③　不正の目的をもって行われたおそれがある当該協会員に対する行為による個人データ（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。）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⑶号関係）

「不正の目的をもって行われたおそれがある当該協会員に対する行為」（以下「不正行為」という。）の主体には、第三者のみならず、従業者も含まれる。また、不正行為の相手方である「当該協会員」には、当該協会員が第三者に個人データの取扱いを委託している場合における当該第三者（委託先）及び当該協会員が個人データを取り扱うに当たって第三者の提供するサービスを利用している場合における当該第三者も含まれる。

当該協会員が「取得しようとしている個人情報」に該当するかどうかは、当該協会員が用いている個人情報の取得手段等を考慮して客観的に判断する。

個人情報データベース等へ入力すること等を予定していれば、最終的に個人情報に該当しない統計情報への加工を行うことを予定している場合等であっても、「個人データとして取り扱われることが予定されている」に該当する。

㈱　協会員が、個人データとして取り扱うことを予定している個人情報の取扱いを第三者に委託する場合であって、当該第三者（委託先）が当該個人情報を個人データとして取り扱う予定はないときも、ここにいう「協会員が第三者に個人データの取扱いを委託している場合」に該当する。

【報告を要する事例】

事例１）不正アクセスにより個人データ（個人情報データベース等へ入力する予定の個人情報を含む。以下、事例５）まで同じ。）が漏えいした場合

事例２）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

事例３）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４）従業者が顧客の個人データを不正に持ち出して第三者に提供した場合

㈱　従業者による個人データ又は個人情報の持ち出しの事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、個人データ又は個人情報を格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合が考えられる。

事例５）従業者の私用の端末又は取引先の端末が情報を窃取するマルウェアに感染し、その後、当該端末と協会員のサーバとの電気通信に起因して、当該サーバも当該マルウェアに感染し、個人データが漏えいした場合

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

事例７）協会員のウェブサイト上に設置された、入力ページに遷移するためのリンクやボタンが第三者に改ざんされ、当該リンクやボタンをユーザーがクリックした結果、偽の入力ページに遷移し、当該ユーザーが当該偽の入力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、当該協会員の入力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

事例８）協会員が、第三者により宛先の改ざんされた返信用封筒を顧客に送付した結果、当該返信用封筒により返信されたアンケート用紙に記入された個人情報が当該第三者に送付された場合であり、かつ、当該協会員が、当該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

㈱　サイバー攻撃の事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、次のイからホが考えられる。

イ　個人データ（個人情報データベース等へ入力する予定の個人情報を含む。ロにおいて同じ。）を格納しているサーバや、当該サーバにアクセス権限を有する端末において外部からの不正アクセスによりデータが窃取された痕跡が認められた場合

ロ　個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、情報を窃取する振る舞いが判明しているマルウェアの感染が確認された場合

ハ　マルウェアに感染したコンピュータに不正な指令を送り、制御するサーバ（Ｃ＆Ｃサーバ）が使用しているものとして知られているＩＰアドレス・ＦＱＤＮ（Fully Qualified Domain Nameの略。サブドメイン名及びドメイン名からなる文字列であり、ネットワーク上のコンピュータ（サーバ等）を特定するもの。）への通信が確認された場合

ニ　個人情報の取得手段であるウェブページを構成するファイルを保存しているサーバや、当該サーバにアクセス権限を有する端末において、外部からの不正アクセスにより、当該ファイルに、当該ウェブページに入力された情報を窃取するような改ざんがされた痕跡が確認された場合

ホ　不正検知を行う公的機関、セキュリティ・サービス・プロバイダ、専門家等の第三者から、漏えいのおそれについて、一定の根拠に基づく連絡を受けた場合

④　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態（第１項第⑷号関係）

「個人データに係る本人の数」は、当該協会員が取り扱う個人データのうち、漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数をいう。「個人データに係る本人の数」について、事態が発覚した当初1,000人以下であっても、その後1,000人を超えた場合には、1,000人を超えた時点で第１項第⑷号に該当することになる。本人の数が確定できない漏えい等において、漏えい等が発生したおそれがある個人データに係る本人の数が最大1,000人を超える場合には、第１項第⑷号に該当する。

事例）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り、当該個人データに係る本人の数が1,000人を超える場合

なお、漏えい等が発生し、又は発生したおそれがある個人データ又は個人情報について、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告を要しない。

⑺　報告義務の主体

漏えい等報告の義務を負う主体は、原則として、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う協会員である。ただし、第１項第⑶号に定める事態について漏えい等報告の義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データ又は個人情報を取り扱い、又は取得しようとしている協会員である（解説⑴参照）。

個人データの取扱いを委託している場合においては、委託元と委託先の双方が個人データ又は個人情報を取り扱っており、又は取得しようとしていることになるため、保護法報告対象事態に該当する場合には、原則として委託元と委託先の双方が報告する義務を負う。この場合、委託元及び委託先の連名で報告することができる。なお、委託先が、報告義務を負っている委託元に当該事態が発生したことを通知したときは、委託先は報告義務を免除される（第１項ただし書参照）。

また、委託元から委託先にある個人データ（個人データＡ）の取扱いを委託している場合であって、別の個人データ（個人データＢ）の取扱いを委託していないときには、個人データＢについて、委託元において報告対象事態が発生した場合であっても、委託先は報告義務を負わず、委託元のみが報告義務を負うことになる。

⑻　「速報」について（第２項）

協会員は、保護法報告対象事態を知ったときは、速やかに、個人情報保護委員会及び本協会に報告しなければならない。

報告期限の起算点となる「知った」時点については、個別の事案ごとに判断されるが、協会員が法人である場合には、いずれかの部署が当該事態を知った時点を基準とする。「速やか」の日数の目安については、個別の事案によるものの、協会員が当該事態を知った時点から概ね３～５日以内である。

個人情報保護委員会への漏えい等報告については、次の①から⑨までに掲げる事項を、原則として、個人情報保護委員会のホームページの報告フォームに入力する方法により行う。速報時点での報告内容については、報告をしようとする時点において把握している内容を報告すれば足りる。

①　「概要」

当該事態の概要について、発生日、発覚日、発生事案、発見者、第15条第１項各号該当性、委託元及び委託先の有無、事実経過等を報告する。