弁護士法人　三宅法律事務所

Miyake　& Partners

Miyake newsletter

個人情報保護法ニュースＮｏ.６

はじめに

　平素より大変お世話になっております。
さて、今回は個人情報保護法ニュース「**個人情報保護法関連の規則・ガイドラインの改正**」をご案内させていただきます。

令和６年１月２３日

弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。

弁護士法人三宅法律事務所
弁護士渡邉雅之、弁護士越田晃基、弁護士岩田憲二郎、弁護士出沼成真（執筆者）
TEL 03-5288-1021 FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp
k-koshida@miyake.gr.jp
k-iwata@miyake.gr.jp
n-idenuma@miyake.gr.jp

個人情報保護法関連の規則・ガイドラインの改正

令和５年（2023 年）12 月 27 日、「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）が公布されるとともに、次の各告示が公布された。

・「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）の一部を改正する告示」（令和５年個人情報保護委員会告示第７号）
・「個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）の一部を改正する告示」（令和５年個人情報保護委員会告示第８号）
・「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）の一部を改正する告示」（令和５年個人情報保護委員会告示第９号）
・「個人情報の保護に関する法律についてのガイドライン（行政機関等編）の一部を改正する告示」（令和５年個人情報保護委員会告示第 10 号）。

これらは、いわゆる Web スキミング[1]による情報流出等が、漏えい等報告等及び安全管理措置の対象となることを明確化するための規則・ガイドラインの改正である。

また、外国にある第三者への個人データの提供（法 28 条関係）に関して、いわゆるガバメントアクセスに関する情報提供に関して、「民間が保有する個人データに対するガバメントアクセスに関する宣言」に示される原則を参考にすることが明記された。

本稿では、これらの改正に関して、令和５年（2023 年）12 月 27 日に公表されたパブリックコメントに対する回答を参考に解説する。

なお、本稿において用いる略語は、本文中に記載のあるもののほか、次のとおりとするとともに、それぞれの改正条文のことを「改正〇〇」と明記する。

個人情報の保護に関する法律	個人情報保護法又は法
個人情報の保護に関する法律施行令	令
個人情報の保護に関する法律施行規則	規則
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）	通則編ガイドライン
個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）	外国第三者提供編ガイドライン
個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）	確認・記録義務編ガイドライン
「『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（案）』、『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）の一部を改正する告示（案）』、『個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）の一部を改正する告示（案）』、『個人情報の保護に関する法律についてのガイドライン（行政機関等編）の一部を改正する	パブコメ回答

[1] 攻撃者が悪意のあるコードをウェブサイトに挿入し、ユーザーが Web ページのフォームに入力したデータを盗み取る攻撃。

告示（案）』及び『個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）の一部を改正する告示（案）』に関する意見募集の結果について」（https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCM1040&id=240000096&Mode=1）の「（別紙）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案等に関する意見募集結果」（https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000265957）	

第１．漏えい等報告等に関する改正

１．改正の背景

法 26 条は、個人データの漏えい、滅失若しくは毀損（以下「漏えい等」という。）が発生し、又は発生したおそれがある場合の個人情報保護委員会への報告および本人への通知（以下「漏えい等報告等」という。）に関する制度を定めているところ、漏えい等報告等を要する「個人の権利利益を害するおそれが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」（法 26 条１項）については、以下の４つの事態が定められている（規則７条各号）[2]。

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（規則７条１号）
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（同条２号）
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（同条３号）
④個人データに係る本人の数が 1,000 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（同条４号）

このうち、上記①から③の事態が発生した場合は、１件でも漏えい等が発生し、又は発生したおそれがある事態の場合には、漏えい等報告等の対象となる。上記①から③のいずれにも該当しない場合は、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の場合に漏えい等報告等の対象となる。

上記③の「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」は、「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」（通則編ガイドライン 3-5-2【個人データの漏えいに該当する事例】事例５）などを想定している。

もっとも、上記③の事態に、いわゆる Web スキミングによる情報流出等が、漏えい等報告等の対象となるか否かは明確ではなかった。今回の改正は、Web スキミングによる情報流出等の事態を漏えい等報告等の対象とするための規則・ガイドラインの改正である[3]。

---

[2] 漏えい等が発生し、又は発生したおそれのある個人データについて、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ている場合には、漏えい等報告等の対象外となる（規則７条１号括弧書）。

[3] 「改正個人情報保護法の施行状況について」（個人情報保護委員会事務局・令和５年９月

具体的には、**「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」**（改正通則編ガイドライン 3-5-2【個人データの漏えいに該当する事例】の「事例６」参照）のような場合を漏えい等報告および本人通知の対象とするための改正である。

２．改正規則７条３号の漏えい等報告等の対象事態

（１）対象となる個人データ

改正規則７条３号の漏えい等報告等の対象事態である「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」の「個人データ」に、**「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」**が含まれることとされる。

規則７条は、法 26 条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 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。（通則編ガイドライン 3-5-1-1「規則第 7 条の「個人データ」の考え方」）

これまでは、「個人データ」についてのみ漏えい等報告等の対象事態としてきたところ、「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」が含まれることになると、法 26 条の委任の範囲内と言えるか問題となる。

この点、個人情報保護委員会は、法 26 条１項本文は、「その取り扱う…個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいもの」を報告対象事態として定めることを施行規則に委任しているところ、**「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「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」により漏えい等した場合、当該個人情報取扱事業者が取り扱う個人データの安全の確保に係る事態が生じており、かつ、当該事態は本人の権利利益に対する影響が大きいと考えられることから、法の委任の範囲内**と考えられる（パブコメ回答５番・６番・16 番・23 番）。

（２）不正行為の相手方

改正規則７条３号は「不正の目的をもって行われたおそれがある個人データ」から「不正

---

27 日）（https://www.ppc.go.jp/files/pdf/230927_shiryou-1.pdf）

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」に改められるが、これは**不正行為の相手方が「個人情報取扱事業者」である必要があることを明確にするものであり、当該部分の規律内容を変更するものではない**（パブコメ回答４番）。

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（通則編ガイドライン 3-5-3-1(3)）。

なお、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「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」に該当する（改正通則編ガイドライン 3-5-3-1(3)（※３））。

（３）不正行為の主体

「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、委託先も含まれる（パブコメ回答 38 番）。

（４）判断基準

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される**（改正通則編ガイドライン 3-5-3-1(3)）。

「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」に該当するかどうかは、**漏えい等又はそのおそれが発生した時点**を基準として、個別の事案に応じて判断される（パブコメ回答 17 番）。

（５）取得しようとしている個人情報に関する事例

改正通則編ガイドライン 3-5-3-1(3)【報告を要する事例】の事例 6)、事例 7）及び事例 8）において、「取得しようとしている個人情報」に該当する事例が示されている（パブコメ回答 11 番）。

改正通則編ガイドラインの上記の事例６）及び事例７）においては、事業者自身が保有するサイト自体が改ざんされ情報漏えいが発生した場合を想定している。

○「取得しようとしている個人情報」に該当する事例（改正通則編ガイドライン 3-5-3-1(3)【報告を要する事例】）

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

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

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

なお、事例５として、「**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、個人データが漏えいした場合**」も新たに追加された。

これは、仮に従業員の私用の端末又は取引先の端末を介したものであるとしても、個人情報取扱事業者のサーバが情報を窃取するマルウェアに感染し、当該マルウェアにより個人データが漏えいしたことに変わりなく、「当該個人情報取扱事業者に対する行為」該当性を否定し得ないことを明確化したものであると考えられる（パブコメ回答 37 番）。さらに進んで、仮に個人情報取扱事業者のサーバがマルウェア感染に感染していなくとも、「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」に該当し得る旨示唆されている（パブコメ回答 37 番）。例えば、従業者の私用端末又は取引先の端末が当該個人情報取扱事業者の業務の用に供されているのであれば、当該端末がマルウェアに感染し、個人データが流通した場合であっても、改正規則７条３号に基づく報告を要すると解されよう。

（６）サイバー攻撃に関する追加事案

改正通則編ガイドライン 3-5-3-1（※４）においては、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が掲げられているが、「個人情報データベース等へ入力する予定の個人情報」に関して、以下の事案が追加されている（下線部が追加箇所）。

（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。）**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**（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。）**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）（略）

（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

（７）その他の事案

ア．なりすましメールが第三者から送信された場合

個人情報取扱事業者になりすましたメールが第三者から送信されたことをもって、直ちに「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」に該当するものではないと考えられる（パブコメ回答 14 番）。

たとえば、第三者が事業者Ａになりすましてメール等を送信し、メール等を受信した者がフィッシングサイト等の複製または模倣サイトに誘導されて個人情報を入力し詐取された場合、なりすまされた事業者Ａには報告義務はないと考えられる。

イ．ＥＣサイト内のクレジットカード決済画面の改ざん

ＥＣサイト内のクレジットカード決済画面が不正に改ざんされたこと等により、カード会員がフィッシングサイトに誘導され、クレジットカード番号や個人情報が第三者に詐取された場合、改ざんがクレジットカード会社「に対する行為」に該当するかどうかは、クレジットカード会社とＥＣサイト運営者との関係、クレジットカード決済画面に入力された個人情報の取扱状況等を踏まえ、個別の事案に応じて判断する必要がある（パブコメ回答 15 番）。

ウ．名刺管理ソフトに登録予定の名刺の窃取

名刺管理ソフトが個人情報データベース等に該当する場合、名刺管理ソフトに登録する予定の名刺上の個人情報は「個人データとして取り扱われることが予定されているもの」に該当し、個人情報取扱事業者の従業員が当該名刺を窃取された場合は、「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」漏えいに該当すると考えられる（パブコメ回答 20 番）。

エ．個人情報取扱事業者が個人情報を取得するまでに行われた行為

個人情報取扱事業者が個人情報を取得するまでに行われた行為であっても、「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」に該当し得る（パブコメ回答 13 番）。

例えば、顧客が事業者Ａに申込書を送付したが、配送過程で窃盗に遭い所在不明となった。この場合、事業者Ａに対する不正の目的で行われた行為での漏えい等に該当し、事業者Ａには報告義務がある。

オ．最終的に統計情報への加工が予定されている場合

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（改正通則編ガイドライン 3-5-3-1(3)）。

カ．委託先ではない提供元の漏えい

事業者Ａが、事業者Ｂから個人情報の提供を受け又は受けようとする場合、提供元となる事業者Ｂに対する第三者の行為により事業者Ｂから当該個人情報が漏えい等したケースにおいて、事業者Ａが事業者Ｂに漏えい等した個人情報の取扱いを委託しておらず、また、事業者Ａが漏えい等した個人情報を取り扱うにあたって事業者Ｂの提供するサービスを利用していないのであれば、通常、事業者Ｂに対する行為は事業者Ａ「に対する行為」に該当しないと考えられるので、提供元となる事業者Ｂに対する第三者の行為により事業者Ｂから当該個人情報が漏えい等したケースは、事業者Ａに対する行為ではないため、事業者Ａには報告義務はない（パブコメ回答 10 番）。

キ．従業員がアンケート用紙を落とした場合

改正通則編ガイドライン 3-5-3-1(3)【報告を要する事例】事例８は、「**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**」に個人情報保護委員会に報告を要する事案である。

これに対して、従業者が誤ってアンケート用紙を落とし、これが見つからないことのみをもって、直ちに「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…漏えい等が発生し、又は発生したおそれがある事態」に該当するものではない（パブコメ回答８番）。

（８）従業員による持ち出し事例

通則編ガイドライン 3-5-3-1(3)【報告を要する事例】事例４は、「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」に個人情報保護委員会への報告を要する事案で改正前から規定されていた事例である。

この事例に関して、改正通則編ガイドラインでは、この事例に関する（※５）（旧※４）につき、下線部分が追加された。

> **従業者による個人データ<u>又は個人情報</u>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<u>又は個人情報</u>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。**

追加された「個人情報」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」の漏えい等のことであり、「個人データとして取り扱われることが予定されていない個人情報」はサーバに格納されていたとしても報告等対象事態に含まれない（パブコメ回答 42 番）。

（９）適用時期

法 26 条 1 項は「個人情報保護委員会規則で定めるものが生じたとき」の報告義務を規定

しているため、本規則の改正規定により新たに報告対象事態となった漏えい等事案については、本規則の施行日である令和 6 年（2024 年）4 月 1 日以降に漏えい等又はそのおそれが生じたものに限って同項に基づく報告義務が課される（パブコメ回答９番）。

３．個人情報保護委員会への報告（法 26 条１項、改正規則８条、改正通則編ガイドライン 3-5-3-2）

（１）報告対象事項（規則８条１項・２項）

個人情報保護委員会への報告事項（速報・確報いずれも）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」が含まれる（規則８条１項２号、２項）が、改正により、規則７条３号に定める事態（**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**）については、**「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」**についても報告対象事項となる。

（２）漏えい等報告の義務を負う主体

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（**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**）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（改正通則編ガイドライン 3-5-1-1（規則第７条の「個人データ」の考え方）参照）。

４．本人への通知義務（法 26 条２項）

（１）通知対象となる事態

個人情報取扱事業者は、規則７条各号の事態を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、規則８条１項１号、２号、４号、５号、９号に定める事項を通知しなければならない。

通知対象となる事態は、個人情報保護委員会への報告対象事態と同じである。したがって、規則７条３号に定める事態については、「個人データ」のほか、「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」も対象となる。

（２）通知義務を負う主体（通則編ガイドライン 3-5-4-1）

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７条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（通則編ガイドライン 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い、又は取得しようとして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本人への通知を行う義務を負う。

第２．安全管理措置

１．講ずべき安全管理措置の内容

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、当該個人情報取扱事業者において個人情報データベース等を構成する前の段階で漏えい等した場合であっても、個人情報データベース等を構成することとなった後の段階で漏えい等した場合、すなわち、個人情報取扱事業者が取り扱っている個人データが漏えい等した場合と同様の結果が生ずることになる。

そのため、個人情報保護法 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。

通則編ガイドラインの改正により、個人情報保護法 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**ことが追記された（改正通則編ガイドライン「10（別添）講ずべき安全管理措置の内容」（※１））。

これは従前からの解釈を明確化したものであり、通則編ガイドラインの改正の施行（令和６年（2024 年）４月１日）前であっても、「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」として、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を講じる必要がある（パブコメ回答 27 番）。

２．保有個人データに関する事項の公表等

個人情報取扱事業者が保有個人データに関して、**「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」**に置かなければならない事項の一つとして、**「法 23 条の規定により保有個人データの安全管理のために講じた措置（略）」**がある（法 32 条１項４号、令 10 条１号）。

「保有個人データの安全管理のために講じた措置」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保有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講じた措置」**も含まれることが明確化された（改正通則編ガイドライン 3-8-1(1)）。

３．外国にある第三者が講ずべき安全管理措置

個人情報取扱事業者が、EU 加盟国及び英国以外の本邦以外の国又は地域にいる第三者に個人データを提供する場合、法第４章第２節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置（「相当措置」）を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している場合には、法 27 条に従い個人データの提供をすることが認められる（法 28 条１項）。

相当措置の一つとして、「安全管理措置（法 23 条の趣旨に沿った措置）」として、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、通則ガイドラインの「10（別添）講ずべき安全管理措置の内容」を参照することとされている（外国第三者編ガイドライン 4-2-7）。

上記１のとおり、法 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ので、相当措置を講ずる外国にある第三者もかかる措置を講ずる必要がある。

４．施行日

第１の漏えい等報告等と同様に、施行期日は令和６年（2024 年）４月１日とされているが、上記１のとおり、従前からの取扱いを明確化したものであるので、現行の安全管理措置においても講ずべき措置である。

第３．ガバメントアクセスに関する基準の明確化

個人情報取扱事業者が外国（EU 加盟国及び英国を除く）にある第三者に個人データを提供する場合、①あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供して本人の同意を得るか（法 28 条１項、２項）、または、②個人データの取扱いについて法第４章第２節の規定により個人情報取扱事業者が講ずべきこととされている措置に相当する措置（「相当措置」）を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備した上で、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに本人の求めに応じて当該必要な措置に関する情報を当該本人に提供した上で法 27 条の規定に従って個人データを提供しなければならない（法 28 条１項、３項）。

①の同意取得時の情報提供として求められる「当該外国における個人情報の保護に関す

る制度に関する情報」（規則 17 条２項２号）の一つとして**「本人の権利利益に重大な影響を及ぼす可能性のある制度」**（外国第三者提供編ガイドライン 5-2(2)②(エ)）が、②の「相当措置の継続的な実施を確保するために必要な措置」（規則 18 条１項１号）として定期的に確認すべき事項および本人の求めに応じて情報提供すべき事項として**「当該相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその内容」**がある。

ガイドラインに記載された上記のいずれの「制度」についても、**「事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度」**（いわゆるガバメントアクセス）が事例として掲げられている（外国第三者提供編ガイドライン 5-2(2)②(エ)【本人の権利利益に重大な影響を及ぼす可能性のある制度に該当する事例】事例１、6-1(1)【相当措置の実施に影響を及ぼすおそれのある外国の制度に該当する事例】事例１、6-2-2(5)【相当措置の実施に影響を及ぼすおそれのある外国の制度の概要についての情報提供に該当する事例】事例１）。

今回のガイドラインの改正により、このガバメントアクセスに関し、**「事業者が保有する個人情報について政府による情報収集が可能となる制度に関して、本人の権利利益に重大な影響を及ぼす可能性のある制度に該当するか否かを判断するに当たっては、例えば、OECD「民間部門が保有する個人データに対するガバメントアクセスに関する宣言」（2022 年）を参照することが考えられる。**」との注記が追加された。この追記については、改正告示の公布日である令和５年 12 月 27 日から施行されている。

「民間が保有する個人データに対するガバメントアクセスに関する宣言」[4]は、2022 年 12 月 14 日から 15 日まで、スペインのグランカナリア島において、議長国のスペイン並びに副議長国のデンマーク、日本、トルコ、英国及び米国のリーダーシップの下、「信頼性のある、持続可能で、包摂的なデジタルの未来の構築による、長期的な復興及び経済成長の促進」をテーマに、デジタル経済政策委員会（CDEP）の閣僚会合で公表された宣言である。

同宣言は、OECD 加盟国での法執行・国家安全保障の目的のためのガバメントアクセスの原則を、OECD 加盟国の既存の法と実務から導き出された共通点として反映したものであり、OECD プライバシーガイドラインを補完し、ガバメントアクセスにかかる事実上の国際スタンダードとして機能することが期待される（パブコメ回答 67 番）。

同宣言は、OECD 加盟国の既存の法と実務から導き出された共通点を反映するものとして、以下のガバメントアクセスに関する共通の原則を宣言している。

> Ⅰ. 法的根拠
>
> 民間部門が保有する個人データへのガバメントアクセスは、当該国の法的枠組みによってその根拠が定められ、また、規制される。この法的枠組みは、政府当局を拘束し、また、法の支配の下で活動する民主的に設立された機関によって採用され、実施される。こ

[4] 令和４年（2022 年）12 月 21 日に開催された第 227 回個人情報保護委員会の添付資料に同宣言および仮訳が公表されている（https://www.ppc.go.jp/aboutus/minutes/2022/20221221/）。

の法的枠組みは、個人が悪用・濫用のリスクに対して十分な保証を得られるよう、ガバメントアクセスに関する目的、条件、制限及び保護措置を定める。
II. 正当な目的 ガバメントアクセスは、特定された正当な目的の追求を支援するものである。政府は、法の支配に従いつつ、当該目的のためだけにアクセスを求める。ガバメントアクセスは、正当な目的に照らして過剰ではない方法で、かつ、必要性、比例性、合理性という法的な基準及び悪用・濫用のリスクから保護するその他の基準に基づき、当該国の法的枠組みで規定され、解釈されるとおりに実施されるものである。 政府は、批判や反対意見を抑えたり、圧迫したりする目的のために、また、年齢、精神障害若しくは身体障害、民族性、先住民の地位、ジェンダーのアイデンティティー若しくは表現、性的志向、又は政治的若しくは宗教的所属を含むがこれらに限らない特性のみに基づいて特定の個人や集団に不利益を被らせる目的のために、個人データへのアクセスを求めない。
III. 承認 適用される基準、規則及び手続きに従ってアクセスが行われることを確保するため、ガバメントアクセスに対する事前承認（「承認」）の要件は、法的枠組みにおいて確立される。 これらの要件は、ガバメントアクセスの結果として生じるプライバシー及びその他の人権と自由への干渉の程度に見合うものである。これらの要件は、承認を求め、付与するための基準、従うべき手続き及び承認を付与する主体を規定する。 より厳格な承認要件は、より深刻な干渉の場合に設けているものであり、司法当局又は公平な非司法当局からの承認を求めることが含まれ得る。緊急事態における承認要件の例外措置は、法的枠組みにおいて規定されるとともに、正当化根拠、条件及び期間を含めて明確に定義される。 承認に係る判断は適切に文書化される。それらの判断は、客観的に、事実に基づいて特定された正当な目的を追求する場合において、かつ、承認要件が満たされていることを確認した上で、行われる。 承認が必要ない場合は、悪用・濫用から保護するために、アクセスに条件や制限を課す明確なルールや、効果的な監督など、法的枠組みで定められた他の保護措置が適用される。
IV. データの取扱い ガバメントアクセスを通じて取得した個人データは、権限を与えられた者のみが処理し、取り扱うことができる。このような処理及び取扱いは、プライバシー、セキュリティ、機密性及び完全性を維持するための物理的、技術的及び管理上の措置を講じることを含む、法的枠組みで規定された要件に従うものとする。これには、個人データが、合法的に処理されること、目的に照らし、また、データの機微性も踏まえて、法的枠組みで許容さ

れる限りにおいてのみ保持されること、そして、事情を考慮のうえ適切な範囲で正確かつ最新の状態に保たれることを確保するためのメカニズムも含まれる。

データの喪失、データへの不正若しくは偶発的なアクセス、又はデータの破壊、利用、変更若しくは開示を探知し、防止し、及び是正するために、また、そのような事例を監督機関に報告するために、内部統制が行われる。

V. 透明性

個人がガバメントアクセスによるプライバシー及びその他の人権と自由への潜在的な影響を考慮することができるように、ガバメントアクセスに関する一般的な法的枠組みは、明確で、かつ、公衆にとって容易にアクセス可能なものである。

個人データに対するガバメントアクセスに関する透明性を提供するためのメカニズムが存在する。これらのメカニズムは、個人や公衆が情報を受ける利益と、国家安全保障又は法執行の活動に支障を及ぼす情報開示を防止する必要性とのバランスをとるものである。

これらのメカニズムには、政府の法的要件の遵守に関する監督機関の公開の報告や、政府の記録へのアクセスを要求するための手続などが含まれる。その他の措置には、例えば、政府による定期的な報告や、該当する場合の個人への通知が含まれる。

民間部門は、法的枠組みに従って、ガバメントアクセスに係る要請に関する統計報告を公表することが認められる。

VI. 監督

ガバメントアクセスが法的枠組みを遵守していることを確保するために、効果的かつ公平な監督のためのメカニズムが存在する。

監督は、組織内のコンプライアンス担当部門、裁判所、議会又は立法機関、独立した行政機関などの組織を通じて行われる。

各国の監督システムは、このような組織がそれぞれに付与された権限に従って活動することによって成り立っている。このような組織は、関連情報の入手と審査、調査又は照会の実施、監査の実施、法的枠組みの遵守と改善に関する政府機関への関与、法的枠組みの違反への対処などの権限を有する。また、このような組織は、政府機関の説明責任を確保するために法的枠組みの違反の報告を受け、それに対応するものであり、また、個人の苦情を受けて救済の任務を行使することが可能である監督機関は、職務を遂行するに当たり、干渉されることなく、また、効果的に職務を遂行するための財政的、人的及び技術的資源を有するものである。監督機関は調査結果を文書化し、報告書を作成し、勧告を行い、それらは可能な限り一般に公開される。

VII. 救済

法的枠組みによって、個人に対して、国内の法的枠組みに対する違反を特定し、是正するための効果的な司法的・非司法的救済が提供される。

このような救済メカニズムにおいては、国家安全保障及び法執行の活動の機密保持の

必要性が考慮される。これには、自分のデータに対してアクセスが行われたかどうか、又は違反が発生したかどうかを個人に通知することを制限することが含まれ得る。

利用可能な救済措置には、適用される条件に従って、アクセスの停止、不適切にアクセス又は保持されたデータの削除、データの完全性の回復及び違法な処理の停止が含まれる。また、状況によっては、個人が被った損害の補償も含まれ得る。