内部不正対策は経営課題

関係者による漏えいが多数

近年、企業や組織において、内部不正による情報セキュリティー事故が原因で事業の根幹を脅かすようなケースが目立つようになってきた。その典型例としては、従業員によって顧客情報が不正に売られたことによる個人情報の大量漏えいや、製品情報が退職の際に不正に持ち出されたことによる技術情報の漏えいなどが挙げられる。また、悪意はないにしても、自宅で業務を行うために社内情報を無断で持ち出し、自宅PCから漏えいさせてしまう例も見られる。

経済産業省の調査において、営業秘密の漏えいがあった企業では、漏えい経路が「中途退職者（正規社員）による漏えい（50・3％）」、「現職従業員などのミスによる漏えい（26・9％）」、「金銭目的などの動機を持った現職従業員などによる漏えい（10・9％）」と報告されている。このように、競争力につながる価値ある営業情報の漏えいは、内部の関係者によるものが多くを占める。

しかし、「自社では内部不正は発生しないだろう」「自社の従業員に不正行為をするものはいない」と考えて、リスクを軽視する中小企業は多い。内部不正対策を講じていないと、事故発生を防止できない可能性があるのはもちろん、事故発生に気付かないために被害が拡大し関係者に迷惑が及んで初めて発覚するようなケースや、原因不明で事故を解明できないケースなど、事後対策に支障をきたすこともある。

さらに、不正行為を行った者を特定できたとしても、注意義務を怠っていたとして、懲戒処分が無効になったり、訴訟が困難になったりしてしまうケースさえ考えられる。このような事態に陥らないためにも、中小企業は内部不正を経営課題の一つとして認識し、経営者のリーダーシップの下、真摯（しんし）に取り組まなければならない。

IPAの防止指針活用を

内部不正対策を整備するに当たっては、独立行政法人情報処理推進機構（IPA）の「組織における内部不正防止ガイドライン」が参考となる。今回は、予防、早期検知、事後対応の観点から取り組むべき対策の一部を紹介する。

組織における内部不正防止ガイドライン

被害を予防するための対策

資産の把握・体制の整備

組織が保持する資産を重要度などで分類し、経営層が責任を持ち、資産の管理体制の整備を積極的に推進することが重要である。

重要情報の管理・保護（アクセス制御、暗号化）

不正競争防止法の営業秘密漏洩罪に問われないためには、「秘密管理性」が重要視される。

アカウント、権限の管理・定期監査

不必要に高い権限を付与しない。また、アカウントを共有しない。

罰則の周知と相互監視の強化

紛失・漏えいを隠蔽（いんぺい）した場合、より懲罰が重くなることを周知することも有効である。

外部記憶媒体の利用制限

USBメモリーなどの外部記憶媒体の利用に制限をかける。また、許可外の機器の接続を禁止する。

被害を早期検知するための対策

システム操作の記録・監視

IPAで行った内部不正に関する実態調査では、効果的な内部不正対策として、アクセスログの監視が上位となっており、効果が期待できる。

被害後の対応のための対策

事後対策に求められる体制の整備

被害の最小化、および影響の拡大を防止するために、求められる対応手順や報告手順などを事前に取り決めておく。

内部不正防止ガイドラインの詳しくはIPAのウェブサイト（https://www.ipa.go.jp/security/fy24/reports/insider/）で確認してほしい。

（独立行政法人情報処理推進機構・江島将和）