インシデント発生時の現場の実態と対応の勘所
～人的リスクと不正の兆候～

株式会社エス・ピー・ネットワーク

本日の内容

■ 情報漏えい・流出事故対応の要領と勘所
～事故対応の現場で起こっていること～

■内部不正の兆候と対応事例
～入退室ログと映像データの解析について～

■ 会社概要

社　　名	株式会社エス・ピー・ネットワーク
本　　社	〒167-0043　東京都杉並区上荻1丁目2番1号　インテグラルタワー TEL：03-6891-5556（代） FAX：03-6891-5570
創　　業	平成8年3月18日（設立：平成元年12月1日）
資　本　金	3億1625万円
従 業 員 数	約320名
取 引 銀 行	三井住友銀行　みずほ銀行　三菱東京UFJ銀行　りそな銀行
許　　可	一般労働者派遣業　般13-08-0452号
認　　定	警備業　東京都公安委員会　第30002092号
届　　出	探偵業　東京都公安委員会　第30100276号
支　　社	大阪支社　福岡支社　名古屋支社
営　業　所	札幌営業所　広島営業所　仙台営業所

主な特長

- （1）警視庁・道府県警の出身者をはじめ、法務・労務・財務・広報等の専門家で構成。
- （2）“発生した危機への対応（クライシスマネジメント）”と“危機の発生防止（リスクマネジメント）”の両面について、コンサルティングと人的支援を展開。
- （3）企業での事件・事故、不祥事発生時に伴う緊急事態対策支援を数多く手がける。
- （4）反社会的勢力リスク対策について、パイオニア的な存在。
- （5）多店舗展開する BtoC 企業の現場（店舗）におけるクレーム、不当要求、不審者・不良客、反社会的勢力対応（対策）の実務支援に膨大な実績を有する。

SPNサポート体制

緊急事態対応

各種資料・報告書作成
・ポジションペーパーの作成と更新管理
・プレスリリース（適時開示資料）
・謹告（新聞社告）の作成支援
・行政等への報告書等の作成支援
・お客様への報告書・説明文書
・謝罪文書作成

記者会見・問い合わせ対応支援
・記者会見運営支援
・問い合わせに対する想定問答集案の作成
・コールセンター運営支援
・クレーム対応等に対する研修・レクチャー

その他対応支援
・被害者対応、行政対応、マスコミ対応、保護者など 全てのステークホルダーへの対応を支援
・原因究明のための各種調査の支援
・対応方針決定会議への参画
・調査のための社内委員会への参画
・関係者ヒアリング等の調査サポート（外部監査）
・再発防止を含む危機管理体制の構築支援
・警察捜査への協力支援
・業務妨害・不当要求対応支援
・身辺警護/施設警備
・（探偵業法に基づく）行動調査
・再発防止に向けた社内研修の実施

プロフィール

講師

高森　一誓　Kazuchika　TAKAMORI　（総合研究室担当　執行役員）

特定社会保険労務士（東京都社会保険労務士会会員）、公認不正検査士（CFE・日本公認不正検査士協会会員・東京不正検査研究会会員）。1999年、株式会社エス・ピー・ネットワーク入社。コンサルティング部長、管理担当執行役員等を歴任、コンサルタント視点と内部管理当事者視点の両面を兼ね備えた講演・コンサルティングを持ち味に、労務管理分野のほか緊急事態対策、情報管理、内部統制全般の領域で活動。2017年より総合研究室担当執行役員。2014年、事業構想大学院大学にて新規事業構想におけるリスクマネジメントのあり方を研究・修了（事業構想修士）。

佐藤　栄俊　Eishun SATO　（総合研究室　上級研究員）

関西大学大学院 総合情報研究科 社会情報学専攻 修了。
エス・ピー・ネットワーク入社後、情報システム管理部門を経て、現在、総合研究室にて主に各企業の情報管理体制構築支援、情報漏えい事案等に従事。また、立教大学大学院にて、企業における不正、人的脅威、ヒューマンエラーについて、総合的実践的危機管理の研究後修了。危機管理広報等のクライシス対応支援からコンプライアンス・内部統制支援、苦情対応マネジメント体制構築、危機管理マニュアル作成まで幅広く手掛ける。

山岡　渉　Sho YAMAOKA　（総合研究室　研究員）

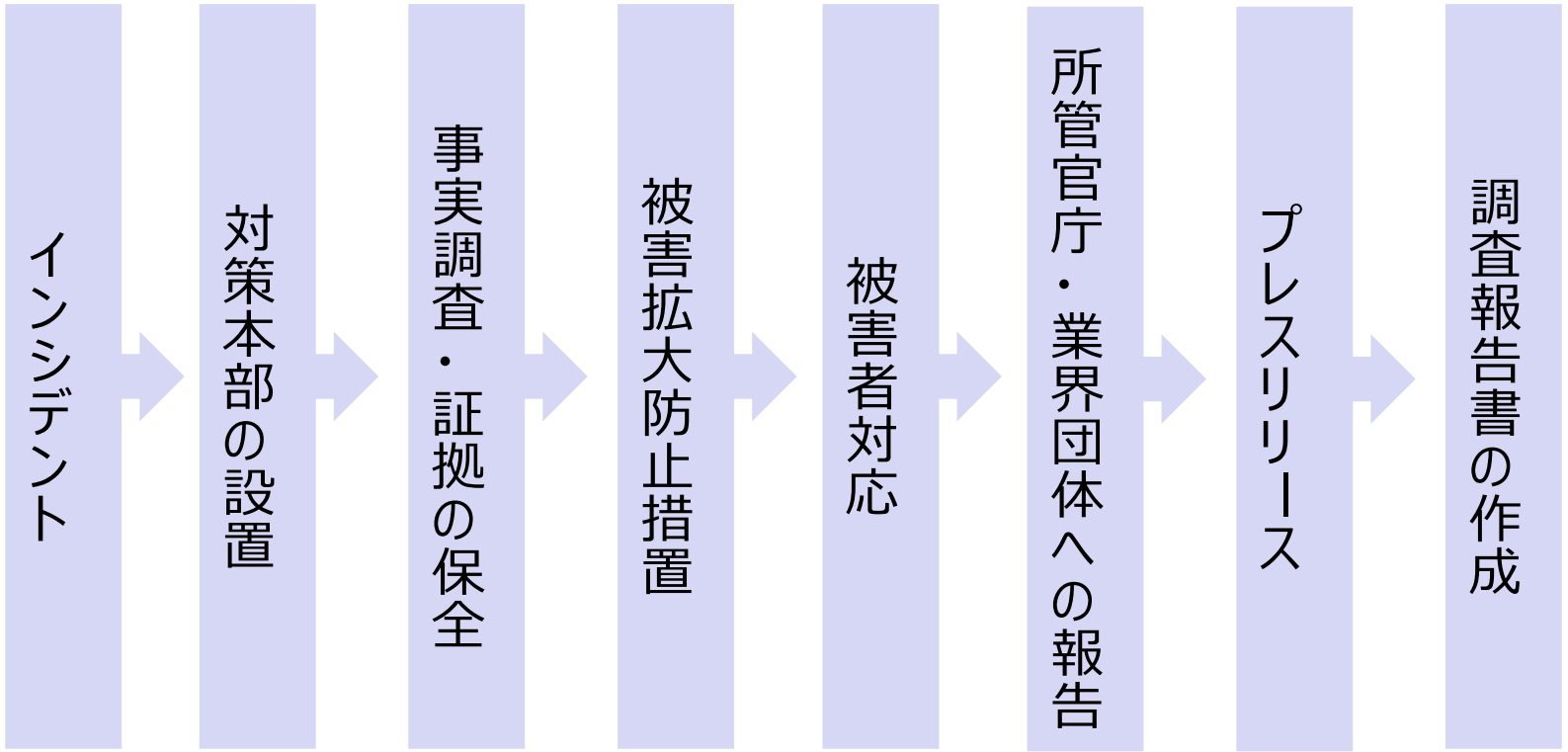
法政大学 国際文化学部卒。ソフトウェア開発会社を経てエス・ピー・ネットワーク入社。セキュリティインシデントにおける緊急対応支援のほか、反社会的勢力や不当要求・不良顧客の対応支援、防災監査、防犯コンサルティング、企業調査、要人警護など幅ひろい業務にあたる。当社サイト連載『企業におけるIoTリスクを考える』などを担当。趣味は美術と格闘技。

情報漏えい・流出事故対応の要領と勘所
～事故対応の現場で起こっていること～

1. 扱う事案の種類と頻度

原因	頻度	例示
管理ミス	多い	情報管理ルールの未設定及び、周知不足。遵守事項の無知、無理解による持ち出し、禁止事項の逸脱、業務上の都合など。 例：自宅への端末の持ち出し、私用端末の使用による紛失、盗難、ウィルス感染など。
誤操作	多い	ボタンの押し間違い、メール・FAX誤送信、書類誤配送、書類誤廃棄、
紛失・置き忘れ	普通	電車、飲食店での紛失、置き忘れ。
盗難	少ない	車上荒らし、事務所荒らし、空き巣などによる被害。
内部犯罪・不正	実態は不明	内部関係者による意図的な持ち出し、消失、名簿売却など。（公表義務を帯びる個人情報漏えいを除けば、ほとんど公表されず）
設定ミス	少ない	Webサイト、クラウド利用時の設定ミスによる、情報の誤開示など。
不正アクセス（サイバー攻撃）	多い	ECサイト、Webサイトへ攻撃、標的型メールによる、機密情報、顧客情報、技術情報などの漏えい。
委託先管理体制の不備	多い	委託先情報管理体制の不備と問題の放置、把握していないことによる事故。 例：脆弱性対策の未実施、誤廃棄、持ち出し、紛失

2. 事故対応の主な流れ



3. 対策本部の設置

実際は機能しないことがほとんど！？

	統括	情報システム	法務/人事	クレーム対応/広報
タスク	対策本部の統括・意思決定	情報流出経路の特定	民事責任の追及、刑事告訴	クレーム対応/プレスリリース、記者会見
内部者	社長・CIO等	情報システム部	法務部/人事部	カスタマーセンター/広報部
外部専門家	外部弁護士/危機管理会社	フォレンジック調査会社	外部弁護士	PR会社/外部弁護士/危機管理会社

※ 外部専門家との間で共有すべき事項

□ 事故を認知した端緒（いつ、誰から、どのような方法で事故を知ったのか）
□ どのような情報が漏えいしたのか（自己の情報か第三者の情報か、情報の内容・範囲・媒体・形式（データ、紙））
□ 情報の管理状況（電子データとしてサーバに存在するのみか、紙媒体としても存在するか、複製物はあるか、保管場所、保管方法、アクセス権者・管理者のリスト）
□ 関係社内組織図
□ 秘密保持、秘密管理に関する社内規定

対応事案からみる問題点①

委託先、派遣社員の第三者からの情報流出

当日の投影のみといたします

対応事案からみる問題点②

不正アクセスによる情報漏えい

当日の投影のみといたします

4. 対応に苦慮する点

・事故時の対応要員が少ない（いない）。

・フォレンジック調査を実施しても、対象範囲がわからないことがほとんど。
※ 結果、最大数を見積もった対応をせざるを得ない。

・フォレンジック調査会社の調査や分析に時間がかかる。（人がいない）
※ 結果、リリースが大幅に遅れる。

・自発的に被害に気づくことはほぼない。
※ 実際に攻撃を受けたのは半年～数年前でも、二次被害が発生するまで発覚しなかった。
※ 情報を発見した第三者、専門機関、カード会社からの通報などで発覚。

・関係各所（行政、カード会社各社、取引先、顧客など）との調整に疲弊する。
（板ばさみ状態）

・「あわよくば無かったことにしたい」ということにもなる。
※二次被害が発生していなければ、問題ないという経営方針になることも。

5. 事故対応要領

発生事実の把握とリスク分析

【主な推進事項】

- 事案の事実関係・被害状況の把握
- 自社における過去の不祥事との関連性や影響度の把握
- 被害（影響）拡大可能性の分析／不確実性の把握
- 法的課題の抽出と分析
- マスコミの関心度分析／インターネット風評のモニタリング
- 経営への影響度分析（業績・株価・関連会社の事業活動等）

5. 事故対応要領

マスターシート（全利害関係者一覧表）の作成

- 利害関係者対応
- 対応状況の進捗管理
- 行政機関への報告
- 社内関係者への報告

コールセンター運営体制の整備（※重要）

- 受付時間の設定
- 回答範囲の設定
- 人員の確保／専門業者委託を検討
- コールスクリプトの作成
- 不当要求・嫌がらせ対応
- エスカレーションルールの策定
- FAQ（よくある質問）の作成
- 対応結果記録表（手書き→集計）

6. 事故対応の特性

情報漏えい事故発生の特性と業務への影響

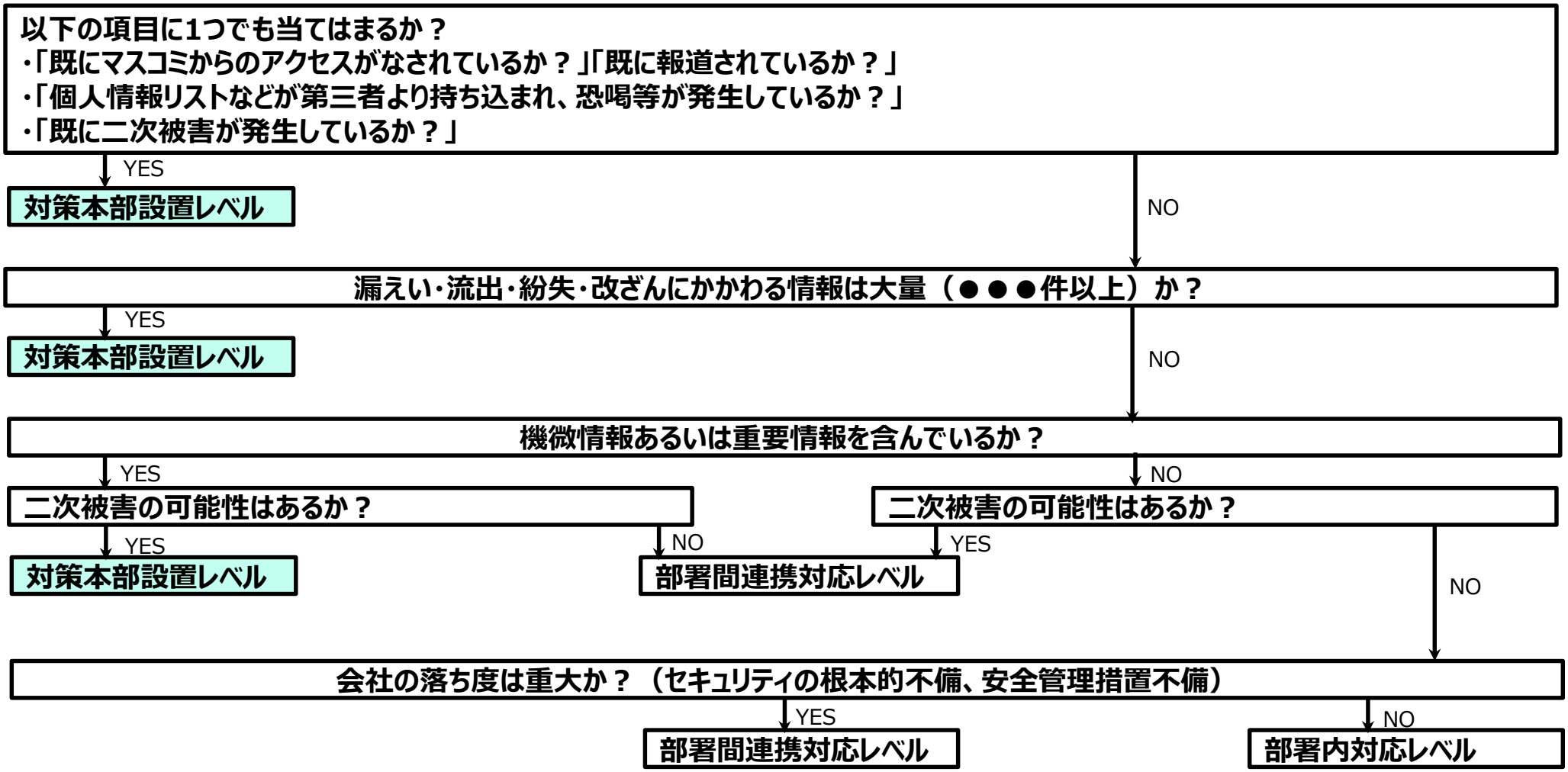
「情報」の特性→想像以上に対応長期化

1．複製容易で何度使っても消えない/持ち出されても気づきにくい
2．インターネット上に一度漏えいした情報は、消去困難と心得る
3．迷惑メールに関するクレームや精神的苦痛に対するクレームが多く、
　情報漏えいとの直接的因果関係の証明は極めて困難
4．情報の価値は、情報利用者が決めるため、どのような形で悪用されるかは分かりにくい

クレームへの対応→想像以上に大変

1．補償に関する内容や、漏えいした情報の悪用への不安から、具体的にどのような対応をするのかというような苦情クレームが続く。2時間以上対応に要する場合もある。
2．情報には色がなく紐もついていないため、回収は困難で、流出ルートの特定や拡散防止も難しい。また、具体的な解決策の提示もむずかしい。
3．便乗して種々の不当要求をしてくる顧客も少なくない。

7. 事故対応のレベル判定



8. 事故対応の要点

①対策費用がかかることを認識する
※郵送代81円×件数、コールセンター300万～、PC等の調査200万～、残業代・休日出勤費用（諸経費）

②たかが「個人情報」とは考えない（正しいリスクの認識）

③全体を俯瞰・統括できる権限者（部署）が指揮を執る（「木を見て森を見ず」を回避）

④リアルタイムの再発防止策をとる～2次被害発生、被害拡大防止⇒「公表」も視野に
※第二、第三の流出（攻撃）は絶対に防ぐ。対象のシステムやサービスは一旦止めるのが望ましい。

⑤漏えいの規模数や、機微性、複雑性を鑑み、外部専門機関（コールセンターや各種調査機関（フォレンジック調査、ITセキュリティ企業等）や効果的なツール・媒体を最大限活用する

⑥記録、証拠を残す（ドキュメント、検討資料、議事録、メール）⇒情報の更新を怠らない

⑦「情報」を適切に開示して、説明責任を果たす

9. 事故対応の要点

■ 危機事態への対応

・隠蔽は通用しないと心得る（隠蔽したとしても内部通報やSNSから事案が発覚する可能性大）

・基本的にはお詫び状の送付が望ましい

→可能であれば、訪問対応（電話での第一報・アポ→訪問謝罪→継続的報告・対応：電話・メール・手紙等）
→金券や粗品その他の金品提供は基本的にさけるべき※但し、ケースバイケース
→金品提供は出しても出さなくても結局クレームが来る（対応負担は変わらず費用はかかる）

・どのような事案であっても、被害者や保護者からのクレームに発展する可能性大

→通常のクレームはコールセンターで対応し、紛糾した案件や不当要求は個別で対応（外部専門要員による支援もふくむ）
→悪質なクレーマーへの対応やメールでの問い合わせ・クレームへの対応は慎重さが必要
Q 今回の漏えい事案によって自分が被害を受けた場合、賠償してくれるのか？
Q 精神的苦痛に対して補償しろ！
Q 今回の個人情報の漏えいが、詐欺・脅迫・恐喝・暴力事件等に結びついたらどうするのか？
Q 責任者と代われ！
Q 家までお詫びに来い！

■ 再発防止策の策定→社会からの信頼回復

・内部統制上の事案発生原因の検証

→仕組み（体制＋ルール＋方針＋教育研修体制）と
→運用（マネジメント＋運用環境＋日々の記録やモニタリング・牽制体制）、
→意識（社員・管理職）を分析・検討

10. 情報漏えいにかかる人的リスクと対策案

情報の流出経路

■ 自社従業員（内部者）による流出
・メール誤送信やPCの置き忘れ、私用端末の利用による流出
・金銭目的での競合他社への情報の売り渡し

■ 提携取引先（関係者）からの流出
・取引先企業の情報管理体制の不備
・意図的な秘密保持契約の違反

■ 外部からの侵入（第三者）による流出
・外部者からの情報システムへの不正アクセス
・事務所内への侵入による情報の持ち出し

10. 情報漏えいにかかる人的リスクと対策案

不正の動機や正当化

- 金銭の困窮や評価
- 職場環境への不満
- 経営への不満
- 納得のいかない解雇や評価
- 上司・会社への恨み
- 会社のため、顧客のため

＜参考＞不正の兆候

■ 組織内の不正リスク環境

- 従業員の離職率が高い
- 従業員の欠勤率が高い
- 遠隔地業務の脆弱な管理
- システム変更、業務手続変更、権限の付与方針が不明確
- 不明確な権限委譲
- 内部/外部監査における指摘事項への対応遅延
- 承認業務の実質形骸化
- 従業員が特定の業務を長期間担当している
- 特定の従業員の業務量が過大になっている
- 人事評価に毎回納得しておらず、不満がある
- 仕事の悩みを誰にも相談しない、孤立している
- 単独作業が多い

■ 個人的状況

- 管理者の部下への無関心
- 常識的なルールや手続きの拒絶
- 取引先、顧客等からの頻繁な苦情
- 些末な事故を繰り返す

＜プライベート面＞

- ギャンブル依存症
- 過度な飲酒や薬物使用の可能性
- 経済的な困窮
- 収入以上の華美な生活習慣
- 同僚、取引先からの金銭の借入

10. 情報漏えいにかかる人的リスクと対策案

限界を認識する

- アクセス権限者等の内部者がこのような対策を意図的に回避して行う不正をシステムによって完全に防ぐことは不可能であることを認識する（内部統制、情報システムとの関係でいえばIT統制の限界論の議論）

痕跡を残す

- 社内システムの操作ログが残る環境を構築することで、不正の兆候としての故意の行動の痕跡を早期に発見して被害を最小限に食い止める。

人による牽制

- 情報システムのみではなく痕跡を残したり、端緒を発見しやすい対策
  （監視カメラ、入退室管理システム、管理者同士の相互監視、上司・役員による監視等の二重、三重の対策を実施して、不正に対するけん制機能・抑止力を強化する）

10. 情報漏えいにかかる人的リスクと対策案

(1) 不正予防策の増強（物理的にできない）

(2) 発覚リスクの増強（やると見つかる）

(3) 見返りの抑制（割に合わない）

(4) 誘因・挑発の排除（その気にさせない）

(5) 弁解余地の排除（言い訳を許さない）

10. 情報漏えいにかかる人的リスクと対策案

予防策の増強 （物理的にできない）	発覚リスクの増強 （やると見つかる）	見返りの抑制 （割に合わない）	誘因・挑発の排除 （その気にさせない）	弁解余地の排除 （言い訳を許さない）
不正対象物の強化	防犯意識の向上	対象の隠蔽	欲求不満の削減	規則の設定
・収納、施錠徹底 ・保管庫・金庫の導入 ・スクリーンロックの設定 ・PCの物理的ロック	・ID証装着例高・声かけ徹底 ・貸出管理実施（ログ記録） ・インシデントの迅速報告徹底 ・防犯意識向上の啓発活動実施	・現金、貴重品、情報の扱者限定 ・存在情報の限定提供 ・組織の融通性との河南 ・情報提供、秘匿ポリシー策定	・良好な職場内コミュニケーション確保 ・面接、コーチングの実施 ・従業員の経済状況把握と支援 ・生活習慣の把握と対応	・社会正義優先原理の宣言 ・誓約書の回収 ・社内規定の繰返し指導、確認 ・規定の定期見直し・修正
出入でのコントロール	自然監視確保	対象の排除	対立の回避	指示サインの掲示
・入室管理の実施 ・「資格と必要性」の確認 ・入室ログ取得と管理 ・カギとIDカードの認証強化	・死角排除による視認性確保 ・遮蔽物の整理、レイアウト工夫 ・PCディスプレイ視認性確保 ・時間的死角排除	・不要在庫、備品の適正処分、管理 ・不要情報の確実な消去、廃棄 ・処分、廃棄の確認（監査）	・配属先配慮などの人事実施 ・「組織的存在意義」の醸成 ・組織内派閥の解消 ・適材適所人事の徹底	・諸室での制限事項等の明示 ・資料への社外秘等サイン明示 ・組織規程集の配布 ・社内ネットでの規定公開
出口での検査	匿名性の排除	所有者の特定	感情のコントロール	良心への働きかけ
・退出管理の実施（ログ記録） ・電子タグ等による持出し管理 ・所持品検査（監査）の実施	・ID証装着の徹底 ・出入、行動ログ取得/管理 ・プリントアウト/情報アクセスログ	・物へのID付与 ・情報へのID付与と変更禁止処理 ・在庫、備品の付番管理徹底 ・漏洩情報の特定技術導入	・従業員の不平不満への対応 ・定期的面接の実施 ・ハラスメントの発見と対応 ・透明性、納得感のある人事/処遇	・良心に働きかける標語の設定 ・掲示や配布による標語の周知 ・標語の浸透促進 ・組織から従業員への「信頼」表明
接近性の抑制	管理者の活用	転売市場への介入	周囲からの圧力を緩和	ルール遵守への支援
・重要エリアへの出入限定 ・重要情報のアクセス制限 ・現金・貴重品取扱機会の低減 ・持ち出し容易性の制御	・明示的「監視」の実施 ・管理者の意識付け ・従業員の意識醸成 ・組織文化醸成、指導、是正実施	・オークション情報チェック ・ネット裏情報チェック ・ポリシー宣言と迅速届出/法的対応 ・情報公表と情報収集窓口設定	・悪しき組織員周の撤廃 ・外の眼導入（組織改革/異動等） ・組織トップの明確な意思表示 ・従業員啓発による組織文化刷新	・運用実態にあったルール制定 ・違反不能な仕組み導入 ・ルールの啓発 ・違反ペナルティ制定、運用徹底
道具や対抗手段のコントロール	組織による系統的モニタリング	対象の低価値化	模範犯罪の阻止	薬物、アルコールへの対応
・携帯電話・スマホ・PC・記憶媒体制限 ・コピー、FAX、プリンタ管理実施 ・メール管理、アップロード管理	・総合的内部統制担当部署設置 ・独立した内部情報収集窓口設置 ・システムによるチェック、監査実現 ・定期不定期監査の並行実施	・盗品の流通性低減手段導入 ・情報暗号化/時限管理 ・線引き小切手利用 ・盗品の製品番号公開と届出	・小さな不正を糺す姿勢維持 ・信賞必罰の徹底 ・事件発生時の顛末公表 ・新規類似対応ポリシー公表	・生活習慣改善の支援 ・外部専門家相談ルート提供 ・解決不能時対応手段

内部不正の兆候と対応事例
～証拠保全のための入退室ログと映像データの解析について～

1. 某遊技場における内部不正事例から

代表的な事例

当日の投影のみといたします

1. 某遊技場における内部不正事例から

代表的な事例

当日の投影のみといたします

2. 不正発生の背景

「不正のトライアングル」による整理

当日の投影のみといたします

3. 制度・風土面からの不正対策

今後求められる不正対策

（1）不正増加の方向性
① （雇用条件が高まらない場合には）従業員の不満の増大
② 労働力不足による採用水準の低下
③ 転売等の容易化
④ 不正な情報交換の活性化
⑤ これらの条件悪化に対応する管理者・管理能力の不足

（2）技術的対策を補う不正対策の必要性
① 「不正撲滅」に向けた経営方針
② 不正発見機能の強化
・内部監査機能の充実
・内部通報制度の活性化、アンケート手法等の複数チャネル整備
・退職者ヒアリング等、現場に即した情報の収集
③不正を許さない制度の整備と徹底
・懲戒制度の再点検
・懲戒処分の公表制度による周知
・弁済の徹底（身元保証制度も再確認）
・刑事事件化

4. 不正行為の抑止における出入管理とカメラ監視

(1) 本パートのスコープ

機密性が求められる場所における不正行為・犯罪を抑止するための出入管理とカメラ監視を考える

(2) 不正をめぐる理論の変遷：原因論から機会論へ

- **原因論**　　不正行為における内的な必然を除去しようとする
  例：性格が悪いし怠け者だから不正をおかす

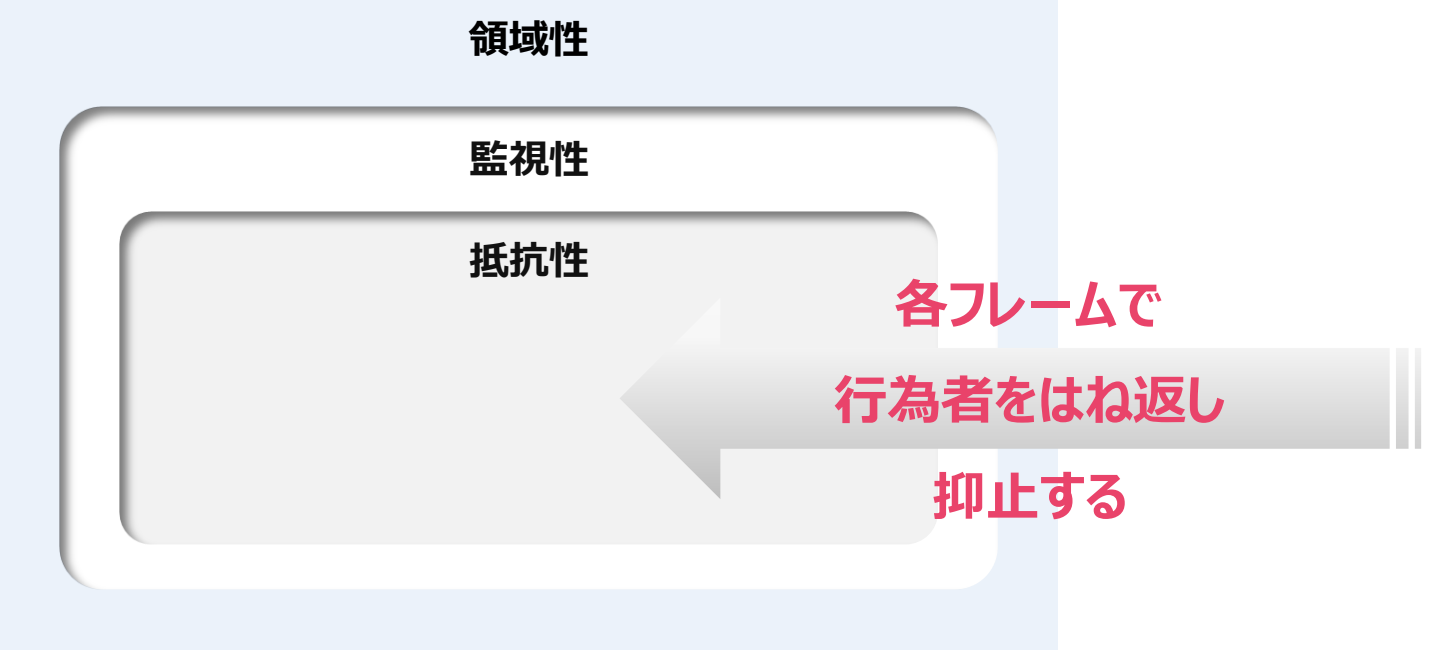
- **機会論**　　不正者は内的な必然に乏しくても
  不正をはたらける機会があれば「やってしまう」

⇒不正をはたらける**機会が生じないような働きかけ**が重要

(3) 機会論における抑止のフレームワーク（参考）

① **領域性**　：接近させない
② **監視性**　：だれかに見られている
③ **抵抗性**　：その行為の対象者（ヒト）からの抵抗

※ プレモダンだが普遍性あり。



(4) 状況的犯罪防止論（コーニッシュとクラーク、2003年）

- 初期犯罪学「合理的選択理論」（1986年）からの到達点
- ５つの類型からの犯罪を抑止
  - ① **予防策の増強**　：物理的な困難を設ける
  - ② **発覚リスクの増強**　：やると見つかる
  - ③ **見返りの抑制**　：見返りが割に合わない
  - ④ **誘因・挑発の減少**　：その気にさせない
  - ⑤ **弁解余地の排除**　：言い訳をさせない

※24ページ図表参照

これらの「**状況**」への介入によって、不正の抑止と検証を可能とする

- リアル　（本パートのスコープ、**主に①と②に作用**）
- バーチャル　（システムセキュリティ施策、不正抑止施策など）

(5) 前項①②にかかるおもな実効策

① 予防策の増強

- **出入でのコントロール入退管理**
- 対象物の強化
- 道具のコントロール　　…など

② 発覚リスクの増強

- **カメラ監視**
- 自然監視性の向上
- 物理的な侵入検知　　…など

フィジカルへの関与が強く
情報セキュリティ施策単独では
制御が困難

※24ページ図表参照

(6) 出入管理の要諦

＜目的＞　特定の域内への、不審なヒト・モノの出入を防止する
＝行為者の権限が及ぶエリアの確定

＜実務＞　「資格と必要性」を確認・記録する

(1)　**資格**　　域内に立ち入る権限を有しているかどうか

(2)　**必要性**　立ち入る必然性があるかどうか

⇒ これら２つの要件を満たさない場合は「不審」とみなす

＜手法＞　(1) ヒトの出入

資格と領域の設定、確認、記録

(2) モノの出入

モノを都度確認し、都度資格を設定、確認、記録

(7) ヒトの出入管理フロー

① 個人証明書の発行

その従業員の基本情報だけでなく、発行資格にかかるデータなども確認できることが望ましい

② セグメント証明書の発行

すべての従業員における証明書チェックが困難な場合は、社員章や職階バッジなどで代用できなくもない

③ 一時入場者への資格付与と記録

いわゆる「部外者」は警戒すべき対象として、入退の日時・目的などを厳格に確認・記録し、臨時資格を標示させ、従業員からの自然監視をうながすのが望ましい

(8) モノの出入管理フロー

① 帳票との照合と記録

送り状や伝票類などとの照合、その過程の記録

② 所持品の精査と記録（＝持ち物検査）

入退における手持ち品だけでなく所持品の精査と記録

③ モノの「出(デ)」の精査

商品、備品など〝持ち出すこと〟は妥当性か、不審点はないか

④ モノの「入(イリ)」の精査

商品、備品など〝持ちこむこと〟は妥当か、不審点はないか

(9) 情報インシデントに際しての出入管理上のリスク（一例）

<ヒトのリスク>

- 入居ビル、入居フロア、執務室への部外者の立ち入り
- 「必要性がないタイミング」における従業員の立ち入り
- 「必要性がないエリア」への従業員の立ち入り

<モノのリスク>

- 害悪を及ぼすモノの持ち込み

例：劇物、法定危険物、盗聴・盗撮器具、キーロガーなど

- 機密性を帯びたモノの持ち出し

(10) カメラ監視の要諦

＜目的＞

① 記録（ →認識・検査）

② 監視（ →認識・検査）

※ 主体はヒトか機械か

※ 対象は従業員か外部か

＜昨今の潮流＞

- カメラのネットワーク化・IoT化が進行
- 録画機器（カメラコントローラ）のサービス化
- 機械検知の精度向上

(11) カメラ監視の要諦

◆ システムに傾斜した情報セキュリティ施策を補完する

- 一般的なパソコンの画面記録サービス、キーロガーなどでは、不正行為者のフィジカルまでは追えない
- 移動と行為のログ（**＝視覚情報・音声情報の優位性**）
- 公判維持の観点からも、行為者を特定するために有用
  - こんにちのサイバーセキュリティ情勢下においては
    行為者の特定は電子的な証跡だけでは特定できない
    （例）アカウントなりすまし、Bluetooth乗っ取りなど
- 電子的な証跡と組み合わせることで、不正・不審の端緒をつかむきっかけとなる

(12) 情報管理インシデントにおけるカメラ監視の有用性

◆不正な立ち入りの検知

- 出入管理で検知できなかった「資格のない者」「必要性のない者」は侵入していないか
- 様相や歩容に不審点はないか、
- 不審な用具を持ちこみ/持ちだしていないか
- 退出後に不審な地点での滞留はないか

◆不審な挙動の検知

- 不必要な領域に侵入していないか
- 業務用具に不審な触れ方をしていないか（時間、様相）
- 通常とは異なる挙動はないか（ふるまい）

(13) 挙動の「不審」とはなにか

◆ 異常値のしきい値を超えるかどうか

＜例＞

- 着衣・歩容・手荷物に調和の取れないモノや様子はないか
- 周囲を気にしていないか
- 進行方向や業務にあたる向きと、視線がずれていないか
- 歩容が緩急を繰り返していないか
- 手指の動きに緊張はないか
- 普段の執務中とは異なる動線をたどっていないか

⇒ **その振るまいが決定的証拠とはならなくても**
ある種の仮説を補強する傍証にはなりうる

(14) 情報インシデントに際してのカメラ映像の精査（一例）

＜ヒトのリスク＞

- 出入管理との不一致
- 入居ビル、入居フロア、執務室内での不審者・不審行為

＜モノのリスク＞

- 視覚上・聴覚上の異常

  例：インジケータランプの点滅やアラートブザーの鳴動

  あるべきものがない、ないべきものがある

(15) 弊社取扱事案からの一例

当日の投影のみといたします

(15) 弊社取扱事案からの一例

当日の投影のみといたします

(16) まとめ

- **執務室のセキュリティ・バイ・デザイン：「環境防犯設計」をはかる**
  - **＜運用＞**

    不正行為、犯罪、インシデントを前提としたリスクコントロール
  - **＜ハード＞**

    機密室を中心に厳格な入退管理・監視体制を敷く
  - **＜ソフト＞**

    上記の体制を敷ける社内環境＝セキュリティ意識の教育・啓発
- **性善説とシステムの全能感に傾斜しない、危機管理が望ましい**

ありがとうございました。