

# セキュリティマネジメント指導ツール 活用セミナー

企業内セキスペが実践する中立的セキュリティ支援  
— 経営 × IT × 現場をつなぐ実践モデル —

2025.12.5

令和6年度事業  
セキュリティマネジメント指導担当  
高橋 幸司

# 自己紹介



## 高橋 幸司

株式会社 東洋 常務執行役員  
NPO)ITコーディネータ協会 理事  
NPO)ITコーディネータ京都 副理事長  
一社)京都府中小企業診断士協会 会員

### 自己紹介

30年近くIT業界での経験を積んできました。ネットワークエンジニアとしてキャリアをスタートさせ、多くの企業に対してネットワークやサーバーの設計・構築を行いました。その後、セキュリティエンジニアとしてセキュリティ対策を様々な事業者へ行ってきました。また、クラウドエンジニアとしてAWSの設計・構築を担当し、スクラッチ開発からDevOps環境の構築、SaaSのインテグレーション、FileMakerやWEBアプリケーションベースの各種システムのPM・SE・PGとして従事して参りました。

### 直近実績

京都府立高校 情報セキュリティ特別授業講師(2018年～)  
京都スマートシティエキスポ セキュリティセミナーパネリスト  
(公社)東山納税協会 DXセミナー講師 等々

### 資格

経産省登録 中小企業診断士  
経産省登録 情報処理安全確保支援士  
経産省認定 ITストラテジスト  
厚生労働省認定 ものづくりマイスター(DX部門)  
デジタル庁認定 デジタル推進委員  
米国PMI認定 Project Management Professional  
JASA 公認情報セキュリティ監査人  
経産省推奨資格 ITコーディネータ  
AWS ソリューションアーキテクト  
AWSデベロッパーアソシエイト  
経産省 技術情報管理認証制度(TICS)審査員

# 本日の目的

---

1. 本事業への参加の動機
2. セキュリティマネジメント指導ツールの特徴
3. 指導事例①：テーマ④セキュリティインシデント対応（会計事務所）
4. 指導事例②：テーマ⑤従業員向けセキュリティ教育（社会福祉法人）
5. 指導事例③：テーマ②情報資産の洗い出しとリスク分析
6. 指導を通して感じた事
7. 企業内人材が公的活動に参加する価値
8. まとめ

01

## 本事業への参加の動機

# 今回のきっかけ

---

ITベンダーに勤務しており自身のスキルアップとしてセキスぺ取得（2014）

その後、情報処理安全確保支援士の制度が開始され登録（2017）

※情報処理安全確保支援士の研修費用等は会社で費用負担頂いている

本業で大阪商工会議所のサイバーセキュリティお助け隊サービスを取り扱い

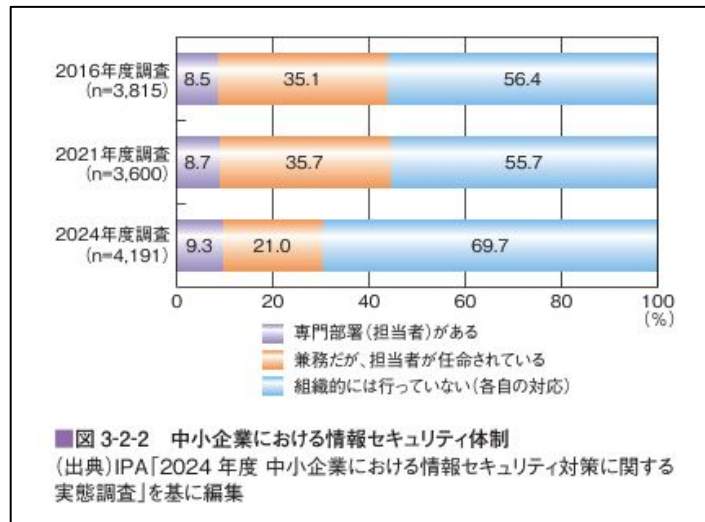
大阪商工会議所から本事業への参加依頼

今回は実証事業の意義から副業として参加

# 私が感じている本事業への意義

- 中小企業のセキュリティ人材は **圧倒的に不足**
- 企業内人材が“外に出る”ことで **人手不足対応**
- 副業スタンスではなく **社会貢献活動**

登録セキスぺの活躍の場と  
ユーザー企業での活用促進が  
望まれている



出典：IPA「情報セキュリティ白書2025」

# 企業内セキスぺの強み（私の場合）

---

- 実務（導入・運用・教育）のリアルを理解
  - 机上のリスクでなく**本当のトラブル**を知っている
- 技術と経営の両方を **橋渡し** できる
  - 社内での上長や経営層の説明・稟議の経験がある
  - ルールや規定作りに関わっている
- 現場の課題を“**翻訳**”し経営層に伝えられる
  - 専門用語を噛み砕いて説明できる
- 診断士・ITC等の資格と親和性が高い
  - 経営戦略策定やDXとの関わりに**セキュリティ観点**を加えられる

# 副業として留意したこと

---

- 中立性（ベンダーフリー）の確保
- 特定製品の推奨を行わない
- オススメを聞かれた場合はカテゴリや複数の選択を提示
- “プロダクトではなく **目的（守る対象）**”を軸に説明
- シラバスに沿って公平性を担保
- データの扱いには注意

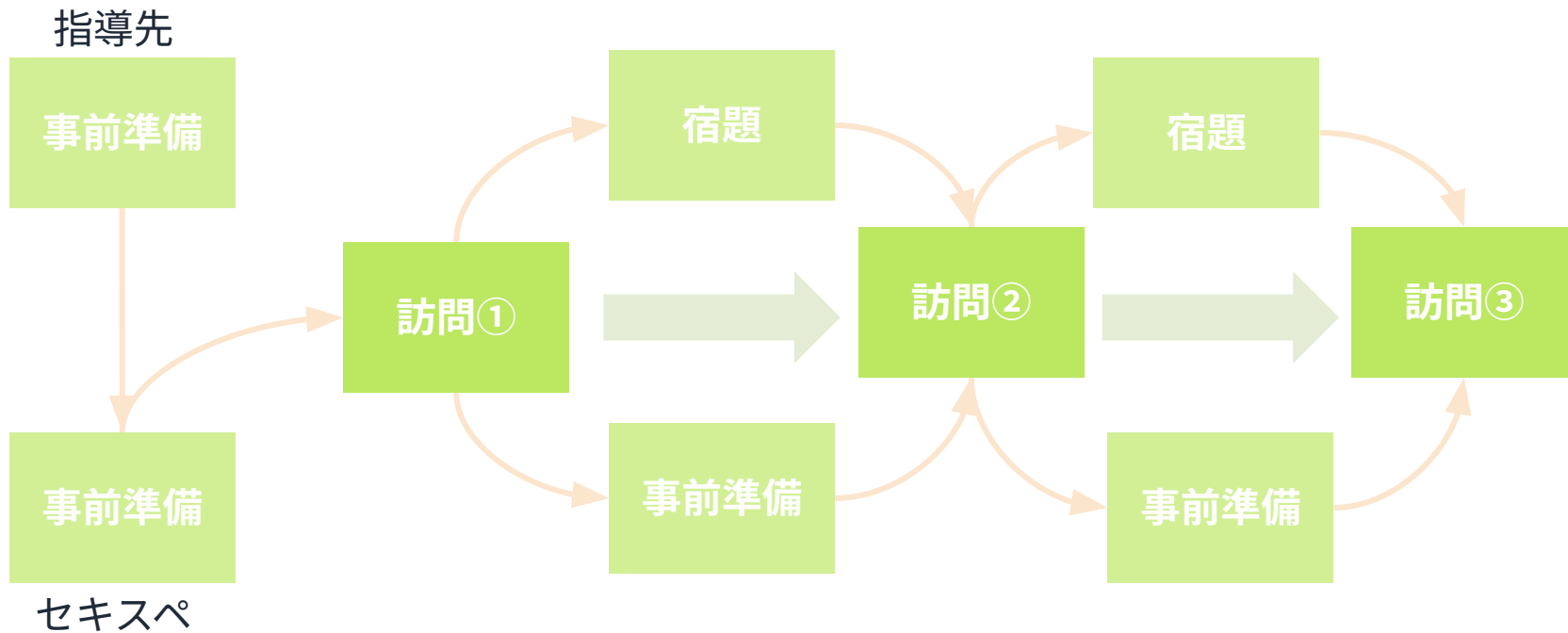


02

# セキュリティマネジメント指導ツールの特徴

# 3回訪問モデル

シラバスに沿って3回訪問（2.0ヶ月程度）  
訪問時間は2時間～3時間



# 指導ツールの良い点

---

- シラバスがとても整理されている
  - 次にやることがハッキリしている
- 計画の大枠を考えなくて良い
  - テーマ毎の計画が整備されている
- ツールを介して企業側とのゴールイメージが共有できる
  - 企業側と専門家の認識ギャップを埋められる
  - ヒアリングから指導の流れで企業側の気づきを促せる
- 成果物が企業の“資産”として残る
- ベンダーフリーで誰でも実施しやすい

# 課題

---

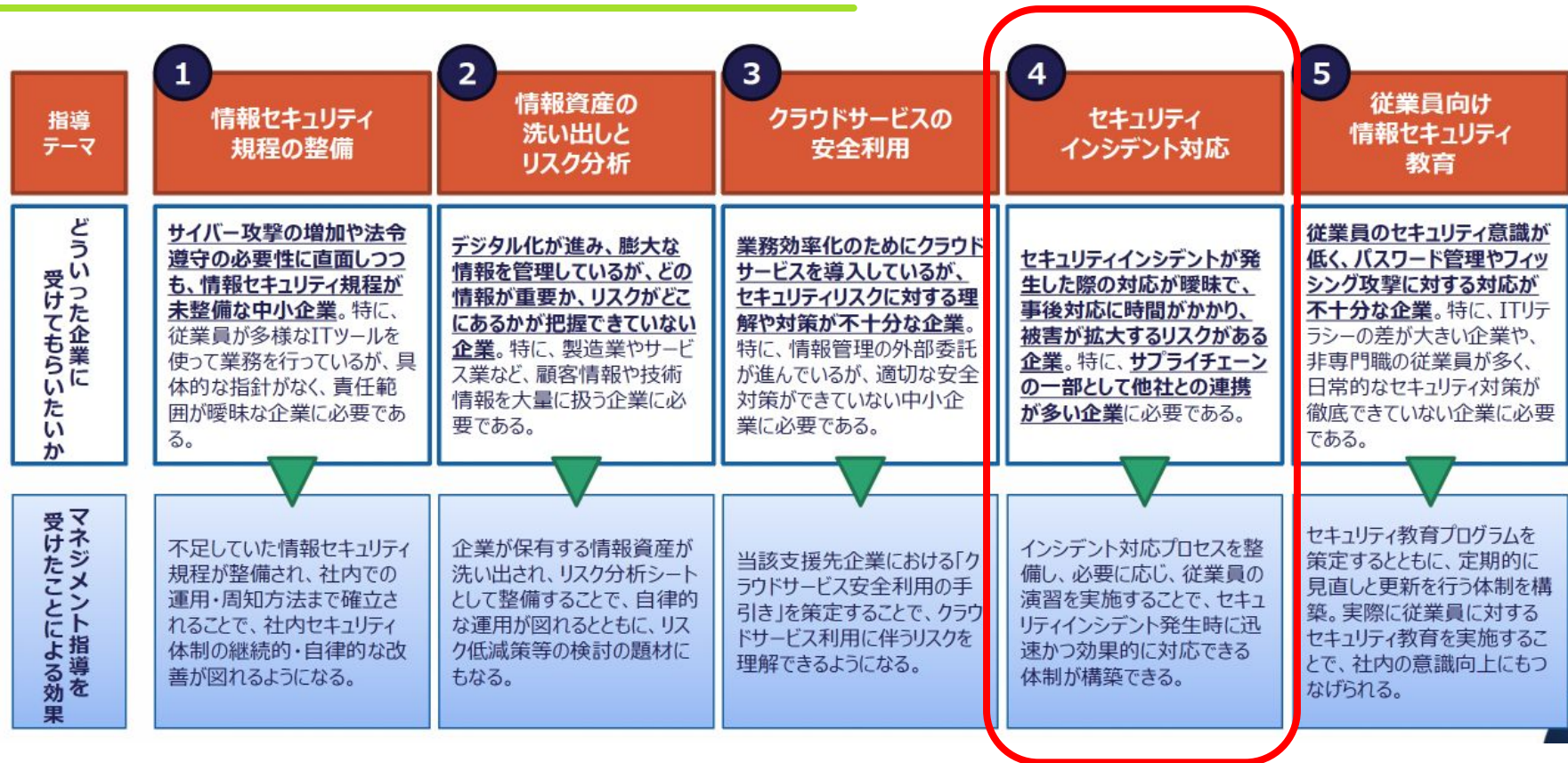
- 3回訪問では深掘りが難しい
- 指導ツールが小規模企業には“やや高度”
- 3回終了後のフォローアップ体制が弱い

03

事例①：テーマ④

セキュリティインシデント対応（会計事務所）

# 指導テーマ④



# 指導テーマ④ 標準的な進め方

1～2  
週間

## 事前準備#1

- \*IPA自社診断(Excel版)の実施依頼
- \*現在のインシデント対応プロセスやポリシー、規程の確認

### 第1回

#### 現状のセキュリティインシデント対応プロセスの評価と重要項目の説明

指導先企業のビジネス内容や組織概要等を聞き取った上で、企業のセキュリティインシデント対応体制を評価し、現状を把握します。既存のインシデント対応プロセスやポリシー、規程等の見直し、改善点等を洗い出します。  
また、簡易なディスカッション演習を実施し、IT-BCPの考え方を説明します。  
作成するインシデント対応手順書の対象テーマ（「ウイルス感染・ランサムウェア感染」「情報漏洩」「システム停止」のいずれか（あるいは複数））を検討します。

2～3  
週間

## 事前準備#2

- \*セキュリティインシデント対応手順書案の検討・策定
- \*専門家からの指導に基づき、インシデント対応手順書のドラフト内容をレビュー

### 第2回

#### セキュリティインシデント対応手順書の検討と評価

指導先企業で検討したインシデント対応手順を確認し、手順書案として仕上げます。  
また、具体的な演習計画（シナリオ含む）の検討を進めます。

2～3  
週間

## 事前準備#3

- \*インシデント対応演習計画を策定（シナリオ含む）
- \*インシデント対応演習実施に向けて、社内調整（演習参加メンバーの選定、スケジュール調整等）

### 第3回

#### インシデント対応机上演習の実施とレビュー

策定したインシデント対応手順書に従い、机上演習を実施します。社員全体ではなく、セキュリティ担当者を対象とした演習とすることも可能です。専門家が演習のコーディネイトを支援します。  
演習結果レビューの考え方について指導するとともに、今後の継続的な演習体制の構築とガイドライン策定に向けたアドバイスをを行います。

計2.0ヶ月  
程度



# 事例① 会計事務所

大阪府		事例No.7
業種	学術研究, 専門・技術サービス業	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
従業員数	3人	
資本金	5千万円以下	C会計事務所
推進担当者	(非公開)	
指導専門家	高橋 幸司 (株式会社東洋 常務執行役員CIO)	

## ■ 企業・団体紹介

関西圏において、多様な法人や個人事業主の会計・税務をサポートし、財務面でのコンサルティングも実施している。

## ■ 参加の動機

数十社のクライアントを抱える中で、サイバーセキュリティに対する漠然とした不安があった。今後、自身でどのように取り組みを進めていべきか、具体的な対策を知りたいと考えた。特にクラウドストレージの利用やルータの脆弱性対策など、ビジネス活動に直結する部分での不安を取り除きたいと考えていた。そのような中、大阪商工会議所から今回の相談会の情報を入手し、十分に安心できる機関からの案内であり、イベントへの参加を決めた。

## ■ 情報セキュリティ上で感じていた課題

- 小規模な会計事務所であるが、顧客の重要な情報を取り扱う必要があることから、かねてより情報セキュリティ対策は重要であると考えていた。
- 第一歩として「サイバーセキュリティお助け隊」サービスを活用し、UTMの設置等は行っているものの、これで十分なのかどうか、取り組みが機能するのかがわからない。
- 効率的な業務推進や顧客との情報共有のために各種のクラウドサービスも積極的に活用していることから、これらの適切な利用の仕方についても確認しておきたいと考えていた。

## 専門家指導のポイント

### ■ 組織の規模に見合った技術的対策が取られている点を評価

サイバーセキュリティに対する不安から、いち早く「サイバーセキュリティお助け隊」サービスを活用してUTMを設置するなど、必要な対策は取られていると思われる。クラウドストレージは、ランサムウェア攻撃被害からのリカバリーの面で有効である点など、対策と効果の関係について説明した。加えてアカウント・パスワードの管理、バックアップ運用について必要なアドバイスをを行った。

一方で、実際にインシデントが発生した場合の対応など、体制面の整備が十分でない可能性があった。

### ■ すでに実施しているセキュリティ対策について実践的な形で効果や課題を検証

セキュリティ対策をどのレベルまで実施すればよいかは、どの企業も悩むところである。実際に、インシデントに対応する手順書を作成した上で、ウォークスルー型で検証を行うことで、対策の効果と残存する課題等が明らかになると考えた。

実際に「ランサムウェア感染」を想定したシナリオを作成し、それに基づく机上訓練を行うことで、現状の対策レベルを確認し今後の課題を明らかにした。

## 指導先企業からのコメント

### ■ 専門家指導の成果

- 小規模組織での対策について、専門家の経験に基づく具体的なアドバイスをいただけたことで、今後の取り組み方針がかなりクリアになった。
- 相談会で明らかになった課題について専門家によるハンズオン指導で対処する今回の枠組みは、事業者にとって大変ありがたい制度であった。

### ■ ご意見・ご感想

指導をいただいた結果をもとに、引き続き課題が残るバックアップ・リストア等の対策について、引き続き取り組んでいきたい。

漠然とした不安



多くの中小企業が抱えている



現状を整理

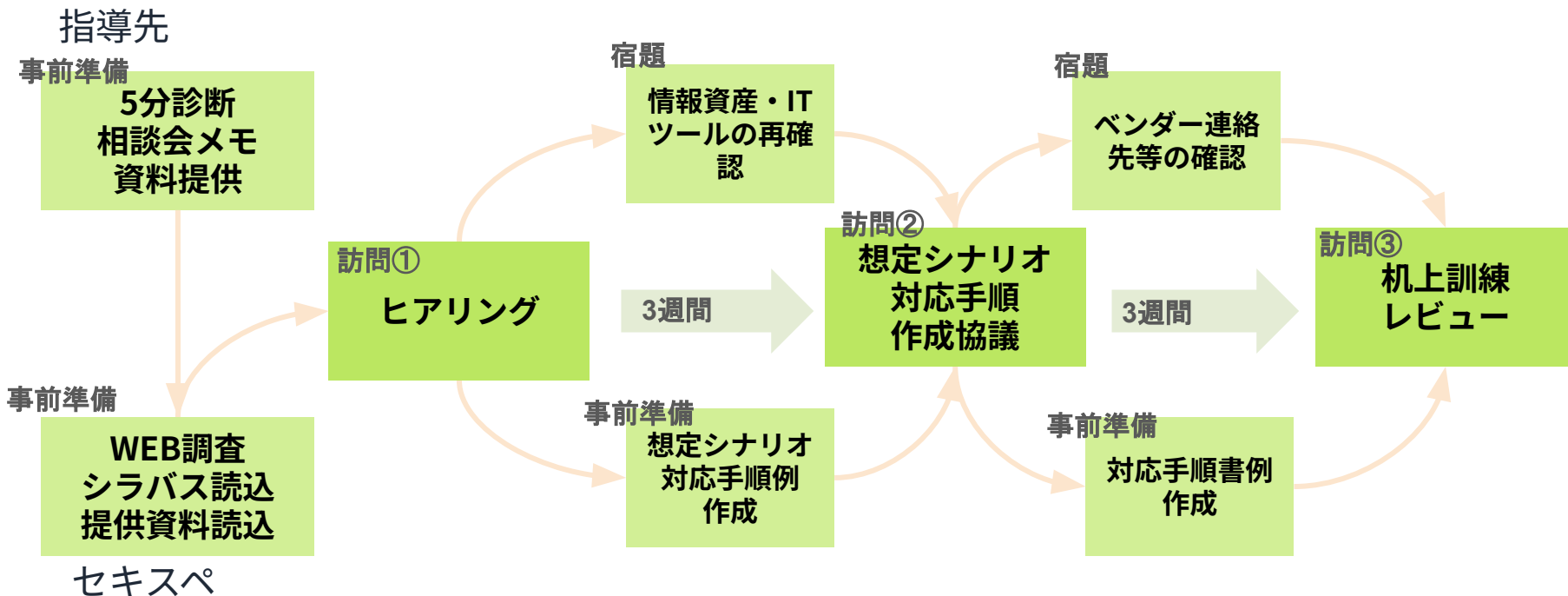


不安感払拭



# 事例① 会計事務所 実施概要

ケース④：インシデント対応 3週間隔の訪問で計画（約2ヶ月）



# 事例① 会計事務所 実施ポイント

---

- **事前準備**
  - 「5分でできる！自社診断（Excel版）」、その他資料の提出依頼
- **訪問①**
  - 指導ツールで準備されているヒアリングシートでヒアリングを進める
  - 3人と小規模事業者のため、規定類は整備されておらず、社長の判断が全てのためIPAの規定サンプルを紹介
  - SaaS等のクラウドサービス利用が多くアカウント管理とバックアップが課題
- **訪問②**
  - 協議によりランサムウェア感染時のインシデント対応を想定
  - 対応手順書の作成に当たり様々な自治体等が公開している対応手順書案を紹介
  - クラウドサービスのヘルプデスク等の連絡先もしくはITベンダーの保守対応先を確認
- **訪問③**
  - 対応手順書を今後継続してブラッシュアップして頂くことを推奨した。

# 事例① 会計事務所 成果

## 指導先企業からのコメント

### ■ 専門家指導の成果

- 小規模組織での対策について、専門家の経験に基づく具体的なアドバイスをいただいたことで、今後の取り組み方針がかなりクリアになった。
- 相談会で明らかになった課題について専門家によるハンズオン指導で対処する今回の枠組みは、事業者にとって大変ありがたい制度であった。

### ■ ご意見・ご感想

指導をいただいた結果をもとに、引き続き課題が残るバックアップ・リストア等の対策について、引き続き取り組んでいきたい。

出典：IPA セキュリティマネジメント指導事例集

- **漠然とした不安**が想定シナリオで演習することで想定できるリスクへと変換
- アカウント管理及びBCP・バックアップの見直しが進む
- ITベンダー等の連絡先を整理することで**経営者の危機対応力が向上**

# 事例① 改善点・学び

---

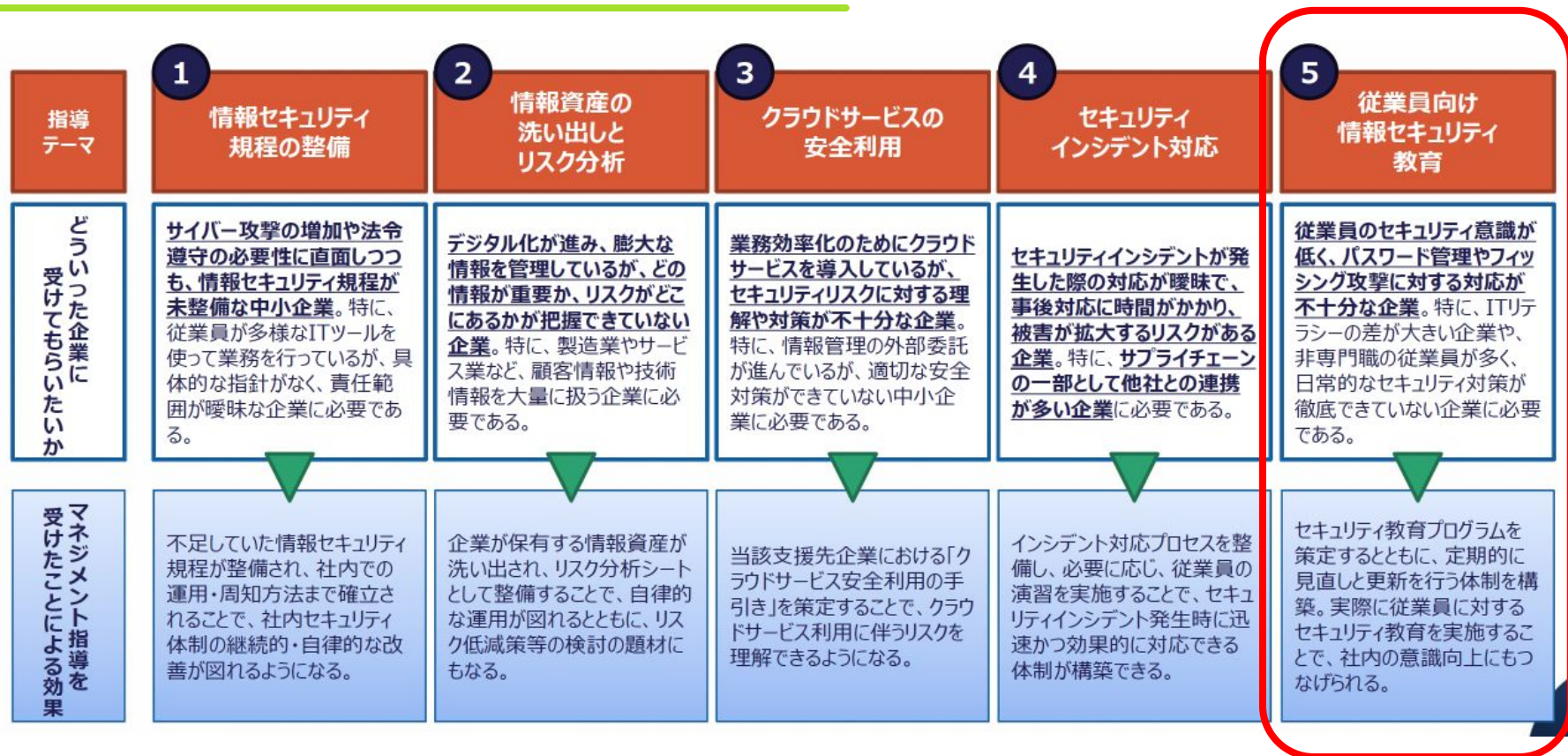
- インシデント対応の指導ツールは少々大きめの企業規模を想定している
  - 小規模企業向けヘアレンジが必要
  - 簡略化されたテンプレートの準備を希望
- **インシデント想定シナリオからバックキャスト的に現状を知る手法は有効**
  - 具体的なシナリオで企業側が実感できる
  - 投資対効果が見えやすくなる
- 継続支援の要望への対応
  - 継続支援できる体制整備が必要

# 04

## 事例②：テーマ⑤

### 従業員向けセキュリティ教育（社会福祉法人）

# 指導テーマ⑤



# 指導テーマ⑤ 標準的な進め方

1～2  
週間

## 事前準備#1

- \*IPA自社診断(Excel版)の実施依頼
- \*現在のインシデント対応プロセスやポリシーの確認

### 第1回

#### 現状のセキュリティ教育計画の評価、セキュリティ教育実施に向けた調整

指導先企業のビジネス内容や組織概要等を聞き取った上で、企業のセキュリティ教育に状況を評価し、現状を把握します。また、企業のニーズも踏まえ、IPA等が提供している各種コンテンツ等も紹介した上で、第2回に実施予定の従業員向け教育の計画を立案します。

2～3  
週間

## 事前準備#2

- \*教育プログラムの内容を確認するとともに、開催に向けた準備作業を行う。
- \*教育実施に向け、従業員（教育対象者）へのアナウンスを行う。

### 第2回

#### 従業員向けセキュリティ教育実施

IPAコンテンツを用い、従業員向けの情報セキュリティ教育を実施します。

2～3  
週間

## 事前準備#3

- \*教育実施後の効果を評価し、次回の教育プログラムに向けた改善点を整理する。
- \*継続的な教育体制構築に向けたアイデアを社内共有する。
- \*社内検討結果を踏まえた、セキュリティ教育計画（改訂版）案を策定する。

### 第3回

#### 教育実施結果のレビューと、以後の継続実施に向けた計画の見直し

教育実施効果分析結果をレビューし、効果があったポイントや要改善点等について指摘します。また、継続的な教育体制の構築に向けて、企業側が策定した計画改訂版について改善アドバイスをを行います。

計2.0ヶ月  
程度



# 事例② 社会福祉法人

## 管理監督機関 からの要請

上流からの圧力

何から実施すれば  
良いか？

優先度をつける

大阪府		事例No.2
業種	医療、福祉	セキュリティ対策の第一歩として従業員の意識を向上
従業員数	100名弱	
資本金	5千万円以下	社会福祉法人がくぶく福祉会
推進担当者	長井 英一郎 様（すいた障がい者就業・生活支援センター副所長）	
指導専門家	高橋 幸司（株式会社東洋 常務執行役員CIO）	

### ■ 企業・団体紹介

大阪府吹田市を拠点に、障がいのある方々の自立支援や地域での共生を目指す支援を行っており、就労支援や生活支援を中心に、利用者の個々のニーズに合わせたサービスを提供している。なかでも、生活介護事業所や就労継続支援B型事業所では、作業活動を通じて働く喜びや生活の充実を支援。また、地域社会とのつながりを重視し、多くの人々がともに支え合う社会の実現を目指している。

### ■ 参加の動機

近年、医療法人や社会福祉法人に対して、厚生労働省からサイバーセキュリティに関する対応がな一層要求されている。当法人でも個人情報を適切に取扱うためのセキュリティ対策を強化したいと考えているが、何から手を付けてよいか分からず、具体的なアドバイスが欲しいと考えた。

大阪商工会議所に開催された相談会には都合により参加できなかったが、後日専門家とのオンラインによる個別相談を経て、指導に臨んだ。

### ■ 情報セキュリティ上で感じていた課題

- まずは従事している職員のセキュリティ意識を高めることが重要であると考えているものの、そのために何を実施すればよいか分からない状態。第一歩として何から取り組めばよいか、具体的なアドバイスが欲しいと考えていた。
- 複数の事業所があるが、具体的な個人情報やメールの取り扱い等は各事業所任せになっている。

### 専門家指導のポイント

#### ■ セキュリティ対策の拠り所となるセキュリティポリシー及び各種規程作成のアドバイス

同法人においては、セキュリティ対策を進める上で重要となるセキュリティポリシーや各種規程が整備されていない状況であった。これではポリシーに沿った従業員教育や、規程に基づいた個人情報の取り扱い等が実施できないと考え、所管省庁からの要件に対応するためにも、可及的速やかにポリシーの策定や規程類を整備するようアドバイスした。

#### ■ 従業員の意識向上に向けた第一歩としての教育実施

本来は整備されたセキュリティポリシーや規程に基づいた従業員教育を行うべきであるが、体制を整えることが難しく、現状では教育実施ができない恐れがあった。そこでまずは法人全体のセキュリティ意識向上をめざす第一歩となる啓発活動として、IPAの動画コンテンツ等を用いて教育を実施。身近な「標的型攻撃メール」を題材に、個人情報の取り扱い、法令等で定められた対処方法などについて具体的にアドバイスを行った。

### 指導先企業からのコメント

#### ■ 専門家指導の成果

- 日常的に使用するメールについての注意事項や個人情報の取り扱いについて基本から教えていただき感謝している。
- 法人内での従業員の意識向上につながった。法人内での今後のセキュリティポリシー及び各種規程の策定に向けても動きがきっかけになった。

#### ■ ご意見・ご感想

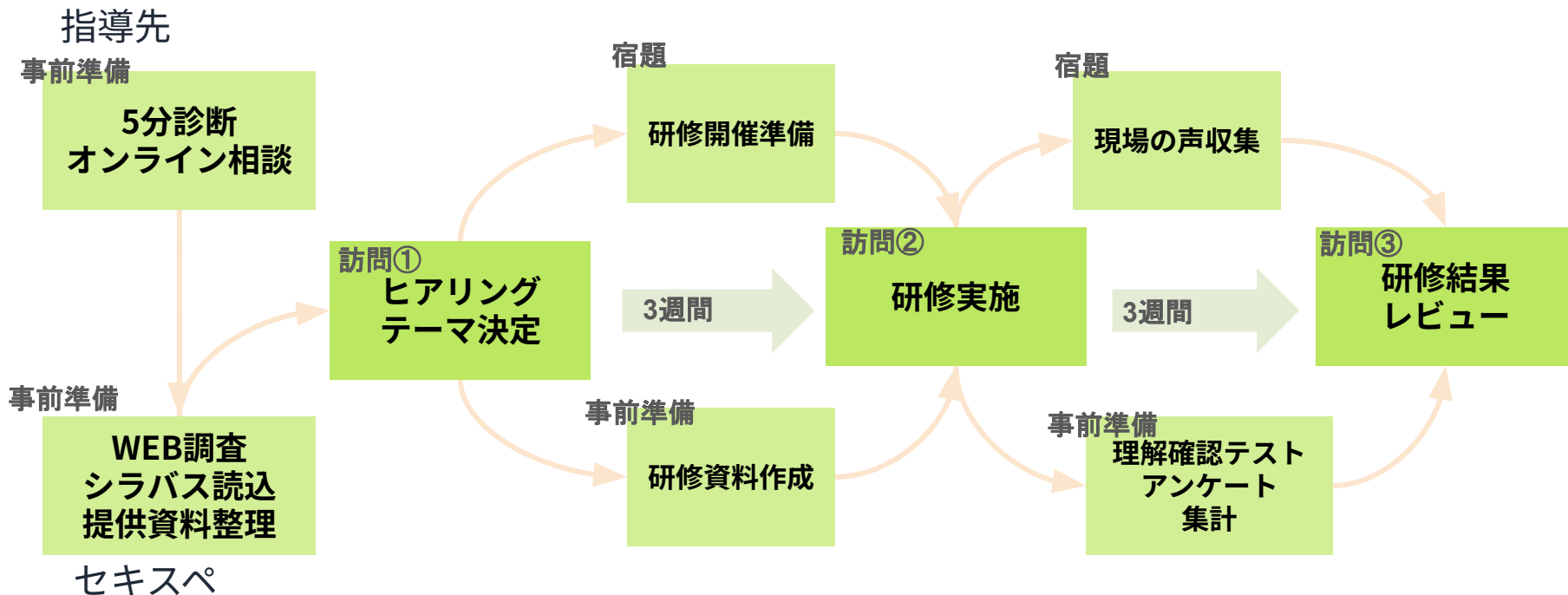
指導専門家の方には今後も引き続き、ITの活用や情報セキュリティに関して継続支援いただきたいと考えている。

出典：IPAセキュリティマネジメント指導事例集



## 事例② 社会福祉法人 実施概要

ケース⑤：セキュリティ教育 3週間隔の訪問で計画（約2ヶ月）



## 事例② 社会福祉法人 実施ポイント

---

- 事前準備
  - オンラインで相談会を実施し希望テーマを協議決定
- 訪問①
  - 企業側の要望を整理し標的型攻撃メールを題材に研修を決定
  - 個人情報取り扱いについても研修に盛り込むことで決定
- 訪問②
  - 指導ツールが準備している構成をベースにアレンジ
  - 理解確認テスト・アンケートを準備
- 訪問③
  - 理解確認テスト・アンケート結果を集計し解説

## 事例② 社会福祉法人 成果と課題

### 指導先企業からのコメント

#### ■ 専門家指導の成果

- 日常的に使用するメールについての注意事項や個人情報の取り扱いについて基本から教えていただき感謝している。
- 法人内での従業員の意識向上につながった。法人内での今後のセキュリティポリシー及び各種規程の策定に向けても動ききっかけになった。

#### ■ ご意見・ご感想

指導専門家の方には今後も引き続き、ITの活用や情報セキュリティに関して継続支援いただきたいと考えている。

### 成果

- メールについて職員の **行動変化**
- 理解度テストで理解の可視化
- アンケートで次の課題の明確化

### 課題

- 規定が古く研修内容に折り込めない場合がある
- 自組織内で継続した研修が困難

これから支援を始めるセキスペには一番扱いやすいテーマ！

# 05

## 事例③：テーマ② 情報資産の洗い出しとリスク分析

**本事例は当日投影のみとなります  
(配布資料非掲載)**

06

指導を通してセキスペとして感じた事

# 制度について

---

- 支援回数の柔軟化（3回 → **段階的モデル** へ）
  - テーマによっては回数増加や段階を設けるのはどうか
  - 複数テーマに渡る場合もあり得る。
- 規模別・業種別ラインナップ
  - 規模・業種によっては指導ツールがそのまま当てはまらない可能性がある
- 支援後フォローアップの仕組み強化
  - 継続支援の要望が多く何かしらのフォローアップ体制が必要
- ITC・診断士との連携
  - DX推進におけるセキュリティ対策にセキスペを活かせないか

# 専門家として

---

- 中立・公平の立場を貫く
  - 本業として得ている知見を抽象化して中立的な立場の大切さ
- 事実と**思い込み解釈**を分離させる
  - 企業側・専門家の思い込みを抑え事実前提で指導する
- “**理解度に合わせる**”ファシリテーション
  - 傾聴と対話を重視したコミュニケーションを心がける
- 継続できる仕組みを残す
  - 指導終了後、自律できる仕組みを助言する

07

## 企業内人材が外部活動に参加する価値



# 社会貢献としての意義

## 社会全体に広がる価値創出のために

- 人材不足への **大きな解決策**
- 企業の壁を超えた知識共有
- 地域のセキュリティ水準向上



# 自社への還元

## 多様な他社の課題に触れる事で

- 経営視点が養われる
- ネットワークが広がる
- インシデント対応力が向上
- **組織変革のヒント** が得られる



# 新しいキャリアの形

---

## 社会とつながる新しい働き方

- 副業ではなく **社会貢献型キャリア**
- 専門家派遣制度を通じた自身の成長
- 企業内に留まらず社会へ広がる働き方



08

まとめ

# まとめ

---

- セキュリティは一社だけでは守れない
- 企業内専門家が“**外へ出る**”ことが地域を強くする
- 指導ツールは技術ではなく“**対話のフレーム**”
- 今日の事例が、皆さまの支援活動のヒントになれば幸いです

**ご清聴ありがとうございました**