証中。

- 令和７年度に、検証結果を踏まえ、**登録セキスペの得意分野・専門領域を可視化**する**「登録セキスペアクティブリスト」を整備する**とともに、リスト掲載項目の一つである**マネジメント指導テーマの拡充など、継続的にリストの掲載内容・運用を改善。**

- 「リスト」の活用を通じて、中小企業が**多大な探索コストをかけることなく**、地域の支援機関等を通じて**登録セキスペを活用するとともに、登録セキスペにとっても活躍の機会が広がる**ことを期待。

セキュリティ人材活用促進実証（マネジメント指導テーマ）

- 業種を問わない「基本の基」のセキュリティ対策として、**中小企業ガイドライン（付属書を含む）の指示項目の実装を目的としたマネジメント指導のテーマ**を設定し、各テーマについて指導マニュアルを整備。
- 令和７年度以降、既存の指導テーマのブラッシュアップや指導テーマの拡充について検討。

	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
ターゲット企業	**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。
期待される効果	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、従業員の訓練も実施することで、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。

（参考）マネジメント指導テーマと支援士試験シラバスの関係

- 令和５年度補正予算事業（中小企業等と登録セキスペとのマッチングを促す場を構築する実証事業）において設定したマネジメント指導テーマは、情報処理安全確保支援士試験（レベル4）シラバスとの対応関係を意識して設定。

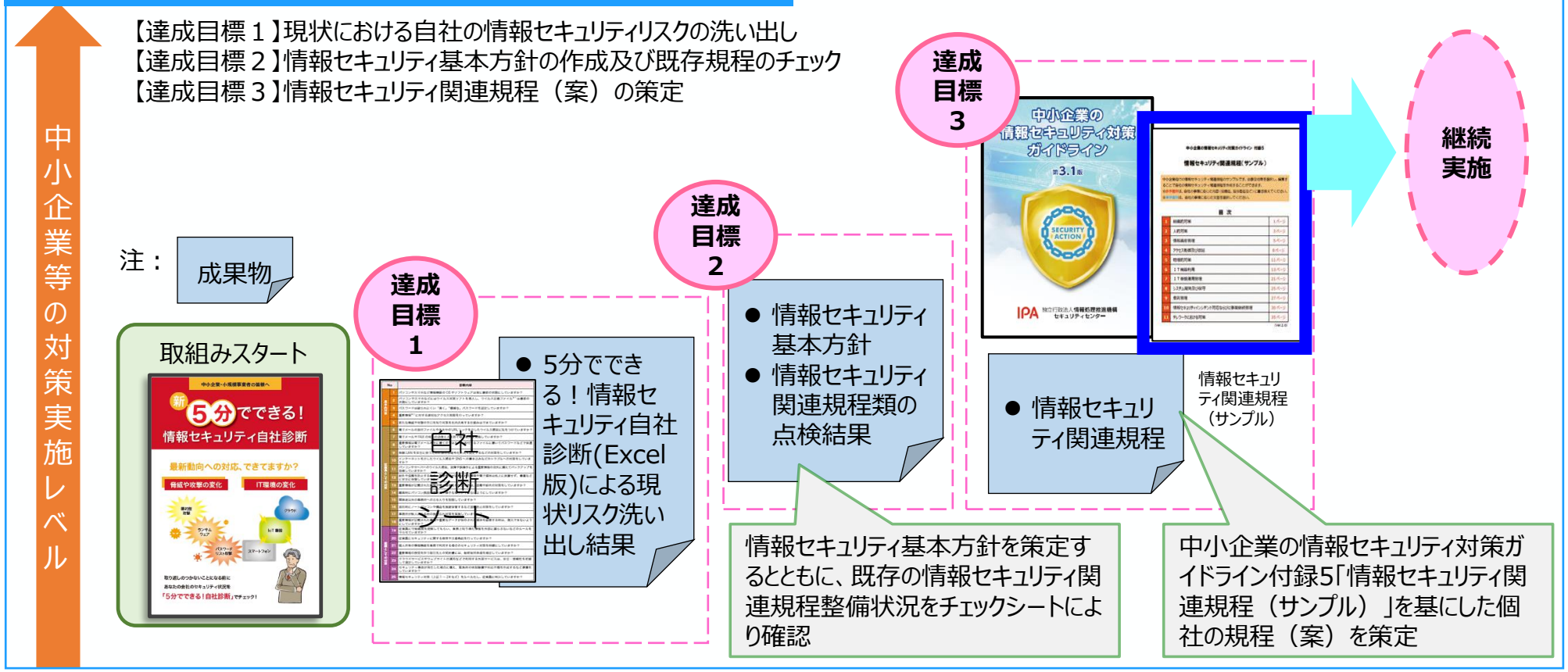
マネジメント指導ツール（テーマ別）		情報処理安全確保支援士試験（レベル4）シラバスとの対応	
テーマ	マネジメント指導の達成目標	シラバス大項目	シラバス小項目
指導テーマ①｜情報セキュリティ規程の整備	【達成目標１】現状における自社の情報セキュリティリスクの洗い出し 【達成目標２】情報セキュリティ基本方針の作成及び既存規程のチェック 【達成目標３】情報セキュリティ関連規程（案）の策定	1 情報セキュリティマネジメントの推進又は支援に関すること	1-1 情報セキュリティ方針の策定 1-4 情報セキュリティ諸規程の策定 1-6 情報セキュリティに関する動向・事例の収集と分析
		3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	3-1 暗号利用及び鍵管理 3-2 マルウェア対策 3-6 脆弱性への対応 3-9 人的管理 3-11 コンプライアンス管理
		4 情報セキュリティインシデント管理の推進又は支援に関すること	4-1 情報セキュリティインシデントの管理体制の構築
指導テーマ②｜情報資産の洗い出しとリスク分析	【達成目標１】現状における自社の情報セキュリティリスクの洗い出し 【達成目標２】自社における情報資産の洗い出し 【達成目標３】抽出した情報資産リストに対するリスク分析の実施	1 情報セキュリティマネジメントの推進又は支援に関すること	1-2 情報セキュリティリスクアセスメント 1-3 情報セキュリティリスク対応 1-6 情報セキュリティに関する動向・事例の収集と分析
指導テーマ③｜クラウドサービスの安全利用	【達成目標１】現状における自社の情報セキュリティリスクの洗い出し 【達成目標２】自社における現状導入済み/利用予定クラウドサービスの洗い出し 【達成目標３】抽出したクラウドサービスに対する安全利用チェック	1 情報セキュリティマネジメントの推進又は支援に関すること	1-4 情報セキュリティ諸規程の策定 1-6 情報セキュリティに関する動向・事例の収集と分析
		2 情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	2-2 製品・サービスのセキュアな導入
		3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	3-3 バックアップ 3-8 アカウント管理及びアクセス管理
指導テーマ④｜セキュリティインシデント対応	【達成目標１】現状における自社の情報セキュリティリスクの洗い出し 【達成目標２】インシデント対応手順書の作成 【達成目標３】作成したインシデント対応手順書に基づく机上演習の実施	1 情報セキュリティマネジメントの推進又は支援に関すること	1-6 情報セキュリティに関する動向・事例の収集と分析
		3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	3-2 マルウェア対策 3-4 セキュリティ監視並びにログの取得及び分析 3-7 物理的セキュリティ管理
		4 情報セキュリティインシデント管理の推進又は支援に関すること	4-1 情報セキュリティインシデントの管理体制の構築 4-2 情報セキュリティ事象の評価 4-3 情報セキュリティインシデントへの対応 4-4 証拠の収集及び分析
指導テーマ⑤｜従業員向け情報セキュリティ教育	【達成目標１】現状における自社の情報セキュリティリスクの洗い出し 【達成目標２】サイバーセキュリティに関する従業員教育の実施 【達成目標３】教育実施結果のレビューと、以後の継続実施に向けた教育計画の策定	1 情報セキュリティマネジメントの推進又は支援に関すること	1-6 情報セキュリティに関する動向・事例の収集と分析
		2 情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	2-7 運用・保守（セキュリティの観点）
		3 情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	3-9 人的管理
		4 情報セキュリティインシデント管理の推進又は支援に関すること	4-3 情報セキュリティインシデントへの対応

セキュリティ人材活用促進実証（指導テーマごとの詳細）

①情報セキュリティ規程の整備

- 「中小企業の情報セキュリティガイドライン(第3.1版)」中の「情報セキュリティサンプル規程」を基に、指導先企業の「情報セキュリティ基本方針（案）」「情報セキュリティ関連規程（案）」の策定・整備について、必要な指導・助言を行い支援。

マネジメント指導業務の達成目標と成果物



②情報資産の洗い出しとリスク分析

- 「中小企業の情報セキュリティガイドライン(第3.1版)」付録7「リスク分析ワークシート」を基に、指導先企業における情報資産の洗い出しとリスク分析を実施し、必要な情報セキュリティ対策について、必要な指導・助言を行い支援。

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情報セキュリティリスクの洗い出し
【達成目標２】自社における情報資産の洗い出し
【達成目標３】抽出した情報資産リストに対するリスク分析の実施

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)による現状リスク洗い出し結果

達成目標2

● 社内における情報資産の洗い出し

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値			重要度	保存期限	登録日	現状から想定される リスク（入力不要・自動表示）			
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性				脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性	リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	3	5年	2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1	可能性：低	3	リスク小
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2	3	7年	2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2	可能性：中	6	リスク大

達成目標3

● 情報資産に対するリスク分析実施

継続実施

③クラウドサービスの安全利用

- 「中小企業の情報セキュリティガイドライン(第3.1版)」付録6「中小企業のためのクラウドサービス安全利用の手引き」を基に作成した「クラウドサービス台帳兼チェックリスト」を用い、指導先企業におけるクラウドサービス安全利用チェックを実施し、必要な情報セキュリティ対策について、指導・助言を行い支援。

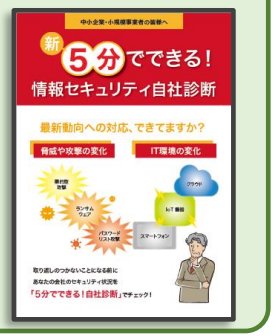
マネジメント指導業務の達成目標と成果物

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情報セキュリティリスクの洗い出し
【達成目標２】自社における現状導入済み/利用予定クラウドサービスの洗い出し
【達成目標３】抽出したクラウドサービスに対する安全利用チェック

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)による現状リスク洗い出し結果

達成目標2

- 社内におけるクラウドサービスの洗い出し

達成目標3

- クラウドサービスに対する安全利用チェック実施

継続実施

④セキュリティインシデント対応

- 「中小企業の情報セキュリティガイドライン(第3.1版)」付録8「中小企業のためのセキュリティインシデント対応の手引き」を基に、支援先企業におけるインシデント対応手順書の作成について、 必要な指導・助言を行い支援 。

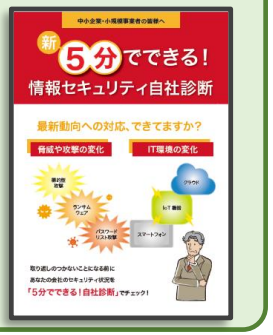
マネジメント指導業務の達成目標と成果物

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情報セキュリティリスクの洗い出し
【達成目標２】インシデント対応手順書の作成
【達成目標３】作成したインシデント対応手順書に基づく机上演習の実施

注：成果物

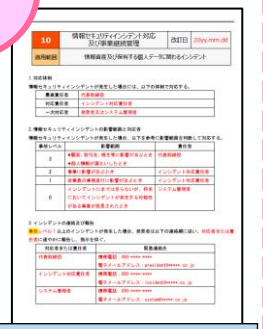
取組みスタート



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)による現状リスク洗い出し結果

達成目標2



- インシデント対応手順書（規程）の作成

達成目標3

インシデント対応机上演習の実施とレビュー

継続実施

⑤従業員向けセキュリティ教育

- IPAが有する教育用コンテンツを活用し、企業のニーズに応じた形で具体的な研修計画を立案し、従業員向けセキュリティ教育を実施。
- 実施後の効果をレビューするとともに、継続的な実施を目指し、セキュリティ教育計画書の策定について、必要な指導・助言を行い支援。

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情報セキュリティリスクの洗い出し
【達成目標２】サイバーセキュリティに関する従業員教育の実施
【達成目標３】教育実施結果のレビューと、以後の継続実施に向けた教育計画の策定

注：成果物

取組みスタート

達成目標1

自社診断シート

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

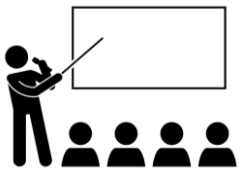
達成目標2

● 従業員向けサイバーセキュリティ教育の実施

達成目標3

セキュリティ教育計画書
目的
対象
実施内容
評価方法

● 教育実施結果のレビューと、以後の教育計画の策定

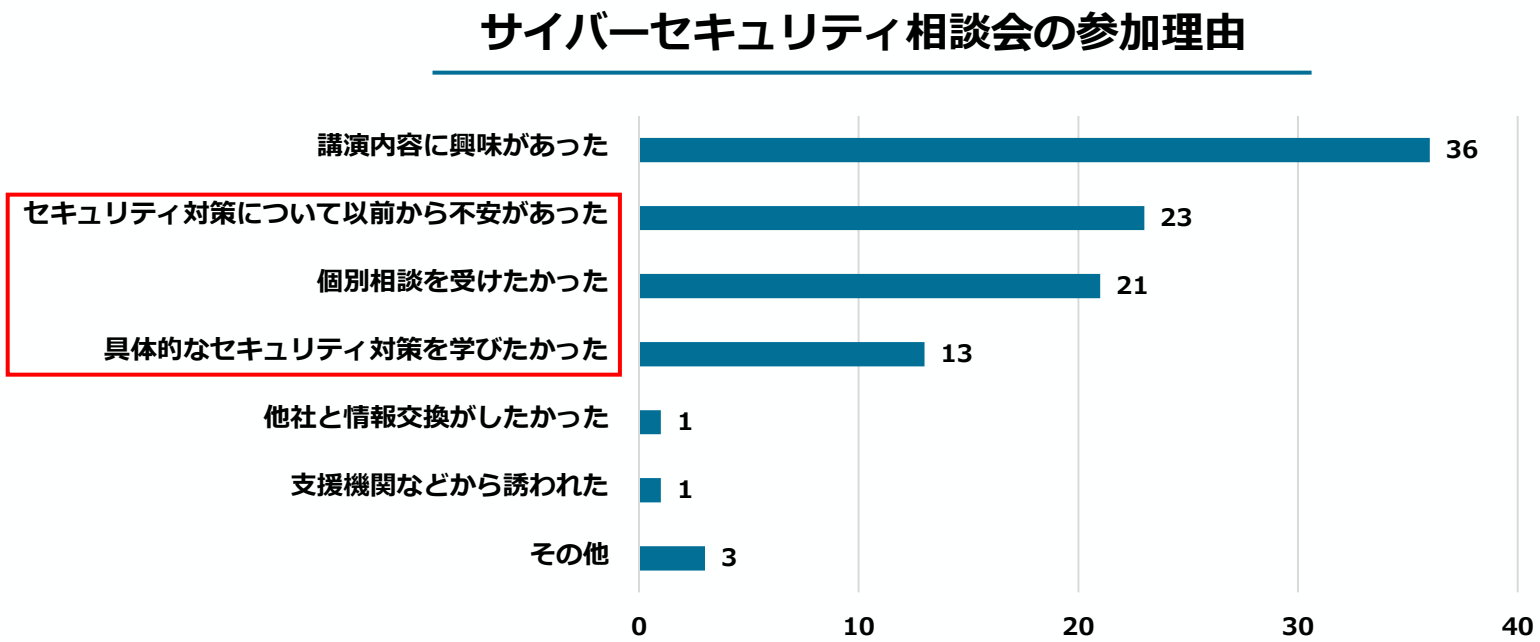


継続実施

セキュリティ人材活用促進実証（相談会参加者アンケート・個別相談の結果）

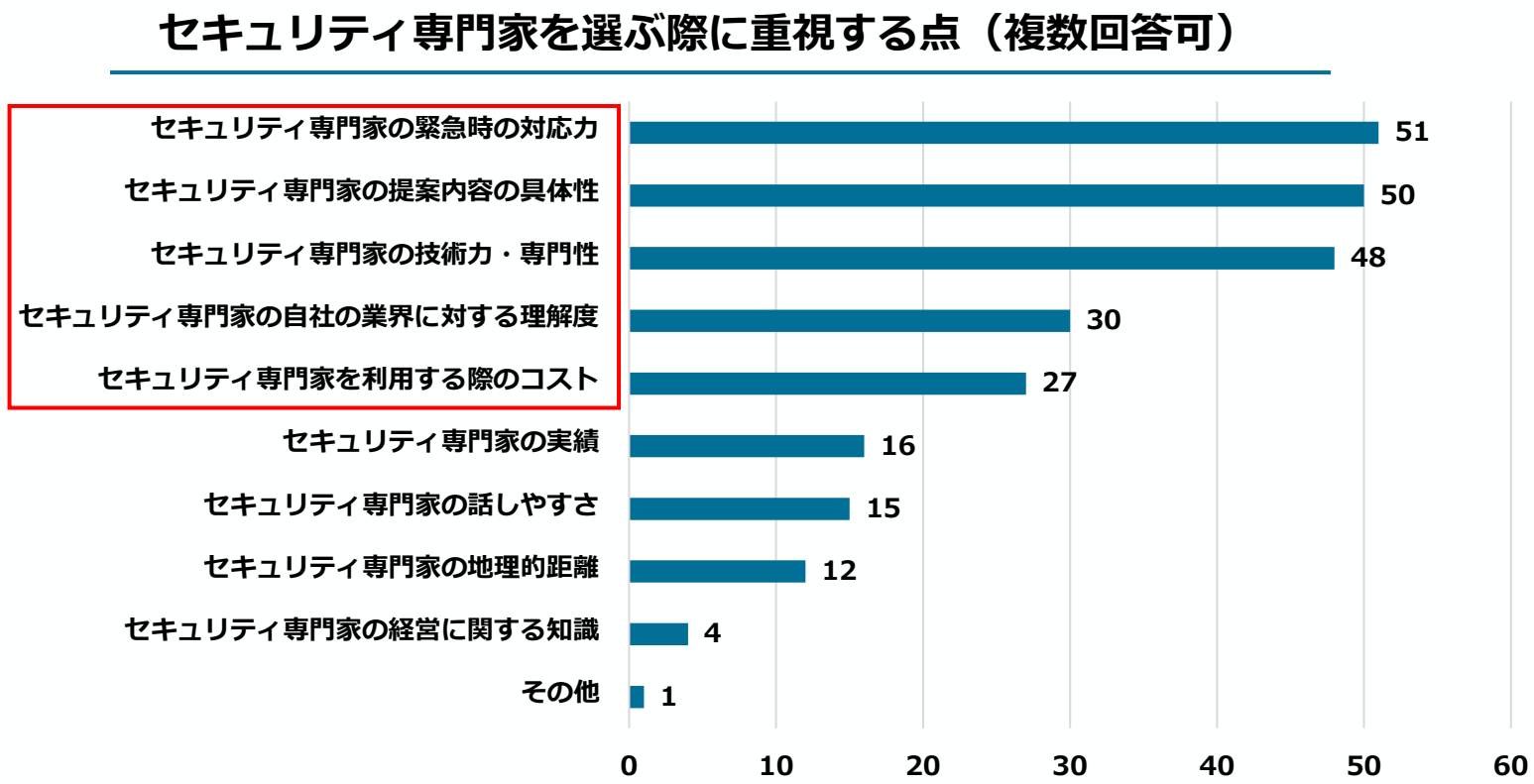
①相談会への参加理由

- 全体の約４割が講演内容そのものに興味があったため参加したと回答した一方で、全体の約６割がセキュリティ対策に関して問題意識がある（セキュリティ対策について以前から不安があった：全体の約23%、個別相談を受けたかった：全体の約21%、具体的なセキュリティ対策を学びたかった：全体の約13%）と回答した。
- セキュリティ対策に関して意識がある社のうち、約２割は自社のセキュリティに関する課題を特定し、具体的なセキュリティ対策を学びたい社であったが、約８割は**セキュリティに対する意識があるものの、どこから始めたらよいかわからない、どこに相談したらよいかわからない**社が占め、そうした**社に対して登録セキスペに相談する機会を提示することができた。**



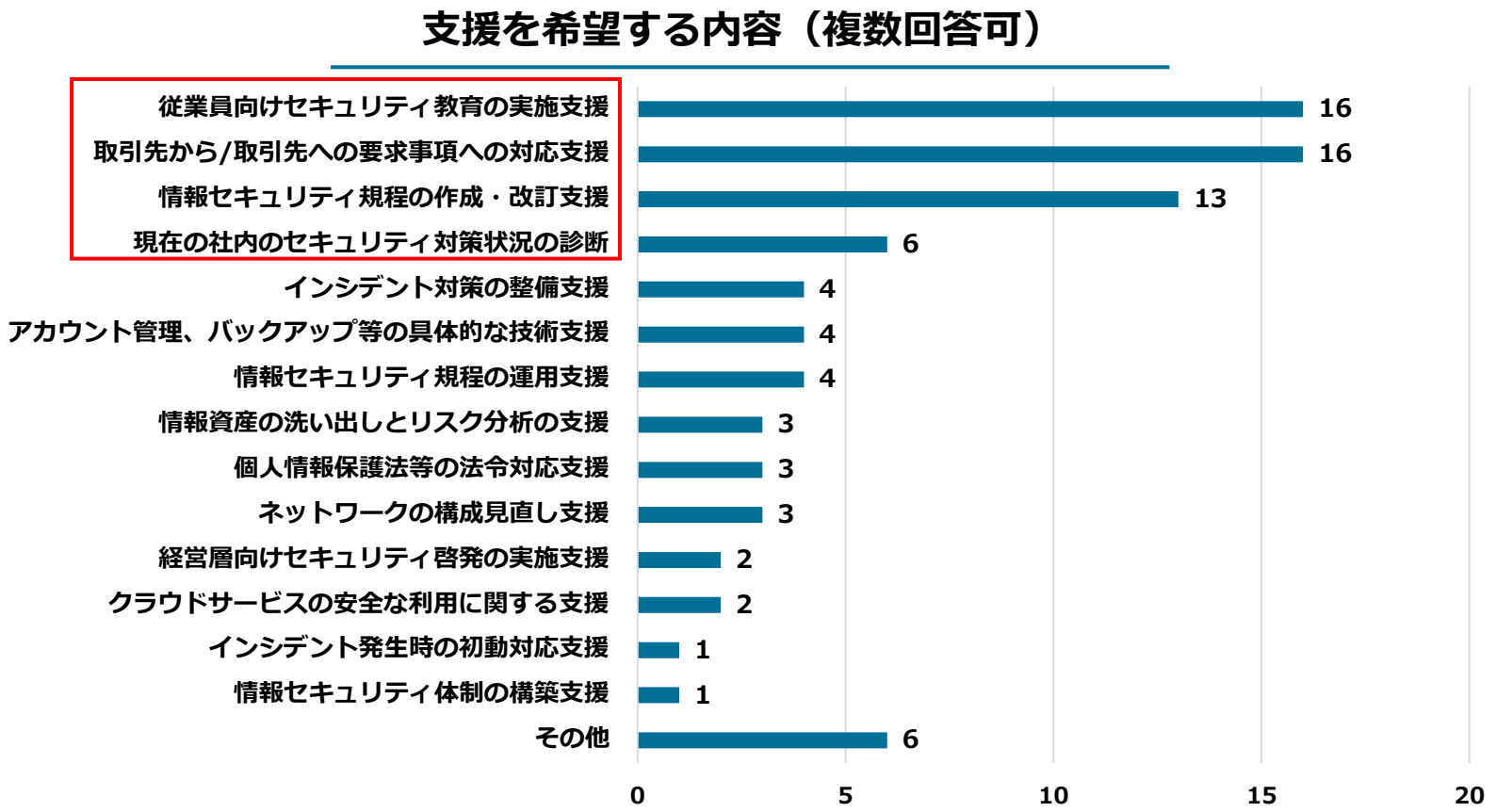
②中小企業が専門家を選定するときに重視する点

- 中小企業がセキュリティ専門家を選定するときに重視する点として、**「緊急時の対応力」「提案内容の具体性」「セキュリティ専門家の技術力・専門性」「自社の業界に対する理解度」「コスト」**が上位に挙がった。
- これらの結果を踏まえ、**「登録セキスペアクティブリスト」の掲載項目について、引き続き検討。**



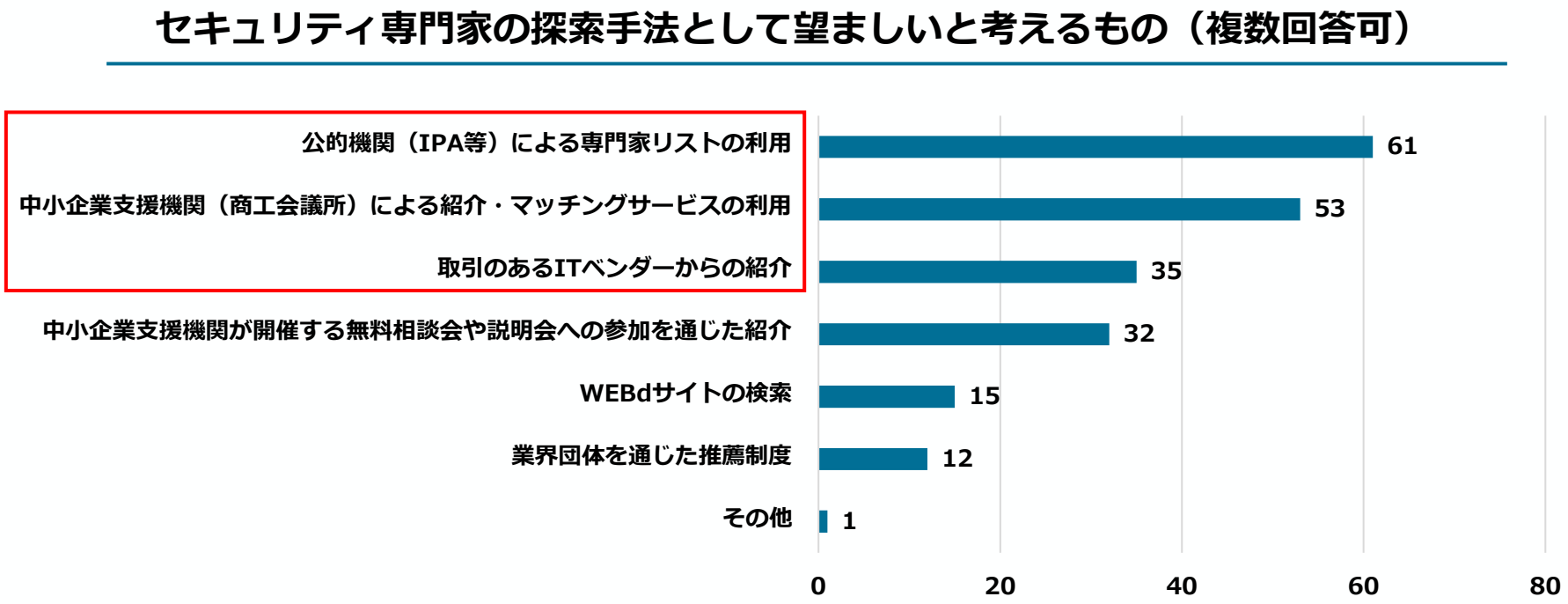
③支援を希望する内容

- 支援を希望する内容（個別相談の中で明らかになったものを含む）として、**「従業員向けセキュリティ教育の実施支援」「取引先から／取引先への要求事項への対応支援」「情報セキュリティ規程の作成・改訂支援」「現在の社内のセキュリティ対策状況の診断」**が上位に挙がった。
- また、これらの支援において、**対策の全体的な進め方、粒度、費用感**についても合わせて相談があった。
- これらを踏まえ、**「登録セキスペアクティブリスト」の掲載項目の一つとして想定しているマネジメント指導テーマの充実・拡充に向けて検討。**



④セキュリティ専門家の探索手法

- セキュリティ専門家の探索手法として望ましいと考えるものとして、**「公的機関（IPA等）における専門家リストの利用」**のほか、**「商工会議所等の中小企業支援機関による紹介・マッチング支援サービス」「取引のあるITベンダーからの紹介」**が上位に挙がった。
- この結果は、必ずしもセキュリティ意識が高くない中小企業に対してもリーチするためには、**支援機関やITベンダー等の中小企業の相談先を介した登録セキスペアクティブリストを活用**することが望ましいことを示唆。



セキュリティ人材活用促進実証（相談会における具体的な相談内容）

- 相談会における具体的な相談内容としては、**成熟度・領域ともに多様**であり、**①標準的なひな形を自社向けにカスタマイズしたい**、**②取組中の対策の妥当性（現状で十分なのか）を第三者的に確認したい**、**③各種ガイドラインの要求事項を自社の具体的対策として落とし込みたい**といったものが挙げられる。

- 個別具体的な課題を持つ企業が存在する一方で、「守るべき情報が無い」「何をどう始めていいか分からない」といった初歩的な段階にある企業も依然として存在するなど、**相談各社におけるセキュリティ課題は、その成熟度や課題領域において非常に多様**。
- 「サンプル規程があることは知っているが、それをどのように使用し、自社用に作り直せばいいのかがわからない」など、**対策の内容や進め方についての具体的なアドバイスを求める相談**が見られた。
- 加えて、「作成した規程の内容が、本当に十分なのか、または自社に合っているかが分からない」「お助け隊に加入しているがセキュリティ対策はこれだけで十分なのか分からない」「ベンダー任せでシステムを構築しているが、この構成でセキュリティ対策ができているか確かめたい」「何を優先してセキュリティ対策を進めていいのか分からない」 など、**自社の判断・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**も存在。
- さらに、**業界別の対策水準の要求に関する相談**（自動車産業における「自工会/部工会・サイバーセキュリティガイドライン」や、医療分野における３省２ガイドライン「医療情報システムの安全管理に関するガイドライン」（厚生労働省）「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省））や、**取引先との事業継続性の確保を目的としたセキュリティ対策の相談**が多く、**要求事項を自社の状況に即した具体的な対策として落とし込む方法**について、実践的な示唆を求める声が複数確認。

登録セキスペアクティブリストの基本設計（案）

- 令和５年度補正予算事業の実施状況を踏まえ、登録セキスペアクティブリストの基本設計について、以下のとおり整理。
- 令和７年度において、登録セキスペアクティブリストを整備し、運用開始を目指すとともに、リスト掲載項目の一つであるマネジメント指導テーマの拡充など、継続的にリストの掲載内容・運用を改善。

Ⅰ　リストの内容

掲載対象者	• 中小企業等に対する**セキュリティコンサルが可能な登録セキスペ**が掲載対象。 ※　登録セキスペとしての専門的知識・技能を所属組織のセキュリティ対策のために発揮することが予定されている者で副業・兼業ができないものは、掲載の対象外と想定（所属組織が中小企業等に対するセキュリティコンサルを行っている場合は、掲載の対象と想定）。
掲載項目	• 企業・支援機関等に対して、「どのような支援を行うことができるか」を示す項目を提示。 • 具体的な項目としては、氏名・連絡先・対象地域、料金・期間・形態（訪問・オンラインなど）のほか、**支援実績のあるテーマ（マネジメント指導テーマその他の支援テーマ）・業界・他の保有資格など**を想定。

Ⅱ　リストの管理運用

管理運用主体	• マネジメント指導テーマの管理と併せて**IPA**とすることを想定。 ※　掲載項目のブラッシュアップ等に当たっては、関係団体と連携することも想定。
登録方法	• 既存の登録セキスペについては、リスト登録を案内し、登録申請を受けることを想定。また、新規登録・更新時にもリスト更新を案内することを想定。 ※　令和５年度補正予算事業の成果物としてのリストにおいては、同事業のマネジメント指導の実績がある者を中心に掲載することを想定。令和７年度以降は、対象者を拡充することを想定。

Ⅱ　リストの管理運用（続き）

更新方法	• **登録者自らによる更新**を想定。 • 確実に更新いただくため、更新等の機会を捕まえて、管理主体から更新依頼をすることも一案。 • 後述のみなし受講制度の対象となる実務経験等に「マネジメント指導」を得出しして位置付け、情報更新の誘因とすることも一案。
活用方法	• リストは公開し、**企業側の発意による利用が可能。セキュリティ対策をどこから始めたらよいかわからない、どこに相談したらよいかわからない企業**や、具体的なセキュリティ対策を実施したい企業が直接利用することを想定。 • 他方で、実証事業の結果を踏まえ、商工会議所等の**支援機関（※１）や、ITベンダー（※２）等の中小企業の相談先を介した活用**も想定。 （※１）令和５年度補正予算事業の中小企業と登録セキスペのマッチング事業において、支援機関を介したマッチングが有効であることを検証中。 （※２）令和５年度補正予算事業の地域ベンダー向け手引書において、登録セキスペの活用についても紐づけを検討中。 • 上記のほか、①支援機関の無料相談窓口にリスト掲載者を配置すること、②支援機関による専門家派遣事業で専門家を選定する際に、リストを活用いただくことを検討。

Ⅲ　その他

- 現在IPAが管理運用している「情報処理安全確保支援士 検索サービス」は、全登録セキスペを管理番号ベースで対象としているものの、氏名・連絡先・保有スキル等が任意項目となっているところ、同サービスの扱いについては「登録セキスペアクティブリスト」の具体化の中で引き続き検討。

（参考１）アクティブリストの完成イメージ（案）

- アクティブリストの掲載項目について、現時点案としては以下のとおり。
- 中小企業や支援機関等が登録セキスペを選定する際に必要となる基礎情報に加えて、詳細情報の掲載項目についても引き続き検討。

検索結果一覧（基礎情報）

	氏名	支援実績のあるマネジメント指導テーマ	支援実績のある業務（マネジメント指導テーマ以外）	支援実績のある業界	支援地域	支援可能期間	支援可能形態（１回あたりの支援料金） ※●●事業による専門家派遣の場合は初回無料	他資格の保有状況	所属形態
①	AAA	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 ④セキュリティインシデント対応 ⑤従業員向けセキュリティ教育	○○○	製造業 建設業	大阪、奈良、京都、兵庫	スポット、 3か月～半年	訪問コンサルティング（××円） オンラインコンサルティング（●●円） 講習・研修（△△円）	ITコーディネータ 中小企業診断士 CISSP 税理士	個人事業主
②	BBB	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	▼▼▼	自動車産業	奈良、滋賀、京都、三重、岐阜	スポット、 １～３か月、 ３か月～半年、 半年～1年	訪問コンサルティング（××円） オンラインコンサルティング（●●円） 講習・研修（△△円） セキュリティ製品の選定・導入支援（■■円）	ITコーディネータ 公認情報セキュリティ監査人	◇◇株式会社所属
③	CCC	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 ⑤従業員向けセキュリティ教育	□□□	金融業 小売業 卸売業	大阪、奈良、和歌山	スポット、 １年以上	訪問コンサルティング（××円） オンラインコンサルティング（●●円） 講習・研修（△△円）	公認会計士 中小企業診断士	個人事業主

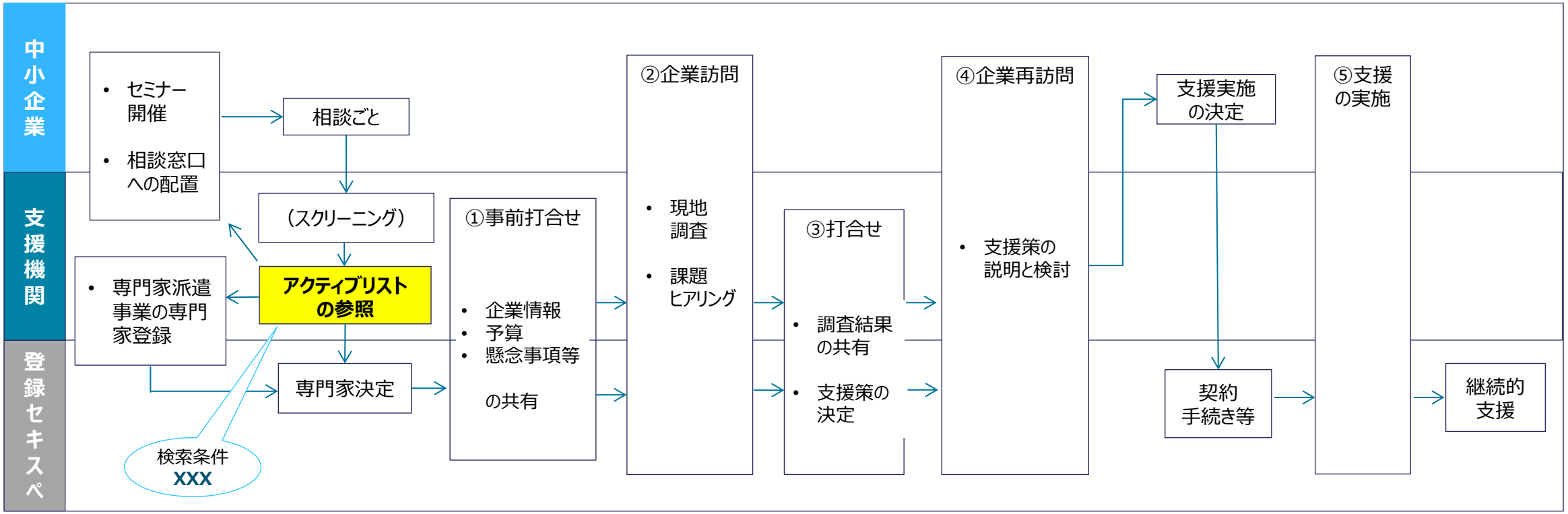
※氏名をクリックすると、専門家の詳細情報（具体的な支援実績、連絡先等）が表示されることを想定。

（参考２）支援機関等におけるアクティブリスト活用シナリオ

活用シナリオ①

（利用者） 中小企業支援機関
（利用目的）中小企業のニーズに合ったセキュリティ対策の実装を支援する登録セキスペを抽出する

登録セキスペが中小企業に対して担う役割	社内ITリソースの補完者としての役割、経営者への説得者としての役割、包括的なセキュリティ戦略の立案と実施者の役割、セキュリティ製品導入後の品質担保者としての役割、効果的なIT投資実現のためのパートナーとしての役割
登録セキスペが支援機関に対して担う役割	支援プログラム実施のための専門的・戦略的パートナーとしての役割
支援機関が中小企業に対して担う役割	中小企業のセキュリティ対策のロードマップ策定、中小企業とセキュリティ専門家・関係者とのネットワーク構築を支援者する役割

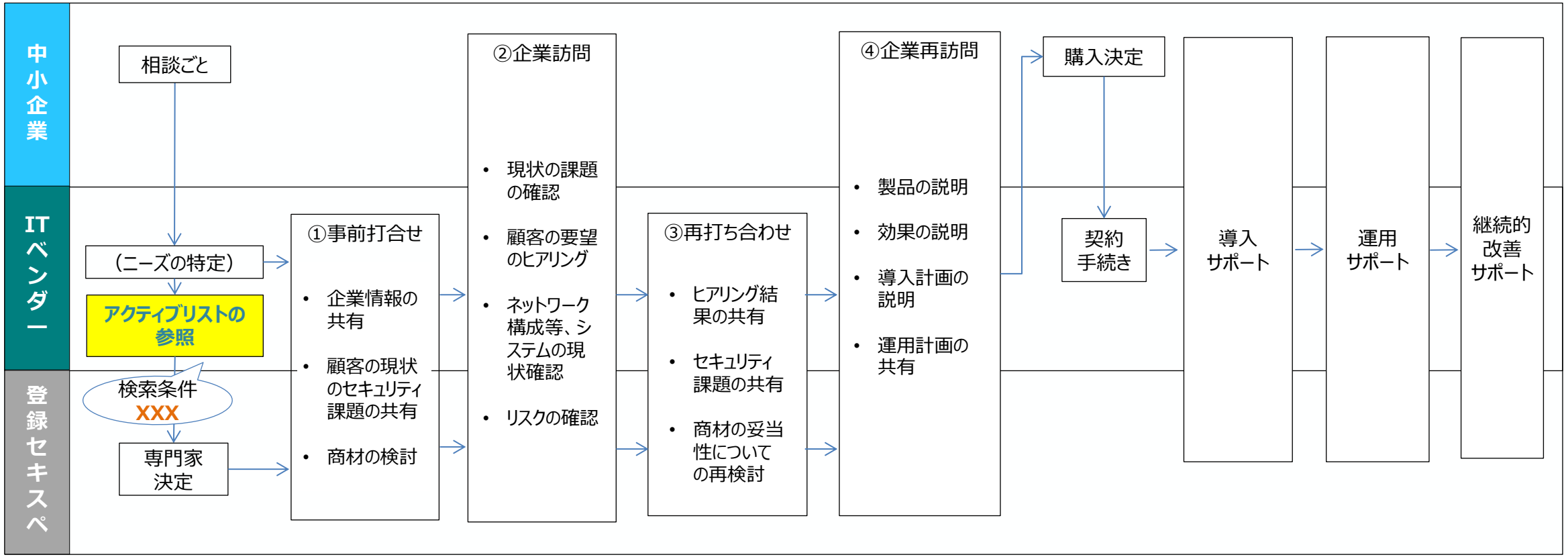


（参考３）支援機関等におけるアクティブリスト活用シナリオ

活用シナリオ②

（利用者）　ITベンダー
（利用目的）顧客の中小企業へセキュリティ商材を導入をサポートする登録セキスペを選定する

登録セキスペが中小企業に対して担う役割	中小企業の立場からのITベンダーからの提案に対する目利き役としての役割、ITベンダーと経営との橋渡し役としての役割、導入後のサポート等を通じた品質の保証者としての役割、効果的なIT投資実現のためのパートナーとしての役割
登録セキスペがITベンダーに対して担う役割	知識・経験の共有者としての役割、経営者との橋渡し役としての役割、品質管理・監督者としての役割

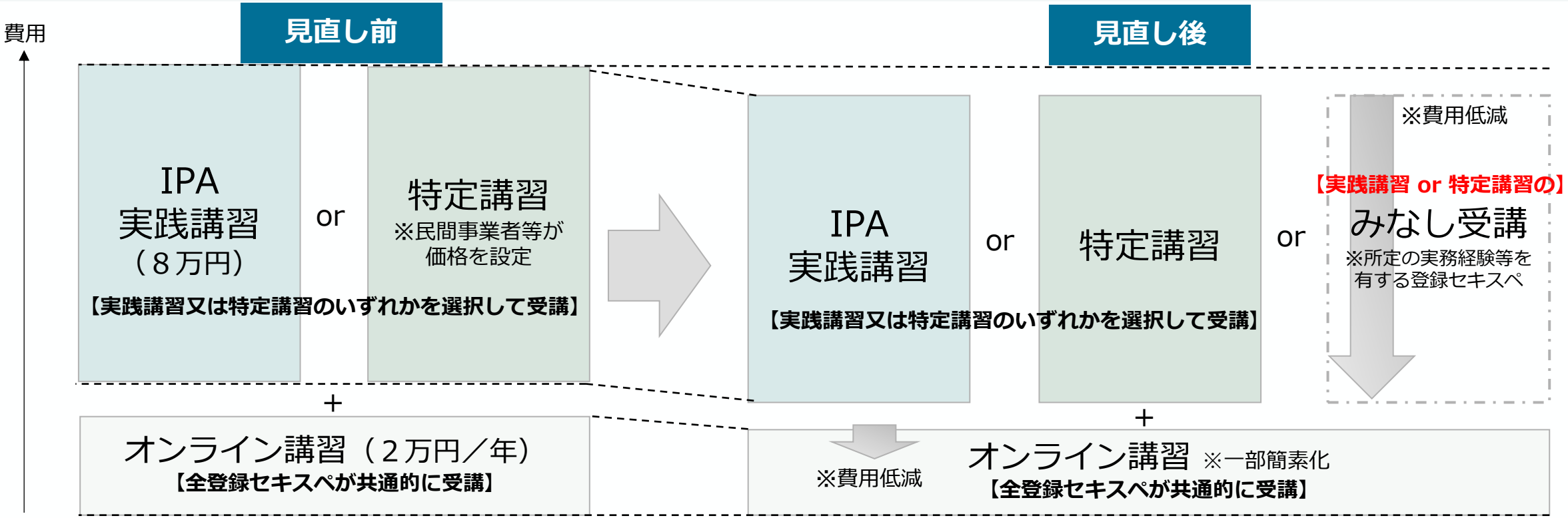


みなし受講制度検討の背景とイメージ

- 更新制導入から４年が経過する中で、登録セキスペの中には、**最新の知識・技能に係る講習と同等以上の内容を有する実務**（相談に応じて情報提供・助言・調査・分析・評価を行いサイバーセキュリティの確保を支援するという法律が定める登録セキスペの業務）**に携わっている者が存在**しており、必ずしも受講義務という形を採らずとも、最新の知識・技能が担保される場合があるものと考えられる。
- 一方で、**実務から遠のいている登録セキスペ**に対しては、更新制度が施行されている中で、**実務に向かわせるインセンティブを設定する**ことが、登録セキスペの一層の活用促進、ひいては事業者のサイバーセキュリティ対策向上につながるものと考えられる。

  ※　更新のための講習費用は合計して少なくとも10万円を超えるものが大半を占めており、登録消除者のアンケートによれば**費用負担が大きいとの意見**がある。

- そこで、登録セキスペの更新に際して、最新の知識や倫理等に関する**最低限の講習受講は引き続き義務**としつつも**一部の講習については所要の実務経験をもって代替し、受講したものとみなす制度を創設**することが考えられる。



（参考）みなし受講制度検討の前提（登録セキスペの業務等）

【登録セキスペの業務】
サイバーセキュリティの確保のための取組に関し、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**を行うとともに、
必要に応じその取組の実施の状況についての**調査、分析及び評価**を行い、その**結果に基づき指導及び助言**を行うことその他**サイバーセキュリティの確保を支援**

【登録セキスペの信頼性の確保】
サイバーセキュリティに関する知識及び技能に関する事項並びに遵守すべき倫理に関する事項を内容とした**法定講習の定期的な受講を義務**付けるとともに、**信用失墜行為の禁止**規定や罰則付きの厳格な**秘密保持義務**を設定

【更新制の導入】
サイバーセキュリティに関する**最新の知識・技能を確実に担保**できるように、登録に３年間の有効期限を設け、**義務講習を受講した者のみ更新**

みなし受講制度の対象とする実務経験の考え方

- みなし受講制度の対象とする実務経験については、講習代替性を充足する必要。
- 講習代替性を検討するに当たっては、①～④を総合的に考慮。

講習代替性

- サイバーセキュリティに関する最新の知識・技能を確実に担保するという法律の趣旨に鑑み、みなし受講制度の対象とする実務経験は、更新時に受講する講習と同等以上の内容・ボリュームを担保するものである必要

①本制度の効果

- 登録セキスペの実務に従事する誘因を設定することで、登録セキスペの一層の活用促進等に効果も期待
- 実践・特定講習の内容と同等以上の内容・ボリュームを有するサイバーセキュリティ関連業務に従事する登録セキスペの講習費用の負担軽減にも資する

②客観的判断

- みなし受講の対象となる実務経験の証跡等を踏まえ、制度の信頼性を確保しつつ、客観的・外形的な判断が可能である必要

③事務負担

- 実効的で持続可能な制度運用が確保されるよう、みなし受講の審査コストを考慮する必要

④その他

- 必要な法令改正も視野に入れて制度設計を行う必要

更新時の義務講習に代替可能な実務経験の水準の担保の考え方（イメージ）

- まず、更新時の義務講習に代替可能な実務経験について検討するため、法令レベルから運用レベルまで整理を行い、義務講習（特定講習）として求める要素を特定。

経済産業省令

- 特定講習（※）は、

ｉ）**支援士試験の科目に係る内容**を行うものとし、特定講習の**総時間は６時間以上**とされるとともに、

ii）半分以上の内容を実習、実技、演習又は発表その他**実践的な方法**により行う

- 上記科目の内容は、情報セキュリティシステムの開発＋（情報処理システム＋関連業務におけるセキュリティ管理）に関する**専門的知識＋専門的能力**

（※）
特定講習の具体的内容は、上記のとおり、経済産業省令に規定されているところ、特定講習は、**機構の講習と同等以上の効果を有すると認められる講習**として経済産業省令で定めるものとされていることから、**機構の講習（実践講習）として求める要素は、特定講習と同様。**

特定講習募集等要領

- 試験科目の内容は、「募集要領」において敷衍されており、具体的には、
  ｉ）**ＩＴスキル標準レベル４相当**（一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の　発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献するレベル）に該当し、

- ii）支援士試験シラバスにおける大項目のいずれかを含むこととされ、具体的には、シラバスの**小項目を複数含む内容**であれば、特定講習として認められる

支援士試験シラバス

- 上記大項目（４項目）が更に詳細化された小項目とその概要等　（必要な指導・助言・支援の内容、要求される知識・技能）を設定

（参考）情報処理安全確保支援士試験シラバスの大項目及び小項目

大項目	小項目	大項目	小項目
１．情報セキュリティマネジメントの推進又は支援に関すること	1-1　情報セキュリティ方針の策定	３．情報及び情報システムの利用におけるセキュリティ対策の適用の推進又は支援に関すること	3-1　暗号利用及び鍵管理
	1-2　情報セキュリティリスクアセスメント		3-2　マルウェア対策
	1-3　情報セキュリティリスク対応		3-3　バックアップ
	1-4　情報セキュリティ諸規程の策定		3-4　セキュリティ監視並びにログの取得及び分析
	1-5　情報セキュリティ監査		3-5　ネットワーク及び機器のセキュリティ管理
	1-6　情報セキュリティに関する動向・事例の収集と分析		3-6　脆弱性への対応
	1-7　関係者とのコミュニケーション		3-7　物理的及び環境的セキュリティ管理
２．情報システムの企画・設計・開発・運用でのセキュリティ確保の推進又は支援に関すること	2-1　企画・要件定義（セキュリティの観点）		3-8　アカウント管理及びアクセス管理
	2-2　製品・サービスのセキュアな導入		3-9　人的管理
	2-3　アーキテクチャの設計（セキュリティの観点）		3-10　サプライチェーンの情報セキュリティの推進
	2-4　セキュリティ機能の設計・実装		3-11　コンプライアンス管理
	2-5　セキュアプログラミング	４．情報セキュリティインシデント管理の推進又は支援に関すること	4-1　情報セキュリティインシデントの管理体制の構築
	2-6　セキュリティテスト		4-2　情報セキュリティ事象の評価
	2-7　運用・保守（セキュリティの観点）		4-3　情報セキュリティインシデントへの対応
	2-8　開発環境のセキュリティ確保		4-4　証拠の収集及び分析

※　特定講習において、網掛けの小項目のみを対象とした講習では十分とは言えないため、他の項目と組み合わせて実施することとされている（募集要項）。

（参考）情報処理安全確保支援士試験シラバスの小項目概要（抄）

大項目	小項目	概　要	要求される知識	要求される技能
1　情報セキュリティマネジメントの推進又は支援に関すること	1-1　情報セキュリティ方針の策定	経営者による情報セキュリティ方針の策定及び改定について，必要な指導・助言を行い，支援する。	・情報セキュリティガバナンス及びITガバナンスに関する知識 ・マネジメントシステム（ISMS，BCMSなど）に関する知識 ・組織マネジメントに関する知識	・組織内外の利害関係者のニーズと期待，組織内の経営戦略，事業戦略によって生じる要求事項を踏まえて情報セキュリティ方針を具体化する能力 ・法令，規制，契約，情報セキュリティに関する動向などによって生じる要求事項を踏まえて情報セキュリティ方針を具体化する能力 ・経営者とコミュニケーションする能力
	1-2　情報セキュリティリスクアセスメント	リスク基準の確立及び維持について，必要な指導・助言を行い，支援する。 リスク特定，リスク分析，リスク評価のプロセスの実施について，必要な指導・助言を行い，支援する。	・情報の特性（機密性，完全性，可用性，真正性，責任追跡性，否認防止，信頼性など）に関する知識 ・リスク，リスク基準，リスク源，脆弱性及び脅威に関する知識 ・情報セキュリティリスクアセスメントのプロセス（特定，分析，評価）に関する知識 ・脅威分析（STRIDE分析，アタックツリー分析（ATA）など）に関する知識	・情報資産損失の大きさ（失われる資産の価値，原因究明及び復旧の費用，社会的説明の費用）を算定し，評価する能力 ・リスク源，脆弱性及び脅威を，新たなITに関するものも含めて列挙する能力 ・情報資産とリスクを関連付けて整理する能力 ・リスクを優先順位付けする能力
	1-3　情報セキュリティリスク対応	情報セキュリティリスクアセスメントの結果に基づく適切な管理策の選定，情報セキュリティリスク対応計画の策定について，必要な指導・助言を行い，支援する。	・リスク対応の選択肢（リスク低減，リスク共有，リスク回避，リスク保有など）に関する知識 ・管理策の実施に要する費用の算定に関する知識 ・サイバー保険に関する知識	・リスクごとに，リスク対応の選択肢を選定する能力 ・リスク対応の実施に適切な管理策を選定する能力 ・情報セキュリティリスク対応計画を作成し，残留リスクと併せて説明する能力
	1-4　情報セキュリティ諸規程の策定	情報セキュリティに関連する諸規程の策定及び改定について，必要な指導・助言を行い，支援する。 事業継続に関する計画の策定及び改定について，必要な指導・助言を行い，支援する。	・法令，規制，規格に関する知識 ・ITの動向（クラウドコンピューティング，仮想化，モバイル，組込みシステム，Web技術，AI（生成AIを含む），ビッグデータ，IoTなど）及びその情報セキュリティへの影響に関する知識 ・事業継続に関する知識	・業務プロセス，業務手順を踏まえた上で，情報セキュリティ諸規程で定めるべき事項を検討する能力 ・検討した事項及びその必要性を説明する能力 ・法令，規制，規格の変化やITの動向を踏まえて情報セキュリティ諸規程をレビューする能力

義務講習に代替可能な実務経験の水準の担保の考え方（イメージ）

- 更新時の義務講習（特定講習）として求める要素を特定後、それに代替可能な（＝みなし受講の対象となる）「実務経験」として求める要素に変換。
- その際には、登録セキスペを、**法定の業務（相談に応じて情報提供・助言／調査・分析・評価を行いサイバーセキュリティの確保を支援するという法律が定める登録セキスペの業務）に向かわせ**、もって**登録セキスペの一層の活用促進・サイバーセキュリティ対策の向上を図る**という**みなし受講制度の政策目的を踏まえて検討。**

義務講習（特定講習）として求める要素	みなし受講の対象となる実務経験として求める要素
• ＩＴスキル標準レベル４相当（一つまたは複数の専門を獲得したプロフェッショナルとして、専門スキルを駆使し、業務上の課題の発見と解決をリードするレベル、プロフェッショナルとして求められる、経験の知識化とその応用（後進育成）に貢献するレベル）	• **支援士試験シラバスの小項目（ＩＴスキル標準レベル４に相当するものとして記載）に該当すること**
• 支援士試験シラバスの小項目に関する業務	• **支援士試験シラバスの小項目に該当するひとかたまりの業務** （左記「６時間以上」は講習の受講時間に関し設定されたものであることを踏まえ、ひとかたまりの業務を実施したかを確認）
• 総時間６時間以上	
• 半分以上の内容を実習、実技、演習又は発表その他実践的な方法	（左記「半分以上が実践的方法」は講習の方法関し設定されたものであることを踏まえ、「実務経験」の要素としては特段の設定を要しないものと整理）

上記のみなし受講制度の政策目的を踏まえ、**「実務経験」は法定の登録セキスペの業務**

ＩＴスキル標準レベル４相当として記載された**支援士試験シラバスの小項目**（シラバスの小分類の概要・要求される知識・技能）**に該当**し、かつ、**同小項目に該当するひとかたまりの業務**について、受講義務の対象講習に代替することを認めることを基本としてはどうか。

更新時の義務講習に代替可能な実務経験の判断手法

- 実務経験が、シラバスの小項目に関する業務（シラバスの小分類の概要及び要求される知識・技能の記載で判断）に該当するものとして、**所属組織（独立系の登録セキスペにあってはその顧客）が、一定の書式の下でこれを証した場合には、みなし受講を認める**ことが相当ではないか。
- **更なる信頼性確保策**として、みなし受講申請書の工夫、申請内容に虚偽がないことの宣誓、サンプル調査の実施等が考えられる。

信頼性確保策の検討例

方策	詳細項目	デメリット・リスク・懸念	実現可能な施策
①シラバス小項目の該当性の判断	対象業務の特定	（具体例を提示する案に対し）例示通りに申請する者が現れる可能性がある	**領域ごとに具体例を示し**、具体例通りの記載は認めないことを明示（cf：建築士の実務経歴証明書）
	レベルの担保	書類審査で知識や技能の深度を見極めることは難しい	**業務内容をITスキル標準レベル４と紐づけ、具体例をもって明示** (cf:技術士試験のように実務経歴証明書の提出を求め、口頭試験を行う方法も考えられるが、リソースと申請期間の問題で非現実的である)
②業務実績を裏付ける証拠資料の提示	証明書	―	• **申請書と申請内容を証明する書類を用意する**（他資格でも必ずセットになっている） • 実施した業務については、**所属組織（独立系であれば顧客）からの証明をもって信頼性を担保**
	業務委託契約書	申請者当人の担当領域が契約内容に織り込まれているケースは稀であり、証拠書類としての機能を果たさない	―
	ログ（GitHub、業務システムの監査ログ、JIRAなど）	証拠書類としての機能は果たしても、申請者当人が実行したかどうかは明確ではないため内容の評価は難しい	―
	成果物や報告書（セキュリティポリシー、監査報告、脆弱性診断など）	機密性の高い情報が多いため対外的に情報を出せないか、仮に出せたとしてもマスキングが必要なため実現可能性が低い	―
	所属長や顧客の署名入りとする	―	（上記「証明書」における記載の通り）
	既存資格保有者によるエンドーズメント	業務内容を正確に評価できる社内や取引先にスペシャリストがいるケースが全てではない	―
	役務提供された側（所属長や顧客）から実施業務の評価や推薦を提示してもらう	申請者当人に見えない形で評価する必要があり、運用上実現可能性が低い	―
③第三者の確認	認証機関の設置（経産省/IPA /支援士会/有識者/既存資格保有者によるエンドーズメント）	• 現行の更新申請期限（更新の60日前）を前提とする場合、いずれの場合であっても、相当のコスト・時間がかかり、期限までの審査が間に合わないリスクが大きい • また、申請者に対しても、早期の申請書提出を強いることになり、申請者の利便性を損なう可能性が高い	―
	ランダムな精査（サンプリングチェック）	―	**申請事案の中からサンプル調査を行う**
④虚偽申告に対するペナルティの導入	罰則規定（資格取り消し、一定期間の業務停止、受験禁止などの措置）	―	経済産業大臣の資格取消権（法第19条第２項）で対応可能
	申請者への宣誓書要求	―	申請書に虚偽の記載がないことの宣誓同意文言の追加

御議論いただきたい事項

【登録セキスペアクティブリストを活用した中小企業支援】

- 実証事業の結果を踏まえたアクティブリストの必要項目の具体化について
- 実証事業の結果を踏まえたマッチング主体・仲介者（支援機関やITベンダー）の役割や中小企業との関わり方を踏まえたアクティブリスト活用方法について
- アクティブリストの広報周知方法について
- アクティブリストの登録・更新方法について
- マネジメント指導を実施することで発生する費用負担について
- アクティブリストの施策インパクトについて

【みなし受講制度】

- 登録セキスペの業務類型（シラバスの小項目）における実務経験、それを達成するために要求される知識・技能の確認手法について

Ⅰ　議論の全体像

Ⅱ　第３回の議論の振り返り

Ⅲ　登録セキスペ
　○登録セキスペアクティブリストを活用した中小企業支援
　○みなし受講制度

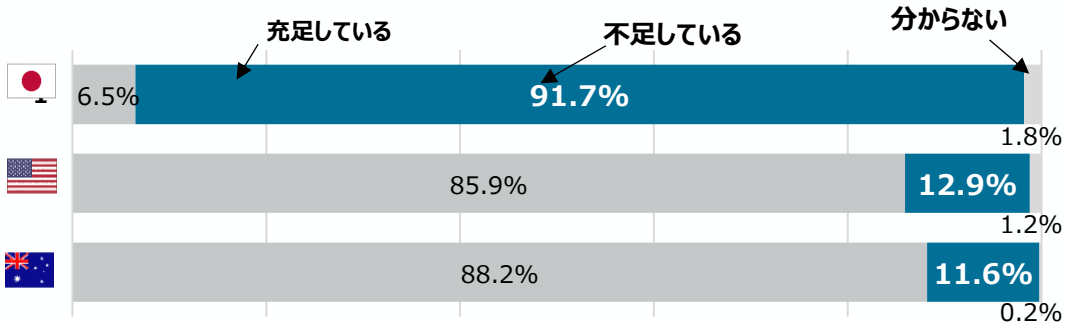
Ⅳ　中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保関係
　○実践的方策ガイドの位置付け等
　○実践的方策ガイドβ版（案）

中堅・中小企業のセキュリティ人材の現状・課題

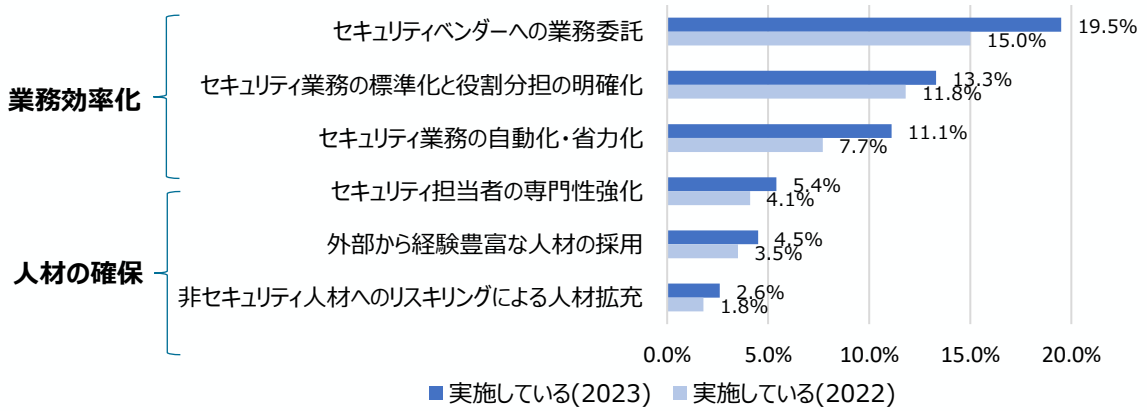
- 民間調査によると、我が国では企業の規模に関わらず、９割の企業がセキュリティ人材が不足していると回答。また、社内のセキュリティ人材不足を補う施策として、人材確保の取組を実施している企業は少ない。
- 経済産業省が実施した企業へのヒアリングでは、社内でのセキュリティ人材の確保と育成が困難であるとの声がある。
- 経済産業省およびIPAでは、企業のセキュリティ人材の確保・育成に資するガイドライン等を策定してきたが、多くの中堅・中小企業においてはセキュリティ人材の確保・育成の取組が実践されていない状況。

→ **中堅・中小企業等の内部でセキュリティ対策を推進する者の育成・確保に向けた施策を検討**

セキュリティ人材の不足状況



セキュリティ人材不足を補う施策の実施状況



企業へのヒアリング結果

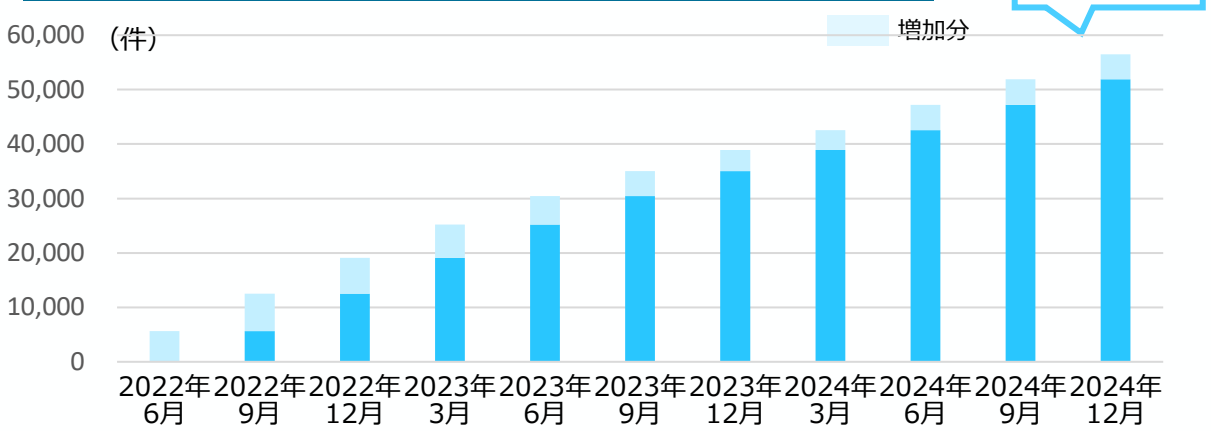
- 社内においてセキュリティの教育をする立場にある人材が不足している。もしくは、知識の偏りがあり内部でのセキュリティ人材育成が困難である。
- 担当者がどのようなスキル・知識をどのレベルで有していることが必要か分からない。適切な外部の研修が、ない/分からない/探すことができない。
- ユーザー側企業においては、広く浅くゼネラリスト的な知識が求められる。ベンダー企業のような高い専門知識は必要とされていない。
- 単に知識だけでなく、現場ではトラブルシューティングなど実践的スキルが重要。実践的スキルの習得には、現場やそれに近い環境で学ぶ必要がある。

出典：NRI セキュア 企業における情報セキュリティ実態調査2023

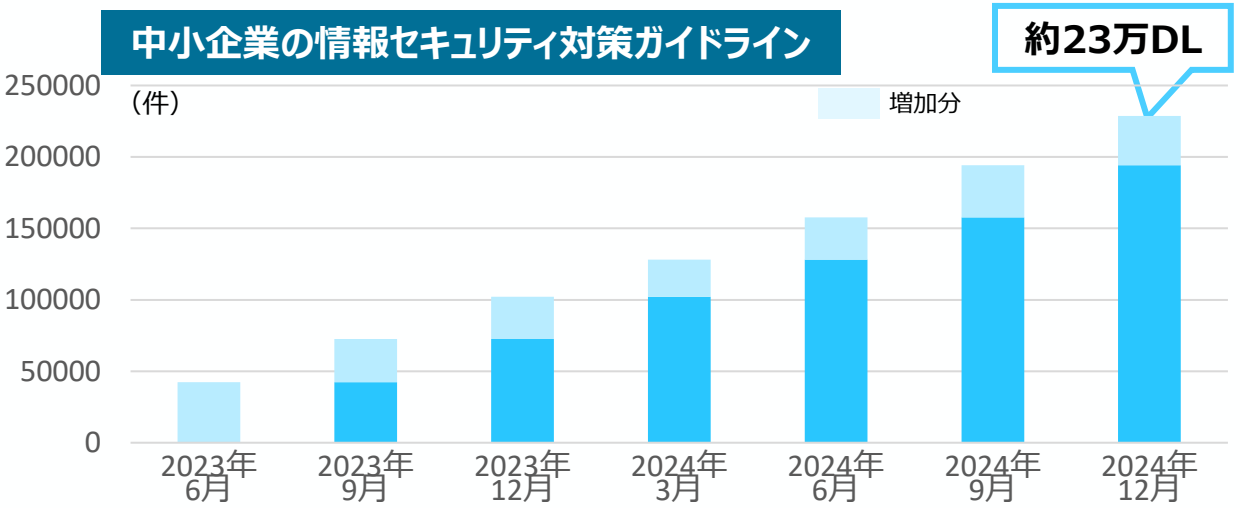
ガイドライン・各種施策の活用状況等

- 2023年6月に改訂した「サイバーセキュリティ体制構築・人材確保の手引き第2版」は、継続して約1,500件/月のダウンロード。中小企業等向け施策である「中小企業の情報セキュリティ対策ガイドライン第3.1版」については約1万件/月のダウンロード。IPAを通じた施策などにより、継続的にサイバーセキュリティ人材の育成、セキュリティ普及活動を実施。
- 中堅・中小企業におけるサイバーセキュリティ人材の確保については、不断の取組が必要。

サイバーセキュリティ体制構築・人材確保の手引き第2版



中小企業の情報セキュリティ対策ガイドライン



人材育成及びセキュリティ関連試験

中核人材育成プログラム修了者数	492名(2017年～2024年)
セキュリティ・キャンプ参加者数	全国大会: 1232名(2004年～) ネクストキャンプ: 53名(2019年～) ジュニアキャンプ：11名(2023年～)
情報処理安全確保支援士	22,845名(2024年10月時点)
登録セキリティマネジメント試験	142,862名(2024年12月時点)

普及啓発活動

IPA　セキュリティ講演者派遣 (2024年度12月末実績)	84件
IPA　セキュリティセミナー支援 (2024年度見込み件数)	セミナー開催支援: 25件 経営イ社向けインシデント机上訓練: 19件

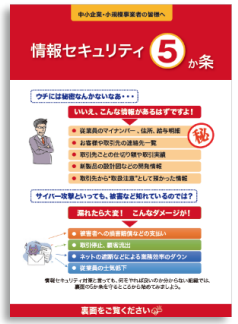
実践的方策ガイドと他施策の連携

- 実践的方策ガイドでは、企業が実施すべきセキュリティ対策を段階的に提示していることから、他のガイドラインやSECURITY ACTION☆1、☆2、検討中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等で示す企業が実施すべきセキュリティ対策と整合性を確保して作成。

１段階目（一つ星）

●情報セキュリティ５か条に取り組む

★一つ星



【情報セキュリテイ５か条】

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

2段階目（二つ星）

●情報セキュリティ自社診断を実施　●基本方針を策定

★★二つ星

【基本方針の記載項目例】

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善

など

<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イメージ>

成熟度の定義	三つ星（★３）	四つ星（★４）	五つ星（★５）
レベル感の説明	サプライチェーン形成企業として最低限満たすべき基準	サプライチェーン形成企業として標準的に満たすべき基準	重要インフラ事業者、経済安全保障上、特に重要なインフラ事業者、関連サプライヤーが満たすべき基準
ガイドラインの相当性を認定	・IPA「中小企業の情報セキュリティ対策ガイドライン」	・○○業界ガイドライン ・・・・	・重要インフラ行動計画 ・・・・
ガイドライン準拠を確認する方法を定義	自己宣言型	第三者認証型	第三者認証型

- 政府調達・補助施策等への要件化
- 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

（出典）第８回 産業サイバーセキュリティ研究会　資料３より抜粋・加工

実践的方策ガイドにおける4つのStep

- 企業が実施するセキュリティ対策を４つのStepに分け、対策の実施に必要なタスク、人材の確保・育成策を提示。

		実施するセキュリティ対策	人材の確保・育成の方策（外部人材の活用）	
（兼任でのみ確保可能）	**Step1「取組の開始」**	**基本的なセキュリティ対策を開始** ・情報セキュリティ5か条の実施	**「兼務であっても、一人はセキュリティ担当者を配置」** ・配置転換、社内公募による人材確保	取組の開始前や取組中において、不明点等を**登録セキスペ等の外部のセキュリティ専門家に相談することも有効**
	Step2「組織的な取組」	**担当者の下で、組織的な取組を開始** ・情報セキュリティに関するルールを規定 ・従業員へのセキュリティルールの周知、注意喚起、教育の検討	**「兼任人材の増員」** ・配置転換、社内公募による兼任人材の増員 ・既存情報、学習コンテンツ、セミナーの活用 ・試験、資格の活用	
（兼任又は専任で確保可能）	**Step3「本格的な取組」**	**セキュリティ体制を構築し、対応すべきリスクに応じたセキュリティ対策を開始** ・平時、有時の対応体制を構築 ・外部専門家(セキスペ等)を活用した資産の洗い出し、リスク分析の実施 ・必要なセキュリティ対策の検討、導入、運用を実施 ・外部委託範囲の適切な決定、契約書・覚書などへのセキュリティ対策の明記	**「自社のセキュリティ体制を構築」** ・専任人材、セキュリティ責任者の任命 ・配置転換、社内公募による兼任人材の増員 ・既存情報、学習コンテンツ、セミナーの活用 ・試験、資格の活用	必要なセキュリティ対策を全て内部人材で実施することは困難であるが、自社で実施する業務と**外部委託が可能な業務**を判断し、適切に**委託先を管理**することが必要
	Step4「継続的な改善より強固な対策」	**より強固なサイバーセキュリティ対策に取り組む** ・システム・ソフトウェアの脆弱性管理 ・インシデントの検知	**「自社のシステムに応じた脆弱性の管理、インシデント対応に必要な人材を確保」** ・セキュリティ対策関連の業務経験を有する人材の中途採用 ・サイバーセキュリティを専門とする教育機関を修了した直後の人材の新卒採用 ・専任の人材による兼任人材への指導 ・教育プログラムの受講	**自社の人材育成、リスクの洗い出し、実施すべき対策の検討等においては、登録セキスペ等の外部のセキュリティ専門家の活用が有効**

（参考）実践的方策ガイドにおける4つのStep

- 「実施するセキュリティ対策」は、「中小企業情報セキュリティガイドライン 3.1版」（IPA・最終更新2024年10月）において示されている４つのstepを参考に整理。

各Stepの概要（p4記載）		活用方法とリンクするセキュリティ対策
Step1 まず始めましょう	**「情報セキュリティ 5か条」を実行**（詳細はp19）	（1）**OSやソフトウェアを最新の状態にする**（2）**ウイルス対策ソフトを導入する** （3）**パスワードを強化する**（4）**共有設定を見直す**（5）**脅威や攻撃の手口を知る**
Step2 現状を知り改善しましょう	「５分でできる！情報セキュリティ自社診断」で**自社の実施状況を把握したうえで、対策の実行**に努める（詳細はp20）	（1）**情報セキュリティ基本方針を作成**（「情報セキュリティ基本方針(サンプル)」を参照） （2）**自社の対策実施状況を把握**（「５分でできる！情報セキュリティ自社診断」を利用） （3）**対策の決定と周知**（「情報セキュリティハンドブック（ひな形）」を参照）
Step3 本格的に取り組みましょう	**自社のリスクに応じた対策規程を作成**、運用後は点検して改善（詳細はp24）	（1）**管理体制の構築**　①責任分担と連絡体制の整備　②緊急時対応体制の整備 （2）DXの推進と**情報セキュリティの予算化** ※自社情報システムについて、インターネットとの接続状況を図にするなどして対策を検討するとともに、予算を確保 （3）**情報セキュリティ規程の作成**　①対応すべきリスクの特定　②対策の決定 ※情報資産管理、アクセス制御及び認証、委託管理、情報セキュリティインシデント対応、事業継続管理対策など （4）**委託時の対策** ※取り扱う情報の種類、委託する業務に適した情報セキュリティ対策を委託先にも実施してもらう 委託先の情報セキュリティ対策が維持されているか、責任をもって管理する
Step4 改善を続けましょう	**より強固な対策を実施** （詳細はp32）	（1）ウェブサイト、クラウド、テレワークの利用等、**自社の状況に応じたセキュリティ対策を実施** （2）**セキュリティサービス、技術的対策の活用（適切な外部委託の活用・管理）** （3）**詳細リスク分析の実施**

御議論いただきたい事項

- 実践的方策ガイドβ版（案）の内容について、内容の過不足、読みやすさ等について議論いただきたい。
- 実践的方策ガイド（β版）をブラッシュアップするために来年度実施予定の調査・実証事業の内容について、御議論いただきたい。
- 実践的方策ガイドを想定読者に届けるための普及策、ガイドの内容を実施するにあたって、必要な支援策について議論いただきたい。

調査・実証事業

β版の使いやすさの確認、向上について

- β版の**見やすさ**、**読みやすさ**、内容が**自社での実施可能か**について、ヒアリング調査
- 企業内でβ版を参照しながら社内人材の確保・育成の取組を実施していただき、課題や考慮点を収集するための実証

事例の収集について

- セキュリティ対策の必要性を訴える事例収集（経営者メッセージの補強）

  → 損害額、事業の停止、サプライチェーンへの影響
- セキュリティ対策の実施事例を収集（実践的方策の補強）

  → 内部セキュリティ人材の確保状況、業務内容、育成方法

普及策の検討

ガイドを目に留めてもらう、手に取ってもらう、読者に届けるための普及について

- 複数の媒体による広報の実施
- 複数の広報手段の活用
- 対象者を絞ったコンテンツの作成
- IPAのセキュリティセミナー教材としての活用

支援策の検討

企業がガイドを実践して人材確保・育成、外部人材の活用できるための支援について

- 既存施策との連携
- 外部人材の探索、活用を支援（補助、支援機関との連携）
- ガイドの内容とリンクした無料学習コンテンツの作成

実践的方策ガイドβ版（案）

１．実践的方策ガイドの目的

企業のサイバーセキュリティ対策を実施するためには、**自社の業務を理解し、対策をリードする人材を組織として確保・育成することが重要**です。

本ガイドは、**これからセキュリティ対策を始める、今後セキュリティ対策を強化していきたい**中堅・中小企業の経営者やサイバーセキュリティ対策の担当者の皆様が、**セキュリティ人材の確保・育成を実践できるようにすることを目的**に、以下の内容をまとめました。

①実施していただきたいセキュリティ対策を段階的に提示

②各段階における社内セキュリティ担当者の役割・業務を提示

③対策を実行するための人材の確保・育成の方策を紹介

本ガイドを活用して、適切なセキュリティ体制の構築、対策の実施に役立てていただければ幸いです。

2. 本ガイドにおけるStepの全体像

本ガイドでは、皆様に実施していただきたいセキュリティ対策を段階的に4つのStepに分けています。
さらに、各Stepにおいて、**「実施するセキュリティ対策」**から**「対策実施のためのタスク」**、**「人材の確保・育成策」**に至るまでを提示しています。
自社の状況に応じたStepから、対策実施のためのタスクや人材確保・育成策を参考に取組を進めてください。

４つのStepを提示

Step1	Step2	Step3	Step4
取組の開始	組織的な取組	本格的な取組	継続的な改善 より強固な対策
兼務の担当者を一人確保	兼務の担当者を増員	専任担当者の確保 兼任担当者の増員	必要な人材・体制の 見直しと確保

Step1の取組は、規模や業種に関わらず、全ての企業が実施しましょう。

各Stepごとに取組を提示

実施するセキュリティ対策 → 対策実施のためのタスク → 人材の確保・育成策

サイバーセキュリティお助け隊サービス https://www.ipa.go.jp/jinzai/riss/index.html

取組の開始前や各Stepの取組と合わせて、中小企業のサイバーセキュリティ対策に不可欠な各種サービス（見守り、駆付け、保険）をワンパッケージで安価に提供する、国が認定したセキュリティサービスである**「サイバーセキュリティお助け隊サービス」**の導入が有効です。

情報処理安全確保支援士（登録セキスペ） https://www.ipa.go.jp/security/otasuketai-pr/

セキュリティに係る専門的な知識、技能を備えた国家資格である**情報処理安全確保支援士（登録セキスペ）**への相談も有効です。サイバーセキュリティに関する相談に応じて、企業の取組に対して分析や評価を行い、その結果に基づいて指導・助言を行います。

3. 経営者の皆様へ

セキュリティ対策を疎かにしたためにシステム障害が発生した場合、**自社の事業活動が停止するおそれ**があります。

また、情報漏えいが発生した場合は、**顧客や取引先からの信用失墜**につながります。

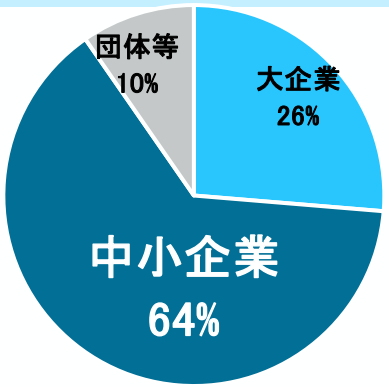
さらに、事業活動の停止は、自社が不利益を被るだけでなく、**自社が属するサプライチェーン全体にも広く影響を与えかねない**ものです。

このように、企業にとって、**セキュリティ対策に取り組むことは必要不可欠であり、社会的な責務です。**経営者の皆様も必要な知識を身に付け、そのリーダーシップで、サイバーセキュリティ対策を進めてくださるようお願いします。**対策を進めるにあたっては、自社の事業を理解してセキュリティ対策を推進したり、いざと言うときにすぐに対応する自社の担当者が必要不可欠**です。また、適切に外部人材を活用することも重要です。

「あなたの対策が、自社や取引の安全を守る第一歩です！」

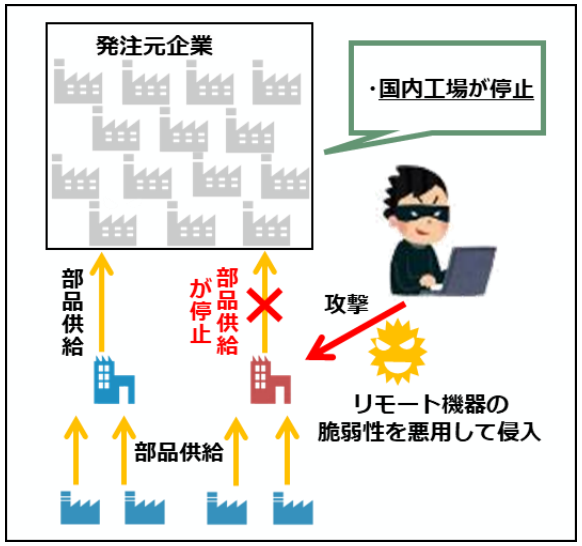
６割の中小企業が
サイバー攻撃の被害に！

ランサムウェア被害企業等の規模別割合



警察庁：「令和6年上半期におけるサイバー空間をめぐる脅威の情勢等について」に基づき作成

被害は取引先にまで影響



4. 段階的な取組 Step 1 取組の開始 1/2

全ての企業が実施すべき基本的なセキュリティ対策に取り組み、自社の業務・情報・従業員・取引先を守る土台を作りましょう。

実施するセキュリティ対策のポイント

基本的な対策を実施しましょう

（情報セキュリティ5か条(1)の実施）

①利用するパソコン等への対策

・OSやソフトウェアの最新化　・ウイルス対策ソフトの導入

対策を実施する対象機器を把握しましょう。

定期的なチェックをしましょう。

②従業員が理解、実施する対策

・パスワードの強化　・攻撃の手口を知る

長く複雑なパスワードを設定し、パスワードを使いまわさない。

不審メール、不正サイトやランサムウェア、攻撃の手口を知りましょう。

③利用するシステムへの対策

・共有設定の見直し

個人情報や企業秘密は正規の必要な人のみアクセスできるようにしましょう。

対策実施のためのタスク

内部人材のタスク

①OSやソフトウェア、NW機器更新のための活動

→ 保有機器を確認し、自動更新設定がある場合は実施します。OS等の更新において従業員の作業が必要な場合は、実施マニュアルを作成し、周知します。

②従業員に対策を周知し、継続してもらうための活動

→ 情報セキュリティ5か条の内容を朝礼や社内メール等によって従業員に周知します。従業員の作業が必要な場合は、実施マニュアルを作成し、周知します。

→ 社内のセキュリティ相談、報告の窓口として対応します。

③利用サービス、NW機器等に適切な設定をする活動

→ 保有するデータやサービス、アカウント等を社内の誰が利用可能か明らかにし、必要に応じてITベンダーと相談して、適切な設定を実施します。

④上記の活動に必要なIT知識を身に付けるための活動

→ 既存コンテンツ活用、資格取得に向けた学習等を実施します。

基本的な取組事項である**情報セキュリティ5か条については、自社において理解のうえ対応することが原則**ですが、外部人材の支援を要する場合、例えば以下のような活用が考えられます。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する助言

→ セキュリティ対策の必要性の理解を助け、情報セキュリティ5か条の実施に必要な助言をします。

②従業員向け教育の提案、実施対応

→ 情報セキュリティ5か条を全従業員で実践するために必要な、セキュリティ担当者への教育、全従業員への講演等を提案・実施します。

※セキュリティ関連タスクに応じた、外部委託の判断基準について、詳しくは「サイバーセキュリティ体制構築・人材確保の手引き(2)」(以下、人材手引き)p20に記載があります。

(1)情報セキュリティ5か条:https://www.ipa.go.jp/security/security-action/download/5point_poster.pdf

(2)サイバーセキュリティ体制構築・人材確保の手引き:https://www.meti.go.jp/policy/netsecurity/tebikihontai2.pdf

Step1　取組の開始 2/2

○基本的なセキュリティ対策を実施するためには、兼務でも社内に１人はセキュリティ担当者を確保しましょう。
○内部だけで実施が難しい対策については、外部の人材・リソースに相談しましょう。
○基本的な映像コンテンツを活用したり、基本的な資格試験へのチャレンジを促しましょう。

確保

社内人材

○情報セキュリティ5か条を実践するために、セキュリティ担当者を兼務でも１人は確保しましょう。

＜**配置転換**＞（人材手引きp25）
○セキュリティの知見がある従業員がいなくても、少しでも関連業務の経験がある者をセキュリティ担当を兼務させます。
・災害対策等を行う部署　・IT部門　・監督者　・PC導入担当

＜**希望者の登用**＞
セキュリティ業務の実施を希望する従業員の社内公募を実施し、セキュリティ担当者を兼務させます。
※自社の事業特性から、高いセキュリティレベルが求められる場合は、外部からの専門人材の採用を検討します。

外部人材の活用

○既にパスがある（付き合いがある）ITベンダーや、商工会・商工会議所等の支援機関と、自社のセキュリティについてコミュニケーションを取り、情報セキュリティ5か条の実施に関する課題、従業員への周知方法、教育方法について相談します。

○IPA情報セキュリティ安心窓口(3)を活用し、セキュリティに関する不安や課題を相談します。

※相談に当たっての注意点
相談ポイントが分からない場合もあるかもしれませんが、例えば「データの漏洩が心配」「従業員の教育が不十分ではないか」「ニュースで聞いたランサムウェア攻撃、自社は大丈夫か」など身近なところから課題を挙げてみましょう。
相談の際には、自社の業種・規模、実施中のセキュリティ対策について簡単に説明することで、より具体的なアドバイスを受けやすくなります。

育成

既存情報、学習コンテンツ、セミナーの活用

○IPA映像コンテンツ(4)の視聴
情報セキュリティ5か条説明：https://www.youtube.com/watch?v=OP7O12w6KnQ
ランサムウェア攻撃の説明：https://www.youtube.com/watch?v=TWqJ5P8oaUM
メール詐欺の説明：https://www.youtube.com/watch?v=6DKJEG3woRU
パスワード強化：https://www.ipa.go.jp/security/chocotto/index.html
○デジタル知識・スキルが学べるデジタル人材育成プラットフォームであるマナビDX(5)のリテラシー講座の受講
○1テーマ5分で情報セキュリティについて勉強できる無料の学習コンテンツIPA5分でできる！情報セキュリティポイント学習(6)による学習

試験、資格の活用

○情報セキュリティを含むIT全般の基本的知識に関する試験「ITパスポート試験(7)」を取得を促し、IT知識を習得。(人材手引きP38)

(3) IPA情報セキュリティ相談窓口：https://www.ipa.go.jp/security/anshin/index.html
(4) IPA映像コンテンツ一覧:https://www.ipa.go.jp/security/videos/list.html
(5)マナビDX：https://manabi-dx.ipa.go.jp/
(6) IPA5分でできる！情報セキュリティポイント学習：https://www.ipa.go.jp/security/sec-tools/5mins_point.html
(7) ITパスポート試験：https://www3.jitec.ipa.go.jp/JitesCbt/index.html

Step2　組織的な取組 1/2

組織的な対策をはじめます。自社の情報セキュリティ基本方針を作成し従業員へ周知しましょう。
また、自社のセキュリティ対策の実施状況を把握し、対策を決定し周知しましょう。

実施するセキュリティ対策のポイント

組織的な取組を開始しましょう

①従業員の指針となる情報セキュリティ基本方針の作成

管理体制の整備、法令・ガイドライン等の遵守、セキュリティ対策の実施など、組織の基本方針を決定し従業員や顧客などの関係者に周知します。

②組織の実施状況の把握

自社が、現在どの程度情報セキュリティ対策を実施できているかを把握します。

③対策の決定と周知

USB等の記録媒体の保管、インターネット利用等に関する従業員としての対策、従業員への教育の実施、緊急時の体制整備など組織としての対策を決定し、周知します。

対策実施のためのタスク

セキュリティ基本方針は自社自身が策定する必要があります。
ただし、方針の内容に関する助言を受けたり従業員への社内教育を実施するためには、外部人材の活用が有効です。

内部人材のタスク

①基本方針を検討、策定する活動

→　「情報セキュリティ基本方針（サンプル）(8)」を参考にして、事業の特徴や顧客の期待などを考慮し、自社に適した基本方針を作成します。

②自社組織のセキュリティ対策の状況を把握する活動

→　「５分でできる！情報セキュリティ自社診断(9)」を利用して、自社のセキュリティ対策の実施状況を把握します。

③自社の対策を決定し、従業員に周知する活動

→　②の診断結果と「５分でできる！情報セキュリティ自社診断」の解説編を参考に、自社で実施すべき対策を決定し、従業員に周知します。

④上記の活動に必要なIT知識を身に付けるための活動

→　既存コンテンツ活用して、資格取得に向けた学習等を実施します。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する課題相談対応

→　企業の事業特性に合わせた情報セキュリティ基本方針について提案します。

→　企業に応じて実施すべきセキュリティ対策を提案します。

②従業員向け教育の提案・実施

→　組織的な対策実施のために必要なセキュリティ担当者への教育、従業員への講習等を提案・実施します。

(8)情報セキュリティ基本方針（サンプル）：https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000108033.pptx

(9) 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/ug65p90000019cbk-att/000055848.pdf

Step2　組織的な取組 2/2

○組織的なセキュリティ対策を実施するために、兼務のセキュリティ担当者を複数確保し、育成しましょう。
○従業員への教育や講習について、外部の人材やリソースを活用しましょう。
○社内の役割に応じた映像コンテンツを視聴したり、少し上位の資格へのチャレンジを促しましょう。

確保

社内人材

○社内ルールを作り、社員に守らせるなど業務量が増えることに応じて、担当者も増やす必要が出てきます。

○そのため、Step1で示した隣接分野での業務経験を有する人材の**＜配置転換＞**、**＜希望者の登用＞**を引き続き実施します。

※自社の事業特性から、高いセキュリティレベルが求められる場合は、外部からの専門人材の採用を検討します。

外部人材の活用

○既にパスがあるITベンダーや、商工会・商工会議所等の支援機関などに、組織的なセキュリティの取組、社内の情報セキュリティ基本方針の作成等について相談します。

○IPAセキュリティプレゼンター(10)を活用し、従業員へのセキュリティ教育や講習が実施可能な人材を確保します。

○セキュリティに関する身近なコミュニティ(*)に参画し、交流・情報収集を行うことで、外部人材の活用の幅が広がる可能性があります。

＊地域SECUNITY
地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティであり、イベントの継続開催による意識向上や人材育成、国や専門家からの情報提供の場となります。詳しくは地域SECUNITY(11)をご覧ください。

育成

既存情報、学習コンテンツ、セミナーの活用

○所属、役職に適したIPA映像コンテンツの視聴
経営者向け動画：https://www.youtube.com/watch?v=qlcIBHlUKd0
全従業員向け啓発動画：https://www.youtube.com/watch?v=5K9U0-ASQM8
新入社員向け啓発動画：https://www.youtube.com/watch?v=FljLaQA-cRU
○IPAセキュリティプレゼンターによる社内セミナー聴講
○マナビDXのセキュリティ関連講座の受講
○IPA重要なセキュリティ情報(12)を確認し、危険性が高い最新のセキュリティ上の問題と対策情報の収集

試験、資格の活用

○組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定する試験である「情報セキュリティマネジメント試験(13)」の資格取得を促し、IT知識を習得。(人材手引きP38)

コミュニティへの参加

○セキュリティに関する地域のコミュニティに参加し、他社担当者からの情報収集、意見交換を実施

(10) IPAセキュリティプレゼンター:https://www.ipa.go.jp/security/sme/presenter/index.html
(11)地域SECUNITY:https://www.meti.go.jp/policy/netsecurity/secunity.html
(12)重要なセキュリティ情報:https://www.ipa.go.jp/security/security-alert/index.html
(13)情報セキュリティマネジメント試験:https://www.ipa.go.jp/shiken/kubun/sg/about.html

Step3　本格的な取組 1/2

本格的なセキュリティ対策をはじめましょう。自社体制の整備、対応すべきリスク(事故が発生したとき事業へ損害を与える危険性)を特定したうえで、適切な対策を記述した情報セキュリティ規程を作成し、実行しましょう。

実施するセキュリティ対策のポイント

組織的な取組を開始しましょう

①管理体制の構築

情報セキュリティ 基本方針を実践し、情報セキュリティ対策を推進する体制として「責任分担と連絡体制の整備」、「緊急時対応体制の整備」をします。

②予算の確保

情報セキュリティ対策の実施に必要な予算を確保します。

③情報セキュリティ規程の作成

「対応すべきリスクの特定」、「対策の決定」をし、自社に適した対策を記述した文書（情報セキュリティ規定）を作成しましょう。規程には、以下の項目が想定されます。

- **情報資産管理**：情報資産の管理や持ち出し方法、バックアップ、破棄などの ルールを定めます。
- **アクセス制御及び認証**：情報資産に対するアクセス制御方針や認証のルールを定めます。
- **委託管理**：業務委託にあたっての選定や契約、評価のルールを定めます。
- **セキュリティインシデント対応、事業継続管理**：情報セキュリティに関する事故対応や事業継続管理などの ルールを定めます。

④点検と改善

計画した情報セキュリティ対策が実行されているか、見落としがないか、確認をしましょう。

対策実施のためのタスク

自社体制の決定、予算確保は経営判断であり、自社自身が決める必要があります。
ただし、専門性の求められるシステム保守(ユーザー権限管理等は自社で実施)、自社規定に沿った対策のうち、内部人材で実施困難なタスクは外部委託が有効です。

内部人材のタスク

①自社のセキュリティ体制を検討、整備する活動

→　「情報セキュリティ責任者」、「教育責任者」、「点検責任者」等の役職の役割と責任を決め、緊急時の連絡体制を整備します。

→　朝礼や社内メール、掲示板等を活用し、従業員に周知します。

②対策に必要な予算を検討し、確保する活動

→　外部専門家やITベンダーを活用し、必要な対策と予算額を検討し、社内で理解を得て予算を確保します。

③情報セキュリティ規程の内容を作成し周知する活動

→　「情報セキュリティ関連規程（サンプル）(14)」を参考に、自社に適した規定を作成します。

④セキュリティ対策の実効性を確保する活動

→　社内確認テストや簡易的な社内監査を実施し、計画したセキュリティ対策を実行されているか、改善点がないかを確認します。

⑤上記の活動に必要なIT知識を身に付けるための活動

→　既存コンテンツを活用し、資格取得に向けた学習等を実施します。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する課題相談対応

→　体制構築、情報資産管理、リスクを特定した上で必要なセキュリティ対策の検討、インシデント発生時の訓練企画などに関して支援を実施します。

②従業員向け教育の提案、実施対応

→　所属、役職に応じた教育計画の提案と実施をします。

③専門性が求められるタスクの実施

→　決定した対策を実現させるためのシステムや機器への設定変更、システム保守等を実施します。

(14)情報セキュリティ関連規定（サンプル）:https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055794.docx

Step3　本格的な取組 2/2

○本格的なセキュリティ対策を実施するために、専任のセキュリティ担当者を確保・育成しましょう。
○特に技術的・専門的な対策については、社内のリテラシーを高めつつ外部の専門家やサービスを活用しましょう。
○インシデント対応に関する映像コンテンツや、高度な研修プログラムへの参加も視野に入ります。

確保

社内人材

○社内に適切な体制を確保するとともに、セキュリティ対策業務に関して知識と経験を持つ人材の確保が必要です。

○Step1で示した隣接分野での業務経験を有する人材の**＜配置転換＞**、**＜希望者の登用＞**を引き続き実施し体制を構築します。

＜人材の採用＞
○他社等でサイバーセキュリティ対策業務に従事した経験を有する人材を中途採用し、自社で活用します。（手引きp25）

外部人材の活用

○情報セキュリティ規程の策定や周知、改善に関して、支援機関等への相談を実施します。
また、ITベンダーに情報セキュリティ規程に沿った必要な対策の実施について相談します。

○外部のセキュリティ専門家の支援を活用し、自社の対策を分析・評価・助言できる人材を確保しコンサルティングを依頼します。

○外部のセキュリティ専門家の支援を活用し、インシデント時の対応や事業継続管理などのルールの策定、訓練等を実施します。

○適切な異常監視、インシデント対応を実施するために、外部のセキュリティサービスを導入します。

育成

既存情報、学習コンテンツ、セミナーの活用

○IPA映像コンテンツの視聴
情報セキュリティ規程作成、運用手順：https://www.youtube.com/watch?v=fot-PEzBZO4
セキュリティインシデント、対応：https://www.youtube.com/playlist?list=PLi57U_f9scILiLjIAlRzTjFOdLto9q78o

○IPA産業サイバーセキュリティセンター(ICSCoE)短期プログラム(15)の受講
責任者向け講習：https://www.ipa.go.jp/jinzai/ics/short-pgm/cyberspex/index.html

試験、資格の活用

○情報システムに係るリスクを分析し、コントロールを検証・評価することによって、組織体の目標達成に寄与し、利害関係者に対する説明責任を果たす監査人や情報システム責任者向けの「システム監査技術者試験(16)」の資格を習得。

(15)ICSCoE短期プログラム：https://www.ipa.go.jp/jinzai/ics/short-pgm/index.html

(16)システム監査技術者試験：https://www.ipa.go.jp/shiken/kubun/au.html

Step4　継続的な改善、より強固な対策 1/2

より強固なセキュリティ対策のためには、人的・組織的な対策だけでなく、技術的な対策の強化・外部の専門セキュリティサービスの活用が必要です。

実施するセキュリティ対策のポイント

組織的な取組を開始しましょう

①利用システムに応じたセキュリティ対策の実施

ウェブサイト、クラウドサービス、テレワーク等、自社が利用するシステム、ソフトウェアに応じたセキュリティ対策を実施しましょう。

②セキュリティサービスの活用、技術的対策の実施

セキュリティ監視、運用などのセキュリティサービスと、セキュリティ機器の設置や対策ソフトなどの技術的対策を自社の環境に合わせて活用しましょう。

③セキュリティインシデント対応の強化

「検知・初動対応」、「報告・公表」、「復旧・再発防止」の3つの段階に分けて、事業継続、早期復旧のために備えましょう。

④詳細なリスク分析の実施

自社が保有する「**情報資産の洗い出し**」→情報資産の重要度と被害の発生可能性を考慮した「**リスク値の算定**」→リスク値の大きいものから、リスクの低減や回避を実現するための「**情報セキュリティ対策の決定**」の手順で、もれなくリスクを特定し対策を検討します。

対策実施のためのタスク

専門性が求められるセキュリティサービスや技術的対策の導入・運用に当たり、必要性の判断、委託仕様の策定を自社で行い、外部委託を活用します。

ただし、セキュリティ対策実施の外部委託先の管理は、自社自身で実施する必要があります。

内部人材のタスク

①自社特性に応じた対策を検討し、外部委託を適切に活用、管理する活動

→　自社の利用するシステム、事業特性に応じたセキュリティ対策を検討し、外部委託を活用してセキュリティサービス、技術的対策に関する情報収集、導入を実施します。

→　インシデント発生を想定し、事業継続の観点から被害の最小化、早期復旧のための備えについて、外部委託を活用して検討、実施します。

→　リスク値の算定やリスクの低減には、外部委託を活用して、脆弱性診断の実施やセキュリティ監視サービスを利用します。

外部人材のタスク

(企業からの依頼に応じて対応)

①企業のセキュリティに関する課題相談対応

→　より強固な対策として、セキュリティサービス、技術的対策に関する提案・導入・運用、適切なインシデント対応体制の整備支援を実施します。

②従業員向け教育の提案、実施対応

→　インシデント発生を想定した社内教育、導入されているセキュリティサービスを従業員が適切に利用できるように教育を実施します。

→

③高い専門知識を必要とするリスク分析の実施

→　情報資産ごとの重要度の算定、リスク脆弱性診断、セキュリティ監視・運用、情報収集、詳細なリスク分析支援などを実施します。

Step4　継続的な改善、より強固な対策 2/2

○より強固なセキュリティ対策を実施するために、新規採用や専門家の役員招聘も視野に入ります。
○技術的対策の相談に加えて、定期的な外部監査の活用や社外の情報共有の枠組みへの参画も視野に入ります。
○専門性を高めるための映像コンテンツの活用や、高度な資格へのチャレンジも促しましょう。

確保

社内人材

○より強固な対策のために、自社の事業を理解し、現状のセキュリティ対策の実効性確保・改善、脆弱性への迅速な対応、新たな対策の検討・実施などが必要です。
○このため、一層高い知識・経験・技能を持った人材を確保し、体制を整備する必要があります。Step3までで示した確保策に加えて、次の取組を実施します。

＜人材の採用＞

○サイバーセキュリティを専門とする教育機関を修了した直後の人材の新卒採用（手引きp25）
○セキュリティ専門家を招聘して、CISO等に任命します。（手引きp20）

外部人材の活用

○ITベンダーに対して、自社の実施している対策、保有するウェブサイト、クラウドサービス、テレワークの利用状況、事業特性などに合わせた追加のセキュリティサービス、技術的対策の必要性について相談します。○法令等遵守対応の為、弁護士等の助言を得るための契約をします。（手引きp20）

○監査には、内部監査(第一者)、外部監査（第二者・第三者）がありますが、営業秘密や個人情報等の特に十分な対策が必要な場合には、外部からのセキュリティ監査を実施する第三者を探します。

○取引先や同業者を経由したサイバー攻撃も増えていることから、日本シーサート協議会(17)や同業界の事業者同士でサイバーセキュリティに関する情報の共有・分析などを行う組織である、ISAC(*)などの情報共有の仕組みを活用します。

育成

既存情報、学習コンテンツ、セミナーの活用

○IPA映像コンテンツの視聴
脆弱性発見手法：https://www.youtube.com/playlist?list=PLi57U_f9scIInRwz4QUipc3d3nL_MicfR
テレワークセキュリティ：https://www.youtube.com/watch?v=zDs88SLymwo
安全なウェブサイト運用：https://www.youtube.com/playlist?list=PLi57U_f9scIJv-3QIRu5Hc2Bz4-D4-Apa

○脆弱性の概要や対策方法等の知識を実習形式で体系的に学べるツール脆弱性体験学習ツール AppGoat(18)による学習

試験、資格の活用

○サイバーセキュリティ対策を推進する人材の国家資格である、情報処理安全確保支援士（登録セキスペ）の資格取得。

コミュニティへの参加

○セキュリティに関する地域のコミュニティに参加し、他社担当者からの情報収集、意見交換を実施
○業界内での情報共有・連携の取り組み推進を図る組織である業界ISACや日本シーサート協議会への参加により情報収集を実施

(17)日本シーサート協議会：https://www.nca.gr.jp/
(18) 脆弱性学習ツールAppGoat：https://www.ipa.go.jp/security/vuln/appgoat/index.html

本ガイドで使用している主な用語の説明

アクセス制御

ユーザ認証とアクセス認可の2段階からなり、利用者や情報機器がデータなどにアクセスすることができる権限や認可を制御する技術です。

監査

組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、 監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのことです。監査には、内部監査（第一者）又は外部監査（第二者・第三者）があります。

クラウドサービス

サーバー等を自前で所有する代わりに、インターネット経由で同様の機能を提供するものをいいます。レンタルサーバー、SaaS(Software as a service)、ASP(Application Service Provider)などがクラウドサービスの一種です。

CISO（Chief Information Security Officer）

経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のことです。

情報資産

様々な「情報」のうち、企業として管理すべき対象として選択されたもの。また、情報システムなども「情報資産」に含める場合があります。

脆弱性

ソフトウェア等における、管理者の意図しない動作やイベントにつながる可能性のあるセキュリティ上の弱点のことです。

セキュリティインシデント（対応）

セキュリティの事故・出来事のことで、単に「インシデント」という事もあります。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象等がインシデントに該当します。インシデント対応には、「検知・初動対応」「報告・公表」「復旧・再発防止の」3つの基本ステップがあります。

ファームウェア

ハードウェア(スマートフォンや家電、ルーターなどのネットワーク機器)を制御するソフトのことです。

リスク分析

リスクの特質を理解し、リスクレベル(ある事象の結果とその起こりやすさとの組合せとして表現されるリスクの大きさ)を決定するプロセスのこと。

セキュリティ監視

組織のITシステムやネットワークを常時モニタリングし、セキュリティ上の脅威を検知・対処するための取り組みのことです。 不審な動きを検知し、被害を未然に防ぎます。

サイバーセキュリティ経営ガイド付録E　用語の定義： https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
中小企業のためのセキュリティインシデント対応の手引き： https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf