Better Life with IT

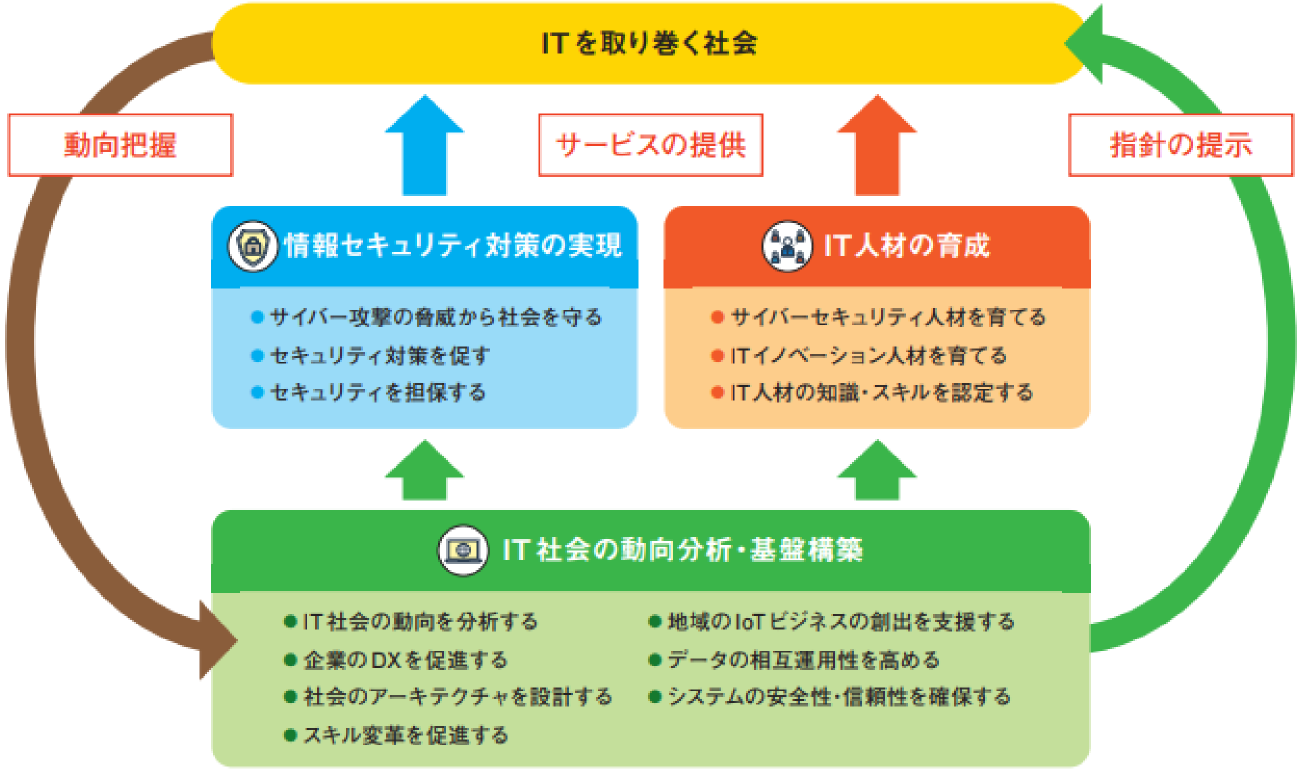
情報セキュリティの最新動向と対策

2023年5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 中小企業支援グループ

独立行政法人情報処理推進機構 （IPA）のご紹介

- 日本のIT国家戦略を技術面、人材面から支えるために設立された、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



ＩＰＡ 検索

サイバーセキュリティ、
なぜ必要？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

デジタル技術の発明
コンピューターの発明
蒸気機関の発明
灌漑技術の発明

超スマート社会
Society 5.0

情報社会
Society 4.0

工業社会
Society 3.0

農耕社会
Society 2.0

狩猟社会
Society 1.0

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

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

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

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

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
防犯やミス防止の**対策もデジタル化**
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”

最近の「組織」における脅威動向

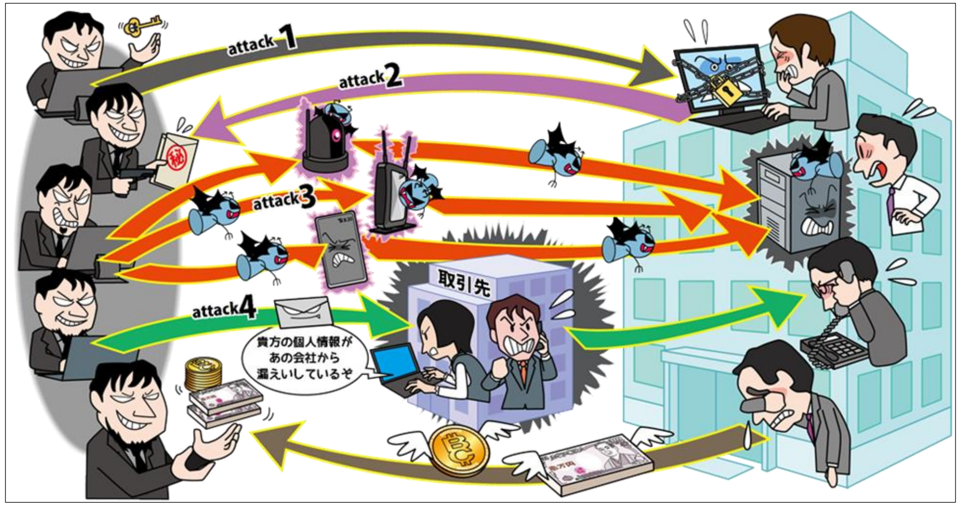
- 情報セキュリティ10大脅威：　IPAが2006年から毎年発行している資料。前年に発生したセキュリティ事故や攻撃の状況等から専門家等が選考したTOP10について解説
- **「ランサムウェアによる被害」が引き続き1位**。2022年も大手自動車部品会社や医療センターなどの被害が発生し社会問題に。
- **「サプライチェーンの弱点を悪用した攻撃」が3位から2位**へ（2019~2021はいずれも4位）。

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

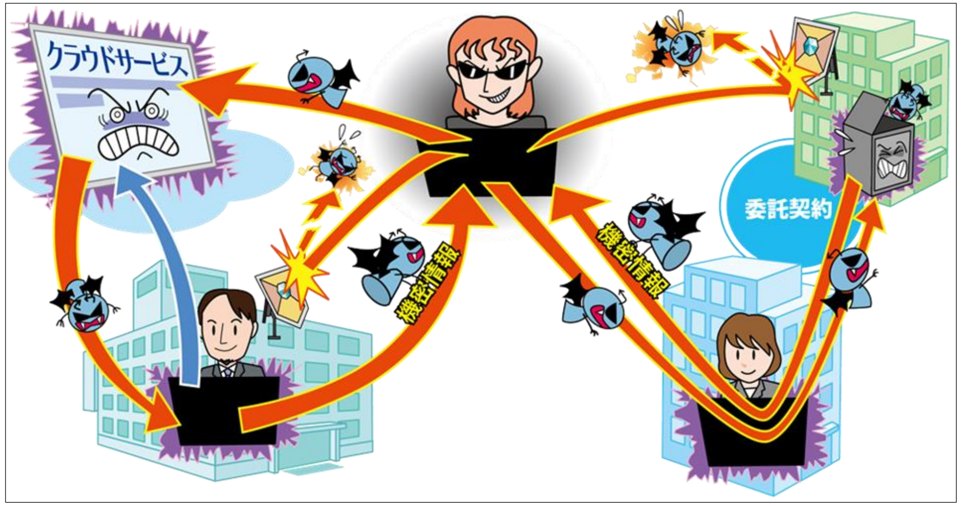
～猛威を振るうランサムウェア。四重の脅迫で被害者を逃がさない～



- 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

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

病院に対するランサム攻撃事例における課題等

状況・課題	情報セキュリティ対策の基本	IPAの提言
・VPN装置の脆弱性管理を実施していなかった ・Windowsその他システムのアップデート未実施	ソフトウェアの更新	SA①OSやソフトウェアは常に最新の状態にしよう！
・アンチウイルスソフトが未稼働	セキュリティソフトの利用	SA②ウイルス対策ソフトを導入しよう！
・短い（５桁）パスワード設定やロックアウト機能が無効となっていた ・VPN装置の脆弱性を利用した認証情報が漏洩したが、ID、パスワードを変更していなかった	パスワードの管理・認証の強化	SA③パスワードを強化しよう！
・VPN装置への接続元IPアドレス制限を怠っていた ・電子カルテシステム、部門システムのIPアドレスに存在するすべてのサーバが「信頼済みサイトゾーン」と設定されていた	設定の見直し	SA④共有設定を見直そう！
・閉域網ではないにもかかわらずインターネット上の脅威を評価していなかった	脅威・手口を知る	SA⑤脅威や攻撃の手口を知ろう！
・「インシデント対応を行う専門家が不在であったため、終始インシデント対応に苦慮している。半田病院のエンジニア派遣要請に各事業者が応じ、現地で対応を協力していればインシデント対応はより迅速に行われたものと考える。」		サイバーセキュリティお助け隊

【出典】徳島県つるぎ町立半田病院コンピュータウイルス感染事案有識者会議調査報告書(https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf)

効果的な解決方法は？

■ セキュリティ対策では、“**ふだんからの「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。

ふだんからの「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」**

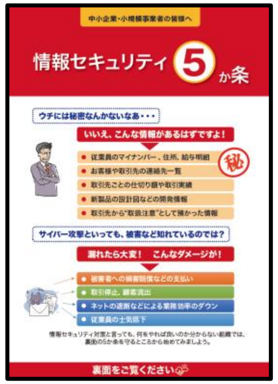
平時の対策支援（社内体制整備、意識向上）

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。

お助け隊サービス

- 相談窓口
  異常監視
- 緊急時対応
- 簡易サイバー保険

中小企業等

相談

駆けつけ等の
対応支援

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
- **「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
- 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

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

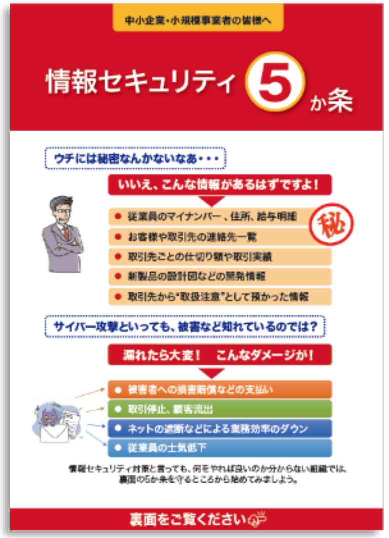
♦ できるところから始めて段階的にステップアップ

Step1
できるところから始める

Step2
組織的な取り組みを開始する

Step3
本格的に取り組む

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
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- 詳細リスク分析の実施方法

情報セキュリティ５か条
SECURITY ACTION ★一つ星を宣言

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

情報セキュリティ関連規程

より強固にするため方策

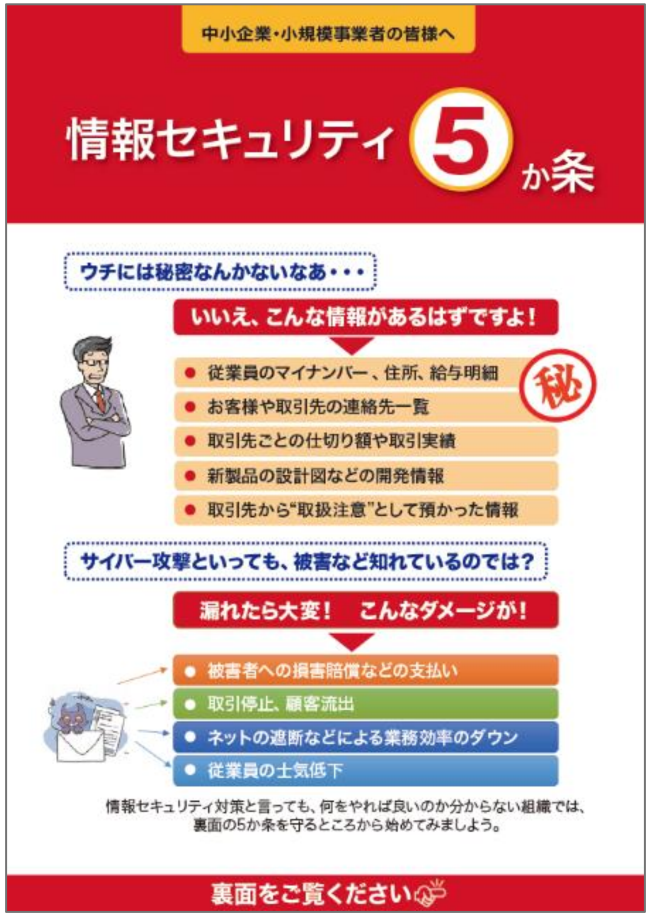
できるところから始める
情報セキュリティ5か条

- 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！



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、ウェブ利用、持ち出し、廃棄など

組織としての対策 7項目

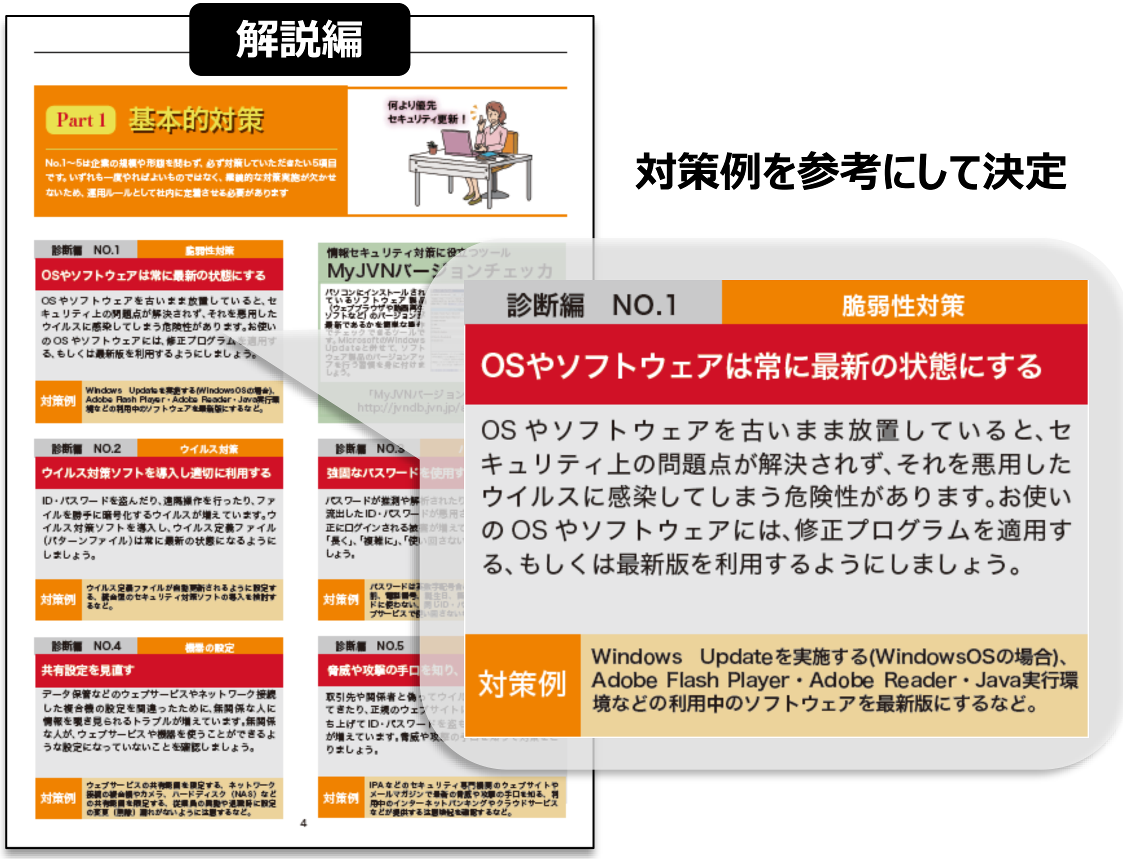
守秘義務、教育、委託先管理、ルール化　など

No		診断内容
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？
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？
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など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？

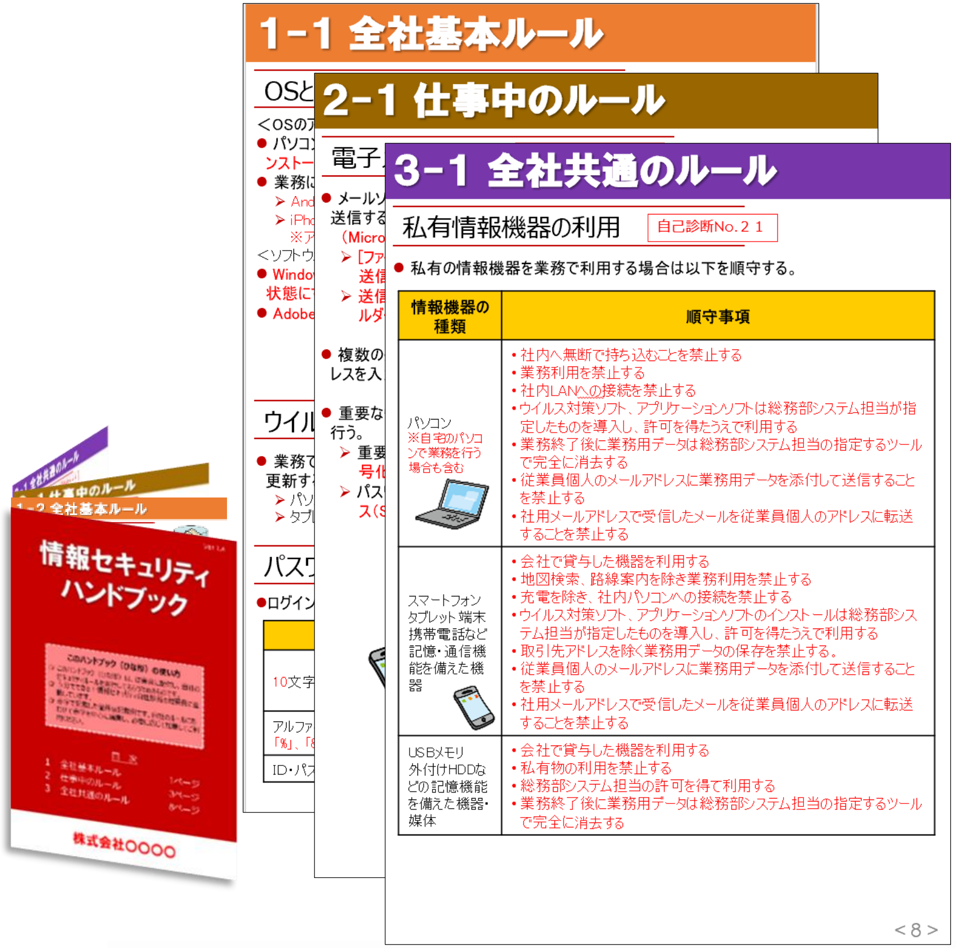
組織的な取り組みを開始する

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



情報セキュリティハンドブックを編集して周知

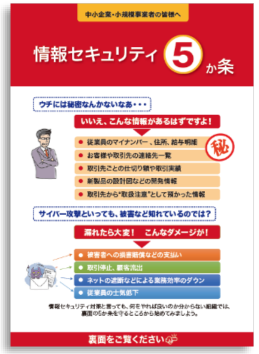
SECURITY ACTION制度について

- 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ない

★一つ星

セキュリティ対策自己宣言



１段階目（一つ星）

- **情報セキュリティ５か条に取り組む**

【情報セキュリティ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

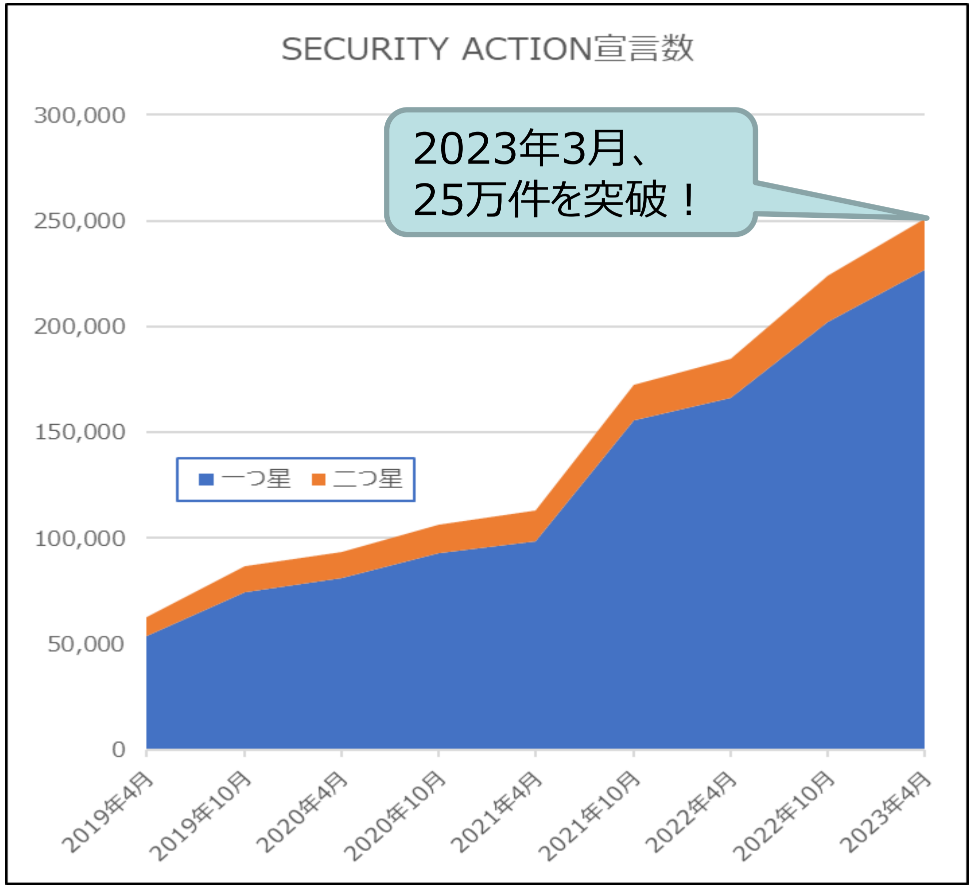
セキュリティ対策自己宣言

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

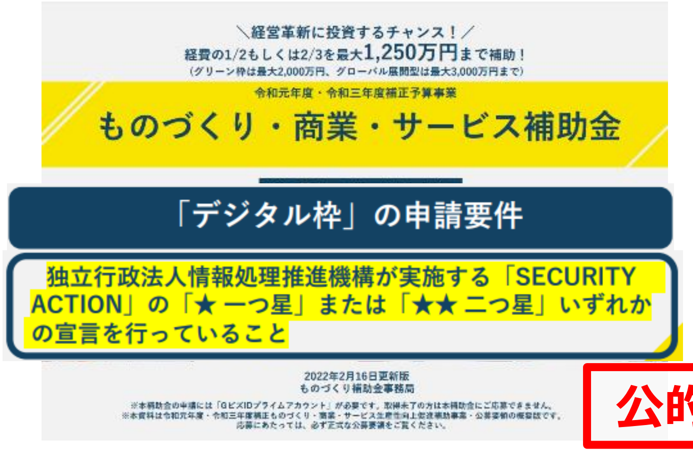
👉 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに

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自己宣言を申請要件としている
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）

□ **令和4年度 デジタル化トライアル事業費補助金**：秋田県
□ **令和4年度 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
□ **令和4年度 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
□ **令和4年度 堺市中小企業デジタル化促進補助金**：大阪府堺市

もしものインシデント（事故）に備えて

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**不可欠なワンパッケージのサービス**を要件としてまとめ、これを満たすものを**「サイバーセキュリティお助け隊サービス」**として登録・公表
  - **「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	ネットワーク及び／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**緊急時には駆け付け支援**
中小企業でも導入・運用できる簡単さ	**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	・ネットワーク一括監視型：**月額１万円以下（税抜き）** ・端末監視型：**月額2,000円以下／台（税抜き）** ・併用型：**これらの和に相当する価格を超えないこと** ※端末1台から契約可能であることが条件

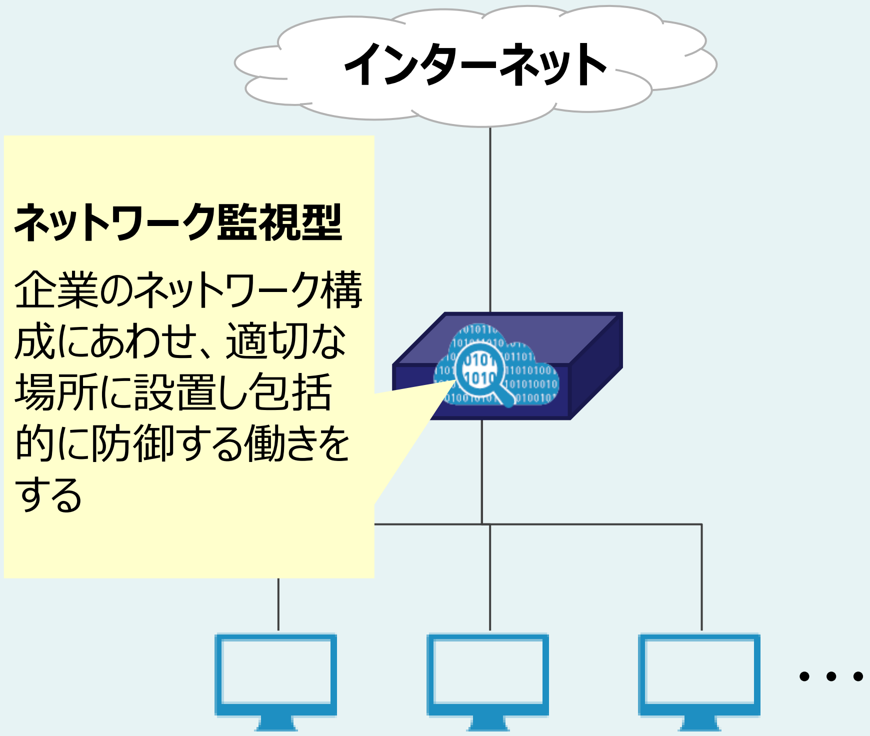
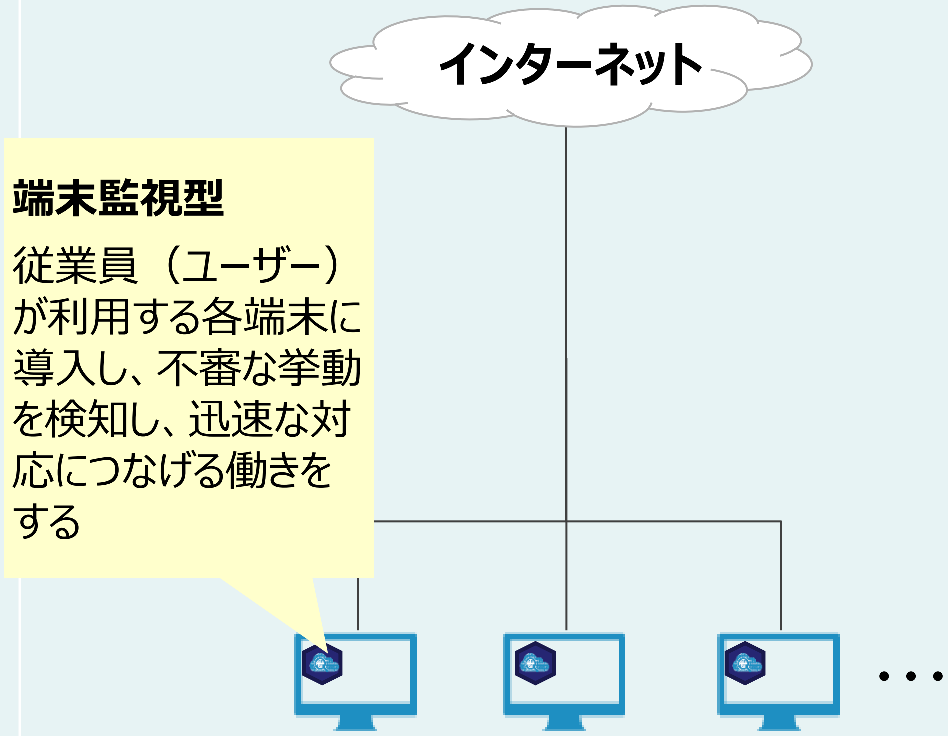
相談窓口、緊急時の対応支援、簡易サイバー保険などを**ワンパッケージで提供**

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

「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。

	ネットワーク一括監視型	端末監視型
構成		

【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。

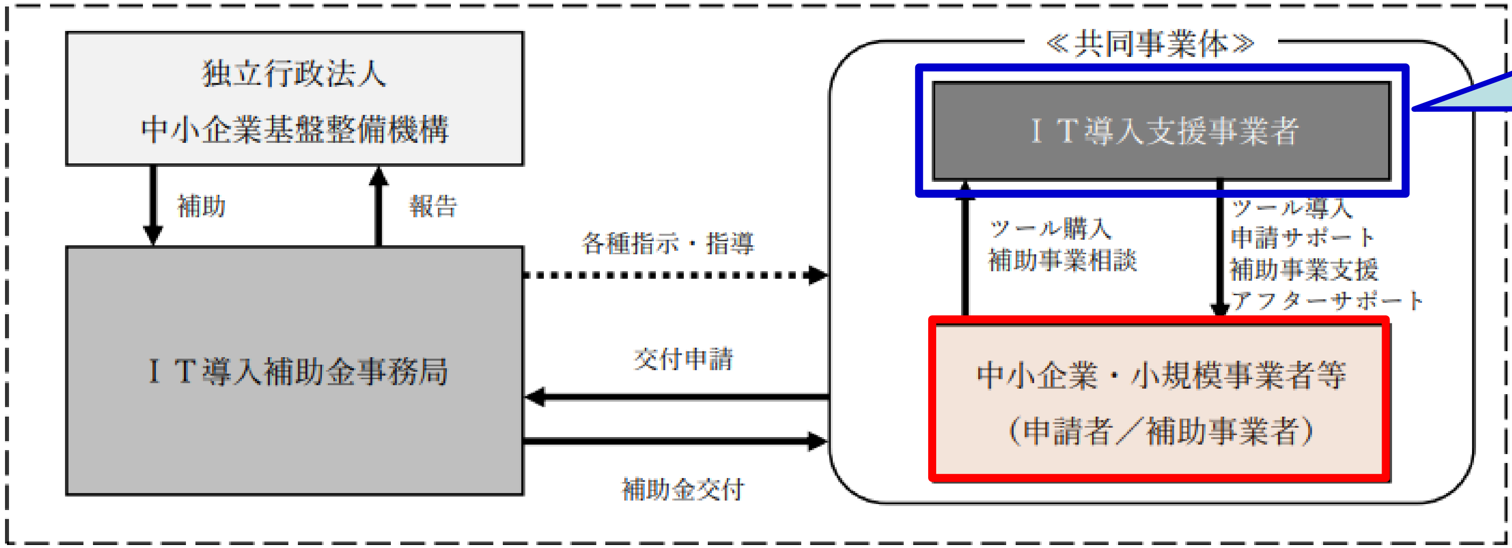
※サイバーセキュリティお助け隊サービス提供事業者　提供情報より

IT導入補助金2023 セキュリティ対策推進枠

- 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

交付申請受付中！第2次締切：
6/2（金）17:00まで
詳しくは、IT導入補助金ウェブサイト
https://www.it-hojo.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

セキュリティプレゼンター

セキュリティプレゼンター制度

- 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「セキュリティプレゼンター」として登録する制度
- 活動地域などを条件にセキュリティプレゼンターを検索可能

セキュリティプレゼンター登録タイプは次の２種類

公開	「情報セキュリティ対策支援サイト」で自身のプロフィール、活動等を掲載しPRすることができる。
コンテンツ利用のみ	「情報セキュリティ対策支援サイト」から、セキュリティ対策資料等をダウンロードすることができる。

情報処理推進機構　セキュリティプレゼンター　企業等

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/

IPA

- 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**

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？

○ 実施している ◉ 一部実施している ○ 実施していない ○ わからない

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（コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる）は最新の状態にしていますか？

○ 実施している ◉ 一部実施している ○ 実施していない ○ わからない

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？

○ 実施している ○ 一部実施している ◉ 実施していない ○ わからない

4. 重要情報（営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のこと）に対する適切なアクセス制限を行っていますか？

○ 実施している ◉ 一部実施している ○ 実施していない ○ わからない

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？

○ 実施している ○ 一部実施している ○ 実施していない ◉ わからない

合計点

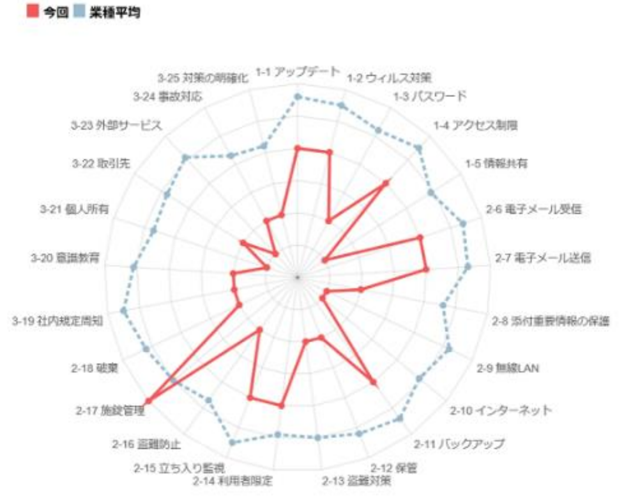
合計点
15 / 100

合計点算出基準

実施しているの合計点	4点
一部実施しているの合計点	16点
実施していないの合計点	0点
わからないの合計点	-5点

コメント

いつ情報流出などの事故が起きても不思議ではありません。



【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

【確認テスト】No.9

Q1 x 不正解

無線LANについて、不適切なのはどれでしょうか。

正答	回答	選択肢
		無線LANは、暗号化が施されているものを選ぶのはもちろん、暗号強度の高いものを選ぶ。
●		急ぎの仕事があったので、街中の無線LANを使って顧客とメールのやり取りを行なった。
	●	無線LANに接続する時は、他人に見られないよう、ファイル共有機能を無効にする。
		社内などで設置した無線LANは、暗号強度の高いものを設定し、パスワードを推測困難

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）。
  - 2022年度配布数：申込み**1,230件**　研修での受講予定者数：**約115万名**

● 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

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**を受け編さん
- 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

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。

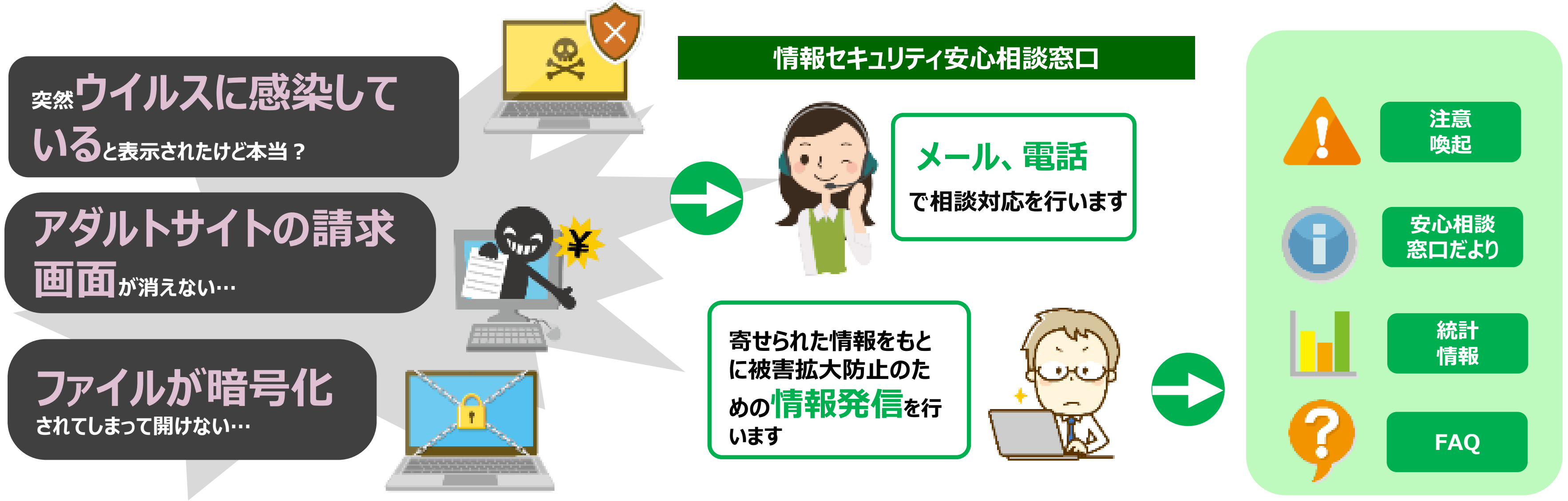
YouTube「IPA Channel」 https://www.youtube.com/user/ipajp/

【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

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

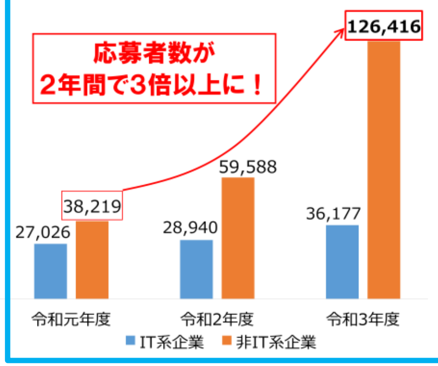
・ITを利活用するすべての社会人・学生が備えておくべきITに関する基礎的な知識が証明できる国家試験。

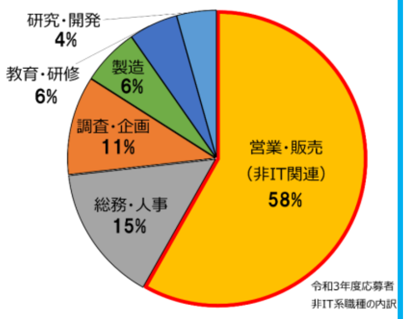
・IT技術に関する基礎知識だけでなく、情報セキュリティや情報モラルに関すること、経営戦略、会計や法務など、ITを活用する上で前提と　なる幅広い知識が試験勉強を通じてバランス良く習得可能。

・バウチャーチケット制度で受験手数料を一括して支払うことができるため、社員にiパスの受験を促進することが可能。

・組織全体のITリテラシーの底上げのため、非IT系企業を中心に活用拡大。

非IT系企業の営業・販売を担当する方の活用が進んでいます



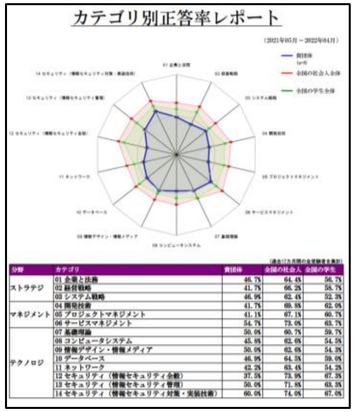


受験申込みはITパスポート試験サイトで受付けています。
また、同サイトでは、合格者の声や企業の声などを掲載していますので、是非ご覧ください。
ITパスポート試験サイト
▶https://www3.jitec.ipa.go.jp/JitesCbt/index.html

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可能。

・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可能。



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。

・自分の都合に合わせて、試験日時や試験会場を選んで、受験申込みが可能

・受験申込み後も試験日を変更することが可能
※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可能

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）	52.7% （令和3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。

・午前試験では、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。
午後試験では、身近な事例をベースにした実践的な問題を出題。

・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る。「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可能。

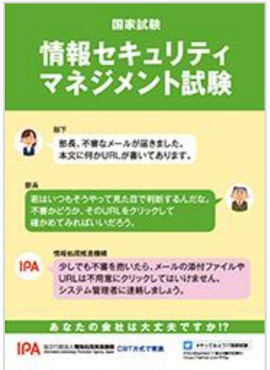
「プラス・セキュリティ」とは・・・
自らの業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のこと。企業におけるデジタル活用が進展する中で「プラス・セキュリティ」の必要性は高まっています。

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

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　紹介サイト
▶https://www.jitec.ipa.go.jp/sg/

試験実施概要



・**CBT方式で実施**
※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可能
・受験申込み後も試験日を変更することが可能
※変更可能期限あり
・試験会場は全国各地に設置
・午前試験と午後試験を同日に受験するだけでなく、試験実施期間内であれば、別日に受験することも可能

試験科目	試験時間	出題形式	出題数 解答数	合格基準	合格率
午前試験	90分	多肢選択式 (四肢択一)	50問 50問	60点 (100点満点)	53.2% (令和3年度平均)
午後試験	90分	多肢選択式	3問 3問	60点 (100点満点)	

2023年4月から通年試験化！

・現在は年2回（上期・下期の一定期間）で試験を実施しているところ、2023年4月から通年での試験実施。
・通年試験化に合わせて、試験時間、出題数、解答数等が変更。出題範囲は従来の午前試験・午後試験に準じます。

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)