IPA 独立行政法人 情報処理推進機構

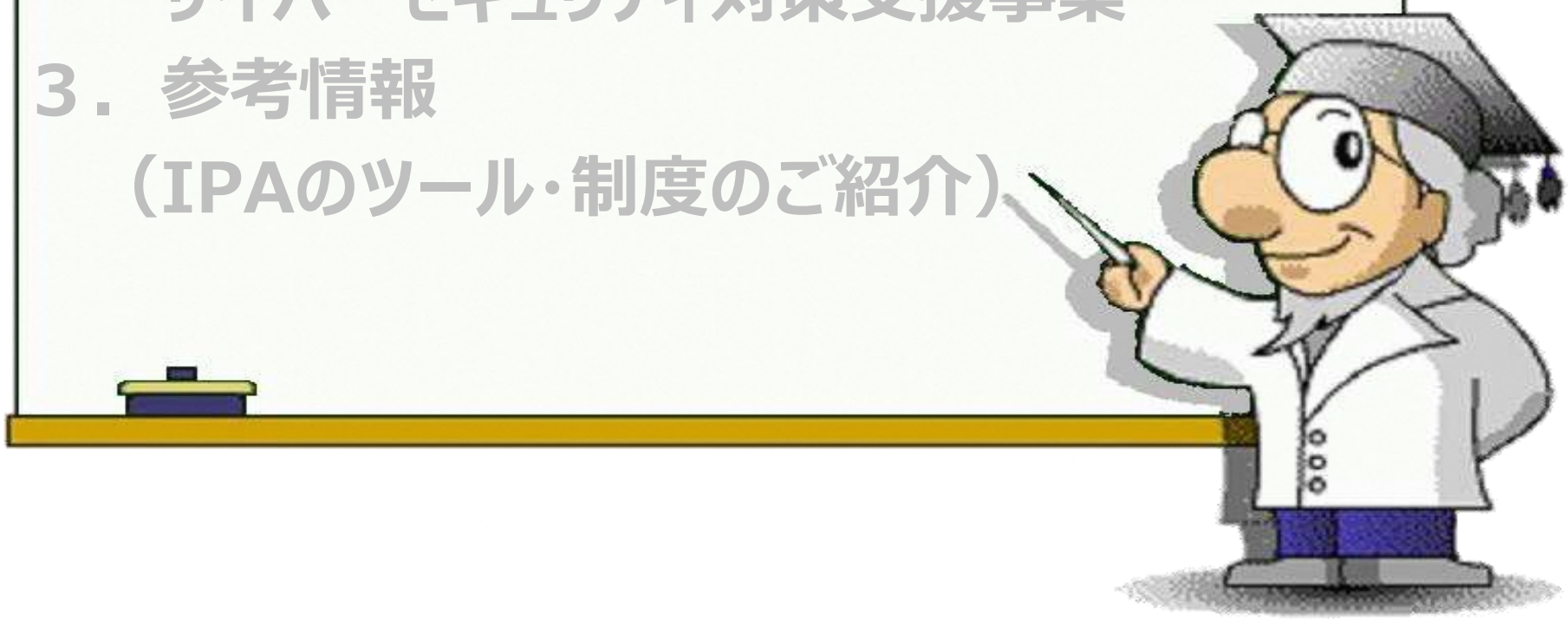
中小企業に必要なセキュリティ対策
～はじめましょう！　SECURITY ACTION～

2021年５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　稲垣克芳

目次



情報セキュリティ10大脅威2021

2021年1月27日発表

https://www.ipa.go.jp/security/vuln/10threats2021.html

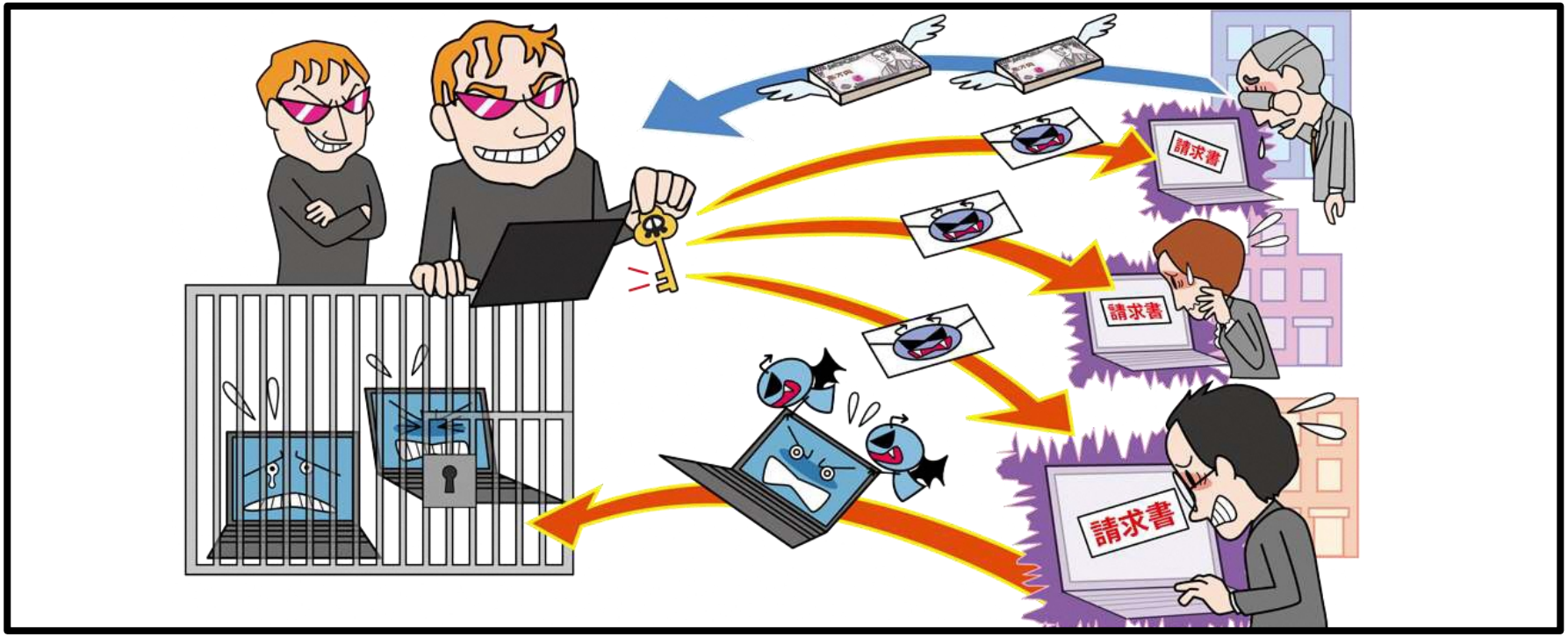
昨年順位	個人の脅威	順位	組織の脅威	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

「組織」の10大脅威の変遷

	10大脅威 2018	10大脅威2019	10大脅威2020	10大脅威2021
1位	標的型攻撃による被害	標的型攻撃による被害	標的型攻撃による 機密情報の窃取	ランサムウェアによる被害
2位	ランサムウェアによる被害	ビジネスメール詐欺による被害	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
3位	ビジネスメール詐欺による被害	ランサムウェアによる被害	ビジネスメール詐欺による 金銭被害	テレワーク等のニューノーマルな働き方を狙った攻撃
4位	脆弱性対策情報の公開に伴う悪用増加	サプライチェーンの弱点を悪用した攻撃の高まり	サプライチェーンの弱点を悪用した攻撃の高まり	サプライチェーンの弱点を悪用した攻撃
5位	脅威に対応するための セキュリティ人材の不足	内部不正による情報漏えい	ランサムウェアによる被害	ビジネスメール詐欺による 金銭被害
6位	ウェブサービスからの 個人情報の窃取	サービス妨害攻撃による サービスの停止	予期せぬIT基盤の障害に伴う業務停止	内部不正による情報漏えい
7位	IoT機器の脆弱性の顕在化	インターネットサービスからの 個人情報の窃取	不注意による情報漏えい	予期せぬIT基盤の障害に伴う業務停止
8位	内部不正による情報漏えい	IoT機器の脆弱性の顕在化	インターネット上のサービスからの個人情報の窃取	インターネット上のサービスへの不正ログイン
9位	サービス妨害攻撃による サービスの停止	脆弱性対策情報の公開に伴う悪用増加	IoT機器の不正利用	不注意による情報漏えい等の被害
10位	犯罪のビジネス化 （アンダーグラウンドサース）	不注意による情報漏えい	サービス妨害攻撃による サービスの停止	脆弱性対策情報の公開に伴う悪用増加

【１位】ランサムウェアによる被害

～組織を狙ったランサムウェアの攻撃が増加～



- 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と脅迫するケースも

【１位】ランサムウェアによる被害

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

- メールから感染させる
  - ・不正な添付ファイルを開かせる
- ウェブサイトから感染させる
  - ・ランサムウェアをダウンロードさせるようにウェブサイトを改ざん
  - ・当該サイトを閲覧するようにメールなどで誘導
- 脆弱性を狙いインターネットから感染させる
  - ・OSの脆弱性を悪用しウイルスを感染させる
  - ・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
- 公開サーバーに不正アクセスし感染させる
  - ・管理用のリモートデスクトップ等でサーバーに不正アクセス
  - ・サーバー上で攻撃者がウイルスを感染させる

【１位】ランサムウェアによる被害

事例/傾向

- **暗号化に加え、情報を暴露すると脅し** (※1,※2)
  - ・2020年11月、ゲームメーカーＡ社の社内システムにおいて
    データの**暗号化**、メールやファイルサーバーの**停止**により業務停止に
  - ・さらに、顧客や株主**情報等を暴露**すると脅迫
  - ・暗号化解除と暴露の取り止めを引き換えに身代金を要求

- **特定の組織に特化したランサムウェア** (※3)
  - ・2020年6月、自動車メーカーＢ社がサイバー攻撃から**大規模システム障害**
  - ・国内外の工場で生産や出荷が一時停止
  - ・従業員のPCが使えなくなる等オフィス系ネットワークシステムにも影響

【出典】 ※1 暗号化と暴露で11億円を要求、カプコン襲った「二重脅迫型」ランサムウェアの脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/112400040/
※2 不正アクセスによる情報流出に関するお知らせとお詫び【第3報】
https://www.capcom.co.jp/ir/news/html/210112.html
※3 ホンダを標的に開発か、ランサムウェア「EKANS」解析で見えた新たな脅威
https://xtech.nikkei.com/atcl/nxt/column/18/00989/062400028/

【１位】ランサムウェアによる被害

対策一覧

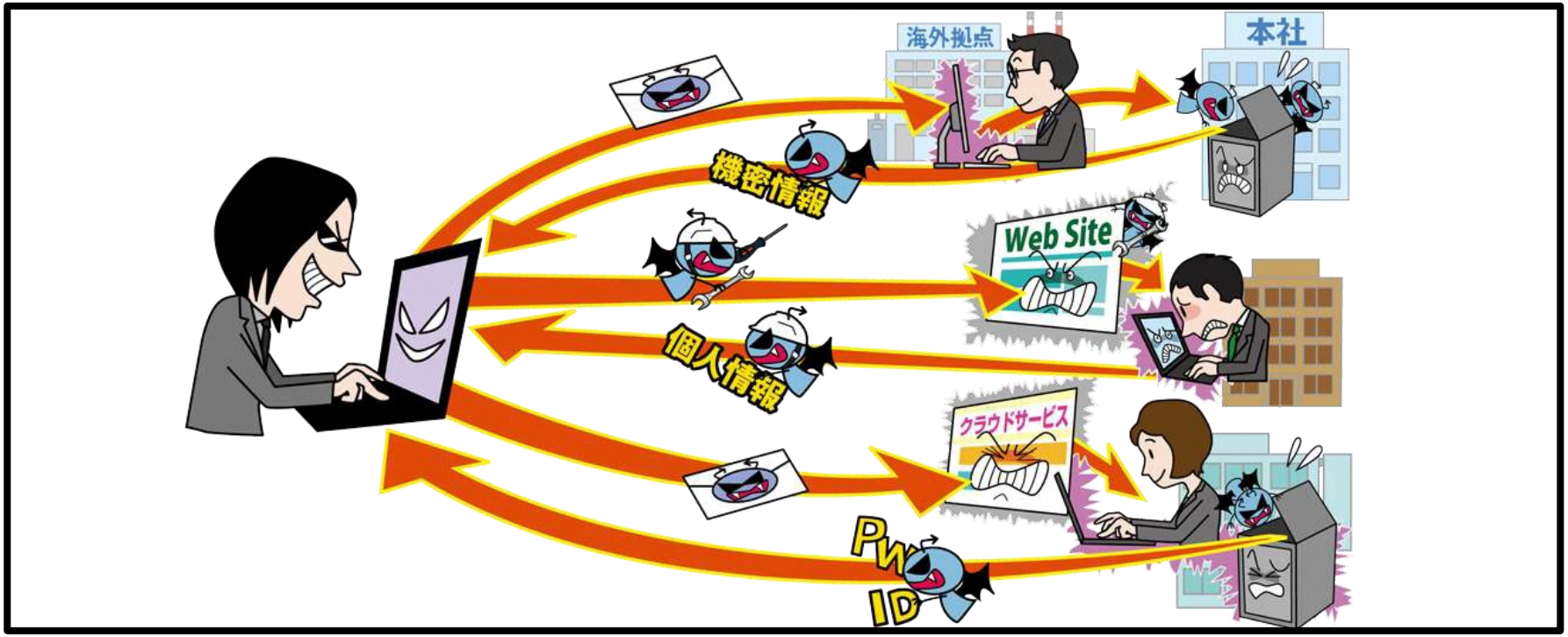
- **経営者層**
  - ・組織としての対応体制の確立
    - -対策の予算の確保と継続的な対策の実施
- **システム管理者、従業員**
  - ・被害の予防
    - -受信メール、ウェブサイトの十分な確認
    - -添付ファイルやリンクを安易にクリックしない
    - -不審なソフトウェアを実行しない
    - -サポートの切れたOSの利用停止、移行
    - -フィルタリングツール（メール、ウェブ）の活用
    - -ネットワーク分離
    - -共有サーバー等へのアクセス権の最小化と管理の強化
    - -バックアップの取得
    - -標的型攻撃対策相当の全般的なセキュリティ対策が必要
    - -復号ツールの活用　（※1）

【出典】

※1　The No More Ransom Project
https://www.nomoreransom.org/

【２位】標的型攻撃による機密情報の窃取

～新型コロナウイルスの影響に便乗した標的型攻撃メールを観測～



- メールやウェブサイトを利用し特定組織のPCをウイルスに感染させる
- 組織内部へ潜入し長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報を窃取やシステムの破壊を

【２位】標的型攻撃による機密情報の窃取

攻撃手口

・ウイルスに感染させて機密情報を窃取

- メールを利用した手口（**標的型攻撃メール**）
  - ・不正な添付ファイルを開かせる
  - ・不正なウェブサイトへのリンクをクリックさせる
  - ・複数回のメールのやりとりで油断させ、その後感染させる手口も
- ウェブサイトを利用した手口
  - ・標的組織が頻繁に利用するウェブサイトを調査し、当該サイトを閲覧するとウイルスに感染するように改ざん（水飲み場型攻撃）
- 不正アクセスによる手口
  - ・標的組織が利用するクラウドサービスや標的組織のウェブサーバーの脆弱性を悪用して不正アクセスし、認証情報等を窃取
  - ・窃取した認証情報等を利用し正規の経路で組織内部のシステムへ侵入しPC やサーバーをウイルスに感染させる

【２位】標的型攻撃による機密情報の窃取

事例/傾向

- **複数の組織における標的型攻撃と思われる不正アクセス報道** (※1,※2)
  - ・電機メーカＡ社
  - ・2020年1月、防衛事業部門のサーバーが不正アクセスを受けたと公表
  - ・27,445件のファイルが不正にアクセスされた
  - ・情報流出等の被害は確認されていない
  - ・2016年12月以降に攻撃を受けていたが、攻撃を検知できておらず

  - ・B重工
  - ・2020年12月、外部からの不正アクセスを受けたと公表
  - ・2020年6月以降、複数の海外拠点＆国内拠点間で不審な通信を確認→発覚
  - ・攻撃は痕跡を残さない高度なもの、一部情報が外部に流出した可能性があり

【出典】 ※1 当社の社内サーバへの不正アクセスについて
https://jpn.nec.com/press/202001/20200131_01.html
※2 当社グループへの不正アクセスについて
https://www.khi.co.jp/pressrelease/news_201228-1j.pdf

【２位】標的型攻撃による機密情報の窃取

メール利用者における対策

- **不審なメールの添付ファイルは開かない**
  - ・不審を抱きにくいような巧妙なメールも増えている
    「添付ファイルを開くとウイルスに感染するかも」という心構えを

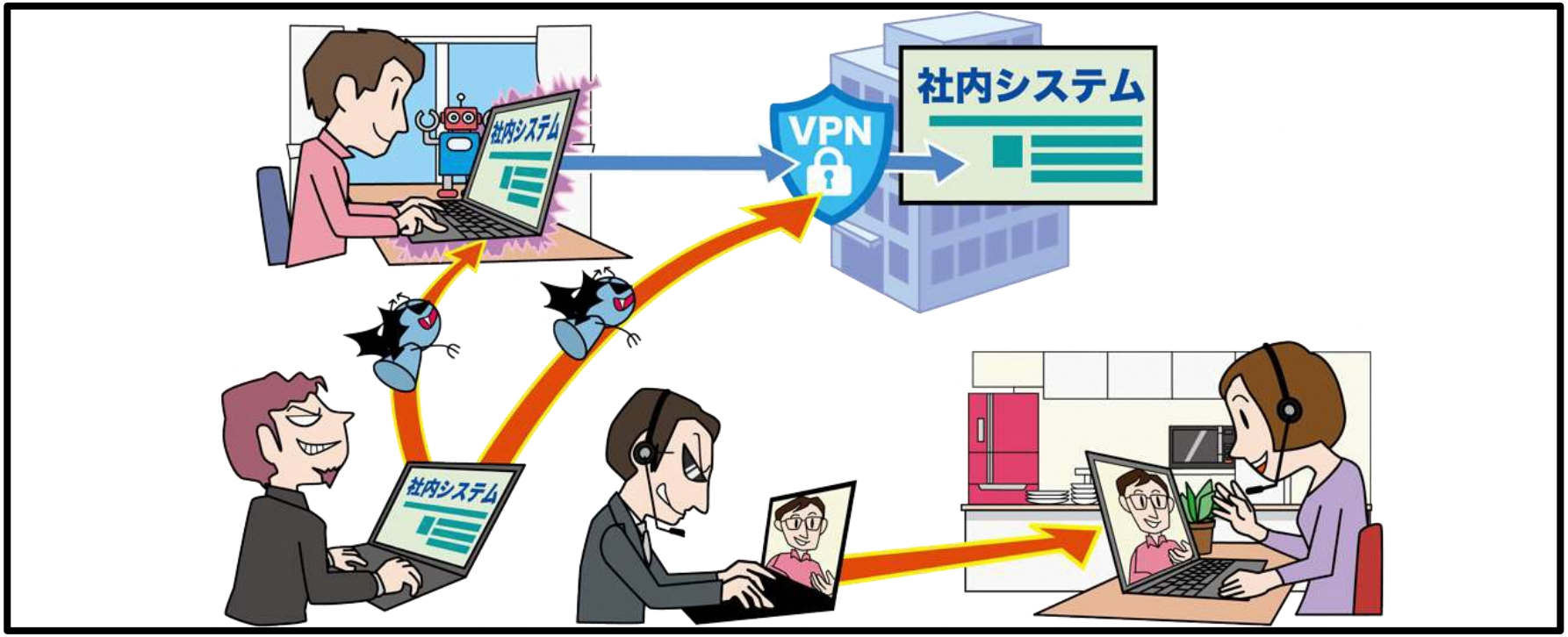
- **WordファイルやExcelファイルのマクロに要注意**
  警告ウィンドウの以下のボタンは押さない
  - ・「マクロを有効にする」
  - ・「コンテンツの有効化」
  - ・「編集を有効にする」

- **マクロを無効にする（Word・Excel 共に）**
  ①[ファイル] → ②[オプション] → ③[トラストセンター] →
  ④[トラストセンターの設定]→⑤[マクロの設定]

- **「.exe」や「.js」などのファイルにも引き続き要注意**

【３位】テレワーク等の ニューノーマルな働き方を狙った攻撃

～テレワーク環境を意識した対策を～



- 組織のテレワークへの移行に伴いWeb会議サービスやVPN等の本格的な活用を狙った攻撃が行われている
- 業務環境の脆弱性を利用され社内システムが不正アクセスに
- Web会議がのぞき見されたり、テレワーク用PCがウイルス感染

【３位】テレワーク等のニューノーマルな働き方を狙った攻撃

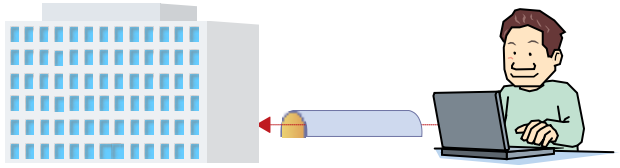
攻撃手口

- **テレワーク用ソフトウェアの脆弱性の悪用**
  - ・VPN等の**テレワーク用**に導入している**製品の脆弱性**を悪用され社内システムへの不正アクセスや、PC内の業務情報等が窃取される
  - ・またWeb会議サービスの脆弱性が悪用されWeb会議がのぞかれる
- **急なテレワーク移行による管理体制の不備**
  - ・テレワークへの急な移行により、**ルール整備やセキュリティ対策が不十分**な環境のままで利用を開始
- **私物PCや自宅ネットワークの利用**
  - ・私物PCでテレワーク実施（私的利用の併用）
    ウェブサイト接続やSNSへアクセス、**私物ソフトウェア**のインストールなどにより、ウイルス感染やテレワーク用の認証情報等が窃取
  - ・組織支給PCにてテレワーク実施
    セキュリティ**対策が不十分な自宅ネットワーク**接続でウイルス感染

【３位】テレワーク等のニューノーマルな働き方を狙った攻撃

事例/傾向

- **在宅勤務中にウイルス感染、社内に拡大**
  - ・2020年4月、**在宅勤務中に**社有PCで社内ネットワークを経由せずに外部ネットワークに接続 → SNS利用時に**ウイルスに感染**
  - ・出社時に当該PCを**社内ネットワーク**に接続→**ウイルス感染が拡大**
- **Web会議サービスに非公開会議へアクセスできる脆弱性**
  - ・2020年7月、Web会議サービス●●に、特定の状況下にて数分で**非公開の会議へアクセスできる脆弱性**があったと発表（報告を受けた2020年4月に修正済）
- **脆弱性の悪用によりVPNのパスワード流出**
  - ・2020年8月、VPN製品の脆弱性が悪用され窃取された**認証情報**約900件がインターネット上で**公開**
  - ・更新プログラムを**適用していないVPN製品**が狙われた悪用された脆弱性は2019年4月にアドバイザリが公開されていた



【３位】テレワーク等のニューノーマルな働き方を狙った攻撃
対策一覧①

組織（テレワーカー）

・情報リテラシーや情報モラルの向上

-セキュリティ教育の受講

・被害の予防（被害に備えた対策含む）

-「情報セキュリティ対策の基本」を実施

-組織のテレワークルール遵守（使用する端末、ネットワーク環境、作業場所等）

・被害を受けた後の対応

-CSIRT※への連絡

組織（経営者層）

・組織としての体制の確立

-CSIRT※の構築

-対策予算の確保と継続的な対策の実施

-テレワークのセキュリティポリシーの策定

※CSIRT：セキュリティインシデント等の問題が発生した際に原因究明や影響範囲の調査等を行う組織。

【３位】テレワーク等のニューノーマルな働き方を狙った攻撃
対策一覧②

組織（セキュリティ担当者、システム管理者）

・被害の予防（被害に備えた対策含む）

-シンクライアント、VPN等のセキュリティに強いテレワーク環境の採用

-テレワークの規程や運用ルールの整備

作業場所や利用環境の規程整備

組織支給PCと私物PCの違いも考慮する必要がある

-セキュリティ教育の実施

-テレワークで利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理

-セキュリティパッチの適用（VPN装置、ネットワーク機器、PC等）

・被害の早期検知

-適切なログの取得と継続的な監視

-ネットワーク監視、防御、UTM・IDS/IPS等の導入

・被害を受けた後の対応

-CSIRTの運用によるインシデント対応

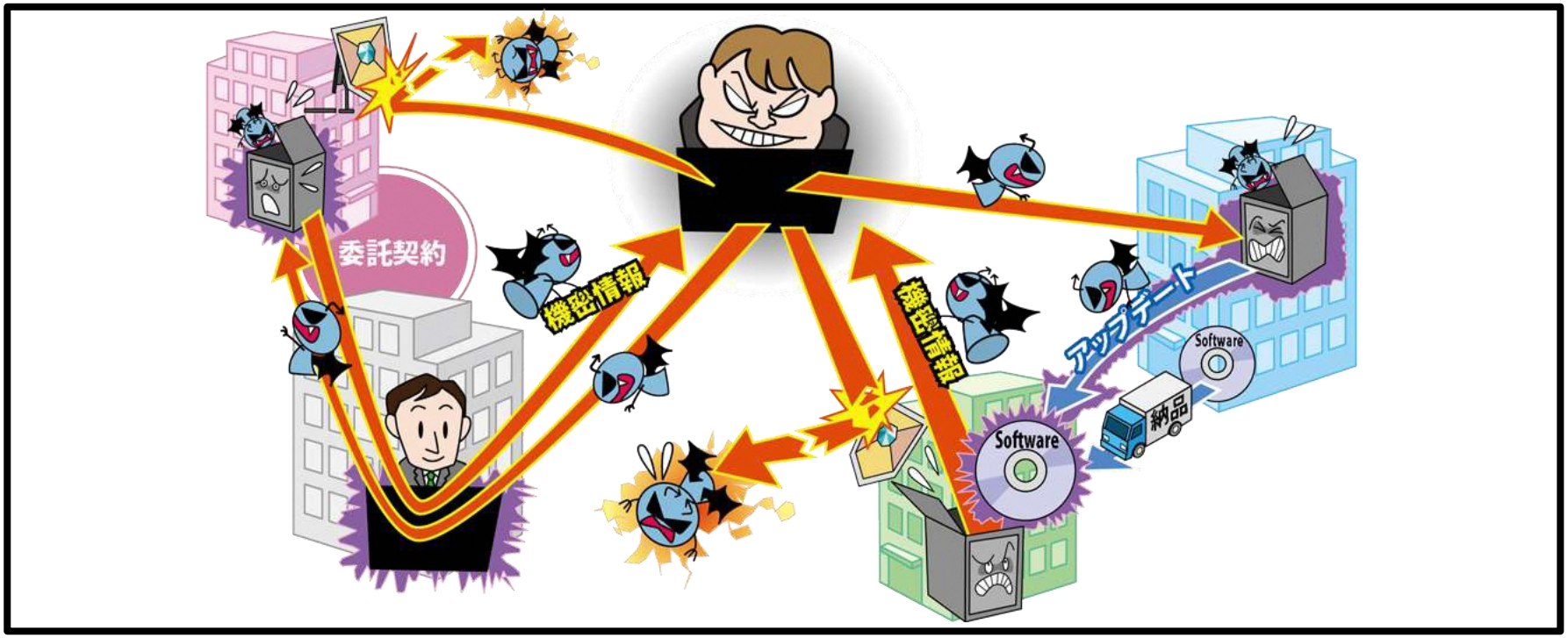
-影響調査および原因の追究、対策の強化

- テレワークを行う際のセキュリティ上の注意事項
  https://www.ipa.go.jp/security/announce/telework.html

【４位】サプライチェーンの弱点を悪用した攻撃

～自組織の対策だけでは不十分？

広がるサプライチェーンを悪用した攻撃被害～



- 原材料や部品の調達、製造、在庫管理、物流、販売、業務委託先などの一連の商流（サプライチェーン）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狙われる
- 一部業務を委託している外部委託先組織から情報が漏えい

【４位】サプライチェーンの弱点を悪用した攻撃

攻撃手口

- **取引先や委託先が保有する機密情報を狙う**
  - **標的となる組織よりもセキュリティが脆弱な委託先等を攻撃し、その組織が委託業務において保有していた標的組織の機密情報等を窃取する。**
- **ソフトウエア開発元等を攻撃し、標的を攻撃するための足掛かりとする**
  - **ソフトウエア開発元を攻撃し、ソフトウエアのアップデートにウイルスを仕込む。**
  - **その後、開発元から公開されたアップデートを適用した利用者がウイルスに感染し、そのウイルスを介して標的組織に侵入する。**

【４位】サプライチェーンの弱点を悪用した攻撃

事例/傾向

中国拠点を足掛かりに国内拠点へ侵入 (※1)

・2019年１月　大手電機メーカＡ社の情報流出
・Ａ社の中国拠点のサーバーがマルウェア感染→拠点内の他端末へと侵入範囲を拡大
・その後、日本国内拠点に侵入し感染を拡大、最終的な感染疑いは国内外含め132台

ソフトウェアの正規のアップデートにバックドア (※2, ※3)

・2020年12月、セキュリティベンダーがサプライチェーン攻撃の発生を発表
・攻撃者がソフトウェアのアップデートファイルにバックドアを仕込む
・配信されたそのアップデートファイルで更新をした組織が感染
・その後バックドアから攻撃者が侵入
・米政府をはじめ多くの米国組織で感染被害が報告され、国内でも感染の形跡が確認

【出典】
※1　不正アクセスによる個人情報と企業機密の流出可能性について（第3報）
https://www.mitsubishielectric.co.jp/news/2020/0212-b.pdf
※2　SolarWinds Security Advisory
https://www.solarwinds.com/ja/securityadvisory
※3　SolarWindsのサプライチェーン攻撃についてまとめてみた
https://piyolog.hatenadiary.jp/entry/2020/12/20/045153

【４位】サプライチェーンの弱点を悪用した攻撃

要因

・サプライチェーンのセキュリティ対策不足

- **サプライチェーンを適切に選定、管理していない**
- **再委託先や再々委託先の管理は困難**

  委託先組織の先に再委託先組織や再々委託先組織がある場合、

  その管理は委託先組織が行うため、

  委託元からのセキュリティ対策管理はさらに難しくなる
- **契約における責任が不明確** (※1)

  IT業務委託契約書において委託元の約8割が「新たな脅威が顕在化した際の対応」について責任範囲を明記していない

  理由は「専門知識・スキルが不足している」が最多の79.6%

【出典】 ※1 「ITサプライチェーンにおける情報セキュリティの責任範囲に関する調査」報告書について
https://www.ipa.go.jp/security/fy30/reports/scrm/index.html

【４位】サプライチェーンの弱点を悪用した攻撃

対策一覧①

委託元組織

・被害の予防

-業務委託や情報管理における規則の徹底
-信頼できる委託先、取引先組織の選定
-委託先からの納品物の検証
-契約内容の確認
-委託先組織の管理

・被害を受けた後の対応

-影響調査および原因の追究、対策の強化
-被害への補償

委託先組織

・被害の予防

-セキュリティの認証取得（ISMS、Pマーク、ISMAP等）
-攻撃者の目的や攻撃手段は多岐にわたるため、
他の脅威の対策も参考に業務に応じた広範な対策が必要

・被害を受けた後の対応

-委託元への連絡

【４位】サプライチェーンの弱点を悪用した攻撃

対策一覧②

委託先/委託元組織共通

・被害の予防

-公的機関が公開しているガイドラインの活用

「サイバーセキュリティ経営ガイドライン」 (※1)

「中小企業の情報セキュリティ対策ガイドライン」 (※2)

【出典】 ※1 「サイバーセキュリティ経営ガイドライン」Ver2.0 （経済産業省/IPA）
https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf
※2 「中小企業の情報セキュリティ対策ガイドライン」 （IPA）
https://www.ipa.go.jp/files/000055520.pdf

（参考）サプライチェーンの弱点を悪用した攻撃（新聞記事）

記事：サイバー攻撃 供給網の穴

サイバー攻撃 供給網の穴 ①

トヨタの取引先を脅迫

身代金要求→拒否で「機密公開」

防御甘い中小入り口

世界の端末「健康診断」も

対策、海外で続々進化

【出典】
サイバー攻撃 供給網の穴>(上) トヨタの取引先を脅迫
： 2020年9月15日 日本経済新聞 朝刊 17ページ

サイバー攻撃 供給網の穴 ②

「次は取引停止」迫る大手

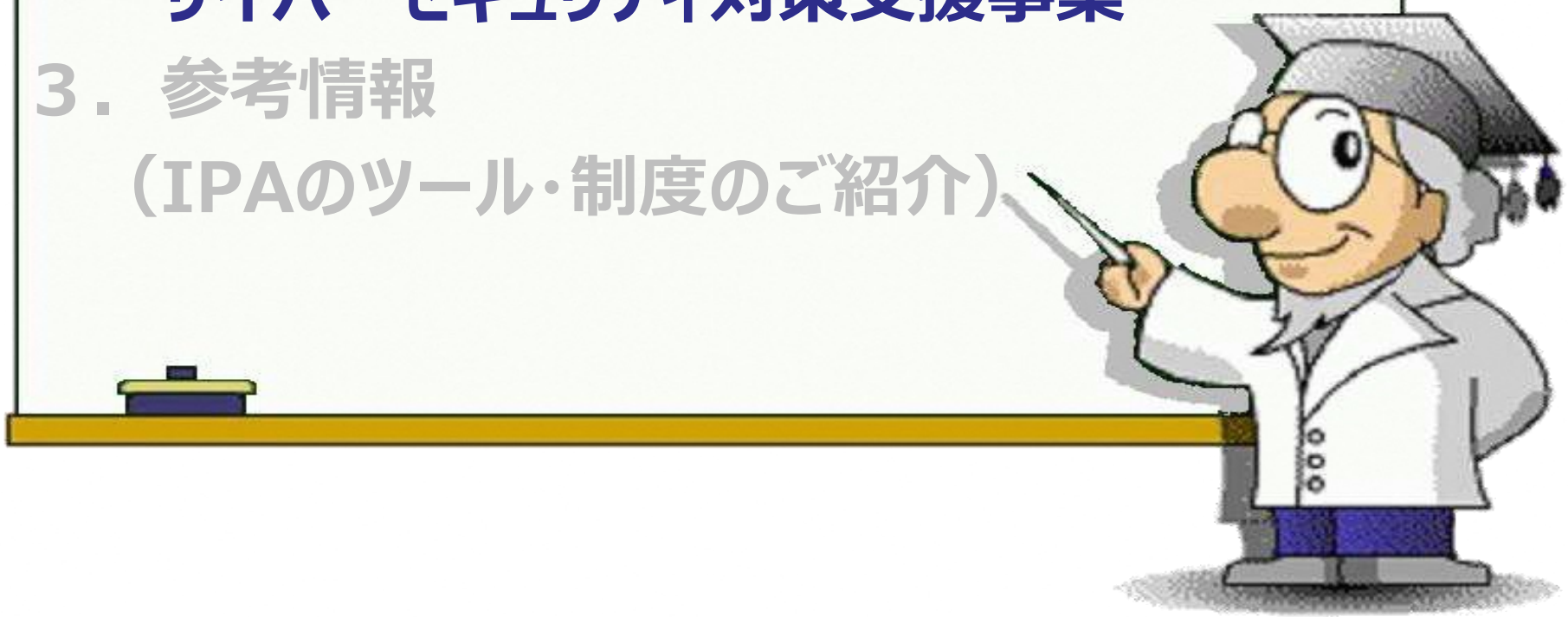
車・防衛…各国で規制強化

中小、人・カネ乏しく苦慮

対策強要 下請法に抵触も

【出典】
サイバー攻撃 供給網の穴>(下)「次は取引停止」迫る大手
： 2020年9月16日 日本経済新聞 朝刊 16ページ

目次



中小企業における現場対応の徹底支援

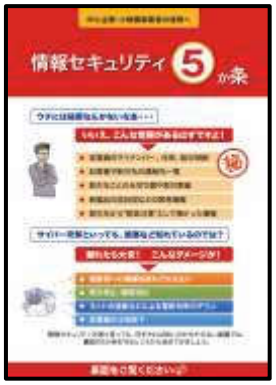
事前の備えから、インシデントが発生してしまった後の対応・復旧支援まで

- セキュリティ対策を始めるに当たって何をやればいいのかわからない、そういった悩みをもつ中小企業に対し、まずは意識を持つ為、セキュリティ対策自己宣言**「SECURITY ACTION」**の取り組み。
- 中小企業にとって重要な情報を漏えい、改ざん、消失などの脅威から保護する為の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」**の発行。
- 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、また簡易保険の実現を目指し、**「サイバーセキュリティお助け隊」**による支援体制を構築。

主に事前支援（防御等）　　**主に事後支援（検知、対応、復旧等）**

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。

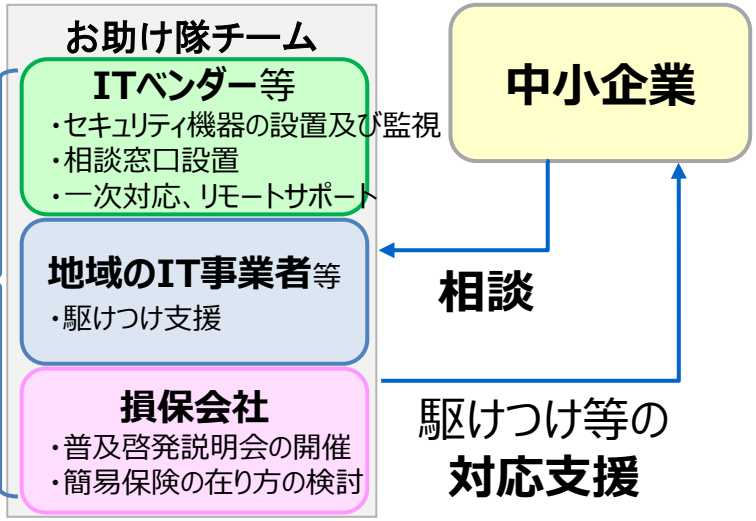


中小企業情報セキュリティ対策ガイドライン

- 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。

サイバーセキュリティお助け隊

- 中小企業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。



SECURITY ACTION 制度概要

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

SECURITY ACTION制度のメリット

- **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

- **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

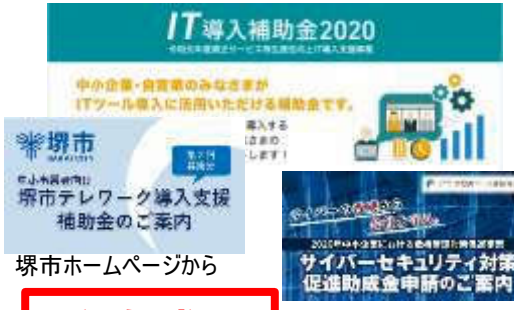
- **公的補助・民間の支援を受けやすく**

  ☞ 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

見える化

信頼関係

中小企業基盤整備機構Facebookアカウントkから



堺市ホームページから

公的補助

東京都中小企業振興公社資料から

自治体補助金・助成金におけるSA制度活用例

1．秋田県での活用例（リモートワーク環境整備支援事業費補助金）

補助金実施機関	秋田県 産業労働部 産業政策課
補助金公募時期	令和２年１０月～１１月
補助対象経費	機器導入費（機器レンタル料含む）、ネットワーク整備費、ソフトウェア導入費、コンサル費用、及び通信費
支給要件 (大規模枠の応募)	**IPAが実施する「SECURITY ACTION」の「★★二つ星」を宣言** （IPAからの通知メール「自己宣言受付確認のお知らせ」等の提出）

2．堺市での活用例（堺市テレワーク導入支援補助金）

補助金実施機関	大阪府　堺市　産業振興局
補助金実施時期	【第１次】令和２年４月受付、【第２次】令和２年９月受付、【第３次】令和２年１１月受付
補助対象経費	テレワーク導入に要する経費（設備費）、テレワーク導入検討や運用に要する経費（委託外注費）、等
支給要件	**【第１次】IPAが実施する「SECURITY ACTION」の「★一つ星」を宣言** **【第2,3次】IPAが実施する「SECURITY ACTION」の「★★二つ星」を宣言** （IPAからの通知メール「自己宣言受付確認のお知らせ」等の提出）

3．東京都での活用例（サイバーセキュリティ対策促進助成金）

助成金実施機関	公益財団法人　東京都中小企業振興公社
助成金実施時期	第１期　令和２年５月より受付　第６期まで
助成対象経費	サイバーセキュリティ対策を実施するために必要となる機器等の導入、およびクラウド利用に係る経費
助成対象事業者	**IPAが実施しているSECURITY　ACTIONの２段階目（★★二つ星）を宣言**している都内の中小企業者・中小企業団体（宣言済みであることをホームページ等で確認できること）

一つ星

情報セキュリティ５か条に取組む

情報セキュリティ５か条

■「できるところから」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

1. OSやソフトウェアは
常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！

1 OSやソフトウェアは常に最新の状態に

■ OSやソフトウェアのセキュリティ上の問題点を放置すると、それらを悪用したウイルスに感染する危険性がある
使用中のOSやソフトウェアには修正プログラムを適用する、もしくは最新版を利用する

＜対策例＞

- Windows Update(Windows OSの場合)/
  ソフトウェア・アップデート(Mac OSの場合)
- OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/
  Java実行環境(JRE)など
  利用中のソフトウェアを最新版にする

2 ウイルス対策ソフトを導入

■ ID･パスワードの盗用、遠隔操作でのPC乗っ取り、ファイルを勝手に暗号化されるウイルスが増加している。

ウイルス対策ソフトを導入し、ウイルス定義ファイル(パターンファイル)は常に最新の状態にする

＜対策例＞

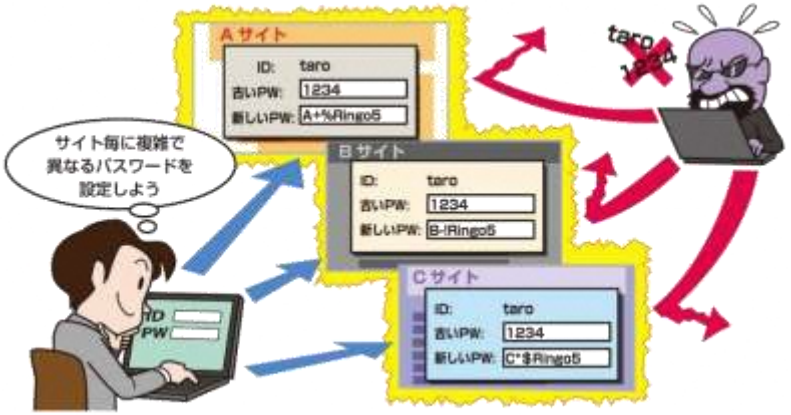
- ウイルス定義ファイルが自動更新されるように設定
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入

3 パスワードを強化

■ パスワードが簡単に推測や解析されたり、ウェブサービスから窃取したID・パスワードが流用されることで、不正にログインされる被害が増加している。パスワードは「**長く**」「**複雑に**」「**使い回さない**」ようにして強化する

＜対策例＞

- パスワードは英数字含めて長い文字数にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 別々のWebサービスにおいては、同じパスワードを使い回さない



4 共有設定を見直す

■ クラウドサービスやネットワーク接続による複合機など、誤った設定により無関係な人に情報を覗き見られるトラブルが増加している
ユーザーとの共有設定には、
情報漏洩や不正アクセスなどへの対策に考慮する

＜対策例＞

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

5 脅威や攻撃の手口を知る

■ 取引先や関係者と偽ってウイルス付のメールを送り、正規のウェブサイトに似せた偽サイトへ誘導し、ID・パスワードを盗用する巧妙な手口が増加している
これらの脅威や攻撃の手口を知り、対策を行う

＜対策例＞

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

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

①基本方針の作成と周知

- 経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために簡潔な文書を作成・周知する
- 中小企業の情報セキュリティ対策ガイドライン付録「情報セキュリティ基本方針（サンプル）」を参考

②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」を活用する

- 25項目の設問に答え、自社の情報セキュリティの問題点を把握
- 解説編の対策例を参考に、社内ルールを作成
- 付録の情報セキュリティハンドブックを活用し、社内ルールの周知

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

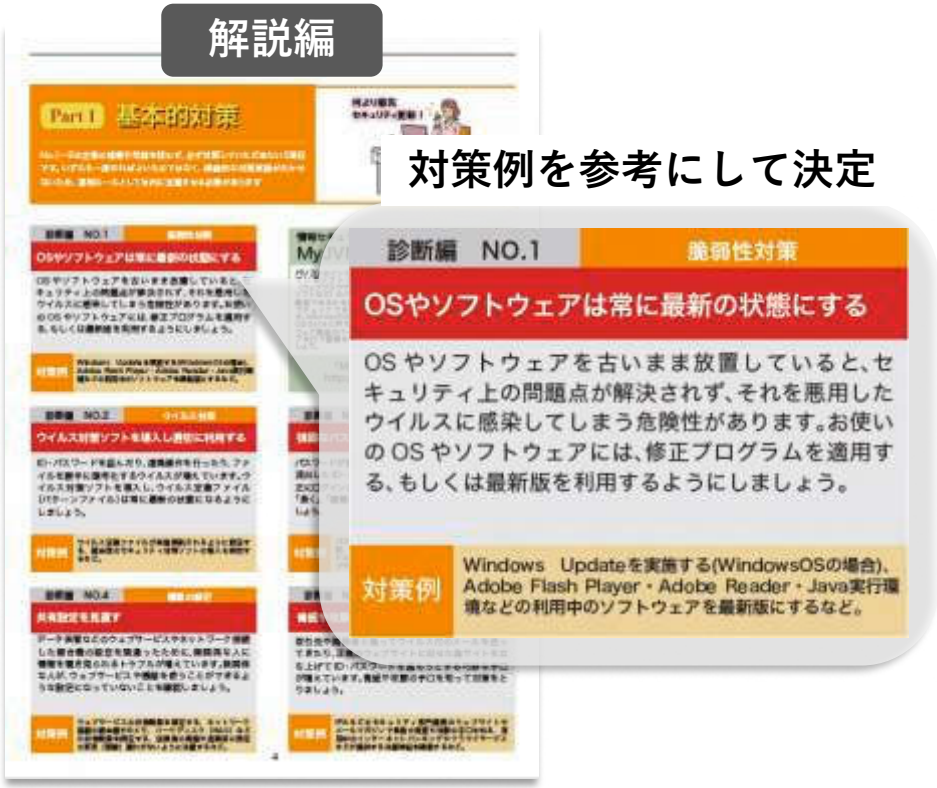
無料

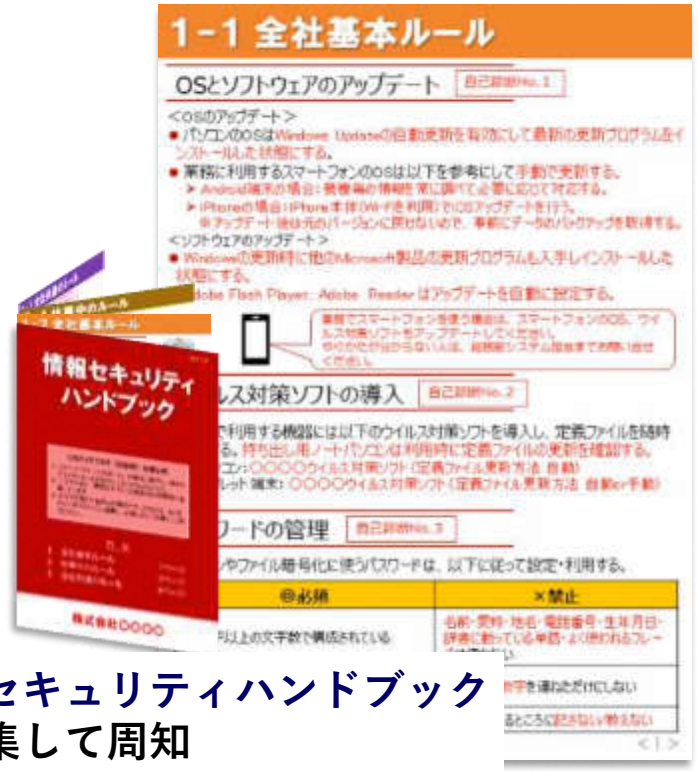
5分でできる！情報セキュリティ自社診断のオンライン版

https://security-shien.ipa.go.jp/diagnosis/selfcheck/index.html

③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する





情報セキュリティハンドブック
を編集して周知

SECURITY ACTION申込方法

1)取組み目標を決める

- 一つ星▶「情報セキュリティ5か条」の実行を宣言
- 二つ星▶「5分でできる！情報セキュリティ自社診断」で実施状況を把握し対策を決定
  「情報セキュリティ基本方針」を公開

ダウンロード：https://www.ipa.go.jp/security/security-action/mark/

2)自己宣言する

- 使用規約に同意してロゴマークをダウンロード
- ロゴマークを表示してSECURITY ACTION自己宣言

ロゴマーク申込：https://security-shien.ipa.go.jp/security/entr

中小企業の情報セキュリティ対策ガイドライン（第３版）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- 情報セキュリティ対策の必要性を理解し、実践する際の手順や手法を分かりやすくまとめたガイドライン
- 本編と実用的な付録で構成
  - 本編 第１部　経営者編
    第２部　実践編
  - 付録
    ① 情報セキュリティ５か条
    ② 情報セキュリティ基本方針（サンプル）
    ③ ５分でできる！情報セキュリティ自社診断
    ④ 情報セキュリティハンドブック（ひな形）
    ⑤ 情報セキュリティ関連規程（サンプル）
    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
    ⑦ リスク分析シート

第1部　経営者編

ガイドラインP.5-14

1 情報セキュリティ対策を怠ることで企業が被る不利益

(1) 金銭の損失

(2) 顧客の喪失

(3) 業務の停滞

(4) 従業員への影響

2 経営者が負う責任

(1) 経営者などに問われる法的責任

(2) 関係者や社会に対する責任

3 経営者は何をやらなければならないのか

(1) 認識すべき「３原則」

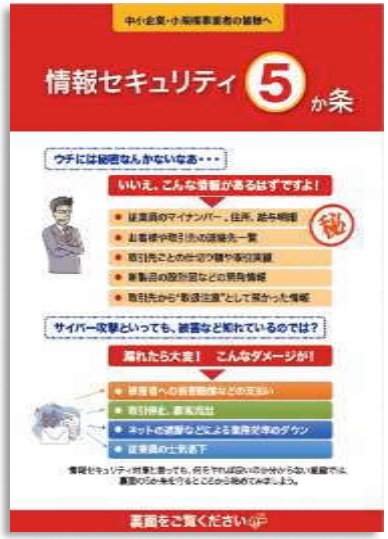
(2) 実行すべき「重要７項目の取組」

第2部 実践編

ガイドラインP.15-54

• 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



SECURITY ACTION
★一つ星を宣言

Step2
組織的な取り組みを開始する

SECURITY ACTION
★★二つ星を宣言

Step3
本格的に取り組む

Step4
より強固にするための方策

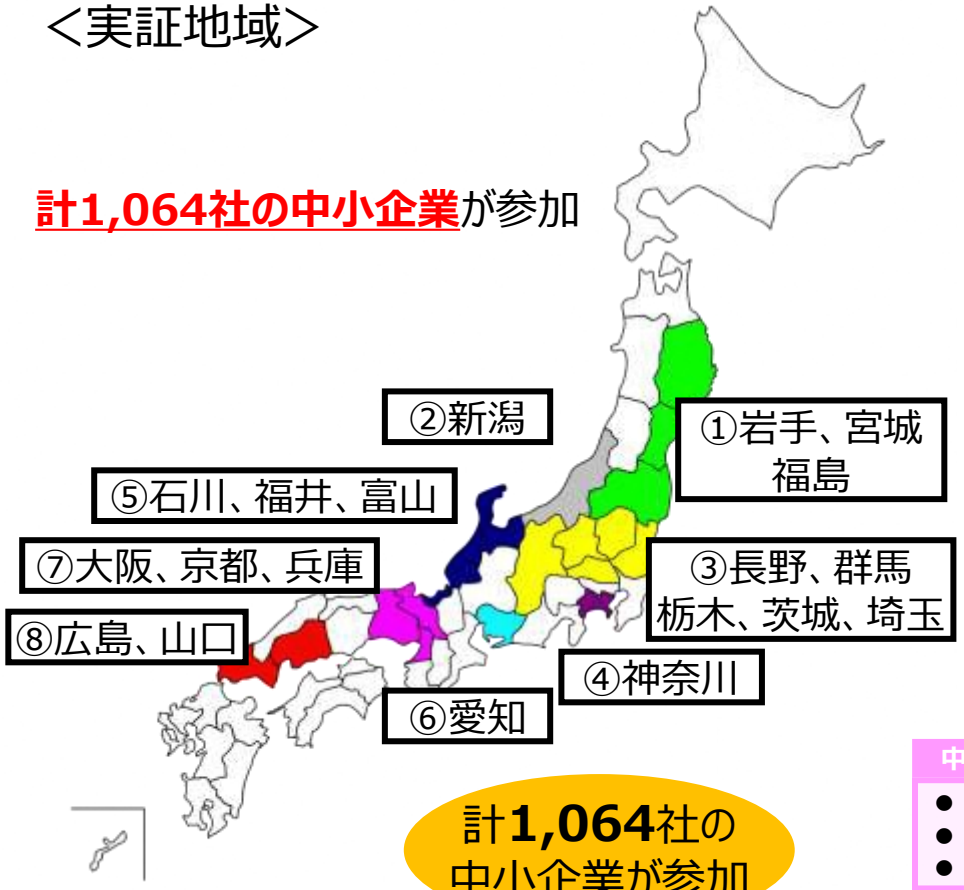
- 情報収集と共有
- ウェブサイトの情報セキュリティ
- クラウドサービスの情報セキュリティ
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- 詳細リスク分析の実施方法

サイバーセキュリティお助け隊実証事業（2019年度の取組）

- 全国**8地域**において、中小企業のセキュリティ対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティサービスの開発を目指し、実証事業を実施。**
- 2019年度の実施内容・成果について、IPAより報告書を公開。（2020年6月15日）

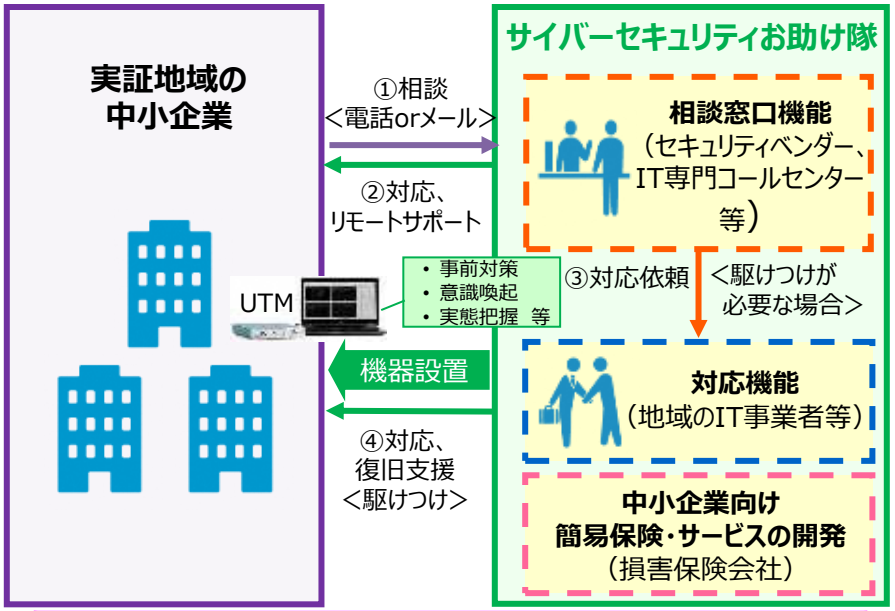
＜実証地域＞

計1,064社の中小企業が参加



計**1,064**社の
中小企業が参加

＜実証のイメージ＞



実証結果

中小企業　側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

2019年度サイバーセキュリティお助け隊実証事業の結果

- 1,064社が参加した実証期間中に、全国８地域で**計910件のアラート**が発生。重大なインシデントの可能性ありと判断し、**対処を行った件数**は**128件**。対処を怠った場合の**被害想定額**が**5000万円**近くなる事案も。
- 実証参加前後の中小企業の意識変化や、お助け隊サービスに求められる機能等が明らかになった。

＜駆け付け支援の対象となった特徴的な対応事例＞

古いOSの使用

・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。

・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。

・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。

・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ホテルWi-Fiの利用

・社員が**出張先ホテルのWi-Fi環境**でなりすましメールを受信し、添付されたマルウェアを実行したことで**Emotetに感染**。

・感染により悪性PowerShellコマンドが実行され、アドレス情報が抜き取られた後、**当該企業になりすまして、取引先等のアドレス宛に悪性メールが送信**された。

サプライチェーン攻撃

・実証参加企業でマルウェア添付メールを集中検知。

・**取引先のメールサーバーがハックされてメールアドレスが漏えい**し、それらのアドレスからマルウェア添付メールが送付されていた。

・メールは賞与支払い、請求書支払い等を装うなりすましメールであり、**サプライチェーンを通じた標的型攻撃**であった。

https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

＜実証参加の成果（参加中小企業のアンケート結果より）＞

- アラート通知が実際にあり、**他人事ではないとの意識につながった。**（大阪府・建設業）
- UTM導入時、当社に**専門知識が無いため、業者と話がかみ合わず、導入に手間取った。**（神奈川県・サービス業）
- 参加することで、情報セキュリティ対策を実施していることを、**外向けにアピールできる**のが良い。（新潟県・電気通信工事業）
- 総務担当がセキュリティを兼務していることもあり、**ワンパッケージでやってくれると非常に助かる。**（石川県・製造業）

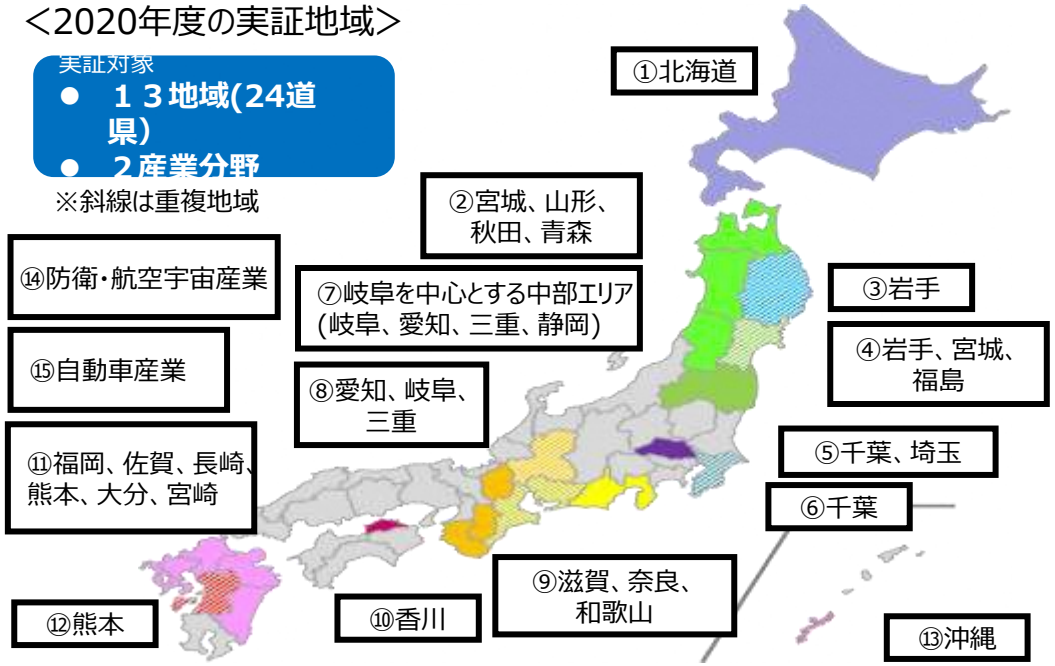
サイバーセキュリティお助け隊実証事業（2020年度の取組）

- 地域の団体、セキュリティ企業、保険会社がコンソーシアムを組み、中小企業向けのセキュリティ対策支援の仕組みの構築を目的とした**実証事業**を実施（全国で**15件**実施）。
- 本事業により、中小企業の事前対策の促進や意識喚起、攻撃実態や対策ニーズの把握を行い、**民間による中小企業向けのセキュリティ簡易保険サービスの実現**を目指す。

＜2020年度の実証地域＞

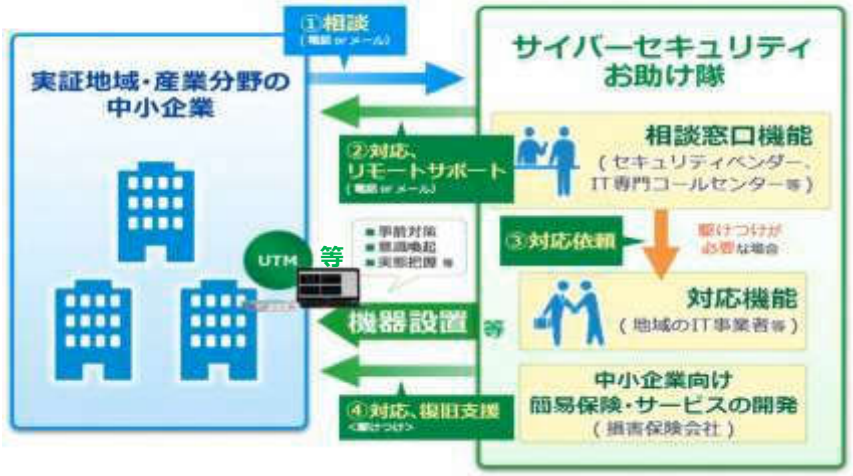
実証対象
- １３地域(24道県)
- ２産業分野

※斜線は重複地域



※2019年度実証地域（全8地域、1064社の中小企業が参加）：
①宮城、岩手、福島②新潟③長野、群馬、栃木、茨城、埼玉④神奈川⑤石川、富山、福井
⑥愛知⑦大阪、京都、兵庫⑧広島、山口

＜実証のイメージ＞



実証結果

中小企業　側
- 自社の攻撃実態等への気付き
- セキュリティ事前対策の促進
- 事後対応への意識向上　　等

保険会社、セキュリティベンダー　側
- 中小企業のセキュリティ対策状況の把握
- 中小企業の被害実態の把握
- 中小企業が求めるサービスの把握　　等

2020年度サイバーセキュリティお助け隊実証事業の結果

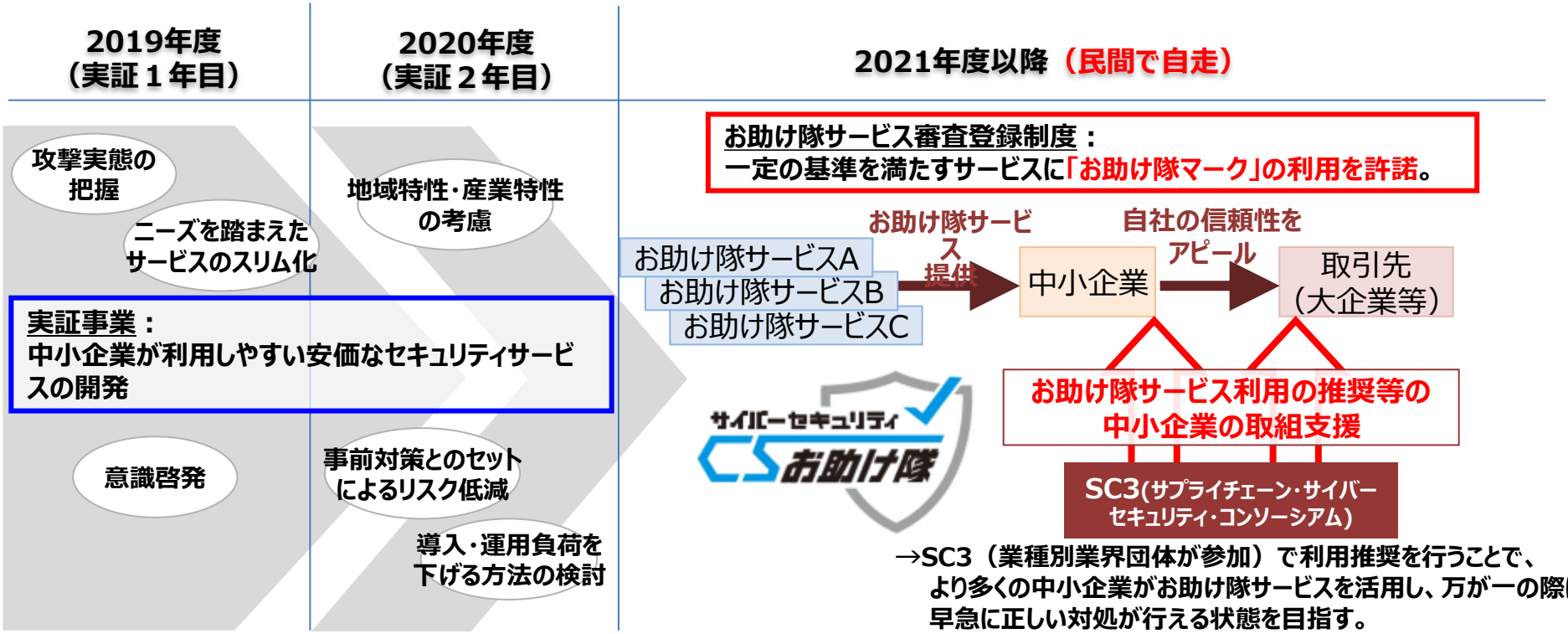
- 新型コロナウイルス感染症拡大の影響もあり、**リモートにより管理可能なサービスの提供**が多く行われ、インシデント発生に際しても**概ねリモートによる支援対応**を実施。

＜2020年度実証事業における具体的な対応事例＞

事例１	UTMサービスを導入した企業において、同一ホストにて断続的に**要注意検知が発生していることが確認**されたため、お助け隊事業者が駆けつけ支援を実施。 対象の**マルウェアと判定されたプログラム**は、インターネットからダウンロードしたフリーソフトであったことが判明、**駆除を実施**した。
事例２	UTMサービスを導入した企業において、PCの「ウィルス対策ソフト」を導入済みであったものの、**「不正なIPアドレスへの通信」が成立していることが確認**されたため、緊急度「高」のアラートを発報、支援を実施。 接続元端末をLANから分離した上、**ウイルス対策ソフトでのフルスキャンを実施した結果、何も検知されなかった**ものの、もし被害に至っていた場合の**被害試算額**は**54,760,000円**にも。
事例３	UTMサービスを導入した企業において、**マルウェアへの感染の疑いがある通信をUTMで検知**、リモート支援により駆除を実施。 該当端末(PC)をLANから分離した上でフルスキャンを実施した結果、**Hacktool及びトロイの木馬、計6件のマルウェアを発見したため駆除を実施**した。

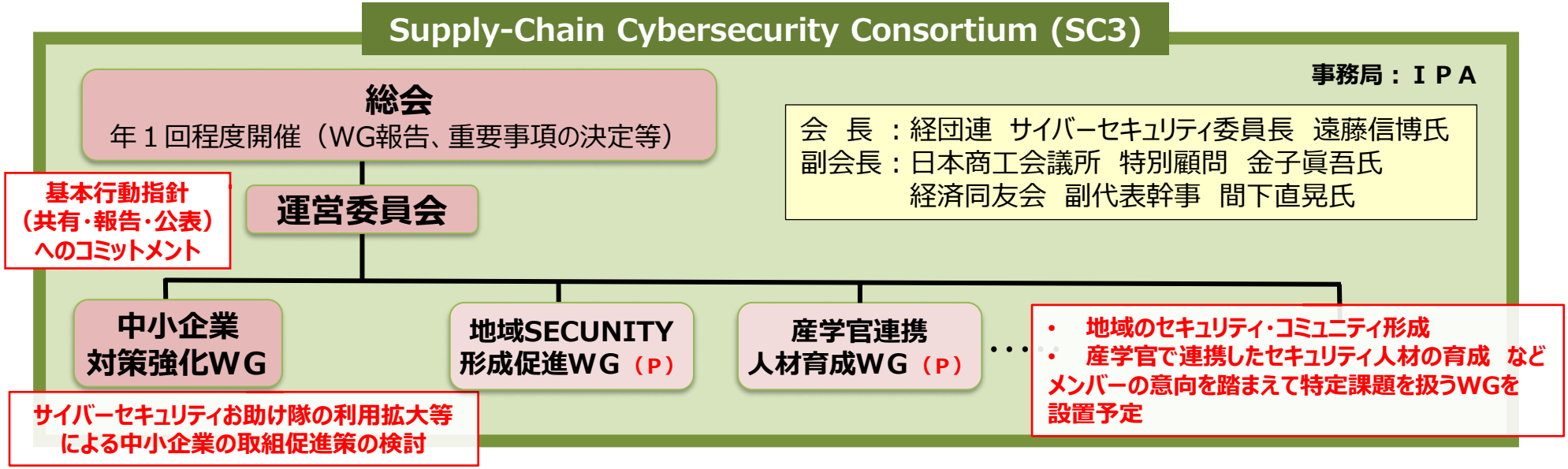
「サイバーセキュリティお助け隊サービス」実証事業から民間サービスへの移行

- 実証事業で得られた知見、及びSC3中小企業対策強化WGにおける議論に基づき、中小企業向けのセキュリティサービス（お助け隊サービス）が満たすべき基準として、**「サイバーセキュリティお助け隊サービス基準」**を２月に策定・公表。
- 同基準を充足するサービスに**「お助け隊マーク」**を付与。IPAにおいてブランド管理を行うとともに普及促進。



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）

- **趣旨：**大企業と中小企業がともにサイバーセキュリティ対策を推進するためのコンソーシアムを立ち上げ、「基本行動指針※」の実践と中小企業・地域を含めたサプライチェーンのサイバーセキュリティ対策を産業界全体の活動として展開していく。
  ※サイバー攻撃事案発生時における、「共有、報告、公表」によるリスクマネジメントの徹底。
- **参加者:** 経済団体、業種別業界団体　等（2021年2月時点で**168会員**）
- **設立日:** 2020年11月1日（設立総会：2020年11月19日）
- **活動:** 特定の課題についてWGを設置し、具体的アクションを展開。



サイバーセキュリティお助け隊サービス基準の概要

(コンセプト)中小企業に対するサイバー攻撃への対処として、**最低限必要なサービス**を**効果的**かつ**安価**に、**確実**に提供する。

主な要件	概要
相談窓口	お助け隊サービスの導入・運用中に関するユーザからの各種相談を受け付ける窓口を一元的に設置／案内
異常の監視の仕組み	・ユーザのネットワークを24時間見守り、攻撃を検知・通知する仕組み（UTM等のツールと異常監視サービスから構成）を提供すること（ネットワーク一括監視型の場合） ・ユーザの端末（PCやサーバ）を24時間見守り、攻撃を検知・通知する仕組み（EDR等のツールと異常監視サービスから構成）を提供すること（端末監視型の場合）
緊急時の対応支援	・営業エリア内であればユーザの指定する場所に技術者を派遣できること ・サービス規約等でユーザと合意した範囲であればリモート対応でも可
中小企業でも導入・運用できる簡単さ	IT・セキュリティの専門知識のないユーザでも導入・運用できるような工夫が凝らされていること
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の場合：月額１万円以下（税抜き）（条件付きで可。PC○台までなら等） ・端末監視型の場合：端末１台あたり月額2,000円以下（税抜き） ・最低契約年数は２年以内 ・初期費用、契約年数等の細かな条件もユーザに分かりやすく説明すること
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各種コストを保証するサイバー保険が付帯されていること
上記機能のワンパッケージ提供	・原則として、これら機能をユーザが個別に契約することなく一元的に購入可能であること（ユーザにおいて手続上の煩雑さを伴わないよう工夫が凝らされていること）
中小企業向けセキュリティ事業の実績	お助け隊実証事業に参加していたこと又は上記構成のサービスを中小企業向けに提供・運用した実績があること
情報共有	お助け隊サービス事業者どうしの深いレベルの情報共有（少なくともアラートの統計情報）に応じること
事業継続性	要員の確保、品質管理等の社内プロセス整備、企業としての安定した財政基盤、経理処理能力等
更新	２年毎に更新審査を受けること

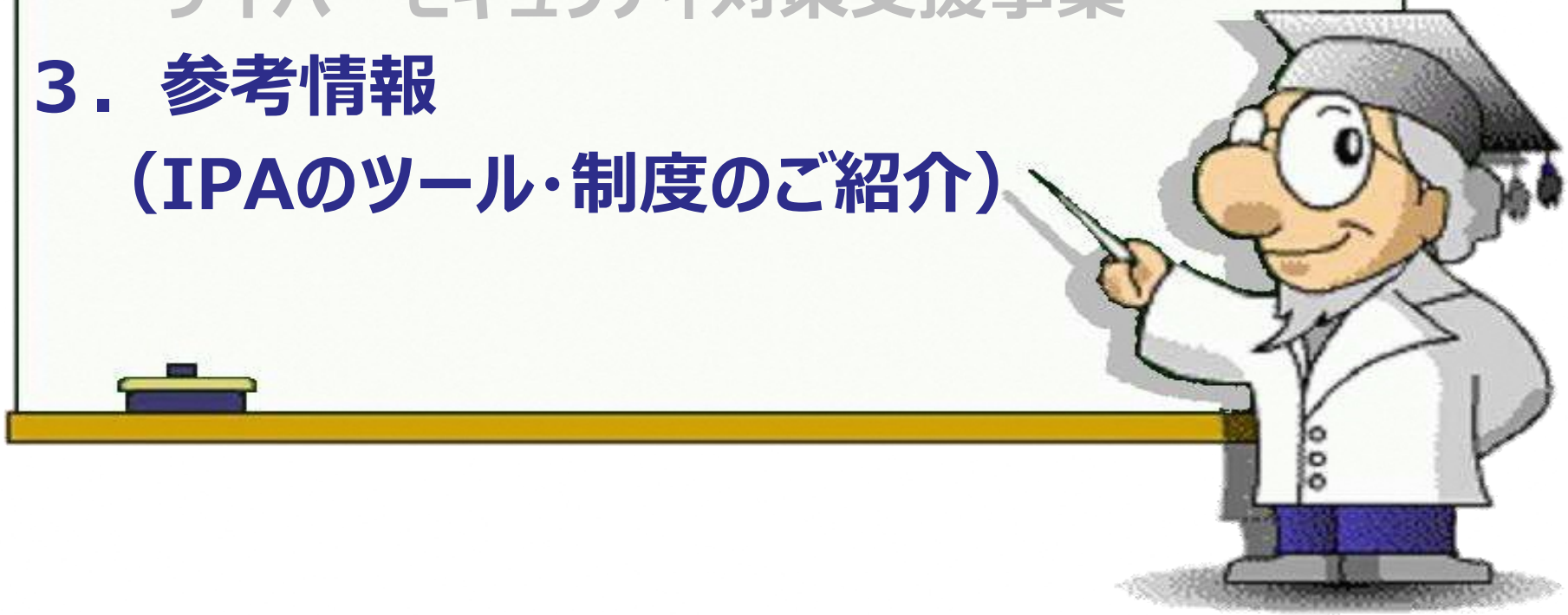
サイバーセキュリティお助け隊サービスの普及に向けて（令和３年度以降）

- 2021年3月に第１回審査を実施予定。
- 2021年4月からは当該審査を経た**「サイバーセキュリティお助け隊マーク」の付けられたサービスの普及を開始。**

「サイバーセキュリティお助け隊サービス」利用の推奨等の普及促進（2021.04～）

IPAにおいてお助け隊のブランドを管理、SC3（業種別業界団体も参加）で利用推奨を行うことで、その普及を促進。
幅広い中小企業において無理なくサイバーセキュリティ対策を導入・運用することを支援し、もってサプライチェーン全体のセキュリティの底上げを図ることを目的。

目次



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「始めたい」「強化したい」「学びたい」中小企業の方々をサポートするポータルサイト

- 5分でできる！自社診断
  ＆ポイント学習
- セキュリティプレゼンター支援
- SECURITY ACTION
  自己宣言者サイト

情報セキュリティ対策支援サイト　検索

情報セキュリティ対策支援サイト

5分でできる！自社診断＆ポイント学習

・職場での日常を取り入れた親しみやすいシナリオで、
セキュリティに関する様々な事例を疑似体験しながら
正しい対処法を**1テーマ5分で**学べる

・学習テーマは自社診断の25の質問と連動

修了証も発行できます

情報セキュリティ対策支援サイト

セキュリティプレゼンター支援

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。

映像で知る情報セキュリティ

https://www.ipa.go.jp/security/keihatsu/videos/

- 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27タイトル。
- YouTube「IPAチャンネル」では27タイトルをいつでも視聴可能。主な映像はDVD-ROMでも提供中。

IPA　映像　**検索**

情報セキュリティ安心相談窓口

・ウイルスや不正アクセスに関する相談にアドバイスを提供
・相談内容から判明したトラブルの傾向、手口、対策に関する情報を公開

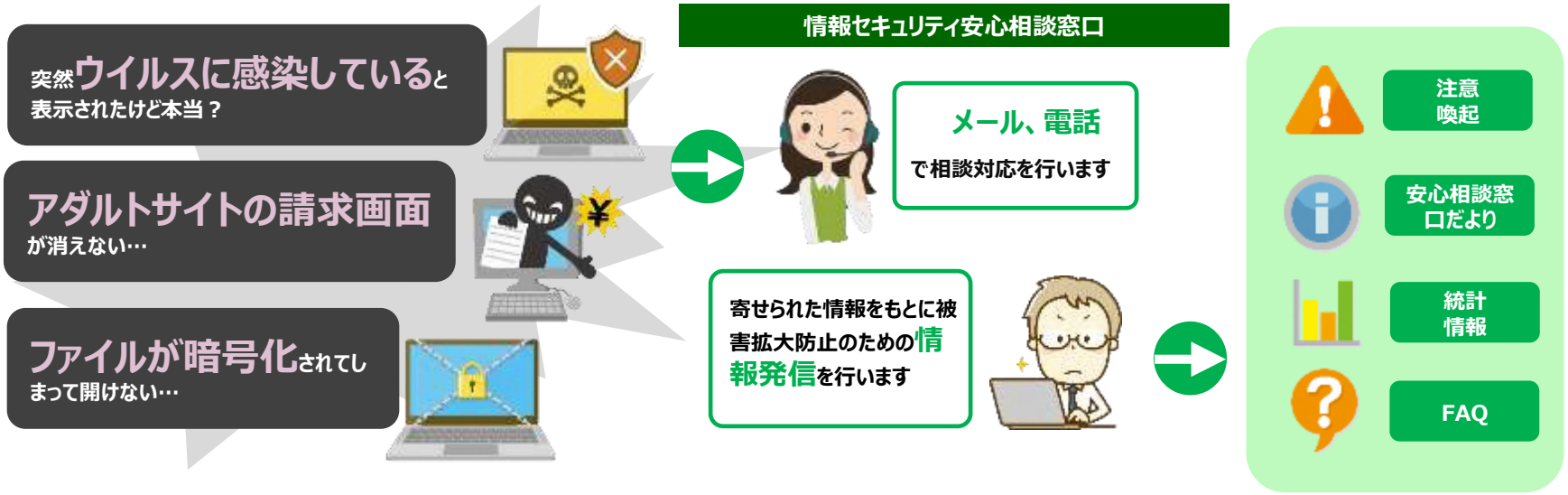
03-5978-7509

電話　平日　10：00-12：00、13：30-17：00

anshin@ipa.go.jp

メール

ポータル　IPA安心相談　検索



テレワークを行う際のセキュリティ上の注意事項

テレワーク勤務者に向けたセキュリティ上の注意事項を公開

https://www.ipa.go.jp/security/announce/telework.html

・**テレワークを行う際**のセキュリティ上の注意事項

・**テレワークから職場に戻る際**のセキュリティ上の注意事項

IT利用者に求められるIT知識を習得できる国家試験

ITパスポート試験

試験の特徴

・ITパスポートは、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。

メリット

試験勉強を通じ、幅広い分野の基礎知識が取得可能！

・情報セキュリティや情報モラルに関する知識が身に付きます
・企業コンプライアンス・法令遵守に貢献する正しい知識が身に付きます
・経営戦略、財務など、経営全般に関する基礎知識が身に付きます
・業務に必要なITの基礎知識が身に付きます
・システム開発などIT管理に関する基礎知識が身に付きます

試験時間・出題形式

試験時間	出題形式	出題数 解答数	基準点	
			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)

試験実施概要

・試験実施日

CBT方式で随時実施中

CBTとは、コンピュータを利用して実施する試験方式のことです。

・インターネットにて受付

情報セキュリティマネジメント試験

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。
社会人として必要な情報セキュリティの知識を体系的に習得できます。
・身近な事例をベースにした実践的な出題。

受験を特にお勧めする方

・業務で個人情報を取り扱う方
・業務部門・管理部門で情報管理を担当する方

試験時間・出題形式

区分	試験時間	出題形式	出題数 解答数	基準点
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)
午後試験	90分	多肢選択式	3問 3問	60点 (100点満点)

試験実施概要

・試験実施日

CBT方式で上期、下期に実施

CBTとは、コンピュータを利用して実施する試験方式のことです。

・インターネットにて受付

新国家資格「情報処理安全確保支援士」

IPA

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人材の質の担保
- 「情報セキュリティスペシャリスト試験」をベースとした新たな試験の合格者を登録
- 継続的な講習受講義務により、最新の知識・技能を維持

②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）

③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

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
試験受験

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

ご清聴ありがとうございました

IPA 独立行政法人 情報処理推進機構