

医療法人社団相和会

「職場の健康管理担当者研修会」

情報セキュリティの脅威と対策の進め方

2024年10月4日

情報処理安全確保支援士

岩本 真人

本日の内容

1. IPA 情報セキュリティ10大脅威

- ランサムウェア攻撃、サプライチェーン攻撃、内部不正
- 個人を狙うネット詐欺

2. 情報セキュリティのリスクと対策

- 情報セキュリティの目的
- 情報セキュリティとリスク
- 情報セキュリティ対策のアプローチ

3. 情報セキュリティ対策の進め方

- (独) 情報処理推進機構 (IPA) による支援施策
 - 中小企業の情報セキュリティ対策ガイドライン
- その他の支援施策、支援者等

※ 本資料は、独立行政法人情報処理推進機構 (IPA) の各種資料からの引用を含んでいます。それらの引用箇所の著作権は独立行政法人情報処理推進機構に帰属します。

1. IPA 情報セキュリティ10大脅威

組織編

- 1位 ランサムウェア攻撃
- 2位 サプライチェーン攻撃
- 3位 内部不正
- 4位～10位

個人編

- 個人を狙うインターネットネット詐欺

「情報セキュリティ10大脅威」とは？

- 2006年からIPAが毎年発行している資料
- 「10大脅威選考会」の投票により情報システムを取り巻く脅威をランク付け
- 脅威の概要、被害事例、対策方法等を解説



<https://www.ipa.go.jp/security/10threats/10threats2024.html>

- 解説書
- 簡易説明資料（スライド形式）
 - 組織編
 - 組織編（英語版）
 - 個人編
 - 個人編（一般利用者向け）
- セキュリティ対策の基本と共通対策
- 知っておきたい用語や仕組み

IPA 情報セキュリティ10大脅威 2024

順位	「組織」向け	昨年順位
1位	ランサムウェアによる被害	1
2位	サプライチェーンの弱点を悪用した攻撃	2
3位	内部不正による情報漏えい等の被害	4
4位	標的型攻撃による機密情報の窃取	3
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6
6位	不注意による情報漏えい等の被害	9
7位	脆弱性対策情報の公開に伴う悪用増加	8
8位	ビジネスメール詐欺による金銭被害	7
9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	5
10位	犯罪のビジネス化（アンダーグラウンドサービス）	10

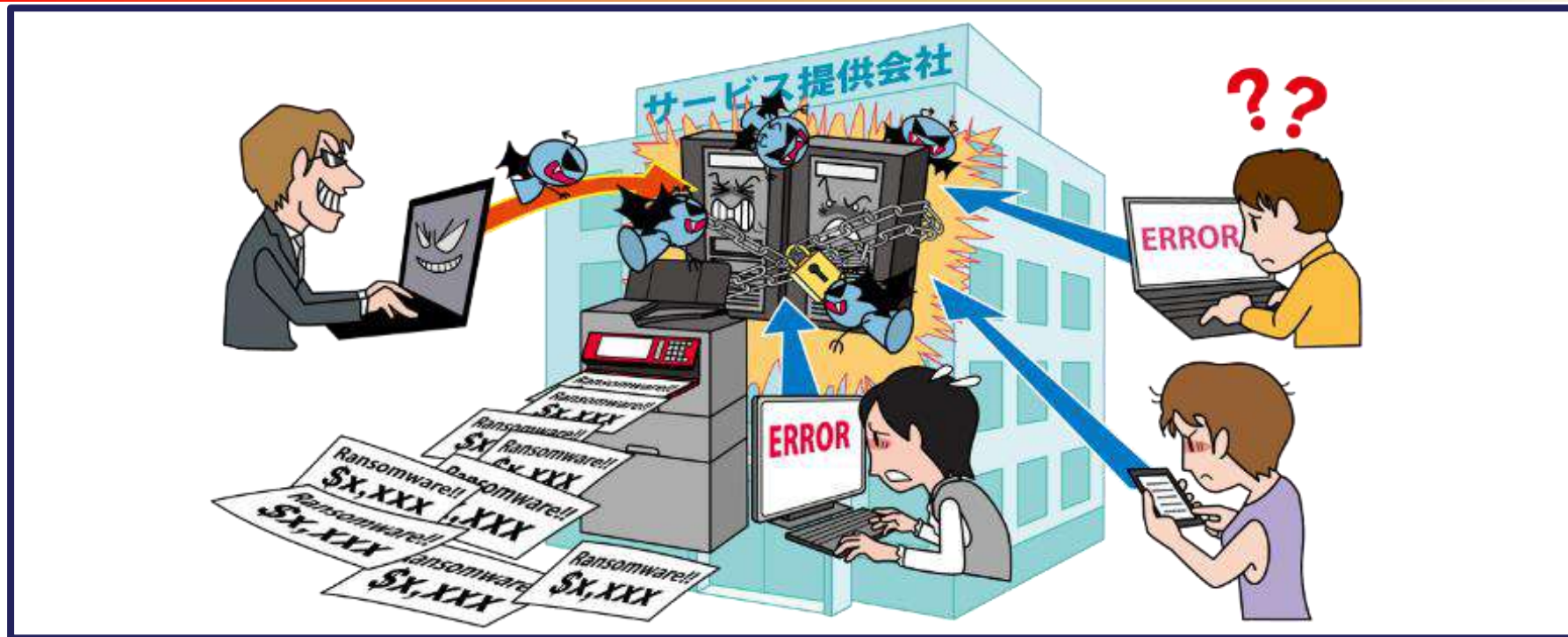
「個人」向け（五十音順）
インターネット上のサービスからの個人情報の窃取
インターネット上のサービスへの不正ログイン
クレジットカード情報の不正利用
スマホ決済の不正利用
偽警告によるインターネット詐欺
ネット上の誹謗・中傷・デマ
フィッシングによる個人情報等の詐取
不正アプリによるスマートフォン利用者への被害
メールやSMS等を使った脅迫・詐欺の手口による金銭要求
ワンクリック請求等の不当請求による金銭被害

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。
- 下記の「情報セキュリティ対策の基本」は常に意識する。

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

【1位】 ランサムウェアによる被害



- PC等に保存されているファイルが暗号化され、**使用不可にされる**
- 復旧と引き換えに**金銭を要求される**
- 情報が窃取されて、**公開され**、さらに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される**ケースもある
- 組織の**規模や業種に関係なく**攻撃される

【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
 - 脆弱性を悪用した手口
 - ソフトウェアの脆弱性を悪用しウイルスを実行（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
 - 不正アクセスによる手口
 - 意図せず公開されているポート(リモートデスクトップ等)からサーバーに不正アクセスさせる
 - サーバー上で攻撃者がウイルスを実行させる(感染させる)
 - メールを利用した手口
 - 不正な添付ファイルを開かせる
 - メール内のリンクをクリックさせる
 - Web サイトを悪用した手口
 - ランサムウェアをダウンロードさせるようにWebサイトを改ざんした
 - 当該サイトを閲覧するようにメールなどで誘導した

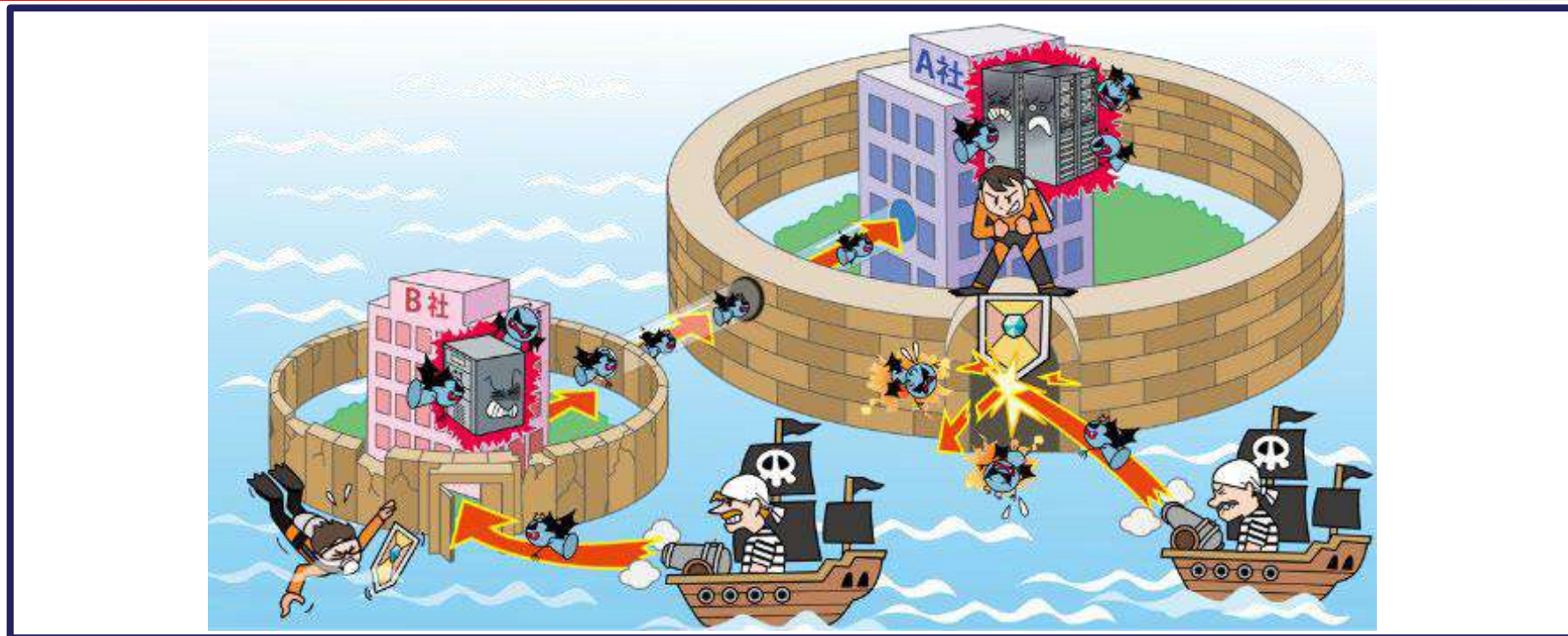
【1位】ランサムウェアによる被害 ～ 対策

- < 経営者層 >
 - 組織としての対応体制の確立
 - インシデント対応体制を整備し、対応する
- < システム管理者、従業員 >
 - 被害の予防
 - インシデント対応体制を整備し、対応する
 - メールの添付ファイル開封や、メールやSMSのリンク、URLのクリックを安易にしない
 - 多要素認証の設定を有効にする
 - 提供元が不明のソフトウェアを実行しない
 - サーバーやクライアント、ネットワークに適切なセキュリティ対策を行う
 - 共有サーバー等へのアクセス権の最小化と管理強化
 - 公開サーバーへの不正アクセス対策
 - 適切なバックアップ運用(取得、保管、復旧訓練)を行う

【1位】 ランサムウェアによる被害 ～ 対策

- <システム管理者、従業員>
 - 被害を受けた後の対応
 - 適切な報告／連絡／相談を行う
 - 適切なバックアップ運用(復旧作業)を行う
 - 復号ツールの活用
 - インシデント対応体制を整備し、対応する
- 身代金の支払いと復旧業者の選定について
 - 原則、身代金を支払わずに復旧を行う
 - 身代金を支払ってもデータの復元や情報の流出を防げるとは限らない
 - 対応を依頼した業者が攻撃者との裏取引で身代金を支払うことで復旧した場合、事実上、自組織が攻撃者に資金提供をしたとみなされるおそれもある
 - 対応を依頼する業者の選定にも注意が必要

【2位】 サプライチェーンの弱点を悪用した攻撃



- 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**)攻撃も存在する
- 取引先や業務を委託している**外部組織から情報漏えい**する

【2位】 サプライチェーンの弱点を悪用した攻撃

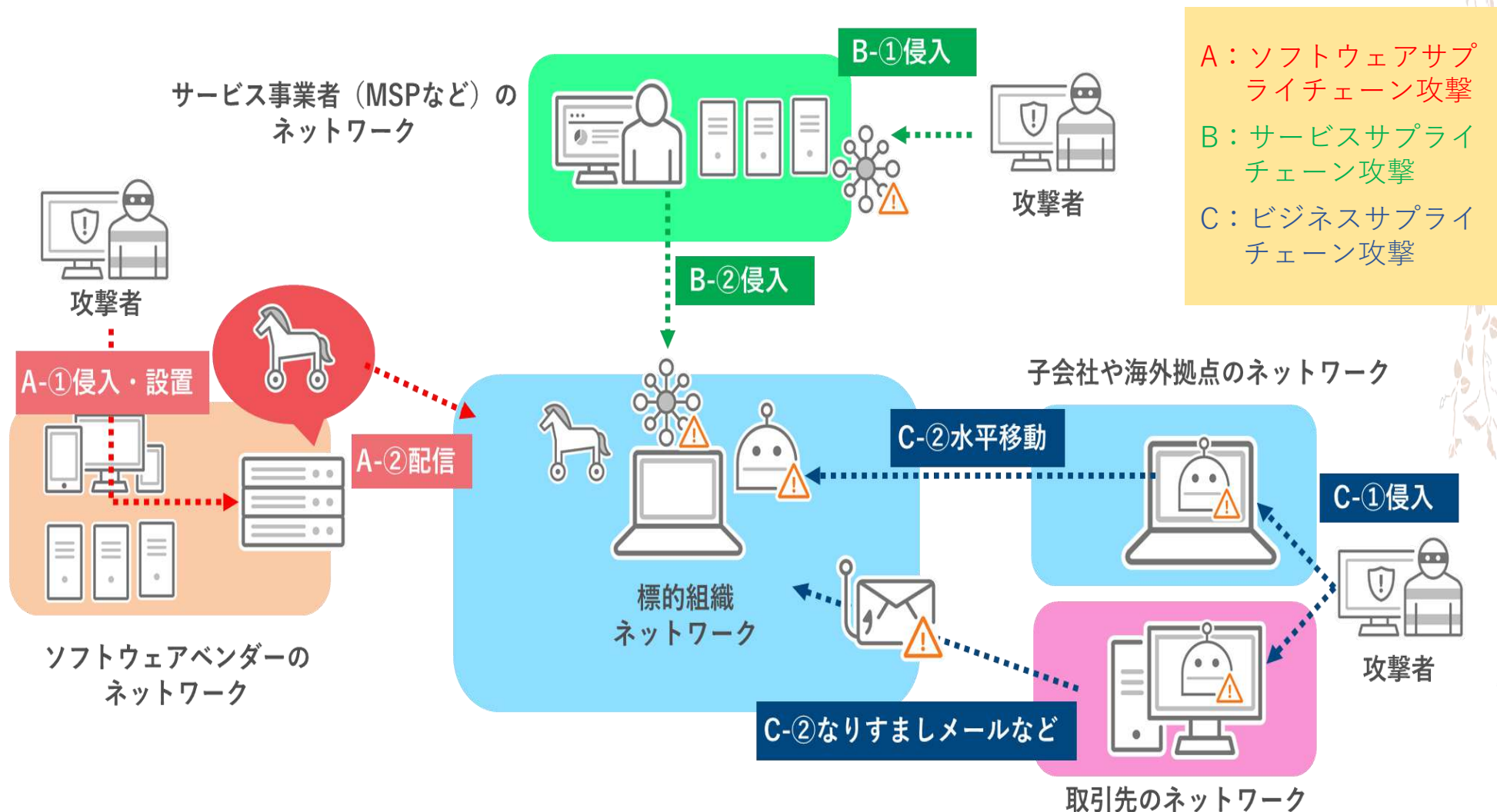
- 2023年の事例/傾向

- 委託先のシステムを介して不正アクセスされ、顧客情報が漏えい
 - 2023年11月、LINEヤフーは同社の保有する顧客情報が漏えいしたことを公表
 - ユーザーに関する情報が約30万件、取引先等に関する情報が約9万件、従業員等に関する情報が約5万件が漏えい
 - 第三者による社内システムへの不正アクセスが原因
 - 委託先企業であるNAVER Cloud社のさらに委託先の企業で従業員のPCがウィルス感染したことが発端

- 最近の事例

- 2024年5月株式会社イセトー（印刷業務受託事業）
 - ランサムウェア攻撃による情報漏えい
 - 自治体から受託していた納税通知書などから住民の個人情報が漏えい
 - 企業から受託していたダイレクトメールから顧客の個人情報が漏えい

サプライチェーン攻撃の種別



- A: ソフトウェアサプライチェーン攻撃
- B: サービスサプライチェーン攻撃
- C: ビジネスサプライチェーン攻撃

トレンドマイクロ 2022年上半期サイバーセキュリティレポート より

【2位】 サプライチェーンの弱点を悪用した攻撃 ～ 対策

- 組織（自組織）
 - 被害の予防
 - 情報管理規則の徹底
 - セキュリティ評価サービス(SRS)を用いた自組織のセキュリティ対策状況の把握
 - 信頼できる委託先、取引先、サービスの選定
 - 契約内容の確認
 - 委託先組織の管理
 - 納品物の検証(ソフトウェアの把握や管理、脆弱性対策の実施等)
 - 被害を受けた後の対応
 - インシデント対応体制を整備し、対応する
 - 被害への補償
- 組織（商流に関わる組織との連携）
 - 被害の予防
 - 取引先や委託先との連絡プロセスの確立
 - 取引先や委託先の情報セキュリティ対応の確認、監査
 - 情報セキュリティの認証取得
 - 公的機関等が公開している資料の活用
 - 被害を受けた後の対応
 - 適切な報告／連絡／相談を行う

【3位】 内部不正による情報漏えい等の被害



- 組織の従業員や元従業員等による機密情報の漏えい
- 組織関係者による不正行為による、組織の社会的信用の失墜、損害賠償による経済的損失
- 不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある

【3位】 内部不正による情報漏えい ～ 攻撃手口

- 内部の従業員は重要情報にアクセスしやすい
- 悪意をもって情報を外部に提供してしまう
- アクセス権限の悪用
 - 付与されたパスワードを悪用し、組織の重要情報を取得する
 - 必要以上のアクセス権限を付与していると被害が大きくなる
- 在職中に割り当てられたアカウントの悪用
 - 在職中に使用していたアカウントを使って不正に情報を取得する
- 内部情報の不正な持ち出し
 - USBメモリー、HDD、メール、クラウドストレージ、スマホカメラ、紙媒体等での持ち出し

【3位】 内部不正による情報漏えい ～ 対策

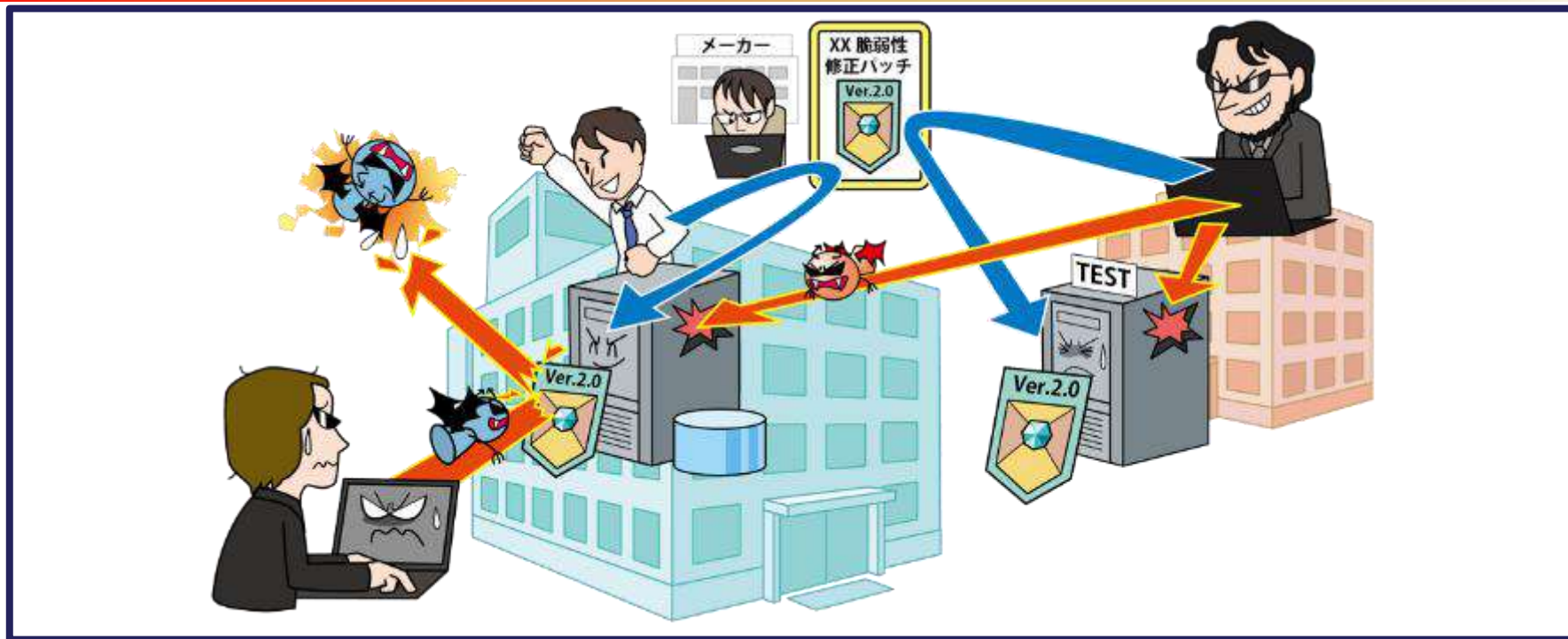
- 内部不正は情報やシステムへの正当なアクセス権を持った社内の者により行われることが多いため、技術的な対策には限界があり、むしろ、人事制度や企業風土も含めた広範な対策を取る必要があります。
- 内部不正を防止する方法として一般的には以下の対策が有効です。
 - 犯行をやりにくくする。（主に物理的、技術的な対策）
 - 行われた犯行が見つかりやすくする。（監視や記録の仕組み）
 - 犯行が割に合わないようにする。（価値のある資産を隠す、罰則を重くする）
 - 犯行を行う動機を生じさせないようにする。（不満やストレスの元を減らす）
 - 犯行の正当化や弁明の余地を与えない。（明確なルール化やコンプライアンス教育）

【4位】 標的型攻撃による機密情報の窃取



- メール等を利用し、特定組織のPCをウイルスに感染させる
- 組織内部に潜入し、長期にわたり侵害範囲を徐々に広げる
- 組織の機密情報窃取やシステムを破壊する

【5位】 修正プログラムの公開前を狙う攻撃



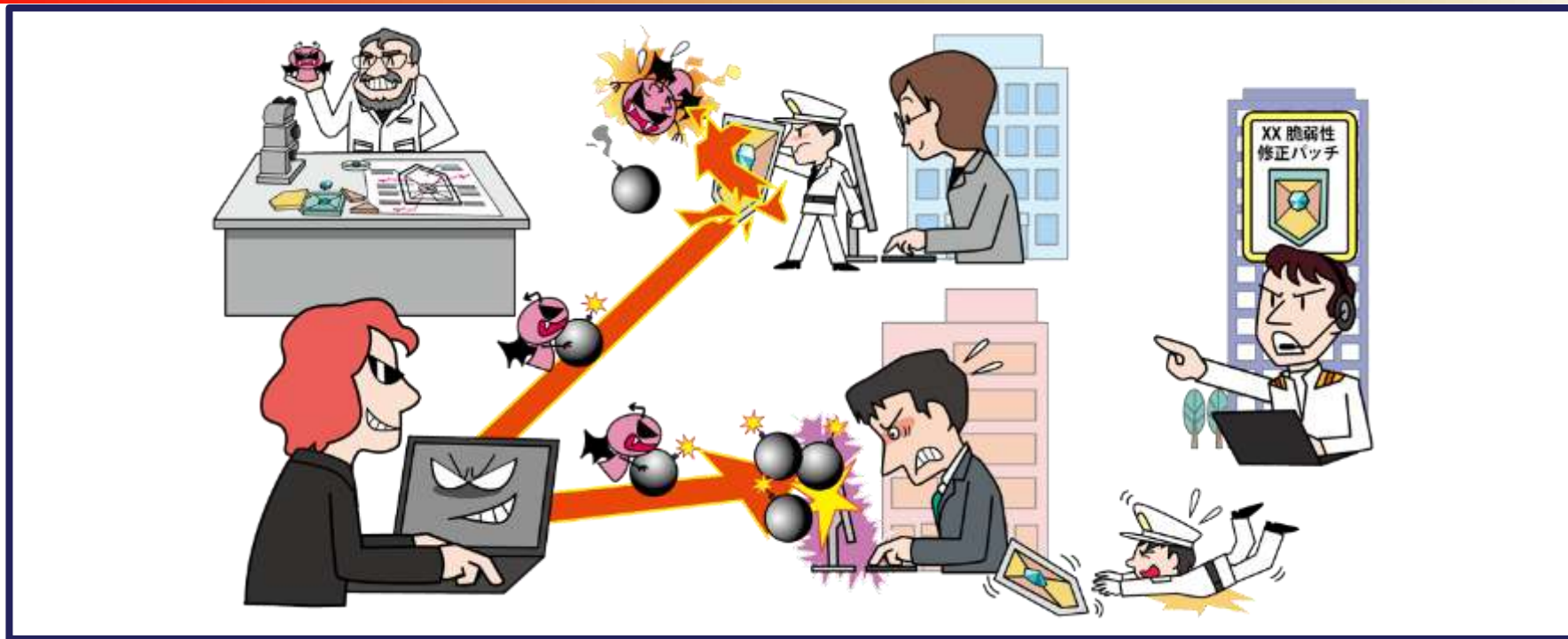
- 脆弱性の修正プログラム(パッチ)や回避策が公開される前に脆弱性を悪用した攻撃が行われる(ゼロデイ攻撃)
- 事業やサービスの停止など、多くのシステムやユーザーに被害が及ぶ
- 脆弱性対策情報が公開された場合は、早急な対応が求められる

【6位】不注意による情報漏えい等の被害



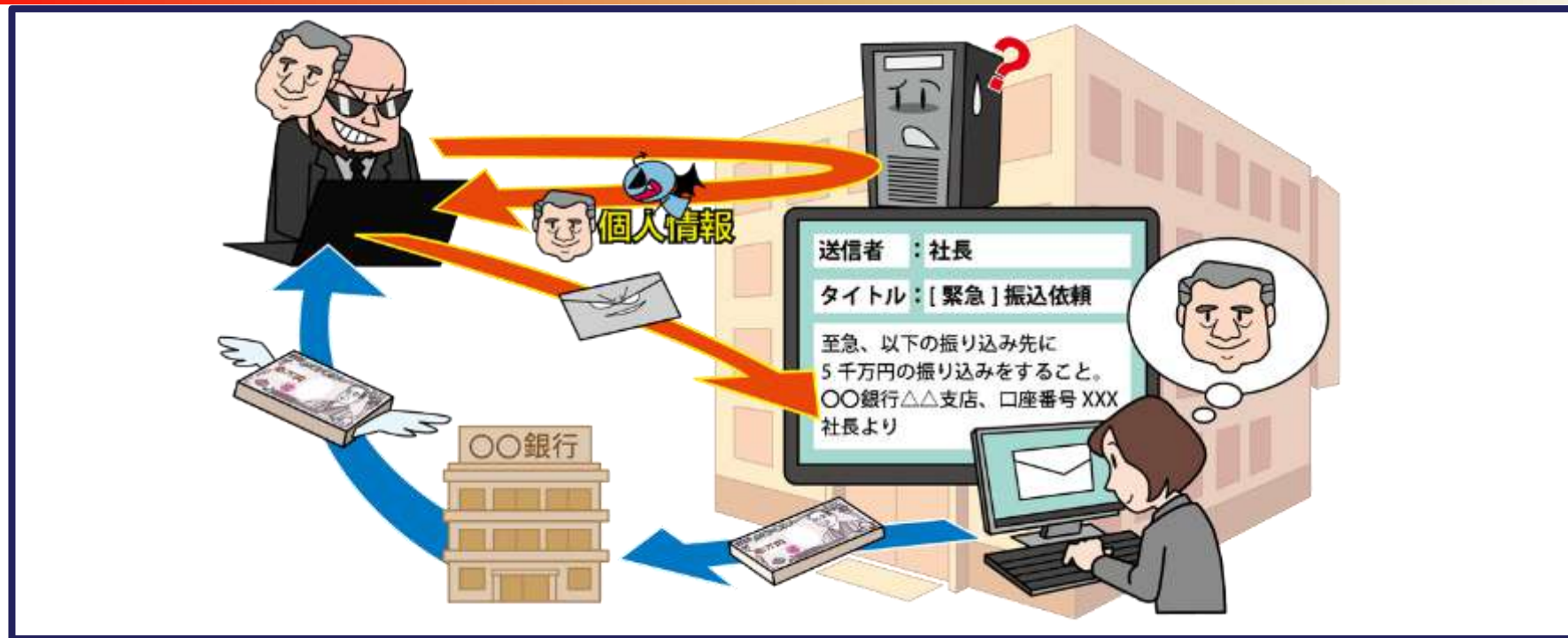
- 従業員の不注意等によって意図せず機密情報を漏えい
- 情報漏えいすることによる社会的信用の失墜、経済的損失、漏えいした情報の悪用による二次被害

【7位】 脆弱性対策情報の公開に伴う悪用増加



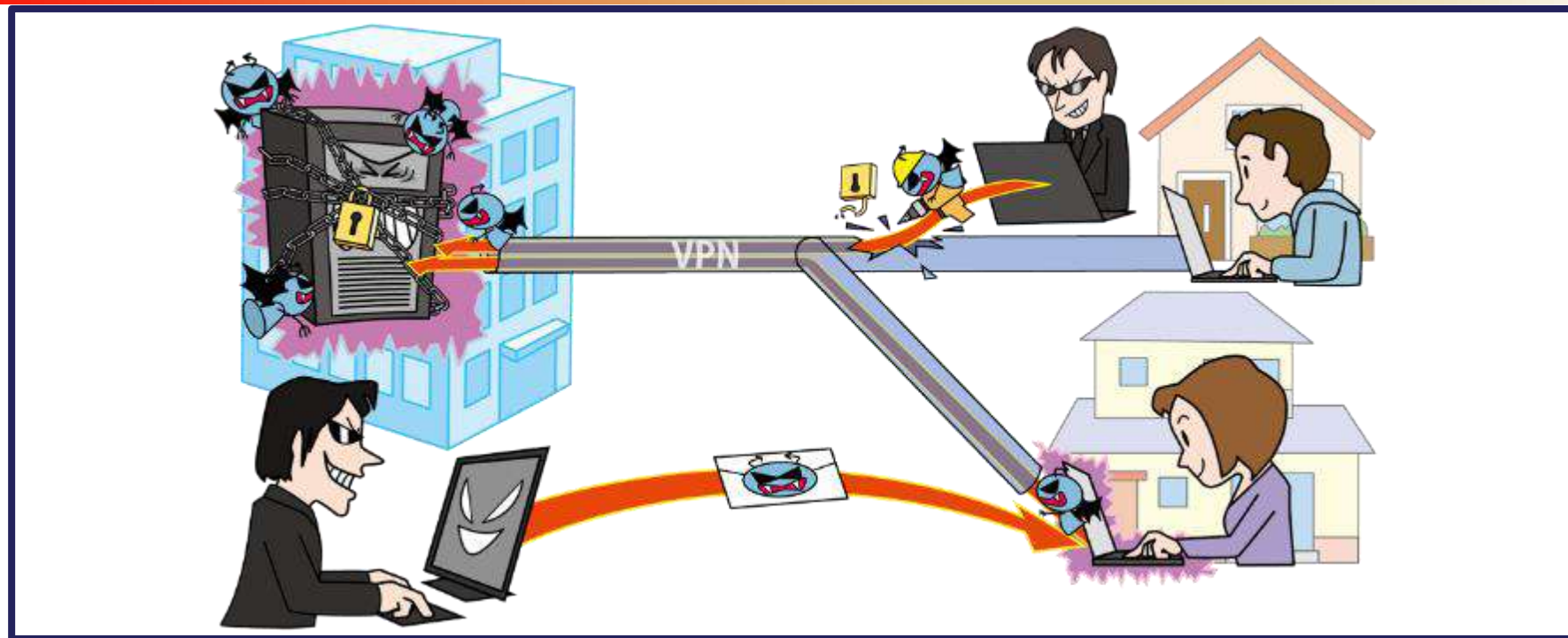
- 脆弱性対策のために公開された脆弱性情報を攻撃者が悪用する
- 広く利用されている製品の脆弱性の場合には被害が広範囲に及ぶ
- 脆弱性情報の公開後、それらを悪用した攻撃が発生するまでの時間が近年は短くなっている傾向がある

【8位】 ビジネスメール詐欺による金銭被害



- 取引先や経営者とやりとりするような **ビジネスメール**を装う
- メールを巧妙に細工し、企業の **金銭**を取り扱う担当者を騙す
- **攻撃者が用意した口座**へ送金させる

【9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



- 2020年以降、感染症対策の一環として政府機関がニューノーマルな働き方の1つであるテレワークを推奨している
- VPN等の本格的な活用がされる中、それらを狙った攻撃が発生
- 業務環境に脆弱性があると、Web会議をのぞき見されるリスクが高まる

【9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

- 私物のパソコンを使う場合
 - 修正プログラムの適用
 - セキュリティソフトの導入および定義ファイルの最新化
 - パスワードの適切な設定と管理
 - 不審なメールに注意
 - USBメモリ等の取り扱いの注意
 - 社内ネットワークへの機器接続ルールの遵守
 - ソフトウェアをインストールする際の注意
 - パソコン等の画面ロック機能の設定
 - テレワークで使用するパソコン等は、できる限り他人と共有しない。共有で使わざるを得ない場合は、業務用のユーザアカウントを別途作成する。
- ネットワークへの接続
 - 自宅のルータは、最新のファームウェアを適用する。
 - 管理用パスワードは初期設定から変更する。
 - 公衆Wi-Fiは安全なものを使う。若しくは、自分のWi-Fiルータ、スマホのテザリングなど使う。
- 公共の場で行う場合
 - カフェ等の公共の場所ではパソコンの画面をのぞかれないように。
 - ウェブ会議を行う場合は、話し声が他の人に聞こえないように。
 - デジタルデータ/ファイルだけではなく、紙の書類等の管理にも注意する。

IPA テレワークを行う際のセキュリティ上の注意事項より（一部修正）
<https://www.ipa.go.jp/security/announce/telework.html>

総務省「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）」

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

- テレワークを実施する際に最低限のセキュリティを確実に確保してもらうための手引き（チェックリスト）
- 対象はセキュリティの専任担当がいらないような中小企業等におけるシステム管理担当者（専門用語について仕組みの詳細まではわからないが、利用シーンがイメージできるレベルの方）
- テレワークの各種方式の解説と、その方式毎のセキュリティ対策チェックリスト
- 設定解説資料
 - ✓ Web会議アプリ
 - ✓ ファイル共有サービス
 - ✓ リモートデスクトップ
 - ✓ VPNルーター



【10位】 犯罪のビジネス化(アンダーグラウンドサービス)



- サイバー犯罪に使用するサービスやツール等の取引市場が存在する
- 通常のブラウザでは検索できないWebサイト上に存在する
- 専門知識は不要で容易にサイバー攻撃が可能になってきている

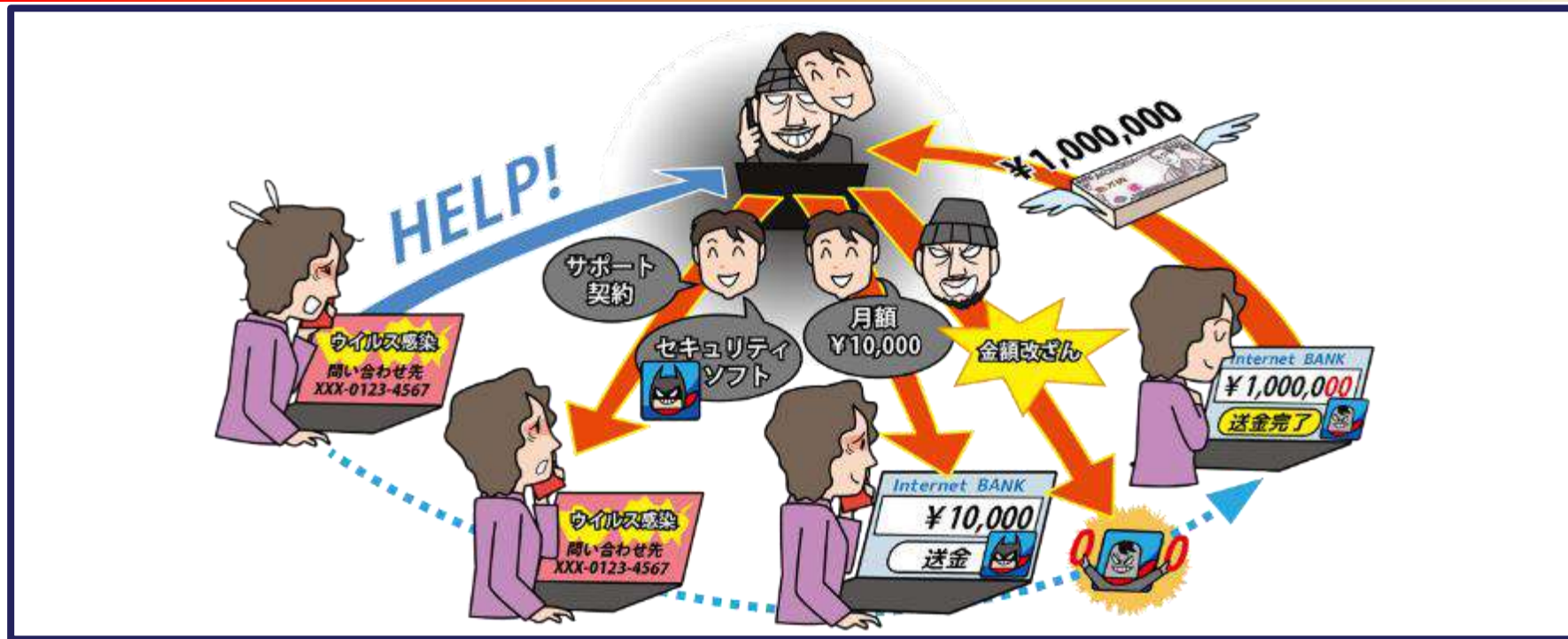
IPA 情報セキュリティ10大脅威 2024 個人編

「個人」向け（五十音順）	脅威の概要
インターネット上のサービスからの個人情報の窃取	<ul style="list-style-type: none">◆ 攻撃者がショッピングサイト等、インターネット上のサービスの脆弱性等を悪用し、個人情報を窃取する◆ 窃取された情報が悪用されると、クレジットカードを不正利用されたり、詐欺メールを送信されたりする
インターネット上のサービスへの不正ログイン	<ul style="list-style-type: none">◆ 利用しているインターネット上のサービスの認証情報（ID、パスワード）が窃取または推測され、不正ログインされる◆ 別のサービスで使い回しをしていた認証情報が漏えいし、不正ログインされる◆ インターネット上のサービスの機能に応じて発生する被害は様々
クレジットカード情報の不正利用	<ul style="list-style-type: none">◆ ウイルス感染やフィッシング詐欺、改ざんされたWebサイトによりクレジットカード情報を詐取される◆ クレジットカード情報をショッピングサイト等で不正利用される
スマホ決済の不正利用	<ul style="list-style-type: none">◆ スマホ決済サービスに不正ログインしてアカウントを乗っ取る◆ スマホ決済サービスの脆弱性等の不備を悪用◆ クレジットカード情報等の窃取や、利用者が意図しない金銭取引を行う
偽警告によるインターネット詐欺	<ul style="list-style-type: none">◆ インターネット閲覧中にウイルス感染やシステム破損に関する偽の警告画面（偽警告）を表示させる◆ 被害者は偽警告の内容を信じて、警告の内容に従ってしまうと不要なソフトウェアのインストールやサポート契約を結ばされる◆ 最終的に、修復費用等として金銭を騙し取られる

IPA 情報セキュリティ10大脅威 2024 個人編

「個人」向け（五十音順）	脅威の概要
ネット上の誹謗・中傷・デマ	<ul style="list-style-type: none">◆ SNS等で他人を誹謗・中傷したり、脅迫・犯罪予告を書き込み、事件になる◆ 誹謗・中傷やデマの発信は犯罪になり、安易に拡散した人も、その行為を特定され、社会的責任を問われる場合がある◆ AI技術を用いて加工された音声や画像、動画は本当か見分けがつきにくく、一層注意が必要になっている
フィッシングによる個人情報等の詐取	<ul style="list-style-type: none">◆ 金融機関や有名企業を装ったフィッシングサイト（偽のWebサイト）へ利用者を誘導する◆ フィッシングサイト上でIDやパスワード、クレジットカード情報等の個人情報を入力させて窃取する
不正アプリによるスマートフォン利用者への被害	<ul style="list-style-type: none">◆ 不正アプリをスマートフォンにインストールしてしまうことで、スマートフォン内の連絡先情報等の個人情報が窃取される◆ スマートフォンの一部の機能を不正利用される◆ 攻撃の踏み台にされることで意図せず加害者になるおそれもある
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	<ul style="list-style-type: none">◆ 周囲に相談しにくいセクステーション（性的脅迫）等のメールやSMS等を送り付けられ、金銭を要求される◆ 脅迫・詐欺のメールの内容は虚偽のものであるが、その内容に騙され、不安に思ったメールやSMS等の受信者が金銭を支払ってしまう
ワンクリック請求等の不当請求による金銭被害	<ul style="list-style-type: none">◆ PCやスマートフォンに請求画面が表示され、金銭を不当に請求される被害が依然として発生している◆ 複数回クリックさせることで、請求の正当性を主張するケースや、クリックをしなくても自動的に請求画面に転送されるケースも存在する

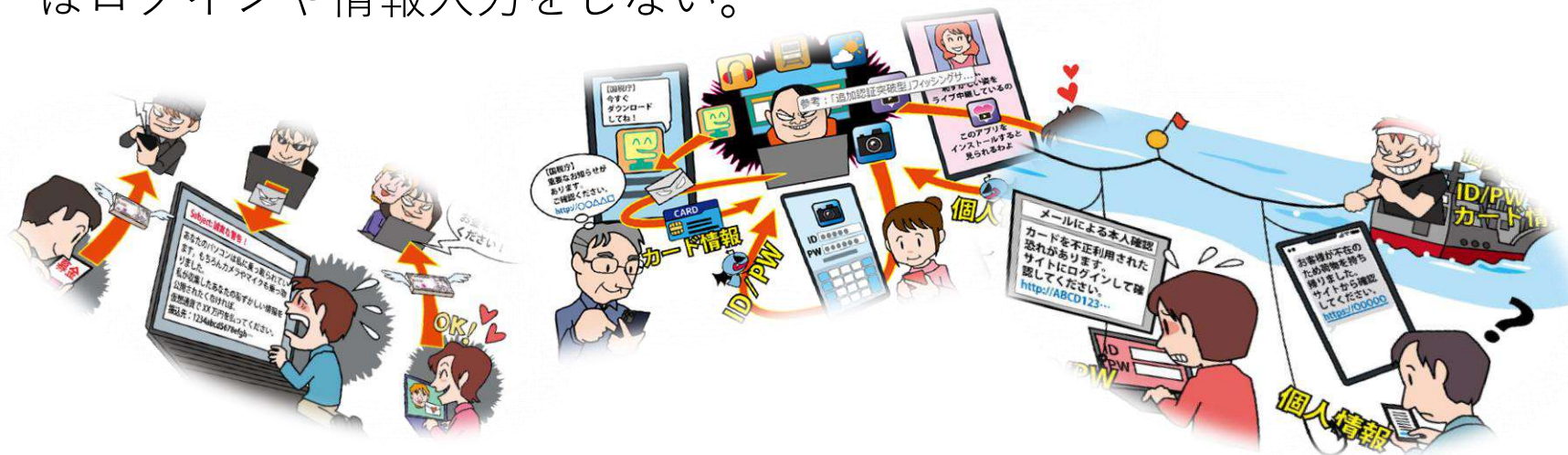
偽警告によるインターネット詐欺



- ◆ インターネット閲覧中にウイルス感染やシステム破損に関する偽の警告画面（偽警告）を表示させる
- ◆ 被害者は偽警告の内容を信じて、警告の内容に従ってしまうと不要なソフトウェアのインストールやサポート契約を結ばされる
- ◆ 最終的に、修復費用等として金銭を騙し取られる

個人編：まとめ

- 詐欺＝人間を騙す犯罪である以上、その手口を知り、騙されないように注意することが基本
 - 新たな機器やサービスの普及に伴いインターネット利用における脅威の手口も変化する。
 - 公的機関の注意喚起やニュースから脅威の手口に関する情報を収集する。
 - Web検索や一般サイト、SNSで表示される広告にも不正なものが存在している事実を知り、クリックに注意する。
 - 偽メールや偽サイトを見抜けると思うな！クリックして飛んだページではログインや情報入力をしない。



情報セキュリティ10大脅威：まとめ

- 情報セキュリティ対策の基本を実践
 - 「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は長年変わらない。
 - 多くの脅威に対して共通して有効な基本対策を確実に実践する。
- 各脅威の手口の把握および対策を実践
 - 脅威に備えるためには攻撃手口やその変化、被害事例、および自組織が抱える要因等を把握することが重要。
 - 「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない。組織ごとの状況を考慮して対策の優先度を決定する。

2. 情報セキュリティのリスクと対策

情報セキュリティの目的

情報セキュリティとリスク

情報セキュリティ対策のアプローチ

情報セキュリティ対策はなぜ必要？

- IT活用がビジネスに利益をもたらす一方で、サイバー攻撃や従業員の不注意などによる損害が多発しています。
- 近年増加しているサイバー攻撃は金銭窃取などを目的としていることが多く日々巧妙化、複雑化、悪質化しています。
- 組織の損害を未然に防ぐために、今や情報セキュリティ対策は必須です。



出展：IPA 「情報セキュリティ5か条コース」より

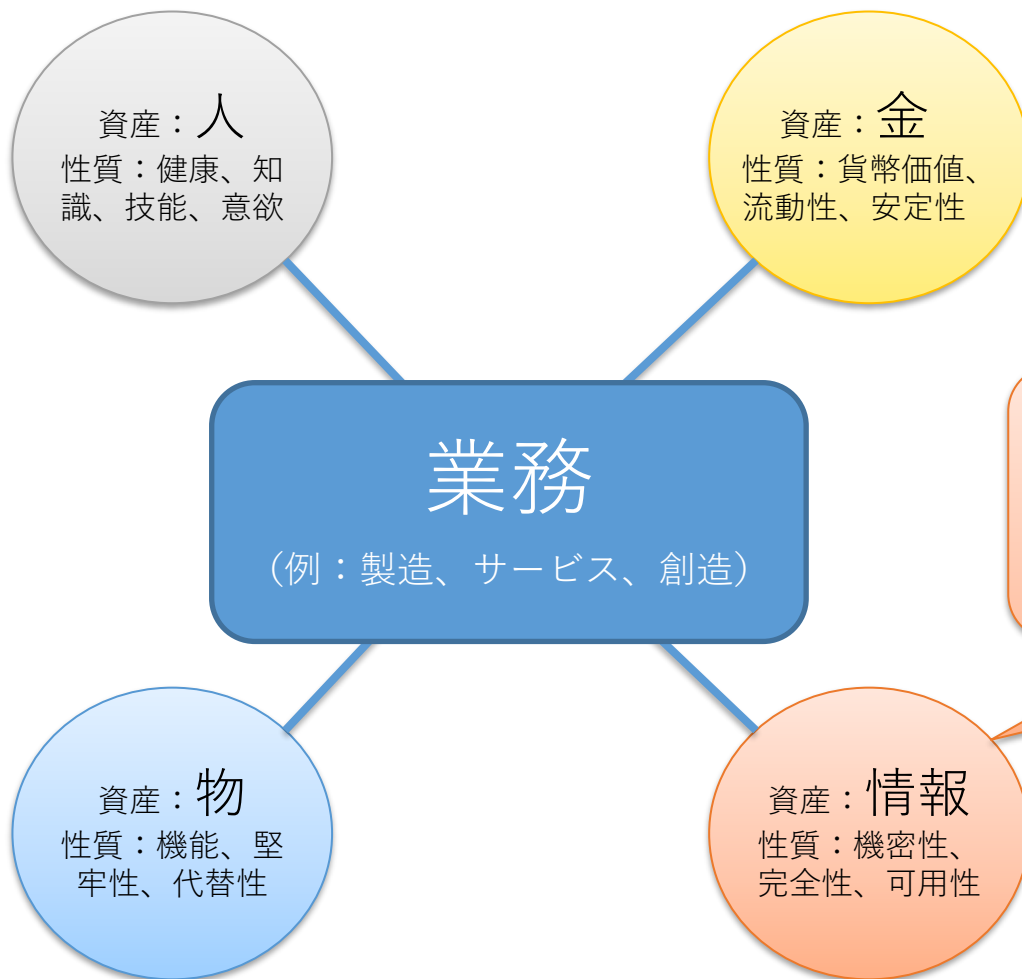
情報セキュリティの目的

- どのような組織でも電子データや書類などの情報を利用して業務を行っています。
- ビジネスで活用し、組織にとって価値がある重要な情報*には様々なものがあります。
- 情報セキュリティの目的は、それら重要な情報の機密性、完全性、および可用性を維持することです。

* 重要な情報を「情報資産」ということがあります。

機密性 (C)	許可された者だけが情報にアクセスできるようにすること
完全性 (I)	情報や情報の処理方法が、正確で完全であるようにすること
可用性 (A)	必要な時に情報や情報資産にアクセスできることを確実にすること

業務保証としての情報セキュリティ



守るべきは業務

業務は資源（資産）を使う

資産は固有の性質（価値）を持つ

機密性（C） 完全性（I） 可用性（A）

情報資産のC I Aが損なわれると業務は回らなくなる。

情報セキュリティの定義

情報資産のC I Aを保つことにより、業務の遂行を保証（任務保証）すること。

情報セキュリティ事故とは

情報資産の例	情報セキュリティ事故の例
顧客リストなどの個人情報	<ul style="list-style-type: none">顧客リストが不正アクセスで漏えいする。(機密性の事故)
設計図などの技術情報	<ul style="list-style-type: none">設計図がランサムウェア※に感染して読めなくなる。(可用性の事故)
予約や注文を受けるECサイト	<ul style="list-style-type: none">サイトがDDoS攻撃※で停止する。(可用性の事故)サイトが不正アクセスにより改ざんされ、外部のサイトへのリンクが埋め込まれる。(完全性の事故)

※ **ランサムウェア**

ファイルを暗号化し、元の状態に戻すための金銭を要求する悪意のあるソフトウェア

※ **DDoS攻撃**

複数のコンピュータから一斉に特定のサーバー等に対して過剰な負荷を与えたり、サーバー等の脆弱性を悪用することによってサービスの運用や提供を妨げる攻撃

自組織の重要情報は何だろう？

- 漏えいしたり、改ざんされたり、利用できなくなると、組織や個人に損害が発生する可能性がある情報が重要情報です。
 - 顧客の氏名、住所、メールアドレス、クレジットカード情報などの個人情報
 - 従業員のマイナンバー、履歴書、顔写真などの個人情報
 - 売上増加に不可欠な営業情報
 - ノウハウ、独自技術などの機密情報
- 「自組織の重要情報は何か？」を認識することが情報セキュリティ対策の第一歩です。

あなたが扱う重要情報資産

-
-
-



情報セキュリティとリスク



平常時

脆弱性
(弱点、セキュリティホール、ヒューマンエラー等)



情報セキュリティ事故 (インシデント) 発生時

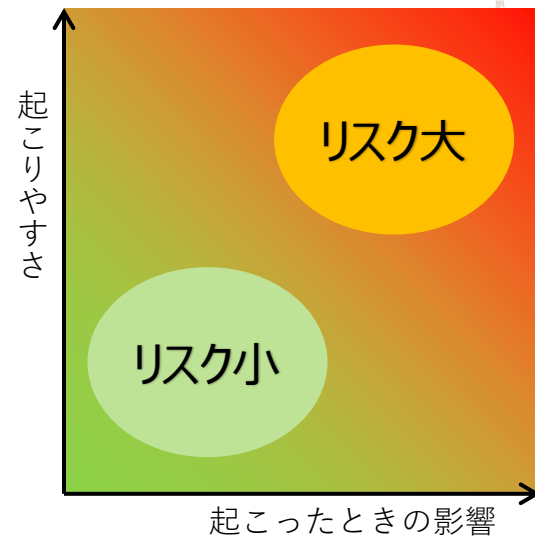
脅威

不正侵入、ウイルス、改ざん、盗聴、自然災害等

情報資産の脆弱性に脅威が作用すると、情報資産の価値 (CIA) が損なわれ、業務の遂行に支障をきたす。⇒ インシデント

インシデントは起きるかもしれないし、起きないかもしれない。
⇒ リスク

リスクの大きさ = 起こったときの影響 × 起こりやすさ
= (情報資産、脅威シナリオ) × (脅威、脆弱性)

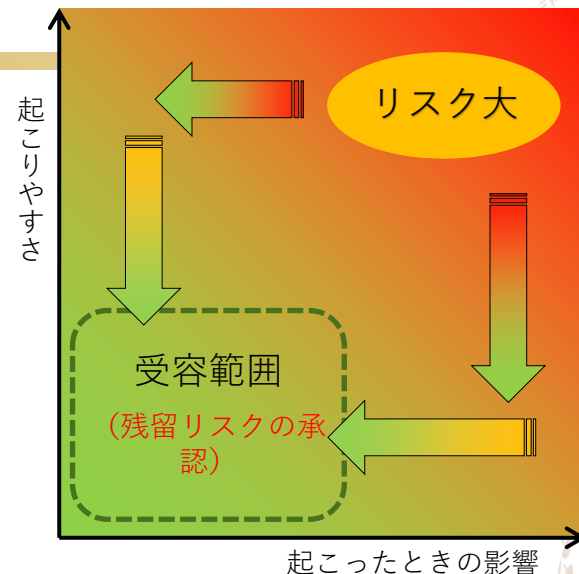


情報セキュリティ対策の考え方

情報セキュリティ対策とは、リスクの大きさを減らすこと。

どこまで減らすのか ⇒ 組織の**受容基準**以下にする。

リスクの大きさ = 起こったときの影響 × 起こりやすさ
 = (情報資産、脅威シナリオ) × (脅威、脆弱性)



対策	考え方	対策例
回避	業務を見直すこと	その業務を止める。情報を持たない。
低減	起こりやすさを減らす	脆弱性を塞ぐ。セキュリティパッチ、アクセス制御、ネットワーク分離など。
	起こったときの影響を減らす	早期検知、暗号化、バックアップ、冗長化など。SOC/CSIRTの整備。情報資産のCIAを強靱にする。
移転	インシデント発生時の損失を転嫁する	サイバーセキュリティ保険、アウトソース。
受容	リスクの大きさが小さいので容認できる。	敢えてそれ以上の対策はしない。(残留リスクは承認する。)

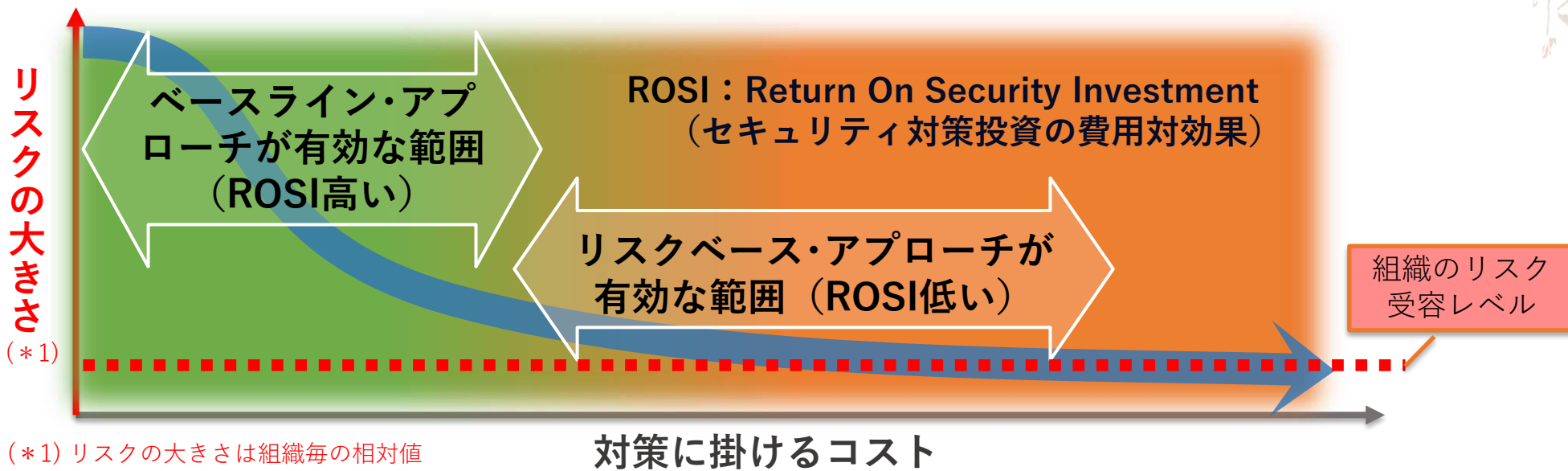
物理的、論理（技術）的、管理的

抑止的、予防的、検知的、是正的、回復/復旧的

情報セキュリティ対策のアプローチ (1)

専門人材、時間、
組織全体の関与

アプローチ	概要	リスク対策の有効性、妥当性	コスト
ベースライン・アプローチ	基準（ガイドライン）→ 対策実施 → 評価	概ね、このような対策をすれば妥当という一般認識を基準とする。	コスト小 (ROSI高い)
リスクベース・アプローチ	ISO 31000：アセスメント（特定、分析、評価）、対応 例：ISMS（ISO/IEC 27001）	自組織の環境や能力、脅威に合わせて最適化する。	コスト大 (ROSI低い)



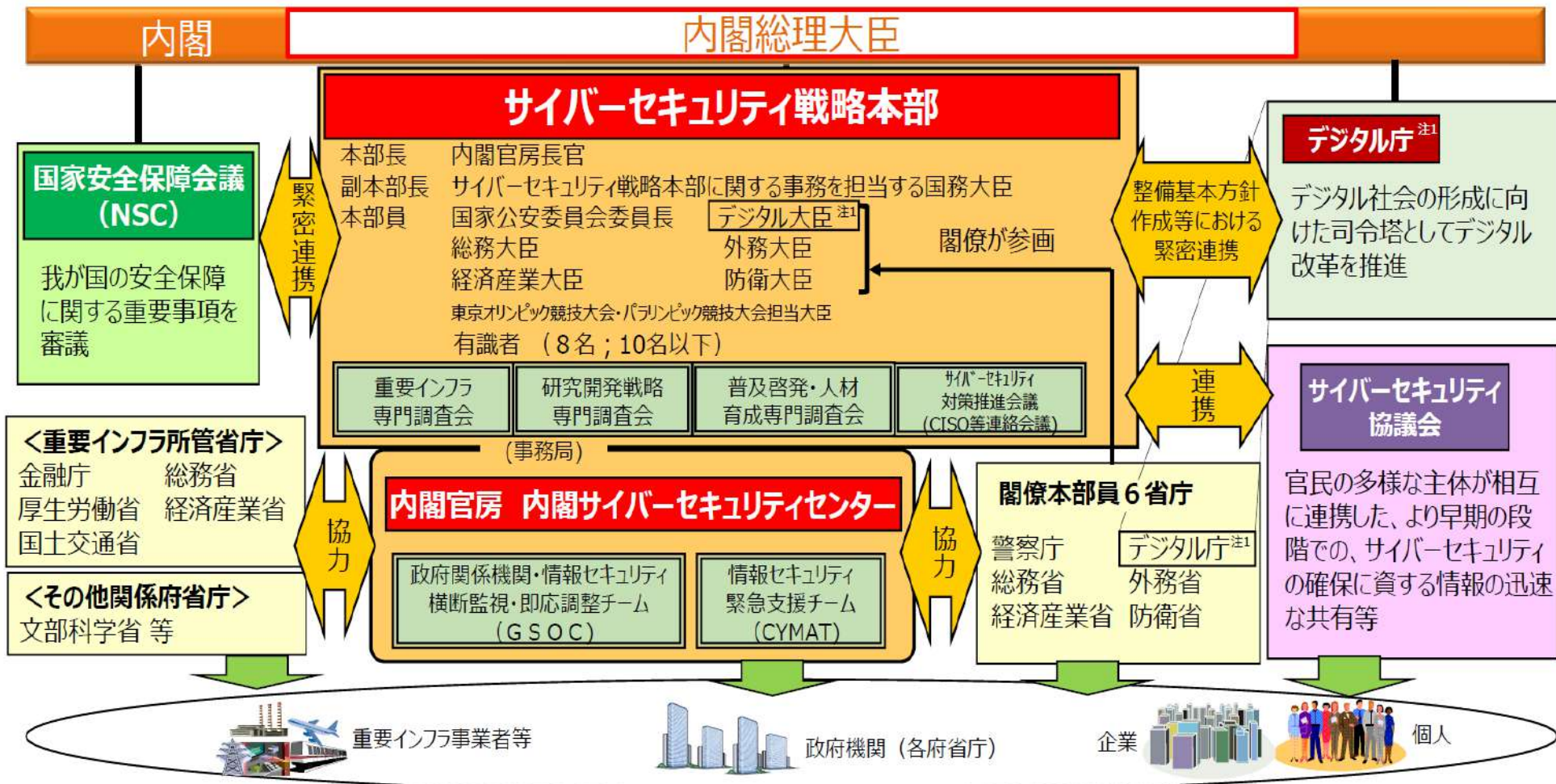
3. 情報セキュリティ対策の進め方

3.1 (独) 情報処理推進機構 (IPA) による支援施策

- IPA 中小企業の情報セキュリティ対策ガイドライン
- IPAのその他の施策、ツール

3.2 その他の支援施策、支援者等

政府のサイバーセキュリティ戦略推進体制



(注1) デジタル社会形成基本法（令和3年法律第35号）、デジタル庁設置法（令和3年法律第36号）。（令和3年9月1日施行）

NISC サイバーセキュリティ戦略 2021年9月


重要インフラのサイバーセキュリティ

官民連携による重要インフラ防護の推進


- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

NISCによる総合調整

重要インフラ所管省庁

- 金融庁
[金融]
 - 総務省
[情報通信、行政]
 - 厚生労働省
[医療]
 - 経済産業省
[電力、ガス、化学、クレジット、石油]
 - 国土交通省
[航空、空港、鉄道、水道、物流、港湾]
- 

重要インフラ(全15分野)

- 情報通信
 - 金融
 - 航空
 - 空港
 - 鉄道
 - 電力
 - ガス
 - 政府・行政サービス
 - 医療
 - 水道
 - 物流
 - 化学
 - クレジット
 - 石油
 - 港湾
- 

関係機関等

- サイバーセキュリティ関係省庁
[総務省、経済産業省等]
- 事案対応省庁
[警察庁、防衛省等]
- 防災関係府省庁
[内閣府、各省庁等]
- サイバーセキュリティ関係機関
[NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者
[サプライチェーン等に関わるベンダー等]

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化



経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

安全基準等の整備及び浸透



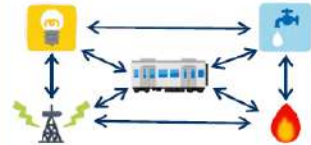
重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化



官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化



分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

NISC 重要インフラのサイバーセキュリティに係る行動計画2024年3月

セキュリティ対策を進める際の支援機関/支援者

- 中小企業等が組織として情報セキュリティ対策を進める際の支援を提供している組織や支援者
 - 支援組織
 - 経済産業省/独立行政法人情報処理推進機構（IPA）
 - 総務省
 - 警察庁、警視庁、道府県警察本部
 - 商工団体（商工会議所、商工会）
 - 所轄官庁（厚生労働省、文部科学省など）、業界団体
 - 支援者
 - 登録セキスペ（情報処理安全確保支援士）
 - セキュリティプレゼンター
 - ITコーディネータ（ITC）
 - 中小企業支援者（中小企業診断士、税理士など）

3. 情報セキュリティ対策の進め方

3.1 (独) 情報処理推進機構 (IPA) による支援施策

- IPA 中小企業の情報セキュリティ対策ガイドライン
 - Step 1 : 情報セキュリティ 5 か条
 - Step 2 : 5 分でできる! 情報セキュリティ自社診断
 - Step 3、Step 4
- IPAのその他の施策、ツール

3.2 その他の支援施策、支援者等

IPAが進める主な対策支援施策（主に中小組織向け）

ガイドライン、ツールなど	中小企業の情報セキュリティ対策ガイドライン	対策のガイドライン、及び、そのガイドラインに沿った対策を進めるためのツール類。
対策導入支援施策	「SECURITY ACTION」制度	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。
	サイバーセキュリティお助け隊サービス	主に事後対応として、最低限必要となる各種サービスをワンパッケージで提供する「お助け隊サービス」を展開、普及させる施策
普及啓発のためのコンテンツ提供やセミナーの開催支援	セキュリティプレゼンター	主にセミナー開催やガイドライン等の解説を行う支援人材を登録し、その活動を支援する制度。
	講習能力養成セミナー	企業内でのセキュリティ講習会の開催方法の習得を目指すもの。
	教材コンテンツ等	学習教材、映像素材、自己診断ツールなど。

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



ガイドラインの全体構成

構 成		概 要
本 編	第1部 経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
	第2部 実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付 録	付録1 情報セキュリティ5か条	組織の規模を問わず必ず実行していただきたい重要な対策を5か条にまとめ説明しています。
	付録2 情報セキュリティ基本方針 (サンプル)	組織としての情報セキュリティに対する基本方針書のサンプルです。
	付録3 5分でできる！ 情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
	付録4 情報セキュリティハンドブック (ひな形)	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
	付録5 情報セキュリティ関連規程 (サンプル)	情報セキュリティに関する社内規則を文書化したもののサンプルです。
	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	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
	付録7 リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。
	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	情報漏えいやシステム停止などのインシデント対応のための手引きです。

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) 業務の停止
- (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」



(1) 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、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

(2) 実行すべき「重要7項目の取組」

- 経営者は、以下の7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

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

• 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

中小企業・小規模事業者の皆様へ

情報セキュリティ **5** か条

うちには秘密なんかないなあ・・・

いいえ、こんな情報があるはずですよ!

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から「取扱注意」として届かった情報

サイバー攻撃といっても、被害など知っているのでは?

漏れたら大変! こんなダメージが!

- 顧客への損害賠償などの支払い
- 取引停止、業務流出
- ネットの遮断などによる業務効率のダウン
- 従業員の高気象下

情報セキュリティ対策と言っても、何をやればいいのか分からない組織では、最初の5か条を守ることもからめましょう。

裏面をご覧ください

中小企業・小規模事業者の皆様へ

新 **5分** でできる!
情報セキュリティ自社診断

最新動向への対応、できてますか?

脅威や攻撃の変化 IT環境の変化

ランサムウェア IoT 監視 クラウド
パスワード リスト攻撃 スマートフォン

取り返しのつかないことになる前に
あなたの会社のセキュリティ状況を
「5分でできる! 自社診断」でチェック!

中小企業の情報セキュリティ対策ガイドライン 付録5
情報セキュリティ関連規程(サンプル)

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な規程を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。
※赤字部分は、自社の事情に依り内容(単語名、括弧書きなど)に変更してください。
※赤字部分は、自社の事情に依り本文を削除してください。

目次

1	総論的対策	1 ページ
2	人的対策	3 ページ
3	情報資産管理	5 ページ
4	アクセス制御及び認証	8 ページ
5	物理的対策	11 ページ
6	IT 機器利用	13 ページ
7	IT 基盤運用管理	21 ページ
8	システム開発及び保守	25 ページ
9	委託管理	27 ページ
10	情報セキュリティインシデント対応の並びに事業継続管理	34 ページ
11	社内体罰	39 ページ
12	個人情報及び特定個人情報取り扱い	40 ページ

(Ver.1.5)

1. 情報収集と共有
2. ウェブサイトの情報セキュリティ
3. クラウドサービスの情報セキュリティ
4. テレワークの情報セキュリティ
5. セキュリティインシデント対応
6. セキュリティサービス例と活用
7. 技術的対策例と活用
8. 詳細リスク分析の実施方法

SECURITY ACTION
★一つ星を宣言

SECURITY ACTION
★★二つ星を宣言

Step 1 情報セキュリティ 5か条

ガイドライン P.19

- 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！



中小企業・小規模事業者の皆様へ

情報セキュリティ **5** か条

ウチには秘密なんかいないなあ・・・

いいえ、こんな情報があるはずですよ！

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から“取扱注意”として預かった情報

サイバー攻撃といっても、被害など知れているのでは？

漏れたら大変！ こんなダメージが！

- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの滞断などによる業務効率のダウン
- 従業員の士気低下

情報セキュリティ対策と言っても、何をやれば良いのか分からない組織では、
裏面のか条を守るところから始めてみましょう。

裏面をご覧ください

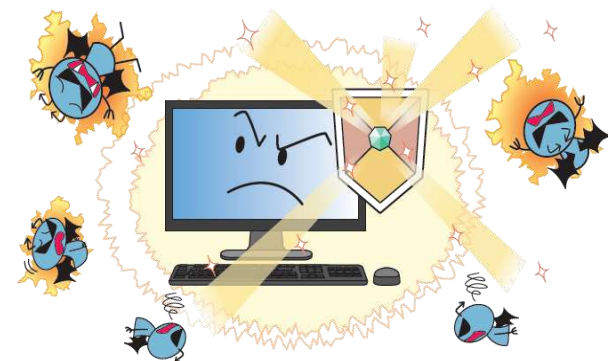
1. OSやソフトウェアは常に最新の状態に

- 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。



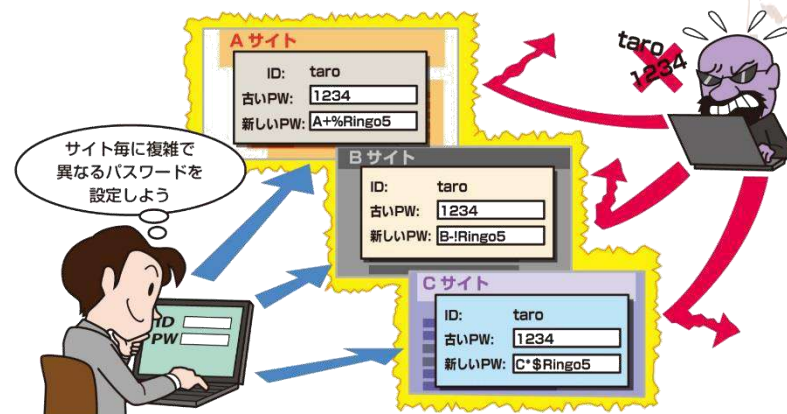
I P A（独立行政法人情報処理推進機構）の資料より引用

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。

ー <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



I P A（独立行政法人情報処理推進機構）の資料より引用

パスワードの管理

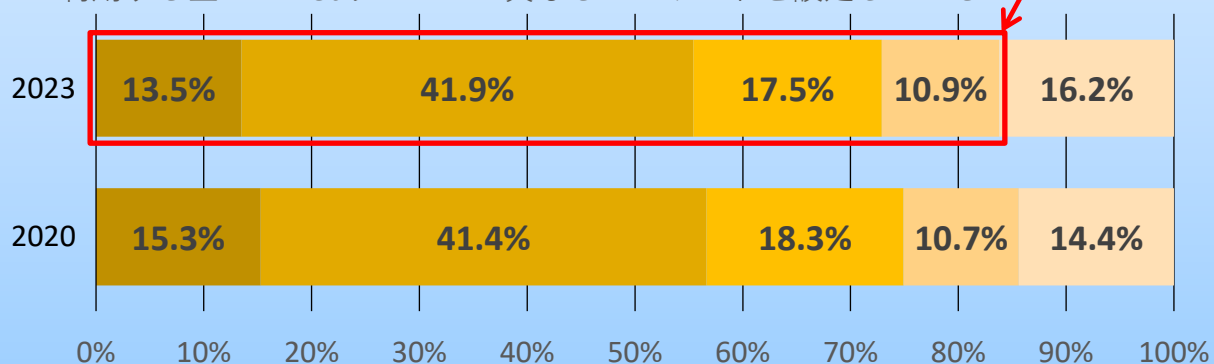
- 他者から見られる所にメモしない、保存しない。
- 複数のサービスで、同じパスワードを使い回さない。
- 漏えいしたり悪用された兆候が見られたら、直ちに変更する。
- サービス提供側で漏えい事故が発生したら、直ちに変更する。

パスワードの使い回しは84%

トレンドマイクロ「パスワードの利用実態調査 2023」 2023年8月

n=1,030

- 1種類のパスワードでほぼ全てのWebサービスを利用している
- 2~3種類のパスワードでほぼ全てのWebサービスを利用している
- 4~5種類のパスワードでほぼ全てのWebサービスを利用している
- 6種類以上のパスワードでほぼ全てのWebサービスを利用している
- 利用する全てのWebサービスで異なるパスワードを設定している

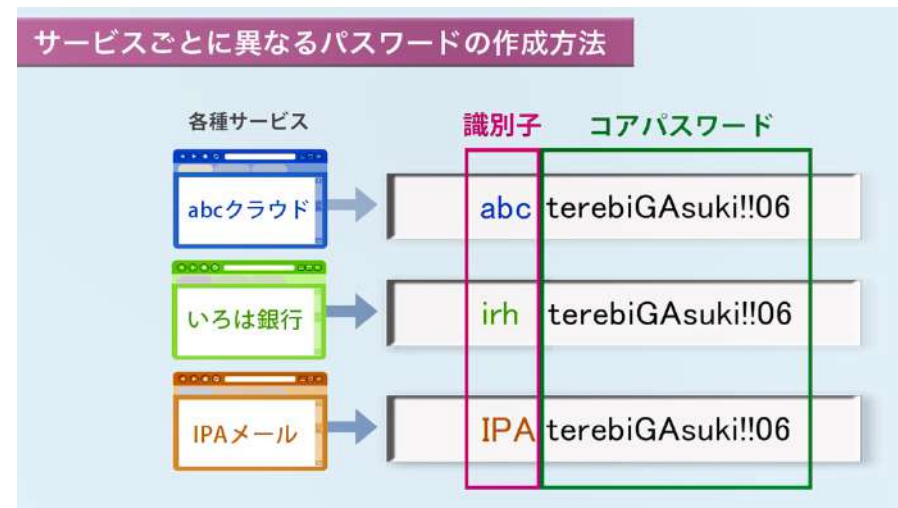


使い回しをしている

異なるパスワードを設定すると忘れてしまう	72.8%
異なるパスワードを考えるのが面倒	48.6%
使いまわしてもリスクはないと思っている	10.4%

強いパスワードの作り方

- IPA動画 「あなたのパスワードは大丈夫？」
 - <https://www.youtube.com/watch?v=IXh0b4KS9gE>
 - 複雑なパスワードの作成方法
 - 使い回しの回避のアイデア
 - 管理方法のヒント



- パスワード管理ソフト
 - 例 パスワードマネージャー
 - 例 ブラウザのパスワード管理機能



パスワード認証への攻撃とパスワード強化

• パスワード認証への攻撃（クラッキング）

– パスワードの推定

- ブルートフォース攻撃（総当たり）
- リバースブルートフォース攻撃（パスワードを固定してIDを変化。）
- 辞書攻撃（password、iloveyou）
- リスト攻撃（qwerty、1qaz2wsx）
- OSINT（例：SNS上の誕生日、趣味）

– パスワードの窃取

- フィッシング（偽サイト）
- キーロガー（スパイウェアの一種）
- ショルダーハッキング（暗証番号などでは要注意）
- 脆弱性の悪用（ソフトウェア、ファームウェアを最新にするしかない。）
- ソーシャルエンジニアリング

• IDとパスワードの漏えいの可能性の確認

- have i been pwned? <https://haveibeenpwned.com/>

• 強いパスワードを作るヒント

- パスフレーズ（好きな言葉（日本語）をローマ字にする）
- 文字置換（a → @, b → 6, g → 9, i → !、password → p@55vv0rcl）
- 文字追加（password → pass#word9）

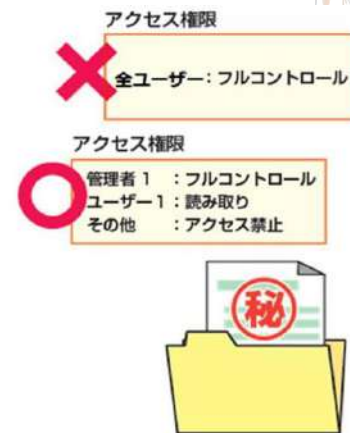
• リスクベースのパスワード選択

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。

ー <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

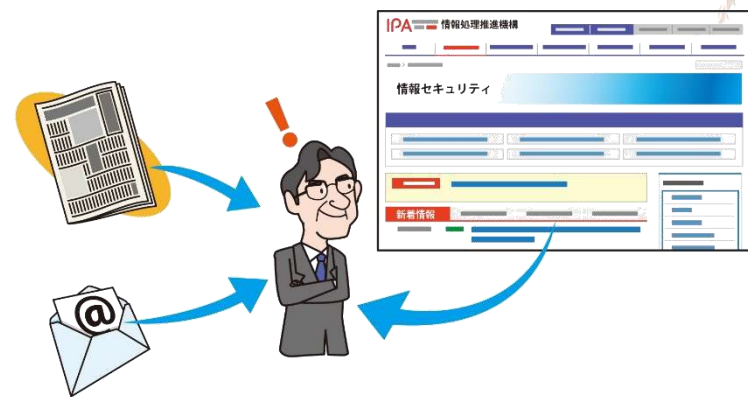


5. 脅威や攻撃の手口を知る

- 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。

ー <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
 - IPA 情報セキュリティ10大脅威
 - IPA 情報セキュリティ安心相談窓口 安心相談窓口だより
- 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

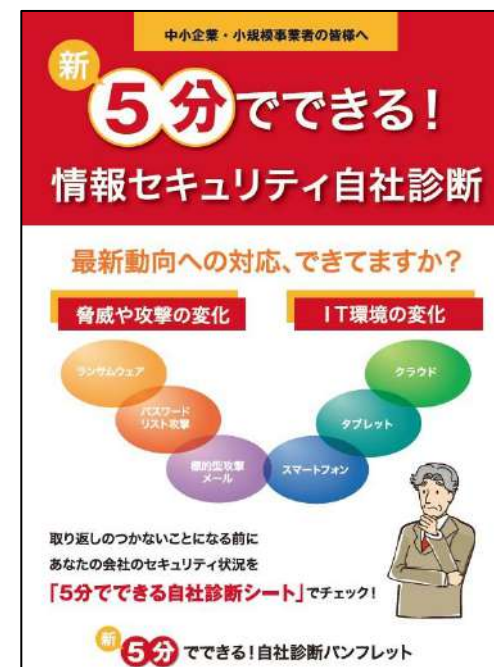


IPA（独立行政法人情報処理推進機構）の資料より引用

Step2 5分でできる！情報セキュリティ自社診断

ガイドライン P.20

- 自社の**セキュリティ対策状況を把握**するために「5分でできる！情報セキュリティ自社診断」を活用しましょう。
 - 25個の診断項目に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できます。
 - パンフレットで対策を学ぶことができます。
 - **ハンドブックひな形**を活用するとルールの社内周知ができます。



I P A（独立行政法人情報処理推進機構）の資料より引用

Step2 5分でできる！情報セキュリティ自社診断 診断項目

- 25個の診断項目に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できます。

- 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、教育、ルール化など

新 5分でできる自社診断シート 組織として最初に取組むべき情報セキュリティ対策の自社診断シート IPA

※診断の前に必ず裏面の□を印してください。
※下記の診断項目を読み、チェック欄の数値を記入してください。
※シートは、最終チェックは管理職の方から記入ください。
※「不明」については、すべての項目が実施されているかをお答えください。一部の記載事項が不明な項目については「不明」としてご記入ください。
※「不明」については、あなたのお力で実施したいのかをお答えください。
※チェックが終了したら裏面に自己診断結果を記入し、裏面のQRコードにアクセスください。

組織名
記入者名
実施年月日 年 月 日

診断項目	No.	診断内容	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	自己診断結果が正しくないと判断している項目
Part 1 基本的対策	1	Windows Updateを、おこなうようにし、常に最新ソフトウェアをインストールしていますか？	△	○	○	○	○
	2	パソコンからウイルスを削除ソフトを導入しウイルスを自動検知するソフトウェアをインストールして定期的にウイルスチェックをおこなっていますか？	△	○	○	○	○
	3	パスワードの定期的な変更、無関係な人にパスワードの提供、パスワードの共有を禁じていますか？	△	○	○	○	○
	4	パスワード管理ツール（パスワードマネージャ）を利用しパスワードを記憶していませんか？	△	○	○	○	○
	5	パスワード管理ツール（パスワードマネージャ）を利用しパスワードを記憶していませんか？	△	○	○	○	○
Part 2 従業員としての対策	6	「不明なメール」や「知らない宛先」からのメールを開かず、メールの送信元を確認して、送信元が不明な場合は削除していませんか？	△	○	○	○	○
	7	「不明なメール」や「知らない宛先」からのメールを開かず、メールの送信元を確認して、送信元が不明な場合は削除していませんか？	△	○	○	○	○
	8	「不明なメール」や「知らない宛先」からのメールを開かず、メールの送信元を確認して、送信元が不明な場合は削除していませんか？	△	○	○	○	○
	9	「不明なメール」や「知らない宛先」からのメールを開かず、メールの送信元を確認して、送信元が不明な場合は削除していませんか？	△	○	○	○	○
	10	「不明なメール」や「知らない宛先」からのメールを開かず、メールの送信元を確認して、送信元が不明な場合は削除していませんか？	△	○	○	○	○
	11	「不明なメール」や「知らない宛先」からのメールを開かず、メールの送信元を確認して、送信元が不明な場合は削除していませんか？	△	○	○	○	○
Part 3 組織としての対策	12	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
	13	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
	14	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
	15	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
	16	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
	17	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
	18	従業員が社外で使用するパソコンは、ウイルス対策ソフトをインストールしてありますか？	△	○	○	○	○
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	2	0	-1	
			4	2	0	-1	

※この自社診断シートで実施している対策が、IPAのガイドラインに準拠しているかどうかを確認するためのものではありません。

IPA（独立行政法人情報処理推進機構）の資料より引用

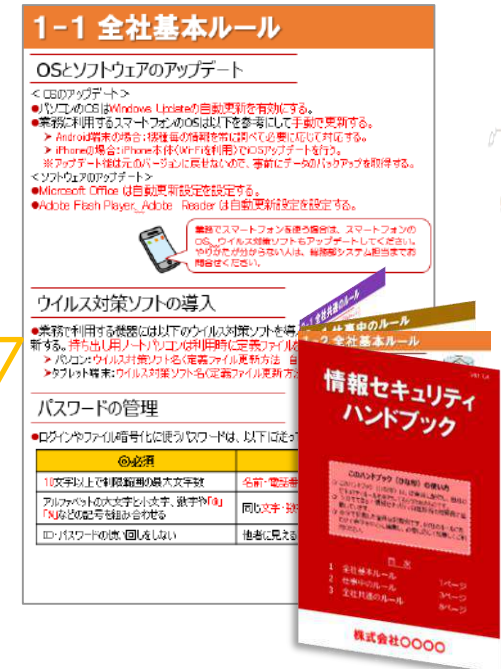
Step2 5分でできる！情報セキュリティ自社診断 診断後のステップ

- 問題のあった項目については、**解説パンフレット**を見て対策を検討しましょう。
- 従業員へ社内ルールを周知するために、「**情報セキュリティハンドブックひな形**」を活用しましょう。



解説パンフレットは、診断項目の解説と対策例を紹介

情報セキュリティハンドブックひな形は、企業によって修正する箇所を赤字、選択する箇所を青字で表記



I P A（独立行政法人情報処理推進機構）の資料より引用

Step3、 Step4

Step3 本格的に取り組む

- (1) 管理体制の構築
- (2) IT利活用方針と情報セキュリティの予算化
- (3) 情報セキュリティ規程の作成
- (4) 委託時の対策
- (5) 点検と改善

Step4 より強固にするための方策

- (1) 情報収集と共有
- (2) ウェブサイトの情報セキュリティ
- (3) クラウドサービスの情報セキュリティ
- (4) セキュリティサービス例と活用
- (5) 技術的対策例と活用
- (6) 詳細リスク分析の実施方法



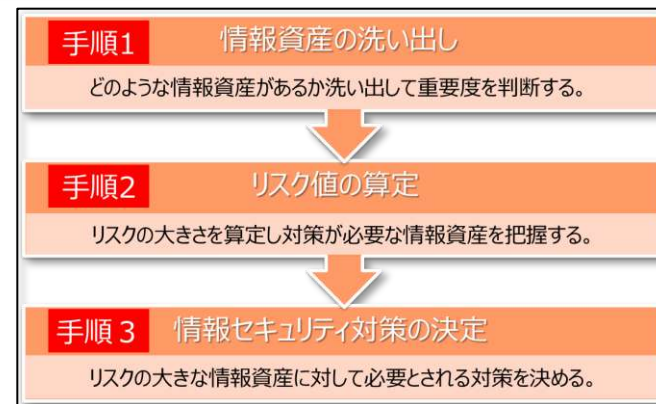
中小企業の情報セキュリティ対策ガイドライン 付録5

情報セキュリティ関連規程(サンプル)

中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。
※赤字箇所は、自社の事情に応じた内容(役職名、担当者名など)に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

目次

1	組織的対策	1ページ
2	人的対策	3ページ
3	情報資産管理	5ページ
4	アクセス制御及び認証	8ページ
5	物理的対策	11ページ
6	IT機器利用	13ページ
7	IT基盤運用管理	21ページ
8	システム開発及び保守	25ページ
9	委託管理	27ページ
10	情報セキュリティインシデント対応ならびに事業継続管理	34ページ
11	個人番号及び特定個人情報の取り扱い	40ページ



Step3 本格的に取り組む

(3) 情報セキュリティ規程の作成

ガイドラインP.26-27

1. 対応すべきリスクの特定

- 経営者が避けたい重大事故から、対応すべきリスクを特定。
- 外部状況：法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など。
- 内部状況：経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など。

2. 対策の決定

- リスクが大きなものを優先して対策を実施
 - いつ事故が起きてもおかしくない
 - 事故が起きると大きな被害になるなど
- リスクな小さなものは許容するなど、合理的に対応
 - 事故が起きる可能性が小さい
 - 発生しても被害が軽微であるなど



3. 規程の作成

- 「情報セキュリティ管理規程（サンプル）」を参考に、自社に適した規程にするために修正を加える
 - サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成
 - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記

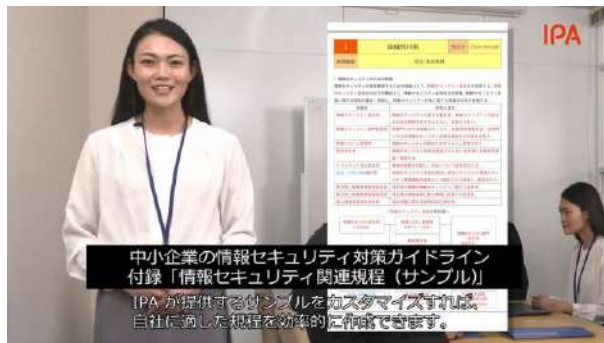
情報セキュリティ関連規程（サンプル）の概要

ガイドラインP.27

1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルールを定めます。
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルールを定めます。
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルールを定めます。
6	IT 機器利用	IT 機器やソフトウェアの利用などのルールを定めます。
7	IT 基盤運用管理	サーバーやネットワーク等のIT インフラに関するルールを定めます。
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルールを定めます。
9	委託管理	業務委託にあたっての選定や契約、評価のルールを定めます。委託先チェックリストのサンプルが付属します。
10	情報セキュリティインシデント対応 及び事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
11	テレワークにおける対策	テレワークのセキュリティ対策についてルールを定めます。

ハケンが解決！ 情報セキュリティ規程作成のポイント

<https://www.youtube.com/watch?v=fot-PEzBZO4>



3. 情報セキュリティ対策の進め方

3.1 (独) 情報処理推進機構 (IPA) による支援施策

- IPA 中小企業の情報セキュリティ対策ガイドライン
- IPAのその他の施策、ツール

3.2 その他の支援施策、支援者等

「SECURITY ACTION」 制度

<https://www.ipa.go.jp/security/security-action/>

「SECURITY ACTION」は中小企業自らが、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です。安全・安心なIT社会を実現するために創設されました。35万者を超える中小企業・事業者が宣言（2024年月6時点）。

情報セキュリティ5か条に取り組む

★ 一つ星



セキュリティ対策自己宣言



- ① OS・ソフトウェアの最新化（パッチ適用、バージョンアップ）
- ② ウィルス対策ソフトの導入
- ③ 強固なパスワード設定
- ④ データ等は必要最低限の人だけに共有
- ⑤ 攻撃の手口の把握

情報セキュリティ自社診断により自社の状況を把握し、「情報セキュリティ基本方針」を定め、外部に公開

★★ 二つ星

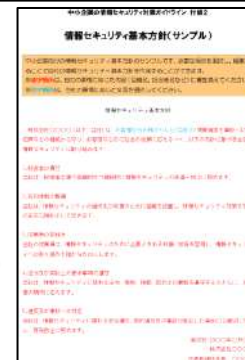


セキュリティ対策自己宣言



25の診断項目により自社の対策状況を把握

「情報セキュリティ基本方針」策定のサンプルも提供



「SECURITY ACTION」制度

SECURITY ACTIONロゴマーク

取組み段階に応じて2種類のロゴマークを提供。
従業員の意識を高め、対外的な信頼の向上に。

ロゴマークを、ポスター、パンフレット、名刺、封筒、
会社案内、ウェブサイト等に表示して、自社の取組みを
アピールしましょう。



IT導入補助金の申請要件になりました

SECURITY ACTION

- IT導入補助金とは、中小企業・小規模事業者等のみなさまが自社の課題やニーズに合ったITツール（ソフトウェア、サービス等）を導入する経費の一部を補助することで、みなさまの業務効率化・売上アップをサポートするものです。
- ITツールの導入時には、セキュリティ面を考慮することも重要です。また導入後も、情報セキュリティ対策の継続や向上をめざす取組みが重要です。
- IT導入補助金を申請するにあたっては**SECURITY ACTIONを宣言することが必須要件**となっています。

サイバーセキュリティお助け隊サービス

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



手遅れになるまえに、
手を打つ。



サイバーセキュリティ問題、起こる前に考えよう！

見守り

(異常の監視)

24時間365日監視
挙動や問題のある攻撃を
検知しあなたのPCと
ネットワークを守ります。

駆け付け

問題が発生したときに、
地域のIT事業者等が
駆け付け対応します。
(リモート支援の場合あり)

保険

簡易サイバー保険で、
駆け付け支援等インシデント
対応時に突発的に発生する
各種コストが補償されます。

ワンパッケージで安価に！

サイバーセキュリティお助け隊サービス サービス基準

- 異常の監視の仕組み（ネットワークまたは端末を24x7監視）
- 緊急時の対応支援（技術者派遣、若しくは、リモート対応）
- 中小企業でも導入・運用できる簡単さ
- 簡易サイバー保険（インシデント発生時の初動対応）
- 相談窓口（価格、契約、導入設置、運用）
- 上記機能のワンパッケージ提供
- 中小企業でも導入・維持できる価格等（1類サービス）
 - 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/端末1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
 - 初期費用が別途必要な場合は、それぞれ、50万円以下。

サービス利用料は、
IT導入補助金の支援
対象になります。
(最大2年分)

映像で知る情報セキュリティ

- 情報セキュリティに関する様々な脅威と対策を10分程度のドラマで分かりやすく解説した映像コンテンツをDVD、動画サイトで提供中



① YouTube IPA Channel 情報セキュリティ普及啓発映像コンテンツ

<https://www.youtube.com/playlist?list=PLF9FCB56776EBCABB>

② 映像で知る情報セキュリティ - 動画ファイル申込み

<https://www.ipa.go.jp/security/videos/download.html>



	<p><u>今、そこにある脅威～組織を狙うランサムウェア攻撃～</u> 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、データを一齐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。</p>	約15分
	<p><u>華麗なる情報セキュリティ対策</u> 「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ます。</p>	8話構成 各話2分

映像で知る情報セキュリティ ～ タイトル例

映像で知る情報セキュリティ

IPA

ドラマやデモンストレーションを通じて最新の脅威と対策を学びましょう！

企業・組織向け

研修に最適！

新作映像



今、そこにある脅威

～組織を揺るがすランサムウェア攻撃～
社員による内部不正で機密情報が外部に流出する危険が急増。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、不正を起させないポイントの他、自社における監査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

サイバー攻撃対策



今、そこにある脅威

～組織を揺るがすランサムウェア攻撃～
現代をとりまく脅威と各目的に企業・組織のネットワークへ侵入し、データを一度に暗号化して使用できなくしたりする「ランサムウェア」攻撃も、本件ではその攻撃の手口と対策などを解説しています。

約15分



What's BEC?

～ビジネスメール詐欺 手口と対策～
取引先などを装ったメールで担当者をだまし、攻撃者が用意した口座へ送金をさせるビジネスメール詐欺の手口と対策を説明します。

約12分



そのメール本当に信用してもいいですか?

～企業の標的型攻撃メールの手口と対策～
企業内の標的型攻撃メールの目録を奥手に、ウイルスが含まれている添付ファイルを開かせる手口を示し、その対策を説明します。

約10分



見えないサイバー攻撃

～標的型サイバー攻撃の組織的な対策～
標的型サイバー攻撃で組織的な対応ができなかったケースの再発ドラマを通じて、標的型サイバー攻撃の組織的な対策のポイントを説明します。

約13分

中小企業向け



あなたの会社のセキュリティドクター

～中小企業向け情報セキュリティ対策の基本～
中小企業の情報セキュリティ対策について、その必要性と今すぐに実施できる「情報セキュリティの見える化」について人間ドラマの解説に見立ててわかりやすく説明します。

約12分



ハケンが解決!

～情報セキュリティ問題の解決ポイント～
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問題の作成から運用までの手順をドラマ形式で説明します。

約12分

日常におけ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

「華麗なる情報セキュリティ対策」シリーズは、企業情報の安全確保のために立ち上がった社員と社員の物語です。組織の従業員が日常行うべき8つの対策をご紹介します。

全8話 各約2分

新入社員向け



3つのかばん

～新入社員が知るべき情報漏えいの脅威～
情報セキュリティ新人研修で以上に言及された3つのカバン、その一つも開くたびに、主人公は組織には守るべき重要な情報があることをまざまざと知ることとなる。

約11分

その他：■「あなたの組織が阻んでいる!～標的型攻撃その脅威と対策～」 ■「今 制敵システムも狙われている!～情報セキュリティの必要性～」 等

映像で知る情報セキュリティ

IPA

ドラマやデモンストレーションを通じて最新の脅威と対策を学びましょう！

共通・一般向け

各映像約10分

情報セキュリティ対策の基本



子ブタと学ぼう!

情報セキュリティ対策のキホン
基本的な情報セキュリティ対策5項目を紹介するアニメーション形式のショートムービー集です。社内研修や啓発イベント等でご利用ください。

全5話 各15～18秒

手口検証動画シリーズ



不在通知の偽SMS

IPA情報セキュリティ安心確認窓口では、寄せられる相談の手口を実施に検証し、その様子も「手口検証動画シリーズ」として公開しています。

全9話 各48秒～4分28秒

不正ログイン対策



あなたのパスワードは大丈夫?

～インターネットサービスの不正ログイン対策～
インターネットサービスを利用するに当たり、ログイン用のパスワード設定で注意すべきこと、更には不正ログイン対策に非常に有効な2段階認証について説明します。

約10分

ネット接続機器のセキュリティ



消費者のためのネット接続機器の安全な選定・利用ガイド

ネットに接続する製品を購入する際により安全な製品を選ぶための確認ポイントと購入した製品を安全に利用するためのポイントをそれぞれ解説。

全2話 各約3分

偽警告



その警告メッセージ、信じて大丈夫?

～ブラウザの偽警告にご用心～
突然「ウイルスに感染したかもしれない」など不安を煽る警告メッセージが表示される。通称「偽警告」の手口と対策について説明します。

約11分

ワンクリック詐欺



検証! スマートフォンのワンクリック請求

①検証! スマートフォンのワンクリック請求
②ワンクリック請求のフナを知ろう!
～巧妙化する手口とその対策～
ワンクリック請求の巧妙な手口やフナにからかわないための予防策や心づかいを詳しく解説します。

各約10分

SNSの心得



あなたの書き込みは世界中から見られてる

～適切なSNS利用の心得～
ケーキ屋でアルバイト中の女子高生美子、つい無気味なSNSに投稿した写真が流出してネットに炎上。近づくモンスターが襲撃し、SNSを安全に利用する心得について学びます。

約11分

青少年の保護者向け



はじめまして、ペアコです。

～親と子のスマホの約束～
保護者が子どもの安全のためにスマートフォン等の設定を調整する「ペアレンタルコントロール」について、解説動画「ペアコ」さんがポイントを絞って説明します。

約12分

小学生向け



キミはどっち?

小学生がインターネットを利用する上で守るべきマナーや自分の個人情報の扱い、さらにはウイルス対策について、アニメでわかりやすく説明します。

約9分

中高生向け



ほんとにあったセキュリティの話

仲良しの3人組が友人・知人の実話をこっそり紹介しています。中高生が気をつけるべき脅威とその対策をドラマを通して学びます。

約9分

視聴方法

YouTubeで視聴

情報セキュリティ普及啓発推進コンタクト (ipajp)

ダウンロード

IPAサイトからお申込みください。一部映像を除く。

IPAサイトからお申込みください。

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



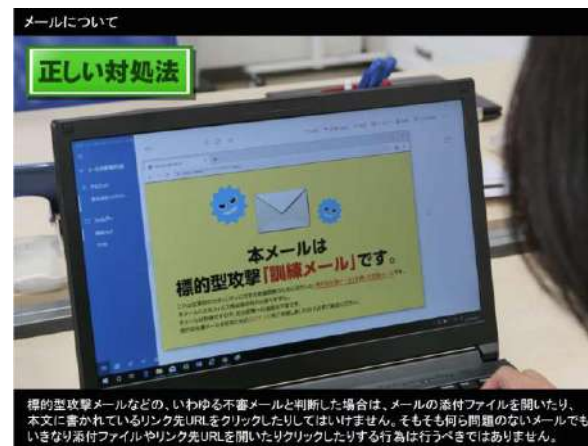
IPA 政府特命機関
情報処理推進機構
〒113-8501 東京都文京区本郷2-7-12 情報処理推進機構
本部2階 (110号) 10号室
E-mail: ipasec@ipajp.go.jp

2024.1 Version 12.0

5分でできる!!情報セキュリティポイント学習

<https://security-shien.ipa.go.jp/learning/index.html>

- 「5分でできる! 情報セキュリティポイント学習」は、中小企業で働く方を対象とした、**1テーマ5分**で情報セキュリティについて勉強できる**学習ツール**です。
- 職場の日常の1コマを取り入れた親しみやすい学習テーマで、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**を学ぶことができます。



確認テスト 問題

No.4 メールについて
～標的型攻撃メールへの対処と対策～

Q1

標的型攻撃メールの対策の説明として、適切でないものはどれか。

選択肢	
<input type="radio"/>	1. ウイルス対策ソフトをインストールして使用する。
<input type="radio"/>	2. 不審なメールか分からないので、周りの人にもメールを見せて確認してもらう。
<input type="radio"/>	3. 本当に送ったのかを確認するため、送り主に確認の返信をしてみる。
<input type="radio"/>	4. 本当に送り主が送ったのか確認が取れるまで、添付されているファイルは開かない

次のページで正解と解説を確認しましょう

3. 情報セキュリティ対策の進め方

3.1 (独) 情報処理推進機構 (IPA) による支援施策

- IPA 中小企業の情報セキュリティ対策ガイドライン
- IPAのその他の施策、ツール

3.2 その他の支援施策、支援者等

NISC インターネットの安全・安心ハンドブック

<https://security-portal.nisc.go.jp/guidance/handbook.html>

- 内閣サイバーセキュリティセンター（NISC）製作。
- みんなが安心して使えるネット社会を実現するためには、その時々サイバーセキュリティに関する正しい知識を身に付け、実行するとともに、家族や友人など身の回りの人達にも伝えていくことが大切です。
- サイバーセキュリティに関する基本的な知識を紹介し、誰もが最低限実施しておくべき基本的なサイバーセキュリティ対策を実行してもらうことで、更に安全・安心にインターネットを利活用してもらうことを目的に制作したものです。

プロローグ インターネットにある基本的なリスクやトラブルを知ろう

第1章 まずはサイバーセキュリティの基礎を固めよう

第2章 よくあるサイバー攻撃の手口やリスクを知ろう

第3章 SNS・ネットとの付き合い方や情報モラルの重要性を知ろう

第4章 災害・テロ、海外でのトラブル、普段とは違う環境のリスクに備えよう

第5章 スマホやパソコン、IoT機器を安全に利用するための設定を知ろう

第6章 パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう

第7章 【中小組織向け】セキュリティ向上が利潤追求につながることを理解しよう

付録 知っておくと役立つサイバーセキュリティに関する手引き・ガイダンス

おわりに インターネットとよい付き合いを続けるために



インターネットの安全・安心ハンドブック

第7章【中小組織向け】セキュリティ向上が利潤追求につながることを理解しよう

- 1 社内・社外のセキュリティを向上しよう
 - 1.1 セキュリティ対策を実施して負のコストを発生させない
 - 1.2 セキュリティ対策に必要な投資資金を確保する
- 2 災害時の会社のために事業継続計画(BCP)を作ろう
 - 2.1 打たれ強くあるために、どこでも作業できる能力
 - 2.2 人的損失をリカバリする能力
- 3 テレワークとアウトソーシングをうまく利用しよう
 - 3.1 テレワークとBYOD-Bring Your Own Device
 - 3.2 効率的なアウトソーシング
- 4 ファイルの共有設定や情報の公開範囲を見直そう
- 5 企業が気を付けたいサイバー攻撃を知り、情報収集に心掛けよう
 - 5.1 脅威や攻撃の手口を知ろう
 - 5.2 より能動的に情報収集しよう
- 6 企業が気を付けたい乗っ取りのリスクを理解しよう
 - 6.1 サプライチェーン攻撃やオフショア開発によるリスク
 - 6.2 問題が起きると事業継続に影響を及ぼす
- 7 企業が気を付けたいサイバー攻撃の具体例を知ろう
 - 7.1 標的型メール攻撃の具体例
 - 7.2 フィッシング攻撃の傾向
 - 7.3 不正アクセスの傾向
 - 7.4 不正送金の傾向
 - 7.5 ランサムウェアの傾向
 - 7.6 ウェブサービスへの不正ログイン
 - 7.7 ウェブサイトの改ざんやSNSの乗っ取り
 - 7.8 DDoS攻撃
 - 7.9 サイバーセキュリティ以前の情報モラル教育を怠らない
- 8 個人情報法律に則り適切に取り扱おう
- 9 フリー素材の取扱と著作権について注意しよう
- 10 取引先の監督を徹底しよう

サイバーセキュリティ関係法令 Q&A ハンドブック

https://security-portal.nisc.go.jp/guidance/law_handbook.html

- 内閣サイバーセキュリティセンター（NISC）作成。
- 企業における平時のサイバーセキュリティ対策及びインシデント発生時の対応に関する法令上の事項に加え、情報の取扱いに関する法令や情勢の変化等に伴い生じる法的課題等を可能な限り平易な表記で記述しています。
- **Ver. 2.0** 2023年1月1日時点の法令等を基準としている

1. サイバーセキュリティ基本法関連
2. 会社法関連（内部統制システム等）
3. インシデント対応関連総論（当局等対応、関係者対応）
4. 個人情報保護法関連
5. 不正競争防止法関連
6. 労働法関連（秘密保持・競業避止等）
7. 情報通信ネットワーク関連（IoT関連等を含む）
8. 契約関連（電子署名、システム開発、クラウド等）
9. 資格等（情報処理安全確保支援士等）
10. その他各論（リバースエンジニアリング、暗号、情報共有、脅威インテリジェンス、データ消去等）
11. インシデント対応関連（事後的対応等）（ランサムウェア対応、デジタル・フォレンジック、サイバー保険等を含む）
12. 民事訴訟手続
13. 刑事法（サイバー犯罪等）
14. 海外法令（GDPR等）

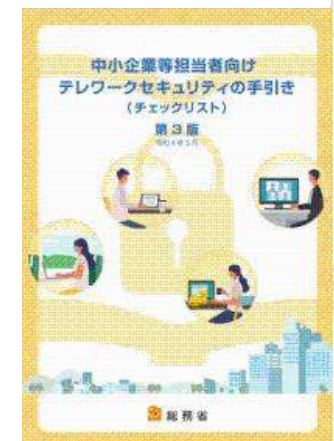
総務省

政策

- [国民のためのサイバーセキュリティサイト](#)
- [ICTサイバーセキュリティ総合対策](#)
- [IoT・5Gセキュリティ総合対策](#)
- [テレワークセキュリティガイドライン](#)
 - [テレワークセキュリティガイドライン（第5版）](#)
 - [中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第3版）](#)
- [タイムスタンプ・eシール](#)
- [スマートシティセキュリティガイドライン（第2.0版）](#)

組織等

- [サイバーセキュリティ統括官室](#)
 - [サイバーセキュリティタスクフォース](#)
- 研究開発法人情報通信研究機構（NICT） [サイバーセキュリティ研究所](#)（研究開発、サイバー演習）
- [ICT-ISAC](#)
 - 通信事業者（ISP含む）、放送事業者、ベンダ（セキュリティ、ソフトウェア、機器、SIer）
 - 脅威情報の情報共有基盤



警察庁/警視庁/警察本部

警察庁 National Police Agency

警視庁について お知らせ 政策

ホーム > 各部署から > サイバー警察局

サイバー警察局

個別事案への対策

- > ランサムウェア被害防止対策
- > Emotet対策
- > フィッシング対策
- > 不正アクセス対策
- > ウェブサイト改ざん対策
- > 有料サイトの料金請求に注意
- > サポート詐欺対策
- > 「偽サイト」「詐欺サイト」に注意!
- > インターネットオークション・フリマサイト利用時のトラブル相談
- > インターネット上の違法情報・有害情報への対策
- > インターネット上の誹謗中傷への対応
- > インターネット上における犯行予告への対応
- > 基本的なセキュリティ対策
- > ビジネスメール詐欺に注意!

警視庁

安全な暮らし 交通安全 相談・お悩み 手続き

トップページ > 安全な暮らし > サイバーセキュリティインフォメーション

サイバーセキュリティインフォメーション

- 注目情報
 - > スマホで詐欺被害にあわないために。「スマホ防犯教室」
 - > 知って防ごう「ネット詐欺」! 犯罪者のメールやネットで騙されない!
 - > メタバース空間内に警視庁サイバーセキュリティセンターを設置
 - > サイバーセキュリティ人材の育成に関する産学官連携協定締結及び1周年記念行事を実施
 - > Emotet(エモテット)感染を疑ったら
 - > マルウェア[ランサムウェア]の脅威と対策 (脅威編)
 - > マルウェア[ランサムウェア]の脅威と対策 (対策編)
 - > 「ライブ配信を騙るフィッシング詐欺」に注意!
 - > テレワーク勤務のサイバーセキュリティ対策!
 - > サイバーセキュリティ学習用ボードゲーム
 - > サイバー空間をめぐる脅威の脅威について
- 被害者・加害者にならないために
 - > 家庭用ルーターの不正利用に関する注意喚起について
 - > インターネットバンキング不正送金被害の防止対策
 - > ポットネット対策
 - > 個人情報流出防止
 - > 守っていますか? ルールとマナー
 - > チート行為はやめましょう!
 - > 違法・有害情報を専門機関に通報
- セキュリティ対策
 - > 個人向けセキュリティ対策
 - > 管理者向けセキュリティ対策
 - > IDとパスワードの適切な管理
 - > Wi-Fi (無線LAN) ルーターをお使いの方へ
 - > スマートフォンを利用している方へ
 - > フィッシング110番
 - > クレジットカード不正利用被害対策
 - > パスワードの再発行機能を悪用した不正アクセスに注意!
 - > 関連リンク集 (個人の方)
 - > 関連リンク集 (中小企業の方)

神奈川県警察 Kanagawa Prefectural Police

警察の紹介 暮らしの安全情報 交通安全 各種相談 採用情報

ホーム > 暮らしの安全情報 > サイバー犯罪

サイバー関連ポータルサイト

更新日: 2024年06月05日

サイバー犯罪 セキュリティ対策 安全教育 各種資料 リンク集

サイバー犯罪

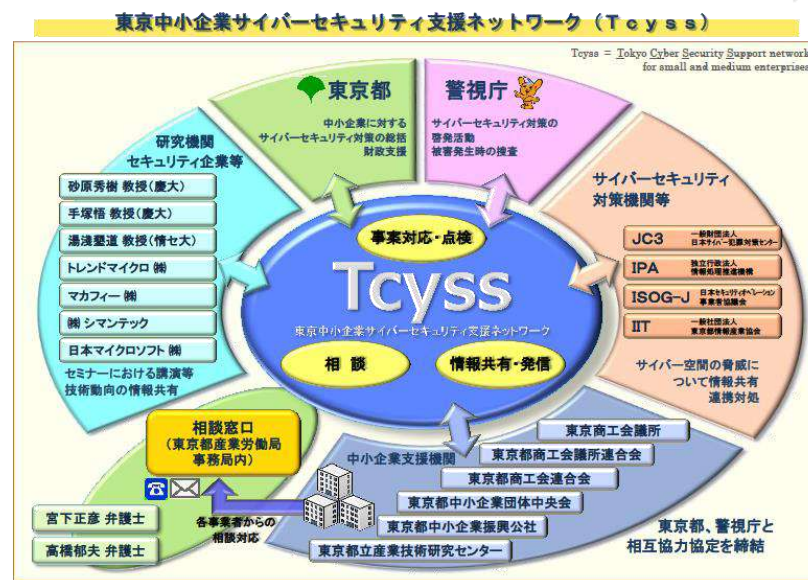
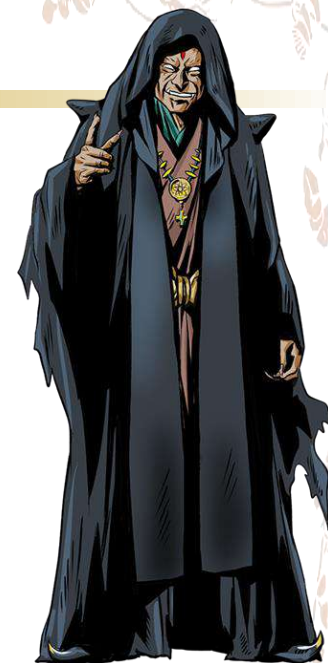
- ・インターネット上の違法情報・有害情報
- ・リベンジボルトについて
- ・児童ポルノについて
- ・インターネットを利用したねずみ講
- ・サイバーセキュリティに関する相談について

セキュリティ対策

- ・情報セキュリティスクエアインターネットを安全・安心に利用するために
- ・すべてのモノにサイバーセキュリティ
- ・Free Wi-Fi (公衆無線LAN) 利用時・提供時のポイント

自治体

- 東京都 (産業労働局)
 - 中小企業向けサイバーセキュリティ対策の極意
 - サイバーセキュリティ相談窓口
 - サイバーセキュリティ対策促進助成金
 - 中小企業サイバーセキュリティ向上支援事業
 - 中小企業サイバーセキュリティ対策強化サポート事業
 - 東京中小企業サイバーセキュリティ支援ネットワーク (Tcyss)
 - 東京都、警視庁
 - 中小企業支援機関 (商工団体等)
 - サイバーセキュリティ対策機関
 - セキュリティベンダ
 - 有識者



支援者 (人数等は2024年8月現在の各組織公表値)

- 登録セキスペ（情報処理安全確保支援士）
 - サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うとともに、必要に応じその取組の実施の状況についての調査、分析及び評価を行い、その結果に基づき指導及び助言を行う。（国家資格）
 - <https://riss.ipa.go.jp/>
 - 22,572人（全国）
- セキュリティプレゼンター
 - IPAのセキュリティ対策資料等を活用して、中小企業等に対して情報セキュリティの普及啓発を行う。（登録制）
 - https://www.ipa.go.jp/security/sme/presenter/eid2eo0000002r6h-att/presenter_list.pdf
 - 約1,800人（全国）、476人（東京都）
内 情報処理安全確保支援士 743人（全国）、222人（東京都）
- ITコーディネータ（ITC）
 - 経営に役立つIT利活用に向け、経営者の立場に立った助言・支援を行い、IT経営を実現する人材。（経済産業省推進資格）
 - <https://itca.force.com/ITCPPProfileSearchPage>
 - 約7,000人（全国）／内 情報処理安全確保支援士 285人（全国）
- 情報処理支援機関（スマートSMEサポーター）
 - 中小企業者等の生産性向上・経営基盤強化に資するITツールを提供するITベンダ等。（認定制）
 - <https://smartsme.secure.force.com/smartsmesearch/>
 - 1,192社（全国）、371社（東京都）



本日のまとめ

- 情報セキュリティの脅威
 - どのようにして情報セキュリティ事故が起きるのかを**知ることが重要**。
 - どのような脅威（攻撃、犯罪手口、うっかりミス）があるのか。脆弱性は何か。
- 情報セキュリティの目的
 - 情報を使って、個人は生活を、組織は活動をしている。この**営みを保証**（事業継続）すること。
 - 自組織にとって重要な業務、情報は何か。
 - 情報セキュリティ対策とは、**リスク**の大きさ（起きたときの影響×起こり易さ）を減らすこと。
- 先ずは基本的な対策を**徹底**する。（ベースライン・アプローチ）
 - 政府機関や業界団体等が提供しているガイドライン、ツールなどを活用する。（例：「中小企業の情報セキュリティ対策ガイドライン」）
 - 様々な支援機関の支援施策や、支援者を活用する。

ご清聴ありがとうございました。

