中小企業のための
セキュリティ人材確保・
育成の実践ガイドブック

企業の情報セキュリティ対策を支える
セキュリティ人材を会社全体で積極的
に確保・育成しましょう。

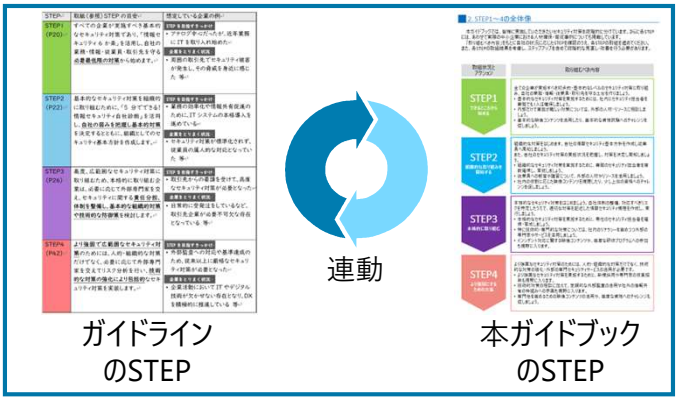
1. 本ガイドブックの目的

中小企業がセキュリティ対策を進めるには、自社の業務やシステムを理解し、対策をリードできる人材を組織として確保し、育成することが重要です。

本ガイドブックは、これからセキュリティ対策を始める中小企業や、現在の対策を強化したい中小企業の経営者やセキュリティ担当者を対象に、セキュリティ人材の確保・育成を実践できるようになることを目的として、中小企業の情報セキュリティ対策ガイドライン（以下「ガイドライン」）を人材面で補完するものとして取りまとめたガイドブックとなります。

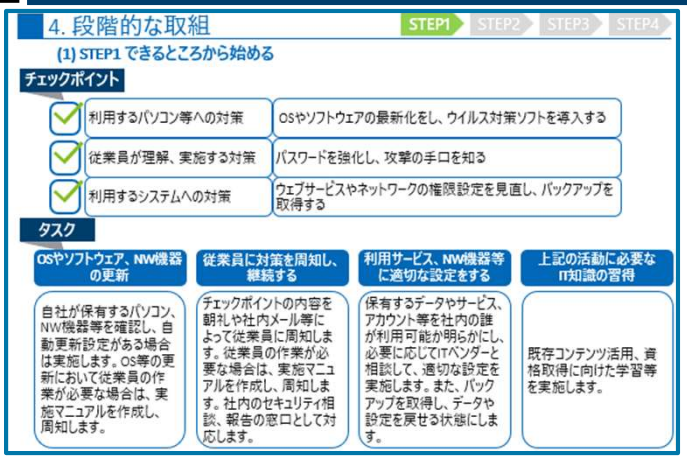
＜本ガイドブックの構成＞

1 実施していただきたい取り組み内容を段階的に提示



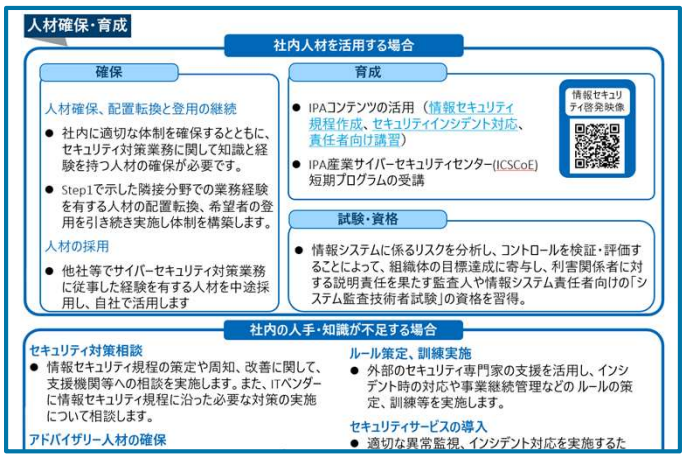
ガイドラインの各STEPに合わせて、セキュリティ人材の育成をどう進めるかを記載しています。

2 STEPごとに社内セキュリティ担当者の業務を提示



STEPごとにガイドラインの取り組み内容をコンパクトにまとめ、セキュリティ担当者が行うチェックポイントや主な業務の概要を記載しています。

3 対策を実行するための人材の確保・育成の方策を紹介



業務の概要に対応したセキュリティ人材について、以下の場合に分けて確保・育成の方策を記載しています。

- 社内で育成する場合
- 社内の人手・知識が不足し外部の専門家を活用する場合

本ガイドブックを活用して、セキュリティ人材の確保・育成を実践することで、
適切なセキュリティ体制の構築、対策の実施に役立てていただければ幸いです。

2. STEP1～4の全体像

本ガイドブックでは、セキュリティ人材の確保・育成を段階ごと（STEP）に分けて説明しています。各STEPには、中小企業へのヒアリング調査を基にした具体的な取り組み事例も載せています。

まず「取り組むべき内容」を確認し、自社の状況に合ったSTEPを選んで進めてください。取り組みの結果を踏まえ、必要に応じて段階的に見直しや改善を行い、次のSTEPへ進んでください。

STEP	取り組むべき内容
STEP1 できるところから始める	全ての中小企業が実施すべき基本的なセキュリティ対策に取り組みましょう。自社の業務・情報・従業員、取引先を守る土台を作りましょう。 • 基本的なセキュリティ対策を実施するためには、社内にセキュリティ担当者を兼務でも1人は確保しましょう • 内部だけで実施が難しい対策については、外部の専門家に相談しましょう • セキュリティ担当者に対して、映像教材を活用した学習や、入門的な資格試験の受験を推奨しましょう
STEP2 組織的な取り組みを開始する	組織的なセキュリティ対策をはじめましょう。自社の情報セキュリティ基本方針を作成し従業員へ周知しましょう。また、自社のセキュリティ対策の実施状況を把握し、対策を決定し周知しましょう。 • 組織的なセキュリティ対策を実施するために、兼務のセキュリティ担当者を役割に応じて複数名を確保し、育成しましょう • 従業員への教育や講習について、外部の専門家を活用しましょう • セキュリティ担当者に対して、社内の所属や役職に応じた映像教材の視聴や、上位の資格試験の受験を推奨しましょう
STEP3 本格的に取り組む	本格的なセキュリティ対策をはじめましょう。体制を整備し、対応すべきリスクを特定したうえで、対策を検討・決定し、情報セキュリティ規程にまとめ、実行しましょう。 • 本格的なセキュリティ対策を実施するために、専任のセキュリティ担当者を確保・育成しましょう • 特に技術的・専門的な対策については、社内のリテラシーを高めつつ外部の専門家やサービスを活用しましょう • セキュリティ担当者に対して、インシデント対応に関する映像教材の視聴や、高度な研修プログラムへの参加を推奨しましょう
STEP4 より強固にするための方策	より強固なセキュリティ対策のためには、人的・組織的な対策だけでなく、技術的な対策の強化や外部の専門セキュリティサービスを活用しましょう。 • より強固なセキュリティ対策を実施するために、新卒採用や専門家を招聘しましょう • 技術的対策の相談に加えて、外部監査の活用や社外の情報共有の枠組みへも参画しましょう。 • セキュリティ担当者に対して、対策をより強固にするための映像教材の活用や、高度な資格試験の受験を推奨しましょう

3. 経営者の皆様へ

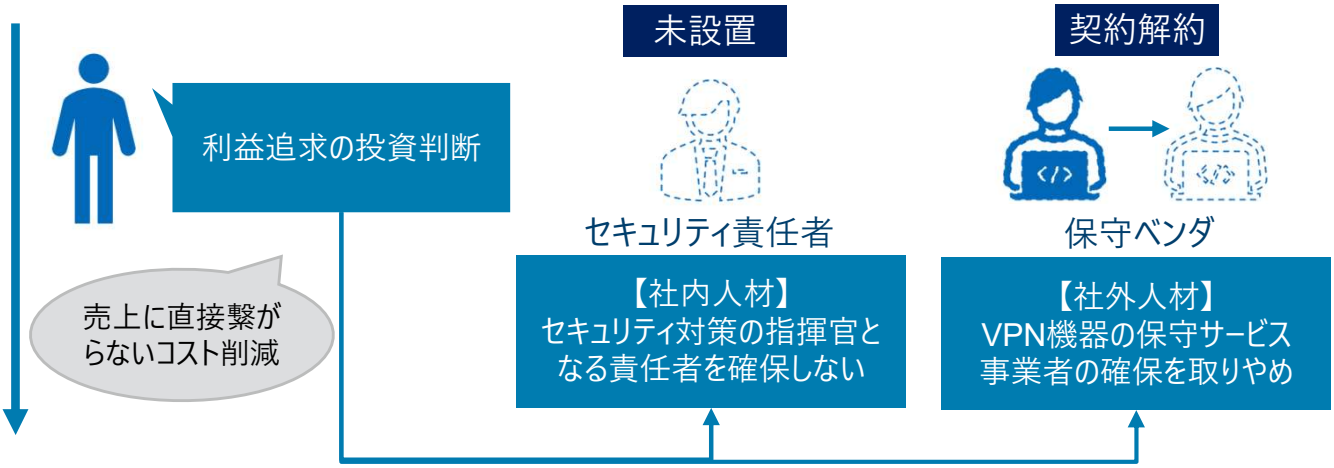
セキュリティ対策を怠ると、サイバー攻撃を受けて事業が止まったり、情報が漏れて取引先や顧客からの信頼を失ったりします。場合によっては、自社だけでなくサプライチェーン全体に影響が広がることもあります。

いざというときに対応する責任者や担当者がいないと、自社の業務を踏まえた対策が進められず、攻撃を受けたときに適切に対処できません。その結果、本来なら防げた被害が発生したり、被害が大きくなったりします。

経営者はセキュリティ対策の重要性を理解し、責任者や担当者を確保することが大切です。誰が、何を、いつまでに行うかを明確にして体制と役割を決め、いつでも対応できる人材を確保しておきましょう。

事例 **セキュリティ責任者不在の結果、ランサムウェア被害が拡大（被害額は計1億2,400万円）**

①セキュリティ対策にかかる人材コストを削減



②セキュリティ責任者がいなかったことで、ランサムウェア感染に対処ができなかった

③人材がおらず、体制やルールもなかったので、被害が拡大し、自社の信用失墜につながった

4. 段階的な取組

STEP1 STEP2 STEP3 STEP4

(1) できるところから始める

チェックポイント

チェックポイントやタスクの詳細は、ガイドラインP20-21を参照ください。

✓ 利用するパソコン等への対策	OSやソフトウェアの最新化をし、ウイルス対策ソフトを導入する
✓ 従業員が理解、実施する対策	パスワードを強化し、攻撃の手口を知る
✓ 利用するシステムへの対策	ウェブサービスやネットワークの権限設定を見直し、バックアップを取得する

タスク

OSやソフトウェアの更新	従業員に対策を周知	利用システム等の適切な設定	上記の活動に必要なIT知識の習得
自社が保有するパソコン等を確認し、OSの自動更新設定がある場合は実施します。OSやソフトウェア等の更新において従業員の作業が必要な場合は、実施マニュアルを作成し、周知します。	チェックポイントの内容を朝礼や社内メール等によって従業員に周知するとともに、社内のセキュリティ相談、報告の窓口として対応します。	保有するデータやサービス、アカウント等を社内の誰が利用可能か明らかにし、必要に応じてITベンダーと相談して、適切な設定を実施します。また、バックアップを取得し、データや設定を戻せる状態にします。	既存コンテンツ活用、資格取得に向けた学習等を実施します。

人材確保・育成

社内人材を活用する場合

確保

兼務でも１人は確保

- チェックポイントを実践するために、セキュリティ担当者を兼務でも１人は確保しましょう

配置転換

- セキュリティの知見がある従業員がいなくても、少しでも関連業務の経験がある者にセキュリティ担当を兼務させます(災害対策等を行う部署・IT部門・監督者・PC導入担当)（「サイバーセキュリティ体制構築・人材確保の手引き」※1 p25 ）

希望者の登用

- セキュリティ業務の実施を希望する従業員の社内公募を実施し、セキュリティ担当者を兼務させます

育成

- IPAコンテンツの活用（情報セキュリティ対策の基本、ランサムウェア攻撃の説明、メール詐欺、パスワードの強化）
- デジタル知識・スキルが学べるデジタル人材育成プラットフォームであるマナビDXのリテラシー講座の受講
- 1テーマ5分で情報セキュリティについて勉強できる無料の学習コンテンツIPA5分でできる！情報セキュリティポイント学習による学習
- 内閣官房国家サイバー統括室(NCO)インターネットの安心・安全ハンドブック中小企業向け抜粋版を社内研修の資料として活用する

情報セキュリティ啓発映像

試験・資格

- セキュリティを含むIT全般の基本的知識に関する試験「ITパスポート試験」を取得を促し、IT知識を習得（「人材手引き」p38 ）

社内の人手・知識が不足する場合

セキュリティ対策の相談

- 既に付き合いがあるITベンダーや、商工会・商工会議所等の支援機関と、自社のセキュリティについてコミュニケーションを取り、チェックポイントの実施に関する課題、従業員への周知方法、教育方法について相談します

相談窓口の活用

- IPA企業組織向けサイバーセキュリティ相談窓口を活用し、セキュリティに関する不安や課題を相談します

※ セキュリティ関連タスクに応じた、外部委託の判断基準について、詳しくは「人材手引き」p20に記載があります

相談の注意点

- 相談ポイントが分からない場合もあるかもしれませんが、例えば「データの漏洩が心配」「従業員の教育が不十分ではないか」「ニュースで聞いたランサムウェア攻撃、自社は大丈夫か」など身近なところから課題を挙げてみましょう
- 相談の際には、自社の業種・規模、実施中のセキュリティ対策について簡単に説明することで、より具体的なアドバイスを受けやすくなります

※1 経済産業省「サイバーセキュリティ体制構築・人材確保の手引き」（以下、「人材手引き」）

4. 段階的な取組

STEP1 STEP2 STEP3 STEP4

【事例】セキュリティ対策の始まりとなる、担当者の任命と体制の整備

企業のプロファイル

業種	建設業	従業員数	30人	セキュリティレベル	STEP1
ITの主要な利用シーン	販売管理、見積管理、経理等の本社業務				

事例の概要

背景

従業員30名規模で建設業を営むA社は、これまでセキュリティ対策をほとんど行っていませんでした。しかし、懇意にしていた取引先がサイバー攻撃により全てのサーバデータが消失して業務が完全に停止するインシデントを経験したことで危機感を持ち、セキュリティ対策が重大な経営課題となったため、社長は人材確保の対応を進めました。

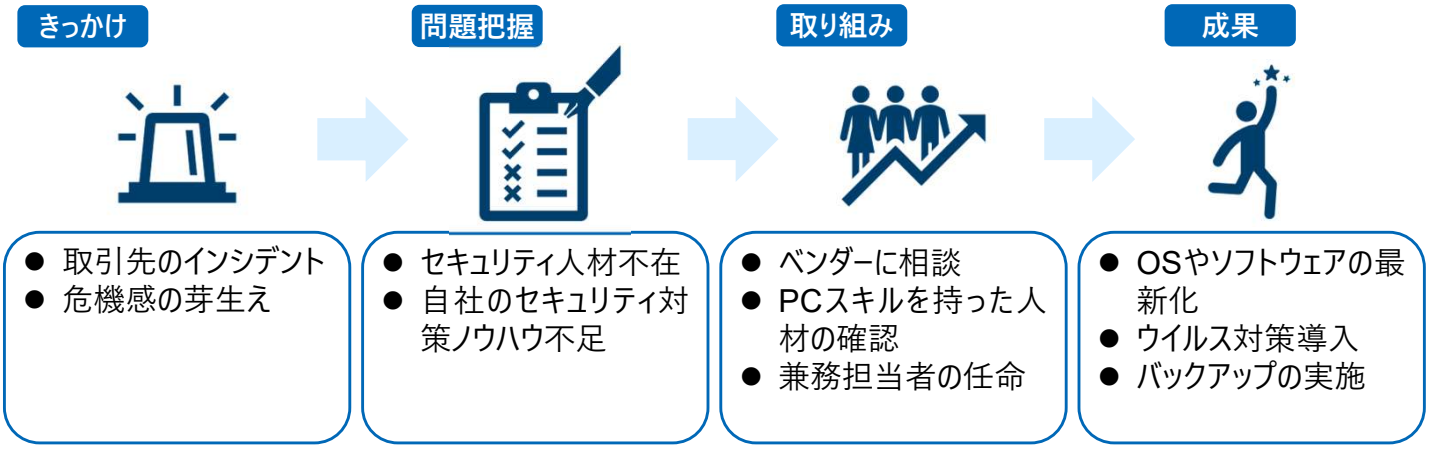
人材確保・育成の対応

1	従業員に、業務でPCをどの程度利用しているか、どういった使い方をしているかなどIT利用状況をヒアリングしたところ、セキュリティに関する知識とスキルを持った人材とノウハウが不足していることを把握した
2	取引のあるITベンダーに相談し、セキュリティ担当者を決めた方が良いこと、担当者は少しでもPCスキルのある人員が望ましいことを確認した
3	従業員と面談を行い、Webサイトの作成を担当している従業員にセキュリティ業務を兼務で任命し、社内とITベンダーの窓口として配置した

成果

配置したセキュリティ担当者がWebサイト作成で培ったPCスキルを活用して、分からないことは外部のITベンダーの担当者に聞きました。OSやソフトウェアの最新化、ウイルス対策や業務上必要なデータのバックアップを行うなど、基本的な取り組みとして、できるところから社内のセキュリティ対策を始められるようになりました。

A社の実践イメージ



取り組みのポイント	セキュリティの専門人材がいなくても、PCを使った業務を担当している従業員を探し、セキュリティ業務を兼務で任命して社内の対策を始めた

4. 段階的な取組
(2) 組織的な取り組みを開始する

チェックポイント

チェックポイントやタスクの詳細は、ガイドラインP22-25を参照ください。

基本方針の作成	管理体制の整備、法令・ガイドライン等の遵守、セキュリティ対策の実施など、組織の基本方針を作成し、従業員や顧客などの関係者に周知
実施状況の把握	機密情報やシステム機器の取扱い、ユーザIDや権限、パスワードの管理、ネットワーク防護等、自社が、現在どの程度セキュリティ対策を実施できているかを把握
対策の決定と周知	USB等の記録媒体の保管、インターネット利用等に関する従業員としての対策、従業員への教育の実施、緊急時の体制整備など組織としての対策を決定し、周知

タスク

基本方針の作成・周知

「情報セキュリティ基本方針（サンプル）」を参考にして、事業の特徴や顧客の期待などを考慮し、自社に適した基本方針を作成します。

セキュリティ対策の状況を把握

「5分でできる！情報セキュリティ自社診断」を利用して、自社のセキュリティ対策の実施状況を把握するとともに、社内のセキュリティ相談、報告の窓口として対応します。

対策の決定と従業員への周知

診断結果と「5分でできる！情報セキュリティ自社診断」の解説編を参考に、自社で実施すべき対策を決定し、従業員に周知します。

上記の活動に必要なIT知識の習得

既存コンテンツ活用、資格取得に向けた学習等を実施します。

人材確保・育成

社内人材を活用する場合

確保

担当者の増員
- 社内ルールの作成、システムの管理、従業員への教育などセキュリティ関連の業務量が増えることに応じて、担当者も増やす必要が出てきます

配置転換、登用の継続
- そのため、STEP1で示した隣接分野での業務経験を有する人材の＜配置転換＞、＜希望者の登用＞を引き続き実施します

育成
- 所属や役職に適したIPAコンテンツの活用（経営者、全従業員、新入社員）
- IPAセキュリティプレゼンターによるセキュリティ教育を聴講
- マナビDXのセキュリティ関連講座の受講
- IPA重要なセキュリティ情報を確認し、危険性が高い最新のセキュリティ上の問題と対策情報の収集

情報セキュリティ啓発映像

試験・資格
- 「情報セキュリティマネジメント試験」の資格取得を促し、IT知識を習得（「人材手引き」p38）

コミュニティへの参加
- セキュリティに関する地域のコミュニティに参加し、他社のセキュリティ担当者からの情報収集、意見交換を実施

社内の人手・知識が不足する場合

セキュリティ対策の相談
- 既に付き合いがあるITベンダーや、商工会・商工会議所等の支援機関などに、組織的なセキュリティの取り組み、社内の情報セキュリティ基本方針の作成等について相談します

教育人材の確保
- IPAセキュリティプレゼンターを活用し、従業員へのセキュリティ教育や講習が実施可能な人材を確保します

身近なコミュニティへの参画
- セキュリティに関する身近なコミュニティに参画し、交流・情報収集を行うことで、外部人材の活用の幅が広がる可能性があります

地域SECUNITY
- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティであり、イベントの継続開催による意識向上や人材育成、国や専門家からの情報提供の場となります

4. 段階的な取組

STEP1 STEP2 STEP3 STEP4

【事例】必要なセキュリティ水準に応じた、人材要件確認と教育実践

企業のプロファイル

業種	製造業	従業員数	10人	セキュリティレベル	STEP2
ITの主要な利用シーン	受発注の管理、工程管理				

事例の概要

背景

従業員10名規模で金属加工業を営むB社は、社内のローカルエリアネットワークでITを利用してセキュリティ対策を行っていました。受発注管理業務をデジタル化した際にインターネット経由でシステムを利用することとなりましたが、インターネット活用時におけるセキュリティ対策として何をやれば良いかわからなかったため、社長はセキュリティ対策に必要な人材育成の対応を進めました。

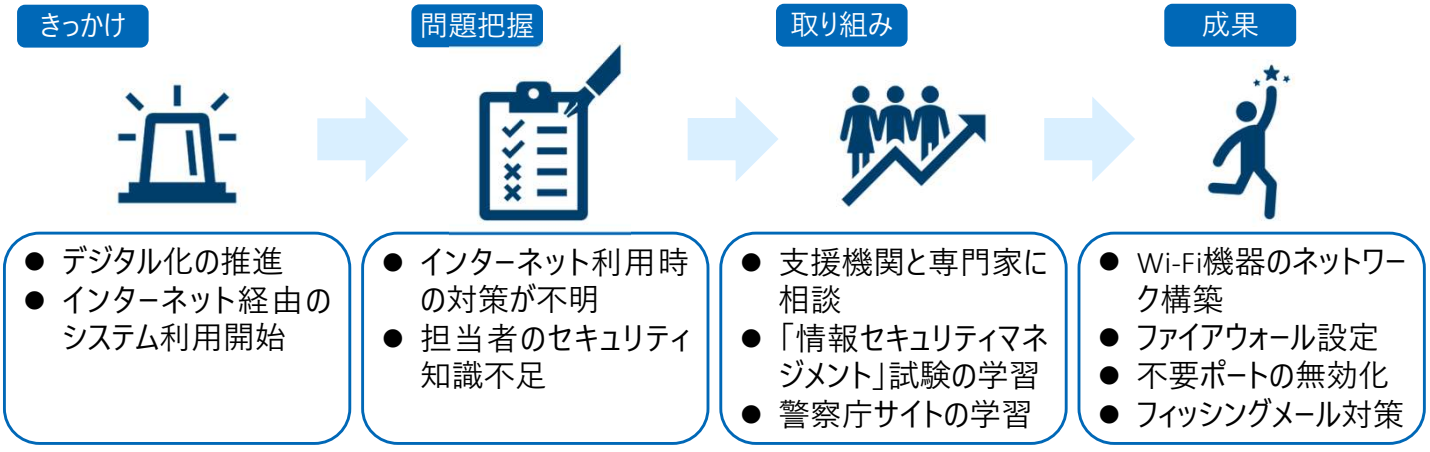
人材確保・育成の対応

1	担当者は総務との兼務でセキュリティに詳しくなく、自社だけでの対応は困難と判断し、補助金制度の活用で付き合いのあった自治体の経営支援課や地域の産業振興機構にセキュリティ対策相談をした
2	産業振興機構からセキュリティ専門家として情報処理安全確保支援士の紹介を受け、セキュリティ対策ベンダーと最低限の会話ができるよう、担当者がセキュリティ知識を身につける提案を受けた
3	専門家に学習方法を相談したところ、IPAの「情報セキュリティマネジメント」資格取得の提案を受け、初めてで分からないこともあったが、外部講習で要点を学び、市販参考書で学習を進め、社長と担当者が資格を取得した
4	警察庁のサイバーセキュリティ対策サイトを活用し、サイバー攻撃の手口や事例、被害の防止対策や被害発生時の相談先を学習した

成果

資格取得前はITベンダーの提案内容が理解しきれないまま採用していましたが、取得後は理解を深めて採用することができました。Wi-Fi機器導入に伴うセキュリティ設定、ファイアウォールにおける不要ポートの無効化、不審メールの見分け方の社内周知を実施するなど、学習した知識を活かして必要な対策を選択して行うことができるようになりました。

B社の実践イメージ



取り組みのポイント

- ✓ 社内だけでは、対応が難しいため、自治体の経営支援課や産業振興機構に相談した
- ✓ 資格取得の学習により、自社に必要なセキュリティ対策(外部接続の課題)を検討し、実装や社内周知を実現できた

参考：IPA 情報処理技術者試験 ：https://www.ipa.go.jp/shiken/index.html
参考：IPA 情報セキュリティマネジメント試験：https://www.ipa.go.jp/shiken/kubun/sg/index.html

4. 段階的な取組
(3) 本格的に取り組む

STEP1 STEP2 **STEP3** STEP4

チェックポイント

チェックポイントやタスクの詳細は、ガイドラインP26-41を参照ください。

体制の整備	セキュリティ対応の役割、責任、権限を明確にしましょう
セキュリティ対策の実行と見直し	策定した基本方針に沿って、リスク分析を行い、必要な対策を実行し、定期的に見直しましょう
取引先/外部情報サービスの管理	取引先のセキュリティ対策状況、自社の機密情報を取り扱う外部情報サービスの利用状況や安全性を把握しましょう
インシデントの対応手順・体制等の整備	セキュリティインシデントが発生した場合の対応手順、対応体制等を定め、インシデントの発生に備えましょう

タスク

人材などを確保し体制を整備

セキュリティ推進活動を担当する部署、役員及び従業員を決定し、責任及び権限を割り当てます。また、守秘義務等の社内ルールを定めます。

セキュリティ対策の実行と定期的な見直し

リスク分析を行い、資産管理や攻撃等の防御・検知といった必要な対策を決定し、実行しましょう。また、セキュリティに関する最新動向を収集し、対策を定期的に見直しましょう。

取引先/外部情報サービスの管理

取引先とのビジネス・システム上の関係やセキュリティ対策状況を把握し、ルール設定や役割整理等を行います。
また、自社の機密情報を扱う外部情報サービスの管理も行います。

インシデントの対応手順・体制等の整備

インシデントが発生した場合に備え、対応手順や連絡体制、役割分担や報告事項を定めます。
また、インシデント発生時における目標復旧時間や時点の整備、バックアップや戻しの手順を定めます。

人材確保・育成

社内人材を活用する場合

確保

人材確保、配置転換と登用の継続

- 社内に適切な体制を確保するとともに、セキュリティ対策業務に関して知識と経験を持つ人材の確保が必要です
- STEP1で示した隣接分野での業務経験を有する人材の配置転換、希望者の登用を引き続き実施し体制を構築します

人材の採用

- 他社等でサイバーセキュリティ対策業務に従事した経験を有する人材を中途採用し、自社で活用します（「人材手引き」p25）

育成

- IPAコンテンツの活用（情報セキュリティ規程作成、セキュリティインシデント対応）
- IPA産業サイバーセキュリティセンター(ICSCoE)短期プログラム、責任者向け講習の受講

情報セキュリティ啓発映像

試験・資格

- 情報システムに係るリスクを分析し、コントロールを検証・評価することによって、組織体の目標達成に寄与し、利害関係者に対する説明責任を果たす監査人や情報システム責任者向けの「システム監査技術者試験」の資格を習得

社内の人手・知識が不足する場合

セキュリティ対策相談

- 情報セキュリティ規程の策定や周知、改善に関して、支援機関等への相談を実施します。また、ITベンダーに情報セキュリティ規程に沿った必要な対策の実施について相談します

アドバイザリー人材の確保

- 自社の対策を分析・評価・助言できる内部人材を確保し、外部のセキュリティ専門家の支援を活用し、コンサルティングを依頼します

ルール策定、訓練実施

- 外部のセキュリティ専門家の支援を活用し、インシデント時の対応や事業継続管理などのルールの策定、訓練等を実施します

セキュリティサービスの導入

- 適切な異常監視、インシデント対応を実施するために、外部のセキュリティサービスを導入します

4. 段階的な取組

STEP1 STEP2 **STEP3** STEP4

【事例】セキュリティ対策組織の設置と役員主導による組織運営

企業のプロファイル

業種	卸売業	従業員数	100人	セキュリティレベル	STEP3
ITの主要な利用シーン	受発注の管理、物流・自動倉庫、経理等の本社業務				

事例の概要

背景

従業員100名規模で再生資源の卸売業を営むC社は、主要な業務プロセスにシステムを導入し、サイバーセキュリティ対策のためにルール整備等を行っていましたが、新たな仕事を受けた大手顧客から、厳格なセキュリティ要件の提示を受けました。チェックの結果、従業員向け教育や訓練、ポリシーや管理体制の構築などが十分でないことが明らかになり、これを受けて社長はセキュリティ対策に必要な人材確保・育成に取り組みました。

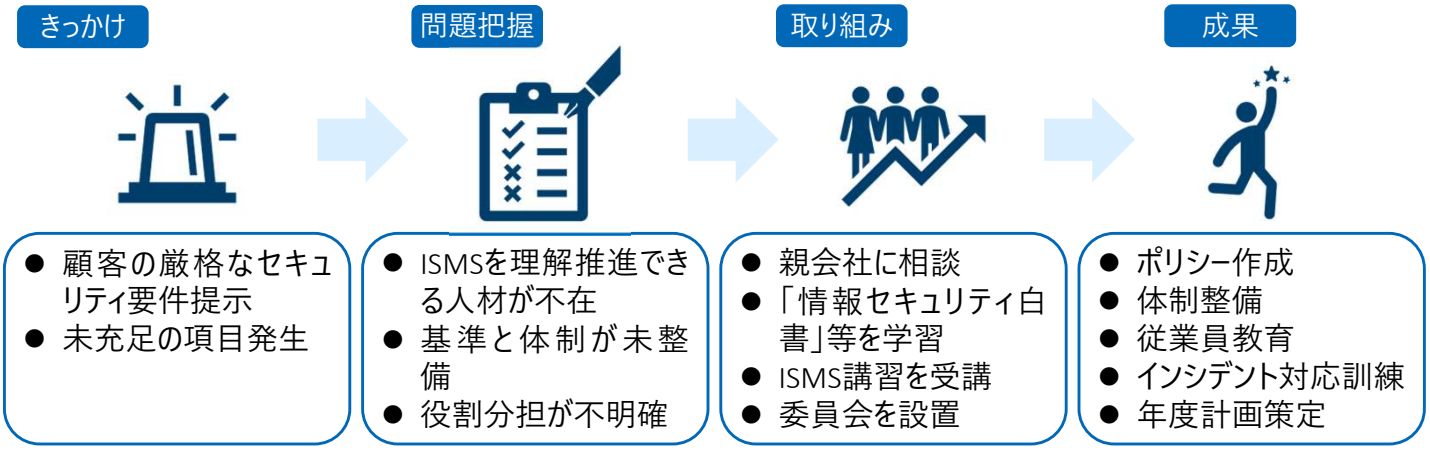
人材確保・育成の対応

1	大手顧客から求められる水準の対策を行う仕組みが無かったため、親会社のセキュリティ部門に対策について相談し、脅威情報の連携や、教育訓練の進め方についてアドバイスを受けた
2	外部の専門家が実施しているISO27001の情報セキュリティマネジメントシステム（ISMS）講習や、IPAで発行されている「情報セキュリティ白書」や「DX白書」等で担当従業員の知識向上を図った
3	セキュリティ対策を推進するため、社内にセキュリティ委員会を設置し、責任者として役員を任命した。また、委員会の運営や実務を担う専門人材の確保や育成にも取り組んだ

成果

親会社のセキュリティ部門の支援を受けながら、複数名の兼務担当従業員による委員会を設置しました。委員会の中では、体制・役割を明確化し、自社セキュリティポリシーを作成して教育やインシデント対応訓練の企画や実行をはじめ、セキュリティ対策に必要な年度予算の検討や確保まで取り組みができるようになりました。

C社の実践イメージ



取り組みのポイント：講習受講や自主的な学習で得た知識をもとに、親会社のサポート・助言のもと、社内の訓練や教育、ポリシー作成など専門性の高い活動に取り組んだ

参考：IPA 書籍・刊行物 ：https://www.ipa.go.jp/publish/index.html
参考：IPA 情報セキュリティ教材・ツール：https://www.ipa.go.jp/security/sec-tools/index.html

4. 段階的な取組

STEP1 STEP2 STEP3 **STEP4**

(4) より強固にするための方策

チェックポイント

チェックポイントやタスクの詳細は、ガイドラインP42-63を参照ください。

✓ 資産ベースのリスク分析	自社に固有のリスクを把握し、必要な対策を補強しましょう
✓ 技術的対策の強化	資産ベースのリスク分析結果や利用システムに応じたセキュリティ対策を実施しましょう
✓ 外部のセキュリティサービスの活用	専門性が求められるセキュリティサービスや技術的対策の導入・運用に当たり、必要性の判断、委託仕様の策定を自社で行い、外部委託を活用しましょう
✓ インシデント対応の強化	事業継続の観点から被害の最小化、早期復旧のための備えを実施しましょう

タスク

資産ベースのリスク分析を実施

情報資産を洗い出し、リスク値を算定し、セキュリティ対策を検討し、決定します。

技術的対策を強化

セキュリティ機器の設置や対策ソフトの導入、自社が利用するシステム・ソフトウェアに応じたセキュリティ対策を実施します。

外部のセキュリティサービスを活用

脆弱性診断、セキュリティ監視・運用などのセキュリティサービスを自社の環境に合わせて活用します。

事業継続を考慮した復旧体制を整備

「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、事業継続、早期復旧のために備えます。

人材確保・育成

社内人材を活用する場合

確保

セキュリティ専門人材の採用

- より強固な対策のために、自社の事業を理解し、現状のセキュリティ対策の実効性確保・改善、脆弱性への迅速な対応、新たな対策の検討・実施等が必要です
- このため、一層高い知識・経験・技能を持った人材を確保し、体制を整備する必要があります。STEP3までで示した確保策に加えて、次の取り組みを実施します
  - ✓ サイバーセキュリティを専門とする教育機関を修了した人材の新卒採用（「人材手引き」p25）
  - ✓ セキュリティ専門家を招聘して、CISO等に任命（「人材手引き」p20）

育成

- IPAコンテンツの活用（脆弱性発見手法、テレワークセキュリティ、安全なウェブサイト運用）
- 脆弱性の概要や対策方法等の知識を実習形式で体系的に学べるツール脆弱性体験学習ツール AppGoatによる学習を実施

情報セキュリティ啓発映像

試験・資格

- サイバーセキュリティ対策を推進する人材の国家資格である、情報処理安全確保支援士（登録セキスペ）の資格を取得

コミュニティへの参加

- セキュリティに関する地域のコミュニティに参加し、他社担当者からの情報収集、意見交換を実施

社内の人手・知識が不足する場合

セキュリティ対策の相談

- ITベンダーに対して、自社の実施している対策、保有するウェブサイト、クラウドサービス、テレワークの利用状況、事業特性などに合わせた追加のセキュリティサービス、技術的対策の必要性について相談します
- 相談先は下記のリストを活用することができます
  中小企業向けサイバーセキュリティ対策支援者リスト

法的助言人材の確保

- 法令等遵守対応のため、弁護士等の助言を得るための契約をします（「人材手引き」p20）

外部監査の実施

- 監査には、内部監査(第一者)、外部監査（第二者・第三者）がありますが、営業秘密や個人情報等の特に十分な対策が必要な場合には、第三者によるセキュリティ監査を実施します

外部組織の仕組み活用

- 取引先や同業者を経由したサイバー攻撃も増えていることから、日本シーサート協議会やISAC※などの組織へ参加し情報を収集します

※Information Sharing and Analysis Centerの略。同業界の事業者同士でサイバーセキュリティに関する情報の共有・分析などを行う組織を指す

4. 段階的な取組

STEP1 STEP2 STEP3 **STEP4**

【事例】セキュリティ専門家育成のための仕組みと制度の設置

企業のプロファイル

業種	情報通信業	従業員数	50人	セキュリティレベル	STEP4
ITの主要な利用シーン	SI事業全般、クラウドの導入/運用/保守業務、経理等の本社業務				

事例の概要

背景

従業員50名規模で情報通信業を営むD社は、保管されているデータのバックアップによるデータ保全は行っていたものの、顧客から、インシデント検知から復旧までの体制や具体的手順を相談されたことをきっかけに、社内の仕組みを確認した結果、検知や体制、対応手順が十分とは言えず検討を進めることとしました。特に、意思決定や社内調整は、社内の人材として行う必要があり、社長は高度なセキュリティ技術を有する従業員の採用を検討しましたが、地方であることや給与体系により採用は困難であったため、在籍する従業員を育成する決心をしました。

人材確保・育成の対応

1	セキュリティ業務に従事している担当と話し合い、高度人材として育成する候補を選定するとともに、情報処理安全確保支援士として育成すべく教材費や受験料負担、合格報奨金等、資格取得奨励制度を設けた
2	制度での支援に加え、教育訓練休暇で学習時間を配慮しながら、社長がメンターとしてキャリアアップの受験相談にのり、担当者が参考書を用いて1年間学習を実施した末、情報処理安全確保支援士を取得した
3	最新の脅威動向やインシデント対応手順を把握できるように、IPAやJPCERT、NCO等の公的機関から情報収集を行った
4	資格を取得した担当者が、自社で行っている監視やモニタリング業務をより効果的に進めるために、社外のセキュリティベンダーサービスの活用を提案・導入した

成果

資格取得や公的機関の活用で得た情報により、セキュリティに関する監視やモニタリングなどサイバー攻撃を早期検知する仕組みや、インシデント発生時の組織としてCSIRTを構築し、対応時の役割や手順を見直しました。また、検知は外部委託し、運用の効率化を図ることができました。

D社の実践イメージ

きっかけ	問題把握	取り組み	成果
			
● 取引先からの相談 ● 社内の仕組みを再確認	● 高度なセキュリティ専門人材が不在 ● 社内体制、仕組みが不十分	● 「情報処理安全確保支援士」試験の学習 ● 公的機関の情報収集 ● 社外サービスの活用	● 最新情報の取得 ● ログ監視体制の整備、効率化 ● インシデント対応体制、手順の整備

取り組みのポイント

✓ 資格取得奨励制度のもと、社内人材を確保し高度専門人材(登録セキスペ)として育成した
✓ 公的機関やコミュニティでの意見交換による最新情報収集や、外部のセキュリティサービス導入等によるインシデント時の体制、検知から復旧までの対応手順を整備した

参考：IPA 情報セキュリティ10大脅威：https://www.ipa.go.jp/security/10threats/index.html
参考：JPCERT/CC 注意喚起：https://www.jpcert.or.jp/at/2025.html
参考：NCO 注意喚起：https://www.cyber.go.jp/news/press/tyuuikanki.html

本書で用いている主な用語の説明

クラウドサービス

サーバー等を自前で所有する代わりに、インターネット経由で同様の機能を提供するものをいいます。レンタルサーバー、SaaS(Software as a service)、ASP(Application Service Provider)などがクラウドサービスの一種です。

情報資産

様々な「情報」のうち、企業として管理すべき対象として選択されたものです。また、情報システムなども「情報資産」に含める場合があります。

脆弱性

情報セキュリティの文脈では、脆弱性はシステムやソフトウェア、ネットワークに存在するセキュリティ上の弱点を指します。この弱点が悪意のある攻撃者に利用されると、データの漏洩、改ざん、破壊、不正アクセスなどのセキュリティインシデントが発生する可能性が生じます。

セキュリティインシデント

セキュリティの事故・出来事のことで、単に「インシデント」という事もあります。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。

セキュリティ監視

組織のITシステムやネットワークを常時モニタリングし、セキュリティ上の脅威を検知・対処するための取り組みのことです。 不審な動きを検知し、被害を未然に防ぎます。

ファームウェア

ハードウェア(スマートフォンや家電、ルーターなどのネットワーク機器)を制御するソフトのことです。

ランサムウェア

「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。感染したパソコンのデータを暗号化するなど使用不可能にし、その解除と引き換えに金銭を要求します。さらに新たな攻撃手法として、ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバー上のデータを窃取した上で一斉に暗号化してシステムを使用不可能にし、データの復旧に対する金銭要求に加えて、窃取したデータを公開しない見返りの金銭要求も行うなど、二重の脅迫を行う場合もあります。

リスク分析

リスクの特質を理解し、リスクレベル(ある事象の結果とその起こりやすさとの組合せとして表現されるリスクの大きさ)を決定するプロセスのことです。

CISO

「Chief Information Security Officer」（最高情報セキュリティ責任者）の略。経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者のことです。

NW機器

「Network機器」の略。ルーターやスイッチなど、ネットワークを構成するための機器のことです。

付録E※1 用語の定義：
https://www.meti.go.jp/policy/netsecurity/downloadfiles/guide_v3.0.pdf
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：
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_8.pdf

※1 経済産業省「サイバーセキュリティ経営ガイドライン」

中小企業のための
セキュリティ人材確保・育成の実践ガイドブック

2026年3月

独立行政法人情報処理推進機構
〒113-6591
東京都文京区本駒込二丁目28番8号文京グリーンコートセンターオフィス
URL　https://www.ipa.go.jp/security/
電話　03-5978-7530
E-mail　isec-pr-cssp@ipa.go.jp