㈭主務大臣等への報告

ａ．個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合

認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。

ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。

・機微にわたる個人データ（㈠思想、信条又は宗教に関する事項、㈡人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、㈢勤労者の団結権、団体交渉その他団体行動の行為に関する事項、㈣集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、㈤保健医療又は性生活に関する事項等）を漏えいした場合

・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合

・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合

・その他認定個人情報保護団体が必要と考える場合

ｂ．個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合

経済産業大臣（主務大臣）に報告を行う。

ｃ．関係機関への報告

認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。

なお、ａ．及びｂ．のいずれの場合も、事業者は次の事例について、認定個人情報保護団体又は主務大臣への報告を月に一回ごとにまとめて実施することができる。

・ファクシミリやメールの誤送信（宛名及び送信者名以外に個人情報が含まれていない場合に限る。）。なお、内容物に個人情報が含まれない荷物等の宅配又は郵送を委託したところ、誤配によって宛名に記載された個人データが第三者に開示された場合については、報告する必要はない（２－２－３－２．【安全管理措置の義務違反とはならない事例（従業者の監督及び委託先の監督の義務違反ともならない場合）】参照）。

㈮事実関係、再発防止策等の公表

二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。

ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。

・影響を受ける可能性のある本人すべてに連絡がついた場合

・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合

・高度な暗号化等の秘匿化が施されている場合（ただし、㈭に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）

・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。ただし、㈭に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。）

【個人データの取扱いに関する規程等に記載することが望まれる事項の例】

以下、⑴取得・入力、⑵移送・送信、⑶利用・加工、⑷保管・バックアップ、⑸消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。

⑴取得・入力

①作業責任者の明確化

・個人データを取得する際の作業責任者の明確化

・取得した個人データを情報システムに入力する際の作業責任者の明確化（以下、併せて「取得・入力」という。）

②手続の明確化と手続に従った実施

・取得・入力する際の手続の明確化

・定められた手続による取得・入力の実施

・権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）での入力作業の実施

・個人データを入力できる端末の、業務上の必要性に基づく限定

・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、ＣＤ－Ｒ、ＵＳＢメモリ等の外部記録媒体を接続できないようにするとともに、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を制限し、媒体及び機器の更新に対応する。）

③作業担当者の識別、認証、権限付与

・個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定

・ＩＤとパスワードによる認証、生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定

・個人データの取得・入力業務を行う作業担当者に付与した権限の記録

④作業担当者及びその権限の確認

・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管と、権限外作業の有無の確認

⑵移送・送信

①作業責任者の明確化

・個人データを移送・送信する際の作業責任者の明確化

②手続の明確化と手続に従った実施

・個人データを移送・送信する際の手続の明確化

・定められた手続による移送・送信の実施

・個人データを移送・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆回線を利用して個人データを送信する場合）

・移送時におけるあて先確認と受領確認（例えば、簡易書留郵便その他個人情報が含まれる荷物を輸送する特定のサービスの利用）

・ＦＡＸ等におけるあて先番号確認と受領確認

・個人データを記した文書をＦＡＸ機等に放置することの禁止

・暗号鍵やパスワードの適切な管理

③作業担当者の識別、認証、権限付与

・個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定

・ＩＤとパスワードによる認証、生体認証等による作業担当者の識別

・作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。）

・個人データの移送・送信業務を行う作業担当者に付与した権限の記録

④作業担当者及びその権限の確認

・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認

・アクセスの記録、保管と、権限外作業の有無の確認