

○ 個人情報保護委員会告示第 号

個人情報の保護に関する法律（平成十五年法律第五十七号）の規定に基づき、個人情報の保護に関する法律についてのガイドライン（通則編）（平成二十八年個人情報保護委員会告示第六号）の一部を次のように改正する。

令和五年 月 日

個人情報保護委員会委員長 丹野美絵子

次の表により、改正前欄に掲げる規定の傍線を付し又は破線で囲んだ部分をこれに順次対応する改正後欄に掲げる規定の傍線を付し又は破線で囲んだ部分のように改め、改正前欄及び改正後欄に対応して掲げるその標記部分に二重傍線を付した規定（以下「対象規定」という。）は、改正前欄に掲げる対象規定を改正後欄に掲げる対象規定として移動し、改正前欄に掲げる対象規定で改正後欄にこれに対応するものを掲げていないものは、これを削り、改正後欄に掲げる対象規定で改正前欄にこれに対応するものを掲げていないものは、これを加える。

改正後	改正前
<p style="text-align: center;">個人情報保護に関する法律についてのガイドライン (通則編)</p> <p style="text-align: center;">目次</p> <p>[1・2 略]</p> <p>3 個人情報取扱事業者等の義務</p> <p style="padding-left: 20px;">[3-1~3-4 略]</p> <p>3-5 個人データの漏えい等の報告等（法第 26 条関係）</p> <p style="padding-left: 20px;">3-5-1 「<u>個人データ</u>」の「<u>漏えい等</u>」の考え方</p> <p style="padding-left: 40px;">[3-5-2~3-5-4 略]</p> <p style="padding-left: 20px;">[3-6~3-11 略]</p> <p>[4~10 略]</p> <p>【付録】</p>	<p style="text-align: center;">個人情報保護に関する法律についてのガイドライン (通則編)</p> <p style="text-align: center;">目次</p> <p>[1・2 同左]</p> <p>3 個人情報取扱事業者等の義務</p> <p style="padding-left: 20px;">[3-1~3-4 同左]</p> <p>3-5 個人データの漏えい等の報告等（法第 26 条関係）</p> <p style="padding-left: 20px;">3-5-1 「<u>漏えい等</u>」の考え方</p> <p style="padding-left: 40px;">[3-5-2~3-5-4 同左]</p> <p style="padding-left: 20px;">[3-6~3-11 同左]</p> <p>[4~10 同左]</p> <p>【付録】</p>

【凡例】

[略]

※ なお、特に断りのない限り、本ガイドラインにおいて示す法令の条番号は、本ガイドラインの公表日（令和 年 月 日）時点の条番号を示すものとする。

[削る]

[1・2 略]

3 個人情報取扱事業者等の義務

[3-1～3-3 略]

3-4 個人データの管理（法第 22 条～第 25 条関係）

3-4-1 [略]

3-4-2 安全管理措置（法第 23 条関係）

[略]

【凡例】

[同左]

※ なお、特に断りのない限り、本ガイドラインにおいて示す個人情報の保護に関する法律の条番号は、令和 3 年改正法による改正後の条番号を示すものとする。

※ その他の法令に係る条文は、本ガイドラインの公表日（令和 4 年 9 月 8 日）時点の条番号を示すものとする。

[1・2 同左]

3 個人情報取扱事業者等の義務

[3-1～3-3 同左]

3-4 個人データの管理（法第 22 条～第 25 条関係）

3-4-1 [同左]

3-4-2 安全管理措置（法第 23 条関係）

[同左]

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。

なお、「その他の個人データの安全管理のために必要かつ適切な措置」には、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の漏えい等を防止するために必要かつ適切な措置も含まれる。

具体的に講じなければならない措置や当該措置を実践するための手法の例等については、「10（別添）講ずべき安全管理措置の内容」を参照のこと。

[3-4-3・3-4-4 略]

3-5 個人データの漏えい等の報告等（法第 26 条関係）

3-5-1 「個人データ」の「漏えい等」の考え方

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない。

具体的に講じなければならない措置や当該措置を実践するための手法の例等については、「10（別添）講ずべき安全管理措置の内容」を参照のこと。

[3-4-3・3-4-4 同左]

3-5 個人データの漏えい等の報告等（法第 26 条関係）

3-5-1 「漏えい等」の考え方

3-5-1-1 規則第7条の「個人データ」の考え方

規則第7条は、法第26条第1項に基づく漏えい等の報告の対象となる事態について定めているところ、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う。

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、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、3-5-1-2（「漏えい」の考え方）から3-5-1-4（「毀損」の考え方）までにおける「個人データ」は、個人情報取扱事業者が取り扱う個人データに加え、「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。

同号に定める事態について、詳細は3-5-3-1（報告対象となる事態）を参照のこと。

3-5-1-2 「漏えい」の考え方

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。

【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

[新設]

3-5-1-1 「漏えい」の考え方

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。

【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) 個人情報取扱事業者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、当該個人情報取扱事業者が、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

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、個人情報取扱事業者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。

（※）個人情報取扱事業者は、個人データの第三者への提供に当たり、原則としてあらかじめ本人の同意を取得する必要がある。

3-5-1-3 「滅失」の考え方

[略]

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

[新設]

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、個人情報取扱事業者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。

（※）個人情報取扱事業者は、個人データの第三者への提供に当たり、原則としてあらかじめ本人の同意を取得する必要がある。

3-5-1-2 「滅失」の考え方

[同左]

3-5-1-4 「毀損」の考え方

[略]

3-5-2 [略]

3-5-3 個人情報保護委員会への報告（法第 26 条第 1 項関係）

3-5-3-1 報告対象となる事態

[略]

規則第 7 条

法第 26 条第 1 項本文の個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

- (1) 要配慮個人情報が含まれる個人データ（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を講じたものを除く。以下この条及び次条第 1 項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第 1 項において「漏えい等」という。）が発生し、又は発生したおそれがある事態
- (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

3-5-1-3 「毀損」の考え方

[同左]

3-5-2 [同左]

3-5-3 個人情報保護委員会への報告（法第 26 条第 1 項関係）

3-5-3-1 報告対象となる事態

[同左]

規則第 7 条

法第 26 条第 1 項本文の個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

- (1) 要配慮個人情報が含まれる個人データ（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を講じたものを除く。以下この条及び次条第 1 項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第 1 項において「漏えい等」という。）が発生し、又は発生したおそれがある事態
- (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

(3) 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。）の漏えい等が発生し、又は発生したおそれがある事態

(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

[略]

[(1) ・ (2) 略]

(3) 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。）の漏えい等が発生し、又は発生したおそれがある事態（規則第7条第3号関係）

「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」（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又は個人情報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

(3) 不正の目的をもって行われた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

(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

[同左]

[(1) ・ (2) 同左]

(3) 不正の目的をもって行われた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（規則第7条第3号関係）

「不正の目的をもって」漏えい等を発生させた主体には、第三者のみならず、従業者も含まれる。

個人情報取扱事業者が個人データ又は個人情報を取り扱うにあ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。

当該個人情報取扱事業者が「取得しようとしている個人情報」に該当するかどうかは、当該個人情報取扱事業者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。

【報告を要する事例】 (※3)

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 (※4)

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、当該端末と個人情報取扱事業者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

【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が漏えいした場合 (※3)

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 (※4)

[新設]

データが漏えいした場合

事例6) 個人情報取扱事業者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、当該個人情報取扱事業者が、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

[新設]

事例7) 個人情報取扱事業者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、当該個人情報取扱事業者が、当該個人情報取扱事業者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

[新設]

事例8) 個人情報取扱事業者が、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を予定していたとき

[新設]

(4) [略]

(4) [同左]

[(※1) ・ (※2) 略]

[(※1) ・ (※2) 略]

(※3) 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

(※3) 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（ア）から（オ）が考えられる。

（ア）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。（イ）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

（イ）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

（ウ）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

（エ）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

（オ）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、

ある事態に該当し得る事例としては、例えば、次の（ア）から（エ）が考えられる。

（ア）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

（イ）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

（ウ）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

[新設]

（エ）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) 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。

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。

3-5-3-2 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個人情報取扱事業者である。ただし、規則第7条第3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個人情報取扱事業者である(3-5-1-1(規則第7条の「個人データ」の考え方)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

一定の根拠に基づく連絡を受けた場合

(※4) 従業者による個人データ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。

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。

3-5-3-2 報告義務の主体

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を取り扱う個人情報取扱事業者である。

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を取り扱っていることになるため、報告対象事態に該当

いることになるため、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（3-5-3-5（委託元への通知による例外）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については、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。

3-5-3-3 速報（規則第8条第1項関係）

規則第8条（第1項）

- 1 個人情報取扱事業者は、法第26条第1項本文の規定による報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告をしようとする時点において把握しているものに限る。次条において同じ。）を報告しなければならない。
 - (1) 概要
 - (2) 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（前条第3号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）の項目
 - (3) 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

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（3-5-3-5（委託元への通知による例外）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については、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。

3-5-3-3 速報（規則第8条第1項関係）

規則第8条（第1項）

- 1 個人情報取扱事業者は、法第26条第1項本文の規定による報告をする場合には、前条各号に定める事態を知った後、速やかに、当該事態に関する次に掲げる事項（報告をしようとする時点において把握しているものに限る。次条において同じ。）を報告しなければならない。
 - (1) 概要
 - (2) 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の項目
 - (3) 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

- (4) 原因
- (5) 二次被害又はそのおそれの有無及びその内容
- (6) 本人への対応の実施状況
- (7) 公表の実施状況
- (8) 再発防止のための措置
- (9) その他参考となる事項

[略]

(1) [略]

(2) 「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（前条第3号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）の項目」

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（規則第7条第3号に定める事態については、同号に規定する個人情報を含む。）の項目について、媒体や種類（顧客情報、従業員情報の別等）とともに報告する。

(3) 「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」

る本人の数

- (4) 原因
- (5) 二次被害又はそのおそれの有無及びその内容
- (6) 本人への対応の実施状況
- (7) 公表の実施状況
- (8) 再発防止のための措置
- (9) その他参考となる事項

[同左]

(1) [同左]

(2) 「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の項目」

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の項目について、媒体や種類（顧客情報、従業員情報の別等）とともに報告する。

(3) 「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」

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（規則第7条第3号に定める事態については、同号に規定する個人情報を含む。）に係る本人の数について報告する。

[(4) ~ (9) 略]

[3-5-3-4・3-5-3-5 略]

3-5-4 本人への通知（法第26条第2項関係）

[略]

3-5-4-1 通知対象となる事態及び通知義務の主体

個人情報取扱事業者は、報告対象事態を知ったときは、本人への通知を行わなければならない。

通知義務を負う主体は、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個人情報取扱事業者である。ただし、規則第7条第3号に定める事態について本人への通知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個人情報取扱事業者である（3-5-1-1（規則第7条の「個人データ」の考え方）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

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について報告する。

[(4) ~ (9) 同左]

[3-5-3-4・3-5-3-5 同左]

3-5-4 本人への通知（法第26条第2項関係）

[同左]

3-5-4-1 通知対象となる事態及び通知義務の主体

個人情報取扱事業者は、報告対象事態を知ったときは、本人への通知を行わなければならない。

通知義務を負う主体は、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を取り扱う個人情報取扱事業者である。

個人データの取扱いを委託している場合において、委託先が、報告義務

双方が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こととなるため、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本人への通知を行う義務を負う。委託先が、報告義務を負っている委託元に3-5-3-3 (1) から (9) までに掲げる事項のうち、その時点で把握しているものを通知したときは、委託先は報告義務を免除されるとともに、本人への通知義務も免除される。なお、委託元への通知を行った委託先は、必要に応じて委託元による本人への通知に協力することが求められる。

3-5-4-2 [略]

3-5-4-3 通知の内容

本人へ通知すべき事項については、漏えい等報告における報告事項のうち、「概要」（規則第8条第1項第1号）、「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（前条第3号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）の項目」（同項第2号）、「原因」（同項第4号）、「二次被害又はそのおそれの有無及びその内容」（同項第5号）及び「その他参考となる事項」（同項第9号）（※）に限られている。これらの事項が全て判明するまで本人への通知をする必要がないというものではなく、本人への通知は、「当該事態の状況に応じて速やかに」行う必要がある（3-5-4-2（通知の時間的制限）参照）。

を負っている委託元に3-5-3-3 (1) から (9) までに掲げる事項のうち、その時点で把握しているものを通知したときは、委託先は報告義務を免除されるとともに、本人への通知義務も免除される。

3-5-4-2 [同左]

3-5-4-3 通知の内容

本人へ通知すべき事項については、漏えい等報告における報告事項のうち、「概要」（規則第8条第1項第1号）、「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の項目」（同項第2号）、「原因」（同項第4号）、「二次被害又はそのおそれの有無及びその内容」（同項第5号）及び「その他参考となる事項」（同項第9号）（※）に限られている。これらの事項が全て判明するまで本人への通知をする必要がないというものではなく、本人への通知は、「当該事態の状況に応じて速やかに」行う必要がある（3-5-4-2（通知の時間的制限）参照）。

本人への通知については、「本人の権利利益を保護するために必要な範囲において」行うものである。

また、当初報告対象事態に該当すると判断したものの、その後実際には報告対象事態に該当していなかったことが判明した場合には、本人への通知が「本人の権利利益を保護するために必要な範囲において」行うものであることに鑑み、本人への通知は不要である。

[略]

[3-5-4-4・3-5-4-5 略]

[3-6~3-11 略]

[4~9 略]

10 (別添) 講ずべき安全管理措置の内容

法第 23 条に定める安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等を次に示す(※1)。

安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量

本人への通知については、「本人の権利利益を保護するために必要な範囲において」行うものである。

また、当初報告対象事態に該当すると判断したものの、その後実際には報告対象事態に該当していなかったことが判明した場合には、本人への通知が「本人の権利利益を保護するために必要な範囲において」行うものであることに鑑み、本人への通知は不要である。

[同左]

[3-5-4-4・3-5-4-5 同左]

[3-6~3-11 同左]

[4~9 同左]

10 (別添) 講ずべき安全管理措置の内容

法第 23 条に定める安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等を次に示す。

安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量

を含む。) 、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。

なお、中小規模事業者(※2)については、その他の個人情報取扱事業者と同様に、法第 23 条に定める安全管理措置を講じなければならないが、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその義務を履行し得るような手法の例を示すこととする。もっとも、中小規模事業者が、その他の個人情報取扱事業者と同様に「手法の例示」に記述した手法も採用することは、より望ましい対応である。

(※1) 法第 23 条に定める「その他の個人データの安全管理のために必要かつ適切な措置」には、個人情報取扱事業者が個人データとして取り扱うために取得し、又は取得しようとしている個人情報の漏えい等を防止するために必要かつ適切な措置も含まれる。そのため、次に掲げる措置及び例示における「個人データ」には、当該個人情報も含まれる。

(※2) 「中小規模事業者」とは、従業員(※3)の数が 100 人以下の個人情報取扱事業者をいう。ただし、次に掲げる者を除く。

- ・その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数合計が過去 6

を含む。) 、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。

なお、中小規模事業者(※1)については、その他の個人情報取扱事業者と同様に、法第 23 条に定める安全管理措置を講じなければならないが、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその義務を履行し得るような手法の例を示すこととする。もっとも、中小規模事業者が、その他の個人情報取扱事業者と同様に「手法の例示」に記述した手法も採用することは、より望ましい対応である。

[新設]

(※1) 「中小規模事業者」とは、従業員(※2)の数が 100 人以下の個人情報取扱事業者をいう。ただし、次に掲げる者を除く。

- ・その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数合計が過去 6

<p>月以内のいずれかの日において 5,000 を超える者</p> <ul style="list-style-type: none"> ・委託を受けて個人データを取り扱う者 <p><u>(※3)</u> 中小企業基本法（昭和 38 年法律第 154 号）における従業員をいい、労働基準法（昭和 22 年法律第 49 号）第 20 条の適用を受ける労働者に相当する者をいう。ただし、同法第 21 条の規定により同法第 20 条の適用が除外されている者は除く。</p> <p>[10-1~10-7 略]</p> <p>【付録】 [略]</p>	<p>月以内のいずれかの日において 5,000 を超える者</p> <ul style="list-style-type: none"> ・委託を受けて個人データを取り扱う者 <p><u>(※2)</u> 中小企業基本法（昭和 38 年法律第 154 号）における従業員をいい、労働基準法（昭和 22 年法律第 49 号）第 20 条の適用を受ける労働者に相当する者をいう。ただし、同法第 21 条の規定により同法第 20 条の適用が除外されている者は除く。</p> <p>[10-1~10-7 同左]</p> <p>【付録】 [同左]</p>
<p>備考 表中の [] の記載は注記である。</p>	

附 則

この告示は、令和六年四月一日から施行する。