中小企業が取り組むべき
サイバーセキュリティの基本

2025年11月27日

独立行政法人情報処理推進機構
セキュリティセンター　普及啓発・振興部　普及啓発グループ
篠嶋 秀雄

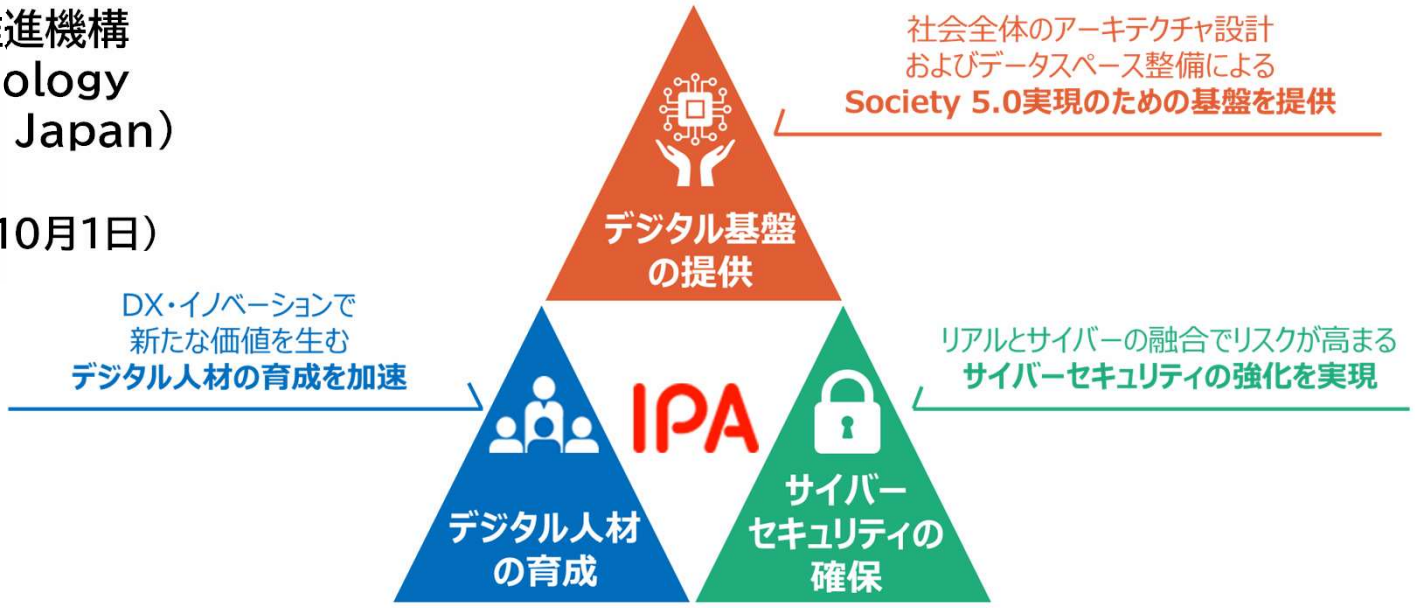
IPA Better Life with IT

独立行政法人情報処理推進機構（IPA）について

日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人。
誰もが安心してITのメリットを実感できる「**頼れるIT社会**」の実現を目指しています。

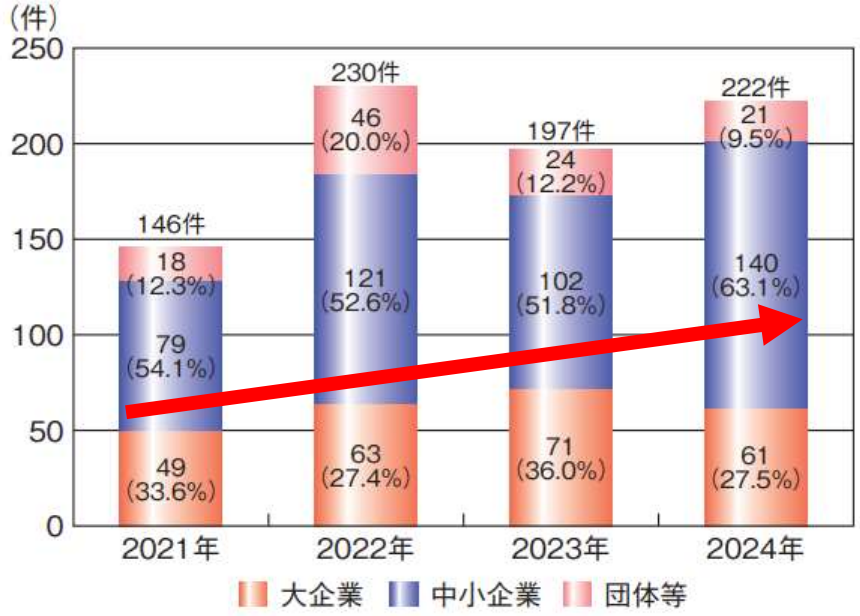
「人材」、「セキュリティ」、「デジタル基盤」の3つの中核事業

■名称: 独立行政法人情報処理推進機構
（Information-technology Promotion Agency, Japan）
■設立: 2004年1月5日
（前身母体の設立は1970年10月1日）
■理事長: 齊藤 裕



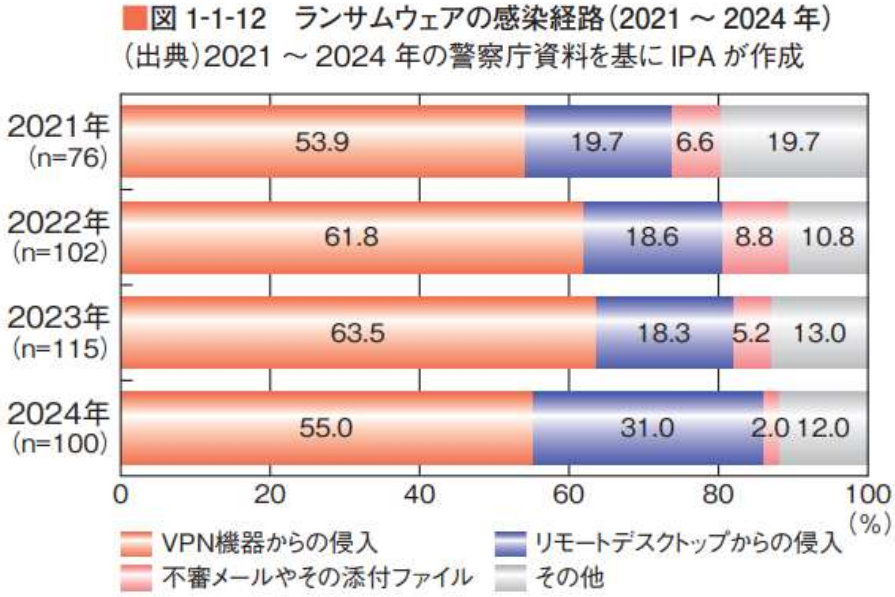
国内における情報セキュリティインシデント状況
情報セキュリティ白書　2025より抜粋

ランサムウェアによる被害



■図 1-1-11　国内のランサムウェアによる被害件数(2021 ～ 2024 年)
(出典)2021 ～ 2024 年の警察庁資料を基に IPA が作成

・国内のランサムウェアによる被害件数は、**前年比 12.7%増**
・企業・団体等の規模別で見ると、**2024年は中小企業の被害件数が増加**



■図 1-1-12　ランサムウェアの感染経路(2021 ～ 2024 年)
(出典)2021 ～ 2024 年の警察庁資料を基に IPA が作成

・2024年のランサムウェアの感染経路としては、有効回答100件のうち**「VPN機器からの侵入」が31.0%**・**テレワーク等で利用される機器からの侵入が8割**を超えている

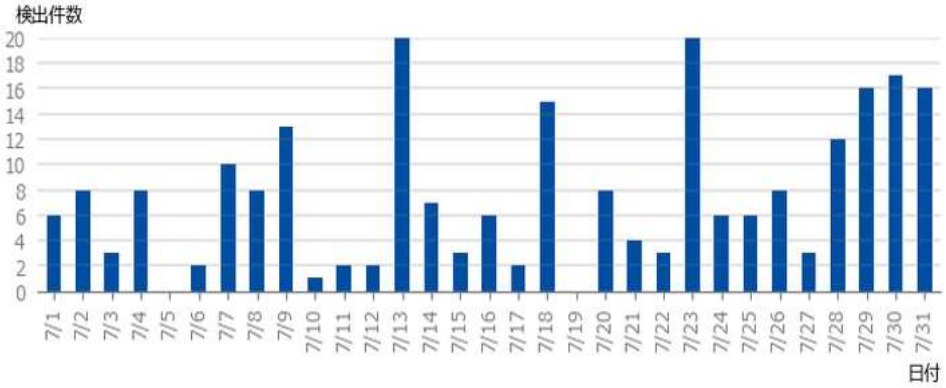
国内における情報セキュリティインシデント状況
フィッシングによる被害/DDoSによる被害

フィッシングによる被害

出典 フィッシング対策協議会 2025/09 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202509.html

・2025年9月にフィッシング対策協議会に寄せられた、フィッシング報告件数は、224,693件。
2025年8月と比較すると31,360件、約16.2%増加

DDoS攻撃による被害



出典 wizSafe Security Signal 2025年7月 観測レポート
図-1 DDoS攻撃の検出件数(2025年7月)
https://wizsafe.iij.ad.jp/2025/08/1957/

・今回の対象期間で検出したDDoS攻撃の総攻撃検出件数は、235件であり、1日あたりの平均件数は7.58件でした。

中小企業が取り組むべきサイバーセキュリティの基本

情報セキュリティ対策の基本

・多数の脅威があるが 「攻撃の糸口」 は似通っている
・基本的な対策の重要性は長年変わらない
・「情報セキュリティ対策の基本」は常に意識

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	**ソフトウェアの更新**	脆弱性を解消し攻撃による リスクを低減する
ウイルス感染	**セキュリティソフトの利用**	攻撃をブロックする
パスワード窃取	**パスワードの管理・認証の強化**	パスワード窃取による リスクを低減する
設定不備	**設定の見直し**	誤った設定を攻撃に利用 されないようにする
誘導(罠にはめる)	**脅威・手口を知る**	手口から重要視するべき 対策を理解する

IPAが提供する対策実践のためのツール、制度

平時の備えから、インシデントが発生してしまった後の対応・復旧支援まで

・情報セキュリティの考え方や段階的に実現する為の方策を紹介する「中小企業の情報セキュリティ対策ガイドライン」。
・ガイドラインをベースに、セキュリティ対策への意識を持つための自己宣言「SECURITY ACTION」。
・常時サイバー環境を監視しつつ、インシデントが発生してしまったが対処方法がわからない、
この様な中小企業の事後対応を支援し、また簡易サイバー保険を付帯した「サイバーセキュリティお助け隊」

平時の対策支援（社内体制整備、意識向上）

中小企業情報セキュリティ対策ガイドライン

中小企業におけるセキュリティ対策の考え方、具体的方策を紹介。

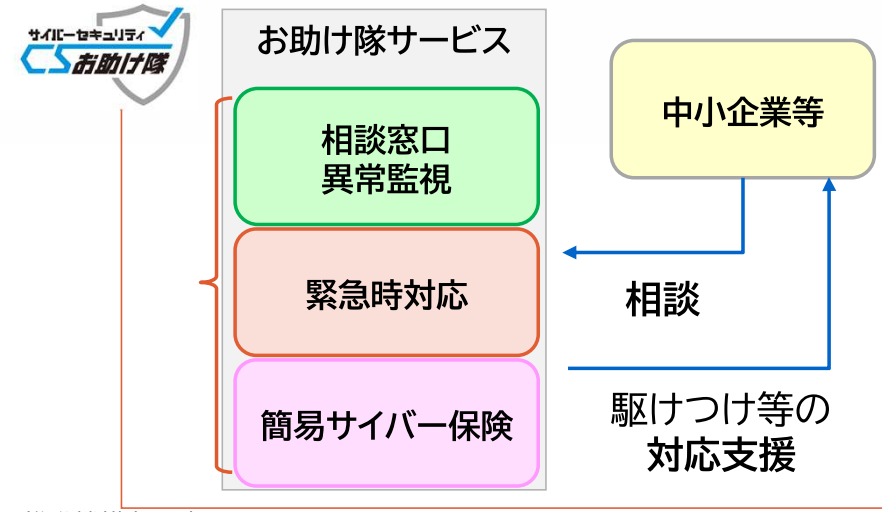
SECURITY ACTION

セキュリティ対策に取組むことを事業者が自己宣言する制度。

有事の対策支援（検知、対応、復旧等）

サイバーセキュリティお助け隊

中小企業等がサイバー攻撃等で困った時の相談窓口、駆けつけ支援体制を構築。



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

https://www.ipa.go.jp/security/guide/sme/about.html

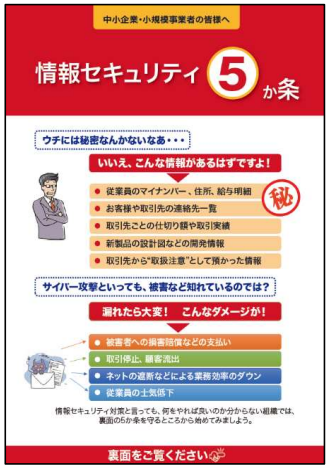
IPA

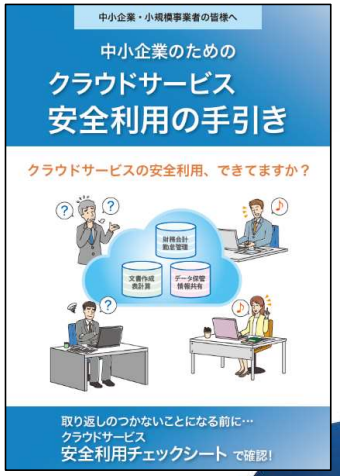
- 中小企業の経営者や実務担当者が、情報セキュリティ**対策の必要性**を理解し、**情報を安全に管理**するための具体的な手順等を示したガイドライン

- 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
  - 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
  - **「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

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
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。





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
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」

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のリーダシップで進める

- 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

経営者は何をやらなければならないのか
（2）実行すべき「重要7項目の取組」

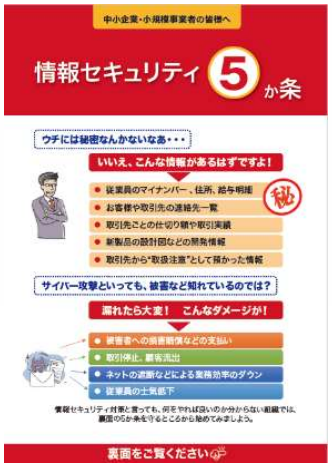
経営者は、以下の7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

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	情報セキィリティに関する最新動向を収集する

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
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

Step1
できるところから始める



情報セキュリティ5か条

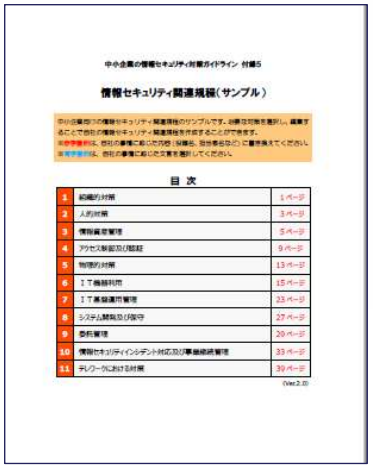
SECURITY ACTION ★一つ星を宣言

Step2
組織的な取り組みを開始する

5分でできる！
情報セキュリティ自社診断

SECURITY ACTION ★★二つ星を宣言

Step3
本格的に取り組む



情報セキュリティ関連規程

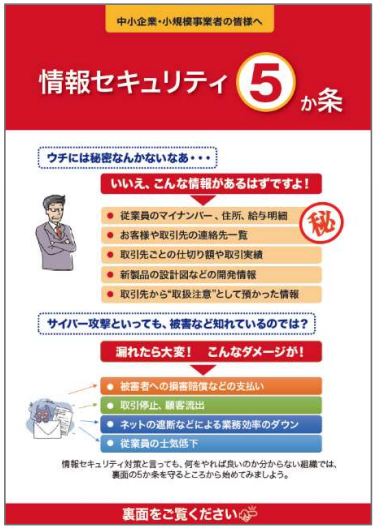
Step4
より強固にするための方策

(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)情報セキュリティサービスの活用
(7)技術的対策例と活用
(8)詳細リスク分析の実施方法

より強固にするため方策

Step1 できるところから始める
(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！

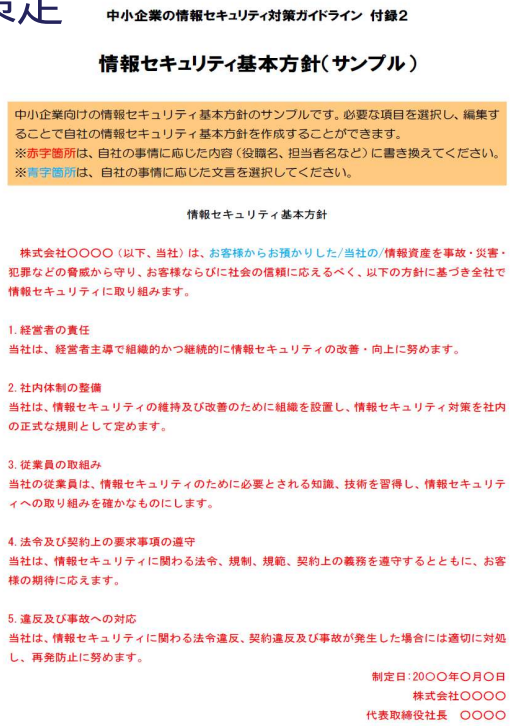
取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

Step2 組織的な取り組みを開始する
(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○○○○(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○○年○月○日
株式会社○○○○
代表取締役社長　○○○○

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　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

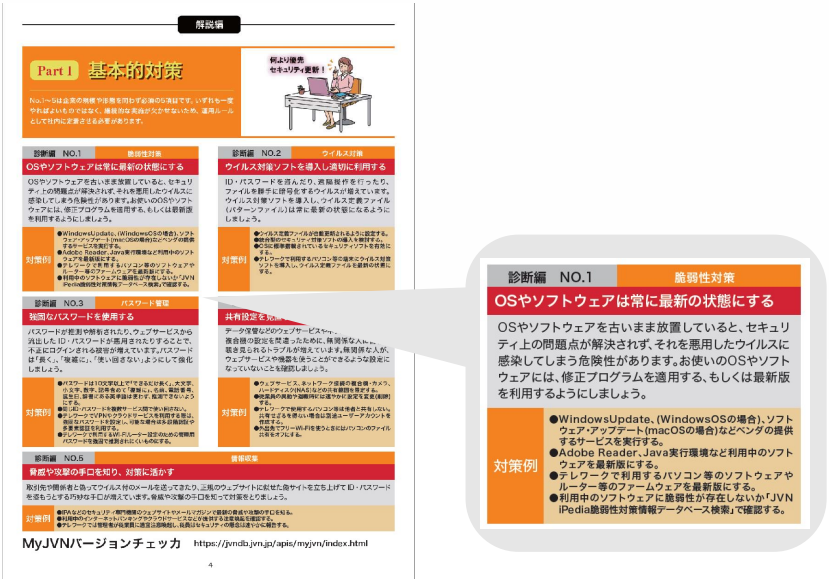
診断項目	No	診断内容	チェック			
			実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？	4	2	0	−1
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1 は最新の状態にしていますか？	4	2	0	−1
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	−1
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	−1
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	−1
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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1
	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？	4	2	0	−1

3

Step2　組織的な取り組みを開始する
（3）対策の決定と周知

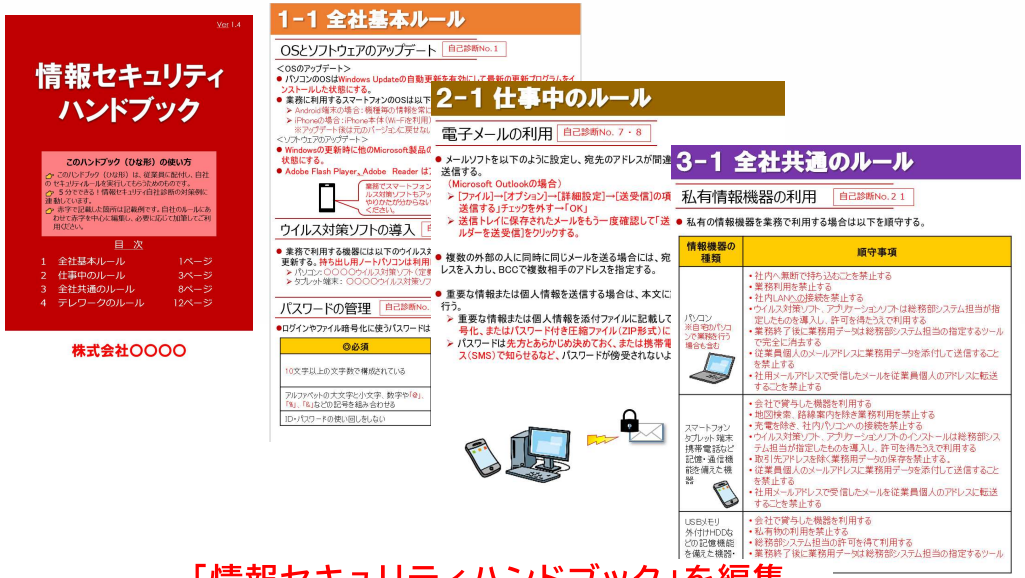
- 自社診断で問題があった項目は、解説編を参考に対策を決定
- 付録4「情報セキュリティハンドブック（ひな形）」を編集して社内周知

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）」



株式会社○○○○

「情報セキュリティハンドブック」を編集
社内周知

Step3　本格的に取り組む
(1)管理体制の構築

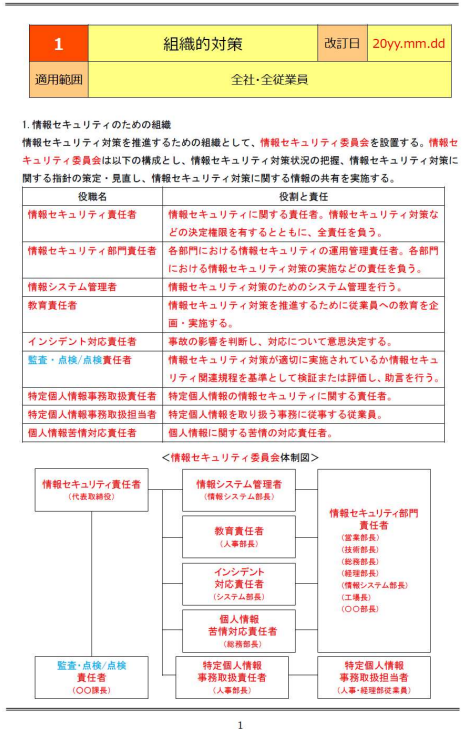
- 情報セキュリティ対策を推進するための管理体制を決定
- 付録5「情報セキュリティ関連規程」を活用して自社の管理体制を社内に周知

【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)	・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

Step3 本格的に取り組む
(2)情報セキュリティ関連規程の作成

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

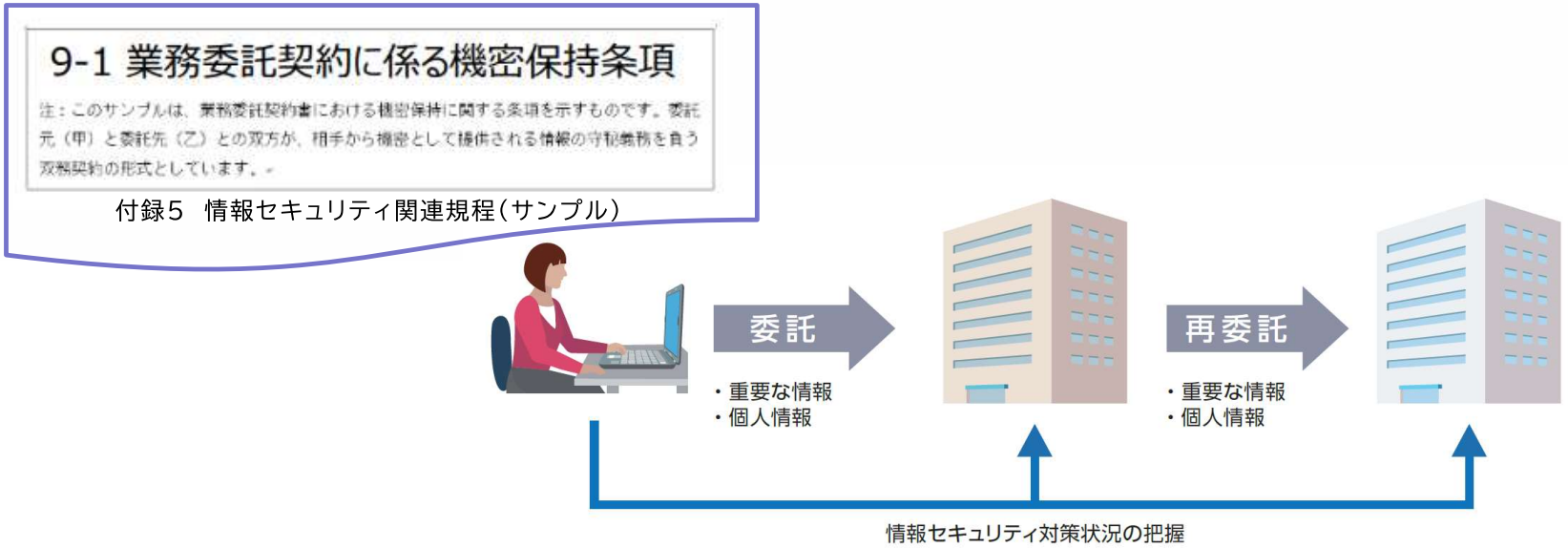
- 付録5「情報セキュリティ関連規程(サンプル)」を参考に、自社に適した規程にするために修正を加える
  - サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成
  - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記

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
(3)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



Step3 本格的に取り組む
(4)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

<u>点検の基準例</u>

- 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
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

(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、運用するためのポイント

(3)クラウドサービスの情報セキュリティ
クラウドサービスを安全に利用するためのポイント

(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

(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

(6)情報セキュリティサービスの活用
情報セキュリティに関する外部サービス

(7)技術的対策例と活用
ITを活用する際の技術的対策

(8)詳細リスク分析の実施方法
「リスク分析シート」(付録7)を活用した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
クラウドサービスの情報セキュリティ

中小企業がクラウドサービスを安全に利用するための確認事項や注意点をまとめた
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

- クラウドサービス安全利用チェックシートで確認すべきことがわかる
- 身近なサービスを例に、何を確認し、どうしたら安全に利用することができるかわかる

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。

Step4　より強固にするための方策
クラウドサービス安全利用チェックシート

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？

Step4　より強固にするための方策
セキュリティインシデント対応

- 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

Step4　より強固にするための方策
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

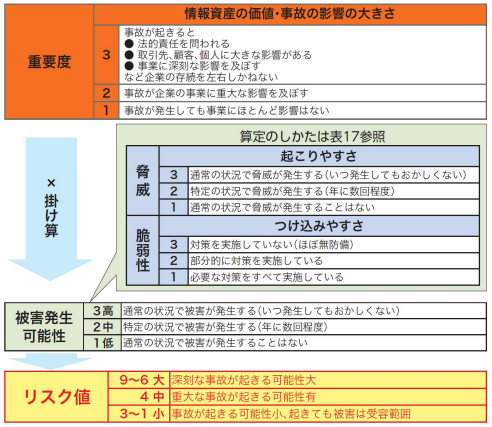
情報セキュリティ対策の決定

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。



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。

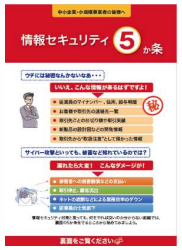
SECURITY ACTION制度

https://www.ipa.go.jp/security/security-action/

- 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度（2025年5月時点で、40万件に到達）
- 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに2段階の取組み目標を用意
- IT導入補助金をはじめ、官公庁や自治体の補助金等を申請する際の要件としても広く参照されている

1段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言



- **情報セキュリティ5か条に取り組む**

【情報セキュリテイ5か条】

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

2段階目（二つ星）

「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たうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言

- **情報セキュリティ自社診断を実施**
- **基本方針を策定**

【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

サイバーセキュリティお助け隊サービス制度

https://www.ipa.go.jp/security/otasuketai-pr/

- 中小企業に対するサイバー攻撃への対処として不可欠なサービス要件をワンパッケージとしてサービス基準にまとめ、これを満たすことが所定の審査機関により確認された民間サービスをIPAが**「サイバーセキュリティお助け隊サービス」**として登録・公表する制度を2021年度から開始。
- 価格要件を緩和し、**監視機能等を拡充したサービスを登録できる「2類」制度**を2024年度に開始
- 2024年5月現在、46社78サービスが登録（1類と2類の合計）。6,922社がサービス利用中（2024年9月時点）

◇「サイバーセキュリティお助け隊サービス基準」（1類）の主な内容

主な要件	概要
相談窓口	ユーザーからの**相談を受け付ける窓口**を設置／案内
異常の監視の仕組み	ネットワーク又は端末を**24時間見守る仕組み**（※）を提供 （※）UTMやEDR等を想定
緊急時の対応支援	インシデント発生などの**緊急時には駆け付け支援**
中小企業でも導入・維持できる価格	・ネットワーク一括監視型：**月額1万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）**
簡易サイバー保険	インシデント対応時に突発的に発生する駆付け費用等を補償する**サイバー保険を付帯**

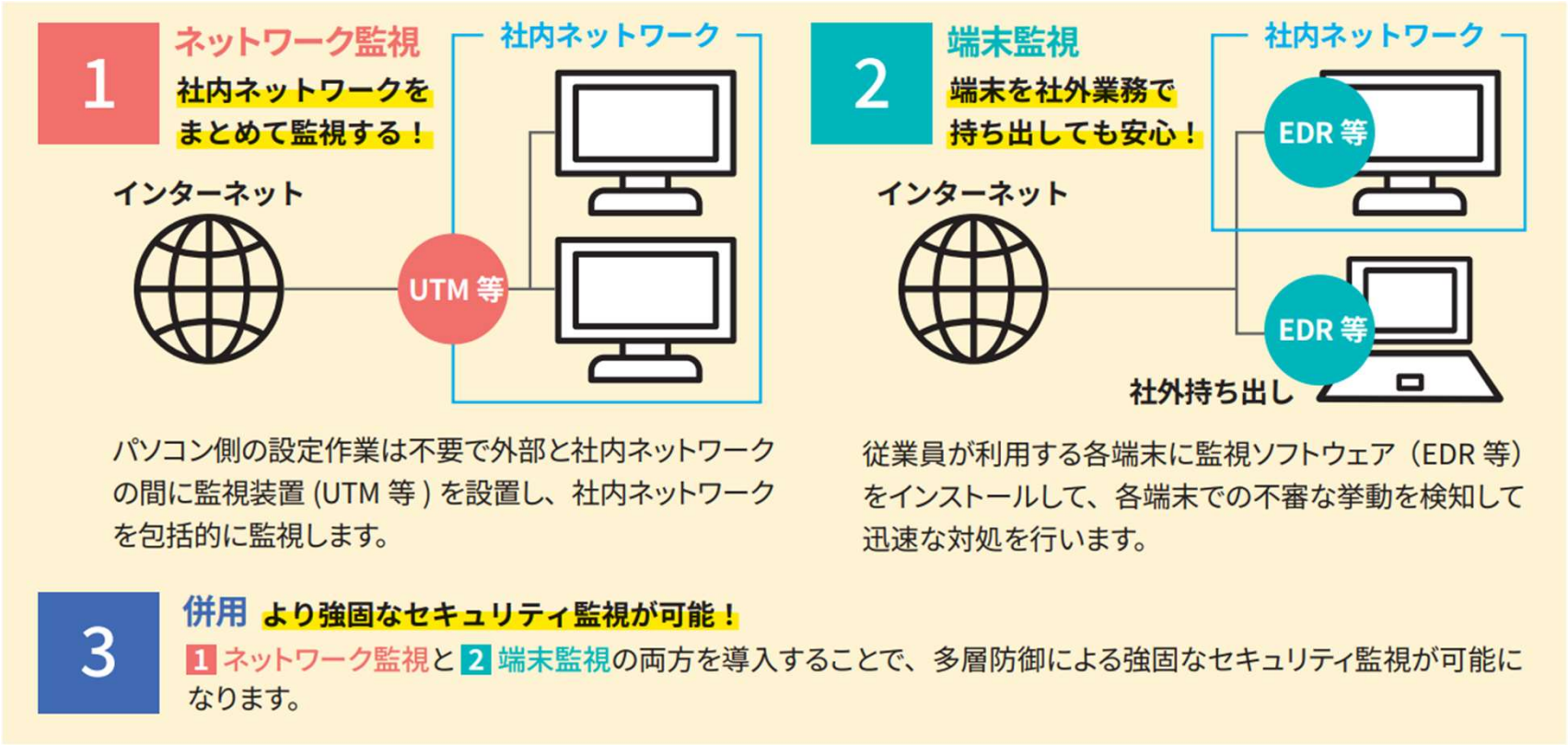
◇2類サービスの要件

・1類（左記）の要件＋以下から1つ以上追加 ※価格要件を緩和

拡充要素	概要
監視対象端末の増加	監視できる端末数の増加（最低50端末以上）
異常監視の仕組みや機能の追加	併用型への変更や監視範囲を追加する機能の追加
新たな提供サービスの追加	毎月実施、または定常的に利用可能な付加的サービスの追加

サイバーセキュリティお助け隊サービス制度
異常の監視の仕組み

監視タイプは「ネットワーク監視」、「端末監視」、「併用」の3種類から選べます



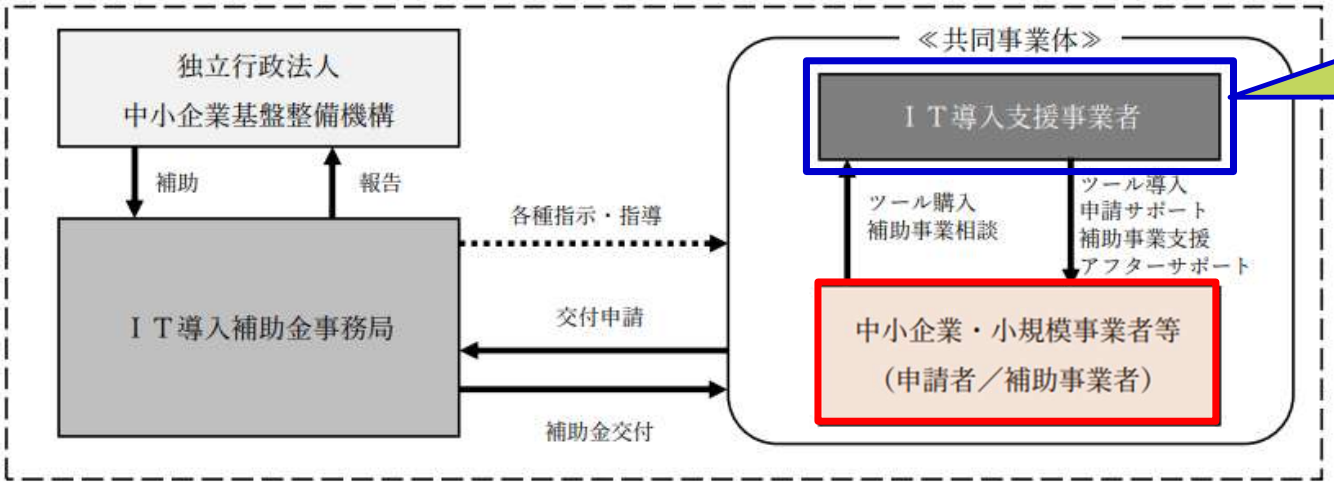
IT導入補助金2025　セキュリティ対策推進枠

https://it-shien.smrj.go.jp/applicant/subsidy/security/

中小企業・小規模事業者等が、**ITツール(「サイバーセキュリティお助け隊サービス」)を導入する際の経費の一部を補助**し、サイバーセキュリティ**対策の強化**を図る

- サイバーインシデントが原因で事業継続が困難となる事態の回避
- サイバー攻撃被害が供給制約・価格高騰を潜在的に引き起こすリスク、中小企業・小規模事業者等の生産性向上を阻害するリスクの低減

種類	セキュリティ対策推進枠
補助額	5万円～**150万円**
補助率	中小企業:1/2以内　**小規模事業者:2/3以内**
機能要件	独立行政法人情報処理推進機構が公表する「サイバーセキュリティお助け隊サービスリスト」に掲載されている いずれかのサービス
補助対象	導入費用・サービス利用料(最大2年分)



お助け隊サービス提供事業者
(または再販協力事業者)
※ IT導入補助金事務局にIT導入支援事業者として別途登録した事業者

詳細は「IT導入補助金2025」
https://it-shien.smrj.go.jp/

※ IT導入補助金2023 公募要領セキュリティ対策推進枠」から転載、引用　https://www.it-hojo.jp/r04/doc/pdf/r4_application_guidelines_security.pdf

企業向けの総合的な相談窓口の設置

・IPAでは、企業・組織向けに、コンピュータウイルス感染や不正アクセス等の**セキュリティインシデントに関する相談や届出、情報提供**を受け付ける窓口を設置！
・セキュリティインシデント等が発生し、お困りの際は、**下記ポータルページ**の活用を！

提供中

詳細はこちらのページにて

■ URL
https://www.ipa.go.jp/security/todokede/incidentportal.html

複数の窓口を整理統合

2025年4月企業向けの**総合的**な相談窓口を**新たに開設**

■「企業/組織向けサイバーセキュリティ相談窓口」

- 各種インシデント発生時の**初動対応**に関する相談
- **標的型サイバー攻撃**に関するインシデント相談
- その他の情報セキュリティに関する一般的な相談
- 脅威情報に関する**情報提供受付**

	相談・届出の例
インシデント発生時の初動対応	• ランサムウェアに感染した。対処方法を相談したい • 自組織のウェブサイトが改ざんされた。対処方法と再発防止策を相談したい　など
標的型サイバー攻撃に関するインシデント相談	• 標的型サイバー攻撃が疑われる事案が発生したため、相談や情報提供を行いたい
脅威情報に関する情報提供受付	• ランサムウェア感染したためインシデント内容を公的機関へ届出(情報提供)したい • サイバー攻撃被害の保険適用を受けるため公的機関への届出を行いたい • 日本国内利用のOS、ブラウザ、メーラ等の脆弱性を届出たい • 日本国内からのアクセスが想定されているインターネット上のウェブサイト等で稼動するシステムの脆弱性など

映像で知る情報セキュリティ

https://www.ipa.go.jp/security/videos/list.html#keihatsu

- 情報セキュリティに関する様々な脅威と対策を**10分程度のドラマなど**で分かりやすく解説した映像コンテンツ掲載。YouTube「**IPAチャンネル**」では全タイトルをいつでも視聴可能
- **社内研修等**営利を目的としない用途に限り、主な映像の**動画ファイルを無償で提供**（ダウンロード）

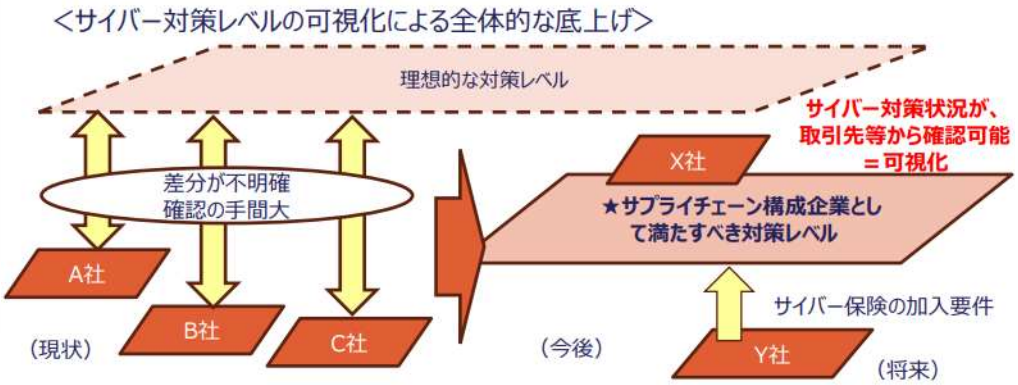
主な映像コンテンツ

	**今、そこにある脅威～内部不正による情報流出のリスク～** 社員による内部不正で機密情報が外部に流出する危機が発覚。機密情報の流出は防げたが、なぜこのような事態が発生したのか、背景を探りつつ内部不正による被害事例や手口、不正を起こさせないポイントの他、自社における経営者や管理部門だけでなく、関連会社や国内外の委託先なども含め、組織全体で実施すべき内部不正対策について解説しています。	約18分
	**今、そこにある脅威～組織を狙うランサムウェア攻撃～** 身代金として金銭を得ることを目的に企業・組織内のネットワークへ侵入し、データを一斉に暗号化して使用できなくしたりする”ランサムウェア攻撃”。本作ではその攻撃の手口、経営者・管理者・システム担当者、従業員が行うべき対策などを解説しています。	約15分
	**華麗なる情報セキュリティ対策** 「華麗なる情報セキュリティ対策」シリーズは、組織の従業員が日常行うべき8つの対策をご紹介しています。	8話構成 各話2分
	**妻からのメッセージ ～ テレワークのセキュリティ ～** テレワークでは職場の情報セキュリティ対策と同様に「情報漏えい」や「不正アクセス」などの被害に遭わないよう対策を講じる必要があります。本映像の主人公と一緒にテレワークのセキュリティ対策を学んでいきましょう。	約10分

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

中小企業を含めたサプライチェーン全体のセキュリティ対策底上げに向けて、2026年度からの制度運用を目指して、
2024年度に制度の基本構想策定、2025年度に、制度実証および制度運用体制整備を進めます。

サプライチェーンに係るセキュリティ対策評価制度（仮称）による効果



https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_supply_chain/index.html

対策レベルのイメージ

	三つ星（★３）	四つ星（★４）	五つ星（★５）
	• ビジネス観点（データ保護、事業継続）及びシステム観点で、重要度に応じて取引先を★3/4/5に分類		
(1)対象事業者のイメージ	・★４・５に該当しない者	・ビジネス観点：重要度中 または ・システム観点：接続あり	・ビジネス観点：重要度大
(2)対策の適用範囲（組織、システム）	・組織的対策 ・システム的対策（自社IT基盤）	・組織的対策 ・システム的対策（自社IT基盤に加えて、発注者内部NWへの接続点）	追加の組織的対策は無し（★４取得が前提） ・システム的対策（自社IT基盤への高度な対策上乗せ、OT等業務システムへの対策の追加
(3) 対策の基本的な考え方	• サイバーセキュリティフレームワーク2.0の６分類に、サプライチェーン対策である「取引先管理」を加えた７分類で検討		
	全てのサプライチェーン企業が最低限実装すべきセキュリティ対策として、基礎的な組織的対策とシステム防御策を中心に構成	上記に該当する企業等が、標準的に目指すべきセキュリティ対策として、ガバナンスからシステム防御・検知、インシデント対応等包括的な対策にて構成	上記に該当する企業等が、高度なサイバー攻撃への対処を念頭に目指すべきセキュリティ対策として、早期の侵入検知、被害の極小化など防護対象システムに対するより高度な対策にて構成
(4) 評価スキームの考え方	• 共通する対策事項の確認省略など、既存の認証制度等を活用可能な仕組みを検討		
	・自己評価 （専門家の助言プロセスを要する）	・第三者評価 （技術要件を中心に一部対策事項について第三者評価を実施）	・第三者評価

- サプライチェーン企業、ひいてはサプライチェーン全体の強靭性（事業継続性に加えてデータ保護を含む）の確保。
- 対策要求の共通化を通じたサプライチェーン対策の重複排除、対策状況の可視化による確認の効率化。

IoT製品セキュリティラベリング制度（JC-STAR）

https://www.ipa.go.jp/security/jc-star/detail.html

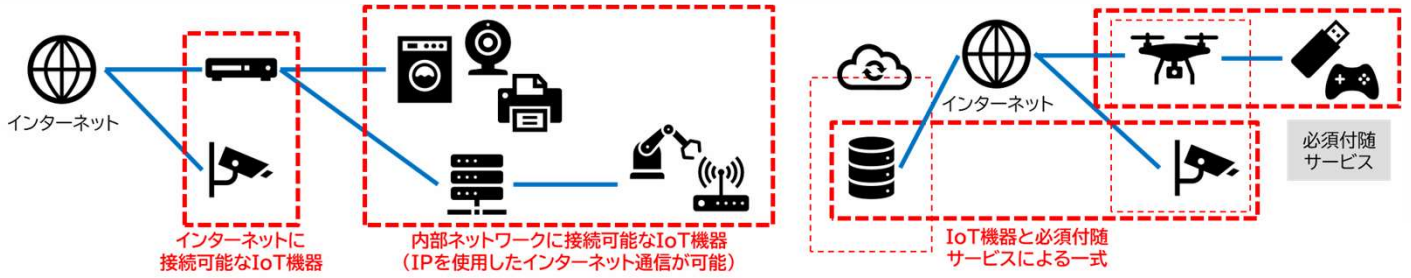
IPA

2025年度から、IoT製品に対するセキュリティ要件（適合基準）への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を開始

- IoT製品が具備するセキュリティ機能として満たしてほしい水準にあることを確認するための制度です。
- 調達者・消費者は製品詳細や適合評価、セキュリティ情報・問合せ先等の情報を簡単に取得でき、セキュリティ要件を満たした安全なIoT製品を選びやすくなります。

JC-STARプロモーションロゴ

JC-STARが対象とするIoT製品



JC-STAR適合ラベル

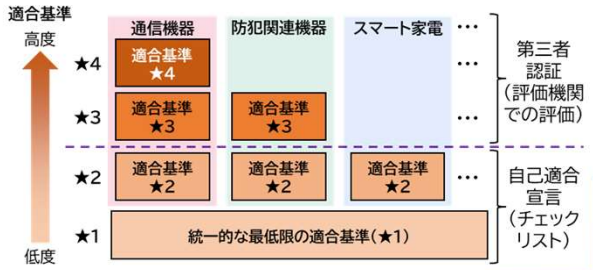
定められた適合基準への適合を示す目印

- IoT製品が予め具備するセキュリティ機能として満たしてほしい水準にあることを確認できる
- 有効期間は2年が基本。延長可
- 有効期間内はアップデートサポートを義務付け

IoT製品が取得した適合ラベルのレベルを表現しています。
★一つがレベル1を、★四つがレベル4を表します。

適合ラベルを取得したIoT製品情報を確認するため、IPAが管理する「適合ラベル取得IoT製品情報ページ」にリンクします。
このページは登録番号ごとに用意されます。

JC-STARの適合基準レベル



IPAメールニュース＆公式アカウント

セキュリティ関連情報、イベント・セミナーの開催情報や情報処理技術者試験に関する情報をメール配信しています。

メールニュースご登録 https://www.ipa.go.jp/mailnews.html

IPAの各種情報を配信する公式アカウントです。このほか、各専門分野の最新情報を発信するアカウントもございます。

X公式アカウント https://x.com/IPAjp/

IPAのイベント情報や情報セキュリティ関連などの最新情報を配信するIPA公式アカウントです。

Facebook公式アカウント https://www.facebook.com/ipaprjp/

情報セキュリティやソフトウェア開発関連など、研修や個人学習に最適な映像コンテンツを見ることができます。

YouTube「IPA Channel」 https://www.youtube.com/user/ipajp/


IPA