令和 7 年度セキュリティ人材活用促進実証に係る業務
実施報告書

2026 年 4 月

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目次

1. 概要

本実施報告書は、「令和 7 年度セキュリティ人材活用環境整備に係る業務」（以下、「本事業」という）の実施結果をまとめたものである。

本事業の背景・目的は以下のとおりである。

近年、大企業を標的としたサイバー攻撃のみならず、サプライチェーン全体の中で対策が相対的に遅れている中小企業を対象とするサイバー攻撃により、中小企業自身及びその取引先である大企業等への被害が顕在化している。一方で、日本企業の約 9 割がセキュリティ人材不足を認識しているという報告がある中、予算や人材が不足している中小企業においては特に、社内外を問わず、セキュリティ対策を適切に助言・判断・評価等ができる人材の育成等が必要となっている。

このような背景のもと、独立行政法人情報処理推進機構（以下、「IPA」という）では、令和 6 年度において、高度なセキュリティ知識を有する専門家である情報処理安全確保支援士（以下、「登録セキスペ」という）と中小企業とのマッチングを促す場を構築する実証として「令和 6 年度セキュリティ人材活用促進実証に係る業務（以下、「令和 6 年度事業」という）」を行い、商工会議所等の中小企業支援機関（以下、「支援機関」という）と連携したサイバーセキュリティ相談会の開催、セキュリティマネジメント指導（テーマ別）の実施等から、中小企業向けセキュリティ支援に係るニーズと課題を把握した。また、中小企業がセキュリティ専門家を探索しやすくするための、登録セキスペが実施可能な業務やスキル等を見える化した「登録セキスペアクティブリスト（試作版）」を作成した。

これらを踏まえて令和 7 年度においては、外部のセキュリティ専門家を活用した、中小企業のセキュリティ人材不足を補完する仕組みの構築に資することを目標に、この「登録セキスペアクティブリスト（試作版）」の内容改善を行い、中小企業向けサイバーセキュリティ対策支援者リスト（以下、「セキュリティ対策支援者リスト」という）とした上で、中小企業及び支援機関等でのリスト活用促進と、登録セキスペのリストへの登録促進の両面からリスト整備を行い、併せて、リストの掲載・運用方法（案）を作成した。また、令和 6 年度事業では、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相談が多くあったことから、セキュリティ対策支援者リストの掲載項目の一つであるセキュリティマネジメント指導のテーマを、「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」[1]（以下「SCS 評価制度」という）の検討事項をもとに拡充した上で、研修等により登録セキスペに情報セキュリティ監査スキルを習得させ、中小企業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）を行える人材を育成する実証を行った。

[1]「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

2. セキュリティ対策支援者リストの活用促進

令和 6 年度事業で作成した「登録セキスペアクティブリスト（試作版）」は、セキュリティ対策支援者リストとして IPA ウェブサイト上の中小企業向けの登録セキスペ活用ページに試行公開[2]した。本事業においては、中小企業及び支援機関等でのリスト活用促進と、登録セキスペのリストへの登録促進の両面からリスト整備を行った。

本章では、「セキュリティ対策支援者リストの表示ページ作成」に関する実施結果について示す。

2.1 セキュリティ対策支援者リストの表示ページ作成

セキュリティ対策支援者リストは、検索をイメージした表示となるページを HTML 形式で作成した。

2.1.1 実施内容

セキュリティ対策支援者リストの表示ページについては、利用者の利便性を高めリスト利用率を向上することを目指し、簡易的な画面タブ絞り込み等による表示が可能となるよう HTML 化を行った。

セキュリティ対策支援者リストは、令和 9 年度に予定している「情報処理安全確保支援士検索サービス」のシステム刷新を機にシステム化を実施予定であるが、本事業では、HTML 化に必要な事項について、令和 9 年度のシステム化を念頭に要件を整理した。

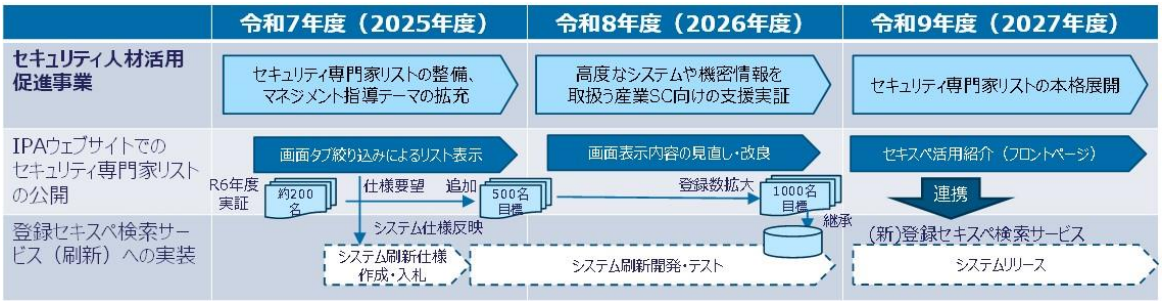


図 1　セキュリティ対策支援者リスト整備ロードマップ

セキュリティ対策支援者リストの表示ページとして作成した内容は、以下のとおりである。

① 検索結果（絞り込み表）の表示

簡易的な絞り込み表は、支援対象地域別（10 分類）、得意業種別（14 分類）とした。

・支援対象地域別（北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄）

・支援可能な業種別（自動車産業、半導体産業、その他製造業、建設業、防衛産業、電力産業、運輸・交通業、小売業、卸売業、サービス業、金融業、医療、教育、その他）

これにより、利用者が支援を依頼する専門家を容易に検索可能とした。

② 専門家個票

[2]「中小企業向けサイバーセキュリティ対策支援者リスト及び活用事例の紹介」：
https://www.ipa.go.jp/security/sme/shien/index.html

専門家個票は、IPA ウェブサイトで試行公開したセキュリティ対策支援者リスト約 200 名に加え、今年度新たにリストへ登録申請者分を作成し、絞り込み表からリンクを張った。

これにより、利用者が専門家の詳細情報が確認可能になるとともに、候補となる専門家を絞り込む表と、候補となった専門家の詳細情報を確認するための専門家個票を分離することで、利用者の利便性と視認性の向上を図った。

③　掲載項目の見直し

支援における初回相談の無料特典の有無に関する記載を追加することにより、利用者の相談へのハードルを低下させた。また、支援実績の表記方法を見直し、利用者向けの実績をわかりやすく提示可能とした。

④　ウェブアクセシビリティの確保

作成するリスト表示ページ（簡易的な絞り込み表、専門家個票）は、JIS X8341-3:2016 適合レベル AA に準拠したウェブアクセシビリティを確保した。

2.1.2　実施結果

セキュリティ対策支援者リストの表示ページ（HTML 形式）については、以下のとおり作成した。

登録番号	氏名	居住地	支援可能な指導テーマ					企業支援実績	支援対象地域	得意とする業界	支援期間					支援料金（1回/2時間あたり）	初回指導割引	支援可能な形態						所属状況	他の資格
			規程整備	情報管理・リスク分析	クラウド安全利用	インシデント対応	従業員教育				スポット対応	1～3か月	3か月～半年	半年～1年	1年以上			訪問	リモート	講演・研修	緊急対策	製品選定・導入	長期支援		
000016	姓001 名001	兵庫県神戸市	可	可	可	可	可		近畿	電力産業/サービス業/教育	可	可	可	可	可	20,000円以上～30,000円未満		可	可	可		可	可	企業勤務	ISMS27001審査員補、情報セキュリティ監査人補
000022	姓002 名002	愛知県岡崎市	可	可		可	可	4件/6年	東海,大阪	自動車産業/その他製造業/小売業/卸売業/サービス業/金融業	可	可	可	可	可	30,000円以上～40,000円未満		可	可	可	可		可	企業勤務	システム監査技術者
000039	姓003 名003	奈良県生駒市	可	可	可	可	可	30件/10年	京都府,大阪府,兵庫県,奈良県	その他製造業/建設業/卸売業/サービス業/各種士業	可	可	可	可	可	40,000円以上		可	可	可		可	可	企業勤務	中小企業診断士
000049	姓004 名004	福岡県福岡市	可	可	可	可	可		福岡県	建設業/運輸・交通業/教育	可	可	可	可	可	30,000円以上～40,000円未満		可	可	可	可	可	可	独立	データベーススペシャリスト、エンベデットシステムスペシャリスト

図 2　セキュリティ対策支援者リストの表示ページ

また、セキュリティ対策支援者リストの表示ページより、各専門家の詳細を閲覧するための個票ページを以下の図のとおり作成した。

独立行政法人 情報処理推進機構

中小企業向けサイバーセキュリティ対策支援者リスト

初回登録日時　2026/1/14 17:02

■基本情報

氏名（カナ）	セイ006 メイ006
氏名	姓006 名006
公開用メールアドレス	006@gmail.com
登録番号	000093
居住地	神奈川県横浜市
所属状況	企業勤務
所属組織	
他の資格	システム監査技術者
所属・関係する団体	
自己PR	
参考URL	

■支援実績

セキュリティ実務経験	3年未満
企業支援経験	経験あり
企業支援実績	0件/0年
企業支援内容	経験なし
得意とする業界	該当なし

■支援可能な範囲

企業規模				
支援対象地域	埼玉,千葉,東京,神奈川			
支援期間	スポット対応	可	1～3か月	
	3か月～半年		半年～1年程度	
	1年以上の長期的支援（顧問契約等）			
	その他：			
支援料金（1回/2時間あたり）	20,000円未満		初回指導割引	
支援可能な形態	訪問によるコンサルティング	可	オンラインコンサルティング	
	講演・研修		インシデント発生時の緊急対策支援	
	セキュリティ製品の選定・導入支援		長期的支援（顧問契約等）	
	補足事項：			
支援可能な指導テーマ	情報セキュリティ規程の整備	可	情報資産の洗い出しとリスク分析	
	クラウドサービスの安全利用		セキュリティインシデント対応	
	従業員向け情報セキュリティ教育	可		

■保有スキル

【0】セキュリティ対策戦略の立案		【1】サイバーセキュリティ対策の方針策定と管理体制づくり	
【2】セキュリティリスクの識別		【3】サイバーセキュリティ対策の実践と運用の強化	
【4】サイバー攻撃の検知、監視、検知後の運用策定		【5】セキュリティインシデント発生時の対応	
【6】セキュリティインシデントからの復旧やコミュニケーション		【7】システム監査	

【保有スキルの凡例】
本表では、専門家が自己評価したスキルの総合点をもとに、以下の記号で成熟度を示しています。
◎：当該分野に精通しており、単独で実行可能
○：当該分野について知識を有し、必要に応じて補完しつつ実行可能

図 3　セキュリティ対策支援者リストの個票ページ

2.2 支援機関等におけるセキュリティ対策支援者リストの活用

IPA では、登録セキスペ活用の広報資料を作成し、各地域の支援機関等の協力により、セキュリティ対策支援者リスト掲載の専門家による中小企業向けセキュリティ相談会を開催するなどして、登録セキスペの活用促進を図った。

2.3 セキュリティ対策支援者リストの活用促進に関する考察

セキュリティ対策支援者リストの活用促進に関する考察を以下に示す。

本事業では、セキュリティ対策支援者リストの登録・変更・終了手続から HTML 公開までの業務フローを標準化し、Excel ベースでマスタ生成・公開チェックを行う仕組みを整備した。これは、令和 9 年度のシステム化を見据えた試行段階としての取組であるが、本格運用に向けては、以下の課題があり対応が必要と考えられる。

(1) 支援者リストの効率的な運用に向けて

- 登録セキスペの有効期限管理と登録継続性
  本事業で整理したフローにおいては、登録セキスペの有効期限管理を考慮しているが、仮に期限が切れた場合に対象データを非公開とした後の扱いについては、リスト掲載・運用（案）には含められていない。積極的に活動する専門家のリスト登録については可能な限り継続した方が望ましいことから、有効期限切れの場合の登録継続を促す専門家へのサポート内容・手順等についても検討し、必要に応じてリスト掲載・運用（案）に反映することが望ましい。
- リスト掲載情報の鮮度維持・活動状況の反映
  専門家リストの運用が継続するにつれて、初期登録の情報がそのまま残ることで鮮度の異なる情報が混在する、活動が活発な専門家とそうでない専門家の区別がつきにくい等、リスト全体としての品質確保が難しくなることが懸念される。信頼できる情報を継続的に提供するために、定期更新をより強力に促す、各専門家情報の最新更新日時を示す等、リスト掲載情報の鮮度を保つことで、リスト全体の品質を確保することも必要である。また、単にリストとしての提示だけではなく、活動実態を反映したリストとすることで、利用者にとっても検索が容易となる。喫緊の活動実態やアクティブな度合いを示せる項目（例：直近 1 年間の支援活動有無や SCS 評価制度への対応可否）の追加等も検討の余地がある。

(2) 支援者リストの活用に向けて

- 検索軸の拡充
  現状の検索軸は、支援地域（10 分類）及び得意業種（14 分類）としているが、利用者である中小企業から見ると、選定基準は、支援実績、指導可能な内容、費用目安等、多岐にわたると考えられる。システム化を見据え、検索軸の拡充に関しての検討が必要となる。
- 中小企業以外の利用促進

現在の専門家リストは、中小企業の方が支援を得るために専門家を探すことが主な利用シーンと想定されているが、それ以外の方の利用シーンについても具体化の上、利用者・利用シーンに応じた周知・案内が効果的と考えられる。例えば、SCS 評価制度における活用はもちろん、商工会議所の相談窓口での利用、補助金申請時の活用、地域金融機関による紹介等が考えられる。

3. セキュリティ対策支援者リストの登録促進

本事業では、全ての登録セキスペを対象に登録セキスペ活用の取組を周知し、ウェビナー形式の「セキュリティマネジメント指導ツール活用セミナー」を開催、指導ツールを活用した指導方法及び指導事例を啓発することで、セキュリティ対策支援者リストへの登録を促進した。

本章では、「セキュリティマネジメント指導ツール活用セミナーの開催」、セキュリティ対策支援者リスト公開のための運用手続を定めた「セキュリティ対策支援者リストの掲載・運用方法（案）作成」及び「セキュリティ対策支援者リスト登録受付・確認・リスト反映」に関する実施結果について示す。

3.1 セキュリティマネジメント指導ツール活用セミナーの開催

令和 6 年度事業では、登録セキスペによる中小企業への訪問指導（セキュリティマネジメント指導）の実施に際し、基本的なセキュリティ対策として、IPA「中小企業の情報セキュリティ対策ガイドライン 」（以下「中小企業ガイドライン」という）等を活用した 5 つの指導テーマを設定し、各テーマについて指導ツール（実施要領及びワークシート等）を整備した。

本事業においては、全ての登録セキスペを対象に登録セキスペ活用の取組を周知し、ウェビナー形式の「セキュリティマネジメント指導ツール活用セミナー」を開催、指導ツールを活用した指導方法及び指導事例を啓発することで、セキュリティ対策支援者リストへの登録を促進した。

3.1.1 実施内容

「セキュリティマネジメント指導ツール活用セミナー」は以下のプログラムで実施した。

表 1 「セキュリティマネジメント指導ツール活用セミナー」プログラム

時刻	内容
13：00～	経済産業省の登録セキスペ活用の取組 （経済産業省サイバーセキュリティ課／情報技術利用促進課（IT イノベーション課））
13：10～	セキュリティマネジメント指導ツールの説明（独立行政法人情報処理推進機構）
14：00～	休憩
14：10～	ゲストスピーカーによる指導ツール活用事例の紹介
15：10～	セキュリティ専門家リストの登録促進について（株式会社三菱総合研究所）
15：20～	質疑応答・閉会

表 2 「セキュリティマネジメント指導ツール活用セミナー」ゲストスピーカーと事例テーマ

開催日	名前	形態	事例企業	事例テーマ
11/7（金）	久保田 秀男氏	副業	A 株式会社【非公開】 （製造業・中部地方）	「自動車業界ガイドラインに沿った具体的なインシデント対応指南」

11/20 （木）	髙橋 真悟氏	個人	深田電機株式会社 （卸売業・愛知県）	「DX による効果を最大限に生かすセキュリティ対策を具体的に指南」
12/5 （金）	高橋 幸司氏	副業	社会福祉法人ぷくぷく福祉会すいた障がい者就業・生活支援センター （医療／福祉・大阪府）	「セキュリティ対策の第一歩として従業員の意識を向上」

表 3　各ゲストスピーカーのプレゼンテーション内容

開催日	名前	プレゼンテーション内容
11/7 （金）	久保田 秀男氏	セキュリティマネジメント指導を始めた動機 副業として取り組むセキュリティマネジメント指導 指導先を知る：事業内容・課題の把握 指導シラバス（ツール）の活用（インシデント対応編） 実際の指導実績と効果 ・ 営業、設計等別にインシデント対応手順書を作成し演習を実施 セキュリティ専門家としての心構え セキュリティマネジメント指導：課題と改善 まとめ ― 指導を通じて得られた学びと今後
11/20 （木）	髙橋 真悟氏	セキュリティマネジメント指導ツールの良かった点 2024 年度に取り組んだマネジメント指導について ・ 指導テーマ「情報セキュリティ規程の整備」 DX 推進のための生成 AI 活用ルールの策定、既存のセキュリティ規程のチェック ・ 指導テーマ「従業員向けセキュリティ教育」「情報資産の洗い出しとリスク分析」 現状の取組状況の評価、従業員に対する 30 分程度の研修 私のマネジメント指導におけるスタンス マネジメント指導にチャレンジした感想 マネジメント指導を通して感じた企業側のニーズ
12/5 （金）	高橋 幸司氏	本事業への参加の動機 セキュリティマネジメント指導ツールの特徴 指導事例（1）テーマ①セキュリティインシデント対応（会計事務所） ランサムウェア感染を想定した対応手順書の作成 指導事例（2）テーマ⑤従業員向けセキュリティ教育（社会福祉法人） 企業側の要望を整理し標的型攻撃メールを題材に研修を決定、理解確認テスト･アンケートを実施 指導事例（3）テーマ②情報資産の洗い出しとリスク分析 指導を通して感じた事 企業内人材が公的活動に参加する価値 まとめ

3.1.2　実施結果

(1)　参加促進

「セキュリティマネジメント指導ツール活用セミナー」の参加促進にあたって、IPA ウェブサイト内において「セキュリティマネジメント指導ツール活用セミナー」のページを構築した。また、チラシを作成し、同ページへの掲載を行った。

図 4　「セキュリティマネジメント指導ツール活用セミナー」チラシ（1/2）

ゲストスピーカー

ゲストスピーカーによる指導ツール活用事例の紹介では、
『セキュリティマネジメント指導事例集』の掲載企業を実際に担当した
情報処理安全確保支援士の方に具体的な実施内容をご説明いただき、中小企業向けセキュリティ専門家
としての心構えとハウツウも含めてご紹介いただきます！

2025年11月7日(金)

久保田 秀男 氏（特定非営利活動法人日本システム監査人協会）

愛知県在住　支援業務形態：副業
中部地方の自動車製造業の企業における指導事例
「自動車業界ガイドラインに沿った具体的なインシデント対応」
その他保有資格：システム監査技術者

2025年11月20日(木)

髙橋 真悟 氏（インフォシア 代表）

愛知県在住　支援業務形態：個人
愛知県の卸売業の企業における指導事例
「DXによる効果を最大限に生かすセキュリティ対策」
その他保有資格：社会保険労務士

2025年12月5日(金)

高橋 幸司 氏（株式会社東洋 常務執行役員・CIO）

京都府在住　支援業務形態：副業
大阪府の社会福祉法人における指導事例
「セキュリティ対策の第一歩として従業員の意識を向上」
大阪府の会計事務所における指導事例
「実施済みセキュリティ対策を机上演習で実践的にレビュー」
その他保有資格：中小企業診断士、ITコーディネータ、ITストラテジスト、
公認情報システム監査人補

- セミナーの詳細は下記ウェブページをご覧ください。
  情報処理安全確保支援士向け「セキュリティマネジメント指導ツール活用セミナー・ケース演習」
  https://www.ipa.go.jp/security/sme/shien/riss-katsuyo-semi.html
- 各回の内容は、ゲストスピーカーの講演以外は共通です。
- 講演資料は全回終了後、上記ウェブページにて公開します。また、アーカイブ動画も後日公開する予定です。
- 情報処理安全確保支援士のご登録者以外の方のお申込みにつきましては、事務局までメールにてご相談ください。
- 本事業は、情報処理安全確保支援士の人材活用について検討する「令和7年度セキュリティ人材活用環境整備」の一環として実施するものです。
- 指導事例や本事業の詳細については下記ウェブページをご参照ください。
  「中小企業向けサイバーセキュリティ専門家リスト及び活用事例の紹介」
  https://www.ipa.go.jp/security/sme/shien/index.html

図 5　「セキュリティマネジメント指導ツール活用セミナー」チラシ（2/2）

(2) 参加状況

「セキュリティマネジメント指導ツール活用セミナー」の参加者は以下のとおり。当初、各回300 名程度の申込を予定していたが、各回、予定以上の多くの申込があった。また、当日の実際の参加者数を申込者数で割った参加率は 9 割程度と高い結果となった。各回のゲストスピーカーが異なることもあり、複数回に参加するケースも見られた。

表 4 「セキュリティマネジメント指導ツール活用セミナー」申込・参加状況

	第 1 回 11/7（金）	第 2 回 11/20（木）	第 3 回 12/5（金）	合計
申込者数	783 名	691 名	660 名	2,134 名
参加者数	727 名	624 名	577 名	1,928 名
参加率	92.8%	90.3%	87.4%	90.3%

(3) セミナーにおける質問及び回答（FAQ）

「セキュリティマネジメント指導ツール活用セミナー」の申込時の質問や、セミナー中の質疑応答を FAQ としてとりまとめ、「セキュリティマネジメント指導ツール活用セミナー」のウェブサイトに公開した。また、セミナー動画（アーカイブ）と説明資料については、後日、同ウェブサイトに公開した。

表 5　「セキュリティマネジメント指導ツール活用セミナー」FAQ

No.	質問	回答
1. マネジメント指導ツールについて		
1-1	セキュリティマネジメント指導ツールは、どこで入手できますか。	セキュリティマネジメント指導（5 テーマ）の実施要領（PDF）は、以下の IPA ウェブサイトからダウンロードできます。 ■中小企業向けサイバーセキュリティ専門家リスト及び活用事例の紹介 https://www.ipa.go.jp/security/sme/shien/index.html セキュリティマネジメント指導テーマ テーマ(1) ～ テーマ(2) また、ワークシート等を含む指導ツール活用セット一式をご希望の方は、以下の IPA ウェブサイトよりお申し込みください。 ■情報処理安全確保支援士向け「セキュリティマネジメント指導ツール活用セミナー・ケース演習」 https://www.ipa.go.jp/security/sme/shien/riss-katsuyo-semi.html 参考資料 「セキュリティマネジメント指導ツール（セット版）」ダウンロード申込フォーム
1-2	セキュリティマネジメント指導ツールの商用利用は可能でしょうか。また、利用可能範囲や利用制限があればお教えください。	セキュリティマネジメント指導の実施要領及び各種ツール（以下、「マネジメント指導ツール」という）は、商用利用の如何を問わず、中小企業向けのセキュリティ対策指導及び講習・セミナー等でご使用いただけます。指導及び講習・セミナー等で使用する際に、実施要領及び各種ツールを一部割愛したり、必要に応じて追加する等のカスタマイズは行っていただいて結構です。詳細は実施要領の「本資料の使用条件」をご覧ください。 なお、実施要領及び各種ツールの著作権は独立行政法人情報処理推進機構（IPA）に帰属しますが、「本資料の使用条件」の範囲でのご使用であれば、当機構からの使用許諾を得る必要はありません。
2. マネジメント指導ツールを用いた指導について		
2-1	セキュリティマネジメント指導を行う際に、指導先企業からよくある質問や対応方法についてまとめた資料はありますか。	セキュリティマネジメント指導の成果が得られた中小企業の好事例（7 社）として、企業が情報セキュリティ対策において感じていた課題と専門家による指導のポイントをまとめた「セキュリティマネジメント指導事例集」が参考になりますのでご参照ください。 ■「セキュリティマネジメント指導事例集」 https://www.ipa.go.jp/security/sme/shien/tbl5kb0000009ual-att/jirei.pdf
2-2	指導先企業へは訪問指導が必須でしょうか。オンラインでの指導でも良いでしょうか。	セキュリティマネジメント指導ツールは、標準的な進め方として 3 回の訪問指導をベースに構成しています。令和 6 年度実証においても、企業様からはセキュリティ専門家の訪問が良かったとのご意見をいただいており、基本的には訪問での指導をお勧めしています。ただし、企業様によっては距離や地理的な問題から、ご相談によりオンラインによる指導の併用もあり得ると考えます。
3. セキュリティ専門家リストについて		
3-1	「中小企業向けサイバーセキュリティ対策支援者リスト」に登録するための手順を教えてください。	「中小企業向けサイバーセキュリティ対策支援者リスト」への登録については、以下の IPA ウェブサイトに登録方法を掲載していますので、内容をご確認の上、申請してください。 ■中小企業向けサイバーセキュリティ対策支援者リスト https://www.ipa.go.jp/security/sme/shien/list.html なお、リスト登録にあたりましては、「セキュリティマネジメント指導ツール活用セミナー」（開催期間：2025 年 11 月～12 月）のアーカイブ配信をご視聴いただき、セキュリティマネジメント指導ツールの内容についてご理解いただくようお願いいたします。 ■情報処理安全確保支援士向け「セキュリティマネジメント指導

		ツール活用セミナー・ケース演習」 https://www.ipa.go.jp/security/sme/shien/riss-katsuyo-semi.html
3-2	「中小企業向けサイバーセキュリティ対策支援者リスト」登録の前提条件はありますか。	「中小企業向けサイバーセキュリティ対策支援者リスト」は、「情報処理安全確保支援士（登録セキスペ）」のうち、中小企業向けのサイバーセキュリティ対策支援が実施できる専門家の得意分野・専門領域を可視化したセキュリティ専門家リストです。したがって、情報処理安全確保支援士として登録していること、専門家として企業の支援に対する活動意向をお持ちの方が、リスト登録の前提条件となります。 なお、中小企業及び支援機関が、リスト登録の専門家の実績やスキル等を見て希望する専門家を選択することになるため、リスト登録申請にあたっては、ご自身の実績経験や、保有するスキルを客観視できるアンケートに回答いただきます。

(4) アンケート調査結果において得られた意見

「セキュリティマネジメント指導ツール活用セミナー」参加者に対して、参加後にアンケートを実施した。全 3 回のセミナーへの参加者のうち、888 名から回答を得られた。主なアンケート結果を以下に示す。

① セミナー全体の満足度

セミナー全体の満足度については、「たいへん参考になった」が 55.1%、「やや参考になった」が 40.9%で、ほぼ参加者全員が参考になったとの回答であった。

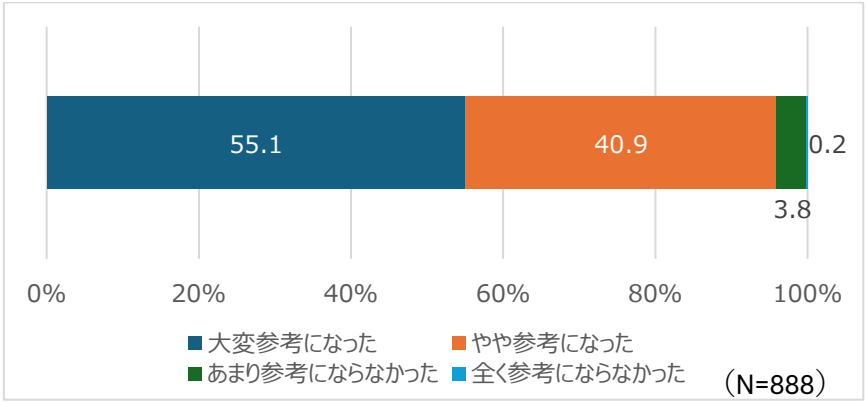


図 6 セミナー全体の満足度

② 支援者リストへの登録・活動意向

セキュリティ対策支援者リスト（専門家リスト）への登録・活動意向については、「専門家リストに登録して、条件が合えば活動したい」が 40.1%、「関心はあるが、少し検討や確認してから考えたい」が 33.1%で、7 割以上の参加者がリスト登録に前向きの回答であった。

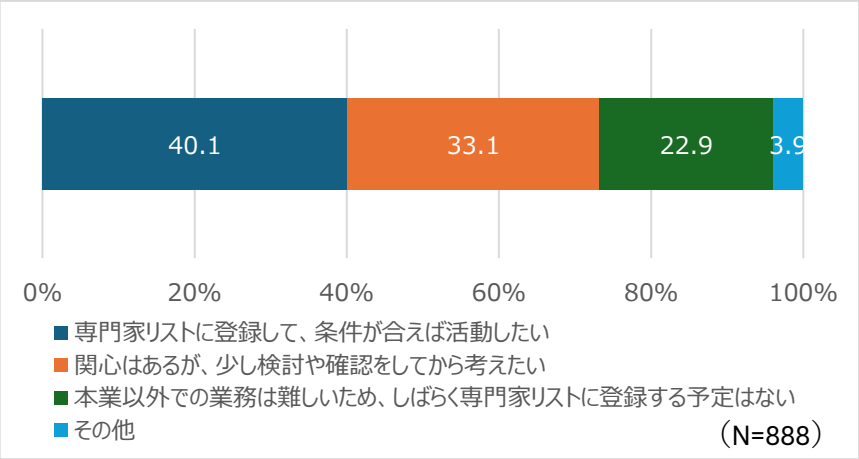
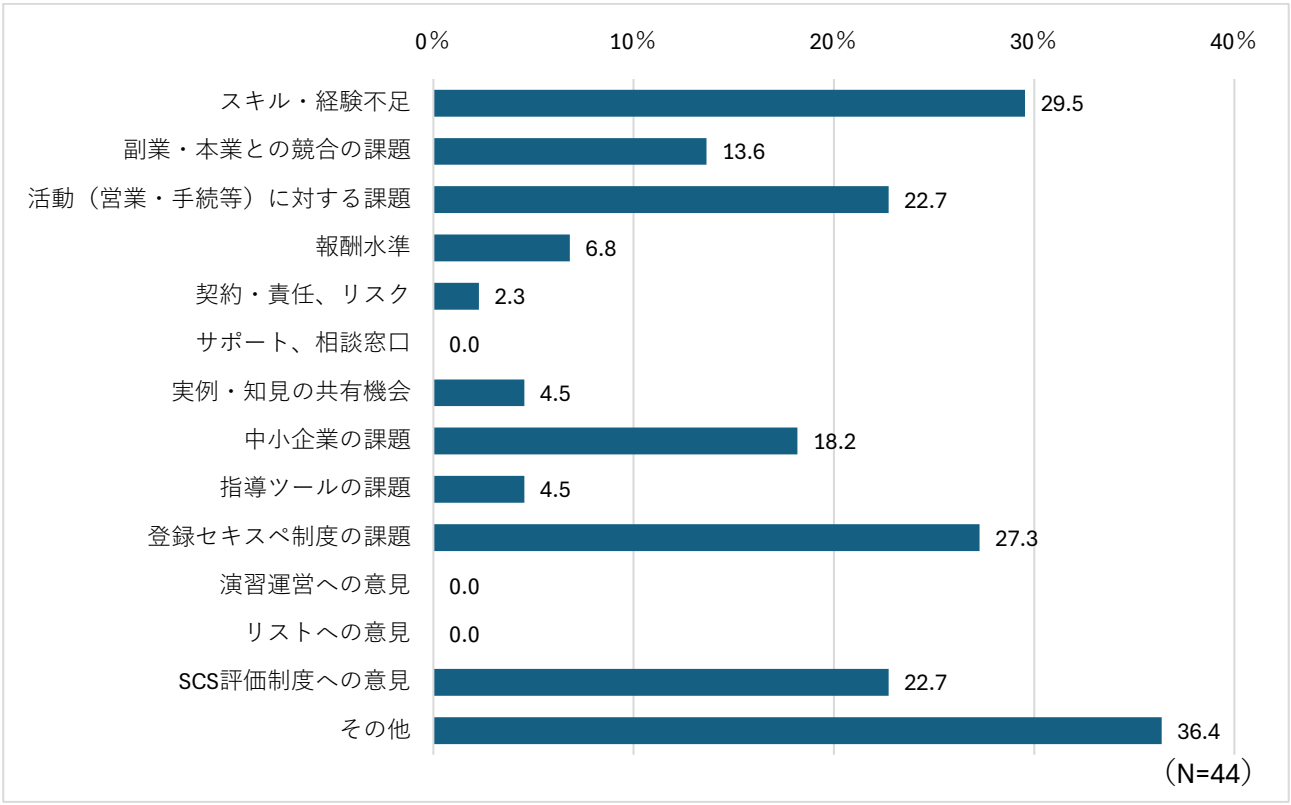


図 7　支援者リストへの登録・活動意向

③　自由記述回答からの分析

自由記述に記載された回答を内容別にみると、登録セキスペとして活動するにあたっての課題や要望等の記載が多く見られた。特に多かった回答は、「スキル・経験不足」（13.3%）という専門家自身の課題、及び「報酬水準」（10.4%）という中小企業に対するセキュリティ支援の環境に関わる課題であった。



注）自由記述回答者 278 名に対する比率。1 名の回答者の回答が複数の項目に関わる場合は複数にカウント

図 8　セミナーアンケート自由記述結果

自由記述で得られた主な回答を以下に示す。

A) 専門家自身の課題

・ スキル・経験等の不足

「指導経験がなく、支援ができるか不安」、「知識に偏りがあり、全体を支援できるか自信がない」、「研修や OJT の機会がほしい」等、専門家としてのスキルや経験等の不足に関わる不安や自信のなさ、またそれを補うための研修や OJT に関する要望がみられた。

・ 副業・兼業、本業との競合の課題

「副業禁止」、「会社の許可が必要」といったそもそも副業が難しい状況や手続きが必要という意見や、「IT 企業・SIer・コンサル等勤務のため、本業と競合する」等の本業と競合することによる活動のしにくさに対する意見があった。また、「公務員であり、勤務時間内での活動を認めたり、特別休暇制度等があるとよい」等の公務員における登録セキスペとしての活動を行うための環境整備・制度に関する意見もみられた。

・ 活動に関する不安

「リストに登録したら、どれぐらいの頻度で案件が来るのかわからない」、「いつまでも声がかからないのでは」、「営業はどのように実施するのか」等、案件獲得に関わる不安に関する意見がみられた。

B) 市場・環境の課題

・ 報酬水準に関する懸念

「中小企業側の希望する価格帯と専門家側の希望する報酬水準が見合わない」、「ボランティアとしてなら考えられる（ただし、ボランティアとして登録すると既登録者と競合する）」、「副業よりプロボノに近いのではないか」等、登録セキスペとしての活動に対する報酬水準が提供する価値に見合わないとする意見がみられた。また、ボランティアとしての活動意向がある場合は、適正な報酬水準を希望する専門家と混在することに対する市場への悪影響を懸念する意見もみられた。

・ 契約や責任、リスクに対する懸念

「契約、NDA 等は自身で締結するのか」、「トラブルが発生した場合はどのように対応したらよいか」、「無償に近い謝金で無限定の保証や賠償責任まで負うのは割に合わない」等、中小企業と直接契約することに対する不安や、責任を負うことへのリスクへの懸念がみられた。

・ サポートや相談窓口に対する要望

「自身で解決できない相談が来た場合、どこに相談すればよいか」等、前述のトラブル等に関わる対応や、相談内容が専門家自身の対応範囲を超えている場合のサポートや相談窓口に対する意見がみられた。また、相談内容が幅広い場合等「チームで支援できる仕組みがあった方がよい」といった意見や「若手や未経験者が OJT 的に参加できるようにしてほしい」等、中小企業への相談への対応体制をアレンジできるような仕組みに対する要望もみられた。

C) 中小企業における課題

・ 中小企業側の意識・投資余力の課題

「セキュリティをコストと見ている企業が多い」、「無料・1 万円未満を望む企業の割合が高い」、「経営課題が山積みで、セキュリティは後回しとなっている」等、中小企業においてセキュリティ対策を行うための意識が高まっていない点や対策費用を確保できない状況に関する課題も指摘された。

D) マネジメント指導ツールに対する要望

・ 指導ツールの活用に関する課題

マネジメント指導ツールに対して「商用利用や社内共有など、利用ルールを明確にしてほしい」、「事例やサンプルがほしい」、「小規模事業者・診療所などの小規模組織に向けたサンプルがほしい」等、より指導ツールを活用するためのルール明示、付加的なコンテンツに対する要望がみられた他、「ツール活用手順や一連の支援プロセスの動画、体験できる講座がほしい」、「ツールを使った演習を実践講習に組み込んでほしい」等、ツールの活用方法を習得するための機会に対する要望も挙がった。

E) 支援者リストに関する課題

・ 支援者リストの存在や登録方法等のわかりにくさ

「そもそも支援者リストを知らなかった」、「登録方法がわからない」、「支援者リストはセキュリティプレゼンターとは異なるのか」、「既に登録済みであるが、内容の修正方法がわからない」等、支援者リストがそもそも認知されていない、あるいは目的そのものや登録・更新方法が理解されていない状況が伺えた。

・ セキュリティ・プライバシーへの懸念、公開情報への要望

「メールアドレスが公開され、スパムの標的になる」、「氏名や連絡先が公開されることに抵抗がある」等、自身の情報を支援者リストに掲載・公開することに対する懸念がみられた。また、「対応可能地域、ボランティア可否、オンラインのみ等の条件を掲載したい」等、細かな条件等を支援者リストに掲載したいというニーズもみられた。

3.2 セキュリティ対策支援者リストの掲載・運用方法（案）作成

令和 6 年度事業の結果、及び中小企業向けセキュリティ相談会等におけるセキュリティ対策支援者リストの活用フィードバックを踏まえ、セキュリティ対策支援者リストの掲載・運用方法（案）を作成した。

3.2.1 実施内容

(1) 目的

セキュリティ対策支援者リストの掲載・運用方法（案）は、セキュリティ専門家からの登録データについて、支援者リストへの登録申請・変更申請・終了申請の各種手続に基づき、事務局がデータを管理し、HTML 形式にてリスト公開までを行うための手順を標準化することを目的とした。

(2) 掲載・運用（案）概要

セキュリティ対策支援者リストの掲載・運用方法（案）については、業務の工程を「申請受付」、「マスタ管理」、「HTML 公開」、「問合せ対応」として整理した。

なお、本事業では、令和 9 年度に整備予定の「登録セキスペ検索サービス」に機能を取り込むまでの暫定運用を示した。具体的には、Excel を用いて、SaaS の申請フォームで申請・出力された「登録、変更、終了」の CSV 元データ（コード版）を整形し、マスタ CSV を生成する「データ整形・CSV 生成作業」、整形された支援者リスト情報を確認する「公開チェック作業」、さらに公開可能と判断したマスタ CSV を公開 HTML ページ（支援者リスト、個票）へ変換する「HTML 変換作業」までの一連の業務手順を示した。

(3) 掲載・運用における業務フロー

セキュリティ対策支援者リストの掲載・運用（案）の作成にあたって、業務フローを以下のように整理した。

① リストへの登録（登録、変更）の受付
リストの掲載を希望する登録セキスペからの申請を受け付ける。

② マスタ管理
申請データをリスト化し、マスタとして管理する。

1) リストへの登録申請（属性、スキル要件、実績等）の内容確認

専門家の情報を登録する際には、属性やスキル要件（スキルチェック結果）、実績等の入力内容に誤りや問題がないかを確認するため、運用管理者のチェックを経た後、必要に応じて専門家への確認等を行った上で、登録情報をリスト化する。運用管理者のチェックの際には、確認項目を一覧化したチェックリストを元に行うものとし、登録情報の品質を確保する。

ただし、「登録」でデータが入力された場合でも既にリスト登録済の場合もあるため、リストへの登録状況を確認の上、登録済みの場合は「変更」のフローとする。

2) リスト記載内容の変更・追加申請の内容確認

専門家自ら変更・追加を申請した場合には、新規の登録と同様、受付を行い、運用管理者のチェックを経た後、必要に応じて専門家への確認等を行った上で、登録情報をリスト化する。

③ HTML 公開

マスタファイルから HTML を出力し、ウェブにて公開する。

④ 問合せ対応

申請者・掲載者からの問合せに対応する。リストに修正が必要であれば、②③の手続を行う。

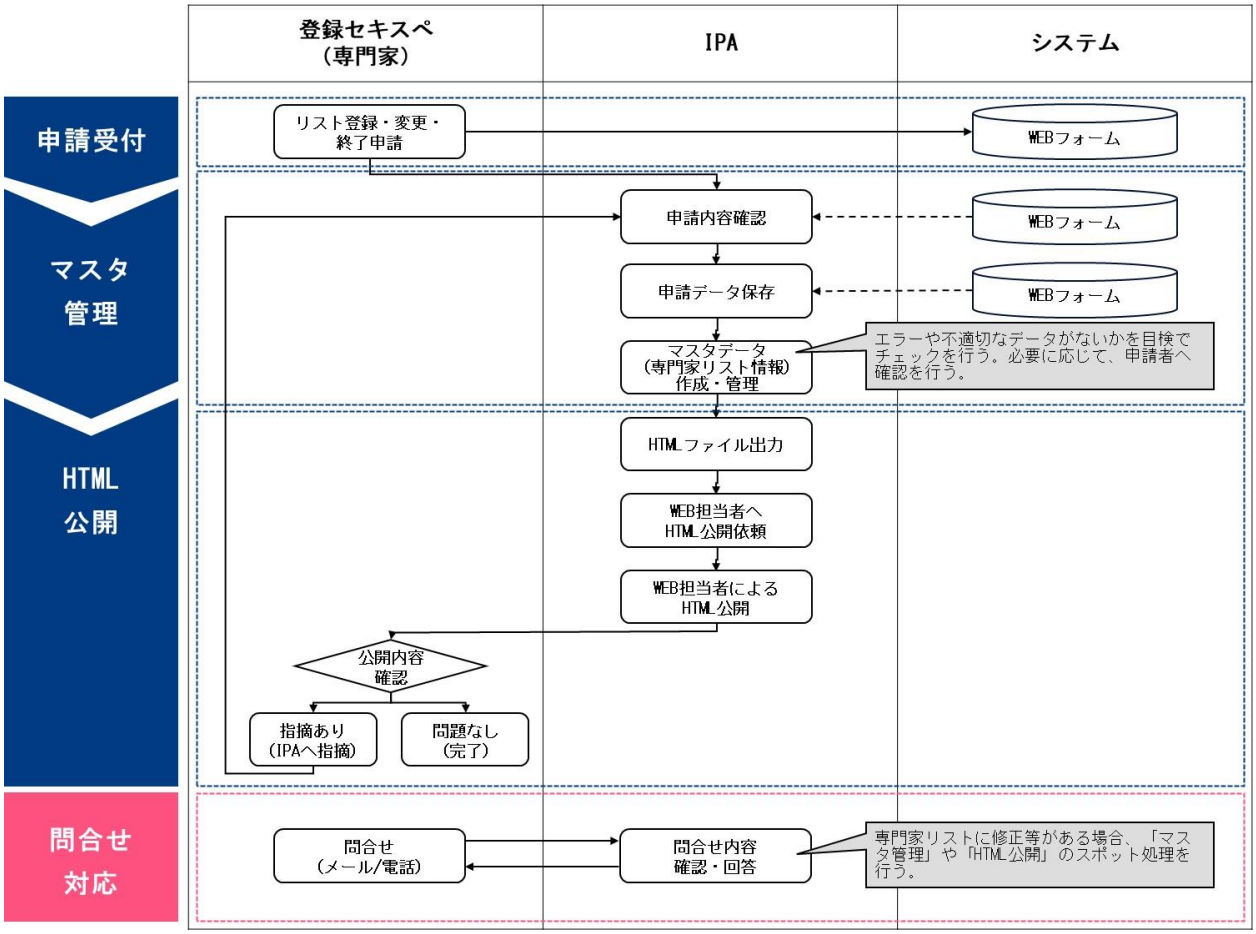


図 9　支援者リスト掲載・運用に関わる業務フロー

なお、業務のうち、有効期限の管理及びリスト利用者からの評価情報の反映については、以下のとおり検討を行った。

① リスト記載内容の更新（有効期限の設定）

リスト登録者の登録申請日（更新日）を個票に記載することで、支援者リストの記載内容がいつの時点の情報かを利用者が確認できるようにした。

一方で、登録セキスペには有効期限があるが、有効期限切れの場合は、リスト表示を取り止める必要があるため、内部的には登録データに「表示／非表示」のフラグを設け、必要に応じて専門家への確認等を行うこととした。

② リスト利用者からの評価情報の反映

リスト利用者（中小企業、支援機関を想定）からの評価情報については、IPA ウェブサイトに支援者リストに問合せ窓口の連絡先を掲載しているものの、今後の運用としては、運用管理者のチェックを経た後、必要に応じて利用者への確認等を行った上で、何らかの方法でリストに反映することを検討することが望ましい。

3.2.2 実施結果

整理した業務フローに基づき、セキュリティ対策支援者リストの掲載・運用方法（案）については、以下の目次で作成した。

表 6　セキュリティ対策支援者リストの掲載・運用方法（案）目次

タイトル
1. はじめに
2.「申請受付」について
3.「マスタ作成」について
4.「マスタ CSV 出力」について
5. HTML 変換作業手順（ブラウザ作業詳細）
6. その他注意事項
付録

なお、各業務について、以下の作業内容を記載した。

- 申請受付
  新規登録・内容変更・掲載終了の申請種類別に 3 通りの受付窓口を作成した。受付及び申請者への受付確認連絡は自動とした。
- マスタ作成
  マスタ管理のうち主作業である「マスタ作成」は、(1) 申請データの保存、(2) 申請データの取込、(3) 申請データの統合（新規登録・内容変更・終了申請の各々のデータ統合)、(4) 申請データの修正（表記揺れや画像データファイル名等の修正)、(5) 整形データの作成（マスタ管理のためのデータ整形)、(6) マスタ追加・更新、(7) 処理結果の保存、の流れで実施した。
- マスタ CSV 出力
  整形ブックのマスタ（Excel 形式）を CSV 形式で出力した。
- HTML 変換
  マスタ CSV から HTML 変換ツールを用いて HTML ファイルを作成、ブラウザ上で動作を確認し、問題がなければウェブサーバー上での確認を経て公開とした。

3.3 セキュリティ対策支援者リスト登録受付・確認・リスト反映

セキュリティ対策支援者リストに対して、IPA ウェブサイトで試行公開したセキュリティ対策支援者リスト（一覧表ダウンロード）約 200 名に加えて、登録促進活動で新規に登録申込みを受けた登録セキスペを合わせて、セキュリティ対策支援者リストの表示ページに掲載した。

3.3.1 実施内容

(1) 登録受付・確認・リスト反映

セキュリティ対策支援者リスト登録受付・確認・リスト反映については、支援者リストの活用に向けて、支援者リストの掲載内容の品質を確保するとともに、登録受付から確認、反映、公開まで遅滞なく円滑に行うことを目的として実施した。

セキュリティ対策支援者リスト登録受付・確認・リスト反映にあたって、以下を実施した。

① 登録申請内容の確認

「セキュリティ対策支援者リストの掲載・運用方法（案)」に基づき、登録申請内容の確認を行った。確認の結果、疑義が生じた事項については、直接、登録申請者に問合わせた上で登録申請内容を修正した。申請内容の確認が取れたものをセキュリティ対策支援者リストの表示ページに掲載した。

② リスト登録者の確保

セキュリティ対策支援者リストの登録者は、令和 6 年度に試行公開したセキュリティ対策支援者リスト掲載者に加え、今年度実施する「セキュリティマネジメント指導ツール活用セミナー」参加者、「セキュリティ専門家向けケース演習」参加者を主な対象として、支援者リストの周知と、リストへの登録を促した。

③ リスト登録受付・確認・リスト反映作業にあたっての問題点等の記録

セキュリティ対策支援者リストへの登録受付作業で問題点等があれば記録し、リストの掲載・運用方法（案）の改善点としまとめた。

(2) 登録項目の見直し

セキュリティ対策支援者リストの項目見直しにあたっては、令和 6 年度時点での項目について課題の有無を整理した後、見直し方針案と見直した場合の効果、見直しにあたっての考慮点について評価の上、最終的な見直し項目を定めた。

追加した主な項目は「初回無償サービス有無」「参考 URL」「写真」である。また、削除した項目は、「年齢」「登録取得年」「保有スキルに関する回答の根拠となる実績や経験」である。

見直し後の支援者リスト項目と選択肢、確認方法を以下に示す。

表 7　支援者リストへの登録項目

項目	番号	必須 任意	設問	選択肢	確認方法
【基本情報】		必須	情報処理安全確保支援士登録番号	（　　）	・「情報処理安全確保支援士検索サービス」で氏名・番号が合致しているか確認。
		必須	氏名	（　　）	・「情報処理安全確保支援士検索サービス」で氏名・番号が合致しているか確認。
		必須	カナ		–
		必須	居住地 （都道府県と市区町村までで可）	（　　）	–
		必須	所属状況	独立 企業勤務 その他（　　）	–
		必須	所属企業・組織名	（　　）	–
		必須	メールアドレス	（　　）	・メールアドレスの形式が正しいか確認。 （xxx@xxx.jp）
		任意	参考 URL		・リンクが表示されるか確認。
		任意	写真		・ファイルサイズが 1M 以内か確認。 ・画像が上半身正面で、不鮮明でないこと。 ・不適切な画像でないこと。
		任意	その他保有資格（複数選択可）	IT コーディネータ 中小企業診断士 税理士 社会保険労務士 行政書士 医療情報技師 IT ストラテジスト システム監査技術者 CISA（公認情報システム監査人） CISSP その他（　　）	・その他に記載されている内容が選択肢と重複していないか確認。 ・その他に記載されている内容が資格かどうか確認。
		必須	所属する団体や組織 （複数選択可）	商工会議所・商工会 中小企業庁関連（中小企業基盤整備機構・よろず支援拠点・都道府県の中小企業支援センター等） 金融機関 日本自動車工業会・日本自動車部品工業会 情報処理安全確保支援士会 IT コーディネータ協会 中小企業診断士協会 税理士会 社会保険労務士会	・その他に記載されている内容が選択肢と重複していないか確認。 ・その他に記載されている内容が実在する団体や組織かどうか確認。

				行政書士会 その他（　　） 該当なし	
【経験・実績】		必須	セキュリティ分野での実務経験年数（単一回答）	3 年未満 3-5 年 5-10 年 10 年以上	－
		必須	企業に対するセキュリティ対策支援の経験有無（単一回答）	経験なし 経験あり	－
		必須	（支援の経験「経験あり」の方） 支援件数	（　　）件	・支援件数が「0」でないことを確認。 ・支援件数が「1,000」以上でないことを確認。
		必須	支援年数	（　　）年	・支援年数が「50」以上でないことを確認。
		必須	主な内容	（　　）	・支援内容が対策支援であることを確認。
【支援可能な範囲等】		必須	支援可能な業界（複数選択可）	自動車産業 半導体産業 その他製造業 建設業 防衛産業 電力産業 運輸・交通業 小売業 卸売業 サービス業 金融業 医療 教育 その他（　　） 該当なし	・その他に記載されている内容が選択肢と重複していないか確認。 ・その他に記載されている内容が業界かどうか確認。
		必須	支援可能な企業規模（複数選択可）	従業員 10 名以下 従業員 11-50 名 従業員 51-100 名 従業員 101-300 名 従業員 301 名以上 該当なし	－

3.3.2　実施結果

(1)　登録促進

見直した支援者リスト登録項目を基に、支援者リストへの登録受付・確認・リスト反映を行った。支援者リストへの登録促進策として、マネジメント指導ツール活用セミナー（全 3 回）における告知を実施した。

加えて実施した支援者リストへの登録促進活動と実際の登録状況については以下のとおり。

表 8　支援者リストへの登録促進活動と登録状況

実施日	実施内容
2025 年 12 月 3 日	マネジメント指導ツールセミナー（第 1・2 回）後のアンケート調査において支援者リストへの登録に関心を示した方を対象としたリスト登録受付開始の案内後、12 月 2～3 週は 50 件を超える新規登録があった。
2025 年 12 月 15 日～2026 年 1 月上旬	ケース演習の募集を開始し、リスト未登録者への登録を必須として申込みを受け付けた。ケース演習受講者 60 名のうち、令和 7 年度新規登録は 43 件、令和 6 年度登録 15 件（登録意向はあるが未登録 2 件）であった。
2026 年 2 月 5 日	マネジメント指導ツールセミナー（第 1～3 回）後のアンケート調査において支援者リスト登録に関心を示した方のうち、リスト未登録の方を対象にリスト登録のリマインドメールを発信。2 月上旬～中旬に 20 件弱の新規登録があった。

2026 年 2 月 16 日時点で令和 6 年度登録者（202 件）含め専門家は 340 件の登録（増加分 138 件）となった。

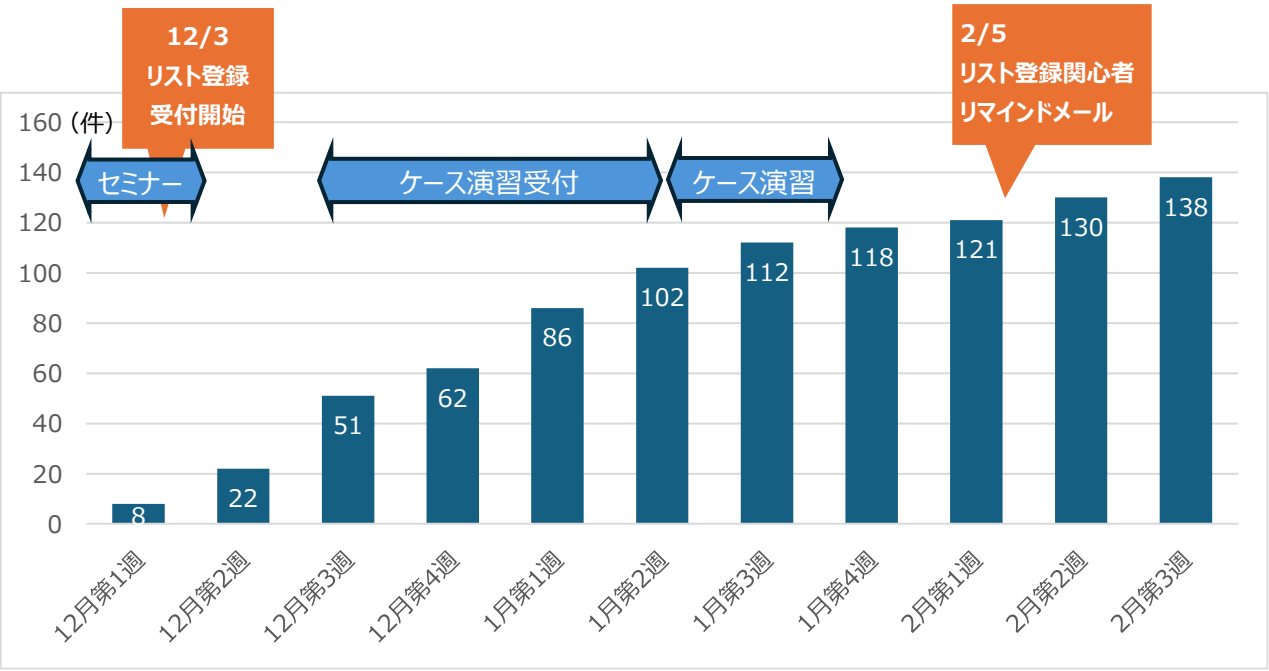


図 10　支援者リスト新規登録件数推移

(2)　登録受付作業における問題点

セキュリティ対策支援者リストへの登録受付作業においては、以下の問題点がみられた。そのため、対応可能な問題点については、改善策を 3.2 に示した「セキュリティ対策支援者リストの掲載・運用方法（案）」に反映した。

表 9　登録受付作業における問題点と改善策

No.	問題点	改善策
1	新規でリスト登録があった場合も、既に登録済みの方による更新の場合がある。	新規・更新で登録入口を分けているが、各々で登録されたデータが新規か更新か確認する作業フローを設定する。
2	登録内容を確認し修正すべき点があった場合、本人に確認を取る項目と、確認不要である項目を明確化する必要がある。	確認項目毎に本人確認の要否を記載する。
3	新規登録者において、セキスペ検索サイトで検索してもヒットしない場合の対応検討が必要である。	登録番号の記載ミスの場合は、正しい登録番号に修正を行う。それ以外の場合は、本人に確認を行う。
4	明示的にリスト掲載終了の連絡がないまま、セキスペ資格がなくなっている方のリスト掲載方針を定める必要がある。	登録データに「公開／非公開」のフラグを設け、本人に確認を行う。支援者リストへの掲載継続を希望する場合、登録セキスペの更新が確認でき次第、リストへの再表示を行う。

3.4 セキュリティ対策支援者リストの登録促進に関する考察

セキュリティ対策支援者リストの登録促進に関する考察を以下に示す。

本事業では、支援者リストの改善を図るとともに、セミナーを通じて支援者リストの周知を行い、新規の登録を促進した。登録促進に関しては、以下の課題があり、対応が必要と考えられる。

(1) 専門家リストの登録促進に向けて

・ 支援者リストの周知に加え登録行動を促す仕組み

セミナーへの参加率約 90%は非常に高く、登録セキスペの関心の高さが示されたとともに、満足度も「参考になった」96%と高かった。一方、活動意向は「登録して条件が合えば活動」(4 割)、「関心はあるが検討したい」(3 割) と高くはあるが、即時に登録可能であるのは限定的である。セミナーを通じ、支援者リストの認知・理解から関心までは可能であるが、登録サイトへの案内や登録方法や登録メリットの提示等を速やかに行う等、登録に向けたきっかけに繋げる仕組みが必要である。

・ 支援者リストの目的や登録・更新方法に関する周知

セミナーアンケートからは、支援者リストが認知されていない、あるいは登録・更新方法が理解されていない状況が伺えた。登録セキスペ個人（登録者や、登録が期待される情報処理安全確保支援士試験受験者・合格者）に対して、あるいは登録セキスペを抱える団体（情報処理安全確保支援士会等）を通じた、支援者リストの定期的な周知は、今後も必要と考えられる。また、リストの目的や登録・更新方法について IPA ウェブサイト等でわかりやすく丁寧に提示することが考えられる。

・ 支援者リストの掲載項目の見直し

自身の情報を支援者リストに掲載・公開することに対する懸念や細かな条件等を支援者リストに掲載したいという意見もあった。支援者リストの掲載項目については本事業で見直しを行ったが、今後も登録者や利用者のニーズ等を踏まえた見直しを行うことが望ましい。

(2) 専門家としての活動意欲の喚起に向けて

・ 登録セキスペとしての活動を阻害する要因の排除

セミナーアンケートからは、登録を阻害する要因は「スキル不安」「報酬」「責任（契約・賠償）」等が挙げられた。これは、後述するケース演習で出た意見とも整合しており、支援者リストの登録促進にあたっては、広報だけでなく、中小企業に対する登録セキスペ支援の環境整備や支援のための個人・チームとしての能力向上を合わせて検討する必要がある。具体的な解決策の要望としては以下が挙げられており、これらの方策については、今後検討の余地があると考えられる。

- ✓ スキル不安に関する課題への解決策
  経験が乏しい専門家の OJT 参加、能力や専門性が異なる専門家のペアやチームでの派遣、専門家からの相談窓口の設置　等

- ✓ 報酬に関する課題への解決策
  提供価値に見合った報酬目安の提示、対策費用が十分に確保できない中小企業に対する補助金等の支援　等
- ✓ 責任（契約・賠償）に関する課題への解決策
  取引における必要事項を記載した標準契約書・NDA 雛形の提示、専門家の責任範囲の明確化、トラブル時の一次対応窓口　等

・ 専門家としての案件獲得や業務負荷等の活動イメージの明確化

登録後にどれぐらいの頻度で案件が発生するか、相談が来ないのではないか、営業はどうするか等、登録から案件形成・獲得までの活動イメージが持ちづらいことが、活動を躊躇する原因となっている可能性がある。セミナーにおいても、専門家の実際の活動事例を聞きたいという意見が多数みられた。そのため、専門家側から得られる活動事例等の周知（セミナーやウェブサイトへのコンテンツ・動画掲載）や、案件の発生状況の公開（リスト情報や SCS 評価制度側から把握できる定量データの提示、商工会議所等における専門家紹介・マッチング実績情報の提示）等、活動状況に関する情報公開が有効と考えられる。

・ 副業や兼業、本業との競合による活動制約への対処

セミナーアンケートからは、副業・兼業の禁止や許可制、本業（SIer／コンサル等）との競合、公務員の制度制約等の活動制約に係る課題が挙げられた。このような課題は専門家側で解決することは困難であり、これらの状況にある専門家については、中小企業からの直接の相談に対して直接支援するというモデルが成立しない。そのため、このような立場にある専門家の活動形態を別の形で促進することも一案と考えられる。（法人経由の派遣、ボランティアとして市場を分けた活動、所属企業のグループ企業や取引先である中小企業への支援　等）

4. セキュリティマネジメント指導テーマの拡充

本事業では、中小企業のセキュリティ対応状況評価及び対策支援を行う人材確保を目的に、セキュリティマネジメント指導ツール（セキュリティアセスメント）を新規に作成するとともに、セキュリティアセスメントで必要となる情報セキュリティ監査のスキルについてケース演習を通じて登録セキスペを育成する実証を行い、受講者をセキュリティ対策支援者リストに登録した。

本章では、「マネジメント指導ツール（セキュリティアセスメント）作成」及び「セキュリティ専門家向けケース演習の開催」に関する実施結果について示す。

4.1 マネジメント指導ツール（セキュリティアセスメント）作成

セキュリティ対策支援者リストの掲載項目の一つであるセキュリティマネジメント指導テーマについて拡充するために、新たなマネジメント指導ツール（セキュリティアセスメント）を作成した。

4.1.1 実施内容

マネジメント指導ツール（セキュリティアセスメント）については、以下の目的及び作成方針とした。

- マネジメント指導ツール（セキュリティアセスメント）の目的
  - 登録セキスペ（専門家）が、アセスメントの基本的な考え方や知識を身に付け、企業の対策状況を確認し、適切な助言・指導ができること
  - サプライチェーン対策評価制度の三つ星（★3）評価を希望する企業に対して、要求事項・評価基準を達成することに向けた、適切な助言・指導ができること
- マネジメント指導ツール（セキュリティアセスメント）の作成方針
  - 他のマネジメント指導ツール（※）と同様の流れ・構成
    ※ 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
  - 3回の企業訪問を前提とした、専門家の実施事項、企業への依頼事項、関連様式を提示
  - 専門家に対して、「アセスメントや監査の考え方の理解」「企業における現状と対策が必要な箇所の把握」「今後、必要な対策を行うための考え方の理解」等を促進するもの（★３基準達成を保証するものではない）。
  - アセスメントの結果、必要な対策支援のために他のマネジメント指導ツールを活用することも想定

4.1.2 実施結果

マネジメント指導ツール（セキュリティアセスメント）に関する位置付け、構成、達成目標と成果物、全体構成は以下のとおり定めて作成した。

(1) マネジメント指導ツール（セキュリティアセスメント）の位置付け

マネジメント指導ツール（セキュリティアセスメント）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）」の説明資料として位置付けた。

これまで策定されたセキュリティマネジメント指導（テーマ別）では、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る。マネジメント指導ツール（セキュリティアセスメント）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するものとした。

セキュリティアセスメントの実施に際しては、SCS 評価制度の中で、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うものとした。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るものとなる。

なお、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る。

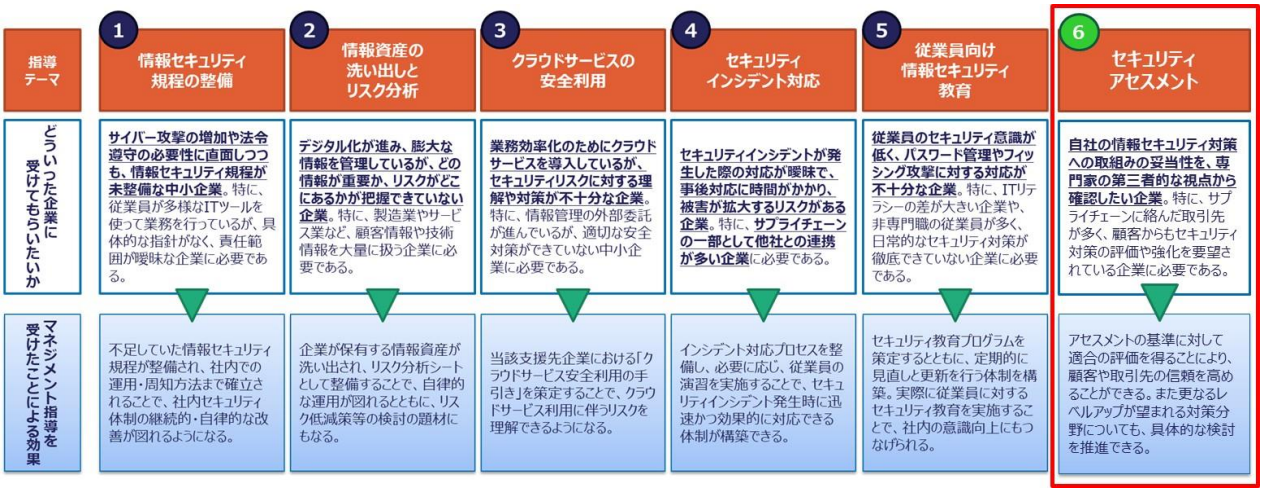


図 11　マネジメント指導ツール（セキュリティアセスメント）の位置付け

(2) マネジメント指導ツール（セキュリティアセスメント）の構成

マネジメント指導ツール（セキュリティアセスメント）の構成としては、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」を作成した。

「実施要領」には、各回の指導の内容（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た。

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た。

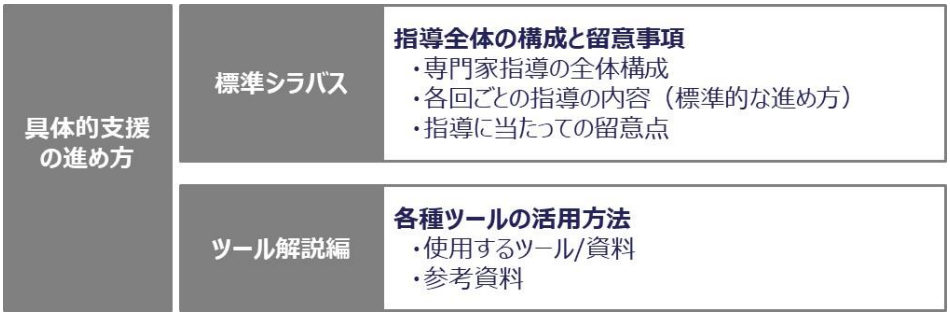


図 12　マネジメント指導ツール（セキュリティアセスメント）の構成

(3) マネジメント指導ツール（セキュリティアセスメント）による達成目標と成果物

「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、必要な助言を行うものとした。

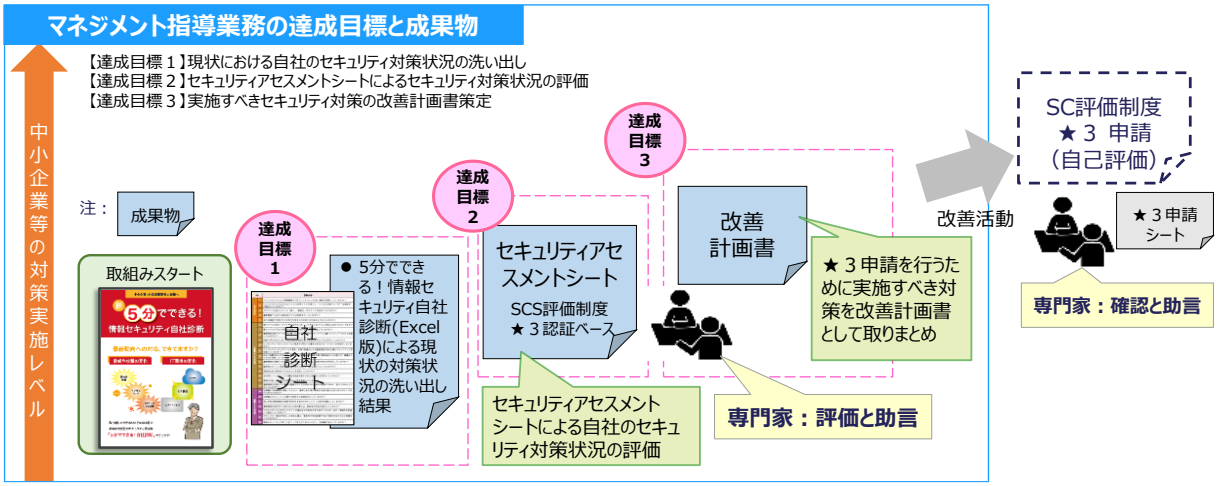
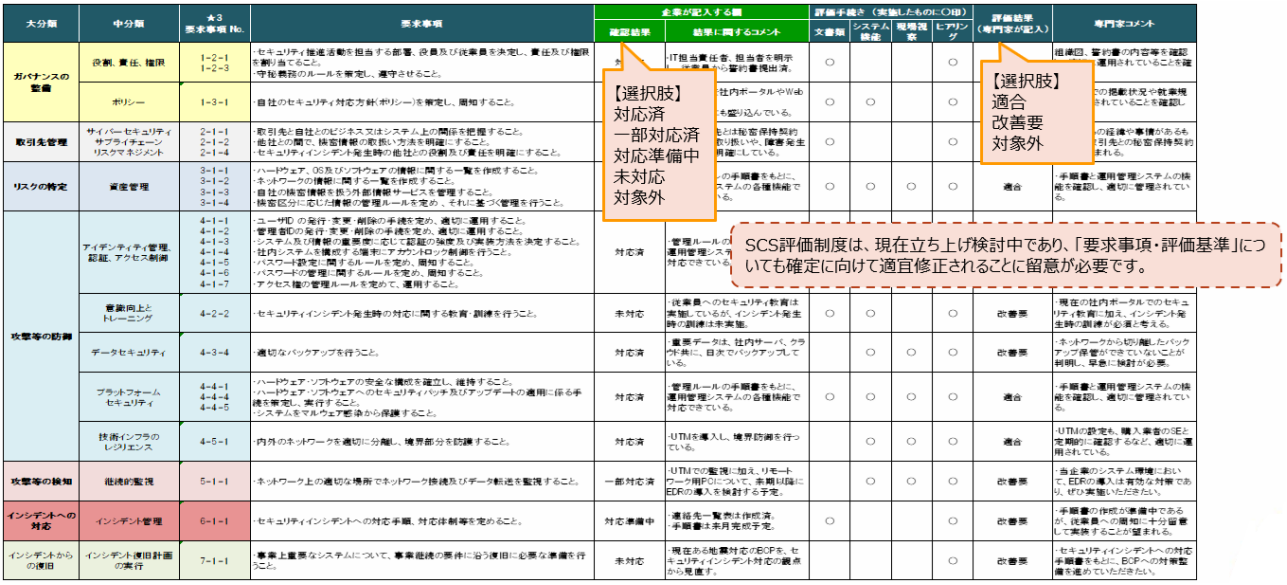


図 13　マネジメント指導ツール（セキュリティアセスメント）の達成目標と成果物

成果物の 1 つである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（2025 年 12 月時点）を基として作成した。マネジメント指導ツール作成時点では SCS 評価制度が立ち上げ検討中の段階であることから、要求事項・評価基準については詳細な項目変更の可能性も考慮し、中分類の括りで企業のセキュリティ対策内容を評価するものとした。

要求事項に基づき、指導先企業において、確認結果（対応済・一部対応済・対応準備中・未対応・対

象外）及び結果に関するコメントを記載し、記載内容を踏まえて専門家が評価手続き（文書類・システム機能・現場観察・ヒアリング）・評価結果・コメントを記載できるものとした。



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○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	システム検査	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。	対応済	・IT担当責任者、担当者を明示 ・従業員から誓約書提出済。	○			○		組織図、誓約書の内容等を確認 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。	対応済	・社内ポータルやWeb も盛り込んでいる。	○	○		○		の実施状況や教育現 されていることを確認。
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フローや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。	対応済	・とは秘密保持契約 取り扱いや、障害発生 用確にしている。	○			○		の経緯や事情があるも 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。	対応済	・の手順書をもとに、 ステムの各種機能で 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 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、購入事者の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施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。

図 14　セキュリティアセスメントシート（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るものである。

作成手順としては、第 2 回指導において、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する。そして、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する。第 3 回指導では、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、改善計画書を合意する。

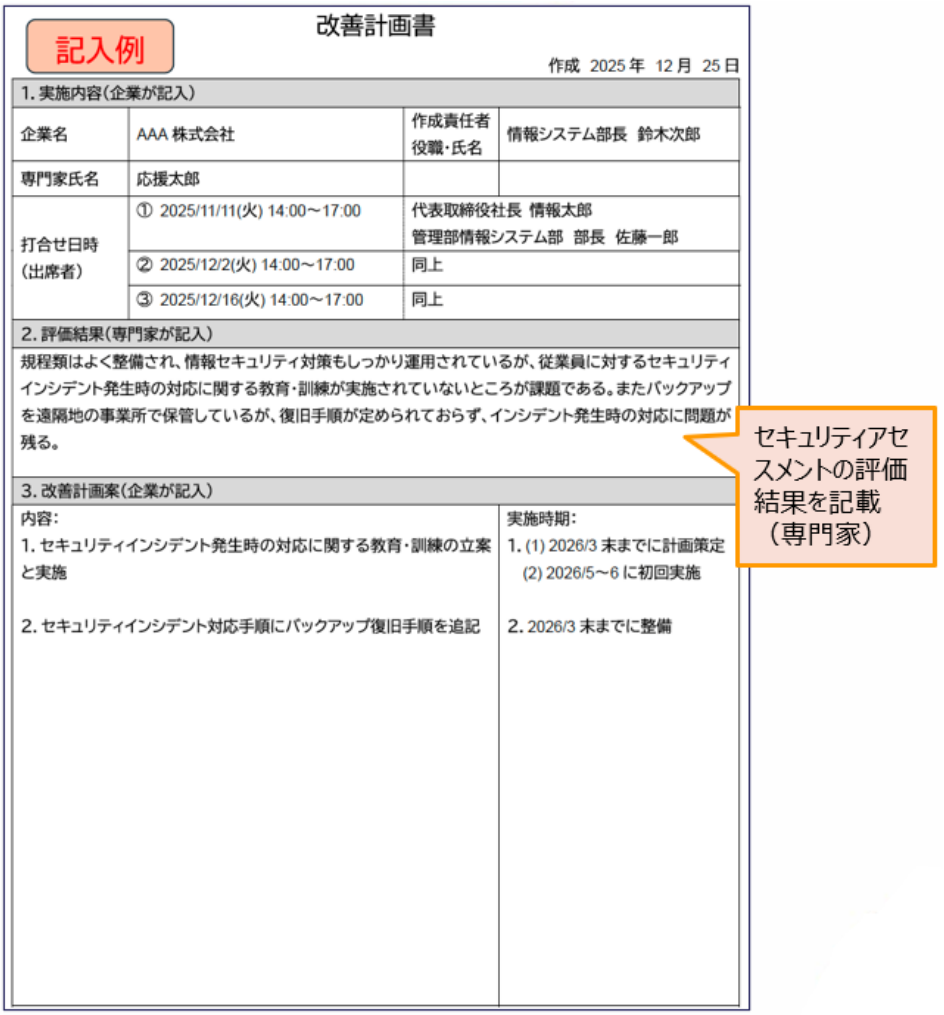


図 15　改善計画書（記入例）

(4)　専門家指導の全体構成

専門家の訪問については、他のセキュリティマネジメント指導ツールと同様、3 回を実施するものとした。1 回目の訪問は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、2 回目は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、3 回目は改善計画書の作成とし、全体を 2 か月程度で実施する内容とした。

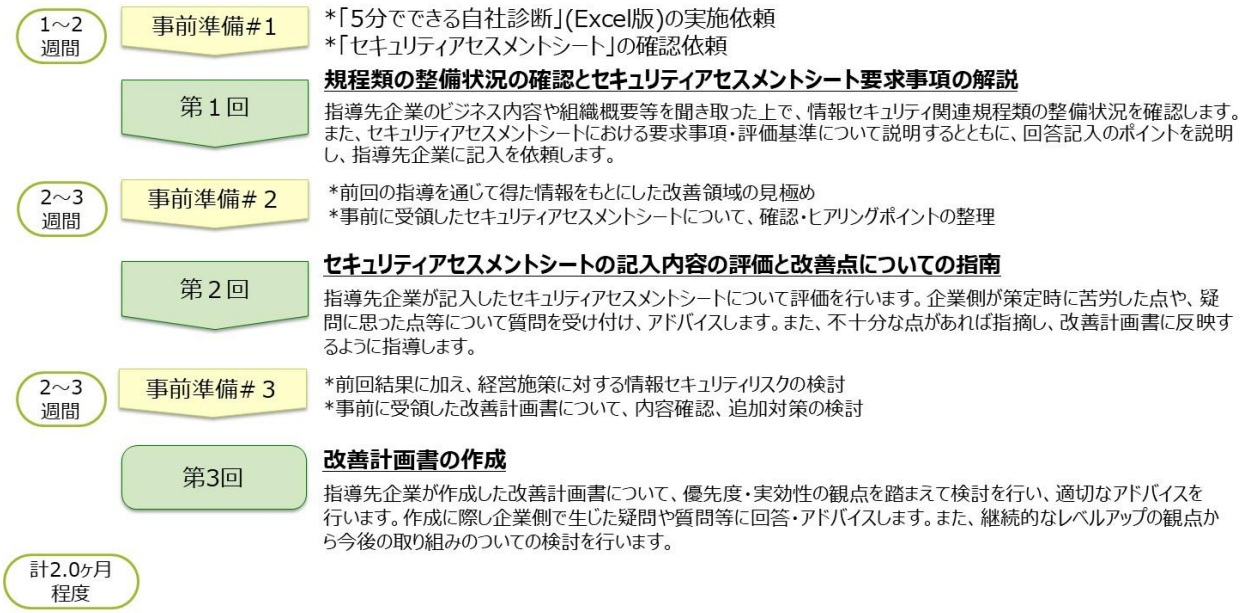


図 16　専門家指導の全体構成

(5) 情報セキュリティ監査の知識

情報セキュリティ監査については、専門家における基礎的な知識の理解を促すため、以下の内容を示した。

- 監査の主な分類と特徴
  助言型監査・保証型監査、セルフチェック・内部監査・外部監査
- 監査のプロセスと監査人の役割・責任
- 内部監査手続きの流れ、内部監査の事例（例：ウィルス対策ソフトの導入&運用）
- 監査における留意点（基準・会社のルール・運用実態の整合性、監査人として心掛けること）

4.2 セキュリティ専門家向けケース演習の開催

登録セキスペが中小企業のセキュリティ対応状況評価及び対策支援を行うために、セキュリティマネジメント指導ツール（セキュリティアセスメント）を活用したケース演習を実施し、受講者にセキュリティアセスメントで必要となる情報セキュリティ監査スキルを含めて教育する実証を行った。

4.2.1 実施内容

(1) ケース演習実施概要

ケース演習は、大阪・東京・名古屋の 3 箇所で各回 20 名程度を対象とし、ワークショップ形式（5 時間）で実施した。演習のファシリテーターは、経済産業省が令和 7 年度に実施した SCS 評価制度実証事業において、評価者として SCS 評価制度の評価基準案に基づく評価を実施した専門家が務めることで、より実践的な知見を提供できる演習とした。

ケース演習の実施概要を以下に示す。

表 10　セキュリティ専門家向けケース演習実施概要

項目	内容
目的	中小企業のセキュリティ対応状況評価及び対策支援を行う人材確保を目的に、登録セキスペがセキュリティアセスメントで必要となる情報セキュリティ監査スキルを含めた教育を実証する。
開催地域・回数	東京、名古屋、大阪等の 3 地域　計 3 回
形式・時間	ワークショップ形式　5 時間
構成	情報セキュリティ監査及びマネジメント指導ツール（セキュリティアセスメント）の解説等の講演（2 時間） グループワークによる演習（3 時間）
対象	中小企業のセキュリティ評価・対策支援を担当する登録セキスペ
参加要件	セキュリティ対策支援者リストへの登録

表 11　セキュリティ専門家向けケース演習　各回概要

	（1）大阪	（2）東京	（3）名古屋
開催日	2025 年 1 月 14 日（水） 10:00～16:00	2025 年 1 月 21 日（水） 10:00～16:00	2025 年 1 月 23 日（水） 10:00～16:00
会場	大阪商工会議所 402 号会議室-B （大阪府大阪市中央区本町橋 2-8）	東商カンファレンスルーム RoomB2 （東京都千代田区丸の内 3-2-2 丸の内二重橋ビル）	ツドイコ名駅東 カンファレンスセンター Room-D （愛知県名古屋市中村区名駅 3 丁目 21-7 名古屋三交ビル 2 階）
定員	最大 20 名	最大 20 名	最大 20 名
ファシリテーター	高谷 幸治 氏 （高谷経営支援事務所 代表）	松長 宏思 氏 （株式会社エッジプランニング 代表取締役）	松長 宏思 氏 （株式会社エッジプランニング 代表取締役）

(2) ケース演習カリキュラム

ケース演習のカリキュラムは、前半の講演（2 時間）と後半のグループワーク（3 時間）に分けて実施した。カリキュラムを以下に示す。

表 12　セキュリティ専門家向けケース演習カリキュラム

	内容	担当	時間	
講演	ケース演習受講にあたっての説明（スケジュール、注意事項等）	事務局	10分	2時間
	マネジメント指導ツール（セキュリティアセスメント）の解説等	ちば経営応援隊	1時間30分	
	サプライチェーン対策評価制度動向の説明	IPA	20分	
グループワーク	1.ファシリテーターからの説明 ・アイスブレイク、「演習の流れ」「ケース事例について」「評価にあたっての留意事項」の説明 ・事例企業（A社）についての説明 ・ケース1を使用した評価に関する説明 ・「３」検討前に「タイムキーパー、発表者、記録係、司会」を決定 ・「４」の発表テーマは、発表前にファシリテーターがグループを指名して決定	ファシリテーター	30分	3時間
	2.参加者各自によるケース2～7の評価実施		20分	
	3.各グループによるケース2～7の評価実施		40分	
	～ 休憩 ～		10分	
	4.グループ順にロールプレイ実施 ・企業担当者役：ファシリテータ、企業社長役：事務局、専門家役：各グループ発表者を設定 ・専門家役から企業側に再確認の項目について質問 ・グループ内で適合・不適合の最終評価を実施 ・専門家役から企業側に評価結果を伝達（不適合の項目について理由と改善策を提案） ・企業側からの質問に専門家役が回答 ・ファシリテータが講評を行い、解答を提示		60分＋予備10分 （15分×４）	
	5.ファシリテーターからの全体講評、質疑応答		10分	

前半の講演では、ケース演習受講にあたっての説明の後、「セキュリティマネジメント指導ツール（セキュリティアセスメント）に関する解説」（1 時間 30 分）及び「サプライチェーン対策評価制度動向の説明」（20 分）を実施した。マネジメント指導ツール（セキュリティアセスメント）の解説においては、マネジメント指導ツール（セキュリティアセスメント）に含まれる情報セキュリティ監査に関わる説明を充実し、受講者が情報セキュリティ監査に関わる基礎知識を理解できるよう試みた。

後半のグループワークでは、ファシリテーターからの評価に関わる説明（30 分）、各自の評価（20 分）、

グループによる評価（40 分）、休憩（10 分）を挟み、ロールプレイ（70 分）、全体講評・質疑応答（10 分）という流れで実施した。

(3) グループワークの流れ

グループワークは、SCS 評価制度における評価基準を利用し、事例企業を対象として、個別またはグループで実際に評価を実施するものとした。

グループワークは、以下に示す流れで実施した。

1	13:00 ～ 13:30	ファシリテーターからの説明	ファシリテータが参加者全員に向け、演習の流れ、ケース事例、評価にあたっての留意事項、事例企業、評価についての説明等を行います。	30分
2	13:30 ～ 13:50	参加者各自の評価	参加者各自でテーマ２から７の評価を実施します。	20分
3	13:50 ～ 14:30	グループ毎の評価	グループ毎にテーマ２から７の評価を実施します。	40分
	14:30 ～ 14:40	（休憩）		10分
4	14:40 ～ 15:50	ロールプレイ	企業担当者役（ファシリテータ）、企業社長役（ファシリテータ補佐）、専門家役（各グループ発表者）として、ロールプレイ形式で評価を実施します。	70分
5	15:50 ～ 16:00	全体講評・質疑応答	ファシリテータから全体講評、及び質疑応答を行います。	10分

図 17　グループワークの流れ

ファシリテーターからの説明事項は以下のとおりである。

① アイスブレイク、＜演習の流れ＞についての説明
② 【ケース事例について】の説明
③ 【評価にあたっての留意事項】の説明
④ 事例企業（A 社）についての説明
⑤ テーマ 1 を使用した評価についての説明
⑥ 「3. 各グループによるケース 2～7 の評価実施」検討前　「タイムキーパー、発表者、記録係、司会」の決定
⑦ 「4. グループ順にロールプレイ実施」における発表テーマは、発表前にファシリテーターがグループを指名して決定

②【ケース事例について】は、要求基準・評価事項等は SCS 評価制度に係る令和 7 年度実証事業の際のものを使用してケースを作成しており、制度開始時には内容が変更となる可能性がある点、また事例企業は実証参加企業（複数社）を参考に作成した架空の企業である点について説明を行った。

③【評価にあたっての留意事項】は、評価の実施方法として以下の点について説明を行った。

- 各評価基準について、「適合」又は「不適合」のいずれかを「評価結果」欄に記入。
- 「適合」と評価した場合には、補足すべき事項があれば「評価結果の補足」欄に記入。

- 「不適合」と評価した場合には、不適合の理由を「評価結果の補足」欄に記入。また、企業への評価結果のフィードバックの際に助言ができるように「適合」となるための改善案を検討。
- 情報不足のため「適合」・「不適合」の評価ができない場合には、一旦「再確認」として「評価結果の補足」欄に「再確認を要する事項」（追加質問）の内容を記載。また、どのような回答の場合に「適合」の評価になるかを検討。
- 「評価のためのガイダンス」に記載がある場合にはその内容を踏まえて評価を実施。

なお、利用する SCS 評価制度における評価基準は、テーマとして中項目を選定した。大項目レベルで様々なものを選択した。

- テーマ 1：1-2-3 守秘義務のルールを策定し、遵守させること。
- テーマ 2：2-1-1 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。
- テーマ 3：3-1-4 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。
- テーマ 4：4-1-1 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。
- テーマ 5：4-3-4 適切なバックアップを行うこと。
- テーマ 6：4-4-1 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。
- ケース 7：5-1-1 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。

テーマ 1 はファシリテーターが説明で利用し、テーマ 2～7 については個別評価の後、グループ評価を実施した。

ロールプレイについては、グループ毎に実施する様子を他の参加者がみながら学ぶ形式とした。実施事項は以下のとおりである。

- A グループから順にロールプレイを実施（15 分×4 グループ）　※発表者の入れ替わり（10 分）
- 企業担当者役：ファシリテーター、企業社長役：ファシリテーター補佐、専門家役：各グループの発表者
- 専門家役から企業側に再確認の項目について質問
- グループ内で適合・不適合の最終評価を実施
- 専門家役から企業側に評価結果を伝達（不適合の項目について理由と改善策を提案）
- 企業側からの質問に専門家役が回答
- ファシリテーターが講評を行い、模範回答を提示

(4) ケース演習資料

資料は、以下の構成で準備した。

表 13　ケース演習　資料構成

資料番号	資料名
―	マネジメント指導ツール　ケース演習　プログラム

資料 1-1	マネジメント指導ツール（セキュリティアセスメント）実施要領
資料 1-2	マネジメント指導ツール（セキュリティアセスメント）アセスメントシート
資料 1-3	マネジメント指導ツール（セキュリティアセスメント）改善計画書
資料 2-1	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)
資料 2-2	別添★3・★4 要求事項案及び評価基準案
資料 3-1	グループワーク資料：グループワークの進め方
資料 3-2	グループワーク資料：事例企業（A 社）
資料 3-3	グループワーク資料：テーマ資料

ケース演習の効果を高めるため、資料は、事前、当日、事後に分けて配布した。ケース演習当日は、PC を用いて評価作業を可能としたため、事前に電子ファイルを配布した。また、事前準備を行うことで参加者の前提知識に差が生じることを避けるため、グループワークの進め方や事例企業等の情報は当日配布とした。事後は復習や参照が可能となるよう、全ての資料を配布した。

表 14　セキュリティ専門家向けケース演習　配付資料

タイミング	配付資料
事前配布 （電子）	・マネジメント指導ツール（セキュリティアセスメント） - 実施要領（pdf）、アセスメントシート（excel）、改善計画書（word） ・サプライチェーン対策評価制度関連資料 - 制度概要説明資料（ppt）、要求事項・評価基準（excel） ・ケース演習資料 - ケース演習進め方 「演習の流れ」「ケース事例について」「評価にあたっての留意事項」「事例企業」 - ケース検討資料（7 ケース分） 1 枚目：企業からの回答を記載したシート 2 枚目：参加者が評価を記載するためのブランクシート
当日配布 （紙）	・ケース演習全体アジェンダ ・マネジメント指導ツール一式 ・サプライチェーン対策評価制度関連資料一式 ・ケース演習資料 - ケース演習進め方 - ケース検討資料（7 ケース分）１・２枚目
事後配布 （電子）	・ケース演習資料 - ケース検討資料（7 ケース分） 3 枚目：参加者が言及してほしい[再確認を要する事項]を記載したシート 4 枚目：想定される再確認の内容に対する回答を記載したシート 5 枚目：企業の回答（初回・再確認）と最終評価の模範解答を記載したシート

※　受講生には PC、及び可能であれば WiFi を用意いただき、事前配布した電子ファイルを持参いただく。（なお、会場においても WiFi 準備）
※　PC 利用が不可の方、WiFi が接続できないケースを想定し、資料は全て紙でも配布する。

レイアウトは、グループワークを実施するため、島型のテーブル配置とし、1 グループ 5 名程度×4

グループ（20 名）を目安として着席いただいた。各島に 1 台のモニタを設置し、グループでの共同作業や発表に利用いただいた。グループのメンバー構成は、個人での活動者と企業勤務者（副業）、企業支援の経験の豊富さ等のバランスを考慮の上、事前に設定した上で実施した。

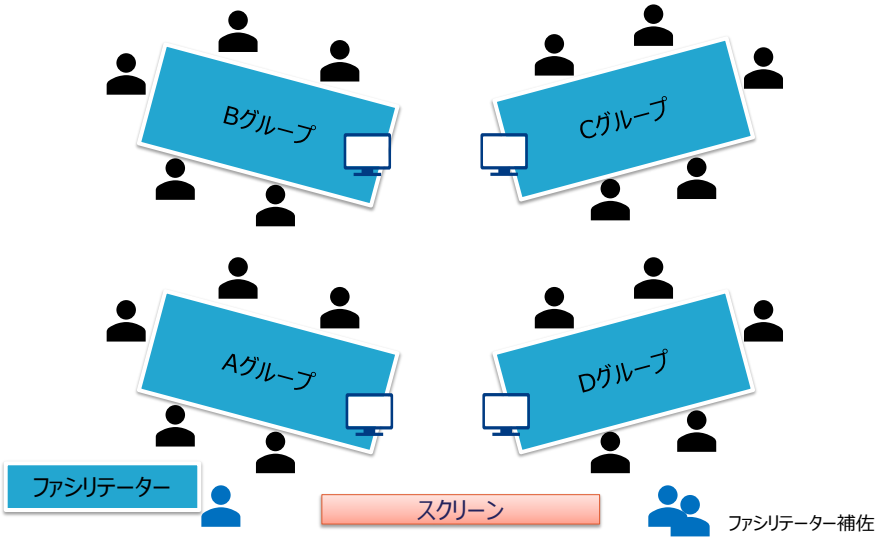


図 18　ケース演習　レイアウトイメージ

4.2.2　実施結果

ケース演習の実施結果は以下のとおり。大阪・東京・名古屋の 3 箇所で開催し、合計 60 名の方に参加いただいた。

表 15　セキュリティ専門家向けケース演習 参加人数

	（1）大阪	（2）東京	（3）名古屋
開催日	2025 年 1 月 14 日（水） 10:00～16:00	2025 年 1 月 21 日（水） 10:00～16:00	2025 年 1 月 23 日（水） 10:00～16:00
参加者	15 名	31 名	14 名

ケース演習後、参加者に対して実施したアンケート調査結果概要を以下に示す。

（1） 参加者属性について

ケース演習参加者におけるマネジメント指導ツールを利用した指導経験があるのは 2 割強、企業に対するアセスメント経験があるのは 3 割程度であった。

今回のケース演習の参加者は、申込者のうち「支援者リスト登録者」及び「マネジメント指導ツールを用いた指導が可能な者」を選定したが、実際にツールの利用や企業に対するアセスメント経験がある参加者は限定的であった。

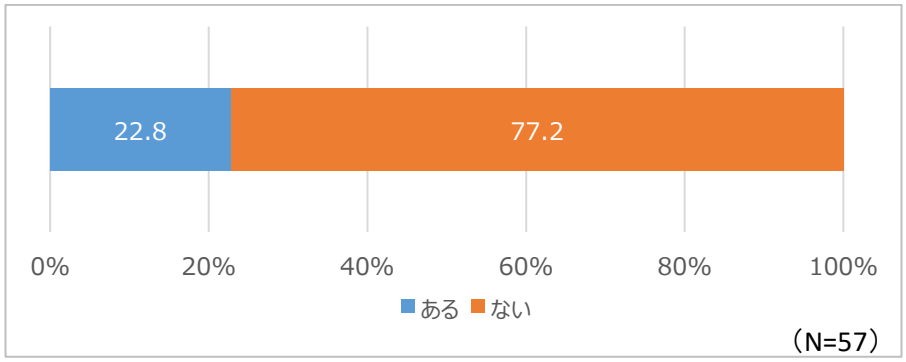


図 19　ケース演習参加者におけるマネジメント指導ツール利用経験

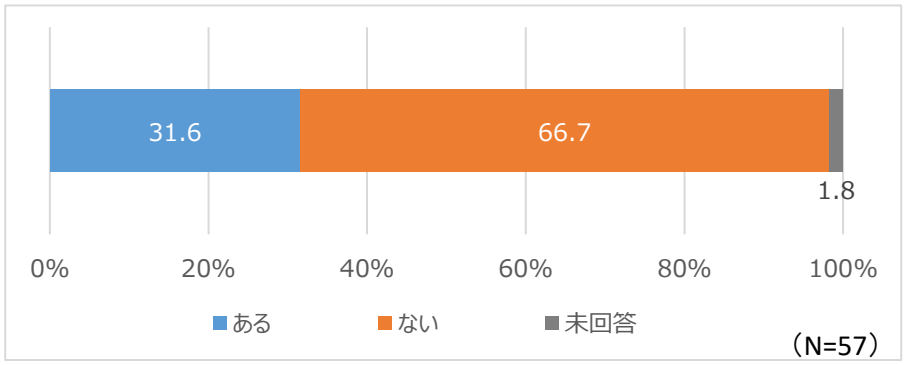


図 20　ケース演習参加者における企業に対するアセスメント経験

(2)　マネジメント指導ツール（セキュリティアセスメント）について

ケース演習参加者において、マネジメント指導ツール（セキュリティアセスメント）は 9 割以上が「理解できた」との回答であった。そのうち「大変よく理解できた」の回答傾向をみると、「専門家指導の 3 回の実施内容」は 7 割が「大変よく理解できた」との回答であったが、「セキュリティアセスメントシートの利用方法」及び「改善計画書の記載方法」は 5 割前後、「監査の方法」については 4 割弱に留まった。

マネジメント指導ツールの指導業務における有用性は、回答者の全てが「役立つと感じる」との回答であった。

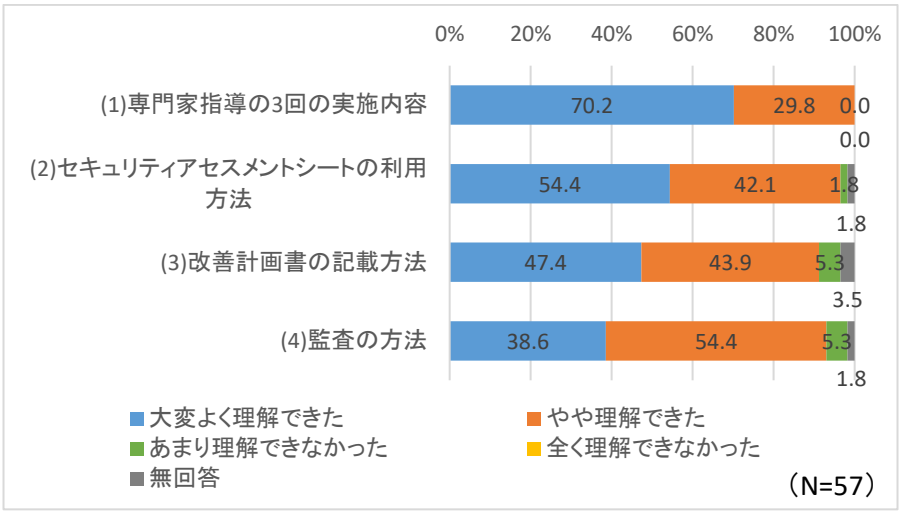


図 21　マネジメント指導ツール（セキュリティアセスメント）の理解

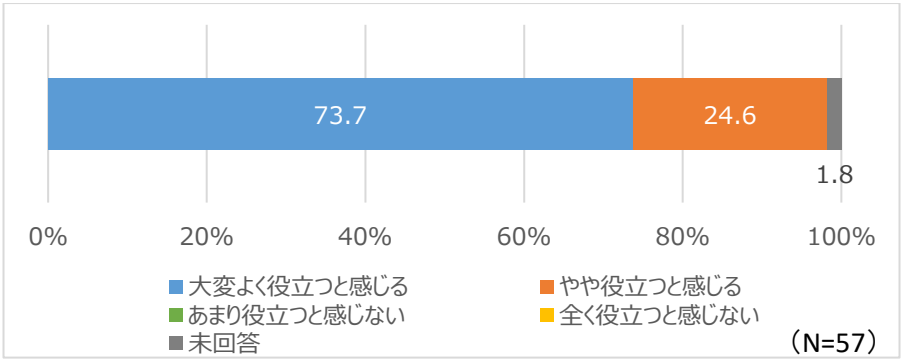


図 22　マネジメント指導ツールの指導業務における有用性

(3)　ケース演習について

ケース演習については、全てのプログラムについて、9 割以上が「有意義であった」との回答であった。特に「大変有意義であった」の回答をみると、「グループワーク（グループ評価）」（75.4%）、「マネジメント指導ツールの説明」（71.9%）の回答が多かった。

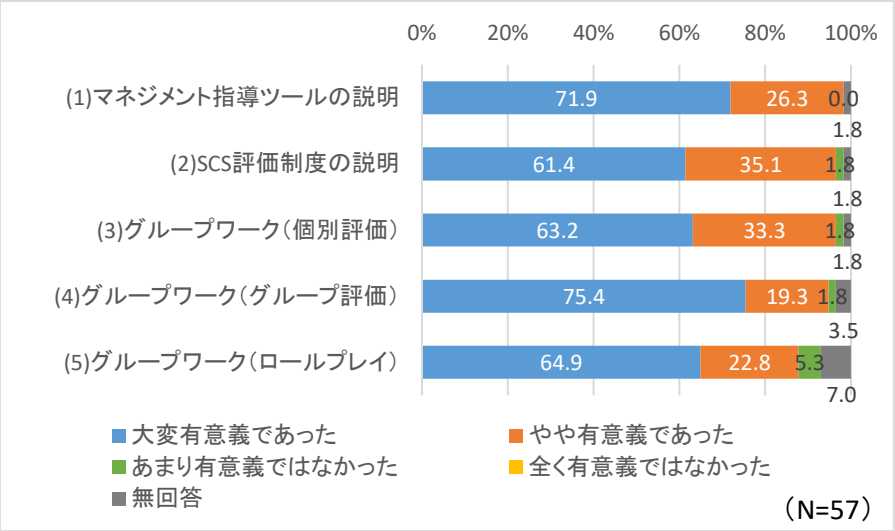


図 23　ケース演習の有意義性

また、グループワークで取り上げたいずれのテーマも 9 割以上が「理解できた」との回答であり、ケース演習（グループワーク）の課題の難易度は 5 割が「適切であった」だが、残りは「難しかった」との回答であった。

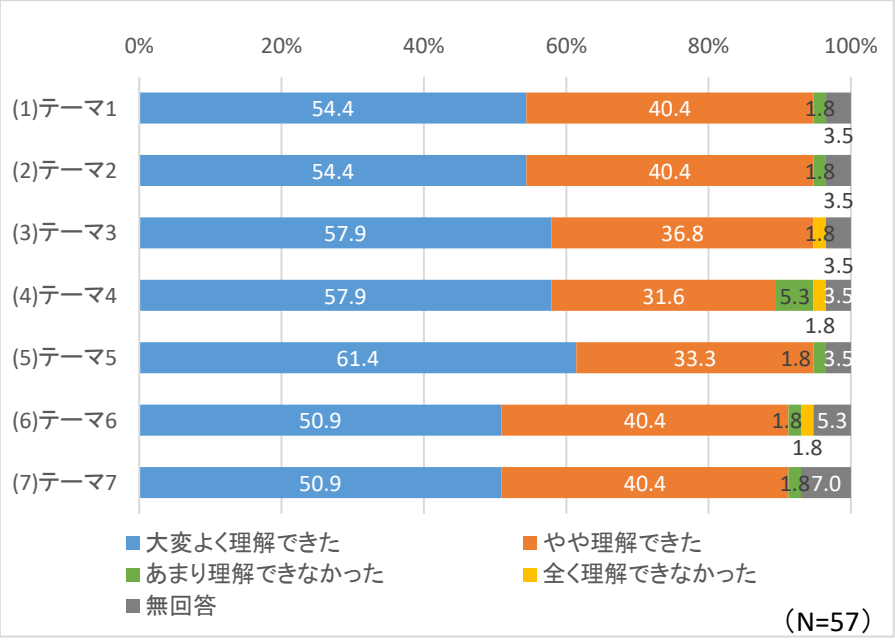


図 24　アセスメントテーマの理解度

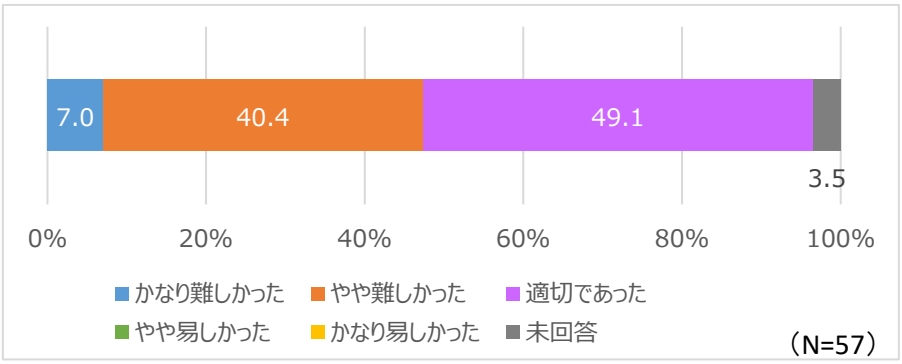


図 25　ケース演習の課題難易度

（4） 登録セキスペの人材活用について

本アンケートでは、ケース演習に関する質問とは別に、登録セキスペとして活動するにあたっての関連質問を設定した。

登録セキスペとして活動する際に連携を希望する相手は、「商工会議所」、「中小企業向け IT ベンダ、セキュリティベンダ」「自身と異なる専門を有する登録セキスペ」が 2 割程度以上であった。

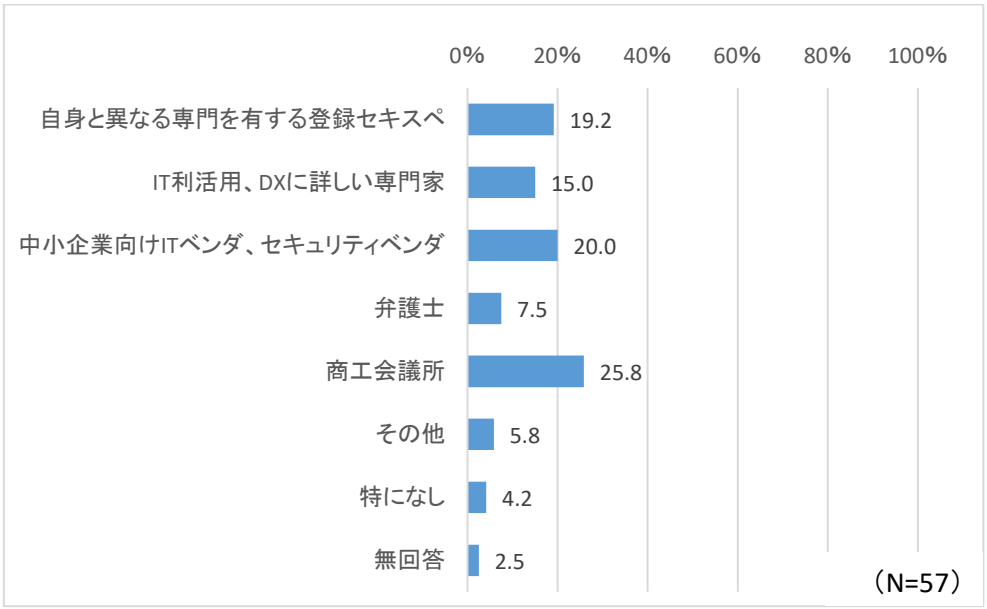


図 26　連携を希望する相手

その他、登録セキスペとして企業支援の活動を行うにあたっての自由記述に関する傾向は以下のとおりであった。

・　登録セキスペとして企業支援の活動を行うにあたっての課題

専門家自身の課題として「スキル・経験等の不足」、「副業・兼業との兼ね合い」等が挙げられた他、市場・環境の課題として「中小企業とのマッチング」、「報酬水準」、「契約・責任」、「継続的な支援」等が挙げられた。また、知名度の低さや資格維持コストの費用負担等制度の課題や、中小企業においてセキュリティが必須ではないという中小企業側の課題が挙げられた。指導ツール

に関する課題としては、判断基準や評価方法が専門家によって異なる点、専門家がツールを適切に使えているか確認する方法がない点が挙げられ、明確な評価基準の設定や評価ガイダンスとの整合性に対する要望があった。

- マネジメント指導ツールやケース演習の活用に向けた運営
  登録セキスペの活動に関する事例集等の「ツール・コンテンツ等の充実」、「活躍の場の拡大」、「研修の場の提供、充実」、「派遣や支援の一元化」等に関する意見が挙げられた。
- 国や IPA、その他団体からの支援や仕組みに対する要望
  「周知、広報の強化」、「マッチング、営業活動への支援」、「研修の場の提供、充実」、「ツール・コンテンツ等の充実」、「アセスメント、監査の向上」、「中小企業への支援」、「専門家への報酬支援」等が挙げられた。

マネジメント指導ツール（セキュリティアセスメント）を活用した活動は、7 割強が「希望する」 であり、「関心はあるが、検討したい」を加えると、9 割以上が活動に対して前向きという結果であった。

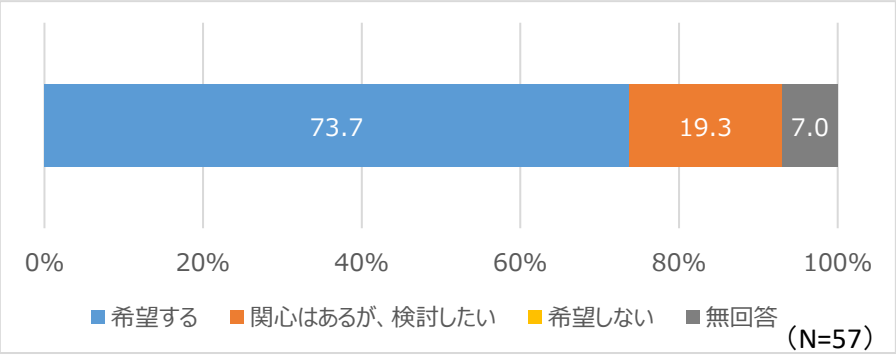


図 27　マネジメント指導ツール（セキュリティアセスメント）を活用した活動希望

4.2.3　参加者ヒアリング実施結果

ケース演習後に実施したアンケート調査において、追加でのヒアリング調査が可能と回答頂いた方 6 名に、登録セキスペとして活動状況・意向や活動するにあたっての課題等について意見を伺った。これらの結果を以下に示す。

- 中小企業に対するセキュリティ対策支援市場の未形成
  「中小企業のセキュリティ意識が低い」、「生産性・DX が優先され、セキュリティは後回し」、「製品やサービスを売り込む意欲が強いベンダへの不信感」、「補助金主導のセキュリティ導入による形骸化」等、中小企業に対するセキュリティ対策支援という市場はまだ形成されていない現状が伺えた。
- 専門家側の活動障壁
  「登録セキスペとしての知名度が低く仕事として成立しづらい」、「有償支援経験がなく自信がない」、「監査やアセスメント品質のばらつきが懸念」、「アセスメント後の署名の責任の重さや免責に関して不安」、「契約・責任のリスク」等、専門家として中小企業を支援する活動を行う際の障

壁、制度設計としての不足点が挙げられた。

- 中小企業と専門家のマッチング困難
  「支援士は仕事がないと言う」、「現場では専門家がいないと言う」、「支援者リストから選ぶのが難しい」、「支援者リストにおいてメールアドレスが公開されることへの抵抗がある」、「支援機関経由の方が機能するのではないか」等の意見が挙げられ、中小企業と専門家個人が直接マッチングするモデルの難しさが指摘された。
- 中小企業に対する専門家支援モデルの曖昧さ
  「アセスメントの質の統一性が気になる」、「SCS 評価制度における★3（自己評価）・★4（アセスメント）との違いが不明確」、「中小企業の支援に対してどこまで立ち入るのか分からない」、「(専門としてはベンダの協力が必要となる場合もあるが) ベンダとどう協働するのかが課題」、「中小企業を支援されてきた方等とのチーム型での支援が必要ではないか」との意見が挙げられ、専門家(登録セキスペ)としての役割定義が制度上も市場上も曖昧であり、支援体制や内容も様々となっていることで、専門家個人として活動しにくいことが伺えた。

なお、これらの課題を解決するために、情報処理安全確保支援士のビジネスモデルを確立するためのPoC[3]を進めている事例をヒアリング対象者の方から紹介いただいた。自ら仕事を作るという観点での他の士業／士業団体を参考とした制度設計、会社員として副業を期待する企業内支援士への案件提供、独立や副業を目指す支援士に対する登記や決算処理・確定申告等のレクチャー等に取り組んでおり、他の支援士における取組や政策面でも参考になる。

4.3 マネジメント指導テーマの拡充に関する考察

ケース演習を活用したセキュリティマネジメント指導ツール（セキュリティアセスメント）の拡充に関する考察を以下に示す。

(1) マネジメント指導ツールの活用に向けて

マネジメント指導ツールの理解度は 9 割以上、有用性も全員が「役立つ」と回答している。「大変よく理解できた」については、「監査の方法」が 4 割弱、「アセスメントシートの利用方法」「改善計画書の記載方法」が 5 割前後であった。ケース演習受講者におけるセキュリティアセスメントの実務経験者は 2～3 割程度であり、指導ツールの理解度と実務への適応力についてはギャップがあると考えられる。

そのため、実務における専門家の評価業務を支援するために、評価品質を一定に保つ施策が有効である。自由記述でも「専門家によって判断が異なる」「評価基準の明確化が必要」との意見がみられたことから、例えば以下のような方策が考えられる。

- ★3 要求事項毎の判断基準の具体化（評価ガイダンスや評価事例等の提供）
- 要求事項や評価基準を満たすエビデンスの例示、専門家コメント記載例等の提示

[3] PoC(Proof of Concept：概念実証)：新しい概念やアイデア等が実現可能か検証すること、そのために実施する実証やテスト等

・　想定 Q&A 集の整備

SCS 評価制度は今後具体的な内容が確定次第、その内容をマネジメント指導ツール（セキュリティアセスメント）にも反映させることが必要となる。SCS 評価制度で定められた要求事項や評価基準、あるいは付随する評価関連コンテンツと整合性を取る形で、指導ツールを利用した評価業務の品質を保つための支援策・サポートコンテンツを整備することが望ましい。

(2) マネジメント指導ツール活用のための研修機会やコンテンツの充実について

ケース演習について有意義と回答したのは 9 割以上であった。特にグループワークについては「大変有意義」との回答が 7 割を超えたものの、難易度については「難しかった」が約半数であった。グループメンバーは企業支援実績が様々となるよう構成したが、グループ内でも受講生のレベル差があった可能性がある。この結果については、マネジメント指導ツール（セキュリティアセスメント）を用いた活動意欲はあるが、実際の評価業務に対して難しさと感じている専門家が多いことが考えられる。

専門家におけるセキュリティ監査やアセスメントの能力を、より実務に即した形で高めるために、以下のような方策が考えられる。

・　レベル別研修体系の構築

今回のケース演習は、一定程度の経験・知見がある層を対象に実施したが、今後は実務経験が全く無い方から経験が豊富な方まで様々な専門家を対象にすることが想定される。そのため、各々の能力に沿ってレベルアップを図るのであれば、未経験者・指導経験者・★3 評価複数回経験者等、実務に関わるレベル別に研修を用意することが効果的である。アンケート結果からもわかるように、セキュリティ監査やアセスメントについては様々なケースに対する判断が必要となるため、グループ形式で受講生同士が知見や意見を共有するような手法が有効であると考えられる。

・　研修素材（テーマやケース等）の拡充

今回のケース演習では、1 つの企業（ケース）、7 つの要求事項（テーマ）を素材として評価に関するグループワークを実施した。アンケート結果からは、グループでの評価を有意義とする回答が多く、専門家自身が評価に関わる様々な経験や知見を蓄積することが、実務において適切な評価を実施するに有効と考えられる。そのため、今後、研修において素材とするテーマの拡充や、対象とするケース（業種や規模、対策状況等）のバリエーション拡大等が有効と考えられる。

・　評価事例の収集・提供

評価に関わる経験や知見を専門家が蓄積するために、研修として専門家同士が意見交換を行う場を充実することは有効だが、コンテンツとして専門家に提供することも有効と考えられる。例えば、適合／不適合の評価事例、改善計画書のサンプル事例等、評価事例に関するコンテンツを収集・蓄積し、専門家に対して提供することで、専門家の活動促進やレベルアップにつながることが期待できる。

5. まとめ

本章では、本事業に関する総括及び今後の取組に向けた提言を示す。

5.1 総括

本事業は、令和 6 年度事業で把握した中小企業へのセキュリティ対策支援ニーズを踏まえ、「セキュリティ対策支援者リスト」の整備を中核として（1）リストの活用促進、（2）リストへの登録促進、（3）セキュリティマネジメント指導テーマ（セキュリティアセスメント）の拡充を一体的に実施した。その結果、リストの試行公開と運用手順の標準化、リスト登録者数の拡大、監査・アセスメントの知見を有する人材の育成支援コンテンツ整備と育成・リスト登録までを実施することができた。今後、支援者リストを活用した中小企業支援基盤を充実するためには、制度面・運用面の一層の整備が必要である。

5.1.1 セキュリティ対策支援者リストの活用促進

令和 6 年度の「登録セキスペアクティブリスト（試作版）」を改善し、支援者リストとして試行公開するとともに、登録・変更・終了から HTML 公開までの業務フローを標準化し、Excel ベースでマスタ生成・公開チェックを行うリスト掲載・運用手順（案）を整備した。これは令和 9 年度のシステム化を見据えた試行段階として、リスト公開と更新を継続可能にする下支えとなった。

本格運用に向けては、（1）登録セキスペ有効期限切れ後の継続支援を含む運用（再表示手順等）の整備、（2）情報の鮮度維持（定期更新の強化、最終更新日時の明示等）と活動実態の反映（アクティブ度・対応可否等の指標化）、（3）検索軸の拡充（実績、対応内容、費用目安、オンライン可否等）と、（4）中小企業以外（支援機関、地域金融機関、補助金・制度手続等）での利用シーンの具体化と周知が課題である。単なる専門家掲載リストに留まらず、利用者が安心して効率的に専門家を選定できるリストへの充実が求められる

5.1.2 セキュリティ対策支援者リストの登録促進

全登録セキスペを対象にウェビナー形式の「セキュリティマネジメント指導ツール活用セミナー」を 3 回開催し、合計申込 2,134 名・参加 1,928 名（参加率約 90%）と高い関心を獲得した。セミナー参加者の 9 割以上が「参考になった」と回答し、FAQ・アーカイブ・資料公開によりコンテンツ資産化を行った。登録促進策（関心層への案内、ケース演習申込時の登録必須化、リマインドメール等）により登録者は増加し、2026 年 2 月 16 日時点で令和 6 年度登録者 202 件を含む 340 件の登録に到達した。また、登録受付における運用課題を整理し、リスト掲載・運用方法（案）に反映した。

セミナーは、支援者リストの認知・理解・関心までの喚起には有効である一方、リスト登録・活動への転換には、（1）登録行動を後押しする導線（分かりやすい手順提示、登録・更新の UX 改善、周知の定期化）、（2）活動阻害要因（スキル不安・報酬・契約／責任）の解消策の提示、（3）案件発生状況や業務負荷の見える化（活動事例・定量情報の公開）等が必要である。特に副業制約や本業競合等の構造要

因があるため、個人と中小企業の直接マッチングだけに依拠せず、支援機関経由の派遣、チーム型支援、法人経由の活動等、複線的な活動形態の設計が重要である。

5.1.3　セキュリティマネジメント指導テーマの拡充

中小企業の対策状況評価ニーズに対応するため、SCS 評価制度★3 の要求事項・評価基準を参照した「マネジメント指導ツール（セキュリティアセスメント）」を新規作成した。また、「マネジメント指導ツール（セキュリティアセスメント）」を活用したケース演習を大阪・東京・名古屋の 3 会場で実施し、合計 60 名が参加した。アンケートではツールの理解度は 9 割以上、有用性は全員が「役立つ」と回答し、ケース演習も 9 割以上が有意義と回答した。一方、理解と実務適応のギャップが示唆された。参加者に向けたヒアリングにおいても、専門家の中小企業への支援市場の未形成、専門家の活動障壁、中小企業と専門家のマッチングの困難さ、専門家の支援モデルの曖昧さ等の課題が明確化した。

マネジメント指導ツールの普及と実務展開には、(1) 評価品質の均質化（判断基準の具体化、エビデンス例、コメント例、Q&A、評価事例の蓄積）、(2) レベル別研修体系の構築と研修素材の拡充（業種・規模・対策状況のバリエーション拡大）、(3) SCS 評価制度の確定内容との整合確保（要求事項・評価関連コンテンツとの一貫性）が必要である。

5.2 今後の取組に向けた提言

本事業により、支援者リストを軸とした中小企業のセキュリティ対策支援の基盤は整備されつつあるが、今後に向けては登録者数の拡大に加え、稼働の拡大についても検討する必要があると考えられる。そのため、今後の取組は（1）支援者リストの信頼性・運用の継続確保、（2）登録セキスペの活動環境整備、（3）アセスメントの品質確保と制度整合、（4）活動までの導線改善やマッチング困難の解消が有効と考えられる。

5.2.1 支援者リストの信頼性・運用の継続確保

支援者リストについては、専門家を掲載するのみならず、より活用を促す方針で運用・品質管理を行うことが有効である。

具体的には、登録情報の鮮度や信頼性の担保のために、各情報の最終更新日時の明示、年次更新の徹底、未更新者の表示制御、活動実態（直近支援有無、対応可能分野等）の可視化により、利用者が安心して効率的に専門家を選べるリストに更新していくことが考えられる。

また、登録セキスペの有効期限管理と継続支援を両立し、登録セキスペ資格の有効期限切れ後の連絡・再表示手順等を運用として明確化し、リストの品質を確保するとともに活動意欲ある専門家がリストから離脱しない仕組みを整えることも有効である。

さらに、利用者の利便性や様々なニーズに応えるために、リスト検索軸の拡充を検討し、令和 9 年度のシステム化を機にデータ構造を整えることが肝要である。

5.2.2 登録セキスペの活動環境整備

支援者リストへの登録を躊躇する要因として、登録セキスペとしての活動阻害要因に対して包括的に対応することが必要である。活動阻害要因としては、スキル不安、報酬への懸念、契約・責任、活動形態の制約（副業・兼業、本業との競合）が挙げられる。

専門家のスキル不安に対しては、能力形成の機会として、OJT 機会の提供、ペアやチームでの派遣による支援、相談窓口等を制度化し、経験が少ない場合も支援実務に入れる環境を整えることが考えられる。

報酬水準や費用に対する懸念については、報酬目安や標準工数モデルの提示、補助金制度等の活用による中小企業の支払能力と専門家の提供価値のギャップ緩和、ボランティアによる活動場所の棲み分け等が考えられる。

中小企業との契約・責任の整理については、標準契約書・NDA 雛形の提供、責任範囲の明確化、トラブル時の対応窓口の整備等により、専門家が過大なリスクを負わずに活動できる基盤を作ることが有効である。

また、専門家個人では解決できない副業・兼業等の阻害要因に対しては、法人経由の派遣、ボランティア枠の設置、所属企業のグループ企業や取引先への支援等、様々な参加形態の設計について、今後の検討が必要である。

5.2.3　アセスメントの品質確保と制度整合

マネジメント指導ツール（セキュリティアセスメント）の活用にあたっては、アセスメントにおける判断のばらつきを可能な限りなくし、専門家のアセスメントに対する取組やすさを向上するとともに、アセスメントの品質を確保し制度の信頼性を維持する必要がある。

評価品質の均質化のためには、判断基準の具体化、評価エビデンス例や専門家コメント例の提示、適合／不適合の評価事例、改善計画書サンプル等を整備し、評価のばらつきを解消することが必要である。

また、専門家のアセスメント能力を育成するための研修体系の充実については、未経験者～経験者までを対象としたレベル別研修、業種・規模別ケースやテーマ等研修素材の拡充が有効である。継続的に能力を高めるという点では、様々なレベルの研修機会の提供に加え、コミュニティの要素を含めた定期的な勉強会、交流会等の場の提供も考えられる。

なお、マネジメント指導ツール（セキュリティアセスメント）は、SCS 評価制度と連動していることから、制度確定後から運用段階においても、継続的に整合性を図りながら整備する必要がある。制度確定後は要求事項や評価基準等の内容を速やかに指導ツールへ反映し、評価関連コンテンツとの一貫性を担保することが求められる。

5.2.4　活動までの導線改善やマッチング困難の解消

専門家のリストへの関心から実際の登録・活動につなげるための円滑な導線確立と、専門家と中小企業のマッチング支援強化により、専門家として活動可能な母数を増やすことが重要である。

リストへの登録導線の改善については、登録／更新手順の簡素化や定期的なリスト周知に加え、セミナー視聴等イベント直後の登録誘導等により、関心を持つ層を登録に促す。

その際に、専門家としての活動イメージを提供することにより、活動への動機づけとすることが有効である。例えば、活動事例の継続的な発信や、案件発生状況やマッチング実績等の定量情報提示により、登録後の案件獲得に関する不安を低減する。

また、マッチング強化として、商工会議所等の支援機関における相談窓口でのリスト活用を標準化し、信頼できる組織が専門家の選定・紹介を担うことで、専門家個人と中小企業の直接マッチングの困難さを解消する。セキュリティ以外の専門を有する専門家や専門家団体との連携により、協力して案件に対応する等の機会を創出することも検討が必要であろう。

別紙 1. マネジメント指導ツール セミナー受講アンケート結果

本章では、マネジメント指導ツール セミナー受講アンケート結果を示す。

(1) セミナー内容の参考度

① セキュリティマネジメント指導ツールの説明

「セキュリティマネジメント指導ツールの説明」については、97.7%が参考になったとの回答であった。

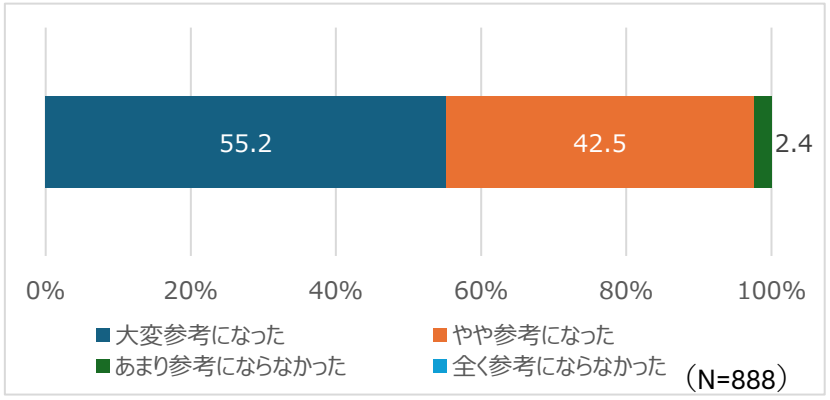


図 28 セキュリティマネジメント指導ツールの説明（IPA）

② ゲストスピーカーによる指導ツール活用事例の紹介

ゲストスピーカーによる「指導ツール活用事例の紹介」については、97.7%が参考になったとの回答であった。

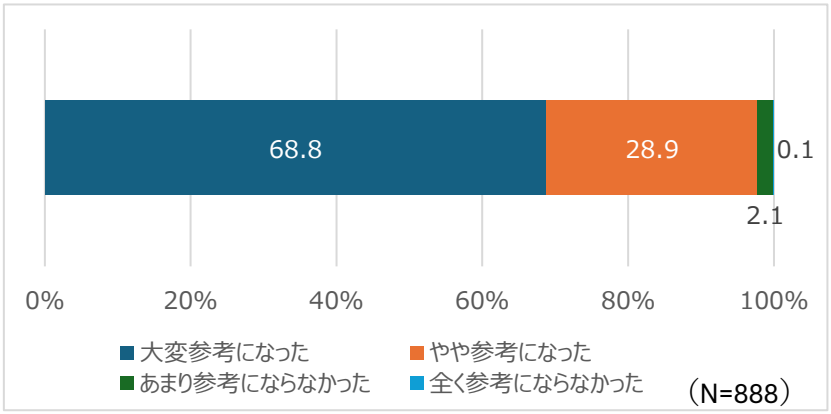


図 29 ゲストスピーカーによる指導ツール活用事例の紹介

③ セキュリティ専門家リストの登録促進

「セキュリティ専門家リストの登録促進」については、92.7%が参考になったとの回答であった。

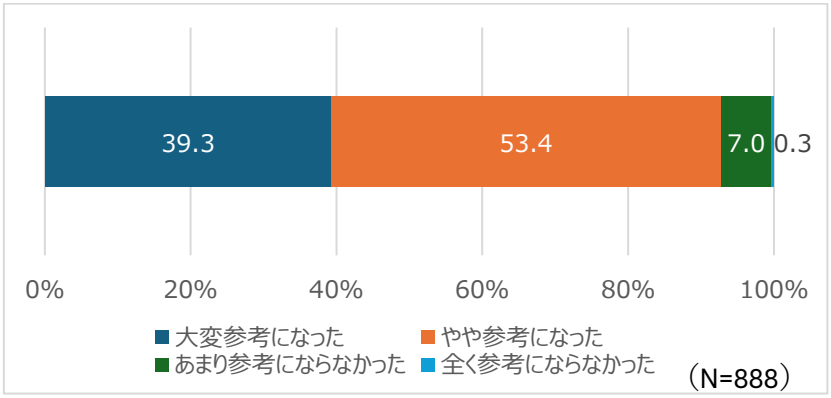


図 30　セキュリティ専門家リストの登録促進

④　セミナー全体

セミナー全体については、96.0%が参考になったとの回答であった。

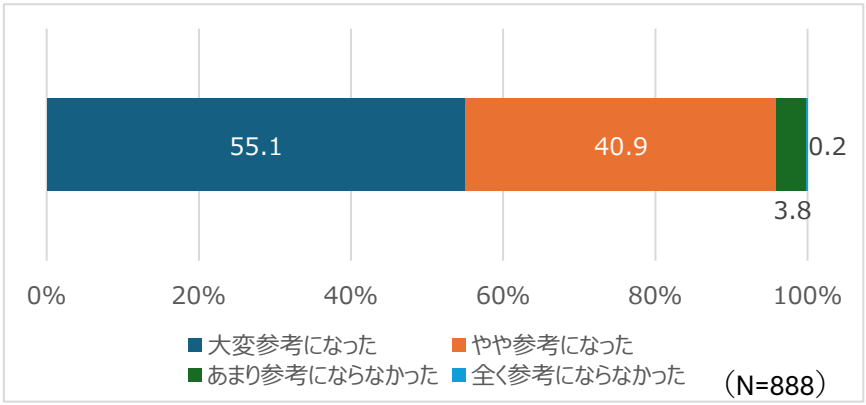


図 31　セミナー全体の満足度

(2)　専門家リスト（支援者リスト）への登録・活動意向

専門家リスト（支援者リスト）への登録・活動意向については、「専門家リストに登録して、条件が合えば活動したい」が 40.1%、「関心はあるが、少し検討や確認してから考えたい」が 33.1%であった。

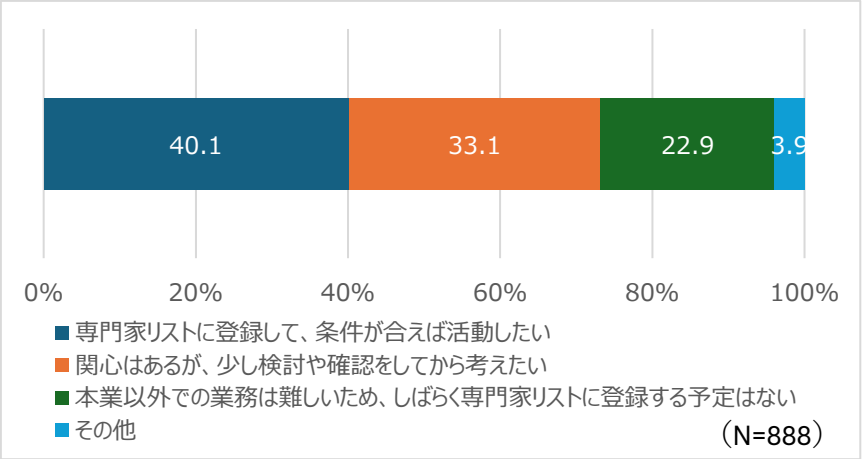


図 32　専門家リストへの登録・活動意向

(3)　登録セキスペの人材活用に関する意見（自由記述）

①　専門家が中小企業を支援するための課題

専門家が中小企業を支援するための課題について、主な意見を示す。

表 16　専門家が中小企業を支援するための課題

	項目	主な意見
1-1	スキル・経験等の不足	・　指導経験がなく、支援ができるか不安。 ・　知識に偏りがあり、全体を支援できるか自信がない。 ・　研修や OJT の機会がほしい。
1-2	副業・本業との競合の課題	・　副業禁止、会社の許可が必要。 ・　IT 企業・SIer・コンサル等勤務のため、本業と競合する。 ・　公務員であり、勤務時間内での活動を認めたり、特別休暇制度等があるとよい。
1-3	リアルな活動のイメージしにくさ	・　リストに登録したら、どれぐらいの頻度で案件が来るのかわからない。 ・　いつまでも声がかからないのでは。営業はどのように実施するのか。
2-1	報酬水準	・　中小企業側の希望する価格帯と専門家側の希望する報酬水準が見合わない。 ・　ボランティアとしてなら考えられる。（ボランティアとして登録すると既登録者と競合） ・　副業よりプロボノに近いのではないか。
2-2	契約・責任、リスク	・　契約、NDA 等は自身で締結するのか。 ・　トラブルが発生した場合はどのように対応したらよいか。 ・　無償に近い謝金で無限定の保証や賠償責任まで負うのは割に合わない。
2-3	サポート、相談窓口	・　自身で解決できない相談が来た場合、どこに相談すればよいか。 ・　チームで支援できる仕組みがあった方がよい。 ・　若手や未経験者が OJT 的に参加できるようにしてほしい。

	項目	主な意見
3-1	中小企業側の意識・制度面の課題	・ セキュリティをコストと見ている企業が多い。 ・ 無料・1 万円未満を望む企業の割合が高い。 ・ 経営課題が山積みで、セキュリティは後回しとなっている。
4-1	マネジメント指導ツールの課題	・ 商用利用や社内共有など、利用ルールを明確にしてほしい。 ・ 事例やサンプルがほしい。小規模事業者・診療所などの小規模組織に向けたサンプルがほしい。 ・ ツール活用手順や一連の支援プロセスの動画、体験できる講座がほしい。 ・ ツールを使った演習を実践講習に組み込んでほしい。

② 専門家リスト登録に関する課題

専門家リストに関する課題について、主な意見を示す。

表 17 専門家リスト登録に関する課題

	項目	主な意見
1-1	登録方法等のわかりにくさ	・ そもそも専門家リストを知らなかった。 ・ 登録方法がわからない。 ・ セキュリティプレゼンターとは異なるのか。 ・ 既に登録済みであるが、内容の修正方法がわからない。
1-2	セキュリティ・プライバシーへの懸念、公開情報への要望	・ メールアドレスが公開され、スパムの標的になる。 ・ 氏名や連絡先が公開されることに抵抗がある。 ・ 対応可能地域、ボランティア可否、オンラインのみ等の条件を掲載したいニーズがある。

別紙 2. マネジメント指導ツール ケース演習アンケート結果

本章では、マネジメント指導ツール ケース演習アンケート結果を示す。

(1) 参加者属性

① 参加した回

ケース演習には 3 回合計で 60 名の方に参加いただき、そのうち 57 名から回答を得た。回答者のうち、1/14（水）大阪が 15 名（26.3%）、1/21（水）東京が 31 名（50.9%）、1/23（金）名古屋が 14 名（22.8%）であった。

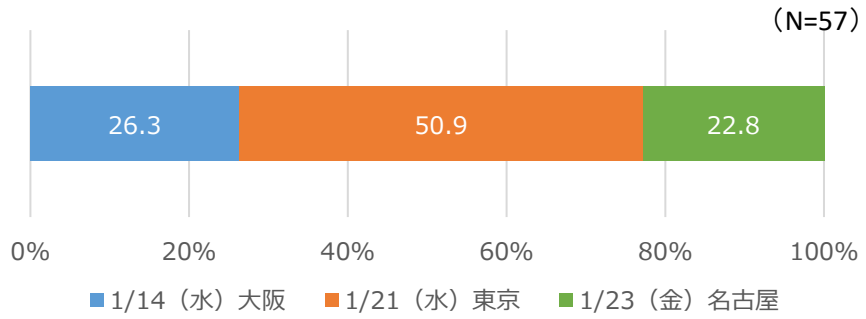


図 33 参加した回

② マネジメント指導ツールを利用した指導経験

マネジメント指導ツールを利用した指導経験については、経験が「ある」が 22.8%、経験が「ない」が 77.2%であった。

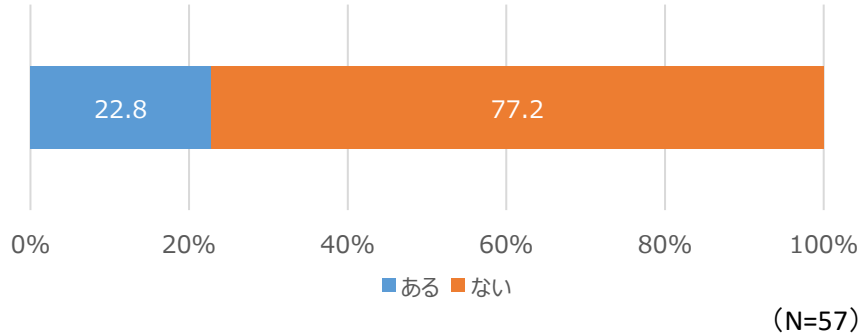


図 34 マネジメント指導ツールを利用した指導経験

③ 利用経験のあるマネジメント指導ツール

利用経験のあるマネジメント指導ツールについては、「情報セキュリティ規定の整備」が 92.3%、「従業員向け情報セキュリティ教育」が 92.3%であった。

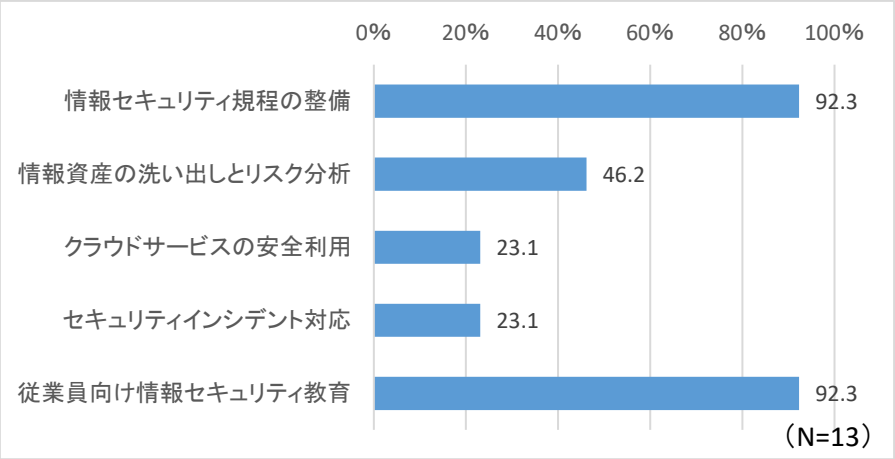


図 35　利用経験のあるマネジメント指導ツール

④　企業に対するアセスメント経験

企業に対するアセスメント経験については、経験が「ある」が 31.6%、経験が「ない」が 66.7%であった。

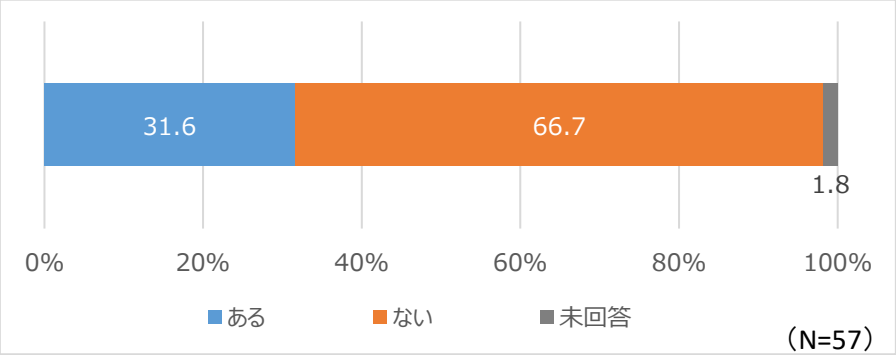


図 36　企業に対するアセスメント経験

(2)　マネジメント指導ツール（セキュリティアセスメント）

①　マネジメント指導ツール（セキュリティアセスメント）の理解度

マネジメント指導ツール（セキュリティアセスメント）の理解については、9 割以上が理解できたとの回答であった。

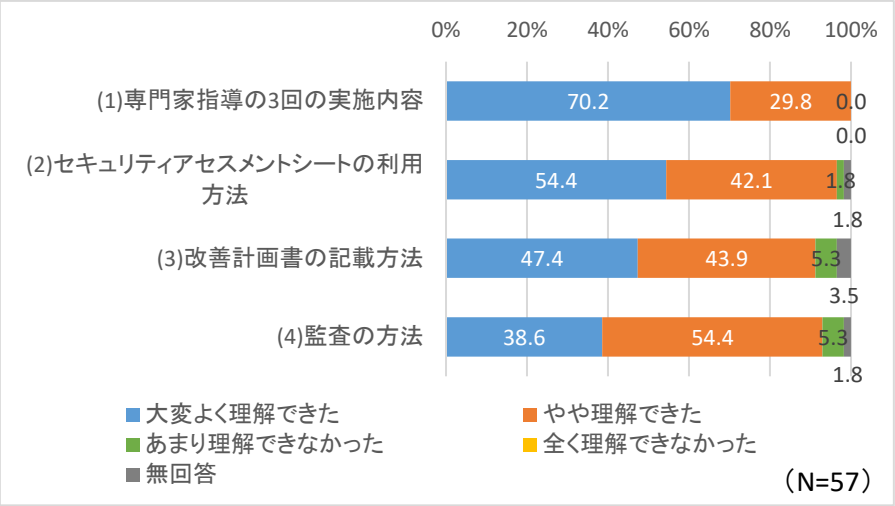


図 37　マネジメント指導ツール（セキュリティアセスメント）の理解

②　マネジメント指導ツールの指導業務における有用性

マネジメント指導ツールの指導業務における有用性については、未回答以外の回答者すべてが役立つと感じるとの回答であった。

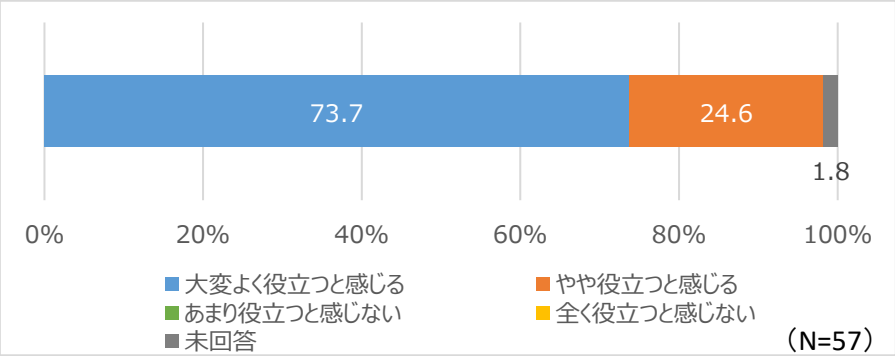


図 38　マネジメント指導ツールの指導業務における有用性

③　初めてマネジメント指導ツールを用いる専門家における実施可能性

初めてマネジメント指導ツールを用いる専門家でも指導が実施可能かについては、91.2%が可能と感じるとの回答であった。

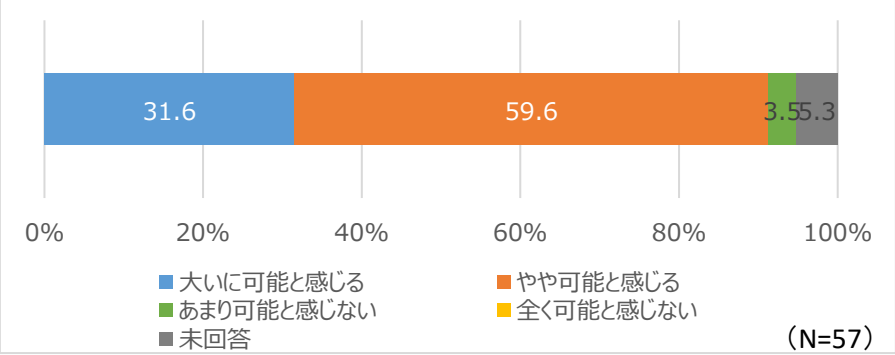


図 39　初めてマネジメント指導ツールを用いる専門家でも実施可能か

(3) ケース演習

① ケース演習は有意義か

ケース演習については、全てのプログラムについて、9 割以上が有意義であったとの回答であった。

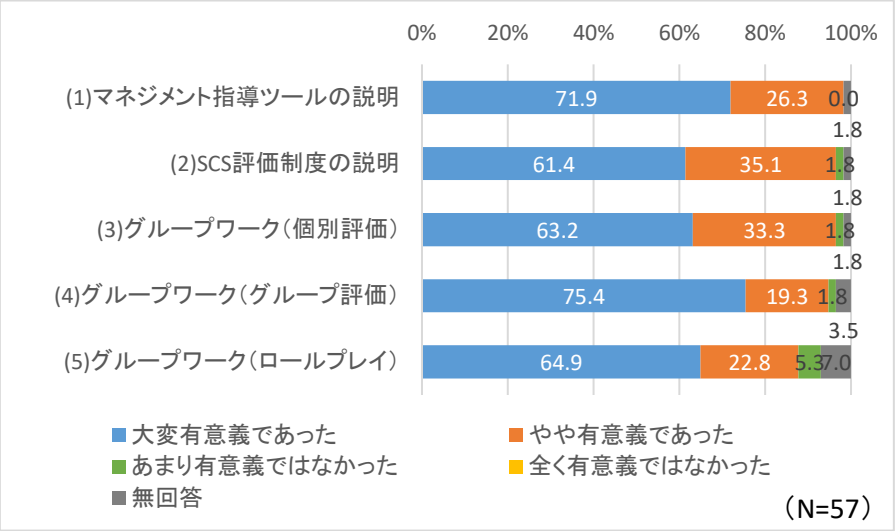


図 40 ケース演習は有意義か

② アセスメントテーマは理解できたか

取り上げたいずれのテーマも 9 割以上が理解できたとの回答であった。

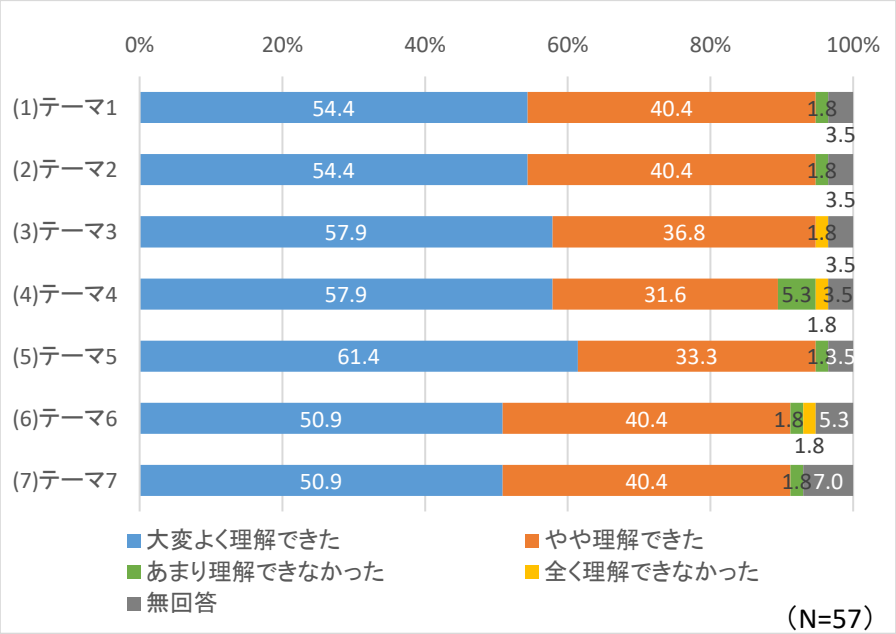


図 41 アセスメントテーマは理解できたか

なお、各テーマの内容（SCS 評価制度における評価基準）を以下に示す。

- テーマ 1：1-2-3 守秘義務のルールを策定し、遵守させること。
- テーマ 2：2-1-1 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。

・　テーマ 3：3-1-4 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。
・　テーマ 4：4-1-1 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。
・　テーマ 5：4-3-4 適切なバックアップを行うこと。
・　テーマ 6：4-4-1 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。
・　テーマ 7：5-1-1 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。

③　ケース演習の課題の難易度

ケース演習の課題の難易度については、49.1%が「適切であった」との回答であった。

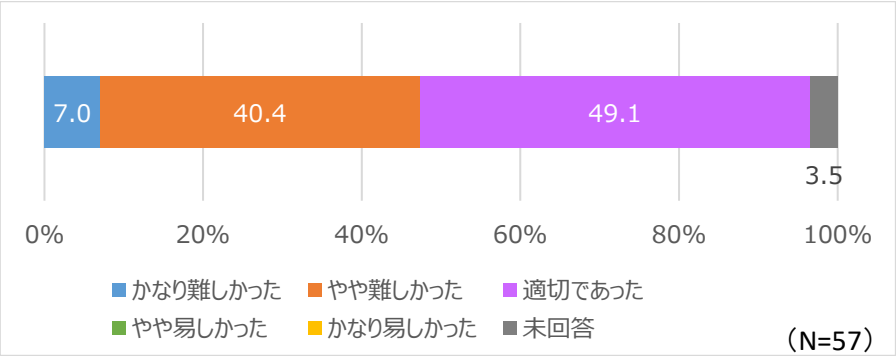


図 42　ケース演習の課題の難易度

④　ケース演習を通じた新たな気づき

ケース演習を通じた新たな気づきについては、87.8%が新たな気づきを得られたとの回答であった。

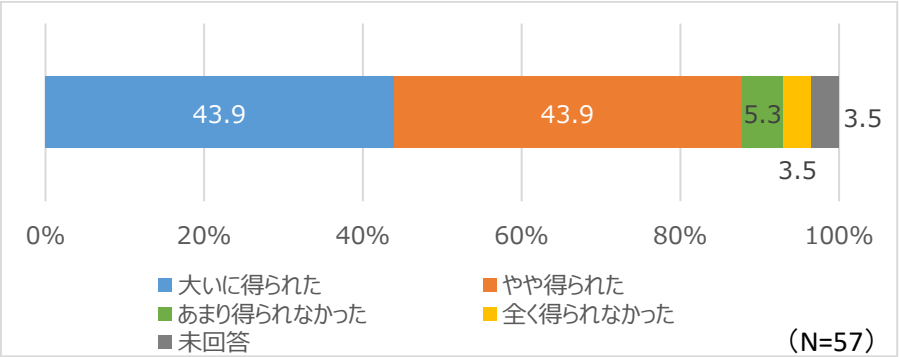


図 43　ケース演習を通じた新たな気づき

⑤　ケース演習の時間の適切さ

ケース演習の時間については、マネジメント指導ツールの説明（90 分）は 89.5%が適切であり、グループワーク（3 時間）は半数近く（47.4%）が短いとの回答であった。

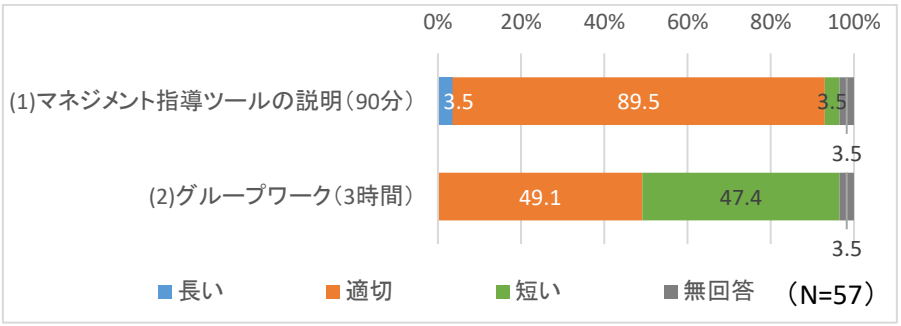


図 44　ケース演習の時間の適切さ

⑥　会場の設備の適切さ

会場の設備については、93.0%が「適切」との回答であった。

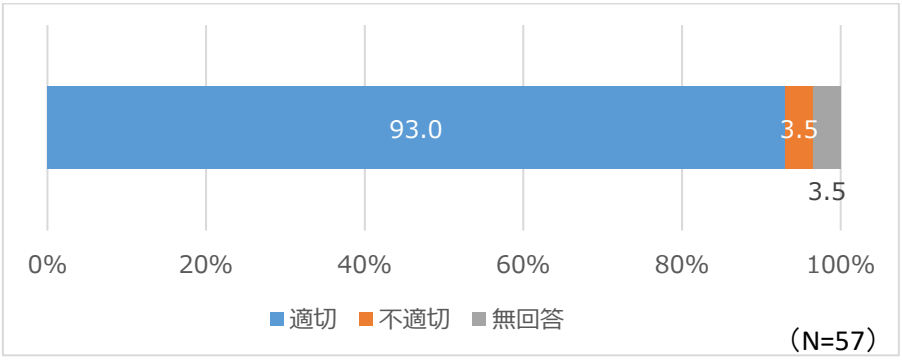


図 45　会場の設備の適切さ

(4)　登録セキスペの人材活用に関する意見

①　登録セキスペとして企業支援の活動を行うにあたっての課題

登録セキスペとして企業支援の活動を行うにあたっての課題について、主な意見を示す。

表 18　登録セキスペとして企業支援の活動を行うにあたっての課題

項目		主な意見
専門家自身の課題	スキル・経験等の不足	✓　単独で実施するまでのサポートがあれば助かる ✓　ケース演習を何度か繰り返しロールプレイの経験が必要 ✓　情報セキュリティ領域の専門的な知見のみでは、効果的な支援にならないのではないかと感じる ✓　本業が非セキュリティ領域のため、自分のスキルセットが十分か自信がない ✓　提案はできるがソリューションとのひもづけに課題がある
	副業・兼業との兼ね合い	✓　勤務先の理解と協力 ✓　副業規定との兼ね合い ✓　団体職員の場合、兼業として行うことが難しい
市場・環	中小企業と	✓　クライアントをこちらから探さないと見つけられない状況にある

項目		主な意見
境の課題	のマッチング	✓ 企業支援の機会を増やす取組、支援をお願いしたい
	報酬水準	✓ 支援サービスの有償化、有償時の価格の適正化
	契約・責任	✓ 業務に対しての責任の範囲を、個人で負担できるレベルに限定的にするのが望ましい
	継続的な支援	✓ 改善計画における具体的な支援
制度の課題		✓ 登録セキスペの知名度の低さ ✓ 資格維持コストの費用負担 ✓ 業務内容が不明確、要件化された業務がない点
中小企業の課題		✓ 企業活動においてセキュリティが必ず必要ではない点
ツール等の課題		✓ 適合か否かの判断基準が個人によって差が出るように感じた ✓ 支援士がツールを適切に使えているのか検証する術が現状なく、支援士任せにならざるを得ない制度になっている ✓ 支援士のレベルにムラが出てしまう（ツールがないとさらにムラがひどくなるので、ツールがあることはとてもいいと思う）。★3 レベルに合わせた支援なので、支援先企業の自己評価にムラが出てしまうのはよくない。グループによるパブコメとして掬い上げるなどして、来年 4 月の制度に向けて反映されるように検討してほしい ✓ 各種ツールを使った指導や評価方法が、指導者や評価者の経験や力量、個別判断によりばらつきが出ないように、明確な基準が設定され、公開されることが重要である ✓ 実際にセキュリティアセスメントを行う際に、評価基準が曖昧だったり、評価基準と評価ガイダンスに差があることが一律的な評価ができない要因になると予想される

② 連携を希望する相手

連携を希望する相手先については、「商工会議所」が最も多く 25.8%、次いで「中小企業向け IT ベンダ、セキュリティベンダ」が 20.0%、「自身と異なる専門を有する登録セキスペ」が 19.2%との回答であった。

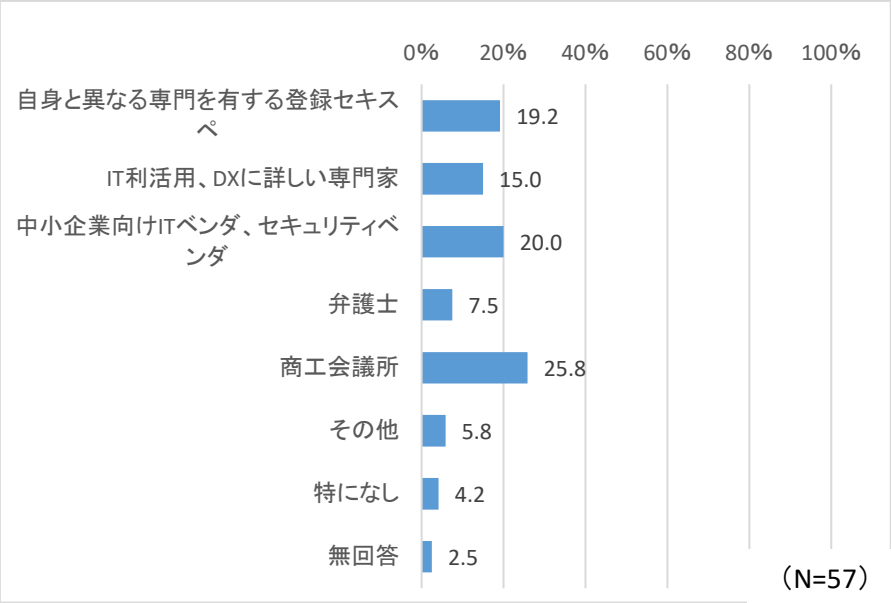


図 46　連携を希望する相手

＜その他の意見＞

- 支援活動の経験者
- サイバー保険を販売している保険屋
- 企業内 SG
- IT コーディネータ
- 産業支援機関、よろず支援拠点（演習座学で価格転嫁の話が出てきたため）
- 中小企業診断士
- 士業や士業協会、各業界の団体

③　マネジメント指導ツールやケース演習の活用にむけた運営

マネジメント指導ツールやケース演習の活用にむけた運営について、主な意見を以下に示す。

表 19　マネジメント指導ツールやケース演習の活用にむけた運営に関する意見

項目	主な意見
ツール・コンテンツ等の充実	✓ 事例集があるとよい ✓ 他の登録セキスペの活動が共有されるとよい ✓ スラックや、ディスコードを使った情報共有の場の提供 ✓ 今後もツールを拡充いただけると大変ありがたい ✓ ビジネスモデルを紹介するようなやり方があるとよい
活躍の場の拡大	✓ 支援士の活動事例を増やし、支援士の活動の幅を広げ、これらの実績を支援士のロールモデルとして提案できれば、多様な領域での活躍をサポートする事業になるのでは ✓ 医師会と連携して各クリニックにセキスペを派遣する ✓ ケース演習で各支援士が評価する結果が一定になるような評価のガイダンスが提供されるような事業運営と、加えて、支援士が星 4 つ以上の認定に関わるスキームがあればよい

項目	主な意見
研修の場の提供、充実	✓ ケース演習の回数を増やす、またはオンラインを活用する（e-ラーニングなど） ✓ ロールプレイはグループ内で行う方が実践経験につながる ✓ 定期的な研修の実施
派遣や支援の一元化	✓ IPA やもしくはその代理の団体にセキスペが所属し、企業がその団体に派遣を依頼する。その団体は適宜、セキスペを支援するようにしてはどうか ✓ 民間に常設事務局機能を設置運用する

④　国や IPA、その他団体からの支援や仕組みに対する要望

国や IPA、その他団体からの支援や仕組みに対する要望について、主な意見を以下に示す。

表 20　国や IPA、その他団体からの支援や仕組みに対する要望

項目	主な意見
周知、広報の強化	✓ 一般企業への周知、広報をお願いしたい ✓ 中小企業に知名度を上げてほしい
マッチング、営業活動への支援	✓ 中小企業を中心とした支援のマッチング ✓ 営業活動を支援してほしい ✓ 仕事を斡旋してくれる仕組みがあればよい
研修の場の提供、充実	✓ 地方での実践的な演習があると助かる ✓ 未経験や経験が浅い登録セキスペへの教育、経験できる機会の提供
ツール・コンテンツ等の充実	✓ 支援士がより現場で活躍できるようなツール類の整備や支援 ✓ 評価の事例集
アセスメント、監査の向上	✓ 監査の考え方については支援士は弱いと思うため、特に今回のアセスメントの指針（ガイダンス）については支援士向けに整備等していただきたい ✓ 生成 AI などで評価について確認できるようにしてもらえると、評価結果のクオリティを統一できる
中小企業への支援	✓ 国や IPA が診断を受ける側の企業に対してインセンティブを用意し、ある程度強制的に進めていくのがよいと思う
専門家への報酬支援	✓ 報酬の検討や更新要件の免除 ✓ 要件化する業務を増やしてほしい

(5) マネジメント指導ツール（セキュリティアセスメント）を活用した活動希望

マネジメント指導ツール（セキュリティアセスメント）を活用した活動希望については、73.7%が「希望する」との回答であった。

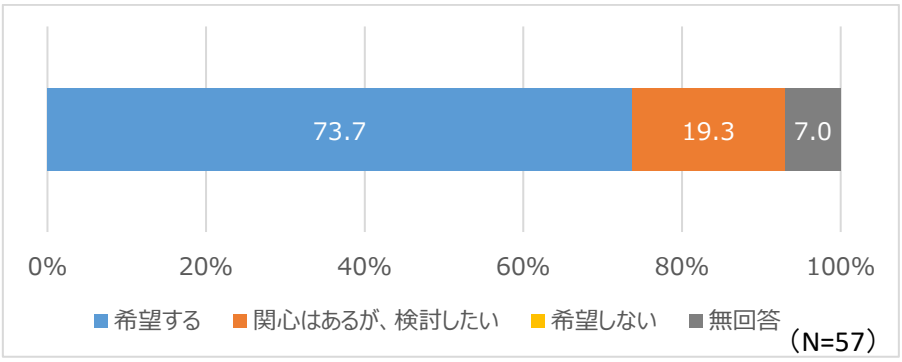


図 47　マネジメント指導ツール（セキュリティアセスメント）を活用した活動希望

以上