

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

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
- 「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」を追加
- 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
 - 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
 - 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



第3.1版の主な変更点

● 第1部 経営者編

- 関連法令を最新の内容に見直し

● 第2部 実践編

- テレワークの情報セキュリティに関する解説を追加
- セキュリティインシデント対応に関する解説を追加

● 付録

- 付録1「情報セキュリティ5か条」、付録3「5分でできる！情報セキュリティ自社診断」の対策例を見直し
- 付録4「情報セキュリティハンドブック（ひな形）」、付録5「情報セキュリティ関連規程（サンプル）」にテレワークの情報セキュリティに関するひな形、サンプルを追加
- 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」を追加

● 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



経営者



責任者・担当者

ガイドラインの構成

- 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

	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。
	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規則を文書化したもののサンプルです。
	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 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

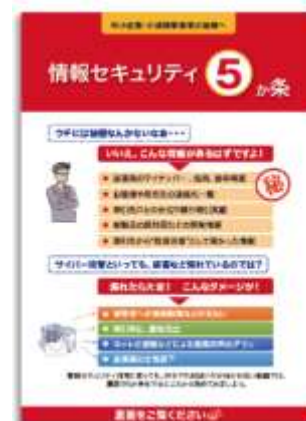
取組 5 緊急時の対応や復旧のための体制を整備する

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

● できるところから始めて段階的にステップアップ

取組状況とアクション	本ガイドラインの活用方法
<p>Step1 まず始めましょう</p>	<p>これまで情報セキュリティ対策を特に意識していない場合は「2. できるところから始める」(P.19)を参照して、「情報セキュリティ5か条」を実行してください。</p> <p>進め方 「情報セキュリティ5か条」を社内で配付するなど、まずできるところから開始してください。</p>
<p>Step2 現状を知り改善しましょう</p>	<p>Step1は実施できていて次に進める場合は「3. 組織的な取り組みを開始する」(P.20)を参照して、「5分でする! 情報セキュリティ自社診断」で自社の状況を把握し、できていない対策の実行に努めてください。</p> <p>進め方 ・「情報セキュリティ基本方針(サンプル)」を参考に基本方針を作成してください。 ・「5分でする! 情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。 ・「情報セキュリティハンドブック(ひな形)」を参考に具体的な対策を定めて従業員に周知してください。</p>
<p>Step3 本格的に取り組みましょう</p>	<p>Step2までは実施できていて次に進める場合は「4. 本格的に取り組み」(P.24)を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。</p> <p>進め方 ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程(サンプル)」を参考に規程を作成してください。 ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。</p>
<p>Step4 改善を続けましょう</p>	<p>「5. より強固にするための方策」(P.32)を参照して、自社に必要な対策を追加実施してください。Step1やStep2に取り組んでいる企業でも、Step4を参照して必要な対策があれば実行してください。</p>



情報セキュリティ5か条



5分でする!
情報セキュリティ自社診断



情報セキュリティ関連規程

- ・ 情報収集と共有
- ・ ウェブサイトの情報セキュリティ
- ・ クラウドサービスの情報セキュリティ
- ・ テレワークの情報セキュリティ
- ・ セキュリティインシデント対応
- ・ セキュリティサービス例と活用
- ・ 技術的対策例と活用
- ・ 詳細リスク分析の実施方法

Step1 できるところから始める 情報セキュリティ5か条

● 付録1「情報セキュリティ5か条」を守るところから始めてみましょう

- ① OSやソフトウェアは常に最新の状態にしよう！
- ② ウイルス対策ソフトを導入しよう！
- ③ パスワードを強化しよう！
- ④ 共有設定を見直そう！
- ⑤ 脅威や攻撃の手口を知ろう！

中小企業・小規模事業者の皆様へ

情報セキュリティ 5 か条

ウチには秘密なんかないなあ・・・

いいえ、こんな情報があるはずですよ！

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り種や取引実績
- 新製品の設計図などの開発情報
- 取引先から「取扱注意」として預かった情報

サイバー攻撃といっても、被害など知れているのでは？

漏れたら大変！ こんなダメージが！

- 顧客への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遅延などによる業務効率のダウン
- 従業員の上乗指下

情報セキュリティ対策と言っても、何をすれば良いのかわからない組織では、優先順位から守るところから始めてみましょう。

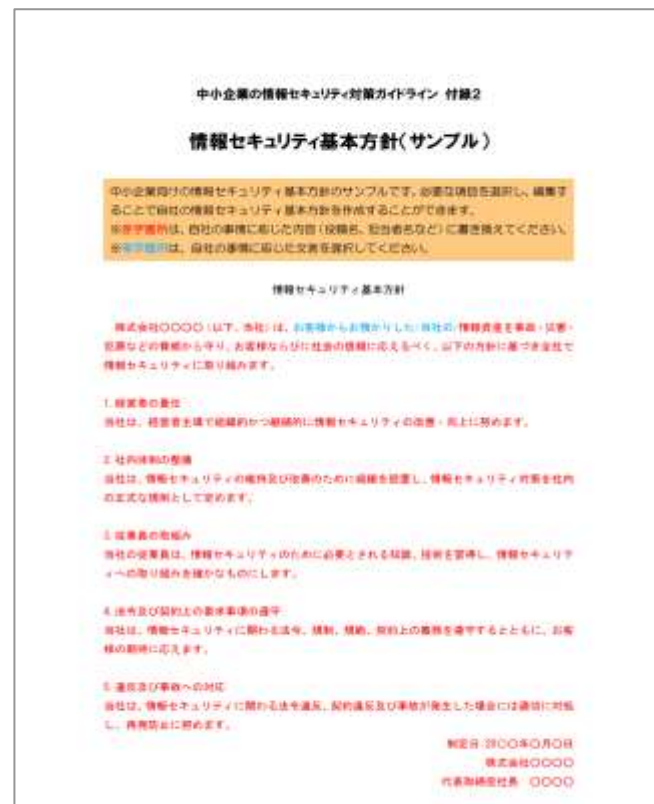
裏面をご覧ください。

(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）**」を参考に作成

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



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」診断編を活用
 - **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 5項目
 - 従業員としての対策 13項目
 - 組織としての対策 7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
 - 付録の**情報セキュリティハンドブック**を活用すると従業員に対する社内ルールの周知が簡単にできる



5分でできる！情報セキュリティ自社診断 診断項目



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	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？
	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	関係者以外の事務所への立ち入りを制限していますか？
	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	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？
	4	重要情報に対する適切なアクセス制限を行っていますか？		17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	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？		18	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？
従業員としての対策	6	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	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	7	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？		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	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？		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	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？		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	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？		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	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？		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？			

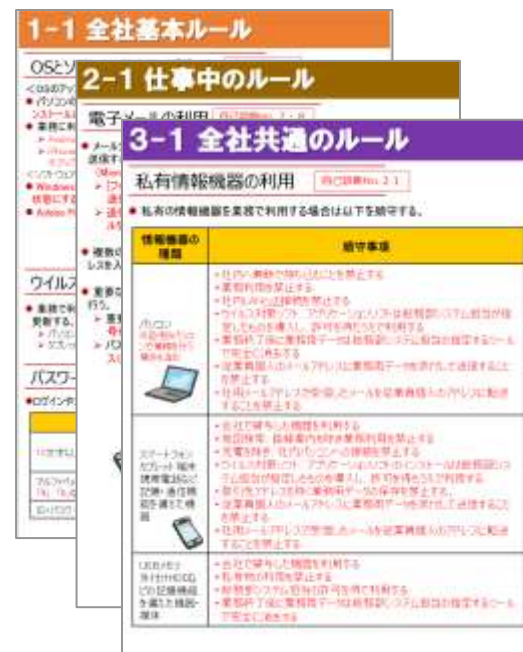
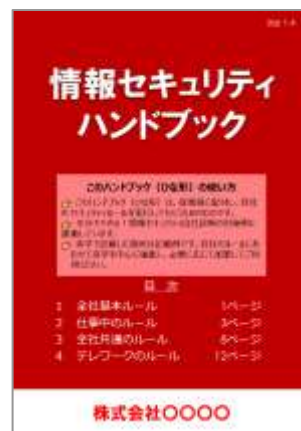
Step2 組織的な取り組みを開始する (3) 対策の決定と周知

- 付録3「5分でできる！情報セキュリティ自社診断」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）」



Step3 本格的に取り組む (1) 管理体制の構築

- 情報セキュリティ対策を推進するための管理体制を決定
- 付録5「**情報セキュリティ関連規程**」を活用して自社の管理体制を社内に周知

【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)

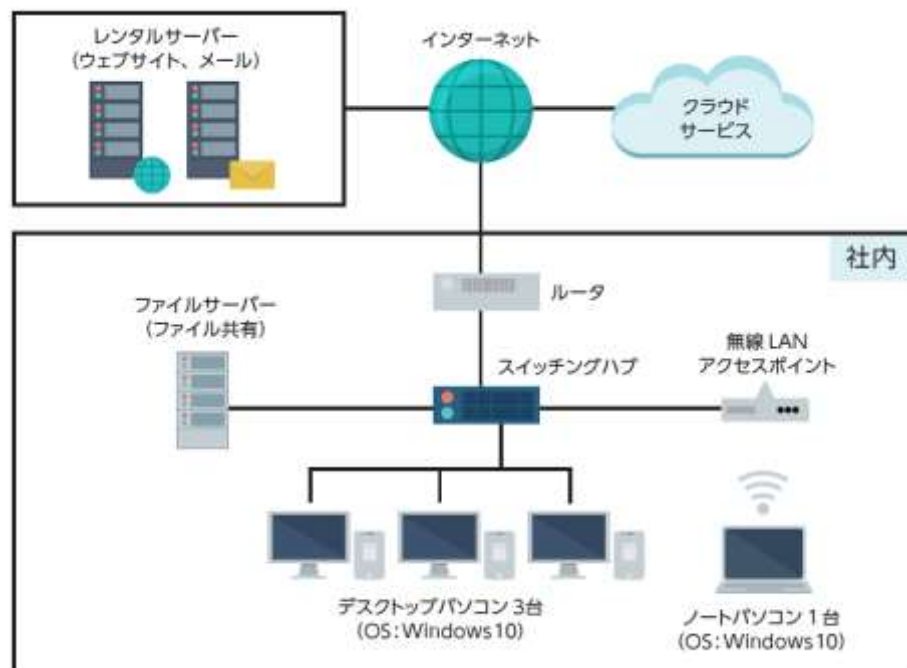
役職名	役割と責任
情報セキュリティ責任者 (例：代表取締役)	事故の影響を判断し、対応について意思決定する。
情報セキュリティ部門責任者 (例：管理部長、営業部長)	<ul style="list-style-type: none"> 事故の原因を調べて情報セキュリティ責任者に報告する。 情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行う。 事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行う。
システム管理者 (例：管理部長兼務)	事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行う。
事故・異常を発見した従業員	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。

社内規程



(2) デジタルトランスフォーメーション (DX) の推進と 情報セキュリティの予算化

- 自社の情報システムについて、インターネットとの接続状況を把握
- 情報セキュリティ対策を検討して**予算を確保**



テレワークを導入するにあたり・・・
クラウドのセキュリティ確認
リモート接続のセキュリティ確保
利用者認証の強化



DX (Digital Transformation)

企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

(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
- リスクが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

- 「情報セキュリティ管理規程（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）の概要



	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 対応ならびに事業継続管理	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。

Step3 本格的に取り組む

(4) 委託時の対策

- 契約書や覚書に具体的な対策を明記
- 個別に契約や覚書を交わすことができる場合は、委託先のサービス規約や情報セキュリティ方針を確認
- 個人情報保護法では、個人データの取り扱いを委託する場合は、必要かつ適切な監督の実行

付録5 情報セキュリティ関連規程（サンプル）

9-1 業務委託契約に係る機密保持条項

注：このサンプルは、業務委託契約書における機密保持に関する条項を示すものです。委託元（甲）と委託先（乙）との両方が、相手から機密として提供される情報の守秘義務を負う双務契約の形式としています。



Step3 本格的に取り組む (5) 点検と改善

- 情報セキュリティ対策が本当に実行されているか、見落としている対策はないか、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
- 点検の基準例
 - その1) 「情報セキュリティ5か条」「5分でできる！情報セキュリティ自社診断」
 - その2) 情報セキュリティ対策に関するルール・規程



より強固にするための方策

- より強固な情報セキュリティ対策に取り組むために、以下の8つの区分について説明情報収集と共有
 - (1) ウェブサイトの情報セキュリティ
 - (2) クラウドサービスの情報セキュリティ
 - (3) テレワークの情報セキュリティ
 - (4) セキュリティインシデント対応
 - (5) セキュリティサービス例と活用
 - (6) 技術的対策例と活用
 - (7) 詳細リスク分析の実施方法

Step4 より強固にするための方策

(1) 情報収集と共有

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ソーシャルメディアに登録
 - セミナーに参加して積極的な情報収集

② 情報共有の枠組み

- 収集した情報は社内の関係者だけではなく、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

(2) ウェブサイトの情報セキュリティ

- ウェブサイトの**運営形態の検討**から**構築**、実際に**運営**するまでの3つの段階に分けて検討事項を説明

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。

インターネット



(3) クラウドサービスの情報セキュリティ

- クラウドサービスの**選定**から**運用**までのセキュリティ対策を3つの段階に分けて検討事項を説明

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



(4) テレワークの情報セキュリティ

- テレワークの情報セキュリティ対策の検討・実施・運用までの進め方について3つの段階に分けて検討事項を説明

テレワークの 方針検討

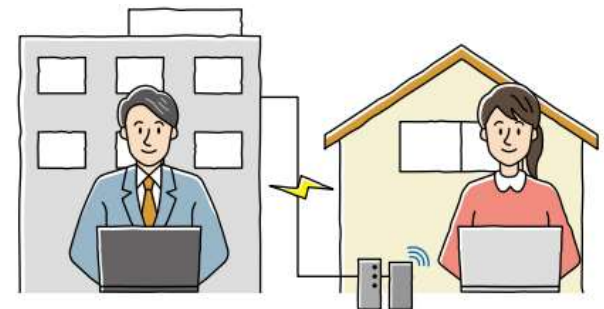
テレワークを行う際のシステム構成や機器をどうするか方針を検討しましょう。

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。



(5) 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対応について3つの実施項目に分けて検討事項を説明

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きましょう。

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きましょう。

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。

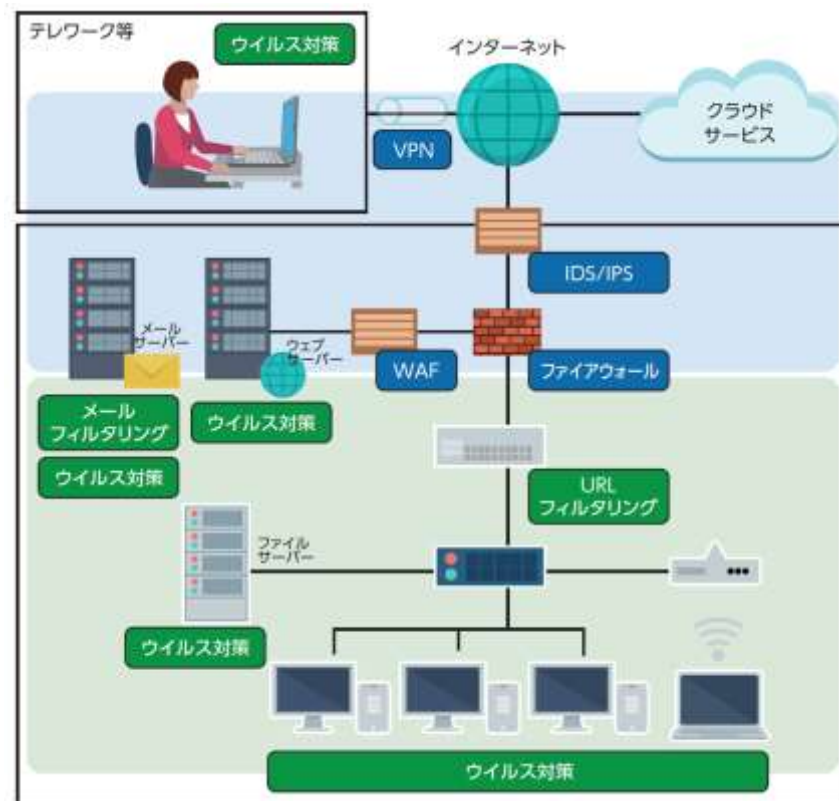
- 付録8「中小企業のためのセキュリティインシデント対応の手引き」を参照のうえインシデント対応を実施
インシデント対応マニュアルの策定にも活用可能！



(6) 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ときに施す技術的対策（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



(7) 情報セキュリティサービスの活用

- 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
- 情報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

(8) 詳細リスク分析の実施方法

- 付録6「リスク分析シート」を使い、以下の手順で行う。

手順 1
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

手順 2
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

手順 3
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

● 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。

情報資産の価値・事故の影響の大きさ	
重要度	3 事故が起ると、 ● 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 など事業の存続を左右しない 2 事故が企業の本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	
算定のしかたは表17参照	
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)
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
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)
	1 低 通常の状況で被害が発生することはない
リスク値	9~8 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中
	3~1 小 軽微な事故が起きる可能性小

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。