中小企業におけるサイバーセキュリティの脅威と対策

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

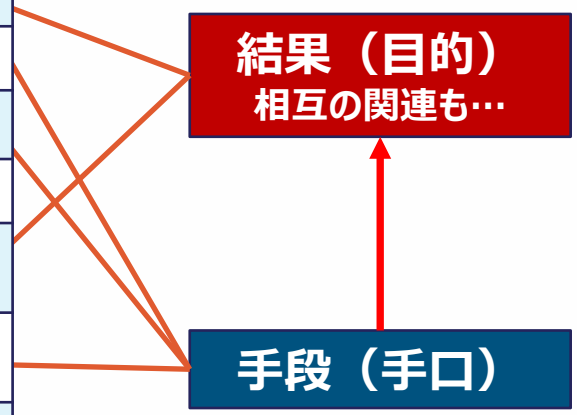
サイバーセキュリティの脅威動向

「情報セキュリティ10大脅威2025」

最近の「組織」における脅威動向

- **ランサムウェア攻撃は引き続き１位、標的型攻撃も5位**と依然として大きな脅威。
- これらの攻撃は、従来の**サプライチェーン経由のリスク**に加え、**ゼロデイや公開直後の脆弱性**を狙った攻撃の脅威が高まっている傾向。

順位	2023	2024	2025
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**	**ランサム攻撃による被害**
2	**サプライチェーンの弱点を悪用した攻撃**	**サプライチェーンの弱点を悪用した攻撃**	**サプライチェーンや委託先を狙った攻撃**
3	**標的型攻撃による機密情報の窃取**	内部不正による情報漏えい等の被害	**システムの脆弱性を突いた攻撃**
4	内部不正による情報漏えい	**標的型攻撃による機密情報の窃取**	内部不正による情報漏えい等
5	テレワーク等のニューノーマルな働き方を狙った攻撃	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**	**機密情報等を狙った標的型攻撃**
6	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組みを狙った攻撃
7	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**	地政学的リスクに起因するサイバー攻撃
8	**脆弱性対策情報の公開に伴う悪用増加**	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS攻撃）
9	不注意による情報漏えい等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺
10	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等



被害事例

- 大規模な業務停止に至った事例
  - KADOKAWAグループ（2024年6月）
    - **出版・物流システムやニコニコ動画等のWebサービス等が停止。**
  - 名古屋港運協会（2023年7月）
    - **名古屋港全ターミナルの作業停止。**
  - 大阪急性期・総合医療センター（2022年10月）
    - **電子カルテを含む基幹システムを使用停止**し、**紙カルテ運用の開始、外来診療の制限、救急受入の停止、予定手術の停止**等の対応を余儀なくされた。

出典：朝日新聞デジタル

出典：名古屋港統一ターミナルシステム

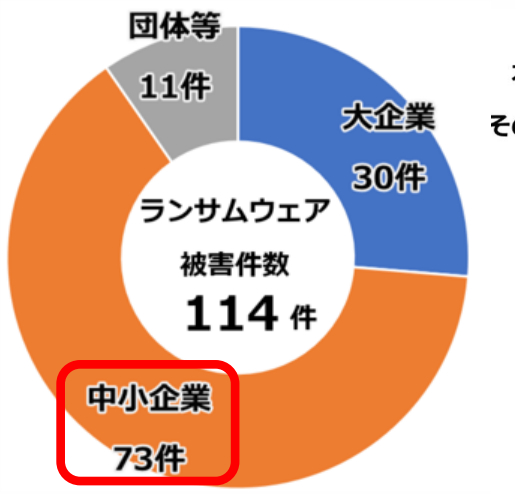
- 委託先を通じた個人情報の流出に至った事例
  - イセトー社（2024年５月）
    - 業務委託元である**地方公共団体、金融機関等の個人情報を含むデータが流出。**

※関係機関の発表や各種報道に基づく

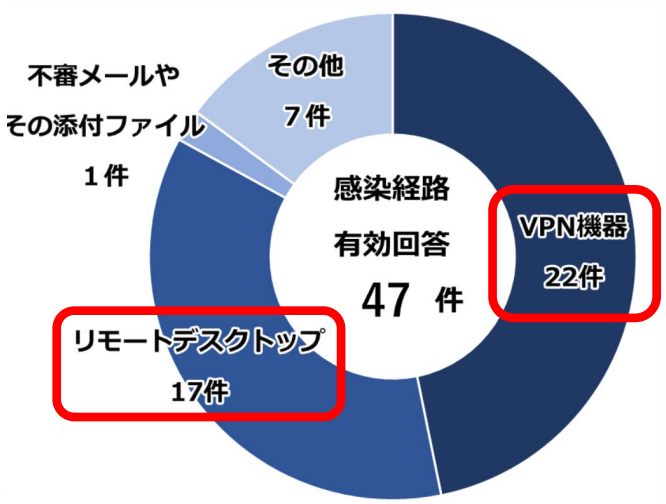
被害傾向

- ランサムウェア被害企業の64%が中小企業
- VPN機器、リモートデスクトップからの侵入で80%以上
- 復旧に要した期間は1週間以上が38%以上
- 半数以上が調査・復旧に500万円以上を要していた

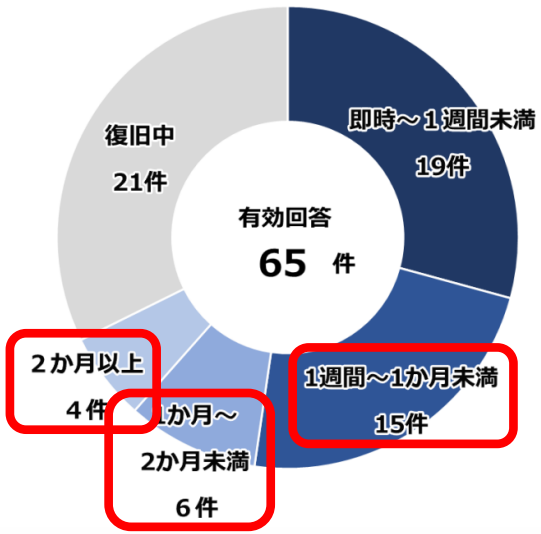
規模別報告件数



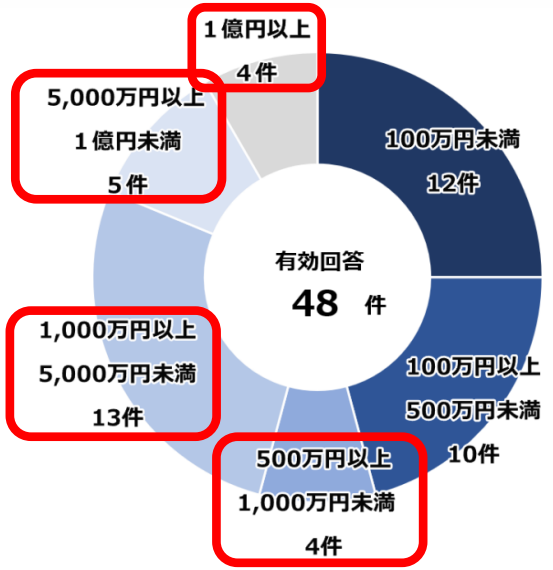
感染経路



復旧に要した期間



調査・復旧費用の総額



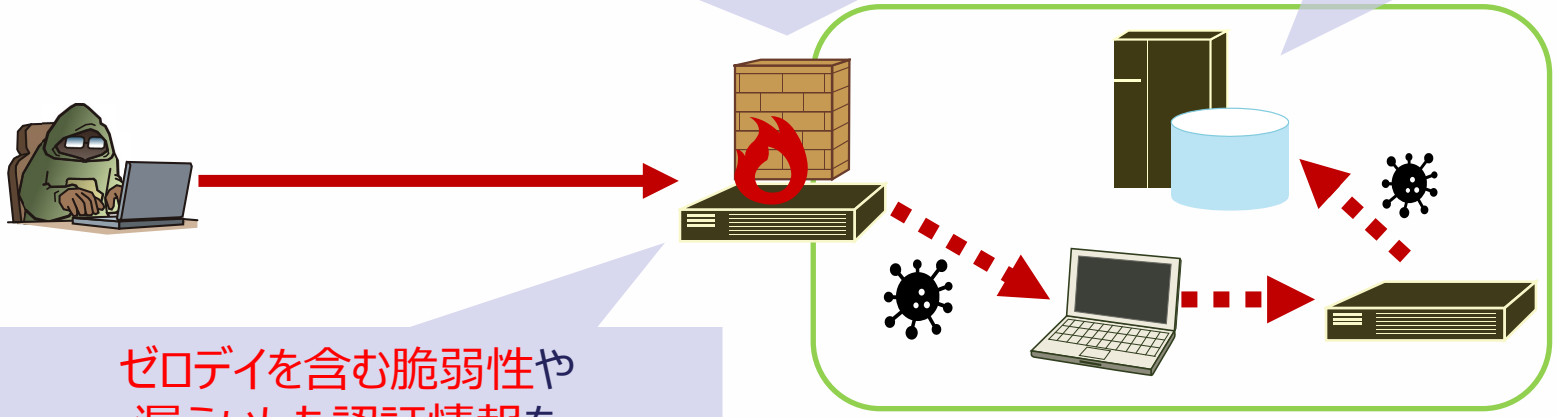
出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」

攻撃手口（ネットワーク貫通型攻撃）

- インターネットとの境界に設置される装置を狙った攻撃。2023年に入って、ゼロデイ脆弱性や公開直後の脆弱性を突いた攻撃が多数発生（2024年に入ってからも頻発）。
- 中継サーバを経由して攻撃することで、自身の真の所在地や身元を隠蔽し、検知や追跡を回避する手法（ORB（Operational Relay Box）化を伴う攻撃）も観測。

インターネットとの境界に設置された装置　例：VPN機器、メールセキュリティGW、オンラインストレージサーバ、Webアプリケーションサーバ、IoTルータ等

ネットワーク内に侵入され、保有情報の漏えいや改ざん等の被害発生



ゼロデイを含む脆弱性や漏えいした認証情報を悪用して組織内ネットワークに侵入

平時から対策を

- IPAでは、2023年8月以降、ネットワーク貫通型攻撃に関する注意喚起を実施。
- 対策として、**日々の各種ログの確認や、製品ベンダから発信される情報の収集、機器の外部公開状態の確認**を促している。

対策の基本

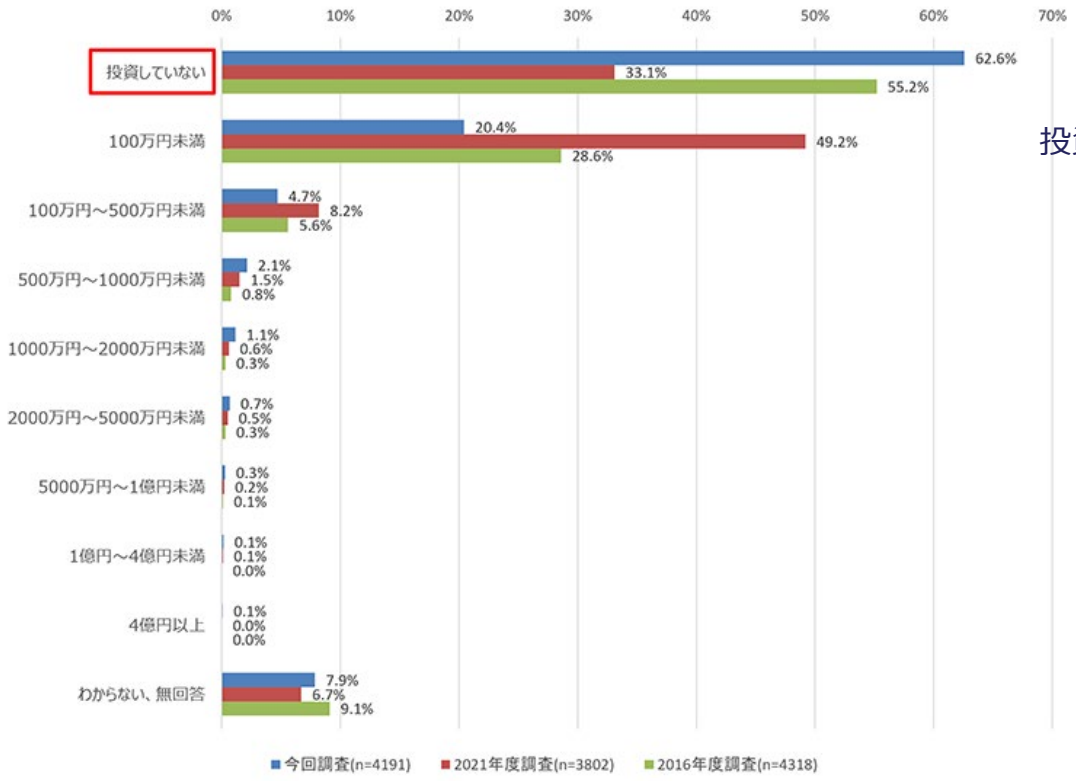
- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 「情報セキュリティ対策の基本」は常に意識

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

中小企業における現状と課題

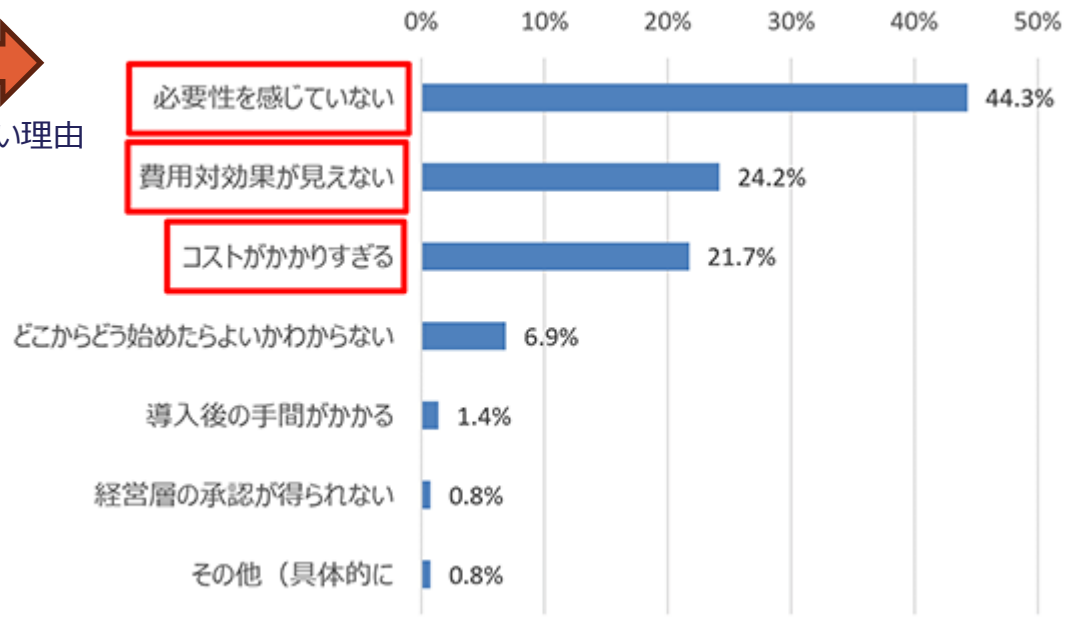
直近過去3期の情報セキュリティ対策投資

- 過去3期における情報セキュリティ対策投資を行っていない企業は**約６割**



質問：直近過去3期の情報セキュリティ対策投資額（IT機器や社員への教育等も含む）の概算について教えてください。（SA）

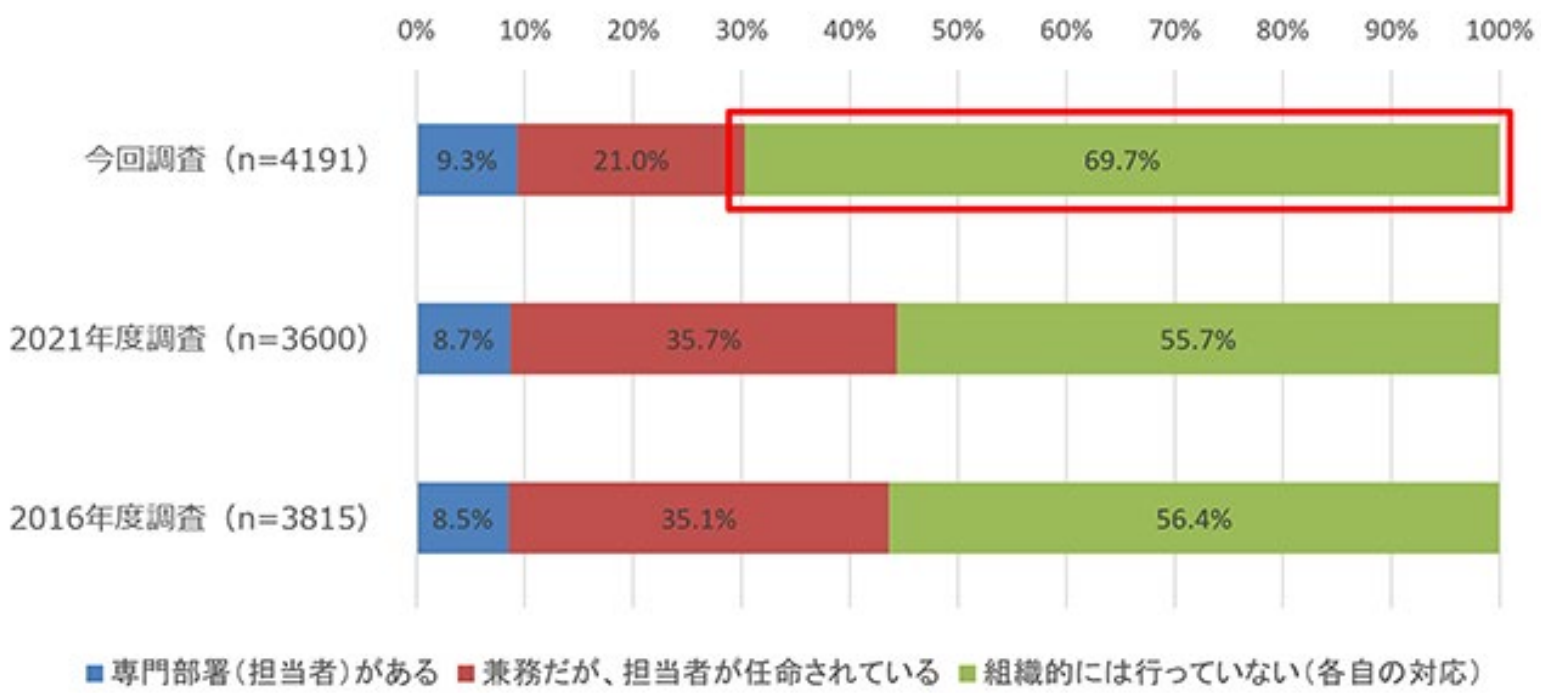
投資していない理由



質問：前問で情報セキュリティ対策投資額について「投資をしていない」とお答えになった一番の理由について教えてください。（SA）

情報セキュリティ体制

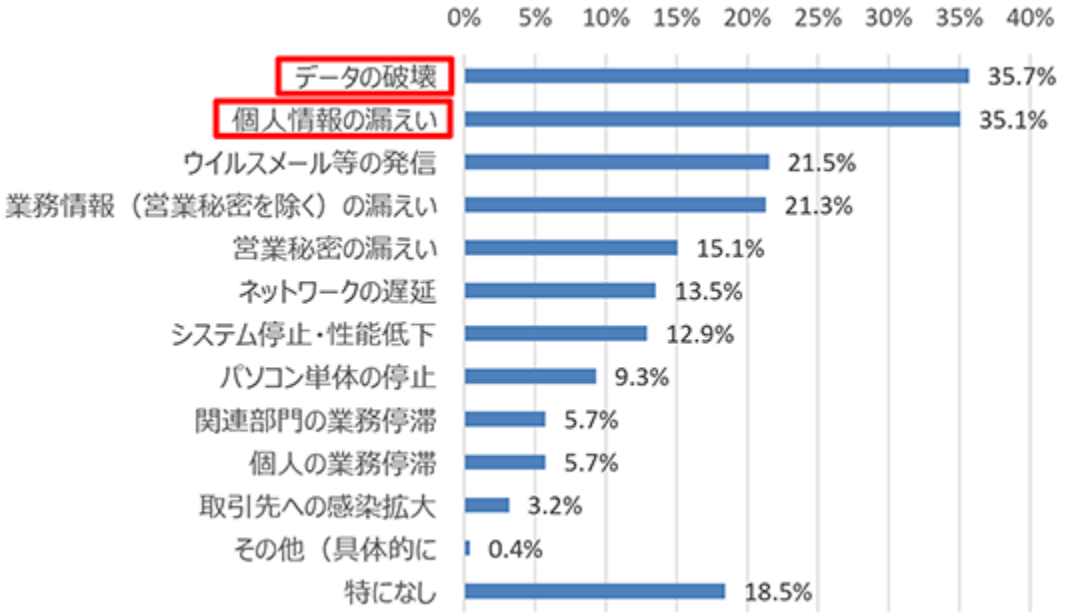
- **約７割**の企業が組織的なセキュリティ体制が整備されていない



質問：貴社の情報セキュリティ対策はどのような体制で行われていますか。(SA)

サイバーインシデントによる被害

- 過去3期内で、サイバーインシデントが発生した企業における被害額の平均は**73万円**（うち9.4%は100万円以上）、
  復旧までに要した期間の平均は**5.8日**（うち2.1%は50日以上）



質問：貴社でサイバーインシデントによる影響で、生じた被害について教えてください。（MA）

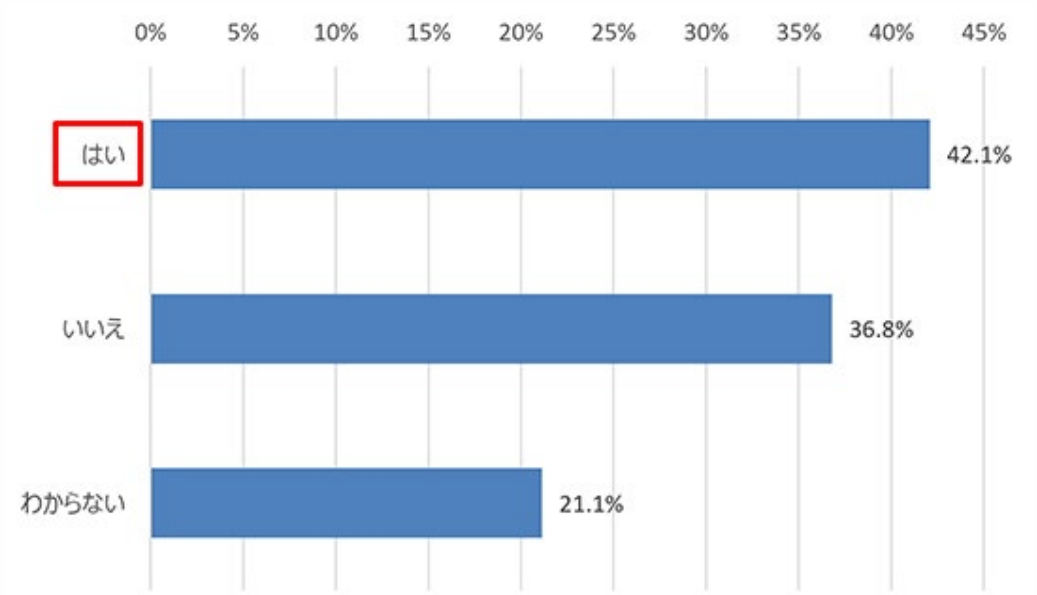
サイバーインシデントによる取引先への影響

- 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**

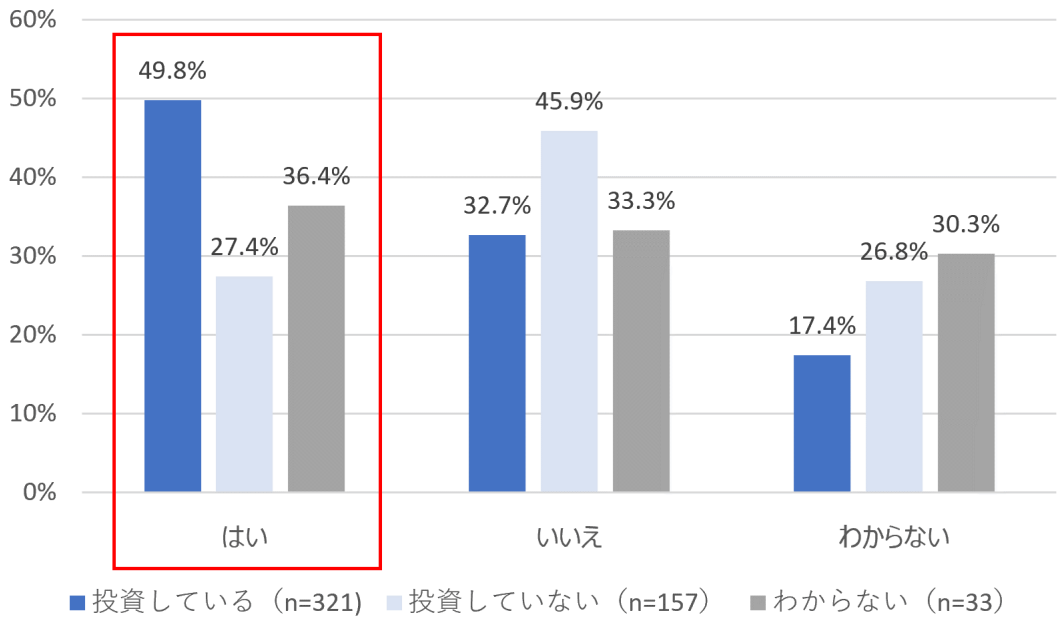
質問：サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。（MA）

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。（SA）



情報セキュリティ対策投資別の集計結果

対策実践のための考え方、ツール・制度

脅威から会社をどう守るのか

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

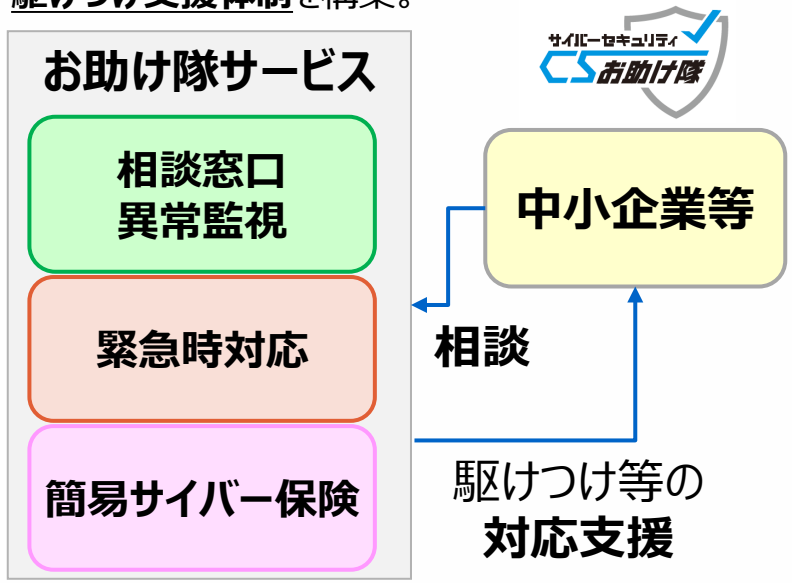
SECURITY ACTION

- 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。



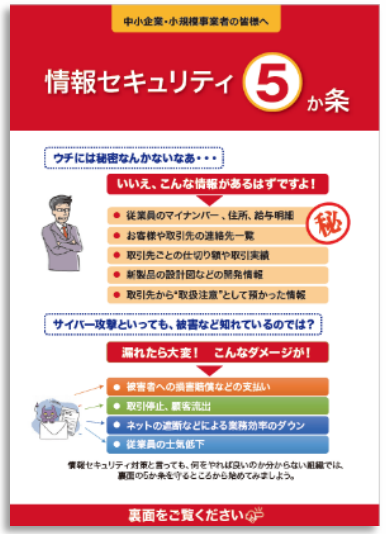
中小企業の情報セキュリティ対策ガイドライン

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

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

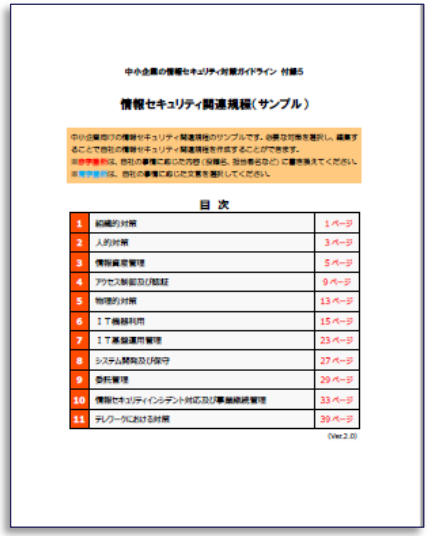
SECURITY ACTION ★一つ星を宣言

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

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）

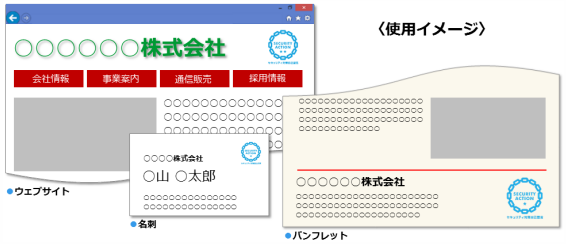
「**情報セキュリティ5か条**」に取組むことを宣言

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

➢ **「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

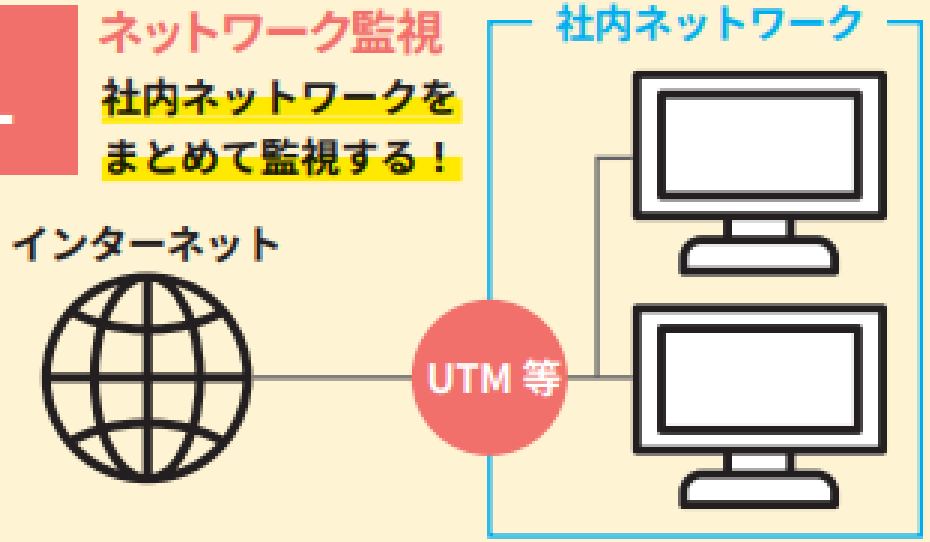
相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

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

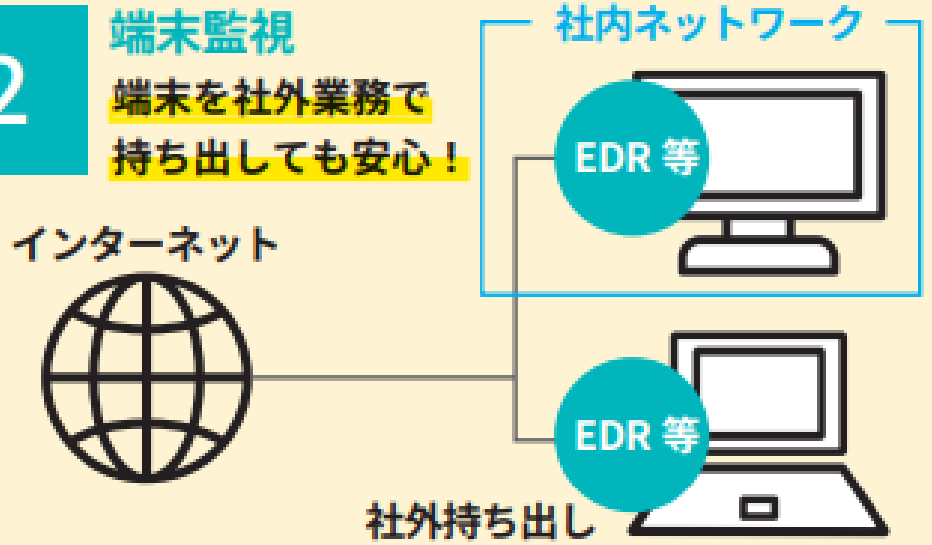
社内ネットワークをまとめて監視する！



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。

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。

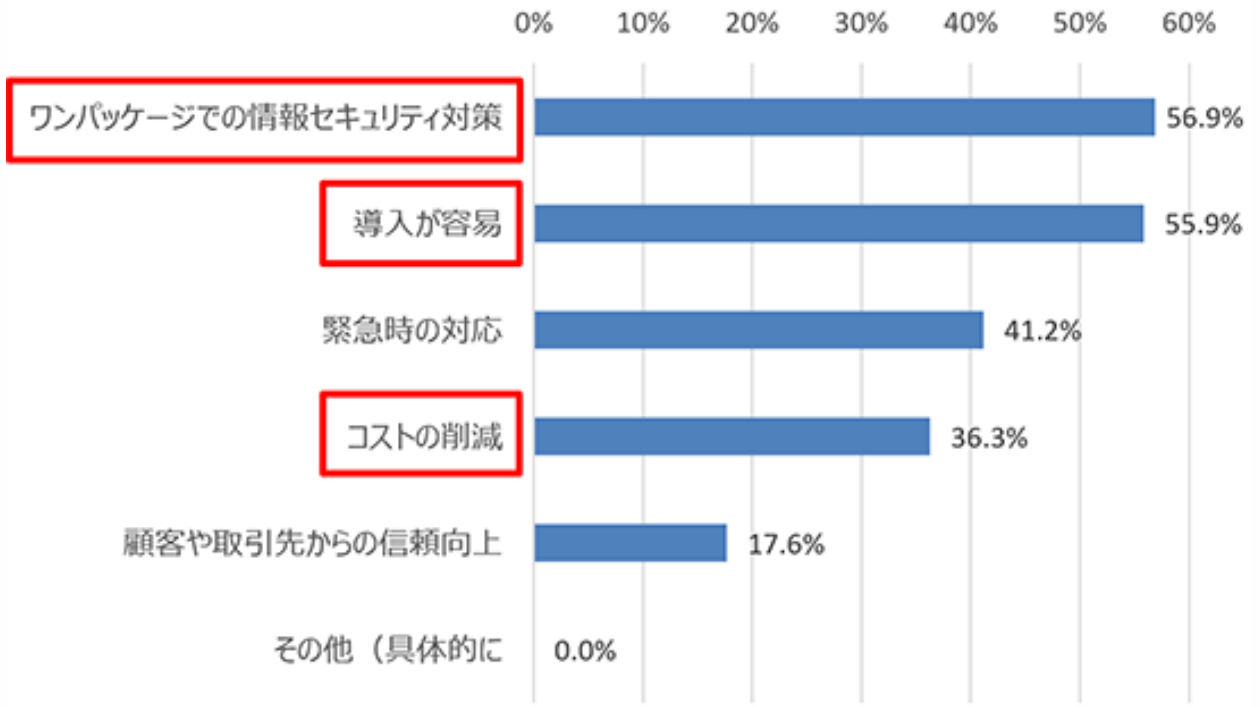
●アラート通知が来るので、**防御できていることが実感でき安心**。本社のほか複数の拠点でも利用しているが**サービス利用料が安い**ので助かっている。

●**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

導入して良かった点

- 導入企業の**５割以上**がセキュリティ対策の導入が容易と回答し、また**３割以上**の企業が費用対効果を実感している



質問：貴社が「サイバーセキュリティお助け隊サービス」を導入して良かった点を教えてください。（ＭＡ）

出典：IPA「2024年度中小企業等実態調査結果（速報版）」

「お助け隊サービス２類」について

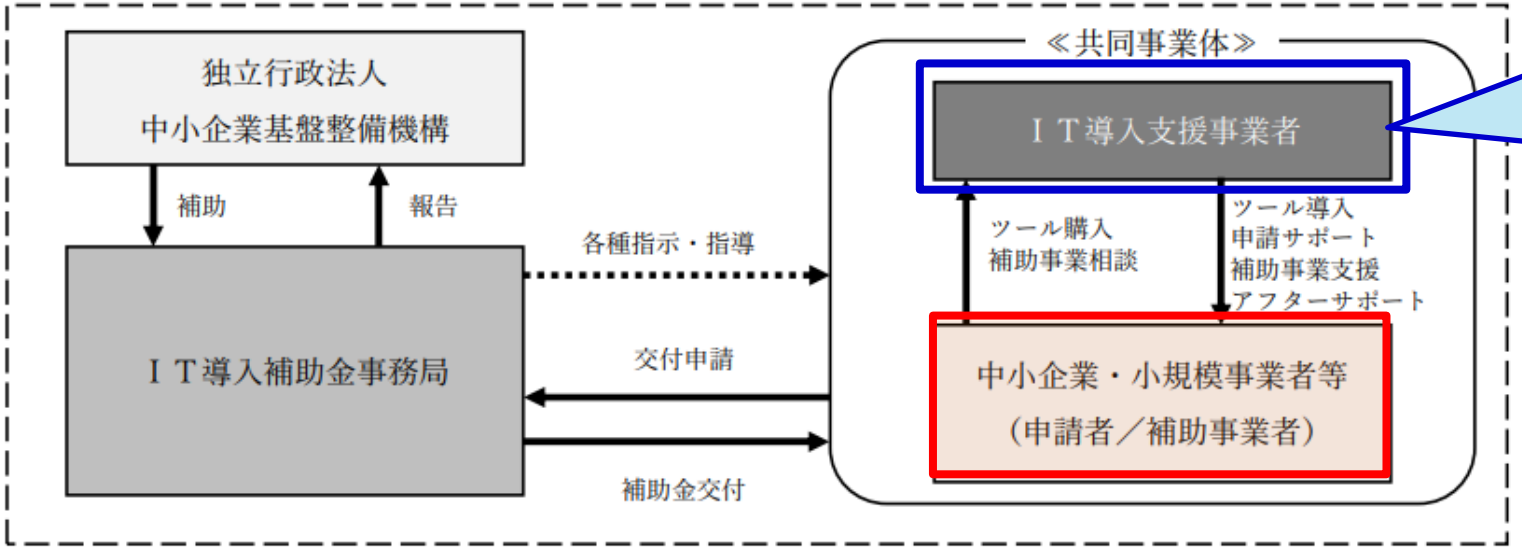
- お助け隊サービス１類のサービス内容では対応することが難しい中規模以上の中小企業へ向け、**お助け隊サービス２類を提供開始**
- お助け隊サービス２類は提供中のお助け隊サービス１類をベースに**監視製品を上位モデルに変更**、**セキュリティに関する機能やサービスの追加**等の拡充を行ったお助け隊サービス
- サービス内容の拡充に伴い、１類サービスで定めている**価格要件は緩和される**

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/

参考情報

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**

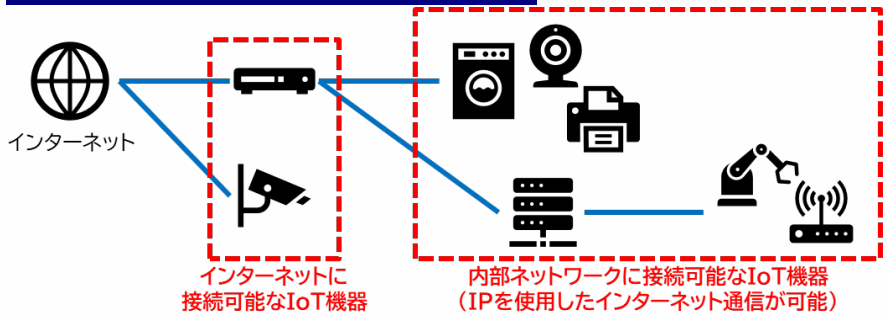
IoT製品セキュリティラベリング制度(JC-STAR)

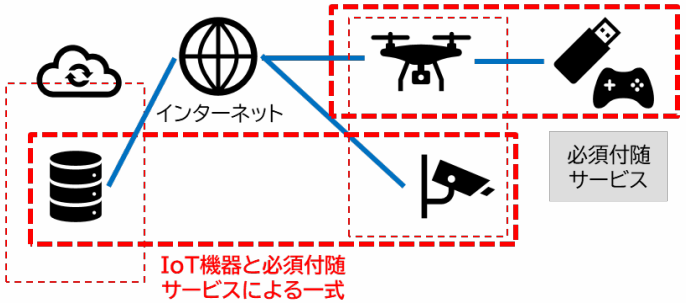
2025年度から、IoT製品に対するセキュリティ要件(適合基準)への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を開始します！

- 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

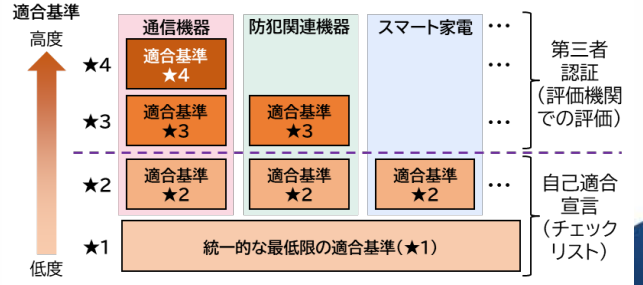
定められた適合基準への適合を示す目印

- 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

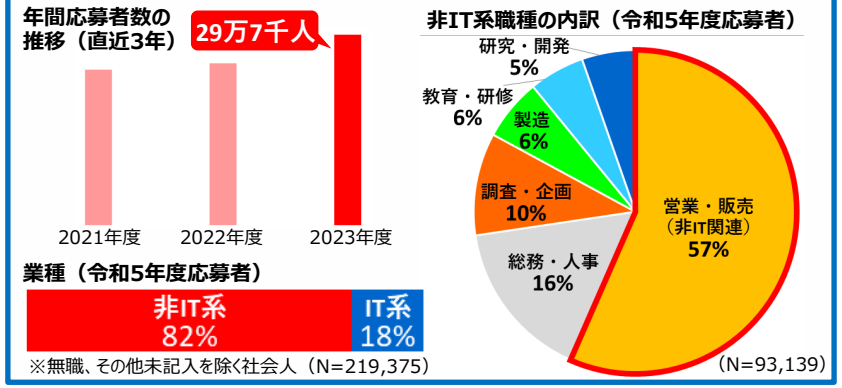
・ITを利活用するすべての社会人・学生が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

・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

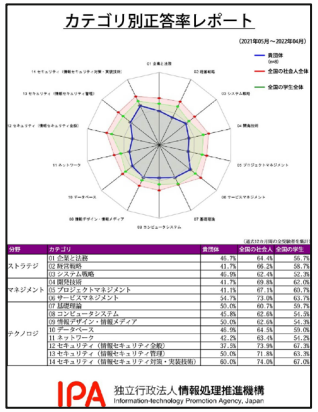


受験申込みはITパスポート試験サイトで受付けています。
また、同サイトでは、合格者の声や企業の声などを掲載していますので、是非ご覧ください。
ITパスポート試験サイト
▶https://www3.jitec.ipa.go.jp/JitesCbt/index.html

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		合格率
			総合評価	分野別評価	
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

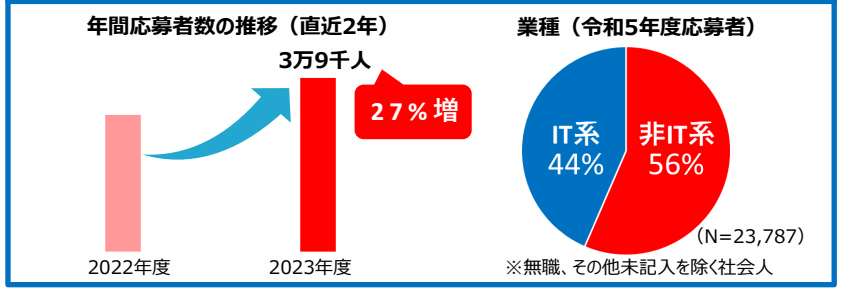
・IT利用者の情報セキュリティ対策に特化した国家試験です。組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的なスキルを認定します。

・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！



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
		科目A	科目B		総合評価
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