情報セキュリティ10大脅威と企業の対策

今年1月に情報処理推進機構が「情報セキュリティ10大脅威2024」※1を発表しました。ここではその結果と、企業が行っているセキュリティ侵害などへの対応状況をみていきます。

2023年の10大脅威は

上記発表による、2023年に発生した組織向けの情報セキュリティ10大脅威は表1のとおりです。

【表1】組織向けの情報セキュリティ10大脅威

順位	脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

独立行政法人情報処理推進機構「情報セキュリティ10大脅威2024」より作成

1位はランサムウェアによる被害、2位はサプライチェーンの弱点を悪用した攻撃、となりました。これは前年と同じ結果です。なお、6位の**不注意による情報漏えい等の被害は、前年の9位から上昇**しています。

企業の被害と対応状況

総務省の調査結果※2によると、インターネット利用企業における過去1年間に発生したセキュリティ侵害で、何らかの被害を受けた割合は62.0%でした。

被害内容では、標的型メールが送られてきたが44.1%、ウイルスを発見または感染が32.4%と高い状況です。

次にデータセキュリティやウイルスへの企業の対応状況をみると、97.8%が対応していると回答しています。また、対応状況として実施されている割合の高いものをまとめると、表2のとおりです。

【表2】データセキュリティやウイルスへの対応状況

対応	割合（%）
端末にウイルス対策プログラムを導入	83.8
サーバにウイルス対策プログラムを導入	57.4
ID、パスワードによるアクセス制御	56.8
ファイアウォールの設置・導入	51.5
社員教育	48.5
OSへのセキュリティパッチの導入	42.0
セキュリティポリシーの策定	40.4

総務省「令和4年通信利用動向調査（企業編）」より作成

パソコンなどの端末にウイルス対策プログラムを導入する企業が80%を超えました。サーバにウイルス対策プログラムを導入、ID、パスワードによるアクセス制御、ファイアウォールの設置・導入も50%を超えています。

セキュリティ侵害等による被害は、企業経営のさまざまな面で大きな影響を及ぼします。自社の情報セキュリティ体制について、対応ができているかどうか、今一度見直してみてはいかがでしょうか。

※1 独立行政法人情報処理推進機構「情報セキュリティ10大脅威2024」
2024年1月に発表されました。詳細は次のURLのページから確認いただけます。https://www.ipa.go.jp/security/10threats/10threats2024.html
※2 総務省「令和4年通信利用動向調査（企業編）」
2023年5月に発表された2022年8月末時点の調査結果です。詳細は次のURLのページの調査の結果、報告書及び統計表一覧、企業編から確認いただけます。https://www.soumu.go.jp/johotsusintokei/statistics/statistics05.html