中小企業へのセキュリティ支援の取り組み

2025年3月

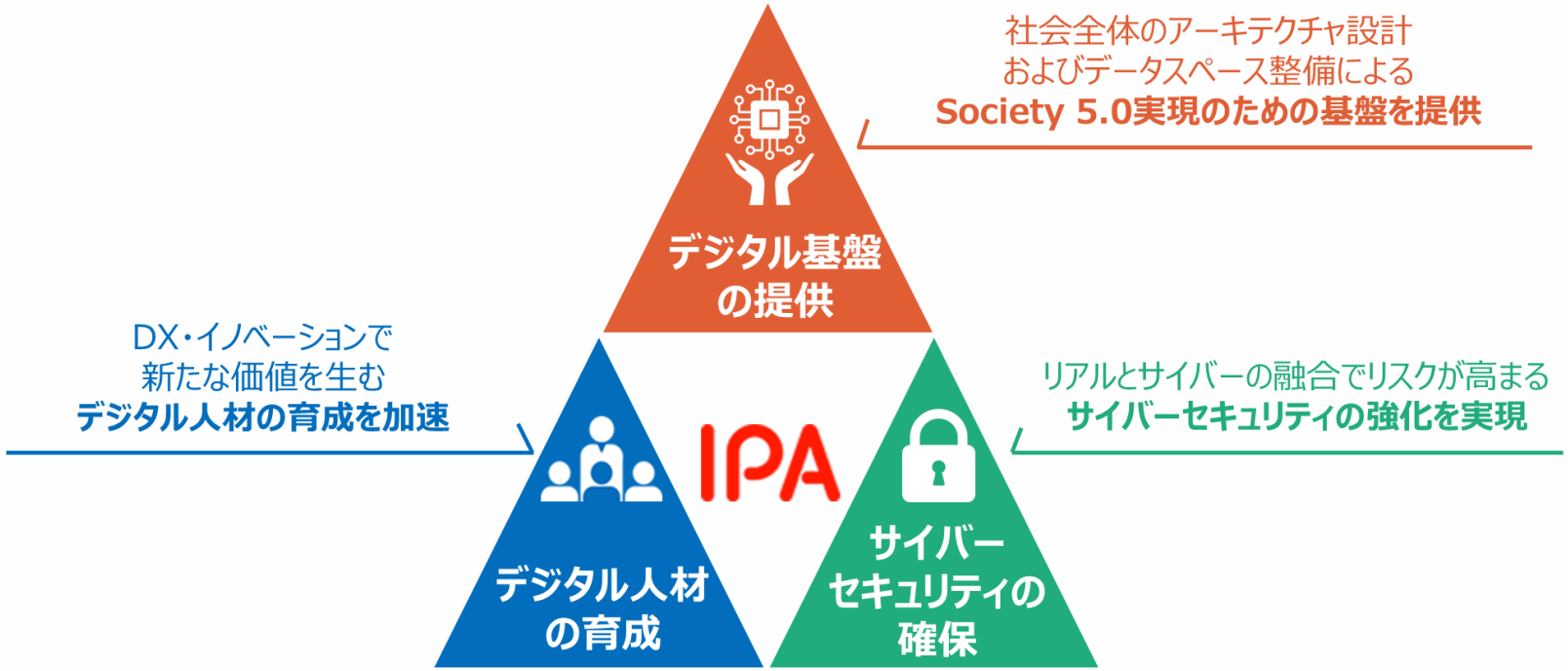
独立行政法人情報処理推進機構（IPA）
セキュリティセンター　普及啓発グループ

IPA Better Life with IT

独立行政法人情報処理推進機構（IPA）とは

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**

サイバーセキュリティに関する業務概要

平時からインシデント発生時まで、サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施。

普及啓発・リテラシー向上支援

- 情報セキュリティ10大脅威、情報セキュリティ白書
- 経営者、社内担当者向け各種ガイドライン・教育コンテンツ
- 地域・中小企業支援
- 情報セキュリティ安心相談窓口
  10,923件（2023年）

SECURITY ACTION
セキュリティ対策自己宣言
累計宣言数約40万者
（2025年3月）

サイバー事案対応（検知・分析・対処調整）

- サイバー情勢分析
- 国家支援型サイバー事案対策
- 情報共有（サイバー攻撃情報・脆弱性）
- セキュリティ監視（独法等）
- サイバー事故原因究明

IPA J-CRAT
2011年創立　341件支援（2023年）

J-CSIP Initiative for Cyber Security Information sharing Partnership of Japan

JVN iPedia
脆弱性データベース
約20万件登録（2024年3月）

セキュリティ基準・評価認証

＜製品・サービスのセキュリティ評価・認証＞ CRYPTREC Cryptography Research and Evaluation Committees

- 暗号技術調査/IT製品ISOセキュリティ認証
- IoT製品セキュリティラベリング（JC-STAR）
- クラウドサービスセキュリティ評価（ISMAP）

＜セキュリティ基準・分析・監査等＞ JC-STAR

- 制御システムセキュリティリスク分析
- サプライチェーンセキュリティ評価
- 独法等情報セキュリティ監査、政府システム監査

人材育成

- 国家資格「情報処理安全確保支援士」
  登録者数21,727名（2023年10月1日時点）
- 中核人材育成プログラム
  累計435名受講（2017年～）
- 若手人材発掘（セキュリティ・キャンプ）
  累計1,073名受講（2004年度～）
- 情報セキュリティコンクール
  応募約５万点（2023年度）

中小企業へのセキュリティ支援の取り組み

ISECの産業界・経済界とのネットワーク

事業者 セキュリティ自己宣言制度

中小企業による自主的な
セキュリティ強化に取組の認定者

宣言数 約39万組織

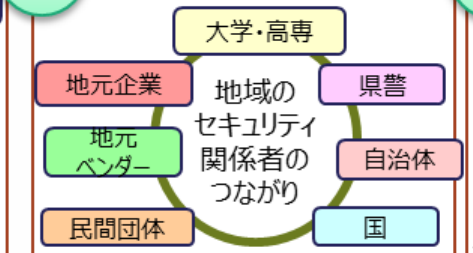
支援組織 情報セキュリティ対策普及推進協議会

【参加団体】
中小企業診断協会　ITコーディネータ協会
全国商工会連合会　日本商工会議所
全国中小企業団体中央会　日本税理士会連合会

日本ネットワークセキュリティ協会
全国社会保険労務士会連合会
情報処理推進機構
中小企業基盤整備機構

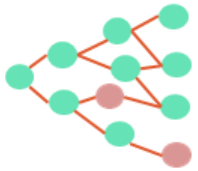
10団体

地域 地域SECUNITY



全国42コミュニティ

サプライチェーン サプライチェーン・セキュリティ・コンソーシアム（SC3）



会長：
遠藤信博 経団連サイバーセキュリティ委員長
参加団体例：
日本自動車工業会、電気事業者連合会、日本商工会議所、全国地方銀行協会 ほか

サプライチェーン全体でのセキュリティ推進運動

173組織

専門家 セキュリティプレゼンター

普及啓発専門家登録バンク

登録数 約1,800名

J-CSIP

NDAを締結し、IPAが情報ハブとなり組織間・Special Interest Group(SIG)間での情報共有を実施

重要インフラ機器製造業者SIG 重工・重電など〔１４組織〕	電力業界SIG 電力ISAC＋電力関連組織〔４６組織〕	ガス業界SIG 日本ガス協会＋ガス事業者〔７９組織〕	業界内の情報共有活動を支援
資源開発業界SIG 石油鉱業連盟＋鉱業会社〔５組織〕	自動車業界SIG 自動車関連団体・企業〔１０組織〕	クレジット業界SIG 日本クレジット協会＋クレジット会社〔４７組織〕	医療業界情報連携体制 医療関連団体〔４組織〕＋団体会員
石油業界SIG 石油連盟＋石油会社〔６組織〕	化学業界SIG 日本化学工業協会＋化学会社〔２４組織〕	鉄鋼業界SIG 日本鉄鋼連盟＋鉄鋼会社〔４組織〕	水道業界情報連携体制 水道関連事業者等〔９組織〕
航空業界SIG 航空関連団体・企業〔７組織〕	物流業界SIG 物流関連団体・企業〔１２組織〕	鉄道業界SIG 鉄道関連団体・企業〔１９組織〕	エアポート業界SIG 空港関連組織〔６組織〕

中小企業
サプライチェーン
地域

重要インフラ
製造業

IPA

一般ユーザー

告示・制度

ウイルス届出	不正アクセス届出
脆弱性届出	暗号

支援組織と連携した普及活動

- 「中小企業の情報セキュリティ対策普及の加速化に向けた共同宣言」を発表

2017年2月7日、一般社団法人中小企業診断協会、全国社会保険労務士会連合会、全国商工会連合会、全国中小企業団体中央会、特定非営利活動法人ITコーディネータ協会、特定非営利活動法人日本ネットワークセキュリティ協会、独立行政法人情報処理推進機構、独立行政法人中小企業基盤整備機構、日本商工会議所、日本税理士会連合会は、中小企業におけるITの利活用拡大に向け、中小企業における情報セキュリティへの意識啓発及び自発的な対策の策定、実践を促進するため、連携して活動することを宣言しました。

- **中小企業の情報セキュリティ普及推進協議会**を設置し、活動を推進

“自発的な情報セキュリティ対策を促す”ための核となる取り組み

SECURITY ACTIONの宣言企業拡大

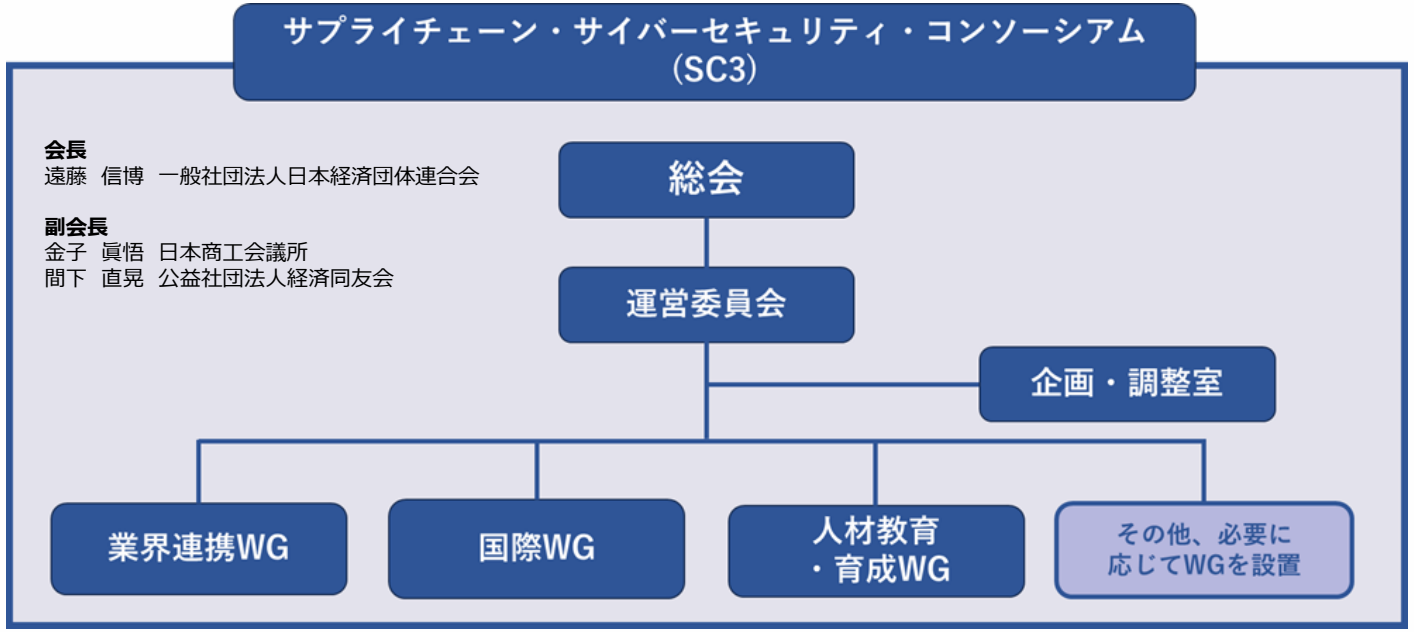
取組１
中小企業向け
普及・啓発活動の推進

取組２
中小企業の情報セキュリティ
に関する相談への対応強化

取組３
中小企業の情報セキュリティ
強化に向けたツールの提供

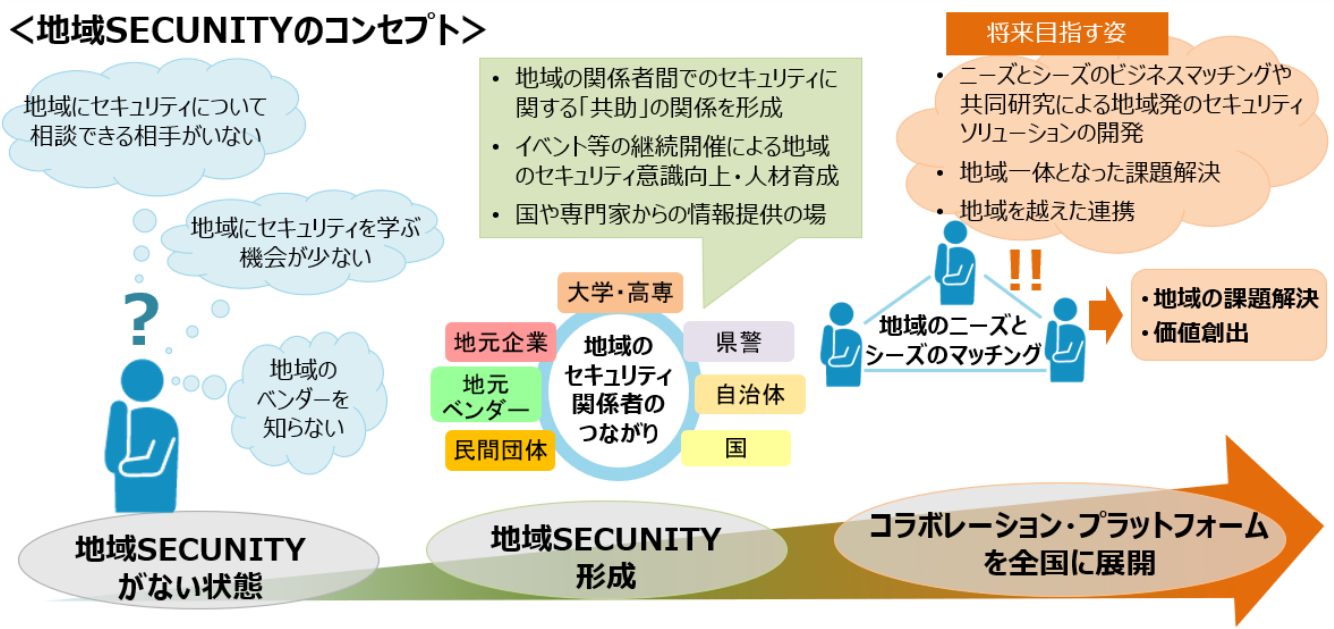
業種・業界団体と連携した普及活動

- 産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的とした「**サプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）**」の活動を支援することで、中小企業を含む日本のサプライチェーン全体でのサイバーセキュリティ対策の強化に向けた取組を推進



地域と連携した普及活動

- 地域の民間企業、行政機関、教育機関、関係団体等が、セキュリティについて語り合い、「共助」の関係を築くコミュニティ「**地域SECUNITY**」の形成支援等を通じ、各地域での取り組みを促進
- 全国42コミュニティの支援を中心に、セミナー支援44回、講師派遣65回、全国連絡会1回などを実施



セキュリティ専門家と連携した普及活動

- IPAのセキュリティ対策資料を活用して、 中小企業等に対して普及啓発を行う人材を登録する「**セキュリティプレゼンター**」制度を運用し、活動を支援することで普及活動を推進
- 登録数　約1,800名
  （情報処理安全確保支援士749名、ITコーディネータ662名、中小企業診断士226名）
- 活動例
  - IPA資料を活用した情報セキュリティ対策セミナーの開催・講演
  - IPA資料に基づく情報セキュリティ対策の助言
  - IPA資料の配布を通じた情報発信、普及啓発

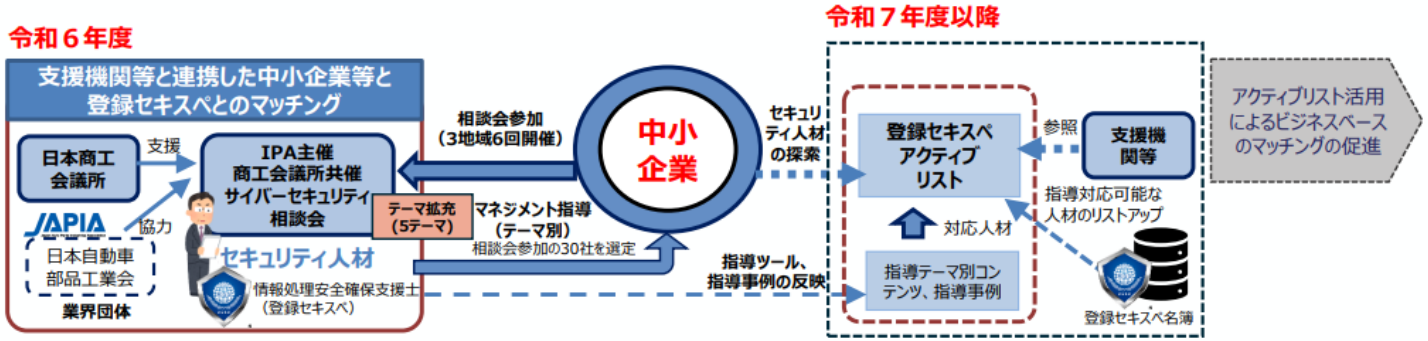
【参考】セキュリティ人材活用促進事業

（参考１）令和５年度補正予算事業（セキュリティ人材活用促進事業）

- 商工会議所等の**支援機関等を通じた効果的な登録セキスペの広報周知の方法**や、**中小企業と登録セキスペの効率的なマッチング方法**について検証。
- 全国各地の多様な**支援機関等が当該場の提供を国費に頼らず自前で実施できるような**（＝支援機関等がマッチング裨益者から対価を得られる）**方策**についても模索。

事業概要

- 支援機関（商工会議所）等と連携した中小企業向けサイバーセキュリティ相談会を３地域計６回開催。
- 相談会参加の中小企業等30社程度に対して、登録セキスペによるマネジメント指導を実施。
- 中小企業等のセキュリティコンサルが対応可能な登録セキスペのリスト（アクティブリスト）について検討。



（出典）経済産業省 産業サイバーセキュリティ研究会WG2

中小企業支援組織向け研修（ダイジェスト）

中小企業支援組織向け講演者派遣

中小企業に対する**情報セキュリティ対策に関する指導力の向上を目的**として、
中小企業への支援を行う組織の経営指導員向け(※)の研修及びイベント等に対し、
情報セキュリティ対策に関する講演者を無償で派遣します。※2025年度は6月頃から開始予定
https://www.ipa.go.jp/security/seminar/koushihaken/sme-shien.html

派遣対象組織	以下の各地域の中小企業支援組織 • 商工会連合会、商工会 • 商工会議所連合会、商工会議所 • 中小企業団体中央会 • 税理士会 • 社会保険労務士会 • 中小企業診断協会 • よろず支援拠点
講演時間	60～120分（標準）
講演費用	無償（講演料、旅費交通費はIPA負担）
講演テーマ	• 情報セキュリティの最新動向 • 中小企業の情報セキュリティ対策ガイドラインを活用した指導方法と身近な対策例 • IPAの中小企業支援策・対策支援ツールの紹介 など 注：研修及びイベントの趣旨や受講者層にあわせ講演内容の調整が可能です

(※)各団体が主催する中小企業向けセミナーへの講師派遣や開催支援も提供

講演の流れ

情報セキュリティの最新動向
を解説

ガイドラインを活用した指導方法と
身近な対策例を紹介

IPAの中小企業支援策や
対策支援ツールを紹介

※講演実施時には、支援者が中小企業向け指導に活用できる資料・教材や対策支援ツール等をご提供します。

情報セキュリティの最新動向

情報セキュリティの動向を知るには…

情報セキュリティ10大脅威を活用してください

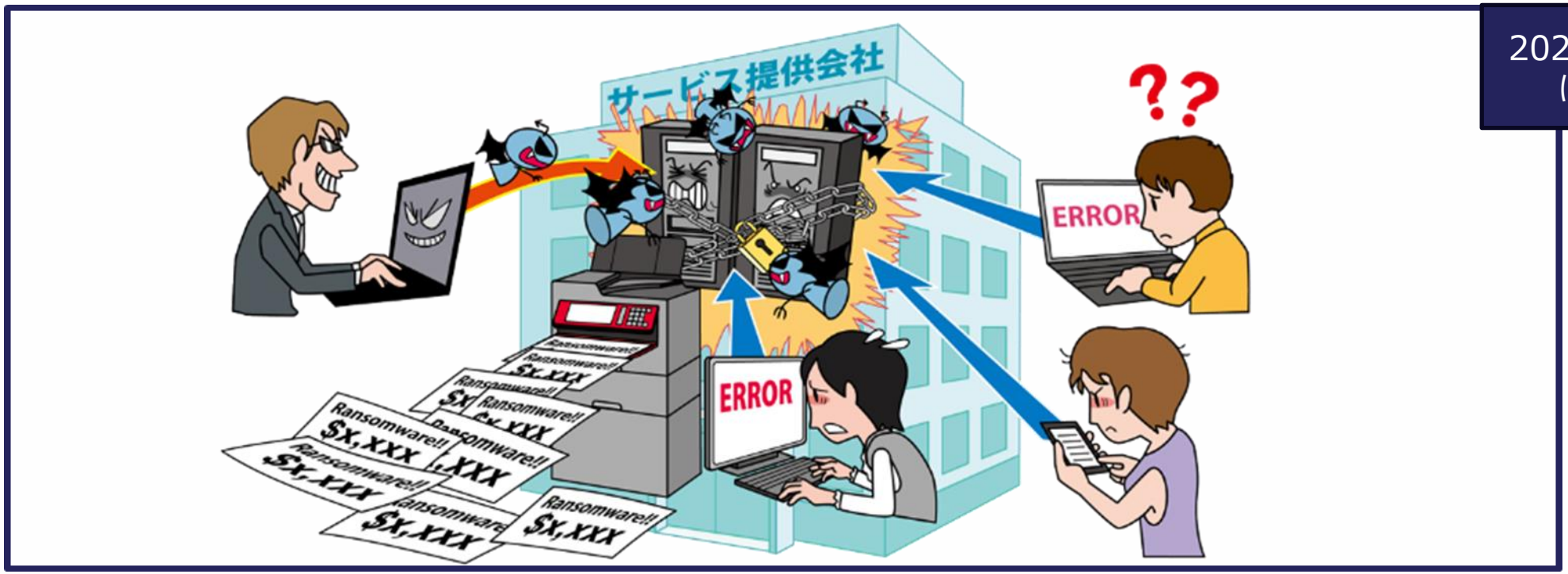
- IPAが2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等から **IPAが脅威候補を選出**
- セキュリティ専門家や企業のシステム担当等から構成される**「10大脅威選考会」が投票**
- **TOP10入りした脅威を「10大脅威」**として脅威の概要、被害事例、対策方法等を解説

情報セキュリティ10大脅威 2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い	昨年順位
1	ランサム攻撃による被害	2016年	10年連続10回目	1
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目	2
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目	5、7
4	内部不正による情報漏えい等	2016年	10年連続10回目	3
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目	4
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目	9
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出	圏外
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目	圏外
9	ビジネスメール詐欺	2018年	8年連続8回目	8
10	不注意による情報漏えい等	2016年	7年連続8回目	6

【1位】ランサムウェアによる被害

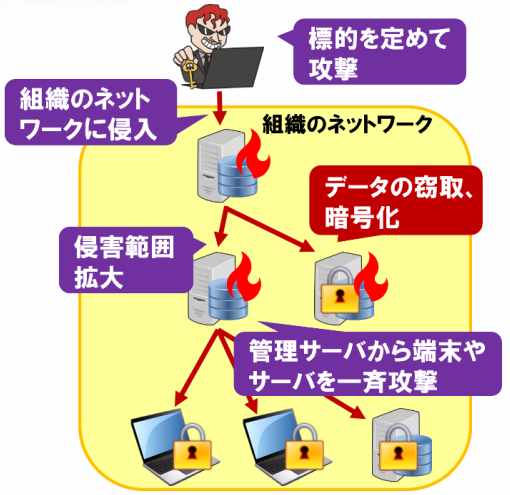
2025年版簡易説明資料は3月末公開予定

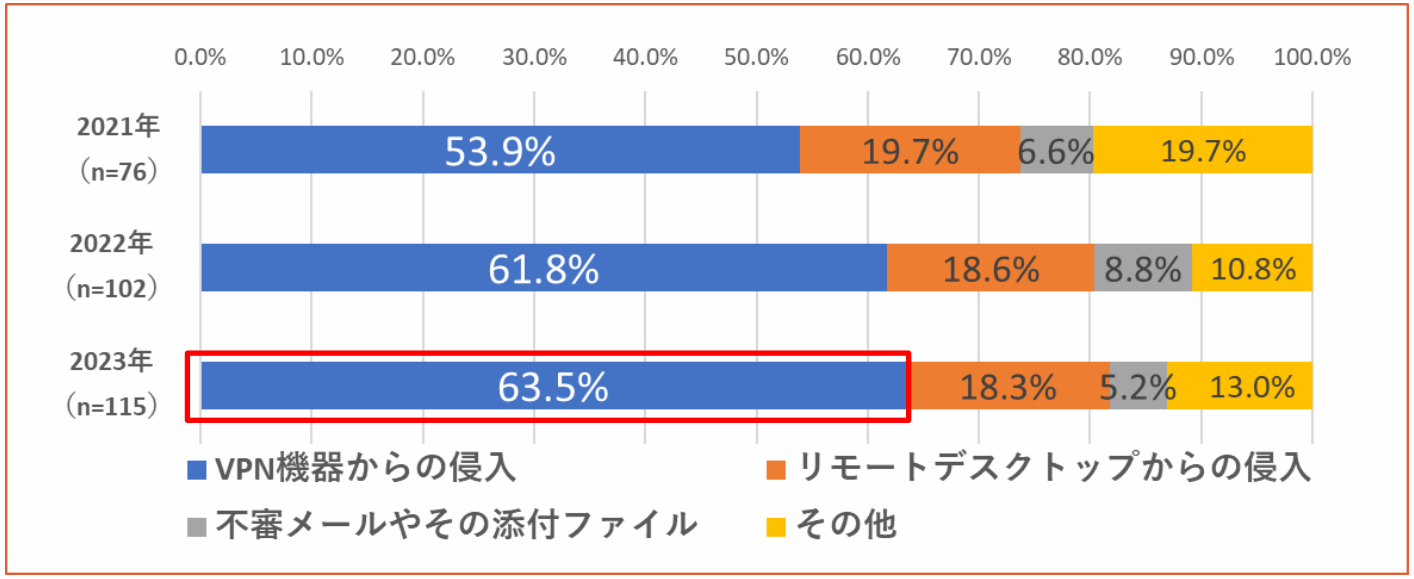


- PC等に保存されているファイルが暗号化され、使用不可にされる
- 復旧と引き換えに金銭を要求される
- 情報が窃取されて、公開され、さらに攻撃を受けている事をビジネスパートナー等に公表すると脅迫されるケースもある
- 組織の規模や業種に関係なく攻撃される

【参考】ランサムウェアの感染(侵入)経路

- **VPN(※)機器からの侵入が60%以上**
  - VPN機器の脆弱性の悪用
  - 脆弱なパスワード
  - 過去に流出したパスワードの悪用





ランサムウェアの感染経路（2021～2023 年）

(※)VPN：Virtual Private Network
テレワーク等で使われる、外部から安全に内部ネットワークに接続するための仕組み

出典）情報セキュリティ白書2024（2021～2023 年の警察庁資料を基にIPA が作成）

【1位】ランサムウェアによる被害

2025年版簡易説明資料は3月末公開予定

- **攻撃手口**

・ウイルス(ランサムウェア)に感染させて金銭を要求

- **脆弱性を悪用した手口**
  - ネットワーク機器やソフトウェアの脆弱性を悪用しウイルスを実行(感染させる)
  - 攻撃ツール等を利用してネットワーク越しに次々と感染させる

- **不正アクセスによる手口**
  - 意図せず公開されているポート(リモートデスクトップ等)からサーバーに不正アクセスさせる
  - サーバー上で攻撃者がウイルスを実行させる(感染させる)

【1位】ランサムウェアによる被害

2025年版簡易説明資料は3月末公開予定

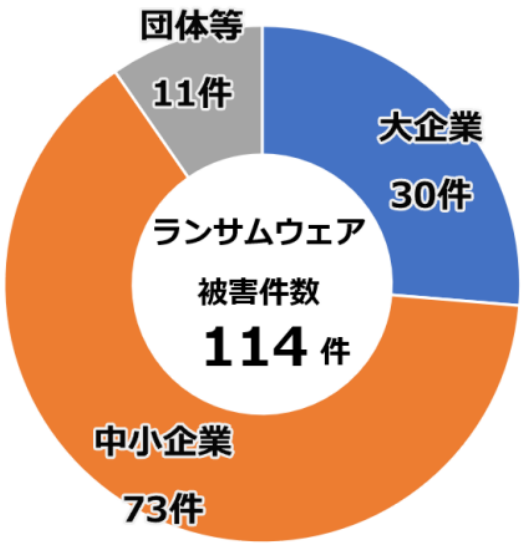
- **攻撃手口**

・ウイルス(ランサムウェア)に感染させて金銭を要求

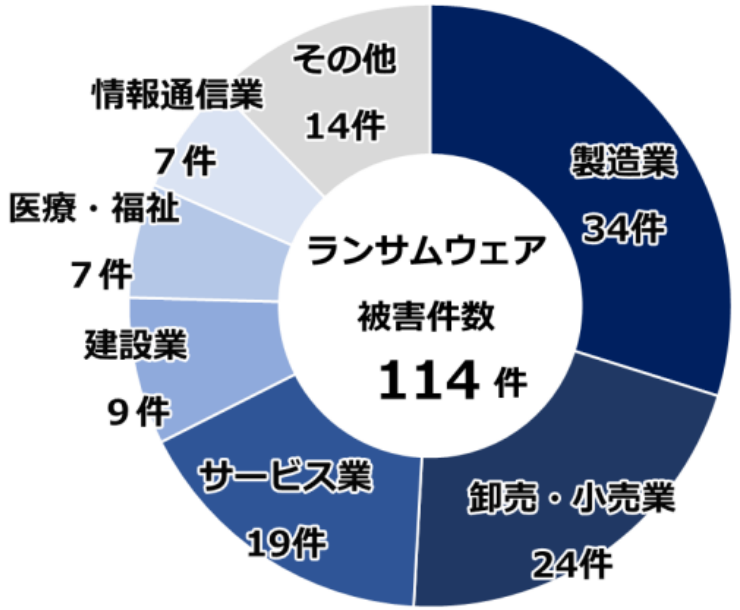
- **メールを悪用した手口**
  - 不正な添付ファイルを開かせる
  - メール内のリンクをクリックさせる
- **Web サイトを悪用した手口**
  - ランサムウェアをダウンロードさせるようにWebサイトを改ざんした
    当該サイトを閲覧するようにメールなどで誘導した

【参考】ランサムウェアによる被害の発生状況

- 中小企業の被害が半数以上
- 業種も不問



被害企業・団体の規模別の被害報告件数（2024年上半期）



業種別の被害報告件数（2024年上半期）

【出典】令和６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/R6kami/R06_kami_cyber_jousei.pdf

【1位】ランサムウェアによる被害

2025年版簡易説明資料
は3月末公開予定

- **2023年の事例/傾向①**
  - **ランサムウェア感染による業務停止**
    - 2023年7月、名古屋港統一ターミナルシステムが
      ランサムウェアに感染した
    - リモート接続機器の脆弱性を悪用した
      不正アクセスが原因であった
    - 物理サーバー基盤および全仮想サーバーが暗号化されている
      ことが判明した
    - 約2日半、ターミナルでの作業停止を余儀なくされた

【1位】ランサムウェアによる被害

2025年版簡易説明資料は3月末公開予定

- **2023年の事例/傾向②**
  - **ランサムウェア感染によるサービス提供停止**
    - 2023年6月、エムケイシステムのデータセンターのサーバーが不正アクセスされ、ランサムウェアに感染した
    - データが暗号化され、社会保険労務士向けクラウドサービス「社労夢」をサービス提供できなくなった
    - 約3,400人のユーザーに影響があり、オンプレミスで動作するパッケージ版が代替として提供された
    - インフラ設備の再構築費用などがかかったため、エムケイシステムは業績予想を下方修正した

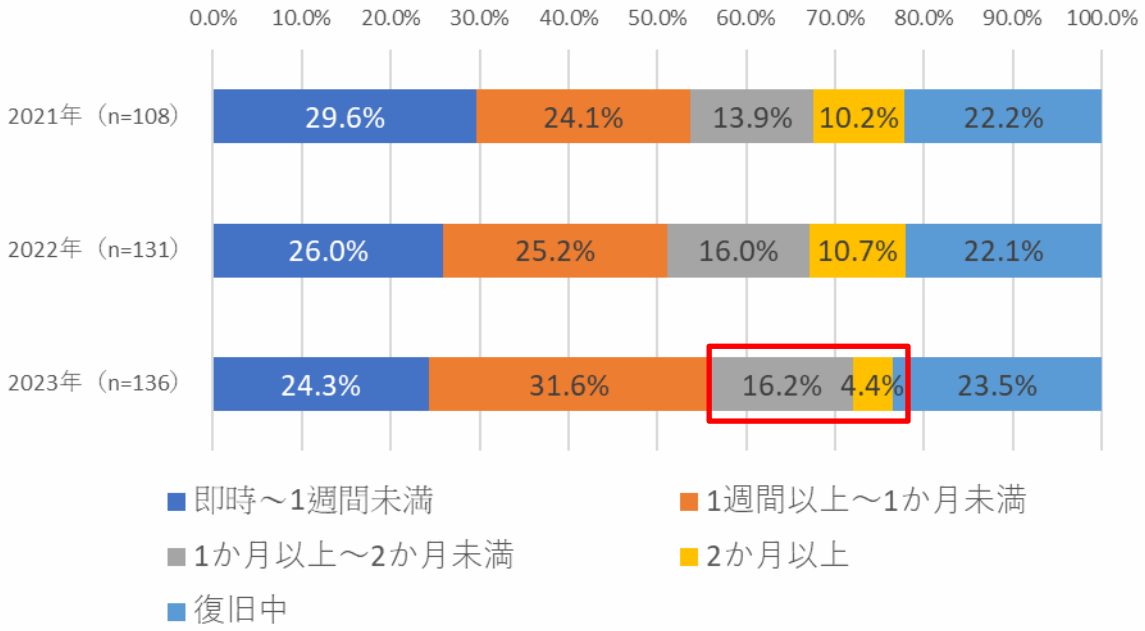
【1位】ランサムウェアによる被害

2025年版簡易説明資料は3月末公開予定

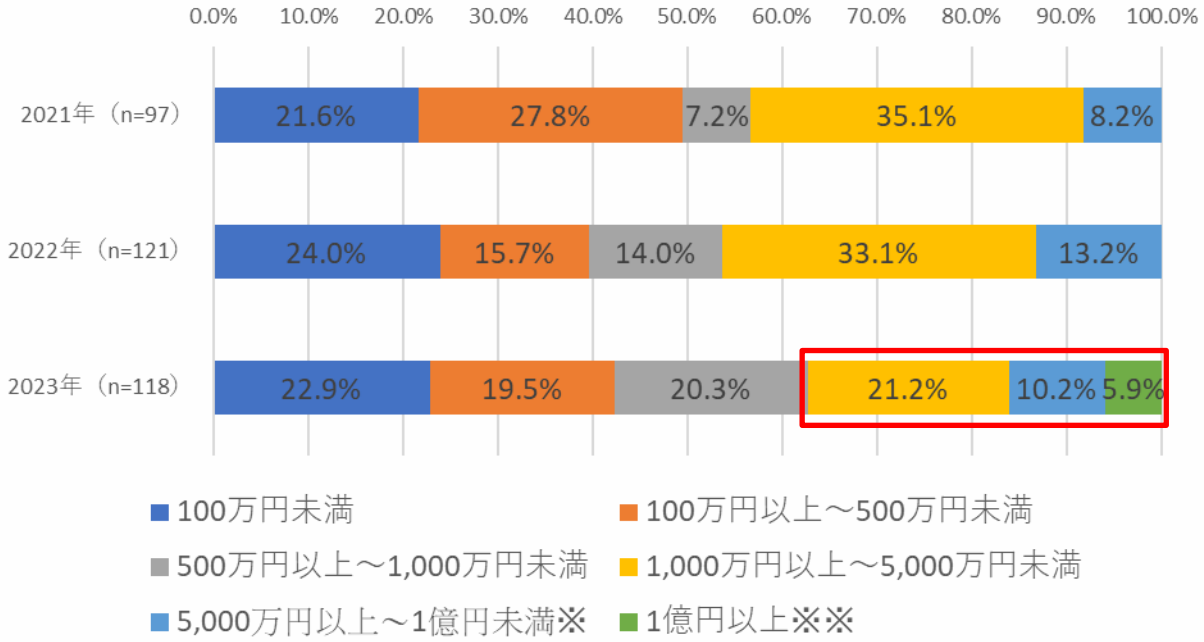
- **2023年の事例/傾向③**
  - **VPN経由で侵入、ランサムウェアを横展開**
    - 2023年1月、ならコープがランサムウェアによる攻撃を受けていたことを公表
    - 原因は、攻撃者が脆弱性を悪用してVPN経由で侵入後、内部情報を収集し、ランサムウェアを横展開したことにある
    - サーバー11台で約49万人の個人情報を含むデータが暗号化されたが、それらの外部への流出は確認されていない
    - バックアップを取っていたデータベースは感染を逃れていたため、データを復元することができた

【参考】ランサムウェアによる被害の発生状況

- 復旧に1～2か月以上を要する場合がある
- 調査・復旧に高額の費用が発生



復旧に要した期間（2021～2023 年）



調査・復旧に要した費用（2021～2023 年）

出典）情報セキュリティ白書2024（2021～2023 年の警察庁資料を基にIPA が作成）

※「令和4年におけるサイバー空間をめぐる脅威の情勢等について」「令和3年におけるサイバー空間をめぐる脅威の情勢等について」では「5,000万円以上」
※※「令和5年におけるサイバー空間をめぐる脅威の情勢等について」から設けられた

【1位】ランサムウェアによる被害

2025年版簡易説明資料
は3月末公開予定

- **対策**
  - **組織(経営者層)**

【組織としての体制確立】

- インシデント対応体制を整備し、対応する
  - CISOを配置する
  - CSIRTを構築する
  - 有事の際の対応フローを確立する
  - 運用手順を社員へ通知する
  - 運用の訓練をする
  - 外部の協力依頼先を用意する
  - 社内規則の整備や予算確保をする

【1位】ランサムウェアによる被害

2025年版簡易説明資料
は3月末公開予定

- **対策**
  - **組織(システム管理者、従業員)**

【被害の予防】

- インシデント対応体制を整備し、対応する
- メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
- 多要素認証の設定を有効にする
- 提供元が不明のソフトウェアを実行しない
- サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
- 共有サーバー等へのアクセス権の最小化と管理強化
- 公開サーバーへの不正アクセス対策
- 適切なバックアップ運用(取得、保管、復旧訓練)を行う

【1位】ランサムウェアによる被害

2025年版簡易説明資料
は3月末公開予定

- **対策**
  - **組織(システム管理者、従業員)**

【被害を受けた後の対応】

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等
- 適切なバックアップ運用(復旧作業)を行う
- 復号ツール※1の活用
- インシデント対応体制を整備し、対応する

【1位】ランサムウェアによる被害

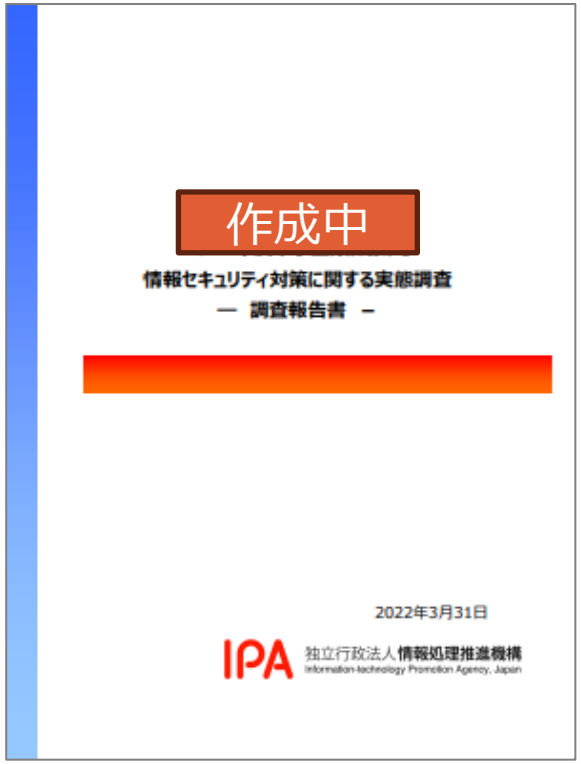
2025年版簡易説明資料は3月末公開予定

- **身代金の支払いと復旧業者の選定について**
  - 原則、身代金を支払わずに復旧を行う
  - 身代金を支払ってもデータの復元や情報の流出を防げるとは限らない
  - 対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある
  - 対応を依頼する業者の選定※1にも注意が必要

中小企業の実態を知るには…

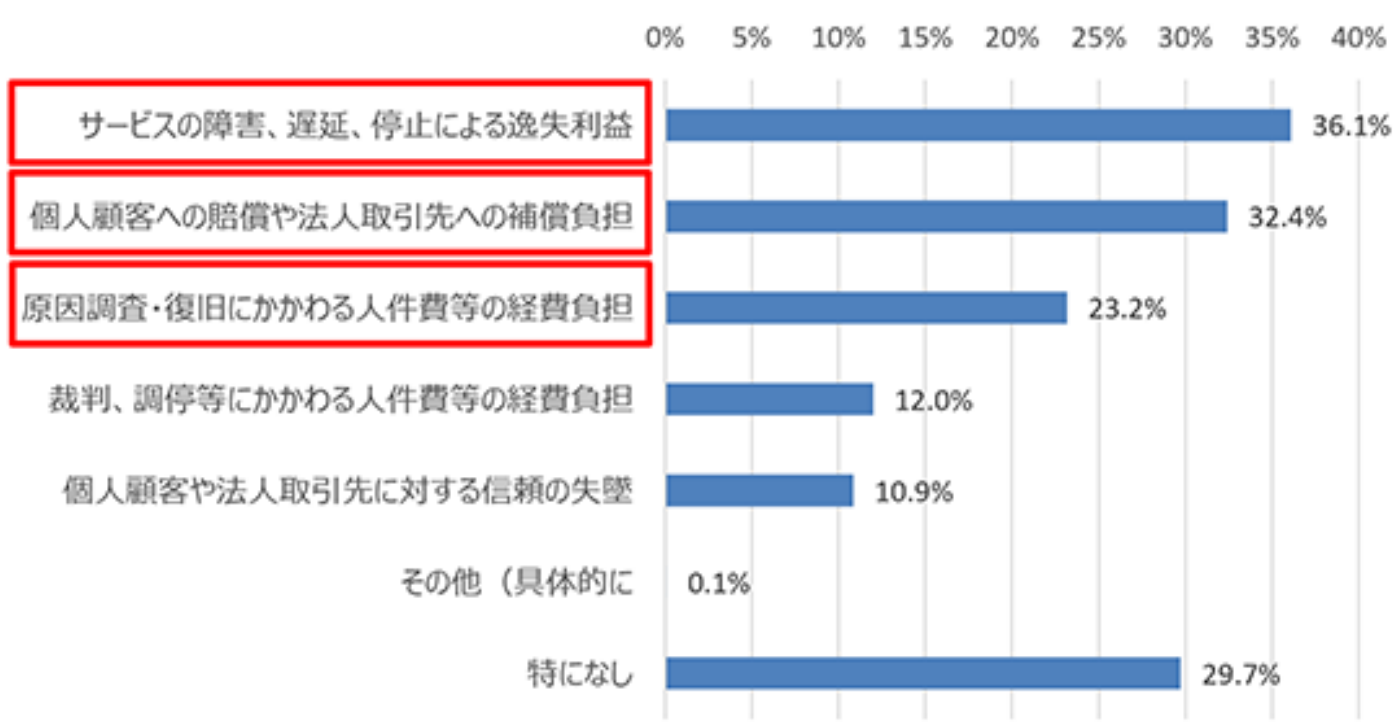
中小企業における情報セキュリティ対策の実態調査報告書を
活用してください

- 2025年2月14日速報版を公開
  - サプライチェーン全体でのサイバーセキュリティの不備が、取引先にも深刻な影響を及ぼしていることが明らかに
- 4月頃に報告書(完全版)を公開予定



サイバーインシデントによる取引先への影響

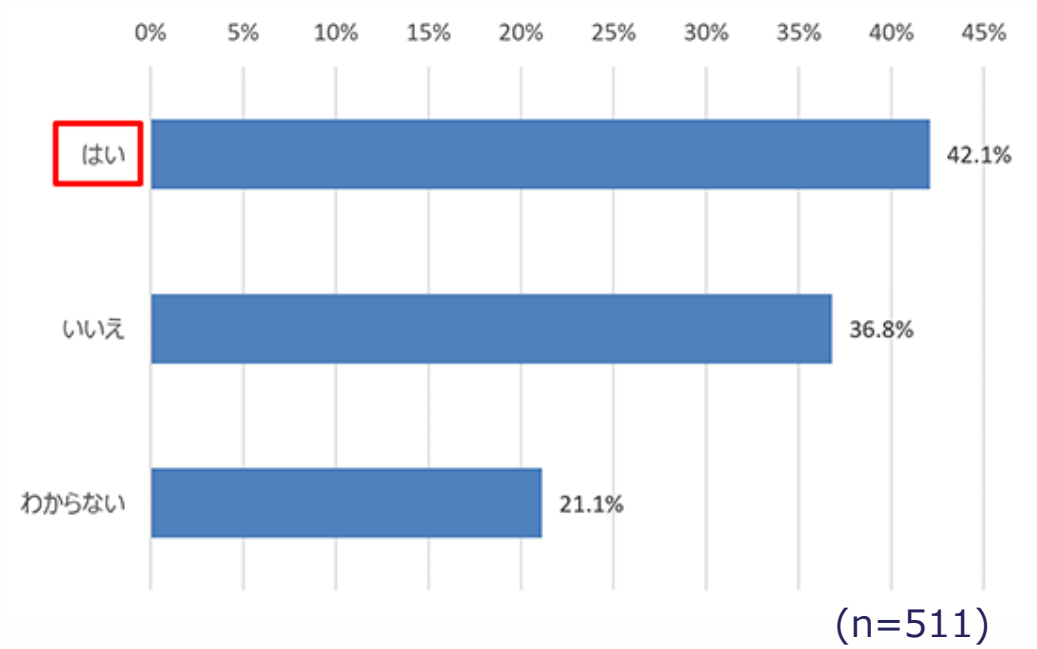
- サイバーインシデントにより取引先に影響があった企業は**約７割**



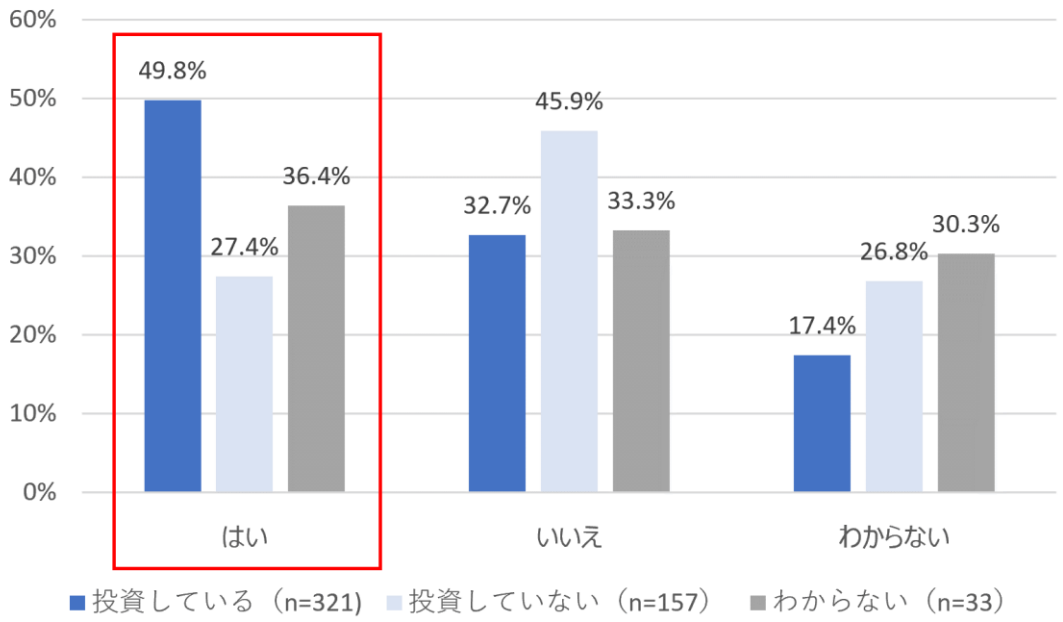
質問：サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。（MA）

情報セキュリティ対策が取引につながったか

- セキュリティ対策投資を行っている企業の**約5割**が、取引につながった



質問：貴社は取引先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。



情報セキュリティ対策投資別の集計結果

ガイドラインを活用した指導方法と身近な対策例

効果的な解決方法は？

- “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

中小企業向け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

平時の対策支援（社内体制整備、意識向上）　**有事の対策支援（検知、対応、復旧等）**

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、具体的方策を解説

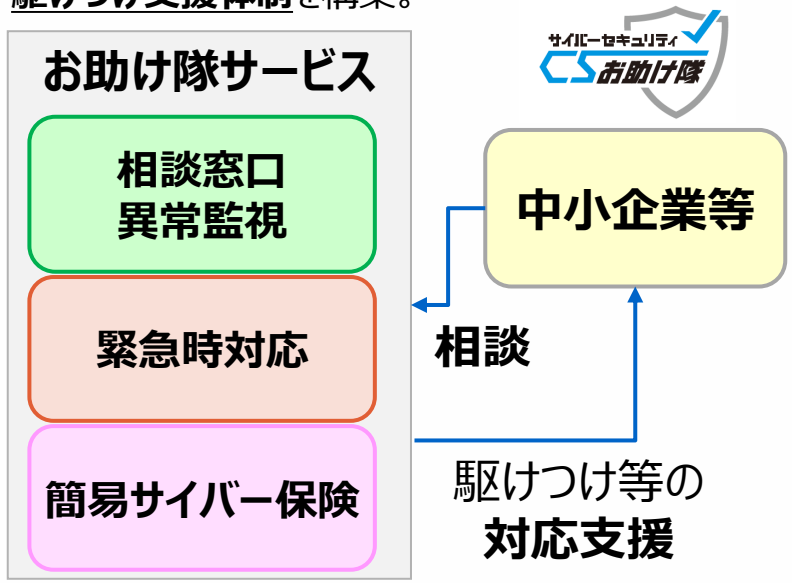
SECURITY ACTION

- 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

SECURITY ACTION ★
セキュリティ対策自己宣言

サイバーセキュリティお助け隊サービス

- 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

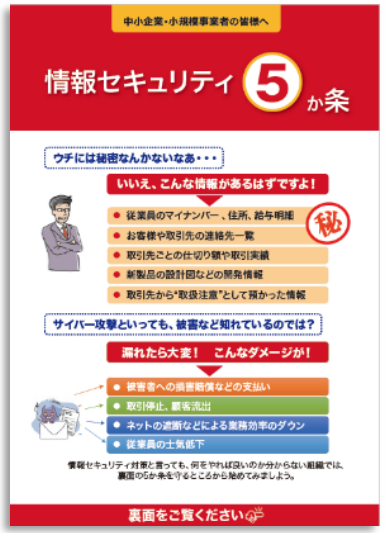
https://www.ipa.go.jp/security/guide/sme/about.html

- 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（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

→何から始めれば良いのか？という状態から、段階的にステップアップできる構成

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

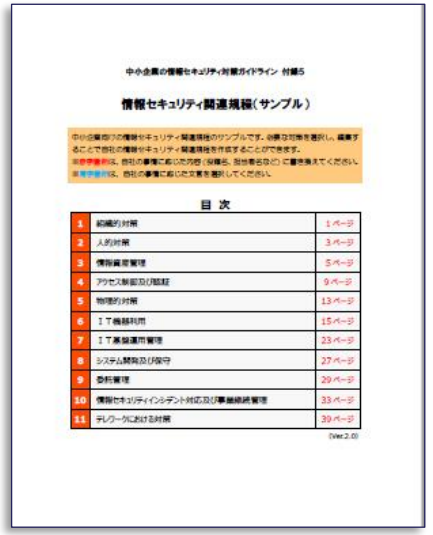
SECURITY ACTION ★一つ星を宣言

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
- ウェブサイトのセキュリティ対策
- クラウドサービスのセキュリティ対策
- テレワークのセキュリティ対策
- 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

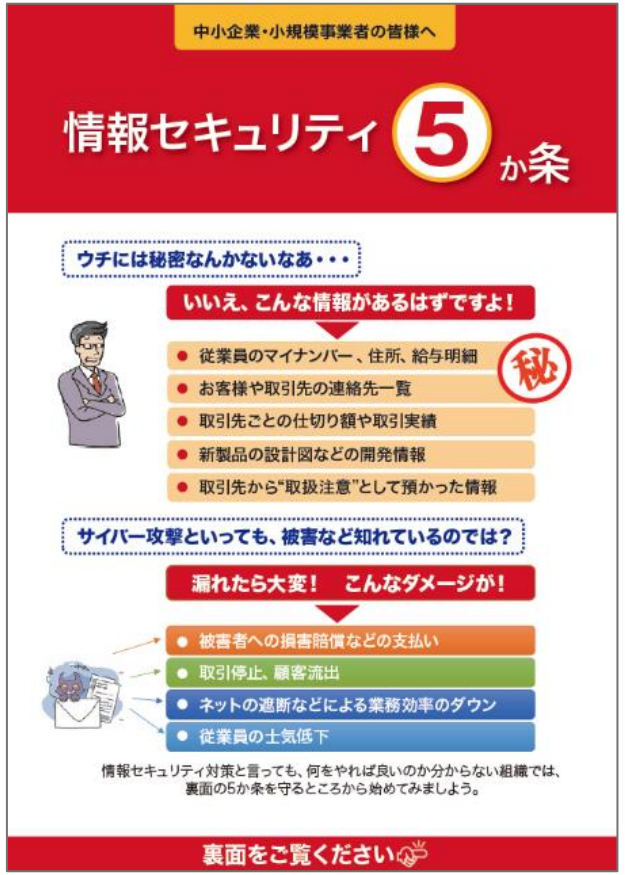
情報セキュリティ5か条

- 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



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
  - 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
    - 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、社内ルールの作成を期待
  - 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

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？

やってみましょう！

5分でできる！
情報セキュリティ自社診断

☑ 診断内容を読み、チェック欄に○を付ける

☑ チェックが終了したら最下段に合計を記入

※以下を利用していない場合は、「実施している　４」に○を付ける
　No. 9　 無線LAN
　No.23　クラウドサービス等の外部サービス

研修ではワークを行うことで実践力を高めます

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段階の取組み目標を用意

１段階目（一つ星）

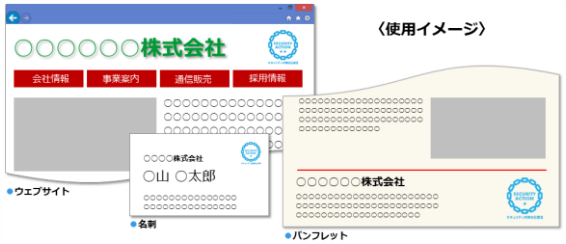
「**情報セキュリティ5か条**」に取組むことを宣言

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

SECURITY ACTION 制度の特長

- 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、名刺などに印刷することで自らの取組み姿勢をアピール



- 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

- **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

申請・加点要件としている補助金・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、取組みを拡大予定

【自治体等におけるSA制度の活用事例】

- **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
- **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**：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 （2023/3）

- **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
- **鹿児島県 かごしま中小企業DX推進事業費補助金（令和6年度）**：鹿児島県
- **堺市中小企業デジタル化促進補助金**：大阪府堺市

- **デジタル化トライアル事業費補助金（2023年度）**：秋田県
- **「情報セキュリティ基本方針 策定支援専門家派遣」事業（2019年度）**：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）（2022年度）**：岐阜県
- **デジタル技術導入補助金（2023年度）**：愛知県 （2023/5） ※採択審査の加点対象
- **デジタル化促進補助金（2023年度）**：北海道札幌市 （2023/5） ※採択審査の加点対象、採択後の自己宣言
- **産業デジタル実装支援事業費補助金（2023年度）**：宮崎県 （2023/9）
- **DX（デジタル化）設備導入補助金（2023年度）**：石川県 （2023/12）

- **DX認定制度**：IPA ※サイバーセキュリティ対策の推進においてセキュリティ監査の実施概要をまとめることが要件であるが、中小企業、個人事業主の場合は二つ星で代替可

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/

- 「見守り」「駆付け」「保険」など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安価にまとめた、民間の事業者から提供されるサービス
- 現在38社から56サービスが展開(2025年2月時点)

➢ **「サイバーセキュリティお助け隊サービス基準」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
緊急時の対応支援	インシデント発生などの**緊急時には対応支援**
価格	・ネットワーク監視型：**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**

サイバーセキュリティ お助け隊

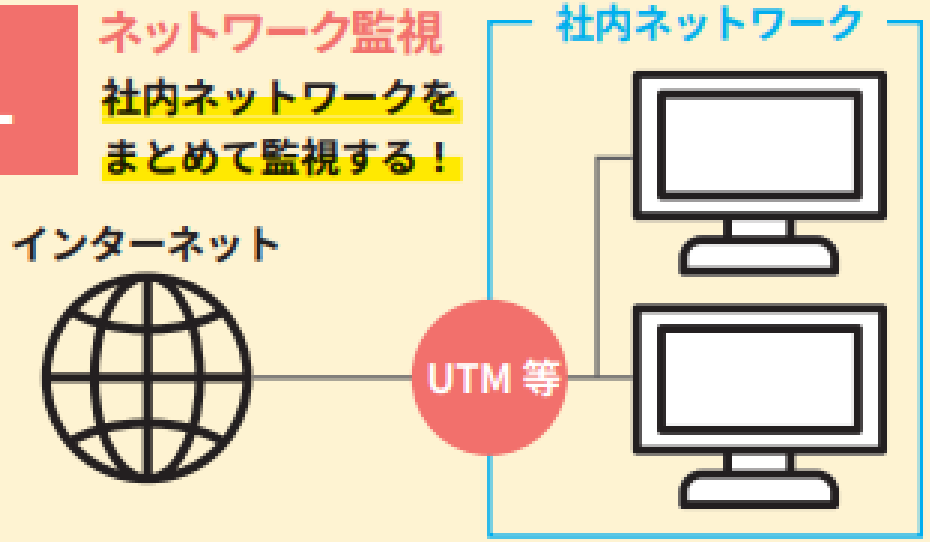
相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

本サービスを採用することを通じて、取引先企業に対する**自社の信頼性のアピール**に

異常の監視の仕組み

1 ネットワーク監視

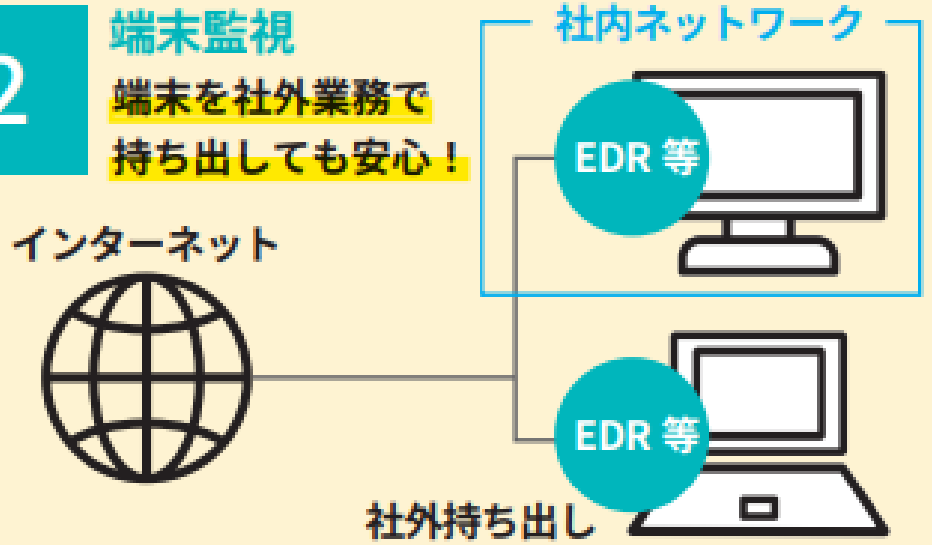
社内ネットワークをまとめて監視する！



パソコン側の設定作業は不要で外部と社内ネットワークの間に監視装置 (UTM 等) を設置し、社内ネットワークを包括的に監視します。

2 端末監視

端末を社外業務で持ち出しても安心！



従業員が利用する各端末に監視ソフトウェア（EDR 等）をインストールして、各端末での不審な挙動を検知して迅速な対処を行います。

3 併用 より強固なセキュリティ監視が可能！

1 ネットワーク監視と 2 端末監視の両方を導入することで、多層防御による強固なセキュリティ監視が可能になります。

「お助け隊サービス２類」について

- お助け隊サービス１類のサービス内容では対応することが難しい中規模以上の中小企業へ向け、**お助け隊サービス２類を提供開始**
- お助け隊サービス２類は提供中のお助け隊サービス１類をベースに**監視製品を上位モデルに変更**、**セキュリティに関する機能やサービスの追加**等の拡充を行ったお助け隊サービス
- サービス内容の拡充に伴い、１類サービスで定めている**価格要件は緩和される**

利用者から寄せられた声

●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。

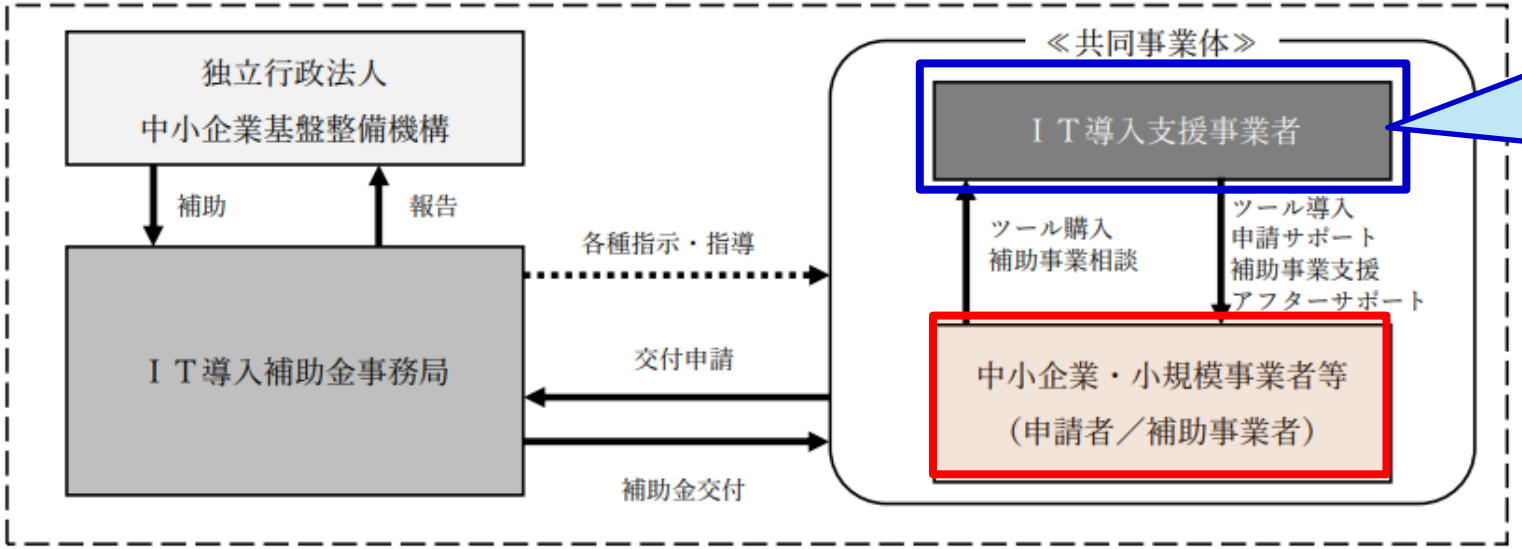
※サイバーセキュリティお助け隊サービス提供事業者　提供情報より

IT導入補助金2025 セキュリティ対策推進枠

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

枠	セキュリティ対策推進枠
補助額	5万円～150万円
機能要件	独立行政法人情報処理推進機構が「サイバーセキュリティお助け隊サ ービスリスト」に掲載しているいずれかのサービス
補助率	1/2以内 ※小規模事業者は２／３以内
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2025」**
https://it-shien.smrj.go.jp/

中小企業支援策・対策支援ツール

企業・組織からのインシデント等に関する相談/届出/情報提供窓口のご案内

- 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けております。
- セキュリティインシデント等が発生し、お困りの際にご活用いただくことができますので、**右記ポータルページ**をご覧ください。

窓口名	相談・届出の例
情報セキュリティ安心相談窓口	• ランサムウェアに感染したため、対処方法について相談したい • 自組織のウェブサイトが改ざんされてしまったため、対処方法と再発防止策について相談したい • その他、情報セキュリティに関する一般的な相談やアドバイスが欲しい（相談先の窓口が不明な場合を含む）
標的型サイバー攻撃特別相談窓口	• 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
コンピュータウイルス・不正アクセスに関する届出窓口	• ランサムウェア感染事象が発生したため、インシデントの内容について公的機関への届出（情報提供）を行いたい • サイバー攻撃被害について、サイバー保険の適用を受けるために公的機関への届出を行いたい
脆弱性関連情報の届出受付	• 日本国内で利用されているOS、ブラウザ、メーラ等の脆弱性の届出 • 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
脆弱性に関する問合せ窓口	• ウェブサイトの脆弱性対策、ソフトウェアの脆弱性、また脆弱性に関する公開資料等の質問

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

詳細はこちらのページにて

映像で知る情報セキュリティ

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

2023年度制作映像

今、そこにある脅威
～内部不正による情報流出のリスク～

2022年度制作映像

今、そこにある脅威
～組織を狙うランサムウェア攻撃～

華麗なる情報セキュリティ対策
（8話構成）

現在、計34本をYouTube内のIPA Channelで公開中。
主要な映像は動画ファイルでも配布。

[企業・組織向け] 内部不正対策、標的型攻撃、ビジネスメール詐欺、ランサムウェア対策、中小企業向け対策、新人研修など

[一般向け] ワンクリック請求、スマホセキュリティ、SNS利用の心得、パスワード、小学生、中高生向けなど

活用実績 (2024/3/1時点)

◆動画ファイルの2023年度申込数 ：

申込み**1,254件** 研修での受講予定者数： **約61万名**

◆インターネット動画再生回数： IPA Channelで全作品の累計 **約622万回**

偽セキュリティ警告(サポート詐欺)画面の閉じ方体験サイト

https://www.ipa.go.jp/security/anshin/measures/fakealert.html

- 近年被害が増加している、**偽セキュリティ警告（サポート詐欺）の画面表示を模擬体験**できるサイト
- 画面を閉じる手順を実践することで被害を未然に防止

サイバーセキュリティアワード2025 Web・コンテンツ部門 最優秀賞を受賞！

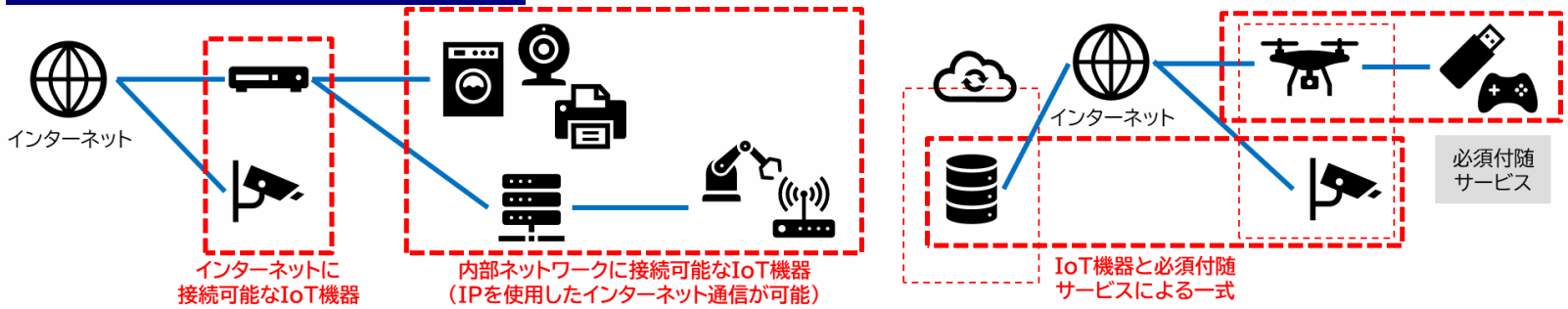
IoT製品セキュリティラベリング制度(JC-STAR)

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します！

- 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

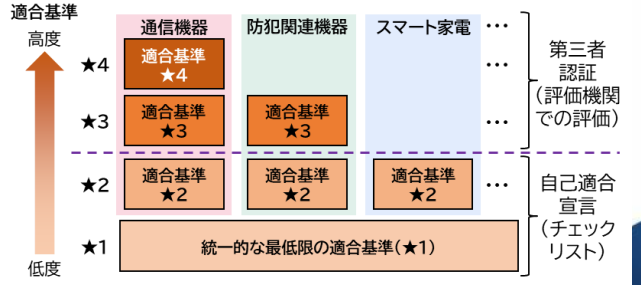
定められた適合基準への適合を示す目印

- 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



IT利用者に必要なITの基礎的知識を証明する
国家試験「ITパスポート試験」（通称：iパス）

iパスの特徴

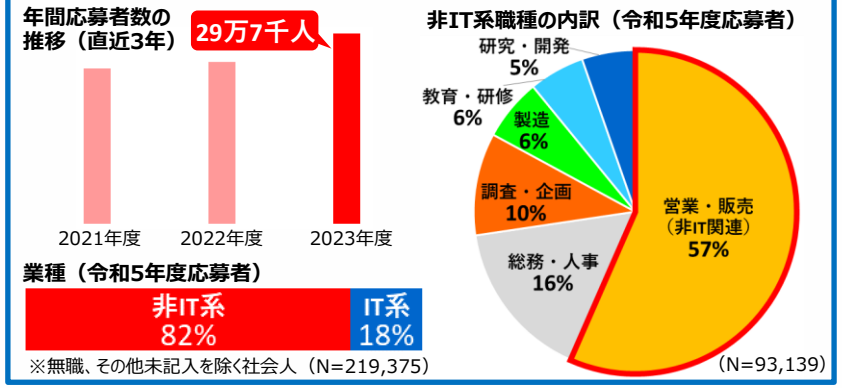
・ITを利活用するすべての社会人・学生が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

・IT技術に関する基礎知識だけでなく、情報セキュリティや情報モラルに関すること、経営戦略、会計や法務など、ITを活用する上で前提となる幅広い知識が試験勉強を通じてバランス良く習得できます。

・バウチャーチケット制度で受験手数料を一括して支払ことができるため、社員のiパス受験を積極的に後押しすることが可能です。

・組織全体のITリテラシーの底上げのために活用されています。

応募者数は年々増加し、2023年度は30万人に迫る！
非IT系企業、営業・販売担当者を中心に活用されています

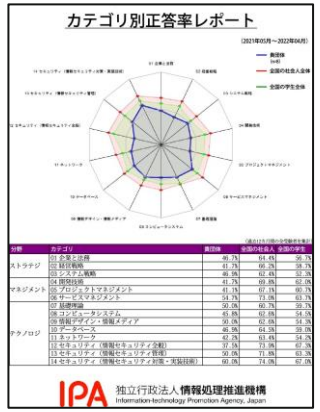


受験申込みはITパスポート試験サイトで受付けています。
また、同サイトでは、合格者の声や企業の声などを掲載していますので、是非ご覧ください。
ITパスポート試験サイト
▶https://www3.jitec.ipa.go.jp/JitesCbt/index.html

社員のIT知識習熟度の確認ができる

・企業担当者は、バウチャーチケットを活用することで、社員の受験申込み状況や成績情報を確認することができ、社員の活用状況を効率的に把握することができます。

・バウチャーチケットを活用すると、社員の平均正答率をレーダーチャート化した「正答率レポート」が確認できます。出題カテゴリごとの正答率や、自組織と他の集団（社会人全体、学生全体）の相対的なポジションを知ることで、組織全体の育成状況や強み・弱みを把握することができます。



試験実施概要

・試験は**CBT方式で随時受験可能**
※CBT方式とは、試験会場に設置されたコンピュータを利用して実施する試験方式のことです

・自分の都合に合わせて、試験日時や試験会場を選んで、受験申込みができます

・受験申込み後も試験日を変更することができます
※試験日の3日前まで変更可能

・試験会場は全国に100箇所以上

・多人数による一斉受験の相談にも応じています

試験時間	出題形式	出題数 解答数	合格基準 総合評価	合格基準 分野別評価	合格率
120分	四肢択一	100問 100問	600点 （1,000点満点）	300点 （1,000点満点）	50.3% （令和5年度平均）

「プラス・セキュリティ」を身につけた人材の育成のために

国家試験「情報セキュリティマネジメント試験」

情報セキュリティマネジメント試験の特徴

・IT利用者の情報セキュリティ対策に特化した国家試験です。組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定します。

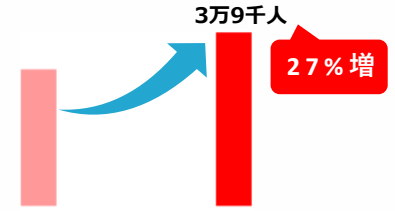
・科目A試験では、情報セキュリティに関する各種対策、関連法規などに加え、技術分野や経営管理などの関連分野も出題。
科目B試験では、身近な事例をベースにした実践的な問題が出題されます。

・サイバーセキュリティ対策は、今や情報システム部門だけでは対応できず、企業では「プラス・セキュリティ」の取組が求められています。
「プラス・セキュリティ」を身につけた人材の育成のために、試験勉強を通じてサイバーセキュリティに関する最新知識を習得させることを目的として活用することもできます。

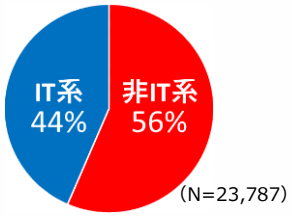
「プラス・セキュリティ」とは・・・
自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと。企業におけるデジタル活用が進展する中で「プラス・セキュリティ」の必要性は高まっています。

応募者の半数以上が非IT系企業、2022年度から応募者が大幅に増加！

年間応募者数の推移（直近2年）



業種（令和5年度応募者）



※無職、その他未記入を除く社会人

受験を特にお勧めする方

・業務で個人情報を取り扱う方

・外部委託先に対する情報セキュリティ評価・確認を行う方

・業務部門・管理部門で情報管理を担当する方

・iパス合格からさらにステップアップを目指す方

試験実施概要

・試験は**CBT方式で随時受験可能**
※CBT方式とは、試験会場に設置されたコンピュータを利用して実施する試験方式のことです

・自分の都合に合わせて、試験日時や試験会場を選んで、受験申込みができます

・受験申込み後も試験日や試験会場を変更することができます
※試験日の3日前まで変更可能

・試験会場は全国に約260箇所

・バウチャーチケットによる受験手数料の一括払いができます

・多人数による一斉受験の相談にも応じています

試験科目	試験時間	出題形式		出題数 解答数	合格基準 総合評価
		科目A	科目B		
科目A・B試験	120分	多肢選択式 (四肢択一)	多肢選択式	60問 60問	600点 (1,000点満点)

推薦者の声や活用事例等を掲載中！
情報セキュリティマネジメント試験　特設紹介ページ
▶ https://www.ipa.go.jp/shiken/kubun/sg/

国家資格「情報処理安全確保支援士」

通称：登録セキスペ
（登録情報セキュリティスペシャリスト）

サイバーセキュリティに関する実践的な
知識・技能を有する専門人材を育成・確保

①人材の見える化
- 資格保持者のみ資格名称を使用
- 登録簿の整備・登録情報の公開（希望しない者を除く）

②人材活用の安心感
- 国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務

③人材の質の担保
- 継続的な講習受講義務により、最新の知識・技能を維持
- 3年に1度の登録更新により、制度の信頼性を確保

企業における安全な情報システムの
企画・設計・開発・運用を支援、
サイバーセキュリティ対策の指導・助言を実施

情報処理安全確保支援士
試験合格

登録簿へ登録
（申請が必要）

- 講習受講
- 資格名称の使用
- 登録情報の公開

まとめ

- 情報セキュリティの脅威は中小企業にとってももはや他人事ではない状況ですが、中小企業の意識や対策状況は十分と言えない状況です。
- IPAでは中小企業のセキュリティ対策水準の向上に向けて、様々な組織・個人と連携して、多面的なアプローチで普及活動を推進しています。
- 対策水準の向上には、中小企業の身近な支援者である皆さまのご協力が不可欠と考えています。引き続きご協力をお願いいたします。