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④｜セキュリティインシデント対応

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。

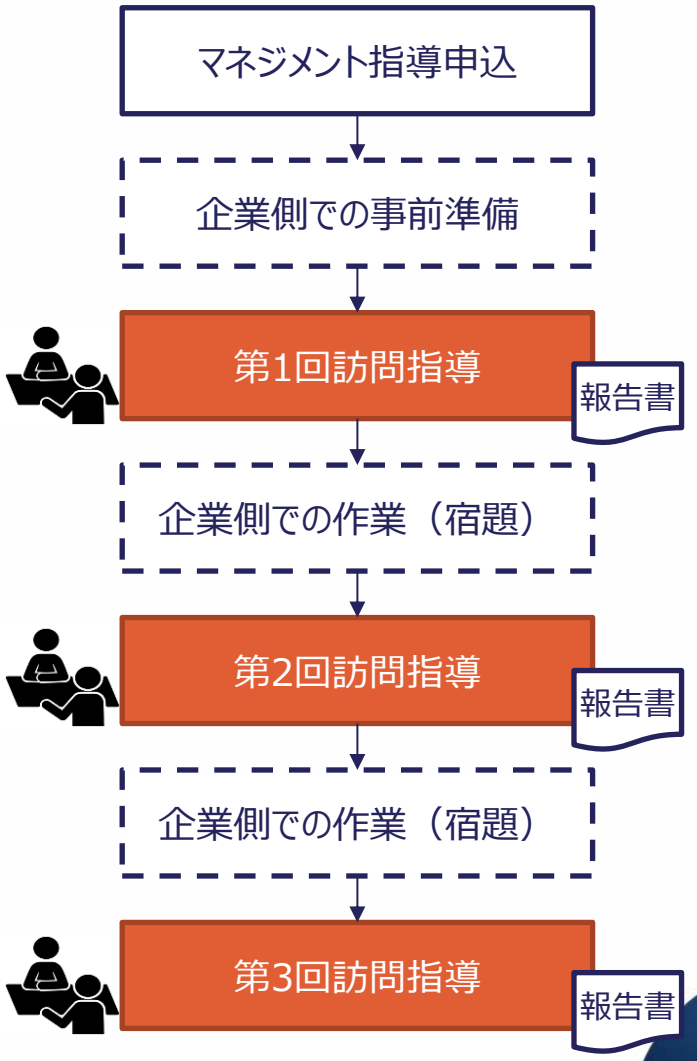
マネジメント指導（テーマ別）では、そのような中小企業に対して、**①情報セキュリティ規程の整備**、**②情報資産の洗い出しとリスク分析**、**③クラウドサービスの安全利用**、**④セキュリティインシデント対応**、そして**⑤従業員向けのセキュリティ教育** の5つの主要なテーマを指導するための具体的な方法と手順を提供しています。

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



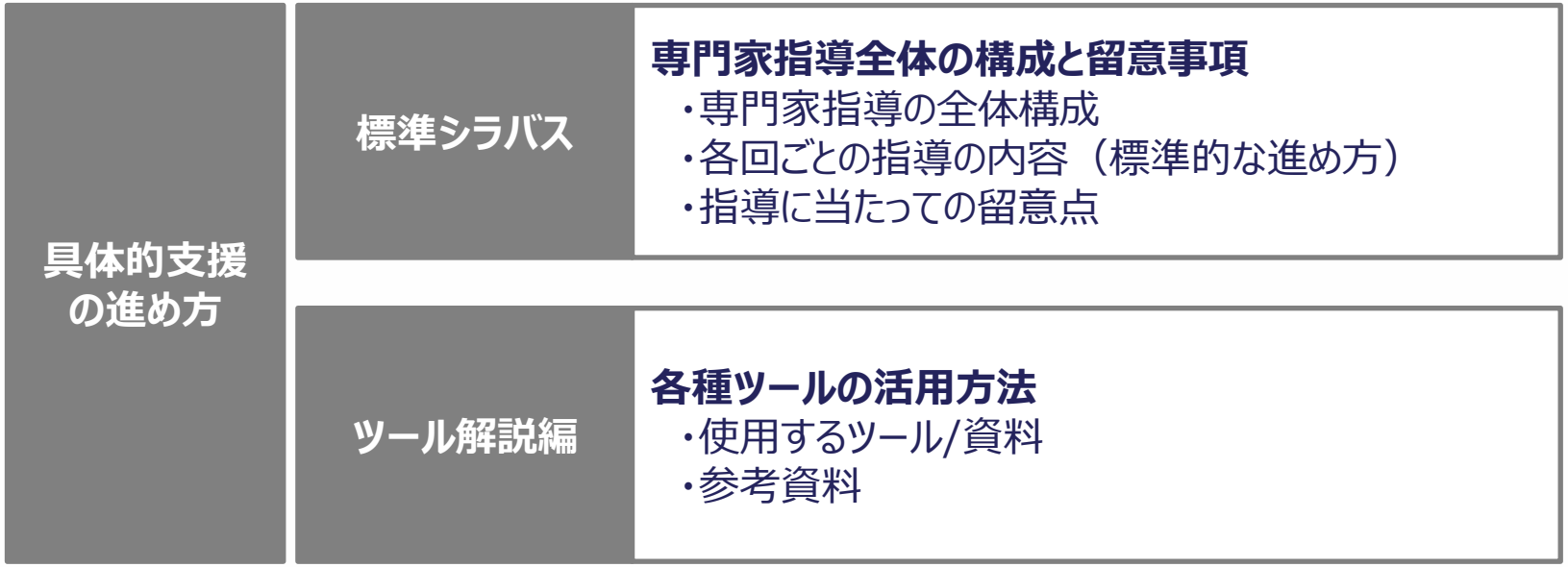
マネジメント指導のテーマと狙い

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④｜セキュリティインシデント対応

【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8「中小企業のためのセキュリティインシデント対応の手引き」を基に、支援先企業におけるインシデント対応手順書を作成します。
- 作成した手順書に基づき、インシデント対応机上演習を実施し、次回以降に向けたレビューを行います。

マネジメント指導業務の達成目標と成果物

中小企業等の対策実施レベル

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

注：成果物

取組みスタート

達成目標1

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

達成目標2

- インシデント対応手順書（規程）の作成

達成目標3

インシデント対応机上演習の実施とレビュー

継続実施

「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
*現在のインシデント対応プロセスやポリシー、規程の確認

第１回

現状のセキュリティインシデント対応プロセスの評価と重要項目の説明

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、企業のセキュリティインシデント対応体制を評価し、現状を把握します。既存のインシデント対応プロセスやポリシー、規程等の見直し、改善点等を洗い出します。
また、簡易なディスカッション演習を実施し、IT-BCPの考え方を説明します。
作成するインシデント対応手順書の対象テーマ（「ウイルス感染・ランサムウェア感染」「情報漏洩」「システム停止」のいずれか（あるいは複数））を検討します。

1～2週間

事前準備＃２

*セキュリティインシデント対応手順書案の検討・策定
*専門家からの指導に基づき、インシデント対応手順書のドラフト内容をレビュー

第２回

セキュリティインシデント対応手順書の検討と評価

支援先企業で検討したインシデント対応手順を確認し、手順書案として仕上げます。
また、具体的な演習計画（シナリオ含む）の検討を進めます。

1～2週間

事前準備＃３

*インシデント対応演習計画を策定（シナリオ含む）
*インシデント対応演習実施に向けて、社内調整（演習参加メンバーの選定、スケジュール調整等）

第3回

インシデント対応机上演習の実施とレビュー

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

計1.5ヶ月程度

「標準的な進め方」の詳細（１）

第1回　現状のセキュリティインシデント対応プロセスの評価と重要項目の説明

		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	インシデント対応プロセスやポリシーの確認と事前評価を実施	インシデント対応プロセスやポリシーの確認と事前評価の実施依頼	【提供】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
	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	インシデント対応プロセスやポリシー等の説明	既存のインシデント対応プロセスやポリシーの見直し、改善点等を洗い出す。 IT-BCPの考え方を説明し、インシデント発生時に事業や自分たちの顧客に何が起きるか（ビジネスインパクト）を考えさせる（担当者に対し、簡易なディスカッション演習を実施）。	【提供】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 【提供】ミニ演習シナリオ 【提供】情報セキュリティ関連規程サンプル抜粋（インシデント対応部分）※必要に応じ
	4	依頼事項についての確認と了解	「ウイルス感染・ランサムウェア感染」「情報漏洩」「システム停止」のいずれか（あるいは複数）について、インシデント対応手順案の作成を指示。	（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、企業側での現時点でのインシデント対応体制や規程整備状況等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　セキュリティインシデント対応手順書の検討と評価

		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	セキュリティインシデント対応手順書案の検討・策定	第2回の資料作成 ・重点改善領域の見極め	【提供】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 【提供】情報セキュリティ関連規程サンプル抜粋（インシデント対応部分）
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	インシデント対応手順書案の説明 インシデント対応机上演習シナリオについて議論	企業が策定したインシデント対応書案について、実際のシステム運用面から具体的に手順を確認し、手順書案として仕上げる。 インシデントシナリオを用いた演習計画案の策定に向けた指南。 次回（第3回）面談時までの企業側宿題として、具体的な演習計画の確認と修正指示。	【成果物】インシデント対応手順書案
	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**＞
- 次回会合時に実施を目指すインシデント対応机上演習のシナリオや進め方についてディスカッションを行います。
- ビジネスで取り扱う情報やサプライチェーンの状況、またそれに伴い必要となる社内でのインシデント対応体制の考え方は、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　インシデント対応机上演習の実施とレビュー

		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	インシデント対応演習の準備（社内調整、演習参加メンバーの選定、スケジュール調整等）	演習シナリオのブラッシュアップ	【提供】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
当日	1	策定したインシデント対応手順書に従い、机上演習を実施	シナリオをベースとしてとして、作成したインシデント対応手順書との読み合わせを実施（ウォークスルー型） 演習結果のレビュー 今後の演習計画についてアドバイス	【成果物】インシデント対応手順書案、机上演習シナリオ、演習計画
	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、具体的なインシデント対応机上演習を実施します。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）
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）

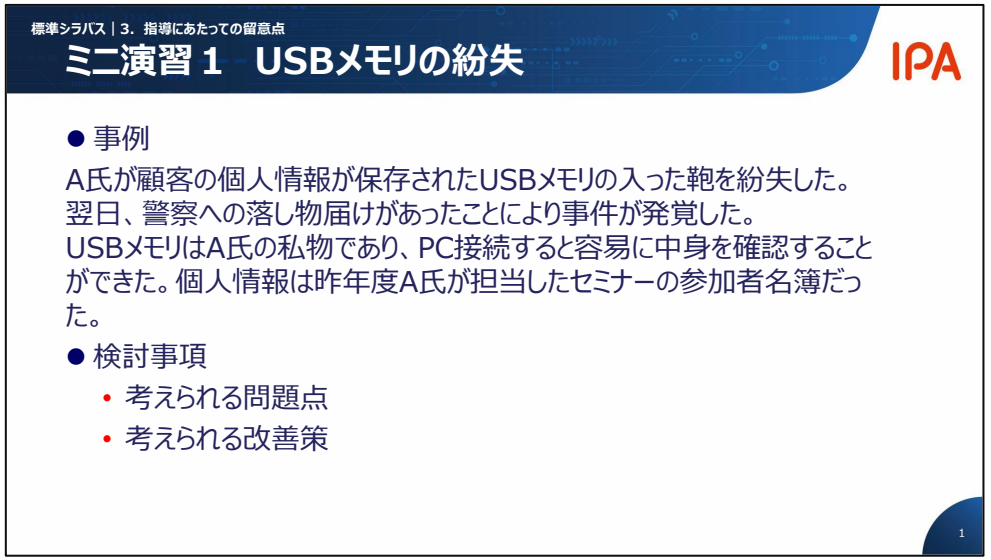
項目No.		診断内容	掘り下げるチェックポイント（例）
基本的対策	1	パソコンやスマホなど、情報機器のOSやソフトウェアは常に最新の状態にしていますか？	①. 状況を管理する担当者は決まっているか ②. 業務外のソフトウェアが勝手に導入されてないか ③. 従業員に、どのように徹底できているか
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	①. すべてのパソコンの更新レベルが把握できているか ②.「社長、役員は別」などの例外的な取り扱いはないか ③. 管理者／使用者がはっきりしないパソコンは無いか
	3	パスワードは破られにくい「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

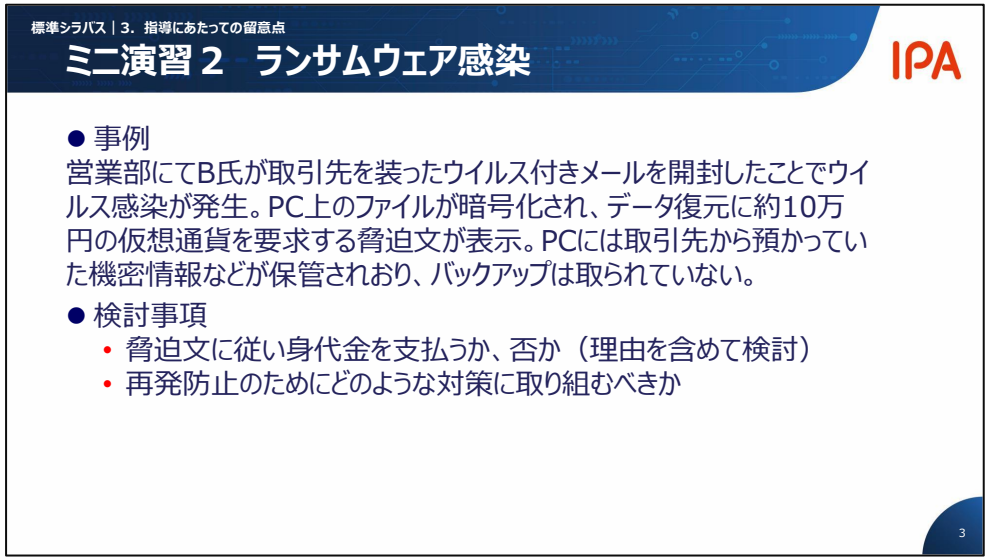
※1　コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれます。
※2　重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や、従業員の個人情報など管理責任を伴う情報のことです。

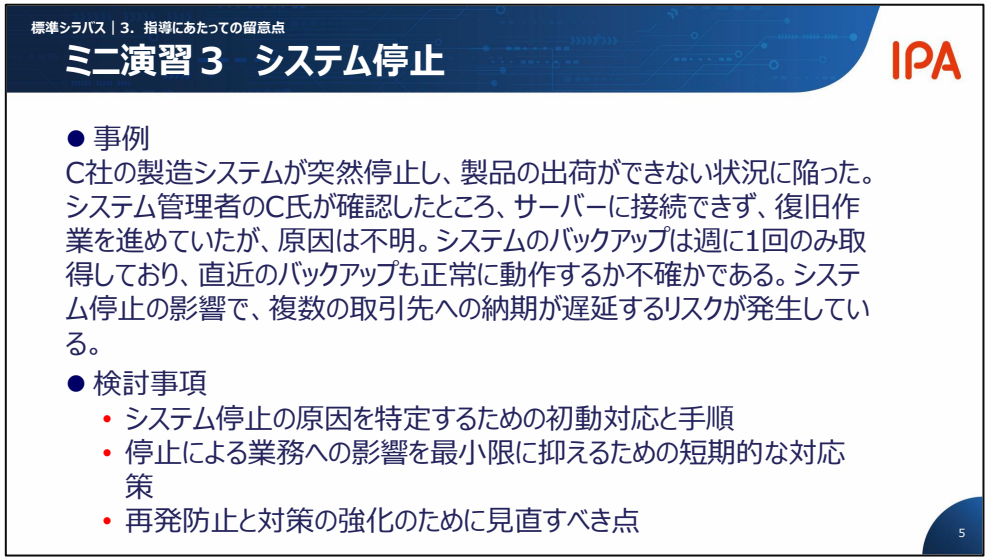
チェックの判断根拠を十分に掘り下げることで、身の丈に合った有効な対策に絞り込みます

使用するツール/資料の内容（ミニ演習シナリオ）

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

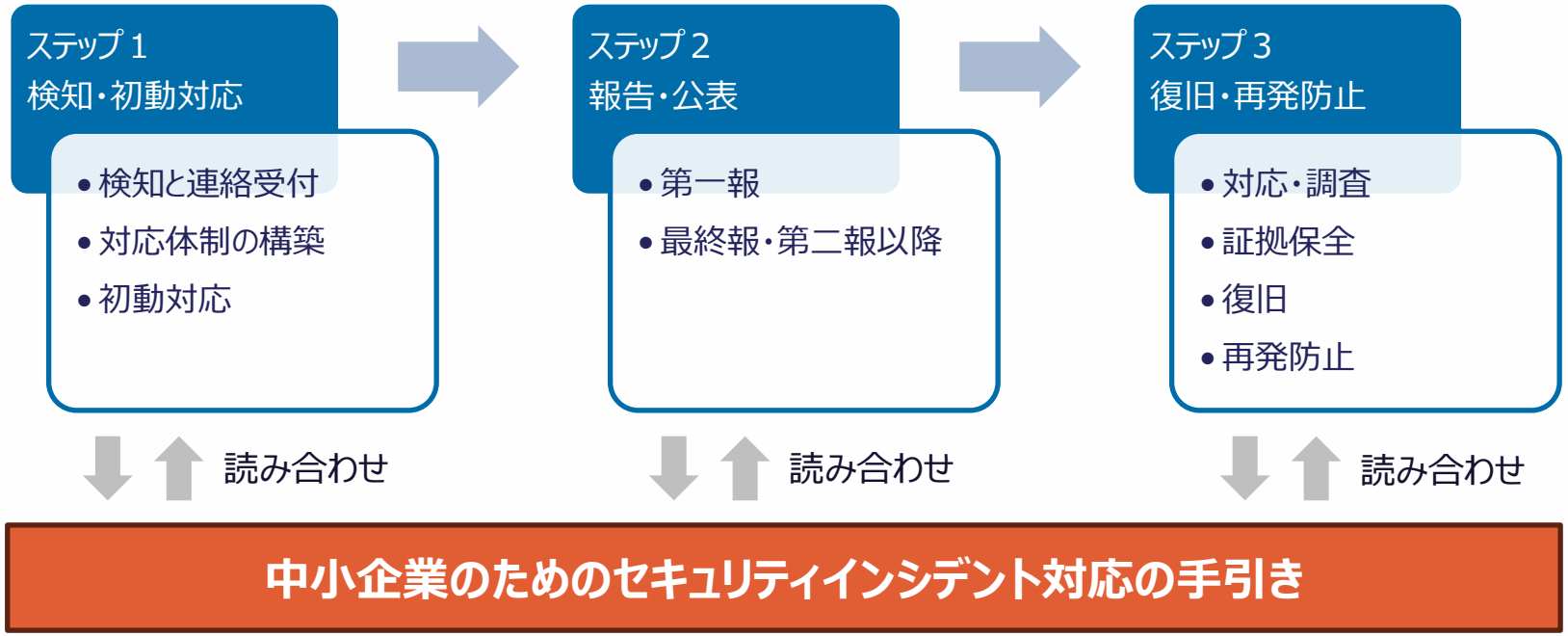






使用するツール/資料の内容（インシデント対応の手引き）

- 「中小企業の情報セキュリティ対策ガイドライン 第3.1版」の付録8「中小企業のためのセキュリティインシデント対応の手引き」をベースに、支援先企業における具体的なインシデント対応手順書を取りまとめます。
- 取りまとめた手順書をベースに、実際に社内にてインシデント対応机上演習を実施します。
- 演習は、あらかじめ用意したシナリオを用い、「検知・初動対応」「報告・公表」「復旧・再発防止」の３つの段階に分けてポイントが確認できるよう工夫し実施します。実際のシステムを使ったフルスケールの演習ではなく、手順書とシナリオを読み合わせるウォークスルー型の演習を想定しています。

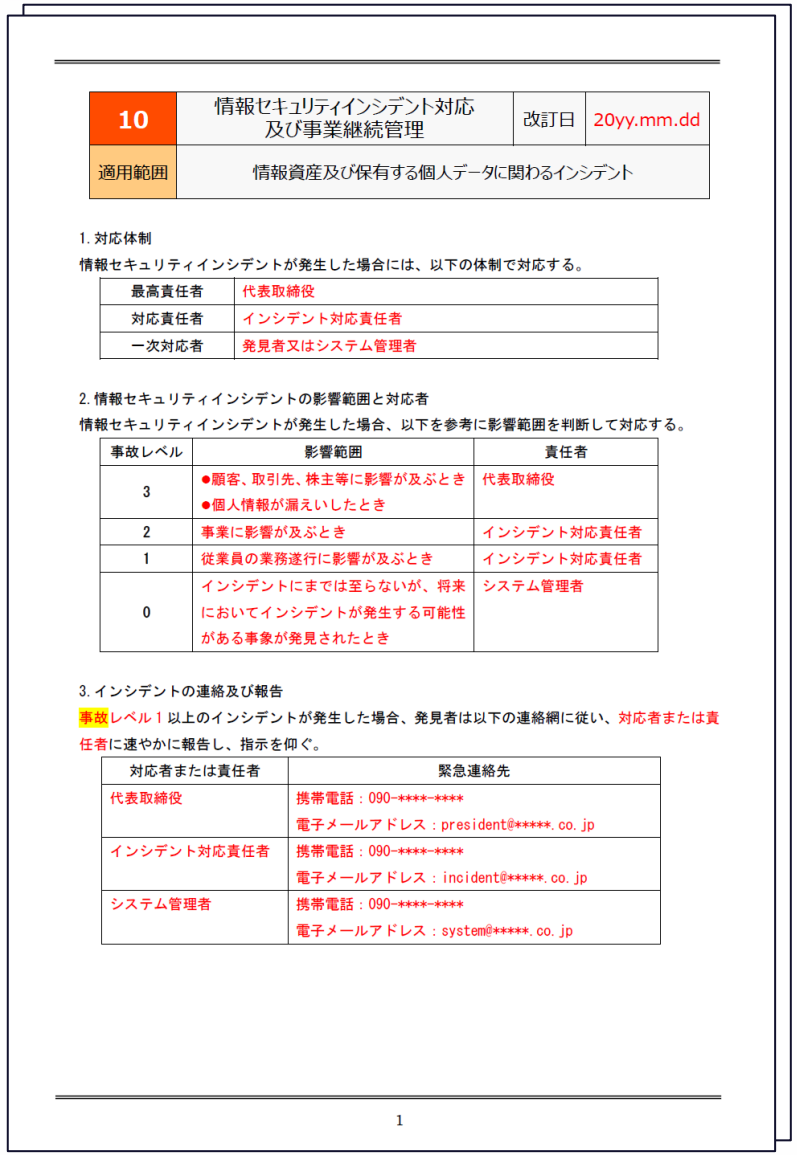


使用するツール/資料の内容（インシデント対応規程）

支援先企業においてインシデント対応に関する基本的な規程等が用意されていない場合、まず「中小企業の情報セキュリティ対策ガイドライン 第3.1版」の付録5「情報セキュリティ関連規程（サンプル）」のうち、「10. 情報セキュリティインシデント対応及び事業継続管理」をベースに、支援先企業における基本的なインシデント対応手順を取りまとめることも有効です。

「10. 情報セキュリティインシデント対応及び事業継続管理」記載項目

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



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

1. 対応体制

情報セキュリティインシデントが発生した場合には、以下の体制で対応する。

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

2. 情報セキュリティインシデントの影響範囲と対応者

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

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

3. インシデントの連絡及び報告

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

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

1

成果物作成の留意点（インシデント対応手順書記載項目例）

「中小企業の情報セキュリティ対策ガイドライン 第3.1版」の付録8「中小企業のためのセキュリティインシデント対応の手引き」をベースに、支援先企業における具体的なインシデント対応手順書を取りまとめます。

【参考】ランサムウェア感染時の対応手順書記載項目例

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

使用するツール/資料の内容（インシデント対応机上演習シナリオ）

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

インシデント対応机上演習シナリオ検討シート

社名：　（　　）

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

企業と協議の上
シナリオを検討

使用するツール/資料の内容（机上演習実施後レビュー）

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

※項目は適宜追加・変更可、必ずしも厳格な運用は必要ない。

インシデント対応机上演習実施後レビュー項目

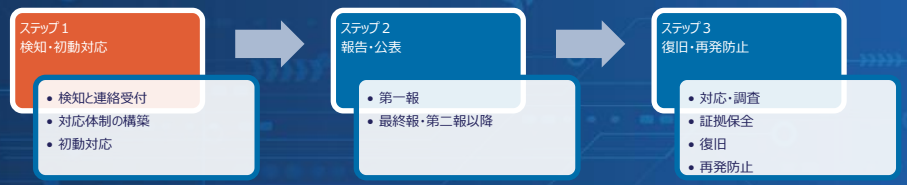
社名：（　　）

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

セキュリティインシデント対応の必要性・目的

- セキュリティインシデントとは、セキュリティの事故・出来事のことです。単に「インシデント」とも呼ばれます。例えば、情報の漏えいや改ざん、破壊・消失、情報システムの機能停止またはこれらにつながる可能性のある事象等がインシデントに該当します。
- インシデント発生による直接的な被害として、攻撃者による不正送金や金銭要求、対応人件費、原因調査や復旧のための外部委託費、復旧までの代替品費、取引先・顧客等への謝罪対応費、法的対応のための弁護士費用等の金銭的被害があります。間接的な被害として、関係者への被害波及、会社の信用低下、事業停止による機会損失等があります。
- インシデント対応の目的は、インシデント発生によるこれら被害とその影響範囲を最小限に抑え、迅速に復旧し、再発を防止することで、 企業の事業継続を確保することです。

ステップ 1 検知・初動対応



● 検知と連絡受付

- インシデントが疑われる兆候や実際の発生を発見した場合は、情報セキュリティ責任者に報告します。
- 外部から通報を受け付けた場合は、通報者の連絡先等を控えます。

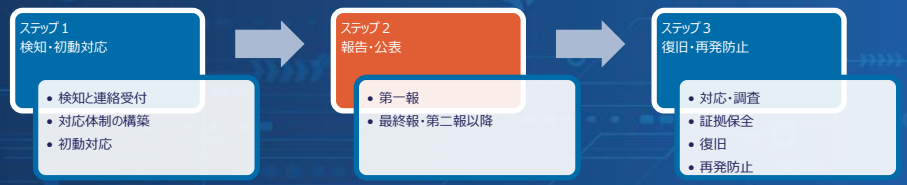
● 対応体制の構築

- 情報セキュリティ責任者は、対応すべきインシデントであると判断したら、速やかに経営者に報告します。
- 経営者は、インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者を定めて、役割分担を明確にします。

● 初動対応

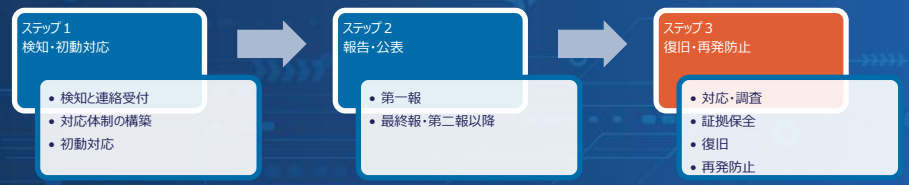
- 初動対応として、対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を行います。ただし、対象機器の電源を切る等、不用意な操作でシステム上に残された記録を消さないようにします。

ステップ２ 報告・公表



- **第一報**
  - すべての関係者への通知が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトや、メディアを通じて公表します。公表によって被害の拡大を招かないよう、時期、内容、対象などを考慮します。
  - 顧客や消費者に関係する場合は受付専用の問い合わせ窓口を開設し、被害が発生・拡大した場合にはその動向を速やかに把握し対応します。
- **第二報以降・最終報**
  - 被害者や、影響を及ぼした取引先や顧客に対して、インシデントの対応状況や再発防止策等に関して報告します。また、被害者に対する損害の補償等を、必要に応じて行います。
  - 個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、犯罪性がある場合は警察、ウイルス感染や不正アクセスの場合はIPAへ届け出ます。

ステップ３ 復旧・再発防止



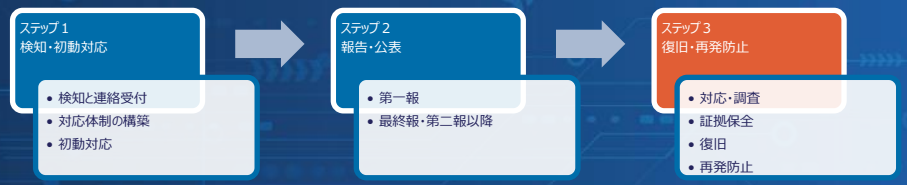
● 調査・対応

- 適切な対応判断を行うために、5W1H（いつ、どこで、誰が、誰を、何を、なぜ、どうしたのか）の観点で状況を調査し情報を整理します。
- 対応方針を基に、原因を調査し、修正プログラムの適用、設定変更、機器の入替データの復元等、必要な修復を行います。
- 自社で対応が難しい場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的機関の相談窓口等に支援、助言を求めます。
- 対応中は、状況や事業への影響等について経営者に適時報告します。

● 証拠保全

- 訴訟対応等を見越して事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバーやネットワーク機器のログ等の調査）を行います。

ステップ３ 復旧・再発防止



- **復旧**
  - 正しく修復できたことが確認できたら、停止したシステムやサービスを復旧します。
  - 復旧後は、経営者に対応結果を報告します。
- **再発防止**
  - インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善等、抜本的な再発防止策を検討し、実施します。

事象ごとの対応のポイント

ウイルス感染・ランサムウェア感染の場合

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

情報漏えいの場合

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

システム停止の場合

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

インシデント対応時に整理しておくべき事項

インシデントの分類	情報漏えい 、ウィルス感染、システム停止など
事業者	事業者の名称 ※自社の受託案件に関連したインシデントの場合は委託元含む関係事業者の名称
担当者・責任者	本件に関する責任者および担当者の所属、氏名
発覚日時	インシデントを認知した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定される原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要・詳細
システム構成・運用状況	システムの物理的所在地やOS、アプリケーションとバージョン構成 ※可能であれば簡単な構成図等も併記 システムの運用状況やセキュリティツール・サービスの利用状況等

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

インシデント発生時の相談窓口

- **企業・組織のためのインシデントの相談・届出・情報提供窓口**

  独立行政法人情報処理推進機構(IPA)
  企業組織向けサイバーセキュリティ相談窓口
  https://www.ipa.go.jp/security/support/soudan.html

- **サイバー犯罪に関する相談**

  都道府県警察本部のサイバー犯罪相談窓口
  https://www.npa.go.jp/bureau/cyber/soudan.html

- **インシデント対応の相談**

  一般社団法人JPCERTコーディネーションセンター(JPCERT/CC)
  インシデント対応依頼
  https://www.jpcert.or.jp/form/
  特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)
  サイバーインシデント緊急対応企業一覧
  https://www.jnsa.org/emergency_response/

インシデント発生時の報告先

- **ウイルス・不正アクセスに関する届出**

  独立行政法人情報処理推進機構(IPA)

  コンピュータウイルス届出窓口、コンピュータ不正アクセス届出窓口

  https://www.ipa.go.jp/security/todokede/crack-virus/about.html

- **個人情報・特定個人情報（マイナンバー）漏えいの報告**

  個人情報保護委員会

  個人情報の漏えい等

  https://www.ppc.go.jp/personalinfo/legal/leakAction/

  特定個人情報の漏えい等

  https://www.ppc.go.jp/legal/rouei/

インシデント対応に役立つ情報

- **サイバー攻撃被害に係る情報の共有・公表ガイダンス**

  サイバー攻撃を受けた被害組織がサイバーセキュリティ関係組織とサイバー攻撃被害に係る情報を共有する際の実務上の参考となるガイダンスです。※

  https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf

- **インシデントハンドリングマニュアル（JPCERT/CC）**

  インシデント発生時から解決までの一連の処理について、代表的なインシデント種別を例にあげ、対応の考え方と、手順の概要を簡潔に説明した資料です。

  https://www.jpcert.or.jp/csirt_material/operation_phase.html

- **ランサムウェア対策特設ページ（IPA）**

  ランサムウェア対策に必要となる情報を集約し、ランサムウェアの感染防止や被害低減のために役立つ情報をタイムリーに公開しています。

  https://www.ipa.go.jp/security/anshin/measures/ransom_tokusetsu.html

※なぜ情報共有が必要なのか？
各組織においては様々なセキュリティ対策製品／サービスを通じて、不正通信先や新たに登場したマルウェアの検知への取組みが日々行われていますが、製品／サービスの検知をすり抜けようとする新たな攻撃手法や特定の業種／分野だけを限定的に狙う攻撃が登場すると、製品／サービスによっては、対応が間に合わない可能性があるため、このタイムラグを埋めるために、情報共有活動による情報入手が必要になります。

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