

安全管理措置	項目	内容
組織的安全管理措置	(1) 組織体制の整備	・個人データの取扱いに関する責任者を設置、個人データを取り扱う従業者及び当該従業者が取り扱う個人データの範囲の明確化
	(2) 規律に従った運用	・法や取扱規程に違反している事実又は兆候を把握した場合の責任者への報告連絡体制を整備
	(3) 取扱状況を確認する手段の整備	・部局単位での個人情報管理台帳作成による取扱状況の把握
	(4) 漏えい等事案に対応する体制の整備	・漏えい等事案発生に対する要領の作成、対応体制の整備、発生時の報告連絡、再発防止策の検討及び決定
	(5) 取扱状況の把握と安全管理措置の見直し	・個人データの取扱状況について、定期的に自己点検、監査部局による監査の実施
人的安全管理措置	従業者の教育	・個人データの取扱いに関する留意事項について、定期的な従業員研修と点検の実施 ・個人データについての秘密保持に関する事項を就業規則に記載、従業員から個人情報保護に関する誓約書の取得
物理的安全管理措置	(1) 個人データを取り扱う区域の管理	・個人データを取り扱う区域において、従業員の入退室管理 ・権限を有しない者による個人データの閲覧を防止する措置を実施
	(2) 機器・電子媒体等の盗難等の防止	・個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を実施
	(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止	・個人データのパスワード等による保護等を行った上で電子媒体に保存
	(4) 個人データの削除、機器・電子媒体等の廃棄	・溶解、適切なシュレッダー処理等の復元不可能な手段の採用 ・電子機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトの使用による消去と上書き、物理的破壊の実施
技術的安全管理措置	(1) アクセス制御	・個人情報を取り扱うことの出来る機器及び当該機器を取り扱う者を明確化し、個人データの不要なアクセスを防止
	(2) アクセス者の識別と認証	・個人情報を取り扱う情報システムは、アクセスする者が正当なアクセス権を有する者であることを識別した結果に基づき認証
	(3) 外部からの不正アクセス等の防止	・情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護するための仕組み導入や運用
	(4) 情報システムの使用に伴う漏えい等の防止	・個人情報の物理的移送やインターネット上で外部に送信する際のデータ漏えい等を防止するための措置や運用