サクセスネット SuccessNet

今月のトピックス

～２０２４年３月号～

情報セキュリティを担保するために

独立行政法人情報処理推進機構から「情報セキュリティ 10 大脅威 2024」が公表されました。このうち「組織」向け脅威を見ると、外部からの攻撃によるもののほか、内部不正や不注意による情報漏えいなど、社内起因の脅威も垣間見られます。

本稿では、社内起因の脅威のうち、内部不正にフォーカスを当て、現況と対策をお伝えするとともに、それを担保する規程の例をご紹介いたします。

１．内部不正による情報漏えいの現況と対応について

東京商工リサーチの調査によると、2023 年の「個人情報漏えい・紛失事故」の件数は 175 件（前年比 6.0%増）となっており、3 年連続で最多件数を更新しました。そのなかで、情報の不正利用や持ち出しにより情報漏えいした「不正持ち出し・盗難」は 24 件（構成比 13.7%）で、前年の 5 件から約 5 倍に増加しています。

情報のデータ化が進み、大量な情報であっても瞬時に操作できるようになりました。そのようなことから、企業における重要な情報は厳格に管理する必要性が高まっています。その管理や脅威への対策としては、次のようなことを実施することが考えられます。

①接近の制御	ルールに基づく適切なアクセス権の付与・管理
②持出し困難化	【書類、記録媒体、物自体等の持出しを困難にする措置】 秘密情報の社外持出しを物理的に阻止する措置　等 【電子データの外部送信による持出しを困難にする措置】 社外へのメール送信・Ｗｅｂアクセスの制限　等 【秘密情報の複製を困難にする措置】 私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限 【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】 秘密情報の消去・返還
③視認性の確保	【管理の行き届いた職場環境を整える対策】 職場の整理整頓（不要な書類等の廃棄、書棚の整理等）

	【目につきやすい状況を作り出す対策】 職場の座席配置・レイアウトの設定、業務体制の構築 【事後的に検知されやすい状況を作り出す対策】 秘密情報の保管区域等への入退室の記録・保存とその周知

２．情報保護に関する規程について

前出のような対策については、漠然と運用するだけでなく、対策を担保する措置が必要です。例えば、企業と労働者とで情報保護に関する覚書を取り交わす、就業規則の服務規律に記載する、別途、情報取り扱いのルールについてのガイドライン等を作成して通知することなどが有効です。

次に、参考として経済産業省が公開している秘密情報管理に関する就業規則「服務規律」への規定例をご案内いたします。

第○条（服務規律）
１．従業員は、職場の秩序を保持し、業務の正常な運営を守るため、職務を遂行するにあたり、次の各号に定める事項を守らなければならない。
　○会社の施設、設備、製品、材料、電子化情報等を大切に取り扱い保管するとともに、会社の許可なく私的に使用しないこと。
　○（以下略）
２.従業員は、入退場に関し、次の各号に定める事項を守らなければならない。
　○警備員から所持品の検査を求められたときは、応じること。
　○会社の許可なく、書類や社品を会社外に持ち出さないこと。
　○会社の指示する手続を経て入退場すること。
　○日常携帯品以外の物品を携帯して入場しないこと。ただし、特に必要な場合は、会社の指示する手続をとること。
　○（以下略）
３．従業員は、従業員証を常時携帯し、入場のとき又は求められたときは、直ちに提示しなければならない。

（経済産業省「秘密情報の保護ハンドブック ～企業価値向上に向けて～」）

３．さいごに

企業の経営資源として、「ヒト」「モノ」「カネ」に「情報」が加わってから長らく経ちますが、ＩＣＴ化の進展も相まって「情報」の価値が年々高まっています。

今一度、自社の情報資産について目を向けながら、保護体制について見直してみてはいかがでしょうか？

※本内容は 2024 年 2 月 14 日時点での内容です。

＜監修＞

社会保険労務士法人　中企団総研