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

IPA Better Life with IT

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
- 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

第3.1版の主な変更点について

- **第1部　経営者編**
  - 関連法令や被害事例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」の対策例を最新の内容に見直し
  - 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

ガイドラインの対象

- **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

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、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。

第1部　経営者編

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」

(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。

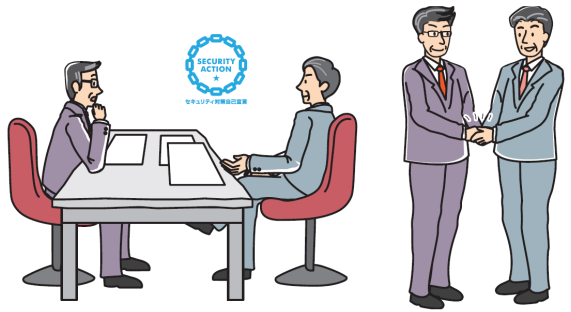
原則 1 情報セキュリティ対策は経営者のリーダーシップで進める

- 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」

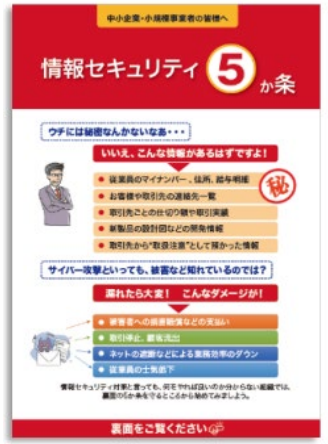
- 経営者は、以下の7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

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

取組状況とアクション	本ガイドラインの活用方法
Step1 まず始めましょう	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。 **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。
Step2 現状を知り改善しましょう	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 分でできる！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。 **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 分でできる！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。
Step3 本格的に取り組みましょう	Step2 までは実施できていて次に進める場合は **「4. 本格的に取り組む」**(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。 **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。
Step4 改善を続けましょう	**「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。



情報セキュリティ 5 か条

情報セキュリティ関連規程

5分でできる！
情報セキュリティ自社診断

- 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

(1) 情報セキュリティ5か条

- 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！

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。

② 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。

③ 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。

④ 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ために、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。

⑤ 脅威や攻撃の手口を知ろう！

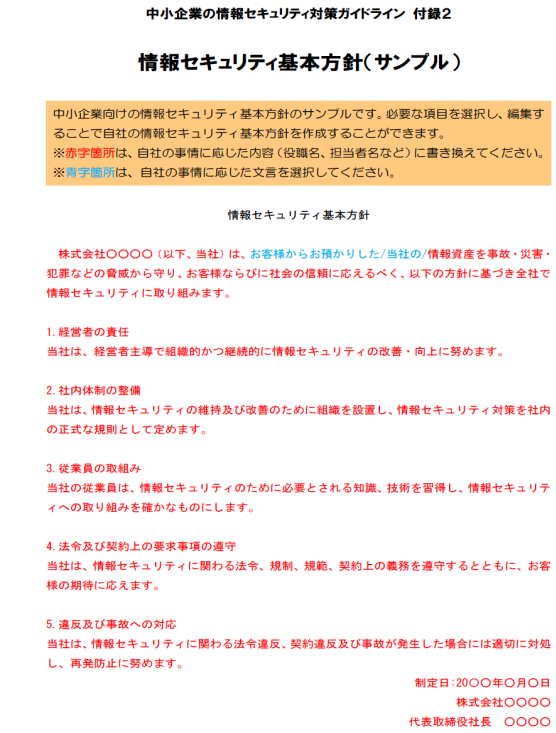
取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする
巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

(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

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。
※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。

1. 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。

2. 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の正式な規則として定めます。

3. 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します。

4. 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。

5. 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

(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　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

診断項目	No	診断内容
Part 1 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？
	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？
	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	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？
	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？
Part 2 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？
	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？
	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？
	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？
	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？
	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？
	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	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？
	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？
	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？
	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？
	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？
Part 3 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？
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？
	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等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？

付録４

5分でできる！情報セキュリティ自社診断

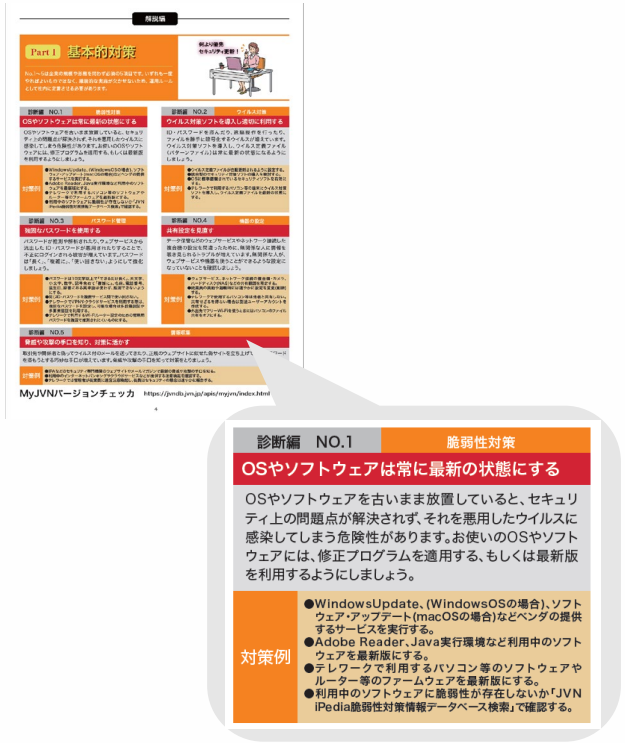
基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルは最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報に対する適切なアクセス制限を行っていますか？
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？
従業員としての対策	6	電子メールの添付ファイルや本文中の URLリンクを介したウイルス感染に気をつけていますか？
	7	電子メールや FAX の宛先の送信ミスを防ぐ取り組みを実施していますか？
	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？
	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？
	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？
	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？
	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？
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？
	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？
	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？
	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？
	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	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？
	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？
	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？

Step2 組織的な取り組みを開始する

(3) 対策の決定と周知

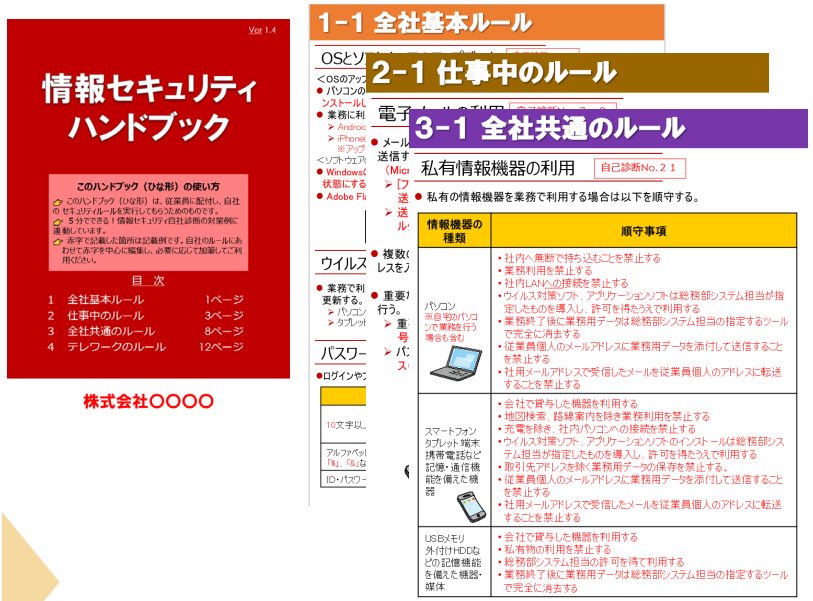
- 自社診断で問題があった項目は、解説編を参考に対策を決定
- 付録4「情報セキュリティハンドブック（ひな形）」を編集して社内周知

付録3「5分でできる！情報セキュリティ自社診断」



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）」



「情報セキュリティハンドブック」を編集
社内周知

(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）	・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。

1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

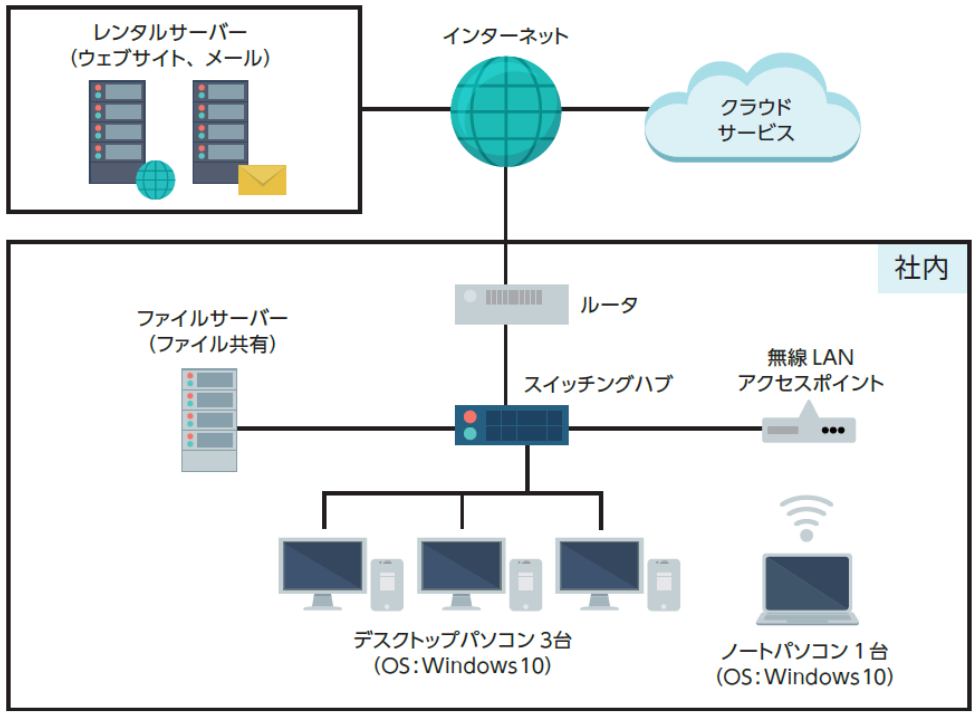
役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
情報システム管理者	情報セキュリティ対策のためのシステム管理を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者	事故の影響を判断し、対応について意思決定する。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。
特定個人情報事務取扱責任者	特定個人情報の情報セキュリティに関する責任者。
特定個人情報事務取扱担当者	特定個人情報を取り扱う事務に従事する従業員。
個人情報苦情対応責任者	個人情報に関する苦情の対応責任者。

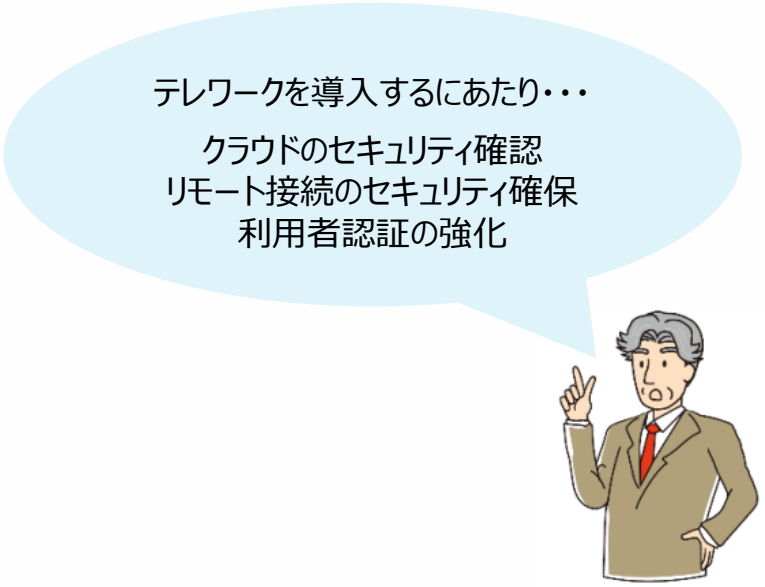
＜情報セキュリティ委員会体制図＞

1

(2) 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





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を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

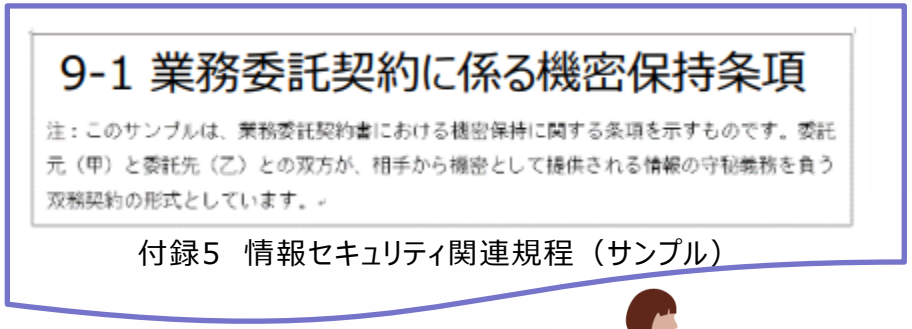
- 付録５「情報セキュリティ関連規程（サンプル）」を参考に、自社に適した規程にするために修正を加える
  - サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成
  - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記

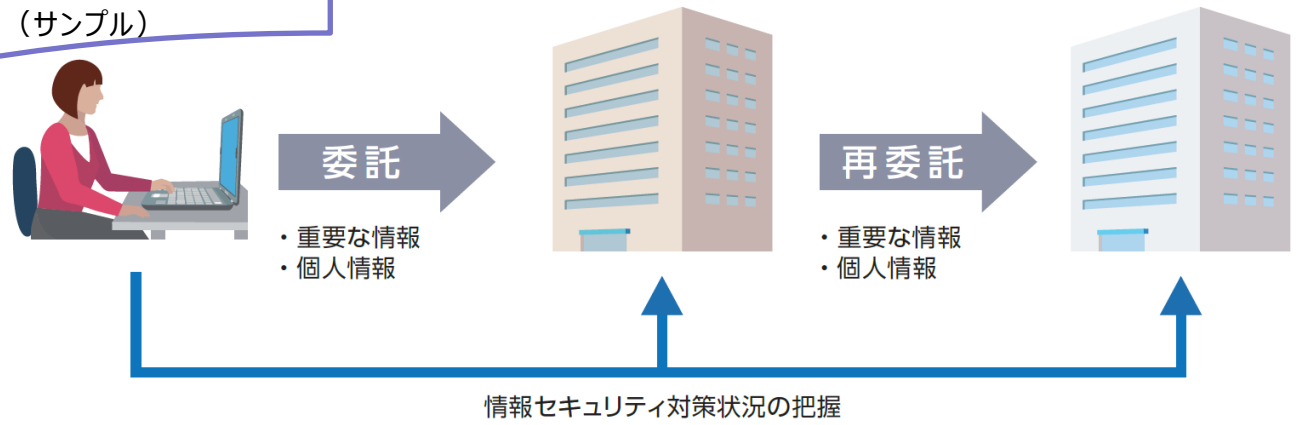
付録５
情報セキュリティ関連規程（サンプル）

	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限方針や認証のルールを定めます。
5	物理的対策	セキュリティ領域の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	システムの開発及び保守	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。業務委託契約書の機密保持に関する条項例と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決めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。
12	テレワークにおける対策	テレワークにおけるセキュリティに関するルールを定めます。

(4) 委託時の対策

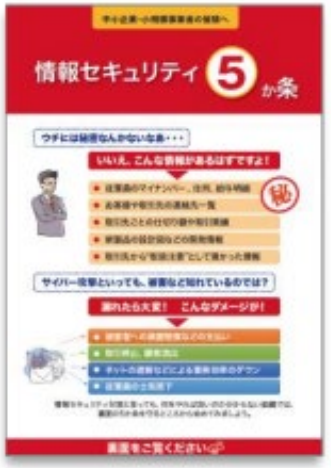
- 契約書や覚書に具体的な対策を明記
- 個別に契約や覚書を交わすことができる場合は、委託先のサービス規約や情報セキュリティ方針を確認
- 個人情報保護法では、個人データの取り扱いを委託する場合は、必要かつ適切な監督の実行





(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



Step4 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

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

(1) 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と情報共有の枠組みについて説明

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

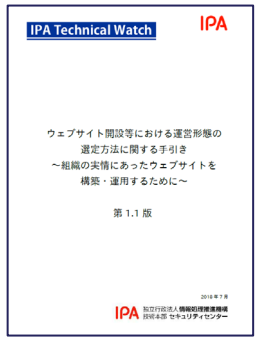
ウェブサイトでの運営形態によってセキュリティ対策が異なるため、**自社の状態に見合った運営形態**を検討しましょう。

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。

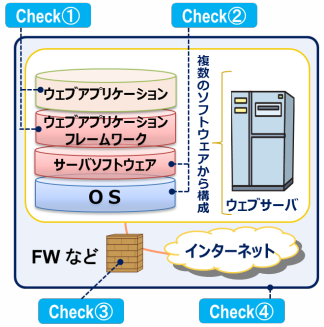
ウェブサイト の運営

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。



ウェブサイト開設等における運営形態の選定方法に関する手引き

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

(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。

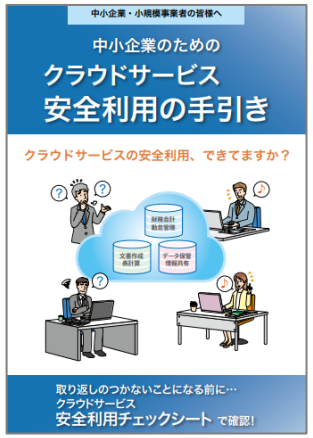
クラウドサービスの運用

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」にて
ポイント(チェックリスト)の各項目について解説



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

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？

(4) 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

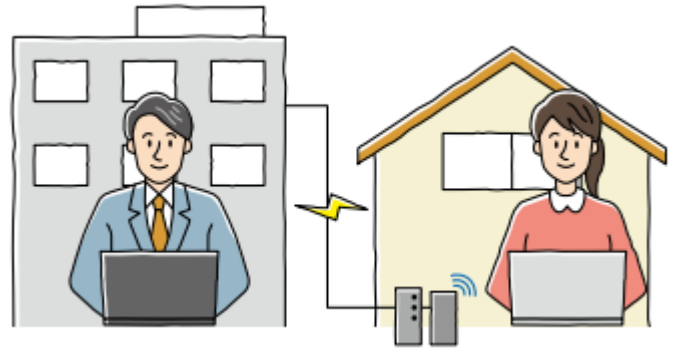
テレワークを行う際のシステム構成や機器をどうするか方針を検討しましょう。

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。



(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いましょう。

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」にて
対応方法の詳細や相談・報告先などを解説

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手引き

- インシデント発生時の対応について、「検知・初動対応」「報告・公表」「復旧・再発防止」の３つの段階に分けて検討事項を説明
- インシデント対応時に整理しておくべき事項や相談窓口・報告先などを紹介

ステップ１
検知・初動対応
- 検知と連絡受付
- 対応体制の構築
- 初動対応

ステップ２
報告・公表
- 第一報
- 最終報・第二報以降

ステップ３
復旧・再発防止
- 対応・調査
- 証拠保全
- 復旧
- 再発防止

(6) セキュリティサービス例と活用

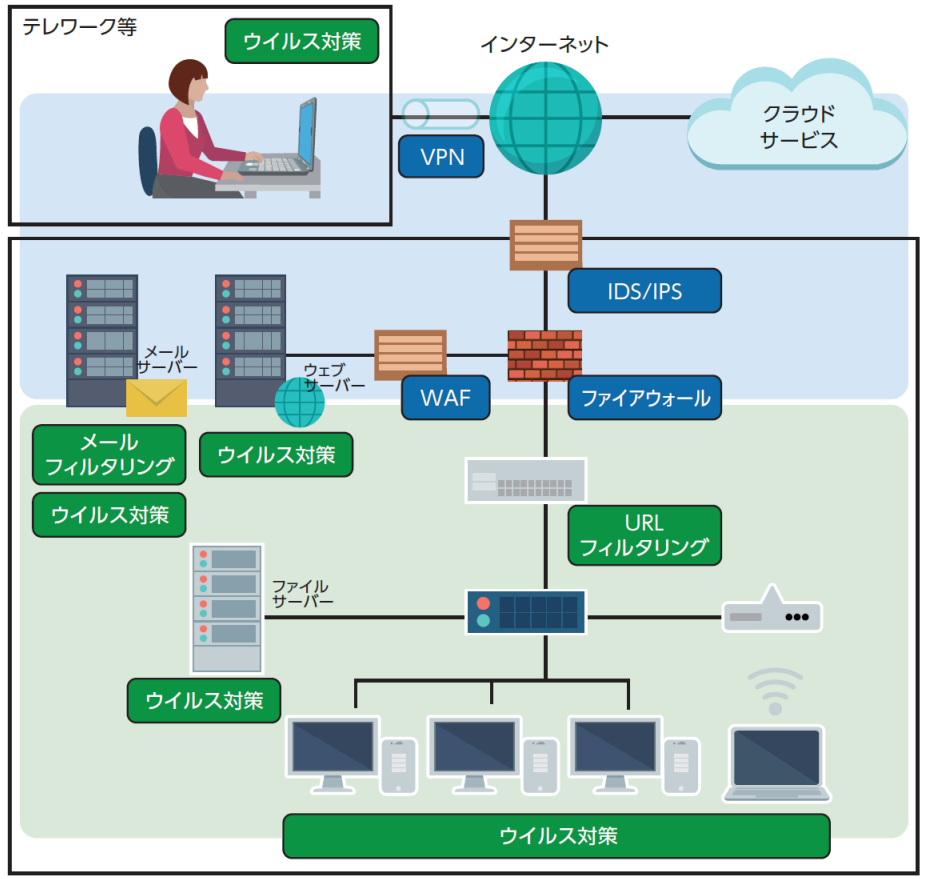
- 外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施することが可能
- セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用

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) 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



(8) 詳細リスク分析の実施方法

- 付録７「リスク分析シート」を活用した詳細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

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

●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。

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

算定のしかたは表17参照

		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
脆弱性		つけ込みやすさ
	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

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。