IPA Better Life with IT

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

【別紙1】指導要領（指導ツール）

2021年6月

独立行政法人情報処理推進機構
セキュリティセンター 中小企業支援グループ

本書の構成

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

「指導要領（指導ツール）」は、情報処理安全確保支援士（RISS）等の専門家が、今後も継続して活用できるものとなるよう、標準カリキュラムを示しつつ、指導先企業の個別事情に応じた独自の工夫と肉付けができるよう、指導に必要なツールの活用方法、経験者の体験による気付きや工夫、コロナ禍に必要な対応など実践的なノウハウを提供する内容としています。

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

パートⅠ 具体的支援の進め方	プログラム1	専門家指導全体の構成と留意事項
	プログラム2	各種ツールの活用方法
パートⅡ 効果的な訪問指導	プログラム3	指導に当たっての心構え
	プログラム4	前年度の訪問指導から学べること
	プログラム5	コロナ禍のセキュリティ対策

パートⅠ　具体的支援の進め方

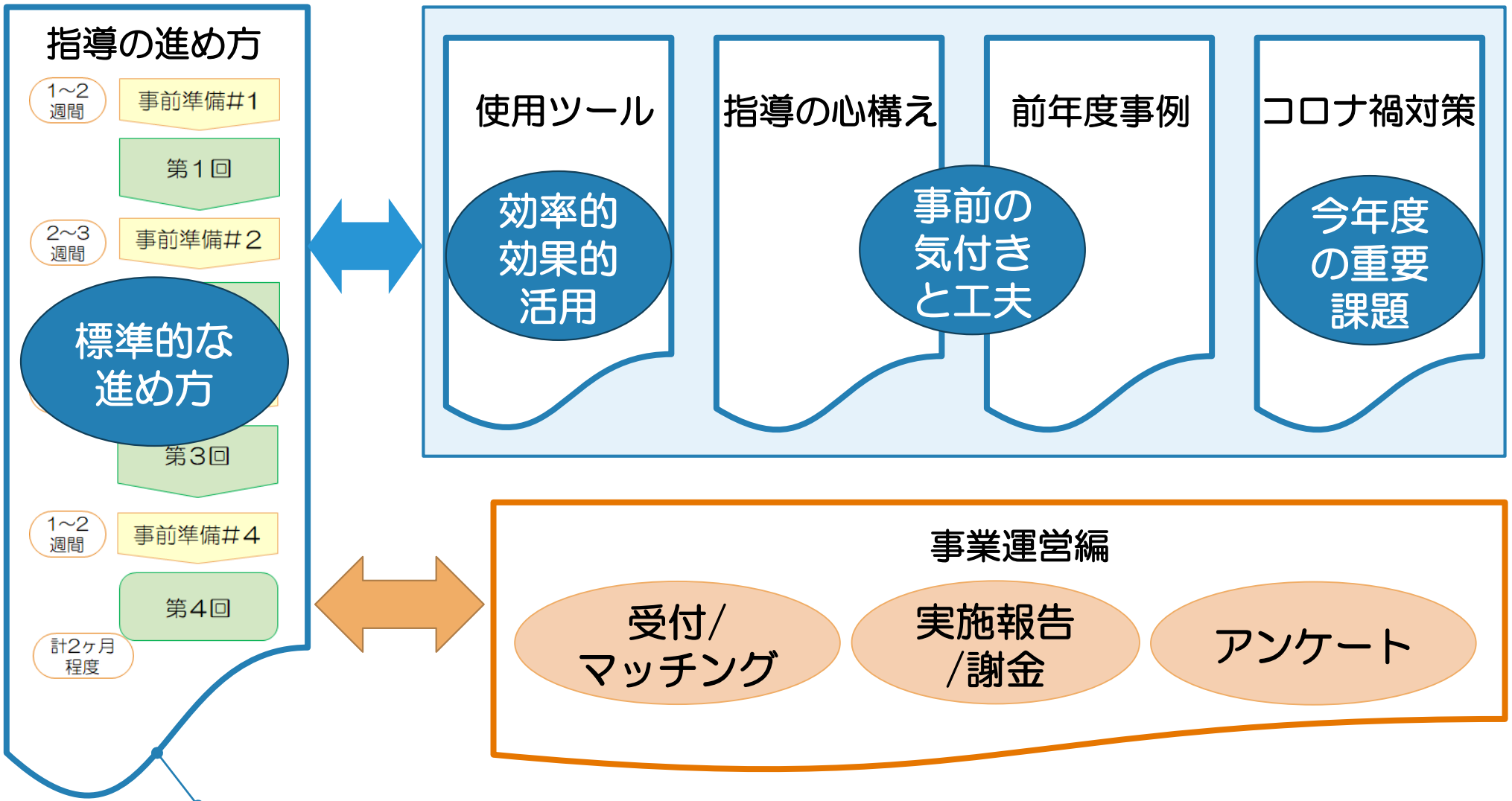
プログラム①
専門家指導全体の構成と留意事項

「専門家指導全体の構成と留意事項」での説明内容

	項目	説明のポイント
1	専門家指導の全体の構成	✓ 指導講習コンテンツの位置付け ＊各コンテンツの主な内容 ✓ 当事業の目標と成果物
2	各回ごとの指導の内容 （標準的な進め方）	✓ 全4回の専門家指導の進め方 ＊企業側・専門家側それぞれの役割・作業 ＊使用するツール/資料（詳細はプログラム②で説明）
3	指導に当たっての留意点 ※プログラム②～⑤の講習コンテンツと併せて理解を深めてください	✓ 指導先企業への依頼や調整事項 ＊企業側の検討体制や事前準備の確認/依頼 ＊コロナ禍の中での指導環境の調整 ＊情報の取り扱い ✓ 初回指導時の留意点 ＊組織的、人的、技術的、物理的対策を幅広く検討 ✓ 対策絞り込みの留意点 ＊検討の対象領域と対策の実効性、継続性 ✓ 成果物作成の留意点 ＊経営者の納得感とフォローアップ

１　専門家指導の全体の構成

各実施要領（指導講習コンテンツ）の位置付け



- ✓ 4回の標準的な専門家指導の内容について、具体的な解説を行います。
- ✓ 併せて、指導先企業への依頼/調整事項や、指導に当たっての基本的な留意点を説明します。
- ✓ 他の講習コンテンツの受講により、標準の進め方に肉付けをして、具体的な指導イメージを描き、指導先企業特有の状況に合わせた対応やアドバイスができるよう、工夫をしてください。

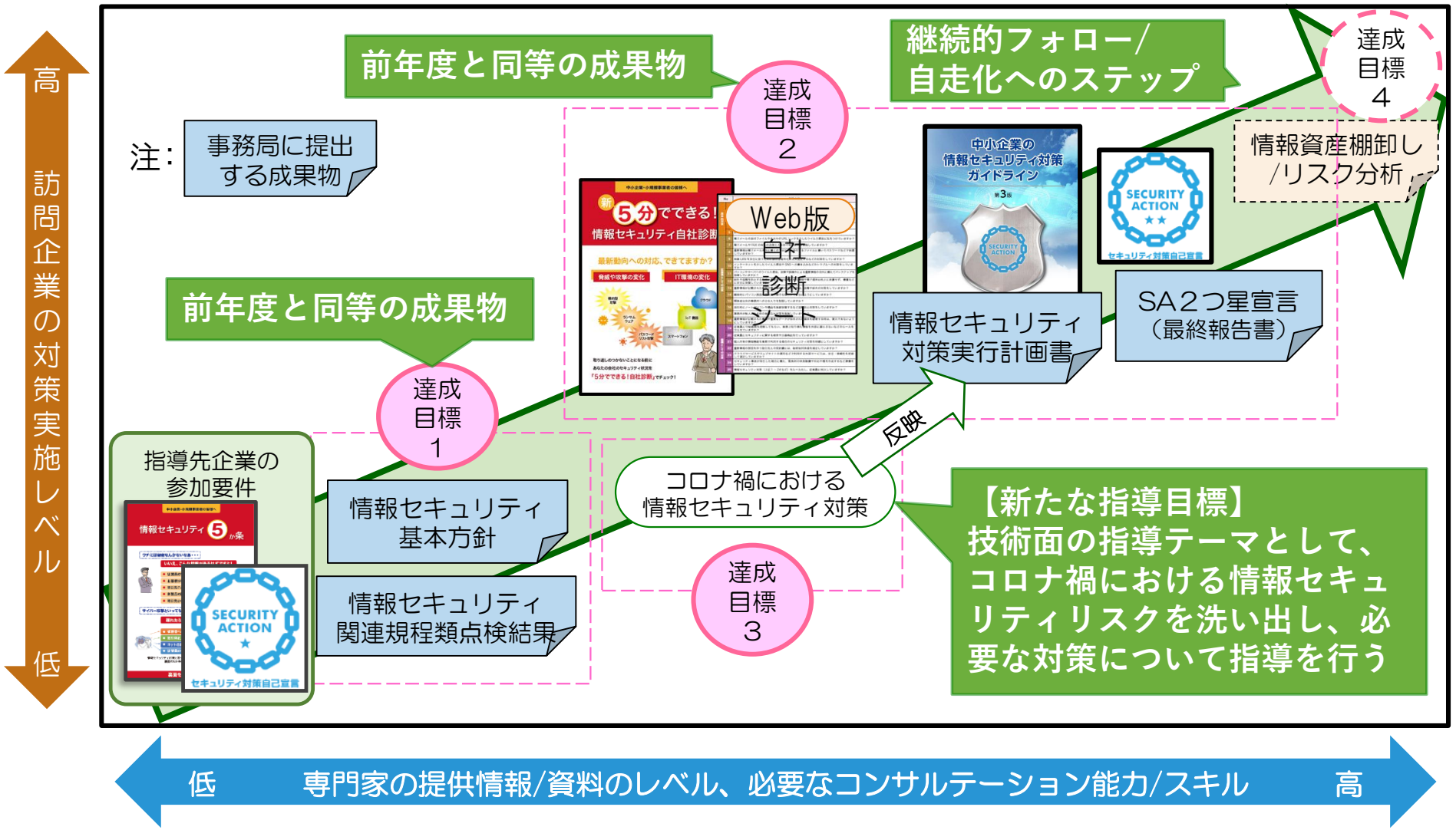
指導講習コンテンツの全体構成と位置付け

		コンテンツの主な内容
パートⅠ 具体的支援 の進め方	プログラム① 「専門家指導全体の構成と留意事項」	● 専門家指導の全体構成 ● 各回ごとの指導の内容（標準プログラム） ● 指導に当たっての留意点
	プログラム② 「各種ツールの活用方法」	● ＩＰＡツールの活用(5分でできる自社診断:Web版、映像コンテンツ、情報セキュリティ対策ガイドライン) ● 提供できるコンテンツ、参考資料
パートⅡ 効果的な 訪問指導	プログラム③ 「指導に当たっての心構え」	● 中小企業経営者が考えていること ● 経営者とのコミュニケション ● コンサルテーションに役立つこと
	プログラム④ 「前年度の訪問指導から学べること」	● 中小企業における情報セキュリティの現状と課題 ● 前年度の専門家指導の実施事例 ● 専門家と経営者のアンケートから気付くこと
	プログラム⑤ 「コロナ禍のセキュリティ対策」	● コロナ禍における必要なセキュリティ対策 ● 専門家指導の中でのWeb会議ツールの活用
理解度確認テストと復習		各プログラムごとに理解度確認テストを受けていただき、理解が不十分な部分について復習していただきます。
事業の概要と運営について		● 事業の全体スケジュール ● 専門家指導の申込み方法など ● 各種提出物、利用コンテンツ、謝金の支払い手続きなど ● Q&Aの対応方法

- 各コンテンツの収録時間は、参加者の集中力が途切れないように30～40分程度の内容になっています。
- 各単元終了毎に理解度の確認テストを受けていただきます。
- テストは10分程度で完了する内容としますが、全問正解を完了条件としています。
- 完了後に、講習の満足度・理解度、講習資料、オンライン方式について、事業への参加意思、要望、等のアンケートに記入いただきます。

当事業の目標と成果物

- ✓ 今年度はコロナ禍での情報セキュリティ対策のアドバイス（達成目標３）を含めた「対策実行計画書」の作成を目指します。尚、終了後に「最終報告書」を事務局宛に提出いただきます。
- ✓ さらに高スキルを保有する専門家については、得意分野の技術的スキルの活用を盛り込み、経営者の信頼を得て将来の自走化に向けた継続的フォローを目指します。（達成目標４）



２　各回ごとの指導の内容
(標準的な進め方)

「標準的な進め方」の全体構成

1～2週間 **事前準備#1**

*指導先企業の情報収集とヒアリングシートの作成
*IPA自社診断(Web版)の実施依頼

第１回

<u>企業の事業や情報システム環境の理解と情報セキュリティリスクの洗い出し</u>

指導先企業の事業内容と情報システム環境を把握し、自社診断の結果をもとに、経営者が認識しているセキュリティ課題（リスク）と当事業への期待値を確認します。

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有無確認の依頼

第２回

<u>情報セキュリティ基本方針や関連規程整備の検討と重点改善領域の絞り込み</u>

基本方針の作成と、必要な関連規程類の検討を行うと共に、自社診断結果をもとに重点改善領域について、ディスカッションと対策の絞り込みを行います。

1～2週間 **事前準備#３**

*前回結果に加え、経営のコロナ禍対策に伴う情報セキュリティリスクの検討

第３回

<u>コロナ禍の情報セキュリティ対策を含む、重点対策の検討と優先順位付け</u>

コロナ禍で急遽対応した経営施策に対する情報セキュリティ面での対策状況を確認し、必要なアドバイスを行うと共に、重点対策と合わせた今後の実行計画を検討します。

1～2週間 **事前準備#４**

*優先順位と実現性を考慮した実行計画案の作成

第４回

<u>情報セキュリティ対策の成果物レビューと訪問指導全体のまとめ</u>

専門家がまとめた実行計画案（一年間程度）についてディスカッションし、合意形成を図ります。また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、二つ星の自己宣言手続きを進めます。

計2ヶ月程度

※テレワーク未導入の企業には、指導期間中に可能な範囲でWeb会議ツールの体験（専門家との事前打合せ等）を行っていただくことを推奨します。

「標準的な進め方」の詳細（１）

第1回　企業の事業やシステム環境の理解と、情報セキュリティリスクの洗い出し

		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 (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 ・訪問指導に当たっての心構え
	2	「5分でできる情報セキュリティ自社診断(Web版)」の実施	同左の実施依頼	【提供】自社診断(Web版)の実施方法
	3	出席メンバー選定 (経営者/従業員等、半日x4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 ・前年度の訪問指導から学べること
	2	提供可能な資料や、認識している情報セキュリティ課題の説明	ヒアリングシートを用いた事業と情報システム環境、情報セキュリティ課題の理解	【提供】標準ヒアリングシート 【提供】IPAの映像コンテンツ
	3	自社診断(Web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(Web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(Web版)の結果のまとめ
	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 ・業務/DB/ネットワークなどのIT環境など 機密保持誓約書の提出 次回のスケジュール調整、依頼事項の確認 ※情報セキュリティ基本方針の作成	（終了後） 専門家から事務局への実施報告提出

＜**実施のポイント**＞

- 第1回の指導では、ヒアリングによって、企業側が認識している現状課題（リスク）について把握します。
- 「５分でできる情報セキュリティ自社診断」は、経営者だけではなく従業員にも実施してもらうことで、実態をより明確にできます。
- 自社診断結果が高得点で、リスクが見えない場合には、本当に対応できているのか、例外的に見逃していることは無いかなど、突っ込んだ質問を行って課題を洗い出し、重点改善領域についてディスカッションします。
- IPA「情報セキュリティ対策ベンチマーク(27項目)」を使って、より高いレベルでの現状把握と他社比較を行うことも有効な方法です。

「標準的な進め方」の詳細（２）

第2回　基本方針や関連規程整備の検討と重点改善領域の絞り込み

		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 (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 ・関連規程類の作成状況確認 ・重点改善領域の見極め	※Web会議ツールにて準備を進めることも検討 【提供】情報セキュリティ基本方針サンプル 【提供】基本方針/関連規程類の整備状況一覧表(確認用ワークシート)
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 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 基本方針の作成指導	【成果物】 ・情報セキュリティ基本方針 ・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 ・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 ・緊急度、重要度、難易度による絞り込み	【成果物】自社診断(Web版)の結果と課題整理
	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） 専門家から事務局への実施報告提出

＜**実施のポイント**＞

- 「５分でできる情報セキュリティ自社診断」の結果を改めて事前に分析し、重点改善領域と思われる項目を提示して、緊急度、重要度、難易度などの視点から、対策の優先順位についてディスカッションを行います。
- 関連規程をどこまで整備しておく必要があるかは、各企業の状況によって異なります。例外対応などの情報セキュリティの抜け穴となる点を極力なくし、また単に規程を作成するだけでなく、継続的に順守していける運用体制や従業員研修の実施についても併せて検討し、実効性を高めるようガイドしていきます。

「標準的な進め方」の詳細（３）

第3回　コロナ禍の情報セキュリティ対策を含む、重点対策の検討と優先順位付け

		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 (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	コロナ禍における経営施策と情報システム環境の状況整理 ・テレワーク推進の課題など	コロナ禍の経営施策に必要な情報セキュリティ対策の説明資料の準備 ・指導講習コンテンツの理解	※実践として、第2回実施の際に、Web会議にて事前準備を進めることを検討
当日	1	コロナ禍の事業継続として実施した経営施策の説明と、情報セキュリティ対策の必要性の理解	コロナ禍の事業継続として実施された対策に対する、必要な情報セキュリティ対策の説明。	【提供】指導講習コンテンツ ・コロナ禍の情報セキュリティ対策
	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 ・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 ・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 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	右記の確認と了承	第4回に向けての準備の依頼 ・SECURITY ACTION二つ星宣言の申請準備	（終了後） 専門家から事務局への実施報告提出

＜**実施のポイント**＞

- 直近の経営の最大課題であるコロナ禍対策について、情報セキュリティ対策の視点から抜け漏れがないか確認と検討を行います。
- Web会議ツールの活用では、取引先との接続環境や、従業員の働く環境など、様々なリスクを踏まえた対策をアドバイスします。
- 対策案については、4つの視点（組織/人/技術/物理的環境）から専門家が事前に案を作成しておきます。
- 当日は、専門家から提示された案をもとに、企業側と実現性や優先順位についてディスカッションを行い、具体的にスケジュール化していきます。

「標準的な進め方」の詳細（４）

第4回　情報セキュリティ対策の成果物レビューと訪問指導全体のまとめ

		企業	専門家	成果物/事務局提供ツールなど
事前準備	1	SECURITY ACTION二つ星宣言の準備	前回訪問時の検討結果を踏まえた実行計画案の修正と更新版の作成(1年程度での実行計画)	-
	2	-	継続した支援の提案作成(可能であれば) 提出依頼資料の準備	-
当日	1	右記のディスカッションと合意 今後の進捗状況のフォロー方法の検討	情報セキュリティ対策実行計画の提示と合意 更なる改善に向けての継続フォローについての提案(可能であれば)	-
	2	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】情報セキュリティ対策実行計画書(コロナ禍対策等を含む) 【成果物】基本方針/関連規程の点検結果 【成果物】自社診断(web版)結果報告 【成果物】SECURITY ACTION二つ星宣言（最終報告書での状況報告）
	3	専門家指導についての評価コメント(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 【成果物】最終報告書

＜**実施のポイント**＞

- 第3回の検討をもとに、専門家は「情報セキュリティ対策実行計画案」を、企業側は「 SECURITY ACTIONの二つ星宣言」の準備を行い、当日は全体の成果物について、レビューと合意を行います。
- 可能であれば、実行計画書の実効性を高めるため、数ヶ月後にチェックポイントを設けるなど、継続した支援活動(有料)の提案を行い、専門家としての次のステップとなる自走化を目指します。
- 計画される情報セキュリティ対策は、経営者が自分事として取り組める実効性と納得感のあるものとします。

３　指導に当たっての留意点

指導先企業への依頼や調整事項

確認・調整事項		依頼・調整のポイント
1	企業側の検討体制(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する ・事業や業務のプロセスに詳しい方 ・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/準備依頼	✓ 会議室/プロジェクター等の環境確認/準備依頼 ・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る ✓ 検討方法は、各専門家のやり方(経験)に委ねる ・原因を掘り下げ、メンバーの納得感と実効性のある対策に結びつける
3	コロナ禍の中での指導環境の調整（コミュニケーション環境） *Web会議ツール *ネットワーク	✓ Web会議ツールの使用経験の有無 ・無し⇒別途事前準備の打ち合わせなどでの試行を提案 ・有り⇒使用中のWeb会議ツール/環境の確認 （企業側の意向に合わせて対応する） ※Web会議の使用ライセンスに要する費用は、専門家(又は企業)の負担となる ✓ コロナ禍の状況によっては、専門家指導をすべてリモート会議で行うことも可能なので、企業側の意向を最優先にして柔軟に対応する。
4	提供を受ける情報の取り扱い *機密保持誓約書	✓ 情報入手に当たっては、指導先企業宛に機密保持の誓約書を提出願います。 ・併せて事務局宛に控えを提出する

初回指導時の留意点

『指導に当たっての心構え/前年度の訪問指導から学べること』参照

✓ 指導する中小企業の特徴/環境を、事前にできる限り理解する。

＊企業のホームページや事前調整の中で得られた情報の整理。
＊特に最初の導入部分をしっかり決めて、相手に伝えること。
・自分は何者で、指導で何をするのか？（事業の主催者の目的と自己紹介）
・今日のテーマは何で、時間はどのくらいで、どういう進め方をするのか？

✓ ヒアリングを通じて、経営者の本音(対策実施の目的)を引き出す。

＊ヒアリングシートの作成等、事前準備をしっかり行う。
＊限られた時間内で、話が脇道に逸れないよう時間管理を行う。
・得られた情報を忘れることが無いようしっかり記録を取る。
・一人でのヒアリングとなるので、可能であれば録音を取らせてもらう。
＊経営者の話を途中でさえぎらず、相手の発言から次の質問をするように心がける。
＊難しいIT関連用語の多用や、技術的な話題に偏らないよう配慮する。
・相手のレベルに合わせて会話する。
＊言葉だけでなく、できる限り映像/図表を使って理解の共有化を図る。
＊一方的に聴くだけでなく、有用な情報提供も交える。
・最近の情報セキュリティインシデントの事例やIPAの提供コンテンツなど。

✓ 中小企業の視点を意識し、経営者の関心事に沿った話題で進行していく。

＊経営資源の不足を前提で考える。（人、金、物、情報、システム）
＊経営者の関心事（売上・利益・販路拡大等）を理解する。
＊情報セキュリティ対策においても、経営者自らのリーダーシップの必要性を強く促す。
＊押し付けでなく、納得感のある対策を経営者自らに導き出してもらう。

初回指導時の留意点　（検討の進め方）

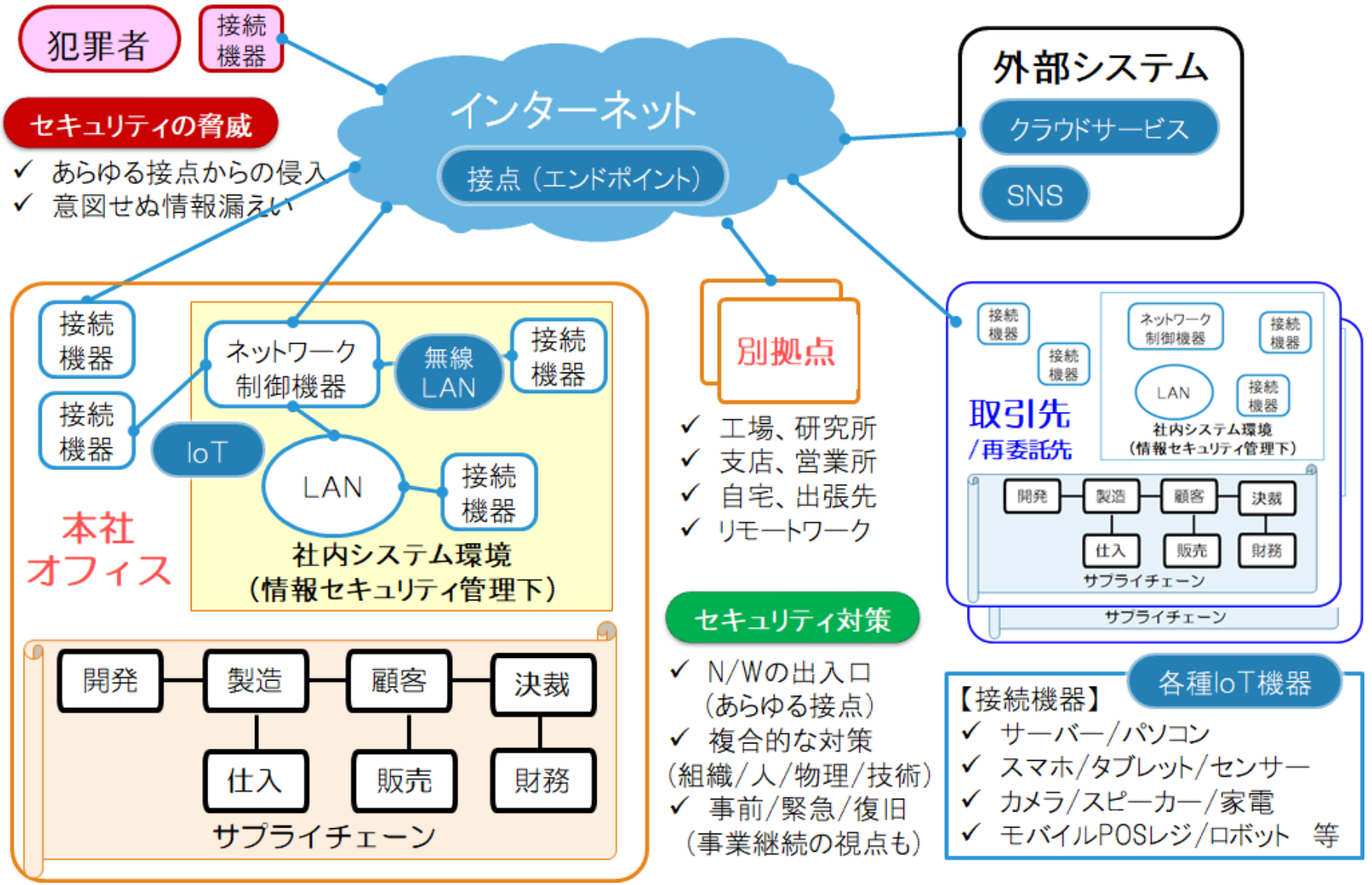
- ✓ 当日の具体的な進行は各指導専門家の経験や手法・スタイルにお任せします。
  ⇒Q&A方式、セッション形式、ファシリテーション、…

- ✓ 各回とも半日（２～３時間程度）の限られた時間ですので、効率的な進行を心がけて下さい。
  ⇒円滑に進めるために事前にタイムスケジュールを組んでください。
  ⇒企業側との合意に基づき、訪問をせずにWeb会議で指導を行うことも可能です。

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 *当日の進め方と準備資料ついての説明と合意 *機密保持誓約書を提出	主催者側としての当事業の目的と、期待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	ヒアリングシートを用いて、内容を聞き漏らすことが無いようにする
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 （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 ⇒できればIPAの映像コンテンツも投影する	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 *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

対策絞り込みの留意点（対策の実効性、継続性）

✓ 指導先企業の事業全体を広範囲に俯瞰・理解した上で、今回の対策検討の対象領域を絞り込んでいく。



対策絞り込みの留意点（対策の実効性、継続性）

- ✓ 検討から対策導入後の運用管理まで、継続的で実効性のある対策となるよう考慮する。
- ✓ 計画される情報セキュリティ対策は、自分事として取り組める納得感のあるものとする。

対策の検討 → 対策の導入 → 対策の運用管理 → 対策の見直し

技術的対策

- ID/パスワード管理
- ネットワーク監視
- アクセス制御
- 脆弱性検知/診断

いつの間にか使われなくなった古いバージョンで役に立たない

導入した対策を継続できるか

物理的対策

- 入退室管理
- 施錠/盗難防止
- 機器/媒体管理

人的対策

- 教育/訓練/資格取得
- 関連情報の周知/徹底
- 誓約書

組織的対策

- 規程/ガイド/PDCA
- 組織/要員配置
- 役割/責任/権限

ルールで縛り過ぎると仕事の生産性を阻害

ルールはあるが、誰も知らない、守られない

幅広い領域での検討と、導入から運用管理までを見据えた検討を進める

導入時のコストだけでなく、運用・維持管理のコストを意識する
特に人に目を向けたコストを意識する

継続的にレベルアップしていけるような仕組みを、組織的対策に組み込む

企業の体力と、情報セキュリティ対策に求められる要件とのバランスを図る

成果物作成の留意点 （要提出の成果物）

『各種ツールの活用方法』参照

	要提出の成果物	留意点
1	「5分でできる情報セキュリティ自社診断(Web版)」による、現状のリスク洗い出し結果	✓ 提出はWeb版だが、集計が容易なEXCEL版を使って、一般従業員、管理者層、経営層の認識のギャップを分析することも検討する。
2	組織的対策の基本となる、情報セキュリティ基本方針と必要な関連規程の点検結果 ※事務局への提出は、基本方針はPDFで、関連規程類は点検結果のExcelの一覧表のみとし、規程そのものの紙やファイルでの提出は不要です。	✓ 基本方針はサンプルを提示して、企業自らが作成し、できる限りホームページなどで外部に開示してもらう。 ✓ 関連規程の点検の中で最低限必要なものを見極め作成計画を具体化する。
3	優先順位付けにより絞り込まれた情報セキュリティ対策の、今後1年程度で実施可能な計画書。（コロナ禍対策を含む）	✓ 継続的に実行(運用)が可能な対策になっているか、またコロナ禍の経営対策に沿ったセキュリティ対策になっているかの面から適切なガイドを行う。
4	SECURITY ACTIONの二つ星宣言 （最終報告書での申請状況報告）	✓ 最終報告書のフォームは、別途事務局より委嘱した専門家に送付します。 ✓ 2つ星申請の状況について、事務局に提出する「最終報告書」の中に記載してください。

成果物作成の留意点（基本方針の作成）

『各種ツールの活用方法』参照

- ✓ 「中小企業の情報セキュリティ対策ガイドライン 第3版」のサンプルをもとに、情報セキュリティ基本方針を作成する。既に作成されたものがあれば、内容に不備・不足が無いか確認し、作成後は、従業員や関係者に文書等で周知・徹底する。
- ✓ 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。

【情報セキュリティ基本方針】

株式会社〇〇〇〇（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

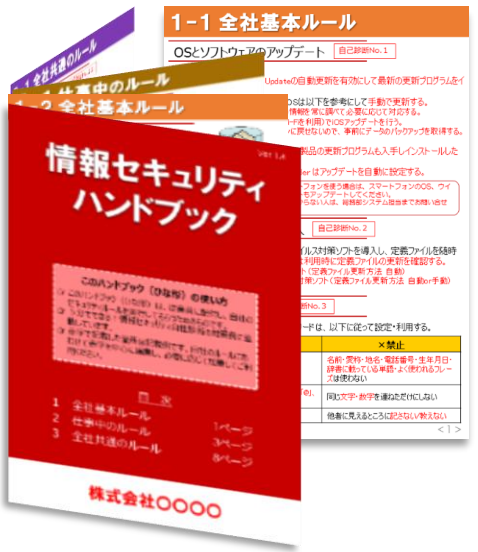
4.法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5.違反及び事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処　し、再発防止に努めます。

制定日:20〇〇年〇月〇日　　株式会社〇〇〇〇　代表取締役社長〇〇〇〇



成果物作成の留意点（関連規程/ガイド類）

『各種ツールの活用方法』参照

以下のIPAのリンク先のサンプルファイルを参考にして、今回の指導実施の結果について記入願います。

情報セキュリティ基本方針の作成は必須です。指導企業先で作成されたものを提出願います。

https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html

*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）

*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）

	関連規程/ガイド類	概要	※今回の見直し（プルダウンメニューで選択）
1	組織的対策	情報セキュリティ管理体制の構築や点検、情報共有などのルールを定めます。	
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を定めます。	
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、破棄などのルールを定めます。	
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を定めます。	
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。	
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を定めます。	
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を定めます。	
8	システムの開発及び保守	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を定めます。	
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。	
10	情報セキュリティインシデント	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を定めます。	
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。	

※以下の選択肢から記入願います。

*新規に作成した（作成予定）

*既存のものを見直し改定した（改定予定）

*特に対応無しと判断した（既存のまま）

*当面は作成の必要なしと判断した

成果物作成の留意点（情報セキュリティ対策実行計画書）

- ✓ 全4回の指導の成果物として「情報セキュリティ対策実行計画書」を作成してください。
  ※今後1年程度の期間で対応できるものに絞り込んでください。

- ✓ 訪問先企業に提示する資料は、各自工夫されたもので構いませんが、事務局宛に指定されたEXCELファイルの様式で記入提出をお願いします。（シート1枚）

プルダウンメニューで選択可

改善分野	現状と課題	具体的改善対策	コロナ禍の対策	絞り込み			実施可否	実施期限	予算、要員等の懸念点
				緊急度	重要度	難易度			
組織的対策									
人的対策									
技術的対策									
物理的対策									

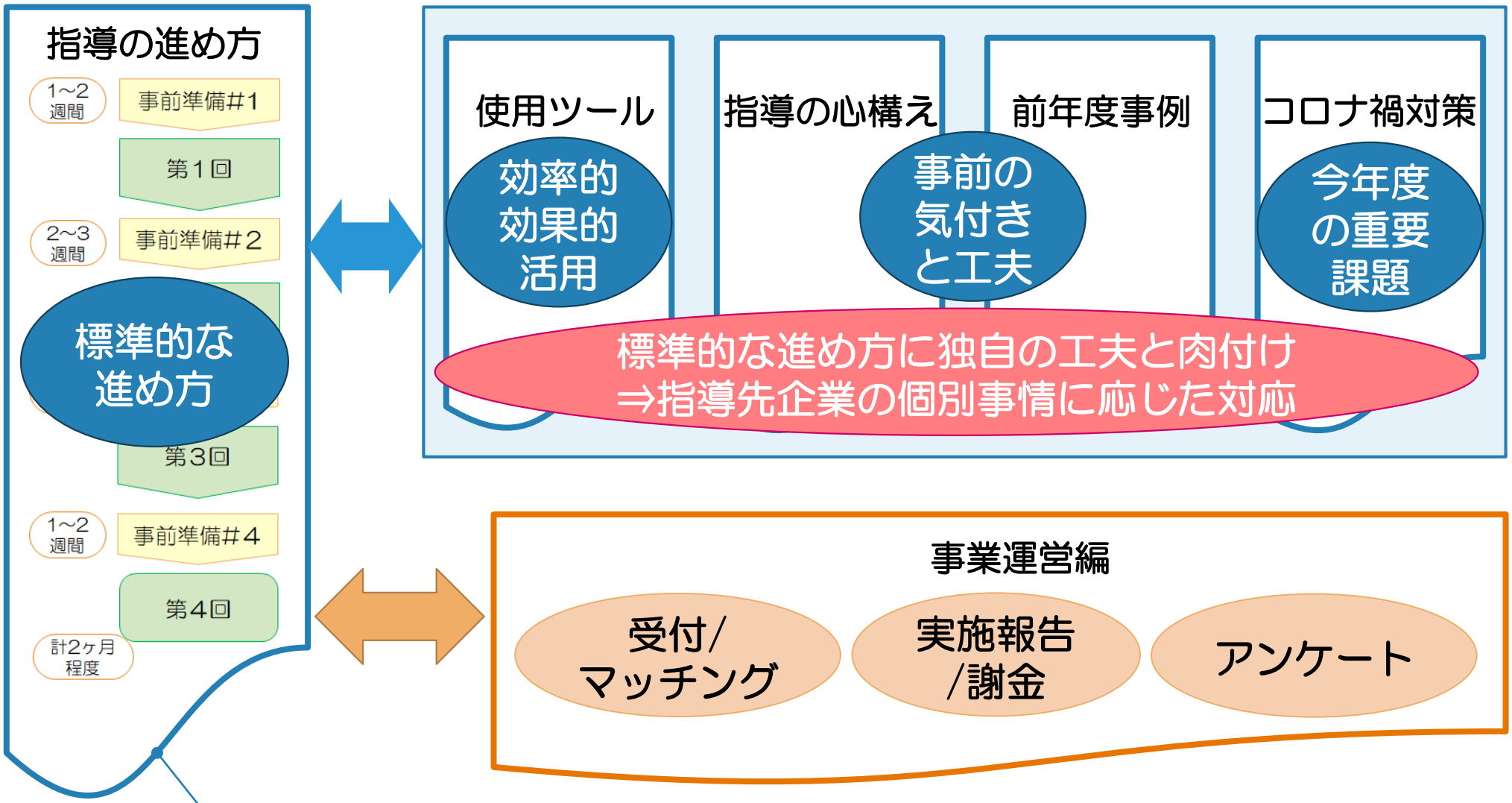
【記入に当たっての注意事項】
1. 実施施策は改善分野ごとに行を追加して記入する。
2. コロナ禍の経営施策に連携した情報セキュリティ対策の場合に、チェック(✓)を入れる。
3. 緊急度(高、中、低)、重要度(高、中、低)、難易度(易、中、難)を評価し、実施の優先順位を判断する。
4. 実施可否を判断し、今後半年～1,2年程度の期間で実施するものを選定する。
5. 予算、要員等、実施に当たっての懸念点を明確にする。

【参考】今年度の専門家指導における前年度との比較

- ✓ 前年度も当事業に参加された方も多くおられると思います。前年度との比較について以下にまとめましたので、ご確認をいただき、今年度も引き続き参加をお願いいたします。
- ✓ 前年度参加を見合わせた皆様にも、ぜひ今年度は積極的に参加いただくようお願いいたします。

項目	前年度との違い	内容の補足
達成目標	前年度とほぼ同じだが、コロナ禍での情報セキュリティ対策を指導内容に追加	●終了後のフォローも含め、専門家としての自走化を、より一層目指す
事務局に提出する成果物	前年度と同じ	●情報セキュリティ対策実行計画書に、コロナ禍の経営施策との関係性を追記
支援対象の企業と前提条件	前年度から対象業種を拡大し、特に36道県地域での企業への支援を増やす	●Security Actionの対象業種が申し込み可能 ●前年と同一の企業への支援はできない
指導回数	前年度と同じく4回 (各回2～3時間程度)	●標準プログラム構成に基づき、指導先企業の状況に合わせて各自工夫する
使用するツール	前年度とほぼ同じ	●5分でできる情報セキュリティ対策自社診断をWeb版で実施（EXCELシートも使用可)
コロナ禍の影響	コロナ禍の情報セキュリティ対策を意識した支援活動とする	●Web会議ツールを積極的に活用し、併せて必要な情報セキュリティ対策をガイドする

まとめ　（他の指導講習コンテンツの活用）



- ✓ 4回の標準的な専門家指導の内容について、具体的な解説を行います。
- ✓ 併せて、指導先企業への依頼/調整事項や、指導に当たっての基本的な留意点を説明します。
- ✓ 他の講習コンテンツの受講により、標準の進め方に肉付けをして、具体的な指導イメージを描き、指導先企業特有の状況に合わせた対応やアドバイスができるよう、工夫をしてください。

パートⅠ　具体的支援の進め方

プログラム②
各種ツールの活用方法

「各種ツールの活用方法」での説明内容

項目		説明のポイント
1	使用するツール/資料の一覧	✓ 各種ツール・資料等のアクセス先 ✓ 事務局への提出物・成果物について
2	使用するツール/資料の内容	✓ ヒアリングシート（カスタマイズ可） ✓ 機密保持契約書 ✓ ５分でできる！情報セキュリティ自社診断 ✓ 中小企業の情報セキュリティガイドライン 第3版 *情報セキュリティ基本方針 *情報セキュリティ関連規程 *SECURITY ACTION 二つ星宣言 ✓ 映像で知る情報セキュリティ ✓ 成果物作成の留意点
3	まとめ	全体のまとめ

1　使用するツール/資料の一覧

使用するツール/資料の一覧

用途	資料/成果物		資料(ファイル)の内容	アクセス先
指導業務時に使用する(参考にする)もの	ヒアリングシート		事業概要と情報管理の現状を理解し、課題整理と目標(期待値)の明確化を行う	IPAのWebサイト ※実施要領 参照
	機密保持誓約書		最初の訪問時に指導先企業へ提出するひな形ファイル *オンライン指導となった場合は、郵送対応	
	IPAの情報セキュリティ普及啓発用資料		以下の資料を指導先企業に持参・提供し、指導に役立てていただく *中小企業の情報セキュリティガイドライン　第3版 *情報セキュリティ5ヶ条 *5分でできる 情報セキュリティ自社診断 *中小企業のためのクラウドサービス安全利用の手引き *はじめましょう情報セキュリティ　SECURITY ACTION	
			映像で知る情報セキュリティ *推奨する視聴映像「あなたの会社のセキュリティドクター」	YouTube IPAチャンネル
	セキュリティプレゼンター向けの IPA提供 各種コンテンツ		セキュリティプレゼンター登録の手続き後に下記URLより様々な普及啓発コンテンツが利用可能 *https://security-shien.ipa.go.jp/presenter/index.html	IPAのWebサイト ※実施要領 参照
	事業説明資料(Eラーニング資料)		専門家指導の具体的な進め方と、効果的な指導を行うための役立つ情報	
事務局へ提出するもの	提出物	機密保持誓約書(写し)	指導先企業へ提出したものの写しを第1回目の実施報告時に添付	
	成果物	① 5分できる 情報セキュリティ自社診断 結果	「5分できる 情報セキュリティ自社診断(Web版)」の結果を提出	
		② 情報セキュリティ基本方針 関連規程の点検結果	作成した情報セキュリティ基本方針および関連規程の点検結果を提出 *「中小企業の情報セキュリティ対策ガイドライン 第3版」の付録(サンプルあり) *関連規程類の作成や見直しに至らなかった場合も点検結果の一覧を提出	
		③ 情報セキュリティ対策 実行計画書	今年度～来年度に向けての情報セキュリティ対策実行計画書を作成・提出	
		④ 最終報告書	SECURITY ACTIONの二つ星宣言の申請状況を確認し、最終報告書に記載	

２　使用するツール/資料の内容

使用するツール/資料の内容　（ヒアリングシート）

	ヒアリング項目	ヒアリング結果(今回の指導で考慮すべき点)
1	訪問先企業の事業内容(業態、製品/サービス、拠点/組織/従業員構成)	
2	業務プロセス(業務の全体像の見える化)とシステム化の状況	
3	顧客/取引先/仕入れ先などのサプライチェーン(事業関係者)	
4	コロナ禍における経営施策と、対応のための情報システム対策	
	*リモートワーク(テレワーク)の実施状況	
5	IT環境と活用状況(特徴的なことの訊き出し)	
	*自社の情報システム構成(事業系システムと社内(管理系)システム)	
	*社内外の情報/コミュニケーションシステムの状況(HP、メール、チャット等)	
	*外部のITサービス(クラウド,SNS)や取引先とのネットワーク接続の状況	
	*主要な情報システムで取り扱っているデータ(種類、量)	
	*IT関連組織体制(開発・保守、運用、ユーザーサポート、障害・事故対応)	
	*IT予算(内、情報セキュリティ関連予算)	
	*従業員のITスキル、リテラシー、情報管理・保護への意識	
	*重要な情報資産(個人情報、営業/特許等)の種類と量	
	*上記の重要情報資産の保管・管理状況(アクセス管理、バックアップ等)	
6	IT活用に関する課題認識と対応	
	*付加価値向上の面から(販路拡大、新規取引先獲得)	
	*使用システムの陳腐化、保守サポート切れ、新技術活用の遅れ	
	*既に計画中/実施中の対策(導入予定の情報システムも含め)	
7	情報セキュリティに関する状況	
	*過去に発生した事故(情報漏えい、詐欺などの被害)と実施した対策	
	*情報セキュリティ事故発生時の対応体制(連絡網、初動・緊急対応)	
	*特に気になっているリスクや、業界・取引先等からの要請(ガバナンス)	
	*計画・実施中の情報セキュリティ対策(研修・訓練、保険加入など)	
	*情報セキュリティインシデントに関する情報の入手先と対策の相談相手	

使用するツール/資料の内容　（ヒアリングシート）

- ✓ 標準のヒアリングシート(EXCELファイル)を提供します。指導先企業向けに各自で適宜追加修正してご使用ください。
- ✓ 喫緊の対策や、経営者が今回のプログラムに対する期待値が明確になるようヒアリングを行ってください。
- ✓ ヒアリングの順序はその場の状況で臨機応変に対応してください。
- ✓ ヒアリングシートをすべて埋めることが目的ではありません。限られた時間の中で、スムーズな進行ができること、重要な確認項目に漏れが無いことを確認するために利用してください。
- ✓ 第１回目のヒアリングにて回答が不明瞭だったり、ヒアリング結果のまとめが不十分だったりする場合には、第2回目指導時の最初に追加の質問や認識の齟齬が無いかの確認を行ってください。

使用するツール/資料の内容　（機密保持誓約書／提出物）

✓ 情報入手に当たっては、機密保持誓約書の提出をお願いします。

【入手する情報（資料）の例】

＊現行の規程/ガイド類
＊主要業務に関する重要データの種類と量
＊情報資産台帳/個人情報管理台帳
＊情報システム/ネットワーク構成図　　など

ＸＸＸ株式会社　　様
（控）専門家指導　運営事務局

ひな型

誓約書

「中小企業の情報セキュリティマネジメント指導業務」の目的達成には、貴社の事業内容と情報システム環境に関する情報を開示していただくことが必要となります。提供いただく情報の取り扱いについて、以下のとおり誓約いたします。

1．訪問を通して知りえた、公開されている情報以外の事業内容（企業・組織・商品・サービスに関わる情報など）並びに情報システム環境（使用機器、ソフトウェア、ネットワーク、データ、利用サービス、情報セキュリティ対策など）の情報について、これを他に漏洩させたり、また盗用させたりすることはいたしません。

2．訪問を通じて作成する資料等に事実と異なる内容の記述は行いません。

3．今回の訪問および資料作成を契機に、情報セキュリティの改善のフォローや追加提案の目的以外で、企業訪問や、メール、文書送付などの営業的な行為は行いません。ただし企業側より要請があった場合は、これに該当しません。

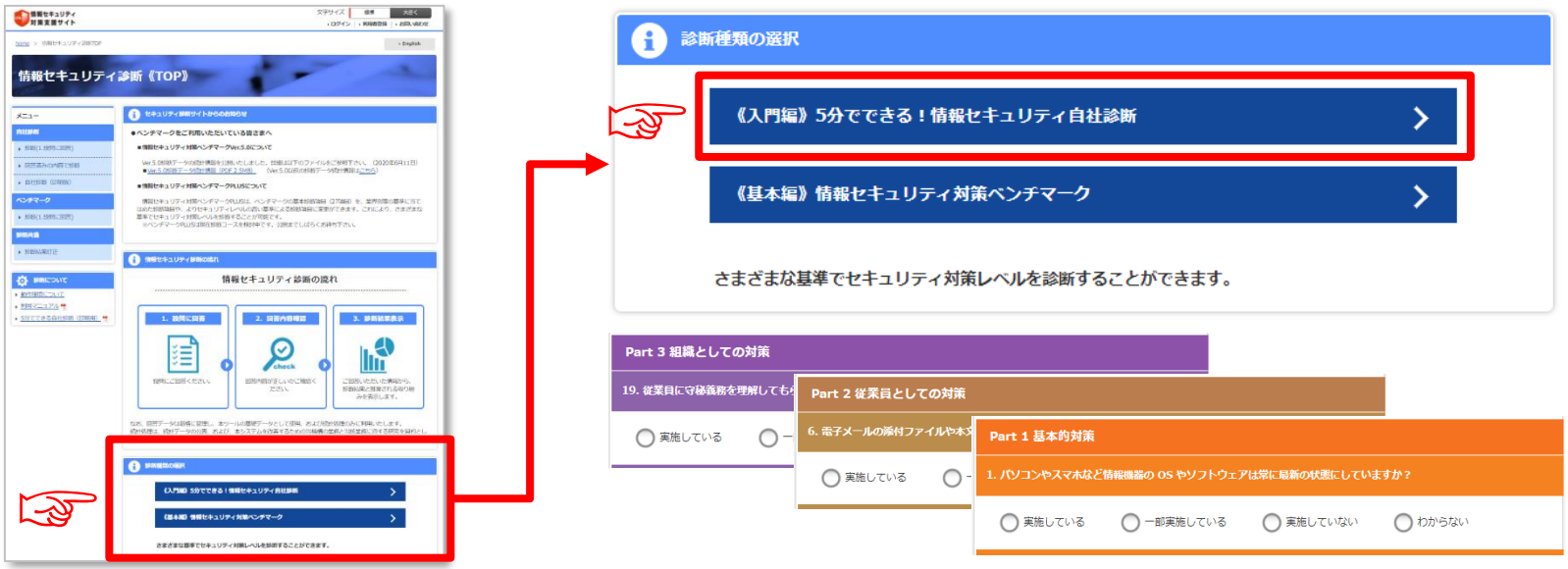
4．成果物は、（独）情報処理推進機構様からの要請に基づく報告資料に使用いたします。

5．その他、善意な市民としての倫理を遵守します。

令和２年　XX　月　XX　日
氏名　　㊞

使用するツール/資料の内容　（自社診断Web版 結果／成果物① ）

- ✓ IPAが提供する「5分でできる！情報セキュリティ自社診断 Web版」を使用します。
  ＊https://security-shien.ipa.go.jp/diagnosis/



- ✓ 第１回目の事前準備として、指導先企業へ自社診断の実施を依頼の上、診断結果を共有してください。診断結果は、ウェブページをPDFファイル化し、成果物として事務局へ提出できるようご準備ください。

- ✓ オンライン版は、ログインをしなくても利用可能です。結果をオンライン上で保存したい場合は、利用者登録が必要です（推奨）。

使用するツール/資料の内容　（自社診断Web版 結果／成果物① ）

- ✓ 第１回目の指導後にヒアリング情報や診断結果をもとに、現状の対策や取組み状況についての分析を改めて行ってください。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、課題の抽出を進めてください。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ってください。

- ✓ Web版の利用が難しい場合は、PDFファイルを印刷して実施してください。PDFファイルは、IPA Webサイトからダウンロードが可能です。

自社診断のための２５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）**
  事務所の安全管理、持ち出し、
  廃棄、電子メール、Web利用など
- **●組織としての対策（7項目）**
  従業員、取引先、ルールなど

- ✓ 必要に応じて、IPA「情報セキュリティ対策ベンチマーク」によるチェックも併せて活用してください。

自社診断実施の留意点

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 ②. 業務外のソフトウェアが勝手に導入されてないか 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 ②.「社長、役員は別」などの例外的な取り扱いはないか 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 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 ②. 設定内容を定期的にチェックしているか 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 ②. 注意喚起が迅速にできる仕組みが整っているか 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む

使用するツール/資料の内容　（情報セキュリティ基本方針／成果物② ）

✓ 「中小企業の情報セキュリティ対策ガイドライン 第3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てください。

⇒https://www.ipa.go.jp/security/keihatsu/sme/guideline/

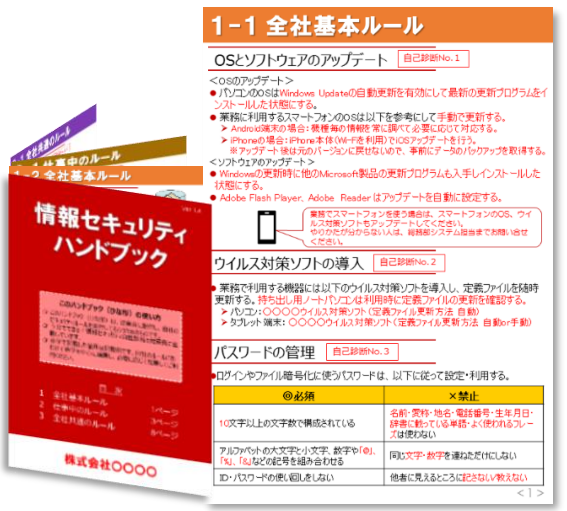
⇒情報セキュリティ基本方針、情報セキュリティ関連規程等

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。



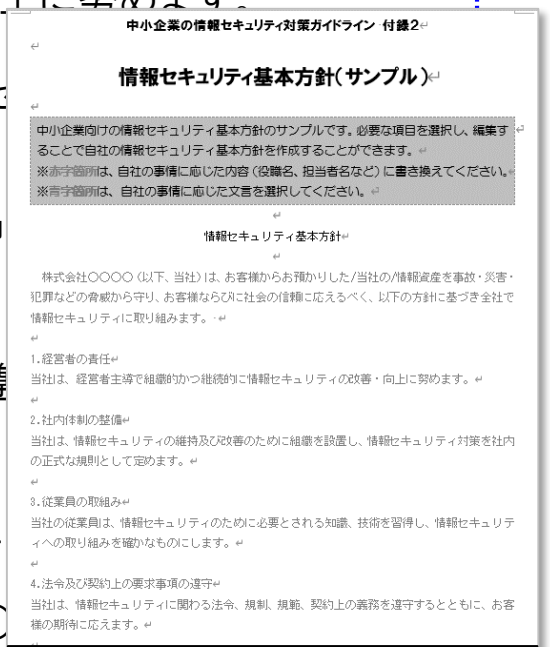
成果物作成の留意点　（情報セキュリティ基本方針／成果物② ）

✓ 既に作成されたものがあれば、内容に不備・不足が無いかの確認をしてください。

【情報セキュリティ基本方針】
株式会社〇〇〇〇（以下、当社）は、お客様からお預かりした／当社の／情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。
2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セ
正式な規則として定めます。
3.従業員の取組み
当社の従業員は、情報セキュリティのために必要とされる知識、技術を習
の取り組みを確かなものにします。
4.法令及び契約上の要求事項の遵守
当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵
の期待に応えます。
5.違反及び事故への対応
当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生
し、再発防止に努めます。

制定日:20〇〇年〇月〇
株式会社〇〇〇〇
代表取締役社長　〇〇〇


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）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
※赤字箇所は、自社の事情に応じた内容（役職名、担当者名など）に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社〇〇〇〇（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み
当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

4.法令及び契約上の要求事項の遵守
当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

情報セキュリティ基本方針（サンプル）

成果物作成の留意点　（関連規程/ガイド類の点検結果／成果物② ）

✓ 情報セキュリティ基本方針以外の関連規程/ガイド類についても、同様に「中小企業の情報セキュリティ対策ガイドライン 第3版」に、ひな形となるファイルが添付されています。必要に応じて見直しや新しく作成することの必要性について検討してください。

	名称	概要
1	組織的対策	情報セキュリティ管理体制の構築や点検、情報共有などのルールを定めます。
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を定めます。
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、破棄などのルールを定めます。
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を定めます。
5	物理的対策	セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
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を定めます。
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を定めます。
8	システムの開発及び保守	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を定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の 機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応ならびに事業継続管理	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を定めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。

成果物作成の留意点　（関連規程/ガイド類の点検結果／成果物② ）

- ✓ 関連規程類の点検結果は、指定の様式に一覧表として作成し事務局へ報告してください。

- ✓ 情報セキュリティ基本方針の作成は必須のため、指導先企業で作成されたものを事務局へ提出してください。
  ＊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）
  ＊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）

	関連規程/ガイド類	※今回の見直し（プルダウンメニューで選択）
1	組織的対策	
2	人的対策	
3	情報資産管理	
4	アクセス制御及び認証	
5	物理的対策	
6	IT機器利用	
7	IT基盤運用管理	
8	システム開発及び保守	
9	委託管理	
10	情報セキュリティインシデント対応ならびに事業継続管理	
11	個人番号及び特定個人情報の取り扱い	

以下の選択肢から記入願います。
＊新規に作成した（作成予定）
＊既存のものを見直し改定した（改定予定）
＊特に対応無しと判断した（既存のまま）
＊当面は作成の必要なしと判断した

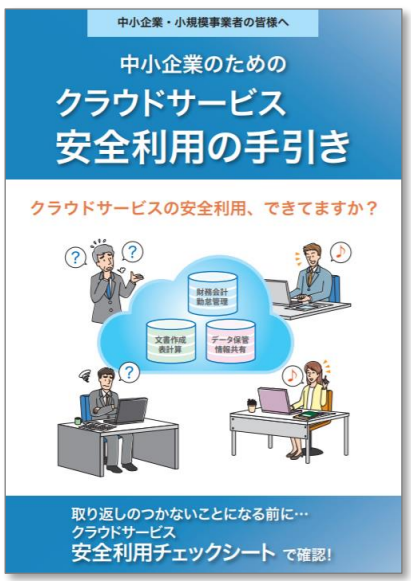
使用するツール/資料の内容　（クラウドサービス安全利用の手引き）

- ✓ クラウドサービスを利用する企業が増加しています。指導先企業の利用状況を確認し、必要な情報セキュリティ対策に取り組んでいるか、安全に利用できているかについての確認を行ってください。

- ✓ 「クラウドサービス 安全利用の手引き」のチェックシートを参考に導入・選定時の留意点や運用・管理のポイントについて確認します。取組みが不十分な場合は、アドバイスを行うと共に、情報セキュリティ関連規程の見直しや今後の実行計画の作成などに取り組んでください。

身近なクラウドサービスの例

- 財務会計、税務申告、給与計算、労務管理などの経営管理アプリケーション
- 顧客管理、販売管理、名刺管理、ホームページ作成などの業務アプリケーション
- 表計算、グループウェア、オンラインストレージなどのオフィスアプリケーション



成果物作成の留意点　（情報セキュリティ対策実行計画書／成果物③ ）

- ✓ 指導先企業が継続的に情報セキュリティ対策に取り組めるよう「情報セキュリティ対策実行計画書」を作成してください。具体的な対策については、今後1年程度の期間で対応できるものに絞り込んでください。

- ✓ 指導先企業に提示する資料は、専門家独自に工夫されたもので構いませんが、事務局への報告には指定の様式で作成してください。

改善分野	現状と課題	具体的改善対策	コロナ禍の対策	絞り込み			実施可否	実施期限	予算、要員等の懸念点
				緊急度	重要度	難易度			
組織的対策									
人的対策									
技術的対策									
物理的対策									

【記入に当たっての注意事項】
1. 実施施策は改善分野ごとに行を追加して記入する。
2. コロナ禍の経営施策に連携した情報セキュリティ対策の場合に、チェック(✓)を入れる。
3. 緊急度(高、中、低)、重要度(高、中、低)、難易度(易、中、難)を評価し、実施の優先順位を判断する。
4. 実施可否を判断し、今後半年～1,2年程度の期間で実施するものを選定する。
5. 予算、要員等、実施に当たっての懸念点を明確にする。

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版 について

- ✓ 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。

成果物作成の留意点　（SECURITY ACTION 二つ星宣言 申請状況確認／成果物④ ）

- ✓ 第4回目の事前準備で、指導先企業へ SECURITY ACTIONの二つ星宣言の申込手続きを進めていただくよう依頼してください。手続きに専門家の支援が必要な場合は、第4回目の訪問指導の中で二つ星宣言の申込手続き完了まで進めていただくことが目標です。

- ✓ 手続き完了日、または手続き完了予定日を確認の上、申請状況について事務局へ報告してください。

- ✓ 二つ星宣言の申込要件として、情報セキュリティ基本方針を外部に公開することが必要です。外部に公開とは、外部の方からお問い合わせがあった際に提示できる状態を求めており、具体的には、自社ウェブサイトへの掲載、会社案内やパンフレットへの記載などの方法を選択いただけます。

使用するツール/資料の内容　（映像で知る情報セキュリティ）

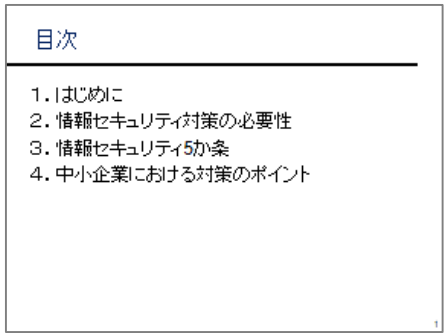
- ✓ 経営者への動機付けとして、IPA製作の映像コンテンツを視聴いただき、補足の解説をしてください。
- ✓ 映像コンテンツは、下記のIPA WebサイトまたはYouTube「IPA チャンネル」から視聴できます。解説資料（PDFファイル）も掲載しています。
  - https://www.ipa.go.jp/security/keihatsu/videos/20170403-3.html
  - https://www.youtube.com/watch?v=OP7O12w6KnQ

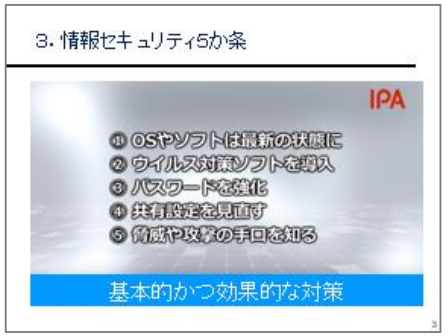
- ウチには機密データはない！
- 情報セキュリティ？
  何に役立つの？
- ITはよくわからないし
  お金がかかるのでしょう？
- 従業員に余計な仕事は
  させたくないヨ！

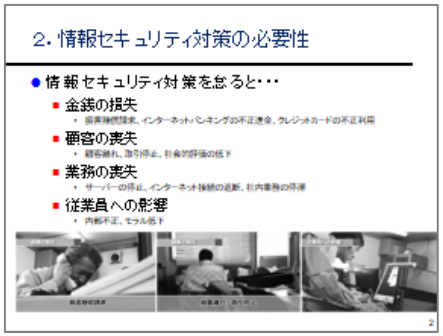
中小企業の情報セキュリティ対策について、その必要性と
今すぐ実践できる対策を人間ドックに見立てて解説します

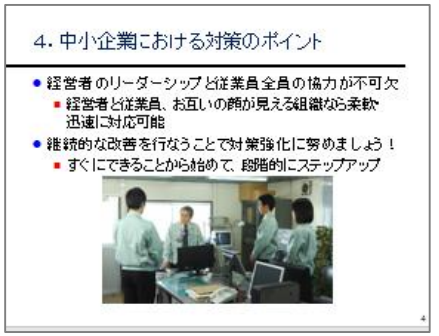
使用するツール/資料の内容　（映像で知る情報セキュリティの解説）

✓ 映像コンテンツの解説資料は、「情報セキュリティ対策の必要性」「情報セキュリティ５か条」などを中心に構成されています。情報セキュリティ対策への意識・意欲向上につながるよう解説をしてください。









✓ 必要に応じて、そのほかの映像コンテンツを視聴・紹介いただくことも可能です。

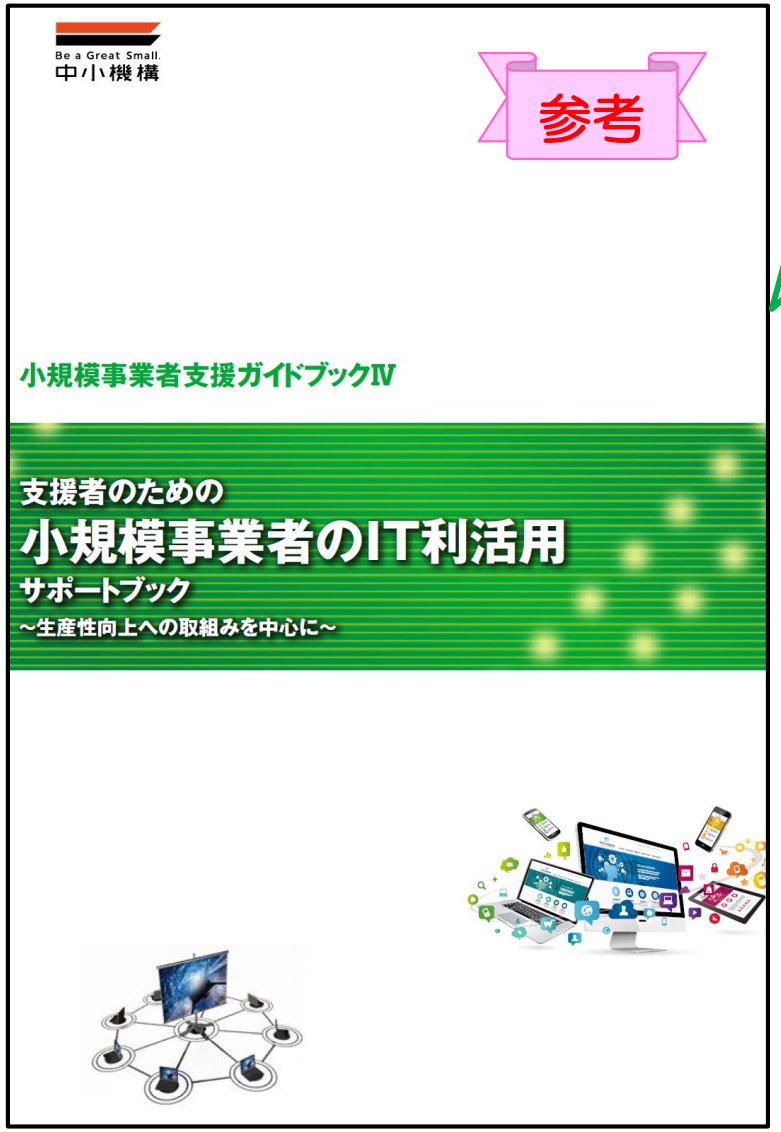
（参考）中小企業向け映像コンテンツ

- あなたの会社のセキュリティドクター -中小企業向け情報セキュリティ対策の基本-
- 寸劇-ぶちあたる前に学べ！あなたの職場の“あるある”セキュリティ事故・対策
- 3つのかばん -新入社員が知るべき情報漏えいの脅威-
- あなたの書き込みは世界中から見られてる -適切なSNS利用の心得-

参考｜セキュリティプレゼンターが利用できる普及啓発資料

✓ IPA Webサイト「情報セキュリティ対策支援サイト」内にセキュリティプレゼンターの活動を支援するための各種普及啓発用資料が用意されています。

参考｜（独法）中小企業基盤整備機構　小規模事業者支援ガイドブック



中小企業のIT活用を指導する上で参考となる資料です。情報セキュリティ対策においても下記の視点を意識して検討を進めてください。

生産性向上 ＝ 付加価値向上 ／ 効率向上

- ✓ できる限り、経営者だけでなく、従業員参画型の取組みとする。
- ✓ 計画される情報セキュリティ対策は、自分事として取り組める実効性と納得感のあるものとする。

【出典】独立行政法人 中小企業基盤整備機構
https://www.smrj.go.jp/tool/supporter/guidebook1/index.html

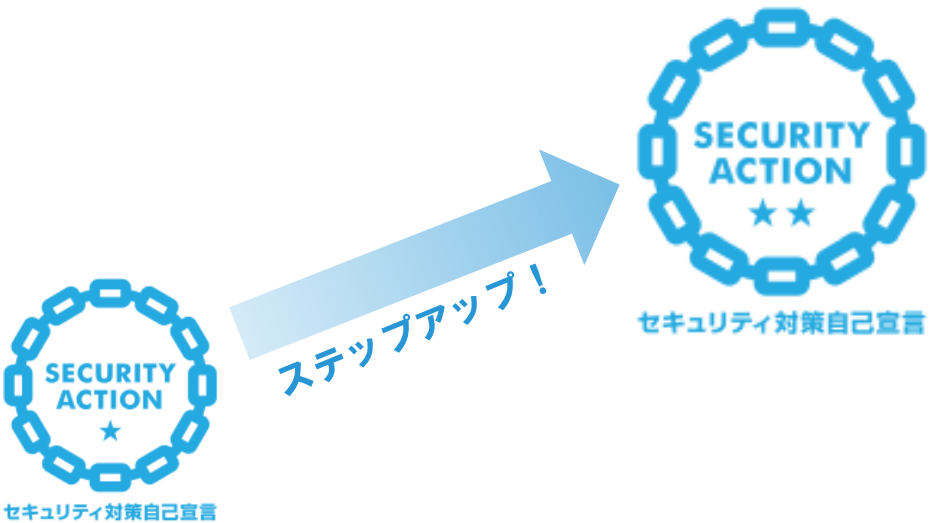
３　まとめ

まとめ

- ✓ 指導を進めるなかで使用するツール・資料については、指導先企業の状況に合わせた活用を行い、情報セキュリティ対策の取組みの推進、レベルの向上を支援してください。

- ✓ 成果物は、指導業務の実施報告に必要なだけでなく、指導先企業が今後も継続して情報セキュリティ対策に取り組むために、有効なものであることが期待されます。専門家としての知見をふまえて、中小企業の強い組織づくりにご尽力いただけるよう本事業への参画をお願いします。

- ✓ 高いスキルを保有する専門家は、得意分野の技術的スキルの活用を盛り込み、経営者と企業側の信頼を得て、将来の自走化に向けた継続的フォローを目指してください。



参考情報（一覧）

- 情報セキュリティ対策支援サイト
  https://security-shien.ipa.go.jp/
- セキュリティプレゼンター支援（普及啓発コンテンツ）
  https://security-shien.ipa.go.jp/presenter/
- 中小企業の情報セキュリティ対策ガイドライン
  https://www.ipa.go.jp/security/keihatsu/sme/guideline/
- 情報セキュリティ診断（5分でできる！自社診断＆ベンチマーク）
  https://security-shien.ipa.go.jp/diagnosis/
- SECURITY ACTION 自己宣言者サイト
  https://security-shien.ipa.go.jp/security/
- 映像で知る情報セキュリティ ～映像コンテンツ一覧～
  https://www.ipa.go.jp/security/keihatsu/videos/
- YouTube「IPAチャンネル」内の 情報セキュリティ普及啓発映像コンテンツ
  https://www.youtube.com/playlist?list=PLF9FCB56776EBCABB

パートⅡ　効果的な訪問指導

プログラム③
指導にあたっての心構え

「指導にあたっての心構え」での説明内容

	項目	説明のポイント
1	日本の中小企業の現状	中小企業のの現状と日本の社会でのサプライチェーン上の位置付け
2	中小企業経営者の関心事	中小企業の経営者が普段関心を持っていることと、 財務諸表（BS・PL・CF）の概要
3	指導先企業を理解する	指導先企業の情報入手と簡易分析
4	効果的コミュニケーション	効果的ヒアリングに向けて （聞くから訊きながら聴くことへ）
5	まとめ	全体のまとめ

1　日本の中小企業の現状

日本の中小企業の現状

１．日本の中小企業とは

（１）中小企業基本法による定義と小規模企業

	中小企業	うち小規模事業者
業種	資本金 または 従業員	従業員
製造業・その他	3億円以下または300人以下	20人以下
卸売業	1億円以下または100人以下	5人以下
サービス業	5,000万円以下または 100人以下	5人以下
小売業	5,000万円以下または 50人以下	5人以下

日本の中小企業の現状

（2）日本の中小企業数（382万社）と従業員数（４，７９４万人）　：（2014年度統計より）

業種		企業数	従業員数
大企業		1万1,000社	1,433万人
中小企業		380万9,000社	3,361万人
	そのうち 中規模企業	（55万7,000社）	（2,234万人）
	そのうち 小規模事業者	（325万2,000社）	（1,127万人）

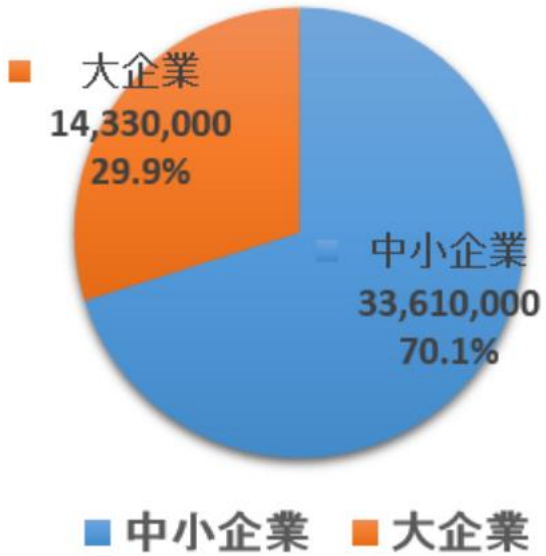
（出典）総務省「平成26年経済センサス－基礎調査」 より

日本の中小企業の現状

１．日本の中小企業とは
（２）日本の中小企業数（382万社）と従業員数（４，７９４万人）
（2014年度統計より）

【企業数】

【従業員数】



１．日本の産業は中小企業によって支えられていると言っても過言ではない
２．日本の産業振興/対策を講じるには、中小企業向けの対策を講じなければならない

（出典）総務省「平成26年経済センサス－基礎調査」 より

中小企業の一般的特徴

２．中小企業の一般的な特徴

（１）強み

①専業の高い技術力

- 「このコトなら任せろ！」との第一人者意識・実現力
- 高い挑戦意識「ヤロウじゃないか！」

②高いコスト競争力

- 管理コスト等が少ないため、コスト競争力が強い

【海外製品とは社会的人件費が異なる（単純比較は困難）】

③迅速な経営判断

- 経営判断までの承認プロセス/関係者が少ない
- オーナー経営者が多く、経営者判断が最優先になる

④柔軟な業務対応力

- 客先の【無理】な要求にできるだけ応じる姿勢がある

中小企業の一般的特徴

２．中小企業の一般的な特徴

（２）弱み

①資金力不足

- 与信力が乏しく銀行借入等が厳しい
- 最新設備投資ができにくい

②最少人員による定常業務の執行：人員/技術等の余裕力不足

- 新技術を取り込む余裕がない
- 一人の担当者が複数業務を兼務している
- 情報システム投資などが後回しになりがちである

③業務の属人化

- 業務処理が文書化されず、担当者任せになりがちである

④従業員の定着率低下

- 従業員が離職しがちで離職率が高い
- 新卒採用の応募がほとんど無い
- 社名/製品のブランド力が弱く、求人しても訴求力がない

⑤事業承継問題の顕在化

- 後継者人材が不足している
- 日本の高度経済成長期に起業した創業者が多く、高齢化している

中小企業のサプライチェーン上の位置付け

３．中小企業のサプライチェーン上の位置付け

（１）サプライチェーン（Supply Chain　「供給連鎖」）とは

①製品の原材料・部品の加工から、製造(組立）/在庫管理/配送/販売/消費までの全体の一連の流れのこと

②最終製品はブランド力のある大企業から消費者に販売されることが多いが、組み込まれている部品や加工/組立/輸送などは中小企業が担うことが多い

（２）サプライチェーン上のセキュリティ管理のポイント

①業務効率化のため、最終製品販売大企業から、部品加工/原材料調達の中小企業まで、ネットワーク接続されていることが多い

②情報を盗もうと企てる悪人は、狙いを定めてネットワーク上の管理の最も弱い企業から、特定のネットワークに侵入する攻撃をしようとする

③中小企業は、一般的に情報セキュリティ対策投資が遅れがちで、悪人がいる国内外から、ネットワーク侵入の入口として狙われることが多い

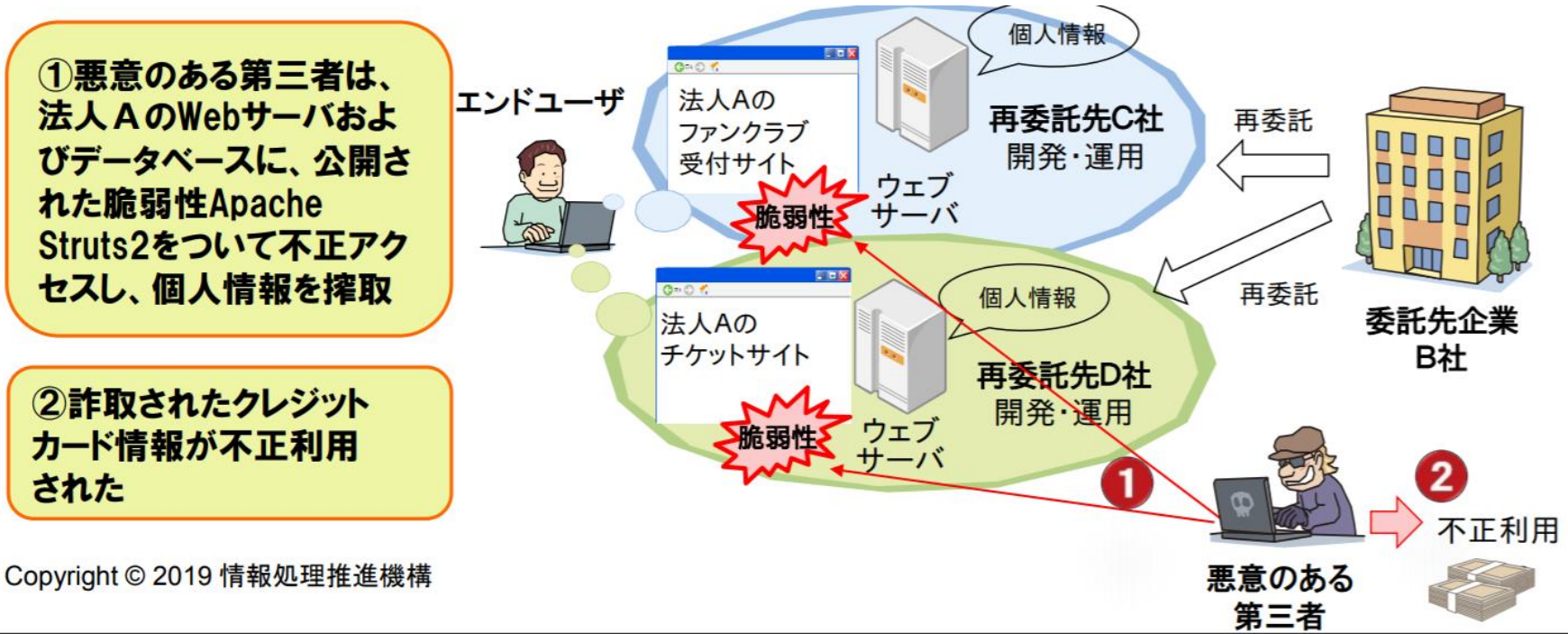
（３）サプライチェーン上のセキュリティレベル

①一番脆弱な企業の管理レベルに全体がなる

サプライチェーン上にある全企業で管理レベルを上げないと効果は少ない。「底上げが必要」

中小企業のサプライチェーン上の位置付け

（4）サプライチェーンのセキュリテイ管理イメージ



IPA 資料より（https://www.ipa.go.jp/files/000073868.pdf ）

ポイント

1．中小企業はサプライチェーンで大企業と一つのネットワークで繋がっている
全体セキュリテイ管理レベルは一番脆弱な企業に合わされる
2．中小企業は全体を考慮して、自社のリスク管理に適正なセキュリティ対策を講じなければならない

２　中小企業経営者の関心事

中小企業　経営者の一般的関心事

2．中小企業経営者の一般的関心事

（１）一般的的に中小企業経営者は、以下を第一優先項目として配慮

①企業永続的存続

- 常に企業を存続させ、「従業員の雇用確保」「取引先との良好な関係維持」「地域への貢献」等に配慮している
- 「従業員の雇用確保」‥家族を含め生活資金を提供する責任を持つ
- 「取引先との良好な関係維持」‥公平な利益分配で共存共栄を目指す
- 「地域への貢献」‥自社の製品やサービスが地域社会貢献していることへの自負/良き市民でありたい

②利益追求

- 「いくら儲かるか/儲かっているか？」が最優先

③資金繰り

- 「いくら手元に現金があるか？」「支払い予定日に現金は足りるか？」
- 現金が不足すると、「信用失墜」し「企業倒産」に繋がる
  「決算上黒字」でも「現金不足」すると「黒字倒産」になることがある
- 「信用失墜」だと「納入後払い方式」が断られ「注文時先払い方式」を要求されることはある

④人材の育成

- 後継者の育成　　・経営者の「片ウデ」の育成

中小企業　企業理念

（２）企業理念

- 企業は目指すべき方向性を示すが、中小企業では設定されていないことが多い
- 経営目標と達成のための戦略と戦術
  経営目標：年度毎などに達成すべき数値目標
  戦略（STORATEGY）：経営目標等を達せるための基本的方針
  戦術（TACTIC S）:具体的行動計画
- これらを従業員に示して、企業として一体感を高めている
  中小企業では、売上目標を示していることが多い
  （情報セキュリティについては具体的目標を示している企業はほとんどない）

１．中小企業の経営者は「情報セキュリティ対策」を常に配慮していることはマレである

（３）財務諸表

年度毎に必ず作成して税務署等に提出し、納税する。（決算後2か月以内）

・個人事業者は12月末日で計算をして、個人所得として税務申告をする

①貸借貸借対照表（BS: Balance　Sheet ）

・企業の全資産の状況をまとめた一覧表である。

・右側（負債＆資本）の名目で調達した資金が、左側（資産）の形になっている。

【貸借対照表】　（例）

資　産		負　債	
流動資産	15,000,000 円	流動負債	5,000,000 円
現金預金	8,000,000 円	買掛金	3,500,000 円
受取手形	2,000,000 円	短期借入金	1,500,000 円
売掛金	4,000,000 円	固定負債	15,000,000 円
商品	1,000,000 円	長期借入金	15,000,000 円
固定資産	15,000,000 円	純資産	
土地	10,000,000 円	株主資本	8,000,000 円
建物	3,000,000 円	資本金	8,000,000 円
機械	2,000,000 円	利益余剰金	2,000,000 円
		繰越利益剰余金	2,000,000 円
合　計		合　計	
	30,000,000 円		30,000,000 円

資本で築いた資　産

他人の資　本

自己の資　本

資産の合　計

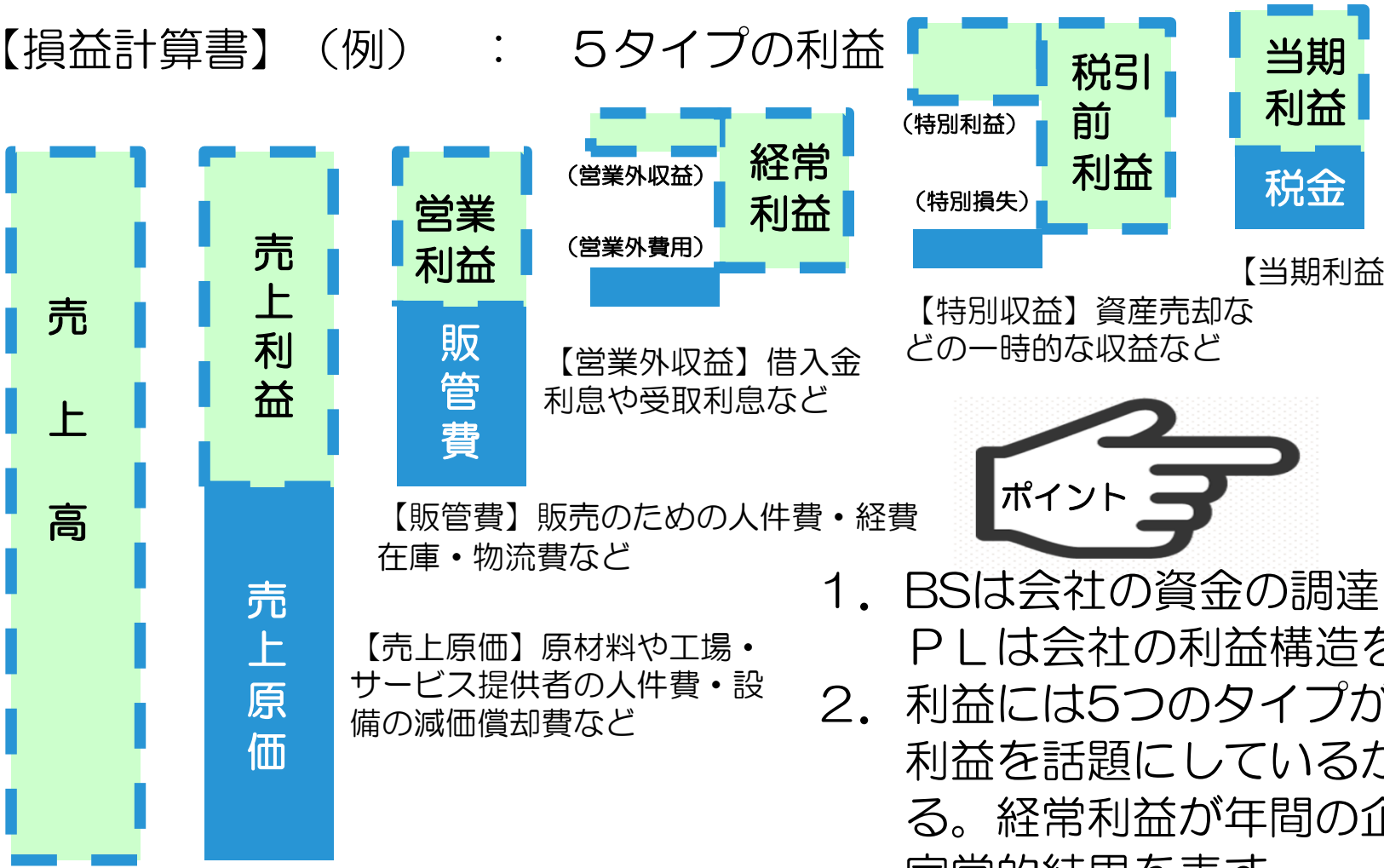
資本の合　計

（３）財務諸表

②損益計算書（PL:　Profit　&　Loss　Report　）

・年度内での資金の流れを示す

【損益計算書】（例）　：　５タイプの利益



【販管費】販売のための人件費・経費
在庫・物流費など

【営業外収益】借入金利息や受取利息など

【特別収益】資産売却などの一時的な収益など

【当期利益】当期の純利益

【売上原価】原材料や工場・サービス提供者の人件費・設備の減価償却費など

1．BSは会社の資金の調達と運用を示し、ＰＬは会社の利益構造を表す

2．利益には5つのタイプがあり、どの利益を話題にしているか、明確にする。経常利益が年間の企業活動の定常的結果を表す

財務諸表

（３）財務諸表

②キャッシュフロー【会社は株主資本移動表を税務署に毎期提出】

- 企業の立場での現金の残高を示す
- （前期末現金残高）＋（今期中現金増加分）－（今期減少分）
  ＝　（今期末現金残高）
- ３タイプのキャシュフローと代表的管理手法がある

①営業活動によるキャシュフロー

- 本業でのキャッシュの流れで、企業がキャッシュを生み出す能力を表す
- プラスの場合、本業から生み出したキャッシュで投資や、借入金の返済原資も確保できるので、望ましい状態
- マイナスの場合、投資を自己資本でできず、借入の返済原資がない

②財務活動によるキャシュフロー

- 金融機関からの資金調達・返済および株式発行による資金調達・配当金の支払、社債発行による資金調達・償還などの財務状況を表す
- プラスの場合は金融機関からの借入金や社債発行で資金を調達した
- マイナスの場合は金融機関からの借入金の返済、社債の償還をした

③投資活動によるキャシュフロー

- 固定資産や投資有価証券などの投資の購入・売却によるキャッシュの流れ
- プラスの場合は、投資した資産を売却してキャッシュを得た
- マイナスの場合は投資をして資金が支出した（継続的投資が望ましい）

財務諸表

（３）財務諸表

②キャッシュ・フロー

管理手法：フリーキャシュ・フロー

・（フリーキャッシュ・フロー）　＝
　　【営業キャッシュ・フロー】　＋　【投資キャッシュ・フロー】

・企業が自由に使用できる余剰資金のを表す

・プラスであることが望ましい

・マイナスの場合、手元のキャッシュが減少していることを表す

１．年度毎に必ず　貸借対照表・曽根喜計算書・株主資本移動表(会社の場合）を作成し、税務処理をしなければならない。企業にとっての財務基本情報になる

２．資金繰りの基本として、キャシュ・フローの管理をして現金の残高を正確に管理する必要がある

３．フリーキャクシュ・フローのプラスを目指す

３　指導先企業を理解する

指導先企業・業界を理解する

※　指導先企業は必ず事前に理解しておく

（１）指導先企業を理解する

・ホームページの検索から企業を知る

・国税庁の法人番号公表サイトから企業登記情報を知る

https://www.houjin-bangou.nta.go.jp/

（２）業界を理解する

・会社名だけでなくお客様の申込書やＨＰから業界を理解する

（企業の一番大きい売上製品・種類が属する業界）

（総務省の日本標準産業分類で分類されている業界）

https://www.soumu.go.jp/toukei_toukatsu/index/seido/sangyo/02toukatsu01_03000044.html

・指導先企業の業界を理解する情報源

① インターネットから（業界動向など）

② 書籍（例：日経業界地図20XX）から

③ 業界団体・同業他社のHP情報から

訪問先企業の簡易分析をする

（3）簡易的　企業分析をする

（例）３Ｃ分析

①Company　自社環境分析

- 理念やビジョン
- 事業（業界）や製品の特徴/競争力
- 現有リソース（ヒト/モノ/カネ）
- 経営者のプロフィール‥等

②Customer 市場環境分析　顧客の市場分析

- 市場規模/成長性/市場環境
- 顧客の消費動向/ニーズ
- 顧客の価値観（求める機能/性能/品質/価格/サービス等）‥等

③Competiter　競合分析

- 競合会社/製品との比較（機能/性能/品質/価格/サービス等）
- 競合のアピールポイント/特徴と対抗アピールポイント/特徴
- 参入障壁
- 競合の今後の戦略/戦術‥等

から、指導先企業の市場価値（ポジショニング）を理解し戦略・戦術を理解する

他の分析手法でも良い　①SWOT分析　②４Ｐ分析　など

4　効果的コミュニケーション

ヒアリングに当たっての心構え（１）

①人間関係の構築
警戒感をほぐす

②信頼感を得る
言動（アイコンタクト）の印象

③相手の理解を深める
出来るだけ予備知識を持って

④相手の現状を訊きとる
現在の最大の関心事等

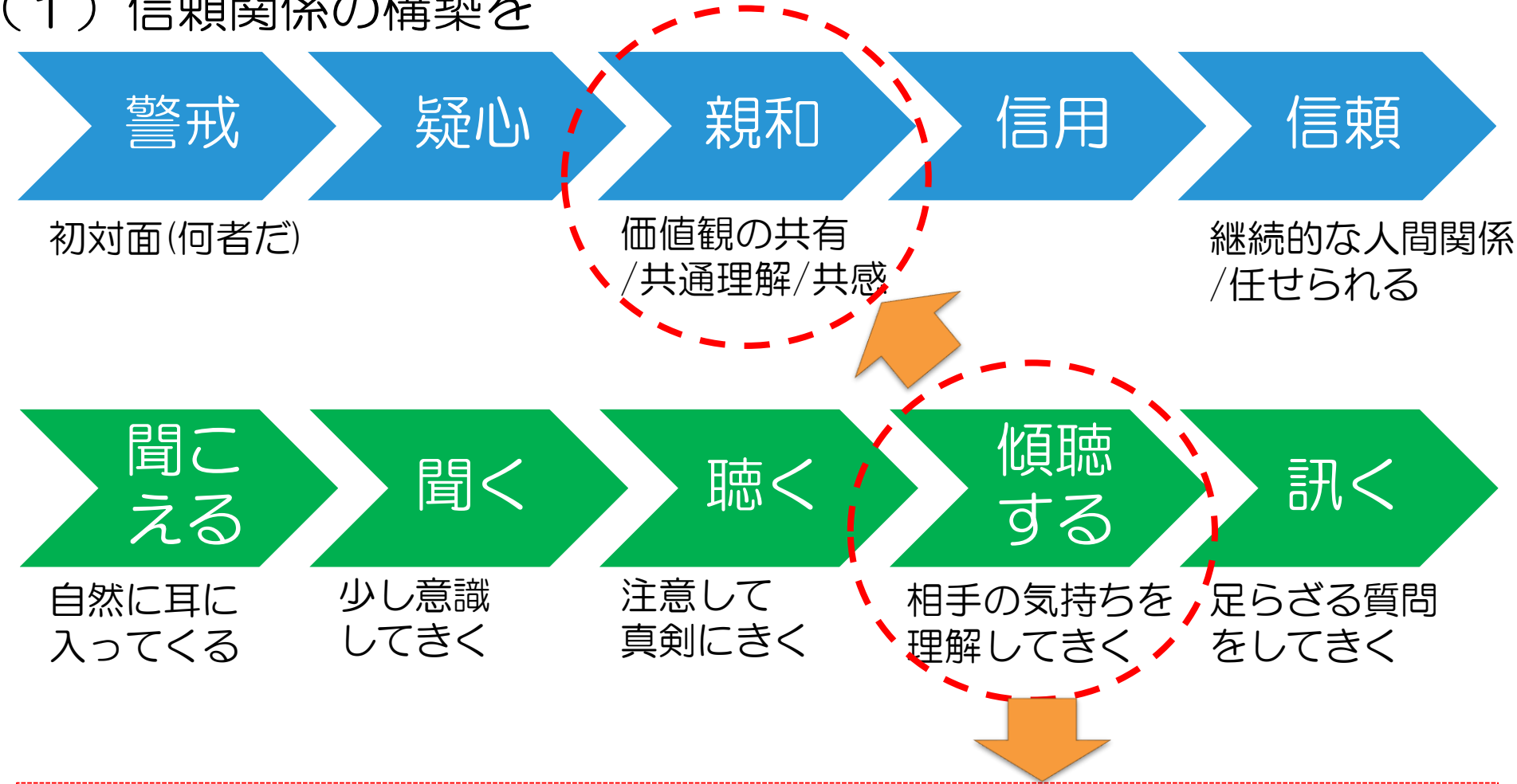
⑤相手の希望を引き出す
どのようになりたいか

基本姿勢

①相手を敬う
②相手の発言を遮らない
（最後まで話させる）
③相手に話させる
（聞くことに徹する）
④無用の議論を避ける
（持論を強調しない）
⑤相手から引き出す
（相ヅチをうつなど）
⑥一項目ずつ確認をする
（一時に多くのテーマに触れない）

ヒアリングに当たっての心構え（2）

（１）信頼関係の構築を



共感的に聞いており、じっくり話を聞いているあいだも、ボディランゲージや声の調子などを熱心に観察し、言葉以外のサインを読みとっている。そして言葉の裏に秘められたメッセージを察知している。

傾聴力/共感力を高めるために

（２）共感とは

相手の意見や行動、感情等をそのとおりだと自分のもののように感じる
この人だったら信頼でき、理解してもらえる（分かってもらえる）

具体的手法
①相手の話を中断させず、最後まで聴く
②あいづち、うなづき、繰り返し、アイコンタクトで自分の気持ちを表現する
③相手の言葉や動作（声の調子やスピードなど）に合わせる（ペーシング）
④相手の感情や雰囲気に合わせる（例：困りました→困られたのですね）
⑤相手と同じ動作をする（ミラーリング）
⑥態度に気を付ける（腕組み/脚組みを解く、手を休める、体を向ける）
⑦相手の価値観を尊重する
⑧相手の想いを受け取る
⑨ニュートラルな立場で聴く
⑩相手の話を要約して投げ返す

質問力を高めるために

（３）質問力

２つの質問のタイプを使い分ける

	クローズド・クエスチョン	オープン・クエスチョン
特徴	相手から回答を引き出す質問（回答は一言になりやすい）	相手に気づきを与える質問
	YES/NOで答えられる(一言になりやすい)	YES/NOで答えられない(説明になりやすい)
	具体的な事象や数値などを確認する質問	WHAT（なに）・WHY（なぜ）・HOW（どうやって）・WHO（だれ）など５W1Hの質問
	答える側の自由度が低く、会話は広がりづらい	答えの自由度が高いので、会話が盛り上がりやすい
	答える側は考える要素が少ないので、信頼関係が成立していない相手にも答えやすい	信頼関係がない相手にオープンクエスチョンをされると、情報をさらけ出すことに警戒心を覚えたりする
質問の例	＊創業して何年になりますか？ ＊従業員は何人ですか？ ＊日曜日は定休日ですか？	＊どうすればもっと売れるとお考えですか？ ＊いま最大の関心事は何ですか？ ＊将来どのような会社にしたいですか？

ジョハリの窓を参考にした質問の投げかけ方

		受け手が 分かっている	受け手が 分かっていない
聞き手が	分かっている	**開かれた窓** ・顕在化している情報を事前にまとめ確認する ・クローズド型の質問 ・事前に質問集を作る	**気付かない窓** ・情報提供型の質問 ・オープン型/クローズド型の質問を組み合わせる ・話しすぎにならないように注意
	分かっていない	**隠された窓** ・潜在化している情報を紳士的に積極的に訊く ・オープン型の質問 ・キーワードを連鎖させる	**未知の窓** ・潜在化要件を早く顕在化させる ・オープン型/クローズド型の質問を組み合わせる ・仮説を立て質問する

※ジョハリの窓：心理学者のジョセフ・ルフト（Joseph Luft）氏とハリントン・インガム（Harrington Ingham）氏の両名によって1955年に考案された概念。自分による自分の分析結果と、他人による自分の分析結果から、自分自身の特性を「4つの窓」（開放、盲点、秘密、未知）に当てはめ、対人関係の進展や自己理解に役立てる。

相手の話を最後まで聴く

（５）効果的ヒアリング

【聞く】と【聴く】【訊く】の違い

- 聞こえてくる（耳に入る）‥‥聞く
- 尋ねる‥‥‥‥‥‥‥‥‥‥‥‥‥訊く
- 共感/興味を持って訊き出す（記憶に残る）‥聴く

効果的な質問をして、相手の話を最後まで聴く

１．心を開いて効果的なコニュニケーションをする
①信頼を得る　　②共感をする
③隠された窓/未知の迄領域の質問をする(ジョハリの窓)
④【聴く】ことに専心する
を実践する

５　まとめ

まとめ

経営者にとって　あなたが役に立つ　ことを目指してください

（１）経営者には、常に【尊敬】をもって接してください

①多くの従業員を雇用する重大な役目を担っています

②経営の卓越した実践者ですが、ＩＴ（情報セキュリティ）についてはあまり経験・知識を持っていないことが通常です

③説明（会話）には、IT用語（カタカナ用語/アルファベット頭文字用語等）を極力避け、漢字用語を使って説明してください

④情報漏洩や情報セキュリティに関する時事問題（新聞ネタ）を、易しく2～3分で解説をして、雰囲気を和らげてください

⑤訪問先に見合った事例を紹介し、見合った提案をしてください。大企業での理想形を求め過ぎないで、手の届く現実的な提案をしてください

⑥【いい提案だけど、ウチには要らない】と断れないように

・断る時の　【3つの】不Ｘ　に注意してください

①　不要・・必要性が理解できない　　②　不急・・今でなくても良い

③　不信・・あなたの話が正しいと思わない

⑦情報セキュリティの専門家として専門性を磨き/知識をつけ、相手から尊敬され、【もう一度会っても良い】と思われる専門家になりましょう

そのために、常に自己研鑽して、知識を吸収しましょう

パートⅡ　効果的な訪問指導

プログラム④
前年度の訪問指導から学べること

「前年度の訪問指導から学べること」での説明内容

	項目	説明のポイント
1	中小企業の情報セキュリティの現状と課題	中小企業の情報セキュリティ対策の状況と抱えている課題からの指導にあたっての留意事項
2	前年度の指導の全体像	指導先企業の業種、規模、役職、体制、参加目的から見える指導にあたっての留意事項
3	前年度の具体的指導事例の紹介	2社の事例について工夫した点を中心に説明
4	前年度のアンケートから参考にできること	前年度の指導先企業からのアンケート結果から見える指導にあたっての留意事項
5	まとめ	全体のまとめ

1　中小企業の情報セキュリティの現状と課題

中小企業の情報セキュリティの現状と課題

(1) 体制

全体：「組織的には行っていない（各自の対応）」50.2%、「兼務だが担当者が任命されている」31.0%

小規模企業　　：「組織的には行っていない（各自の対応）」57.5%
中小企業（100 人以下）：「組織的には行っていない（各自の対応）」43.7%
中小企業（101 人以上）：「兼務だが担当者が任命されている」56.4%

情報通信業と金融業・保険業以外の業種では、
「組織的には行っていない（各自の対応）」が最も多く、多くの企業で担当者が任命されていない。

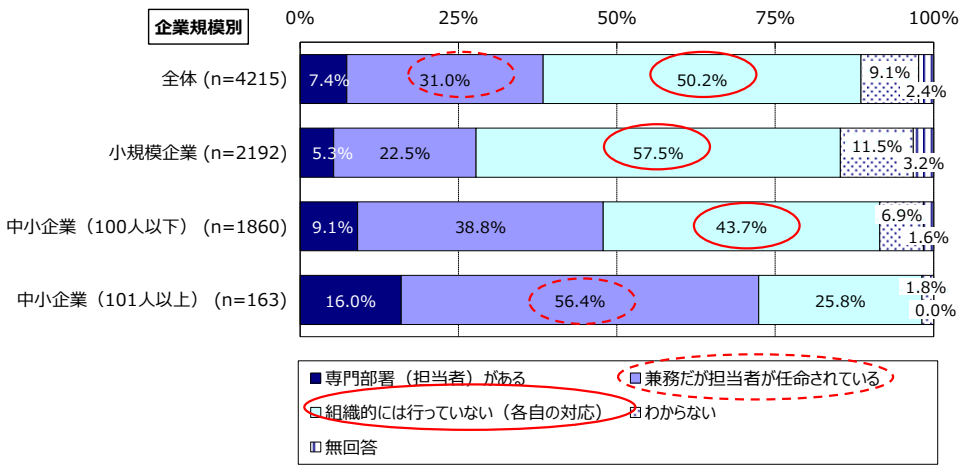


図 2-115　体制（企業規模別）

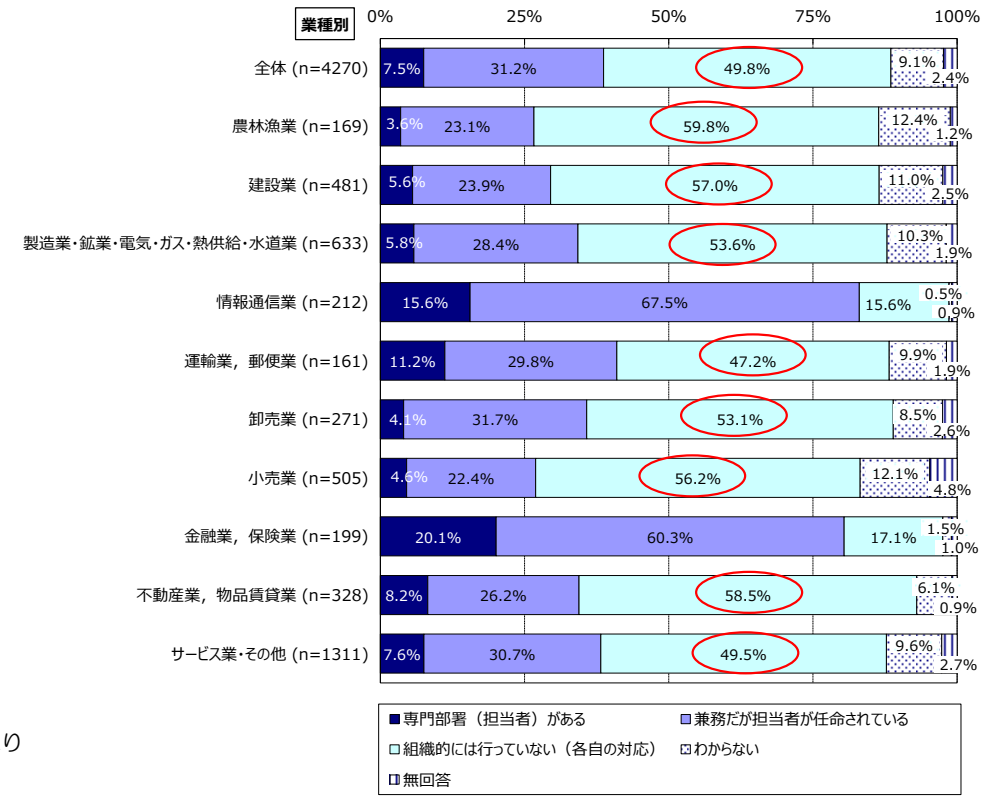


図 2-117　体制（業種別）

IPA「2016 年度中小企業における 情報セキュリティ対策の実態調査- 調査報告書 -」より

中小企業の情報セキュリティの現状と課題

(2) 情報セキュリティ教育

全体：「特に実施していない」60.8%、
「関連情報の周知（社内メール・回覧・掲示板など）」
24.9%、「社内の研修や勉強会」17.3%

小規模企業　　：「特に実施していない」70.5%
中小企業（100 人以下）：「特に実施していない」52.6%
中小企業（101 人以上）：「関連情報の周知」61.3%

情報通信業と金融業・保険業以外の業種では、「特に実施していない」が最も多い。

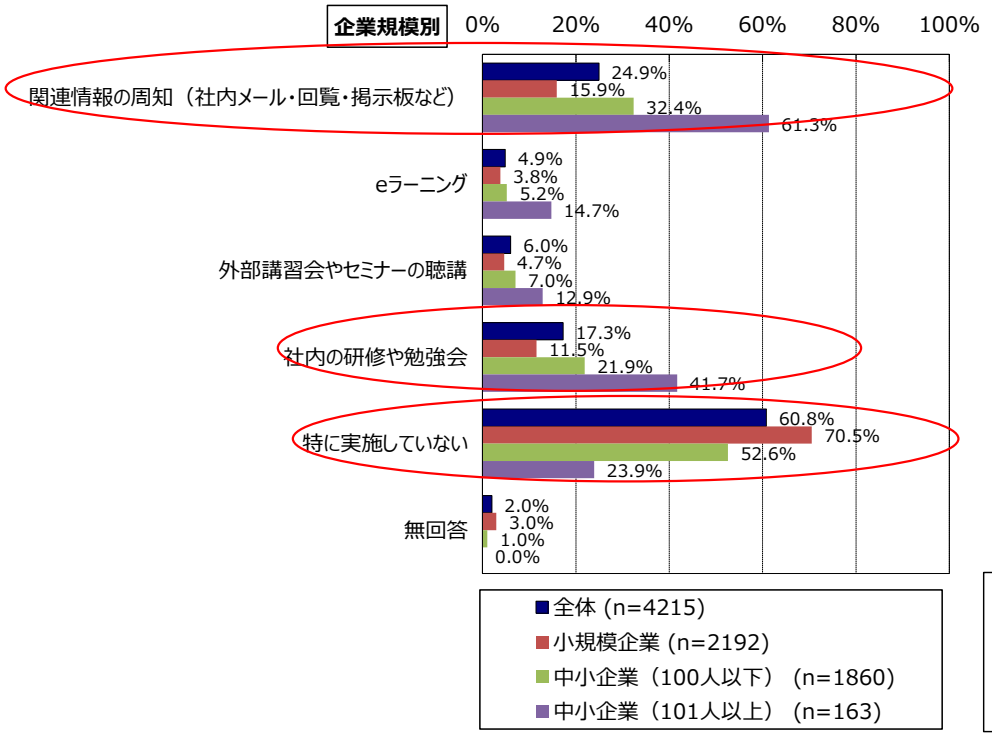


図 2-128　情報セキュリティ教育（企業規模別）

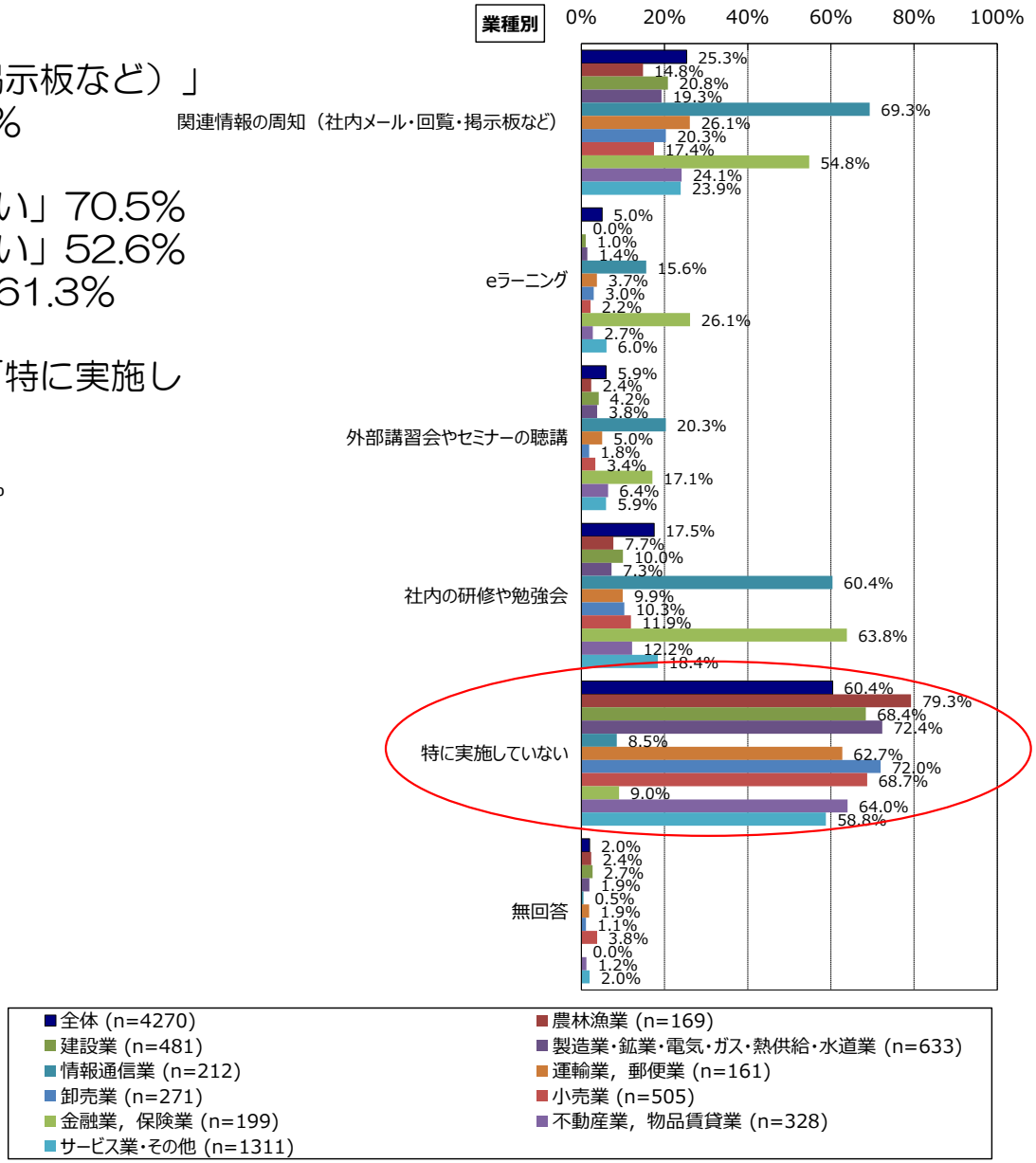


図 2-130　情報セキュリティ教育（業種別）

IPA「2016 年度中小企業における 情報セキュリティ対策の実態調査- 調査報告書 -」より

中小企業の情報セキュリティの現状と課題

(3) 情報セキュリティ対策投資

全体：「IT投資に対策投資を含む」79.4%、
「対策投資額100万円未満」76.2%　　79.4 × 76.2 ＋（100 − 79.4）＝ 81.1%

「対策投資額100万円未満（投資していないを含む）」
小規模企業　：77.0 × 87.7 ＋（100 − 77.0）＝ 90.5%
中小企業（100 人以下）：80.4 × 71.9 ＋（100 − 80.4）＝ 77.4%
中小企業（101 人以上）：86.0 × 42.3 ＋（100 − 86.0）＝ 50.4%

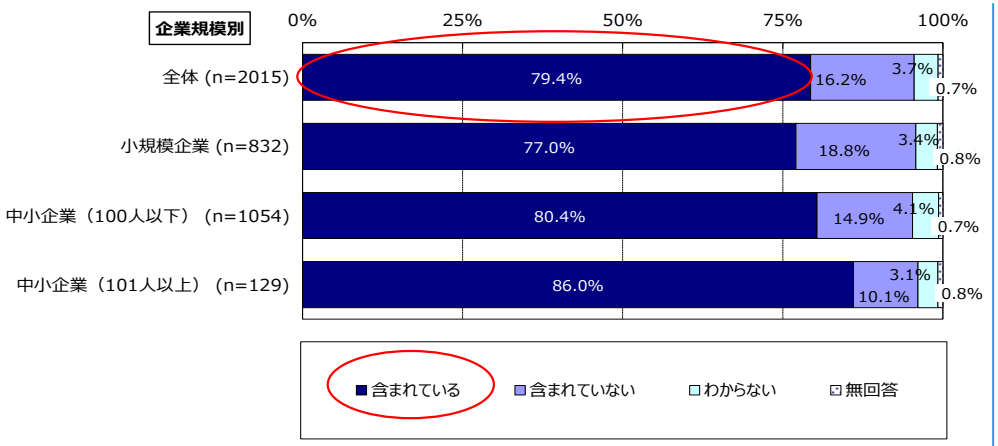


図 2-80　情報セキュリティ対策投資の有無（企業規模別）

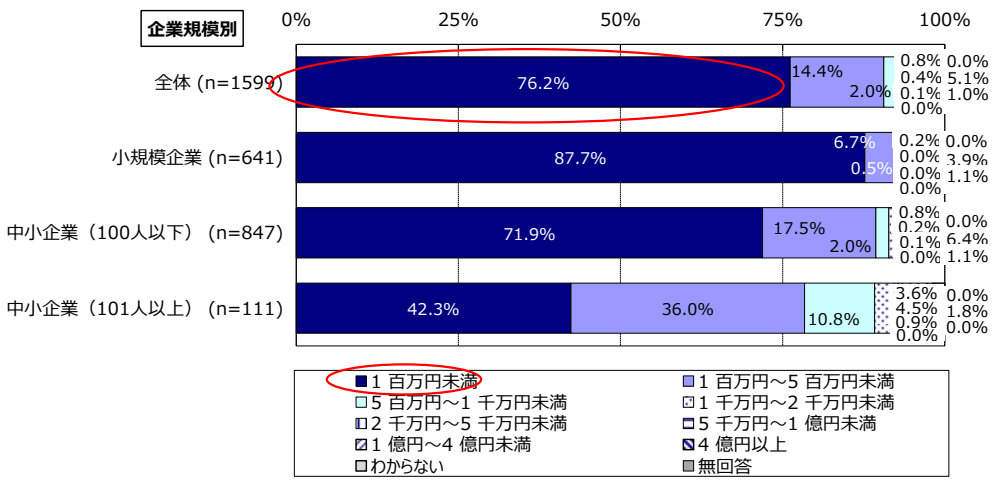


図 2-83　対策投資額（企業規模別）

IPA「2016 年度中小企業における 情報セキュリティ対策の実態調査- 調査報告書 -」より

中小企業の情報セキュリティの現状と課題

(4) 情報セキュリティ対策の取組み状況

SECURITY ACTION 自己宣言事業者で

「ほぼ実践できている」、「十分ではないが実践している」
「重要情報の定期的バックアップ」84.6%
「不審な電子メール受信時のルール決め、対策製品活用」74.5%
に対して
「情報セキュリティに関する規程、手順書を策定する」30.9%（1～5名では23%）

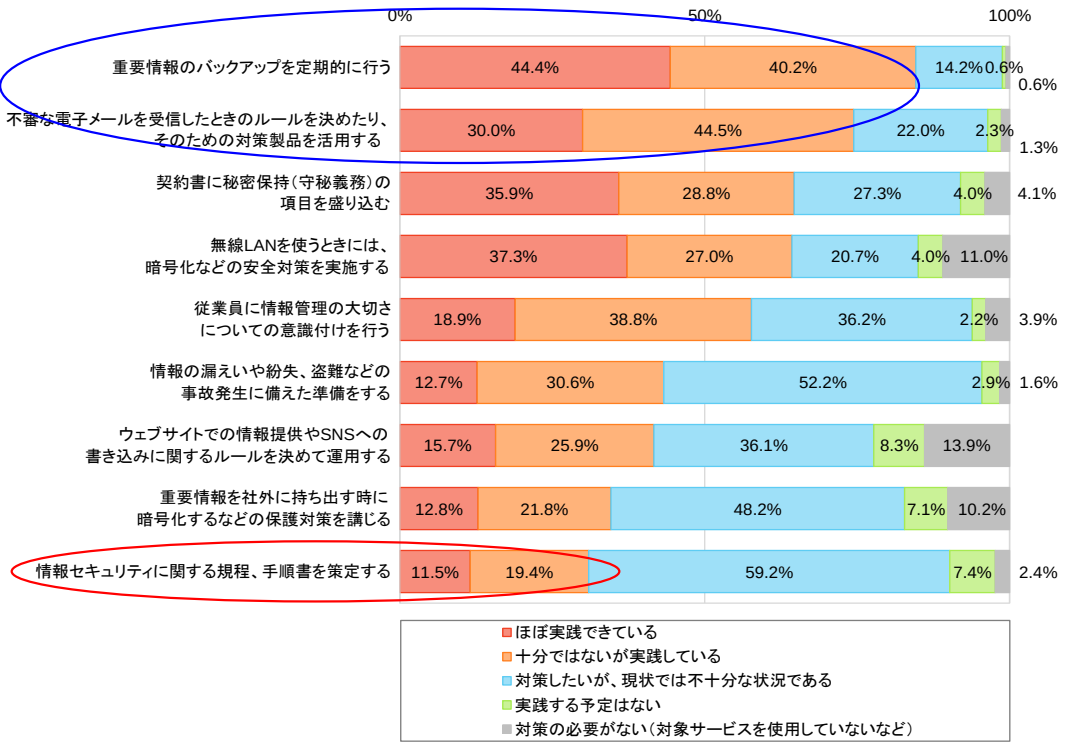


図 3-12　情報セキュリティ対策の取組み状況（Q12）

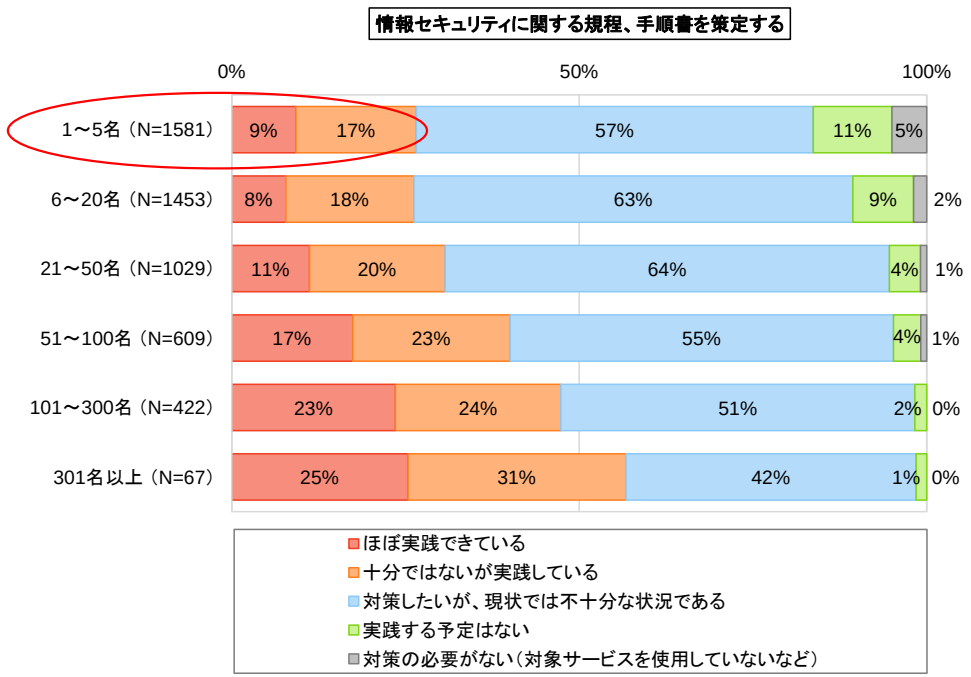


図 3-34　総従業員別 セキュリティ対策について貴社の取組み状況① (Q12×Q2)

IPA「2018 年度SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査- 調査報告書 -」より

(4) 情報セキュリティ対策を進める上での課題点

SECURITY ACTION 自己宣言事業者で

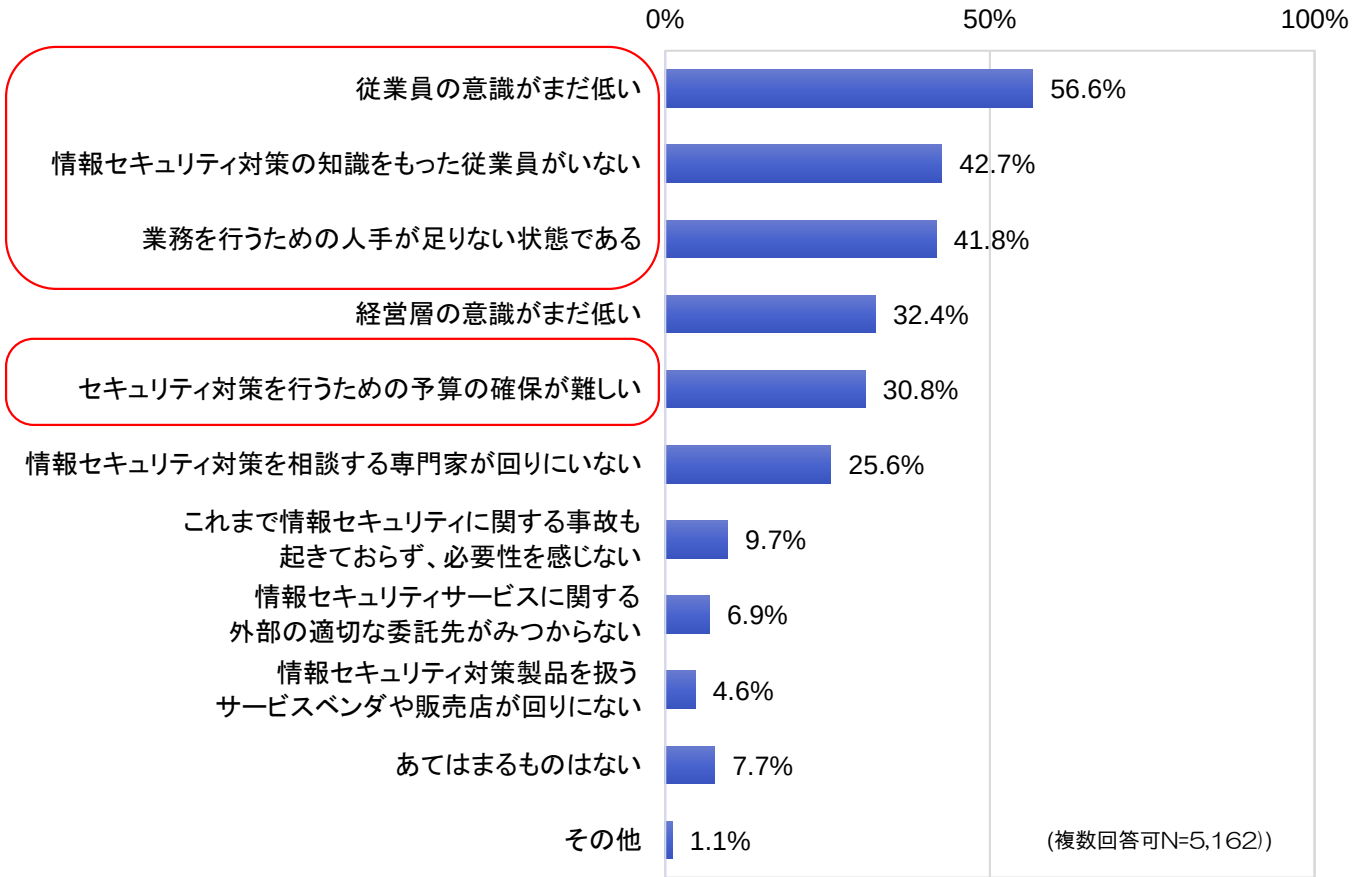


図 3-13　情報セキュリティ対策を進める上での課題点（Q13）

IPA「2018 年度SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査- 調査報告書 -」より

(4) 情報セキュリティ対策を進める上での課題点

表 3-11　総従業員数別 情報セキュリティ対策を進める上での課題点（Q13×Q2）（複数回答可）

	従業員の意識がまだ低い	情報セキュリティ対策の知識をもった従業員がいない	業務を行うための人手が足りない状態である	経営層の意識がまだ低い	セキュリティ対策を行うための予算の確保が難しい	情報セキュリティ対策を相談する専門家が回りにいない	これまで情報セキュリティに関する事故も起きておらず、必要性を感じない	情報セキュリティサービスに関する外部の適切な委託先がみつからない	情報セキュリティ対策製品を扱うサービスベンダや販売店が回りにない	その他
全体（N=5162）	56.6%	42.7%	41.8%	32.4%	30.8%	25.6%	9.7%	6.9%	4.7%	1.1%
1～5 名（N=1581）	30.8%	40.4%	33.6%	25.9%	32.1%	28.5%	11.0%	8.0%	6.3%	0.9%
6～20 名（N=1453）	61.8%	46.0%	41.4%	31.9%	29.4%	23.7%	10.8%	7.4%	5.2%	0.8%
21～50 名（N=1029）	70.4%	45.9%	46.6%	36.5%	29.4%	25.9%	8.8%	5.5%	3.1%	1.4%
51～100 名（N=609）	74.9%	41.7%	49.4%	38.3%	33.7%	24.5%	7.2%	6.2%	3.9%	2.1%
101～300 名（N=422）	73.2%	35.5%	48.1%	37.4%	31.0%	21.8%	7.6%	4.7%	1.4%	0.9%
301 名以上（N=67）	73.1%	26.9%	58.2%	47.8%	28.4%	26.9%	1.5%	9.0%	6.0%	1.5%

IPA「2018 年度SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査- 調査報告書 -」より

中小企業の情報セキュリティの現状と課題

⑸ まとめ

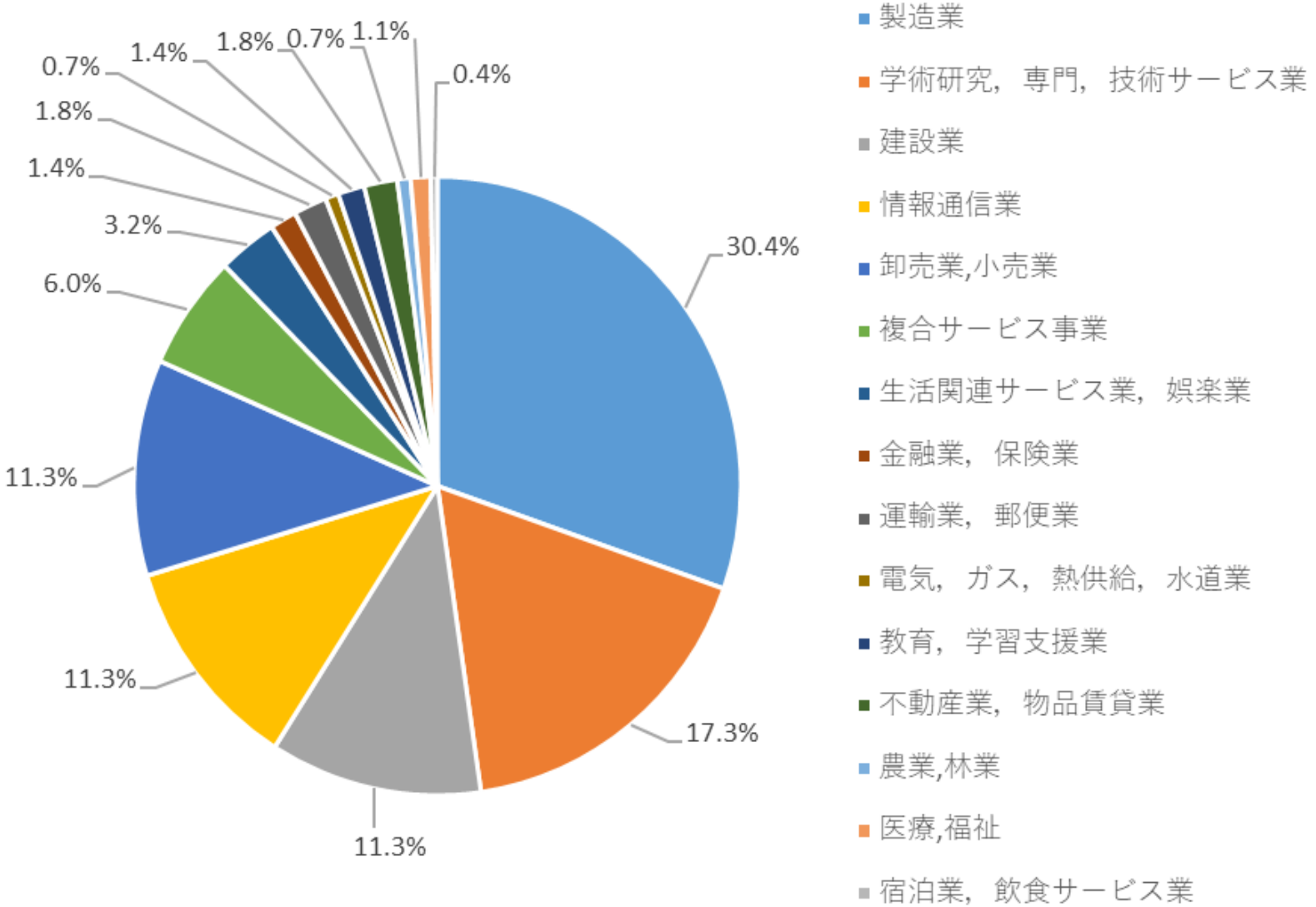
多くの中小企業では

- ✓ 情報セキュリティ対策が組織的には行えていない
  組織的に行われていても、担当者は兼務のことが多い
- ✓ 情報セキュリティに関する規程、手順書が整備されていない
- ✓ 情報セキュリティ対策のための予算が乏しい
- ✓ 情報セキュリティ対策の知識を持った社員がいない
- ✓ 情報セキュリティの教育が実施されていない
- ✓ 経営層の意識も低いところが多い（企業規模が大きいほど）

２　前年度の指導の全体像

前年度の指導の全体像

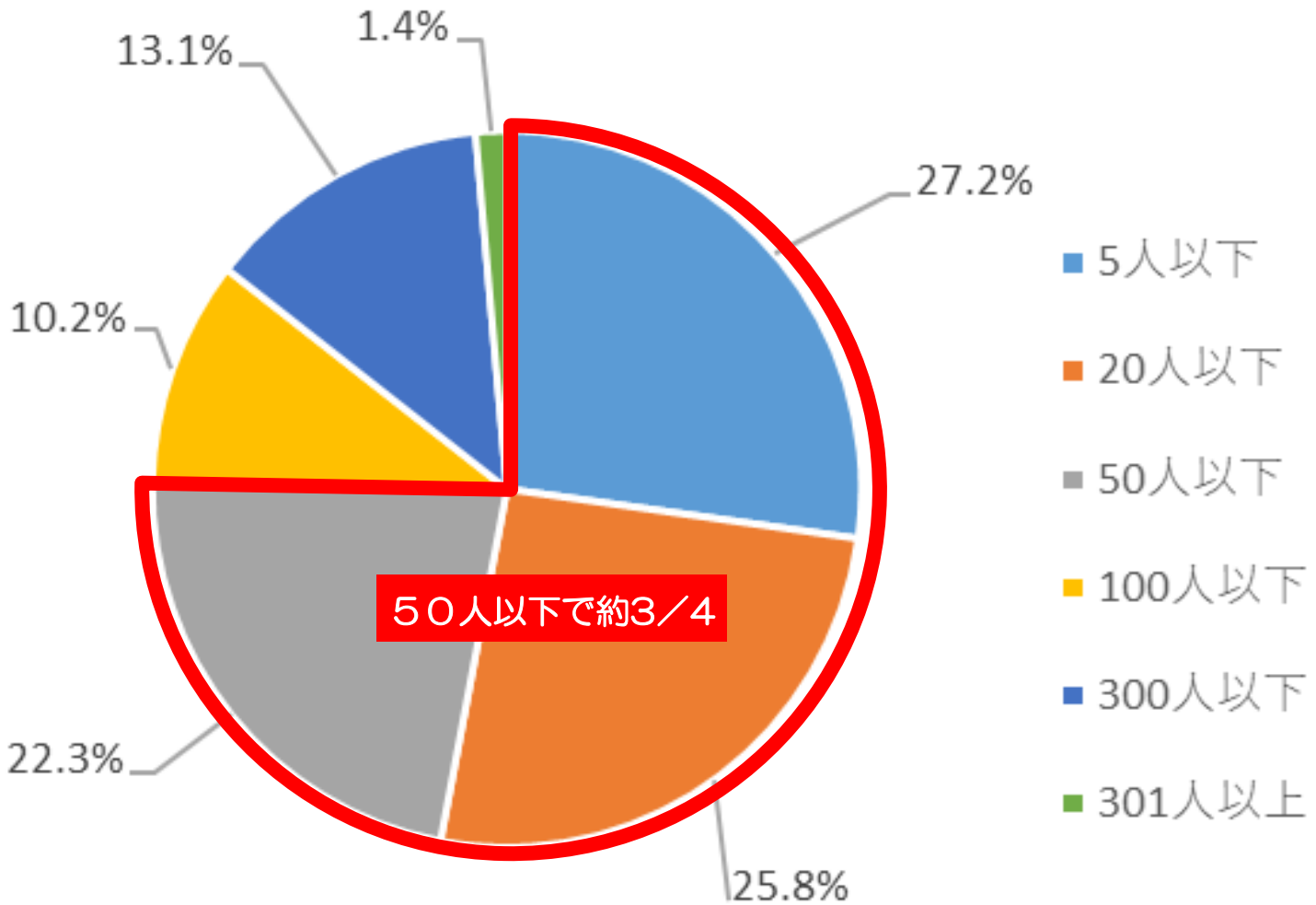
(1) 指導先企業の業種



IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書」より

前年度の指導の全体像

(2) 指導先企業の規模（従業員数）

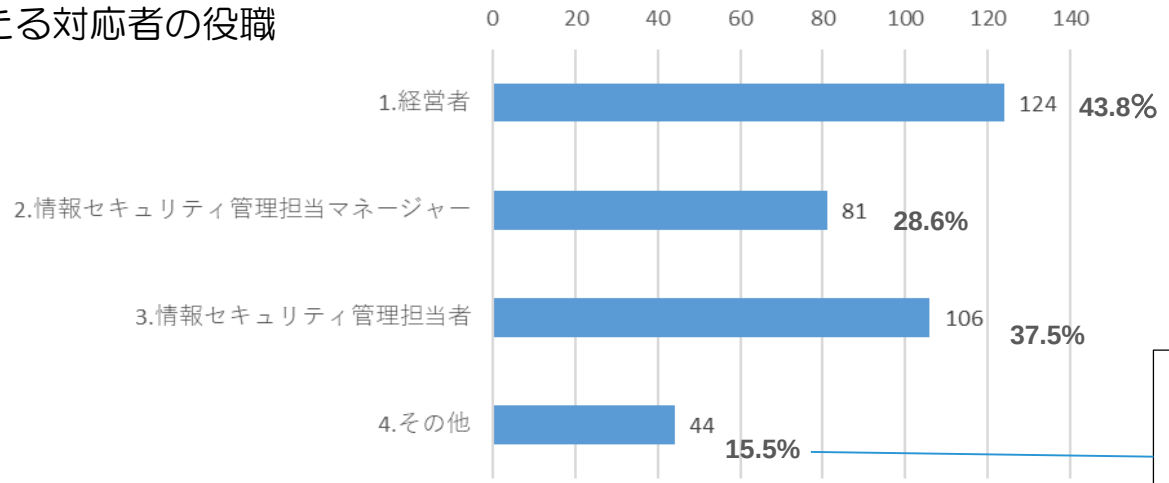


IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書」より

前年度の指導の全体像

(3) 指導先企業の対応者の役職 と 情報セキュリティ管理体制

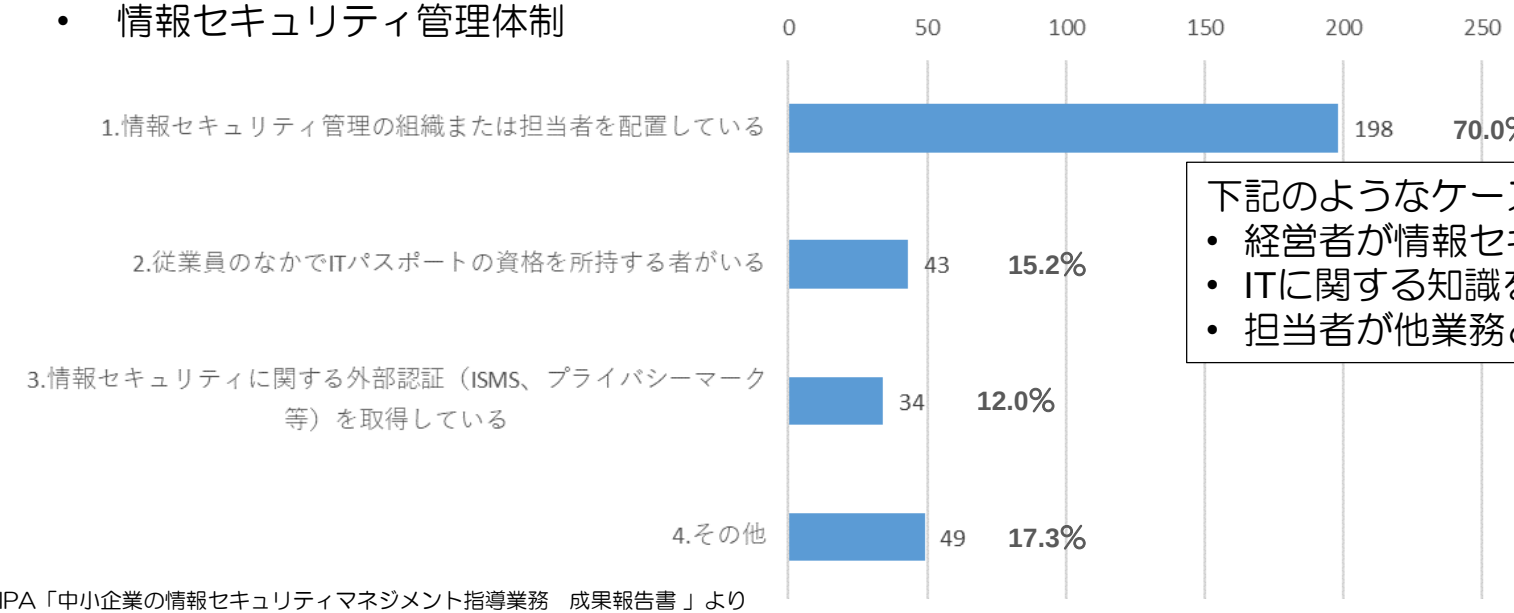
- 主たる対応者の役職



下記のようなケースがある
- 経営者も同席
- 担当者が経営者へ説明

•WEB制作ならびにパソコン等の機器の管理者
•営業
•総務部社員、総務部長、総務・経理担当
•ＩＳＭＳ推進会メンバー
•情報システム管理者、情報システム部長
•品質保証担当

- 情報セキュリティ管理体制

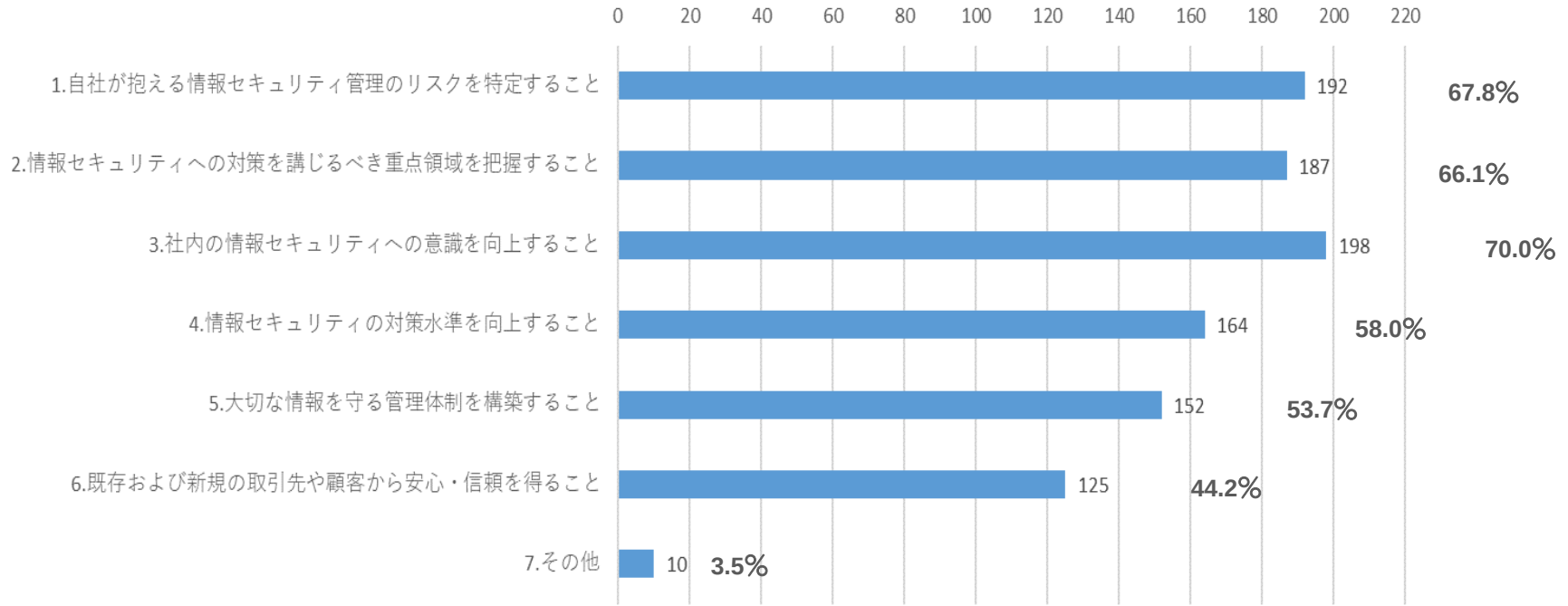


下記のようなケースもある
- 経営者が情報セキュリティ管理を担当
- ITに関する知識を有する専務が担当
- 担当者が他業務と兼務

IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書 」より

前年度の指導の全体像

(4) 指導先企業の参加目的



「その他」の主な回答内容

- 当社のセキュリティ対策状況は、指導員の考える水準と比較して、十分か不足かの評価を得たい
- 情報セキュリティ関連規定を文書化し発行する事
- 情報セキュリティ規程を構築すること
- 経営層に情報セキュリティに対して問題があることを認識してほしかったため他社が行っている情報セキュリティマネジメントとはどのようなものかを知りたかった
- 顧客から情報セキュリティの監査を１月下旬に控えているため、その組織、文書の体制づくりとしての水準アップのため
- ISMS 認証取得に備えて

IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書 」より

前年度の指導の全体像

⑸ まとめ

- ✓ 50人以下の規模が3/4を占めていた

- ✓ 経営者が出席されたケースが4割以上
  出席されない場合でも、経営者への説明を意識することが必要

- ✓ 情報セキュリティ管理の組織、担当者は、経営者の場合がある
  経営者でなくても、他にIT以外の主たる業務を持っていることがある

- ✓ 参加目的は、「自社のリスク特定」「対策の重点領域把握」「社内の意識向上」「対策水準の向上」
  「管理体制の構築」などで、「規程の整備」が直接の目的ではない
  「規程」は、あくまでも上記の目的を達成するために「整備」

IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書 」より

３　前年度の
具体的指導事例の紹介

前年度の具体的指導事例の紹介

(1) 事例１（企業概要）

業種	建設業
所在地	神奈川県
従業員数	12名
面談者	専務取締役
IT環境	クライアントPC（ユーザ管理なし（HomeEdition）、一部Wi-Fi、一部XP） スマホ（個人所有あり） NAS プリンタ複合機 ルータ UTM VPNルータ 業務システムでクラウドサービスの利用あり
IT担当	代表取締役、専務取締役
情報セキュリティ担当	専務取締役

前年度の具体的指導事例の紹介

（1）事例１（指導概要）

準備	企業情報調査（HPで）、ヒヤリング項目整理（事務局提供のヒヤリングシートを元に）、 指導業務説明資料（自己紹介を含む）
１回目 （10/17）	ヒヤリング 　経営方針、支援への期待、事業の状況（業務内容、サプライチェーンなど）、社内体制、 　ステークホルダと情報の流れ、情報の種類、情報システム環境（現状と今後の計画） 依頼 　自社診断の実施（複数名）
準備	利用製品の仕様調査、送付いただいた自社診断結果3件の集計・分析、**資産管理台帳の作成**、 **基本方針・関連規程の案作成**（IPAの雛形をベース）、 １回目の結果、自社診断結果と重点対策領域・要対策項目、基本方針・関連規程の要検討項目をまとめた資料作成
２回目 （11/1）	１回目の確認（追加確認あり）、自社診断結果と重点対策領域・要対策項目の説明、 基本方針・関連規程の作成方針の説明と要検討項目の討議
準備	アクセス制御の方針・方法検討、具体的対策の検討、関連規程の追加検討、 **改善対策実行計画の検討・作成** 基本方針のメール送付・代表取締役確認済み版の受領
３回目 （11/4）	２回目の確認、アクセス制御の方針・方法の説明・検討、改善対策実行計画の検討
準備	関連規程の追加検討・修正、**ハンドブックの作成**（IPAの雛形をベース）
４回目 （11/18）	３回目の確認、関連規程の最終確認、ハンドブックの確認、 改善対策実行計画の確認（企業側の日程検討結果を反映）、今後の対応についての意見交換
後処置	レビュー結果を反映した成果物一式をメールで送付

標準カリキュラムでは企業が作成

標準カリキュラム外

前年度の具体的指導事例の紹介

（1）事例１（指導業務説明資料）

株式会社[redacted]御中

情報セキュリティマネジメント指導業務について

2019年10月7日

ITCはまさき ITCoordinators HAMASAKI

指導員紹介

ITCはまさき ITCoordinators HAMASAKI

田中 孝典

ITコーディネータ、情報処理安全確保支援士

第000537号
（情報処理安全確保支援士）

1980年：メーカ系ソフト開発会社に入社。
セキュリティソフトの開発、セキュリティ製品の輸入販売などを担当。
ITシステムへのセキュリティ対策の提案・構築も担当。

2014年：NPO法人 ちば経営応援隊 に入会
創業スクール、創業実践塾などでビジネスプラン・創業計画の講師。
セキュリティコンサル事業の立ち上げに参画。
現場の教育用コンテンツを作成・提供。

2015年11月より、独立系SI会社の品質・情報セキュリティ・
個人情報マネジメントシステムの改善を支援。社内研修も担当。

2015年：ITCはまさき の立ち上げに参画

【出身地】 岡山県　　【居住地】 横浜市戸塚区
【活動】 NPO法人 ITコーディネータ協会、ITC千葉ネットワーク、ちば経営応援隊
ITCはまさき 会員
独立行政法人情報処理推進機構（IPA）　セキュリティプレゼンター制度に登録
上記を通じて中小企業のIT経営、情報セキュリティ対策を支援

本プログラムの目標と成果物

ITCはまさき ITCoordinators HAMASAKI

① 「５分でできる情報セキュリティ自社診断」の診断結果

② 情報セキュリティ基本方針/関連規程類

③ 改善対策実行計画

④ SECURITY ACTION制度の二つ星の自己宣言

本プログラムの構成

ITCはまさき ITCoordinators HAMASAKI

第１回	情報システム環境の理解とリスクの洗い出し 御社の事業内容と情報システム環境を把握し、経営者の方が認識している御社のセキュリティ課題（リスク）と当プログラムへの期待値を確認させていただきます。
事前準備#２	(自社診断の実施し、結果をご提出いただきます)
第２回	重点改善領域の絞り込みと基本方針の策定 ご提出いただいた自社診断結果から、潜在化しているリスクも把握したうえで、基本方針と重点改善領域についてディスカッションを行います。
事前準備#３	(現在の関連規程類を点検し、具体的な対策案を作成いただきます)
第３回	関連規程等の検討と具体的改善対策の立案 情報セキュリティ基本方針に基づき、必要な関連規程類の検討を行うと共に、具体的対策案の妥当性や優先順位についてディスカッションを行います。
事前準備#４	(情報セキュリティ基本方針を完成し、必要な関連規程のドラフトを作成いただきます)
第４回	対策や規程類などの成果物レビューとまとめ 指導員が提示いたします実行計画案（一年間程度）についてディスカッションし、合意形成を図ります。また御社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、二つ星の自己宣言の準備を行います。

前年度の具体的指導事例の紹介

(1) 事例１（自社診断結果3件の集計、分析）

- 事務局から提供された自社診断シートをもとに集計用シートを作成
- 回答の分布を見える化（経営者の回答を青、従業員の回答を赤（わからない）か黄（実施していない））
- これをもとに弱点を説明

診断項目	No	診断内容	該当するものにプルダウンで「✓」を入力　（択一選択） 実施している（4点）	一部実施している（2点）	実施していない（0点）	わからない（-1点）
Part 1	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	2		
	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		1	1
Part 2	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？		1	2	
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？		2	1	
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？		1		2
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？			1	2
	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？			1	2

※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。

A 実施しているの合計点	B 一部実施している の合計点		C 分からないの合計点
40 点	50 点	マイナス(-)	-17 点
A+B+C 合計		73	点
100点換算		24.3	点

平均点を表示 →

前年度の具体的指導事例の紹介

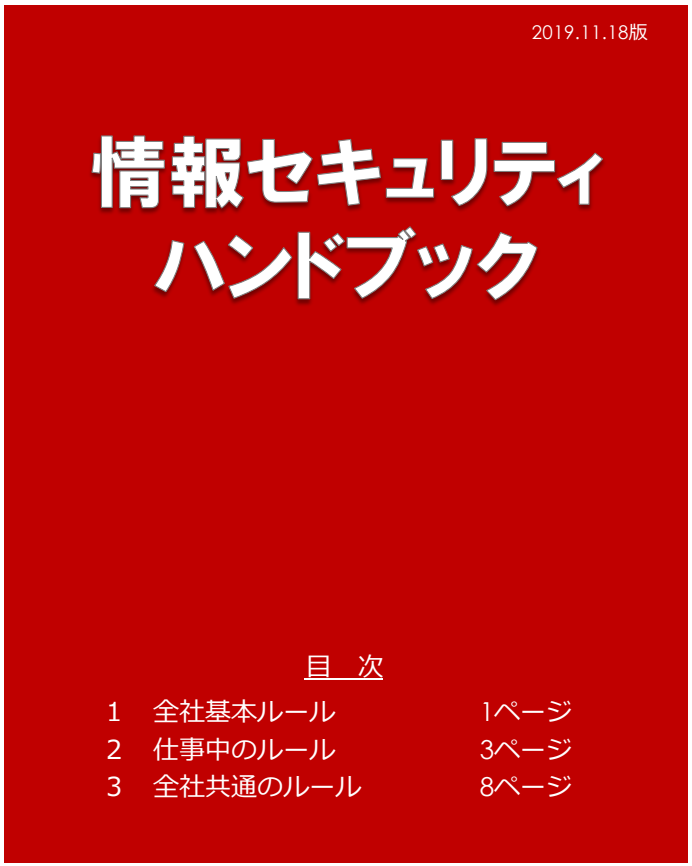
(1) 事例１（関連規程）

- 自社システムはなく、開発予定もなかったので「システム開発及び保守」は作成せず
- 「個人番号及び特定個人情報の取り扱い」に関する規定は作成されており、中身も十分であったので作成せず

	関連規程/ガイド類	対応
1	組織的対策	新規に作成
2	人的対策	新規に作成
3	情報資産管理	新規に作成
4	アクセス制御及び認証	新規に作成
5	物理的対策	新規に作成
6	ＩＴ機器利用	新規に作成
7	ＩＴ基盤運用管理	新規に作成
8	システム開発及び保守	作成の必要なし
9	委託管理	新規に作成
10	情報セキュリティインシデント対応ならびに事業継続管理	新規に作成
11	個人番号及び特定個人情報の取り扱い	既存のもので十分

前年度の具体的指導事例の紹介

(1) 事例１（ハンドブック）

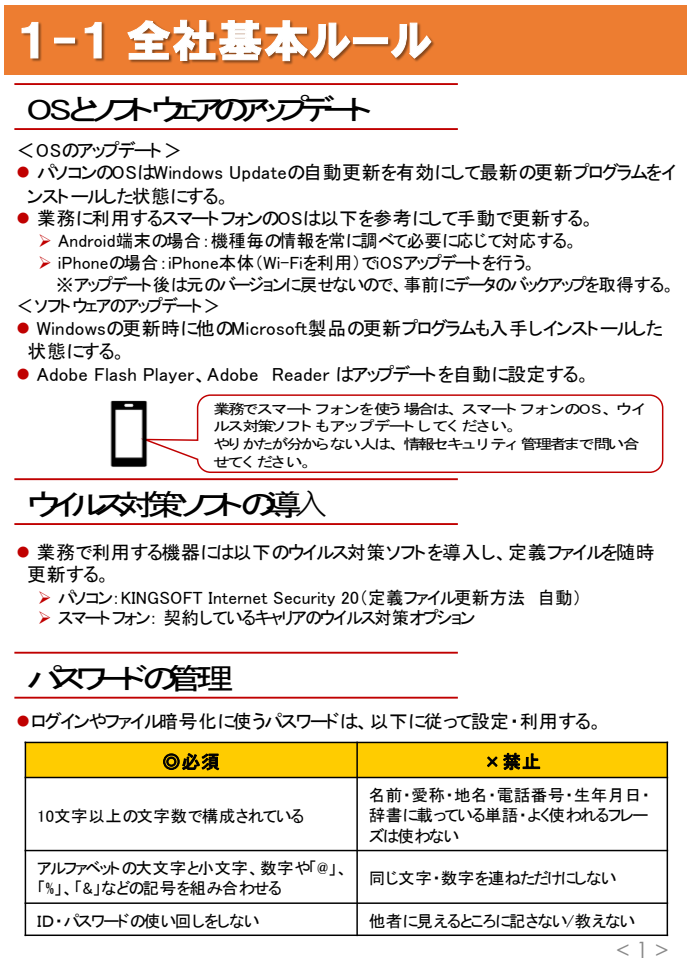


2019.11.18版

情報セキュリティ
ハンドブック

目　次

株式会社



1－1 全社基本ルール

OSとソフトウェアのアップデート

＜OSのアップデート＞
- パソコンのOSはWindows Updateの自動更新を有効にして最新の更新プログラムをインストールした状態にする。
- 業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。
  - Android端末の場合：機種毎の情報を常に調べて必要に応じて対応する。
  - iPhoneの場合：iPhone本体（Wi-Fiを利用）でiOSアップデートを行う。
    ※アップデート後は元のバージョンに戻せないので、事前にデータのバックアップを取得する。

＜ソフトウェアのアップデート＞
- Windowsの更新時に他のMicrosoft製品の更新プログラムも入手しインストールした状態にする。
- Adobe Flash Player、Adobe　Reader はアップデートを自動に設定する。

業務でスマート フォンを使う 場合は、スマート フォンのOS、ウイルス対策ソフト もアップデート して く ださい。
やり かたが分からない人は、情報セキュリティ 管理者まで問い合せてく ださい。

ウイルス対策ソフトの導入

- 業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイルを随時更新する。
  - パソコン：KINGSOFT Internet Security 20（定義ファイル更新方法　自動）
  - スマートフォン：契約しているキャリアのウイルス対策オプション

パスワードの管理

- ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

◎必須	×禁止
10文字以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない
アルファベットの大文字と小文字、数字や「@」、「%」、「&」などの記号を組み合わせる	同じ文字・数字を連ねただけにしない
ID・パスワードの使い回しをしない	他者に見えるところに記さない/教えない

＜１＞

前年度の具体的指導事例の紹介

(1) 事例１（工夫した点・苦労した点）

工夫した点

- ✓ 指導先企業の負担は最低限にとどめた（体制を考慮）
  - ➢ 基本方針、関連規程、情報資産管理台帳、実行計画等を作成
    （企業は検討だけで済むように）
- ✓ 投資は必要最低限に抑えた
  - ➢ Windowsバージョンアップのための新しいPC、バックアップ用HDDだけ
  - ➢ WindowsはHome Editionのまま
  - ➢ AD、LDAP等のユーザ認証基盤は導入しない
- ✓ すぐに運用に入れるように考慮
  - ➢ 規程だけでは従業員が理解できないと思い、より業務内容に近いハンドブックを作成
- ✓ 経営側の思い込みの排除
  - ➢ 自社診断を３名（１名経営、従業員２名）に実施してもらい、
    経営側と従業員との認識のギャップを明らかにした

苦労した点

- ✓ アクセス制御の実現
  - ➢ 認証基盤がなく、Windows Home Edition、NASを使用している
- ✓ Windows XPから10への移行
  - ➢ 使用しているメーラーがWindows標準（バージョン間の仕様差）

前年度の具体的指導事例の紹介

(1) 事例２ （企業概要）

業種	サービス業
所在地	千葉県
従業員数	25名
面談者	社長、情報システム担当者（兼務）
IT環境	クライアントPC（ユーザ管理なし、顧客と共有するPCあり） NAS（複数台、部署・職位で使用するNASが異なる） 複合機 プリンタ 専用出力装置と制御用PC ルータ 業務システムで複数のクラウドサービス利用あり
IT担当	他業務と兼務
情報セキュリティ担当	社長

前年度の具体的指導事例の紹介

（1）事例２ （指導概要）

準備	企業情報調査（HPで）、ヒヤリング項目整理（事務局提供のヒヤリングシートを元に）、 指導業務説明資料（自己紹介を含む）
１回目 （11/8）	ヒヤリング 　経営方針、支援への期待、事業の状況（業務内容、サプライチェーンなど）、社内体制、 　ステークホルダと情報の流れ、情報の種類、情報システム環境（現状と今後の計画） 依頼 　自社診断の実施（複数名）
準備	利用製品の仕様調査、送付いただいた自社診断結果5件の集計・分析、資産管理台帳の作成、 基本方針・関連規程の案作成（IPAの雛形をベース）、 １回目の結果、自社診断結果と重点対策領域・要対策項目、基本方針の要検討項目をまとめた資料、システム概略図、情報管理の考え方作成
２回目 （11/22）	１回目の確認、自社診断結果と重点対策領域・要対策項目の説明、 基本方針の説明と要検討項目（情報管理の方法を中心）の討議
準備	システム概略図の修正、ユーザとアクセス範囲・機器・利用外部サービス・NASのアクセス制御・IPアドレスの一覧（外部接続の有無を含む）の作成（具体的対策の検討を含む）、関連規程の検討
３回目 （12/5）	２回目の確認、各種一覧の説明、関連規定の説明と要検討項目の討議
準備	関連規程の追加検討・修正、各種一覧への検討結果反映、改善対策実行計画の作成
４回目 （12/23）	３回目の確認、関連規程の最終確認、改善対策実行計画の確認
後処置	レビュー結果を反映した成果物一式をメールで送付

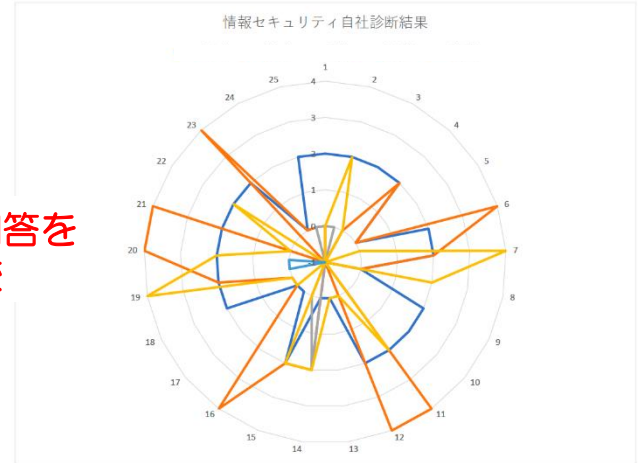
情報管理の方法を検討する必要があり、規程類は３回目以降に

前年度の具体的指導事例の紹介

(1) 事例２ （自社診断結果の分析）

事例１の集計に加えて、グラフ化

業種の平均と比較を表示

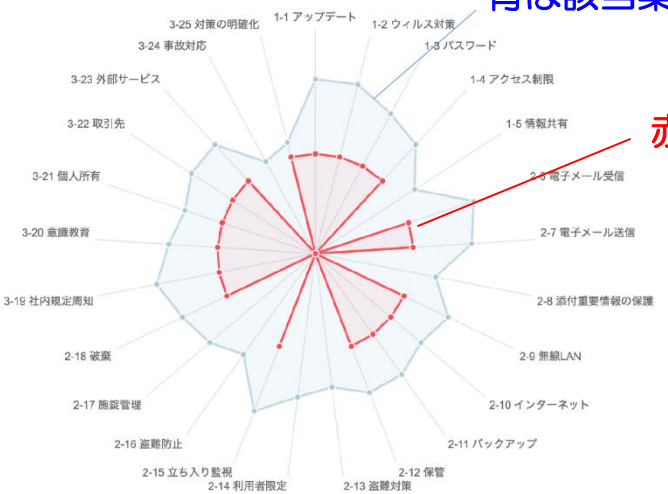


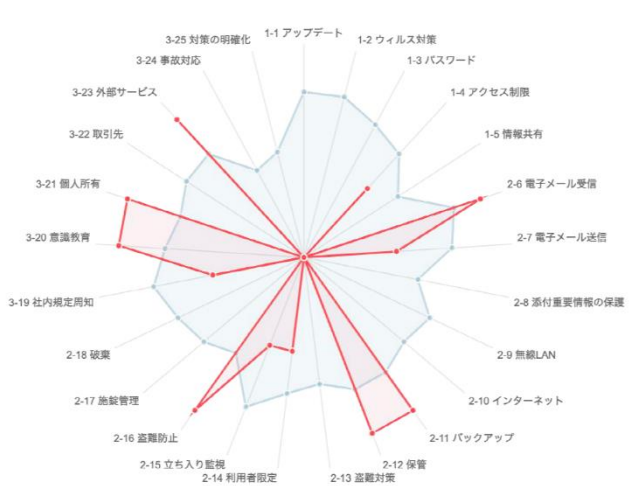
個人毎の回答を
重ねて比較

個人A

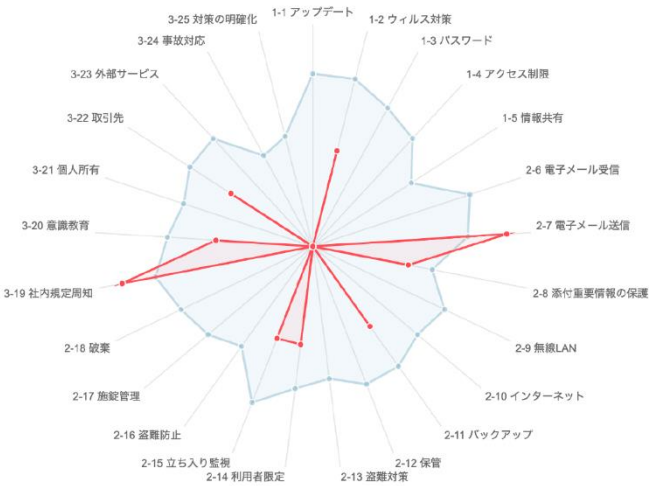
青は該当業種の平均

赤は個人の回答





個人B



個人C

前年度の具体的指導事例の紹介

(1) 事例２ （作成した一覧（その１））

本事例では、社内は3つのエリアに分かれており、次の特徴を持っていた。

- ✓ PCはエリア内では共有される
- ✓ エリア内では個人管理とする情報資産がない

また、ユーザ管理システムを構築しないようにし、かつ管理負担を増やさないことを考慮して、
ユーザごとにアクセスできる範囲とその権限を下のような一覧にまとめた。

ユーザとアクセス範囲の一覧

2019/12/23

No	ユーザ名	パスワード	用途	種別	OS	アクセス先と権限										
						場所										
						装置等										
1																
2																
3																
4																
5																
6																
7																
8																
9																
10																

「種別」はWindowsのユーザ種別
「OS」はWindouwsのバージョン

【凡例】 更新： データの変更が可能（プリンタの場合は印刷可能）
読取： データの利用だけが可能
×： アクセス不可

前年度の具体的指導事例の紹介

(1) 事例２ （作成した一覧（その２））

情報資産へのアクセス権限を明確にすることと、今後の情報システムの管理をしやすくすため、
下記のよう一覧表を作成した。
実際は、情報を入力して提供した。

NASのアクセス制御一覧

2019/12/23

No	種別	設置場所	共有フォルダ名	ユーザ								
1												
2												
3												
4												

外部サービス一覧

2019/12/23

No	サービス名	提供者	用途	使用者							
1											
2											
10											

【凡例】 ○：使用可能
△：許可を得た人だけ使用可能
×：使用不可

IPアドレス一覧

2019/12/23

No	設置場所	機器	管理番号	IPアドレス	サブネットマスク	インターネット許可
1						
2						
3						

機器一覧

2019/12/23

No	種別	製品名/型番	ベンダー名	仕様	用途	設置場所		
1								
2								
3								
4								

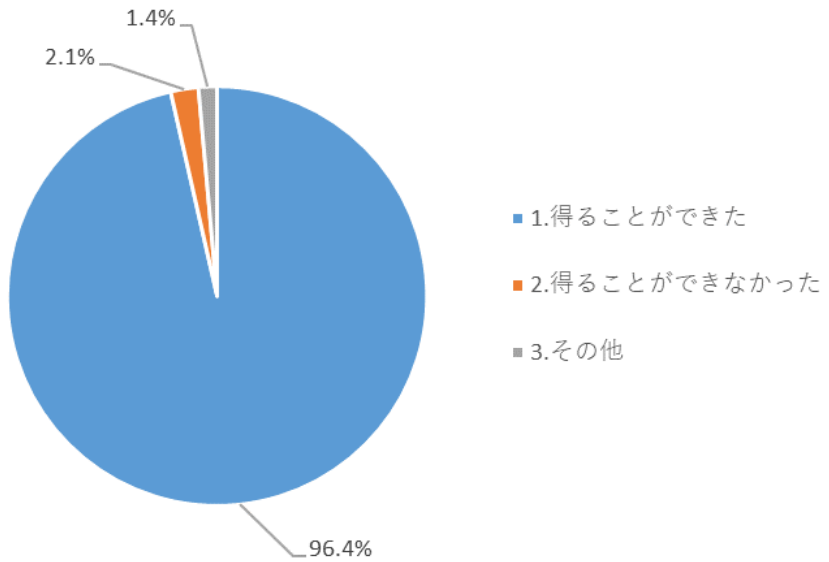
４　前年度のアンケートから参考にできること

前年度のアンケートから参考にできること

（1）指導先企業の対応者の成果

「得ることができた」主な理由（抜粋）

- ポリシーの策定、規程の制定並びに情報資産管理台帳の整備について、業種、事業規模や環境に応じた指導をいただいた
- 自社のセキュリティレベルを把握し、取り組むべき課題及び対策が明確になった
- 自社のセキュリティレベルの客観的評価並びに、不足部分のご指摘を頂けた。
- 情報セキュリティ基本方針と情報セキュリティ関連規程を策定でき、今後、情報セキュリティを向上させていく足掛かりを作ることができた
- セキュリティ管理者と従業員のセキュリティに対する認識の違いがあることが認識できた
- 社員個人の意識を向上させるべく、教育が必要だと改めて思った
- これまで情報セキュリティはハードウエア面のみを考えていたが、その上位に人的要因を含めた管理体制の整備が必要なことが認識できた
- Windows 7 パソコンを使い続けることの危険性や、従業員への情報セキュリティ教育の必要性を認識した
- 情報セキュリティマネジメントを理解し、３年間の中期経営計画に反映した



「得ることができなかった」主な理由

- 終始、話がかみ合わず、自社の現状と先方が話したいことがマッチしなかった

「その他」を選択した主な理由（抜粋）

- 課題の洗い出しはできたが、具体的な指針まで指導は得られなかった
- 方向性は見いだせたが、事業規模や業種に合ったものを運用して行くには、当社の事業や業種に合った専門家との相談が必要だと感じた

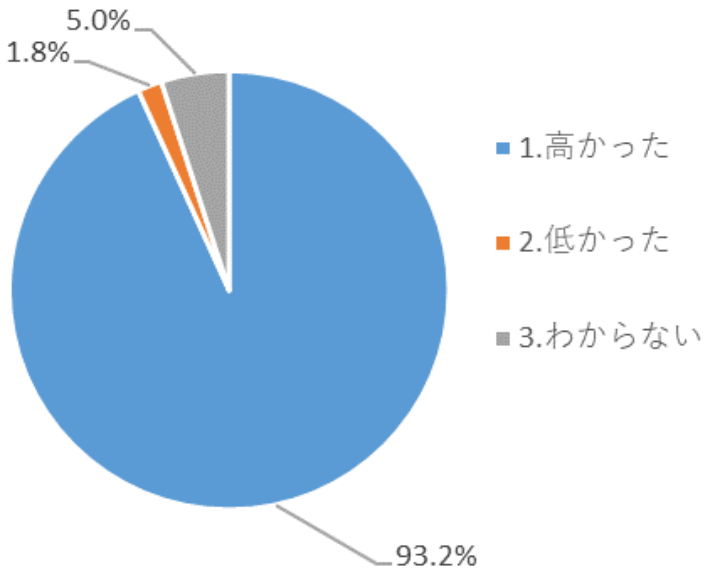
IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書」より

前年度のアンケートから参考にできること

(2) 指導先企業の専門家に対する評価（知識・専門力）

「高かった」主な理由（抜粋）

- 具体的な事例等豊富な知識で取り組んで頂いた
- 実際の現場で習得された技術や知識をベースに指導いただいたので、現実的な規定を策定するためのよいインプットとなった
- 一般人には難しい専門用語もなるべく使わず、とても分かりやすく説明できるだけの知識の深さがあった
- 常に最新の危機管理の情勢について教えて頂けた。ISO27001、法令や事例に関する質疑にも的確に応答されていた
- 質問の対応方法に長所短所を添えて頂き、判断基準を明確にアドバイスしていただけた
- 現行の独自の取組みの考慮の甘いところを見抜いた
- 画一的な内容で実現が困難な指摘をいただくことがなく、弊社の状況に合わせて、アドバイスをいただけた。教科書的ではなく実戦的な経験を教えていただいた
- 疑問に対して、1つの対処法だけでなく、複数の対処法のアイデアを提示してもらい、当社でできる範囲で選択ができた
- 物理的な問題から IT機器、ソフトウェアと幅広く経験談を交えて指導いただいた



「低かった」主な理由
記載なし

「わからない」を選択した主な理由（抜粋）

- 専門的なレビューというよりも、情報セキュリティ関連規定、インシデント体制についての指導が主となってしまったので、専門知識を披露する場が限られてしまったのではないかと思われます
- 自身が担当したことのある、弊社より大きい規模の企業でのセキュリティに関する取組みについて話をされたが、話の引き出しがそれしかなく、弊社にはマッチしない内容だった

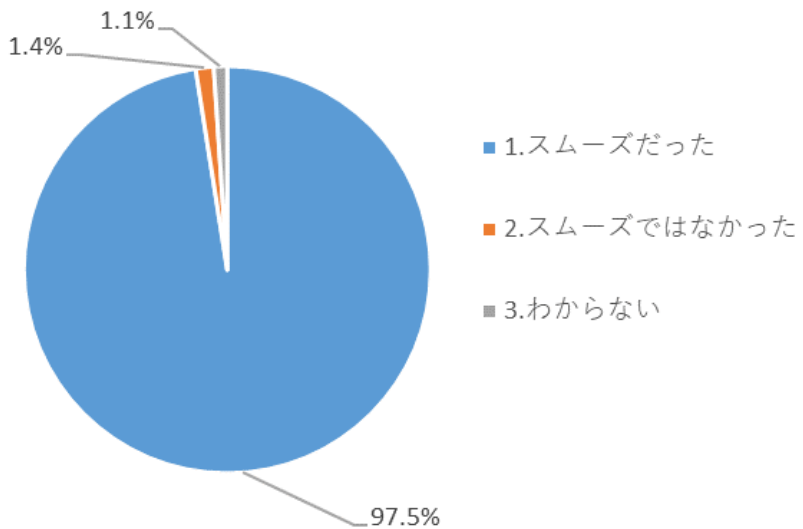
IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書 」より

前年度のアンケートから参考にできること

(3) 指導先企業の専門家に対する評価（コミュニケーション）

「スムーズだった」主な理由（抜粋）

- アドバイスを頂く際にはわかりやすい用語（説明）で教えて頂いた
- 今回の目標や次回への課題を明確に提示してくださった
- 専門家の話し方がゆっくりとやさしく論理的だった
- 経営層に対しても的確かつ丁寧に情報セキュリティの重要性を説明頂き、担当者ともうまくコミュニケーションが取れ、的確に整備が進められた
- 個人的な興味のある話から、大局の情報管理の認識までへと昇華して教えて頂けた訪問のみならず、メール・電話でもフォローをしっかりして頂けました。
- 例題を交えながらの指導だったので、身近に感じられた
- 指導日以前からメールにてやり取りさせていただき、当日までにやるべきことが明確な状態で指導日を迎えることができた
- 毎回提案書や前回の指導のチャート等を作成して頂き、分かりやすく説明頂けた
- 一方的に話を聞くだけではなく 適宜問題形式で従業員に答えるようなやりとりでスムーズにコミュニケーションがとれました



「スムーズではなかった」主な理由

- 指導のスケジュールがタイトで十分に理解し合えなかった
- 内容はよくわかり、意思疎通できていたが、こちらで進行を促さないと先に進まない場面があった

「わからない」を選択した主な理由

記載なし

IPA「中小企業の情報セキュリティマネジメント指導業務　成果報告書 」より

前年度のアンケートから参考にできること

(4) まとめ

指導にあたって留意すること

- ✓ 指導先の現状（事業内容・方向性、体制、予算なども） を正しく把握する
- ✓ 課題及び対策が明確にする
- ✓ 専門用語をなるべく使わず、事例や経験談などを交えて分かりやすく説明する
- ✓ 対策などの選択肢は長所・短所を示し、指導先が選択できるようにする
- ✓ 判断基準を明確に示す
- ✓ 相手に気付いてもらう指導をする
- ✓ 業種、事業規模、環境など指導先に応じた指導をする
- ✓ 毎回、今回の目標や次回への課題を明確に提示する
- ✓ 前回の指導結果をチャートなどにまとめる
- ✓ 必要に応じてメール・電話でもフォローする
- ✓ 主体性を持って推進する

５　まとめ

まとめ

標準カリキュラムにとらわれず、指導先の実態にあった指導を心がけてください

- 従業員規模・体制
- 情報資産の重要度・利用者
- IT環境

- ✓ 追加投資は、最低限かつ企業の状況にあった提案を心がけてください
- ✓ 企業が自ら改善を続けられるように心がけてください
- ✓ わかりやすく、丁寧な説明を心がけてください
- ✓ 主体性を持って進めてください

前年度のアンケートでは、ほとんどの企業が指導に満足しています。恐れずに指導に臨んでください。

参考資料

- 「2016 年度中小企業における 情報セキュリティ対策の実態調査　－ 調査報告書 －」（IPA）
  https://www.ipa.go.jp/files/000058502.pdf

- 「2018 年度SECURITY ACTION 宣言事業者における情報セキュリティ対策の実態調査
  － 調査報告書 －」　（IPA）
  https://www.ipa.go.jp/files/000072383.pdf

- 「中小企業の情報セキュリティマネジメント指導業務　成果報告書 」　（IPA）
  https://www.ipa.go.jp/files/000082717.pdf

パートⅡ　効果的な訪問指導

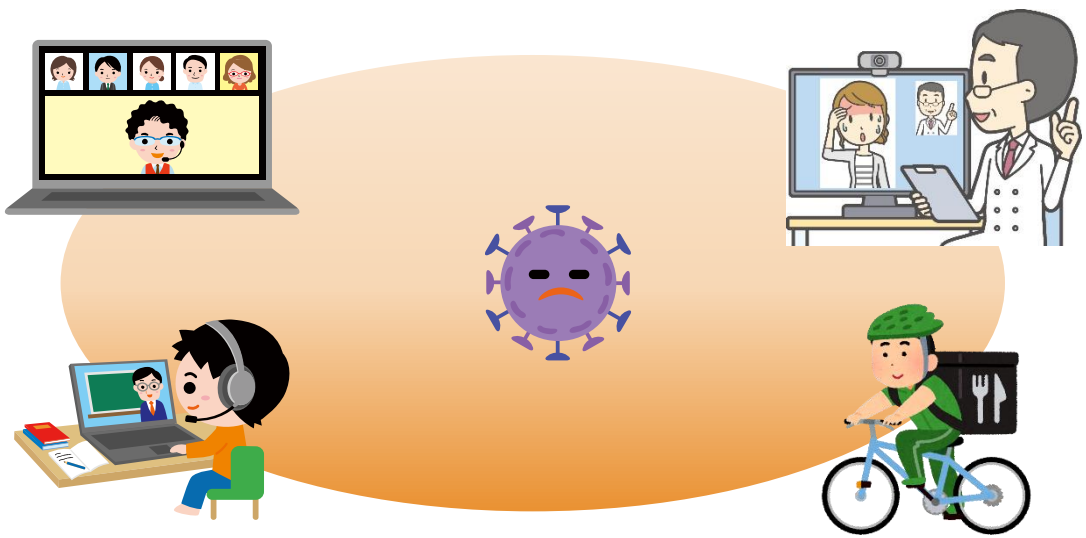
プログラム⑤
コロナ禍のセキュリティ対策

はじめに（コロナ禍におけるIT利活用状況）

新型コロナウイルス感染症の影響により、世の中の仕組み、やり方が大きく変わってきています。多くの企業がテレワーク勤務を導入し、学校ではオンライン授業が幅広く行われ、病院ではオンライン診療が広がりつつあります。今や、会議や講習会もオンラインで行われるのは当たり前になってきています。

しかし、今回の騒動では、急ごしらえで、その場しのぎ的にITを導入した企業・団体も多く、導入を急ぐあまり、ITは導入したものの情報セキュリティ面での考慮が疎かになっている例も見受けられます。本単元では、コロナ禍でのIT利用時に特有の事象について、指導時に注意する点について学習を行います。ポリシー、および実行計画策定時の補足情報として参考にして下さい。

学習内容はセキュリティマネージメント指導に活かす為の情報提供ですが、RISSの方々への情報提供でもあります。アフターコロナに向け、最新知識習得の第一歩となることを願っております。



1　テレワーク導入・実施に絡む指導上の注意点

テレワーク導入・実施時のセキュリティ上の注意事項

事務所を離れた場所で勤務を行うことにより、セキュリティ上、新たなリスクが発生し、既存リスクが増大しています。テレワークの導入・実施を行う上で特に注意が必要なリスクを以下に示します。

悪意のあるソフトウェア

- マルウェア、ランサムウェアに感染するリスク
- BYODによるリスク

遺失・盗難に伴うリスク

- ノートPCやスマートフォン、USBメモリ等の紛失

重要情報の漏洩

- 無線LAN利用による情報漏洩リスク
- 紙資料に絡むリスク

社内システムへの不正侵入

- 利用者認証情報の漏洩に伴う社内ネットワークへの不正侵入
- テレワーク用社内接続経路の設計、設定ミスによる不正侵入

外部サービスの利用に伴うリスク

- パブリッククラウドサービスの利用に伴うリスク
- Twitterやインスタグラム等のSNS投稿に伴う情報漏洩

テレワーク導入・実施に絡む指導時の留意点

①マルウェア、ランサムウェアに感染するリスク

事象	テレワーク利用端末がマルウェア、ランサムウェアに感染し、リモート接続を通じて社内ネットワークに汚染が広がり、重要情報が漏洩してしまう
固有の原因	・テレワーク中にはインターネットを利用する機会が多くなる。 ・事務所外でPCを操作すると不審サイトへのアクセス、メールの添付ファイルへの警戒心も疎かになりがち。 ・周りに相談する人がおらず、不用意な行動を取ってしまう可能性が高くなる。 ・ネットワークフィルタリング機能が適用できない、または手薄になってしまう。
対策	・OSや使用アプリのアップデートを確実に行い、最新の状態にしておく。 ・テレワーク端末にはウイルス対策ソフトを導入し、最新のパターンファイルを適用する設定を行う。 ・利用PC毎にネットワークフィルタリング機能を設定する。 ・テレワーク勤務者への教育、注意喚起を定期的に実施する。
指導時の留意点	・テレワーク端末の利用規則を定め、セットアップ時の手順は明確になっているか ・テレワークを終了し、社内LANに接続する時の規則・手順は明確になっているか

テレワーク導入・実施に絡む指導時の留意点

②BYODによるリスク

事象	個人所有のパソコンやスマートフォンを業務で利用（BYOD）する場合には、企業が用意する機器とは異なり、管理が行き届かず、マルウェアに感染するリスクが高まる
固有の原因	・BYODでテレワークを実施する場合、ウイルス対策ソフト用のパターンファイルやアプリの最新版への更新がなされない等、企業が用意する機器に比べ、セキュリティの確保が難しくなる。 ・マルウェアに感染した端末で社内システムに接続することにより、悪意のあるソフトウェアが社内システムに侵入してしまう。
対策	・私物機器の利用の業務への利用は許可制にする。 ・BYOD時のルールを明確にする ・許可を受けた端末のみ社内システムへの接続を許可し、接続時にはOSアップデートの状況、ウイルス対策ソフトの状況を確認する。
指導時の留意点	・BYODの利用規則を定め、ルールは明確になっているか ・社内システム接続時に接続端末のチェックを行っているか

テレワーク導入・実施に絡む指導時の留意点

③ノートPCやスマートフォン、USBメモリ等の紛失

事象	テレワーク用端末等を紛失する事により、機密情報が漏洩してしまう。
固有の原因	・テレワークに使用する端末等（ノートPC、スマートフォン、ＵＳＢメモリ等）を遺失または盗難により紛失してしまう。
対策	・ノートPCは紛失時の情報漏洩に備え、ハードディスクの暗号化、および、起動時のパスワード、PIN入力を施す。 ・スマートフォンはセキュリティロック機能を掛ける。紛失時にはリモートロック機能を使い、端末を利用不可にする。 ・USBメモリや可搬媒体は暗号化を施した上で、タグやストラップを付け、紛失の可能性を減らす。 ・事務所外での保管ルールを定め、ルールを順守するようテレワーク勤務者への教育、注意喚起を計画的に実施する
指導時の留意点	・テレワーク時の可搬端末、メディアの取り扱いは明確になっているか ・テレワーク実施者への教育は計画的に行われているか

テレワーク導入・実施に絡む指導時の留意点

④無線LAN利用による情報漏洩

事象	テレワーク実施場所での無線LAN経由で盗聴をされ、重要情報が漏洩してしまう
固有の原因	・利用するアクセスポイントの設定ミス。 （暗号化の有無、暗号化強度、パスワードの強度、他者の接続） ・予期せぬアクセスポイント（公衆Wi-FI、悪意のあるアクセスポイント）に接続してしまう。
対策	・自宅等利用するアクセスポイント、Wi-Fiルータの設定を確認 暗号化：行う（必須） 暗号化強度：WPA3, WPA2,WPA,WEP（暗号強度の強い順） MACアドレスフィルタリング：設定（推奨） SIIDブロードキャスト：無効（推奨） ・接続先アクセスポイントの確認
指導時の留意点	・テレワーク執務先別（在宅、シェアオフィス、公衆無線LAN）に無線LANも利用規則は明確になっているか

テレワーク導入・実施に絡む指導時の留意点

⑤紙資料に絡むリスク

事象	テレワーク用に家庭に持ち帰った紙の資料、事務所外で印刷した紙の資料より重要情報が漏洩してしまう。また、紛失・廃棄により原本を喪失してしまう。
固有の原因	・以下のような原因で、紙の資料より重要情報が漏洩してしまう 新聞、雑誌等に紛れ、古紙回収に出してしまう。 ・家族の鞄に紛れて入れてしまい、そのまま持ち出してしまう。 ・持ち帰りの移動中に紛失してしまう。 ・サテライトオフィス、コンビニ等で印刷を行い、印刷物を回収し損なう。
対策	・紙の資料の厳格な管理を行う。 ・作業空間と居住空間の明確な分離を行う。 ・事務所外で印刷を行う時は、印刷物の回収漏れに注意する。 ・事務所外での印刷のルールを定め、利用者は順守する。 ・紙の資料は極力廃止し、電子データとする。 ・複製のみ持ち出し可とし、原本の持ち出しは行わない。
指導時の留意点	・業務関連紙面の持ち出しの管理は台帳等で厳格に管理されているか ・事務所外での印刷、紙媒体の取り扱いは明確になっているか

テレワーク導入・実施に絡む指導時の留意点

⑥利用者認証情報の漏洩に伴う社内ネットワークへの不正侵入

事象	社内ネットワークにアクセスするための認証情報漏洩により、悪意のある第三者が従業員に成り済まして社内ネットワークに侵入する。
固有の原因	・事務所外より社内ネットワークにアクセスするための認証情報（ID、パスワード、ユーザ認証証明書 等）が漏洩したことにより第三者が成り済まして社内ネットワークに侵入する。
対策	・社内ネットワークにアクセスするための認証情報の厳格な管理を行う。 ・二要素認証、ワンタイムパスワード認証、MAC アドレス認証機能を導入する。
指導時の留意点	・認証情報の取り扱いの規則は明確になっているか ・認証情報漏洩等緊急事態発生時の連絡体制はテレワーク用に見直しが行われているか ・認証情報の取り扱いについてテレワーク勤務者への教育は計画的に行われているか

テレワーク導入・実施に絡む指導時の留意点

⑦テレワーク用社内接続経路の設計、設定ミスによる不正侵入

事象	テレワーク端末より社内ネットワークにアクセスするためのネットワーク経路を確立する時の設計、設定ミスによる不正侵入。
固有の原因	・事務所外より社内ネットワークにアクセスするための経路設定時の考慮もれ、設定誤り。
対策	・ネットワーク変更を行う時には、手順書通りの作業を実施し、設定変更後に外部からの侵入の可能性が無いかをチェックする。 ・定期的にアクセスログの監視を行う。
指導時の留意点	・認証情報の漏洩に備え、多段階認証、多要素認証等の対策は行われているか ・不必要に解放されているポートがないか等の監視は定期的に行われているか ・アクセスログの監視は定期的に行われているか

★要注意事例★
2020年８月にパッチ未適用のVPN装置（パルスセキュア社製）からのＩＤ・パスワード大量流出事件が発生しています。ネットワーク関連機器自体のソフトウェアアップデートも重要です。

テレワーク導入・実施に絡む指導時の留意点

⑧パブリッククラウドサービスの利用に伴うリスク

事象	ファイル共用サービス等のパブリッククラウドサービスを利用する事により情報漏洩が起きる。また、クラウドサービスの認証情報が漏洩する事により部外者がサービスを利用してしまう。
固有の原因	・テレワーク利用者が利便性を優先し、ファイル共用サービス等のパブリッククラウドサービスを利用し、システムの脆弱性、アクセス権限の設定ミス等により機密情報が漏洩してしまう。 ・事業所外部からのクラウドサービス利用により、認証情報が漏洩してしまう。
対策	・パブリッククラウドの利用ルールを整備し、安全に利用するためのサービス、利用手順等を明確にする。 ・テレワーク勤務者は定められたルールに従い、認められた範囲内でサービスを利用する。 ・多段階認証、多要素認証等を積極的に利用する。
指導時の留意点	・利用可能なサービス等を明確に定めているか ・職務に沿ったアクセス権限の見直しを随時実施しているか ・多段階認証等を利用できるサービスを積極艇に利用しているか ・認証情報の取り扱いについてテレワーク勤務者への教育は計画的に行われているか

テレワーク導入・実施に絡む指導時の留意点

⑨Twitterやインスタグラム等のSNS投稿に伴う情報漏洩

事象	テレワーク端末からTwitterやインスタグラム等のSNSに投稿する事により、機密情報が漏洩してしまう。
固有の原因	・テレワーク時、特に私物機器を利用した場合、SNSにログオンした状態で作業をしてしまい、業務上の機密情報を公開してしまう。 ・家庭で作業を行っているPC画面の内容がSNSの投稿に映りこんでしまい、機密情報が漏洩してしまう。
対策	・BYOD時には、ウイルス対策ソフトの導入、OS、アプリの最新化を必ず実施する。 ・画面映り込みを防止するため、プライバシーフィルターを装着する。 ・SNS利用のルールを定め、テレワーク勤務者は定められたルールに従う。 ・テレワーク勤務者への教育、注意喚起を計画的に実施する。
指導時の留意点	・私物機器の取り扱いルールは明確になっているか ・テレワーク時ののぞき見防止ルールは明確になっているか ・テレワーク勤務者への教育は計画的に行われているか

２　業界別の固有の注意点

業界別の固有の注意点（オンライン診療）

オンライン診療に関する指針は厚生労働省が**「オンライン診療の適切な実施に関する指針（平成30 年３月）」**として策定しているので、オンライン診療に関する指導を実施する際には当指針に則った対策が施されているかを確認する必要があります。以下にその要点を示します。

オンライン診療とは

・Web会議サービス等を利用して遠隔地にいる患者の診察及び診断をリアルタイムで実施。

ガイドラインの考え方

・個人情報の保護に最大限の配慮が必要。
・患者側端末は個人所有のスマートフォン等多様であるため、オンライン診療サービス提供者側で万全のセキュリティ対策を講じる。
・情報セキュリティ対策について患者・医師・オンライン診療サービス提供事業者の三者での合意を行う。
・医療情報システムとの接続を行う場合と接続を行わない場合とで対策が大きく分かれる。

指導時の留意点

・指針に即したセキュリティ対策を行っているか。
・指針で示す情報セキュリティに関するルール（セキュリティ対策の内容、セキュリティ事案や損害発生時の責任の所在、データ保存の有無や保存内容等）を厳守したサービスであるかを規約等で確認・理解しているか。
・利用者（医師）に対して、十分な情報セキュリティ教育を実施する体制となっているか。

業界別の固有の注意点（教育機関）

教育機関には多くの機微な情報を含む個人情報が含まれており、情報漏洩が発生すると、社会的影響も大きい。しかし、例年、２００件前後の個人情報漏洩(※1)が発生しているのも現状である。また、新型コロナウイルスの影響により、急遽オンライン授業を取り入れた教育機関も多く、情報セキュリティにはしっかりした対策が求められます。ポリシー策定時には**「教育情報セキュリティポリシーに関するガイドライン（令和元年 12 月版）」**を参照し、抜け漏れがないかを確認して下さい。（※1：ISEN「令和元年度　学校・教育機関における個人情報漏えい事故の発生状況 -調査報告書- 第１版」）

ガイドラインの考え方

- 基本理念を基に、情報セキュリティポリシーの策定と運用ルールの見直しを行うことを期待
- 情報セキュリティインシデントが発生時の拡大防止・迅速な復旧や再発防止の対策を講じること
- 情報セキュリティに関する意識・リテラシーを高め、主体的にその対策に取り組むこと

情報セキュリティ基本理念

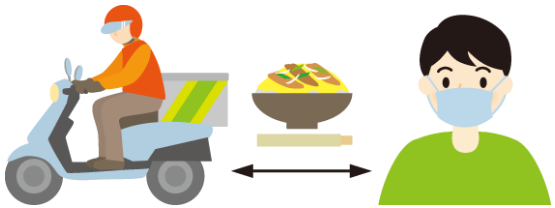
①組織体制の確立（情報セキュリティの責任体制を明確化し、対策実施のための組織作りを行う）
②児童生徒による機微情報へのアクセスリスク対応
③インターネット経由による標的型攻撃のリスクへの対応
④教育現場の実態を踏まえた情報セキュリティ対策の確立
⑤教職員の情報セキュリティに関する意識の醸成
⑥教職員の業務負担軽減及びICTを活用した多用な学習の実現

指導時の留意点（オンライン学習）

- セキュリティが適切に確保されているサービス、およびサービス提供者を選定しているか
- 利用者（生徒、教職員）に対するITリテラシー教育は計画的に実施されているか

業界別の固有の注意点（飲食業）

飲食業は新型コロナウイルスによる影響が大きい業界です。外出制限や営業時間の短縮により、個人宅へのデリバリを始めた店舗も多く、今までは、個人情報はほとんど保有していなかった小規模店舗が多くの個人情報を扱うようになり、その管理体制が整備されているかに注意する必要があります。また、外部サービス利用時には、サービス提供元のセキュリティレベルを考慮して選定しているかを確認する必要があります。



指導時の留意点

■顧客の個人情報の保有の有無を確認し、有の場合は管理体制を確認する

（自店舗内で保存している場合）

・保存媒体、情報の内容、アクセス権、保存期間　等

（外部サービス利用の場合）

・サービス選定時のサービス提供元のセキュリティレベルの確認

・クレジットカード決済を行う場合は、その扱い

（従業員への教育）

・個人情報の取り扱いに関する教育・啓発は定期的に実施されているか

３　Web会議サービスの
セキュリティ上の留意点

Web会議サービスのセキュリティ上の留意点

多くの企業が、テレワーク実施時にWeb会議サービスを利用しています。Web会議サービスを導入・利用するにあたり、注意すべき点をIPAがまとめていますので、その資料を基に、中小企業にセキュリティ指導を行う上での要点を以下に示します。詳細は「**Web会議サービスを使用 する際のセキュリティ上の注意事項**」の資料を参照してください。

Web会議サービス選定時に考慮すべきポイント

会議データの所在

Web会議データで扱うデータ保存場所は情報漏洩リスクに大きく影響する。
データ保存場所がクラウドの場合、会議の機密性を考慮し、以下の確認を行う。

- 国内のデータセンターにデータは保存されるか
- 復元不可能な形で削除可能か

暗号化

Webサイト等で、暗号アルゴリズムや通信方式の確認を行う。
特に、暗号化の方式として暗号鍵の扱いが以下のどちらかは重要。

①サービス提供者が暗号鍵をもたないエンドツーエンド暗号化方式
　暗号鍵は参加者のみが保有するため、サービス提供者は復号できない
②サービス提供者が暗号鍵を持ち会議データがサーバで復号可能な方式
　サービス提供者を信頼できても海外には政府によるサーバのデータの強制収容リスクあり
※上記の両方式を選択できる場合、エンドツーエンド暗号化を選択するとサーバでの復号を必要とする機能は使えなくなる可能性がある

Web会議サービスのセキュリティ上の留意点

Web会議サービス選定時に考慮すべきポイント

会議参加者の確認・認証方式

意図しない者の会議へ参加を防ぐためには、会議案内メールの安全な経路での配付と共に、会議参加者の確認・認証方式の選定が重要であり、主催者が、参加者を容易に確認でき、必要に応じ参加者を強制退室できる機能も重要

（主な会議参加者の確認・認証方式）

- 会議パスワード設定機能
- 待機室（ロビー）での参加者確認機能
- 参加者の事前登録機能
- 参加者名の設定機能
- 二要素認証

プライバシーポリシー

Web会議 サービスでは音声・映像、参加者のメールアドレス等の属性等様々な個人情報を扱うので、これら個人情報が会議目的以外で第三者提供を含め使用されないこと、個人情報保護法等の法律 、 規制 に準拠していることを確認する。

脆弱性と企業姿勢

サービス提供者のウェブサイト、JVN iPedia、ニュース等の脆弱性情報をウォッチし、Web 会議サービスの脆弱性の発生状況、対策状況を把握すると共に、サービス提供者のセキュリティに対する取組姿勢と情報公開の姿勢を確認する。

Web会議サービスのセキュリティ上の留意点

Web会議サービスを安全に開催するためのポイント

会議の準備時

- ✓ 会議の機密性の確認
- ✓ 会議の機密性に応じたWeb会議開催方法の決定
  - ① エンドツーエンド暗号化の会議は利用可能か？否の場合、サーバで万が一復号されるリスクは許容可能か？
  - ② 外部組織の人が参加する場合には、セキュリティポリシーに準拠の同意を得たか？
  - ③ Web会議サービス参加者の制限を明確にし、会議の設定を適切に行う
  - ④ 意図しない参加者が登場した場合に備え、強制退室機能が利用可能なことを確認
- ✓ Web会議開催案内
  - ① 会議 URL 、 会議パスワード等を記載した会議開催案内 の送付経路は安全か？
  - ② 機密性の高い会議では 、メールの題名は機密性を悟られない文面となっているか？

会議の実施時

- ✓ 参加者の確認
- ✓ 会議終了後のデータ削除

その他の一般的注意事項

- ✓ 会議で使用するクライアント端末のセキュリティ
  クライアントソフト、OS等は、最新の状態にアップデートされているか
- ✓ 会議の参加環境（意図しない映り込みや音声の漏えいを避ける）に配慮する

Web会議サービスのセキュリティ上の留意点

機密性別のWeb会議の開催例

	機密性「高」の会議	機密性「中」の会議	機密性「低」の事前申し込みを必要とする講習会
資料共有、録画機能	使用しない 資料は別途共有	使用しない 資料は別途共有	使用可
データセンター	国内のみを使用する契約	輸出管理上のグループAの国の データセンターのみを使用する契約	制限しない
暗号化	エンドツーエンド	参加者端末、サーバ間の通信は暗号化	参加者端末、サーバ間の通信は暗号化
会議案内	会議パスワードを設定、 待機室機能を有効とし、 会議パスワードは会議案内メールとは別経路で安全に届ける。	会議パスワードを設定、待機室機能を有効とし、会議パスワードは会議案内メールとは別経路で安全に届ける。	参加者事前登録の機能を使用し、参加者の事前確認をするとともに、会議のURLは参加者のみに届ける。
参加者の確認	組織外参加者については会議実施時に声、顔での確認を行う。	担当をアサインし確認を行う。	担当をアサインし確認を行う。

４　指導時のWeb会議サービスの利用について

指導時のWeb会議サービスの利用について

指導は、実際に指導先を訪れ、指導することが原則ですが、指導先企業の要望等、その他必要に応じてオンラインで行うこともできます。オンラインで指導を行う時の注意点を説明します。指導先に既に環境があれば、当該ツールを利用するのが最善になります。環境が無ければ、セキュリティ上、信頼のおけるツールの利用を検討して下さい。

セキュリティ上の留意点

- ✓Web会議サービスは有料版を利用する
- ✓ミーティング情報の件名に機密情報は記載しない
- ✓会議URLは慎重に取り扱う
- ✓ミーティング録画ファイルは適宜削除する
- ✓アプリケーションは最新状態に保つ

運営上の留意点

- ✓接続のトラブルも考え、時間に余裕を持って参加する
- ✓参加前にマイク、カメラのチェックを行う
- ✓ツールの使い方は練習を行い、事前に把握しておく
- ✓正確な情報伝達にはチャット機能も利用する
- ✓相手に伝えるためには少し大げさに反応する

5　参考資料

参考資料

◆ 「テレワークを行う際のセキュリティ上の注意事項」 （IPA）
https://www.ipa.go.jp/security/announce/telework.html
テレワークを行う際にセキュリティ上注意すべきことを網羅的に説明しています。他機関によるテレワーク関連セキュリティ情報へのリンクも多数掲載されています。

◆ 「Web会議サービスを使用する際のセキュリティ上の注意事項」 （IPA）
https://www.ipa.go.jp/security/announce/webmeeting.html
テレワークには必須のツールであるWeb会議サービスを導入、利用するにあたり、セキュリティ上注意すべきことをまとめた資料。

◆ 「テレワークにおけるセキュリティ確保」 （総務省）
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
「テレワークセキュリティガイドライン」「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」等へのリンクが掲載されています。

◆ 「オンライン診療に関するホームページ」 （厚生労働省）
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/rinsyo/index_00010.html
オンライン診療を適切に実施するための関係情報を紹介しています。オンライン診療時のセキュリティ関連の情報は「オンライン診療の適切な実施に関する指針」を参照。

◆ 「教育情報セキュリティポリシーに関するガイドライン」 （文部科学省）
https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1397369.html
地方公共団体が、設置する学校を対象とする情報セキュリティポリシーの策定や見直しを行う際の参考となるよう、学校における情報セキュリティポリシーの考え方及び内容について解説した資料。