令和6年度セキュリティ人材活用促進実証に係る業務 実施報告書概要版

2025年5月

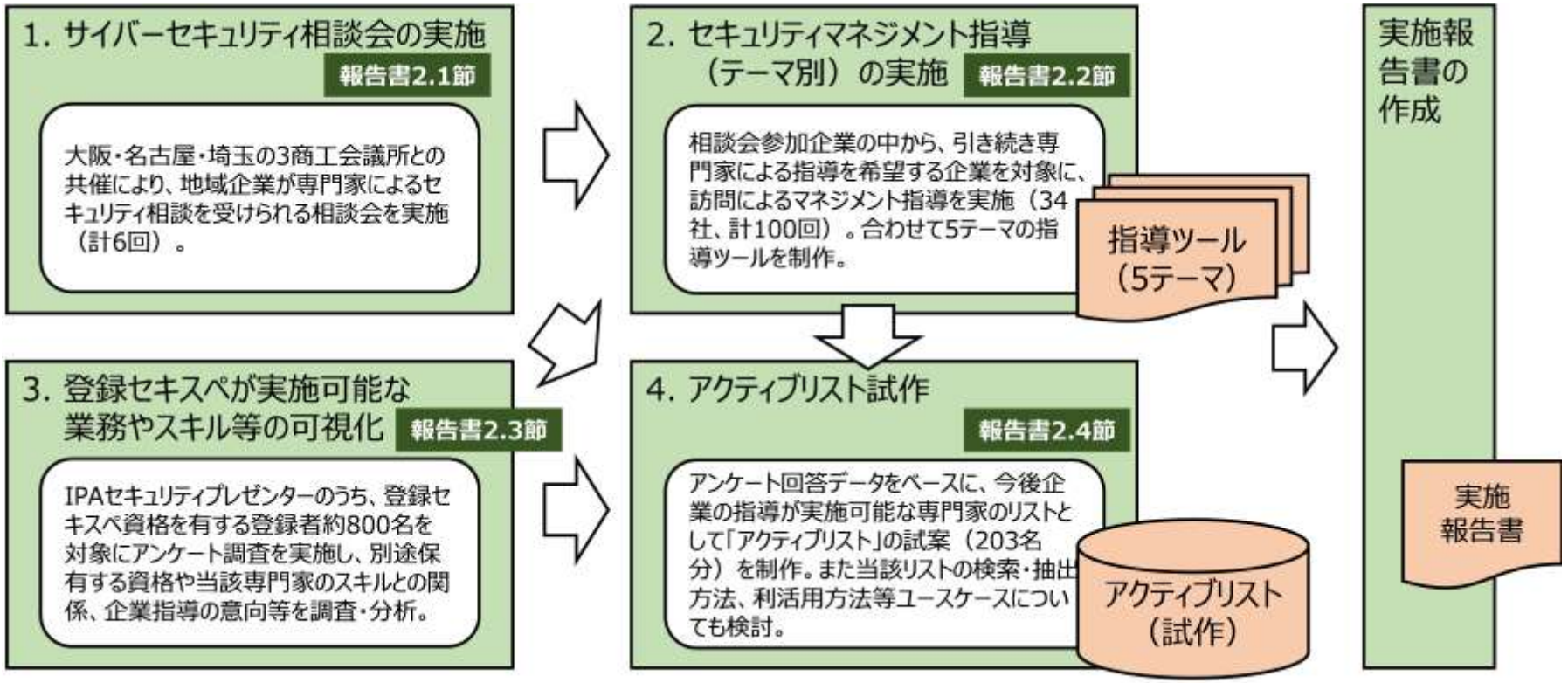
独立行政法人情報処理推進機構
セキュリティセンター

IPA Better Life with IT

事業の目的・背景と全体像

- 情報セキュリティ対策が強固とはいえない**中小企業を対象としたサイバー攻撃が顕在化**しており、中小企業においても対策の実践に当たって必要となる**セキュリティ人材の確保やサービス支援策の強化**が求められている。
- このような背景のもと本事業では、中小企業等と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）との**マッチングを促す場を構築する実証**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専門家を探索しやすくするため、**登録セキスペが実施可能な業務やスキル等を見える化**した人材プールリスト（以下「**アクティブリスト**」という）を試作した。

《事業全体像》



1．実証事業の概要（サイバーセキュリティ相談会）

- **中小企業等と登録セキスペとのマッチング**を促す場として、大阪・名古屋・埼玉の**３商工会議所との共催**による**サイバーセキュリティ相談会**を実施（計6回）した。相談会参加企業105社のうち、55社が**登録セキスペによる個別相談**を行い、マッチング後、34社が**登録セキスペによる訪問指導（マネジメント指導）**を実施、参考になる指導事例を**ベストプラクティス**（7事例）として取りまとめた。

《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走型支援（３回訪問）を実施（各回ごとに目標を設定）。

講演の様子

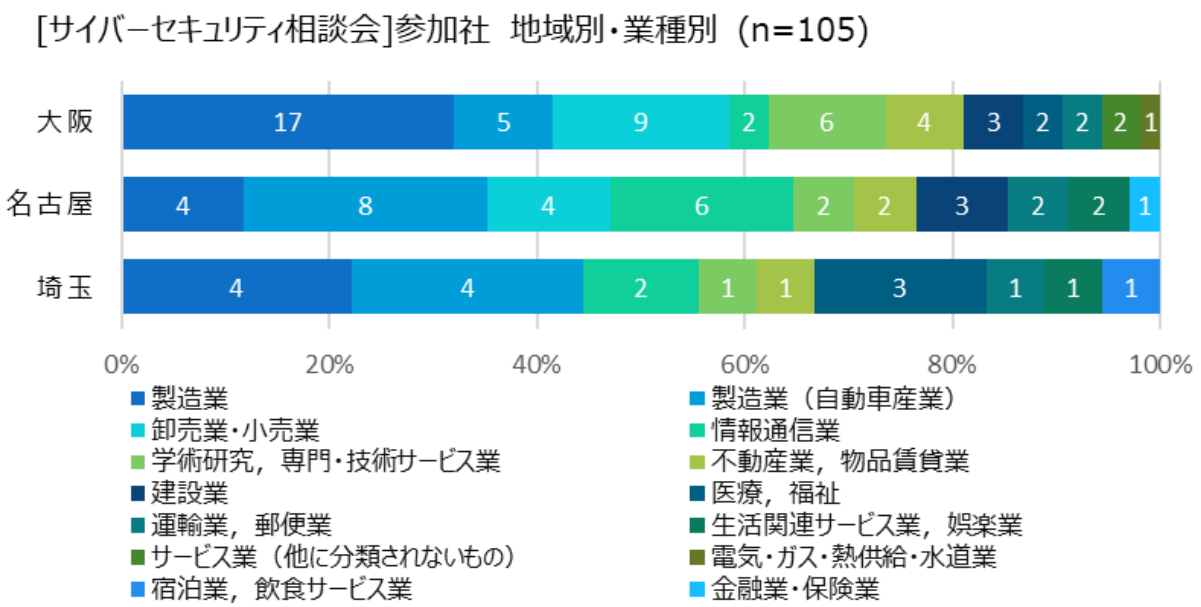
個別相談の様子

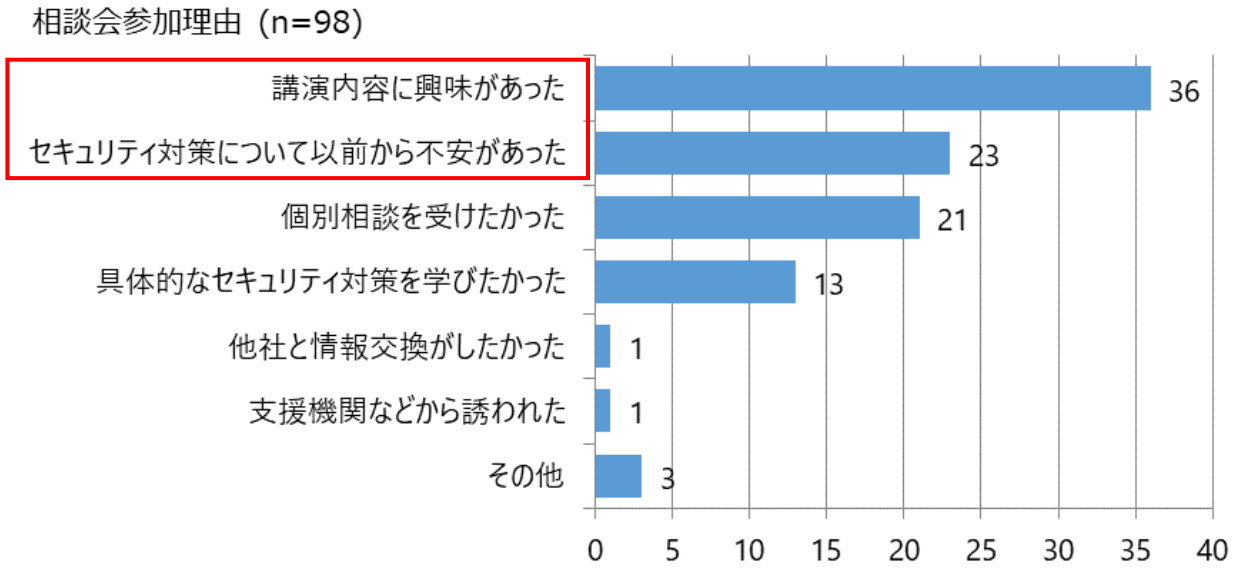
指導事例集（ベストプラクティス）

相談会広報チラシ例

1. サイバーセキュリティ相談会
① 相談会参加企業の業種と参加理由

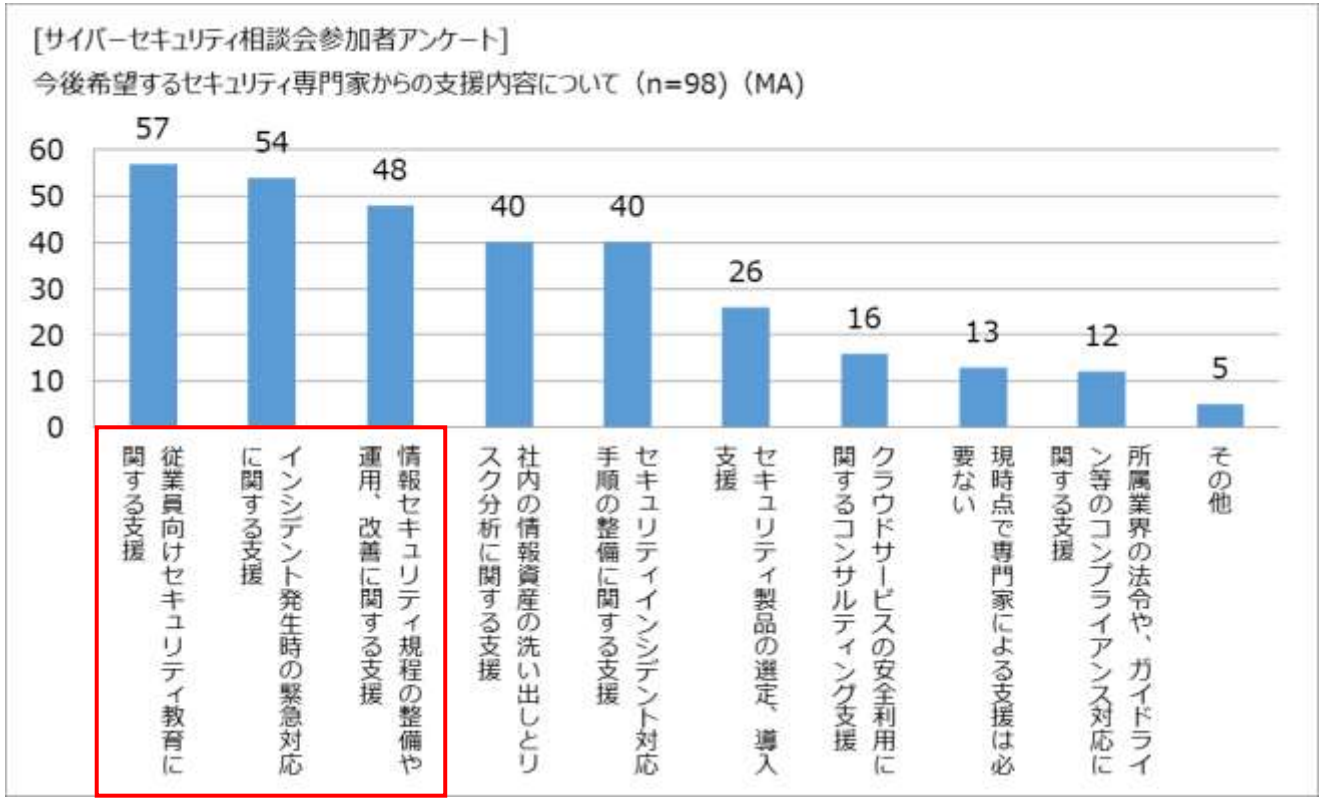
- サイバーセキュリティ相談会には、**3商工会議所で合計105社（122名）が参加**。地域別の傾向は、大阪は製造業を中心としながらも、幅広い業種からの参加が見られた。名古屋では製造業、特に自動車産業からの参加が多く、埼玉では製造業と医療・福祉分野からの参加が比較的多かった。
- 相談会参加の動機は、「講演内容そのものに興味があった」、「セキュリティ対策について以前から不安があった」とする回答が**全体の約６割**を占め、**セキュリティ対策について具体的な対策を実施する前の準備段階（情報収集段階）**にいる参加者が多かった。

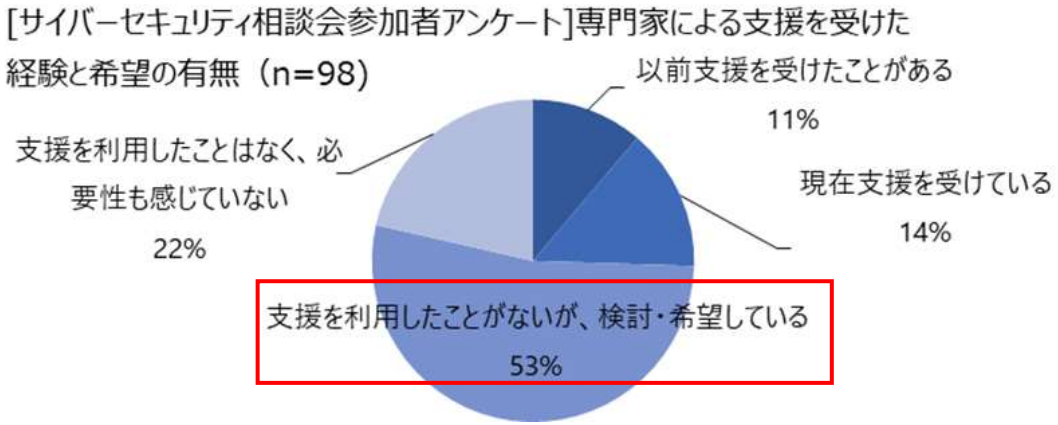




1. サイバーセキュリティ相談会
② 希望するセキュリティ専門家からの支援内容

- **セキュリティ専門家の支援内容**で希望する上位3項目は、「従業員向けセキュリティ教育」、「インシデント発生時の緊急対応」、「情報セキュリティ規程の整備」であり、**緊急対応のニーズ**に加え、**従業員教育、規程整備といった体制整備へのニーズ**があることが示された。
- セキュリティ専門家による支援を受けている・受けたことがある企業は全体の25%だが、**希望・検討している企業は全体の53%**で、今後、**セキュリティ専門家による支援が期待**されていることが明らかになった。



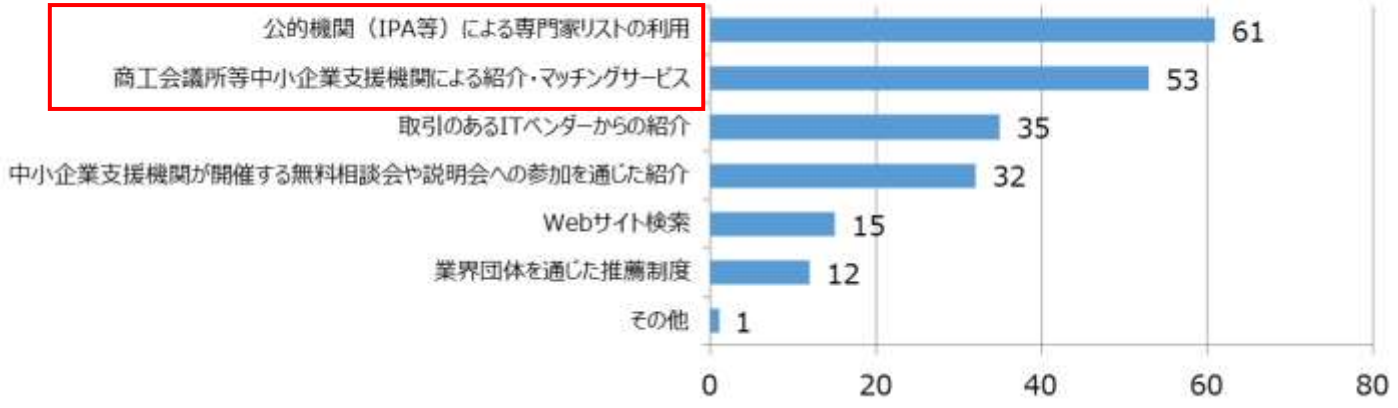


1．サイバーセキュリティ相談会
③ 専門家を選定するときに重視する点と探索手法

- 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」が上位にあがった。このことから、セキュリティ専門家の**インシデント発生時の対応**、**セキュリティ対策提案時の具体性**、**技術力・専門性**が重要であることがうかがえる。
- **セキュリティ専門家の探索方法**は、「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」が上位にあがった。このことから、中小企業に対してリーチするためには、**専門家リストを活用**した商工会議所等の**支援機関と連携したマッチングサービス**が望ましいことが示唆された。

[サイバーセキュリティ相談会参加者アンケート] 専門家を選ぶ際に重視する点（3つまで） (n=98)(MA)

[サイバーセキュリティ相談会参加者アンケート]希望する専門家の探し方（n=98)(MA)



1．サイバーセキュリティ相談会
④ 相談会における具体的な相談内容

➢ セキュリティ相談会における登録セキスペによる個別相談（55社）の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**といったものがあげられた。

相談会における具体的な相談内容（個別相談）

- 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」「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を複数確認。

2．実証事業の概要（セキュリティマネジメント指導）

- セキュリティ相談会の参加企業のうち、希望する34社に対して**訪問指導（マネジメント指導）を実施**した。
- マネジメント指導の実施に際し、業種を問わない基本的なセキュリティ対策として、「中小企業の情報セキュリティ対策ガイドライン（付録を含む）」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。

	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。

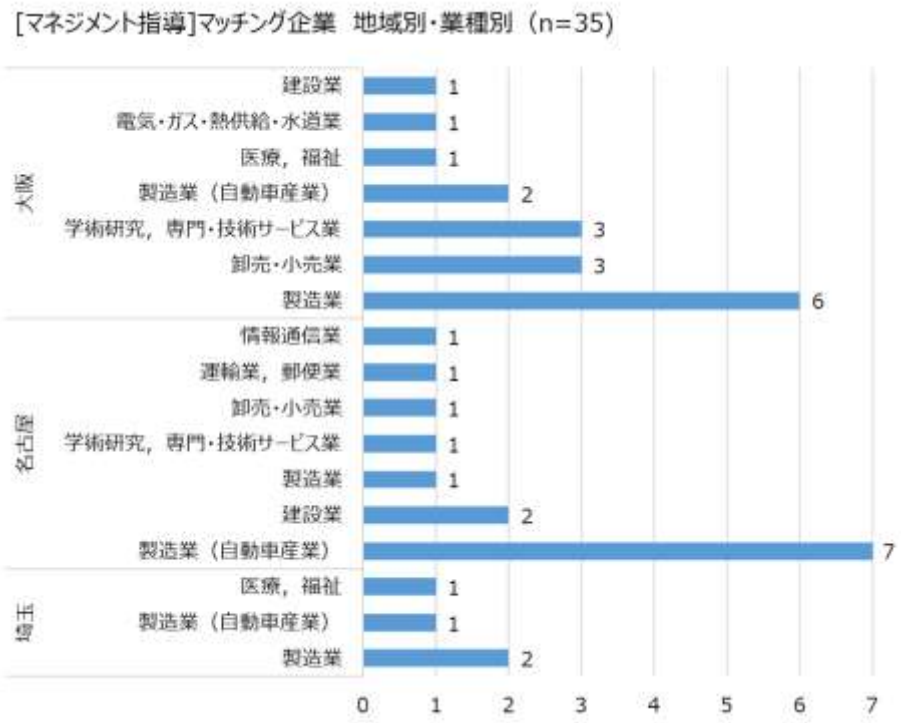
2．セキュリティマネジメント指導
① 中小企業と登録セキスペのマッチング

- サイバーセキュリティ相談会の個別相談を経て、訪問指導を希望する**企業と登録セキスペとのマッチング**を行い、34社に対してテーマ別の**セキュリティマネジメント指導（全3回訪問）**を実施した。
- マッチングに際しては、**指導先業の個別相談時の内容や希望するマネジメント指導テーマ、指導専門家の対象分野等を考慮**し、各企業に指導専門家の割り当てを行った（マッチング）。
- 実際の訪問指導は、マネジメント指導のテーマ毎に全3回の訪問指導を効率的に行うため、**各回の標準的な指導の進め方を示したシラバスを整備**して行った。

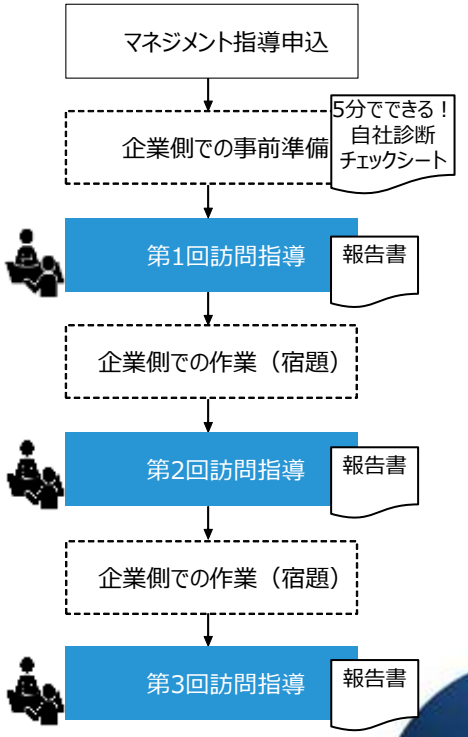
《マネジメント指導実施件数》

テーマ / 地域	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．従業員向けセキュリティ教育	総計
大阪	10	1	1	1	4	17
名古屋	2	2	2	4	3	13
埼玉	3	1	0	0	0	4
総計	15	4	3	5	7	34

※個別相談（55社）を経て、マネジメント指導にマッチングできた企業は35社であったが、1社が指導開始直前に辞退したため、34社に対して実施した。
※原則として全3回の訪問指導を予定していたが、指導実施34社のうち2社については、指導先企業との協議により2回で指導が終了したことから、総訪問回数は、（32社×3回）＋（2社×2回）＝合計100回となった。



マネジメント指導の流れ



2．セキュリティマネジメント指導
② 訪問指導の実施結果（指導テーマ別）

- セキュリティマネジメント指導（34社）実施の結果、**指導ツール**については改善の余地はあるもの**概ね有効に活用**されたことが確認された。また、**約9割の指導先企業**が、**支援内容が当初の目的を達成**することができたと評価しており、**登録セキスペによる中小企業への伴走型支援が有効**であることが示された。

マネジメント指導の実施結果（指導テーマ別）

情報セキュリティ規程の整備	サンプル規程等、指導ツールのボリュームの多さについての指摘はあったものの、指導先企業からは「**セキュリティ関連規程を制定でき、今後の教育・運用についても有益な助言を得られた**」など、目標が達成できたとの評価が多かった。規程類の整備以外にも、**経営層への情報セキュリティの必要性の説明等の機会を得られた**ことを、追加の成果として評価する企業もあった。
情報資産の洗い出しとリスク分析	「リスク分析シート」による**情報資産洗い出し及びリスク評価がスムーズに行えた**との声が多く、指導先企業からは「かねてからの悩み事であった情報資産の一覧表を作成することができた」との評価があった。指導専門家の「**まず情報資産の洗い出しを優先し、その後リスク分析を踏まえたセキュリティ対策を取る**べき」との助言が、指導先企業に理解され指導が実施された例が多かった。
クラウドサービスの安全利用	指導専門家からは「チェックリストに基づき、**利用中のクラウドサービスの問題点を洗い出し、対策方法と今後の取り組みについて助言**できた」との評価がある一方で、指導先企業からは「クラウドサービス利用についてのセキュリティの強化やルール作りが果たせなかった」との声もあり、**指導先企業の今後必要となる情報セキュリティ対策についての助言に至らなかった例**もあった。
セキュリティインシデント対応	指導先企業からは「**指導ツールが分かり易く、参考例などもあり、そのまま会社に提示ができた**」、「**インシデント対応訓練の実施が良好な社員教育となった**」など、指導に対する高評価を得た。一方、指導専門家からは、対外組織との連携、他社事例の内容を踏まえた訓練など、より実践的な目標に到達できなかったとの意見もあった。
従業員向け情報セキュリティ教育	指導先企業からは「**指導ツールの内容が動画と連携しており、受講者全員が理解できた**」、「従業員の意識向上につながる」など、動画と組み合わせる教育手法について、高い評価を得た。一方、指導専門家、指導先企業の双方から、**指導ツールは一般的な内容となるため、個別の企業の事情に合わない内容もあった**との声もあった。

2．セキュリティマネジメント指導
③ 指導事例集（ベストプラクティス）

- マネジメント指導後の報告内容により、**指導の成果が得られた好事例を「ベストプラクティス」**として取り上げることとして、改めて指導先企業・指導専門家へのヒアリングを行い、**指導事例集（7社）を作成**した。
- 指導事例集では、掲載企業の取組みや業界動向等ビジネス環境を踏まえ、企業が**情報セキュリティ上で感じていた課題**と、**専門家による指導のポイント**を記載し、**得られた成果（企業側での変化）**について整理した。

《マネジメント指導事例集（ベストプラクティス）》

No.	地域	指導先企業・団体名	業種	指導専門家	事例タイトル
1	愛知県	深田電機株式会社	卸売業	髙橋 真悟 氏	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
2	大阪府	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	高橋 幸司 氏	セキュリティ対策の第一歩として従業員の意識を向上
3	大阪府	エルメック株式会社	電気業	田中 基貴 氏	効率的な情報セキュリティ対策の進め方や体制の整備
4	大阪府	株式会社ウチダ	製造業	田中 基貴 氏	限られたマンパワーを最大化する専門家の視点
5	中部地方	A株式会社 （非公開）	製造業	久保田 秀男 氏	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
6	大阪府	B法律事務所 （非公開）	サービス業	野村 陽子 氏	被害の経験に基づく研修内容で経営者の意識を改革
7	大阪府	C会計事務所 （非公開）	サービス業	高橋 幸司 氏	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

2．セキュリティマネジメント指導
（参考）指導テーマ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)」の付録5「情報セキュリティ関連規程（サンプル）」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・助言を行う。

マネジメント指導業務の達成目標と成果物

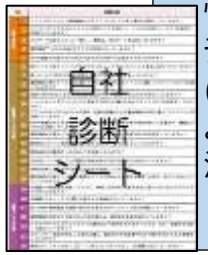
中小企業等の対策実施レベル

【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】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

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

- 情報セキュリティ基本方針
- 情報セキュリティ関連規程類の点検結果

情報セキュリティ基本方針を策定するとともに、既存の情報セキュリティ関連規程整備状況をチェックシートにより確認

達成目標3

- 情報セキュリティ関連規程

情報セキュリティ関連規程（サンプル）

中小企業の情報セキュリティ対策ガイドライン付録5「情報セキュリティ関連規程（サンプル）」を基にした個社の規程（案）を策定

継続実施

2．セキュリティマネジメント指導
（参考）指導テーマ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) 」の付録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の実施について、必要な指導・助言を行う。

マネジメント指導業務の達成目標と成果物

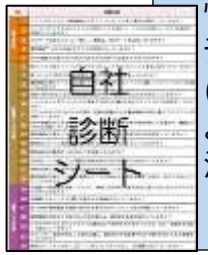
中小企業等の対策実施レベル

【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

達成目標1

取組みスタート



● 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

● 社内における情報資産の洗い出し

達成目標3

● 情報資産に対するリスク分析実施

継続実施

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

2．セキュリティマネジメント指導
（参考）指導テーマ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) 」の付録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の洗い出しと安全利用チェックの実施について、必要な指導・助言を行う。

マネジメント指導業務の達成目標と成果物

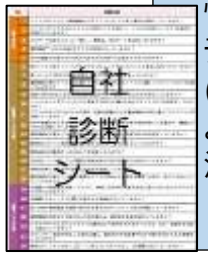
中小企業等の対策実施レベル

【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

2．セキュリティマネジメント指導
（参考）指導テーマ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) 」の付録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、指導先企業におけるインシデント対応手順書の作成、及び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について、 必要な指導・助言を行う 。

マネジメント指導業務の達成目標と成果物

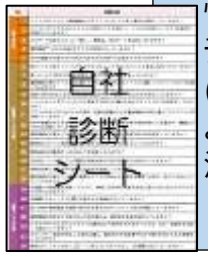
中小企業等の対策実施レベル

【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

2．セキュリティマネジメント指導
（参考）指導テーマ⑤：従業員向けセキュリティ教育

➢ IPAの教育用コンテンツを活用して、企業のニーズに応じた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。教育実施結果をレビューし、継続的な実施を目指したセキュリティ教育計画書の策定について、必要な指導・助言を行う。

マネジメント指導業務の達成目標と成果物

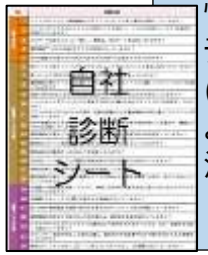
中小企業等の対策実施レベル

【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

達成目標1

取組みスタート



● 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

2．セキュリティマネジメント指導
（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

- 本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）シラバスとの対比関係を意識して設定した。

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
指導ツール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
指導ツール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
指導ツール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
指導ツール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
指導ツール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

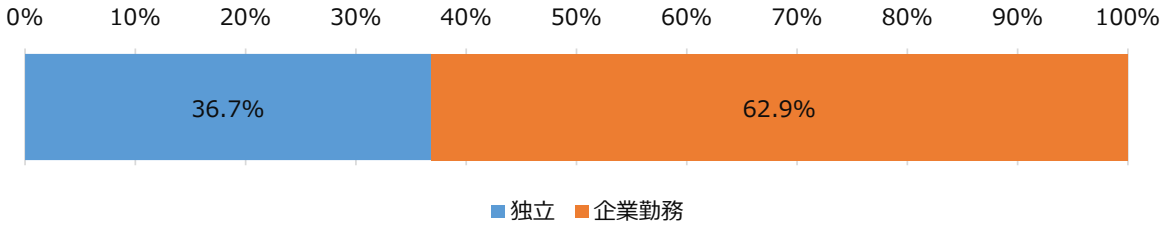
3．登録セキスペが実施可能な業務やスキル等の可視化

- **登録セキスペが提供可能な業務やスキル等を可視化**するため、IPAセキュリティプレゼンターのうち、登録セキスペ資格を有する登録者約800名を対象に**Webアンケート調査を実施**し、**221件の有効回答**を得た。

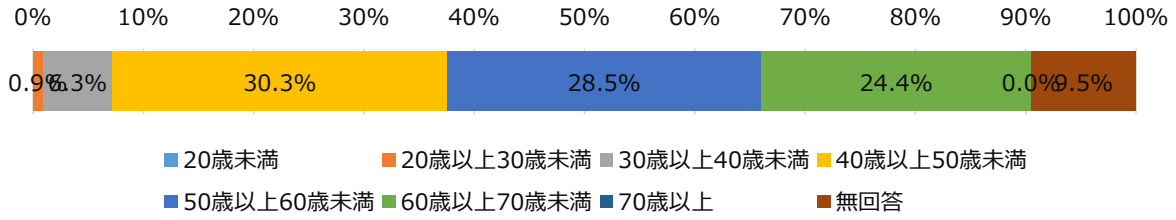
《回答者属性》

- 回答者の所属状況は36.7%が独立、62.9%が企業勤務。年齢分布は50歳以上70歳未満が全体の約5割を占める。
- セキュリティ分野での実務経験は5年以上が29.0%、10年以上が40.3%を占める。
- 企業に対するセキュリティ対策支援経験は68.8%約が経験ありと回答、そのうち10件以上の支援経験者は24.9%。

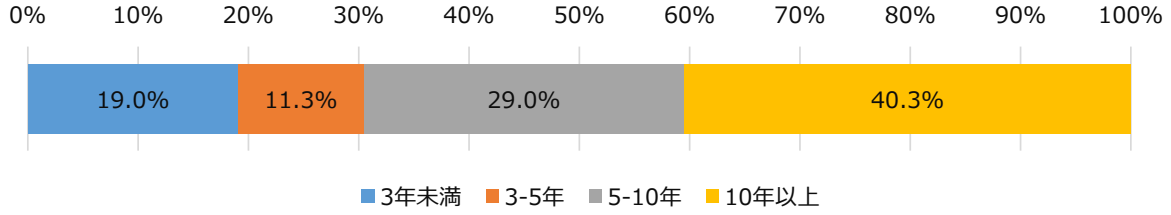
回答者の所属状況 (n=221)



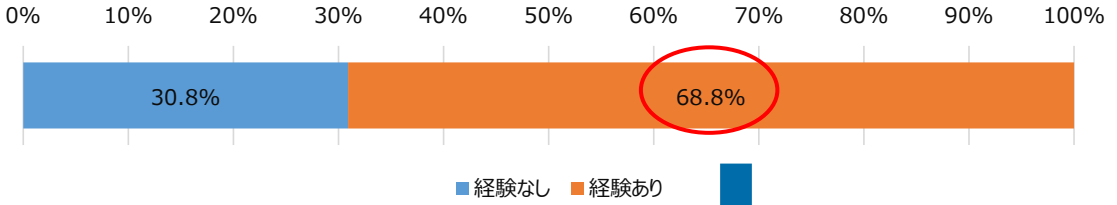
回答者の年齢分布 (n=221)



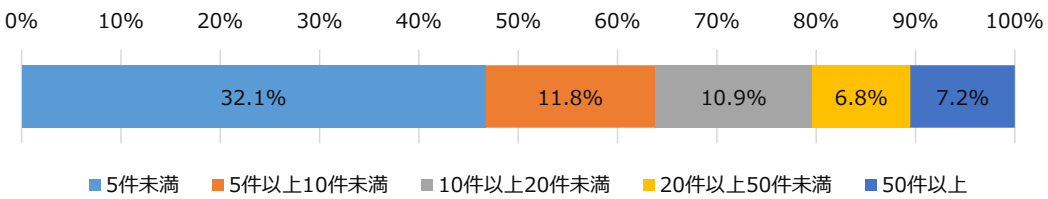
セキュリティ分野での実務経験年数 (n=221)



企業に対するセキュリティ対策支援経験 (n=221)



支援件数 (n=152)



3．登録セキスペが実施可能な業務やスキル等の可視化
① スキルアンケート項目の設計

➢ セキュリティ専門家スキル調査アンケートの実施にあたっては、**中小企業へのセキュリティ支援を行うセキュリティ専門家に必要なスキルを分析**し、その結果に基づいて**アンケート項目を作成**した。併せて、別途保有する資格や、セキュリティ支援実績、得意業種、支援可能地域、対応できるマネジメント指導テーマ等を調査し、**アクティブリスト試作のベース情報**とした。

《セキュリティ専門家スキル調査アンケート項目の設計》

NIST Cybersecurity Framework 2.0
1.統治（Govern）
2.特定（Identify）
3.防御（Protect）
4.検知（Detect）
5.対応（Respond）
6.復旧（Recover）

セキュリティ支援領域
1. セキュリティ対策の体制づくりと管理
2. セキュリティリスクの識別
3. 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と監視、検知後の運用の策定
5. サイバー攻撃発生時の対応
6. インシデントからの復旧とコミュニケーション

①中小企業へのセキュリティ支援領域として「NIST Cybersecurity Framework 2.0 : Small Business Quick-Start Guide（以下「NIST CSF2.0という」） 」を参考に６つの支援領域を定めた。
②NIST CSF2.0ガイドに示された中小企業向け実行項目を基に、支援内容と支援に必要とされる専門家スキル（アセスメント基準）の洗い出しを行った。
③洗い出したスキルは6つの大分類（支援領域）と小項目（アセスメント基準）に整理し、項目ごとに専門家の実行レベルを問うアンケート項目を作成した。実行レベルの具体的な評価方式は、0～3*の4段階の自己評価で行ってもらうこととし、また、小項毎の回答根拠となる実績・経験を自由記述形式で記入できるようにした。（*0:知識・経験なし1:基礎知識のみ2:サポートがあれば実行可能3:単独実行可能）

支援領域と必要とされる専門家スキルの対応例（S1：セキュリティ対策の体制づくりと管理）

支援領域	必要とされる専門家スキル（アセスメント基準）	NIST Cybersecurity Framework 2.0 Small Business Quick-Start Guide 実行項目に対応する支援策
1. セキュリティ対策の体制づくりと管理	経営戦略理解力：企業のビジョン、経営目標、マーケティング戦略を理解し、サイバーセキュリティインシデントがもたらすビジネスリスクを正しく評価できる	・サイバーセキュリティリスクがビジネスの使命達成をどのように妨げるかについて企業が正しく理解するための支援を行う。(GV.OC-01)
	業界固有ガイドライン知識：特定業界のサイバーセキュリティガイドラインを詳細に説明し、適用できる	・法的、規制上、契約上のサイバーセキュリティ要件や業界固有のガイドラインを理解するための支援を行う。(GV.OC-03)
	セキュリティ体制構築能力：企業規模や業種に応じた適切なセキュリティ体制を設計・構築できる	・サイバーセキュリティ戦略の開発と実行を担当する責任者を確立し、責任者がその役割を理解するための支援を行う(GV.RR-02)
	サイバーリスク定量化スキル：サイバー攻撃による潜在的な経営損失を具体的な数値で算出できる	サイバーリスクが顧客企業の業務もしくはビジネスに対して及ぼす、全体的または部分的な損失を正しく計算・評価する。(GV.OC-04)
	サイバー保険知識：各種サイバー保険商品の特徴、適用範囲、コスト効果を比較説明できる	・ビジネスリスクを踏まえ、必要なサイバーセキュリティ保険の加入支援を行う。(GV.RM-04)
	サプライチェーンリスク評価能力：取引先やクラウドサービス提供者のセキュリティリスクを評価できる	・正式な関係を結ぶ前に、サプライヤーや取引先など第三者がもたらすサイバーセキュリティリスクを洗い出し、評価する支援を行う。(GV.SC-06)
	経営層説得力（セキュリティ重要性）：セキュリティ対策の重要性を他のビジネスリスクと比較しながら経営者に説明できる	・サイバーセキュリティリスクを他のビジネスリスクと同等に、優先的に管理する重要性を企業が理解するための支援を行う。(GV.RM-03)
	セキュリティ文化醸成能力：組織全体のセキュリティ意識向上のための具体的な施策を提案・実施できる	・経営者がセキュリティリスクを認識し、企業内に倫理的、継続的にリスク改善を行う文化を醸成することの重要性を理解するための支援を行う。(GV.RR-01)
	セキュリティポリシー運用力：セキュリティポリシーの策定から日常的な運用、評価、改善までのプロセスを管理できる	・情報セキュリティポリシーを社内に伝達し、実施、維持するための支援を行う(GV.PO-01)

3．登録セキスペが実施可能な業務やスキル等の可視化
② スキルアンケート回答者の保有スキル状況

➢ セキュリティ専門家スキル調査アンケートの回答者（221名）の**保有スキル状況の集計結果**は以下のとおり。

登録セキスペの「強み」スキル：　情報資産の洗い出しや、それに基づくリスク分析、アカウント管理、アクセス管理、社内セキュリティ教育等の支援（S2,S3）においては、約33%の専門家が「単独での支援が可能」と回答。

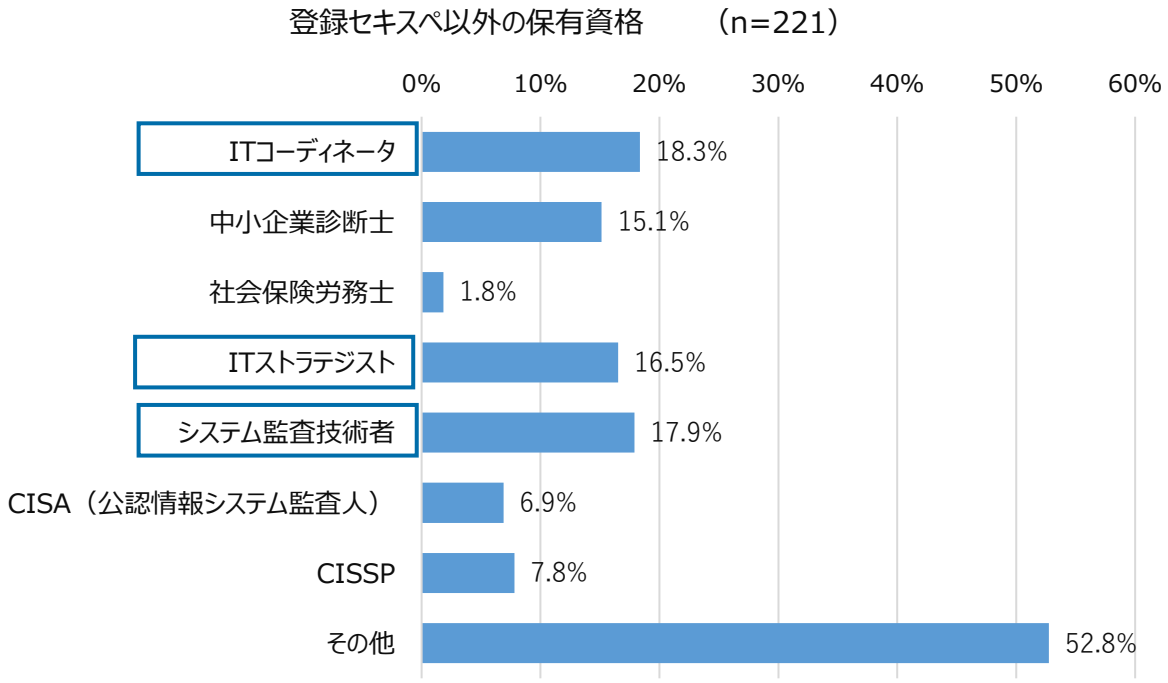
登録セキスペの「弱み」スキル：　セキュリティインシデント発生時の対応と復旧対応支援（S5,S6）においては、約40%の専門家が「実践的な運用には至っていない」段階であると回答。

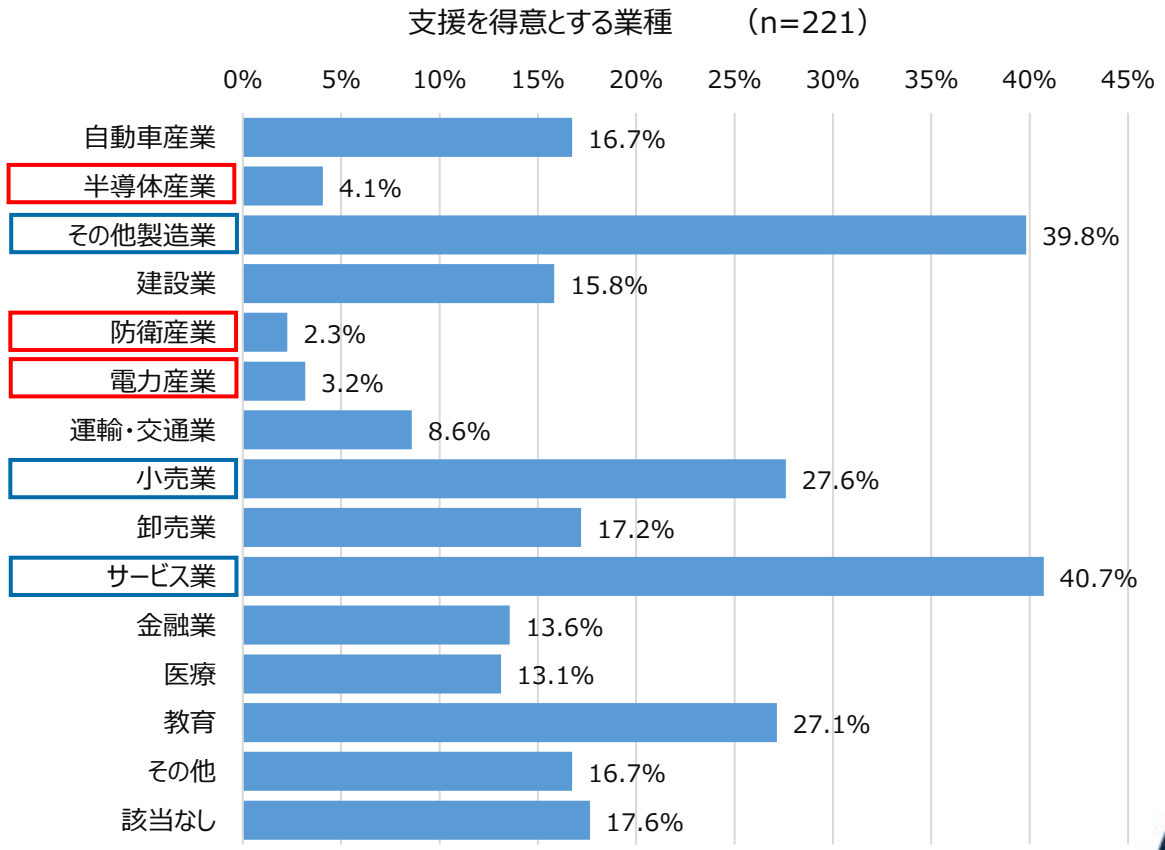
（n=221）

スキルNo.	スキル名（支援領域）	実行可能な支援能力	単独での支援が可能	他の専門家の指導・サポートがあれば支援可能	実践的な運用には至っていない
S1	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	経営戦略の理解、経営者とのコミュニケーション、サイバーセキュリティ対策体制の構築、サイバーセキュリティ対策の基本方針の構築と運用、外部リスク評価力、コンプライアンス対応	52名	137名	32名
S2	セキュリティリスクの識別	情報資産の洗い出しと情報資産管理台帳の運用設計、潜在リスクの特定と評価、リスクに基づくサイバーセキュリティ対策の策定、現存対策の評価及び改善点の指摘、社内外におけるサイバーセキュリティ対策の推進	74名	119名	28名
S3	サイバーセキュリティ対策の実践と運用の強化	アカウント管理、アクセス管理、データ管理、システムセキュリティ管理、コンテンツセキュリティ管理、社内セキュリティ教育の策定と運用	73名	129名	19名
S4	サイバー攻撃の検知と監視、検知後の運用策定	セキュリティインシデント対処教育の策定と実施、ウイルス対策ソフトの運用、システム・ネットワークの監視、外部監視サービスの導入、インシデント初動の運用設計と教育実施能力	46名	139名	36名
S5	サイバー攻撃発生時の対応	セキュリティインシデント対応（セキュリティインシデント対応計画の策定、セキュリティインデント調査・対応、セキュリティインシデント報告・公表支援）	50名	82名	89名
S6	セキュリティインシデントからの復旧とコミュニケーション	セキュリティインシデント復旧支援、インシデント事後報告書作成、データ復旧、復旧行動の優先順位付け、ステークホルダーとのコミュニケーション	42名	91名	88名

3．登録セキスペが実施可能な業務やスキル等の可視化
③ 登録セキスペ以外の保有資格と支援を得意とする業種

- セキュリティ専門家スキル調査アンケートの回答で、登録セキスペ以外で最も保有の多い資格は、「ITコーディネータ」、「システム監査技術者」、「ITストラテジスト」の３つであった。
- 支援を得意とする上位3業種は、「サービス業」、「製造業（自動車産業、半導体産業を除く）」、次いで「小売業」）であった。一方、最も少ない下位3業種は、「防衛産業」、「電力産業」、「半導体産業」であった。

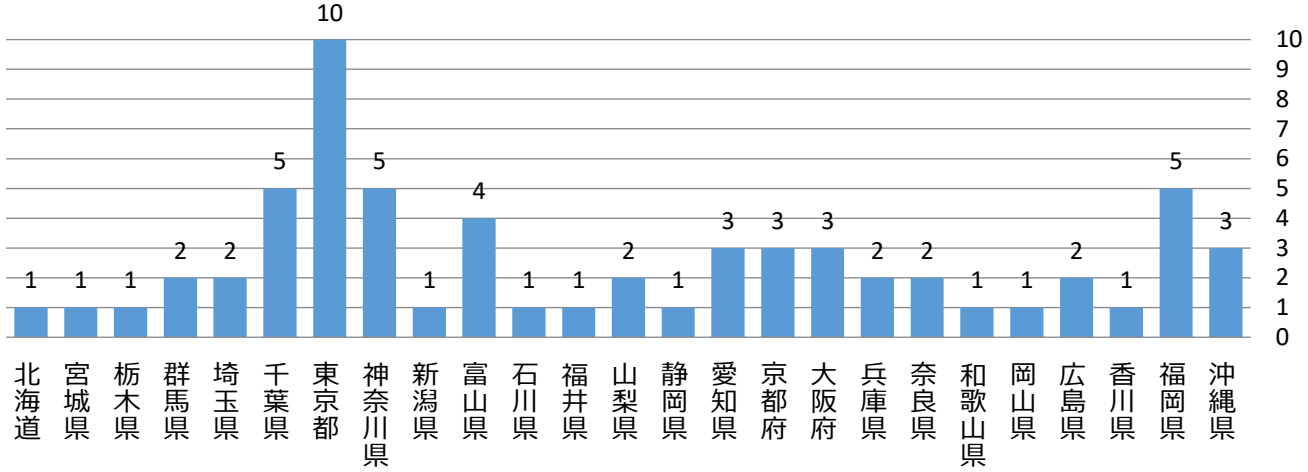




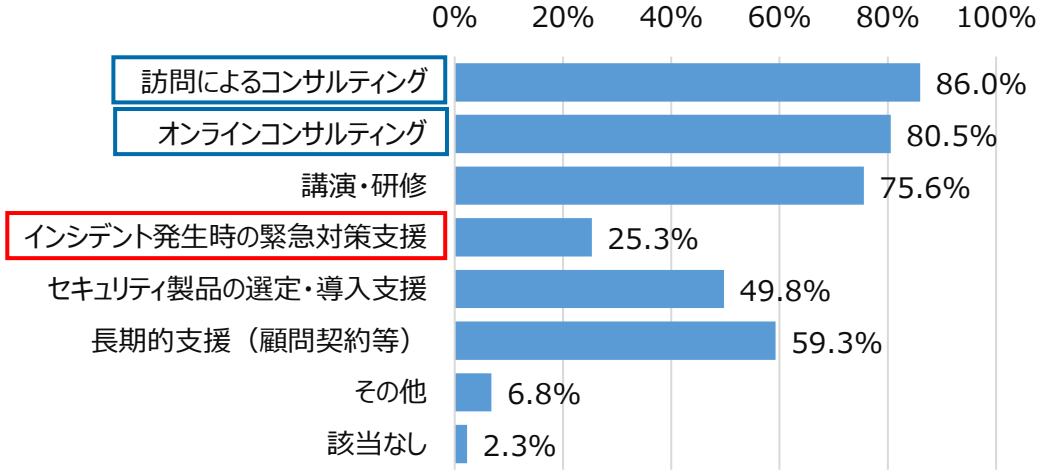
3．登録セキスペが実施可能な業務やスキル等の可視化
④ 商工会議所等とのつながり、希望する支援形態

- セキュリティ専門家スキル調査アンケートで、商工会議所・商工会とつながりがあると回答した登録セキスペが存在する地域は25都道府県、22県においてはつながりがある登録セキスペが不在。一方、登録セキスペが支援可能な地域については、アンケート回答により全国的に支援の提供が可能であることが判明した。
- 登録セキスペが希望する支援形態は、「訪問によるコンサルティング」が最も多く、「オンラインコンサルティング」もほぼ同等数の登録セキスペが希望すると回答した。一方、「インシデント発生時の緊急対策支援」を希望する登録セキスペは全体の約25%で、スキル調査の保有スキルの状況と連動する結果となった。

（居住地別）商工会議所・商工会とつながりがある登録セキスペ　（n＝63）



登録セキスペが希望する支援形態　（n=221）



《中小企業の支援可能なセキュリティ人材》
セキュリティ専門家スキル調査アンケートの回答221件のうち、5件はスキル無回答、10件は勤務先都合で中小企業への支援不可、3件はリスト掲載NGであった。このため、計18件についてはアンケート集計や分析の対象とするものの、アクティブリスト掲載情報としては除外することとした。この結果、次項で述べるアクティブリスト掲載対象者は203件とした。

4．アクティブリストの試作

- 本事業における中小企業とセキュリティ専門家とのマッチング、及びセキュリティ専門家スキルアンケート調査で得られた結果を基に、登録セキスペの得意分野・専門領域を可視化し、**中小企業のセキュリティ支援が実施可能なセキュリティ専門家リスト**として、**アクティブリストを試作**した。

《アクティブリストの基本事項の整理》

Ⅰ　リストの目的

- 登録セキスペがその専門性を中小企業への支援に活用できる場の創出
- 地域の中小企業、特に重要産業におけるセキュリティ対策の推進

Ⅱ　リスト掲載対象者

- 登録セキスペ資格を有する者で、中小企業に対するセキュリティ対策支援が可能な者
（企業に所属する者で副業・兼業で支援が可能な者もリスト掲載対象とする）
※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

Ⅲ　リスト管理・運用方式

- リストの掲載情報の信頼性の確保のため、以下の運用体制を検討する
・リスト掲載のセキュリティ専門家の資格要件確認
・定期的なリスト掲載情報の更新と実績の追加

Ⅳ　検索・表示機能

- リストの掲載情報の検索及び表示方法について検討する
（検索例）支援内容／支援地域／業種／料金／支援期間

Ⅴ　リスト掲載項目

1．専門家の基本情報：
・氏名、登録セキスペ登録番号、写真
・所属状態（独立/企業所属）、所属組織・企業名
・居住地、連絡先（メールアドレス）

2．支援能力に関する情報：
・IPAが提供する指導ツールを活用したセキュリティ支援の対応
（情報セキュリティ規程の整備、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、従業員向けセキュリティ教育の5テーマ）
・保有する他の資格（中小企業診断士、ITコーディネータ等）
・得意とする業界
・中小企業支援の実績、具体的な支援事例
・スキル調査に基づく、得意とする支援領域

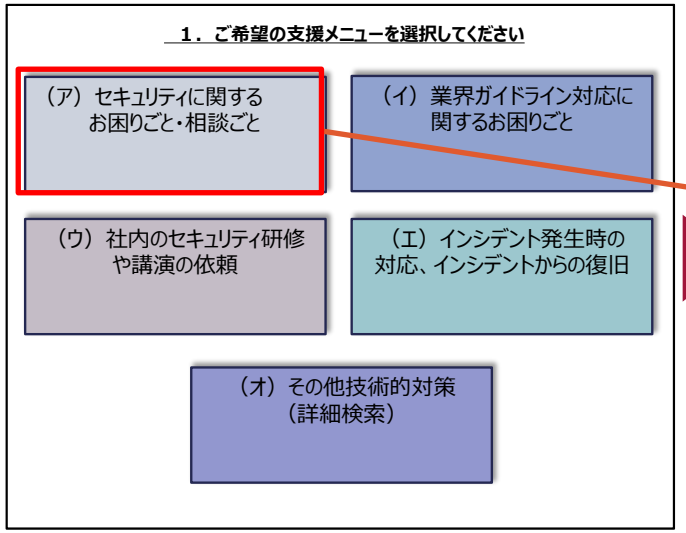
3．サービス提供条件に関する情報：
・支援形態（訪問/オンライン、コンサル/研修等）
・料金（1回2時間あたりの支援料金）
・支援可能期間
・支援可能地域

4．自己PR：
・支援実績や得意分野に関する自由記述

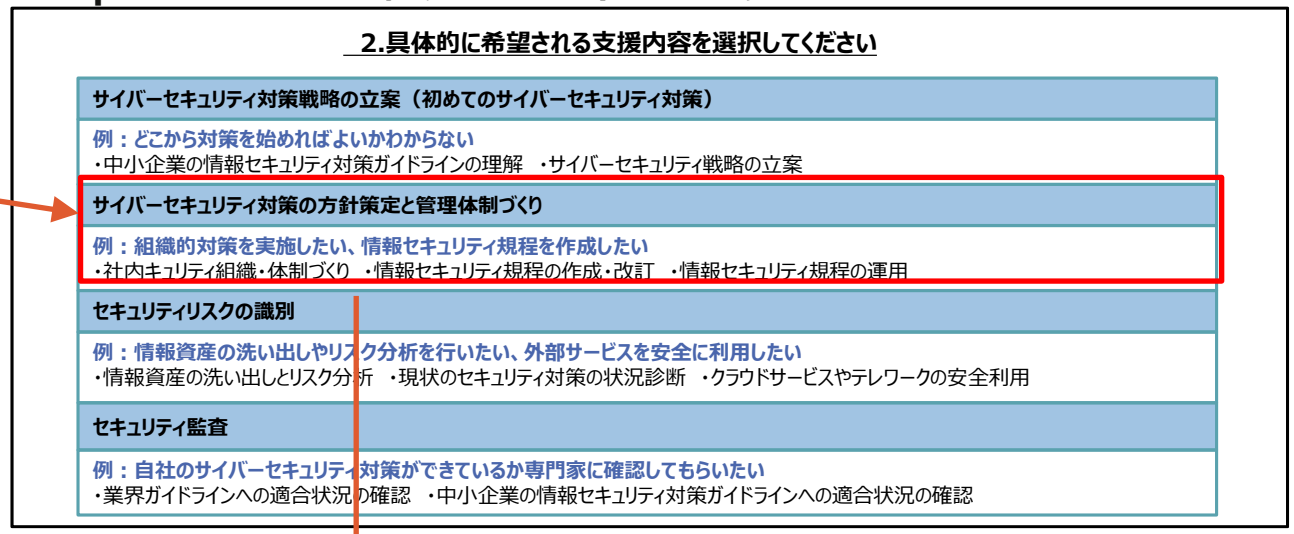
4. アクティブリストの試作
① リスト画面遷移の検討

➢ アクティブリストをシステム（WEBインターフェイスを想定）実装する際の画面遷移の考え方について検討した。

Step1:初めに希望する支援内容を選択する



Step2:支援内容の詳細や希望の条件を入力する



Step3:条件に適合したセキュリティ専門家の名前をクリック

氏名	支援可能な指導テーマ	中小企業支援実績	得意とする業界	支援対象地域	支援形態	支援期間	支援料金（1回2時間あたり）	保有する他の資格	所属状況	所属先
AAA	1．情報セキュリティ規程の作成 2．情報資産の洗い出しとリスク分析		製造業、建設業	大阪、奈良、京都、兵庫	訪問コンサルティング、オンラインコンサルティング、講習・研修	スポット、3か月～半年	1回：40,000～	・CISSP	企業勤務	XX XX
BBB	1．情報セキュリティ規程の作成 5．従業員セキュリティ教育	・ISMS認証取得支援、Pマーク認証取得支援	自動車産業	奈良、滋賀、京都、三重、岐阜	訪問コンサルティング、オンラインコンサルティング、講習・研修、セキュリティ製品の選定・導入支援	スポット、1～3か月、3か月～半年、半年～1年	1回：50,000～	・ITコーディネータ	独立	XX XX

Step4:セキュリティ専門家の詳細が個票として表示される

4. アクティブリストの試作
② 支援メニューと専門家スキルの対応

➢ セキュリティ専門家スキル調査アンケートで回答を得た**登録セキスペの保有スキルを可視化**し、アクティブリストの「得意とする支援領域」に表記することで、**リスト利用者が直感的にセキュリティ専門家のスキルレベルを把握**できるようにした。

《セキュリティ専門家の保有スキル評価例》

例：支援領域S1の小項目(S1-a,S1-b,S1-c) のスキル回答に対する評価

【S1】 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	専門家A	専門家B	専門家C
S1-a 経営戦略の理解、経営者とのコミュニケーション（質問数5） [評点:13点]	3点×5 計15点:評点以上 **スキル有り**	3点×2、2点×3 計12点:評点以下	3点×3、2点×1、1点×1 計12点:評点以下
S1-b サイバーセキュリティ対策体制の構築、サイバーセキュリティ対策の基本方針の策定と運用（質問数2） [評点:5点]	3点×2 計6点:評点以上 **スキル有り**	3点×1、2点×1 計5点:評点以上 **スキル有り**	3点×1、2点×1 計5点:評点以上 **スキル有り**
S1-c 外部リスク評価力、コンプライアンス対応（質問数2） [評点:5点]	3点×1、2点×1 計5点:評点以上 **スキル有り**	3点×2 計6点:評点以上 **スキル有り**	2点×1、1点×1 計3点:評点以下
総合評価	◎	○	

↑上記の例では、専門家AはS1スキル「◎」、専門家Bは「○」、専門家Cは「空白」と表記される。

【保有スキルの評価方法】

Step１：小項目(a,b,c)評点の設定

スキル調査では、支援領域（S1～S6）の下に複数の小項目（a, b, c）を設け、より詳細にスキルの保有状況を聞いている。これらの小項目には、含まれる質問項目数に応じた評点を設定した。

【評点】設定： 質問数が1項目: 評点3点、質問数が2項目: 評点5点、質問数が3項目: 評点7点、質問数が4項目: 評点10点、質問数が5項目: 評点13点

Step２：専門家回答データの小項目ごとの集計と評価

専門家が回答した内容は、小項目ごと単純合計し評点と比較する。評点より高い得点を有するものだけを「スキル有り」と判断。

質問回答：0～３

（0:知識・経験なし、1:基礎知識のみ、2:サポートがあれば実行可能、3:単独実行可能）

Step３：スキル（支援領域）毎の総合評価

全ての回答を小項目ごとに集計・評価後、支援領域ごとにスキルを有しているか、総合評価を行った。

【総合評価】：「◎」（二重丸）：当該スキル領域のすべての小項目が設定評点以上である場合
「○」（丸）：当該スキル領域において1つの小項目のみが設定評点に達していない場合
無表記: 当該スキル領域において2つ以上の小項目が設定評点に達していない場合

Step4:アクティブリストへの反映

アクティブリストの「得意とする支援領域」へ可視化した各セキュリティ専門家のスキル状況を反映した。

4. アクティブリストの試作
（参考）アクティブリスト（試作）一覧表イメージ

➢ 本事業で作成したアクティブリスト（試作）の一覧表イメージを以下に記す。

《アクティブリスト（試作）一覧表イメージ》

氏名	支援可能な指導テーマ	中小企業支援実績	得意とする業界	支援対象地域	支援形態	支援期間	支援料金（1回/2時間あたり）	保有する他の資格	所属状況	所属先	得意とする支援領域							
											0	1	2	3	4	5	6	7
AAA	1．情報セキュリティ規程の作成 2．情報資産の洗い出しとリスク分析		製造業、建設業	大阪、奈良、京都、兵庫	訪問コンサルティング、オンラインコンサルティング、講習・研修	スポット、3か月～半年	1回：40,000円以上	・CISSP	企業勤務	XX XX	◎	◎	◎					
BBB	1．情報セキュリティ規程の作成 5．従業員セキュリティ教育	・ISMS認証取得支援、Pマーク認証取得支援	自動車産業	奈良、滋賀、京都、三重、岐阜	訪問コンサルティング、オンラインコンサルティング、セキュリティ製品の選定・導入支援	スポット、1～3か月	1回：20,000円以上～30,000円未満	・ITコーディネータ	独立	XX XX	○	○	○	○				
CCC	1．情報セキュリティ規程の作成 2．情報資産の洗い出しとリスク分析 5．従業員セキュリティ教育	・中小企業向け情報セキュリティマネジメント対応	金融業、小売業、卸売業	大阪、奈良、和歌山	訪問コンサルティング、オンラインコンサルティング、講習・研修	スポット、1年以上	1回：30,000円以上～40,000円未満	・公認システム監査人 ・中小企業診断士	独立	XX XX	◎	◎		○				◎

4. アクティブリストの試作
③ アクティブリスト活用の検討

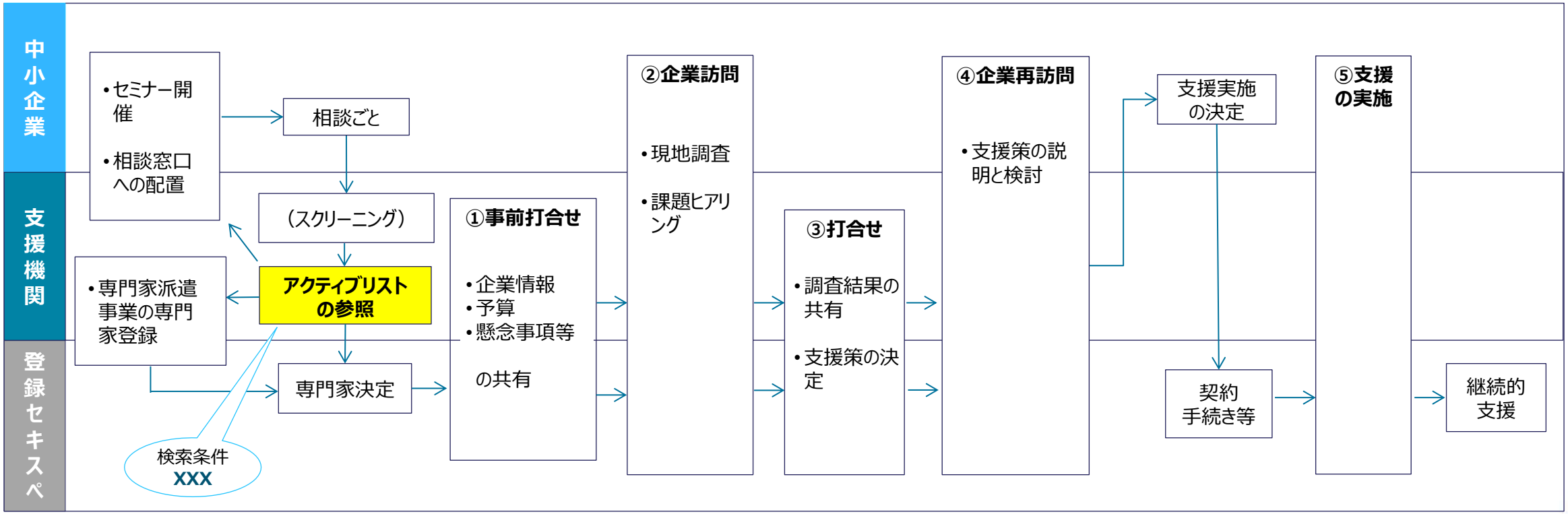
- サイバーセキュリティ相談会の参加者アンケートによると、**中小企業がセキュリティ専門家を探す際**には、「公的機関（IPA等）による専門家リストの利用」、「商工会議所等、中小企業支援機関による紹介」、「取引のあるITベンダーからの紹介」を望む声が多く、**「信頼性」、「身近さ」、「地域性」を重視**することが判明した。
- そこで、アクティブリストの活用について、中小企業がセキュリティ専門家を直接探索する場合の他、**①中小企業支援機関との連携**、**②ITベンダーにおける利用**の2つの活用シナリオを想定し、リストの活用方法について検討した。

活用シナリオ	アクティブリストの活用検討
①中小企業支援機関との連携	• 商工会議所等の中小企業支援機関は、中小企業からは「安心」「信頼」できる情報発信者として評価する声が多く聞かれ、サイバーセキュリティの技術的対応、対策セミナーや講演等の実施について、期待されていることが示唆された。また、指導専門家からは中小企業とのマッチング機会の創出について、商工会議所等の支援機関に対する期待は高かった。 • そこで、中小企業支援機関が行うセミナーや相談窓口、専門家派遣事業の担い手として、アクティブリストを活用して地域のセキュリティ専門家を選定、または中小企業とのマッチングを行うことが考えられる。
①ITベンダーにおける利用	• 中小企業のシステム開発やシステム機器の納入前後に、セキュリティ的観点からの確認を行うことが求められてきており、中小企業の立場からのITベンダーの提案に対する目利き役としての役割、ITベンダーと中小企業経営者との橋渡し役としての役割等、登録セキペの活用の場となる可能性があることが分かった。 • 今後、システム開発及び導入案件の中で、セキュリティ専門家を必要とするケースは多くなると予想され、ITベンダーとユーザー企業の双方が、必要とするセキュリティ専門家を適切に見つける仕組みとして、アクティブリストの活用が考えられる。

4. アクティブリストの試作
（参考）アクティブリスト活用シナリオ①（中小企業支援機関）

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

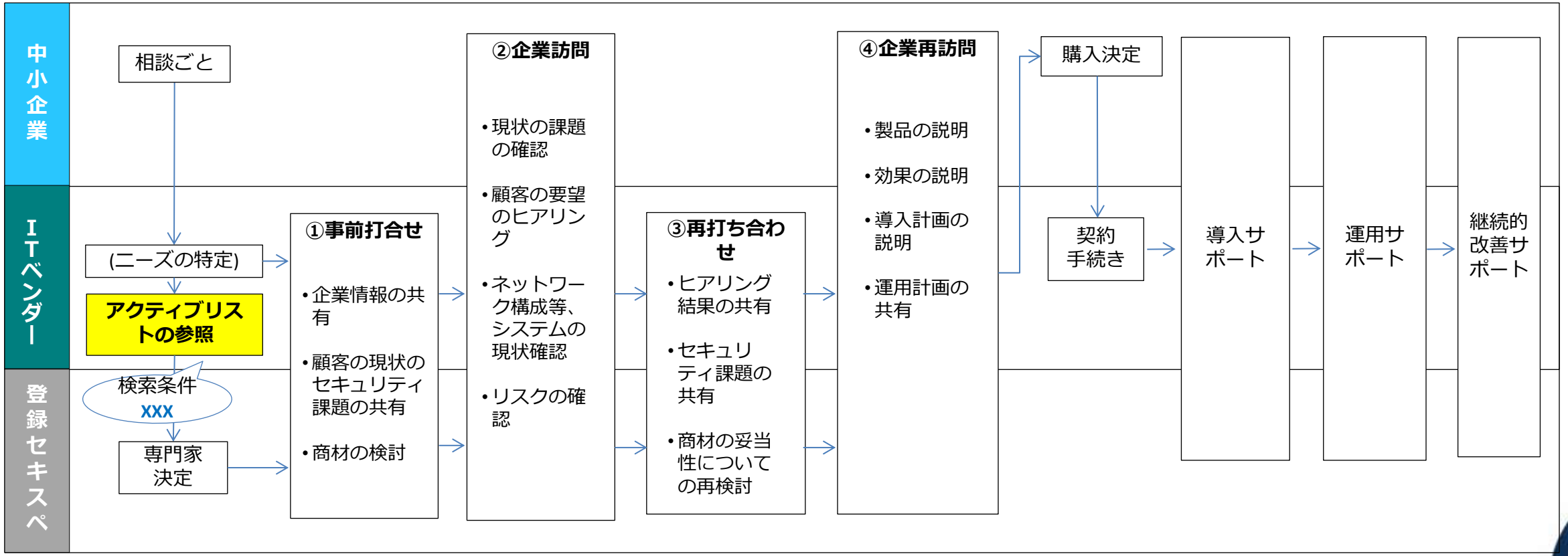
登録セキスペが中小企業に対して担う役割	社内ITリソースの補完者としての役割、経営者への説得者としての役割、包括的なセキュリティ戦略の立案と実施者の役割、セキュリティ製品導入後の品質担保者としての役割、効果的なIT投資実現のためのパートナーとしての役割
登録セキスペが支援機関に対して担う役割	支援プログラム実施のための専門的パートナーとしての役割
支援機関が中小企業に対して担う役割	中小企業とセキュリティ専門家・関係者とのネットワーク構築を支援者する役割



4. アクティブリストの試作
（参考）アクティブリスト活用シナリオ②（ITベンダー）

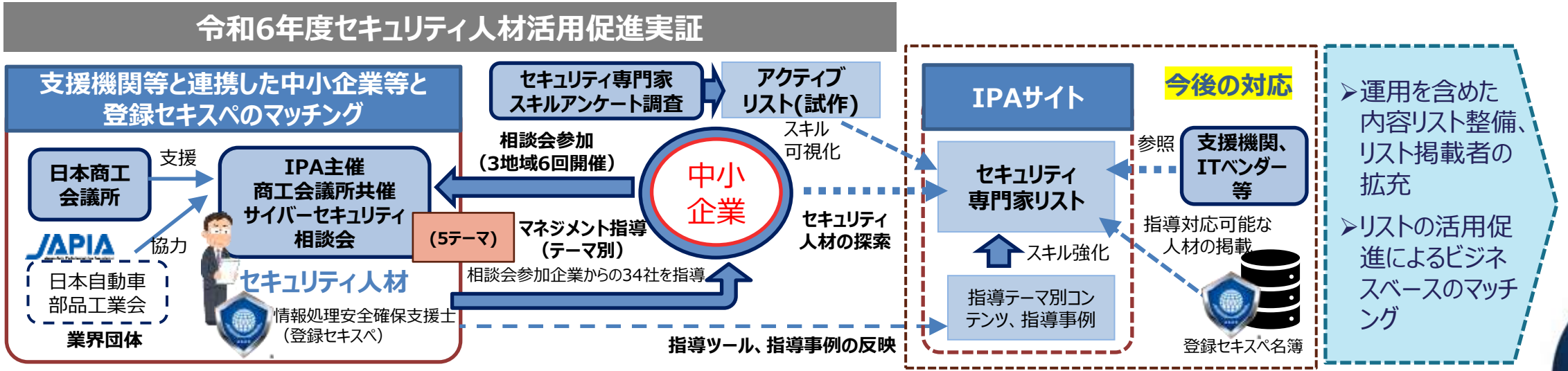
活用シナリオ②	（利用者）　ITベンダー （利用目的）顧客の中小企業へのセキュリティ商材導入をサポートする登録セキスペを選定する

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



まとめ

- 本事業では、**中小企業等と登録セキスペのマッチング**を促す場として、商工会議所との共催による**サイバーセキュリティ相談会**（3地域6回）を開催し、個別相談を経て希望する企業に対して、登録セキスペによる**セキュリティマネジメント指導**（訪問指導）を実施、参考になる**指導事例をベストプラクティス**として取りまとめた。
- セキュリティマネジメント指導の実施に際し、中小企業セキュリティ対策ガイドライン（付録を含む）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。
- また、**登録セキスペが提供可能な業務やスキル等を可視化**するため、**セキュリティ専門家スキル調査アンケート**を実施し、中小企業とセキュリティ専門家とのマッチング実証の結果も含めて、中小企業のセキュリティ支援が実施可能な登録セキスペの**アクティブリストを試作**した。
- 今後は、**セキュリティ専門家リスト**として、運用を含めた**リストの整備**及び**リスト掲載者の拡充**、中小企業支援機関等との連携を中心とした**リストの活用促進**によるビジネスベースのマッチングが望まれる。




IPA