# 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

2025 年 5 月

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

目次

# 1. はじめに

## 1.1. 本事業の目的、背景

近年、中小企業においても IT 化が進み、業務の効率化やサービスレベルの向上等が図られている。その一方で、機密情報を狙ったサイバー攻撃は日々発生し、その被害が確認されている。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や、それに起因する取引先の大企業等の被害も顕在化しており、サプライチェーン単位での攻撃が増加する中、必要十分なセキュリティ対策を実施できない企業が狙われることで大きな経済的損失をもたらすおそれがある。そのため、予算や人材が不足している中小企業において効果的なセキュリティ対策を実践できるよう、規模等に応じたセキュリティ対策を提示するとともに、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、独立行政法人情報処理推進機構（以下「IPA」という）では、令和元年度及び令和 2 年度において、高度なセキュリティ知識を有する専門家である情報処理安全確保支援士（以下「登録セキスペ」という）[1]等を活用した「中小企業の情報セキュリティマネジメント指導業務」[2] [3]を実施した。そこでは、中小企業の情報セキュリティ対策向上には、専門家による伴走型支援サービスが有効であり、自治体、商工会議所等との連携強化が重要であることが報告されたところである。

今回、登録セキスペ等専門家のさらなる活用促進を図るため、中小企業とセキュリティ人材とのマッチングを促す場を構築する実証を実施した。具体的には、業界団体や商工会議所等の経済団体等（以下「支援機関」という）と連携して、登録セキスペでかつ IPA セキュリティプレゼンターの登録者をセキュリティ専門家として起用し、サイバーセキュリティ相談会の開催、セキュリティマネジメント指導（テーマ別）の実施、及び登録セキスペが実施可能な業務やスキル等に関するアンケートを実施した。これらの実証を通じて、支援機関のセキュリティ対策に係る課題ニーズの把握と、中小企業がセキュリティ専門家を探索しやすくするための、登録セキスペが実施可能な業務やスキル等を見える化した人材プールリスト（以下「アクティブリスト」という）の整備について検討を行ったところである。また、これらの検討結果から、将来的な対応としての「アクティブリスト」活用によるビジネスベースのマッチング促進に向けた施策の方向性を考察した。

---

[1] 情報処理安全確保支援士（通称：登録セキスペ、英語名：RISS）
サイバーセキュリティ対策を推進する人材の国家資格。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、サイバーセキュリティの確保を支援する。
https://www.ipa.go.jp/jinzai/riss/index.html

[2] 「2019 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」報告書について
https://www.ipa.go.jp/archive/security/reports/2019/sme-management.html

[3] 「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」報告書について
https://www.ipa.go.jp/security/reports/sme/management2021.html

### 1.2. 本事業における実施事業の全体像

本事業は主に以下の構成で実施した。

(1) サイバーセキュリティ相談会の開催
(2) セキュリティマネジメント指導（テーマ別の実施）
(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) 実施報告書の作成

(1)については、中小企業向けの情報提供及び個別のセキュリティ相談を推進するため、大阪・名古屋・埼玉の 3 地域において計 6 回、地域の商工会議所との連携のもとで相談会（以下「サイバーセキュリティ相談会」という）を実施したものである。また、相談会参加者のうち希望する企業（34 社）（以下「指導先企業」という）を対象に、(2)としてセキュリティマネジメント指導（伴走型支援）を計 100 回実施した。マネジメント指導実施に際しては、後述する５つのセキュリティ対策テーマを設定の上、標準的な指導に使用できる指導ツールを作成し、指導先企業に必要な内容を適切に判断した上で予め依頼したセキュリティ専門家（以下「指導専門家」という）が指導する形をとった。

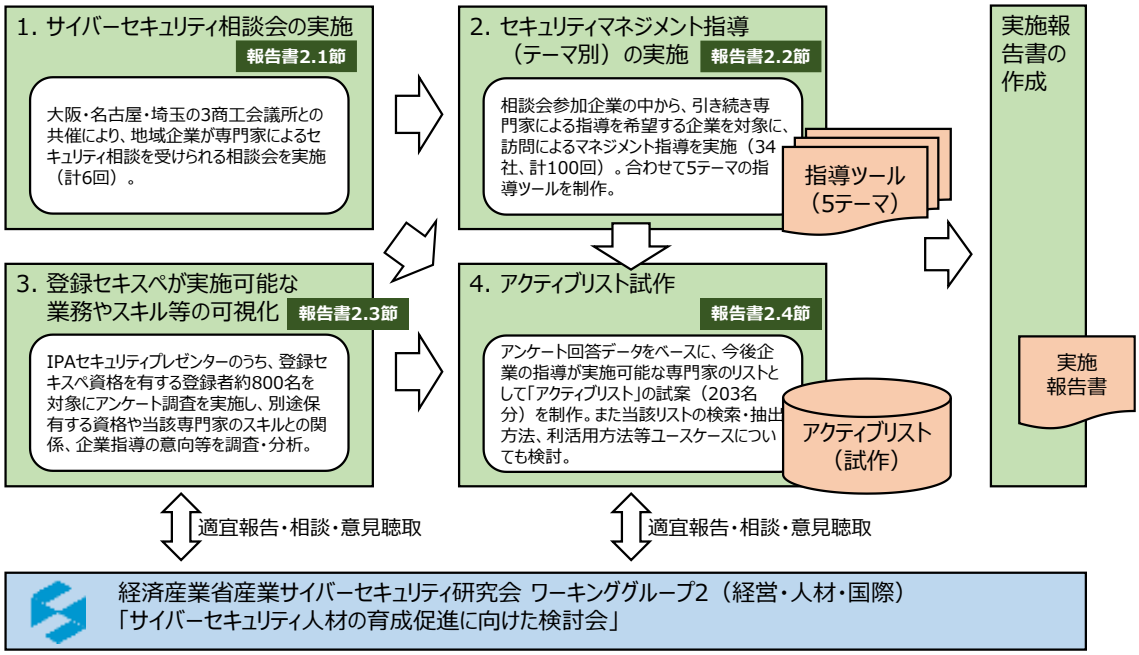
またこれらの作業と並行し、(3)として、セキュリティ専門家が今後地域の中小企業の支援を行う上で必要となるスキルや業務内容を明らかにするため、セキュリティ専門家に対してアンケートを実施し、詳細な分析を行った。この結果も踏まえ、今後地域の中小企業に対するセキュリティ支援を行う上で役立つ「アクティブリスト」を試行的に作成し、これを活用する施策のあり方等について考察した。これらの分析を行うにあたっては、実証に参加いただいた指導先企業、マネジメント指導を担当した指導専門家、併せて商工会議所等支援機関へのヒアリングを実施し、現場の生声を反映する形で、実践的かつ効果的な施策につながるよう工夫した。

さらに本事業は、経済産業省が事務局を務める産業サイバーセキュリティ研究会ワーキンググループ 2（経営・人材・国際）「サイバーセキュリティ人材の育成促進に向けた検討会」[4]において、実証事業の内容を適宜報告し、有識者からの意見も反映する形で推進した。

以下、事業の全体像を示す。

次章以降において、実施した各事業について詳述する。

[4] サイバーセキュリティ人材の育成促進に向けた検討会
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_keiei/cyber_human/index.html




図表 1-1 令和 6 年度セキュリティ人材活用促進実証に係る業務事業全体像

## 2. 実施事業内容

### 2.1. サイバーセキュリティ相談会

本事業においては、商工会議所等支援機関と連携の上、地域の中小企業等を対象としたサイバーセキュリティ相談会を、大阪、名古屋、埼玉の 3 地域で計 6 回開催した。相談会は IPA が主催、地域の商工会議所が共催する形で実施した。

相談会では参加企業がセキュリティ専門家と個別の相談を受けられるように設定するとともに、後続で行うマネジメント指導（テーマ別）の実施希望企業を募った。

以下、各相談会の開催概要を示す。

#### 2.1.1. 開催概要

| | | 大阪 | 名古屋 | 埼玉 |
|---|---|---|---|---|
| 第1回 | 開催日程 | 2024/10/24(木)<br>13:00～16:00 | 2024/10/21(月)<br>13:00～16:00 | 2024/10/15(火)<br>13:00～16:00 |
| | 開催場所 | 大阪商工会議所<br>4 階 402 号会議室 | 名古屋商工会議所<br>5 階会議室 BC | さいたま商工会議所<br>2F 第 1・2 ホール |
| | 参加申込期間 | 9/11～10/8<br>（定員超過締切） | 9/18～10/21 | 9/13～10/15 |
| 第2回 | 開催日程 | 2024/11/18(月)<br>13:00～16:00 | 2024/11/20(水)<br>13:00～16:00 | 2024/11/25<br>13:00～16:00 |
| | 開催場所 | 大阪商工会議所<br>5 階 502 号会議室 | 名古屋商工会議所<br>3 階第 5 会議室 | さいたま商工会議所<br>2F 第 1・2 ホール |
| | 参加申込期間 | 9/11～11/14<br>（定員超過締切） | 9/18～11/8<br>（定員超過締切） | 9/18～11/25 |

図表 2-1 サイバーセキュリティ相談会開催概要

各回とも、IPA ウェブサイト内に申込受付フォームを作成し、個別相談の希望有無及び後続のマネジメント指導（テーマ別）の希望有無等についても併せて情報を取得した。

なお、大阪開催分については、IPA による参加受付と並行して大阪商工会議所でも参加を取りまとめていたため、開催前に参加者情報を統合した。

参加申込者に対しては、特に相談会申込者に対しては相談内容の事前聞き取りメール連絡（後述）を入れるとともに、開催 1～3 日前にリマインドメールを送信した。

### 2.1.2. プログラム概要

相談会当日のタイムスケジュール及びプログラムは、各回とも以下のとおり。

| 開始時間 | 内容 |
|---|---|
| 12:00 | 講演者、セキュリティ専門家会場入り |
| 12:10 | （講演者）マイクテスト、資料投影、動線確認<br>（セキュリティ専門家）マネジメント指導ツールの説明 |
| 12:40 | 参加者入場開始、受付開始 |
| 13:00 | 開会<br>IPA による相談会開催内容の説明 |
| 13:10 | 講演 |
| 14:10 | IPA からのご案内 |
| 14:20 | 商工会議所からのご案内 |
| 14:30 | 参加アンケート記入、個別相談の無い参加者は退室<br>個別相談受付設置 |
| 14:50 | サイバーセキュリティ個別相談１回目 |
| 15:10 | 休憩 |
| 15:15 | サイバーセキュリティ個別相談２回目 |
| 15:35 | 休憩 |
| 15:40 | サイバーセキュリティ個別相談３回目 |
| 16:00 | 閉会 |

図表 2-2 サイバーセキュリティ相談会タイムスケジュール・プログラム

### 2.1.3. セミナー講演者及びセキュリティ専門家

（１） セミナー講演者

各回のセミナー講演者及びタイトルは以下のとおり。

セミナー講演者の出講にあたっては、事務局から依頼文書を発行し、承諾いただく手続きをとった。また、講演 1 回あたりの報酬 15,000 円（税込）と当日会場までの交通費（実費）を支払うこととし（辞退者を除く）、当日の講演に向けて、講演資料の準備等、事務的な連絡・調整を随時行った。

| 回・日程 | 講演タイトル・セミナー講演者（所属） |
|---|---|
| 大阪 第 1 回<br>（10/24） | 「お客様に選ばれ続けるためのサイバーセキュリティ経営」<br>原 一矢 氏<br>（ビットフロー・マネジメント株式会社 代表取締役） |
| 名古屋 第 1 回<br>（10/21） | 「まずはここからはじめるセキュリティ対策の第一歩」<br>大喜 康生 氏<br>（情報処理安全確保支援士会 理事） |
| 埼玉 第 1 回<br>（10/15） | 「今、企業が気を付けるべき『サイバー犯罪』」<br>小野 稔晃 氏<br>（埼玉県警察本部 生活安全部 サイバー局サイバー対策課 対策・官民連携係 警部補） |
| 大阪 第 2 回<br>（11/18） | 「情報漏洩インシデント ～たかが USB、されど USB～」<br>小坂谷 聡 氏<br>（小坂谷・中原法律事務所 弁護士） |
| 名古屋 第 2 回<br>（11/20） | 「中小企業のセキュリティ対策 ～設備保守回線からの侵入防止対策～」<br>鈴木 春洋 氏<br>（IPA セキュリティセンター 研究員） |
| 埼玉 第 2 回<br>（11/25） | 「今、企業が気を付けるべき『サイバー犯罪』」<br>小野 稔晃 氏<br>（埼玉県警察本部 生活安全部 サイバー局サイバー対策課 対策・官民連携係 警部補） |

図表 2-3 サイバーセキュリティ相談会 セミナー講演者及び講演タイトル

（２） 相談会対応セキュリティ専門家

各回の相談会にて相談対応いただいたセキュリティ専門家は以下のとおり。

これらのセキュリティ専門家は、登録セキスペでかつ IPA のセキュリティプレゼンターにも登録している方のうち、大阪・名古屋・埼玉の各地域で活動可能としている方をピックアップし、個別に依頼を行ったものである。依頼に際しては事務局から依頼文書を発行し、承諾いただく手続きをセキュリティ専門家に対して行った。

また、相談会 1 回あたりの報酬は 1 人 15,000 円（税込）とし、当日会場までの交通費（実費）を支払うこととした（辞退者を除く）。

| 回（日程） | セキュリティ専門家（所属・保有資格等） |
|---|---|
| 大阪 第１回<br>（10/24） | 清水 俊彦 氏（えがお IT 研究所合同会社 代表、情報処理安全確保支援士、システムアーキテクト）<br>高橋 幸司 氏（株式会社東洋 常務執行役員 CIO、情報処理安全確保支援士、中小企業診断士、IT コーディネータ）<br>野村 陽子 氏（株式会社ブルーオーキッドコンサルティング 取締役、情報処理安全確保支援士、中小企業診断士）<br>原 一矢 氏（ビットフロー・マネジメント株式会社 代表取締役、情報処理安全確保支援士、中小企業診断士、CISSP） |
| 名古屋 第1回<br>（10/21） | 一ノ瀬 誠 氏（合同会社 River-Win 代表、情報処理安全確保支援士、中小企業診断士、IT ストラテジスト、システム監査技術者）<br>久保田 秀男 氏（情報処理安全確保支援士、システム監査技術者）<br>三代 健一郎 氏（情報処理安全確保支援士、プロジェクトマネージャー）<br>大喜 康生 氏（情報処理安全確保支援士会 理事、情報処理安全確保支援士、中小企業診断士、システム監査技術者、CISA、CISM） |
| 埼玉 第１回<br>（10/15） | 遠藤 貴芳 氏（情報処理安全確保支援士、IT コーディネータ、PMP）<br>上ヶ平 裕彦 氏 (上ヶ平 IT 事務所 代表・情報処理安全確保支援士、IT コーディネータ、上級ウェブ解析士)<br>堀内 靖大 氏（ジーアールアイ株式会社 代表、情報処理安全確保支援士） |
| 大阪 第２回<br>（11/18） | 高谷 幸治 氏（高谷経営支援事務所 代表、情報処理安全確保支援士、中小企業診断士、IT ストラテジスト、システム監査技術者）<br>田中 基貴 氏（コンサルティング・リンクスル 代表、情報処理安全確保支援士、中小企業診断士、IT ストラテジスト、ネットワークスペシャリスト）<br>渡邊 功 氏（Nextplanning 合同会社 代表、情報処理安全確保支援士、中小企業診断士、IT コーディネータ、システム監査技術者、ISMS 主任審査員）<br>野村 陽子 氏（株式会社ブルーオーキッドコンサルティング 取締役、情報処理安全確保支援士、中小企業診断士） |
| 名古屋 第2回<br>（11/20） | 櫛田 康仁 氏（櫛田経営と IT 相談事務所 代表・情報処理安全確保支援士、IT コーディネータ、CISA）<br>高橋 真悟 氏（インフォシア 代表・情報処理安全確保支援士、社会保険労務士)<br>寺島 敬 氏（情報処理安全確保支援士、応用情報処理技術者） |
| 埼玉 第２回<br>（11/25） | 浅井 隆弘 氏（情報処理安全確保支援士、システム監査技術者、QMS 主任審査員、EMS 主任審査員、ISMS 審査員）<br>高橋 直也 氏（情報処理安全確保支援士、監理技術者（電気通信））<br>田神 正志 氏（情報処理安全確保支援士、ネットワークスペシャリスト） |

図表 2-4 個別相談対応専門家一覧

### 2.1.4. 広報その他イベント実施に向けた準備作業

イベント実施に向けて、あらかじめ設定されていた日程に基づき、各商工会議所の会場予約手続きを行った。前半の講演パートに加え、後半の個別相談パートがあることから、会場の前半分のレイアウトはスクール形式に、後半分のレイアウトは相談ブースとして島型形式でかつ間仕切りを配置した。なお、この会場レイアウトについては、参加者数の推移を見ながら適宜変更を行い、開催直前まで調整を続けた。

イベントの広報に際しては、各商工会議所から会員企業向けに案内（チラシ・メールマガジン等）を配布するとともに、関連する地域の経済産業局や経済団体等、及び一般社団法人日本自動車部品工業会（部工会）の協力を得て周知活動を行った。

当日の配布資料については、各会場とも以下を準備した。

・議事次第
・講演資料
［IPA 普及啓発資料］・「中小企業の情報セキュリティ対策ガイドライン 第 3.1 版」（冊子）
・「新・5 分でできる！情報セキュリティ自社診断」（パンフレット）
・「中小企業のためのクラウドサービス安全利用の手引き」（パンフレット）
・「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」（パンフレット）
・その他、商工会議所提供資料等

図表 2-5 相談会配布資料一式

また、相談会までの待ち時間には IPA の映像コンテンツを投影することにしたため、会場 PC に格納する手配を行った。

### 2.1.5. 個別相談会開催イメージ

前半の講演及び施策紹介終了後、同会場後方に設置した相談ブース（各会場 3 か所または 4 か所設置）において、セキュリティ専門家による個別相談会を開催した。

相談は 1 社あたり原則 20 分間とし、セキュリティ専門家 1 人あたり 2～3 社の相談に対応いただいた。

個別相談の実施イメージは以下の写真のとおりである。

図表 2-6 相談会の様子

相談会における相談がよりスムーズに進むように、個別相談に参加申込者に対し、事前に E メールにて当日の相談予定内容を聞き取った。この内容に基づき、事務局にて、対応いただくセキュリティ専門家の専門分野等を考慮した上で、相談会のタイムテーブル作成と割り振りを行った。またこれらの企業情報については、事前にセキュリティ専門家に共有し、短時間でできるだけ深い内容の相談が進められるよう工夫した。

相談後は、事務局が準備した WEB フォームにより、各セキュリティ専門家が個別相談レポートを作成し提出した。レポートでは個別の相談内容、セキュリティ専門家がアドバイスを行った内容に加え、後続のマネジメント指導（テーマ別）の参加希望についても併せて聞き取った。相談内容はなるべく詳細に記載することとし、業種や業界、指導内容等、後続のマネジメント指導におけるセキュリティ専門家とのマッチングに活用できる情報取得を試みた。

### 2.1.6. サイバーセキュリティ相談会分析

（１） 全体の参加率

サイバーセキュリティ相談会には、3 商工会議所合計で 105 社（122 名）からの参加があった。申込数に対する参加率は 3 地域とも高く、全体で約 85%に達した。通常の商工会議所におけるセミナーの参加率は６～７割程度であることから、相談会の参加者は、明確な目的意識のもと申し込みを行ったことがうかがえる。

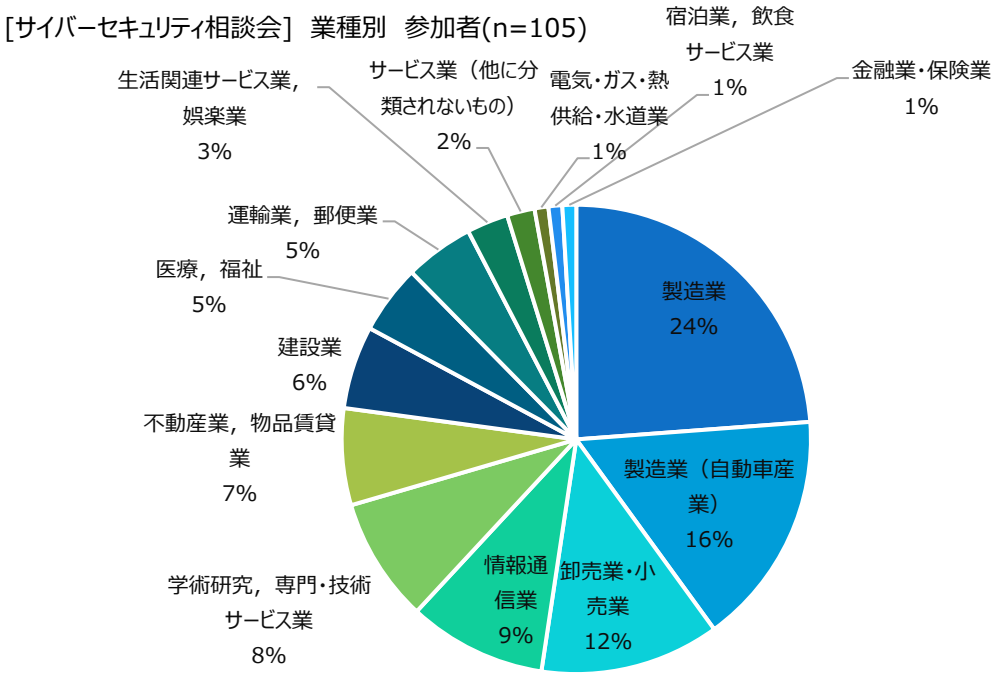
【地域別サイバーセキュリティ相談会の申込・参加状況】

| | 大阪 | 名古屋 | 埼玉 |
|---|---|---|---|
| 相談会申込数（社数） | 68 | 35 | 19 |
| 相談会参加数（社数） | 52 | 34 | 19 |
| 参加率 | 76% | 97% | 100% |

図表 2-7 サイバーセキュリティ相談会参加申込者数、参加者数、参加率

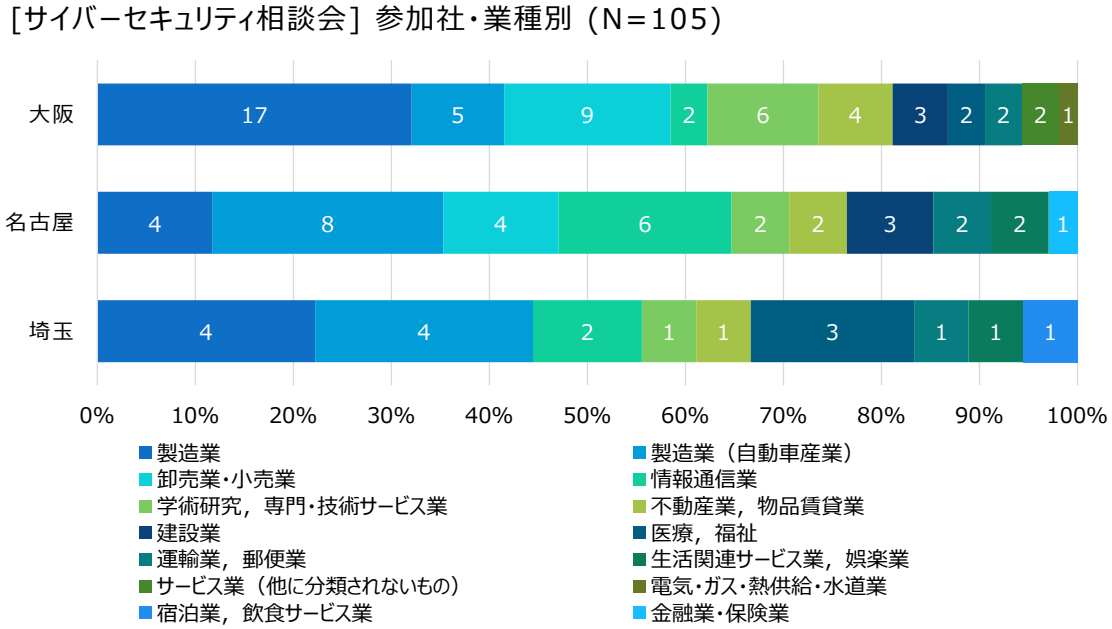
（２） 参加企業の業種分布

業種別相談会の主な参加状況は以下のとおり、製造業：25 社（24%）、製造業（自動車産業）：17 社（16%）、卸売業・小売業：13 社（12%）、情報通信業：10 社（9%）、学術研究・専門・技術サービス業：９社（8%）となった。




図表 2-8 サイバーセキュリティ相談会参加者の業種別割合

上記を地域別に分けた結果は下記のとおりである。




図表 2-9 サイバーセキュリティ相談会参加者の業種別割合（地域別）

３地域に共通して製造業、並びに製造業（自動車産業）からの出席が全体の 35%～45%を占めた。

地域別の傾向は、大阪において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。一

方、名古屋では製造業、特に自動車産業からの参加が顕著であり、地域特性が表れる結果となった。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。

### 2.1.7. サイバーセキュリティ相談会参加者アンケート分析

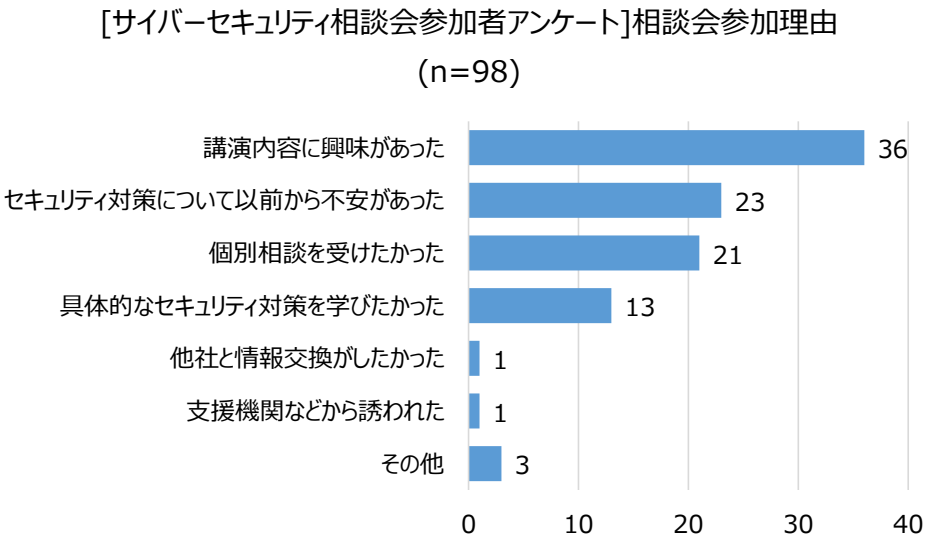
相談会の参加者に対して、終了後にアンケートを実施した。以下、その分析結果（抜粋）について説明する。

■アンケート回答者数

| 日程・会場 | 埼玉① 10/15 | 名古屋① 10/21 | 大阪① 10/24 | 大阪② 11/18 | 名古屋② 11/20 | 埼玉② 11/25 | 合計 |
|---|---|---|---|---|---|---|---|
| 回答者数 | 5 | 19 | 23 | 21 | 17 | 13 | 98 |

図表 2-10 アンケート回答者数

（1） 参加者の参加動機



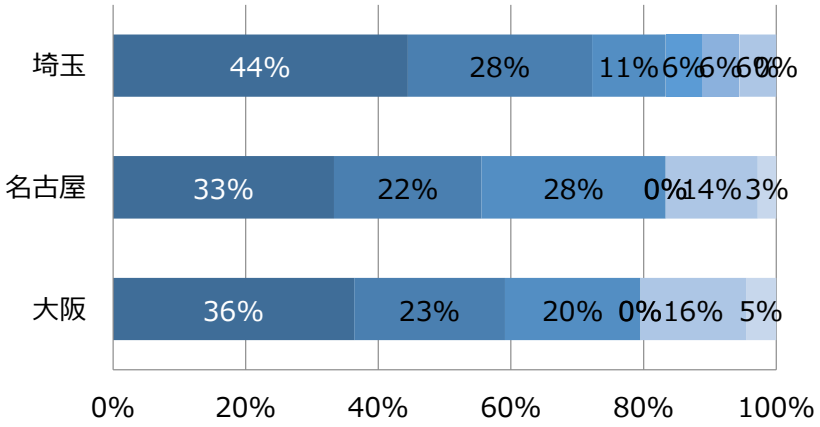

図表 2-11 サイバーセキュリティ相談会への参加理由

参加者アンケートによると、相談会参加への動機について、「講演内容に興味があった」、「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 60%超を占めた。

「個別相談を受けたかった」、「具体的なセキュリティ対策を学びたかった」と回答した 34%と比較すると、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、具体的な対策を求めた参加者と比べて約 2 倍いたことになる。

なお、地域別参加動機は下記の表のとおり。

[サイバーセキュリティ相談会参加者アンケート] 地域別 相談会参加動機
（n =98)




| | 大阪 | 名古屋 | 埼玉 |
|---|---|---|---|
| 講演内容に興味があった | 36% | 33% | 44% |
| セキュリティ対策について以前から不安があった | 23% | 22% | 28% |
| 個別相談を受けたかった | 20% | 28% | 11% |
| 支援機関などから誘われた | 0% | 0% | 6% |
| 他社と情報交換がしたかった | 0% | 0% | 6% |
| 具体的なセキュリティ対策を学びたかった | 16% | 14% | 6% |
| その他 | 5% | 3% | 0% |

図表 2-12 サイバーセキュリティ相談会への参加理由（地域別）

参加動機における地域差は見られず、共通して個社の具体的な対策前の準備段階（情報収集段階）にいる参加者が、全体の 6 割～7 割を占めている。

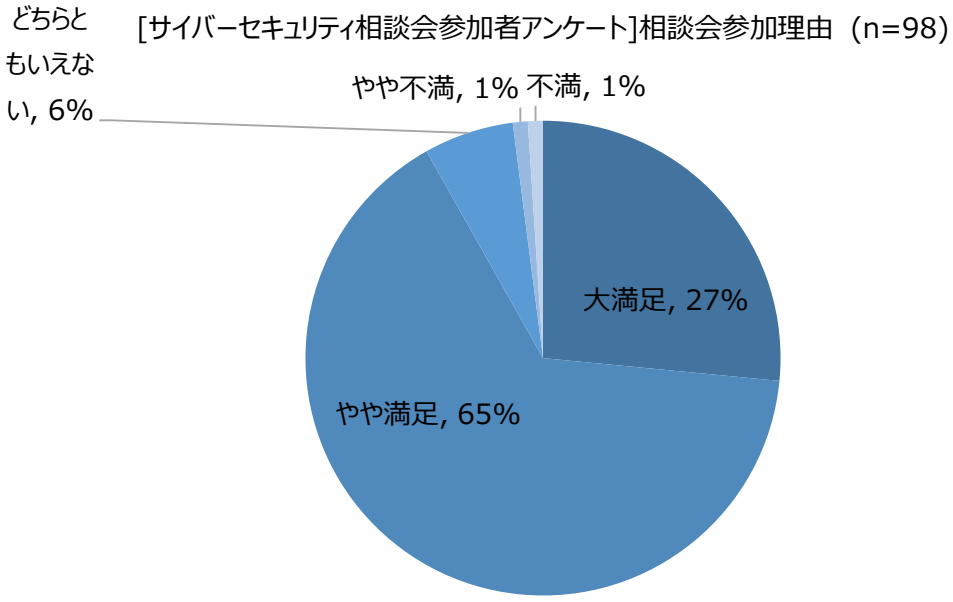
（２）　参加者の満足度

アンケート回答者の約 92%が、サイバーセキュリティ相談会への参加を「満足した」と回答。

具体的な理由については、サイバーセキュリティ対策を進めるための具体的なツールやサービス、直近のサイバーセキュリティの動向についての情報収集が可能であったとの声が多く聞かれた。

詳細コメントは以下のとおり：

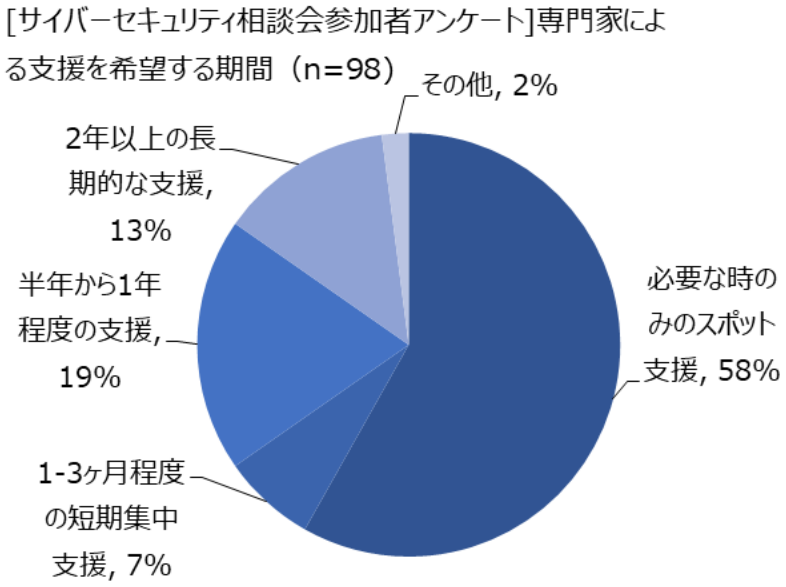
- 無償サービスが豊富にあることを知ることができて良かった。
- 情報セキュリティポリシーのテンプレートがあることを知ることができた。
- 中小企業の情報セキュリティ対策ガイドライン、５分でできる！情報セキュリティ自社診断のチェックリスト等がもらえた。参考にして社内規程を設けたい。
- 直近のサイバーセキュリティ事情を知ることができた。
- セキュリティの脅威が何年も変わっていないことを初めて知った。




図表 2-13 相談会の満足度

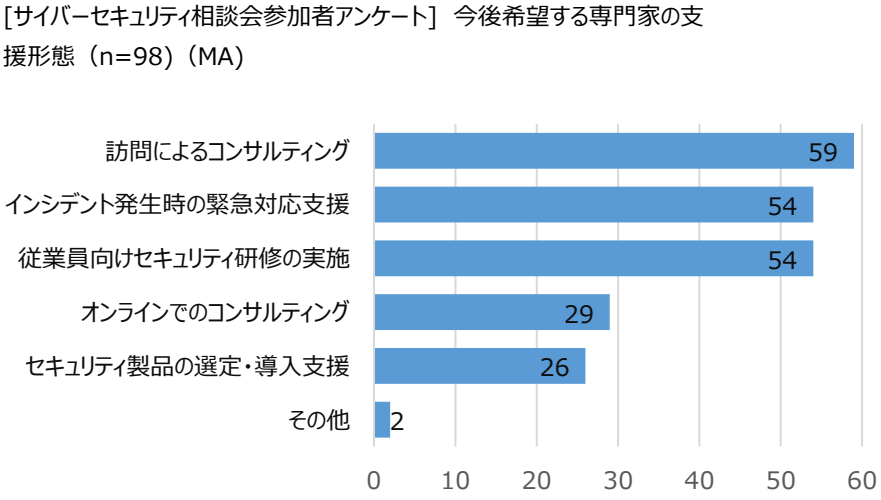
（３）　支援期間、形態の希望

希望するセキュリティ専門家による支援期間の選好として、「必要な時のみのスポット支援」を希望する企業が全体の 58%を占めた。一方で、「長期的な支援」を望む企業も全体の約 40%に達し、ニーズの多様性が示唆された。




図表 2-14　セキュリティ専門家による支援を希望する期間

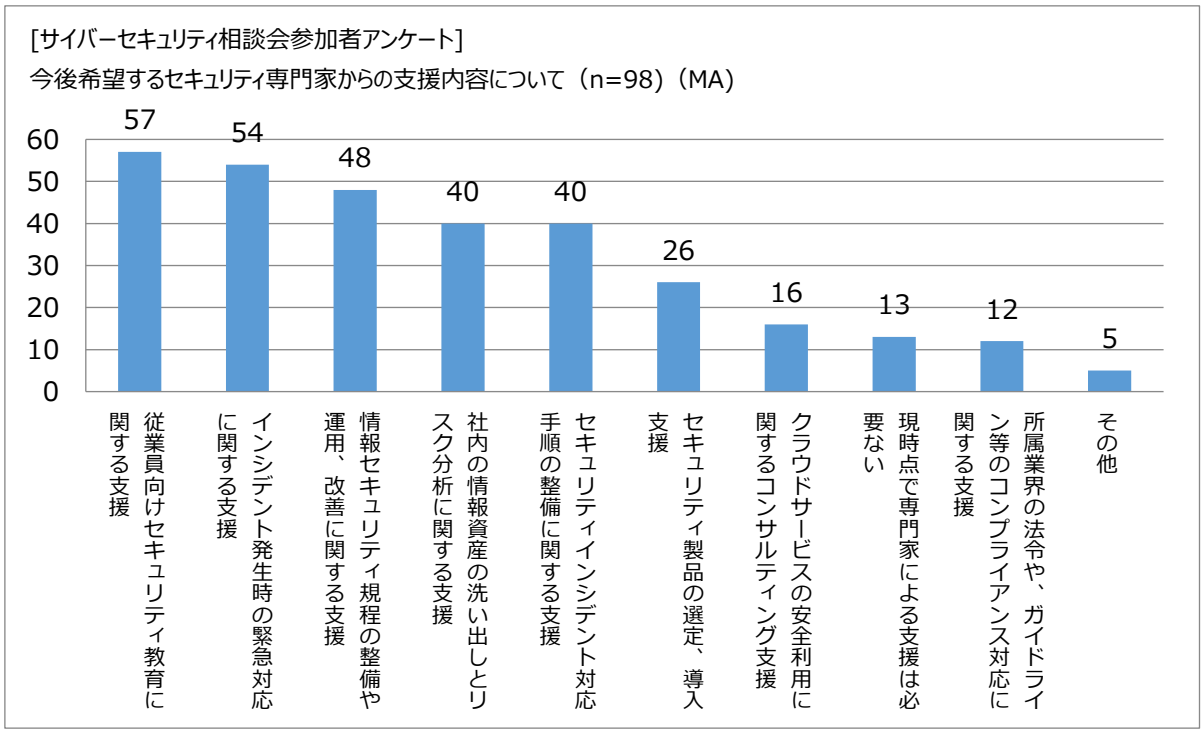
また、今後希望するセキュリティ専門家の支援形態は、「訪問によるコンサルティング」、「インシデント発生時の緊急対応支援」、「従業員向けセキュリティ研修の実施」を望む企業が全体の約 50%以上を占め、訪問方式の希望はオンライン方式の 2 倍であった。




図表 2-15　今後希望するセキュリティ専門家による支援の形態

（４）　支援内容の希望

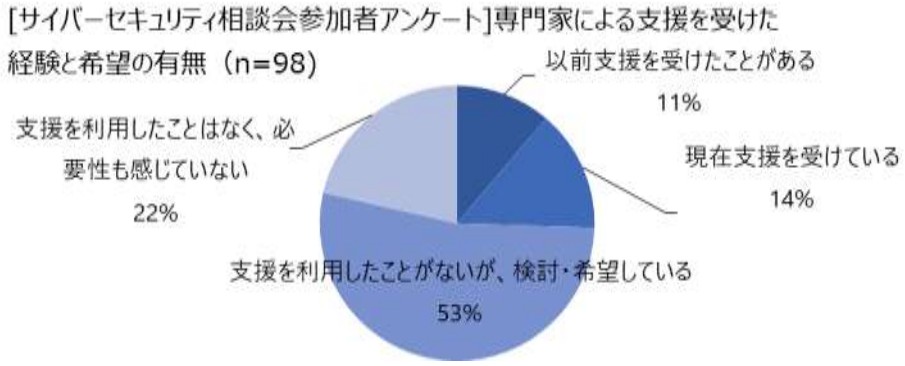
最も希望するセキュリティ専門家からの支援内容の上位３項目は、「従業員向けセキュリティ教育」（57 件）、「インシデント発生時の緊急対応」（54 件）、「情報セキュリティ規程の整備」（48 件）であり、スポット的なニーズへの対応と長期的な取組み対応ニーズの両方があることが示された。




図表 2-16　今後希望するセキュリティ専門家からの支援内容

（５）　支援を受けた経験と今後の希望

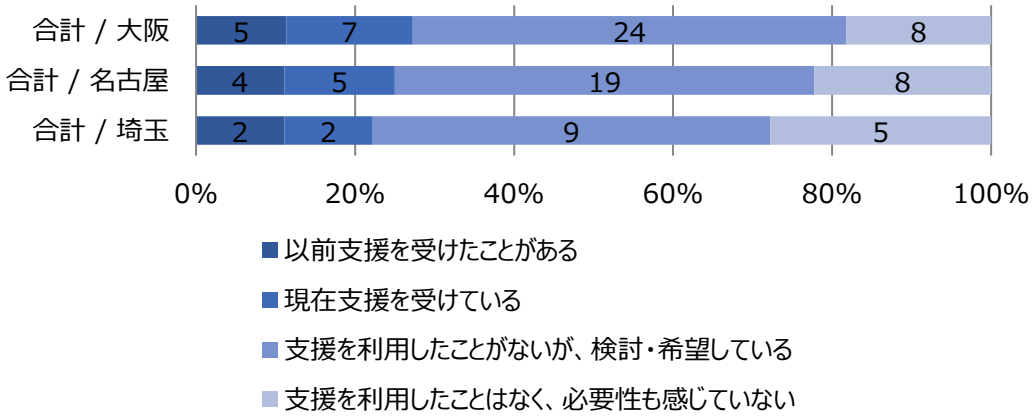
セキュリティ専門家によるセキュリティ支援を希望、検討している企業は全体の 53%であった。過去に支援を受けた経験のある企業を含めると、全体の 78%がセキュリティ専門家によるセキュリティ対策支援を現実的な手段として認識していることが明らかになった。




図表 2-17　セキュリティ専門家による支援を受けた経験・希望の有無

上記の結果を地域別別に見た結果は下記のとおり。

[サイバーセキュリティ相談会参加者アンケート]地域別　専門家による支援を受けた経験と希望の有無　（n=98）



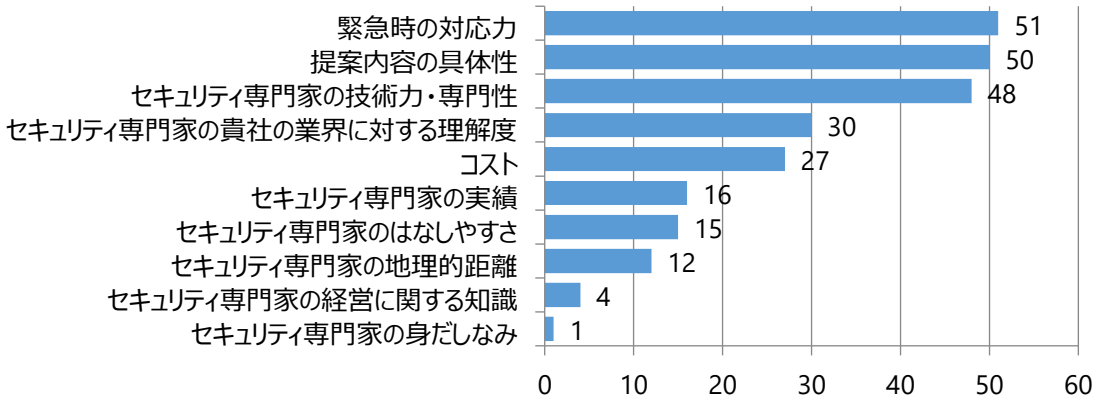

図表 2-18　セキュリティ専門家による支援を受けた経験・希望の有無（地域別）

支援経験における地域差は見られない。大阪・名古屋に比べ、埼玉では 10%ほど、支援の必要性を感じていない層が多い。

（６）　セキュリティ専門家の選定基準

アンケート回答者のセキュリティ専門家を選ぶ基準は「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。「緊急時の対応力」とは、インシデント発生時の対応を意味していると解されるので、多くのアンケート回答者にとって、セキュリティ専門家の選定は、いざという時の対応を重視していることがうかがえる。

[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)



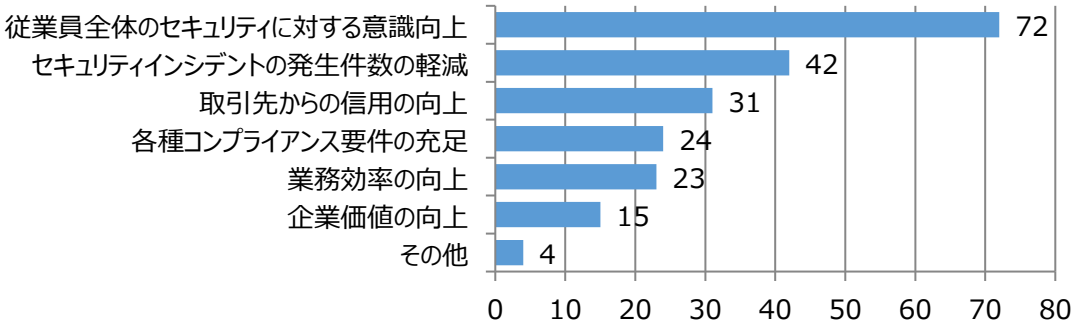

図表 2-19　セキュリティ専門家の選定基準

（７）　セキュリティ対策に期待する効果

セキュリティ対策の効果として重視する指標で最も多く回答を集めたのは「従業員全体のセキュリティに対する意識向上」で（73%）、続いて「セキュリティインシデントの発生件数の軽減」、「取引先からの信用の向上」であった。「従業員全体のセキュリティに対する意識向上」が「セキュリティインシデントの発生件数の軽減」、「取引先からの信用の向上」、「各種コンプライアンス要件の充足」を上回ることから、回答者の多くは本格的なセキュリティ対策の実装イメージが明確でない様子がうかがえる。

また、「取引先からの信用の向上」も、３割に達し、サプライチェーンセキュリティへの意識が浸透しつつある様子も示唆された。

[サイバーセキュリティ相談会参加者アンケート]セキュリティ対策の効果として重視する指標(n=98)(MA)（3つまで）

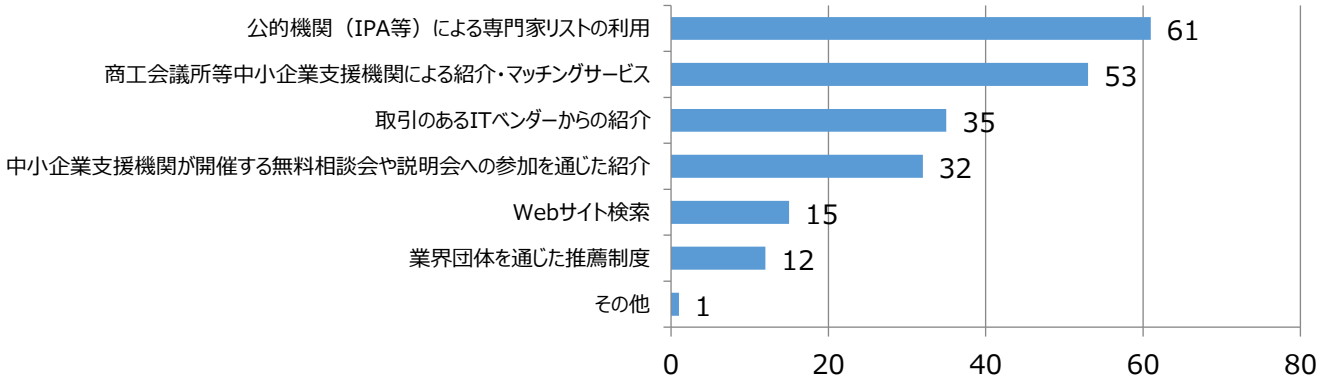



図表 2-20　セキュリティ対策の効果として重視する指標

（８）　希望するセキュリティ専門家の検索ルート

セキュリティ専門家の探索方法には「公的機関（IPA 等）によるセキュリティ専門家リストの利用」、「商工会議所等の中小企業支援機関による紹介」が上位にあがった。また、「取引のある IT ベンダーからの紹介」も約３割が選択した。

[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)




図表 2-21　セキュリティ専門家の探し方についての希望

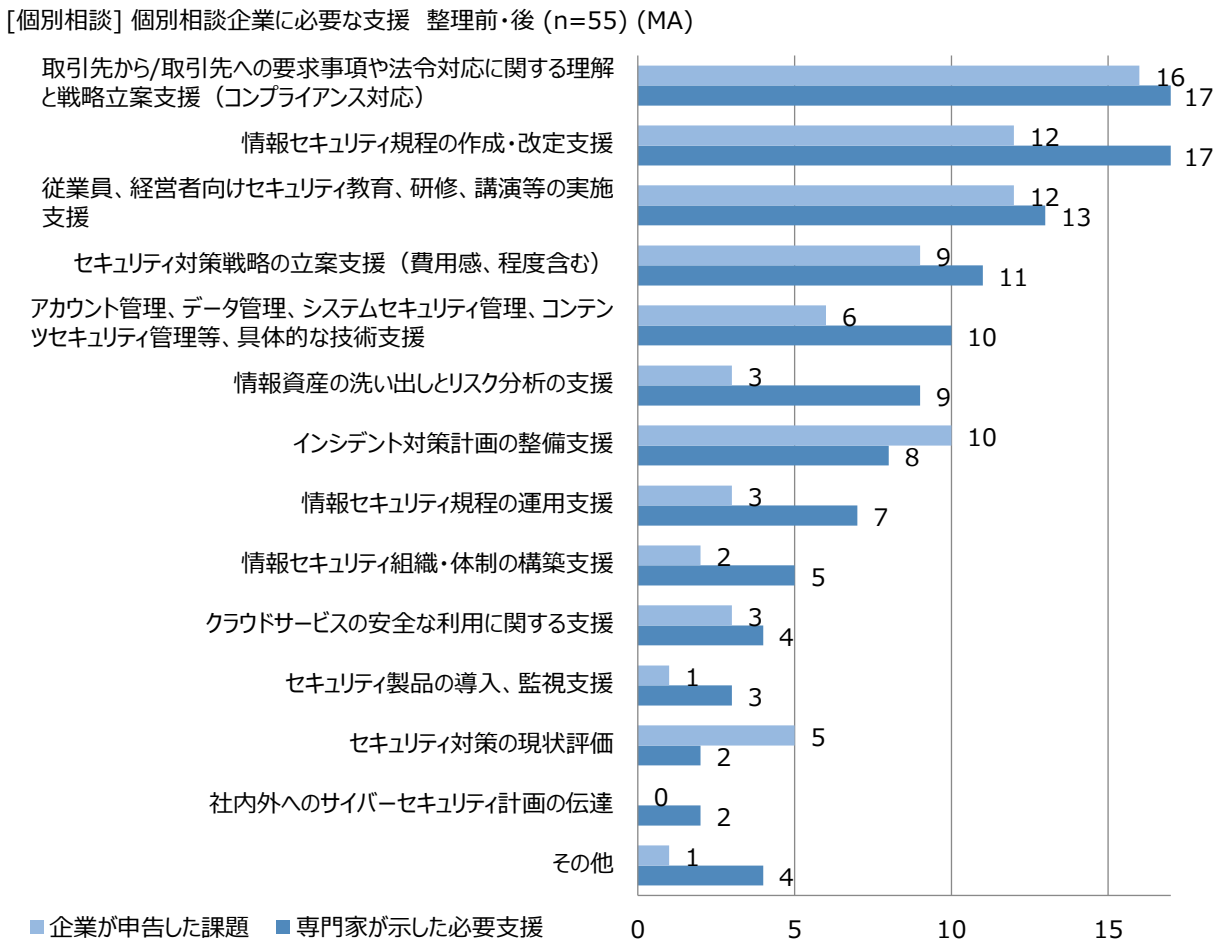
### 2.1.8. 個別相談分析

（１） 個別相談者の課題の整理

個別相談に参加した企業が当初認識していた課題と、セキュリティ専門家が相談を通じて見極めた実際の課題との間には、ギャップがあることが確認された。

特徴的な例として、「情報資産の洗い出しとリスク分析」は企業側の申告では 3 件であったのに対し、セキュリティ専門家の診断では 9 件と判断され、また「情報セキュリティ規程の作成・改定」についても申告の 12 件から実際には 17 件へと増加した。これらは企業自身が必要性を認識していなかったものの、セキュリティ専門家の視点から重要な対策として見出された支援であると考えられる。

一方で、「セキュリティ対策の現状評価」は申告の 5 件から実際には 2 件へ、「インシデント対策計画整備」は申告の 10 件から 8 件へと減少した。これらは企業が課題として認識していたものの、セキュリティ専門家の診断により、より優先度の高い別の支援が必要と判断されたケースといえる。



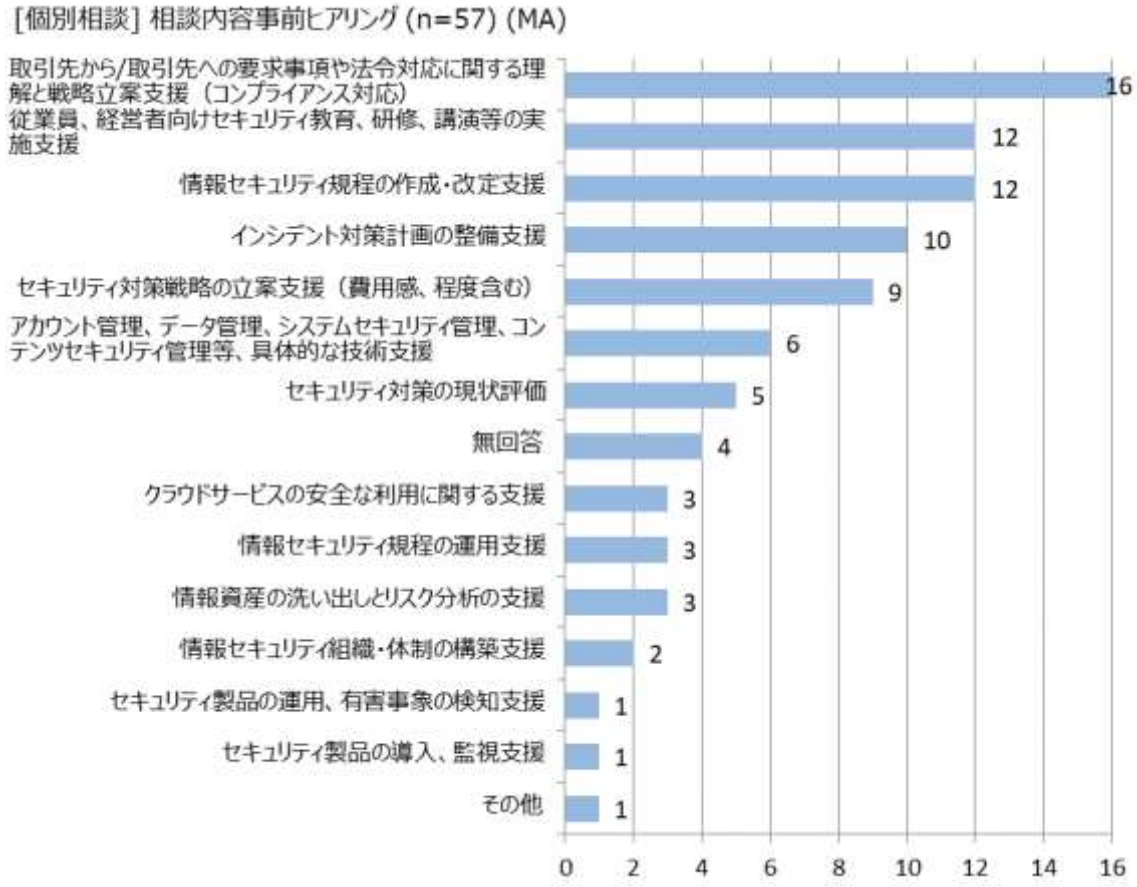

図表 2-22 個別相談企業が申告した課題と、セキュリティ専門家が示した支援内容のギャップ

これらのギャップは、企業の自己認識には限界があるということと、適切な支援内容を見極める上でセキュリティ専門家の専門性が重要な役割を果たすことを示しており、支援を開始する前段階において個別相談を実施することの有効性を示唆している。

（ア） 相談内容 ヒアリング結果

サイバーセキュリティ相談会の開催前に、個別相談の申込者に対して、事前のメールによるヒアリングを実施し、相談予定の課題について確認した。

相談予定の上位課題は、「取引先から・取引先への要求事項や法令対応」、「従業員、経営者向けセキュリティ教育、研修、講演等」、「情報セキュリティ規程の作成・改定支援」、「インシデント対策計画の整備支援」であった。

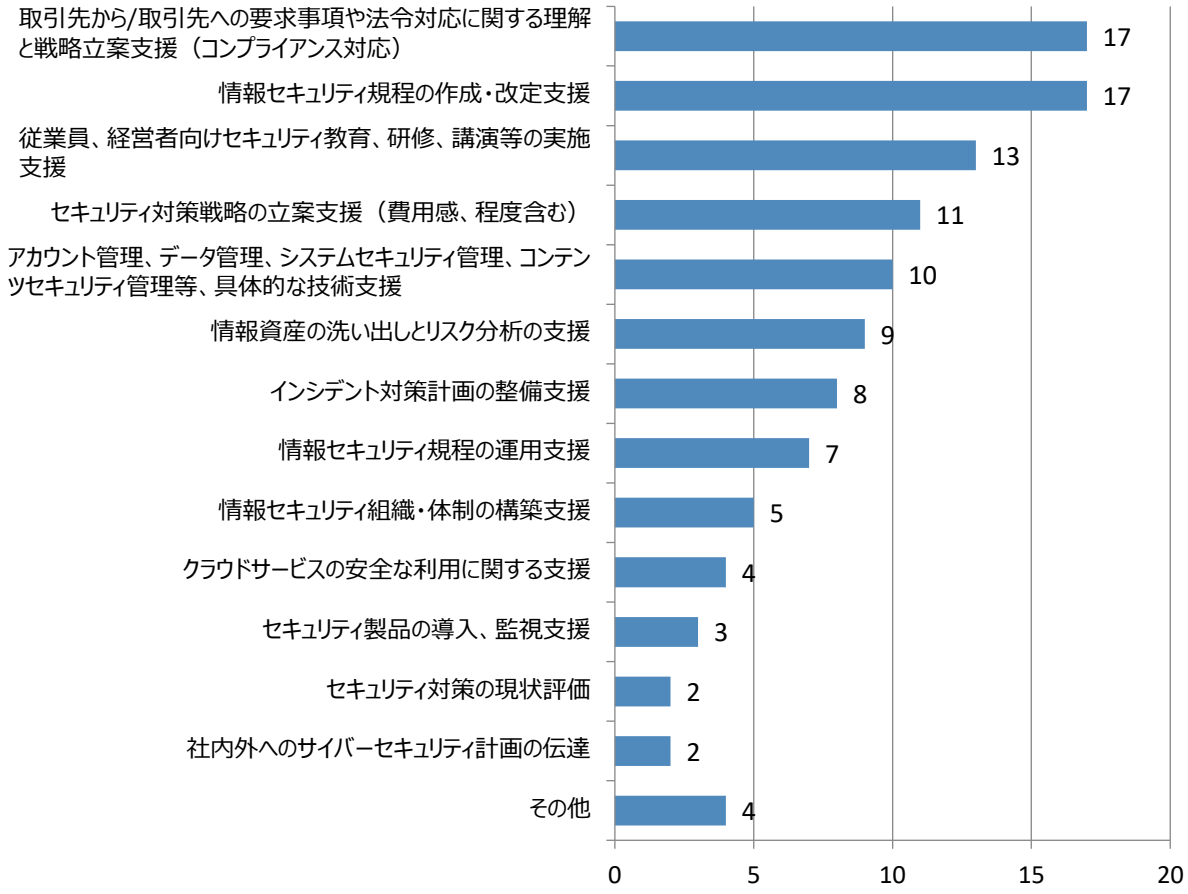



図表 2-23 個別相談申込者への相談内容に関する事前ヒアリング結果

（イ）　セキュリティ専門家による整理

セキュリティ専門家が個別相談を通じて企業の課題を、その背景も含めて整理した結果が下の表である。「情報セキュリティ規程の作成・改定支援」と「取引先からの要求事項・法令対応支援」がそれぞれ 17 社と最も多く、次いで「従業員向けセキュリティ教育」が 13 社、「セキュリティ対策戦略の立案支援」が 11 社、「基本的な技術支援（アカウント管理等）」が 10 社という結果となった。規程整備や法令対応といった基盤的な部分での支援が求められている。

[個別相談] 個別相談企業に必要な支援 (n=55) (MA)

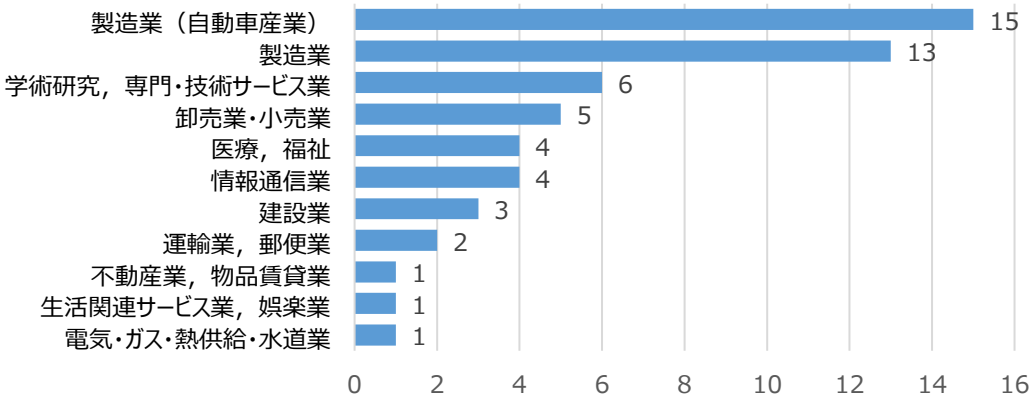



図表 2-24　セキュリティ専門家が整理した個別相談企業に必要な支援内容

（２）　個別相談　業種別参加企業

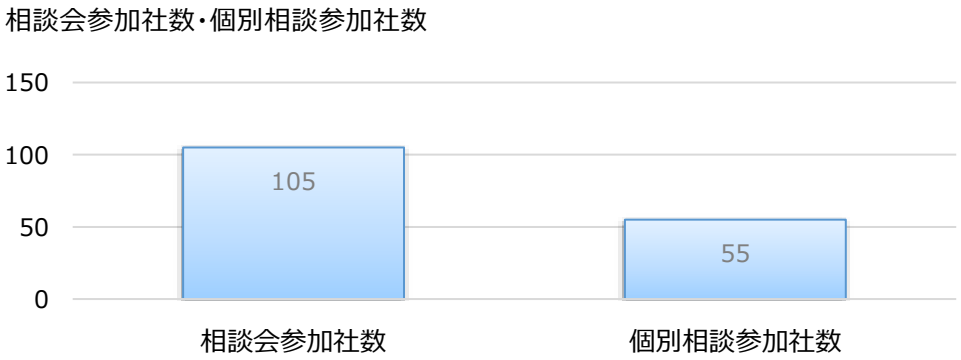
個別相談へ参加した企業は、「製造業(自動車産業)」、「製造業」「学術研究、専門・技術サービス」の３業種が最も多かった。

[個別相談]　参加社・業種別　（n＝55）



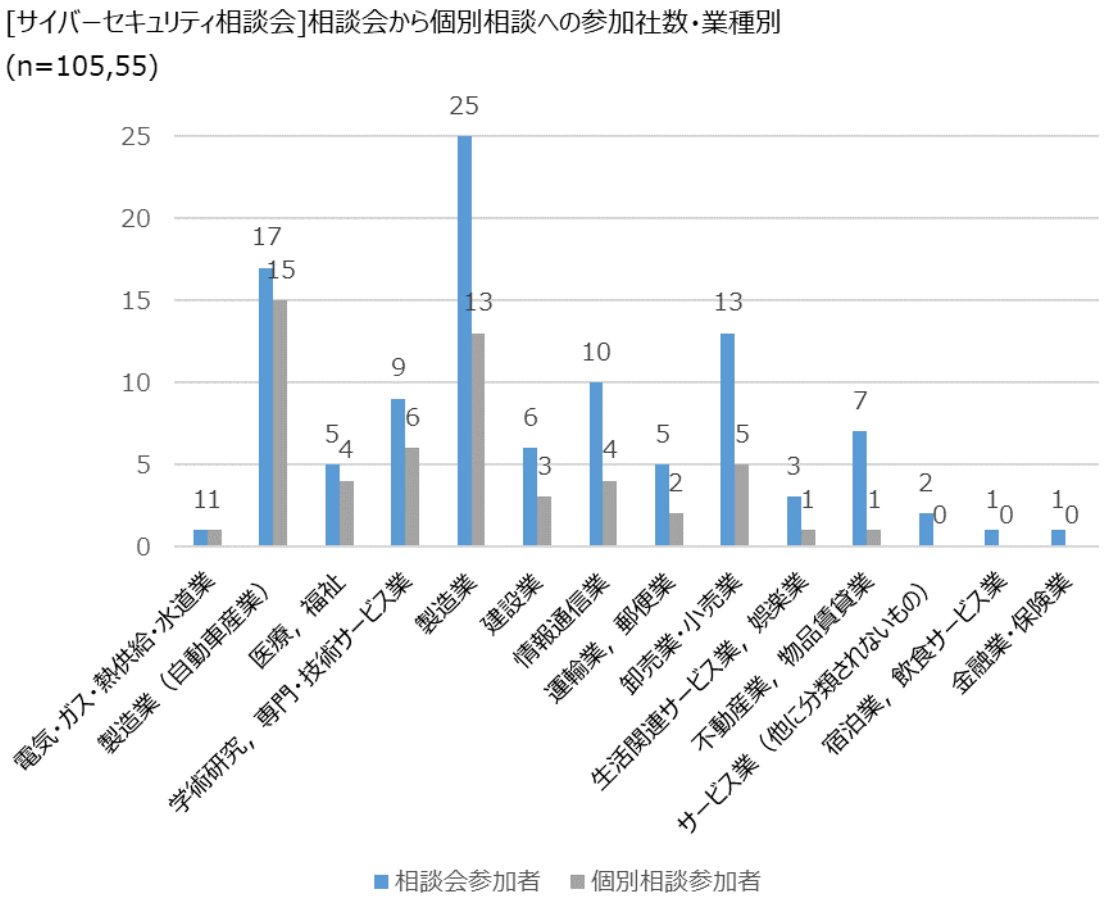

図表 2-25　個別相談参加企業の業種内訳

また、相談会から個別相談への移行率は以下のとおり。




図表 2-26　相談会から個別相談への移行率

相談会から個別相談への移行した企業は参加者の 52%であった。約半数が個別相談を受けたことになる。業種別移行率は、「電気・ガス・熱供給・水道業」、「製造業（自動車産業）」、「医療・福祉」が最も高く、相談会参加者の８割以上が個別相談に移行した。




図表 2-27 相談会から個別相談へ移行した参加社数（業種別）

製造業はサイバーセキュリティ相談会において最多の参加数（25 社）を記録したものの、個別相談への移行率は 50%（25 社から 13 社）にとどまった。個別相談実施企業数の 22%を占める大きな割合ではあるが、移行率の観点からは他業種と比較して特に強いニーズがあるとは言えない状況である。

一方、製造業（自動車産業）については、相談会参加者全体の 16%（17 社）という比較的少ない参加数ながら、そのうちの 88%（15 社）が個別相談に移行しており、業界として高い関心とニーズの存在が示唆された。同様に、規制産業（電気・ガス・熱供給・水道業、医療・福祉）については、相談会への参加数こそ少なかったものの、個別相談への移行率は 80-100%という高い値を示した。また、学術研究・専門・技術サービス業においても 67%の移行率が確認され、これらの業種における支援ニーズが示された。

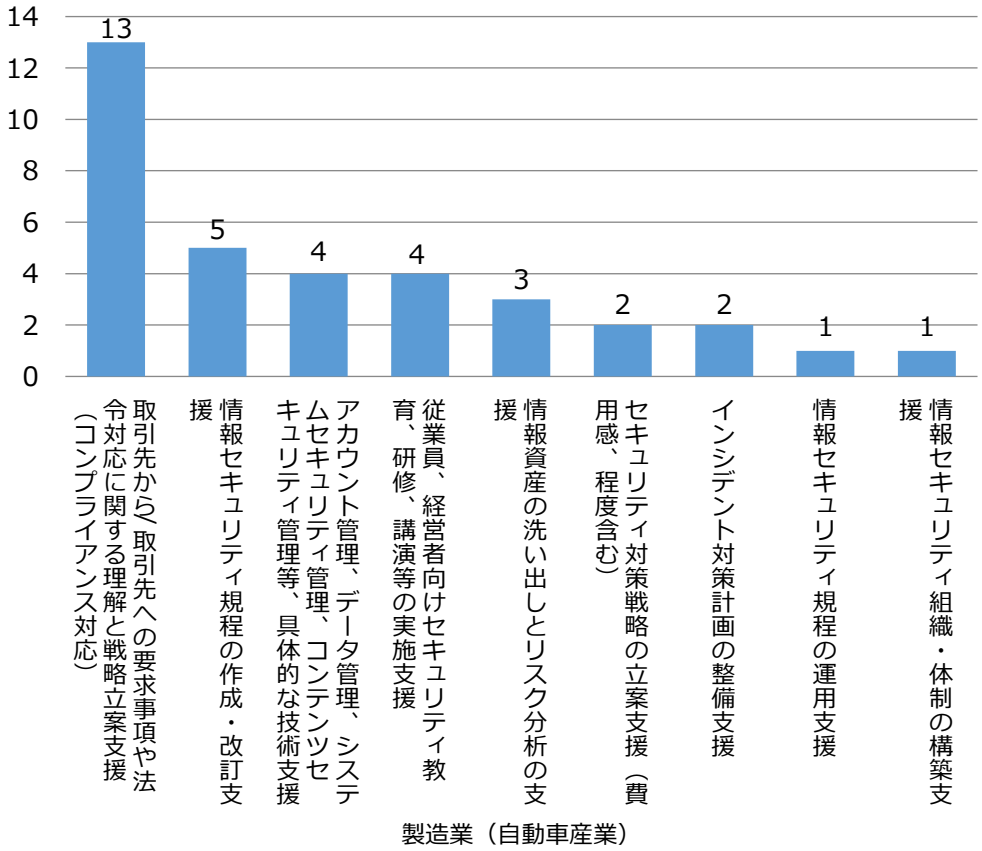
移行率上位 4 業種の相談内容傾向を次項に示す。

（３）　個別相談への移行率　上位４業種における個別相談

（ア）　製造業（自動車産業）

製造業（自動車産業）の企業からは、自工会ガイドラインへの対応に関する相談が寄せられた。相談事例としては、「情報セキュリティ規程の作成」、「インシデント対策（対応訓練）」、「従業員教育」、「情報資産台帳の作成」、「共有 PC の管理方法」等があり、いずれも、中小企業が取引先から要求された対応事項について、具体的な実施方法が分からず、セキュリティ専門家に指南を求めているような相談であった。

[個別相談]「製造業（自動車産業）」における必要支援（n=15）（MA）




図表 2-28　製造業（自動車産業）分野において必要とされる支援

[相談事例]

■情報セキュリティ規程の作成

・昨年より業界団体（自動車業界）によるセキュリティガイドラインへの適用が強く求められていることもあり、本年の年末までにはセキュリティ規約一式を規定することで、ガイドラインにも対応を取っていきたいと考えている。

・情報セキュリティ規程の整備 2024 年度内に自動車産業サイバーセキュリティガイドライン（レベル１）の達成を予定している。

・取引先から毎年、情報セキュリティに関するアンケートが来るが、できていないことが多く、三段階評価の一番低い評価になっている。取引先の評価を上げるため、情報セキュリティ規程を作りたいが、どのような内容にしたら良いかわからない。
・取引先からの要請で、情報セキュリティ規程の整備が必要。

■インシデント対応
・IATF の要求の中にウイルス感染などへの対応訓練が求められている。どのように実施すれば良いのか
・インシデント対応などどこまで義務付けられているのかのレベル感が分からず、どう対応していいのかがわからない

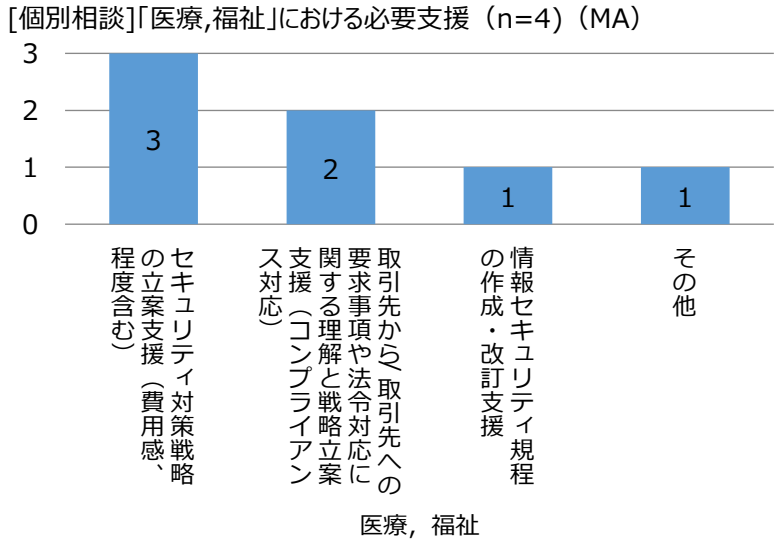
■従業員教育
・自工会サイバーセキュリティ対応として、従業員教育を実施している。愛知県警にも相談してセキュリティ教育を実施している毎回 16%の従業員がダミーウィルスに感染してしまい、よい方法はないか？
・自工会サイバーセキュリティガイドラインの対策項目の判断で教育方法がよくわからない。
・ノートパソコンを外に持ち出すことのある外回りの営業・設計担当者に対してセキュリティ意識向上の研修を行いたい。
・情報セキュリティ教育をどう実施したらいいかわからない

■情報資産台帳の作成
・情報資産台帳の作成方法がわからない。
・自工会の情報資産のチェックシートに沿って台帳は作成。その他情報セキュリティの態勢整備を行っている。その整備について十分であるか否かなどを確認してほしい。

■共有 PC/アカウント管理
・共有アカウントを使用しているため、操作ログの個人判別とパスワードの課題がある。どのように解決すればいいのかわからない。

（イ） 医療、福祉

医療・福祉分野における企業の支援ニーズを分析すると、最も多かったのが「セキュリティ対策戦略の立案支援」であり、特に対策の費用感や実施程度に関する具体的な指針を求める声が目立った。次いで「取引先から/取引先への要求事項や法令対応に関する理解と戦略立案支援」へのニーズが高く、これは医療情報システムのガイドラインや個人情報保護法などへの対応要請を反映したものと考えられる。



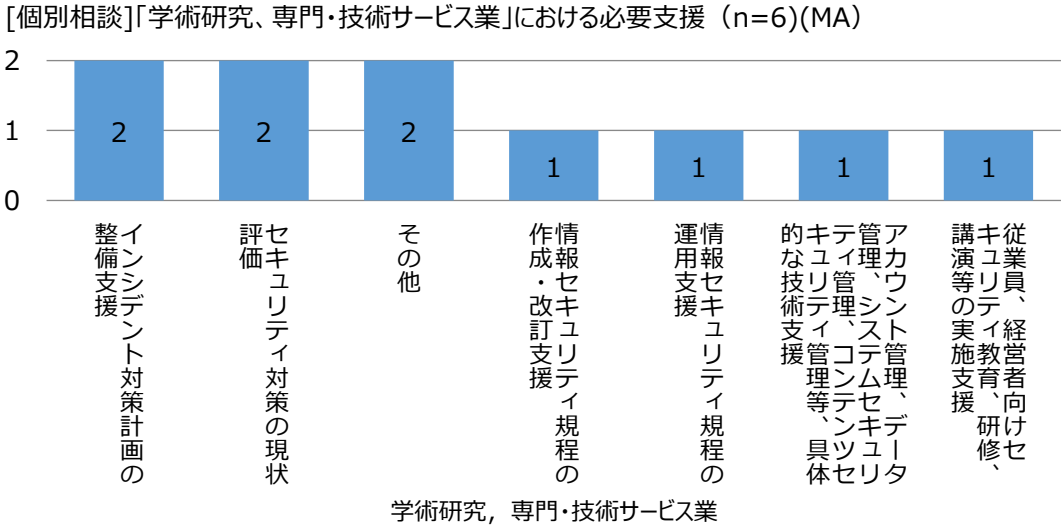

図表 2-29 医療・福祉分野において必要とされる支援

（ウ） 電気・ガス・熱供給・水道業

電気・ガス・熱供給・水道業においては、参加企業が 1 社のみで、規程の整備が必要であったとのこと。

（エ） 学術研究、専門・技術サービス業

個別相談への移行率が 70%弱で 4 番目に高く、必要とされた支援は下記のとおり。



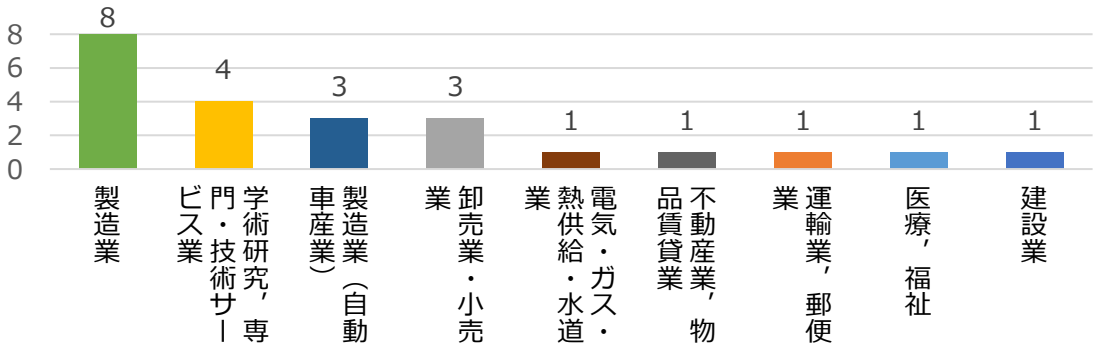

図表 2-30 学術研究、専門・技術サービス業分野において必要とされる支援

（４）　地域別・個別相談分析

（ア）　大阪

大阪で最も多かった個別相談企業の業種は「製造業」であった。

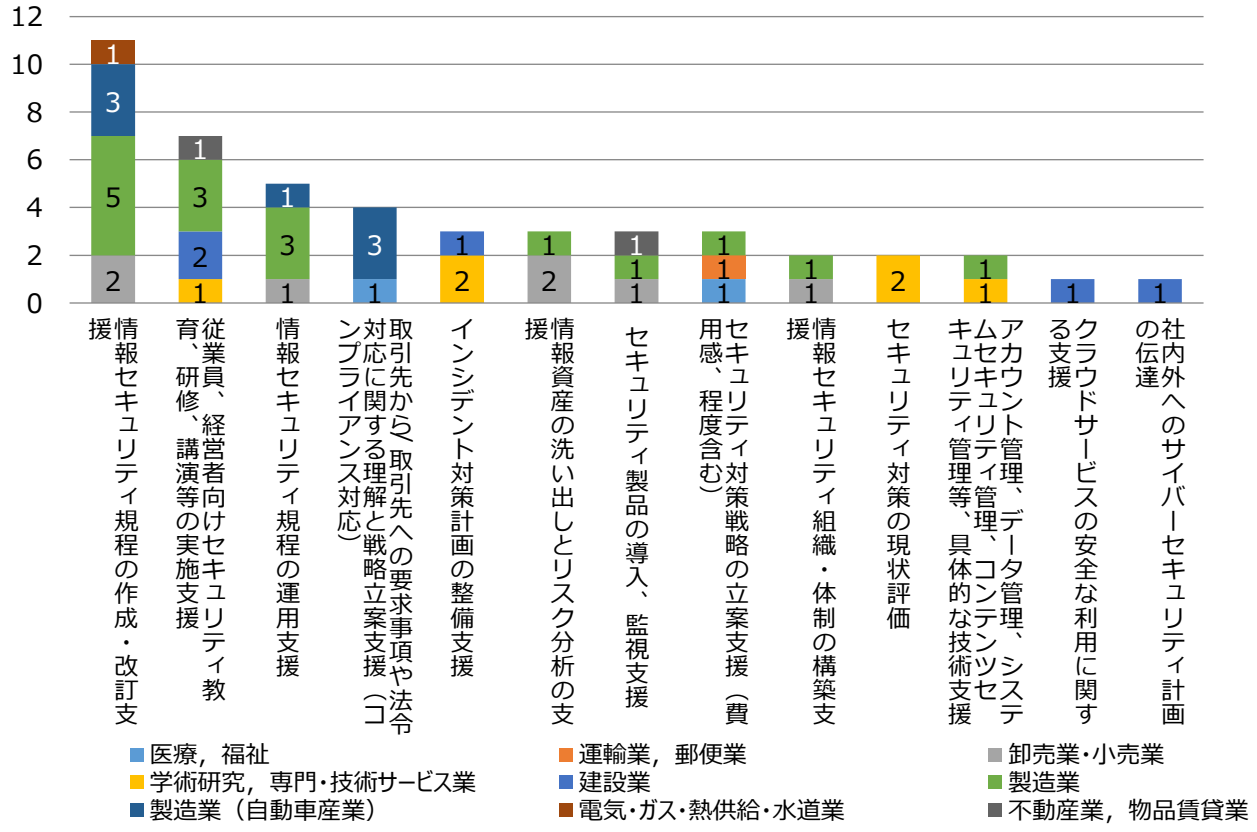
[個別相談][大阪]　参加社・業種別(n=23)




図表 2-31　個別相談参加企業の業種内訳（大阪）

最も必要とされる支援は「情報セキュリティの規程の整備」であった。セキュリティ対策の基礎的段階にいる企業が多く参加したことを表している。

[個別相談][大阪] 専門家が示した必要支援・業種別（n=23)(MA)




図表 2-32　個別相談参加企業において必要とされる支援（大阪）

個別相談の内容をみると、大阪では、「IPA 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」、「規程作成したが、今後どのように推進していくか分からない」など、対策の内容、運用方法、進め方についての具体的なアドバイスを求める相談が多かった。

また、「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、この構成でよいのか確かめたい」など、企業は自社のセキュリティ対策について、「これで十分か」、「これが適切か」、「優先順位はこれでよいか」といった観点から、セキュリティ専門家に第三者的な視点での評価を求めていた。具体的には、セキュリティ対策の包括的な妥当性を確認したいという要望が顕著に見られた。

[相談事例]

■情報セキュリティ規程の作成・改定・運用について

・既にあるセキュリティ規程（ハンドブック）が網羅的か、大企業並みの過剰な内容となっていないかレビューいただき、必要に応じてアドバイスが欲しい。
・セキュリティポリシーや規約がほぼない状態。IPA の資料の利用も試みたが、どこまでやればよいのか、正解が何かがわからなくて困っている。
・セキュリティ規程は策定済みだが社内周知の進め方について悩んでいる。また私自身も、インシデント発生時に備えて、何を規程に盛り込むべきかわからない。
・昨年より業界団体（自動車業界）によるセキュリティガイドラインへの適用が強く求められていることもあり、本年の年末までにはセキュリティ規約一式を策定したいと考えている。経営陣のセキュリティ投資への理解が乏しく、予算確保が困難な状況だが、どのように進めていけばいいか。

■セキュリティ対策の初歩段階における漠然としたお悩み

・数百社と取引があり、個人情報、取引口座情報、使用電力情報などの情報が漏えいすると事業存続に関わると考えているが、まだ何も対策ができていない。サイバーセキュリティお助け隊は加入予定だが、他の対策について相談したい。
・弊社の PC は古い物が多く、ほとんどが Windows10。どこから手を付ければいいか、緊急度の相談をしたい。
・特許や商標などの企業秘密の漏洩が心配だが、ファイルサーバのアクセス権の設定も実施できておらず、また、情報セキュリティ関連の規程もない。どこから始めればいいのか。
・同業他社が今年 10 月にサイバー攻撃を受けて業務システムが停止した。必要な対策レベルやインシデント発生時の責任範囲、賠償金額の基準、免責となる対策水準を知りたい。
・総務部兼務でシステムを担当しているが、物理的に離れた工場（従業員 100 名規模）で、ウイルスソフトが入っていない PC を、IT リテラシーの低い高齢の従業員が使用している。どのようにセキュリティ対策を進めていいかわからない。

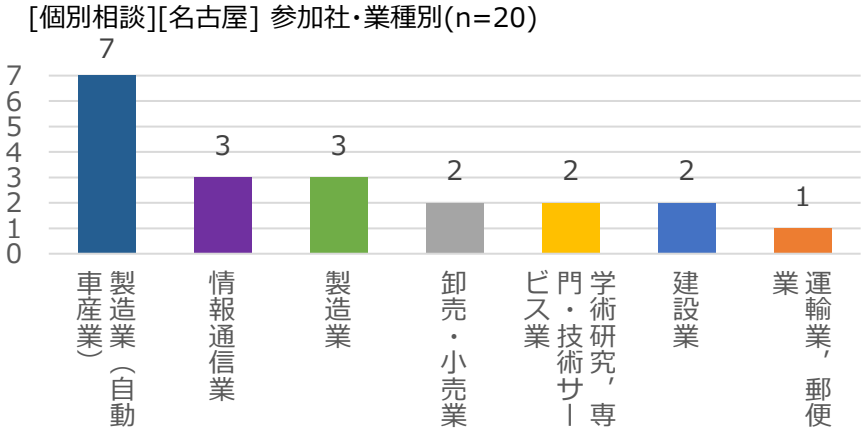
■社内のセキュリティ対策状況の診断について

・ベンダーの提案を受けて構成したシステムを運用しているが、ウイルス感染等のリスクがないか、判断いただきたい。
・社内ネットワークに某社の UTM を導入しているが、監視や不正侵入検知の対応は行っていない。本当に守られているのか。また、お助け隊の監視サービスだけの契約は可能か。
・UTM のレポートを見ても、対処方法がわからない。
・スタッフがサポート詐欺サイトで案内された番号に電話してプログラムをダウンロードしてしまったが、実行前に気づいて中止し、その後ウイルススキャンでは検出されなかったが、タスクマネージャーが起動できない症状が出ている。マルウェア感染が心配である。

■従業員向け教育について
・最近入社したため、IT 活用やセキュリティ教育をすすめようとしても古参社員からの反発が大きい。どのように進めたらよいか。
・PC を使わない人が半数以上を占めている。そういった人達に対するセキュリティ教育はどうすればいいのか。

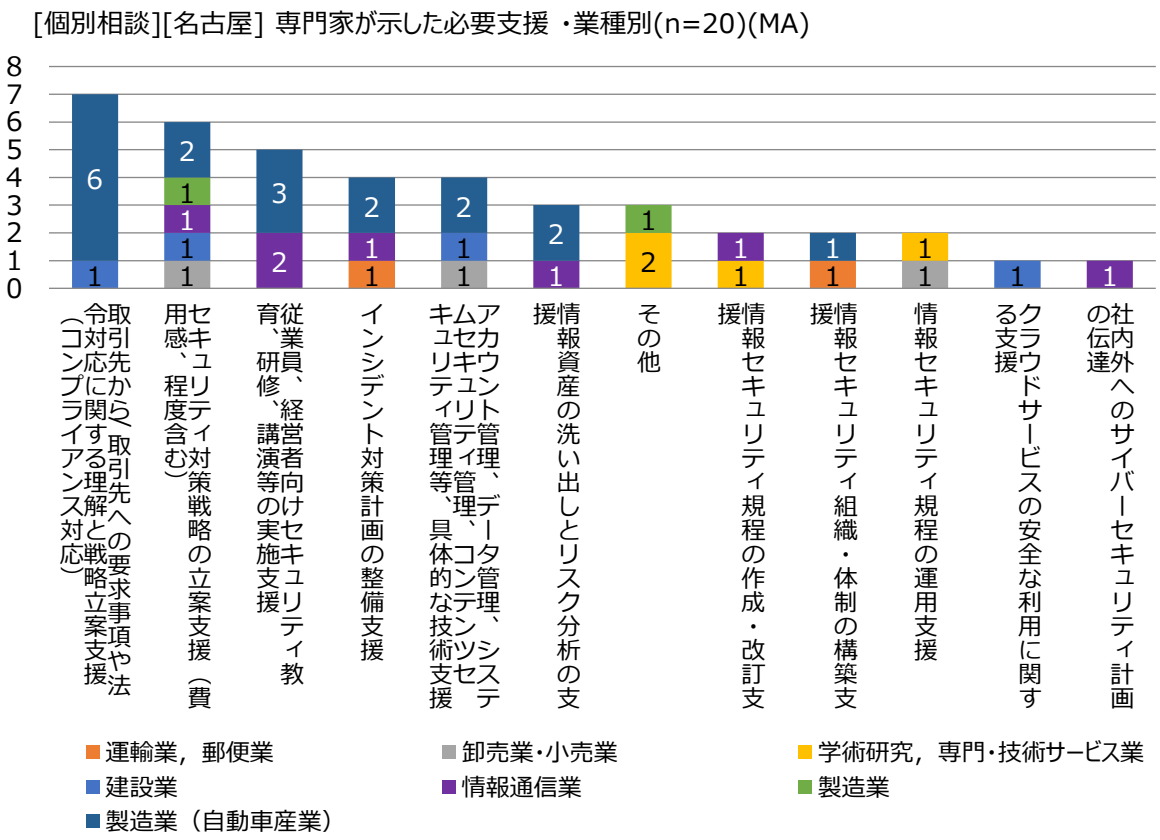
（イ） 名古屋

名古屋の個別相談では、約 35%を「製造業（自動車産業）」が占めた。




図表 2-33 個別相談参加企業の業種内訳（名古屋）

名古屋で個別相談者が最も多く必要とする支援は「取引先から/取引先への要求事項や法令対応」であった。当該支援が必要な相談者の内訳は、製造業（自動車産業）が 6 件、建設業が 1 件であった。




図表 2-34 個別相談参加企業において必要とされる支援（名古屋）

名古屋では、自動車産業における自工会ガイドラインへの準拠など、取引先からの具体的な要求事項への対応に関する相談が顕著だった。これらの相談は、サプライチェーン上の各社企業が取引先との事業継続性を強く意識している現状を浮き彫りにした。

また、FA ネットワークの構築方法や海外取引先への対応、行政書士による登録セキスペの探索方法など具体的な課題を持つ企業や、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があり、各社のセキュリティ課題は、領域や成熟度により多岐に渡っていた。

[相談事例]

■自工会サイバーセキュリティガイドラインへの準拠

・自工会サイバーセキュリティガイドラインの対策項目のうち、教育方法がよくわからない。

・自動車部品メーカーとして取引先からガイドラインへの準拠が求められることが多くなった（自工会ガイドライン、TISAX 認証の取得など）が、特にインシデント対応など、どこまで義務付けられているのか、レベル感が分からない。

・IATF の要求の中にウイルス感染などへの対応訓練が求められているが、どのように実施すれば良いのか分からない。

・自工会サイバーセキュリティ対応として、従業員教育を愛知県警にも相談して実施しているが、メー

ル訓練では社長を始め 16%の従業員がダミーウィルスに感染してしまった。教育方法についてのアドバイスが欲しい。

■取引先のセキュリティ対策
・ベンチャー企業として創業間もない。今後取引先に重要情報を提供する必要があるものの、事業規模が小さいために取引先への要求が難しく、情報漏洩への対策方法について懸念を抱えている。
・翻訳業務において、客先からパスワードなしメールが届いた場合に内容が漏洩する可能性はどのくらいあるか。対策方法はあるか。

■社内のシステム、セキュリティ対策状況の診断
・自社システムはクラウドとオンプレミスのどちらを選択したら良いかわからない。
・情報セキュリティに対する全般的な体制整備（基本的なところから） 自社のネットワーク構成、システム構成図などもわからないため、その作成などもアドバイス等をお願いしたい。

■従業員向け教育
・外部とのメールのやり取りは代表メールのみとし、1 日数回、担当者がメールの振り分け作業を行っている。経営者にメールの運用を考え直してもらうにはセキュリティをどうしたらいいか。
・経営層、従業員のサイバーセキュリティに対する理解が得られず、古いルールを更新することができない。どのような働き掛けをすれば皆がサイバーセキュリティを意識するようになるかを相談したい。

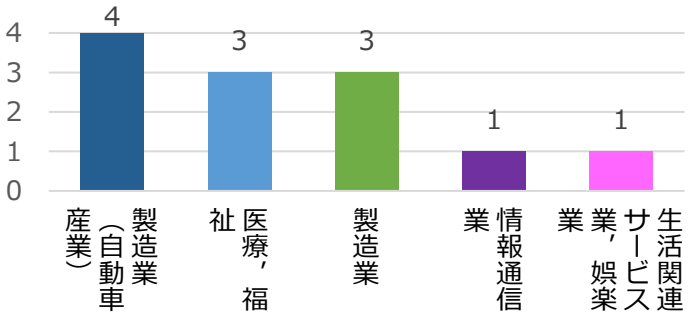
■インシデント対応
・ISMS のマニュアルに沿い、インシデント対応についても、体制、対応ルールを決めているが、特にランサムウエアのケースにおいて、BCP 面も考慮し、インシデント発生前の対応、発生時の初動、対処について具体的な情報を知りたい。
・インシデント訓練の他社事例について教えてほしい。

■その他
・行政書士として中小企業の規程づくりの仕事を頼まれることが多いが、セキュリティに関する内容は知見がないことも多く、情報処理安全確保支援士のようなセキュリティ専門家を頼りたいが、システムなどで検索しても企業内で活躍されている方も多く独立されている方になかなか出会えない。
・土木中心の建設会社だが、システムベンダーが、同業他社のサイバーセキュリティ事故を引き合いに、次々に新しいハードウェアやソフトウェアを提案してくる。本当に必要なものなのか判断がつかない。
・盗まれて困る情報を持っていないのに対策にお金をかける意味があるのか。
・情報セキュリティ対策にかける予算はどの程度がよいのか、他社ではどのくらいの費用をかけているのか。
・サイバーセキュリティ対策の現場リーダーの育成について教えてほしい。

（ウ）　埼玉

埼玉の参加者で最も多かった業種は「製造業（自動車産業）」、次いで「医療、福祉」であった。

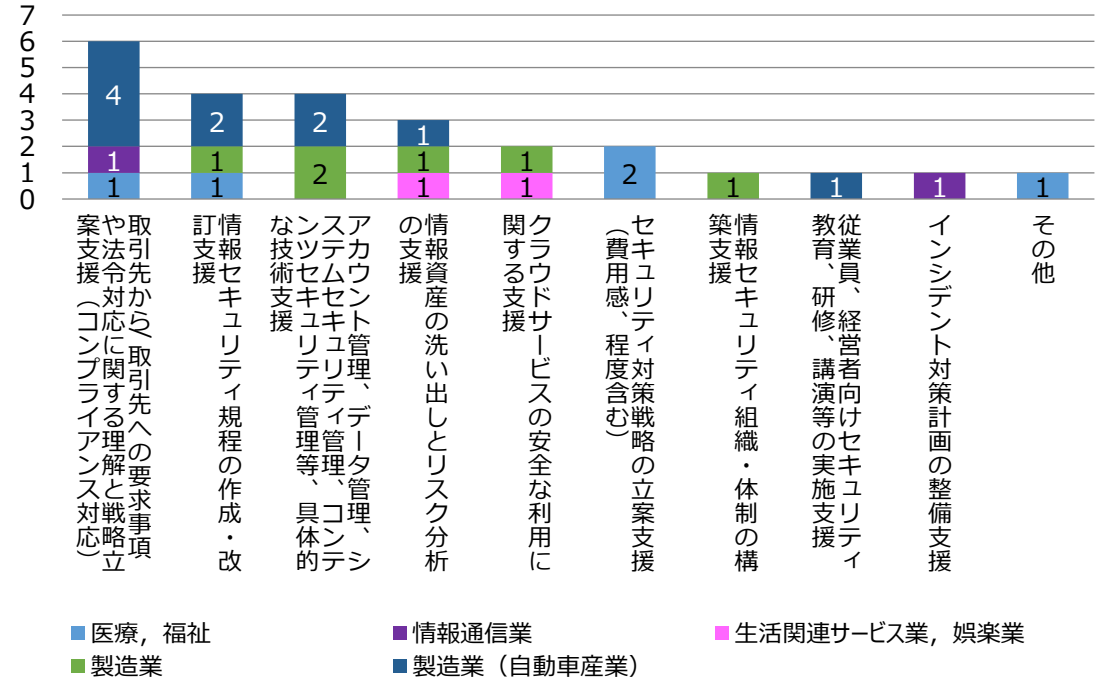
[個別相談][埼玉]参加社・業種別(n=12)




図表 2-35 個別相談参加企業の業種内訳（埼玉）

また、埼玉でも「取引先から/取引先への要求事項や法令対応」が最も必要とされる支援であった。

[個別相談][埼玉]　専門家が示した必要支援・業種別 (n=12) (MA)




図表 2-36 個別相談参加企業において必要とされる支援（埼玉）

埼玉の特徴は、製造業、特に自動車産業からの相談が顕著で、自工会サイバーセキュリティガイドラインへの対応が中心的な課題となっていた。特に製造現場での共有 PC 管理に関して、業界の要求事項を自社の現場に適した形で実践する具体的な方法が求められていた。

これらの要求事項対応に関する相談に対し、セキュリティ専門家は、製造現場の特性を踏まえた実践的な対策を提案。監視カメラを活用したアクセス管理など、具体的かつ実効性の高い解決策を示した。さらに、当日は、茨城県や千葉県など遠方からも、自動車産業の企業が個別相談を目的としてサイバーセキュリティ相談会に参加する企業が見られた。セキュリティ専門家も企業の困窮した状況を知り、要望があればマネジメント指導に積極的に協力する意志を事務局に示すなど、サプライチェーン全体のセキュリティ対策の底上げを支援する強い意識が感じられた。

加えて、医療・福祉業界からの「3 省 2 ガイドライン」や「個人情報保護法」などの業界ガイドラインや法令への準拠を強く意識する相談もあった。

[相談事例]

■自工会サイバーセキュリティガイドラインへの準拠

・自工会サイバーセキュリティガイドラインで求められている「共用パソコンのアカウント管理」「共用の NAS データの閲覧管理」について対応方法がよくわからない。
・工場で使用する共有端末について、①操作ログの問題:共有アカウントである為、誰が操作したか分からない。②パスワードの問題:複数人で使用する為、パスワードの管理が困難であるという問題がある。自工会から対応が求められているものの、具体的な対策の方法がわからず、相談先もいない。

■取引先のセキュリティ対策

・厚生労働省及び経済産業省・総務省が制定している 3 省 2 ガイドラインに電子カルテベンダが従わない。

■セキュリティ対策のはじめ方

・社会福祉法人として 60～70 台の PC と NAS サーバを保有しているが、十分な管理ができていない。担当者 1 人で管理するのは限界で、何から手を付けていけば良いのか知りたい。
・昨年度、グループ構成する会社が増え、取引先が増えたことで、情報漏洩対策等を本格的に行いたい。1 人で社内の IT 化などを担当しているため、支援が欲しい。
・高額な営業提案が多かったため、IT ベンダーとの契約を解消し、1 人でシステム環境を再構築した。セキュリティ専門家ではないため、セキュリティの取り組み方が全く分からない。

■従業員向け教育

・セキュリティ教育理解度の確認方法や理解度不足への再教育・再試験方法などがわからない。

・セキュリティ教育資料の選定・作成に時間がかかる。

■インシデント対応
・インシデント発生時の届け出等の対応がわからない。また、インシデント発生時に関係者に報告するためのフォーマットが欲しい。

■その他
・個人情報員会への報告の仕方がわからない。
・基幹システムをオンプレからクラウドサービスへ移行予定だが、移行後の個人情報取扱いについて、注意すべき点を教えてほしい。
・お客様からお預かりするデータは、メールまたは USB で保管しているが、どの媒体が安全性が高いのか、望ましい形式を教えてほしい。

### 2.1.9. サイバーセキュリティ相談会のまとめ

①サイバーセキュリティ相談会

3商工会議所で合計105社（122名）から参加があり、申し込みから実際の参加率は約85%と高い水準を示した。これは通常の商工会議所におけるセミナーの参加率（70%程度）と比較しても高く、本事業の相談会への参加者は、明確な目的意識を有していたことがうかがえる。

参加者の相談会参加の動機は、「講演内容に興味があった」、「セキュリティ対策について以前から不安があった」との回答が全体の 60%超を占める。「個別相談を受けたかった」、「具体的なセキュリティ対策を学びたかった」と回答した参加者は 34%。このことから、具体的な対策の前の、準備段階（情報収集段階）の参加者がその約 2 倍いたこととなり、多くの企業がる情報収集のために参加していることが明らかとなっている。

② サイバーセキュリティ相談会参加者アンケート

相談会参加者の、セキュリティ専門家支援に対するニーズについて、まずは支援期間については、スポット対応への需要が全体の 58%と最も高く、また、訪問方式の指導を希望する声は、オンライン方式の約 2 倍であった。

セキュリティ専門家の紹介経路については、情報処理推進機構（IPA）や商工会議所等の公的機関を介した紹介が最も選好され、次いで IT ベンダーからの紹介が望まれている。

支援内容に対する期待としては、「緊急時の対応力」が最も重視されており、コストは最優先事項とはされていない。また、インシデント発生時の対応が支援内容として高い関心を集めている点が特徴的である。

また、アンケート調査では、セキュリティ専門家による支援に対して 78%という高い関心が示された。希望される支援内容は、「インシデント発生時の対応」、「従業員教育」など、単発的なニーズへの対応と、「情報セキュリティ規程の整備」など長期的な基盤整備のニーズの両方があることが示された。

③個別相談

個別相談を実施した結果、中小企業が必要とする支援の上位 3 項目は、「情報セキュリティ規程の整備」、「取引先からの要求事項及び法令対応」、「従業員セキュリティ教育」であった。地域間で顕著な差異は観察されず、各参加企業の業種特性に応じて支援ニーズが異なる傾向が示唆された。特に名古屋、埼玉では、参加企業の多数が「製造業（自動車産業）」であり、「取引先からの要求事項及び法令対応」が最も顕著なニーズとして浮上した。一方、大阪では業種の多様性が高く、提案された支援内容も広範囲に及んだ。全体として、多くの企業が初期段階にあり、「情報セキュリティ規程の整備」が最も求められる支援となっていた。

相談会から個別相談への移行率を業種別に分析したところ、製造業内において「製造業（自動車産業）」の移行率は 88%と、自動車産業以外の「製造業」の移行率 48%と比較し、約 1.8 倍に達した。さらに、医療・福祉、電気・ガス・熱供給・水道業などの規制産業においても、同様に高い移行率（約 80%）が観察された。この結果から、業界ガイドラインや取引先からの具体的な要求事

項といった外部要因が、中小企業における具体的なセキュリティ対策推進の原動力の 1 つであることを示唆している。

また、本実証事業を通じて、企業が認識する課題とセキュリティ専門家が診断した実際の課題との間にギャップが見出された。特徴的なのは、「情報資産の洗い出し」（申告 3 件→実際 9 件）、「情報セキュリティ規程の作成・改定」（申告 12 件→実際 17 件）といった基盤的・体系的な対策の必要性が、企業の認識以上に高かった点である。一方、「セキュリティ対策の現状評価」（申告 5 件→実際 2 件）、「インシデント対策計画整備」（申告 10 件→実際 8 件）といった事後的対策については、企業の認識ほどの優先度はないと判断された。このギャップは、企業のセキュリティ対策に対する認識が、インシデント対応など目に見える脅威へ向きがちである一方、それを支える体系的なセキュリティ対策への理解が不足していることを示唆すると考える。このように俯瞰的な観点で中小企業を導くことが可能なのは、セキュリティ専門家をおいて他にならないと推測する。

④製造業（自動車産業）におけるガイドライン対応支援

本実証事業において、特に「取引先の要求事項対応」については、自動車産業からの要望加が顕著であった。

当該テーマ下における自動車産業各社の相談内容は、「従業員教育」、「規程作成」、「インシデント対策」、「共有アカウント管理」、「情報資産台帳作成」の 5 つであった。

これら相談に共通する特徴として、取引先から示された要求事項と製造現場の実態との間でのギャップ解消に悩む相談者の姿があった。相談者は、要求事項の具体的理解への助けや対策を実施する方法の提案を求めていた。

上記に対し、セキュリティ専門家は個社のシステム構成や人員体制等を詳細に聞き取った上で、製造現場という特殊な環境の制約の中で実現可能な妥協点を見出すという支援アプローチを取っていた。このことから、自動車産業への支援においては、セキュリティ専門家の技術的知見に加え、業界特性と現場実態への理解、ガイドラインへの深い知見、そしてこれらを統合する柔軟な提案力がセキュリティ専門家に求められることが明らかとなった。

## 2.2. マネジメント指導（テーマ別）

セキュリティ個別相談会に参加した企業のうち、希望する企業に対して、セキュリティ専門家が 3 回訪問し、当該企業の課題解決に向けた指導を行う「セキュリティマネジメント指導（テーマ別）」を実施した。以下、本事業の概要を示す。

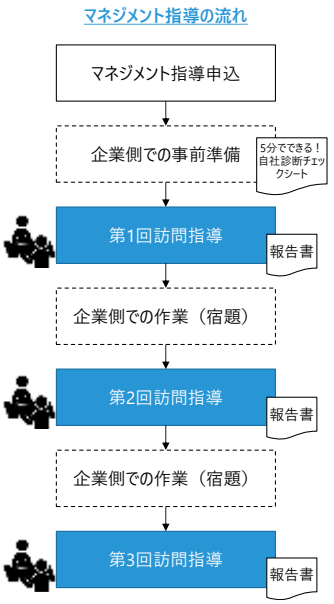
### 2.2.1. 全体概要

セキュリティマネジメント指導は、前述のサイバーセキュリティ相談会に参加した企業に対し、引き続いての訪問指導を希望するかを尋ねた上で、訪問指導を希望する企業に、予め依頼した指導専門家の専門性や得意分野を加味し、適切と思われる方の割り当てを行った（マッチング）。

指導に際しては、以下の５つのテーマを設定した上で、指導先の中小企業にもっとも適切な支援内容を選べるようにした。加えて、各テーマに対して、3 回訪問によって標準的な指導を行えるようにするためのツール（教材）を作成し、指導専門家・指導先企業双方に提供することとした。

| 指導テーマ | 1 情報セキュリティ規程の整備 | 2 情報資産の洗い出しとリスク分析 | 3 クラウドサービスの安全利用 | 4 セキュリティインシデント対応 | 5 従業員向け情報セキュリティ教育 |
|---|---|---|---|---|---|
| どういった企業に受けてもらいたいか | **サイバー攻撃の増加や法令遵守の必要性に直面しつつも、情報セキュリティ規程が未整備な中小企業。**特に、従業員が多様なITツールを使って業務を行っているが、具体的な指針がなく、責任範囲が曖昧な企業に必要である。 | **デジタル化が進み、膨大な情報を管理しているが、どの情報が重要か、リスクがどこにあるかが把握できていない企業。**特に、製造業やサービス業など、顧客情報や技術情報を大量に扱う企業に必要である。 | **業務効率化のためにクラウドサービスを導入しているが、セキュリティリスクに対する理解や対策が不十分な企業。**特に、情報管理の外部委託が進んでいるが、適切な安全対策ができていない中小企業に必要である。 | **セキュリティインシデントが発生した際の対応が曖昧で、事後対応に時間がかかり、被害が拡大するリスクがある企業。**特に、**サプライチェーンの一部として他社との連携が多い企業**に必要である。 | **従業員のセキュリティ意識が低く、パスワード管理やフィッシング攻撃に対する対応が不十分な企業。**特に、ITリテラシーの差が大きい企業や、非専門職の従業員が多く、日常的なセキュリティ対策が徹底できていない企業に必要である。 |
| マネジメント指導を受けたことによる効果 | 不足していた情報セキュリティ規程が整備され、社内での運用・周知方法まで確立されることで、社内セキュリティ体制の継続的・自律的な改善が図れるようになる。 | 企業が保有する情報資産が洗い出され、リスク分析シートとして整備することで、自律的な運用が図れるとともに、リスク低減策等の検討の題材にもなる。 | 当該支援先企業における「クラウドサービス安全利用の手引き」を策定することで、クラウドサービス利用に伴うリスクを理解できるようになる。 | インシデント対応プロセスを整備し、必要に応じ、従業員の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。 |

図表 2-37 マネジメント指導におけるテーマ設定の考え方（上）と指導の流れ（右）




各指導テーマの選定、ツール作成に際しての考え方、作成内容等については後述する。

また、3 回の指導後には指導先企業・セキュリティ専門家側双方に実施後アンケートを実施し、指導の成果や得られたアウトプット、企業側で残された課題、事業運営上の課題等について聞き取りを行った。

加えて、これら指導後の報告内容（セキュリティ専門家側・企業側双方）を勘案し、指導実施により成果が得られた好例を「ベストプラクティス」として取り上げることとして、改めて企業・セキュリティ専門家へのヒアリングを通じて事例集を作成した。本件についても後述する。

### 2.2.2. 指導専門家

本事業において活動いただいた指導専門家は以下のとおり。原則としてセキュリティ相談会で相談対応いただいたセキュリティ専門家（及びセミナー講演者）を、各企業を訪問してマネジメント指導を行う指導専門家として再度起用した。

| | | | |
|---|---|---|---|
| 大阪 | 清水 俊彦 氏 | 名古屋 | 久保田 秀男 氏 |
| 大阪 | 高谷 幸治 氏 | 名古屋 | 三代 健一郎 氏 |
| 大阪 | 高橋 幸司 氏 | 名古屋 | 大喜 康生 氏 |
| 大阪 | 田中 基貴 氏 | 名古屋 | 高橋 真悟 氏 |
| 大阪 | 野村 陽子 氏 | 名古屋 | 寺島 敬 氏 |
| 大阪 | 原 一矢 氏 | 埼玉 | 浅井 隆弘 氏 |
| 大阪 | 渡邊 功 氏 | 埼玉 | 遠藤 貴芳 氏 |
| 名古屋 | 一ノ瀬 誠 氏 | 埼玉 | 堀内 靖大 氏 |

図表 2-38 マネジメント指導 指導専門家一覧

また、訪問指導に際しては、指導先企業が確定し、第 1 回目の訪問日時が決まった段階で個別に指導専門家としての就任を依頼し、承諾をいただく手続きをとった。第 2 回目以降の訪問日時は第 1 回訪問時に指導先企業・指導専門家の間で調整した。

指導専門家への謝金は訪問 1 回あたり 26,400 円（税込）とし、別途訪問に際して必要な交通費（実費）を支払うこととした（辞退者を除く）。

### 2.2.3. 事前準備事項

マネジメント指導実施に際し、事前の準備として以下の作業を行った。

（1） 指導ツールの作成

マネジメント指導のテーマ別に、作業すべきテンプレートや 3 回の指導においてそれぞれどのレベルまで達成することが望ましいか等標準的な流れを整理した指導ツールを作成した。また、テーマ共通の資料として、企業に事前に記入いただく「5 分でできる！情報セキュリティ自社診断」Excel シートを準備した。詳細は後述。

（2） 指導専門家への事前説明

指導ツールの内容及び指導の流れについて、個別相談会の会場で指導専門家に対してあらかじめ説明を行った。

（3） 企業・指導専門家間の各種調整

個別相談を受けた企業に対し、マネジメント指導を受けるか否かの意思確認を行った。企業が希望する内容と指導専門家の対象分野を考慮し、割り当て（マッチング）を行った（詳細後述）。希望する

企業に対しては初回指導を希望する日程、希望するテーマ等を聞き取り、指導専門家ともやり取りをしながら、具体的な調整を行った。

また、各回訪問指導後に指導専門家から提出いただく報告書フォーマットも併せて作成し、指導専門家側に提示した。

（４） マネジメント指導完了後アンケート作成

マネジメント指導後に指導先企業・指導専門家双方に対して実施するアンケートを準備した。アンケート調査票及び分析結果は後述。

### 2.2.4. 企業・指導専門家のマッチング

個別相談時の内容やその後の企業への聞き取り、指導専門家の対象分野等を考慮し、各企業に指導専門家を割り当てる作業を行った（マッチング）。その結果、計 35 社に対してそれぞれ指導専門家を割り当て、訪問指導を順次進めた。マッチング結果は以下の表のとおり（順不同）。

なお、指導開始直前に上記のうち 1 社が辞退を申し出たため、実際の指導は 34 社に対して実施した。

| 地域 | 訪問先企業の業種 | 担当指導専門家 |
|---|---|---|
| 大阪 | 学術研究、専門・技術サービス業 | 野村 陽子 氏 |
| 大阪 | 製造業 | 野村 陽子 氏 |
| 大阪 | 建設業 | 野村 陽子 氏 |
| 大阪 | 学術研究、専門・技術サービス業 | 野村 陽子 氏 |
| 大阪 | 製造業 | 渡邊 功 氏 |
| 大阪 | 製造業 | 渡邊 功 氏 |
| 大阪 | 電気・ガス・熱供給・水道業 | 田中 基貴 氏 |
| 大阪 | 製造業（自動車産業） | 田中 基貴 氏 |
| 大阪 | 製造業 | 清水 俊彦 氏 |
| 大阪 | 製造業 | 清水 俊彦 氏 |
| 大阪 | 製造業（自動車産業） | 清水 俊彦 氏 |
| 大阪 | 卸売業・小売業 | 高谷 幸治 氏 |
| 大阪 | 卸売業・小売業 | 高谷 幸治 氏 |
| 大阪 | 学術研究、専門・技術サービス業 | 高橋 幸司 氏 |
| 大阪 | 医療、福祉 | 高橋 幸司 氏 |
| 大阪 | 卸売業・小売業 | 高橋 幸司 氏 |
| 大阪 | 製造業 | 原 一矢 氏 |
| 名古屋 | 製造業（自動車産業） | 大喜 康生 氏 |

| 地域 | 訪問先企業の業種 | 担当指導専門家 |
|---|---|---|
| 名古屋 | 運輸業、郵便業 | 寺島 敬 氏 |
| 名古屋 | 製造業（自動車産業） | 寺島 敬 氏 |
| 名古屋 | 製造業（自動車産業） | 三代 健一郎 氏 |
| 名古屋 | 製造業（自動車産業） | 三代 健一郎 氏 |
| 名古屋 | 学術研究、専門・技術サービス業 | 三代 健一郎 氏 |
| 名古屋 | 卸売業・小売業 | 高橋 真悟 氏 |
| 名古屋 | 製造業（自動車産業） | 高橋 真悟 氏 |
| 名古屋 | 製造業 | 櫛田 康仁 氏 |
| 名古屋 | 製造業（自動車産業） | 久保田 秀男 氏 |
| 名古屋 | 情報通信業 | 久保田 秀男 氏 |
| 名古屋 | 建設業 | 一ノ瀬 誠 氏 |
| 名古屋 | 建設業 | 一ノ瀬 誠 氏 |
| 名古屋 | 製造業（自動車産業） | 一ノ瀬 誠 氏 |
| 埼玉 | 製造業（自動車産業） | 堀内 靖大 氏 |
| 埼玉 | 製造業（自動車産業） | 堀内 靖大 氏 |
| 埼玉 | 製造業 | 浅井 隆弘 氏 |
| 埼玉 | 医療、福祉 | 遠藤 貴芳 氏 |

図表 2-39 マネジメント指導企業と指導専門家のマッチング結果一覧

### 2.2.5. 指導ツール作成

マネジメント指導実施に際し、3 回の訪問における標準的な指導の流れや達成基準等を示した指導ツールをあらかじめ作成した。作成に際しては、令和元年度及び令和 2 年のマネジメント指導で用いたツールを参考に、「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」、「従業員向け情報セキュリティ教育」の 5 つのテーマを設定した上で、IPA「中小企業の情報セキュリティ対策ガイドライン第 3.1 版[5]」及び同付録資料等の内容を加味した。

指導ツール作成にあたっては、当該テーマがどういった企業に必要であるか、背景や施策の対象となる企業像などを確認した上で、マネジメント指導の目標（ゴール）を設定し、全 3 回の指導内容のモデルプランをシラバスとして整理した。また、併せて指導の際に記入可能なワークシート等も必要に応じ整備した。各テーマにおける達成目標は以下のとおりである。

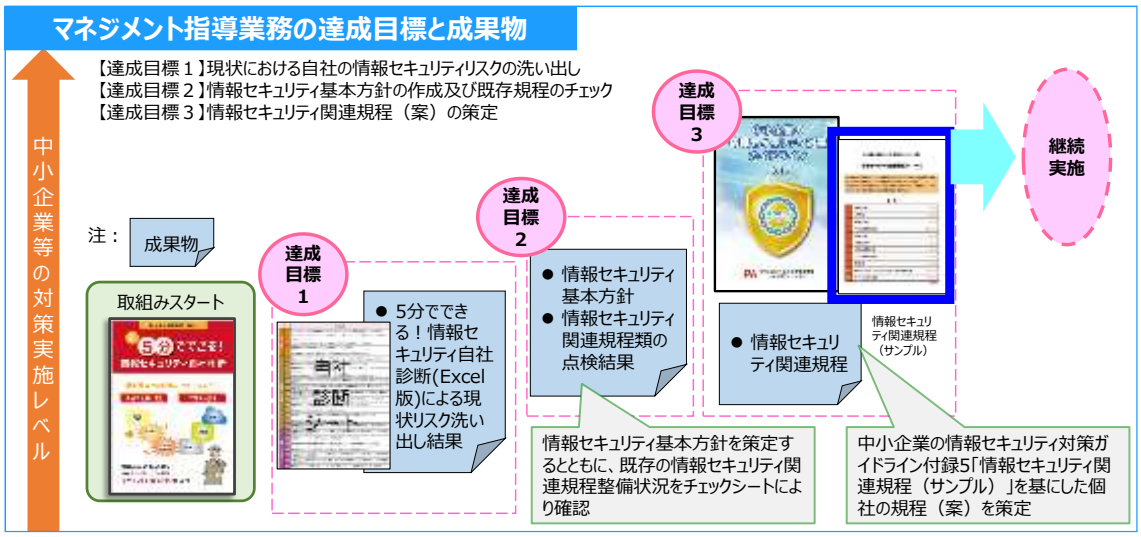
[5] 中小企業の情報セキュリティ対策ガイドライン第 3.1 版
https://www.ipa.go.jp/security/guide/sme/about.html

| マネジメント指導ツール（テーマ別） | |
|---|---|
| テーマ | マネジメント指導の達成目標 |
| 指導ツール①<br>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<br>【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<br>【達成目標３】情報セキュリティ関連規程（案）の策定 |
| 指導ツール②<br>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<br>【達成目標２】自社における情報資産の洗い出し<br>【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 |
| 指導ツール③<br>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<br>【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<br>【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 |
| 指導ツール④<br>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<br>【達成目標２】インシデント対応手順書の作成<br>【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 |
| 指導ツール⑤<br>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<br>【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<br>【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 |

図表 2-40 マネジメント指導（テーマ別）における達成目標一覧

（１） 情報セキュリティ規程の整備

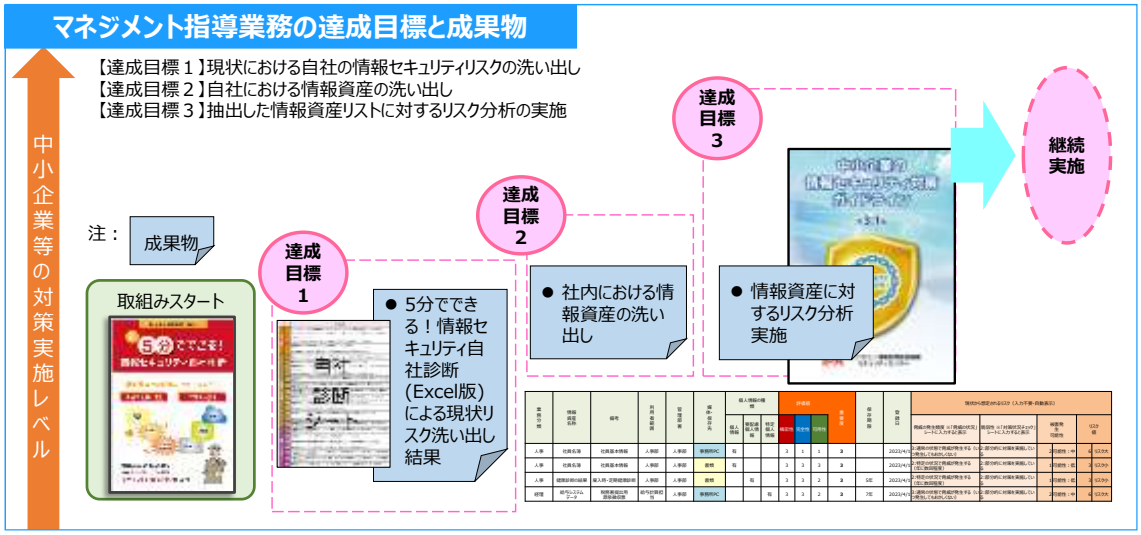
「中小企業の情報セキュリティガイドライン(第 3.1 版)」の付録 5「情報セキュリティ関連規程（サンプル）」を基に、指導先企業の「情報セキュリティ基本方針（案）」、「情報セキュリティ関連規程（案）」の策定・整備について、必要な指導・助言を行う。




図表 2-41 テーマ① 情報セキュリティ規程の整備における達成目標と成果物

（２） 情報資産の洗い出しとリスク分析

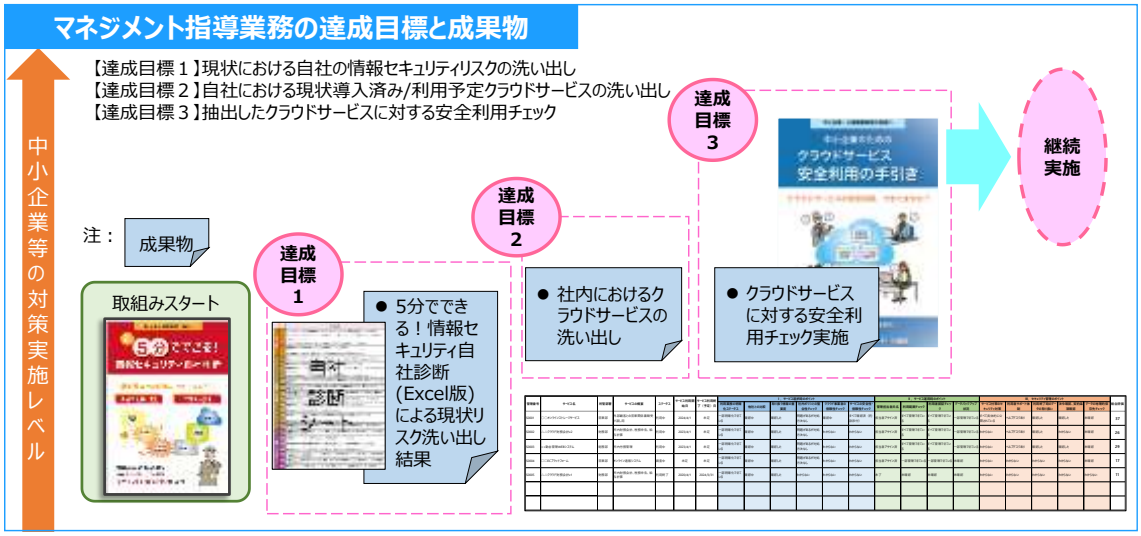
「中小企業の情報セキュリティガイドライン(第 3.1 版)」の付録 7「リスク分析ワークシート」を基に、 指導先企業における情報資産の洗い出しとリスク分析を実施について、必要な指導・助言を行う。




図表 2-42 テーマ② 情報資産の洗い出しとリスク分析における達成目標と成果物

（３） クラウドサービスの安全利用

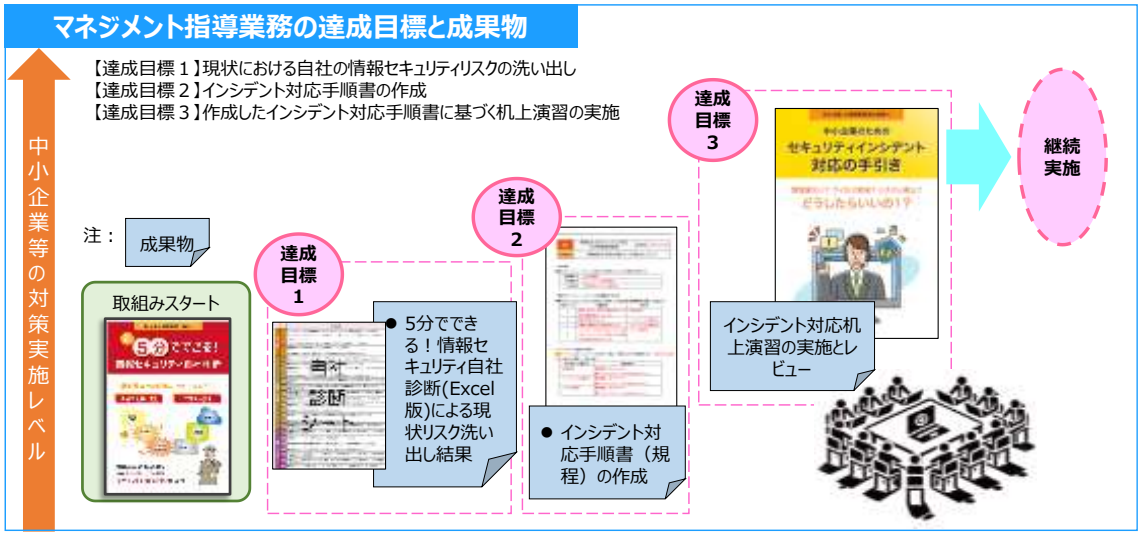
「中小企業の情報セキュリティガイドライン(第 3.1 版)」の付録 6「中小企業のためのクラウドサービス安全利用の手引き」を基に作成した「クラウドサービス台帳兼チェックリスト」を用い、指導先企業におけるクラウドサービスの洗い出しと安全利用チェックの実施について、必要な指導・助言を行う。




図表 2-43 テーマ③ クラウドサービスの安全利用における達成目標と成果物

（４） セキュリティインシデント対応

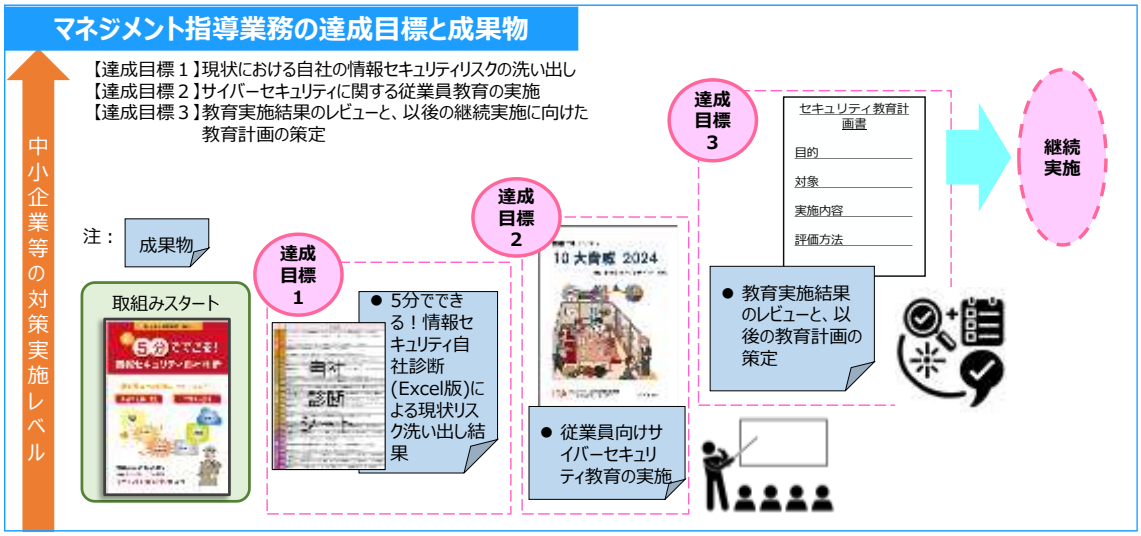
「中小企業の情報セキュリティガイドライン(第 3.1 版)」の付録 8「中小企業のためのセキュリティインシデント対応の手引き」を基に、指導先企業におけるインシデント対応手順書の作成、及び作成したインシデント対応手順書に基づく机上演習の実施について、 必要な指導・助言を行う。




図表 2-44 テーマ④ セキュリティインシデント対応における達成目標と成果物

（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。




図表 2-45 テーマ⑤ 従業員向けセキュリティ教育における達成目標と成果物

また、各テーマのゴール達成を目指す上で、全 3 回の訪問指導を効率的に推進するため、各回の標準的な指導の進め方を示した「シラバス」を整備した。以下にサンプル（情報セキュリティ規程の整備）を示す。

## シラバスのサンプル｜情報セキュリティ規程の整備

### シラバス案

■第1ステップ（指導申込み～第1回面談まで）

**チェックシートに基づく、現在の情報セキュリティ規程の自己評価**

| | | 企業 | 専門家 | 成果物/事務局提供ツールなど |
|---|---|---|---|---|
| 事前準備 | 1 | 提供可能な社内資料の準備<br>(企業紹介のパンフレット等) | ホームページなどによる企業の情報収集とヒアリングシートの作成（企業・事業の理解） | 【提供】指導講習コンテンツ |
| | 2 | 「5分でできる！自社診断（Excel版）」による自己診断の実施 | -（事務局にて配布済） | 【提供】5分でできる！自社診断チェックシート（Excel版） |
| | 3 | 「情報セキュリティ関連規程チェックシート」による自己診断の実施 | 同左の実施依頼 | 【提供】情報セキュリティ関連規程チェックシート |
| | 4 | 出席メンバー選定<br>(経営者/従業員等、半日x3回) | 専門家指導の作業内容、全体スケジュール案の作成、初回訪問日程の事前確認 | 初回のスケジュール調整 |
| 当日 | 1 | 右記説明に対するディスカッション(確認・了解) | 今回の訪問指導の目標、作業内容、全体スケジュール、成果物等の説明と合意 | 【提供】指導講習コンテンツ<br>【提供】サンプル基本方針／関連規程＊ |
| | 2 | 自社診断(Excel版)の結果の理解と課題認識についてのディスカッション | 自社診断(Excel版)の結果についての説明と、改善領域に関する現状確認と要望の確認 | 【成果物】自社診断(Excel版)の結果のまとめ |
| | 3 | 「情報セキュリティ関連規程チェックシート」の結果と課題認識についてのディスカッション | 「情報セキュリティ関連規程チェックシート」結果から得られる要改善点や今後の作業のポイント等説明 | 【成果物】情報セキュリティ関連規程チェックシート（途中版、引き続き作業指示） |
| | 4 | 右記依頼についての確認と了解 | 必要な追加情報の提供依頼<br>・業務/DB/ネットワークなどのIT環境など<br>次回のスケジュール調整、依頼事項の確認 | （終了後）<br>専門家から事務局への実施報告提出 |

■第2ステップ（第1回面談～第2回面談）
**新規程案の作成・チェックと適切な運用方法についての指南**

| | | 企業 | 専門家 | 成果物/事務局提供ツールなど |
|---|---|---|---|---|
| 事前準備 | 1 | 依頼された必要情報の準備 | 前回訪問で得た情報の整理・分析<br>(理解に齟齬が無いか訪問時に確認する) | - |
| | 2 | 情報セキュリティ基本方針の検討と案の作成 | 第2回の資料作成<br>・関連規程類の作成状況確認<br>・重点改善領域の見極め | 【提供】サンプル基本方針／関連規程＊<br>【提供】情報セキュリティ関連規程チェックシート |
| 当日 | 1 | 依頼された必要情報の提供・説明 | 提供された情報の確認・質疑応答 | - |
| | 2 | 基本方針/関連規程の有無/作成状況の説明<br>基本方針(案)の提示と作成 | 基本方針/関連規程の有無/作成状況の確認<br>基本方針の作成指導 | 【成果物】<br>・情報セキュリティ基本方針<br>・基本方針/関連規程類の整備状況確認一覧表 |
| | 3 | 右記説明に対するディスカッション<br>・対策の有用性と優先順位の判断 | 前回得た情報をもとにした、重点改善領域の説明とディスカッション<br>・緊急度、重要度、難易度による絞り込み<br>・規程や条文のスコープ（対象範囲）、ISMSの文書体系の考え方や既存文書との整合性チェック、流用の考え方など、規程整備に際し考慮しなければならない項目等 | 【成果物】情報セキュリティ関連規程チェックシート |
| | 4 | 必要な追加情報の提供了解 | 改善領域の対策検討に必要な追加情報の提供依頼 | （終了後）<br>専門家から事務局への実施報告提出 |

■第3ステップ（第2回面談～第3回面談）
**新規程の運用方法の確認**

| | | 企業 | 専門家 | 成果物/事務局提供ツールなど |
|---|---|---|---|---|
| 事前準備 | 1 | 急がれる改善施策の実現性の検討<br>(実現のための課題や対策の事前検討) | 前回訪問結果の整理と、絞り込んだ具体的対策の実施計画案の作成 | - |
| | 2 | 新規程の社内周知を含む運用手順案の作成 | 適宜アドバイス | 【提供】サンプル基本方針／関連規程＊ |
| 当日 | 1 | 経営施策の説明と、情報セキュリティ対策の必要性の理解 | 新規程に基づき、今後必要となる情報セキュリティ対策の説明 | 【提供】指導講習コンテンツ |
| | 2 | 右記のディスカッションを通じて提示された対策案の実現性検討<br>・必要とされるリソース:人・物・金 | これまでの検討を踏まえた、具体的対策の実行計画の検討<br>・優先して検討すべき対策やスケジュール案の提示とディスカッション<br>対策実施に当たっての運用ルールの検討 | ※前回確認した関連規程の整備状況確認が、新たな対策実施に際して見直す必要がないか改めて確認 |
| | 3 | 作成した成果物の説明と合意 | 右記の成果物のレビューと合意 | 【成果物】基本方針/関連規程の点検結果及び新たに策定した基本方針（規程そのものは提出不要）<br>【成果物】自社診断(Excel版)結果報告 |
| | | 専門家指導についての評価コメント<br>(アンケート)を事務局に提出 | 指導結果のまとめと評価 | （終了後）指導結果のまとめと評価を行い、事務局への実施報告を行う<br>【成果物】最終報告書 |

図表 2-46 標準シラバス案（サンプル「情報セキュリティ規程の整備」）

### 2.2.6. 指導ツールの評価

マネジメント指導実施後、指導専門家・企業双方に行ったアンケートを基に、指導ツールの使いやすさ等の評価について調査結果を以下に示す。

| 【１．情報セキュリティ規程の整備】 |
|---|
| ① 評価： |
| ・ 「一つの型として利用できたので、企業にとって、所要時間や完成がイメージしやすかった」「初回の指導の導入としては良かった」 など、マネジメント指導を一定の期間内に、一定品質で進行させるためには助かったとの声が多かった。 |
| ② 課題： |
| ・ 指導専門家、指導先企業の双方からサンプル規程等、指導ツールのボリュームの多さが指摘 |

| |
|---|
| された。特に 3 回の指導で内容を完全に網羅するためには時間が足りないとの意見があった。<br>・ 指導先企業からは、「企業側に一定レベルの情報セキュリティについての知見や意識が求められる内容である」との意見が複数あった。 |
| ③指導ツール利用状況： |
| ・ 指導ツールに基づいて指導を行った： 5 名<br>・ 指導ツールに自ら資料を追加して指導を行った：10 名 |
| ④ 改善・拡充要望： |
| ・ IPA の「ちょこっとプラスパスワード」や映像コンテンツが古くなっている。「5 分でできる情報セキュリティ自社診断」の解説だけでも最新事例を入れて欲しい。（複数名が指摘）<br>・ 企業提出用の訪問回数に応じたスケジュール（ガントチャート）様式（複数名が指摘）<br>・ 様々な業種に対応したガイドライン集。<br>・ 企業によりわかりやすく説明するためガイドライン、ポリシー、スタンダード、プロシージャの関係についての説明が欲しい。<br>・ 関連規定(サンプル)で出てくる専門用語/技術用語の解説集<br>・ 業種別の規程作成ツール。 製造業、海外商社、士業向けといったバリエーションを希望<br>・ サイバー保険の選択肢、監査/点検担当者に教育すべき情報セキュリティ内部監査認定などの受講選択肢、脆弱性診断ツール、クライアント監視ツールなど IT ツールの選定ツール<br>・ 組織的対策の必要性、経営層への説得材料の掲載<br>・ 情報セキュリティ部門責任者への具体的な作業の振り方、難易度の低いセキュリティの具体的作業など、作業に組織を関与させる例や具体的な役割例。企業がぶつかる壁は他部署・組織・経営層の巻き込みである。<br>・ PC やスマートフォン、IOT デバイス等、端末管理についての規模別ベストプラクティス集<br>・ 関連規程を組織に定着させるためのストーリー<br>・ AI を使って、企業の実態に沿った規程であることを添削できるツールがあるとよい。 |

図表 2-47 テーマ① 情報セキュリティ規程の整備 指導ツールに対する意見

| 【２．情報資産の洗い出しとリスク分析】 |
|---|
| ① 評価： |
| ・ 「コンテンツ作成の時間が短縮できた」、「標準的な手順を伝えることができた」、「漏れのない情報資産の洗い出しを実行できた」、「洗い出しの実行により、対策すべき箇所が明確になった」、 「リスク値の算定が使いやすかった」など、マネジメント指導を効率的にかつ効果的に進めるためにツールは有効に活用できたとの評価を得た。<br>・ 指導先企業からは「リスク分析シートは、利用方法や説明が充実しておりスムーズに使用できた」などの声も挙がった。 |
| ② 課題： |

| |
|---|
| ・　特に無し |
| ③　指導ツール利用状況： |
| ・　指導ツールに基づいて指導を行った：2 名<br>・　指導ツールに自ら資料を追加して指導を行った：2 名 |
| ④　改善・拡充要望： |
| ・　カスタマイズする場合のガイドがあると良い<br>・　業界ごとの情報資産サンプル<br>・　指導フローチャート、進捗管理表 |

図表 2-48　テーマ②　情報資産の洗い出しとリスク分析　指導ツールに対する意見

| 【3．クラウドサービスの安全利用】 |
|---|
| ①　評価： |
| ・　「指導時に必要な事項に絞って対話ができ、話しが発散せずにすむ」、「「中小企業のためのクラウドサービス安全利用の手引き」の内容とリンクしており、企業側が説明内容と照らし合わせながらチェックを行えるツールとなっていた」など、指導ツールの実効性の高さが評価された。<br>・　企業側からは「ツールが網羅的な作りこまれていたため、当社のような小さな企業にも当てはめて活用できた」などの声があった。 |
| ②　課題： |
| ・　「企業の本当のニーズにマッチするかは、正直わからない」等、指導ツールの有効性は、指導先企業のニーズに応じて変化することを示唆する意見があった。 |
| ③　指導ツール利用状況： |
| ・　指導ツールに基づいて指導を行った：1 名<br>・　指導ツールに自ら資料を追加して指導を行った：2 名 |
| ③　改善・拡充要望： |
| ・　「確認した」、「確認中」、「まだ確認していない」という選択肢の項目について、再考が必要。SLA においても、ただ確認するだけでなく、それが良い内容なの、か悪い内容なのかの判断基準が最も重要なのでは。現状は、約款に SLA に関する記述があれば「確認した」になってしまい、評価が高くなってしまう。あまり意味のない稼働率目標が記述されている場合もある。<br>・　インターネットバンキングの安全利用に関する評価（認証方式等）<br>・　個票から台帳にコピーする方法が難しい。普通にコピー＆貼り付けをすると「総合評価」欄が別の行の計算結果になってしまう。<br>・　サプライヤーとユーザーのペルソナ設定が理解できない |

図表 2-49　テーマ③　クラウドサービスの安全利用　指導ツールに対する意見

| 【４．セキュリティインシデント対応】 |
| --- |
| ① 評価： |
| ・ 「わかりやすい内容で参考例などもあり、そのまま会社に提示ができた」、「基本的な項目を網羅していた」、「指導先の担当者が理解しやすい構成となっていた」など、指導ツールが有効に活用でたと評価された。<br>・ 指導先企業からは、「ツールに沿って資料を作成する事で、ある程度の成果物が出来上がった。解り易く理解度もあがった」などの声もあった。 |
| ② 課題： |
| ・ 特に無し |
| ③ 指導ツール利用状況： |
| ・ 指導ツールに基づいて指導を行った：２名<br>・ 指導ツールに自ら資料を追加して指導を行った：３名 |
| ③ 改善・拡充要望： |
| ・ 自動車産業等、主だった業界にあわせたツール<br>・ インシデント訓練事例集<br>・ インシデント報告書のサンプル |

図表 2-50 テーマ④ セキュリティインシデント対応 指導ツールに対する意見

| 【5．従業員向けセキュリティ教育】 |
| --- |
| ① 評価： |
| ・ 「指導ツールの内容が動画と連携しており、使いやすかった」、「パワーポイントに要点がまとまっており、動画閲覧後、資料を見返していただくことができるのでよかった」、「セキュリティプレゼンターサンプル資料を基に、個別で話したい内容を追記すればよかったので使いやすかった」等、指導時特に動画とのスムーズな連携ができたことを評価する声が多かった。<br>・ 指導先企業からは、「IPA 動画を活用した説明もあり、受講者全員が理解できたと感じる」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。 |
| ② 課題： |
| ・ 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があった。 |
| ③ 指導ツール利用状況： |
| ・ 指導ツールに基づいて指導を行った：２名<br>・ 指導ツールに自ら資料を追加して指導を行った：５名 |
| ④ 改善・拡充要望： |
| ・ プレゼンター資料の増強<br>・ 研修テーマ毎の「理解度確認テスト」<br>・ 「指導テーマ⑤｜サンプルプログラム①_標的型サイバー攻撃メールの手口と対策」の資料を一部用いたが、統計データやメールの見分け方が少し古い。今回は補足や追加資料による説 |

| |
|---|
| 明が必要だった。 |

図表 2-51 テーマ⑤ 従業員向けセキュリティ教育 指導ツールに対する意見

○まとめ

指導ツールの使い勝手について、いくつかの重要な示唆が得られた。

まず、指導ツールはマネジメント指導の場で概ね有効に活用されたことが確認された。特に、限られた時間の中で効率的に指導を進めるうえで役立ち、指導先企業の理解を深めるのにも貢献したとの声が寄せられた。

一方で、指導ツールだけでは十分な指導が難しく、全体の 68%の指導専門家が独自に補足資料を用意して指導にあたったという実態も明らかになった。その背景として、ツールの内容が一般的であるため、企業ごとの状況に合わせた調整が指導専門家に求められていることが指摘された。

また、指導ツールの改善に関しては、さまざまな建設的な提案が寄せられた。具体的には、補足資料や事例集の充実、用語の説明追加、指導スケジュールのテンプレートなどが挙げられ、いずれも実用的なアイデアであった。これらの意見を踏まえ、今後、指導ツールのさらなる改善に取り組んでいく必要がある。

**＜参考＞マネジメント指導テーマと支援士試験シラバスとの関係**

本事業において設定したマネジメント指導テーマは、今後中小企業等支援を行う場で登録セキスペが活躍することを想定し、情報処理安全確保支援士試験（レベル 4）との関連も踏まえて検討した。具体的には、同試験のシラバスとの対応関係を意識し、どの指導テーマを実施することがシラバスの項目に該当するかを整理した。以下にその概要を示す。

| 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<br>【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<br>【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<br>1-4 情報セキュリティ諸規程の策定<br>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<br>3-2 マルウェア対策<br>3-6 脆弱性への対応<br>3-9 人的管理<br>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<br>【達成目標 2】自社における情報資産の洗い出し<br>【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<br>1-3 情報セキュリティリスク対応<br>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<br>【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<br>【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<br>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<br>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<br>【達成目標 2】インシデント対応手順書の作成<br>【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<br>3-4 セキュリティ監視並びにログの取得及び分析<br>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<br>4-2 情報セキュリティ事象の評価<br>4-3 情報セキュリティインシデントへの対応<br>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<br>【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<br>【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 |

図表 2-52 マネジメント指導テーマと情報処理安全確保支援士試験シラバスとの関係

### 2.2.7. 指導実施件数

各地域別のマネジメント指導（テーマ別）実施企業数は以下のとおり。

また、原則として各 3 回の訪問指導を予定していたが、全 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。

| 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 |

図表 2-53 マネジメント指導実施件数等

■地域ごとの指導人数、指導件数

| 地域 | 指導専門家人数 | 指導先企業数 |
|---|---|---|
| 大阪 | 7 人 | 17 社 |
| 名古屋 | 6 人 | 13 件 |
| 埼玉 | 3 人 | 4 社 |

図表 2-54 地域ごと指導専門家数・指導件数

■指導テーマごとの件数

| 指導テーマ | 指導先企業数 |
|---|---|
| 情報セキュリティ規程の整備 | 15 社 |
| 情報資産洗い出しとリスク分析 | 4 社 |
| クラウドサービスの安全利用 | 3 社 |
| セキュリティインシデント対応 | 5 社 |
| 従業員向けセキュリティ教育 | 7 社 |

図表 2-55 指導テーマごと件数

■本事業において実施した指導専門家のテーマごとの指導件数

| | | | 情報セキュリティ規程の整備 | 情報資産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 | 計 |
|---|---|---|---|---|---|---|---|---|
| 1 | 浅井 隆弘 氏 | 埼玉 | 0 | 1 | 0 | 0 | 0 | 1 |
| 2 | 一ノ瀬 誠 氏 | 名古屋 | 0 | 0 | 2 | 1 | 0 | 3 |
| 3 | 遠藤 貴芳 氏 | 埼玉 | 1 | 0 | 0 | 0 | 0 | 1 |
| 4 | 久保田 秀男 氏 | 名古屋 | 0 | 1 | 0 | 1 | 0 | 2 |
| 5 | 三代 健一郎 氏 | 名古屋 | 1 | 1 | 0 | 0 | 1 | 3 |
| 6 | 清水 俊彦 氏 | 大阪 | 3 | 0 | 0 | 0 | 0 | 3 |
| 7 | 大喜 康生 氏 | 名古屋 | 0 | 0 | 0 | 1 | 0 | 1 |
| 8 | 高谷 幸治 氏 | 大阪 | 2 | 0 | 0 | 0 | 0 | 2 |
| 9 | 高橋 幸司 氏 | 大阪 | 0 | 1 | 0 | 1 | 1 | 3 |
| 10 | 高橋 真悟 氏 | 名古屋 | 1 | 0 | 0 | 0 | 1 | 2 |
| 11 | 田中 基貴 氏 | 大阪 | 2 | 0 | 0 | 0 | 0 | 2 |
| 12 | 寺島 敬 氏 | 名古屋 | 0 | 0 | 0 | 1 | 1 | 2 |
| 13 | 野村 陽子 氏 | 大阪 | 2 | 0 | 1 | 0 | 1 | 4 |
| 14 | 原 一矢 氏 | 大阪 | 1 | 0 | 0 | 0 | 0 | 1 |
| 15 | 堀内 靖大 氏 | 埼玉 | 2 | 0 | 0 | 0 | 0 | 2 |
| 16 | 渡邊 功 氏 | 大阪 | 0 | 0 | 0 | 0 | 2 | 2 |
| 合計 | | | 15 | 4 | 3 | 5 | 7 | 34 |

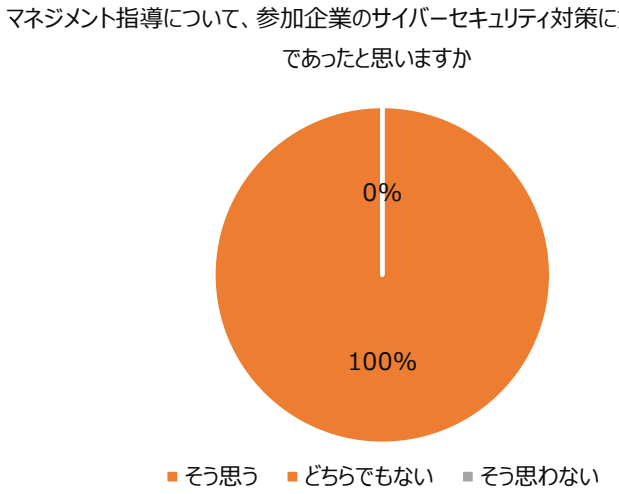
図表 2-56 指導専門家ごと・テーマごと指導件数

### 2.2.8. 指導終了後アンケート回答

マネジメント指導が終了した時点で、企業・指導専門家それぞれに完了後アンケートを実施した。アンケート集計結果は以下（抜粋）のとおり。

■マネジメント指導の企業のサイバーセキュリティ対策への貢献（指導専門家）

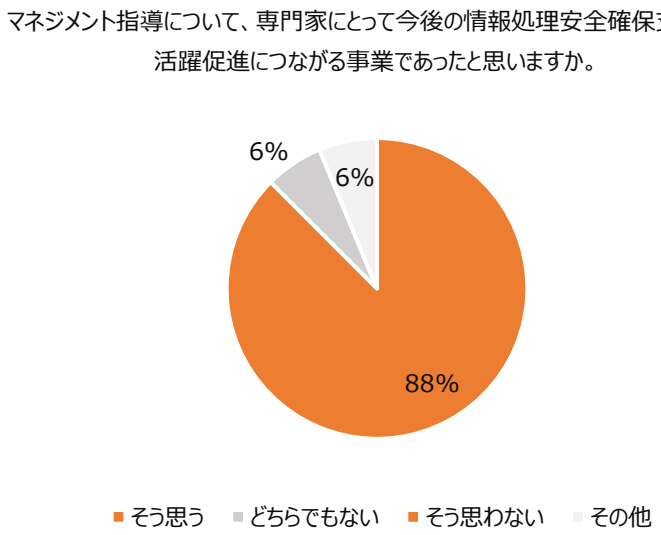
「マネジメント指導は、参加企業のサイバーセキュリティ対策に貢献した事業であったか」との問には、すべての指導専門家が「貢献した」と回答した。




図表 2-57 マネジメント指導の成果（企業のサイバーセキュリティ対策への貢献）に対する考え方（指導専門家の意見）

■マネジメント指導の登録セキスペ活用への貢献（指導専門家）

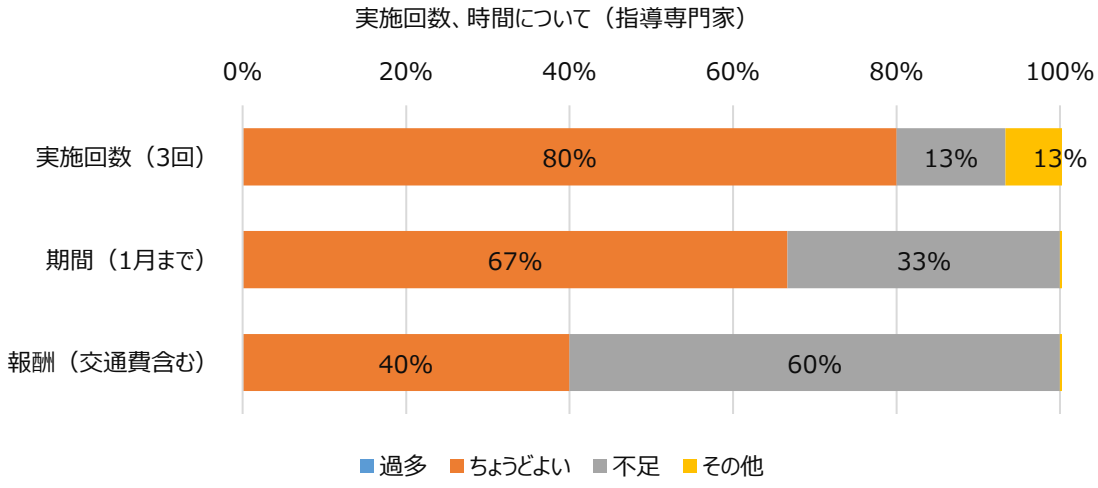
「専門家にとって情報処理安全確保支援士の活躍促進につながる事業であったと思うか」との設問では、9 割近い指導専門家がその効果を確信する結果となった。




図表 2-58 マネジメント指導が登録セキスペの活躍促進につながるかどうか（指導専門家の意見）

■マネジメント指導の適正な実施回数・時間・報酬（指導専門家）

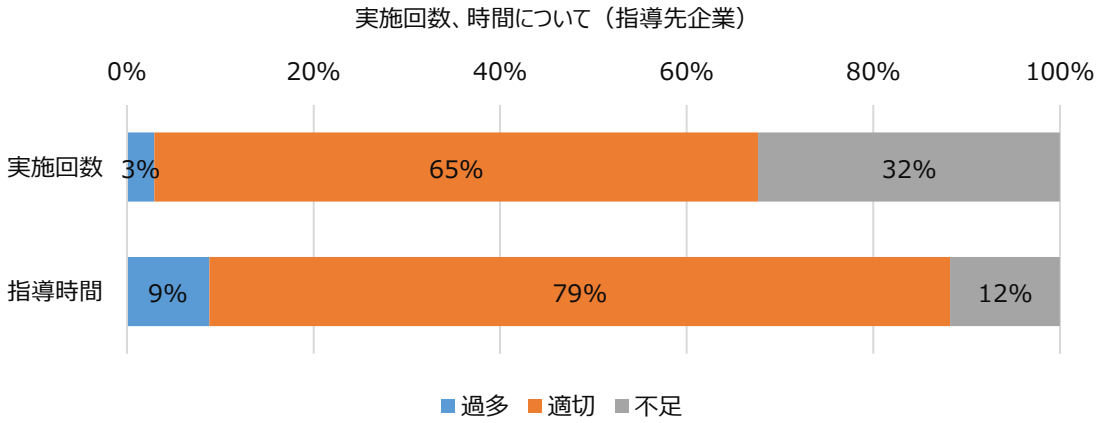
今回の支援事業について、それぞれ「実施回数」（最大３回）、「実施期間」（１月まで）、「報酬」（交通費を含む）の妥当性についての設問が以下である。回数・期間は「ちょうどよい」と回答した指導専門家が目立ったが、「報酬」については６割の指導専門家が「不足」であると回答した。




図表 2-59 マネジメント指導の実施回数・時間についての意見（指導専門家の意見）

■マネジメント指導の実施回数・時間の評価（指導先企業）

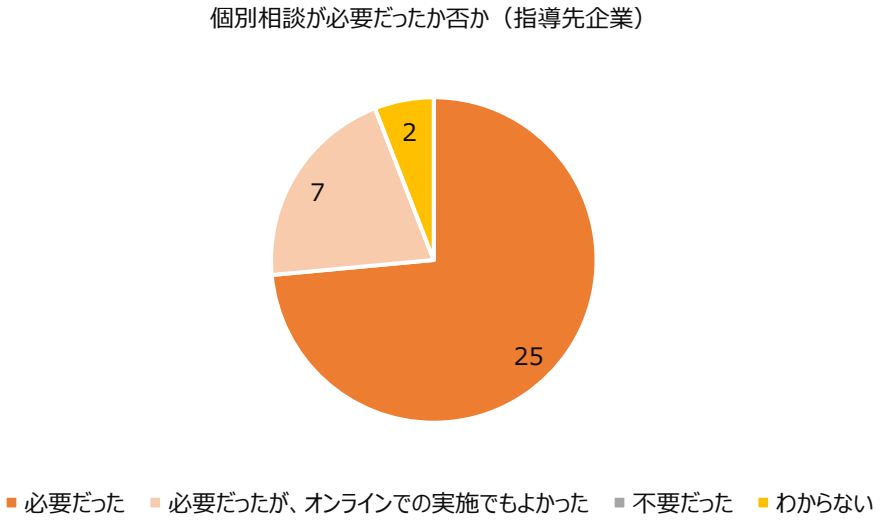
一方、同様の設問について、指導先企業の回答は以下のような結果であった。




図表 2-60 マネジメント指導の実施回数・時間についての意見（指導先企業の意見）

■個別相談の必要性（指導先企業）

指導先企業に対し、マネジメント指導実施に先立って実施した個別相談の必要性について尋ねたのが以下の設問である。ほとんどの企業が「事前の個別相談があってよかった」と回答した。その理由は多くが「先に大まかな課題を相談することで、訪問時の指導がスムーズに行えた」「企業だけではっきり課題が見えていなかったが、指導専門家と話すことで当面取り組むべきポイントが明らかになった」等の意見が得られた。

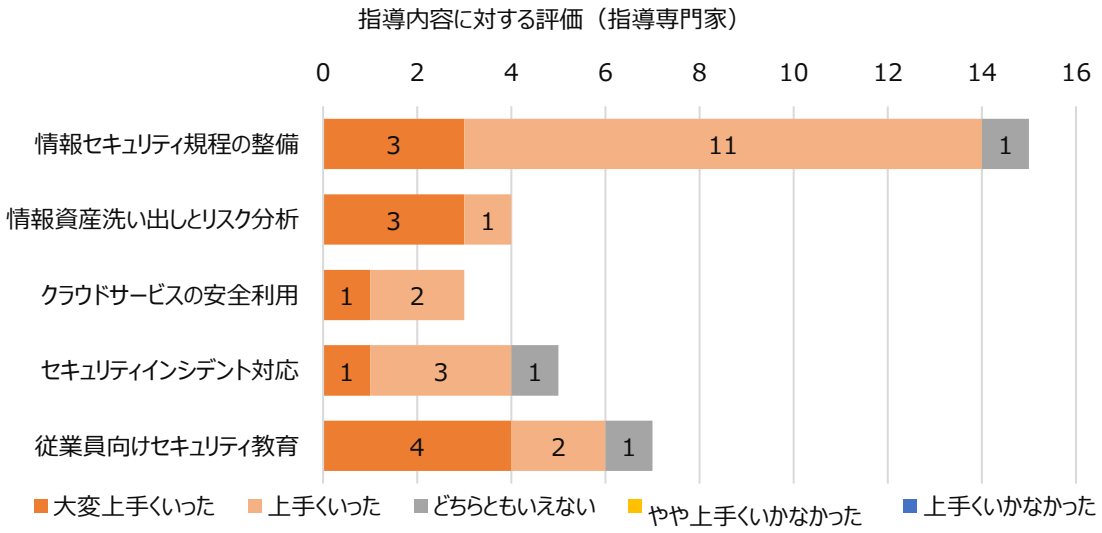



図表 2-61 個別相談の必要性（指導先企業意見）

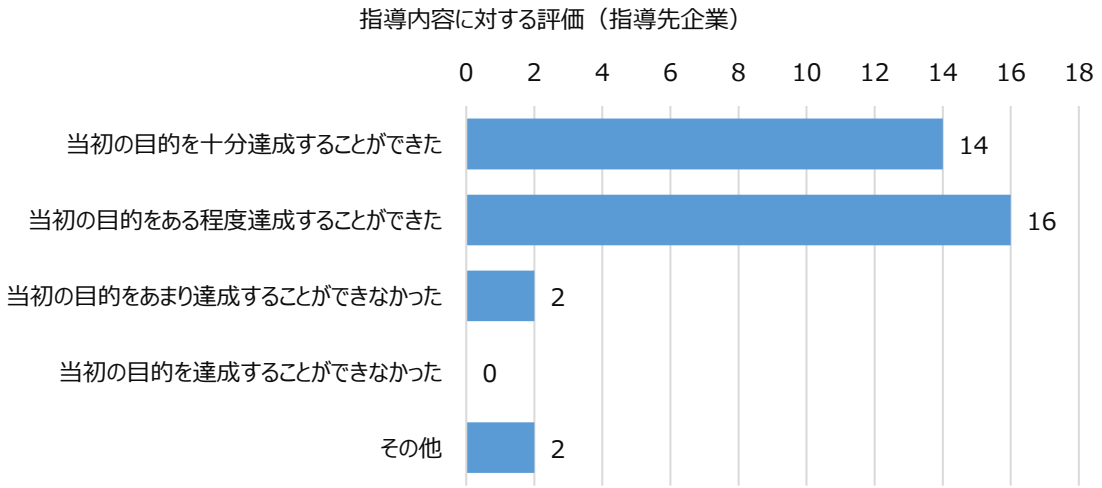
■指導内容に対する評価（指導専門家、支援先企業）

指導内容についての評価としては、指導専門家側の評価では、テーマにかかわらずほとんどの案件で「うまくいった」旨の回答が得られた。一部、3 回の訪問指導では目標とするレベルまで達することが時間的に難しかったもの等があったが、概ね 3 回の指導の中で成果を上げることができたものと思料する。

これは指導先企業から見た結果にも表れており、当初想定していた結果を十分あるいはある程度達成できたという回答が大半を占めた。




図表 2-62 指導内容に対する評価（指導専門家の意見）




図表 2-63 指導内容に対する評価（指導先企業の意見）

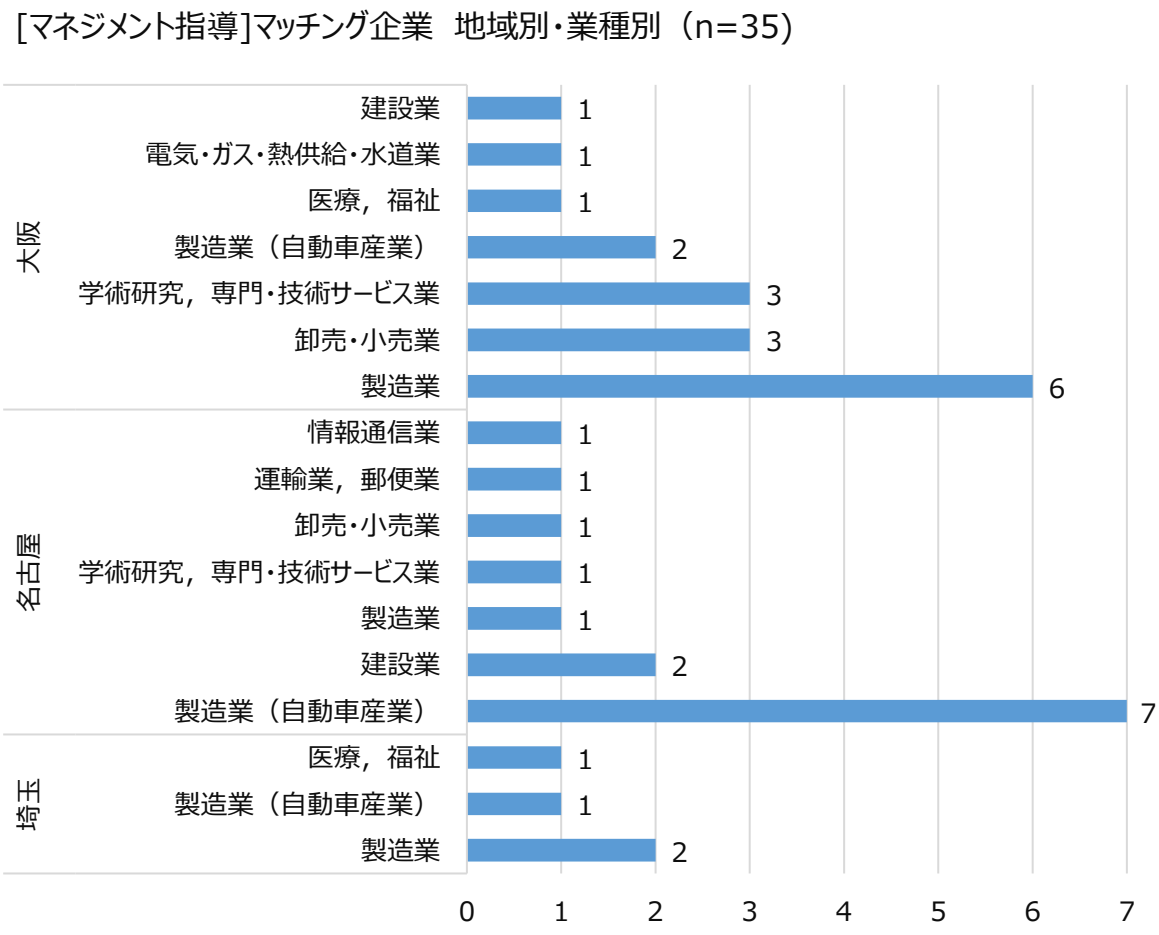
### 2.2.9. 訪問指導の実施結果

（１） 全体状況

（ア） マッチング：マネジメント指導移行 35 社の業種、地域

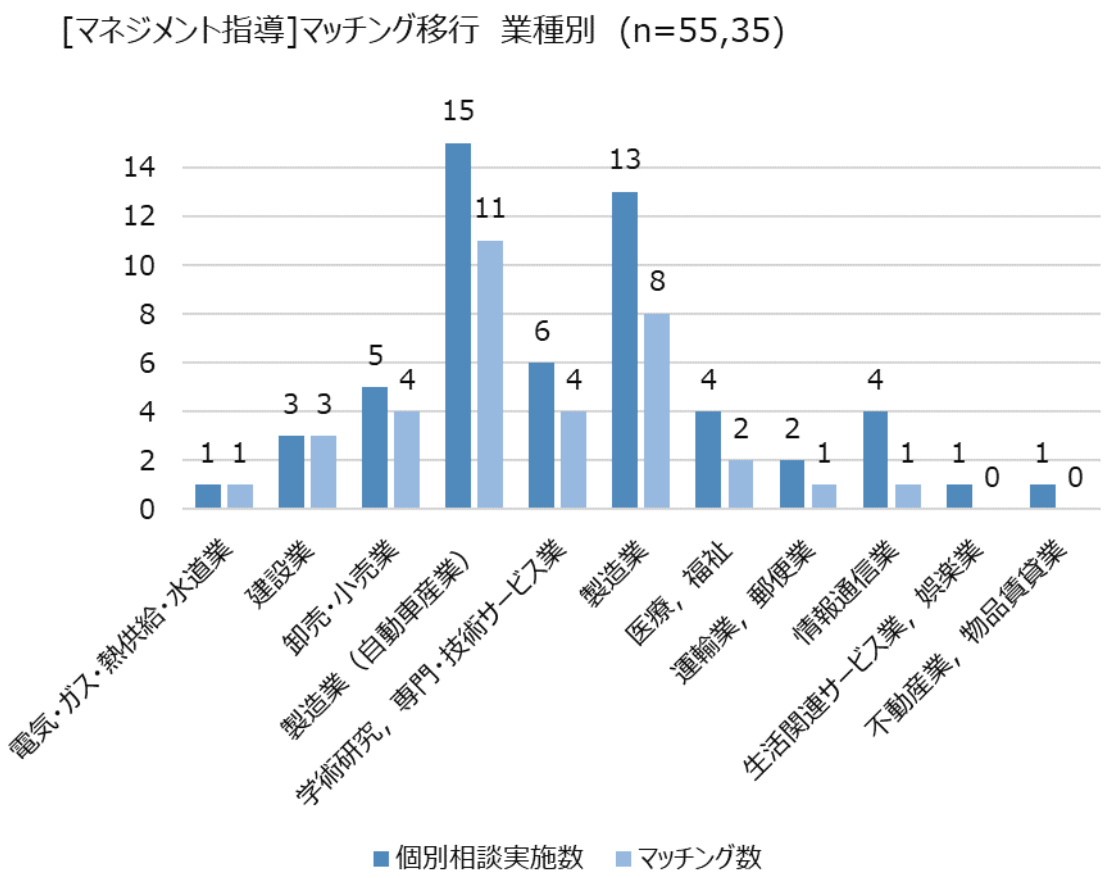
個別相談（55 社）を経て、マネジメント指導にマッチングできた企業は 35 社であった。

マッチングした企業の地域、業種別の集計は以下の表のとおり。多様な業種の企業が指導専門家との話し合いの上、マネジメント指導に進むことを決定した。




図表 2-64 マネジメント指導のマッチング企業（地域別・業種別）

35 社の業種ごとの、個別相談からマネジメント指導への移行率を以下のグラフで示す。どの業種も移行率に大きな偏りがない。最も高い移行率を示した業種は、「電気・ガス・熱供給・水道業」、「建設業」、「卸売・小売業」、「製造業（自動車産業）」の 4 業種であった。




図表 2-65 マネジメント指導への移行（業種別）

（イ） マッチング：マネジメント指導辞退 20 社の分析

個別相談を実施後、マネジメント指導へ移行しなかった企業は 20 社であった。この 20 社について、マネジメント指導に進まなかった理由を調査した結果、理由としては１．相談事が個別相談で解消できた ２．社内のスケジュールとの競合 ３．現状が継続した支援を求めていない４．その他 の４パターンに分類された。

マネジメント指導へ移行しなかった理由(n=20)

| 辞退パターン | 件数 |
|---|---|
| 1.相談ごとを、個別相談で解消できた | 7 件 |
| 2.社内のスケジュールとの競合 | 3 件 |
| 3.現状、訪問支援を求めていない | 4 件 |
| 4.その他 | 6 件 |

図表 2-66 マネジメント指導へ移行しなかった理由

「1.相談ごとを、個別相談で解消できたケース」については、「自社のネットワーク構成」「インシデント対応計画」について、企業側が資料を持ち込み、ピンポイントで質問をするような相談であった。

「2.社内のスケジュールとの競合」のケースは、企業側に既に実行、計画されているプロジェクトがあるため、本事業のスケジュールとの都合が合わないケースであった。

「3.現状、訪問支援を求めていない」ケースは、指導専門家からマネジメント指導の提案をしたものの、「現状、支援を求めていない」との理由でマッチングが不成立に終わったケースである。

４．「その他」については、「経営者の判断による辞退」 が 3 件、「個別相談で期待していた回答が得られなかった」が 2 件、「何を指導してもらうのかが分からないので辞退する」が 1 件であった。

このうち、「個別相談で期待していた回答が得られなかった」とされたケース 2 件の詳細を、企業へのヒアリングと指導専門家の相談報告結果から記す。

| | 企業の辞退理由 | 指導専門家の個別相談報告 |
|---|---|---|
| 1 | インシデント発生時の対応や、サイバー保険等を相談したかったが、指導専門家の領域外であるとのことであった。 | 同業他社がサイバー被害に遭ったことを受け、インシデント発生時にどの範囲まで取引先に責任を追い、それは金額換算でいくらになるのか、どこまで対策をすれば責任を追わなくて済むか知りたいとのことだった。責任範囲や想定される被害金額はケースバイケースなのでアドバイスは実施していない。手始めに情報資産の洗い出しとリスク分析を薦めたが、ご本人の関心は薄かった。 |
| 2 | インシデント時の責任体制の構築や連絡先の整備など、社内の体制や運用に関する相談をしたが、思っているような回答を得られなかった。 | インシデント対応の体制を CSIRT に昇格し、日本シーサート協議会に参加して、他企業と情報交換をしてはどうかとアドバイスをおこなった。企業規模からいえば、大企業であるのでより専門的な情報の入手先や窓口が求められていた。 |

図表 2-67 個別相談で期待していた回答が得られなかった」としてマネジメント指導を辞退したケースの詳細

２件とも、個別相談内容が、マネジメント指導において指導が可能な範囲の内容でなかった様子がうかがえる。

（ウ） マネジメント指導テーマ、業種別、地域別分布状況

マネジメント指導テーマの、業種別、地域別分布状況は下記のとおりとなった。５つのテーマが満遍なく多様な業種、地域で採用されていた。

【地域別・マネジメント指導実施件数】

| 地域 | 指導テーマ | 件数 |
|---|---|---|
| 大阪 | １．情報セキュリティ規程の整備 | 10 件 |
| | ２．情報資産の洗い出しとリスク分析 | 1 件 |

| 地域 | 指導テーマ | 件数 |
|---|---|---|
| | ３．クラウドサービスの安全利用 | １件 |
| | ４．セキュリティインシデント対応 | １件 |
| | ５．従業員向けセキュリティ教育 | ４件 |
| 名古屋 | １．情報セキュリティ規程の整備 | ３件 |
| | ２．情報資産の洗い出しとリスク分析 | ３件 |
| | ３．クラウドサービスの安全利用 | ２件 |
| | ４．セキュリティインシデント対応 | ４件 |
| | ５．従業員向けセキュリティ教育 | ２件 |
| 埼玉 | １．情報セキュリティ規程の整備 | ３件 |
| | ２．情報資産の洗い出しとリスク分析 | １件 |

図表 2-68 地域別・マネジメント指導実施件数

【業種別・マネジメント指導実施件数】

| 業種 | 指導テーマ | 件数 |
|---|---|---|
| 製造業（自動車産業） | １．情報セキュリティ規程の整備 | ３件 |
| | ２．情報資産の洗い出しとリスク分析 | ２件 |
| | ４．セキュリティインシデント対応 | ３件 |
| | ５．従業員向けセキュリティ教育 | ２件 |
| 製造業 | １．情報セキュリティ規程の整備 | ６件 |
| | ２．情報資産の洗い出しとリスク分析 | １件 |
| | ５．従業員向けセキュリティ教育 | ２件 |
| 学術研究，専門・技術サービス業 | １．情報セキュリティ規程の整備 | ２件 |
| | ４．セキュリティインシデント対応 | １件 |
| | ５．従業員向けセキュリティ教育 | １件 |
| 卸売・小売業 | １．情報セキュリティ規程の整備 | ３件 |
| | ２．情報資産の洗い出しとリスク分析 | １件 |
| 建設業 | ３． クラウドサービスの安全利用 | ３件 |
| 医療，福祉 | １．情報セキュリティ規程の整備 | １件 |
| | ５．従業員向けセキュリティ教育 | １件 |
| 電気・ガス・熱供給・水道業 | １．情報セキュリティ規程の整備 | １件 |
| 情報通信業 | ２．情報資産の洗い出しとリスク分析 | １件 |
| 運輸業，郵便業 | ４．セキュリティインシデント対応 | １件 |

図表 2-69 業種別・マネジメント指導実施件数

（エ） マネジメント指導完了状況

マネジメント指導完了状況について、35 社中 32 社が全 3 回の指導を完了、2 社が 2 回目の指導で終了、1 社がマネジメント指導開始直前に辞退をした。辞退理由は、業務が繁忙のため、指導を受けるために必要な社内の体制を整えることができないとのことであった。

【指導テーマ別｜マネジメント指導プログラム完了状況一覧】

| 指導テーマ | マッチング企業数 | 事前辞退 | 2 回目の指導で終了 | 3 回の指導を終了 |
|---|---|---|---|---|
| 1．情報セキュリティ規程の整備 | 16 社 | 1 社 | 1 社 | 14 社 |
| 2．情報資産の洗い出しとリスク分析 | 4 社 | | | 4 社 |
| 3．クラウドサービスの安全利用 | 3 社 | | | 3 社 |
| 4．セキュリティインシデント対応 | 5 社 | | 1 社 | 4 社 |
| 5．従業員向けセキュリティ教育 | 7 社 | | | 7 社 |

図表 2-70 指導テーマ別｜マネジメント指導プログラム完了状況一覧

また、2 回の指導でマネジメント指導を終了した 2 社については、両者とも指導ツールで指定されたゴールを未達成のまま、自ら指導の中断を決断した。2 社の辞退理由は以下のとおり：

| | 指導 2 回目でマネジメント指導を終了した理由 |
|---|---|
| 1 件目 | 繁忙期と社員の退職が重なり、指導を受ける余裕がなくなった。当初の目標であった 2 つ星は、計 2 回の指導で取得できたため、区切りもよい。 |
| 2 件目 | 目標としていたインシデント訓練シナリオの見直しが 2 回目の指導で終了したため。 |

図表 2-71 指導 2 回目でマネジメント指導を終了した企業の辞退理由

（オ） マネジメント指導実施後評価（マネジメント指導終了後アンケート調査による）

マネジメント指導完了後、企業と指導専門家両方に指導の満足度等を聞く指導終了後アンケートを実施した。指導テーマ別に、指導専門家、指導先企業のマネジメント実施評価を一覧にした表を下に示す。

【指導テーマ別 指導専門家・企業 マネジメント指導実施評価一覧】

| 指導テーマ | 実施件数 | 指導専門家評価 | 企業評価 |
|---|---|---|---|
| 1.情報セキュリティ規程の整備 | 15 件 | ◎ 3<br>〇11<br>△1 | ◎9<br>〇5<br>△ 1 |
| 2.情報資産の洗い出しとリスク分析 | 4 件 | ◎ 3<br>〇1 | ◎1<br>〇3 |
| 3.クラウドサービスの安全利用 | 3 件 | ◎1<br>〇2 | 〇 2<br>△ 1 |

| 指導テーマ | 実施件数 | 指導専門家評価 | 企業評価 |
|---|---|---|---|
| 4.セキュリティインシデント対応 | 5 件 | ◎1<br>〇3<br>△1 | ◎3<br>〇2 |
| 5.従業員向けセキュリティ教育 | 7 件 | ◎4<br>〇2<br>△1 | ◎1<br>〇4<br>△ 1<br>不明 1 |

図表 2-72 指導テーマ別 指導専門家・企業 マネジメント指導実施評価一覧

※◎は「指導が大変成功した」（指導専門家）、「当初の目的を十分達成できた」（企業）
〇は「指導が成功した」（指導専門家）、「当初の目的をある程度達成できた」（企業）
△は「指導の成果はどちらともいえない」（指導専門家）、「当初の目的をあまり達成できなかった」（企業）を表す。

指導専門家・指導先企業共に、概ねマネジメント指導は成功であったと評価したが、指導専門家から 3 件、指導先企業からも 3 件ずつ、指導成果が出なかったとする意見も聞かれた。

また、全体的な傾向としては、「情報セキュリティ規程の整備」、「セキュリティインシデント対応」については、指導専門家が指導先企業の評価と比べて自身の指導について低い評価を下しており、一方で、「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」、「従業員向けセキュリティ教育」の指導結果については、指導先企業の方が指導専門家の評価と比べて厳しい評価を下す傾向もうかがえた。

（２）　指導テーマごとの分析

（ア）【１．情報セキュリティ規程の整備（全 15 件）】

| | | 指導専門家 | | |
|---|---|---|---|---|
| | | 指導は大変成功した | 指導は成功した | どちらともいえない |
| 指導先企業 | 当初の目的を十分達成した | 2 | 7 | 0 |
| | 当初の目的をある程度達成した | 1 | 4 | 0 |
| | 方向性が違った（当初の目的をあまり達成できなかった） | 0 | 0 | 1 |

図表 2-73 マネジメント指導の評価（情報セキュリティ規程の整備）

テーマ「情報セキュリティ規程の整備」15 件の指導結果においては、指導専門家、指導先企業の指導の評価は概ね一致した結果となった。

・「当初の目的を十分達成できた」と回答した企業 8 社

「当初の目的を十分達成できた」と回答した 8 社からは、「当初の目標どおりの成果が得られた」、「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、設定した目標を達成できたとの評価が多く寄せられた。また、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や、セキュリティ・DX に関する役員を交えた協議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。

・「当初の目的をある程度達成できた」と回答した企業 5 社

「当初の目的をある程度達成できた」と回答した 5 社からは、達成度が限定的となった理由として、主に自社側の課題が挙げられた。「2 時間×3 回という指導時間では、IT 知識の少ない担当者には消化が難しく、社内の協力を得るのに苦労した」、「目標に向けて進められたものの、自社の知識や体制が不十分で、十分な成果を上げられなかった」など、長期的、組織的な視点から評価している姿が見て取れる。

・専門家が「どちらともいえない」、企業が「方向性が違った」と回答した 1 件

一方、指導専門家が「どちらともいえない」、指導先企業が「方向性が違った」と評価した 1 件について、指導専門家は当該指導の振り返りとして、「社員の退職があり指導が 2 回で終了、規程の作成という目標を達成することができなかった」と回答。一方で、指導先企業側は「リスクの洗い出し、具体的な対応策のアドバイスが欲しかったが、訪問の内容が規程を作成という方針だったので、希望と合わなか

った」と回答し、双方の認識に相違がみられた。

個別相談の記録をたどると、当初、指導先企業は個人情報漏洩への危機感から、情報資産の洗い出しとリスク分析を希望していた。しかし、指導専門家は、より本質的な課題解決のため、セキュリティ基本方針と規程の整備を優先すべきと判断し、マネジメント指導をテーマ「1.情報セキュリティ規程の整備」のもと、進められていた。このケースは、指導専門家の適切な見立てと指導先企業側の直接的なニーズとの間のギャップが最後まで解消されなかった例といえる。ただし、これはどちらかの過失というよりも、優先順位の認識の違いによって生じた結果と考えられる。

（イ） 【２．情報資産の洗い出しとリスク分析(全４件)】

| | | 指導専門家 | | |
|---|---|---|---|---|
| | | 指導は大変成功した | 指導は成功した | どちらともいえない |
| 指導先企業 | 当初の目的を十分達成した | 1 | 0 | 0 |
| | 当初の目的をある程度達成した | 2 | 1 | 0 |
| | 当初の目的をあまり達成できなかった | 0 | 0 | 0 |

図表 2-74 マネジメント指導の評価（情報資産の洗い出しとリスク分析）

指導テーマ「２．情報資産の洗い出しとリスク分析」 の指導 4 件においては、概ね指導専門家、指導先企業双方から、満足のいく指導であったとの評価が得られた。

・専門家が「指導は大変成功した」、企業が「当初の目的を十分達成した」と、双方の評価が合致した１ケース

本案件において、指導専門家は「同じ自動車関連の企業に勤めているものとして、困りごとを共有でき、的確にアドバイスした上で、自工会/部工会サイバーセキュリティガイドライン Lv2 の達成を実現できた」とし、企業は「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」と評価した。また、本ケースを個別相談時までさかのぼると、当初、指導先企業は自工会/部工会サイバーセキュリティガイドラインにおける教育方法について相談したが、指導専門家は情報資産の洗い出しを優先すべきと判断した。当初の相談内容と実際の指導内容は異なっていたものの、指導専門家が同業種の経験を活かして企業の本質的なニーズ（自工会/部工会サイバーセキュリティガイドライン Lv2 の達成）を見抜き、適切な支援方針を提案できたことが成功につながったと考えられる。

・専門家が「大変成功した」、企業が「目標をある程度達成した」と両者に温度差が見られた２件

1 件目は、指導先企業から「整理事項の洗い出しは納得できたが、1 回の作業では十分な理解に至

らなかった」、「指導回数が不足していた」との声が聞かれた。一方で、専門家からは「良好な関係性を構築でき、助言を受け入れてもらえた。今後も継続的な支援を求められている。」と評価をしている。本要点については、指導先企業側からは「専門家の説明により各項目の理解が進んだ」との評価もあり、企業側は指導専門家の助言が正しいとは思いつつも、より実質的な課題解決を念頭に、当該評価を下したことが見て取れる。

2 件目は、指導先企業と指導専門家の着目点の違いが、評価の差となって表れた事例である。指導先企業からは「マネジメント指導を通じてセキュリティ意識は高まったものの、最終的には従業員一人一人の意識と知識が重要だと感じ、『個人のセキュリティ意識チェックシート』のような具体的なツールの必要性を感じている」との回答があった。一方、指導専門家は「中小企業の規模に即した情報資産の区分方法を用いて洗い出しを行ったことで、理解が促進されたのではないか」と技術面での成果を高く自己評価している。個別相談時を振り返ると、指導先企業は「セキュリティ対策の着手点が不明確」、「社員の意識向上が難しい」という課題を抱えていた。これに対し指導専門家は、「まずネットワーク構成図などのシステムの洗い出しを行い、その後にリスクを踏まえた従業員教育を進める」という段階的なアプローチを助言した。評価の差が生じた背景には、指導専門家が提供した技術的な指導は確かに適切であったものの、指導先企業側には「従業員の意識向上」という更なる課題が残されているという認識があったためと考えられる。つまり、この事例は技術面での成功と、組織面での課題という異なる次元での評価が混在していたケースといえる。

（ウ） 【３．クラウドサービスの安全利用(全 3 件)】

| | | 指導専門家 | | |
|---|---|---|---|---|
| | | 指導は大変成功した | 指導は成功した | どちらともいえない |
| 指導先企業 | 当初の目的を十分達成した | 0 | 0 | 0 |
| | 当初の目的をある程度達成した | 1 | 1 | 0 |
| | 当初の目的をあまり達成できなかった | 0 | 1 | 0 |

図表 2-75 マネジメント指導の評価（クラウドサービスの安全利用）

指導テーマ「３．クラウドサービスの安全利用」 ３件の指導結果においては、指導先企業が「当初の目的を十分達成した」と回答したケースはなく、「ある程度達成」が２件、「あまり達成できなかった」が１件となった。

・専門家が「大変成功した」、企業が「目標をある程度達成した」と回答した１件

本案件では、指導専門家は「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提案した」と回答した一方で、指導先企業は「クラウドサービス導入時の注意点などを教えていただいたので、今後の規定整備に役立てたい」と回答をした。指導専門家が技術的観点に基づく助言をしたが、指導先企業は、将来の規程作成という別の目標に重点を置いた評価となっている、この案件は、当初は指導専門家から「情報セキュリティ規程の整備」を提案されていたところを、指導先企業の要望により「クラウドサービスの安全利用」テーマに変更になったという経緯がある。つまり、当該評価は、指導専門家に対するものではなく、あくまでも指導先企業側のセキュリティ対策状況に関する自己評価であると考える。

・専門家が「指導は成功した」としたが、企業が「目標をあまり達成できなかった」と回答した１件

指導専門家は、「指導先社長の疑問点に丁寧に回答していることで信頼を得られた。指導終了後も継続して連絡があり、指導に対する満足度は高かったと考える」と対話面での成功を自己評価しているが、指導先企業側からは指導の本質的な有効性について、「クラウドサービスの評価が中心でしたが、採用しているツールが業界上位のものが多く、企業としての信頼性が高いことが明らかであり、クラウドサービス提供会社の社会的な影響力や企業規模を鑑みると分析する必要があったのか疑問でした。また、クラウドサービスについて実質的なセキュリティの強化やルール作りが果たせなかった」と回答があった。本案件については、３回の指導終了後も指導専門家と指導先企業の間で継続的な連絡が保たれており、良好な関係性が構築されていることは確かである。しかし、指導先企業が必要としていた具体的なクラウドサービス利用のルール作りに対して、提供された支援内容（クラウドサービスの評価）が適切に対応できていなかったことが、支援に対する評価の違いとなって表れている。指導先企業はマネジメント指導において、現状の改善に向けた実質的な支援を求めていたことが示唆された。

（エ）【４．セキュリティインシデント対応(全５件)】

| | | 指導専門家 | | |
|---|---|---|---|---|
| | | 指導は大変成功した | 指導は成功した | どちらともいえない |
| 指導先企業 | 当初の目的を十分達成した | 1 | 2 | 0 |
| | 当初の目的をある程度達成した | 0 | 1 | 1 |
| | 当初の目的をあまり達成できなかった | 0 | 0 | 0 |

図表 2-76 マネジメント指導の評価（セキュリティインシデント対応）

指導テーマ「４．セキュリティインシデント対応」のマネジメント指導結果 5 件においては、全体的に指導先企業と比べ、指導専門家のほうが、より厳しく指導を高く評価している傾向があった。

・専門家が「大変成功した」、企業も「目標を十分達成した」と回答した１件

当該案件については、指導専門家は「自身の経験をもとに、ともするとシステム対応に偏りがちなインシデント対応訓練を、顧客、経営、対外的な対応等を含む組織的訓練となるよう設計した」と回答、また指導先企業側からも、「演習の実施が良好な社員教育となった」との回答を得られた。指導専門家の経験を活かし、指導先企業の深層ニーズに合致した訓練支援を実施できたことが、高評価につながったと考える。

・専門家が「指導は成功した」、企業が「目標を十分達成した」と回答した２件

当該２件について、指導専門家は、「指導先企業が小規模事業者だったため、今後も必要となる外部の専門家との連携支援策を提示出来なかった」、「もっと他社事例を踏まえた内容で訓練を実施したかった」など、と回答。一方で、指導先企業は「2 月に社内でインシデント訓練を予定しており、その訓練シナリオの検討に大いに役立った」、「自社ができていることとできていないことがクリアになった」と回答していることから、指導先企業側の実務的ニーズは満たされたものの、指導専門家側が、より実践的な目標を設定しており、その目標に 3 回の指導では到達できなかったものと解釈される。

・専門家が「どちらともいえない」と回答するも、企業が「目標をある程度達成した」と回答した１件

当該案件については、指導専門家は「3 回の訪問回数では、既存のインシデント対応手順のブラッシュアップや実際の訓練の実施までたどりつくのが難しかった。」と指導目標の未達成を指摘。一方、指導先企業は「経営層を含めたインシデント対応について、十分に策定できなかった」とするものの、「インシデント対応訓練の手順、対応フローの修正は完了した」と回答しており、指導先企業としては、指導を通じて課題がある程度解決されたことを示唆している。目標の達成に至らなかった理由として、指導先企業側から指導専門家の時間配分について低めの評価があったことを考慮すると、指導専門家の時間管理能力や指導推進力が、課題であったことを示している。

（オ） 【５．従業員向けセキュリティ教育(全７件)】

| | | 指導専門家 | | |
|---|---|---|---|---|
| | | 指導は大変成功した | 指導は成功した | どちらともいえない |
| 指導先企業 | 当初の目的を十分達成した | 1 | 0 | 0 |
| | 当初の目的をある程度達成した | 1 | 2 | 1 |
| | 当初の目的をあまり達成できなかった | 1 | 0 | 0 |

| | | | | |
|---|---|---|---|---|
| | 不明 | 1 | 0 | 0 |

図表 2-77 マネジメント指導の評価（従業員向けセキュリティ教育）

指導テーマ「5．従業員向けセキュリティ教育」 7 件のマネジメント指導結果について、全体的に指導専門家の満足度は高いものの、指導先企業側は控えめに評価とする傾向がみられた。

・専門家が「大変成功した」、企業も「目標を十分達成した」と回答した 1 件

当該案件については、指導専門家は「機微な情報を取り扱う業界だったため、企業からのリクエストのもと、個人情報の取り扱いの説明を加えた従業員教育を実施した」と回答、また、指導企業側も、「初めての社員教育だったが、法人内での従業員の意識向上につながり、また、法人内でのセキュリティポリシーの策定に向けて動くきっかけとなった」と回答した。

本件を個別相談までさかのぼると、当初、指導専門家は、指導先企業の対策状況を聞き取り、まずは「情報セキュリティ規程の整備」から開始する必要があると判断していた。しかし、取引先からの要請に対応しなければならないという指導先企業の状況を踏まえ、今回のマネジメント指導では従業員向けセキュリティ教育から着手するアプローチを選択した。その結果、指導先企業が自ら次のステップとして「情報セキュリティ規程の整備」の必要性を認識するに至ったことは、支援の成功を示している。一見遠回りに見えるが、このアプローチは、指導先企業の実情と優先順位に寄り添うことで、より確実な成果につながった好例といえる。

・専門家が「大変成功した」、企業が「ある程度達成」「あまり達成できなかった」[不明]と回答した 3 件

指導先企業が「ある程度達成」と回答した 1 件については、指導専門家は、「攻撃手法の専門用語を受講者わかりやすく説明できた」としたものの、指導先企業は「DX 推進室のメンバーは理解できたが、製造現場や他の間接部門のメンバーは理解できなかった。今後の課題として社内教育の見直しを行う」と回答した。これは、中小企業の実情に即した説明レベルの設定が課題であったと考えられる。

「あまり達成できなかった」と回答した 1 件については、指導専門家は「教育を通じて、セキュリティ規定の見直しや、今後必要な対策の道筋を作ることができた」と成果を回答した一方で、指導先企業は「経営層が時間の都合上、研修に参加できなかった。経営層へのセキュリティ教育が課題として残った」と回答。ここには、指導先企業の本質的なニーズを十分に把握しないまま、自己評価を行った専門家側の課題が表れている。

指導の目標達成度を「不明」と回答した 1 件については、指導先企業はその理由として、「従業員の意識変容を数値化できない」ことをあげ、さらに「実際の社内運用」を今後の課題としても挙げており、今回の支援を一過性のものとして終わらせるのではなく、継続的な組織変革の一環として捉える誠実な姿勢を示している。一方で、指導専門家は「数十名の参加者を得た研修の実施」という定量的な成果を評価しており、支援の評価軸における時間的視野の違いが表れている。

・専門家が「どちらともいえない」、企業が「ある程度達成」と回答した 1 件

当該案件については、指導専門家は「申込時の依頼内容が初回のヒアリングにより変更になったため、中途半端な結果に終わった」と評価している。一方、指導先企業は「従業員のセキュリティ教育の実施を通じて、業務規程を整備するきっかけとなった」と回答があった。

本件の経緯は、当初の個別相談時には担当者が「従業員セキュリティ教育」を希望していた。しかし、マネジメント指導当日に、経営層との話し合いによって、指導テーマが「情報資産の洗い出しとリスク分析」と変更になった。しかし、実際の指導の過程で再び担当者の意向により、「セキュリティ教育」に方向が変化した。ヒアリング結果、判明したことだが、セキュリティ担当者は現状の対策に特段の問題意識を持っていなかったのに対し、経営層は担当者の対策内容の可視化を求めており、そのために「情報資産の洗い出しとリスク分析」を提案したという状況があった。この事例は、中小企業が限られた人員体制の中で、経営層とセキュリティ担当者の間の認識のギャップが埋められないまま支援が進められた結果、指導の方向性が定まらなかったケースで、中小企業におけるセキュリティ対策の組織的な運用における典型的な課題を示唆していると言える。

（カ）　マネジメント指導前の個別相談の評価について

本事業のセキュリティマネジメント指導の実施にあたっては、前述のとおり、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指導専門家とのマッチングを行った。この点、マネジメント指導終了後アンケートの中で、指導先企業 34 社に対し、マネジメント指導前の個別相談の評価について意見を得た。以下にアンケート記述内容を記す。

**１．安心感**

- 「初めの一歩」の相談だったので、言葉のニュアンスや伝えたいことを、顔を見ながら話しことができたのでよかった。
- 情報セキュリティに関する無料の相談先が無かったのでうれしい。
- 指導いただく上でのアプローチとしては必要だと思う。
- 事前相談会無しで直接訪問による「マネジメント指導」だけだったら、なかなか申し込めなかった。
- セキュリティ対策の現状や、担当者の雰囲気などを直接見聞きでき、安心感があった。

**２．支援の方向性の明確化**

- 個別相談により、自社の状況に合った進め方を提示していただけた。
- 実施前に相談内容・情報を共有できた。
- 大体の方向性をお伝えできた。それによって大まかに事前準備ができた。
- 何ができていて、何を聞いてよいかが分からなかったが、相談ができて良かった。
- 分からないことを専門家に直接聞けるのはとてもありがたい。その場でクリアにならなくてもそのあと指導を受けられた点もとてもありがたかった。

**３．個別相談実施形式**

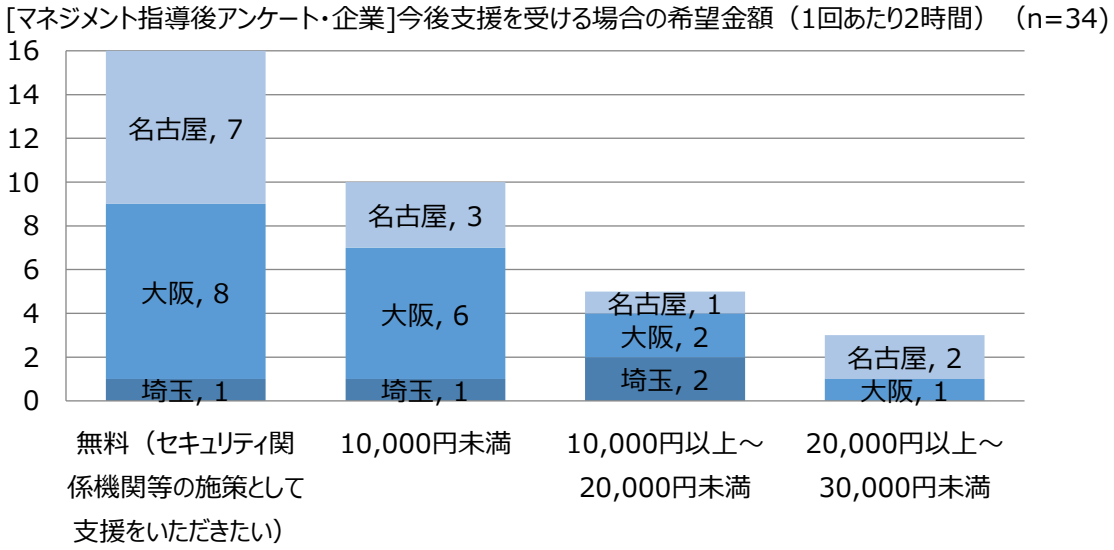
- 弊社はいくつかの相談内容があった為、事前相談の 20 分という短時間と感じた。オンラインにてもう+10 分あれば、もう少し個別相談する内容について、より具体的に絞り込めたのではないかと感じた。
- 個別相談自体はよかったが、形式については、オンラインでの個別相談でもよかった。対面でなくてはいけない理由はない。

意見を総合すると、個別相談の事前実施は、マネジメント指導の効果を高める重要なステップであり、事前の準備や方向性の整理、指導専門家との信頼関係構築において有効だったことが確認された。今後は、企業の相談内容に応じた適切な時間設定や、オンラインでの柔軟な対応などを検討することで、より広範囲な相談者に対し、支援をつなげられる可能性がある。

（３）　指導先企業の課題

（ア）　マネジメント指導料金

マネジメント指導終了後の指導先へのアンケート結果によると、約 47%の企業が「無料」の支援を希望すると回答。



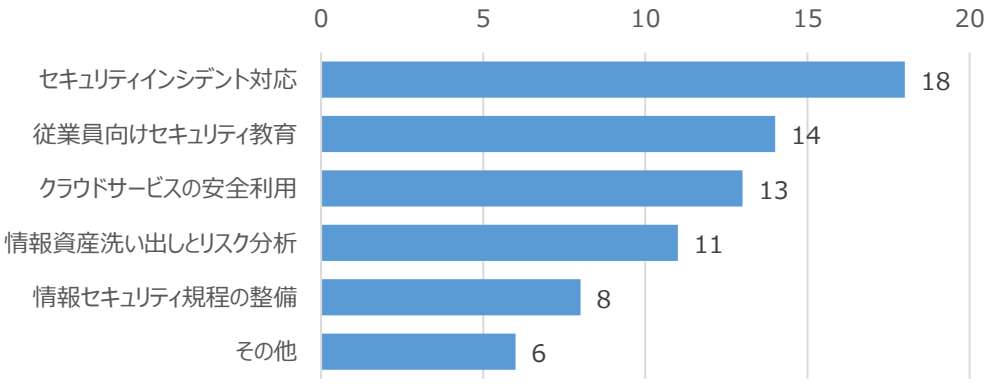

図表 2-78　今後指導を受ける場合の希望金額（1 回あたり）

「無料」の支援を希望する理由としては、「引き続きの指導をお願いしたと思っているが、簡単に有料で専門家の指導を受けることを決められない」、「有料支援については、どのような内容で、どのような効果があるか見極めてからの判断」、「1,2 回の無料指導の後、有償サポートを決定することは充分に考えられる」など、約半数の中小企業が、専門家による支援に対しての対価の支払いについて、慎重であることが判明した。一方で、「何かコトが起こった時は有料であろうがサポートをいただく必要がある」等、具体的な問題やインシデントが発生した際には、有償支援を是認する姿勢がうかがえた。

（イ）　今後支援を希望する指導テーマ

今回指導を受けた 34 社の約 53%が、今後支援を希望する指導テーマについて「セキュリティインシデント対応」と回答した。他にも「従業員向けセキュリティ教育」、「クラウドサービスの安全利用」が上位に来る結果となった

[マネジメント指導後アンケート・企業]今後指導を希望する指導テーマ
(n=34)（MA)




図表 2-79 今後指導を希望するテーマ

（ウ） 指導先企業のセキュリティ対策の課題

マネジメント指導終了後のアンケートで指導先企業からセキュリティ対策の課題として挙げられた点は、「専門知識が足りなく、専門家の指導内容をあまり理解できないメンバーもいた」、「指導期間が限られていたため、宿題をこなすことが難しかった」等、IT 知識や時間が足りないといった内容であった。

一方で、指導専門家からは、指導先企業の本質的な課題について指摘があった。以下に詳細を記す。

| 指導専門家からみた指導先中小企業の課題 |
|---|
| ①「中小企業だから」と担当者自らがセキュリティ対策の取り組みレベルを下げたり、諦めたりしている面も多く見受けられた。<br>②担当者が他の業務と兼務ということもあり、実務優先な傾向があり、実施している対策や課題等を経営層と共有できていないことがあった。<br>③「従業員教育にわざわざ時間を取るのが難しい」、「従業員の IT リテラシーが低いためどういった方法がよいかわからない」など、相談者（経営者）自身が教育実施に消極的なケースがあった。<br>④根強い組織文化についての悩み相談を受けた。情報セキュリティ対策を行うための経営層への動機付け、IT リテラシーの低いメンバーや消極的・協力してくれない中間管理職への関与のさせ方、推進方法、協力してくれる部署での担当者間での既成事実の推進等。<br>⑤ISO27000 取得企業であったが、従業員教育については未対応な面が多く見受けられた。必要性は認識されているものの、教育のための人員・時間を割くことを経営層及び各部門の管理者層に上申しても認められないと、担当者自身が感じていた。 |

図表 2-80 指導専門家による指摘（中小企業の課題）

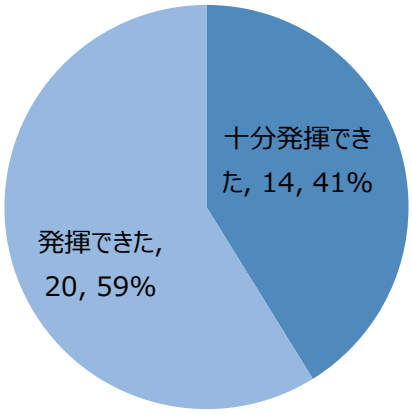
これらの課題は、経営者や組織など、「ひと」に関わるものが多く、中小企業に共通する問題である。課題に対応した指導専門家は、組織文化や人材不足といった中小企業の本質的な課題に直面し、対応の難しさを感じたとのことであった。

（４）　指導専門家の課題

（ア）　スキル発揮の機会

マネジメント指導終了後アンケートを実施した結果、34 件のマネジメント指導において、指導専門家全員が自身のスキルを発揮できる機会であったと回答した。

[マネジメント指導後アンケート・指導専門家]　マネジメント指導は、
自身のスキルを発揮する機会であったかについて（n＝34)




図表 2-81 マネジメント指導が自身のスキルを発揮できる機会であったか

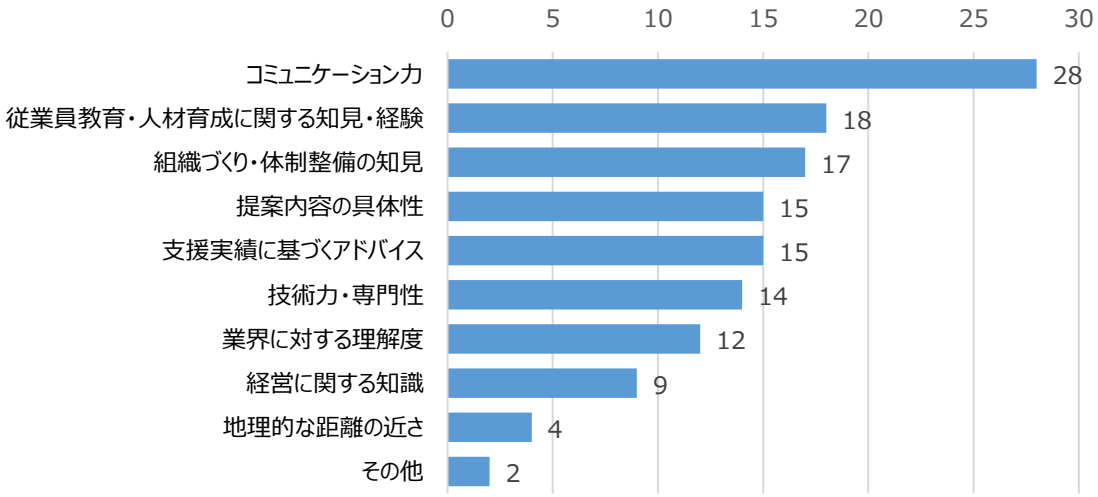
アンケート回答によると、「金融業での経験が主だが、システムのみでなく、顧客対応、経営的なもの、対外的な対応なども経験しており、それが役に立てた」、「CSIRT 構築支援の経験を活かせた」など、今までの自身の知識や経験が活かせたとするコメントや、「経営全般の事例を踏まえて対話」、「コンサルタントとしての傾聴ノウハウを活用」、「参加者の巻き込みを意識したファシリテーション」など、コミュニケーション面で自身の保有するセキュリティ以外の分野の知識やノウハウを活用できたとするコメントも目立った。

（イ）　指導を通じ、重要と感じたスキル

[マネジメント系]

指導専門家がマネジメント指導を通じて、重要と感じたスキルとして、最も多く回答が多かったのは「コミュニケーション力」で、次いで「従業員教育・人材育成に関する知見・経験」、「組織づくり・体制整備の知見」が挙げられた。

[マネジメント指導後アンケート・指導専門家]マネジメント指導を通じ、重要と感じたスキル
（n=16)(MA)




図表 2-82 マネジメント指導に際し重要であると感じたスキル

なぜ、「コミュニケーション力」、「従業員教育・人材育成に関する知見・経験」、「組織づくり・体制整備の知見」が重要と感じられたのかについて、別アンケート項目「指導するうえで苦労したことや工夫したこと」から読み取れることがあった。

以下の表のとおり、マネジメント指導で指導専門家が苦労・工夫した内容を分類した。

| 苦労した点・工夫した点 | 回答者数 |
|---|---|
| 1.担当者の理解度促進、支援の受け入れやすさの追求 | 13 |
| 2.組織の巻き込み | 11 |
| 3.時間配分等 | 5 |
| 4.自工会サイバーセキュリティガイドラインの理解 | 2 |
| 5.特になし | 3 |

図表 2-83 マネジメント指導に際して専門家が苦労・工夫した点

指導専門家が苦労した点、工夫した点として最も多く挙がったのは、「分かりやすい言葉の使用」、「やさしい理解度確認テストの作成」など、「企業側の担当者にとっての、支援の受け入れやすさの追求」であった。

また、次に回答が多かったものとしては、経営者の理解促進や、全社の巻き込みなど、「企業側が組織的に対策を進めるための支援」であった。この課題を克服するため、“組織全体の巻き込みを意識したファシリテーションを行った”などの対策を講じたなどの意見もあった。

以上のように、指導専門家は、マネジメント指導の効果的な実施に向けて、技術面以外でも多くの工夫を凝らしており、その結果が、( 2 )の重要と感じたスキル　の回答へとつながったと考えられる。

また、この結果からは、今後マネジメント指導の指導専門家を育成するにあたっては、コミュニケーション能力やファシリテーションスキルといったソフトスキルを養成するプログラムの開発も必要であると考える。

[技術・専門系]

マネジメント指導を実施後、指導専門家が重要と感じた技術・専門系のスキルには、以下のような意見があげられた。

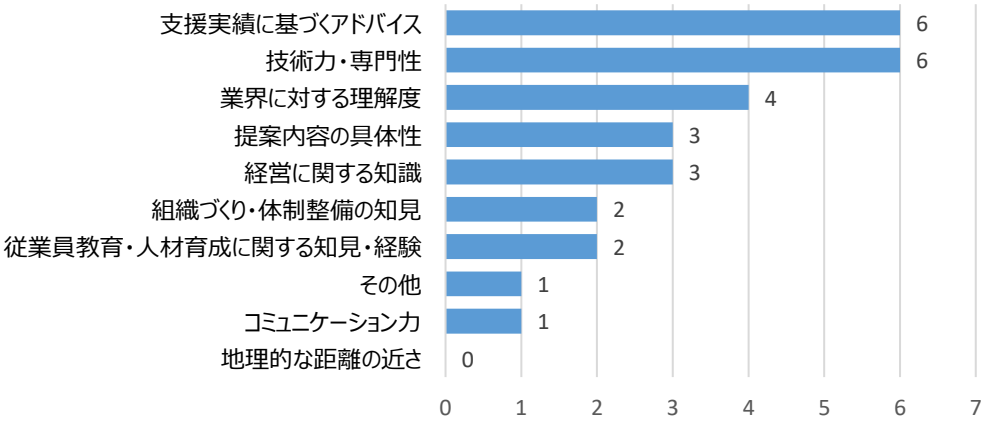
- 具体的なツールの機能などの知識が回答に必要な場面があった
- 最新のサイバーセキュリティに関するニュース
- Wi-Fi や NAS などの社内ネットワークに関する知識。
- 情報処理安全確保支援士レベルの「技術力・専門性」
- 情報資産の洗い出し、リスクアセスメントは、それほど技術力・専門性は必要無いが、対策についてはサイバーセキュリティに関する脅威、脆弱性の知識が必要
- Microsoft365 についての知識
- Windows パソコンの使い方、スマホの使い方
- リスク管理や BCP といった、分野での知識が役に立った。
- 自工会ガイドラインの理解度

これらから、マネジメント指導においてはマネジメント系スキルに加えて、上記のような技術・専門の知識が必要・重要と感じられていることが認識された。

（ウ）　指導を通じ、不足していたスキル

マネジメント指導終了後アンケートによると、現在、指導専門家自身に不足していると感じるスキルで最も回答が多かったものは、「支援実績に基づくアドバイス」、「技術力・専門性」であった。

[マネジメント指導後アンケート・専門家]中小企業を支援するにあたり、自身に不足しているスキル（n=16)(MA)




図表 2-84 指導に際し、不足していると感じたスキル

足りないとされる「技術力・専門性」の詳細について、下記の具体的な声があげられた。

- セキュアプログラミングに関する知識
- 具体的なセキュリティソリューションに関する知識、技術力
- 各種ツールの概要は理解しているが、長期運用や使いこなしの経験が不足
- モバイルは得意だが、PC 領域の最新技術
- ネットワーク関連の知識
- ソフトウェア・アプリ開発に関する知識・経験

これらは、最新のセキュリティ技術の知識や、実際のシステム運用に触れる機会が少ないセキュリティ専門家の現状が表れており、セキュリティ専門家の定期的な技術アップデートのニーズが示唆されているのではないかと考えられる。

「支援実績に基づくアドバイス」については、今回の実証事業のようなマネジメント指導の機会を増やすことが、直接的な解決策であると考えられる。

１つ特徴的な意見として、“マネジメント全般を担当しているが技術的なことは直接やっていないので、個人で行うというより、必要な要素に合わせてチームで対応する方法がよいと思う”という声があった。

セキュリティ対策支援の多様な側面（マネジメント、技術、コミュニケーション等）を考慮すると、異なる強みを持つ専門家がチームとして支援にあたる方式は、効果的なアプローチとして検討の価値があると考える。

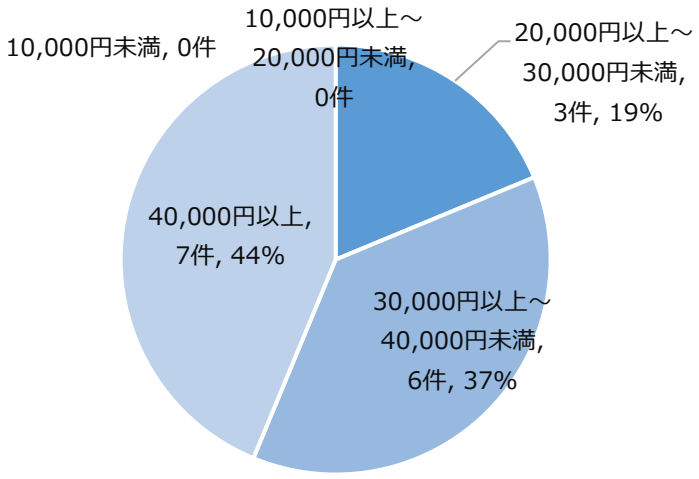
（エ） マネジメント指導料金

マネジメント指導終了後アンケート結果によると、今回の実証の報酬額については、約 56%が少ないと回答。「1 回の訪問につき 8 時間ほどを準備に費やす」、「時給換算すると、特定分野への専門家の

報酬とは思えない額」などの意見があった。

また、今回と同様ののマネジメント指導を実施する場合における、希望する報酬額は 4 割強が「40,000 円以上／回」と回答した。

[マネジメント指導後アンケート・専門家] 同様の内容のマネジメント指導について、適切と思われる報酬額 (n=16)




図表 2-85 今後同様のマネジメント指導を実施する際に適切であると思われる報酬額（専門家の意見）

### 2.2.10. マネジメント指導まとめ

①マネジメント指導の分析と示唆

指導先企業と指導専門家、双方から高い評価を得た指導事例に共通するのは、指導専門家が企業のニーズを的確に捉え、企業目線の支援を提供できていた点である。一方で、指導専門家が技術的な観点から必要と判断した支援内容（情報セキュリティ規程の整備や情報資産の洗い出し等）と、指導先企業が感じている課題との間にズレが生じていたケースにおいては、専門家の満足度に対して企業側の評価が低いケースが見られた。

従業員向けセキュリティ教育では、まず指導先企業の求める具体的な教育支援を実施し、その過程で規程整備等の必要性について企業の理解を促すというアプローチが効果的であった。また、指導の過程で支援テーマが変更されるケースや、時間配分に課題が見られたケース、指導ツールの内容と指導先企業のニーズが乖離していたケースなど、実践面での課題点も幾つか明らかになった。さらに、支援の評価についての課題も浮かび上がった。例えば、コミュニケーションが良好であったと指導専門家が自己評価したケースでも、指導先企業からは時間配分等に課題が指摘されるなど、専門家が自分では気づいていない課題を指導終了後アンケートで確認することができた。

今後は様々な指導事例を専門家間で共有する機会なども、セキュリティ専門家を支援するためには必要であると考えられる。

②指導先企業側の課題の現状と今後の希望

指導先企業側の現状の課題としては、「セキュリティに関する専門知識不足」を挙げる声が複数あった一方で、指導専門家が指摘した組織的な課題については、指導先企業のアンケート回答での言及は見られなかった。今後希望する支援内容としては、「インシデント対応」が最も多く、次いで「従業員セキュリティ教育」、「クラウドサービスの安全利用」が続いている。特筆すべき点として、上位 2 つの希望はサイバーセキュリティ相談会参加者アンケート結果と一致していた。

また、支援料金については、約半数の指導先企業が無料支援を希望した。一方で、セキュリティインシデントが発生した際の有償支援については、一定の受容性が確認された。これらの結果は、中小企業における支援費用の支出は、明確な投資対効果が認識できると思われた場合に、受容される傾向を示していると考える。また、多くの中小企業は、初めての支援では、「初回無料」を希望するとのことであった。

③指導専門家側の課題と改善点

マネジメント指導終了後アンケート結果からは、最新のセキュリティ技術の知識や実際のシステム運用に触れる機会が不足している指導専門家の現状が明らかとなった。また、指導先企業の組織に関する課題への対応に苦労したという声も、複数の指導専門家から挙がった。指導専門家の定期的な技術スキルのアップデートや、組織運営のノウハウを学ぶ機会へのニーズがあることがうかがえる。

支援料金については、44%の指導専門家が同様の内容の指導について 4 万円以上を希望しており、指導料金への意識については指導先企業との間で、乖離が見られた。

### 2.2.11. 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（指導専門家側・指導先企業側双方）から、指導実施により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、マネジメント指導事例集を作成した。取り上げた事例（7 社）は以下のとおり。

なお、いくつかの指導先企業は、事例としての活動内容の発表は可能であるものの、社名の特定を避けたいという希望があり、匿名（非公開）での掲載とした。

| No. | 地域 | 事例掲載企業・団体名<br>(順不同) | 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 | 高橋 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 |

図表 2-86 マネジメント指導事例（ベストプラクティス）掲載一覧

指導事例の掲載内容は、掲載企業の取組みや業界の動向等ビジネス環境を踏まえ、相談会・マネジメント指導に参加したきっかけ、情報セキュリティ上で感じていた課題等、加えて、企業の悩みを踏まえた専門家による指導のポイントを記載し、結果として得られた成果（企業側での変化）について整理した。ヒアリングに際しては、指導の際の状況に加え、事業全体への意見、とりわけ指導ツールや事務局対応等も含め忌憚のない意見をいただいた。

| 愛知県 | 事例No.1 |
|---|---|
| 業種 | 卸売業 |
| 従業員数 | 97人 |
| 資本金 | 5千万円以下 |
| 推進担当者 | 大坪 啓二 様（管理部 プロジェクトマネジャー） |
| 指導専門家 | 高橋 真悟（インフォシア 代表） |

**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**

深田電機株式会社

### ■企業・団体紹介

電設資材の商社として、国内の主要メーカーより電気設備に関わる資材を仕入れ、電気工事店や設備店に販売。また、顧客におけるエネルギーマネジメントやZEB（Net Zero Energy Building）に関するプランニングも行っている。

### ■参加の動機

同社では「DXで、社員のしあわせ、お客様のしあわせを！」をDX推進方針として掲げ、社内業務の効率化及び顧客サービスの向上を強力に推し進めている。2025年2月には「DX認定事業者」にも認定された。このDXの取り組みを進める上で、情報セキュリティ対策は最重要課題であると位置づけており、各種の規程運用や新たな取り組みを推進する上でのセキュリティ対策のあり方等について、具体的なアドバイスが欲しいと考えていた。そのような中で今回の相談会・個別指導の案内を入手したが、日ごろから活用している商工会議所からの案内ということもあって参加することとした。

### ■情報セキュリティ上で感じていた課題

- セキュリティに関する規程は整備して従業員に周知したものの、どこまで理解が進んでいるのかが不安であった。
- DXの取り組みを継続的に進めていく上で、規程やルールの見直しや改善を常に図っていくための運用方法について、専門的な見地からのアドバイスが欲しいと考えていた。

## 専門家指導のポイント

### ■整備済みセキュリティ規程について改善点を具体的に指示

最近になって整備した各種のセキュリティ規程をチェックし、曖昧な書きぶりになっていた点などについて改善案を提案。まず、情報セキュリティに関する各役職の役割と責任を明確にし、規程の見直し時期を明確に定めた。情報資産管理の面では、バックアップデータの管理方法やアカウントの整理などの具体的な管理方法を定め、セキュリティ領域を設定し入室管理を強化するなどの物理的対策を実施。さらに、重要データを安全に取り扱うためのチェック体制と、第三者への提供に関する対策などについても整備を行った。

### ■生成AIの利活用に向けて、制限と利用促進のバランスをとった形での規程作成を支援

DX活動の目玉として、業務の効率性アップやクリエイティビティ確保に向けて、同社では生成AIの社内利用を促進したいと考えている。一方で、これを安全に活用するための規程整備も必須であるとの考えから、今回の指導で「生成AI利活用時の規程」を整備することとした。

一方で、情報セキュリティを意識して過度に制限を設けたことで、かえって利用を阻害するようなことにはしたくないとの要望から、バランスも考え、他の機関のガイドライン等も参考にしつつ、独自の規程策定を後押しした。

また規程の周知・運用に向けた具体的なアドバイスも行った。

## 指導先企業からのコメント

### ■専門家指導の成果

- 短期間の指導の中で効率的にアドバイスをいただき、規程の運用改善のポイントを明らかにできた。また、生成AIに関するルール作成まで踏み込んでいただけたことで感謝している。

### ■ご意見・ご感想

今回の生成AI活用以外にも、RPA対応など、まだまだ対処しなければならない案件がある。指導いただいた結果をもとに、DXの成果を最大限に引き出すためのセキュリティ対策の取り組みを継続的に進めていきたい。

図表 2-87 マネジメント指導事例（ベストプラクティス）コンテンツサンプル

## 2.3.　セキュリティ専門家スキル調査アンケート

### 2.3.1.　アンケート実施概要

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に登録している登録セキスペ（約 800 名）を対象としたスキルアンケート調査を実施した。アンケート項目の設計においては、本実証事業の趣旨を踏まえ、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。アンケート回収後、アンケート結果を取りまとめ、中小企業や商工会議所等の支援機関がセキュリティ専門家を効率的に探索できるよう、アクティブリストを試作した。

アンケートは IPA セキュリティプレゼンター登録の登録セキスペから合計 236 件の回答を得たが、うち 15 件が重複回答であったため、有効回答は 221 件（有効回答率 3 割）となった。

■アンケート実施期間

2024 年 12 月 25 日(水)～2025 年 2 月 3 日(月)

■公開方法、周知方法

IPA ウェブサイトでの掲示、及び IPA からの依頼メール（リマインド 1 回）

■アンケート回答方式

ウェブフォームでの設問掲示・回答（選択肢型、数値記入型、文字自由記述型の設問を組み合わせ）

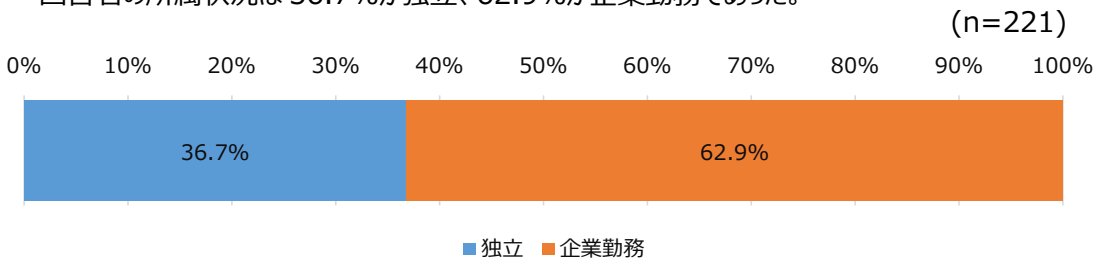
※調査項目一覧は別紙参照。

### 2.3.2.　アンケート回答者の属性

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）の属性は以下のとおり。

（１）　回答者の所属状況

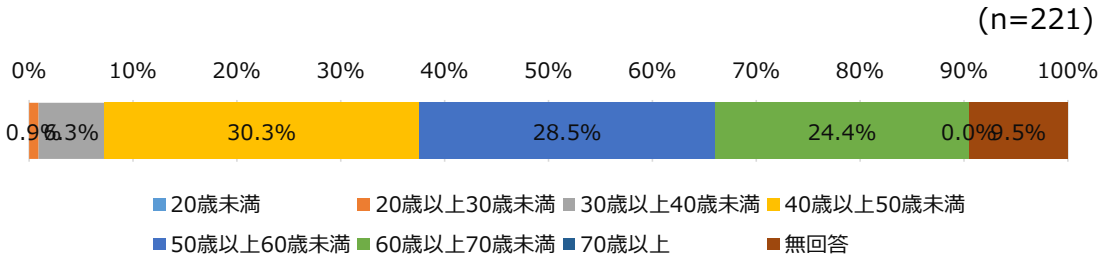
回答者の所属状況は 36.7%が独立、62.9%が企業勤務であった。




図表 2-88 アンケート回答者の所属状況

（２）　回答者の年齢分布

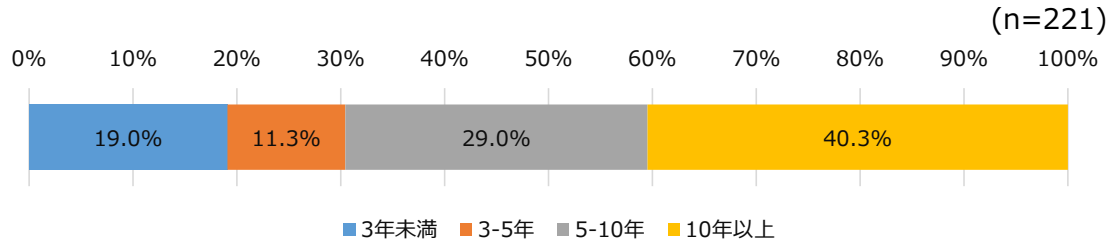
回答者の年齢分布は 50 歳以上 70 歳未満が全体の約 5 割を占める。




図表 2-89　アンケート回答者の年齢分布

（３）　セキュリティ分野での実務経験年数

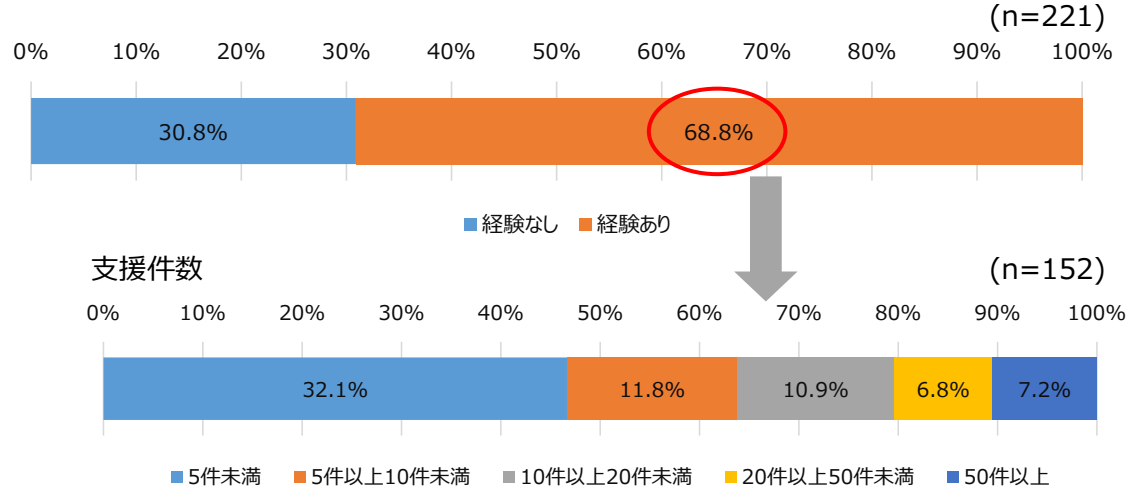
回答者のセキュリティ分野での実務経験は 5 年以上が 29.0%、10 年以上が 40.3%を占める。




図表 2-90　回答者のセキュリティ分野での実務経験年数

（４）　企業に対するセキュリティ対策支援経験

回答者の企業に対するセキュリティ対策支援経験は 68.8%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%。

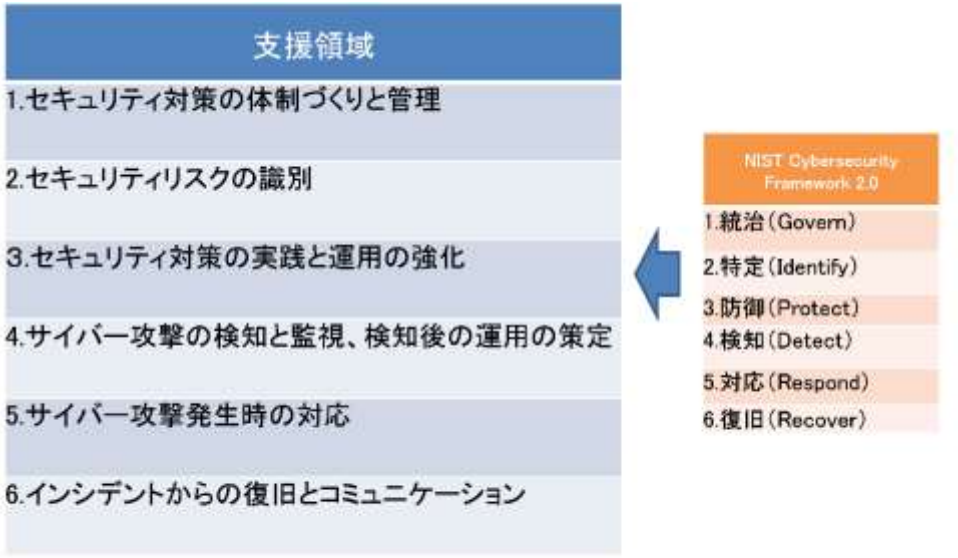



図表 2-91　回答者の企業に対するセキュリティ対策支援経験

### 2.3.3. スキル調査項目の設計

本アンケートは、中小企業へのセキュリティ対策支援が行える登録セキスペを「アクティブリスト」の形でデータ化することを目的に、各々の登録セキスペがどのような支援が可能か、また、どのようなスキルを有しているかを把握することとした。そのため、基準に基づきセキュリティ専門家の支援可能領域の可視化を行い、スキル調査項目の設計を行った。以下にその概要を示す。

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」）[6]」を参考に、6 つの支援領域を定めた。




図表 2-92 NIST CSF2.0 とアンケート調査項目との関係

[6] NIST Cybersecurity Framework 2.0：Small Business Quick-Start Guide
https://www.nist.gov/cyberframework/quick-start-guides

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。

例：S1. セキュリティ対策の体制づくりと管理

右項目の支援を行うために必要なスキル。本調査では、この各スキルについて、専門家の実行レベルを問う設問を設定し、調査を行った。

中小企業向けクイックスタートガイドに記載された「中小企業に求められる」対策項目ごとに、それを実現するために必要支援を検討した

| 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) |

図表 2-93 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）

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）

S1a-1,2,3,4,5, b-1,2, c-1,2 が実際の調査項目となる

| 支援領域 | スキル No. | 小項目（アセスメント基準） | No. | 必要とされる専門家スキル |
|---|---|---|---|---|
| 1．サイバーセキュリティ対策の方針策定と管理体制づくり | S1 | a.経営戦略の理解、経営者とのコミュニケーション | 1 | 経営戦略の理解：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 |
| | | | 2 | 経営層への説得（サイバーセキュリティ対策）：サイバー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 |
| | | | 3 | 経営層への説得（セキュリティ文化の醸成）：企業全体がセキュリティ意識をもつことの重要性について経営者に説明できる |
| | | | 4 | リスクの定量化：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 |
| | | | 5 | サイバーセキュリティ対策保険の知識：リスクに基づく加入要否の判断から、各保険商品の補償内容・適用範囲・費用対効果を考慮した最適な商品を選定するための支援を実行できる |
| | | 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構築と運用 | 1 | サイバーセキュリティ対策責任者の設定：サイバーセキュリティ対策の企画・実行における責任者を特定し、その役割・権限・責任範囲を明確にするための支援を実行できる |
| | | | 2 | サイバーセキュリティ対策の方針の策定と運用： サイバーセキュリティ対策の方針の策定から周知、運用、維持を行うための支援を実行できる |
| | | c.外部リスク評価力，コンプライアンス対応 | 1 | サプライチェーンリスクの評価：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 |
| | | | 2 | サイバーセキュリティに関する法令、規制、業界固有ガイドライン等の知識：サイバーセキュリティセキュリティに関する法律や、規程、取引要件となる業界のサイバーセキュリティガイドラインを理解し、適用のための支援を実行できる |

図表 2-94 支援スキルと指導実行レベルの考え方

また、アンケート項目には、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についても併せて調査を行った。

セキュリティ専門家スキル調査アンケート項目は、「4.3.セキュリティ専門家スキルアンケート項目一覧」を参照。

### 2.3.4. セキュリティ専門家の支援能力分析

（１） 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の概要は以下のとおり（n=221）

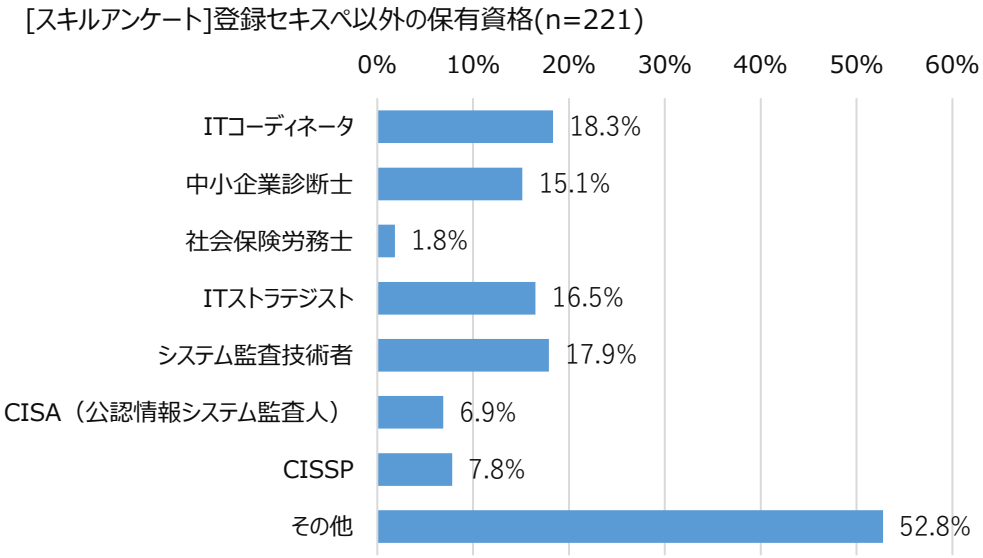
| スキル No. | スキル名（支援領域） | 実行可能な支援能力 | 単独での支援が可能 | 他の専門家の指導・サポートがあれば支援可能 | 実践的な運用には至っていない |
|---|---|---|---|---|---|
| S1 | サイバーセキュリティ対策の方針策定と管理体制づくり | 経営戦略の理解、経営者とのコミュニケーション、サイバーセキュリティ対策体制の構築、サイバーセキュリティ対策の基本方針の構築と運用、外部リスク評価力、コンプライアンス対応 | 52名 | 137名 | 32名 |
| S2 | セキュリティリスクの識別 | 情報資産の洗い出しと情報資産管理台帳の運用設計、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 |

図表 2-95 専門家スキルアンケート集計結果（保有スキル状況）

登録セキスペの「強み」スキル・「弱み」スキルの全体的な傾向としては「S2:セキュリティリスクの識別」、「S3:サイバーセキュリティ対策の実践と運用の強化」スキルが求められる支援においては、約 33%の登録セキスペが単独支援可能と回答した。一方で、「S5:セキュリティインシデント発生時の対応」、「S6:セキュリティインシデントからの復旧やコミュニケーション」スキルが求められる支援においては、約 40%の登録セキスペが“実践的な運用には至っていない”段階であると回答した。

（２）　スキルアンケート回答者が保有する他の資格

セキュリティ専門家スキル調査アンケートの回答者が、保有している登録セキスペ以外の資格は以下のとおり。

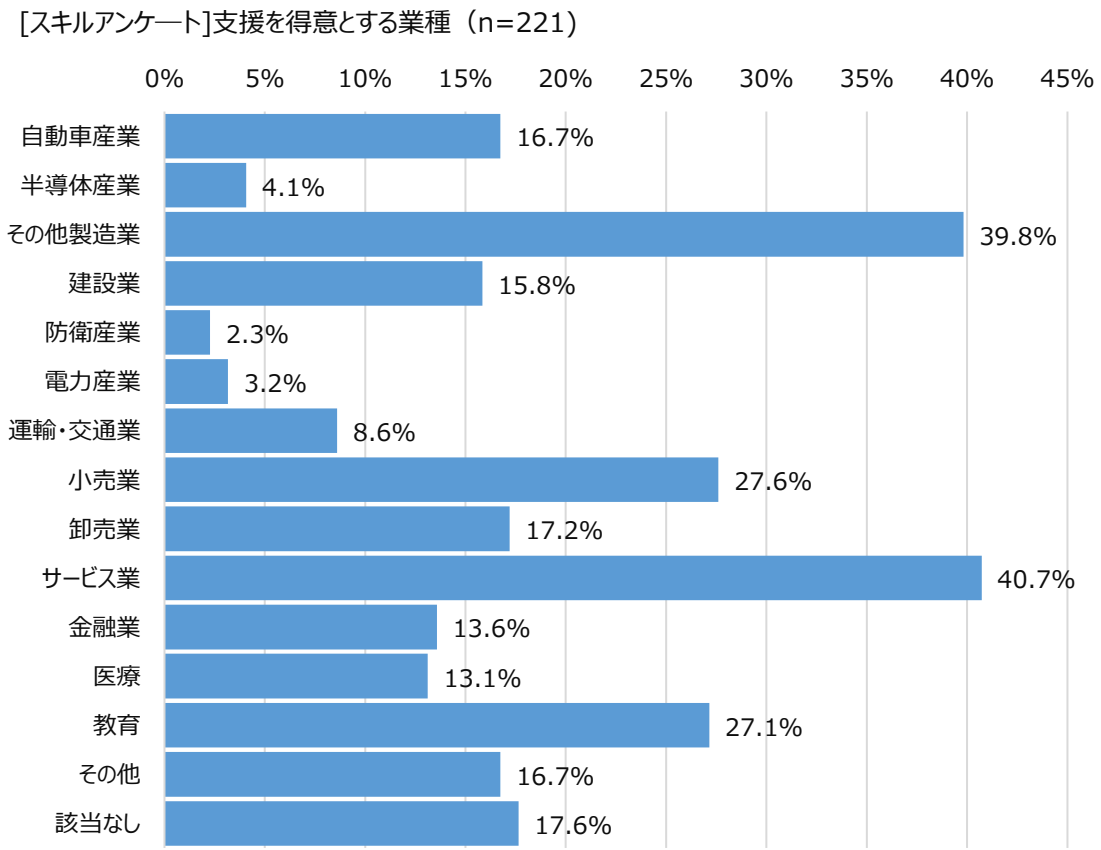



図表 2-96 回答者が保有する資格

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。また、登録セキスペ以外の保有資格を回答しなかった専門家は、61 名（約 27%）だった。

（３）　スキルアンケート回答者が得意とする業種

セキュリティ専門家スキル調査アンケートの回答者が得意とする業種については、以下のとおり。




図表 2-97　支援を得意とする業種

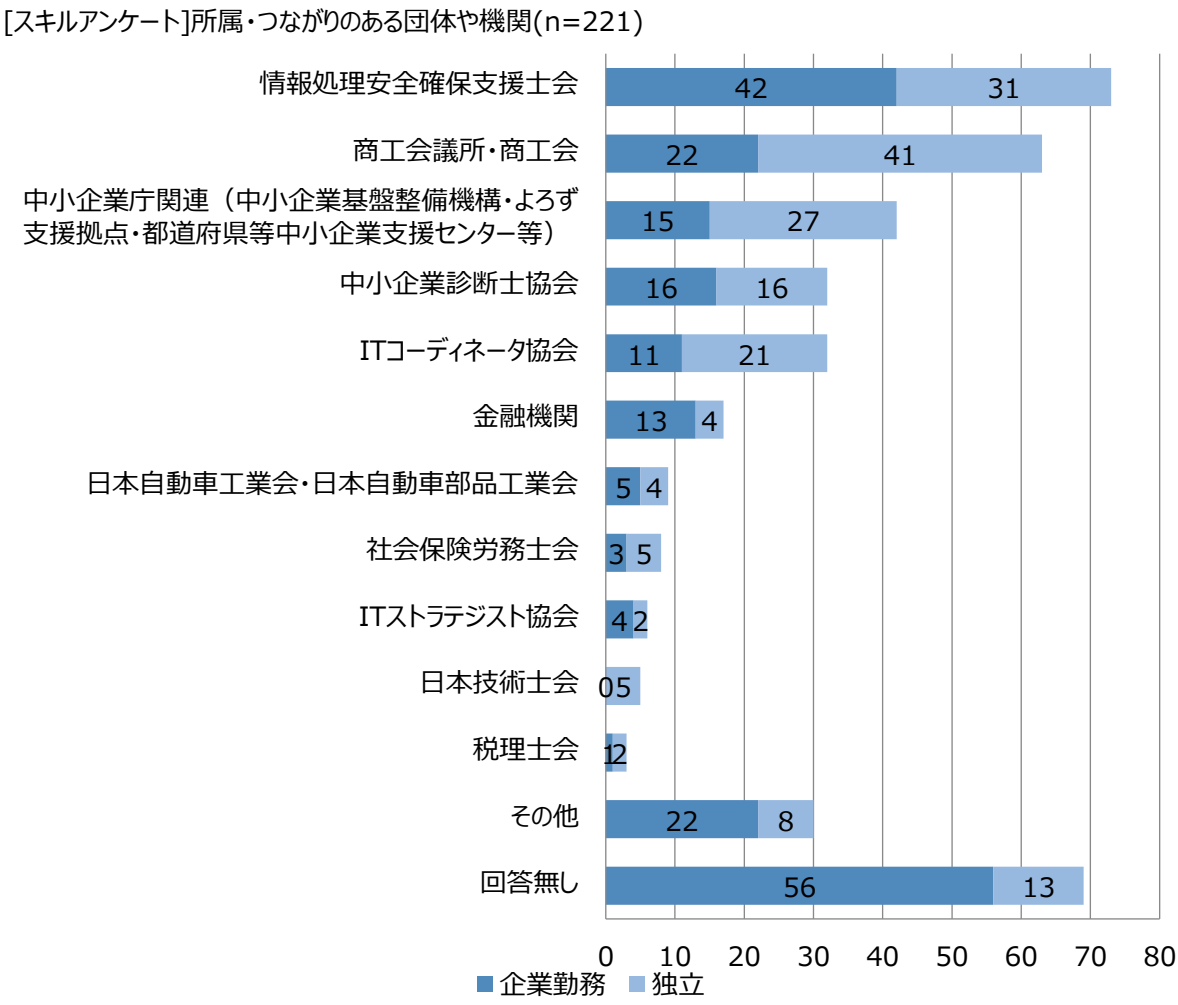
登録セキスペが支援を得意とする上位 3 業種は「サービス業」（40.7%）、「製造業（自動車産業、半導体産業を除く）」(39.8%)、次いで「小売業」（27.6%）であった。

一方で、得意とする登録セキスペが最も少ない下位 3 業種は、「防衛産業」(5 名・2.3%)、「電力産業」(7 名・3.2%)、「半導体産業」(9 名・4.1%)であった。

これら 3 産業は重要産業の 1 つでもあるため、業種に特化した登録セキスペの育成が望まれる。

（４）　スキルアンケート回答者とつながりのある団体

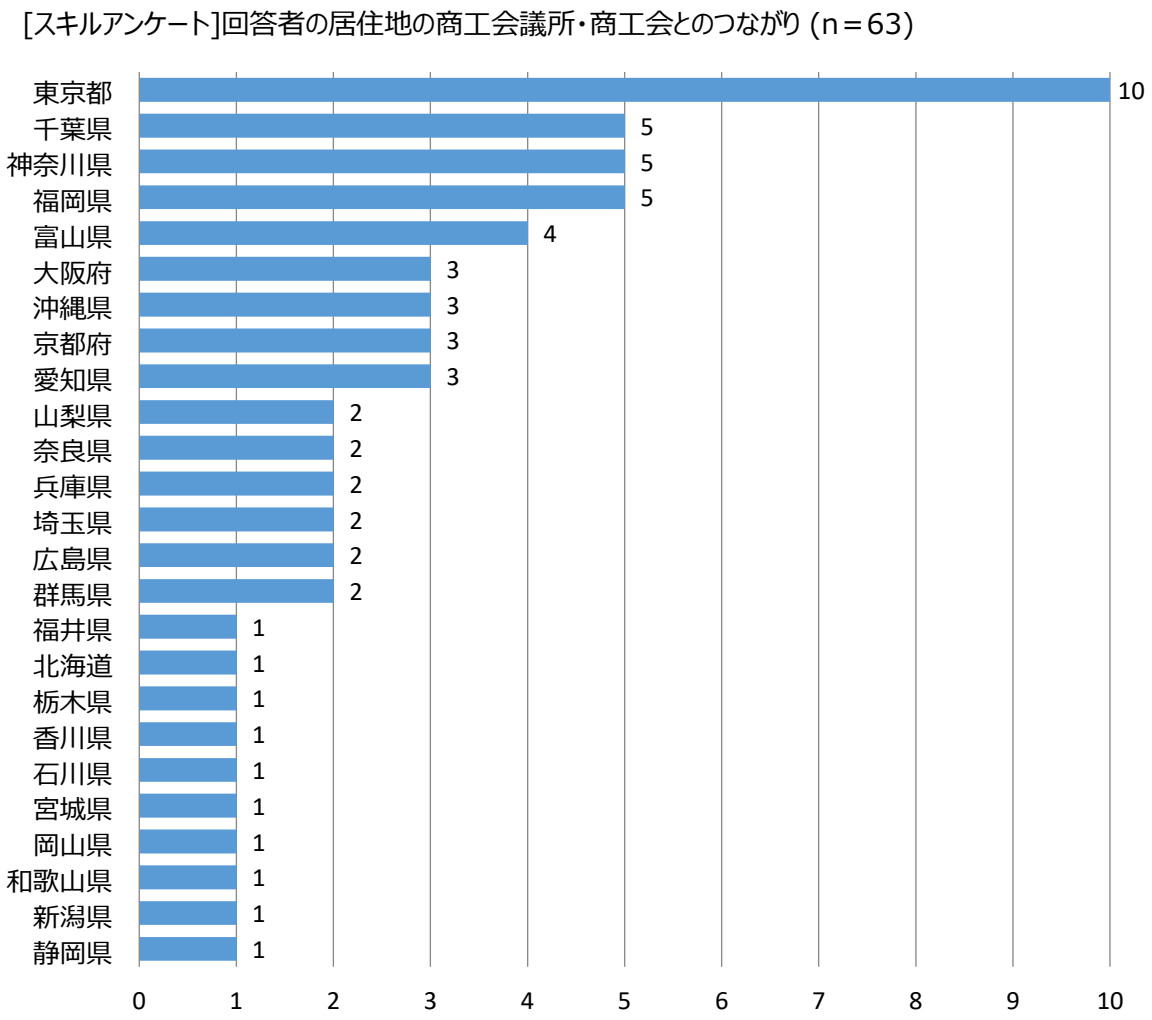
セキュリティ専門家スキル調査アンケートの回答者が所属する、あるいはつながりのあると回答した団体や機関は、以下のとおり。




図表 2-98 回答者が所属している・つながりのある団体等

69 名（32.6%）の登録セキスペが、現在所属する資格・業界団体について「該当なし」と回答。また、「商工会議所・商工会」、「中小企業庁関連（中小企業基盤整備機構・よろず支援拠点・都道府県等中小企業支援センター等）」、「IT コーディネータ協会」においては、つながりがあると回答した登録セキスペのうち、独立した登録セキスペが企業に勤務する登録セキスペの約 2 倍いた。

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 28.5%の、居住地別グラフを示す。




図表 2-99 地域の商工会議所や商工会とつながりがある登録セキスペ（居住地別）

地域の商工会議所・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、上記 25 都道府県であり、したがって残り 22 県においては商工会議所とつながりがある登録セキスペが不在である。この結果は、地域によって商工会議所と連携がある登録セキスペの数に差があることが示されている。

■登録セキスペの資格団体所属状況について

セキュリティ専門家スキル調査アンケートの回答者のうち、登録セキスペ、中小企業診断士、IT コーディネータの 3 資格において、資格保有者の資格団体へのつながり状況を確認したところ、中小企業診断士が 88%と最も高く、次いで IT コーディネータが 78%、登録セキスペが 32%という結果となった。

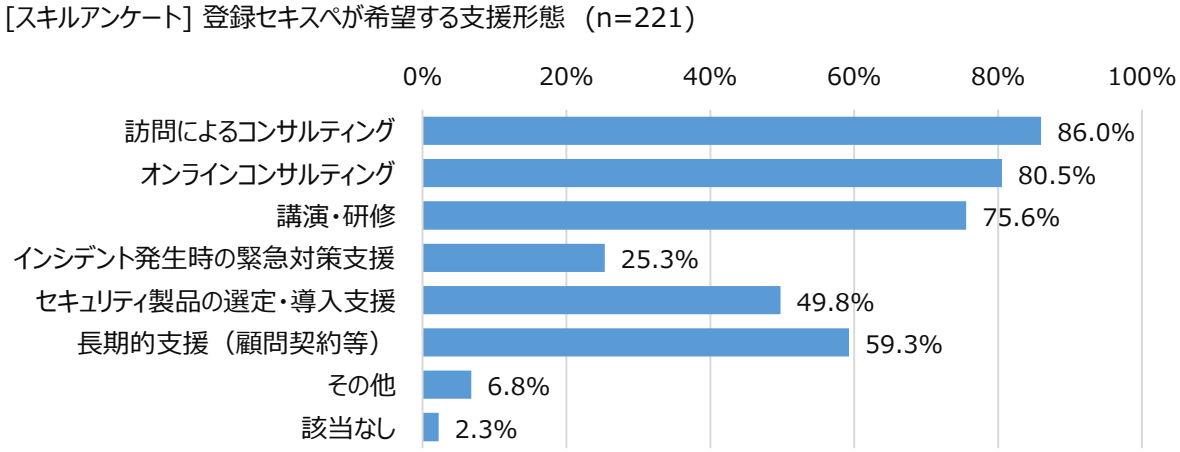
| | 資格保有者 | 資格団体所属回答数 | 所属率 |
|---|---|---|---|
| 1． 登録セキスペ | 221 | 72 | 32% |
| 2．中小企業診断士 | 34 | 30 | 88% |
| 3．IT コーディネータ | 40 | 31 | 78% |

図表 2-100 登録セキスペ、中小企業診断士、IT コーディネータ資格における団体所属状況

現在、情報処理安全確保支援士会の会員数が約 500 名（所属率 2.5%）とのことなので、本スキルアンケート回答者における所属率が高いとはいえ、他の資格と比較し半分以下の割合でしか所属していない状況が確認された。

（5） スキルアンケート回答者が希望する支援形態

セキュリティ専門家スキル調査アンケートによると、登録セキスペが希望する支援形態は以下のとおり。



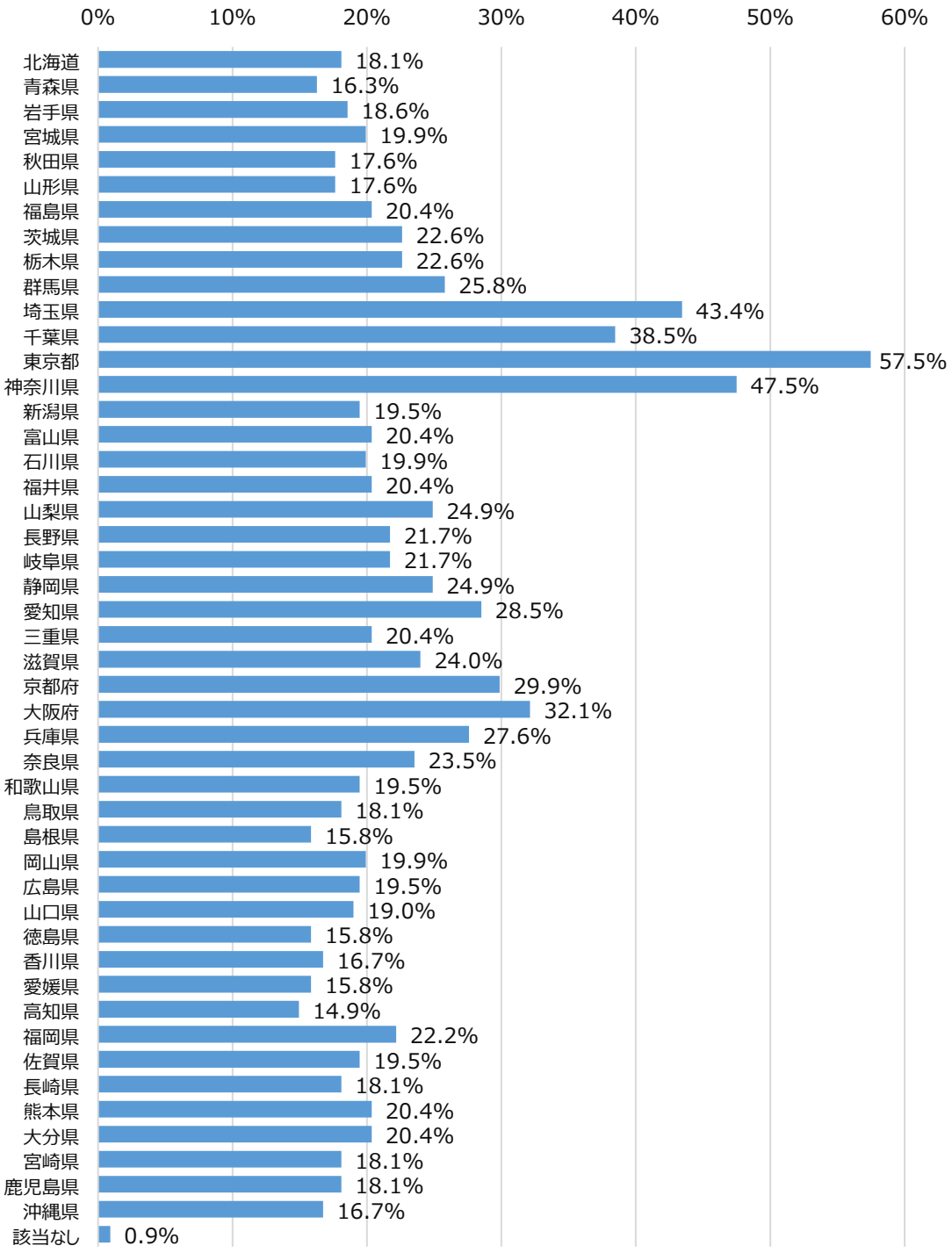

図表 2-101 登録セキスペが希望する支援形態

「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 25.3%で、アンケート調査の保有スキル結果と連動する結果となった。また、「訪問によるコンサルティング」の回答が 86.0%で最も多く、「オンラインコンサルティング」も 80.5%と、ほぼ同等の数の登録セキスペが希望すると回答した。

（６）　スキルアンケート回答者が支援可能な地域

登録セキスペが支援可能な地域についての回答は以下のとおり。全国的に支援の提供が可能であることが判明した。

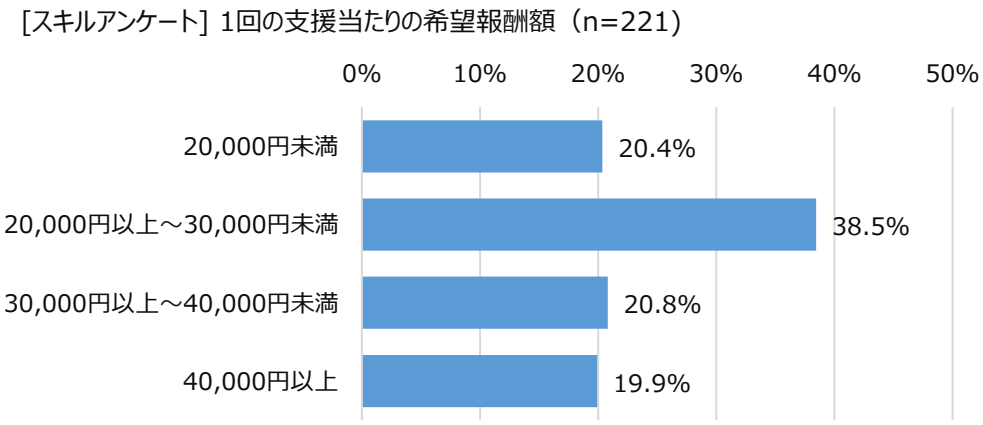
[スキルアンケート] 支援提供可能な地域(n=221)




図表 2-102　回答者が支援可能な地域

（７）　スキルアンケート回答者が希望する報酬額

登録セキスペが希望する１回あたりの支援にかかる希望報酬金額は、「2 万円～3 万円」との回答者が 38.5%と最多であった。




図表 2-103　回答者が希望する指導報酬額（1 回あたり）

### 2.3.5.　中小企業の支援可能なセキュリティ人材

アンケート回答者数は前述のとおり 221 件であったが、このうち 5 件は前項のスキル部分の回答がされていなかった。また、回答者のうち 10 件は、登録セキスペの資格は有しているものの、所属先での勤務の関係等により、中小企業に対する支援を行うことができないとの回答であった。

本アンケートは、前述のとおり、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、中小企業へのセキュリティ対策支援が行えるセキュリティ専門家を掲載したアクティブリストのベース情報とすることも目途に実施したものである。これらのスキル無回答者や支援不可の方については、アクティブリストの掲載対象としてそぐわないと判断した。

また、本アンケートを基に試作するアクティブリストは、中小企業等へのセキュリティコンサルティングが対応可能な人材リストとして公開する予定であることを説明し、回答者の本人同意を得て回答いただいたが、リストへの掲載が NG であると回答した方が 3 名いた。これらスキル無回答者、支援不可の方、リスト掲載 NG の方、計 18 名についてはアンケートの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。

## 2.4. アクティブリスト試作

### 2.4.1. アクティブリスト作成の目的

本実証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、以下の 2 点を目的にアクティブリストを試作した。

・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

### 2.4.2. アクティブリスト基本事項の検討

アクティブリストの基本事項について、以下のとおり整理を行った。

（１） リスト掲載対象者

アクティブリストの掲載対象者は、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を掲載対象とする。アクティブリストは、登録セキスペの専門知識・技能を中小企業のセキュリティ対策支援に活用することを目的とするため、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外と想定）

なお、今回の実証においては、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、セキュリティ専門家スキルアンケートを実施。その回答内容に基づき、アクティブリストを試作した。

（２） リスト掲載項目

本実証事業におけるサイバーセキュリティ相談会やセキュリティマネジメント指導の結果から、中小企業がセキュリティ専門家を選定する際に重視する情報として、以下の項目をアクティブリストの掲載項目として設定した。

①基本情報：
・氏名、登録セキスペ登録番号、写真
・所属状態（独立/企業勤務）、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実行可能な支援領域

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

（３） リスト管理・運用方式

アクティブ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情報の追加

（４） 検索・表示機能

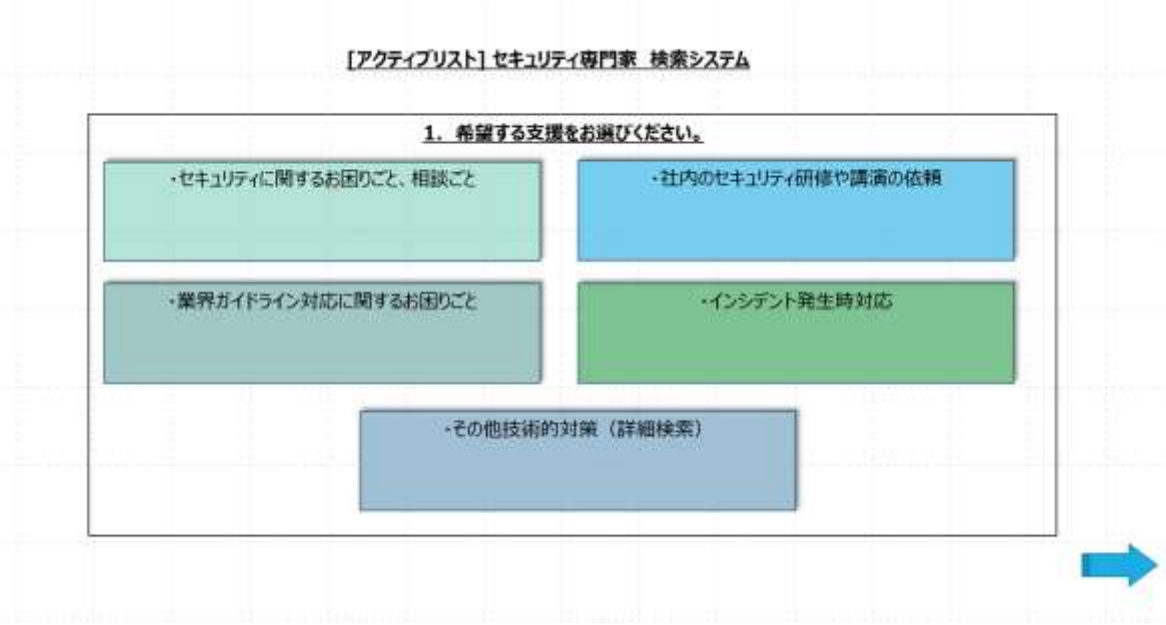
アクティブリストの掲載情報の検索及び表示方法について検討する。

・（検索例）支援内容／支援地域／業種／料金／支援期間

（５）　リスト画面遷移の検討

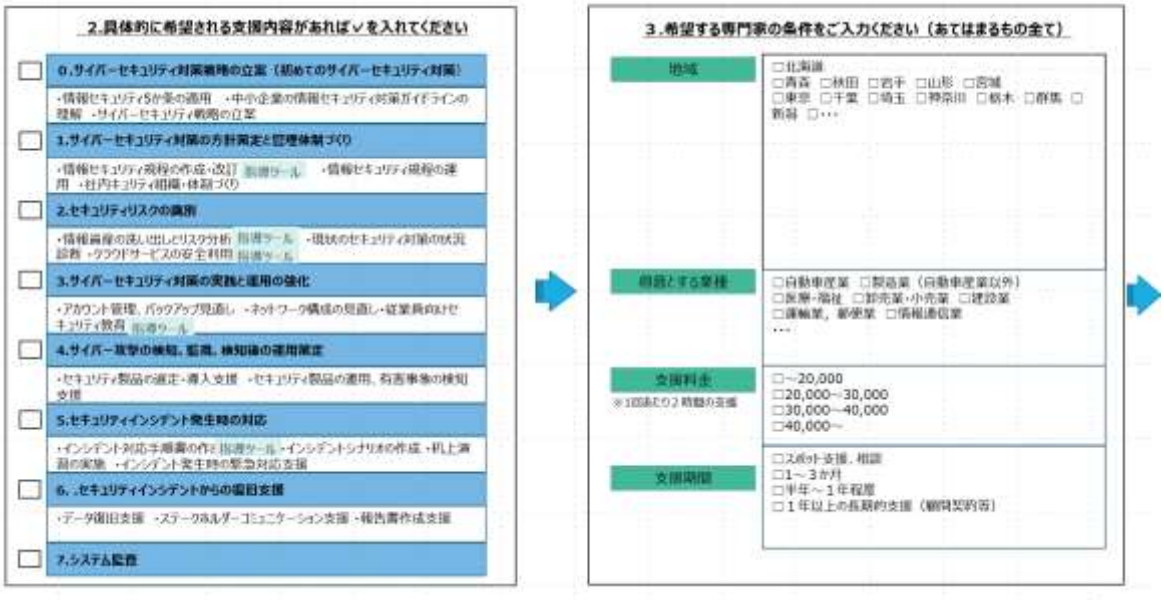
アクティブリストをシステム（WEB インターフェイスを想定）で操作する際の画面遷移の考え方について、以下のとおり検討を行った。

Step1:初めに希望する支援内容を選択する




図表 2-104　アクティブリスト検索画面（１）

Step2:支援内容の詳細や希望の条件を入力する



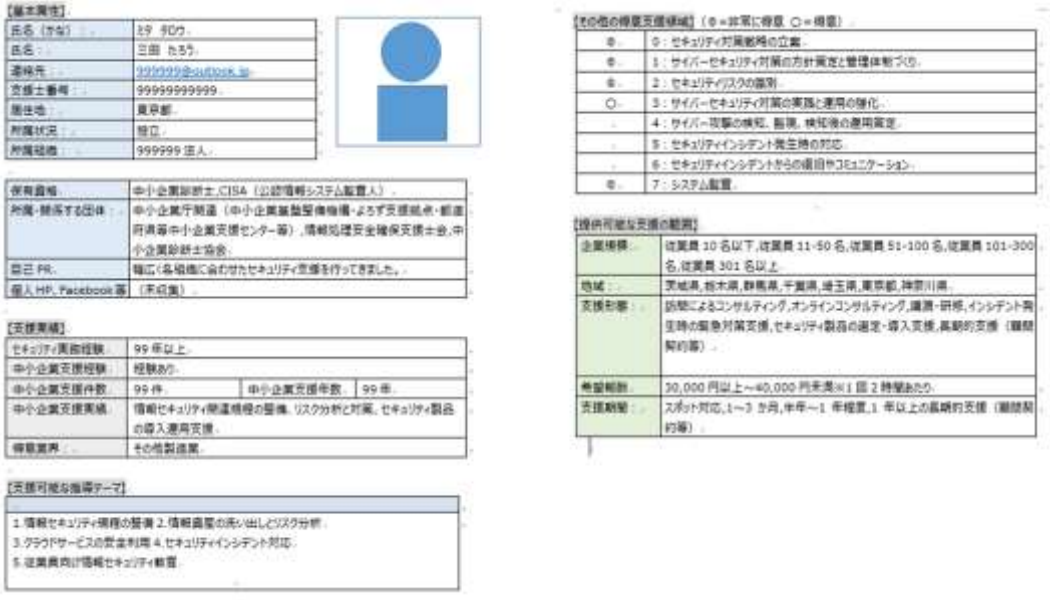

図表 2-105　アクティブリスト検索画面（２）

画面１.２.３. の指定条件をセキュリティ専門家スキルア調査シートの情報と対応付けを行えば、条件に沿ったセキュリティ専門家の絞り込みが可能。また、支援内容については、指定された支援項目について、高い自己評価点を回答したセキュリティ専門家順に一覧表示を行うことも有効と考えられる。

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


図表 2-106 アクティブリスト検索画面（３）

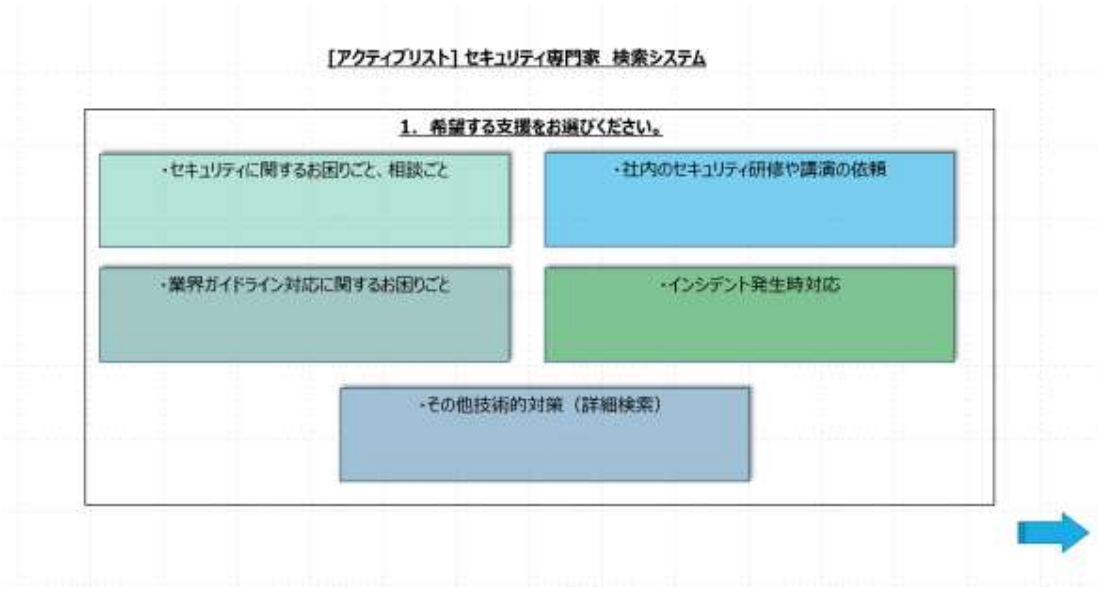
Step4:セキュリティ専門家の詳細が個票として表示される




図表 2-107 アクティブリスト検索画面（４）

（６）　専門家検索メニューの検討

本実証事業の結果を踏まえ、セキュリティ専門家を検索する際の支援メニュー（大項目５つ）について検討した。前節で提示した検索画面図を、以下に再掲載する。




図表 2-108 アクティブリスト検索画面（１）＝再掲

各メニューの設定理由と期待される効果は以下のとおりである。

（ア）　セキュリティに関する相談全般（セキュリティに関するお困りごと、相談ごと）

サイバーセキュリティ相談会の個別相談企業やマネジメント指導事例集（ベストプラクティス）掲載企業へのヒアリングを通じて、中小企業の多くは相談の入り口段階で「本当に必要な支援」を明確に把握できていないことが判明した。実際の個別相談においても、専門家による課題整理を経て、初めて必要な支援が特定されるケースが多く見られた。「企業は自社に何の支援が必要か分かっていない」、「最初は小さな困りごとの解消から入っていく」というセキュリティ専門家からの指摘を踏まえ、幅広い相談に対応できる入口として本メニューを設定した。

（イ）　社内セキュリティ研修・講演（社内のセキュリティ研修や講演の依頼）

本メニューは、セキュリティ対策への着手のしやすさを重視して独立項目とした。サイバーセキュリティ相談会の参加者アンケートや個別相談の事前ヒアリングにおいて、最も要望の多かった支援内容であり、事前準備の負担が少ない研修形式は、特にセキュリティ対策の準備段階にある企業にとって取り組みやすい特徴がある。また、セキュリティ専門家からも「支援活動の初めの一歩として研修・教育は取り組みやすい」との意見が得られており、有効な支援形態として期待できる。

（ウ）　業界ガイドライン対応（業界ガイドライン対応に関するお困りごと）

本実証事業において、サイバーセキュリティ相談会から個別相談への高い移行率を示した業種は、いずれも取引先からのセキュリティ要求事項への対応が背景にあった。外部要因による動機とはいえ、今後、さらなる要請拡大が予想される中、「相談相手がいない」という企業からの声も多くあった、本メニューによる支援ニーズがあることが想定される。

（エ）　インシデント発生時対応（インシデント発生時対応）

本メニューは、インシデント発生時の具体的な支援体制を示すことを目的としている。IT 専門人材が不在の中小企業にとって、インシデント発生後に適切な対応者を探すことは困難である。また、多くの IT ベンダーはインシデント対応の専門要員がいないケースも多い。このため、インシデント発生時に相談可能なセキュリティ専門家へのアクセス手段を提示することは、中小企業の安心感につながるものと考えられる。

（オ）　その他技術的対策（その他技術的対策（詳細検索））

本メニューは、主に IT ベンダーによる活用を想定している。具体的な技術要件が明確な利用者向けに、セキュリティ専門家の知見を提供する窓口として設定した。このルートは、セキュリティ専門家の活躍機会を広げるだけでなく、IT ベンダーが提供するサービス・製品のセキュリティ品質向上にも貢献することが期待される。

これら 5 つの支援メニューは、中小企業のセキュリティ対策の段階や状況に応じた多様なニーズに対応するとともに、専門家の活動機会の拡大も考慮したものとなっている。特に、初期段階の企業が利用しやすい項目から、具体的な要件に基づく専門的支援まで幅広いニーズへの入り口となり得る構成とすることで、セキュリティ対策の普及促進に寄与することを目指している。アクティブリストをシステムに実装する際に、検索機能要件として検討することが望まれる。

（７）　支援メニューと専門家スキルの対応

アクティブリストの運用においては、リスト利用者は支援メニューから支援内容を選択し、セキュリティ専門家を検索、セキュリティ専門家が支援可能な指導テーマや、支援実績、得意業界、支援対象地域、支援形態・料金等を参照して選定することが想定される。その際、セキュリティ専門家の保有スキルを可視化し、支援メニューに対応した保有スキル評価の高い順からリスト表示をすると、リスト利用者が使い易くなるとの想定の下、セキュリティ専門家スキル調査アンケートで登録セキスペの保有スキルの調査を行った。

そこで、収集した、登録セキスペの保有スキルの評価データ（0～3 の 4 段階評価）をリスト利用者にとって分かり易く、かつ効果的に、アクティブリスト上に表示するため、以下の変換方法を採用した。

■スキル評価の表示方法

アクティブリストでは、支援メニュー（「0.サイバーセキュリティ対策戦略の立案（初めてのサイバーセキュリティ対策）～「7.システム監査」）のスキルレベルを「◎」（二重丸）、「○」（丸）、または無表記（該当なし）の３段階で表示する。これにより、利用者は直感的に専門家のスキルレベルを把握することが可能となる。

■評価変換アルゴリズム

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ている。

【評点】
質問数が 1 項目の場合：評点 3 点
質問数が 2 項目の場合：評点 5 点
質問数が 3 項目の場合：評点 7 点
質問数が 4 項目の場合：評点 10 点
質問数が 5 項目の場合：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。

（例：調査項目 S1-a の評価）

S1-a 下には 5 つの質問項目があり、従って評点は 13 点。この場合、専門家 A だけが評点の 13 点よりも高いスコアを回答したので「スキル有り」と評価。

| 【S1-a】<br>評点：13 点 | 専門家 A | 専門家 B | 専門家 C |
|---|---|---|---|
| S1-a-1 | 3 | 2 | 1 |
| S1-a-2 | 3 | 2 | 3 |
| S1-a-3 | 3 | 3 | 3 |
| S1-a-4 | 3 | 3 | 2 |
| S1-a-5 | 3 | 2 | 3 |
| 合計 | 15 | 12 | 12 |

図表 2-109 専門家の回答内容とスキル評価の対応例

※専門家の回答は 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）のいずれかとなる。

Step 3 ：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、評価をした後、その評価状況をまとめ、最終的にスキルを有しているか、総合評価を行う。

【総合評価方法】
「◎」（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

（例：スキル S1 の総合評価）

| 【S1】 | 専門家 A | 専門家 B | 専門家 C |
|---|---|---|---|
| S1-a | 15 点:評点以上 | 12 点:評点以下 | 12 点:評点以下 |
| S1-b | 5 点:評点以上 | 5 点:評点以上 | 5 点:評点以上 |
| S1-c | 5 点:評点以上 | 5 点: 評点以上 | 3 点:評点以下 |
| 総合評価 | ◎ | ○ | |

図表 2-110 スキル総合評価の例

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「」と評価される。

Step4:アクティブリスト一覧へのスキル状況の反映

専門家のスキル状況（「◎」、「○」）は、支援領域と紐づけられ、アクティブリスト一覧に表示される。

以下の具体例を用いて、アクティブリストへの反映方法について試作する。

- 上記の例では、専門家 A は S1 スキルが「◎」、専門家 B は「○」、専門家 C は「表示なし」となった。
- 支援メニュー0.～7.と各調査スキルは対応しており、「S1」スキルは支援メニュー0,1 に対応している
- したがって、アクティブリスト上ではスキル「０」「１」の下に、「S1」のスキル状況が表示される

（例：S1 スキルのアクティブリスト上での表示のされ方）

| 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 | … | スキル状況<br>支援メニュー０.～7.毎に対応するスキルの保有状況が◎、○で表される仕様 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 専門家 A | 1.情報セキュリティ規程の作成<br>５.従業員セキュリティ教育 | … | 製造業、建設業 | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | ◎ | ◎ | | | | | | |
| 専門家 B | 1. 情報セキュリティ規程の作成 | … | 自動車産業 | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| | | | | | ○ | ○ | | | | | | |
| 専門家 C | ２.情報資産の洗い出しとリスク分析 | | | | | | | | | | | |
| | | | | | | | | | | | | |

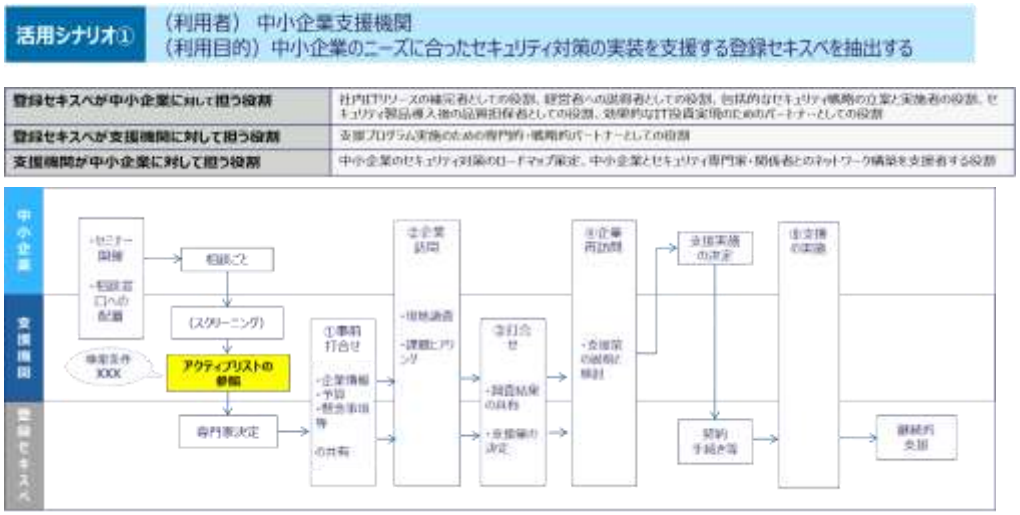
図表 2-111 各専門家のスキルをアクティブリスト表示する際の例

### 2.4.3. アクティブリスト活用の検討

（１） 活用シナリオ

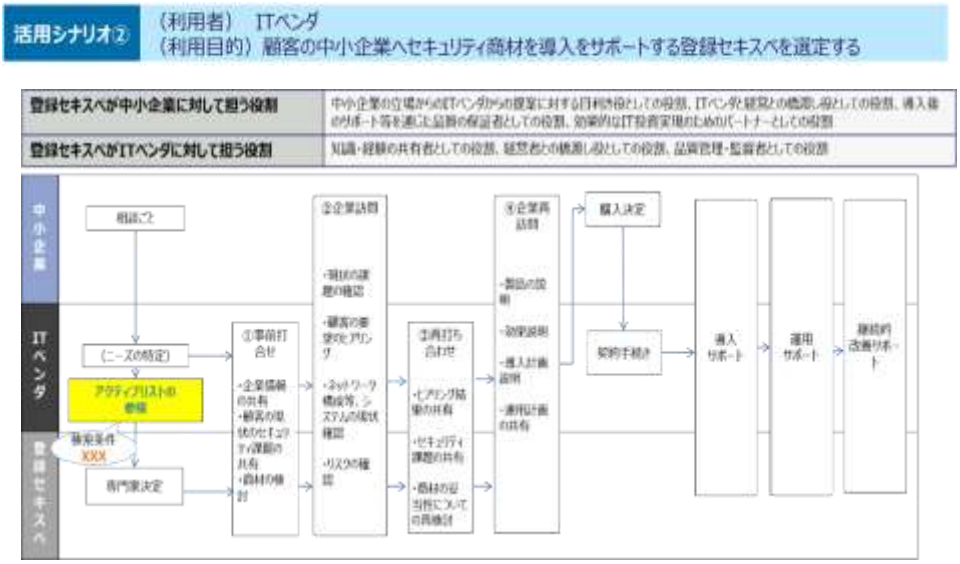
本実証事業においては、アクティブリストの主な活用者及び活用のシナリオとして、以下の 2 ケースを想定した。活用シナリオ①の商工会議所等の中小企業支援機関は、中小企業がサイバーセキュリティに関する相談ごとを持ち掛ける先として、最もポピュラーな相談先であると考えられる。また、活用シナリオ②の IT ベンダーは、中小企業にとって具体的に IT システムや各種サイバーセキュリティ対策のサポートを発注する先となる。これらの主体におけるアクティブリスト活用を考えることで、今後の登録セキスペの活用の場を広げることができると考えられる。

①中小企業支援機関




図表 2-112 アクティブリスト活用シナリオ例（中小企業支援機関）

②IT ベンダー




図表 2-113 アクティブリスト活用シナリオ例（IT ベンダー）

（２）　中小企業の視点

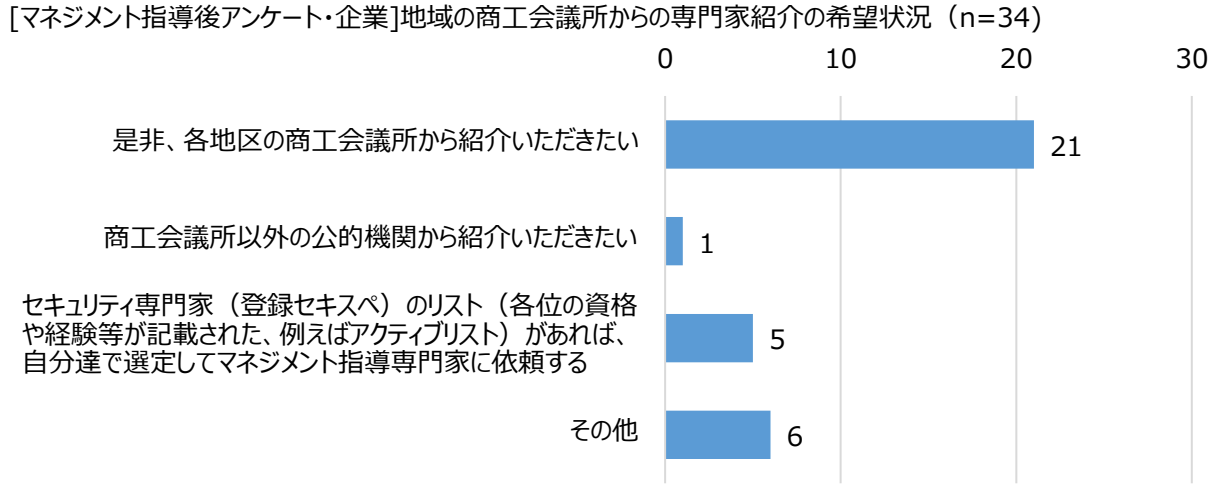
（ア）　中小企業が希望するセキュリティ専門家の紹介ルート

■　サイバーセキュリティ相談会参加者からの声

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、セキュリティ対策を支援する専門家の探し方について、「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」等、公的機関を介した専門家紹介を望む声が約半数との結果となったが、「取引のある IT ベンダーからの紹介」も約 17%の声もあった。

■　マネジメント指導実施企業からの声

マネジメント指導終了後のアンケートによると、セキュリティ専門家の紹介方法として、「公共機関からの仲介」を希望した企業が全体の約 67%を占め、「専門家リストがあれば自力で探す」と回答した企業は、約 15%にとどまった。




図表 2-114　地域の商工会議所からの専門家紹介の希望（マネジメント指導実施企業の意見）

特に商工会議所からの紹介を希望する理由として、適切な専門家の選定に対する不安が挙げられた。また、地元の商工会議所を通じた紹介では、対面での対応が可能であることや、地域の事業環境に関する知見を期待できること、地域に根差した団体である点での安心感など、地域性を重視する意見が多く寄せられた。

■　指導事例集（ベストプラクティス）対象企業からの声

マネジメント指導事例集（ベストプラクティス）の対象企業へのヒアリングでは、指導専門家紹介のルートとして、商工会議所等、地域の信頼できる機関を通じた紹介を望む声が多く聞かれた。

その理由として、地元の専門家の方がコミュニケーションを取りやすく、商工会議所経由での地元専門家の紹介が望ましいとする意見や、商工会議所による専門家の紹介は、中小企業の実情に合った支援が期待できるという点で、信頼性が高いなどの意見があった。商工会議所等の地域の支援機関に

よる適切な専門家の選定は、専門知識を持たない中小企業にとって有効との意見もあった。
また、普段から関係のある取引先企業からの専門家紹介ルートについての意見も出された。これらの意見からは、中小企業が、専門家を仲介する機関において、「信頼性」と「身近さ」を重視する意向が明確に表れている。

（イ）　中小企業のアクティブリスト活用イメージ

マネジメント指導事例集（ベストプラクティス）の対象企業をヒアリングした結果によると、中小企業では、リストを直接検索して専門家を探すのではなく、支援機関等を介した活用を想定しているケースが多いことが示唆された。具体的な活用機関としては、商工会議所の他にも、産業支援機関（大阪産業創造館等）、業界団体（税理士会等）、行政機関（労働局等）、自動車工業会などの業界団体が例として挙げられた。

これらの意見を総合すると、中小企業が日常的に関わりを持つ団体が、アクティブリストリストを活用し、中小企業にセキュリティ専門家を紹介するルートが主流との意見であった。

また、アクティブリストの品質に関する要望も多く寄せられた。具体的には、情報の更新頻度、適切な情報量（見やすさ）、信頼できる機関からの発信と掲載場所などが重要視されており、情報の信頼性や精度を担保することが、中小企業から頼られるリストとなるために必要であることが強く示唆された。

企業が直接アクティブリストを活用するケースとしては、商工会議所等への相談前の事前調査資料として使用することが想定されるとの声があった。また、注目すべき点としては、リストだけでは専門家の能力や相性を判断することは難しいという指摘も多く、初回のマッチング機会と組み合わせれば活用できるとする意見が複数挙がった。また、初回相談は無料であることが望ましいとの声も聞きかれた。

○まとめ

中小企業へのセキュリティ専門家紹介においては、「信頼性」、「身近さ」、「地域性」が重要な要素として浮かび上がった。これらの要素を兼ね備えた機関や企業からの専門家紹介を望む傾向が強いことが、ヒアリングなどから明らかとなった。普段から付き合いのある取引先企業、業界団体、ITベンダーからの専門家紹介ルートも案として挙がった。

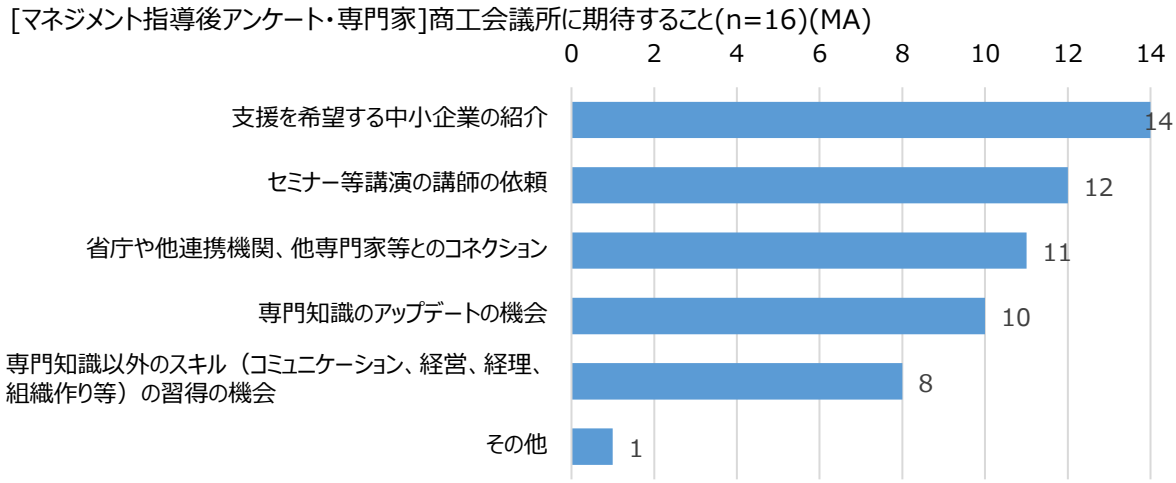
同様に、中小企業からの直接セキュリティ専門家へのアプローチのではなく、「信頼できる」機関を介した、初回相談無料の個別相談と組み合わせた活用方法が現実的であるという意見が多くみられた。

また、アクティブリストに掲載される情報の更新頻度や、信頼性を重視する傾向も強いことが明らかになった。

（３）　商工会議所ルートの検討

（ア）　セキュリティ専門家の商工会議所への期待

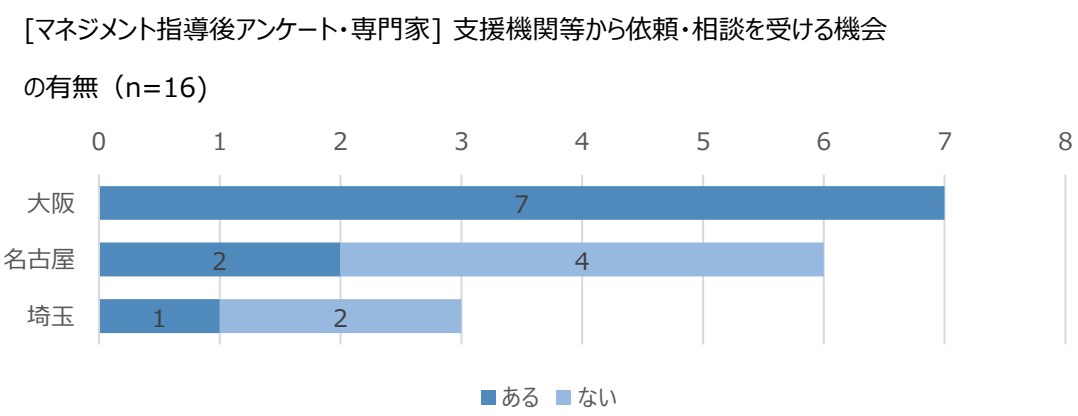
マネジメント指導終了後アンケートによると、セキュリティ専門家が商工会議所に期待する役割について、回答者の約 89%が「支援を希望する中小企業の紹介」を求めると回答した。また、支援を希望する中小企業の紹介以外にも、「セミナー等講演の依頼」、「省庁や他の連携機関、専門家とののコネクション」についても、7 割近くの専門家から期待する声があがった。




図表 2-115　商工会議所に期待すること（専門家の意見）

また、現状においてセキュリティ専門家が支援機関等から依頼や相談をうける機会については、専門家の 60%が「ある」と回答し、協力体制が存在することが示唆された。しかし、頻度については、年に数回程度とする回答が大多数であり、頻繁な連絡は行われていない様子である。

地域別では、大阪では 7 名全ての指導専門家が支援機関と連携していると回答したが、名古屋においては 2 名、埼玉においては 1 名から相談・依頼を受ける機会があると回答があった。

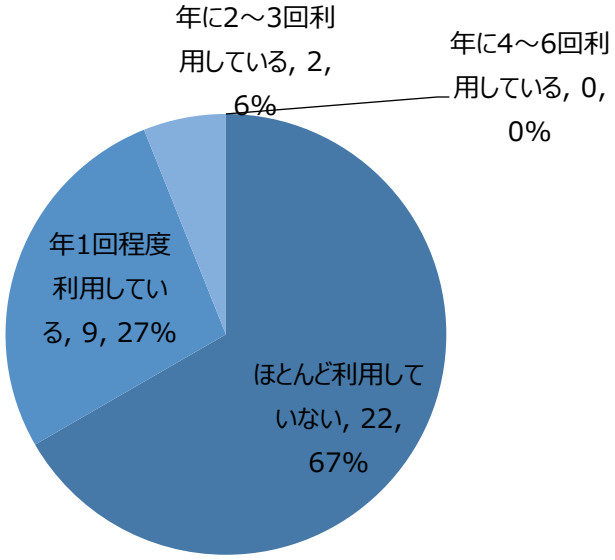



図表 2-116　専門家が支援機関等から相談を受ける機会の有無

（イ）　中小企業の商工会議所への期待

マネジメント指導終了後の指導先企業へのアンケートの回答によると、全体の約 67%の企業が商工会議所とのサイバーセキュリティに関連する関わりがほぼないと回答した。

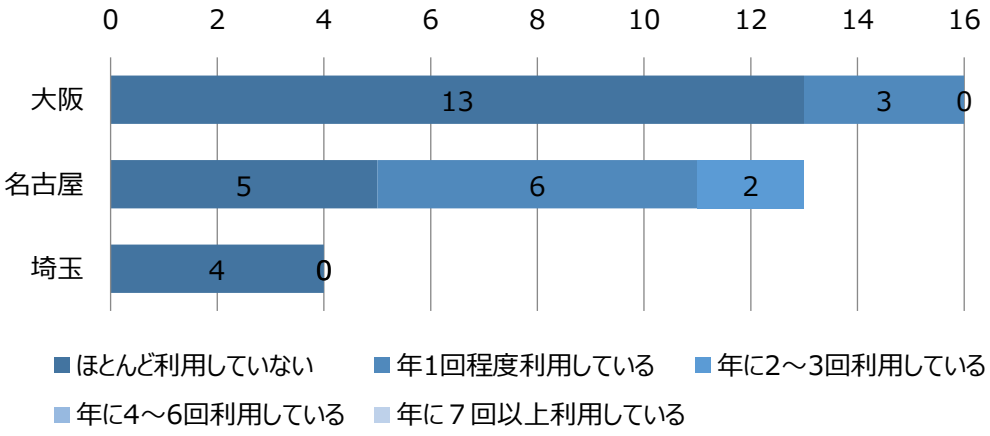
[マネジメント指導後アンケート・企業]サイバーセキュリティ相談等における、商工会議所の利用状況 (n=34)




図表 2-117 サイバーセキュリティ関連の相談等での商工会議所との関わりの有無（企業の意見）

以下に地域別のグラフを示す。

[マネジメント指導後アンケート・企業]サイバーセキュリティ相談等における商工会議所の利用状況・地域別（n=34）



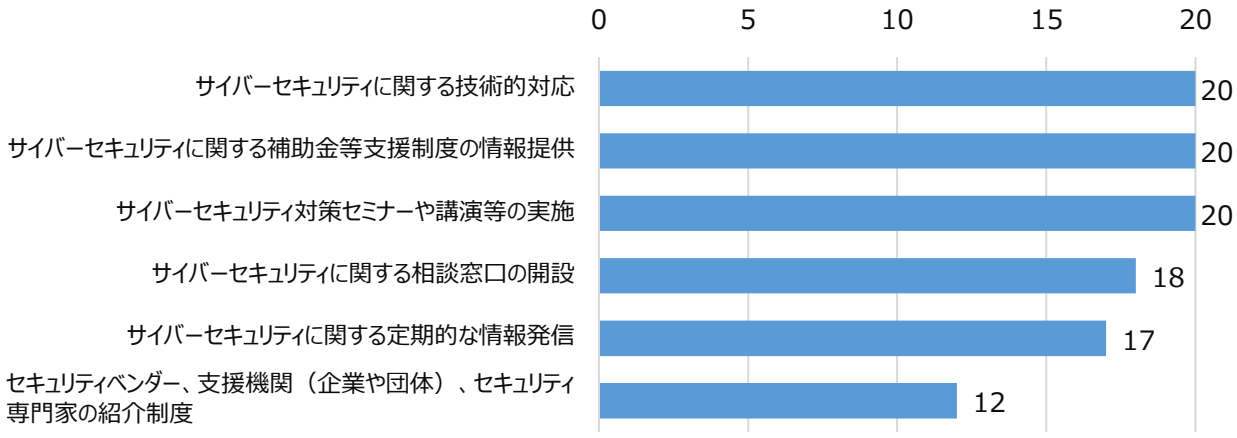

図表 2-118 サイバーセキュリティ関連の相談等での商工会議所との関わりの有無（企業の意見、地域別）

名古屋においては、商工会議所をサイバーセキュリティに関する相談事に「利用している」と回答した企業が約 62%であった。一方、大阪及び埼玉では利用率が 0%から 23%にとどまり、地域によって、サイバーセキュリティ相談における商工会議所の活用度合いに差が表れた。

商工会議所との関わりがある企業からは、「普段から商工会議所のセミナー等によく参加している。商工会議所で開催されるということで安心感もあり、場所もよくわかっているのでありがたい」、「商工会議所の情報は日ごろからウォッチしている」、「今回の相談会は、お助け隊のメルマガで知った」など、サイバーセキュリティに関する情報源として商工会議所を積極的に活用している実態が明らかとなった。また、マネジメント指導事例集（ベストプラクティス）の掲載企業へのヒアリングからも、「安心感がある」、「場所がよくわかっている」など、商工会議所に対する信頼感が確認された。このことは、商工会議所が中小企業にとって信頼できるチャネルとしての基盤を有していることを示している。商工会議所においては、既存の基盤を活かしつつ、サイバーセキュリティ分野における活動を活性化させることで、より効果的な支援体制を構築できる可能性が示唆される。

一方、マネジメント指導を受けた中小企業が商工会議所に期待することとして、約 60%の企業が「サイバーセキュリティに関する技術的対応」、「サイバーセキュリティに関する補助金等支援制度の情報提供」、「サイバーセキュリティ対策セミナーや講演等の実施」をあげ、サイバーセキュリティに関する総合的な窓口として、商工会議所が企業からが期待されていることが示唆された。

[マネジメント指導後アンケート・企業]サイバーセキュリティに関して、商工会議所に期待すること
（n=34）（MA）




図表 2-119 商工会議所に期待すること（企業の意見）

○まとめ

登録セキスペの活用において、中小企業への専門的支援は重要なポイントであり、特に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。今回のマネジメント指導に参加した指導専門家全員が「支援を希望する中小企業の紹介」を商工会議所に求めているとアンケートに回答した。

一方で、中小企業側は、現時点では約 67%の企業は商工会議所とサイバーセキュリティに関する関わりを持っていないもの、商工会議所との関わりがある企業からは、商工会議所を「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、関係構築においては大きな潜在的可能性が確認された。また、商工会議所への期待としては、サイバーセキュリティの技術的対応、補助金申請支援、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。

これらを総合すると、商工会議所は中小企業のサイバーセキュリティ対策における中核的な支援機関としての役割を担う可能性を有していると言える。経営支援等で既に構築された信頼関係の基盤を活かしつつ、セキュリティ専門家と中小企業を効果的に結びつけるマッチング機能を果たすことで、「地域における中小企業のサイバーセキュリティ支援の要」としての位置付けとなると考えられる。

（４）　IT ベンダールートの検討

IPA では令和 6 年度、本実証事業とは別事業の「地域 IT ベンダーのセキュリティ対応能力強化支援業務」を実施する中で、登録セキスペ等セキュリティ専門家との連携等について地域 IT ベンダーへのヒアリングを行った。その結果によると、システム開発案件の RFP（提案依頼書）において、登録セキスペ資格保有者をプロジェクトマネージャーとしてアサインすることを要件とするケースや、システムのセキュリティ要件を確認する際の申請時に登録セキスペの承認を必要とするケースが増加しているとのことである。このような状況に対し、IT ベンダー各社は今後の対応として、セキュリティ人材の社内育成を検討しているが、時間的・金銭的な負担が大きく、多くの企業が困難さを訴えている。

一方、マネジメント指導事例集（ベストプラクティス）の掲載企業のヒアリングからは、システム開発時におけるセキュリティ要件に関する第三者的立場からの助言について、具体的なニーズが確認できた。

○まとめ

IT ベンダーや中小企業のヒアリングからは、システム開発やシステム機器の納入前後における、セキュリティ的観点からの助言の需要があり、今後、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。

システム開発におけるセキュリティ対応は、大企業ではすでにシステム設計監査、運用監査、システム構築上の監査などにおいて、重要な確認事項となっており、中小企業におけるシステム開発案件にも広がっていくものと考えられる。

従って、今後 IT ベンダーが、セキュリティ専門家を開発案件の中で必要とするケースは多くなる予想され、社内でのセキュリティ人材育成の困難さを考えると、外部の専門家の活用が活発化する可能性がある。このような状況に対応するため、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られる仕組みとして、アクティブリストの活用が考えられる。

同時に、登録セキスペにはセキュリティ専門家として、様々な企業の状況や要望に応じて柔軟な解決策を提示できる課題解決力が、これまで以上に求められることとなると思われる。

# 3. まとめ

## 3.1. 実施結果の総括

本実証事業は、わが国中小企業の情報セキュリティ対策向上に向けて、登録セキスペ等セキュリティ人材の活用について、具体的な実証を通じ、施策の有効性や今後の課題を明らかにすることを目的に実施したものである。具体的には、地域の中小企業に対する、商工会議所等支援機関との連携によるサイバーセキュリティ相談会、セキュリティ専門家として登録セキスペを起用したセキュリティマネジメント指導を実施した。併せて、セキュリティ専門家へのスキル調査アンケートを行い、中小企業へのセキュリティ対策支援が可能なセキュリティ専門家人材リストである、登録セキスペアクティブリストを試作した。これらを通じて、今後の中小企業に対するセキュリティ専門家の活用施策を考える上での貴重な情報を収集することができた。

**中小企業の課題と支援ニーズ**

中小企業においては、セキュリティ人材の不足に加え、自社のセキュリティ課題を適切に診断する能力に限界があることが確認された。また、具体的なセキュリティ対策の実施については、取引先からの要請等の外部要因がトリガーとなっている状況も明らかとなった。

セキュリティ支援を行う専門家の選定においては、「地域性」と「信頼性」を持つ支援機関からの仲介を重視する傾向が強く見られた。特に地域の事業環境に精通した支援機関からの紹介を求める声が顕著であり、地元での対面支援を望む傾向があることが確認された。また、セキュリティ対策への投資に対しては総じて慎重な姿勢が見られ、特に初回は無料での支援を求める傾向が強い。注目すべきは、本事業においてマネジメント指導を受けた企業においても、その支援の有効性を認識しながらも、継続的な支援に対する費用支払いについては依然として慎重な姿勢を示していることである。これは支援の効果に不確さが残っていることが主な要因と考えられる。

**中小企業（自動車産業）の特徴的な課題**

サイバーセキュリティ相談会から個別相談への移行率は自動車産業で 88%（17 社中 15 社）と非常に高く、自動車工業会（自工会）のサイバーセキュリティガイドラインへの対応が相談会参加の中小企業の課題となっていることが明らかとなった。多くの中小企業がガイドラインの要求事項の具体的な実施方法について専門家からの指南を求めており、業界特化型の支援ニーズがあることが明らかになった。

**セキュリティ専門家の状況と課題**

今回スキル調査を行ったセキュリティ専門家については、企業勤務・独立を問わず中小企業支援への関心が高く、積極的な意欲を示していることが確認された。インシデント対応等の実践的経験には課題があるものの、基本的な支援スキルを保有していることも明らかとなった。一方、現状では情報処理安全確保支援士の独占業務が無く、専門性を発揮する機会や資格維持のメリットが不十分であるとの認識も示された。

本事業で実施したマネジメント指導においては、専門家、指導先企業の双方から高い満足度が得ら

れた。また、今回用意した指導ツール（5 テーマ）も、充分活用できることが確認された。しかし、指導を通じて、最新技術や技術の実際の運用についての知識不足を認識する専門家も多くいた。

**商工会議所等支援機関との連携における課題**

商工会議所等支援機関との連携については、商工会議所自体が登録セキスペの資格制度や、セキュリティ専門家を活用にした中小企業支援について、十分な理解を持っていないという現状がある。既存の経営専門相談員制度との併存や、「知っている人でなければ紹介できない」という専門家を紹介する側の意識も存在する。これらの課題解決に向けて、アクティブリストの展開においては、登録セキスペの制度や支援内容の周知や、既存制度との調和を図り、支援機関にとってもメリットのある事業スキームの構築が必要となる。

**IT ベンダーとの連携における課題**

デジタル技術の進化に伴い、セキュリティ要件が重視されるシステム開発案件が増加するなど、IT 業界においても、構造的な変化の兆しが見えており、セキュリティ専門家にとって新たな活躍の場となる機会となることが予想される。アクティブリストには、こうした時代の変化を捉え、専門家の新たな活用機会を後押しするツールとしての役割も期待される。

**アクティブリストの技術的な課題**

専門家人材プールアクティブリストの作成については、基本的には中小企業、専門家、支援機関、IT ベンダーからの合意を得られている。活用方法の課題ついては上述のとおりだが、リストそのものについての課題を聞き取ることができた。具体的には情報の正確性や鮮度の維持、さらには類似リストの散在による情報更新の煩雑さなどの課題が指摘された。

### 3.2.　今後の施策の方向性の考察

本事業の実証から得られた結論として、アクティブリスト活用による中小企業とセキュリティ専門家のビジネスベースのマッチングを促進するためには、支援機関等関係者との信頼構築を前提とした、セキュリティ専門家の活用基盤の整備が不可欠である。以下、今後の施策の方向性について考察した結果を示す。

**中小企業のセキュリティ対策支援強化にむけて**

中小企業の現状を踏まえ、情報収集段階にある企業が次のステップに進むための支援策として、本事業でも有効性が確認された、アクティブリスト掲載のセキュリティ専門家を活用したセキュリティセミナー及び相談会の開催が有効である。具体的には、地域の支援機関や業界団体等と連携し、特定の業種やニーズに特化したセミナー開催が考えられる。特に「地域性」と「信頼性」を重視する中小企業のニーズに適う、商工会議所等の地域の支援機関を活用した専門家紹介の仕組みの検討が重要である。

**業界特化型支援の強化（自動車産業等）**

自動車産業等、特定の業界ガイドライン対応に高いニーズが示された業種については、業界特化型の支援体制の構築を進める必要があると考える。特に自工会・部工会サイバーセキュリティガイドラインへの対応が課題となっている中小企業においては、相談先が無く、対策が遅れる企業が多くあるとの声が聞かれた。業界特性を理解した専門性の高い専門家とのマッチング機会の創出が求められる。具体的には、業界団体と連携したガイドライン対応に特化した相談窓口の設置や、要求事項のテーマ毎のセミナーの開催など、より具体的な支援プログラムの整備を進めるべきである。

**セキュリティ専門家の活躍機会創出とスキル向上**

セキュリティ専門家については、まずはその専門性を活かした収入機会と支援機会の創出が必要であると考える。また、より効果的な支援を行う専門家を育成するために、専門家同士の交流促進とスキルアップ機会の創出が求められる。本実証事業の調査により、インシデント対応やインシデント発生後の事業継続など、特定分野における専門家の実践的スキルの弱みが明らかとなった。また、アンケートやヒアリングを通じて、専門家から他の専門家との交流機会の創出を期待する声が多く聞かれた。セキュリティに関する技術が日々進化する中、専門家同士が知見を共有し、互いに学び合える場の重要性は明らかである。例えば、中小企業支援の初心者がベテラン専門家とのペア支援を通じて実践的なスキルを習得できる機会を設けるなど、専門家コミュニティ全体の支援力向上を図ることで、登録セキスペ資格の社会的価値の向上にもつながると考えられる。

**商工会議所等支援機関との連携強化**

商工会議所等支援機関においては、セキュリティ専門家の活用施策に理解をいただき、信頼関係を構築することが必要である。例えば全国の商工会議所に対し、登録セキスペ制度の周知や活用方法の

理解促進を図るとともに、各地の商工会議所等支援機関と専門家の交流機会、或いは業界団体等との意見交流の場を設けるなど、関係構築を進めることが重要である。また、商工会議しよの経営指導員とセキュリティ専門家の交流機会を設けることも効果的であると考えられる。

また、セキュリティ専門家の紹介が商工会議所等支援機関自身のメリット（会員サービスの充実、地域産業基盤の強化等）につながることも理解していただき、積極的な参画を促す仕組みづくりを行うことが重要である。業界団体や地域企業との連携による重層的な支援体制の構築や、地域の警察や関係機関と連携したセミナーの開催など、地域における各種事業者がお互いの目的を果たすことができる協力関係の構築が求められている。

**IT ベンダーとの新たな連携モデル構築**

システム開発におけるセキュリティ要件の重要性が高まっている現状を踏まえ、IT ベンダーとセキュリティ専門家の連携促進については今後もより進めていく必要があると考える。社内でのセキュリティ人材育成に課題を抱える IT ベンダーにとって、外部のセキュリティ専門家との連携は有効な解決策となり得る。専門家からも、IT ベンダーとの交流を通じ、最新技術のアップデート機会を求める声が挙がっていることから、今後、地域の IT ベンダーとセキュリティ専門家を交えた交流会を定期的に開催するなどを進めていくことが必要である。

以上、今後の施策の方向性の考察において、登録セキスペが中小企業へのセキュリティ支援で実施可能な業務やスキル等を見える化アクティブリストは、中小企業及び支援機関等にとって有効なツールとなり得る。今後はアクティブリストの内容充実と利用のし易さを考慮し、リスト掲載の専門家の拡充を図って行く必要がある。

以上

# 4. 参考資料

## 4.1. サイバーセキュリティ相談会参加者アンケート項目

### サイバーセキュリティ相談会　参加者アンケート

このたびは、サイバーセキュリティ相談会にご参加いただきありがとうございました。
今後の中小企業支援施策強化のため、以下の質問につきまして、ご回答をお願いいたします。

1. **相談会に関する評価**
   1. 本日の相談会に参加された一番の理由は何ですか？以下から1つお選びください。
      - ☐ 1. 講演内容に興味があった
      - ☐ 2. セキュリティ対策について以前から不安があった。
      - ☐ 3. 個別相談を受けたかった
      - ☐ 4. 支援機関などから誘われた
      - ☐ 5. 他社と情報交換がしたかった
      - ☐ 6. 具体的なセキュリティ対策を学びたかった
      - ☐ 7. その他（具体的にご記入ください:　　）
   2. 本日の相談会の満足度をお聞かせください。
      - ☐ 1. 大変満足
      - ☐ 2. やや満足
      - ☐ 3. どちらとも言えない
      - ☐ 4. やや不満
      - ☐ 5. 不満
   3. 相談会で特に参考になった点をお聞かせください。（自由記述）

      _____
   4. 今後どのような形態のセキュリティ対策セミナーに参加したいと思われますか？最大3つまでお選びください。
      - ☐ 1. 対面式の講義形式セミナー
      - ☐ 2. オンラインライブセミナー（リアルタイムで質問可能）
      - ☐ 3. オンデマンド型のビデオ講座（都合の良い時間に視聴可能）
      - ☐ 4. 少人数制のグループワークショップ
      - ☐ 5. 実機を使用した実践的なハンズオントレーニング
      - ☐ 6. 複数回にわたる連続講座
      - ☐ 7. 業界別セミナー・ワークショップ・
      - ☐ 8. . その他（具体的に:_____）
   5. 本日ご出席いただいた相談会を下記からお選びください。
      - ☐ 1. 10/15(火) サイバーセキュリティ相談会 in 埼玉

□ 2. 10/21(月) サイバーセキュリティ相談会 in 名古屋
□ 3. 10/24(木) サイバーセキュリティ相談会 in 大阪
□ 4. 11/18(月) サイバーセキュリティ相談会 in 大阪
□ 5. 11/20(水) サイバーセキュリティ相談会 in 名古屋
□ 6. 11/25(月) サイバーセキュリティ相談会 in 埼玉

**2. セキュリティ対策について**

1. セキュリティ対策に関わり、セキュリティ専門家から専門的支援を受けたことはありますか。
   □ 1. 現在支援を受けている
   □ 2. 以前支援を受けたことがある
   □ 3. 支援を利用したことがないが、検討・希望している
   □ 4. 支援を利用したことはなく、必要性も感じていない

2. 現在ご利用中、または過去にご利用されたことのあるセキュリティ対策支援内容について、あてはまるものすべてにチェックをお願いいたします。
   □ 1. セキュリティコンサルティング
   □ 2. 脆弱性診断・ペネトレーションテスト、セキュリティ監視・運用サービス等技術的支援
   □ 3. セキュリティ教育・研修支援
   □ 4. 社内の情報資産の洗い出しとリスク分析
   □ 5. セキュリティ関連規程の作成・整備
   □ 6. インシデント対応手順の整備
   □ 7. その他(具体的にご記入ください: )

3. セキュリティ専門家を探す際に、どのような方法が望ましいとお考えでしょうか。あてはまるものすべてにチェックをお願いいたします。
   □ 1. 公的機関(IPA 等)によるセキュリティ専門家リストの利用
   □ 2. 商工会議所等 中小企業支援機関による紹介・マッチング支援サービス
   □ 3. 取引のある IT ベンダーからの紹介
   □ 4. 中小企業支援機関が開催する無料相談会や説明会への参加を通じた紹介
   □ 5. 業界団体を通じた推薦制度
   □ 6. Web サイト検索
   □ 7. その他(具体的にご記入ください: )

4. セキュリティ専門家を選ぶ際に、特に重視される点はどのようなことでしょうか。以下の中から□ 3 つまでお選びください。
   □ 1. 提案内容の具体性
   □ 2. セキュリティ専門家の技術力・専門性
   □ 3. セキュリティ専門家の実績
   □ 4. 貴社の業界に対する理解度

□ 5. 支援専門家の経営に関する知識
□ 6. セキュリティ専門家の緊急時の対応力
□ 7. セキュリティ専門家のはなしやすさ
□ 8. セキュリティ専門家の身だしなみ
□ 9. セキュリティ専門家の地理的距離
□ 10. コスト

5. 今後セキュリティ専門家による支援のご利用を検討されるにあたり、どのような形態の支援をご希望されますか。以下の中から 3 つまでお選びください。
□ 1. 訪問によるコンサルティング
□ 2. オンラインでのコンサルティング
□ 3. 従業員向けセキュリティ研修の実施
□ 4. インシデント発生時の緊急対応支援
□ 5. セキュリティ製品の選定・導入支援
□ 6. その他（具体的にご記入ください: ）

6. セキュリティ専門家による支援サービスとして、どの程度の期間での支援をご希望されますか。
□ 1. 必要な時のみのスポット支援
□ 2. 1-3 ヶ月程度の短期集中支援
□ 3. 半年から 1 年程度の支援
□ 4. 2 年以上の長期的な支援
□ 5. その他（具体的にご記入ください: ）

7. 具体的にどのような内容の支援をご希望されますか。あてはまるものすべてにチェックをお願いいたします。
□ 1. 情報セキュリティ規程の整備・運用・改善に関する支援
□ 2. 社内の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に関するコンサルティング
□ 4. セキュリティインシデント対応手順の整備
□ 5. 従業員向けセキュリティ教育
□ 6. 所属業界の法令やガイドライン等のコンプライアンス対応支援
□ 7. 現時点で専門家による支援は必要ない
□ 8. その他（具体的にご記入ください: ）

8. セキュリティ対策の効果として、特に重視されている指標はどのようなものでしょうか。以下の中から 3 つまでお選びください。
□ 1. セキュリティインシデントの発生件数の軽減
□ 2. 従業員全体のセキュリティに対する意識向上
□ 3. 各種コンプライアンス要件の充足

□ 4. 業務効率の向上
□ 5. 企業価値の向上
□ 6. 取引先からの信用の向上
□ 7. その他（具体的にご記入ください：　　）

9. 現在のセキュリティ対策について、課題と感じていらっしゃることをお聞かせください。優先度の高いものから 3 つまでお選びください。
□ 1. 社内のセキュリティ専門人材が不足している
□ 2. セキュリティ対策の費用対効果が不明確である
□ 3. 経営層のセキュリティ対策への理解が十分でない
□ 4. 従業員全体のセキュリティ意識が低い
□ 5. 取引先からの要求への対応が難しい
□ 6. 技術的な対策の実装・運用が困難である
□ 7. IT ベンダーからの提案が適切かどうかについて判断できない
□ 8. 自社のシステム環境を理解している担当者が社内にいない
□ 9. その他（具体的にご記入ください：　　）

10. 以下の既存の中小企業向けセキュリティ対策施策について、知っているものをお選びください。
□ 1. SECURITY ACTION セキュリティ対策自己宣言
□ 2. サイバーセキュリティ お助け隊サービス
□ 3. 中小企業の情報セキュリティ対策ガイドライン
□ 4. 5分でできる 情報セキュリティ自社診断
□ 5. 5分でできる 情報セキュリティポイント学習
□ 6. 企業・組織向け インシデントポータル
□ 7. セキュリティプレゼンター
□ 8. どれも知らない

11. その他、セキュリティ支援サービスに関するご要望やご意見がございましたら、ご自由にご記入ください。

_____

_____

**3. 回答者属性**

1. 会社の従業員数をご記入ください。_____

2. 会社の主な業種をご記入ください。_____

3. 会社の所在地を「〇〇県〇〇市」という形でご記入ください。
（例：埼玉県さいたま市）_____

4. 所属する部署を以下から選択してください。

- □ 1. 総務部門
- □ 2. 経営企画部門
- □ 3. 情報システム部門
- □ 4. 情報セキュリティ部門
- □ 5. 事業部門
- □ 6. その他

5. 役職を以下から選択してください。（最も近いものを 1 つお選びください）

- □ 1. 経営者
- □ 2. 役員
- □ 3. 部門長・部長
- □ 4. 課長
- □ 5. 担当者

以上です。ご協力いただき、誠にありがとうございました。

### 4.2. マネジメント指導アンケート項目

#### 4.2.1. 指導先企業アンケート

## マネジメント指導　指導先企業アンケート

この度は、マネジメント指導にご参加いただき、誠にありがとうございます。
支援施策の検討のため、お手数ではございますが、本アンケートへのご記入をお願いいたします。

【0. 貴社について】
①貴社名（　　）
②貴社における情報セキュリティ担当者の設置状況を教えてください。
- □ 専任の担当者がいる
- □ 兼任の担当者がいる
- □ 担当者はいない

【1. マネジメント指導について】
Q1-1「セキュリティマネジメント指導」に参加された目的をお選びください。（複数選択可）
- □ 情報セキュリティに関する規程を整備するため
- □ 取引先や顧客から安全・安心・信頼を獲得するため
- □ 情報セキュリティに関するリスクを特定して分析を行い、対策を検討するため
- □ 情報セキュリティ管理体制やインシデントの対応手順を整備するため
- □ 社内の情報セキュリティ教育や人材育成に関するアドバイスを受けるため
- □ 社内の情報セキュリティに対する意識の向上を図るため
- □ 経営層に情報セキュリティに対する関心を持ってもらうため
- □ その他（具体的に：　　）

Q1-2　今回受けたセキュリティマネジメント指導テーマをお選びください
- □ 情報セキュリティ規程の整備
- □ 情報資産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

Q1-3　セキュリティマネジメント指導について
Q1-3-1　今回参加いただいた相談会の 2 部で実施した、事前の個別相談は必要でしたか？
- □ 必要だった
- □ 必要だったが、オンラインでの実施でもよかった
- □ 不要だった
- □ わからない

Q1-3-2 上記回答の理由を教えてください：
（　　）

Q1-3-3 1指導テーマ当たりマネジメント指導の実施回数(3回)について、どのようにお感じですか？

□ 少ない
□ 適切
□ 多い

Q1-3-4 (Q1-3-3で「少ない」,「多い」を選んだ方)何回程度が適切だと思われますか？

□ 1回 □ 2回 □ 4回 □ 5回以上

Q1-3-5 今回実施したマネジメント指導では、1回当たり指導時間を2時間と設定させていただきましたが、どのようにお感じですか？

□ 指導時間2時間は短かった
□ 指導時間2時間は適切であった
□ 指導時間2時間は長かった

Q1-3-6 (Q1-3-5で「短かった」,「長かった」を選んだ方)1回当たりの指導時間は、何時間程度が適切だと思われますか？

□ 1時間未満 □ 1時間 □ 3時間 □ 4時間 □ 5時間以上

【2. 指導プログラムについて】

Q2-1 マネジメント指導を受け、当初の目的を達成することが出来ましたか？

□ 当初の目的を十分達成することができた
□ 当初の目的をある程度達成することができた
□ 当初の目的をあまり達成することができなかった
□ 当初の目的を達成することができなかった
□ その他

Q2-2

上記回答の理由を教えてください。

(　　)

Q2-3 マネジメント指導で得られた成果(物)は何ですか(例:業務規程の整備、従業員教育の実施等)

(　　)

Q2-4 今回のマネジメント指導で果たせなかった課題がありましたら、ご記入ください

(　　)

Q2-5 今回受けたマネジメント指導の内容を、自社の各拠点(支社/支店、工場、グループ会社等)に展開されますか

□ 展開する
□ 展開しない

□ 検討中
□ わからない

Q2-6（展開される場合）その際、各地域のセキュリティ専門家のサポートが必要ですか?
□ 今回指導をしていただいたセキュリティ専門家に、継続して対応いただきたい
□ 可能であれば、その地域のセキュリティ専門家にサポートをお願いしたい
□ 自社内で展開するので不要
□ わからない

Q2-7 セキュリティマネジメント指導ツールについて

Q2-7-1 今回の指導で使用したセキュリティマネジメント指導ツールは、分かりやすく作られておりましたでしょうか？
□ 非常によく理解できた
□ よく理解できた
□ 普通
□ あまり理解できなかった
（具体的な内容: ）
□ ほとんど理解できなかった
（具体的な内容: ）

Q2-7-2 セキュリティマネジメント指導ツールの充足度はいかがだったでしょうか？
□ とても不足していた
□ やや不足していた
□ 適切であった
□ やや充足していた
□ とても充足していた

（具体的な内容: ）

【3. セキュリティ専門家について】

Q3 セキュリティ専門家について

Q3-1 今回指導を担当したセキュリティ専門家の技量はいかがでしたか。5 段階で評価してください。

| | 悪い | | | | 良い |
|---|---|---|---|---|---|
| テーマについての専門的知識 | 1 | 2 | 3 | 4 | 5 |
| 説明内容の丁寧さ・分かり易さ | 1 | 2 | 3 | 4 | 5 |
| 指導内容が要望に合っていた | 1 | 2 | 3 | 4 | 5 |
| 時間配分 | 1 | 2 | 3 | 4 | 5 |
| 人柄・態度・言葉遣い | 1 | 2 | 3 | 4 | 5 |
| 指導する意欲 | 1 | 2 | 3 | 4 | 5 |

| | | | | | |
|---|---|---|---|---|---|
| コミュニケーションの取り方 | 1 | 2 | 3 | 4 | 5 |

Q3-2 今回指導を担当したセキュリティ専門家に対するコメント（要望事項、対応等）があればお聞かせ下さい。

【4. 事務局について】

Q4 事務局の対応について

Q4-1 事務局の連絡対応はいかがでしたか。5 段階で評価してください。

| | 悪い | | | | 良い |
|---|---|---|---|---|---|
| 初回指導日の日程調整 | 1 | 2 | 3 | 4 | 5 |
| 指導テーマ・指導専門家の連絡 | 1 | 2 | 3 | 4 | 5 |
| 実施案内書類の送付 | 1 | 2 | 3 | 4 | 5 |
| その他の事務局対応 | 1 | 2 | 3 | 4 | 5 |
| 事務局に対する満足度 | 1 | 2 | 3 | 4 | 5 |

Q4-2 事務局の対応に関して、お気づきの点がございましたらお知らせください。

【5. 今後について】

Q5 今後の指導について

Q5-1 今後も機会があれば、セキュリティ専門家からの指導を受けたいと思われますか？

- ☐ 今回のように無料であれば受けたい
- ☐ 有料でも受けたい
- ☐ より継続した指導を受けるため、コンサルタント契約（顧問契約）も検討したい
- ☐ 検討中
- ☐ 分からない

Q5-2 今後指導を受ける場合、今回と同じ専門家に担当してもらいたいと思われますか？

- ☐ 同じ専門家を希望する
- ☐ 別の専門家を希望する
- ☐ どちらでもよい
- ☐ 分からない

Q5-3 今回受けたマネジメント指導テーマ以外で受けたい指導テーマがあれば教えてください。
（複数選択可）

- □ 情報セキュリティ規程の整備
- □ 情報資産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
- □ その他（具体的に: ）

Q5-4 マネジメント指導/コンサルティング指導を受ける場合の条件について

Q5-4-1 今後、貴社がセキュリティ専門家による指導を受ける場合、希望する指導期間を教えてください
（複数選択可）

- □ スポット対応
- □ 1～3 か月
- □ 3 か月～半年
- □ 半年～1 年程度
- □ 1 年以上の長期的支援（顧問契約等）

Q5-4-2 指導を希望される場合は、どのような支援形態をご希望されますか？（複数選択可）

- □ 訪問によるコンサルティング
- □ オンラインコンサルティング
- □ 講演・研修
- □ インシデント発生時の緊急対策支援
- □ セキュリティ製品の選定・導入支援
- □ 長期的支援（コンサルティング契約等）
- □ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

Q5-4-3 1 回 2 時間程度のセキュリティマネジメント指導を受ける場合、希望される 1 回あたりの指導料金をお聞かせください。

- □ 無料（セキュリティ関係機関等の施策として支援をいただきたい）
- □ 10,000 円未満
- □ 10,000 円以上～20,000 円未満
- □ 20,000 円以上～30,000 円未満
- □ 30,000 円以上～40,000 円未満
- □ 40,000 円以上

Q5-4-4 指導を希望される場合の年間予算規模を教えてください。

- □ 無し（予算化していない/予算化が難しい）
- □ 10 万円未満
- □ 10 万円以上～50 万円未満
- □ 50 万円以上～100 万円未満
- □ 100 万円以上～500 万円未満
- □ 500 万円以上

Q5-4-5 今回の指導内容（指導ツール、指導方法など）について、改善すべき点があれば教えてください。

【6. 商工会議所等の支援機関との関わりについて】

Q6 商工会議所等、支援機関との関わりについて

Q6-1 現在、「サイバーセキュリティお助け隊」サービスを利用されていますか？

- □ 利用中
- □ 検討中
- □ 利用予定なし
- □ わからない

Q6-2 サイバーセキュリティ対策に関する相談などについて、商工会議所等の支援機関を普段から利用されていますか？

- □ ほとんど利用していない
- □ 年 1 回程度利用している
- □ 年に 2～3 回利用している
- □ 年に 4～6 回利用している
- □ 年に7回以上利用している

Q6-3 「利用している」と回答された場合、利用の目的について、下記よりお選びください。（複数選択可）

- □ サイバーセキュリティに関する困りごとの相談
- □ サイバーセキュリティに関する技術的対応
- □ サイバーセキュリティに関する補助金等支援制度の情報収集
- □ セキュリティベンダー、支援機関（企業や団体）、セキュリティ専門家の紹介
- □ サイバーセキュリティ対策セミナーや講演等の受講
- □ サイバーセキュリティに関する定期的な情報収集
- □ その他（具体的に: ）

Q6-4 Q6-2 で「ほとんど利用していない」と回答された場合、その理由をお聞かせください。

（ ）

Q6-5 サイバーセキュリティ対策に関し、商工会議所等の支援機関に期待するサービスを下記よりすべてお選びください。（複数選択可）

- □ サイバーセキュリティに関する相談窓口の開設
- □ サイバーセキュリティに関する技術的対応
- □ サイバーセキュリティに関する補助金等支援制度の情報提供
- □ セキュリティベンダー、支援機関（企業や団体）、セキュリティ専門家の紹介制度

□ サイバーセキュリティ対策セミナーや講演等の実施
□ その他サイバーセキュリティに関する定期的な情報発信
□ その他（具体的に：　　）

Q6-6 支援機関に対するご要望等があれば、教えてください。

Q6-7 今回のマネジメント指導では、指導にあたるセキュリティ専門家を、各地域の商工会議所から紹介いたしました。今後も今回と同様に、地域の商工会議所からのセキュリティ専門家の紹介を希望されますか？
□ 是非、各地区の商工会議所から紹介いただきたい
□ 商工会議所以外の公的機関から紹介いただきたい
□ セキュリティ専門家（登録セキスペ）のリスト（各位の資格や経験等が記載された、例えばアクティブリスト）があれば、自分達で選定してマネジメント指導専門家に依頼する
□その他（　　）

Q6-8 Q6-7 で回答された理由をよろしければ教えてください。

【回答者】
貴社名：
部署名：
氏名：
役職：

ご協力いただきありがとうございました。

### 4.2.2. 指導専門家アンケート

（１） 指導全般に関するアンケート

## マネジメント指導　専門家向けアンケート

この度は、マネジメント指導にご参加いただき、誠にありがとうございます。
支援施策の検討のためお手数ではございますが、本アンケートへのご記入をお願いいたします。

1. **基本情報**
   1. 専門家氏名をご記入ください。

      _____

2. **施策についての評価**
   1. マネジメント指導について、参加企業のサイバーセキュリティ対策に貢献した事業であったと思いますか
      - □ 1. そう思う
      - □ 2. どちらでもない
      - □ 3. そう思わない
      - □ 4. . その他（具体的に:_____）

      上記の評価とした理由を具体的にお聞かせください。

      _____

   2. マネジメント指導について、専門家にとって今後の情報処理安全確保支援士の活躍促進につながる事業であったと思いますか。
      - □ 1. そう思う
      - □ 2. どちらでもない
      - □ 3. そう思わない
      - □ 4. . その他（具体的に:_____）

      上記の評価とした理由を具体的にお聞かせください。

      _____

   3. 設定した指導テーマ５テーマ以外に設定したらいいと思うテーマがありましたら、ご記入ください。

      _____

   4. 実施回数（3 回）は適切であったと思いますか
      - □ 1. 多い
      - □ 2. ちょうどよい

□ 3. 少ない

□ 4. その他（具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

上記の評価とした理由を具体的にお聞かせください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

5. 期間（1 月まで）は適切であったと思いますか

□ 1. 長い

□ 2. ちょうどよい

□ 3. 短い

□ 4. その他（具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

上記の評価とした理由を具体的にお聞かせください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

6. 形式（対面での実施）は適切であったと思いますか

□ 1. 適切であった

□ 2. 適切でなかった

□ 3. その他（具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

上記の評価とした理由を具体的にお聞かせください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

7. 報酬（交通費含む）は適切であったと思いますか

□ 1. 多い

□ 2. ちょうどよい

□ 3. 少ない

□ 4. その他（具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

上記の評価とした理由を具体的にお聞かせください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

8. 今回の内容であれば報酬は1回あたり、いくらが適切と思いますか

￥＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

9. 次回同様の支援事業があった場合、協力したいと思いますか

□ 1. 協力したい

□ 2. 条件による(　　)
□ 3. 協力したくない
□ 4. わからない
□ 5. その他(具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)

上記の評価とした理由を具体的にお聞かせください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

10. 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下さい(あてはまるものすべて)
□ 1. 専門家としての実績を積むことができた
□ 2. 専門家のスキルアップがはかれた
□ 3. 専門家としての知名度向上がはかれた
□ 4. 顧客開拓となるコネクションができた
□ 5. 顧客目線での視野を獲得できた
□ 6. 十分な報酬を得ることができた
□ 7. 社会貢献を行うことができた
□ 8. 特になかった
□ 9. . その他(具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)

11. ご自身が得意であるスキルについて、あてはまるのをすべて選択ください。
□ 1. 提案内容の具体性
□ 2. 技術力・専門性(具体的に:　　)
□ 3. 支援実績に基づくアドバイス
□ 4. 業界に対する理解度
□ 5. 経営に関する知識
□ 6. コミュニケーション力
□ 7. 地理的な距離の近さ
□ 8. 組織づくり・体制整備の知見
□ 9. 従業員教育・人材育成に関する知見・経験
□ 10 . その他(具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿)

12. 不足していると感じているスキルについて、あてはまるのをすべて選択ください。
□ 1. 提案内容の具体性
□ 2. 技術力・専門性(具体的に:　　)
□ 3. 支援実績に基づくアドバイス
□ 4. 業界に対する理解度
□ 5. 経営に関する知識
□ 6. コミュニケーション力

□ 7. 地理的な距離の近さ
□ 8. 組織づくり・体制整備の知見
□ 9. 従業員教育・人材育成に関する知見・経験
□ 10. その他（具体的に:＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

13. 今後、行ってみたい指導内容、指導方法等がございましたら、ご自由にご記入ください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

14. その他、マネジメント指導全般について、お気づきの点やご提案がございましたら、ご自由にご記入ください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

**3. 協力機関等との連携について**

1. サイバーセキュリティ分野で商工会議所等の協力機関から依頼や相談を受けることがありますか
□ 1. ある
□ 2. ない

1-1「ある」場合、内容や頻度についてお聞かせください

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

1-2「ない」場合、その理由をお聞かせください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

2. 協力機関に期待するものを下記よりすべて選択してください。
□ 1. 支援を希望する中小企業の紹介
□ 2. セミナー等講演の講師の依頼
□ 3. 専門知識のアップデートの機会
□ 4. 専門知識以外のスキル（コミュニケーション、経営、経理、組織作り等）の習得の機会
□ 5. 省庁や他連携機関、他専門家等とのコネクション
□ 6. その他（具体的に: ）

3. 他の専門家と意見交換や相談等の交流の機会はありますか。
□ 1. ある
□ 2. ない

1-1「ある」場合、内容や頻度についてお聞かせください

1-2「ない」場合、その理由をお聞かせください。

4. 今後の情報処理安全確保支援士の活用機会の促進や資格・制度の広報等についてご提案があれば、ご自由にご記入ください。

5. 協力機関に対するご要望等がございましたら、ご自由にご記入ください。

6. これまでの中小企業に対する支援活動において、専門家として直面した課題があれば教えてください。またそれをどのように克服したのか、ご自由にご記入ください。

以上です。ご協力いただき、誠にありがとうございました。

（２）　指導先企業ごとのアンケート

この度は、マネジメント指導にご参加いただき、誠にありがとうございます。

支援施策の検討のため、お手数ではございますが、本アンケートへのご記入をお願いいたします。

1.基本情報

1.専門家氏名をご記入ください。＿＿＿＿＿＿＿＿＿＿＿＿＿＿

2.指導先企業名をご記入ください。＿＿＿＿＿＿＿＿＿＿＿＿＿＿

3.マネジメント指導テーマをご記入ください。＿＿＿＿＿＿＿＿＿＿＿＿＿＿

4.支援成果をご記入ください。

（　　）

5. 今回のマネジメント指導で、果たせなかった課題があればご記入ください。

（　　）

2. マネジメント指導実施状況について

1.マネジメント指導はどのように実施しましたか。

□ 1.　指導ツールの内容に基づき支援を実施した

□ 2.　指導ツールの内容以外も付け加えながら支援を実施した

□ 3.　指導ツールは用いず、独自の支援内容で実施した

□ 4.．その他（具体的に：　　）

2.　（指導ツール以外の内容を加えた場合）理由について記載してください。

□ 1.　指導ツールの内容は既に対策ができていたから

□ 2.　指導ツールの内容が適切でないと判断したから

□ 3.　指導専門家として当該企業にとって必要と判断したから

□ 4.　企業からの要望があったから

上記の理由をお聞かせください。

（　　）

（指導ツール以外のツールを用いた場合）実施した支援内容を記載してください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

3. 指導ツールについて

1. 指導ツールの内容は適切でしたか。

□ 1.　適切だった

□ 2.　どちらともいえない

□ 3.　適切でなかった

□ 4.　その他（　　）

上記の理由をお聞かせください。

（　　）

2.指導ツールの内容の使いやすさはどうでしたか。

□ 1. 使いやすかった

□ 2. どちらともいえない

□ 3. 使いにくかった

□ 4. その他（　　）

上記の理由をお聞かせください。

（　　）

3.指導ツールは企業のニーズとマッチしていましたか。

□ 1. マッチしていた

□ 2. どちらともいえない

□ 3. マッチしていなかった

□ 4. その他（　　）

上記の理由をお聞かせください。

（　　）

4.指導ツールを使用した際のメリットとデメリットについて、ご記入ください。

メリット

（　　）

デメリット

（　　）

5. 他にあったらいいなと思うツールがあれば、ご記入ください。

（　　）

6. 指導ツールについて改善点やご要望等があれば、ご記入ください。

（　　）

4.指導評価について

1.今回の支援内容の総合評価をお聞かせください。

□ 1. 大変上手くいった

□ 2. 上手くいった

□ 3. どちらともいえない

□ 4. やや上手くいかなかった

□ 5. 上手くいかなかった

上記の評価とした理由を具体的にお聞かせください。

（　　）

2.マネジメント指導中ご自身のスキルを十分に発揮できましたか。

□ 1. 十分発揮できた

□ 2. 発揮できた

□ 3. どちらともいえない

□ 4. あまり発揮できなかった

□ 5. 発揮できなかった

上記の評価とした理由を具体的にお聞かせください。

（　　）

3.今回のマネジメント指導は、自身の既存知識や対応能力に比してレベルはどうでしたか。

□ 1. 十分対応できるレベルだった

□ 2. ちょうど良かった

□ 3. レベルが高く対応できなかった

（対応できなかった場合）その内容とそれを克服するための課題を具体的にお聞かせください。

（　　）

4. 今回の案件において特に重要と感じたスキルについて、あてはまるものをすべて選択してください。

□ 1. 提案内容の具体性

□ 2. 技術力・専門性（具体的に：　　）

□ 3. 支援実績に基づくアドバイス

□ 4. 業界に対する理解度

□ 5. 経営に関する知識

□ 6. コミュニケーション力

□ 7. 地理的な距離の近さ

□ 8. 組織づくり・体制整備の知見

□ 9. 従業員教育・人材育成に関する知見・経験

□ 10．その他（具体的に：　　）

5. 指導するうえで苦労したことや工夫したことについて、ご記入ください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

_____

_____

_____

以上です。ご協力いただき、誠にありがとうございました。

### 4.3. セキュリティ専門家スキルアンケート項目

セキュリティ専門家スキル調査アンケート

**【回答者情報】**

| | |
|---|---|
| 氏名　※必須 | |
| 居住地（都道府県と市区町村までで可）<br>※必須 | |
| 所属状況　※必須<br>（いずれか○で選択） | 独立　・　企業勤務 |
| 所属組織・企業名　※必須 | |
| メールアドレス　※必須 | |
| 年齢 | 歳 |

**【資格・経験について】**

問 1. 情報処理安全確保支援士登録番号　※必須

第 _____ 号

問 2. 登録年（西暦）　※必須

_____ 年

問 3. その他保有されている資格を選択してください。（複数選択可）

- □ IT コーディネータ
- □ 中小企業診断士
- □ 社会保険労務士
- □ IT ストラテジスト
- □ システム監査技術者
- □ CISA（公認情報システム監査人）
- □ CISSP
- □ その他（_____）

問 4. セキュリティ分野での実務経験年数を選択してください。　※必須

- ○ 3 年未満
- ○ 3-5 年
- ○ 5-10 年
- ○ 10 年以上

問 5-1. 企業に対するセキュリティ対策支援の経験はありますか。 ※必須

○ 経験なし
○ 経験あり

問 5-2.「経験あり」の場合、支援実績について記入してください。

| | |
|---|---|
| (1) 支援件数 ※必須 | _____ 件 |
| (2) 支援年数 ※必須 | 約 _____ 年 |
| (3) 支援内容 ※必須 | |

問 6. セキュリティ対策支援において得意とする業界を選択してください。（複数選択可） ※必須

□ 自動車産業
□ 半導体産業
□ その他製造業
□ 建設業
□ 防衛産業
□ 電力産業
□ 運輸・交通業
□ 小売業
□ 卸売業
□ サービス業
□ 金融業
□ 医療
□ 教育
□ その他（_____）
□ 該当なし

問 7. 所属している組織やつながりのある団体があれば選択してください。（複数選択可） ※必須

□ 商工会議所・商工会
□ 中小企業庁関連（中小企業基盤整備機構・よろず支援拠点・都道府県等中小企業支援センター等）
□ 金融機関
□ 日本自動車工業会・日本自動車部品工業会
□ 情報処理安全確保支援士会
□ IT コーディネータ協会
□ 中小企業診断士協会
□ 税理士会

□ 社会保険労務士会
□ 行政書士会
□ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
□ 該当なし

**【セキュリティ対策支援が可能な範囲等について】**

問 8. あなたが、中小企業に対するセキュリティ対策支援が可能な「企業規模」を選択してください。（複数選択可） ※必須

□ 従業員 10 名以下
□ 従業員 11-50 名
□ 従業員 51-100 名
□ 従業員 101-300 名
□ 従業員 301 名以上
□ 該当なし

問 9. あなたが、中小企業に対するセキュリティ対策支援が可能な「都道府県」を選択してください。（複数選択可） ※必須

□ 北海道 □ 青森県 □ 岩手県 □ 宮城県 □ 秋田県 □ 山形県 □ 福島県
□ 茨城県 □ 栃木県 □ 群馬県 □ 埼玉県 □ 千葉県 □ 東京都 □ 神奈川県
□ 新潟県 □ 富山県 □ 石川県 □ 福井県 □ 山梨県 □ 長野県 □ 岐阜県
□ 静岡県 □ 愛知県 □ 三重県 □ 滋賀県 □ 京都府 □ 大阪府 □ 兵庫県
□ 奈良県 □ 和歌山県 □ 鳥取県 □ 島根県 □ 岡山県 □ 広島県 □ 山口県
□ 徳島県 □ 香川県 □ 愛媛県 □ 高知県 □ 福岡県 □ 佐賀県 □ 長崎県
□ 熊本県 □ 大分県 □ 宮崎県 □ 鹿児島県 □ 沖縄県
□ 該当なし

問 10. あなたが、中小企業に対するセキュリティ対策支援が可能な「支援形態」を選択してください。（複数選択可） ※必須

□ 訪問によるコンサルティング
□ オンラインコンサルティング
□ 講演・研修
□ インシデント発生時の緊急対策支援
□ セキュリティ製品の選定・導入支援
□ 長期的支援（顧問契約等）
□ その他（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）
□ 該当なし

問 11. 現在、中小企業に対するセキュリティ対策支援の拡充のため、下記の 5 テーマに関する IPA の普及啓発資料を指導用ツールとして整備しています。あなたが支援が可能な「テーマ」を選択してください。（複数選択可）※必須

□ 情報セキュリティ規程の整備（※1）
□ 情報資産の洗い出しとリスク分析（※2）
□ クラウドサービスの安全利用（※3）
□ セキュリティインシデント対応（※4）
□ 従業員向け情報セキュリティ教育（※5）
□ 該当なし

（各テーマの狙い・指導先企業への効果など）
※1 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。
※2 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。
※3 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。
※4 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。
※5 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。

問 12. あなたが、中小企業に対するセキュリティ対策支援をする際に希望する「1 回（2 時間）あたりの報酬額」を選択してください。 ※必須

○ 20,000 円未満
○ 20,000 円以上～30,000 円未満
○ 30,000 円以上～40,000 円未満
○ 40,000 円以上

問 13. あなたが、中小企業に対するセキュリティ対策支援が可能な「期間」を選択してください。（複数選択可）※必須

□ スポット対応
□ 1～3 か月
□ 3 か月～半年
□ 半年～1 年程度
□ 1 年以上の長期的支援（顧問契約等）
□ 支援不可 理由（＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿）

問 14. 中小企業に対するセキュリティ対策支援における、あなたの強み（自己 PR）を 50 文字以内で記入してください。

＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

_____

_____

**【情報処理安全確保支援士の講習について】**

問 15. 過去に受講経験のある講習を選択してください。（複数選択可） ※必須

- □ オンライン講習
- □ 実践講習
- □ 特定講習

問 16. これまでに受講された講習の主な分野を選択してください。（複数選択可）

- □ セキュリティ監視・運用
- □ セキュリティ調査分析・研究開発
- □ 脆弱性診断・ペネトレーションテスト
- □ セキュリティ統括
- □ その他（_____）
- □ 該当なし（更新時期未到来のため）

問 17-1. 講習料の金額感を選択してください。※必須

| | かなり低額 | やや低額 | 妥当、適正 | やや高額 | かなり高額 | 分からない |
|---|---|---|---|---|---|---|
| オンライン講習 | ○ | ○ | ○ | ○ | ○ | ○ |
| 実践講習 | ○ | ○ | ○ | ○ | ○ | ○ |
| 特定講習 | ○ | ○ | ○ | ○ | ○ | ○ |

問 17-2. 理由について記入してください。

_____

_____

_____

【保有スキルについて】

**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**

**a. 経営戦略の理解、経営者とのコミュニケーション**

（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）

| a-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | 経営戦略の理解：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 | ○ | ○ | ○ | ○ |
| (2) | 経営層への説得（サイバーセキュリティ対策）：サイバー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 | ○ | ○ | ○ | ○ |
| (3) | 経営層への説得（セキュリティ文化の醸成）：企業全体がセキュリティ意識をもつことの重要性について経営者に説明できる | ○ | ○ | ○ | ○ |
| (4) | リスクの定量化：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 | ○ | ○ | ○ | ○ |
| (5) | サイバーセキュリティ対策保険の知識：リスクに基づく加入要否の判断から、各保険商品の補償内容・適用範囲・費用対効果を考慮した最適な商品を選定するための支援を実行できる | ○ | ○ | ○ | ○ |

a-2. 回答の根拠となる実績や経験について記入してください。

**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構築と運用**

（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）

| b-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | サイバーセキュリティ対策責任者の設定：サイバーセキュリティ対策の企画・実行における責任者を特定し、その役割・権限・責任範囲を明確にするための支援を実行できる | ○ | ○ | ○ | ○ |
| (2) | サイバーセキュリティ対策の方針の策定と運用： サイバーセキュリティ対策の方針の策定から周知、運用、維持を行うための支援を実行できる | ○ | ○ | ○ | ○ |

b-2 回答の根拠となる実績や経験について記入してください。

### c. 外部リスク評価力、コンプライアンス対応

（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）

| | | | | | |
|---|---|---|---|---|---|
| c-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
| (1) | サプライチェーンリスクの評価：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 | ○ | ○ | ○ | ○ |
| (2) | サイバーセキュリティに関する法令、規制、業界固有ガイドライン等の知識：サイバーセキュリティセキュリティに関する法律や、規程、取引要件となる業界のサイバーセキュリティガイドラインを理解し、適用のための支援を実行できる | ○ | ○ | ○ | ○ |

| |
|---|
| c-2 回答の根拠となる実績や経験について記入してください。 |

## S2. セキュリティリスクの識別

### a. 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

（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）

| | | | | | |
|---|---|---|---|---|---|
| a-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
| (1) | 情報資産の管理：情報資産管理台帳を作成し、継続的に更新・運用するプロセスを設計・実施できる | ○ | ○ | ○ | ○ |
| (2) | 情報資産リスクの評価：情報資産持つリスクを体系的に分類、評価し、優先順位付けができる | ○ | ○ | ○ | ○ |

| |
|---|
| a-2 回答の根拠となる実績や経験について記入してください。 |

### b. 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

（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）

| | | | | | |
|---|---|---|---|---|---|
| b-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
| (1) | リスク対応策の策定と文書化：リスク管理表に基づき、各リスクへの対応策を具体化し、文書化する支援を実行できる | ○ | ○ | ○ | ○ |
| (2) | サイバーセキュリティ対策の評価：既存のサイバーセキュリティ対策の効果について評価し、改善点を指摘できる | ○ | ○ | ○ | ○ |

| b-2 回答の根拠となる実績や経験について記入してください。 |
|---|

### c. 社内外における、サイバーセキュリティ対策の推進

（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）

| c-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | サイバーセキュリティ対策の社内外への発信（コミュニケーション）：サイバーセキュリティ対策やポリシーの内容、実施計画や運用について企業内外に発信する支援を実行できる | ○ | ○ | ○ | ○ |
| (2) | セキュリティ文化の醸成 ：企業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・実施ができる | ○ | ○ | ○ | ○ |

| c-2 回答の根拠となる実績や経験について記入してください。 |
|---|

## S3. サイバーセキュリティ対策の実践と運用の強化

### a. アカウント管理、アクセス管理

（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）

| a-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | アカウント管理・アクセス管理：適切なアカウント・アクセス管理ポリシーを設計し、アカウントの分類や権限管理を効果的に実施できる | ○ | ○ | ○ | ○ |

| a-2 回答の根拠となる実績や経験について記入してください。 |
|---|

**b. 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**

（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）

| | | | | | |
|---|---|---|---|---|---|
| b-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
| (1) | システム更新：ソフトウェア、OS の更新管理に関する支援を実施できる | ○ | ○ | ○ | ○ |
| (2) | データバックアップ：適切な方式や頻度でのデータバックアップ実施と管理の支援を実施できる | ○ | ○ | ○ | ○ |
| (3) | 暗号化：暗号化を実施すべき情報機器を特定し、データ保護対策実施のための支援を実施できる | ○ | ○ | ○ | ○ |

| |
|---|
| b-2 回答の根拠となる実績や経験について記入してください。 |

**c. 社内セキュリティ教育の策定と運用**

（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）

| | | | | | |
|---|---|---|---|---|---|
| c-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
| (1) | 社内セキュリティ教育の策定：既存の社内セキュリティ教育を評価し、効果的な教育の策定と運用のための支援を実施できる | ○ | ○ | ○ | ○ |

| |
|---|
| c-2 回答の根拠となる実績や経験について記入してください。 |

**S4. サイバー攻撃の検知と監視、検知後の運用策定**

**a. セキュリティインシデント対処教育の策定と実施**

（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）

| | | | | | |
|---|---|---|---|---|---|
| a-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
| (1) | セキュリティインシデント対処の教育：セキュリティインシデントの一般的な兆候を識別する方法について、効果的な社員教育を実施できる | ○ | ○ | ○ | ○ |

| |
|---|
| a-2 回答の根拠となる実績や経験について記入してください。 |

**b. 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**

（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）

| b-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | ウイルス対策ソフトの運用：　適切なウイルス対策ソフトの選定、導入、運用設計を行い、効果的に実行する支援を実行できる | ○ | ○ | ○ | ○ |
| (2) | システム・ネットワークの監視：　システムおよびネットワークの監視に関する知識を持ち、必要な運用体制を設計・実装できる | ○ | ○ | ○ | ○ |
| (3) | 外部監視サービスの導入：　中小企業向けの外部監視サービスについて熟知し、適切なサービスの選定と導入のための支援を実行できる | ○ | ○ | ○ | ○ |

| b-2 回答の根拠となる実績や経験について記入してください。 |
|---|

**c. インシデント初動の運用設計と教育実施能力**

（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）

| c-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | 初動対応設計：セキュリティ事象の検知時の初動について、適切な運用を設計できる | ○ | ○ | ○ | ○ |

| c-2 回答の根拠となる実績や経験について記入してください。 |
|---|

## S5. サイバー攻撃発生時の対応

**a. 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）**

（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）

| a-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | セキュリティインシデント対応計画の策定：情報セキュリティインシデント対応計画の策定と管理・運用体制を構築する支援を実行できる | ○ | ○ | ○ | ○ |
| (2) | セキュリティインシデント分析：発生した事象に基づき、セキュリティインシデントの原因、被害とその影響範囲を正確に分析できる | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| (3) | 封じ込め戦略立案：発生した事象に基づき、適切なセキュリティインシデント封じ込め対策を設計できる | ○ | ○ | ○ | ○ |
| (4) | セキュリティインシデントの報告と公表：セキュリティインシデント発生時における関係者への報告・公表プロセスを適切に実施および管理する支援を実行できる | ○ | ○ | ○ | ○ |

| |
|---|
| a-2. 回答の根拠となる実績や経験について記入してください。 |

## 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

### a. セキュリティインシデント復旧支援

（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）

| a-1 | 次の項目の習熟度を選択してください。 | 0 | 1 | 2 | 3 |
|---|---|---|---|---|---|
| (1) | インシデント復旧支援：セキュリティインシデント発生時のビジネス復旧に関する責任の所在を正しく理解するための支援を実行できる | ○ | ○ | ○ | ○ |
| (2) | インシデント事後報告書作成：インシデントの詳細、時系列、影響範囲から、実施された対応・教訓までを正確かつ簡潔に文書化する支援を実行できる | ○ | ○ | ○ | ○ |
| (3) | データ復旧：セキュリティインシデントからの復旧時に、正しいバックアップデータを選定し、効果的な復旧を行うための支援を行える | ○ | ○ | ○ | ○ |
| (4) | 復旧行動の優先順位付け：セキュリティインシデント復旧対応について、適切に優先順位付けを行える | ○ | ○ | ○ | ○ |
| (5) | ステークホルダーとのコミュニケーション：インシデント対応中の関係者、顧客等利害関係者への適切な頻度と内容での情報共有を管理できる | | | | |

| |
|---|
| a-2. 回答の根拠となる実績や経験について記入してください。 |