サイバー脅威動向と中小企業における基本的なセキュリティ対策について

2025年2月28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 普及啓発・振興部
普及啓発グループ 小山祐平

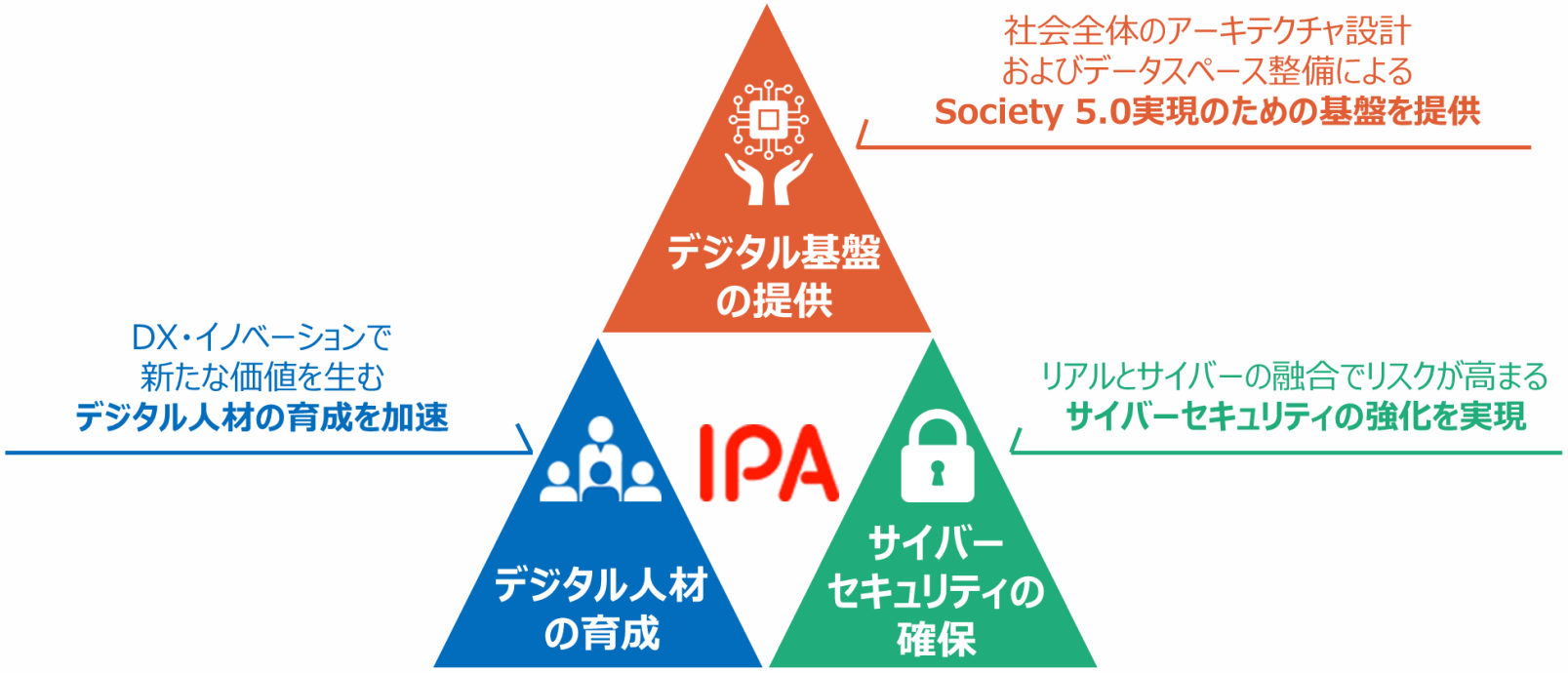
IPA Better Life with IT

IPAの紹介

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。

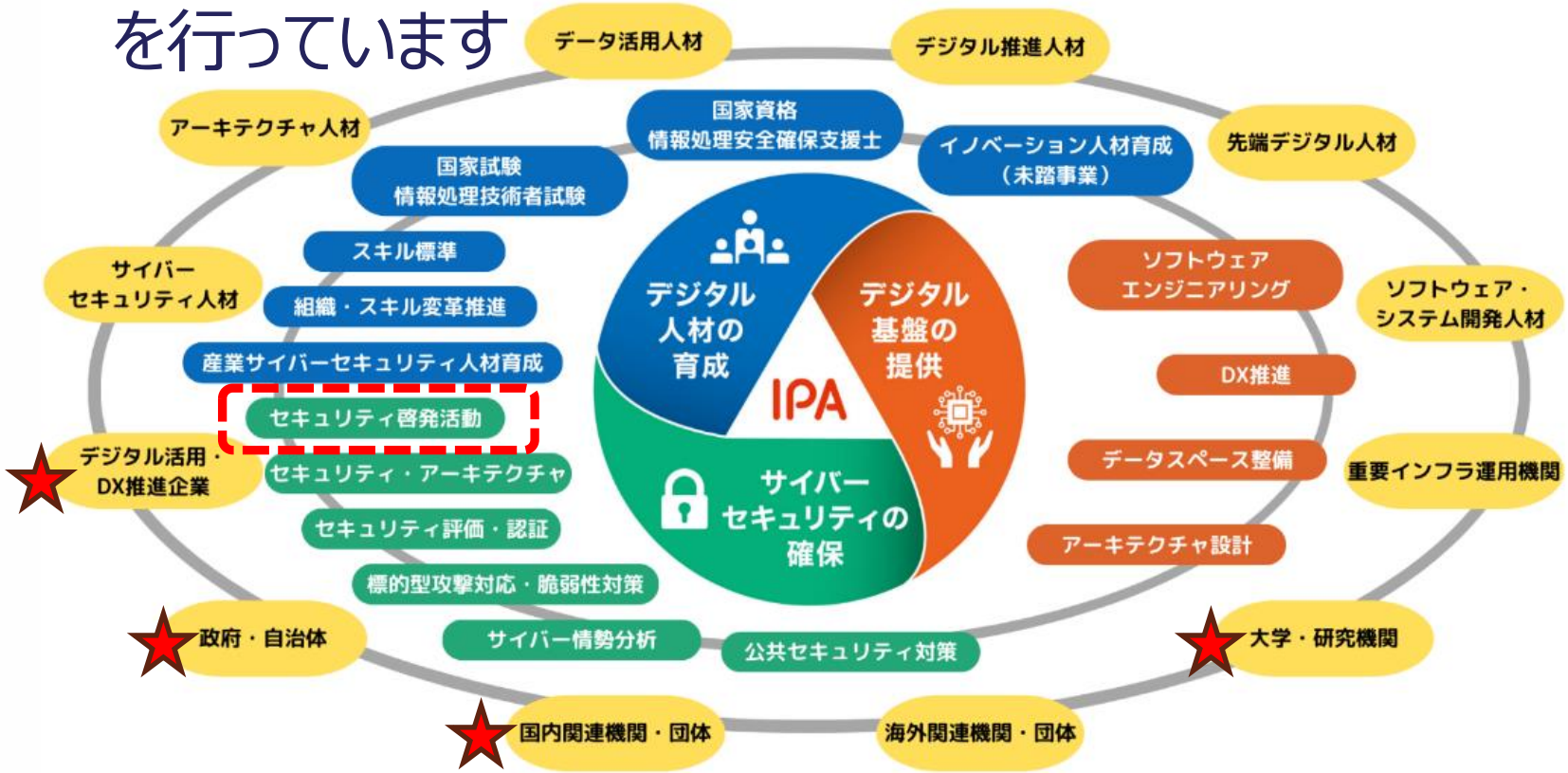
「**人材**」、「**セキュリティ**」、「**デジタル基盤**」の3つの中核事業



■ **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**

IPAの取り組み

- デジタルで豊かな社会の実現に向けて、幅広い取り組みを行っています



『IPA』で検索！

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39万者
（2024年12月）

サイバーセキュリティ CSお助け隊

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）

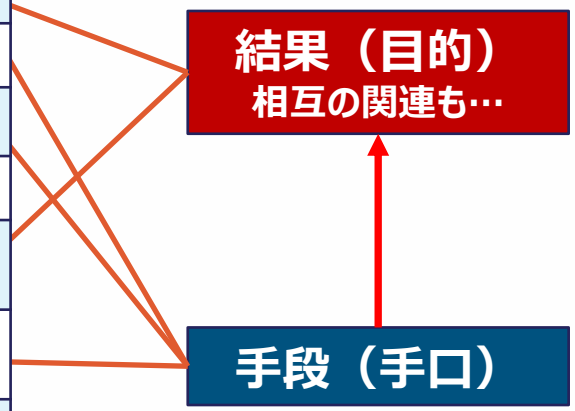
サイバー脅威動向

「情報セキュリティ10大脅威2025」

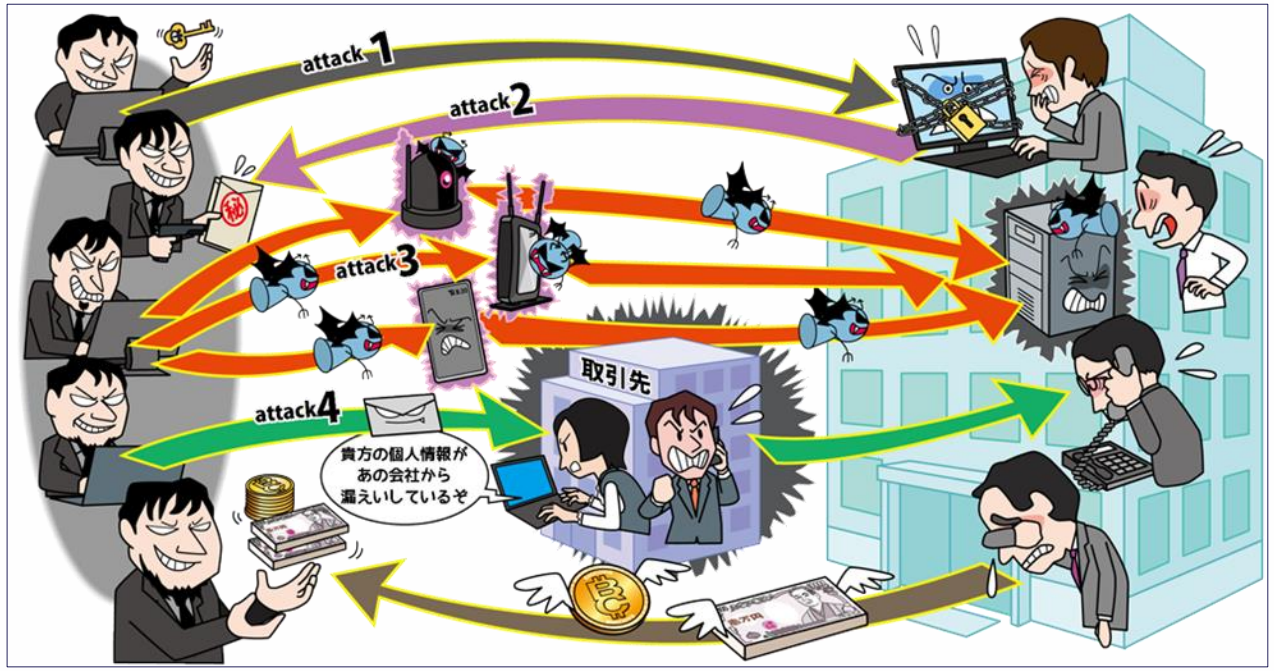
最近の「組織」における脅威動向

- **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



【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
- 組織の規模や**業種に関係なく**攻撃される

【出典】 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

ランサムウェア攻撃事例（１位）

- 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

※関係機関の発表や各種報道に基づく

ランサムウェア攻撃事例（１位）

- **業務委託先が被害を受けた事例**
  - **関通社･倉業サービス社(2024年9月)**
    - 物流関連システム等の停止による業務影響。一部個人情報漏えい等の疑い(関通社は後に漏えいの事実なしと公表)
  - **東京ガス子会社（2024年6月）**
    - 同社の子会社(東京ガスエンジニアリングソリューションズ)が受託していた委託元組織(水道局･ガス局等)の個人情報漏えいの疑い
  - **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した疑い
    - 情報管理に一部不備あり、同社が取得していたISMS認証などが一時停止

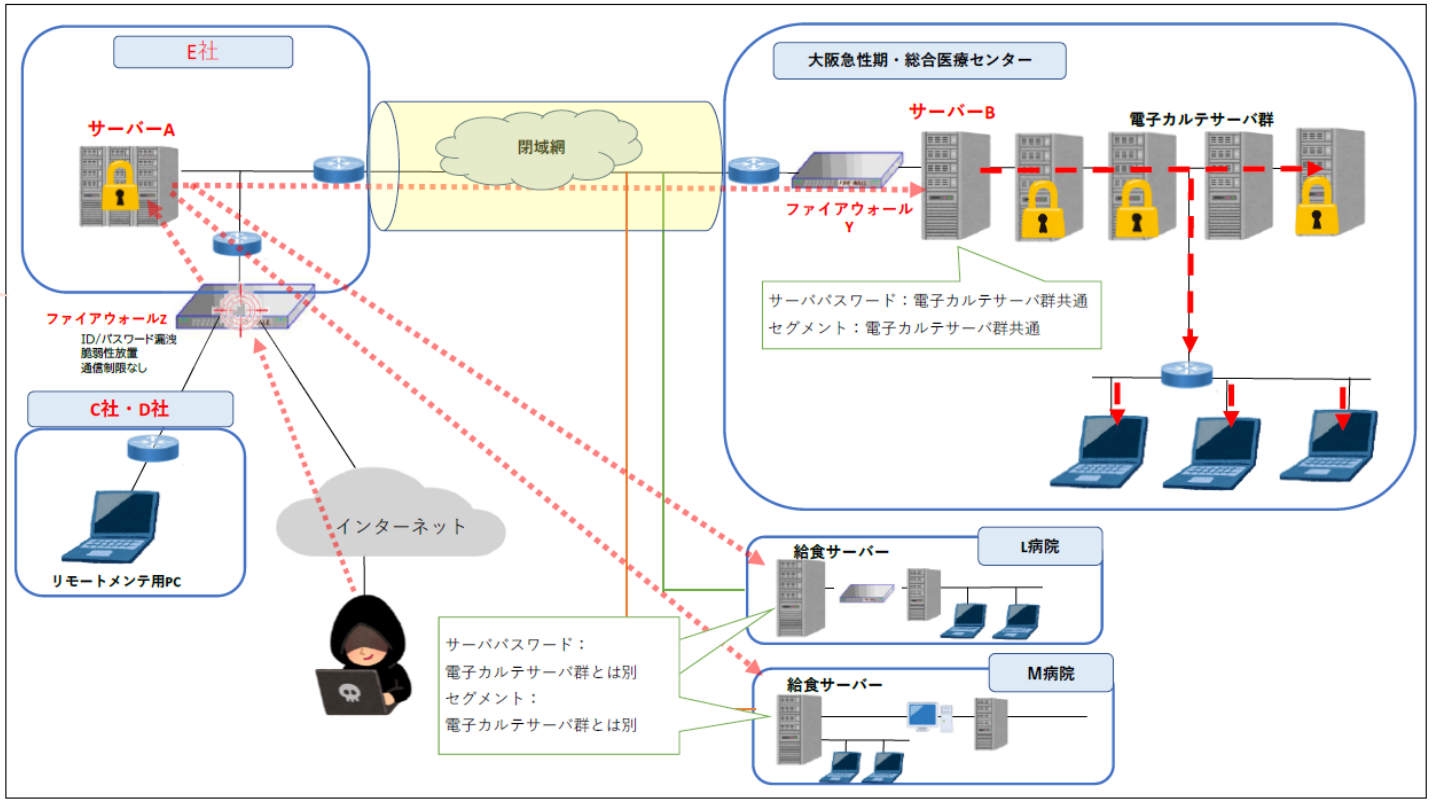
※関係機関の発表や各種報道に基づく

参考）取引先を侵入経路とした攻撃

《大阪急性期・総合医療センターへのランサムウェア攻撃事案》（2022年10月）

- 取引先事業者の脆弱な機器を介して侵入された。

VPN機器（FW）
・脆弱性の放置
・ID/PWの漏えい

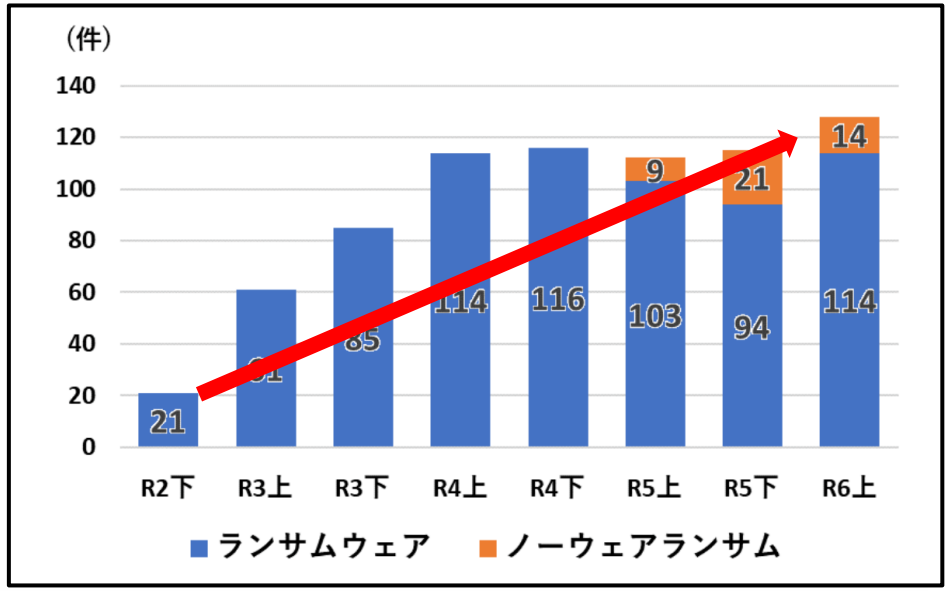


出典：大阪急性期・総合医療センター情報セキュリティインシデント調査委員会「調査報告書」

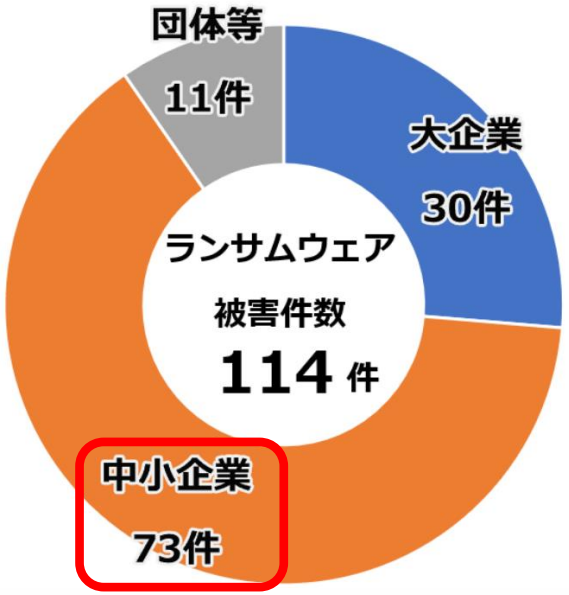
サイバー攻撃は企業規模、業種を問わない
～警察庁のレポートに見られるランサムウェアの状況①～

- ランサムウェアの被害は右肩上がり。64%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

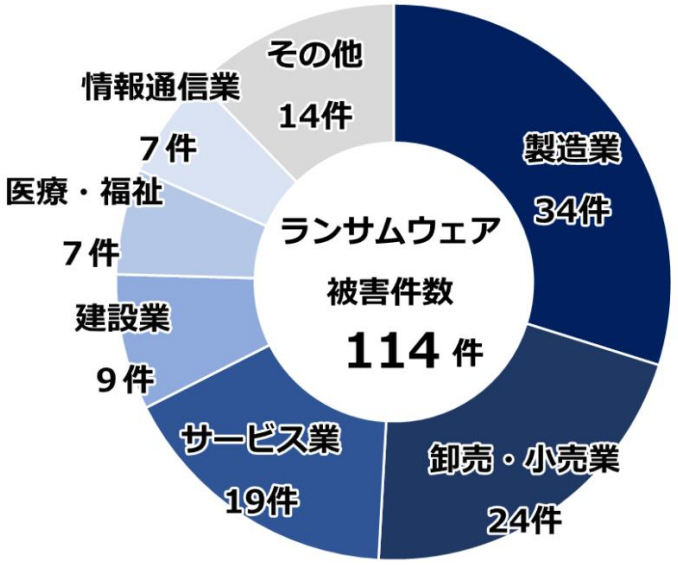
企業・団体等におけるランサムウェア被害の報告件数の推移



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

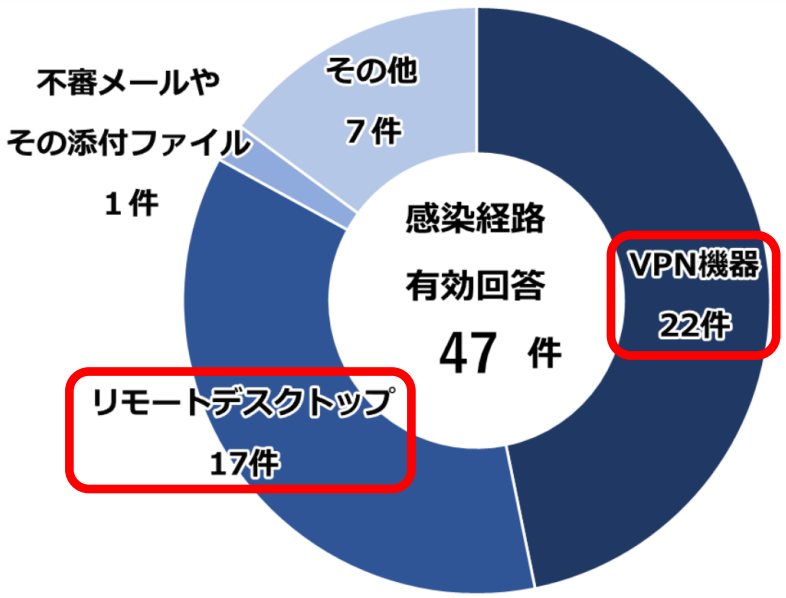


令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）：
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

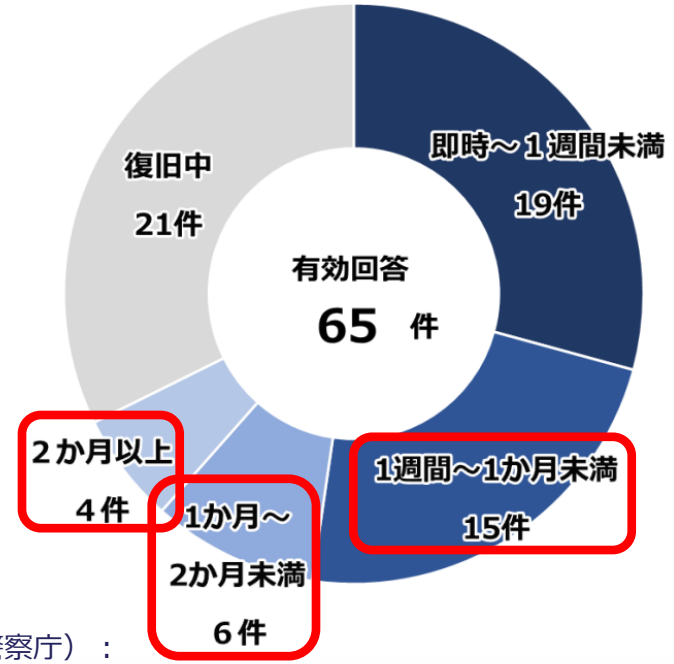
ランサムウェアに感染してしまった場合の影響は甚大
～警察庁のレポートに見られるランサムウェアの状況②～

- 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38%以上
- 半数以上が調査・復旧に500万円以上を要していた。

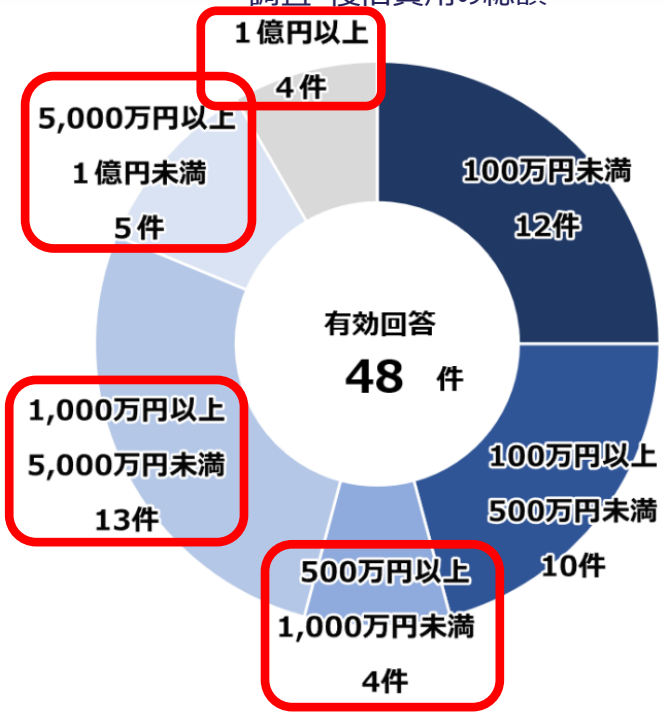
感染経路



復旧に要した期間



調査・復旧費用の総額



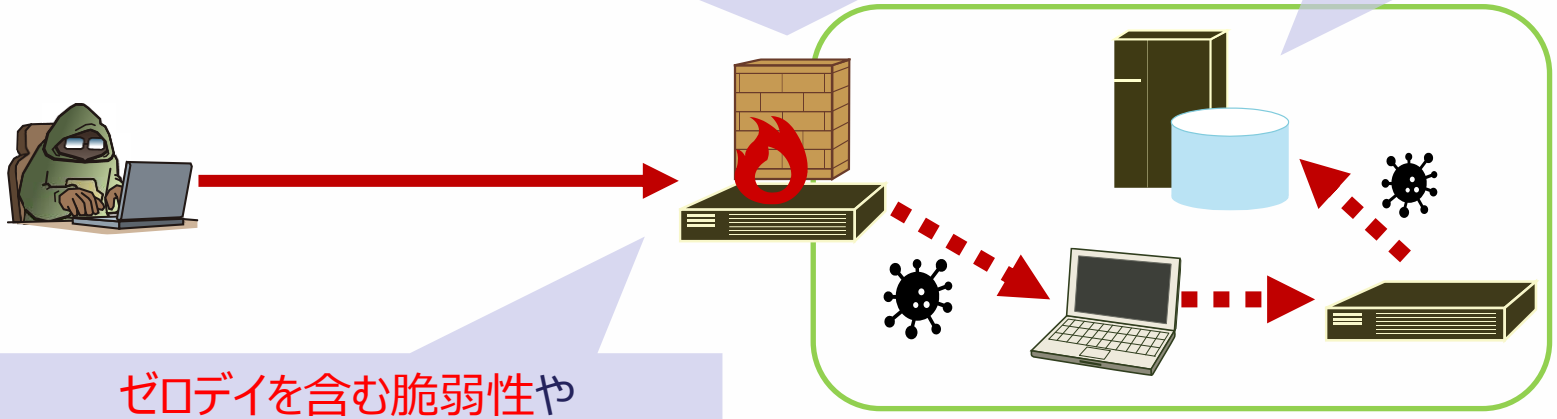
令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）：
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

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

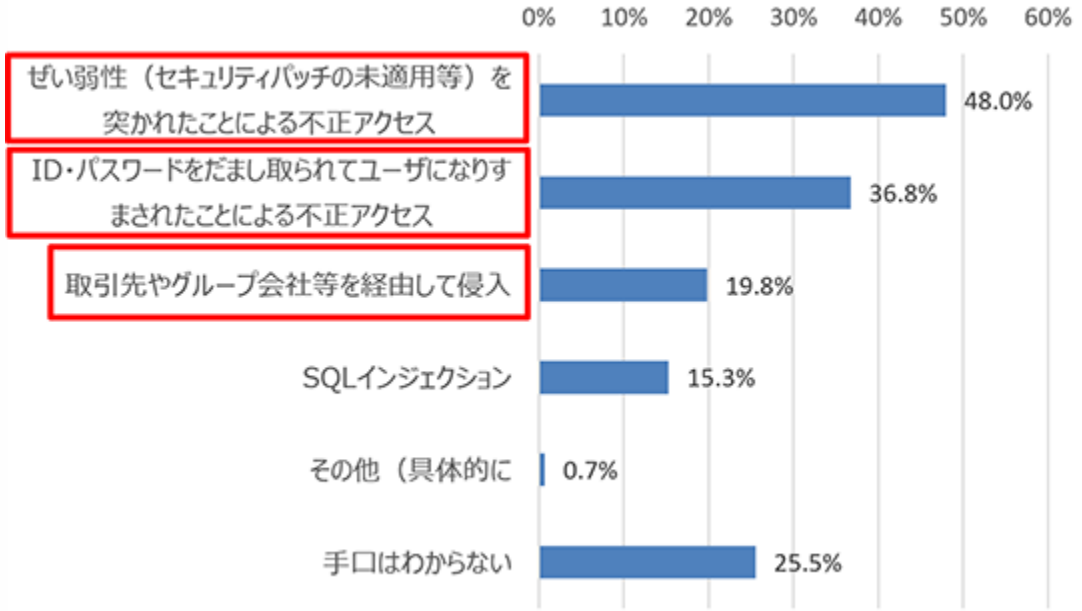
平時から対策を

- 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。

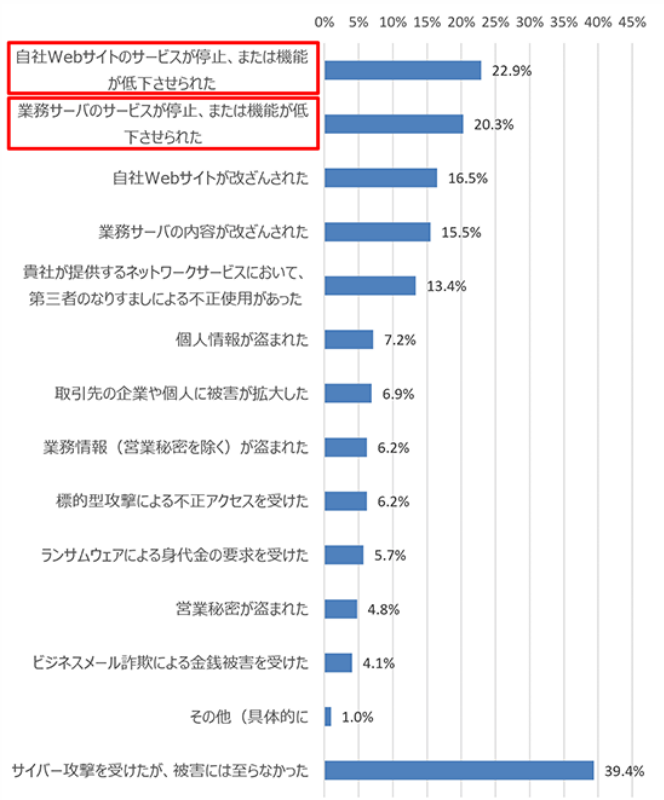
中小企業における状況と課題

不正アクセスの手口・被害の内容

- 不正アクセスされた企業の**約５割**が脆弱性を突かれ、他社経由での侵入も**約２割**



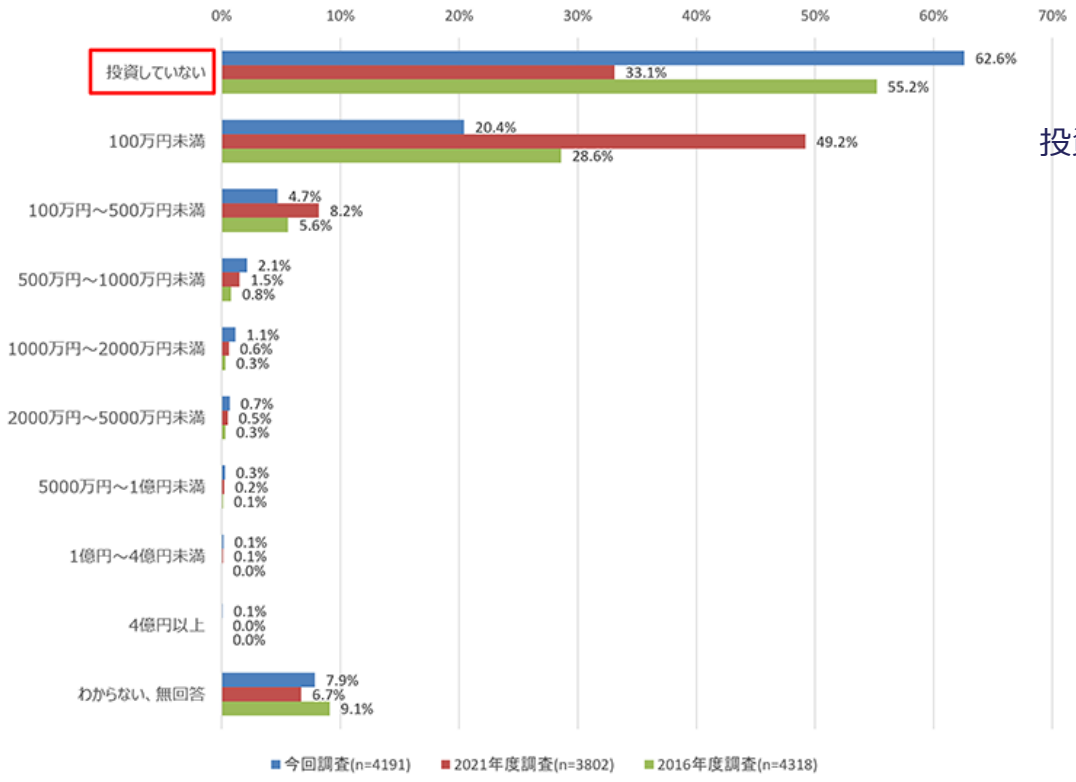
質問：貴社が受けたサイバー攻撃の手口について教えてください。（MA）



質問：貴社が受けたサイバー攻撃の被害について教えてください。（MA）

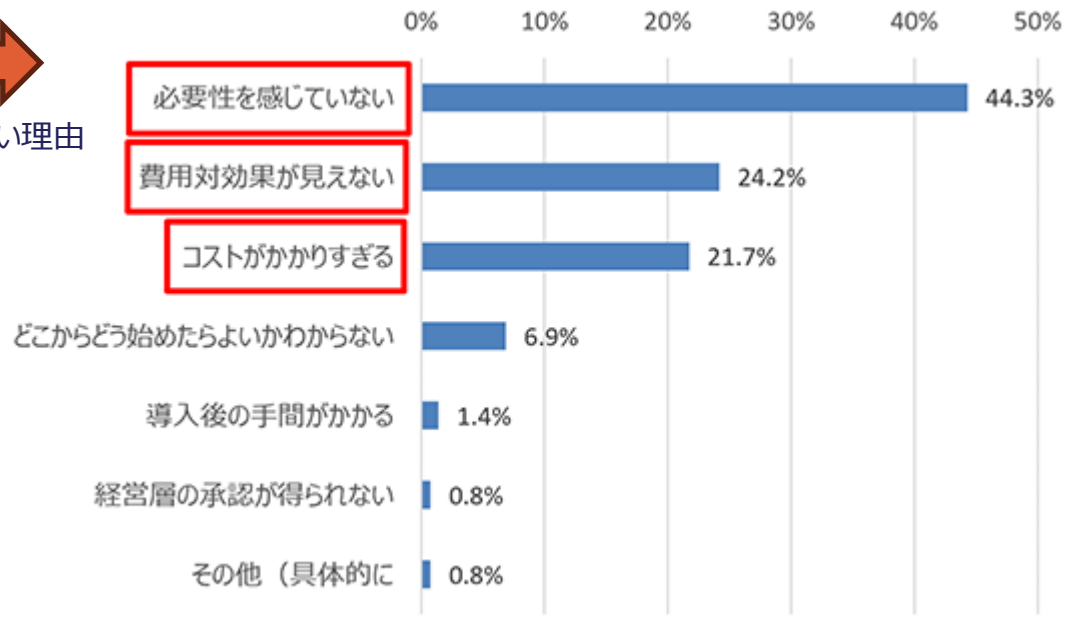
直近過去3期の情報セキュリティ対策投資

- 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）

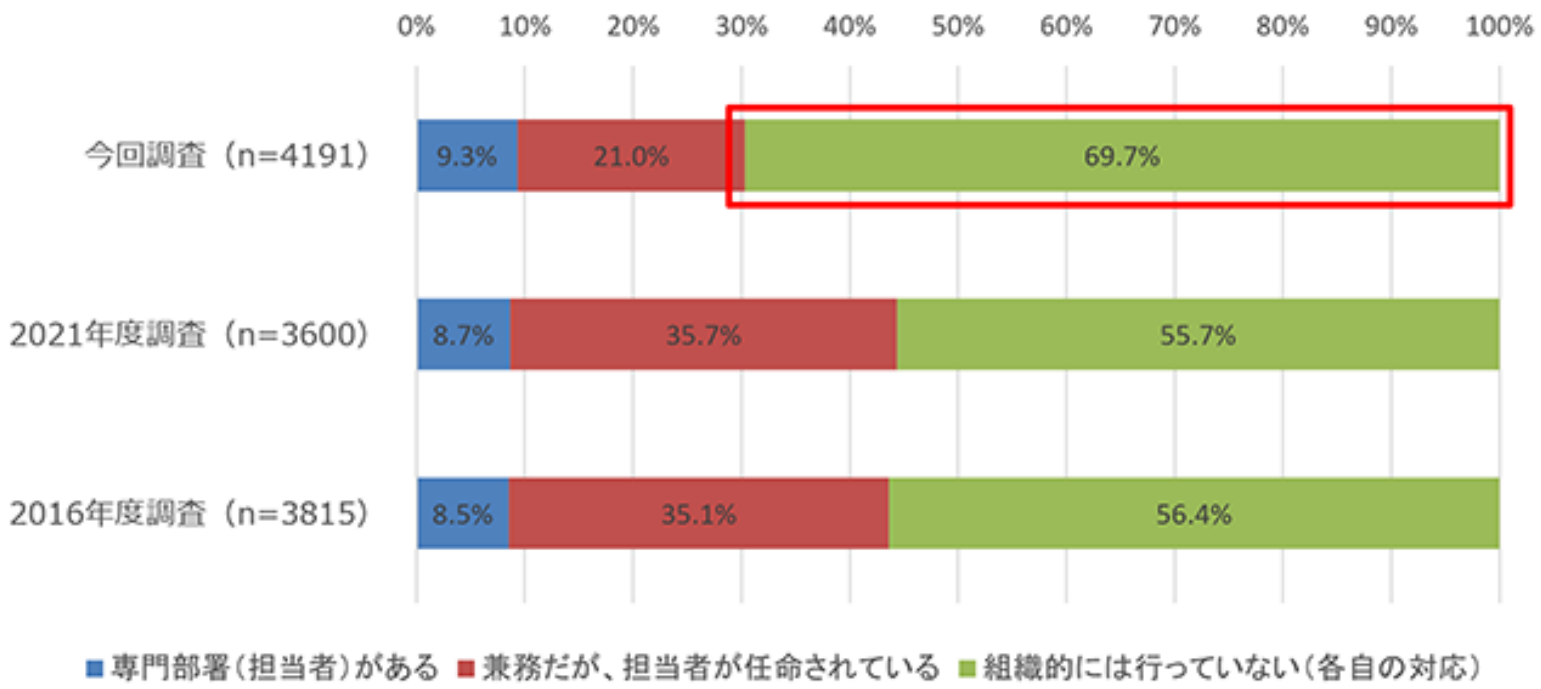
投資していない理由



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

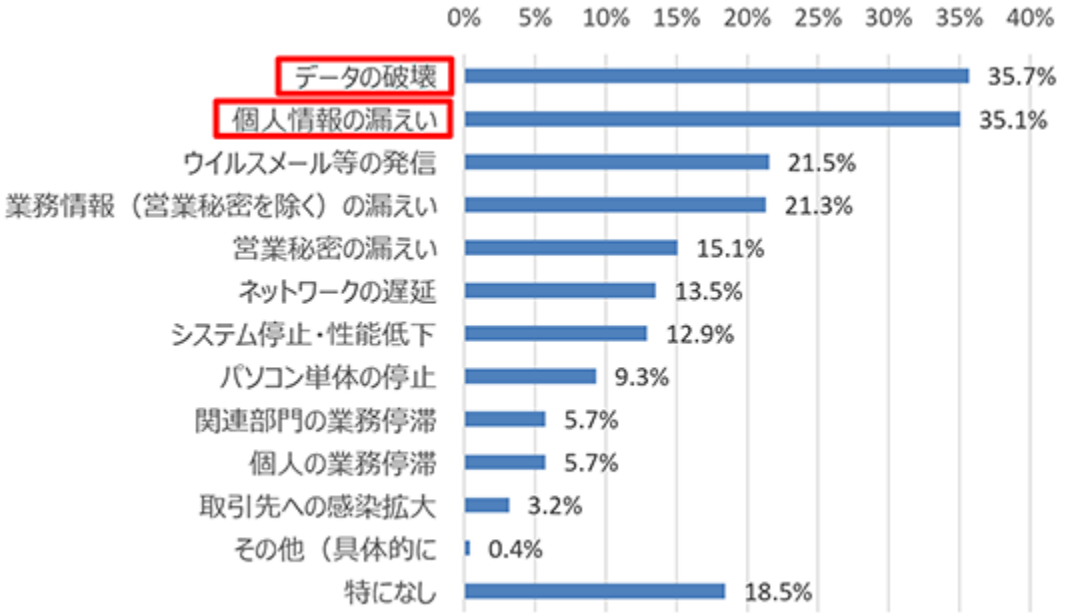
- **約７割**の企業が組織的なセキュリティ体制が整備されていない



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

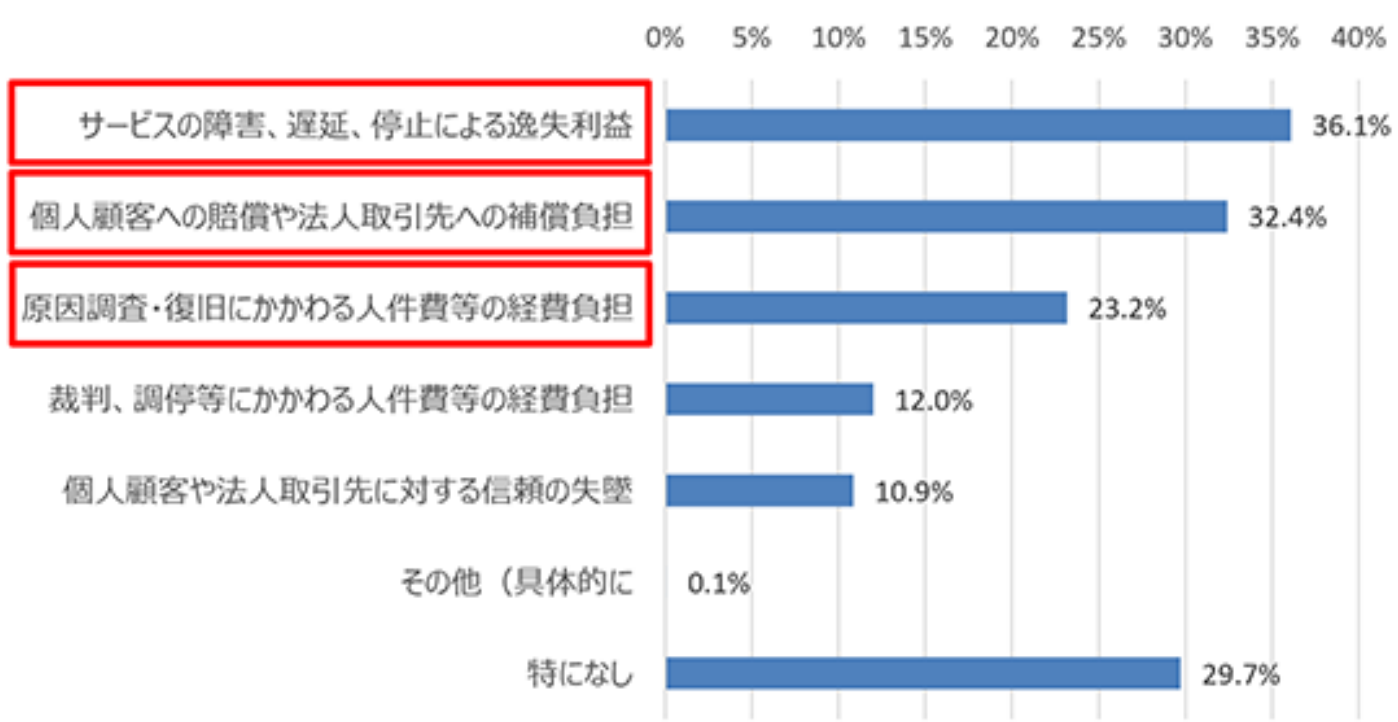
- 過去3期内で、サイバーインシデントが発生した企業における被害額の平均は**73万円**（うち9.4%は100万円以上）、
  復旧までに要した期間の平均は**5.8日**（うち2.1%は50日以上）



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

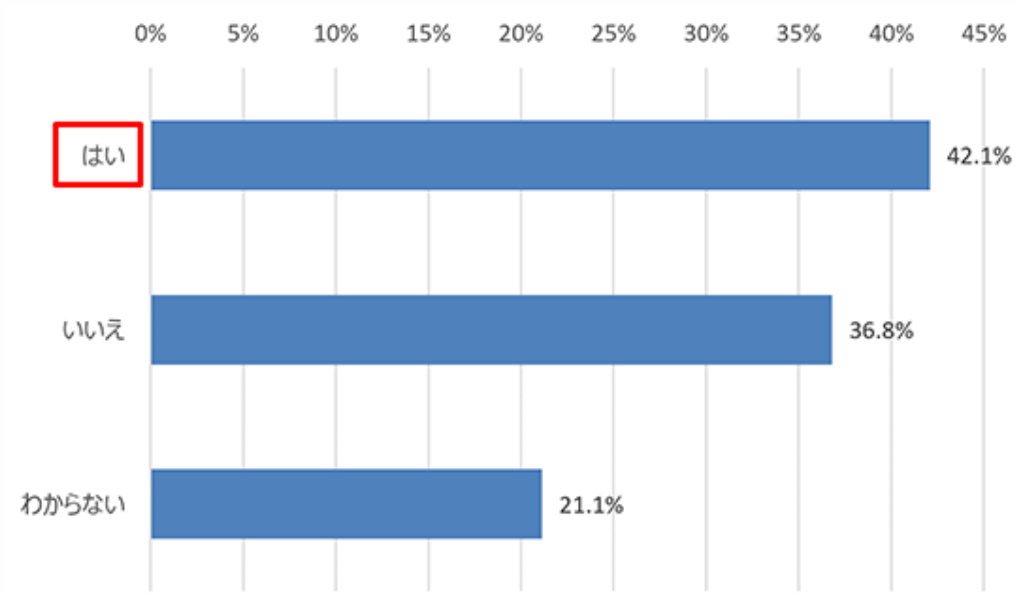
- サイバーインシデントにより取引先に影響があった企業は**約７割**

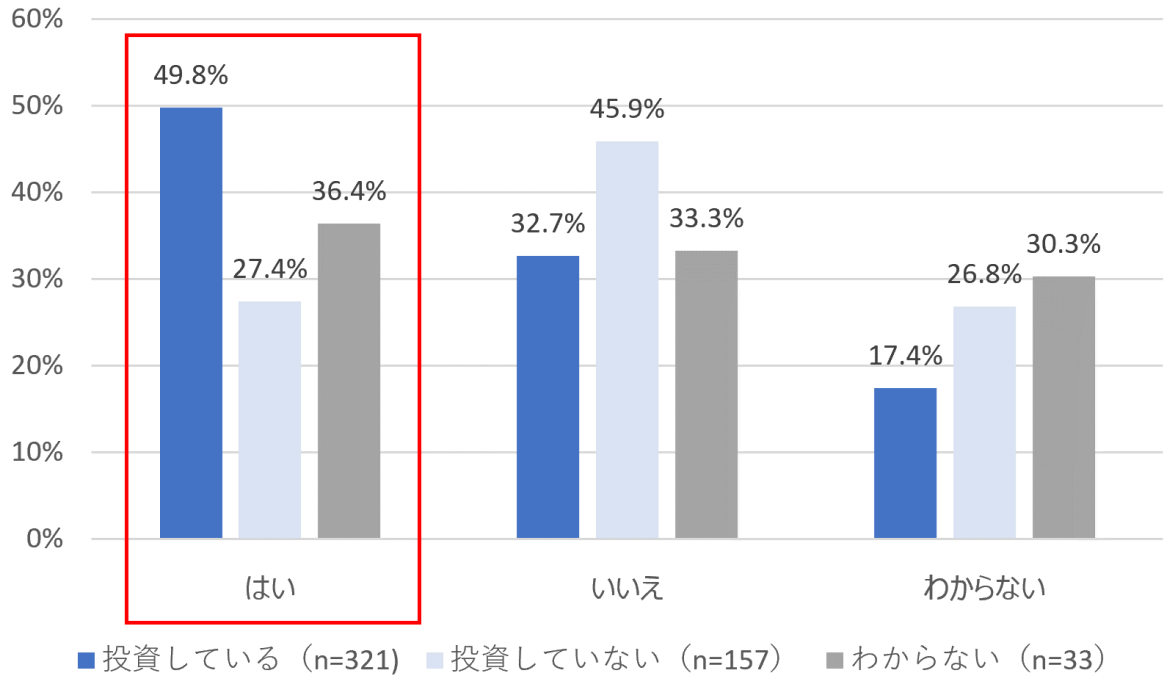


質問：サイバーインシデントにより貴社の取引先（サプライチェーン）に影響はありましたか。影響が及んだ場合はその内容について教えてください。（MA）

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



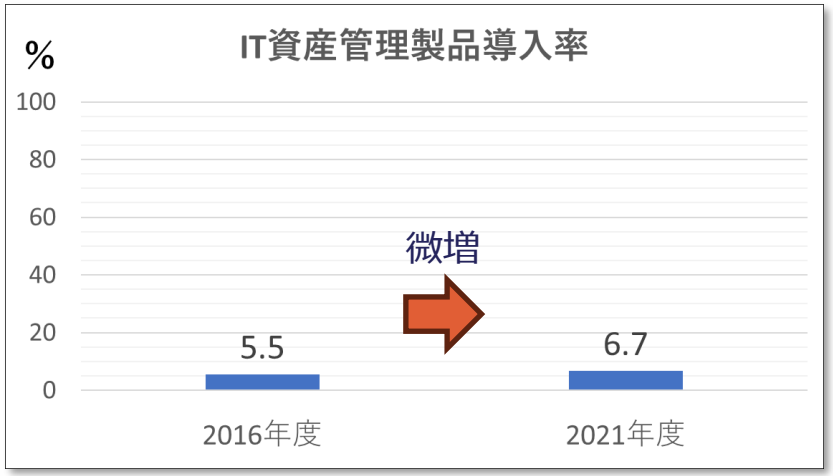


質問：貴社は取引先（発注元企業）から要請された情報セキュリティ対策を行ったことが取引先との取引につながった大きな要因だと思いますか。（SA）

IT資産管理とアタックサーフェスマネジメント

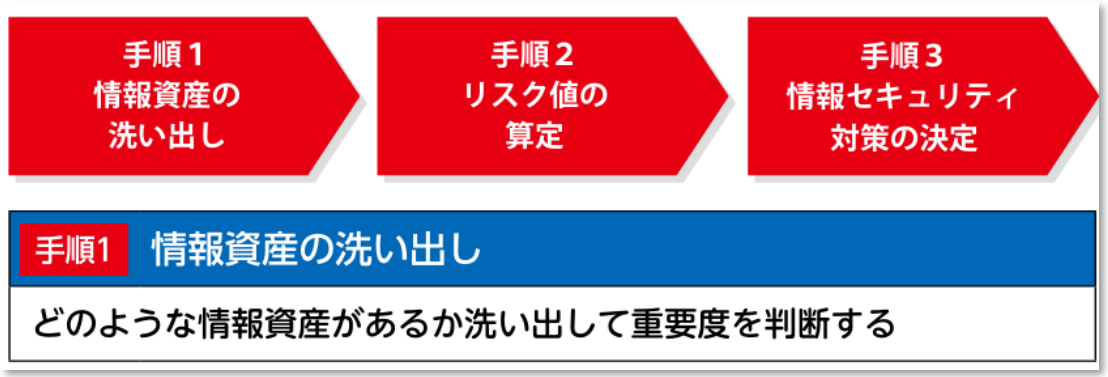
- 組織やサプライチェーンでのIT資産管理（組織で運用しているIT機器が何か、稼働ソフトウェアも含めた管理）が不十分で脆弱性が残置し、ランサムウェア攻撃や標的型攻撃のターゲットになるリスクがあります。
- 特に、中小企業では、IT資産の管理が進んでいないため、取り組むことが重要です。

IT資産管理状況（2016→2021）



出典：IPA「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」

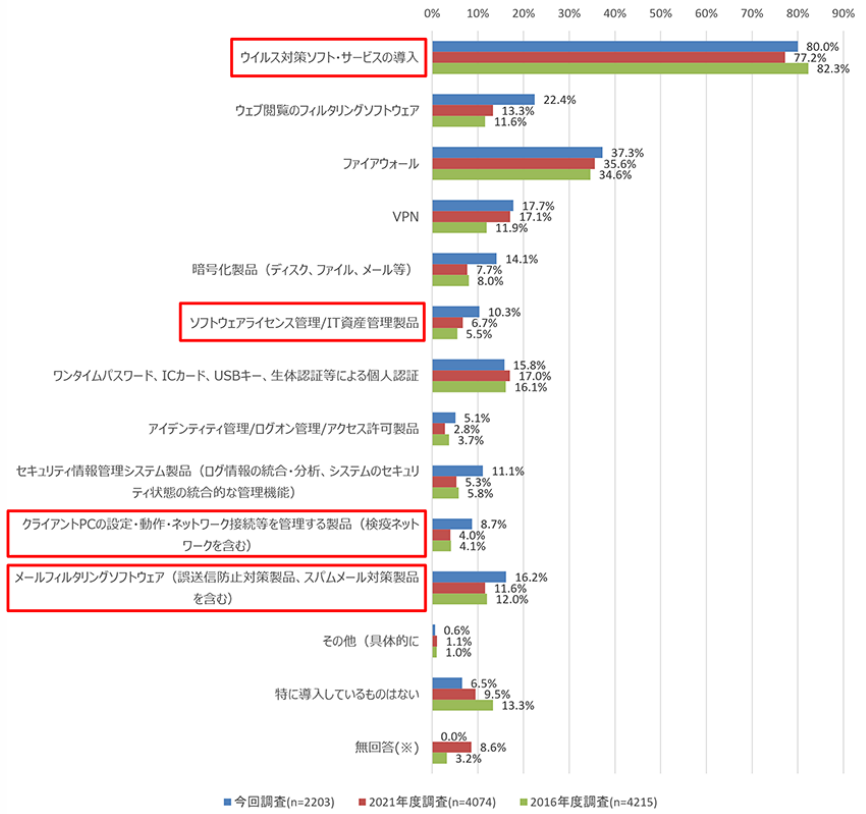
IT資産の洗い出しと管理は セキュリティ対策の“一丁目一番地”



出典：IPA「中小企業の情報セキュリティ対策ガイドラインV3.1」

情報セキュリティ関連製品やサービスの導入状況

- 情報セキュリティ関連製品やサービスの導入状況は**微増**



質問：貴社では情報セキュリティ関連製品やソフトウェアを導入していますか。導入している情報セキュリティ関連製品やソフトウェアを教えてください。（MA）

対策の基本

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**かつ**多層的**に
- 公的機関等が提供する**ツール**や**制度を活用**

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**

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

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
機器やソフトウェア脆弱性	最新の更新プログラムの適用	脆弱性を悪用した攻撃を防ぐ
ウイルス感染	セキュリティ対策ソフトの利用	攻撃をブロック、検知する
パスワード窃取・解析	パスワードの管理・認証の強化	パスワード窃取による不正アクセスを防ぐ
設定不備	共有設定や公開設定の見直し	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

＋実施するためのルール・体制づくり

中小企業向け支援ツール、制度

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

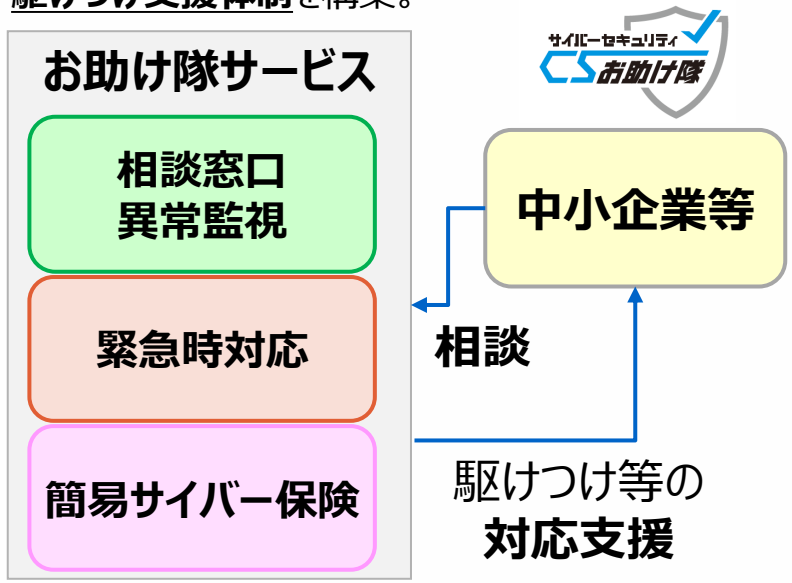
SECURITY ACTION

- 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

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)

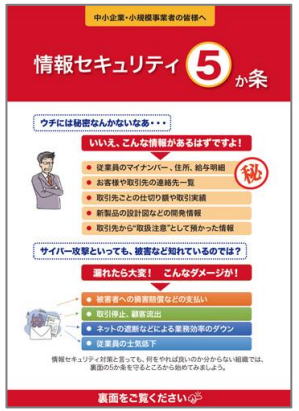
付録4：情報セキュリティハンドブック（ひな形）(PowerPoint)

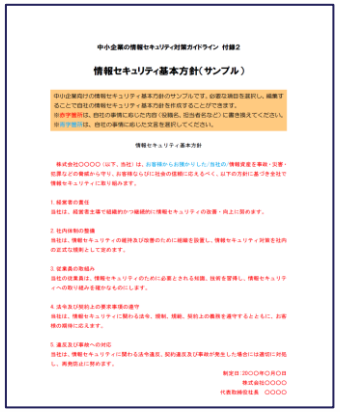
付録5：情報セキュリティ関連規程（サンプル）(Word)

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)

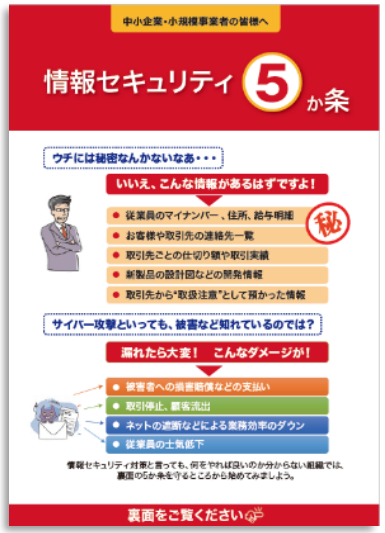




本ガイドラインの活用法

- **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

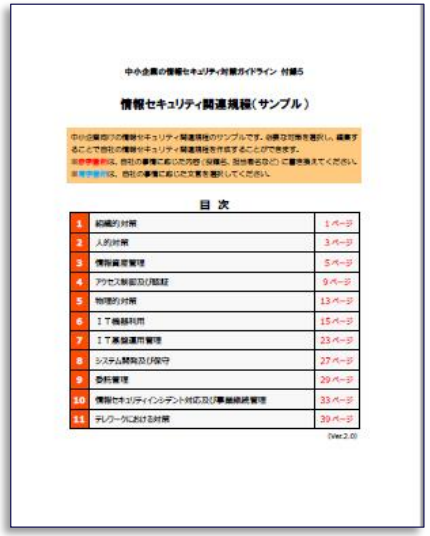
SECURITY ACTION ★一つ星を宣言

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

情報セキュリティ5か条

IPA

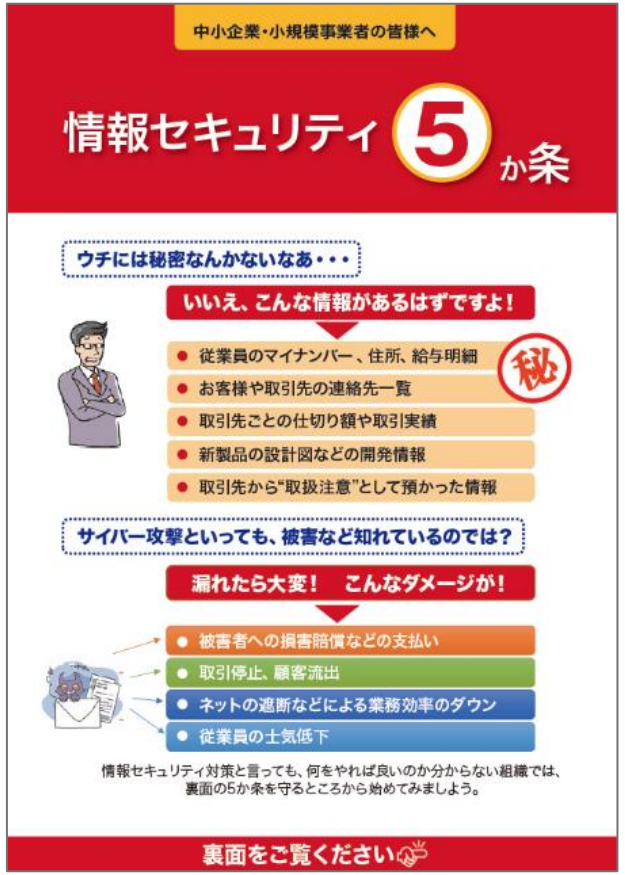
SECURITY ACTION
セキュリティ対策自己宣言

● 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

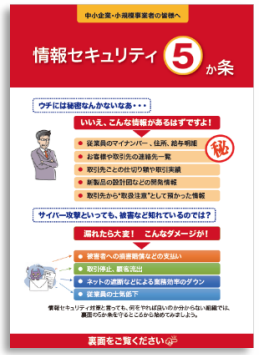


SECURITY ACTION制度について

- 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



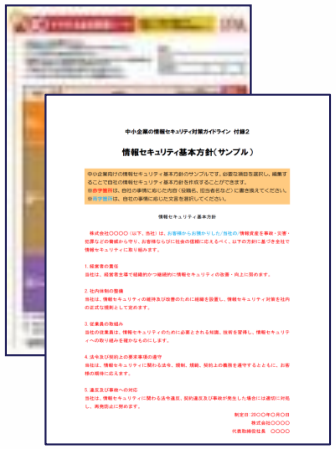
１段階目（一つ星）

●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



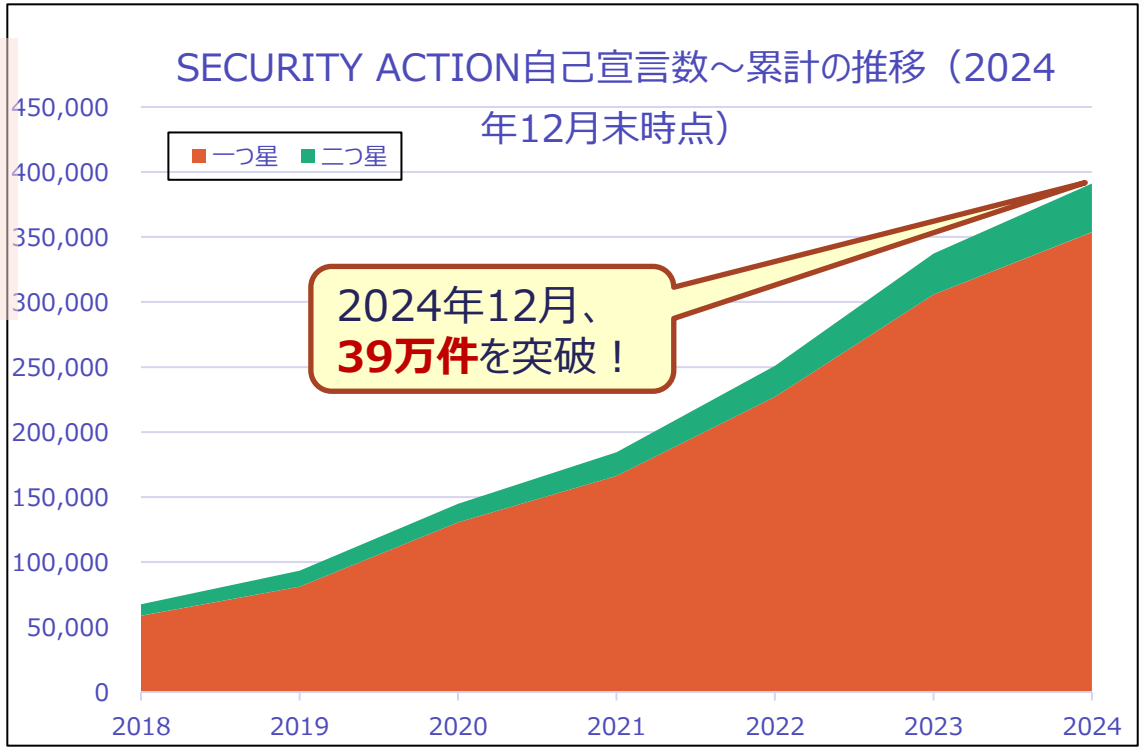
2段階目（二つ星）

●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



【参考】自治体等におけるSECURITY ACTION制度の活用

- 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

【自治体等におけるSA制度の活用事例】 ※2024年10月時点

- **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)(16 次締切分まで）：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**

- **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**
- **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**
- **デジタル技術導入補助金：愛知県**
- **デジタル化促進補助金：北海道札幌市**
- **産業デジタル実装支援事業費補助金：宮崎県**
- **2023年度年度 DX（デジタル化）設備導入補助金：石川県（令和5年度新規）**
- **かごしま中小企業DX推進事業費補助金：鹿児島県 【令和6年度新規】**

- **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

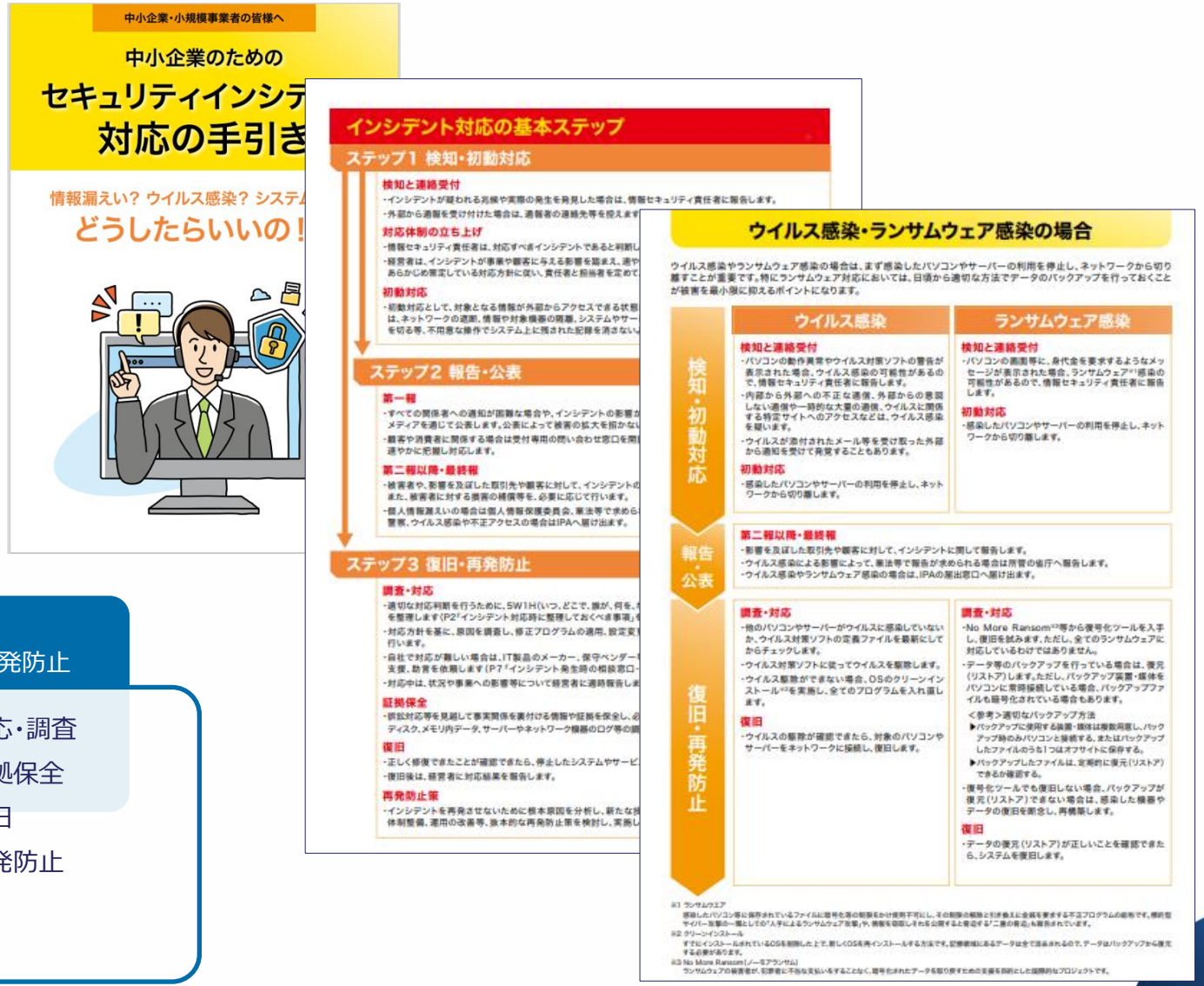
中小企業の情報セキュリティ対策ガイドライン付録8

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

https://www.ipa.go.jp/security/sme/ps6vr7000001buco-att/ps6vr7000001bucx.pdf

IPA

- 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

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/sme/otasuketai/index.html

- 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**38社**から**56サービス**が展開
- ネットワーク監視型、端末監視型、ネットワーク監視・端末監視併用型あり
- **IT導入補助金（セキュリティ対策推進枠）**が利用可能　※2024年度の募集は終了

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

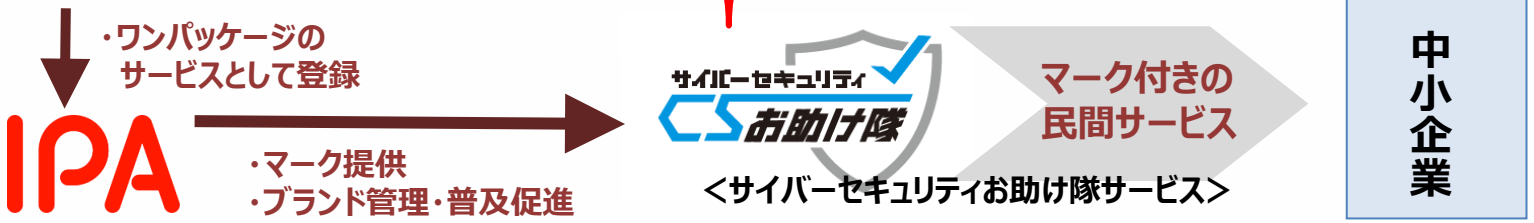
24時間見守る仕組み
ネットワーク監視型
端末監視型
その併用型

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

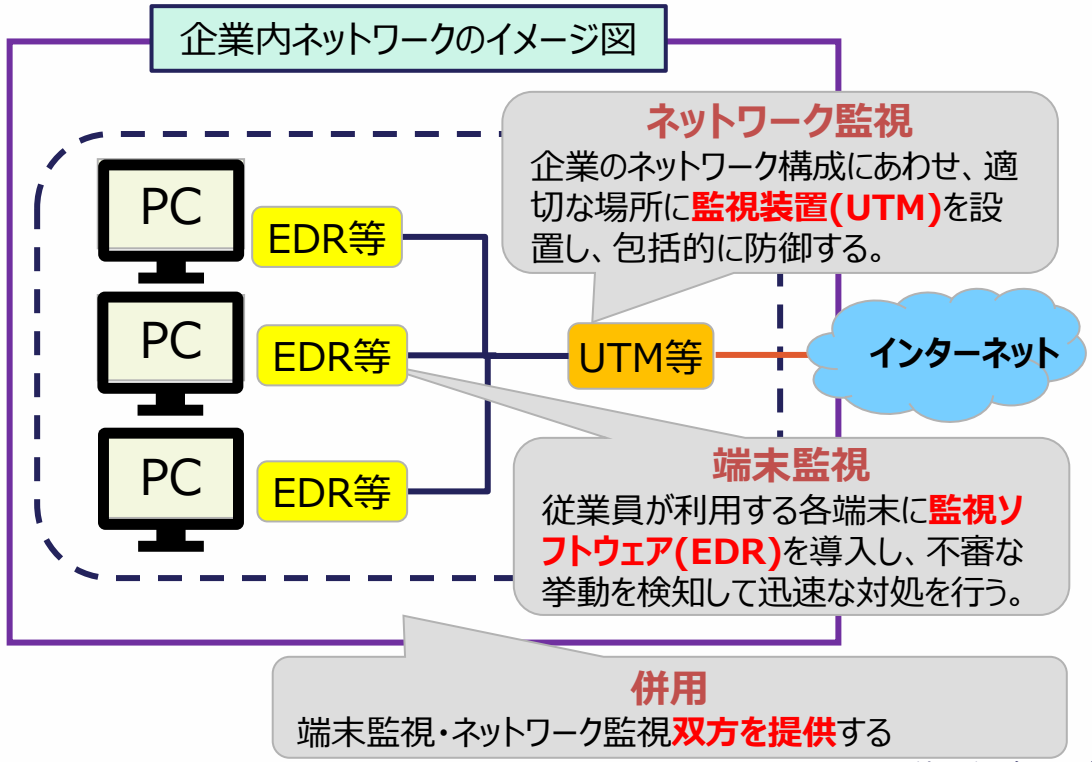
中小企業でも導入、維持できる価格
・ネットワーク監視型：月額１万円以下
・端末監視型：月額2,000円以下／台
・併用型：これらの合算相当価格以下



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**、**端末監視**またはその両方（**併用**）による異常監視の仕組みを提供。

◇サイバーセキュリティお助け隊サービスの監視タイプ

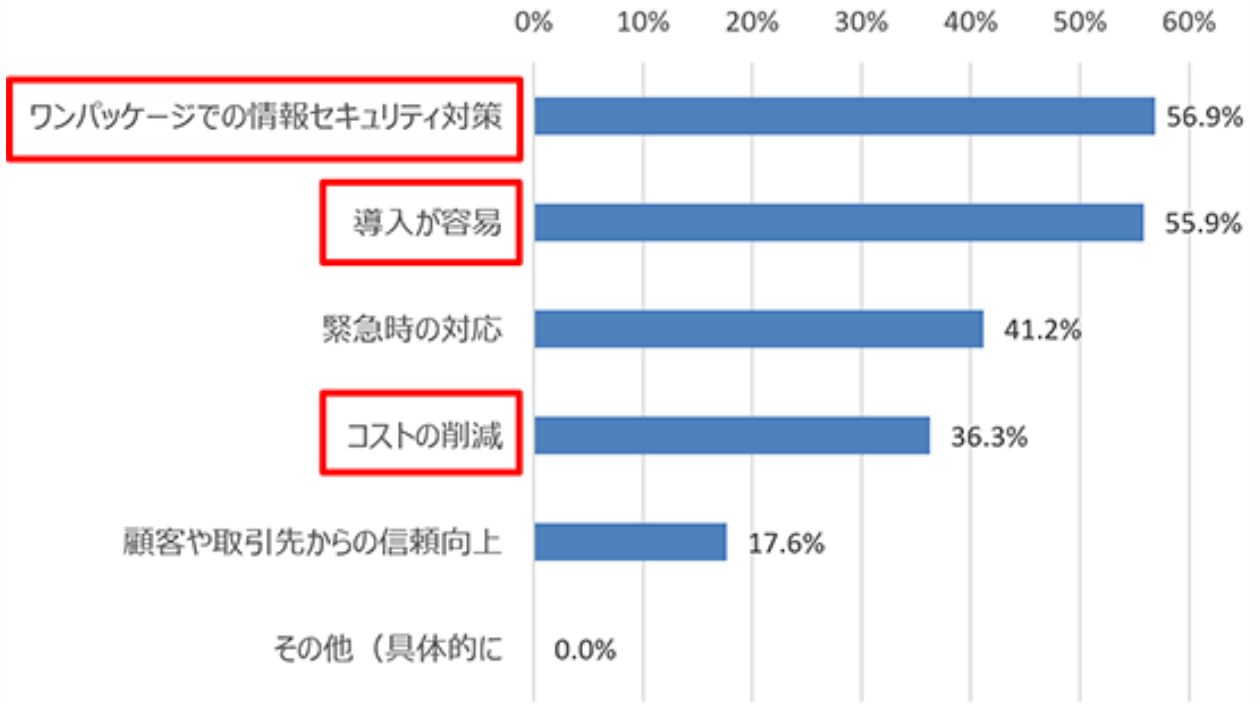


タイプ	特長（メリット）	導入の注意点
ネットワーク監視	• 機器1台で監視が可能なため、設定やバージョンアップ等の更新作業などの**運用コスト、業務負担が軽い**。（セキュリティ管理者のみの対応）	• 内外の通信を監視するため、機器導入により**メールの送受信に時間**がかかったり、ネットワーク接続に遅延が生じたりする可能性があるため確認が必要。
端末監視	• 社外での打ち合わせであったり、テレワーク勤務など、**社内ネットワーク外に持ち出されたPCであっても監視が可能**。	• 導入する**PC台数に応じてコストが高くなる**ため、社内ネットワークに接続しているPC台数の確認と、セキュリティソフトによってはインストールできないPCもあり、確認が必要。
併用	• ネットワーク監視と端末監視の両方を設置し、**多層的に防御**を行う形態のため、**より強固なセキュリティ監視**が可能。	• ネットワーク監視、端末監視の**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）。

※UTM(Unified Threat Management)：ネットワークセキュリティ監視装置
※EDR(Endpoint Detection and Response)：エンドポイントセキュリティソフトウェア

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

- 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。あてはまるものを下記よりすべてお選びください。（ＭＡ）

【参考】IT導入補助金2025　セキュリティ対策推進枠

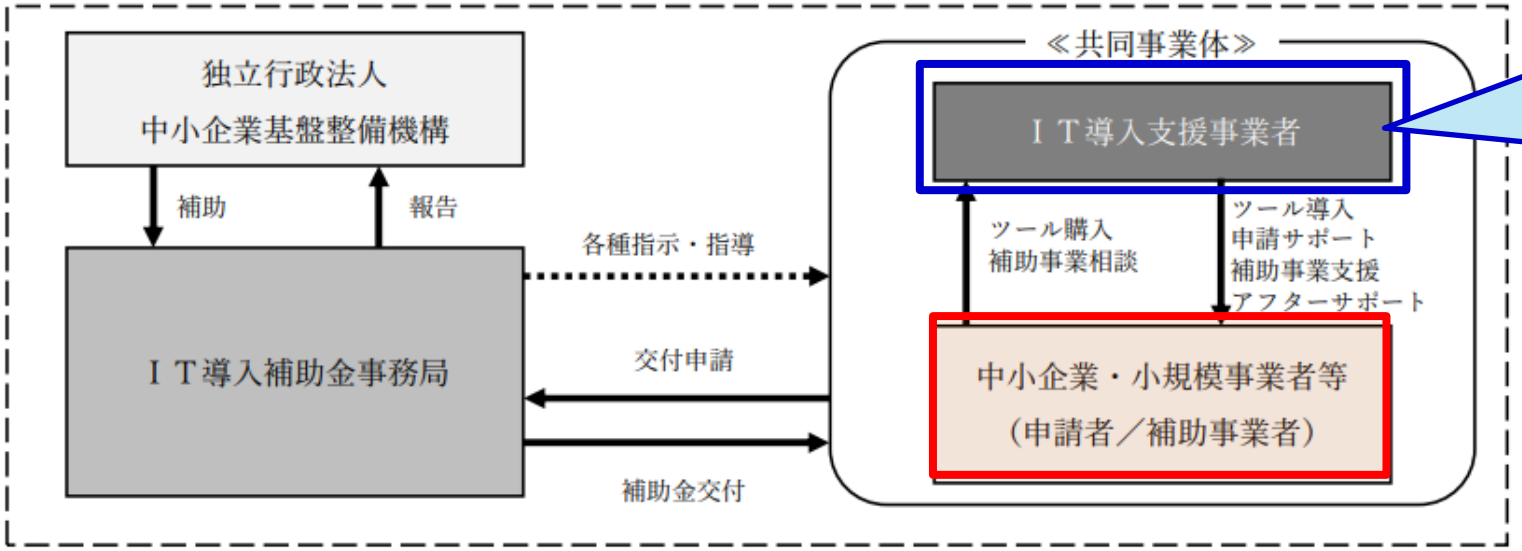
https://it-shien.smrj.go.jp/applicant/subsidy/security/

IPA

● 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	1/2以内 ※小規模事業者は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	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2024 公募要領セキュリティ対策推進枠」から転載、引用
https://it-shien.smrj.go.jp/pdf/r5_koubo_security.pdf

その他の支援ツール、制度

「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

- 組織の情報漏えいに関する内部不正対策に特化したガイドライン。2022年4月に改訂第5版発行。
  - 内部不正は「動機・プレッシャー」「機会」「正当化」の３要因が揃った時に発生
  - 組織における内部不正対策のポイントはそれぞれの要因の低減

【組織における内部不正防止ガイドライン】

1．背景
2．概要
3．用語の定義と関連する法律
4．内部不正を防ぐための管理のあり方
- 4-1　基本方針
- 4-2　資産管理
- 4-3　物理的管理
- 4-4　技術・運用管理
- 4-5　原因究明と証拠確保
- 4-6　人的管理
- 4-7　コンプライアンス
- 4-8　職場管理
- 4-9　事後対策
- 4-10　組織の管理

付録Ⅰ～Ⅷ（内部不正事例、チェックリスト等）

状況的犯罪予防の5原則
1．やりにくくする
2．やれば捕まる
3．わりにあわない
4．動機を減らす
5．いいわけさせない
をベースに整理

ECサイトを運営する中小企業の皆様へ

ECサイト構築・運用セキュリティガイドライン

https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

- 近年、ECサイトからの**個人情報及びクレジットカード情報の流出事件**が多数発生。被害の大半が**中小企業の自社構築サイト**
- ECサイトの構築・運用に**必要なセキュリティ対策とその実践方法**をまとめて解説するガイドライン

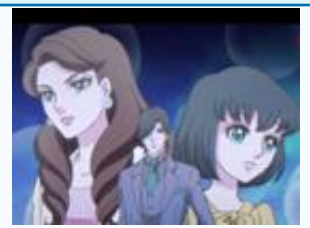
- 「**第1部　経営者編**」と「**第2部　実践編**」で構成
- 「第1部　経営者編」
  - ECサイトを**新規構築、あるいは既に運営している経営者向け**に、自社のECサイトにおけるセキュリティ**対策の必要性**を説明
- 「第2部　実践編」
  - 対策実践の責任者、担当者が、ECサイトの構築時・運用時に**優先する対策**や、自社のECサイトの状況に**見合った対策の範囲や実現方法**を適切に決めていただくための内容

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
- **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

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

■ URL

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

詳細はこちらのページにて

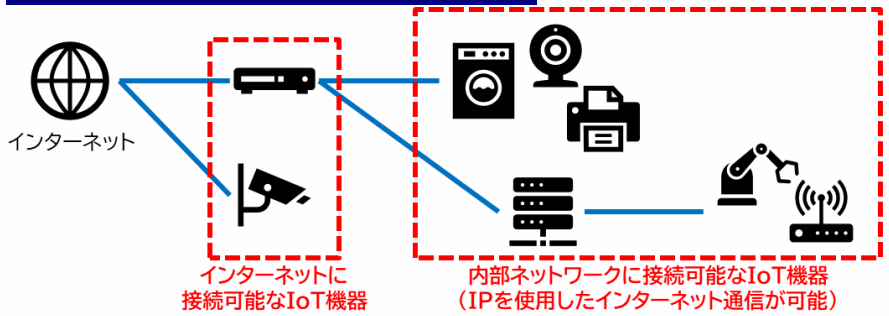
IoT製品セキュリティラベリング制度(JC-STAR)

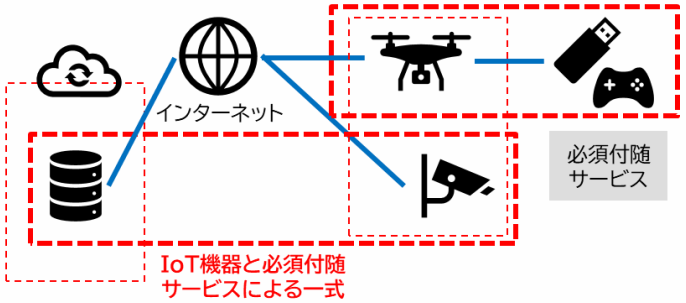
2025年度から、IoT製品に対するセキュリティ要件(適合基準)への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を開始

- 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

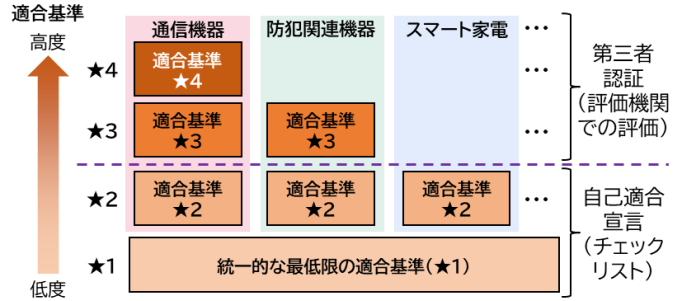
定められた適合基準への適合を示す目印

- 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。

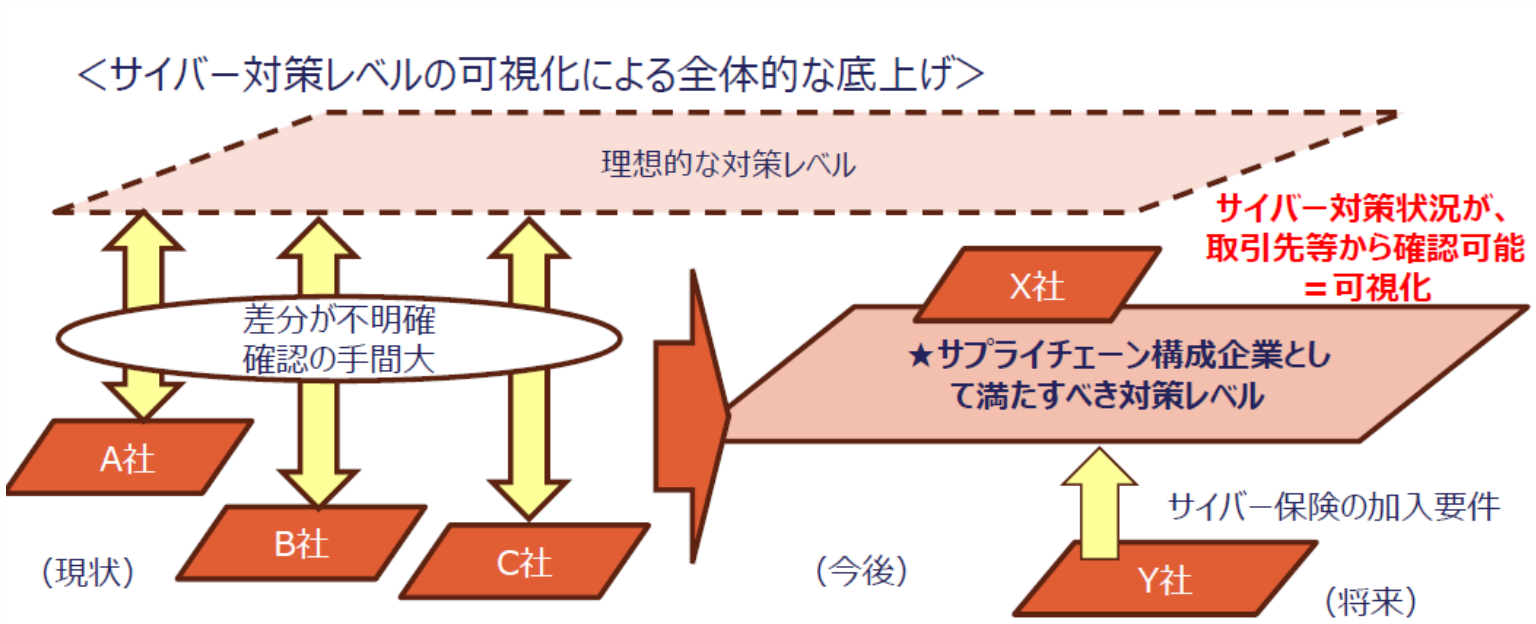
JC-STARの適合基準レベル



参考）政府における検討動向

- サプライチェーン企業のセキュリティ対策の強化に資する観点から、政府では、現在 「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の検討が進められています。

経済産業省「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に関するSWG」第1回資料5より



セキュリティ対策評価制度（イメージ）

三つ星（★３）	四つ星（★４）	五つ星（★５）
サプライチェーン形成企業として最低限満たすべき基準	サプライチェーン形成企業として標準的に満たすべき基準	重要インフラ事業の関連サプライヤーが満たすべき基準
(該当するガイドライン) • ○○ガイドライン…	• △△ガイドライン…	• ●●ガイドライン…
(対策の確認方法) • 自己宣言	• 診断ツール	• 第三者確認