Security Protection Network
RISK FOCUS REPORT

vol. 2

「情報セキュリティ編
～情報漏洩における人的リスク～」

SPN リスクフォーカスレポート vol.2
第 1 版　2013 年 6 月
株式会社エス・ピー・ネットワーク　総合研究室

SPN リスクフォーカスレポート vol.02

情報セキュリティ編～情報漏洩における人的リスク～

〈執筆者〉
株式会社エス・ピー・ネットワーク
総合研究室　研究員　佐藤 栄俊

目　次

1 はじめに

企業・組織で発生している不正アクセスやウィルス感染、情報漏洩等の情報セキュリティ事故のニュースが連日のように報道されている。その被害は増加傾向にあり、ますます深刻化している。近年の情報セキュリティ事故は、これまでの愉快犯的な行為から、経済的利得や企業等の組織活動の妨害といったものが目立つようになるなど、犯罪の目的が変化・多様化している。

情報セキュリティ事故は、発生場所の相違から、「組織の外部からの攻撃」と「内部における不正行為」の 2 つに大きく分類することができる。組織外部からのサイバー攻撃は、インターネットから組織のネットワークに対するウィルス攻撃や DDoS(Distributed Denial of Service attack)による攻撃、標的型攻撃メール送付等がある。一方、組織内部で起きるのが、内部者による不正行為である。

内部者は、情報や情報システムにアクセスできる権限を持つ者の場合が多く、アクセス制限等による技術的対策のみでは限界がある。そのため、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する必要がある。(1)

組織における顧客情報・個人情報・機密情報等の漏洩や流出が当該組織に与える損害は、情報漏洩の検出/エスカレーション（原因究明）と顧客への通知、事後対応等の直接的なコストに加え、顧客離れに伴う事業面での損失、株価の下落、信用の失墜、そして長期にわたる営業効率の悪化、システムの再構築費用等々、非常に大きな負担となる。

そのうえ、たとえ、技術的なセキュリティ対策やマニュアルの整備、研修の実施や誓約書の提出等、内部統制システムを構築することによって、情報漏洩リスクを一定程度低減できたとしても、「人」が介在する以上、「人」に起因する運用上のリスク（＝人的脅威）をゼロにすることはできない。特に、人的脅威の中でも、「故意による内部犯行」が発生すると、大きな被害・影響をもたらす。したがって、その対策についても、その他の情報セキュリティ上の類型とは異なる対応が必要となるのであり、本レポートでは組織内の漏洩事故における人的脅威を中心に考察をおこなうこととする。

また、情報漏洩に至るまでのリスク構造から、潜在的要因を検証し、漏洩事故を予防するための方策について検討する。

※なお、本レポートにおける「人的脅威」とは、人によるデータの誤削除・紛失、入力ミス、設定間違い等の偶発的な脅威と不正アクセス、持ち出し、改竄等の意図的な行為を指す。

---

(1) 独立行政法人情報処理推進機構(2012)「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-」http://www.ipa.go.jp/security/fy23/reports/insider/index.html

2 問題意識

国内における組織の内部者による不正や違反行為に関する実証的な取り組み事例の紹介は、2010 年に公表された財団法人社会安全研究財団による「情報セキュリティにおける人的脅威対策に関する調査報告書」[2]がある。この報告書では、サイバー犯罪で検挙された事例として、悪意を持った内部者の不正行為を対象に分析している。ただし、JNSA（NPO 日本ネットワークセキュリティ協会）が 2010 年に実施した「2010 年のインシデントに関する調査～発生確率編～」[3]によると内部者の不正行為には、必ずしも悪意を持っていたとは言い難い「うっかりミス」や業務遂行上迫られた「ルール違反」等の事案が多数あると指摘している。

ハインリッヒの法則では、1件の重大な事故・災害の背景には、29件の軽微な事故・災害が起こっており、300件もの「ヒヤリ・ハット[4]」が起きていると言われる。情報セキュリティ事故を「重大な事故・災害」と捉えるとすると、犯罪として立件に至った重大な事案の背景にある、犯罪として立件に至らなかったもの（「29件の軽微な事故・災害」に該当）や、ヒヤリ・ハットに関するもの（「300件のヒヤリ・ハット」）も発生しないように対策を講じる必要がある。

したがって、内部者による不正や違反行為の対策を検討するには、犯罪として立件に至らない事例やヒヤリ・ハットに関する事例についても幅広く情報を収集することが必要である。しかし、これらの情報は、「風評被害が発生する恐れ」や「利害関係者との調整がつかない」等の理由から公開されることが稀であり、実際には、他社事例の情報共有は困難である。

そこで、このような状況を克服するため、企業・組織が取るべき情報漏洩に関わる内部不正やルール違反防止のための方策を立てるためには、不正者が不正行為を働く動機や背景等の特徴を明らかにすることが有効である。

内部の脅威に注目した取り組みの研究調査として、財団法人社会安全研究財団は、「情報セキュリティにおける人的脅威対策に関する調査研究報告書」[5]において、その環境等に予防の観点を導入した環境犯罪学や犯罪心理学の理論を援用している。

上記、調査報告書では―――

犯罪者となるリスクを持つ人については、犯罪者が犯罪に至る「機会」や「動機」を取り除き、犯罪者となるリスクを持つ人を減少させるための対策や、犯罪者になることを抑制する力を強化するための方策が考えられるとしている。これは、劣悪な組織環境が不正の原因になっているのであれば、そのような組織環境を改善することや、社会的な規範を順守する価値観を持つよう教育する、などを挙げている。

---

[2] 財団法人社会安全研究財団(2010)「情報セキュリティにおける人的脅威対策に関する調査報告書 」http://www.syaanken.or.jp/?p=1865

[3] NPO 日本ネットワークセキュリティ協会セキュリティ被害調査ワーキンググループ(2011)「情報セキュリティインシデントに関する調査報告書～発生確率編～」http://www.jnsa.org/result/incident/2011.html

[4] 重大な事故や災害に至らないが、重大事故につながりかねない事故寸前の危険な事例のこと

[5] 財団法人社会安全研究財団(2010)「情報セキュリティにおける人的脅威対策に関する調査報

潜在的な被害者（物）については、潜在的な被害者（物）が持つ犯罪被害への抵抗性を高めるための対策が考えられる。これは、侵入盗の被害に遭いにくい家屋作りのために「戸締りを完全にする」「窓のガラスを割れにくいものにし、面格子や雨戸を付ける」といった対策をとることが挙げられる。

環境については、犯罪を誘発する「環境」を作らない、あるいは誘発要因を減らすための対策が考えられる。これは、潜在的な内部不正者に「結果的に(or 絶対に)損する（得はしない）」と知らしめる環境設計にすることも重要な対策となるとしている。

上記調査概要からも明らかなように、情報セキュリティ事案における、内部不正者による「機会」や「動機」、「正当化」いわゆる、不正のトライアングルによる犯行の成立を未然に防ぐための総合的な対策が講じられるべきである。

つまり、情報セキュリティ事案も、他の犯罪と同様に、犯罪者となるリスクを持つ人、潜在的な被害者（物）、環境のそれぞれについてバランスの取れた、整合性のある一群の対策を構築・実行していく必要があることを示している。

3 情報漏洩の概要

(1)情報漏洩事案の概観

2011 年の個人情報漏洩件数の原因別比率[6]は、「誤操作」、「管理ミス」、「紛失・置き忘れ」の上位 3 つで約 80%を占めている。「管理ミス」に区分される事故は、組織としてルールが整備されていない、もしくは、ルールは存在しているものの遵守されていないために、社内や主要な経路で流出し、発生する事故である。ルールが整備されていないことによる事故は、発見が遅れ、事故に至る経緯を明確にできない場合も多い。

また、ルールが徹底されていないことによって発生する事故は、比較的早く発見され、経緯も明確にしやすい場合が多い。発見の遅れや経緯が不明確なままの場合は、事故の被害を大きくする。

「誤操作」および「紛失・置き忘れ」はヒューマンエラーに起因する原因である。これへの人的な対策としては、セキュリティ教育など組織内のヒューマンエラー自体の数を減らす予防効果の高い手法が重要となってくる。ヒューマンエラーは必ず起こることを前提として、暗号化などの漏洩対策や、紛失したとしても被害が拡大しない対策（フェールセーフの考え方）も併せて実施することも肝要である。

ここで、着目すべきは情報漏洩の原因として、組織内部の人的要因が合計で約 8 割を占

告書 」http://www.syaanken.or.jp/?p=1865

[6] NPO 法人日本ネットワークセキュリティ協会(2012)「2011 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～ 2012」
http://www.jnsa.org/result/incident/2011.html

めているということである。昨今の情報漏洩問題の傾向として、不正アクセスや新種のウィルス等の方に焦点が当てられがちであるが、当該データを見てわかるように、情報漏洩の本質的対策を考える上で、まず組織内の人的要因に目を向けるべきであることがわかる。

また、日本ネットワークセキュリティ協会が実施した「2010 年情報セキュリティ事故に関する調査報告書～個人情報漏えい編～」[7]によると、原因が内部者の不正である（事件）件数ベースは少ないものの、事故 1 件当たりの個人情報流出数で見ると、第 1 位の不正アクセス（13 万 8492 人）に次いで多い（7 万 8457 人）ことから、発生時の影響が多大であることがわかる。

さらに最近、企業における情報漏洩リスクの一つとしてクローズアップされているのが、産業スパイなどの事例である。これらは個人情報以外の機密上の流出に繋がるだけでなく、組織防衛のために隠蔽される可能性が高い。これらの表沙汰にならない潜在的な事故の発生・流出件数まで含めると、その数は相当な規模に膨れ上がることが予想される。今や、情報漏洩問題は看過できない非常に大きな問題になってきている。(損害の発生頻度が高く(8割)、損害も大きい（7 万人。第 2 位）事からすると、リスクマトリクス等を使ったリスク算定としても、対処優先順位の高いリスクであるといえる)。

なお、内部不正による情報漏洩事例としては、下記のようなものがある。

【内部不正による主な漏洩事例】

○ 半導体関連企業からの技術情報漏洩

半導体関連企業に勤務する従業員が、在日ロシア連邦通商代表部員から謝礼を受け、会社のパソコンから技術情報や企業情報等の社外秘情報を外部記憶装置にコピーし、渡していた。

○ 証券会社システム担当部長代理による顧客データ持ち出し・売却

証券会社のシステム担当であった部長代理が、同社のデータベースに不正にアクセスし 148 万人の顧客データを持ち出し、うち 5 万人分を名簿業者に売却していたことが判明した。

○ 元従業員による営業秘密侵害

元従業員が、在職当時にアクセス権のあった営業秘密をコピーして保有しており、退職後に海外競合企業に営業秘密を開示していたことが明らかになった。

○ 保険代理店から名簿業者に顧客情報の売却

[7] NPO 法人日本ネットワークセキュリティ協会(2011)「2010 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～2011」

廃業した保険代理店から、外資系保険会社 4 社の顧客情報 2 万 5000 件以上が名簿業者に売却されていた事件が発生した。また、翌月には同じ保険代理店から、通信販売会社の顧客情報 3 万 5000 件が売却されていたことも明らかになった。

(2)犯罪心理学の理論の適用

情報漏洩事案に限らず、その他内部不正や不祥事における不正行為者が、その置かれた環境との相互作用に影響されることを前提とし、その環境について一定のパターンを分析・導出できれば、その結果を予防に利用できると考えられる。

そこで、以下、不正行為者の行動とその環境などに予防の観点をおいた犯罪心理学の理論を適用し情報漏洩についての考察を進める。

1) 不正のトライアングル理論

米国のドナルド・R・クレッシーが提唱した業務上横領の発生要因に関する理論[8][9]。同教授は、イリノイなどの刑務所に横領関連の罪で服役中の 503 人を対象に裁判資料の分析や聞き取り調査を行い、「善人による背信行為」の因果関係の解明を試みた。

その結果、横領は「雇用主の資産を託された者が、①他人と共有できない金銭的な問題を抱え、②信頼された立場を利用すれば見つからずに問題を解決できると認識し、③利用しても問題ないと理由づけられる場合」に発生するという理論を構築した。この 3 つの要因は「不正のトライアングル」と呼ばれ「動機・プレッシャー」、「機会」、「正当化」という言葉で説明されることが多い。

幾つかの内部不正事例からもわかるように、情報漏洩リスク（紛失、流出、改竄、盗難）への対策として、情報システムセキュリティ対策や社内のマネジメントシステム（体制、ルール）を日々の運用において強化・推進していく必要があるのは当然である。

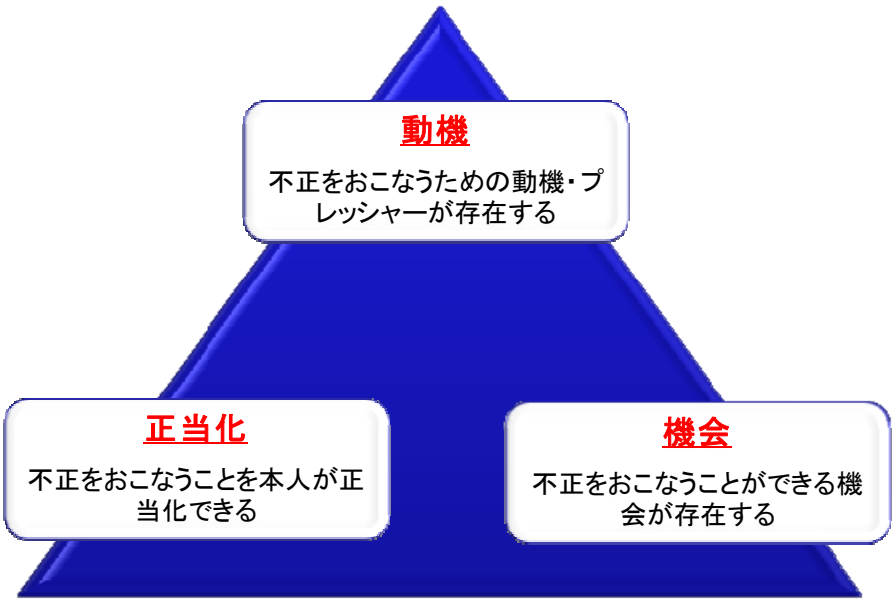
しかし、普段の業務の中には、「組織的な意思」とかけ離れた個人の裁量が入り込んだ判断や、意思決定・行動などが属人的な裁量に任されている活動プロセスが少なからずあり、そのため不正を生じさせうる余地が厳然として存在する。内部不正を防ぐためには、不正者が不正行為を働く「動機」や、「機会」や「正当化」の提供といった背景・環境等の特徴・メカニズムを明らかにすることにより、それに応じた対策を講じていく必要がある。

このように、「不正のトライアングル理論」とは、犯行に至る動機/プレッシャー、犯行を行いやすい機会、犯行を自己正当化する事由の 3 つの要因が同時または連続的に起こり、内部不正が誘発されるとする理論である。

---

[8] 財団法人社会安全研究財団リチャード・ウォートレイ他編著「環境犯罪学と犯罪分析」

[9] 日本公認会計士協会監査基準委員会報告書第 35 号「財務諸表の監査における不正への対応」でも、「不正は、不正に関与しようとする『動機・プレッシャー』、不正を実行する『機会』、不正行為に対する『姿勢・正当化』に関係している」とある。



不正のトライアングル

例えば、資産の流用に関する不正は、一般的に以下のような事象が不正発生の要因となり得る。なお、下記はあくまで例示であり、実際は個々の企業のおかれている状況等を勘案して分析することになる。

【動機】

一般的に不正を働く動機・プレッシャーとは、不正を実行する際の心理的な契機を意味し、個人的な理由・組織的な理由の両方が原因となり得る。例えば、

■ 経営者または従業員の個人的な債務（借金等）があり、一方で価値が高く、容易に持ち出すことが可能な資産（現金等）の存在がそれ自体を流用するプレッシャーの役割を有している。（個人的な理由）

■ 企業・組織とその構成員との間に敵対的／対立的な関係がある。（組織的な要因）

→既知または予想される（特定が容易な）従業員の解雇

→従業員福利や給与制度の変更（質的低下）または変更の予想

→期待と一致しない処遇（昇進や報酬等）

【機会】

一般的に不正を働く機会とは、不正が実行可能な統制環境が存在（残存）する状態を意味し、主に組織的な理由が原因となり得る。例えば、

■ 容易に流用され易い資産に対する流用され易い機会の存在（規則運用的な理由）

■ 資産に関する統制の不備（制度的な理由）

→一般的な統制面：モニタリングが不十分、職務分離・相互牽制が不十分、重要な役割を担っている従業員が強制（有給）休暇を取得していない等

→物理的な統制面：自動化した統制に対するアクセス制限が不十分等

→説明責任に関する統制面：資産移動に関する取引の承認システムが不十分、記録と資産の網羅的・逐次的な検証が不十分、資産に関する記録管理が不十分、聖域・タブーの存在

【正当化】

一般的に不正を働く姿勢・正当化とは、不正を思い止まらせるような倫理観等が欠落させる環境と心理作用であり、不正を働かないという堅い意思が保てない状態を意味する。例えば、

- 資産の流用に関するリスクを考慮したモニタリングの欠如、または当該リスク軽減措置に対する無視・無関心
- 会社に対する不満（処遇等）の表現としての行動
- 少額な窃盗の容認（犯罪感覚の麻痺）
- 資産が流用された可能性（結果）を示す行動（ライフスタイルの変化等）

情報セキュリティ事案におけるこれらの要因を取り除くための牽制策とは、不正を犯すことを思い止まらせ（動機及び正当化事由に対する手当て）、問題の発生を抑制し、関連行為を牽制する（犯行機会に対する手当て）ということであり、具体的には、トップによる情報セキュリティ確保に対する強い意思と態度表明、情報セキュリティ教育・訓練、監視の徹底などの対策が挙げられる。

予防策としては、不正／過失行為の発生原因を排除した上で、利用権限の制限やアクセス権限の定期的見直し、また定期的な保守・メンテナンスなどが考えられる。また、検知策としては不正アクセスの監視、取得ログなどの相互監視などがあり、このような各種対策の組み合わせによる総合的アプローチが効果的である。

2）ルーティン・アクティビティ理論（日常活動アプローチ）

コーエンとフェルソン[10]（Cohen and Felson,1979）は、「社会変化と犯罪率の傾向-ルーティン・アクティビティアプローチ」の論文の中で、1947 年から 1974 年までの犯罪発生率の変化とライフスタイルの変化との関係を検討した。その結果、青少年人口が増加したこと、持ち運び可能な小型の家電製品が普及したこと、共稼ぎ家庭が増加したこと、伝統的な社会の連帯感が希薄化したことなど、1960 年代以降の市民のライフスタイルの変化が、犯罪発生率の増加に寄与することを指摘し、ルーティン・アクティビティ理論（routin activity theory）を提唱した。ここに示されるライフスタイルの変

[10] Cohen,L.E. and Felson,M.,Social change and crime rate trend:A routin activity approach,American Sociological Review,1979

化や、日常生活の行動の主な場が、家庭から、家の外にある職場や、その他の活動の場へと移行したことを背景としており、そうしたルーティンアクティビティ（日常生活行動）の構造変化こそが、動機づけられた犯罪者と好適なターゲットと監視者の不在が、時間と空間の中で収束・収斂する機会を増幅させ、結果として犯罪が増加したことを説明している。

ルーティン・アクティビティ理論では、犯罪成立を構成要素に分割し、犯罪の発生には、①動機づけられた犯罪者、②好適なターゲット、③違反に対処できる監視者の不在が時間的・空間的に収束することが不可欠であると考える。つまり、犯罪者の日常生活の“場”と被害者の日常生活の“場”が重なり合い、かつ犯罪を行いやすい環境的条件があるところで、犯罪が発生すると考えるのである。彼らの言う監視者というのは、警察官やガードマンのことではなく、地域住民や通行人など一般の人々を意味しており、いわゆる社会の眼が日常生活における犯罪発生を抑制させる役割を持つと考える。犯罪者のライフスタイルの変化だけではなく、被害者側のライフスタイルの変化にも注目し、違法な犯罪行為も日常の遵法的な行動パターンに依拠すると考える点で特徴的である。

このルーティン・アクティビティ理論に基づくと、時間的、空間的な場の中で、①動機づけられた犯罪者、②好適なターゲット、③監視者の不在の 3 つの条件が揃わないようにすることが効果的な犯罪予防となる。これらのうち、「動機づけられた犯罪者」を減少させる効果的な施策を立案することは困難であるが、「好適なターゲット」と「犯罪者が接点を持つ機会を減少」させること、監視の目を強化するなど、状況的な要因については比較的操作が可能である。フェルソン(11)(Felson,2002)は、犯罪予防のための対策として、犯罪を行わないような教育をすること、安全な環境を設計すること、犯罪を行う場を取り除くこと、さらに逮捕と訴訟手続き、裁判と有罪判決、刑罰と社会復帰までの 6 段階の過程が挙げ、犯罪発生を抑制する現実的な機会は、安全な環境を設計することと犯罪を行う場を取り除くことにあると指摘している。

これは、犯罪を未然に防ぐためにはこれらを同時に出現させないよう、「監視者」、「行動規制者」、「管理」が必要であることを示す。

3）状況的犯罪予防の理論

以上のように、ルーティン・アクティビティ理論や合理的選択理論では、不正者の意図や目標対象に対して、外部からのコントロールや抑止が困難な場合もある。一方、監視者の設置などによって外部からのコントロールが可能な「環境」を適切に定めることを主眼として、犯罪機会を低減・予防する研究に、状況犯罪予防の理論がある。

状況犯罪予防とは、「ある特定の犯罪問題を削減するための、極めて実践的かつ効果的な手段」と定義され、犯罪に関連する多くのプロセスや要因から犯罪を予防する方策を検討するために用いられるものである。

「状況的犯罪予防論」は、イギリス内務省調査部を中心として研究されてきた。1980 年代に入って R. クラーク、P. ナコーによる「設計による防犯」、K. ヘール、G. レイ

(11) Felson,M.,Crime and Everyday Life,3rd edition,Sage Publication,2002

コックによる「状況的犯罪予防」などがレポートされている。これらは以下の 4 つの基本原則から構成されている。

① 犯罪予防の目的は、犯罪の機会を減少させることにある
② 犯罪予防の対象は、具体的な特定の犯罪形態である
③ 犯罪予防の方法は、犯罪者の構成や環境の一般的な改善ではなく、犯罪発生の可能性がある環境に直接働きかけ、管理･設計および操作するものである
④ 犯罪予防の重点は、犯罪の際の労力とリスクを増大させ、犯罪から得ることができる利益を減少させることにある。

上記状況的犯罪予防の理論を踏まえ、情報セキュリティに関して、各プロセス等を踏まえた企業としての人的・組織的対策の視点を整理すると下記の通りである。

イ） 予防策の増強

不正を物理的・論理的に予防する企業・組織の対策としては、ファイルサーバへのアクセス制御や脆弱性パッチの適用、暗号化、USB 等外部ポートの制限、ソフトウェアによる外部装置への書き込みの無効化等が考えられる。

また、不正の対象となる物（人）へのアクセス性をコントロール・制限することが重要である。物や情報などの対象へのアクセス可否を左右するのは「資格（アクセス権限）と必要性」の要件であるが、これについては対象（情報）ごとに決めておく必要がある。ある人物が、例えアクセスの「資格」を有している場合でも、状況からその「必要性」がない場合には、入口での規制が必要である。例えば、その組織の一員であり入室資格を有している場合でも、通常は、深夜休日の入室は、業務実施との関係で「必要性」がないのであれば、そのアクセスについて確認できる仕組みと、アクセスすることへの正当性や理由等を確認する運用が必要となることなどが挙げられる。この要件を、十分に吟味して定めることが、「入口でのコントロール」による、内部要因による事故防止の成否を決めることになる。

その意味では、アクセスログを記録することは極めて重要であり、後日、調査の可能性を残しておくことで、内部不正予防の意味がある。

さらに、対象（情報）に近づけないようにすることは、魔が差して生ずる従業員の犯行企図を、芽のうちに摘み取る対策も検討しなければならない。

犯行ターゲットへのアクセス性や、持ち出し容易性を制御し、職場内で犯行対象物を扱う機会を減らすことも予防策を強化する。重要エリアへの出入制限、重要情報へのアクセス制限､現金や貴重品取扱機会の低減などを具体的施策として用意し、犯行企図の萌芽を摘み取るために、「犯行が出来ない」ようにすることが重要である。

ロ） 発覚リスクの増強

犯行が発覚する仕組みを構築しておけば､抑止力強化として働くものと考えられる。ここでは、防犯意識の向上や拡大、匿名性の排除、職場管理者の利用、公共監

視の強化等があげられる。ここでは、写真付き社員証の常時携帯、グループ ID の禁止、侵入検知システムの導入等が考えられる。

また、組織内で行われている行為を、常に見えるようにしておくことが重要である。視界を妨げる物を整理する、レイアウトを工夫する等によって、死角をできるだけ排除することが基本である。

さらには、PC のディスプレイの表示を誰もが見えるようにする、メールのやり取りを見えるようにしておくなどの方策も考えられる。夜間や休日などの単独勤務を禁ずることも、“時間的な死角”を排するという意味で、この自然監視性の範疇に入る。

その他、組織内で行われた行為に対して、その行為主体を確認することができるようにしておくことで、不正の発生を防止する効果が期待できる。具体的には ID カード等による出入管理システム導入と社員行動の把握、ID 常時装着の徹底などによって実現する。プリントアウトや情報アクセスのログなど、総合的なログ管理を行うことも有効である。

異常が発生した場合の、状況のトレーサビリティを高め、事後の監査・追跡を行いやすい仕組みを作ることで、内部不正に対する牽制を行う。「魔が差す」ことは、その人間の組織や社会における地位や立場に関係なく起こり得ることに留意する。組織で働く「すべての人間」の行動について、匿名性を排除、行動の主体を明確にし、責任分岐点がきちんと認識されるようにすることが重要である。

ハ) 見返りの抑制

犯罪が割に合わなければ、犯行を抑止できるものと考えられる。ここでは、犯罪対象物の隠蔽、犯罪対象物の排除、所有者の明確化、犯罪利益をなくす等が挙げられる。対策としては、重要情報の限定提供、車上荒らし対応、廃棄 PC・ディスクの破壊、不要個人情報の破棄、電子署名/電子透かし等の利用、オークションサイト情報の確認等がある。

物や情報などの内部不正の対象を、物理的に取り去り、置かない具体例としては、以下の通りである。例えば、パソコンや情報媒体の廃棄にあたっては、記録された情報を確実に消去し、情報の確実な消去が保証されない場合には、情報記憶媒体を物理的に破壊した後に、廃棄する。パソコン、情報媒体の廃棄に際しては、無知によるミスを発生させないための従業員教育・啓発も重要である。

また、物や情報などの内部不正の対象に対して、何らかの方法で ID を付与することで、不正に持ち出されたとしても、所有者が判るようにしておくことである。在庫などの内部不正の対象になり得るものについては、その唯一性を証明できる製造番号等の記録を残しておくことも有効である。在庫や備品など、現金以外の物品が組織内部から不正に持ち出された場合、その物品は、何らかの方法・ルートで転売され、換金されることが多い。そのため、組織内部から物品が不正に持ち出される事実があった場合、ネットに流れるオークション情報や裏情報をチェックし、もしそこで不正に持ち出されたことが明らかな物品を発見した場合は、警察等への速

やかな届け出や法的措置を取る。

ニ）誘因・挑発の排除

犯罪を行う気持ちにさせないことで、犯罪予防を図る必要がある。

対策としては、適切な人事管理、正しさを追求する組織風土、ヒヤリ・ハットへの対応と根本原因分析等が考えられる。

自分の能力が発揮できて、周囲との良好なコミュニケーションがとれる自分の「社会的な居場所」としての「快適な職場環境」がある場合、人は、その快適な環境を失うことにつながる内部不正をしようとは思わない。逆に、過大なフラストレーションやストレスを感じ、コミュニケーションも十分に取れない職場では、従業員の職場に対するネガティブな感情が膨らんで、そのはけ口として内部不正を働く犯罪企図が発生しやすくなる。

高利の借金を抱え、その返済に追われる状況に追い込まれた人間は、強いストレスを抱えて、それから逃れるために、横領などの内部不正に至ることがある。面接やカウンセリングなどによって、個人のストレス等を把握し、彼らが抱える問題を認識した場合、その解決を手助けすることは犯罪誘因を取り除き、内部不正を防ぐうえで特に有効である。

個人的な借金の要因となる交友関係や、なんらかの依存症的悪癖がある場合、それに対応することも重要である。

また、相互不信や部門間軋轢等を内包する組織では、そのはけ口として内部不正が発生する確率が高くなる。そこで、組織内における相互不信や対立の要因を除去し、組織内にわだかまりや、マイナス要因としての対抗心や不信感が蓄積することがないようにする対策が重要となる。組織の合併などで組織内に派閥的グループができてしまった場合には、意識してそれを解消する必要がある。具体的には「組織の意志」としての、派閥を超越した判断基準を明示する、派閥や出身組織を考慮しない「適材適所」人事を行うなどの施策が重要になる。

組織には、従業員の一人ひとりがもつ感情や価値観のぶつかり合いの結果として、鬱憤が溜ることがある。悪い形で鬱憤が蓄積した組織では、そのはけ口として内部不正が発生しやすい。それゆえ、組織の個々の構成員が、己の感情をコントロールし、組織内に悪い形の鬱憤が溜りにくいようにする対策が重要である。

具体的な施策として、組織を構成する一人ひとりの不平・不満や希望を適切な方法で吸い上げ、それに対応する機会を、組織の制度として意識的に設けることが挙げられる。

昇格降格などの人事異動や、業績評価などを行うタイミングは、人の感情が揺れ易く、結果として組織内に鬱憤が溜りやすい時期でもあり、制度として面接を行う機会を設け、不平や不満の緩和を行うのが望ましい。評価項目と評価基準を明確にした、透明性のある業績評価の実施による納得感のある処遇の実現が、組織に鬱憤を溜めないための鍵である。

また、組織内で「セクハラ」や「パワハラ」などのハラスメントが横行していた

りすると、組織内に鬱憤を蓄積させる原因となる。そのため、どのような行為がハラスメントにあたるかを周知し、研修による啓発を行って、組織内でハラスメント行為を起こさせない体制を作ることが重要になる。

組織によっては、過去からの悪しき因習によって、半ば公然と内部不正が行われていることがあるかもしれない。また、法規やガイドライン等の変更によって、過去は認められていた行為が、突然、不正となる場合もある。組織文化として、当たり前のように内部不正が許容され続けている場合は、それを是正するには相当のエネルギーを要する。

このような場合は、組織のトップが、悪しき因習からの決別と新しい組織文化の創設を組織の構成員一人ひとりに対して明確に宣言することが必要不可欠である。また、善良かつ公正な「外部の眼」の導入と、かつその「外部の眼」が「組織文化を変える権限を持っていること」の二要件も重要である。

ホ) 弁解余地の排除

犯罪理由を正当化させてはいけない。特に「属人風土」的組織では、会社ぐるみの不正が形成されてしまう可能性があり、それを防止する必要がある。

この対策では、セキュリティポリシーの策定、社内規程／セキュリティポリシーの教育・研修、関係者への機密保持契約の締結、ポスター／画面バナー等の活用による告知、情報の重要度設定、無権限者へのシステムによる注意喚起、送信メールの管理者コピー、法令遵守教育・周知等が考えられる。

内部不正行為に及ぶ弁解の余地をなくし、たとえ従業員が犯罪企図を持つに至ったとしても、実際の犯行として顕在化することを抑える対策である。組織における、多くの内部不正は「言い訳」によって自己正当化され遂行される。一部業界で問題となることの多い「談合」も「組織のため」を言い訳として、正当化されることが多い。内部不正行為に及ぶ前の自己正当化に利用される弁解の余地を取り除くことで、たとえ従業員が犯罪企図を持ったとしても、実際の犯行にブレーキをかけておくのである。

状況的犯罪予防の情報セキュリティアプローチ

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 ・組織の融通性との勘案 ・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
出入口でのコントロール	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	・小さな不正を許さず姿勢維持 ・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

参考：財団法人社会安全研究財団「環境犯罪学と犯罪分析」、独立行政法人情報処理推進機構「組織内部者の不正行為によるインシデント調査」

5）割れ窓理論

アメリカの犯罪学者ジョージ・ケリング[12]は、大都市における落書きや割れた窓を放置しておくと、街が荒れ、無秩序となって凶悪犯罪などが多発するなど、悪の連鎖現象が現出することを『割れ窓理論』として考案した。主な論点は、以下の二点である。

（1）非社会的・非道徳的なことが「放置」されていると、モラル低下につながる。

（2）「放置」に対して、声を上げることができない雰囲気＝「傍観者効果」が働く。

企業・組織内におけるコンプライアンス違反が「放置」されていると、社内規定や上司の指示・命令をタテマエ的であると認知し、社員間の信頼関係が崩れ、社内モラルの低下につながることが考えられる。

単に「放置」しないだけでなく、さらに一歩進めて、内部不正を発生させる内部要因の自然的発生の抑制まで視野に入れた場合、労務環境（労務形態・労務ルール・労務実態）に働き掛けて、不正を引き起こすことが、誰の眼から見ても、合理的にも、長期的にも、割に合わないという理解に至る状況（仕掛け・シナリオ）を創出し、周知できるよう必要な対策を明確に打ち出すべきである。

[12] G.L.ケリング、C.M コールズ、小宮信夫監訳(2004)「割れ窓理論による犯罪防止-コミュニティの安全をどう確保するか-」文化書房博文社

そのためには、何と言っても不正を生まない組織文化の醸成こそが各種対策を有効なものとすることを強く認識する必要がある。本来善良であるにも関わらず、性弱という人間の本性に働き掛けて、「不正の誘惑に負けない」「不正なる企図はそもそも持たない」「不正行為結果の影響（デメリット）は、必ず不正動機の思惑（メリット）レベルを上回る」とする確固たる自覚と信念を持たせ、内部不正を受け付けない、或いは生まない組織文化の醸成による組織の持続的な発展･定着を真に志向すべきである。

これは、犯罪原因論の組織運用・組織文化への適用である。ただ、その適用に当たっては、組織の構成員たる人間は、組織から離れたパーソナルな「一個人」でもあり、それぞれが人間的弱さを内在しているということを忘れてはいけない。問題は企業として、その弱さを際立たせない組織文化の醸成・構築に取り組むべきところにある。

何もこれは、内部不正に絡んだ情報漏洩に限った話しではない。すべての企業不祥事に関して、従業員・幹部に対する企業倫理教育に真摯に取り組む実践の姿勢は、そのような組織文化のなかで強固に、かつしなやかに育まれるものであることを全企業人が、再度深く胸に刻み込むべきである。

4 故意による情報漏洩

（1）意識調査

独立行政法人情報処理推進機構（IPA）技術本部セキュリティセンターは、2012 年 7 月 17 日付けで「組織内部者の不正行為によるインシデント調査」[13]の報告書を公表した。

この報告書は、国内の一般企業の 3,000 名の社員と 110 名の経営層やシステム管理者に対して、内部不正に関する意識調査を行ったものである。

「内部不正の気持ちを低めると考えられるもの」の設問には、社員の回答は「社内システムの操作の証拠が残る（54.2%）「顧客情報などの重要な情報にアクセスした人が監視される（37.5%）」が上位を占めた。一方で、経営者やシステム管理者の回答は「開発物や顧客情報などの重要情報は特定の職員のみアクセスできる(20.9%)」「システムの管理者以外に、情報システムへのアクセス管理が操作できない（12.7%）」が上位を占めている。

情報システム運用における内部不正抑止のために有効と考える対策において、管理される側（従業員）と管理する側（経営者・システム管理者）とでは、内部不正に対する観点の違いが見られる。従業員は、ログが残るという行為の痕跡に対して脅威を感じているのに対し、経営者・システム管理者は、アクセスさせないというアクセス制御という水際防衛を重視していることが分かる。

[13] 独立行政法人情報処理推進機構(2012)「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-」http://www.ipa.go.jp/security/fy23/reports/insider/index.html

（2）情報システム運用にかかる内部不正抑止策の有効性の検証

本調査結果から判断すると、経営者等が講じているアクセス制限の方策は、内部不正への抑止力になっていない可能性がある。

不正は発生のメカニズムとしては、「不正の機会」、「不正の動機」「不正の正当化事由」に着目した不正トライアングル理論が有名であるが、上記調査結果を、このトライアングルの各要素に対する対策として当てはめた場合、従業員（システム利用者）は「内部不正の気持ち（動機）を低める」対策を脅威に感じているのに対し、経営陣・システム管理者は、「アクセスさせない(不正の機会を作らない)対策が有効であると考えているものと分析できる。

それでは、この仮説をベースに、情報システム運用にかかる内部不正抑止策について考察してみる。なお、今回は情報システムを例にとって検証を行うが、この検証は、不正トライアングル理論に基づく内部不正抑止策として、「不正の動機」に着目すべきか、「不正の機会」に着目すべきかという視点で捉えると、広く内部不正対策全般に対しても普遍性を有する可能性がある。

内部不正を抑止する目的は、内部不正によるロスの極小化（内部不正を実行できる機会の減少、動機の抑制、万が一の際の経済的損失等の損害の極小化）にある。とすれば、検証のための事例としてまず考えなければいけないのは、内部不正によるロス、すなわち、企業にとっての損害が大きいケースについての対策である。この点、過去の個人情報漏えい等に関するインシデント報告等を見ても、内部不正に係る情報漏洩で被害の大きいケースは、正当なアクセス権限を持つ人物が正当な作業手順で、不当なデータ収集・持ち出しを故意に行ったというケースである。

ここで注目すべき点は、「正当なアクセス権限を持つ者」による「故意」の行動である。正当なアクセス権限を有する以上、そもそもアクセス制御というシステム管理者側の内部不正対策は、全く抑止力として機能していない。したがって、対策として考えた場合、社内システムの操作ログが残る環境を構築することで、不正の試行や着手としての故意の行動の痕跡というミドルクライシス(14)を早期に発見して被害を最小限に食い止める、あるいは、ログ解析により内部不正痕跡が残ることによって自分が処分される等の不利益は受けたくないという形で、行為者の不正の動機に直接アプローチする対策の方が有効であることを意味している。

また、退職予定者等の不利益処分の抑止力が働かない行為者にとっては、このログ取得の対策にも一定の限界があることは認められるが、それとて、不正競争防止法等での刑事的対処も可能であることから、アクセス制限のように全く抑止力がないということはない。

ミドルクライシスとは、企業に内在している様々な「リスク」が、対外的な顕在化（＝「クライシス」）に発展する前の姿（日々、業務上発生している種々のトラブル、問題事象であって、いわゆる「今そこにある危機」「若干の危機」）であり、さらには、過去に発生した「ミ

(14) 株式会社エス・ピー・ネットワーク渡部洋介(2011)「ミドルクライシスマネジメント～内部統制を活用した企業危機管理 vol.1 反社会的勢力からの隔絶」

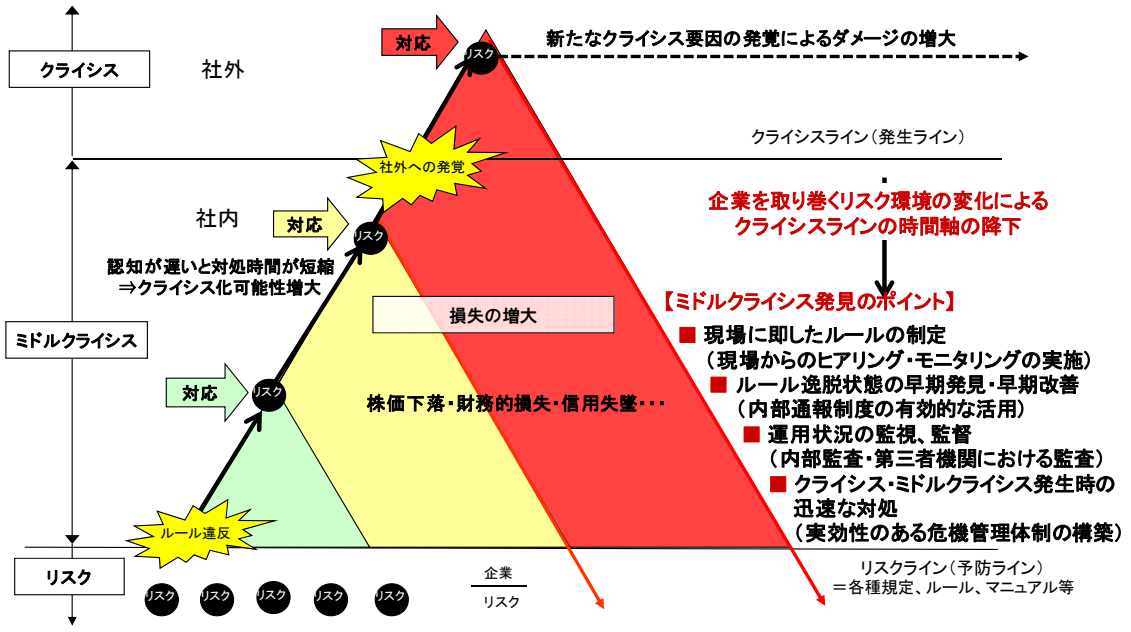
ドルクライシス」が、もはや社内で忘れ去られてしまうような状態が放置された状態のことと当社では定義している。

企業は、設立したその瞬間からさまざまなリスクを背負い、各ステークホルダーとの関係も生じる。例えれば、リスクが氷山の一角として海面より頭を出している状態であり、それらは必ずクライシス化する（あるいは必ず繰り返される）ことを認識しておくべきである。

そして、そのステークホルダーに対する責任を果たすべく、リスクを水際で予防するための各種規程、ルール等を定める。しかし、それらでは対処しきない種々の事象に対応する（あるいは、対応していかざるを得ない）局面も生じ、また、規程やルール自体が形骸化することもある。

やがて、現状や実態とそれらルール等とが乖離し、ルール違反等が発生、常態化することによって、社内のリスクライン（予防ライン）を超えて、「リスク」が「ミドルクライシス」として社内的に顕在化してくる。

このミドルクライシスが多発する状況を社内で放置すれば「クライシス」（危機、問題発生）へと発展し、対外的にその事態が発覚することになる。そして、内部告発や、最近では、2 ちゃんねる等への書き込みやツイッターやブログ等での情報発信（意図的か無意識を問わない）などによって、社内の情報が早い段階で社外に流出する状況が散見されるなど、対外的な発覚時点であるクライシスライン（問題発覚ライン）が急速に低下している。ミドルクライシスが対外的に顕在化するまでの猶予（社内でミドルクライシスに対処できる時間）が短縮される傾向にあることにも注意が必要である。



ミドルクライシス

さて、不正の痕跡を残させるという観点からは、

①ログ監視ツールの導入や運用方法の改定、ファイルの暗号化などを実施する

②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）

③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、例えば、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

等を実施して、内部関係者がデータ等を不正に操作したという不正の事実が、確実に分かる体制の構築が重要になる。

また、ISO27001 では、ユーザー操作履歴や各種セキュリティ事象を記録した監査ログの取得と保存、情報システムの設備の使用状況の監視、アクセス制御方針の確立、ユーザー登録や登録削除についての手順、パスワードの割当てに関する管理プロセス、ユーザーのアクセス権の見直し、パスワードの選択および利用時のユーザーへの要求事項など、アクセス管理全般に亘り、アクセス制限とログの取得両面からの対策を定義していることを付記しておく。

(3)情報システム運用における特権アカウントの管理

内部不正の抑止という観点から、情報漏洩防止や内部不正防止をはじめとする技術的セキュリティ対策と、内部統制における IT 全般の統制についての対策を検討した場合、いわゆる特権 ID の管理が重要になる。

特権 ID とは、システム設定の変更、ユーザーアカウントの新規作成や更新・抹消、アプリケーションのインストール、ファイル内容の閲覧などを唯一おこなえる特別な権限を持つ ID である。

具体的には、UNIX や Linux なら「root」、Windows なら「administrator」といった ID で、サーバ OS、ネットワーク機器 OS、データベースなどであらゆる操作が可能となる。

この特権 ID が悪用されると、サーバ OS、ネットワーク機器 OS、データベースなどであらゆる操作が可能である以上、システム設定の不正変更やマルウェア等の不正情報取得ツールのインストール、そして機密情報へのアクセスや持ち出しまで、あらゆる形態の不正行為が可能になってしまう。コンピューターウイルスや不正アクセスにより、リモートコントロールや特権 ID 情報の取得を行おうとするハッカーたちの狙いも正にここにある。

このように、内部不正によって情報漏洩が引き起こされる要因の 1 つとして、この情報システム管理用の特権 ID の管理が不十分であることが挙げられる。

情報システムの運用で高い操作権限を持つ特権 ID による事故・不正は、企業内の情報を全て握られ、コントロールされることを意味しており、極めて重大なリスクである。情報セキュリティマネジメントの国際標準である ISO27001/ISMS の要求事項でも、「特権の割当及び利用は、制限し、管理しなければならない」、「すべての従業員、契約相手及び第三者の

利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了時に削除し、また、変更に合わせて修正しなければならない」としている。

見方を変えれば、特権 ID の管理レベルは、当該企業の内部統制（システム管理体制、顧客保護等管理体制）や危機管理体制の実効性が問われる問題であるから、経営者としては、情報システム担当者に全てを一任することなく、適宜、その状況等を把握しながら、人事ローテーション等により、特権 ID 利用による不正の発生を抑止していくように努めなければならない。

内部不正対策としては、システムを利用する立場の従業員による不正ばかりに目が行きがちである。一方、システムを管理する立場の従業員（あるいは役員）による不正のリスクは、企業存続そのものを揺るがしかねないより重大な経営課題であることを改めて認識しなければならない。

なお、金融情報システムセンター（FISC）の「金融機関等コンピュータシステムの安全対策基準・解説書」[15]や PCIDSS（Payment Card Industry Data Security Standard）など、金融業界の各ガイドラインでも特権 ID の管理が明記されており、アカウント管理の不備は金融庁検査の指摘事項ともなり得る。

金融機関等コンピュータシステムの安全対策基準・解説書（一部抜粋）

各種資源、システムのアクセス権限を明確にすること
パスワードが他人に知られないための措置を講じておくこと。
各種資源、システムへのアクセス権限の付与、見直し手続きを明確化すること。
ファイルに対するアクセス制限機能を設けること。
本人確認機能を設けること。
ID の不正使用防止機能を設けること。
アクセス履歴を管理すること。
不正アクセスの監視機能を設けること。

[15] 金融情報システムセンターの「金融機関等コンピュータシステムの安全対策基・解説」

管理者アカウント（特権 ID）の管理に関する ISO27001 の要求事項（一部抜粋）

アクセス権の削除	すべての従業員、契約相手及び第三者の利用者の情報及び情報処理施設に対するアクセス権は、雇用、契約又は合意の終了後に削除しなければならず、また、変更に合わせて修正しなければならない。
監査ログ取得	利用者の活動、例外処理及び情報セキュリティ事象を記録した監査ログを取得しなければならず、また、将来の調査及びアクセス制御の監視を補うために合意された期間、保持しなければならない。
システム使用状況の監視	情報処理設備の使用状況を監視する手順を確立しなければならず、また、監視活動の結果を定めに従ってレビューしなければならない。
ログ情報の保護	ログ機能及びログ情報は、改ざん及び認可されていないアクセスから保護しなければならない。
アクセス制御方針	アクセス制御方針は、アクセスについての業務上及びセキュリティの要求事項に基づいて確立し、文書化し、レビューしなければならない。
利用者登録	すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備えなければならない。
特権管理	特権の割当て及び利用は、制限し、管理しなければならない。
利用者アクセス権のレビュー	管理者は、正式のプロセスを使用して、利用者のアクセス権を定められた間隔でレビューしなければならない。
パスワードの利用	パスワードの選択及び利用時に、正しいセキュリティ慣行に従うことを、利用者に要求しなければならない。
利用者の識別及び認証	すべての利用者は、各個人の利用ごとに一意な識別子（利用者 ID）を保有しなければならない。また、利用者が主張する同一性を検証するために、適切な認証技術を選択しなければならない。

(4)特権 ID やシステム管理者権限に対する対策の現状

管理者用アカウントの適切な無効化等の確実な措置は、企業・組織にとって当然実施されていると思われがちである。しかし、IT システムが規模を拡大しているなかで、サーバ仮想化によるサーバ台数の増加し、ルーター、セキュリティ・アプライアンスなどの管理者用アカウントの管理は一層煩雑になっている。それに伴い書類上で削除されているはずの当該アカウントが有効であったりするなどの現実がある。

実際の企業の現場では、情報システムの運用において「特権 ID を共有で利用している」、

「特権 ID 利用の申請ルールが徹底されていない」、「申請なしに権限を与えてしまう」、「証跡不足により、誰が・いつ・なにをしたか特定できない」、「退職者、異動者の ID 削除漏れが多い」といった諸問題が残存したまま潜在化した漏洩リスクとなっていることを認識する必要がある。

この特権 ID やシステム管理者権限の悪用は、情報セキュリティ分野の制度が整っているとされている組織・企業においてでさえ、起こり得ることを改めて認識する必要がある。

(5)デジタル・フォレンジック 1

内部不正による情報の漏洩原因をつかむためには、調査時点でアクティブなデータ以外にも、既に削除されたデータやメールなどが重要な情報源となる。内部不正や不祥事への対応として、一次不祥事の事実調査や社内処分だけではなく、構造的な不正発生原因にまで遡ることが必要であり、それが二次不祥事や再発防止策に繋がる。

情報漏洩や不正の原因を解明するための技術的アプローチとして「デジタル・フォレンジック」[16][17]というデジタルデータの証拠保全および調査・手法がある。

「ライブドア粉飾決算事件によるメールや重要ファイルの削除による証拠隠滅」「大相撲八百長問題による力士たちが携帯電話のメールのデータを消去、携帯電話を破壊して証拠隠滅」「大阪地検特捜部で主任検事が証拠物件であるフロッピーのファイル日付を改竄」等のニュースからも分かるように、これらの事件で警察・検察当局でも「デジタル・フォレンジック」による調査手法がとられ、隠滅・改竄・消去されたデータが復元されたことによって注目を集めた。

「デジタル・フォレンジック」は、パソコンやサーバ、さらに携帯電話やスマートフォンを介した犯罪や不正行為に対して、削除されたデータやメールなどの不正や犯罪に関わる重要な情報を復元可能とする。また、被害を受けた企業や組織が加害者とされてしまう「なりすまし」や「踏み台」などの外部からの不正行為も、フォレンジックの活用により、事実関係を明らかにすることができる。

さらに、時系列に外部接続した外付け HDD の使用履歴や USB メモリの利用状態、インターネットの利用履歴、使用頻度、持ち出されたデータ、ダウンロードした画像やファイル、暗号化したファイルなどのパスワード解析など、断片化したファイルや機密文書の欠片、画像ファイルの一部分だけを復元することも可能になる。

企業や組織にとっては、情報漏洩やデータ改竄などのインシデントの防止はもとより、早急な対応による被害拡大の防止、事後の再発防止や信頼回復も大切な課題とされている。不正の社内調査における「白か黒」の事実認定の決め手としても「デジタル・フォレンジック」

---

[16] 特定非営利活動法人 デジタル・フォレンジック研究会(2006)「デジタル・フォレンジック辞典」日科技連出版社

[17] Michael G. Solomon,K Rudolph,Ed Tittel 、AOS 法務 IT 推進会・訳、佐々木隆仁 、柳本英之・監(2012)「デジタル訴訟の最先端から学ぶコンピュータ・フォレンジック完

を活用した手法が、今後より一層普及していくと考えられる。

(6)デジタル・フォレンジック 2

「デジタル・フォレンジック」調査のプロセスは大きく分けると、1.「証拠保全」、2.「解析」、3. 「報告」の 3 つの段階から成り立っている。

1.では、調査対象媒体のデータを全く書き換えることなくコピーして、証拠の保全を行なう。これは、対象媒体のデータが改変されないようにする機能（書き込み禁止機能）を持つ専用機を用いることで、調査対象媒体のデジタルデータが改変されずに複製される。
2. 次に、データの保全が終わると証拠となり得る情報を抽出し、解析を行なう。これはゴミ箱から故意に削除したファイルを復元したり、インターネット閲覧、メール送受信履歴を取得することで証拠の隠滅や、コンピュータで何が行なわれてかを浮かび上がらせる。
3.では、解析した結果をもとに、訴訟資料や不祥事の報告書として活用する。

「デジタル・フォレンジック」調査は、本件のような事例以外にも、不正会計や不正アクセス調査、労務管理(過労死)などに関する訴訟のための証拠収集にも有効であるといえる。

また「デジタル・フォレンジック」の活用事例は公表されることがほとんどないが、警察による「電磁的記録の解析等の技術支援件数」によっても推測でき、その増加傾向は明らかである。

(7)デジタル・フォレンジック 3

2012 年には、証券取引監視委員会の調査によって、業界最大手の証券会社、その他大手などが軒並み公募増資に関わる公表前の情報を機関投資家に漏洩させたことが明らかになった。一例を挙げると、企業が増資を計画する際に、調整役のシンジケート部やアナリストに増資情報が集まる。この情報が外部に漏れないようにするための情報の壁(ファイヤーウォール）が存在するが、営業部が、この壁を越えて情報を収集し、機関投資家に増資情報を耳打ちしていたという。

本件のようなインサイダー取引に関連する情報漏洩も、スマートフォン、携帯電話、パソコンを通じて発生している場合が多く「デジタル・フォレンジック」を活用して証跡を辿ることが可能である。

「デジタル・フォレンジック」を活用したインサイダー取引の調査方法としては、

1. サーバ・パソコン・スマートフォン・携帯電話から証拠の保全（元のデータとの同一性が証明できる形式での複製を行なう）
2. 保全された証拠データの復元・調査
3. 機密ファイルへのアクセスログ、メールサーバー、通話履歴、メール、サイトへの閲覧履歴、位置情報などの解析

※シンジケート部、アナリストとのやりとりや、機密ファイルへのアクセス。機関投資家との隠語でのやり取りなどが把握できる。

先の大手証券会社によるインサイダー取引では、再発防止策として、機関投資家向け営業のチャット機能の制限、通話録音機能付き携帯電話使用の義務化、通話録音保存期間の延長等、IT 機器の使用を制限するとしている。

その他、営業部との情報伝達の見直し、営業部門とシンジケート部、アナリストとの接触制限、コンプライアンス研修の強化、職務倫理研修の定期的実施を挙げているが、組織のモラルハザードが蔓延している状況では、ルールの強化だけでは再発防止に限界があり、特に IT 機器の制限に関しては、十分とはいえない。

インサイダー取引に関連する情報漏洩対策は、事後対策としての「デジタル・フォレンジック」と事前対策としてのログ管理によるパソコン・スマートフォンの利用状況の記録やその周知、機密ファイルへのアクセス制限等による不正行為を防止し、内部統制を強化する上でより重要になると考えられる。

また、SEC（証券取引等監視委員会）の見解にあるように、証券業界において重要情報の漏洩が慣例・常態化していることを鑑みると、規制や対策の穴への継続的の対処が必急務である。

5　過失による情報漏洩

企業・組織における情報漏洩の要因は、USB メモリ等の記憶媒体の紛失や従業員のデータ持ち出し、紙媒体紛失等の内部要因によるものが依然として多くの割合を占めている。下記事例のような持ち出しによる情報漏洩は、明文化されたルールがあるにも関わらず、日常的にルールを逸脱する行為の「自己正当化」「ルールに対する規範意識の麻痺」がその背景にある。

厳密にルールに照らせば正しくないという認識を持ちつつも、提出期限や納期などのやむに止まれぬ事情から、「作業・仕事を早く終わらせたい」という現実的な要請があり、その行為を日常的な行為として、いわば実務慣行として定着化されてしまう。そうしたルール違反の感覚が希薄化（「麻痺」）し、次第に標準化され、ローカルルールとして「正当化」されてしまう状況が、頻発する情報漏洩の背景にあると考えられる。

○　小学児童情報入った USB 紛失　男性教諭が校外に持ち出し／北海道
→学校は個人情報が入った USB メモリの校外への持ち出しを禁止していた。

○　個人情報：小学校教頭の車から児童名簿盗難／山梨
→同小は名簿の校外持ち出しを原則禁じていた。

○　個人情報：学校職員、千人分の情報入り私物 USB 紛失　市教委に届き発覚／新潟
→同市教委によると、口座番号などが入った USB メモリは通常金庫で保管され、学外への持ち出しや、私物 USB メモリへのコピーを禁止していた。

今回紹介した事例のように、禁止されているはずの記録媒体の持ち出しや、情報の複製等の行為の「常態化（ルールの逸脱が日常化してしまう）」が、結果的には車上窃盗の被害や紛失、不正アクセスによる情報漏洩などを発生させている。

これらの行為は、当事者自身には、会社に損失を与えようなどという悪意や企図はないものの、ローカルルール（本来のルールが変形し現場だけで運用されているルール）により運用されたり、管理要件が不明確となっている領域に対して、組織や業務環境が都合のよいルールの解釈を許してしまっている（統制環境）結果と捉えることができる（内部統制システムとしての脆弱性）。

このような現実の背景には、実際の現場では、社内ルールなどの厳守よりも、契約上の納期の厳守の方が優先されてしまう実態がある。

ルール設定当初は情報漏洩防止のために、冗長化された手続きやチェックも必要であるとしていたものが、業務効率優先の組織運営のために形骸化し、自宅や社外への情報の持ち出しといった行為がなし崩し的に行われ、最終的にはそのルール逸脱のやり方が新たなローカルルールとして形成されてしまっていると考えられる。ましてや、各組織でリストラや人員整理が進められていれば、一人ひとりに掛かる業務負担は当然重くなり、効率性を求めるあまり、ルールの形骸化やローカルルール化に拍車がかかりやすい。

その上、本来はルールの適正な運用を管理すべき上司や所属長が業務効率や売上げ向上のために（そして、部下の業務効率という「自己正当化」のために）、日常的なルール逸脱が黙認されることによって、職場全体の情報漏洩リスクに対する認識が希薄化し、個々のリスク感覚も麻痺するという悪循環に陥る。さらに、自宅での業務を推奨・命令する場合に至ると、仕事とプライベートの区別もつきにくく、いわばプライベートの延長線で、緊張感が緩んだ状態で業務が実施されやすく、情報漏洩リスクは一層高まることになる。

（1）悪意のないルール違反への対策

情報漏洩にかかる事故に限らず、ルール違反は（そもそもルールを知らない場合を除けば）本質的には意図的な行為である。人は、「人」の特性上、不遵守行為による“損失と利益”を天秤にかけ、見込まれる損失より利益（「楽」ができるという本人にとってのメリットも含む）が上回ると判断する場合には、違反に手を染めてしまう[18]。

組織・企業としては、「人」の心理や行動に関する理解を深めた上での、環境面での対策を検討する必要がある。

---

[18] ジェームズ・リーズン（塩見、高野、佐相訳）(1994)「組織事故 - 起こるべくして起こる事故からの脱出」日科技連

1）業務量や負荷の適正化

過大な業務量・作業負荷や無理な作業スケジュールを強いることは、集中力や注意力を散漫にさせ、その結果として、単純ミスや社内規則・ルールを逸脱した情報の持ち出し行為を誘発しやすい。ルールに違反した情報の持ち出しを防止するためには、業務量や負荷の適正化を保つことがまずもって大切である。

もともと、マニュアル化された作業や繰り返し作業には、人によって得手不得手があるが、それ以外にも、多くの人に共通して不得手な作業がある。それは、時間的プレッシャーのかかる作業、注意が分散する作業、安閑と多忙が混在する監視作業などである。これらは、今のところ、タイムシフトや適材配置などを工夫し、対処せざるを得ない。

また、作業の効率化や省略の誘惑にかられやすくなるし、単純ミスによる漏洩のリスク（オペレーショナル・リスク）も増すことから、そのような作業遂行上のリスクも予め認識しておくことがより重要となる。

さらに、情報の持ち出しについては、基準を曖昧にせず、その情報が漏洩したリスクを想定･勘案し､明確にした上で厳格にルールを設定し運用することが重要である。

情報を持ち出していなければ漏洩しなかったと推察される事例が散見されており、情報は決まった場所で取り扱い､そこ以外には持ち出さないという意識を徹底させるのが大前提であるから、これを厳守できるような作業環境の整備・構築が不可欠である（私物の持込み禁止エリアでの作業、バックチェックの実施などの「行動」制限がその中心となる)。

2）作業指示の明確化

不明確な作業指示やあいまいな作業手順は､確認の省略や情報の持ち出しなどの判断ミス・ルール逸脱を誘発する。機密情報や個人情報を取り扱う業務は、社員だけではなく派遣社員や臨時雇用者が担当することも念頭において､対策を検討しなければならない。

対策としては、まず、作業のルールや手順自体が本当に作業の実態に整合したものであることを確認した上で、具体的で明確なルールを策定することである。特に、作業者が適切な判断を下し、必要な確認手順を省略せずに実施できるよう、ルールや手順の意味、目的を明示し、確実に理解させる必要がある。逆に、日常的な逸脱や軽微な手順の変更を黙認する風潮や手順の変更・逸脱等があっても、周囲や管理者が発覚しにくい状況は、ルール逸脱を助長すると考えられる。

なお､個人情報の取り扱いに関する法律の基本事項や組織としての対応方針は､常に、関係者全員に周知徹底し続けることが重要である｡漏洩事故に関する基本的な教育や意識啓発は、一過性のものとせず、定期的に実施することで浸透が図られる。

情報漏洩に関する事故・トラブルについても、社内の事例や他社事例を交えて、その事故に至るまでのプロセスや結果的に被った損害を周知することが効果的である｡漏洩事故事例の収集・分析といった取り組みは、翻って自社の状況と照らし合わせることを

通じて、日常の業務の中に潜在化するリスクを発見する端緒となり、組織として情報を共有し活かし、実態に適合した解決策を見出すことに繋がると思われる。

3）個人の姿勢や価値観

個人の姿勢や価値観を会社の方針に沿ったものとしていく取り組みは、組織内での悪意ある行動や利己的な目的行為を促進もするし、防止もする。防止に資する日常業務への取り組み姿勢や組織への帰属意識といった観念は、教育や訓練によって一朝一夕で定着するものではない。しかしながら、現実には組織内の人事異動や人事評価によりこの観念が正されもするし、歪みもする。多くの事例はこの歪みにより発生しており、企業の対策として、継続的な意識啓発や多様な事例を通して、この観念が歪まないような教育を実施していくしかない。

個人情報や機密情報を取り扱う作業者には、技能だけではなく、作業方法や作業手順を遵守する能力、それ以上に重要情報を取り扱うこと自体の意味を深慮できるセンスと能力が必要とされているため、作業者の適正をチェックし、十分な意識を持った要員の選定が重要な対策となってくる。

6　情報漏洩における組織管理の在り方

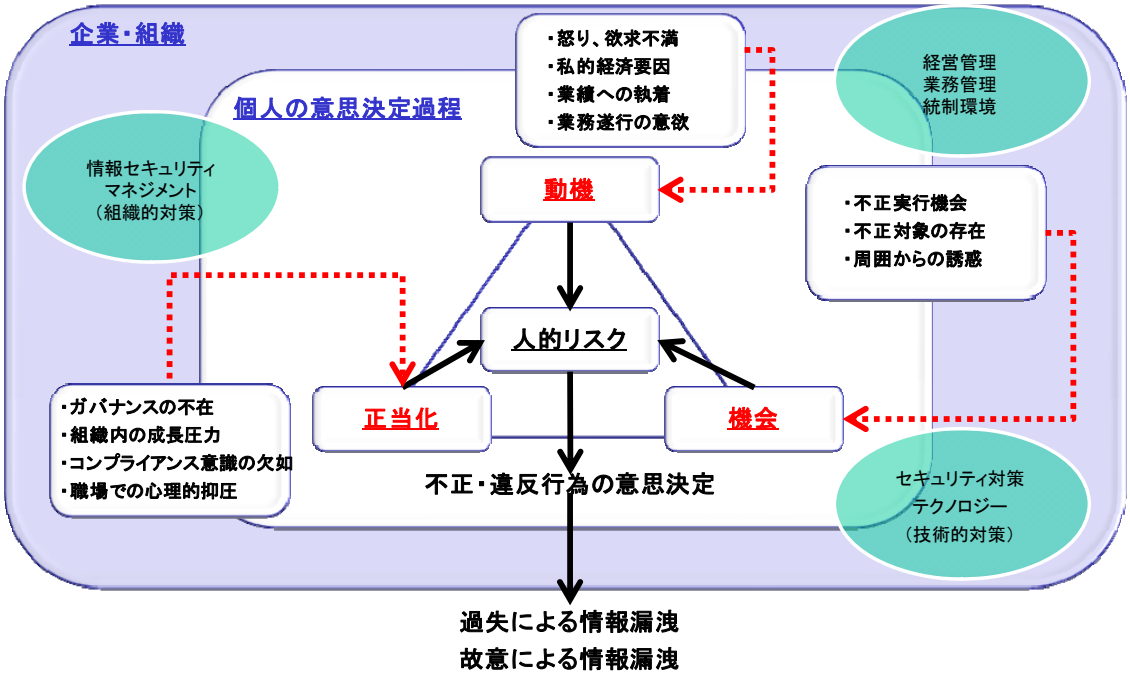
(1)情報漏洩に対する個人・組織的対応

ヒューマンエラー対策には、「個人の視点」に基づく計画の策定・実施と「組織の視点」による継続的な運用が必要不可欠である。個人的な視点とは、人間をよく知り、当事者の視点で作業負担や心理状況を捉えることである。

対策の検討、実施に際しては、人間の特性と業務実態との整合を図り、当事者が情報セキュリティの意義を理解し主体的に取り組むことが肝要である。この視点を欠いた対策は、効果が薄いばかりでなく、関係者の負担増大に繋がり、新たなヒューマンエラーの要因にすらなる。

一方、組織の視点とは、ヒューマンエラー防止に対する組織的な取り組みである。「エラーはどんな人間でも起こし得る」「エラーは組織や環境に誘発される」という基本認識の下、システムマネジメントおよびモラルマネジメントを高い水準で維持しつつ、対策の継続的な運用が求められる。組織マネジメントの良否は、当然のことながら、組織内の人間に様々な影響を及ぼす。

ヒューマンエラーが致命的な事象に結びつくのは、情報漏洩に限ったことではない。多くの企業において発生する不適切な事象は、直接間接ヒューマンエラーに関与するものが多いが、未だこのことが十分認識されていないといえる。



(2)事故に対する認識

「不安全行為」とは、基本的に「作業実施者」(現場担当者)による行為であるが、従来、人間工学では、「基本的エラータイプ」と言われる「スリップ」(不適切な注意)、「ラプス」(不適切な記憶)、「ミステイク」(誤り)の3つで事故を分析している(19)。

これに一つ追加するとすれば、「バイオレーション」(違反)の一種として「規則逸脱」がある。「規則逸脱」には、「日常的違反」(日常的に行っている違反)、「合理化違反」(より合理的ではないかと行う違反)、「創意工夫的違反」(効率を上げるために行う違反)がある。

ただ、これは、そうした違反を許した組織(管理者)の側にも問題がある。つまり、組織(管理者)としては、そのような効率優先のみからの創意工夫を受け入れ、より良い物とするためのシステムは変える、あるいは手順を変更することもできたということも考慮する必要があると考えられる。

このように、組織(管理者)が安全かどうかをきちんと評価しない、あるいは違反を見逃がしていることも事故に繋がるわけであり、事故分析にはこうしたタイプのエラーも十分に考慮する必要がある。組織的な過誤を分析するには、現場担当者ではなく、管理者の行為を見ていくことも重要である。

従来、人間工学は過失しか分類していなかったが、最近の組織過誤を分析するには以下のような分類が有効である。

「能力・経験不足(過失)」、「注意力不足・看過(過失)」、「努力不足・無責任(誤規則放置)(認識ある過失)」、「怠慢・放置(不作為)(未必の故意)」及び「意図的違反(隠蔽・規則改竄)(故意)」などある。

(19) (2005)ヒューマンエラーの考察

また、組織的な過誤の原因としては、コミュニケーションの不足も考慮する必要がある。先の組織的な過誤の分類に加えて、このコミュニケーションエラーの分類を行うことにより、組織過誤の全体像が掴めるのではないのかと考えられる。組織事故は安全問題（善意の行為だがエラーとなるもの）との関連性が高い一方、不祥事はセキュリティ問題（本質的に悪意であると社会から指弾されるもの）との関連性が高いと考えられる。両者の関係については、組織事故がその原因や対応においてコミュニケーションと倫理的問題を内在し、その対応に失敗すれば、不祥事という社会的問題にまで発展することになってしまうことを組織的に認識しておかなければならないことを要請する。

7 情報漏洩における人的脅威への対応

社員、幹部含めた各個人が、情報漏洩に対する危機意識や認識を欠いているため情報漏洩事案が頻発すると言ってしまえば、それまでである。しかし、企業・組織として情報漏洩リスクを極小化するためには、個人の「自己正当化」を許してしまう会社側に脆弱性があることの認識から出発し、そのような作業環境を改善する必要がある。その上で、当事者が一生懸命に業務に取り組む過程での情報の持ち出しや複製による流出が、例えば納期を守れなかったとき以上に、組織に対して、結果的により甚大な被害を与えてしまう可能性があることを発信し、周知し続けるしかない。職員に悪意があるかないかということ以上に、全員がルール違反の結果をすぐに、具体的にイメージ・認識できるような組織風土を創造することが急務といえよう。

そのための第一歩として、情報漏洩発生の多様な要因・動機を分析・整理しつつ、現行のルールの存在の周知はもちろんのこと、ルールのさらなる明確化と周知（社員教育）の強化、外部メディアの無許可使用の禁止や機密情報資料の管理強化、そして、全社員による端末の定期検査、管理職によるルール順守状況の確認徹底等、情報流出の継続的な監視等の対策を総合的・全社的に粛々と進めていくしかない。

また、不正トライアングル理論の援用等の犯罪学・犯罪心理学・犯罪環境学に基づく内部不正対策を立案する場合、「不正の動機」や「不正の正当化事由」というような行為者の心理的要因に関しては、属人的要素が強すぎることから、把握し切れないとの理由でこの対策は軽視される傾向にある。

一方で、業務環境の統制や管理体制の強化により、不正をできないようにする「不正の機会」抑制型の対策は、管理者の存在・管理ルール・管理のための各種帳票等の存在等、見栄えもよく、社内に対して牽制や成果を形が見えるメリットもあることから、企業内においても、推奨・推進されることが多い。

しかしながら、「不正の機会」抑制型の対策は実は非常に大きな「不正の機会」を生み出すという盲点を含んでいることに留意しなければならない。前段のアクセス権限者による故意の情報の持ち出しにせよ、後段の特権 ID 付与者の不正にせよ、“正当な権限者による不正”によるリスクは極めて重大かつ甚大な被害をもたらす。

経営者やシステム管理者は、一般従業員等のシステム利用者による「不正の機会」を減らすた

めのアクセス制限が有効と考えているが、最もリスクの大きい“正当な権限者の不正”に対しては、全く無力であり、運用を間違えれば、両刃の剣となることを十分に認識しておくことが重要である。

自宅への業務の持ち帰りは、情報漏洩リスクだけではなく、就労者の過労リスクやメンタルリスクの温床にもなりかねないことをも、深く理解しておかねばならない。

そのような、複合リスク発生のメカニズムを内在する就労形態にも注意して眼を向けておかないと、いずれ、社内ルールは形骸化せざるを得ない。それを踏まえた上で、不明確な役割分担や責任の所在の曖昧さが日常的に散見されないような、実効性のある情報管理体制の構築が今後も重要になると考えられる。

8 今後の課題

企業における情報漏洩リスクの一つとしてクローズアップされている産業スパイやサイバースパイ活動は、攻撃の前にソーシャル・エンジニアリング[20]を利用して標的社員に近づいてくるともいわれている。最近では、Facebook、Twitter 等の SNS を利用し、組織内の特定の従業員になりすますことにより、標的社員の情報を取得するといった手口もある。

ソーシャル・エンジニアリングの手口は、多岐にわたり、臨機応変に人間の心理につけ込み情報を詐取するため、技術的な対策だけでは必ずしも有効とはいえない。日常の業務における対策として有効なことは、ソーシャル・エンジニアリングの脅威に対する理解と警戒であり、基本中の基本である情報管理ルールの徹底と周知にきめ細かく注意を払うことである。

また「そんなあからさまな手口には騙されるわけがない・・・」との思い込みや自信を排除していくことも必要である。

ソーシャル・エンジニアリング（Social Engineering）は、直訳すると「社会工学」であり、従来は「人間の社会的行動を科学的に研究して、社会生活上の実際問題を解決しようとする学問」という意味で使われていた。

情報セキュリティにおいては、機械的な手段や技術的な手段ではなく、人間の行為や、行動における心理的な弱点を狙う手法によって、個人情報や機密情報などを詐取する行為や手口を指す。

場合によっては、フィッシングやトロイの木馬などのマルウェア（悪意を持ったソフトウェア）を使った手法なども、ソーシャル・エンジニアリングに含まれる。これらは、不正アクセスなどを成功させるための補足手段として用いられ、またソーシャル・エンジニアリングの手口は多岐にわたり、さまざまな形で組み合わせて用いることが多い。

前述のとおり、ソーシャル・エンジニアリングとは、情報セキュリティ分野では、機械的（mechanical）な手段や技術的（technical）な手段ではなく、人間の行為や行動における心理

[20] クリストファー・ハドナジー、成田光彰訳(2012)「ソーシャル・エンジニアリング 最大の弱点“人間”をハッカーの魔の手から守るには」日経 BP 社

的（psychological）な弱点を狙う手法により、個人情報や機密情報などを詐取するという特徴を有する。ソーシャル・エンジニアリングの手口にはさまざまな種類があるが、古典的かつ典型的な手口として以下の 3 種類が挙げられる。

① なりすまして情報を聞き出す

一般的な手口として、上司になりすますことで権威に弱い人間から情報を詐取する手口や、同僚や仲間を装うことで相手が心を許し、善意から情報提供することを狙うなどの手口が用いられる。具体的には、相槌を打ったり、質問・関心を装うことで、対象者に次々と情報を出させるように仕向ける手法で、我々の身近でも、またインターネット掲示板等でもよく用いられる手口である。

例えば、

・社内のシステム管理者になりますまして、利用者から情報を引き出す。
・初心者の利用者や女性社員になりすまして、システム管理者から情報を引き出す。
・取引先、見込み客、実在する顧客になりすまして、情報を引き出す。
・公共サービスの人間等、第三者になりすまして、情報を引き出す。

等の手口が挙げられる。

② ゴミ箱をあさる

ハッキングの対象として狙ったネットワークに侵入するために、ゴミ箱に捨てられた資料から、ユーザー名やパスワード等の情報を探し出す手口である。

トラッシング(Trashing,Dumpser Diving)、あるいはスキャベンジング(Scavenging)とも呼ばれ、ゴミとして廃棄された書類などから目的の情報を盗みだす手口を指す。

不用意にゴミ箱に捨てたメモ書き（得意先の担当者氏名や電話番号、住所などを書き込んだものなど）だけではなく、フロッピーディスクや CD、DVD などの記憶媒体をそのまま捨てたものもターゲットとなる。外部からネットワークに侵入する際に、初期の手順として行われることが多いのがトラッシングといわれている。ハッキングの対象として狙ったネットワークに侵入するために、ごみ箱に捨てられた資料から、サーバやルーターなどの設定情報、ネットワーク構成図、IP アドレスの一覧、ユーザー名やパスワードといった情報を探し出す。

具体的には、

・業務終了後、従業者が帰宅した深夜などに、企業のゴミ収集場に忍び込み、収集される前にゴミをあさる。
・清掃業者になりすまし、フロア内のゴミ箱をあさる。清掃業者自身が、あるいは清掃業者を共犯者にして、ゴミ箱をあさる場合もある。
・ゴミの回収業者になりすまして、収集場のゴミを持ち帰る。回収業者自身が、あるいは回収業者を共犯者にして、ゴミを持ち帰る場合もある。

等の手口が挙げられる。

③ 肩越しに入力内容を見る

パスワードなどの重要な情報を入力しているところを後ろから近づいて、覗き見る手口である。

単純な手口ではあるが、成功すれば労せずしてパスワードやクレジットカードの番号等を入手することができる。

具体的には、

・清掃業者や運送業者を装い、構内へ侵入する。清掃業者や運送業者自身が、あるいはそのような業者を共犯にして、侵入する場合もある。
・偽装または盗み出した、あるいは拾得した ID カードや社員証を悪用し、入館システムを通過したり、警備員のチェックを受けずに侵入する。
・入室が許可されている従業者の後について、同伴人を装い認証を受けずに侵入する。
・ディスプレイの横に貼り付けた付箋紙に記入してあるパスワードを盗み見たり、ビジネスフォンの横に貼り付けたメモ書きから担当者名や電話番号を盗み見たりする。
・パソコンに向かっている操作者の背後に回り、入力しているパスワードを盗み見る（ショルダーハックとも呼ばれる）。
・不在者の机上に置かれた手帳や、重要な書類などを盗み見る。

等といった手口が挙げられる。

※ その他、エレベーターの中やオープンスペース、飲食店、喫煙所での会話も要注意である。悪意はなくとも、大声で社内に関することや、業務内容を話していれば否が応でも耳に入る。

最近の動向としては、外部からの攻撃の下調べとして、実名制のソーシャルネットワークサービス（SNS）が利用されるケースもある。特に近年では、SNS を用いて、システム管理者を装い「パスワードの有効期限が切れています。至急現在のパスワードを入力してください。」というメッセージを送信したり、友人であるかのように装い、重要情報を入手しようと試みる手口もある。

国内でも Facebook や Linkedin 等、実名登録制 SNS の利用者が増えており、本名や勤務先を登録して公開しているユーザーが増えている。さらに、SNS 上のメッセージで業務内容にかかわる書き込みをしていることも少なくない。

ところが、SNS 利用が攻撃者側にソーシャル・エンジニアリングを容易に行わせる原因ともなるということも認識しておく必要がある。SNS に機密情報を書き込んでしまうのは論外であるが、報道されてしまうような「炎上騒動」に発展する事故も多数ある。この点は多くの人が認識するようになっているが、普通（安全）に使っているつもりでも、外部からの攻撃に悪用され

るリスクが潜んでいるということを認識する必要がある。

SNSのメッセージ機能を使って、不正サイトに誘導する手法も攻撃者にとっては有効である。攻撃者はSNSのアカウントを作成して、ターゲットに対して普通に友達リクエストを送る。いったん「友達」となれば、相手のページにメッセージを投稿できる状態になる。SNS 上とはいえ友達関係にあるというだけで、リンクをクリックする心理的な障壁は下がる。さらに短縮 URL を使うと、サイト URL の怪しさも隠せてしまう。

SNS を利用する動機は「より幅広い人との交流を深めていきたい」、「新しいマーケット開拓のきっかけにしたい」というユーザーが殆どであり、積極的につながりを増やしていくことと、外部からの攻撃を回避しようとすることとの間で、相反する使い方が求められる。ただ、それは利用者の自己責任でバランスを取ればいい、という単純なものではない。

例えば、情報を発信する術を手に入れたユーザーが一旦情報を出し始めると、他のユーザーからの反応やレスポンスがあると、より多くの情報を出し、ユーザーの関心を引こうとしたり、自分があたかも人気者や情報通であると勘違いしやすくなる。

また、意見等への賛同者を求める傾向が強まり、反対意見の者を公然とバッシングしたりして、その過程で、更に別の情報や素材が持ち出され、本来書き込まれるべきではない種々の情報が、「活字」として、「オープンスペース」に持ち出されてしまう。炎上といわれる事態が発生するのも然り、SNS 推奨者の書き込みやツイートを見ていても、この傾向が顕著であることは明白である。

SNS 利用には、自身の仕事や職務上の立場について記述する、実際の知り合いであると確証の取れないアカウントと友達関係になる、の 2 種類のリスクがある。

企業・組織は従業員の SNS 活用に対して、企業を狙う外部からの攻撃を認識するとともに、「どのようなことに注意すべきか」「どのような行為をしてはならないか」等の「企業姿勢」とともに、問題が発生した場合あるいは、発生する恐れがある場合の「行動指針」についてガイドライン等で明示しておくことが、企業のリスク対策上必要となる。

上記のように、ソーシャル・エンジニアリングの手口は多岐に渡り、悪意のある者がどのような手段を使ってでも、不正に情報を入手しようとするのかを知っておくことも有効な防衛策の一つである。

日常的に注意を払うためには、各従業者が、必要最低限のモラルを守り、情報セキュリティに関する意識を高めることが重要である。さらに、情報リテラシーやメディアリテラシーの効用、情報を発信するということの本来の意味、さらにネットメディアの特性やネットユーザーの心理などの理解等、多角的な意識付けや危機感の醸成が必要である。

企業・組織にとって、個人情報や機密情報が重要であるとの認識は持っていても、ソーシャル・エンジニアリングの危険性やその具体的手口を知らなければ、いざというときに対応できない可能性がある。

ソーシャル・エンジニアリングは、このような人間の特性を利用して、正当なアクセス権を持つ人間を騙し、内部機密情報への正当なアクセス権を手に入れる。このように、正当なアクセス

権を得て、攻撃者になった者に対しては、もはや今までの技術的対策のみでは防御し切れない。

これらの対応に当たっては、当該手法をよく理解するとともに、継続的な教育・訓練や警戒心の喚起を行い、常に一定レベルの注意力を、社員一人ひとりに働き掛け、維持させることが有効であると考えられる。今後の課題としては、外部からの攻撃に対する対策も検討する必要がある。

■ 参考文献

・ローレンス・W・シャーマン他編著『エビデンスに基づく犯罪予防』財団法人 社会安全研究財団
・警察庁：平成 21 年警察白書
・シドニー・デッカー、芳賀繁監訳(2009)「ヒューマンエラーは裁けるか安全で公正な文化を築くには」東京大学出版会
・芳賀繁(2003)「失敗のメカニズム　忘れ物から巨大事故まで」角川書店
・独立行政法人情報処理推進機構(2009)「情報セキュリティ白書 2009」 毎日コミュニケーションズ
・独立行政法人情報処理推進機構(2010)「情報セキュリティ白書 2010」 毎日コミュニケーションズ
・独立行政法人情報処理推進機構(2011)「情報セキュリティ白書 2011」 毎日コミュニケーションズ
・独立行政法人情報処理推進機構(2012)「情報セキュリティ白書 2012」 毎日コミュニケーションズ
・岡本浩一・今野裕行(2003)「リスクマネジメントの心理学 事故・事件から学ぶ」新曜社
・舞田竜宣・杉山尚子(2008)「行動分析学マネジメント」日本経済新聞出版社
・経済産業省：技術情報等の適正な管理の在り方に関する研究会 報告書
・M.H.ベイザーマン/D.A ムーア、長瀬勝彦訳(2011)「行動意思決定論バイアスの罠」白桃書房
・小林直樹、日経デジタルマーケティング編(2012)「ソーシャルリスクビジネスで失敗しない 31 のルール」日経 BP
・AOS テクノロジーズ株式会社佐々木隆仁(2011)「デジタルデータは消えない」幻冬舎ルネッサンス
・野村総合研究所(2012)「IT ソリューションフロンティア特集 情報セキュリティ対策の最新動向」

〈編集・発行〉
株式会社エス・ピー・ネットワーク　総合研究室
本社：〒167-0043　東京都杉並区上荻 1-2-1 インテグラルタワー
http://www.sp-network.co.jp
TEL：03-6891-5556　　FAX：03-6891-5570