令 和 ６ 年 ３ 月 １ 日
個 人 情 報 保 護 委 員 会

「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａの更新

個人情報の保護に関する法律施行規則の一部を改正する規則（令和５年個人情報保護委員会規則第５号）等が令和６年４月１日に施行されること等を踏まえ、「『個人情報の保護に関する法律についてのガイドライン』に関するＱ＆Ａ」について、以下のとおり更新いたしました。

なお、更新後のＱ＆Ａは、令和６年４月１日から適用されます。

１　ガイドライン（通則編）

１-６　個人データの漏えい等の報告等（法第 26 条関係）（令和３年９月追加）

（「個人データ」の漏えい等の考え方）

Ｑ６－１　施行規則第７条に規定する「個人データ」には、どのような情報が含まれますか。

Ａ６－１　施行規則第７条に規定する「個人データ」とは、個人情報取扱事業者が取り扱う個人データをいいます。

ただし、同条第３号に規定する「個人データ」には、「当該個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているもの」が含まれるため、次の①から④までの情報が同号に規定する「個人データ」に該当します。

①　個人情報取扱事業者が取り扱う個人データ

②　個人情報取扱事業者が取り扱う個人情報（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に限る。）

③　個人情報取扱事業者が取得しようとしている個人データ

④　個人情報取扱事業者が取得しようとしている個人情報（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に限る。）

（令和６年３月追加）

（報告の対象となる事態）

Ｑ６－７　第三者の作成した個人情報取扱事業者の正規のウェブサイトに偽装したウェブサイト（いわゆるフィッシングサイト）に本人がアクセスし、ID やパスワード等を入力した場合、「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、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」（施行規則第７条第３号）に該当し報告対象となりますか。具体的には、以下の場合は報告対象となりますか。

① 本人が、当該個人情報取扱事業者の正規のウェブサイトや当該個人情報取扱事業者が送信したメール等を経由せずに偽のウェブサイトにアクセスし、ID やパスワード等を入力した場合

② 第三者が、偽のウェブサイトに遷移するリンクを、当該個人情報取扱事業者の正規のウェブサイト又は当該個人情報取扱事業者が送信したメール等に不正に設置又は記載し、本人が、当該リンクをクリックして当該偽のウェブサイトにアクセスし、ID やパスワード等を入力した場合

Ａ６－７　それぞれ次のように考えられます。

①：個人情報取扱事業者の正規のウェブサイトに偽装したウェブサイト（以下本項において「偽装ウェブサイト」という。）を第三者が不正に作成する行為は、直ちに「当該個人情報取扱事業者に対する行為」に該当するものではないと考えられます。また、本人が第三者に個人情報取扱事業者の取り扱う個人データ（当該個人情報取扱事業者が取得し、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。以下本項において同じ。）と同じ内容の情報を詐取されたのみでは、第三者に当該個人情報取扱事業者の取り扱う個人データが漏えいしたこととはなりません。そのため、①のようなケースは、当該個人情報取扱事業者による報告対象になるものではないと考えられます。

②：第三者が、偽装ウェブサイトに遷移するリンクを、当該個人情報取扱事業者の正規のウェブサイトや当該個人情報取扱事業者が送信したメール等に不正に設置等する行為は「当該個人情報取扱事業者に対する行為」に該当すると考えられます。

また、偽装ウェブサイトに入力された情報が、当該個人情報取扱事業者が「取得しようとしている」情報に該当するか否かは、個別の事案ごとに判断されます。例えば、正規のウェブサイト上の、ID 及びパスワード等を入力する入力ページに遷移するためのリンクが改ざんされていた場合に、当該リンクをクリックした個人が、当該クリックにより遷移した偽の入力ページにおいて ID 及びパスワード等を入力したときには、当該 ID 及びパスワード等は、当該個人情報取扱事業者が「取得しようとしている」情報に該当すると考えられます。

そのため、②のようなケースの第三者の行為が原因となり、本人が、当該個人情報取扱事業者が「取得しようとしている」個人情報を偽装ウェブサイトに入力し、当該個人情報が第三者に送信された場合、当該個人情報の「漏えい」に該当するため、当該個人情報取扱事業者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等を予定していれば、当該個人情報取扱事業者による報告対象になると考えられます。

いずれにせよ、正規のウェブサイトを運営する個人情報取扱事業者においては、本人が

個人情報を詐取される等の被害に遭わないよう、対策を講じる必要があると考えられます。

（令和６年３月追加）

（報告の対象となる事態）

Ｑ６－~~６~~８　~~本人が第三者の作成した~~個人情報取扱事業者の正規のウェブサイトに偽装したウェブサイト（いわゆるフィッシングサイト）~~にアクセスし、当該個人情報取扱事業者が取り扱う個人データと同じ内容の情報（ID やパスワード等）を入力した場合、報告対象となりますか。また、偽装したウェブサイト~~に本人が入力した~~当該情報~~ ID やパスワード等を利用して、第三者が本人になりすまし、個人データが表示される当該個人情報取扱事業者の正規のウェブサイトにログインした場合、報告対象となりますか。

Ａ６－~~６~~８　~~本人が第三者に個人情報取扱事業者の取り扱う個人データと同じ内容の情報を詐取されたのみでは、第三者に当該個人情報取扱事業者の取り扱う個人データが漏えいしていないことから、当該個人情報取扱事業者による報告対象にならないと考えられます。~~

~~なお、正規のウェブサイトを運営する個人情報取扱事業者においても、本人が個人情報を詐取される等の被害に遭わないよう、対策を講じる必要があると考えられます。~~

~~ただし、~~個別の事案ごとに判断され~~るものの~~ますが、偽装したウェブサイトに本人が入力した~~個人情報取扱事業者が取り扱う個人データと同じ内容の~~情報（ID やパスワード等）を利用して、第三者が本人になりすまし、個人データが表示される当該個人情報取扱事業者の正規のウェブサイトにログインした場合には、一般的には、「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ…の漏えい等が発生し、又は発生したおそれがある事態」が生じたものとして、報告対象となると考えられます。

（令和~~５~~６年３月更新）

（報告の対象となる事態）

Ｑ６－~~８~~10　~~取り扱う~~個人データ又は個人データとして取り扱われることが予定されている個人情報の一部が漏えいし、当該漏えいした個人データ又は個人情報によっては第三者が特定の個人を識別することができない場合でも、報告対象となりますか。

Ａ６－~~８~~10　施行規則第７条第１号、第２号及び第４号に定める事態について、漏えい等した情報が個人データに該当するかどうかは、当該情報を取り扱う~~個人データを漏えい等した~~個人情報取扱事業者を基準に判断するため、報告対象事態に該当すれば、報告が必要となります。

施行規則第７条第３号に定める事態について、漏えい等した情報が同号に規定する「個人データ」に該当するかどうかは、当該情報を取り扱い、又は取得しようとしている個人

情報取扱事業者を基準に判断するため、報告対象事態に該当すれば、報告が必要となります。

（令和６年３月更新）

（報告の対象となる事態）

Ｑ６－16　「不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該個人情報取扱事業者が取得し、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」（施行規則第７条第３号）について、ガイドライン（通則編）３－５－３－１（３）には、「不正行為の相手方である「当該個人情報取扱事業者」には、当該個人情報取扱事業者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）及び当該個人情報取扱事業者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。」とありますが、例えばどのような者が考えられますか。

Ａ６－16　例えば、個人情報取扱事業者が、個人データ又は個人情報（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に限る。以下本項において同じ。）の取得・利用その他の取扱いの手段として第三者を活用している場合における、当該第三者が考えられます。

（例）

○個人情報取扱事業者が、ダイレクトメールの発送業務を外部事業者に委託し、これに伴い、ダイレクトメールの送付先である顧客の氏名や住所等の個人データを当該外部事業者に伝えている場合における、当該外部事業者

○個人情報取扱事業者が入力フォーム作成ツールを利用して個人情報を取得・管理している場合における、当該ツールの提供事業者

○個人情報取扱事業者がストレージサービスを利用して個人データ又は個人情報を保管している場合における、当該サービスの提供事業者

○SNS を運営する個人情報取扱事業者が、第三者のウェブサイトに当該 SNS の「ボタン」等を設置し、当該ウェブサイトを閲覧したユーザーの閲覧履歴等の個人情報を取得している場合における、当該第三者

○決済代行サービスを提供する個人情報取扱事業者が、EC サイトの決済ページにタグを設置し、当該ページに入力されたクレジットカード情報等の個人情報を取得している場合における、当該 EC サイトの運営事業者

○決済代行サービスを提供する個人情報取扱事業者が、自らの管理する決済ページに遷移するリンクを EC サイトに設置し、当該ページに入力されたクレジットカード情報等の個人情報を取得している場合における、当該 EC サイトの運営事業者

○個人情報取扱事業者が、入力フォーム最適化サービスやスマートフォンサイト自動

変換サービス等を利用し、自己のウェブサイト上の入力ページに入力された個人情報を取得している場合における、当該サービスの提供事業者

○個人情報取扱事業者が、短縮 URL 作成サービスを利用し、当該サービスを利用して作成された短縮 URL に係るリンクをクリックして自己のウェブサイト上の入力ページに遷移した個人から個人情報を取得している場合における、当該サービスの提供事業者

○個人情報取扱事業者が、アクセス解析ツールを利用し、自己のウェブサイトを閲覧したユーザーの閲覧履歴等の個人情報を取得・管理している場合における、当該ツールの提供事業者

○個人情報取扱事業者が、返信用封筒を顧客に配布し、配送事業者による当該返信用封筒の配送を通じて個人情報を取得している場合における、当該配送事業者

（令和６年３月追加）

（報告の対象となる事態）

Ｑ６－~~14~~17　ガイドライン（通則編）３－５－３－１の「（※４~~３~~）（イ）」に、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。）「~~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」とありますが、個人データ又は個人情報データベース等へ入力する予定の個人情報を格納しているサーバにおいてマルウェアを検知した場合には、漏えいのおそれがあると判断されますか。

Ａ６－~~14~~17　ガイドライン（通則編）３－５－３－１（※４~~３~~）は、漏えいが発生したおそれがある事態に該当し得る事例を示したものであり、単にマルウェアを検知したことをもって直ちに漏えいのおそれがあると判断するものではなく、防御システムによるマルウェアの実行抑制の状況、外部通信の遮断状況等についても考慮することになります。

（令和６年３月更新）

以上