情報セキュリティマネジメント試験合格講座 午後試験対策 12

- 内部不正の要因分析

1. モデルの策定

(1) モデルⅠ:営業職員による個人情報の持ち出しや不正利用
インタビュー調査概要によると、不正行為者は一般社員(営業職を含む)が最も多く、個人情報を対象とした内部不正の事例が最も多い。

なお、営業職員とは、営業に関連した業務に携わる従業者(元従業者を含む)であり、個人情報の中には、顧客情報や従業員情報などが含まれる。

(2) モデルⅡ:開発者による開発情報の持ち出しや不正利用
判例調査によると、不正行為者は開発者が最も多く、開発情報を対象とした内部不正の事例が最も多い。

なお、開発者とは、開発に関連した業務に携わる従業者(元従業者を含む)であり、開発情報の中には、ソースコードや設計情報および社内システムの仕様情報などが含まれる。

2. 内部不正の要因分類
国内の既存調査では、ルーティンアクティビティ理論に倣って、内部犯行発生に不可欠な要因を「犯罪者となるリスクを持つ人」、「潜在的な被害者(物)」、「環境」としている。

これに対して、不正のトライアングルでは、「動機・プレッシャー」、「機会」、「正当化」の三つの要因から内部不正が発生するとしている。

事例調査結果における傾向と、これらの要因を比較し、IPA の調査では、内部不正誘発要因を「動機・プレッシャー」、「環境」と「機会」を統合した「環境・機会」、国内の既存調査および不正のトライアングルにはないその他の要因として、「(内部不正者の)知識・経験」と設定する。

犯行が離職後に発覚する場合と、企業に在籍している状態で発覚する場合の2種類のケースがある。前者は離職（転職）が起因した不正行為で、離職後の転職先での利用を計画的に行なっている事例もある。後者は自らが作成した成果物は自分の所有であると誤って認識し、離職の意志がないケースである。

(1) 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（業務量やノルマなど）や慢心および帰属意識などが含まれる。

	モデルⅠ（営業）	モデルⅡ（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。 頻繁に転職を繰り返す傾向にある。

要因の詳細

（ア） 自分が作成した成果物（顧客情報の一覧など）は自由に使ってよいと思う
（イ） 条件のいい企業から転職の誘いがあり、これまでの成果（顧客情報）を公開することで、有利に転職できると思う
（ウ） 社内の人事評価に不満がある
（エ） 上司の仕事への取り組み方や上司の人間性に不満がある
（オ） プロジェクトや業務の進め方に不満がある
（カ） 業務が忙しいため、自宅で作業する必要がある
（キ） 給与や賞与に不満がある、退職金に不満がある
（ク） 不当だと思う解雇通告を受けた
（ケ） 職場で人間関係のトラブルがある
（コ） ルールを違反しても個人や企業を特定されない自信がある

✓ 関連するキーワード

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、慢心など

(2) 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)や物理的な環境および組織のルールや教育などが含まれる。例えば、システム的な環境としては、アクセス権限、出入検査など。物理的な環境としては、職場環境、持込・持出制限などを含む。

	モデルⅠ(営業)	モデルⅡ(開発)
環境 機会	業績を求める傾向になり、ジョブローテーションが少ない。 評価および接遇処遇への納得度が低い場合もある。 監視が不在であり、不正行為を行う時間がある。	評価および接遇処遇への納得度が低い。 監視が不在であり、不正行為を行う時間がある。

要因の詳細

(ア) システム管理がずさんで、情報を簡単に持ち出せることを知っている
(イ) パソコンや USB メモリなどの情報端末の持込制限が厳しい(情報端末への書き込み以外の方法で保存する必要がある)
(ウ) 職場に管理者がいないため、見つからない、監視カメラがない
(エ) 情報の持ち出しに関して社内に相談窓口がない
(オ) ログインするための ID やパスワードの管理が徹底されていない
(カ) 職場への入退口に警備員がいない(誰もが職場に入ることができる)
(キ) 不正を行う充分な時間がある、頻繁にルール違反が繰り返されている
(ク) 社内ルールや規則が徹底されていない、罰則がない
(ケ) 社内ルールや規則が厳しく、遵守するための負担が大きい
(コ) 社内教育の制度が整っていない
(サ) 重要な情報が暗号化されていない(重要な情報を誰もが閲覧できる)
(シ) 備品に会社の管理シールが貼られていない
(ス) 社内への入退出時に手荷物検査がない

✓ 関連するキーワード

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・教育など

(3) 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、詳細には特定の経験や権限・役割(持っていること)や知識(知っていること)およびスキル(できること)などが含まれる。例えば、正当に付与されたアクセス権限を行使して重要情報を不正に持ち出す場合などを含む。

	モデルⅠ(営業)	モデルⅡ(開発)
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している。	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している。

要因の詳細

(ア) 顧客情報などの重要な情報を自由に持ち出せる権限をもっている
(イ) 顧客情報などの重要な情報を自由に持ち出せる技術的なスキルがある
(ウ) 同僚も重要な情報を自由に持ち出していることを知っている
(エ) 社内の誰にも知られずに、重要な情報を持ち出せる方法を知っている
(オ) これまでにも、誰からも注意や指摘を受けなかった
(カ) かつて同僚がルール違反を行ったことが発覚したが、処罰されなかった
(キ) 管理者ではないが、不正操作した証拠を消去することができる
(ク) 社員の大半のセキュリティ設定が管理されず、社員任せになっている

✓ 具体例

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もっているなど

出典: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－」