10　協会員は、第１項、第６項及び第７項に規定する事態が発覚した場合は、当該事態の内容等に応じて、次の各号に掲げる事項について必要な措置を講じなければならない。

⑴　事業者内部における報告及び被害の拡大防止

⑵　事実関係の調査及び原因の究明

⑶　影響範囲の特定

⑷　再発防止策の検討及び実施

⑸　個人情報保護委員会への報告及び本人への通知

11　協会員は、第１項、第６項又は第７項に基づき個人情報保護委員会又は監督当局に報告するときは、本協会に対しても同じ事項を報告しなければならない。

（解説）

⑴　第１項に規定する「個人データ」とは、協会員が取り扱う個人データをいう。

ただし、同項第⑶号に規定する「個人データ」には、「当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているもの」が含まれる。

そのため、同号に定める事態との関係では、解説⑵から⑷までにおける「個人データ」は、協会員が取り扱う個人データに加え、「当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているもの」を含む。

同号に定める事態について、詳細は解説⑹を参照のこと。

⑵　個人データの「漏えい」とは、個人データが外部に流出することをいう。

なお、個人データを第三者に閲覧されないうちに全てを回収した場合は、漏えいに該当しない。また、協会員が自らの意図に基づき個人データを第三者に提供する場合は、漏えいに該当しない。

【個人データの漏えいに該当する事例】

事例１）個人データが記載された書類を第三者に誤送付した場合

事例２）個人データを含むメールを第三者に誤送信した場合

事例３）システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となっていた場合

事例４）個人データが記載又は記録された書類・媒体等が盗難された場合

事例５）不正アクセス等により第三者に個人データを含む情報が窃取された場合

事例６）協会員のウェブサイトの入力ページが第三者に改ざんされ、ユーザーが当該ページに入力した個人情報が、当該第三者に送信された場合であり、かつ、当該協会員が、当該ページに入力される個人情報を個人情報データベース等へ入力することを予定していたとき

⑶　個人データの「滅失」とは、個人データの内容が失われることをいう。

なお、下記の場合であっても、その内容と同じデータが他に保管されている場合は、滅失に該当しない。また、協会員が合理的な理由により個人データを削除する場合は、滅失に該当しない。

【個人データの滅失に該当する事例】

事例１）個人情報データベース等から出力された氏名等が記載された帳票等を誤って廃棄した場合

㈱　当該帳票等が適切に廃棄されていない場合には、個人データの漏えいに該当する場合がある。

事例２）個人データが記載又は記録された書類・媒体等を社内で紛失した場合

㈱　社外に流出した場合には、個人データの漏えいに該当する。

⑷　個人データの「毀損」とは、個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となることをいう。

なお、下記事例２）及び事例３）の場合であっても、その内容と同じデータが他に保管されている場合は毀損に該当しない。

【個人データの毀損に該当する事例】

事例１）個人データの内容が改ざんされた場合

事例２）暗号化処理された個人データの復元キーを喪失したことにより復元できなくなった場合

事例３）ランサムウェア等により個人データが暗号化され、復元できなくなった場合

㈱　同時に個人データが窃取された場合には、個人データの漏えいにも該当する。

⑸　報告すべき事態が発覚した場合に講じるべき措置（第10項）

協会員が本条に基づき報告すべき事態（第１項、第６項及び第７項に規定する事態）が発覚した場合に当該事態の内容等に応じて講じるべき必要な措置の内容は、次のとおりである。

①　事業者内部における報告及び被害の拡大防止

責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

②　事実関係の調査及び原因の究明

漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

③　影響範囲の特定

上記②で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。

④　再発防止策の検討及び実施

上記②の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。

⑤　個人情報保護委員会への報告及び本人への通知

解説⑹から⑯を参照のこと。

なお、漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表することが望ましい。

⑹　保護法に基づく報告対象事態（第１項）

協会員は、次の①から④までに掲げる事態（以下「保護法報告対象事態」という。）を知ったときは、個人情報保護委員会から権限の委任を受けている監督当局（財務局長若しくは財務支局長又は都道府県知事）及び本協会に報告しなければならない（第１項、第11項）。

なお、保護法報告対象事態に該当しない漏えい等事案であっても、協会員は個人情報保護委員会及び本協会に任意の報告をすることができる。

保護法報告対象事態における「おそれ」については、その時点で判明している事実関係に基づいて個別の事案ごとに蓋然性を考慮して判断することになる。漏えい等が発生したおそれについては、その時点で判明している事実関係からして、漏えい等が疑われるものの漏えい等が生じた確証がない場合がこれに該当する。

①　要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態（第１項第⑴号関係）

【報告を要する事例】

事例１）従業員の健康診断等の結果を含む個人データが漏えいした場合

②　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態（第１項第⑵号関係）

財産的被害が生じるおそれについては、対象となった個人データの性質・内容等を踏まえ、財産的被害が発生する蓋然性を考慮して判断する。

【報告を要する事例】

事例１）ＥＣサイトからクレジットカード番号を含む個人データが漏えいした場合

事例２）送金や決済機能のあるウェブサービスのログインＩＤとパスワードの組み合わせを含む個人データが漏えいした場合