令和7年度セキュリティ人材活用環境整備に係る業務実施報告書概要版

2026年4月

独立行政法人情報処理推進機構
セキュリティセンター

1. 概要

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、令和6年度*1に作成した「登録セキスペアクティブリスト（試作版）」の改善を行い、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、登録セキスペへのリスト登録促進の両面からリストの整備を行った。

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（SCS評価制度）」*2 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 令和6年度セキュリティ人材活用促進実証
https://www.ipa.go.jp/security/reports/sme/riss-katsuyo2024.html
*2 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
表示ページ作成

- セキュリティ対策支援者リストについて、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、簡易的な絞り込み表示が可能となるようHTML化を行い、公開した*3。
- 当機能は「情報処理安全確保支援士検索サービス」に今後追加される予定のため、HTML化に必要な事項や要件および今後の課題を整理した。

リストページ

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

個票（個人詳細）ページ

*3 中小企業向けサイバーセキュリティ対策支援者リストの紹介
https://www.ipa.go.jp/security/sme/shien/list.html

2. セキュリティ対策支援者リストの活用促進
表示ページ作成・支援者リストの活用促進に関する考察（今後の課題）

【実施内容】

	項目	内容
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。 • 地域…北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄 • 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
2	専門家個票	リストからリンクを張り、専門家の詳細情報を参照可能にした。 リスト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。

【今後の課題】

項目	内容
登録セキスペの有効期限管理と登録継続性	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・手順等について検討を要する。
リスト掲載情報の鮮度維持・活動状況の反映	信頼できる情報を継続的に提供するため、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。
検索軸の拡充	中小企業が専門家を選定する際の基準は、支援実績、指導可能な内容、費用等、多岐にわたるため、検索軸の拡充が必要。
中小企業以外の利用促進	中小企業が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、それ以外にも、商工会議所の相談窓口での利用、補助金申請時の活用、地域の金融機関による紹介等も考えられる。今後は利用者・利用シーンに応じたより効果的な周知・案内が必要。

3. セキュリティ対策支援者リストの登録促進
セキュリティマネジメント指導ツール活用セミナーの開催

- 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」を開催し、登録セキスペ活用の取組みや指導ツールを活用した指導方法および指導事例を周知するとともに、セキュリティ対策支援者リストへの登録を促進した。
- 当初、各回300名程度の申込を予定していたが、多くの申込があり、参加者数を申込者数で割った参加率は約9割と高い結果となる。各回のゲストスピーカーが異なることもあり、複数回に参加する登録セキスペもいた。
- セミナー参加申込時の質問や、セミナー中の質疑応答をFAQとしてとりまとめ、アーカイブ動画や説明資料と共にウェブ公開した。

プログラム

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

	申込者数	参加者数	参加率	ゲストスピーカー	形態	事例企業とテーマ
第1回 11/7(金)	783名	727名	92.8%	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」
第2回 11/20(木)	691名	624名	90.3%	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」
第3回 12/5(金)	660名	577名	87.4%	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」
合計	2,134名	1,928名	90.3%			

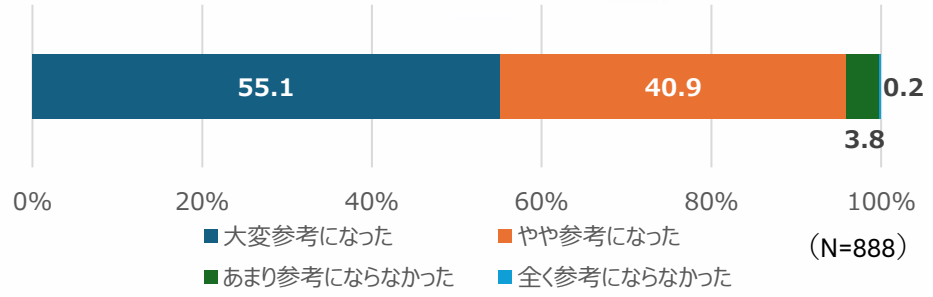
3. セキュリティ対策支援者リストの登録促進
セキュリティマネジメント指導ツール活用セミナーの開催

【アンケート結果】

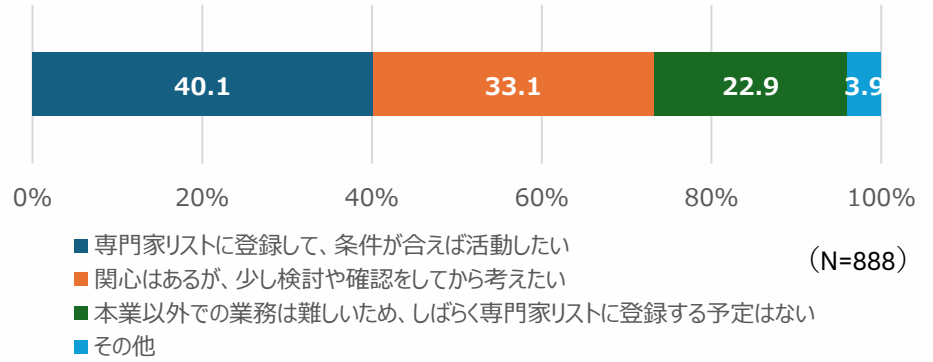
- セミナー全体の満足度について
  「たいへん参考になった」が55.1%、「やや参考になった」が40.9%で、ほぼ参加者全員が参考になったと回答。

- 支援者リストへの登録・活動意向について
  「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に回答。

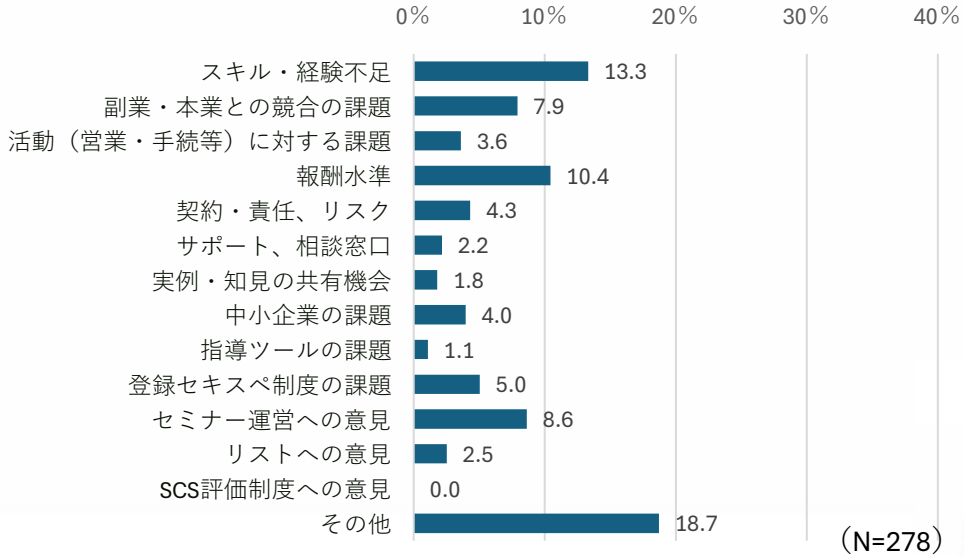
- 自由記述の回答からの分析
  内容別にみると、登録セキスペとして活動するにあたっての課題や要望等の記載が多く見られた。
  多かった回答は、「スキル・経験不足」(13.3%)という専門家自身の課題、及び「報酬水準」(10.4%)という中小企業に対するセキュリティ支援の環境に関わる課題であった。



(N=888)



(N=888)



(N=278)

3. セキュリティ対策支援者リストの登録促進
セキュリティマネジメント指導ツール活用セミナーの開催

（参考）自由記述の主な回答

項目		内容
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。
	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。「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。「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。
	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。
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。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。
	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。
	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。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。
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の指摘。
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。「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機会に対する要望。
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、目的そのものや登録・更新方法が理解されていない状況。
	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。「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。

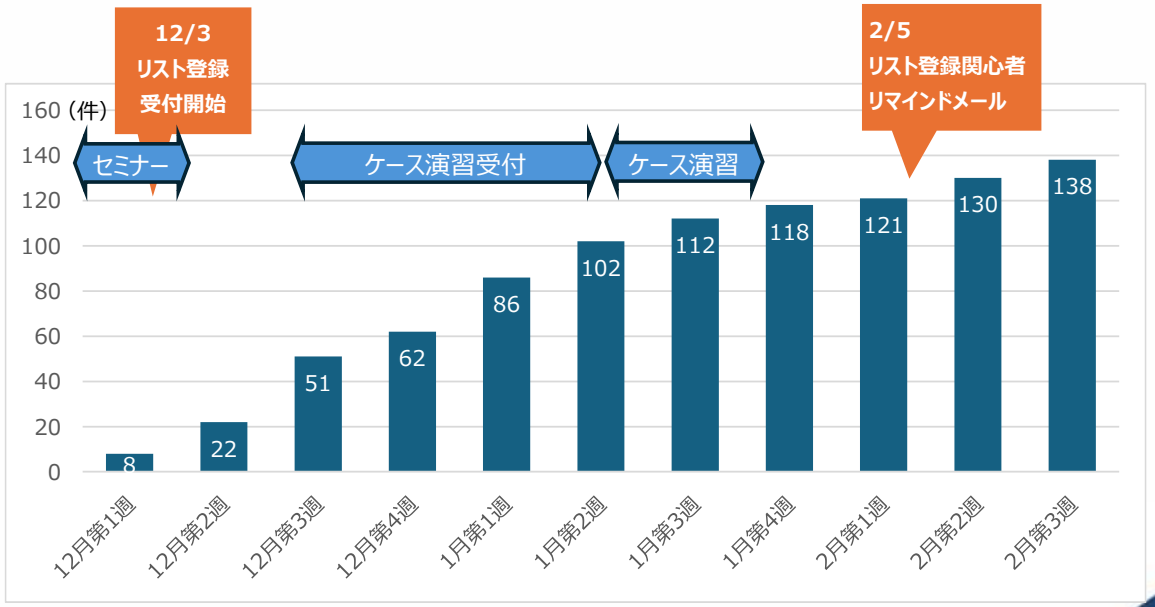
3. セキュリティ対策支援者リストの登録促進
リスト登録受付・確認・反映（登録者のデータ管理・運用）

- 令和6年度の登録者データと令和7年度以降の登録者データを統合し、今後は新規分・変更分の申請を定常的に受け付けてリストに反映する。
- 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。
- 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。
- 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（138件増）。

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に受付開始の案内後、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、支援者リスト未登録者に対して登録を必須として申込みを受付。ケース演習受講者60名のうち、令和7年度の新規登録43名、令和6年度の既登録15名、登録意向はあるが未登録2名であった。
2026年2月5日	マネジメント指導ツール活用セミナー（第1・2・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、リスト未登録者を対象に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。

支援者リスト新規登録件数推移



3. セキュリティ対策支援者リストの登録促進
支援者リストの登録促進に関する考察（今後の課題）

- 支援者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

    セミナー参加率が約90%と登録セキスペの関心は高く、満足度も「参考になった」が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、即時に登録可能は限定的であった。登録方法の案内やメリットの提示を速やかに行う等、きっかけに繋げる仕組みが必要。
  - 支援者リストの目的や登録・更新方法に関する周知

    アンケートから、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。登録セキスペや、登録が期待される情報処理安全確保支援士試験合格者に対して定期的な周知が必要。
  - 支援者リストの掲載項目の見直し

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

    アンケートから、登録を阻害する要因は「スキル不安」「報酬」「責任（契約・賠償）」等が挙がった。
    - ✓ 「スキル不安」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チームでの派遣、専門家用相談窓口の設置等
    - ✓ 「報酬」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）」への解決策…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

    登録後の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。活動事例等の周知や案件の発生状況等の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

    アンケートから、副業・兼業の禁止や許可制、本業との競合、公務員の制度制約等の活動制約に係る課題が挙がった。このような立場にある登録セキスペの活動を別の形態で促進することも考えられる（法人経由の派遣、ボランティアとして市場を分けた活動、グループ企業や取引先企業への支援等）。

4. セキュリティマネジメント指導テーマの拡充
マネジメント指導ツール「セキュリティアセスメント」

これまで、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。

⑥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。

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

4. セキュリティマネジメント指導テーマの拡充
マネジメント指導ツール「セキュリティアセスメント」

【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」および「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」

【方針】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）。

【構成】セキュリティアセスメントを行うに当たって、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」とした。

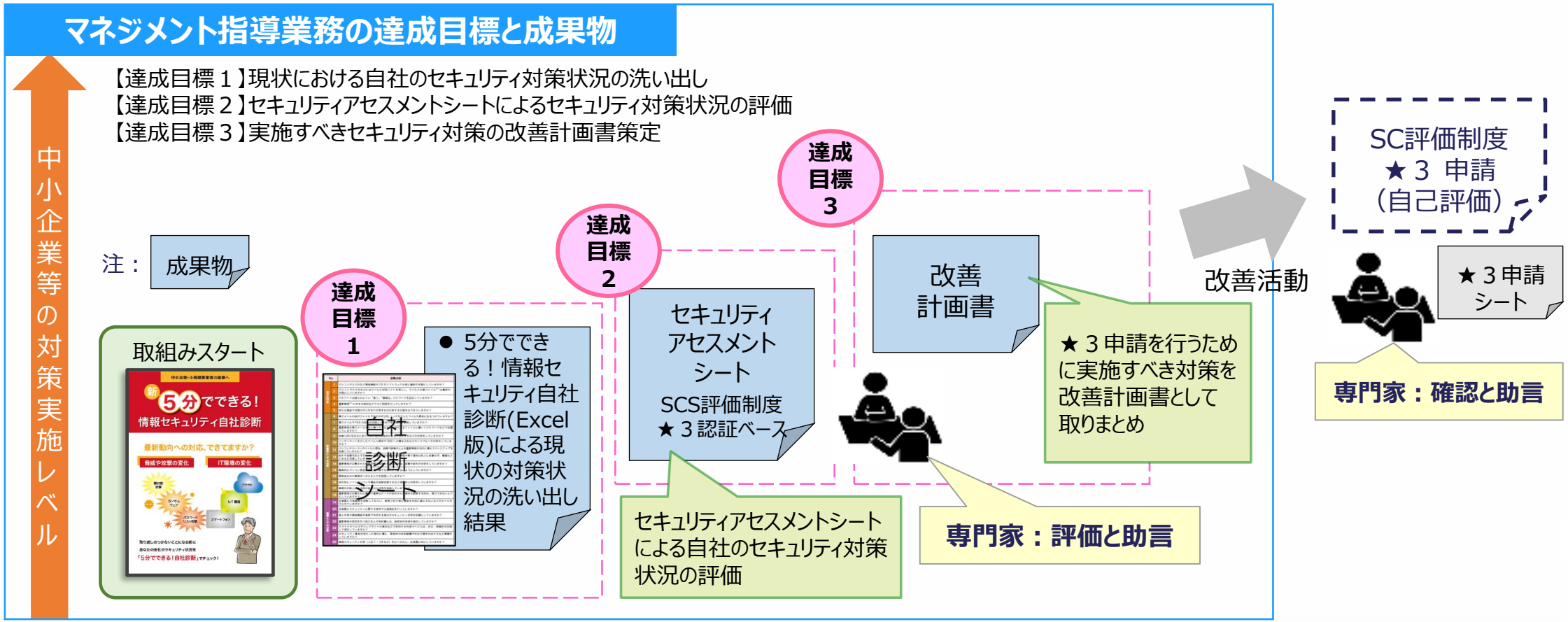
- 「実施要領」には、各回の指導の内容（標準的な進め方）に加えて、指導に当たっての留意点および使用するツールや資料の活用方法を記載し、実践的なノウハウを提供。
- 「セキュリティアセスメント」の実施については、SCS評価制度の中で、全ての企業が最低限実装すべきセキュリティ対策とされる、★3の要求事項・評価基準に基づくフレームワークで構成した『セキュリティアセスメントシート』を用いて行うものとした。これにより実施した企業は、SCS評価制度の★3申請を行うために実施すべき対策（改善事項）が明らかになり、自律的なセキュリティ対策の強化が期待できる。

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

4. セキュリティマネジメント指導テーマの拡充
マネジメント指導ツール「セキュリティアセスメント」

【指導テーマ⑥：セキュリティアセスメント】

- 「サプライチェーン強化に向けたセキュリティ対策評価制度（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。



4. セキュリティマネジメント指導テーマの拡充
マネジメント指導ツール「セキュリティアセスメント」

- 『セキュリティアセスメントシート』は、SCS評価制度★3の要求事項・評価基準（2025年12月時点）を基に作成。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	システム機能	現場視察	ヒアリング		
ガバナンスの整備	役割、責任、権限	1-2-1 1-2-3	・セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てること。 ・守秘義務のルールを策定し、遵守させること。	対	・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 に運用されていることを確
	ポリシー	1-3-1	・自社のセキュリティ対応方針(ポリシー)を策定し、周知すること。		を社内ポータルやWeb にも盛り込んでいる。	○	○		○		の掲載状況や就業規 されていることを確認し
取引先管理	サイバーセキュリティサプライチェーンリスクマネジメント	2-1-1 2-1-2 2-1-4	・取引先と自社とのビジネス又はシステム上の関係を把握すること。 ・他社との間で、機密情報の取扱い方法を明確にすること。 ・セキュリティインシデント発生時の他社との役割及び責任を明確にすること。		先とは秘密保持契約 取り扱いや、障害発生 明確にしている。	○			○		の経緯や事情があるも 取引先との秘密保持契約 まれる。
リスクの特定	資産管理	3-1-1 3-1-2 3-1-3 3-1-4	・ハードウェア、OS及びソフトウェアの情報に関する一覧を作成すること。 ・ネットワークの情報に関する一覧を作成すること。 ・自社の機密情報を扱う外部情報サービスを管理すること。 ・機密区分に応じた情報の管理ルールを定め 、それに基づく管理を行うこと。		ルの手順書をもとに、 システムの各種機能で いる。	○	○	○	○	適合	・手順書と運用管理システムの機能を確認し、適切に管理されている。
攻撃等の防御	アイデンティティ管理、認証、アクセス制御	4-1-1 4-1-2 4-1-3 4-1-4 4-1-5 4-1-6 4-1-7	・ユーザID の発行・変更・削除の手続を定め、適切に運用すること。 ・管理者IDの発行・変更・削除の手続を定め、適切に運用すること。 ・システム及び情報の重要度に応じて認証の強度及び実装方法を決定すること。 ・社内システムを構成する端末にアカウントロック制御を行うこと。 ・パスワード設定に関するルールを定め、周知すること。 ・パスワードの管理に関するルールを定め、周知すること。 ・アクセス権の管理ルールを定めて、運用すること。	対応済	・管理ルールの 運用管理システ 対応できている。						
	意識向上とトレーニング	4-2-2	・セキュリティインシデント発生時の対応に関する教育・訓練を行うこと。	未対応	・従業員へのセキュリティ教育は実施しているが、インシデント発生時の訓練は未実施。	○	○		○	改善要	・現在の社内ポータルでのセキュリティ教育に加え、インシデント発生時の訓練が必須と考える。
	データセキュリティ	4-3-4	・適切なバックアップを行うこと。	対応済	・重要データは、社内サーバ、クラウド共に、日次でバックアップしている。		○	○	○	改善要	・ネットワークから切り離したバックアップ保管ができていないことが判明し、早急に検討が必要。
	プラットフォームセキュリティ	4-4-1 4-4-4 4-4-5	・ハードウェア・ソフトウェアの安全な構成を確立し、維持すること。 ・ハードウェア・ソフトウェアへのセキュリティパッチ及びアップデートの適用に係る手続を策定し、実行すること。 ・システムをマルウェア感染から保護すること。	対応済	・管理ルールの手順書をもとに、運用管理システムの各種機能で対応できている。	○	○	○	○	適合	・手順書と運用管理システムの機能を確認し、適切に管理されている。
	技術インフラのレジリエンス	4-5-1	・内外のネットワークを適切に分離し、境界部分を防護すること。	対応済	・UTMを導入し、境界防御を行っている。		○	○	○	適合	・UTMの設定も、購入業者のSEと定期的に確認するなど、適切に運用されている。
攻撃等の検知	継続的監視	5-1-1	・ネットワーク上の適切な場所でネットワーク接続及びデータ転送を監視すること。	一部対応済	・UTMでの監視に加え、リモートワーク用PCについて、来期以降にEDRの導入を検討する予定。		○	○	○	改善要	・当企業のシステム環境において、EDRの導入は有効な対策であり、ぜひ実施いただきたい。
インシデントへの対応	インシデント管理	6-1-1	・セキュリティインシデントへの対応手順、対応体制等を定めること。	対応準備中	・連絡先一覧表は作成済。 ・手順書は来月完成予定。	○			○	改善要	・手順書の作成が準備中であるが、従業員への周知に十分留意して実装することが望まれる。
インシデントからの復旧	インシデント復旧計画の実行	7-1-1	・事業上重要なシステムについて、事業継続の要件に沿う復旧に必要な準備を行うこと。	未対応	・現在ある地震対応のBCPを、セキュリティインシデント対応の観点から見直す。				○	改善要	・セキュリティインシデントへの対応手順書をもとに、BCPへの対策整備を進めていただきたい。

【選択肢】
対応済
一部対応済
対応準備中
未対応
対象外

【選択肢】
適合
改善要
対象外

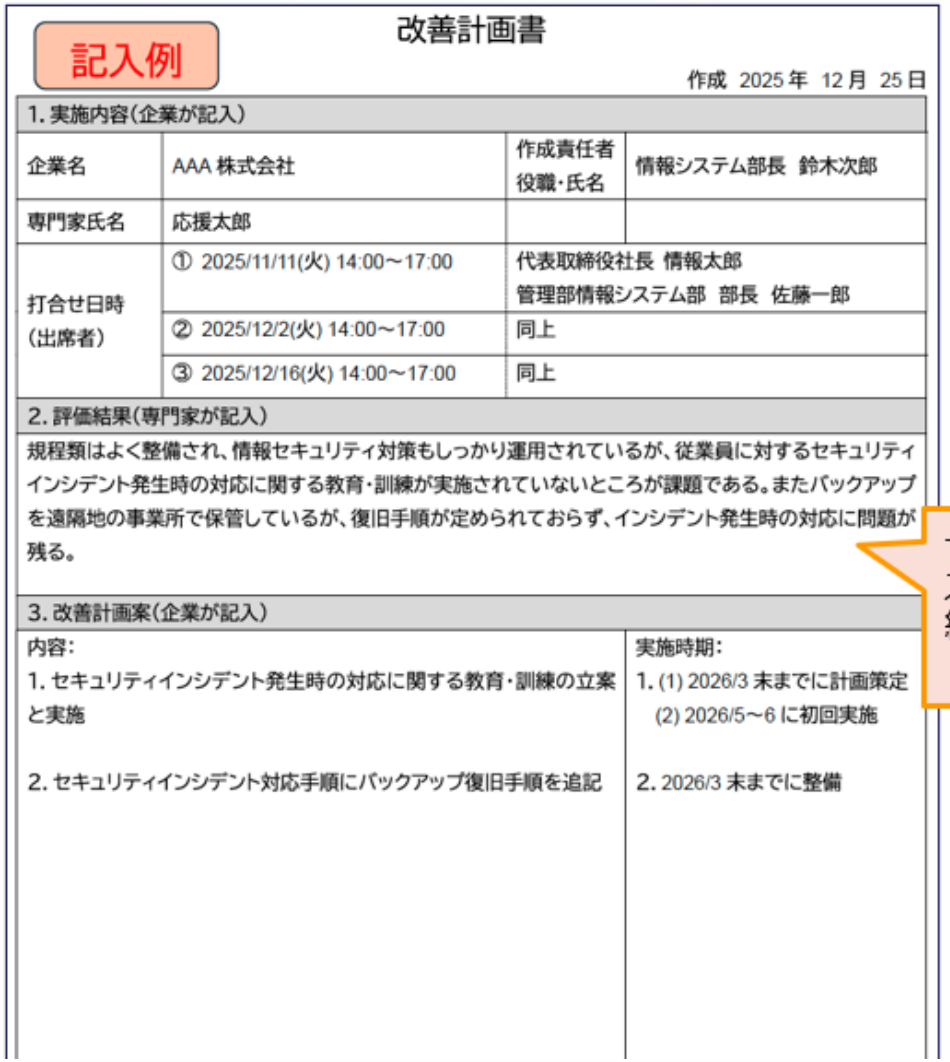
SCS評価制度は、現在立ち上げ検討中であり、「要求事項・評価基準」についても確定に向けて適宜修正されることに留意が必要です。

4. セキュリティマネジメント指導テーマの拡充
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』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。
- 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。

  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。



記入例

改善計画書

作成 2025 年 12 月 25 日

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

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

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

セキュリティアセスメントの評価結果を記載（専門家）

4. セキュリティマネジメント指導テーマの拡充
セキュリティ専門家向けケース演習の開催

- 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。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。
- 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。

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

	(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 （大阪市中央区）	東商カンファレンスルーム RoomB2 （東京都千代田区）	ツドイコ名駅東カンファレンスセンター　Room-D （名古屋市中村区）
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）

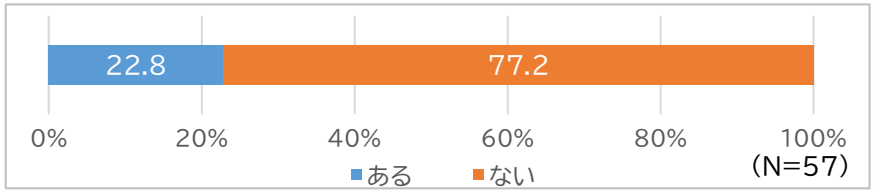
	内容	担当	時間	
講演	ケース演習受講にあたっての説明（スケジュール、注意事項等）	事務局	10分	2時間
	マネジメント指導ツール（セキュリティアセスメント）の解説等	ちば経営応援隊	1時間30分	
	サプライチェーン対策評価制度動向の説明	IPA	20分	
グループワーク	1.ファシリテーターからの説明 ・アイスブレイク、「演習の流れ」「ケース事例について」「評価にあたっての留意事項」の説明 ・事例企業（A社）についての説明 ・ケース1を使用した評価に関する説明 ・「3」検討前に「タイムキーパー、発表者、記録係、司会」を決定 ・「4」の発表テーマは、発表前にファシリテーターがグループ指名し決定	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	

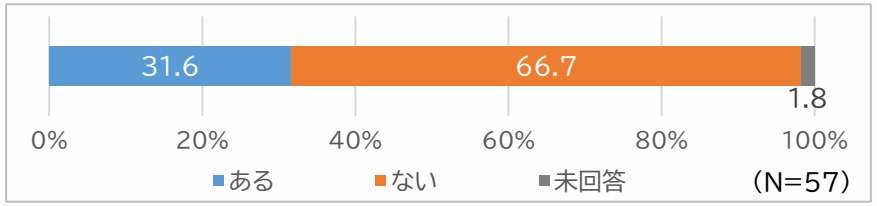
4. セキュリティマネジメント指導テーマの拡充
セキュリティ専門家向けケース演習の開催

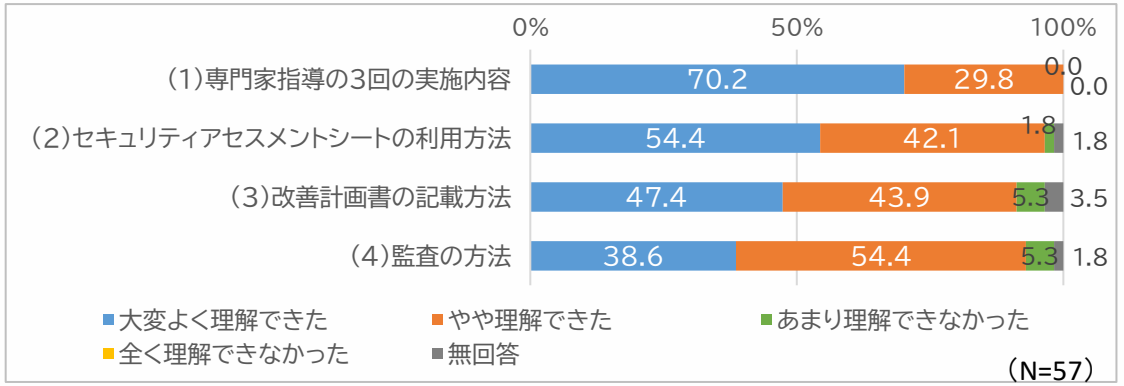
【実施結果】

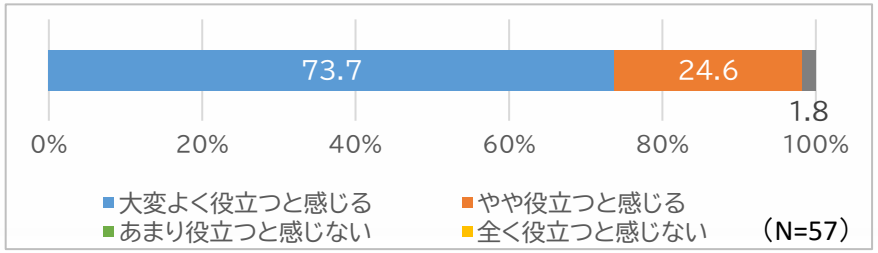
- 合計60名が参加。
- 参加者におけるマネジメント指導ツールを利用した指導経験があるのは2割強、企業に対するアセスメント経験者は3割程度。
- 今回の参加者は申込者のうち「支援者リスト登録者」及び「マネジメント指導ツールを用いた指導が可能な者」を選定したが、実際にツールの利用や企業に対するアセスメント経験がある参加者は限定的であった。
- 参加者において、マネジメント指導ツール「セキュリティアセスメント」は9割以上が「理解できた」と回答。
  そのうち「大変よく理解できた」の回答傾向をみると、「専門家指導の3回の実施内容」は7割が「大変よく理解できた」との回答であったが、「セキュリティアセ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」と回答。

	(1)大阪	(2)東京	(3)名古屋	計
参加者	15名	31名	14名	60名



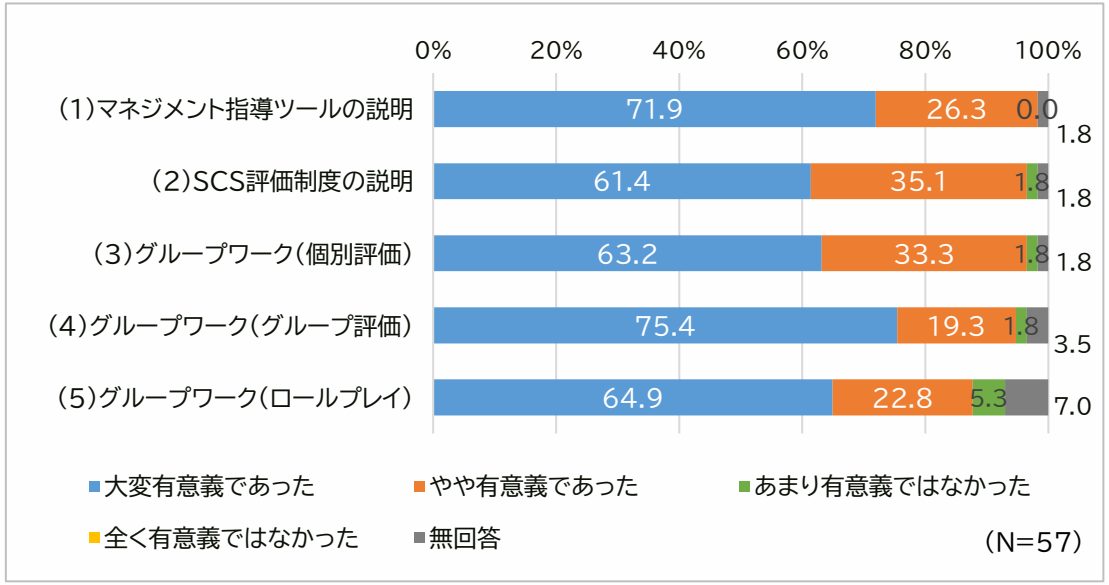


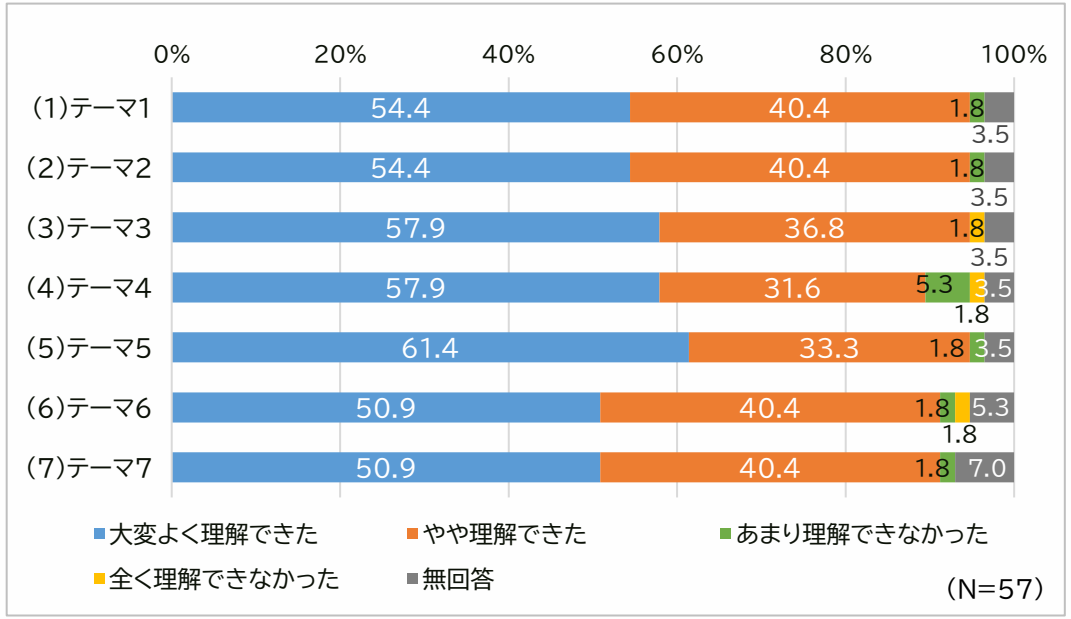


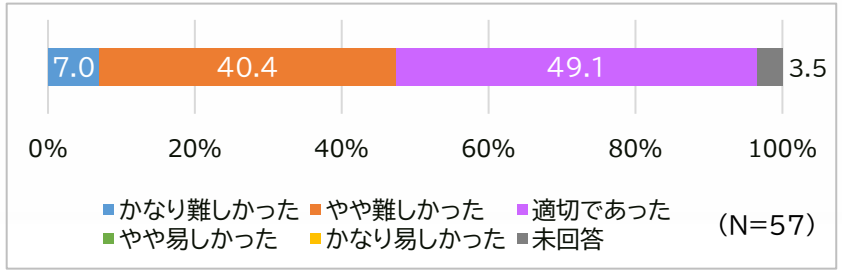


4. セキュリティマネジメント指導テーマの拡充
セキュリティ専門家向けケース演習の開催

- 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」と回答。
  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。
- 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」と回答。
  課題の難易度は5割が「適切であった」、残りは「難しかった」と回答。

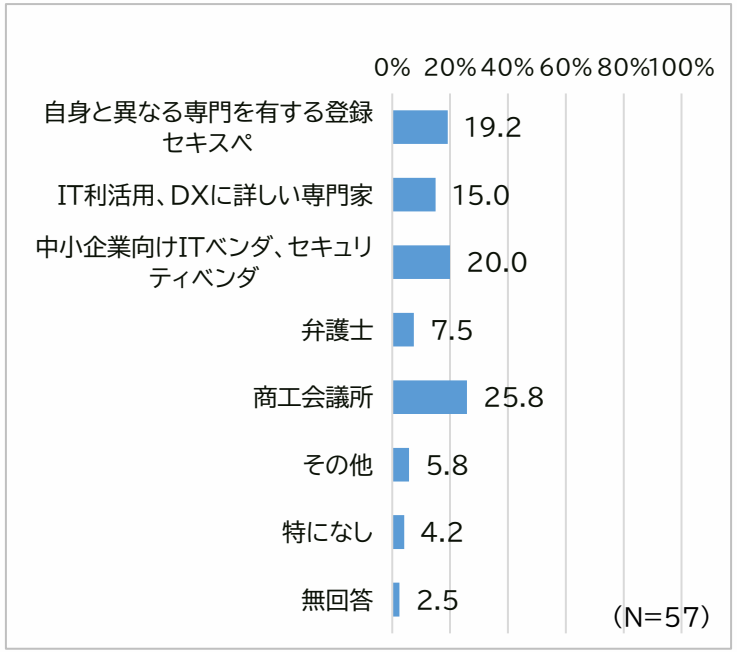


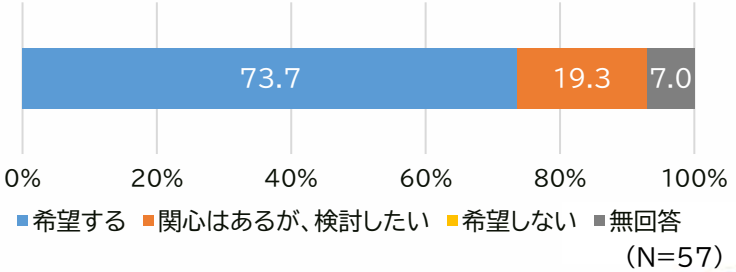




4. セキュリティマネジメント指導テーマの拡充
アンケート結果

- 登録セキスペが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割以上。
- 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
  - 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に対する意見
    「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。
  - 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。
- 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」。「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。





4. セキュリティマネジメント指導テーマの拡充
ヒアリング調査

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収集。

- 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」、「現場では専門家がいない」、「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。

4. セキュリティマネジメント指導テーマの拡充
マネジメント指導テーマの拡充に関する考察（今後の課題）

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、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
     - 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
     - 研修素材（テーマやケース等）の拡充
     - 評価事例の収集・提供

5. まとめ

【総括】

	本事業での実施事項	今後の方向性
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 ● 登録・変更・終了からHTML公開までの業務フローを標準化し、リスト掲載・運用手順（案）を整備。	● 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整備、（2）情報の鮮度維持と活動実態の反映、（3）検索軸の拡充、（4）中小企業以外での利用シーンの具体化と周知が課題。
セキュリティ対策支援者リストの登録促進	● 「セキュリティマネジメント指導ツール活用セミナー」を3回開催、参加1,928名と高い関心を獲得。FAQ・アーカイブ・資料公開によりコンテンツを資産化。 ● 支援者リストは、令和6年度登録者202件を含む340件の登録に到達。	● 支援者リスト認知に加え、登録・活動には、（1）登録行動を後押しする導線、（2）活動阻害要因の解消策提示、（3）案件発生状況や業務負荷の見える化等が必要。 ● 支援機関経由等の活動設計も重要。
セキュリティマネジメント指導テーマの拡充	● 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）」を作成。 ● 「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3会場で実施、合計60名が参加。	● 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、（2）レベル別研修体系の構築と研修素材の拡充、（3）SCS評価制度の確定内容との整合確保が必要。

【今後の取組に向けて】

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
● より活用を促す方針で運用・品質管理を行うことが有効。 ● 登録情報の鮮度や信頼性の担保により、利用者が安心して効率的に専門家を選べるリストに。 ● 登録セキスペの有効期限管理と継続支援を両立し、活動意欲ある専門家が離脱しない仕組み。 ● 利用者の利便性や様々なニーズに応えるため、検索軸の拡充を検討し、システム化を視野にデータ構造を整備。	● 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。 ● 専門家のスキル不安に対する能力形成の機会提供。 ● 報酬水準や費用に対する懸念に対して、報酬目安や標準工数モデルの提示、補助金制度等の活用等。 ● 契約・責任については、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。 ● 専門家個人の副業・兼業等の阻害要因に対しては、様々な参加形態の設計。
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**
● 評価品質の均質化が必要。 ● 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。 ● 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、継続的な研修機会としてコミュニティの場も有効。 ● 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評価制度と継続的に整合性を図りながら整備、評価関連コンテンツとの一貫性を担保。	● 支援者リスト認知から活動までの導線確立、マッチング支援強化により、活動可能な専門家の母数増が重要。 ● 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。 ● 専門家としての活動イメージを提供することにより、活動へ動機づけ。 ● 支援機関の相談窓口でのリスト活用等、信頼できる組織が専門家の選定・紹介を実施。


IPA