

環境省所管事業分野における個人情報保護に関する

ガイドライン（改正案）の概要

① 第三者からの適正な情報取得

第三者からの提供により個人情報を取得する場合に実施することが望ましいとする対応を追記

- ・ 第三者から個人情報を取得する場合は、提供元の個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）の遵守状況を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得経緯を示す書面等の点検又はこれに代わる合理的な方法により、当該個人情報の取得方法等を確認した上で、適法に取得されたものと確認ができない場合は、その取得を自粛することを含め、慎重に対応することが望ましい

② 安全管理措置の強化

事業者内部又は外部からの不正行為による個人情報の漏えい等を防止する手法として講じることが望ましいとする措置及び例示の追記

- ・ 責任所在の明確化のための措置
(例)
個人データの安全管理の実施及び運用に関する責任及び権限を有する個人情報保護管理者の設置や事業者内の個人データの取扱いの点検・改善等の監督を行う部署や委員会の設置
- ・ 新たなリスクに対応するための安全管理措置の評価、見直し及び改善に向けた監査実施体制の整備
(例)
個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者による事業者内の対応の確認
- ・ 漏えい等に早期に対処するための体制整備
(例)
漏えい等が発生した場合又は発生のおそれがある場合の連絡体制の整備

・不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性に基づく限定

(例)

スマートフォン、パソコン等の記録機能を有する機器の接続の制限及び機器の更新への対応

・入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館（室）管理の実施

(例)

入退館（室）の記録の保存

・盗難等の防止のための措置

(例)

カメラによる撮影や作業への立会い等による記録又はモニタリングの実施や記録機能を持つ媒体の持込み・持出し禁止又は検査の実施

・情報システムからの漏えい等を防止するための技術的安全管理措置

(例)

個人データへのアクセスにおける識別と認証、個人データへのアクセス制御、アクセス権限の管理、アクセス操作の記録及び不正が疑われる異常な記録の存否の定期的な確認、情報システムへの外部からのアクセス状況の監視及び当該監視システムの動作の定期的な確認、ソフトウェアに関する脆弱性対策

③ 委託先等の監督の強化

委託先の選定に当たって実施することが望ましいとする対応を追記

・委託先の安全管理措置が、少なくとも法第 20 条で求められるものと同等であることを確認するため、委託する業務内容に応じて、委託先の体制や規定等の確認に加え、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行った上で、個人情報保護管理者等が、適切に評価することが望ましい

委託契約等に定めることが望ましいとする事項及び例示を追記

・委託先の個人データの取扱いに関する事項

(例)

委託先において個人データを取り扱う者を明確にすること、委託先において講ずべき安全管理措置の内容

- ・委託された個人データの再委託に関する事項

(例)

再委託の可否及び再委託を行うに当たっての委託元への文書による事前報告又は承認

- ・契約内容が遵守されなかった場合の措置

(例)

安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項

委託先における個人データの取扱状況を把握するために望ましいとする対応を追記

定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者が、委託内容等の見直しを検討することを含め、適切に評価することが望ましい

再委託・再々委託時において実施することが望ましいとする対応を追記

委託元は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、定期的に監査を実施する等により、再委託先に対して監督を適切に果たすこと、また再委託先が法第 20 条に対する安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も同様とする。