Ksisnetだより

発行:Ksisnet事務局
令和 3年10月12日
Vol.98

「情報セキュリティ10大脅威2021」（組織） 6位

内部不正による情報漏えいについて

「情報セキュリティ10大脅威2021(組織編)」で、「内部不正による情報漏えい」が第６位にランクインしています。組織に勤務する従業員や元従業員等の組織関係者による機密情報の持ち出しや、従業員が情報管理のルールを守らずに情報を持ち出した事による情報の紛失・漏えいが発生しています。昨年の第２位から順位を下げているものの、組織関係者による不正行為は、組織の社会的信用の失墜、損害賠償による経済的損失により、組織に多大な損害を与えます。

<攻撃手口>

1 アクセス権限の悪用
付与された権限を悪用し、組織の重要情報を窃取する。必要以上に高いアクセス権限が付与されている場合、より重要度の高い情報が窃取され、被害が大きくなるおそれがある。

2 在職中に割り当てられたアカウントの悪用
組織の離職者が、在職中に使用していたアカウントを悪用し、組織内部の情報を窃取する。

3 内部情報の不正な持ち出し
組織内部の情報を、USBメモリーやHDD等の外部記憶媒体、メール、クラウドストレージ、スマホカメラ、紙媒体等を利用し、外部に不正に持ち出す。

<情報漏えいした場合の組織への影響>

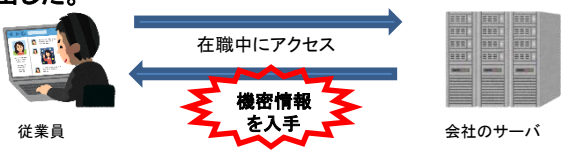
- 組織の社会的信用の失墜
- 損害賠償による経済的損失

情報の重要性や漏えい規模によっては、組織の弱体化に繋がる可能性がある。

組織の経営の根幹を揺るがすインシデントに発展するおそれ

<事例1>

従業員が金銭目的で、勤めていた会社の営業機密を含む情報を、サーバーから自身の記憶媒体にコピーして持ち出した。



従業員は退社した後、持ち出した情報を某国の外交官に渡し、その対価として金銭を受領。元従業員は、不正競争防止法違反に問われて、有罪判決を受けている。

<事例2>

某市役所職員が、市職員約2,700名分の個人情報を、地元新聞社のメールに送信して漏えいさせた。漏えいした情報は、当該職員が業務に使用していたPCの前の利用者がごみ箱に捨てたままにしていたものであり、当該職員が引き継いだ際にこれを発見し、上司に報告せずに保存していた。

当該職員は懲戒免職になっている。

<対策／対応>

○ 基本方針の策定
経営者が積極的に関与し、組織横断的な管理体制を構築する。

○ 重要資産の把握と体制の整備
重要資産を把握し、重要度に合わせてランク付けし、重要情報の管理者を定める。

○ 重要情報の管理と保護
重要情報の利用者IDやアクセス権の登録等に関する手順を定めて運用し、離職等に伴い不要になったIDは直ちに削除する。

○ 物理的管理の実施
重要情報格納場所等への入退室を管理する。
記録媒体の利用制限や持ち出しを管理し、廃棄する際には適切にデータ消去する。

○ 情報リテラシーや情報モラルの向上
情報取扱ポリシーの策定及び内部不正者への懲戒処分等を規定した就業規則を整備し、従業員に対するコンプライアンス教育を定期的に実施する。
離職者とは秘密保持契約を締結し、離職後の情報漏えいを防止する。

○ 被害の早期検知
重要情報へのアクセス履歴及び使用者の操作履歴のログ等を記録し、定期的に監視する。

○ 被害を受けた後の反応
- 関係者、関係機関への連絡
- 警察への連絡
- ＣＳＩＲＴ等所定の連絡先への連絡
- 影響調査および原因の追究、対策の強化
- 内部不正者に対する適切な処罰の実施

参考 ＩＰＡ（情報処理推進機構）