

信託セミナー

改正個人情報保護法に対する
実務対応

浅井国際法律事務所弁護士 浅井 弘 章



— 目 次 —

はじめに（改正の動向と改正法対応上の留意点）

1. 不適正な利用の禁止に関する規定の「新設」（明確化）
2. 「外国にある第三者」への提供の制限に関する改正
3. 漏えい等の報告等に関する改正

4. 保有個人データに関する事項の公表等に関する改正
5. 個人関連情報の第三者提供の制限等の新設
6. 開示請求に関する改正
7. 利用停止等請求に関する改正

はじめに（改正の動向と改正法対応上の
留意点）

弁護士の浅井と申します。どうぞよろしくお願ひします。時間も限られているので、早速内容に入ります。レジユメの「改正の動向と改正法対応上の留意点」からスタートしていきたいと思います。

まず、レジユメの①の点です。2021年8月に「個人情報の保護に関する法律についてのガイドライン」（以下、「ガイドライン」という。）の通則編およびその改正に伴い「「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」（以下、「個人情報保護法Q&A」という。）の改訂が行われており、実務上これが重要です。併せて、②にあるよ

うに、パブリックコメントの回答が公表されていますが、件数が膨大で、大手企業においても全てをチェックしてそれに沿った実務対応、整理をするのは、皆さん、大変お忙しい状況だと思いますので、そのなかではなかなか難しい面もあります。パブリックコメントの概要版等が個人情報保護委員会から公表され、また、個人情報保護法Q&Aの中で一部パブリックコメントの回答が文章化されていますので、そういったものを参照しながら実務対応を進めるのが無難かと思います。もちろん、パブリックコメントの回答を全部ご検討いただき、それを踏まえてご対応いただくのがベストではありますが、件数が膨大というところもあり、それに代えて個人情報保護法Q&A、あるいはパブリックコメントの回

答の概要版を少なくともご覧になっていただき、そうしたものに記載されている点に注意して、それに即してご対応いただくのが重要かと思えます。

③のところですが、今日お話しする令和2年改正個人情報保護法と言われているもののほかに令和3年改正個人情報保護法というものがあります。これにより、個人情報保護法の条文番号が大きく変わっています。また、学術研究機関等に関する個人情報の取扱いに関する条項が明文化されています。この条文番号が大きく変わっているところに関して、社内文書、あるいは対外公表文書などにおいて、「個人情報保護法第〇条に基づき」とか、「個人情報保護法第〇条に定める」といった形で条文番号を引用しているケースがありますので、そういったものを改定していくことが必要になると思えます。本日お話しする条文については、新しい条文の番号ではなく、令和2年改正法の番号を示しています。

④のところ、2021年9月に「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」も改定されています。個人情報に関する規定とともに特定個人情報、つまりマイナンバーを含む個人情報の取扱いに関するルールを一緒に規定していたり、あるいは関連する規定として整理していたりする場合もあると思えますが、マイナンバーの取扱いに関するガイドラインも改定されていますので、そういったものも踏まえ、社内規定等を改定していただくことが重要になると思えます。

⑤のところですが、昨年末に金融分野ガイドライン等の改正案が公表されており、パブリックコメントが1月に実施されています。この金融分野ガイドライン等の改定後に、「金

融機関における個人情報保護に関するQ&A」（以下、「金融分野Q&A」という。）の改定がなされる可能性があると思えます。実務的な最終着地点は金融分野Q&A、特に漏えい対応の関係について金融分野Q&Aをご覧になり、最終的にどういう実務対応をするのか等を確定する形になると思えます。金融分野Q&A以外のところは既に案等が出ており、実務の方向性がほぼ明らかになっていますので、それを踏まえて信託会社・信託銀行における実務上の留意点についてお話しします。

1. 不適正な利用の禁止に関する規定の「新設」（明確化）

(1) 法改正の内容

アのところにあるように、違法または不当な行為を助長し、または誘発するおそれがある方法により個人情報を利用してはならないといった規定が新設されます。個人情報保護委員会では「新設」ではなく「明確化である」と説明していますので、現行法においてもこういった不当な行為を助長するおそれのある方法、あるいは不当な行為を誘発するおそれのある方法で個人情報を利用してはならないといったルールがあるということでしょう。しかし、企業実務の観点からみますと、これまでこういった観点から企業が明確にリーガルチェックをしていたかという点、必ずしもそうではないと思えますので、不当な行為を助長するおそれがあるかどうかという見地から、改正法施行後はリーガルチェックやコンプライアンスチェックをしておくことが重要になると思えます。

不当な行為あるいはそのおそれといったものについて、特に下線を引いていますが、運

用にかなり幅のある概念かと思えます。個々の事案において、非常に保守的な運用をされている金融機関などにおかれては、不当な行為を助長するおそれがあるのではないかとコンプライアンスの判断をする見方もあると思えますし、個人情報保護委員会が公表している事例などと比較対照すると、あのようなひどい事例はないということで、不当な行為を助長するおそれがある方法により個人情報を利用していると評価されるおそれはないといったような双方の見方がありえると思えます。いずれにしても、個人情報保護委員会の裁量・運用の幅が非常に広い規定なので、最初のうちは慎重な対応をしておくことが望ましいと思えます。

今のところで、信託会社・信託銀行が改正個人情報保護法第16条の2の規定に違反した場合の影響は結構大きな影響があります。(ア)にあるように、個人情報保護委員会による是正勧告等の対象になるので、対外公表もされるし、マスコミ等へのプレスリリースもなされると思えます。それから(イ)にあるように、利用者から利用停止請求あるいは消去請求を受ける原因になります。対外公表されてマスコミ対応が必要になる上に、契約者・顧客からいろいろな利用停止等の請求や消去の請求を受ける理由になるので、一定数そういった請求への対応が必要になってくる可能性があると思われます。この2つの影響があるので、適用範囲が非常に広い可能性のある規定・規律について、最初のうちは慎重な見地から対応するのが無難ではないかと思えます。

(2) 実務上の留意点

ここでは、2点挙げています。まず1つ目のアとして、個人情報を利活用することを内

容とする新規プロジェクト等の企画時の留意点です。最近の個人情報保護に関する相談は、自社単体で個人情報を利活用するという事案は比較的少なく、金融機関・信託会社に限らず、サービス業、IT企業、ベンダーといった複数の業態の企業が参加して、個人情報を利活用してプロジェクトを進めようと検討されているケースにおいて、第三者への提供に関する問題や個人情報の利用目的に関する相談を受けるケースが多いです。そういった複数の企業が関与する新規プロジェクトだと、一部の会社においては、今回の新しいプロジェクトのうち、一部については不当な行為を助長する、あるいは誘発するおそれがあるのではないかということで避けたほうがよいのではないかといった慎重な意見をおっしゃる企業も出てくる一方で、個人情報保護委員会が公表している事案などと比較すると全然問題がないプロジェクトだから、不当な行為を助長するおそれはないといった意見をお持ちの企業が大半だといったケースもありえると思えます。それぞれプロジェクトに参加する企業により、個人情報保護法第16条の2に該当するかどうかについて意見が分かれるところが出てくると思えます。最終的にはもちろん個人情報保護委員会の事後的な判断を見ないとわからないところではありますが、参加企業ごとに意見が違ってしまうと、全ての企業が問題ないと判断するまで、そのプロジェクトが実施できなくなります。プロジェクトを止めるか実行させるかということで、非常に難しい判断を法務・コンプライアンス部門がせざるを得ない場面も出てくると思えます。外部の弁護士の意見も、何が不当なのか、どのような場合におそれがあるのかといったところで、弁護士ごとに意見が違う場合があ

ると思います。こういった判断をすればよいのかというところで、非常に迷う場面もこれから増えてくると感じています。

今のところでは、個人情報に関する苦情対応の負担の増加という点を挙げています。従来、個人情報の利用に関しては、目的外利用をしてはならないとか、利用目的を明示しなければならないといった規制しかありませんでしたので、個人情報の利用に関する苦情が来た場合には、「こういった形で利用目的を公表し、明示しています。今回の利用は、この利用目的の中のこの項目に含まれます」という形で比較的簡単に対応でき、それ以降は同じ回答を繰り返していくことで、個人情報に関する照会、特に利用に関する苦情に対応していたかと思います。ところが改正後は、不当な行為を助長・誘発するおそれがあるのかどうかといった点も含めて回答することが必要になります。非常に強いクレームをおっしゃってくる顧客への対応において、説明の工夫が必要になってくると考えています。

2. 「外国にある第三者」への提供の制限に関する改正

(1) 法改正の内容について

法改正の内容に関する説明の前に、現時点における法制度について簡単に振り返ります。現行法においても、個人データの外国にある第三者への提供——越境移転などと言いますが——を行う場合には、一定の対応を事業者が行う必要があります。

図の左側の「現行」のところに書いてあるように、越境移転する場合は、①本人の同意を得る、②外国にある第三者が一定の基準に適合する体制を整備している、③越境移転先

の国の法制度がわが国と同等の水準にある——具体的にはEU、イギリスが挙げられます——の3条件のいずれかを満たすことが必要です。信託会社・信託銀行におかれては、現行、これらのいずれかに該当するとの整理をして越境移転を行っていると思います。

改正後は、図の右側のところですが、特に①と②の実務対応について、それぞれ追加の義務を新設しています。まず、本人の同意を得て越境移転する場合ですが、同意の取得時に移転先の外国における個人情報保護法制などを参考情報として提供しなければいけないという義務（同意取得時の参考情報の提供義務）を新設しています。

基準に適合する体制を整備した事業者に対する提供については、改正後は、相当措置の継続的な実施を確保するために「必要な措置」を実施することが求められます。「継続的な」というところがポイントであり、基準適合体制を整備する者に提供した後に、モニタリングを継続的に実施することを確保する体制に必要な措置を講じてくださいということです。具体的には、年に1回程度、書面による回答などを通じて、継続的に相当措置——日本の個人情報保護取扱事業者が講ずることとされている措置と同等の措置——が実施されているのかなどを、確認する必要があります。

加えて、本人の求めに応じて「必要な措置」に関する情報の提供を受けてくださいというルールが加わっています。本人から事後的な請求があった場合には、具体的にどのような措置を講じているのか情報の提供を受けて、本人に説明する必要があります。

以上が改正の全体像です。以下、レジюмеにこれらをより詳しく記載していますので、それに沿って改正内容とその実務上のポイント

トについて話をしていきます。

まず、アですが、信託会社・信託銀行は「外国にある第三者への個人データの提供を認める」旨の本人の同意を得ようとする場合には、法定の方法により、あらかじめ当該本人に参考となるべき情報を提供しなければいけないということで、同意取得時の参考情報の提供義務を個人情報保護法第24条第2項に規定しています。具体的には、①外国の名称、②当該外国における個人情報保護法制に関する情報、③提供先の第三者が講ずる個人情報保護措置に関する情報を提供しなければいけません。

②当該外国における個人情報保護法制に関する情報を事業者に提供する場合には、その国の個人情報保護法制を調べた上で、その法制度に関する情報を提供しなければいけません。この点に関しては、個人情報保護委員会において、一定数の主立った外国の個人情報保護法制を調査・公表しています。そういったものを参考にしながら、②については情報提供していくことになると思います。

③当該第三者が講ずる個人情報保護措置に関する情報も提供することが必要になります。※のところに書いているように、①～③について情報提供が難しい場合には、一定の代替措置が認められます。

イは、先ほどお話しした基準適合体制を整備したもの、個人データを「外国にある第三者」に提供した場合に関するものを記載したのですが、これは同じことの繰り返しになりますので、説明は割愛します。

(2) 金融分野ガイドラインの改正案

信託協会の加盟会社におかれては、金融分野ガイドラインの適用を受ける会社が多いと

お見受けしています。もちろん加盟会社におかれては、金融分野ガイドラインの適用がない場合もあると思いますが、そういった会社では(2)は無視していただければと思います。金融分野ガイドラインの適用がある加盟会社を念頭において、(2)を説明させていただきます。

アのところで、本人の同意に基づく場合の上乗せ措置がいくつか設けられています。①、②に記載している内容については、同意の取得の際の留意点を上乗せで求めています。①では、書面で同意を得る、個人情報の取扱いに関する条項を目立つ形で記載する、あるいは確認欄を設けて本人にチェックしてもらう等で、本人の意思が明確に反映できる方法により同意して確認をしてください、といった同意取得時の留意点です。②では、同意書面に記載すべき事項を追加するといった上乗せ措置が設けられています。

①、②で設けられている上乗せ措置ですが、国内において個人データを第三者に移転する場合について、現行法でも設けられている留意点とほぼ同じものになります。もしこれを機に①、②に係る越境移転についての同意文言を改定する場合には、現行の国内移転において、どのような同意文言を使っているのかを確認しながら、それと同じような形で越境移転に関する同意文言を設ける（修正する）といった対応がいちばんスマートではないかと思います。①、②は全く新しい規律というわけではなく、現行の国内移転におけるルールとして既に導入されているものなので、金融分野ガイドラインの適用のある信託会社・信託銀行におかれては、国内移転に関しては既に対応済みのルールかと思いますが、そこにおける自社の実務対応を踏まえ、越境移

転の同意文言を改定するのがスマートかと思
います。

③ですが、信託会社・信託銀行において、
事後的に提供先の第三者を特定できた場合に
は、本人の求めに応じて一定の情報提供と説
明を行ってくださいといったことが冒頭に書
かれています。越境移転の場合、最初から提
供先の第三者が明確に特定できている場合
と、同意を得る際には提供先の第三者が確
定していない場合の双方があると思います。
提供先を既に特定している場合には、1社の
名前を明記した上で同意を得ればよいわけ
ですが、提供先が明確に1つに特定できな
い場合には、包括的な表現で同意を得るこ
とになります。同意を得た後に提供先の第
三者が特定され、本人から請求があった場
合には、具体的にどういう会社であるかも
含めて、施行規則第17条第2項各号に定
める情報を提供することが必要になります。
それから、こういった情報提供が可能だとい
うことを個人情報保護宣言（以下、「プライバ
シー・ポリシー」という。）などに含めて
対外公表することが努力措置として求めら
れる形になります。

④では、今お話ししたように、同意を取
得する時点において第三者が特定できず、
事後的に提供先の第三者が所在する外国
が特定できた場合には、外国の名称をイ
ンターネットのホームページ等に掲載す
ることが努力措置として求められています。
以上が本人の同意を得て越境移転する場
合の金融分野ガイドラインでの上乗せ措
置です。

今のところは、相当措置を講ずる方法
による場合の上乗せ措置です。海外委託
等の場合によく使われている類型で、相
当措置を講ずる方法による第三者の越境
移転の場合についても金融分野ガイドラ
イン上、いくつか上乗

せ措置が設けられています。

まず①ですが、先ほどお話ししたように、
継続的なモニタリングが必要になってき
ますので、年に1回アンケートを行い、そ
れに回答してもらう形で相当措置の実施
状況をモニタリングする必要が出てき
ます。その確認方法として、第三者の事
務所に実際に行ってみる方法、あるいは
書面により報告を受ける方法のいずれか
の方法で確認することが努力措置として
求められています。言い換えると、口頭
で確認をするだけではNGということです。
金融分野ガイドラインの適用のある事
業者におかれては、アンケートに回答し
てもらい、書面で報告を受けるといった
形で年に1回、海外委託先について相
当措置の実施状況のモニタリングを行
うことが必要になります。

②は先ほどの同意に基づく場合に近い
ですが、本人に一定の情報請求権がある
ことをプライバシー・ポリシーなどと一
体として、インターネットのホームペ
ージで常時掲載するなどして周知する
ことが求められています。

③も先ほどの同意に基づく越境移転
の場合に近いです。提供先の第三者は
確定していると思いますので、相当措
置を講ずる方法により外国にある第
三者——海外委託先などが典型例
です——に個人データを提供した場合、
提供先の第三者が所在する外国の
名称をインターネットのホームペ
ージに掲載するなどにより公表する
ことが努力措置として求められて
います。

以上が金融分野ガイドラインの適用
のある加盟会社における留意点です。

(3) 実務上の留意点

まず、アで、信託会社・信託銀行による「外

国にある第三者」への提供の代表例をいくつか記載しています。もちろんこのほかに、例えばデータ入力を外国にある第三者に依頼をする、あるいは個人情報を含む文書の翻訳を外国にある第三者に依頼するといったことで、海外委託という形で個人データを越境移転させる場合があると思いますが、信託銀行が加盟会社に多いこともあるので、銀行絡みの例を多めに挙げています。

レジュメにあるように、①外国送金、②エクスポージャー等を移転する国際金融取引、③ FATCA に基づく IRS への年次報告、④ 海外事業者のクラウドサービスの利用があります。④は、クラウドサービスの内容次第では、外国にある第三者への提供に該当しない場合があります。ここで言っているのは外国にある第三者への提供に該当しないものではなく、外国にある第三者への提供に該当する海外事業者のクラウドサービスの利用を念頭に置いています。⑤は、従業員の海外出向などに伴う出向先との間の人事情報に関するやりとりです。そういったものが信託会社・信託銀行による外国にある第三者への提供に該当すると思いますし、それぞれ現行の業務においても独自のものがあると思います。そういったものについて、同意に基づくものと整理しているのか、あるいは相当措置を講ずる方法により、あるいは基準適合体制を充たす事業者ということで整理して越境移転しているのか、すなわち現行法上どのような整理をしているのかを踏まえ、改正法にどう対応していくのかをそれぞれ検討することになると思います。

イは、本人の同意を得る方法により対応している場面における実務対応上の留意点についてお話しします。まず、(ア)で、参考情報の

提供の履行方法についてです。先ほどお話ししたように、個人情報保護法第24条第2項に従って本人に対し同意を取得するに際して、一定の参考情報の提供を行わなければいけないというルールが新設されています。具体的には、外国の名称、当該外国における個人情報保護法制、当該第三者が講じる個人情報保護措置の内容といったものを説明した上で越境移転に関する同意を得る必要があります。これらの情報の内容が結構なボリュームになるので、それを全部紙に書くのではなく、それらがまとめて掲載されているウェブサイトを用意して、その URL を本人に教えることで、参考情報の提供をしたことになるかというのが実務上よくある質問の1つです。

レジュメの記載内容は個人情報保護委員会の個人情報保護法 Q & A から抜粋したもので、Q12-10とそれへの回答(A12-10)です。実務上重要なのは下線部分ですので、その内容について説明します。ウェブサイトを利用した方法による情報提供の場合であっても、例えば、当該 URL を本人にとって分かりやすい場所に掲載した上で、同意の可否の判断の前提として、本人に対し当該情報の確認を明示的に求めるなど、本人が当該 URL に掲載された情報を閲覧すると合理的に考えられる形で情報提供を行う必要がある、という回答になっています。実務上、この下線部分の要件を充たしているかどうかに関する相談が最近非常に多いです。ウェブサイトの URL を本人に提供する方法で同意を得ることを検討している加盟会社におかれては、A12-10の下線部分の要件を充たす形で情報を提供することが重要です。

次に、(イ)は、第三者が講ずる個人情報保護措置の確認方法についてであり、こちらも最

近、相談が多い事項の1つです。国の参考情報として提供しなければならないものは、①外国の名称、②第三者が所在する国の個人情報保護法制、③提供先の第三者が講じている個人情報保護措置の確認の3つです。②の提供先の国の個人情報保護法制については、個人情報保護委員会が公表している内容等を利用して参考情報を提供することが考えられると思います。③の第三者が講じている個人情報保護措置については、当然、提供先の第三者ごとに違っていますので、提供元である各社において、どういう措置を講じているのかを第三者に確認するなどの方法により確認しなければいけないということになります。

Q12-12は、第三者が講ずる個人情報保護措置に関する情報はどういう方法で確認すればよいかという質問です。個人情報保護委員会の回答はA12-12で、具体的には提供先の外国にある第三者に確認する方法、提供先の外国にある第三者との間で締結している契約——海外委託先と締結している業務委託契約において当該第三者による個人データの取扱いについて定めている場合には、当該契約——を確認する方法などが考えられます、という形で回答しています。いずれももっともな回答かと思いますが、提供先の第三者が講ずる個人情報保護措置を提供元で顧客に説明する形になりますので、他社の状況を提供元が説明する形になります。提供先の第三者が海外の公的機関等の場合には契約関係がないので、提供先の確認などは不要だと思います。しかし、業務委託契約等を締結したり、一定の契約関係があったりする事業者の場合、提供先の第三者が講ずる個人情報保護措置について最終的な説明の文案ができた場合には、後日、第三者から、それは実態と違っている

といったことを言われてしまうと、第三者との関係が悪化してしまったり、第三者が講ずる個人情報保護措置について適切でない情報提供を行っていたということになりかねませんので、提供先の第三者に、第三者が講じている個人情報保護措置の内容を確認する機会を設けるのが無難かと思います。相手が外資系の企業等の場合には、そういう確認をしても何の返事もないケースも多いと理解しています。しかし、契約関係がある民間の事業者である場合には、提供先の第三者に全く無断で独断的な情報提供をするのではなく、提供先の外国にある第三者に確認をした上で情報提供をすることがビジネス上でも一般的だと思います。この辺りの対応については各社いろいろお考えがあると思いますし、ケース・バイ・ケースで、第三者との関係や契約関係も踏まえ、どう対応するのかを最終的に判断いただければと思います。

ウは、相当措置を講ずる方法により越境移転をする場合における留意点です。先ほど述べたように、年に1回、海外委託先などについてのモニタリングを実施していると思いますので、そのモニタリングに関するアンケートのチェック項目を改正法に則した項目に改定することが必要かと思います。外国にある第三者の企業によっては、アンケートになかなか協力してくれない企業もあるかと思いますが、改正後においてはモニタリングが義務化されていますので、従来から非常に非協力的だった越境移転先・海外委託先などについてどう対応していくのか方針を策定することも重要ではないかと思います。

3. 漏えい等の報告等に関する改正

(1) 法改正の内容

漏えい等の報告等に関する改正については、レジュメでは、個人情報保護法の改正内容および通則編に関するガイドラインに即して記載しています。金融分野ガイドラインの適用を受ける金融機関におかれては、これらのほかに個人情報保護委員会と金融庁のQ&Aを踏まえた実務対応が実務上重要になってくると思います。

金融分野ガイドラインに関するQ&Aの改定版は、まだ公表されておらず、改正内容が明らかになっていません。今後、公表されると思いますので、そういったものを踏まえ、最終的な実務対応を確定していただければと思います。金融分野ガイドラインが適用される事業者は個人情報保護法と金融分野ガイドライン双方を遵守する必要がありますので、ここでは、その前提である個人情報保護法上の取扱いのルールを説明したいと思います。

まず、アですが、レジュメに記載しているように、個人データの漏えい、滅失、棄損など一定の事態が発生した場合においては、法定の方法で当該事態が生じた旨を個人情報保護委員会などに報告しなければいけません。現在の金融分野ガイドラインにおいては、金融庁などに報告する形になっていると思います。報告を要する場合は、レジュメに記載している①から④の場合です。まず①ですが、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た場合、あるいはそのおそれがある場合には、それらが1件でも報告が必要になります。括弧で記載しているように、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については

報告の対象外になりますので、高度な暗号化がなされていたかどうかというところが1つポイントになってきます。一般的な事業会社が個人の顧客の要配慮個人情報を取得するケースはほぼないですが、金融機関におかれては要配慮個人情報を取得しているケースがかなりあり、それが1件でも漏えいしてしまうと、結構なスピード感で当局報告が必要になりますので、これは少し重めの義務かと思えます。したがって、高度な暗号化がなされているかどうかというところがポイントになってくると思います。

高度な暗号化については、レジュメに記載しているように、個人情報保護委員会の個人情報保護法Q&Aで参考になる考え方が記載されていますので、こういったものを使い、職員に対して外に持ち出せるタブレットやノートパソコンを提供している場合には、個々の端末が高度な暗号化がなされているものに該当するのかどうかを事前に検討しておくことが実務上重要ではないかと思えます。端末がなくなった後に高度な暗号化に該当するのかどうかを検討していると、後ほどお話しする、時間的な要件に間に合わない可能性もあります。端末ごとに要報告の端末なのかそうではないのかということ事前に整理しておく、実務対応がしやすいのではないかと考えます。

続きまして、②の個人情報保護法による当局報告が必要な2つ目の類型です。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のある個人データの漏えい等が発生した場合にも当局報告が必要になります。こういったものが何故必要なのかということですが、漏えいした個人データを利用して本人になりすまして財産の処分が行われるおそれがある

ので、そういったことを踏まえ、当局報告を必須にしているという回答がパブリックコメントでなされています。信託会社・信託銀行におかれては、何らかの形で財産的なものに関連する情報を保有しているケースが大半なので、どのような情報が該当するのかが実務上の関心が高いところかと思います。パブリックコメントの回答などにおいては、例えばレジュメに書いているように、住所、電話番号、メールアドレス、SNS アカウントのみの漏えい、銀行口座の情報の一部のみの漏えい、クレジットカード番号の下4桁のみの漏えいについては該当しないといった説明がなされています。こういったものが該当するのにはある程度わかりやすくなっていると思いますので、こういったものを踏まえ、即時に個人情報保護法に基づく当局報告が必要な事案かどうかを判断できるチェックシートのようなものを作成しておくことが望ましいと思います。

※のところを実務上の論点を挙げています。財産的被害が生ずるおそれがある個人データの漏えいが発生した後、信託会社・信託銀行が被害防止措置を講じ、その結果、財産的被害が生じるおそれがほぼなくなった場合でも当局報告が必要かという論点があると思います。普通、企業は、財産的被害が生じるおそれのある個人データの漏えいが発生した場合、例えばクレジットカードであれば利用を停止したり、新しいクレジットカード番号をすぐに発行したりといった被害防止措置を講じるかと思います。これについては、パブリックコメントの回答において、そういった被害防止措置を講じて、その結果、財産的被害が生じるおそれがほぼなくなった事案においても当局報告はしてくださいといった非常

に厳しめの回答が出ています。こういったものに該当する財産的被害が生ずるおそれがある個人データが漏えいした場合については、ほぼ報告しなければいけないことになると思います。

さらに、③不正の目的を持って行われたおそれのある個人データの漏えい等が発生し、また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、または発生したおそれがある事態についても当局報告が必要になります。③、④については、時間の兼ね合いもあるので詳細な説明は割愛させていただければと思います。

続きまして(イ)のところ、報告に関する時間的な要件があります。これは個人情報保護法に基づく説明になっているので、便宜上、個人情報保護委員会と表記していますが、当局への報告は速やかに、具体的には事態発生を知った時点からおおむね3～5日以内に報告すべきとされています。これは土日・祝日を含みます。すなわち金曜日の夕方に発覚したケースでは、初日を算入して日数をカウントするのか否かにもよりますが、概ね週明けの水曜日頃までに速報をすることが求められます。先ほどお話したように、要配慮個人情報1件でも漏えいした場合には、こういったスピード感での対応が必要になります。最近3連休も結構多いので、金曜日の午後に発生した事案への対応はかなりタイトです。以上が速報という形での報告で、速報した後、確報、すなわち最終報告をすることが必要になります。それについては事態発生を知った日から原則として30日以内に報告することが求められています。

それから(ウ)です。委託先で漏えい等が発生

する場合もあると思われませんが、委託先と委託元の双方が原則として報告義務を負う形になります。しかし、委託先が委託元に対し漏えいの通知をしたときには、委託先の報告義務は免除されますので、実務上は委託元で報告をすることになると思います。委託先としては委託元に通知をしてお詫びするという対応をされることが多いのではないかと予想しています。

今のところで、上記アの①から④の場合、信託会社は一定の場合を除き、本人に対し、法定の方法により上記事態が生じた旨を通知しなければいけないということで、本人への通知も法律上の義務に改められています。従来から金融分野ガイドラインの適用のある信託銀行などにおかれては、本人通知を送っていたと思いますが、各銀行により通知の様式やスタイルは全然違っていました。私も本人への通知文の作成、あるいはその修正、リーガルチェックを担当するケースが非常に多く、各社によって違っていましたが、改正後は従来の実務にかかわらず、法定の事項を記載した通知書を作成するところがコンプライアンス上の重要なポイントです。過去の同種事案で使用した通知書を流用するのではなく、改正法が適用される事案においては、個人情報保護法第22条の2第2項に基づく規律に適合した通知書を作成することが必要です。

(2) 実務上の留意点

事前に質問をいただいていますので、その質問を読み上げた上で回答します。質問は、「金融庁の「金融機関における個人情報保護に関するQ&A」の問Ⅱ-2の回答では、「個人情報には、他の情報と容易に照合すること

ができ、それにより特定の個人を識別することができるものが含まれますが、事業者において通常の業務における一般的な方法で、他の情報と容易に照合が可能であり、それにより特定の個人を識別することが可能であるならば、他の第三者から見て特定の個人を識別することができないとしても、当該情報は個人情報に該当するものと考えられます」という記述があります。当該情報としては、顧客番号等が考えられますが、具体例をご教授いただけますでしょうか。」というものです。これは、おっしゃるとおり、顧客番号などが考えられると思います。例えば融資に関する書類であれば、顧客の融資の案件番号のようなものがこれに該当すると思います。

質問には続きがあります。「また、例えば顧客の連絡を電子メールで送信し、もし誤送信した場合、メール本文に本人を特定する内容が記載されていなかったとしても、本文の冒頭に宛名（顧客の氏名）を記載し、末尾に送り主名（弊社名および担当者名）を記載しているので、弊社の取引先であると誤送信先には分かってしまいます。本事案は、個人情報の漏えいに該当すると判断してよろしいでしょうか。」という内容です。結論としては、おっしゃるとおりかと思います。

4. 保有個人データに関する事項の公表等に関する改正

(1) 現行法の概要

現行法でも、①信託会社の名称、②全ての保有個人情報の利用目的、③開示請求等に応じる手続きといったものを本人の知り得る状態に置かなければいけないという義務が課されています。※のところにるように、本人

の知り得る状態に置くというのは、本人の求めに応じ、本人から請求があった場合には遅滞なく回答する場合を含みます。インターネット上のホームページに掲載する形で、名称や利用目的、開示請求等に応じる手続きといったものを対外公表している信託会社が多いかと思えます。プライバシー・ポリシーの中に①から④の事項をまとめて記載しているケースが少なくないと思えます。

(2) 法改正の内容

本人の知り得る状態に置かなければならない項目が追加・拡大されています。具体的に追加されている項目は、①のところにあるように、安全管理のために講じた措置や信託会社の住所、代表者の氏名などです。これらを本人の知り得る状態に、例えばプライバシー・ポリシーの中に記載してくださいということです。

(3) 実務上の留意点

これを踏まえ、プライバシー・ポリシーの見直しを多くの加盟会社で行われていると思えますので、実務上の留意点についてお話しします。

まず、公表事項が追加されていますので、プライバシー・ポリシーの見直しが当然必要になります。先ほど申しあげたように、信託会社の住所、代表者の氏名等を本人の知り得る状態に置かなければいけないことになっています。実務上の論点としては、住所や代表者の氏名をプライバシー・ポリシーの中に明記するのか、それともプライバシー・ポリシーの中に会社概要のようなものへリンクを張って、そこで閲覧できる状態にするかということがあります。インターネットのホームペ

ージ上には、会社概要のページとプライバシー・ポリシーのページが別々にあると思います。プライバシー・ポリシーの中に住所、代表者の氏名を明示すると、代表者や本店の住所が変わるたびにプライバシー・ポリシーを改定しなければいけないという煩わしさがあるので、プライバシー・ポリシーの中では、住所、代表者の氏名についてはこちらをご覧くださいという形で、会社概要のページにリンクを張る形で対応することも考えられると思います。

それから、後ほど少しお話ししますが、法定の公表事項に開示請求等に応じる手続きを記載することになっています。開示請求等への対応の手続きもプライバシー・ポリシーの中に記載しているケースが多いかと思えます。開示請求等への対応の手続きも改定が必要になると思えますので、後ほど開示請求のところで具体的にお話しできればと思います。この点はレジュメには記載していませんが、相談が多い点なので、注意いただければと思います。

以上のほか、イのところに書いているように、安全管理のために講じた措置の追加がありますので、この点について詳しく説明をしていきます。今回、安全管理のために講じた措置について、本人の知り得る状態に置くこと、例えばプライバシー・ポリシーの中に記載することなどが求められています。①に書いているように、安全管理措置の概要をウェブサイトに掲載して、その具体的な内容については、個々の顧客から質問があった場合に、その顧客にだけ遅滞なく回答するという対応も可能です。何から何まで全部ウェブサイトに書かなければいけないわけではありません。実務的には、ウェブサイトにどこまで掲

載し、照会があった場合に個別に回答するのはどこからなのか、線引きをすることが重要かと思います。私の感覚では、概要や骨子をウェブサイトに掲載して、それより詳しく知りたい顧客がいれば個別に質問してもらい、その質問に対する回答の中で分かりやすく説明するという実務対応の方針を持っている会社が多いかと思います。

②のところで、安全管理のために講じた措置についてです。個人情報保護法の第20条だけでなく、第21条、第22条に基づき講じた措置についても公表する必要があります。安全管理ということになると第20条だけのように感じるのですが、第21条、第22条に基づき講じた措置についてプライバシー・ポリシーの中に書いていない会社があった場合には、第21条、第22条に基づき講じた措置についても、その概要をウェブサイトに掲載することを検討する必要があります。

③の外部環境の把握についてです。個人データを保管しているA国における個人情報の保護に関する制度を把握した上で安全管理措置を実施している、といった形で公表することが事例として示されています。この事例の出典は個人情報保護委員会のガイドライン（通則編）です。こういった形で外部環境を把握した上で安全管理措置を講じている旨を公表すること、本人の知り得る状態に置くことが求められています。

外部環境の把握に関して、事例の下にいくつか記載しています。外国において個人データを取り扱っている場合については、外国の名称とともに、本人の保有個人データの安全管理のために講じた措置について、本人の知り得る状態に置く必要があることも個人情報保護委員会のパブリックコメントへの回答で

明らかにされていますので、これについてどこまで対応するかというところが論点になります。具体的に、外国において個人データを取り扱っている場合が挙げられています。クラウドサービスの利用の場合や個人データの取扱いの委託の場合などを含め、外国において個人データを取り扱う場合が1つ目に例示されています。2つ目に、外国にある支店や事務所に個人データを取り扱わせる場合、3つ目に、外国にある支店や委託先に個人データを取り扱わせる場合、4つ目に、再委託先に個人データを取り扱わせる場合です。このような場合には、当該外国の名称、保有個人データの安全管理のために講じた措置について、本人の知り得る状態に置くことが通則編等で求められています。これらは通則編のガイドラインにおける規定ですので、信託会社だけではなく、全ての事業者にも適用されます。どのレベルの運用になるのかはまだ分かりません。4月以降、全ての事業者が委託先やクラウド利用を含め、網羅的に調査して外国の名称を対外公表するのか、そうではなく個別に顧客から質問があった場合には答えるという対応をするのか、蓋を開けてみないと分かりませんが、ポイントの1点目としては、全ての事業者にも適用されるレベルの規制です。

金融機関はその場合にどのように対応するのか悩ましいところではありますが、少なくとも保有個人データの安全管理のために講じた措置の詳細、即ち、すべての委託先やクラウド利用の状況については、対外公表はせずに、顧客から質問があったら回答するという対応になるかと思います。個々のクラウドサービスの利用や個々の委託先についてどういった措置を講じているのかについて、ホームページで公表するのは少し過剰反応だと思い

ます。そういったものは対外公表せずに、個々の顧客から問い合わせがあった場合には、差し支えない範囲で回答することになるかと思えます。外的環境の把握に係る規制との関係で、外国の名称をホームページに公表するのか、それとも、それについても個別に質問があった場合に回答するのかという辺りは、各社のビジネス判断によると思えます。

ウの共同利用の公表文言の見直しについて、信託会社・信託銀行におかれては、個人情報のグループ内利用も含めて共同利用を行っている、あるいは業界団体ベースの共同利用を行っているケースが多いと思えます。共同利用を行う場合には、個人情報保護法に従い、法定の事項を公表する必要がありますが、法定の公表事項、必要的記載事項が拡大しているので、共同利用を公表している文書・帳票といったものについて見直しが必要になるかと思えます。こちらについても、ホームページのほかにもいろいろなところに記載されていると思えますので、そういったものについて改正法対応をしていくことが重要になると思えます。

事前の質問をいただいていますので、それに回答します。質問は、「今回の改正に伴い、公表事項へ保有個人データの処理の方法について記載することが求められています。金融機関は顧客等からさまざまな個人データを取得していると思われそうですが、自社が保有している個人データのうち、特に自社の業務上重要であると思われるものに絞って記載することで問題はないと考えてよろしいのでしょうか。それとも、保有している個人データ全てについて言及しなければならないのでしょうか。もし後者だとすると、公表事項はかなりの分量になりますし、事業者側の負担も大き

くなるのではないかと危惧しています。2021年12月時点では、公表事項の項目としての保有個人データの処理方法については、ウェブ上で検索してもそれほど扱っているウェブサイトは見当たらない状態なので、現時点でご解説いただける情報がありましたらお願いしたいと考えています。」という内容です。

「処理の方法」について質問をいただいています。安全管理措置の内容をプライバシー・ポリシー等に記載することが求められているだけで、データ処理全般に関する記載を求められているわけではないと思えます。先ほどお話ししたように、膨大な分量の内容を対外公表する事業者は多くないと私は予想しています。そういった実情も踏まえ、どこまでを対外公表して、どこからの事項を顧客から質問があった場合には回答するという線引きの問題かと思えます。

5. 個人関連情報の第三者提供の制限等の新設

(1) 法改正の内容

後ろに行くにつれ、重要度がだんだん下がっていくようにレジユメの項目建てを構成・整理をしています。残り時間の関係もありますので、残りは若干駆け足で説明させていただきます。

個人関連情報の典型例は、インターネットの閲覧履歴、位置情報、クッキー等に関する情報かと思えます。この義務規定の創設ですが、ご存知のとおり、プラットフォーマー、インターネット上の広告業者などの個人関連情報取扱事業者が、提供先の第三者、例えば信託会社・信託銀行が「提供先の第三者」にあたりますが、信託会社・信託銀行が個人情

報に当たらない情報（個人関連情報）を個人データとして取得することが想定される時は、一定の場合を除くほか、本人の同意が得られていることなどについて、あらかじめ法定の方法により確認をすることが求められ、確認しない場合には、個人関連情報を第三者に提供してはならないといったルールが新設されます。

(2) 実務上の留意点

アにあるように、信託会社・信託銀行の業務においてサードパーティークッキーなどを利用している業務があると思います。そういった場合は法的な見地から同意を取らなければいけないので、影響が出てくると思います。改正法対応が必要なのか、改正後も引き続き利用できるものなのか、慎重な検討が必要かと思えます。各社によって考えが違っている部分もありますし、まだ整理が不確定な部分もあるので、非常に悩ましい事案が多いと感じています。

イのところで、金融機関では、不正契約の防止のため、電話番号の使用履歴のデータや携帯端末等の情報などを取得したり、データ分析会社等を利用したりしている場合があります。こうした電話番号等については個人関連情報に該当する可能性があるという指摘がパブリックコメントの中でなされています。過去、犯罪に利用された電話番号をたまたま使っている人から申し込みがあった場合、信託会社・信託銀行としては、その時点で、その電話番号を使った人が誰か、その段階で分かることとなります。これは個人関連情報を個人データとして取得していることになるのではないかという指摘がありますので、不正契約の防止のために、犯罪等に使われた電話

番号を取得している場合においては、改正法対応が必要ではないかという見地から、リーガルチェックを行う必要があると思います。

ウのところです。ターゲティング広告を行う場合の利用目的の特定・明示方法についての対応が必要になってきます。これは個人情報保護法の改正というよりは、利用目的の特定に関する個人情報保護委員会のガイドライン（通則編）の改正を受けたものです。具体的には、本人の行動・関心等の情報を分析する場合、すなわちプロファイリングなどを行う場合については、事例1）に記載しているように、「取得した閲覧履歴や購買履歴等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします」といったように、どういう情報を分析して、どういうことに利用するのかを分かりやすく本人に示す必要がある旨、ガイドライン（通則編）の改正で明確化されています。したがって、プロファイリングなどを行っている業務がある場合には、個人情報の利用目的を改定・追加することが必要になるかと思えます。

6. 開示請求に関する改正

(1) 現行法の実務運用

現行の開示の方法に関しては紙と定めている会社が多く、基本的に電磁的データでの開示請求には応じていないケースが多いと思います。

(2) 法改正の内容

ところが、改正後においては、電磁的な記録の提供による方法その他の方法で開示を請求することができるといった形で、本人に選

択権を認めています。電磁的な記録の提供による方法か、紙の交付による方法か、本人が指定した方法で開示することを求めています。もちろん、電磁的な記録の提供が非常に困難な場合については別ですが、まずはそれが原則として導入されるということです。

イとウは細かい点になるので割愛します。

エのところでは、従来は保有個人データに関する開示請求という形だったのですが、第三者提供記録（個人情報保護法に基づき作成しなければならないとされる一定の記録）についても開示請求が認められた点が今回の大きな改正点です。これらを反映した形でプライバシー・ポリシーを改定することが必要になると思います。

(3) 実務上の留意点

まず、アの開示請求書の様式の改定です。開示請求書の様式をインターネット上で対外公表している企業もありますが、開示請求書の様式を改定する必要があります。具体的には、従来は保有個人データの開示請求書という「保有個人データ」に限定した記載がありました。改正後は保有個人データだけではなく第三者提供記録についても開示の請求が認められることとなりますので、それを何らかの形で明確化するような様式の見直しを行うことが必要になる可能性があると思います。

それから、従来は紙で回答する方法が一般的でしたので、それを前提にした様式になっていました。改正後においては電磁的な記録による提供か、紙の交付による提供かを本人が選択できる形になりますので、そういった選択欄を設ける改定が必要になると思います。そのほか、各社ごとに帳票の特徴がある

と思いますので、そういったものを踏まえて改定することが必要になると思います。

イのところでは、音声データそのものの開示が必要になる場合もあると思います。音声データの開示というと、コールセンター業務を委託していれば、コールセンター会社との協議が必要になる可能性があると思います。実際の音声の当事者はコールセンター会社の従業員である可能性もあるかと思うので、そういった音声を開示することがよいのか、開示する場合の実務対応をどうするのか、開示する場合はコールセンター会社で一定の加工処理を行う可能性があると思いますが当該費用を誰がどう負担するのか、そういったことを含め、コールセンター会社と取り決めることも必要になってくると思います。実務上、コールセンターに苦情が入り、それが長期化して、その際に過去のコールセンターの録音データに関する請求を受けることが時々あります。そういったものについて、まず、それが保有個人データに該当するかどうかを検討した上で、該当する場合には音声データを開示せざるを得ない場合が出てくると思います。コールセンター会社とそういった場合の実務運営などの取り決めをしておくことが望ましいと思います。

※のところでは事前の質問をいただいています。「現行、当行では開示請求の受付について、店頭窓口にて本人確認の上、書面交付による対応フローとしています。今回の改正はあくまで交付方法に関する改正であり、受付方法は現行どおりという理解でよろしいでしょうか。例えば、仮に受付自体もインターネット、メール等の電磁的方法で行う必要がある場合は、本人からの開示請求か否かをどのように確認するのが課題となります。」という

内容です。受付方法については現行どおりでよいと思います。

7. 利用停止等請求に関する改正

(1) 現行法の概要

利用停止等請求に関して、外見上は大きな改正がなされていますが、そもそも信託会社・信託銀行におかれては、1年間に利用停止等の請求がなされる件数はかなり少ないと理解しています。改正内容自体は大きく見えますが、実務へのインパクトという意味では小さいと思いますので、社内の規定に詳細な規定があるのであれば必要な改定を行っておくぐらいでよいと思います。

(2) 法改正（追加）の内容

下線部分ですが、保有個人データの取扱いにより当該本人の権利または正当な利益が害されるおそれがある場合等にも利用停止等の請求ができるということで、利用停止請求ができる事由を拡大しています。ただ、信託会社・信託銀行におかれては、顧客の権利利益を侵害するような形で個人データを利用しているといったケースはほほないかと思imasので、実務上、利用停止等の請求が認められるケースはあまりないのではないかと感じています。

(3) 実務上の留意点

レジュメに記載していませんが、実務上、利用停止請求自体はあまりないと思いますし、先ほど申しあげた、追加された事由に該当する事案もあまりないと思いますので、影響は少ないと感じています。

事前に質問をいただいております、「利用停止の請求に実務上どこまで対応できるか、法令やシステム上の制限から対応できない場合に、どのような代替措置を取れるかという点に課題を感じています。」という内容です。システム上、利用停止ができないとか、コンプライアンス上の理由からデータを削除できないシステムになっていたりすると、対応が難しいところではあると思いますが、そもそも利用停止をしなければいけない事態はほほないと思います。もし利用停止しなければいけない事態になった場合には、顧問弁護士やシステムベンダー等と相談して、どう対応するのかを検討していくことになると思います。

以上で私の説明を終わります。ご清聴ありがとうございました。

本稿は、令和4年1月27日に開催された信託セミナーにおける浅井国際法律事務所 弁護士 浅井弘章氏の講演内容を取りまとめたものです。

(あさい・ひろあき)

2022年1月
信託協会・信託セミナー

改正個人情報保護法に対する実務対応

浅井国際法律事務所
弁護士 浅井 弘章

※ 本レジュメは、2022年1月20日時点の公表情報をもとに作成しています。今後の動向にご留意ください。

はじめに(改正の動向と改正法対応上の留意点)

- ① 実務上、2021年8月に行われたガイドライン(通則編)の改正、Q&Aの改訂・新設が重要。
- ② ガイドライン(通則編)などのパブコメ回答が2021年8月に公表されているが、件数が膨大である。
- ③ 本日、ご説明する「令和2年の個人情報保護法の改正」のほかに、「デジタル庁設置法及びデジタル社会の形成を図るための関係法律の整備に関する法律の一部の施行に伴う個人情報保護法の改正」(令和3年個人情報保護法改正)があり、これにより、個人情報保護法の条文番号が大きく変り、また、学術研究機関等が関係する個人情報の取扱いに係る条項が明文化されている。
- ④ 2021年9月、「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」などが改定されている。
- ⑤ 2021年12月に、「金融分野ガイドライン」等の改定案が公表され、現在、パブコメ手続中である。
- ⑥ 上記⑤の「金融分野ガイドライン」等の改定が終わった後、「金融分野ガイドラインに関するQ&A」の改定がなされる可能性がある。

1. 不適正な利用の禁止に関する規定の「新設」(「明確化」)

(1) 法改正の内容

ア 信託会社は、違法・不当な行為を助長し、又は誘発するおそれがある方法により個人

情報を利用してはならない旨の規定を「新設」する(新 16 条の2¹)。

イ 信託会社が新 16 条の2に違反した場合の効果・影響

(ア) 個人情報保護委員会による「是正勧告」の対象になる(新 42 条 1 項)。

(イ) 利用停止・消去請求の対象になる(新 30 条 1 項)。

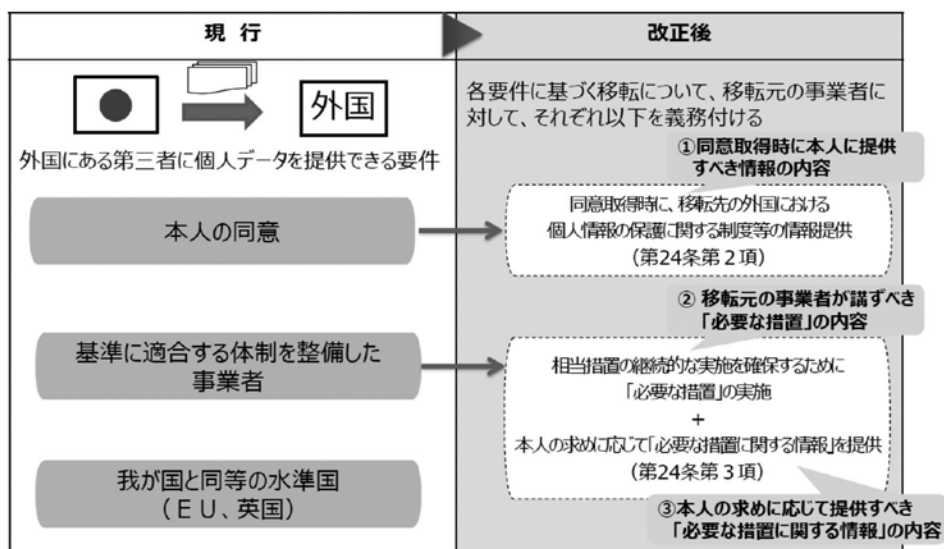
(2) 実務上の留意点

ア 個人情報の利活用を目的とする新規プロジェクト等の企画時の留意点

イ 個人情報に関する苦情対応の負担の増加

2. 「外国にある第三者」への提供の制限に関する改正

(1) 法改正の内容について



出典:個人情報保護委員会ホームページ

ア 信託会社は、「外国にある第三者への個人データの提供を認める」旨の本人の同意を得ようとする場合には、法定の方法より、あらかじめ、当該本人に参考となるべき情報(次の①～③)を当該本人に提供しなければならない(新 24 条 2 項)。

¹ 本レジュメでは、現行法と比較した規制内容の改正を理解しやすくするため、個人情報保護法の条文については、原則として、令和3年改正個人情報保護法による改正前の条文番号を用いています。但し、金融分野ガイドラインの改正内容を引用している箇所については、当該改正内容を尊重し同改正後の条文番号を用いています。

- ① 外国の名称
- ② 適切かつ合理的な方法により得られた当該外国における個人情報保護制度に関する情報
- ③ 当該第三者が講ずる個人情報保護措置に関する情報

※ ①から③の情報提供が難しい場合には、代替措置が認められている。

イ 信託会社は、相当措置を講ずる方法により、個人データを「外国にある第三者」に提供した場合には、法定の方法により、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なければならない(新24条3項)。

※ 措置の内容

- ① 当該第三者による相当措置の実施状況並びに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を、適切かつ合理的な方法により、定期的に確認すること。
- ② 当該第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データの当該第三者への提供を停止すること。

(2) 金融分野ガイドラインの改正案

ア 本人の同意に基づく場の上乗せ措置

- ① 本人の同意を得る場合には、原則として、書面(電磁的記録を含む。以下同じ。)によることとする。なお、信託会社があらかじめ作成された同意書面を用いる場合には、文字の大きさ及び文章の表現を変えること等により、個人情報の取扱いに関する条項が他と明確に区別され、本人に理解されることが望ましい。または、あらかじめ作成された同意書面に確認欄を設け本人がチェックを行うこと等、本人の意思が明確に反映できる方法により確認を行うことが望ましい(新3条)。
- ② 本人の同意を得る際には、原則として、書面によることとし、当該書面における記載を通じて、施行規則17条2項から4項までの規定により情報提供が求められる事項に加えて、
 - ・ 個人データの提供先の第三者
 - ・ 提供先の第三者における利用目的
 - ・ 第三者に提供される個人データの項目を本人に認識させた上で同意を得ることとする。

本人の同意を得ようとする時点において、「個人データの提供先の第三者」に掲

げる事項が特定できない場合には、これに代わる本人に参考となるべき情報を当該本人に認識させた上で同意を得ることとする(新13条1項)。

- ③ 信託会社は、事後的に提供先の第三者を特定できた場合は、本人の求めに応じて、施行規則 17 条2項各号に定める情報を提供することとする。また、このような情報提供の求めが可能である旨を前項に定める書面における記載を通じて本人に認識させるとともに、20 条に定める「個人情報保護宣言」と一体としてインターネットのホームページへの常時掲載又は事務所の窓口等での掲示・備付け等により、公表することとする。ただし、本人から情報提供の求めがあった場合であっても、例えば、情報提供することにより信託会社の業務の適正な実施に著しい支障を及ぼすおそれがある場合等は、同項各号に定める情報の全部又は一部について情報提供しないことができる。情報提供しない場合であっても、信託会社は、本人に対し、遅滞なくその旨を通知するとともに、その理由を説明することとする(新13条2項)。
- ④ 信託会社は、法 28 条1項の規定により本人の同意を得ようとする時点において、個人データの提供先の第三者が所在する外国が特定できなかった場合、事後的に提供先の第三者が所在する外国が特定できたときには、当該外国の名称をインターネットのホームページへの掲載等により、公表するとともに、定期的に更新することが望ましい(新13条4項)。

イ 相当措置を講ずる方法による場合の上乗せ措置

- ① 第三者に個人データを提供した場合に施行規則 18 条1項1号の規定により当該第三者による相当措置の実施状況を確認する際には、個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法により確認を行うこととする(新13条3項)。
- ② 信託会社は、法 28 条3項及び施行規則 18 条に基づき、本人の求めに応じて事後的に情報を提供する旨を 20 条に定める「個人情報保護宣言」と一体としてインターネットのホームページへの常時掲載又は事務所の窓口等での掲示・備付け等により、公表することとする(新13条3項)。
- ③ 信託会社が、相当措置を講ずる方法により、外国にある第三者に個人データを提供した場合には、提供先の第三者が所在する外国の名称をインターネットのホームページへの掲載等により、公表するとともに、定期的に更新することが望ましい(新13条4項)。

(3) 実務上の留意点

ア 信託会社による「外国にある第三者」への提供の事例

- ・ 外国送金
- ・ エクスボージャー等を移転する国際金融取引
- ・ FATCAに基づくIRSへの年次報告

- ・ 海外事業者のクラウドサービスの利用(クラウドサービスの内容次第では、「外国にある第三者」への「提供」に該当しない場合がある)
- ・ 従業員の海外出向など

イ 「本人の同意を得る」方法により対応している場面における実務対応上の留意点

(ア) 参考情報の提供の履行方法について

Q12-10 法第 24 条第2項の規定による本人への情報提供の方法として、必要な情報が掲載されたウェブサイトの URL を本人に提供することは認められますか。

A12-10 個別の事案ごとに判断されますが、例えば、施行規則第 11 条の3第2項から第4項までの規定により求められる情報が掲載された Web ページが存在する場合に、当該 Web ページの URL を自社のホームページに掲載し、当該 URL に掲載された情報を本人に閲覧させる方法も、施行規則第 11 条の3第1項における「適切な方法」に該当すると考えられます。

ただし、この場合であっても、例えば、当該 URL を本人にとって分かりやすい場所に掲載した上で、同意の可否の判断の前提として、本人に対して当該情報の確認を明示的に求めるなど、本人が当該 URL に掲載された情報を閲覧すると合理的に考えられる形で、情報提供を行う必要があると考えられます。

(イ) 第三者が講ずる個人情報保護措置の確認方法

Q12-12 施行規則第 11 条の3第2項第3号の「当該第三者が講ずる個人情報の保護のための措置に関する情報」を確認する方法として、どのような方法が考えられますか。

A12-12 個別の事案ごとに判断する必要がありますが、例えば、提供先の外国にある第三者に確認する方法や、提供先の外国にある第三者との間で締結している契約において、当該第三者による個人データの取扱いについて定めている場合に、当該契約を確認する方法等が考えられます。

ウ 相当措置を講ずる方法による場面における実務対応上の留意点

3. 漏えい等の報告等に関する改正

(1) 法改正の内容

ア 信託会社は、一定の場合を除き、その取り扱う個人データの漏えい、滅失、毀損その

他の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あるものとして法定の事由が生じたときは、法定の方法により、当該事態が生じた旨を個人情報保護委員会に報告しなければならない(新 22 条の2第1項)。

(ア) 報告を要する場合

- ① 要配慮個人情報に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。以下同じ。)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事態

※ 「高度な暗号化」の意義

Q6-16 「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」とは、どのような場合が該当しますか。

A6-16 報告を要しない「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」に該当するためには、当該漏えい等事案が生じた時点の技術水準に照らして、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について、これを第三者が見読可能な状態にすることが困難となるような暗号化等の技術的措置が講じられるとともに、そのような暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されていることが必要と解されます。(後略)

- 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

→漏えい等した個人データを利用し、本人になりすまして、財産の処分が行われる場合を想定している。

→【報告事由に該当しない事例】

- ・ 住所、電話番号、メールアドレス、SNS アカウントのみの漏えいは、これに該当しない。
- ・ 銀行口座の情報の一部のみの漏えい
- ・ クレジットカード番号の下4桁のみの漏えい

※ 実務上の論点

漏えい発生後、信託会社が、被害防止措置を講じ、財産的被害が生ずるおそれがなくなったとしても、当局報告が必要か？

- 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

(イ) 時間的要件

個人情報保護委員会への報告は、速やかに(事態の発生を知った時点から概ね3日～5日(土日・祝日を含む)以内)報告をする。

速報後の確報については、原則30日以内にする。

(ウ) 委託の場合の取扱い

委託先で、個人情報保護委員会への報告が必要な情報漏えい事案が発生した場合、原則として、委託元と委託先の双方が報告する義務を負います。ただし、委託先が、個人情報保護委員会への報告義務を負っている委託元に対して、所定の事項を通知したときは、報告が免除される。

イ 上記アの場合、信託会社は、一定の場合を除き、本人に対し、法定の方法により、当該事態が生じた旨を通知しなければならない(新22条の2第2項)。

(2) 実務上の留意点

※ 事前質問

金融庁の「金融機関における個人情報保護に関するQ&A」の間Ⅱ-2の回答で、『「個人情報」には、他の情報と容易に照合することができ、それにより特定の個人を識別することができるものが含まれますが(問Ⅱ-1参照)、事業者において通常の業務における一般的な方法で、他の情報と容易に照合が可能であり、それにより特定の個人を識別することが可能であるならば、他の第三者から見て特定の個人を識別することができないとしても、当該情報は「個人情報」に該当するものと考えられます。』という記述があります。

当該情報としましては、お客様番号等が考えられますが、具体例をご教授頂けますでしょうか。また、例えば、お客様への連絡を電子メールで送信し、もし誤送信した場合、メール本文に本人を特定する内容が記載されていなかったとしても、本文の冒頭に宛名(お客様氏名)を記載し、末尾に送り主名(弊社名及び担当者名)を記載しておりますので、弊社の取引先であると誤送信した先には分かってしまいます。本事案は、個人情報の漏洩に該当すると判断してよろしいでしょうか。

4. 保有個人データに関する事項の公表等に関する改正

(1) 現行法の概要

信託会社は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態(※)に置かなければならない(27条1項)。

- ① 信託会社の名称
- ② 全ての保有個人データの利用目的
- ③ 開示請求等に応じる手続
- ④ 前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として施行令で定めるもの

※ 「本人の知り得る状態」には、本人の求めに応じて遅滞なく回答する場合を含む

(2) 法改正の内容

保有個人データに関し、本人の知り得る状態(※)に置かなければならないこととされる事項に、①安全管理のために講じた措置(新施行令8条1号)と②信託会社の住所及び代表者の氏名などを加える(新27条1項1号)。

(3) 実務上の留意点

ア プライバシー・ポリシーの見直しについて

イ 「安全管理のために講じた措置」の内容について

- ① 安全管理措置の概要をウェブサイトに掲載し、その具体的な内容については、本人の求めに応じ、遅滞なく回答するという実務対応も許容される。
- ② 法20条、21条(従業者の監督)、法22条に基づき講じた措置についても、公表が必要である。
- ③ 「外部環境の把握」について

「事例) 個人データを保管しているA国における個人情報の保護に関する制度を把握した上で、安全管理措置を実施 (※8)

(※8) 外国……の名称については……本人が合理的に認識できると考えられる形で情報提供を行う必要がある。」(ガイドライン(通則編))

- ・ 「クラウドサービスの利用や個人データの取扱いの委託等を含めて、外国における個人データを取り扱う場合には、当該外国の名称とともに、保有個人データの安全管理のために講じた措置について、本人の知りうる状態に置く必要があります」。

- ・「外国にある支店や事務所に個人データを取り扱わせる場合、外国にあるデータセンターで個人データを保存する場合には、外国において個人データを取り扱うこととなるため、当該外国の名称とともに、保有個人データの安全管理のために講じた措置について、本人の知りうる状態に置く必要があります。」。
- ・「外国にある支店や委託先に個人データを取り扱わせる場合、その取扱いの対象となるデータが日本にあるサーバーに保存されていたとしても、外国において個人データを取り扱うことになりはしないため、当該外国の名称とともに、保有個人データの安全管理のために講じた措置について、本人の知りうる状態に置く必要があります。」
- ・「外国にある委託先又は再委託先に個人データを取り扱わせる場合には、外国において個人データを取り扱うことになるため、当該外国の名称とともに、保有個人データの安全管理のために講じた措置について、本人の知りうる状態に置く必要があります。」。

ウ 共同利用の公表文言の見直しについて(新 23 条 5 項 3 号)

→ 必要的記載事項が追加された。

※ 事前質問

今回の法改正に伴い、公表事項へ保有個人データの処理の方法について記載することが求められております。

金融機関は顧客等から様々な個人データを取得していると思われませんが、自社が保有している個人データの内、特に自社の業務上重要であると思われるものに絞り記載することで問題はないと考えて宜しいのでしょうか。それとも保有している個人データ全てについて言及せねばならないのでしょうか。もし後者だとすると公表事項がかなりの分量になりますし、事業者側の負担も大きくなるのではないかと危惧しております。

2021年12月時点では公表事項の項目としての保有個人データの処理方法については Web 上で検索してもそれほど扱っている Web サイトは見当たらない状態ですので、現時点でご解説頂ける情報がございましたらお願いしたいと考えております。

5. 個人関連情報の第三者提供の制限等の新設

(1) 法改正の内容

ア 個人関連情報・個人関連情報取扱事業者の定義の新設

個人関連情報： 生存する個人に関する情報であつて、個人情報、仮名加工情報

及び匿名加工情報のいずれにも該当しないもの(新 26 条の2第1項)。

(具体例) 氏名と結び付いていないインターネットの閲覧履歴、位置情報、クッキー等

個人関連情報取扱事業者:特定の個人関連情報を電子計算機を用いて検索することができるように体系的に構成したものを事業の用に供している者(新 26 条の2第 1 項)。

イ 義務規定の創設

個人関連情報取扱事業者は、第三者(提供先)が個人関連情報を個人データとして取得することが想定されるときは、一定の場合を除くほか、本人の同意が得られていることなどについて、あらかじめ施行規則で定めるところにより確認することをして、当該個人関連情報を当該第三者に提供してはならない(新 26 条の2)。

※ 「第三者(提供先)が個人関連情報を個人データとして取得することが想定されるとき」とは、具体的にはどのような場合か？

- ① 提供先が個人データとして取得することを提供元の事業者(個人関連情報取扱事業者)が想定している場合(例えば、事前に個人関連情報を受領した後に、他の情報と照合して個人データにするといった旨を告げられている場合など)
- ② 取引状況等の客観的に事情に照らして、個人データとして取得することが一般人の認識を基準として想定できる場合

(2) 実務上の留意点

ア サードパーティークッキーなどを利用している場合には、影響がある。

イ 金融機関では、不正契約の防止のため、電話番号の使用履歴データ、携帯端末等の情報の取得やデータ分析会社等の利用を行っている場合がある。こうした「電話番号」が「個人関連情報」に該当する可能性がある。

ウ ターゲティング広告を行う場合の利用目的の特定・明示方法について(ガイドライン(通則編))。

「本人から得た情報から、本人に関する行動・関心等の情報を分析する場合、個人情報取扱事業者は、どのような取扱いが行われているかを本人が予測・想定できる程度に利用目的を特定しなければならない。

【本人から得た情報から、行動・関心等の情報を分析する場合に具体的に利用目的を特定している事例】

事例 1)「取得した閲覧履歴や購買履歴等の情報を分析して、趣味・嗜好に応じた新商品・サービスに関する広告のために利用いたします。」

事例 2)「取得した行動履歴等の情報を分析し、信用スコアを算出した上で、当該スコアを第三者へ提供いたします。」

6. 開示請求に関する改正

(1) 現行法の実務運用

開示の方法は「書面」(紙)と定めている会社が多く、基本的に電磁的データでの開示請求には応じていない。

(2) 法改正の内容

ア 本人は、信託会社に対し、当該本人が識別される保有個人データの電磁的記録の提供による方法その他の施行規則で定める方法による開示を請求することができると改める(新 28 条 1 項)。

イ 信託会社は、上記アによる請求を受けたときは、一定の場合を除き、本人に対し、当該本人が請求した方法(当該方法による開示に多額の費用を要する場合等)は、書面の交付による方法)により、遅滞なく、当該保有個人データを開示しなければならないと改める(新 28 条 2 項)。

ウ 信託会社は、上記アにより本人が請求した方法による開示が困難であるとき等は、本人に対し、遅滞なく、その旨を通知しなければならない(新 28 条 3 項)。

エ 上記アから上記ウまでは、第三者提供記録(信託会社が個人データを第三者に提供したときに作成しなければならないこととされる記録及び信託会社が第三者から個人データの提供を受けるに際して作成しなければならないこととされる記録をいう。)について準用する(新 28 条 5 項)。

(3) 実務上の留意点

ア 開示請求書の様式の改定

イ 音声データそのものの開示が必要な場合の実務対応(私見)

※ 事前質問

現行、当行では開示請求の受付について、店頭窓口にて本人確認のうえ書面交付による対応フローとしています。今回の改正はあくまで交付方法に関する改正であり、受付方法は現行通りという理解でよろしいでしょうか。例えば、仮に受付自体もインターネットメール等の電磁的方法で行う必要

があれば、本人からの開示請求か否かをどのように確認するのが課題となります。

7. 利用停止等請求に関する改正

(1) 現行法の概要

ア 信託会社は、本人から、当該本人が識別される保有個人データが、16条の規定に違反して本人の同意なく目的外利用がされている、又は17条の規定に違反して偽りその他不正の手段により個人情報が取得され若しくは本人の同意なく要配慮個人情報が取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去(以下「利用停止等」という。)の請求を受けた場合であって、その請求に理由があることが判明したときは、遅滞なく利用停止等を行わなければならない(30条)。

(2) 法改正(追加)の内容

ア 本人は、信託会社に対し、当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合等の一定の場合(※)には、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる(新30条5項)。

※ 次の①から③までのいずれかに該当する場合については、原則として、遅滞なく、利用停止等又は第三者提供の停止を行わなければならない。

① 利用する必要がなくなった場合

→「当該個人情報取扱事業者が利用する必要がなくなった」とは、利用目的が達成され当該目的との関係では当該保有個人データを保有する合理的な理由が存在しなくなった場合や利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等をいう。

② 当該本人が識別される保有個人データに係る法第22条の2第1項本文に規定する事態が生じた場合

③ 当該本人の権利又は正当な利益が害されるおそれがある場合

→「本人の権利又は正当な利益が害されるおそれがある場合」とは、法目的に照らして保護に値する正当な利益(※5)が存在し、それが侵害されるおそれがある場合をいう。

(※5) 「正当」かどうかは、相手方である個人情報取扱事業者との関係で決まるものであり、個人情報取扱事業者に本

人の権利利益の保護の必要性を上回る特別な事情がない限りは、個人情報取扱事業者は請求に応じる必要がある。本人の権利利益の保護の必要性を上回る特別な事情があるかどうかを判断するに当たっては、例えば、以下のような事情を考慮することになる。

- (ア) 本人又は第三者の生命、身体、財産その他の権利利益を保護するために当該保有個人データを取り扱う事情
- (イ) 法令を遵守するために当該保有個人データを取り扱う事情
- (ウ) 契約に係る義務を履行するために当該保有個人データを取り扱う事情
- (エ) 違法又は不当な行為を防止するために当該保有個人データを取り扱う事情
- (オ) 法的主張、権利行使又は防御のために当該保有個人データを取り扱う事情

イ 信託会社は、上記アの請求を受けた場合であって、その請求に理由があることが判明したときは、一定の場合を除き、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならない(新 30 条 6 項)。

(3) 実務上の留意点

※ 事前質問

利用停止の請求に実務上どこまで対応できるか、法令やシステム上の制限から対応できない場合にどのような代替措置を取れるか、という点に課題を感じております。

以上

[講演者紹介]

一橋大学法学部卒業、1999 年弁護士登録。銀行、信託銀行、保険会社、金融機関の業界団体、公的機関、製薬会社、出版社などの顧問弁護士等を務める。個人情報保護法・番号法対応のほか、取引・事務のオンライン化・デジタル化対応、犯罪収益移転防止法、FATCA 対応、実特法(CRS)対応などを専門とする。

100-0005 千代田区丸の内3-4-1新国際ビル8階 浅井国際法律事務所
電話 03-3213-2011