情報処理安全確保支援士向け
「セキュリティマネジメント指導ツール活用セミナー」

中小企業支援
のための

# セキュリティマネジメント指導ツールの紹介

2025年11月

独立行政法人情報処理推進機構(IPA)
セキュリティセンター　普及啓発・振興部
普及啓発グループ

# 目次


## 1. 令和６年度事業の実施結果

## 2. セキュリティマネジメント指導ツールの解説

指導テーマ①：情報セキュリティ規程の整備

指導テーマ②：情報資産の洗い出しとリスク分析

指導テーマ③：クラウドサービスの安全利用

指導テーマ④：セキュリティインシデント対応

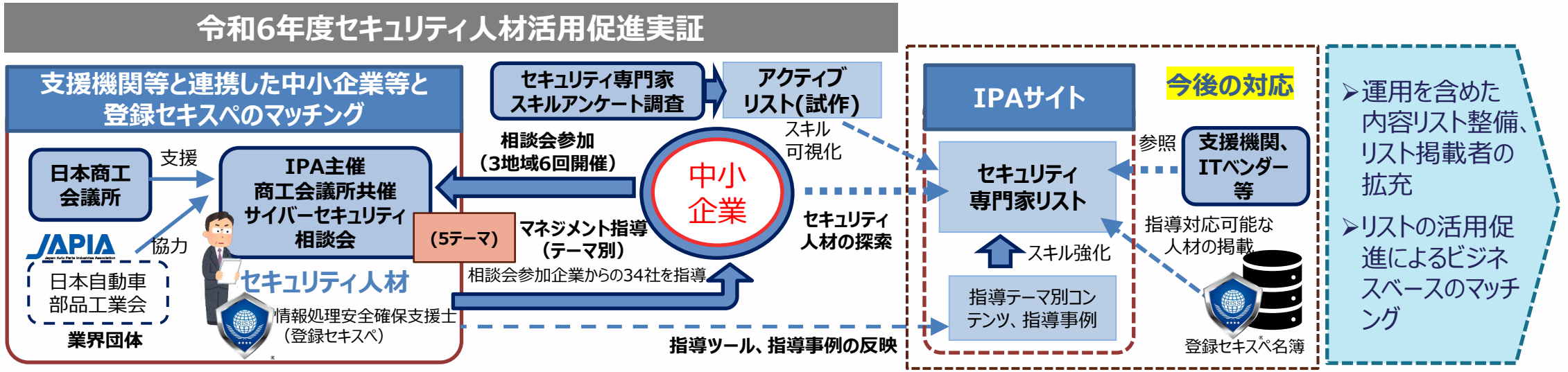
指導テーマ⑤：従業員向けセキュリティ教育

## 3. 令和７年度事業の実施概要

# １．令和６年度事業の実施結果

# 令和6年度事業
# セキュリティ人材活用促進実証の結果

- 令和6年度セキュリティ人材活用促進実証では、**中小企業と情報セキュリティの専門家である情報処理安全確保支援士（登録セキスペ）のマッチング**を促す場として、商工会議所との共催による**サイバーセキュリティ相談会**（3地域6回）を開催し、個別相談を経て希望する企業に対して、登録セキスペによる**セキュリティマネジメント指導**（訪問指導）を実施、参考になる**指導事例をベストプラクティス**として取りまとめた。
- セキュリティマネジメント指導の実施に際し、中小企業セキュリティ対策ガイドライン（付録を含む）を活用した**５つの指導テーマ**を設定し、各テーマについて**指導ツール（実施要領及びワークシート等）を整備**した。
- また、**登録セキスペが提供可能な業務やスキル等を可視化**するため、**セキュリティ専門家スキル調査アンケート**を実施し、中小企業とセキュリティ専門家とのマッチング実証の結果も含めて、中小企業のセキュリティ支援が実施可能な**セキュリティ専門家リスト（登録セキスペ アクティブリスト）を試作**した。




※「令和6年度セキュリティ人材活用促進実証に係る業務」報告書について
https://www.ipa.go.jp/security/reports/sme/riss-katsuyo2024.html

# 1．サイバーセキュリティ相談会

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

**《中小企業等と登録セキスペのマッチングフロー》**

**商工会議所と連携したサイバーセキュリティ相談会**

- 商工会議所と連携したサイバーセキュリティ相談会を開催。
- 専門家によるセキュリティ対策の必要性等を訴求する基調講演を実施。

**登録セキスペによる個別相談**

- 相談会参加者のうち希望者に対して登録セキスペによる個別相談を実施。
- 自社のセキュリティ対策の課題を特定・優先づけを実施。

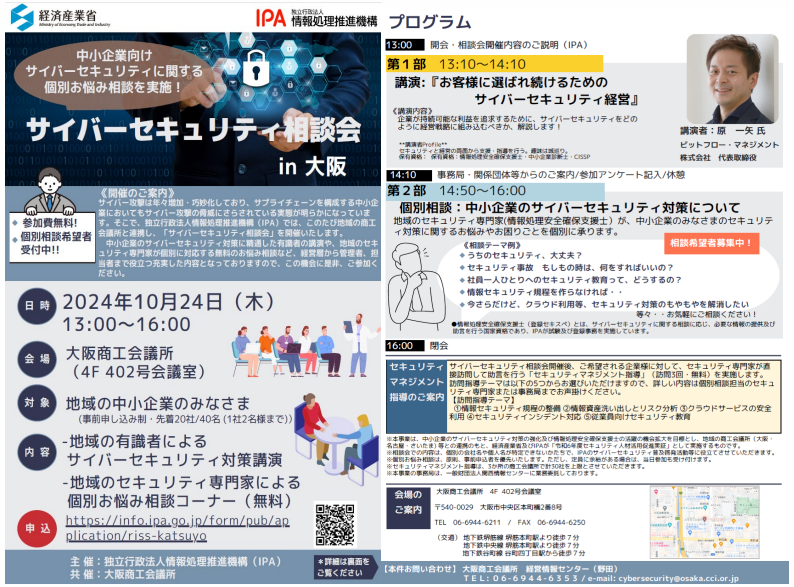
**登録セキスペによるマネジメント指導**

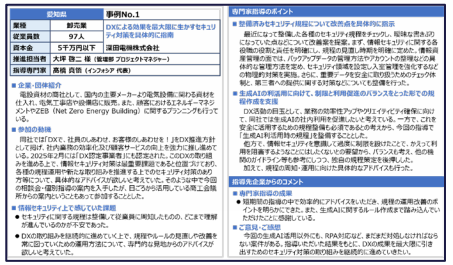
- 個別相談参加者のうち希望者に対し、５つのマネジメント指導テーマの中から選択したテーマについて伴走型支援（３回訪問）を実施（各回ごとに目標を設定）。

**講演の様子**

**個別相談の様子**

**相談会広報チラシ例**

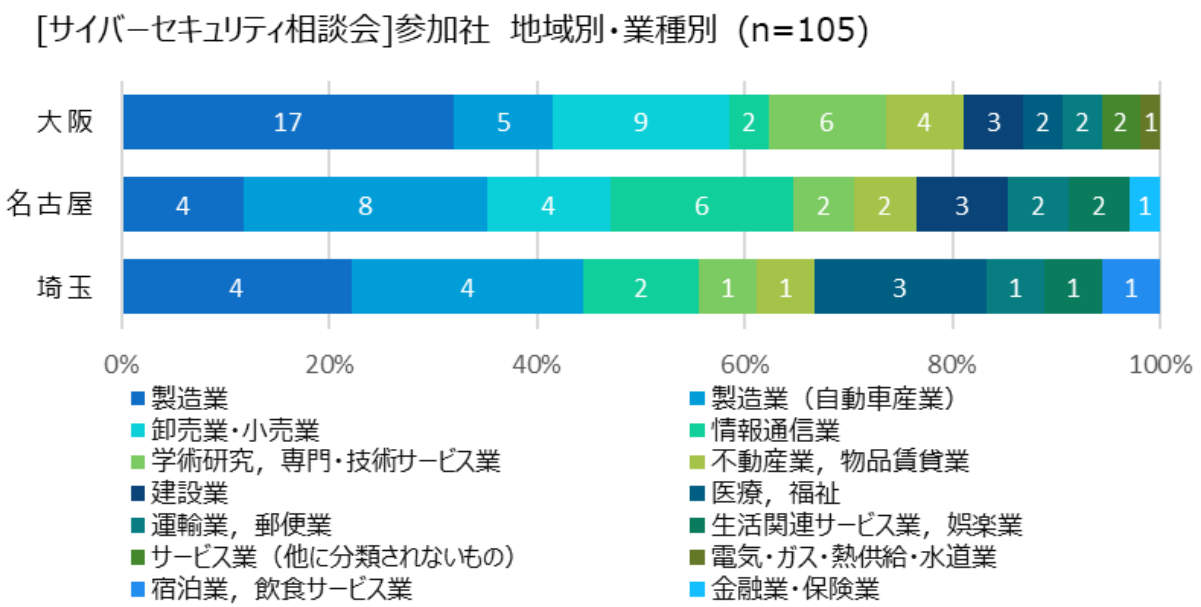


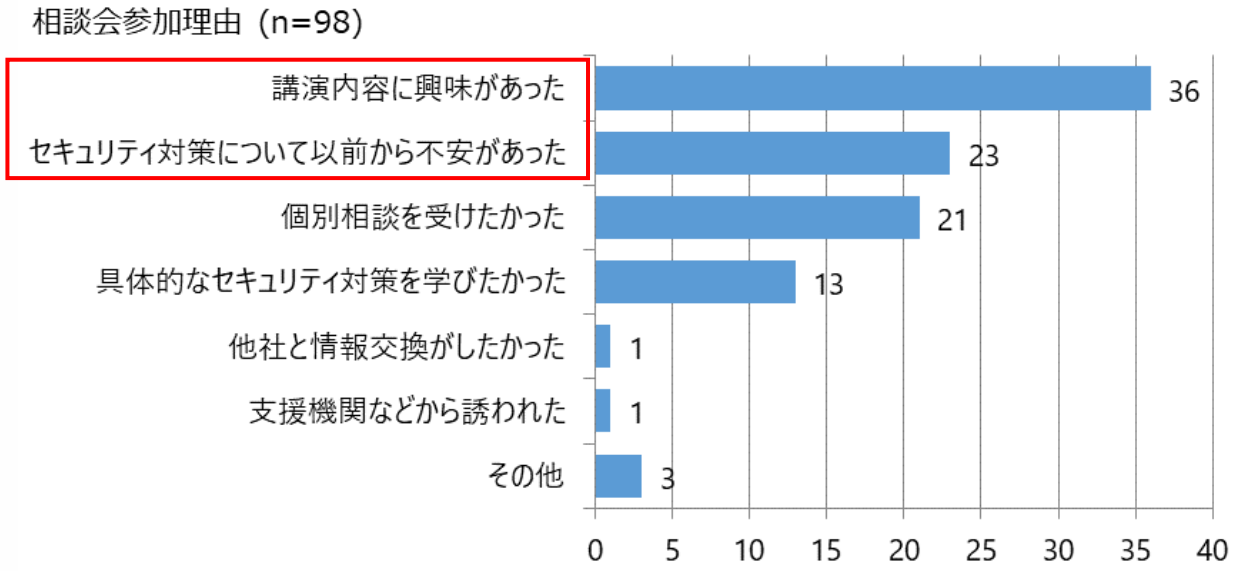



**指導事例集**
**（ベストプラクティス）**

# 1. サイバーセキュリティ相談会
## ① 相談会参加企業の業種と参加理由

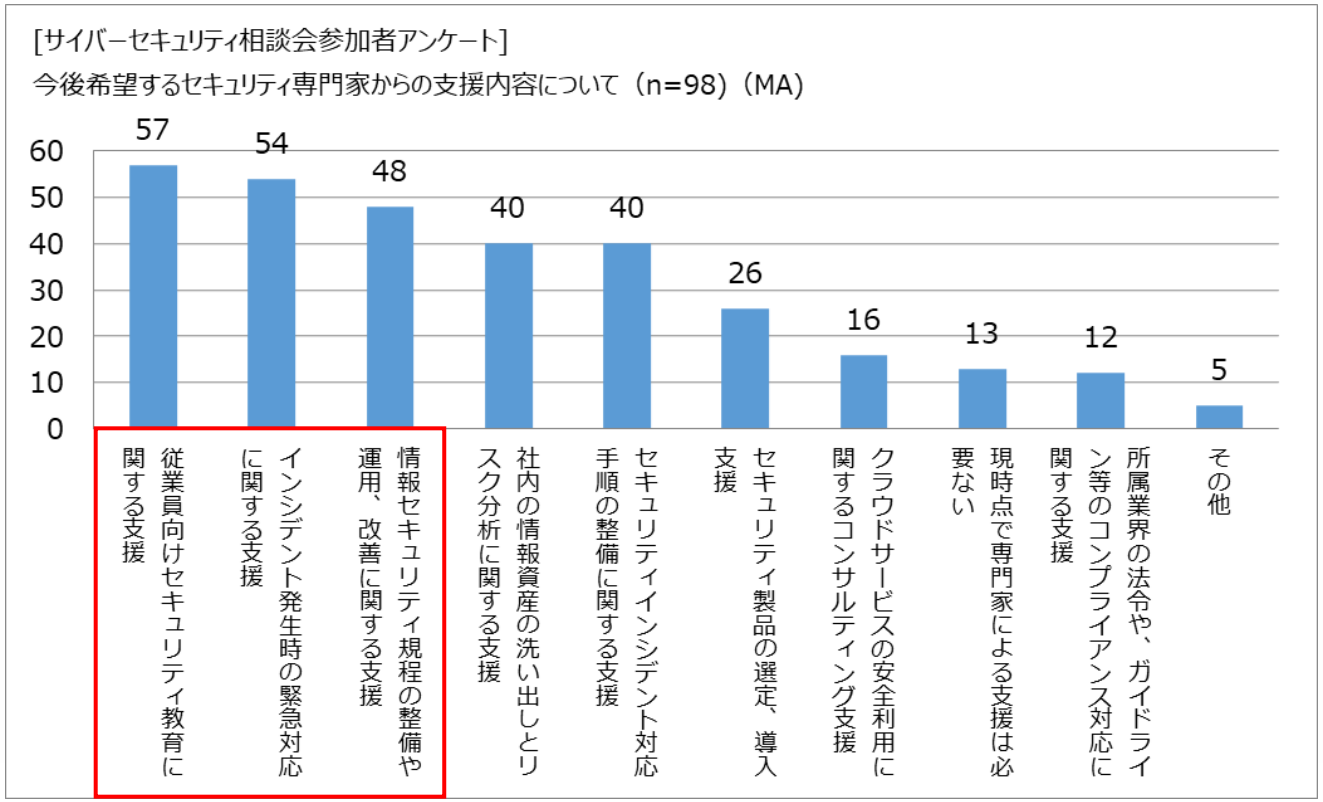
- サイバーセキュリティ相談会には、**3商工会議所で合計105社（122名）が参加**。地域別の傾向は、大阪は製造業を中心としながらも、幅広い業種からの参加が見られた。名古屋では製造業、特に自動車産業からの参加が多く、埼玉では製造業と医療・福祉分野からの参加が比較的多かった。
- 相談会参加の動機は、「講演内容そのものに興味があった」、「セキュリティ対策について以前から不安があった」とする回答が**全体の約６割**を占め、**セキュリティ対策について具体的な対策を実施する前の準備段階（情報収集段階）**にいる参加者が多かった。

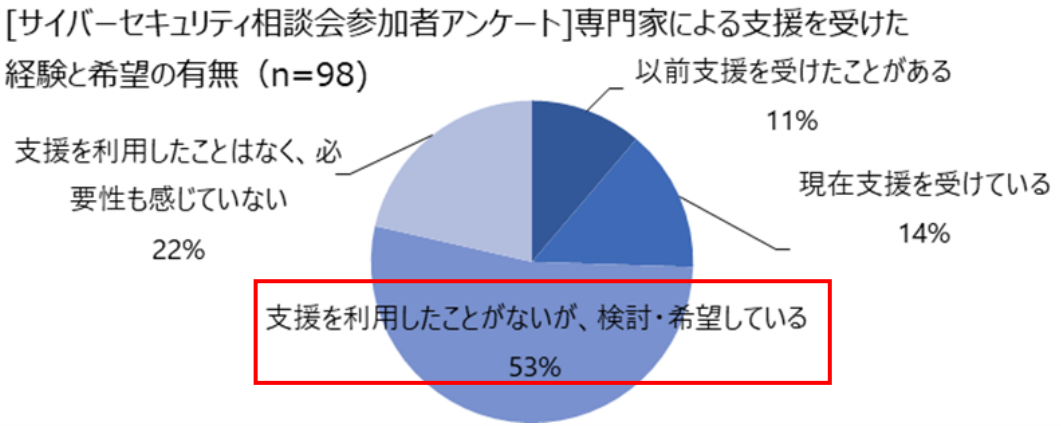


# 1. サイバーセキュリティ相談会
## ② 希望するセキュリティ専門家からの支援内容

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

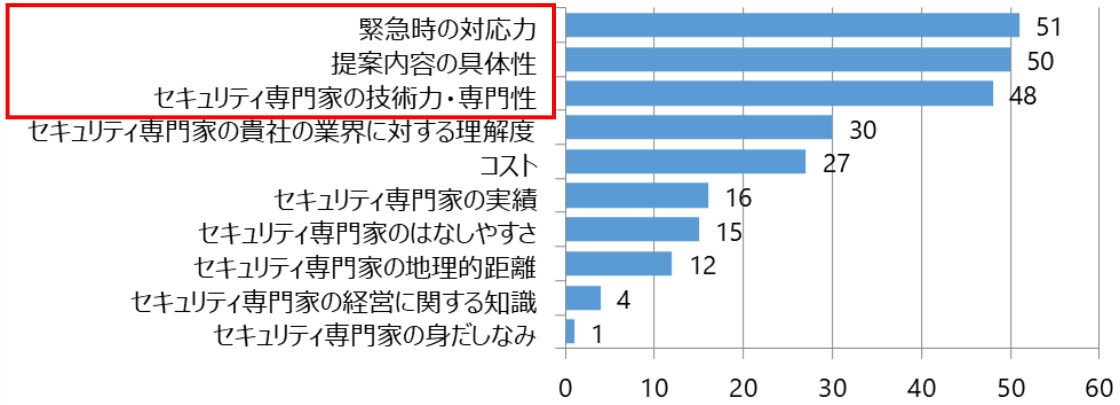


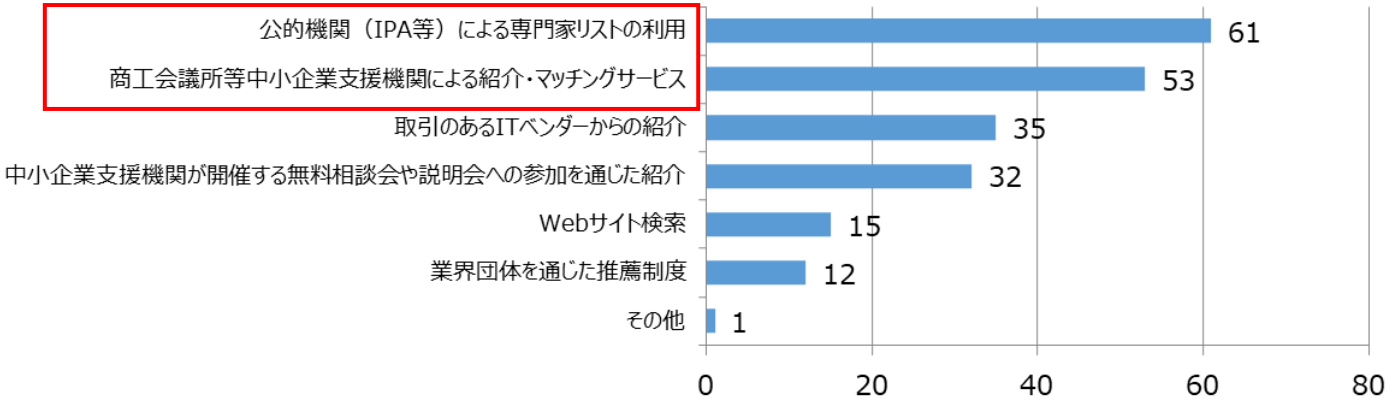
# 1．サイバーセキュリティ相談会
## ③ 専門家を選定するときに重視する点と探索手法

- 中小企業が**セキュリティ専門家を選定するときに重視する点**として、「緊急時の対応力」、「提案内容の具体性」、「セキュリティ専門家の技術力・専門性」が上位にあがった。このことから、セキュリティ専門家の**インシデント発生時の対応、セキュリティ対策提案時の具体性、技術力・専門性**が重要であることがうかがえる。
- **セキュリティ専門家の探索方法**は、「公的機関（IPA等）における専門家リストの利用」のほか、「商工会議所等の中小企業支援機関による紹介・マッチング支援サービス」が上位にあがった。このことから、中小企業に対してリーチするためには、**専門家リストを活用**した商工会議所等の**支援機関と連携したマッチングサービス**が望ましいことが示唆された。

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




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



# 1．サイバーセキュリティ相談会
## ④ 相談会における具体的な相談内容

➢ セキュリティ相談会における登録セキスペによる個別相談（55社）の具体的な相談内容としては、**成熟度・領域ともに多様**であり、①**標準的なひな形を自社向けにカスタマイズしたい**、②**取組中の対策の妥当性（現状で十分なのか）を第三者的に確認したい**、③**各種ガイドラインの要求事項を自社の具体的対策として落とし込みたい**といったものがあげられた。

**相談会における具体的な相談内容（個別相談）**

- 個別具体的な課題を持つ企業が存在する一方で、「守るべき情報が無い」「何をどう始めていいか分からない」といった初歩的な段階にある企業も依然として存在するなど、**相談各社におけるセキュリティ課題は、その成熟度や課題領域において非常に多様**。
- 「サンプル規程があることは知っているが、それをどのように使用し、自社用に作り直せばいいのかがわからない」など、**対策の内容や進め方についての具体的なアドバイスを求める相談**が見られた。
- 加えて、「作成した規程の内容が、本当に十分なのか、または自社に合っているかが分からない」、「お助け隊に加入しているがセキュリティ対策はこれだけで十分なのか分からない」、「ベンダー任せでシステムを構築しているが、この構成でセキュリティ対策ができているか確かめたい」、「何を優先してセキュリティ対策を進めていいのか分からない」 など、**自社の判断・取組の妥当性を、専門家の第三者的な視点から確認したいというニーズ**も存在。
- さらに、**業界別の対策水準の要求に関する相談**（自動車産業における「自工会/部工会・サイバーセキュリティガイドライン」や、医療分野における３省２ガイドライン「医療情報システムの安全管理に関するガイドライン」「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」（総務省・経済産業省））や、**取引先との事業継続性の確保を目的としたセキュリティ対策の相談**が多く、**要求事項を自社の状況に即した具体的な対策として落とし込む方法**について、実践的な示唆を求める声を複数確認。

# 2．セキュリティマネジメント指導

- セキュリティ相談会の参加企業のうち、希望する34社に対して**訪問指導（マネジメント指導）を実施**した。
- マネジメント指導の実施に際し、業種を問わない基本的なセキュリティ対策として、「中小企業の情報セキュリティ対策ガイドライン（付録を含む）」を活用した**５つの指導テーマ**を設定し、各テーマについて**指導ツール（実施要領及びワークシート等）を整備**した。

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

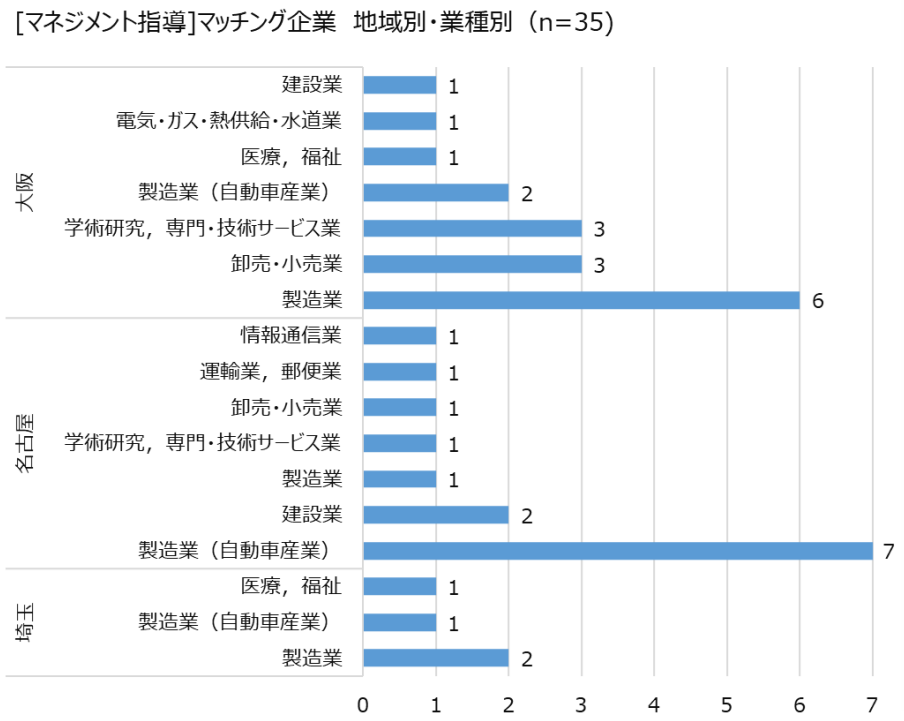
# 2．セキュリティマネジメント指導
## ① 中小企業と登録セキスペのマッチング

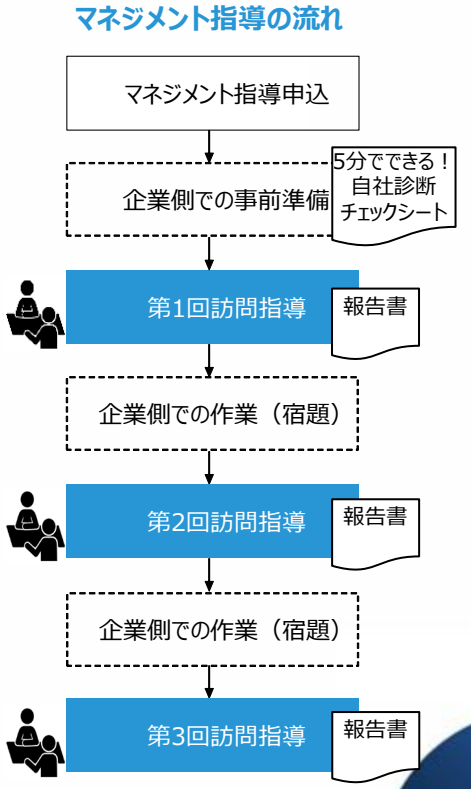
- サイバーセキュリティ相談会の個別相談を経て、訪問指導を希望する**企業と登録セキスペとのマッチング**を行い、34社に対してテーマ別の**セキュリティマネジメント指導（全3回訪問）**を実施した。
- マッチングに際しては、**指導先業の個別相談時の内容や希望するマネジメント指導テーマ、指導専門家の対象分野等を考慮**し、各企業に指導専門家の割り当てを行った（マッチング）。
- 実際の訪問指導は、マネジメント指導のテーマ毎に全3回の訪問指導を効率的に行うため、**各回の標準的な指導の進め方を示したシラバスを整備**して行った。

**《マネジメント指導実施件数》**

| テーマ / 地域 | 1．情報セキュリティ規程の整備 | 2. 情報資産の洗い出しとリスク分析 | 3．クラウドサービスの安全利用 | 4．セキュリティインシデント対応 | 5．従業員向けセキュリティ教育 | 総計 |
|---|---|---|---|---|---|---|
| 大阪 | 10 | 1 | 1 | 1 | 4 | 17 |
| 名古屋 | 2 | 2 | 2 | 4 | 3 | 13 |
| 埼玉 | 3 | 1 | 0 | 0 | 0 | 4 |
| 総計 | 15 | 4 | 3 | 5 | 7 | 34 |

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



# 2．セキュリティマネジメント指導
## ② 訪問指導の実施結果（指導テーマ別）

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

**マネジメント指導の実施結果（指導テーマ別）**

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

# 2．セキュリティマネジメント指導
## ③ 指導事例集（ベストプラクティス）

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

**《マネジメント指導事例集（ベストプラクティス）》**

| No. | 地域 | 指導先企業・団体名 | 業種 | 指導専門家 | 事例タイトル |
|---|---|---|---|---|---|
| 1 | 愛知県 | 深田電機株式会社 | 卸売業 | 髙橋 真悟 氏 | DXによる効果を最大限に生かすセキュリティ対策を具体的に指南 |
| 2 | 大阪府 | 社会福祉法人ぷくぷく福祉会<br>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<br>（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<br>（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<br>（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 |

# 3．アクティブリストの試作

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

**《アクティブリストの基本事項の整理》**

## Ⅰ　リストの目的

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

## Ⅱ　リスト掲載対象者

- 登録セキスペ資格を有する者で、中小企業に対するセキュリティ対策支援が可能な者
（企業に所属する者で副業・兼業で支援が可能な者もリスト掲載対象とする）
※所属組織が中小企業等に対するセキュリティコンサルを行っている場合は掲載の対象と想定

## Ⅲ　リスト管理・運用方式

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

## Ⅳ　検索・表示機能

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

## Ⅴ　リスト掲載項目

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

2．支援能力に関する情報：
・IPAが提供する指導ツールを活用したセキュリティ支援の対応
（情報セキュリティ規程の整備、情報資産の洗い出しとリスク分析、クラウドサービスの安全利用、セキュリティインシデント対応、従業員向けセキュリティ教育の5テーマ）
・保有する他の資格（中小企業診断士、ITコーディネータ等）
・得意とする業界
・中小企業支援の実績、具体的な支援事例
・スキル調査に基づく、得意とする支援領域

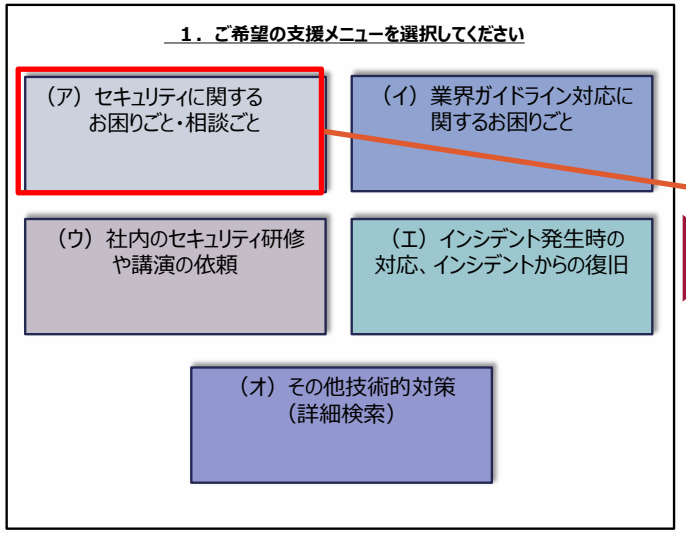
3．サービス提供条件に関する情報：
・支援形態（訪問/オンライン、コンサル/研修等）
・料金（1回2時間あたりの支援料金）
・支援可能期間
・支援可能地域

4．自己PR：
・支援実績や得意分野に関する自由記述

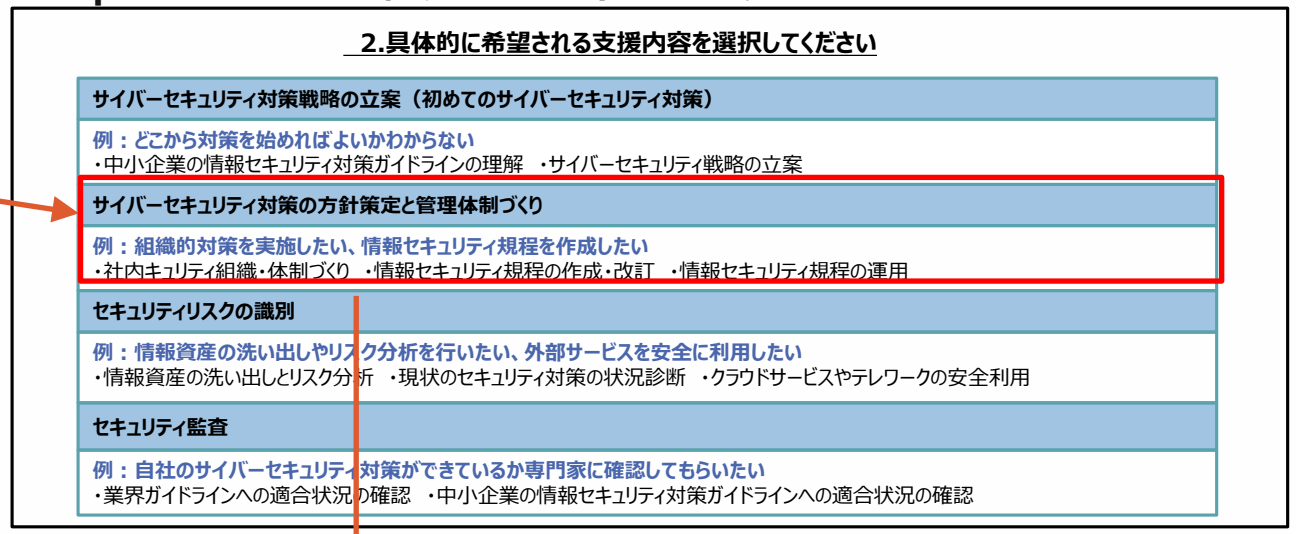
# 3．アクティブリストの試作
# ① リスト画面遷移の検討

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

## Step1:初めに希望する支援内容を選択する



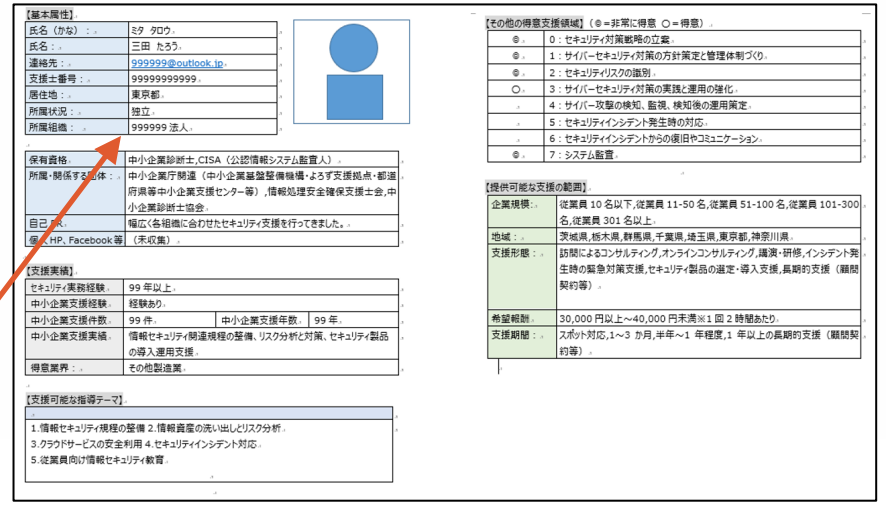

## Step2:支援内容の詳細や希望の条件を入力する




## Step3:条件に適合したセキュリティ専門家の名前をクリック

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

## Step4:セキュリティ専門家の詳細が個票として表示される



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

➢ 本事業で作成したアクティブリスト（試作）の一覧表イメージを以下に記す。

**《アクティブリスト（試作）一覧表イメージ》**

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

# 4. アクティブリストの試作
## ② アクティブリスト活用の検討

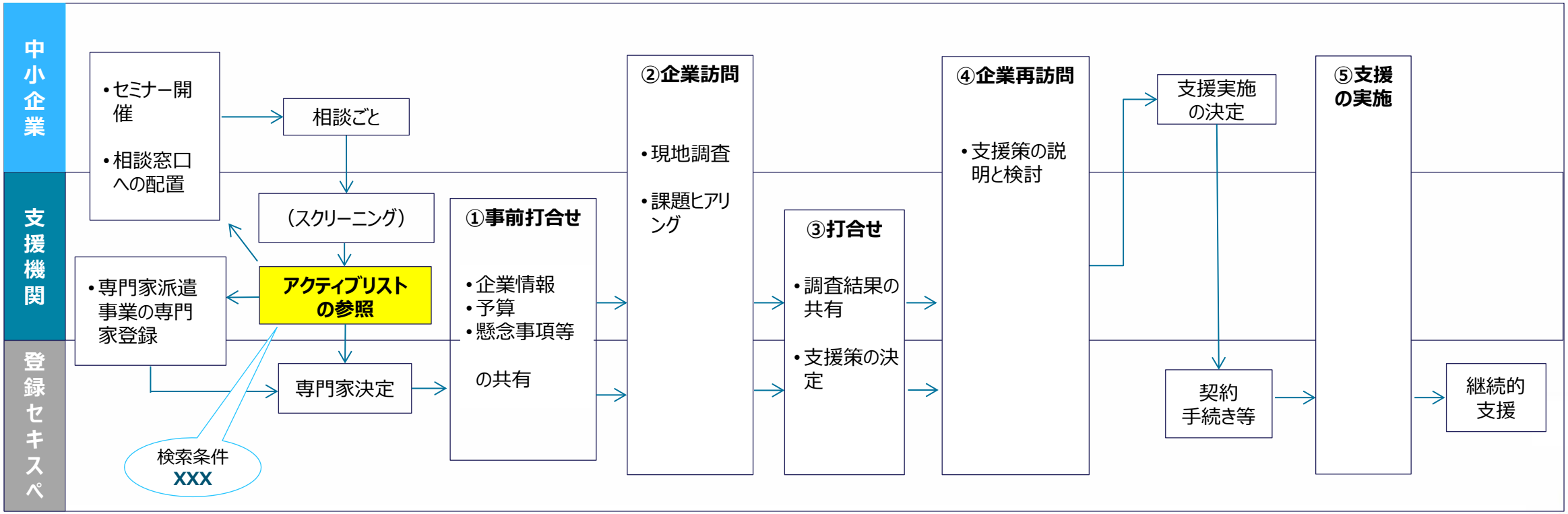
- サイバーセキュリティ相談会の参加者アンケートによると、**中小企業がセキュリティ専門家を探す際**には、「公的機関（IPA等）による専門家リストの利用」、「商工会議所等、中小企業支援機関による紹介」、「取引のあるITベンダーからの紹介」を望む声が多く、**「信頼性」、「身近さ」、「地域性」を重視**することが判明した。
- そこで、アクティブリストの活用について、中小企業がセキュリティ専門家を直接探索する場合の他、**①中小企業支援機関との連携**、**②ITベンダーにおける利用**の2つの活用シナリオを想定し、リストの活用方法について検討した。

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

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

| 活用シナリオ① | （利用者） 中小企業支援機関<br>（利用目的）中小企業のニーズに合ったセキュリティ対策を支援する登録セキスペを抽出する |
|---|---|

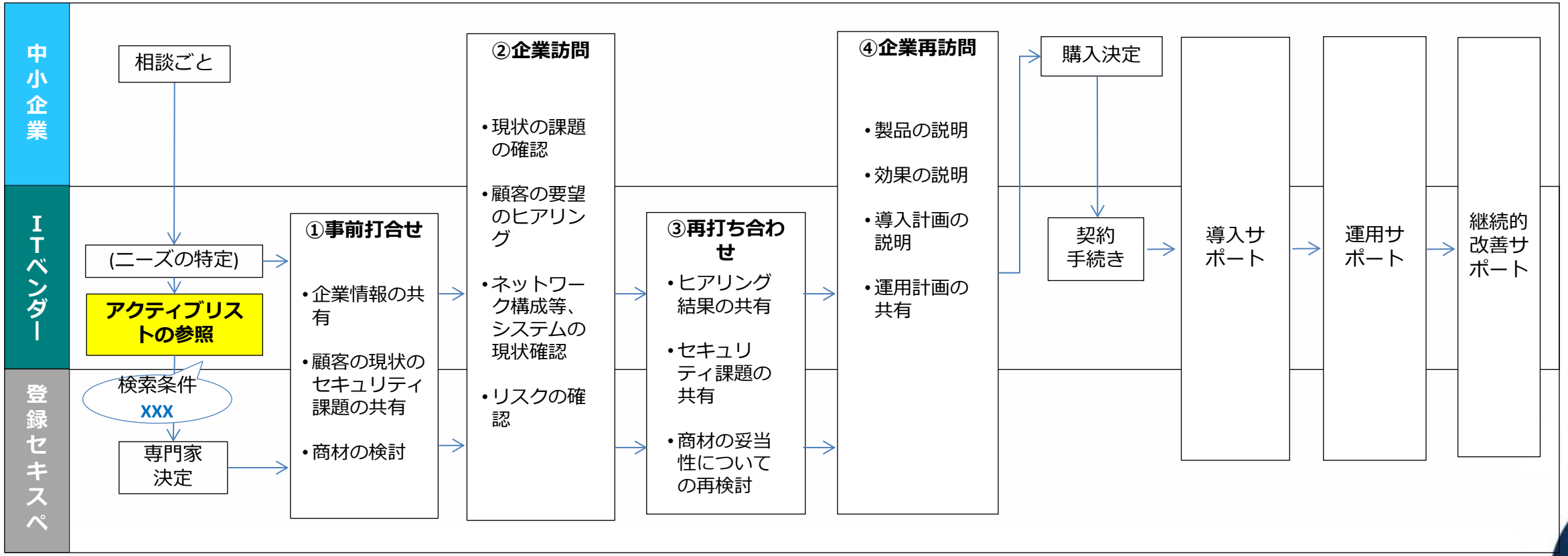
| | |
|---|---|
| **登録セキスペが中小企業に対して担う役割** | 社内ITリソースの補完者としての役割、経営者への説得者としての役割、包括的なセキュリティ戦略の立案と実施者の役割、セキュリティ製品導入後の品質担保者としての役割、効果的なIT投資実現のためのパートナーとしての役割 |
| **登録セキスペが支援機関に対して担う役割** | 支援プログラム実施のための専門的パートナーとしての役割 |
| **支援機関が中小企業に対して担う役割** | 中小企業とセキュリティ専門家・関係者とのネットワーク構築を支援者する役割 |



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

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

| | |
|---|---|
| **登録セキスペが中小企業に対して担う役割** | 中小企業の立場からのITベンダーからの提案に対する目利き役としての役割、ITベンダーと経営との橋渡し役としての役割、導入後のサポート等を通じた品質の保証者としての役割、効果的なIT投資実現のためのパートナーとしての役割 |
| **登録セキスペがITベンダーに対して担う役割** | 知識・経験の共有者としての役割、経営者との橋渡し役としての役割、品質管理・監督者としての役割 |



# ２．セキュリティマネジメント指導ツールの解説

# セキュリティマネジメント指導の全体像

中小企業は経営資源に制約から、限られたリソースの中で情報セキュリティ対策を行う必要がありますが、どの部分に対策の重点を置くべきかが、必ずしも明確でないケースが多くあります。

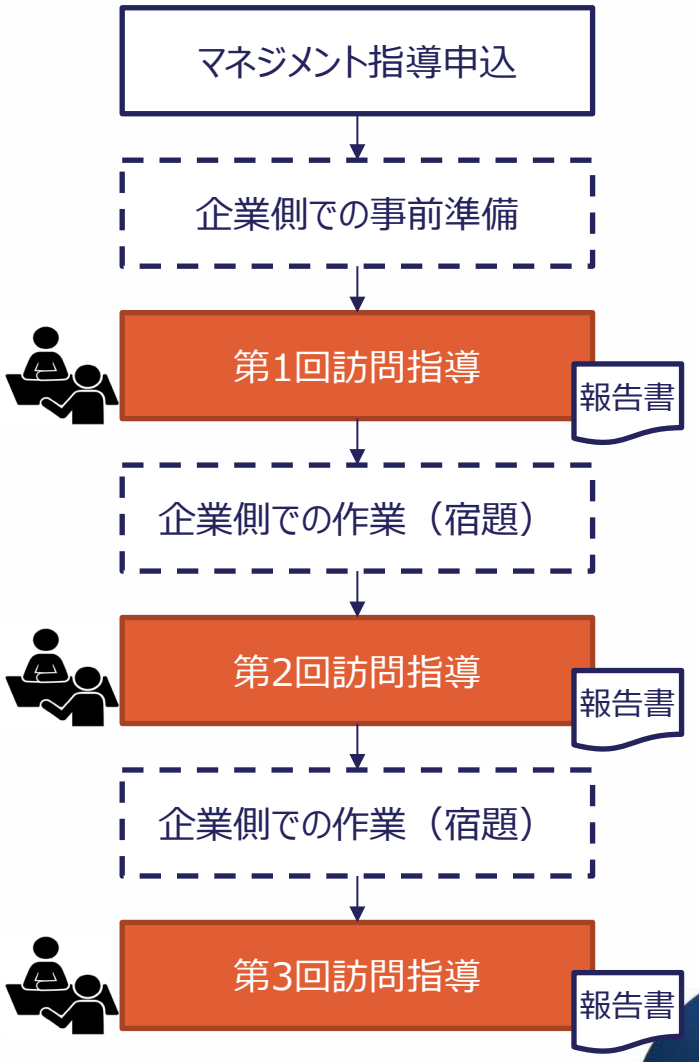
セキュリティマネジメント指導ツールは、そのような中小企業に対して、**①情報セキュリティ規程の整備**、**②情報資産の洗い出しとリスク分析**、**③クラウドサービスの安全利用**、**④セキュリティインシデント対応**、**⑤従業員向けのセキュリティ教育** の5つの主要なテーマを設定し、セキュリティ専門家が中小企業を訪問指導する際の基本的なフレームワークとして、具体的な方法と手順を提供しています。

各テーマにおいては、どのような企業がその指導を必要としているのか、指導によって達成されるべき目標、さらには具体的な作業内容や使用ツール、指導後の効果等を想定しています。これにより、セキュリティ専門家は指導先の企業ごとに、適切な指導計画を立て、効率的に支援を行うことができると考えています。

また、セキュリティマネジメント指導ツールには、セキュリティ専門家が指導先企業の現場で利用できる具体的なシラバスやチェックシート、ガイドライン等も含まれています。実際には、指導先企業の実情に応じた柔軟な対応が必要になることと思いますが、指導ツールの活用によって指導内容の見える化と一貫性が確保されるので、企業においても自助的なセキュリティ対策の強化にもつなげることが期待できると考えます。

セキュリティ専門家の皆さまにおかれましては、本指導ツールに記載された趣旨をご理解の上、中小企業へのセキュリティ個別指導にご活用ください。

マネジメント指導の流れ



# セキュリティマネジメント指導ツールの構成

- セキュリティマネジメント指導の5つの指導テーマについて、主にIPAの「**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**」を活用した3回の標準的な訪問指導内容（**標準シラバス**）を設定し、指導先企業の依頼・調整事項や指導にあたっての基本的な留意点を説明する「**実施要領**」を作成しました。
- 「実施要領」には、各回ごとの指導の内容（標準的な進め方）に加えて、指導に当たっての留意点を記載し、**使用するツール/資料の活用方法**を記載した、実践的なノウハウを提供する内容としています。

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

# 【参考】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

- 中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドラインです。
- ガイドラインは、中小企業の情報セキュリティ対策の考え方や実践方法について、本編２部と付録より構成されています。

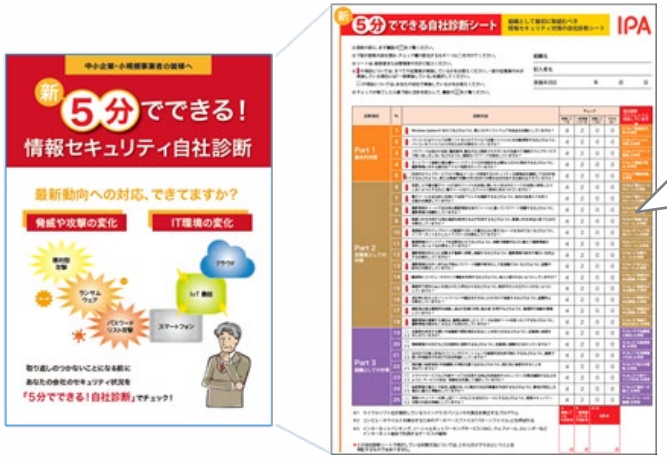
| 構　成 | | 概　要 |
|---|---|---|
| 本編 | 第１部　経営者編 | 経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。 |
| 本編 | 第２部　実践編 | 情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。 |
| 付録 | 付録１　情報セキュリティ５か条 | 組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。 |
| 付録 | 付録２　情報セキュリティ基本方針（サンプル） | 組織としての情報セキュリティに対する基本方針書のサンプルです。 |
| 付録 | 付録３　５分でできる！情報セキュリティ自社診断 | あまり費用をかけることなく実行することで効果がある25 項目のチェックシートです。 |
| 付録 | 付録４　情報セキュリティハンドブック（ひな形） | 従業員に対して対策内容を周知するために作成するハンドブックのひな形です。 |
| 付録 | 付録５　情報セキュリティ関連規程（サンプル） | 情報セキュリティに関する社内規則を文書化したもののサンプルです。 |
| 付録 | 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 | クラウドサービスを安全に利用するための手引きです。15 項目のチェックシートが付いています。 |
| 付録 | 付録７　リスク分析シート | 情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。 |
| 付録 | 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 | 情報漏えいやシステム停止などのインシデント対応のための手引きです。 |

セキュリティマネジメント指導ツール

# 事前の準備

# 「5分でできる！情報セキュリティ自社診断」

- 第１回目の訪問指導の事前準備として、指導先企業へIPAが提供する「**5分でできる！情報セキュリティ自社診断**」の実施を依頼の上、診断結果を共有します。
- 第１回目指導後に、診断結果やヒアリング情報をもとに、**指導先企業の現状のセキュリティ対策や取組み状況についての分析**を改めて行います。
- 第２回目の指導時には、診断項目について「なぜそのように評価したか」、「例外はないか」などを掘り下げ、課題の抽出を進めます。重点改善領域と思われる項目を提示し、緊急度・重要度・難易度などの視点から、対策の優先順位付けについてディスカッションを行います。




**自社診断のための25項目**

**●基本的対策（5項目）**
脆弱性対策、ウイルス対策、
パスワード強化など

**●従業員としての対策（13項目）**
標的型攻撃メール、電子メール、ウェブ利用、
持ち出し、廃棄など

**●組織としての対策（7項目）**
守秘義務、教育、委託先管理、ルール化など

※　Excelファイルをそのまま、または印刷して実施してください。Excelファイルは、IPA Webサイトからダウンロードが可能です。
https://www.ipa.go.jp/security/guide/sme/5minutes.html

# 自社診断実施の留意点（自社診断結果）

| 項目No. | | 診断内容 | 掘り下げるチェックポイント（例） |
|---|---|---|---|
| 基本的対策 | 1 | パソコンやスマホなど、情報機器のOSやソフトウェアは常に最新の状態にしていますか？ | ①. 状況を管理する担当者は決まっているか<br>②. 業務外のソフトウェアが勝手に導入されてないか<br>③. 従業員に、どのように徹底できているか |
| | 2 | パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？ | ①. すべてのパソコンの更新レベルが把握できているか<br>②.「社長、役員は別」などの例外的な取り扱いはないか<br>③. 管理者／使用者がはっきりしないパソコンは無いか |
| | 3 | パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？ | ①. 従業員に、どのように徹底できているか<br>②. 例外的に認められていることは無いか |
| | 4 | 重要情報※2 に対する適切なアクセス制限を行っていますか？ | ①. 初期設定のままになっている機器はないか<br>②. 設定内容を定期的にチェックしているか<br>③. 例外的に認められていることは無いか |
| | 5 | 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？ | ①. 利用中のウェブサービスの棚卸しができているか<br>②. 注意喚起が迅速にできる仕組みが整っているか<br>③. セミナーなどの外部の情報も共有できているか |

※1　コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。
※2　重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や、従業員の個人情報など管理責任を伴う情報のことです。

チェックの判断根拠を十分に掘り下げることで、身の丈に合った有効な対策に絞り込みます

# 当日タイムスケジュールの提示

- 訪問指導当日の具体的な進行は、指導先企業の状況を踏まえて進めます。
  ⇒ 対面でのQ&A方式、ワークショップ方式、グループ討議方式等、状況に即した方式を設定します。
  ⇒ 状況によっては、訪問をせずにWeb会議で指導を行うこともあり得ます。
- 各回とも半日（２～３時間程度）の限られた時間ですので、効率的に進行します。
  ⇒ 可能な限り事前に、当日のタイムスケジュールをセキュリティ専門家から提示します。

＜当日タイムスケジュール（例）＞

| 初回の例 | 時間 | 項目 | 考慮点 |
|---|---|---|---|
| 13:30-13:40 | 10分 | *自己紹介と当事業内容全体の説明/確認<br>*当日の進め方と準備資料についての説明と合意<br>*情報の取り扱い | セキュリティマネジメント指導の目的と、目標とする成果物を明確に伝える |
| 13:40-14:40 | 60分 | *企業の事業（業務）内容と情報システム環境の理解 | 企業ホームページ等での事前確認を踏まえて、効率的にヒアリングを進める |
| 14:40-14:50 | 10分 | 休憩 | |
| 14:50-15:30 | 40分 | *情報セキュリティ自社診断結果の確認<br>(事前準備できてない場合はその場で実施) | 自社診断の実施者自身のコメントを確認する(経営者、従業員それぞれの視点で) |
| 15:30-16:10 | 40分 | *情報セキュリティに関する今回の指導を通じての経営者の期待値の理解　⇒IPAの映像コンテンツの投影も交えて行う | IPA映像コンテンツの解説を行うと共に、企業側の現状や経営者の意向を確認していく |
| 16:10-16:20 | 10分 | *追加で必要となる情報の提供依頼 | 第2回の準備作業に間に合うように、できる限り早めの対応を依頼する |
| 16:20-16:30 | 10分 | *全体を通してのQ&A<br>*次回以降の日程と準備事項の確認 | 第2回目の冒頭で前回の振り返りを行う |

# 指導先企業への依頼や調整事項

- 指導を円滑に進めるため、指導先企業へ依頼する事項を予め伝えておき、調整が必要な事項の有無を明らかにしておきます。

＜指導先企業への確認・調整依頼事項＞

| | 確認・調整事項 | 依頼のポイント |
|---|---|---|
| 1 | 企業の検討体制(参加メンバー)等の調整 | ✓ 経営層に加え、以下の現場のリーダー層～課長クラスに参加いただくことを推奨します。<br>・事業や業務のプロセスに詳しい方<br>・ITシステムの運用管理を担っている方 |
| 2 | 打ち合わせ場所や環境の確認/準備 | ✓ 会議室/プロジェクター等の環境確認/準備をお願いします。<br>・映像コンテンツの投影や、ディスカッションの効率に大きな影響があります。 |
| 3 | 指導環境の調整（コミュニケーション環境） | ✓ 原則として訪問による現地指導を行いますが、初回を除く2回目以降で訪問と同等の指導がオンラインでも可能であることが見込まれ、かつ指導企業が合意した場合に、オンラインによる指導を行う場合もあります。 |
| 4 | 提供を受ける情報の取り扱い | ✓ 指導企業にいただいた情報は、専門家において取り扱いに留意します。 |

## セキュリティマネジメント指導ツール

# テーマ①｜情報セキュリティ規程の整備

# 指導業務の達成目標と成果物

➢「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・助言を行います。

## マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

【達成目標１】現状における自社の情報セキュリティリスクの洗い出し
【達成目標２】情報セキュリティ基本方針の作成及び既存規程のチェック
【達成目標３】情報セキュリティ関連規程（案）の策定

注：成果物

取組みスタート

達成目標1

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

達成目標2

● 情報セキュリティ基本方針
● 情報セキュリティ関連規程類の点検結果

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

達成目標3

● 情報セキュリティ関連規程

情報セキュリティ関連規程（サンプル）

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

継続実施

# 各回ごとの指導の内容（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
*情報セキュリティ関連規程に関するチェックシートの作成依頼

**第１回**

**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**

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、企業側セルフチェックシートに基づきヒアリングを行い、当該企業における情報セキュリティ規程のうち改善すべき点や追加作成すべきもの等について指摘・指導します。

2～3週間

**事前準備＃２**

*前回の指導を通じて得た情報をもとにした改善領域の見極め
*現行の基本方針や規程類の問題点確認、修正案作成

**第２回**

**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**

指導先企業が作成した新規程案についてチェックするとともに、企業が策定時に苦労した点や疑問に思った点等について質問を受け付け、アドバイスします。また、不十分な点があれば指摘し、再度修正・作成の指示を出します。

2～3週間

**事前準備＃３**

*前回結果に加え、経営施策に対する情報セキュリティリスクの検討
*従業員への周知計画を含む適切な運用方法案作成

**第3回**

**新規程の運用方法の確認**

新規程の運用案について確認し、適切なアドバイスを行います。作成に際し企業側で生じた疑問や質問等に回答・アドバイスします。また、重点対策と合わせた今後の実行計画を検討するとともに、企業側で作成した基本方針や規程の見直し案について、マネジメントシステムの実効性の視点からレビューを行います。

計2.0ヶ月程度

# 使用するツール/資料の内容（基本方針サンプル）

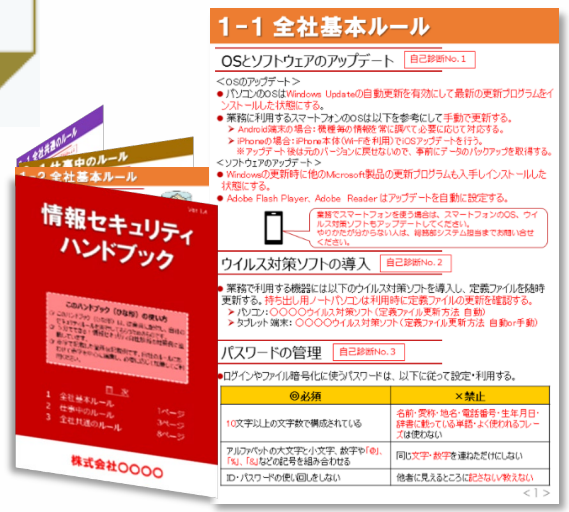
- 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」にひな形となるWORDファイルが付録されています。
  サンプルをもとに情報セキュリティ基本方針を作成します（既に作成されたものがあれば、内容に不備・不足が無いか確認）。
  ⇒ https://www.ipa.go.jp/security/guide/sme/about.html
  ⇒ 情報セキュリティ基本方針

**情報セキュリティ基本方針の記載項目例**

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

- 「情報セキュリティに関する基本方針」の作成後は、従業員や関係者に文書等で周知・徹底を図ります。

- 基本方針を盛り込んだ「情報セキュリティハンドブック」を作成し、配布することも有効です。



# 使用するツール/資料の内容（関連規程サンプル）

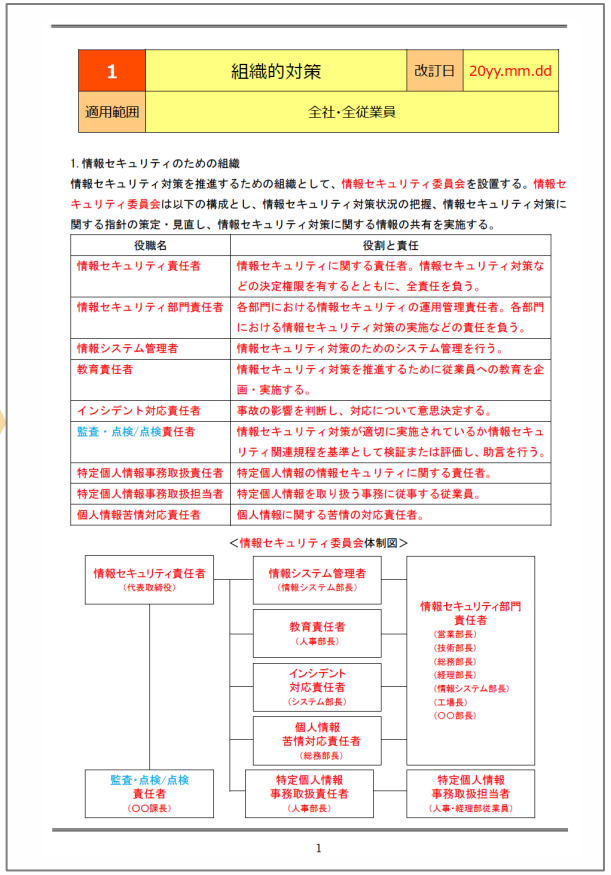
- サンプル規程をもとに、企業独自の情報セキュリティ関連規程（案）を策定します。
  - 中小企業の情報セキュリティ対策ガイドライン 付録２ 情報セキュリティ基本方針（サンプル）
  - 同 付録５ 情報セキュリティ関連規程（サンプル）または 自動車産業向け情報セキュリティ関連規程（サンプル）

【表８】情報セキュリティ管理のための役割と責任分担（例）

| 役職名 | 役割と責任 |
|---|---|
| 情報セキュリティ責任者 | 情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。 |
| 情報セキュリティ部門責任者 | 各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。 |
| システム管理者 | 情報セキュリティ対策のためのシステム管理を行います。 |
| 教育責任者 | 情報セキュリティ対策を推進するために従業員への教育を企画・実施します。 |
| 点検責任者 | 情報セキュリティ対策が適切に実施されているか点検します。 |

【表９】緊急時対応体制の役割と責任（例）

| 役職名 | 役割と責任 |
|---|---|
| 情報セキュリティ責任者<br>（例：代表取締役） | 事故の影響を判断し、対応について意思決定する。 |
| 情報セキュリティ部門責任者<br>（例：管理部長、営業部長） | ・事故の原因を調べて情報セキュリティ責任者に報告する。<br>・情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行う。<br>・事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行う。 |
| システム管理者<br>（例：管理部長兼務） | 事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行う。 |
| 事故・異常を発見した従業員 | 事故や異常の内容を情報セキュリティ部門責任者に報告する。 |



| 1 | 組織的対策 | 改訂日 | 20yy.mm.dd |
|---|---|---|---|
| 適用範囲 | 全社・全従業員 | | |

1. 情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

| 役職名 | 役割と責任 |
|---|---|
| 情報セキュリティ責任者 | 情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。 |
| 情報セキュリティ部門責任者 | 各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。 |
| 情報システム管理者 | 情報セキュリティ対策のためのシステム管理を行う。 |
| 教育責任者 | 情報セキュリティ対策を推進するために従業員への教育を企画・実施する。 |
| インシデント対応責任者 | 事故の影響を判断し、対応について意思決定する。 |
| 監査・点検/点検責任者 | 情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。 |
| 特定個人情報事務取扱責任者 | 特定個人情報の情報セキュリティに関する責任者。 |
| 特定個人情報事務取扱担当者 | 特定個人情報を取り扱う事務に従事する従業員。 |
| 個人情報苦情対応責任者 | 個人情報に関する苦情の対応責任者。 |

<情報セキュリティ委員会体制図>



1

## 情報セキュリティ規程の作成

**付録5「情報セキュリティ関連規程（サンプル）」（全11規程）を参考に、自社に適した規程にするために修正を加える**

- サンプル文中の赤字、青字部分を**自社向けに修正**すれば、自社の情報セキュリティ規程が完成
- サンプルに明記されていなくても**必要な対策や有効な対策**があれば**追記**

# 【参考】情報セキュリティ関連規程（サンプル）の項目

## ◇情報セキュリティ関連規程（サンプル）

| | 名称 | 概要 | 項目 |
|---|---|---|---|
| 1 | 組織的対策 | 情報セキュリティのための管理体制の構築や点検、情報共有などのルール | 1.情報セキュリティのための組織<br>2.情報セキュリティ取組みの監査・点検/点検<br>3.情報セキュリティに関する情報共有 |
| 2 | 人的対策 | 取締役及び従業員の責務や教育、人材育成などのルール | 1.雇用条件<br>2.従業員の責務<br>3.雇用の終了<br>4.情報セキュリティ教育<br>5.人材育成 |
| 3 | 情報資産管理 | 情報資産の管理や持ち出し方法、バックアップ、破棄などのルール | 1.情報資産の管理<br>2.情報資産の社外持ち出し<br>3.媒体の処分<br>4.バックアップ |
| 4 | アクセス制御及び認証 | 情報資産に対するアクセス制御方針や認証のルール | 1.アクセス制御方針<br>2.利用者の認証<br>3.利用者アカウントの登録<br>4.利用者アカウントの管理<br>5.パスワードの設定<br>6.従業員以外の者に対する利用者アカウントの発行<br>7.端末の識別による認証<br>8.端末のタイムアウト機能<br>9.標準設定等 |
| 5 | 物理的対策 | セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルール | 1.セキュリティ領域の設定<br>2.関連設備の管理<br>3.セキュリティ領域内注意事項<br>4.搬入物の受け渡し |
| 6 | IT機器利用 | IT機器やソフトウェアの利用などのルール | 1.ソフトウェアの利用<br>2.ＩＴ機器の利用<br>3.クリアデスク・クリアスクリーン<br>4.インターネットの利用<br>5.私有ＩＴ機器・電子媒体の利用<br>6.標準等 |
| 7 | IT基盤運用管理 | サーバーやネットワーク等のITインフラに関するルール | 1.管理体制<br>2.ＩＴ基盤の情報セキュリティ対策<br>3.ＩＴ基盤の運用<br>4.クラウドサービスの導入<br>5.脅威や攻撃に関する情報の収集<br>6.廃棄・返却・譲渡<br>7.ＩＴ基盤の情報セキュリティ要件及び標準 |

# 【参考】情報セキュリティ関連規程（サンプル）の項目（続き）

## ◇情報セキュリティ関連規程（サンプル）

| | 名称 | 概要 | 項目 |
|---|---|---|---|
| 8 | システム開発及び保守 | 独自に開発及び保守を行う情報システムに関するルール | 1.新規システム開発・改修<br>2.脆弱性への対処<br>3.情報システムの開発環境<br>4.情報システムの保守<br>5.情報システムの変更 |
| 9 | 委託管理 | 業務委託にあたっての選定や契約、評価のルール（委託先チェックリストのサンプルが付属） | 1.委託先評価基準<br>2.委託先の選定<br>3.委託契約の締結<br>4.委託先の評価<br>5.再委託 |
| 10 | 情報セキュリティインシデント対応及び事業継続管理 | 情報セキュリティに関する事故対応や事業継続管理などのルール | 1.対応体制<br>2.情報セキュリティインシデントの影響範囲と対応者<br>3.インシデントの連絡及び報告<br>4.対応手順<br>5.届出及び相談<br>6.情報セキュリティインシデントによる事業中断と事業継続管理<br>7.事業継続計画 |
| 11 | テレワークにおける対策 | テレワークのセキュリティ対策についてのルール | 1.テレワーク共通ルール<br>2.情報機器のセキュリティ<br>3.ネットワーク機器のセキュリティ：テレワークのネットワーク環境<br>4.勤務中のルール<br>5.データ・書類の保存<br>6.社内問い合わせ・緊急連絡先 |

# 使用するツール/資料の内容（関連規程チェックシート）

- 関連規程を点検する上で、サンプル規程の項目ごとにチェックが可能な点検シートを提供しています。
- 既存の規程や各種運用規則等との不整合、スコープの違い等について確認してください。あまり細部にこだわりすぎないようにしてください。全体像の把握ができる程度で構いません。

## ＜情報セキュリティ規程チェックシート（抜粋）＞

| No1 | 項目 | No2 | チェック項目（大） | No3 | チェック項目（中） | No4 | チェック項目（細） | 項目の有無チェック | 既存規程における条文・ページ番号等 | 既存規程において課題であると考えられるポイント（規程のスコープ（対象範囲）の不整合など） |
|---|---|---|---|---|---|---|---|---|---|---|
| 記入例 | 情報資産管理 | - | 情報資産の管理 | 1.1 | 情報資産の特定と機密性の評価 | | | 有 | p.5｜1.情報資産の管理｜1.1情報資産の特定と機密性の評価 | 情報資産管理の範囲が全社的に位置づけられていない。 |
| 1 | 組織的対策 | 1 | 情報セキュリティのための組織 | | | | | | | |
| | | 2 | 情報セキュリティ体制図 | | | | | | | |
| | | 3 | 情報セキュリティ取り組みの監査・点検／点検 | | | | | | | |
| | | 4 | 情報セキュリティに関する情報共有 | | | | | | | |
| 2 | 人的対策 | 1 | 雇用条件 | | | | | | | |
| | | 2 | 従業員の責務 | | | | | | | |
| | | 3 | 雇用の終了 | | | | | | | |
| | | 4 | 情報セキュリティ教育 | | | | | | | |
| | | 5 | 人材育成 | | | | | | | |
| 3 | 情報資産管理 | 1 | 情報資産の管理 | 1.1 | 情報資産の特定と機密性の評価 | | | | | |
| | | | | 1.2 | 情報資産の分類の表示 | | | | | |
| | | | | 1.3 | 情報資産の管理責任者 | | | | | |
| | | | | 1.4 | 情報資産の利用者 | | | | | |

セキュリティマネジメント指導ツール

# テーマ②｜情報資産の洗い出しとリスク分析

# 指導業務の達成目標と成果物

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

## マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

【達成目標１】現状における自社の情報セキュリティリスクの洗い出し
【達成目標２】自社における情報資産の洗い出し
【達成目標３】抽出した情報資産リストに対するリスク分析の実施

注：成果物

取組みスタート

達成目標1

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

達成目標2

● 社内における情報資産の洗い出し

達成目標3

● 情報資産に対するリスク分析実施

継続実施

| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 個人情報の種類 | | | 評価値 | | | 重要度 | 保存期限 | 登録日 | 現状から想定されるリスク（入力不要・自動表示） | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 個人情報 | 要配慮個人情報 | 特定個人情報 | 機密性 | 完全性 | 可用性 | | | | 脅威の発生頻度 ※「脅威の状況」シートに入力すると表示 | 脆弱性 ※「対策状況チェック」シートに入力すると表示 | 被害発生可能性 | リスク値 |
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | 事務所PC | 有 | | | 3 | 1 | 1 | 3 | | 2023/4/1 | 3:通常の状態で脅威が発生する（いつ発生してもおかしくない） | 2:部分的に対策を実施している | 2 | 可能性：中 6 リスク大 |
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | 書類 | 有 | | | 3 | 3 | 3 | 3 | | 2023/4/1 | 2:特定の状況で脅威が発生する（年に数回程度） | 2:部分的に対策を実施している | 1 | 可能性：低 3 リスク小 |
| 人事 | 健康診断の結果 | 雇入時・定期健康診断 | 人事部 | 人事部 | 書類 | | 有 | | 3 | 3 | 2 | 3 | 5年 | 2023/4/1 | 2:特定の状況で脅威が発生する（年に数回程度） | 2:部分的に対策を実施している | 1 | 可能性：低 3 リスク小 |
| 経理 | 給与システムデータ | 税務署提出用源泉徴収票 | 給与計算担当 | 人事部 | 事務所PC | | | 有 | 3 | 3 | 2 | 3 | 7年 | 2023/4/1 | 3:通常の状態で脅威が発生する（いつ発生してもおかしくない） | 2:部分的に対策を実施している | 2 | 可能性：中 6 リスク大 |

# 各回ごとの指導の内容（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
*「リスク分析シート」における情報資産洗い出し作業の実施依頼

**第１回**

**社内情報資産の洗い出し**

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、企業側が作成した分析シートに基づきヒアリングを行い、必要に応じ加筆修正指示を行います。

2～3週間

**事前準備# 2**

*前回の指導を通じて得た情報をもとにリスク分析を実施
*特に「リスク大」と評価された資産に対するリスク低減策や回避策について検討

**第２回**

**社内情報資産のリスク値の算定**

指導先企業側が作成した分析シートに基づきヒアリングを行い、必要に応じ加筆修正指示を行うとともに、企業側が示したリスク回避策や低減策についてアドバイスを行います。また、継続的な運用方法の考え方について指南します。

2～3週間

**事前準備# 3**

*リスク評価案に対する見直しを実施
*リスクの大小に応じて、それぞれ低減策や回避策を検討しFIXさせる

**第3回**

**社内情報資産に対する情報セキュリティ対策等運用方法の検討**

企業側が作成したリスク評価案及び運用方法（実施計画案）についてチェック・レビューを行います。

計2.0ヶ月程度

# 使用するツール/資料の内容（リスク分析シート）

- 「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」の付録7「リスク分析シート」をもとに、社内での情報資産の洗い出し及びそれらに対するリスク分析を実施します。
  ⇒ https://www.ipa.go.jp/security/guide/sme/about.html
- リスク分析結果をもとに、今後の社内での情報セキュリティ対策を見直します。

**情報資産の洗い出し**
どのような情報資産があるか洗い出して重要度を判断する

**リスク値の算定**
優先的・重点的に対策が必要な情報資産を把握する

**情報セキュリティ対策の決定**
リスクの大きな情報資産に対して必要とされる対策を決める

| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 個人情報の種類 | | | 評価値 | | | 重要度 | 保存期限 | 登録日 | 現状から想定されるリスク（入力不要・自動表示） | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 個人情報 | 要配慮個人情報 | 特定個人情報 | 機密性 | 完全性 | 可用性 | | | | 脅威の発生頻度 ※「脅威の状況」シートに入力すると表示 | 脆弱性 ※「対策状況チェック」シートに入力すると表示 | 被害発生可能性 | | リスク値 | |
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | 事務所PC | 有 | | | 3 | 1 | 1 | **3** | | 2023/4/1 | 3:通常の状態で脅威が発生する（いつ発生してもおかしくない） | 2:部分的に対策を実施している | 2 | 可能性：中 | 6 | リスク大 |
| 人事 | 社員名簿 | 社員基本情報 | 人事部 | 人事部 | 書類 | 有 | | | 3 | 3 | 3 | **3** | | 2023/4/1 | 2:特定の状況で脅威が発生する（年に数回程度） | 2:部分的に対策を実施している | 1 | 可能性：低 | 3 | リスク小 |
| 人事 | 健康診断の結果 | 雇入時・定期健康診断 | 人事部 | 人事部 | 書類 | | 有 | | 3 | 3 | 2 | **3** | 5年 | 2023/4/1 | 2:特定の状況で脅威が発生する（年に数回程度） | 2:部分的に対策を実施している | 1 | 可能性：低 | 3 | リスク小 |
| 経理 | 給与システムデータ | 税務署提出用源泉徴収票 | 給与計算担当 | 人事部 | 事務所PC | | | 有 | 3 | 3 | 2 | **3** | 7年 | 2023/4/1 | 3:通常の状態で脅威が発生する（いつ発生してもおかしくない） | 2:部分的に対策を実施している | 2 | 可能性：中 | 6 | リスク大 |

付録７「リスク分析シート」

# 成果物作成の留意点（情報資産管理台帳の作成）

- 社内の情報資産を洗い出し、情報資産管理台帳（リスク分析シート）を作成します。

  - **情報資産**

    営業秘密など事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報など管理責任を伴う情報

  - **情報資産管理台帳**

    情報資産管理台帳は洗い出した情報資産を「見える化」するための方法

| 業務分類 | 情報資産名称 | 備考 | 利用者範囲 | 管理部署 | 媒体・保存先 | 個人情報の種類 | | | 保存期限 | 登録日 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | 個人情報 | 要配慮個人情報 | 特定個人情報 | | |
| | | | 事部 | 人 部 | | 有 | | | | |
| | | | 人事部 | 部 | | 有 | | | | |
| 人事 | 健康診断の結果 | 雇入時・定 | 部 | | 頭 | | 有 | | | 23/4/1 |
| 経理 | 給与システムデータ | 税務署源泉徴収票 | 算当 | | PC | | | 有 | | 23/4/1 |

情報資産に関連する業務や部署名を記入

情報資産の内容を簡潔に記入

必要に応じて説明等を記入

情報資産を利用してよい部署等を記入

情報資産の管理責任がある部署等を記入

情報資産の媒体や保存場所を記入

個人情報の有無を記入

情報資産の保存期間を記入

情報資産の登録日を記入

- 情報資産洗い出しに際しては、日常どのような電子データや書類を利用して業務を行っているかを考えて洗い出すと、作成しやすくなります。

# 成果物作成の留意点（機密性・完全性・可用性の評価）

- 機密性、完全性、可用性が損なわれた場合の事業への影響や法律で安全管理義務があるなど、右の評価基準を参考に評価値３～１を記入する

✓ **機密性（Confidentiality）**
アクセスを許可された者だけが情報にアクセスできる

✓ **完全性（Integrity）**
情報や情報の処理方法が正確で完全である

✓ **可用性（Availability）**
許可された者が必要な時に情報資産にアクセスできる

**【表12】情報資産の機密性・完全性・可用性に基づく重要度の定義**

| 評価値 | | 評価基準 | 該当する情報の例 |
|---|---|---|---|
| **機密性**<br>アクセスを許可された者だけが情報にアクセスできる | 3 | 法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている | ●個人情報（個人情報保護法で定義）<br>●特定個人情報（マイナンバーを含む個人情報） |
| | | 守秘義務の対象や限定提供データ[12]として指定されている<br>漏えいすると取引先や顧客に大きな影響がある | ●取引先から秘密として提供された情報<br>●取引先の製品・サービスに関わる非公開情報 |
| | | 自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため）<br>漏えいすると自社に深刻な影響がある | ●自社の独自技術・ノウハウ<br>●取引先リスト<br>●特許出願前の発明情報 |
| | 2 | 漏えいすると事業に大きな影響がある | ●見積書、仕入価格など顧客（取引先）との商取引に関する情報 |
| | 1 | 漏えいしても事業にほとんど影響はない | ●自社製品カタログ<br>●ホームページ掲載情報 |
| **完全性**<br>情報や情報の処理方法が正確で完全である | 3 | 法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている | ●個人情報（個人情報保護法で定義）<br>●特定個人情報（マイナンバーを含む個人情報） |
| | | 改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある | ●取引先から処理を委託された会計情報<br>●取引先の口座情報<br>●顧客から製造を委託された設計図 |
| | 2 | 改ざんされると事業に大きな影響がある | ●自社の会計情報<br>●受発注・決済・契約情報<br>●ホームページ掲載情報 |
| | 1 | 改ざんされても事業にほとんど影響はない | ●廃版製品カタログデータ |
| **可用性**<br>許可された者が必要な時に情報資産にアクセスできる | 3 | 利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある | ●顧客に提供しているEC サイト<br>●顧客に提供しているクラウドサービス |
| | 2 | 利用できなくなると事業に大きな影響がある | ●製品の設計図<br>●商品・サービスに関するコンテンツ（インターネット向け事業の場合） |
| | 1 | 利用できなくなっても事業にほとんど影響はない | ●廃版製品カタログ |

12 ▲限定提供データ 不正競争防止法で次のように定義されています。「第二条 7 この法律において「限定提供データ」とは、業として特定の者に提供する情報として電磁的方法（電子的方法、磁気的方法その他人の知覚によっては認識することができない方法をいう。次項において同じ。）により相当量蓄積され、及び管理されている技術上又は営業上の情報（秘密として管理されているものを除く。）をいう。」

# 成果物作成の留意点（重要度の算定）

- 重要度は、機密性、完全性、可用性いずれかの最大値で判断する

| 判断基準 | 重要度 |
|---|---|
| 機密性・完全性・可用性評価値のいずれかまたはすべてが「3」の情報資産 | 3 |
| 機密性・完全性・可用性評価値のうち最大値が「2」の情報資産 | 2 |
| 機密性・完全性・可用性評価値すべてが「1」の情報資産 | 1 |

- 重要度の判断例

●『独自技術に基づいた設計図』(書類)

**機密性**：主力製品の設計図であり、流出すると他社との差別化ができなくなり、売上が減少する …… 評価＝3

**完全性**：改ざんや無断の変更があると、製造に支障がある…… 評価＝2

**可用性**：原本のCADデータはサーバーに保存してあり、必要なときに閲覧や再印刷が可能なので、利用できなくなっても困ることはない…… 評価＝1

情報資産管理台帳　重要度欄

| 評価値 | | | 重要度 |
|---|---|---|---|
| 機密性 | 完全性 | 可用性 | |
| 3 | 2 | 1 | 3 |

機密性の3が最大値なので重要度は3

●『自社のホームページ』(電子データ)

**機密性**：公開しているホームページであり、クレジットカード情報など機密情報の保存はしていない …… 評価＝1

**完全性**：不正アクセスで価格が改ざんされたり、ウイルスが仕掛けられると顧客や閲覧者に被害が発生し、信用を失う…… 評価＝3

**可用性**：サーバーの障害などでアクセスできなくなると、来店客が減少し、売上も減少する …… 評価＝3

情報資産管理台帳　重要度欄

| 評価値 | | | 重要度 |
|---|---|---|---|
| 機密性 | 完全性 | 可用性 | |
| 1 | 3 | 3 | 3 |

完全性と可用性の3が最大値なので重要度は3

# 成果物作成の留意点（リスク値算定の全体イメージ）

| 重要度 | | 情報資産の価値・事故の影響の大きさ |
|---|---|---|
| | 3 | 事故が起きると<br>● 法的責任を問われる<br>● 取引先、顧客、個人に大きな影響がある<br>● 事業に深刻な影響を及ぼす<br>など企業の存続を左右しかねない |
| | 2 | 事故が企業の事業に重大な影響を及ぼす |
| | 1 | 事故が発生しても事業にほとんど影響はない |

× 掛け算

算定のしかたは**右図**参照

| | | 起こりやすさ |
|---|---|---|
| 脅威 | 3 | 通常の状況で脅威が発生する（いつ発生してもおかしくない） |
| | 2 | 特定の状況で脅威が発生する（年に数回程度） |
| | 1 | 通常の状況で脅威が発生することはない |

| | | つけ込みやすさ |
|---|---|---|
| 脆弱性 | 3 | 対策を実施していない（ほぼ無防備） |
| | 2 | 部分的に対策を実施している |
| | 1 | 必要な対策をすべて実施している |

| 被害発生可能性 | | |
|---|---|---|
| | 3高 | 通常の状況で被害が発生する（いつ発生してもおかしくない） |
| | 2中 | 特定の状況で被害が発生する（年に数回程度） |
| | 1低 | 通常の状況で被害が発生することはない |

| リスク値 | | |
|---|---|---|
| | 9～6 大 | 深刻な事故が起きる可能性大 |
| | 4 中 | 重大な事故が起きる可能性有 |
| | 3～1 小 | 事故が起きる可能性小、起きても被害は受容範囲 |

重要度は3～1の数値、被害発生可能性、脅威、脆弱性は3～1の数値、リスク値は算定結果を大・中・小で表す

| 脅威 ＼ 脆弱性 | 3 | 2 | 1 |
|---|---|---|---|
| 3 | 3 | 2 | 1 |
| 2 | 2 | 1 | 1 |
| 1 | 1 | 1 | 1 |

計算式　脅威÷（4－脆弱性）
（小数第1位を切り上げ）

# 成果物作成の留意点（リスク対応方法の検討）

- リスク値の算定により、優先的・重点的に対策が必要な情報資産に対して、リスクが事業に与える影響を考慮した上で、**リスクの対応方法**を検討し、**情報セキュリティ対策**を決定する

| リスク対応方法 | 内容 | 対応例 |
|---|---|---|
| ①低減する | 脆弱性に対して情報セキュリティ対策を講じることにより、**脅威の発生可能性を下げる** | マルウェア対策ソフトを導入する、外部記憶媒体の接続を制限する等 |
| ②保有する | リスクが事業に与える影響小さい、あるいは対策にかかる費用が損害額を上回る場合などは、**対策を講じず許容範囲内として現状を維持**する。 | （対策を講じた後に残ったリスク、および対策されずに残ったリスクは、**残留リスク**とも言われる） |
| ③回避する | 脅威発生の要因を停止あるいは全く別の方法に変更することで、**リスクが発生する可能性を取り去る**。 | 外部からの不正アクセスという脅威に対し、機密情報が保存されているサーバは外部接続を行わないこと等 |
| ④移転する | 自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで**自社の負担を下げる**。 | 社内サーバをセキュリティ対策の充実した外部クラウドサービスに移行する、情報セキュリティに関連した保険商品に加入する等 |

セキュリティマネジメント指導ツール

# テーマ③｜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

# 指導業務の達成目標と成果物

➢「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・助言を行います。

## マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

【達成目標１】現状における自社の情報セキュリティリスクの洗い出し
【達成目標２】自社における現状導入済み/利用予定クラウドサービスの洗い出し
【達成目標３】抽出したクラウドサービスに対する安全利用チェック

注：成果物

取組みスタート

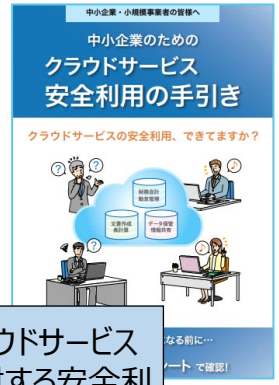
達成目標１

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

達成目標２

● 社内におけるクラウドサービスの洗い出し

達成目標３




● クラウドサービスに対する安全利用チェック実施

継続実施

| 管理番号 | サービス名 | 所管部署 | サービスの概要 | ステータス | サービス利用開始日 | サービス利用終了（予定）日 | 利用業務の明確化ステータス | 他社との比較 | 取り扱う情報の重要度 | 社内ポリシとの適合性チェック | クラウド事業者の信頼性チェック | サービスの安全性・信頼性チェック | 管理担当者氏名 | 利用範囲チェック | 利用者認証チェック | データバックアップ状況 | サービス付帯のセキュリティ対策 | 利用者サポート体制 | 利用終了時のデータの取り扱い | 証明書、契約書、規約書 | データの地理的保存先チェック | 総合評価 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | I．サービス選択時のポイント | | | | | | II．サービス運用時のポイント | | | | | III．セキュリティ管理のポイント | | | | |
| S0001 | ○○オンラインストレージサービス | 営業部 | 外部顧客との営業関係書類受け渡し用 | 利用中 | 2024/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | 確認中 | すべて確認済（約款添付） | 所当者アサイン済 | すべて管理できている | すべて管理できている | 一部管理できている | すべて具体的に公開されている | ヘルプデスクあり | 確認した | 確認した | 未確認 | 37 |
| S0002 | △△クラウド財務会計v2 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用中 | 2023/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | わからない | わからない | 所当者アサイン済 | すべて管理できている | すべて管理できている | 一部管理できている | わからない | ヘルプデスクあり | 確認した | わからない | 未確認 | 26 |
| S0003 | ××総合管理WEBシステム | 総務部 | 所内労務管理 | 利用中 | 2023/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | わからない | わからない | 所当者アサイン済 | すべて管理できている | すべて管理できている | 一部管理できている | わからない | ヘルプデスクあり | 確認した | 確認した | 未確認 | 29 |
| S0004 | □□ECプラットフォーム | 営業部 | オンライン通販システム | 調査中 | 未定 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | わからない | わからない | 所当者アサイン済 | 一部管理できている | 一部管理できている | 未確認 | わからない | わからない | わからない | わからない | 未確認 | 17 |
| S0005 | △△クラウド財務会計v1 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用終了 | 2020/4/1 | 2024/3/31 | 一部明確化できている | 確認中 | 確認した | わからない | わからない | わからない | 未了 | 未確認 | 未確認 | 未確認 | わからない | わからない | わからない | わからない | わからない | 11 |
| | | | | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | |

# 各回ごとの指導の内容（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
*「クラウドサービス台帳」における既存/予定クラウドサービス洗い出し作業の実施依頼

第１回

**既存及び検討中クラウドサービスの洗い出し**

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、企業側が作成したクラウドサービス台帳に基づきヒアリングを行い、必要に応じ加筆修正指示を行います。

2～3週間　事前準備#２

*前回の指導を通じて得た情報をもとにチェックを実施
*特に「チェックが十分でない」と評価されたクラウドサービスに対するリスク低減策や回避策について検討
*社内運用に向けて、当該企業用のクラウドサービス利用ガイドライン案及び安全利用チェックシートの案を作成

第２回

**チェックシートに基づく、クラウドサービスのリスク評価**

企業側が作成したチェックシート及びガイドライン案に基づきヒアリングを行い、必要に応じ加筆修正指示を行うとともに、企業側が示したリスク回避策や低減策についてアドバイスを行います。また、継続的な運用方法の考え方について指南します。

2～3週間　事前準備#３

*各サービスの安全利用チェックについて引き続き検討
*社内運用に向けて、周知の方法や運用プランを策定

第3回

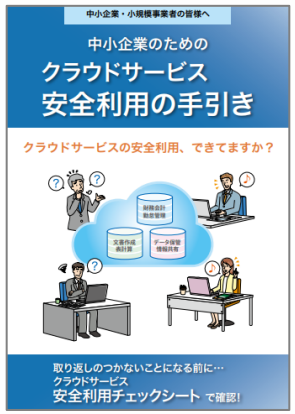
**チェックシートに基づく、クラウドサービスのリスク評価（継続）**

引き続き、企業側が作成したチェックシート及びガイドライン案に基づきヒアリングを行い、必要に応じ加筆修正指示を行うとともに、企業側が示したリスク回避策や低減策についてアドバイスを行います。また、継続的な運用方法の考え方について指南します。
また、以後の継続運用に際してのアドバイスも行います。

計2.0ヶ月程度

# 使用するツール/資料の内容（クラウドサービスチェックリスト）

- 「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」の付録6「クラウドサービス安全利用の手引き」の考え方をもとに、「クラウドサービス台帳兼安全利用チェックリスト」を作成します。
- チェックリストをもとに、今後の社内でのクラウドサービス安全利用策を検討します。




**クラウドサービスの選定**

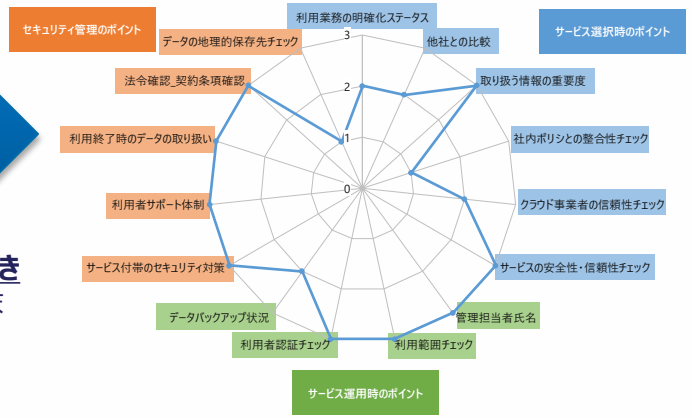
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、**業務のセキュリティ要件に見合ったサービス**を選定しましょう。

**クラウドサービスの運用**

クラウドサービスは**提供者と利用者が連携して運用**するため、その特性を理解して運用しましょう。

**クラウドサービスのセキュリティ対策**

**クラウドサービス利用者が対応すべきセキュリティ対策**を理解して実施しましょう。




**＜クラウドサービス台帳兼安全利用チェックシート＞**

| 管理番号 | サービス名 | 所管部署 | サービスの概要 | ステータス | サービス利用開始日 | サービス利用終了（予定）日 | Ⅰ．サービス選 | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | 利用業務の明確化ステータス | 他社との比較 | 取り扱う情報の重要度 |
| S0001 | ○○オンラインストレージサービス | 営業部 | 外部顧客との営業関係書類受け渡し用 | 利用中 | 2024/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した |
| S0002 | △△クラウド財務会計v2 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用中 | 2023/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した |
| S0003 | ××勤怠管理WEBシステム | 総務部 | 所内労務管理 | 利用中 | 2023/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した |
| S0004 | □□ECプラットフォーム | 営業部 | オンライン通販システム | 調査中 | 未定 | 未定 | 一部明確化できている | 確認中 | 確認した |
| S0005 | △△クラウド財務会計v1 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用終了 | 2020/4/1 | 2024/3/31 | 一部明確化できている | 確認中 | 確認した |
| | | | | | | | | | |
| | | | | | | | | | |

# 成果物作成の留意点（クラウドサービスごとの確認）

- 「クラウドサービス台帳兼安全利用チェックリスト」作成に際しては、「**クラウドサービスの選択**」「**クラウドサービスの運用**」「**セキュリティ管理**」の3つのフェーズにおける確認ポイントに留意し、それぞれどの水準まで安全利用チェックが進められているかを記載します。
- リストアップ対象は、すでに社内で活用しているクラウドサービスに加え、今後利用を検討しているサービスも含めます。
- まずは、「クラウドサービス台帳兼チェックリスト」シートのA列～I列に、導入済み及び今後導入予定のクラウドサービスを列挙してください。
- システムごとに個票を作成し、そのデータを一覧表に転記することもできます。

**クラウドサービス台帳兼安全利用チェックシート**

| 管理番号 | サービス名 | 作成日 | 記入担当者氏名 | 所管部署 | サービスの概要 | ステータス | サービス利用開始（予定）日 | サービス利用終了（予定）日 |
|---|---|---|---|---|---|---|---|---|
| 記入例01 | ○○オンラインストレージサービス | 2024/11/01 | 山田 一郎 | 営業部 | 外部顧客との営業関係書類受け渡し用 | 利用中 | 2024/4/1 | 未定 |
| 記入例02 | △△クラウド財務会計v2 | 2024/11/02 | 吉田　太郎 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用中 | 2023/4/1 | 未定 |
| S0001 | ××勤怠管理WEBシステム | 2024/11/03 | 鈴木 花子 | 総務部 | 所内労務管理 | 利用中 | 2023/4/1 | 未定 |
| S0002 | □□ECプラットフォーム | 2024/11/04 | 山田 一郎 | 営業部 | オンライン通販システム | 調査中 | 未定 | 未定 |
| S0003 | △△クラウド財務会計v1 | 2024/11/05 | 吉田　太郎 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用終了 | 2020/4/1 | 2024/3/31 |
| S0004 | クラウド顧客管理システムZZZ | 2024/11/06 | 山田 一郎 | 営業部 | 顧客管理、営業管理、広報PRメルマガ管理等 | 調査中 | 未定 | 未定 |
| S0005 | WEBメール「Aメール」 | 2024/11/07 | 山田 一郎 | 営業部 | ■■プロジェクトにおけるJV関係者間共通メール | 調査中 | 未定 | 未定 |

- 選択するときの確認ポイント（６項目）
  - 何に使うか、どんな情報を扱うか？
  - サービス事業者は信頼できるか？
- 運用するときの確認ポイント（４項目）
  - 誰が使うのか、どう管理するか？
  - 誰が責任を持つか？
- セキュリティ管理のポイント（５項目）
  - 事業者のセキュリティ対策は、サポートは？
  - データ保存先は何処の地域か？

# 成果物作成の留意点（記入用個票からチェックシートへの転記）

クラウドサービス安全利用チェックシート（個票）

| | |
|---|---|
| 管理番号： | S0005 |
| 対象サービス名： | WEBメール「Aメール」 |
| 作成日： | 2024/11/07 |
| 記入担当者氏名： | 山田 一郎 |
| 所管部署： | 営業部 |
| サービスの概要： | ■■プロジェクトにおけるJV関係者間共通メール |
| ステータス： | 調査中 |
| サービス利用開始（予定）日： | 未定 |
| サービス利用終了（予定）日： | 未定 |

| 分類 | No | チェック項目 | ポイント | チェック |
|---|---|---|---|---|
| Ⅰ．選択するときのポイント | 1 | どの業務で利用するか明確にする | どの業務をクラウドサービスで行い、どの | |
| | 2 | クラウドサービスの種類を選ぶ | 業務に適したクラウドサービスを選定し、 | |
| | 3 | 取扱う情報の重要度を確認する | クラウドサービスで取扱う情報が漏えい、 | |
| | 4 | セキュリティのルールと矛盾しないようにする | 自社のルールとクラウドサービス活用との | |
| | 5 | クラウド事業者の信頼性を確認する | クラウドサービスを提供する事業者は信 | |
| | 6 | クラウドサービスの安全・信頼性を確認する | サービスの稼働率、障害発生頻度、障 | |
| Ⅱ．運用するときのポイント | 7 | 管理担当者を決める | クラウドサービスの特性を理解した管理担 | 担当者アサイン中 |
| | 8 | 利用者の範囲を決める | クラウドサービスを適切な利 | 一部管理できている |
| | 9 | 利用者の認証を厳格に行う | パスワードなどの認証機能に | 未確認 |
| | 10 | バックアップに責任を持つ | ービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確 | 一部管理できている |
| Ⅲ．セキュリティ管理のポイント | 11 | 付帯するセキュリティ対策を確認する | サービスに付帯するセキュリティ対策が具体的に公開されていますか？ | 一部公開されている |
| | 12 | 利用者サポートの体制を確認する | サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？ | ヘルプデスクなし |
| | 13 | 利用終了時のデータを確保する | サービスの利用が終了したときの、データの取り扱い条件について確認しましたか？ | 確認中 |
| | 14 | 適用法令や契約条件を確認する | 個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？ | 確認中 |
| | 15 | データ保存先の地理的所在地を確認する | データがどの国や地域に設置されたサーバに保存されているか確認しましたか？ | 未確認 |

「クラウドサービス安全利用チェックシート｜記入用個票」シート

## ＜個票からの転記手順＞

① 「個票」ファイルの「クラウドサービス安全利用チェックシート｜記入用個票」シートに必要事項を記入します。

② 「貼り付けデータ生成」シートのA2～X2セルの値をコピーします。

③ コピーした情報を、「クラウドサービス台帳兼チェックリスト」ファイルの「一覧表」シートで、既存データの続きに「値貼り付け」します。
「形式を選択して貼り付け」→「値」

以下の1行をコピーし、一覧表の最下部に付け足して「**値貼り付け**」してください。

**この範囲をコピー**

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S0005 | WEBメール「Aメール」 | 45603 | 山田 一郎 | 営業部 | ■■プロジェクトにおけるJV関係者間共通メール | 調査中 | 未定 | 未定 | 明確化できていない | 確認中 | 確認中 | 問題があるが対処方法なし | 確認した | 一部確認済（約款添付） | 担当者アサイン中 | 一部管理できている | 未確認 | 一部管理できている | 一部公開されている | ヘルプデスクなし | 確認中 | 確認中 | 未確認 |

「貼り付けデータ生成」シート

クラウドサービス台帳兼安全利用チェック

| | | | | | | | | Ⅰ．サービス選択時のポイント | | | | | Ⅱ．サービス運用時のポイント | | | | Ⅲ．セキュリティ管理のポイント | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 管理番号 | サービス名 | | 担当者氏名 | 所管部署 | サービスの概要 | ステータス | サービス利用開始（予定）日 | サービス利用終了（予定）日 | 利用業務の明確化ステータス | 他社との比較 | 取り扱う情報の重要度 | 社内ポリシとの整合性チェック | クラウド事業者の信頼性チェック | サービスの安全性・信頼性チェック | 管理担当者氏名 | 利用範囲チェック | 利用者認証チェック | データバックアップ状況 | サービス付帯のセキュリティ対策 | 利用者サポート体制 | 利用終了時のデータの取り扱い | 法令確認_契約条項確認 | データの地理的保存先チェック |
| 記入例01 | ○○オンラインストレージサービス | 2024/11/ | | 営業部 | 外部顧客との営業関係書類受け渡し用 | 利用中 | 2024/4/1 | 未定 | すべて明確化できている | 確認した | 確認した | 問題がないことを確認済 | 確認した | すべて確認済（約款添付） | 担当者アサイン済 | すべて管理できている | すべて管理できている | すべて管理できている | すべて具体的に公開されている | ヘルプデスクあり | 確認した | 確認した | 確認した |
| 記入例02 | △△クラウド財務会計v2 | 2024/11/02 | | 財務部 | 所内財務会計、税務申告、給与計算 | 利用中 | 2023/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | わからない | わからない | 担当者アサイン済 | すべて管理できている | すべて管理できている | 一部管理できている | わからない | ヘルプデスクあり | 確認した | わからない | 未確認 |
| S0001 | ××勤怠管理WEBシステム | 2024/11/03 | 鈴木 花子 | 総務部 | 所内労務管理 | 利用中 | 2023/4/1 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | わからない | わからない | 担当者アサイン済 | すべて管理できている | すべて管理できている | 一部管理できている | わからない | ヘルプデスクあり | 確認した | 確認した | 未確認 |
| S0002 | □□ECプラットフォーム | 2024/11/04 | 山田 一郎 | 営業部 | オンライン通販システム | 調査中 | 未定 | 未定 | 一部明確化できている | 確認中 | 確認した | 問題があるが対処方法なし | わからない | わからない | 担当者アサイン済 | 一部管理できている | 一部管理できている | 未確認 | わからない | わからない | わからない | わからない | 未確認 |
| S0003 | △△クラウド財務会計v1 | 2024/11/05 | 吉田 太郎 | 財務部 | 所内財務会計、税務申告、給与計算 | 利用終了 | 2020/4/1 | 2024/3/31 | 一部明確化できている | 確認中 | 確認した | わからない | わからない | わからない | 未了 | 未確認 | 未確認 | 未確認 | わからない | わからない | わからない | わからない | わからない |
| S0004 | クラウド顧客管理システムZZZ | 2024/11/06 | 山田 一郎 | 営業部 | 顧客管理、営業管理、広報PRメルマガ管理等 | 調査中 | 未定 | 未定 | すべて明確化できている | 確認中 | 確認した | 問題がないことを確認済 | 確認中 | すべて確認済（約款添付） | 担当者アサイン済 | すべて管理できている | 一部管理できている | 未確認 | すべて具体的に公開されている | ヘルプデスクあり | 確認中 | 確認した | 確認中 |
| S0005 | WEBメール「Aメール」 | 2024/11/07 | 山田 一郎 | 営業部 | ■■プロジェクトにおけるJV関係者間共通メール | 調査中 | 未定 | 未定 | 明確化できていない | 確認中 | 確認中 | 問題があるが対処方法なし | 確認した | 一部確認済（約款添付） | 担当者アサイン中 | 一部管理できている | 未確認 | 一部管理できている | 一部公開されている | ヘルプデスクなし | 確認中 | 確認中 | 未確認 |

**ここに「値」で貼り付け**

# 成果物作成の留意点（クラウドサービスのリスク評価）

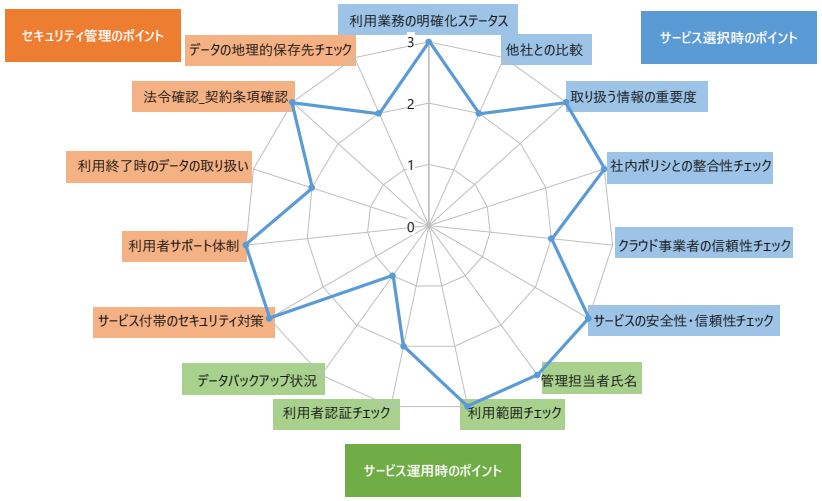
- 一覧表に記載されたサービスは、別シートで個票として分析結果を表示することができます。
- 個票では、「対象サービス名」の欄を選択することで、各サービスの安全利用チェックレベルに応じたレーダーチャートを表示します。
- レーダーチャートのへこみ部分等をもとに、安全利用チェックの方法や水準について検討してください。

クラウドサービス安全利用チェックシート（個票）

| | |
|---|---|
| 管理番号： | S0004 |
| 対象サービス名： | クラウド顧客管理システムZZZ |
| 作成日： | 2024/11/06 |
| 記入担当者氏名： | 山田 一郎 |

| 分類 | No | チェック項目 | ポイント | チェック |
|---|---|---|---|---|
| Ⅰ．選択するときのポイント | 1 | どの業務で利用するか明確にする | どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？ | すべて明確化できている |
| | 2 | クラウドサービスの種類を選ぶ | 業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？ | 確認中 |
| | 3 | 取扱う情報の重要度を確認する | クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、クラウドサービスが停止した場合の影響を確認しましたか？ | 確認した |
| | 4 | セキュリティのルールと矛盾しないようにする | 自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？ | 問題がないことを確認済 |
| | 5 | クラウド事業者の信頼性を確認する | クラウドサービスを提供する事業者は信頼できる事業者ですか？ | 確認中 |
| | 6 | クラウドサービスの安全・信頼性を確認する | サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？ | すべて確認済（約款添付） |
| Ⅱ．運用するときのポイント | 7 | 管理担当者を決める | クラウドサービスの特性を理解した管理担当者を社内に確保していますか？ | 担当者アサイン済 |
| | 8 | 利用者の範囲を決める | クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？ | すべて管理できている |
| | 9 | 利用者の認証を厳格に行う | パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど） | 一部管理できている |
| | 10 | バックアップに責任を持つ | サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？ | 未確認 |
| Ⅲ．セキュリティ管理のポイント | 11 | 付帯するセキュリティ対策を確認する | サービスに付帯するセキュリティ対策が具体的に公開されていますか？ | すべて具体的に公開されている |
| | 12 | 利用者サポートの体制を確認する | サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？ | ヘルプデスクあり |
| | 13 | 利用終了時のデータを確保する | サービスの利用が終了したときの、データの取り扱い条件について確認しましたか？ | 確認中 |
| | 14 | 適用法令や契約条件を確認する | 個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？ | 確認した |
| | 15 | データ保存先の地理的所在地を確認する | データがどの国や地域に設置されたサーバに保存されているか確認しましたか？ | 確認中 |

| | |
|---|---|
| 所管部署： | 営業部 |
| サービスの概要： | 顧客管理、営業管理、広報PRメルマガ管理等 |
| ステータス： | 調査中 |
| サービス利用開始（予定）日： | 未定 |
| サービス利用終了（予定）日： | 未定 |




クラウドサービス安全利用チェックレベル

安全利用チェックレベル評価点： 38 /45点

# 【参考】クラウドサービスチェックリストの項目別点数化

- 各チェック項目は、安全性確認の度合いごとに4段階（3点・2点・1点・0点）のポイントを付しています。
- 各項目の取り組み状況とポイントの関係は以下の通りです。

| 項目 | 3点 | 2点 | 1点 | 0点 |
|---|---|---|---|---|
| **利用業務の明確化ステータス** | すべて明確化できている | 一部明確化できている | 明確化できていない | わからない |
| **他社との比較** | 確認した | 確認中 | まだ確認していない | わからない |
| **取り扱う情報の重要度** | 確認した | 確認中 | まだ確認していない | わからない |
| **社内ポリシとの整合性チェック** | 問題がないことを確認済 | 一部不整合があるが修正対応中 | 問題があるが対処方法なし | わからない |
| **クラウド事業者の信頼性チェック** | 確認した | 確認中 | まだ確認していない | わからない |
| **サービスの安全性・信頼性チェック** | すべて確認済（約款添付） | 一部確認済（約款添付） | まだ確認していない | わからない |
| **管理担当者氏名** | 担当者アサイン済 | 担当者アサイン中 | 未了 | わからない |
| **利用範囲チェック** | すべて管理できている | 一部管理できている | まだ確認していない | わからない |
| **利用者認証チェック** | すべて管理できている | 一部管理できている | まだ確認していない | わからない |
| **データバックアップ状況** | すべて管理できている | 一部管理できている | まだ確認していない | わからない |
| **サービス付帯のセキュリティ対策** | すべて具体的に公開されている | 一部公開されている | 公開されていない | わからない |
| **利用者サポート体制** | ヘルプデスクあり | ヘルプデスクなし | まだ確認していない | わからない |
| **利用終了時のデータの取り扱い** | 確認した | 確認中 | まだ確認していない | わからない |
| **法令確認_契約条項確認** | 確認した | 確認中 | まだ確認していない | わからない |
| **データの地理的保存先チェック** | 確認した | 確認中 | まだ確認していない | わからない |

## セキュリティマネジメント指導ツール

# テーマ④｜セキュリティインシデント対応

# 指導業務の達成目標と成果物

➢「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・助言を行います 。

## マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

【達成目標１】現状における自社の情報セキュリティリスクの洗い出し
【達成目標２】インシデント対応手順書の作成
【達成目標３】作成したインシデント対応手順書に基づく机上演習の実施

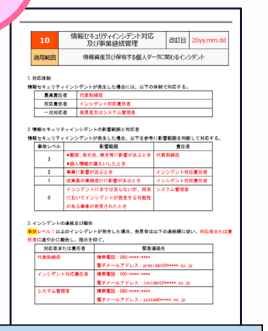
注： 成果物

取組みスタート

達成目標1

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

達成目標2



● インシデント対応手順書（規程）の作成

達成目標3

● インシデント対応机上演習の実施とレビュー

継続実施

# 各回ごとの指導の内容（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**

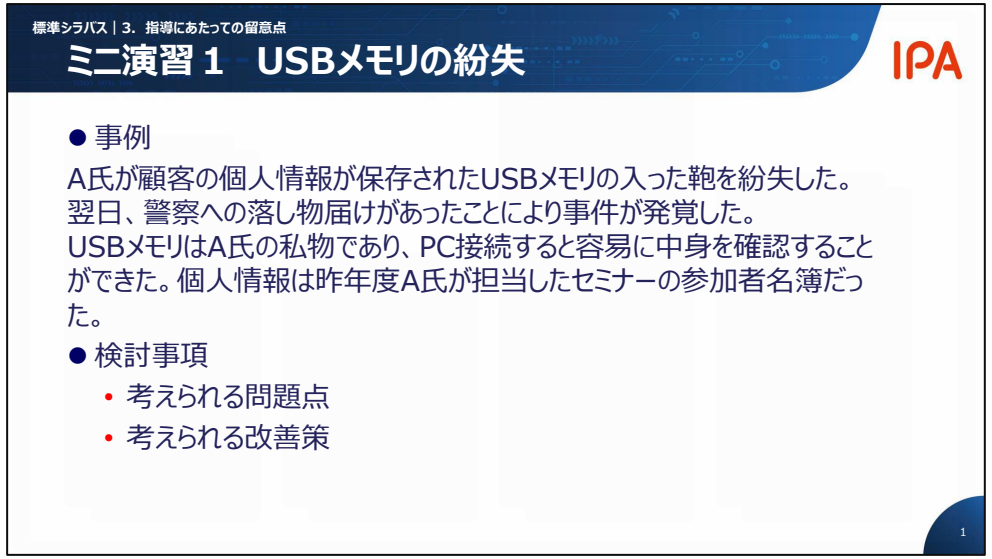
**インシデント対応机上演習の実施とレビュー**

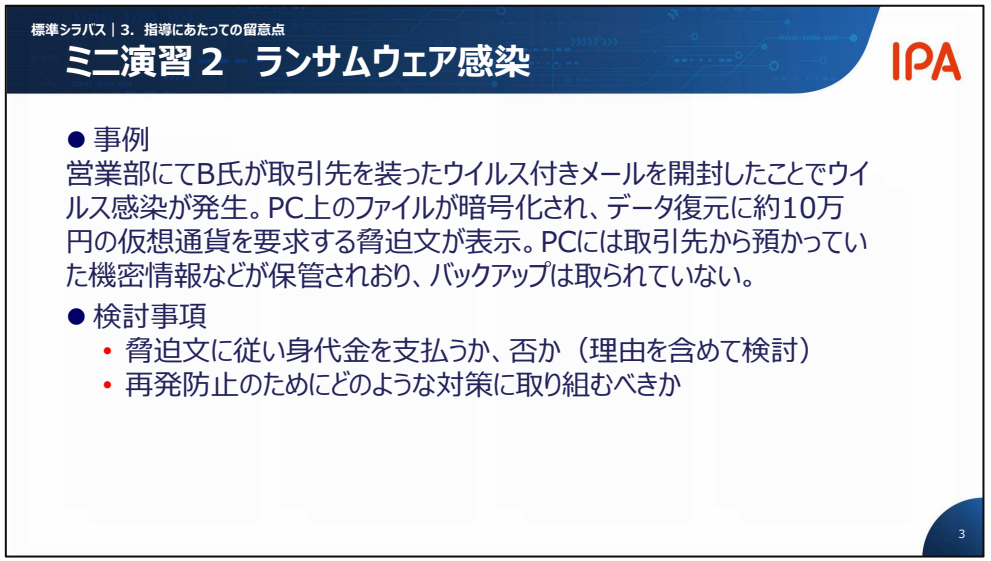
策定したインシデント対応手順書に従い、机上演習を実施します。社員全体ではなく、セキュリティ担当者を対象とした演習とすることも可能です。専門家が演習のコーディネイトを支援します。
演習結果レビューの考え方について指導するとともに、今後の継続的な演習体制の構築とガイドライン策定に向けたアドバイスを行います。

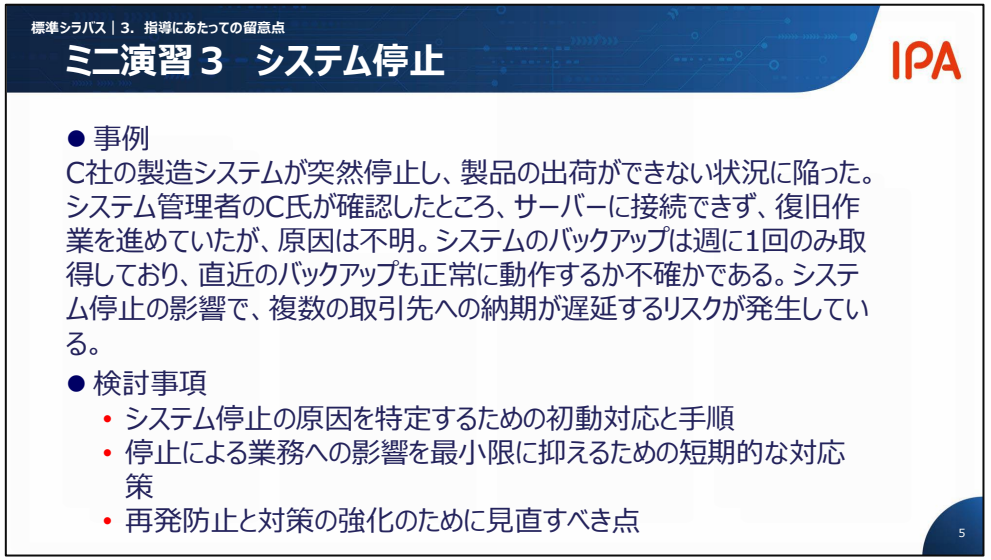
計2.0ヶ月程度

# 使用するツール/資料の内容（ミニ演習シナリオ）

- インシデント対応に関する基本的な考えや担当者の意識を把握するために、初回指導において簡易なディスカッション演習を実施することも有効です。
- 必要に応じ、以下のサンプル演習シナリオ等をもとに、現時点でインシデントが発生した場合にどのような対応をとることができるかを確認します。

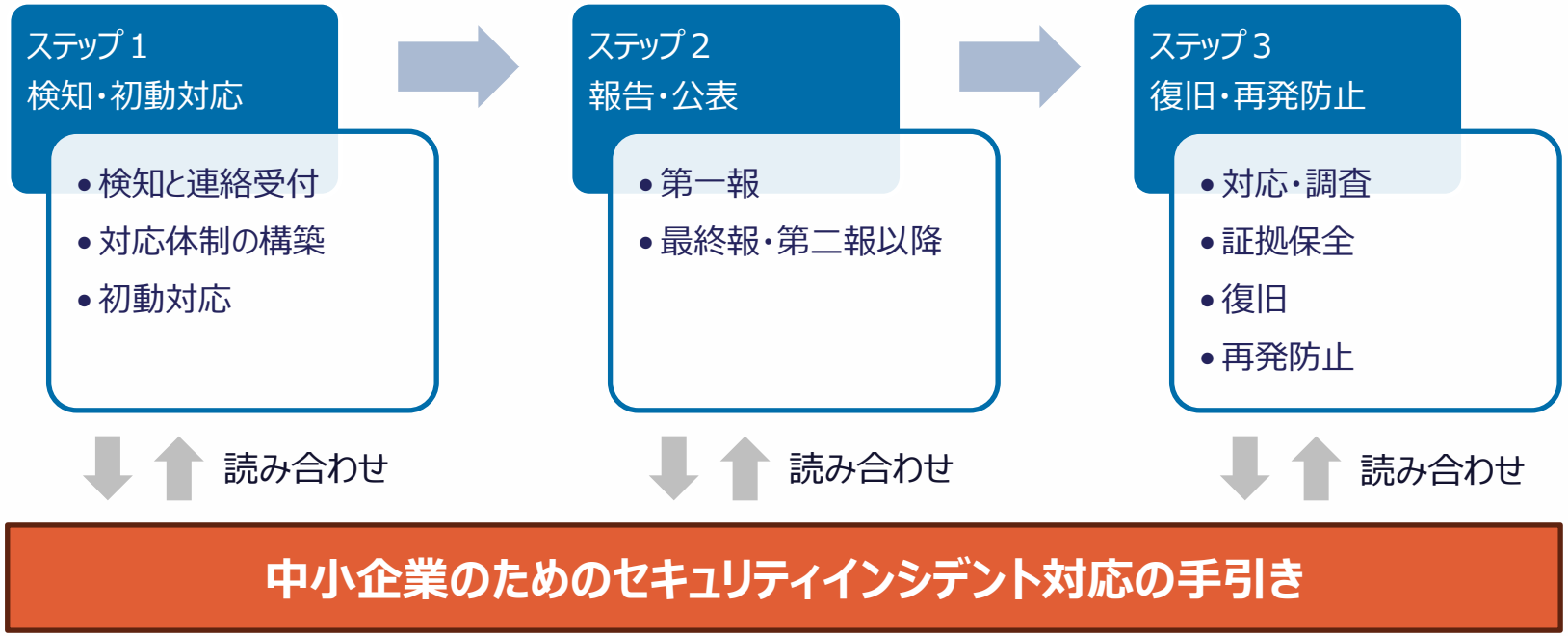


# 使用するツール/資料の内容（インシデント対応の手引き）

- 「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」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」をベースに、指導先企業における具体的なインシデント対応手順書を取りまとめます。
- 取りまとめた手順書をベースに、実際に社内にてインシデント対応机上演習を実施します。
- 演習は、あらかじめ用意したシナリオを用い、「検知・初動対応」「報告・公表」「復旧・再発防止」の３つの段階に分けてポイントが確認できるよう工夫し実施します。実際のシステムを使ったフルスケールの演習ではなく、手順書とシナリオを読み合わせるウォークスルー型の演習を想定しています。

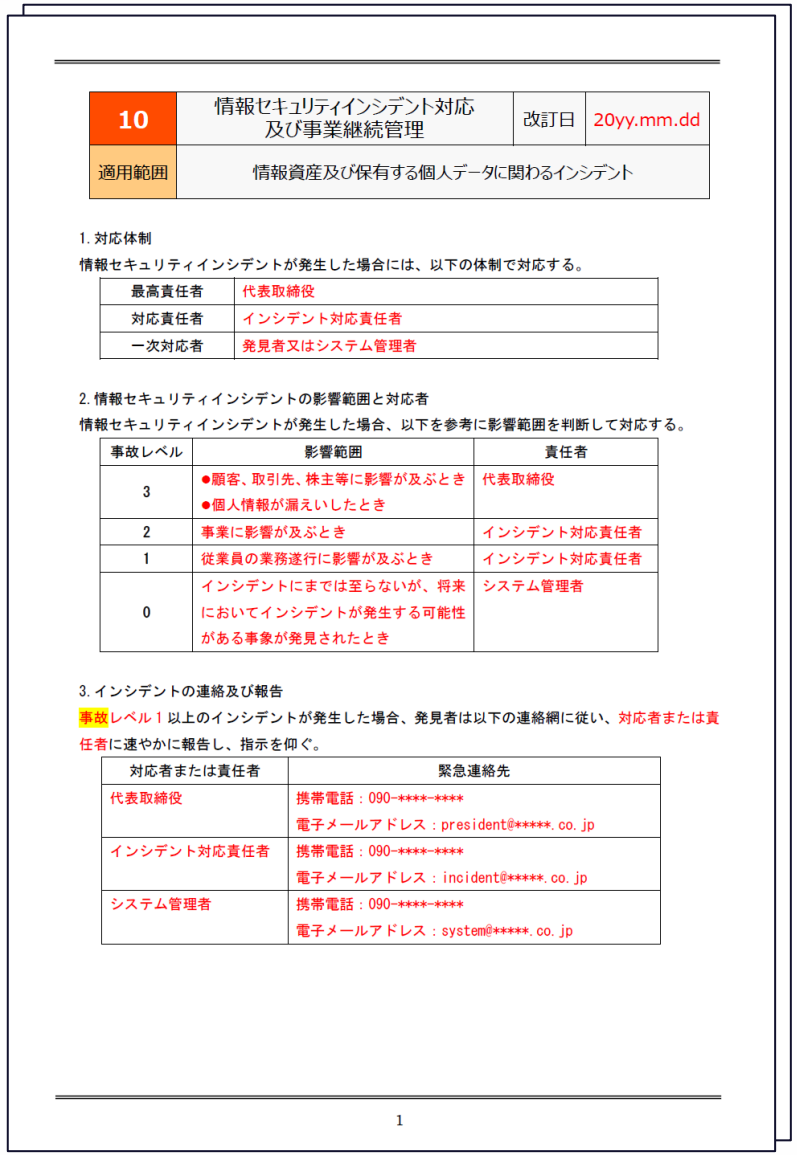


# 使用するツール/資料の内容（インシデント対応規程）

指導先企業においてインシデント対応に関する基本的な規程等が用意されていない場合、まず「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」の付録5「情報セキュリティ関連規程（サンプル）」のうち、「10. 情報セキュリティインシデント対応及び事業継続管理」をベースに、指導先企業における基本的なインシデント対応手順を取りまとめることも有効です。

## 「10. 情報セキュリティインシデント対応及び事業継続管理」記載項目

1. 対応体制
2. 情報セキュリティインシデントの影響範囲と対応者
3. インシデントの連絡および報告
4. 対応手順
    1. 漏えい・流出発生時の対応
    2. 改ざん・消失・破壊・サービス停止発生時の対応
    3. ウイルス感染時の初期対応
5. 届け出及び相談
6. 情報セキュリティインシデントによる事業中断と事業継続管理
7. 事業継続計画



| 10 | 情報セキュリティインシデント対応及び事業継続管理 | 改訂日 | 20yy.mm.dd |
|---|---|---|---|
| 適用範囲 | 情報資産及び保有する個人データに関わるインシデント | | |

1. 対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

| | |
|---|---|
| 最高責任者 | 代表取締役 |
| 対応責任者 | インシデント対応責任者 |
| 一次対応者 | 発見者又はシステム管理者 |

2. 情報セキュリティインシデントの影響範囲と対応者

情報セキュリティインシデントが発生した場合、以下を参考に影響範囲を判断して対応する。

| 事故レベル | 影響範囲 | 責任者 |
|---|---|---|
| 3 | ●顧客、取引先、株主等に影響が及ぶとき<br>●個人情報が漏えいしたとき | 代表取締役 |
| 2 | 事業に影響が及ぶとき | インシデント対応責任者 |
| 1 | 従業員の業務遂行に影響が及ぶとき | インシデント対応責任者 |
| 0 | インシデントにまでは至らないが、将来においてインシデントが発生する可能性がある事象が発見されたとき | システム管理者 |

3. インシデントの連絡及び報告

事故レベル1以上のインシデントが発生した場合、発見者は以下の連絡網に従い、対応者または責任者に速やかに報告し、指示を仰ぐ。

| 対応者または責任者 | 緊急連絡先 |
|---|---|
| 代表取締役 | 携帯電話：090-****-****<br>電子メールアドレス：president@*****.co.jp |
| インシデント対応責任者 | 携帯電話：090-****-****<br>電子メールアドレス：incident@*****.co.jp |
| システム管理者 | 携帯電話：090-****-****<br>電子メールアドレス：system@*****.co.jp |

1

# 成果物作成の留意点（インシデント対応手順書記載項目例）

「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」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」をベースに、指導先企業における具体的なインシデント対応手順書を取りまとめます。

【参考】ランサムウェア感染時の対応手順書記載項目例

| ステップ | フェーズ | 手順項目 | 詳細手順 | 担当者 | 予め準備しておかなければならないもの |
|---|---|---|---|---|---|
| 検知・初動対応 | 検知と連絡受付 | 感染兆候の検知 | IT管理担当者が社内PCやサーバーの感染兆候（暗号化やメッセージ表示）を確認し、クラウドサービスの異常も検知する。 | IT管理担当者 | 連絡先リスト、感染兆候チェックリスト |
| | 初動対応 | 感染端末の隔離 | IT管理担当者が感染端末をネットワークから切断し、クラウドサービスのアクセスも一時停止。 | IT管理担当者 | 感染端末隔離手順、連絡先リスト |
| | 対応体制の立ち上げ | インシデント対応会議の開催 | IT管理担当者が経営管理部長に状況を報告し、インシデント対応会議を招集。経営管理部長がインシデント対応会議にて、IT管理担当者、製造管理部門主任、経営層などの役割分担を確認。 | 経営管理部長 | 役割分担リスト、連絡先リスト |
| | 対応体制の立ち上げ | 関係者への周知 | IT管理担当者が経営管理部長にインシデント発生を報告し、経営管理部長が全従業員に使用停止を通知。必要に応じて取引先にも速報。 | IT管理担当者、経営管理部長 | 連絡先リスト |
| 報告・公表 | 第一報 | 初期報告 | IT管理担当者が感染範囲を報告し、経営管理部長および社長に対し詳細を報告。社長が主要取引先に発生を説明。 | IT管理担当者、経営管理部長、社長 | 連絡先リスト、詳細報告書テンプレート |
| | 第二報以降・最終報 | 詳細報告書の作成 | IT管理担当者が感染経路や対応進捗を含む報告書を作成し、経営管理部長が取引先や従業員に適切に説明できるよう調整。 | IT管理担当者、経営管理部長 | 詳細報告書テンプレート |
| | 第二報以降・最終報 | 外部への公表（必要に応じて） | 経営管理部長が外部に対し必要に応じ、復旧状況と再発防止策の進捗を報告。 | 経営管理部長 | 報告書テンプレート |
| 復旧・再発防止 | 調査・対応 | 感染経路の調査と対応策の策定 | IT管理担当者が感染経路の調査を行い、具体的な対応策を策定。製造管理部門主任と協力して影響範囲を確認。 | IT管理担当者、製造管理部門主任 | 原因調査ツール、対応策計画テンプレート |
| | 証拠保全 | 証拠データの収集と保全 | IT管理担当者が証拠データ（ログファイルや不審ファイル）を収集し、安全な場所に保管。後日分析のための準備。 | IT管理担当者 | 証拠データ保全手順、保全ツール |
| | 復旧 | ウイルス駆除およびシステムの再構築 | IT管理担当者が感染端末をウイルス駆除し、製造管理部門主任が製造ラインの影響確認。必要に応じシステムを再構築。 | IT管理担当者、製造管理部門主任 | ウイルス駆除ツール、隔離手順 |
| | 復旧 | バックアップからのデータ復旧 | IT管理担当者がクラウドバックアップから重要データをリストアし、製造管理部門主任が整合性を確認。 | IT管理担当者、製造管理部門主任 | バックアップ・リストア手順 |
| | 復旧 | パスワードの再設定 | IT管理担当者がパスワードを再設定し、経営管理部長が従業員に新しいパスワード設定の案内を実施。 | IT管理担当者、経営管理部長 | パスワードリセット手順 |
| | 再発防止策 | 原因分析と再発防止策の実施 | IT管理担当者が原因分析を行い、経営管理部長が再発防止策を計画、従業員教育の実施準備。外部監査依頼も含む。 | IT管理担当者、経営管理部長 | 原因分析ツール、再発防止策チェックリスト、監査計画 |

# 使用するツール/資料の内容（インシデント対応机上演習シナリオ）

- 「インシデント対応机上演習シナリオ検討シート」をベースに、企業独自の情報やあらかじめ策定したインシデント対応手順書を踏まえ、具体的なシナリオを策定します。
- 策定したシナリオに沿って、専門家によるコーディネートのもと、インシデント対応手順書記載の各項目が正しく処理できるかどうか、関係者を含めて読み合わせを行います。
- インシデント対応手順書に記載された作業内容、作業担当者、事前準備しておかなければならない文書等について、逐次確認を進めていきます。
- シート様式に対して厳格な運用は必須ではありません。状況に応じ実効的なシナリオを策定してください。

**インシデント対応机上演習シナリオ検討シート**

社名：　（　　）

| 項目 | 内容例（テンプレート） | シナリオ検討用メモ |
|---|---|---|
| シナリオ名 | 1. ウイルス感染／ランサムウェア感染<br>2. 情報漏えい<br>3. システム停止 | 1. ウイルス感染／ランサムウェア感染<br>2. 情報漏えい<br>3. ○○システム停止　（※いずれかを選択） |
| 想定インシデント | ランサムウェア感染により、システムがロックされ、重要データが暗号化された | |
| 発生シナリオ | 社員が外部からのメールを開封し、添付ファイルをダウンロード。ダウンロードしたファイルにランサムウェアが仕込まれていた | |
| 影響範囲 | 社内のファイルサーバおよび重要な顧客情報にアクセスできなくなる | |
| 演習目的 | インシデント対応手順書記載内容の抜け漏れチェック、インシデント発生時の初動対応力向上、チーム間の連携強化。経営層への報告フローの確認 | |
| 演習実施者 | 情報システム担当者、セキュリティ担当者、経営層（役員） | |
| 演習進行 | 専門家の指導のもと、インシデント発生から復旧・再発防止に至るまで、あらかじめ策定したインシデント対応手順書に従って対応が進められるかどうかを読み合わせる（ウォークスルー型演習） | |
| 役割分担 | システム担当者:ログ確認・遮断対応、セキュリティ担当者:情報の集約と管理、経営層:影響範囲の確認と指示出し | |
| 使用する資料 | インシデント対応規程、インシデント対応手順書、社内報告用テンプレート、外部機関への報告文テンプレート、各種システム関連手順書 | |
| 想定する課題 | 初動対応が迅速に行えるか、対応の中でのコミュニケーションが十分に確保できるか、外部機関への対応方法が必要十分か、など | |
| 評価ポイント | 初動対応の適切性、チーム間の連携度、経営層への情報伝達の正確性 | |
| 事後分析の内容 | インシデント対応の課題と改善策の洗い出し、演習で得られた知見の共有、次回演習への反映項目の検討 | |
| 実施日 | YYYY年MM月DD日 | |
| 備考 | 演習参加者には、演習終了後にフィードバックを依頼 | |

企業と協議の上
シナリオを検討

# 使用するツール/資料の内容（机上演習実施後レビュー）

- インシデント対応机上演習を実施後、演習に参加した担当者や経営層等にインタビューを行い、全体的な評価や、演習実施に伴い浮かび上がってきた課題、要改善項目等について洗い出し、共有します。

※項目は適宜追加・変更可、必ずしも厳格な運用は必要ない。

**インシデント対応机上演習実施後レビュー項目**

社名：（　　）

| レビュー項目 | 記載例 | 詳細（具体的に記載） |
|---|---|---|
| 演習の目的達成度 | 初期対応の手順確認と関係部署の連携強化を目的として実施。目的達成度は80%で、初期対応における情報共有が円滑に行われたものの、一部連携に時間を要した。 | 企業と協議の上評価を記載 |
| 対応手順の理解度 | 全員が基本的な対応手順を理解していたが、手順書の参照部分について一部混乱が見られた。特に報告ラインの再確認、及びバックアップデータのリストア手順の再確認が必要。 | |
| 連携・コミュニケーション | 全体的にスムーズにコミュニケーションが図られたが、初期段階での情報共有に遅れが生じた。今後は専用チャットツールの活用を検討。 | |
| リーダーシップの発揮 | リーダーが状況把握と指示出しを的確に行ったが、緊急時の優先順位判断に時間がかかった。今後、意思決定フローの簡略化が必要。 | |
| 情報共有と記録の適切さ | 一部情報が正確に共有されなかった場面があったため、記録の担当者を明確にする必要あり。今後、共有時にメモや記録をリアルタイムで確認する体制が望ましい。 | |
| 課題点および改善点 | 関係部署への連携スピードが課題となった。次回演習までに連絡経路を再確認し、各部署での担当者リストを明示化する予定。 | |
| 次回演習に向けたアクションアイテム | 手順書の改訂（報告フローの簡略化），関係部署間の情報共有方法の検討（チャットツールの導入を含む），意思決定プロセスの確認と、優先順位の考え方についての再確認 | |
| 総合評価 | 演習全体の評価は良好で、初期対応の確認に有効だった。ただし、迅速な意思決定と連携強化が次の課題となる。 | |

# 【参考】インシデント事象ごとの対応のポイント

- **ウイルス感染・ランサムウェア感染の場合**

  ウイルス感染やランサムウェア感染の場合は、まず感染したパソコンやサーバーの利用を停止し、ネットワークから切り離すことが重要です。特にランサムウェア対応においては、日頃から適切な方法でデータのバックアップを行っておくことが被害を最小限に抑えるポイントになります。

- **情報漏えいの場合**

  情報漏えいには、ネットワークへの「不正アクセス」、従業員による「内部犯行」、電子メールの「誤送信」、Webでの「誤公開」、「紛失・置忘れ」等によるものがあります。特に、不正アクセスによる情報漏えいは、データの大量流出につながるおそれがあることから、インターネットに接続しているサーバへの対策が必要です。また、不正アクセスや内部犯行は犯罪性があるため、警察への届け出も必要になります。

- **システム停止の場合**

  システム停止の原因は、サイバー攻撃などのセキュリティの問題も含め、不具合・ソフトウェアのバグ、機器の故障、など様々な原因が想定され、異常の発見時には原因がわからないことがあります。原因がわからない場合は、セキュリティの問題の可能性も含めて対応を行う必要があります。また、システムの停止は事業や企業経営に重大な影響を与える場合があるので、経営者は事業継続計画（BCP）を策定し、これに備える必要があります。

※サイバーセキュリティ経営ガイドライン 付録C「インシデント発生時に組織内で整理しておくべき事項」も参考になります
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

セキュリティマネジメント指導ツール

# テーマ⑤｜従業員向けセキュリティ教育

# 指導業務の達成目標と成果物

➢ 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・助言を行います。

## マネジメント指導業務の達成目標と成果物

【達成目標１】現状における自社の情報セキュリティリスクの洗い出し
【達成目標２】サイバーセキュリティに関する従業員教育の実施
【達成目標３】教育実施結果のレビューと、以後の継続実施に向けた教育計画の策定

中小企業等の対策実施レベル

注：成果物

取組みスタート

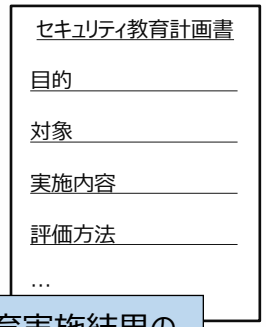
達成目標１

● 5分でできる！情報セキュリティ自社診断(Excel版)による現状リスク洗い出し結果

達成目標２

● 従業員向けサイバーセキュリティ教育の実施

達成目標３




● 教育実施結果のレビューと、以後の教育計画の策定

継続実施

# 各回ごとの指導の内容（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行います。

計2.0ヶ月程度

# 使用するツール/資料の内容（教育計画書）

- 専門家の指導のもと、従業員向けの情報セキュリティ教育計画書を策定してください。
- 研修当日のプログラムも合わせて作成し、実施に向けて社内調整を行ってください。
- 従業員向け情報セキュリティ教育実施後、受講者に対するアンケートを実施、集計結果を分析・評価してください。

| 情報セキュリティ教育計画書（例） | |
|---|---|
| 研修名 | テレワーク勤務時のセキュリティの注意事項 |
| 実施時期 | 20××年10月 1日(火)　[第1回] 10：00～11：00<br>25日(金)　[第2回] 16：00～17：00 |
| 受講方法 | Web会議システム **※各自のPCで受講してください** |
| 対象者 | 全従業員 **※パートタイマー、派遣社員の方も受講してください。** |
| プログラム | ・映像で知る情報セキュリティの上映<br>・自社のセキュリティルールの説明 |
| 講　師 | 情報システム担当 |
| 特記事項 | 第1回、第2回いずれかを必ず受講してください。 |

# 成果物作成の留意点（教育目的･テーマを決める）

## 教育目的の検討

- 自社の**従業員に必要なセキュリティの知識やスキル**を検討します。
- 従業員の職種や役職、また、業務で利用する情報システムによって、**必要とされる知識やスキルは様々**です。
- **対象者やIT環境**など状況に適した目的を決めましょう。

例1
対象者　：全従業員
研修目的：『情報セキュリティ規程』を周知する

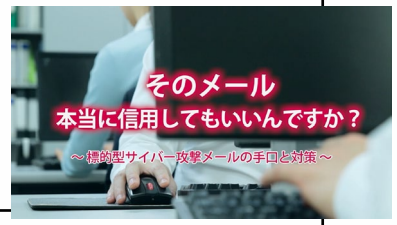
例2
対象者　：テレワーク勤務する従業員
研修目的：テレワーク勤務時に使用する情報システムセキュリティ上の注意事項を周知する

## 教育テーマの検討

- セキュリティに必要な知識やスキルは多岐に渡るため、短時間に、多くを伝えても、**全てを理解し実行するのは難しい**ことがあります。
- 受講者の的確な理解が得られるように、要点を絞るとともに、**計画的に教育の機会**を設けましょう。
- テレワークやクラウドシステムの導入など、情報システムの変更に伴い、新たな対策が必要になった場合など、**状況に適したテーマ**を決めましょう。

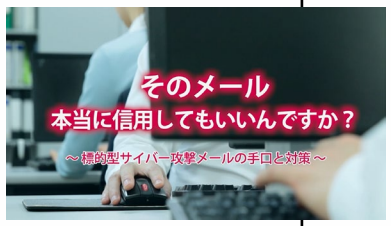
# 成果物作成の留意点（当日プログラムを作る）

- 教育計画書を作成したら研修当日のプログラムを作ります。
- その際、受講者が理解できたか、実行できているかなど、**効果測定をあらかじめ計画**します。効果測定の方法は、**テストやアンケート**を実施したり、職場での**行動を観察**する、などがあります。

| サンプルプログラム（60分） | | | 使用教材 |
|---|---|---|---|
| 10:00<br>（10分） | 映像上映<br>「そのメール本当に信用してもいいんですか？<br>～標的型サイバー攻撃メールの手口と対策～」 | 映像で知る情報セキュリティを上映する | IPA映像で知る情報セキュリティ（動画サイト）<br>  |
| 10:10<br>（30分） | 解説 | 解説 | 資料 |
| 10:40<br>（10分） | Q&A | | |
| 10:50<br>（10分） | 理解度確認テスト | 効果測定の後、講師が解説する | 資料 |

# 「映像コンテンツ」を使った研修会 サンプルプログラム①

- 標的型メール攻撃対策研修

| サンプルプログラム（60分） | | | 使用教材 |
|---|---|---|---|
| 10:00<br>（10分） | 映像上映<br>「そのメール本当に信用してもいいんですか？<br>～標的型サイバー攻撃メールの手口と対策～」 | 映像で知る情報セキュリティを上映する | IPA映像で知る情報セキュリティ（動画サイト）<br>  |
| 10:10<br>（30分） | 解説 | 自社で実施している対策を周知する<br>• 使用しているソフトウェアの更新方法<br>• ウイルス対策ソフト自動更新の方法<br>• 自社に送られてきた不審メールの紹介<br>• 不審メールを受信したときの対応方法 など | 自社作成資料<br> |
| 10:40<br>（10分） | Q&A | | |
| 10:50<br>（10分） | 理解度確認テスト | 効果測定の後、講師が解説する | 自社作成資料<br> |

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.pptx

# 「映像コンテンツ」を使った研修会 サンプルプログラム②

- 内部不正対策研修

| サンプルプログラム（60分） | | | 使用教材 |
|---|---|---|---|
| 10:00<br>（10分） | 映像上映<br>「今、そこにある脅威<br>～内部不正による情報流出のリスク～」 | 映像で知る情報セキュリティを上映する | IPA映像で知る情報セキュリティ（動画サイト）<br> |
| 10:10<br>（30分） | 解説 | 自社で実施している対策を周知する<br>• 使守秘義務および競業避止義務<br>• アクセス制限、私物記録媒体の使用禁止<br>• アクセスログ取得、入退室管理<br>• メールやウェブサービスのログ監視・管理 など | 自社作成資料<br> |
| 10:40<br>（10分） | Q&A | | |
| 10:50<br>（10分） | 理解度確認テスト | 効果測定の後、講師が解説する | 自社作成資料<br> |

サンプルプログラム②_内部不正による情報流出のリスク.pptx

# 【参考】情報セキュリティ教材を入手する

- 情報セキュリティ教材は次のサイトからダウンロードできます。
  https://www.ipa.go.jp/security/sec-tools/index.html

# 【参考】映像で知る情報セキュリティ

- 情報セキュリティ上の様々な脅威と対策を**10分程度のドラマ映像**などを通じて学べる映像教材です。
- YouTube「**IPA Channel**」でいつでも視聴可能です。
  主な映像はダウンロードも可能です。

[企業・組織向け]
内部不正対策、標的型攻撃、ビジネスメール詐欺、
ランサムウェア対策、中小企業向け対策、新人研修など

[一般向け]
ワンクリック請求、スマホセキュリティ、SNS利用の心得、
パスワード、小学生、中高生向けなど

https://www.ipa.go.jp/security/videos/list.html　IPA　映像　**検索**

# ３．令和７年度事業の実施概要

# 令和7年度事業
# セキュリティ人材活用環境整備の概要

- 令和7年度は、中小企業及び支援機関等での**セキュリティ専門家リストの活用促進**と、**登録セキスペの登録促進**、併せて、**中小企業のセキュリティ対応状況評価を行う人材確保**を目指す「**セキュリティ人材活用環境整備事業**」を実施する。

## ①セキュリティ専門家リストの活用促進

- 令和６年度事業では、登録セキスペの得意分野・専門領域を可視化する「登録セキスペ アクティブリスト」を試作した。令和7年度においては、登録セキスペアクティブリスト（試作版）を内容改善後、**セキュリティ専門家リスト**として**IPAウェブサイト上で公開**、登録セキスペ活用の**広報資料を作成**して、中小企業及び支援機関へ登録セキスペの**活用促進**を図り、**フィードバック**を得ることで、**セキュリティ専門家リストの整備**を行う。

## ②セキュリティ専門家リストの登録促進

- 併せて、全ての登録セキスペを対象に**登録セキスペ活用の取組みを周知**し、令和6年度事業で作成したセキュリティマネジメント指導ツール（5テーマ）の**活用セミナー**を開催、マネジメント指導ツールを活用した**指導方法及び指導事例を啓発**することで、**セキュリティ専門家リストへの登録を促進**する。

## ③セキュリティマネジメント指導テーマの拡充

- 令和６年度事業では、中小企業が自社の取組の妥当性を**専門家の第三者的な視点から確認**したいというニーズ等が確認できた。これを踏まえ、令和7年度においては、サプライチェーン対策評価制度実証と連携して、**セキュリティマネジメント指導のテーマを拡充(セキュリティアセスメント)**した上で、研修等により登録セキスペにアセスメントの実践に必要な**情報セキュリティ監査スキルを習得**させ、**中小企業のセキュリティ対応状況評価及び対策支援を行う人材を確保**する。

# セキュリティ人材活用環境整備
# ①セキュリティ専門家リストの活用促進

**【セキュリティ専門家リストの活用促進の進め方】**

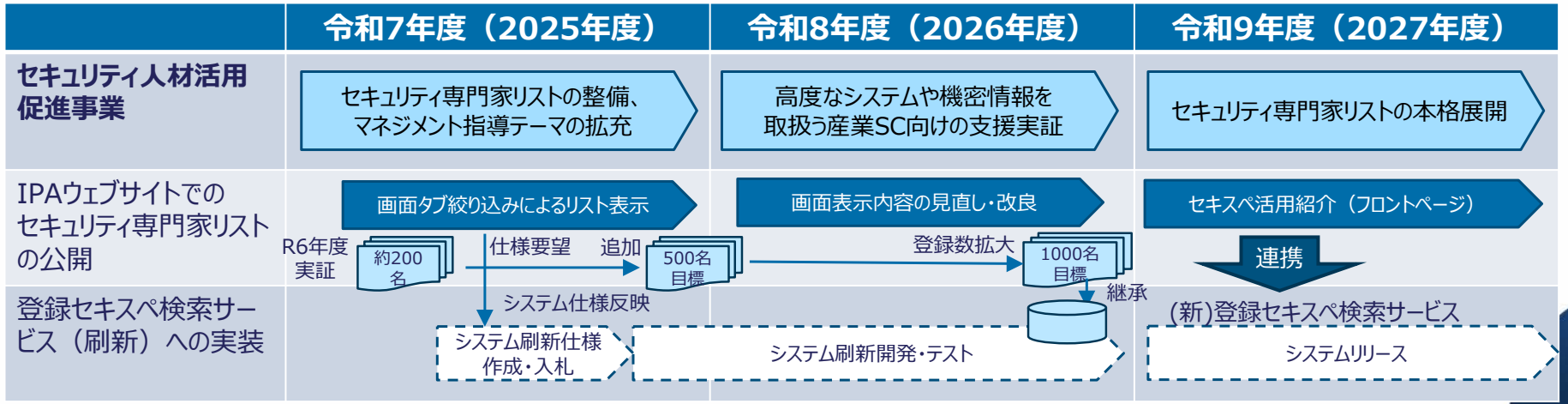
① IPAウェブサイト上に、中小企業向けの**登録セキスペ活用ページ**を作成し、「登録セキスペアクティブリスト（試作版／約200名）」の記述内容等の改善を行って、**セキュリティ専門家リスト**（一覧表ダウンロード）として公開する。併せて、登録セキスペ活用の**広報資料を作成**する。

② 各地域の商工会議所等の中小企業支援機関、地域SECUNITY等の協力により、セキュリティ専門家リスト掲載の専門家による**中小企業向けセキュリティ相談会**を開催（IPAセミナー講師派遣事業）、中小企業と登録セキスペのマッチング機会を創出することで、セキュリティ専門家**リストの活用のフィードバック**を得る。

③ 令和6年度事業の結果、及びセキュリティ専門家リストの活用フィードバックを踏まえ、**リストの掲載・運用方法(案)を作成**した上で、リスト表記の見直しを含めた整備を行う。具体的には、令和6年度事業で検討したリスト検索イメージをもとに、簡易的な画面タブ絞り込み等による**リスト表示ページを作成**して行う。

**【参考】**
**セキュリティ専門家リストのシステム化**

セキュリティ専門家リストのシステム化は、令和9年にシステム刷新予定の「登録セキスペ検索サービス」において実装予定



# セキュリティ人材活用環境整備
# ②セキュリティ専門家リストの登録促進

**【セキュリティ専門家リストの登録促進の進め方】**

① 全ての登録セキスペ（2.3万人）を対象に**登録セキスペ活用の取組みを周知**し、令和6年度事業で作成したセキュリティマネジメント指導ツール（5テーマ）を活用した、**指導方法及び指導事例を啓発する活用セミナー**を開催（ウェビナー形式/約2.5時間。計3回。各回300名、計900名の参加見込）することで、登録セキスペの**セキュリティ専門家リストへの登録を促進**する。

② セキュリティ専門家リストの掲載は、IPAウェブサイトで試行公開したセキュリティ専門家リスト（一覧表ダウンロード/約200名）に、**登録促進活動での新規登録者を加えて公開**する（登録目標：計約500名）

③ セキュリティ専門家リストへの登録申込みを受付けの際は、予め作成した**リストの掲載・運用方法(案)**に基づき、登録申請内容の確認を行った上で、セキュリティ専門家リストに反映する。

**【参考】セキュリティマネジメント指導ツール（5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 |
|---|---|---|---|---|---|
| ターゲット企業 | サイバー攻撃の増加や法令遵守の必要性に直面しつつも、情報セキュリティ規程が未整備な中小企業。 | 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。 | 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。 | 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。 | 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。 |

# セキュリティ人材活用環境整備
# ③セキュリティマネジメント指導テーマの拡充

**【マネジメント指導テーマの拡充（セキュリティアセスメント）の実施方法】**

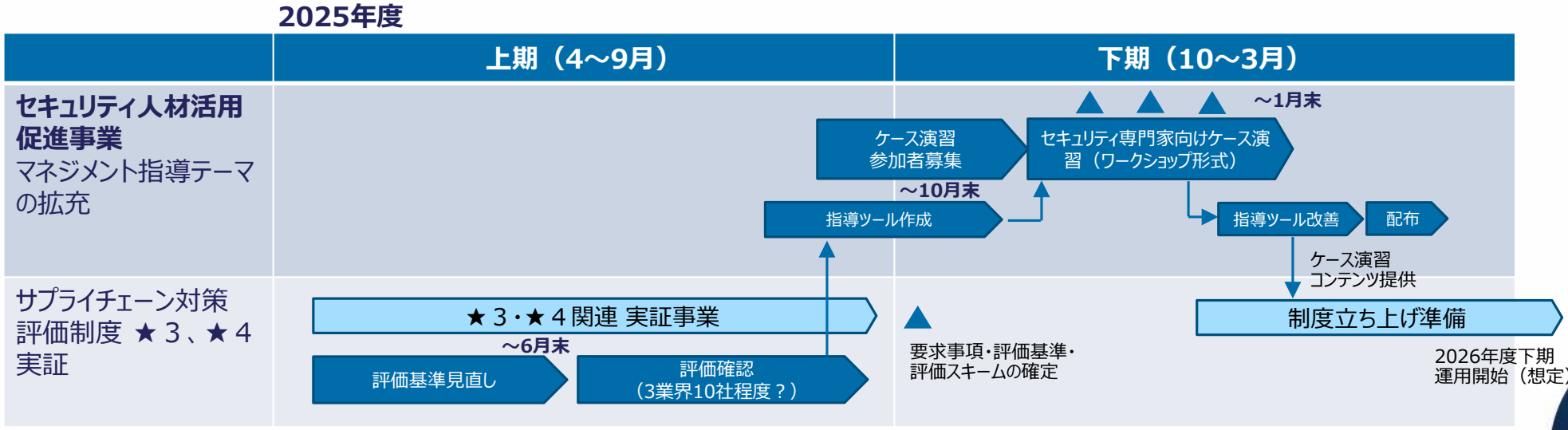
① マネジメント指導テーマへのセキュリティアセスメント要件の追加にあたっては、「サプライチェーン強化に向けたセキュリティ対策評価制度※」の三つ星（★３：全てのサプライチェーン企業が最低限実装すべきセキュリティ対策）の要求事項・評価基準をもとに、**要求事項の遵守状況を確認し、また、要求事項を達成するための助言も併せて行える**ようにするための**指導ツール**（実施要領及びワークシート等）を作成する。

② 拡充したマネジメント指導ツール（セキュリティアセスメント）をもとに、登録セキスペを対象に、**中小企業のセキュリティ評価・対策支援を担当するセキュリティ専門家向けのケース演習**（ワークショップ形式5時間）を東京、名古屋、大阪の3地域で計3回開催（各回20名上限）する。※ケース演習の受講者はセキュリティ専門家リストへの登録が参加要件

※「令和「サプライチェーン強化に向けたセキュリティ対策評価制度構築に向けた中間取りまとめ」を公表
https://www.meti.go.jp/press/2025/04/20250414002/20250414002.html

**【参考】サプライチェーン対策評価制度との連携**

★３★４実証事業で作成された要求事項・評価基準をもとに、マネジメント指導ツール（セキュリティアセスメント）を作成する。



# 中小企業向けサイバーセキュリティ対策支援者リスト

https://www.ipa.go.jp/security/sme/shien/list.html

- 国家資格「**情報処理安全確保支援士（登録セキスペ）**※」の資格者のうち、**中小企業向けのサイバーセキュリティ対策支援**が実施できる専門家の**得意分野・専門領域を可視化**したリスト（支援対象地域別）
- 現段階の情報を試行公開（PDF）。今後、整備・拡充する予定

※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、セキュリティの確保を支援する。国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務を有する。https://www.ipa.go.jp/jinzai/riss/index.html

- 掲載専門家の**支援対象地域別**にリスト化
  - 支援対象地域：北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄
- 掲載専門家が支援可能な**指導テーマ**、支援**実績**、得意とする**業界**、支援可能**形態**、支援**料金**、保有**資格**、保有**スキル**等を記載
- 専門家による中小企業指導の支援ツール（5テーマの実施要領）を整備・公表
  - テーマ(1) 情報セキュリティ規程の整備
  - テーマ(2) 情報資産の洗い出しとリスク分析
  - テーマ(3) クラウドサービスの安全利用
  - テーマ(4) セキュリティインシデント対応
  - テーマ(5) 従業員向け情報セキュリティ教育

IPA