信託セミナー

改正個人情報保護法を踏まえた実務対応について

堀総合法律事務所弁護士　髙　木　いづみ
堀総合法律事務所弁護士　冨　松　宏　之

― 目　次 ―

はじめに

ただいまご紹介いただきました、堀総合法律事務所の弁護士の髙木です。本日は、まず、改正法のポイントと改正法の施行に際して各金融機関において主にどのような点に対応されたかについてお話しします。次に改正法への対応のポイントに関して五つの事項についてお話しし、最後に今後の課題についてお話しします。なお、資料の３頁に法律等の名称の略称に係る凡例を記載しています。説明の中では、例えば「金融分野における個人情報保護に関するガイドライン」を「金融ガイドライン」と呼ぶなど、この凡例の略称を用いることがあります。

1．改正個人情報保護法の主な変更点と対応のポイント

まず、改正法施行に際して、金融分野の個人情報取扱事業者がどのような対応をされたかをお話しするに当たって、主な改正点を大まかに振り返ってみます。

今回の個人情報保護法の改正は、2005年４月の施行から10年以上が経過し、この間にさまざまな環境の変化や事件、不具合などが発生したため、これらに対応することを目的として行われました。改正の背景としては、主に四つの点があると思います。これに対応して、改正のポイントも大きく四つに分けられると思います。

資料の５頁をご覧ください。まず、一つ目の背景としては、情報通信技術の飛躍的な進

展に伴い、個人の行動や状態に関するパーソナルデータが事業者に大量に集積されるようになったことが挙げられます。このような大量のパーソナルデータが悪用されると、個人のプライバシー侵害を招きかねない反面、企業がパーソナルデータをビッグデータとして利活用することにより、国民生活の利便性向上や国民の健康増進に役立つ可能性があります。しかしながら､改正法施行前においては、その定義の曖昧さから、パーソナルデータが個人情報として規制されるかどうかが不明確なグレーゾーンが大きかったと思います。そのため、事業者が萎縮してパーソナルデータの利活用がなされないといった弊害が生じていました。

このような背景を受け、改正法では、個人情報として規制される範囲を明確化するべく、個人識別符号を個人情報として明確に位置づける一方で、特定の個人を識別できないように加工した「匿名加工情報」という概念を導入し、一定のルールに則ったパーソナルデータの利活用を可能としました。また､「要配慮個人情報」という類型を設け、取得には原則として本人同意を得ることを必要とするなどの保護の強化も行われました。

二つ目の背景としては、改正前は個人情報保護法に関する事業者の監督は主務大臣によるものとされており、事業分野ごとにガイドラインが策定され運用されてきましたが、それぞれのガイドラインの運用の齟齬や重複等の問題があったと思います。そこで改正法では、事業者に対する一元的監督を実現するために、主務大臣制を廃止し、事業者に対する一元的監督を行う機関として「個人情報保護委員会」が設置されました。

三つ目の背景としては、ベネッセ事件で大規模な個人情報の漏えい問題が顕在化したことが挙げられます。この事件では、再委託先の管理の不十分さが露呈したことに加えて、漏えいした情報が名簿業者を通じて拡散されていたことが社会的議論を呼んだことは、皆さまもご記憶のことと存じます。そこで改正法では、名簿業者によるデータ流通を規制するべく、個人情報の流通経路を辿ることを可能とするための規制を置くとともに、不正に個人情報を提供した場合の罰則規定を設けています。また、オプトアウト規定を利用する個人情報取扱事業者は、所定の事項について個人情報保護委員会への届け出を行うこととされました。これについては、個人情報保護委員会から届け出された事項が公表される仕組みになっています。

四つ目の背景としては、企業の事業活動のグローバル化に伴い、情報流通もグローバル化し、世界各国で個人情報とプライバシー保護に関する法整備が進められたという環境の変化が挙げられます。そこで改正法では、データ流通のグローバル化に対応するために、外国の事業者に対する個人情報保護法の適用範囲を明確化するとともに、事業者による外国にある第三者に対する個人データの提供について新たな規制を設けました。

以上の四つが改正法のポイントであると思いますが、これを受けて金融分野の個人情報取扱事業者がどのような対応をされたかについてお話しする前に、金融分野の個人情報取扱事業者に対する監督関係について確認しておきたいと思います。

資料の６頁にあるように、改正法では、個人情報取扱事業者の個人情報の取扱いに関する監督を一元的に個人情報保護委員会が行うものとされました。個人情報取扱事業者に対

する報告徴収、立入検査、指導･助言、勧告、命令はすべて個人情報保護委員会の権限とされています。この監督権限を背景として、個人情報保護委員会によって公表されたのが、いわゆる通則ガイドラインと言われる、基本となるガイドラインをはじめとする４種類のガイドラインです。

一方で、個人情報保護委員会の監督権限のうち報告徴収や立入検査については、金融分野の個人情報取扱事業者に関する権限は金融庁、財務局、あるいは地方公共団体に委任されています。これを受けて、個人情報保護法第６条の「格別の措置」に該当するものとして、金融庁と個人情報保護委員会が共同で金融ガイドラインと実務指針を公表しています。

本日ご出席の皆さまの会社については、４種類のガイドラインに加えて、金融ガイドラインと実務指針が適用されるものと思います。また、信託協会は認定個人情報保護団体ですので、信託協会の対象事業者になっている事業者については、信託協会が定めた「個人情報の保護と利用に関する指針」および「個人データの安全管理措置等に関する指針」を遵守する必要があります。

さらには、信託兼営金融機関は、銀行業に関する認定個人情報保護団体である、全国銀行個人情報保護協議会の対象事業者にもなっているものと思います。したがって、信託兼営金融機関については、全国銀行個人情報保護協議会の個人情報保護指針等も遵守する必要があります。

それ以外に､資料の７頁に記載したように、皆さまの業務に関係する認定個人情報保護団体としては、日本証券業協会、日本投資顧問業協会、金融先物取引業協会、日本クレジット協会などがあります。これらの認定個人情報保護団体の対象事業者になっている事業者については、各団体が定める保護指針等が重畳適用されることになります。

金融分野の個人情報取扱事業者における改正法への対応のポイントの説明に戻ります。金融分野の個人情報取扱事業者においては、主に四つの観点で改正法への対応を検討されたものと思います。資料の８頁をご覧ください。まず一つ目は、個人情報の定義の明確化への対応です。具体的には、「個人識別符号」という概念が新たに設けられたことにより、個人識別符号に該当する情報で、これまで個人情報として取り扱っていなかったものがないかの確認作業が必要であったものと思います。

二つ目は、「要配慮個人情報」という概念が新たに設けられたことへの対応です。要配慮個人情報については、他の個人情報とは異なる規制が設けられていますので、これまで取得・利用していた個人情報のうち、要配慮個人情報に該当するものをピックアップして、要配慮個人情報の規制に即した取扱いに変更するための見直しが必要であったものと思います。

三つ目は、個人データの提供・取得に際して、確認・記録義務が課されたことへの対応です。改正後の個人情報保護法の第25条および第26条では、同法第23条第１項各号または同条第５項各号に該当する場合を除いては、原則として個人データの提供・取得に当たっては確認および記録の作成が義務付けられることになりました。そこで、各部署の業務における個人データの提供・取得の場面を洗い出し、それぞれが確認・記録義務の対象となるケースに当たるか、当たる場合には、従来の対応で確認・記録義務が満たされているか

の確認が必要であったものと思います。

四つ目は、外国にある第三者への個人データの提供についての対応です。改正法では、外国にある第三者への個人データの提供について、国内にある第三者への個人データの提供とは異なる規制が設けられました。具体的には、改正後の個人情報保護法第24条においては、外国にある第三者への個人データの提供に当たっては、原則として本人の同意が必要とされました。留意すべき点として、同法第23条第５項各号に列挙されている個人データの委託や共同利用等の場合について、同法第23条で規定されている個人データの第三者提供との関係においては、提供する相手方は「第三者」に該当しないものとされています。しかしながら、外国にある第三者が委託先等である場合には、同法第24条の規定が適用されることとなっていますので、この点においても対応が必要であったものと思います。このように、各部署の業務において、外国にある第三者に個人データの提供を行っている場面を洗い出して､同意取得がなされているか、あるいは同意取得を不要とする例外的ケースに該当しているかといった確認が必要となったものと思います。

以上の四つの対応のポイントですが、これらについて私どもは、はじめは３番目と４番目のポイント、特に３番目のポイントへの対応が大変なのではないかと思っておりましたが、実際に対応された企業にお聞きすると、２番目のポイントへの対応が特に大変であったという声が非常に多くありました。これは、金融分野の個人情報取扱事業者においては、ご存じのとおり改正前より要配慮個人情報と類似した概念として、機微情報（いわゆるセンシティブ情報）について、金融ガイドラインにより、他の個人情報とは異なる取扱いが定められていました。また、実務指針では、機微情報については他の情報とは異なる安全管理措置を講じることが求められていました。

今回の改正によって、要配慮個人情報はすべて機微情報に該当することとなりましたが、これに加えて一連のパブリックコメントなどの手続において、機微情報の範囲が明確になり、従来に比べ広い範囲のものが機微情報に該当することが明らかになりました。これにより、これまでよりも広い範囲の情報を機微情報として取り扱わなければならなくなったことについて、実務的な影響が大きかったものと思われます。

2.　個人情報の定義の明確化への対応と漏えい事案等への対応

ここからは、改正法の対応のポイント四点に外部委託を加えた五つの点について、具体的な対応のポイントをお話しします。個人情報の定義の明確化についてですが、まずここでは定義の明確化に加えて、漏えい事案等への対応に係る法改正前後における変更点についてもお話ししたいと思います。

まず、個人情報の定義に関してですが、改正前の個人情報においては、資料10頁にあるように、「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により、特定の個人を識別することができるものと定義されていました。いわゆる特定個人識別可能性のあるものが、個人情報に該当するものとされていたということです。そして、この特定個人識別可能性のある情報には、他の情報と容

易に照合することができ、それによって特定の個人を識別することができることとなるもの、いわゆる容易照合性のあるものを含むとされていました。

改正法では、この個人情報の概念の基本構造は変更されていませんが、「個人識別符号」という新たな概念が導入されています。改正後の条文の構造から明らかなとおり、個人識別符号は特定個人識別可能性や容易照合性とは関係なく、ある情報が個人識別符号に該当すればそれのみで個人情報に該当するという関係にあります。逆に言うと、個人識別符号に該当しない情報だから個人情報に該当しないというわけではなく、特定個人識別可能性、容易照合性があれば、そのような情報も従来どおり個人情報に該当することになります。

このように、個人識別符号は、それに該当するとそれのみで個人情報に該当することとなりますので、改正法の施行に当たっては、個人識別符号に該当するものを個人情報として取り扱っているかどうかをチェックする必要があったものと思います。

もっとも、個人識別符号に該当するものは資料11頁に記載のとおりですが、個人識別符号として新たに個人情報の概念に加わった情報に関しては、改正前においても、これらを単独で取得・利用するというよりは、それ以外の個人を識別することができる情報、すなわち、氏名、住所などと一緒に取得・利用していたものと思います。そうすると、これらは従来から個人情報に該当するものとして取り扱われていたものと思います。したがって、個人識別符号という概念が新たに導入されたことによって、改正法施行の際には、念のための確認作業は必要であったものの、多くの個人情報取扱事業者において実務を変更する必要はなかったものと思います。

個人情報概念に関しては、もう１点、今回の改正に際して明確になった点があります。それは、個人情報の一部を取り出した情報が第三者に提供される場合、当該情報の特定個人識別可能性と容易照合性については、提供元、提供先のいずれを基準にして判断するかという点です。例えば顧客の住所、氏名、顧客番号と、顧客の購買履歴という情報を保有する個人情報取扱事業者があり、そのうち顧客番号と購買履歴のみを取り出して第三者へ提供することを想定するとします。この場合、提供元では顧客番号をキーにして、顧客の住所、氏名等の特定個人を識別することができる情報と結びつけることができます。一方、提供を受けた先では、顧客の情報は顧客番号と購買履歴しかありませんので、通常、この情報だけでは特定の個人を識別することはできないと思います。このような情報の提供が個人データの提供に該当するのかどうか。仮に意図せずして、これらの情報が漏えいしてしまった場合、それは個人データの漏えいに該当するのかどうか。あるいは、顧客番号と購買履歴のみを取り出し、それを分析のために第三者へ提供して、第三者からその分析結果のレポートを受け取る場合に、個人データの取扱いの委託に当たるのかどうか。改正前においては、そういったことが必ずしも明確ではなかったと思います。

この点については、資料12頁に記載した通則パブコメによれば、個人情報の提供に際しての個人情報該当性については、提供元で判断することが明確にされています。したがって、提供元で特定個人識別可能性、容易照合性が認められ、個人情報に該当するような情報を第三者に提供した場合、提供先において

は特定個人識別可能性、容易照合性が否定されたとしても、個人情報の提供に当たることになります。このように考えると、個人情報を非個人情報化して第三者に提供する方法は、匿名加工情報のかたちにして提供する方法に限られることになります。

また、先ほどの例のように、顧客番号と購買履歴のみの情報を委託先に提供して分析してもらう場合においても、個人データの取扱いの委託に該当することになりますので、個人データの取扱いの委託としての安全管理措置を講じることが必要になるものと思います。

このような、提供先においては、特定個人識別可能性、容易照合性がないようなデータが意図せず漏えいした場合であっても、提供元においては特定個人識別可能性、容易照合性が認められる以上、形式的には個人データの漏えいに該当することになると思います。

次に、どのような場合に個人情報の漏えい等として本人通知や金融庁への報告等の対応が必要となるかについて見ていきたいと思います。資料13頁をご覧下さい。ご存じのとおり、金融分野の個人情報取扱事業者において個人情報等の漏えい事案等が発生した場合には、雇用管理情報や株主情報などを除き、個人情報保護委員会の告示ではなく、金融ガイドラインと実務指針に基づいて対応することになっています。また、報告先も個人情報保護委員会ではなく、金融庁、財務局または地方公共団体となっています。

なお、個人番号を含む特定個人情報の漏えい等については、他の個人情報とは異なる取扱いが定められていますが、本日は時間の関係上、特定個人情報に関しては割愛します。

資料13頁にあるとおり、実務指針2-6-1では、個人データの漏えい等の事案が発生した場合には、「監督当局等への報告」、「本人への通知等」、「二次被害の防止・類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表」の三つの対応が求められています。この個人データに関する漏えい事案等への対応についての実務指針の規定は義務規定になっています。一方、個人データに該当しない個人情報の漏えいについては、金融ガイドライン第17条によって報告が求められていますが、こちらは努力義務となっています。なお、雇用管理情報と株主情報に関しては、金融ガイドラインではなく個人情報保護委員会が公表している「個人データの漏えい等の事案が発生した場合等の対応について」という告示によることになりますが、こちらでは個人データの漏えい等についても報告は努力義務となっています。

資料14頁をご覧下さい。「個人データ」と「個人データに該当しない個人情報」の違いについてです。この点はすでにご存じのことと思いますので、詳しい説明は省略しますが、法人情報のデータベースの中にある法人代表者の氏名等の情報が個人データに該当するかについて、金融機関 Q&A の問Ⅱ-6で資料14頁にあるような回答がなされています。この記載内容は、個人データの考え方の整理に非常に役立つ内容であると思います。個人情報保護法や各種ガイドラインにおいては、個人データと個人データ以外の個人情報の取扱いについては規制が異なります。しかし、金融機関においては、顧客情報について個人データか個人データ以外の個人情報かを細かく区別することなく、顧客情報として同様の取扱いがされていることが多いと思います。もっとも、漏えい等対応に関しては、先ほどの法人

の代表者の情報のように、個人データか個人データ以外の個人情報かを見極め、異なる取扱いをしている事業者もあるようです。

話を戻します。資料15頁をご覧下さい。実務指針では個人データの漏えい等について、監督当局への報告、本人通知が義務付けられていますが、FAXの誤送信、郵便物の誤送付、メールの誤送信などについては、一定の場合には、四半期に１回まとめて報告を行えばよいことになっています。また、郵便誤配など他責による事案に関しては、原則として報告不要とされています。今回の改正法の施行に際し、この点は実務が大きく変わった点であると思います。また、報告の頻度に関しても、改正法の前後において、月次から四半期ベースに変更され、実務の対応が軽減されているものと思います。

郵便誤配など他責による事案ですが、これもすべてにおいて報告不要とされているわけではなく、「本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さい」と言えない場合には、報告が必要となります。したがって、誤配されたものについて、何らかの理由で回収ができない、あるいは回収できたものの、誤配された郵便物に重要な情報が含まれており、開封されてしまっているなどといった場合には、報告を行ったほうがよい場合もあると思います。そういう意味で、金融分野の個人情報取扱事業者においては、郵便誤配の場合であっても、社内では報告を求めたうえで、漏えい事案等への対応をされる部署において個別の事案ごとに報告が必要であるかどうかを判断することが必要になるものと思います。

また、FAXの誤送信、郵便物の誤送付、メールの誤送信などについては、一定の場合には、四半期に１回まとめて報告を行うことができるようになっているものの、これも個人情報取扱事業者が個別の事案ごとに、漏えい等した情報の量、機微情報の有無、二次被害や類似事案の発生の可能性等を検討し、直ちに報告を行う必要性について判断をした上で、報告を行うことが必要となっています。したがって、この点についても、各事業者において漏えいした情報の件数や漏えいした情報の内容に鑑みたレピュテーションリスクの大きさなども考慮した上で、四半期報告でよいものと、都度報告すべきものとを見極めることが必要になるものと思います。

そのほか、先ほどお話ししたとおり、皆さま方の会社は、信託協会をはじめ、複数の認定個人情報保護団体の対象事業者になっているものと思います。各認定個人情報保護団体の定める保護指針においては、個人データの漏えい事案等については監督当局とともに、所属する個人情報保護団体への報告を求めています。報告の基準については、信託協会であれば、「信託協会　漏えい事案等報告基準」が定められています。この報告基準によると、郵便誤配など他責の事案については、当局報告を行う事案を除き、報告を要しないとされています。また、FAXの誤送信、郵便物の誤送付、メールの誤送信については、機微情報や特定個人情報等が含まれている場合、あるいは漏えい事案等における個人情報等の本人の数が10名以上である場合等、一定の場合を除き、回収や削除が確認できている場合には報告を要しないことになっています。

資料16頁は、当局への報告基準と信託協会への報告基準を私がまとめたものですが、この基準を見る限り、協会への報告を要する範囲は、監督当局に報告するものより若干狭い

と見受けられます。もっとも、金融機関によっては、当局に報告すべき事案と、認定個人情報保護団体に報告すべき事案を分けることなく、認定個人情報保護団体の指針の対象外とされている業務に関するものを除き、監督当局へ報告する事案についてはすべて認定個人情報保護団体にも報告を行うという対応を行っているところもあるようです。

信託兼営金融機関については、全国銀行個人情報保護協議会、日本証券業協会、日本投資顧問業会、日本クレジットカード協会等、複数の認定個人情報保護団体の対象事業者となっていると思われますので、それぞれの認定個人情報保護団体が定める基準にしたがった報告が必要になります。

また、年金関連業務を取り扱う事業者においては、私的年金分野における個人情報の漏えい等については、従来どおり、厚生労働省地方厚生（支）局への報告が必要とされていることに注意が必要です。

資料17頁をご覧ください。個人データの漏えい事案等については、原則として当局への報告とともに本人通知を要することになりますが、金融機関 Q&A 問Ⅳ-17においては、高度な安全化処理等が施されている場合や、即時に回収できた場合等、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない、または極めて小さい場合等については、本人への通知の省略も可能とされています。

先ほどの提供元基準によれば、提供元においては個人データに該当するものの、提供先においては特定個人識別可能性、容易照合性がない情報が漏えいした場合については、基本的に、この権利利益の侵害の可能性がない場合に該当するものとして本人通知は行わないという対応も考えられます。

資料の18頁をご覧ください。金融分野の個人情報取扱事業者であっても、株主や従業者の個人情報の漏えい事案等については個人情報保護委員会の告示によることとなりますが、個人情報保護委員会の告示では、個人データの漏えいであっても個人情報保護委員会への報告や本人通知は努力義務とされています。また、報告については、実質的に個人データが外部に漏えいしていないと判断される場合や、FAX もしくはメールの誤送信または荷物の誤配などのうち軽微なものである場合には報告不要とされています。

資料18頁に記載したとおり、個人情報保護委員会の告示では、どのようなケースが実質的に個人データ等が外部に漏えいしていないと判断される場合に該当するのか等に関する具体例が広範に記載されています。そのため、金融分野における個人データの漏えい事案等における本人通知の要否などを判断するに当たっても、この記載の内容は参考になるものと思います。

資料19頁は、改正法の施行以降に公表された金融機関の個人情報の漏えい事案等を私がまとめたものです。実務指針では、個人データの漏えいに係る公表は、二次被害の防止、類似事案の発生回避等の観点から行うべきものとされていますが、実際にどのような事案について公表を行うかについては、各社それぞれの基準で判断されているものと思われます。

3.　要配慮個人情報概念の導入への対応

先ほど申し上げましたとおり、要配慮個人情報については、金融分野の個人情報取扱事

業者が最も対応に苦慮された点であると思います。金融ガイドラインでは改正法施行前から、努力義務として、機微情報については、例外的な場合を除き、本人同意の有無に関わらず、取得・利用、第三者提供を行わないものとされていました。また、実務指針においては、機微情報に該当するものについては、取扱者を限定するなど、他の個人情報とは異なる取扱いが求められていましたので、金融機関においては、これにしたがって機微情報について厳重な管理をされてきたものと思います。

改正法では「要配慮個人情報」という概念が新たに設けられました。要配慮個人情報については、取得には原則として本人の同意が必要とされ、またオプトアウトに基づく第三者提供は禁止されています。一方、機微情報については、金融ガイドラインにおいてその概念等が一部変更されたものの基本的には規制が維持されています。機微情報は要配慮個人情報を含む、より広い概念と整理されています。これにより、金融機関においては、機微情報のうち要配慮個人情報については改正法の規制にしたがうとともに、要配慮個人情報を含む機微情報については従来どおり金融ガイドラインの規制にしたがうことが必要となっています。

資料21頁では、要配慮個人情報と機微情報の関係について、金融機関 Q&A 問Ⅲ-1に記載されている内容を紹介しています。これをご覧いただくとお分かりになるように、要配慮個人情報と機微情報の関係は四つのカテゴリーに分けられます。一つ目が、従来の金融ガイドラインにおける機微情報と要配慮個人情報の範囲が重なるもの（①）、二つ目が、従来の機微情報の範囲が要配慮個人情報より広いもの（②）、三つ目が、要配慮個人情報にのみ該当するもの（③）、四つ目が、従来の機微情報にのみ該当するもの（④）です。これらのうち、今回の改正で対応が必要になったのは、②と③に該当するものです。③については、新たに要配慮個人情報になったものですが、社会的身分、犯罪により害を被った事実、刑事事件に関する手続、少年の保護事件に関する手続にかかる情報がこれに該当します。犯罪により害を被った事実としては、金融機関であれば、例えば振込め詐欺被害に遭った事実が該当します。また、刑事事件に関する手続については、交通事故を起こして書類送検された事実などが該当します。

要配慮個人情報については、通則パブコメなどにおいて、推知情報や真偽不明な情報は要配慮個人情報には該当しないとされています。例えば第三者からの伝聞として、「Ｂの父は○○病らしい。」と聞いた場合など、真偽が不明である場合、その情報は要配慮個人情報には当たらないものとされています。また、勤務先が特定の宗教団体や政治団体であるような場合、そのこと自体はその人の信教や政治的な思想を推知させるものの、確定的な情報ではないので、要配慮個人情報には該当しないと整理されています。そのため、ある情報がある時点までは推知情報や真偽不明な情報であったとしても、ある時点からは要配慮個人情報に該当することがあります。例えばある人がわき見運転で交通事故を起こしてしまったという情報に関しては、やがて刑事事件に発展する可能性はあるものの、その時点においては要配慮個人情報ではないと思います。一方、これに立件されたという情報が加わると、要配慮個人情報に該当します。このように情報の確度や段階により、要配慮

個人情報に該当するか否かが異なってくることがあります。そうすると、ある段階までは要配慮個人情報ではないが、ある段階から要配慮個人情報として取扱うという対応をしなければならなくなり、そのようなことをするのであれば、最初から要配慮個人情報と同様に取り扱ったほうが対応としては楽であるということで、幅広に取り扱っている金融機関もあると思います。

このように、新たに加わった③に該当するものについては、実務の取扱いの変更が必要になりますが、それ以外に②についても通則パブコメ等によって、従来は機微情報に該当すると考えられていなかったような情報が、保健医療に係る機微情報の範囲に含まれることが明らかになり、実務への影響が大きかったものと思います。例えば障害者手帳の身体障害の等級に関する情報を取得した場合には、当然に機微情報に該当します。しかしながら、犯罪収益移転防止法に基づく取引時確認において、本人確認に障害者手帳を利用した場合、そのこと自体は機微情報には該当しないと考えていた金融機関も多かったのではないかと思います。

また、金融機関においては、顧客本人に書いてもらうべき書類について、顧客が目や手が不自由であるために代筆をする場合、金融庁の監督指針などに基づいて、その書類には「ご本人は手が不自由であるため、○○が代筆」など、代筆の理由を記載する手続になっていると思います。このような場合に、代筆の理由として記載された「手が不自由である」などという記載を、機微情報に該当するものとして扱っていなかった金融機関も多いのではないかと思います。

しかしながら、資料22頁で掲げた通則パブコメでは、障害者手帳を所持しているという事実自体が要配慮個人情報に該当するものとされています。また、「手が不自由」、「目が不自由」という記載自体も要配慮個人情報に該当するということが明確にされています。さらには資料21頁にあるように、医師等の診察によらず、自己判断により市販薬を服用しているという事実については、要配慮個人情報には該当しないものの、保健医療に関する情報として、機微情報に含まれるとされています。

このように、改正法の施行に際して、従来、保健医療に関する情報として機微情報に該当するものと考えられていたものよりも広い範囲の情報が機微情報に含まれることが明らかになっています。

このような情報は、日々業務を遂行する中で金融機関が通常取得しているもので、営業日誌に記載したり、あるいは通話録音の中に含まれていたりということがあると思います。そして、これらが機微情報に該当することとなると、実務上の取扱いや対応の変更が必要となってきます。

資料23頁をご覧ください。要配慮個人情報に該当し、かつ機微情報に該当するということになった場合、金融機関ガイドライン第５条にしたがうことが必要になります。また、改正法第17条第２項の例外に該当しない限り、取得には本人同意が必要になります。

金融ガイドラインとの関係では、金融機関が一般に取得している機微情報の多くは、第５条第１項⑦の「保険業その他金融分野の事業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供する場合」に該当するものと思い

ます。

また、本人の同意については、通則ガイドライン3-2-2において、「書面又は口頭等により本人から適正に直接取得する場合は、本人が当該情報を提供したことをもって、当該個人情報取扱事業者が当該情報を取得することについて本人の同意があったものと解される」こととされています。

さらには、本人を目視し、または撮影することにより、その外形上明らかな要配慮個人情報は、政令で「要配慮個人情報を本人の同意なく取得することができる場合」に該当するとされているとともに、金融ガイドラインの機微情報との関係でも、機微情報から除外されるものとされています。したがって、これまで金融機関において取得されてきた情報で、新たに要配慮個人情報や機微情報に該当するものとされた情報の取得、利用そのものに関しては、本人同意や金融ガイドライン第５条との関係で、基本的にその取扱いが問題となることはないものと思います。一方、実務指針においては機微情報については取扱者を限定するなど、他の個人情報より慎重な取扱いが求められています。

資料24頁をご覧ください。例えば、実務指針（別添２）の「金融分野における個人情報保護ガイドライン第５条に定められている「機微情報」の取扱いについて」では、取得、入力、利用、保管、保存、移送、送信、消去、廃棄という各段階において、必要最小限のものに限定したアクセス権限の設定、およびアクセス制御の実施が求められています。これを受けて金融機関では、従前より機微情報の保管を役席者に限定するなど、限定した取扱いをしていたものと思います。しかしながら、今回、障害者手帳で本人確認を行ったことまでが機微情報に含まれることになったことで、従来の機微情報と同じレベルでこれらの情報を取り扱おうとすると、障害者手帳が本人確認書類であった場合には、その本人確認記録については機微情報として役席者が保管しなければならないといったことが生じることとなるため、実務上の取扱いに悩んだ金融機関も多かったと思います。

ご存じのとおり、金融ガイドラインにおいては、「…しなければならない」とされているものは義務規定です。一方、「…することとする」などは努力義務であるとされています。金融ガイドライン第５条の規定も機微情報の取扱いに関しては努力規定になっています。また、実務指針では、安全管理措置に関する部分は義務規定であるものの、機微情報に関する別添２の部分に関しては一部の例外を除き努力規定となっています。もっとも、監督機関が定めたガイドラインである以上、金融機関においては、努力規定、努力措置とされているものであっても遵守しなければならないと考えて対応されているものと思います。

実務指針別添２では、機微情報の取扱いに関する安全管理措置として、取扱者を必要最小限に限定することなどを求めていますが、情報の内容や利用の対応に合わせて、必要最小限の範囲は変わり得るものと思います。したがって、障害者手帳を本人確認書類として取得し、その後の取引においても利用するような場合には、必要に応じて、支店の担当者全員を取扱者にするなど、臨機応変に取扱い規則を変更するという対応もあり得ると思います。

改正法施行の時点において、このような対応をされていない金融機関においても、今後、リスクベースの対応を考える中で、このよう

な観点から見直しを行うことも考えられるものと思います。

4. 個人データの提供にかかる確認・記録義務への対応

それでは、確認・記録義務への対応、外国にある第三者への提供への対応、外部委託の見直しについて冨松からご説明します。なお、本項目以下では、「金融分野の個人情報取扱事業者」を単に「金融機関」などと言うことがあります。

資料の26頁をご覧ください。改正法における確認・記録義務の内容については、すでにご承知のことと思いますので、簡単な説明のみにさせていただきます。先ほども説明がありましたが、ベネッセ事件をきっかけとして、名簿業者の暗躍が広く世の中に知れ渡りました。こうして自分の個人情報が知らないところで流通することについて国民の不安が大きくなったことから、情報の流通経路を追跡できるようにすることが必要と考えられるようになりました。確認・記録義務に関する改正はこのような事情を背景に行われたものです。

具体的には、改正法では個人データの提供側および受領側の双方に、個人データの授受に関する年月日、相手方の氏名または名称、当該個人データの内容等の記録義務を課し、また記録義務を果たした結果として生じる記録の保存義務を課しました。また、受領側には記録義務の前提として確認義務を課しています。根拠条文は、提供者側の記録義務が第25条、受領者側の確認義務が第26条です。

まず、提供者側の記録義務について確認すると、本人の同意を得て行う第三者提供とオプトアウトによる第三者提供では、記録すべき内容に違いがあります。資料27頁をご覧いただき、不要な部分がどこかをご確認いただければと思います。

オプトアウトの場合には、本人の同意を得ているわけではありませんので、「本人の同意を得ている旨」の欄は「不要」になります。本人の同意を得て提供する場合には、「提供年月日」が必須ではないこととされています。もちろん年月日についても、自主的に記録を残すことは問題ありません。

次に、受領者側の記録義務について確認すると、本人の同意を得て行う第三者提供、オプトアウトによる第三者提供、私人等から提供された個人データの受領で、それぞれ記録すべき内容に違いがあります。資料28頁をご覧いただき、提供者の記録義務と同様に、不要な部分がどこかを押さえていただければと思います。

なお、オプトアウトの場合に、「委員会による公表」に係る記録が必要とされているのは、法第23条第２項でオプトアウトを行う場合には個人情報保護委員会への届け出が必要であり、そのような届け出がなされた場合には、同条第４項により個人情報保護委員会から公表されることとなっているため、このような手続が適法に行われていることを確認するためのものです。このような記録を通じて、万一、個人情報の流出があった場合に、自分が誰に提供した情報が、どのような経路で流通したかを特定することができるようにするとともに、個人情報を扱う事業者に対しては刑事罰を科す規定が設けられ、個人情報の漏えいに対する抑止的効果を及ぼそうとしています。

他方、改正法施行前に改正法の詳しい内容

および実務対応に関するセミナーを行いましたところ、「金融機関においても、このような確認・記録義務を行うことが求められるのか」、「どのようなフォーマットに記録すればよいか」、「一括記録する場合には、どのような頻度で行えばよいか」など、ご心配の声を多数いただきました。確認・記録義務は金融機関等の実務における工数を増やすとともに、マニュアル等を整備して事前に準備を行うことが必要となるため、その影響について非常に懸念されているようでした。

そこで、次に、改正法が施行された現在、金融機関がどのように確認・記録義務に対応されているのか、またその根拠は何かという点についてお話しします。結論から先に申し上げると、金融機関において、現在、日常的な業務の中で確認・記録義務の履行として、従前とは異なる書類を作成しているところは少ないと思われます。その理由としては、まず個人情報保護委員会がこのような実務上の懸念を、パブリックコメント手続等を通じて把握し、確認・記録義務の範囲を限定的に解釈していることが挙げられます。改正法の内容は影響力が大きいわりに、規定としては極めてシンプルであり、解釈の幅があるように思います。個人情報保護委員会はこのような曖昧さを４種の基本ガイドラインと業務分野ごとのガイドライン、パブリックコメント手続における回答、Q&A 等で補うように努力しています。そして、この確認・記録義務についても、第三者ガイドラインやパブリックコメント手続における回答において、法律上の例外に加えて、解釈上、確認・記録義務の適用を受けない例外的な場合を細かく例示し、その範囲が不用意に拡大することを防止しています。

資料29頁をご覧ください。法律上の例外としては、まず「法令に基づく場合」、「人の生命、身体、又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき」等、法第23条第１項に定める場合が挙げられます。また、委託、共同利用、合併等の事業承継という法第23条第５項に定める場合や、個人データを提供する第三者が法第２条第５項各号の「国の機関」や「地方公共団体」などである場合にも、確認・記録義務は生じません。

そして、解釈上の例外としては、資料30頁に記載している四つの場合が挙げられます。例えば、個人情報を「本人に代わって」提供する場合については、実質的に見れば本人による提供であり、「提供者」による提供ではないと整理され、確認・記録義務を履行する必要はないものとされました。本人から別の者の口座へ振込依頼を受けた仕向銀行が、振込先の口座を有する被仕向銀行に対し、当該振込依頼に係る情報を提供する場合が、このような場合に該当します。これは、第三者ガイドラインに関する意見募集結果（パブリックコメント）の843番に記載があります。

このほか、金融機関の営業員が家族とともに来店した顧客に対し、保有金融商品の損益情報等を説明する場合には、顧客の家族は「受領者」に該当せず、また、ホームページ等で公表されている情報の提供のような不特定多数の者が取得可能な公開情報の提供については、「提供」に該当しないことから、例外的に確認・記録義務はないこととされています。

もっとも、確認・記録義務がないことと、本人の同意が不要ということは別の問題なので、注意が必要です。このような解釈上の例外は、確認・記録義務が正常な事業活動を行

っている事業者に対する過度な負担となることを避けるため、現実的な規制のあり方として示したものとされており、適用場面が限られていることに注意いただきたいと思います。

また、このような例外要件による整理のほか、従来から金融機関が顧客より徴収している「個人情報の取扱いに関する同意書」等の書面により、記録に代替していることも考えられます。

このように、金融機関においては、確認・記録義務がないということではなく、例外要件に照らして不要と判断されたり、他の書面で代替可能と整理しているに過ぎず、イレギュラーな事態が生じた際には確認・記録義務の履行の要否を検討する必要があるため、注意が必要です。

5. 外国にある第三者への提供への対応

次に、外国にある第三者への提供に関する実務対応について説明させていただきます。資料33頁をご覧ください。旧法においては、外国にある第三者への個人データの提供や、外国にある第三者に関する日本の個人情報保護法の適用に関する規定は設けられていませんでした。

しかし、経済のグローバル化や電子商取引が進展するとともに、国外に拠点を有しながら、日本向けに商品・役務の提供を行い、その際に日本の居住者等に係る個人情報を取得する事業者が増加しています。

また、先進国を中心に、世界中で高速通信網が整備されるとともに、コンピュータ等の性能も高度化している昨今では、大量の情報が瞬時に、そして国境を越えて流通することが可能となっています。さらに、その流通手段も、従来から存在した電子メール等に加え、SNS、大容量データ送信サービス、クラウド等、多様化し、また手軽になっています。

こうした情報通信技術の発達は、その副作用として、本来流通すべきではない情報をも容易に流通させてしまうという状況を生んでいます。個人情報もまさに「本来、流通すべきではない情報」であり、これを実効的に取り締まる目的で、改正法により新たな規制が置かれました。

具体的には、第１に、域外適用と呼ばれるものです。資料34頁をご覧ください。先ほど述べたように、国外に拠点を有しながら日本向けに商品・サービスの提供を行い、日本の居住者等に係る個人情報を取得する事業者が増加しています。よって、国内だけ規制を強化しても十分とは言えない状況にあります。外国に拠点がある者についても、国内事業者と同様に規制が及ぶものとすべきです。そこで、一部の規定を除き、外国の事業者についても、国内事業者とほぼ同様の規律を及ぼしています。

しかし、法の域外適用は、「法の地理的な適用範囲は自国領域内に限定される」という属地主義の原則の例外です。したがって、外国の事業者と日本との間に特別の関連性があることや、法の適用を及ぼす必要性・合理性が認められる必要があります。そのため、法の域外適用の対象事業者は、国内にある者に対する物品または役務の提供に関連して、その者を本人とする個人情報を取得した個人情報取扱事業者に限定されています。

第２に、外国執行当局との協力が挙げられます。外国の事業者に関しても個人情報保護委員会の指導、助言、勧告等の規定は適用さ

れるものの、処分性を有する報告、立入検査、是正命令等は外国の国家主権との抵触が問題となるため適用されません。そのため、日本国内の本人の権利利益を保護するために、外国執行当局の協力を必要とする場面があることから規定が設けられたものです。

資料35頁をご覧下さい。第３に、外国にある第三者への個人データの提供に関する規定です。改正法は、個人データが外国へ転出する段階でのコントロールを強化すべく、外国にある第三者に個人データを提供する場合には、事業者は原則として、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならないとしました（法第24条）。これも従来にない規制ですから、これまで外国にある第三者に情報提供をしていた場合、例えば海外でコールセンターが運営されている場合等について、金融機関を含む国内の事業者では新たな対応が必要となります。

もっとも、この規制についても例外があります。第１に、法第23条第１項各号に掲げる場合です。これは法令に基づく場合等の、国内事業者が、国内の第三者に個人データを提供する際に、例外的に本人同意が不要となる場合を定めたものです。国内にある第三者への提供に際して本人同意が不要となるので、外国にある第三者に対する提供に際しても本人同意が不要というのは理解がしやすいと思います。なお、法第23条第１項各号については、国内にある第三者と同様に規律されていますが、同条第５項の外部委託等については、国内にある外部委託先（第三者）への提供の際に本人同意が不要であるのと異なり、外国にある外部委託先（第三者）への提供の際には原則として本人同意が必要となるため、注意が必要です。

第２に、「外国」が「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるもの」である場合です。具体的な国は個人情報保護委員会の告示で指定されることになっていますが、現時点において、その指定はまだされていません。なお、指定対象としては、アメリカやEU加盟国が想定されていると言われています。

第３に、「第三者」が「個人データの取扱いについて、この節（法「第４章　個人情報取扱事業者の義務等」の「第１節」）の規定により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を継続的に講ずるために必要なものとして、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者」である場合です。つまり、国外にある第三者自身がきちんとした個人情報保護のための管理体制を敷いている場合です。

それでは、次に、実務ではどのような整理をしているかを確認していきたいと思います。

実務上の対応としては、原則どおり、外国にある第三者への提供に際して本人同意を取得する方法と、例外要件に該当すると整理する方法の二つが考えられます。

資料の36頁をご覧ください。先ほど説明した三つの例外のうち、法令に基づく場合等の法第23条第１項各号に該当する場合は、国内にある第三者への提供と同様のものです。

また、「個人の権利利益を保護する上で、我が国と同等の水準にあると認められる個人情報保護に関する制度を有している外国」についても、その細かい要件について、昨年12月に委員会規則案が公表されパブリックコメント手続に付されていますが、具体的な国名

を指定する告示はまだされていません。

さらに言うと、例えばコールセンターの外注先等は個人情報保護体制を整備しているような先進国ではない場合が多いように思われますので、このような例外要件に該当することにより、全く対応不要と整理することは難しいように思われます。

そうすると、３番目の例外要件に基づき、本人同意が不要と整理することができるかどうかを検討することとなります。

資料の37頁をご覧ください。この点、委員会規則第11条第１号は、その具体化として「個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第４章第１節の規定の趣旨に沿った措置の実施が確保されていること」と定めています。この「適切かつ合理的な方法」は個々の事例ごとに判断されるべきものですが、個人データの提供先である外国にある第三者が、我が国の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を継続的に講ずることを担保することができる方法であることが必要とされています。そして、そのような方法の具体例として、外国にある事業者に個人データの取扱いを委託する場合には提供元と提供先との間の契約書等、同一企業グループの内部で個人情報を移転する場合には提供元と提供先に共通して適用される内規やプライバシーポリシー等が挙げられます。

資料の38頁をご覧ください。先ほどの「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者」という要件の具体化として、規則第11条第２号は「個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること」と定めています。外国ガイドライン3-3によると、「『個人情報の取扱いに係る国際的な枠組みに基づく認定』とは、国際機関等において合意された規律に基づき権限のある認証機関等が認定するものをいい、当該枠組みは、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を継続的に講ずることのできるものであること」が必要であるとし、具体例として、その外国にある第三者がアジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）システムの認証を取得していることを挙げています。

資料の39頁をご覧ください。グループ会社等についてこの３番目の例外要件、中でも規則第11条第１号に該当するものとして整理されているところもあると思いますが、利用目的の通知や開示請求への対応に関する体制整備については負担感があるとの声も聞かれるところであり、例外要件に基づく整理は難しいとして、原則どおり本人の同意を得て提供するという整理が現実的だと判断されることもあるようです。

この点、確かに外国ガイドライン2-1によれば、外国にある第三者に個人データを提供する場合には、国内にある第三者に対する同意とは別に、外国にある第三者への提供について同意を取得しなければならないとされてはいるものの、個人情報の第三者提供に関する同意書をすでに用いている実務では、同意書における同意の対象として国内にある第三者のみならず、外国にある第三者を追加する方法も現実的な選択肢となっているようです。この場合、書面を改定すればよく、柔軟に対応できることがその理由のようです。

なお、この「外国」については、ある程度

明確にする必要があり、Q&A9-2、および外国パブコメ715では、この方法の具体例が挙げられています。資料39頁にも記載していますので、ご確認いただければと思います。

6. 外部委託の見直し

資料の41頁をご覧ください。続いて、外部委託についてです。改正法において法律の条文自体に変更はありませんでした。また、その具体的内容について、個人情報保護法の改正前においても、すでに金融ガイドラインや安全管理措置等についての実務指針の改正により、委託先管理の厳格化等の手当てがなされていました。

今般の個人情報保護法の改正においては、各種ガイドラインやQ&Aの追加・改定がなされていますが、その内容については、基本的には、金融ガイドラインや実務指針が先取りして行っていた改正内容に包含されるものと考えられます。そこで、金融ガイドラインの適用を受ける事業者にとっては、従前の実務について、新たな対応を迫られるものではないと評価することができると思います。

例えば、平成27年7月9日から適用された金融ガイドラインや実務指針の改正において、改正後の金融ガイドライン第12条では、委託先の選定に関して、「委託先の選定に当たっては、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行った上で、個人データ管理責任者等が適切に評価することが望ましい」という文言が追加されました。また、「委託先が再委託を行おうとする場合は、委託元は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法について、委託先に事前報告又は承認手続きを求める、直接又は委託先を通じて定期的に監査を実施する等により、委託先が再委託先に対して（中略）委託先の監督を適切に果たすこと、再委託先が法第20条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする」として、再委託以降の委託先管理にも、法第20条に基づく安全管理措置を講ずることを十分に確認することが望ましいとされていました。今回の個人情報保護法の改正と合わせて制定された通則ガイドラインでは、3-3-4において、基本的にこれらの内容が踏襲されています。

そして、「委託を受けた者に対して必要かつ適切な監督を行っていない事例」として、個人データの安全管理措置の状況を契約締結時およびそれ以後も適宜、把握せず、外部の事業者に委託した結果、委託先が個人データを漏えいした場合等、四つのケースが紹介されています。資料42頁にも記載していますので、ご確認いただければと思います。

なお、Q&Aにおいては、委託先管理と関連して、配送事業者、通信事業者、クラウドサービス提供者等の外部事業者を利用する場合に、個人データの取扱いを委託していると言えるかということについて、解説がされています。基本的な考え方としては、個人データの中身について当該外部事業者が関知しない場合には、個人データの取扱いの委託ではないと整理されています。もっとも、安全管理措置を講ずる義務の観点からは、これらの外部事業者の選択や安全な配送方法の指定等の措置を講ずる必要があるとされています。

なお、今般の改正に合わせ、金融ガイドラ

インや安全管理措置等についての実務指針も改定がなされ、通則ガイドラインと共通する規制についてはそちらに準拠するものと整理されました。そのため、今後は金融ガイドラインや実務指針と合わせ、４種の基本ガイドラインについても参照する必要があるため、注意が必要です。

この章のまとめですが、先ほど申し上げたとおり、今般の改正内容はすでに適用されている金融ガイドラインや安全管理措置等についての実務指針の改正に沿ったものであり、金融機関等における委託先管理については、これらに準拠して厳重に行われているものと考えられます。したがって、改正法の施行により、具体的に契約書の文言を修正する等の対応が必要になる場合は多くないように思われます。

7.　今後の課題・見直しのポイント等

資料の45頁をご覧ください。これまで改正法の概要とともに、改正前の事業者の皆様の反応に関する話を交えながら、改正後における実務の対応状況について解説してきました。結果として、改正法の施行によって金融機関等の事業者の実務において、改正前に不安視されていたような作業負担が大幅に増えるといった影響は、現時点においては特段生じていないものと思われます。

これは個人情報保護委員会から順次公表されたガイドライン等の内容に則り、どのように整理すれば現場の負担増を回避することができるかについて、全国銀行協会や信託協会等の業界団体が慎重に検討して、パブリックコメント手続等で改正法によって求められる対応範囲を的確に確認したことの一つの成果ではないかと思われます。

そして、今後の課題を挙げるとすれば２点あると思います。資料46頁をご覧ください。一つは要配慮個人情報の取扱いです。先ほど申し上げたように、要配慮個人情報の取扱いについては、実務上、保守的な運用がなされており、いわば過剰反応となっている部分があるように思われます。法令上求められている水準が事例の積み重ねとともに、より具体的に明らかになっていくことにより、現在の実務上の負担が適切な水準となるように調整が続けられるものと考えられます。

また、要配慮個人情報については、科学技術のさらなる発展とともに新たな問題も生じてくるため、そのような問題に対処していくことも課題になってくると思います。例えば業務上、サービス向上の目的等のために行っている通話録音について、現時点において検索性がないとして個人データとして扱っていない場合であっても、検索機能の技術の向上により、音声データの内容について直接検索可能となった場合には、新たに保有個人データとして管理が必要となります。その通話内容に通院の事実や身体障害がある等の事実が含まれている場合には、要配慮個人情報の取得ということになります。取得の際の本人の同意については、これらの通院の話や身体に障害があることが本人からの発話であれば、推定的同意があると整理できるようにも思われますが、要配慮個人情報として管理する必要が生じるため、当該通話内容に関する音声データについては、通常の通話内容の音声データよりも慎重に取扱う必要が出てきます。

また、近年目覚ましい進歩を遂げている AI（人工知能）のさらなる進化に伴い、識別可能性が高まることも考えられます。そうすると、

声紋鑑定等の専門的な鑑定によらずとも、通話の音声のみで特定個人が識別できたり、防犯カメラ画像から特定個人を自動識別する機能等も登場する可能性があります。そうした技術の進歩とその普及に伴い、新たに対応を検討する必要が生じることが予想されます。

二つ目は匿名加工情報です。資料の47頁をご覧ください。匿名加工情報は改正法の目玉の一つでありながら、改正法施行後約９か月たっても、まだその活用事例は多くないように思われます。その理由の一つには、加工基準に曖昧さが残るため、どの程度加工すれば匿名加工情報として認められるかが分かりにくく、他方で保守的に匿名化の程度を高度化すればするほど、利活用するためのデータとしての価値が低くなるというジレンマを抱えているからではないかと思います。

資料の48頁をご覧ください。金融機関では、イオン銀行が他に先駆けて匿名加工情報を作成した旨が公表されています。そこでは「性別、年代（５歳刻み）、居住する都道府県、郵便番号、職種、業種、世帯構成に関する情報、ご契約カード種類、店番号、口座開設経過月数、預金等の当行各種金融商品の取引状況および審査結果、現在および次回のポイントクラブステージ」という項目が設定されています。また、一般財団法人日本情報経済社会推進協会（JIPDEC）が匿名加工情報の事例集を公表しています。

もっとも、これらのすべてが法令上、要求される加工基準を確実に満たしている保証はありません。したがって、こういった事例は自己責任において参照する必要がありますが、このような事例の集積によって加工基準の概念が徐々に明らかになれば、ある時期から爆発的に匿名加工情報の利活用が増大する可能性もあると思います。

なお、医療分野については、平成29年５月12日にいわゆる医療ビッグデータ法が公布され、１年以内に施行されます。この法律においては、認定匿名加工医療情報作成事業者が認定され、医療分野の研究開発に資するための匿名加工医療情報を作成することとされています。こうした医療分野の匿名加工情報から、その利活用の価値が認知されて、他の分野での匿名加工情報の利活用が促進されることも十分考えられます。

今後の実務上の対応の見直しや新規事業の開発において大切なのは、個人情報の重要性について十分に理解しつつ、今後新たに生じる事態に法令遵守の観点から的確に対応し、他方でマーケティングや商品開発等のために個人情報が内包する有益な特徴を最大限に活かすことだと思います。

そのためにはプロアクティブに情報収集を行い、個人情報保護法の規制の外延を分析するとともに、新たな時代におけるデータ活用の方法を探求し、これを適時、的確に実行していくことが必要となると思われます。

ご清聴、ありがとうございました。

本稿は、平成30年２月26日に開催された信託セミナーにおける堀総合法律事務所弁護士髙木いづみ氏・冨松宏之氏の講演内容を取りまとめたものである。

（たかぎ・いづみ、とみまつ・ひろゆき）

1

改正個人情報保護法を踏まえた実務対応について

2018年2月26日
堀 総合法律事務所
弁護士　髙木いづみ
弁護士　冨松　宏之

2

本セミナーの構成

1. 改正個人情報保護法の主な変更点と対応のポイント
2. 個人情報の定義の明確化への対応と漏えい事案等への対応
3. 要配慮個人情報概念の導入への対応
4. 個人データの提供にかかる確認・記録義務への対応
5. 外国にある第三者への提供への対応
6. 外部委託の見直し
7. 今後の課題・見直しのポイント等

3

【凡 例】

略 称	正式名称等
個人情報保護法／法	個人情報の保護に関する法律（平成15年5月30日法律第57号）
改正法	「個人情報の保護に関する法律および行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律」（平成27年法律第65号）
改正	改正法に基づく改正
事業者	個人情報取扱事業者
政令	個人情報の保護に関する法律施行令
委員会規則／規則	個人情報の保護に関する法律施行規則
通則ガイドライン	個人情報の保護に関する法律についてのガイドライン（通則編）
外国ガイドライン	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）
第三者ガイドライン	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）
金融ガイドライン	金融分野における個人情報保護に関するガイドライン
実務指針	金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針
漏えい等対応	個人データの漏えい等の事案が発生した場合等の対応について
通則パブコメ	通則ガイドライン（案）に関する意見募集結果（平成28年11月30日）
外国パブコメ	外国提供ガイドライン（案）に関する意見募集結果（平成28年11月30日）
QA	「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するQ＆A
金融機関Q＆A	「金融機関における個人情報保護に関するQ＆A」
一問一答	瓜生和久編著「一問一答　平成27年改正個人情報保護法」

4

1．改正個人情報保護法の主な変更点と対応のポイント

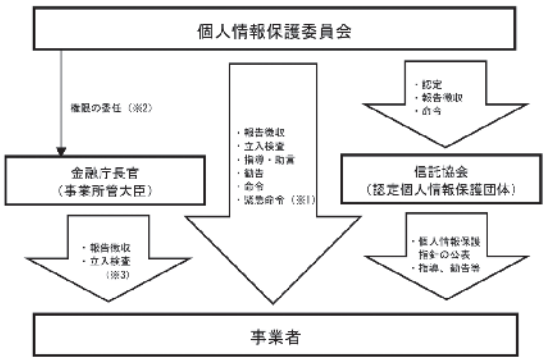
5

(1) 改正の背景と改正法のポイント

(1) パーソナルデータの利活用促進のためのグレーゾーンの解消
　⇒「個人識別符号」、「匿名加工情報」概念の新設
　　「要配慮個人情報」に関する規制の導入
(2) 事業者に対する一元的監督
　⇒「個人情報保護委員会」を新設し、監督権限を一元化
(3) いわゆる名簿業者に対する規制
　⇒個人データの第三者提供に係る確認・記録作成等を義務化
　　「個人情報データベース等提供罪」の新設
　　オプトアウトに関する個人情報取扱事業者の届出と個人情報保護委員会による公表
(4) データ流通のグローバル化に対する対応
　⇒外国にある第三者への個人データの提供の制限
　　個人情報保護法の域外適用

6

(2) 金融分野の個人情報取扱事業者に対する監督



※1　「勧告」を前提とする「命令」と異なり、「緊急命令」は法定の要件が充足されれば、直ちにこれを行うことができる。
※2　金融庁長官は、内閣総理大臣から委任された権限の一部を、財務局長等に再委任するものとされている。
※3　金融庁や財務局等には勧告・命令等の権限はなく、金融庁や財務局等が報告徴収や立入検査を行った場合は、その結果が委員会に報告され、それに基づき、委員会が勧告・命令等を行う。

7

金融分野における認定個人情報保護団体

対象事業分野	名　　称
信託業	一般社団法人信託協会
銀行業	全国銀行個人情報保護協議会
証券業	日本証券業協会
投資信託委託業及び投資法人資産運用業	一般社団法人投資信託協会
投資運用業及び投資助言・代理業	一般社団法人日本投資顧問業協会
金融先物取引業	一般社団法人金融先物取引業協会
全般	一般財団法人日本情報経済社会推進協会（JIPDEC）
クレジット事業	一般社団法人日本クレジット協会

8

(3) 金融分野の個人情報取扱事業者における改正個人情報保護法への対応のポイント

(1) 個人情報の定義の明確化への対応
- ✓「個人識別符号」に該当する情報の取扱状況の確認

(2) 要配慮個人情報規制への対応
- ✓「要配慮個人情報」に該当する情報の洗出しと実務対応の変更

(3) 個人データの提供・取得に際しての確認・記録義務への対応
- ✓ 個人データの提供・取得の場面の洗出しと新たな対応の要否の確認（実務の取扱いの変更）

(4) 外国にある第三者への個人データの提供
- ✓ 外国にある第三者への提供場面の洗出し
- ✓ 法4章1節の規定の趣旨に沿った措置の実施の確保又は同意取得の対応

9

2. 個人情報の定義の明確化への対応と漏えい事案等への対応

10

個人情報の定義

【改正前】（法2条）

この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（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こととなるものを含む。）をいう。

【改正後】

生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

一　当該情報に含まれる氏名、生年月日その他の記述等（略）により特定の個人を識別することができるもの（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こととなるものを含む。）

二　個人識別符号が含まれるもの

※特定個人識別可能性、容易照合性

11

(1) 個人識別符号(法2条1項1号)

①特定個人の身体的特徴を電子的に変換した符号
　DNA、虹彩の模様、手のひら・甲・指の静脈の形状、指紋又は掌紋等
②特定個人の身体的特徴に関係なく発行される符号
(ⅰ)サービスの利用・商品の購入に関してサービスの利用者・商品の購入者ごとに割り当てられる符号・・・政令なし
(ⅱ)それ以外の符号であって、個人に発行されるカード等に記載、記録される符号
　旅券番号、基礎年金番号、運転免許証番号、保険証の記号・番号、マイナンバー等

個人識別符号 ⇒ それのみで個人情報
個人識別符号に該当しない符号 ⇒ 特定個人識別可能性、容易照合性の有無を検討

12

(2) 提供元基準か提供先基準か　※通則パブコメ

No.	該当箇所		寄せられた御意見等	御意見等に対する考え方
19	2-1	個人情報	(該当箇所) 通則編　2　定義　2-1　個人情報（法第2条第1項関係） P.6　16行(＊4) (ご意見) 「他の情報と容易に照合することができ」るとは、事業者の実態に即して個々の事例ごとに判断されるべきであると解説されているが、容易照合性については提供先が有する情報等によると考えられる。従って、提供元では提供先で「個人情報」に該当するか否かが必ずしも判断できないことから、提供前に、提供元が提供先における容易照合性についてどのように配慮すべきかについて解説してほしい。 (理由) 提供先では、個人情報に該当しない情報を提供したと思っても、提供先で保有する情報と照合することにより、個人が特定される場合が想定されるため。 【日本製薬工業協会　研究開発委員会】	ある情報を第三者に提供する場合、当該情報が「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こととなる」かどうかは、当該情報の提供元である事業者において「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こととなる」かどうかで判断します。

13

(3) 金融分野の個人情報取扱事業者の漏えい事案等への対応

実務指針2-6-1(個人データ、義務)

漏えい事案等が発生した場合には、次に掲げる事項を実施しなければならない

①監督当局等への報告

②本人への通知等

③二次被害の防止・類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表

※個人データに該当しない個人情報については、金融ガイドライン17条(報告は努力義務)

※雇用管理情報、株主情報は「個人データの漏えい等の事案が発生した場合等の対応について」(平成29年個人情報保護委員会告示第1号)による(報告は努力義務)

14

「個人データ」と「個人データに該当しない個人情報」 ※金融機関Q&A

(問Ⅱ-6)法人の代表者の情報は「個人情報」に当たるか。また、法人情報のデータベースの中に法人代表者の氏名等があった場合、当該情報は「個人データ」に当たるのか。

(答)

法人の代表者の情報は、個人情報保護法第2条第1項の定義に該当するため、「個人情報」に当たります。取引先企業の担当者名といった情報も、同法第2条第1項の定義に該当するため、「個人情報」に当たります。

また、法人の代表者の氏名等が(単に文字列検索が可能なのではなく、個人情報としての属性に着目して)検索可能な場合には、当該データベースは「個人情報」が検索できるように体系的に構成されているといえ、「個人情報データベース等」に該当するものと考えられます。ただしデータベース等があくまで法人情報のみの検索が可能なように構成されているもので、(法人代表者等の)個人情報の検索が可能なように体系的に構成されていない場合には、当該データベース等は「個人情報データベース等」には該当せず、そこに含まれている個人情報も「個人データ」に該当しないこととなります。

15

漏えい事案等発生時の当局報告　※金融機関Q&A

（問Ⅳ-11） 個人情報等の漏えい事案等が発生した場合の監督当局等への報告は、どこまで厳密に行う必要があるのか。例えば、FAXの誤送信、郵便物等の誤送付及びメールの誤送信などによる個人情報等の漏えい等で、当該情報の量や性質等に鑑みて、漏えい事案等としては軽微と思われるものまで、発生段階で必ず監督当局等へ報告する必要性があるのか。

（答）

「個人データ」については、業務指針2-6-1において、漏えい事案等が発生した場合には、監督当局等への報告を実施しなければならないとされており（義務規定）、「個人データ」の漏えい事案等が発生した場合は、金融機関は、当局への報告を行う必要があります。

一方、「個人情報」及び「加工方法等情報」については、金融分野ガイドライン第17条において、「監督当局等に直ちに報告することとする」（努力規定）と規定されています。

ただし、FAXの誤送信、郵便物等の誤送付及びメール誤送信などについては、個人情報取扱事業者が個別の事案ごとに、漏えい等した情報の量、機微（センシティブ）情報の有無及び二次被害や類似事案の発生の可能性などを検討し直ちに報告を行う必要性が低いと判断したものであれば、業務上の手続きの簡素化を図る観点から、四半期に一回程度にまとめて報告しても差し支えありません。

このほか、郵便局員による誤配など、個人情報取扱事業者の責めに帰さない事案については、原則として報告を要しません。ただし、「本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さい」とはいえない場合については、上記の諸事情を検討したうえで、都度直ちに又は四半期に一回程度にまとめてご報告して頂く必要があります。

他方で、いかなる場合でも対外公表を行う場合は都度直ちにご報告していただく必要があります。

16

個人データの漏えい事案等の報告の要否及び方法

<table>
<tr><th>具体例</th><th colspan="3">監督当局への報告</th><th colspan="3">信託協会への報告</th></tr>
<tr><td>原則</td><td colspan="3">都度直ちに報告</td><td colspan="3">都度直ちに報告</td></tr>
<tr><td rowspan="3">FAX誤送信、郵便物等の誤送付、メール誤送信など</td><td rowspan="2">個人情報取扱事業者が個別の事案ごとに、漏えい等した情報の量、機微情報の有無及び二次被害や類似事案の発生の可能性などを検討のうえ</td><td>直ちに報告を行う必要性が低いと判断したもの
⇒四半期に1回程度にまとめて報告可能</td><td></td><td>(1)誤送信等の先及びその内容等が確認され、回収・削除済みである等により誤送信等の先からの漏えい及び二次被害の発生の可能性が極めて低いもの
(2)誤廃棄・紛失で、社外で紛失等したものではなく、社内（委託先含む）での誤廃棄である可能性が極めて高い等により二次被害の発生の可能性が極めて低いこと</td><td>原則報告不要</td><td></td></tr>
<tr><td>直ちに報告を行う必要性が低いとはいえないと判断したもの
⇒都度直ちに報告</td><td></td><td>上記(1)、(2)に該当するもののうち以下のいずれかに該当する場合
①個人番号、特定個人情報、機微情報又は個人信用情報に係る漏えい事案等の場合
②漏えい事案等における個人情報等の本人の数が10名以上である場合
③本人から信託協会へ漏えい事案等にかかる苦情・相談の申し出がある場合
④二次被害が発生した漏えい事案等の場合
⑤漏えい事案等の事実関係を公表する場合</td><td>事案の内容等に応じて、直ちに報告を行う必要性が低いと判断したもの
⇒四半期に1回程度にまとめて報告可能</td><td></td></tr>
<tr><td></td><td></td><td></td><td>事案の内容等に応じて、直ちに報告を行う必要性が低いとはいえないと判断したもの
⇒都度直ちに報告</td><td></td></tr>
<tr><td rowspan="3">郵便局員による誤配など（他責）</td><td>原則</td><td>報告不要</td><td></td><td>原則</td><td>報告不要</td><td></td></tr>
<tr><td>本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいとはいえない場合</td><td>個人情報取扱事業者が個別の事案ごとに、漏えい等した情報の量、機微情報の有無及び二次被害や類似事案の発生の可能性などを検討のうえ</td><td>直ちに報告を行う必要性が低いと判断したもの
⇒四半期に1回程度にまとめて報告可能</td><td rowspan="2">監督当局に報告を行う場合</td><td rowspan="2">個人情報取扱事業者が個別の事案ごとに、漏えい等した情報の量、機微情報の有無及び二次被害や類似事案の発生の可能性などを検討のうえ</td><td>直ちに報告を行う必要性が低いと判断したもの
⇒四半期に1回程度にまとめて報告可能</td></tr>
<tr><td>直ちに報告を行う必要性が低いとはいえないと判断したもの
⇒都度直ちに報告</td><td>直ちに報告を行う必要性が低いとはいえないと判断したもの
⇒都度直ちに報告</td></tr>
</table>

※対外公表を行う場合は、いずれの場合も監督当局、信託協会へ都度直ちに報告

17

漏えい事案等発生時の本人への通知　※金融機関Q&A

（問Ⅳ-17）個人情報等の漏えい事案等が発生した場合は、金融機関は本人に通知する必要があるのか。

（答）

「個人データ」については、実務指針2-6-1において、「漏えい事案等が発生した場合には、本人への通知等を実施しなければならない。」（義務規定）とされており、「個人データ」の漏えい事案等が発生した場合は、金融機関は、本人への通知等を行う必要があります。

一方、「個人情報（個人データ以外の個人情報）」及び「加工方法等情報」については、金融分野ガイドライン第17条第3項で、「個人情報等の漏えい事案等の事故が発生した場合には、当該事案等の対象となった本人に速やかに当該事案等の事実関係等の通知等を行うこととする。」（努力義務）とされており、「個人情報」及び「加工方法等情報」の漏えい事案等が発生した場合には、本人への通知等を求められます。

なお、「個人データ」の漏えい数が多数であり、本人への通知が困難である場合には、公表によって本人への通知に代替するケースもあるものと思われます。また、例えば、漏えい事案等が発生した場合において、高度な暗号化処理等が施されている場合や即時に回収できた場合等、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さい場合等には、本人への通知を省略しうるケースもあるものと思われます。

18

「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第1号）

個人データの漏えい等について報告は努力義務、以下の場合には報告を要しない

① 実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合（以下は例示）

- 漏えい等事案に係る個人データ又は加工方法等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
- 漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合
- 漏えい等事案に係る個人データ又は加工方法等情報によって特定の個人を識別することが漏えい等事案を生じた事業者以外ではできない場合（ただし、漏えい等事案に係る個人データ又は加工方法等情報のみで、本人に被害が生じるおそれのある情報が漏えい等した場合を除く。）
- 個人データ又は加工方法等情報の滅失又は毀損にとどまり、第三者が漏えい等事案に係る個人データ又は加工方法等情報を閲覧することが合理的に予測できない場合

② FAX若しくはメールの誤送信、又は荷物の誤配等のうち軽微なものの場合（以下は例示）

- FAX若しくはメールの誤送信、又は荷物の誤配等のうち、宛名及び送信者名以外に個人データ又は加工方法等情報が含まれていない場合

19

金融機関の個人情報の漏えいに係る公表事例（2017年6月～2018年2月）

	金融機関名	公表年月	情報の内容	漏えい等の態様	件数	原因
1	イオン銀行	2018年2月	キャッシュカード一体型クレジットカードの請求明細	他の会員の請求明細書が混入	調査中	委託先のシステムの不具合
2	日新火災	2017年12月	満期を迎えた火災保険契約の顧客情報	従業員が顧客情報を第三者へ提供	905件	従業員による漏えい
3	東京海上日動保険	2017年12月	氏名、法人名、住所、電話暗号、メールアドレス、生年月日、性別、証券番号、車台番号、銀行口座情報、健康情報	子会社である保険代理店が不正アクセスを受け、メールボックス内の個人情報が流出	5400人	不正アクセス
4	高知銀行	2017年12月	顧客氏名、口座番号、取引金額、残高、振込依頼人の電話番号	ATMジャーナル紙が所在不明	2万6922件	誤廃棄の可能性
5	上光証券	2017年11月	顧客の氏名、住所、メールアドレス	ウェブサイトが不正アクセスを受け、同社のセミナーへ参加予定だった顧客情報が流出	83件	不正アクセス
6	鳥取銀行	2017年9月	顧客の氏名、住所、電話番号、口座番号、取引金額、印影	支払や入金時の伝票、納付依頼書、小切手などを綴った伝票綴りが所在不明	記載なし	誤廃棄の可能性
7	筑波銀行	2017年9月	顧客の氏名、口座番号、金融機関、支店番号、入出金金額、取引後残高、振込依頼人氏名、電話番号、受取人氏名・口座番号	ATM記録紙が所在不明	1324件	誤廃棄の可能性
8	豊和銀行	2017年8月	顧客の氏名、銀行コード、支店コード、口座番号、取引金額、残高	ATM記録紙が所在不明	4万1700件	誤廃棄の可能性
9	野村證券	2017年8月	名刺	名刺を収納したファイルが所在不明	800枚	記載なし
10	マネースクエア・ジャパン（M2J）	2017年7月	顧客の氏名、住所、メールアドレス、電話番号、生年月日、ID、現金残高、銀行口座情報、職業、保有金融資産の概要、投資経験、投資目的	不正アクセスにより顧客情報が流出	2455件	不正アクセス
11	南日本銀行	2017年7月	顧客の氏名、住所、電話番号、生年月日、口座番号、取引金額	伝票綴り紛失	5805件	誤廃棄の可能性
12	佐賀銀行	2017年6月	1億円以上の大口預金者の氏名、住所、電話番号、預金残高、取引店番号、顧客番号	元社員が持ち出し、共犯者に提供	169人	従業員による漏えい

20

3. 要配慮個人情報概念の導入への対応

21

(1) 要配慮個人情報と機微情報の関係　※金融機関Q&A問Ⅲ−1

（参考）機微（センシティブ）情報の対象範囲

	旧機微情報 （旧金融分野ガイドライン 第６条第１項）	要配慮個人情報 （個人情報保護法第２条第３項 ・施行令第２条）	機微情報 （金融分野ガイドライン 第５条第１項）
①旧機微情報＝要配慮個人情報	・人種 ・民族 ・犯罪歴 ・信教（宗教、思想及び信条） ・政治的見解	・人種 ※人種、世系又は民族的若しくは種族的出身を広く意味する。 ・犯罪の経歴 ・信条 ※個人の基本的なものの見方、考え方を意味し、思想と信仰の双方を含むもの。	・人種 ・犯罪の経歴 ・信条
②旧機微情報＞要配慮個人情報	・保健医療 ※例えば、医師等の診断等によらず、自己判断により市販薬を服用しているといったケースを含み、要配慮個人情報より対象が広い。	・病歴 ・身体障害、知的障害、精神障害等 ・健康診断等の結果 ・医師等による保健指導・診療・調剤	（保健医療） ・病歴 ・身体障害、知的障害、精神障害等 ・健康診断等の結果 ・医師等による保健指導・診療・調剤 ・その他（例えば、医師等の診断等によらず、自己判断により市販薬を服用しているといったケース）
③要配慮個人情報のみ		・社会的身分 ・犯罪により害を被った事実 ・刑事事件に関する手続 ・少年の保護事件に関する手続	・社会的身分 ・犯罪により害を被った事実 ・刑事事件に関する手続 ・少年の保護事件に関する手続
④旧機微情報のみ	・労働組合への加盟 ・門地 ・本籍地 ・性生活		・労働組合への加盟 ・門地 ・本籍地 ・性生活

22

(2) 要配慮個人情報該当性　※通則パブコメ

No	該当箇所		寄せられた御意見等	御意見等に対する考え方
229	2-3	要配慮個人情報	2. 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）（案）に対する意見等 身体障害、知的障害、精神障害等の情報が要配慮個人情報に含まれるとしているが、具体的な障害名を含まない情報（例えば「目が不自由」、「手が不自由」と記録すること）についても要配慮個人情報の対象となるか。実務上、目の不自由な顧客に対して代筆対応するケースがあり、その際、代筆の理由として「目が不自由」、「手が不自由」と行内的に記録を残しておくことがあるため、確認したい。 【一般社団法人全国銀行協会】	御指摘の事例は要配慮個人情報に該当しますが、政令第7条第1号の、本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合に該当するものと思われます。
230	2-3	要配慮個人情報	2. 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）（案）に対する意見等 「(7)身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること」において、例えば、「①『身体障害者福祉法（昭和24年法律第283号）別表に掲げる身体上の障害』があることを特定させる情報」として「都道府県知事、指定都市の長又は中核市の長から身体障害者手帳の交付を受け並びに所持していることが又は過去に所持していたこと」との記載があるが、犯罪収益移転防止法等で求められる本人確認資料で同手帳の写しを取り扱う場面において、同手帳の障害名や身体障害者等級表による級別などの情報をマスキング等すれば、具体的な障害内容が特定されないことから、要配慮個人情報の取得には該当しないと整理いただきたい。 【一般社団法人全国銀行協会】	身体障害者手帳を所持している事実は要配慮個人情報に該当することから、本人確認資料として同手帳の写しを取り扱う場合は、要配慮個人情報の取得と考えられます。なお、本人確認資料として本人から提出があった場合は、本人の同意があったものと考えられます。

23

(3) 要配慮個人情報かつ機微情報に該当する場合に求められる対応

・金融ガイドライン第５条　機微（センシティブ）情報

１　金融分野における個人情報取扱事業者は、・・・（・・以下「機微（センシティブ）情報という。）については、次に掲げる場合を除くほか、取得、利用又は第三者提供を行わないこととする。

（略）

⑦ 保険業その他金融分野の事業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供する場合

・個人情報保護法第１７条（適正な取得）

２　個人情報保護取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

・通則ガイドライン３－２－２

（※2）「本人の同意」については、2-12（本人の同意）を参照のこと。なお、個人情報取扱事業者が要配慮個人情報を書面又は口頭等により本人から適正に直接取得する場合は、本人が当該情報を提供したことをもって、当該個人情報保護取扱事業者が当該情報を取得することについて本人の同意があったものと解される。

24

実務指針(別添2)
金融分野における個人情報保護に関するガイドライン第5条に定める「機微（センシティブ）情報」（生体認証情報を含む。）の取扱いについて

金融分野における個人情報取扱事業者は、金融分野ガイドライン第5条に基づき、機微（センシティブ）情報について、同条第1項各号に掲げられた場合を除き、取得、利用又は第三者提供を行わず、同条第2項に基づき、同条第1項各号の事由を逸脱した取得、利用又は第三者提供を行うことのないよう、本実務指針Ⅰ～Ⅲに規定する措置に加えて、7-1、7-1-1、7-1-2、7-1-3、7-1-4、7-1-5に規定する措置を実施することとする。また、機微（センシティブ）情報に該当する生体認証情報（略）の取扱いについては、別添2に規定する全ての措置を実施しなければならない。

7-1-1　金融分野における個人情報取扱事業者は、6-1に規定する取得・入力段階における取扱規程において、機微（センシティブ）情報の取扱いについては、6-1に規定する事項に加えて、次に掲げる事項を定めることとする。

①金融分野ガイドライン第5条第1項各号に掲げる場合のみによる取得

②取得・入力を行う取扱者の必要最小限の限定

③取得に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項

25

4. 個人データの提供にかかる確認・記録義務への対応

26

確認・記録義務の内容①

- 背景：ベネッセ事件を契機に、名簿業者の暗躍が認知された
  ⇒個人情報が流通することについての国民の不安が増大
  ⇒情報の流通経路を追跡できることが必要
  ⇒確認・記録義務の制度化
- 義務の内容：
  ✓提供側及び受領側の双方に、個人データ授受に関する年月日、相手方の氏名又は名称、当該個人データの内容等（詳細は次頁及び次々頁のスライド参照）の記録義務・保存義務
  ✓受領側には、更に、記録義務の前提として確認義務
  ✓根拠条文：提供者側が25条、受領者側が26条

27

確認・記録義務の内容②

提供者/記録の内容	提供年月日	第三者の氏名等	本人の氏名等	個人データの項目	本人同意を得ている旨
オプトアウトによる第三者提供	必要	必要	必要	必要	不要
本人の同意による第三者提供	不要	必要	必要	必要	必要

28

確認・記録義務の内容③

受領者/確認記録の内容	提供年月日	第三者の氏名等	取得の経緯	本人の氏名等	個人データの項目	委員会による公表	本人の同意
オプトアウトによる第三者提供に基づく受領	必要	必要	必要	必要	必要	必要	不要
本人の同意による第三者提供による受領	不要	必要	必要	必要	必要	不要	必要
私人等からの第三者提供による受領	不要	必要	必要	必要	必要	不要	不要

29

確認・記録義務の内容④

- 法律上の例外:
  - 法令に基づく場合（法23条1項1号）
  - 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき（法23条1項2号）
  - 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき（法23条1項3号）
  - 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき（法23条1項4号）
  - 個人データの取扱いを委託することに伴い当該個人データが提供されている場合（法23条5項1号）
  - 合併等の事業承継に伴い個人データが提供されている場合（法23条5項2号）
  - 共同利用に係る個人データにおいて、その旨並びに共同して利用されている個人データの項目等につき、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき（法23条5項3号）
  - 第三者が国の機関である場合（法2条5項1号）
  - 第三者が地方公共団体である場合（法2条5号2項）
  - 第三者が独立行政法人等である場合（法2条5号3号）
  - 第三者が地方独立行政法人である場合（法2条5項4号）

30

確認・記録義務の内容⑤

- 解釈上の例外:
  - 「提供者」に不該当：本人による提供又は本人に代わっての提供であり、実質的に「提供者」による提供ではない
  - 「受領者」に不該当
  - 「提供」に不該当：不特定多数の者が取得可能な公開情報の提供
  - その他の場合：「本人に代わって」又は「提供者が、最終的に本人に提供することを意図した上で、受領者を介在して第三者提供を行う」個人データの授受等

31

確認・記録義務に関する実務対応

- 結論：

  日常的な業務の中で、確認・記録義務の履行として、従前とは異なる書類を作成している事業者は少ないと思われる。

- 理由：

  ✓確認・記録義務には、法律上の例外とガイドライン等による例外が存在する

  ∵ 実務に不当に過大な影響が及ばないよう配慮

  ✓従前用いていた書面による確認・記録義務の代替

32

5. 外国にある第三者への提供への対応

33

外国とのデータ授受に関する改正内容①

- 改正法で新たに設けられたもの
- 背景：
  (i) 経済のグローバル化や電子商取引が進展すると共に、国外に拠点を有しながら、日本向けに商品・役務の提供を行い、その際に、日本の居住者等に係る個人情報を取得する事業者が増加
  (ii) 高速通信網の整備と情報端末の処理速度の高速化
  (iii) 流通手段も多様化
  ⇒ 大量の情報が瞬時に、国境を越えて流通
  ⇒ 本来流通するべきではない情報も流通する可能性
- 内容：(i) 域外適用、(ii) 外国執行当局との協力、(iii) 外国にある第三者への提供

34

外国とのデータ授受に関する改正内容②

(i) 域外適用

✓ 外国に拠点がある者についても、一部の規定を除き、国内事業者とほぼ同様の規律が及ぶ

✓ もっとも、法の域外適用は、属地主義の原則の例外であるから、外国の事業者と日本との間に特別の関連性があることや法の適用を及ぼす必要性・合理性が認められる必要

⇒ 法の域外適用の対象事業者は、「国内にある者に対する物品又は役務の提供に関連してその者を本人とする個人情報を取得した個人情報取扱事業者」（法75条）に限定（一問一答144頁）

⇒ そのような「個人情報取扱事業者」とは、具体的には、外国に活動の拠点を有する事業者のうち、日本の居住者等国内にある者に対して物品やサービスの提供を行い、それに関連してその者を本人とする個人情報を取得した者をいう（一問一答142頁）

35

外国とのデータ授受に関する改正内容③

(iii) 外国にある第三者への提供

✓原則：外国にある第三者に個人データを提供する場合には、事業者は、原則として、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない（24条）

✓例外：

① 法23条1項各号に掲げる場合

② 「外国」が「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるもの」である場合

③ 「第三者」が「個人データの取扱いについてこの節（※）の規定により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者」である場合

※ 法「第4章 個人情報取扱事業者の義務等　第1節 個人情報取扱事業者の義務」を指す。以下同じ。

36

外国とのデータ授受に関する改正内容④

例外事由に関する具体的検討：

① 法23条1項各号に掲げる場合

⇒ 国内にある第三者への提供に際しても同意が不要な場合

② 「外国」が「個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるもの」である場合

⇒ 現時点では、具体的な国について個人情報保護委員会による指定なし

③ 「第三者」が「個人データの取扱いについてこの節の規定により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者」である場合

⇒ 実務上は③の例外事由該当性が重要ではないか

37

外国とのデータ授受に関する改正内容⑤

例外事由に関する具体的検討：

③「第三者」が「個人データの取扱いについてこの節の規定により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者」である場合

⇒ 規則11条では、この要件を具体化：

1項「事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、法第4章第1節の規定の趣旨に沿った措置の実施が確保されていること」

- ✓「適切かつ合理的な方法」は、個々の事例ごとに判断されるべきものであるが、個人データの提供先である外国にある第三者が、我が国の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を継続的に講ずることを担保することができる方法である必要があるとされている
- ✓ このような方法の具体例として、①外国にある事業者に個人データの取扱いを委託する場合には、提供元と提供先との間の契約書等、②同一企業グループの内部で個人情報を移転する場合には、提供元と提供先に共通して適用される内規・プライバシーポリシーが挙げられる。

38

外国とのデータ授受に関する改正内容⑥

例外事由に関する具体的検討：

2項「個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること」

- ✓ 外国ガイドライン3－3は、「個人情報の取扱いに係る国際的な枠組みに基づく認定」とは、国際機関等において合意された規律に基づき権限のある認証機関等が認定するものをいい、当該枠組みは、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を継続的に講ずることのできるものである必要がある」とする
- ✓ 具体例として、外国にある第三者が、アジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）システムの認証を取得していることを挙げている
- ✓ なお、外国ガイドライン3－1は、提供元の事業者がアジア太平洋経済協力会議（APEC）の越境プライバシールール（CBPR）システムの認証を取得しており、提供先の「外国にある第三者」が当該事業者に代わって個人情報を取り扱う者である場合には、当該事業者がCBPRの認証の取得要件を満たすことも「適切かつ合理的な方法」の一つであると解されるとする

39

外国にある第三者への提供に関する実務対応

- 例外要件③に基づく整理　or
- 原則どおり、 本人の同意を得て提供するという整理

⇒ 個人情報の第三者提供に関する同意書を従来から用いている実務では、この同意書における同意の対象に国内にある第三者のみならず外国にある第三者を追加する方法も選択されているようである

⇒ なお、この「外国」については、ある程度明確にする必要があり、QA9－2及び外国パブコメ715では、この方法の具体例として、①提供先の国名又は地域名を個別に示す方法（例：米国）、②実質的に本人から見て提供先の国名を特定できる方法（例：本人がサービスを受ける際に実質的に本人自身が個人データの提供先が所在する国等を決めている場合）、③国名を特定する代わりに外国にある第三者に提供する場面を具体的に特定する方法が挙げられている

40

6. 外部委託の見直し

41

外部委託の見直し①

- 個人情報保護法の条文自体に変更はない
- 今般の改正以前に、金融ガイドラインや安全管理措置等についての実務指針が改定され、金融機関等においては、その際に、委託先管理の厳格化等への対応が必要であった
- 今般の改正において、金融ガイドライン等も改定され、通則ガイドラインと共通する部分については記載を省略することとしたため、今後は、金融ガイドライン等のみならず、通則ガイドライン等の4種の基本ガイドラインを参照する必要があるため注意を要する
- 金融ガイドラインの改定に対応済みの事業者にとっては、今般の改正のために、新たな実務対応を迫られることは多くないように思われる

42

外部委託の見直し②

「委託を受けた者に対して必要かつ適切な監督を行っていない事例」（通則ガイドライン3-3-4）

事例1）個人データの安全管理措置の状況を契約締結時及びそれ以後も適宜把握せず外部の事業者に委託した結果、委託先が個人データを漏えいした場合

事例2）個人データの取扱いに関して必要な安全管理措置の内容を委託先に指示しなかった結果、委託先が個人データを漏えいした場合

事例3）再委託の条件に関する指示を委託先に行わず、かつ委託先の個人データの取扱状況の確認を怠り、委託先が個人データの処理を再委託した結果、当該再委託先が個人データを漏えいした場合

事例4）契約の中に、委託元は委託先による再委託の実施状況を把握することが盛り込まれているにもかかわらず、委託先に対して再委託に関する報告を求めるなどの必要な措置を行わず、委託元の認知しない再委託が行われた結果、当該再委託先が個人データを漏えいした場合

43

外部委託の見直し③

外部事業者へ個人データの取扱いを委託したといえるかについてのQ＆A
（QA5-26。なお、QA5-33～35も参照）

（Q5-26）**配送事業者、通信事業者等の外部事業者を利用して、個人データを含むものを送る場合は、当該外部事業者に対して当該個人データの取扱いを委託（法第23条第5項第1号）しているものと考えられますか。**

（A5-26）一般的に、外部事業者を利用して、個人情報データベース等に含まれる相手の氏名、住所等宛に荷物等を送付する行為は、委託に該当すると解されます。

ただし、配送事業者を利用する場合、通常、当該配送事業者は配送を依頼された中身の詳細については関知しないことから、当該配送事業者との間で特に中身の個人データの取扱いについて合意があった場合等を除き、当該個人データに関しては取扱いの委託をしているものではないものと解されます。

また、通信事業者による通信手段を利用する場合も、当該通信事業者は、通常、通信手段を提供しているにすぎず、通信を依頼された中身の詳細について関知するものでないことから、同様に通信の対象である個人データについてはその取扱いを委託しているものではないものと解されます。

なお、いずれの場合も、外部事業者を利用する個人情報取扱事業者には、安全管理措置を講ずる義務が課せられているため、中身の個人データが漏えい等しないよう、適切な外部事業者の選択、安全な配送方法の指定等の措置を講ずる必要があります。

44

7．今後の課題・見直しのポイント等

45

今後の課題・見直しのポイント①

- 今般の改正法の施行によって、金融機関等の事業者の実務において、改正前に不安視されていたような作業負担が大幅に増えるといった影響は、現時点においては、特段生じていないものと思われる
- もっとも、今後、更なる検討や対応が必要となるものとして、以下の2つが考えられる
  - (i) 要配慮個人情報
  - (ii) 匿名加工情報

46

今後の課題・見直しのポイント②

今後、更なる検討が必要となるもの

(i) 要配慮個人情報

✓ 現在の実務は保守的な運用がなされており、いわば「過剰反応」となっている部分があるようにも思われる

⇒法令上求められている水準が事例の積み重ねとともにより具体的に明らかになっていくことにより、現在の実務上の負担が適切な水準となるように、調整が続けられるのではないか

⇒科学技術の更なる発展とともに、新たな問題も生じうる

例）通話録音、防犯カメラ画像

47

今後の課題・見直しのポイント③

今後、対応が必要となるもの

（ii） 匿名加工情報

✓ 改正法の目玉の一つでありながら、改正法施行後約9ヶ月経っても、まだその活用事例は多くない

∵ ①加工基準に曖昧さが残るため、どの程度加工すれば匿名加工情報として認められるのかが分かりにくい。②他方で、保守的に匿名化の程度を高度化すればするほど、利活用するためのデータとしての価値が低くなるというジレンマがある。

✓ 金融機関では、イオン銀行が、他に先駆けて匿名加工情報を作成し公表

✓ JIPDECも匿名加工情報の事例集を作成し公表
（https://www.jipdec.or.jp/protection_org/u71kba00000001hh-att/AOP_006.pdf）

48

今後の課題・見直しのポイント④

イオン銀行の匿名加工情報の作成例

「性別、年代（5歳刻み）、居住する都道府県、郵便番号、職種、業種、世帯構成に関する情報、ご契約カード種類、店番号、口座開設経過月数、預金等の当行各種金融商品の取引状況および審査結果、現在および次回のポイントクラブステージ」という項目を設定

（https://www.aeonbank.co.jp/privacy/rule/tokumei.html）

49

今後の課題・見直しのポイント⑤

今後の見直しのポイント

大切なことは、個人情報の重要性について十分に理解して、今後新たに生じる事態に法令遵守の観点から的確に対応しつつ、他方で、マーケティングや商品開発等のため、個人情報が内包する有益な特徴を最大限に生かすこと

⇒ そのためには、プロアクティブに情報収集を行い、個人情報保護法の規制の外延を分析するとともに、新たな時代におけるデータ活用の方法を探求し、これを適時かつ的確に実行することが必要ではないか

50

ご静聴いただき、ありがとうございました。