情報資産と情報セキュリティ

情報資産とは

企業経営や組織運営上で役に立つ多様な要素や能力のことを経営資源と言い、主要な経営資源は一般に「ヒト」「モノ」「カネ」と「情報」の 4 つであるとされています。
企業は物を作ったり、販売したり、サービスを 提供したりする中で付加価値を生み、その対価を得ることで成り立っています。その企業活動は、お客様の情報、市場の情報、仕入先の情報、生産管理情報など、様々な情報によって企画・管理され、情報を的確に取り扱うことで正しい経営ができるのです。
自治体などの組織においても、住民等の個人情報をはじめとする様々な組織運営上の情報が適正に管理されていることが重要なことは言うまでもありません。

その情報そのものと、情報を収集したり処理したり保管したりするための装置を情報資産といいます。
企業や自治体などの組織体には、多くの情報資産が存在しており、それらは、コンピュータ、記録媒体、紙、または人の記憶や知識など、さまざまな形態をとります。

情報資産の存在場所と特徴

存在場所	データタイプ	内容	例	特徴
情報機器	デジタル	サーバーなどに電子的に保存されている情報	パソコンやサーバーなどに保管されている個人情報、人事・財務情報、営業情報、技術情報などの各種電子データ	ネットワークからアクセスされて、不正アクセス、情報漏えい、情報改ざんのターゲットになりやすい
記録媒体	デジタル	容易に持ち運び可能な記録媒体（または装置）に保存されている情報	携帯電話、スマホ・タブレット、USB メモリ、CD-ROM、ノートパソコンなどに保管された各種電子データ	持ち出しが容易で、盗難や紛失のおそれが高い

紙	アナログ	紙などに印刷された情報	名簿や決算報告書などの印刷物、FAX で受信した各種情報	持ち出しが容易で、一目で内容が見られてしまう 写真などでの複写も容易 多量の紙の情報は活用しづらい
人	アナログ	人の記憶・知識	社長や技術者などに聞かなければわからない営業情報や技術知識、知見など	属人的で組織としての活用に難がある 「その人が居なくなる」ことがリスクとなる

情報セキュリティとは

情報資産は安全に保管され、必要な時に的確に活用されて初めて資産としての価値を持つものになります。

情報資産を脅かす具体的な脅威として、機密情報の漏えいや不正アクセス、データの改ざん、サービスの停止などが挙げられます。
悪意のない、例えば地震や火災などの災害から情報資産を守ること、社員や職員のミスから情報が漏えいすることを予防すること、あるいは悪意のある、例えば、外部からの不正アクセスやウィルスによる電子データの漏えいや改ざんを防止すること、など、様々な脅威から情報資産を保護し、必要な時点で的確に活用できるようにしておくことが、情報セキュリティです。

情報セキュリティ対策は、情報資産の「機密性」、「完全性」、「可用性」の三要素を確保しつつ、企業や組織の正常な活動を維持するために実施されるべきものですが、具体的な対策は、保有している情報資産の特質をよく検討し、費用面と三要素のバランスを考慮しながら行うことが大切です。
（三要素についての詳細は、「機密性・完全性・可用性」のページを参照ください。）