

法第20条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

ガイドライン

- ◆個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、**組織的安全管理措置、人的安全管理措置、物理的安全管理措置、及び技術的な安全管理措置**を講じなければならない。
- ◆その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じる。(本ガイドラインでは、各安全管理措置を講じる際に望まれる事項を具体的に示した。)

組織的安全管理措置

安全管理について従業者(法第21条参照)の責任と権限を明確に定め、安全管理に対する規程や手順書(以下規程等という)を整備運用し、その実施状況を確認すること。

具体的には、組織体制の整備、規程等の整備と規程等に従った運用、個人データ取扱台帳の整備、評価、見直し及び改善、事故又は違反への対処など。

人的安全管理措置

従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や、教育・訓練などの措置。

物理的安全管理措置

入退館(室)の管理、個人データの盗難の防止対策、機器・装置等の物理的な保護などの措置。

技術的安全管理措置

個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視など、個人データに対する技術的な安全管理措置。

具体的には、アクセスにおける識別と認証、アクセス権限の管理、アクセスの記録、情報システムに対する不正ソフトウェア対策、移送・通信時の対策、情報システムの動作確認、情報システムの監視など。