情報セキュリティ対策研修会

中小企業向け情報セキュリティ対策セミナー

2025年12月12日　東京税理士会日本橋支部　情報システム委員会

サイバー攻撃の最新事例と防御法

IPAセキュリティプレゼンター　高山和子

氏名	高山和子
所属	あいな税理士法人　日本橋支店　代表税理士 ＆オフィスたかやま行政書士法人 ＆ (NPO)ITCちば経営応援隊
略歴	税理士、行政書士、ITコーディネータ（経済産業省推進資格）認定番号　9029592020C、弥生会計、給与認定インストラクター
参加事業	東京都IT専門家登録　東京都DX、生産性向上　IT専門家デジタルナビゲーター事業
実績	DX補助金、テレワーク補助金、IT導入補助金、ものづくり補助金申請ほかサポート　補助金関連の総件数　150件以上　ITサポート総件数100件以上

目次

１．はじめに
２．情報セキュリティ対策の必要性
３．情報セキュリティ5か条
４．中小企業における対策のポイント
５．SECURITY ACTION制度解説
６．サイバーセキュリティお助け隊サービス制度
７．資料とビデオの案内

1．はじめに

情報セキュリティ10大脅威 2025

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い
1	ランサム攻撃による被害	2016年	10年連続10回目
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目
4	内部不正による情報漏えい等	2016年	10年連続10回目
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目
9	ビジネスメール詐欺	2018年	8年連続8回目
10	不注意による情報漏えい等	2016年	7年連続8回目

IPA情報セキュリティ10脅威2025参照

情報セキュリティ10大脅威2025

情報セキュリティ10大脅威2025　初心者用ビデオ　7分

https://www.youtube.com/watch?v=_sstT8IQFkA

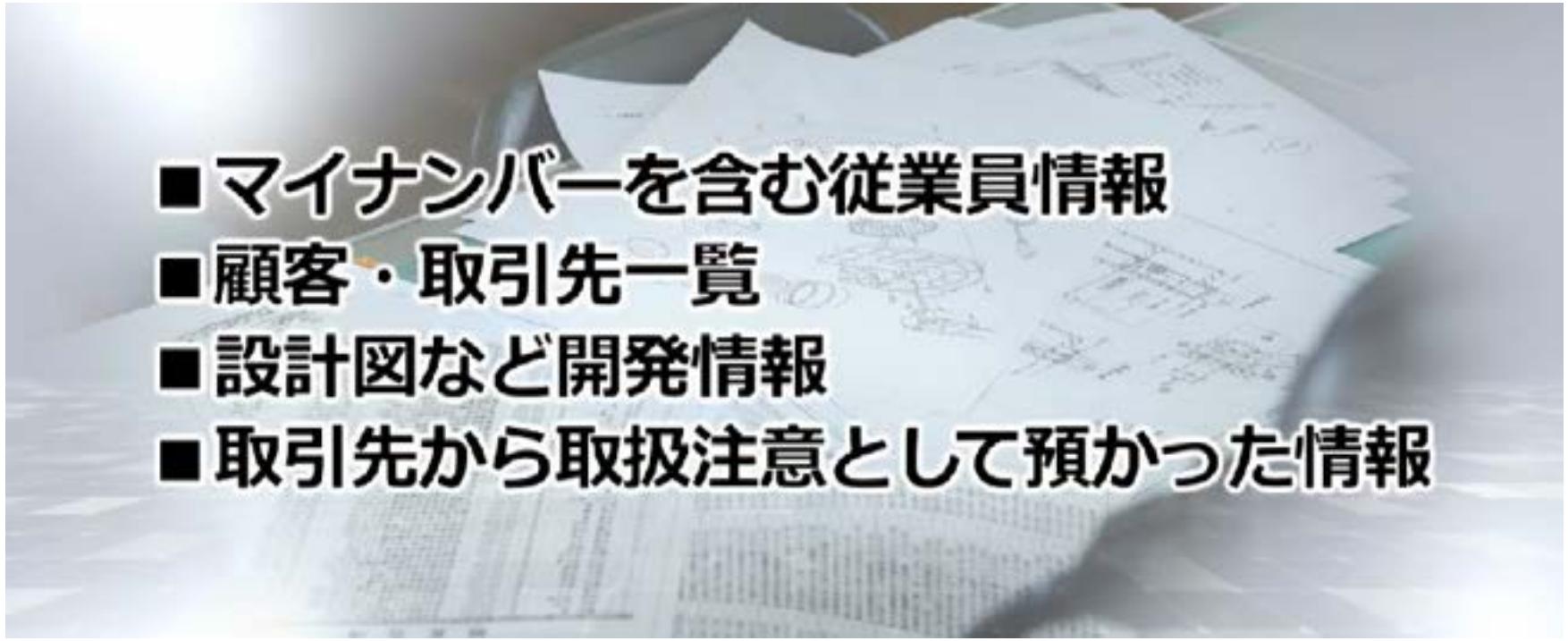
相談窓口一覧　個人　11分03秒　組織　11分08秒

今年もIPAより「情報セキュリティ10大脅威 2025」が公表されました。

資料に基づき、内容を「できるだけそのまま」ご紹介したいと思います。 詳細は下記のURLをご参照ください。 https://www.ipa.go.jp/security/10threats/10threats2025.html　情報セキュリティ10大脅威 2025 (PDFファイルサイズ：4.0MB、ページ数：108P)

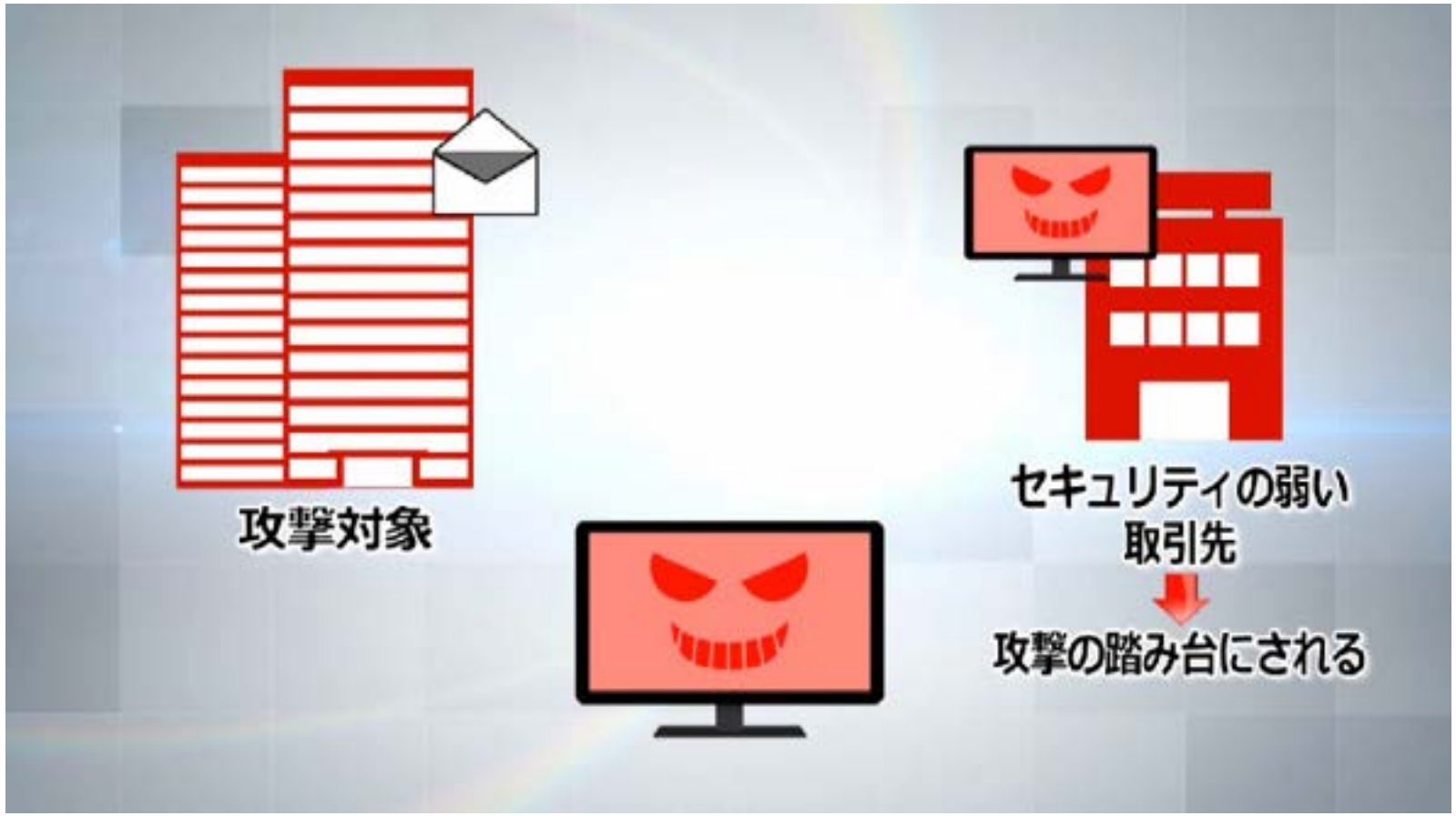
２．情報セキュリティ対策の必要性

- あなたの会社からこれらの情報が外部に漏れたらどうなるか考えてみましょう



２．情報セキュリティ対策の必要性

- 標的とする企業を攻撃するために、セキュリティの弱い企業を攻撃の踏み台にする



２．情報セキュリティ対策の必要性

- 情報セキュリティ対策を怠ると・・・
  - 金銭の損失
    - 損害賠償請求、インターネットバンキングの不正送金、クレジットカードの不正利用
  - 顧客の喪失
    - 顧客離れ、取引停止、社会的評価の低下
  - 業務の喪失サーバーの停止、インターネット接続の遮断、社内業務の停滞
  - 従業員への影響
    - 内部不正、モラル低下

今、そこにある脅威～組織を狙うランサムウェア攻撃～ ビデオ15分（３－２－１ルール説明あり）

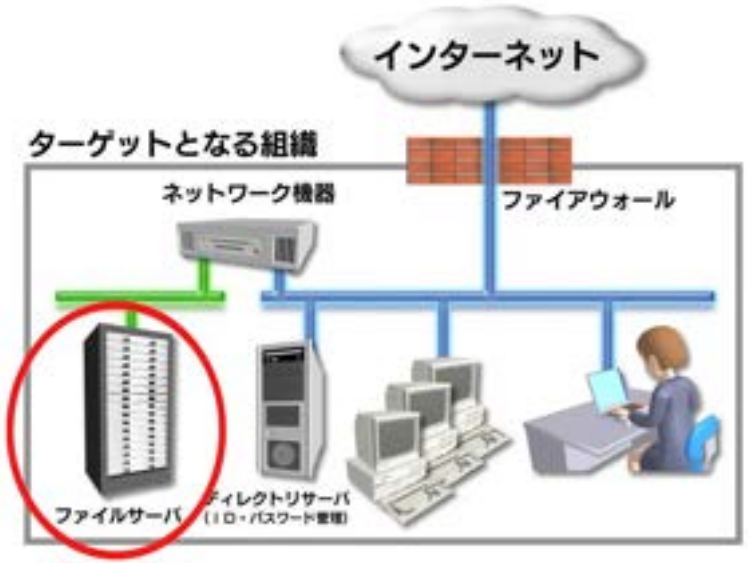
https://www.youtube.com/watch?v=TWqJ5P8oaUM

２．情報セキュリティ対策の必要性

ランサムウエアの紹介、侵入のビデオ　侵入経路ビデオご覧ください

デモで知る！ 標的型攻撃によるパソコン乗っ取りの脅威と対策(約7分)

https://www.youtube.com/watch?v=dSWrKh5FHKA

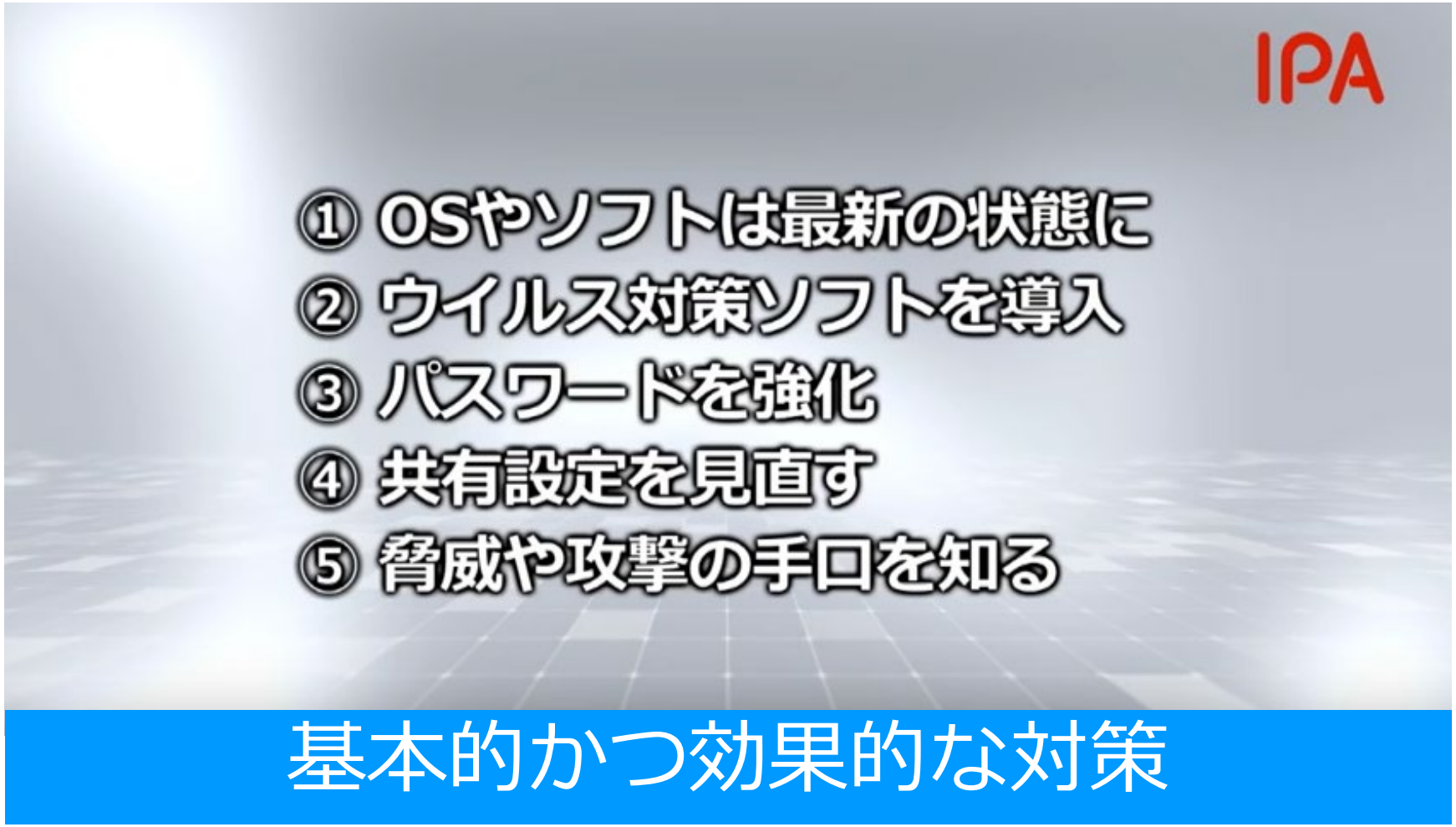


IPA

２．情報セキュリティ対策の必要性

- **2025年の事例/傾向**
  - **ランサムウェア感染によるサービス提供停止**
    - 2025年9月29日、Asahi Group Holdings（アサヒグループ）飲料・食品（ビール等）国内の複数工場・物流／出荷・受注システムがサイバー攻撃を受け国内６工場で生産停止。グループが、ランサムウェアの関与を示唆する攻撃として、Qilin が27ギガバイト・9,300件超の内部ファイルを盗んだと主張。
    - 2025年10月20日、ASKUL Corporation（アスクル）小売／物流・ECサービス物流・ECサービスを提供するアスクルがランサムウェア攻撃を受け、オンライン受注・出荷停止。RansomHouseの攻撃で顧客データの流出懸念もあり、連携する小売店も影響を受けました。

３．情報セキュリティ５か条



3．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

- OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。お使いの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/iOSの場合)
- OSバージョンアップ、セキュリティアップデート(Android の場合)
- 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ウイルスが増えています。
- 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なるようにしましょう。

＜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製品(ファイアウォールや脆弱性対策など複数のセキュリティ機能を搭載したもの)を導入する

③ パスワードを強化

- パスワードが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えています。
  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

④　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機器は必要な人にのみ共有されるよう設定しましょう。

＜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ってきたり、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巧妙な手口が増えています。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

組織的な対策を進めるために

- 「5分でできる！情報セキュリティ自社診断」を使って、情報セキュリティ対策状況を把握してみましょう。
- https://www.ipa.go.jp/security/guide/sme/5minutes.html
- 診断項目
  - ウイルス対策
  - パスワード管理
  - 電子メールのルール
  - Web利用のルール
  - 保管のルール
  - 持ち出しのルール
  - 取引先管理
  - 従業員教育…など

４．中小企業における対策のポイント

- 経営者のリーダーシップと従業員全員の協力が不可欠
  - 経営者と従業員、お互いの顔が見える組織なら柔軟・迅速に対応可能
- 継続的な改善を行なうことで対策強化に努めましょう！
  - すぐにできることから始めて、段階的にステップアップ

SECURITY ACTION 制度概要

- 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）

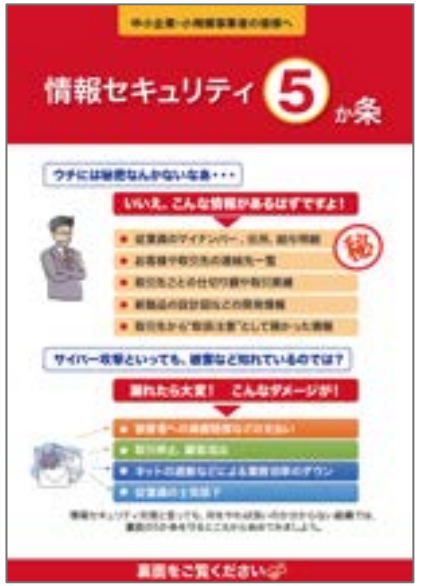
「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、「情報セキュリティ基本方針」を定め、外部に公開したことを宣言

  - SECURITY ACTION 自己宣言数40万件を突破！（2025年4月）

一つ星の取組み目標

- 「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



二つ星の取組み目標

- 「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

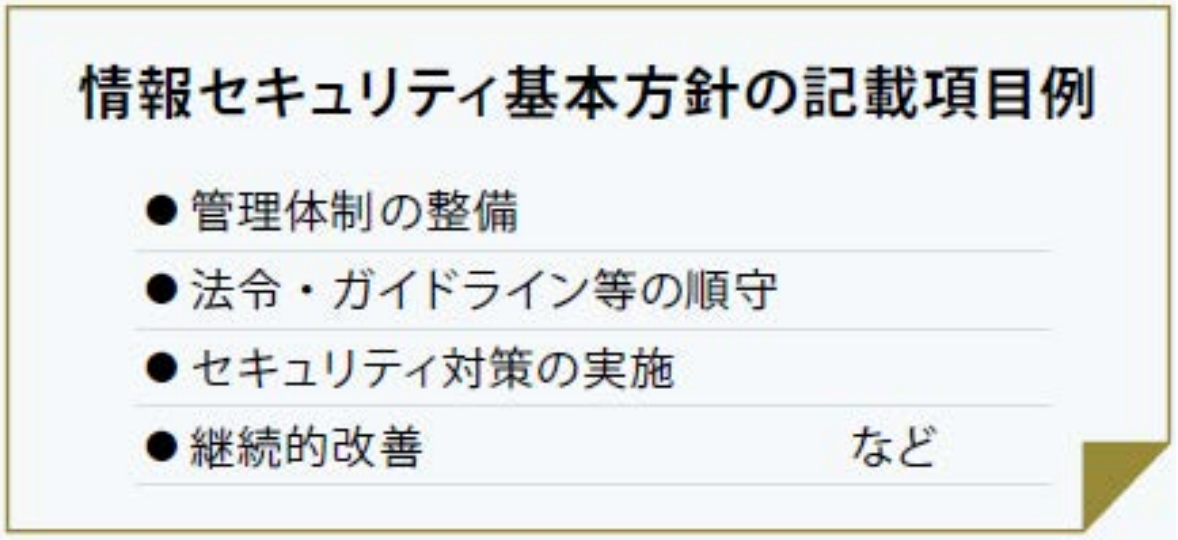
＋

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

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



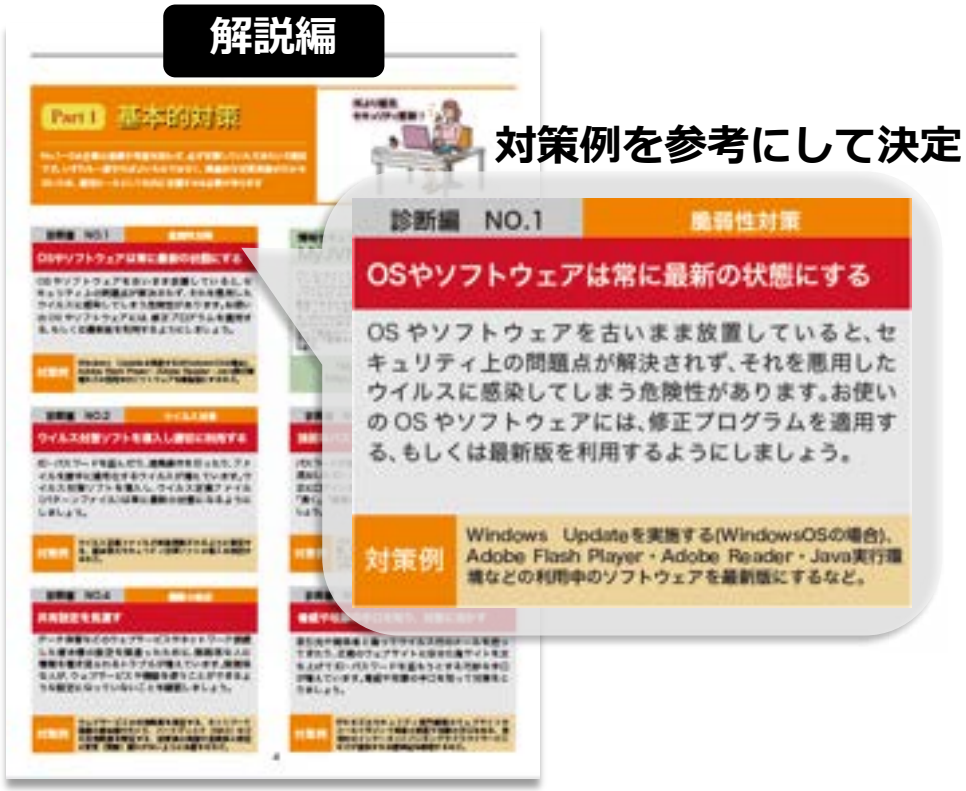
②実施状況の把握

- 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項目の設問に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できる
  - 解説編の対策例を参考に、社内ルールを作成することができる
  - 付録の情報セキュリティハンドブックを活用すると従業員に対する社内ルールの周知が簡単にできる

5．SECURITY ACTION制度解説（二つ星）

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



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

6．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サービス要件をワンパッケージとしてサービス基準にまとめ、これを満たすことが所定の審査機関により確認された民間サービスをIPAが**「サイバーセキュリティお助け隊サービス」**として登録・公表する制度を2021年度から開始。
- 価格要件を撤廃し、**監視機能等を拡充したサービスを登録できる「2類」制度**を2024年度に開始
- 2025年3月現在、46事業社78サービスが登録（1類と2類の合計）。

◇「サイバーセキュリティお助け隊サービス基準」(1類)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 (※)UTMやEDR等を想定
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・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）**
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**

◇2類サービスの要件

・1類（左記）の要件＋以下から1つ以上追加 ※価格要件は撤廃

拡充要素	概要
監視対象端末の増加	監視できる端末数の増加（最低50端末以上）
異常監視の仕組みや機能の追加	併用型への変更や監視範囲を追加する機能の追加
新たな提供サービスの追加	毎月実施、または定常的に利用可能な付加的サービスの追加

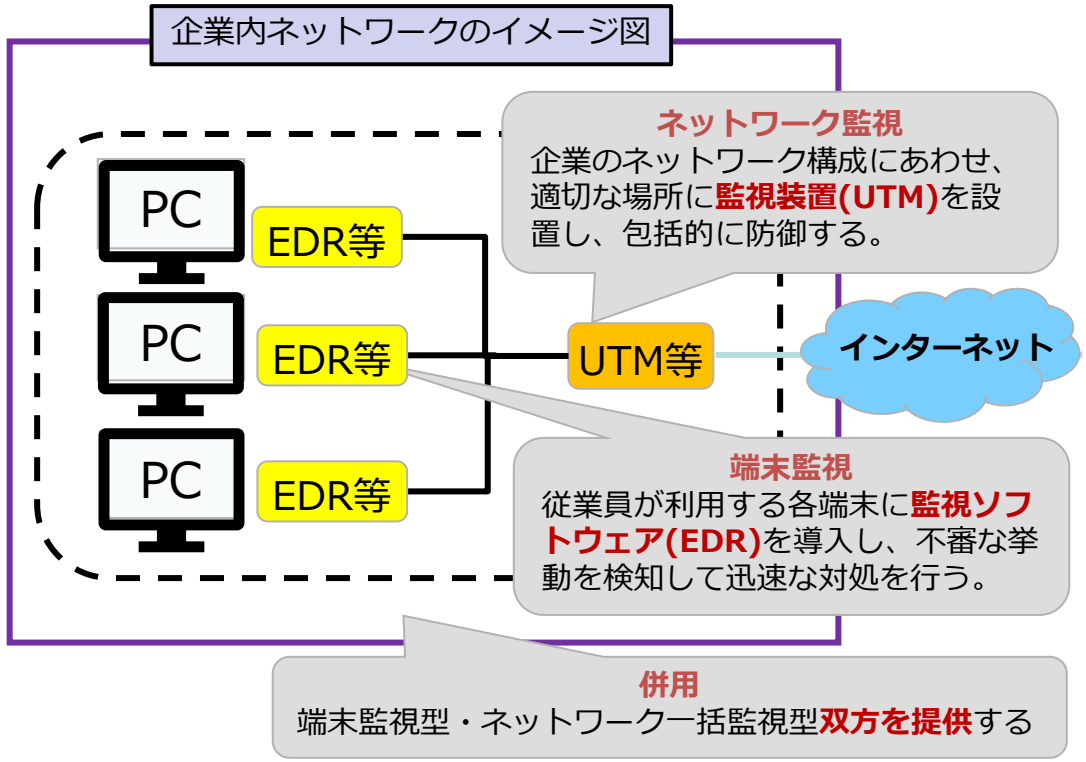
IPA ・マーク提供、ブランド管理・普及促進 → サイバーセキュリティ お助け隊 ・ワンパッケージのサービスとして提供 → 中小企業等

6．サイバーセキュリティお助け隊サービス制度

異常監視の仕組み

- 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	• ネットワーク一括監視型と端末監視型の両方を設置し、**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。	• ネットワーク一括監視型、端末監視型の**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

導入のメリット①

ワンパッケージで簡単導入

(1)相談窓口
(2)異常の監視の仕組み
(3)緊急時の対応支援
(4)中小企業でも導入・運用できる簡単さ
(5)簡易サイバー保険

企業のセキュリティ対策に必要な(1)～(5)をまとめて導入できます。

- 専用の窓口で、ユーザーからの質問にお答えします
- ネットワークや端末を24時間見守り・監視しています
- インシデント発生などの緊急時には駆付け支援いたします
- 専門知識がなくても大丈夫！
- サイバー保険付きで安心

（＊サービスによって提供内容が異なります。詳しくは各サービス内容をご確認下さい。）

導入のメリット②

中小企業が導入・維持できる価格

端末1台からでもＯＫ！

ネットワーク一括監視型の場合、サービスによって監視対象の端末数が異なります

・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

価格設定に上限があり、サービス運用コストを抑えられます。

- コストを抑えたセキュリティ対策の導入が可能
- 各企業に適した監視型（ネットワーク一括監視型・端末監視型・併用型）を選択することで、効果的な運用ができます
- サービスの維持・管理が無理なくできます

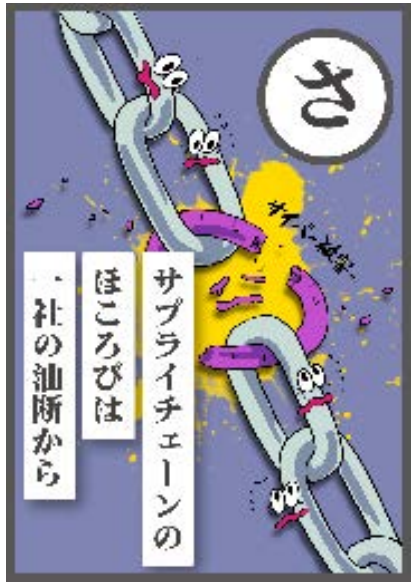
（＊導入時に、別途初期費用が必要となる場合があります。詳しくは各サービス内容をご確認下さい。）
（＊「サイバーセキュリティお助け隊サービス」以外のオプション設定の場合は価格が異なります。）

導入のメリット③

サプライチェーンの中の
中小企業を狙った攻撃が
確認されています！

安心・信頼性をアピール

**自社のセキュリティを高めるとともに、取引先や、グループ企業のセキュリティを守ることにも
つながります**



サプライチェーンにおけるセキュリティ対策にもなります。

- 取引先企業に対してアピール可能
- セキュリティ対策は、企業としての社会的信用を高めます
- 企業のBCPに貢献
- セキュリティ対策をすることで、企業の機密事項や顧客の
  個人情報を守ります

6．サイバーセキュリティお助け隊サービス制度

PRサイトのご紹介

- サイバーセキュリティお助け隊サービスのPRサイトを公開中。分かりやすく親しみやすい動画コンテンツとともに登録サービスを紹介。

https://www.ipa.go.jp/security/otasuketai-pr/

経済産業省 商務情報政策局
サイバーセキュリティ課長
武尾 伸隆 様の推奨コメントを掲載しております。

推奨コメント

2分40秒のサイバーセキュリティお助け隊サービスのプロモーション動画。

動画コンテツ

掲載内容

ご利用者
中小企業の声

お助け隊サービスを利用されている中小企業様の声を掲載しています。（今後追加予定）

IT導入補助金に関する
お知らせ

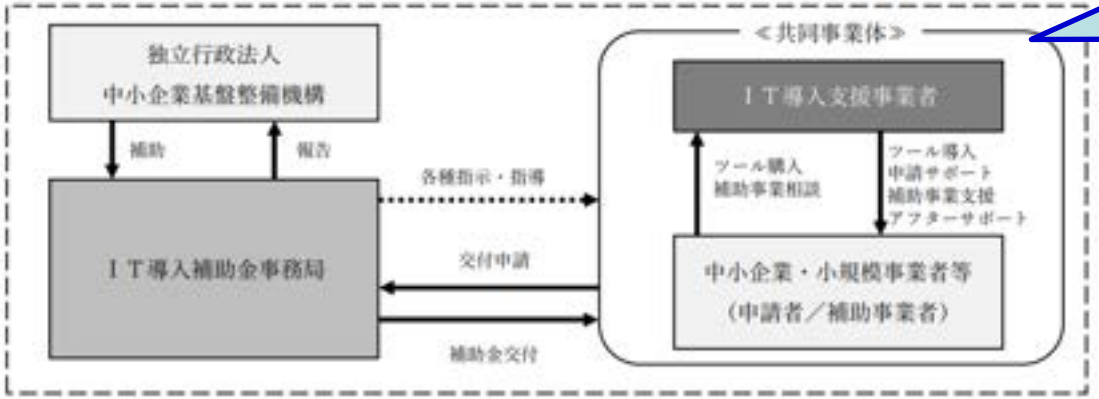
IT導入補助金のお助け隊サービスとの連携についての説明と、申請方法についてお知らせしております。

【参考】IT導入補助金2025 セキュリティ対策推進枠

- 中小企業・小規模事業者等が、**ITツール（「サイバーセキュリティお助け隊サービス」）を導入する際の経費の一部を補助**し、サイバーセキュリティ**対策の強化**を図る

- サイバーインシデントが原因で事業継続が困難となる事態の回避
- サイバー攻撃被害が供給制約・価格高騰を潜在的に引き起こすリスク、中小企業・小規模事業者等の生産性向上を阻害するリスクの低減

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/

7.資料とビデオ案内

https://www.ipa.go.jp/security/guide/sme/about.html

７.資料とビデオ案内

そのメール本当に信用してもいいんですか？ ～標的型サイバー攻撃メールの手口と対策～　９分 （メール訓練　おすすめ）

https://www.youtube.com/watch?v=5K9U0-ASQM8&t=18s

今、そこにある脅威～組織を狙うランサムウェア攻撃～　15分

https://www.youtube.com/watch?v=TWqJ5P8oaUM&t=815s

今、そこにある脅威～内部不正による情報流出のリスク～NEW　17分

https://www.youtube.com/watch?v=VDAYBeA1TTc

What’s BEC？～ビジネスメール詐欺 手口と対策 ～【日本語字幕版】

12分

https://www.youtube.com/watch?v=6DKJEG3woRU

映像コンテンツ一覧

https://www.ipa.go.jp/security/videos/list.html#keihatsu

この電子版は、社内で研修用に使用してください。

リンクをクリックすることでビデオを視聴できます。

ご清聴ありがとうございました

制度・支援策のお問い合わせ先
IPAセキュリティセンター　ISEC-PR-NW@IPA.GO.JP