令和6年サイバーセキュリティセミナーin長崎

デジタル活用の推進に向けたサイバーセキュリティの基本

2024年7月22日

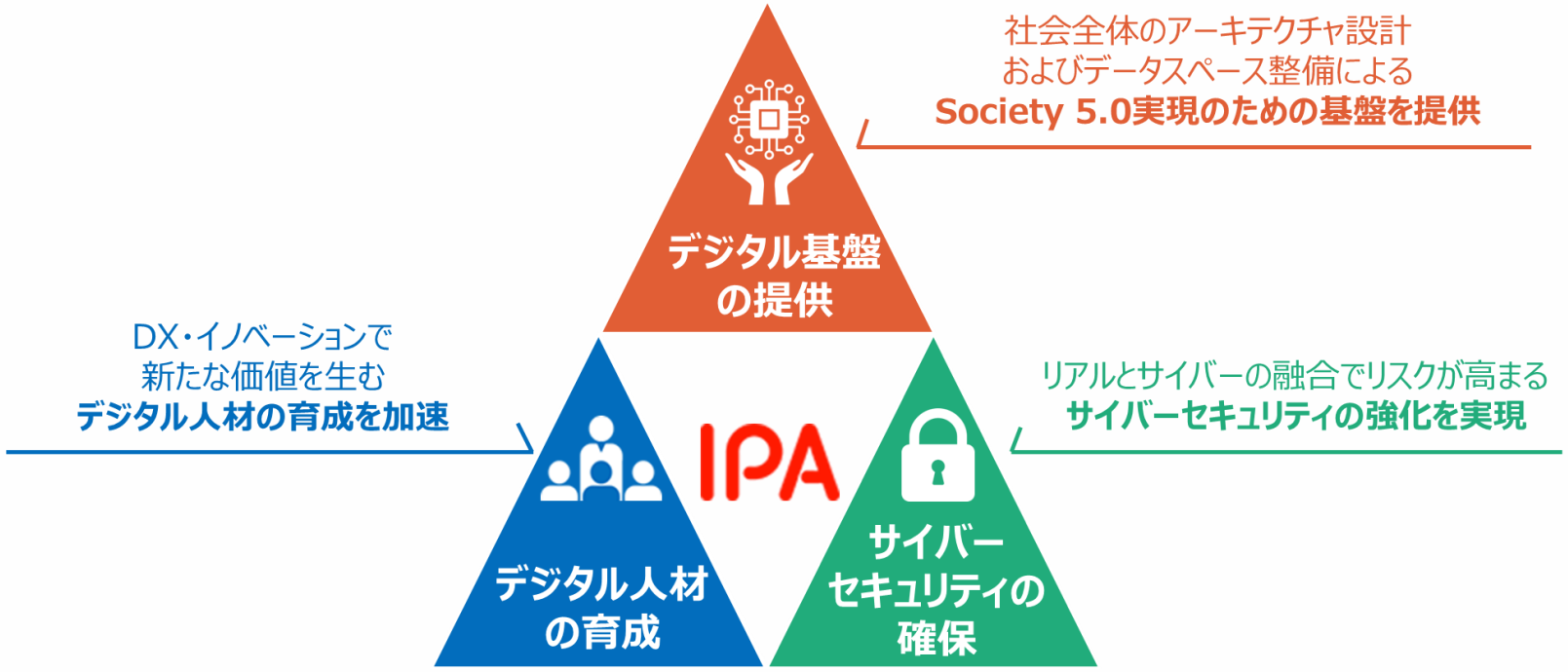
独立行政法人情報処理推進機構（IPA）
セキュリティセンター　セキュリティ普及啓発・振興部
シニアエキスパート　横山　尚人

IPA Better Life with IT

独立行政法人 情報処理推進機構（IPA）について

日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人。
誰もが安心してITのメリットを実感できる「 **頼れるIT社会** 」の実現を目指しています。

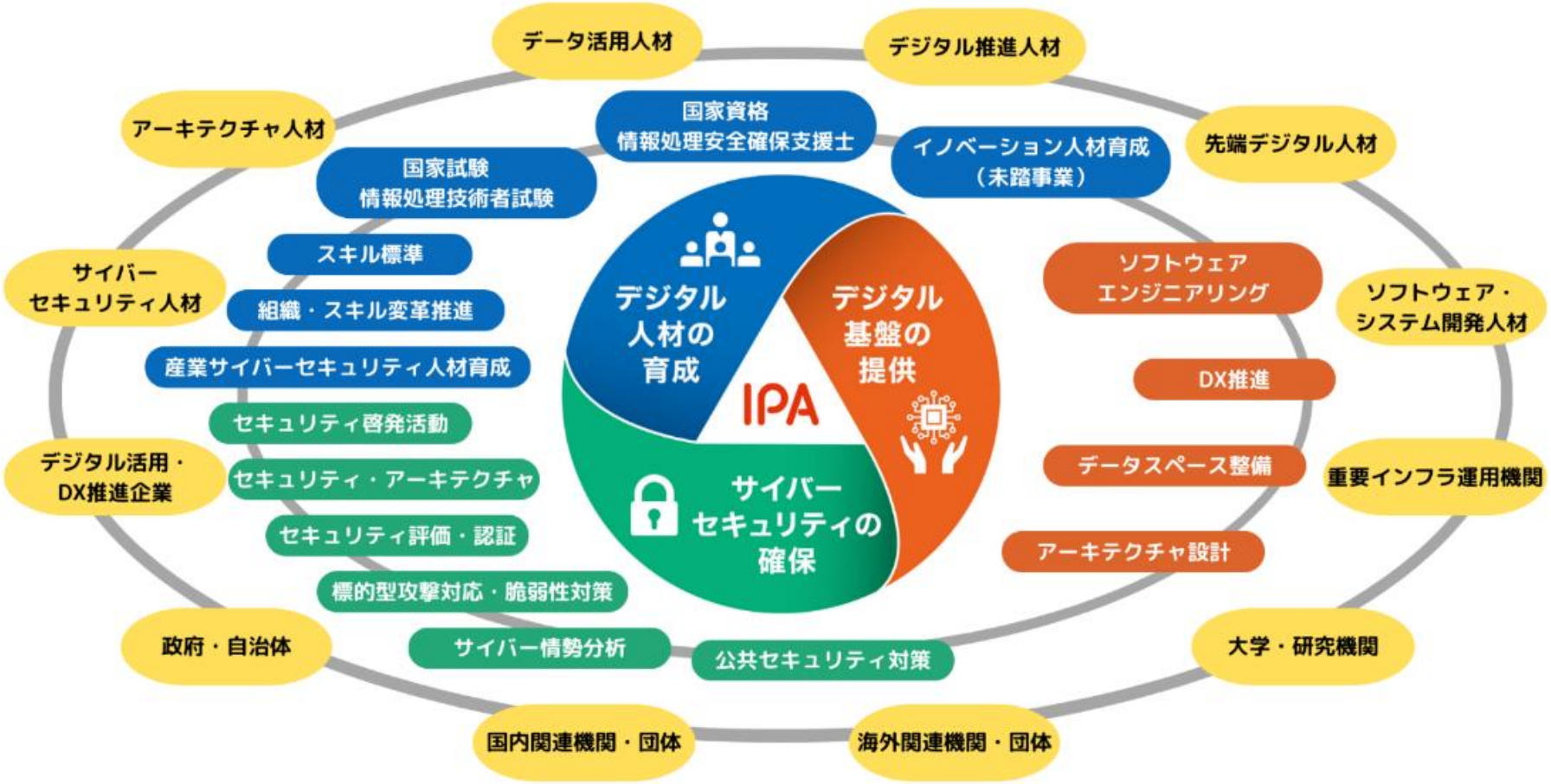
「**人材**」、「**セキュリティ**」、「**デジタル基盤**」の3つの中核事業



■名称: 独立行政法人情報処理推進機構
(Information-technology Promotion Agency, Japan)
■設立: 2004年1月5日
（前身母体の設立は1970年10月1日）
■理事長: 齊藤 裕

IPAの取り組み

- デジタルで豊かな社会の実現に向けて、幅広い取り組みを行っています



『IPA』で検索！

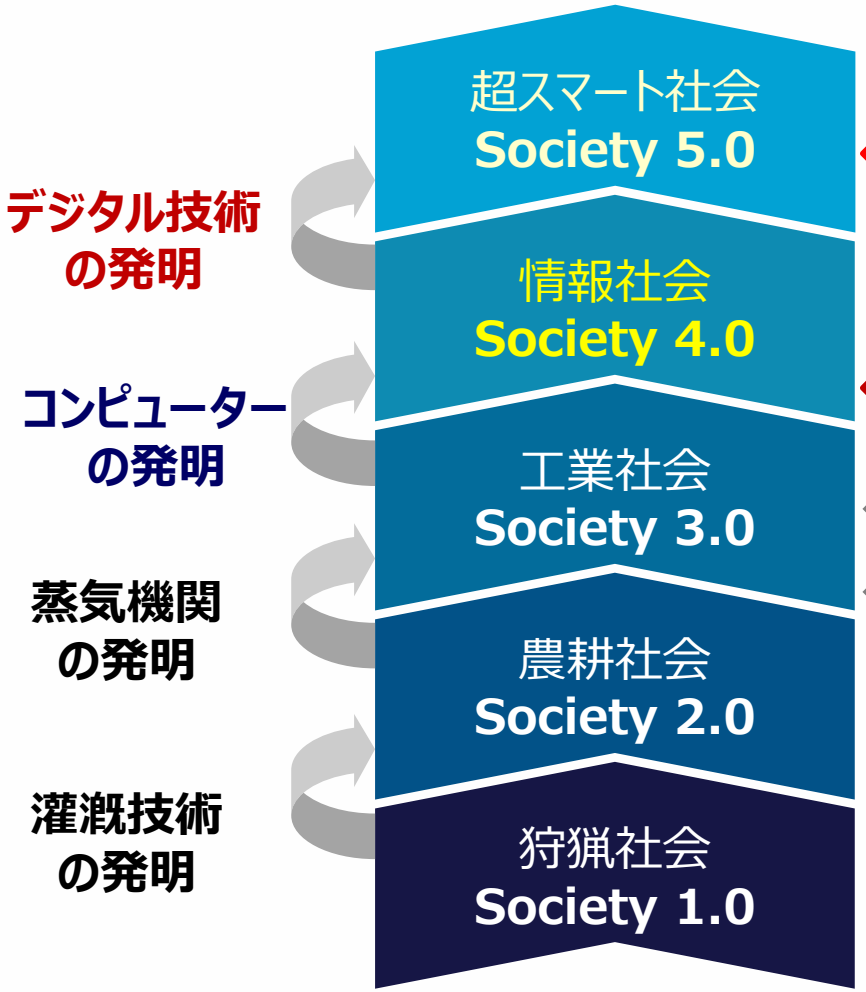
本題に
はいる前に

日本が抱える課題とデジタル技術の必要性

- 日本が抱える課題の解決には**デジタル技術の活用は必要不可欠**

＜日本が抱える課題の例＞	＜デジタル技術を使った解決策の例＞
人口減少と少子高齢化	AIによる業務の自動化・省力化
都市部への人口集中	リモートツールによる遠隔業務の促進
インフラの老朽化	データ分析による事故の予測・回避
災害リスクの高まり	クラウドサービスの利用によるデータ保全

イノベーションによる社会と産業の進歩



いままさに
第4次産業革命 ＝ データとデジタルの時代

- **データ**が動力源
- **AI・IoT・ロボット**などのテクノロジーで課題を解決
- **デジタル化**が進む
- **DXを体現する企業**が台頭

仕事も生活も、デジタル技術を活用する時代に！

1970年代~
第3次産業革命

- **コンピューティング・パワー**が動力源
- **PC・インターネット**が基盤
- **自動化・情報化**が進む
- **IT産業**が台頭

1760~1830年代
第1次産業革命

- **石炭**が動力源
- **紡績機**が主要基盤
- **機械工業化**が進む
- **軽工業**が主流

1860~1900年代
第2次産業革命

- **石油・電力**が動力源
- **モーター・製造ライン**が基盤に
- **大量生産・大量輸送・大量消費**が実現
- **重化学工業**が主流

業務用パソコン・タブレット端末・スマートフォンの利用状況
利用している：93.3%
2021年度 中小企業における情報セキュリティ対策に関する実態調査
https://www.ipa.go.jp/security/reports/sme/about.html

ちなみに、
世帯普及率（2021年）
・パソコン： 69.8% ⬆
・スマートフォン：88.6% ⬆
・固定電話： 66.5% ⬇
※令和4年版 情報通信白書
https://www.soumu.go.jp/johotsusintokei/whitepaper/r04.html

DXとは？ 概要

デジタルトランスフォーメーション(DX) とは

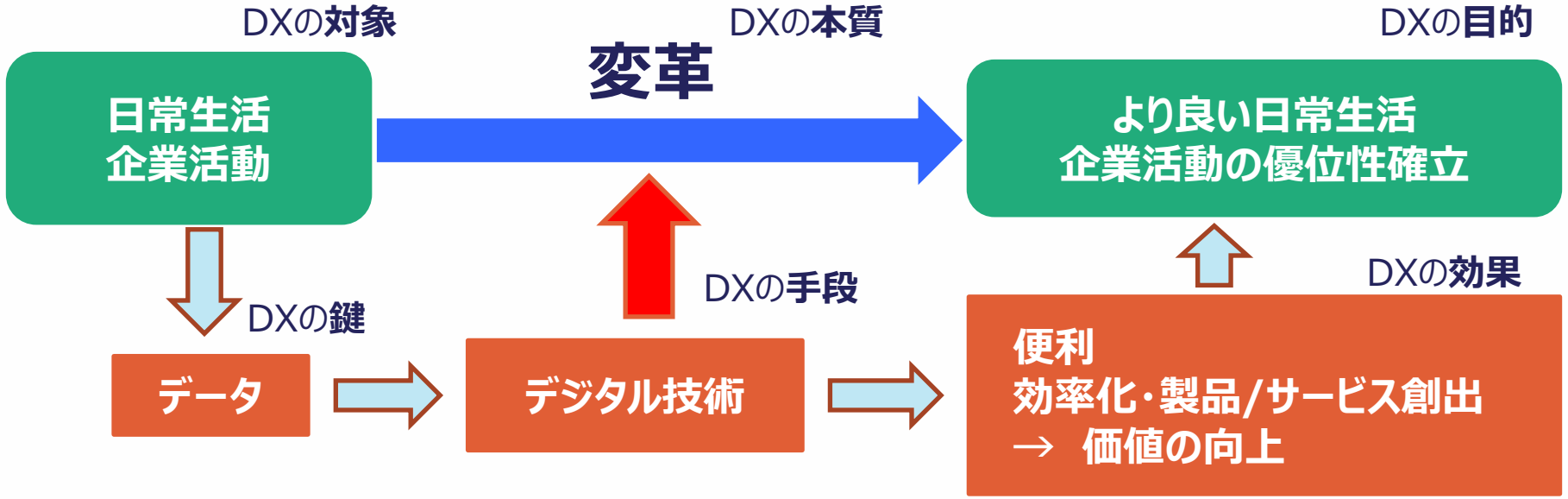
・デジタル技術を浸透させることで、生活をより良いものにする

※2004年にスウェーデンのウメオ大学のエリック・ストルターマン教授が提唱

・企業がデジタル技術を利用して、業務や組織を変革して優位性を確立

※2018年に経済産業省が策定したDX推進のためのガイドライン

「企業がビジネス環境の激しい変化に対応し、**データとデジタル技術を活用**して、顧客や社会のニーズを基に、**製品やサービス、ビジネスモデルを変革**するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、**競争上の優位性を確立**すること。」



DXの３つのステップ

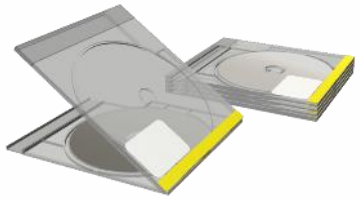
デジタイゼーション　デジタルデータ化

デジタライゼーション　個別の業務のデジタル化

デジタルトランスフォーメーション　ビジネスモデルの変革

DXの例：音楽・動画サブスク

10年前



4Gネットワーク（低速）
ガラケー　　パケット制限

技術的に無理
コスト的に無理

現在

5Gネットワーク（高速）、WiFi
スマートフォン　　パケット使い放題

技術・コスト面解決
こっちの方が便利

▼みなさんの事業

	今の形	新しい形	
2024年の技術	今の形	新しい形	今あるテクノロジーで、新しい形はあるのか
2029年の技術	今の形	新しい形	将来のテクノロジーで、新しい形はあるか

将来のテクノロジーで、今の形は成り立つか

サイバーセキュリティって必要？

いままでも・・・

- （紙の）書類、現金
- 現物

→

- 戸締り。書棚・引き出し・金庫収納、施錠
- 見張り、記録簿
- 手口の巧妙化、悪質化に備えて対応（鍵の付替え、防犯カメラ） … etc.

- 社内ネットワーク＝オフィス
- ウェブサイト＝ショールーム
- ECサイト＝店舗

↓

仕事をデジタル化したら
その防犯もデジタル化
仕事が便利になったぶん、犯罪者にも便利
“実物を扱わない、時間や距離の制約がなくなる”

防犯・防災、何かあった時のための備えは、
いままでどおりに必要
いままで以上に大切

情報セキュリティ10大脅威

https://www.ipa.go.jp/security/10threats/index.html

- IPAが情報セキュリティ対策の普及を目的に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**IPAが脅威候補を選出**、セキュリティ専門家や企業のシステム担当等から構成される**「10大脅威選考会」が投票**、**TOP10入りした脅威を「10大脅威」**として脅威の概要、被害事例、対策方法等を解説

＜解説書＞

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

最近の「組織」における脅威動向

- **「ランサムウェアによる被害」**が引き続き**1位**。
- **「サプライチェーンの弱点を悪用した攻撃」**が引き続き**2位**。
- 「修正プログラムの公開前を狙う攻撃（**ゼロデイ攻撃**）」、「**脆弱性**対策情報の公開に伴う悪用増加」も上昇

⇒ 挙げられた脅威個々や順位ではなく、手段（手口）と結果（犯罪者・攻撃者の目的）を**関連づけて捉える**必要

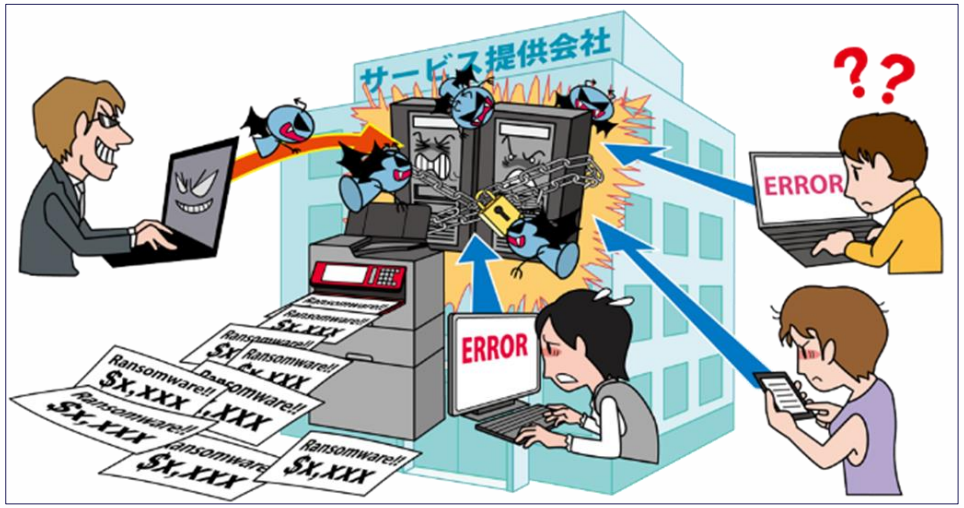
順位	2022	2023	2024
1	**ランサムウェアによる被害**	**ランサムウェアによる被害**	**ランサムウェアによる被害**
2	標的型攻撃による機密情報の窃取	**サプライチェーンの弱点を悪用した攻撃**	**サプライチェーンの弱点を悪用した攻撃**
3	**サプライチェーンの弱点を悪用した攻撃**	標的型攻撃による機密情報の窃取	**内部不正による情報漏えい等の被害**
4	テレワーク等のニューノーマルな働き方を狙った攻撃	**内部不正による情報漏えい**	**標的型攻撃による機密情報の窃取**
5	**内部不正による情報漏えい**	テレワーク等のニューノーマルな働き方を狙った攻撃	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**
6	脆弱性対策情報の公開に伴う悪用増加	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**	不注意による情報漏えい等の被害
7	**修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）**	ビジネスメール詐欺による金銭被害	**脆弱性対策情報の公開に伴う悪用増加**
8	ビジネスメール詐欺による金銭被害	**脆弱性対策情報の公開に伴う悪用増加**	ビジネスメール詐欺による金銭被害
9	予期せぬIT基盤の障害に伴う業務停止	不注意による情報漏えい等の被害	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	不注意による情報漏えい等の被害	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪のビジネス化（アンダーグラウンドサービス）

結果（目的）
相互の関連も…

手段（手口）

情報セキュリティ10大脅威2024　1位～2位

【1位】ランサムウェアによる被害
～組織の規模や業種は関係なし！次の標的はあなたの組織かも？～



- 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

【２位】サプライチェーンの弱点を悪用した攻撃
～ビジネスもセキュリティ対策も関係組織で二人三脚を～

- 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
- 取引先や業務を委託している**外部組織から情報漏えい**

【出典】 令和５年上半期におけるサイバー空間をめぐる脅威の情勢等について(警察庁)
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R05_kami_cyber_jousei.pdf

情報セキュリティ10大脅威2024　3位～4位

【3位】内部不正による情報漏えい
～組織の情報を狙っているのは身内かも!?不正をゆるさない体制作りを～

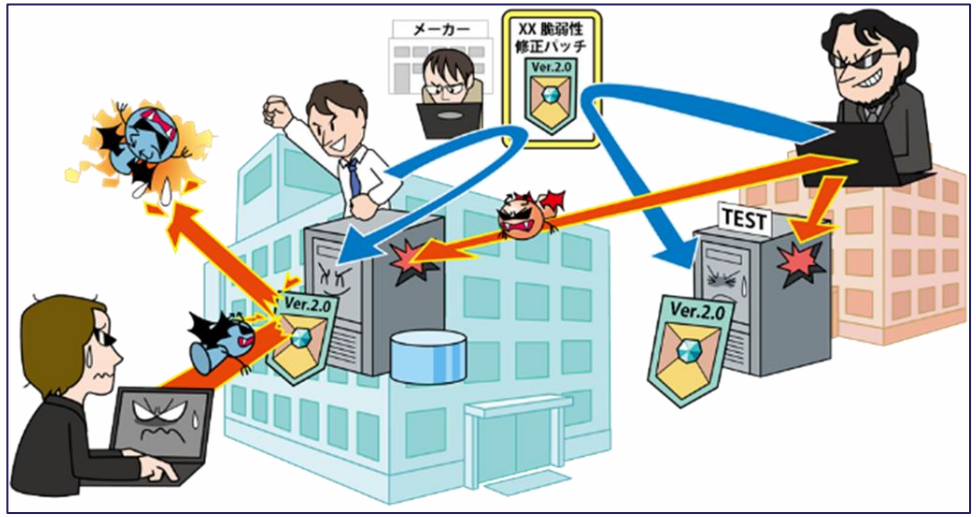
- 組織の**従業員や元従業員等**による機密情報の漏えい
- 組織関係者による不正行為による、組織の**社会的信用の失墜**、損害賠償による**経済的損失**
- 不正に取得した情報を**他組織に持ち込んだ場合、その組織も**損害賠償等の対象になるおそれがある

【4位】標的型攻撃による機密情報の窃取
～攻撃手口は様々、隙を作らない対策を～

- 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**システムの破壊**を行う

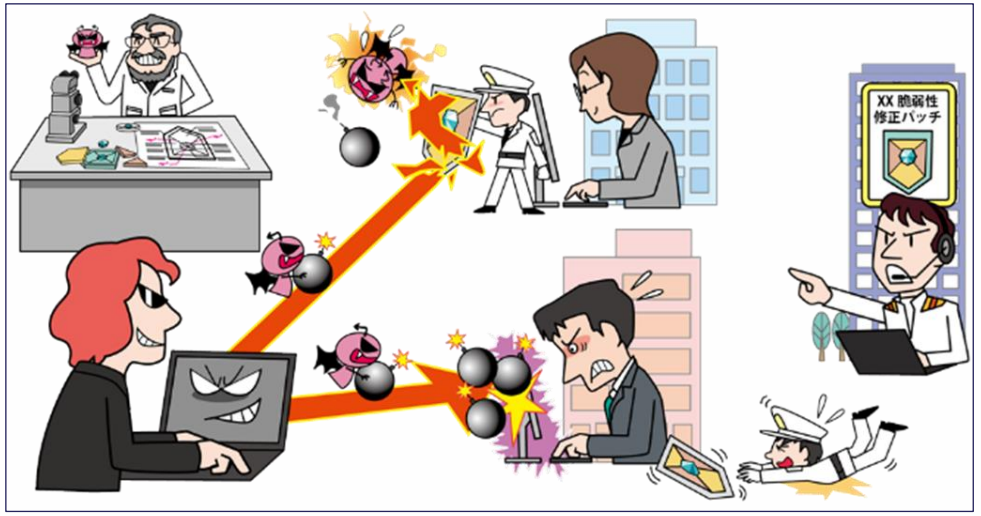
情報セキュリティ10大脅威2024　5位と7位

【5位】修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)
～脆弱性対策情報が公開されたら即時対応を～



- 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
- **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

【7位】脆弱性対策情報の公開に伴う悪用増加
～放置せず、傷口が広がる前に速やかな処置を～



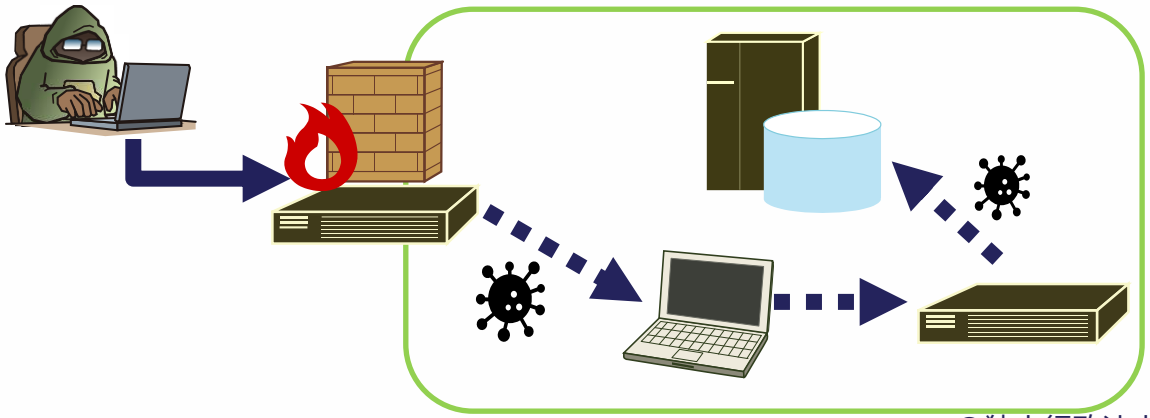
- 脆弱性対策のために公開された**脆弱性情報を攻撃者が悪用**する
- 広く利用されている製品の脆弱性の場合は**被害が広範囲**に及ぶ
- 脆弱性情報の公開後、それらを悪用した**攻撃が発生するまでの時間が近年は短くなっている**傾向がある

激化するネットワーク貫通型攻撃

- インターネットとの**境界に設置される装置を狙った攻撃が激化**。
- 自宅や出張先から組織ネットワークに接続するために利用される**VPN機器等の脆弱性が狙われる**。
- 最新のセキュリティパッチの適用や、機器の認証情報が漏えいしていないかの注意が必要。

ネットワーク貫通型攻撃とは

組織のネットワークと**インターネットとの境界に設置されるセキュリティ製品やVPN機器、サーバ等の脆弱性が狙われる**。
インターネットとの境界に設置される装置から**内部に侵攻され、保有情報の漏えいや改ざんにつながる**。また、ダークウェブ等に漏えいした機器の**認証情報が悪用されること**も。



近年、ネットワーク境界に設置される装置を狙った攻撃が増加

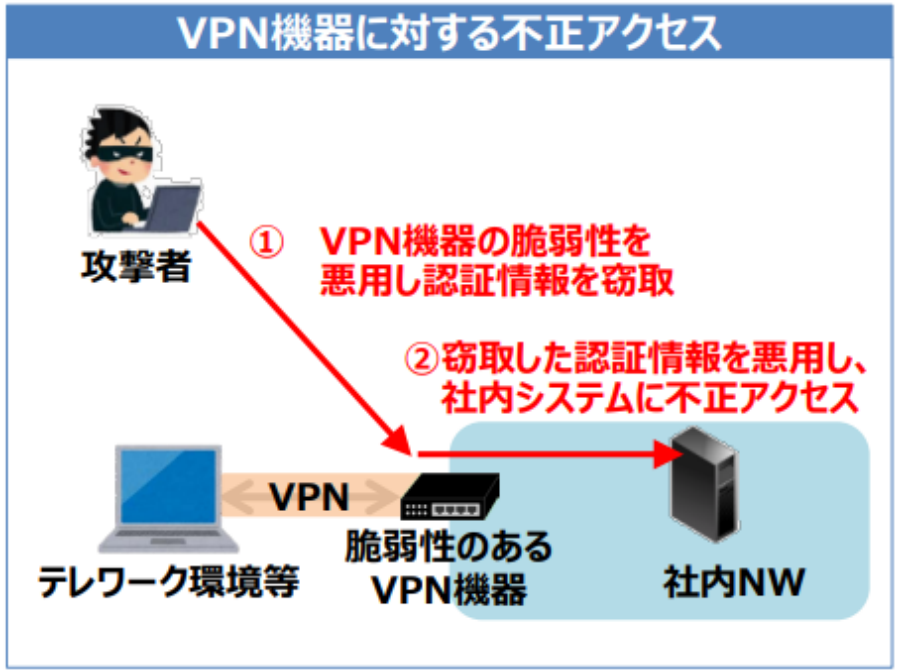
VPN機器に加え、メールセキュリティゲートウェイ、オンラインストレージサーバ、Webアプリケーションサーバ、ネットワーク機器等が攻撃の対象となる。
近年、これらの装置を狙った攻撃が増加しており、**2024年に入ってからも頻発**している。

平時から対策を

IPAでは、2023年8月及び2024年4月に、ネットワーク貫通型攻撃に関する注意喚起を実施。

当該注意喚起にて、**日々の各種ログの確認や、製品ベンダから発信される情報の収集、機器の外部公開状態の確認**を促している。

ネットワーク境界がアタックサーフェス（攻撃対象領域）に



出典)「最近のサイバー攻撃の状況を踏まえた経営者への注意喚起」2020/12/18 経済産業省

2023/8/1	**インターネット境界に放置された装置に対するサイバー攻撃について～ネットワーク貫通型攻撃に注意しましょう～** https://www.ipa.go.jp/security/security-alert/2023/alert20230801.html
2023/10/19	**オンラインストレージの脆弱性対策について** https://www.ipa.go.jp/security/security-alert/2023/alert20231019.html
2024/04/18	**アタックサーフェスの Operational Relay Box 化を伴うネットワーク貫通型攻撃に** https://www.ipa.go.jp/security/security-alert/2024/alert_orb.html

必要となる対策

- サプライチェーン全体での取組み
  - 迅速・的確な情報連携
  - 相互理解・相互確認
- 企業個々の取組み
  - ルール、組織体制の整備、確立（万一の際の対応～復旧手順を含む）
  - 組織の外部（インターネット）からアクセス可能なIT資産、リスクの把握
  - 検知、防御の仕組みの導入、運用

企業個々での
必要な対策とは？

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**な対策から
- 組織の実態、必要性に合わせ**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**
- **“万が一”**に備えた**準備**を

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」を常に意識することが重要**

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

情報セキュリティ対策の基本＋α

- 昨今はクラウドサービスの利用も一般的になってきている
- クラウドサービスを利用を想定した＋αの対策を行い、
  備える必要がある

備える対象	情報セキュリティ対策の基本＋α	目的
インシデント全般	**責任範囲の明確化**(理解)	インシデント発生時に、誰(どの組織)が対応する責任があるのか、を明確化(理解)する
クラウドの停止	**代替策の準備**	業務が停止しないように代替策を準備する
クラウドの仕様変更	**設定の見直し**	仕様変更により意図せず変更された設定を適切な設定に直す(設定不備による情報漏えいや攻撃への悪用を防止する)

脅威から会社をどう守るのか
効果的な解決方法は？

■ セキュリティ対策では、“**平時からの「人」の対策**”と“**有事に向けた「仕組み」による対策**”の**両方に並行して取組む**ことが重要。

平時からの「人」の対策（防御等）

- サイバーセキュリティマネジメント体制の整備
- 情報セキュリティ規程の作成、周知徹底
- 教育等による社員意識醸成、向上

＋

有事に向けた「仕組み」による対策（検知、対応、復旧等）

- 目に見えないサイバー攻撃を可視化、異常の監視
- 何か起きた場合の緊急対応・復旧

IPAが提供する対策実践のためのツール、制度

平時の備えから、インシデントが発生してしまった後の対応・復旧支援まで

情報セキュリティの考え方や段階的に実現する為の方策を紹介する**「中小企業情報セキュリティガイドライン」**。
ガイドラインをベースに、セキュリティ対策への意識を持つための自己宣言**「SECURITY ACTION」**。
常時サイバー環境を監視しつつ、インシデントが発生してしまったが対処方法がわからない、この様な中小企業の事後対応を支援し、また簡易サイバー保険を付帯した**「サイバーセキュリティお助け隊」**

平時の対策支援（社内体制整備、意識向上）

中小企業情報セキュリティ対策ガイドライン

- 中小企業におけるセキュリティ対策の考え方、具体的方策を紹介。

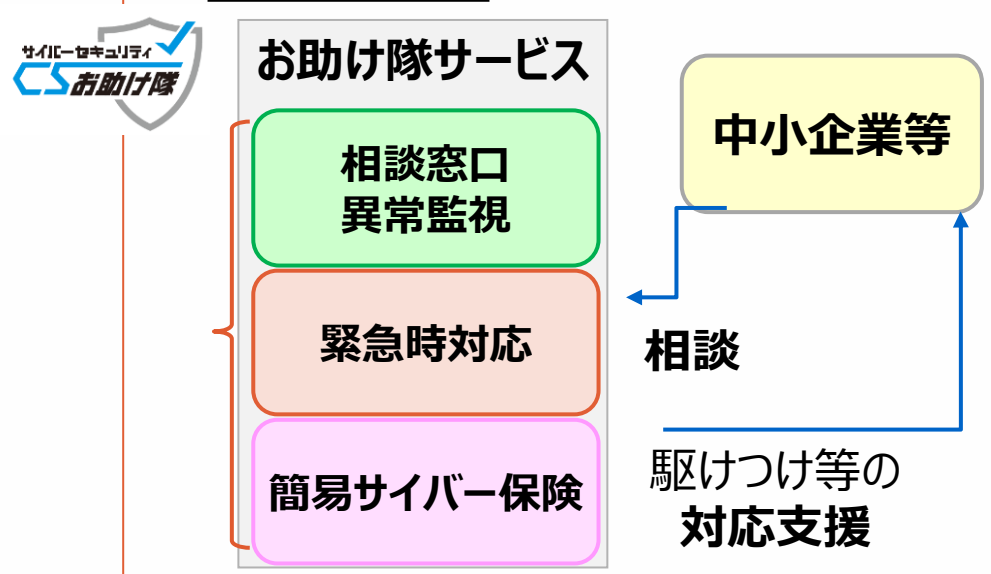
SECURITY ACTION

- セキュリティ対策に取組むことを事業者が自己宣言する制度。

有事の対策支援（検知、対応、復旧等）

サイバーセキュリティお助け隊

- 中小企業等がサイバー攻撃等で困った時の**相談窓口、駆けつけ支援体制**を構築。



日頃からの「人」の対策

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
  - **「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」**を追加

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

付録一覧

付録1：情報セキュリティ5か条(PDF)

付録2：情報セキュリティ基本方針（サンプル）(Word)

付録3：5分でできる！情報セキュリティ自社診断(PDF)

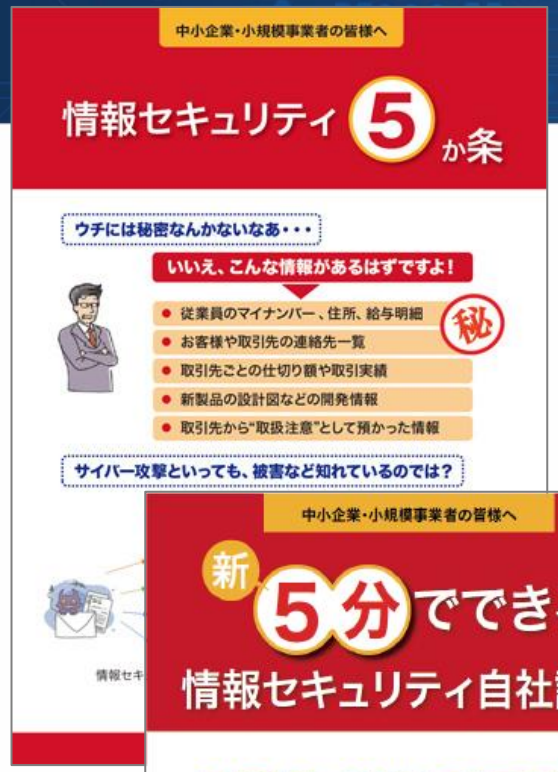
付録4：情報セキュリティハンドブック（ひな形）(PowerPoint)

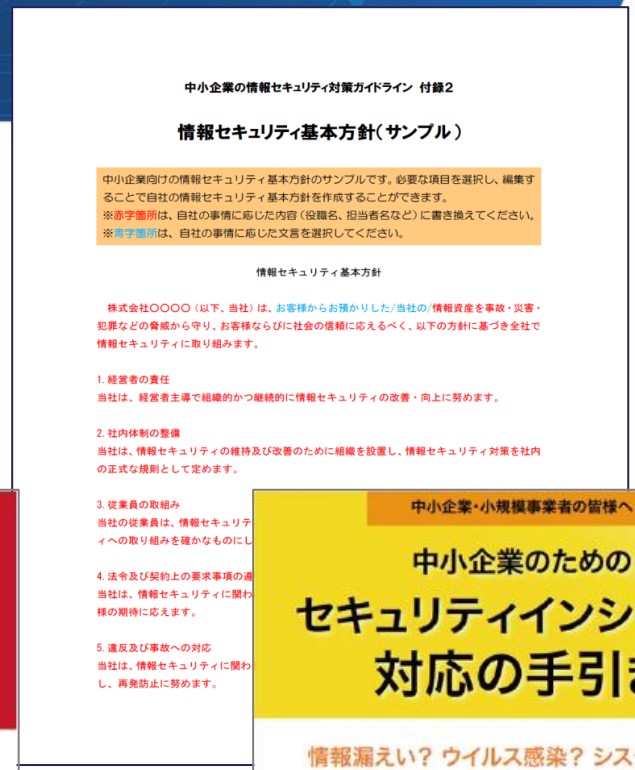
付録5：情報セキュリティ関連規程（サンプル）(Word)

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(PDF)

付録7：リスク分析シート（全7シート）(Excel)

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手引き(PDF)





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)　事業の停止
(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」

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」と実行すべき「重要7項目の取組」

- 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
原則２	**委託先**の情報セキュリティ対策まで考慮する
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

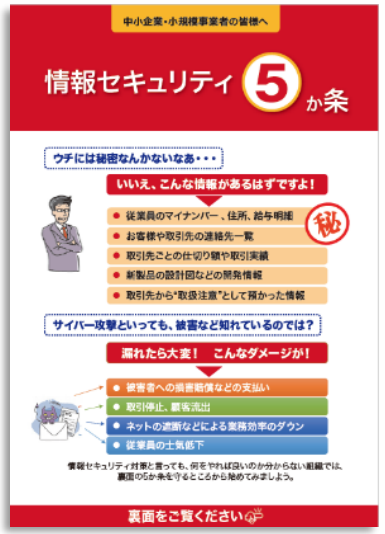
- 経営者は、以下の**７項目**を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

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

第２部 実践編

- **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

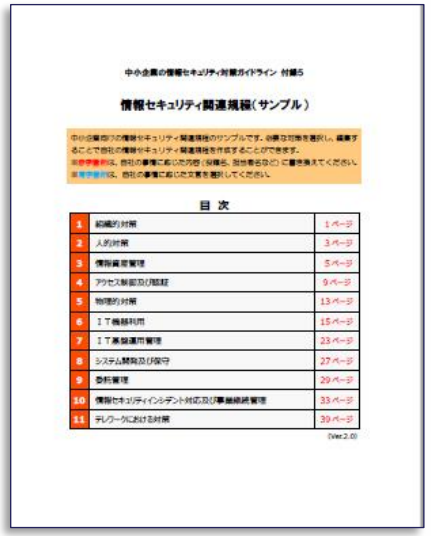
SECURITY ACTION ★一つ星を宣言

Step2
組織的な取り組みを開始する

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
- テレワークの情報セキュリティ
- セキュリティインシデント対応
- セキュリティサービス例と活用
- 技術的対策例と活用
- 詳細リスク分析の実施方法

より強固にするため方策

日頃からの「人」の対策
～“はじめの一歩”と“二歩目”～

できるところから始める

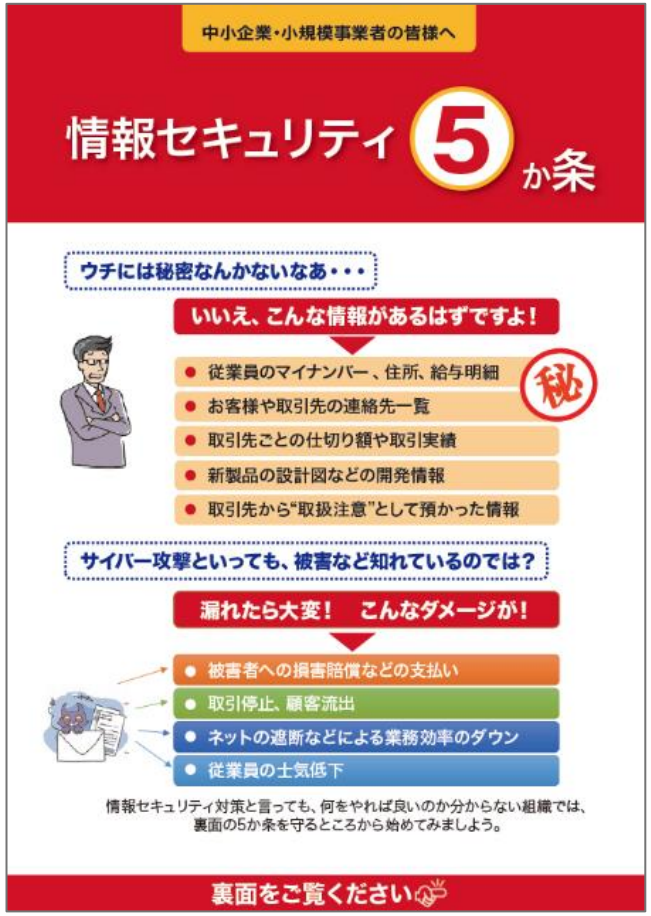
情報セキュリティ5か条

- 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！



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
  https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055848.pdf
  - **25項目の設問**に答えることで、自社の情報セキュリティ上の**問題点の把握**が可能
  - **解説編**の対策例を参考に、**社内ルールの作成**が可能
  - ガイドライン付録の**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**が可能

5分でできる！情報セキュリティ自社診断

自社診断のための25項目

- 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

診断項目	No	診断内容
Part 1 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？
Part 2 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、重要情報が記載された書類や電子媒体は机上に放置せず、書庫など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や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？
Part 3 組織としての対策	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握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合に備え、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？

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

対策例を参考にして決定

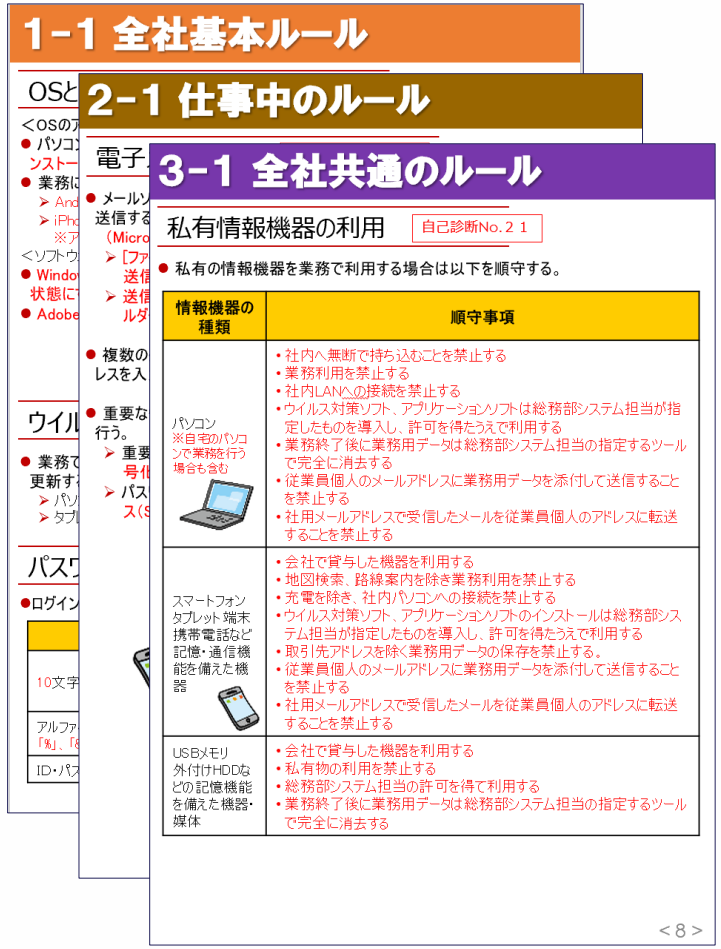
診断編 NO.1 脆弱性対策

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、もしく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、Java実行環境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「JVN iPedia脆弱性対策情報データベース検索」で確認する。



情報セキュリティハンドブックを編集して周知

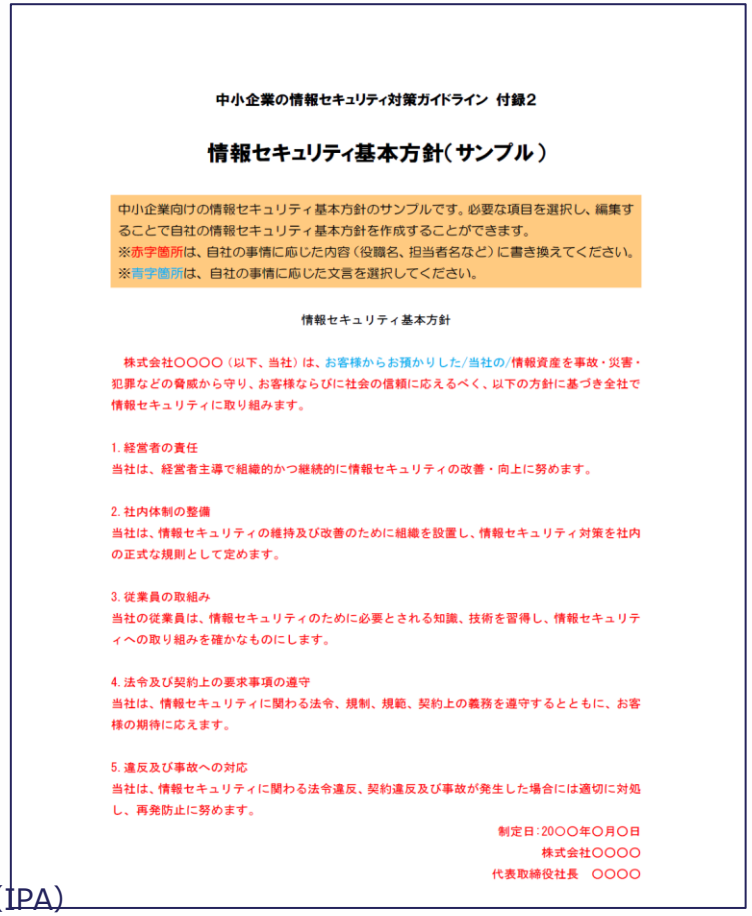
組織的な取り組みを開始する

「情報セキュリティ基本方針」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
- 付録の**「情報セキュリティ基本方針（サンプル）」**を活用

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・ガイドライン等の整備
- セキュリティ対策の実施
- 継続的改善　　など



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○○○○（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、規制、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○○年○月○日
株式会社○○○○
代表取締役社長　○○○○

SECURITY ACTION ★★
セキュリティ対策自己宣言

対策実践に向けた“はじめの一歩”、そして“2歩目”
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（※）
- 「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段階の取組目標**を用意
- 宣言者数は、約33万件（2024年3月現在）

※IPAが各企業等の情報セキュリティ対策状況等を認定する、あるいは認証等を付与する制度ではありません。

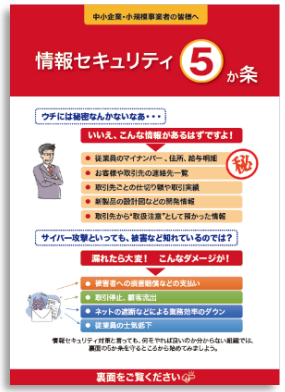
１段階目（一つ星）

●情報セキュリティ５か条に取り組む

【情報セキュリテイ５か条】

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

★一つ星



2段階目（二つ星）

●情報セキュリティ自社診断を実施
●基本方針を策定

【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

★★二つ星

SECURITY ACTION制度のメリット

1．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

2．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

3．**公的補助**・民間の支援あり

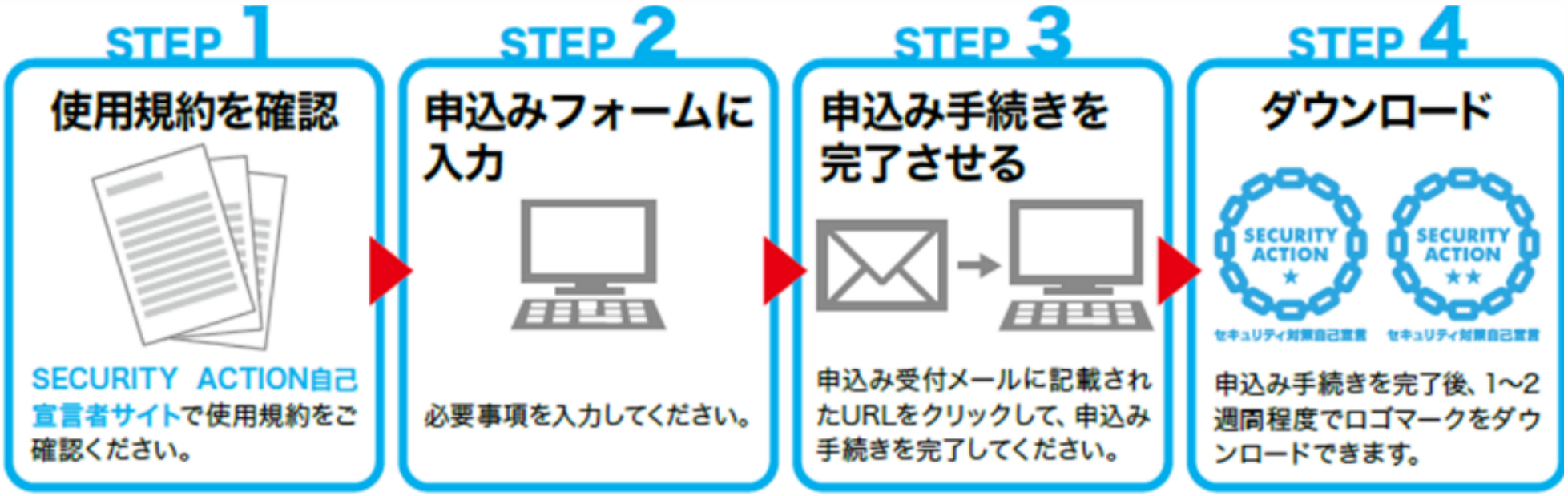
👉 SECURITY ACTIONを要件または加点要素とする補助金、普及賛同企業等から提供される様々な支援策が利用可能（SECURITY ACTION普及賛同企業等：https://www.ipa.go.jp/security/security-action/promotion/index.html）

見える化

信頼関係

公的補助

SECURITY ACTION 申込手順



SECURITY ACTION自己宣言者サイト

https://security-shien.ipa.go.jp/security/entry/

日頃からの「人」の対策
～本格的に取り組み、強固にしていくために～

本格的に取り組む
管理体制の構築

- 情報セキュリティ対策を推進するための**管理体制**を決定
- 付録5「情報セキュリティ関連規程（サンプル）」を活用して自社の管理体制を社内に周知

【表８】情報セキュリティ管理のための役割と責任分担（例）

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	情報セキュリティ対策のためのシステム管理を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

【表９】緊急時対応体制の役割と責任（例）

役職名	役割と責任
情報セキュリティ責任者 （例：代表取締役）	事故の影響を判断し、対応について意思決定する。
情報セキュリティ部門責任者 （例：管理部長、営業部長）	・事故の原因を調べて情報セキュリティ責任者に報告する。 ・情報セキュリティ責任者の判断・意思決定に基づき適切な処置を行う。 ・事故の原因や被害が情報システムに関係する場合はシステム管理者と連携して適切な処置を行う。
システム管理者 （例：管理部長兼務）	事故の原因や被害が情報システムに関係する場合は情報セキュリティ部門責任者と連携して適切な処置を行う。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告する。

社内規程

1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者。情報セキュリティ対策などの決定権限を有するとともに、全責任を負う。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者。各部門における情報セキュリティ対策の実施などの責任を負う。
情報システム管理者	情報セキュリティ対策のためのシステム管理を行う。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施する。
インシデント対応責任者	事故の影響を判断し、対応について意思決定する。
監査・点検/点検責任者	情報セキュリティ対策が適切に実施されているか情報セキュリティ関連規程を基準として検証または評価し、助言を行う。
特定個人情報事務取扱責任者	特定個人情報の情報セキュリティに関する責任者。
特定個人情報事務取扱担当者	特定個人情報を取り扱う事務に従事する従業員。
個人情報苦情対応責任者	個人情報に関する苦情の対応責任者。

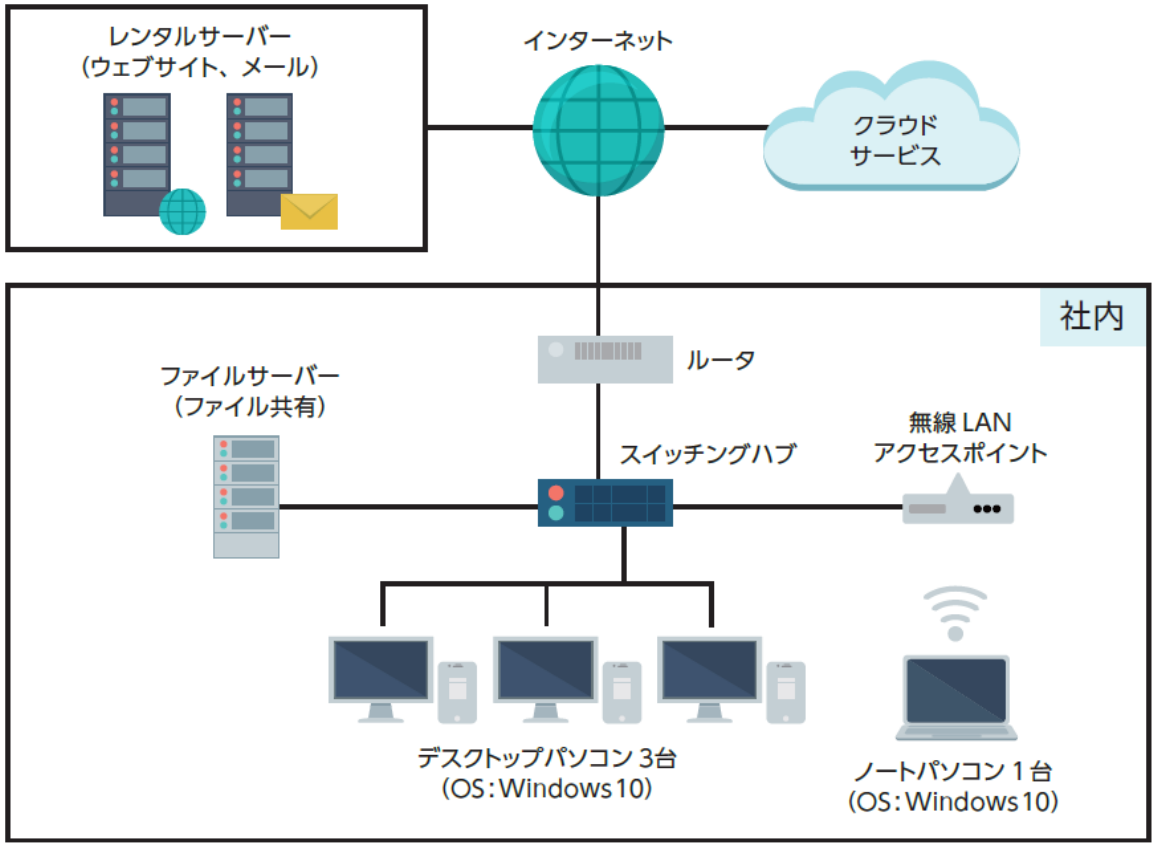
<情報セキュリティ委員会体制図>

1

本格的に取り組む

DXの推進と情報セキュリティの予算化

- 自社の情報システムについて、インターネットとの接続状況を把握
- 情報セキュリティ対策を検討して予算を確保



テレワークを導入するにあたり・・・

クラウドのセキュリティ確認
リモート接続のセキュリティ確保
利用者認証の強化

DX（Digital Transformation）

企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。

情報セキュリティ規程の作成（1）

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

本格的に取り組む情報セキュリティ規程の作成（2）

③規程の作成

- 付録5「情報セキュリティ関連規程（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

	名称	概要
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限方針や認証のルールを定めます。
5	物理的対策	セキュリティ領域の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	システムの開発及び保守	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。業務委託契約書の機密保持に関する条項例と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ならびに事業継続管理	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決めます。
11	個人番号及び特定個人情報の取り扱い	マイナンバーの取り扱いに関するルールを定めます。
12	テレワークにおける対策	テレワークにおけるセキュリティに関するルールを定めます。

より強固にするための方策

- **より強固な情報セキュリティ対策に取り組むために、以下の8つの区分について説明**

(1) **情報収集と共有**
  - 情報セキュリティに関する情報収集の方法と情報共有の枠組み

(2) **ウェブサイトの情報セキュリティ**
  - ウェブサイトを安全に構築し、運用するためのポイント

(3) **クラウドサービスの情報セキュリティ**
  - クラウドサービスを安全に利用するためのポイント

(4) **テレワークの情報セキュリティ**
  - テレワークを安全に実施するためのポイント

(5) **セキュリティインシデント対応**
  - セキュリティインシデント発生時の対応

(6) **セキュリティサービス例と活用**
  - 情報セキュリティに関する外部サービス

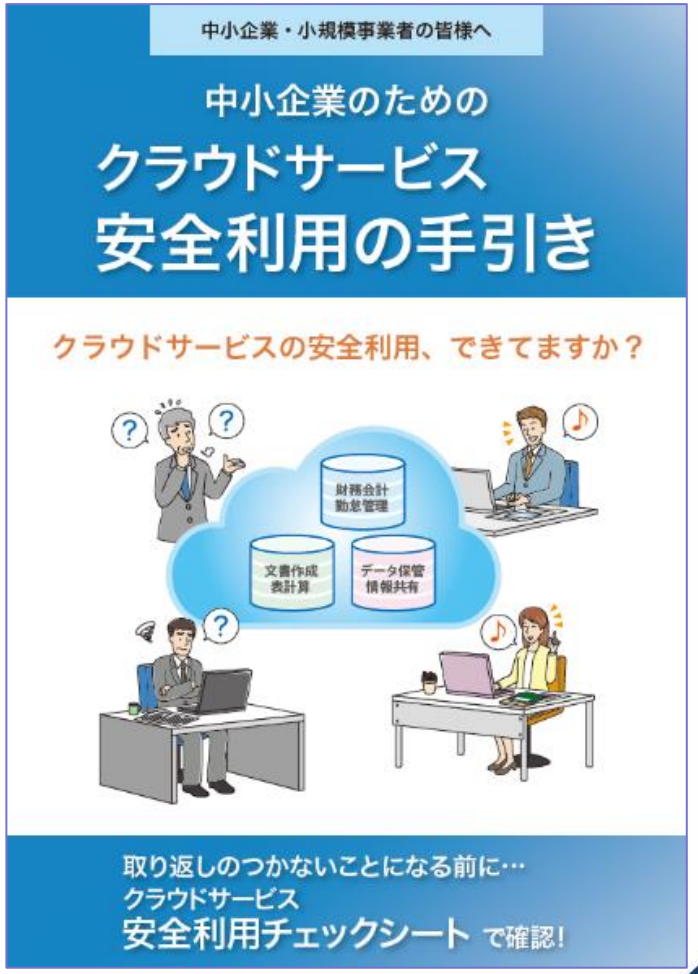
(7) **技術的対策例と活用**
  - ITを活用する際の技術的対策

(8) **詳細リスク分析の実施方法**
  - 「リスク分析シート」（付録7）を活用した詳細リスク分析の実施方法

付録6 クラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/sme/f55m8k0000001wcf-att/000072150.pdf

- クラウドサービスを安全に利用するためには、何をやれば良いのか、を説明
  - **クラウドサービス安全利用チェックシート** ⇒ 確認すべきことの把握
  - 解説編 ⇒ 身近なサービスを例に、何を確認し、どうしたら**安全に利用することができるか**説明



クラウドサービスの情報セキュリティ

- クラウドサービスの選定から運用までのセキュリティ対策を３つの段階に分けて検討事項を説明

クラウドサービスの選定

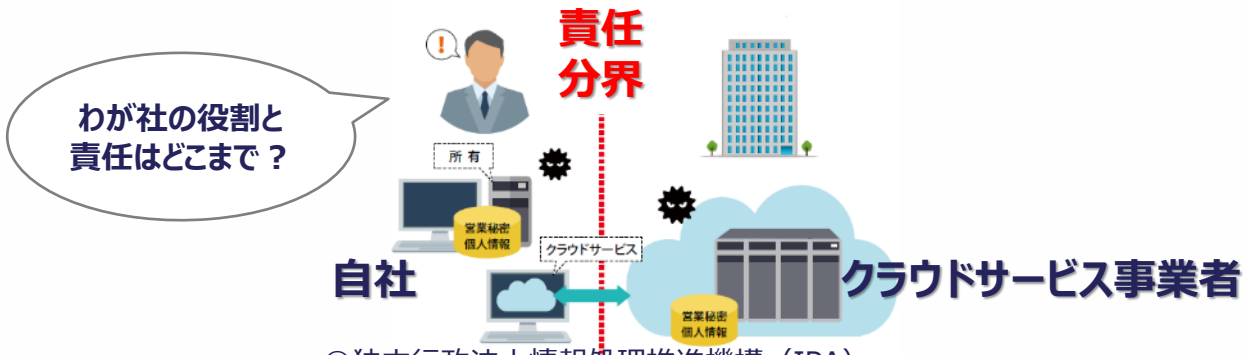
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、業務のセキュリティ要件に見合ったサービスを選定しましょう。

クラウドサービスの運用

クラウドサービスは提供者と利用者が連携して運用するため、その特性を理解して運用しましょう。

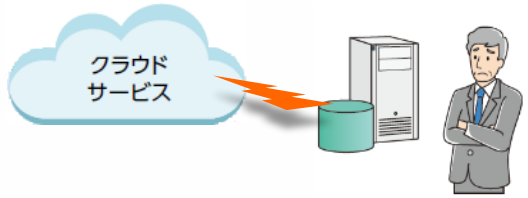
クラウドサービスのセキュリティ対策

サービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。



選択するときの確認ポイント（抜粋）

11	**付帯するセキュリティ対策を確認する**	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	**利用者サポートの体制を確認する**	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	**利用終了時のデータを確保する**	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
14	**適用法令や契約条件を確認する**	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
15	**データ保存先の地理的所在地を確認する**	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

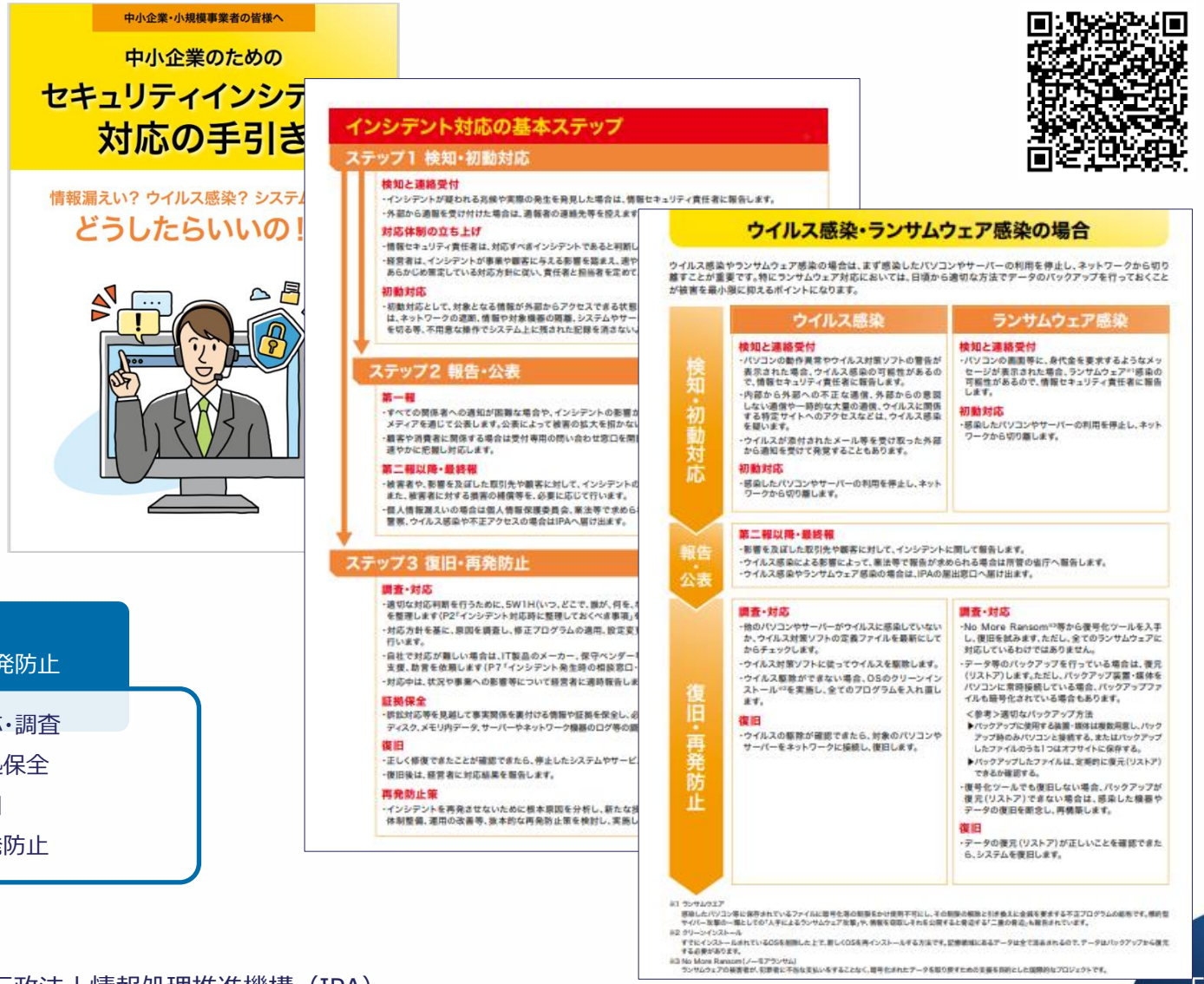


万一の事態に備えて

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

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf

- インシデント対応時に整理しておくべき事項のリストや、「**検知・初動対応**」「**報告・公表**」「**復旧・再発防止**」といった基本ステップごとのアクションを提示
- 「**ウイルス感染・ランサムウェア感染**の場合」「**情報漏えい**の場合」「**システム停止**の場合」といった場合ごとに解説するほか、相談窓口や報告先も紹介

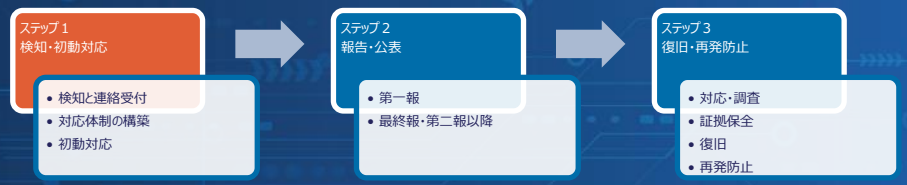


ステップ1 検知・初動対応
- 検知と連絡受付
- 対応体制の構築
- 初動対応

ステップ2 報告・公表
- 第一報
- 最終報・第二報以降

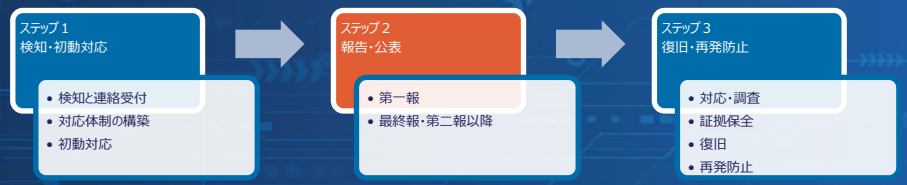
ステップ3 復旧・再発防止
- 対応・調査
- 証拠保全
- 復旧
- 再発防止

ステップ１　検知・初動対応



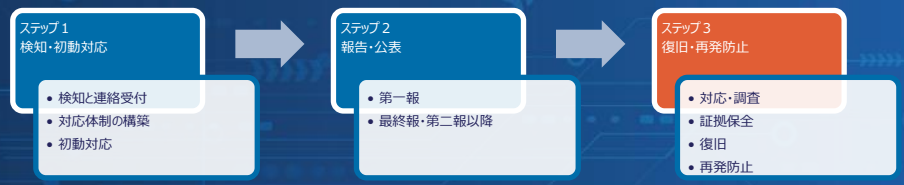
- **検知と連絡受付**
  - インシデントが疑われる兆候や実際の発生を発見した場合は、情報セキュリティ責任者に報告
  - 外部から通報を受け付けた場合は、通報者の連絡先等を記録。
- **対応体制の構築**
  - 情報セキュリティ責任者は、対応すべきインシデントであると判断したら、速やかに経営者に報告
  - 経営者は、インシデントが事業や顧客に与える影響を踏まえ、速やかにインシデント対応のための体制を立ち上げ、あらかじめ策定している対応方針に従い、責任者と担当者を定めて、役割分担を明確化
- **初動対応**
  - 初動対応として、対象となる情報が外部からアクセスできる状態にある場合や、被害が広がる可能性がある場合は、ネットワークの遮断、情報や対象機器の隔離、システムやサービスの停止を実施。
    - ただし、対象機器の電源を切る等、不用意な操作でシステム上に残された記録を消さないよう注意

ステップ２ 報告・公表



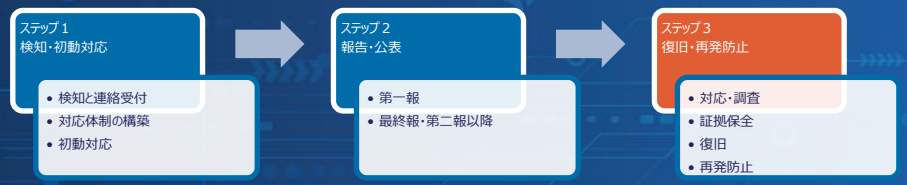
- **第一報**
  - すべての関係者への通知が困難な場合や、インシデントの影響が広く一般に及ぶ場合は、状況をウェブサイトや、メディアを通じて公表
    - 公表によって被害の拡大を招かないよう、時期、内容、対象などを考慮
  - 顧客や消費者に関係する場合は受付専用の問い合わせ窓口を開設し、被害が発生・拡大した場合にはその動向を速やかに把握し対応
- **第二報以降・最終報**
  - 被害者や、影響を及ぼした取引先や顧客に対して、インシデントの対応状況や再発防止策等に関して報告。また、被害者に対する損害の補償等を、必要に応じて実施
  - 個人情報漏えいの場合は個人情報保護委員会、業法等で求められる場合は所管の省庁等、犯罪性がある場合は警察、ウイルス感染や不正アクセスの場合はIPAへ届け出

ステップ３ 復旧・再発防止



- **調査・対応**
  - 適切な対応判断を行うために、5W1H（いつ、どこで、誰が、誰を、何を、なぜ、どうしたのか）の観点で状況を調査し情報を整理
  - 対応方針を基に、原因を調査し、修正プログラムの適用、設定変更、機器の入替データの復元等、必要な修復を実施
  - 自社で対応が難しい場合は、IT製品のメーカー、保守ベンダー等の外部専門組織や公的機関の相談窓口等に支援、助言を要請
  - 対応中、担当（責任）者は、状況や事業への影響等について経営者に適時報告

ステップ３ 復旧・再発防止



- **証拠保全**
  - 訴訟対応等を見越して事実関係を裏付ける情報や証拠を保全し、必要に応じてフォレンジック調査（パソコンのハードディスク、メモリ内データ、サーバーやネットワーク機器のログ等の調査）を実施
- **復旧**
  - 正しく修復できたことが確認できたら、停止したシステムやサービスを復旧を実施
  - 復旧後は、経営者に対応結果を報告
- **再発防止**
  - インシデントを再発させないために根本原因を分析し、新たな技術的対策の導入、ルールの策定、教育の徹底、体制整備、運用の改善等、抜本的な再発防止策を検討、実施

事象ごとの対応のポイント

- **ウイルス感染・ランサムウェア感染の場合**
  - まず感染したパソコンやサーバーの**利用を停止**し、**ネットワークから切り離す**ことが重要
  - **ランサムウェア対応**では、日頃から**適切な方法でデータのバックアップ**実施が**被害を最小限化**のポイント
- **情報漏えいの場合**
  - 情報漏えいには、ネットワークへの「**不正アクセス**」、従業員による「**内部犯行**」、電子メールの「**誤送信**」、Webでの「**誤公開**」、「**紛失・置忘れ**」等によるもの
  - 特に、**不正アクセスによる情報漏えい**は、**データの大量流出**につながるおそれがあるため、**インターネットに接続しているサーバへの対策**が必要
  - 不正アクセスや内部犯行は**犯罪性**があるため、**警察への届け出**も必要
- **システム停止の場合**
  - システム停止は、サイバー攻撃などのセキュリティ上の問題、不具合・ソフトウェアのバグ、機器の故障、など**様々な原因**が想定され、**異常の発見時**には**原因不明の可能性**あり。**原因不明の場合は、セキュリティ上の問題の可能性も含めて対応**を行う必要
  - また、**システムの停止**は事業や企業**経営に重大な影響**を与える場合があるので、経営者は**事業継続計画（BCP）を策定**し備える必要

インシデント対応時に整理しておくべき事項

インシデントの分類	情報漏えい 、ウィルス感染、システム停止など
事業者	事業者の名称 ※自社の受託案件に関連したインシデントの場合は委託元含む関係事業者の名称
担当者・責任者	本件に関する責任者および担当者の所属、氏名
発覚日時	インシデントを認知した日時
発生日時	調査で判明したインシデントの発生日時
発生事象	表面化している事柄、被害、影響など
対応経過	発生から現時点までの時系列での経過
想定される原因	現時点で想定される直接的な原因
被害を受けたシステムの状況	被害を受けたシステムの概要・詳細
システム構成・運用状況	システムの物理的所在地やOS、アプリケーションとバージョン構成 ※可能であれば簡単な構成図等も併記 システムの運用状況やセキュリティツール・サービスの利用状況等

※サイバーセキュリティ経営ガイドライン 付録C「ンシデント発生時に組織内で整理しておくべき事項」も参考になります
https://www.meti.go.jp/policy/netsecurity/mng_guide.html

有事に向けた「仕組み」による対策

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**不可欠なサービスをワンパッケージ**で要件化した**民間サービス**の登録制度。2021年4月から開始
- 現在**35社**から**45サービス**が展開
- **IT導入補助金（セキュリティ対策推進枠）**が利用可能

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

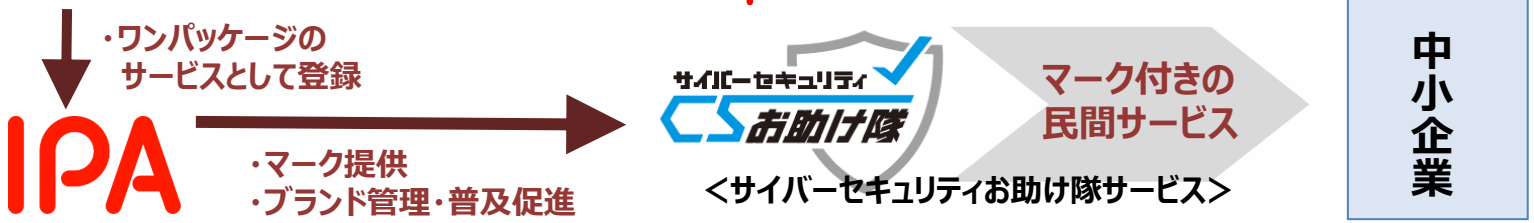
24時間見守る仕組み
ネットワーク監視型
端末監視型
その併用型

緊急時の対応支援
インシデント発生などの緊急時に駆け付け支援

導入・運用のしやすさ
専門知識がなくても導入・運用できるような工夫

簡易サイバー保険
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

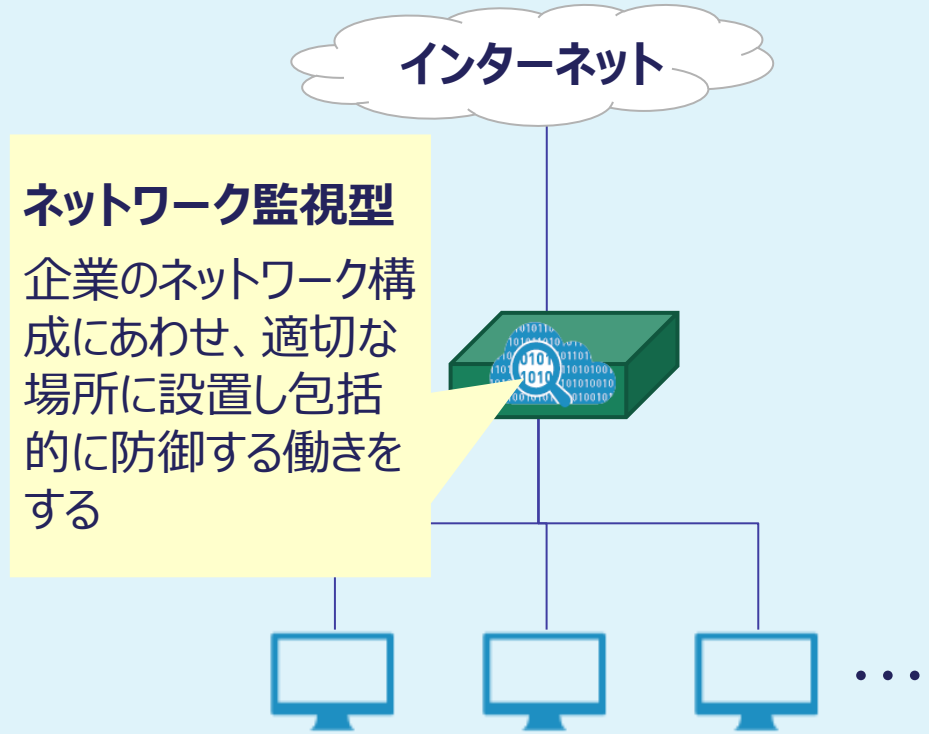
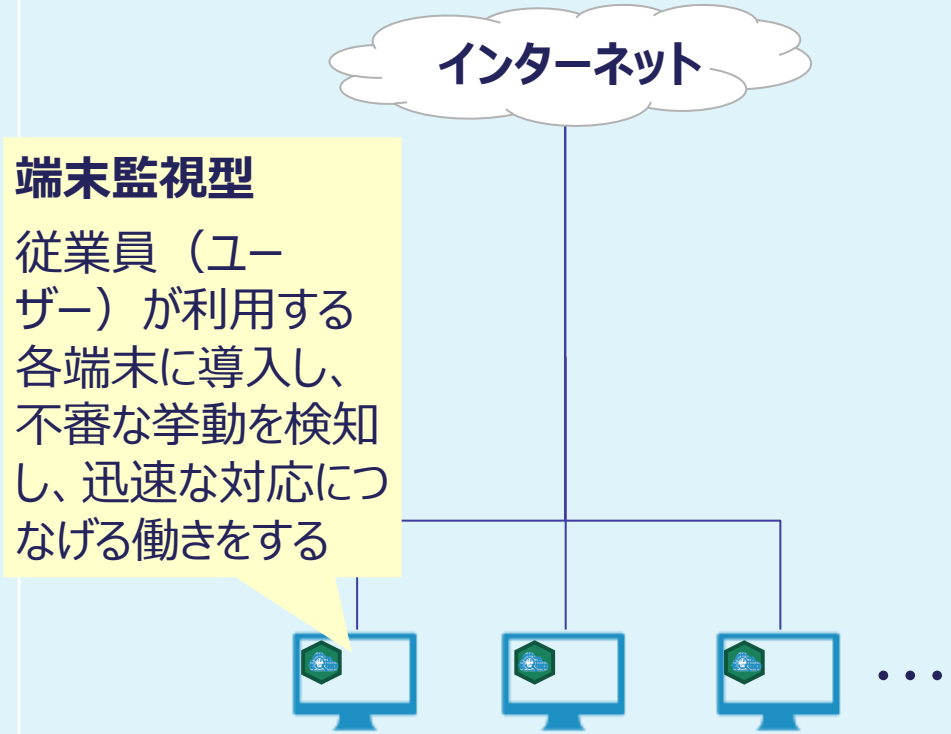
中小企業でも導入、維持できる価格
・ネットワーク監視型：月額１万円以下
・端末監視型：月額2,000円以下／台
・併用型：これらの合算相当価格以下



「サイバーセキュリティお助け隊サービス」

異常の監視の仕組み

- 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もっとも大切**。
- サイバーセキュリティお助け隊サービスでは、**ネットワーク監視型**、**端末監視型**、またはその**両方（併用型）**による異常の監視を提供。

	ネットワーク監視型	端末監視型
構成		

セキュリティ監視の仕組みの選び方
どれを選べばいいのか？ <<監視型による特長と選ぶ時のポイント>>

監視型	説明	
	特長	選ぶ時のチェックポイント
ネットワーク監視型	（一般的に）**インターネットと社内ネットワークの間にUTM等の監視機器**を設置し、**ネットワーク通信（内外）の監視、防御**する形態のもの	
	【メリット】 • **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を従業員一人一人が行う必要がなく、**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）	**自社のネットワーク負荷が耐えられるか** • **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。
端末監視型	（一般的に）社内**ネットワークに接続しているPC**に、**EDR等のセキュリティソフトウェアをインストール**して、**端末内部の挙動を監視、防御**する形態のもの	
	【メリット】 • 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。**	**社内ネットワークに接続しているPC台数と導入可能か** • 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もあり得、自社のPCに導入可能かの確認が必要。
併用型	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**を行う形態のもの	
	【メリット】 • **より強固**なセキュリティ監視が可能。	**運用の手間の確認を** 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）。対応可能か確認が必要。

身内の不正を防ぐための目配り

内部不正による秘密情報漏えい事例

・以下すべて記事を抜粋した公知情報。転職に関連する情報漏えい事案が目立ちます。

■ **ソフトバンク → 楽天モバイル** 2021年1月逮捕
ソフトバンクに勤務していた2019年12月、5Gや基地局の情報を私用アドレスへメール、翌年1月に楽天モバイルに転職
https://www.asahi.com/articles/ASPD76D17PD7UTIL035.html
2022年12月「懲役2年、執行猶予4年、罰金100万円」判決

■ **はま寿司 → かっぱ寿司** 2022年9月逮捕
田辺氏：2014年～2017年にはま寿司取締役、その後、グループ会社の社長
2020年10月ころ、各店舗毎の売り上げデータ、仕入れ値などのデータを持ち出し
2020年11月かっぱ寿司顧問、2021年2月かっぱ寿司社長就任
https://www.asahi.com/articles/ASR503QDTR5ZUTIL00H.html
2023年5月「懲役3年、執行猶予4年、罰金200万円」判決

■ **相澤病院 → 他の医療機関** 2023年3月公表
2022年5月元職員 A は後輩職員 B に対し、業務マニュアルが見たいと言って業務用のフォルダーに保存してあったデータ（個人情報及び医療情報計3,137 名分）をコピーして窃取
2023年1月通院治療中の患者の申し出により、元職員 A から他医療機関での治療を勧誘された事実が判明
https://aizawahospital.jp/aiz/wp-content/uploads/2023/03/important_news.pdf
2023年12月「懲役1年6月、執行猶予3年、罰金50万円」判決

■ **兼松 → 双日** 2023年4月逮捕
2022年夏ころ、30代男性社員が競業他社である兼松より転職
その後、転職元が営業秘密の持ち出しを疑い調査、その上で警察に相談、2023年4月、当該男性社員逮
https://www.nikkei.com/article/DGXZQOUE081GO0Y3A001C2000000/

情報セキュリティにおける最大の弱点は…

- 情報管理上、最も脆弱なのは**「人がからむ内部不正」**ではないか。そもそも「人」の特性を考えてみると…
  - 内部事情に精通～組織において何が重要な情報なのかを把握
    → 漏えいされる情報の質・量ともインパクト大であることが多い
  - 外的／内的要因から心理的な弱点が生じることがある
  - 人は常に正常に稼働しているとは限らない「脆弱な存在」
    （疲れている・悩んでいる・忙しい・・・）
  - もちろん、うっかりすることがあるのも人間…

内部不正防止が重要である理由

- **内部不正事案の発生は組織の存続を危機に晒す場合がある**
  - 組織へのダメージは従業員にも累が及ぶ
- **問題事案の発生が内部不正であると簡単にわかる保証はない**
  - そもそも問題に気付けず、外部からの指摘で重大事案が発覚することも多い
- **事前にとることのできる対策がさまざまある**
  - 100%完璧な予防策というものはないが「完璧でない＝効果なし」ではない

内部不正の防止に取り組み、組織と従業員を守る

「組織における内部不正防止ガイドライン」

https://www.ipa.go.jp/security/guide/insider.html

- 組織の情報漏えいに関する内部不正対策に特化したガイドライン。2022年4月に**改訂第5版**発行。

【組織における内部不正防止ガイドライン】

1．背景
2．概要
3．用語の定義と関連する法律
4．内部不正を防ぐための管理のあり方
- 4-1　基本方針
- 4-2　資産管理
- 4-3　物理的管理
- 4-4　技術・運用管理
- 4-5　原因究明と証拠確保
- 4-6　人的管理
- 4-7　コンプライアンス
- 4-8　職場管理
- 4-9　事後対策
- 4-10　組織の管理

付録Ⅰ～Ⅷ（内部不正事例、チェックリスト等）

状況的犯罪予防の5原則
1．やりにくくする
2．やれば捕まる
3．わりにあわない
4．動機を減らす
5．いいわけさせない
をベースに整理

内部不正防止ガイドラインの構成
10の観点･33の対策項目

・対策項目各々のリスク、対策のポイントについて整理

番号	観点（分類）	対策項目	番号	観点（分類）	対策項目
1	基本方針	（１）経営者の責任の明確化 （２）総括責任者の任命と組織横断的な体制構築	6	人的管理	（２０）教育による内部不正対策の周知徹底 （２１）従業員モニタリングの目的等の就業規則での周知 （２２）派遣労働者による守秘義務の遵守 （２３）雇用終了の際の人事手続き （２４）雇用終了及び契約終了による情報資産等の返却
2	資産管理： 秘密指定とアクセス管理	（３）情報の格付け区分 （４）格付け区分の適用とラベル付け （５）情報システムにおける利用者のアクセス管理 （６）システム管理者の権限管理 （７）情報システムにおける利用者の識別と認証	7	コンプライアンス	（２５）法的手続きの整備 （２６）誓約書の要請
3	物理的管理	（８）物理的な保護と入退管理 （９）情報機器及び記録媒体の資産管理及び物理的な保護 （１０）情報機器及び記録媒体の持出管理 （１１）個人の情報機器及び記録媒体の業務利用及び持込の制限	8	職場環境	（２７）公平な人事評価の整備 （２８）適正な労働環境及びコミュニケーションの推進 （２９）職場環境におけるマネジメント
4	技術的管理	（１２）内部不正モニタリングシステムの適用 （１３）ネットワーク利用のための安全管理 （１４）重要情報の受渡し保護 （１５）情報機器や記録媒体の持ち出しの保護 （１６）組織外部での業務における重要情報の保護 （１７）業務委託時の確認 （第三者が提供するサービス利用時を含む）	9	事後対策	（３０）事後対策に求められる体制の整備 （３１）処罰等の検討及び再発防止
5	原因究明と証拠確保	（１８） 情報システムにおけるログ・証跡の記録と保存 （１９） システム管理者のログ・証跡の確認	10	組織の管理	（３２）内部不正に関する通報制度の整備 （３３）内部不正防止の観点を含んだ確認の実施

内部不正を生み出す３要因　不正のトライアングル*

・内部不正は「動機・プレッシャー」「機会」「正当化」の３要因が揃った時に発生

*ドナルド・R・クレッシー（米国の組織犯罪研究者）による

動機・プレッシャー

不正行為のきっかけ、原因：
処遇への不満やプレッシャー等（業務量、ノルマ等）

（具体例）

- **人事に不満**
- **金銭問題を抱えている**
- **高いノルマを課されている**

×

機会

不正行為の実行を可能・容易にする環境：
IT技術不備や物理的な環境、組織のルール不備等

（具体例）

- **掣肘のないシステム管理権限**
- **情報持ち出し可能な環境**
- **同じ業務を長期間担当**

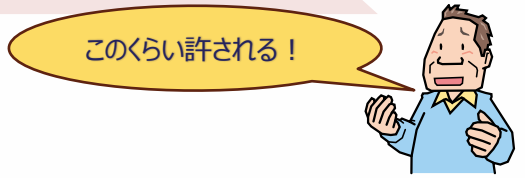
×

正当化

自分勝手な理由づけ、倫理観の欠如：
都合の良い解釈
他人への責任転嫁等

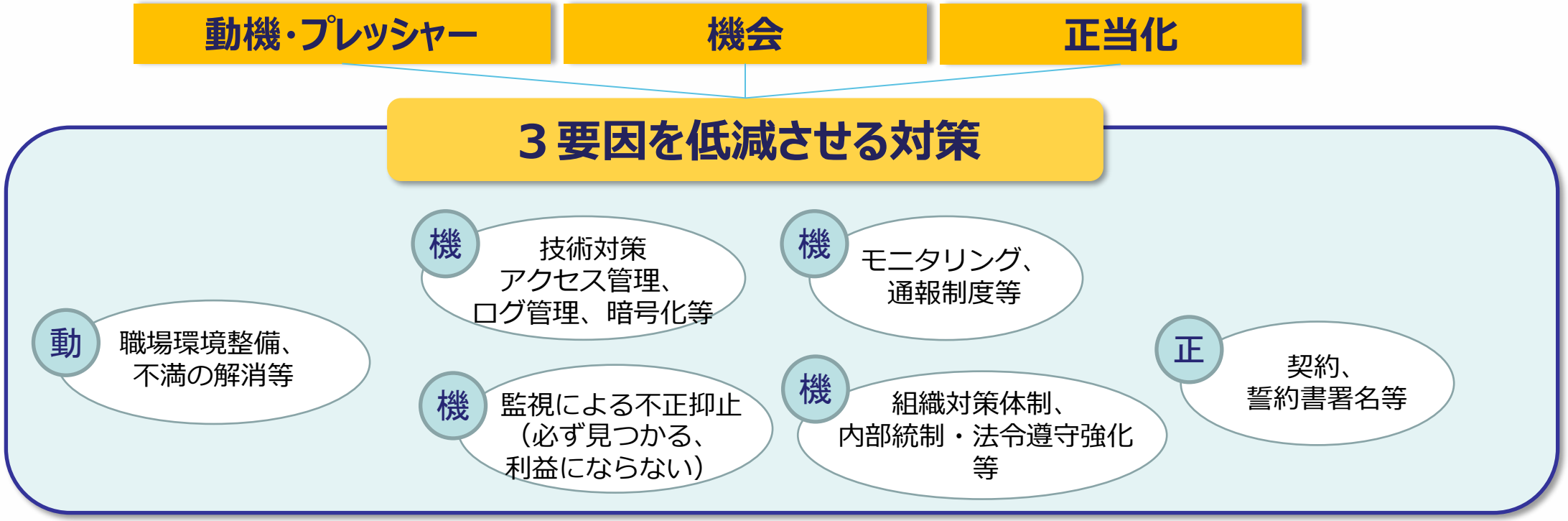
（具体例）

- **個人の評価と処遇のギャップ**
- **サービス残業の恒常化**
- **会社へのうらみ**

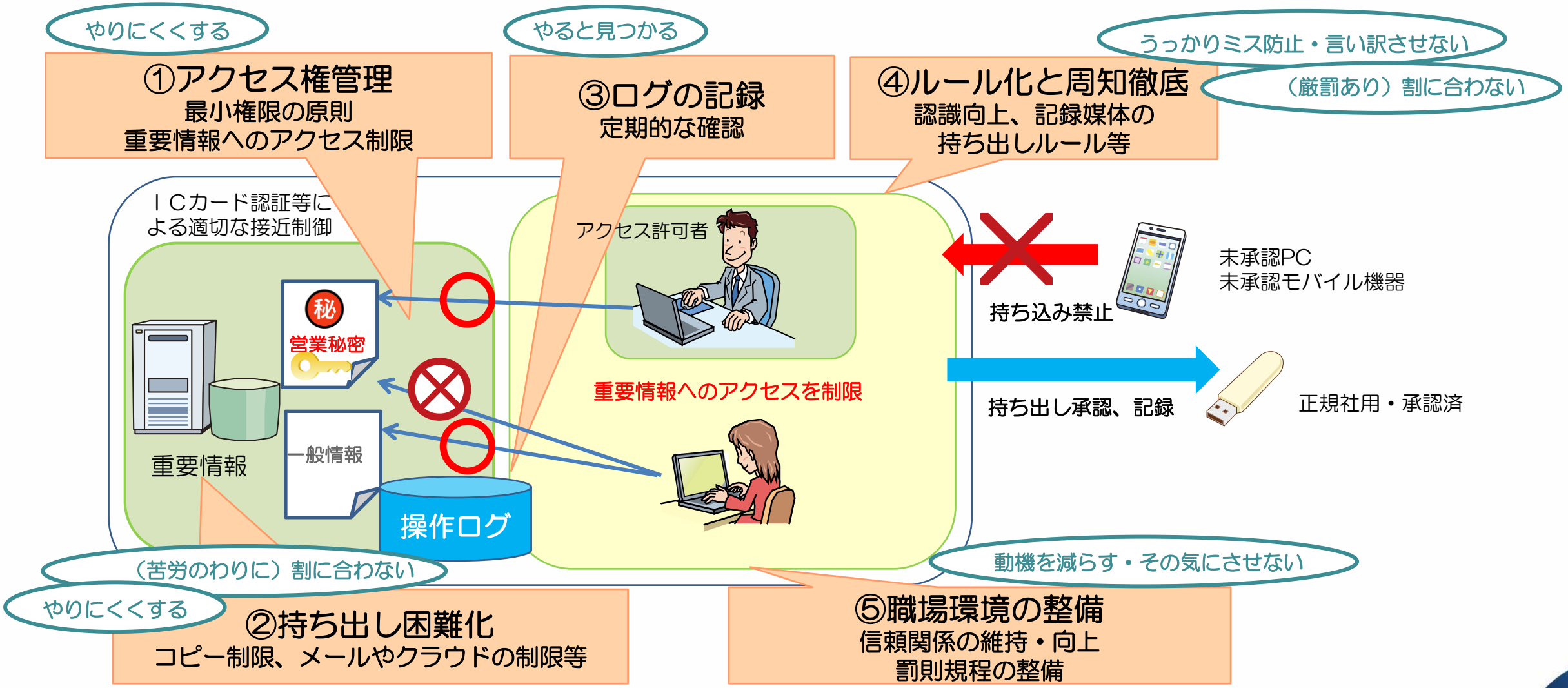


内部不正防止対策の要諦：３要因の低減

・組織における内部不正対策のポイントは
「動機・プレッシャー」と「機会」と「正当化」それぞれの要因の低減



内部不正防止のポイント　状況的犯罪予防論*を応用した基本原則



＊状況的犯罪予防論：犯罪学者のCornish&Clarke（2003）が提唱した、都市空間における犯罪予防の理論

内部不正防止のための基本施策：経営層が関与した管理体制整備

- 内部不正の対策が経営者の責任であることを組織内外に示す「基本方針（ポリシー）」を策定
- 経営者による意思決定を組織全体に周知徹底
- 組織横断的な実施状況が把握できる管理体制を企業の規模や実情に応じ構築

組織横断の取り組み

内部不正防止対策の10の観点（分類）と関連部門

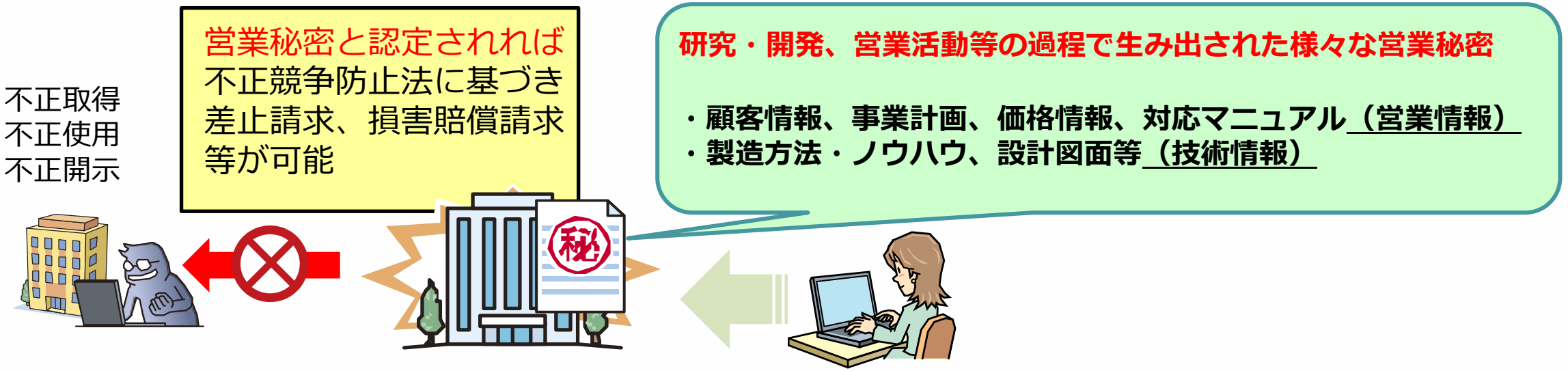
観点（分類）	経営者	情報システム部	総務部	人事部	法務・知財部	営業・開発等の各部門
1.基本方針	○					
2.資産管理		○				○
3.物理的管理		○	○			○
4.技術的管理		○				○
5.証拠確保		○				○
6.人的管理			○	○	○	○
7.コンプライアンス			○	○	○	○
8.職場環境			○	○		○
9.事後対策		○				○
10.組織の管理		○				○

内部不正防止のための基本施策：
重要情報の特定と格付け区分

重要情報の特定（明確化）

- 少なくとも**重要情報**と**一般情報**の２つに分けて管理（情報の格付け区分）
- **重要度ごとに取扱いルール**を定め、**定期的に見直す**（取扱範囲、廃却方法等）
- 従業員にわかるように「機密情報」等を**表示**（ラベル付け）

※営業秘密として**不正競争防止法**の法的保護を受けるためにも重要



組織における内部不正防止ガイドライン　付録

- 付録Ⅰ　内部不正事例集
  企業・組織にとっての「他山の石」用途
- 付録Ⅱ　内部不正簡易チェックシート
  対策導入支援用。対策の指針をまとめ、組織横断的な担当俯瞰も目指す
- 付録Ⅲ　Ｑ＆Ａ集
- 付録Ⅳ　他ガイドライン等との関係
  JIS Q 27001、営業秘密管理指針/秘密情報の保護ハンドブック、個人情報保護ガイドライン等
- 付録Ⅴ　基本方針の記述例
- 付録Ⅵ　内部不正防止の基本５原則と25分類
- 付録Ⅶ　対策の分類
  企業や組織の環境別対策、不正行為の種類別対策
- 付録Ⅷ　テレワークに係る対策一覧

「企業の内部不正防止体制に関する実態調査」から

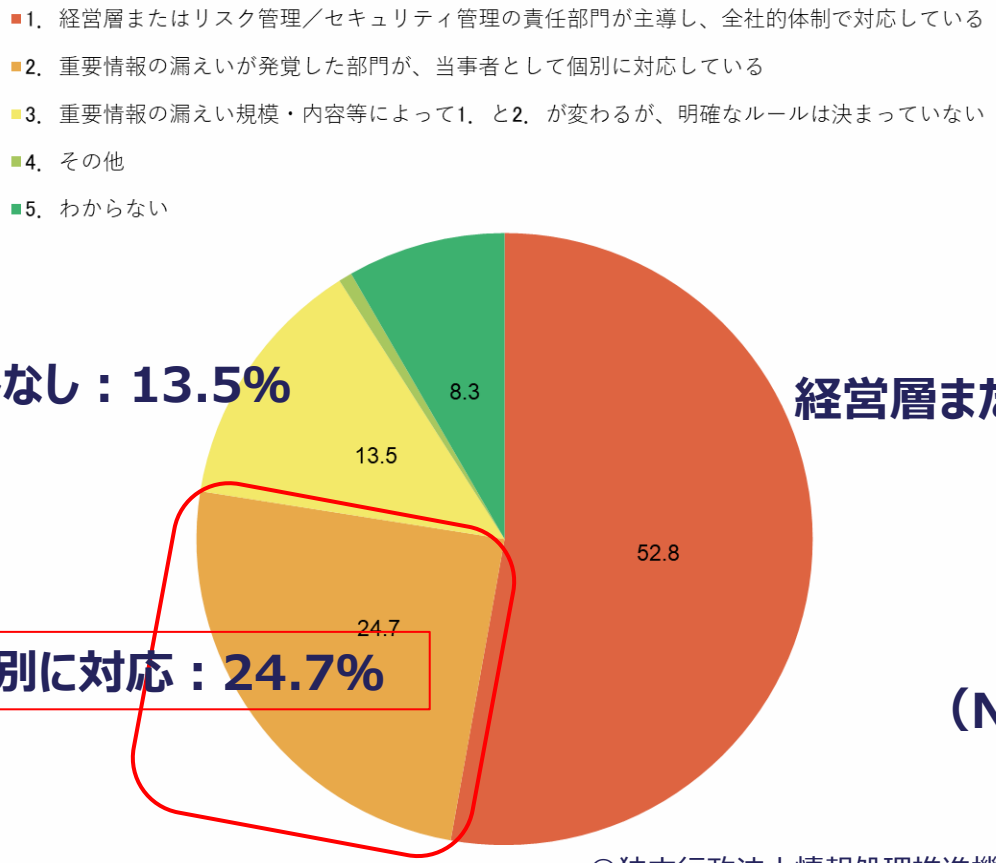
https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

IPA

IPA　2022年度実施

- **内部不正対策に取り組む組織的体制**
  →重要情報漏えい対応を全社体制で行える割合は半数
  現場組織の個別対応がかなり残っている状況

Q10.重要情報が漏えいした時の組織的対応



明確なルールなし：13.5%

経営層または統括責任部門が主導：52.8%

当事者部門が個別に対応：24.7%

（N=1,179）

「企業の内部不正防止体制に関する実態調査」から

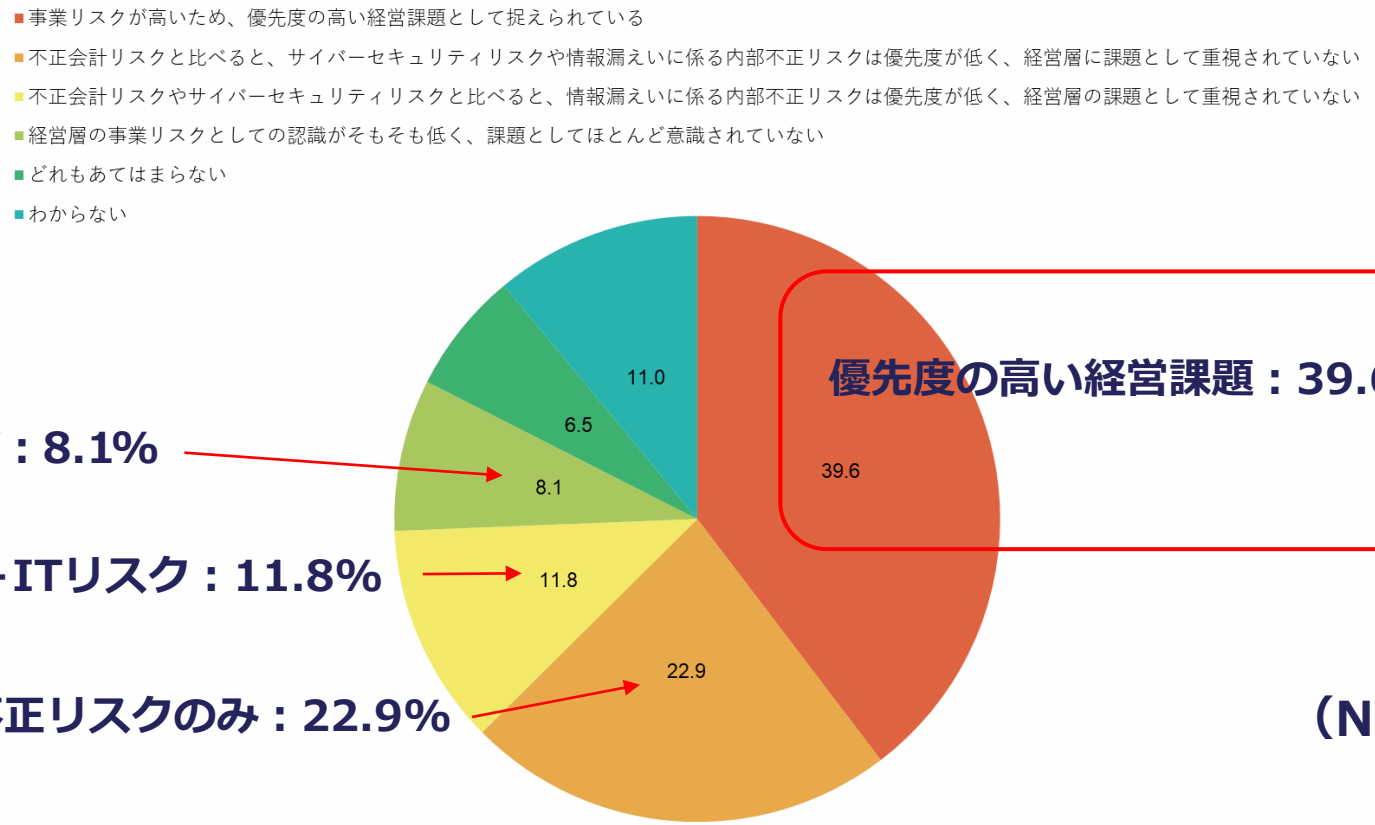
https://www.ipa.go.jp/security/reports/economics/ts-kanri/20230406.html

IPA　2022年度実施

- **内部不正対策に取り組む経営層の姿勢**

→経営層が内部不正リスクを優先度の高い経営課題とした率は約40%

Q30. 貴社では、内部不正リスクは重要な経営課題として捉えられていますか。



優先度の高い経営課題：39.6%

課題として認識せず：8.1%

一般的な不正リスク+ITリスク：11.8%

一般的な不正リスクのみ：22.9%

（N=1,179）

実施率が低い各内部不正対策（同実態調査）

実施率（%）	対策（選択肢の要約）　IPA　2022年度実施
27.7	異動時・昇進時・新プロジェクトへの参加・終了時などに秘密保持契約締結または誓約書提出を求める
22.9	営業や技術の重要人物の退職が決まった段階で、重要情報へのアクセス監視及びアクセスログ確認等を強化する
21.4	重要情報を含む電子文書は容易に判別できるようにする
21.3	重要情報は定期的に棚卸しを行い、不要なものを消去する
21.1	BYODは許可しない
19.8	ガイドライン等に従い会社支給PCのテレワーク対策を強化する
19.8	テレワークで扱える重要情報の範囲をルール化する
19.7	使用できるクラウドやクラウドで扱う重要情報をルール化する
18.4	委託先等との重要情報の受渡しを厳格に管理、暗号化する
17.6	委託先等の情報漏えい対策を契約時・契約中に確認する
15.9	組織内外で内部不正事故が起こった場合、組織内で共有する

抽出した課題から必要とされる教育・啓発の在り方

■ 内部不正防止に関する知識の取得・周知・教育のあり方

（1）情報漏えい、内部不正防止に関する社内のルール・規程等を学ぶ機会を増やすこと

（2）従業員に内部不正防止の知識を根付かせる。特に「してはいけないこと」を教育すること

（3）内部不正に関する動画等の教育コンテンツ、グループディスカッション、セルフチェック等、多様なツールや教育機会を活用した「知識を組織に根付かせる取り組み」

IPAチャネル（Youtube)で
内部不正対策動画を公開しています！

■ 内部不正防止に関する組織の体制のあり方

（1）内部不正防止に責任を負う組織の権限を実効的に確保し、全社的に対応すること

（2）組織の基本方針に基づいた内部不正対策を具体的に計画し、実施する責任・権限を明確にすること

（3）経営層の不正に対する対策の透明性を確保し、内部不正対策のマネジメントシステムを実効的に機能させること

■ 内部不正防止対策

（1）個人情報以外の重要情報も特定、管理を行うこと

（2）悪意の内部不正対策に対しては、低コストの従業員教育とあわせて各種技術的対策でカバーし、コストと効果を最適化すること

（3）中途退職者、中途採用者の内部不正に対応できる対策（アクセスログの活用、NDA等）

内部不正対策のまとめ

■ ガイドラインは網羅的なToBe。自分の企業・組織の優先課題は？

是非、トップダウンで体制・対策の整備を。内部不正対策も手薄な課題、優先すべき対策を見極め順次実施しましょう。

情報漏えいに関する内部不正対策でも、個人情報保護と営業秘密保護では意識に差が生じがち。

基本対策筆頭の「重要情報の特定・格付け管理」でも、永く継続する課題となってしまうこともあります。

■ 内部不正対策は毅然としつつ従業員への配慮を

アクセスログ管理の徹底ひとつでも、従業員への働きかけとして二つの側面を持ちます。

▶北風：悪いことをすると必ずばれる、という抑止力を期待（毅然として）

▶太陽：善意の従業員の皆さんを守るために対策するのだ、という説明（あたたかく）

■ 経営層の対策も分け隔てなく

近年、経営層の中途退職による内部不正事例も目立ちますので抜かりなく。

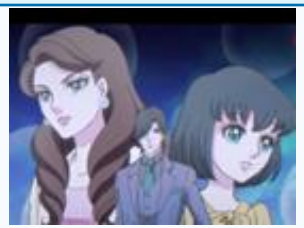
【ご参考1】IPAが提供する サイバーセキュリティ関連の 主なツール、施策等

映像で知る情報セキュリティ

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

- 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**33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
- **社内研修等**営利を目的としない用途に限り、主な映像の**動画ファイルを無償で提供**（ダウンロード）

● 主な映像コンテンツ

	**今、そこにある脅威～内部不正による情報流出のリスク～** 社員による内部不正で機密情報が外部に流出する危機が発覚。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、不正を起こさせないポイントの他、自社における経営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
	**今、そこにある脅威～組織を狙うランサムウェア攻撃～** 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、データを一斉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。	約15分
	**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、組織の従業員が日常行うべき8つの対策をご紹介しています。	8話構成 各話2分
	**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。	約10分

情報セキュリティ安心相談窓口

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

IPA

- 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。
- 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実施。

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

ECサイトを運営する中小企業の皆様へ

ECサイト構築・運用セキュリティガイドライン

https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

IPA

- 近年、ECサイトからの**個人情報及びクレジットカード情報の流出事件**が多数発生。被害の大半が**中小企業の自社構築サイト**
- ECサイトの構築・運用に**必要なセキュリティ対策とその実践方法**をまとめて解説するガイドライン

- 「**第1部　経営者編**」と「**第2部　実践編**」で構成
- 「第1部　経営者編」
  - ECサイトを**新規構築、あるいは既に運営している経営者向け**に、自社のECサイトにおけるセキュリティ**対策の必要性**を説明
- 「第2部　実践編」
  - 対策実践の責任者、担当者が、ECサイトの構築時・運用時に**優先する対策**や、自社のECサイトの状況に**見合った対策の範囲や実現方法**を適切に決めていただくための内容

制御システムのリスク分析・普及

■ **制御システムについて、リスク分析を起点としたセキュリティ対策の普及促進を目的に、以下を実践**

① 各種事業者でのリスク分析の実施
② リスク分析で得られた知見に基づく「業界ガイド」や「リスク分析ガイド」の作成・改訂
③ 作成したガイドに沿ったリスク分析セミナーを実施し、リスク分析の取組の普及促進

※「重要インフラの情報セキュリティに係る行動計画（重要インフラ行動計画）」の「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」（サイバーセキュリティ本部決定文書）では、情報セキュリティリスクアセスメントの実施が推奨されている。

・セミナー・講演によるリスク分析の普及
・業界動向等の調査
・対策技術等の調査

【リスク分析実施分野】
スマートメーター、ガス、水道、医療、化学、石油、鉄道、自治体(焼却炉）、新電力(火力）、物流、スマート工場等

受講生からリスク分析上の課題・要望等をアンケートやヒアリングで収集、事業計画に反映

・業界ガイド作成
・リスク分析ガイド改訂
・セミナーコンテンツ拡充
・各種対策事例の紹介

制御システムを利用する事業者のセキュリティリスク分析への理解が深まり、制御システムのリスク分析に取り組む組織が増加することで、各事業者におけるセキュリティレベルの飛躍的な向上と継続的な維持見直しが達成されることを狙う。

【ご参考2】IPAにおける DXの促進事業

DXの促進事業　1/3

国内外のDX戦略・技術・人材の動向や、新たな技術の社会実装に向けた 課題と解決策などの調査・分析を行い、企業のDX推進やSociety5.0の実現に向けた社会基盤の構築に貢献しています。

DX白書

DXに関する国内外の最新動向を調査・分析して「白書」として公表しています

https://www.ipa.go.jp/publish/wp-dx/dx-2021.html

DXポータルサイト

用語集や企業へのインタビュー記事を掲載した「DXポータルサイト」を公開しています。

https://dx.ipa.go.jp/

DXの促進事業　2/3

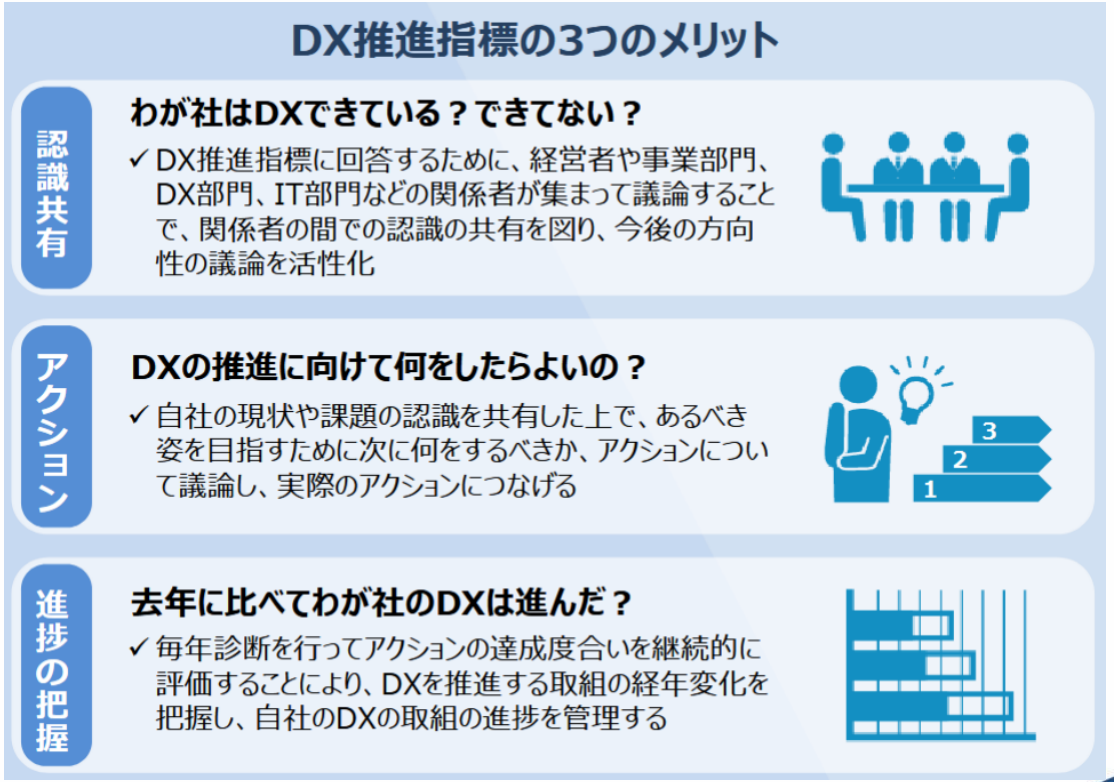
DX認定制度

DX推進の準備が整っていると認められた企業を国が認定する制度。IPAは本制度の事務局として、DX認定の審査事務など担当

https://www.meti.go.jp/policy/it_policy/investment/dx-nintei/dx-nintei.html
https://www.ipa.go.jp/digital/dx-nintei/

DX推進指標

DXに関する35問からなる自己診断と、他社比較ができる「ベンチマーク」を活用して、DXに関する自社の課題や、次に実施すべきアクションが検討できる指標



https://www.ipa.go.jp/digital/dx-suishin/

DX促進事業　3/3

地域DX推進ラボ／地方版IoT推進ラボ

地域の課題解決や新たな価値創造に向けて、地域のDXプロジェクトを創出する取組みを行っています。

地域DX推進ラボ

DX Acceleration Local Lab

各地域のDX実現に向けた取組を加速させるため、DXによる地域の経済発展とウェルビーイングの向上を目指す取組を選定し支援

地方版 IoT 推進ラボ

IoT Acceleration Local Lab

地域における新たな価値創造に向けて、IoTプロジェクトを創出する取組を選定し支援

＜地域DX推進ラボ／地方版IoT推進ラボのポータルサイト＞

https://local-iot-lab.ipa.go.jp/　（2023年6月20日時点）

まとめ

まとめ

まず大前提として
- **デジタルの活用**は、これからのビジネスにおいて**必須**。サイバー空間は**新たなビジネス領域**
- DXの推進によって**企業のさらなる成長**を！

- 仕事をデジタル化したら、**防犯もデジタル化**
- 仕事が便利になったぶん、**犯罪者にも便利**
- “実物を扱わない、時間や距離の制約がなくなる” ⇒ **いままで以上の防犯**が必要

- まずは、 **基本的**な対策から。組織の実態、必要性に合わせ**段階的**に
- 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**
- 外側だけではなく**内側にも目配り**を
- **万が一**に備えた**準備**を

DX、サイバーセキュリティの推進においては、
IPAのツール、制度をご活用ください！