

令和2年度

中小企業の情報セキュリティマネジメント指導業務

成果報告書

2021年6月4日



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

目 次

はじめに	1
1. 業務の概要.....	2
1.1. 事業名	2
1.2. 実施期間.....	2
1.3. 目的	2
1.4. 対象	4
1.5. 事業概要.....	5
2. セキュリティマネジメント指導に係る事務局の設置.....	7
3. 指導先企業の募集及び受付	8
3.1. 中小企業等の募集活動.....	8
3.2. 参加する中小企業等の申込受付	14
3.3. 指導先企業と専門家のマッチング	17
4. セキュリティマネジメント指導に係る指導要領（指導ツール）の作成....	18
5. 専門家の募集・登録及び指導講習会の開催	23
5.1. 専門家の募集案内の作成	23
5.2. 専門家の募集活動	23
5.3. 指導講習会の開催	23
5.4. 専門家の登録手続	29
6. 専門家の指導管理及び謝金支払い	32
6.1. 実施要領の作成.....	32
6.2. 専門家指導の結果	38
6.3. 専門家への委嘱.....	43
6.4. 指導先企業別の指導最終報告.....	44
6.5. 専門家からの問い合わせ対応.....	52
6.6. 専門家による指導実績のまとめ	53
7. 指導先企業及び専門家へのアンケート実施	54
7.1. 指導先企業アンケート.....	54
7.2. 専門家（登録セキスペ（RISS））アンケート.....	73
7.3. 指導先企業へのヒアリング調査	77
8. 中小企業向けの伴走型支援サービス検討のための関係調査	82
8.1. 調査の目的	82

8.2. 自治体事業調査の方法.....	82
8.3. 自治体事業調査の結果.....	83
8.4. 伴走型支援サービスの実現に関する考察.....	85
9. 成果報告.....	87
9.1. 本事業の成果（有効性の検証）.....	87
9.2. 中小企業等の現状と課題.....	88
9.3. 専門家の現状と課題.....	89
9.4. 事業運営に関する課題.....	90
9.5. 登録セキスペ（RISS）の活用機会の検討.....	92
資料.....	94
添付資料 1 中小企業向け募集チラシ.....	94
添付資料 2 専門家向け募集チラシ.....	95
別紙 1 指導要領（指導ツール）	
別紙 2 セキュリティマネジメント指導事例集	

はじめに

本書は、独立行政法人情報処理推進機構（以下「IPA」という。）が令和2年度に実施した「令和2年度中小企業の情報セキュリティマネジメント指導業務」の成果報告書である。

本事業の活動の詳細は1章から8章にまとめられており、9章で総括している。

1. 業務の概要

1.1. 事業名

令和2年度中小企業の情報セキュリティマネジメント指導業務

1.2. 実施期間

令和2年9月4日（金）から令和3年2月15日（月）

1.3. 目的

あらゆる産業活動においてサプライチェーンのセキュリティリスクの問題が顕在化しつつある昨今、標的型攻撃などのサイバー攻撃の対象は政府機関や大企業だけでなく、中小企業の場合は取引先を標的とした攻撃の踏み台にされるケースも増加している。IPAが公表した「情報セキュリティ10大脅威 2020¹」によれば、「サプライチェーンの弱点を悪用した攻撃」が、組織における脅威のランキングで2年連続4位にランクインしていることから、サプライチェーンを構成する中小企業のサイバーセキュリティ対策を進めることは喫緊の課題である。

また、IPAが実施した「2018年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査報告書²」では、中小企業においては、情報セキュリティに関する規程や手順書の策定が現状では不十分、情報セキュリティ対策を相談する専門家が周りにいない等のマネジメント上の課題が確認された。

そこでIPAでは、令和元年度に「中小企業の情報セキュリティマネジメント指導業務³」として、全国の中小企業を対象に情報セキュリティに関する専門家（以下「専門家」という。）を派遣し、中小企業の各現場に応じたリスクの洗い出しから、セキュリティ基本方針や関連規程の策定に向けた支援を行う情報セキュリティマネジメント指導（以下「セキュリティマネジメント指導」という。）を実施した。専門家には情報処理安全確保支援士⁴（以下「登録セキスペ

（RISS）」という。）等を起用し、参加した指導先中小企業（以下「指導先企業」という。）382社に1社あたり4回の派遣を行ったところ、アンケートでは96.4%の指導先企業が、専門家による指導を受けて情報セキュリティの管理・運用・実践等において成果を得ることができたと回答し、身近な専門家の有効性や役割の重要性が確認された。他方、当該業務の課題として、登録セキスペ（RISS）からは中小企業との繋がり（コネクション）やコンサル業務への不安（スキ

¹ <https://www.ipa.go.jp/security/vuln/10threats2020.html>

² <https://www.ipa.go.jp/security/fy30/reports/sme/index.html>

³ <https://www.ipa.go.jp/security/fy2019/reports/sme/management.html>

⁴ 2016年10月改正の「情報処理の促進に関する法律」に基づく、セキュリティ国家資格保持者
<https://www.ipa.go.jp/siensi/>

ル不足)等が示されていたこと、指導先企業が3大都市圏(首都圏⁵・中京圏⁶・近畿圏⁷)に偏重する傾向となっていたこと等があげられた。

さらに、新型コロナウイルス対応の一環で企業がテレワーク等の業務のデジタル化を急速に進める中、大阪商工会議所が令和2年6月に実施した「中小企業のテレワークについての緊急アンケート調査⁸」では、中小企業のテレワーク実施企業の46%が「運用規程を(殆ど)整備しないまま導入」し、セキュリティの強化が課題であると回答しており、テレワークを導入する中小企業のサイバーセキュリティ対策強化が急務である。

これらのことから、令和2年度においては、IPA中期目標に即して、特に3大都市圏以外の地域(以下「36道県地域」という。)の中小企業の参加を促進しつつ、情報セキュリティに関する人的リソースが不足しているサプライチェーンを構成する中小企業、及びテレワーク導入等の業務のデジタル化を進める中小企業に対して、登録セキスペ(RISS)等の専門家を派遣するセキュリティマネジメント指導を実施した。

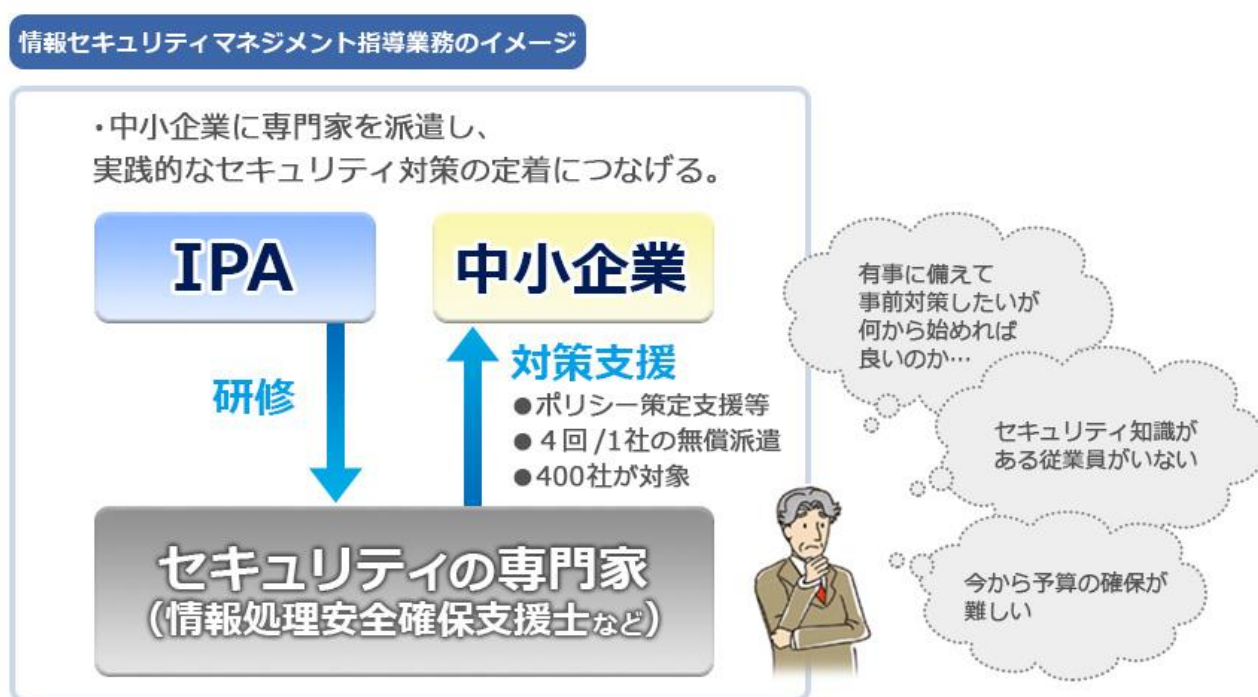


図 1 本事業の実施イメージ

⁵ 首都圏: 東京都、神奈川県、埼玉県、千葉県

⁶ 中京圏: 愛知県、岐阜県、三重県

⁷ 近畿圏: 大阪府、京都府、兵庫県、奈良県

⁸ https://www.osaka.cci.or.jp/Chousa_Kenkyuu_Iken/press/200619telwk.pdf

本事業の実施にあたっては、専門家派遣・指導により中小企業の情報セキュリティ対策水準の向上を図ると共に、本事業で作成した指導要領の有効性を確認し、指導ツールとして今後の専門家による中小企業等への支援に役立たせるものとした。併せて、セキュリティに係る最新の知識・技能を備えた専門人材である登録セキスペ（RISS）が活躍する機会を創出するため、中小企業向けの伴走型支援サービスの検討に関して必要な情報を収集した。

1.4. 対象

本事業で指導業務の対象とした「中小企業等」の定義は以下のとおりである。

表 1 セキュリティマネジメント指導における中小企業等の定義

業種分類	定義
① 製造業、建設業、運輸業	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
② 卸売業	資本金の額又は出資の総額が1億円以下の会社又は常時使用する従業員の数が100人以下の会社及び個人事業主
③ サービス業(ソフトウェア業又は情報処理サービス業、旅館業を除く)	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が100人以下の会社及び個人事業主
④ 小売業	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が50人以下の会社及び個人事業主
⑤ ゴム製品製造業(自動車又は航空機用タイヤ及びチューブ製造業並びに工場用ベルト製造業を除く)	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が900人以下の会社及び個人事業主
⑥ ソフトウェア業又は情報処理サービス業	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
⑦ 旅館業	資本金の額又は出資の総額が5千万円以下の会社又は常時使用する従業員の数が200人以下の会社及び個人事業主
⑧ その他の業種(上記以外)	資本金の額又は出資の総額が3億円以下の会社又は常時使用する従業員の数が300人以下の会社及び個人事業主
⑨ 医療法人、社会福祉法人	常時使用する従業員の数が300人以下の者
⑩ 学校法人	常時使用する従業員の数が300人以下の者
⑪ 商工会・都道府県商工会連合会及び商工会議所	常時使用する従業員の数が100人以下の者
⑫ 中小企業支援法第2条第1項第4号に規定される中小企業団体	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑬ 特別の法律によって設立された組合又はその連合会	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑭ 財団法人(一般・公益)、社団法人(一般・公益)	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者
⑮ 特定非営利活動法人	上記①～⑧の業種分類に基づき、その主たる業種に記載の従業員規模以下の者

※ 「常時使用する従業員」とは、労働基準法第20条の規定に基づく「予め解雇の予告を必要とする者」を意味する。また、会社役員及び個人事業主は予め解雇の予告を必要とする者に該当しないため、「常時使用する従業員」には該当しないものとする。

※ 上記に該当する事業者であっても、法人格のない任意団体、公序良俗に反する事業者は対象外とする。

1.5. 事業概要

(1) セキュリティマネジメント指導に係る事務局の設置（2章で詳述）

業務開始後、仕様書の要件を満たす事務局を設置した。

(2) 指導先企業の募集及び受付（3章で詳述）

中小企業等の募集活動（チラシの作成・送付、事業告知）、参加中小企業等の申込受付、指導先企業と専門家のマッチングを実施した。

(3) セキュリティマネジメント指導に係る指導要領（指導ツール）の作成（4章で詳述）

専門家が、指導先企業へのセキュリティマネジメント指導を適切に行うために、セキュリティマネジメント指導の具体的な支援の進め方等を記した指導要領（指導ツール）を作成した。

(4) 専門家の募集・登録及び指導講習会の開催（5章で詳述）

登録セキスペ（RISS）等の専門家を対象に、専門家の募集案内の作成、専門家の募集活動、指導講習会の開催（E-ラーニング形式でのオンライン講習）、専門家の登録手続を実施した。

(5) 専門家の指導管理及び謝金支払い（6章で詳述）

専門家が指導を行うための調整業務や進捗管理を記した実施要領の作成、及び謝金支払いのための各種事務手続（支援実績の報告、門家への委嘱、指導先企業別の指導最終報告、専門家からの問い合わせ対応、専門家による指導実績のまとめ）を実施した。

(6) 指導先企業及び専門家へのアンケート実施（7章で詳述）

指導先企業及び専門家を対象に、指導先企業アンケート、専門家（登録セキスペ（RISS））アンケート、指導先企業へのヒアリング調査を実施した。

(7) 中小企業向けの伴走型支援サービス検討のための関係調査（8章で詳述）

登録セキスペ（RISS）の活用機会の創出を目的に、都道府県、政令指定都市、及び県庁が所在する市が行う中小企業向け専門人材派遣支援の状況を文書調査し、登録セキスペ（RISS）派遣等のサービスの実施可能性を考察した。

(8) 実施報告書の作成（9章で詳述）

本事業の本事業の成果（有効性の検証）を含む実施報告書を作成した。

「図 2 本事業の実施概要と各タスクの実施スケジュール」に、本事業の実施概要と各タスクの実施スケジュール、並びに本書の構成を示す。

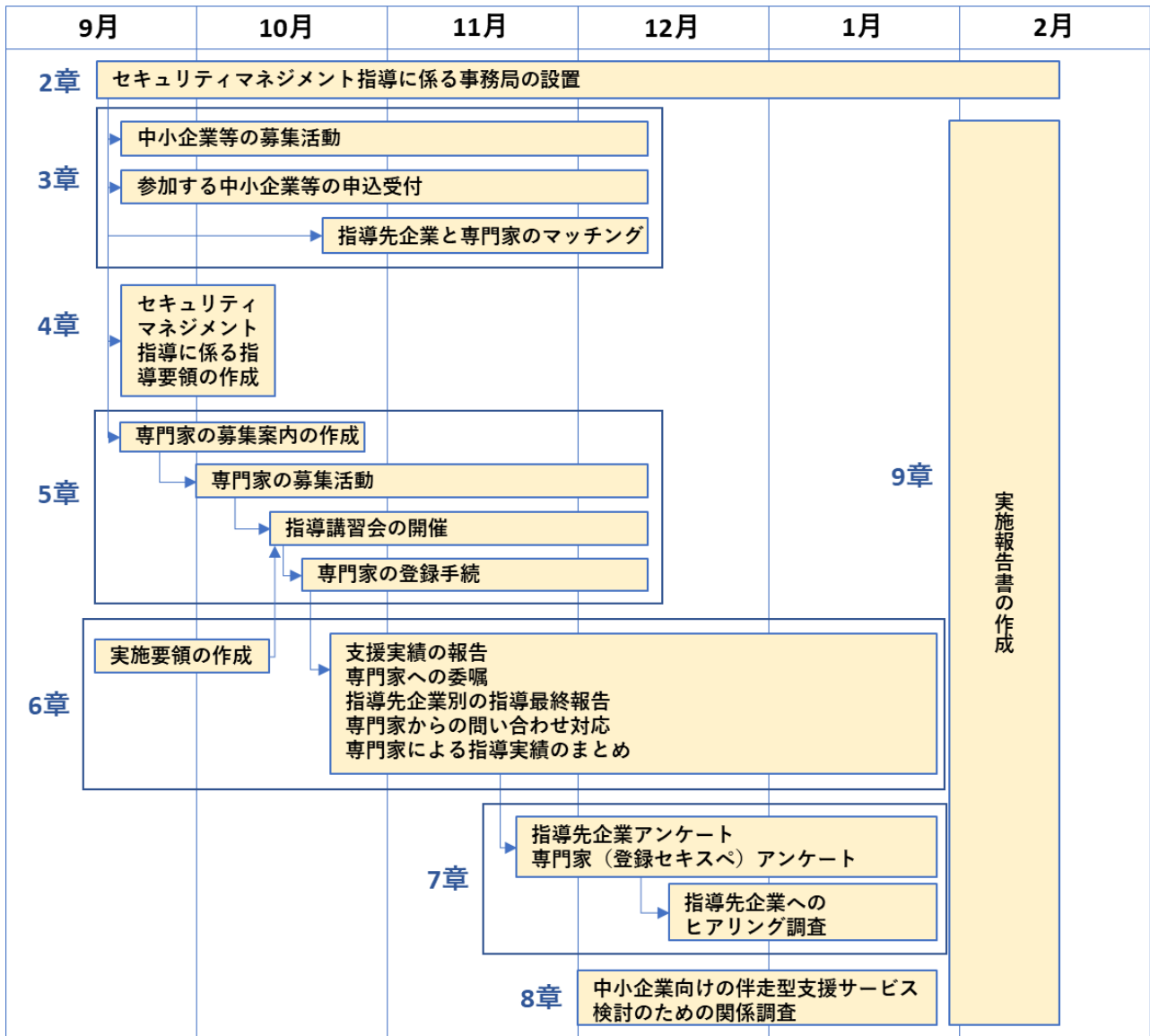


図 2 本事業の実施概要と各タスクの実施スケジュール

2. セキュリティマネジメント指導に係る事務局の設置

業務開始後、以下の要件を満たす事務局を設置した。

<事務局の設置要件>

- ・事務局責任者及び要員を配置。
- ・本事業関係者との連絡用メーリングリストの設置、及び電話・ファックスによる連絡受付体制の整備。
- ・各種申込受付及びアンケート用の Web サイトを用意（ASP サービス利用）。
- ・問い合わせ対応用に、専用の電話番号、E メールアドレスを取得。
- ・事務局の設置期間は、令和 2 年 9 月 17 日（木）～令和 3 年 2 月 15 日（月）（業務完了時）（休日は行政機関の休日に関する法律（昭和 63 年法律第 91 号）第 1 条に規定する日）。

<設置した事務局>

富士ゼロックス株式会社 公共営業部 内

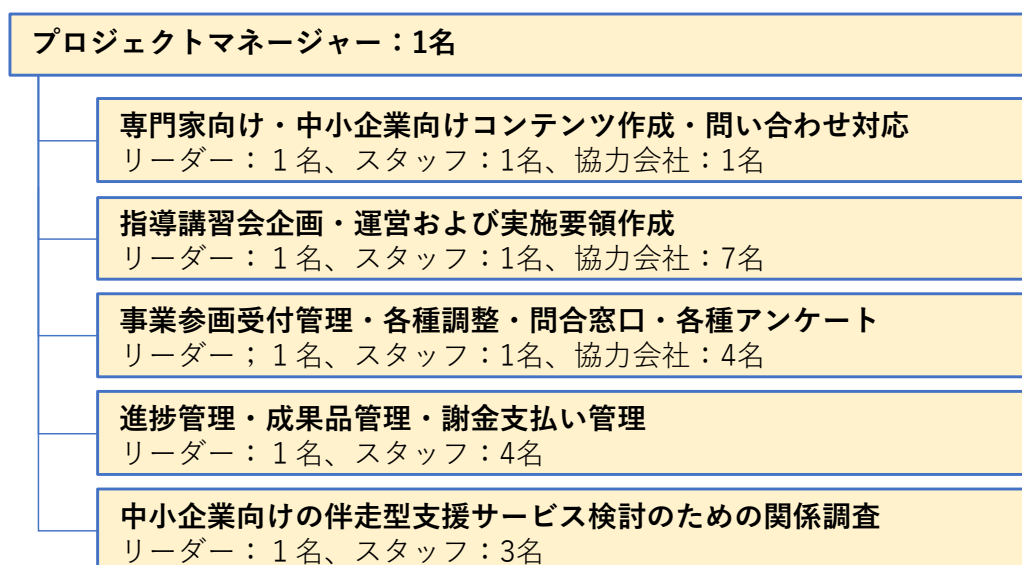
『中小企業の情報セキュリティマネジメント指導業務』事務局

〒135-0061 東京都江東区豊洲 2-2-1 豊洲ベイサイドクロスタワー22F

※本事業の事務局業務については、富士ゼロックス株式会社に委託して実施した。

<事務局の体制>

事務局の実施体制は、「図 3 事務局の実施体制」のとおりである。



※兼務もあるため、要員数は延べ数

図 3 事務局の実施体制

3. 指導先企業の募集及び受付

3.1. 中小企業等の募集活動

本事業は、コロナ禍のもと非常に厳しい社会環境のなか、10月～12月初旬までの2か月強の期間に渡って中小企業等の募集活動を実施した。募集結果は、中小企業等の申込数が合計413社となり、目標である400社を達成することができた。

(1) IPAのWebサイト掲示用案内ページ・募集チラシ等の作成

中小企業等に対する事業告知の手段として、Webサイト掲示用案内を作成し、IPAのWebサイトにて掲示した。

また、本事業の事業案内チラシ（以下「募集チラシ」という。）を作成し、中小企業等に対する事業告知の活動等で活用した。作成したチラシは添付資料1のとおりである。

(2) 中小企業等に対する事業告知

令和元年度に実施したセキュリティマネジメント指導（以下「前年度事業」、又は「前年度」という。）では、指導先企業が3大都市圏（首都圏・中京圏・近畿圏の11都府県）に偏重する傾向となっていたことから、本年度は、3大都市圏以外の36道県地域を中心に指導先企業の募集活動を行った。具体的には、募集チラシの配布、Webサイトへの事業案内掲載、テレマーケティング、メルマガ・メールニュース等のメール配信等による事業告知を延べ約14万社に行った。

本年度実施した告知方法別の主なアプローチ規模は、「表2 募集告知方法別アプローチ規模一覧表」のとおりである。

表2 募集告知方法別アプローチ規模一覧表

告知方法	規模
募集チラシの配布	約16,800枚 (商工会、商工会議所、よろず支援拠点、中小機構地域本部、IPAセミナー ほか)
Webサイトへの事業案内掲載	8サイト (IPA、中小機構、お助け隊事業者、情報サービス産業協会、行政書士会 ほか)
テレマーケティング	13,000事業者 (中小企業5,000、医療法人4,000、学校法人1,000、DMフォロー等3,000)
メルマガ・メールニュース等のメール配信	83,000社以上(リマインドを含めるとのべ135,000社以上) (IPA、経済産業局、中小企業庁、中小機構、お助け隊事業者他)
DM(FAX、封書)	7,189事業者 (業界団体組織会員企業、事務局協力会社顧客企業他)
SNS(Twitter+facebook)	約20,000フォロワー (IPA、経済産業局、日本電信電話協会)
専門家による参加促進活動(事前指名)	専門家約450名 (専門家登録した登録セキスペ(RISS)、ITコーディネータ(ITC))

(3) 中小企業等からの参加申込数の推移

参加申込みを受付けた中小企業等の総数は413社であり、そのうち申込み後キャンセルを除く有効な申込数は395社であった。

受付開始後、10月1日（木）～12月11日（金）までの期間における、中小企業等の申込数の推移を「図4 中小企業の申込数の推移」に示す。図が示すとおり、募集開始から11月中旬までは、1営業日あたりの平均申込数5.2社で推移し、募集数が当初想定を下回っていたが、11月中旬から特定非営利活動法人ITコーディネータ協会の協力のもと、ITコーディネータ（ITC）に指導先企業の参加促進活動を要件に専門家への参加登録を開始したことに加えて、「各経済産業局メルマガ会員へのメルマガ配信」、「お助け隊実証参加企業へのメール配信」、「SECURITY ACTION 宣言者向けメールニュース」、及び事務局関連のチャネルを活用したメルマガ・DM等による中小企業等への募集活動を加速化したことにより、1営業日あたりの平均申込数が13.6社に増加し、中小企業等の申込ペースが約2.6倍になった。

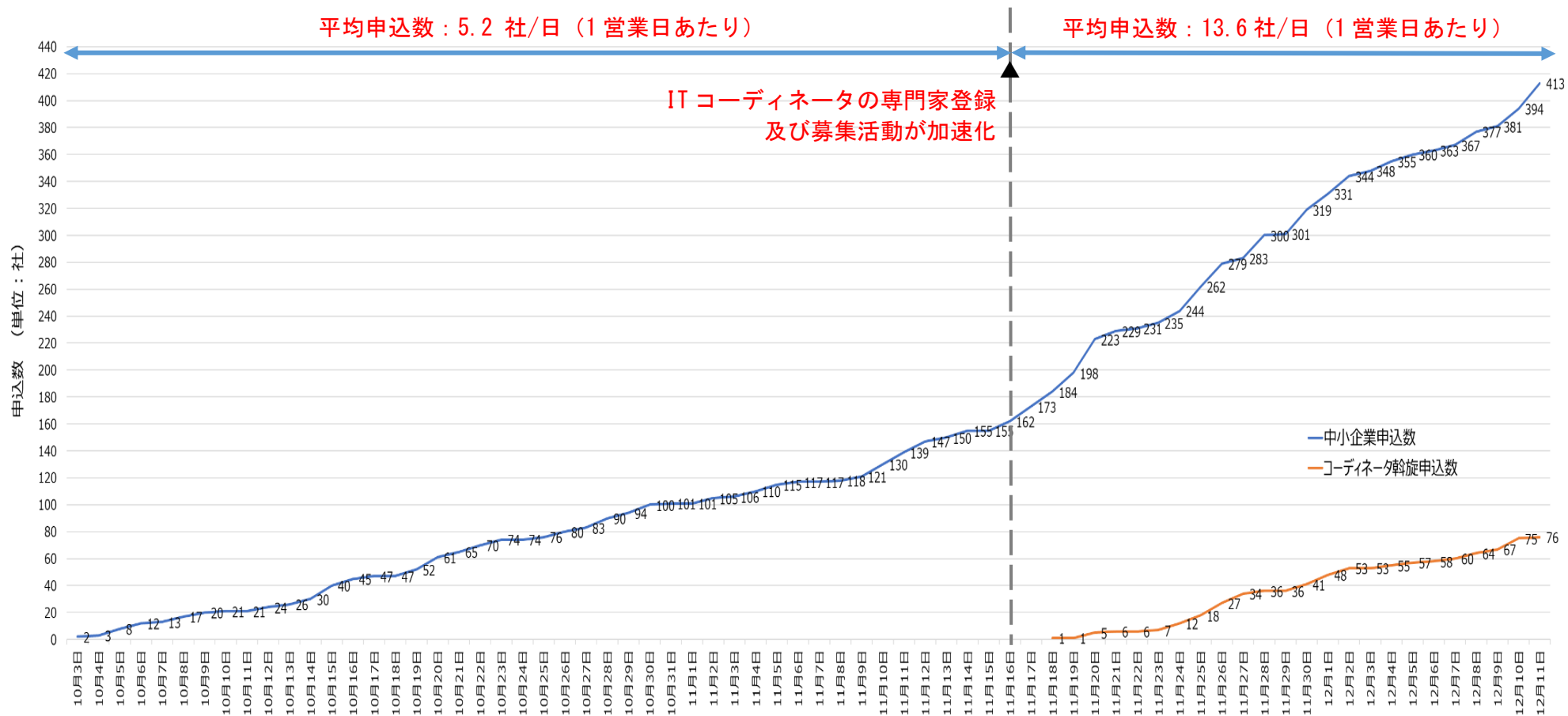


図 4 中小企業の申込数の推移

(4) 主たる募集告知方法における実施現場からの声

本事業で実施した各種募集告知活動のうち、主たる活動として、商工団体（商工会・商工会議所）への募集チラシ配布、テレマーケティング、専門家による参加促進活動を取り上げ、それぞれの実施者から収集した生の声を以下に示す。

募集チラシ配布に対する商工会・商工会議所からの声

募集チラシの配布による告知を行った商工会・商工会議所のうち 17 団体に対して TEL ヒアリングを実施し、9 か所の団体から回答を得た。

商工会・商工会議所では、コロナ禍の影響により、補助金、融資等事業継続等に関する対応の優先度が高く、セキュリティに対しては事業者の関心が低いこともあって、本事業の告知活動の優先度が低い状況であった。また、商工会・商工会議所主催のセミナー等の開催が困難であったため、セミナー配布物として募集チラシを中小企業に直接渡す機会が少なく、募集チラシによる告知効果が得られにくい状況であった。募集チラシ以外の有効な告知施策として、経験上メール配信による効果が高いとの声もあった。

以下に募集チラシ配布に対する商工会・商工会議所からのヒアリング結果を示す。

【質問 1】事業案内チラシの中小企業への配布状況（窓口置き、手渡し、他）について

- 受付相談窓口隣接又は近傍のマガジンラックに配架。
- セキュリティ関連の相談があった際に手渡しする。
- 興味を持たれた方はチラシを持ち帰っている。

【質問 2】チラシ以外に有効な広報手段について（メルマガ、会報誌への挟み込み、他）

- メール配信、会報チラシ折り込み、ホームページ等があるが、メール配信が最も効果が高い感触。
- プッシュ型にするなら、会報へのチラシ折り込みや会報記事として情報提供するのが有効。
- 例年であればセミナー等で配布物に折り込み直接お渡しするが、今年はセミナー開催が困難。
- チラシ、メルマガでの効果にあまり差を感じない、チラシは目に留まるので良いと思う。

【質問 3】中小企業様の反応や喫緊での関心の有無などについて

- コロナ禍でも持続化給付金などで、相談窓口にはお客様が多く来られる。
- 時節柄、事業継続、売り上げ向上に向けた相談が多い。
- 最近相談で窓口に来る人は増えているが、セキュリティの相談があるかどうかはわからない。
- 相談内容に合致すればチラシを渡すが、セキュリティに関する相談はあまり聞かない。

【質問 4】事業案内チラシの分かり易さ（中小企業目線での評価）について

- 白黒のチラシが多い中でカラーが目立ちやすい。内容についても概ね理解できる。
- 事業者目線で見ても訴求ポイントの分かりやすい印象。
- チラシが配布されてきたことは認識しているが、具体的なチラシの内容までは把握していない。

テレマーケティングにおける現場オペレータからの声

テレマーケティングによる中小企業等の参加申込数は、募集想定 100 社 (=10,000 コールの 1%) に対して 31 社 (0.3%) となり、想定に比べ募集活動の成果をあげることができなかった。

テレコールの開始当初は、「IPA」の組織名認知度が予想以上に低いことや、無料施策ということに不信感をいだく方もあり、電話での事業説明が困難な状況であった。

これらの問題点を解決するために、途中でテレコールのトークスクリプトの見直しを実施した結果、案内がスムーズになり、説明を聞いていただけようになった。しかし、事業への参加を社内検討してもらっても、実施期間が短くて日程調整が困難なケースや、経営層が不要と判断するケース等があって、申込みまでに至らなかったケースもあった。

以下にテレマーケティングにおける現場オペレータのヒアリング結果を示す。

【問題点】

資料送付後、フォローした企業が事業参加申込みまで至らない。

【要因分析】

テレマーケティング現場の声より、資料送付後のフォロー時に資料の説明する間もなく、すぐに断られるケースが多く、無料の施策という点に疑念を持たれたり、組織名のなじみがなく認知度が薄いことが、コールスクリプトのミスマッチが主な要因となっている。

【改善策】

(ア) 疑念解消、信頼度アップのためにスクリプトフレーズを見直す

- 経済産業省の補助事業で、国家資格を持った専門家が事前に指導講習を受け、品質の高い支援を提供します。
- 前年度も実施しており、全国 382 社が参加して 96%以上の満足度を得ている事業です。
- 具体的な成果、事業者様側の負担がどのようなものか、送付資料にも記載しています。

(イ) 資料送付時のメール署名を一見して分かりやすい表記に変更

- 『情報セキュリティ専門家派遣事務局(経産省補助事業)』

【改善対応後の反応】

コールスクリプト変更後、資料送付後のフォローにおける案内がスムーズになり、コール先の担当者に事業内容を理解してもらえるようになった。しかし、募集チラシ等の資料を見て、実施期間が短い、年末年始で日程調整が難しい、というような反応が多かった。折り返し【連絡希望】のリードも日程調整を理由に申込みに至らないこともあった。また、電話対応した担当者には内容を理解してもらえたが、経営層の判断で不要となったケースもあった。

専門家による指導先企業の参加促進活動における声

専門家による指導先企業の参加促進活動において、20社以上の企業から事前指名⁹を受けた登録セキスペ（RISS）が2名存在した。この2名に個別ヒアリングを行ったところ、本事業の事前説明活動及び企業からの信頼獲得の工夫等を徹底することが重要との意見を得た。これらの声をノウハウ集としてとりまとめ、「専門家指名及び効率的な指導についてのノウハウ・工夫」として専門家向けWebサイトで展開した。

以下に当該登録セキスペ（RISS）からのヒアリング結果を示す。

【ポイント1. 中小企業の参加促進に向けた告知活動】

- 経済団体への活動
⇒地域の商工会議所への説明訪問（所属会員の事業者への告知）
* 商工会議所にてチラシ配布、会報掲載、メルマガ送信の協力依頼
⇒地域の中小企業家同友会への説明訪問（所属会員の事業者への告知）
* 会員用イントラネット、会報誌への寄稿の協力依頼
- 異業種ビジネス交流会や勉強会 等への活動⇒各種異業種ビジネス交流会での告知
* オンラインイベントや勉強会での事業説明機会の確保
* 交流会を通じて面識の拡大を図ることで声掛けできる・相談してもらえるような信頼関係を築く（勧誘感を全面に出すと壁をつくられてしまうので注意）
- 取引先パートナー等への活動⇒専門家及び専門家所属団体の取引先パートナーとのコラボ
* 取引先パートナーの顧客へのチラシ配布・メルマガ配信の協力依頼
* 要望のあった取引先パートナーの顧客には訪問説明を実施
- SNSでの活動⇒Facebook・Twitterでの事業告知（例：月に3回ほどの投稿）

【ポイント2. 中小企業の参加促進に向けた説明活動】

- 事業説明は訪問が基本⇒メルマガ、チラシだけでは事業の主旨を伝わりにくい
- 事業説明内容⇒事業の目的、4回の業務の流れ（事業者と専門家のアクション）、事業のアウトプット、事業者の負担感（とくに事業に割かれる時間）、事業者のメリット（SECURITY ACTIONによる社会的信頼）、前年の実績（参加社数・事例紹介）

【ポイント3. 中小企業の参加促進に向けた攻めの一押し】

- キーワード
「セキュリティ対策における最恐の脆弱性は人間です。」
「経営者として、自社が被害者だけではなく加害者になることは避けなければなりません。」
「会社も健康診断が必要です。」
「ランサムウェアにより全てのデータが見えなくなることがあります」
「メールが見知らぬ他人に転送されることがあります。（例：「Emotet」と呼ばれるウイルス）」
- 事業者の情報収集
⇒ホームページ等で経営理念、事業内容、どのような情報を扱っているかを把握しておき、相手側の気持ちに寄り添い訪問時に質問をすると、事業者側の心の壁がなくなる。
例）社名の由来の質問、経営理念の策定期間や考え方、最近話題の取組み（ニュース掲載）等
⇒業界全体の課題などは、知ったかぶりをせずにダイレクトに質問をする。

【ポイント4. その他、留意事項】

- ⇒専門家自身が利害関係のない第三者であることをPRするとベター。
- ⇒事業者は何をどこまですれば良いのか悩んでいるので、見えるもの（今回の事業アウトプット）を提示することで、より前向きに取り組んでもらえる。
- ⇒お客様の置かれている状況の事前把握は必須。
- ⇒こちら（専門家）から動かないと事業申込みはしてもらえない。「申込みしてください」だけではなく、申込手順や申込みフォームに必要な入力内容、申込後の専門家マッチング、初回指導業務までの具体的な流れの説明が必要である。
- ⇒お客様の時間的な負担や業務負担がどの程度あるか、予め話しておく心安心してもらえ。

⁹ 事前指名：本事業では参加申込み時に中小企業等により専門家指名があった場合にはそれを前提にマッチングを実施した。

3.2. 参加する中小企業等の申込受付

(1) 申込状況

事務局にて、令和2年10月1日（木）～令和2年12月11日（金）の期間、中小企業等からの本事業への参加申込みを受付けた。

申込みを受けた中小企業等へ事務局から候補となる地域の専門家リストを提供し、中小企業等の指名によりマッチングを実施した。

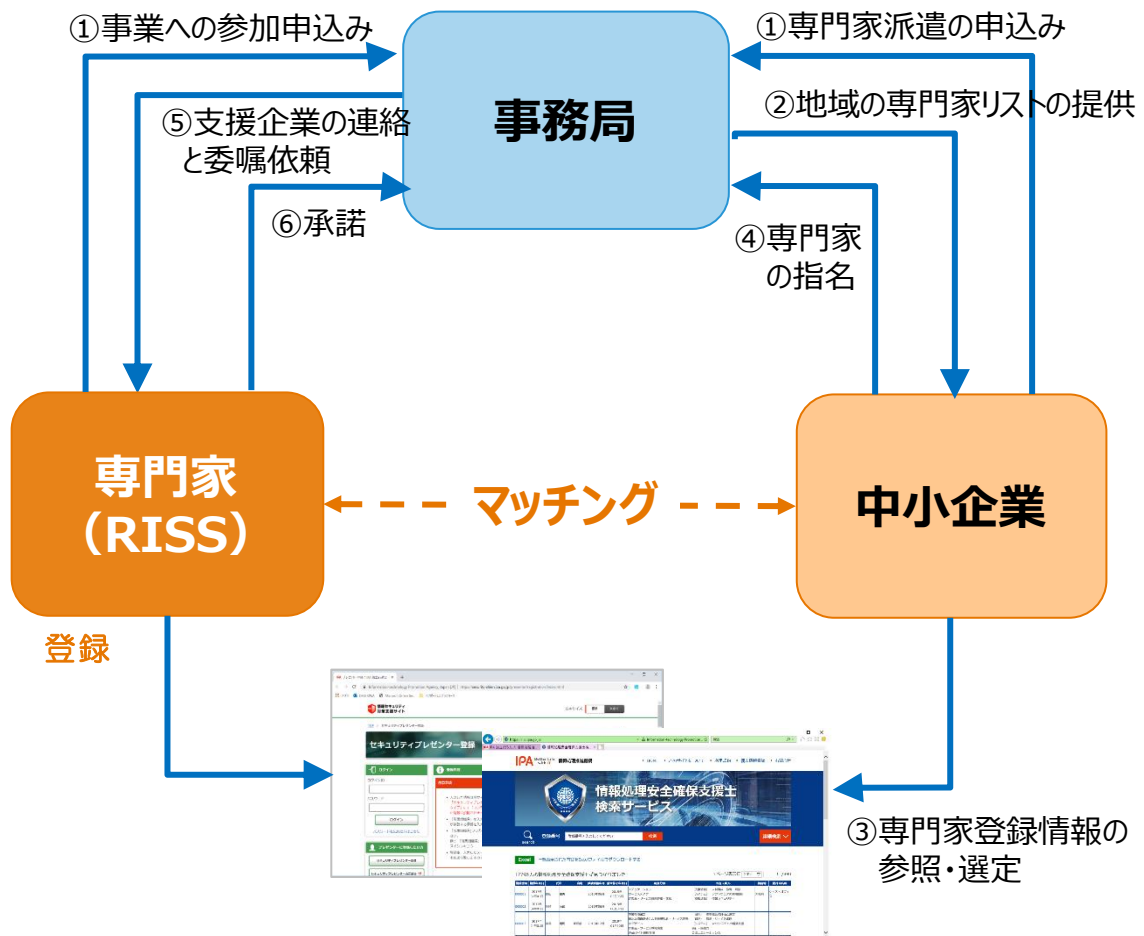


図 5 中小企業からの申込受付フロー

受付期間における、都道府県別の中小企業等の申込数を「図 6 本年度の都道府県別の中小企業申込数」に示す。受付けた申込総数は 413 社で、36 道県地域は 179 社（43.3%）、3 大都市圏（11 都府県）は 234 社（56.7%）であった。36 道県地域の中小企業の参加を促進した結果、前年度の 36 道県地域の割合（34.6%）に比べ約 10%増加した。なお、岡山県の参加申込数には、1 者で 20 社以上の企業を指導した事例を含んでいる。

中小企業申込の分布（合計413件）

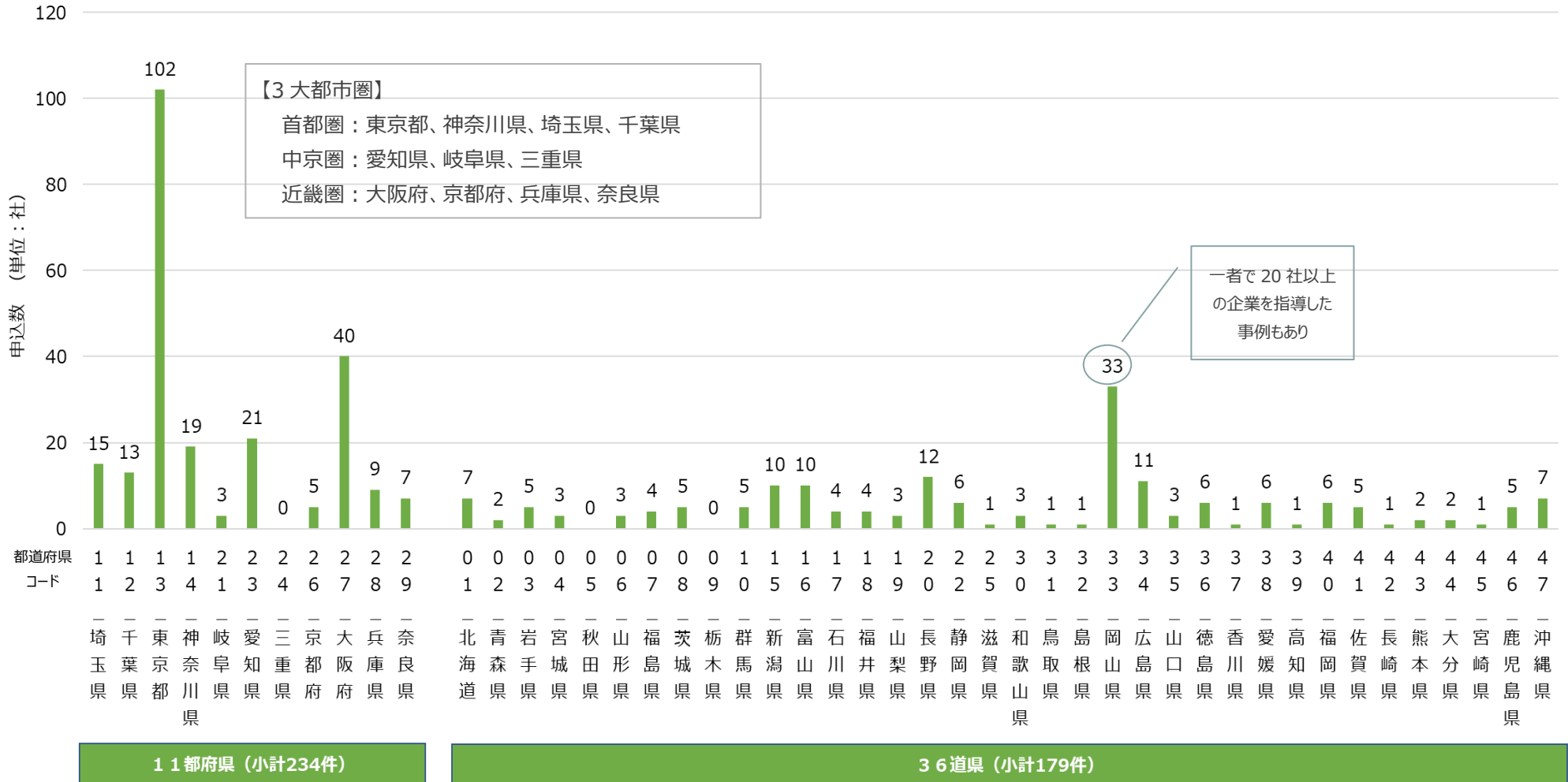


図6 本年度の都道府県別の中小企業申込数

(2) 中小企業等からの問い合わせ対応

中小企業等からの問い合わせは総数で67件であり、前年度の81件に比べて14件減少した。前年度との問い合わせ区分の比較を「表3 中小企業からの問い合わせ (%)」に示す。

本年度は、「事業ルール」「SECURITY ACTION」の問い合わせ数が前年度より増加し、「事業内容」「事業スケジュール」「指導先企業の負担」の問い合わせ数は前年度より減少した。

問い合わせ数が増加した「事業ルール」については事業参加条件に関する問い合わせが多く、本年度は事業参加要件である中小企業等の定義を変更した影響と想定される。また「SECURITY ACTION」についてはSECURITY ACTIONの自己宣言サイトの掲載内容及び宣言手順等についての問い合わせが多く、自己宣言サイトのわかり易い掲載内容の工夫が必要と言える。

問い合わせ数が減少した「事業内容」「事業スケジュール」「指導先企業の負担」については、前年度の実績を踏まえ、事業告知の説明内容を改善した成果と言える。

なお、特筆すべき事項として、専門家に対するクレームが0件であったことがあげられる。

表3 中小企業からの問い合わせ (%)

問い合わせ区分	前年度	本年度	主要な問い合わせ内容
1:事業の内容	13.6	5.9	・「情報セキュリティ対策実行計画書」はどのようなものか。 ・専門家からのセキュリティ指導が無料とのチラシを見たが、指導全てが無料なのか。
2:事業ルール	9.9	22.1	・自社が中小企業の定義を満たしているのか。 ・機密保持契約はどのようになっているか。
3:事業スケジュール	13.6	7.4	・具体的な申込み期限と指導の期限を教えてください。 ・4回の訪問指導の期間はどれくらいか。
4:指導先企業の負担	6.2	1.5	・利用規約の成果物は必ず提出しなくてはならないのか。 ・自社診断シートはどれくらい時間がかかるのか。 ・基本方針の作成にはどれくらい時間を要するのか。
5:申込方法	7.4	4.4	・申し込んでから、決定までの流れを教えてください。 ・申込時に一つ星宣言を行ってなくても申し込めるか。
6:専門家指名	3.7	8.8	・候補の専門家が2名送られてきたが、何を基準に第1希望・第2希望とすれば良いかわからない。
7:状況の問い合わせ	24.7	14.7	・まだ中小企業の募集は行っているか。空きはあるか。
8:日程変更	3.7	0.0	(本年度なし)
9:キャンセル	2.5	2.9	・これから4回の日程組む事が難しいので、参加辞退したい。
10:SECURITY ACTION	7.4	19.1	・SECURITY ACTION 宣言を申請したがその後のメールが届かない。 ・一つ星宣言をしていることが応募条件となっているが、最終的にはどのレベルまで指導してもらえるのか。
11:アンケート	0.0	8.8	・オンラインでの指導を受けていないため、その箇所は回答ができないが、選択をしないと進めないようである。
12:その他	7.4	4.4	・担当した専門家に今後も継続して指導してもらいたいが、専門家の所属企業が副業禁止のため契約が行えない。本事業同様に、IPA や公的機関が何らかの形で介在して、専門家を派遣するようなスキームはないか。

3.3. 指導先企業と専門家のマッチング

(1) マッチング状況

中小企業等の参加申込総数 413 件のうち、申込み後キャンセルが 18 件あったため、専門家とマッチングされた件数は 395 件であった。このうち、242 件（61.3%）は、専門家の指導先企業の参加促進活動等により事前指名ありであった。「表 4 マッチング状況サマリ」に、マッチング状況のサマリを示す。

事前指名ありの登録セキスペ（RISS）は、前年度の 154 件から 168 件にやや増加した。また、事前指名ありの IT コーディネータ（ITC）は、前年度の 80 件から 74 件にやや減少した。

表 4 マッチング状況サマリ

都道府県	マッチング数				計	都道府県	マッチング数				計
	指名あり		指名なし				指名あり		指名なし		
	RISS	ITC	RISS	ITC			RISS	ITC	RISS	ITC	
01_北海道	2	0	5	0	7	25_滋賀県	0	0	1	0	1
02_青森県	0	0	1	0	1	26_京都府	0	3	1	0	4
03_岩手県	2	0	3	0	5	27_大阪府	18	0	21	0	39
04_宮城県	0	2	1	0	3	28_兵庫県	8	0	1	0	9
05_秋田県	0	0	0	0	0	29_奈良県	1	2	2	0	5
06_山形県	2	0	1	0	3	30_和歌山県	1	0	1	0	2
07_福島県	0	3	1	0	4	31_鳥取県	0	0	1	0	1
08_茨城県	2	2	0	0	4	32_島根県	0	0	1	0	1
09_栃木県	0	0	0	0	0	33_岡山県	25	1	5	0	31
10_群馬県	1	1	3	0	5	34_広島県	3	1	7	0	11
11_埼玉県	5	5	5	0	15	35_山口県	0	0	3	0	3
12_千葉県	6	4	2	0	12	36_徳島県	1	0	5	0	6
13_東京都	49	18	33	0	100	37_香川県	1	0	0	0	1
14_神奈川県	7	4	8	0	19	38_愛媛県	0	4	2	0	6
15_新潟県	2	3	3	0	8	39_高知県	0	0	0	0	0
16_富山県	2	6	2	0	10	40_福岡県	2	1	3	0	6
17_石川県	1	0	3	0	4	41_佐賀県	1	3	1	0	5
18_福井県	1	1	1	0	3	42_長崎県	0	0	1	0	1
19_山梨県	1	2	0	0	3	43_熊本県	1	0	0	0	1
20_長野県	9	0	3	0	12	44_大分県	0	1	1	0	2
21_岐阜県	1	0	1	0	2	45_宮崎県	0	0	1	0	1
22_静岡県	0	1	5	0	6	46_鹿児島県	2	2	1	0	5
23_愛知県	10		11	0	21	47_沖縄県	1	4	2	0	7
24_三重県	0	0	0	0	0	合計	168	74	153	0	395

4. セキュリティマネジメント指導に係る指導要領（指導ツール）の作成

セキュリティマネジメント指導業務の実施にあたり、IPAのセキュリティ対策支援ツールを活用した4回の標準的な指導内容（標準カリキュラム）と、指導先企業への依頼・調整事項や指導にあたっての基本的な留意点を説明する「指導要領（指導ツール）」を作成した。（別紙1参照）

(1) 指導業務の達成目標と成果物

「指導要領（指導ツール）」の作成にあたっては、中小企業等の対策実施レベルに即して、セキュリティマネジメント指導業務の達成目標と成果物を明確にするものとした。

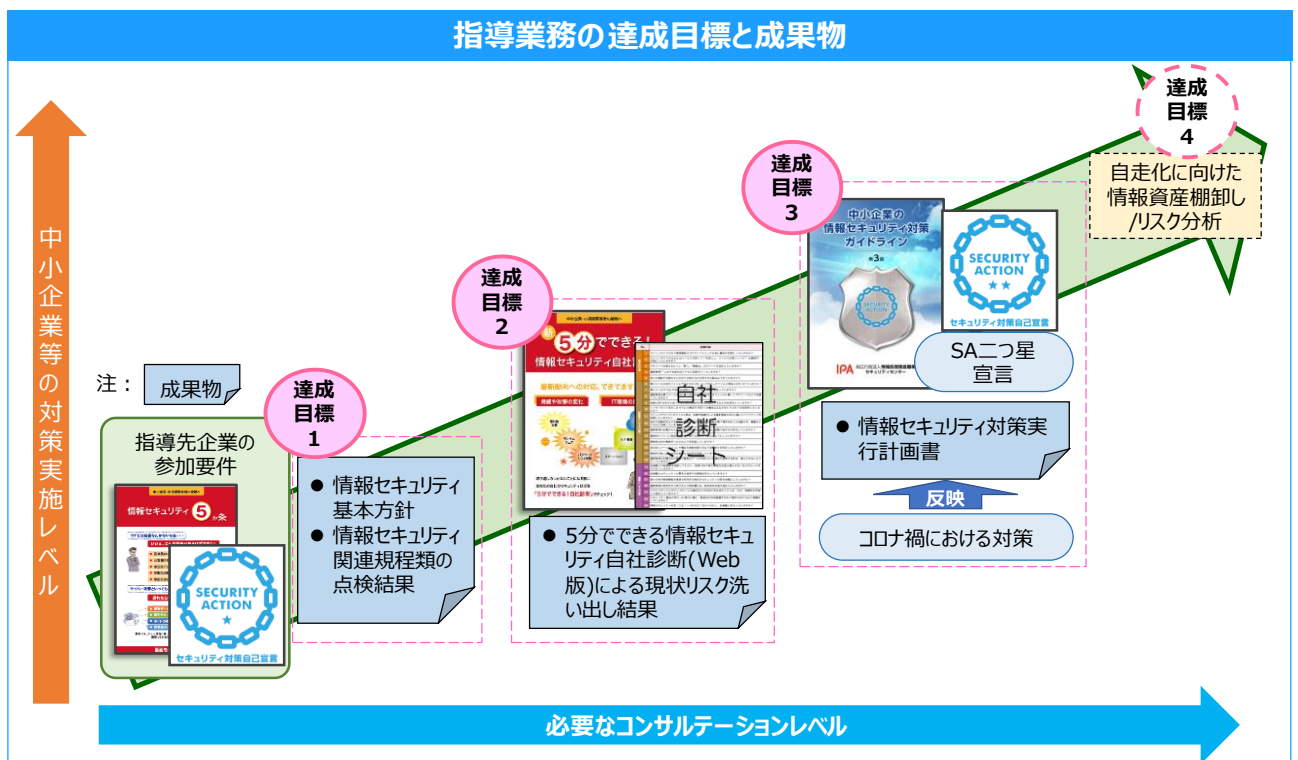


図 7 指導業務の達成目標と成果物

前年度は情報セキュリティ基本方針の作成（達成目標1）、5分でできる自社診断シートによる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）、情報セキュリティ対策実行計画の策定（達成目標3）を目標としていたが、本年度はコロナ禍での情報セキュリティ対策を含めた目標とした。また、さらに高度な情報セキュリティ対策を目指す企業は、専門家が経営者の信頼を得て、将来の自走化に向けた情報資産棚卸し/リスク分析を含む継続的フォローを目指すこととした（達成目標4）。

本事業の達成目標と成果物を「表5 達成目標と成果物」に示す。

表 5 達成目標と成果物

指導業務の達成目標	成果物
1. 情報セキュリティ基本方針の作成	<ul style="list-style-type: none"> ● 情報セキュリティ基本方針 ● 情報セキュリティ関連規程の点検結果
2. 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	<ul style="list-style-type: none"> ● 「5分できる情報セキュリティ自社診断(Web版)」による現状のリスク洗い出し
3. 情報セキュリティ対策実行計画の策定	<ul style="list-style-type: none"> ● 情報セキュリティ対策実行計画書(コロナ禍での情報セキュリティ対策を含む) ● SECURITY ACTION 二つ星宣言
4. (自主目標) 自走化に向けた継続的フォロー	<ul style="list-style-type: none"> ● 自走化に向けた情報資産棚卸し/リスク分析

(2) 指導要領（指導ツール）の構成

「指導要領（指導ツール）」は、専門家が今後も継続して活用できるものとなるよう、標準的な情報セキュリティ対策の指導の進め方（標準カリキュラム）を示しつつ、指導先企業の個別事情に応じた独自の工夫と肉付けができるよう、指導に必要なツールの活用方法、経験者の体験による気づきや工夫、コロナ禍に必要な対応など実践的なノウハウを提供する内容とした。

「指導要領（指導ツール）」の構成としては、指導講習会でのテキストとすることを前提に、「具体的支援の進め方」と「効果的な指導」という2つの観点でパート分けした構成とした。

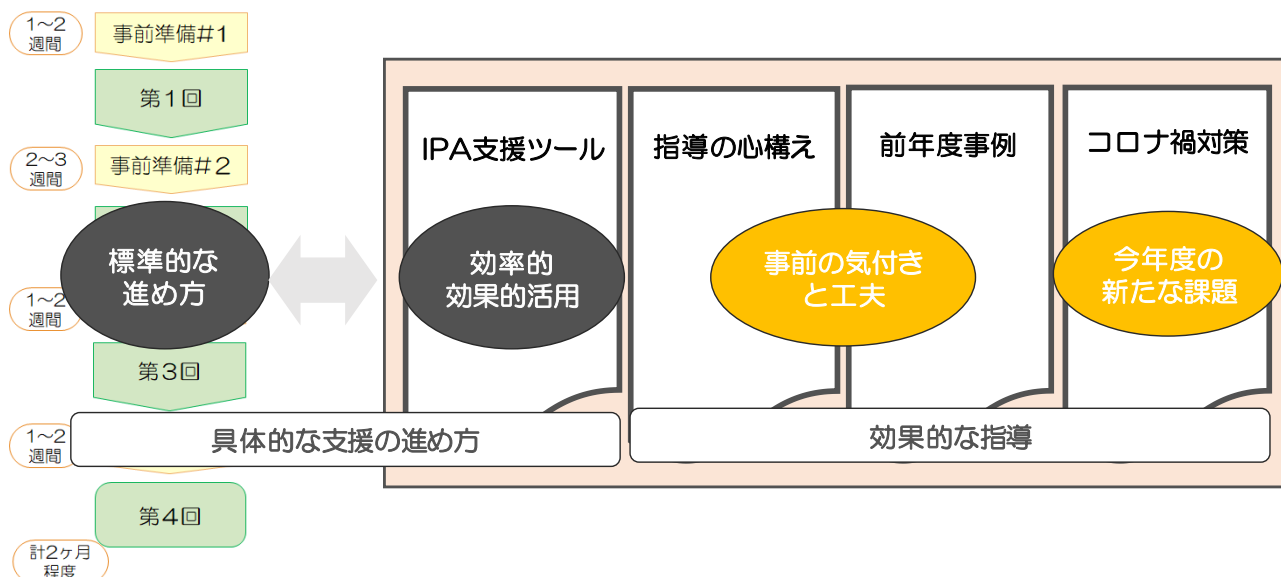


図 8 指導要領（指導ツール）のコンテンツ構成

(3) 指導要領（指導ツール）の記載項目

「指導要領（指導ツール）」の「具体的支援の進め方」のパートでは、指導業務における達成目標と成果物を説明し、それらを達成するための全4回の指導の進め方（標準カリキュラム）と、指導の中で活用する支援ツールの活用方法について解説した。

また、「効果的な指導」のパートでは、中小企業の経営者とのコミュニケーションに役立つ知識や、前年度に実施した指導事例や終了後のアンケートからの気付きなどを盛り込んだ。さらに、本年度はコロナ禍という状況の中で必要となるセキュリティ対策に関する知識、及び指導業務をオンラインで行えるよう Web 会議ツールの活用についても加えている。

「指導要領（指導ツール）」の記載項目内容を「表 6 指導要領（指導ツール）の記載項目」に示す。

表 6 指導要領（指導ツール）の記載項目

タイトル		記載項目
具体的支援の進め方	1 専門家指導全体の構成と留意事項	<ul style="list-style-type: none"> ● 専門家指導の全体構成 ● 目標と成果物 ● 標準的な進め方（標準カリキュラム）
	2 各種ツールの活用方法	<ul style="list-style-type: none"> ● IPA ツールの活用方法 （5分のできる自社診断:Web版、映像コンテンツ、情報セキュリティ対策ガイドライン） ● 提供できるコンテンツ、参考資料
効果的な指導	1 指導にあたっての心構え	<ul style="list-style-type: none"> ● 中小企業経営者が考えていること ● 経営者とのコミュニケーション ● コンサルテーションに役立つこと
	2 前年度の訪問指導から学べること	<ul style="list-style-type: none"> ● 中小企業における情報セキュリティの現状と課題 ● 前年度の専門家指導の実施事例 ● 専門家と経営者のアンケートから気付くこと
	3 コロナ禍のセキュリティ対策	<ul style="list-style-type: none"> ● コロナ禍における必要なセキュリティ対策 ● 専門家指導の中での Web 会議ツールの活用

(4) 「具体的な支援の進め方」の内容

4回の指導についての標準的な進め方（標準カリキュラム）は「図 9 標準カリキュラムの内容」のとおりとした。平均的には、4回の指導を2か月程度で実施できることを前提として作成した。

また、各種ツールの活用方法としては、「5分のできる情報セキュリティ自社診断（Web版）」結果から、課題を掘り下げるポイントや、成果物のひな型となる IPA が提供するサンプルの紹介、経営者への動機付けとして IPA 製作の映像コンテンツの紹介等を行う内容とした。

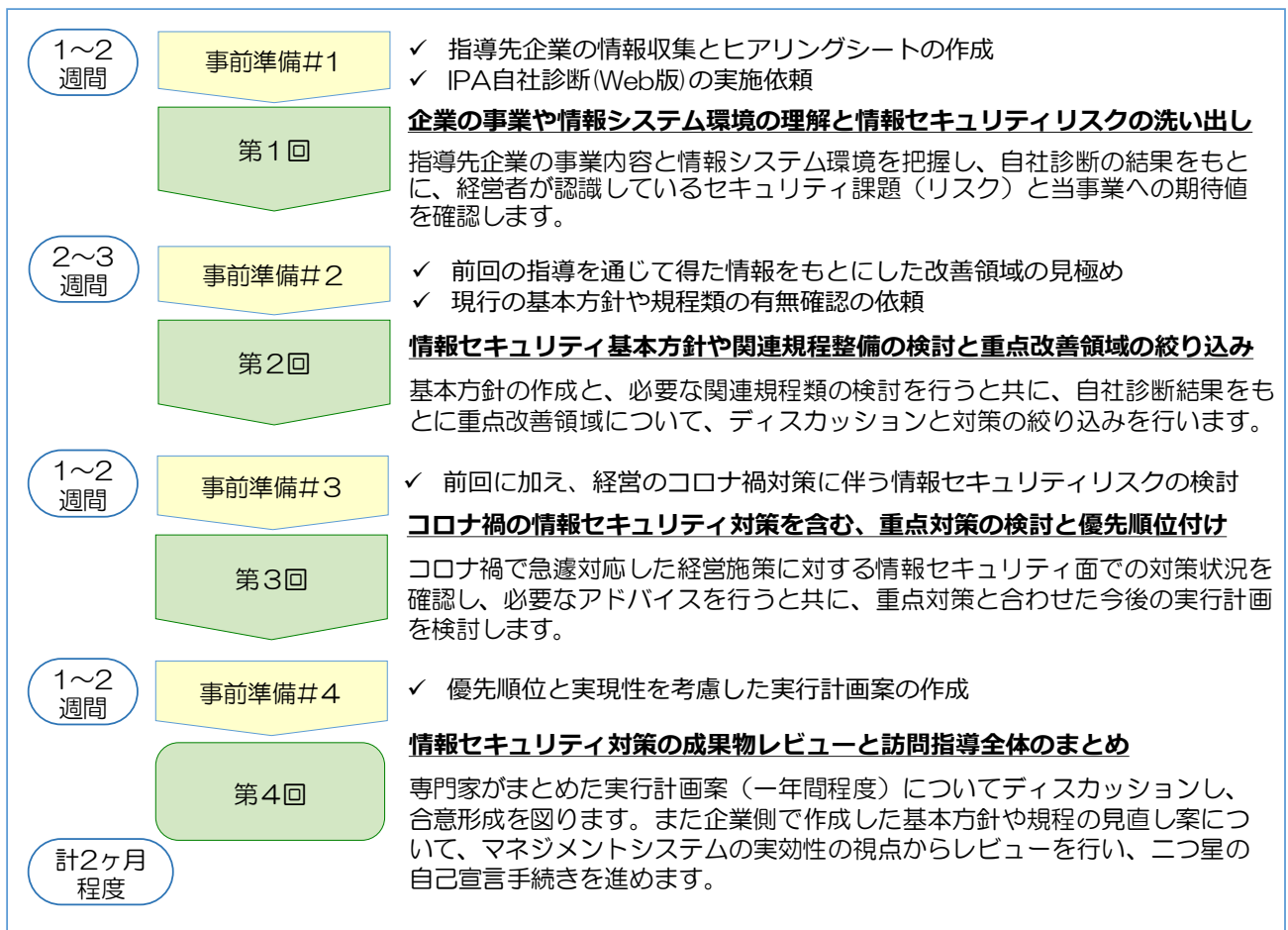


図 9 標準カリキュラムの内容

(5) 「効果的な指導」の内容

「効果的な指導」の内容を「表 7 「効果的な指導」パートでの説明項目とポイント」に示す。効果的な指導を行うために必要となる知識として、指導の際に中小企業の経営層とのコミュニケーションを図るにあたっての心構え、前年度の指導実施の経験談、新たな課題となっているコロナ禍におけるテレワークの導入にあたっての情報セキュリティ対策について、ノウハウ提供を行う内容とした。

さらに、コロナ禍においては指導業務も訪問形式で実施できない可能性があることから、指導先企業にオンラインで指導を行う場合の留意事項についても記載した。

表 7 「効果的な指導」パートでの説明項目とポイント

項目		説明のポイント
指導にあたっての心構え		
1	日本の中小企業の現状	中小企業の現状と日本の社会でのサプライチェーン上の位置付け
2	中小企業経営者の関心事	中小企業の経営者が普段関心を持っていること 財務諸表(B/S・P/L・CF)の概要
3	指導先企業を理解する	指導先企業の情報入手と簡易分析
4	効果的コミュニケーション	効果的ヒアリングに向けて(聞くから訊きながら聴くことへ)
前年度の訪問指導から学べること		
1	中小企業の情報セキュリティの現状と課題	中小企業の情報セキュリティ対策の状況と抱えている課題からの指導にあたっての留意事項
2	前年度の指導の全体像	指導先企業の業種、規模、役職、体制、参加目的から見える指導にあたっての留意事項
3	前年度の具体的指導事例の紹介	2社(建設業/サービス業)の事例について工夫した点を中心に説明
4	前年度のアンケートから参考にできること	前年度の指導先企業からのアンケート結果から見える指導にあたっての留意事項
コロナ禍のセキュリティ対策		
1	テレワーク導入・実施に絡む指導上の注意点	ウイルスへの感染リスク、BYOD ¹⁰ によるリスク、各種ツールの紛失リスク等、テレワーク導入に絡む様々な情報漏洩リスクの要因と対策について説明
2	業界別の固有の注意点	一般的な企業とは異なる、医療業界、教育機関、飲食業界における注意事項
3	Web会議サービスのセキュリティ上の留意点	Web会議サービス選定時に考慮すべきポイントと、安全に会議を開催するためのポイント
4	指導時のWeb会議サービスの利用について	オンラインで指導を行う時の注意点 (セキュリティ上と活用上(事前確認など)) 主なWeb会議サービスのセキュリティ機能
5	参考資料の提示	「テレワークを行う際のセキュリティ上の注意事項」、「Web会議サービスを使用する際のセキュリティ上の注意事項」(IPA) 「テレワークにおけるセキュリティ確保」(総務省) 「オンライン診療に関するホームページ」(厚生労働省) 「教育情報セキュリティポリシーに関するガイドライン」(文部科学省)

¹⁰ BYOD(Bring Your Own Device): 個人のプライベート端末を使用して業務を行うことで、テレワーク導入準備や運用コストを抑える効果がある。

5. 専門家の募集・登録及び指導講習会の開催

5.1. 専門家の募集案内の作成

専門家に対する事業告知の手段として、Web サイト掲示用案内を作成し、IPA の Web サイトにて掲示した。また、専門家向けの募集チラシ（PDF ファイル）を作成し、専門家に対する事業告知の活動等で活用した。作成したチラシは添付資料 2 のとおりである。

5.2. 専門家の募集活動

登録セキスペ（RISS）等のセキュリティの専門家に対して、以下のとおり事業告知を行い、3 大都市圏（首都圏・中京圏・近畿圏の 11 都府県）以外の 36 道県地域を中心に募集活動を実施した。

IPA マネジメント指導 専門家ホームページ

- 10/1（木）：IPA マネジメント指導 専門家ホームページ公開（IPA）
- 10/5（月）：事務局（富士ゼロックス）申込 Web サイトにて募集受付開始

登録セキスペ(RISS)向け案内メール

- 10/26（月）：登録セキスペ（RISS）案内メール（ALL）配信（IPA）
- 11/6（金）：登録セキスペ（RISS）向け案内メール第 2 弾（36 道県地域）配信（IPA）

IPA セキュリティプレゼンター勉強会等での専門家募集チラシ配布

- 10/9（金）：岡山、10/16（金）：静岡、10/20（火）：福岡、10/27（火）：名古屋、
- 11/5（木）：東京、11/12（木）：仙台、11/20（金）：高松、11/25（水）：金沢

情報処理安全確保支援士会の会員への事業案内

- 9/24（木）：一般社団法人情報処理安全確保支援士会（JP-RISSA）に対して、会員への事業案内を依頼（JP-RISSA 会員向けホームページに案内掲載）

IT コーディネータ(ITC)向け案内メール

- 11/16（月）：特定非営利活動法人 IT コーディネータ協会の協力のもと、IT コーディネータ（ITC）に対して、36 道県地域を中心とした指導先企業の参加促進活動込みの案内メールを配信

5.3. 指導講習会の開催

(1) 開催概要

申込受付を行った専門家候補者に対して、指導要領（指導ツール）をテキストとする指導講習会を実施した。指導講習会は以下のとおり、E-ラーニング形式でのオンライン講習で開催した。

- 開催期間：2020 年 10 月 13 日（火）～2020 年 12 月 16 日（水）
- 講師：NPO 法人ちば経営応援隊の以下の専門家が担当した。
（敬称略）

ちば経営応援隊 理事長 浅井 鉄夫、理事 川名 正幸
会員 坂本 ゆみか、会員 田中 孝典、会員 十河 敏郎

- プログラム：プログラムと講師を「図 10 指導講習会プログラム（オンライン形式）」に示す。構成としては、冒頭説明 5 分、講義 225 分（6 単元）、理解度確認テスト 60 分（15 分×4 回）、講義間休憩 75 分（15 分×5 回）の計 6 時間（360 分）で設計した。

指導講習会プログラム		講師	時間	コンテンツの主な内容
本講習会の構成、進め方の説明		事務局	5 分	Eラーニング受講についての説明
パートⅠ 具体的支援の進め方				
1	具体的支援の進め方① 「専門家指導全体の構成と留意事項」	川名	40分	<ul style="list-style-type: none"> ● 事業の位置づけ（狙い） ● 達成目標と訪問指導の流れ ● 全4回のカリキュラム構成と内容について具体的に解説 ● 訪問企業への依頼/調整事項や企業訪問に当たっての基本的な留意事項
理解度確認テスト				
2	具体的支援の進め方② 「各種ツールの活用方法」	坂本	40分	<ul style="list-style-type: none"> ● ツールの紹介(5分でできる自社診断:Web版、映像コンテンツ、情報セキュリティ対策ガイドライン、ヒアリングシート) ● 映像コンテンツ「あなたの会社のセキュリティドクター」の視聴と解説 ● 中小企業の情報セキュリティガイドライン、クラウドサービス安全利用の手引き」などの紹介、解説
パートⅡ 効果的な訪問指導				
1	効果的な訪問指導① 「指導に当たっての心構え」	浅井	40分	<ul style="list-style-type: none"> ● 日本の中小企業の現状（規模・分類/判断の迅速性） ● 経営者の一般的な関心事 ● 訪問先企業を理解するポイント ● 効果的なコミュニケーション手法 ● 最近の関心事
理解度確認テスト				
2	効果的な訪問指導② 「前年度の訪問指導から学べること」	田中	30分	<ul style="list-style-type: none"> ● 情報セキュリティ対策が進んでいない状況 ● 前年度訪問指導の全体像（希望、業種、クレーム等） ● 前年度の事例紹介 ● 工夫した点、苦労した点
理解度確認テスト				
3	効果的な訪問指導③ 「コロナ禍のセキュリティ対策」	十河	30分	<ul style="list-style-type: none"> ● コロナ禍におけるIT利用状況（概要） ● テレワーク導入時の注意点およびセキュリティポリシー策定時の留意点 ● 業界別コロナ対応 ● Web会議システム導入時のセキュリティ上の留意点 ● オンライン指導を行うにあたってのWeb会議システム利用について
理解度確認テスト				
パートⅢ 事業の運営				
1	事業の運営、謝金のお支払いについて	事務局	40分	<ul style="list-style-type: none"> ● 企業と専門家とのマッチング方法 ● 希望する専門家の申込み受付方法 ● 委嘱手続きと謝金のお支払い ● 進捗管理について ● 事業の全体スケジュール ● Q&Aの対応方法（FAQとしての情報蓄積）
指導講習会受講に関するアンケート				

図 10 指導講習会プログラム（オンライン形式）

(2) E-ラーニング受講状況

指導業務を行う専門家登録にあたっては、指導講習会の全プログラムの受講を条件とした。事務局の申込 Web サイトから、指導講習会の参加申込みを受付けた方には、事務局から E-ラーニングシステムへのアクセスパスワードを発行し、受講を開始するフローで実施した。

指導講習会の参加申込総数は1,035名であり、このうち受講を最後まで完了したのは599名(57.9%)で、受講完了に至らず途中終了してしまった受講者が少なからず発生した。「表8 資格別E-ラーニング受講状況」に、登録セキスペ(RISS)、ITコーディネータ(ITC)別の受講申込数と受講完了者数を示す。

表 8 資格別E-ラーニング受講状況

受講状況	RISS	ITC	合計
受講申込者数	882名	153名	1035名
受講完了者数	489名	110名	599名
受講完了率	55.4%	71.9%	57.9%

一方、受講申込数と受講完了数を都道府県別にみると、「図11 都道府県別の受講申込者と受講完了者(人数)」に示すとおり、3大都市圏(11都府県)の受講申込者が多くなっている。

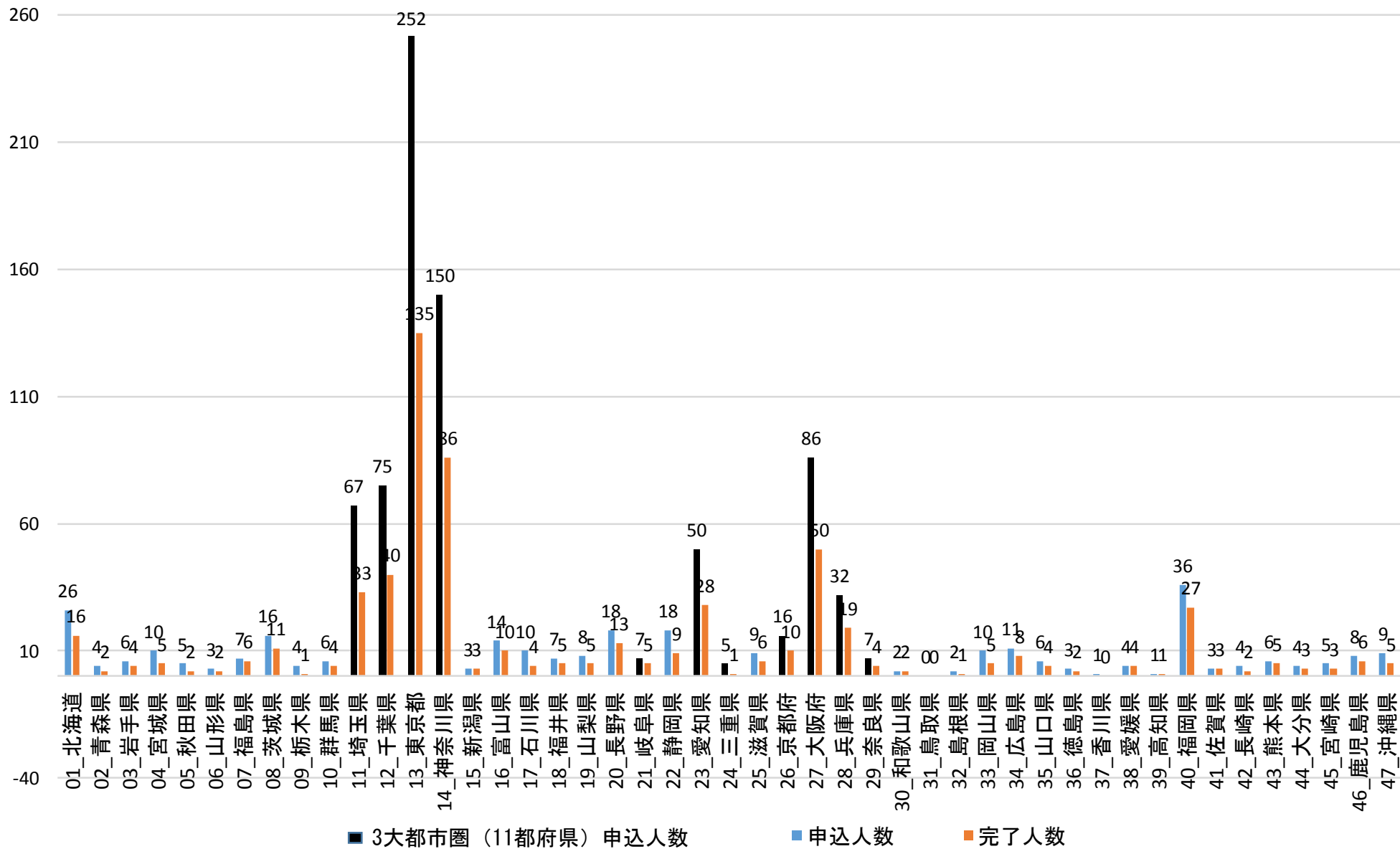


図 11 都道府県別の受講申込者と受講完了者（人数）

(3) 受講に要した時間と日数

指導講習会のEラーニングプログラムを受講完了した599人について受講履歴を分析したところ、「表9 受講完了者の受講期間と学習時間の傾向」に示すように、1日のうちに受講を完了している受講者(227名)の平均学習時間は6時間であった。実際にログとして残っている学習時間には、休憩時間や、受講完了後に再度閲覧した時間も含まれていることから、想定とおりの学習時間で実施できていたと考えられる。

一方、受講期間にはバラツキがあるものの、1週間以内の受講完了が443名で全体の74.0%となっており、Eラーニングという特性を活かし、受講者各自の都合に合わせたペースで受講を進めることができていたことがうかがえる。

表9 受講完了者の受講期間と学習時間の傾向

受講期間	人数(人)	平均学習時間
1日	227	約6時間
2日	71	約7時間
1週間以内	145	約11時間
2週間以内	87	約9時間
3週間以内	31	約13時間
4週間以内	21	約8時間
1か月以上	17	約8時間
計	599	約9時間

(4) 受講者アンケートの結果

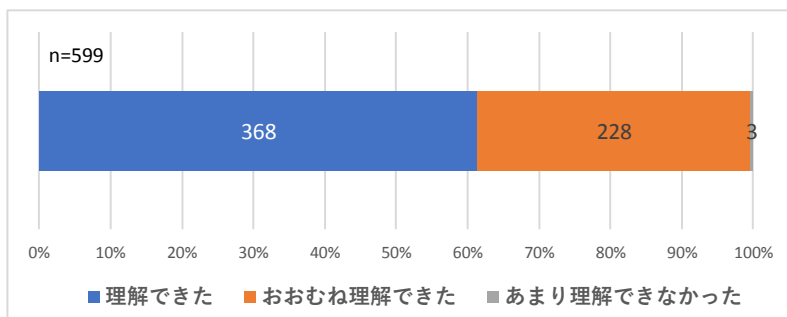
指導講習会の最後に、指導講習会受講に関するアンケートを実施した。

「図12 指導講習会の受講者アンケート結果」に示すアンケート結果から、説明資料(テキスト)を含め、講習の内容については、「理解できた」、「おおむね理解できた」を合わせて95.5%の受講者が講習内容を理解したとの回答を得た。講習の内容については、「説明が丁寧でわかりやすかった」、「スライドと音声解説があって理解しやすかった」という声が多くあり、指導要領(指導ツール)の内容も好評だった。

また、受講者の78.6%が集合教育よりも「Eラーニング形式のほうが良い」と回答し、Eラーニングによる指導講習は「時間や場所の制約がないため受講しやすい」という声が多くあった。

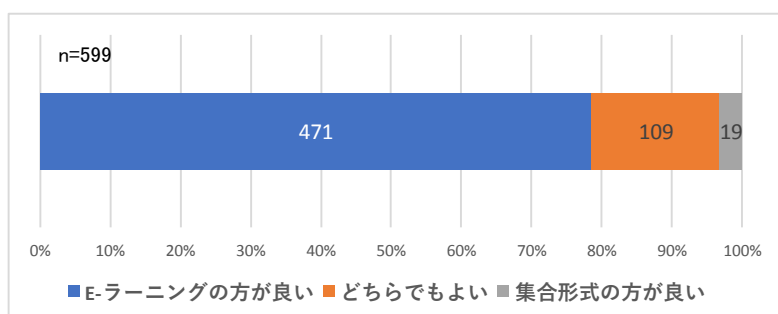
「Eラーニングなので途中で止めたり見直しができて理解できた」という声もあり、繰り返し視聴できるという点でも、Eラーニング形式は有効であったと言える。少数ではあるが3.2%の受講者が「集合形式のほうが良い」と回答した理由としては、「その場で質疑応答の内容が聞ける」、「他の登録セキスペ(RISS)との交流の場となる」という意見があがっていた。

【質問 1】 ご覧いただきました動画及び説明資料の内容は理解できましたか？



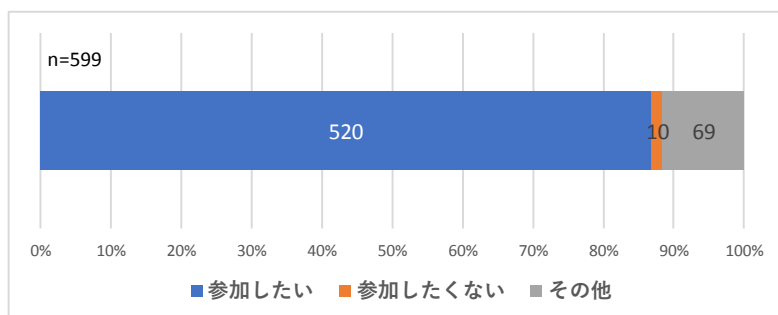
「理解できた」、「おおむね理解できた」を合わせて 99.5%の受講者が講習内容を理解したと回答した。

【質問 2】 集合形式の講習ではなく E-ラーニングとしましたが、感想をお聞かせください。



78.6%が「E-ラーニングが良い」と回答。集合教育の方を望む声は 3.2%という結果であった。

【質問 3】 講習を受けて本事業に指導専門家として参加したいと思いましたか？



事業に「参加したい」という回答が 86.8%だったが、実際の専門家登録は 452 名であったことから、何らかの理由により参加ができなかった方が 1 割程度いたと考えられる

図 12 指導講習会の受講者アンケート結果

(5) 指導講習会開催のまとめ

指導講習会の開催内容は概ね好評であった。特に E-ラーニング形式でのオンライン開催については、時間や場所の制約がないという理由で、受講者からはたいへん良い評価となった。

一方、受講を開始後、数週間学習が進まない受講者に対して受講の催促連絡等を行ったケースも生じた。また、受講完了は 60%未満に留まり、途中終了した受講者も少なからずいたことから、E-ラーニング形式で講習会を開催する場合には、受講促進の取組みが課題となる。

5.4. 専門家の登録手続

指導講習会受講者のうち、本事業に参画する専門家の登録手続を行い、登録した専門家の総数は452名であった（登録セキスペ（RISS）360名、ITコーディネータ（ITC）92名）。「図13 本年度の都道府県別の専門家登録数」に専門家の都道府県別の登録状況を示す。

登録した専門家のうち、36道県地域は147名（32.5%）、3大都市圏（11都府県）は305名（67.5%）であった。前年度は、336名（都道府県記載なし28名除く）で、36道県地域は114名（33.9%）、3大都市圏（11都府県）は222名（66.1%）であったので、36道県地域の占める割合は同等であった。なお、専門家の登録数が少ない地域は、前年度とほぼ同じ傾向であった。

登録専門家の分布（合計452名（RISS360名／ITC92名））

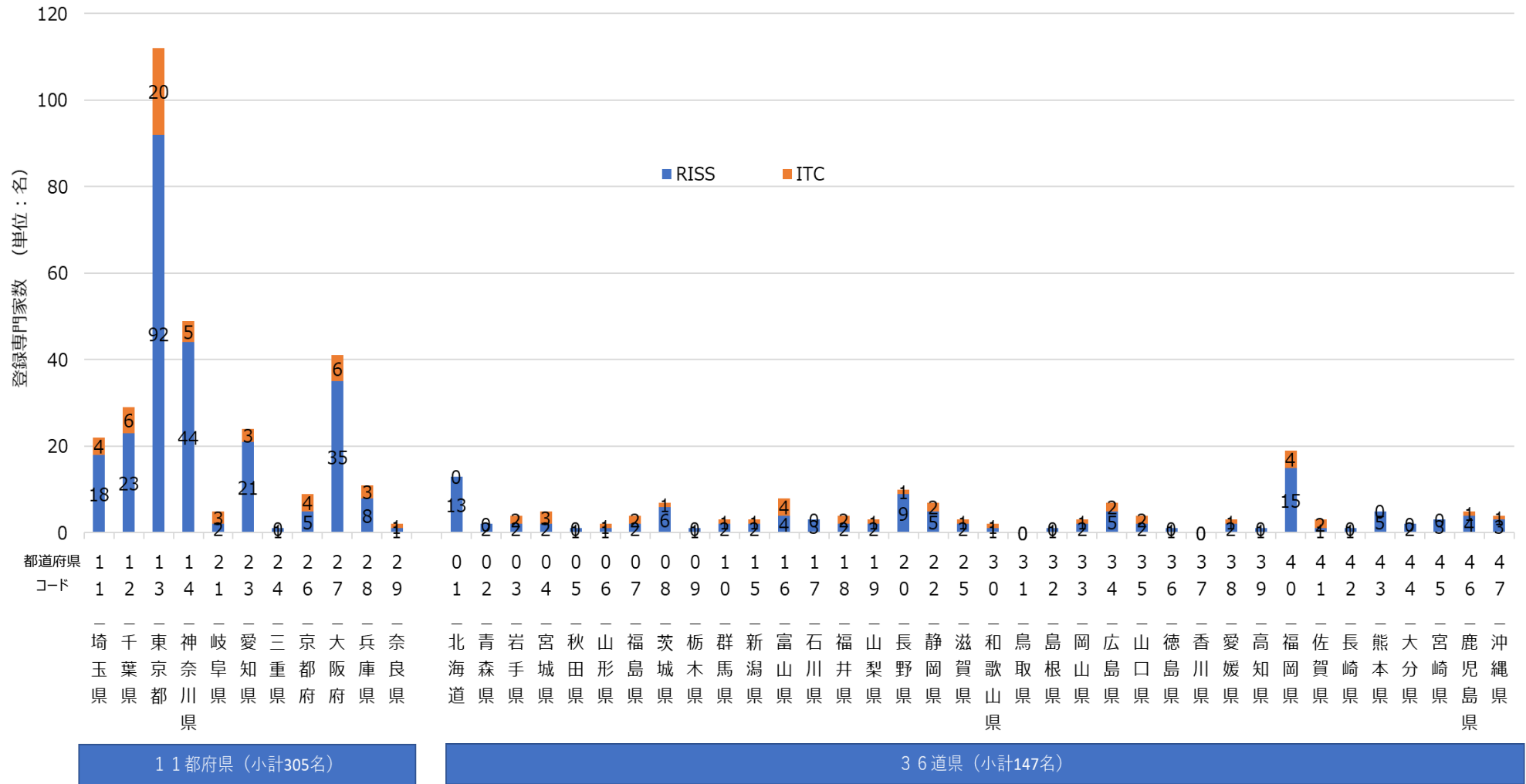


図 13 本年度の都道府県別の専門家登録数

登録した専門家 452 名のうち、実際にマッチングが成立した専門家の実数（マッチング成立専門家数、マッチング成立率）について、登録セキスペ（RISS）と IT コーディネータ（ITC）の各々の成立状況を「表 10 専門家のマッチング成立状況」に示す。本年度の登録セキスペ（RISS）のマッチング成立率は 50.0%であった。前年度は、58.9%であったので、登録セキスペ（RISS）のマッチング成立率は若干減少した。

表 10 専門家のマッチング成立状況

申込状況	RISS	ITC	合計
専門家登録数	360 名	92 名	452 名
マッチング成立専門家数	180 名	36 名	216 名
マッチング成立率	50.0%	39.1%	47.8%

また、登録セキスペ（RISS）のマッチング成立実数について、36 道県地域と 3 大都市圏（11 都府県）における本年度と前年度の比較を「表 11 登録セキスペ（RISS）の 36 道県及び 3 大都市圏におけるマッチング成立状況」に示す。

前年度は、3 大都市圏（11 都府県）でマッチング成立した登録セキスペ（RISS）の方が多かったが、本年度では若干ながら 36 道県地域でマッチング成立した登録セキスペ（RISS）の方が多い結果となった。

表 11 登録セキスペ(RISS)の 36 道県及び 3 大都市圏におけるマッチング成立状況

RISS 所在区域	いつ	専門家登録した RISS 人数	マッチング成立した RISS 人数	割合
36 道県地域	前年度	96 名	55 名	57.3%
	本年度	110 名	57 名	51.8%
3 大都市圏 (11 都府県)	前年度	213 名	132 名	62.0%
	本年度	250 名	123 名	49.2%

6. 専門家の指導管理及び謝金支払い

6.1. 実施要領の作成

事務局として専門家への謝金の支払い事務を実施するにあたり、専門家向けに本事業への参加登録方法から、指導開始後の進捗報告、及び謝金の請求までの事務処理の流れについて記載した「実施要領」を作成した。

「実施要領」は、Eラーニング型式で実施した指導講習会の最後の単元で説明を行い、IPAの専門家募集サイトにダウンロード資料として「指導要領（指導ツール）」と共に掲載した。

(1) 実施要領の構成

「実施要領」の内容は、導入部分での事業概要説明と、具体的な手続に関する説明を5つのパートで構成した。前年度の事業において、企業に所属している専門家も多く存在していることが分かったため、そういった専門家が副業として本事業に参加しやすくなるよう、委嘱手続のパターンを増やして対応するよう工夫し、「実施要領」で詳しく説明するようにした。

表 12 実施要領の内容構成

	記載項目	記載内容
0	事業の概要説明（はじめに）	<ul style="list-style-type: none">● 「実施要領」の内容について● 専門家と企業とマッチング方法について● 委嘱条件
1	本事業への参加登録方法	<ul style="list-style-type: none">● 専門家登録の前提条件● Webサイトからの専門家登録● 委嘱（個人/法人）パターンの選択● 専門家登録後の事業の流れ
2	専門家への指導業務委嘱の手続	<ul style="list-style-type: none">● 個人への委嘱手続● 法人口座を利用する個人への委嘱手続● 法人間の取引とする委嘱手続
3	業務の進捗報告と成果物の提出	<ul style="list-style-type: none">● 指導実施後の進捗報告● 指導計画の提出（第1回指導報告）● 第2回～第4回の指導報告● 指導最終報告の提出● 成果物の提出
4	謝金の請求と受取り	<ul style="list-style-type: none">● 謝金請求の流れ● 請求書の起票について● 指導終了書（受講者記入）について● 謝金の受取り（振込日等）● 源泉徴収について
5	書類送付先、問い合わせ等	<ul style="list-style-type: none">● 関連資料一覧と入手方法● 書類の送付先、問い合わせ先

(2) 専門家の登録条件と委嘱条件

本事業の指導専門家としての登録条件は、以下の4つとした。指導講習が集合形式からオンライン形式に変わり、Eラーニングの受講完了を条件とした以外は、前年度と同条件である。

<指導専門家の登録条件>

1. 国家資格である情報処理安全確保支援士（RISS）等の情報セキュリティ専門資格を有していること
2. IPAセキュリティプレゼンターとして登録されていること
3. 中小企業の支援に対して意欲があること
4. 指導講習（Eラーニング）を受講し、確認テスト、アンケート回答を完了していること

また、委嘱条件も基本的には前年度と同様であるが、本年度は、事業開始当初から法人口座への支払いや法人への委嘱（法人間の取引）を想定した事務処理を設計しているため、委嘱条件「2. 謝金の支払い（2）」に法人への支払いを行う場合の条件を追記した。

<委嘱条件>

1. 謝金

謝金の額は1回当たり45,000円（消費税込み）とし、実施業務や手続きに係わる諸経費（書類の郵送、印刷、等）及び交通費等、全てを含むものとする。

やむを得ず、自家用車やレンタカーを利用した場合も支給しない。

2. 謝金の支払い

(1) 当月分を翌月末日までに指定口座に振り込む。ただし、支払日が土曜日、日曜日、又は祝日に当たった場合は、その前日とする。

(2) 謝金に対し所得税10.21%を源泉徴収する。振込口座は、原則、個人口座とするが、やむを得ず法人口座を指定した場合であっても、同様に源泉徴収を行う。

但し、法人で委嘱手続きを行う場合は源泉徴収を行わない。

3. 守秘義務

指導により知り得た指導先中小企業等の秘密を厳守するとともにこれを自己の利益に利用してはならない。本事業の専門家としての登録期間の終了後も同様とする。

4. 損害賠償

指導専門家本人の責に帰すべき事由により、指導先中小企業等に対して損害を生じさせた場合は、その範囲内で専門家は賠償の責任を負う。

5. 免責

専門家指導実施中に専門家自身が死亡、ケガ及びその他不測の事態に遭遇した場合、国、運営主体及び事務処理等実施機関は、その補償について一切責任を負わない。

6. 留意事項

(1) 専門家指導業務は、自己の高度な専門知識、経験等に基づき、誠実にこれを行うこと。

(2) 本事業の専門家指導以外には、本事業の指導専門家の肩書きの記載された名刺を使用しない等、肩書き等の使用には十分注意すること。

(3) 本事業の業務とその他の業務とは厳に区別を行い、後者の場合には、相手方において本事業に関係するとの誤解を与えないようにすること。

(4) 専門家指導業務を遂行するために必要な機器、設備、消耗品等については、自己の責任と費用負担において、これを用意すること。

(委嘱条件 続き)

7. 登録の取消し

次の各号のいずれかに該当するときは、指導専門家としての委嘱・登録を取り消すことができるものとする。(専門家としての登録の抹消を含む)。なお、取り消した場合には、氏名及び取消理由を公表する場合がある(ただし、(8)を除く)。

- (1) 専門家としての義務を守らない場合
- (2) 本事業の目的又は内容から逸脱した行為を行ったと認められる場合
- (3) 登録内容に虚偽があることが判明した場合
- (4) 国、事務処理等実施機関に虚偽の報告をしたことが判明した場合
- (5) 本事業の実施要領その他法令に違反する行為を行ったと認められる場合
- (6) 事後評価において支援内容が適正でないと認められる場合
- (7) 社会的信用を失墜する行為を行った場合
- (8) 心身に著しい障害があるため、専門家としての業務に耐えられないと認められる場合
- (9) その他、本事業の専門家として不適合と認める場合

(3) 委嘱手続のパターンについて

前年度の事業において、企業に所属しながら参加する専門家には、それぞれの企業によって様々な副業ルールがあること、また、自身が経営する法人への謝金振込を希望する場合があることが分かった。また、所属先の企業に副業の制度がなく参加ができないという登録セキスペ(RISS)からの声もあった。前年度は事案の発生都度、例外処理として対応したが、本年度はより多くの登録セキスペ(RISS)がスムーズに事業に参加し、コンサルティング実績やスキルアップを図ることができるよう、当初から委嘱方法について3つのパターン(表13参照)で事務処理を設計して対応した。

表 13 指導専門家への委嘱手続のパターン

委嘱パターン		内容
A	個人への委嘱	本事業の基本となる手続で、指導専門家個人宛てに委嘱状を発行し、謝金の振込みも、指導専門家個人名義の口座へ振込を行った。
B	法人口座利用の個人への委嘱	指導専門家個人宛てに委嘱状を発行するが、謝金は指導専門家が所属する法人口座に振込を行った(指導専門家自身が個人事業主として登録している法人口座への振込も含む)。
C	法人間の取引とする委嘱	所属企業に副業等の規程がない場合等に、企業宛てに委嘱状を発行して就任を承諾してもらい、謝金も法人口座に振込を行った。又は、指導専門家自身が起業している場合も、その法人との取引として、法人への委嘱と法人口座への振込を行なった。

また、専門家が副業として本事業に参加する場合には、委嘱を承諾するにあたって所属企業内で副業申請など手続が必要となる。そのため、事業趣旨と委嘱内容について記載した「事務局からの

所属企業あてレター」を用意し、専門家の希望に応じて提供を行った。

(4) 指導専門家登録の方法

オンラインによる「指導講習会」の受講完了後、本事業への参加を希望する専門家は、事務局の「指導専門家登録サイト」より、「委嘱条件」に同意のうえ登録を行ってもらった。

<指導専門家の登録事項>

<input type="checkbox"/> RISS登録番号	<input type="checkbox"/> 氏名（フリガナ）	<input type="checkbox"/> 住所（郵便番号 建物名）
<input type="checkbox"/> 連絡先（メールアドレス）	<input type="checkbox"/> 連絡先（電話番号）	<input type="checkbox"/> 活動可能地域（都道府県、市区町村）
<input type="checkbox"/> RISS以外の保有資格（選択式）	<input type="checkbox"/> Sプレゼンター登録について	<input type="checkbox"/> オンライン指導の可否（利用可能なツールの選択）
<input type="checkbox"/> 委嘱の形態（3パターン）	<input type="checkbox"/> 所属企業宛てレターの要・不要 ※所属企業に副業申請等を行う場合に添付する書類として提供します。	
<input type="checkbox"/> 中小企業からの事前指名の有無 ※専門家からの勧誘等により、中小企業からの指名が見込まれている場合に登録してください。		
<input type="checkbox"/> 経験者への同行（OJT）希望 ※単独で支援することが不安な場合に、経験者の支援先に同行してみたいかどうかの意向確認。同行先での支援は無償です。（意向に沿えない場合もありますのでご了承ください。）		

この段階で、希望する委嘱のパターンのほか、オンラインでの指導の可否、中小企業等からの事前指名の有無、OJTの希望などの把握を行った。

(5) 指導の進捗管理

前年度は、専門家が指導の実施回ごとに作成する「実施報告書」を、指導進捗と謝金支払いの両方に準用していたことから、全指導回分をまとめて謝金請求する専門家の進捗管理がタイムリーに実施できないという課題があった。このため、本年度は指導回ごとの実施報告は指導実施後1週間以内にメールで報告を求めることとし、指導進捗がタイムリーに把握できるように改善した。

また、報告に使用する様式は、「第1回実施報告兼計画書（様式6）」と「第2回～4回指導実施報告書（様式7）」の2つに分け、第1回の指導訪問で指導先企業と調整した後、第2回以降の指導スケジュール予定を把握できるようにした。これにより、次回以降の指導について予定した日程から1週間以上経っても報告がない場合は、事務局から進捗確認のフォローを行う運用とした。

指導の実施

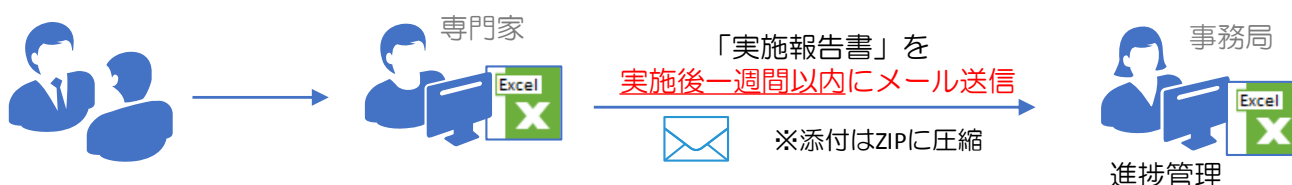


図 14 指導の進捗管理

(6) 謝金の支払い

謝金の請求は実施回ごと、又は複数回のまとめた請求のどちらでも可としたが、原則として指導終了後1か月以内に実施することとした。請求時の証憑として、指導先企業に当日の指導終了後に記載、捺印していただく「指導終了書（様式5）」を「請求書（様式4a又は様式4b）」に添付し、原本を事務局宛てに郵送することとした。また、第4回指導分の支払いは指導要領（指導ツール）で指定された成果物の提出が確認されることを条件とした。

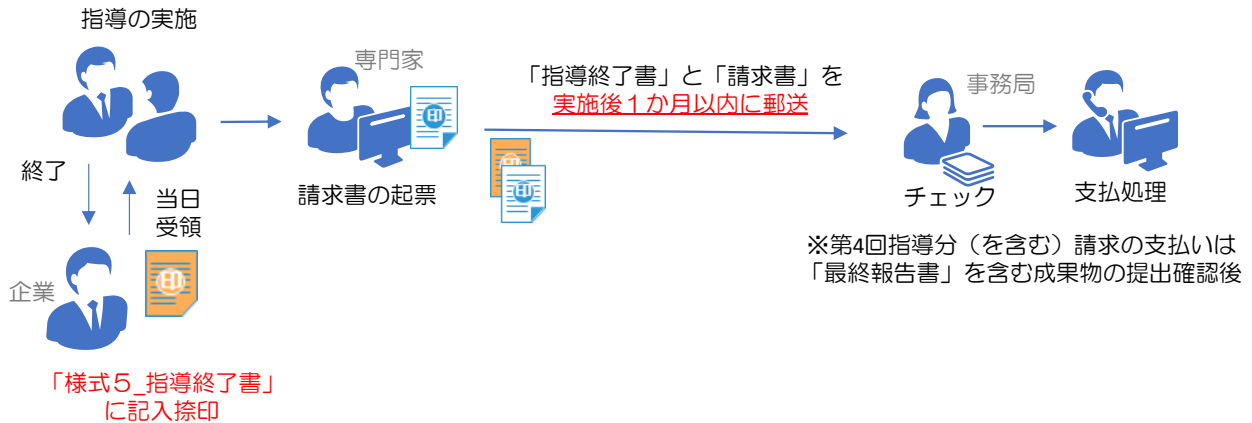


図 15 謝金支払いの流れ

謝金の支払いは、月末請求締め翌月25日払いを基本として、委嘱手続で登録した口座に振込みを行った。ただし、事業最終月は2021年2月15日（月）の振込みとした。謝金の最終支払い期日を考慮し、当初の請求書等の最終提出は「2021年1月25日（月）必着」で案内を行った。

源泉徴収は法人間の取引による委嘱でない限り実施し、源泉徴収を行う場合には別途マイナンバーの取得を行った。

(7) 成果物の提出

「指導要領（指導ツール）」で指定された「表14 事務局に提出する成果物」に記載の成果物は、電子ファイルをメール添付で提出を受ける運用とした。

表 14 事務局に提出する成果物

成果物		提出時のファイル形式
成果物①	「5分でできる情報セキュリティ自社診断」	PDF ファイル
成果物②	情報セキュリティ基本方針	PDF ファイル
	関連規程の点検結果	PDF ファイル (Excel ファイルでも可)
成果物③	情報セキュリティ対策実行計画書	PDF ファイル (Excel ファイルでも可)
成果物④	指導最終報告 (SECURITY ACTION 二つ星宣言申請状況報告)	Excel ファイル

(8) 手続様式一式

専門家の指導管理及び謝金支払いについて、事務が準備した様式一覧を「表 15 手続き様式一覧」にまとめる。事務局から書面で郵送する様式 1 から様式 3（別紙含む）以外の様式は、IPA の専門家 Web サイトに掲載しダウンロードして利用するよう案内した。また、記載に不備が生じないよう、それぞれの様式には記入例を添付して展開した。

表 15 手続き様式一覧

様式	目的	名称	用途
様式 1	委嘱 手続	委嘱状	専門家への指導業務担当依頼
様式 2		就任承諾書	委嘱状に対する専門家の承諾書
様式 3		謝金振込口座登録依頼書	謝金の振込口座の指定
様式 3（別紙）		法人口座振込同意書	源泉徴収同意確認（Bのみ）
様式 4a	謝金の 支払い	請求書（個人）	個人委嘱（A、B）の請求書
様式 4b		請求書（法人）	法人委嘱（C）の請求書
様式 5		指導終了書	指導先企業からの指導実施確認
様式 6	進捗 確認	第 1 回実施報告兼計画書	第 1 回指導終了報告と指導計画
様式 7		第 2 回～4 回指導実施報告書	第 2 回以降の指導の進捗報告
指導最終報告		指導最終報告	指導先企業ごとの指導後状況報告

6.2. 専門家指導の結果

(1) 指導実績の進捗状況

「図 16 指導予定及び実績進捗状況推移」に、専門家による指導予定及び実績の進捗状況推移を示す。

マッチング総数 395 件のうち、中小企業側の社内都合による途中終了 2 件を除く 393 件が予定どおり指導業務を終了することができた。本年度は、指導要領（指導ツール）及び実施報告、謝金手続等の入念な事前準備により、指導業務の進捗が指導 1 回目に作成した予定とおり推移し、比較的順調であった。なお、指導業務終了のうち、3 件については標準指導カリキュラム（4 回）を回数短縮して実施した。

指導途中終了 2 件及び指導回数短縮 3 件の内訳は以下のとおりである。

【指導途中終了】

- ・指導 1 回目で終了 1 社（東京／海外本社の意向のため）
- ・指導 2 回目で終了 1 社（沖縄／製品製造多忙のため）

【指導回数短縮】

- ・指導回数 3 回で完了 3 社
（神奈川／テレワークセクション指導スキップのため）
（大阪／3、4 回目のカリキュラムを同日午後に実施）
（大阪／3、4 回目のカリキュラムを同日午後に実施）

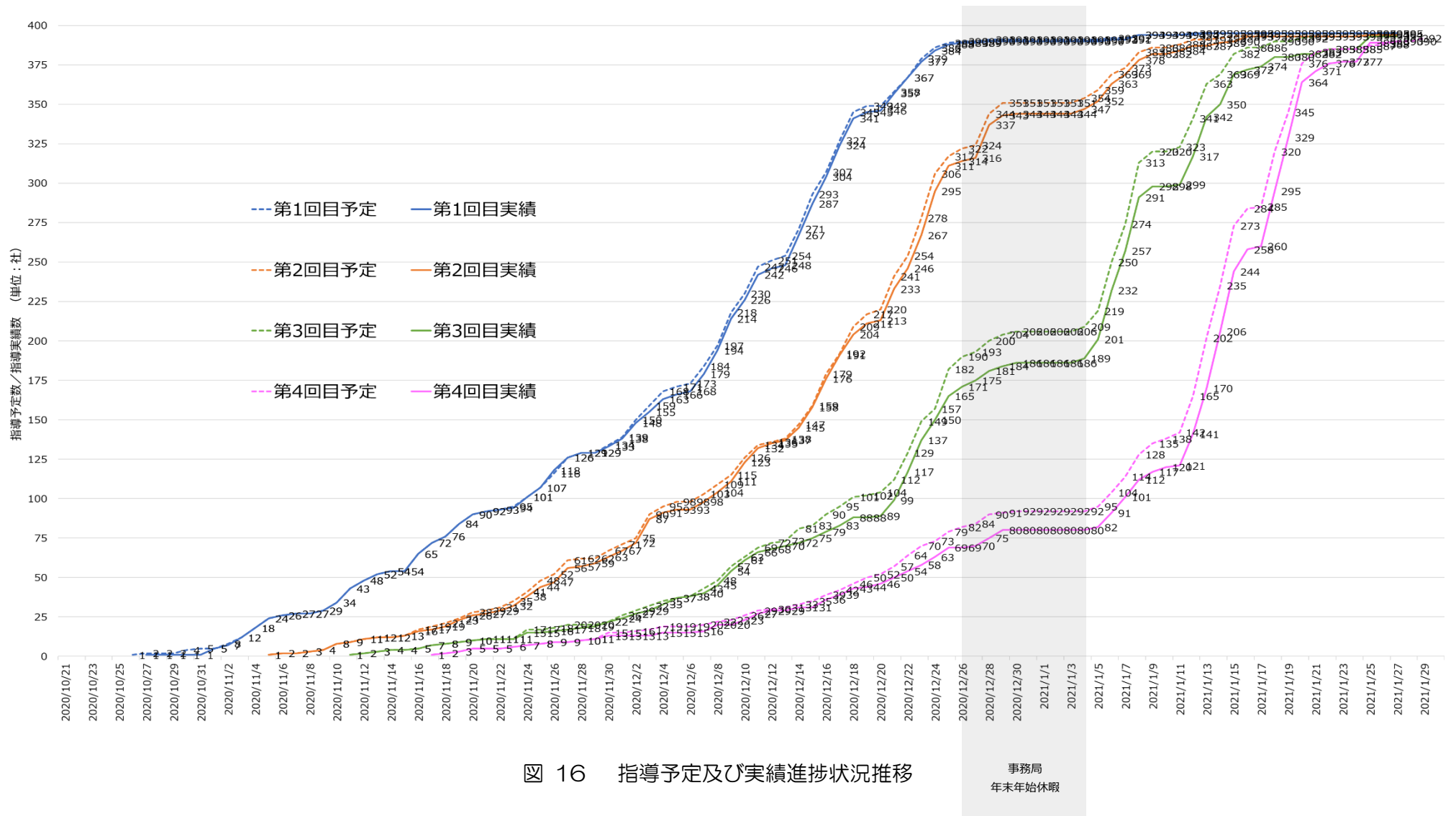


図 16 指導予定及び実績進捗状況推移

(2) 1社あたりの指導完了までの所要日数について

1社あたりの指導完了までの所要日数のヒストグラムを「図 17 1社あたりの指導における所要日数の分布」に示す。標準指導カリキュラム（4回）を完了した企業数 390 社のうち、367 社（94%）が 60 日（2 か月）以内で指導完了できた。また 26～30 日で指導完了した企業数が 80 社（21%）あり最多を占めた。

指導にあたって専門家に提供した標準指導カリキュラムに基づく指導要領（指導ツール）は、2 か月以内で指導完了することを前提に制作したツールであり、90%以上の企業が 2 か月に以内に指導完了していることから、概ね想定とおりの効果が得られたカリキュラムであったことが分かる。

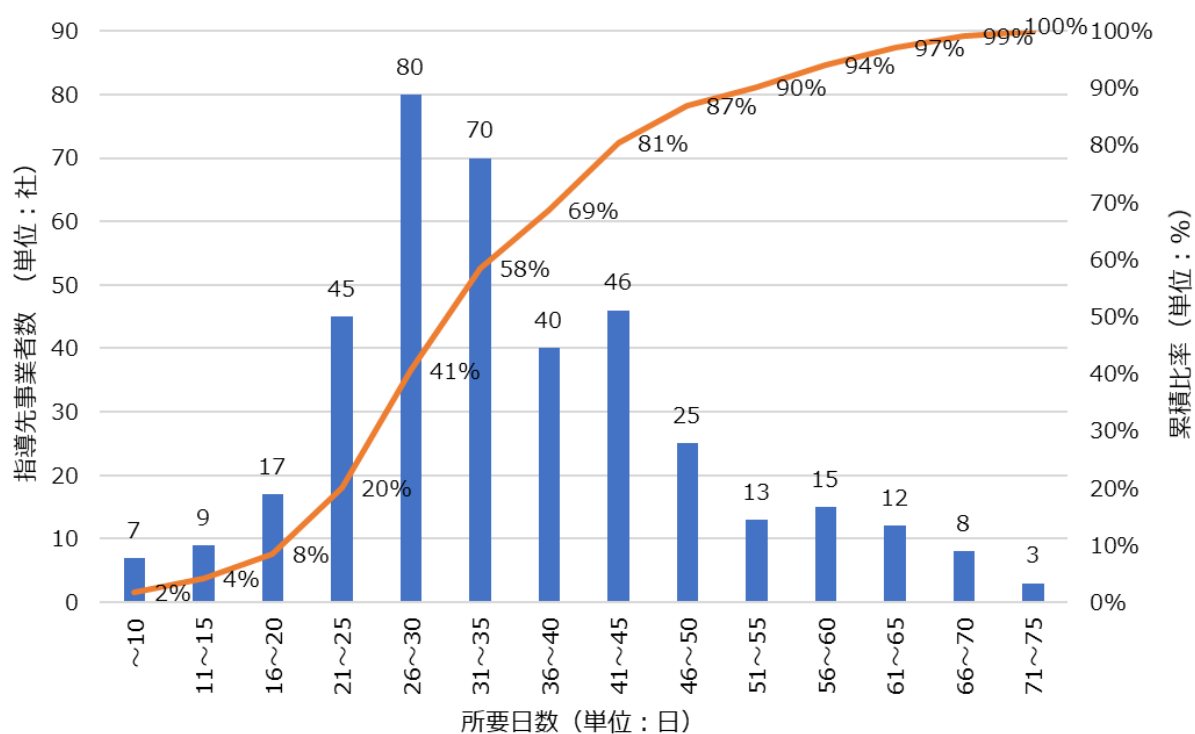


図 17 1社あたりの指導における所要日数の分布

(3) OJT 制度の成果

コンサルティングに係る経験・スキル（コミュニケーション含む）の不足から、セキュリティマネジメント指導業務へ参加する障壁が高いと感じる専門家に対して、本年度はコンサルティング経験が豊富な登録セキスペ（RISS）との同行による OJT 制度を設け、OJT 参加者 13 名、OJT 指導者 13 名にてチームを組み、計 14 社（一組だけ 2 社実施）で OJT を実施した。

OJT 参加者及び OJT 指導者の声を以下に示す。両者ともに非常に好評の声が多く、指導受け入れ側からは、2 名体制での指導によるメリット（説得力が高まる、新たな気づき）についての言及も多かった。参加者からは制度継続を希望する声が多数あった。一方で、参加者と受け入れ側の調整作業等、OJT 制度に係るルールや運用面での準備不足の指摘があり、今後の改善が必要と考える。

【OJT 参加者側の声】

- とても丁寧なヒアリングの仕方、並びに具体例を提示しながらの対策案の指導について、ノウハウを得ることができた。 同行することにより、これまでの不安が払拭できた。
- 経営者から直接、話を聞くことにより、指導先企業の指導業務に対する期待と不安を速やかに把握し、対応することの重要性が分かった。単に、IPA の指針とおりにではなく、臨機応変に対応できるように準備する必要性を学んだ。
- 具体例を交え、IPA の各種資料を柔軟に活用し説明されていた。非常に有意義な時間であった。
- 訪問前の事前打ち合わせにて、前年度の実施内容と、それを踏まえた上で、今回の進め方を把握することができた。実際に同席しないとわからないお客様とのやりとりの仕方や、空気の作り方も学ぶことができた。また、ただ同席するだけでなく、最近のセキュリティ脅威の動向について、指導先企業に説明する時間も設けていただき、専門家としての知見を活かす機会も手にすることができた点が非常にありがたかった。
- ノウハウは得られたものの、やはり 1 回限りの OJT では 1 人で実践できるまでには至らなかった。とても良い制度なので、今後も継続していただきたいと考える。
- 同行前の調整を専門家同士だけではなく、ある程度事務局にて調整してほしい。 同行制度は今後も続けていくと良いと思う。
- 非常に良い制度と考える。 来年度以降も本事業を開催する場合は、ぜひ同行制度を継続してほしい。 私自身も次回単独で指導業務を無事に完了することができたら、次々回は OJT 受入を行い、後進の指導にも協力したいという気持ちがある。
- 情報処理安全確保支援士同士の仕事を通したつながりを作るきっかけにもなると感じ、参加をして良かったと思う。
- OJT の進め方は各専門家に一任されていたと思う。後進育成にも慣れているベテランの方に同行できた場合は特に問題ないが、そうではない場合、指導の進め方や役割分担で悩むかもしれない。そのため、OJT をスムーズに行うためのマニュアル、実施事例共有等の整備が必要と感じた。

【OJT 指導者側の声】

- 1名よりも専門家が2名体制で対応するスタイルは見た目にも説得力があり、指導先担当者も安心感が増すと思う。 OJT 参加者とは、コロナ感染防止のため Web 会議ツールによる2時間ほどの打ち合わせを行い、双方にとって時間節約、業務への負担軽減となった。
- 私とは違う視点で OJT 参加者が発言されたことがあり、指導者として学びと気づきがあった。1名で指導するよりも複数名で指導したことで説得力が増した。
- 各回のカリキュラムの中で、OJT 参加者の練習を兼ねて、お客様先で話していただくきっかけを用意した。OJT 参加者も事前に詳しく調べて話していただけたので、お客様への説得力が増したと思う。
- 顧客の困りごととその場で対応するところを見て、小規模事業者の情報セキュリティの実際を知ってもらえた。
- お客様にとっては、専門家が2名同席しているお徳感があったと考える。追加説明が有効である場合に、OJT 参加者が気づいて追加の話ができた。これから支援業務に携わる方々に対し、少しは役に立てた。
- 指導先企業との打ち合わせ時、OJT 参加者から指導先企業の課題に対してアドバイスをいただいた。複数の情報処理安全確保支援士が、それぞれ別の視点で助言することができたため、指導先企業により多くの課題解決の選択肢を提供できたのではないかと思う。
- 1人でのコンサルティングの場合、基本的に1人の意見となるが、情報処理安全確保支援士が2名で一部でも説明することで、同じ提案を行った場合でも、より実現性や正当性を強調することができた。
- 同行制度を受け入れることによるインセンティブが必要。
- 経験の少ない OJT 参加者を伴ってのセキュリティ提案なので、情報漏洩などのリスクが不安だった。OJT を引き受ける側が安心できる説明が事務局からあると、もっと受入れやすいと思う。
- スケジュール調整、連絡の責任範囲を最初に明確にしたほうがよい。 OJT 希望者の同行を指導先企業に連絡して了承を得るのは、OJT 指導者自身が行うのか、それとも事務局が事前に連絡済みなのか、といった部分でとまどうことがあった。
- OJT 参加者の参加義務を明らかにしてほしい。 4回ともに参加するのか、自主性にまかせるのかわからない。
- OJT 参加者に自分が作成した資料を配布すべきかどうか明確でない。OJT 参加者はその作成資料を自身の指導資料として利用できるのでは、渡すのには躊躇があった。
- OJT 参加者にはたいへんたいへん満足いただけたと思う。 私自身も自己成長につながった。次回も機会があれば引き受けたい。
- OJT は、OJT 参加者、OJT 指導者、指導先企業の3者にメリットがある制度だと感じた。 最初の指導先として、事前指名がなく指導先企業を探すことが難しい方には OJT は良い制度だと思う。次回も希望者があれば、OJT の受け入れを行いたい。

6.3. 専門家への委嘱

(1) 委嘱パターンの状況

専門家への委嘱パターンの状況を「表 16 委嘱のパターン別実績」に示す。

表 16 委嘱のパターン別実績

委嘱のパターン	登録時点		委嘱実績	
	人数	割合	人数	割合
A:個人への委嘱	375	83.0%	171	79.2%
B:法人口座利用の個人への委嘱	19	4.2%	10	4.6%
C:法人間の取引とする委嘱	58	12.8%	35	16.2%
合計	452	100%	216	100%

専門家の登録時点並びにマッチング後の委嘱実績においても、全体の約8割は「A:個人への委嘱」を希望していた。

また、「C:法人間の取引とする委嘱」で登録を希望した専門家には理由を確認したところ、「指導を実施する専門家自身が経営している（代表者である）法人で取引したい」が36人（62.1%）、「勤務先の制度上の理由で勤務先の業務としなければ指導業務に参加ができない、又は就業時間外にしか活動ができないから」が19人（32.8%）、未回答が3人（5.2%）という結果であった。

委嘱実績の全体割合からみると2割程度ではあるが、個人として謝金を受取る方法では参加しづらい立場にある専門家が一定数存在しており、本年度、事務手続の枠を拡げて対応したことは有意義であったと考える。

(2) 委嘱後の指導実績

委嘱した専門家に対しては、委嘱条件に基づき謝金として45,000円/指導回の支払いを行った。指導先企業の都合から予定されていた回数が実施されず途中終了する、又は複数回分の指導を同日に行う指導回数短縮といった対応が生じていた。

全ての専門家による第1回から第4回までのそれぞれの実績回数合計は「表 17 委嘱した指導専門家による指導実績」のとおりであった。

表 17 委嘱した指導専門家による指導実績

指導回	実施回数	備考
第1回目	395回	委嘱を行った全指導専門家が実施
第2回目	394回	1回目で途中終了 1件
第3回目	393回	2回目で途中終了 1件
第4回目	390回	3回目で終了又は3.4回を同時実施 3件
計	1,572回	

6.4. 指導先企業別の指導最終報告

事務局における指導状況管理の最終確認として、各指導先企業での4回目の指導終了後に、指導を担当した専門家から「指導最終報告」として、「表 18 企業別指導最終報告の内容」に記載の報告項目(1)～(5)の報告を受けた。以下に報告状況の集計結果を示す。

表 18 企業別指導最終報告の内容

報告項目		内容
(1)	指導先企業の概況	<ul style="list-style-type: none"> ●指導先企業の参加人数 ●経営層参加の有無 ●標準カリキュラムの適性 ●経営層/従業員の取組意欲とセキュリティ知識 ●テレワーク導入状況
(2)	指導状況	<ul style="list-style-type: none"> ●指導内容(標準カリキュラムに加えたこと) ●指導する上で工夫したこと
(3)	指導の成果	<ul style="list-style-type: none"> ●SECURITY ACTION 二つ星宣言の状況 ●経営層/従業員のセキュリティに対する取組意欲の変化 ●企業としての情報セキュリティレベルの変化
(4)	有償による継続フォローについての提案状況	<ul style="list-style-type: none"> ●有償継続フォロー提案実施の有無 ●企業側の継続フォローニーズ
(5)	指導事例としての適性	<ul style="list-style-type: none"> ●横展開できる指導事例としての適性 ●事例掲載協力の可否

(1) 指導先企業の概況

指導への参加状況

指導先企業の指導への参加状況は、1名で指導を受けている企業が最も多いが、概ね1～3名で指導を受けている。また、8割以上の企業で経営層が参加している。

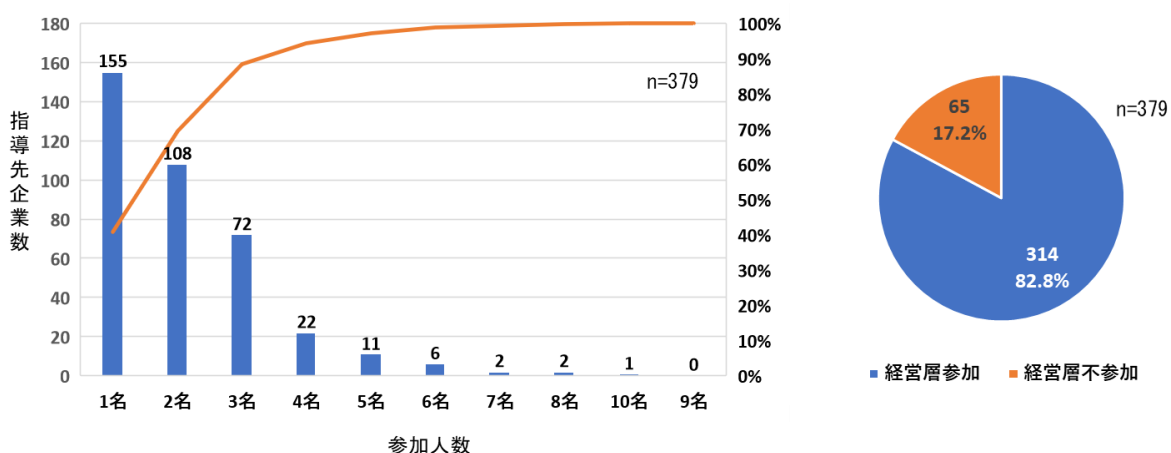


図 18 指導への参加状況

標準カリキュラムの適性

指導先企業の状況として、標準カリキュラムによる指導の適性を確認したところ、73.6%が「ちょうど良いレベル」との報告があった。「もの足りないレベル」との報告も5.5%あり、情報セキュリティ対策が進んでいる企業も本事業に参加していたことが推察できる。

n=379

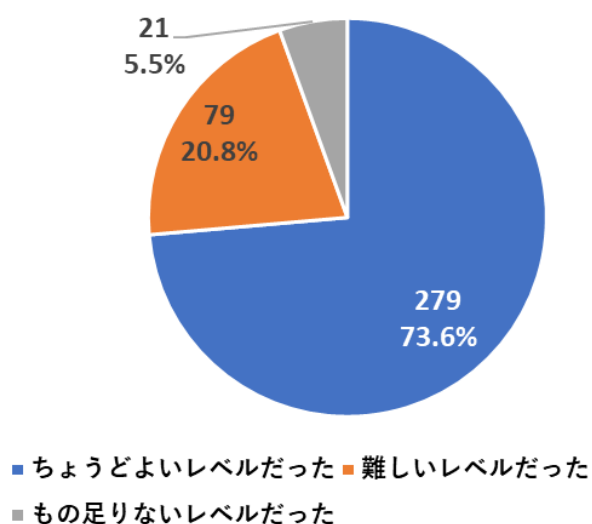


図 19 標準カリキュラムの適性

経営層/従業員の取組意欲とセキュリティ知識

初回訪問時（指導前）の所感として、「セキュリティに対する取組意欲は高いが知識が不足している」状況の企業が多かった。取組意欲については、指導先企業の8割で経営層が参加していることから、総じて経営層の意欲が高いと感じた専門家が多くなっていると推察できる。

n=379

n=379

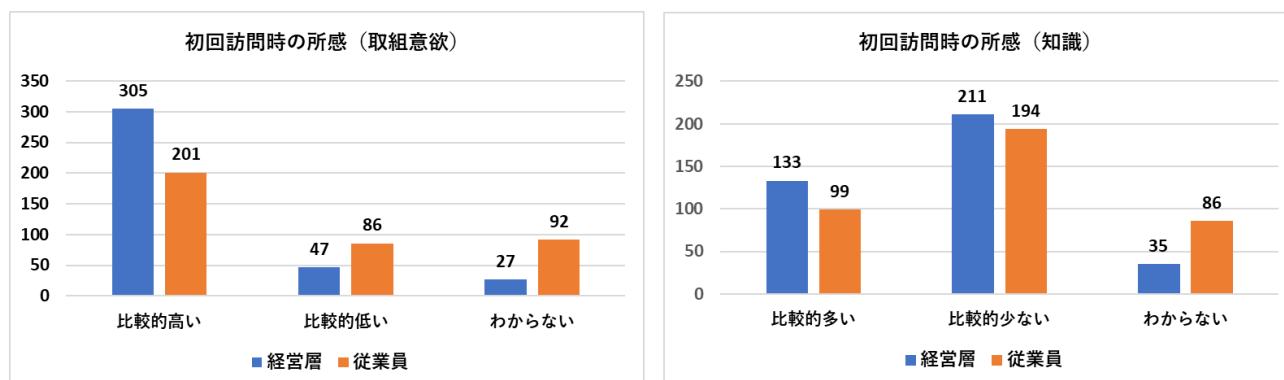


図 20 経営層/従業員の取組意欲とセキュリティ知識

テレワークの導入状況

テレワークは52.5%の指導先企業が導入していたが、「十分に活用できていない」企業が15.3%あり、全体として中小企業のテレワークの活用が進んでいない状況だった。

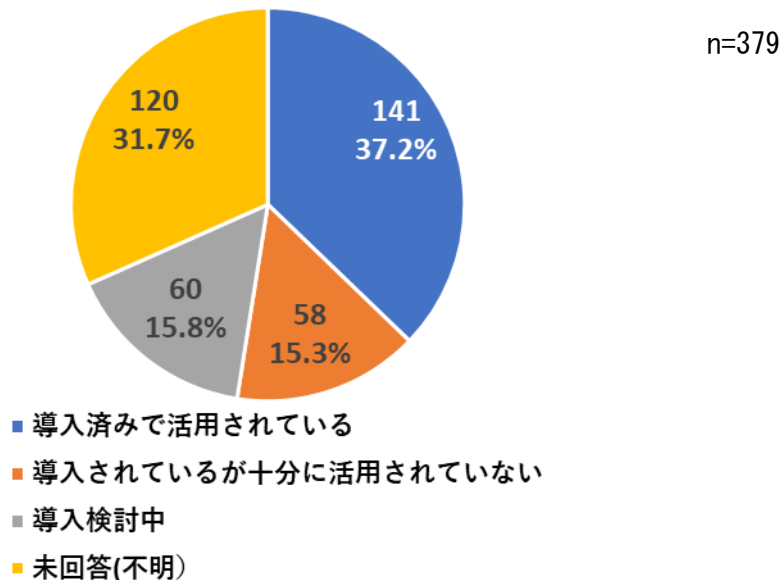


図 21 テレワークの導入状況

(2) 指導状況

指導状況について

指導内容については、「標準カリキュラム以外の内容も加えながら実施した」との報告が55.9%あり、標準カリキュラム以外の指導を行った理由としては「当該企業にとって必要と判断したから」との理由が多かった。専門家が標準カリキュラムを基本としながらも、企業の状況を診断したうえで、必要な指導を行っていたことがうかがえる。

標準カリキュラムで規定した成果物のほかに、以下の成果物が作成された。

- ・情報セキュリティハンドブック
- ・秘密保持誓約書のひな型
- ・クラウドシステム等選定基準、利用ルール
- ・テレワーク関連規程 等

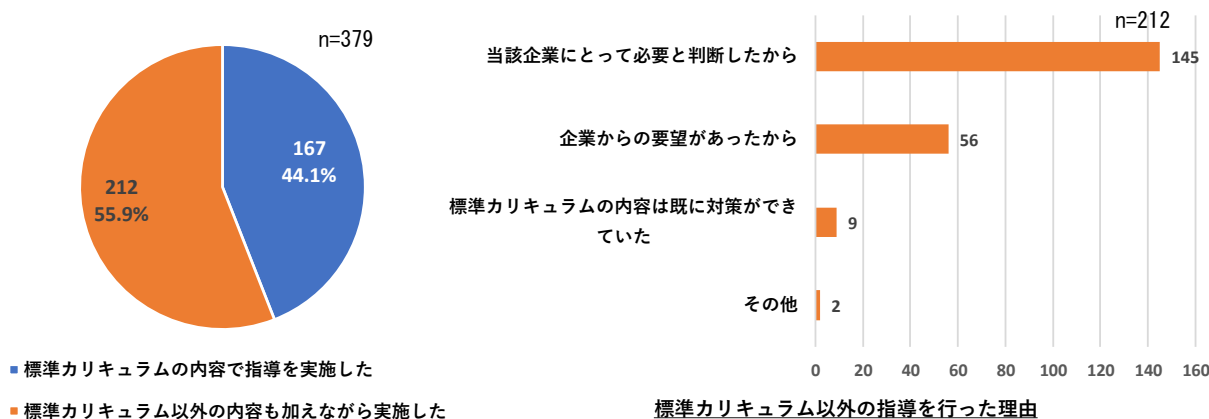


図 22 指導状況について

指導する上で苦労したこと、工夫したこと(自由記述)

指導専門家から多くの声が寄せられたが、本年度はオンラインで指導を行ったことによる苦労や、指導の工夫が必要になったとするコメントが多かった。オンライン指導は、指導先企業とのオンラインでのコミュニケーションを上手く行うことが成功のポイントとする意見が多く、今回の指導による工夫が、今後のオンライン指導方法の知見となると思われる。

<オンラインの指導で工夫したこと>

- オンライン指導で行ったことにより、企業の実態を視覚によって知ることができず、ホームページからの情報や会話からのみ理解する必要があるため、的確な状況判断に苦労した。そこで、こちらからの一方的な情報提供に偏らず、経営者の方に積極的に発言をしてもらうように心がけた。
- 2回目以降はオンラインでの指導だったので、規定類などの現物確認が難しかった。
- 会社全体の情報リテラシー不足しており、情報提供依頼時に先方が何を出して良いのかわからず、作業が滞ることが多い。それに伴い、少ない時間でのオンラインのやり取りは困難を極めた。
- オンラインでの実施となり、現場状況を目で確認することができなかつたため、かなり詳細なヒアリングを心がけた。
- コロナの影響で急遽オンラインの実施に変更した。オンラインだと会話が難しくなるため苦労した。
- オンラインでの実施を活かし、必要な情報をインターネットから検索し、提示することで、言葉や事前準備した資料以外にも、状況に応じた情報を交えて指導するように工夫した。
- 指導先もオンラインでの指導も希望していたこともあり、第1回目以外はオンラインでの指導を行った。資料などを画面共有しながら指導を進めたので、対面での指導と変わりなく行うことができた。2回目は大雪と重なり、参加者が定刻に揃わなかったが、何とか指導を実施することができた。テレワークを実施している企業だったため、オンラインでの業務遂行に慣れていたことも助かった。
- オンライン会議方式で行ったことやマスク越しであったため、相手の表情や反応が分かりにくいことにやり難さがあった。そのため、一方的な説明口調にならないように、質問を交えるなど、会話のキャッチボールができるように心がけた。

(3) 指導の成果

SECURITY ACTION 二つ星宣言の申請状況

指導先企業の SECURITY ACTION 二つ星宣言の申請状況は、最終報告の提出締切時点で「宣言済み」、「申請済み」合わせて 32.8% だった。

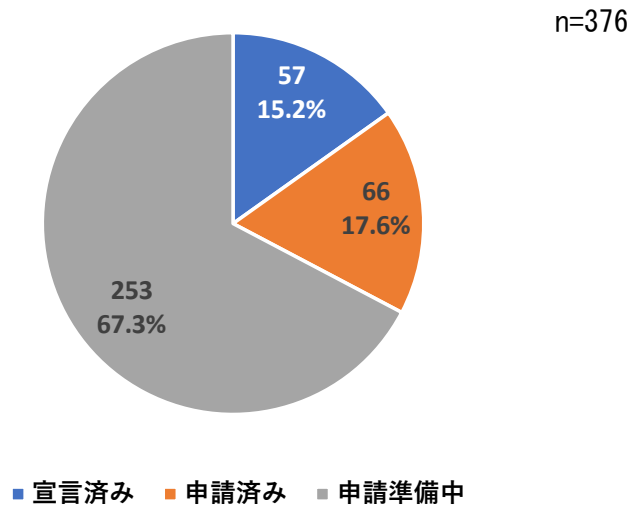


図 23 SECURITY ACTION 二つ星宣言の申請状況

経営層/従業員のセキュリティに対する取組意欲の変化

指導先企業のセキュリティに対する取組意欲は、経営層においては 84.4%、従業員においては 68.3% が向上したとの報告があり、経営層と従業員で差があるものの、前年度同様に指導先企業のセキュリティ意識の向上が図れたことが伺える。（前年度：経営層 86.4%、従業員 68.0% が取組意欲向上）

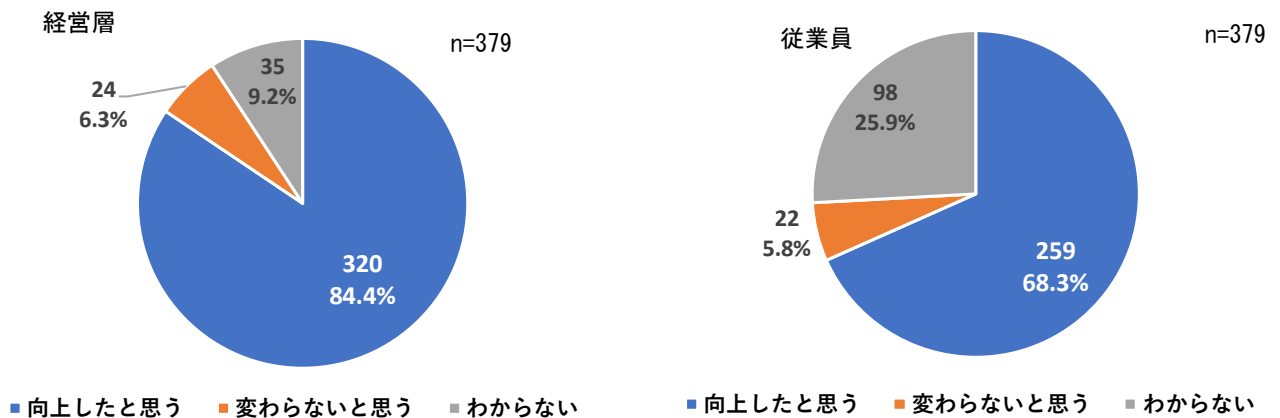


図 24 経営層/従業員のセキュリティに対する取組意欲の向上（指導後）

企業としての情報セキュリティレベルの変化

指導先企業の情報セキュリティレベルについては、97.6%が「向上したと思う」と報告し、前年度の結果（92%）を上回った。向上した理由としては、「規程類が整備できたから」、「実施体制を確立することができたから」が多く、指導業務の結果、関連規程や実施計画を実施するための体制作りができたことが伺える。

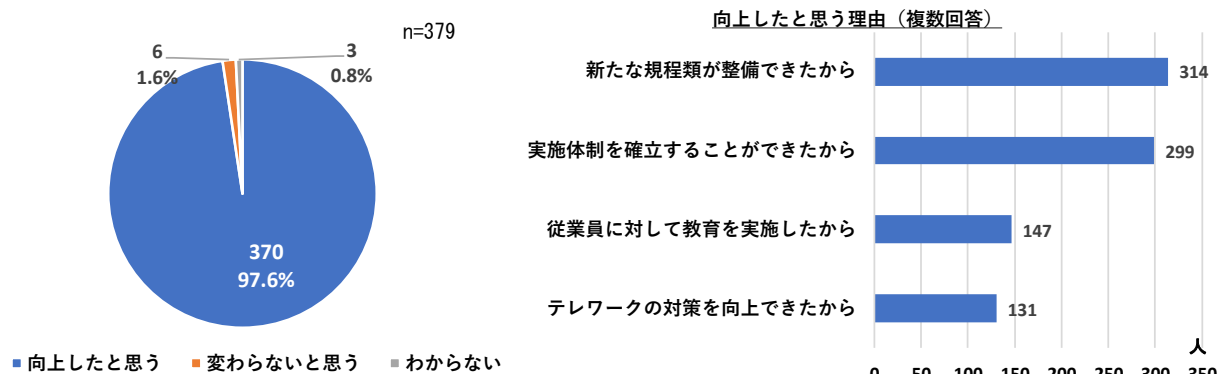


図 25 企業としての情報セキュリティレベルの変化

(4) 有償による継続フォローについての提案実施状況

有償継続フォローについての提案と結果

64.1%の専門家が指導先企業へ有償での継続フォローを提案したところ、回答のあった企業のうち、15.7%（37社）の指導先企業から実際に依頼があった。また、46.8%（110社）の指導先企業が有償サービスを検討しているとの回答があり、有償でも専門家による支援のニーズがあることが確認できた。

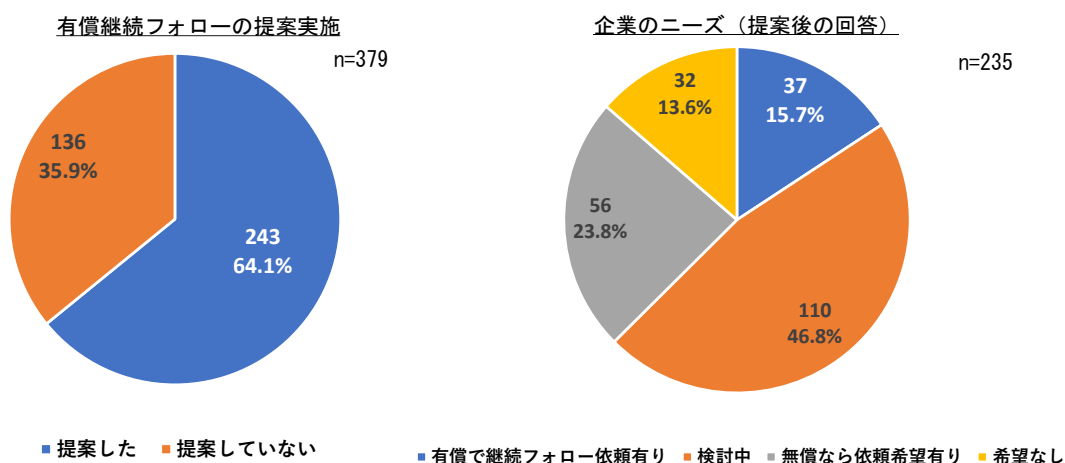


図 26 有償継続フォロー提案実施の状況

(5) 指導事例としての適性

横展開する事例として適しているか

指導先企業の事例が、他の中小企業においても参考になる指導事例であるとの報告があったのは 42.0% (159 件) であったが、事例として取り上げる場合の協力については、ほとんどの専門家から「協力できる」という回答を得た。実際に、指導事例としてインタビューを依頼した専門家からは全て承諾を得た (企業側の都合で実施できなかったケースはあり)。

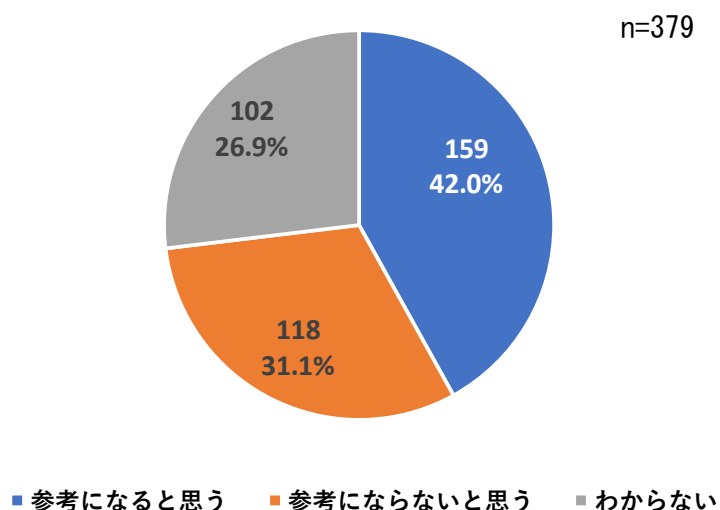


図 27 横展開する事例として適しているか

(6) 指導最終報告のまとめ

専門家からの報告によれば、本事業に参加した指導先企業は、ほぼ全社がセキュリティレベルを向上することができた。また、経営層と従業員も、それぞれセキュリティに対する取組意欲が向上し、セキュリティ意識の向上を図ることができた。

指導先企業から、有償による継続フォローの依頼を獲得した実績ができたことも、登録セキスぺ（RISS）の自走化に向けて大きな成果であった。指導業務の標準カリキュラムを基本としながらも、専門家がそれぞれの経験や知見を活かして、指導先企業のニーズに合ったコンサルティングを行い、企業の信頼を得られた結果と考えられる。

6.5. 専門家からの問い合わせ対応

専門家からの問い合わせは総数で 497 件であった。前年度との問い合わせ区分の比較を「表 19 専門家からの問い合わせ」に示す。

問い合わせ件数は、「5: 手続」「10: 実施報告」「12: 講習会」が多いが、「5: 手続」「10: 実施報告」については前年度より件数が減少した。前年度の業務実績から、事務局の事前準備を改善した結果と考えられる。

「12: 講習会」の問い合わせ内容は、E-ラーニングシステムの発行 ID、操作等に関する内容が多数を占め、講習内容に関する問い合わせは、ほとんどなかった。

表 19 専門家からの問い合わせ

問い合わせ区分	前年度 (%)	本年度 (%)	主要な問い合わせ内容
1: 事業全般	2.8	5.8	・謝金を受け取らずに参加は可能か。 ・指導業務の時間帯は平日の日中だけか。
2: 事業への参加	3.1	6.6	・プレゼンター登録がまだ公開されていない状態だが、中小企業側は自身を指名して申し込んでもらっても大丈夫か。
3: 副業について	4.4	2.0	・地方公務員は、副業や兼業等を行う際には所属組織への届け出が必要のため、記載事項を確認したい。
4: プレゼンター登録	4.9	2.8	・「コンテンツ利用」での登録ではダメなのか。 ・登録を行ったが、検索サイトにはまだ表示されない。
5: 手続	17.2	14.7	・就任承諾書の住所はプレゼンター登録の住所で良いか。 ・請求書は1ヶ月以内であれば数回分をまとめて良いか。
6: 指導先	4.9	6.0	・指名いただいた企業からの申込が入っているか。 ・本社と事業所が存在するが、別々に申し込むのか、1社で1回の申込みで良いのか。
7: マッチング	7.2	4.8	・マッチングはどのように行われるのか。 ・お客様へ本事業を案内し、依頼を受けても良いか。
8: 指導用資料	14.9	6.8	・ガイドラインの冊子をもらえないか。 ・自社診断のレーダーチャートが画面から消える。
9: 指導実施	9.3	9.5	・訪問指導は1ヶ月で終わらせなければいけないか。 ・オンラインの実施は許されているのか。
10: 実施報告	27.5	14.1	・指導修了書と請求書はまとめて送るのか。また、提出方法はどのように送るのか。 ・前年度と提出する成果物は違うのか。
11: SECURITY ACTION	2.6	3.0	・一つ星宣言をまだしていない場合はどうすれば良いか。 ・二つ星宣言登録の際、「情報セキュリティ基本方針の外部公開」が条件になるが、外部公開どのような手段か。
12: 講習会	0.0	20.3	・初回用 URL の有効期限が切れてしまった。 ・ID とパスワード設定用 URL の通知が来っていない。
13: OJT	0.0	1.8	・RISS の資格がなくても参加することは可能か。 ・初回訪問だけでなく、全4回とも同行可能か。
14: その他	1.3	1.6	指導先企業からの質問で、指導終了後にホームページなどで指導を受けたことを宣伝したいが問題ないか。

6.6. 専門家による指導実績のまとめ

本年度はコロナ禍という状況から、指導業務への影響が懸念されていたが、指導先企業の希望によってはオンラインによる指導も実施され、専門家による指導の工夫もあって、無事に指導業務を終えることができた。また、1社あたりの指導先企業の指導期間は、概ね1か月程度で行われているケースが多く、標準カリキュラムで想定していた指導期間2か月以内に準じて指導が進められた。

専門家からの指導先別の指導最終報告の結果によると、「指導の結果、情報セキュリティレベルが向上した」との報告が97.6%となり、指導成果も達成することができた。さらに、本年度は有償による継続フォローを指導先企業に提案するよう推奨したところ、6割以上の指導専門家が提案を行い、その結果37社からは実際に継続した指導依頼を受け、110社が有償サービスを検討しているとの報告があった。これは、指導先企業に情報セキュリティの継続的な取組みの重要性を啓発できたことに加えて、指導専門家として指導先企業の信頼を得られた結果と考えられる。

7. 指導先企業及び専門家へのアンケート実施

7.1. 指導先企業アンケート

(1) 指導先企業アンケート概要

専門家より指導最終報告を受領後に、事務局から指導先企業へアンケートの回答を依頼した。その結果を以下に示す。

(2) 指導先企業アンケート結果のサマリ

回答数は、327/393 件で回収率 83.2%であった（前年度は 283/378 件で回収率 74.9%）。

【質問 1】 あなたの会社の業種は何ですか？ （択一選択）

製造業、サービス業（他に分類されないもの）、卸売業・小売業、学術研究・専門・技術サービス業、情報通信業、医療・福祉、建設業が 84.0%を占める。上位を占める回答者の業種は、ほぼ前年度と同様であった。

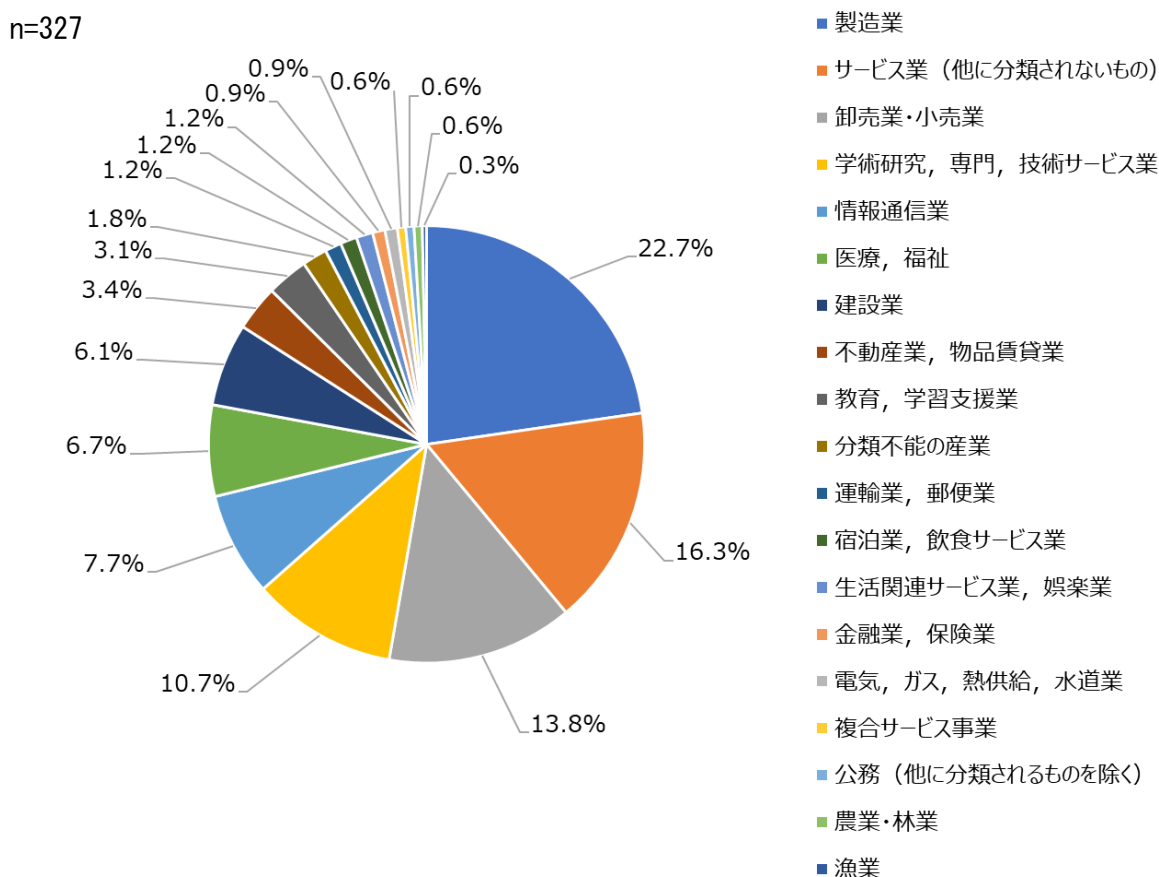


図 28 指導先企業の業種別割合

【質問2】 あなたの会社の従業員数を教えてください。(択一選択)

50人以下の事業者が全体の72.9%を占める。また、50人以下の各従業員区分の占める割合も前年度とほぼ同様であった。

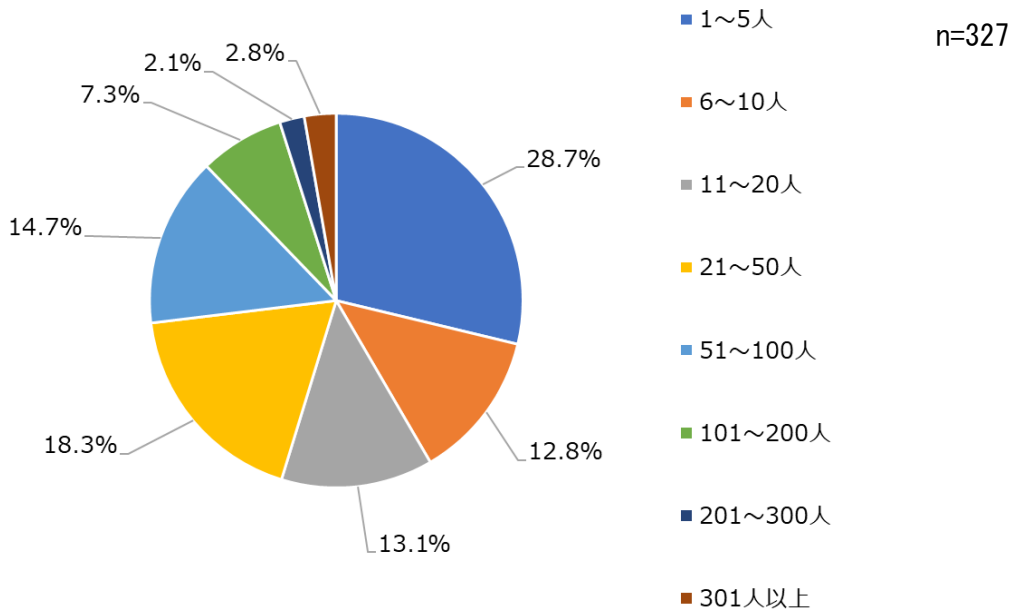


図 29 指導先企業の従業員数規模の割合

【質問3】 資本金又は出資総額を教えてください。(択一選択)

5千万円以下の事業者が全体の83.6%を占める。

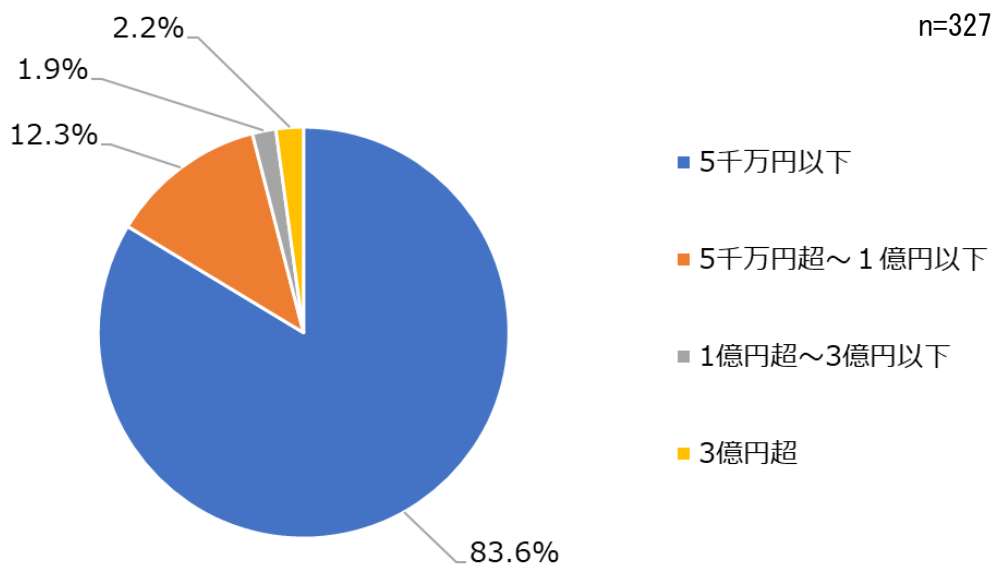


図 30 資本金又は出資総額規模の割合

【質問 4】 あなたの役職は何ですか？（複数選択）

回答者の 45.3%が経営者であった。各役職の回答数の割合も前年度とほぼ同様であった。

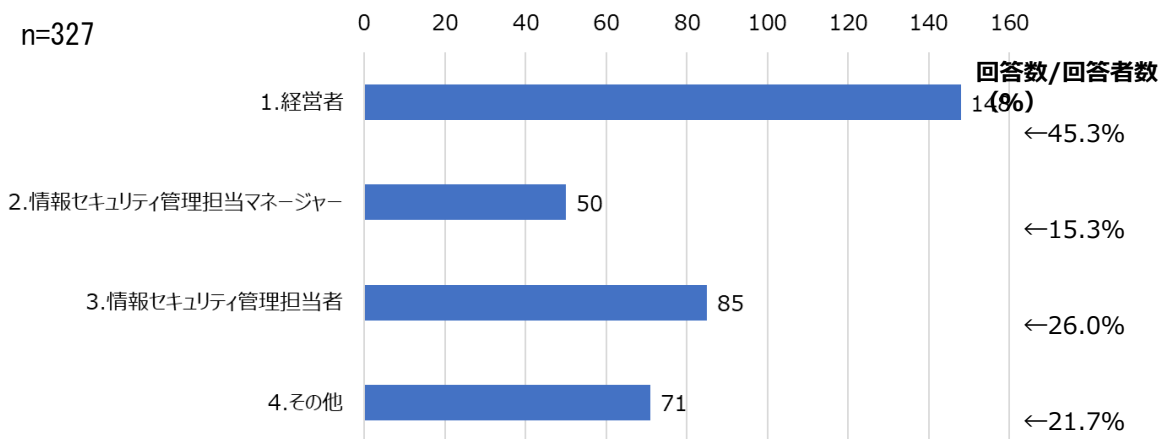


図 31 回答者の役職

「その他」の主な回答

- 総務部社員、総務部長、総務・経理担当
- ISMS推進会メンバー
- システム管理・運用担当者
- 役員、取締役

【質問 5】 あなたの会社における情報セキュリティ管理体制等の整備状況をご回答ください。

（複数選択）

「情報セキュリティ管理の組織または担当者を配置している」と回答者の 57.8%が回答。各整備状況の選択肢の回答数の割合は、前年度とほぼ同様であった。

「情報セキュリティ管理体制等の整備状況」と「業種」とのクロス集計からは、特徴的な傾向は見られなかった。

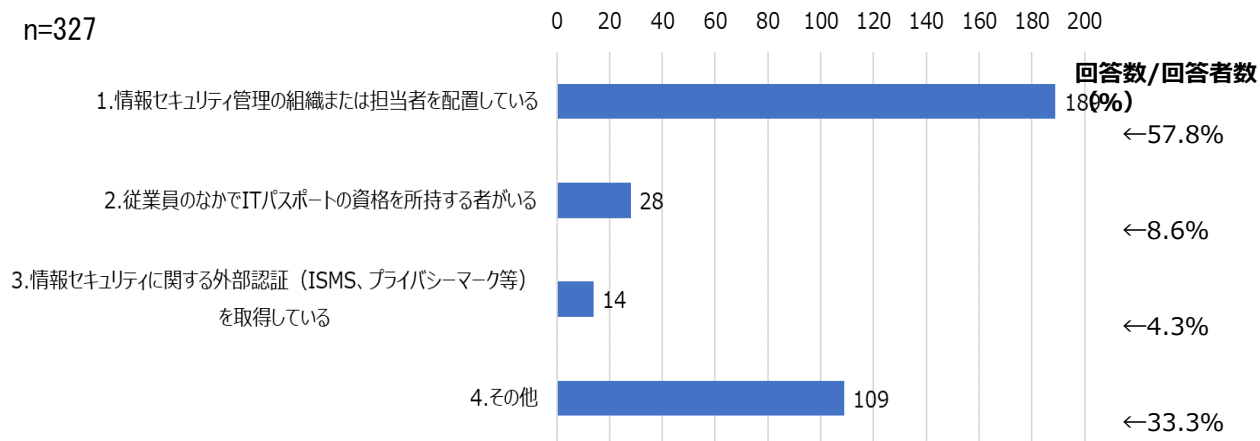


図 32 情報セキュリティ管理体制等の整備状況

「その他」の主な回答

- QMS 認証済み、ISMS、ISMS-CLD 審査員補、情報セキュリティマネジメント有資格者配置。
- 経営管理、総務、システム担当が、チームを組んで対応している。
- 個人情報保護マネジメントシステムにおいて個人情報保護に係る体制がある。
- 情報セキュリティマネジメント資格取得済み。

「情報セキュリティ管理体制等の整備状況」と「業種」のクロス集計

n=327

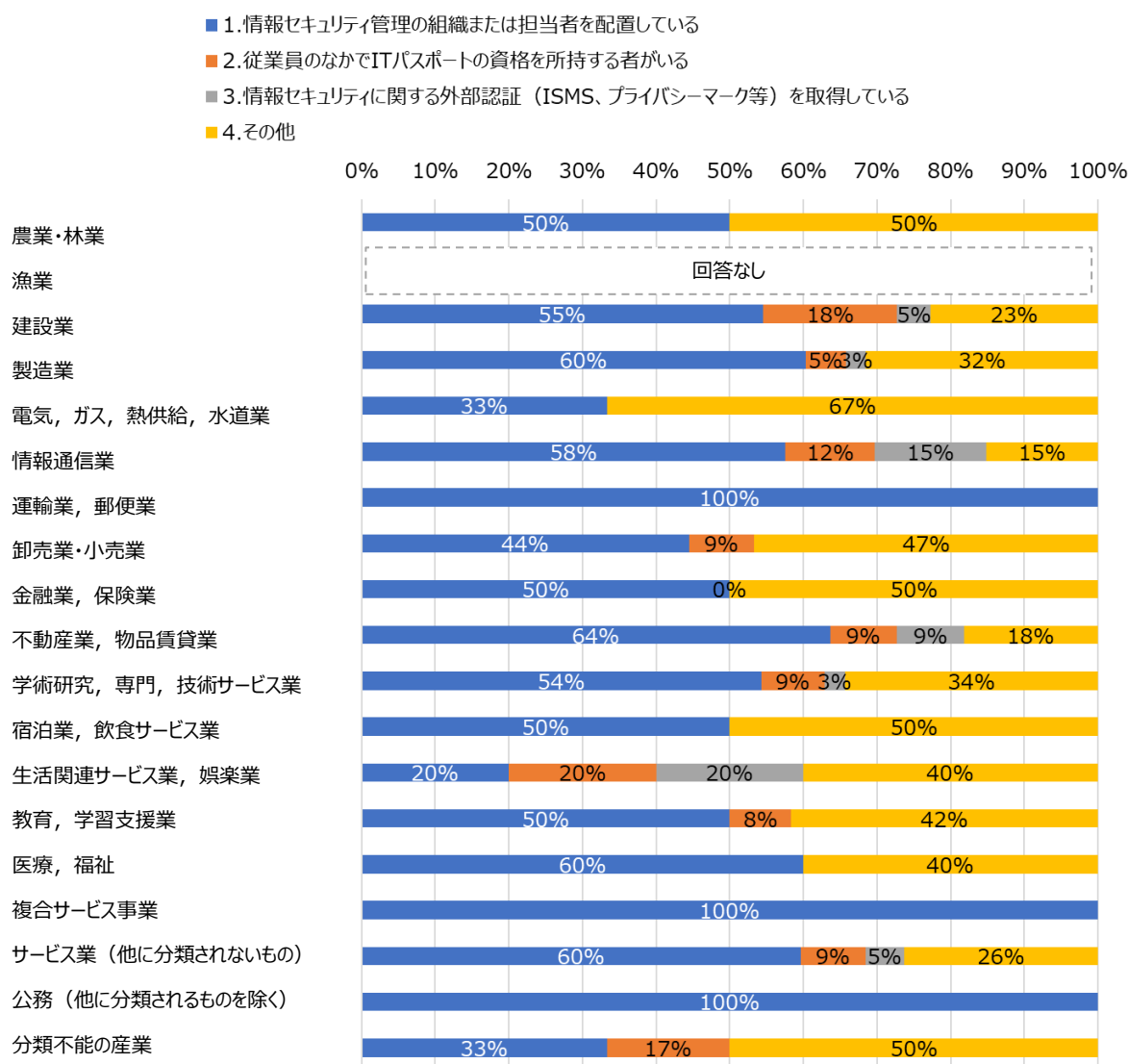


図 33 「情報セキュリティ管理体制等の整備状況」と「業種」のクロス集計

【質問6】「中小企業の情報セキュリティマネジメント指導」へ参加された目的は何ですか？

(複数選択)

回答選択肢 1. ~5. の回答数の割合は、約 40~50%を占めている。前年度とほぼ同様であった。「事業参加目的」と「業種」とのクロス集計からは、特徴的な傾向は見られなかった。

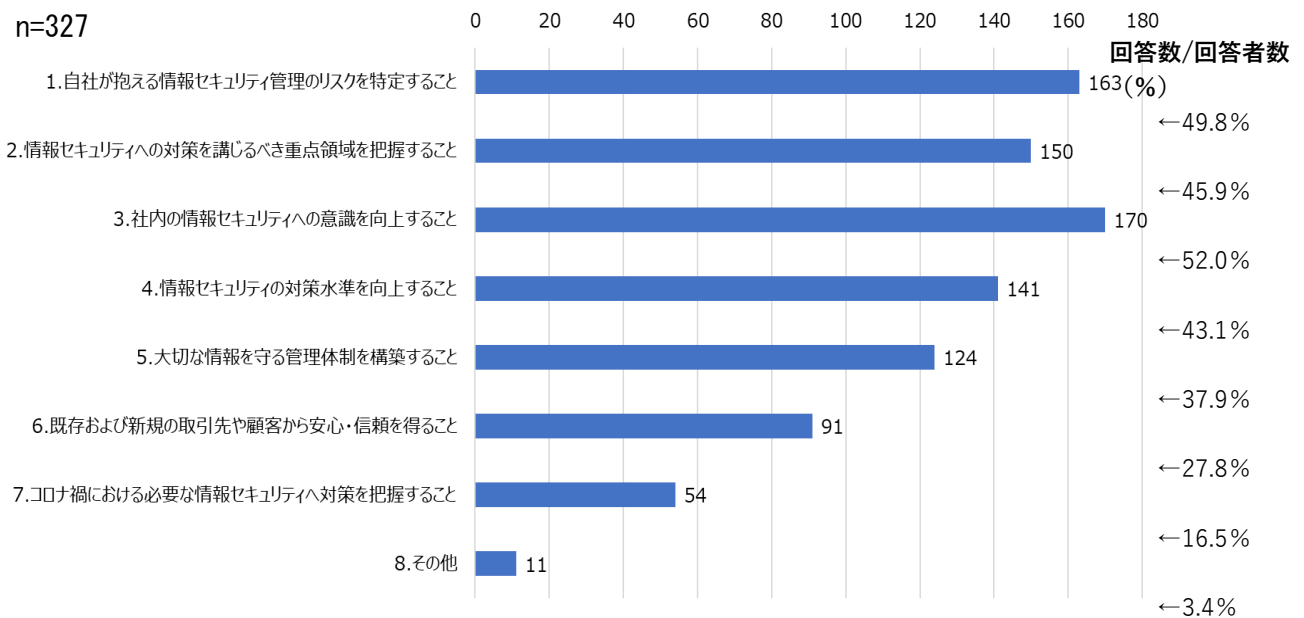


図 34 事業参加目的

「その他」の主な回答

- 当社の対策状況を共有して社員が把握し、各自がセキュリティ意識を向上できるようにする。
- テレワーク IT 助成金支給に際しての付属プログラムの参加。
- 情報セキュリティ管理体制を整備する、情報セキュリティポリシーの作成のため。
- 社内の情報セキュリティの見直しという意味で外部からの客観的な意見・指摘が欲しかった。
- テレワークへの移行にあたり、新たに講じる対策について理解すること。
- EC サイトを導入したこと、サーバーなどネットワークに関しても機器が増えることでこれから必要なセキュリティへの考えを知りたかった。

「事業参加目的」と「業種」のクロス集計

n=327

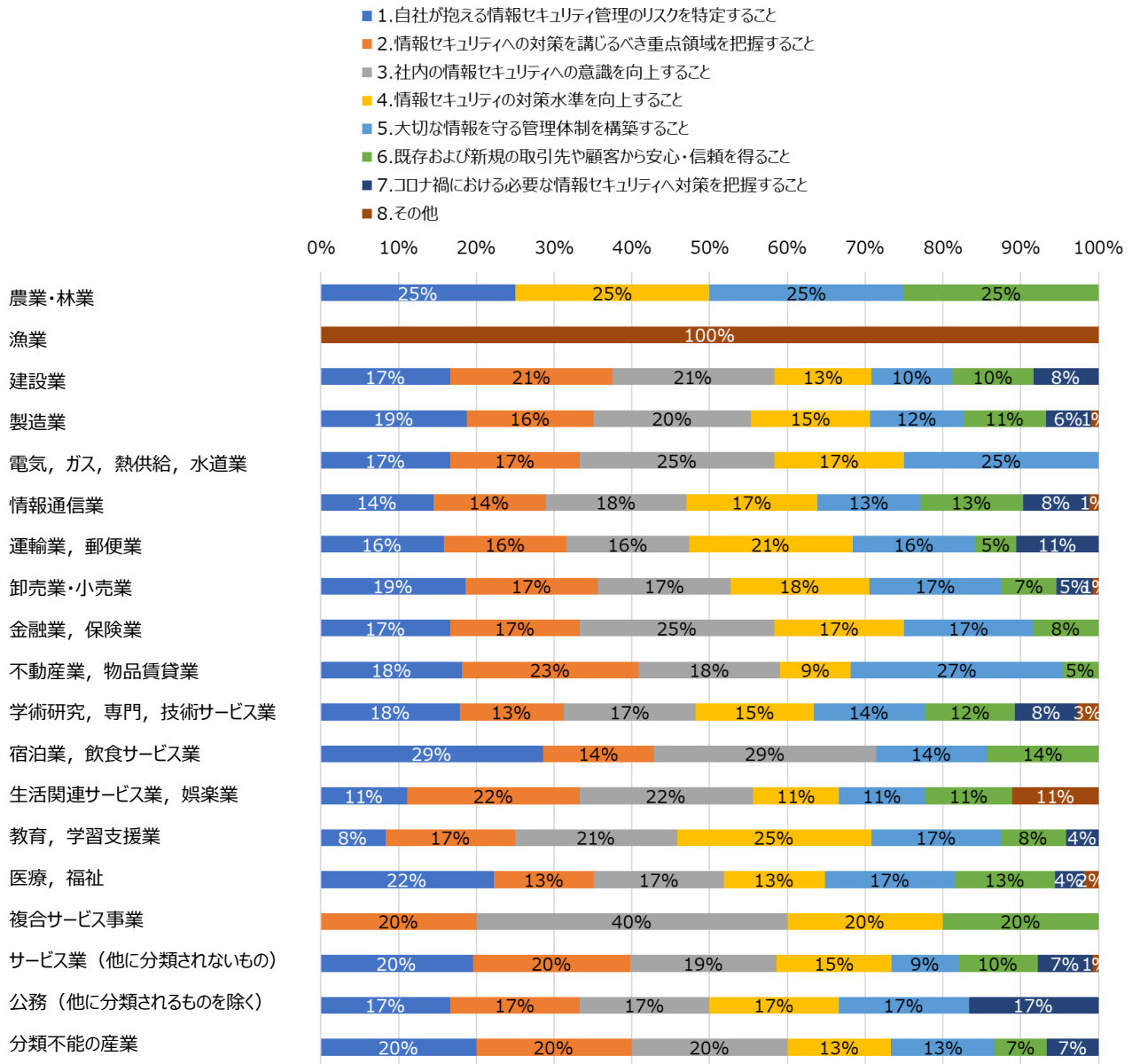


図 35 「事業参加目的」と「業種」のクロス集計

【質問7】 専門家による指導を受けて、情報セキュリティの管理・運用・実践等において成果を得ることができましたか？（択一選択）

回答者の97.6%が今回の指導で成果が得られたと回答し、前年度と同様に指導による成果が確認された。（前年度：96.4%）

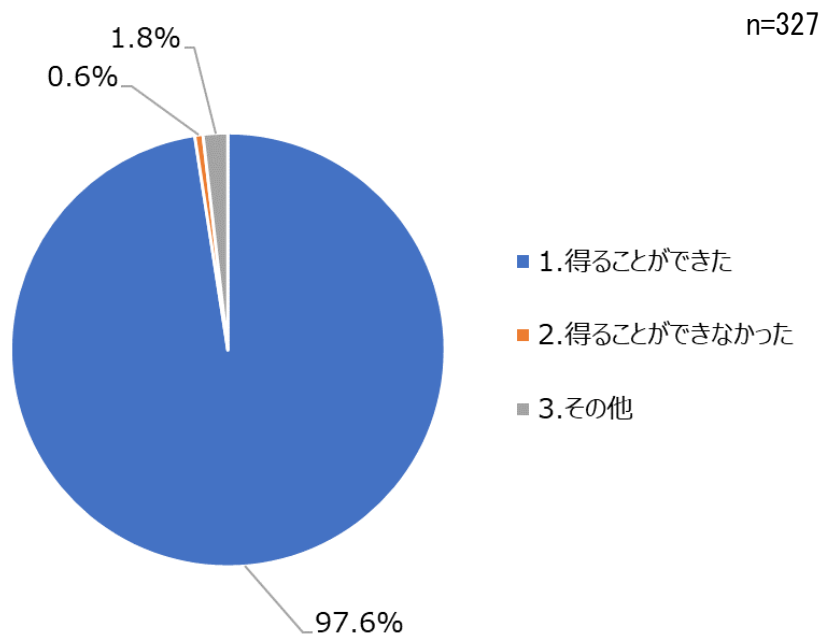


図 36 指導による成果について

「得ることができた」を選択した主な理由

- 情報セキュリティの脆弱部分の洗い出しをすることができ、業態、事業規模、事業取引など自社環境に応じた情報セキュリティへの取組事項を整理することができた。
- 経営陣が「セキュリティ」という言葉に対して、社内での問題を言葉にして数値で評価することで、曖昧でかつ軽視していた状況を改めることができた。
- 社内にセキュリティ対策委員会を設置する事となり、継続的な体制ができた。
- 自社の取組むべき事項が良く分かった。また、社員研修用の資料（動画）紹介やハンドブック作成のアドバイスをもらい、整備するまでに至った。
- 参加したメンバーの情報セキュリティに関する意識が高まり、社内の核となって今後の対策に向け取り組むことができるようになった。
- 指導を受けて自社の手薄なところに気づき、その対応が顧客への PR にもなることに気づいた。

「得ることができなかった」を選択した主な理由

- 専門家の意見が標準的な対策に終始し、当社の現状の引き上げに対する助言がほぼなかった。どうやったら標準的な対策を現実の会社に適用できるかを聞いたかった。

「その他」を選択した主な理由

- 今から実践していく段階で、成果として感じるまでに至っていない。

【質問 8】 訪問指導を実施した専門家に対する所見について教えてください。

【質問 8-1】 専門家の指導力・意欲はいかがでしたか？（択一選択）

専門家の指導力・意欲は、回答者の 95.1%が高かったと回答し、前年度と同様に非常に高い評価を得た。（前年度：93.2%）

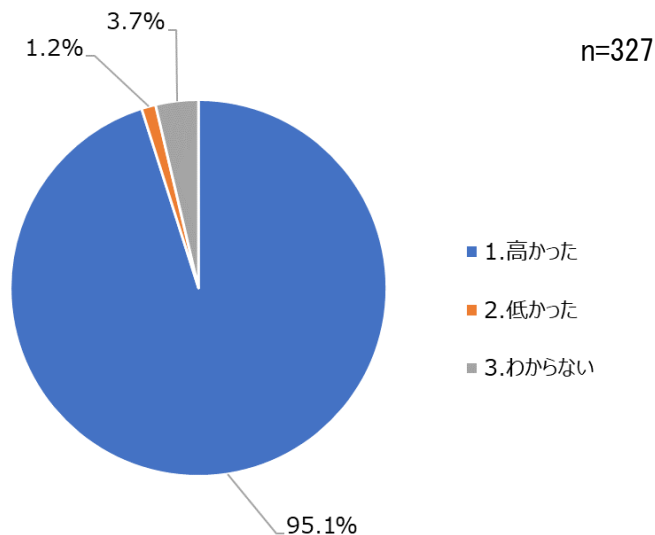


図 37 専門家の指導力・意欲について

「高かった」を選択した主な理由

- 理解度に合わせて丁寧にヒアリングし具体例は出しながらわかりやすく噛み砕いで指導してくれた。また、疑義に対してのレスポンスが極めて速かった。
- コンサル中に生じた不明点などは、常にその日中にフォローしてくださった。弊社が取り組み易い対策を親身になって考え、整理したうえでアドバイスをくださった。
- 当方の気が付かない課題に対しても、他社実例などを交えながら、分かり易く詳細な説明、指導をいただいた。
- 初めて指導されるとのことであったが、専門知識はもちろん質問にも丁寧に答えていただき助かった。物理的な盗聴・盗撮被害も懸念されており、専門知識の枠を超えてアドバイスいただけたことに感謝している。
- 初回で説明した弊社の状況や使用システムで、ご自身が使われたことがないものなども、次回までに仕様を確認していただくなど、意欲的にご対応いただけた。
- 親身になって当社のヒアリングを行った上で費用面や人材面などを考慮して、当社の身の丈に合った情報セキュリティ対策を指導してもらえた。
- 通常の知識伝達にとどまらず、様々な事例を取り上げながら包括的に、かつ団体の内情を鑑みた提案を行ってもらえた。
- 指導担当者は毎回具体的なリスクの実例やそれに派生する出来事まで、多岐にわたる話題を用意していた。わかりやすい知識共有に、参加者全員がセキュリティに対して理解を深めることができた。

「低かった」を選択した主な理由

- 準備不足を感じた

「わからない」を選択した主な理由

- 普通

【質問 8-2】 専門家の知識・専門力はいかがでしたか？（択一選択）

専門家の知識・専門力は、回答者の 91.7%が高かったと回答し、前年度と同様に非常に高い評価を得た。（前年度：92.2%）

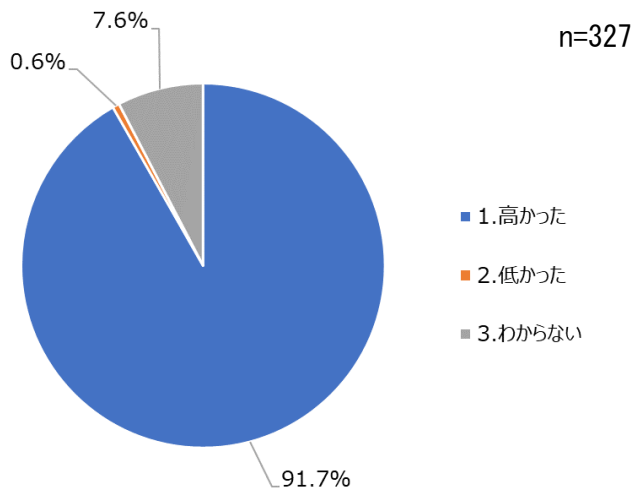


図 38 専門家の知識・専門力について

「高かった」を選択した主な理由

- セキュリティに関して、非常に豊富な知識があり、過去・現在・未来（予測）という時間軸を絡めて、セキュリティ情勢をご説明いただいた。
- ネットワーク、サーバー等幅広い知識を持ち相談にも乗っていただいたから。
- 知識、専門力という点では、我々が日常的に情報収集するより以上の情報をお持ちであり、適宜情報を我々にインプットいただいたので、今後を活用させていただきたい。
- 事件・事事故例をわかりやすく説明してもらえた。技術的な質問、ツールやソフトについても即答してもらえた。
- 実際に利用可能な暗号化装置やソフトを教えていただき、専門家の方の実務経験に裏打ちされた提案をいただいた。
- 弊社のシステム内容の把握も早かった。システム構築に関する知識もあり、たいへん有用であった。ネットワーク図だけでは見えてこない部分も、ヒアリングにより引き出してもらえた。
- 教育現場の情報に詳しく、かつ、質問に対しても要領よく答えてくれた。
- 誓約書などの見本やデータ分析などを提示してもらい、視認化しやすかった。
- 専門用語の使用は最小限であり、初心者にもわかりやすく説明いただいた。
- 情報セキュリティの基本はもとより最新動向についても情報があり、事業規模にあった指導内容で分かりやすかった。

「低かった」を選択した主な理由

- 質問に対する回答が不十分と感じた。

「わからない」を選択した主な理由

- その他の指導者の指導を受けていないため、比較できない
- 個別の技術的質問については、より特化した専門家・知見をひいてくる必要がある。

【質問 8-3】専門家とのコミュニケーションはスムーズでしたか？(択一選択)

専門家とのコミュニケーションに関して、回答者の 97.2%がスムーズだったと回答し、前年度と同様に非常に高い評価を得た。(前年度：97.5%)

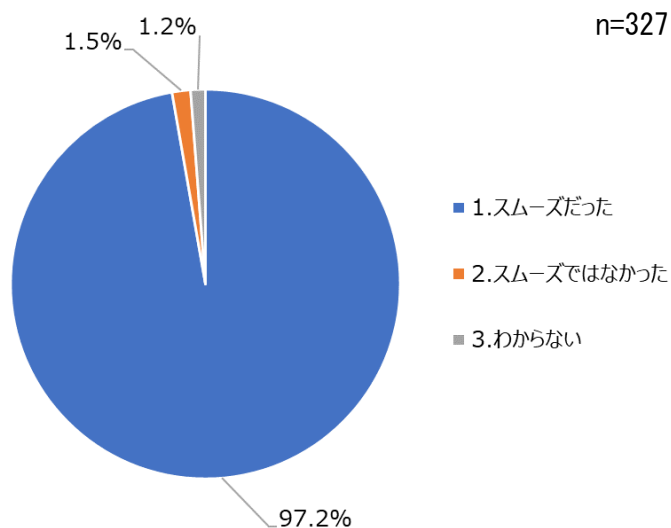


図 39 専門家とのコミュニケーションについて

「スムーズであった」を選択した主な理由

- リモートでの対応に応じてくれて、コロナ禍の環境下でもスムーズに進んだ。
- こちらからの連絡に対するレスポンスが早く、意見を受け入れていただきながらの提案など、非常に話しやすく、密にコミュニケーションがとることができた。
- 堅苦しい雰囲気ではなく、かつ、弊社の身の丈にあった方法を提示していただけたので賛同しやすかった。
- 話し方が明瞭でとても良かった。専門家の人柄が良い。レスポンスも早く、スムーズであった。
- 難しい問題等もユニークな例えで和ませていただいた。
- 講義だけでなく、時事ネタを交えながら楽しく行えた。
- 比較的柔軟にアイデアを出してくださる方で、弊社の特性に非常にマッチし、同席した上層部などもたいへん喜んでいました。
- こちらの意図する事をご理解いただき、又わからない専門用語もかみ砕いて分かり易くご教授いただいた。こちらが抱えている問題点についても話しやすく、とても良いコミュニケーションを取りながらのご指導いただいた。
- こちらのレベルに合わせ、会話や作業の際にやりやすい雰囲気作りしていただけた。
- 体験談などざっくばらんにできた。経営者同士通じるところがある。

「スムーズでなかった」を選択した主な理由

- コロナ拡大により Web 指導がメインとなったが、通信状況が悪かったため。

「わからない」を選択した主な理由

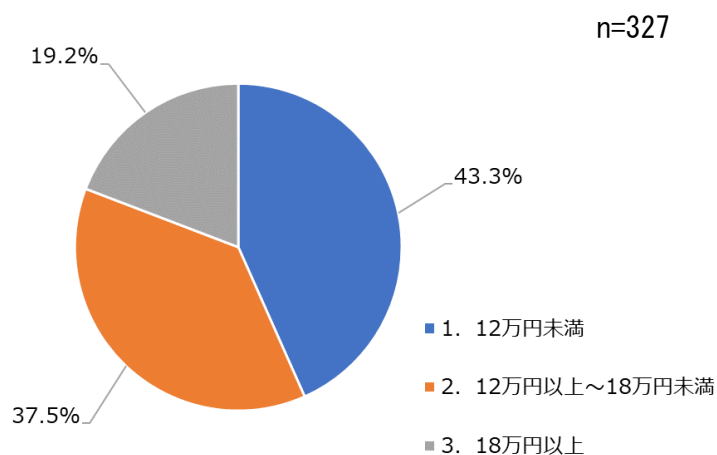
なし

【質問9】情報セキュリティマネジメントの専門家による今回の訪問指導4回の成果に対する対価について、適正と考えられる金額を以下の選択項目よりお選びください。(択一選択)

適正金額の各回答の割合は、12万円未満が43.3%（前年度回答42%）と最も多かったが、12万円以上～18万円未満、18万円以上と回答した企業の合計が56.7%と過半数を占めた。

「訪問指導4回の対価についての回答」と「マッチングにおける専門家指名の有無」とのクロス集計では、18万円以上と回答した回答者の73.8%が専門家を指名した事業者であった。

図 40 訪問指導4回の対価について



「訪問指導4回の対価についての回答」と「マッチングにおける専門家指名の有無」の関連性

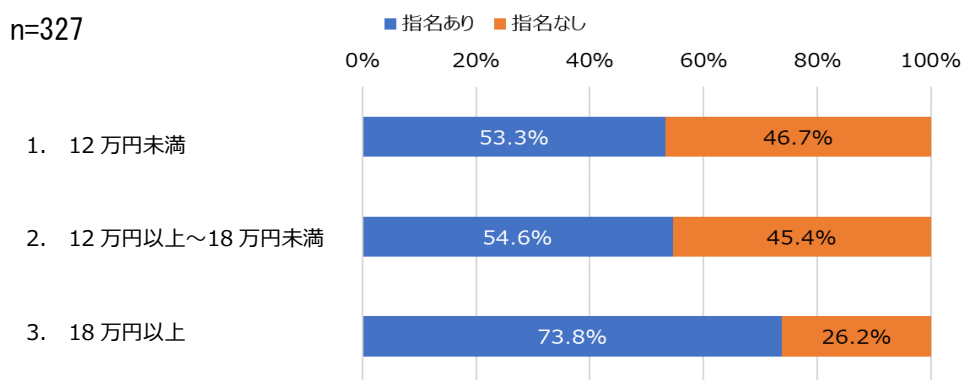


図 41 「適正金額についての回答」と「マッチングにおける専門家指名の有無」のクロス集計

【質問 10】 今回の情報セキュリティマネジメントの専門家による指導を受けて、今後実施すべきとお考えの、情報セキュリティへの取り組みは何ですか？（複数選択）

回答選択肢 1 と 2 の回答数の割合は、約 70~80%を占めている。前年度とほぼ同様であった。今回の指導の成果が一過性で終わらないよう、関連規程や運用ルール等の定期的な改善、見直しが必要と考えている事業者が多いといえる。「情報セキュリティへの取組」と「業種」とのクロス集計からは、特徴的な傾向は見られなかった。

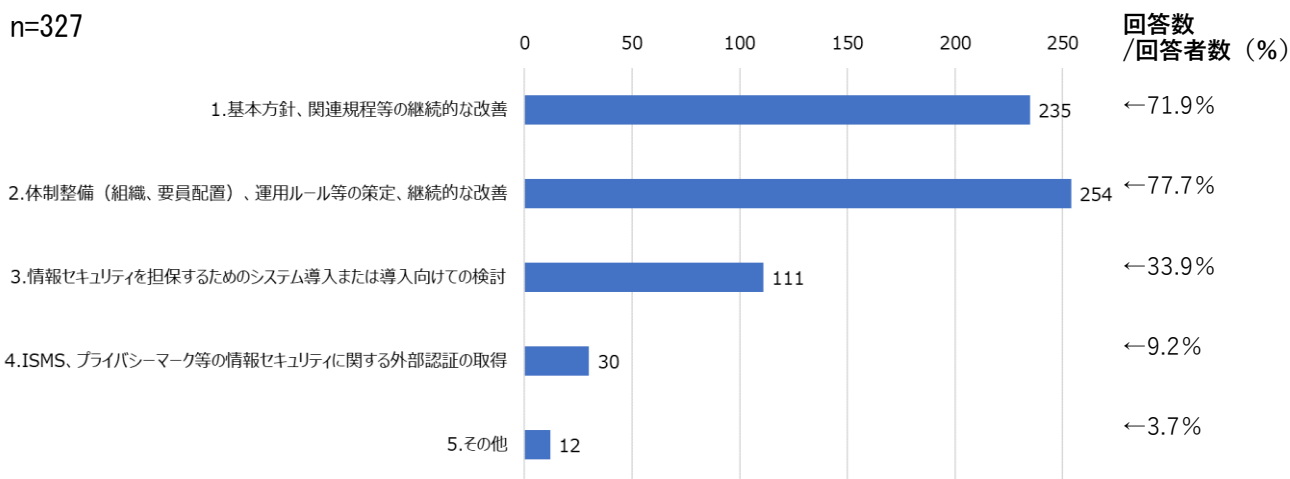


図 42 情報セキュリティへの取組

選択した主な理由

- 関連規程や運用ルール等は、策定後も定期的な改善、見直しが必要と考えているため。
- スタッフの入れ替わりやスキルの差、業務の移り変わり、使用するソフトのバージョンの変更、時代が求めるセキュリティレベルの変化に合わせるため、運用ルール等は定期的にメンテナンスする必要があると感じた。
- 今回策定したルールが画餅にならないような仕組みが必要であり、そのための定期監査を指導者に依頼した。
- 経営者、担当者の意識改善及び策定中方針の実施継続のため。インシデント対応の構築が必要と感じたため。
- 自工会サイバーセキュリティガイドラインへの対応のため。今後、大手企業・取引先からの要求が想定されるため。
- 社内でルール決りを徹底すると同時に、外部に向けても取り組みがアピールできるよう、ISMS 認証等の維持もあわせて行っていきたい。
- システム導入などで運用の負荷低減や改善をするため。
- プライバシーマークとの連携を行うため。
- 教育機関であるので教職員の教育及び意識改革が重要であると感じた。
- 社内ルールの策定が不十分なので、機器等を万全にしたとしても社員が個々に自覚を持たないと、意味がないので関連規程の整備及び指導が必要と考える。
- 弊社を選んでいただくための顧客・潜在顧客への PR 方法を工夫したい。

「情報セキュリティへの取組」と「業種」のクロス集計

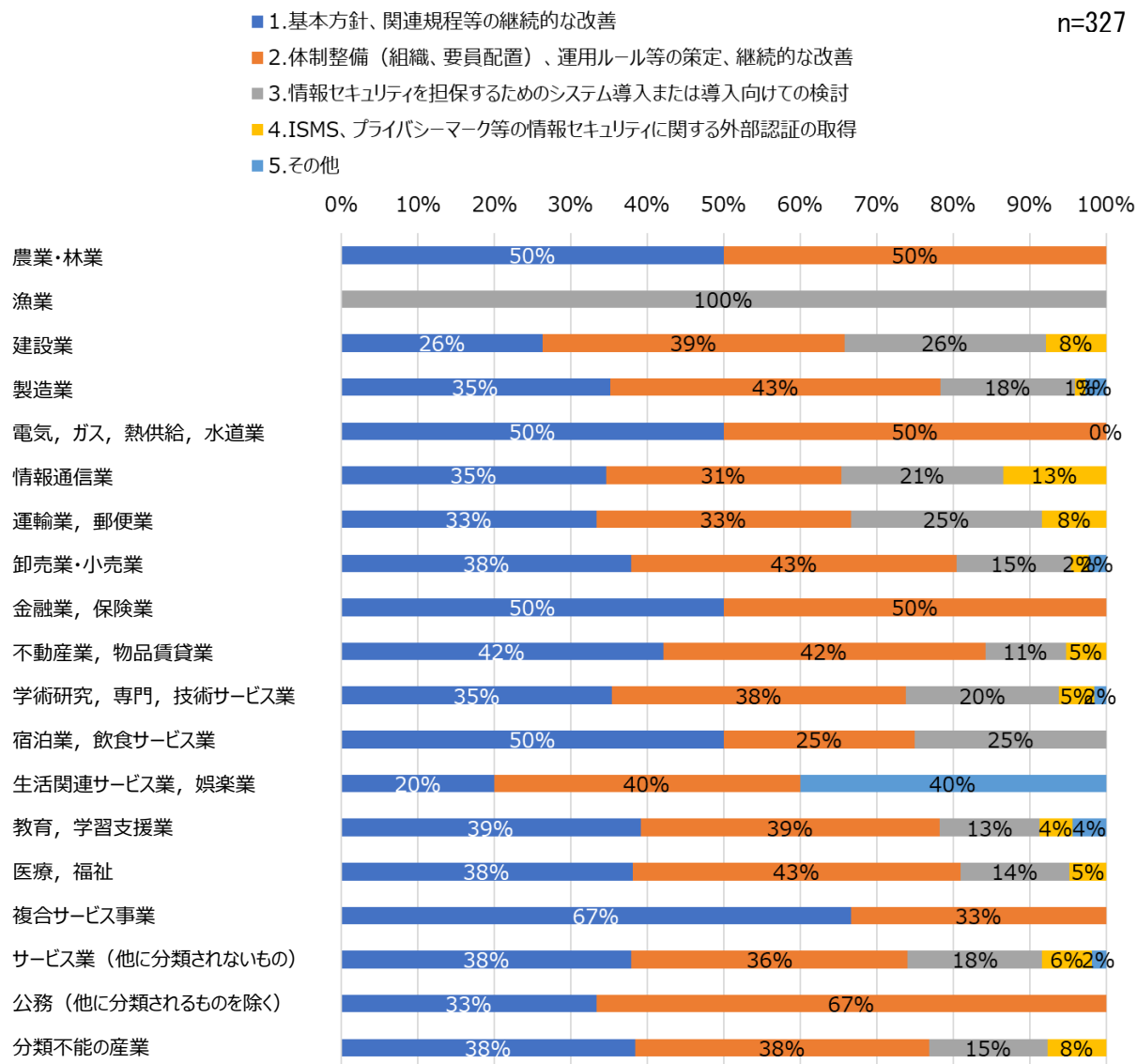


図 43 「情報セキュリティへの取組」と「業種」のクロス集計

【質問 11】 質問 10 を実施するにあたり、情報セキュリティの専門家による指導・支援を希望しますか？（択一選択）

回答者の 41.7%が「1. 一時的な相談等の軽微な支援を希望する」として最も回答が多かったが、「2. 案件ごとのコンサルティング」13.2%、「3. 定常的な支援」8.9%との回答もあり、程度の差はあれ、合わせて 63.8%の指導先企業が継続指導・支援を希望した。

各回答を選択した理由（自由記述）から言える傾向としては、「1. 一時的な相談等の軽微な支援」を選択する企業は、リソース面・コスト面での企業体力に余力がないため、簡易的な相談支援の希望に留まる傾向が見られる。また、「2. 案件ごとのコンサルティング」、「3. 定常的な支援」を選択する企業は、情報セキュリティにおけるリスク・課題及び取り組むべき対策計画（システム導入・認証取得など）が明確になっており、実行に移す準備段階にある傾向が見られる。なお、「希望しない」を選択する企業の多くは、予算確保の困難を理由にあげているが、今回の指導による意識変革をきっかけに、自発的に取り組んでいく意識の高い企業も見られた。

n=327

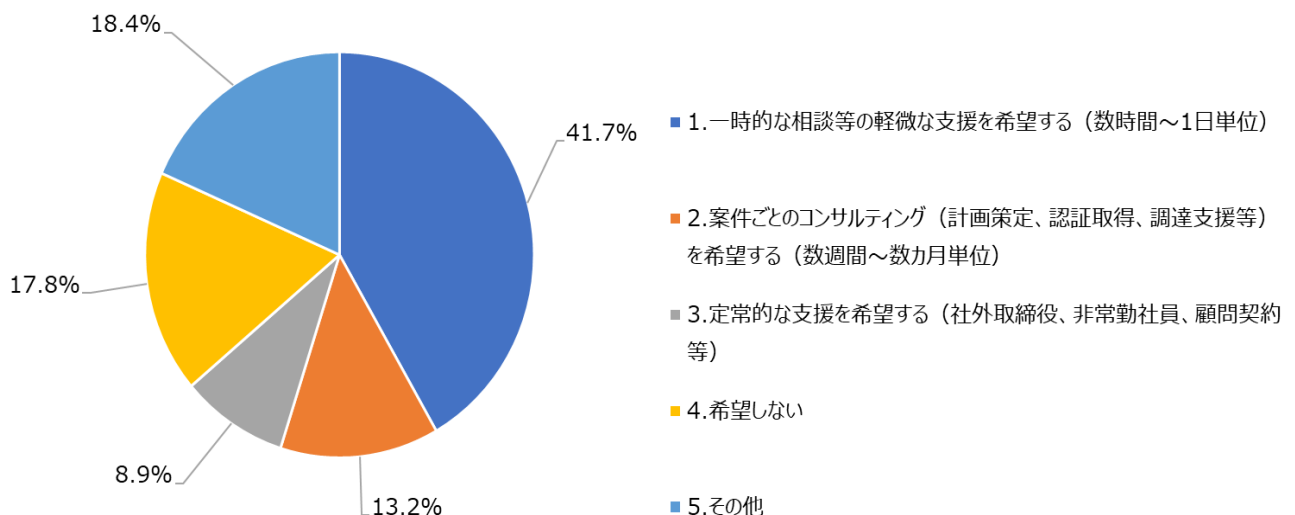


図 44 情報セキュリティの専門家による指導・支援の希望

「1. 一時的な相談等の軽微な支援を希望する（数時間～1日単位）」を選択した主な理由

- 情報セキュリティは、年々、新しい対応方法（常識）が出てくるかと思うので、課題が出てきた際に、相談させていただきたい。
- 情報セキュリティについて気軽に相談できる場所がないため。
- コスト面で専任者を置く企業体力がないので、現行は相談にとどめるしかないのかと思う。
- 実現したい内容に対して相談する相手を見つけるのが難しいので、マッチングするサービスがあれば良いと思う。（例えばセキュリティ向上やアクセス制御を目的とした社内 LAN の構築であるとか）

- セキュリティ関連で問題が発生した時、困った時、迷った時などに、経験・知識豊富な専門家にスピーディでスムーズな解決策、適切なアドバイスを受けたいと考えたため。金額はそんなにかげられないが、簡単に相談できる相手として存在してくれたら便利である。
- その年のセキュリティの潮流を教わり、遅れていないかをまずは数時間～1日の相談で確認する必要がある。その後、対策が必要である場合には案件ごとのコンサルティングが必要になってくるので、まずは定期的な確認のための支援を希望する。
- セキュリティの対策を行っている経過など情報共有していきたい。お互いにフィードバックができるため、お互いに利益があると思う。
- 組織として恒常的な位置付けを確立するために定期的な指導を受けることができればと考える。監査の視点も加えてチェックをしていただきたい

「2. 案件ごとのコンサルティング（計画策定、認証取得、調達支援等）を希望する（数週間～数カ月単位）」を選択した主な理由

- 関連規程を全て完成させるために、また、職員周知を行うために実際にお願ひした。
- 実施計画を策定頂いたので、進捗状況の確認、アドバイスの継続的な指導を希望する。
- 社内に専門的な知識を有する者がいないため、案件ごとに支援を希望。外部の専門家のアドバイスを有効に活用したい。
- 今回のように、国の支援により無料の場合であれば希望する。
- セキュリティ以外の業務を兼務しているので必要な時にまとまった時間で指導してほしい。
- ISMS 認証の取得を目指したいが、ハードルが高く分からないことが多いため。今後の体制構築、認証取得については計画段階であるため未定ではあるが、当社予算都合によりサポートの依頼は検討する。

「3. 定常的な支援を希望する（社外取締役、非常勤社員、顧問契約等）」を選択した主な理由

- ウイルス等の最新危機管理体制を構築したい。不正アクセス等の不安が続いている。
- 専門知識を持った人材の育成又は採用は難しいので、外部の力を借りる必要がある。
- 現に顧問契約を締結する予定。
- アドバイザー的に会社の状況を把握しつつ、1～3か月に1度程度のミーティングを持つなど、情報収集と改善アドバイスをいただける仕組みは是非とも導入したい。
- 今回の指導で多方面のいろんな課題が見えてきたので、都度相談させていただきたい。
- 情報セキュリティ関係のリスクを考えて定常的なご支援（顧問契約等）を希望したいと考えるが、コスト面が気になる。

「4. 希望しない」を選択した主な理由

- まずは弊社内で対応・整備できる事項に着手する。
- それほど予算がない。

- 今回の研修により、当面の運用は自社でできると考えているため。
- 今後は取引ベンダーと具体的に検討を行うため。
- 事業規模が小さすぎるため。今後、事業規模の拡大に伴って検討したい。
- 今回ご指導いただいた内容で、まずは意識改革を進める。そのうえで次のステップに移る段階で、支援を希望することがあるかと思われる。

「5. その他」を選択した主な理由

- 年に1~2回、最新のサイバー攻撃の実例を無料で教えていただければ参考になる。
- 指導、支援はあったほうが良いと思うが、金銭的な面で可能かがわからない。
- コンサルティング料金による。他の診療所での情報セキュリティの経費化のモデルケースが少ない。今後、経費をどれくらい割り当てるべきか、そこがいまのところ判断できない。
- 定期的な社員研修を希望するが、それ以外は、まだ考えが及ばない。
- 情報セキュリティ対策実行計画書に基づいて実施・評価してから判断。
- 自主的な改善を積み重ねて判断していきたいと思う。支援が必要だが、(1) 内部の基本的な教育体制が整っていないため、現時点で支援を受けても効果が上がらない
(2) 内部での優先順位が低く現状では予算が得にくいため。
- 小規模企業でも、気軽に相談できる連絡先がほしい。(過去、トラブルがあったときに IPA の対応だけでは解決に至らなかった)

【質問 12】 オンライン（Web 会議）を利用して専門家による指導を受けた方のみお答えください。
オンラインを利用して専門家による指導を受けての感想をお聞かせください。（択一選択）

オンライン（Web 会議）を利用して指導を受けた指導先企業の 95.8%が、「特に問題なかった」としている。場所、移動時間に捉われない等、指導先企業、専門家の両者にとってメリットがあったと言える。

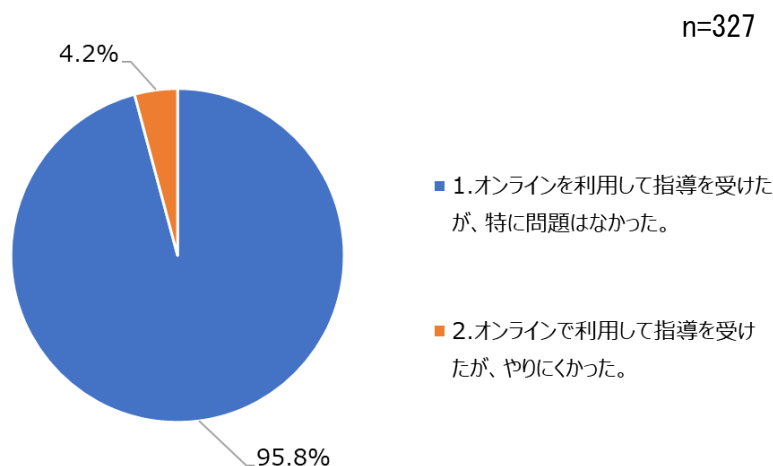


図 45 オンラインを利用した専門家指導を受けた感想

「1. オンラインを利用して指導を受けたが、特に問題はなかった。」を選択した主な理由

- 画面共有しながら音声途切れることもなく、特に問題なかった。ただ、受講者側の問題だが、対面と比べると、受け身で聞く姿勢になりがちだった気がする。
- 弊社は全てオンラインで業務をしているので、この点は特に抵抗はなかった。逆に IPA がオンラインでのコンサルを受容していただいたのが嬉しかった。
- リモート環境下でのコミュニケーションに慣れたため。
- 弊社の回線状況で、重く感じる場面もあったが、特に問題ないと感じた。
- Web 会議ツールを用いて指導を受けたが、特に問題はなかった。ただ、専門家の目で直接状況を見ていただければ、より多くの改善点を指摘してもらえたのではないかと、という思いはある。
- 会社、自宅と場所を変えて試してみたが、快適だった。
- 相互間の移動時間の短縮や、打合せ場所を問わないので非常に便利だった。
- Web ミーティング中心の打合せでしたが、事前に資料に纏めていただき、共有しながら進行して分かり易かった。
- 来訪よりも楽だと思う。日常で Web 会議を積極的に取り入れようと思った。
- 大雪の影響により、1 度だけオンラインにて会議を行った。指導担当者はオンライン用に話がスムーズにできるよう、準備を怠っていなかったように思える。

「2. オンラインで利用して指導を受けたが、やりにくかった。」を選択した主な理由

- 音声聞き取りづらかった。
- 資料の共有を行う際に、主にメールを使用していたため、当日にご覧いただきたい資料を共有する際に不都合があった。

【質問 13】 本事業に対するご意見・ご要望がございましたら、ご自由にお書きください。

回答数 327 件のうち、127 件から自由回答があった。内訳と代表的なコメントを以下に示す。

《好評な意見》 : 104/127 件 (82%)

「指導への満足・感謝」に関する代表コメント (ほか同様コメント 78 件)

- とても有益で、中小企業にとってはとてもありがたい制度と思う。無料で指導いただいたが、有料レベルのクオリティとコミットメントでしっかりサポートしていただき、感謝しかない。
- DX¹¹や働き方改革 (IT 活用) 等の言葉が溢れているが、実施以前にセキュリティの管理をしっかり行うことが大切だと思う。中小企業は IT 担当者が不在の所も多いため、この施策は非常に有効かと思う。4 回の指導は非常にありがたかった。
- 自分でセキュリティに関しての相談窓口を見つけ、価値の分からないものにお金を払って相談することはハードルが高い。今回はセキュリティを考えるうえでとても良いきっかけになった。本当に良い支援策だと思う。弊社の場合は、専門家に見ていただきたいものがたくさんあったのでオンサイトでお願いしたが、オンサイトにこだわる他の支援機関も多い中、オンラインも選べたところが素晴らしいと思う。
- 情報セキュリティマネジメントへの必要性について社内 (経営層) への認識が高まったこと、作業を進めていくうえでの行程が理解できたため、大変参考になった。

「事業継続の要望」に関する代表コメント (ほか同様コメント 19 件)

- 国からの予算が出て専門家の方に指導いただける機会があれば、今後もお願いしたいと思う。中小零細企業には、とても有益な事業だと思う。
- 社員の意識改革に大いに役に立ち、ありがたかった。是非このような窓口を設けてほしい。
- 小規模な企業のセキュリティ向上に資するありがたい支援だった。今後も継続していただきたい。

《不評な意見》 : 6/127 件 (5%)

「指導の期間が短い・余裕がない」に関する代表コメント (ほか同様コメント 3 件)

- 実施期間が 2 か月程しかなかったため、日程調整が難しかった。他の業務もあるので、もう少し期間に余裕が欲しいと感じた。

「指導者への不満」に関する代表コメント (ほか同様コメント 1 件)

- 専門家の質や、指導内容について、もうちょっと整理したうえで実施してほしい。現在の内容では、専門家の事前準備に非常に左右されてしまう。

¹¹ DX(デジタルトランスフォーメーション): IT の活用を通じて、ビジネスモデルや組織を変革し、競争上の優位性を確立すること。

《その他》 : 17/127 件 (13%)

特徴的なコメント

- より多くの企業が支援を受けることで、セキュリティアクション二つ星宣言企業が増え、自己宣言ではなく、認定制度になる様な取り組みを期待する。知名度がまだまだ低いと思われるため、知名度向上をお願いしたい。
- セキュリティ対策講義や指導を受講した修了書が欲しい。賞状形式で、もらえれば社内や応接室へ掲示し、会社の取り組みを社内外に公表でき、取り組みをより目に見える形で知らしめられると考える。
- 中小零細企業では情報セキュリティ対策について、相談できるところがほとんど無いか、知られていないように思う。そのため、恐怖心から不必要に高額な設備をメーカーから言われるまま導入し、分からないから IT 化やクラウド化はできる限り避けるというような判断をしているケースもあると感じる。自社に必要な情報セキュリティ対策を体系的に理解し、優先順位をつけて知りたいというニーズは多いと思う。
- コロナ禍でなければセミナーや集団教育など、他社との接点を得られたらよかったと思う。自社の悩みや問題を共有しつつ、他社がどのように取り組んでいるのか、ベンチマークができる機会になればと思う。

(3) 指導先企業アンケートまとめ

アンケート全体を通して、情報セキュリティマネジメントに関する指導内容、指導成果及び専門家に対して、回答者の 95%前後が非常に高い評価をしている。指導への満足・感謝に関連する自由記述コメントが、コメント総数 127 件中、104 件 (82%) と多く、本事業が一定の成果をあげた裏付けとなった。

指導内容・指導成果に対する高評価の主なポイントとしては、「業態、事業規模、事業取引など自社環境に応じた情報セキュリティ取組事項の整理」、「基本方針を外部発信及び二つ星の宣言」、「経営陣はじめ職員メンバーの情報セキュリティに関する意識の高まり」等があげられる。

専門家に対する高評価の主なポイントとしては、「指導力・意欲」の点では、理解度に合わせた丁寧なヒアリング、他社実例などを交えた分かり易い詳細な説明、内情を鑑みた提案など、「知識・専門力」の点では、ネットワーク、サーバー、ツール・ソフト及びシステム構築に関する有用な専門知識、実務経験に裏打ちされた専門力、情報セキュリティの基本・最新動向に関する豊富な知識など、「コミュニケーション力」の点では、レスポンスの速さ、話し方が明瞭、レベルに合わせた会話や作業しやすい雰囲気作りなどが回答者からあげられた。

また、事業継続を望む声も自由記述コメントも 22/127 件 (17%) あり、支援を望む声が一定数あると推定される。無料であれば是非参加したいとの意見も散見された。

7.2. 専門家（登録セキスペ（RISS））アンケート

指導専門家として登録し、実際に指導先企業とのマッチングが成立した指導専門家のうち、登録セキスペ（RISS）のみを対象に、本事業に参加したことの意義や今後の活動の方向性についての意識調査をアンケート形式で実施した。

(1) 専門家（登録セキスペ（RISS））アンケート概要

実施期間：2020年12月15日（火）～2021年1月29日（金）

対象者：指導先企業とのマッチングが成立した登録セキスペ（RISS）

回収率：98.3% 配布数180人 回収数177

(2) 専門家（登録セキスペ（RISS））アンケート結果

【質問1】本事業への参加によって、あなたが得られたことを教えてください。（複数回答）

登録セキスペ（RISS）の指導専門家のうち、97.2%とほぼ全員が「登録セキスペ（RISS）としての実績」を事業参加の成果として捉えている。「スキルアップが図れた」という回答も多く、スキルと経験を磨く良い機会になったことが伺える。一方で「顧客開拓となるコネクションができた」との回答は37.3%で、今後の登録セキスペ（RISS）の自走化に向けての課題が確認できた。

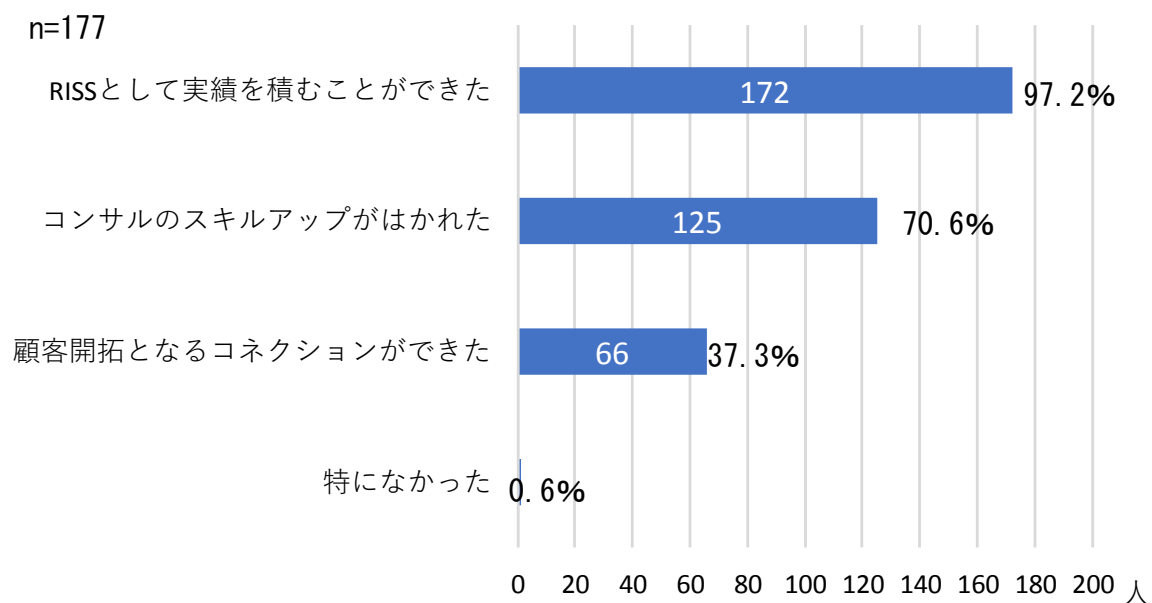


図 46 本事業に参加して得られたこと

【質問 2】これまでに本指導業務(前年度も含む)以外に、同様の業務(コンサルティングやアドバイス)と
いった経験や実績はありますか？

指導専門家の登録セキスペ (RISS) のうち 35.0%のが、これまでに自身でコンサルティングを行った経験がなかったことがわかった。経験が「ない」と回答した登録セキスペ (RISS) からは、今回の経験を活かして次のような前向きな意見もみられた。

- 中小企業の実態の一例をよく知る事ができた。自身の勤務先での活動において、有用なバックグラウンドとする事ができると考えている。
- 指導した企業に対して継続して関わっていければと思っている。
- マネジメントシステムを構築するにあたり、作業段取りや進め方がわかるようになった。

n=177

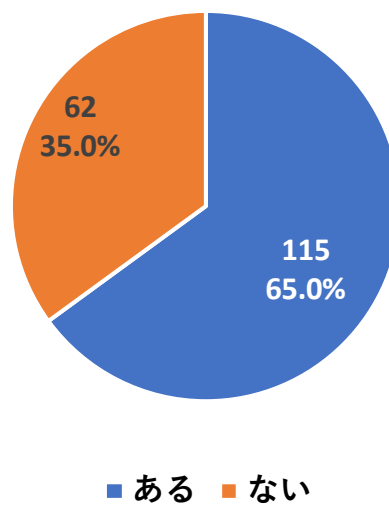


図 47 本事業以外でのコンサル経験

【質問 3】今後の 3 年間で、どのように RISS の資格を活かしていきたいですか？

今後の登録セキスペ（RISS）資格の活かし方については、「起業して独立しており、売上拡大に活かしたい（31.6%）」、「自身による起業に役立てたい（14.7%）」と合わせて 46.3%が独立コンサルタントとして資格を役立てたいとしている。

また、「退職後のセカンドキャリアに活かしたい（10.7%）」という回答や、その他回答として、「副業として活用したい」、「副業の幅をひろげたい」という副業に関する意見が多くあったことから、働き方が多様化する中で、本業の仕事にプラスした収入手段として登録セキスペ（RISS）資格を活かしたいと考える方がいることが確認できた。

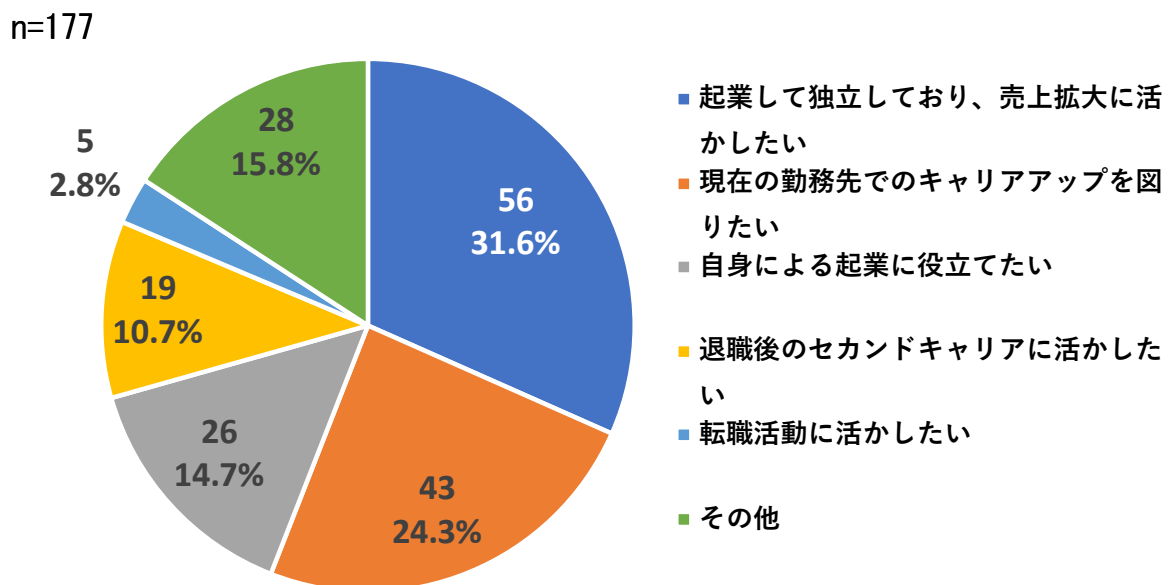


図 48 今後の登録セキスペ（RISS）資格の活かし方

【質問 4】あなたは、RISS(資格)を武器に中小企業を対象とした有償の支援サービスによって、継続的なビジネスにつなげていくことが可能だと思いますか？

登録セキスペ（RISS）による、中小企業を対象とした有償化ビジネスの可能性については、「可能だと思う」という回答が 37.3%あったもの、「難しいと思う」という回答も 45.2%あった。「難しい」と回答した理由については、「登録セキスペ（RISS）知名度や有効性が広く知られていない」とのコメントの他、「中小企業では情報セキュリティはコストという意識が強い」、「中小企業のコスト面の負担が大きい」など、中小企業側のコスト的な課題についても挙げられた。

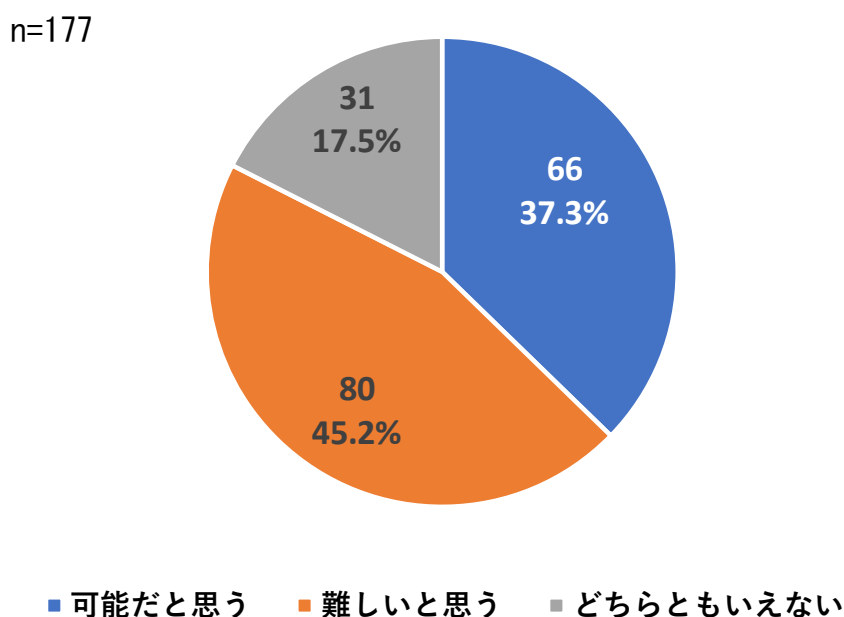


図 49 登録セキスペ（RISS）による有償支援ビジネスの可能性

(3) 専門家（登録セキスペ（RISS））まとめ

今回専門家登録した登録セキスペ（RISS）のうち、35.0%が、指導（コンサルティング）の経験がないという状況だった。本事業への参加によって、97.2%が「実績を積むことができた」と回答していることから、本事業のように、登録セキスペ（RISS）の実績を積む機会を提供する支援策の必要性が明らかになった。

有償による支援サービスの実現には、「難しいと思う」と回答も相当数あり、「難しい」理由としては、「登録セキスペの知名度や有効性が広く知られていない」、「中小企業のコスト面の負担が大きい」とするコメントが多かった。また、本事業が「顧客開拓となるコネクションができた」とする回答が 37.3%にとどまったことを考えると、登録セキスペ（RISS）の知名度向上と中小企業向けの顧客開拓の促進が、有償による支援サービスの実現の課題であると言える。

7.3. 指導先企業へのヒアリング調査

(1) 指導先企業ヒアリング調査の実施

指導先企業へのアンケートの中から、中小企業等にとって参考となる取組みを抽出して、指導先企業 8 社に対するヒアリング調査を実施した。ヒアリング調査は、当該指導先企業の指導を担当した専門家と連携して、専門家も同席のうえ、全てオンラインにて実施した。ヒアリング調査の概要を「表 20 事例ヒアリング調査先一覧」に示す。

ヒアリング調査結果は、今後の中小企業のセキュリティ向上、並びに登録セキスペ（RISS）の指導力向上に役立てることを目的に、「セキュリティマネジメント指導事例集」（別紙 2 参照）として取りまとめた。

表 20 事例ヒアリング調査先一覧

No.	地域	企業・団体名	業種	指導専門家 (敬称略)	事例集タイトル
1	新潟県	株式会社 鈴木コーヒー	卸売・小売業	武内 正一郎	小売・卸売業の EC と DX 推進に伴うセキュリティ対策の強化
2	東京都	株式会社 primeNumber	IT サービス業	村瀬 一志	事業拡大を見据えた情報セキュリティ対策の強化
3	東京都	小津社会保険 労務士事務所	社会保険事務	村瀬 一志	業務の IT 化に伴う個人情報管理の改善
4	愛知県	名東技研株式会社	技術サービス業	一ノ瀬 誠	派遣先で業務を行う社員の情報セキュリティ教育
5	岡山県	倉敷商工会議所	商工会議所	大久保 茂人	会員事業者の機密情報を扱う責任を再認識
6	岡山県	社会福祉法人 天成会	福祉サービス業	大久保 茂人	医療・福祉業におけるプライバシー情報の適切な管理
7	広島県	株式会社ナガト	製造業	瀧川 智昭	サプライチェーン上の必須要件となる情報セキュリティ対策
8	大分県	株式会社九州機設	技術サービス業	深水 伸二	情報セキュリティの実装には対外的宣言が重要

(2) 指導先企業ヒアリング調査の結果

指導先企業 8 社へのヒアリング調査の結果について、「本事業へ参加動機」、「セキュリティ上の課題」、「専門家指導のポイント」、「指導先企業からみた成果」の観点から概要を以下に示す。

【事例 No.1 鈴木コーヒー（新潟県、卸売・小売業）】

－小売・卸売業の EC と DX 推進に伴うセキュリティ対策の強化－

[本事業へ参加動機]

事業の生産性を高めるため、オンラインストアの構築や受発注業務の電子化等、経営者として DX を強力に進めてきたが、情報セキュリティ対策が十分かどうか不安があった。

[セキュリティ上の課題]

DX 推進にあたり、これまでシステムやデバイス導入を優先してきた。また、BYOD も導入していたが、社員のセキュリティ意識に個人差があるので、教育等の対策の必要性を感じていた。

[専門家指導のポイント]

業務で活用する IT 全般（無線 LAN、パソコン、業務利用して良い個人所有デバイスの条件など）について、利用ルールが未整備であったため、網羅的に整備するよう指導を行った。

[指導先企業からみた成果]

今回の指導を受けて、問題の可視化と整理が非常に役立った。策定したルールの遵守について、実行施策を担う IT・セキュリティ担当者を配置することにした。

指導専門家の方は、情報処理安全確保支援士に加え、IT コーディネータとしての知見も保有されているため、今後も IT の活用や情報セキュリティに関して継続した支援を依頼した。

【事例 No.2 株式会社 primeNumber(東京都、IT サービス業)】

—事業拡大を見据えた情報セキュリティ対策の強化—

[本事業へ参加動機]

事業拡大に向けてエンジニア以外の人材確保も必要な中、上場企業ではどのようなセキュリティ対策を行っているのか、将来の自社の上場可能性も見据えて情報を得ておきたいと思った。

[セキュリティ上の課題]

これまではセキュリティに関しても一定の知識を有しているエンジニア系社員ばかりだったが、社員や拠点を増やしていくことを考えた場合に、このままで良いのか不安を感じていた。

[専門家指導のポイント]

テレワークが増えることも踏まえ、事故を防ぐための具体的な教育テキスト（マニュアル）などを新たに整備し、社員教育を充足することで、社員の意識向上を図るよう指導を行った。

[指導先企業からみた成果]

人や拠点が増えていく場合でも、クオリティを保ったまま情報セキュリティ対策を行っていくにはどうしたらよいのか、具体的な情報を得ることができ、役職員の認識が深まった。

有用なものであれば有償でもよいので、社員への情報セキュリティ教育をスポット的に専門家に依頼することを検討したい。

【事例 No.3 小津社会保険労務士事務所(東京都、社会保険事務)】

—業務の IT 化に伴う個人情報管理の改善—

[本事業へ参加動機]

給与計算等の委託のため個人情報を預かっているが、事務所として IT 化が進み、クラウドサービスも活用する中、現状のままで本当に大丈夫なのか、第三者に確認してもらいたかった。

[セキュリティ上の課題]

クラウドサービスを活用するようになり、業務用パソコンもセキュリティ対策したものを支給しているが、最近はテレワークすることも多く、運用面での不安は感じていた。

[専門家指導のポイント]

クラウドサービス利用の場合は、データにアクセスするためのアカウントとパスワードの管理が重要だが、所内では同じアカウントを共有利用していたため、運用ルールの改善を指導した。

[指導先企業からみた成果]

コロナ禍によって、顧客企業のテレワークが増え、在宅からの情報アクセスに関する規程等を含めた就業規則の改訂相談が増えている。今回受けた指導は、本来業務にも活かすことができそうである。顧客からは社労士の仕事以外の相談を受けることもあり、同じ士業として、情報処理安全確保支援士を紹介する機会もあると考えている。

【事例 No.4 名東技研株式会社(愛知県、技術サービス業)】

－派遣先で業務を行う社員の情報セキュリティ教育－

[本事業へ参加動機]

社員は中途採用者が多く、情報セキュリティ意識や知識にはバラツキがあり、社内の情報セキュリティに関する体系的な管理・教育が整備できていないため、本事業に参加した。

[セキュリティ上の課題]

昨年、社員が派遣先のルールに基づくテレワーク中に、セキュリティ事故を起こしてしまった。会社としては、体制整備と社員への情報セキュリティ教育が必須だと感じた。

[専門家指導のポイント]

人材が大きな経営資源となっている業態なので、取引先との情報のやり取りに重点を置いたセキュリティルールを策定し、全従業員への教育によって徹底を図るよう指導した。

[指導先企業からみた成果]

セキュリティ事故を発生させないための業務上必要なルールの策定や教育体制が整った。事故発生時のエスカレーション体制も規程に盛り込み、万が一の事故発生時にも備えができた。指導成果を受けて、策定したルールが定着していくよう社員教育の強化を図り、会社としてさらにお客様からの信頼を得るために、PマークやISMSの取得を目指して推進していきたい。

【事例 No.5 倉敷商工会議所(岡山県、商工会議所)】

－会員事業者の機密情報を扱う責任を再認識－

[本事業へ参加動機]

専務理事から、電子メールの添付ファイルのパスワード設定運用について問われ、セキュリティ対策ができていないことに気づき、本事業が商工会議所も支援対象となることから参加した。

[セキュリティ上の課題]

会員事業者との補助金関係のやり取りを電子メールの添付ファイルで行うことが増えたが、申請書に企業の機密情報も含まれていながら、電子メールの運用ルールを設けていなかった。

[専門家指導のポイント]

商工会議所では職員にテレワークを導入する可能性も検討していたことから、テレワーク導入も見据えた関連規程の整備をターゲットにして、セキュリティ対策の実行計画を立案した。

[指導先企業からみた成果]

今回の指導で、機密情報の定義を整理し、紙と電子の機密情報を扱うにあたって必要なルールが明確になったので、次のステップとして職員に教育・啓発していきたい。

言行一致の活動から、会議所の会員である中小企業経営者に、情報セキュリティの重要性についてもっと啓発していくべきと気付いた。必要に応じて情報処理安全確保支援士を紹介したい。

【事例 No.6 社会福祉法人天成会(岡山県、福祉サービス業)】

－医療・福祉業におけるプライバシー情報の適切な管理－

[本事業へ参加動機]

職員には個人情報等の保管場所に気を付けるよう周知していたが、パソコンに入力された情報の取扱いはあまり意識していなかったところ、運用上の対策強化の勧めを受けて参加した。

[セキュリティ上の課題]

入所者や家族に関するプライバシー情報(家族関係、生い立ち)等は、職員には外で口外しないよう戒めてはいたが、聞き取りメモ等の取扱いが曖昧で、個人の意識任せとなっていた。

[専門家指導のポイント]

現状診断の結果、職員のセキュリティ意識にバラツキがあった。このため、情報の取扱いについて全職員が同じ認識で対応が図れるよう、機密性のレベル付けによる台帳管理を指導した。

[指導先企業からみた成果]

台帳管理により、個人情報管理をより厳格に実行できるようになった。また、職員への教育は、各リーダーにセキュリティ管理の業務を持たせて組織として意識を高めるようにしたい。現在、介護記録の電子化も進めていることから、IT化の推進も含めて情報処理安全確保支援士に相談して進め、定期的なリスクチェックもお願いしたい。

【事例 No.7 株式会社ナガト(広島県、製造業)】

—サプライチェーン上の必須要件となる情報セキュリティ対策—

[本事業へ参加動機]

取引先の手動車メーカーから、定期的に当社がどのようなセキュリティ対策を行っているのか問合せを受けていた。取引先に信頼してもらうため、対策強化の必要性が生じていた。

[セキュリティ上の課題]

業務部は業務が幅広く、離れた9か所の工場のセキュリティ管理がなかなか行き届かない。情報セキュリティ知識のない従業員の行動に、情報漏洩リスクがあるのではないかと感じていた。

[専門家指導のポイント]

現場目線で取組めるセキュリティ対策の検討を進め、改善項目は緊急度、重要度、難易度の観点から点数化して、優先順位が分かるように実行計画を作成した。

[指導先企業からみた成果]

どこから手を付けてよいかわからなかったが、社内体制と現場対策の両面の課題が明らかになり、また、対策の優先順位を付けてもらったので、トップとボトムの両輪でセキュリティ対策を本格的に推進する風土ができた。本事業の次のステップとして、対策の実行度合いを専門家が監査してくれるような支援事業があればありがたい。

【事例 No.8 株式会社九州機設(大分県、技術サービス業)】

—情報セキュリティの実装には対外的宣言が重要—

[本事業へ参加動機]

IT化専任者が中途採用で入社し、本事業を知って参加した。経営者にセキュリティ対策の重要性をより理解してもらうためにも、外部の指導は良い機会になると考えた。

[セキュリティ上の課題]

セキュリティに関する物理的な面では対策を行っていたが、会社としてのポリシーや規程が整備できていなかった。対外的にポリシーを示すことが、取引先への信用上必要と感じていた。

[専門家指導のポイント]

担当者が感覚的に捉えていた課題について、外部の目で見える化して経営者に示し、課題共有を図ることで、会社として情報セキュリティ体制強化を進めるよう指導を行った。

[指導先企業からみた成果]

事業で提示されていた標準的なカリキュラムによって、基本ポリシー、関連規程の整備といった成果物がまさに求めていた成果で、必要だったものが全て揃えることができた。「会社として宣言」これができたことがとても重要だった。経営者の情報セキュリティに対する理解が深まったことも、対外的な信頼の向上につながると考えている。

(3) 指導先企業ヒアリング調査のまとめ

指導先企業8社へのヒアリング調査を通して共通していたことは、「物理的な対策にはある程度配慮しているが、運用面での対策には不安がある」ということであった。専門家の指導事例の中で

は、「5分でできる自社診断」を活用して、運用上のどこにリスクがあるのか見える化し、対策と実行計画の作成を支援したものもあり、指導先企業が感じていた不安を解消していた。

また、企業や団体としてのセキュリティ基本方針（ポリシー）を作成して公表し、取組みを宣言するにあたっては、担当者がボトムアップ的に対策を講じているような場合では、外部の専門家の視点で現状のリスクを明らかにすることは、経営トップの理解を得るためにも有効であることが事例により明らかになった。

指導事例に協力した企業・団体のうちいくつかは、指導を担当した登録セキスペ（RISS）に引き続き有償での支援を求める声があり、いかに専門家が人的にも技術的にも、指導先企業の信頼を得る指導を行ったかがうかがえた。

8. 中小企業向けの伴走型支援サービス検討のための関係調査

8.1. 調査の目的

中小企業等では、一般的に人的リソースが不足していることにより IT 専任者がいる割合が低く、日常的なセキュリティ対策に取り組むことができていない企業が多い。そこで、人的リソース不足を補うためには、外部専門家による伴走型支援サービスの活用検討と普及促進が望まれるが、その中においても、セキュリティに係る最新の知識・技能を備えた専門人材である登録セキスペ (RISS) の活用機会の創出が課題である。

本調査は、登録セキスペ (RISS) を活用した中小企業向けの伴走型支援サービスの検討に関する必要な情報として、都道府県、政令指定都市、及び県庁が所在する市が行う中小企業向け専門人材派遣支援事業について文書調査を実施し、それらの自治体事業の支援策の中で、登録セキスペ (RISS) の活用の可能性について考察を行った。

8.2. 自治体事業調査の方法

① 調査対象の自治体

以下の自治体（総計 121 自治体）を対象として調査を行った。

- 道府県：46 道府県
- 道府県庁所在地：46 都市
- 東京都：1 都
- 特別区：23 区
- 県庁所在地でない政令指定都市：5 都市

② 対象事業及び文書調査の方法

調査対象の自治体ホームページから、中小企業支援を対象にした事業で、「専門家派遣」、「相談窓口」、「働き方改革支援」といったキーワードにより事業の抽出を行った。なお、自治体単独事業のみを対象とし、国の施策として実施している「よろず支援拠点」や、商工会連合会等の事業などは含めないこととした。

③ ピックアップした事業の分類

ピックアップした事業について、以下の基準で分類を行った。

- ◎… 支援や相談内容に「情報セキュリティ」が明示されている事業
- … 支援や相談内容に IT 関連のメニューが含まれている事業
- △… IT 関連のメニューは明示されていない経営改善支援事業
- ×… 支援領域が限定、又は支援が補助金等の支給のみの事業

④ サンプル自治体への状況確認

分類結果のうち、特に登録セキスペ（RISS）の活躍の場として適正が高いと想定した◎の事業について、所管組織に支援事業の状況や、登録セキスペ（RISS）の活用の可能性について電話によるヒアリングを行った。

8.3. 自治体事業調査の結果

(1) 文書調査の結果

調査の結果、121自治体における状況は以下のとおりとなった。

該当する事業のなかった自治体 46 （内訳：3 県 43 市区）

抽出事業数 99 件 （75 自治体）

抽出した事業を前述の事業分類基準で 4 つのカテゴリーに分類し、分類ごとに考察を行った。

表 21 文書調査結果の考察

事業の分類	調査結果の考察
◎に分類した事業 (4 件)	<ul style="list-style-type: none"> 支援内容の対象となる課題の例示として、「情報セキュリティ」が明示されている。実際に派遣されている専門家がどの資格保有者かは不明であるが、登録セキスペ（RISS）が十分に対応可能な事業と考えられる。
○に分類した事業 (61 件)	<ul style="list-style-type: none"> 都道府県、市区ともに直接事業を実施している自治体は秋田県と東京都のみで、ほとんどが公益財団法人等を通じてサービス運営を行っている。 公益財団法人で行っている事業は、多くが専門家派遣事業で、業務への IT 導入に取り組む中小企業の課題解決の支援も行う事業のため、◎に分類した事業同様に情報セキュリティ分野の参入も十分に可能性がある。派遣する専門家として、IT コーディネータ（ITC）が含まれていることが多い。 ただし、支援内容の対象となる課題の例示として「IT 導入」、「ICT の活用」といった用語はあるが、「情報セキュリティ」、「サイバーセキュリティ」という用語が使われておらず、経営課題のキーワードとして明示がない。 東京 23 区では、荒川区、新宿区、品川区が直接の専門家派遣事業を行っているが、その他の区は単独事業は行っておらず、公益財団法人東京都中小企業振興公社の専門家派遣事業を利用する中小企業助成金支援を行っている場合が多い。
△に分類した事業 (15 件)	<ul style="list-style-type: none"> 支援メニューに「IT 導入」は明示されていないが、中小企業の様々な相談を受け付けて、相談に応じている。 ワーク・ライフ・バランス支援アドバイザー（働き方の改善）や、テレワーク導入支援アドバイザーの派遣など、直接的ではないが、IT 導入やセキュリティにも影響のあるテーマで事業が行われている。
×にした分類事業 (19 件)	<ul style="list-style-type: none"> 支援対象分野に限定があるため、その事業そのものに参入することは不可。 ものづくり支援に関連して、「IoT 等専門家派遣事業」（栃木県）、「IoT コーディネータ派遣事業」（新潟県）等があり、IoT（Internet of Things）や AI 等の新しい技術領域の専門家派遣が単独で事業化されている。

(2) サンプル自治体に対するヒアリング調査の結果

抽出した事業のうち、支援や相談内容に「情報セキュリティ」が明示されている◎に分類した4事業を実施している自治体に対して、電話にてヒアリング調査を行った。4事業（3つの自治体）の支援内容の概要を以下に示す。

表 22 ◎に分類した事業のサマリ

自治体及び運営主体	事業名	支援内容
千葉県 商工労働部 雇用労働課 働き方改革推進班	令和2年度テレワーク導入支援	新型コロナウイルス感染防止対策として、新規にテレワークの導入を希望する中小企業等を対象に、専門家を派遣し、テレワークの社内試行を支援する。
東京都 産業労働局商工部内 Tcyss 事務局	サイバーセキュリティ相談窓口	サイバーセキュリティに関する無料相談窓口を開設し、対策の強化や情報流出事案、セキュリティポリシーの策定、セミナーの開催等に関する相談を受付けている。
東京都 産業労働局商工部経営支援課 (NTT 東日本 (株) 受託運営)	中小企業サイバーセキュリティ向上支援事業	コロナ禍を機に中小企業によるオンラインの活用が一層進むことを踏まえ、中小企業の自立的なサイバーセキュリティ対策につなげる支援を実施。(100社程度を対象とする)
京都府 公益財団法人京都産業 21	専門家派遣	経営の向上を目指す意欲のある中小企業者や創業者が抱えている経営・技術等の諸問題に対して、幅広い分野の民間専門家が相談や診断助言を行う(専門家派遣対象メニューとして「情報セキュリティ」を明記)

東京都及び千葉県では、コロナ禍によるテレワーク（オンライン）の活用増加に伴う情報セキュリティ上の課題に対応する事業となっている。また、京都府の事業は、公益財団法人京都産業 21 が運営するもので、特に課題を限定している事業ではないが、専門家派遣対象となるメニューとして「情報セキュリティ」が明記されていた。これらの自治体へのヒアリング調査結果について以下に示す。

① 対応案件におけるセキュリティ関連テーマの割合

東京都の事業は、サイバーセキュリティを対象とした事業であるが、実績として年間平均 100 件程度とのことだった。千葉県及び京都府については、セキュリティ分野のみの支援要望はほとんどなく、京都府においては令和 2 年度に 2 件ほどあったという状況だった。現状としては、自治体が実施する専門家派遣事業に登録セキスペ (RISS) を活用するには、中小企業のニーズの掘り起しが必要である。

② 案件に対応している専門家の保有資格について

東京都の事業では、連絡先となっている専門家の保有資格としては、弁護士、IT コーディネータ (ITC)、CISSP (Certified Information Systems Security Professional) など様々な資格の中

に登録セキスペ（RISS）も存在している。

京都府も様々な分野で登録された専門家が検索できるようになっているが、情報システム分野で登録されている専門家としては、IT コーディネータ（ITC）が多い。

③ 登録セキスペ（RISS）の認知度

「情報処理安全確保支援士（登録セキスペ）という資格を知っていますか」という質問に対して、東京都、千葉県では「知っている」という回答だったが、京都府では「知らなかった」という回答だった。

④ 登録セキスペ（RISS）を登録（派遣）することについての意見

実施している専門家派遣の事業として、登録セキスペ（RISS）を活用することについての意見を伺ったところ、活用について否定的な意見は無かったが、どのような資格保有者であっても、資格を持っているだけでは中小企業の現場で求められる能力を必ずしも持っているとは限らない、という意見があり、資格以外にも現場での対応力が求められている。

8.4. 伴走型支援サービスの実現に関する考察

自治体事業調査の結果から、中小企業向けの伴走型支援サービスの実現化に向けて、3の仮説を立て、それぞれの仮説に対する施策案を考察した。以下に、仮説1)～3)と対応する施策案を示す。

仮説1) 情報処理分野（IT系）の公共事業には、「情報セキュリティ」を経営課題として明示することにより、登録セキスペ（RISS）を活用できるのではないか。

◎に分類したような「情報セキュリティ」をテーマとして扱う事業については、専門家として登録セキスペ（RISS）資格保有者が存在することを強く訴求していくことで、直接的に活動機会の拡大につながっていくと考えられる。

一方、○及び△に分類したような、経営課題全般を対象とした専門家派遣等の支援事業については、支援対象となる経営課題のメニューとして「情報セキュリティ」が明示されていないことが多いため、このままではニーズが顕在化されにくいと考えられる。そのため、当該事業を行う自治体において、「情報セキュリティ分野」を支援メニューに明示化することで、潜在的に情報セキュリティに不安をもつ中小企業等からの相談等が顕在化し、登録セキスペ（RISS）の活動機会の拡大につながることを期待できる。

仮説2) テレワーク拡大の中で、他土業と登録セキスペ (RISS) との協業が有効ではないか。

ワーク・ライフ・バランス支援アドバイザー（働き方の改善）の派遣や、テレワーク導入支援アドバイザー派遣事業では、就業規則にテレワーク勤務規程を追加（又は就業規則に追記）するため、社会保険労務士の派遣が行われていることが多いことが分かった。厚生労働省から発行されている「テレワークモデル就業規則～作成の手引き～」¹²においても、「テレワーク勤務規程にはセキュリティ事項を定めて遵守すること」と記載されているが、派遣された社会保険労務士は、情報セキュリティは専門外であるため、登録セキスペ (RISS) が協力することで付加価値を創出できると考えられる。実際に、本事業の指導事例として取り上げた社会保険労務士事務所からは、顧客企業からの相談内容によっては、登録セキスペ (RISS) と協業したいとの意見があった。

また、テレワーク関連機器導入に関しては、IT コーディネータ (ITC) 等が派遣される場合があるが、業種や業務によって機密情報の種類や扱い方が異なることから、セキュリティに関する最新知識や技能をもつ登録セキスペ (RISS) が、IT+セキュリティの分野で協業することで、セキュリティ対策を万全とすることできると考えられる。

仮説3) 伴走型サービスを進めるにあたっては、中小企業の経営者に情報セキュリティ対策が重要な経営課題であるという認識を持ってもらう必要がある。

◎事業に分類した事業においては、「情報セキュリティ」が支援メニューとして明示されているものもある中、実際に支援を実施した案件が少ない。中小企業等では、「情報セキュリティ対策」が経営課題であることの認知が不足しており、経営者に対して「情報セキュリティ」に対する認識を持ってもらうための施策が必要と考える。また、本事業の事例紹介企業を担当した指導専門家からも、情報セキュリティ対策はボトムアップだけでは不十分で、経営トップがトップダウンとして取り組むことで上手くできるというコメントが多かった。

その際の施策案として、自治体や事業を運営する公益財団法人、又は商工会議所等では、中小企業を対象実際にとして様々な経営テーマで無料のセミナーが開催されていることに注目し、多数の参加の見込まれるテーマで開催されているセミナーの中で、登録セキスペ (RISS) が講演者となって「情報セキュリティワンポイントセミナー」を行い、中小企業の経営者にも気付きを持ってもらうことで、コンサルティングに繋げていく活動が効果的なのではないかと考えられる。

¹² <https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/TWmodel.pdf>

9. 成果報告

9.1. 本事業の成果（有効性の検証）

本事業では、以下の成果を得ることができた。

成果 1：多くの企業で取組意欲、セキュリティレベル、継続改善の意識が向上した

専門家が4回目の指導終了後に提出する指導先別の指導最終報告では、指導の結果、経営層においては84.4%、従業員においては68.3%がセキュリティに対する取組意欲が向上したとの報告があった。経営層と従業員で差があるものの、指導先企業のセキュリティ意識の向上が図れたことがうかがえる。指導先企業でセキュリティレベルに関しても、専門家の指導最終報告では97.6%が向上したとの報告があり、指導先企業のほとんどでセキュリティレベルの向上が図れた。

また、指導先企業へのアンケートでは、専門家の指導を受けて今後実施すべきと考える情報セキュリティの取り組みについて、77.7%が「体制整備・運用ルールの方策・継続的な改善」、71.9%が「基本方針・関連規程等の継続的な改善」と回答（複数回答可）しており、指導先企業の継続改善の意識が高いことがうかがえる。

成果 2：セキュリティマネジメント指導に係る指導要領の有効性が確認できた

本事業では、セキュリティマネジメント指導業務の実施にあたり、IPAのセキュリティ対策支援ツールを活用した指導4回の標準的な指導内容（標準カリキュラム）と、指導先企業への依頼・調整事項等を説明する「指導要領（指導ツール）」を作成した。

専門家の指導最終報告では、指導先企業の状況として73.6%が使用した標準カリキュラムが「ちょうど良いレベルだった」との報告があった。一方、指導先企業へのアンケートでは、97.6%が今回の指導で成果が得られたと高い評価結果を回答しており、これらのことから、本事業のセキュリティマネジメント指導に係る指導要領（指導ツール）が有効に機能したことが確認できた。

また、専門家の指導最終報告では、指導内容について55.9%が「標準カリキュラム以外の内容も加えながら実施した」と報告していて、指導を担当した専門家が標準カリキュラムを基本としながらも、指導先企業の状況を診断したうえで、必要な指導を行っていたことがうかがえる。このことは、指導要領（指導ツール）に、中小企業の指導の心構えや、前年度指導経験者のノウハウ提供等、コンサルティングマインドに係る内容も含めたことが、プラスに働いたものと考えられる。

成果 3：身近な専門家による中小企業へのセキュリティ支援ニーズが改めて確認された

指導先企業へのアンケートでは、専門家の指導力・意欲について 95.1%、専門家の知識・専門力について 91.7%が高かったと回答し、非常に高い評価を得た。また、63.8%の指導先企業が、今後も専門家による一時的／定常的な指導・支援を希望するとした。指導先企業が、専門家の指導・支援を希望する理由としては、以下が挙げられている。

<情報セキュリティの専門家の指導・支援を希望する理由のコメント>

- ・情報セキュリティについて気軽に相談できる場所がないため継続的な支援が必要
- ・情報セキュリティは、年々新しい常識が出てくるので専門家の支援が必要
- ・経営層の理解促進には外部の意見も必要なので、運用段階においても専門家の支援が必要
- ・社内の人材では補えない部分を、顧問契約や外注といった形態で支援して欲しい。

一方、専門家の指導最終報告では、64.1%の専門家が指導先企業へ有償での継続フォローを提案したところ、回答のあった企業のうち、15.7%（37社）の指導先企業から実際に依頼があったことに加え、46.8%（110社）の企業も検討するとの回答があった。

これらのことから、身近な専門家による中小企業へのセキュリティ支援ニーズがあることが改めて確認された。

9.2. 中小企業等の現状と課題

本事業では、9.1 で示した成果を得られた一方、中小企業等における情報セキュリティ対策に係る課題も明らかになった。

中小企業の課題：セキュリティ対策に係る人的リソース不足、コスト負担の余裕が無い

本事業において、専門家の指導・支援を継続的に希望する中小企業も少なからずあった一方で、指導先企業へのアンケートでは、「予算が限られているため困難」、「費用負担があるなら継続は厳しい」といった声も多く寄せられた。

また、IPA が実施した「2018 年度 SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査報告書」では、中小企業が情報セキュリティ対策を進める上での課題点の回答（複数回答可）として、「情報セキュリティ対策の知識をもった従業員がいない」が 42.7%、「業務を行うための人手が足りない状況である」が 41.8%、「セキュリティ対策を行うための予算確保が難しい」が 30.8%であることを踏まえれば、中小企業の情報セキュリティ対策を進めるにあたり、人的リソースは厳しい状況にあるとともに、セキュリティ投資に係るコスト負担の余裕が無いことも大きな課題となっていることがうかがえる。

9.3. 専門家の現状と課題

本事業では、前年度に引き続き、セキュリティの専門家として登録セキスペ（RISS）等を起用したところであるが、中小企業等の情報セキュリティ対策向上に向けて、登録セキスペ（RISS）が活躍する機会を創出するための課題も明らかになった。

専門家（登録セキスペ）の課題1：コンサルティングに係るスキルアップ

専門家（登録セキスペ（RISS））へのアンケート結果から、指導を行った登録セキスペ（RISS）のうち、35.0%はコンサルティングの未経験者であった。今後、より多くの登録セキスペ（RISS）が、中小企業等のセキュリティマネジメント指導で活躍できるようにするためには、本事業のように実際に中小企業等への指導を経験できる場への参加等により、コンサルティングに係るスキルアップを図ることが必要であると考えられる。

なお、本年度事業においては、コンサルティングに係る経験・スキル（コミュニケーション含む）が不足していると感じる専門家に対して、コンサルティング経験が豊富な専門家との同行によるOJT制度を設けたが、本OJT制度には13名の専門家の参加があり好評であった。OJT制度に係るルールや運用面での準備不足の指摘もあったが、OJT制度が今後の登録セキスペ（RISS）のスキルアップ施策として有効であることが確認された。

専門家（登録セキスペ）の課題2：中小企業とのコネクション強化

本事業においては、指導先企業の募集手段として、中小企業等に対する各種事業告知活動を行うとともに、前年度と同様に、専門家が中小企業等に対して自らを指名してもらう参加促進活動を推奨した。その結果242件が中小企業等からの事前指名ありで、そのうち登録セキスペ（RISS）が事前指名を受けた件数は168件であり、前年度の154件に比べて微増という結果であった。

一方、本年度事業では、一人で20社以上企業からの事前指名を受けた登録セキスペ（RISS）が2名存在した。この2名から、個別ヒアリングにより「専門家指名及び効率的な指導についてのノウハウ・工夫」を聴取したところ、地域の商工団体（商工会議所、商工会等）への説明訪問による協力依頼により、経営セミナーでのチラシ配布、商工団体の会報やメルマガへの寄稿等の中小企業等とのコネクション強化を図る活動を実践していたことが分かった。このような日頃の活動は、登録セキスペ（RISS）の今後の活動に対して大きな示唆となるのではないかと考える。

専門家（登録セキスペ）の課題3：登録セキスペの知名度の向上と活躍の場の拡大

専門家（登録セキスペ）のアンケートにおいて、「登録セキスペ（RISS）資格を武器に中小企業を対象とした有償の支援サービスによって、継続的なビジネスにつなげていくことが可能だと思うか」という問いに対して、「可能だと思う」の回答が37.3%あったものの、「難しいと思う」との回答も45.2%あった。「難しい」と回答した理由については、「中小企業側のコスト的な課題」と併せて、「登録セキスペ（RISS）の知名度や有効性が広く知られていない」とするコメントが挙げられた。

登録セキスペ（RISS）の知名度の向上と共に、継続的なビジネスとして活躍できる場を創出していくためには、本事業で実施した、都道府県、政令指定都市、及び県庁が所在する市が行う中小企業向けの伴走型支援サービスに関する調査において考察した、登録セキスペ（RISS）の活用施策案が、今後の取組みの参考になると考えられる。

【参考】＜登録セキスペ（RISS）の活用施策についての考察＞

施策案1) 情報処理分野（IT系）の派遣事業に対して、支援対象の経営課題として「情報セキュリティ」を明示する。

施策案2) テレワークが普及する中で、他士業（社労士、ITC等）との連携より、IT+セキュリティを付加価値とした協業を行う。

施策案3) 自治体、商工団体等の協力を得て、登録セキスペ（RISS）が講演者となったセミナーを行うことで、経営者に情報セキュリティ対策が重要な経営課題であるとの認識を啓発する。

9.4. 事業運営に関する課題

本事業は、前年度に引き続き実施したものであり、前年度の実績と課題を踏まえた改善策を講じ、実施要領作成などの準備段階での工夫を行うことにより、実施期間が短いながらも成果をあげることができた。しかし、一部においては、事業運営に関する課題が見受けられた。

事業運営の課題1：事業内容の告知の工夫

前年度は、指導先企業が3大都市圏（首都圏・中京圏・近畿圏の11都府県）に偏重する傾向となっていたことから、本年度は、3大都市圏以外の36道県地域を中心に、募集チラシの配布、Webサイトへの事業案内掲載、テレマーケティング、メルマガ・メールニュース等のメール配信等による事業告知を行った。

しかし、募集チラシ配布を行った商工団体（商工会・商工会議所等）においては、コロナ禍の影響により、補助金、融資等事業継続等に関する対応の優先度が高く、また、商工会・商工会議

所主催のセミナー等の開催が困難であったため、セミナー配布物として募集チラシを中小企業に直接渡す機会が少なく、募集チラシによる告知効果が得られにくい状況であった。

また、テレマーケティングによる募集活動は、「IPA」の組織名認知度が予想以上に低いことや、無料施策ということに不信感をいだく方もあり、電話での事業説明が困難なことから、想定に比べ募集活動の成果をあげることができなかった（想定約30%）。

募集期間後半からは、「各経済産業局メルマガ会員へのメルマガ配信」、「お助け隊実証参加企業へのメール配信」、「SECURITY ACTION 宣言者向けメールニュース」、及び事務局関連のチャンネルを活用したメルマガ・DM等による中小企業等への募集活動を加速化、専門家による指導先企業の参加促進活動（事前指名）により、指導先企業の募集目標を達成することができた。

専門家による指導先企業の事前指名は242件と、マッチング総数395件の61.3%であったことから、中小企業等への募集活動は、日頃の信用醸成の中で培われた信頼関係が重要で、事業内容の告知の工夫が必要であると言える。

なお、本事業の中小企業等の申込総数は413社で、36道県地域は179社（43.3%）、3大都市圏（11都府県）は234社（56.7%）であった。36道県地域の中小企業の参加を促進した結果、前年度の36道県地域の割合（34.6%）に比べ約10%増加した。

事業運営の課題2：オンライン講習の活用と受講促進の取組み

本事業では、専門家の指導講習会をEラーニング型式のオンライン講習で実施した。Eラーニング実施後の受講者アンケートでは、78.6%の受講者が「Eラーニングの方が良い」と回答しており、「集合形式の方が良い」と回答した3.2%を大幅に上回った。理由としては、「Eラーニングは時間や場所の制約がないため受講しやすい」という声が多くあった。「Eラーニングなので途中で止めたり見直しができるので理解できた」という声もあり、繰り返し視聴できるという点でも、Eラーニング形式は有効であったと言える。今後も、登録セキスペ（RISS）への教育を実施する際にはEラーニングを活用することで、効率的に多くの受講者の参加を促せるのではないかと考えらえる。

一方、受講を開始しても数週間学習が進まない受講者もいて、受講の催促連絡等を行う必要があるケースも生じた。また、受講完了は60%未満に留まり、途中終了した受講者も少なからずいたことから、Eラーニング形式で講習会を開催する場合には、受講促進の取組みが課題となる。

9.5. 登録セキスペ（RISS）の活用機会の検討

9.1～4 で示した、本事業の成果と課題を踏まえ、セキュリティの専門家である登録セキスペ（RISS）の活用機会について検討を行った。

本事業の結果、中小企業等の情報セキュリティ対策向上には、登録セキスペ（RISS）による中小企業向けの伴走型支援サービスが有効であると考えられる。しかし、中小企業等はセキュリティ対策に係る人的リソースが不足していることや、コスト負担の余裕が無いことから、伴走型支援サービスの実現には、公的機関・自治体や商工団体などが役割を分担するかたちで、登録セキスペ（RISS）との連携強化することが重要である。

以下に、登録セキスペ（RISS）活用による中小企業向け伴走型支援サービス実現のためのフレームワーク案として、期待される各組織の役割についての考察を示す。

<登録セキスペ（RISS）>

本事業で有効性が確認されたセキュリティマネジメント指導の指導要領（指導ツール）をベースにしつつ、継続的支援を有償サービス（伴走型支援サービス）として提供することで、中小企業等のセキュリティ対策に係る人的リソース不足を補うことが期待できる。取り組みのポイントとしては、登録セキスペ（RISS）の日常の活動として、各関係者とのコミュニケーションを図ることで、顧客の紹介や具体的な引き合いを増やすこと、並びに登録セキスペ（RISS）自身がスキルアップを図ることで、コンサルティング実施時に顧客との信頼関係を築くことが重要となると考えられる。

<公的機関・自治体>

関係省庁、独立行政法人等の公的機関及び自治体においては、セミナー等を通じた中小企業等のセキュリティの意識向上や、経営支援、IT 導入支援、教育支援等の中小企業向け支援事業（専門人材派遣支援を含む）を継続するとともに、それら施策の支援メニューに「情報セキュリティ分野」を明示化し、併せて専門人材派遣の要件に、登録セキスペ（RISS）資格保有者の参加を推奨する等の取り組みが重要であると考えられる。

<商工団体>

商工会議所、商工会等の商工団体においては、登録セキスペ（RISS）と連携したセミナー開催などで中小企業のセキュリティ意識の向上を促すとともに、セキュリティに関する相談対応として登録セキスペ（RISS）を活用する等の取り組みが重要であると考えられる。

情報処理安全確保支援士会>

一般社団法人情報処理安全確保支援士会（JP-RISSA）においては、RISS 推進団体として、RISS 向けコンサルティングスキル向上研修（OJT、OFF-JT）、優良事例の展開、各地域におけるRISS のコミュニティ形成等のサポート支援、他士業との連携支援の役割が期待される。

<他士業>

社会保険労務士やITコーディネータ（ITC）等の他士業と登録セキスペ（RISS）との協業により、中小企業等のテレワーク導入やIT導入におけるセキュリティ対策を万全とする支援を行うことが期待される。

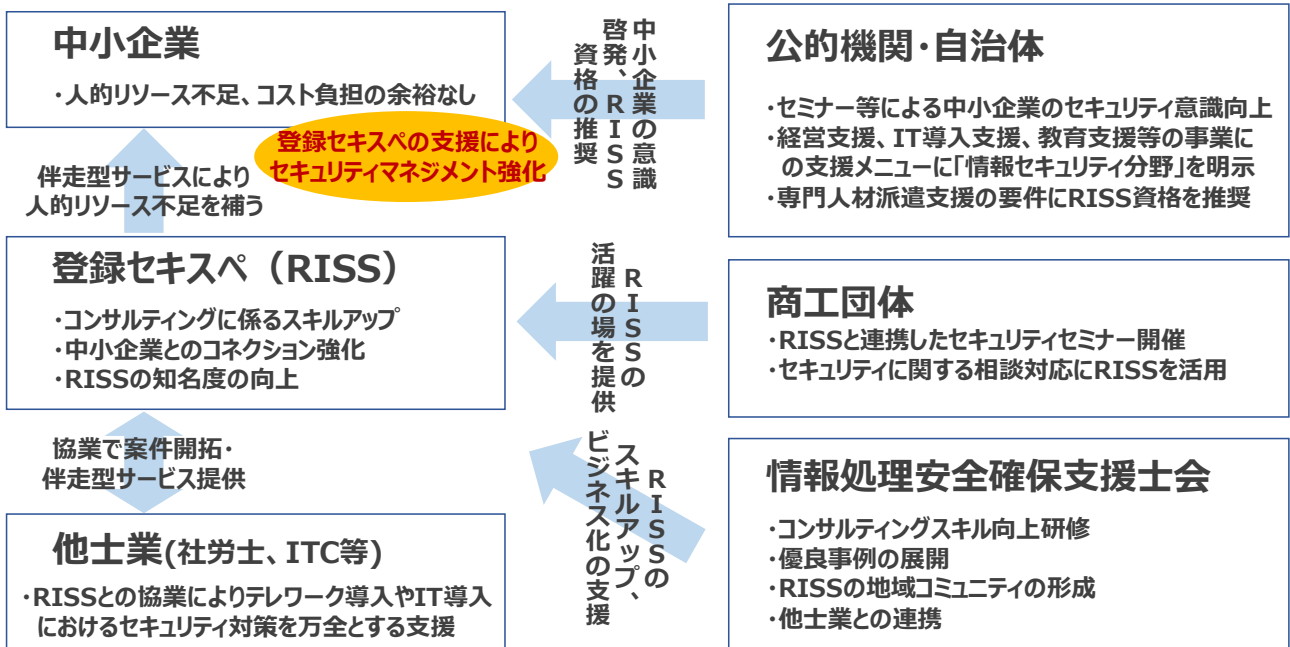


図 50 登録セキスペ（RISS）活用による伴走型支援サービス実現のフレームワーク案

資料

添付資料 1 中小企業向け募集チラシ

経済産業省補助事業
令和2年度中小企業向け情報セキュリティマネジメント指導業務のご案内

IPA 独立行政法人 情報処理推進機構

情報セキュリティ対策は、 企業を守る 重要な取組です

対策を怠ったことで、下記のような事故が
おこっています。

ポイント 1 最も多い原因 **5,500件**
古いOSの使用でマルウェアに感染

ポイント 2 増加傾向 **4,925件**
私物の端末から業務用の全PCに感染

ポイント 3 増加傾向
出張先のWi-Fi環境でマルウェアに感染

Windows XPでしか動作しないソフトウェア対策のために、マルウェア対策ソフトを導入したWindows 10端末を使用し、マルウェアに感染。

マルウェアに感染しているiPhoneが会社のWi-Fiに接続して登録されていた。Wi-Fiを接続して社内LANに侵入し業務用の全PCに感染、業務停止や顧客情報が流出。

出張先でより安全なメールを閲覧、受け取られたマルウェアを実行し、Encryptに感染。アドレス帳の盗み取り、顧客企業にとりまわし、取引先等のアドレス帳に悪影響メールが送信された。

このようなことになる前に事前の対策が必須です!!

セキュリティ対策を支援するコンサル事業を参加無料で実施!

セキュリティ専門家がある企業の活動を支援し、社内のセキュリティリスクの洗い出しや、セキュリティレベルの測定実施といったコンサルティングを実施を行います。半年の参加費アンケートでは、専門家による指導で成果を測定した企業は94.4%にも上り、ご自身の声が多数寄せられました。

情報セキュリティの専門家も無料派遣
400社限定!

オンラインによる指導も対応します。

mail / 1 社内のリスクが何かわかる	mail / 2 リスクの対策方法がわかる
mail / 3 専門家の支援で安心	mail / 4 取引先からの信頼度アップ

本事業および個人情報の取り扱いに関するお問い合わせ先
【中小企業向け情報セキュリティマネジメント指導業務】事務局（富士ゼロックス）
TEL:03-6801-6911 受付10:30~17:00 年中無休 Mail:info@sme-security.jp
https://www.ipa.go.jp/security/kaihatsu/sme/management/index.html

お申し込みは裏面をご覧ください!!

情報セキュリティマネジメント指導業務のイメージ

中小企業に専門家を派遣し、実践的なセキュリティ対策の定着につなげる。

IPA 研修	中小企業 対策支援 ポリシー策定支援など 400社以上の専門家 400社が対象	事業内容 中小企業向け情報セキュリティに関するマネジメント体制の構築を目的に、全国の中小企業400社を対象に専門家（情報処理工学専攻支援士等）が訪問し、標準に即したリストの洗い出しやマネジメント上のセキュリティ対策方針や経営課題の測定に向けた支援を実施します。
------------------	--	--

セキュリティの専門家
(情報知識 安全確保支援士など)

企業に寄り添って、実践的かつスピーディな対応が得意です。

セキュリティの知識が、より社員のレベルアップにつながります。

セキュリティ対策の効果が、社員のモチベーションアップにつながります。

「情報知識 安全確保支援士」とは、
「セキュリティは、活用・使用が前提だが、**悪化度が低減**というのが大前提だった。」
「既存のルールがあっても、組織文化やIT環境の状況によって、安全管理が不十分な部分があることで、**改善の余地が広がった。**」
「中小企業向け情報セキュリティ対策は、人的になりながら、外部の専門家の積極的支援から**強行に導入するべき点を強調**した点での効果は大きかった。」
「業務改善という点で大きな成果があった。**強行した理由についてもご説明**した点で、他の中小企業への影響が大きい。」

募集要項

専門家派遣期間
10月20日 末 ▶ 1月(予定)

お申し込み方法 (Webから申し込みよりお申し込みください)
<https://sme-security.jp/sv/kigyoo>

お申し込みから終了までの流れ (10月上旬~12月初旬期間予定)

- お申し込みフォームより参加のお申込み
- お申込み完了のご連絡を事務局よりメール送信
- 専門家派遣訪問日程を提示（お申し込み後3営業日以内）
訪問コンサルする専門家を候補リストから指名（最大4名）
- 訪問コンサルする専門家決定のご連絡
お申込みを頂いた場合は、訪問先より派遣の専門家をご案内します。
- 訪問日調整
- SECURITY ACTION宣言一つ星以上のご登録（お申込後の企業のみ）
- 訪問コンサル（企業別）
【1回あたり約2時間、期間11.5~2か月も実施】お申し込みの申し込み日より実施可能です。
- コンサル終了後、アンケート調査

情報知識 安全確保支援士とは ▶ サイバーセキュリティ分野の国家資格で、資格者は政府機関や企業等における情報セキュリティ確保を支援します。

※ 詳細はこちらをご覧ください。
Q 情報知識安全確保支援士

すでに10万の中小企業等がSECURITY ACTIONを宣言! 自社への信頼度をアップしています。

製造業 1 1
卸売業 2 2
サービス業 3 3

SECURITY ACTION宣言のメリット
自社の宣言が県のホームページで紹介され、
県民にもつながる。
セキュリティ対策の宣言を公にすることで
信頼度がアップ。

詳しくは、SECURITY ACTION
サイトへ
<https://www.ipa.go.jp/security/security-action/index.html>

添付資料 2 専門家向け募集チラシ

独立行政法人情報処理推進機構 主催
経済産業省補助事業
令和2年度 中小企業の情報セキュリティ
マネジメント指導業務
専門家募集のご案内

IPA 独立行政法人 情報処理推進機構

背景・目的

あらゆる産業活動においてサブプライムリスクの特性が顕在化しつつある昨今、サブプライムリスクを構成する中小企業のサイバーセキュリティ対策を進めることは喫緊の課題です。さらに、新型コロナウイルス感染症対応による急激な在宅勤務テレワークの拡大によって生じた「利用環境の変化やそれを行ったサイバー攻撃など、新たに生じた脅威セキュリティリスクへの取り組みも重要と認識です。中小企業の情報セキュリティ対策水準を向上するためには、情報セキュリティに関する実務の向上の他に、身近で実務に相談ができる専門家とのつながりや、専門家による指導を通じた具体的な対策の実施を促す必要があります。そこで、地域で活躍している情報セキュリティ専門家等と連携し、中小企業における情報セキュリティマネジメント体制の構築に向けた支援を行うため、昨年度に引き続き専門家派遣事業を実施します。

事業内容

全国各地域で活躍している情報処理安全確保支援等の専門家の豊富な知識・ノウハウ・スキルをフル活用した中小企業への指導を実施します。
 (実施期間:2020年10月下旬～2021年1月(予定))

- 中小企業の情報セキュリティガイドラインに基づく支援
- 情報セキュリティ診断とリスクの洗い出し
- 重点的に対策を講じるべき領域の特定(コロナ禍における情報セキュリティ対策含む)
- 情報セキュリティ基本方針、関連規程の策定支援等

※1社あたり計4回の現地訪問またはオンラインによる指導を実施(標準1回あたり約2時間、指導時間は1コマから可能です)

参加メリット

- 1 専門家としての実績が積みまます**
 専門家としての経験・実績を積むことで活動の幅が広がります
 (指導に対して謝金が支払われます)
- 2 中小企業との継続的な関係構築**
 一過性の指導ではなく、中小企業との継続的な関係を構築するきっかけとなります
- 3 優良指導は事例として公開**
 指導実績はウェブ上に掲載することができ、優良な指導事例は情報処理推進機構(IPA)が取りまとめて公開します

謝金あり

本事業をご理解いただくためにE-ラーニング形式でオンライン講習を受けていただきます。オンライン講習受講後、本事業への参加をご判断いただけますので、お気軽に参加ください。
 (参加資格:情報処理安全確保支援士等の専門家や中小企業支援に関心のある方)

参加申込は、裏面をご覧ください

IPA 独立行政法人 情報処理推進機構

オンライン講習会 概要

パート	オンライン講習プログラム	時間(目安)	主な内容
1	具体的支援の進め方① [専門家志望全体の構成と留意事項]	40分	●達成目標と訪問指導の流れ ●全4回のカリキュラム構成と内容について具体的に解説 ●訪問企業への依頼/調整事項や企業訪問に当たっての基本的な留意事項 理解度確認テスト
2	具体的支援の進め方② [各種ツールの活用方法]	40分	●ツールの紹介(5分ですべての白社診断:Web版、設備コンテンツ、情報セキュリティ対策ガイドライン、ヒアリングシート) ●設備コンテンツ[あなたの会社のセキュリティドクター]の構築と解説 ●中小企業の情報セキュリティガイドライン、クラウドサービス安全利用の手引きなどの紹介、解説 理解度確認テスト
1	効果的な訪問指導① [無難に当たっての心構え]	40分	●日本の中小企業の現状(規模/分類/割合の迅速性) ●経営者の一般的な関心事 ●訪問先企業を理解するポイント ●効果的コミュニケーション手法 ●意図の喚起 理解度確認テスト
2	効果的な訪問指導② [昨年度の訪問指導から学ぶこと]	30分	●情報セキュリティ対策が進んでいない状況 ●昨年度の訪問指導の全体像(希望、疑問、クレームなど) ●昨年度の事例紹介 ●工夫した点、苦労した点 理解度確認テスト
3	効果的な訪問指導③ [コロナ禍のセキュリティ対策]	30分	●コロナ禍における「利用状況(報酬)」 ●テレワーク導入時の注意点およびセキュリティポリシー策定の留意点 ●業務別コロナ対応 ●Web会議システム導入時のセキュリティ上の留意点 ●オンライン指導を行うにあたってのWeb会議システム利用について 理解度確認テスト
1	事業の運営、謝金の支払いについて	30分	●希望する専門家の申込み受付方法など ●業務手続きと謝金のお支払い ●連絡事項について

指導要領受取に関するアンケート

参加お申し込み方法

指導専門家を希望される方は、以下の事業案内サイトにアクセスして募集要項をご確認のうえ、オンライン講習に参加申込みをしてください。 ※取寄せした個人情報、本事業のための受け、登録、連絡のみに使用いたします。

本事業および個人情報の取り扱いに関するお問い合わせ先

[中小企業の情報セキュリティマネジメント指導業務] 事務局(富士ゼロックス内)
 TEL: 03-6801-6911 (平日10:30~17:30、年末年始除く)
 Mail: info@sme-security.jp
 事業案内サイト: <https://www.jpago.jp/security/keihatsu/sme/management/supporter.html>
 ※本事業関係者については、富士ゼロックス株式会社にて開設しています

参加申込の欄に開示する個人情報は、独立行政法人 情報処理推進機構が定めるプライバシーポリシーに準じて適切に取り扱います。