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②｜情報資産の洗い出しとリスク分析

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。

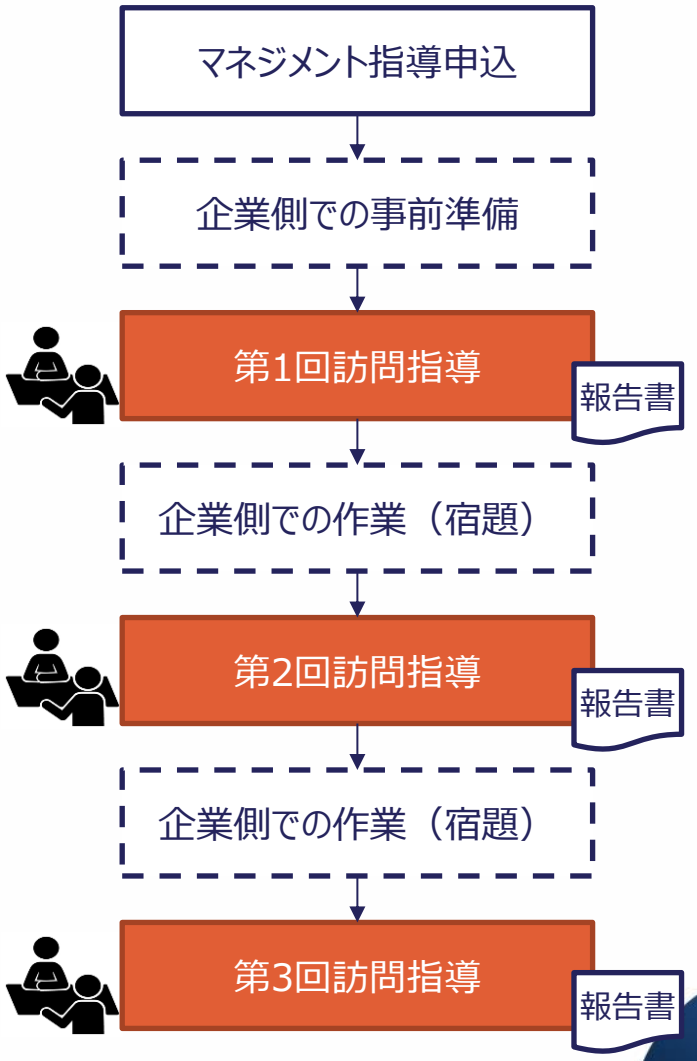
マネジメント指導（テーマ別）では、そのような中小企業に対して、**①情報セキュリティ規程の整備**、**②情報資産の洗い出しとリスク分析**、**③クラウドサービスの安全利用**、**④セキュリティインシデント対応**、そして**⑤従業員向けのセキュリティ教育** の5つの主要なテーマを指導するための具体的な方法と手順を提供しています。

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



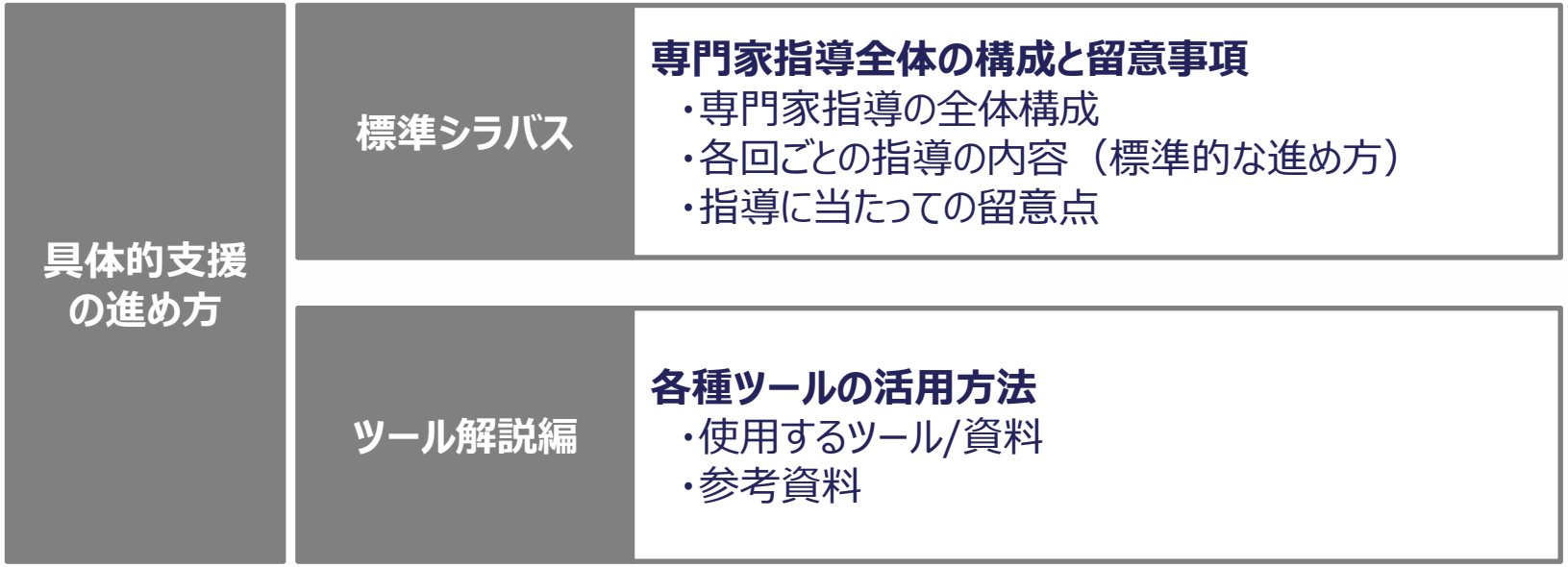
マネジメント指導のテーマと狙い

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② | 情報資産の洗い出しとリスク分析

【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)」における付録7「リスク分析ワークシート」を基に、指導先企業における情報資産の洗い出しとリスク分析を実施し、今後必要となる情報セキュリティ対策についてアドバイスします。
- 必ずしも、社内全ての情報資産の洗い出し、リスク分析を完璧に行わなくとも、一部のトライアル的な実施でも構いません。

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】自社における情報資産の洗い出し（一部または全部）
【達成目標３】抽出した情報資産リストに対するリスク分析の実施
（一部または全部）

注：成果物

取組みスタート

達成目標1

自社診断シート

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

達成目標2

- 社内における情報資産の洗い出し

達成目標3

- 情報資産に対するリスク分析実施

継続実施

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

「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
*「リスク分析シート」における情報資産洗い出し作業の実施依頼

第１回
社内情報資産の洗い出し
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、企業側が作成した分析シートに基づきヒアリングを行い、必要に応じ加筆修正指示を行います。

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リスク分析を実施
*特に「リスク大」と評価された資産に対するリスク低減策や回避策について検討

第２回
社内情報資産のリスク値の算定
支援先企業側が作成した分析シートに基づきヒアリングを行い、必要に応じ加筆修正指示を行うとともに、企業側が示したリスク回避策や低減策についてアドバイスを行います。また、継続的な運用方法の考え方について指南します。

1～2週間 → 事前準備＃３
*リスク評価案に対する見直しを実施
*リスクの大小に応じて、それぞれ低減策や回避策を検討しFIXさせる

第3回
社内情報資産に対する情報セキュリティ対策等運用方法の検討
企業側が作成したリスク評価案及び運用方法（実施計画案）についてチェック・レビューを行います。

計1.5ヶ月程度

「標準的な進め方」の詳細（１）

第1回　社内情報資産の洗い出し

		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	（事前配付）	【提供】5分でできる！自社診断チェックシート（Excel版）
	3	「リスク分析シート」による情報資産洗い出し	情報資産洗い出しの実施依頼	【提供】リスク分析シート
	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
	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	「リスク分析シート」の結果と課題認識についてのディスカッション	「リスク分析シート」結果を踏まえ、各情報資産に対するリスク評価の考え方について指南（重要度が高いもの等）	【成果物】リスク分析シート（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	シートにリストアップした各情報資産について、指導内容を踏まえ、次回までにリスク分析作業を実施	（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、企業側での情報資産洗い出し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　社内情報資産のリスク値の算定

		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	リストの見直しを行うとともに、支援先企業においてリストアップした情報資産についてリスク評価を実施	第2回の資料作成 ・リスク回避/低減策について整理 ・重点改善領域の見極め	【提供】リスク分析シート
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	各情報資産に対するリスク分析結果と、考えられるリスク回避・低減策について説明・ディスカッション	企業側のリスク回避・低減策に対しアドバイス・ディスカッション （*リスク評価の考え方について指南する。特に「C・I・A」の観点から、事業への影響度合いが高いものや法令・法律で義務付けられている項目など、重視すべきポイント等について伝える。企業側からの疑問や質問に答える。）	【成果物】リスク分析シート
	3	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**＞
- 「リスク分析シート」の結果を改めて事前に分析し、リスク大と評価されうる項目を指摘して、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。
- リスク回避・低減策の考え方は、各企業の状況によって異なります。ビジネスの内容や取り扱う情報の性質、社外関係先の状況も踏まえ、過度にハードルを上げることにならないよう、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　社内情報資産に対する情報セキュリティ対策等運用方法の検討

		企業	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	リスク分析結果を踏まえ、リスクへの対応方法を検討し、情報セキュリティ対策を検討する	適宜アドバイス	【提供】リスク分析シート（対策状況シート）
当日	1	特に高リスクであった情報資産に対するリスク回避・低減策を含む情報セキュリティ対策案について説明	対策状況シートをもとに、企業側のリスク回避・低減策に対しアドバイス・ディスカッション	【成果物】リスク分析シート
	2	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3回までの面談・ディスカッションを経て、リスク分析シートを完成させます。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、引き続き社内での情報セキュリティ対策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）
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

●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）
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（リスク分析シート）

- 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」の付録7「リスク分析シート」をもとに、社内での情報資産の洗い出し及びそれらに対するリスク分析を実施します。
  ⇒ https://www.ipa.go.jp/security/guide/sme/about.html
- リスク分析結果をもとに、今後の社内での情報セキュリティ対策を見直します。

情報資産の洗い出し
どのような情報資産があるか洗い出して重要度を判断する

リスク値の算定
優先的・重点的に対策が必要な情報資産を把握する

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

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

付録７「リスク分析シート」

成果物作成の留意点（情報資産管理台帳の作成）

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

➢ **情報資産**

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

➢ **情報資産管理台帳**

情報資産管理台帳は洗い出した情報資産を「見える化」するための方法

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

情報資産に関連する業務や部署名を記入

情報資産の内容を簡潔に記入

必要に応じて説明等を記入

情報資産を利用してよい部署等を記入

情報資産の管理責任がある部署等を記入

情報資産の媒体や保存場所を記入

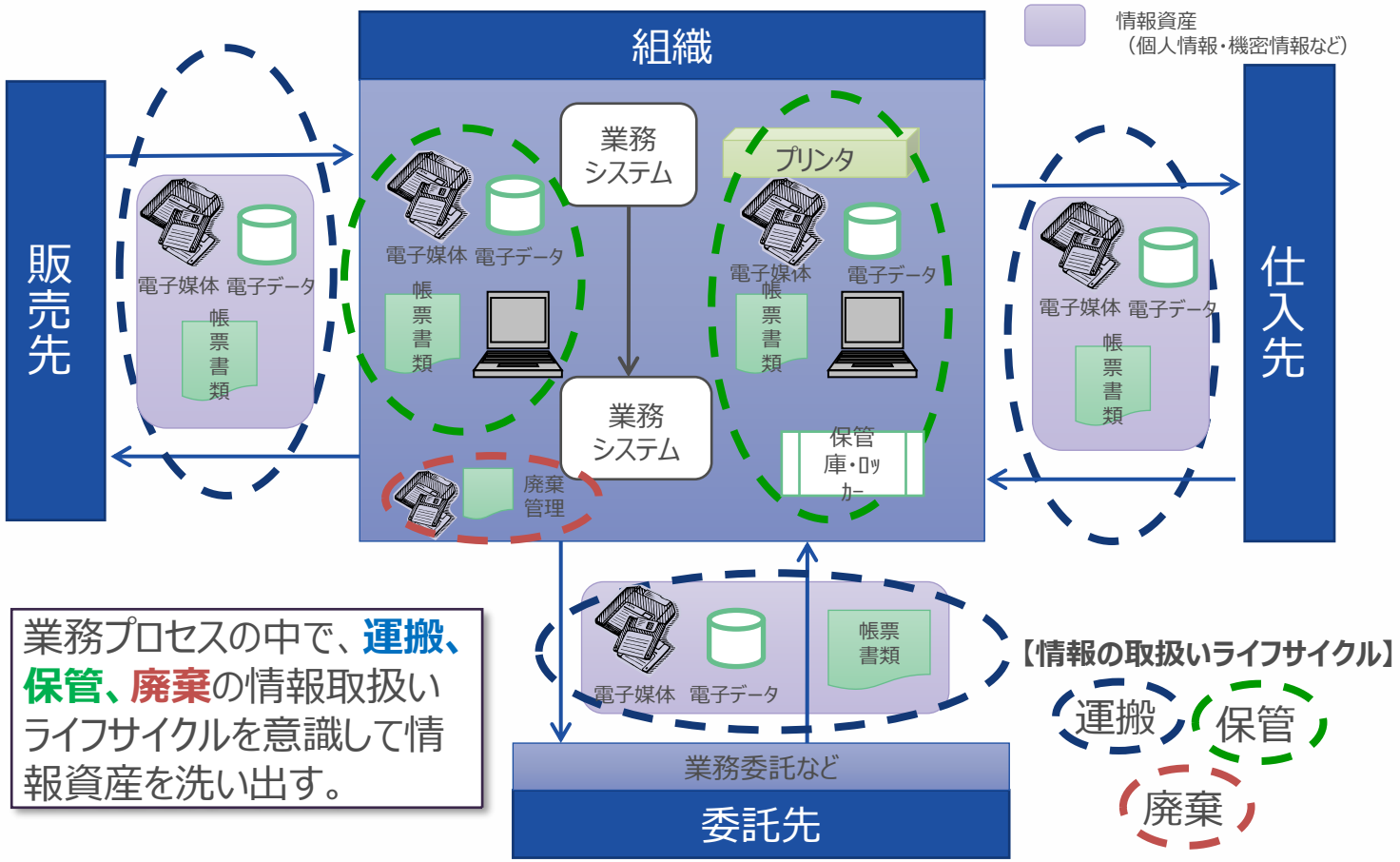
個人情報の有無を記入

情報資産の保存期間を記入

情報資産の登録日を記入

成果物作成の留意点（情報資産の洗い出し）

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



成果物作成の留意点（機密性・完全性・可用性の評価）

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

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

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

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

【表12】情報資産の機密性・完全性・可用性に基づく重要度の定義

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

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

成果物作成の留意点（重要度の算定）

- 重要度は、機密性、完全性、可用性いずれかの最大値で判断する

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

- 重要度の判断例

●『独自技術に基づいた設計図』(書類)

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

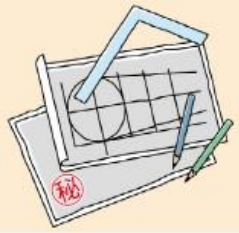
完全性：改ざんや無断の変更があると、製造に支障がある…… 評価＝2

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

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
3	2	1	3

機密性の3が最大値なので重要度は3



●『自社のホームページ』(電子データ)

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

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

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

情報資産管理台帳　重要度欄

評価値			重要度
機密性	完全性	可用性	
1	3	3	3

完全性と可用性の3が最大値なので重要度は3

成果物作成の留意点（リスク値の算定）

- 対策の優先度を決めるため、情報資産ごとにリスク値(リスクの大きさ)を算定する
- リスク値は「重要度」「脅威」「脆弱性」の数値から算定する。重要度は先に算定しているので、ここでは脅威と脆弱性から被害発生可能性を算定する

リスク値 ＝ 重要度 × 被害発生可能性

機密性、完全性、可用性により算定

脅威・脆弱性から算定

成果物作成の留意点（「脅威」の識別）

- **「脅威の状況」シート**で、媒体・保存先ごとの脅威がどのくらいの頻度で発生する可能性があるかを「対策を講じない場合の脅威の発生頻度」欄に表示されるリストから１～３のいずれかを選択する

社内サーバー	情報窃取目的の社内サーバーへのサイバー攻撃	3：通常の状況で脅威が発生する（いつ発生してもおかしくない）
	情報窃取目的の社内サーバーでの内部不正	2：特定の状況で脅威が発生する（年に数回程度）
	社内サーバーの故障による業務に必要な情報の喪失	1：通常の状況で脅威が発生することはない

媒体・保存先　個別の脅威　脅威の発生頻度（1～3から選択）

- 媒体・保存先
  書類、可搬電子媒体、事務所PC、モバイル機器、社内サーバー、社外サーバー

成果物作成の留意点（「脆弱性」の認識）

- **「対策状況チェック」シート**で、55項目の「情報セキュリティ診断項目」ごとに自社における実施状況を「実施状況」欄に表示されるリストから１～４のいずれかを選択する

物理的セキュリティ対策	業務を行う場所に、第三者が許可なく立ち通りができないようにするための対策（物理的に区切る、見知らぬ人には声をかける、等）が講じられていますか？	2：一部実施している
	最終退出者は事務所を施錠し退出の記録（日時・退出者）を残すなどのように、事務所の施錠をしていますか？	1：実施している
	高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？	3：実施していない／わからない
	秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？	4：自社に該当しない

情報セキュリティ診断項目(チェック項目)

実施状況(1～3+4:自社に該当しない)

成果物作成の留意点（リスク値の算定）

- **「脅威」の識別** と **「脆弱性」の認識** が完了すると、「現状から想定されるリスク」欄に、情報資産ごとに「脅威の発生頻度」「脆弱性」「被害発生可能性」「リスク値」が表示される

現状の状況から想定されるリスク（入力不要・自動表示）					
脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性※「対策状況チェック」シートに入力すると表示	被害発生可能性		リスク値	
3：通常の状況で脅威が発生する（いつ発生してもおかしくない）	2：部分的に対策を実施している	2	可能性：中	4	リスク大
2：特定の状況で脅威が発生する（年に数回程度）	2：部分的に対策を実施している	1	可能性：低	2	リスク中

情報資産ごとの脅威の発生頻度

情報資産ごとの脆弱性（対策状況）

情報資産ごとの被害発生可能性（高・中・低の3段階）

情報資産ごとのリスク値（大・中・小の3段階）

成果物作成の留意点（成果物／診断結果シート）

情報セキュリティ対策の種類（付録5 情報セキュリティ関連規程名称）		情報セキュリティ関連規程策定の必要性	対策状況チェックの診断結果（対策の実施率）	対策検討・実施の要否
1	組織的対策	◎	50.0%	不足する対策を検討・実施してください
2	人的対策	◎	50.0%	不足する対策を検討・実施してください
3	情報資産管理	○	50.0%	不足する対策を検討・実施してください
4	アクセス制御及び認証	ー	50.0%	（該当する情報資産なし）
5	物理的対策	◎	50.0%	不足する対策を検討・実施してください
6	IT機器利用	ー	50.0%	（該当する情報資産なし）
7	IT基盤運用管理	ー	50.0%	（該当する情報資産なし）
8	システム開発及び保守	△	50.0%	不足する対策を検討・実施してください
9	委託管理	△	50.0%	不足する対策を検討・実施してください
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	◎	50.0%	不足する対策を検討・実施してください

成果物作成の留意点（リスク値算定の全体イメージ）

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

× 掛け算

算定のしかたは**右図**参照

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

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

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

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

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

脅威 ＼ 脆弱性	3	2	1
3	3	2	1
2	2	1	1
1	1	1	1

計算式　脅威÷（4－脆弱性）
（小数第1位を切り上げ）

成果物作成の留意点（脅威例に応じたリスクのレベル（例））

脅威の例	重要度(a)	脅威	脆弱性	被害発生可能性(b)	重要度(a)×被害発生可能性(b)	リスク値
1,000人を超える顧客の個人データを保存しているノートパソコンの盗難 （脆弱性）データを暗号化していない	3	2	**3**	**2**	**6**	**リスク大**
（対策改善）ハードディスクやデータを暗号化する	3	2	**1**	**1**	**3**	**リスク小**
クレジットカード番号を含む顧客の個人データを保持したECサイトへ不正アクセスされることによる情報漏えい （脆弱性）ウェブサイトの技術的脆弱性を認識せず対策が不十分	3	3	**3**	**3**	**9**	**リスク大**
（対策改善）ECサイトの設計･開発段階から脆弱性を作り込まないように技術的セキュリティを実装する	3	3	**1**	**1**	**3**	**リスク小**
メールの添付ファイルを開いてしまいランサムウェアに感染し､サーバーのデータとオンラインバックアップが暗号化される （脆弱性）オンラインバックアップしか取得していない	3	3	**2**	**2**	**6**	**リスク大**
（対策改善）定期的にオフラインバックアップを取得する	3	3	**1**	**1**	**3**	**リスク小**

成果物作成の留意点（リスク対応方法の検討）

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

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

成果物作成の留意点（参考：情報セキュリティ関連規程（サンプル））

対策検討にあたっては中小企業の情報セキュリティ対策ガイドライン付録「情報セキュリティ関連規程(サンプル)」をベースラインとして組み合わせて活用することができる

	名称	概要
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。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	テレワークのセキュリティ対策についてルールを定めます。

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://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


IPA