

# 中小企業の情報セキュリティ対策ガイドライン第4.0版

2026年3月

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

# 中小企業の情報セキュリティ対策ガイドライン第4.0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
- 本編2部と付録より構成
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載（第1部）
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明（第2部）
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録
- 2026年3月27日公表



# 第4.0版の主な変更点について

## ● 第2部 実践編

- 中小企業実態調査結果及びサプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）を受けて、第2部実践編を全面的に改訂

## ● 付録

- 付録1「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」を追加
- 付録3「5分でできる！情報セキュリティ自社診断」、付録4「情報セキュリティハンドブック（ひな形）」を第2部実践編のSTEP2に合わせて見直し
- 付録5「情報セキュリティ関連規程（サンプル）」を第2部実践編に合わせて見直し
- 付録6「資産管理台帳」を見直し

## ● 対象組織

- 全ての業種の中小企業および小規模事業者  
(法人、個人事業主、各種団体も含む)

## ● 想定読者

- 経営者と情報セキュリティ対策を実践する責任者・担当者

## ● 記載範囲

- 業務におけるITの活用および情報資産の管理に関する情報セキュリティ対策を取り扱う
- 工場設備や制御システム等の分野は本ガイドラインの対象外

# ガイドラインの構成

	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、及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。
	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 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	セキュリティ対策を実施するために必要な人材の確保・育成のための方策ガイドです。
	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ルールを文書化したもののサンプルです。
	付録6 資産管理台帳 (サンプル)	情報資産及び関連するネットワーク機器、ソフトウェア、ハードウェアを一覧化したもののサンプルです。
	付録7 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。

## 1. 情報セキュリティ対策を怠ることで企業が被る不利益

- (1) 金銭の損失
- (2) 顧客の喪失
- (3) 事業の停止
- (4) 従業員への影響

## 2. 経営者が負う責任

- (1) 経営者などに問われる法的責任
- (2) 関係者や社会に対する責任

## 3. 経営者は何をやらなければならないのか

- (1) 認識すべき「3原則」
- (2) 実行すべき「重要7項目の取組」



# 経営者は何をやらなければならないのか

## (1) 認識すべき「3原則」

- 経営者は、以下の**3原則**を認識し、対策を進める。

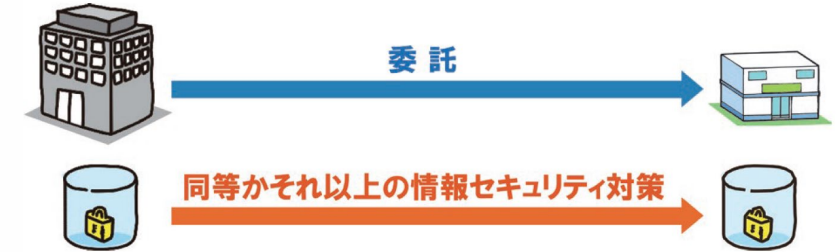


**原則 1** 情報セキュリティ対策は経営者のリーダーシップで進める

- 経営者は、IT活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策の実施を主導

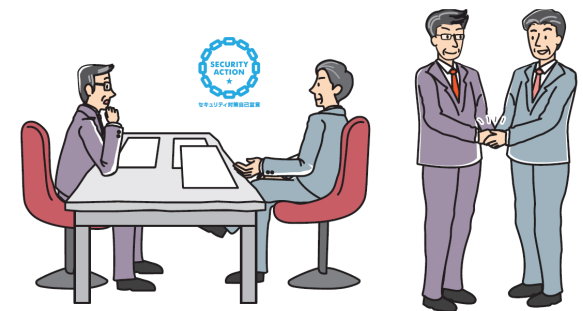
**原則 2** 委託先の情報セキュリティ対策まで考慮する

- 必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は、対処を検討



**原則 3** 関係者とは常に情報セキュリティに関するコミュニケーションをとる

- 情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいが発生した際にも、説明責任を果たすことができ、信頼関係を維持することが可能



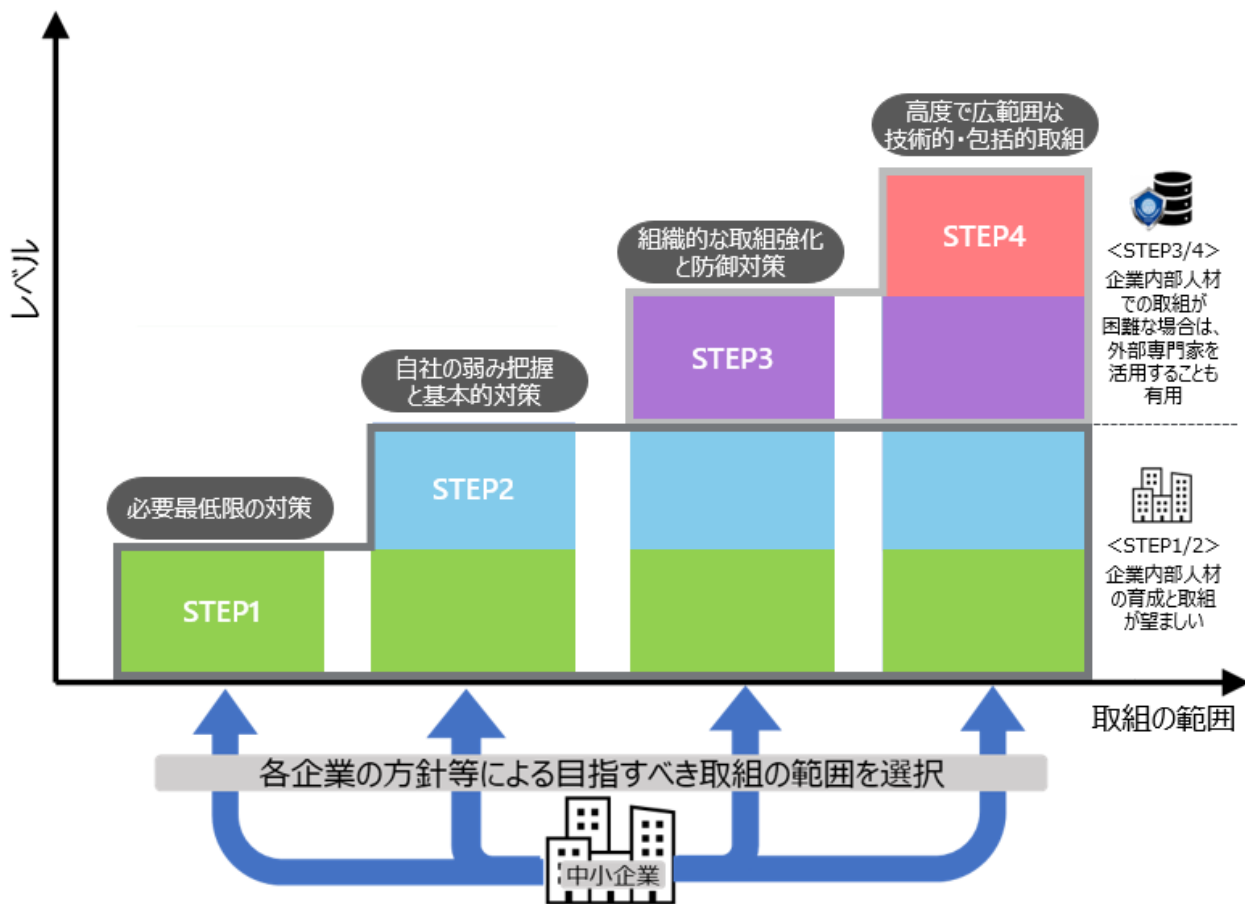
## (2) 実行すべき「重要7項目の取組」

- 経営者は、以下の7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

取組 1	情報セキュリティに関する組織全体の対応方針を定める
取組 2	情報セキュリティ対策のための予算や人材などを確保する
取組 3	必要と考えられる対策を検討させて実行を指示する
取組 4	情報セキュリティ対策に関する適宜の見直しを指示する
取組 5	緊急時の対応や復旧のための体制を整備する
取組 6	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組 7	情報セキュリティに関する最新動向を収集する

# 第2部 実践編

- できるところから始めて**段階的にステップアップ**



STEP	取組の目安	想定している企業の例
STEP1 (P20)	すべての企業が実施すべき基本的なセキュリティ対策であり、「情報セキュリティ6か条」を活用し、自社の業務・情報・従業員・取引先を守る必要最低限の対策から始めます。	STEPを目指すきっかけ ●アナログ中心だったが、近年業務にITを取り入れ始めた 企業をとりまく状況 ●周囲の取引先でセキュリティ被害が発生し、その脅威を身近に感じた等
STEP2 (P22)	基本的なセキュリティ対策を組織的に取り組むために、「5分でできる! 情報セキュリティ自社診断」を活用し、自社の弱みを把握し基本的対策を決定するとともに、組織としての情報セキュリティ基本方針を作成します。	STEPを目指すきっかけ ●業務の効率化や情報共有促進のために、ITシステムの本格導入を進めている 企業をとりまく状況 ●セキュリティ対策が標準化されず、従業員の属人的な対応となっていた等
STEP3 (P26)	組織的な取組を強化し、セキュリティ対策に本格的に取り組む企業は、必要に応じて外部専門家を交え、セキュリティに関する体制を整備し、基本的な組織的対策や技術的な防御対策を実施します。	STEPを目指すきっかけ ●取引先からの要請を受けて、高度なセキュリティ対策が必要となった 企業をとりまく状況 ●日常的に受発注をしているなど、取引先企業が必要不可欠な存在となっている等
STEP4 (P42)	より強固で広範囲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、必要に応じて外部専門家を交えてリスク分析を行い、技術的な対策の強化により包括的なセキュリティ対策を実施します。	STEPを目指すきっかけ ●外部監査への対応や基準達成のため、従来以上に厳格なセキュリティ対策が必要となった 企業をとりまく状況 ●企業活動においてITやデジタル技術が欠かせない存在となり、DXを積極的に推進している等

# (1) 情報セキュリティ6か条

- **情報セキュリティ6か条**を守るところから始めてみましょう

## No1. OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いのOS やソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。

## No2. ウイルス対策ソフトを導入しよう！

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。

## No3. パスワードを強化しよう！

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

## No4. 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違っただめに、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

## No5. バックアップを取ろう！ ※第4.0版において追加

故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えたり、暗号化されてしまうことがあります。事業が継続できるようバックアップを取得しておきましょう。

## No6. 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイト に似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

# (1) 情報セキュリティ基本方針の作成と周知

- 経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために簡潔な文書を作成・周知
- 付録2「**情報セキュリティ基本方針（サンプル）**」を編集して策定

## 付録2「情報セキュリティ基本方針（サンプル）」

### 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

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。  
 ※赤字箇所は、自社の事情に応じた文章を選択してください。

#### 情報セキュリティ基本方針

株式会社〇〇〇（以下、当社）は、お客様からお預かりした/自社の「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恥えべく、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。

- 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。
- 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での正式な規則として定めます。
- 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、技術を取得し、情報セキュリティへの取組みを確かなものにします。
- 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、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。
- 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  
 代表取締役社長 〇〇〇

# STEP2 組織的な取り組みを開始する (2) 実施状況の把握

● 自社のセキュリティ対策の実施状況を把握するために、  
付録3「5分でできる！情報セキュリティ自社診断」を活用

- 25項目の設問に答えるだけで、  
自社の情報セキュリティの問題点を  
簡単に把握できる

- 基本的対策 6項目
- 従業員としての対策 11項目
- 組織としての対策 8項目

- 解説編の対策例を参考に、  
社内ルールを作成することができる

付録3「5分でできる！情報セキュリティ自社診断」

中小企業・小規模事業者の皆様へ

**5分**でできる！  
情報セキュリティ自社診断

最新動向への対応、できていますか？

脅威や攻撃の変化  
脆弱性攻撃、ランサムウェア、標的型攻撃、サプライチェーン攻撃

IT環境の変化  
IoT機器、クラウド、AI、スマートフォン

取り返しのつかないことになる前に  
あなたの会社のセキュリティ状況を  
「5分でできる！自社診断」でチェック！

No	診断内容
Part 1 基本的対策	1 パソコンやスマートフォンなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2 パソコンやスマートフォン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 <sup>1)</sup> は最新の状態にしていますか？
	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？
	4 データの共有設定を必要人に限定していますか？
	5 故障や誤操作、ウイルス感染などによる重要情報 <sup>2)</sup> の消失に備えて定期的にバックアップを取得していますか？
	6 新たな脅威や攻撃の手法を知り対策を社内共有する仕組みはできていますか？
Part 2 従業員としての対策	7 電子メールの添付ファイルや本文中の URL リンクを介したウイルス感染に気をつけていますか？
	8 電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	9 重要情報の受け渡しは、暗号化など安全な手段で行っていますか？
	10 無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	11 インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？
	12 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？
	13 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14 重要情報が記載された書類や重要なデータが保存された媒体を破壊する時は、復元できないようにしていますか？
	15 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	16 関係者以外の事務所への立ち入りを制限していますか？
	17 退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
Part 3 組織としての対策	18 内部ネットワークを守るため、不正アクセス対策機能を設定していますか？
	19 ウェブサイトで公開すべきでない情報を公開していませんか？
	20 従業員に情報セキュリティに関する教育や注意喚起を行っていますか？
	21 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23 クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24 セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	25 情報セキュリティ対策（上記 1～24 など）をルール化し、従業員に明示していますか？

## 5分でできる！情報セキュリティ自社診断

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？	従業員としての対策	14	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
	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は最新の状態にしていますか？		15	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	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？		16	関係者以外の事務所への立ち入りを制限していますか？
	4	データの共有設定を必要な人に限定していますか？		17	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	5	故障や誤操作、ウイルス感染などによる重要情報の消失に備えて定期的にバックアップを取得していますか？		18	内部ネットワークを守るため、不正アクセス対策機能を設定していますか？
	6	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？		19	Webサイトで公開すべきでない情報を公開していませんか？
従業員としての対策	7	電子メールの添付ファイルや本文中の URLリンクを介したウイルス感染に気をつけていますか？	組織としての対策	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	8	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？		21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	9	重要情報の受け渡しは、暗号化など安全な手段で行っていますか？		22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	10	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？		23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	11	インターネットを介したウイルス感染や SNS への書き込みなどのトラブルへの対策をしていますか？		24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管していますか？		25	情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？			

# STEP2 組織的な取り組みを開始する (3) 対策の決定と周知



- 自社診断で問題があった項目は、解説編を参考に対策を決定
- 付録4「**情報セキュリティハンドブック（ひな形）**」を編集して社内周知

付録3「5分でできる！情報セキュリティ自社診断」

付録4「情報セキュリティハンドブック（ひな形）」

**脆弱性対策**

**No. 1 OSやソフトウェアは常に最新の状態にする**

OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が発生します。それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。

**対策例**

- Windows Update、(WindowsOSの場合)、ソフトウェア・アップデート (macOSの場合) などベンダの提供するサービスを実行する。
- Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
- 利用中のソフトウェアに脆弱性がないか、MyJVN(バージョンチェック)を確認する。
- 脆弱性が存在した場合は、手順に沿って修正パッチを適用する
- サポートのあるOS、ソフトウェア、ネットワーク機器を利用する

**情報セキュリティハンドブック**

このハンドブック（ひな形）の使い方

- このハンドブック（ひな形）は、従業員に配布し、自社のセキュリティポリシーを実行するためのものです。
- 5分でできる「情報セキュリティ自社診断」の結果を参照しています。
- 赤字で記載した箇所は注意例です。自社のルールと状況に合わせて修正してください。
- 黄色で記載した箇所は、適切な情報セキュリティポリシーの項目を参照して修正してください。

**目次**

1 全社基本ルール	1ページ
2 仕事中的ルール	3ページ
3 全社共通のルール	8ページ
4 テレワークのセキュリティ	11ページ

株式会社〇〇〇

**1-1 全社基本ルール**

**2-1 仕事中的ルール**

**3-1 全社共通のルール**

**私有情報機器の利用** [自己診断No. 2.1]

● 私有の情報機器を業務で利用する場合は以下を遵守する。

情報機器の種類	遵守事項
複数の外部アドレスを入力する	<ul style="list-style-type: none"> <li>社内用で保持されたものを禁止する</li> <li>業務利用を禁止する</li> <li>社内LANへの接続を禁止する</li> <li>ウイルス対策ソフト、アプリケーションは総務部システム担当が指定したものを導入し、許可を得たうえで利用する</li> <li>業務終了後に業務用データは総務部システム担当の指定するツールで完全消去する</li> <li>従業員個人のメールアドレスに業務用データを送信して送信することを禁止する</li> <li>社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する</li> </ul>
スマートフォン	<ul style="list-style-type: none"> <li>会社で提供した機器を利用する</li> <li>充電を禁止、社内/社外への接続を禁止する</li> <li>ウイルス対策ソフト、アプリケーションのインストールは総務部システム担当が指定したものを導入し、許可を得たうえで利用する</li> <li>取引先アドレスを除く業務用データ一時的保存を禁止する</li> <li>従業員個人のメールアドレスに業務用データを送信して送信することを禁止する</li> <li>社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する</li> </ul>
USBメモリ、外部HDDなどの記憶機器を挿入した機器	<ul style="list-style-type: none"> <li>会社で提供した機器を利用する</li> <li>私有情報の保存を禁止する</li> <li>総務部システム担当の許可を得て利用する</li> <li>業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する</li> </ul>

「情報セキュリティハンドブック」を編集し、社内周知

解説編を参考に、対策を決定

# (1) 情報セキュリティ基本方針の作成

- セキュリティ推進活動に係る自社の基本方針を文書化し、社内外に周知

## 付録2「情報セキュリティ基本方針（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

株式会社〇〇〇〇（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。

- 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。
- 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での正式な規則として定めます。
- 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する。
- 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。
- 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

## STEP3 本格的に取り組む (2) 体制の整備

- セキュリティ対応の役割、責任、権限を明確化
- 対策の実行に必要な人材は、付録1「**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**」を活用して確保・育成

付録1「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」



- STEPごとに、社内セキュリティ担当者の役割・業務を提示し、対策を実行するための人材の確保・育成の方策を紹介
- あわせて実際の中小企業における人材確保・育成事例についても掲載



### 4. 段階的な取組

(1) できるところから始める

STEP1 STEP2 STEP3 STEP4

チェックポイント

- 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、HW機器の更新	従業員に対策を周知し、継続する	利用サービス、HW機器等に適切な設定をする	上記の活動に必要なIT知識の習得
-------------------	-----------------	-----------------------	------------------

人材確保・育成

社内人材を活用する場合

確保

- 業務でも1人は確保
- チェックポイントを実施するために、セキュリティ担当者を業務でも1人は確保しましょう。
- 配属転換（人材手引書p25）
- 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業務させます。（災害対策等を行う部署・IT部門・監督者・PC導入担当）
- 希望者の費用
- 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業務させます。

社内の人手・知識が不足する場合

支援機関との連携

- 緊に付き合いたいITベンダーや、商工会・商工会振興所の支援機関は、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整備に関する課題、従業員への周知方法、教育方法について相談します。
- IPA企業組織向けサイバーセキュリティ相談窓口の活用
- 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「サイバーセキュリティ体制構築・人材確保の手引書」p20に記載があります。

### 4. 段階的な取組

【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

STEP1 STEP2 STEP3 STEP4

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、これまでサイバー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、顧客にしていた取引先がサイバー攻撃により全てのサーバー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、社員は人材確保の対応を進めました。

人材確保・育成の対応

- 従業員にヒアリングを行い、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聞き、社内のIT利用状況を確認し、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
- 取引のあるベンダーに相談し、セキュリティ担当者を決めた方がよいこと、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
- 従業員と面談を行い、PCを使い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業務で任命し、社内と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、わからないことは外部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、基本的な取組点として、できるところから社内のセキュリティ対策を始めるようになりました。

A社の実践イメージ

きっかけ	問題把握	取り組み	成果
<ul style="list-style-type: none"> <li>取引先のインシデント</li> <li>危機感の芽生え</li> </ul>	<ul style="list-style-type: none"> <li>セキュリティ人材不在</li> <li>自社のセキュリティ対策ノウハウ不足</li> </ul>	<ul style="list-style-type: none"> <li>ベンダーに相談</li> <li>PCスキルを持った人材の確認</li> <li>業務担当者の任命</li> </ul>	<ul style="list-style-type: none"> <li>OSの最新化</li> <li>ソフトウェアの最新化</li> <li>ウイルス対策導入</li> <li>バックアップの実施</li> </ul>

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業務で任命して社内の対策を始めた。

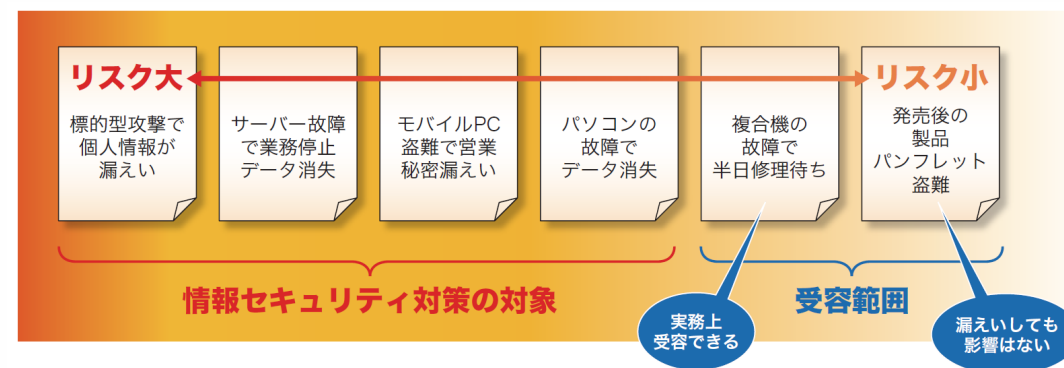
# (3) 情報セキュリティ規程の作成

## ① 対応すべきリスクの特定

- 経営者が避けたい重大事故から、対応すべきリスクを特定
  - 外部状況：法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など
  - 内部状況：経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など

## ② 対策の決定

- リスクが大きなもの優先して対策を実施
  - いつ事故が起きてもおかしくない
  - 事故が起きると大きな被害になるなど
- リスクな小さなものは許容するなど、合理的に対応
  - 事故が起きる可能性が小さい
  - 発生しても被害が軽微であるなど



## ③ 規程の作成

- 付録5「**情報セキュリティ関連規程 (サンプル)**」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

# 情報セキュリティ関連規程（サンプル）

	名称	概要
1	組織的管理策	<p>以下についてルールを定めます。</p> <ul style="list-style-type: none"> <li>✓ 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</li> <li>✓ 情報資産の管理や持ち出し方法、破棄</li> <li>✓ 情報資産に対するアクセス制御方針や認証</li> <li>✓ 業務委託にあたっての選定や契約、評価 ※委託先チェックリストのサンプルが付属</li> <li>✓ 情報セキュリティに関する事故対応や事業継続管理</li> </ul>
2	人的管理策	<p>以下についてルールを定めます。</p> <ul style="list-style-type: none"> <li>✓ 取締役及び従業員の責務や教育、人材育成</li> <li>✓ テレワークのセキュリティ対策</li> </ul>
3	物理的管理策	<p>以下についてルールを定めます。</p> <ul style="list-style-type: none"> <li>✓ 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</li> </ul>
4	技術的管理策	<p>以下についてルールを定めます。</p> <ul style="list-style-type: none"> <li>✓ IT機器やソフトウェアの利用、サーバーやネットワーク等のITインフラ</li> <li>✓ バックアップ、リストア手順</li> <li>✓ 独自に開発及び保守を行う情報システム</li> </ul>

# STEP3 本格的に取り組む (4) 資産管理

STEP1

STEP2

STEP3

STEP4

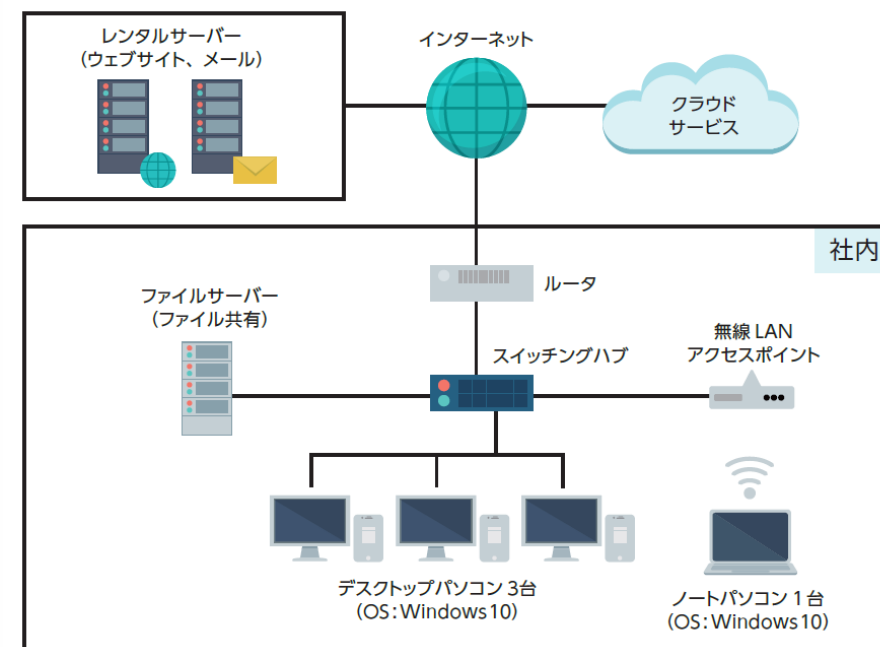


- 付録6「**資産管理台帳（サンプル）**」の「情報資産管理台帳」シートを活用して、自社の業務で利用している情報資産を把握

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	評価値				保存期限	登録日
						機密性	完全性	可用性	重要度		
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	3	1	1	3		2023/4/1
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	3	3	2	3	5年	2023/4/1
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	3	3	2	3	7年	2023/4/1
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類	2	2	2	2		2023/4/1
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	3	3	3	3		2023/4/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	可搬電子媒体	3	2	2	3		2023/4/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	モバイル機器	3	2	2	3		2023/4/1
営業	受注契約書	受注契約書原本（過去10年分）	営業部	営業部	書類	2	3	2	3		2023/4/1
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	社内サーバー	1	2	2	2		2023/4/1

# (5) 攻撃等の防衛

- 下記を参照して、必要な対策を検討・実施
  - IDアクセス制御
    - IDや認証の管理、重要な設備への入退室管理等の物理的対策
  - データセキュリティ
    - 暗号化や適切な保管、バックアップ
  - プラットフォームセキュリティ
    - 安全な構成の確立、端末やサーバーの基礎的な保護
    - ログの取得
  - 技術インフラの境界防護
    - 社内外ネットワークの分離と境界部分の防護
  - 意識向上とトレーニング
    - 適切な教育とルールの周知



# STEP3 本格的に取り組む (6) 攻撃等の検知

STEP1

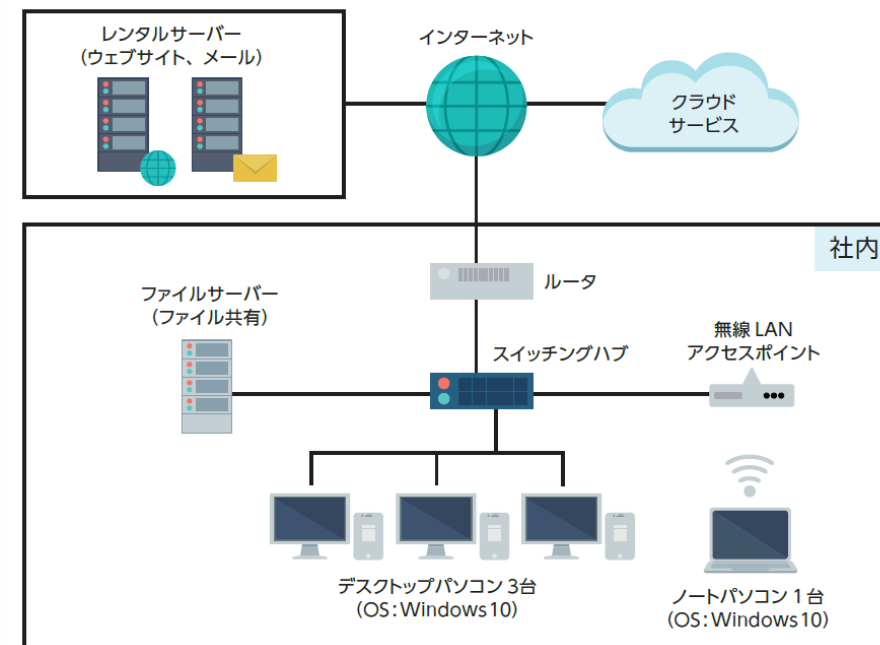
STEP2

STEP3

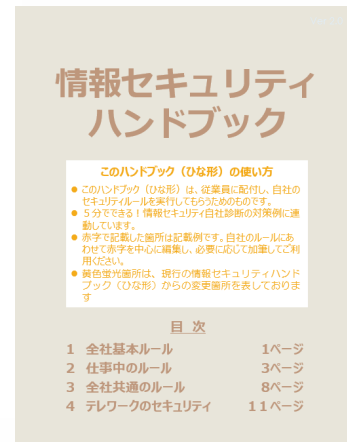
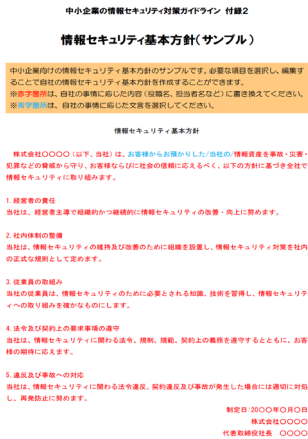
STEP4



- 下記を参照して、必要な対策を検討・実施
  - システムやネットワーク、機器の状態の監視・分析
    - ネットワーク接続及びデータ転送の監視
    - ハードウェア及びソフトウェアの状態及び挙動の監視



- 情報セキュリティ対策が本当に実行されているか、見落としていないか、対策がセキュリティ事故防止のために役に立っているか、等を確認
- 点検基準例
  - 1. 「情報セキュリティ6か条」「5分でできる！情報セキュリティ自社診断」
  - 2. 作成した情報セキュリティ対策に関するルール・規程



株式会社〇〇〇〇



## (8) インシデント対応体制等の整備

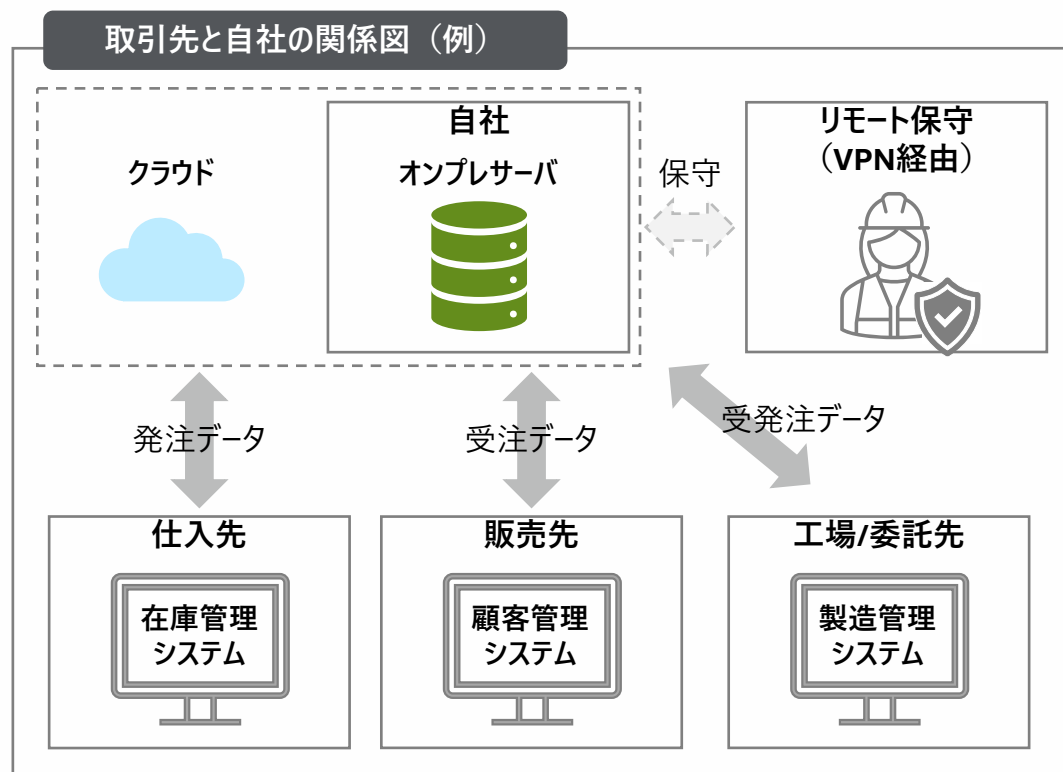
- インシデントの対象範囲とレベル、判定基準を定義
- インシデントへの対応手順や対応体制、復旧手順を規定

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

## STEP3 本格的に取り組む

## (9) 取引先/外部情報サービスの管理

- 取引先との関係、セキュリティ対策状況を把握
- 自社の機密情報を取り扱うクラウドサービスなどの外部サービスの利用状況、安全性を把握



# (10) 情報収集と共有

## ● 情報セキュリティに関する情報収集の方法、情報共有について説明

### ① 情報収集の方法

- 定常的に情報収集ができる方法を検討し、体制を整備
- 情報セキュリティの専門機関、セキュリティベンダーなどのメールマガジンやSNSに登録
- セミナーに参加して積極的な情報収集

### ② 組織内での共有

- 定期的な会議やメール配信、社内ポータルサイトを活用
- 情報セキュリティに関する最新情報のデータベースを構築

### ③ 情報共有の枠組み

- 取引先や同業者に対しても共有することで、対策の向上を図る
- 共有する情報に機密情報が含まれる可能性がある場合は、守秘義務契約を交わす
- 情報共有の枠組みとしては、日本シーサート協議会の他、業界別のISAC\*が組織されている場合がある

\* ISAC(Information Sharing and Analysis Center)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

# STEP4 より強固にするための方策

- 資産ベースのリスク分析を行い、各企業固有のリスクを把握
- リスク分析結果に応じて技術的対策をさらに強化
  - (1) 資産ベースのリスク分析
  - (2) 技術的対策例と活用
  - (3) セキュリティサービス例と活用
  - (4) ウェブサイトの情報セキュリティ
  - (5) クラウドサービスの情報セキュリティ
  - (6) テレワークの情報セキュリティ
  - (7) セキュリティインシデント対応

# (1) 資産ベースのリスク分析

- 付録6「**資産管理台帳（サンプル）**」の「リスク値算定」シートを活用した資産ベースのリスク分析の実施方法を説明

## 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

### ● 情報資産管理台帳の作成

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します。

● 情報資産ごとの機密性・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を踏まえて、評価値を記入します。

### ● 機密性・完全性・可用性の評価値から重要度を算定

重要度は、機密性、完全性、可用性いずれかの最大値で判断します。

## 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

情報資産の価値・事故の影響の大きさ	
重要度	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がねない
	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

起りやすさ	
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

## 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

### ① リスクを低減する

自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げる

### ② リスクを保有する

事故が発生しても許容できる、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、現状を維持する。

### ③ リスクを回避する

仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくす。

### ④ リスクを移転する

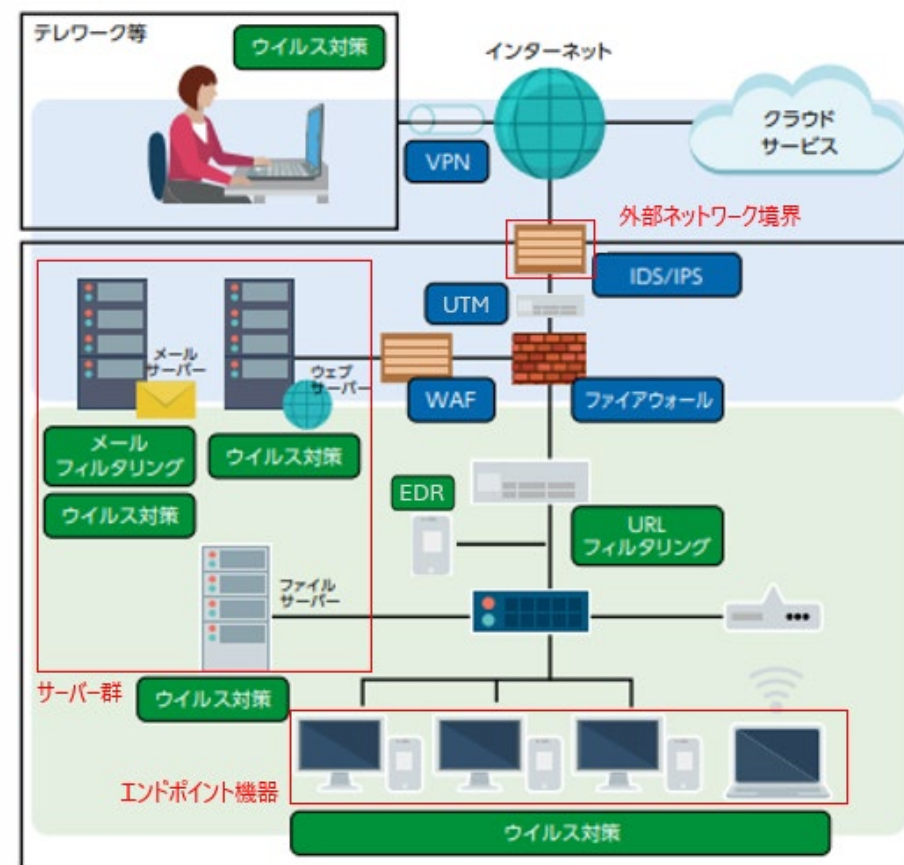
自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げる。

## STEP4 より強固にするための方策

## (2) 技術的対策例と活用

- コンピュータやインターネットを利用する際の技術的対策（製品やソフトウェア）を紹介

- ① ネットワーク脅威対策
- ② コンテンツセキュリティ対策
- ③ アクセス管理
- ④ システムセキュリティ管理
- ⑤ 暗号化
- ⑥ データの破棄



## (3) セキュリティサービス例と活用

- 外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施することが可能
- セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用
  - ① 情報セキュリティコンサルテーション
  - ② 情報セキュリティ教育サービス
  - ③ 情報セキュリティ監査サービス
  - ④ 脆弱性診断サービス
  - ⑤ デジタルフォレンジックサービス
  - ⑥ セキュリティ監視・運用サービス
  - ⑦ 機器検証サービス

## ● ウェブサイトを安全に構築し、運営するためのポイントを説明

### ウェブサイト 運営形態の検討

ウェブサイトでの運営形態によってセキュリティ対策が異なるため、自社の状態に見合った運営形態を検討しましょう。

### ウェブサイトの 構築

ウェブサイトの**技術的な脆弱性を認識**したうえで、必要なセキュリティ対策を設計・開発の段階から検討しましょう。

### ウェブサイトの 運営

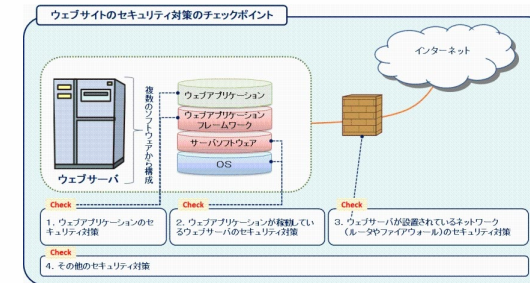
運用開始後に発覚した情報セキュリティ上の問題にも適切に対応し、ウェブサイトの安全性を維持向上しましょう。



ECサイト構築・運用  
セキュリティガイドライン



安全なウェブサイトの作り方



安全なウェブサイトの  
運用管理に  
向けての20ヶ条

技術的な解説については手引き・ガイドラインを紹介

# (5) クラウドサービスの情報セキュリティ

- クラウドサービスを安全に利用するためのポイントを説明

## クラウドサービスの 選定

クラウド化する業務によって重視すべきセキュリティ対策は異なるため、業務のセキュリティ要件に見合ったサービスを選定しましょう。

## クラウドサービスの 運用

クラウドサービスは提供者と利用者が連携して運用するため、その特性を理解して運用しましょう。

## クラウドサービスの セキュリティ対策

クラウドサービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。

付録7「**中小企業のためのクラウドサービス安全利用の手引き**」にて  
ポイント(チェックリスト)の各項目について解説



1	どの業務で利用するか明確にする	どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	取扱う情報の重要度を確認する	クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？
5	クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？
7	管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
9	利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
10	バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？
11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

# (6) テレワークの情報セキュリティ

- テレワークを安全に実施するためのポイントを説明

## テレワークの 方針検討

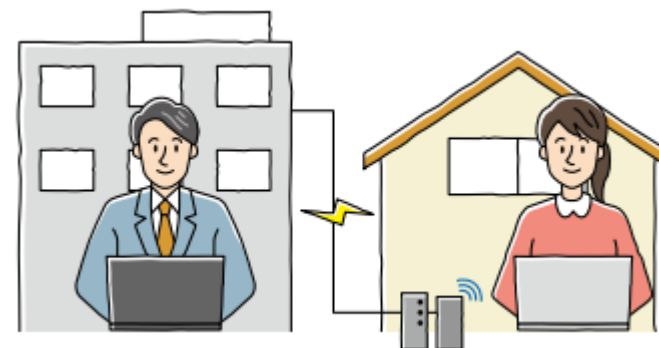
テレワークを行う際のシステム構成や機器をどうするか方針を検討しましょう。

## テレワークの セキュリティ対策

テレワークで利用するシステム構成や機器によって必要なセキュリティ対策を構築しましょう。

## テレワークの 運用

テレワークに関するルールを定め、テレワーク勤務者に周知し、事故に気をつけて安全に運用しましょう。



# (7) セキュリティインシデント対応

- セキュリティインシデント発生時の対応に関するポイントを説明

## 検知・初動対応

インシデントを検知した場合は、速やかに情報セキュリティ責任者へ連絡し、被害を拡大させないための初動対応を行います。

## 報告・公表

顧客や関係者、行政機関、一般・メディア等に対して、必要な場合は適時の報告や情報公開を行います。

## 復旧・再発防止

システム管理者や外部専門組織と協力して、迅速な復旧作業や根本的な再発防止策を検討しましょう。

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**」にて対応方法の詳細や相談・報告先などを解説



# (参考) 本ガイドラインと中小企業施策の関係性

対応の指針



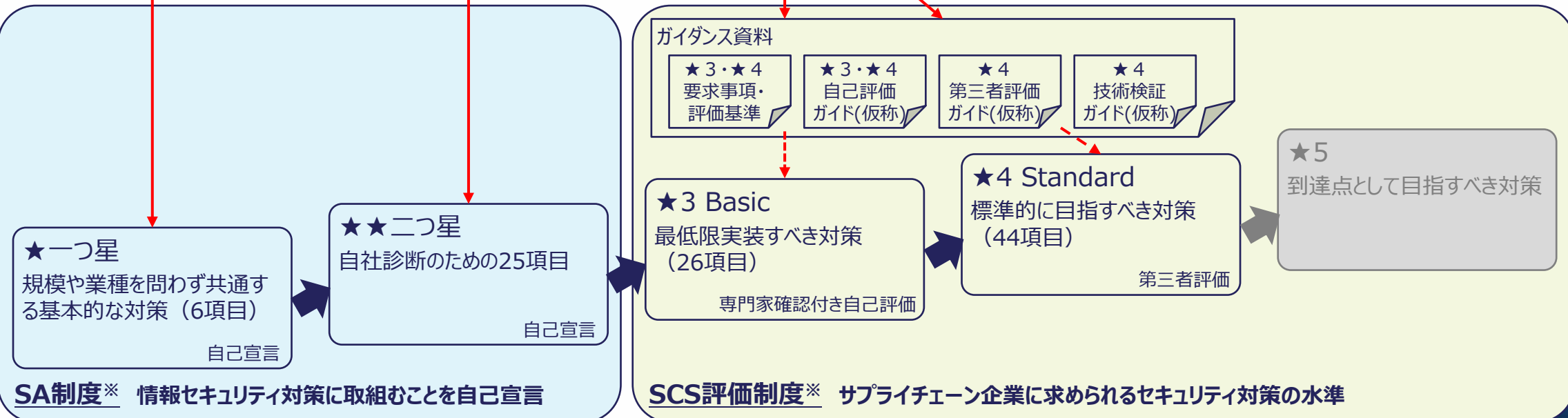
対応状況の可視化・評価

## 中小企業の情報セキュリティ対策ガイドライン 情報セキュリティ対策に取り組む際の指針



【凡例】

- ↔ 制度⇔ガイドライン間の対応関係
- ↔ 制度/ガイドライン内の対応関係



※SECURITY ACTION制度

※サプライチェーン強化に向けたセキュリティ対策評価制度

IPA