

# 情報セキュリティ10大脅威2025（組織編） から学ぶ脅威と対策

2025年11月27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 普及啓発・振興部

エキスパート 金山 栄一 CISSP

## ■ 金山栄一（かなやま えいいち）

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  
普及啓発・振興部 エキスパート

IPA「企業組織向けサイバーセキュリティ相談窓口」と「情報セキュリティ安心相談窓口」での相談対応のほか、情報セキュリティ対策全般の普及啓発活動に従事。

### 略歴

防衛省サイバー防衛隊、陸上自衛隊サイバー防護隊、陸上自衛隊通信学校サイバー防護課程主任教官等、自衛隊の通信・IT・サイバー部隊に37年間勤務し、2021年8月定年退官  
2021年9月IPA入構、現職務

CISSP、情報処理安全確保支援士（登録番号5476）  
予備自衛官（一等陸尉）



P 5

情報セキュリティ10大脅威とは

P 9

脅威の紹介

P 31

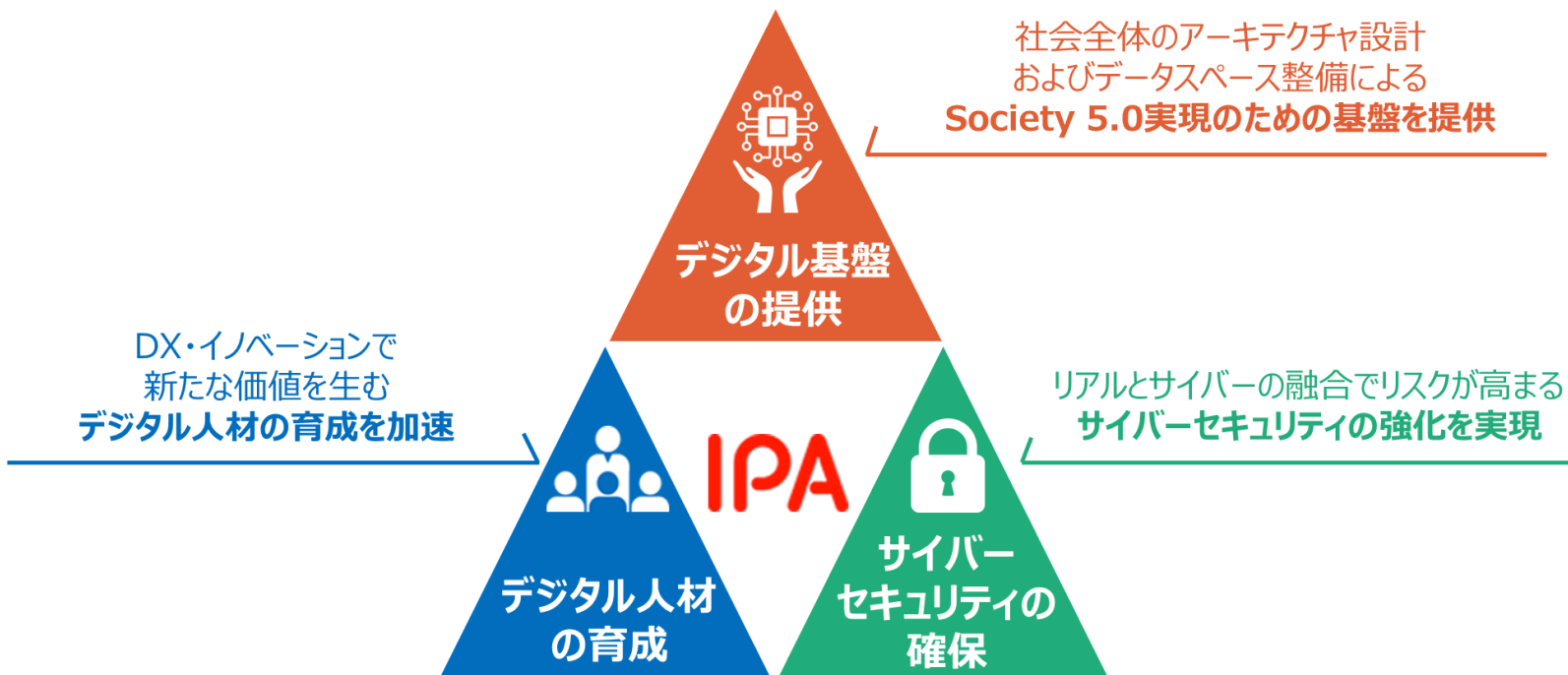
共通対策とは

P 40

参考情報・資料紹介

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



# サイバーセキュリティに関する業務概要

■ 平時からインシデント発生時まで、サイバーセキュリティのマネジメントからオペレーションまでトータルな施策・対応を実施。

## リテラシー向上

- ・ 情報セキュリティ10大脅威、情報セキュリティ白書
- ・ 経営者向け、社内セキュリティ担当者向けの各種ガイドライン
- ・ 従業員教育コンテンツ（動画教材など）
- ・ 地域・中小企業支援
- ・ 情報セキュリティ安心相談窓口

12,525件（2024年度）

累計宣言数  
約40万者  
（2025年4月）



## オペレーション（検知・分析・対応調整）

- ・ 情報共有枠組（サイバー攻撃情報・脆弱性）
- ・ 国家支援型サイバー攻撃対策
- ・ サイバー事故原因究明
- ・ サイバー情勢分析
- ・ セキュリティ監視（独法等）



脆弱性データベース

約23万件登録（2025年3月）



2011年創立 341件支援（2023年）

## セキュリティ基準・評価認証

### <製品・サービスのセキュリティ評価・認証>

- ・ IoT製品セキュリティラベリング（JC-STAR）
- ・ クラウドサービスセキュリティ評価（ISMAP）



### <セキュリティ基準・分析・監査等>

- ・ 制御システムセキュリティリスク分析
- ・ サプライチェーンセキュリティ評価
- ・ 独法等情報セキュリティ監査、政府システム監査



## 人材育成

- ・ 中核人材育成プログラム
- ・ 若手人材発掘（セキュリティ・キャンプ）
- ・ 国家資格「情報処理安全確保支援士」

累計435名受講（2017年～）

累計1,073名受講（2004年度～）

登録者数23,751名（2025年4月1日時点）

- ・ 情報セキュリティコンクール

応募約5万点（2023年度）



# 1. 情報セキュリティ10大脅威とは

---

# 「情報セキュリティ10大脅威」とは？

- IPAが2006年から毎年発行している情報セキュリティについての啓発資料
- 前年に発生したセキュリティ事故やサイバー攻撃の状況等から  
**IPAが10大脅威の候補になる脅威を選出**
- セキュリティの専門家や企業のシステム担当者等から構成される  
**「10大脅威選考会」が脅威の候補に投票**
- **TOP10入りした脅威を「10大脅威」として**  
脅威の概要、脅威の手口、被害事例、対策方法等を解説



様々な脅威が存在する



情報を扱う立場によって注意すべき脅威も異なる



➤ 家庭等でパソコンやスマホを利用する人

**「個人編」**



➤ 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

**「組織編」**

**「個人」と「組織」の2つの立場から脅威を解説**



# 情報セキュリティ10大脅威（組織編）の動向

- **ランサムウェア攻撃、サプライチェーンや委託先を狙った攻撃**が昨年に引き続き上位。標的型攻撃も5位と依然として大きな脅威。**内部不正**の4位にも着目。
- **個々の企業の脆弱性を突いた攻撃**だけでなく、**サプライチェーンや委託先を狙った攻撃**からの脅威が高まっている傾向。

順位	2023	2024	2025
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	ランサム攻撃による被害
2	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	サプライチェーンや委託先を狙った攻撃
3	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	システムの脆弱性を突いた攻撃
4	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	内部不正による情報漏えい等
5	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）	機密情報等を狙った標的型攻撃
6	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	リモートワーク等の環境や仕組みを狙った攻撃
7	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	地政学的リスクに起因するサイバー攻撃
8	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	分散型サービス妨害攻撃（DDoS 攻撃）
9	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	ビジネスメール詐欺
10	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）	不注意による情報漏えい等

前回5位と7位を統合

結果（被害）  
相互の関連も...

サイバー攻撃の  
手段（対象）  
・サプライチェーン  
・システムの脆弱性  
・VPN/リモートアクセス  
...

## 2. 脅威の紹介

---

- ◆ ランサム攻撃による被害
- ◆ サプライチェーンや委託先を狙った攻撃
- ◆ 内部不正による情報漏えい等

# 1位 ランサム攻撃による被害例

## ● 大規模な業務停止に至った事例

### KADOKAWAグループ（2024年6月）

- フィッシング攻撃等により従業員のアカウント情報が窃取され、社内ネットワークに侵入されたことが原因と推測
- 複数のサービスが停止したほか、約25万4,000人分の個人情報や企業情報の漏えいが判明
- 攻撃組織が公開したとされる情報が、SNS 等を通じて拡散

## ● データ暗号化による金銭要求を受けた事例

### ソフトウェア開発/支援会社（2024年6月）

- 資本金9,000万円の会社
- 攻撃者はサーバーの脆弱性およびVPN ルーターの設定不備を悪用して同社内ネットワークに侵入、複数のサーバーに対してデータの暗号化を行い、同社に対して金銭を要求。調査により、サーバのイベントログの消失、バックドア設置の痕跡も確認されている。
  - 個人情報を含む情報漏えいの可能性があったが、同年8月時点では外部への流出や二次被害は確認されていないとのこと。

# 1位 ランサム攻撃による被害例（進行中の事案）



アサヒGHD システム障害 復旧めど立たず 一部出荷手作業で対応

2025年10月1日午後6時08分

シェアする

<https://news.web.nhk/newsweb/na/na-k10014938171000>

## ● 被害の概要（同社ホームページの公表情報より）

- 国内グループ各社のシステムを利用した受注・出荷業務の停止
- お客様相談室などのコールセンター業務の停止
- システム障害は日本国内に限定
- 10月に予定されていた新商品発売延期
- アサヒ飲料工場フェスタ（イベント）中止
- 流出した情報をインターネット上で確認 → 本資料作成時：詳細調査中

## ● タイムライン

- 9月29日7時頃 システム障害の発生を確認
- 9月29日昼頃 警察へ被害相談
- 9月29日 サイバー攻撃によるシステム障害発生について（第1報）
- 10月3日 サイバー攻撃によるシステム障害発生について（第2報）  
ランサムウェアによる攻撃を受けたことを公表
- 10月7日 ランサム攻撃グループQilinが犯行声明
- 10月8日 サイバー攻撃によるシステム障害発生について（第3報）  
情報漏えいを確認、製造・出荷の一部再開
- 10月14日 サイバー攻撃によるシステム障害発生について（第4報）  
個人情報流出の可能性と調査中であることを公表

（本資料作成時ここまで）



# 1位 ランサム攻撃による被害例（進行中の事案）



## アスクル ランサムウェア被害 受注や出荷停止 復旧めど立たず

2025年10月19日午後8時58分

シェアする

<https://news.web.nhk/newsweb/na/na-k10014953501000>

### ● 被害の概要（同社ホームページの公表情報より）

- ASKUL、ソロエルアリーナ、LOHACOの受注・出荷業務の停止
- ASKUL LOGISTが受託する物流業務の停止
- ECのお客様からのお問い合わせに関する一部の情報が流出

### ● タイムライン

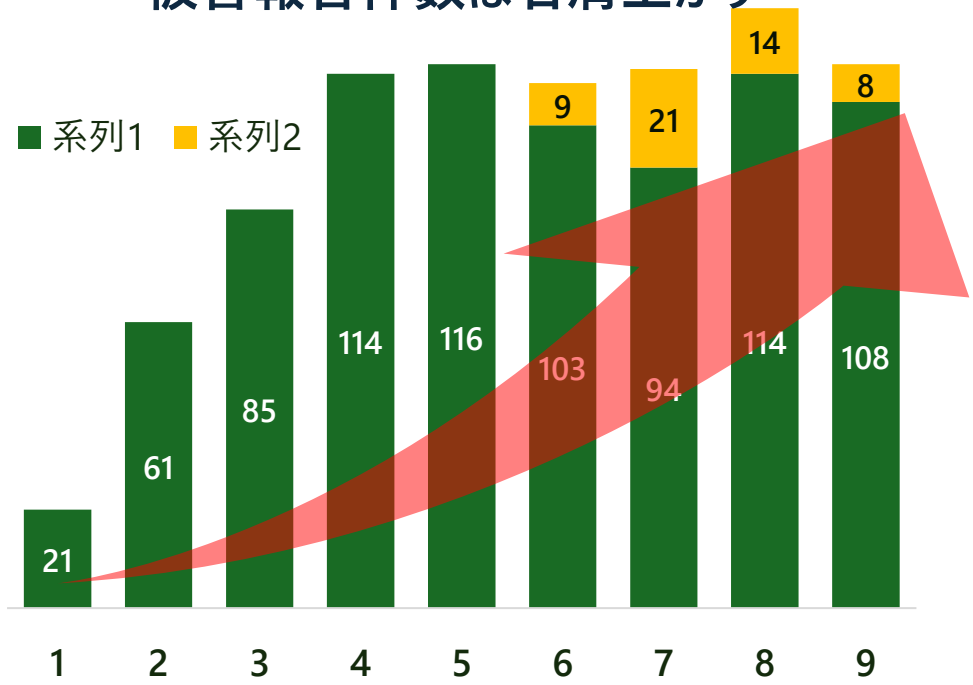
- 10月19日 ランサムウェア感染によるシステム障害について（第1報）
- 10月22日 ランサムウェア感染によるシステム障害について（第2報）  
物流システム障害、LINEやフーの協力体制
- 10月29日 ランサムウェア感染によるシステム障害について（第3報）
- 10月30日 ランサム攻撃グループRansomHouseが犯行声明
- 10月31日 ランサムウェア感染によるシステム障害について（第4報）  
ハッカー集団の犯行声明の事実関係の確認中
- 10月31日 ランサムウェア感染によるシステム障害について（第5報）  
流出を確認した情報、注意喚起
- 11月6日 ランサムウェア感染によるシステム障害について（第6報）  
サービスの段階的復旧計画
- 11月11日 ランサムウェア感染によるシステム障害について（第7報）  
流出した情報の件数が拡大したことを確認、Web再開

（本資料作成時ここまで）

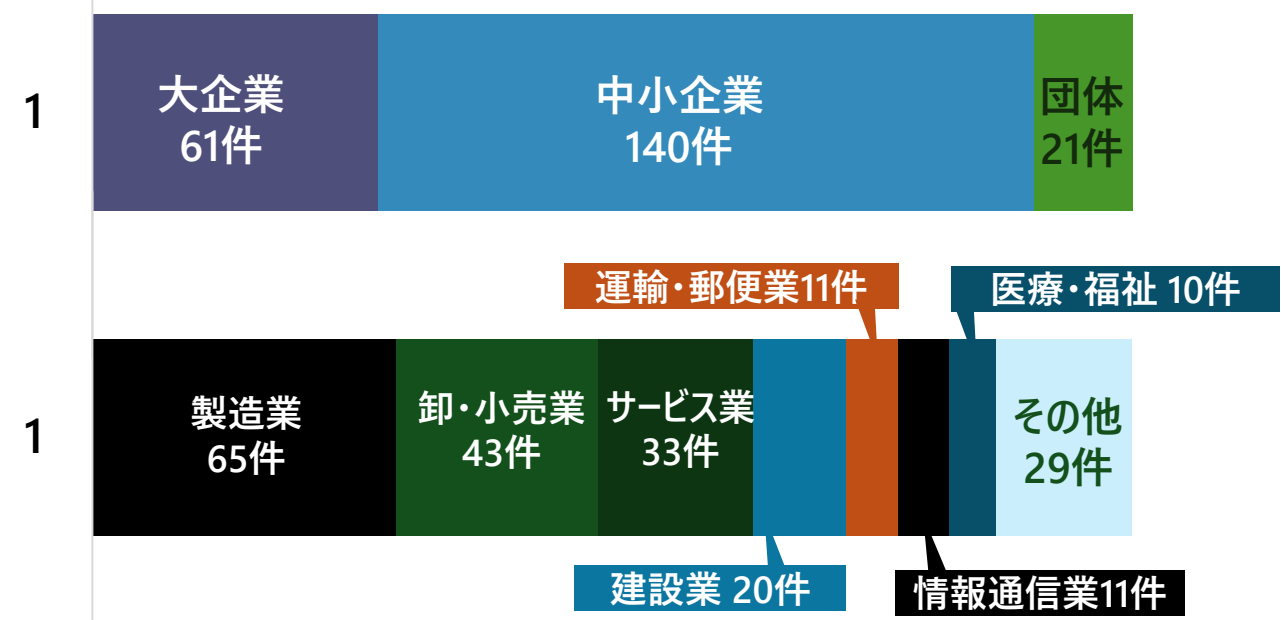
ランサムウェア被害は右肩上がり、その6割以上が中小企業  
企業規模・業種を問わずサイバー攻撃は進化・拡大

◆ 発注元・取引先企業等**サプライチェーン全体への波及被害や攻撃の足掛かり**となる懸念も

企業・団体等におけるランサムウェアの被害報告件数は右肩上がり



企業・団体のランサムウェア被害報告の222件：規模・業種は多種多様

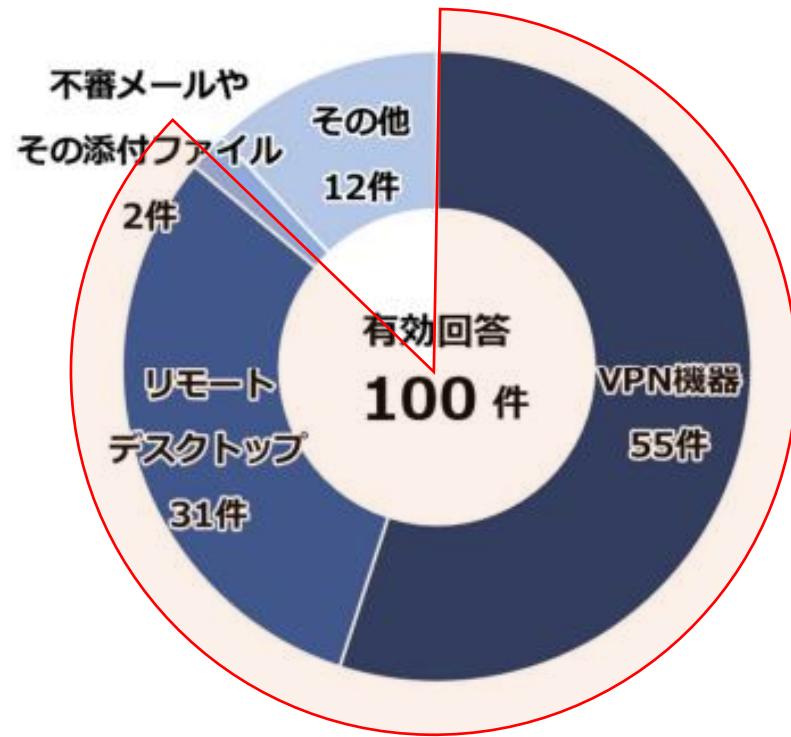


出典 「令和 6 年におけるサイバー空間をめぐる脅威の情勢等について（警察庁）」をもとにIPAが作成  
[https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06\\_cyber\\_jousei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf)

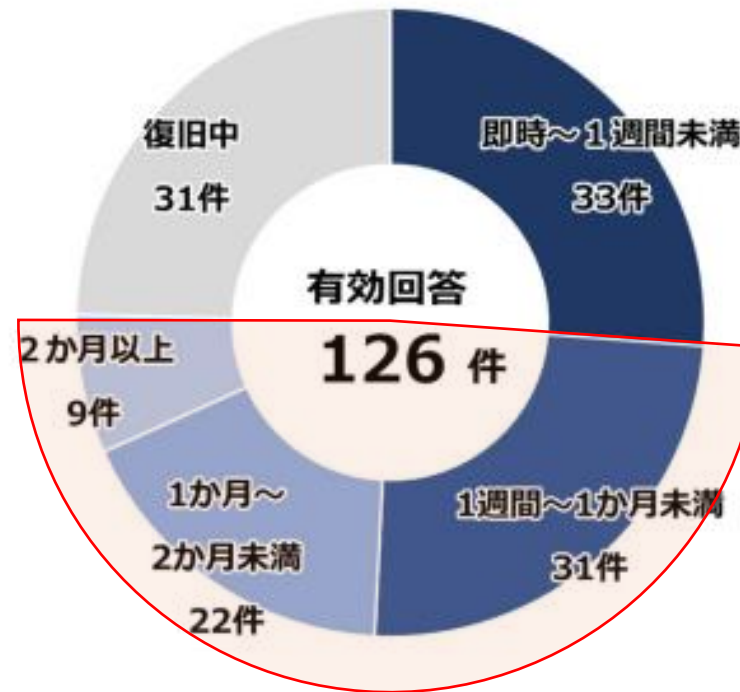
# 警察庁のレポートに見られるランサムウェア攻撃の状況 ランサムウェアに感染してしまった場合の影響は甚大

- **VPN機器、リモートデスクトップからの侵入が8割強**
- 復旧に要した期間**1週間以上が約半数**
- **6割強**が調査・復旧に**500万円以上**を要していた。

感染経路



復旧に要した期間



調査・復旧費用の総額



令和6年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/R6/R06\\_cyber\\_jousei.pdf](https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf)

- 攻撃者は、**身代金が支払われるまで**何重にも脅迫する。
- ランサムウェアを用いずに脅迫をする攻撃 (**No Where Ransom**)が流行っている。

		攻撃内容	身代金を支払わせる際の脅迫内容
<u>従来型</u> <u>二重脅迫</u> <u>三重脅迫</u> <u>四重脅迫</u>	{ { { {	データ暗号化	データを復元したければ・・・
		機密情報の窃取	機密情報を公開されたくなければ・・・
		DDoS攻撃準備	DDoS攻撃をされたくなければ・・・
		取引先情報の窃取	情報漏えいを取引先に知られたくなければ・・・



## 2位 サプライチェーンや委託先を狙った攻撃

### ● サプライチェーン攻撃とは？

サプライチェーンの中で**セキュリティ対策が甘いところを狙った攻撃**

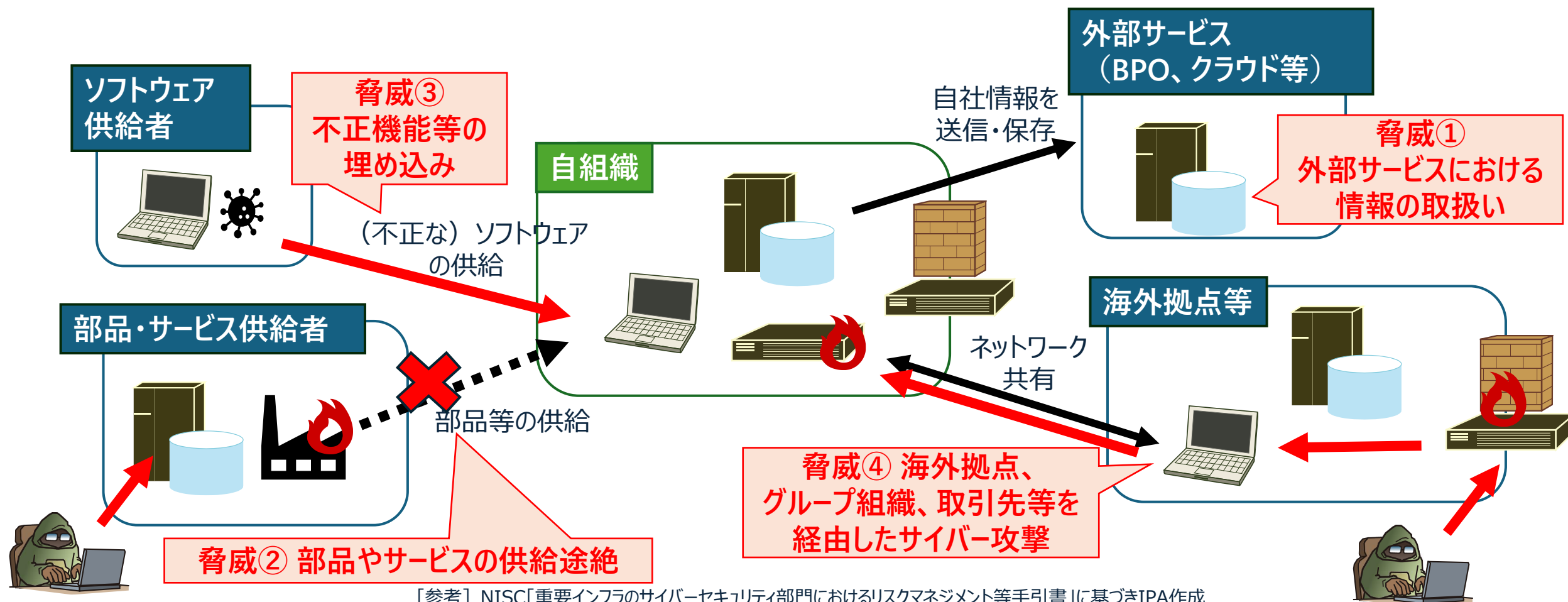


### ● 2種類のサプライチェーン

- ・ 調達、製造、在庫管理、物流、販売、業務委託先等の一連の商流
  - ・ 取引先、委託先、グループ企業
  - ・ 利用している外部サービス
- ・ ソフトウェア開発のライフサイクルに関わるサプライチェーン(**ソフトウェアサプライチェーン**)

# サプライチェーンに係る脅威の全体像

- サプライチェーンに係る脅威は、「不正機能等の埋め込み」「部品・サービスの提供途絶」「機密情報の漏えい等」「取引先等を踏み台とした不正侵入」等、性質の異なる複数のリスクを包含している。それぞれに応じた対策が必要



[参考] NISC「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」に基づきIPA作成

## 2位 サプライチェーンや委託先を狙った攻撃

### ●業務委託先からの顧客情報の漏えい事例

#### ダイレクトメール代行会社（2024年5月）

- **VPN 経由の不正アクセス**を受け、同社の**端末やサーバー等がランサムウェア攻撃を受けた**事例。同年6月には、攻撃者が窃取したとされる情報のダウンロード用 URLが攻撃者グループのリークサイトに掲載された。
- 多数の自治体・民間企業が同社に印刷業務等を委託していた。このため、この攻撃によって業務委託元の組織から**情報漏えいに関するお知らせが多数公表**され、自治体だけでも約50万件以上の個人情報の漏えいが判明している。

#### 脅威①

**外部サービスにおける情報の取扱い**

### ●委託先への攻撃に起因するサービス停止事例

#### 物流代行・倉庫賃貸会社（2024年9月）

- 悪意ある第三者から**不正アクセス**を受け、サーバーがランサムウェアに感染した事例。これにより、**入出庫関連のシステムが停止し、生産・出荷業務の一部が一時停止**となった。また、この攻撃によって影響を受けた業務委託元の多数の組織からも、出荷の遅延や一時停止等が公表された。

#### 脅威②

**部品やサービスの供給途絶**

### ●ソフトウェアサプライチェーンの悪用事例

- 2024年3月、Linux 環境で広く利用されている「XZ Utils」というツールに悪意のあるコードが仕込まれたことが確認された。この悪意あるコードは共同開発者によって挿入されており、特定の条件下でリモートからシステム全体へ不正アクセスできるおそれがあった。

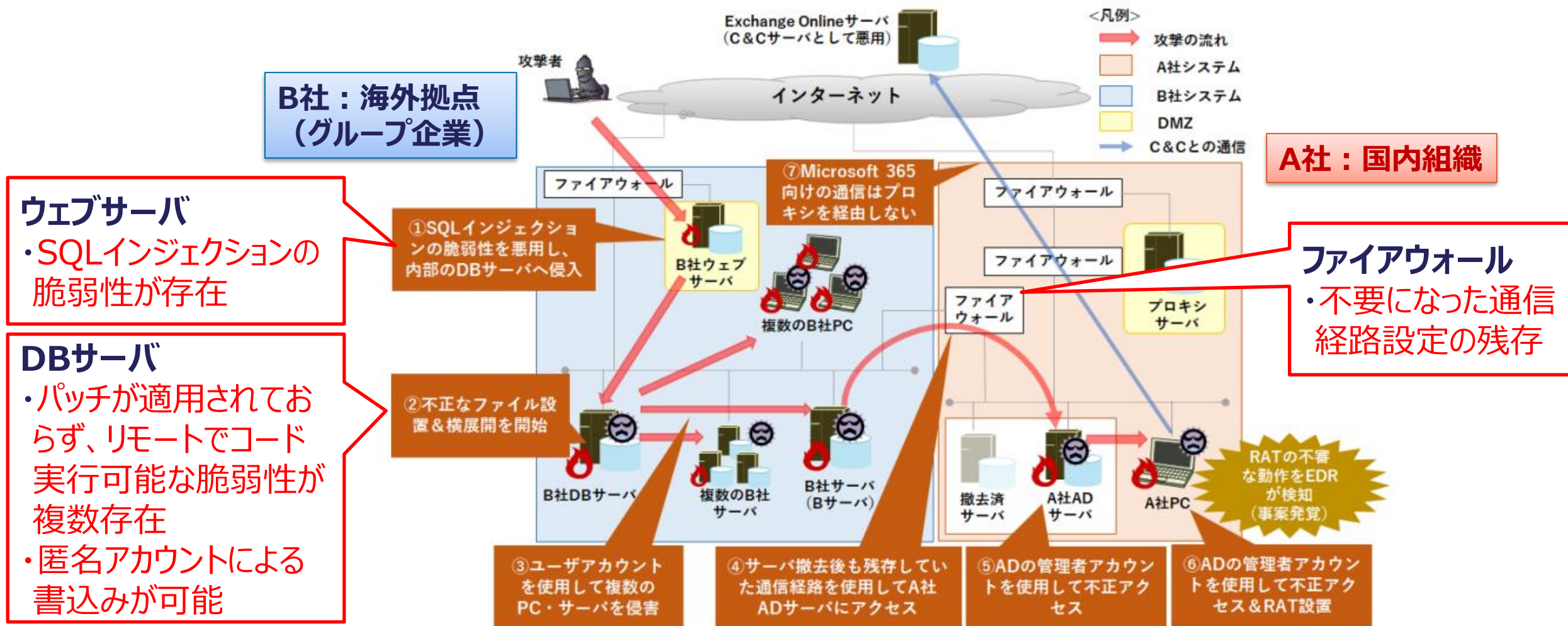
#### 脅威③

**不正機能等の埋め込み**



# 海外グループ企業を有する日系企業への標的型攻撃の事例

- 海外拠点が標的型攻撃を受け、侵入された後、国内組織まで横展開された。



出典：IPA「サイバー情報共有イニシアティブ（J-CSIP）運用状況[2023年1月～3月]」



## ● サプライチェーン攻撃を受けてしまう要因

- サプライチェーンを適切に選定、管理できていない  
→そもそも**セキュリティにおけるサプライチェーンリスクの認識が甘い**
- 再委託先や再々委託先の管理が困難  
→再委託先、再々委託先組織の管理は委託先組織が行うため、**委託元から再委託先などのセキュリティ対策管理は難しい**

## ● サプライチェーン攻撃を受けた後の対応が難しい要因

- 情報セキュリティに関する**責任範囲が不明確**  
→契約時に情報セキュリティに関する**責任範囲を明確に定めていない**場合、インシデント発生時の対応がスムーズにできない

## ● 被害の予防(サプライチェーン攻撃の被害を受けないための対策)

- 自組織における情報セキュリティ対策を実施する。  
→ISMS、Pマーク、SOC2、ISMAP等に**適合した運用**をする。また、運用を定期的に見直す。
- **セキュリティ面で信頼できる**委託先、取引先、サービスの選定  
→委託先、取引先における**情報管理等の規則を確認する**
- 契約内容を確認する
  - 情報セキュリティ上の**責任範囲の明確化**
  - インシデント発生時の対応や運用方法、補償内容
  - 委託先組織の**セキュリティ対策状況や情報管理の実態を定期的を確認できる契約**とする

環境の変化や情報セキュリティ情勢の変化等に対応できるよう、契約内容を見直す機会を持つ

## ● 被害の予防(サプライチェーン攻撃の被害を受けないための対策)

- 取引先や委託先との**連絡プロセスの確立**
- 委託先組織の管理  
→セキュリティ対策状況や情報管理の実態を確認する
- 納品物の検証を行う
  - **組み込まれているソフトウェアやOSSも把握**する
  - **OSSの脆弱性情報を収集**し、問題がないかを確認する。
- 公的機関が公開している資料の活用  
→サイバーセキュリティ経営ガイドラインと支援ツール(経済産業省)  
[https://www.meti.go.jp/policy/netsecurity/mng\\_guide.html](https://www.meti.go.jp/policy/netsecurity/mng_guide.html)

## ● 被害を受けた後の対応

- 関係各所への報告・連絡・相談
- 契約に基づいた**インシデント対応**
- 契約に基づいた被害への**補償対応**
- 影響調査、原因特定、および再発防止策の策定



## ● 内部不正とは？

- ・組織の従業員/元従業員による悪意ある不正行為
  - ・**個人情報**の窃取
  - ・**営業秘密等の不正取得・持出**
    - ・機密情報の**改ざん**
    - ・**ミスの隠蔽**のための情報削除

組織内の**情報管理の不備**による「ヒト」を通じた  
営業上の秘密情報・技術情報等の情報漏えい

## ● 内部不正による情報漏えい等の影響

- ・**社会的信用の失墜**
- ・損害賠償等による**経済的損失**

# 転職に関連する情報漏えい事案

## ◆ 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 → かつぱ寿司 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月かつぱ寿司顧問、2021年2月かつぱ寿司社長就任

<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](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/DGXZQOUE081G00Y3A001C2000000/>

- ◆ 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 ⇒ 漏えい情報の質・量ともインパクト大
  - 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かず、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**



# 内部不正を生み出す3要因『不正のトライアングル』

「組織における内部不正防止ガイドライン」より

- ・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

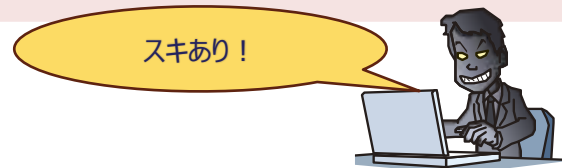


## 機会

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

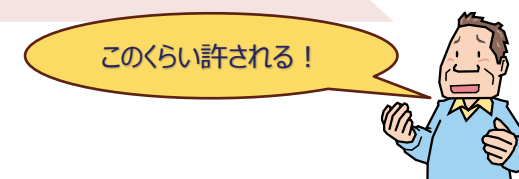


## 正当化

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）

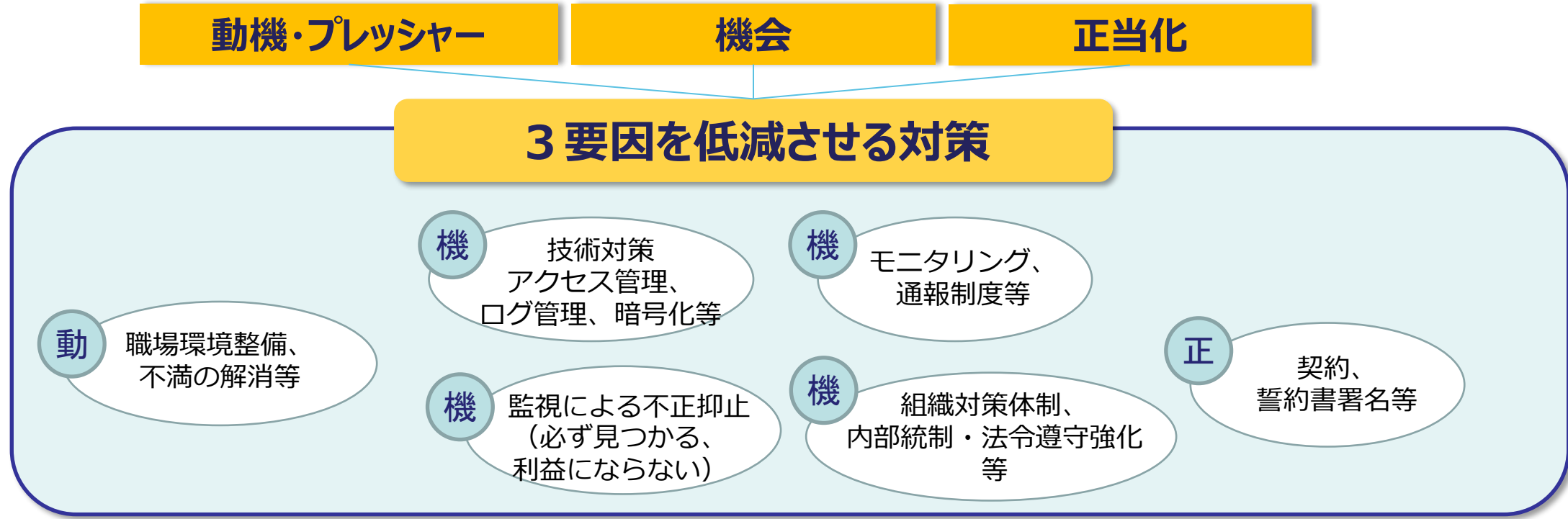
- ・ 個人の評価と処遇のギャップ
- ・ サービス残業の恒常化
- ・ 会社へのうらみ

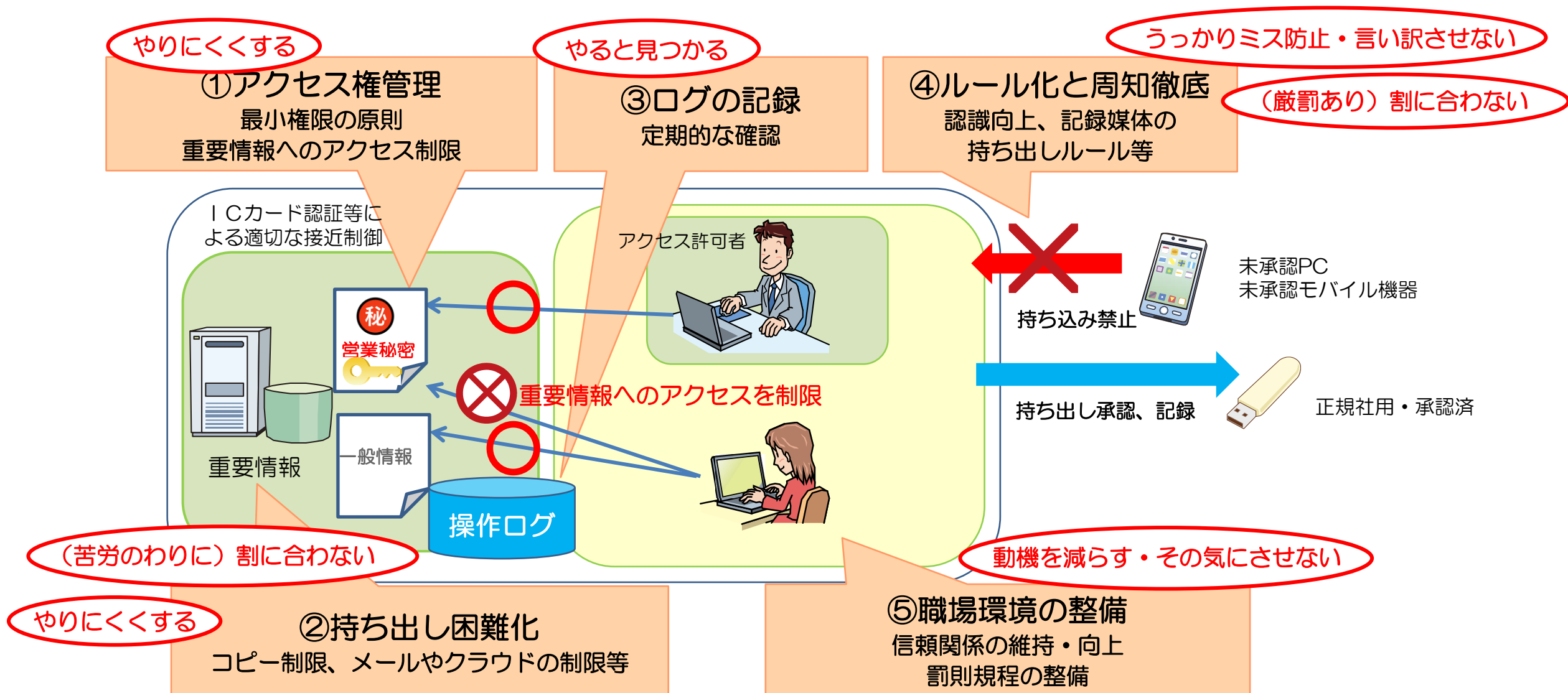


# 内部不正防止のための対策 3 要因の低減

「組織における内部不正防止ガイドライン」より

- ・ 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





\* 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

### 3. 共通対策とは

---



- 多数の脅威があるが「攻撃の手口」は似ている
- 基本的な対策方法は年月が経っても変わらない
- 下記の「情報セキュリティ対策の基本」は常に意識

攻撃の手口	情報セキュリティ対策の基本	目的
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
ソフトウェアの脆弱性の悪用	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
設定不備の悪用	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	手口から重要視すべき対策を理解する

# パスワードが第三者に突破されるとどうなるか

## ● 10大脅威の関連テーマ

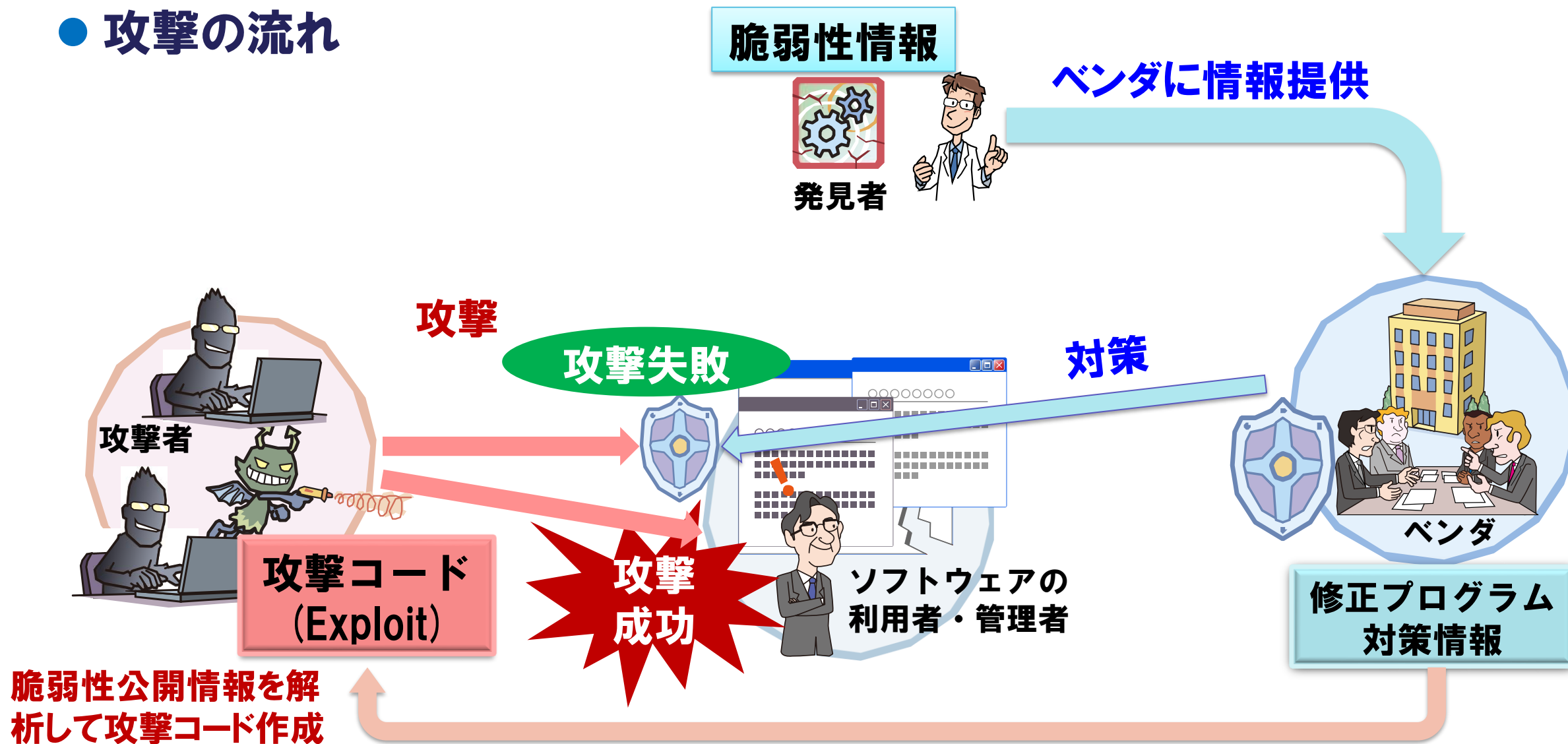
攻撃内容	10大脅威の関連テーマ
機密情報の窃取	クレジットカード情報の不正利用
	スマホ決済の不正利用
	フィッシングによる個人情報の搾取
	ビジネスメール詐欺
	メールやSMS等を使った詐欺・脅迫の手口による金銭要求
	機密情報等を狙った標的型攻撃
	地政学的リスクに起因するサイバー攻撃
システム情報の改ざん	ワンクリック請求等の不当請求による金銭被害
	偽警告によるインターネット詐欺
	不正アプリによるスマートフォン利用者への被害
ウイルス感染	ランサム攻撃による被害
その他	サプライチェーンや委託先を狙った攻撃
	インターネット上のサービスからの個人情報の窃取
	インターネット上のサービスへの不正ログイン

10大脅威では毎年20テーマを取り上げており、  
そのうち14テーマにおいてパスワード突破が原因。  
→**突破されにくいパスワードの設定が非常に重要**

- パスワードは推測や類推されず、偶然一致しないように設定
  - できるだけ**長く** → 偶然一致や総当たり（全組み合わせ試行）を困難に
  - **複雑**に（規則性のない文字列） → 推測をさける
  - **使い回さない** → 類推を避ける
- 2段階認証、多要素認証の使用・設定
  - 推奨されない多要素認証 → 電子メール・SMSによるOTPや認証コード
- 強い認証方式（パスキー等）の利用

# ソフトウェアの更新を怠るとどうなるか

## ● 攻撃の流れ





- ソフトウェアの脆弱性の解消には、ソフトウェアのアップデートが必要

- 修正プログラムがリリースされてから適用するまでの**期間が長期化**すると、脆弱性を悪用した**攻撃をされる可能性が非常に高くなる**。

- 修正プログラムを迅速に適用する

→ **利用しているソフトウェアの把握**と**継続的な情報収集**が必要

[参考]MyJVNバージョンチェッカ(IPA)

<https://jvndb.jvn.jp/apis/myjvn/vccheckdotnet.html>

- 自動更新機能を活用する(Windows等)



- ウイルス対策機能でウイルスの感染を未然に防ぐ
- ファイアウォール機能で不正な通信をブロックする

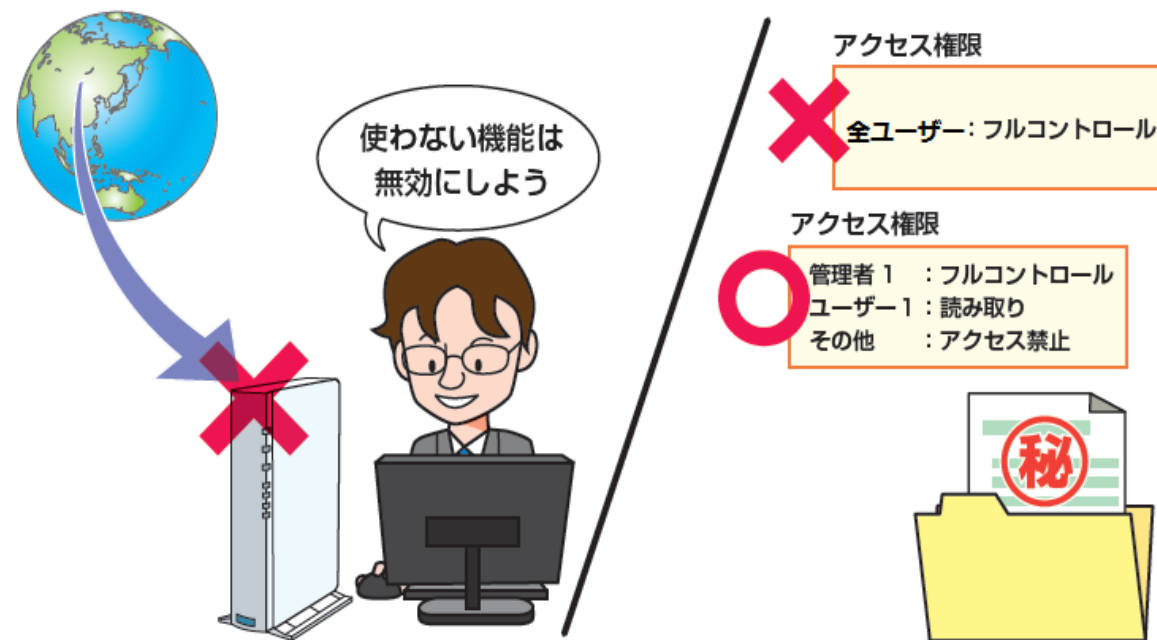
※通常のPC(Windows)であれば…

- 最低限、**Windows標準のセキュリティ機能は有効にする (Microsoft Defender)**
- その他**市販のセキュリティソフトの利用**も検討



- 利用する機器やソフトの仕様を理解して適切に運用する

- 初期パスワードからパスワードを変更する(IoT機器等)
- サーバーやクラウドサービスの**公開設定を確認**する  
→バージョンアップや仕様変更によって意図しない設定変更がされる場合があるため注意
- **アクセス制限**の設定を確認する
- **不要な機能は無効化**する

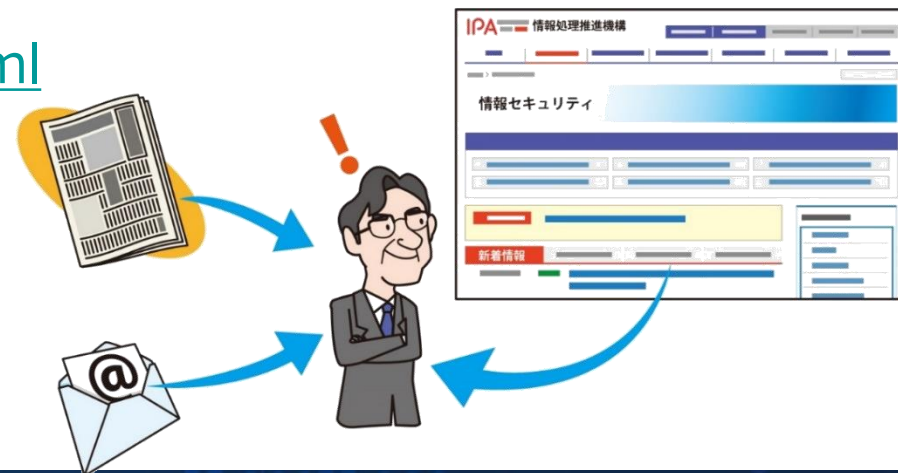


- 公的機関の注意喚起やニュース等から脅威の手口に関する情報を収集
- 変化する手口を理解して適切な対策を実践

- ソフトウェア開発ベンダや、注意喚起や情報発信を行っている公的機関の **SNSアカウントをフォロー** する
- 公的機関やニュースサイトの **メールマガジンを利用** する

→[参考] IPAメールニュース

<https://www.ipa.go.jp/mailnews.html>





### 3. 参考情報 / 資料紹介

---

# 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>

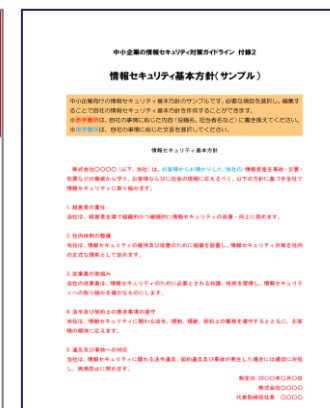
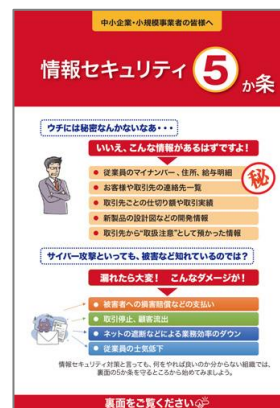


IPA

- ◆ 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

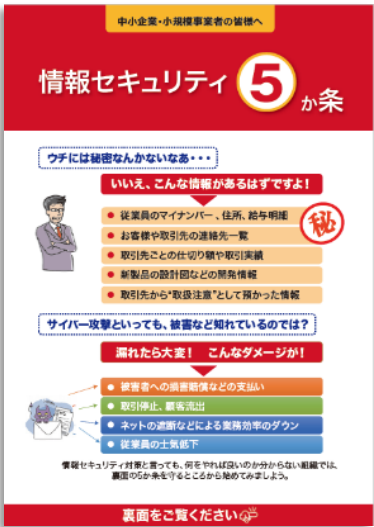


付録1：情報セキュリティ5か条(PDF)
付録2：情報セキュリティ基本方針（サンプル）(Word)
付録3：5分でできる！情報セキュリティ自社診断(PDF)
付録4：情報セキュリティハンドブック（ひな形）(PowerPoint)
付録5：情報セキュリティ関連規程（サンプル）(Word)
付録6：中小企業のためのクラウドサービス安全利用の手引き(PDF)
付録7：リスク分析シート（全7シート）(Excel)
付録8：中小企業のためのセキュリティインシデント対応手引き(PDF)



## ・ 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

セキュリティ対策自己宣言

Step2  
組織的な取り組みを開始する



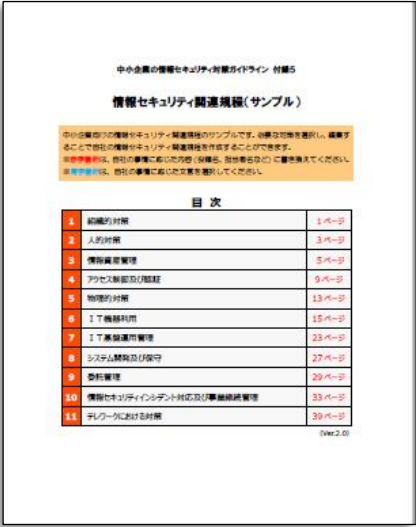
5分で行える！  
情報セキュリティ自社診断



SECURITY ACTION  
★★二つ星を宣言

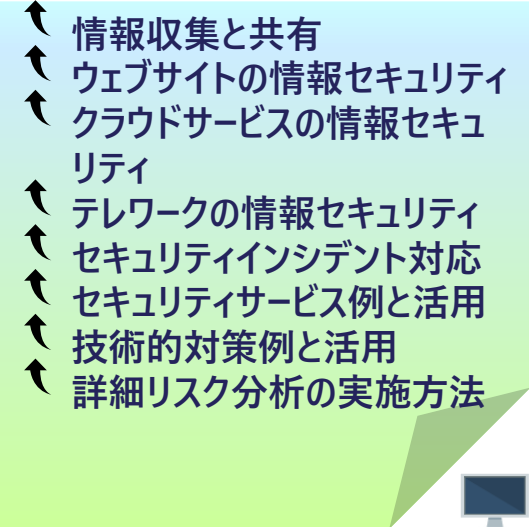
セキュリティ対策自己宣言

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



より強固にするため方策



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

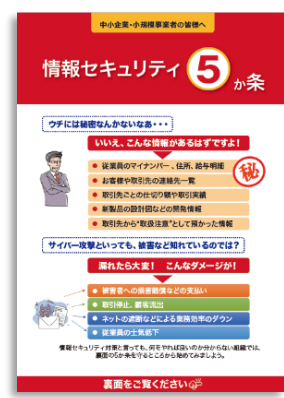
## ■ 中小企業自らが情報セキュリティ対策に取り組むことを自己宣言する制度 (※)

- 「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
- 2017年4月開始。「**人がいない**」、「**お金がない**」、「**何をどうやれば良いのかわからない**」との声に応えることを目的
- 対策に取り組むことを「**見える化**」。会社（組織）の内外に向けて宣言
- **IT導入補助金**の申請要件
- 宣言者数は、約42万件（2025年月7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）

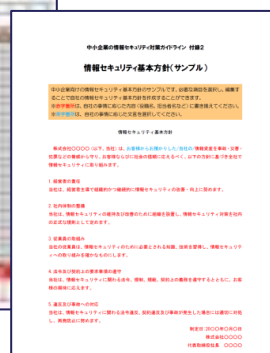
#### ●情報セキュリティ5か条に取り組む



### 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

★★二つ星





# サイバーセキュリティお助け隊サービスの活用を！

<https://www.ipa.go.jp/security/sme/otasuketai-about.html>



手遅れになるまえに、  
手を打つ。



「見守り」「駆付け」「保険」など中小企業のセキュリティ対策に  
不可欠なサービスをワンパッケージで安価に提供

## 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。

## 駆付け

問題が発生したときに、  
地域の IT 事業者等が  
駆付け対応します。  
(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！



- ◆IPAでは企業組織向けに、セキュリティに関する総合的な相談窓口を設けています。
- ◆セキュリティインシデント等が発生した際などにご活用ください。



受付可能な相談内容	
各種インシデント発生時の 初動対応に関する相談	<ul style="list-style-type: none"><li>• 起きている事象をヒアリングして、被害が発生しているか否かを判断します</li><li>• 被害が発生している場合、有効な応急処置についてご案内します</li><li>• インシデント対応を行う専門業者一覧の紹介をします</li><li>• 他に必要な相談・報告先等の紹介をします</li></ul>
標的型サイバー攻撃に関する インシデント相談	<ul style="list-style-type: none"><li>• 国家支援型と推定される標的型サイバー攻撃（APT）を受けた場合は、専門的知見をもとに支援を実施します</li></ul>
その他の情報セキュリティに関する 一般的な相談	<ul style="list-style-type: none"><li>• 中小企業などにおける、情報セキュリティ対策ガイドラインや各種支援ツール・支援施策などをご案内します</li></ul>
脅威情報に関する 情報提供	<ul style="list-style-type: none"><li>• IPAによる被害拡大防止策の実施や注意喚起のために、標的型サイバー攻撃や、その他の脅威情報に関して情報提供を受け付けています。</li></ul>



メール

[cs-support@ipa.go.jp](mailto:cs-support@ipa.go.jp)



ウェブサイト

<https://www.ipa.go.jp/security/support/soudan.html>



IPA