最新セキュリティマネジメント（第37回）

中小企業の内部不正対策を強化する3つのポイント

2024.06.18

企業にとって、重要な顧客情報や設計情報などが外部に流出する原因は内部不正である場合が少なくない。こうした内部不正による情報漏えい事件は後を絶たない。中でも、小規模企業の内部不正に対するセキュリティ体制が不十分なケースが目立ち、企業経営の大きなリスクになっている。このリスクにどう向き合えばよいのか。独立行政法人情報処理推進機構（以下：IPA）が興味深いレポートを発表したので紹介する。

内部不正対策が遅れる中小企業

2024年5月30日、IPAは『2023年度「内部不正防止対策・体制整備等に関する中小企業等の状況調査」報告書』を発表した。内容は、IPAがこれまでの調査で指摘してきた問題点や課題をまとめたものだ。中小企業における内部不正防止策の課題として、次の3つを挙げている。

1. 内部不正防止が「重要な経営課題」として認識されていない
2. 営業秘密は各社の業務に依存するため定義が難しく、守るべき情報資産を特定できていない
3. サイバーセキュリティ対策を講じているものの、内部不正対策は後手に回りがち

これらに心当たりのある中小企業の経営者も多いのではないだろうか。実際に、大企業と中小企業では内部不正についての認識や対策の実施、組織的な対応に大きな差があると浮き彫りになった。

例えば、内部不正防止とサイバーセキュリティ確保を意識的に分けて扱う企業の割合は、従業員1万1人以上の企業では約8割、全体平均でも約6割を占めているのに対して、従業員21人から100人の企業では約4割にとどまっている。

また、個人情報以外の秘密情報に格付け表示がされており、秘密情報であると認知できるようになっているか、という問いに対して、従業員21人から300人の企業ではそうした表示がなされている割合は約2割だった。従業員1万1人以上の企業は約4割が認知できるとしており、小規模企業はその半分程度という結果だった。

不正発生時の対応、体制についても大きな違いがある。重要な秘密情報が不自然に取り扱われている場面を目撃したら報告するよう徹底されており、上層部に報告できない場合は内部通報ができる体制やルールが確立されている割合は、従業員数が多くなるほど高くなる傾向が明らかになった。

内部不正に向き合うための3つのファーストステップ… 続きを読む