セキュリティマネジメント指導（テーマ別）実施要領

テーマ①｜情報セキュリティ規程の整備

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

本資料の位置づけ（指導の全体像）

本資料は、セキュリティ専門家が中小企業に対して行う訪問指導「**セキュリティマネジメント指導（テーマ別）**」の説明資料です。

訪問指導では、専門家が中小企業の特性に応じたセキュリティ対策を指導する際の基本的なフレームワークを提供することを目的としています。特に中小企業は、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、どの部分に重点を置くべきかが明確でないケースが多々あります。

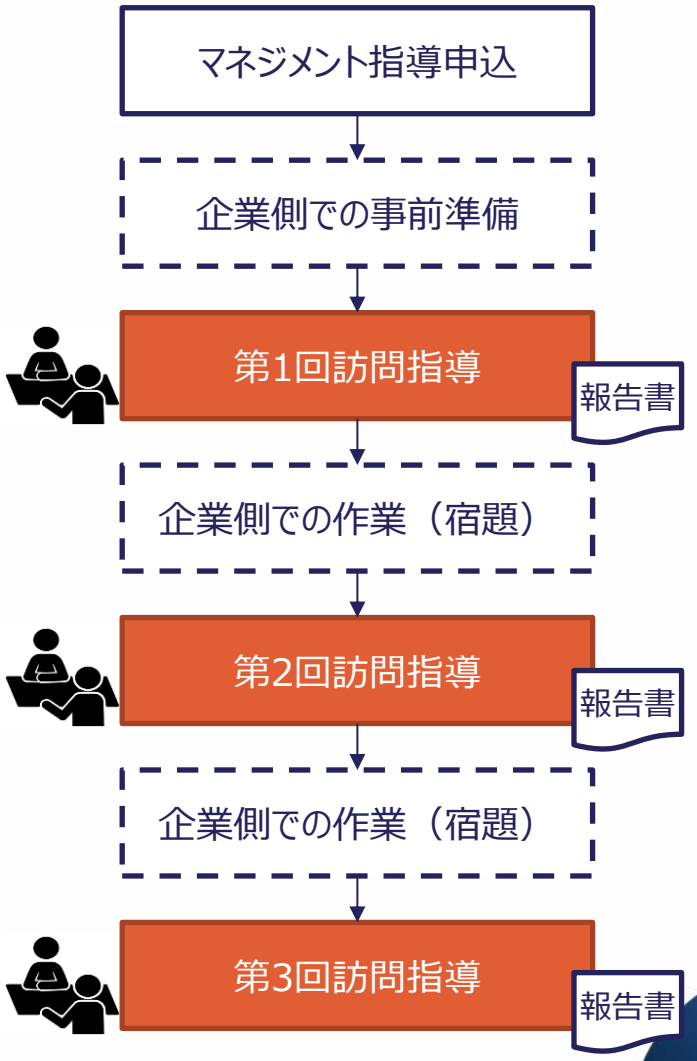
マネジメント指導（テーマ別）では、そのような中小企業に対して、**①情報セキュリティ規程の整備**、**②情報資産の洗い出しとリスク分析**、**③クラウドサービスの安全利用**、**④セキュリティインシデント対応**、そして**⑤従業員向けのセキュリティ教育** の5つの主要なテーマを指導するための具体的な方法と手順を提供しています。

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、指導後の効果の考え方等を想定しています。これにより、専門家は訪問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。

本資料では、専門家が現場で利用できる具体的なシラバスやチェックシート、ガイドラインも挙げております。実際には企業に訪問した際は、企業の実情に応じた柔軟な対応をお願いすることとなりますが、ツール活用によってある程度訪問指導の際の一貫性が確保され、企業においても自律的なセキュリティ対策の強化が期待できると考えます。

専門家のみなさまにおかれましては、本資料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対応ください。

マネジメント指導の流れ



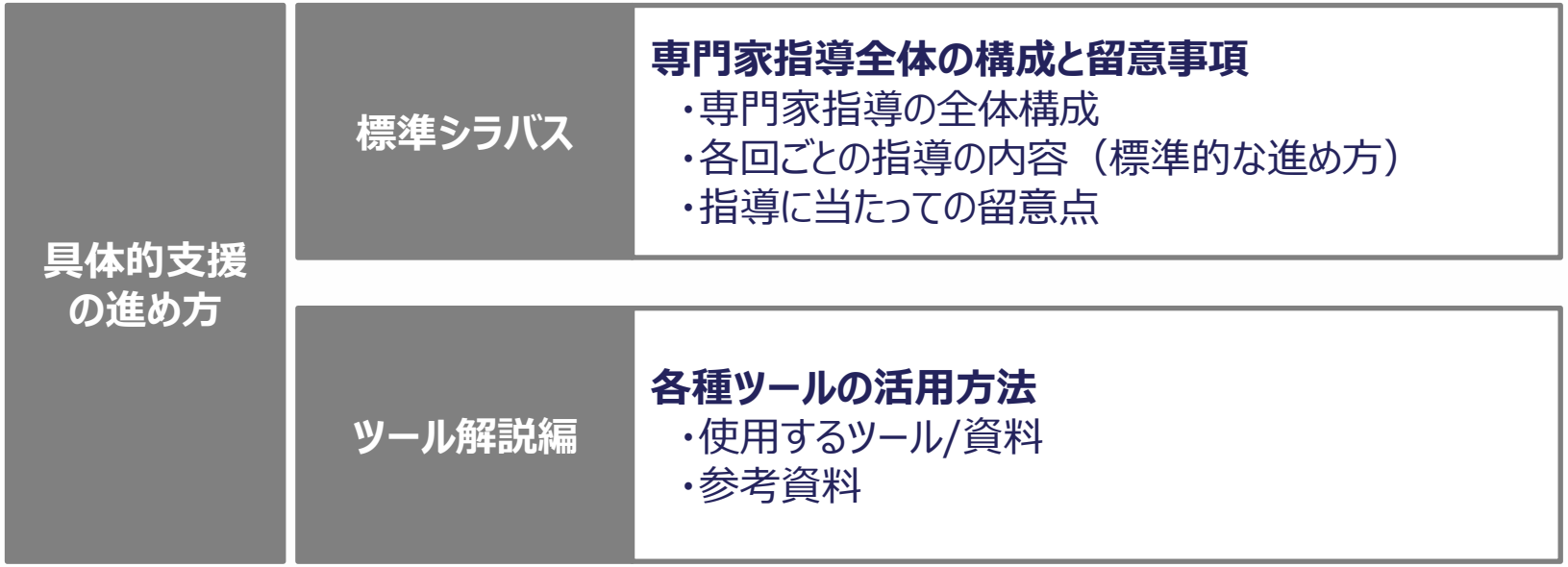
マネジメント指導のテーマと狙い

今回用意したマネジメント指導のテーマは以下の5テーマです。
企業の実情に即し、原則として以下のテーマから選定の上、企業への訪問指導を行っていただきます。

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

本書の構成

- 企業へのマネジメント指導を行うにあたり、5つの指導テーマについて、主にIPAのセキュリティ対策支援ツールを活用した3回の標準的な専門家の指導内容（標準シラバス）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、標準シラバスを示しつつ、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。



テーマ① | 情報セキュリティ規程の整備

【標準シラバス】
専門家指導全体の構成と留意事項

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)」における「情報セキュリティサンプル規程」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）」を策定・整備します。
- 指導期間中にすべての規程を網羅整備しなくとも、トライアル的な取り組みとしていただいても構いません。

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

「標準的な進め方」の全体構成

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
支援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。

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
支援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。

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
*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1.5ヶ月程度

「標準的な進め方」の詳細（１）

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

		企業	専門家	成果物/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！自社診断（Excel版）」による自己診断の実施	（事前配布）	【提供】5分でできる！自社診断チェックシート（Excel版）
	3	「情報セキュリティ関連規程チェックシート」による自己診断の実施	自己診断の実施依頼	【提供】情報セキュリティ関連規程チェックシート
	4	出席メンバー選定 (経営者/従業員等、半日x3回)	専門家指導の作業内容、全体スケジュール案の作成、初回訪問日程の事前確認	初回のスケジュール調整
当日	1	説明事項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 【提供】サンプル基本方針／関連規程
	2	自社診断(Excel版)の結果の理解と課題認識についてのディスカッション	自社診断(Excel版)の結果についての説明と、改善領域に関する現状確認と要望の確認	【成果物】自社診断(Excel版)の結果のまとめ
	3	「情報セキュリティ関連規程チェックシート」の結果と課題認識についてのディスカッション	「情報セキュリティ関連規程チェックシート」結果から得られる要改善点や今後の作業のポイント等説明	【成果物】情報セキュリティ関連規程チェックシート（途中版、引き続き作業指示）
	4	依頼事項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	（終了後） 実施報告書の作成

＜**実施のポイント**＞
- 第1回の指導では、ヒアリングによって、企業側での情報セキュリティ関連規程の現時点での整備状況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　新規程案の作成・チェックと適切な運用方法についての指南

		企業	専門家	成果物/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	【提供】サンプル基本方針／関連規程 【提供】情報セキュリティ関連規程チェックシート
当日	1	依頼された必要情報の提供・説明	提供された情報の確認・質疑応答	-
	2	基本方針/関連規程の有無/作成状況の説明 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	説明事項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 ・規程や条文のスコープ（対象範囲）、ISMSの文書体系の考え方や既存文書との整合性チェック、流用の考え方など、規程整備に際し考慮しなければならない項目等	【成果物】情報セキュリティ関連規程チェックシート
	4	必要な追加情報の提供了解	改善領域の対策検討に必要な追加情報の提供依頼	（終了後） 実施報告書の作成

＜**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　新規程の運用方法の確認

		企業	専門家	成果物/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	新規程の社内周知を含む運用手順案の作成	適宜アドバイス	【提供】サンプル基本方針／関連規程
当日	1	経営施策の説明と、情報セキュリティ対策の必要性の理解	新規程に基づき、今後必要となる情報セキュリティ対策の説明	【提供】指導講習コンテンツ
	2	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	作成した成果物の説明と合意	成果物のレビューと合意	【成果物】基本方針/関連規程の点検結果及び新たに策定した基本方針 【成果物】自社診断(Excel版)結果報告
		専門家指導についての評価	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う 【成果物】最終報告書

＜**実施のポイント**＞
- 第2回までの検討をもとに、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）	✓ 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。

【ツール解説編】
各種ツールの活用方法

使用するツール/資料の内容（自社診断結果）

- 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

- 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）

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）

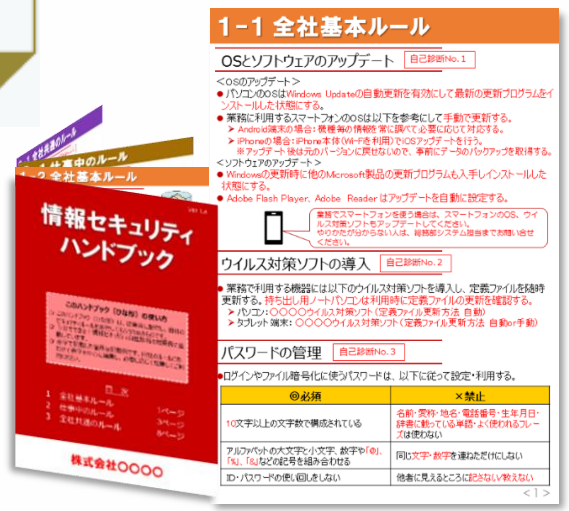
- 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」にひな形となるWORDファイルが付録されています。
  サンプルをもとに情報セキュリティ基本方針を作成します（既に作成されたものがあれば、内容に不備・不足が無いか確認）。
  ⇒ https://www.ipa.go.jp/security/guide/sme/about.html
  ⇒ 情報セキュリティ基本方針

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。



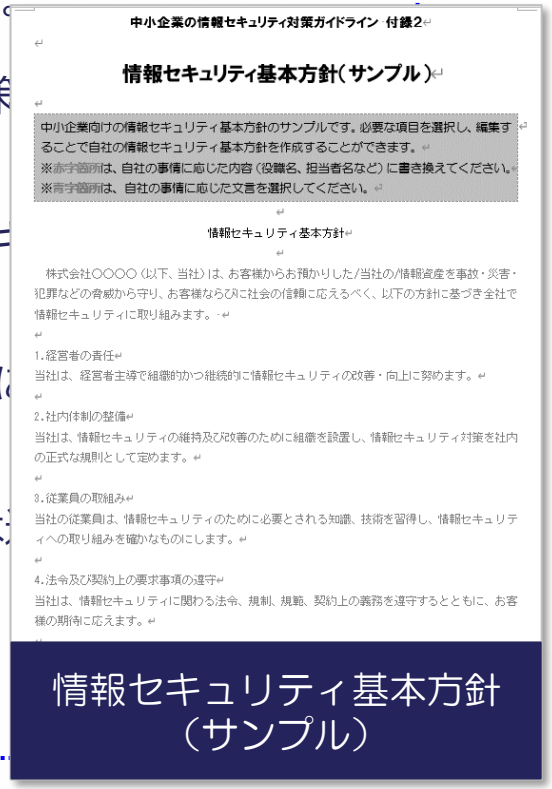
成果物作成の留意点（基本方針）

- 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）

使用するツール/資料の内容（関連規程類の点検）

- 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。
（情報セキュリティ規程チェックシート）

No	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（関連規程類の点検シート）

- 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ご確認ください。
- 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。

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					

使用するツール/資料の内容（関連規程類の策定 ）

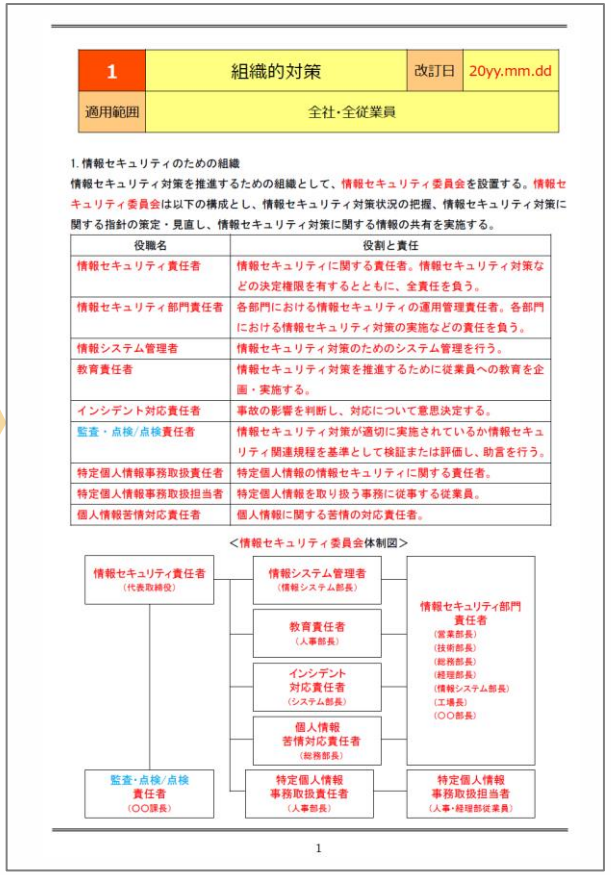
- サンプル規程をもとに、企業独自の情報セキュリティ関連規程（案）を策定します。
  - 中小企業の情報セキュリティ対策ガイドライン 付録２ 情報セキュリティ基本方針（サンプル）
  - 同 付録５ 情報セキュリティ関連規程（サンプル）または 自動車産業向け情報セキュリティ関連規程（サンプル）

【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 （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 （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。 ・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。 ・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 （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**

成果物作成の留意点（関連規程類の策定）

◇情報セキュリティ管理規程（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 2.情報セキュリティ取組みの監査・点検/点検 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 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	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 2.情報資産の社外持ち出し 3.媒体の処分 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 2.利用者の認証 3.利用者アカウントの登録 4.利用者アカウントの管理 5.パスワードの設定 6.従業員以外の者に対する利用者アカウントの発行 7.端末の識別による認証 8.端末のタイムアウト機能 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 2.関連設備の管理 3.セキュリティ領域内注意事項 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 2.ＩＴ機器の利用 3.クリアデスク・クリアスクリーン 4.インターネットの利用 5.私有ＩＴ機器・電子媒体の利用 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 2.ＩＴ基盤の情報セキュリティ対策 3.ＩＴ基盤の運用 4.クラウドサービスの導入 5.脅威や攻撃に関する情報の収集 6.廃棄・返却・譲渡 7.ＩＴ基盤の情報セキュリティ要件及び標準

成果物作成の留意点（関連規程類の策定）

◇情報セキュリティ管理規程（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 2.脆弱性への対処 3.情報システムの開発環境 4.情報システムの保守 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 2.委託先の選定 3.委託契約の締結 4.委託先の評価 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 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及び報告 4.対応手順 5.届出及び相談 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
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 2.情報機器のセキュリティ 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 4.勤務中のルール 5.データ・書類の保存 6.社内問い合わせ・緊急連絡先

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

- 中小企業の情報セキュリティ対策支援サイト
  https://www.ipa.go.jp/security/sme/isec-portal.html
  - 5分でできる！情報セキュリティ自社診断
    https://www.ipa.go.jp/security/guide/sme/5minutes.html
  - 情報セキュリティ対策ベンチマーク
    https://www.ipa.go.jp/security/sec-tools/benchmark.html
  - ５分でできる！ポイント学習
    https://www.ipa.go.jp/security/sec-tools/5mins_point.html
- セキュリティプレゼンター向け資料ダウンロード
  https://www.ipa.go.jp/security/sme/presenter/presenter-materials.html
- 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
- SECURITY ACTION セキュリティ対策自己宣言
  https://www.ipa.go.jp/security/security-action/
- 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/videos/list.html
- 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