令 和 ７ 年 ７ 月 １ 日
個 人 情 報 保 護 委 員 会

「『個人情報の保護に関する法律についてのガイドライン』に関するＱ＆Ａ」の更新

重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律の一部の施行に伴う関係政令の整備等に関する政令の施行に伴い、「『個人情報の保護に関する法律についてのガイドライン』に関するＱ＆Ａ」中、「１－10 講ずべき安全管理措置の内容」について、以下のとおり更新いたします。

なお、更新後のＱ＆Ａは、令和７年７月１日から適用されます。

（全般）

Ｑ10－７　標的型メール攻撃や、その他不正アクセス等による個人データの漏えい等の被害を防止するために、安全管理措置に関して、どのような点に注意すればよいですか。

Ａ10－７　ガイドライン（通則編）に記載されている技術的安全管理措置の各項目を遵守することや、それらについて従業者に対して必要な研修・注意喚起を行うことに加え、次のような措置を講ずることが考えられます。

○不正アクセス等の被害に遭った場合であっても、被害を最小化する仕組み（ネットワークの遮断等）を導入し、適切に運用すること。
○巧妙化する攻撃の傾向を把握し、適宜必要な対策を従業者に周知すること。
○個人データを端末に保存する必要がある場合、パスワードの設定又は暗号化により秘匿すること（なお、データの暗号化又はパスワードによる保護に当たっては、不正に入手した者が容易に解読できないように、暗号鍵及びパスワードの運用管理、パスワードに用いる文字の種類や桁数等の要素を考慮することも有効な取組と解されます）。

また、~~内閣サイバーセキュリティセンター（NISC）~~国家サイバー統括室や独立行政法人情報処理推進機構（IPA）等がホームページで公表しているセキュリティ対策等を参考にすることも考えられます。

（令和~~５~~７年~~３~~７月更新）

以上