Security Days Fall 2025
～実践的なワークショップで学ぶ！中小企業向け サイバーセキュリティ対策入門～

2025年10月24日（A00版）

一般社団法人首都圏産業活性化協会

自己紹介

- 小川 直樹(おがわ なおき)

  一般社団法人 首都圏産業活性化協会
  地域DX促進事業プロジェクトリーダー

- 保有資格・公職
  - ITコーディネータ
  - 経済産業省登録　中小企業診断士
  - 公認情報システム監査人(CISA)
  - 情報処理推進機構　情報処理技術者試験委員

首都圏産業活性化協会(TAMA協会)の概要

設立

1998年　関東経済産業局の呼びかけにより、
「TAMA産業活性化協議会」（任意団体）設立

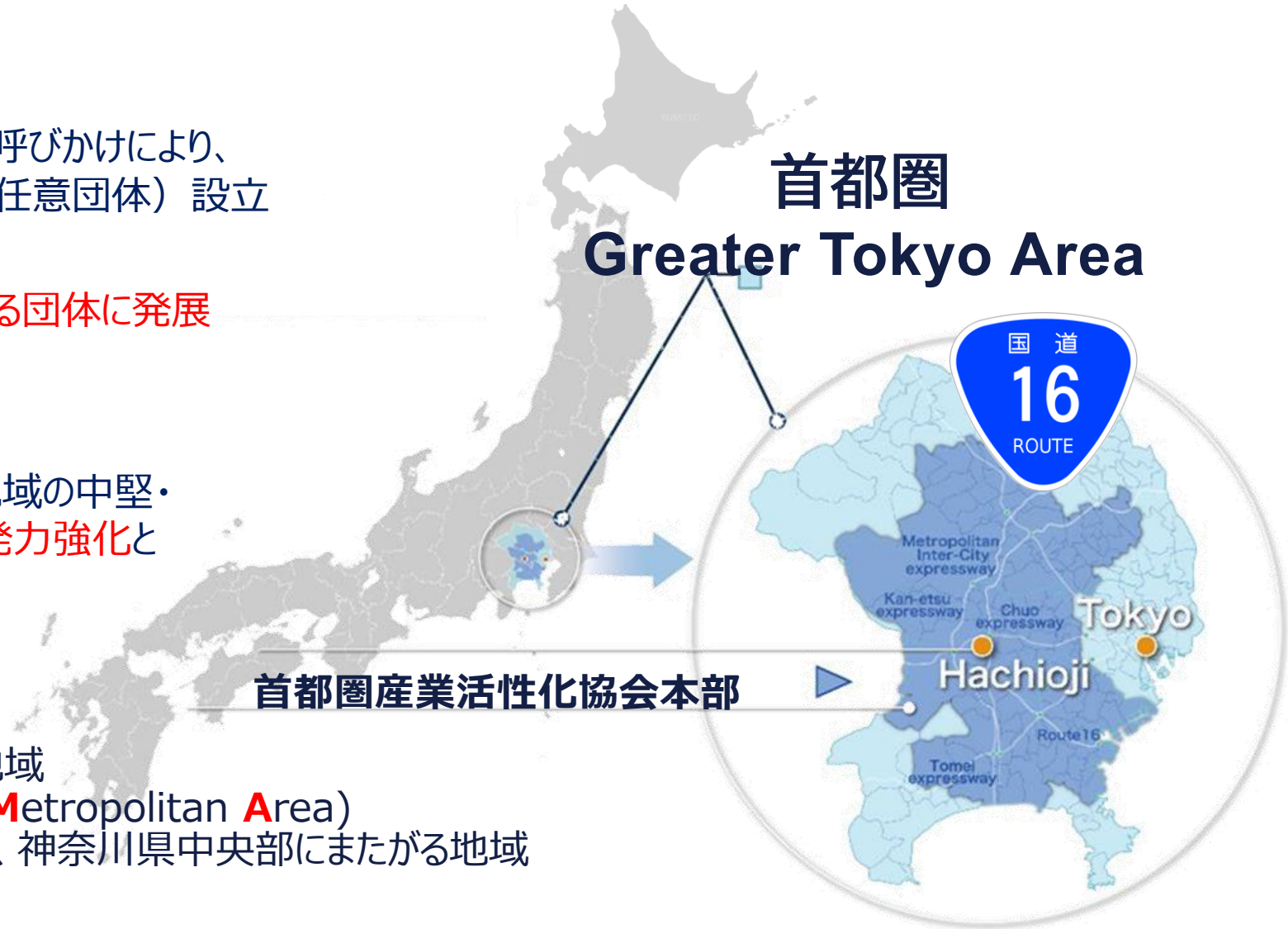
2001年に法人化
企業や大学などの連携を促進する団体に発展

ミッション

産学官の強固な連携の下で、地域の中堅・
中小企業の製品・サービスの開発力強化と
市場拡大、新規創業環境整備

活動地域

■ **ＴＡＭＡ**　技術先進首都圏地域
(**T**echnology　**A**dvanced **M**etropolitan **A**rea)
埼玉県南西部、東京都多摩地区、神奈川県中央部にまたがる地域



目次

- 今、知っておくべきサイバーセキュリティの最新情報
- 【ワーク】情報セキュリティ自社診断
- 具体的にどうやるのか？
- 情報セキュリティハンドブックの紹介
- まとめ

今、知っておくべき
サイバーセキュリティの最新情報

イントロダクション

このセクションの概要

1. 中小企業にとっても他人事ではないサイバーセキュリティの脅威
2. どんな脅威があるのか？
    - ランサムウェア攻撃
    - サプライチェーン攻撃
3. 【ワーク】 情報セキュリティ自社診断

セキュリティといえば情報漏洩でしょう？

うちには守るべき情報なんて大したものないよ？

営業や生産活動を止めないために必要

- 情報漏洩ではなく「営業や生産活動を止めないために」必要です
- 「ランサムウェア」による攻撃は業務を停止させます
  - 右図はIPA（情報処理推進機構：経産省所管）の公表しているセキュリティリスクのランキングです
  - ランサムウェアは4年連続の1位です
  - 「業務を再開したければ身代金（ransom）をよこせ」と脅されます

2024	2023	2022	組織の脅威
1位	1位	1位	ランサムウェアによる被害
2位	2位	3位	サプライチェーンの弱点を悪用した攻撃
3位	4位	5位	内部不正による情報漏えい
4位	3位	2位	標的型攻撃による機密情報の窃取
5位	6位	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	9位	10位	不注意による情報漏えい等の被害
7位	8位	6位	脆弱性対策情報の公開に伴う悪用増加
8位	7位	8位	ビジネスメール詐欺による金銭被害
9位	5位	4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
10位	10位	NEW	犯罪のビジネス化（アンダーグラウンドサービス）

引用：情報セキュリティ10大脅威 2024：IPA 独立行政法人 情報処理推進機構

アサヒGHD サイバー攻撃被害の概要

発生確認日時
2025年9月29日 午前7時頃

攻撃の種類

ランサムウェア
（ハッカー集団Qilinが犯行声明）

被害の経過

9/29
システム障害確認、全社システム遮断

9/29-10/5
受注・出荷・生産停止状態が継続

10/6
社外からの電子メール一部復旧
手作業での限定受注開始

現在
復旧のメド立たず
情報漏洩の可能性を確認

社内への影響

全30工場の生産停止
ビール全6工場の操業停止
受注・出荷業務の一斉停止
コールセンター業務停止
メールを含む情報システム遮断

取引先への影響

セブン・ファミマでPB商品出荷停止
松屋での「スーパードライ」販売休止
新商品12品の発売延期
小売店・外食・卸への広範な配送遅延

競合他社への波及

キリン・サントリー・サッポロで出荷制限
受注殺到による在庫調整の必要性

被害規模の統計

30	6
全工場生産停止	ビール工場操業停止
12	7+
新商品発売延期	影響日数（継続中）

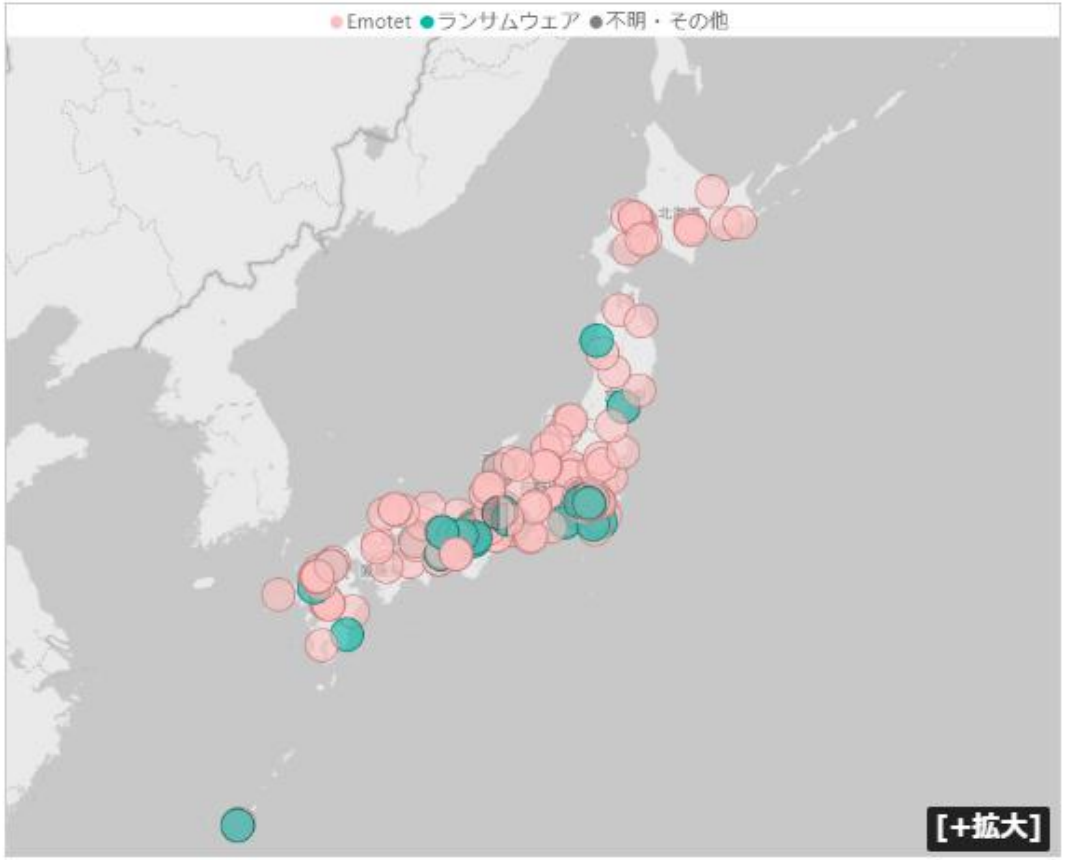
復旧対応状況

大きな企業だから狙われた？

うちは狙われるような大した企業じゃないよ？

サイバー攻撃は無差別攻撃です

- 攻撃する側は、攻撃先を特に調査せずに攻撃してきます
  - 攻撃に成功してから調べます
- 右図は「マルウェア感染」の発生した組織の所在地をマーキングしたものです
  - 全国にわたって攻撃されています
  - 業種も企業規模も関係ありません

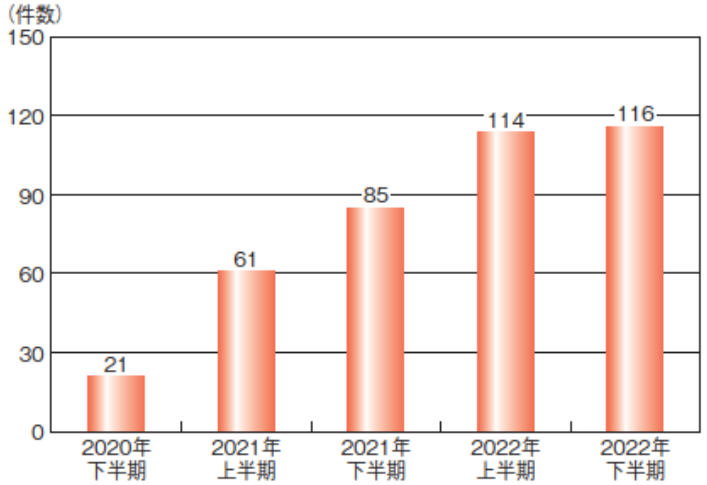


【図4】「マルウェア感染」被害組織の所在地

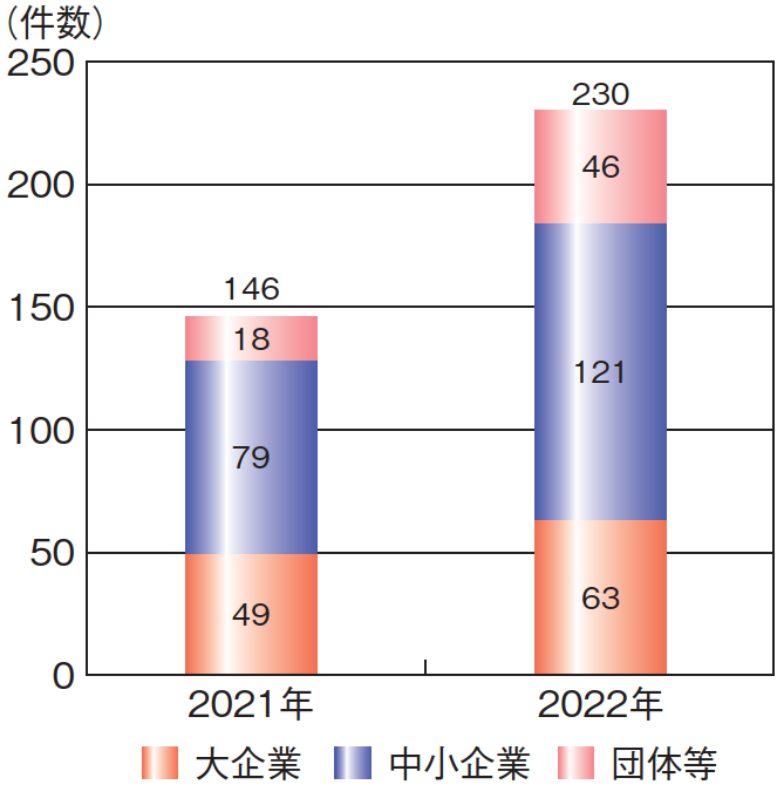
引用：[2023年1月公開]過去3年分の国内セキュリティインシデント集計 | Digital Arts Security Reports | デジタルアーツ株式会社（daj.jp）

中小企業のランサムウェア被害件数も増えています

- 被害は企業、団体等の規模を問わず広範に及んでいる。
- 中小企業の被害件数も前年比53.2%増。



企業・団体等のランサムウェア被害の報告件数の推移
(出典)情報セキュリティ白書2023



企業規模別ランサムウェア被害の報告件数の推移
(出典)情報セキュリティ白書2023

サイバー攻撃の被害は自社にとどまらなくなる

- 2022年3月1日、トヨタの全国の生産ラインが停止しました
  - 下請工場がサイバー攻撃を受けた影響です
  - 理由は部品供給不足ではなく、「下請工場を経由してトヨタ本体も狙われる可能性があるから」（同部品を供給する下請工場はほかにもあった）

ホーム ＞ ニュース ＞ 経済

トヨタ、きょう国内全工場を停止…部品メーカーがサイバー攻撃受けた可能性

2022/03/01 00:00　この記事をスクラップする

トヨタ自動車は２８日、３月１日に国内全１４工場２８ラインの稼働を停止すると発表した。部品メーカーのシステム障害で、部品の供給を受けられなくなった。サイバー攻撃を受けた可能性があるという。トヨタは２日以降の稼働については、状況を見て判断するとしている。

トヨタ自動車本社

現時点で原因は特定されていない。岸田首相は２８日、トヨタ自動車の稼働停止について、「実態を確認させている。ロシアとの関係等についても、しっかりと確認した上でなければ答えることは難しい」と首相官邸で記者団に語った。

システム障害が起きたのは、樹脂部品などを製造する小島プレス工業（愛知県豊田市）。同

引用：トヨタ、きょう国内全工場を停止…部品メーカーがサイバー攻撃受けた可能性：読売新聞（yomiuri.co.jp）

サプライチェーン攻撃

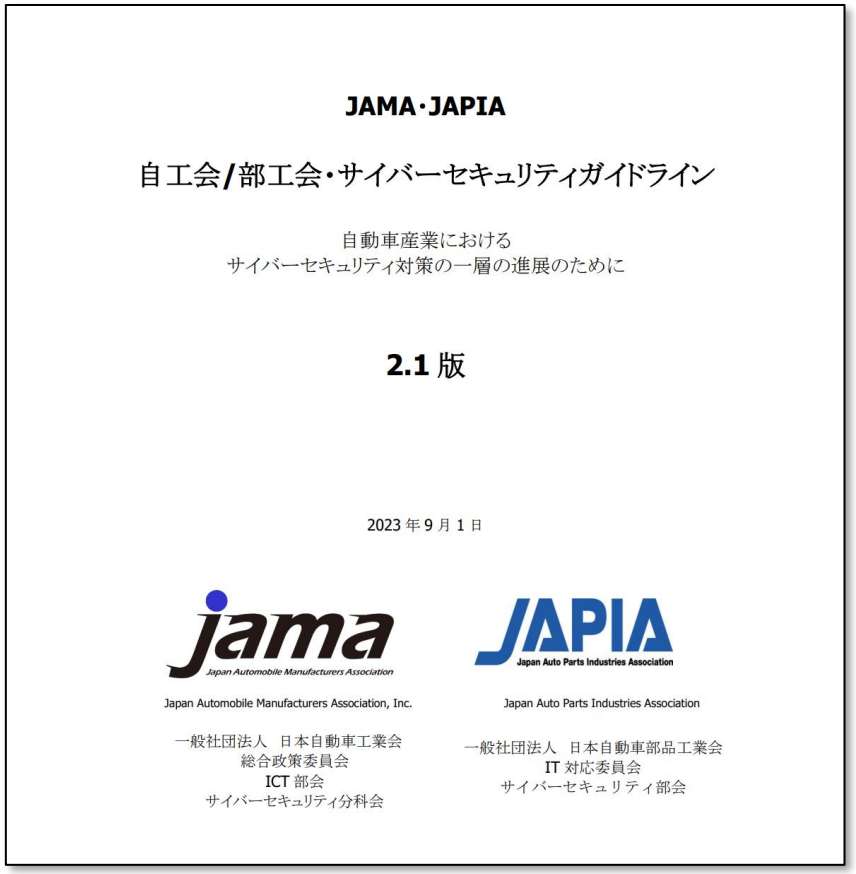
- 下請から親事業者を狙う攻撃を「サプライチェーン攻撃」と言います
  - サプライチェーン＝供給連鎖
- 前述の10大脅威の2位です
  - 1位と2位の組み合わせでトヨタの生産ラインは止まりました
- 親事業者に損害を与えた場合、取引停止、損害賠償のリスクがあります。

2024	2023	2022	組織の脅威
1位	1位	1位	ランサムウェアによる被害
2位	2位	3位	サプライチェーンの弱点を悪用した攻撃
3位	4位	5位	内部不正による情報漏えい
4位	3位	2位	標的型攻撃による機密情報の窃取
5位	6位	7位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6位	9位	10位	不注意による情報漏えい等の被害
7位	8位	6位	脆弱性対策情報の公開に伴う悪用増加
8位	7位	8位	ビジネスメール詐欺による金銭被害
9位	5位	4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
10位	10位	NEW	犯罪のビジネス化（アンダーグラウンドサービス）

引用：情報セキュリティ10大脅威 2024：IPA 独立行政法人 情報処理推進機構

今後、ビジネスの場に参加する要件になる

- 自動車業界では業界団体のガイドラインによって、業界内での役割ごとに遵守すべきセキュリティレベルを定めています
  - 満たさなければ業界から弾かれることでしょう
- 他業界についても、サイバーセキュリティの要求は強くなる方向になるでしょう（弱まることはありません）



JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.1 版

2023 年 9 月 1 日

jama
Japan Automobile Manufacturers Association

Japan Automobile Manufacturers Association, Inc.

一般社団法人　日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会

JAPIA
Japan Auto Parts Industries Association

Japan Auto Parts Industries Association

一般社団法人　日本自動車部品工業会
IT 対応委員会
サイバーセキュリティ部会

引用：自工会/部工会・サイバーセキュリティガイドライン（jama.or.jp）

情報セキュリティ自社診断

自社のセキュリティ状態の確認

- セキュリティ対策を講じるための第一歩として、「自社のセキュリティ状態がどの程度なのか」を理解することが必要です。
- そこで、お勧めしたいのが、独立行政法人情報処理推進機構（IPA）が提供する「5分でできる情報セキュリティ自社診断」です。

引用：情報処理推進機構（IPA）「5分でできる！情報セキュリティ自社診断」

診断結果1

Part 1 基本的対策

No.1～5は企業の規模や形態を問わず、必ず対策していただきたい5項目です。いずれも一度やればよいものではなく、継続的な対策実施が欠かせないため、運用ルールとして社内に定着させる必要があります

/20 点

「必ず対策していただきたい5項目」

Part 2 従業員としての対策

No.6～18は従業員として注意すべき項目です。重要情報を日々扱っていると慣れによる人為的ミスが発生しやすくなります。また、脅威の形が日々変化しているので、油断しないように注意する必要があります。

/52 点

Part 3 組織としての対策

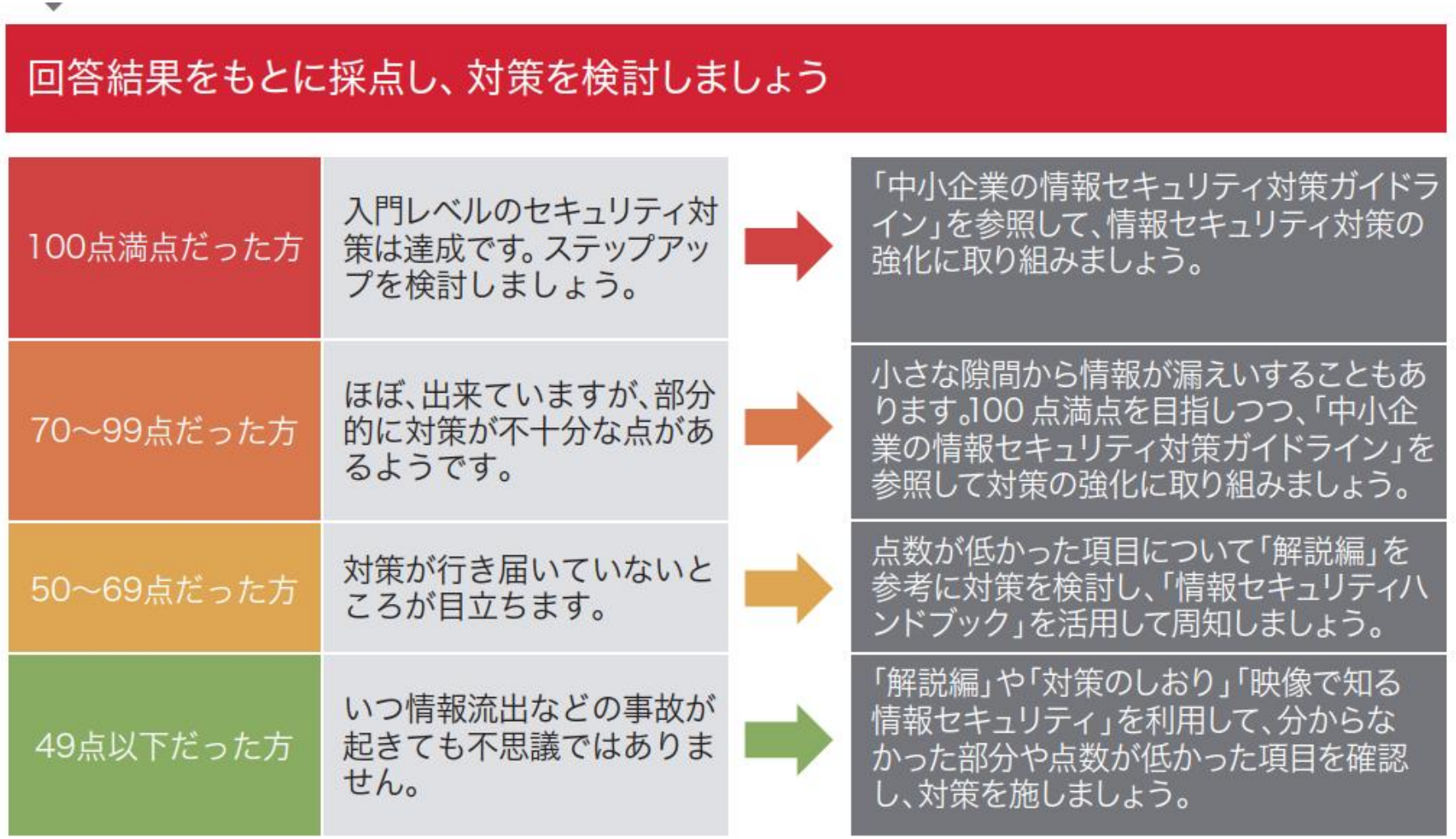
No.19～25は組織としての方針を定めた上で、実施すべき対策です。情報セキュリティのルールは明文化して社内で共有することにより、従業員の意識を高めるようにしましょう。

/28 点

/100 点

引用：情報処理推進機構(IPA)「5分でできる！情報セキュリティ自社診断」

診断結果　解説



引用：情報処理推進機構(IPA)「5分でできる！情報セキュリティ自社診断」

「一番弱いところ」を底上げします

- 「桶の理論」と呼ばれます
- 桶は最も低いところから水が漏れます
- サイバーセキュリティも最も低いところから破られます
- 最も低いところをカバーするだけでも効果を見込めます

具体的にどうやるのか？

イントロダクション

このセクションの概要

1. 中小企業の情報セキュリティ対策ガイドラインの紹介
2. 情報セキュリティ5か条の徹底
3. 5か条に追加：生成AI導入時の留意事項
4. 情報セキュリティハンドブックの紹介

そうはいってもよくわからんよ

まず、何から始めれば良いのかわからん

ガイドラインを
使いましょう

「中小企業の情報セキュリティ対策ガイドライン」の活用のススメ

- 中小企業向けガイドラインが情報処理推進機構(IPA)から出ています。
- 「中小企業の情報セキュリティ対策ガイドライン」の内容
  - 経営者向け

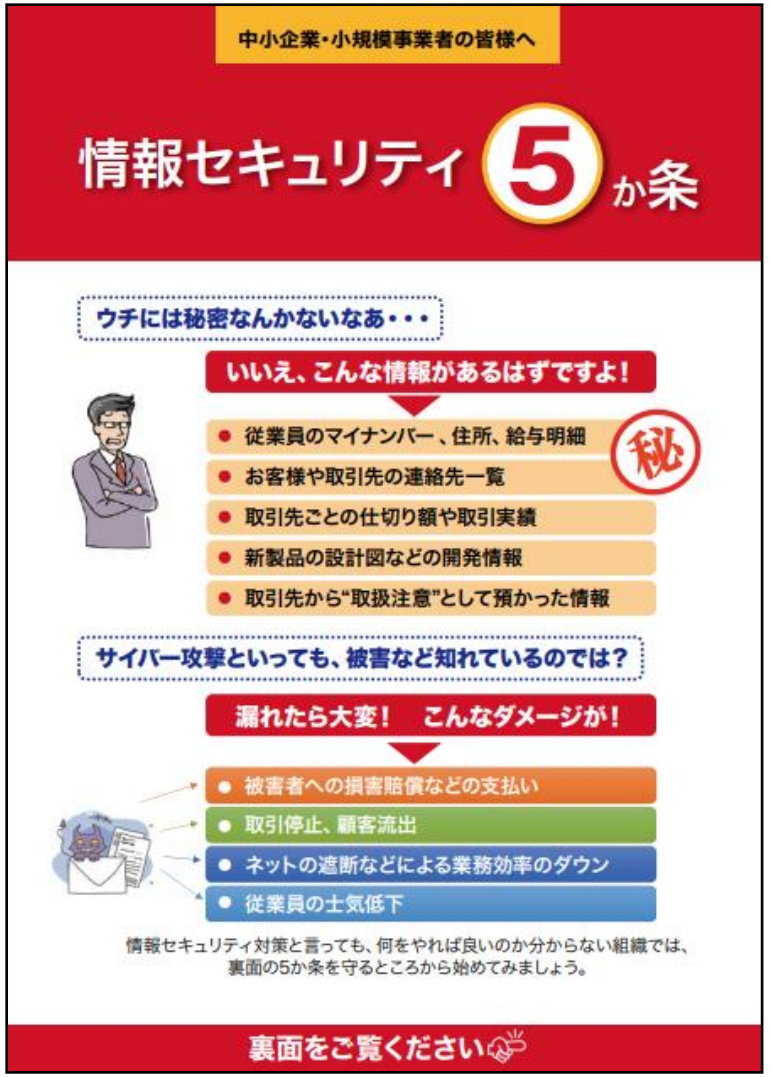
    経営者が認識すべき責任
  - 実務者向け

    情報セキュリティ対策の実務的な進め方

引用:中小企業の情報セキュリティ対策ガイドライン｜情報セキュリティ｜
(https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf)

情報セキュリティ5か条の徹底

- まず、5カ条に関して、自社での徹底方法を決めてください。
- その上で、パンフレットを従業員に配るだけでも、ある程度の効果が見込めます。
- 徹底して取り組むと、5か条だけでも結構なセキュリティ強化を見込めます



No.1 OSやソフトウェアは常に最新の状態にする

- OSやソフトウェアにはセキュリティパッチが公開されています
- 攻撃側からすると、パッチは「ここに脆弱性があります」という情報になります
- そのため、最新版ではないソフトは攻撃されやすい状態です
- 最新版にすることで、最新の攻撃手法以外は受けにくくなります

OSとソフトウェアのアップデート　情報セキュリティハンドブックの記載例

＜OSのアップデート＞

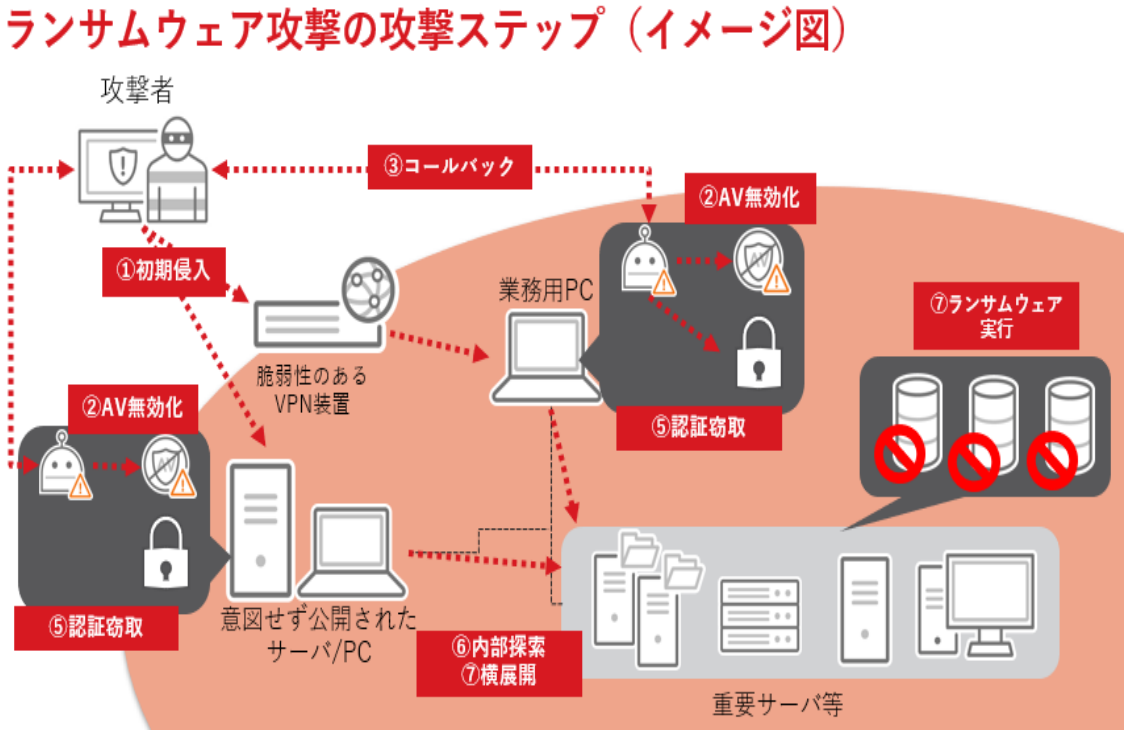
- PCのOSはWindows Updateの自動更新を有効にして最新の更新プログラムをインストールした状態にする。
- 業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。
  - Android端末の場合：機種毎の情報を常に調べて必要に応じて対応する。
  - iPhoneの場合：iPhone本体（Wi-Fiを利用）でiOSアップデートを行う。

＜ソフトウェアのアップデート＞

- Windowsの更新時に他のMicrosoft製品の更新プログラムも入手しインストールした状態にする。
- Adobe Flash Player、Adobe Reader はアップデートを自動に設定する。

【事例】OSやソフトウェアの更新を怠ることによるリスク

- 名古屋港コンテナターミナルのランサムウェア被害（2023年）
- 原因：保守作業に利用するVPN装置のソフトウェアの更新が見落とされていた
- 対策：システムの脆弱性を修正するためのアップデートとセキュリティパッチの適用を徹底



トレンドマイクロ社ホームページより
https://www.trendmicro.com/ja_jp/jp-security/23/g/securitytrend-20230710-01.html

No.2 ウィルス対策ソフトを導入し適切に利用する

- ウィルス対策ソフトを使うことで、攻撃がやってきたときにアラートが上がり、異変に気づきやすくなります。
  - 特にメール添付ファイルやダウンロードファイル
- 長期間未使用だったPCを再び利用する際は、ウィルス対策ソフトが最新状態か確認する必要があります。

ウィルス対策ソフトの導入

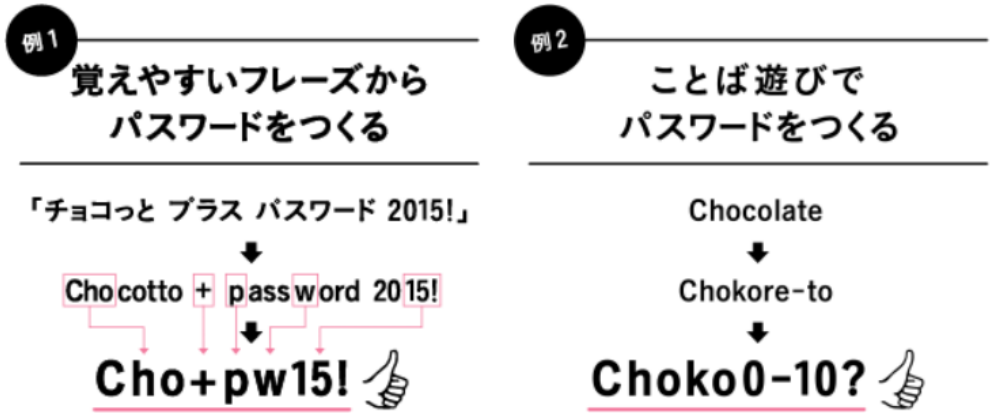
情報セキュリティハンドブックの記載例

- 業務で利用するPCには以下のウィルス対策ソフトを導入し、定義ファイルを随時更新する。
- 持ち出し用ノートPCは利用時に定義ファイルの更新を確認する。

情報機器の種類	順守事項
PC	• OS・ソフトウェアはインターネットに接続した状態で自動更新を有効にして最新の更新プログラムを導入すること。 • ウィルス対策ソフトの定義ファイルは自動で更新すること。 • 社内標準外ソフトウェアのインストールは禁止すること。
スマートフォン	• 指定されたMDM(モバイル機器管理)エージェントをインストールし、データの暗号化や遠隔でのデータ消去等の対策を行うこと。※MDMについては、2025年4月以降、導入を検討する。 • OSは以下を参考にして自動で更新すること。 Android端末の場合:機種毎の設定画面で自動システムアップデートを選択する。 iPhoneの場合:デバイスの自動アップデートを有効にする • アプリを導入する際は、公式のマーケットを利用すること。

No.3 強固なパスワードを使用する

- 最低12文字以上とも言われます
  - 生成AIでパスワード解読　半数を1分で解析、米社調査 - 日本経済新聞（nikkei.com）
- 12文字も覚えられませんが、ちょっとの工夫ですこしだけ強化できます
  - チョコっとプラスパスワード｜IPA 独立行政法人 情報処理推進機構



※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。

パスワードの管理

情報セキュリティハンドブックの記載例

●ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

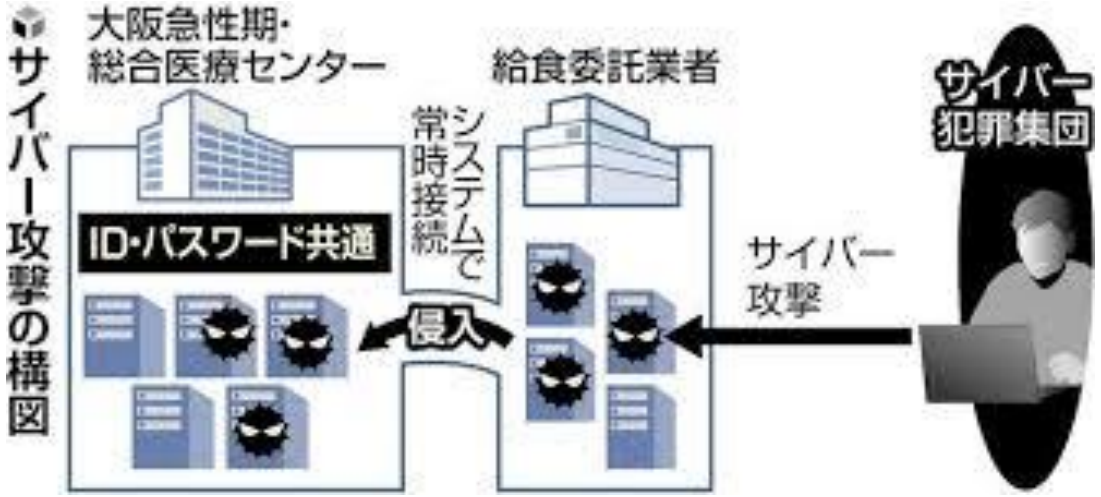
◎必須	×禁止
12桁以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない
アルファベットの大文字と小文字、数字や「@」、「%」、「&」などの記号を組み合わせる	同じ文字・数字を連ねただけにしない
ＩＤ・パスワードの使い回しをしない	他者に見えるところに記さない/教えない

【事例】弱いパスワードが引き起こすリスク

- 大阪急性期･総合医療センターの
  ランサムウェア被害（2023年）

- 原因： 電子カルテの管理用IDとパスワードが使い回しされていた。電子カルテシステムのサーバーには、負荷を軽くするため、ウィルス対策ソフトが設定されていなかった。

- 対策：使い回されていたパスワードを全て異なるものに変更し、ウィルス対策ソフトを設定



読売新聞オンラインより
https://www.yomiuri.co.jp/national/
20230329-OYT1T50114/

No.4 共有設定を見直す

- PCのフォルダ共有設定を間違えて行っている場合、外出先で覗き見られることがあります
  - PCの設定確認はすこし難しく、PCに詳しい従業員に作業指示しましょう
- 業務を楽にするために、必要以上に共有権限を付与している場合があります
  - PC設定ではなく業務ルールの問題なので、ルールの見直しが必要です

利用者アカウントの管理　情報セキュリティハンドブックの記載例

- 利用者の業務・職務に応じた必要最低限のアクセス権を付与する。
- 利用者アカウントは、情報セキュリティ部門責任者の承認に基づき登録する。
- 利用者アカウントが不要になる場合、情報セキュリティ部門責任者は、当該アカウントの削除または無効化する。
- 利用者アカウントは、原則、利用者1名につき1つを発行する
- 複数の利用者が共有するアカウントを発行する場合は、事前にシステム管理者の承認を得る。
- 極秘情報を含む重要な企業機密情報および個人情報は、PCに保管せずにサーバに保管する。

No.5 脅威や攻撃の手口を知り、対策に活かす

- いわばKY（危険予知）するための情報リテラシーを身に着けることです。
- 生成AIの登場によって、標的型攻撃メールのリスクが高まっています。
- IPAがたくさんの教育コンテンツを発信していますので、それをもとに従業員への注意喚起を定期的に実施してください。
  - 映像コンテンツ一覧（IPA）
  - 5分でできる！ポイント学習（IPA）
  - 情報セキュリティ対策支援サイト（IPA）

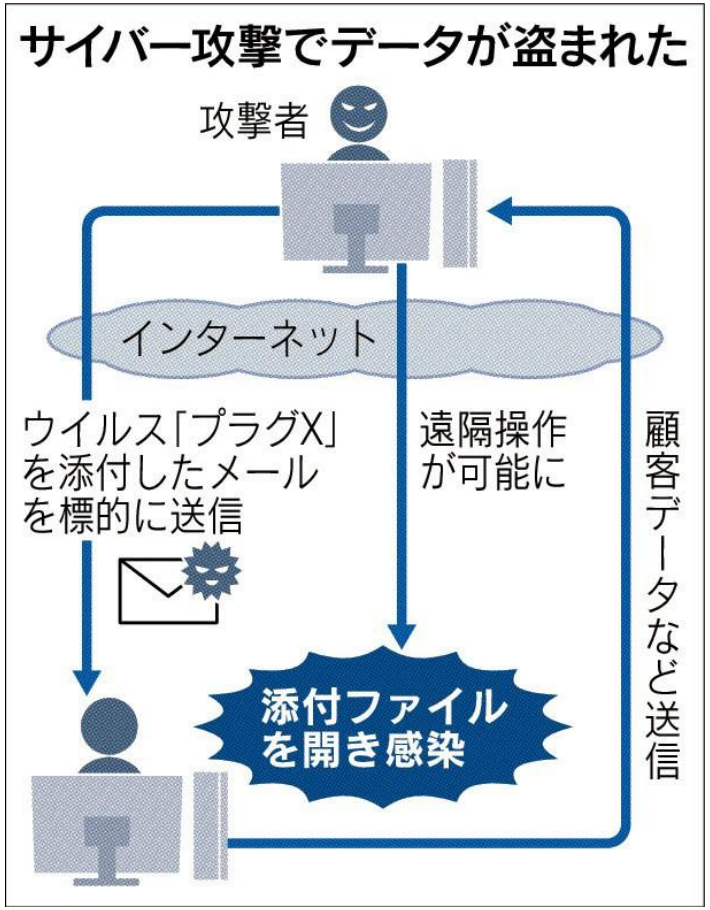
標的型攻撃メール対策　情報セキュリティハンドブックの記載例

＜ウイルス感染の防止＞
標的型攻撃メールによるウイルス感染を防止するため以下の内容に複数合致する場合は十分に注意し、安易に添付ファイルを開いたり、リンクを参照したりしない。

- メールのテーマ（件名・見出し）
  ①知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容
  ②心当たりのないメールだが、興味をそそられる内容
  ③これまで届いたことがない公的機関からのお知らせ
  ④組織全体への案内
  ⑤心当たりのない決済や配送通知
  ⑥ID やパスワードなどの入力を要求するメール
- 差出人のメールアドレス
  ①フリーメールアドレスから送信されている
  ②差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる

【事例】従業員の情報リテラシーが低いことによるリスク

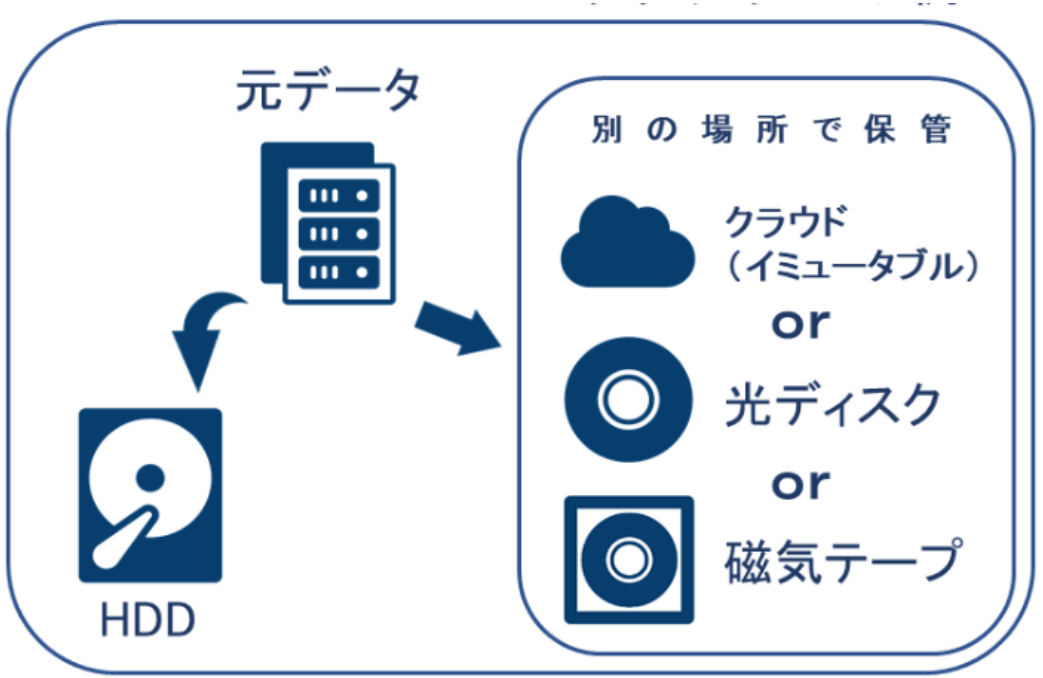
- JTBの顧客情報漏洩（2016年）
  フィッシングメールにより約793万人の顧客情報が漏洩する事件が発生
- 原因：従業員が不正なメールのリンクをクリックしてしまい、マルウェアがインストールされた
- 対策：フィッシングメール対策として、従業員教育を強化し、不正アクセス防止のためにシステムの強化



日経新聞より
https://www.nikkei.com/article/DGXZZO03723210X10C16A6000000/

【5箇条に追加】バックアップを強化しよう！

- ランサムウェア攻撃に備えて、バックアップ用の外部記憶装置はバックアップ時以外は物理的に接続しない
- 業務データだけではなく、システムの稼働に必要な設定ファイルやプログラムも含める
- 潜伏期間を持つランサムウェアに備えて、最新だけではなく、過去の複数の地点に復旧できるようする
- バックアップはエラーゼロで完了



引用：大阪府警察「ランサムウェアにご注意！」

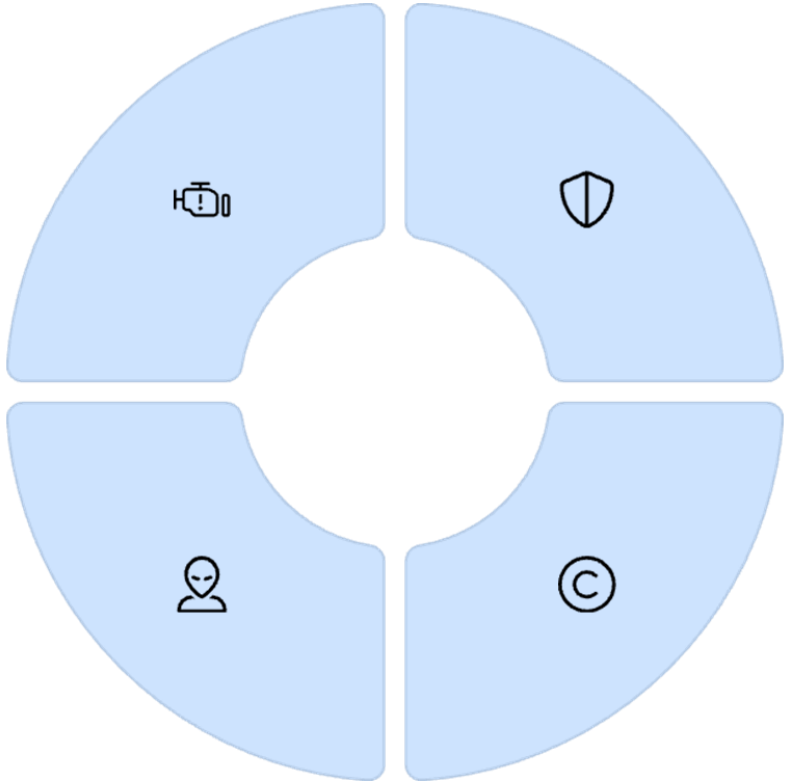
【5箇条に追加】生成AI導入時の留意点

ハルシネーション

AI生成コンテンツには事実と異なる情報（幻覚）が含まれることがあります。必ず人間が確認しましょう。

人間との役割分担

AIは道具であり、最終判断は人間が行うべきです。適切な役割分担を考えましょう。



情報セキュリティ

機密情報や個人情報を入力する際は、適切なセキュリティ対策が施されたツールを使用しましょう。

著作権問題

AI生成コンテンツの著作権や法的責任は明確になっていない部分があります。利用規約を確認しましょう。

個人アカウントでは必ず実施して欲しいオプトアウト設定

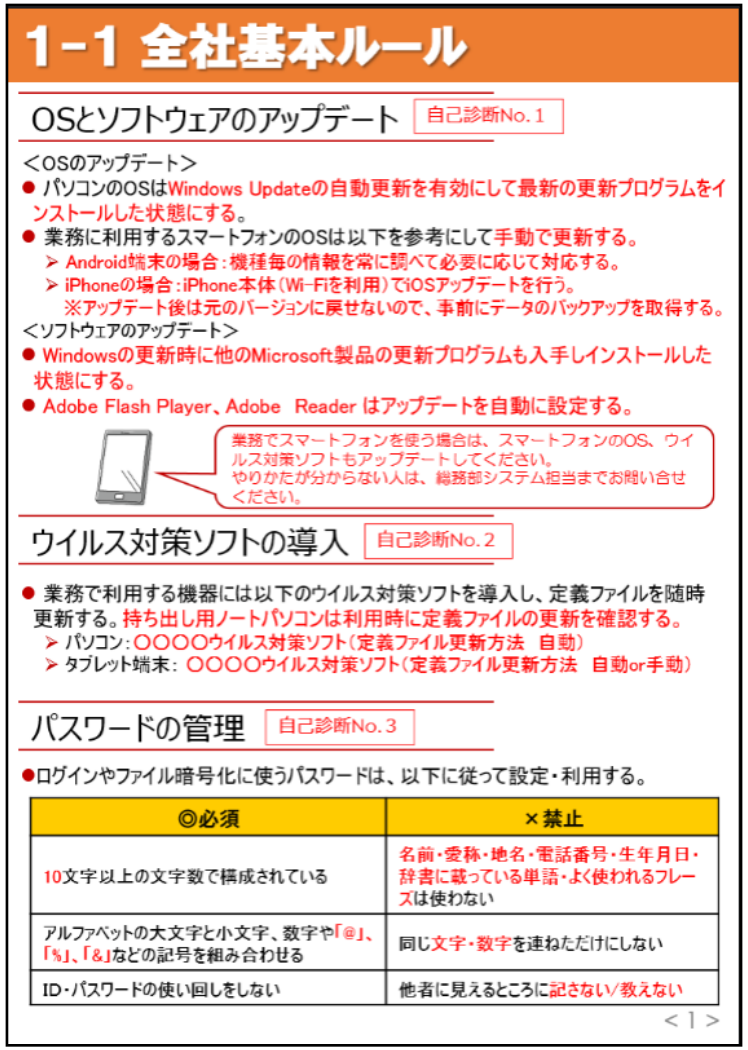
個人アカウントのデフォルトの状態は、入力された
個人情報や機密情報が、生成AIの学習に使われます。
下記の手順で、必ず「オプトアウト設定」を行ってください。

従業員向けハンドブックの紹介

- 情報セキュリティハンドブック

  https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000108033.pptx

  - 全従業員にルールを作業レベルで周知するものです
- これを自社に合うようにカスタマイズしましょう



1-1 全社基本ルール

OSとソフトウェアのアップデート　自己診断No. 1

＜OSのアップデート＞
- パソコンのOSはWindows Updateの自動更新を有効にして最新の更新プログラムをインストールした状態にする。
- 業務に利用するスマートフォンのOSは以下を参考にして手動で更新する。
  - Android端末の場合：機種毎の情報を常に調べて必要に応じて対応する。
  - iPhoneの場合：iPhone本体（Wi-Fiを利用）でiOSアップデートを行う。
    ※アップデート後は元のバージョンに戻せないので、事前にデータのバックアップを取得する。

＜ソフトウェアのアップデート＞
- Windowsの更新時に他のMicrosoft製品の更新プログラムも入手しインストールした状態にする。
- Adobe Flash Player、Adobe Reader はアップデートを自動に設定する。

業務でスマートフォンを使う場合は、スマートフォンのOS、ウイルス対策ソフトもアップデートしてください。
やりかたが分からない人は、総務部システム担当までお問い合せください。

ウイルス対策ソフトの導入　自己診断No. 2

- 業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。
  - パソコン：○○○○ウイルス対策ソフト（定義ファイル更新方法　自動）
  - タブレット端末：○○○○ウイルス対策ソフト（定義ファイル更新方法　自動or手動）

パスワードの管理　自己診断No. 3

- ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

◎必須	×禁止
10文字以上の文字数で構成されている	名前・愛称・地名・電話番号・生年月日・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
アルファベットの大文字と小文字、数字や「@」、「%」、「&」などの記号を組み合わせる	同じ文字・数字を連ねただけにしない
ID・パスワードの使い回しをしない	他者に見えるところに記さない/教えない

< 1 >

引用：情報セキュリティハンドブック（サンプル）（IPA）

注意点:実施できる程度に抑えてください

- 情報セキュリティハンドブックは17ページあり、何もないところから覚えるにはすこし量が多いです
- 厳しいルールを課すだけではセキュリティは高まりません
- 厳しすぎると、従業員は仕事をするために抜け道を探し始めます
- 実情に沿った、実施可能な施策を行うことが重要です

「使いにくいセキュリティはセキュリティではない」

引用:DockerCon EU 2015: Day 1 General Session

※コックさんは自分の仕事をするために
知らず知らずに危ないことをしています

当協会のサイバーセキュリティ関連の支援メニューのご紹介

Step.1
セキュリティに対する従業員の感度の低い企業向け

- **サイバーセキュリティの重要性**に関する認知拡大
- 時間をかけずに実行できる対策に絞っての実行

Step.2
セキュリティの必要性は認識しているが何を行えばよいか分からない企業向け

- ワークショップによる**情報セキュリティ管理規程の策定**
- **従業員向け勉強会**の開催
- **サイバーセキュリティ対策の実行計画**策定

今後、無料でご参加できるセミナーやワークショップをご案内しますので、ご興味ある方は、名刺交換をお願いします。

まとめ

- 最近の情報セキュリティリスク動向
- 情報セキュリティ自社診断
- 基本的な情報セキュリティ対策
- 情報セキュリティハンドブックの紹介

ありがとうございました

※右のQRコードをスマホからスキャンして
アンケートへのご協力をお願いします。