業界セキュリティガイドライン適用のマネジメント指導業務　実施要領

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

IPA Better Life with IT

本書の構成

- 業界セキュリティガイドラインの適用にあたり、業界向け情報セキュリティ関連規程（サンプル）及びIPAのセキュリティ対策支援ツールを活用した4回の標準的な専門家の指導内容（標準カリキュラム）と、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」は、セキュリティの専門家による指導の下、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など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	**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 ・各回毎の指導の内容（標準的な進め方） ・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** ・使用するツール/資料 ・参考資料

プログラム①
専門家指導全体の構成と留意事項

専門家からの説明内容

	項目	説明内容
1	専門家指導の全体構成	✓ 実施要領の位置付け、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 ＊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

当事業の目標と成果物

- 「中小企業の情報セキュリティガイドライン(第3.1版)」をもとに、業種特性および業界固有の情報取扱い、業界専門用語等を反映し、業界共通の基本的なセキュリティ対策（業界団体対応版）として策定します。
- 策定した「業界団体対応版」に対応した「業界向けサンプル規程」を策定し、これを基にした個社の「規程（案）」、及び今後「業界団体対応版」に準拠するためのセキュリティ対策の進め方をまとめた「実行計画書（案）」を策定します。

マネジメント指導業務の達成目標と成果物

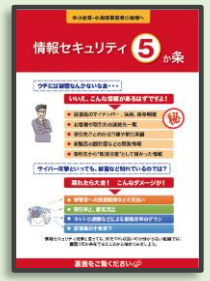
中小企業等の対策実施レベル

【達成目標１】情報セキュリティ基本方針の作成
【達成目標２】現状における自社の情報セキュリティリスクの洗い出し
【達成目標３】情報セキュリティ対策実行計画の策定
【達成目標４】自走化に向けた情報資産棚卸し/リスク分析
および必要なセキュリティ対策の実装（継続対応）

注：成果物

達成目標1

取組みスタート

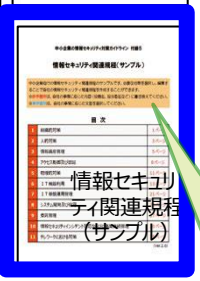


- 情報セキュリティ基本方針
- 情報セキュリティ関連規程類の点検結果

達成目標2

- 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3



- 情報セキュリティ対策実行計画書

今後の自社で取り組む情報セキュリティ対策の進め方を実行計画書にまとめる

達成目標4

自走化に向けた情報資産棚卸し/リスク分析

必要なセキュリティ対策の実装

- 関連規程の整備
- 技術的対策
- セキュリティサービス利用 等

業界共通の基本的なセキュリティ対策（業界団体対応版）に対応した「業界向けサンプル規程」を基にした個社の規程（案）を策定する

「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(EXCEL版)の実施依頼
	第１回	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 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。
1～2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	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 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、経営施策に対する情報セキュリティリスクの検討
	第３回	情報セキュリティ対策の重点対策の検討と優先順位付け 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	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 専門家がまとめた業界セキュリティガイドライン適合のための実行計画案（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ます。

計1.5ヶ月程度

「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
	2	「5分でできる情報セキュリティ自社診断(EXCEL版)」の実施	同左の実施依頼	【提供】自社診断(EXCEL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
	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(EXCEL版)の結果の理解と課題認識についてのディスカッション	自社診断(EXCEL版)の結果についての説明と、改善領域に関する現状確認と要望の確認	【成果物】自社診断(EXCEL版)の結果のまとめ
	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 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。

「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(EXCEL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　情報セキュリティ対策の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	経営施策と情報システム環境の状況整理	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	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	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
	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	（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**＞
- 直近の経営施策を踏まえ、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）から専門家が助言します。
- 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	–	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	業界セキュリティガイドライン適合のための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】業界セキュリティガイドライン適合のための実行計画書 【成果物】基本方針/関連規程の点検結果・業界向け情報セキュリティ関連規程の適用 【成果物】自社診断(EXCEL版)結果報告
	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」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。

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	企業様の検討体制(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。 ・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	✓ 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。 ・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。 ✓ 検討方法は、各専門家のやり方(経験)を踏まえ実施します。 ・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ます。 （企業によって、検討方法が異なる場合があります）
3	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をお知らせください。 ・無し⇒別途事前準備の打ち合わせなどでの試行を提案します。 ・有り⇒使用中のWeb会議ツール/環境をお知らせください。 （企業様の環境や意向に合わせて対応します） ※Web会議の使用ライセンスに要する費用は、専門家が負担することも可能です。 ✓ 企業様の希望によっては、専門家指導のうち何回かをリモート会議で行うことも可能なので、企業様の意向をお知らせください。
4	提供を受ける情報の取り扱い	✓ 企業様にいただいた情報は専門家、及び事業を実施する情報処理推進機構（委託先を含む）において取り扱いに留意します。 ✓ 情報の取り扱いに関して希望があれば相談に応じます。

初回指導時の留意点

専門家限り

- 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、企業様の状況を踏まえて進めます。
  ⇒ Q&A方式、セッション形式、ファシリテーション等、様々な形態を想定します。
- 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。
  ⇒ 円滑に進めるために可能な限り事前にタイムスケジュールを専門家から提示します。
  ⇒ 企業様との合意に基づき、訪問をせずにWeb会議で指導を行うことも可能です。

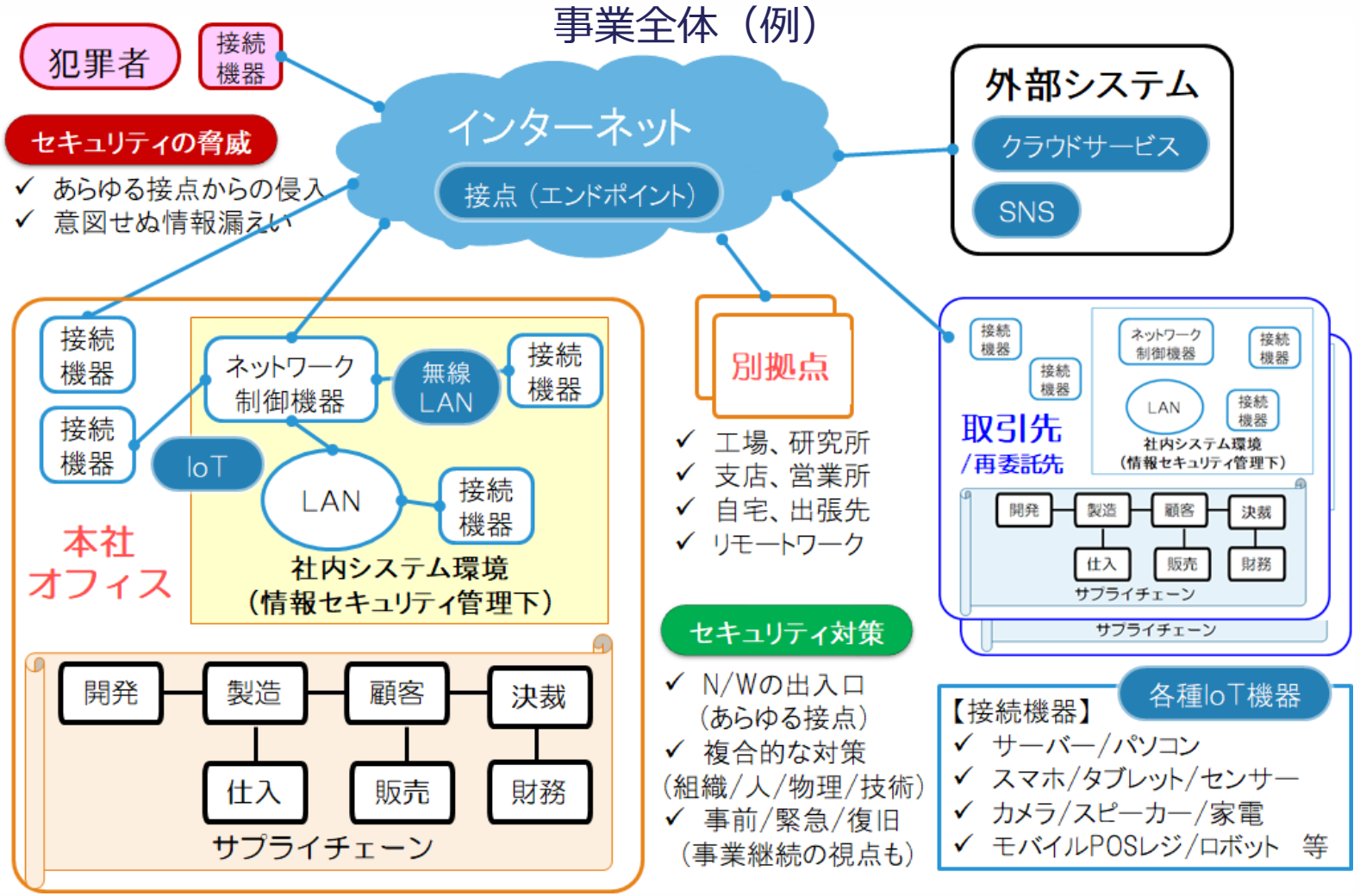
進め方（例）

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 *当日の進め方と準備資料についての説明と合意 *情報の取り扱い	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）

参考

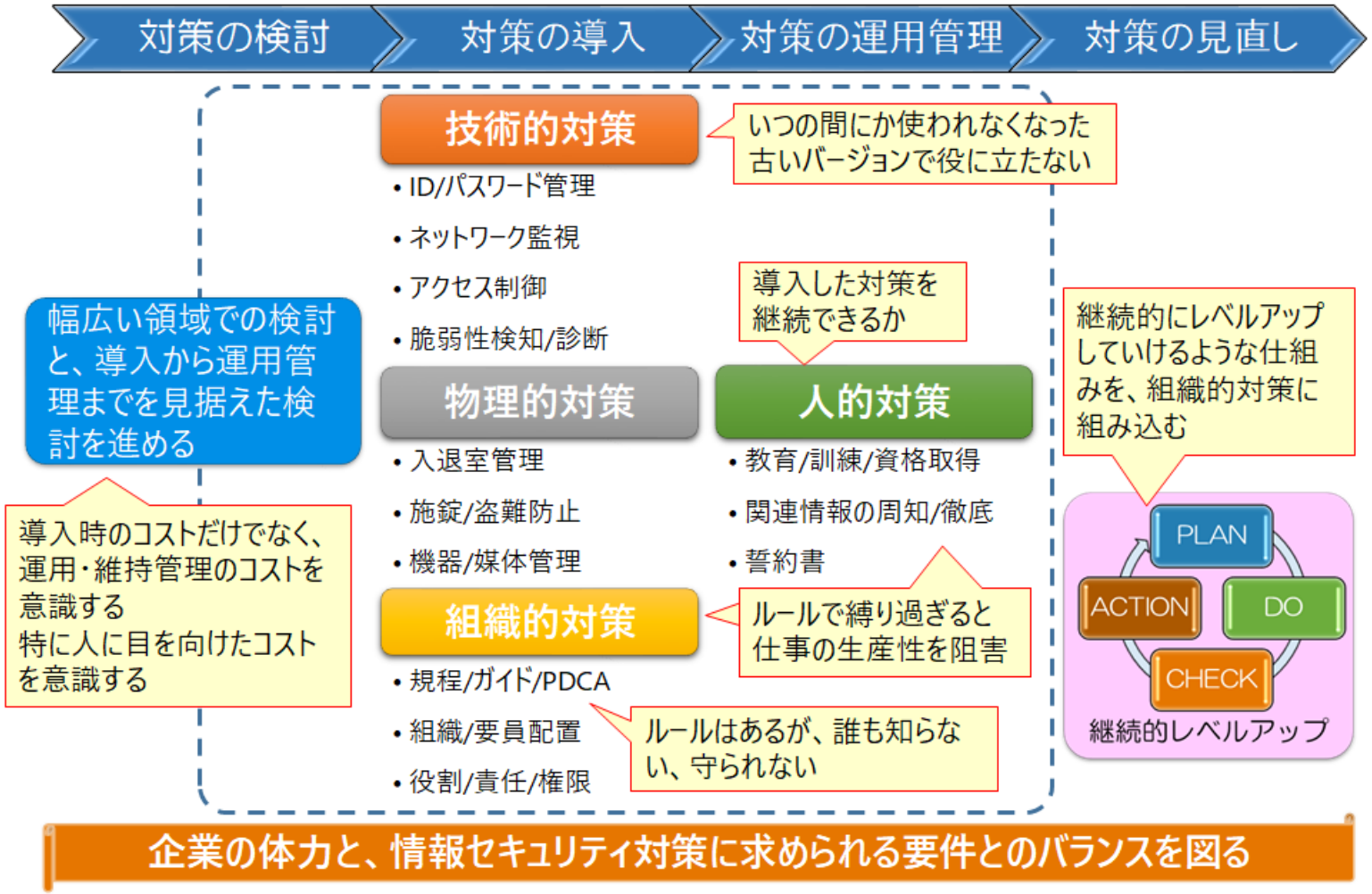
- 指導先企業の事業全体を広範囲に俯瞰した上で、今回の対策検討の対象領域を絞り込んでいきます。



対策絞り込みの留意点（対策の実効性、継続性）

参考

- 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します。
- 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します。



『各種ツールの活用方法』参照

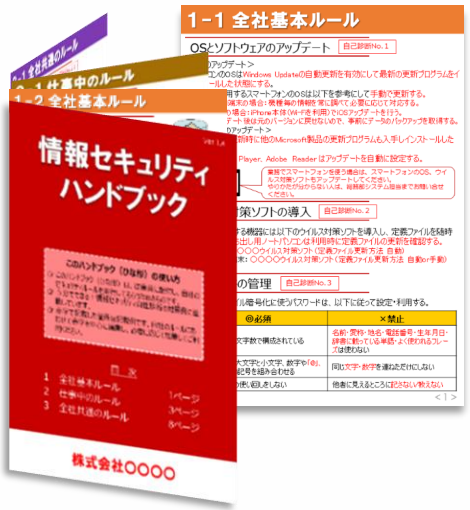
成果物作成の留意点 （要提出の成果物）

	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(EXCEL版)」による、現状のリスク洗い出し結果	✓ 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可能です。
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 業界向け情報セキュリティ関連規程の適用結果 ※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いただきます。 ✓ 関連規程の点検の際には、業界向け情報セキュリティ関連規程を適用します。 ✓ 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します。
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	✓ 継続的に実行(運用)が可能な対策になっているか、また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います。

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3.1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・不足が無いか確認し、作成後は、従業員や関係者に文書等で周知・徹底します。
- 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。



【情報セキュリティ基本方針】
株式会社○○○○（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、及び別途提示する業界向け情報セキュリティ関連規程（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反映します。
- 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します。
  https://www.ipa.go.jp/security/guide/sme/about.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）

	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、廃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を定めます。	
11	テレワークにおける対策	テレワークにおけるＩＴ機器利用やＩＴ基盤運用管理、勤務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（対策実行計画書）

- 全4回の指導の成果物として「業界ガイドライン適合のための実行計画書」を作成します。
  ※ 今後1年程度の期間で対応できるものに絞り込みます。

- 指定されたEXCELファイルの様式で記入します。(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	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. 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。

プログラム②
各種ツールの活用方法

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	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）

専門家限り

- 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（自社診断結果／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」を使用します。
- 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

- 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、診断結果を共有します。
- 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。

自社診断実施の留意点（自社診断結果／成果物① ）

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みます

使用するツール/資料の内容（基本方針／成果物② ）

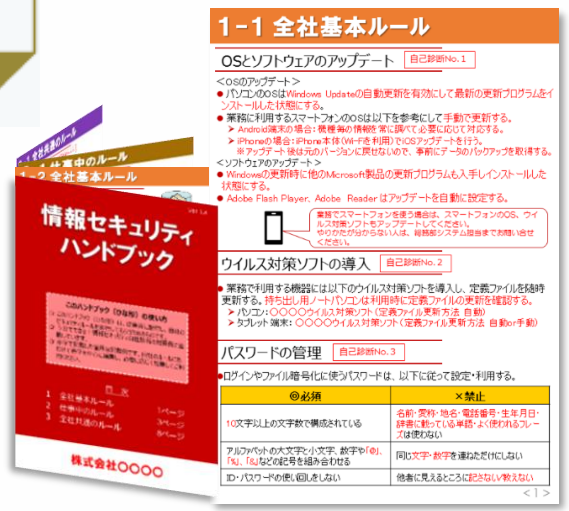
- 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」にひな形となるWORDファイルが付録されています。
  サンプルをもとに情報セキュリティ基本方針を作成します。
  ⇒ https://www.ipa.go.jp/security/guide/sme/about.html
  ⇒ 情報セキュリティ基本方針

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。



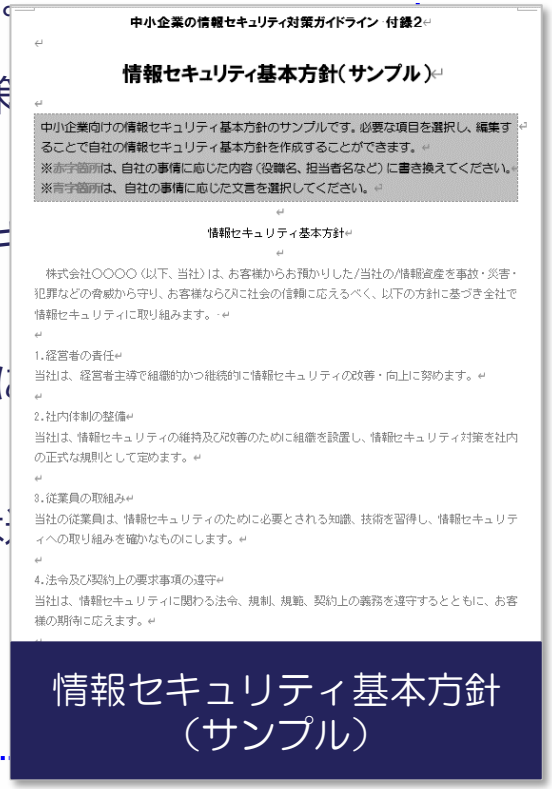
成果物作成の留意点（基本方針／成果物② ）

- 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ます。

【情報セキュリティ基本方針】
株式会社○○○○（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
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
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
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
し、再発防止に努めます。

制定日:20○○年○月○日
株式会社○○○○
代表取締役社長　○○○○


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○○○○（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）
  - 業界向け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、廃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を定めます。	
11	テレワークにおける対策	テレワークにおけるＩＴ機器利用やＩＴ基盤運用管理、勤務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（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」を作成します。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みます。

改善分野	現状と課題	具体的改善対策	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. 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。

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。

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/guide/sme/about.html
- 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

様式一覧

- 【様式1】ヒアリングシート
- 【様式2】関連規程類の点検結果シート
- 【様式3】業界ガイドライン適合のための対策実行計画書