個人情報保護法規則・ガイドラインの改正案の公表（2023 年 9 月 13 日）

2023 年 9 月 19 日

弁護士　中井　杏

＜目次＞
1.安全管理措置の対象拡大
2.漏えい等報告の対象拡大
3.外国制度の調査について
4.今後のスケジュールと必要な実務対応

2023 年 9 月 13 日、個人情報保護委員会から個人情報保護法規則とガイドラインの改正案が公表され、9 月 14 日からパブリックコメントが開始されました。

特に実務に影響があるのは、安全管理措置と漏えい等報告の対象拡大であり、今後、情報セキュリティ規程やそれに伴う運用の見直しが必要となります。

本ニューズレターでは、現時点で示されている改正案の内容と、必要となると予想される実務対応について解説します。

1. 安全管理措置の対象拡大

安全管理措置義務（個人情報保護法 23 条）の対象については、通則ガイドラインに、以下の文言が追加されています。

「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。」

個人情報保護法 23 条は、「個人データ」の安全管理措置のために必要かつ適切な措置を講じることを義務付けています。すなわち、散在情報である「個人情報」は、個人情報データベース等を構成している「個人データ」と異なり、安全管理措置義務の対象ではないことになります。

例えば、金融分野ガイドライン Q&A 問Ⅱ-7 では、契約書等の書類の形で本人から提出され、これからデータベースに登録しようとしている情報について、「データベース化されていない個人情報は、たとえ通常データベース管理される性質のもので、かつ、これからデータベース化される予定であったとしても、『個人データ』には当たりません。」と示されています。

このように契約書等の書類の形で本人から受領した情報は、データベースに登録するまでは「個人情報」であり、これまで安全管理措置義務の対象であるとは示されていませんでしたが、今回の改正案により、「個人データとして取り扱うことを予定している」のであれば「個人データ」としての安全管理措置の一環として当該義務の対象になることが明らかになりました。

また、「取得し、又は取得しようとしている個人情報」が安全管理措置義務の対象とされている点については、

次に述べる漏えい等報告の対象拡大と合わせ読むと、個人情報を取得しようとする段階においても安全管理措置を施す必要があると考えられます。例えば、顧客にウェブサイトの入力ページに個人情報を入力してもらい、顧客の個人情報を取得しようとする場合、当該入力ページが改ざんされることで不正者に個人情報を盗み取られることがないような措置を講じることも、安全管理措置の一環に含まれることになることが明らかになったと考えられます。

なお、従業者及び委託先の監督（個情法 24 条、25 条）については、特段ガイドラインの変更はありませんが、これらは安全管理措置義務（個情法 23 条）の一環としての規律であるため、従業者及び委託先の監督義務についても同様の改正案の影響が及ぶものと考えられます。

以上から、実務対応としては、情報セキュリティ規程や安全管理措置の運用において、①データベース化が予定されている個人情報についても安全管理措置の対象となっているか、②データベース化が予定されている個人情報を取得する方法についても安全管理措置を施しているか、を確認する必要があると考えられます。

2.漏えい等報告の対象拡大

(1)規則・ガイドラインの改正案

本改正規則案では、漏えい等報告の対象について定める個人情報保護法規則 7 条 3 号（※）が、以下のとおり改正されています。

現在：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

改正案：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

改正通則ガイドライン案には、報告を要する事例として、以下の事例が追加されています。

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

(2)改正案のポイント

現在の規則では、報告の対象は、「個人データの漏えい等」であるため、個人情報取扱事業者において現に個人情報データベース等を構成している個人情報が外部に流出した場合のみ、漏えい等報告の対象となっていました。すなわち、上記事例 6 のように、個人情報取扱事業者が不正な攻撃を受けた場合であっても、個人情報取扱事業者のサーバを経由することなく、直接不正者に個人情報が送信される事例については、漏えい等報告の対象ではないと解されていました。

しかし、今回の改正規則案では、「取得しようとしている個人情報」の漏えい等も報告の対象となったため、個人情報取扱事業者が不正な攻撃を受けたことに起因して、個人データが不正者に流出したのであれば、本人から不正者に直接送信されたものであっても、漏えい等報告の対象になったと考えられます。

そこで、実務対応としては、下記の解説も踏まえ、漏えい等報告の対象を定めた情報セキュリティ規程や、漏えい等発生時の対応フローを見直す必要があります。

(3)「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」

ア　「当該個人情報取扱事業者」

不正の目的をもって行われた行為を受ける者としては、個人情報取扱事業者のみならず、委託先や、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を含むとされています。

改正通則ガイドライン案の記載からは、第三者に含まれる者の具体例は不明確ですが、例えば、個人情報の入力フォームを設置したウェブサイトの運用管理を業務委託している際の業務委託先などが考えられます。

実務対応としては、これまで個人データの取扱いの委託契約において、委託先で漏えい等が発生した際に委託元に速やかに報告することを義務付ける条項を定めてきましたが、今後は第三者とのサービス提供契約等においても、個人情報を不正者に提供させるような不正な目的をもって行われた行為が発生した場合に、サービス提供者が速やかに通知することを義務付ける条項をいれることを検討する必要があります。

イ　「当該個人情報取扱事業者に対する行為」

改正規則案で漏えい等報告の対象となっているのは「当該個人情報取扱事業者に対する行為」による漏えい等であり、改正通則ガイドライン案によれば個人情報取扱事業者のウェブサイトが改ざんされた場合などが想定されています。

したがって、フィッシングサイトであっても、個人情報取扱事業者のウェブサイトが改ざんされたことにより、顧客がフィッシングサイトに遷移させられた場合は、漏えい等報告の対象になりますが、検索エンジンで検索をした結果として表示された個人情報取扱事業者のウェブサイトと類似したウェブサイト（フィッシングサイト）に顧客がアクセスし個人情報を入力してしまった場合や、SMS でフィッシングサイトが送られ顧客が当該フィッシングサイトにアクセスして個人情報を入力してしまった場合は、漏えい等報告の対象には含まれないと考えられます。

(4)「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」

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」が含まれたことにより、取得しようとしている個人情報と、取得したものの未だデータベース化されていない個人情報も、漏えい等した場合には報告の対象となっています。

「取得しようとしている個人情報」とは、「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」とされています。今後、パブコメや Q&A により外延が明確になることが期待されますが、改正通則ガイドライン案の具体例を踏まえると、入力ページに個人情報を入力させる場合など、現に個人情報を取得しようとしている場合は、これに含まれると考えられます。

(5)「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」

改正通則ガイドライン案では、「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。」と示されています。

「個人データとして取り扱われることが予定されている」か否かが、個人情報取扱事業者の主観によって判断されるか、当該個人情報の通常の取り扱われ方等が考慮されるかなどについては、今後のパブコメや Q&A で明らかにされることが期待されます。

(6)「個人データ」の定義

本改正によって、安全管理措置（個情法 23 条）及び不正の目的による漏えい等報告の対象（個情法 26 条、規則 7 条 3 号）の「個人データ」の範囲に変更があったものの、それ以外の条文における「個人データ」の定義には影響はないと考えられます。

例えば、個人データの提供を受けた際の確認記録義務（個情法 30 条 1 項）に関して、確認記録義務ガイドラインの改正案では、従前どおり「個人データには該当しない個人情報として提供を受けた場合、仮に、後に当該個人情報を個人情報データベース等に入力する等したときにおいても、法第 30 条の確認・記録義務は適用

されない」との解釈が維持されており、注釈として安全管理措置と漏えい等報告では「個人データ」の考え方が異なることが追記されています。

したがって、データベース化されていない段階の個人情報については、引き続き第三者提供に関する規制（個情法 27 条）や確認記録義務（個情法 29 条、30 条）は適用されません。

3.外国制度の調査について

外国にある第三者に対し個人データを提供するための同意を取得する際、当該外国の個人情報保護制度に」関する情報を提供することが義務付けられています（法 28 条 2 項、規則 17 条 2 項 2 号）。このうち、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（いわゆるガバメントアクセス）、本人の権利利益に重大な影響を及ぼす可能性がある制度に該当するか否かを判断するに当たっては、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ことが追記されました。

4.今後のスケジュールと必要な実務対応

本改正案は、9 月 14 日から 10 月 13 日までパブリックコメントが行われており、11 月下旬～12 月中旬に公布されることとされております。通例では、この後 Q&A や各分野別ガイドラインの改正も行われることが予想されます。

そして、改正された規則及び安全管理措置と漏えい等報告に関するガイドラインの施行は、2024 年 4 月 1 日とされております。

企業においては、11 月下旬～12 月中旬に公表されるであろうパブリックコメントの結果や公布される規則、ガイドライン、Q&A の改正内容を注視しつつ、2024 年 4 月 1 日までに、個人情報保護規定や情報セキュリティ規程、インシデント対応マニュアル、第三者との契約等を改正内容に沿ったものとなるよう見直しを行うことが必要となります。

以 上