ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会
2015 年度　ワーキンググループ２(WG2)
最終報告書

内部犯行問題に関する検討

目次

1. 背景・目的

- 不正アクセスやウイルス感染、情報漏えい等の情報セキュリティの事故の発生原因は、組織の外部からの攻撃と内部における不正行為の大きく2つに分類される。
- 外部からの攻撃に対しては、システム担当部署による技術的対策の実施により、一定の効果を期待することができる。
- 一方、内部における不正行為の場合、その行為者は、情報や情報システムにアクセスする権限を有する場合が多く、アクセス制御等による技術的な対策のみでは不正行為を抑止することは難しい。内部不正を防止するためには、技術的な対策と合わせ、不正行為が発生する環境要因や心理的要因等についても考慮し、組織横断的な対策を講じる必要がある。
- 企業における情報セキュリティ対策において、これまで不正行為が発生する環境要因や心理的要因にフォーカスされてこなかったために、情報システム部門が対処すべきリスクとされる傾向があった。
- WG2では、内部不正行為について様々な視点で検証し、情報セキュリティ対策は、システム担当部署のみではなく、他の部署も含めた組織横断的な対策が必要であることを理解し、内部不正に対する対策の考え方を身につけることを目的とした。
- 昨年度は、IPA「組織における内部不正ガイドライン」のチェックリストをベースにした検討を行ったが、本年度は、会員企業各社の事例の検証を行った。さらに、内部不正対策を検討するにあたり、環境犯罪学や経済学等の新たな視点についても検討を実施した。

2. 検討メンバー

■ 検討メンバー　（社名：五十音順　氏名：敬称略）　◎主査　〇副主査

株式会社インフォセック	小村　克彦
株式会社京王ITソリューションズ	田中　淳一郎
株式会社ジェイティービー	◎戸田　磨
新日本有限責任監査法人	〇青波　久恵
積水化学工業株式会社	〇平尾　安明
デロイトトーマツリスクサービス株式会社	丸山　満彦
日本電気株式会社	甲田　輝彦
富士通株式会社	平野　秀幸
富士ゼロックス株式会社	相田　昌史
三菱電機インフォメーションネットワーク株式会社	昆　資之

（事務局）

株式会社三菱総合研究所	川口　修司
	綿谷　謙吾

3．昨年度の検討内容と残課題

■IPA「内部不正防止ガイドライン」付録の「内部不正チェックシート」を基に、自己評価を使用する場合の課題、具体的に対策を実施する場合の課題について検討を行い、以下の意見が出された。

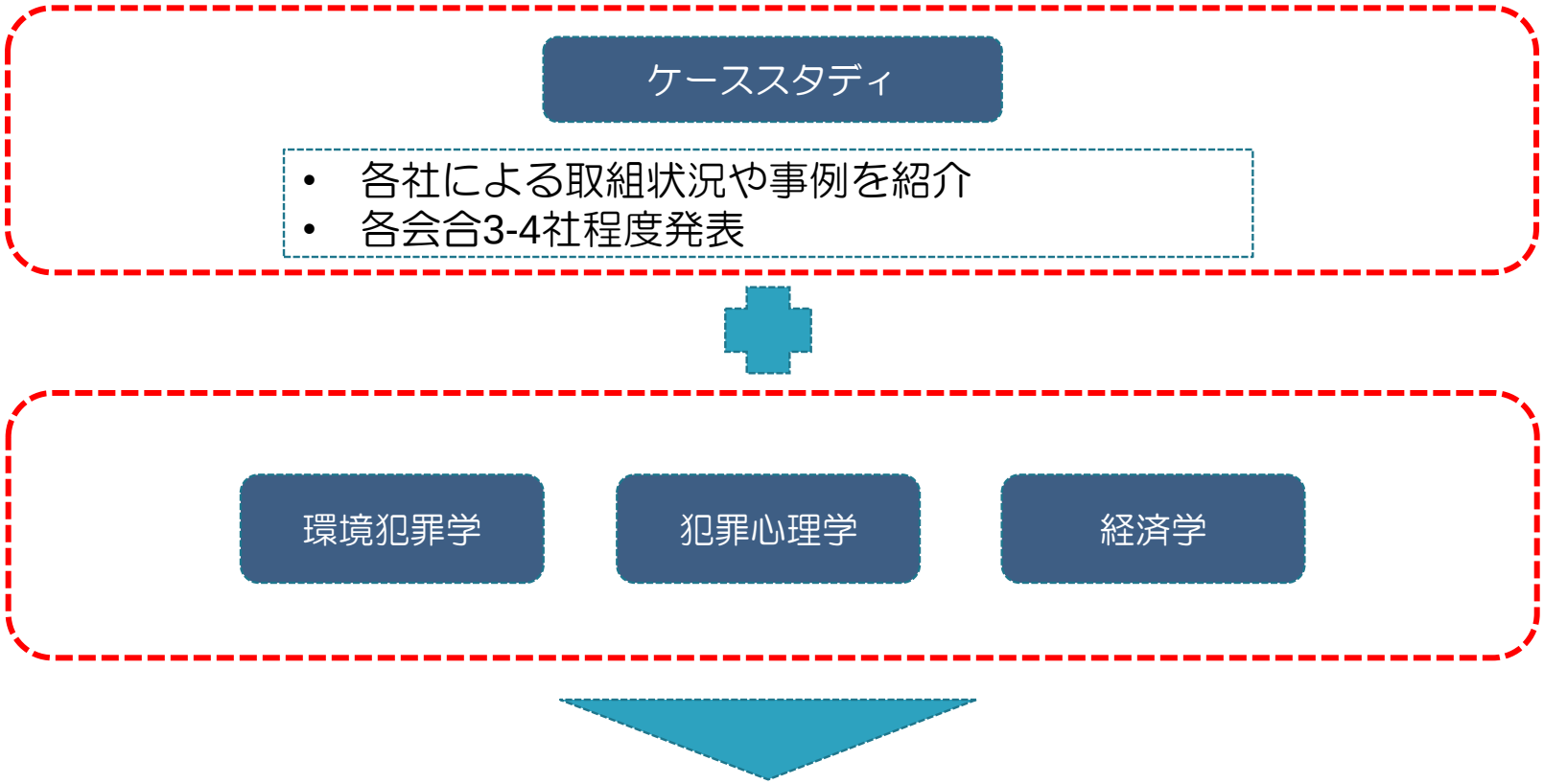
- 評価実施者が情報セキュリティの知識を十分持ち合わせていない場合は、正確な評価が難しい
- 自己評価を行う場合は、その判断基準をわかりやすく定義する必要がある
- 自己評価結果の妥当性を第三者が判断できる枠組みが必要
- 外部委託先の評価は、委託先による自己評価のみではなく、現場確認が必要
- IPAガイドラインにある職場環境の項目にフォーカスをあてた施策を検討する必要がある
- 内部不正対策の他サイバー攻撃対策による情報漏洩対策として、社員の情報リテラシー教育や性善説から性悪説への意識改革が必要となる
- チェックリストを活用して現状把握し、遵守・実施できていない事項は、リスクベースで対応方針を検討し対策を実施するなど、PDCAサイクルを定期的にまわす必要がある

内部不正対策として、情報システム部門だけではなく他部署との連携を進める方策の検討

- ワークライフバランスや業務プロセスの可視化等は一般の会社では推進されているが、なぜセキュリティと関係するかを議論する必要がある
- 職場環境や人的管理の実施項目は情報システム部門だけでは対応できず、人事や総務との連携が重要となる
- IPAガイドラインでも情報システム部門が主担当となる部分の議論はなされているが、他部署をどのように巻き込んでいくかの視点はまだない

4. 今年度の検討方針

■ 学術的なアプローチと各社の取組や事例を通して、内部不正対策に応用可能な知見を抽出
■ 特に、昨年度のWGでは十分に検討できなかつた、組織的対策に着目して検討する



内部不正対策への応用検討・昨年度検討結果の深化

５．先行研究・事例紹介

5.1　内部不正の特徴

種類		システム悪用	情報流出Ⅰ（道具的犯行）	情報流出Ⅱ（表出的犯行）	破壊行為
個人的・人格的な特徴（IT能力/技術）		業務で使用している端末が使用できる程度のIT技術のものが多くを占めていた（高いIT能力を有さない）	システム管理などの相対的に高いIT技術を有する者が多い。		
環境要因	業務の専門性	分業化され、専門化された業務についているものが多く、業務の監視性については、全体的に低い状況であった。			
	職場への不満内容	経営支援のシステム自体に不信感を抱いていた者や、経営者や上司の態度に強い不満を抱いているものがいた	上司とそりが合わないことや、経営者との対立、多忙や責任の重圧によるストレスの他、業績が上がらない為に収入減少へのストレス	経営者や上司からの屈辱的な扱いや、対立場面での上司との喧嘩、能力の評価や報酬が期待より低いこと、経営方針や経営者の生活態度への疑問など	能力が認められず解雇されたり、慣れない業務を担当させられて低い評価を受けたり、努力や能力が評価されないといったことが不満。
犯行状況	動機	経済的なひっ迫感		嫌がらせや鬱積した感情の発散。	
	その他	個々の事例や分類よって大きく異なり、日常業務で使用していたシステムに、組織の内部または外部からアクセスして犯行を行った事例や、情報収集のためキーロガーを利用していた事例、他の従業員のメールを自宅で自動受信設定していた事例もあった。			

（出所）IPA「組織内部者の不正行為によるインシデント調査　-調査報告書-」をもとに一部加筆修正

※情報流出Ⅰ（道具的犯行）…情報持ち出しなどの違反行為が、ある目的（例えば情報売却による金銭獲得）に沿った合理的な手段
　情報流出Ⅱ（表出的犯行）…情報持ち出しなどの違反行為が、心理的満足を得る（例えば鬱憤晴らし、情報を把握することで心理的な優位性を保つ）手段

5.2　内部不正対策のポイント

対策・ポイント	詳細項目	内容	論点
時期に応じた対策	入社前	• 採用予定者が担当することとなる職務を遂行するために必要な適性を有しているかのチェックを行う。 • 情報及び情報システムの取り扱い及び利用に関して契約に盛り込み及び違反した場合の措置についても書き込んでおく。 • 労働条件、処遇条件について採用時に明確化しておく。	• 職務遂行上必要となるスキル・能力を明確にする必要があるが、人事部はすべて把握できない • 採用時に明確化した労働条件を順守する必要がある • 個人情報の関係から入社前調査の徹底は難しい。入社後の確認が重要となる。 • SNSのチェックをどの程度実施するか
	在職中	• 職場全体のコミュニケーションを良くしておく。 • 抑止システムの整備及び兆候の把握。	• 在職中も転勤・異動があるため、職務遂行上必要となるスキル・能力を明確にする必要がある
	退職期	• コミュニケーションが重要、アカウントの無効化。	• 孤立させないことが重要
	退職後	• 退職後もモニターが必要であることを認識すべき	• アカウントの無効化が漏れていないか（システム管理者権限など） • 退職前のログを見て不審な行動がないか確認 • 退職者のメールアカウントを上司に振り替えて、退職後の顧客と不審なやり取りが無いかチェック（本来の目的は仕事の引継ぎ）
情報システム面からのポイント	システム運用	システム開発者・運用者による犯行を防ぐための対策として以下のポイントがある。 • システム開発・運用は複数の者で担当する。 • システムへのアクセス権限を適切に管理する。 • 実際の業務に当たっても一人に任せきりにしない。 • チェックシステムを導入しておく。	• システム対策に加え上司の承認が必要としたり、複数人体制で行ったりするように手順を決める • ログの取得で証拠を残す、さらに通知することで抑止にもなる • システム部門が何を行っているかが見えない執務環境がある

（出所）IPA「組織内部者の不正行為によるインシデント調査　-調査報告書-」をもとに一部加筆修正

5.3　内部不正の要因分類

分類	内容
動機・プレッシャー	内部者が不正行為を起こす動機であり、内部不正行為に至るプレッシャー（業務量・ノルマ等）や慢心及び帰属意識などが含まれる。 ＊キーワード：転職、満足度、給与・賃金・賞与、不公平感、怨恨、業務量、ノルマ、好奇心・顕示欲、慢心等
環境・機会	不正行為を行った内部者が、環境によって受ける要因であり、技術（ＩＴシステム）や物理的な環境及び組織のルールや教育などが含まれる。 ＊キーワード：アクセス制御、出入検査、職場環境管理、持出・持込制限、監視、時間、コミュニケーション、ルール・規則、告知・教育等
知識・経験	不正行為を行った内部者が、持っている知識や経験であり、特定の経験や権限・役割（持っていること）や知識（知っていること）及びスキル（できること）などが含まれる。 ＊例示：持ち出す方法を知っている、発覚しなかったことを知っている、証拠を削除することができる、アクセスする権限を持っている等

■　営業社員と開発者による違い

	営業	開発
動機・プレッシャー	・業務が日々繁忙または業務上のノルマがきつく、自宅でも業務をする必要がある。 ・情報を使い転職を有利に進めたい。	・自らが作成したファイルのオーナーは自分であり、自分の所有物であるという誤った認識がある。 ・頻回転職が数例存在する。
知識・経験	・社内システムを利用する程度のＩＴ技能を有する。 ・対象物へのアクセス権限を有する。	・ソフトウェア開発ができる程度のＩＴ技能を有する。 ・対象物へのアクセス権限を有する。
環境・機会	・ジョブローテーションが少ない。 ・評価、接遇処遇の納得度が低い ・監視が不在であり、不正行為を行う時間がある。	・評価、接遇処遇の納得度が低い ・監視が不在であり、不正行為を行う時間がある。
要因外の特徴	・犯行の発覚は、離職後に発覚する場合のみであり、離職後の転職先での利用を計画的に行っている事例もある。	・犯行が離職後に発覚する場合と、在籍中に発覚する場合がある。前者は離職（転職）が起因した不正行為で、後者は自らが作成した成果物は自分の所有であると誤認。

（出所）IPA「組織内部者の不正行為によるインシデント調査　-調査報告書-」をもとに一部加筆修正

5.4各社事例紹介フォーマット

◎実際にあった事例を通して内部不正を察知する感度を高める。

- 動機を知る
- 不正行為者の役職や特徴を知る
- 事故後の検証から得られた前兆を知る
- 事故の概要を知る
- 既存のルールが事故の未然防止につながっているのかを知る

分類	情報の持ち出し
動機・目的	
不正行為者	
前兆	
概要	
関連ルール	

5.5　事例紹介　①

分類	情報の不正利用
動機・目的	金銭的な利益取得
概要	職員のインサイダー取引
再発防止策	職員などに対する自己点検の実施、株取引規制強化、業務部門運営体制の見直し等

分類	買い上げデータの不正登録
動機・目的	金銭的（ポイント）な利益取得
概要	顧客の買い上げデータを自己に付替え、ポイントを不正窃取
再発防止策	ポイント付与異常値アラート機能等

分類	横領
動機・目的	金銭的な利益取得
概要	収入印紙の横領、在庫、購入、使用の管理が担当者任せ
再発防止策	印紙使用の複数管理

分類	架空取引
動機・目的	金銭的な利益取得（多額の借金、遊興）
概要	商談のねつ造・架空売り上げ、商品の転売
再発防止策	管理体制の見直し等

5.5　事例紹介　②

分類	情報の持ち出し
動機・目的	転職
概要	営業情報、契約情報が特定のアドレスに送信され社外に流出
再発防止策	職員などに対する自己点検の実施、株取引規制強化、業務部門運営体制の見直し等

分類	作業時間の水増し
動機・目的	金銭的な利益取得
概要	繁忙で業務負荷が高い状況下で、自己申告形式の作業報告書を水増しし請求
再発防止策	入退室のログと作業報告書の整合を確認

分類	システム情報漏えい
動機・目的	会社への報復
概要	在職中にアプリケーションインストール情報を抜き取り、退職後に著作権保護団体へ告発
再発防止策	ダウンロード履歴の保存、ライセンス遵守の徹底

分類	情報の持ち出し
動機・目的	金銭的な利益取得
概要	キャッシュカード情報を不正に入手し、偽造カードを作成。金銭を不正に引き出す
再発防止策	再委託業務のチェック体制の見直し

5.5　事例紹介　③

分類	不適切な売上計上
動機・目的	プロジェクトの売上・利益の水増し（海外）
概要	作業が開始されていないにも関わらず、SEのローディングコストとして計上
再発防止策	海外赴任者向け教育、海外拠点長向けマニュアルの徹底、管理体制の見直し

分類	費用・工数の振替
動機・目的	誤った認識・思い込み
概要	AシステムとBシステムの開発費の総額をAシステムの売上原価として計上
再発防止策	コンプライアンス教育、点検活動の強化、管理体制の見直し

分類	支払い金額の不正操作
動機・目的	プロジェクト原価の悪化の回避
概要	派遣社員に工数を過少申告させ、その分を翌期へ繰り越し
再発防止策	取引先巡回調査の強化、コンプライアンス教育、管理体制の見直し

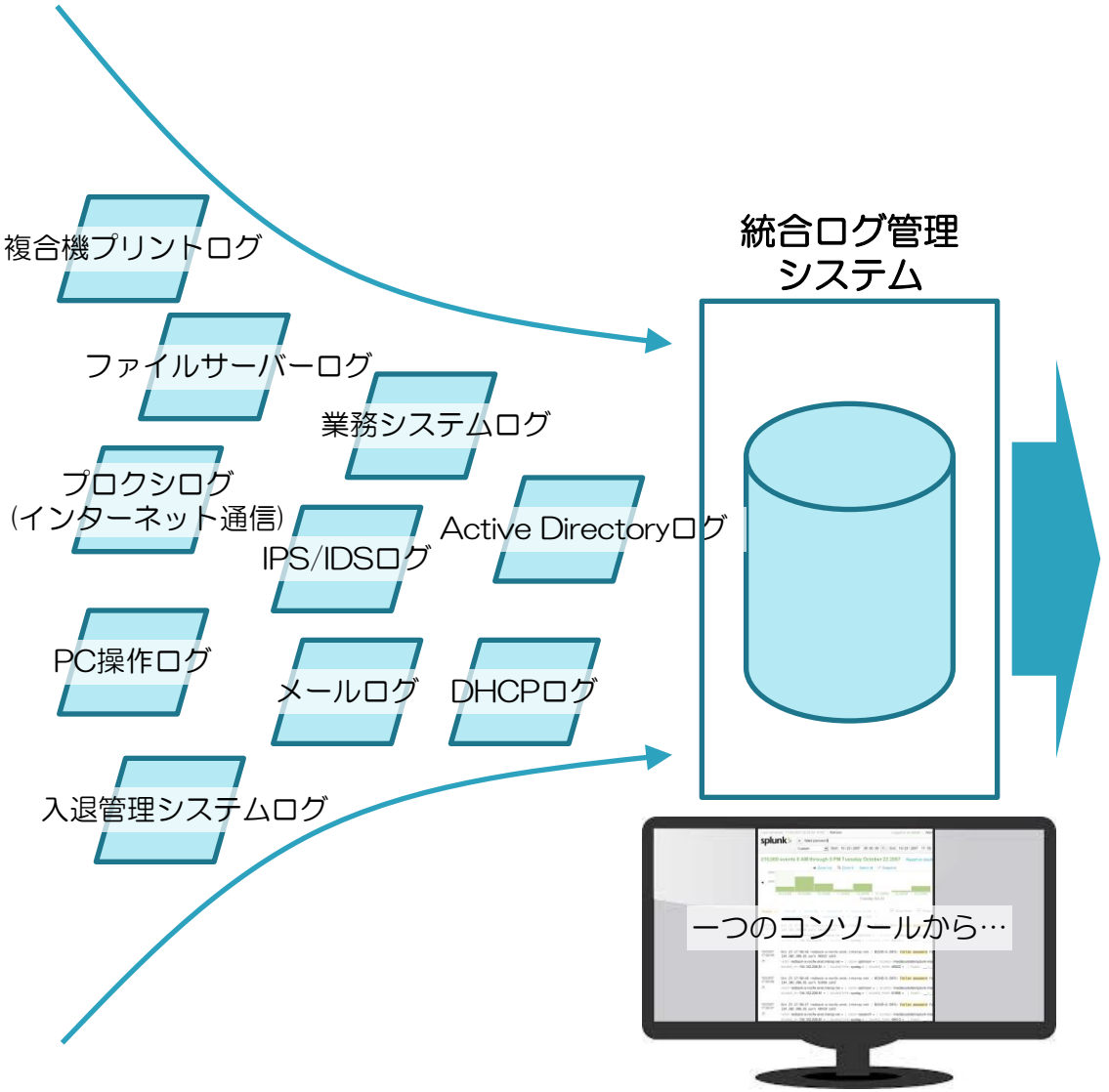
分類	勤怠処理の不正申告
動機・目的	不正な勤務管理の正当化、給与の不正受給
概要	遅刻や欠勤をしても正常勤務として不正に申告、管理者は勤務場所が異なっていた
再発防止策	コンプライアンス教育、管理体制の見直し

5.6　事例研究から得られた知見・論点・対策

知見・論点	対策
• 金銭的目的と会社のためのつじつま合わせが多い • 内部不正の情報漏洩事案は表に出てこない。明らかになるのは紛失、盗難関係。管理部門が気づかない事例もあるのではないか • 情報漏えいや金銭の窃取の発覚は事後の場合が多い	• モニタリングシステムを導入し、従業員にモニタリング状況を通知
• 行為者自身が情報漏えいだと思っていないケースが多い。業務上必要だから共有している。扱う情報が重要なものだという認識が薄い。 • 当事者の悪意のある事例と悪意のない事例がある。悪意のない人の内部不正対策をどうするか • 対策方法は教育だけか	• 守るべき情報と守らなくてもよい情報を分ける必要がある • 当事者は想像力に欠けている。べからず事例集を出すと言われたことしかやらなくなる • 具体的な事例集に加え、従業員の倫理観を涵養することが必要
• 規程をどのように理解させるか • 規程を作るときのルールはどうあるべきか • 規程を作成した後のモニタリングはどのように行うか	• 規程の目的（なぜ作られたか、内部監査のチェック項目にもしてる）や管理者、改定履歴等を明示し規程の存在を認識してもらう • 規程の定期的な見直しを実施する • 規程は必要なものに限定し作りすぎない • ガイドブックを作成し紙で配布 • 内部統制で規程の順守状況を確認。規程通りに運用しているか、運用に合わせて規程を改定
• E-learningの受講をどのように徹底するか • 色々な部署がやりたいが、現場の負担にもなる • E-leaningを実施した後のフォロー。理解していない人の教育をどうするか	• 閲覧時間を設定する、確認テストを工夫 • E-learningの講座数を集約し、実施時期を分散させる • 重要なテーマは繰り返し実施する
• 風通しがよくルールが守れる職場風土をどのように醸成するか • よい方向にも悪い方向にも流れる可能性がある大多数の社員をどのようにしてよい方向に持っていくか	• 何かミスを犯した時に隠さず報告できる環境を作る。ミスが起きた時に個人を責めずに部署で共有し再発防止に活かす • 職場単位でコンプライアンス研修を実施する取組みがある

６．内部不正を未然に防止する（対策例）

6．内部不正を未然に防止する（対策例）①
～統合ログ管理システムの概要～



内部不正対策→コンプライアンス部門

調査内容の例：
- 外部クラウドサービスをたくさん利用している人は？
- プライベートアドレスにメールをたくさん送信している人は？
- 深夜早朝・休日に頻繁にPCやネットを使用している人は？
- USBストレージを頻繁に接続、使用している人は？

閾値を設定し、アラート発報も可能

サイバー攻撃対策→IT部門／CSIRT

検知内容の例：
- インターネットへの大量のデータ送信をしているPCは？
- ドライブバイダウンロード攻撃のURLを踏んだPCは？
- ブラックリストIPアドレスと通信しているPCは？
- マルウェア検知の動向は？

６．内部不正を未然に防止する（対策例）②
～統合ログ管理システムによる不正の兆候の検出～

Information Security Governance Association

目的	手段	監視／検知すべき事象
会社情報を社外に持ち出す。 ＊動機としては、第三者に販売して金銭的利益を得る、転職先で役立てる、私的に持っていたいなど様々なものが考えられるが、本表では区別しない。	・ファイルサーバーから自分のPCにファイルをダウンロードする。 ・業務システムから自己のＰＣにデータをダウンロードする。	・ファイルサーバーからＰＣへのファイルの大量ダウンロード ・ファイルサーバーのクロール行為（アクセス可能なディレクトリ／フォルダーを片っ端から開いていく）
	・ノートＰＣ、スレート型端末、その他のポータブルデバイスにファイルをコピーして社外に持ち出す。	・ＵＳＢストレージデバイスのＰＣへの頻回な接続 ・ＵＳＢストレージデバイスへのファイルの大量コピー ・ストレージ以外のデータ転送用ＵＳＢデバイス（スゴイケーブル、Transfer Jetなど）のPCへの頻回な接続
	・インターネット経由で情報をアップロードする。	・特定のPCからインターネットへの大量の上り方向の通信（プロトコル問わず） ・ＰＣ遠隔操作ツールサイト（TeamViewerなど）への頻回な接続 ・フィルタリング解除PCからクラウドサービスサイトへの頻回な接続
	・メールを利用して社外に持ち出す。	・社外への送信メール（通数、バイト数）の増加（本人の過去トレンドとの比較） ・個人向けプロバイダーアドレス、フリーメールアドレスへの頻回なメール送信
	・紙にプリント、コピーして社外に持ち出す。	・特定のＩＤによる大量のプリント、コピー
	・周囲に不審に思われないよう人のいない時間に作業をする。	・深夜、早朝、休日の頻回なログイン（ＡＤ、ファイルサーバー、業務システムなど） ・深夜、早朝、休日の大量のプリント、コピー

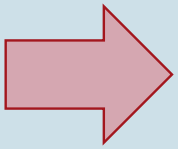
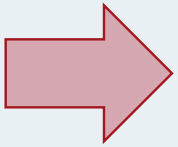
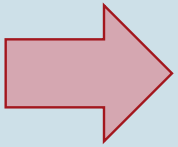
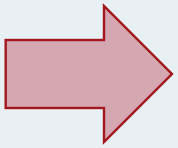
6．内部不正を未然に防止する（対策例）③
～統合ログ管理システムによる不正の兆候の検出～

ISGA
Information Security Governance Association

目的	手段	監視／検知すべき事象
・自己にアクセス権のない情報（ファイル、業務システムの画面、メールなど）を盗み見る、取得する ・自己に権限のない操作をする。	・他人のID・PWを利用してファイル ・サーバー、業務システムにログインする。（なりすまし）	・本人の管理下にない端末からのログイン ・同一IDによる複数端末からの同時ログイン（本人の管理下にない端末を識別） ・不正ログイン攻撃（同一IDに対するブルートフォースアタック）
	・周囲に不審に思われないよう人のいない時間に作業をする。	・深夜、早朝、休日の頻回なログイン（AD、ファイルサーバー、業務システムなど）
ファイル・データの消去・改ざんにより業務を混乱させる。（会社に損害を与える。）	・ファイルサーバーにアクセスし大量のファイルを削除する。	・アクセス者が所有権、作成者ではないファイルの大量削除
ファイルサーバー、業務システムの停止、破壊により業務を混乱させる。（会社に損害を与える。）	・サーバーに侵入し、管理者権限を奪う。	・イントラネット内ノードからの（許可を受けていない）ポートスキャン、脆弱性スキャン
	・周囲に不審に思われないよう人のいない時間に作業をする。	・深夜、早朝、休日の頻回なログイン（AD、ファイルサーバー、業務システムなど）
【不特定】 様々な不正行為に利用可能	・会社に管理されていないPC（私物など）をイントラネットに接続して使用する。	・DHCPにより取得されたIPアドレス、および正規の手続きにより許可された固定IPアドレス以外の固定IPアドレスによるイントラネットへの接続 ・PC資源管理ツールに登録されていない、かつ固定IPアドレス使用機器として登録されていないMACアドレスによるイントラネットへの接続

6．内部不正を未然に防止する（対策例）④
～統合ログ管理システム導入によるメリット～

ISGA
Information Security Governance Association

	導入前		導入後
調査範囲	・特定の従業員（退職予定者、密告のあった者など） →うまく隠れながら不正を働いている者を見逃してしまう。		疑いの有無にかかわらず、全従業員を対象に、異常な振舞いを発見できる。
調査対象のログの量・種類	・担当者が精査できるログのデータ量が限られる。☹ ・異なるシステムのログの突合が困難。☹ →不正行為の全体像がわからない。		多種大量のログを多面的に、また組み合わせて調査できる。
調査頻度・時期	・調査依頼があったとき月に4～5件までが限度。☹ →不正行為のタイミングがわからず、決め手が発見できないことも。		日時サイクルでの調査が可能。 レポート対象の異常事象については、すぐに（翌日）発見可能。
調査方法・手順	・生のログデータから異常事象を読み取れる形にする作業が手作業でとても大変。☹ →担当者の知識・熟練を要する。☹		システムが自動で処理するので、調査内容の設定後は、日々の専門家による作業は不要。

7.　経済学的アプローチ

(1)情報の経済学　プリンシパル・エージェント問題

- 依頼人(プリンシパル)と代理人(エージェント)間にある情報の非対称性を原因としたモラルハザードの問題。依頼人は代理人がどのように行動するか監視することができず、依頼人が望むとおりに代理人が動くとは限らない。

- 現実的に企業(管理者)は従業員すべての行動を把握することは不可能。
- 監視を強化することにより、企業(管理者)は従業員の不正を検知できる可能性が高まるが、従業員は会社に対して不信感を抱いたり仕事に対するモチベーションが低下する可能性がある。これにより、会社と従業員の信頼関係にひびが入り、従業員の会社に対するロイヤリティが低下する可能性がある。

(2)アイデンティティ経済学

- 個人の行動が規範や理想と合致した時の利得、または合致しないときの損失を「アイデンティティ効用」とし、社会規範(企業理念等)等が個人の行動に影響を与えるかを分析

危険！

社会的カテゴリー	インサイダー	アウトサイダー
特徴	企業と自身を同一視するタイプ	企業と自身を重ね合わせないタイプ
規範と理想	• 企業のために働くべき • 理想は大いに頑張ること	• なるべく手を抜きたい • 自己中心的で、企業のことは考えない
アイデンティティ効用の損益	• 頑張らずに手を抜くとアイデンティティ効用を失う	• 組織のために働くとアイデンティティ効用を失う
必要な賃金	• 企業のために働くことに満足しているため、努力を引き出すためのボーナスは少なくてよい	• 勤勉に働かせるためには、失われたアイデンティティ効用を埋め合わせるボーナスが必要

■ 企業にとってインサイダーは理想的な人材(賃金が相対的に低くても頑張ってくれる)
■ 企業はアウトサイダーに働きかけ企業への帰属意識を高めてもらうことが重要となる

7.　経済学的アプローチ

(3) 行動経済学

- 合理的な個人を前提とせずに、さまざまな実験や調査をもとに人間の行動や意思決定を分析
- ダン・アリエリー(2012)「ずる　嘘とごまかしの行動経済学」によると、不正を促す(減らす)要因は下表のとおり
  - 人は会社の事務用品(ペンやコピー用紙)は盗みやすいが会社のお金を盗むことには抵抗感がある(自分の行動を正当化するのが難しい、正当化できれば不正を働く可能性、創造的な人ほど正当化が得意)
  - 非常にストレスがかかっている状況では判断能力が低下し、不正を行いやすくなる
  - 作業を実施する際に、署名させたり会社の規則を読ませたりすることで、不正を行う意欲が減る(道徳心が呼び起こされる)
  - 監視は不正を抑制する効果があるが、監視者と不正を行うものが癒着していれば不正を促す

	要因
不正を促す要因	正当化の能力
	利益相反
	創造性
	一つの反道徳的行為
	消耗
	他人が自分の不正から利益を得る
	他人の不正を目撃する
	不正の例を示す文化

	要因
不正に影響なし	不正から得られる金額
	捕まる確率
不正を減らす要因	誓約
	署名
	道徳心を呼び起こすもの
	監視

8．まとめ

■ 内部不正対策は、経営・人・組織・職場環境・技術の視点から総合的に検討する必要がある。

経営層

- 社長直轄でリスク管理し、部門横断的に取組むことが重要
- 内部不正対策の強化は経営トップが自ら率先して示すべき
- 対策のための人と予算等のリソースを確保

人的対策

- 不正行為者の動機や目的を、事例研究等により網羅的に把握
- 管理監督者による日常的な観察により不正予備軍を察知
- 管理監督者が注視すべき点を例示し、その対応策を検討
- 不正は人目を避けた時間に行われることが多く、労務管理の徹底も重要

組織・職場環境

- 管理者は悪意のない不正の場合、不正自体を責めず、報告しないことを責めるべき
- ルールと業務の実態が一致していないケースがある。ルールに実効性を持たせ、内部不正を起こしにくい環境を整備
- 全ての部署がリスク視点で主管業務を見て対応し、他部署の視点からリスクを見ることも重要

技術的対策

- 内部不正の「手段」を事例研究等により網羅的に把握
- 「手段」の実行過程で検知できる事象に対する監視活動により未然防止

8．今後の課題

人的・組織的対策の検討

- 事例研究等を通して、情報システム部門だけで内部不正対策を実施するには限界があり、人的・組織的対策の必要性を再確認できた。
- ただし、具体的な人的・組織的対策までは落とし込めておらず、具体的方策を検討するのが今後の課題である。

理論的アプローチの対策への応用

- 環境犯罪学や経済学からの理論的なアプローチを試みたが、そこで得られた知見を内部不正対策するところまで検討できていない
- 内部不正対策に援用できる可能性がある知見もあったため、今後はそれを具体的な対策や事例への適用等を検討する必要がある。