# 2024年度ISSスクエアシンポジウム研究成果発表

# 内部不正防止ガイドラインへの提言
## ～最近の事例調査より～

2025年2月28日
マネジメント分科会

# マネジメント分科会の紹介

## マネジメント分科会の研究方針

様々なルール・基準と実際の乖離に注目し、

実際のシステムや環境、予算、組織文化・人に合わせた対策を

調査・議論を通して、総合的に検討

## メンバー

- リーダー：稲葉 緑 准教授
- M2：澤、齋藤、KANG、加藤(美)
- M1：伊藤、対馬、西村、町田、加藤(寛)

# 目次

# 1. 研究テーマ

## マネジメント分科会のテーマ：内部不正とその対策

## 選定理由

### 被害額が大きい


THREAT REPORT

2022 Ponemon Cost of Insider Threats Global Report

*Independently conducted by Ponemon Institute*

External attackers aren't the only threats modern organizations need to consider in their cybersecurity planning. Malicious, negligent and compromised users are a serious and growing risk. As the 2022 Cost of Insider Threats: Global Report reveals, insider threat incidents have risen 44% over the past two years, with costs per incident up more than a third to $15.38 million.

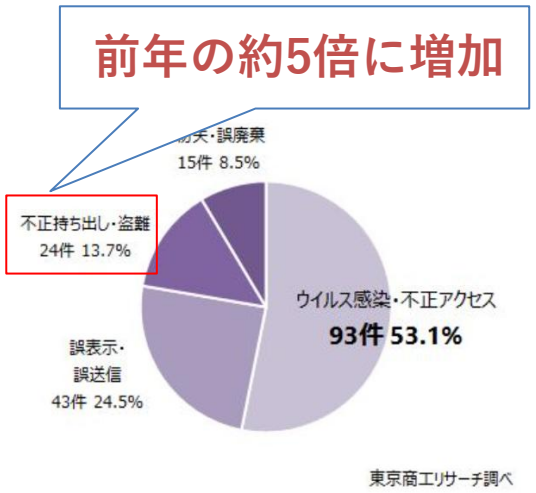
Here are just a few highlights from this year's report:

内部脅威インシデント1件のコストは過去2年で3分の1以上増加しており、1,538万ドルに達する。

on an annualized basis.

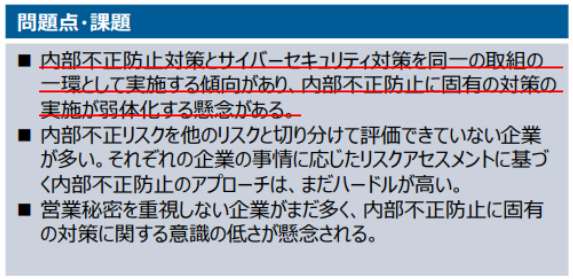
Ponemon Institute「2022 Ponemon Cost of Insider Threats Global Report」

### 被害件数が増加傾向




東京商工リサーチ「2023年「上場企業の個人情報漏えい・紛失事故」調査」

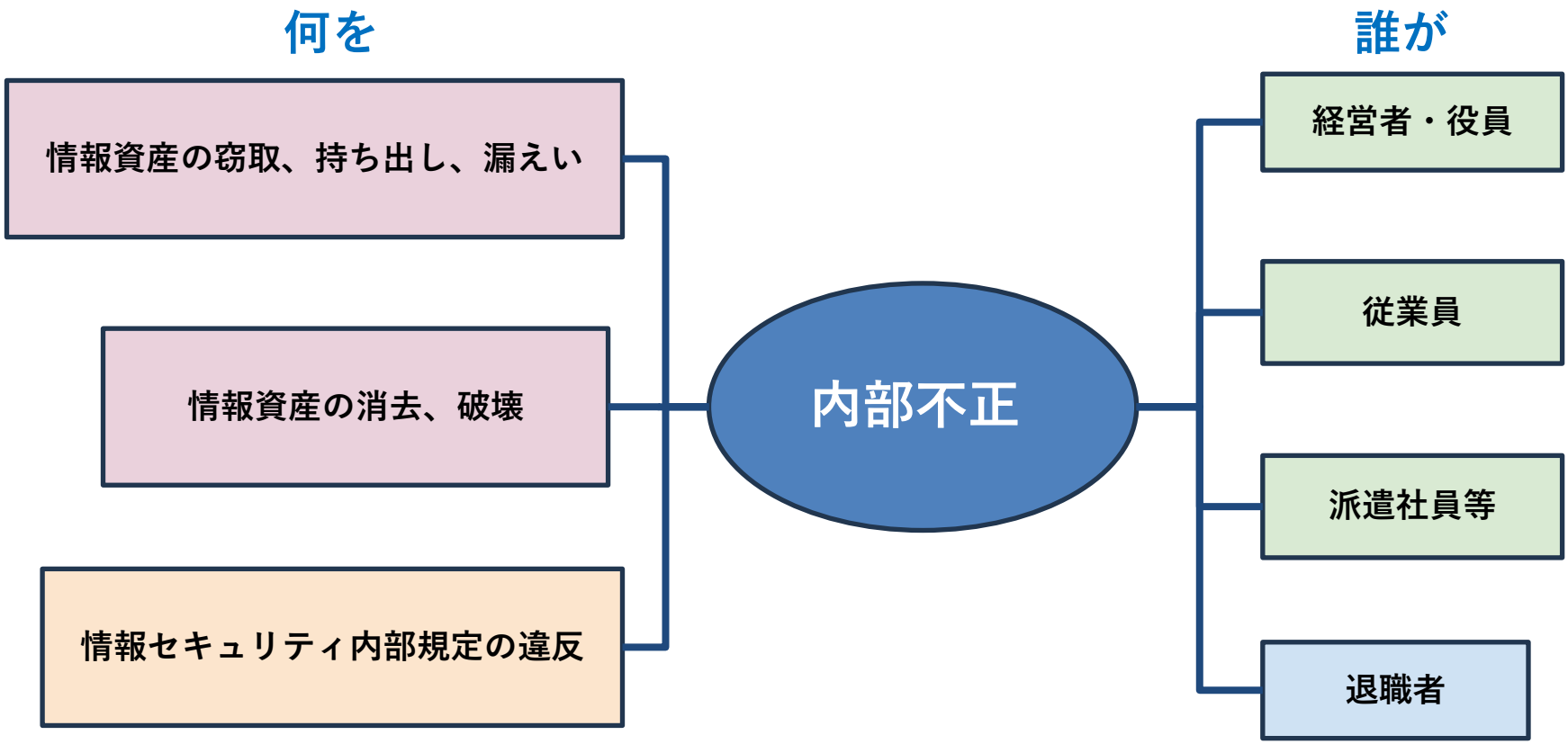
### サイバー攻撃とは対策が異なる


問題点・課題

- 内部不正防止対策とサイバーセキュリティ対策を同一の取組の一環として実施する傾向があり、内部不正防止に固有の対策の実施が弱体化する懸念がある。
- 内部不正リスクを他のリスクと切り分けて評価できていない企業が多い。それぞれの企業の事情に応じたリスクアセスメントに基づく内部不正防止のアプローチは、まだハードルが高い。
- 営業秘密を重視しない企業がまだ多く、内部不正防止に固有の対策に関する意識の低さが懸念される。

IPA「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」より

# 1-1. 「内部不正」とは




**IPA『組織における内部不正防止ガイドライン』での定義**

# 1-2. 今年度の研究テーマ

**内部不正とその対策に関する問題**

候補：

- ガイドラインの問題　→　今年度のテーマ
- 企業が対策を導入するにあたっての障壁

# 1-3. IPA『組織における内部不正防止ガイドライン』


1. 基本方針（経営者の責任、ガバナンス）
2. 資産管理（秘密指定、アクセス権）
3. 物理的管理
4. 技術・運用管理
5. 原因究明と証拠確保
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

- 初版は**2013年3月**
  （2022年4月に改訂5版）
- 全136ページ
- 10の観点、33項目の具体的対策

| No | 内容 | 直接部門 | 関連部門 情報システム部門 | 総務部門 | 人事部門 | 法務知財部門 | 社内外監査 |
|---|---|---|---|---|---|---|---|
| 4-3. 物理的管理 | | | | | | | |
| (8) | 重要情報の格納場所や取り扱う領域等を物理的に保護するために壁や入退管理策によって保護していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | | |
| (9)-① | PC 等の情報機器や USB メモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がないように管理・保護していますか? | 実施済み 着手 未実施 | [ ] | | | | |
| (9)-② | 情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認していますか? | 実施済み 着手 未実施 | [ ] | | | | |
| (10) | モバイル機器や携帯可能な記録媒体を外部に持ち出す場合には、持ち出しの承認及び記録等の管理をしていますか? | 実施済み 着手 未実施 | [ ] | | | | |
| (11) | 個人のモバイル機器及び記録媒体の業務利用及び持込を制限していますか? | [ ] | 実施済み 着手 未実施 | | | | |
| 4-4. 技術・運用管理 | | | | | | | |
| (12) | モニタリングシステムが提供する AI 監視機能等(例:ふるまい解析機能)の有効性を評価していますか? | | 実施済み 着手 未実施 | | | | |
| (13) | 組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトや SNS、外部のオンラインストレージ等の使用を制限していますか? | | 実施済み 着手 未実施 | | | | |
| (14)-① | 委託先等の関係者への重要情報の受渡しは、受渡しから廃棄迄を含めて管理していますか? | 実施済み 着手 未実施 | [ ] | | | | |
| (14)-② | インターネット等の組織外を介す重要情報の受渡しでは、誤って関係者以外に渡ってしまうことも考慮し、暗号化等で保護していますか? | 実施済み 着手 未実施 | [ ] | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 4-6. 人的管理 | | | | | | |
| (20)-① | 従 この 得 職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | |
| (20)-② | 教育を定期的に繰り返して実施し、教育内容を定期的に見直しに更新していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | |
| (21) | 従業員の行動や心身の状態のモニタリングの目的が、従業員の適正かつ健全な従業を支援し、従業員を内部不正から 保護する ためであることを、就業規則 で 広く 周知していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | [ ] |
| (22) | 派遣労働者による重要情報の漏えい等の不正行為が発生しないように、派遣元と協力して、秘密保持義務を課していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | [ ] |
| (23) | 雇用の終了時に秘密保持義務を課す誓約書の提出を求めていますか?（推奨） | 実施済み 着手 未実施 | | [ ] | [ ] | [ ] |
| (24) | 役職員の雇用終了時および提供等の契約先との契約終了時に、取り扱いを委託した情報資産の全てを返却または完全消去し、情報システムの利用者 ID や権限を削除していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | [ ] |
| 4-7. コンプライアンス | | | | | | |
| (25) | 就業規則等の内部規程を整備し、正式な懲戒手続を備えていますか? | 実施済み 着手 未実施 | | [ ] | [ ] | [ ] |
| (26) | 役職員に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等を徴収していますか? | 実施済み 着手 未実施 | | [ ] | [ ] | [ ] |
| 4-8. 職場環境 | | | | | | |
| (27) | 公平で客観的な人事評価を整備するとともに、業績に対する評価を開示する機会を設ける等、人事評価や業績評価の整備を推進していますか?（推奨） | | | [ ] | 実施済み 着手 未実施 | |
| (28) | 業務量及び労働時間の適正化等の適切な労働環境を整備するとともに、業務を支援する体制や相談しやすい環境を整える等職場内において良好なコミュニケーションを組織全体で推進していますか?（推奨） | | | | 実施済み 着手 未実施 | [ ] |

# 1-4. リサーチ・クエスチョン

IPAの内部不正防止ガイドラインがあるにもかかわらず、
内部不正の件数が増加しているのはなぜだろう？

RQ１：最近の内部不正インシデントには、IPAの内部不正ガイドラインでカバーされない質的な変化があるのではないか？

RQ２：最近の世の中の変化に、IPAの内部不正防止ガイドラインの効果を阻害する要因があるのではないか？

# 2. 国内事例調査

## 調査概要

2022年以降の内部不正による国内インシデント

## 調査対象①　国内インシデントニュース

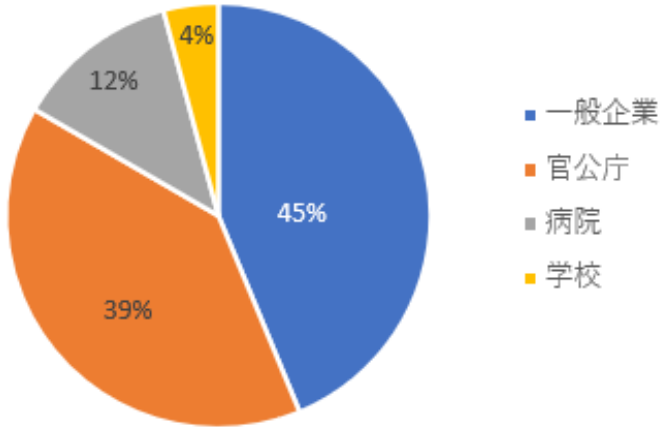
- 調査範囲：2022/11/29～2024/11/20（外部公開日）
- 調査元　：Security NEXT（セキュリティニュースサイト）

## 調査対象②　国内の裁判事例

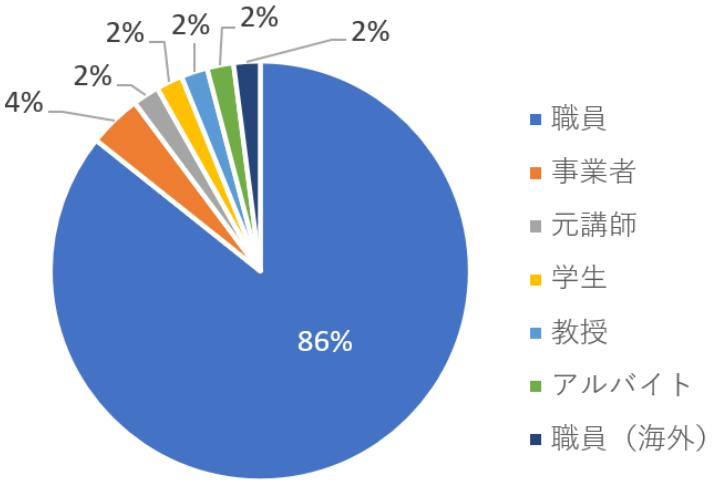
- 調査範囲：2022/1/1（裁判日付）以降
- 調査元　：Westlaw Japan（国内の判例データベース）
  以下をキーワードとして調査（計23件）
  - 営業秘密
  - 個人情報データベース

# 2-1. 国内事例調査①「Security NEXT」より

## 誰が



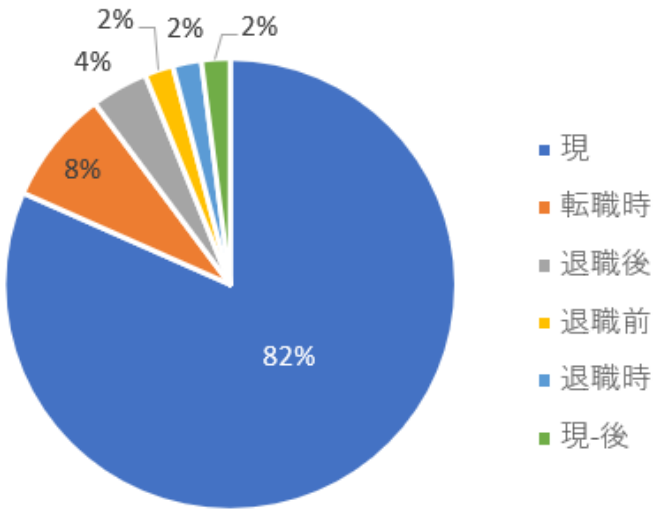

業界別では、一般企業の割合が一番多く、次に官公庁（地方行政等を含む）が多い結果となった。




職員が不正を働く割合が最も多いが、アルバイトによる不正も事例として存在した。

# 2-1. 国内事例調査①「Security NEXT」より

## いつ

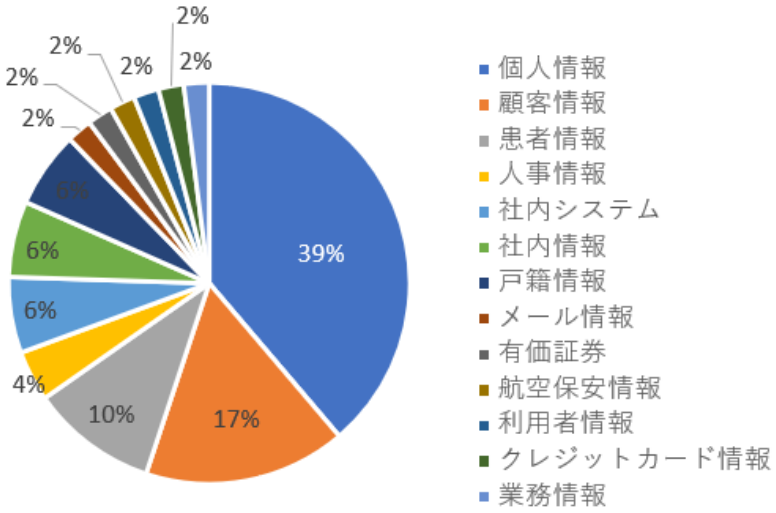



現職時に不正をはたらく割合が最も多く、転職時の犯行は少ない結果となった。

ただし、現職時に今後転職する可能性については、ニュースサイトからは読み取れなかった。

# 2-1. 国内事例調査①「Security NEXT」より

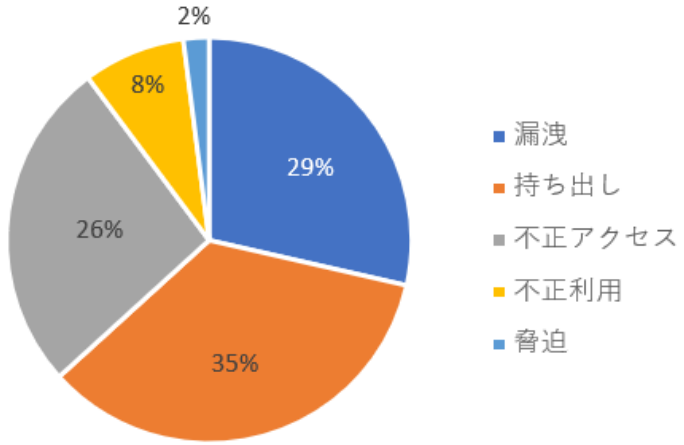
## 何を




半数以上が個人情報に関するものであり、社内に関する情報は個人情報に比べると少ない結果となった。

- 個人情報(個人,患者,戸籍) 約55%
- 社内情報(顧客,人事,メール) 約35%

## どうした

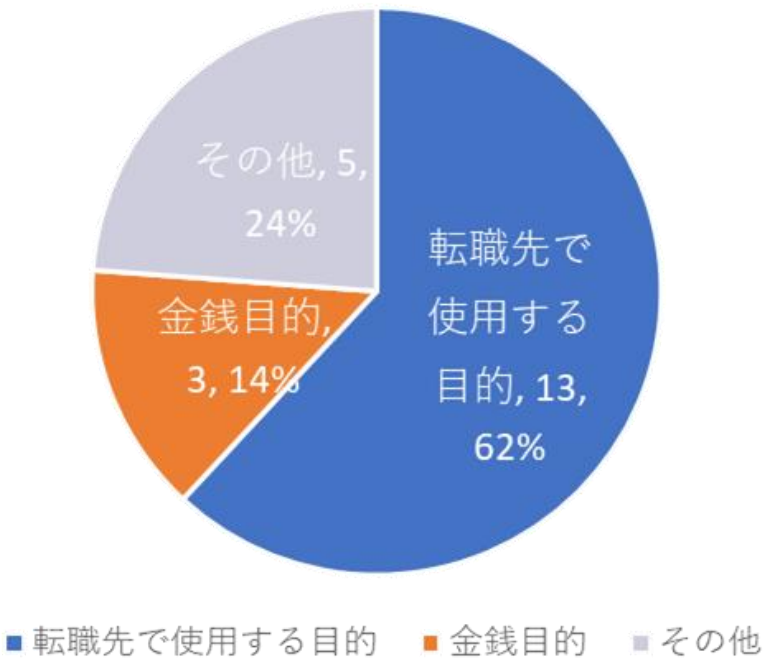



漏洩や持ち出しが全体の6割以上を占めた。

なお、「不正アクセス」は本来アクセスできないはずの情報にアクセスする職権乱用等も含む。

# 2-2. 国内事例調査②「Westlaw Japan」より

## 動機




※「転職先で使用する目的」には、
退職後に自社で使用する目的を含む

## 持ち出し方法

| 持出し方法 | 件数 | 割合 |
|---|---|---|
| メールで外部送信 | 6 | 24% |
| 私用クラウドへアップロード | 4 | 16% |
| USB | 2 | 8% |
| HDDコピー | 2 | 8% |
| チャットツールで外部送信 | 2 | 8% |
| 業務用クラウドから私用PCへダウンロード | 2 | 8% |
| 記録媒体（具体的内容不明）の持出し | 1 | 4% |
| ファイル転送サービスの利用 | 1 | 4% |
| スマートフォンに入力して記録 | 1 | 4% |
| 動画撮影 | 1 | 4% |
| 不明 | 3 | 12% |
| 合計 | 25 | 100% |

※複数に該当する場合はそれぞれカウント

# 2-2. 国内事例調査 ～個別事例～

| 組織 | 不正概要 | 手法 |
|---|---|---|
| 某通信企業子会社の委託先従業員 | 10年以上にわたり計928万人分の個人情報を名簿業者に売却 | 詳細不明 |
| 某商社の従業員 | 会社システム上に保存された機密情報を持ち出し | 私用のGoogle Drive |
| 某学習塾の講師 | 在校児童の個人データをスマートフォンに打込み盗撮した写真等とともにSNSに掲載 | スマートフォン |
| 某ITサービス企業の元従業員 | テスト設計書の電子ファイルを無断で転職先へ持ち込み | 私用のチャットツール |
| 某社の従業員 | 得意先電子元帳の複製を作成し第三者に送信 | LINEの画像キャプチャ機能 |
| 某マスメディアの委託先従業員 | 顧客情報にアクセスできる機械を路上で元参議院議員に開示し、同議員が当該画面を動画で撮影 | デバイス持出し、動画撮影 |

※個人情報保護委員会の行政処分事例や判例より抜粋

# 2-3. リサーチクエスチョン１への回答

**RQ１：最近の内部不正インシデントには、IPAの内部不正ガイドラインでカバーされない質的な変化があるのではないか？**

**動機や持ち出し手法に目新しい傾向はみられず、**

**引き続き既存の対策が重要**

※チャットツール、スマートフォンへの入力、動画撮影についてはIPAのガイドラインに明記はないが、許可ソフトウェア以外の禁止(IPA 13)や業務利用デバイスの持ち出し(IPA 10)、個人デバイスの持ち込み(IPA 11)に該当

# 3 - 1. 世の中の変化

- 雇用の流動化（転職、副業、フリーランス）
- 人材不足
- 地政学的脅威
- 攻撃グループや攻撃手法の多様化

⇒ **ガイドラインを適用しても、**
**その効果を妨げる要因があるのではないか？**

# 3 - 1. 世の中の変化

## 国内事例

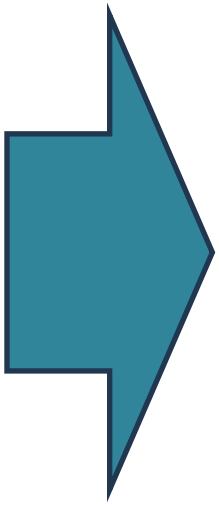
| 組織 | 概要 | 脅威 |
|---|---|---|
| 某学習塾の講師 | 在校児童の個人データをスマートフォンに打込み**盗撮した写真等とともにSNSに掲載** | **資質問題** |
| 某通信企業子会社の委託先従業員 | **10年以上**にわたり計928万人分の個人情報を名簿業者に売却 | **長期間の犯行** |

## 海外事例

| 組織 | 概要 | 脅威 |
|---|---|---|
| 某セキュリティベンダー（米） | 企業が北朝鮮の**偽労働者を採用**（米国の身元有効な人物情報より写真を差し替えて利用） | **なりすまし** |
| 某自動車企業（米） | ランサムウェアグループが勤務する従業員に**報酬100万ドルで攻撃要請** | **攻撃者からの要請** |

# 3-2. リサーチクエスチョン２への回答

RQ２：最近の世の中の変化に、IPAの内部不正防止ガイドラインの効果を阻害する要因があるのではないか？



IPAの内部不正防止ガイドラインによる対策は、
アクセス権管理や物理デバイス制限など、
犯行手段を塞ぐ対策に偏っているが、

**プロアクティブな対策もあわせて必要**

# 3-3. プロアクティブな対策

## ① 強制休暇の実施

同じ職務を続けていると、不正をしやすい環境が生まれる

・不正ができない環境を突発的に作る、不正を発見できる機会を作る

## ② 従業員エンゲージメント向上

金銭目的のみで働いていると、不正の誘惑に負けやすい

・企業の理念やビジョンを明確にし、従業員に周知する

・従業員を承認したり褒める文化をつくる

## ③ 入社時チェック

入社時チェックというと
**セキュリティクリアランス**？
でも一般企業でそんなことやりきれない…

# 3-3. 入社時チェックとは

| 脅威 | 実施項目 |
|---|---|
| **なりすまし** | ✓ **面接時**：出身大学近くのお気に入りの飲食店を答えさせるなどカジュアルな質問を実施する<br>✓ **履歴書**：検索エンジンを使用して取得した職歴や学歴の連絡先に確認をとる |
| **資質問題** | ✓ **テスト　**：心理分析テストや性格分析テストを実施する<br>✓ **SNS確認**：SNSでのふるまいを確認する<br>✓ **勤務態度**：現職や前職の関係者にヒアリングする |

※採用のため、第三者より応募者の情報を取得する場合は、原則として本人の同意が必要

**バックグラウンドチェックには有料サービスも…**
**基本調査：3~5万円、詳細調査：5~10万円**（出典：エン転職）

米国では過失採用の一環から95%の雇用者が実施しており、
日本でも外資系や一部の企業で実施されている。（出典：テイタン）

# 4. まとめ

分科会のテーマ「内部不正とその対策に関する問題」に対し、IPAの『内部不正防止ガイドライン』を取り上げ、２つの問いをたてて調査を行った。

RQ１：最近の内部不正インシデントには、IPAの内部不正ガイドラインでカバーされない質的な変化があるのではないか？

→ 動機や持ち出し手法に目新しい傾向はみられなかった。

RQ２：最近の世の中の変化に、IPAの内部不正防止ガイドラインの効果を阻害する要因があるのではないか？

→ 長期間に及ぶ犯行や資質問題、海外事例のなりすまし等を考慮すると、強制休暇による不正抑制や、一層の従業員エンゲージメント向上、入社時チェックなどのプロアクティブな対策も必要である。

# ご清聴ありがとうございました

# 参考資料

## [1．研究テーマ]


- Ponemon Institute. "2022 Ponemon Cost of Insider Threats Global Report". https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats
- 東京商工リサーチ. “2023年の「個人情報漏えい・紛失事故」が年間最多　件数175件、流出・紛失情報も最多の4,090万人分”. 2024/1/19. https://www.tsr-net.co.jp/data/detail/1198311_1527.html
- IPA. “2023年度「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」報告書”. 2024/5/30. https://www.ipa.go.jp/security/reports/economics/ts-kanri/20240530.html
- IPA. “組織における内部不正防止ガイドライン”. 2023/10/30（最終更新日）. https://www.ipa.go.jp/security/guide/insider.html

## [2．国内事例]


- Security NEXT. “内部犯行関連の記事一覧”. https://www.security-next.com/category/cat191/cat25/cat173
- 個人情報保護委員会. “報道発表資料”. https://www.ppc.go.jp/news/press/
- Westlaw Japan　https://www.westlawjapan.com/


## [3．海外事例]


- Patrick Howell O'Neill. “テスラ従業員、報酬100万ドルを蹴ってハッキング計画をFBIに通報”. 2020/9/3. https://www.technologyreview.jp/s/217844/how-a-1-million-plot-to-hack-tesla-failed/
- KnowBe4. “北朝鮮の偽IT労働者に関するFAQ”. https://www.knowbe4.jp/blog/north-korean-fake-it-worker-faq

## ［3．プロアクティブな対策］


- マンパワーグループ株式会社. “従業員エンゲージメントを向上させるには？”7つ“の効果的な施策を解説！”. 2024/05/20（最終更新日）. https://mpg.rightmanagement.jp/hrcafe/consulting/211108-2.html
- Stu Sjouwerman. “North Korean IT Worker Threat: 10 Critical Updates to Your Hiring Process”. KnowBe4. https://blog.knowbe4.com/north-korean-it-worker-threat-10-critical-updates-to-your-hiring-process
- Darren Williams. “Ransomware Groups Now Recruiting your Emplyess”. BlackFog. 2024/1/22（最終更新日）. https://www.blackfog.com/ransomware-groups-recruiting-your-employees/
- エン転職. “バックグラウンドチェックとは？ 調査内容や実施方法、費用、注意点を解説”. 2024/4/26. https://saiyo.employment.en-japan.com/blog/background-check
- テイタン. “雇用者なら知っておきたい”アメリカで95％の企業がバックグラウンドチェックを行っている理由”. https://www.teitan.co.jp/knowledge/column/hiring3/