IT資産管理の重要性

■ IT資産管理に潜むリスクを把握して、手を打ってみませんか？

「IT資産管理」の目的は、ITシステムを活用するうえで、財務計上するための在庫把握や、セキュリティ強化、ライセンス使用におけるコンプライアンスの徹底、ITコストの適正化などがあります。
また、昨今の経営環境・IT環境の変化に伴い、IT資産管理の目的が拡大しています。
企業の皆様は、情報技術の進化に伴ってハード・ソフト面での複雑化、テレワークの普及といった新たな課題に対応すべく、「IT資産管理」の効率化は避けては通れない状況にあります。

ITの普及と企業の課題

2000年のIT革命以降、社会のデジタル化が進み、従業員の一人一人にパソコンが普及しました。
このことで、全ての従業員の働き方も変わりましたが、2005年の個人情報保護法施行、2018年以降の働き方改革の推進やCOVID-19の影響から、下記のように企業がIT管理を強化することも増えました。

ITの普及に伴う企業が抱える課題

1. コンプライアンス徹底の観点から不正なコピー利用などの違法行為を防ぐ、ハード・ソフトウェアの使用状況管理強化
2. 顧客の個人情報の保護や企業情報の漏洩防止の観点から情報の扱いを制限する内部統制の強化
3. ウィルスなどのマルウェア（悪意あるソフト）による、ネットワークへのサイバー攻撃対策強化
4. 日々進化し複雑化する情報技術に伴うIT資産コストの適正化

IT資産管理が未対応の場合のリスク

ここからは、IT資産管理が未対応の場合に生じる3つのリスクについてご紹介します。

1.コンプライアンス違反のリスク

IT資産管理の不徹底により違反を犯してしまうケースとして、ソフトウェアライセンス違反があります。
ソフトウェアは著作権法で保護されています。「契約しているライセンス数以上のソフトウェアをPCにインストールしている」という状態は著作権法の「無断複製」にあたり、違反行為になります。
その場合、刑事罰や民事訴訟といった法的リスク、それに伴う企業の信用失墜といった事態も発生しかねません。

最悪の場合、刑事罰（著作権法）では、以下のリスクがあります。
- 企業/団体に対して、3億円以下の罰金
- 代表者に対して、10年以下の懲役又は1000万円以下の罰金
- 従業員に対して、10年以下の懲役又は1000万円以下の罰金（又はこれらの併科）

民事でも同様に、企業/団体・代表者・従業員それぞれに民事責任が発生する可能性があります。

2.セキュリティ低下のリスク

自組織のPC台数、使用者といったことを把握していなければ様々なセキュリティ対策に抜け漏れが発生してしまいます。
IPA（Information-technology Promotion Agency：情報処理推進機構)が年に1回発表している「情報セキュリティ10大脅威 2025」では、「組織」向けの脅威の順位として「ランサムウェアによる被害」が5年続けて1位となっています。

※出典：IPA（独立行政法事情報処理推進機構）「情報セキュリティ10大脅威 2025」より

ランサムウェアとは？

ネットワークなどを通じて感染を広げるマルウェアの一種で、ソフトウェアの脆弱性を利用して攻撃を行い、制限解除と引き換えに身代金を要求します。

各PCにインストールされているソフトウェアやそのバージョン、アップデートが把握できていなければそれらによる攻撃にも対応もできません。
サイバー攻撃などの被害に遭っているのは大企業が中心とイメージがあるかもしれませんが、実はそうではありません。攻撃者が情報セキュリティ対策が十分でない中小企業を狙い、侵入し、そこから大企業へ攻撃するケースが非常に多いのです。

また、前述の「情報セキュリティ10大脅威 2025」では、「組織」向けの脅威の順位として「内部不正による情報漏えい」が4位、「不注意による情報漏えい等」が10位と内部の悪意や、不注意による情報漏洩も高い順位にあります。
こういったリスクに対しては、社内のポリシー策定とセキュリティ教育も欠かせない要素です。

情報セキュリティ10大脅威 2025（組織）

1位：ランサムウェアによる被害
2位：サプライチェーンや委託先を狙った攻撃
3位：システムの脆弱性を突いた攻撃
4位：内部不正による情報漏えい等
5位：機密情報を狙った標的型攻撃
6位：リモートワーク等の環境や仕組みを狙った攻撃
7位：地政学的リスクに起因するサイバー攻撃
8位：分散型サービス妨害攻撃(DDoS攻撃)
9位：ビジネスメール詐欺
10位：不注意による情報漏えい等
※出典：IPA「情報セキュリティ10大脅威 2025」より引用

企業や組織のセキュリティ対策・行動指針を明らかにする「情報セキュリティポリシー」を作ることで、社内のセキュリティルールを確立し、従業員それぞれがセキュリティの知識や意識を身に着けることで、リスクある行動の回避や、感染の疑いがある際の早期連絡などを促すことが可能になります。同時に、各PCやサーバーの個人情報や機密情報、社外秘のデータについてはログの保存や監視、情報の棚卸しや、適切なアクセス権の付与により、内部統制も強化され、情報の漏洩のリスクも下がります。

3.ITコストに関するリスク

ライセンスの利用実態、調達/導入/利用/破棄といったITライフサイクル、自社IT環境の構成を把握していなければ、余剰な契約や無駄な導入・投資により、余計なコストが発生してしまいます。また、削減すべきコストもみえてきません。
こういったことが頻発すると、本当に投資すべきタイミングを判断しにくくなったり、投資に踏み切っても、効果を最大化できないといったリスクもでてきます。

IT資産管理を妨げる要因

そろそろIT資産管理を効率化した方がよさそうだと感じていても、実際にはなかなか着手できない状況があるのでないでしょうか。

例えば、貴社においても次のような状況はありませんか。

- 端末が多い
- 部署ごとに管理している
- 人手不足で効率化まで手が回らない
- セキュリティ対策は難しい・人材がいない
- なにから始めたらいいのかわからない

適切なIT資産管理に向けて

IT資産の管理は、全社で一律的な管理を行うのが最も効率的な方法です。

IT資産管理の対象は、基本的には有形資産であるハードウェア、無形資産であるソフトウェアやライセンスです。

- **ハードウエア**

  PC（パソコン）、社用スマートフォン、サーバー、ネットワーク機器、
  プリンタや複合機、各種周辺機器
- **ソフトウェア**

  WindowsなどのOS、エクセルなどのOfficeアプリケーション、Adobe
- **ライセンス**

  ソフトウェアやクラウドサービスの利用権限

まずは、IT資産（PC、ファイルサーバー、ネットワーク機器など）の棚卸し、余剰ライセンスの確認、ライフサイクル※やコストを評価することをおすすめします。

ご契約いただきましたIT Expert Servicesでは、IT運用サポートのみならず、IT資産可視化のご支援も可能ですので、是非ご活用いただき、自社のIT資産管理、IT環境を適切化し、次のIT投資を検討してみませんか。

SECURITY ACTIONについて

IPAでは中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度として「SECURITY ACTION」を用意しています。

企業や組織のセキュリティ対策・行動指針を明らかにする「情報セキュリティポリシー」のサンプルのダウンロードも可能です。

社内のセキュリティルール、従業員の意識、社外へのアピールなどに是非ご活用ください。

※参考：IPA.SECURITY ACTION.「SECURITY ACTIONとは？」.
https://www.ipa.go.jp/security/security-action/sa/

同時に、セキュリティ対策の第一歩として、情報資産管理台帳を作成し、セキュリティリスクを評価することもおすすめします。

中小企業の情報セキュリティ対策ガイドラインについて

経済産業省とIPAが出している中小企業の情報セキュリティ対策ガイドラインが大変参考になります。
是非ご一読いただきご活用下さい。
※参考：IPA.情報セキュリティ.
「中小企業の情報セキュリティ対策ガイドライン」および「付録 7：リスク分析シート」.
https://www.ipa.go.jp/security/guide/sme/about.html

IT運用/管理のサポートは、IT Expert Servicesにお任せください

IT Expert Servicesでは、ご契約頂いたIT機器の情報をリモートで自動収集し、継続的なIT資産管理のサポートをいたします。IT資産管理のみならず、日常のIT運用・管理業務の支援、障害発生時の復旧支援など、ITに関する業務に幅広く対応しておりますので、ご契約のIT機器の追加など是非お気軽にご相談ください。

(2023年9月発行月次レポート「ITトピックス」の内容を一部修正して掲載おります。)