【公表予定】
資　料　6

# サイバーセキュリティ対策・内部不正防止対策

## 第10回営業秘密官民フォーラム

2024年6月28日

独立行政法人情報処理推進機構
セキュリティセンター長
高柳 大輔

# ご説明内容

- 「情報セキュリティの10大脅威2024」と
  セキュリティの脅威に係る注意喚起

- IPAの営業秘密保護・管理関連活動
  「内部不正防止対策・体制整備等に関する
  中小企業等の状況調査」ご紹介

Copyright © 2024 独立行政法人 情報処理推進機構

# 情報セキュリティ10大脅威 2024 脅威ランキング

https://www.ipa.go.jp/security/vuln/10threats2024.html

IPA

| 順位 | 組織 | 前年順位 |
|---|---|---|
| 1位 | ランサムウェアによる被害 | 1位 |
| 2位 | サプライチェーンの弱点を悪用した攻撃 | 2位 |
| 3位 | 内部不正による情報漏えい等の被害 | 4位 |
| 4位 | 標的型攻撃による機密情報の窃取 | 3位 |
| 5位 | 修正プログラムの公開前を狙う攻撃（ゼロディ攻撃） | 6位 |
| 6位 | 不注意による情報漏えい等の被害 | 9位 |
| 7位 | 脆弱性対策の公開に伴う悪用増加 | 8位 |
| 8位 | ビジネスメール詐欺による金銭被害 | 7位 |
| 9位 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 5位 |
| 10位 | 犯罪のビジネス化（アンダーグラウンドサービス） | 10位 |

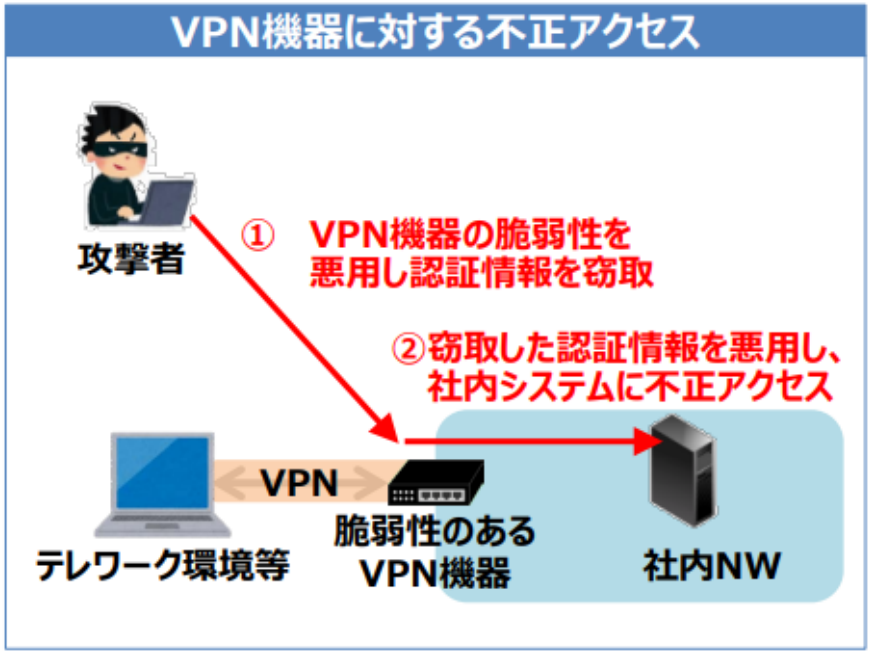
**「ネットワーク貫通型攻撃」（ネットワークの境界の機器の脆弱性を狙った攻撃）が拡大**

**Barracuda**
（CVE-2023-2868）
**ArrayAG**
（CVE-2022-42897、CVE-2023-28461）
**Fortinet**
（CVE-2023-27997他）
**Citrix**
（CVE-2023-4966、CVE-2023-4967）
**Ivanti**
（CVE-2023-46805、CVE-2024-21887）
**ColdFusion**
（CVE-2023-29300）
**Check Point**
（CVE-2024-24919）
・・・

IPAが脅威候補を選出し、専門家約200名からなる「10大脅威選考会」が投票

Copyright © 2024 独立行政法人 情報処理推進機構

# ネットワーク境界がアタックサーフェスに



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

| | |
|---|---|
| **2023/08/01** | **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<br>〜ネットワーク貫通型攻撃に注意しましょう〜**<br>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**<br>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ついて**<br>https://www.ipa.go.jp/security/security-alert/2024/alert_orb.html |

Copyright © 2024 独立行政法人 情報処理推進機構

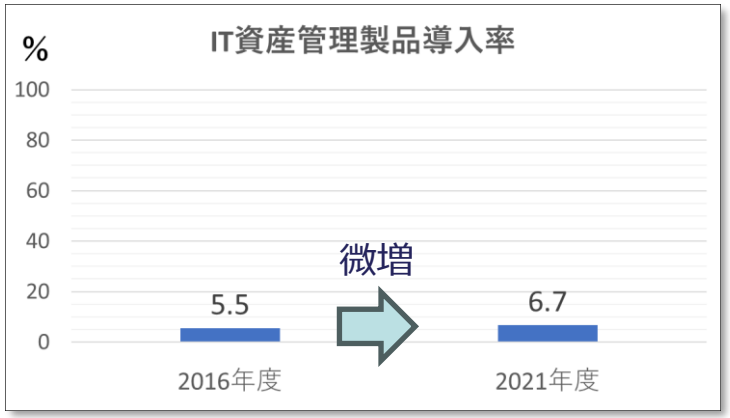
# 資産管理の不備を狙った脆弱性への攻撃に注意

10大脅威　1位、2位、3位、5位、8位関連

**組織、サプライチェーンのIT資産管理の不備から脆弱性残置→攻撃被弾**
**→ランサムウェア感染や機微情報の窃取への発展　にご注意！継続しています！**

中小企業では**IT資産管理（組織で運用しているIT機器が何か、稼働ソフトウェアも含めた管理）が不十分**で、管理不備による脆弱性を突いた攻撃で組織内に侵入される事例多発

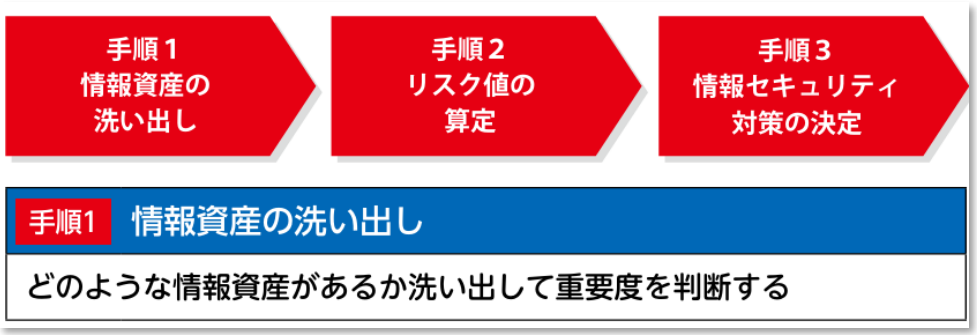
・IT資産管理状況（2016→2021）




IPA「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」（2021）より

https://www.ipa.go.jp/security/reports/sme/about.html

・IT資産の洗い出しと管理は
セキュリティ対策の一丁目一番地




「中小企業の情報セキュリティ対策ガイドライン V3.1」P54；詳細リスク分析の実施方法より

https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

Copyright © 2024 独立行政法人 情報処理推進機構

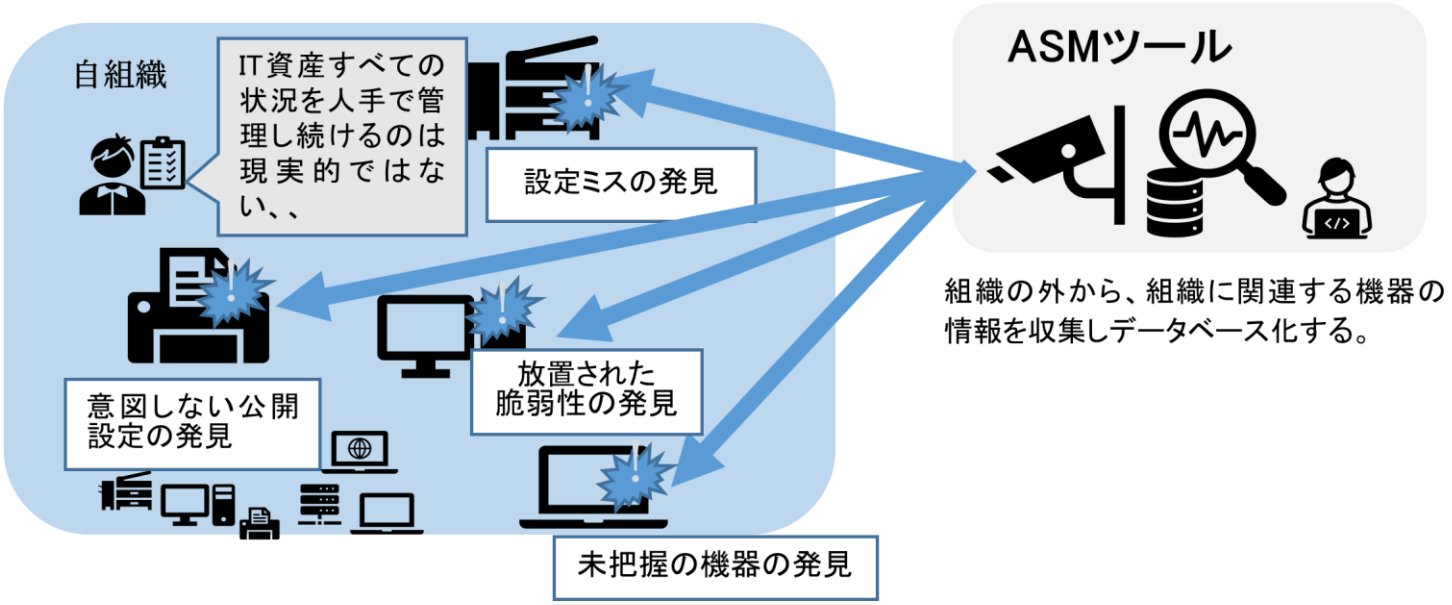
# 参考）ASM（Attack Surface Management）導入ガイダンス

**「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織のIT資産を発見し管理する～」**
**2023年5月29日　経済産業省**

https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html

**一般的なASMの特徴とイメージ**

- インターネットにつながっている世界中の機器の公開情報を継続的に収集・蓄積
- 特定の条件に合致する機器などを検索可能（無料でも可能）




Copyright © 2024 独立行政法人 情報処理推進機構

# 営業秘密保護・管理の啓発に係るIPAの取り組み

10大脅威　3位！

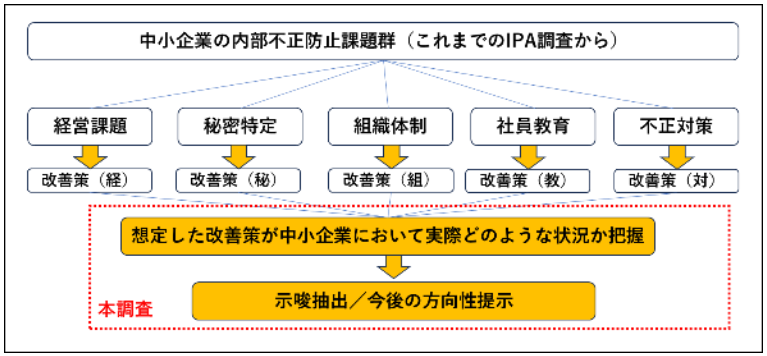
## 1.「組織における内部不正防止ガイドライン」第5版

・内部不正防止の重要性や対策の体制、 関連する法律などの概要

・「基本方針」「資産管理」「技術的管理」「職場環境」「事後対策」等の10の観点、合計33項目の具体的な対策を示したガイドライン

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

## 2. 企業の内部不正防止体制に関する実態調査（2024年5月公開）




・中小企業の情報管理の課題・改善策整理

・経営者の意識、基本方針の策定状況、組織体制の整備状況、対策の実態、取組み事例等を調査

詳細はこちらです！

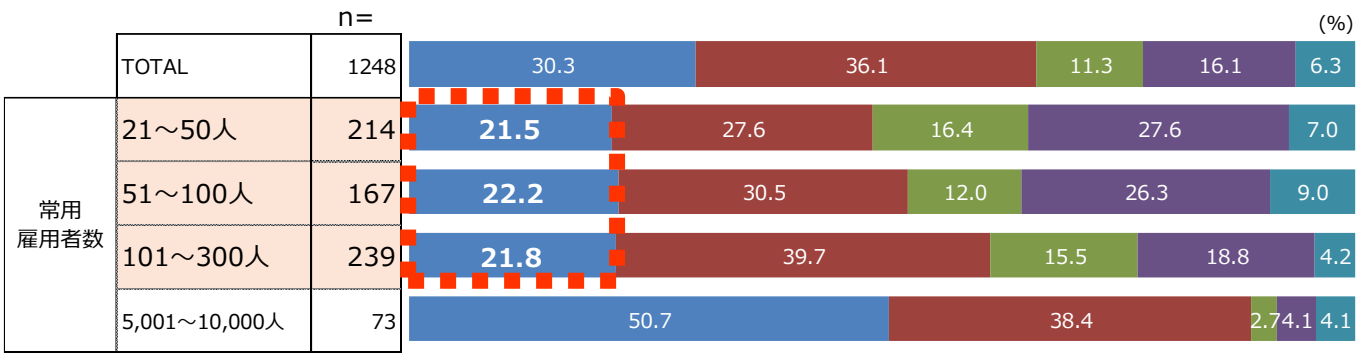
**https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html**

Copyright © 2024 独立行政法人 情報処理推進機構

# 中小企業における内部不正対策は喫緊の課題

## 中小企業における**秘密情報の格付け表示**の実施割合は大企業に比べて低い。

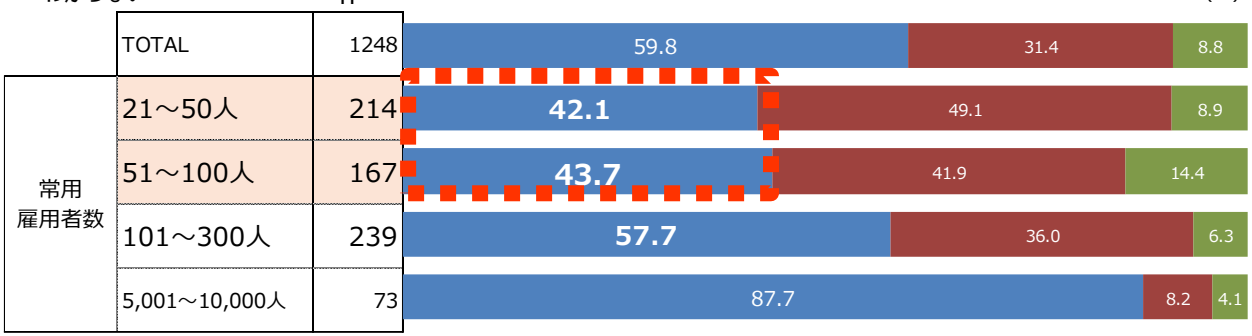
**・格付けの表示などによって秘密情報であることを従業員は認知できるか**




**「何を守るべきか」の把握・共有は情報管理の基本**

## 中小企業では**内部不正防止の基本方針を重点的に定めた**割合は大企業に比べて低い。

**・経営層は内部不正防止とサイバーセキュリティ確保を分けた基本方針を定めているか**




**組織的な内部不正対策が十分とは言えない**

調査で得た知見は新作の映像コンテンツにも反映

（内部不正防止対策・体制整備等に関する中小企業等の状況調査（2024年5月）を基に再構成）

Copyright © 2024 独立行政法人 情報処理推進機構

# 参考）内部不正対策の動画コンテンツ

## 内部不正防止教育に役立つ映像コンテンツの新作をリリースしました（2024/3）

実際にあった近年の事例から

**・主な手口**
**・不正を起こさせないポイント**
**・対策を行うべき各部門の役割**

等をわかりやすく解説

【新作】今、そこにある脅威～内部不正による情報流出のリスク～
**https://www.youtube.com/watch?v=YVBHBIf23gA**

IPA映像コンテンツ一覧
**https://www.ipa.go.jp/security/videos/list.html#keihatsu_new**

Copyright © 2024 独立行政法人 情報処理推進機構

IPA Better Life with IT

＜お問い合わせ･ご相談先＞
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
isec-info@ipa.go.jp