Security Days Spring 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3月12日（A10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

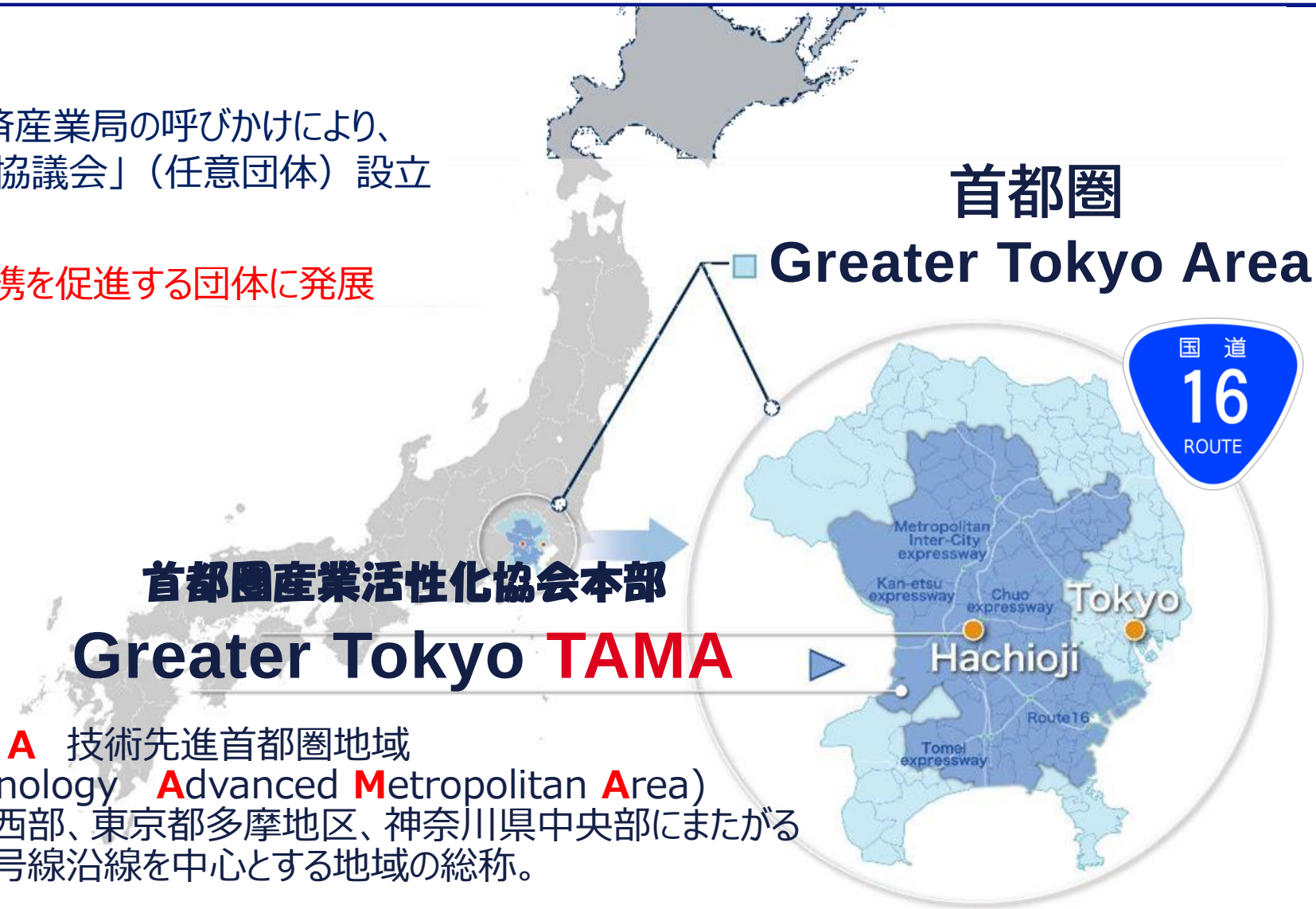
- 保有資格・公職
  - ITコーディネータ
  - 経済産業省登録　中小企業診断士
  - 公認情報システム監査人(CISA)
  - 情報処理推進機構　情報処理技術者試験委員

首都圏産業活性化協会の概要

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



首都圏産業活性化協会本部

Greater Tokyo TAMA

■ **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
国道１６号線沿線を中心とする地域の総称。

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
- 【ワークショップ1】 自社のセキュリティ状態の確認
- 具体的にどうやるのか？
- 【ワークショップ2】 情報セキュリティ対策のケーススタディ

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. 【事前課題の確認】– 情報セキュリティ自社診断

2024年 国内におけるサイバーセキュリティ攻撃の動向

■2024年の主な被害

- ランサムウェア被害による情報漏洩が多数発生
- サプライチェーン攻撃やネットワーク接続装置（VPN）の脆弱性を突く攻撃が顕著

■2024年末～2025年にかけて

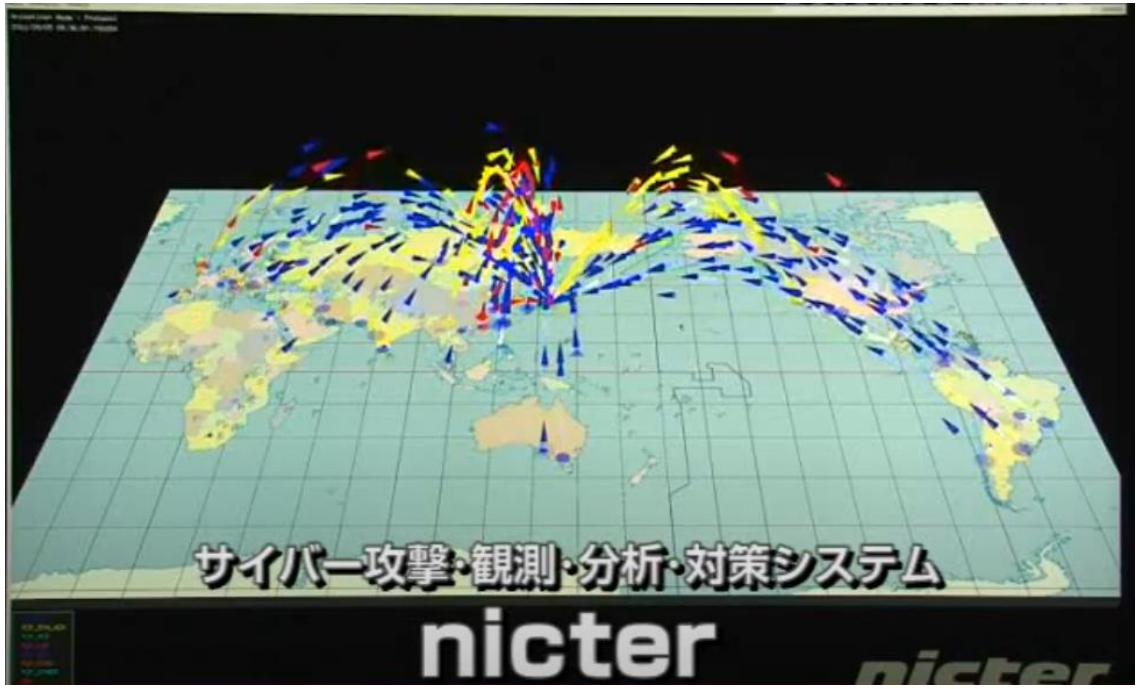
- JAL、三菱UFJ銀行、りそな銀行、みずほ銀行、NTTドコモなど金融機関や通信会社の重要インフラを標的とした攻撃が多発

2024年 国内におけるサイバーセキュリティ攻撃の動向

- NICT（情報通信研究機構）によれば、日本へのサイバー攻撃数は、年間約6,000億回に！
- 中国、インド、ロシア、ブラジルといった新興国からの攻撃が急増

	国名（国コード）	ホスト数	割合
	中国（CN）	63,463	31%
	インド（IN）	22,307	11%
	アメリカ（US）	16,686	8%
	台湾（TW）	8,925	4%
	ロシア連邦（RU）	7,848	4%
	ブラジル（BR）	6,659	3%

サイバー攻撃観測・分析システム
「NICTER」



多発するサイバーセキュリティの被害状況

日付	企業名	攻撃手口	被害影響
2/9	住友重機械工業株式会社	不正アクセス	サーバーが被害に遭い、情報漏洩の可能性、詳細は不明。
2/16	株式会社イズミ	ランサムウェア攻撃	社内ネットワークが遮断され業務影響、復旧に3ヶ月以上かかる。
4/16	LINE株式会社	不正アクセス	情報漏洩、ユーザーへの影響、詳細は不明。
5/10	JR東日本	不正アクセス	モバイルSuicaが一時的に使用不可、交通インフラに影響
5/19	岡山県精神科医療センター	ランサムウェア攻撃	データの暗号化、業務停止、患者情報の流出の可能性
5/26	株式会社イセトー	ランサムウェア攻撃	一部サーバやPCが暗号化され、業務に影響、復旧に3ヶ月以上
5/27	積水ハウス	不正アクセス	約83万人分の個人情報が漏洩した可能性
6/9	株式会社KADOKAWA	ランサムウェア攻撃	ニコニコ動画のサービス停止、出版事業の流通が平常時の3分の1に減少、個人情報の流出の可能性。
7/5	JAXA	不正アクセス	機密情報を含むデータが漏洩。ただし、ロケットや衛星の運用など安全保障に関わる情報は、漏洩はしていない模様。
9/12	株式会社関通	ランサムウェア攻撃	倉庫管理システムがランサムウェア攻撃を受けて停止、ガンバ大阪のECサイトなど同社の顧客の約47社が個人情報が漏洩
10/11	カシオ計算機株式会社	ランサムウェア攻撃	8478件の個人情報流出、業務に影響

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

ランサムウェアにより業務が2か月止まる

- 病院の電子カルテシステムが停止することで診療が滞る例が複数発生しています
  - つるぎ町立半田病院
    2021年10月～、復旧まで2か月
  - 大阪急性期・総合医療センター
    2022年10月31日～2023年1月11日、復旧まで2か月半
- 工場であれば、売上が2か月分なくなります。場合によっては、そのまま倒産です。

ランサムウエア（身代金要求型ウイルス）攻撃の被害を2021年10月に受けた徳島県のつるぎ町立半田病院は2022年6月7日、経緯などをまとめた有識者会議による調査報告書をつるぎ町議会に提示した。

半田病院は2021年10月にランサムウエア被害に遭った

［画像のクリックで拡大表示］

引用：ランサム被害の徳島・半田病院、報告書とベンダーの言い分から見える根深い問題｜日経クロステック（xTECH）（nikkei.com）

大きな病院だから狙われた？

うちは狙われるような大した企業じゃないよ？

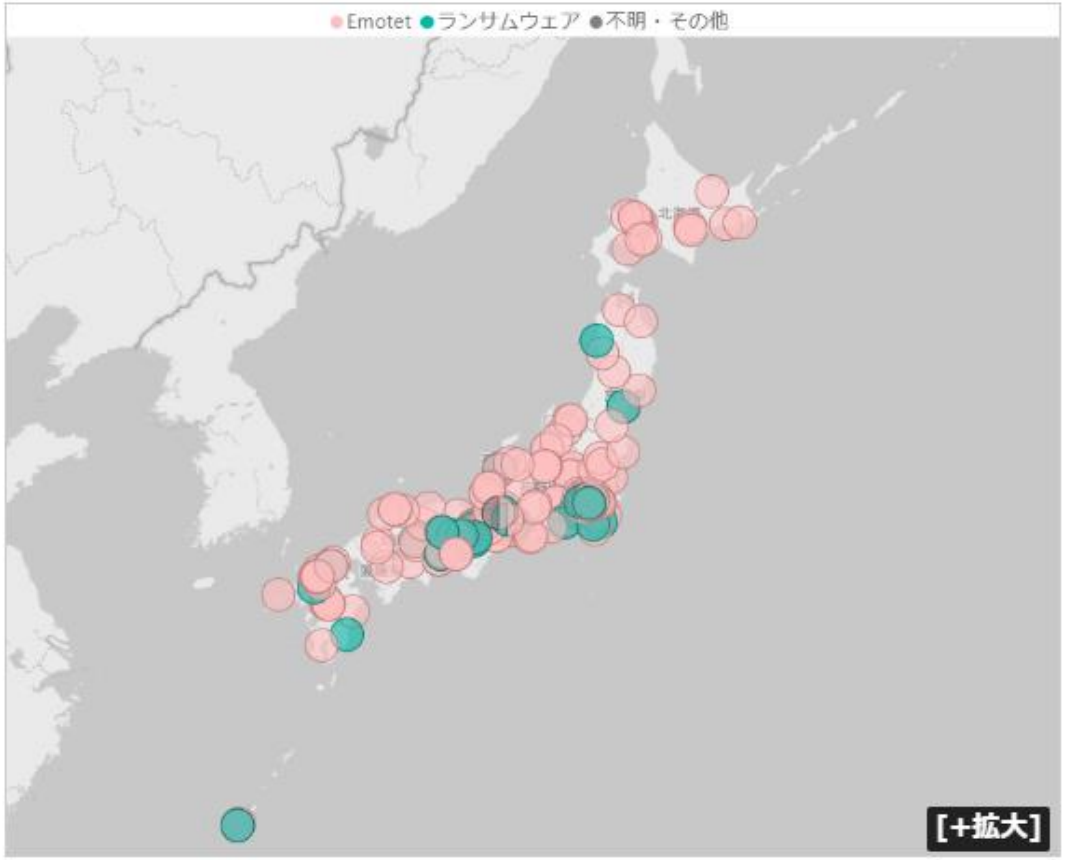
半田病院は山奥にある

- つるぎ町立半田病院は徳島の山奥にあります
- 病床数120床。規模はさほど大きくありません
- 犯人にとって下調べしにくく、不便すぎる場所です

引用：googleマップ

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

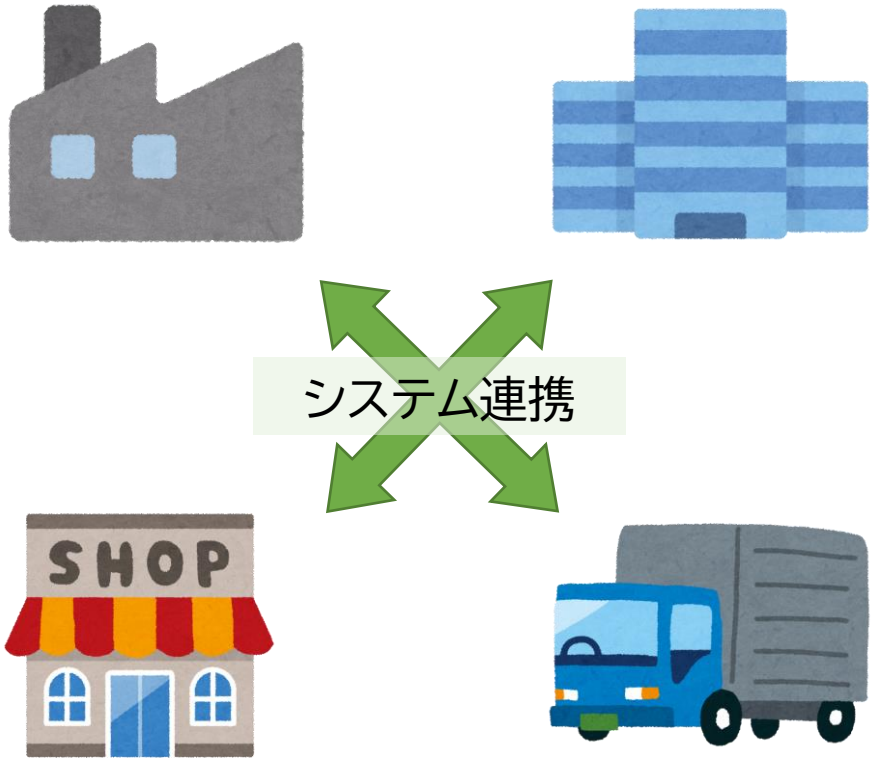


【図4】「マルウェア感染」被害組織の所在地

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）

拡大する企業間ネットワーク

- DXにより広がる企業間ネットワーク
  - 企業間の受発注（EDI）
  - 親事業者・下請企業間の調達情報共有
  - 工場間の在庫情報共有
  - 小売の情報を即座に工場に届ける（POSシステム）
- 企業間ネットワークによって、ビジネス効率はアップしますが……



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

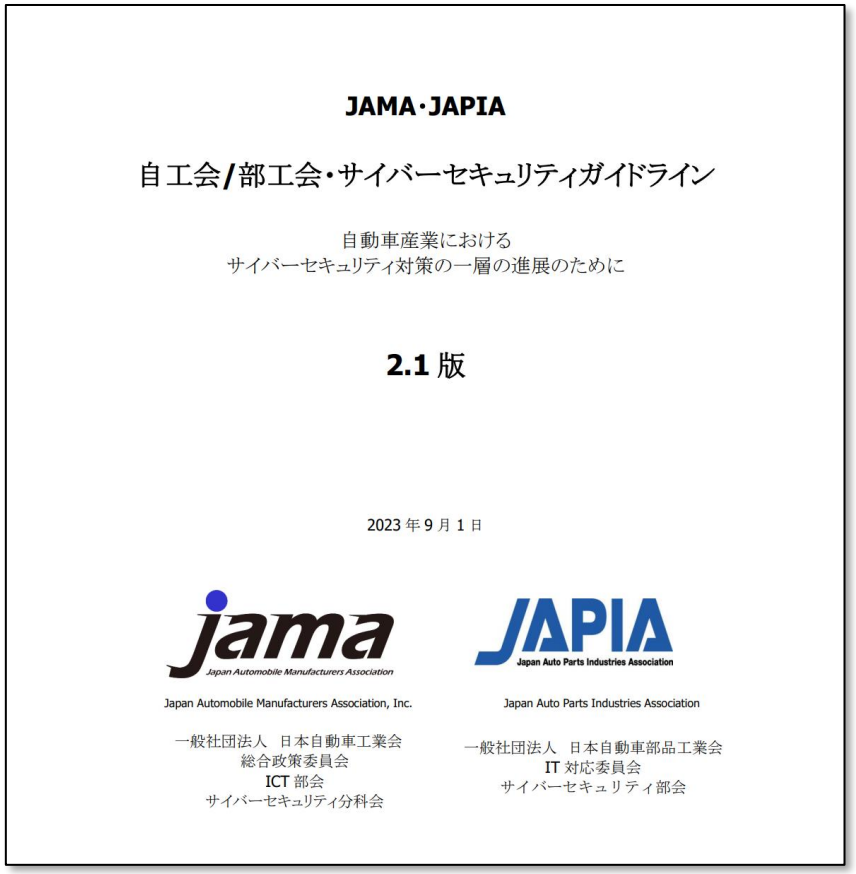
- 下請から親事業者を狙う攻撃を「サプライチェーン攻撃」と言います
  - サプライチェーン＝供給連鎖
- 前述の10大脅威の2位です
  - 1位と2位の組み合わせでトヨタの生産ラインは止まりました
- 親事業者に損害を与えた場合、取引停止、損害賠償のリスクがあります。

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）

【ワークショップ1】 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

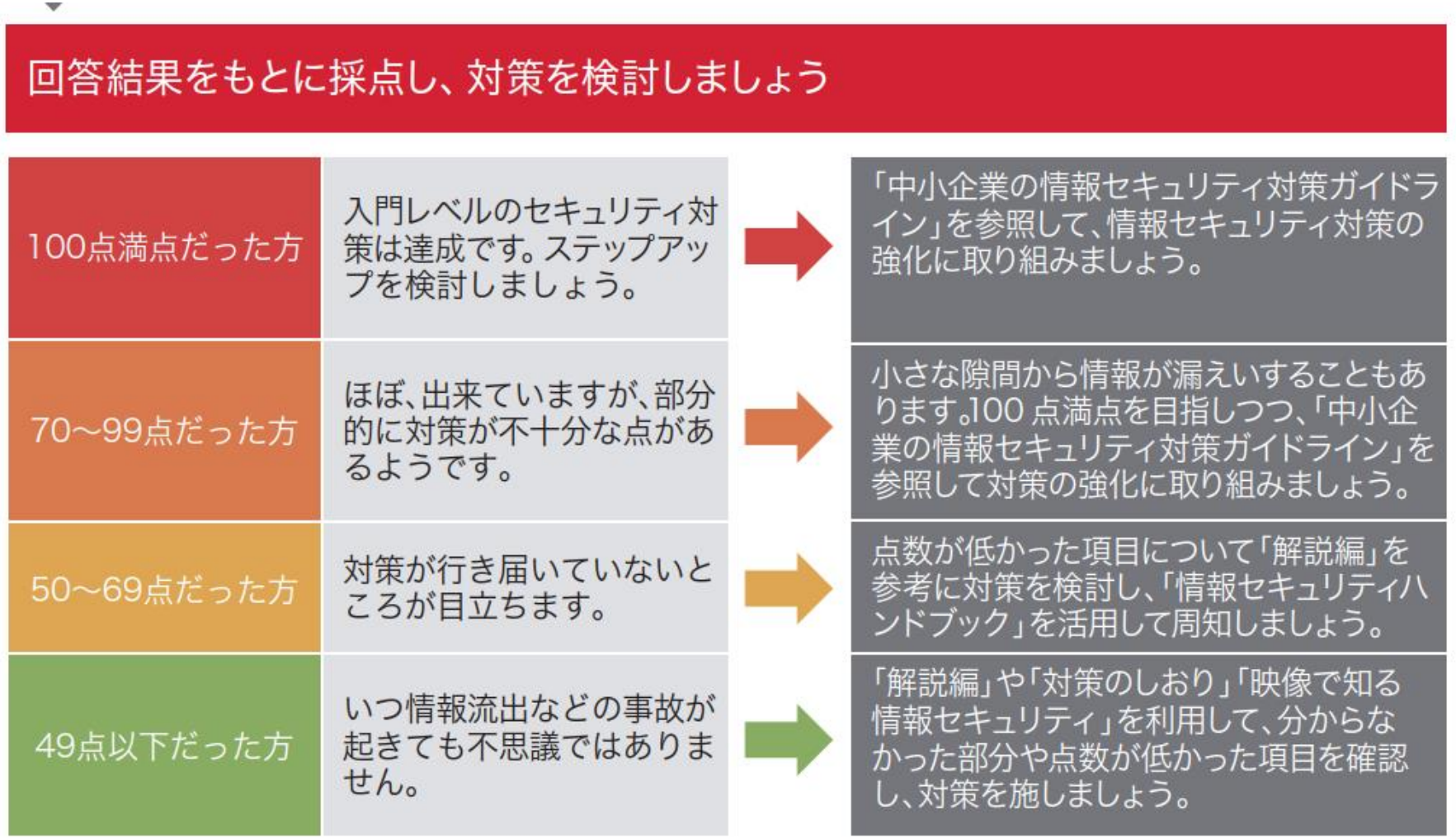
No.19～25は組織としての方針を定めた上で、実施すべき対策です。情報セキュリティのルールは明文化して社内で共有することにより、従業員の意識を高めるようにしましょう。

/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. 中小企業におけるサイバーセキュリティの具体的なステップ
2. 情報セキュリティ5か条の活用
3. Security Action一つ星の申請
4. 【ワークショップ2】- ケーススタディ

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)

中小企業におけるサイバーセキュリティの具体的なステップ

- 前章で紹介しました「中小企業の情報セキュリティ対策ガイドライン」では、下記の4ステップを推奨しています。

1.（何も行動していない場合は）できるところから始める

何もないところにPDCAのPから始めると企画倒れするので、まずやってみる（Dから行う）

2.（ある程度行動しているなら）組織的な取り組みを開始する

PDCAのCAを行えるように、自社診断チェックリストを行い、ハンドブックを修正する

3.（組織的に動いているなら）本格的に取り組む

改めてPを行う。セキュリティ関連規程を作成し、PDCAを回せるようにする

4.（PDCAが回り始めたら）改善を続ける

より強固な施策を取り込んでいき、スパイラルアップを図る

取組状況とアクション	本ガイドラインの活用方法
Step1 まず始めましょう	これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**(P.19) を参照して、「情報セキュリティ 5 か条」を実行してください。 進め方 「情報セキュリティ 5 か条」を社内で配付するなど、まずできるところから開始してください。
Step2 現状を知り改善しましょう	Step1 は実施できていて次に進める場合は**「3. 組織的な取り組みを開始する」**(P.20) を参照して、「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、できていない対策の実行に努めてください。 進め方 ・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。 ・「5 分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。 ・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。
Step3 本格的に取り組みましょう	Step2 までは実施できていて次に進める場合は**「4. 本格的に取り組む」**(P.24) を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。 進め方 ・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。 ・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。 ・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。
Step4 改善を続けましょう	**「5. より強固にするための方策」**(P.32) を参照して、自社に必要な対策を追加実施してください。Step1 や Step2 に取り組んでいる企業でも、Step4 を参照して必要な対策があれば実行してください。

引用：中小企業の情報セキュリティ対策ガイドライン（IPA）

1. できるところから始める

- 今まで特段のことを何もしていない場合は、手を付けやすいところから行います
  - 何もないところからPDCAを回すのは大変です
- 「手を付けやすいところ」として「情報セキュリティ5か条」が用意されています。ここから着手するのがわかりやすいです

Step1
まず始めましょう

これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**(P.19) を参照して、「情報セキュリティ 5 か条」を実行してください。

進め方

「情報セキュリティ 5 か条」を社内で配付するなど、まずできるところから開始してください。

引用：中小企業の情報セキュリティ対策ガイドライン（IPA）

2. 組織的な取り組みを開始する

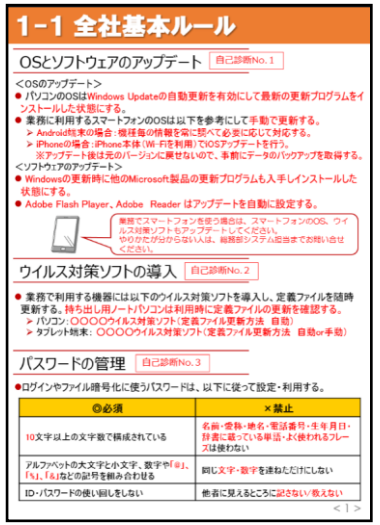
- とりあえずのDができたら、CAに行きましょう
- Checkの道具として「5分でできる！情報セキュリティ自社診断」が使えます
- Actとして「情報セキュリティハンドブック」で改善を行い、「情報セキュリティ基本方針」で次のPをする体制を作ります

Step2
現状を知り改善しましょう

Step1 は実施できていて次に進める場合は
「3. 組織的な取り組みを開始する」（P.20）を参照して、「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、できていない対策の実行に努めてください。

進め方

- 「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。
- 「5分でできる！情報セキュリティ自社診断」で現状の対策を把握し、実施すべき対策を検討してください。
- 「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。


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把握し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。

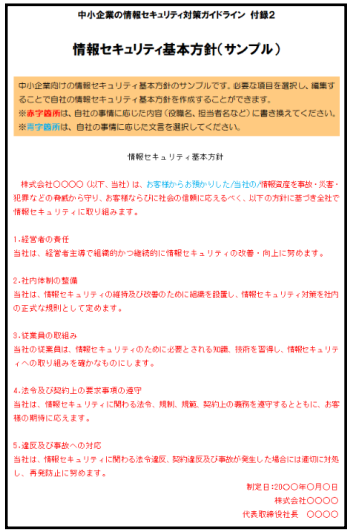
ウイルス対策ソフトの導入 自己診断No. 2

● 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：〇〇〇〇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：〇〇〇〇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・姓名・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


中小企業の情報セキュリティ対策ガイドライン 付録2

情報セキュリティ基本方針（サンプル）

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針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。

情報セキュリティ基本方針

株式会社〇〇〇〇（以下、当社）は、お客様からお預かりした/当社の情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1.経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

2.社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

3.従業員の取組み
当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

4.法令及び契約上の要求事項の遵守
当社は、情報セキュリティに関わる法令、規則、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

5.違反及び事故への対応
当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日：20〇〇年〇月〇日
株式会社〇〇〇〇
代表取締役社長　〇〇〇〇

引用：中小企業の情報セキュリティ対策ガイドライン（IPA）

3. 本格的に取り組む

- 「できるところから始める」だけでは、十分であるか、漏れがないかわかりません
  - ほとんどの場合に不十分であり、漏れがあります
- 施策が必要な対象を
  「リスク分析シート」
  で洗い出し、必要な施策を立案、
  「情報セキュリティ関連規程」
  でルール化、実施していきます（P、D）
- 工数や費用の掛かる施策もでてきます。社内体制や予算の確保が必要になります

Step3
本格的に取り組みましょう

Step2 までは実施できていて次に進める場合は
「4. 本格的に取り組む」（P.24）を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。

進め方

・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。
・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。
・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。

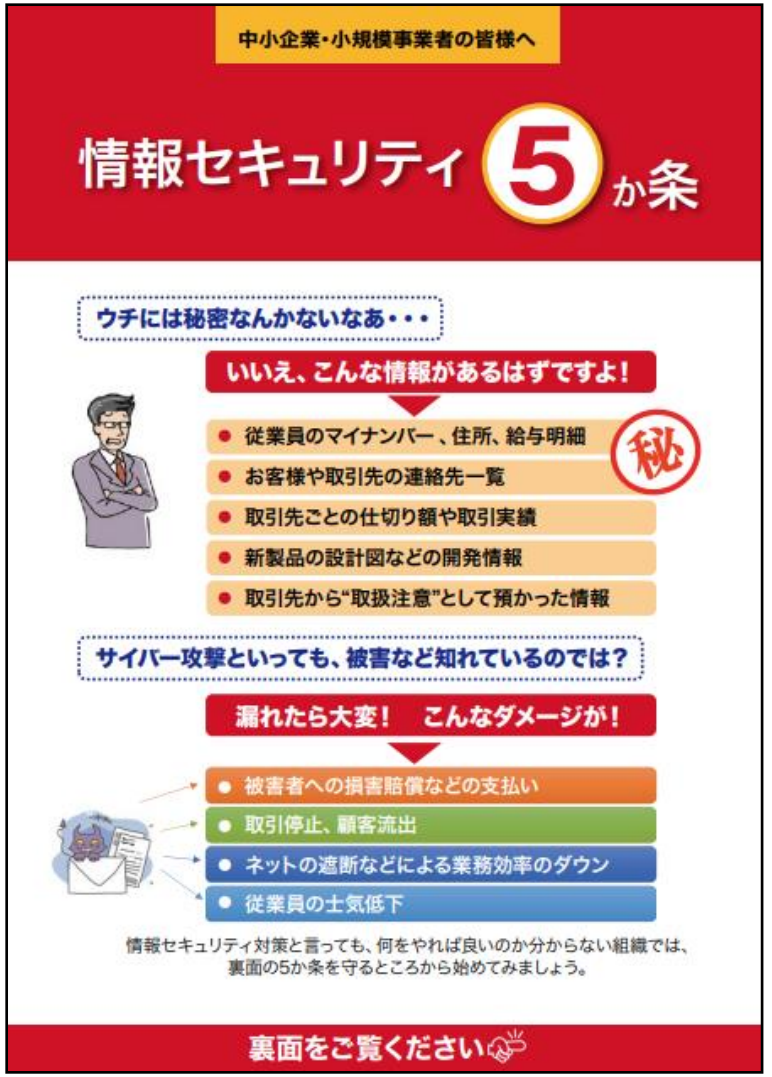
情報資産管理台帳

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日	現状から想定される リスク（入力不要・自動表示）			
						個人情報	要配慮個人情報	特定個人情報	機密性	完全性	可用性	重要度			脅威の発生頻度 ※「脅威の状況」シートに入力すると表示	脆弱性 ※「対策状況チェック」シートに入力すると表示	被害発生可能性	リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2 可能性：中	6 リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1 可能性：低	3 リスク小
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	3	5年	2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1 可能性：低	3 リスク小
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	3	3	2	3	7年	2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2 可能性：中	6 リスク大
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1 可能性：低	2 リスク小
経理	発行済請求書控	当社発行の請求書の控え（過去3年分）	総務部	総務部	書類				2	2	2	2		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1 可能性：低	2 リスク小
共通	電子メールデータ	重要度は退任のため最高値で評価	担当者	総務部	事務所PC	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2 可能性：中	6 リスク大
共通	電子メールデータ	Gmailに転送	担当者	総務部	社外サーバー	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2 可能性：中	6 リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	社内サーバー	有			3	3	3	3		2023/4/1	3:通常の状態で脅威が発生する（いつ発生してもおかしくない）	2:部分的に対策を実施している	2 可能性：中	6 リスク大
営業	顧客リスト	得意先（直近５年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			3	2	2	3		2023/4/1	2:特定の状況で脅威が発生する（年に数回程度）	2:部分的に対策を実施している	1 可能性：低	3 リスク小

引用：中小企業の情報セキュリティ対策ガイドライン（IPA）

本セミナーではStep1に取り組みます

- Step1をクリアできている企業についても、基本的対策が、しっかり運用できているか？再点検の意味で、取り組みに参加してください。
- まず、情報処理推進機構（IPA）が発行している「情報セキュリティ5カ条」から開始しましょう。



引用：情報セキュリティ5カ条（IPA）

Security Actionとは

- 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
  - 認定制度ではありません
  - 「取り組んでいること」を宣言します。取り組みが完了していなくても構いません
  - 「一つ星」「二つ星」があります

引用：SECURITY ACTIONとは？：SECURITY ACTION セキュリティ対策自己宣言（ipa.go.jp）

Security Actionのメリット

- Security Actionは助成金の要件や加点要素になっています

全国

- IT導入補助金
- ものづくり補助金（デジタル枠）
- 事業承継・引継ぎ補助金（経営革新）
- 地域医療介護総合確保基金を利用したICT導入支援事業
- 事業再構築補助金（サプライチェーン強靭化枠）

都道府県

- 秋田県 デジタル化トライアル事業費補助金
- 東京都中小企業振興公社 令和5年度サイバーセキュリティ対策促進助成
- 東京都中小企業振興公社 情報セキュリティ基本方針策定支援専門家派遣事業
- 岐阜県 令和4年度中小企業等スマートワーク促進補助金（情報セキュリティ事業）
- 堺市 中小企業デジタル化促進補助金
- 愛知県 デジタル技術導入補助金

Security Action 一つ星の要件

- 要件は「『情報セキュリティ5か条』に取り組むこと」です
  - 取り組んでいればOKです。完璧である必要はありません
  - とはいえ、事故を起こしたときに説明がつかなくなるため、きちんと取り組みましょう
- 宣言すると次のメリットが得られます
  - 右図のロゴマークを使用できます
  - 一部の補助金の要件を満たします

引用:SECURITY ACTION ロゴマークの使用申込方法：SECURITY ACTION セキュリティ対策自己宣言（ipa.go.jp）

申請要件の「5か条に取り組むことを宣言」とは

- 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

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！

宣言方法

- 「SECURITY ACTION自己宣言者サイトTOP」にアクセスし、手順書に従い入力していきます
  - 自己宣言者サイト https://security-shien.ipa.go.jp/security/index.html
  - 申込方法 https://www.ipa.go.jp/security/security-action/entry/
- 受理されるまで「1～2週」となっていますが、実務上は3～4日程度で処理されるようです（※保証はありませんので補助金申請のスケジュールにはご注意ください）

引用：SECURITY ACTION自己宣言者サイト TOP：IPA 独立行政法人 情報処理推進機構

せっかくですので徹底しましょう

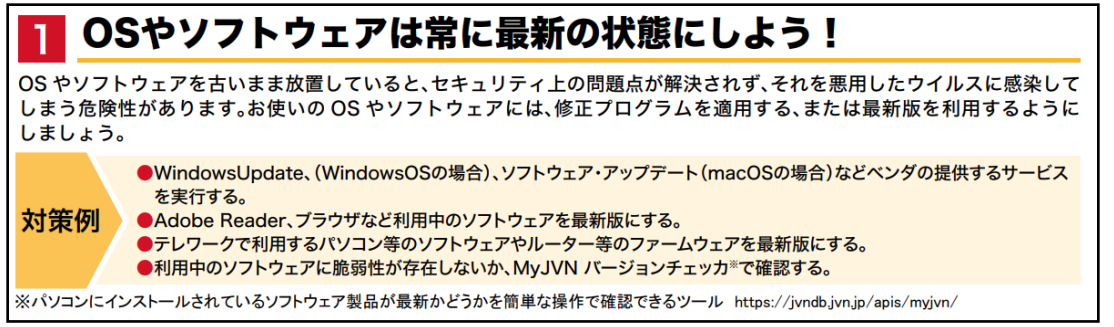
- 5カ条＋αを徹底することだけでも、結構な効果が見込めます
  - 10大脅威に対し、
    黄色背景がある程度の効果を
    見込めるものです

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

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



1 OSやソフトウェアは常に最新の状態にしよう！

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、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 やソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。

対策例

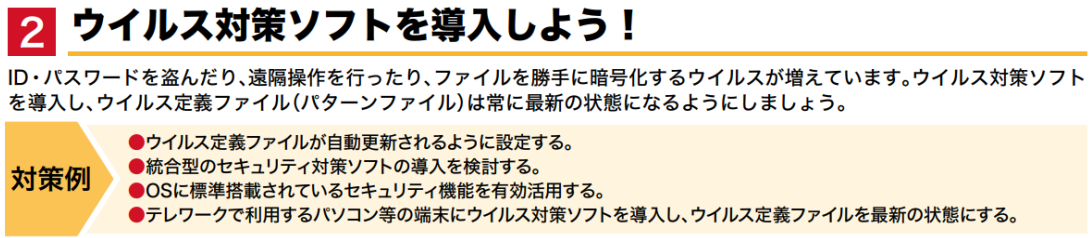
- WindowsUpdate、(WindowsOSの場合)、ソフトウェア・アップデート(macOSの場合)などベンダの提供するサービスを実行する。
- Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
- テレワークで利用するパソコン等のソフトウェアやルーター等のファームウェアを最新版にする。
- 利用中のソフトウェアに脆弱性が存在しないか、MyJVN バージョンチェッカ※で確認する。

※パソコンにインストールされているソフトウェア製品が最新かどうかを簡単な操作で確認できるツール　https://jvndb.jvn.jp/apis/myjvn/

- サポート期限の切れたOS、ソフトウェアを使っていませんか？(特にoffice製品)
- ソフトウェアの更新時に、再起動が求められた場合に、業務の停止を嫌って、再起動を延期していませんか？
- WiFiルータやUTMなどのファームウェアは確認しましたか？
- 利用中のPC/機器をすべて洗い出しましたか？
- 定期的に状態を確認する仕組みや体制を整えていますか？

No.2 ウイ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。



2 ウイルス対策ソフトを導入しよう！

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。

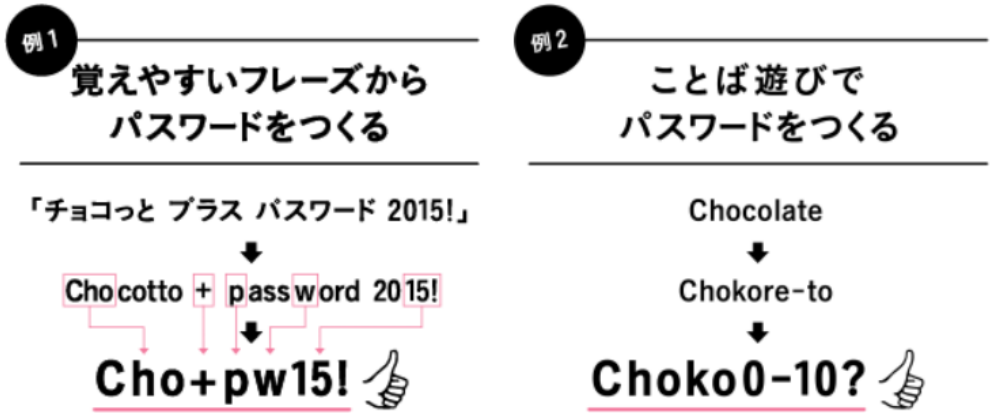
対策例

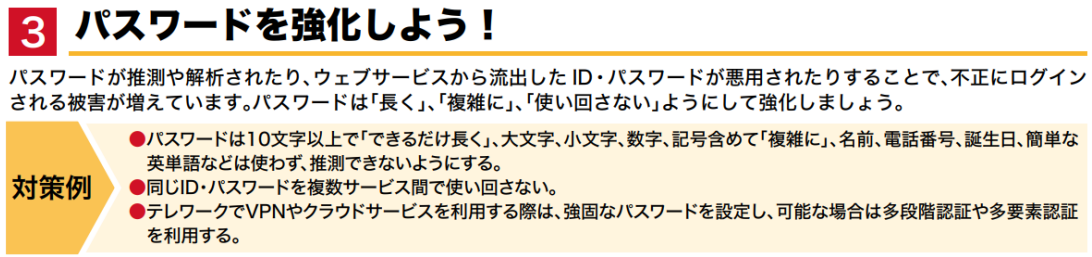
- ウイルス定義ファイルが自動更新されるように設定する。
- 統合型のセキュリティ対策ソフトの導入を検討する。
- OSに標準搭載されているセキュリティ機能を有効活用する。
- テレワークで利用するパソコン等の端末にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。

- Mac/LinuxにはOS標準の対策ソフトがないため、独自に導入していますか？
- Windowsでウィルス対策ソフトがバンドルされている場合、サポートの契約更新またはOS標準ソフトへの変更はしましたか？
  - 特に購入後1年以上経っている場合はOS標準ソフトも無効化されている場合が多いです
- IoT機器への導入検討・代替手段の検討は行いましたか？（通常は単純な適用ができない）
- ウィルス対策ソフトのライセンス更新はしていますか？

No.3 強固なパスワードを使用する

- 現代では15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）
- 15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

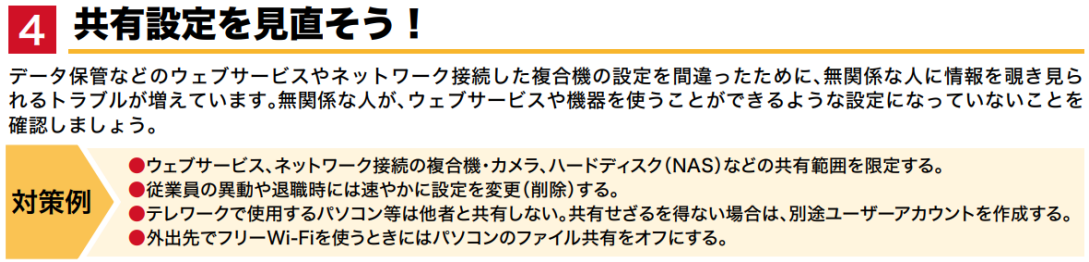




- パスワード管理ソフトの利用は検討しましたか？
- 初期パスワードから変更しましたか？
  - 特にWiFiルータやIoT機器
  - 河川カメラ338台が稼働停止、初期パスワード変更せずサイバー被害｜日経クロステック(xTECH)（nikkei.com）

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



4 共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、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。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

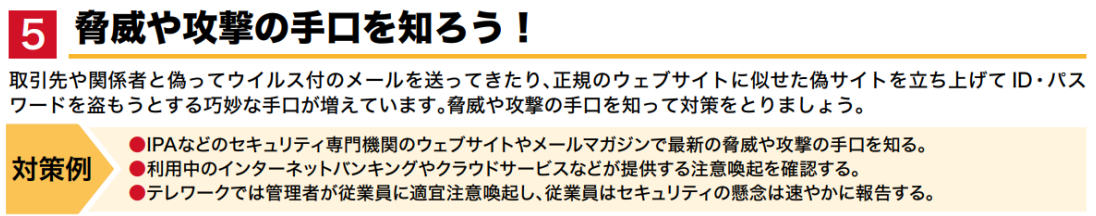
対策例

- ウェブサービス、ネットワーク接続の複合機・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は速やかに設定を変更（削除）する。
- テレワークで使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
- 外出先でフリーWi-Fiを使うときにはパソコンのファイル共有をオフにする。

- 異動時に前部署の権限を「引継ぎのため」と称してそのまま持っていませんか？
  - その際、「銀行振込依頼と承認の両方の権限を持っている」ような状況になっていませんか？
- 定期的に従業員の権限の棚卸しをしていますか？

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を身に着けることです。
- IPAがたくさんの教育コンテンツを発信していますので、それを利用するのが手っ取り早いです
  - 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)



5 脅威や攻撃の手口を知ろう！

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。

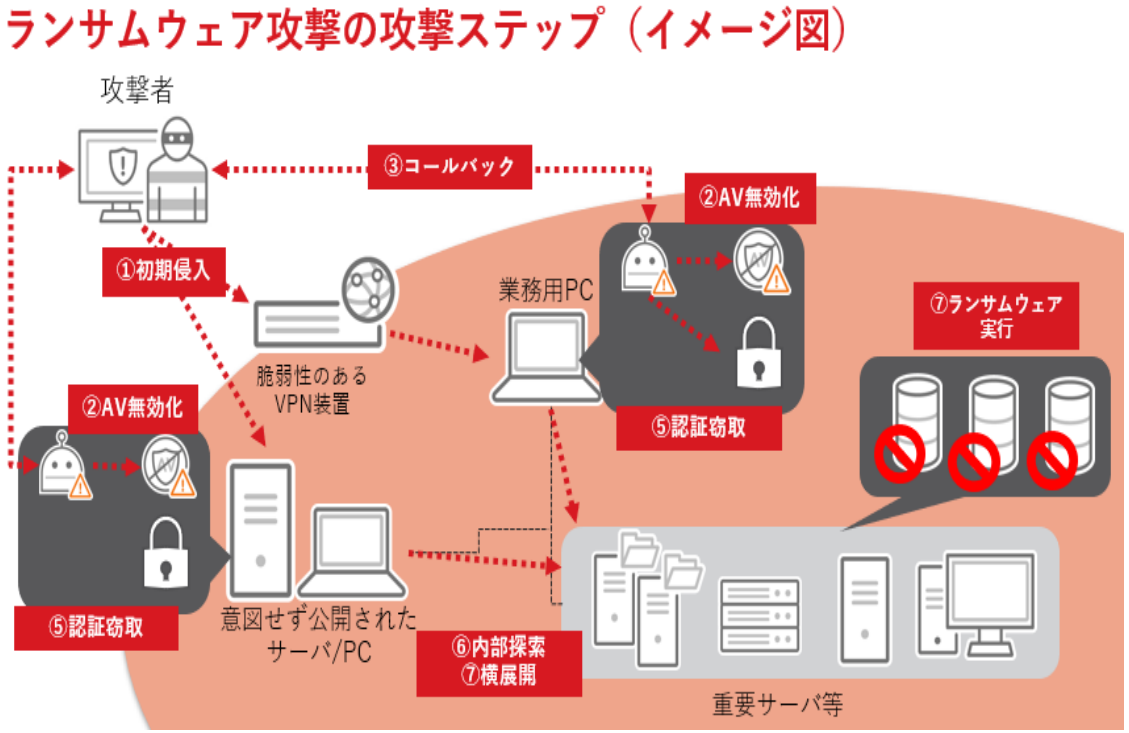
対策例

- 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。
- テレワークでは管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。

- 全従業員に対して定期的な教育機会を与えていますか？
- セキュリティ担当者により専門的な教育機会を与えていますか？
- セキュリティの懸念を報告・相談する連絡経路を設定・周知していますか？

【事例】OSやソフトウェアの更新を怠ることによるリスク

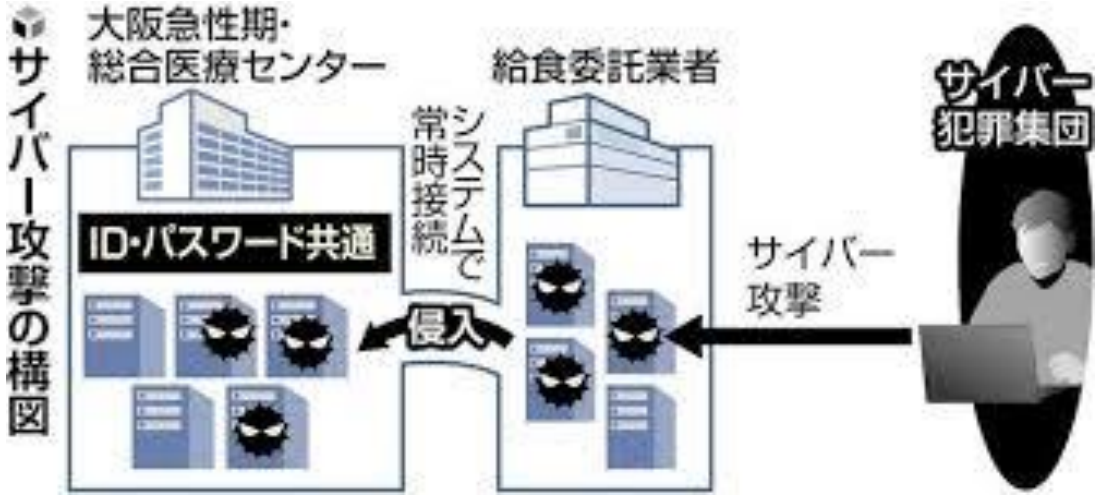
- 名古屋港コンテナターミナルのランサムウェア被害（2023年）
- 原因： 保守作業に利用するVPN装置のソフトウェアの更新が見落とされていた
- 対策： システムの脆弱性を修正するためのアップデートとセキュリティパッチの適用を徹底



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

【事例】弱いパスワードが引き起こすリスク

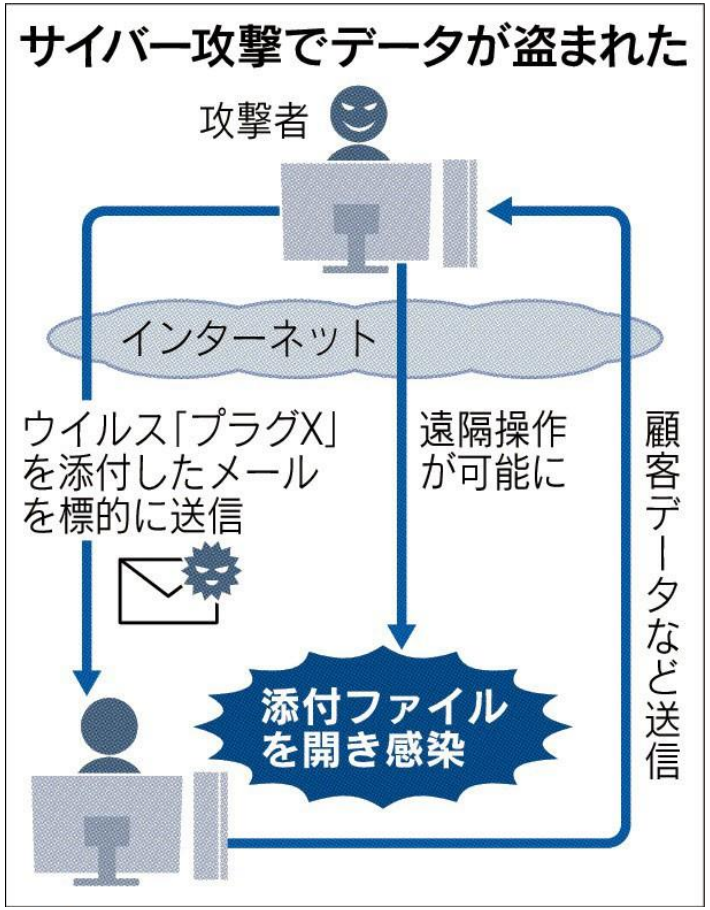
- 大阪急性期・総合医療センターのランサムウェア被害（2023年）
- 原因： 電子カルテの管理用IDとパスワードが使い回しされていた。電子カルテシステムのサーバーには、負荷を軽くするため、ウイルス対策ソフトが設定されていなかった。
- 対策：使い回されていたパスワードを全て異なるものに変更し、ウイルス対策ソフトを設定



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

【事例】従業員の情報リテラシが低いことによるリスク

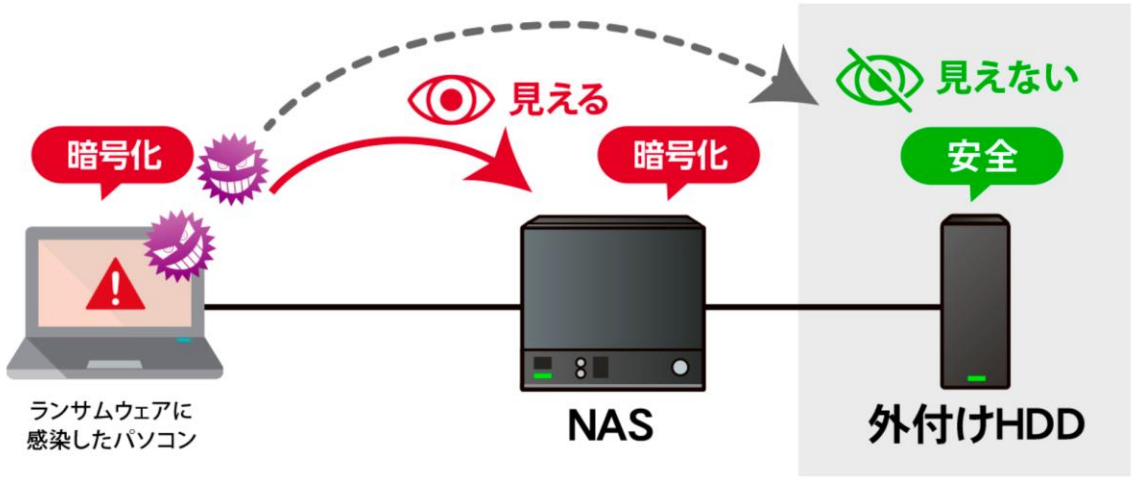
- JTBの顧客情報漏洩（2016年）
  フィッシングメールにより約793万人の顧客情報が漏洩する事件が発生
- 原因：従業員が不正なメールのリンクをクリックしてしまい、マルウェアがインストールされた
- 対策：フィッシングメール対策として、従業員教育を強化と不正アクセス防止のためにシステムの強化



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オフラインに保管する。
- 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



【ワークショップ2】情報セキュリティ対策のケーススタディ

株式会社メカトロテクノロジーは、従業員数50人の中小製造業で、主に機械部品の製造しており、親会社から多くの機密性の高い図面情報を預かっている。

多忙なスケジュールのため、従業員の多くが、業務の中断を嫌って、OSやソフトウェアのアップデートを怠っている。

ウイルス対策ソフトは導入されているが、全ての端末に導入されているか把握できていない。特に、工場内のPCへのウイルス対策ソフトの導入が不確かな状態である。

パスワードの複雑さや更新頻度に関する明確なガイドラインはなく、従業員の多くは、自身の生年月日など短いパスワードを長く使用している。

従業員は業務データを自分のローカルPCに保管しており、これらのデータのバックアップは取得されていない。

営業は、外出時にノートPCを持ち出しているが、覗き見防止用フィルタはつけていない。

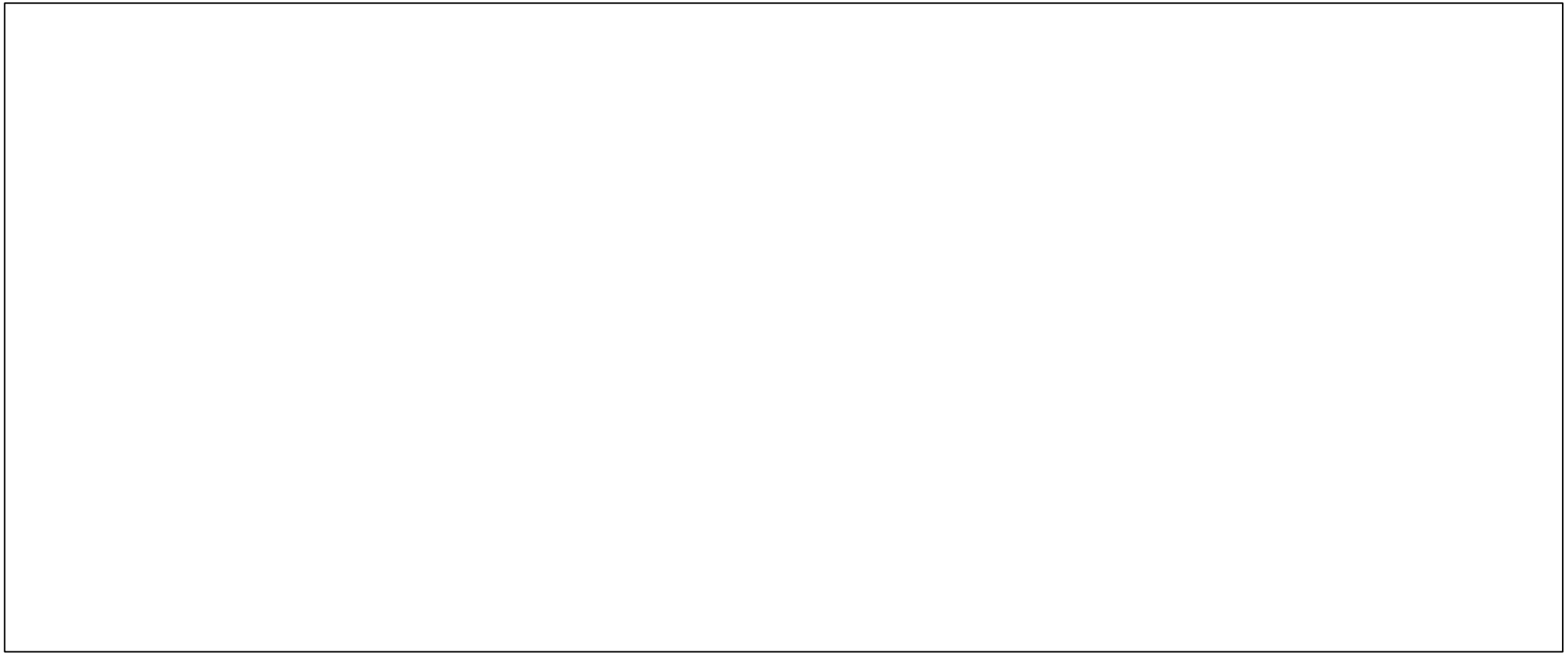
【ワークショップ2】情報セキュリティ対策のケーススタディ

問1. あなたの会社と似ている点をピックアップしてください。

問2. 情報セキュリティ5か条を基に、当社のリスクと、すぐに始められる対策を考えてみましょう。

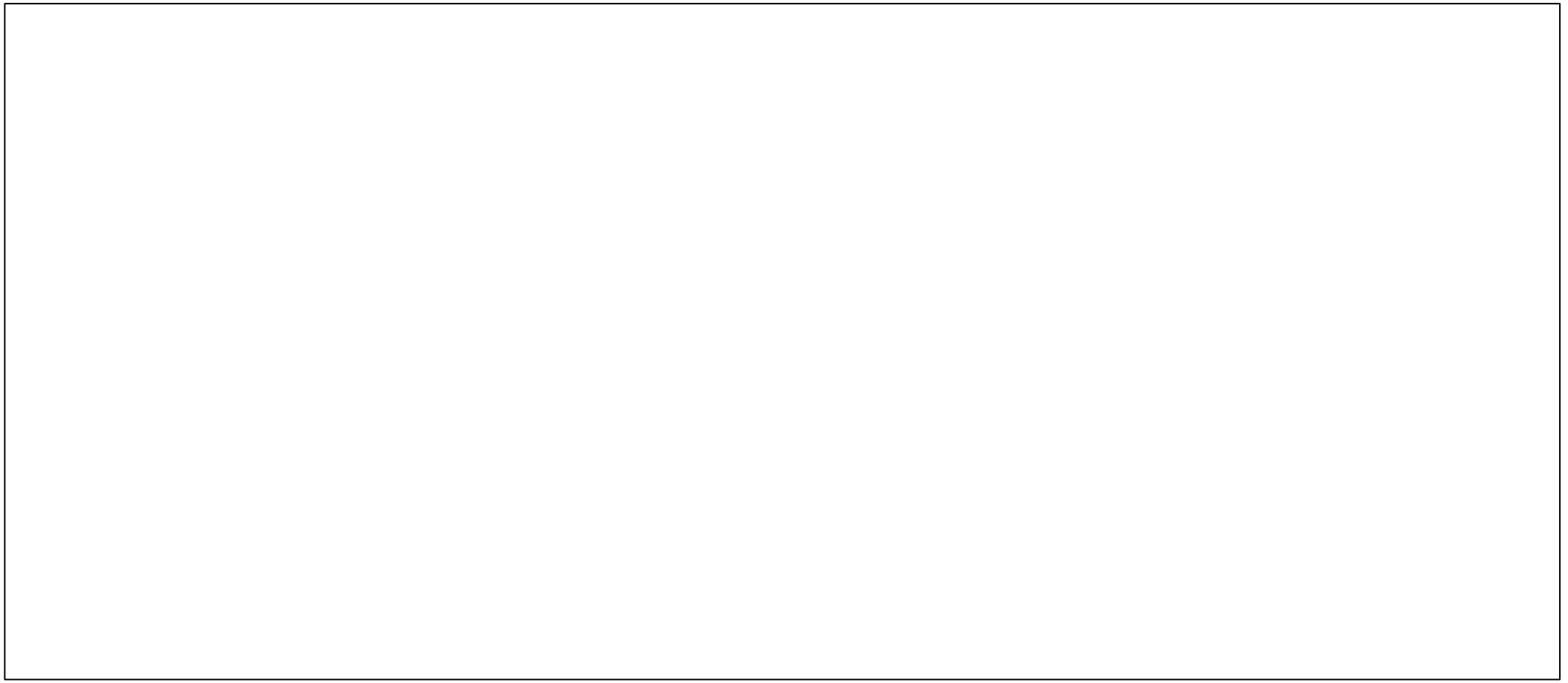
当社のリスクの洗い出し

情報セキュリティ5か条の観点でリスクの洗い出し



すぐに始められる対策の洗い出し

すぐに始められる対策



解答例1

情報セキュリティ5か条の観点での当社のリスクを洗い出し

- 古いosとソフトウェアが原因となるマルウェア感染と感染の拡大
- ウイルス対策ソフトが未導入端末のマルウェア感染と感染の拡大
- 単純なパスワードが原因となる不正アクセスと情報漏えいの発生
- PCのディスク故障によるローカルPCのデータの消出
- 外出時に、覗き見による重要情報の流出

解答例2

すぐに始められる対策

- 自動アップデートの設定を義務化し、定期的な監査を行う。セキュリティパッチの適用を確実にするためのポリシーを策定する。
- 各部門のリーダーに指示を出して、所属員の端末を確認し、ウイルス対策ソフトの導入と運用状況をチェックする。未導入の端末には速やかにソフトをインストールし、定期的な監査を実施する。
- パスワードの長さや複雑さに関するルールを設定して、ルールが遵守されるように従業員教育を実施する。
- 覗き見防止フィルタの導入、従業員教育を実施し、最新の脅威や攻撃手口についての認識を高める。

まとめ

- 最近の情報セキュリティリスク動向
- ワークショップ：
  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

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。

ありがとうございました