金融機関の予防型内部不正リスク管理

- 情報持出し、着服などの内部不正のリスク予兆をとらえるログデータ活用術 -

株式会社エルテス

IRI事業部　エバンジェリスト

永易 靖規

登壇者紹介

株式会社エルテス

IRI営業部　エバンジェリスト

永易 靖規

サイバーセキュリティ企業で営業責任者として会社の
株式上場後、2021年株式会社エルテス参画。
従業員数10000人以上の大手企業を中心に内部脅威対策
の導入実績を増やし、サービス向上の企画を実施。

会社名	株式会社エルテス （ 英語表記：Eltes Co., Ltd ）
創　業	2004年4月28日
資本金	1,270百万円（2025年8月末時点）
所在地	本　　店　岩手県紫波郡紫波町紫波中央駅前2-3-94 オガールセンター内 東京本社　東京都千代田区霞が関3-2-5　霞が関ビルディング6階
従業員数	472名（2025年8月末時点・連結）
上場市場	東京証券取引所グロース（証券コード 3967）

役　員

代表取締役	菅原 貴弘	取締役	三川 剛
社外取締役	伊藤 豊	監査役	宮崎 園子
監査役	本橋 広行	監査役	高橋 宜治

連結子会社

株式会社AIK
SSS株式会社
株式会社GloLing
株式会社SRIA Lab
株式会社エルテスキャピタル
株式会社And Security
東和警備株式会社
プレイネクストラボ株式会社
アクター株式会社
ISA株式会社
株式会社JAPANDX
JDXソリューションズ株式会社
株式会社イーリアルティ

取得認証

JIS Q 27001:2014　(ISO/IEC 27001:2013)　No. C2022-02171-R1
JIP-ISMS517-1.0　(ISO/IEC 27017:2015)　No. PJRJ2022-037

事業内容

デジタルリスク事業

- 24時間365日体制でモニタリングし、リスクを早期検知するリスクモニタリング
- Webレピュテーションリスクのコンサルティング
- 企業のPCログ等の解析によって、情報漏洩や労務リスクなどの内部脅威検知

AIセキュリティ事業

- 警備業務のDX化を支援するDXプロダクト「AIKシリーズ」の開発・提供
- 安全・安心を提供する警備保障サービス

DX推進事業

- デジタル田園都市国家構想にも沿った、行政サービスのデジタル化支援
- SESとラボ型開発のハイブリッドによるクライアントニーズに沿ったDX支援

スマートシティ事業

- 不動産管理業務のDX化ソリューション開発・提供
- プロパティ・マネジメントサービスの提供
- エストニアのサイバネティカ社と連携したデータ連携プラットフォーム構築

オフィス環境

Entrance

Meeting Room

Work Space

内部不正の実態（全体）

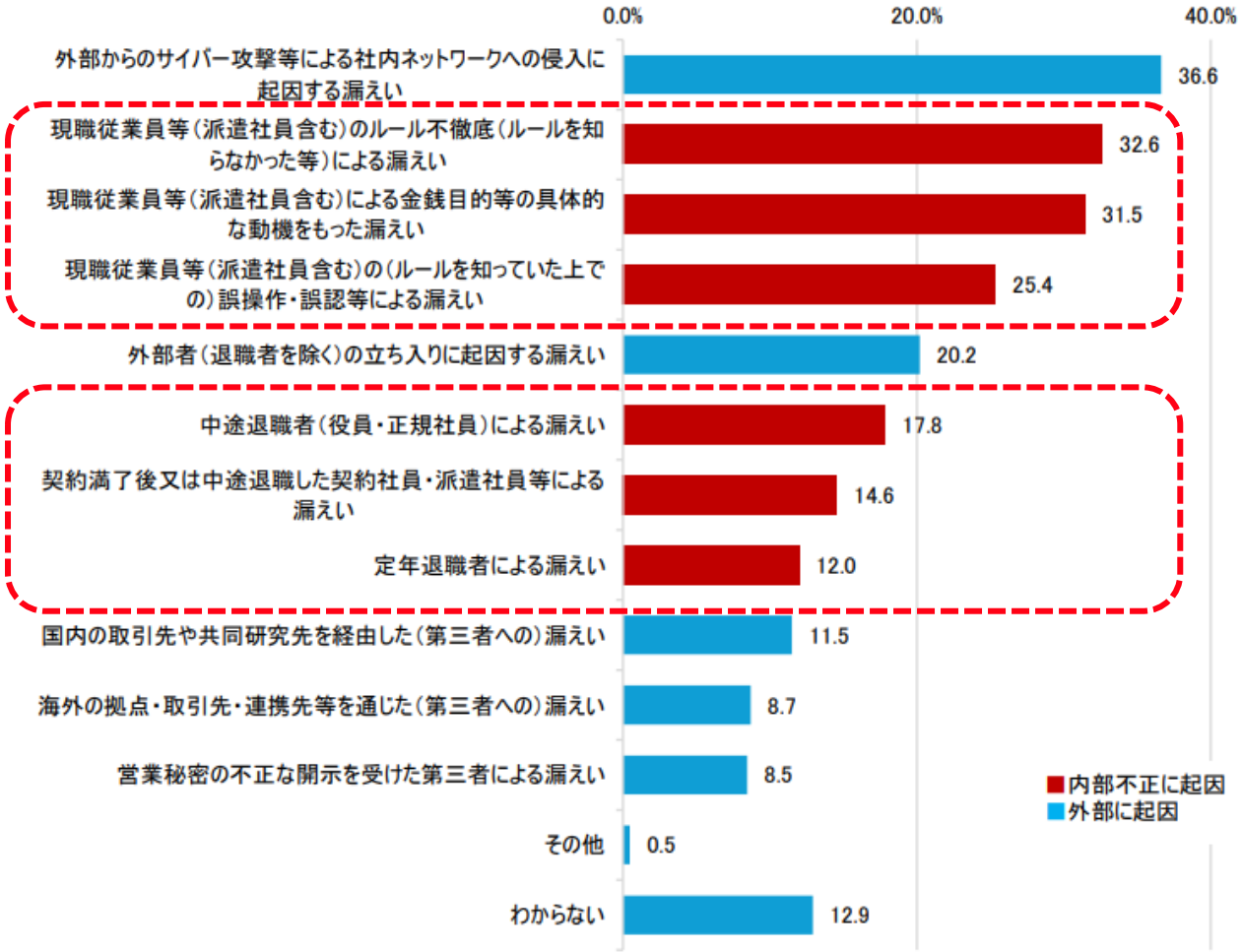
情報漏洩は内部関係者による漏洩が**7割**以上

情報セキュリティ10大脅威 2025

	原因
1	ランサムウェアによる被害
2	サプライチェーンや委託先を狙った攻撃
3	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等**
5	機密情報等を狙った標的型攻撃
6	リモートワーク等の環境や仕組みを狙った攻撃
7	地政学的リスクに起因するサイバー攻撃
8	分散型サービス妨害攻撃（DDoS攻撃）
9	ビジネスメール詐欺
10	**不注意による情報漏えい等**

出典：独立行政法人 情報処理推進機構（IPA）「情報セキュリティ10大脅威 2025」を元に作成

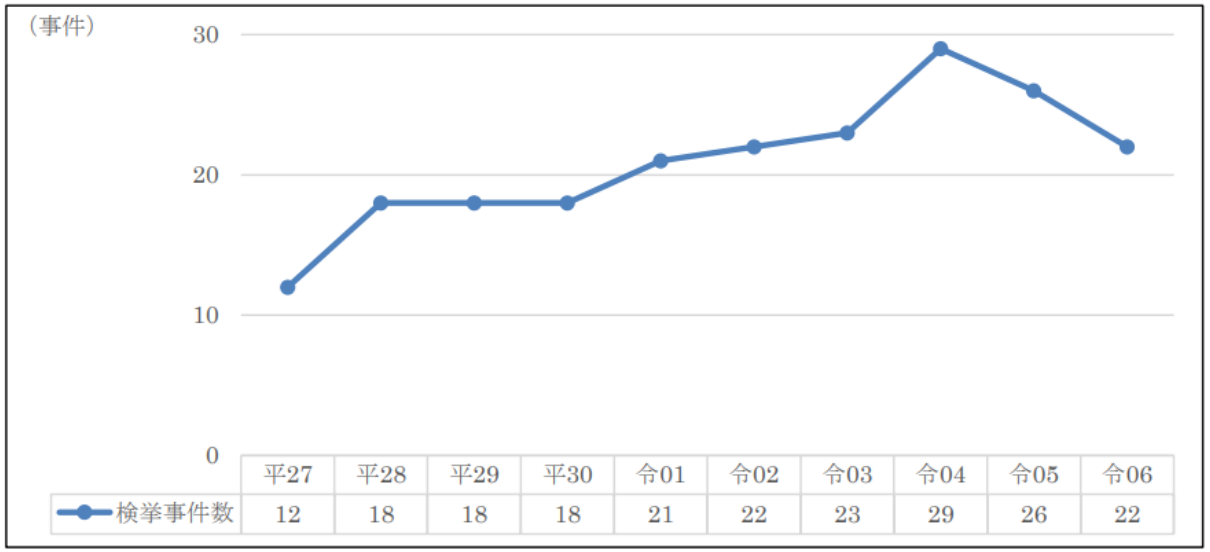
情報漏洩のルート



出典：独立行政法人 情報処理推進機構（IPA）「企業における営業秘密管理に関する実態調査2024」調査実施報告書

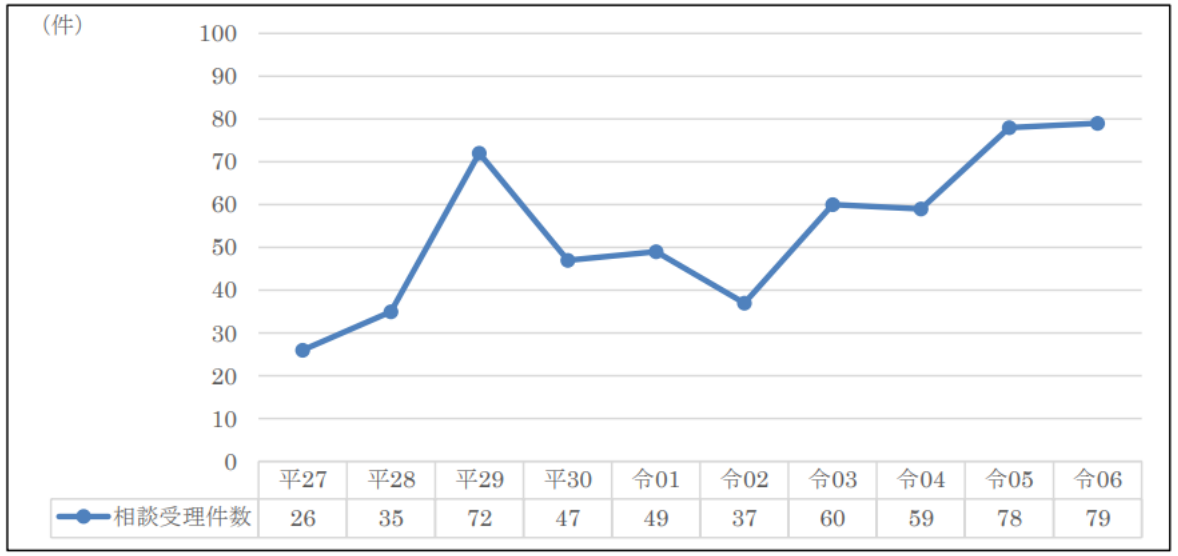
営業秘密持ち出しの実態

営業秘密侵害事犯の検挙事件数の推移



	平27	平28	平29	平30	令01	令02	令03	令04	令05	令06
検挙事件数	12	18	18	18	21	22	23	29	26	22

営業秘密侵害事犯に関する相談受理数の推移



	平27	平28	平29	平30	令01	令02	令03	令04	令05	令06
相談受理件数	26	35	72	47	49	37	60	59	78	79

相情報秘密侵害事件は**年間20～30件**前後発生

相談件数は**過去最多水準**（79件）に達し、トラブルが身近になっている

出典：警察庁「令和6年における生活経済事犯の検挙状況等について」より引用

相次ぐ内部不正のインシデント

2021 2022 2023 2024 2025 2026

- ⚠ **通信業界**での**技術情報**の持ち出し
- ⚠ **外食業界**での**製品情報**の持ち出し
- ⚠ **不動産業界**での**顧客情報**の持ち出し
- ⚠ **商社**での**営業秘密**の持ち出し
- ⚠ **通信業界**での**顧客情報**の持ち出し
- ⚠ **海外企業**での**機密情報をChatGPTにアップロードし、情報流出**
- ⚠ **金融業界**での**顧客情報**の持ち出し
- ⚠ **不動産業界**での**顧客情報**の持ち出し
- ⚠ **電子部品メーカー**での**技術情報**の持ち出し
- ⚠ **金融業界**での**顧客情報**の持ち出し
- ⚠ **運輸業界**での**取引先企業情報**の持ち出し
- ⚠ **生命保険業界**での**顧客情報**の持ち出し

内部不正は
業種や企業規模を問わず
多数発生している

- **各種法規制の動き**
- **業界での規制強化**

- ✓ GDPRなどの世界的な情報管理の潮流を受けた、個人情報保護法の強化
- ✓ 日本証券業協会は証券会社での顧客情報の管理ルールを強化
- ✓ 不正競争防止法の改正に合わせた、営業秘密の管理強化

シャドーAIリスク

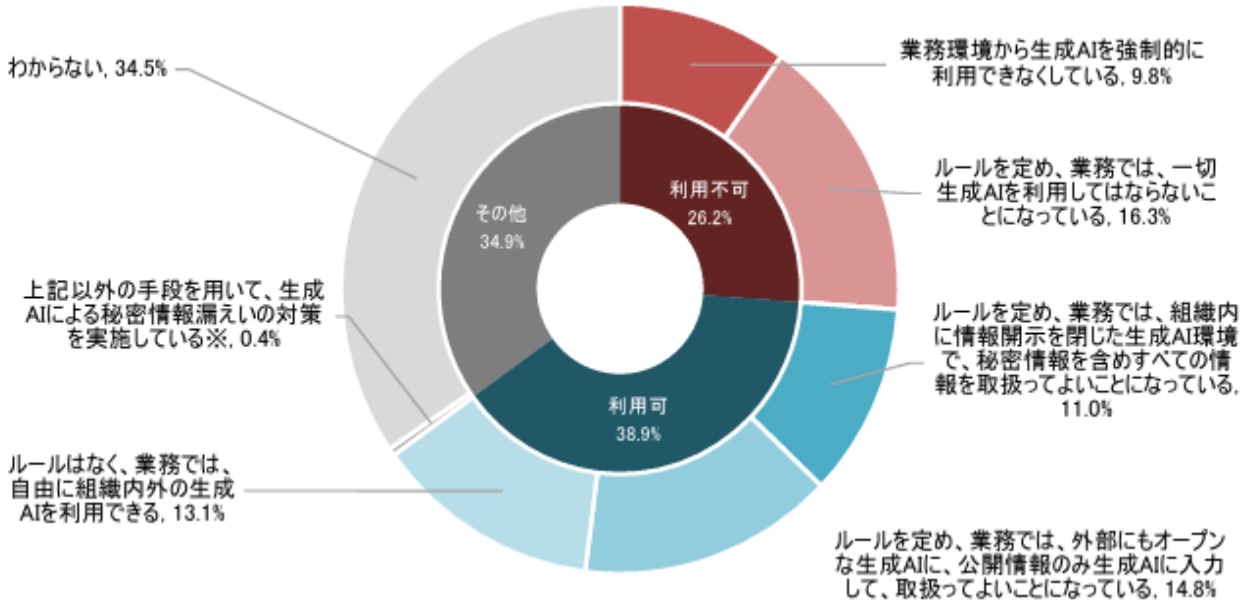
■ 背景

昨今、国内の企業の生成AIの活用が増えている。

その中で独立行政法人 情報処理推進機構(IPA)が8月29日に公開した「企業における営業秘密管理に関する実態調査2024」では生成AIに対してのルールや利用の状況を報告しており、**約52%の企業が生成AIの利用についてルールを定めている。**

IRIではその背景からブラックボックス化されやすい生成AIの利用がルールに従って運用されているかを可視化するため機能拡張をしました。

■ 生成AIの業務利用可否と取扱い可能な情報の種別(n=1200)



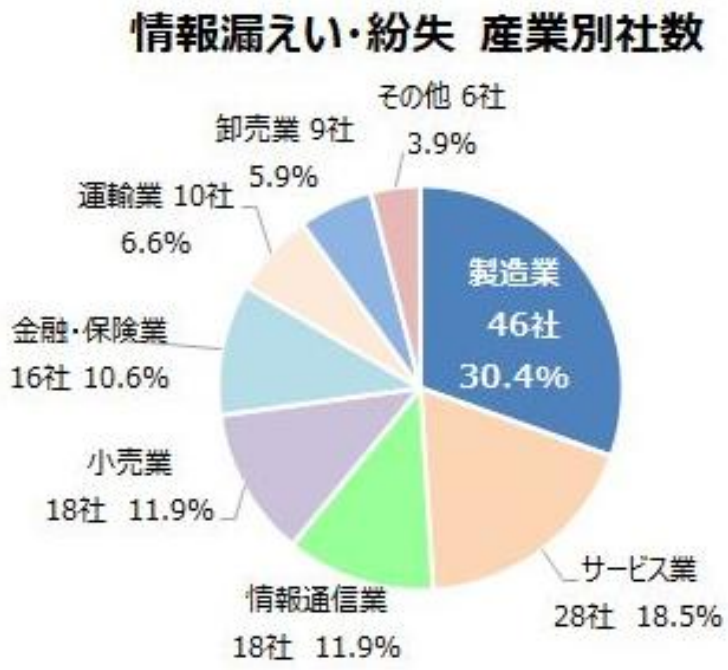
引用元：IPA「企業における営業秘密管理に関する実態調査2024」 20250829

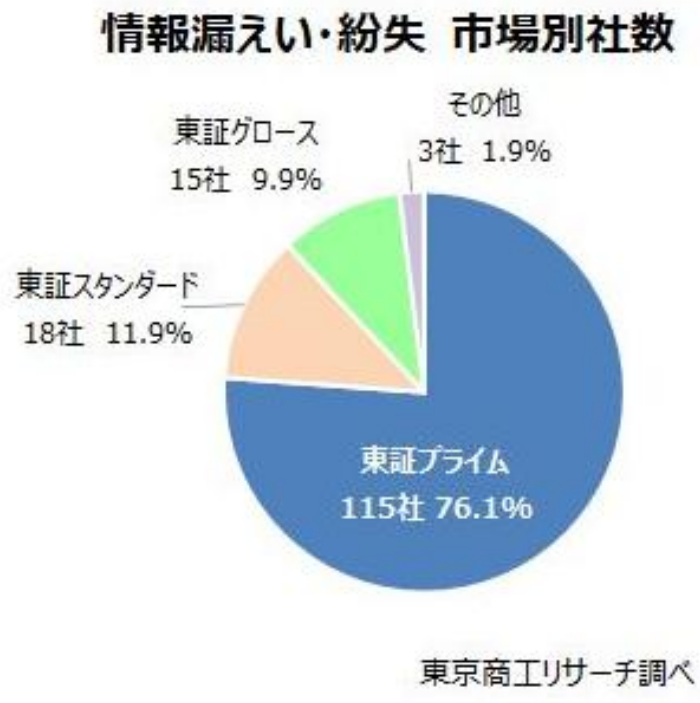
金融機関に関連した内部不正

金融業界の情報漏洩の実態

情報漏洩・紛失事故を公表した企業の中で金融・保険業界は**10.6%**を占めている。

2024年「上場企業の個人情報漏えい・紛失事故」調査





出典：東京商工リサーチ 2024年「上場企業の個人情報漏えい・紛失事故」調査

金融業界の内部不正事例

個人情報を多く扱う金融業界における内部不正は経営リスクとなり得る

発生	企業分類	事象概要
2021年	証券	証券会社の元従業員による顧客情報の不正持ち出し
2024年	生命保険	生命保険会社の従業員による情報持ち出し
2024年	信用金庫	信用金庫の従業員による個人情報漏洩
2025年	銀行	銀行従業員によるメール誤送信での情報漏洩
2026年	生命保険	出向者による代理店情報の持ち出し

実際に起きている内部不正事案

内部不正検知事例①

情報持ち出し

✓ 転職に伴う業務ナレッジの持ち出し

検知内容

検知行動	• 共有フォルダからローカルフォルダへ業務情報の集約 • ファイルの加工 • 個人メールアドレスをBCCに含んだメール送信
分析対象	• メールログ • ファイル操作ログ

対応

対応部門	✓コンプライアンス部門
内容	1. 所属上長への事実確認 2. 本人との面談 3. 社内罰則規定に沿った対応

効果

◆ **営業秘密の流出防止**

◆ **売り上げ毀損リスクの防止**

◆ **企業の信用毀損リスクの防止**

※複数の発生事案を組み合わせた事例となっております。

内部不正検知事例②

情報持ち出し

✓ なりすましによる開発コードの情報持ち出し

検知内容

検知行動	• 情報持ち出し申請の実施 • 通常とは異なるアカウントの挙動（端末/時間帯..etc） • 上長アカウントでログイン • 上長アカウントで情報持ち出し申請の許可
分析対象	• ログオン/ログオフログ • 申請承認ログ

対応

対応部門	✓コンプライアンス部門
内容	1. 上長へのヒアリング 2. 本人との面談 3. 持ち出されたファイルと目的の確認 4. ファイルの回収 5. 社内規定に基づく罰則

効果

◆ セキュリティリスクの増大の防止

◆ 企業の信用毀損リスクの防止

◆ 技術情報の持ち出し防止

※複数の発生事案を組み合わせた事例となっております。

内部不正検知事例③

情報持ち出し

✓ 独立目的での顧客リストの持ち出し防止

検知内容

検知行動	• 独立・企業に関するサイト閲覧 • 名刺情報の一括出力 • 顧客リストデータのコピー • Bluetoothを利用したファイルの転送
分析対象	• Webサイト閲覧ログ • ファイル操作ログ

対応

対応部門	✓情報システム部門
内容	1. 本人へPC持参のもと面談実施 2. 持ち出し先PCでの情報削除と誓約書サイン

効果

◆ **売り上げ毀損リスクの防止**

◆ **営業秘密の流出防止**

※複数の発生事案を組み合わせた事例となっております。

内部不正検知事例④

情報持ち出し

✓ 業務に関係のない興味関心による個人情報の閲覧

検知内容

検知行動	• 普段と異なる（自身の担当ではないと考えられる）顧客情報の閲覧傾向
分析対象	• WEBアクセスログ（アクセス/ダウンロード） • CRM閲覧ログ

対応

対応部門	✓コンプライアンス統括室
内容	1. 本人との面談 2. 閲覧行動の目的ヒアリング 3. 個別注意喚起

効果

◆ セキュリティリスクの増大の防止

◆ 企業の信用毀損リスクの防止

◆ 営業秘密の流出防止

※複数の発生事案を組み合わせた事例となっております。

内部不正検知事例⑤

情報持ち出し

✓ 着服目的での顧客情報の閲覧

検知内容

検知行動	• 前任担当顧客情報の閲覧
分析対象	• CRM閲覧ログ • 顧客別担当者一覧

対応

対応部門	✓コンプライアンス統括室
内容	1. 本人との面談 2. 閲覧行動の目的ヒアリング 3. 個別注意喚起

効果

◆ セキュリティリスクの増大の防止

◆ 企業の信用毀損リスクの防止

◆ 営業秘密の流出防止

※複数の発生事案を組み合わせた事例となっております。

内部不正対策のアプローチと「可視化」のステップ

内部統制におけるログ活用の有効性

内部統制を構成する基本的要素の一つに**「モニタリング」**があり、
有効的に機能しているかを継続的に評価するプロセスが必要となる

1

不正行為の抑止と早期発見
ログが常に記録されているという意識により、内部不正の抑止に繋がる

2

業務の可視化とリスク管理
従業員の業務の実態を把握し、統制の有効性を検証するためのデータとして活用可能となる

3

監査証跡
情報システムの信頼性や安全性、効率性、有効性などが確保されていることを実証する証拠となる

4

セキュリティインシデントへの早期対応
ログを分析することで情報漏洩の有無などを迅速かつ正確に特定し、被害を最小化するために役立つ

内部不正を発見するための主な手法

ルールベース

- 規制・業務ルールが明確である
- 数値や範囲（閾値）で切れる
- 不正のパターンがある程度決まっている

アノマリー

- 行動の個人差が大きく定義しにくい
- 未知の新種の不正への対応が必要
- 白黒つけにくいグレーな行動の検知

対象とする不正の性質に基づき手法を選択。**実際には両方の手法を併用するケースが一般的**です。

ルールベースでの考え方

規制・業務ルールが明確

例 ファイルサーバにある機密フォルダの持出し禁止ルール。ストレージからローカルに移動し、個人メールに送付した挙動。

閾値で切れる

例 大量のファイルコピー。日常業務の数量や容量の一定閾値を超えたコピー操作の捕捉。

パターンがある程度決まっている

例 機密ファイルを個人アドレスへ送付。タイトルなし、CCなし、ファイル名リネーム等の隠蔽パターン。

検知事例：個人情報を出向元環境経由で持出し未遂

※ 本資料に記載内容は実際の顧客情報ではなく、講演目的で再現・加工したものです。
※ 事例は一般的なリスクの一例であり、特定企業・個人を指すものではありません。

メール送信ログ　ファイル操作ログ　従業員所属台帳

脅威シナリオ	個人情報リストをコピー・改名し、出向元企業の自身のメールアドレスに添付送信。 ※出向元企業のセキュリティの甘さを利用し、出向元企業の環境から自身の端末への持出し未遂。
発覚経緯	個人情報リストのコピー・改名・外部送信の一連の行為を検知し、不正送信が判明。

タイムライン	検知行為	検知詳細（検知したログの中身 / 一部抜粋）
8/23 10:42	重要情報の入手 重要情報のファイル入手	【UserId】yamada@sample.com 【コピー元】¥¥svr¥DB¥クライアントフォルダ¥010_台帳一覧¥カスタマー台帳_v3.2.xlsx 【コピー先】C:¥Users¥yamada¥Desktop¥カスタマー台帳_v3.2.xlsx 【イベント種別】FileCopy
8/23 10:55	重要情報の変更 隠ぺい目的でファイル名変更	【UserId】yamada@sample.com 【元ファイル名】カスタマー台帳_v3.2.xlsx 【新ファイル名】report_202508.xlsx 【イベント種別】FileRename
8/23 11:02	不審なメール送信 出向元企業の自身のアドレスへメール送信	【From】yamada@sample.com 【To】yamada@parent-company.co.jp 【Subject】業務情報の定期送付 【添付ファイル】report_202508.xlsx

検知事例：転職先での活用で研究成果を“深夜に撮影”

※ 本資料に記載内容は実際の顧客情報ではなく、講演目的で再現・加工したものです。
※ 事例は一般的なリスクの一例であり、特定企業・個人を指すものではありません。

脅威シナリオ	転職先での活用を狙い、深夜に研究成果ファイルを開き、個人スマホで撮影
発覚経緯	大量コピーと深夜の異常アクセスを検知。内部監査部による本人面談で撮影の事実が判明。

ファイル操作ログ

タイムライン	検知行為	検知詳細
8/6 22:22	他者と異なるコピー 共有フォルダからローカルフォルダへの大量ファイルコピー	【アカウント名】kajita.kohei 【PC名】HOST018AKJ 【コピー元】¥¥svr¥010_技術本部¥研究開発¥次世代材料¥設計図面¥ 【コピー先】C:¥Users¥kajita.kohei¥Desktop¥Backup¥20250715¥ 【ファイル数】182 【イベント種別】FileCopy
8/6 22:28 ～ 8/16 23:12	普段と異なる参照 深夜帯に普段アクセスしないファイルの参照	【アカウント名】kajita.kohei 【PC名】HOST018AKJ 【ファイルパス】C:¥Users¥kajita.kohei¥Desktop¥Backup¥20250715¥試験結果¥report_202506_final.xlsx 【イベント種別】FileAccess 【アカウント名】kajita.kohei 【PC名】HOST018AKJ 【ファイルパス】C:¥Users¥kajita.kohei¥Desktop¥Backup¥20250715¥設計図面¥prototype_v3.dwg 【イベント種別】FileAccess

アノマリーの考え方

グレーな行動

例 担当外顧客への継続的かつ執拗なアプローチ（閲覧等）など、着服等の予兆行動。

個人差が大きい行動

例 夜間作業（通常勤務外の時間帯）でのアクセスなど一律の閾値設定が困難な挙動。

新種の不正

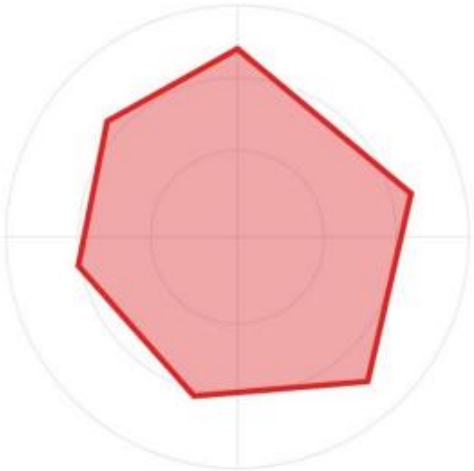
例 シャドーITやAI（他者が利用していないSaaS）の利用など未定義の不正形態。

アノマリーを活用した着服防止策

STEP 01 行動異常の抽出

- 担当外顧客への継続アクセス
- CRM入力の常態的な遅延
- 入力内容の不整合・矛盾
- 統計上の少数行動（異常値）
- 長期的・継続的な特異性
- 過去事例に見られる行動ログ

STEP 02 リスクの可視化



不信行動の重複を検知

単一の事象ではなく、複数の異常が
重なった人物を「高リスク」として抽出

STEP 03 文脈の精査・警戒

業務的妥当性の検証

検知された行動が引継ぎ等の「正当な理由」に基づくものか、行動ログから確認。

論理的整合性の確認

CRMの記録と実際の行動に、説明不可能な時間的・内容的な乖離がないか精査。

警戒レベルの引き上げ

合理的理由が欠如し、反復性がある場合は「着服の予兆」として個別調査を実施。

“兆候に気づき、先手を打つ”内部脅威対策へ

リスクに対して先手を打つ

- ✓ すべての操作を制御で封じ込めるのは、業務効率や現実性の観点から限界がある
- ✓ 内部起因の情報漏洩の多くには、“静かに進行する予兆”が存在している
- ✓ 性善説に頼るのではなく、兆候を早期に可視化し、先手を打つ体制が重要

見逃さない仕組みの条件

- ✓ 点在するログをシステムをまたいで横断的に把握できること
- ✓ 個別の異常値ではなく、“いつもと違う振る舞い”としてリスク検知できること
- ✓ 定期的な振り返りで傾向の変化に気づける運用体制があること

目指すべき姿

- ✓ 不正の兆しが、ログから“見える化”される
- ✓ 兆候を起点に、対策が“前倒し”で実行される
- ✓ 検知→対応→評価→改善が循環し、“見て終わらない”運用が根付く

内部不正防止の基本原則

・犯行を難しくする

・捕まるリスクを高める

・犯行の見返りを減らす

・犯行の誘因を減らす

・犯罪の弁明をさせない

内部不正を防ぐための管理方法

■ログの記録と保存

4-5.原因究明と証拠確保

（１８）情報システムにおけるログ・証跡[71]の記録と保存

内部不正の早期発見及び（３０）の事後対策の影響範囲の観点から、重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定めた期間に安全に保存することが望ましい。

■ログの分析（モニタリング）

4-4.技術・運用管理

（１２）内部不正モニタリングシステムの適用

AI 等の最新技術を組み入れた内部不正モニタリングシステムは、監視機能の有効性だけではなく、役職員保護のための適切な設定ができるものを選定し、人手による判断と組み合わせる等により説明責任を果たすことができる方法で運用しなければならない。

出展：独立行政法人情報処理推進機構（IPA）「組織における内部不正防止ガイドライン　第5版」

運用を行う上での配慮

内部不正で配慮が必要な主なポイント

1. 不正の主体は原則特定されている（不特定ではない）
2. 無自覚による不正行為の存在の認知
3. 組織や集団によってルールや慣習が異なり不正の判断基準が変わる
4. AIなどを分析に活用する場合は判断プロセスが理解可能である必要がある
5. 可能性として外部からの不正アクセスが考えられる
6. 行動プロセスの確認によって信頼すべきかどうかを判断する

1.外部脅威と異なり不正の主体は原則特定されている（不特定多数ではない）

内部脅威は不正を行う主体が限定的であるため特定可能
対象が限定されているため相応の配慮が必要

	外部脅威	内部脅威
関連情報	● 多い　研究機関やベンダーが多く集合知を活用しやすい	● 少ない　参考情報が少ない
脅威の変化	● 常に新たな脅威が発生	● 組織の事情や運用状況によって脅威が変化
攻撃主体	● 不特定の組織や人物で限定できていない	● 特定されており限定的

2.無自覚による不正行為の存在の認知

ルールそのものの認識不足による意図しない不正
ソーシャルエンジニアリングなどによる無自覚による詐欺行為の被害の認知

ルール周知

・ルール変更および周知の際、従業員に認知させることは容易ではない

運用の開始

・ルールが正しく運用されているかの確認自体が難しい

意図しないルール逸脱

・ルールの認知が十分でないため意図しないルール逸脱の可能性

3.構成する組織や集団によってルールや慣習が異なり不正の判断基準が異なる

不正であるかどうかの判断基準は組織構成やルールなどによって異なる
外部からジョインした人にとっては以前の慣習が不正となる場合もある

組織の構成やルールによって
不正の判断基準が変わる

具体的な行動内容を
基準に定性的に判断

4.分析にAIなどのテクノロジーを活用する場合は判断プロセスが理解可能である必要がある

不正の疑いが生じた場合、それが客観的に説明が可能な状態の必要がある
AIを活用する場合、行動の外れ値としての異常でフィルタリングなどは可能
ディープラーニングやニューラルを用いるなどで、なぜ不正であるかの合理的な説明ができないような判断はしない

具体的な調査および証跡の確認

不正の疑いのある事象に
関連する行動と証跡を
ログなどで収集

具体的に証跡を集め不正と判断される
根拠が客観的に説明できる状態にする

5.可能性として外部からの不正アクセスが考えられる

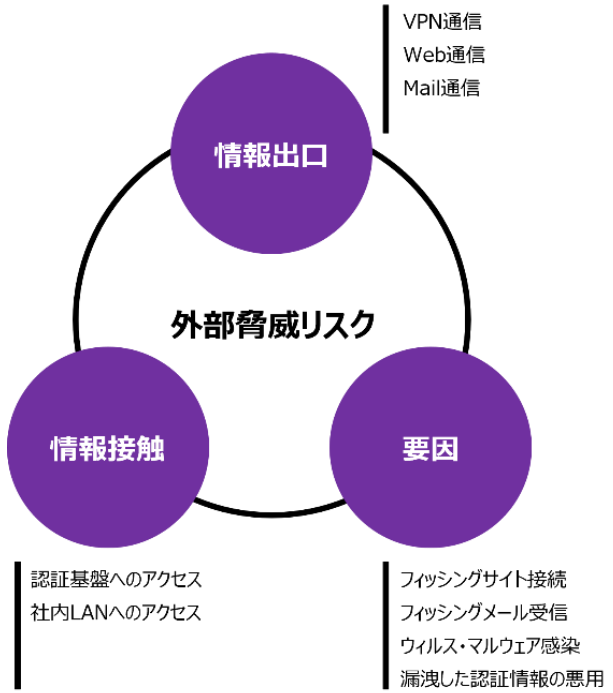
外部脅威からの内部侵入の不正アクセスの可能性が考えられるため、例外の想定をする

認証基盤への不正アクセス

普段と異なる特権アカウントが利用された端末を特定
複数ロケーションからの認証成功事象の発生
通常利用以外のアカウントによる認証成功端末の特定
無効アカウントによる認証基盤へのアクセス試行

VPNへの不正アクセス

複数同時接続が発生しているアカウントのの特定



ご清聴ありがとうございました。

株式会社エルテス
営業本部　IRIセールス部
Tel　　：03-6550-9281
E-mail：iri-sales@eltes.co.jp