IPA Better Life with IT

サイバー攻撃の脅威と中小企業のセキュリティ対策のポイント

独立行政法人 情報処理推進機構
セキュリティセンター 企画部 中小企業支援グループ
芳賀　政伸（中小企業診断士）

情報処理推進機構（IPA）とは

経済産業省の政策実施機関として：

情報セキュリティ対策を実現

- ウイルス・不正アクセス等の**情報受付**
- 情報セキュリティ対策の**普及啓発**
- 標的型サイバー攻撃情報の**共有・初動対応**

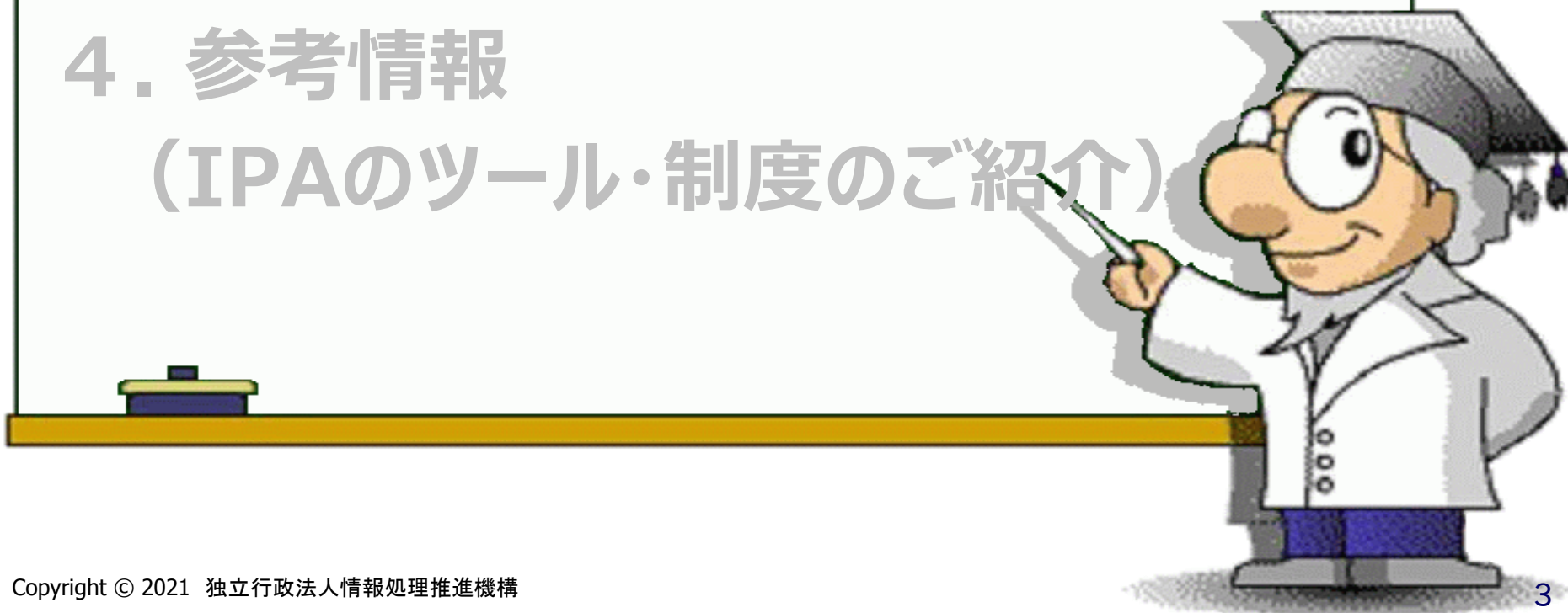
IT人材を育成

- 国家試験「**情報処理技術者試験**」実施、国家資格「**情報処理安全確保支援士**」認定
- **イノベーション人材**の育成・発掘の取組
- 産業サイバーセキュリティ対策を担う**中核人材**育成

IT社会の動向を調査・分析し基盤構築

- **先端技術情報**の収集・調査分析
- 各種**指針**の策定・**ガイドライン**の公開
- IT利活用のための**基盤構築**

目次



情報セキュリティ10大脅威2021

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

- 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

脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人 **「個人」**

- 企業や政府機関などの組織
- 組織のシステム管理者や社員・職員 **「組織」**

「個人」と「組織」の２つの立場で脅威を解説

情報セキュリティ10大脅威2021
「個人」および「組織」向けの脅威の順位

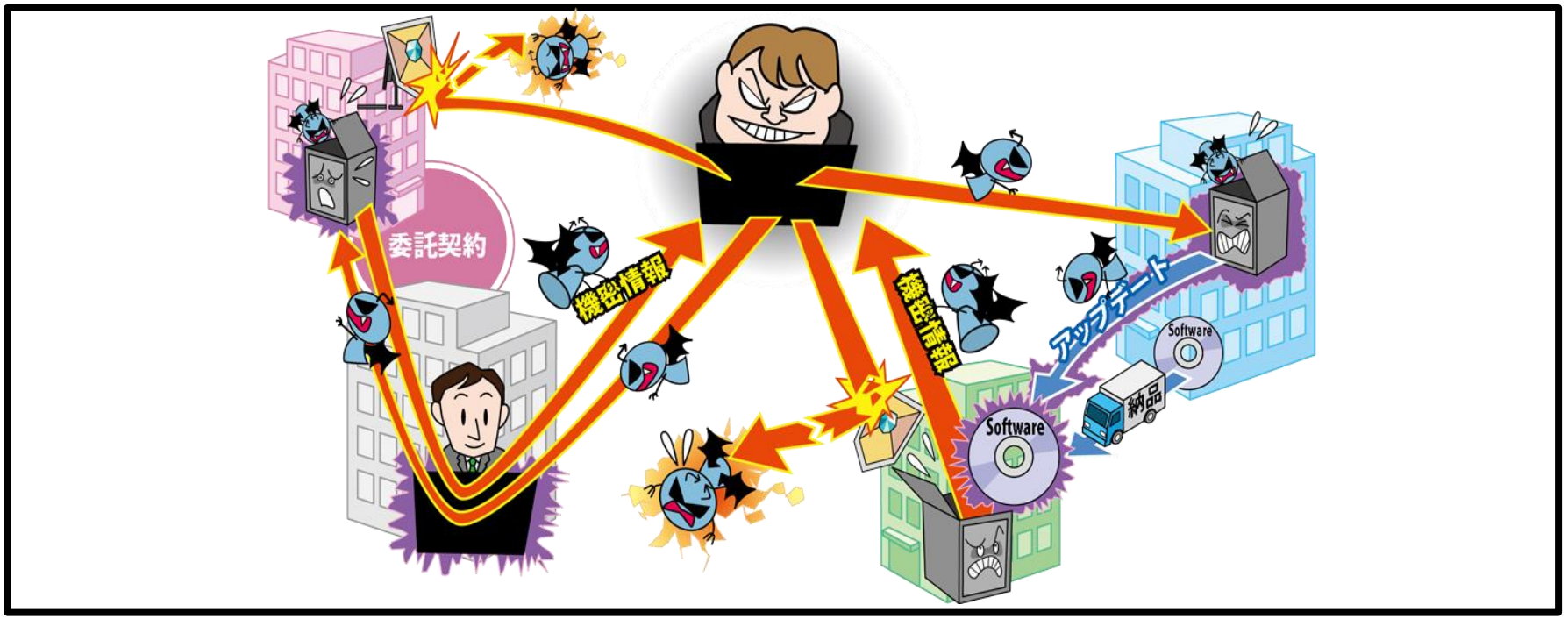
IPA

NEW： 初めてランクインした脅威

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

【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、業務委託先等の一連の商流（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
- 取引先や一部業務を委託している外部組織から情報漏えい

【4位】サプライチェーンの弱点を悪用した攻撃

- 攻撃手口

サプライチェーンの中でセキュリティが脆弱な組織を狙う

- 標的組織の取引先や委託先を攻撃し、それらが保有する標的組織の機密情報を狙う
- ソフトウェ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

  ソフトウェアのアップデートにウイルスを仕込み、アップデートを適用した利用者にウイルスを感染させる等

【4位】サプライチェーンの弱点を悪用した攻撃

- 2020年の事例/傾向①
  - 中国拠点を足掛かりに国内拠点へ侵入(※1)
    - ・2019年に大手電機メーカーから情報流出が確認された
    - ・中国拠点のサーバーがウイルスに感染していた
    - ・中国拠点を足掛かりに国内拠点へ侵入しウイルス拡散
    - ・最終的に感染の疑いがある端末は国内外含め132台
    - ・既存の防御をすり抜ける高度かつ巧妙な攻撃だった

【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

【4位】サプライチェーンの弱点を悪用した攻撃

- 2020年の事例/傾向②
  - ソフトウェアの正規のアップデートにバックドア（※1,※2）
    - 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
    - ソフトウェアのアップデートファイルにバックドアが仕込まれた
    - アップデートファイルで更新した組織が感染
    - その後バックドアから攻撃者が組織に侵入
    - 米政府をはじめ多くの米国組織で感染被害の報告あり
      ※国内でも感染の形跡が確認された

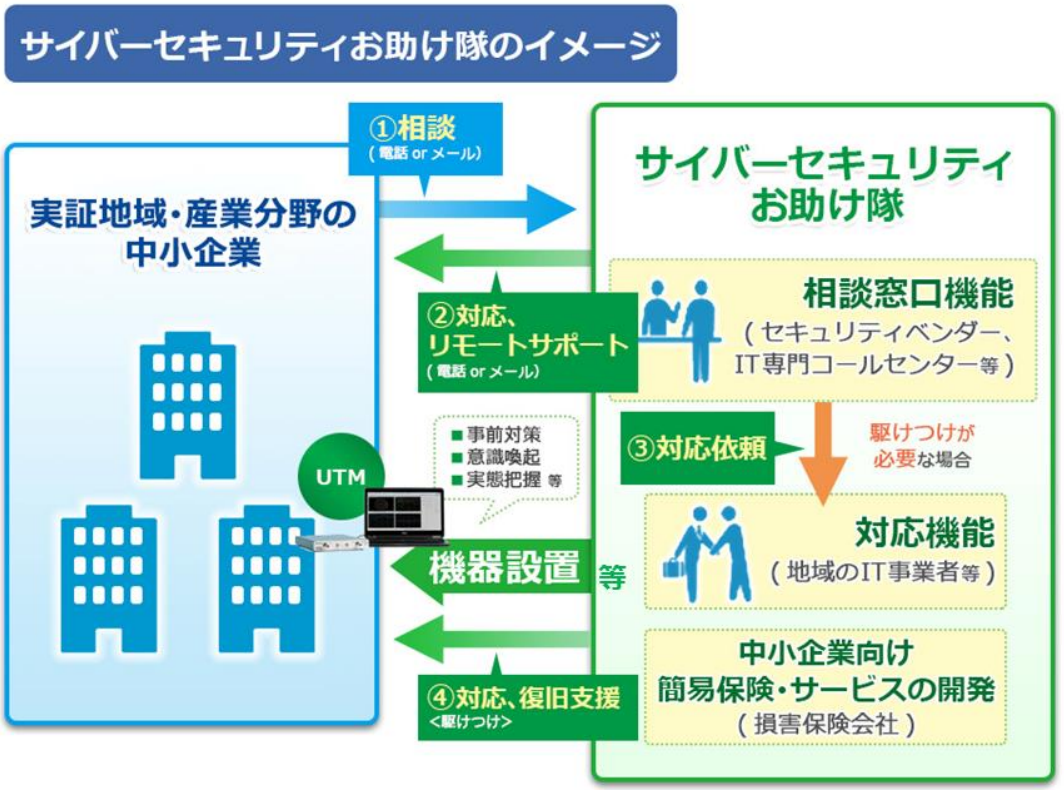
【出典】
※1 SolarWinds Security Advisory
https://www.solarwinds.com/ja/securityadvisory
※2 SolarWindsのサプライチェーン攻撃についてまとめてみた
https://piyolog.hatenadiary.jp/entry/2020/12/20/045153

サイバーセキュリティお助け隊実証事業

中小企業の被害実態等を把握することで、**中小企業向け事後サービスに必要な人材スキルやサービス内容等を明らか**にし、**中小企業の支援機能を低コストで構築**するために実証事業を実施（2019年度、2020年度）

- 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を構築。
- **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**を目指し、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を把握。

- 2019年度には**全国8地域**で中小企業**1,064社**が参加。
- 2020年度には**15の地域・産業分野**で中小企業**1,117社**が参加。



サイバーセキュリティお助け隊
2019年度実証事業における対応事例

- 実証期間中に、重大なインシデントの懸念・可能性ありと判断し、**対処・支援を行った件数**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＞

サイバーセキュリティお助け隊
2020年度実証事業における対応事例

IPA

- 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。

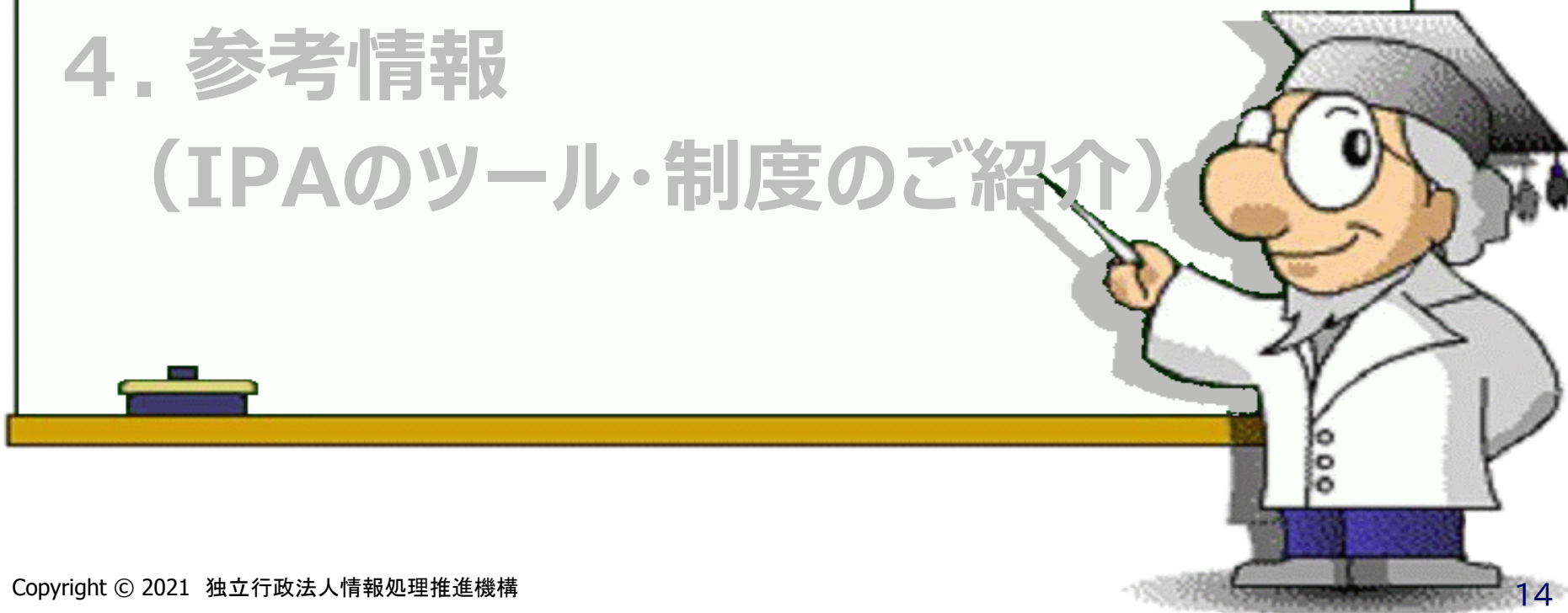
狙われる中小企業の対策が急務！

- 大企業だけではなく、**中小企業もサイバー攻撃のターゲットになっている**
- 取引先攻撃への踏み台にされる懸念
- サイバー攻撃だけではなく、内部不正やミスによる情報漏えいや情報の棄損、消失もあり得る

- 金銭的被害、業務停止・遅延、信用失墜。。。

- せっかく築き上げたものを失わないために、**中小企業においてもセキュリティ対策を行うことが急務！**

目次



映像をご覧ください

中小企業における情報セキュリティ対策の必要性と、まず実践して欲しい対策を人間ドックの診断に見立てて、わかりやすくご説明します。

映像をご覧ください

このページは白紙です

情報セキュリティ10大脅威でみる

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

情報セキュリティ対策の基本	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

できるところから始める

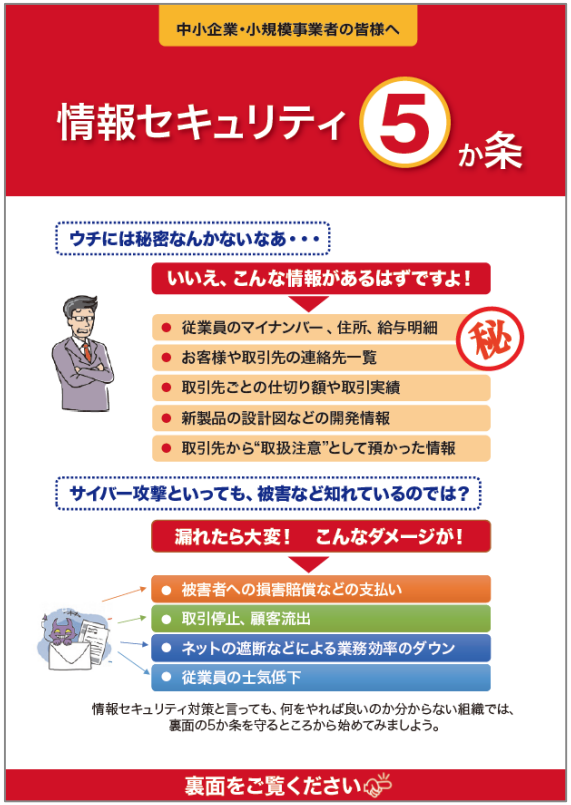
情報セキュリティ５か条

- 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。

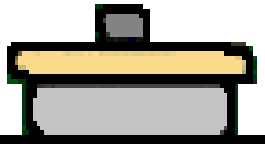
1. **OSやソフトウェアは常に最新の状態にしよう！**
2. **ウイルス対策ソフトを導入しよう！**
3. **パスワードを強化しよう！**
4. **共有設定を見直そう！**
5. **脅威や攻撃の手口を知ろう！**



https://www.ipa.go.jp/files/000055516.pdf

ソフトウエアの脆弱性（ぜいじゃくせい）対策

1 OSやソフトウェアは常に最新の状態にしよう！

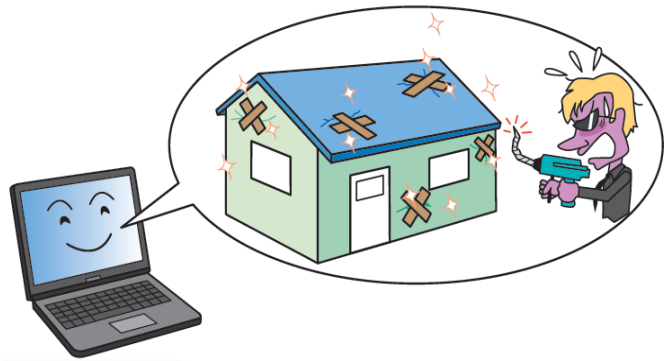


ＯＳやソフトウェアは常に最新の状態にする

- OSやソフトウェアのセキュリティ上の弱点を放置していると、それを悪用したウイルスに感染したり、攻撃を受けたりする危険性があります。
- 利用しているOSやソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

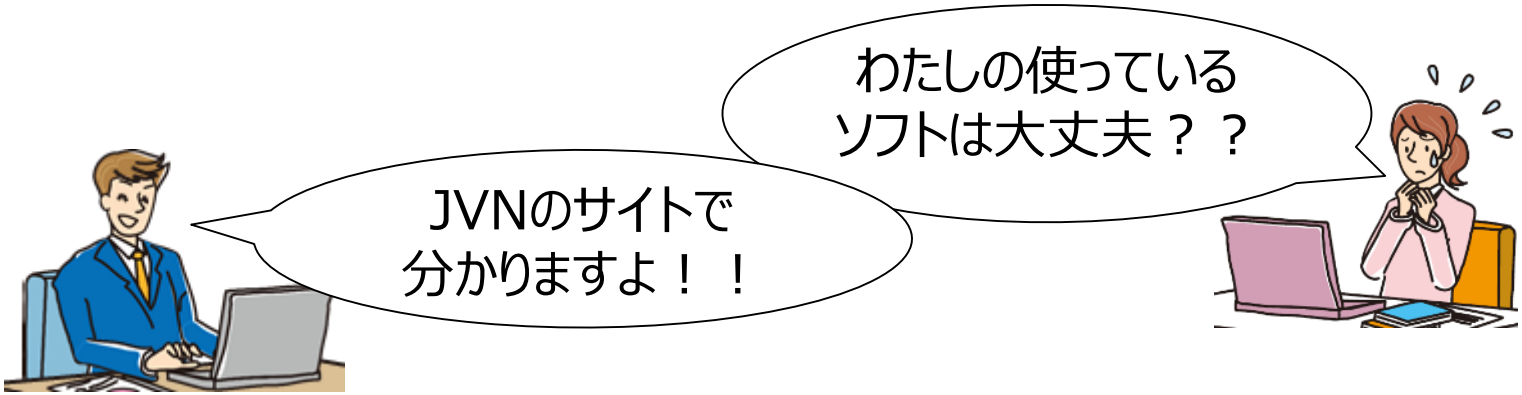
＜対策例＞

- 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



ぜいじゃくせい 脆弱性(セキュリティホール)とは

- ソフトウェアやシステムなどに潜むセキュリティ上の弱点のことで、セキュリティホールともいいます。



JVN iPedia 脆弱性対策情報データベース

https://jvn.jp

JVN は、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。JPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営しています。

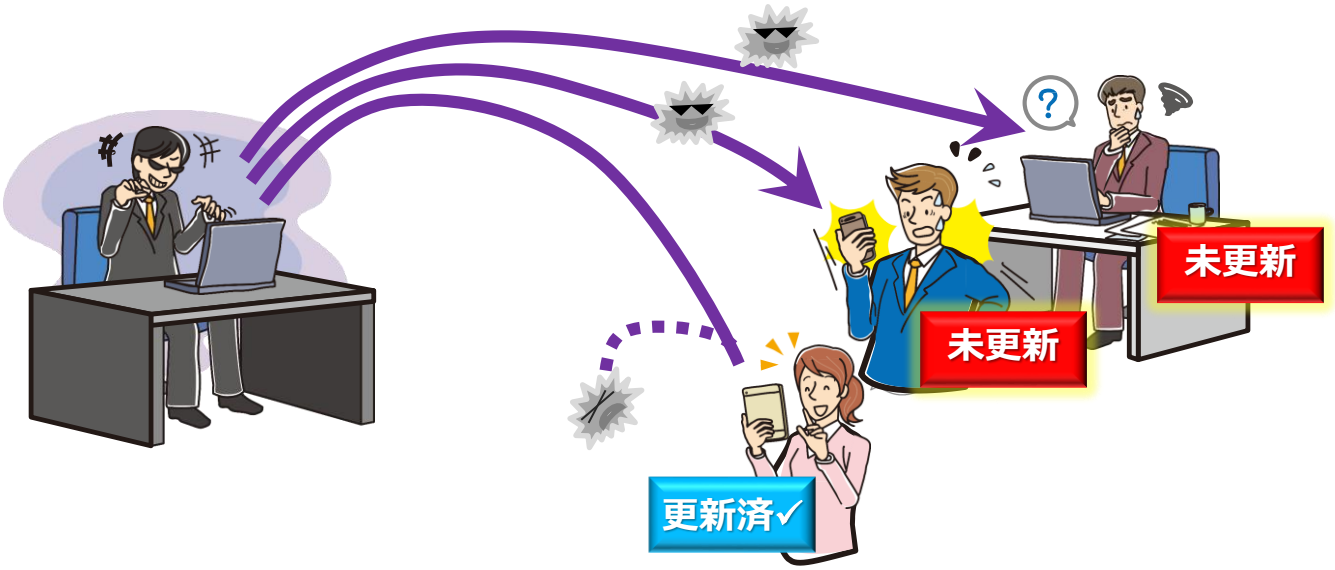
ソフトウェアに脆弱性があると…

不正なコードが仕込まれたウェブサイトを閲覧しただけで…

- コンピュータへの不正アクセスが行われる。
- コンピュータウイルスに感染させられる。

などの脅威にさらされることになります。

脆弱性の解消は必須です!



脆弱性の解消方法

Microsoft社の場合

- Windows UpdateでOS関連を更新
- Windows Updateの詳細オプションで他のMicrosoft製品を更新

Apple社の場合

- macOS ソフトウェア・アップデートでOSと付属するアプリケーションを更新

※ Microsoft社・Apple社は初期設定で自動的に更新される設定になっています。

その他のソフトウェア

- 公表された方法で最新版またはセキュリティ更新を適用

※ ソフトウェアやメーカー、ベンダーにより更新方法が異なることがあるのでホームページやJVN(P.21)、MyJVNバージョンチェッカ(P.25)で確認しましょう。

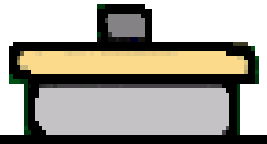
MyJVNバージョンチェッカ

http://jvndb.jvn.jp/apis/myjvn/

- パソコンにインストールされているソフトウェアのバージョンが最新であるかを簡単な操作で確認できる無償ツール

コンピュータウイルス対策

2 ウイルス対策ソフトを導入しよう！

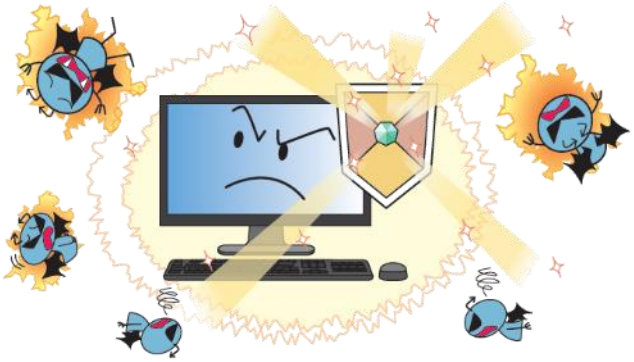


ウイルス対策ソフトを導入し適切に利用する

- パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するなど、悪質なウイルスが急増しています。
- ウイルス対策ソフトを導入し、不審サイトへのアクセスやメール受信など、感染経路にも気をつけましょう。
- 新種のウイルスは日々発見され拡散しているため、常に新種も検出できるようにしなければ感染してしまう可能性があります。最新のウイルス対策ができるように設定を確認しましょう。

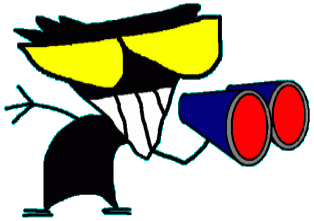
＜対策例＞

- ウイルス定義ファイルが自動更新されるように設定する
- 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)を導入する



ウイルス対策ソフトの設定

- ウイルス対策ソフトは水際でウイルスを発見し、感染を予防する「自動保護(リアルタイム保護)」にして、「発見したらすぐ駆除する」設定にすることを推奨します。
- ウイルスの種類は日々増加しているので、ウイルスの「手配書」であるウイルス定義ファイルが常に最新の状態になるよう「自動更新」を推奨します。

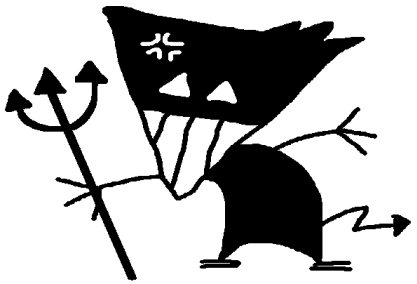


ウイルス対策ソフトに関する勘違い

- ウイルス対策ソフトは万能薬？
  これさえあればウイルスなんか怖くない？
  - ウイルス対策ソフトの利用は予防手段のひとつです。
  - 新種のウイルスや亜種を取り逃がす場合もあります。
  - 壊されたファイルやシステム環境は復旧できません。
  - だから…

ウイルスの感染経路を理解する…

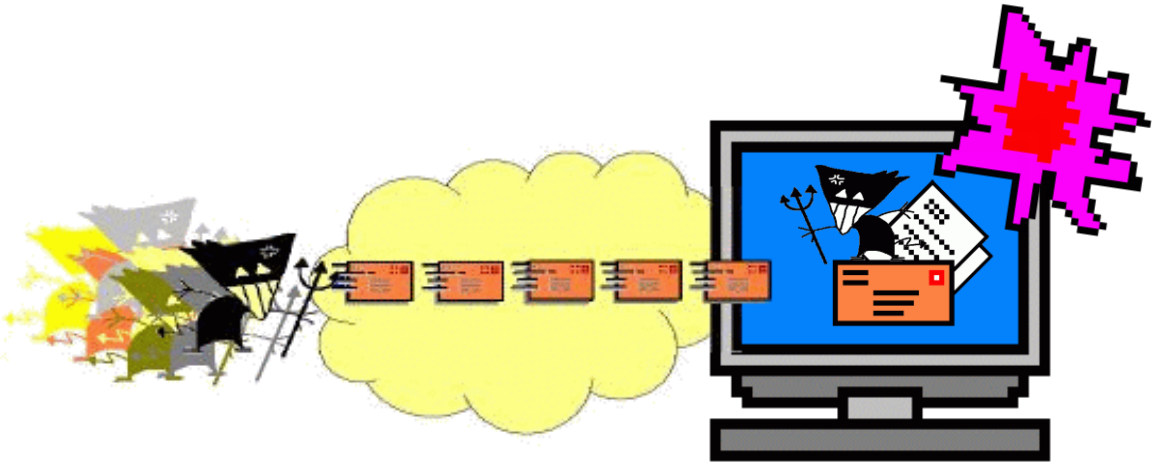
1. 電子メールからの感染
   - 電子メールの添付ファイルを開くことにより感染
2. ウェブサイトからの感染
   - ウイルスが仕掛けられたウェブサイトを閲覧することにより感染
   - ウェブサイトからダウンロードしたファイルを開いたら感染
   - スマホに不正アプリをインストールしてしまい感染
3. USBメモリなど外部記憶媒体からの感染
   - USBメモリの不正ファイルを開いて感染



電子メールからの感染

- メールの添付ファイル※を開くことにより感染
- メール本文にあるURLのリンク先のサイトにアクセスして感染

※送信者のパソコンがウイルスに感染していることで、送られてくるファイルが感染していたり、添付ファイルがウイルスそのものである場合もある



電子メールからの感染に対する予防

- ☑ ウイルス対策ソフトの正しい運用
- ☑ OSやソフトウェアの脆弱性の解消
- ☑ メーラーのセキュリティ設定の強化
  (外部コンテンツブロック設定など)
- ☑ メール本文はテキスト形式で表示
  (HTML形式は見栄えは良いが不正な仕掛けが施せる)
- ☑ スパムメールのフィルタリング

  ウイルス感染させられないように…
- ☑ 身に覚えのないメールを開かないように社員教育
- ☑ 不審なメールに関する情報共有

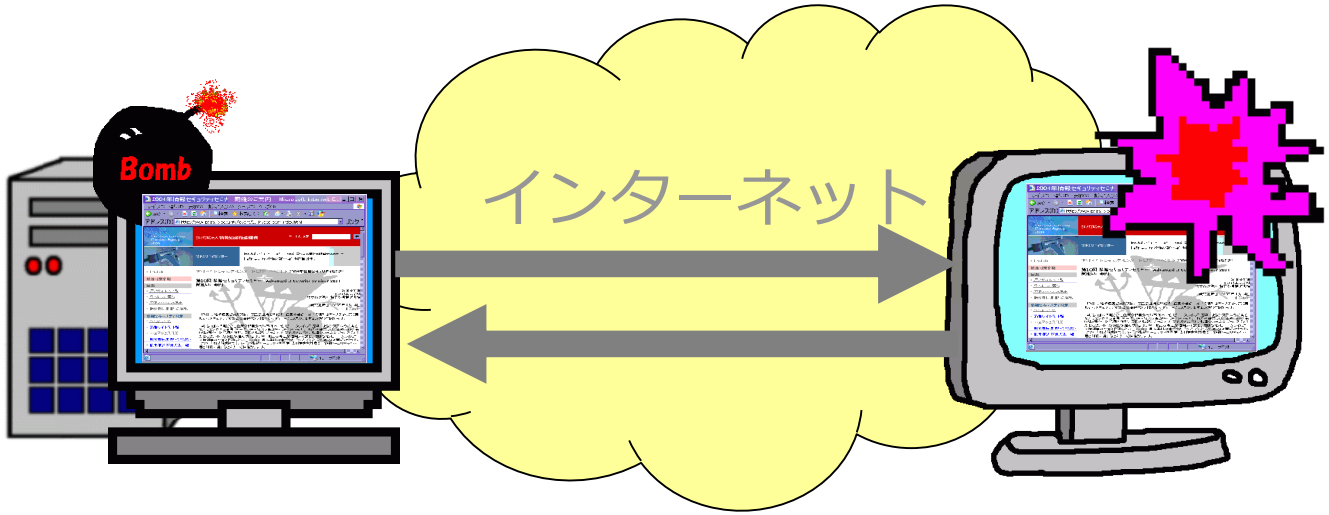
犯罪被害につながるメール注意喚起
(一般財団法人 日本サイバー犯罪対策センター公式サイト)
https://www.jc3.or.jp/topics/virusmail.html

ウェブサイトからの感染

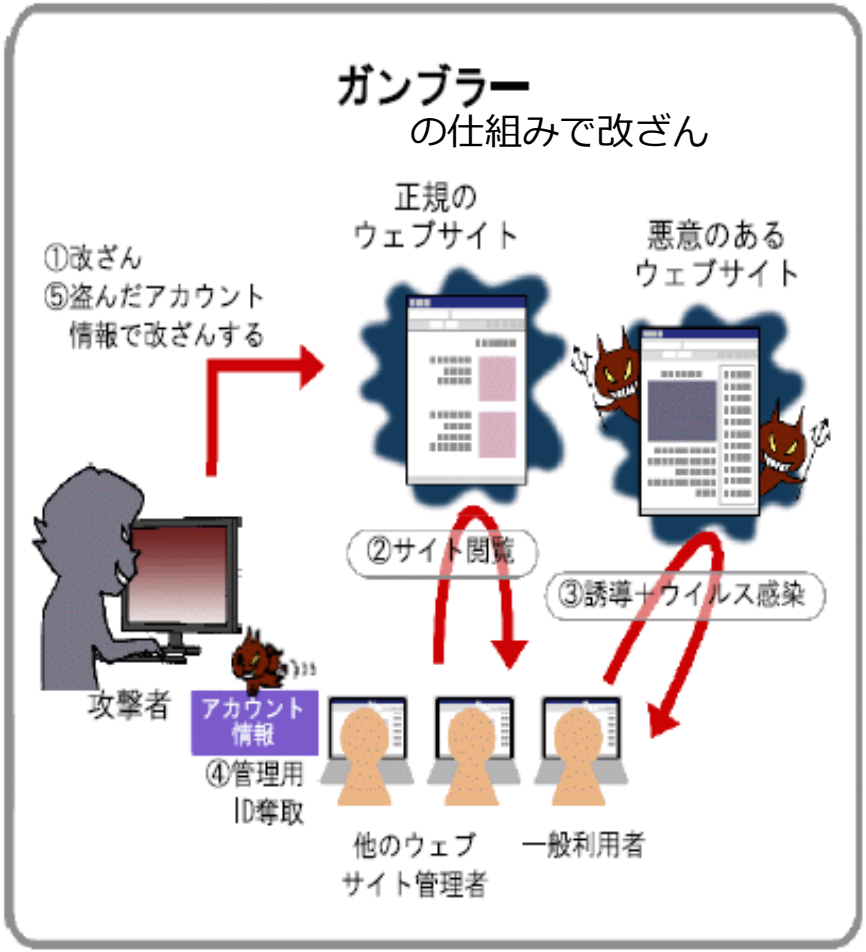
- ウイルスが仕掛けられたウェブサイトを閲覧することにより感染

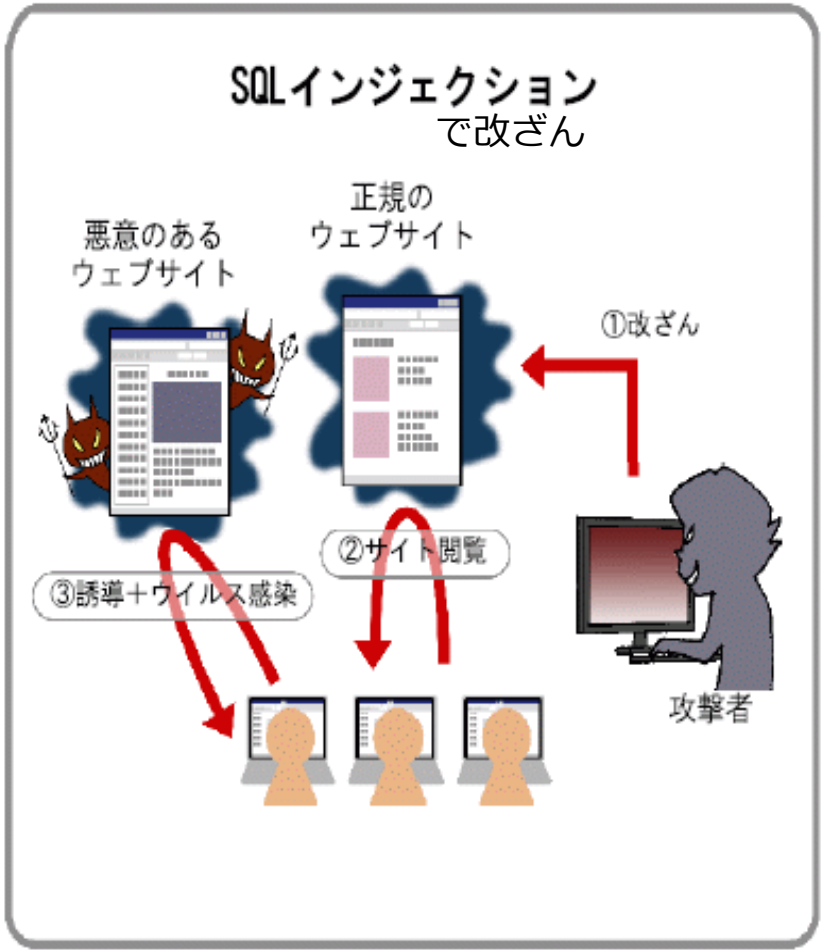
  迷惑メール　インスタントメッセンジャー　SNS
  ブログサイト　アダルトサイト

  などに記載された不正なリンクから悪意のあるウェブサイトに誘導され感染



よく見るサイトが改ざんされて…





ガンブラー:ウェブ経由でパソコンにウイルスを感染させようとする攻撃手法
SQLインジェクション:データベースを不正に操作して重要な情報を盗んだりウェブサイトを改ざんする攻撃手法

ウェブサイトからの感染に対する予防

- ☑ ウイルス対策ソフトの正しい運用
- ☑ OSやソフトウェアの脆弱性の解消
- ☑ ブラウザのセキュリティ設定を強化する
  (例えば必要時以外のスクリプトの抑止、不要なアドオンの抑止など)
- ☑ ウェブフィルタリングの利用

悪意あるサイトにアクセスしないために…

- ☑ 不審なサイトにアクセスしないように社員教育
- ☑ 不審なサイトに関する情報共有
- ☑ スマホアプリは公式マーケットなど信頼できるサイトからインストール

ウェブサイトの実在性確認

- ウェブサイトが本物のウェブサイトであることを確認する方法に「SSLサーバ証明書」があります。
- 「SSLサーバ証明書」とは、ウェブサイトの身元を明示するためのもので、ブラウザの鍵マークをクリックすることでサイトの運営組織を確認することができます。
- 不審なサイトを見分ける方法のひとつとして有効ですが、誰でも取得できる「SSLサーバ証明書」を使った詐欺サイトもあるので証明書の種類も確認するようにしましょう。

SSL/TLSサーバ証明書とは
一般財団法人日本情報経済社会推進協会 公式サイトから
https://itc.jipdec.or.jp/ssl/ssl_cert.html

USBメモリなどからの感染

- USBメモリを挿すと感染するケースもあり、OSの「自動再生」機能はオフにします。
- USBメモリに不正ファイルを仕掛け、利用者を騙して開かせ、ウイルスに感染させるケースも多く、USBメモリの取扱いには十分な注意が必要です。
- 他にも、SDカードなど各種記憶媒体やウェブサイトからダウンロードしたファイルに、ウイルスが仕掛けられている場合もあります。
- ウイルスの入ったスマホをケーブルでパソコンに接続して感染することもあり、外部機器の扱いには注意が必要です。

USBメモリなどからの感染に対する予防

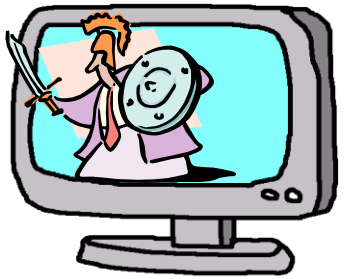
- ☑ ウイルス対策ソフトの正しい運用
- ☑ OSやソフトウェアの脆弱性の解消
- ☑ 私物など業務外で使用するUSBメモリなどの機器を業務で使用しない
- ☑ USBメモリなどを他者に貸したり借りたりしない
- ☑ 不用意に出所不明なファイルを開かない
- ☑ 企業・組織のルールに従う

…さらに注意するなら

- ☑ 感染しても影響がない環境で事前に接続テストをする…
- ☑ 紛失など情報漏えい対策も忘れずに…

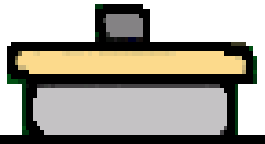
ウイルス対策まとめ

- ウイルス対策ソフトの利用
- ソフトウェア・アプリの脆弱性解消
- 利用するブラウザやメーラーなどのセキュリティ設定の強化
- 怪しいサイトからのファイルやアプリのダウンロード、不審なメールの添付ファイルやURL記載に注意
- 不用意にUSBメモリなどの外部機器と接続しない



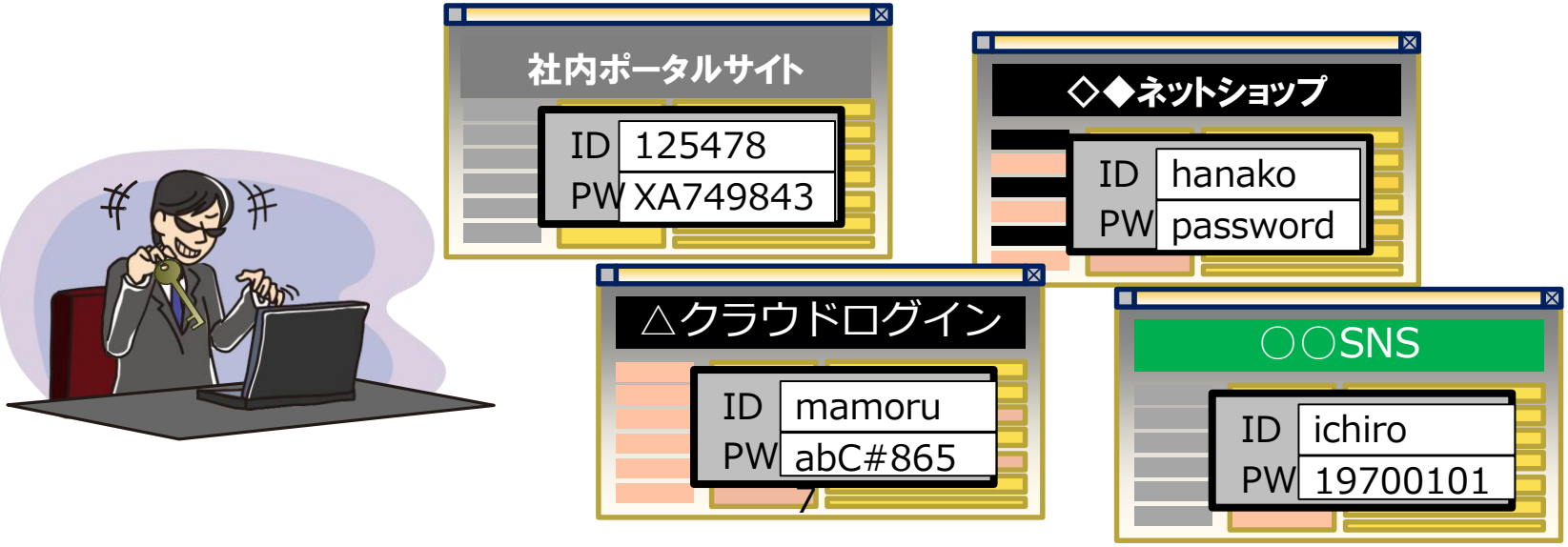
パスワード管理

3 パスワードを強化しよう！



いたるところでパスワードが必要…

- パソコンやスマホにログインする際だけでなく、インターネットサービス利用などで多くのパスワードが必要です。
- パスワードは情報システムやインターネットの扉を開く鍵に相当し、盗用されると不正にログインされ、情報漏えいや金銭被害が発生するおそれがあります。

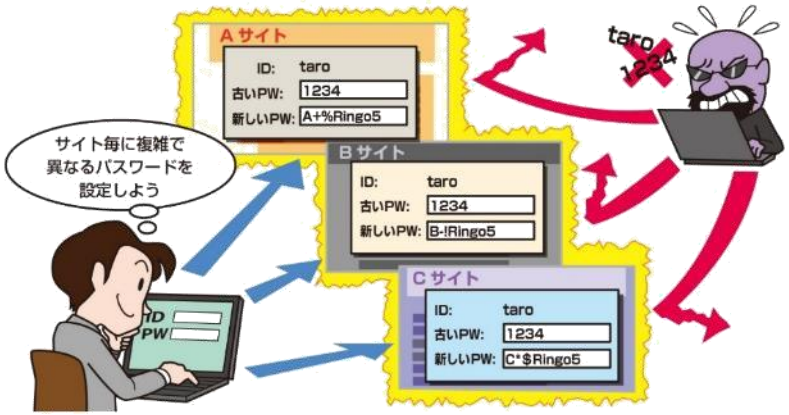


強固なパスワードを使用する

- パスワードが推測や解析されたり、ウェブサービスから流出したＩＤ・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。
- 安易なパスワードやパスワードの使い回しなどは、パスワードの悪用や不正の原因になり、大変危険です。
- パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

＜対策例＞

- パスワードは英数字記号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
- 同じＩＤ・パスワードをいろいろなウェブサービスで使い回さない



破られないために

パスワードの掟　作り方

- 他者が推測しやすい名前、愛称、電話番号、誕生日などは避け自分だけが憶えやすいものを使う
- 辞書に載っている単語、よく使われるフレーズは使わない
- 同じ文字を連ねただけ、数字だけ、アルファベットだけは避け、大文字/小文字、数字、記号を混ぜる
- 文字数(桁数)を多くして、できる限り長くする

悪用されないために
パスワードの掟　使い方

- ☑ 他者から見られる所にメモしない、保存しない
- ☑ 複数のサービスで、同じパスワードを使い回さない※
- ☑ 漏えいしたり悪用された兆候が見られたら、直ちに変更する
- ☑ サービス提供側で漏えい事故が発生したら、直ちに変更する

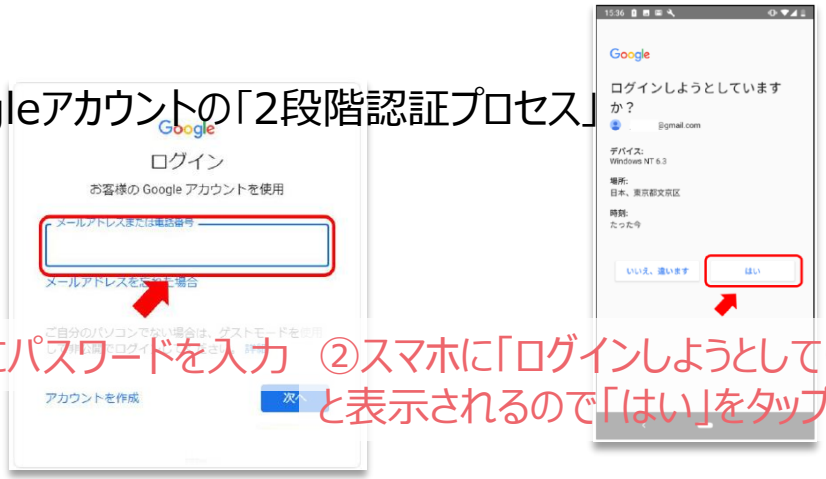
※7割以上の人がパスワードを使い回しています！！
IPA「情報セキュリティの脅威に対する意識調査」から
サービス毎に異なるパスワードを設定している割合
2015年　27.3%
2014年　29.2%
2013年　27.2%
2012年　22.2%

安心相談窓口だより
不正ログイン被害の原因となるパスワードの使い回しはNG
～ちょっとした工夫でパスワードの使い回しを回避～
https://www.ipa.go.jp/security/anshin/mgdayori20160803.html

多要素認証を活用する

- クラウドなどインターネットを通じたサービスの多くが、パスワードによる認証を採用しています。
- インターネットサービスは外部からの攻撃を受けやすく、パスワードが窃取されると不正にログインされる危険性が極めて高くなります。
- 不正ログイン対策として複数の要素(記憶、所持、生体情報)を用いた「多要素認証」や同じ要素の認証を多段で実施する「多段階認証」などの認証方式を提供しているサービスがあります。

例)Googleアカウントの「2段階認証プロセス」



①パソコンにパスワードを入力　②スマホに「ログインしようとしていますか?」と表示されるので「はい」をタップ

安全なパスワードとは？

IPA　チョコっとプラスパスワードから

https://www.ipa.go.jp/chocotto/pw.html

- ✔ 最低でも8文字以上の文字数で構成されている。
- ✔ パスワードの中に数字や、「@」、「%」、「"」などの記号も混ぜている。
- ✔ パスワード内のアルファベットに大文字と小文字の両方を入れている。
- ✔ サービスごとに違うパスワードを設定している。

例1 覚えやすいフレーズから パスワードをつくる

「チョコっと プラス パスワード 2015!」

↓

Chocotto + password 2015!

↓

Cho+pw15! 👍

例2 ことば遊びで パスワードをつくる

Chocolate

↓

Chokore-to

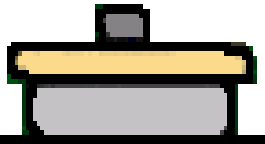
↓

Choko0-10? 👍

※こちらのパスワードは公開用のサンプルですので、使用しないでください。

機器の設定

4 共有設定を見直そう！

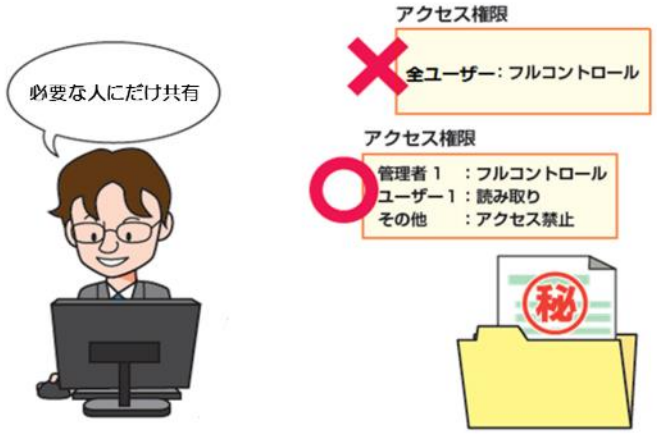


共有設定を見直す

- データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため、無関係な人に情報を覗き見られるトラブルが増えています。
- クラウドサービスやネットワーク接続機器は
  必要な人だけが共有するように設定しましょう。

＜対策例＞

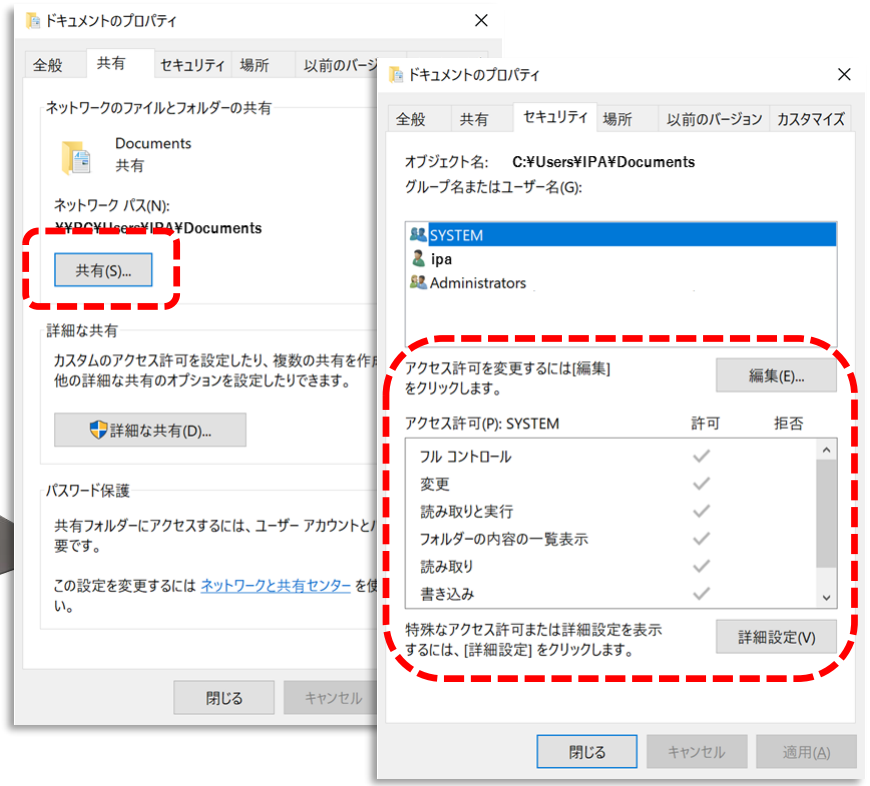
- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する



例えばこんな対策…

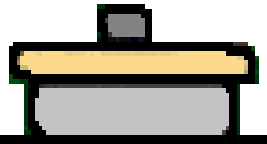
- クラウドサービスの共有範囲を限定する。
- ネットワークに接続するオフィス機器の共有範囲やアクセス権を設定する。
- 従業員の異動や退職時には設定の変更(削除)漏れがないように注意する。

Windows10の設定画面



情報収集

5 脅威や攻撃の手口を知ろう！



脅威や攻撃の手口を知り対策に活かす

- 取引先や関係者と偽ってウイルス付のメールを送ってくる手口
- 正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする手口
- 会費無料と謳っておきながら突然高額な請求画面を表示する手口

脅威や攻撃の手口を知って対策をとりましょう！

＜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

組織的な情報収集を

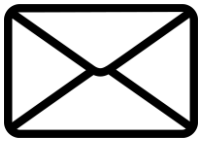
- IPAやセキュリティ関連機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知ることで、罠に気付き、被害を防止することができます。
- 情報収集の担当者を決め、メールや掲示板で社内に注意喚起するなどの体制を作りましょう。

安心相談窓口だより
https://www.ipa.go.jp/security/anshin/mgdayoriindex.html

公開日	主な対象	タイトル
2019/10/8	一般 組織	更新：性的な映像をばらまくと恐喝し、仮想通貨で金銭を要求する迷惑メールに注意
2019/9/18	一般 組織	スマートフォンで偽のセキュリティ警告からアプリのインストールへ誘導する手口に注意
2019/3/20	一般 組織	宅配便業者をかたる偽ショートメッセージで、また新たな手口が出現

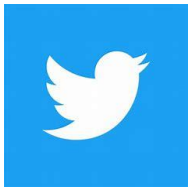
サイバーセキュリティ注意喚起サービス「icat for JSON」
https://www.ipa.go.jp/security/vuln/icat.html

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/about/mail/



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。

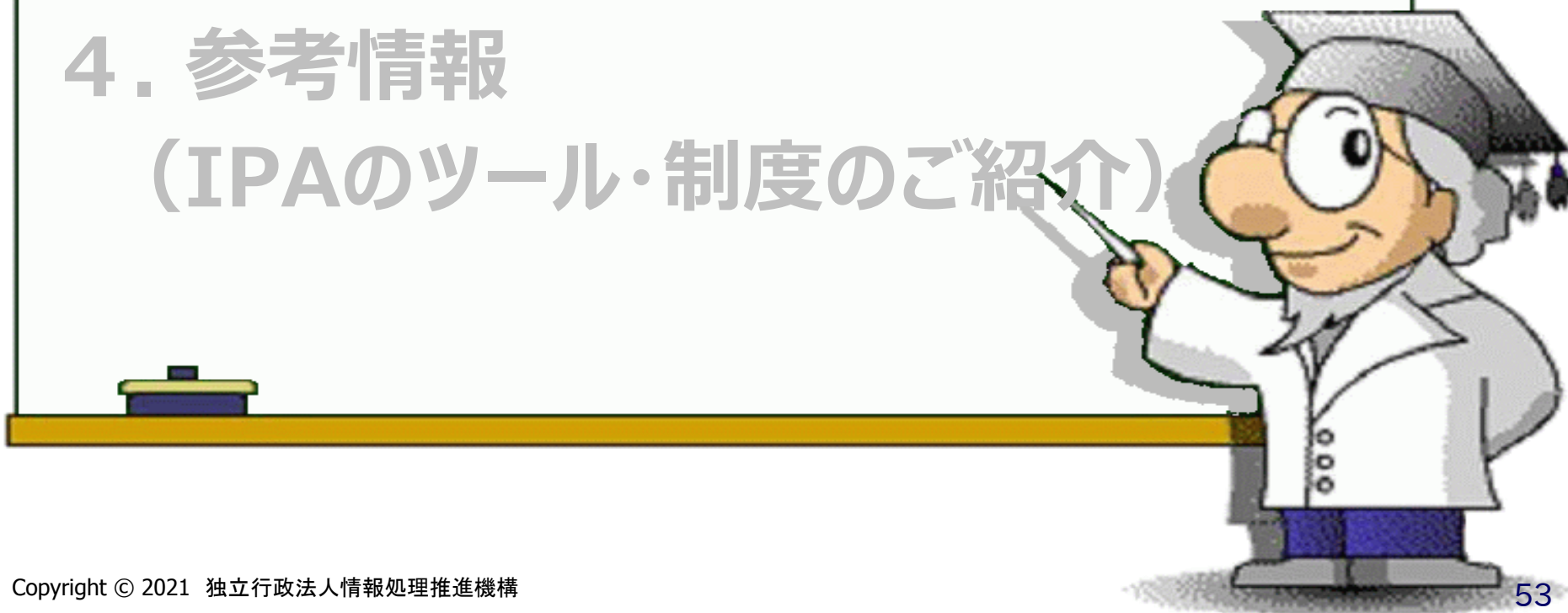
Facebook公式アカウント https://www.facebook.com/ipaprjp/

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/

目次

1．サイバーセキュリティの状況
2．中小企業が取組むセキュリティ対策
3．SECURITY ACTIONのご紹介
4．参考情報
（IPAのツール･制度のご紹介）



情報セキュリティ対策のよくある質問

- どこからどう始めたら良いか？
  - まずは、基本的なセキュリティ対策から
  - 組織の実態に合わせ段階的に
- 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

SECURITY ACTION の取組みから始める

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　IT導入補助金2021サイト より

https://www.it-hojo.jp/

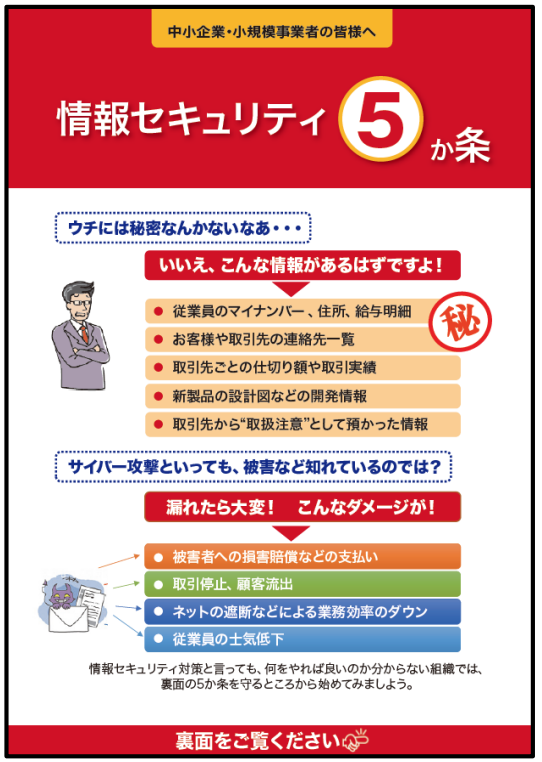
公的補助

一つ星

SECURITY ACTION 一つ星

「情報セキュリティ５か条」に取組むことを宣言

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！



二つ星

SECURITY ACTION 二つ星

1. 「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する
2. 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

＋

情報セキュリティ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

自社診断のための25項目

IPA

- 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、持ち出し、廃棄、ウェブ利用など

組織としての対策 7項目

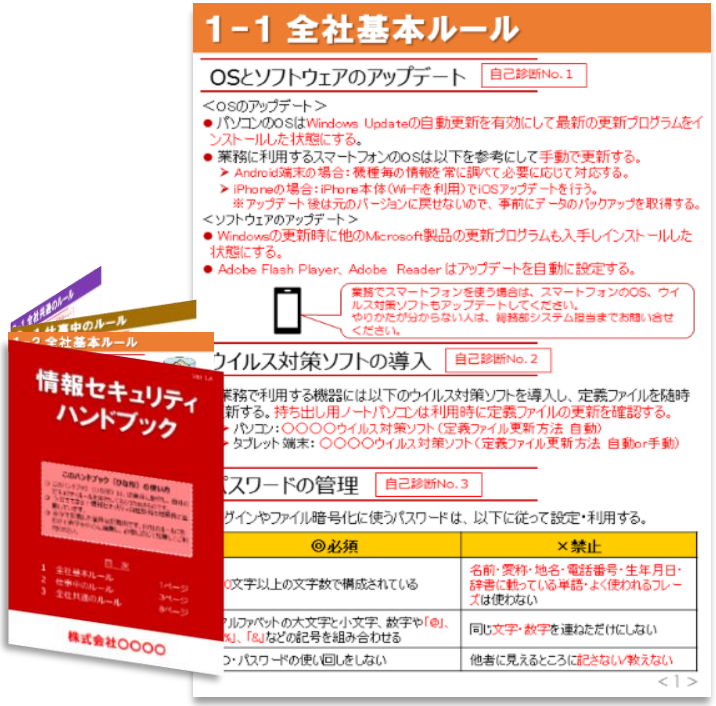
守秘義務、インターネット利用、ルール化など

	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
	14	離席時にパソコン画面の覗
	15	関係者以外の事務所への立
	16	退社時にノートパソコンや
	17	事務所が無人になる時の施
	18	重要情報が記載された書類にしていますか？
組織としての対策	19	従業員に守秘義務を理解し守らせていますか？
	20	従業員にセキュリティに関
	21	個人所有の情報機器を業務
	22	重要情報の授受を伴う取引
	23	クラウドサービスやウェブ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？

チェック			
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	2	0	-1
4	2	0	-1
4	2	0	-1
4	2	0	-1
4			

対策の決定と周知

- 自社診断で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



情報セキュリティ対策の更なる強化

中小企業の情報セキュリティ対策ガイドライン

入門から本格的対策までこれ一冊！

- 情報を安全に管理するための具体的な手順
- 企業が認識すべき「3原則」
- 企業がやらなければならない「重要7項目の取組」
- ウェブサイトの運用・クラウドサービス安全利用の手引き

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

経営者は何をやらなければならないのか

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

・経営者は情報セキュリティ対策の重要性を認識する　　・自らリーダーシップを発揮して対策の実施を主導する

⇒ 要するに、社長自ら、「我が社は情報セキュリティ対策を実施します！」と社内外に表明すること。

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する

⇒ 要するに、情報セキュリティ対策について、自社だけでなく、仕事をお願いしている相手先もよく確認しましょう！ということ。

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常日頃より関係者に伝えておく
　⇒ 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、説明責任を果たすことができ、信頼関係を維持することが可能

⇒ 要するに、なにか事件が起きた時、慌てずしっかり「社長としての説明責任」が果たせるように、日頃から状況把握しておきましょう！ということ。

経営者は何をやらなければならないのか

実行すべき「重要7項目の取組」

IPA

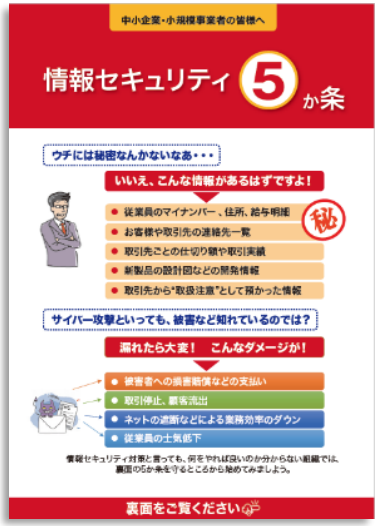
- 経営者は以下の７項目を自ら実践する、あるいは
- 情報セキュリティ対策の責任者・担当者に指示し、確実に実行する

取組１	情報セキュリティに関する組織全体の対応方針を定める
取組２	情報セキュリティ対策のための予算や人材などを確保する
取組３	必要と考えられる対策を検討させて実行を指示する
取組４	情報セキュリティ対策に関する適宜の見直しを指示する
取組５	緊急時の対応や復旧のための体制を整備する
取組６	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組７	情報セキュリティに関する最新動向を収集する

具体的な進め方

・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

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
- 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

より強固にするため方策

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」を実行
- 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/

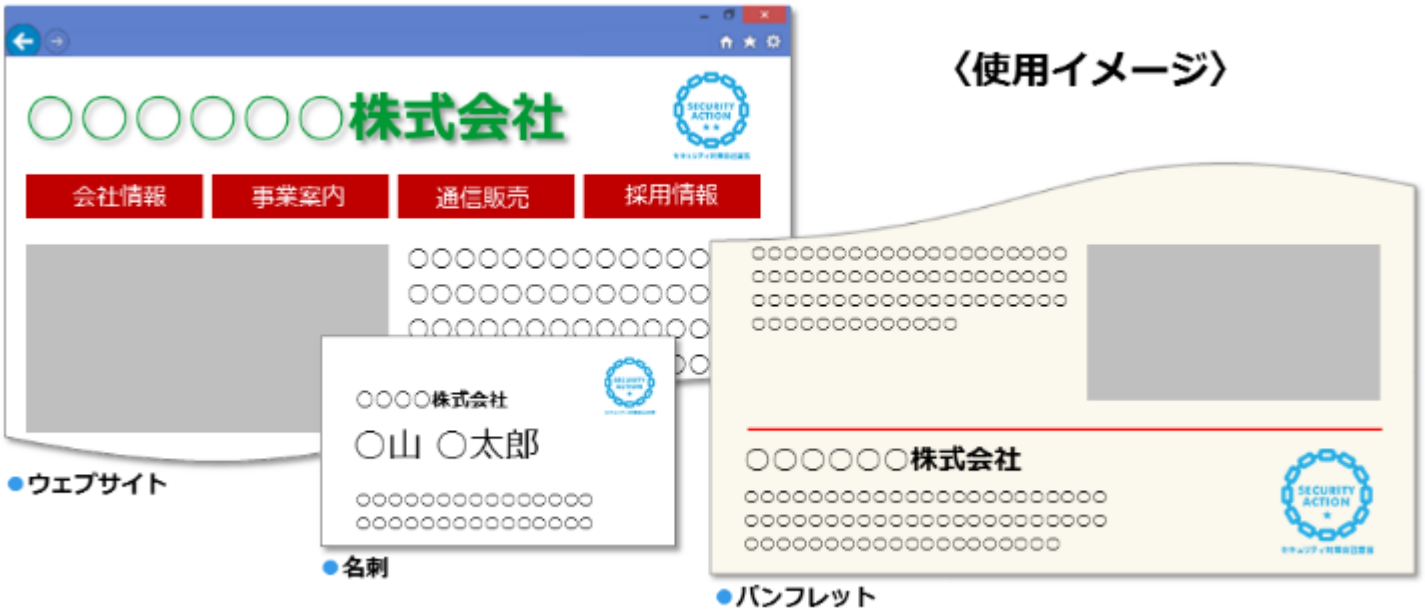
2)自己宣言する

- 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/entry/

ロゴマークの使用方法

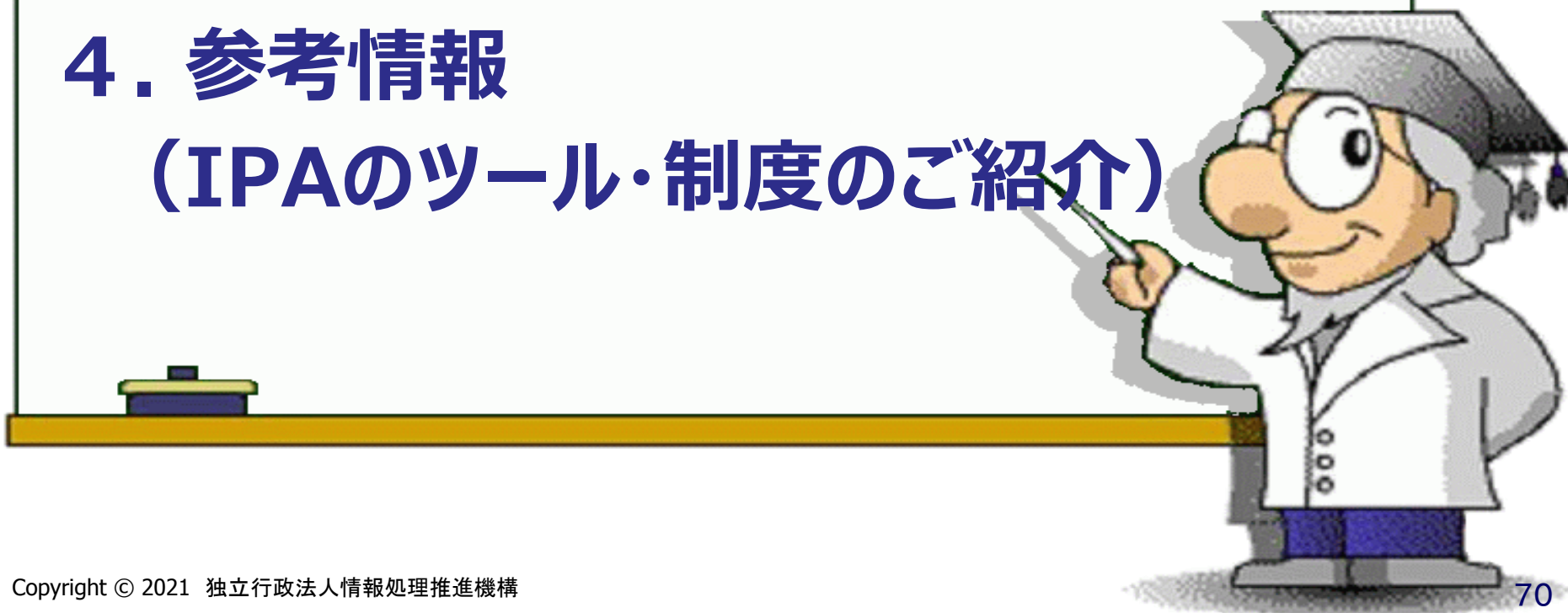
- ロゴマークは、ポスター・パンフレット・名刺・封筒・ウェブサイト等に無償で使用でき、情報セキュリティ対策の取り組みをアピールします。



〈使用イメージ〉

目次

1．サイバーセキュリティの状況
2．中小企業が取組むセキュリティ対策
3．SECURITY ACTIONのご紹介
4．参考情報
（IPAのツール･制度のご紹介）



【参考】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/keihatsu/sme/otasuketai/index.html

- 中小企業向け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）**
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**

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

・ワンパッケージのサービスとして登録

IPA

・マーク提供
・ブランド管理・普及促進

サイバーセキュリティ お助け隊

マーク付きの民間サービス

中小企業

＜サイバーセキュリティお助け隊サービス＞

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

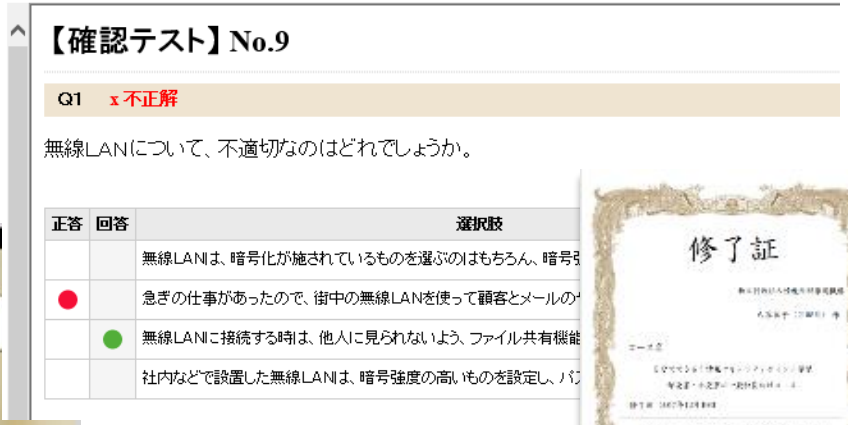
- 5分でできる！自社診断＆ポイント学習
- セキュリティプレゼンター支援
- SECURITY ACTION 自己宣言者サイト

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29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。主な映像はDVD-ROMでも提供中。

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。
(詳しい説明へ)

約10分

New 2021/03/10

ハケンが解決！ 情報セキュリティ規程作成のポイント
中小企業のセキュリティ担当者に向けて社内の情報セキュリティ規程の作成から運用までの手順をドラマ形式で説明します。
(詳しい説明へ)

約12分

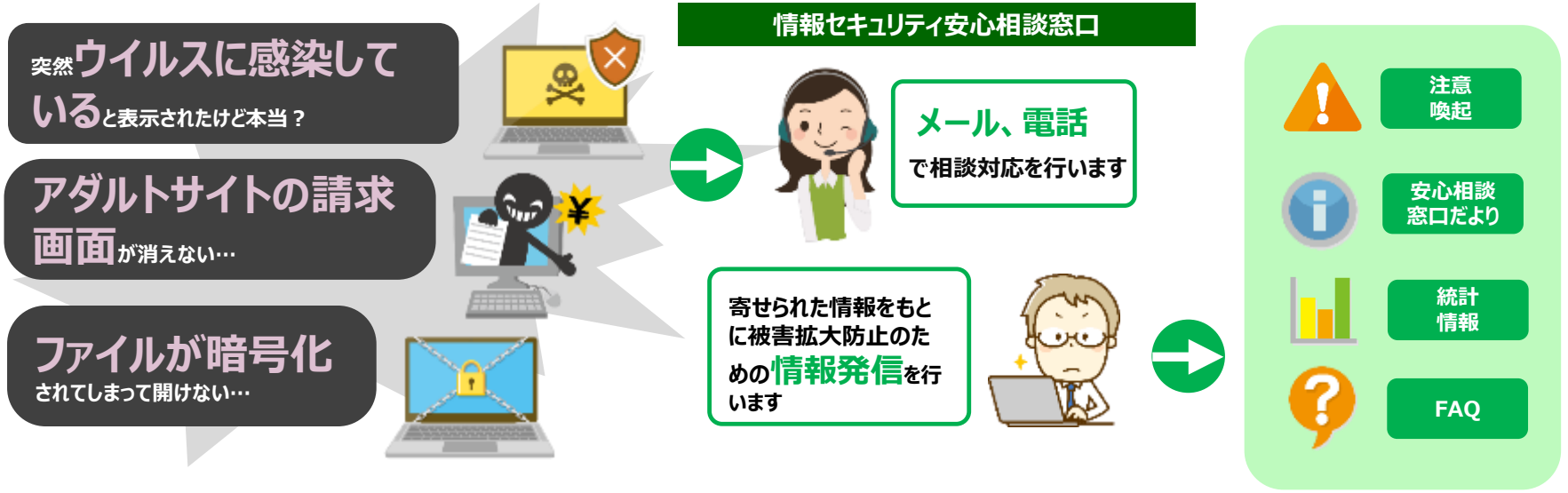
New 2021/

IPA　映像　検索

情報セキュリティ安心相談窓口

https://www.ipa.go.jp/security/anshin/index.html

IPAでは、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を開設しています。寄せられる相談に対して、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図っています。



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。

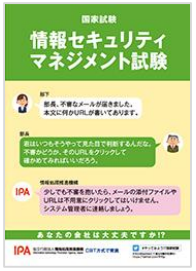
受験を特にお勧めする方

・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」

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

独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591 東京都文京区本駒込二丁目28番8号
文京グリーンコート センターオフィス
TEL 03-5978-7508　FAX 03-5978-7546
電子メール　**isec-pr-nw@ipa.go.jp**
URL　https://www.ipa.go.jp/security/

SECURITY ACTION自己宣言者サイト
https://security-shien.ipa.go.jp/security/entry/