金融機関における個人情報保護に関するＱ＆Ａ

令和７年 10 月
個人情報保護委員会事務局
金融庁

Ⅰ　総論

（問Ⅰ－１）金融分野において、個人情報保護法の体系と各業法の体系の関係はどのようなものか。

（答）

個人情報保護法の体系では、個人情報の保護に関する法律（以下「個人情報保護法」という。）、個人情報の保護に関する法律施行令（以下「個人情報保護法施行令」という。）及び個人情報の保護に関する法律施行規則（以下「個人情報保護法施行規則」という。）のほか、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）（以下「通則ガイドライン」という。）を基礎[注１]として、金融分野における個人情報保護に関するガイドライン（以下「金融分野ガイドライン」という。）及び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（以下「実務指針」という。）があり、適用対象は「個人情報取扱事業者」で、主に「個人データ」の取扱いに関する規定が定められています（なお、金融分野ガイドライン及び実務指針は、各業法に基づく規定を含みます。）。

一方、銀行法や保険業法等の一部の業法の体系では、各業法の施行規則（内閣府令）において、①個人顧客情報の安全管理措置等、②個人顧客情報の漏えい等報告等、③返済能力情報の取扱い、④特別の非公開情報の取扱い等が定められており、各業態の監督指針等において、個人顧客情報につき、通則ガイドライン、金融分野ガイドライン及び実務指針等の規定に基づく適切な取扱いの確保が求められています。

各業法の規定の適用対象となる各業態の金融機関[注２]がとるべき①個人顧客情報の安全管理措置等や②個人顧客情報の漏えい等の報告等の対象は、個人顧客に関する「個人データ」となります。

（注１）金融分野ガイドライン及び実務指針は、通則ガイドラインを基礎とした上で、金融分野の個人情報の性質及び利用方法に鑑み、個人情報の取扱いに関して、金融分野における個人情報取扱事業者に特に厳格な措置が求められる事項等を規定しています。

したがって、金融分野ガイドラインにおいて特に定めのない部分については、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（外国にある第三者への提供編）（以下「外国第三者提供ガイドライン」という。）、同ガイドライン（第三者提供時の確認・記録義務編）、同ガイドライン（仮名加工情報・匿名加工情報編）及び同ガイドライン（認定個人情報保護団体編）が適用されることとなります（金融分野ガイドライン第１条）。

（注２）本Ｑ＆Ａにおいて、「金融機関」とは、貸金業法における「貸金業者」等、金融分野における事業者を広く含みます。ただし、個人顧客情報の保護に関する規定の内容については、各業法によって異なるものもあります。

Ⅱ　個人情報・個人データ

（問Ⅱ－１）官報や民間の新聞等により公表されている情報であっても「個人情報」に当たるか。

（答）

「個人情報」とは、個人情報保護法第２条第１項において、「生存する個人に関する情報であって、

① 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）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。）

② 個人識別符号が含まれるもの

のいずれかに該当するもの」とされています。官報や民間の新聞等により公表されている情報であっても、上記要件に該当すれば、「個人情報」に該当するものと解されます。

（問Ⅱ－２）それ単体では特定の個人を識別することができない情報であれば、それは「個人情報」に当たらないのか。例えば、住宅ローンの残高など、金額のみが記載され、その他氏名等が記載されていないものは「個人情報」に当たらないのか。

（答）

「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（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、それ単体では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。

したがって、住宅ローンの残高のみが記載された情報であったとしても、当該情報を取り扱う事業者において、氏名その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、全体として、「個人情報」に該当することとなるため、ケースバイケースでの判断が必要と考えられます。

また、「個人情報」に該当しない場合であっても、個人に関する情報である限り、「個人関連情報」（個人情報保護法第２条第７項）に該当することとなり（ただし「仮名加工情報」や「匿名加工情報」に該当する場合を除く。）、個人関連情報の第三者提供の制限等（個人情報保護法第 31 条）の規制の対象となります（問Ⅱ－８参照）。

（問Ⅱ－３）「個人情報」と「個人データ」の違いは何か。

（答）

「個人情報」とは、生存する個人に関する情報であって、

① 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。）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。）

② 個人識別符号が含まれるもの

のいずれかに該当するものをいいます（個人情報保護法第２条第１項）。

一方、「個人データ」とは、こうした「個人情報」を容易に検索することができるように体系的にまとめた「個人情報データベース等」（問Ⅱ－４参照）を構成する「個人情報」をいいます（個人情報保護法第 16 条第３項）。つまり、「個人情報」は、「個人情報データベース等」を構成した時点で「個人データ」でもある「個人情報」になり、一方、「個人情報データベース等」を構成していない「個人情報」は「個人データ」ではない「個人情報」になります。

「個人情報」が「個人情報データベース等」に入力され「個人データ」に該当した場合、「個人データ」ではない「個人情報」の場合よりも個人情報取扱事業者（通則ガイドライン 2-5 参照）の遵守すべき事項が多くなります（個人情報保護法第 22 条～第 30 条）。

※法第 23 条に定める「その他の個人データの安全管理のために必要かつ適切な措置」には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる。また、法第 26 条に関し、規則第７条第３号関係に規定する「個人データ」には、「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」が含まれる。

なお、「個人データ」のうち、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止の全てに応じることのできる権限を有するもの（政令で定める一定要件を満たすものを除きます。）を「保有個人データ」といいますが（個人情報保護法第 16 条第４項、通則ガイドライン 2-7）、「保有個人データ」については、個人情報取扱事業者の遵守すべき事項が「個人データ」の場合よりも更に追加されます（個人情報保護法第 32 条～第 37 条）。

（参考）個人情報、個人データ、保有個人データの義務規定の差異

第 17 条	利用目的の特定	○	○	○
第 18 条	利用目的による制限	○	○	○
第 19 条	不適正な利用の禁止	○	○	○
第 20 条	適正な取得	○	○	○
第 21 条	取得に際しての利用目的の通知等	○	○	○
第 22 条	データ内容の正確性の確保等		○	○
第 23 条	安全管理措置		○	○
第 24 条	従業者の監督		○	○
第 25 条	委託先の監督		○	○
第 26 条	漏えい等の報告等		○	○
第 27 条	第三者提供の制限		○	○
第 28 条	外国にある第三者への提供の制限		○	○
第 29 条	第三者提供に係る記録の作成等		○	○
第 30 条	第三者提供を受ける際の確認等		○	○
第 32 条	保有個人データに関する事項の公表等			○
第 33 条	開示			○
第 34 条	訂正等			○
第 35 条	利用停止等			○
第 36 条	理由の説明			○
第 37 条	開示等の請求等に応じる手続			○

（問Ⅱ－４）「個人情報データベース等」とは何か。

（答）

「個人情報データベース等」とは、個人情報を含む情報の集合物であって、

① 特定の個人情報をコンピュータを用いて検索できるように体系的に構成したもの、又は

② コンピュータを用いていない場合であっても、五十音順に索引を付して並べられた顧客カード等、個人情報を一定の規則に従って整理することにより特定の個人情報を容易に検索することができるよう体系的に構成したものであって、目次、索引、符号等により一般的に容易に検索可能な状態に置かれているもの

をいいます（個人情報保護法第 16 条第１項、通則ガイドライン 2-4)。

（問Ⅱ－５）個人情報が五十音順等に整理されておらず、コンピュータを用いたデータベースにランダムに入力されているが、サーチ機能等で容易に検索が可能な場合には、当該データベースは「個人情報データベース等」に該当するのか。

（答）

「個人情報データベース等」のうちコンピュータを用いたものとは、特定の個人情報をコンピュータを用いて検索できるように体系的に構成したものをいいます（個人情報保護法第 16 条第１項第１号、通則ガイドライン 2-4）。

検索可能であれば、常に「個人情報データベース等」に該当するわけではありません。例えば、通常のコンピュータであれば、氏名等の文字を手がかりにしてテキスト情報に含まれる個人情報を検索することができますが、それだけでは「個人情報データベース等」には該当しません。個人情報としてのそれぞれの属性（氏名、生年月日等）に着目して検索できるように体系的に構成されている必要があります。

なお、コンピュータへの入力がランダムであっても、例えば、表計算ソフトにおいて、氏名の順番はランダムであるものの、列ごとに氏名列、住所列、借入金列というように体系的に構成されており、そのソート機能等を用いて、それらの個人情報を検索できるように再構成することが容易である場合には、「コンピュータを用いて検索できるように体系的に構成したもの」に当たり、「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。

（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。したがって、当該法人の代表者の氏名等は、「個人データ」に該当すると考えられます。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、（法人代表者の氏名等の）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」には該当しないこととなります。

（問Ⅱ－７）顧客から提出された書類と「個人データ」について、

① 契約書等の書類の形で本人から提出され、これからデータベースに登録しようとしている情報は「個人データ」に該当するか。

② データベースに登録した後の契約書等は「個人データ」に該当するか。

③　その後データベースから例えば紙にメモするなどして取り出された情報は、「個人データ」に該当するのか。それとも当該メモ自体が容易に検索可能な形で整理されていないのであれば、「個人データ」ではない「個人情報」として扱われるのか。

（答）

① 「個人データ」とは、「個人情報データベース等を構成する個人情報」をいいます（個人情報保護法第 16 条第3項）。データベース化されていない個人情報は、たとえ通常データベース管理される性質のもので、かつ、これからデータベース化される予定であったとしても、「個人データ」には当たりません。

② また、記載されている情報がデータベース化され、「個人データ」となったとしても、契約書等の書類そのものは、「個人情報データベース等を構成する」とはいえないため、「個人データ」には該当しません。

もっとも、当該契約書等が、ファイリングされるなどして、それ自体「特定の個人情報を容易に検索することができるよう体系的に構成したものであって、目次、索引、符号等により一般的に容易に検索可能な状態に置かれている」といえる場合には、当該契約書等は「個人情報データベース等を構成する」といえ、「個人データ」に該当します。

③ また、「個人情報データベース等」から紙面に出力されたものやそのコピーは、それ自体が容易に検索可能な形で体系的に整理された一部でなくとも、「個人データ」の「取扱い」の結果であり、個人情報保護法上の様々な規制がかかります。

「個人情報データベース等」から紙にメモするなどして取り出された情報についても、同様に「個人データ」に該当します。

なお、その出力されたものやそのコピーが、委託先や第三者に提供された場合は、当該委託先や第三者にとっては、（その出力されたものやコピーが容易に検索可能な形で体系的に整理されない限り）当該情報は「個人データ」には該当しないと考えられます（この場合、当該委託先や第三者にとっては、当該情報は個人情報又は個人関連情報に該当するものと考えられます）。ただし、委託元や第三者提供元にとっては、それらを委託・提供する行為は「個人データ」の「取扱い」であり、個人情報保護法上の様々な規制がかかります。

（問Ⅱ-8）「個人関連情報」とは何か。「個人関連情報」を第三者に提供する場合に留意すべき事項には、どのようなものがあるか。

（答）

「個人関連情報」とは、「生存する個人に関する情報であって、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」をいいます（個人情報保護法第２条第７項）。具体的には、ある個人の属性情報（性別・年齢・職業等）、ある個人のウェブサイトの閲覧履歴及びある個人の位置情報等が想定されます（いずれも「個人情報」に該当する場合は、「個人関連情報」には該当しないこととなります。）。なお、いわゆる統計情報は、特定の個人との対応関係が排斥されている限りにおいては、「個人に関する情報」ではないため、「個人関連情報」に該当しないこととなります。

個人関連情報取扱事業者は、「個人関連情報」（個人関連情報データベース等を構成するものに限る。）を第三者に提供する場合において、第三者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には、原則として、

① 当該第三者が個人関連情報取扱事業者から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の当該本人の同意が得られていること

② 外国にある第三者への提供にあっては、上記①の本人の同意を得ようとする場合において、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報が当該本人に提供されていること

をあらかじめ確認しなければならないとされています（個人情報保護法第 31 条第 1 項）。

（注）「個人関連情報を含む情報の集合物であって、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その他特定の個人関連情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの」を「個人関連情報データベース等」といい、「『個人関連情報データベース等』を事業の用に供している者」を「個人関連情報取扱事業者」といいます（個人情報保護法第 16 条第 7 項）。

すなわち、個人関連情報取扱事業者が、「個人関連情報」を第三者に提供する場合において、提供先の第三者が当該個人関連情報を「個人データ」として取得することが想定される場合には、個人データの第三者提供に準じた規制が課せられています。

Ⅲ　機微（センシティブ）情報

（問Ⅲ－１）金融分野ガイドライン第５条第１項第８号に規定する「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」とは、具体的にどのような場合を想定しているのか。

（答）

金融分野ガイドライン第５条第１項は、機微（センシティブ）情報を「法第２条第３項に定める要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活（これらのうち要配慮個人情報に該当するものを除く。）に関する情報（本人、国の機関、地方公共団体、学術研究機関等、法第 57 条第１項各号に掲げる者若しくは施行規則第６条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。）」と規定し、その取得、利用又は第三者提供を原則として禁止しています。

金融分野ガイドライン第５条第１項第８号は、機微（センシティブ）情報の取得、利用又は第三者提供について、①各種法令や社会通念等に照らして「適切な業務運営」と判断されること、②「本人の同意」があること、③「業務遂行上必要な範囲」内であることを要件としています。

例えば、金融機関が保険金の支払いや借り手の与信判断をするために、被保険者や借り手の健康状態に関する情報を各種法令や社会通念等に照らし適切といえる方法で、かつ保険金の支払いや与信判断のために必要な範囲内で、被保険者や借り手から同意を得て取得することが考えられます。反対に、保険金の支払いや借り手の与信判断のために本籍地等に関する情報を取得することは、「業務遂行上必要な範囲」内であるとは認められないことから、原則として、取得等を行うことはできないものと考えられます。ただし、業務遂行上、本籍地の取得等の必要性が認められる場合は、例外として本籍地の取得等が認められることもあり得ます。

また、金融機関においては、機微（センシティブ）情報について、金融分野ガイドラインに加え、銀行法等の各業法の施行規則が適用されることに留意する必要があります。

（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

（問Ⅲ－２）金融分野ガイドライン第５条第３項に規定する「機微（センシティブ）情報を、第１項に掲げる場合に取得、利用又は第三者提供する場合には、（中略）個人情報の保護に関する法令等に従い適切に対応しなければならないことに留意する」とは、具体的にどのような点に留意する必要があるのか。

（答）

金融分野ガイドライン第５条第３項については、機微（センシティブ）情報を、同条第１項に掲げる場合に取得、利用又は第三者提供する場合には、個人情報の保護に関する法令等の規制が前提となることを確認的に規定しているものです。

すなわち、機微（センシティブ）情報は、要配慮個人情報とそれ以外の情報によって構成されていますが、個人情報保護法においては、例えば、機微（センシティブ）情報のうち要配慮個人情報を取得するに当たっては、同法第 20 条第２項に従い、一定の場合を除いて、あらかじめ本人の同意を得なければならないこととされています。また、機微（センシティブ）情報を含むか否かを問わず、個人データを第三者提供するに当たっては、同法第 27 条第１項に従い、一定の場合を除いて、あらかじめ本人の同意を得なければならないこととされています。

このため、例えば、金融分野ガイドライン第５条第１項第５号から第７号には、「本人の同意に基づき」との記載はありませんが、同第５号から第７号の場合に機微（センシティブ）情報を取得する場合等には、上記のとおり個人情報の保護に関する法令等に従い適切に対応する必要があります。

（参考）

金融分野ガイドライン第５条第１項に規定する機微（センシティブ）情報については、「本人、国の機関、地方公共団体、学術研究機関等、法第 57 条第１項各号に掲げる者若しくは施行規則第６条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。」と規定されており、いわゆる公知なものや外形から明らかなものは機微（センシティブ）情報に該当せず、第５条第１項各号の規定は適用されません。

この点、要配慮個人情報のうち、いわゆる公知なものや外形から明らかなものについては、上記のとおり第５条第１項各号の規定は適用されませんが、個人情報保護法第２条第３項で規定する要配慮個人情報であることに変わりはないことから、個人情報の保護に関する法令等に従い適切に対応する必要があります。

（問Ⅲ－３）金融分野ガイドライン第５条第４項に規定する「機微（センシティブ）情報を第三者へ提供するに当たっては、法第 27 条第２項（オプトアウト）の規定を適用しないこととする」とは、機微（センシティブ）情報のうち要配慮個人情報を除く情報についても適用しないということか。

（答）

個人情報保護法第 27 条第２項において、個人データを構成する要配慮個人情報については、オプトアウト手続によって第三者提供することができないとされています。

機微（センシティブ）情報のうち要配慮個人情報を除く情報についても、情報の性質上特に慎重な取扱いが求められると考えられることから、要配慮個人情報と同様、オプトアウト手続によって第三者提供することは適切ではないこととするものです。

Ⅳ　安全管理措置等

（問Ⅳ－１）安全管理措置の内容は個人情報保護法と各業法のどちらでも義務化されているが、求められていることはどう違うのか。

（答）

各業法の体系において、監督指針等に以下の規定が盛り込まれていることからも分かるように、基本的に個人情報保護法の体系及び各業法の体系で求めている措置は同じです。ただし、措置の対象となっている情報の範囲などに若干の違いがあります。

○ 個人である顧客に関する情報については、各業法施行規則等の規定に基づき、その安全管理及び従業者の監督について、当該情報の漏えい、滅失又は毀損の防止を図るために必要かつ適切な措置として以下の措置が講じられているか。

・　金融分野ガイドライン第８条及び第９条の規定に基づく措置

・　実務指針Ⅰ、Ⅱ及び別添２の規定に基づく措置

○ 個人である顧客に関する情報の取扱いを委託する場合には、各業法施行規則等の規定に基づき、その委託先の監督について、当該情報の漏えい、滅失又は毀損の防止を図るために必要かつ適切な措置として以下の措置が講じられているか。

・　金融分野ガイドライン第 10 条の規定に基づく措置

・　実務指針Ⅲの規定に基づく措置

個人情報保護法では、安全管理措置の対象は「個人データ」とされています。したがって、例えば、金融機関自身の雇用管理情報や株主情報の中に含まれる個人データ、法人顧客に関する情報の中に含まれる個人データなど、個人顧客に関する情報でないものも措置の対象となります。なお、「個人データ」を対象とする安全管理措置の中には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる点に留意する必要があります。

一方、各業法の体系においては、安全管理措置の対象は「個人顧客情報」とされており、金融機関自身の雇用管理情報や株主情報の中に含まれる個人情報、法人顧客に関する情報の中に含まれる個人情報は、措置の対象外となります。

（問Ⅳ－２）なぜ個人情報保護法に加え、各業法で個人情報の安全管理が求められているのか。

（答）

個人情報保護法の体系（個人情報保護法－通則ガイドライン及び金融分野ガイドライン－実務指針等）は、個人の権利利益を保護することを目的としているもので、銀行法などの各業法の体系（法律－施行規則－監督指針等）は、金融機関の業務の公共性等に鑑み、その業務の健全かつ適切な運営を確保するという観点から、個人顧客情報の適正な管理を求めているものです。

個人情報保護法の体系に加え、各業法の体系においても個人顧客情報の安全管理措置等を求めていますが、具体的な措置の内容は、各業態の監督指針等において基本的に個人情報保護法の体系で求めている内容を準用しています。これには、個人情報保護法上の個人情報取扱事業者でもあり各業法の規制対象でもある金融機関が、二つの法規に服することによる混乱を回避するという意味があります。

（問Ⅳ－３）実務指針に基づき基本方針や取扱規程等を整備するにあたっては、いかなる事項をこれに盛り込む必要があるか。

（答）

実務指針は、個人情報取扱事業者が、安全管理に係る基本方針の整備、取扱規程等の整備、安全管理措置に係る実施体制の整備等を行うに当たり、事業者における「個人データ」の安全管理のために必要かつ適切な内容を盛り込むことを求めています。

事業者は、個人情報保護法第 23 条に基づき、「個人データ」の安全管理のために必要かつ適切な措置を講じる必要があるところ、安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とする必要があります。このため、事業者は、上記事情を考慮して、安全管理措置を講ずるための具体的な手法を決定し、これを基本方針や取扱規程等に盛り込む必要があります。

（問Ⅳ－４）実務指針１－２において整備することが求められている「個人データの安全管理に係る取扱規程」は、各事業者においては「細則」「マニュアル」等、名称や形式を問わないという理解でよいか。また、個々の規程の構成が実務指針と一致せずとも、当該事業者で定めるルール全体として実務指針に規定する措置に対応していれば、事業者全体の「個人データの安全管理に係る取扱規程」として問題ないか。

（答）

実務指針１－２で定める「個人データの安全管理に係る取扱規程」は、管理段階ごとに措置内容等を明確化することを求めるものであり、その名称や形式の統一を求めるものではありません。したがって、個々の規程の構成を実務指針の記載と一致させる必要は必ずしもないほか、管理段階ごとの取扱規程を、業務単位や商品単位ごとのように、実務に即して盛り込むことも可能です。ただし、その際には、事業者全体として、①実務指針７－１から７－６－１までに定められた事項が管理段階ごとに全て盛り込まれていること、②事業者内の部署や商品ごとに定めた規程において盛り込まない事項がある場合には合理的な理由があること、が求められます。

Ⅴ　漏えい等報告

(問Ⅴ-1)「個人データ」の「漏えい、滅失、毀損」とは、どのようなものを指すのか。具体的には、
① 「個人データ」を記録した電磁的記録媒体が破損したが、その内容と同じデータが他に保管されている場合は、「個人データ」の「滅失」又は「毀損」に当たるか。
② 従業員が「個人データ」を不正に持ち出して第三者に提供した場合、「個人データ」の「漏えい」に当たるか。また、どのような場合に、「個人データ」の「漏えい」が発生した「おそれ」が認められるか。
③ 「個人データ」を記録したUSBメモリを紛失した場合、「個人データ」の「漏えい」又は「滅失」に当たるか。
④ 「個人データ」が記録された電磁的記録媒体が盗難されたが、電磁的記録媒体にパスワードを設定していた場合も、「個人データ」の「漏えい」に当たるのか。
⑤ 暗号化処理された「個人データ」の復元キーを喪失したことにより、「個人データ」を復元できなくなった場合、「個人データ」の「毀損」に当たるのか。

（答）

「個人データ」の「漏えい」とは「個人データが外部に流出すること」、「滅失」とは「個人データの内容が失われること」、「毀損」とは「個人データの内容が意図しない形で変更されることや、内容を保ちつつも利用不能な状態となること」をいいます。

① 「個人データ」を記録した電磁的記録媒体が破損した場合、原則として個人データの「滅失」又は「毀損」に当たります。ただし、その内容と同じデータが他に保管されている場合には、当該「個人データ」の「内容」は失われていないと認められるため、「個人データ」の「滅失」又は「毀損」には当たりません。

（注）個人データを記録した携帯電話、ノートパソコン、PDA等についても、電磁的記録媒体と同様です。

② 従業員が「個人データ」を不正に持ち出して第三者に提供した場合、「個人データ」の「漏えい」に当たります。従業員による個人データの持ち出しの事案について、「漏えい」が発生したおそれがある事態に該当し得る事例としては、例えば、個人データを格納しているサーバや、当該サーバにアクセス権限を有する端末において、通常の業務で必要としないアクセスによりデータが窃取された痕跡が認められた場合が考えられます。

③ 「個人データ」を記録したUSBメモリを社内で紛失した場合には「個人データ」の「滅失」、社外で紛失した場合（社外に流失した場合）には、「個人データ」の「漏えい」に当たります。個別の事例ごとに判断することとなりますが、紛失場所が社内か社外か特定できない場合には、「個人データ」の「漏えい」（又は「漏えい」の「おそれ」）に該当すると考えられます。

④ 「個人データ」が記録された電磁的記録媒体が盗難された場合、「個人データ」の「漏えい」に当たります。これは、電磁的記録媒体にパスワードを設定していた場合も同様です。

⑤ 暗号化処理された「個人データ」の復元キーを喪失したことにより、「個人データ」を復元できなくなった場合、当該「個人データ」は「内容を保ちつつも利用不能な状態」となったと認められるため、「個人データ」の「毀損」に当たります。

（問Ⅴ-2）個人データ等の漏えい等が発生した場合、金融機関は個人情報保護委員会又は監督当局に報告する義務を負うか。

（答）

金融機関は、個人データ等の漏えい等が発生した場合、以下のとおり、個人情報保護委員会又は監督当局に報告する義務又は努力義務を負います。

⑴ 個人情報保護法に基づく報告（金融分野ガイドライン第 11 条第１項前段：義務規定）

個人情報保護法第 26 条第１項に基づき、個人情報保護法施行規則第７条各号に定める事態を知ったときは、通則ガイドライン 3-5-3 に従って、個人情報保護委員会、金融庁長官、財務局長、財務支局長又は都道府県知事に報告を行う必要があります（報告先については、問Ⅴ-３をご参照下さい）。

※個人情報保護法施行規則第７条各号に定める事態（通則ガイドライン 3-5-3-1）

① 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、又は発生したおそれがある事態

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

③ 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

④ 個人データに係る本人の数が 1,000 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

なお、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、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合には、報告を要しません。

※個人情報保護法施行規則第７条の「個人データ」の考え方（通則ガイドライン 3-5-1-1）

規則第７条は、法第 26 条第１項に基づく漏えい等の報告の対象となる事態について定めているところ、規則第７条に規定する「個人データ」とは、個人情報取扱事業者が取り扱う個人データをいう。

ただし、同条第３号に規定する「個人データ」には、「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」が含まれる。

そのため、同号に定める事態との関係では、「個人データ」は、個人情報取扱事業者が取り扱う個人データに加え、「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。

⑵ 各業法に基づく報告（金融分野ガイドライン第 11 条第１項後段：義務規定）

各業法（銀行法第 12 条の２・銀行法施行規則第 13 条の６の５の２等）に基づき、その取り扱う個人顧客に関する「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を知ったときは、監督当局に報告を行う必要があります（各業法等）。

なお、個人顧客に関する「個人データ」の漏えい等が、個人情報保護法施行規則第７条各号に定める事態にも該当する場合には、上記⑴の個人情報保護法に基づく報告も併せて行う必要があります。

（注）漏えい等が発生し、又は発生したおそれがある個人顧客に関する個人データについて、「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」が講じられている場合であっても、各業法に基づく報告を行う必要があります。

（注）金融機関自身の雇用管理情報や株主情報の中に含まれる個人データの漏えい等については、各業法、金融分野ガイドライン及び実務指針の対象外であるため、各業法に基づく報告（義務）、金融分野ガイドライン第 11 条第２項に基づく報告（努力義務）の対象とはなりません。

⑶　金融分野ガイドラインに基づく報告（金融分野ガイドライン第 11 条第２項：努力義務）

金融分野ガイドライン第 11 条第２項は、金融機関が取り扱う情報の性質やその取扱方法の特殊性等に鑑み、「金融分野における個人情報取扱事業者は、次に掲げる事態（前項に規定する事態を除く。）を知ったときは、同項の規定に準じて、監督当局に報告することとする。」との努力義務を定めています。

※金融分野ガイドライン第 11 条第２項に定める「次に掲げる事態」

①　その取り扱う個人情報の漏えい等が発生し、又は発生したおそれがある事態

②　その取り扱う仮名加工情報に係る削除情報等（法第 41 条第１項の規定により行われた加工の方法に関する情報にあっては、その情報を用いて仮名加工情報の作成に用いられた個人情報を復元することができるものに限る。）又は匿名加工情報に係る加工方法等情報の漏えいが発生し、又は発生したおそれがある事態

金融機関においては、金融分野ガイドライン第 11 条第２項に基づき、「法人顧客に関する個人データ」の漏えい等事案、「顧客（個人・法人を問わない）に関する個人情報」の漏えい等事案、「仮名加工情報に係る削除情報等」又は「匿名加工情報に係る加工方法等情報」の漏えい事案が発生した場合には、基本的には監督当局に報告することが望ましいと考えられます。

（表１）個人データ等の漏えい等の発生時における個人情報保護委員会又は監督当局への報告に関する規定

規定	対象となる情報	対象事業者	位置付け
⑴個人情報保護法に基づく報告	「個人データ」 （個人情報保護法施行規則第７条各号に該	個人情報取扱事業者	報告義務

	当する事態が生じたとき）		
⑵各業法に基づく報告	個人顧客に関する個人データ	各業法の適用を受ける全ての金融機関	報告義務
⑶金融分野ガイドラインに基づく報告（⑴⑵を除く）	・個人情報 ・仮名加工情報に係る削除情報等 ・匿名加工情報に係る加工方法等情報 （ただし、個人顧客に関する個人データを除く）	金融分野における個人情報取扱事業者	報告の努力義務

（表２）対象となる情報の整理（報告の義務がかかるのは網掛けの部分）

	個人に関する情報	
	「個人データ」	個人情報、削除情報等及び加工方法等情報
顧客	⑴の報告義務 ⑵の報告義務	⑶の努力義務
非顧客	⑴の報告義務（注） ⑶の努力義務（注）	⑶の努力義務（注）

（注）金融機関自身の雇用管理情報や株主情報の中に含まれる個人データの漏えい等について、個人情報保護法第 26 条第１項に基づき漏えい等報告を行う場合には、個人情報保護委員会に対して報告を行う必要があります。

また、金融機関自身の雇用管理情報や株主情報の中に含まれる個人データや個人情報等の漏えい等については、各業法、金融分野ガイドライン及び実務指針の対象外であるため、⑵の報告義務、⑶の努力義務の対象とはなりません。ただし、これらの情報であっても、漏えい等が発生し、金融機関の信用を害するおそれがある場合には、任意に監督当局へ報告していただくことが望ましいと考えます。

（問Ⅴ-3）個人データ等の漏えい等が発生した場合において、漏えい等報告を行う場合の報告先はどこか。

（答）

１．個人情報保護法に基づく報告（金融分野ガイドライン第 11 条第１項前段）

個人情報保護法第 26 条第１項に基づき漏えい等報告を行う場合の報告先は、以下のとおりとなります。

⑴ 個人情報保護法第 150 条第１項及び同条第４項の規定により同法第 26 条第１項の規定による権限が金融庁長官に委任されている事業者のうち、

・その権限を金融庁長官が行使することとなる事業者（各業法における監督権限を金融庁長官が行使することとされている事業者）は、金融庁長官に宛てて、金融庁の担当課室に報告書を提出してください。

・その権限が個人情報保護法第 150 条第６項又は第７項の規定により財務局長又は財務支局長に委任されている事業者（各業法における監督権限を財務局長又は財務支局長が行使することとされている事業者）は、当該事業者の主たる所在地を管轄する財務局長又は財務支局長に宛てて、各財務局又は財務支局の担当課に報告書を提出してください。

・個人情報保護法第 170 条の規定によりその権限に属する事務を地方公共団体の長（都道府県知事等）が行使することとなる事業者（各業法における監督権限を地方公共団体の長が行うこととされている事業者）は、地方公共団体の長に宛てて、各地方公共団体の担当部署に報告書を提出してください。

提出された報告書等については、個人情報保護委員会に共有されます。

⑵ 個人情報保護法第 150 条第１項及び同条第４項に基づき同法第 26 条第１項の規定による権限が金融庁長官に委任されていない事業者は、個人情報保護委員会に宛てて、個人情報保護委員会のホームページの報告フォームに入力する方法又は当該ホームページに別途示されている方法により、個人情報保護委員会事務局に報告書を提出してください。

（注）金融機関自身の雇用管理情報や株主情報の中に含まれる「個人データ」の漏えい等について、個人情報保護法第 26 条第１項に基づき漏えい等報告を行う場合には、個人情報保護委員会に対して報告を行う必要があります。

２．各業法に基づく報告（金融分野ガイドライン第 11 条第１項後段）

各業法に基づき漏えい等報告を行う場合の報告先は、各業法における権限の範囲に応じ、金融庁長官、財務局長、財務支局長又は地方公共団体の長となります。

各業法について、金融庁と他省庁の共管となっている場合には、当該他省庁に対しても報告書を提出する必要があります（問Ⅴ-12 参照）。

３．金融分野ガイドライン第 11 条第２項に基づく報告（努力義務）

金融分野ガイドライン第 11 条第２項に基づき漏えい等報告を行う場合の報告先は、上記２．と同様に、金融庁長官、財務局長、財務支局長又は地方公共団体の長となります。

事業者に適用される各業法が金融庁と他省庁の共管となっている場合には、上記２．と同様に、当該他省庁に対しても報告書を提出することが望ましいと考えられます（問Ⅴ-12 参照）。

（問Ⅴ－４）特定個人情報の漏えい等が発生した場合、金融機関は個人情報保護委員会又は監督当局に報告する義務を負うか。

（答）

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（以下「番号法」という。）第 29 条の４第１項に基づき、個人番号利用事務等実施者は、番号法第 29 条の４第１項及び第２項に基づく特定個人情報の漏えい等に関する報告等に関する規則第２条各号に定める事態を知ったときは、個人情報保護委員会に報告を行う必要があります（義務規定）。

※上記規則第２条各号に定める事態

① 次に掲げる特定個人情報（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。）の漏えい等が発生し、又は発生したおそれがある事態

イ 情報提供ネットワークシステム及びこれに接続された電子計算機に記録された特定個人情報

ロ 個人番号利用事務実施者が個人番号利用事務を処理するために使用する情報システムにおいて管理される特定個人情報

ハ 行政機関、地方公共団体、独立行政法人等及び地方独立行政法人が個人番号関係事務を処理するために使用する情報システム並びに行政機関、地方公共団体、独立行政法人等及び地方独立行政法人から個人番号関係事務の全部又は一部の委託を受けた者が当該個人番号関係事務を処理するために使用する情報システムにおいて管理される特定個人情報

② 次に掲げる事態

イ 不正の目的をもって行われたおそれがある特定個人情報の漏えい等が発生し、又は発生したおそれがある事態

ロ 不正の目的をもって、特定個人情報が利用され、又は利用されたおそれがある事態

ハ 不正の目的をもって、特定個人情報が提供され、又は提供されたおそれがある事態

③ 個人番号利用事務実施者又は個人番号関係事務実施者の保有する特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態

④ 次に掲げる特定個人情報に係る本人の数が 100 人を超える事態

イ 漏えい等が発生し、又は発生したおそれがある特定個人情報

ロ 番号法第９条の規定に反して利用され、又は利用されたおそれがある個人番号を含む特定個人情報

ハ 番号法第 19 条の規定に反して提供され、又は提供されたおそれがある特定個人情報

また、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）においては、特定個人情報を取り扱う事業者は、上記規則第２条各号の事態に該当しない漏えい等事案においても、個人情報保護委員会に報告するよう努めることとされています（努力義務）。

※上記規則第２条各号の事態に該当しない漏えい等事案

漏えい等又はそのおそれのある事案その他の番号法違反の事案又は番号法違反のおそれのある事案のうち、上記規則第２条各号の事態に該当しない事案

特定個人情報の漏えい等が発生した場合は、番号法に基づき、個人情報保護委員会に宛てて、個人情報保護委員会のホームページの報告フォームに入力する方法又は当該ホームページに別途示されている方法により、個人情報保護委員会事務局に報告書を提出してください。また、番号法第 29 条の４に基づく報告については、上記規則第３条に基づき速報・確報の２段階による報告が必要となります。

なお、特定個人情報の漏えい等が、「個人データ」の漏えい等にも該当する場合には、個人情報保護法又は各業法に基づく報告も併せて必要となる場合があります(問Ⅴ-2参照)。報告先については、問Ⅴ-３のとおりです。

(問Ⅴ-５) 個人情報等の漏えい等は、各業法上の「不祥事件」に該当するのか。

(答)

個人情報等の漏えい等が「不祥事件」に該当するか否かは、漏えい等の生じた経緯、漏えい等した情報の内容等から、各業法の規定に照らして個別に判断する必要があります。

なお、例えば、銀行法の体系では、「不祥事件」とは、銀行法施行規則第 35 条第 8 項に規定されている行為を行ったことをいい、これらに当てはまらない場合には、基本的に「不祥事件」には該当しません。

(問Ⅴ-6)個人データの漏えい等について、個人情報保護法第 26 条第１項の定める漏えい等報告の報告対象事態に該当するとともに、各業法の定める漏えい等報告の報告対象事態にも該当する場合には、どのように報告を行えばよいか。

(答)

双方の報告対象事態に該当する場合には、双方の法に基づく報告を行う必要があります。

ただし、一つの報告書を提出することで、双方の法に基づく報告を一括して行うことも可能です。双方の法に基づく報告を一括して行うための報告様式として、本Ｑ＆Ａ付属の（別紙様式１）を示します。また、ランサムウェア事案（「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和７年５月 28 日関係省庁申合せ）（以下「関係省庁申合せ」という。）２.（１）に規定するランサムウェア事案をいう。）に係る報告を行う場合には、（関係省庁申合せ 別添様式２）を用いることができます。

(問Ⅴ-７) 本Ｑ＆Ａ付属の様式又は（関係省庁申合せ 別添様式２）を用いて漏えい等報告を行う場合、本Ｑ＆Ａ付属の様式の根拠規定を記載する欄や（関係省庁申合せ 別添様式２）の「５.（４）本様式の届出先・報告の根拠規定等」の欄をどのように書けばよいか。

(答)

個人情報保護法に基づく報告の場合(問Ⅴ-２（１）参照）には、個人情報保護法第 26 条第１項を根拠条文として記載することになります。

各業法に基づく報告の場合(問Ⅴ－２（２）参照）には、各業法の報告義務に関連する条文（例：銀行法施行規則第 13 条の６の５の２、金融商品取引業等に関する内閣府令第 123 条第１項第６号の２）を根拠条文として記載することになります。

金融分野ガイドライン第 11 条第２項に基づく報告の場合(問Ⅴ－２（３）参照）には、金融分野ガイドライン第 11 条第２項を根拠条文として記載することとなります。

（注）問Ⅴ－６のとおり、一つの報告書を提出することで、個人情報保護法・各業法の双方の法に基づく報告を一括して行うことも可能です。この場合、当該報告書には、双方の法令上の根拠条文を並べて記載する必要があります。

（問Ⅴ－８）各業法に基づく監督当局への報告について、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データの漏えい等で、当該情報の量や性質等に鑑みて、漏えい等事案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へ報告する必要性があるのか。

（答）

個人顧客に関する個人データについては、各業法において「当該事態が生じた旨を金融庁長官等に速やかに報告することその他の適切な措置」を講じることとされており（義務規定）、金融機関は、その取り扱う個人顧客に関する個人データの漏えい等事案が発生した場合は、監督当局への報告その他の適切な措置を行う必要があります。

ここでいう「速やかに報告することその他の適切な措置」については、以下のとおり考えられます。

① 原則として、その取り扱う個人顧客に関する「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を知ったときは、「速やかに」（当該事態を知った時点から概ね３～５日以内を目安として）、その時点で把握している当該事態の概要等を監督当局に報告する必要があります。また、その後、当該事態の概要等が判明した場合には、判明次第、改めて監督当局に報告する必要があります。

② ＦＡＸの誤送信、郵便物等の誤送付、メールの誤送信等については、金融機関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等を検討し、「速やかに」報告を行う必要性が低いと判断したものであれば、業務の手続の簡素化を図る観点から、四半期に一回程度にまとめて監督当局に報告することも差し支えありません。

③ 郵便局員による誤配等、金融機関の責めに帰さない事案については、監督当局に報告する必要はないと判断いただいても差し支えありません。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は、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た上で、都度「速やかに」又は四半期に一回程度にまとめて報告を行う必要があります。

④ 他方で、いかなる場合でも、漏えい等事案の事実関係等を公表する場合には、都度「速やかに」監督当局に報告する必要があります。

（参考）各業法に基づく報告の様式は、法令等において特段指定をしておりませんが、一例として、本Ｑ＆Ａ付属の（別紙様式１）及び（別紙様式２）の様式を示します（軽微と思われるものについては、（別紙様式２）を参照してください。）。

（注）個人情報保護法に基づく報告の報告方法については、通則ガイドライン 3-5-3 をご参照下さい。

（問Ⅴ－９）各業法に基づく監督当局への報告について、どのような事項を報告書に記載すれば良いのか。

（答）

法令等において特段報告の様式を定めてはおりませんが、一例として、本Ｑ＆Ａ付属の（別紙様式１）の様式を示します。（別紙様式１）と同内容の情報を全て報告しなければならないというわけではありませんが、各業法における個人顧客情報の漏えい等報告に係る規定の趣旨にのっとり、必要十分な内容を監督当局に報告する必要があります。

なお、ランサムウェア事案に係る報告を行う場合には（関係省庁申合せ 別添様式２）を用いることができます（問Ⅴ－６参照）。また、個人情報保護法第 26 条第１項に基づく報告が必要な事案に該当しない場合において、（関係省庁申合せ 別添様式２）を用いるときは、（関係省庁申合せ 別添様式２）別紙１「（１）報告の種別」の記載は省略することができます。

また、漏えい等事案のうち、軽微なものについては、（別紙様式２）を一例として示します（問Ⅴ－８参照）。

（問Ⅴ-10）金融機関が本人同意を得て個人データを第三者に提供した後、提供先の第三者において当該個人データが漏えい等した場合、提供元の金融機関は漏えい等報告をする必要があるか。また、金融機関が個人データの取扱いの委託に伴って個人データを委託先に提供した後、委託先において当該個人データが漏えい等した場合、委託元の金融機関は漏えい等を報告する必要があるか。

（答）

金融機関が本人同意を得て「個人データ」を第三者に提供した後、提供先の第三者において当該「個人データ」が漏えい等したとしても、提供元の金融機関は漏えい等報告の義務を負いません。

他方、金融機関が個人データの取扱いの委託（個人情報保護法第 27 条第５項第１号）に伴って「個人データ」を委託先に提供した後、委託先において当該「個人データ」が漏えい等した場合には、原則として、委託元と委託先の双方が漏えい等報告の義務を負うことになります（通則ガイドライン 3-5-3-2）。

（問Ⅴ-11）各業法に基づく監督当局への報告について、金融分野とそれ以外の分野の事業を行っている場合において、金融分野以外の事業において取り扱う個人データ等の漏えい等が発生した場合も、各業法に基づき監督当局に報告する必要があるのか。

（答）

各業法、金融分野ガイドライン及び実務指針は、金融分野における個人情報の取扱いを対象としています。このため、金融分野以外の事業において取り扱う個人データ等の漏えい等が発生したとしても、各業法に基づき、監督当局に報告する必要はありません。

（問Ⅴ-12）事業者に適用される各業法が金融庁と他省庁の共管となっている場合、金融分野ガイドライン第 11 条第１項後段及び同条第２項に基づき報告する場合は、所管しているいずれかの省庁に報告すれば、他の省庁への報告は必要ないのか。

（答）

各業法に基づく報告（金融分野ガイドライン第 11 条第１項後段）について、当該業法が金融庁と他省庁の共管となっている場合には、各業法で報告先として規定する監督当局及び当該他省庁の双方に対して、報告をする必要があります（問Ⅴ－３参照）。

また、金融分野ガイドライン第 11 条第２項に基づく報告について、事業者に適用される各業法が金融庁と他省庁の共管となっている場合には、上記と同様、監督当局及び当該他省庁の双方に対して、報告をすることが望ましいと考えられます（問Ⅴ－３参照）。

（問Ⅴ-13)個人データ等の漏えい等が発生した場合、金融機関は本人に通知する義務を負うか。

（答）

金融機関は、個人データ等の漏えい等が発生した場合、以下のとおり、本人に通知等する義務又は努力義務を負います。

⑴ 個人情報保護法に基づく通知等（金融分野ガイドライン第 11 条第３項前段：義務規定）

個人情報保護法第 26 条第２項に基づき、個人情報保護法施行規則第７条各号に定める事態を知ったときは、通則ガイドライン 3-5-4 に従って、本人への通知を行う必要があります。本人への通知が困難である場合は、本人の権利利益を保護するために必要な代替措置を講ずることによる対応が認められます。

※個人情報保護法施行規則第７条各号に定める事態（通則ガイドライン 3-5-3-1）

① 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、又は発生したおそれがある事態

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

③　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

④　個人データに係る本人の数が 1,000 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

なお、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、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合には、本人への通知等を要しません。

⑵　金融分野ガイドラインに基づく通知等（金融分野ガイドライン第 11 条第３項後段：努力義務）

金融分野ガイドライン第 11 条第3項後段は、金融機関が取り扱う情報の性質やその取扱方法の特殊性等に鑑み、「金融分野における個人情報取扱事業者は、次に掲げる事態（施行規則第7条各号に定める事態を除く。）を知ったときも、これに準じて、本人への通知等を行うこととする。」との努力義務規定を定めています。

金融機関が取り扱う情報の性質等に鑑みれば、基本的には全ての漏えい等事案について本人への通知等を行うことが望ましいと考えられます。

なお、本人への通知が困難である場合には、代替措置として、事案の公表を行うことも考えられます。また、例えば、漏えい等した個人データについて、高度な暗号化等の秘匿化措置が講じられている場合や、漏えいした個人データを即時に回収した場合等、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、本人への通知を要しないものと考えられます。

※金融ガイドライン第 11 条第３項後段に定める「次に掲げる事態」

①　その取り扱う個人データ（仮名加工情報である個人データを除く。）の漏えい等が発生し、又は発生したおそれがある事態

②　その取り扱う個人情報（仮名加工情報である個人情報を除く。）の漏えい等が発生し、又は発生したおそれがある事態

③　その取り扱う仮名加工情報に係る削除情報等（法第 41 条第１項の規定により行われた加工の方法に関する情報にあっては、その情報を用いて仮名加工情報の作成に用いられた個人情報を復元することができるものに限る。）又は匿名加工情報に係る加工方法等情報の漏えいが発生し、又は発生したおそれがある事態

（問Ⅴ-14）「個人データ」の漏えい等が発生した場合、事実関係及び再発防止策等について、公表すべきか。

（答）

個人情報取扱事業者は、「個人データ」の漏えい等が発生した場合、漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表することが望ましいと考えられます（通則ガイドライン 3-5-2）。

また、金融分野ガイドライン第 11 条第４項は、金融機関が取り扱う情報の性質やその取扱方法の特殊性等に鑑み、その取り扱う個人情報の漏えい等が発生した場合においても、「当該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、当該事案等の事実関係及び再発防止策等について、速やかに公表することとする。」との努力義務規定を定めています。金融機関が取り扱う情報の性質等に鑑みれば、基本的には全ての事案について速やかに公表することが望ましいと考えられます。

なお、例えば、インターネット上の掲示版等に漏えいした個人データがアップロードされており、個人情報取扱事業者において当該掲示板等の管理者に削除を求める等、必要な初動対応が完了しておらず、事実関係等を公表することで、かえって被害が拡大することが想定される場合等においては、当該時点（必要な初動対応が完了していない時点）において公表を行う必要はないと考えられます。

Ⅵ　第三者提供等

（問Ⅵ－１）防犯カメラに映った偽造キャッシュカードの実行犯の映像情報を本人の同意なく他の金融機関に提供することは、個人情報保護法上問題がないか。

（答）

防犯カメラに映った映像情報も、それによって特定の個人が識別される場合は、「個人情報」に該当します（個人情報保護法第２条第１項）。

その場合、原則として個人情報の利用目的を本人に通知又は公表しなければなりませんが、「取得の状況からみて利用目的が明らかであると認められる場合」には、その利用目的を公表等する必要がないとされており（個人情報保護法第 21 条第４項第４号）、一般に、防犯目的のためにビデオカメラを設置し撮影する場合は、「取得の状況からみて利用目的が明らか」であると認められるものと解されます。

ただし、特定の個人を識別できる防犯カメラの映像情報を他の金融機関に提供する場合については、「取得の状況からみて利用目的が明らか」であり、利用目的の範囲内といえるかは、状況に応じ判断されることになります。

しかし、仮に当該情報提供が利用目的を超えた利用に当たるとしても、偽造キャッシュカードの実行犯の映像情報を他の金融機関に提供する場合は、個人情報保護法第 18 条第3項第2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）に該当するため、本人の同意を得ることなく当該映像情報を他の金融機関に提供することができるものと考えられます。

なお、特定の個人を識別できる防犯カメラの映像情報は「個人情報」には該当しますが、特定の個人情報を検索することができるように「体系的に構成」されたものでない限り、個人情報データベース等には該当しないと解されます。すなわち、記録した日時について検索することは可能であっても、特定の個人に係る映像情報について検索することができない場合には、個人情報データベース等には該当せず、個々の映像情報は「個人データ」には該当しないと解されます。また、仮に個々の映像情報が「個人データ」に該当し、個人情報保護法第 27 条の第三者提供の制限の規定の対象となる場合であっても、個人情報保護法第 27 条第１項第2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）に該当するため、本人の同意を得ることなく当該映像情報を他の金融機関に提供することができるものと考えられます。

（問Ⅵ－２）「個人データ」に該当する顧客の取引内容を、本人の同意を得ずに、その内容を知る家族に伝えることはできるか。

（答）

個人情報取扱事業者は、一定の場合を除き、あらかじめ本人の同意を得ないで、「個人データ」を「第三者」に提供することを禁じられています（個人情報保護法第 27 条第１項）。本人の同意を得ずに、「第三者」に「個人データ」を提供した場合、「第三者」が当該「個人データ」の内容をあらかじめ知っていたか否かにかかわらず、個人情報保護法第 27 条第１項に違反することとなります。

ここで、「第三者」とは「個人データ」を提供しようとする個人情報取扱事業者及び当該「個人データ」に係る本人のいずれにも該当しない者をいい、本人の家族であっても、「第三者」に該当します。よって、「個人データ」に該当する顧客の取引内容を本人の同意を得ずに、その内容を知る家族に伝えた場合、個人情報保護法第 27 条第１項に違反することとなります（なお、ここにいう「本人の同意」における「本人」については、未成年者又は成年被後見人の法定代理人が含まれると考えられます。）。

ただし、明示的な同意がなくとも、例えば、本人が家族を連れて金融機関に融資の申込みをしに来た際に入手した情報を、後日当該家族に伝える場合等、本人が当該家族等に対する個人データの提供に同意していると判断できる場合は、個人情報保護法第 27 条第１項に違反しないこととなります。

（注）個人情報保護法第 27 条第１項は、本人の同意を得ないで「個人データ」を第三者に提供し得る一定の場合として、

① 法令に基づく場合（第１項第１号）、

② 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、本人の同意取得が困難な場合（第１項第２号）、

等を掲げています。なお、個人情報保護法第 27 条第１項に規定する「法令」には、「条例」も含まれます。

（問Ⅵ-３）金融分野ガイドライン第３条で、個人情報保護法第 18 条、第 27 条、第 28 条及び第 31 条に定める本人の同意を得る場合には、原則として、書面によらなければならないとされているが、「紙」を用いた同意以外に、例えば、どのような形式が「書面」に該当するのか。また、電話により同意を得た事実を任意様式に記録し保存する方式でも金融分野ガイドライン上「書面」による同意を得たと解することができるか。

（答）

金融分野における個人情報取扱事業者は、個人情報保護法第 18 条、第 27 条、第 28 条及び第 31 条に定める本人の同意を得る場合には、原則として、書面によることとされています（金融分野ガイドライン第３条）。

金融分野ガイドラインにおいて「書面」は「電磁的記録を含む。」とされており、また、個人情報保護法第２条第１号において「電磁的記録」は「電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。」とされています。一般に想起される「紙」のみを「書面」として定める趣旨ではなく、「同意に関し、本人の意思が明確に反映できる方法による確認が可能であり、かつ、事後的に検証可能な方法」であれば、「書面」と認められると解されます。

このため、インターネットの画面上で顧客に同意欄をクリックさせる方法、自動音声ガイドによるプッシュホン操作の電子記録、電話により同意を取得し、それを録音するなどの方法等も金融分野ガイドライン第３条に規定された「書面」の一つの例と考えられます。

他方、電話により同意を得た事実を個人情報取扱事業者が任意様式に記録し保存する方法では、「本人の意思が明確に反映できる方法により確認が可能」とも、「事後的に検証可能」ともいえないため、金融分野ガイドライン第３条に規定された「書面」による同意には該当しないと考えられます。

ただし、上記の任意様式に記録する方法で保存したものについて、その後に本人からその内容について署名等で確認を得ている場合等は、「同意に関し、本人の意思が明確に反映できる方法による確認が可能であり、かつ、事後的に検証可能な方法」といえるため、金融分野ガイドライン第３条に規定された「書面」による同意に該当すると考えられます。

（問Ⅵ－４）債権譲渡の実務においては、債権の譲渡人は譲受人に対し、債権者としての十分な管理回収を行わせしめ、譲渡人及び譲受人の経済的利益を保護するため、債権そのものに加えて債務者に関連する個人情報を移転することが不可欠であるが、こうした場合にも、個人情報保護法上、債務者本人から第三者に提供することについて明示的な同意を得ることが必要なのか。

（答）

債権譲渡に際しての債務者に係る「個人データ」の取扱いについては、以下のような整理が可能であると考えられます。

債権譲渡に付随して譲渡人から譲受人に対して当該債権の管理に必要な範囲において債務者及び保証人等に関する「個人データ」が提供される場合には、個人情報保護法第 27 条により求められる第三者提供に関する本人の同意を事実上推定できるため、改めて明示的に本人の同意を得る必要は個人情報保護法上ないものと解されます。

ただし、上記解釈は、債務者が民法第 466 条第２項に基づく譲渡制限特約(注)を求めていないことを根拠としており、例えば、債権譲渡に伴い第三者提供される「個人データ」の本人が、譲渡制限特約を結ぶことを要求できない立場にある場合等については、同意の事実上の推定が及ばない可能性があることに留意する必要があります。

また、「債権の管理」とは譲渡及び回収等をいいます。そのため、「個人データ」が当該債権の譲渡及び回収等に必要といえるか否かについて、譲渡人等の側で慎重な検討が必要です。仮に、同じ債務者等に関する「個人データ」であっても、当該債権の管理に必要であるという合理的な説明ができない場合は、同意の推定は及ばないものと考えられます。

なお、本人たる債務者又は保証人等が債権譲渡に伴う「個人データ」の第三者提供について明示的に拒否する意思を示し、これにより、当該債権の管理に支障を来し、債権の譲渡人又は譲受人の財産等の保護のために必要な場合には、個人情報保護法第 27 条第１項第２号の定めに該当するため、本人たる債務者等の同意なく当該「個人データ」を債権の譲受人に提供することができるものと解されます。

ただし、当該債権の管理に支障を来すか否かの判断は個別具体的な状況によるため、それが否定されれば、当該データの譲受人への提供は個人情報保護法第 27 条に違反したものとなることに留意が必要です。

以上については、証券化の場合にも適用され得ると考えます。証券化の前提である債権の譲渡に関連して行われるデューデリジェンスや譲受人の選定等、当然必要な準備行為についても、（債権の管理に必要な範囲に含まれるものとして）同意の事実上の推定が及ぶものと解されます。

したがって、債権譲渡の準備行為のため、当該債権の債務者等に関する情報を、譲渡先候補者に対して開示することについても、当該「個人データ」の開示が、債権譲渡のために「当然必要な準備行為」であり、「債権の管理に必要な範囲に含まれる」と認められる場合には、債権の譲渡人等の側で合理的に説明できる限りにおいて同意の事実上の推定が及ぶものと解されます。

（注）民法第 466 条第１項では、「債権は、譲り渡すことができる。ただし、その性質がこれを許さないときは、この限りでない。」とされており、第２項では、「当事者が債権の譲渡を禁止し、又は制限する旨の意思表示（以下「譲渡制限の意思表示」という。）をしたときであっても、債権の譲渡は、その効力を妨げられない。」とされ、第３項では、「前項に規定する場合には、譲渡制限の意思表示がされたことを知り、又は重大な過失によって知らなかった譲受人その他の第三者に対しては、債務者は、その債務の履行を拒むことができ、かつ、譲渡人に対する弁済その他の債務を消滅させる事由をもってその第三者に対抗することができる。」とされています。また、民法第 466 条の５第１項では、「預金口座又は貯金口座に係る預金又は貯金に係る債権（以下「預貯金債権」という。）について当事者がした譲渡制限の意思表示は、第 466 条第２項の規定にかかわらず、その譲渡制限の意思表示がされたことを知り、又は重大な過失によって知らなかった譲受人その他の第三者に対抗することができる。」とされています。民法においては、このように債権の自由譲渡性が保証されており、譲渡できない性質を有する、あるいは一部の譲渡制限特約が付されている債権を除き、債務者の意思にかかわらず譲渡することが可能となっており、債権譲渡を禁止又は制限したい場合には債務者は譲渡制限の意思表示をすることが必要とされています。したがって、債務者がこのような譲渡制限の意思表示をすることが可能であるにもかかわらず、それをしていない場合には、個人情報保護法第 27 条により求められる個人データの第三者提供に関する債務者本人の同意を事実上推定できると考えられます。

（注）個人情報保護法における「本人の同意」の解釈については、通則ガイドライン 2-16 を参照。同意の事実上の推定は、例外的な局面で認められ得るに過ぎないものであるため、十分御留意ください。

（問Ⅵ-５）生活保護の適正な実施のために行う調査の一環として、社会福祉事務所員から生活保護申請者の資産や収入状況等の個人データの提供を要請された場合において、本人の同意を得ずに、当該要請に応じて個人データを提供することはできるか。

（答）

個人情報取扱事業者は、一定の場合を除き、あらかじめ本人の同意を得ないで、「個人データ」を第三者に提供することを禁じられています（個人情報保護法第 27 条）。

一方、生活保護の適正な実施のためには、生活保護申請世帯及び生活保護受給世帯の資産及び収入の状況把握が不可欠です。そのため、生活保護法（昭和 25 年法律第 144 号）第 29 条は、保護の決定若しくは実施又は同法第 77 条若しくは第 78 条の規定の施行のために必要があるときは、保護の実施機関及び福祉事務所長が、要保護者又は被保護者であった者及びその扶養義務者の資

産、収入及び支出の状況等につき、銀行、信託会社、要保護者又は被保護者であった者及びそれらの者の扶養義務者の雇主その他の関係人に、報告を求めることができる旨が規定されています。

当該規定に基づく任意調査について、法令の規定で情報の提供そのものが義務付けられているわけではありませんが、第三者（福祉事務所長）が情報の提供を受けることについて法令上の具体的な根拠があるところであり、当該要請に応じて個人データを福祉事務所長に提供することは、個人情報保護法第 27 条第1項第1号における「法令に基づく場合」に該当するため、個人データを提供する際に本人の同意を得る必要はありません。

（問Ⅵ-６）未払賃金立替払制度（賃金の支払の確保等に関する法律第７条）の適正な実施のために行う調査の一環として、倒産した事業主の賃金支払い能力の有無を把握するために、労働基準監督署から、倒産会社及びその代表者、個人事業主等の関係者が保有する預金口座の残高状況や賃金未払期間における保有預金口座の取引状況等の個人データの提供を要請された場合において、本人の同意を得ずに、当該要請に応じて個人データを提供することはできるか。

（答）

個人情報取扱事業者は、一定の場合を除き、あらかじめ本人の同意を得ないで、「個人データ」を第三者に提供することを禁じられています（個人情報保護法第 27 条）。

一方、未払賃金立替払制度（賃金の支払の確保等に関する法律（昭和 51 年法律第 34 号）第７条）の適正な実施のためには、倒産した事業主の賃金支払い能力の有無を把握するために、倒産会社及びその代表者、個人事業主等の関係者が保有する預金口座の残高状況や賃金未払期間における保有預金口座の取引状況等を把握することが不可欠です。そのため、賃金の支払の確保等に関する法律第 12 条の２第１項は「都道府県労働局長、労働基準監督署長又は労働基準監督官は、この法律の施行に関し、関係行政機関又は公私の団体に対し、資料の提供その他必要な協力を求めることができる。」と規定し、また同条第２項は「前項の規定による協力を求められた関係行政機関又は公私の団体は、できるだけその求めに応じなければならない。」と規定しています。

賃金の支払の確保等に関する法律第 12 条の２第１項に基づく要請に応じて労働基準監督署長に個人データを提供することは、個人情報保護法第 27 条第1項第1号における「法令に基づく場合」に該当するため、個人データを提供する際に本人の同意を得る必要はありません。

（問Ⅵ-７）個人情報取扱事業者が、弁護士法第 23 条の２に基づいてなされる報告の請求を弁護士会から受けた場合において、本人の同意を得ずに、当該報告の請求に応じて個人データを弁護士会に提供することはできるか。

（答）

個人情報取扱事業者は、一定の場合を除き、あらかじめ本人の同意を得ないで、「個人データ」を第三者に提供することを禁じられています（個人情報保護法第 27 条）。

一方、弁護士法（昭和 24 年法律第 205 号）第 23 条の２は、弁護士が、受任している事件について、所属弁護士会に対し、公務所又は公私の団体に照会して必要な事項の報告を求めることを申し出ることができ、当該報告請求の申出を受けた弁護士会は、当該申出が適当でないと認める

ときは、その拒絶をすることができ、そうでない場合は、当該申出に基づいて、公務所又は公私の団体に照会して必要な事項の報告を求めることができる旨を規定しています。

当該規定に基づき、弁護士会が公務所等に対して照会を行った場合、一般的には、報告することによって得られる公共的利益が報告しないことによって守られる秘密、プライバシー、名誉等の利益を上回ると認められる場合において、公務所等に弁護士会に対する報告義務があると考えられることは、複数の判例も認めるところです。したがって、第三者（弁護士会）が情報の提供を受けることについて法令上の具体的な根拠があることから、弁護士会からの照会に対する回答は、個人情報保護法第 27 条第１項第１号における「法令に基づく場合」に該当するため、当該報告の請求に応じて個人データを提供する際に本人の同意を得る必要はないものと考えられます。

ただし、弁護士会の前歴照会に区長が応じて、公権力の違法な行使に当たるとされた判例（最高裁判所昭和 56 年４月 14 日最高裁第三小法廷判決）にも見られるように、具体的な報告内容によっては、プライバシー権の侵害等を理由に損害賠償請求が認容されるおそれがあることから、報告を行う際にあらかじめ本人からの同意を得ることが望ましいですし、仮に同意が得られない場合に報告に応じるか否かは、その照会の理由や当該個人情報の性質等に鑑み、個別の事案ごとに慎重に判断をする必要があると考えられます。

（問Ⅵ-８）本人の同意に基づいて外国にある第三者に個人データを提供する場合、具体的にどのような点に留意する必要があるのか。

（答）

個人情報取扱事業者は、外国（注 1）にある第三者に個人データを提供する場合、本人に以下の情報を提供した上で、本人から当該第三者への個人データの提供を認める旨の同意を得る必要があります（個人情報保護法第 28 条第１項及び第２項並びに個人情報保護法施行規則第 17 条第２項）。

①当該外国の名称
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の保護に関する制度に関する情報（注２）（注３）
③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

この際、金融分野ガイドライン第 13 条第１項は、金融分野における個人情報取扱事業者は、個人情報保護法施行規則第 17 条第２項から第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、以下の情報を提供することと規定（努力義務）しています。

④個人データの提供先の第三者
⑤提供者の第三者における利用目的
⑥第三者に提供される個人データの項目

また、金融分野ガイドライン第 13 条第１項は、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取得するに当たり、あらかじめ作成された同意書面を用いる場合には、外国にある第三者への提供に関する条項が他の個人情報の取扱いに関する条項と明確に区別され、本人に理解されることが望ましいとしています。具体的には、例えば、文字の大きさやフォントを変えるほか、Web ページで本人の同意を得る場合は他の個人情報の取扱いに関する条項とチェックボックスを分けることが考えられます。

これらの他、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い場合の対応は問Ⅵ-９、個人情報保護法第４章第２節の規定により個人情報取扱事業者が講ずべき措置に相当する措置（以下「相当措置」という。）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法施行規則第 16 条に定める基準に適合する体制（以下「基準適合体制」という。）を整備していることを根拠として外国にある第三者に個人データを提供する場合の対応は問Ⅵ-10 を参照してください。

（注１）「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等」（平成 31 年個人情報保護委員会告示第１号）に定める国は除きます。具体的には、令和３年９月時点で EU（アイスランド、アイルランド、イタリア、エストニア、オーストリア、オランダ、キプロス、ギリシャ、クロアチア、スウェーデン、スペイン、スロバキア、スロベニア、チェコ、デンマーク、ドイツ、ノルウェー、ハンガリー、フィンランド、フランス、ブルガリア、ベルギー、ポーランド、ポルトガル、マルタ、ラトビア、リトアニア、リヒテンシュタイン、ルーマニア及びルクセンブルク）及び英国が該当します。（外国第三者提供ガイドライン３参照。）

（注２）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た上で当該第三者に個人データを提供した後に、当該外国における個人情報の保護に関する制度の変更があり、我が国の個人情報保護法との間の本質的な差異の認識に影響を及ぼすような重要な変更がなされたことを提供元の事業者が認識した場合には、本人に情報提供することが望ましいと考えられます。

（注３）個人情報保護委員会では、一定の国又は地域における個人情報の保護に関する制度について調査し、我が国の個人情報保護法との間の本質的な差異の把握に資する一定の情報を公表しています。

個人情報保護法第 28 条第２項の趣旨には、外国にある第三者に対する個人データの提供に伴うリスクについて、本人の予測可能性を高めるという点のほか、外国にある第三者に対して個人データを提供する個人情報取扱事業者においても、従前以上に、提供先の外国にある第三者における事業環境等を認識することを促すという点が含まれます。また、個人情報取扱事業者が同項に基づいて本人に対して提供すべき情報の具体的内容は、個別の事案に応じて異なり得ます。したがって、個人情報保護法施行規則第 17 条第２項第２号に基づく「適切かつ合理的な方法」による確認は、外国にある第三者に対して個人データを提供する個人情報取扱事業者の責任において行うべきものであり、個人情報保護委員会が提供する情報は、あくまで補助的なものとして参照する必要があります。もっとも、当該事業者が当該外国における個人情報の保護に関する制度に関する情報について一般的な注意力をもって適切かつ合理的な方法により確認を尽くした結果、当該事業者として本人に提供すべき情報が、上

記のとおり個人情報保護委員会が補助的なものとして提供する情報（以下「委員会提供情報」といいます。）と同じであった場合には、当該委員会提供情報を個人情報保護法施行規則第17条第２項第２号の「適切かつ合理的な方法」により得られた情報として本人に提供することは考えられます。なお、当該事業者が、当該委員会提供情報以外にも個人情報保護法施行規則第17条第２項に基づいて本人に対して提供すべき情報を保有している場合には、当該情報も本人に対して提供する必要があります。

また、その場合、当該事業者は、当該委員会提供情報の掲載されたWebページのURLを自社のホームページに掲載し、当該URLの指定するWebページに掲載された情報を本人に閲覧させる方法も、個人情報保護法施行規則第17条第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を同意書面の本人にとって分かりやすい場所に掲載するほか、紙媒体の同意書面を用いる場合には当該URLの近くにQRコードを掲載すること等により、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の指定するWebページ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。

（参考）

「外国における個人情報の保護に関する制度等の調査」（個人情報保護委員会ウェブサイト）
https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#gaikoku

（問Ⅵ-９）外国にある第三者への個人データの提供に関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が所在する外国が特定できない場合、具体的にどのような点に留意する必要があるか。

（答）

個人情報取扱事業者は、外国にある第三者への個人データの提供に関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が所在する外国が特定できない場合、本人に以下の情報を提供した上で、本人から当該第三者への個人データの提供を認める旨の同意を得る必要があります（個人情報保護法第28条第１項及び第２項並びに個人情報保護法施行規則第17条第３項）。

①当該外国が特定できない旨及びその理由（提供先が定まる前に、本人同意を得る必要性を含みます。）
②当該外国の名称に代わる本人に参考となるべき情報（移転先となる外国の候補等）

この際、移転先となる外国の候補が具体的に定まっており、当該外国の名称に代わる本人に参考となるべき情報の提供が可能であるにもかかわらず、これを本人に情報提供しなかった場合は、適法な情報提供とは認められません。このため、個人情報取扱事業者は、個人情報保護法施行規則第17条第２項から第４項までの規定により情報提供が求められる事項について本人に改めて情報提供した上で、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る必要があります。

また、金融分野ガイドライン第 13 条第２項は、金融分野における個人情報取扱事業者は、事後的に提供先の第三者が所在する外国を特定できた場合には、本人の求めに応じて、以下の①及び②の情報を、事後的に提供先の第三者が講ずる個人情報の保護のための措置についての情報提供が可能となった場合には、本人の求めに応じて、以下の③の情報を、本人に提供することと規定（努力義務）しています（外国第三者提供ガイドライン 5-3 参照）。また、このような情報提供の求めが可能である旨を同意書面における記載を通じて本人に認識させるとともに、金融分野ガイドライン第 20 条に定める「個人情報保護宣言」（プライバシーポリシー等）に記載の上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、公表することと規定（努力義務）しています。

①当該外国の名称
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の保護に関する制度に関する情報
③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

さらに、この場合、金融分野ガイドライン第 13 条第４項は、金融分野における個人情報取扱事業者は、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、当該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こと等により、公表するとともに、定期的（年に１回程度又はそれ以上の頻度）に更新することが望ましいと規定（努力義務）しています。

（問Ⅵ-10）外国にある第三者に個人データを提供する際、基準適合体制を整備していること根拠として当該第三者に個人データを提供する場合、具体的にどのような点に留意する必要があるのか。

（答）

金融分野における個人情報取扱事業者は、基準適合体制を整備していることを根拠として外国にある第三者に個人データを提供する場合には、当該提供の時点で、当該第三者による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内容、当該外国の制度が存在する場合においては、当該第三者による相当措置の継続的な実施の確保の可否を、適切かつ合理的な方法により、確認する必要があります。

また、金融分野における個人情報取扱事業者は、基準適合体制を整備していることを根拠として外国にある第三者に個人データを提供した後は、個人情報保護法第 28 条第３項に従い、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必要があります。具体的には、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（年に１回程度又はそれ以上の頻度）に確認すること等が求められます（外国第三者提供ガイドライン 6-1 参照）

この際、金融分野ガイドライン第 13 条第３項は、金融分野における個人情報取扱事業者は、当該第三者による相当措置の実施状況を確認するにあたり、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（当該第三者からホワイトペーパー等の形で報告を受け、それ

を参照することにより、当該第三者による相当措置の実施状況を確認できる場合を含みます。）により確認を行うことと規定（努力義務）しています。なお、これらの方法は、外国にある第三者に提供する個人データの規模及び性質並びに個人データの取扱状況等に起因するリスクに応じたものとする必要があります。

また、基準適合体制を整備していることを根拠として外国にある第三者に個人データを提供した場合は、本人の求めに応じて、当該必要な措置に関する情報を本人に提供する必要があります（個人情報保護法第 28 条第３項）。金融分野ガイドライン第 13 条第３項は、金融分野における個人情報取扱事業者は、本人の求めに応じて事後的に情報を提供する旨を個人情報保護宣言に記載の上インターネットのホームページへの常時掲載等により、公表することと規定（努力義務）しています。

さらに、金融分野ガイドライン第 13 条第４項は、金融分野における個人情報取扱事業者は、基準適合体制を整備していることを根拠として外国にある第三者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こと等により、公表するとともに、定期的（年に１回程度又はそれ以上の頻度）に更新することが望ましいと規定（努力義務）しています。