最新セキュリティマネジメント（第26回）

「不正のトライアングル」の観点で内部不正を防ぐ

2023.07.24

独立行政法人情報処理推進機構（以下、IPA）では、2023年5月31日に「情報セキュリティ10大脅威 2023」解説書に個人編とコラムを追加し、再編集した解説書の改訂版を発表した。目に留まったのが「内部不正、あなたの組織は大丈夫？」というコラムだ。そこでは内部不正を防ぐために「不正のトライアングル」を考える必要があるとされている。どんなことをさしていて、どう役立てればよいのだろうか。

適切な対策を講じるには不正の原因の理解が不可欠

情報セキュリティを考える上で、内部不正に対する対策は重要だ。IPAの「情報セキュリティ10大脅威2023」でも内部不正は組織編の第4位に挙げられている。テレワークなど不正が行われやすい環境が広がっていることもあり、昨年の第5位からランクアップしている。

内部不正の具体的な行為としては、重要情報や情報システムなどの情報資産の窃取、持ち出し、漏えい、消去・破壊などが考えられる。実際に起きてしまうと、情報システムが使えなくなったり、情報が外部に流出したりして被害が発生する。個人情報の流出は損害賠償の発生や社会的信用の失墜など、大きなトラブルにつながるケースが増えている。

多くの業務がITを駆使して処理されている今は、さまざまな従業員が情報システムにアクセスできるようになっている。それだけに内部不正が発生するリスクは増大し、さらにテレワークのような働き方も新たなリスクを生み出している。企業としてはこの事実を正面から受け止め、内部不正を防ぐための対策を講じる必要がある。

しかし、業務効率化のためにITの利用を促す以上、過剰な対策を講じればITの利便性を阻害することにもなりかねない。こうしたジレンマを回避するには、内部不正の原因を正しく理解し、対策を講じていく必要がある。そのヒントとしてIPAのコラムでは「不正のトライアングル」が紹介されている。

不正のトライアングルとは、アメリカの犯罪学者であり、社会学者であるドナルド・レイ・クレッシーが犯罪調査から不正の原因として導き出した3つの要素、「機会」「動機」「正当化」を指す。人間はこれら3つの要素がそろった時に不正を働く場合が多い。

「情報セキュリティ10大脅威2023」のコラムではこの3つの要素をベースに、内部不正が発生する原因と基本対策が解説されている。情報セキュリティの観点から3つの要素をどう捉えていけばよいのだろうか。

情報セキュリティの観点から3つの要素を把握する

「機会」とは不正行為が実行可能な状況にあることだ。情報セキュリティの観点では、価値ある情報がいつでも盗み出せる状態を意味する。本来は閲覧できないデータが目の前にあれば、つい手を出そうという心理が働くときもある。組織としてはこういう状況は決して好ましくはないだろう。

対策として提案されているのが、環境を適切に定めることだ。不正行為をやりにくくしたり、やった場合に見つかりやすくしたりすることが基本になる。例として、アカウントのライフサイクルやデータのライフサイクルに基づいてアクセス権限の管理を徹底すること、重要情報への多要素認証を実施すること、ログを記録することなどが示されている。

確かに、アクセスするための手段がしっかりと管理されていて、あらゆるログが記録されていれば、不正を見つけやすくなり、従業員に対する抑止力にはなるはずだ。退職した従業員のIDがいつまでも残っているという状況は論外だろう。

次の「動機」は、不正を働くに至る必要性や誘因をさす。一般的な犯罪の背景となっている貧困や社会への不満などは従業員の内部不正にも当てはまる理由であり、組織の一員としてはミスを隠したいという意識も大きな動機になる。対策としては日頃から従業員とのコミュニケーションを密にして、状況を把握しておく必要がある。

テレワークには「疎外感」や「不公平感」を高めるという一面もあるため、特に配慮が必要だ。モラル教育を実施するとともに、相談窓口を設けるなどきめ細かなフォローが内部不正の発生を防ぐことにつながる。

トライアングルの3つ目の要素は、不正行為を正しい行為だと思い込む「正当化」だ。「会社が自分の能力を正しく評価してくれないから」など、責任を他者に押し付ける責任転嫁の心理が働くケースは多い。コラムでは正当化を防ぐ方法として、言い訳をさせないためのルール化とルールの周知徹底、未承認のデバイスをつなげないようにする仕組みづくり、さらに「うっかりしていた」というケースを防ぐための内部講習の実施などを挙げている。

これら3つの要素がそろうと内部不正が起きやすいのであれば、そろわないような具体的な対策を講じれば内部不正を防げるはずだ。IPAでは内部不正防止にテーマを絞った「組織における内部不正防止ガイドライン」も公開している。具体的な対策を考える上で、参考にしてみてはどうだろうか。