連載「プロマネの現場から」
第 192 回　情報セキュリティにおける内部不正と発見的統制

蒼海憲治（大手 SI 企業・製造業系事業部門・技術総括部長）

前号（第１９１回『ランサムウェアの脅威』）においては、独立行政法人情報処理推進機構（IPA：以下 IPA）による「情報セキュリティ 10 大脅威」の中でも、ここ数年、被害が大きいランサムウェアによる脅威について取り上げ、ランサムウェアなどによる情報セキュリティインシデントに備えるための様々な防御策について紹介しました。情報セキュリティの統制には、予防的統制と発見的統制との大きく２つがありますが、その防衛策の多くは、予防的統制と呼ばれるものです。インシデント発生を未然に防ぐための統制であり、論理的および物理的な制限やポリシーや手順、訓練プログラムなどを事前に整備することで、企業内のシステムや情報へのアクセスを限定することにより、社員や外注パートナーなどの認証情報を管理し、外部からの不正なアクセスを防止することです。一方、重要な情報が漏えい・流出したことを早期に検知し、また牽制するための施策として発見的統制があります。既に発生しているインシデントの発見と対応を支援するための統制を実施することで、事後になりますが脅威への被害を軽減します。正しい認証を経てアクセスし、操作された結果の情報セキュリティインシデントの事例としては、社員や外注パートナーなどによる内部不正があります。IPA の「企業における営業秘密管理に関する実態調査 2020」報告書（＊１）によると、「中途退職者による漏えい」「現職従業員などの誤操作・誤認識等による漏えい」の内部不正が情報漏えいルートの過半を占める原因でした。

内部不正が起きた場合、企業・組織の社会的信用が失墜、顧客や取引先などに対する損害賠償や補填による経済的損失、企業・組織としての経済的な競争力の大幅な低下、業績の悪化により従業員への処遇が悪化、その結果、会社存続の危機につながる恐れがあります。たった一人の社員が過ちを犯してしまったとしても、組織の存続や従業員の生活をおびやかす脅威になりうるため、内部不正は経営者・経営陣が真摯に向き合わなければならない経営課題の一つといえます。自部門においても、職場の離職者・退職者に対して過去半年分の操作ログ・入退室ログ等をチェックするとともに、また、そのことを周知することで牽制をしています。外部からの攻撃だけでなく、内部からの攻撃に対応するためには、予防的統制と発見的統制の両方の施策を合わせて防衛策を準備する必要があります。

今回は、内部不正が発生する原因及び、その対策について紹介したいと思います。

「内部不正による情報セキュリティインシデント実態調査」報告書（＊２）によると、内部不正の動機の約 6 割が「意図していない違反」です。「うっかり違反した」が 40.5%、「ルールを知らずに違反した」が 17.5%であり、合計 58.0%、全体の約 6 割は「うっかり」によるもので、故意ではありませんでした。その一方、残りの 42.0%は、故意によるもので、その理由は「業務が忙しく、終わらせるために持ち出す必要があった」

が 16.0%、「処遇や待遇に不満があった」が 11.0%などでした。

前者は、「うっかり」ミスを防ぐために、誤操作をエラーとするようなしくみを作るとともに、情報の格付けやアクセス権限等のルールや規則を明確にし、社員・外部パートナーへの周知徹底をすることが有効になります。

後者は、所属企業・組織に対する不満などの内部不正を行う動機が基となるため、しくみやルール・規則の整備に加え、社員のエンゲージメントにも配慮する必要があります。

内部不正が行われる主な手口としては、

・アカウント権限の悪用：特定の業務目的で付与されたアカウント権限を悪用し、重要情報を盗み出すケース
・アカウントの悪用　　：離職・退職後にアカウントを悪用するケース
・誤操作・うっかり　　：意図しない行動・操作により、情報漏えいが起こるケース

「誤操作・うっかり」は、最近はクラウドサービスの利用が拡大していることもあり、ドラッグアンドドロップのような小さな誤操作が、グローバル規模の重大な情報セキュリティインシデントを引き起こすリスクも高まっています。

不正行為が発生する条件については、組織犯罪を研究する米国の学者ドナルド・R・クレッシーが提唱した「不正のトライアングル」があります。人が不正行為に走るときには、①不正を行う動機(不正を行わざるを得ないというプレッシャー、組織への強い不満)、②不正を行う機会（情報を盗むことができ、たとえ盗んだとしても誰も気づかないだろう）、③不正を行うことに対する正当化事由(不正行為を正当化する理由)の３つがあります。

「①不正を行う動機」には、「情報を流出させることで報酬を得たい」「有利な条件で転職したい」といった私的な動機や「自分を苦しめた職場や上司・同僚を困らせたい・迷惑をかけたい」「苦しいプロジェクトを中断させたい」という私怨・プレッシャーなどがあります。

「②不正を行う機会」には、情報へのアクセス権を持っており、不正ができる地位・職能・役割を持っていること。それを利用しても不正が発覚する可能性が低いと思われていることがあります。

そのため、不正行為の発生確率を減らすためには、「不正のトライアングル」の要素に対する対策を施すことが重要になってきます。IPA の「内部不正防止ガイドライン」においては、不正防止の基本原則を５つ挙げています。

・犯行を難しくする（やりにくくする）
・捕まるリスクを高める（やると見つかる）
・犯行の見返りを減らす（割に合わない）
・犯行の誘因を減らす（その気にさせない）

・犯罪の弁明をさせない（言い訳させない）

また、「内部不正を防ぐための管理のあり方」として、組織内において具体的な内部不正対策を講じるために、１０の観点から必要な対策をできる限り網羅的に示されています。
１．基本方針
２．資産管理
３．物理的管理
４．技術・運用管理
５．原因究明と証拠確保
６．人的管理
７．コンプライアンス
８．職場環境
９．事後対策
１０．組織の管理

「１．基本方針」においては、「経営者の責任、ガバナンス」の重要性を示しています。「組織における内部不正防止では、組織全体において効果的な対策を推進する上で経営者の関与が非常に重要であり、経営者のリーダーシップによる基本方針の策定及び組織的な管理体制の構築が必要」であること。「経営者が主導する形で、内部不正対策の体制と仕組みを構築し、運用させることで内部不正防止に対する意識や取り組みを組織内に徹底させることが可能となります」

「４．技術・運用管理」においては、「（１２）内部不正モニタリングシステムの適用」として、「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。」としています。内部不正モニタリングシステムにより、ログを常時監視し、行動に重大な変化が生じた場合にこれをリアルタイムに検知することができるようになります。「深夜時間帯の大量のファイルダウンロード、重要性が高い情報へのアクセス、役職員の離職、個人用クラウドストレージへの同期など、組織が高リスクと判断した特定タイプの行動を監視することもできます。」ただし、AI やアルゴリズムによる自動的な判断に対して、判断結果に対する説明責任を果たすために、人間の判断も必要になります。

　内部不正モニタリングシステムとして、「Internal Risk Intelligence（内部脅威検知）」サービスがあります。企業内のログデータや管理情報を統合的に分析し、内部不正・サービス残業などのリスク行動を検知するサービスです。様々なログデータを活用し、社員・

外部パートナーの振る舞いを検知することで、情報持ち出しや不就労（サボり）や超過勤務の是正、セキュリティポリシーを逸脱する行為等の見えないリスクを事前に予兆するものです。自部門だけで対応が困難な場合、外部サービスの利用もあわせて、防衛していくことが必要になります。

（＊１）「企業における営業秘密管理に関する実態調査 2020」報告書について：掲載日 2021 年 3 月 18 日
独立行政法人情報処理推進機構セキュリティセンター
https://www.ipa.go.jp/archive/security/reports/2020/ts-kanri.html

（＊２）「内部不正による情報セキュリティインシデント実態調査」報告書について：公開日：2016 年 3 月 3 日・アーカイブ掲載日：2023 年 12 月 15 日
独立行政法人情報処理推進機構技術本部 セキュリティセンター
https://www.ipa.go.jp/archive/security/reports/economics/insider.html