「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の改正案（概要）

本資料は、改正案のポイントをとりまとめたものであり、実際の改正後のガイドラインの条文については、別紙の新旧対照表を参照。

１．安全管理措置

安全管理措置については、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程度を考慮し、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ものとする。その際には、特に、中小企業者（※）においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

（※）実際のガイドラインでは、中小企業基本法第２条第１項各号に掲げる中小企業者をいう。以下同じ。

（a）技術的安全管理

望まれる手法の例示として、以下を追加する。

① 個人データの監視システムについて、定期的にその動作を確認すること。

② 個人データへのアクセスやダウンロードに関するログについて、不正が疑われる異常な記録の存否を定期的に確認すること。

（b）物理的安全管理

望まれる手法の例示として、以下を追加する。

① 例えば、カメラによる撮影や作業への立ち会い等により、記録又はモニタリングを実施すること。

② 入退室の際の業務上許可を得ていない記録機能を有する媒体・機器の持ち込み・持ち出しの禁止又は検査の実施。

③ 入退室の記録を保存すること。

（c）組織的安全管理

望まれる手法の例示として、以下を追加する。

① 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者である個人情報保護管理者（ＣＰＯ）については、原則として、役員を任命すること。また、事業の規模等に応じ、社内に個人データの取扱いを総括する部署を設ける、ＣＰＯが代表者となり個人データの取扱いを監督する「管理委員会」を設置するなど、必要かつ適切な体制を整備すること。

② 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イ対策に十分な知見を有する者が社内の対応を確認する（必要に応じ、外部の知見を有する者を活用し確認することを含む。）など、監査実施体制を構築すること。

③ スマートフォン等の記録機能を有する機器の接続を制限し、機器の更新に対応するよう規程を整備すること。

（d）人的安全管理

① 教育・訓練等を実施する対象である従業者には、派遣社員等の直接雇用関係にない者も含まれることを明確化する。

２．委託先の監督

委託先の監督に当たっては、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程度を考慮し、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ものとする。その際には、特に、委託先が中小企業者になる場合においては、その事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

（a） 委託先の監督

① 委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第２０条及び本ガイドラインで求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、必要に応じ、委託先の社内体制、規程等の点検、実地検査等を行った上で、その結果について、個人情報保護管理者（ＣＰＯ）等が適切に評価することが望ましいものとする。

ⅰ）組織的安全管理措置
ア）個人データの安全管理措置を講じるための組織体制の整備
イ）個人データの安全管理措置を定める規程等の整備と規程等に従った運用
ウ）個人データの取扱状況を一覧できる手段の整備
エ）個人データの安全管理措置の評価、見直し及び改善
オ）事故又は違反への対処

ⅱ）人的安全管理措置
ア）雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結
イ）従業者に対する内部規程等の周知・教育・訓練の実施

ⅲ）物理的安全管理措置
ア）入退館（室）管理の実施
イ）盗難等の防止
ウ）機器・装置等の物理的な保護

ⅳ）技術的安全管理措置
ア）個人データへのアクセスにおける識別と認証
イ）個人データへのアクセス制御
ウ）個人データへのアクセス権限の管理
エ）個人データのアクセスの記録
オ）個人データを取り扱う情報システムについての不正ソフトウェア対策
カ）個人データの移送・送信時の対策
キ）個人データを取り扱う情報システムの動作確認時の対策
ク）個人データを取り扱う情報システムの監視

② 定期的に（少なくとも年１回）委託業務の監査を実施すること等により、委託契約に盛り込んだ内容の実施状況等を調査した上で、その結果について、個人情報保護管理者（ＣＰＯ）等が、委託の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ものとする。

③ 契約に盛り込むことが望まれる事項として、以下を追加する。

- 委託先で個人データを取り扱う者の役職又は氏名等（委託先で作業する委託先の従業者以外の者を含む。）に関する事項（契約書とは別のリスト等により、個人データを取り扱う者を把握する場合も考えられる。）。
- 安全管理に関する事項が遵守されず、委託先から個人データが流失した場合の損害賠償責任。

（b） 再委託先以降の監督

① 再委託を行う場合には、委託を行う場合と同様、委託元は、委託先が再委託を行う相手方、再委託に係る業務内容及び再委託先における個人データの取扱方法等について、委託先から事前報告又は承認の申請を求めること、及び委託先を通じて、又は必要に応じて自らが、定期的に監査を実施することが望ましいものとする。

② これらにより、委託元は、委託先が再委託先に対して法第２２条の委託先の監督を適切に行うこと、及び、再委託先が法第２０条に基づく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ものとする。

③ 再委託先が再々委託（それ以降の更なる委託を含む。）を行う場合以降も、再委託を行う場合と同様とする。

３．適正取得

① 第三者から個人情報を取得する場合（※）において、提供元の選定に当たっては、その保護法の遵守状況（例えば、オプトアウト、利用目的、開示手続き、問い合わせ・苦情の受付窓口をＨＰに明記していることなど）を確認することが望ましいものとする。

（※）

・ 法令に基づき提供される場合
・ 委託、承継、共同利用等の場合
・ 不特定かつ多数の者が購入することができるものから取得する場合

を除く。（実際のガイドラインでは、保護法第２３条第１項各号及び同条第４項各号、保護法施行令第２条第２号を引用。）

② 第三者から個人情報を取得する場合には、その都度、当該個人情報の取得方法等について、例えば、取得の経緯を示す契約書等の書面を点検する等により、適法に入手されていることを確認することが望ましいものとする。

③ 第三者から個人情報を取得する場合において、当該個人情報が適法に入手されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、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ものとする。