【講演レポート】JIPDEC セミナー

個人情報保護法規則/ガイドライン改正の実務対応のポイント

牛島総合法律事務所
弁護士　中井　杏氏

2023 年 12 月に個人情報保護法規則及びガイドラインが改正され、2024 年 4 月 1 日に施行されます。本講演では、主に、安全管理措置・漏えい等報告への改正対応として施行までに行うべき実務対応について解説します。

改正の全体像

対象と内容

今回の改正対象は、個人情報保護法規則 7 条 3 号とガイドラインです。Web スキミングによる個人情報流出事案を背景とした、安全管理措置・漏えい等報告の対象について、また、外国制度の調査について OECD のガバメントアクセスに関する宣言の参照などが示されています。なお、今回の改正では外国制度の調査に関しては特に対応の必要がない企業がほとんどだと思われます。

対応事項

今回の改正に伴う、安全管理措置・漏えい等報告の対応事項は下記 6 点です。

① プライバシーポリシーの改正
② 社内規程（個人情報取扱規程など）の改正
③ 個人データの取扱委託契約書の見直し
④ 個人情報を取得するために利用するサービスの契約見直し
⑤ 基準適合体制のための契約書の修正
⑥ 社内への周知

改正の問題意識「Web スキミング」

安全管理措置・漏えい等報告が改正される背景となった「Web スキミング」（図 1）とは、典型的には EC サイトに仕掛けられる攻撃手法です。現行の個人情報保護法規則では、漏えい等報告の対象は、個人情報取扱事業者側でデータベース化された個人情報（＝個人データ）が漏えいした場合のみとなっており、Web スキミングによって漏えいした個人情報は報告対象外でしたが、利用者側から見れば、攻撃者に個人情報を取得されてしまっては、個人情報取扱事業者を経由しているか否かに関わらず生じる被害は同様なため、利用者から攻撃者に直接情報が流出してしまった事象に関しても個人情報保護委員会への報告が必要であるとして今回の改正が行われたと考えられます。

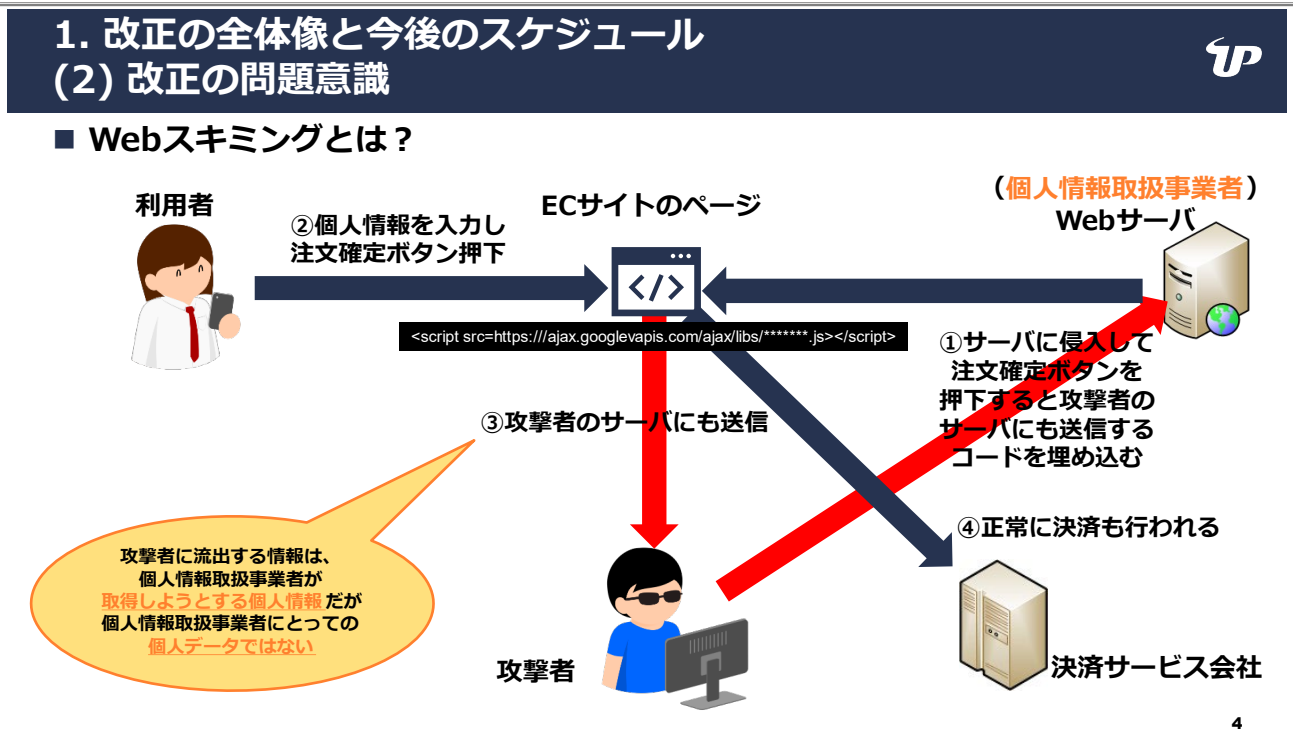

図 1　Web スキミングとは？

安全管理措置の対象明確化

安全管理措置とは

改めて、安全管理措置とは「個人情報取扱事業者は、個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のため、組織的、人的、物理的、技術的安全管理措置及び外的環境の把握等を行わなければならない」と定められています。

今回の改正で、「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」情報への必要かつ適切な措置も含まれる、ということが明らかになりました。

「個人情報」と「個人データ」

個人情報保護法には「個人情報」と「個人データ」という概念があり、個人情報のうちデータベース化されていない散財情報は個人情報、検索ができるなどデータベース化された情報は個人データとして扱われます。

今回の改正によって、「個人データの安全管理措置」には、データベース化する予定があるのであれば、取得しようとしている個人情報も、取得後まだデータベース化されていない個人情報も安全管理措置を行わなければならないことが明らかになりました。

取得しようとしている個人情報とは何か（Web スキミングの場合）

EC サイト利用時の Web スキミングを例（図 2）に、「取得しようとしている個人情報」とは具体的に何を指すか説明します。利用者が EC サイトで注文確定ボタンを押し、個人情報取扱事業者側のサーバーが情報を受信するという場合、この受信の直前までを「取得しようとしている個人情報」といい、事業者側が受信した時点で「取得した個人情報」、データベース化した時点で「個人データ」になります。

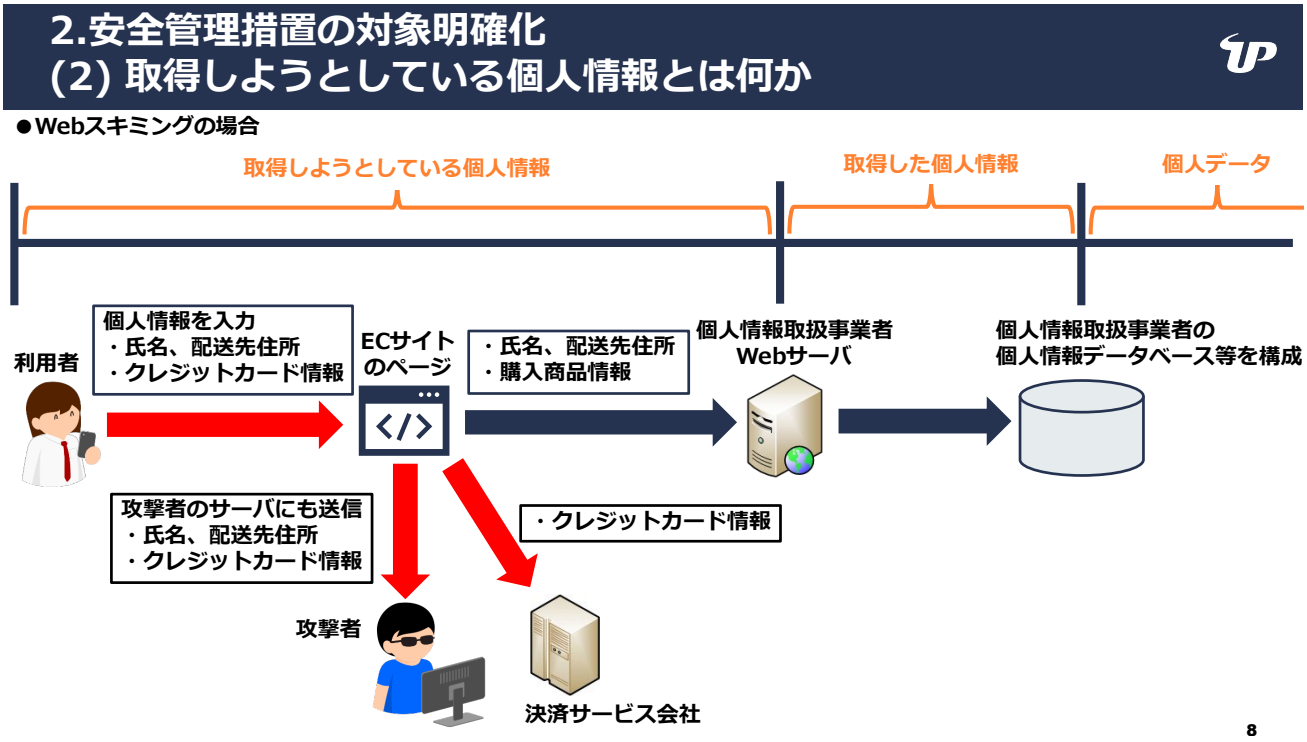

図 2　取得しようとしている個人情報とは何か（Web スキミングの場合）

取得しようとしている個人情報とは何か（オフラインの場合）

お客様に紙の申込書に個人情報を記載していただき、申込書を受領した営業社員が会社に持ち帰りデータベース化する場合を想定します。この場合、申込書を渡されるまでの間は「取得しようとしている個人情報」であり、受け取った後は「取得した個人情報」、自社のデータベースに入力した時点で「個人データ」になります。お客様から申込書を受領後、会社に持ち帰るまでの間に盗難、紛失などが起きないよう安全管理措置を講じなければならないことが明らかになったということになります。

取得しようとしている個人情報とは何か（その他の例）

例（図 3）として、委託関係にない第三者から個人情報の提供を受ける場合でも、自社を原因とする漏えいを防止するために必要かつ適切な措置を行わなければなりません。図 3 でいう B 社が A 社から情報を収集するために Web 上の入力フォームなどを利用した際などに、その情報を第三者に送信させるといった攻撃を受けることがないような措置が必要です。

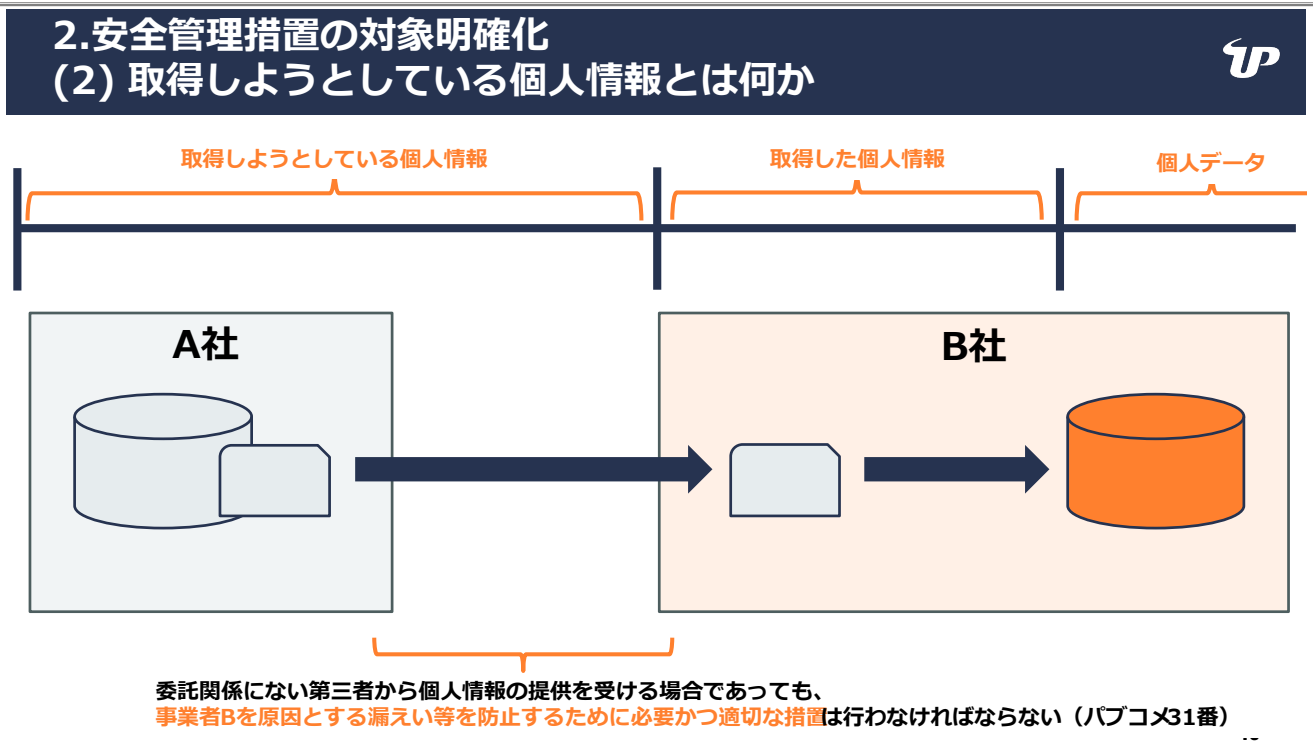

図３　取得しようとしている個人情報とは何か（委託関係にない第三者からの個人情報の提供）

保有個人データに関する事項の公表等

安全管理措置の対象明確化に関連して、上記以外にも２つ改正がありました。１点目は保有個人データに関する事項の公表等です。令和２年改正で安全管理措置について本人が知り得る状態（プライバシーポリシーでの公表等）に置かなければならないとされましたが、今回その安全管理措置の対象が明確化されたため、個人データとして取り扱う予定がある「取得しようとしている個人情報」や「取得した個人情報」に対する漏えい等防止措置に関する記載も記載することが必要になります。

また、外国にある第三者への個人データの提供を基準適合体制※1 で行っている場合も、今回の改正に沿った内容に修正していくことになります。

なお、安全管理措置に関する部分に関しては対象の拡大ではなく、あくまでも従前からの解釈を明確にしたものですので、施行日の４月１日を待つことなく直ちに対応していただく必要があります。

※1　基準適合体制とは（牛島総合法律事務所）

漏えい等報告の対象拡大

改正内容

「漏えい等報告」について現行法では、「個人データ」の漏えい、滅失、毀損が発生し下記４つに該当する場合は個人情報保護委員会への報告が必要だと定められております。

①　要配慮個人情報

②　財産的被害が生じるおそれのある情報

③　不正行為

④　本人が 1000 人を超える場合

今回の改正規則では③「不正行為」の場合のみ報告対象が追加されており、「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」に当たる場合は報告が必要となりました。また、それに伴い本人通知の対象も拡大されています。

ガイドラインで示された具体例※2では、Web スキミング、フィッシングサイト、紙のアンケート用紙の送付先の改ざんなどの不正が掲載されています。

※2　(令和 6 年 4 月 1 日施行)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）3-5-3-1（個人情報保護委員会）

「当該個人情報取扱事業者」とは

不正行為の標的である「当該個人情報取扱事業者」には、個人情報取扱事業者はもちろんのこと、委託先や外部の事業者などの第三者も含まれることになりました。第三者とは、個人情報の入力フォームを設置した Web サイトの運用・管理を業務委託している委託先のほか、紙のアンケートの回収等を業務委託した場合の委託先などが想定されています。

「当該個人情報取扱事業者に対する行為」とは

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」による漏えい等です。個人情報取扱事業者の Web サイトが改ざんされた場合や、顧客の申込書が配送過程で窃盗等により所在不明になった場合、また、Web サイトの改ざんにより、利用者がフィッシングサイトに遷移させられた場合なども考えられます。

一方で、検索エンジンで検索した際に表示されたフィッシングサイトに利用者がアクセスし、当該フィッシングサイトに個人情報を入力してしまった場合や、SMS で一方的に送り付けられたフィッシングサイトの URL に利用者がアクセスし個人情報を入力してしまった場合は、「当該個人情報取扱事業者に対する行為」ではないため報告の対象にはなりません。

「取得しようとしている個人情報」とは

「取得しようとしている個人情報」に何が含まれるかについては明確な解釈は示されておらず、現状は個人情報の取得手段等を考慮して客観的に判断すると述べられるに留まっています。そのため今後の運用や解釈を見ながら対応していくことになります。

「個人データとして取り扱われることが予定されているもの」の基準時は

「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」の判断基準時は、漏えい等またはその

おそれが発生した時点です。当初から自社のデータベースに登録をしようと思っていたが、まだ登録していない段階で漏えい等した場合は報告対象となり、当初の予定が変更されデータベースに登録しないと決めた後に発生した漏えい等については報告対象外です。

個人情報保護委員会に対する漏えい等報告は、漏えい等の事態を知ったときから概ね3～5日以内（初日参入）に速報を行わなければならないところ、個人情報の漏えい等が発生した際に、個人情報保護委員会への報告が必要かどうかを迅速に判断するためには、自社が保有する情報をどういったデータサイクルで取り扱うのかをあらかじめ関係者が把握できる社内体制を構築することが考えられます。

実務対応

実務対応の全体像について

今回の改正に伴う実務対応として考えられる事項は図4にあげた5つです。

4. 実務対応

■ **全体像**

	対応事項	根拠	対応時期
1	プライバシーポリシーの改正	通則GL3-8-1	直ちに
2	社内規程の改正		
	(1)安全管理措置の対象	通則GL3-4-2	直ちに
	(2)漏えい等報告	施行規則7条3号	2024/4/1まで
3	委託契約書の修正		
	(1)安全管理措置の対象	通則GL3-4-4、3-4-2	直ちに
	(2)漏えい等報告	施行規則7条3号	2024/4/1まで
4	第三者との覚書締結	施行規則7条3号	2024/4/1まで
5	基準適合体制のための契約書等の修正		
	(1)安全管理措置の対象	外国第三者GL4-2、 通則GL3-4-2	直ちに
	(2)漏えい等報告	施行規則7条3号	2024/4/1まで

20

図4　実務対応の全体像

1. プライバシーポリシーの改定（通則 GL3-8-1、直ちに対応）

安全管理措置の対象の部分を、「取得しようとしている個人情報」を含んだ形で記載しているか否かをご確認ください。なお、プライバシーポリシーにおける保有個人データに関する事項の公表は、本人の求めに応じて遅滞なく回答するということでも法令上は問題はなく、プライバシーポリシーに書かなくても問題はありません。しかし、監督当局がある事業者について調査をしようとする際に、プライバシーポリシーをチェックすることはままあることから、プライバシーポリシーに安全管理措置についての記載をするのであれば、小さな修正ではありますが、ぜひ対応していただくことをお勧めします。

2. 社内規程の改定

安全管理措置（通則 GL3-4-2、直ちに対応）

社内規程も改正に合わせて修正します。具体的には、安全管理措置の対象が「個人データ」となっている場合には、個人データとして取り扱うことが予定されている「取得し、又は取得しようとしている個人情報」が含まれることを追記します。

漏えい等報告の対象（施行規則 7 条 3 号、4 月 1 日までに対応）

社内規程において、漏えい等の報告の対象となる規則 7 条を引用した規定を設けている場合は、改正後の規則と合致しているか確認し、修正を行ってください。

社内規程改定のポイント

社内規程の修正対応ポイントとしては、実際の文章の修正はもちろんですが、従業員の皆さんへの周知を徹底していただくことが重要になります。漏えいと報告の義務をしっかり果たすためには、インシデントが発生した際に速やかに現場から法務やコンプライアンス部門に情報共有を行うことが何より重要です。そのため、日頃から従業員とはインシデント発生時の対応について情報共有を行い、密にコミュニケーションをとるようにしてください。

3. 委託契約の修正

個人データの取り扱いを委託している場合の委託契約は、委託契約で定める安全管理措置の対象の修正は直ちに行い、漏えい等報告の対象の修正は 4 月 1 日までに対応してください。この場合、安全管理措置や漏えい等報告の条項を修正する形も考えられますし、契約の目的の部分で契約書自体が対象としている個人情報の対象を改正規則・ガイドラインに合わせて特定することでも対応は可能です。

4. 第三者との覚書締結

労力がかかることが想定される重要なポイントが第三者との覚書の締結です。取得しようとしている個人情報の漏えい等についても報告が義務付けられたため、個人データの取り扱いを委託していない運用委託先やサービス提供元との契約に関しても見直す必要があります。

運用委託先やサービス提供元においてインシデントが発生し、第三者に個人情報が流出した場合の報告義務を条項にいれておくことで、自社から個人情報保護委員会への報告を非常にスムーズに行うことができます。すでに条項でインシデント報告義務が定められている場合でも、速報や確報の期限に間に合うように報告期限を定めているかなど今一度見直していただけるとよいかと思います。

具体的には、広くインシデント報告という形で条項を作成し、情報漏えいを含むインシデントが発生した場合は直ちに委託者へ報告する旨を記載することが考えられます。報告事項に関しては、自社から

個人情報保護委員会へ報告しなければならない事項のうち、当該第三者に協力してもらわなければ確認できない事項を列記することで、第三者からの情報の吸い上げがスムーズに行えると思います。個人情報保護委員会への報告には期限があるため、速報や確報期限より若干早めに第三者から自社の報告期限を設定するとよいかと思います。自社から個人情報保護委員会へ報告する義務がありますので、早期の正確な情報提供を行ってもらうためにも、ぜひ第三者と交渉を行い条項を入れていただくことをおすすめします。

5. 基準適合体制のための契約書等の修正

越境移転の場合、基準適合体制のための契約書も修正します。例えば外国にある委託先とのデータ移転契約や外国にあるグループ企業とのグループポリシーに安全管理措置、漏えい等に関する規定が含まれる場合はその対象が今回の改正に応じたものになっているか確認してください。

6. 個人情報取扱台帳

個人情報取扱台帳については、すでに個人データの取り扱いについてはカバーされている場合は、法令上新たな対応は必須ではないと思われます。ただし、より詳細に個人情報の取り扱い状況を把握するために、個人情報を取得する際に利用するサービスについての項目を追加することも不利益にはならないかと思います。

以上、4 月 1 日の施行に向けてぜひ対応を進めていただければと思います。

牛島総合法律事務所　　弁護士　中井　杏氏

京都大学法学部卒業、中央大学法科大学院修了。
18 年弁護士登録、牛島総合法律事務所入所。
21 年から 23 年まで個人情報保護委員会へ出向、同年牛島総合法律事務所にて実務再開。
個人情報・プライバシー、営業秘密などの情報管理に関する案件を多く取り扱う。
【著作】
「『犯罪予防や安全確保のための顔識別機能付きカメラシステムの利用について』の解説」（NBL1242 号）
「実務問答　個人情報保護法（第 3 回）AI 開発における学習用データの利用目的と学習済みパラメータの取扱い」（NBL1254 号）　他

本内容は、2024 年 2 月 27 日に開催された JIPDEC セミナー「個人情報保護法規則/ガイドライン改正と、今後のデータ管理の要諦」講演内容を取りまとめたものです。