サイバー空間における脅威の動向と必要な対策
～万が一にどう備えるべきか～

2023年10月27日

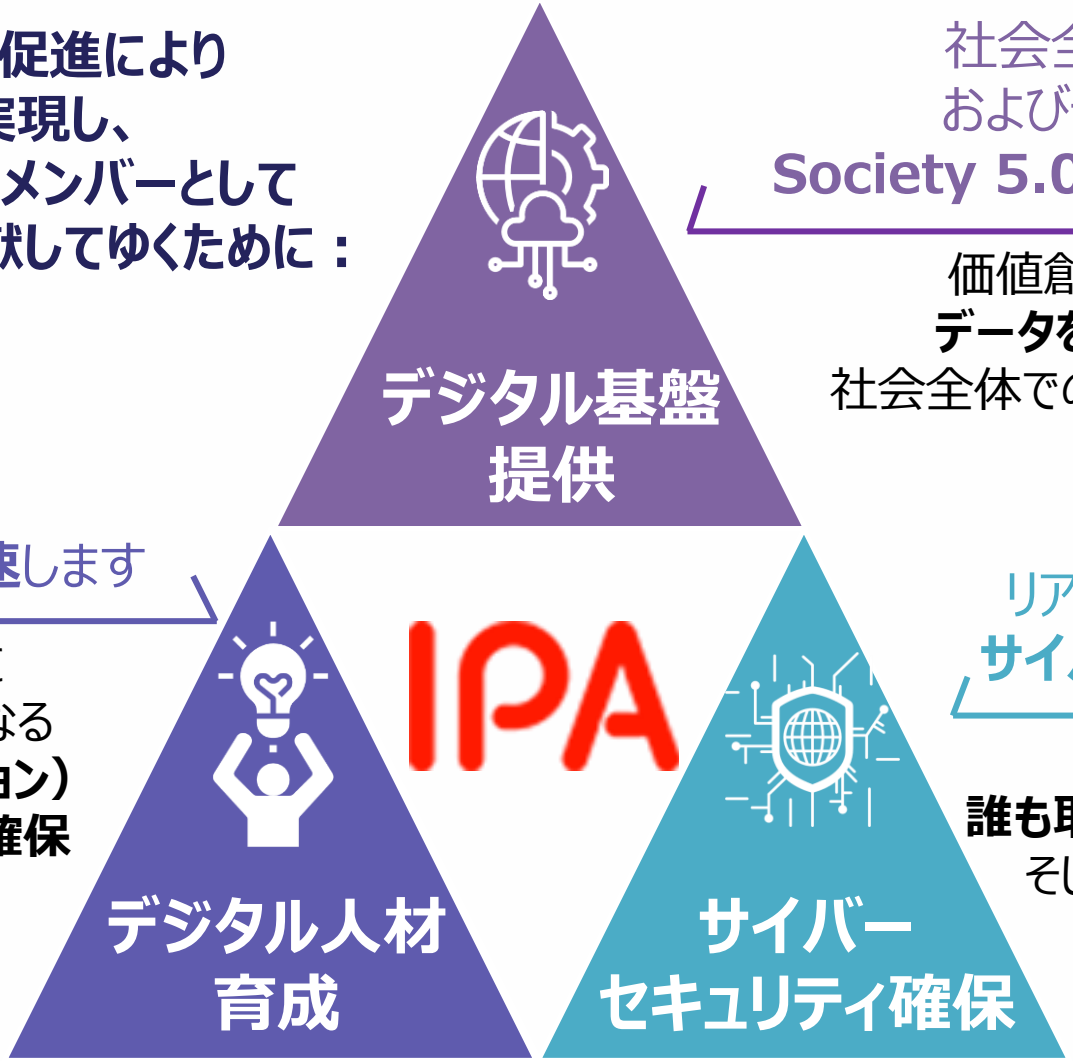
独立行政法人情報処理推進機構（IPA）
セキュリティセンター セキュリティ普及啓発・振興部
シニアエキスパート　横山 尚人

IPA Better Life with IT

公的プラットフォーマーとしてデータ駆動型社会を牽引するために：
第五期中期計画*のIPA事業3つの柱

*令和5年度からの5年間

デジタル技術の利用促進により
豊かな暮らしを実現し、
グローバルコミュニティのメンバーとして
直面する課題の解決に貢献してゆくために：



社会全体のアーキテクチャ設計
およびデータスペース整備による
Society 5.0実現のための基盤を提供します

価値創造と競争力の源泉となる
データを使いこなす環境の整備と
社会全体での**デジタルエコシステムの最適化**

DX・イノベーションで
新たな価値を生む
デジタル人材の育成を加速します

リテラシー底上げと同時に
課題解決と成長の切り札となる
破壊的な変革（ディスラプション）
をリードできる人材の育成・確保

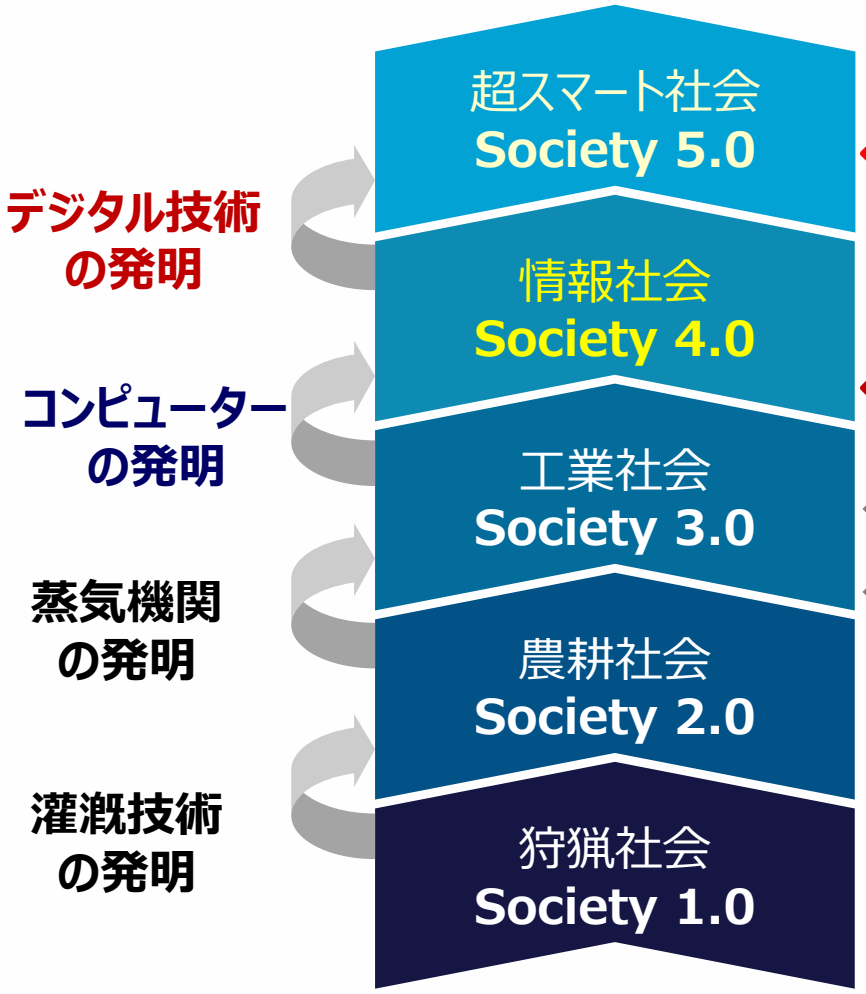
リアルとサイバーの融合でリスクが高まる
サイバーセキュリティの強化を実現します

国家・経済の**安全保障への貢献**、
誰も取り残さないサイバーセキュリティの確保、
そして**自主的なセキュリティ対策**を支える
インフラの提供

サイバーセキュリティ、
なんで必要？何をする？

サイバーセキュリティの話の前に・・・。

イノベーションによる社会と産業の進歩



これから
第4次産業革命 ＝ データとデジタルの時代

- **データ**が動力源
- **AI・IoT・ロボット**などのテクノロジーで課題を解決
- **デジタル化**が進む
- **DXを体現する企業**が台頭

1970年代~**現在**
第3次産業革命

- **コンピューティング・パワー**が動力源
- **PC・インターネット**が基盤
- **自動化・情報化**が進む
- **IT産業**が台頭

1860~1900年代
第2次産業革命

- **石油・電力**が動力源
- **モーター・製造ライン**が基盤に
- **大量生産・大量輸送・大量消費**が実現
- **重化学工業**が主流

1760~1830年代
第1次産業革命

- **石炭**が動力源
- **紡績機**が主要基盤
- **機械工業化**が進む
- **軽工業**が主流

仕事も生活も、デジタル技術を活用する時代に！

業務用パソコン・タブレット端末・スマートフォンの利用状況
利用している：93.3%
2021年度 中小企業における情報セキュリティ対策に関する実態調査
https://www.ipa.go.jp/security/reports/sme/about.html

ちなみに、
世帯普及率（2021年）
・パソコン： 69.8% ⬆
・スマートフォン：88.6% ⬆
・固定電話： 66.5% ⬇
※令和4年版 情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/r04.html

情報セキュリティ10大脅威2023

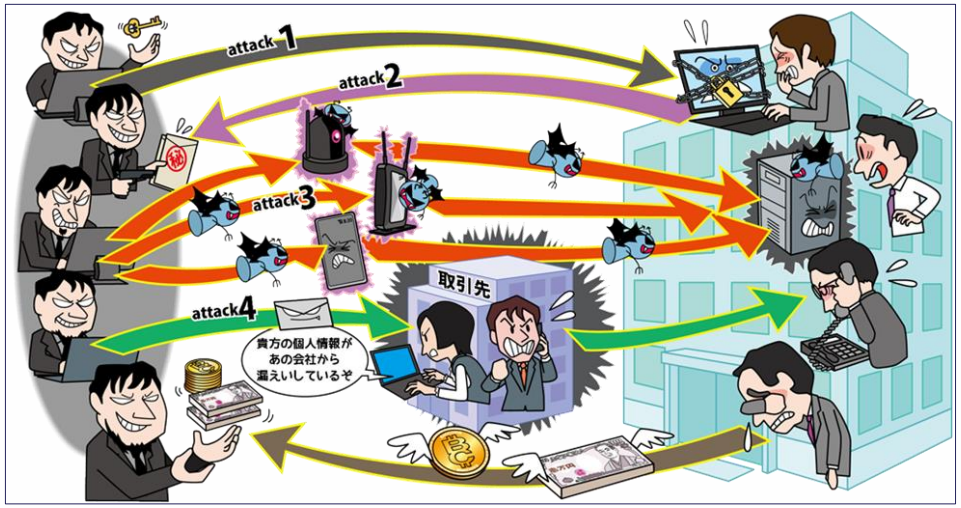
最近の「組織」における脅威動向

- 情報セキュリティ10大脅威： IPAが2006年から毎年発行している資料。前年に発生したセキュリティ事故や攻撃の状況等から専門家等が選考したTOP10について解説
- **「ランサムウェアによる被害」が引き続き1位**。2022年も大手自動車部品会社や医療センターなどの被害が発生し社会問題に。
- **「サプライチェーンの弱点を悪用した攻撃」が3位から2位**へ（2019~2021はいずれも4位）。
- **「内部不正による情報漏えいも徐々」**に順位が上昇

順位	2021	2022	2023
1	**ランサムウェアによる被害**	**ランサムウェアによる被害**	**ランサムウェアによる被害**
2	標的型攻撃による機密情報の窃取	標的型攻撃による機密情報の窃取	**サプライチェーンの弱点を悪用した攻撃**
3	テレワーク等のニューノーマルな働き方を狙った攻撃	**サプライチェーンの弱点を悪用した攻撃**	標的型攻撃による機密情報の窃取
4	**サプライチェーンの弱点を悪用した攻撃**	テレワーク等のニューノーマルな働き方を狙った攻撃	**内部不正による情報漏えい**
5	ビジネスメール詐欺による金銭被害	**内部不正による情報漏えい**	テレワーク等のニューノーマルな働き方を狙った攻撃
6	**内部不正による情報漏えい**	脆弱性対策情報の公開に伴う悪用増加	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
7	予期せぬIT基盤の障害に伴う業務停止	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	ビジネスメール詐欺による金銭被害
8	インターネット上のサービスへの不正ログイン	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加
9	不注意による情報漏えい等の被害	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害
10	脆弱性対策情報の公開に伴う悪用増加	不注意による情報漏えい等の被害	犯罪のビジネス化（アンダーグラウンドサービス）

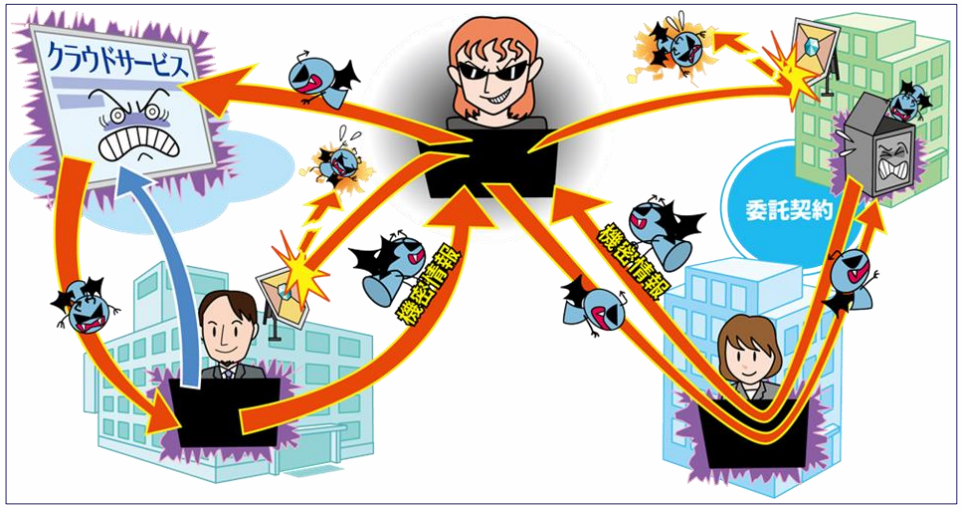
情報セキュリティ10大脅威2023　1位～2位

【1位】ランサムウェアによる被害
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～



- PC等に保存されているファイルを暗号化され**使用不可に**
- 復旧と引き換えに**金銭を要求される**
- 情報を窃取しそれを公開する、攻撃を受けている事を**ビジネス パートナー等に公表**すると脅迫するケースも

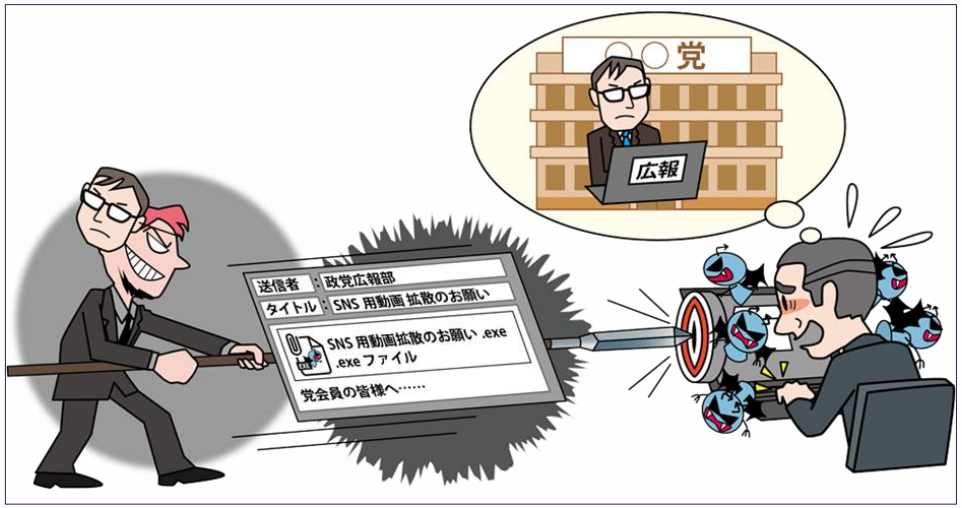
【２位】サプライチェーンの弱点を悪用した攻撃
～自組織だけでなく、委託先や利用しているサービスも適切な管理を～



- 調達から販売、業務委託等**一連の商流**において、セキュリティ**対策が甘い組織が攻撃の足がかり**として攻撃される
- ソフトウェア開発のライフサイクルに関与するモノや人の繋がりを足掛かりとする（ソフトウェアサプライチェーン）攻撃も存在
- 取引先や業務を委託している**外部組織から情報漏えい**

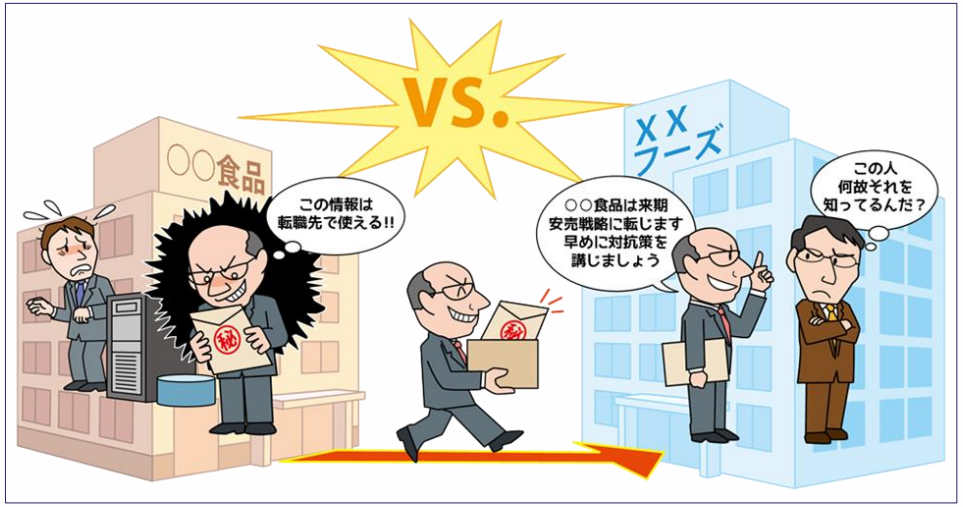
情報セキュリティ10大脅威2023　3位～4位

【3位】標的型攻撃による機密情報の窃取
～メールが来たらまずは疑え！？意識は常に高く～



- メール等を利用し特定組織のPCを**ウイルス**に感染させる
- 組織**内部に潜入**し長期にわたり侵害範囲を徐々に広げる
- 組織の**機密情報窃取**や**システムの破壊**を行う

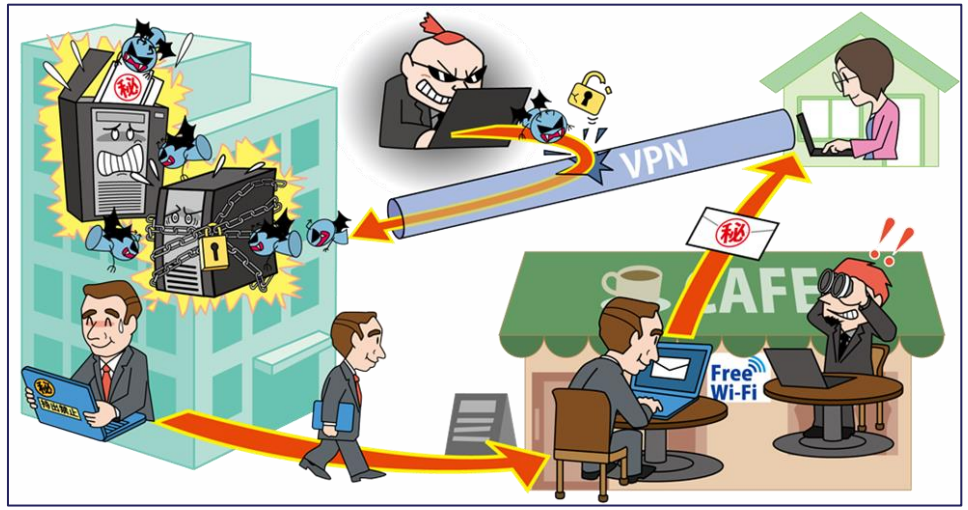
【4位】内部不正による情報漏えい
～不正に情報を取得しない、取得させない、使用しない！ ～



- 組織の**従業員や元従業員等**による機密情報の漏えい
- 組織関係者による不正行為による、組織の**社会的信用の失墜**、損害賠償による**経済的損失**
- 不正に取得した情報を**他組織に持ち込んだ場合、その組織も**損害賠償等の対象になるおそれがある

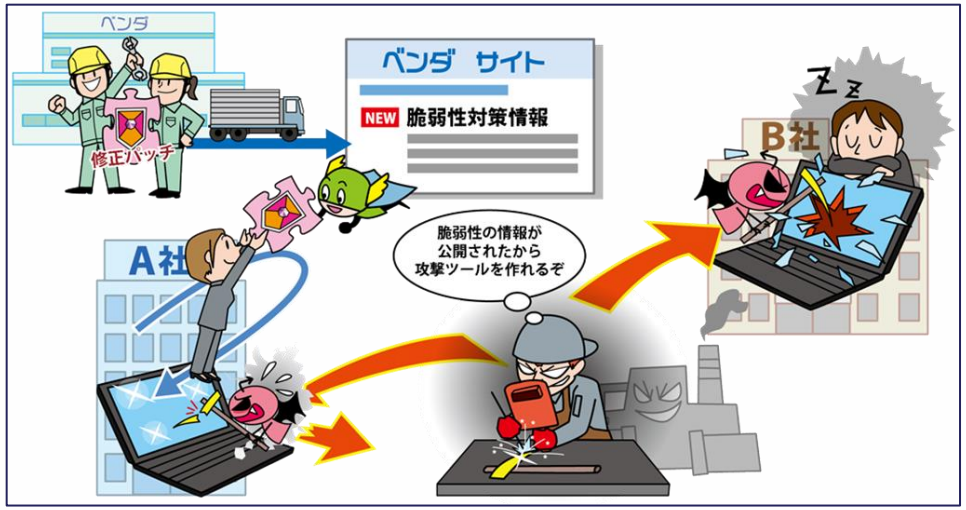
情報セキュリティ10大脅威2023　5位と8位

【5位】テレワーク等のニューノーマルな働き方を狙った攻撃
～未だ脆弱なテレワーク環境が狙われる～



- 新型コロナウイルス対策の1つとして、テレワークが急速に普及
- ウェブ会議サービスやVPNの本格的な活用がされる中、それらを狙った攻撃が発生
- ウェブ会議ののぞき見やテレワーク用PCのウイルス感染のおそれ

【8位】脆弱性対策情報の公開に伴う悪用増加
～「後で対応しよう」、その数日が命取り～

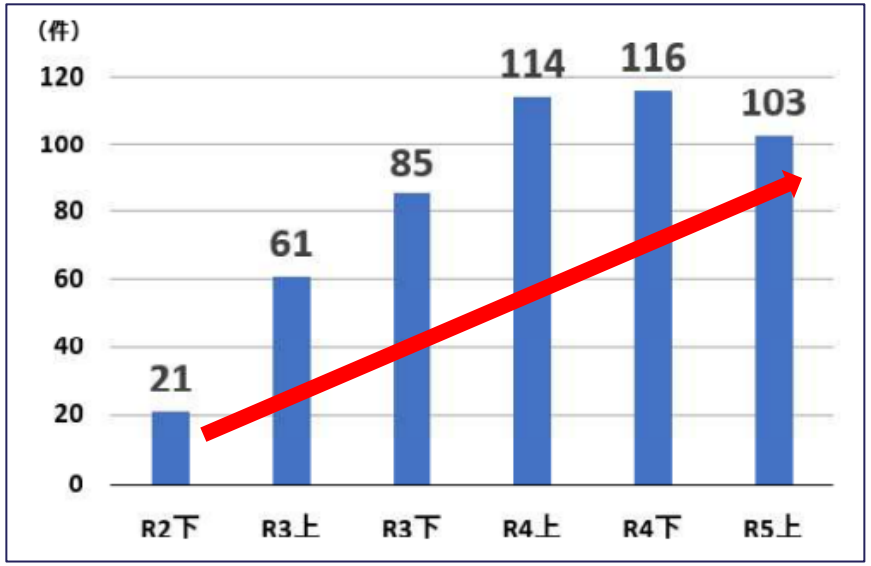


- 新脆弱性対策のために公開された脆弱性情報を攻撃者が悪用
- 脆弱性情報の公開後、攻撃コードが流通して攻撃が本格するまでの時間が近年は短くなっている傾向
- 広く利用されている製品の脆弱性の場合は被害が大きくなる

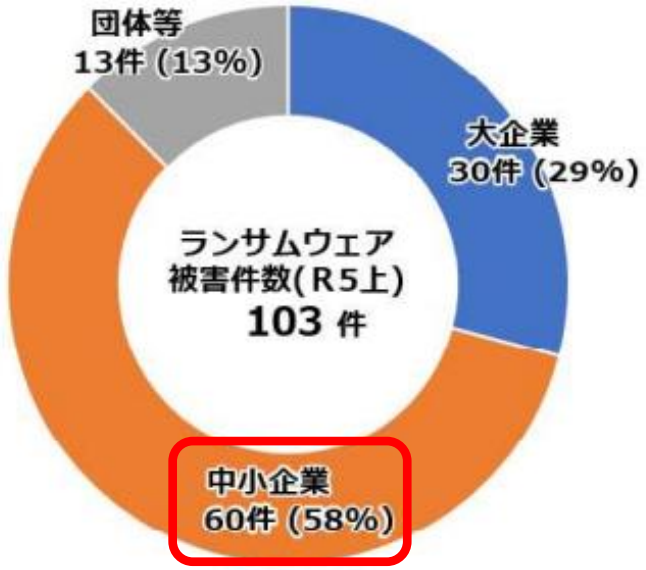
サイバー攻撃は企業規模、業種を問わない
～警察庁のレポートに見られるランサムウェアの状況①～

- ランサムウェア被害の被害は右肩上がり。58%は中小企業
- あらゆる業種が被害。企業自体の被害のみならず、発注元、取引先企業への被害波及、攻撃の足掛かりとされる懸念

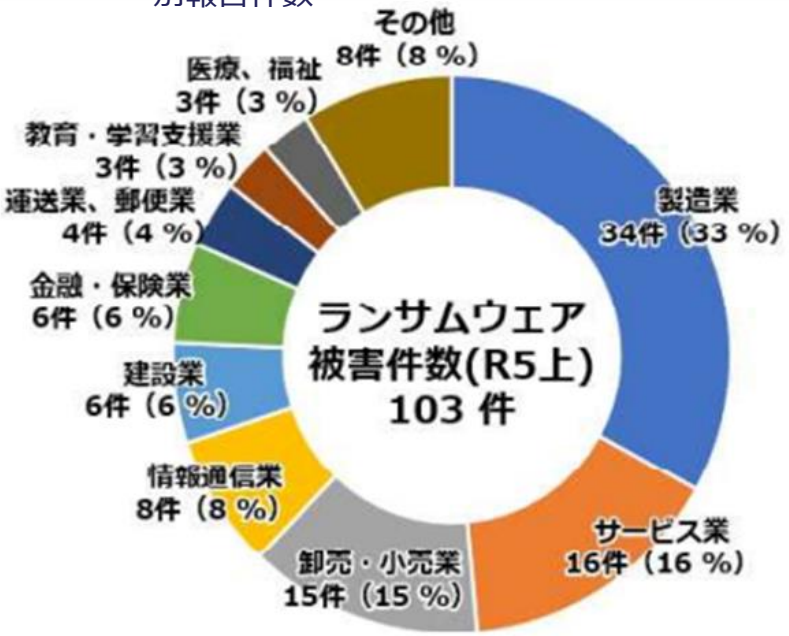
企業・団体等におけるランサムウェア被害の
報告件数の推移



ランサムウェア被害の企業・団体等の
規模別報告件数



ランサムウェア被害の企業・団体等の業種
別報告件数

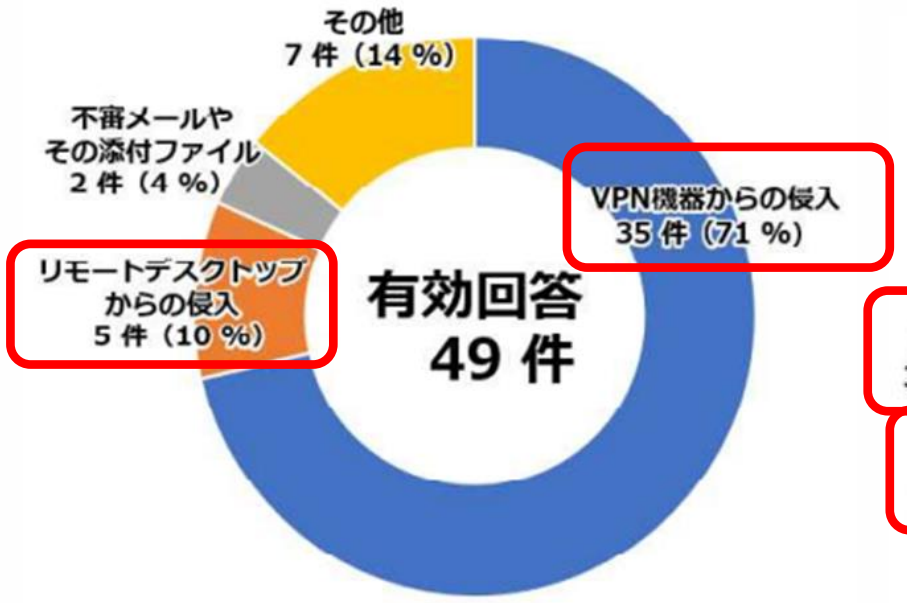


令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）：
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

ランサムウェアに感染してしまった場合の影響は甚大
～警察庁のレポートに見られるランサムウェアの状況②～

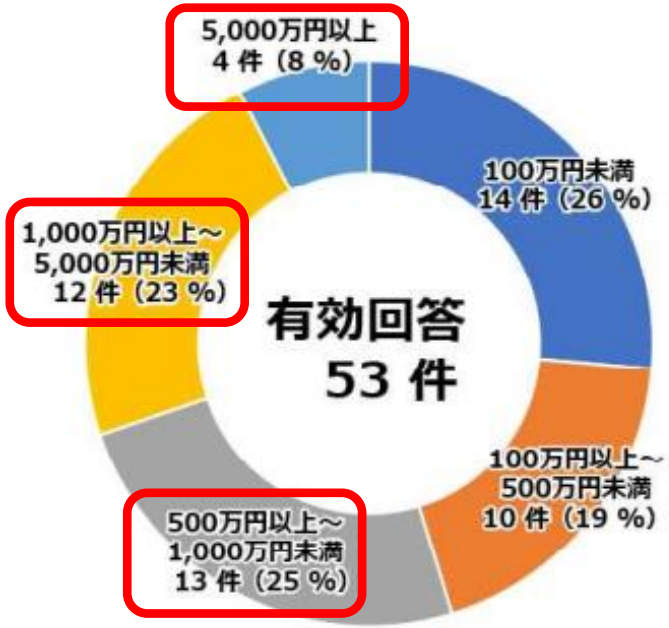
- VPN機器、リモートデスクトップからの侵入で80%以上
- 復旧に要した期間1週間以上が約半数。
- 半数以上が調査・復旧に500万円以上を要していた。

感染経路



復旧に要した期間

調査・復旧費用の総額



令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）：
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

サイバーセキュリティって必要？

いままでも・・・

- （紙の）書類、現金
- 現物

⇒

- 戸締り。書棚・引き出し・金庫収納、施錠
- 見張り、記録簿
- 手口の巧妙化、悪質化に備えて対応（鍵の付替え、防犯カメラ） … etc.

仕事をデジタル化したら
防犯やミス防止も**デジタル化**
仕事が便利になったぶん、**犯罪者にも便利**
“実物を扱わない、時間や距離の制約がなくなる”

なにを守る？

保有している情報の

機密性　**許可された者だけ**が情報に**アクセスできる**ようにすること

完全性　保有する情報が**正確**であり、**完全**である状態を保持すること

可用性　許可された者が**必要なとき**に**いつでも**情報にアクセスできるようにすること

よくある質問

どこからどう始めたら良いか？

- まずは、**基本的**な対策から
- 組織の実態、必要性に合わせ**段階的**に

どこまで実施すれば良いか？

- リスクを**受容**できるレベルまで
- 組織における**改善点**を把握し、対策の**周知・実践**

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

脅威から会社をどう守るのか
効果的な解決方法は？

■ セキュリティ対策では、“**平時からの「人」の対策**”と“**有事に向けた「仕組み」による対策**”の**両方に並行して取組む**ことが重要。

平時からの「人」の対策（防御等）

- サイバーセキュリティマネジメント体制の整備
- 情報セキュリティ規程の作成、周知徹底
- 教育等による社員意識醸成、向上

＋

有事に向けた「仕組み」による対策（検知、対応、復旧等）

- 目に見えないサイバー攻撃を可視化、異常の監視
- 何か起きた場合の緊急対応・復旧

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**「中小企業情報セキュリティガイドライン」**。
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。

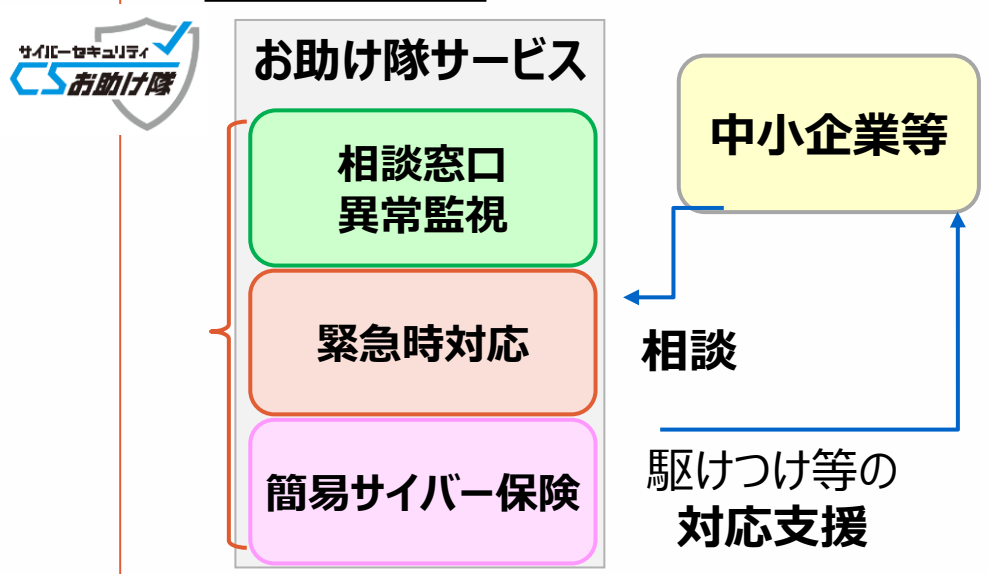
SECURITY ACTION

- 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。



日頃からの「人」の対策

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

- 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

付録一覧

付録1：情報セキュリティ5か条(PDF)

付録2：情報セキュリティ基本方針（サンプル）(Word)

付録3：5分でできる！情報セキュリティ自社診断(PDF)

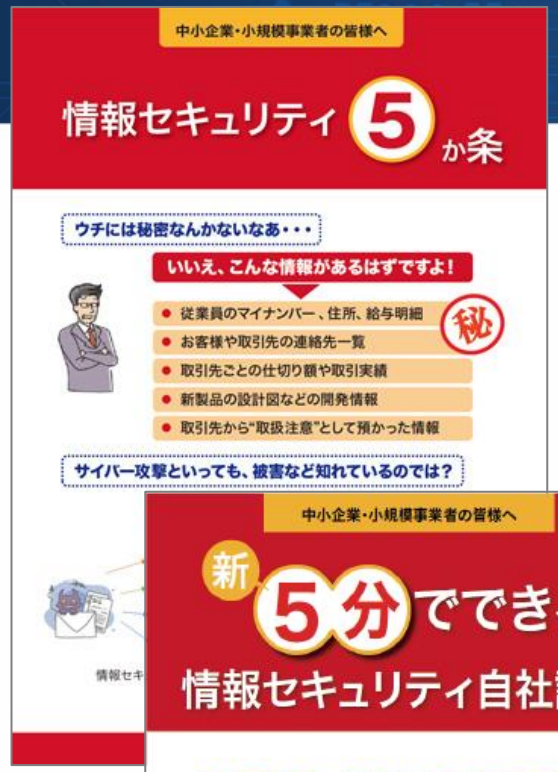
付録4：情報セキュリティハンドブック（ひな形）(PowerPoint)

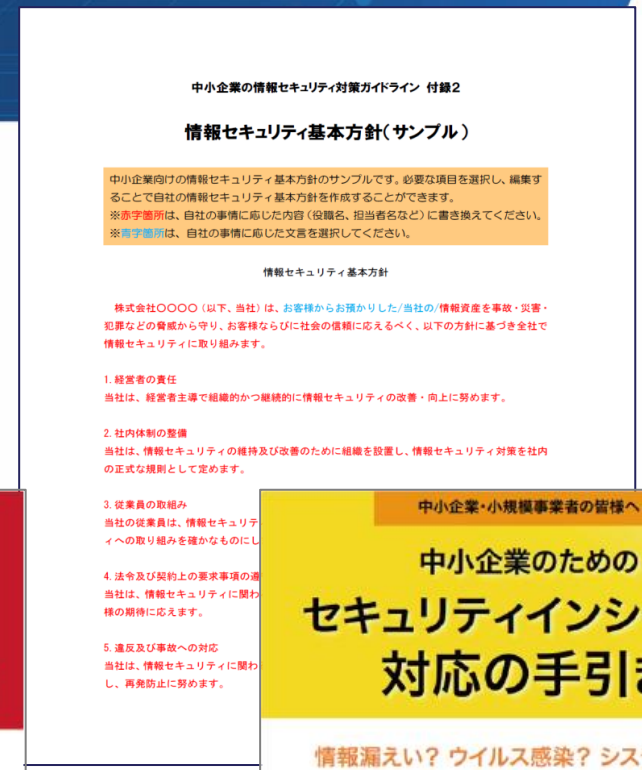
付録5：情報セキュリティ関連規程（サンプル）(Word)

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(PDF)

付録7：リスク分析シート（全7シート）(Excel)

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(PDF)





【参考】中小企業の情報セキュリティ対策ガイドライン第3.1版の構成と主な改訂の概要

- **中小企業におけるITの利活用**が進む一方で、**新たな脅威も発現**し、**事業に悪影響を及ぼすリスク**も高まっている。
- DX推進やテレワーク普及といった動向や、情報セキュリティ関連技術の進展状況も踏まえつつ、**関連法令の記載内容の見直し**や、中小・小規模事業者においても普及が進む**テレワーク時のセキュリティ対策**や、**インシデント対応**を追記。

	構成	改訂内容
本編	第１部　経営者編	関連法令や被害事例の内容を見直し
	第２部　実践編	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（PDF）	対策例を最新の内容に見直し
	付録２　情報セキュリティ基本方針（サンプル）（Word）	
	付録３　５分でできる！情報セキュリティ自社診断（Word）	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）(PowerPoint)	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５　情報セキュリティ関連規程（サンプル）（Word）	テレワークの情報セキュリティに関するひな形、サンプルを追加等
	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（PDF）	
	付録７　リスク分析シート（Excel）	
	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（PDF）	新規追加。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

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」

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明確に整理し、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などが発生した際にも、関係者の不信感の高まりを抑えることが可能

実行すべき「重要7項目の取組」

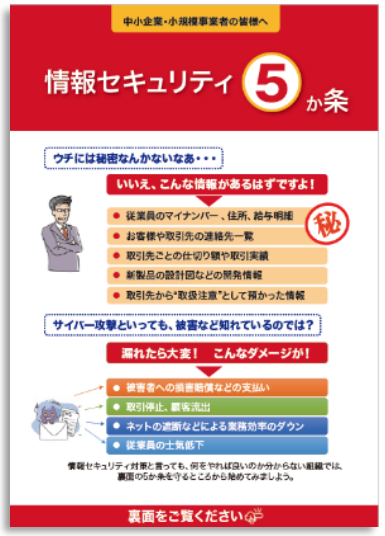
- 経営者は、以下の**７項目**を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

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**

Step1
できるところから始める



情報セキュリティ５か条

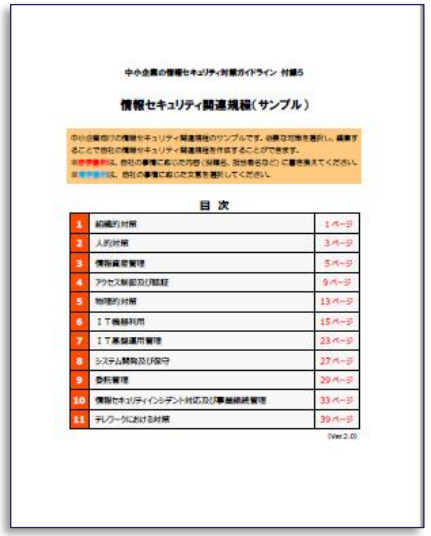
SECURITY ACTION ★一つ星を宣言

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

- 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

より強固にするため方策

日頃からの「人」の対策
～“はじめの一歩”と“二歩目”～

できるところから始める

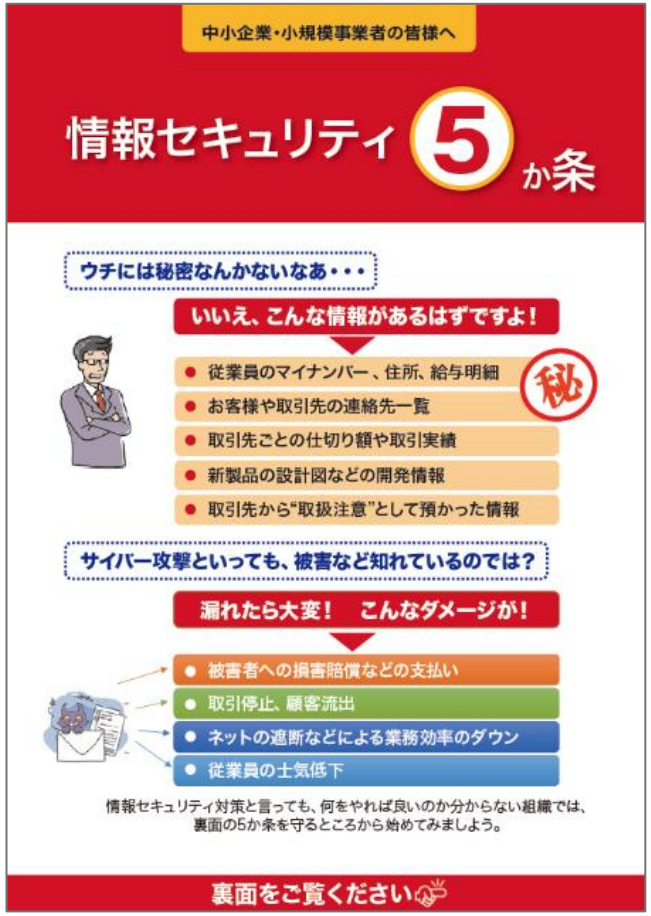
情報セキュリティ5か条

- 情報セキュリティ対策と言っても、
  何をやれば良いのか？

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！



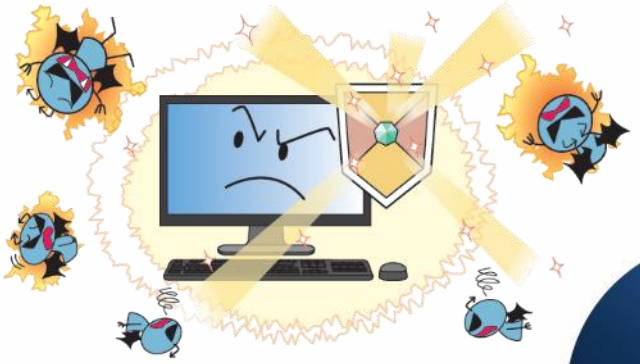
① OSやソフトウェアは常に最新の状態に

- 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。
- 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。
- パソコン、スマホだけではなく、**ネットワークに繋がるすべての機器**も対象。
  - たとえば、サーバー、無線LANルーター、プリンターなどなど
  - **ウェブサイト**に使われているアプリケーションも点検を

②　ウイルス対策ソフトを導入

- **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**したりするウイルスが増加。
- 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。

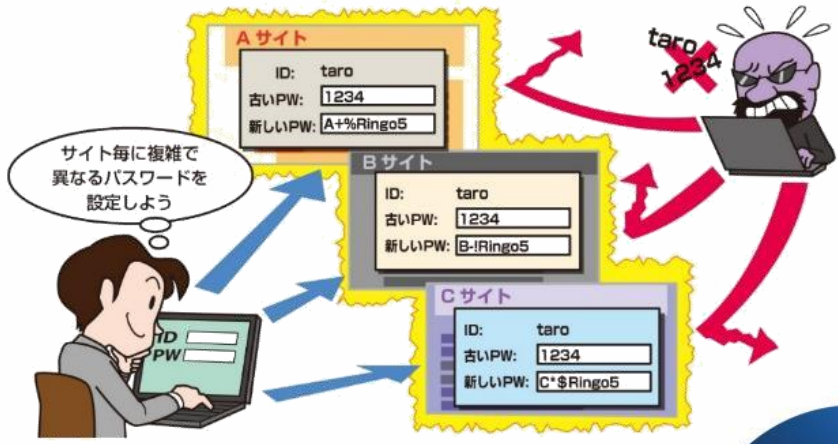
  - ウイルス定義ファイルが**自動更新**されるように設定
  - 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入する



③　パスワードを強化

- 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**が増加。
- パスワードは「**長く**」、「**複雑**に」、「**使い回さない**」ようにして強化を。
  - パスワードは英数字記号含めて長い文字数にする
  - 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
  - 同じID・パスワードをいろいろなシステム、ウェブサービスで使い回さない
- **多要素認証**※も積極活用を。

※ サービス利用時に行う利用者認証を、3 つの要素（①知っているもの②持っているもの③本人自身に関するもの）のうち、2 つ以上の要素を用いて行うもの。3 つの要素すべてを使う場合などもあり得る
① 知っているもの＝パスワード
② 持っているもの＝カード、スマホ、USBセキュリティキー　など
③ 本人自身に関するもの＝指紋、顔、虹彩　など
（内閣サイバーセキュリティセンター「インターネットの安全・安心ハンドブック」より）



【小ネタ】使い回さないパスワード作成の一例

コアパスワードとサービスごと固有の文字列を作り、組み合わせる

～コアパスワードの作り方～

1. 短いフレーズを作る	• テレビが好き
2. ローマ字にする	• terebigasuki
3. 一部を大文字にする	• terebiGAsuki
4. 記号を追加する	• terebiGAsuki!!
5. 数字を追加する	• terebiGAsuki!!06

完成したコアパスワードに
サービス固有の文字列を
追加してパスワードを作る

・いろは銀行の場合
IrhterebiGAsuki!!06

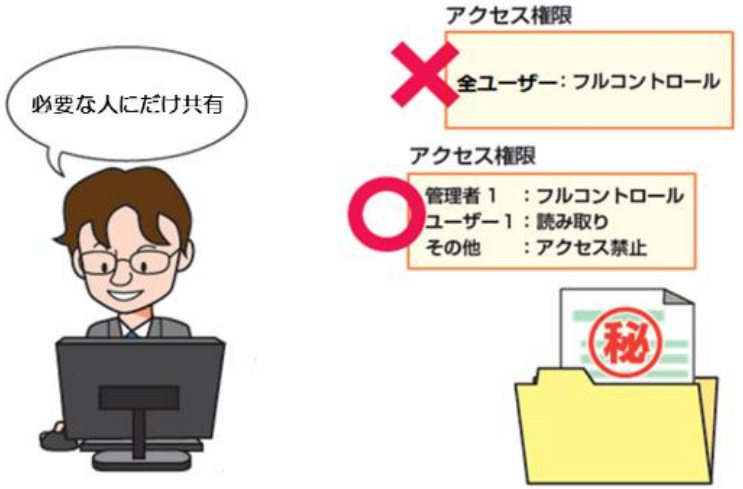
・IPAサービスの場合
IPAterebiGAsuki!!06

詳しくはコチラをCheck!!「安心相談窓口だより　不正ログイン被害の原因となるパスワードの使い回しはNG」
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

④ 共有設定を見直す

- 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。
- **無関係な人**が、ウェブサービスや機器を**使うことができない設定**になっていることの確認を。

- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスクなどの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する



⑤ 脅威や攻撃の手口を知る

- **取引先や関係者と偽って**ウイルス付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**が増加。
- 脅威や攻撃の**手口を知って適切な対策**を！

- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

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**「5分でできる！情報セキュリティ自社診断」**を活用
  https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf
  - **25項目の設問**に答えることで、自社の情報セキュリティ上の**問題点の把握**が可能
  - **解説編**の対策例を参考に、**社内ルールの作成**が可能
  - ガイドライン付録の**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**が可能

セキュリティ対策自己宣言

自社診断のための25項目

- 25項目の設問に答え、自社の情報セキュリティ対策の実施状況を把握

基本的対策　5項目

脆弱性対策、ウイルス対策、パスワード強化など

従業員としての対策 13項目

標的型攻撃メール、電子メール、持ち出し、廃棄、ウェブ利用など

組織としての対策 7項目

守秘義務、インターネット利用、ルール化　など

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？

組織的な取り組みを開始する

対策の決定と周知

- 問題があった項目は、**解説編**を参考に対策を決定
- 付録「**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

対策例を参考にして決定

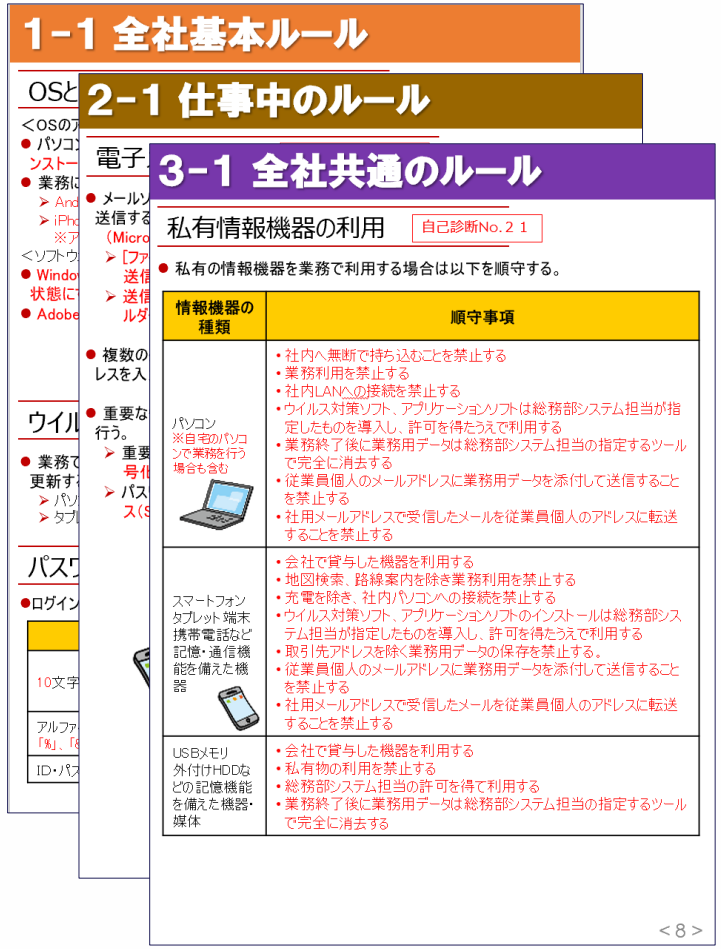
診断編 NO.1 脆弱性対策

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。

対策例

- ●WindowsUpdate、(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、Java実行環境など利用中のソフトウェアを最新版にする。
- ●テレワークで利用するパソコン等のソフトウェアやルーター等のファーム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存在しないか「JVN iPedia脆弱性対策情報データベース検索」で確認する。

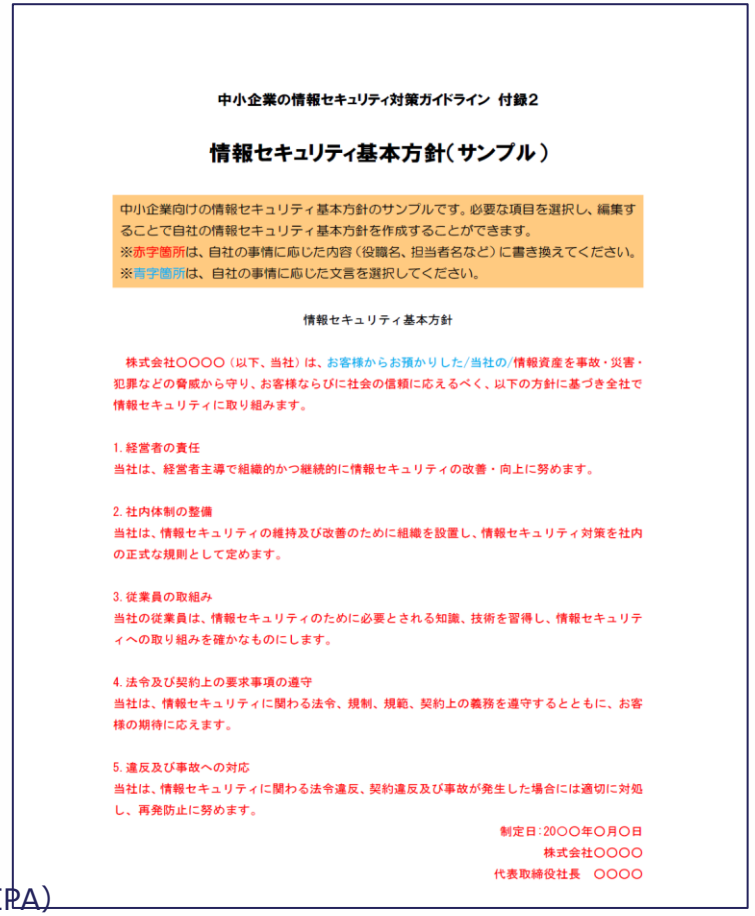


組織的な取り組みを開始する

「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
- 付録の**「情報セキュリティ基本方針（サンプル）」**を活用

- **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・ガイドライン等の整備
  - 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　○○○○

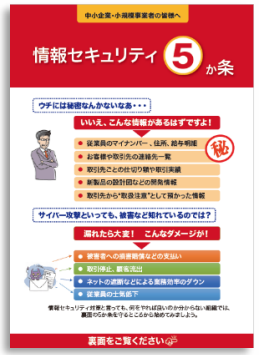
SECURITY ACTION ★★
セキュリティ対策自己宣言

SECURITY ACTION制度について

- 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（※）
  - 「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段階の取組目標**を用意

※IPAが各企業等の情報セキュリティ対策状況等を認定する、あるいは認証等を付与する制度ではありません。

★一つ星



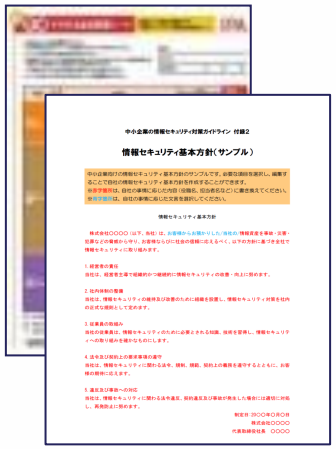
１段階目（一つ星）

●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！

★★二つ星



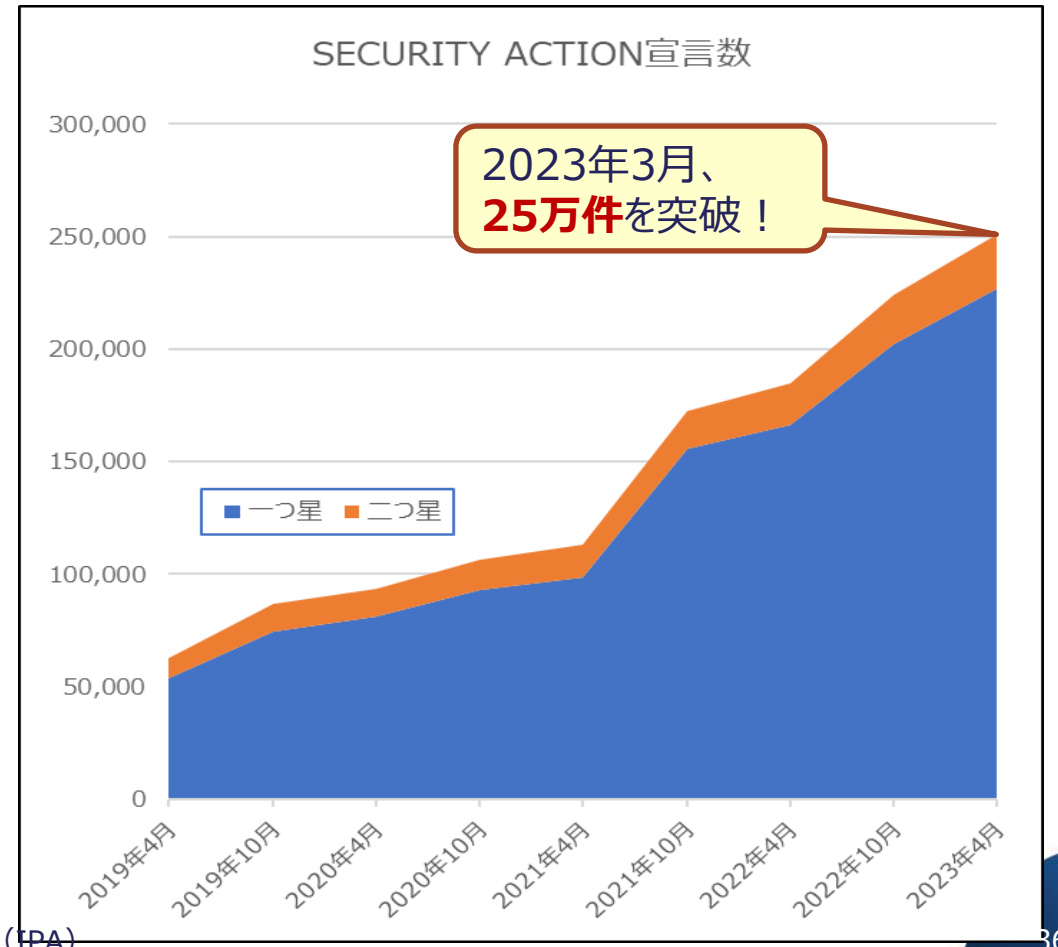
2段階目（二つ星）

●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



SECURITY ACTION制度のメリット

1．情報セキュリティ対策への取組みの**見える化**

☞ ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに 印刷することで自らの取組み姿勢をアピール

2．顧客や取引先との**信頼関係**の構築

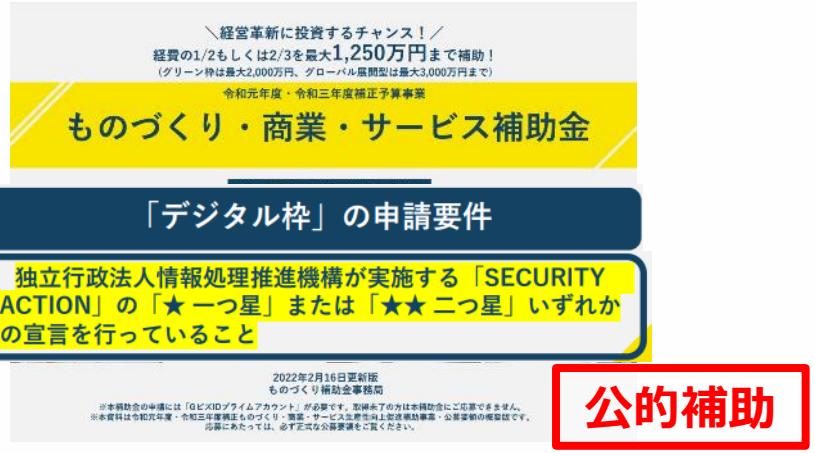
☞ 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに

3．**公的補助**・民間の支援を受けやすく

☞ SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能

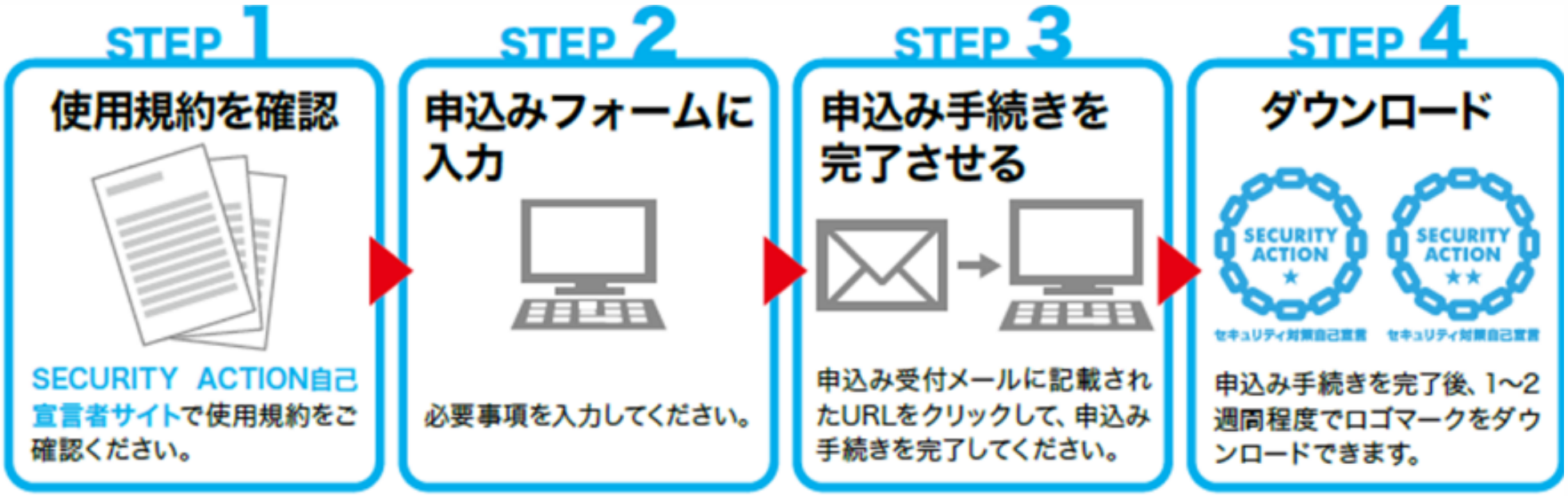
見える化

信頼関係



公的補助

SECURITY ACTION 申込手順



SECURITY ACTION自己宣言者サイト

https://security-shien.ipa.go.jp/security/entry/

SECURITY ACTION自己宣言を活用している補助金・助成金

- デジタル化やサイバーセキュリティ対策などを支援するIT導入の補助金申請の要件、加点要素にするなど、各種補助金・助成金制度において**SECURITY ACTION制度を活用**
- 引き続き各地方自治体や団体組織等とも連携の上、取組みの拡大を促進

- IT導入補助金（通常枠・セキュリティ対策推進枠・デジタル化基盤導入枠）：中小企業庁
- ものづくり補助金（デジタル枠）：中小企業庁
- 事業承継・引継ぎ補助金（経営革新）：中小企業庁
- 地域医療介護総合確保基金を利用したICT導入支援事業（令和４年度）：厚生労働省
  ※実施主体は各都道府県
- 事業再構築補助金（サプライチェーン強靭化枠）：中小企業庁【令和5年度新規】
  （令和5年3月下旬頃公募開始、令和5年度末までに3回程度の公募を実施予定）

- デジタル化トライアル事業費補助金：秋田県
- サイバーセキュリティ対策促進助成金：東京都中小企業振興公社
- 「情報セキュリティ基本方針 策定支援専門家派遣」事業：東京都中小企業振興公社
- 中小企業等スマートワーク促進補助金（情報セキュリティ事業）：岐阜県
- 堺市中小企業デジタル化促進補助金：大阪府堺市
- 愛知県デジタル技術導入補助金：愛知県【令和5年度新規】
- デジタル化促進補助金：北海道札幌市【令和5年度新規】
- 産業デジタル実装支援事業費補助金：宮崎県【令和5年度新規】

日頃からの「人」の対策
～本格的に取り組み、強固にしていくために～

本格的に取り組む
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（サンプル）」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。

社内規程

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

本格的に取り組む

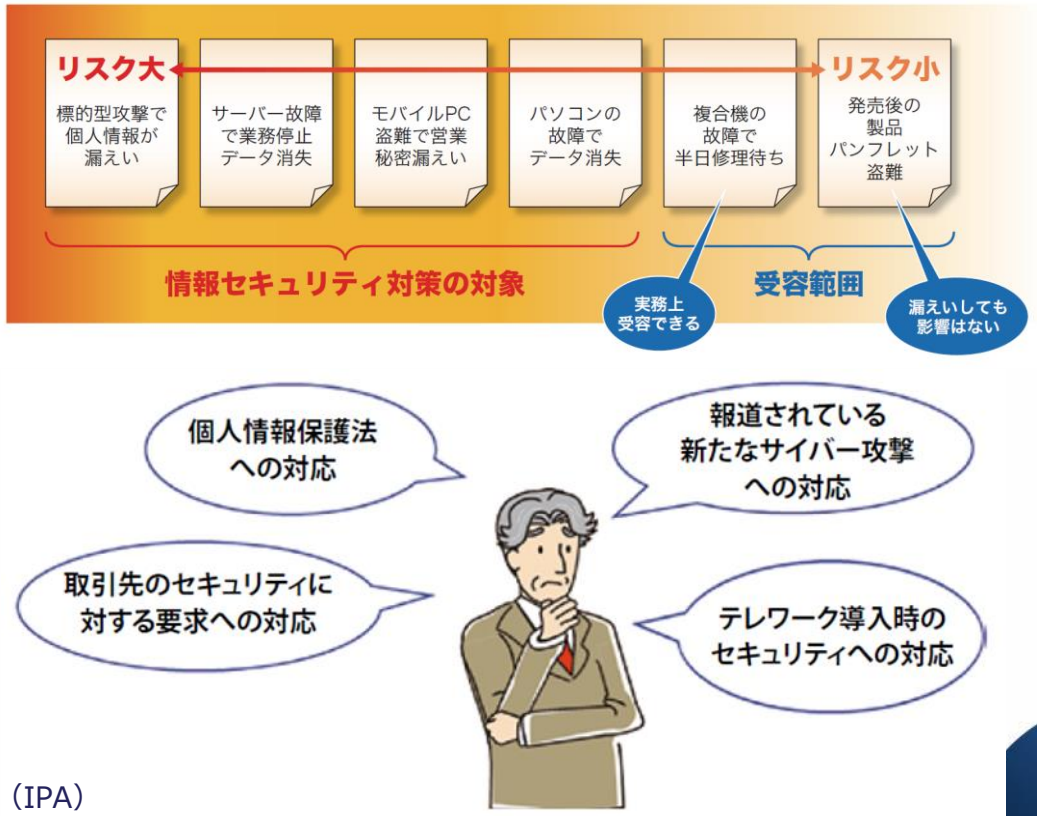
情報セキュリティ規程の作成（1）

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



本格的に取り組む情報セキュリティ規程の作成（2）

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）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。

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み

(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

(6) **セキュリティサービス例と活用**
- 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

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

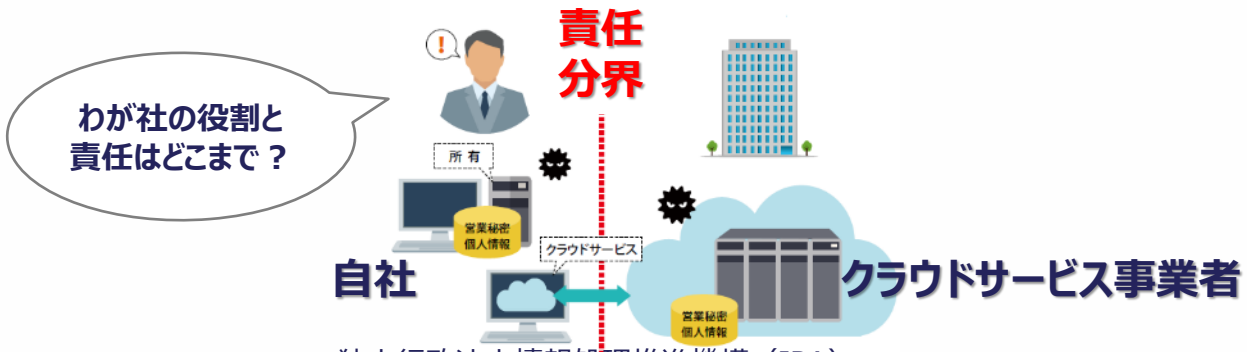
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、業務のセキュリティ要件に見合ったサービスを選定しましょう。

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。

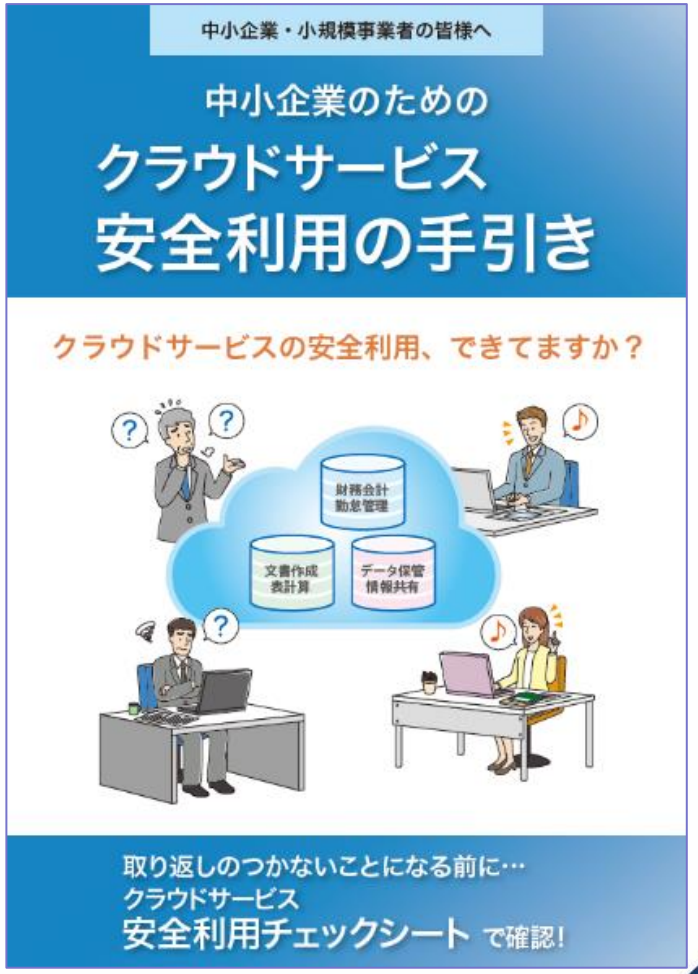
クラウドサービスのセキュリティ対策

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。



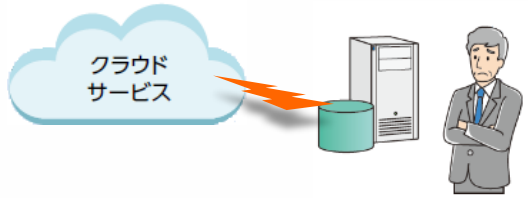
中小企業のための
クラウドサービス安全利用の手引き

- クラウドサービスを安全に利用するためには、何をやれば良いのか、を説明
  - **クラウドサービス安全利用チェックシート** ⇒ 確認すべきことの把握
  - 解説編 ⇒ 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**説明



選択するときの確認ポイント（抜粋）

1 2	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？
3 4 5	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？
6 7	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？
8 9 10	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？



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。

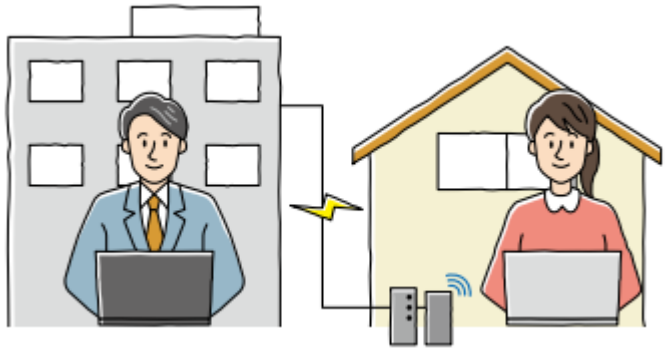
テレワークのセキュリティ対策

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。

- **VPN方式**
  - テレワーク端末から社内ネットワークに通信を暗号化して接続する方式
- **リモートデスクトップ方式**
  - テレワーク端末から社内パソコン等の端末に接続する方式
- **スタンドアロン（持ち帰り）方式**
  - テレワーク端末を社内ネットワークに接続せずに使用する方式
- **クラウドサービス方式**
  - インターネット上のクラウドサービスに直接接続する方式



テレワーク方式ごとのセキュリティ対策における留意点

- **VPN方式**
  - テレワーク端末にデータ保存が可能。端末の紛失や盗難、不正操作による情報漏えいリスク
  - 対策：テレワーク端末のハードディスクやSSDなどの暗号化やデータの遠隔消去等の対策
- **リモートデスクトップ方式**
  - 社内パソコンの画面をテレワーク端末画面に随時転送して遠隔操作。オフィスと同等の業務可能。社内パソコンからテレワーク端末にデータをコピーして保存することも可能→ 端紛失/盗難/不正操作による情報漏えいリスク
  - 対策：社内パソコンからテレワーク端末へのコピー制限。
- **スタンドアロン（持ち帰り）方式**
  - テレワーク端末にデータを保存→ 端末の紛失や盗難、不正操作による情報漏えいリスク
  - 対策：端末のハードディスクやSSDなどの暗号化やデータの遠隔消去等の対策。必要最低限のデータのみ許可を得て持出し。インターネット利用に際してはウイルスや不正アクセスへの対策等
- **クラウドサービス方式**
  - テレワーク端末から社内ネットワークを経由せず直接インターネットに接続
  - 通信の暗号化やサービスにログインするときの認証強化などの対策要
  - 使用するサービスのセキュリティ仕様を確認し、必要な対策を検討
  - テレワーク端末にウイルスソフト導入、ハードディスク・ SSD などの暗号化やデータの遠隔消去等の対策。
  - クラウドサービス上にデータを保存する場合、保存データ把握・管理する必要

【参考】テレワーク関連セキュリティ情報

- **総務省**
  - テレワークセキュリティガイドライン第5版（2021年5月）
  - 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）
  - https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
  - テレワークのセキュリティに関する相談対応体制の強化（2020年7月）
    https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00076.html

- **IPA**
  - 映像コンテンツ「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。
    - 再生時間：約10分
    - 公開日：2021/03/10

    https://www.youtube.com/watch?v=zDs88SLymwo

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

NEW

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf

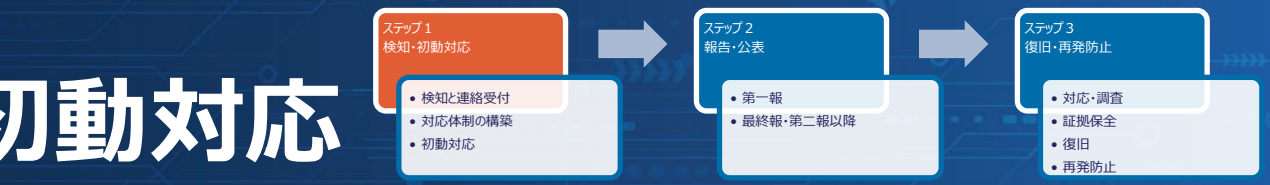
- インシデント対応時に整理しておくべき事項のリストや、「**検知・初動対応**」「**報告・公表**」「**復旧・再発防止**」といった基本ステップごとのアクションを提示
- 「**ウイルス感染・ランサムウェア感染**の場合」「**情報漏えい**の場合」「**システム停止**の場合」といった場合ごとに解説するほか、相談窓口や報告先も紹介

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

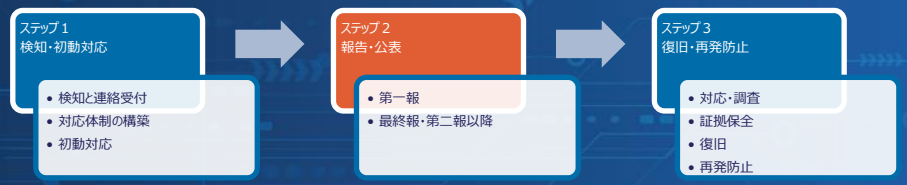
ステップ3
復旧・再発防止
- 対応・調査
- 証拠保全
- 復旧
- 再発防止

ステップ１ 検知・初動対応



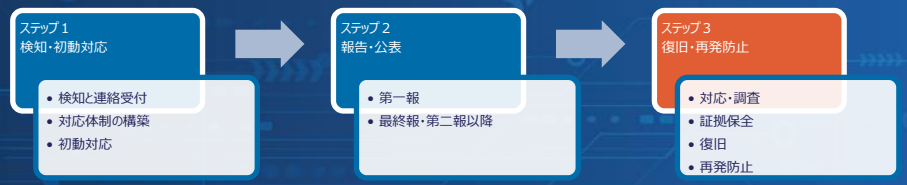
- **検知と連絡受付**
  - インシデントが疑われる兆候や実際の発生を発見した場合は、情報セキュリティ責任者に報告
  - 外部から通報を受け付けた場合は、通報者の連絡先等を記録。
- **対応体制の構築**
  - 情報セキュリティ責任者は、対応すべきインシデントであると判断したら、速やかに経営者に報告
  - 経営者は、インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者を定めて、役割分担を明確化
- **初動対応**
  - 初動対応として、対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を実施。ただし、対象機器の電源を切る等、不用意な操作でシステム上に残された記録を消さないよう注意

ステップ２ 報告・公表



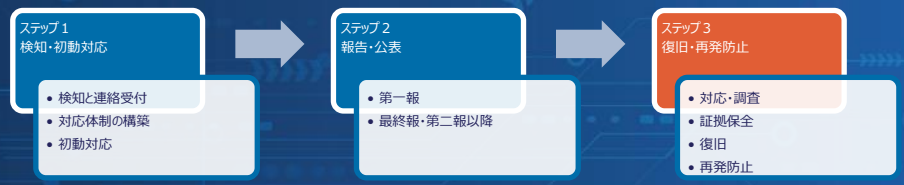
- **第一報**
  - すべての関係者への通知が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトや、メディアを通じて公表
    - 公表によって被害の拡大を招かないよう、時期、内容、対象などを考慮
  - 顧客や消費者に関係する場合は受付専用の問い合わせ窓口を開設し、被害が発生・拡大した場合にはその動向を速やかに把握し対応
- **第二報以降・最終報**
  - 被害者や、影響を及ぼした取引先や顧客に対して、インシデントの対応状況や再発防止策等に関して報告。また、被害者に対する損害の補償等を、必要に応じて実施
  - 個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、犯罪性がある場合は警察、ウイルス感染や不正アクセスの場合はIPAへ届け出

ステップ３ 復旧・再発防止



- **調査・対応**
  - 適切な対応判断を行うために、5W1H（いつ、どこで、誰が、誰を、何を、なぜ、どうしたのか）の観点で状況を調査し情報を整理
  - 対応方針を基に、原因を調査し、修正プログラムの適用、設定変更、機器の入替データの復元等、必要な修復を実施
  - 自社で対応が難しい場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的機関の相談窓口等に支援、助言を要請
  - 対応中、担当（責任）者は、状況や事業への影響等について経営者に適時報告

ステップ３ 復旧・再発防止



- **証拠保全**
  - 訴訟対応等を見越して事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバーやネットワーク機器のログ等の調査）を行います。
- **復旧**
  - 正しく修復できたことが確認できたら、停止したシステムやサービスを復旧します。
  - 復旧後は、経営者に対応結果を報告します。
- **再発防止**
  - インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善等、抜本的な再発防止策を検討し、実施します。

事象ごとの対応のポイント

- **ウイルス感染・ランサムウェア感染の場合**

  ウイルス感染やランサムウェア感染の場合は、まず感染したパソコンやサーバーの利用を停止し、ネットワークから切り離すことが重要です。特にランサムウェア対応においては、日頃から適切な方法でデータのバックアップを行っておくことが被害を最小限に抑えるポイントになります。

- **情報漏えいの場合**

  情報漏えいには、 ネットワークへの「不正アクセス」、従業員による「内部犯行」、電子メールの「誤送信」、Webでの「誤公開」、「紛失・置忘れ」等によるものがあります。特に、不正アクセスによる情報漏えいは、データの大量流出につながるおそれがあることから、インターネットに接続しているサーバへの対策が必要です。また、不正アクセスや内部犯行は犯罪性があるため、警察への届け出も必要になります。

- **システム停止の場合**

  システム停止の原因は、サイバー攻撃などのセキュリティの問題も含め、不具合・ソフトウェアのバグ、機器の故障、など様々な原因が想定され、異常の発見時には原因がわからないことがあります。原因がわからない場合は、セキュリティの問題の可能性も含めて対応を行う必要があります。また、システムの停止は事業や企業経営に重大な影響を与える場合があるので、経営者は事業継続計画（BCP）を策定し、これに備える必要があります。

インシデント対応時に整理しておくべき事項

インシデントの分類	情報漏えい 、ウィルス感染、システム停止など
事業者	事業者の名称 ※自社の受託案件に関連したインシデントの場合は委託元含む関係事業者の名称
担当者・責任者	本件に関する責任者および担当者の所属、氏名
発覚日時	インシデントを認知した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定される原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要・詳細
システム構成・運用状況	システムの物理的所在地やOS、アプリケーションとバージョン構成 ※可能であれば簡単な構成図等も併記 システムの運用状況やセキュリティツール・サービスの利用状況等

※サイバーセキュリティ経営ガイドライン 付録C「ンシデント発生時に組織内で整理しておくべき事項」も参考になります
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

有事に向けた「仕組み」による対策

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**不可欠なサービスをワンパッケージ**で要件化した**民間サービス**の登録制度。2021年4月から開始
- 現在**35社**から**45サービス**が展開
- **IT導入補助金（セキュリティ対策推進枠）**が利用可能

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

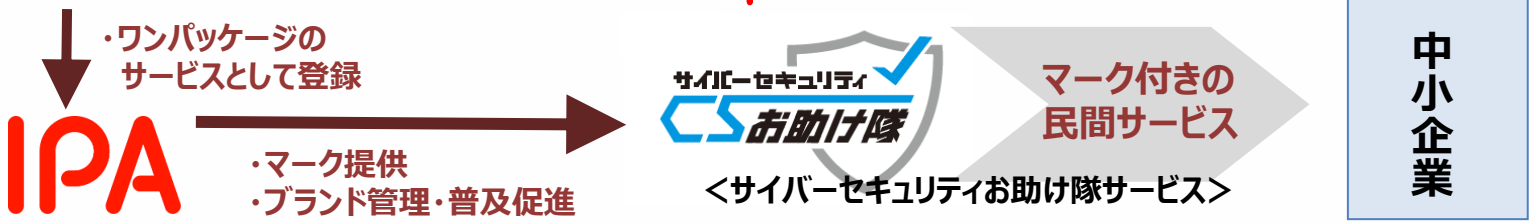
24時間見守る仕組み
ネットワーク監視型
端末監視型
その併用型

緊急時の対応支援
インシデント発生などの緊急時に駆け付け支援

導入・運用のしやすさ
専門知識がなくても導入・運用できるような工夫

簡易サイバー保険
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

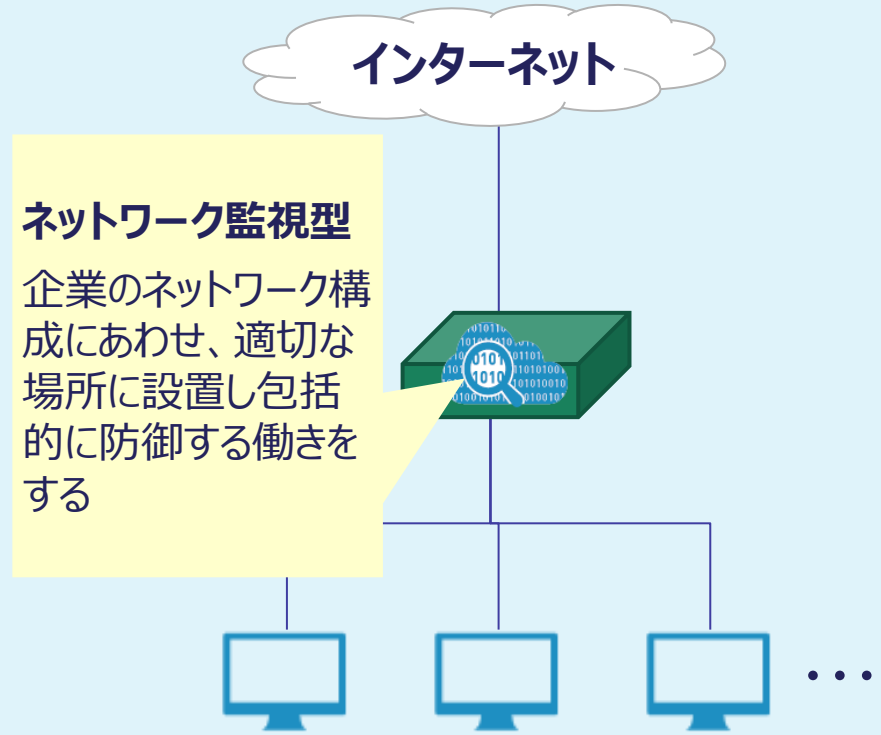
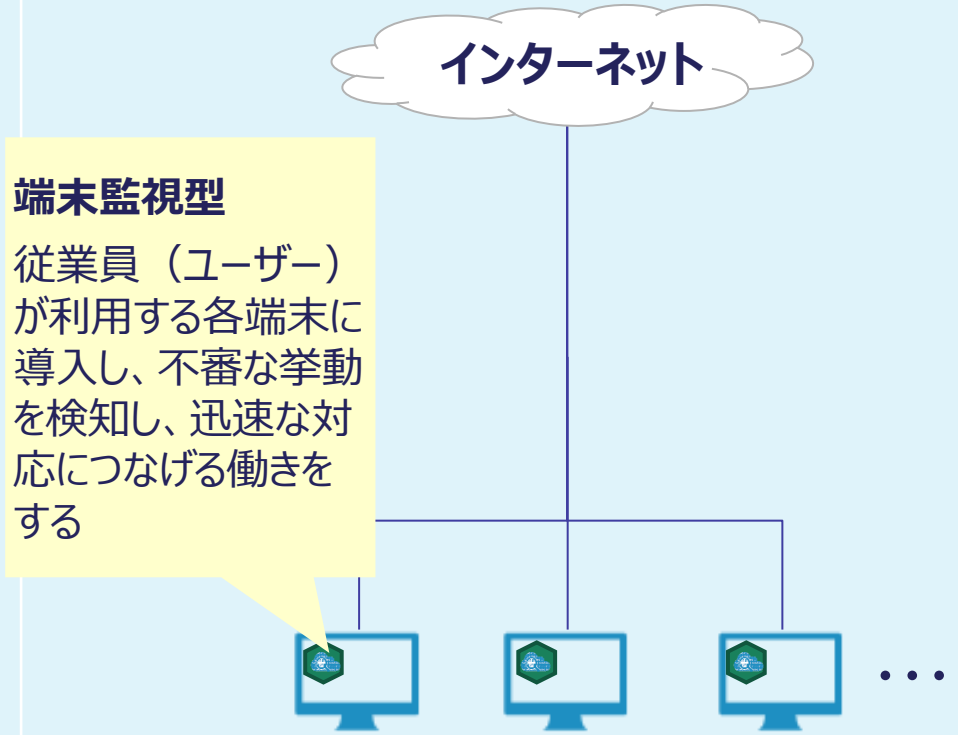
中小企業でも導入、維持できる価格
・ネットワーク監視型：月額１万円以下
・端末監視型：月額2,000円以下／台
・併用型：これらの合算相当価格以下



「サイバーセキュリティお助け隊サービス」

異常の監視の仕組み

- セキュリティ対策では、目に見えないサイバー攻撃を可視化し、**侵入等の異常に素早く気付くことがもっとも大切**。
- サイバーセキュリティお助け隊サービスでは、**ネットワーク監視型**、**端末監視型**、またはその**両方（併用型）**による異常の監視を提供。

	ネットワーク監視型	端末監視型
構成		

セキュリティ監視の仕組みの選び方
どれを選べばいいのか？ <<監視型による特長と選ぶ時のポイント>>

監視型	説明	
	特長	選ぶ時のチェックポイント
ネットワーク監視型	（一般的に）**インターネットと社内ネットワークの間にUTM等の監視機器**を設置し、**ネットワーク通信（内外）の監視、防御**する形態のもの	
	【メリット】 • **機器1台で監視が可能**なため、設定やバージョンアップ等の更新作業などの運用を従業員一人一人が行う必要がなく、**運用コスト、業務負担が軽い**。（セキュリティ管理者のみの対応）	**自社のネットワーク負荷が耐えられるか** • **内外の通信を監視**するため、機器導入により**メールの送受信に時間**がかかったり、**ネットワーク接続に遅延**が生じたりする可能性があるため確認が必要。
端末監視型	（一般的に）社内**ネットワークに接続しているPC**に、**EDR等のセキュリティソフトウェアをインストール**して、**端末内部の挙動を監視、防御**する形態のもの	
	【メリット】 • 社外での打ち合わせであったり、**テレワーク勤務**など、**社内ネットワーク外に持ち出されたPCであっても監視が可能。**	**社内ネットワークに接続しているPC台数と導入可能か** • 導入する**PC台数に応じてコストが高く**なるため、社内ネットワークに接続しているPC台数の確認と、**セキュリティソフトによってはインストールできない**PCもあり得、自社のPCに導入可能かの確認が必要。
併用型	ネットワーク一括監視型と端末監視型の両方を設置し、**多層的に防御**を行う形態のもの	
	【メリット】 • **より強固**なセキュリティ監視が可能。	**運用の手間の確認を** ネットワーク一括監視型、端末監視型の**それぞれを導入することの運用の手間・コストが発生**(セキュリティ管理者、従業員それぞれの対応が必要）。対応可能か確認が必要。

【お助け隊サービス】中小企業ユーザーの主な声

＜サイバーセキュリティお助け隊サービスについて中小企業から寄せられた声＞

●自社の対策が不十分であることにより、**取引先に迷惑をおかけするわけにはいかない**ため、サイバーセキュリティお助け隊サービスの導入を決めた。

●検知・監視してくれるだけでなく**何かあった時の事後対応まで含まれる**ところがよい。セキュリティについて全く分からないので、**まとめてお任せできるところにお願いしたい**と考えていた。

●アラート通知が来るので、**防御できていることが実感でき安心**。本社のほか複数の拠点でも利用しているが**サービス利用料が安い**ので助かっている。

●**何も無いということがわかる**ことも良い点。**セキュリティレポートをストックしておくことで、報告資料としても使える**ので助かっている。

※サイバーセキュリティお助け隊サービス提供事業者　提供情報より

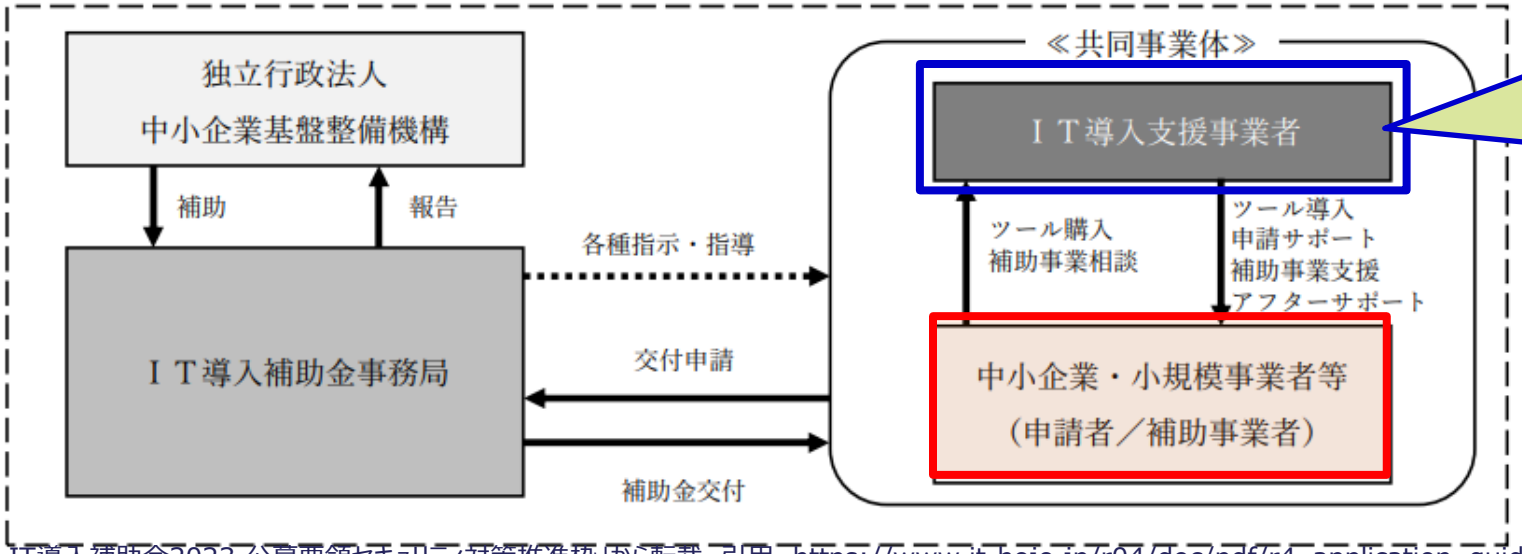
IT導入補助金2023　セキュリティ対策推進枠

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～100万円
補助率	1/2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	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2023」**
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

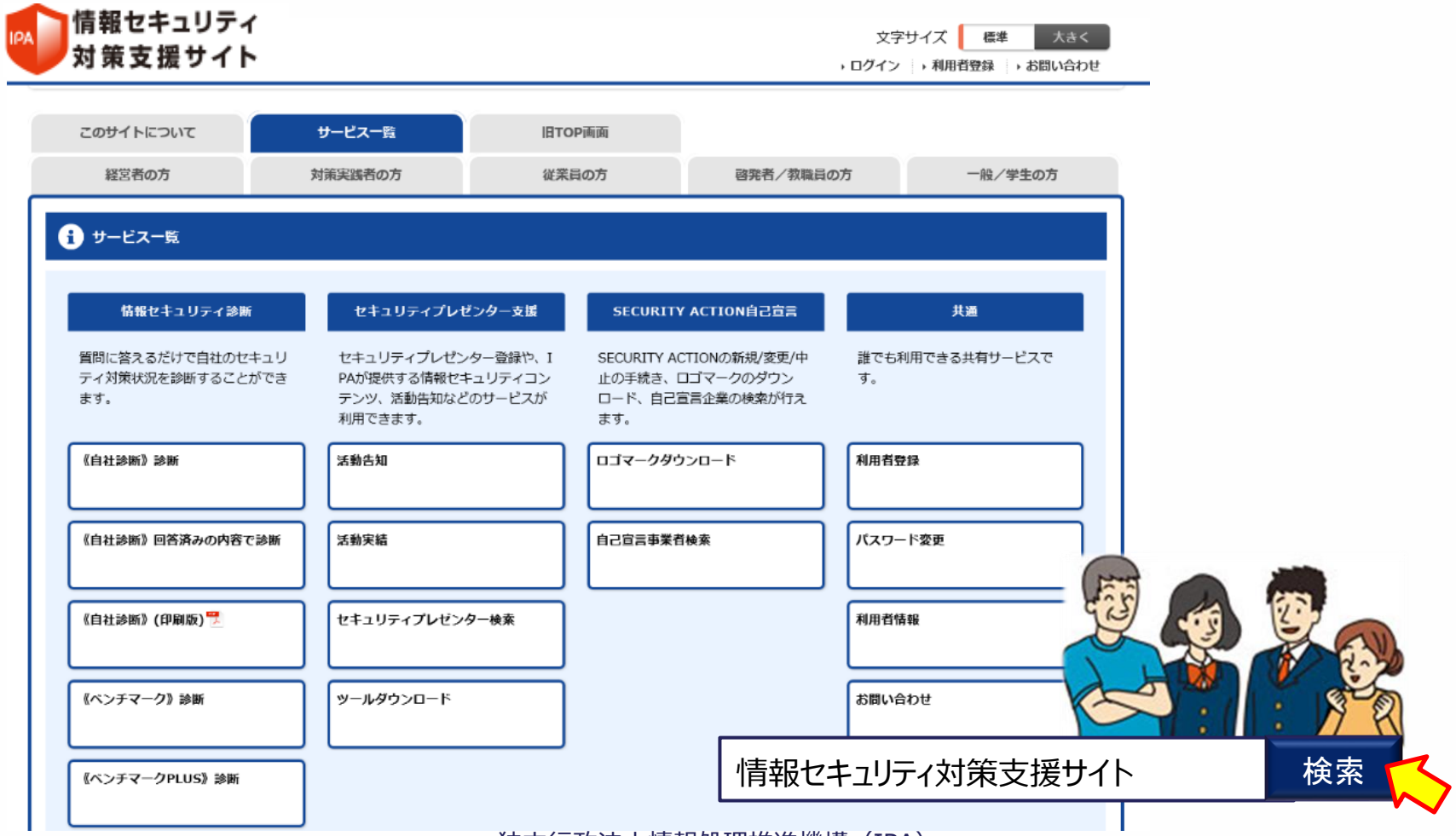
【ご参考】IPAが提供する ツール、制度等

【参考】IPAの提供ツール、制度等

情報セキュリティ対策支援サイト

https://security-shien.ipa.go.jp/

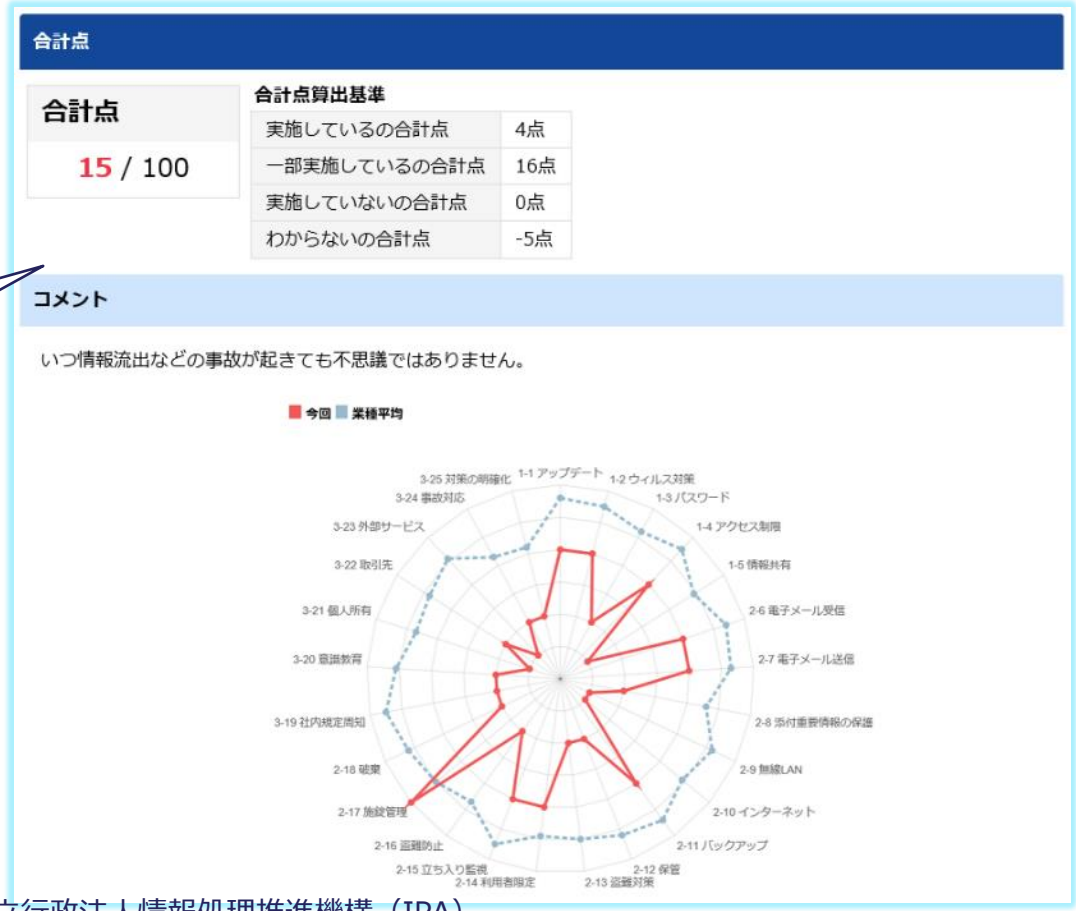
- 情報セキュリティ対策を、「**知**りたい」「学びたい」「**始**めたい」「**続**けたい」の方々をサポート



【参考】IPAの提供ツール、制度等
オンライン版5分でできる！情報セキュリティ自社診断
https://security-shien.ipa.go.jp/diagnosis/selfcheck/

- 自社のセキュリティ状況をオンラインで診断。
- オンライン版では、過去の診断結果や同業他社との比較も可能。

オンラインで回答すると
自動で採点します

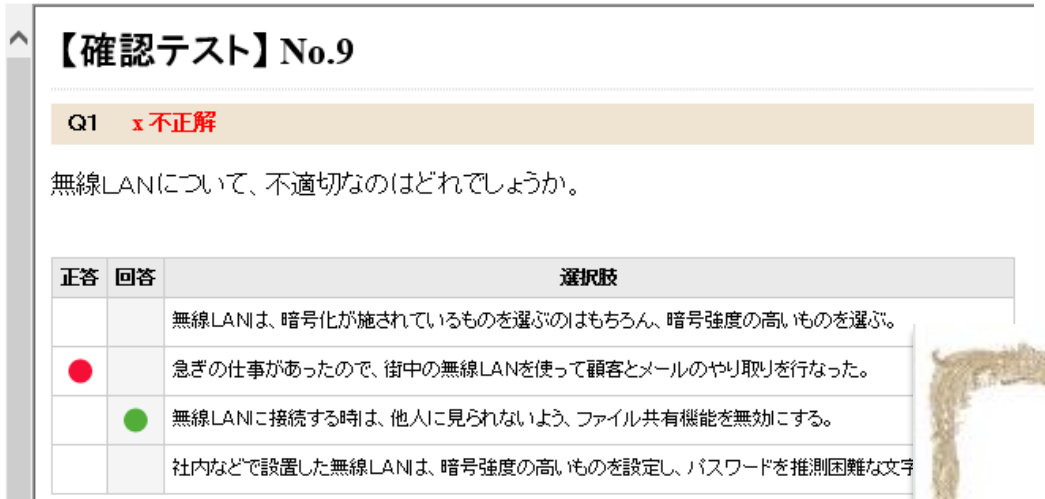


【参考】IPAの提供ツール、制度等

5分でできる！ポイント学習

https://security-shien.ipa.go.jp/learning/

- インターネット接続環境があれば、**いつでもどこでも学習可能**な、eラーニングシステム
- １テーマ**5分**。情報セキュリティ自社診断と連動



修了証も発行できます!!

映像で知る情報セキュリティ

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

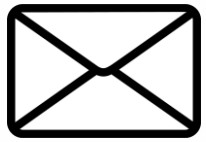
- 情報セキュリティに関する様々な脅威と対策を**10分程度のドラマなど**で分かりやすく解説した映像コンテンツ**33タイトル。**YouTube「**IPAチャンネル**」では全タイトルをいつでも視聴可能
  - 累計再生回数**約531万回**（2023年3月末現在）
- **社内研修等**営利を目的としない用途に限り、主な映像の**動画ファイルを無償で提供**（DVD/ダウンロード）

● 主な映像コンテンツ

	**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

IPA　映像　検索

⑥ 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。

Twitter公式アカウント https://twitter.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/

組織における内部不正防止ガイドライン

https://www.ipa.go.jp/security/guide/insider.html

- 内部不正防止の重要性や対策の体制、関連する法律などの概要を平易な文体で説明。
- 「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の10の観点のもと、合計33項目からなる具体的な対策の提示
- 各対策項目では、「対策の指針」を冒頭に記し、対策しない場合のリスクと、具体的な対策のポイントを整理する構成
- 内部不正の事例のほか、自組織の内部不正対策の状況を把握するための33項目のチェックシート、対策のヒントとなるQ&A集などを付録として用意

【参考】IPAの提供ツール、制度等

情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html

- 一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する**技術的な相談**に対してアドバイスを提供する相談窓口。
- 相談に対して、**事象の分析や助言**を行うほか、相談内容から判明したトラブルの**傾向、手口、対策に関する情報の公開**により、国民のセキュリティリテラシーの向上と対策の促進を実施。

電話 **03-5978-7509**

平日10:00-12:00 、13:30-17:00

メール **anshin@ipa.go.jp**

ポータル IPA安心相談 検索

ご清聴
ありがとう
ございました