SECTION 1

金融機関における個人情報保護問題

金融機関における個人情報保護と聞いて、何が思い浮かぶでしょうか。最も多い答えは、「顧客の個人情報を正当な理由なく第三者に漏えいしてはならない」というものだと思います。これは、金融機関が負っている守秘義務の観点からも説明できます。この点については最高裁が「金融機関は、顧客との取引内容に関する情報や顧客との取引に関して得た顧客の信用にかかわる情報などの顧客情報につき、商慣習上又は契約上、当該顧客との関係において守秘義務を負」うと判示しています（最高裁決定平成19年12月11日）。

実際にも、企業が保有する個人情報の漏えい事件が起こると、社会問題として報道されます。このような報道が株価に影響することもありますし、広く報道された通信教育事業者大手における個人情報漏えい事件のように、企業や役員に対する損害賠償事件に発展することもあります。

顧客情報を漏えいさせてはならないという観点は、個人情報保護の重要な項目の1つです。しかし、金融機関が個人情報保護において求められるのは、守秘義務の遵守だけではありません。金融機関は、お客さまだけでなく、株主、従業員など、多くの個人とかかわりをもちます。そして、事業を遂行するなかで、金融機関は多数の個人情報を保有・利用し、必要に応じて個人情報を第三者に提供したり、第三者と共同で活用したりします。このような場合に、個人情報を適切に取り扱うことも、個人情報保護の大事な一環です。

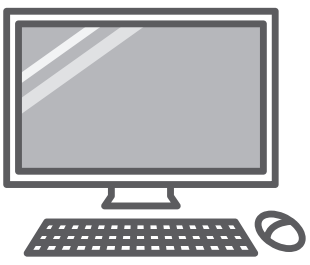
近時、情報通信技術が飛躍的に発展し、スマートフォン、SNS等を通じて、大量の個人に関するデータを事業者が収集・集積できるようになりました。このような大量のデータを利活用することにより、生活の利便性の向上等が期待されています。金融機関においても、いわゆるフィンテック（FinTech）と呼ばれるサービス分野において、金融機関に集積された大量のデータを解析し、商品やサービスの開発に活用しようとする動きがあります。

一方で、事業者が大量に集積された個人に関するデータを保有していることに対しては、データが悪用されたり、不適切に利用されたりすることによるプライバシー侵

害が消費者サイドにおける重大な関心事となっています。

たとえば、鉄道事業者がICカードに記録された乗降履歴に関する情報を、本人を特定できないよう加工して他の事業者に提供したケースでは、サービス利用者から多数の批判が起こりました。

これらの事情の下で、社会における個人情報に対する意識は高まっているといえます。とりわけ、社会インフラとして、重要な立場から公共性の高い業務を営む金融機関には、このような個人情報に対する意識の高まりに応え、個人情報を適切に取り扱うことが求められているといえるでしょう。



ケーススタディで学ぶ！個人情報保護

本章の内容

SECTION 1

個人情報の漏えいとその対応

個人情報の漏えいとその対応

⑴　個人情報漏えい事案の類型と防止策

金融機関の内部に保管されている個人情報の外部への漏えい事案は、主に３つの態様に分類されます。

①　従業員の過誤にもとづく個人情報の漏えい

１つ目は、従業員の業務上の過誤にもとづく漏えいです。たとえば、個人情報が記録された書類やノート型パソコン、CD-R、USBメモリ、SDメモリーカード等の記録媒体を外に持ち出してカバンごと紛失してしまったというケース、顧客Ａに送るべき郵便物の封筒に誤って別の顧客Ｂの宛名ラベルを貼ってしまったために、Ａの個人情報がＢに漏えいしたというケース、ファクシミリの番号や電子メールのアドレスを十分確認せずに送信した結果、個人情報が第三者に漏えいしてしまったというケースなどが典型的な事例としてあげられます。また、金融機関内の一定の場所に保管してあるべき個人情報が見当たらない（紛失してしまっている）というケースもこの類型に当たります。

これらのケースでは、個人情報が意図的に外部に流出されたわけではないため、それ以上に拡散することはさほど多くはないのですが、万一、悪意のある第三者の手に入ってしまうようなことになれば、重大な漏えい事件に発展するおそれがあります。

このような従業員の過誤による個人情報の外部流出を未然に防ぐ方法としては、個人情報を扱う場合のルールを策定し、その徹底を図ることが重要です。たとえば、個人情報を含む業務情報へのアクセス権限を明確にし、業務上不必要な情報にアクセスさせないこと、個人所有のノート型パソコンやUSBメモリ等の記録媒体の持込みおよび使用を禁止すること、業務外での電子メールやインターネットの使用を禁止すること、やむを得ず社外に情報を持ち出す際にはパスワードの設定や暗号化を行い、第三者に渡っても内容を見られないようにすること、業務用のパソコンにファイル共有ソフト等のソフトウェアをインストールさせないこと、個人情報を扱う仕事場では私物

の携帯電話やスマートフォン、ノート型パソコン、タブレット端末、デジタルカメラの持込みや使用を禁止すること、SNSの使用を禁止することなどが考えられます。

また、郵便物の誤送付やファクシミリの誤送信を防ぐために、複数の従業員のチェックを経ることをルール化し、それを徹底することなどが考えられます。個人情報が記載されている帳票等の書類や個人データが記録されている記録媒体の紛失を防ぎ、早期に漏えい事故を発見するためには、自部署や自店で定期的に行う検査の項目にこれらのチェック項目を含めた対応をとる必要もあると考えられます。

②　従業員の故意にもとづく個人情報の漏えい

2つ目は、従業員による意図的な個人情報の漏えいです。これには現職の従業員が不正に持ち出す場合もあれば、従業員が退職するにあたって持ち出す場合もあります。このような不正行為の目的としては、持ち出した個人情報を第三者に売却して不当に利益を得ようとするもの、勤務先や上司への恨み等からくる嫌がらせのようなもの、転職した先や独立した後の営業活動への利用をもくろむものなど、様々なものが考えられます。

このような従業員の不正行為を抑制するためにまず行うべきことは、システム上の手当てとして個人情報にアクセスできる権限をもつ従業員の数を必要最小限に設定することです。情報にアクセスできる従業員が限定されていれば、不正行為の機会を減少させるとともに、漏えい行為を実行した者を特定することが容易になり犯行を隠すことが困難になるでしょうから、故意に情報を持ち出そうとする者に対する抑止効果が期待できます。また、従業員の人事異動や退職に際して、IDを消去することにより、アクセスできないようにすることも重要です。

そのほかの対策として、相当の費用を要するものではありますが、個人情報を扱う部屋の出入り口に入退室を管理するシステムを導入したり監視カメラを設置したりする方法、あるいは、個人情報が記録されているパソコンにIDカードや指紋での認証システムを導入するといった方法も有効であると考えられます。

③　外部からの侵入に起因する個人情報の漏えい

3つ目は、外部からの侵入により、個人情報の漏えいに至る場合です。

最近では、メールの添付ファイルに仕込まれたコンピュータウイルスに感染させることにより、パソコン内部の情報をネットワーク上に公開させ、インターネット経由で流出に至らしめる悪質なケースなどが増えています。また、ファイル共有ソフト（Winny、Shareなど）を使用することによるリスクを熟知しないまま、安易に個人情報の入った業務用パソコンにインストールしたり、あるいはファイル共有ソフトがイ

ンストールされている私物パソコンに個人情報を入れてしまったりして、ウイルスに感染し個人情報の流出事故に至るケースも少なくありません。

とくに注意が必要なのは、「標的型サイバー攻撃」です。

このような外部からの侵入への対策としては、まずは自社の情報システムにおけるコンピュータウイルス対策を高度化させておくことが重要であることはいうまでもありません。

それとともに、外部からの不審なメールに添付されているファイルを開いたり、メール上のリンクをクリックしたりすることのないよう、研修等を通じて従業員に周知すること、また、ファイル共有ソフトのインストールを禁止するなど、社内のルールを整備することなどで対処する必要があるでしょう。さらに外部から侵入された場合でも二次被害を小さくできるような体制を構築することも重要です。

個人情報の漏えいが発生した場合の対応

このように、個人情報の漏えいを回避するためには、事前の予防的対策をしっかりとっておくことが重要であることは間違いありません。しかしながら、コンピュータ技術は日々進歩し、各企業の保有する情報システムに侵入する手段は巧妙化しているため、情報セキュリティを高度化させても、自社システムへの不正アクセスを完全に遮断することはできません。また、どんなに社内ルールを徹底しても、これに従業員等が従わないケースが必ず一定数は出てきます。いかに事前防止策を尽くしたとしても、個人情報の漏えいを完全に排除することができない以上、個人情報が漏えいした場合を想定して、どのような対応をとるべきかをあらかじめ考えておくことが肝要になります。

漏えい事案が発生した場合に、もっとも重要なことは、被害の拡大を防止することです。そのためには、第三者に流通するおそれがほとんどない場合（たとえば、社内でシュレッダーにかけてしまった蓋然性が高い場合）を除き、できるだけ早く、漏えいした個人情報の対象である顧客等に対し、漏えいの事実を伝えることが必要です。なぜなら、顧客も自分の個人情報が漏えいしたことを知っていれば、詐欺などに利用されそうになった場合でも、警戒心を働かせて被害を防ぐことができるかもしれませんし、個人情報を悪用しようとする者に対しても抑止効果が期待できるからです。

他方で、漏えいした個人情報の流通を防止するためには、漏えいした情報の範囲や保有者を知る必要があり、そのためには、漏えいルートや影響範囲を特定し、漏えいした原因を究明することが必要です。顧客リストが出回っているという外部からの情

報により個人情報漏えいの事実が発覚したような場合には、漏えいルートが分からないことも少なくありません。そのため、金融機関内での調査だけではなく、警察等捜査機関への通報により、漏えいルートを解明すべき場合も出てくるでしょう。

事実関係の全体像を把握し、ある程度詳細な部分まで判明したら、次になぜそのような事案が発生したのか、金融機関としての個人情報保護態勢のどこに問題があったのか、役職員のモラルやコンプライアンス意識が薄弱であったのか、それともセキュリティシステムの脆弱性に原因があったのか等の分析を行うことが必要になります。

そのような分析結果をもとに、それに対応する再発防止策を策定して、これを公表するとともに実行していくことが必要です。これらの対応については、個GL通則３－５－２の記載が参考になります。個人データの漏えい事案等の事故が発生した場合の事後的な対応について、個情法26条は、個人情報取扱事業者に対し、個人情報保護委員会への報告（速報および確報の２段階）および本人への通知を行う義務を課しています。いずれの義務も個情則７条各号に定める場合にのみ発生します。そして、個人データの漏えい等の場合にだけ適用があり、個人データに該当しない個人情報の漏えい等の場合には適用がありません。

上記の個情法26条にもとづく対応に加えて、金融GLは、個人データ（個情則７条に定める場合を除く）、個人情報、仮名加工情報に係る削除情報等または匿名加工情報に係る加工方法等情報について漏えい等またはそのおそれがある場合（個情則７条に定める場合を除く）に、金融機関が講ずべき措置を次のとおり定めています（金融GL11条２項・３項・４項）。

⑴　個GL通則３－５－３に準じた、業法上の監督当局への報告
⑵　個GL通則３－５－４に準じた、本人への通知等
⑶　事業所内部における報告及び被害の拡大防止
⑷　事実関係の調査及び原因の究明
⑸　影響範囲の特定
⑹　再発防止策の検討及び実施
⑺　事実関係及び再発防止策等の公表（事態の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から速やかに行う）

個人情報の漏えいと金融機関への影響

個人情報の漏えいが金融機関に及ぼす影響は、法的責任から生じるものと法的責任と関係なく生じるものとに分けることができます。さらに、法的な責任には、行政上の責任、刑事上の責任および民事上の責任があります。

法的責任としては、行政上の責任として、個情法上、個人情報保護委員会から同法違反の行為を是正するための必要な措置の勧告や命令を受けること、また、業務改善命令や業務停止命令を受けることがあげられます。

次に、刑事上の責任としては、個情法上、個人情報保護委員会からの命令に違反した場合に罰金等を科せられたりすることがあげられます。

最後に民事上の責任としては、訴訟外の費用・損失として見舞金・見舞品の購入・送付費用や、個人情報の流出による架空請求などの詐欺被害を受けたりした場合に生じる経済的損害に対する賠償、あるいは本人が不安な状態に置かれることから生じる精神的損害に対する慰謝料などの支払いがあげられます。訴訟となった場合には、相手方に対する損害賠償のほかに、弁護士費用を含めた訴訟費用を負担することを余儀なくされることになります。また、金融機関で生じた事案ではありませんが、通信教育事業者における個人情報漏えい事件では、株主による役員責任の追及（株主代表訴訟）にまで発展しました。

法的責任と関係なく生じる影響としては、直接的には、謝罪広告やお詫び状の作成・送付費用その他の諸費用があげられますが、それ以外にも、重要なお客さまとの取引の停止・解約や新規取引の締結不可による損失、漏えい事件発生後の業績の低下のほか、社員間に不安や不満が生じたり、士気が低下したりすることなども考えられます。このような、社会的信用の失墜や企業イメージのダウンによる経営上の損失のほうが、法的な責任より遥かに影響が大きいとも考えられます。

以上のことから、とくに個人情報の取扱量が多く、顧客との信頼をベースに業務を行っている金融機関としては、個人情報の漏えいによる影響は極めて大きいといえます。場合によっては企業の存続にかかわる問題にまで発展するおそれがあるということを十分に認識し、個人情報の漏えい防止に努めることが重要です。

SECTION 8

マイナンバー法による予想事案

(1) 預金取引（新規普通預金口座の開設）

当行窓口に、普通預金口座の開設を希望するお客さまのＡさんが来店されました。「本人確認書類をお持ちですか」とお尋ねしたところ、その日は、本人確認書類として、マイナンバーが記載されたカードしかお持ちでないとのことでした。本日中にお手続きをされたいとのご希望です。窓口で対応したテラーのＢさんですが、右往左往しています。

質問

普通預金口座を開設する際、本人確認書類として、マイナンバーが記載された書類、具体的には、個人番号カード（マイナンバーカード）や通知カード、個人番号通知書マイナンバーが記載された住民票の写しを用いてもよいのでしょうか。

また、用いてもよい場合には、どのような点に気を付けて、対応すればよいでしょうか。

解説

(1) 本人確認の根拠法令 ― 犯罪による収益の移転防止に関する法律

金融機関が個人顧客に対し普通預金口座を開設するには、犯収法にもとづき、本人特定事項（氏名、住居および生年月日）、取引を行う目的、職業を確認しなければなりません（同法４条１項）。本人特定事項の確認は、犯収法に定められた本人確認書類により行う必要があります（同法４条１項１号・犯収則６条１項１号イ・７条１号）。

本事案では、マイナンバーが記載された公的書類を本人確認書類として用いることができるかが、問題になります。

(2) マイナンバーが記載された公的書類を本人確認書類とすることができるか？

マイナンバーが記載された公的書類には、個人番号カード（マイナンバーカード）と通知カード、個人番号通知書があります。また住民票の写しにもマイナンバーが記載される場合があります。

結論からいうと、個人番号カード（マイナンバーカード）とマイナンバーの記載された住民票の写しについては、本人確認書類とすることができますが、通知カードと個人番号通知書は本人確認書類とすることができません。この点については、2015（平成27）年９月18日に公布された犯収則の改正が関連します。以下、説明します。

個人番号カード（マイナンバーカード）は、2016（平成28）年１月１日に施行された改正後の犯収則７条１号イにおいて、本人確認書類として明示されました。

通知カードについては、関係省庁から本人確認書類として取り扱うことが適当でないとの見解が出されたことから、本人確認書類に含まない扱いとされています。

条文上は、犯収則７条１号ホの「官公庁から発行され、又は発給された書類その他これに類するもので、当該自然人の氏名、住居及び生年月日の記載があるもの」が認められているものの、「（国家公安委員会、カジノ管理委員会、金融庁長官、総務大臣、法務大臣、財務大臣、厚生労働大臣、農林水産大臣、経済産業大臣及び国土交通大臣が指定するものを除く。）」という例外がカッコ書きで規定され、改正の公布日（2015（平成27）年９月18日）から施行されています。これを受けて、「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第七条第一項に規定する通知カード」が上記カッコ書きにもとづいて指定されています（犯収則７条１号ホの規定にもとづき、書類を指定する件（平成27年国家公安委員会、金融庁、総務省、法務省、財務省、厚生労働省、農林水産省、経済産業省、国土交通省告示第２号・第４号））。これにより、通知カードを、本人確認書類とすることはできない扱いとなっています。また、個人番号通知書については、「住所」の記載がありません。そのため、犯収則７条１号ホの定める書類にそもそも該当しないので、個人番号通知書を本人確認書類として利用することはできません。

なお、「住民票の写し」については、本人確認書類として用いることが認められています（犯収則７条１号ニ）。

⑶　マイナンバーが記載された公的書類による本人確認の場合の注意点

犯収法にもとづいて本人特定事項の確認、その他の取引時確認を行った場合、これに関する確認記録を作成し、取引終了日等から７年間保存しなければなりません（同法６条）。

この確認記録の作成および保管に関して、マイナンバーが記載された公的書類を取り扱う際には、犯収法上の観点だけでなく、マイナンバー法上の観点からも慎重な注意が必要です。

マイナンバー法は、社会保障・税・災害対策などに必要な範囲として同法で定める

範囲を超えて、マイナンバーを収集・保管することを禁止しています（同法９条・20条）。犯収法上の取引確認記録に、本人確認書類を特定するに足りる事項として、マイナンバーを記録することは、マイナンバー法19条各号、別表のいずれにも該当しませんので、法令上認められません（事業者・別冊GLQ&AQ20－２）。

したがって、マイナンバーを確認記録に含めないようにする必要があります。

個人番号カード（マイナンバーカード）が本人確認書類として用いられる場合、記録事項である「顧客等又は代表者等の本人特定事項の確認のために本人確認書類又は補完書類の提示を受けたときは、当該本人確認書類又は補完書類の名称、記号番号その他の当該本人確認書類又は補完書類を特定するに足りる事項」（犯収則20条１項17号）については、個人番号以外の事項（たとえば発行者や有効期間）を記載することとされています（犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令案に関するパブリックコメントの結果・別紙第１「「犯罪による収益の移転防止に関する法律の一部を改正する法律の施行に伴う関係政令の整備等に関する政令案」等に対する御意見・御質問に対する警察庁及び共管各省庁の考え方について」87番）。書類の名称のみでは「特定するに足りる」とはいえず、発行者および有効期限についても記録する必要があるとされている点に留意する必要があります（上記「考え方について」152番）。

実務対応

⑴ マイナンバーが記載された書類の取扱い

マイナンバーが記載された公的書類のうち、個人番号カード（マイナンバーカード）、マイナンバーが記載された住民票の写しは、犯収法にもとづく本人特定事項の確認書類とすることができます。

個人番号カード（マイナンバーカード）、マイナンバーが記載された住民票の写しを受け取るときには、十分な注意が必要です。

なお、2020（令和２）年４月施行（2018（平成30）年11月公布）の「犯罪による収益の移転防止に関する法律施行規則の一部を改正する命令」等により、本人特定事項の確認が厳格化されています。

顧客との対面時においては、個人番号カード（マイナンバーカード）であれば１枚でよいですが（犯収法４条１項・犯収則６条１項１号イ）、住民票の写しの場合はこれに加えて、書留郵便等により転送不要郵便物等として送付する必要があります（犯収法４条１項・犯収則６条１項１号ロ）。

郵送等の顧客と対面しない場合においては、個人番号カード（マイナンバーカード）であっても１枚では足りず、さらにもう１種類の本人確認書類の送付が必要となり、かつ書留郵便等により転送不要郵便物等として送付する必要があります（犯収法４条１項・犯収則６条１項１号リ）。住民票の写しの場合はコピーではなく、市役所等から交付された住民票の写し原本であれば、これ１種類だけでよく、あとは書留郵便等により転送不要郵便物等として送付すればよいこととされています（犯収法４条１項・犯収則６条１項１号チ）。

個人番号カード（マイナンバーカード）は、裏面にマイナンバーが記載されていますので、コピーを取る際も、裏面はコピーしないようにします。業務上やむを得ず裏面のコピーが必要となる場合は、コピー後に、マイナンバー部分をマスキングしなければなりません。できれば、お客さまの前でマスキングしたほうが、お客さまにとっても安心でしょう。

また、個人番号カード（マイナンバーカード）の写しの送付を受ける場合には、表面の写しの送付を受けることで足り、裏面の送付を受ける必要はありません。仮に裏面の写しの送付を受けた場合には、マスキングをする必要があるとされています（上記「考え方について」87番）。

また、マイナンバーが記載された住民票の写しは、裏面ではなく、表面にマイナンバーが記載されています。これらをコピーする場合は、コピー後に、マイナンバー部分をマスキングしなければなりません。

⑵　有効期間

個人番号カード（マイナンバーカード）は、18歳以上の方については有効期間が10年（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に規定する個人番号、個人番号カード、特定個人情報の提供等に関する命令26条１項１号）で、18歳未満の方については有効期間が５年（同項２号）です。

犯収法にもとづく本人特定事項の確認書類の有効期間の確認の際には、この点に留意しましょう。

⑶　今後の取扱い

2015（平成27）年の通常国会で改正マイナンバー法が成立し、2018（平成30）年（マイナンバー法の一部を改正する法律附則１条６号施行日）に、普通預金口座とマイナンバーが紐づけられるようになりました。紐づけ後は、マイナンバーを普通預金口座の開設・管理に利用することが、マイナンバー法上適法な行為となります。

また、2021（令和３）年５月には、「預貯金者の意思に基づく個人番号の利用による

預貯金口座の管理等に関する法律」も公布されましたが、こちらはまだ施行されていません。施行日は、公布日から３年以内の範囲で政令にて定められます。

いずれにしても、ここで注意したいのが、お客さまが金融機関にマイナンバーを渡す意図です。2015（平成27）年改正において金融機関がマイナンバーを収集、保管することが可能となったのは、お客さまの預貯金口座を開設する場合です。そのため、金融機関は、お客さまがあくまで本人確認書類として提示しているのか、任意の預貯金付番への対応を求めているのか、当該お客さまの意向を確認し、対応する必要があります。

キーワード

・犯収法
・本人特定事項の確認
・個人番号カード（マイナンバーカード）
・マイナンバーの利用範囲の制限
・マイナンバーの提供の求めの制限
・マイナンバーの収集等の制限
・マイナンバーの保管の制限