2019 年 6 月 26 日　全 10 頁

# 今さら聞けない個人情報保護法のＱ＆Ａ⑤

## 金融関連分野での扱いはどうなっているの？

金融調査部　研究員
藤野　大輝

［要約］

- ここもと、個人情報の保護に関する制度改正が、国内外で相次いでいる。わが国では、2015 年 9 月に個人情報保護法が改正され、2017 年 5 月 30 日から全面施行されている。個人の医療情報に関しては、別途、次世代医療基盤法が 2017 年 5 月に公布され、2018 年 5 月 11 日から施行されている。海外では EU で GDPR（EU 一般データ保護規則）が 2018 年 5 月 25 日から施行されている。

- 本シリーズでは、改正された個人情報保護法に関する基本的な事項をＱ＆Ａ形式で紹介する。

- 今回は、金融分野の個人情報取扱事業者が個人データを取り扱う際に、特に気を付けなければならない点について取り上げる。

【目次】

## はじめに

個人情報の利活用が活発化しており、足下では情報銀行の事業化も本格的に進められている。様々な業種の事業体が個人情報の利活用を検討しているが、特に金融機関は、保有する個人情報の量も膨大であり、かつ資産情報や決済情報等、金融機関だからこそ持っている情報もあり、ビッグデータとしての利活用に期待が寄せられている。

一方、個人にとって自分の資産情報や決済情報はセンシティブなものであり、金融機関に対する個人情報の保護の規制も、その量や質に鑑みて、他業種よりも厳しいものとなっている。銀行法等においても、顧客情報の適正な取扱い等について規定されており、また、金融庁の定める金融検査マニュアルや監督指針においても、顧客情報の管理について定められている。

個人情報保護法に関しては、一般的なガイドライン（「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）」）に加え、「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）が公表されている。これは、金融分野の個人情報の性質や利用方法等に鑑み、金融分野の個人情報取扱事業者（金融庁が所管する分野の個人情報取扱事業者を指す。以下同様）に特に厳格な措置が求められる事項等（図表 1）を規定したものである。

本稿では、この金融分野ガイドラインを基に、金融機関等が特にどのような点に注意して個人情報を扱えばいいのかを Q&A 形式で紹介する。

金融分野ガイドラインは、個人情報保護法等を踏まえ、金融分野における個人情報について保護のための格別の措置が講じられるよう必要な措置を講じ、金融分野の事業者が個人情報の適正な取扱いの確保に関して行う活動を支援する具体的な指針として個人情報保護委員会・金融庁が定めるものである。

ガイドラインの規定には、従わない場合は法の規定違反と判断されうる義務規定と、規定違反と判断されることはないが個人情報取扱事業者が特に厳格な措置を取ることが求められる努力義務規定がある。本稿では、義務規定についてのみ太字で表記することで区別する[1]。

**図表 1　金融機関等が個人情報を取り扱う際に特に注意するべき点**

| | |
|---|---|
| ① | **第三者提供時等のほかに本人からの同意が必要な場面** |
| ② | **原則として書面による対応が求められる場面** |
| ③ | **個人信用情報機関とのデータのやり取り** |
| ④ | **機微情報の取扱い** |
| ⑤ | **安全管理措置** |
| ⑥ | **個人情報保護宣言** |
| ⑦ | **個人情報保護法に準拠する際の対応** |

（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

[1] 努力義務規定についても「こととする」、「望ましい」などの表記の違いがあるが、原則として金融分野ガイドラインの原文通りとしている。

## Ｑ１：金融分野で追加的に本人の同意が必要な場面って？

**Ａ１：金融分野の個人情報取扱事業者は、与信事業に際して個人情報を取得する場合は、利用目的について本人の同意を得る。また、個人信用情報機関に個人データを提供する場合は、本人の同意を得る。特に、与信事業に係る個人の返済能力に関する情報を個人信用情報機関へ提供する場合は、オプトアウトに基づく提供は行わない。**

個人情報取扱事業者は、個人情報を取得する際には、**その利用目的を特定し、本人に通知、公表しなければならない。**金融分野の個人情報取扱事業者も同様であり、例えば以下のような利用目的が考えられる。

- **当社の預金の受入れ**
- **当社の与信判断・与信後の管理**
- **当社の保険の引受け、保険金・給付金の支払い**
- **当社、関連会社、提携会社の金融商品・サービスの販売・勧誘**
- **当社、関連会社、提携会社の保険の募集**
- **当社内部における市場調査、金融商品・サービスの開発・研究**
- **特定の金融商品・サービスの購入に際しての資格の確認**

金融分野ガイドラインでは、金融分野の個人情報取扱事業者は、与信事業に際して個人情報を取得する場合は、その個人情報の利用目的について本人に通知、公表するだけでなく、本人の同意を得ることとしている。この利用目的は、契約書等に記載する場合は、他の契約条項等とは明確に分離して記載する。

利用目的の同意を得る際、事業者が与信の条件として、取得した個人情報を当該事業以外の金融商品の「ダイレクトメールの発送等」に利用目的として同意させることは、取引上の優越的な地位を不当に利用していると考えられ、本人はその「ダイレクトメールの発送等」に係る利用目的を拒否することができる。

与信事業に際して個人情報を個人信用情報機関に提供する場合は、**その旨を利用目的に明示しなければならず**、その利用目的について本人から同意を得ることとされている。

その際には、個人データが個人信用情報機関、当該機関の会員企業に提供されることを本人に明確に認識させた上で同意を得る。同意を得る際には、会員企業として当該データを利用する者を、同意を得る書面等に記載する。

特に、与信事業に係る個人の返済能力に関する情報を個人信用情報機関に提供するに当たっては、オプトアウトによる提供は行わないこととされている。

なお、本人が利用目的に同意しなかった場合でも「サービスを提供しなければならない」という規定はないということには注意が必要である。

## Ｑ２：書面で対応する必要がある場面って？

**Ａ２：金融分野の個人情報取扱事業者は、本人の同意を得る際、利用目的の通知をする際、個人データの共同利用に関する通知をする際は、それぞれ原則として書面で行う。**

金融分野の個人情報取扱事業者が個人情報の取得等に際して本人に利用目的を通知する場合は、原則として、書面によることとされている。ここで言う「書面」は電子的記録を含み、「紙」だけでなく、「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る。例えば、インターネットの画面上で同意欄に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、電話による同意の録音等はいずれも「書面」の例であると考えられる。以下、書面というときは同様の解釈をするものとする。

例えば、ＱＡ１で示した与信事業に際しては、利用目的を明示する書面に確認欄を設けて本人の同意を得ることが望ましい。利用目的を公表する場合は、自らの金融商品の販売方法等の事業の態様に応じて、インターネットのホームページや事務所の窓口等で掲示・公表する等、**適切な方法によらなければならない。**

また、利用目的外利用などに当たって本人の同意を得る場合は、原則として、書面によることとされている。個人データの第三者提供を行う際に本人から同意を得るときも、原則として、書面により行う。その際は、以下の三点を書面に記載し、本人に認識させた上で同意を得る。

**①個人データを提供する第三者**
**②提供を受けた第三者における利用目的**
**③第三者に提供される情報の内容**

これらの同意において事業者があらかじめ作成された同意書面を用いる場合は、文字の大きさや文章の表現を変更することで、個人情報の取扱いに関する条項が他と明確に区別され、本人に理解されるとともに、同意書面のチェック欄に本人がチェックを行う等、本人の意思が明確に反映できる方法で確認を行うことが望ましい。

個人データを共同利用する際には、**個人データを共同利用者に提供する前にあらかじめ以下の５点を本人に通知するか、本人が容易に知り得る状態にしなければ本人の同意が必要である**が、この共同利用に係る通知も、原則として、書面によって行う。

**①共同利用をする旨**
**②共同利用される個人データの項目**
**③共同利用する者の範囲**
**④共同利用する者の利用目的**
**⑤共同利用される個人データの管理について責任を有する者の氏名・名称**

特に③共同利用する者の範囲を通知等する際は、共同利用する者を個別に列挙することが望ましい。もしくは、共同利用する者の外延を示す場合には、**本人が容易に理解できるように共同利用する者を具体的に特定しなければならない。**例えば、「当社及び有価証券報告書に記載されている、当社の子会社」といった記載をすることが考えられる。

## Ｑ３：個人信用情報機関とのデータのやり取りで気をつけることは？

**Ａ３：ＱＡ１で示したことのほか、金融分野の個人情報取扱事業者は、個人信用情報機関から得た資金需要者の返済能力の情報は、その資金需要者の返済能力の調査以外の目的に使用することのないよう、慎重に取り扱う。**

ＱＡ１で示した通り、与信事業に際して個人情報を個人信用情報機関に提供する場合は、**その旨を利用目的に明示し**、利用目的について本人から同意を得る。また、個人データを個人信用情報機関に提供する場合は、会員企業にも個人データが提供されることを明確に認識させた上で本人から同意を得る。

このほか、金融分野の個人情報取扱事業者は、個人信用情報機関から資金需要者の返済能力の情報を得た場合は、その情報を資金需要者の返済能力の調査以外の目的に使用することのないように慎重に取り扱うこととされている。

## Ｑ４：機微情報って何？

**Ａ４：機微情報とは、図表 2 に該当する情報のことを指す。ただし、図表 3 に該当するものを除く。**

**図表２　機微情報に該当する情報**

| | | |
|---|---|---|
| ① | 要配慮個人情報 | |
| ② | 労働組合への加盟 | に関する情報<br>（ただし①に当たるものを除く） |
| ③ | 門地 | |
| ④ | 本籍地 | |
| ⑤ | 保健医療 | |
| ⑥ | 性生活 | |

（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

**図表 3　機微情報に該当しない情報**

| | | |
|---|---|---|
| ① | 本人 | により公開されているもの |
| ② | 国の機関 | |
| ③ | 地方公共団体 | |
| ④ | 放送機関、新聞社、通信社<br>その他の報道機関（個人を含む） | |
| ⑤ | 著述を業として行う者 | |
| ⑥ | 大学その他の学術研究を目的とする機関、<br>団体またはそれらに属する者 | |
| ⑦ | 宗教団体 | |
| ⑧ | 政治団体 | |
| ⑨ | 外国政府、外国の政府機関、<br>外国の地方公共団体または国際機関 | |
| ⑩ | 本人を目視、撮影することにより取得するその外形上明らかなもの | |

（注）④～⑧については、外国の者もこれに該当する。
（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

Ｑ４－ａ：機微情報はどう扱えばいいの？

Ａ４－ａ：金融分野の個人情報取扱事業者は、機微情報の取得、利用、第三者提供は行わないこととされている（なお、図表 4 の場合を除く）。また、例外により機微情報を取得し、第三者に提供する場合であっても、オプトアウトによる第三者提供は行ってはならない。

金融分野の個人情報取扱事業者は、機微情報の取得、利用、第三者提供は行わないこととされている。ただし、図表 4 に該当する場合は一定の取得・利用・第三者提供が認められる。

**図表 4　機微情報を取得・利用・第三者提供することができる場合**

| | |
|---|---|
| ① | 法令等に基づく場合 |
| ② | 人の生命、身体または財産の保護のために必要がある場合 |
| ③ | 公衆衛生の向上または児童の健全な育成の推進のため特に必要がある場合 |
| ④ | 国の機関等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 |
| ⑤ | 源泉徴収事務等の遂行上必要な範囲において、政治・宗教等の団体、労働組合への所属・加盟に関する従業員等の機微情報を取得、利用、第三者提供する場合 |
| ⑥ | 相続手続による権利義務の移転等の遂行に必要な限りにおいて、機微情報を取得、利用、第三者提供する場合 |
| 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情報を取得、利用、第三者提供する場合 |
| ⑧ | 機微情報に該当する生体認証情報を本人の同意に基づき、本人確認に用いる場合 |

（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

例えば、図表 4 の⑦に該当する事例としては、金融機関が保険金の支払いや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適切な方法で、かつ必要な範囲内で、本人から同意を得て取得等することは認められると考えられる。一方で、保険金の支払いや与信判断のために、「本籍地」に関する情報を取得することは、業務遂行上必要な範囲外であるため、認められないと考えられる（ただし、業務遂行上の必要性が認められる場合は取得等ができることもあり得る）。

図表 4 に該当する場合に機微情報を取得、利用、第三者提供するに当たっては、これらの場合を逸脱した取得、利用、第三者提供を行わないように、特に慎重に機微情報を取り扱うこととされている。また、図表 4 に該当する場合に機微情報を第三者提供するときは、オプトアウトによる第三者提供は行わないとされている[2]。

なお、機微情報には要配慮個人情報が含まれているが、要配慮個人情報については、個人情報保護法に則った扱いをする必要がある。たとえ図表 4 に該当して取得、利用、第三者提供を行う場合であっても、機微情報の中でも特に要配慮個人情報は**取得する際は本人から同意を得なければならない**等の点に注意しなければならない。

## Ｑ５：金融分野ではどんな安全管理措置をとればいいの？

**Ａ５：金融分野の個人情報取扱事業者は、個人データを取り扱う上で、「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」に沿って、図表 5 の「組織的安全管理措置」、「人的安全管理措置」、「技術的安全管理措置」を含む適切な措置を取らなければならない。**

金融分野の個人情報取扱事業者は、安全管理措置として、図表 5 の**「組織的安全管理措置」、「人的安全管理措置」、「技術的安全管理措置」を含む適切な措置を取らなければならない。**

**それぞれについて具体的な措置としては、個人情報保護委員会・金融庁「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」に従った措置を取る必要がある。**

また、金融分野の個人情報取扱事業者は、個人情報保護法に定められている通り、個人データの安全管理が図られるよう、**従業者および委託先に対する必要かつ適切な監督を行わなければならない。**従業者・委託先の監督についても、**「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」に従った措置を取ることが求められる。**

[2] 図表 4 の①～④に該当し、本人の同意を得ることが困難な場合等、同意なしで第三者提供できる場合を除いては、原則として、本人の同意が必要であると考えられる。

**図表 5　金融分野の安全管理措置**

<table>
<tr><th></th><th colspan="2">基本方針・取扱規程等の整備</th><th>実施体制の整備</th></tr>
<tr><td rowspan="2">組織的<br>安全管理措置</td><td>規定等の整備</td><td>①基本方針の整備<br>②取扱規程の整備<br>③個人データの取扱状況の点検・監査に係る規程の整備<br>④外部委託に係る規程の整備</td><td rowspan="2">①個人データの管理責任者等の設置<br>②就業規則等における安全管理措置の整備<br>③個人データの安全管理に係る取扱規程に従った運用<br>④個人データの取扱状況を確認できる手段の整備<br>⑤個人データの取扱状況の点検・監査体制の整備と実施<br>⑥漏えい事案等に対応する体制の整備</td></tr>
<tr><td>各管理段階における安全管理に係る取扱規程</td><td>①取得・入力段階における取扱規程<br>②利用・加工段階における取扱規程<br>③保管・保存段階における取扱規程<br>④移送・送信段階における取扱規程<br>⑤消去・廃棄段階における取扱規程<br>⑥漏えい事案等への対応の段階における取扱規程</td></tr>
<tr><td>人的<br>安全管理措置</td><td colspan="2">－</td><td>①従業者との個人データの非開示契約等の締結<br>②従業者の役割・責任等の明確化<br>③従業者への安全管理措置の周知徹底、教育、訓練<br>④従業者による個人データ管理手続の遵守状況の確認</td></tr>
<tr><td>技術的<br>安全管理措置</td><td colspan="2">－</td><td>①個人データの利用者の識別・認証<br>②個人データの管理区分の設定・アクセス制御<br>③個人データへのアクセス権限の管理<br>④個人データの漏えい・毀損等防止策<br>⑤個人データへのアクセスの記録・分析<br>⑥個人データを取り扱う情報システムの稼働状況の記録・分析<br>⑦個人データを取り扱う情報システムの監視・監査</td></tr>
</table>

（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

## Ｑ６：個人情報保護宣言って何？

**Ａ６：金融分野の個人情報取扱事業者は、個人情報保護に関する考え方・方針に関する宣言である「個人情報保護宣言」を策定し、その宣言に関する内容をインターネットのホームページや事業所の窓口等で公表することとされている。**

金融分野の個人情報取扱事業者は、個人情報に対する取組方針をあらかじめ分かりやすく説明することの重要性に鑑み、個人情報保護に関する考え方・方針に関する宣言である「個人情報保護宣言」を策定することとされている。

個人情報保護宣言には、本人の権利利益保護の観点から、事業活動の特性、規模、実態に応じて、図表 6 に掲げる点を考慮した記述をできるだけ盛り込むことが望ましい。

**図表 6　個人情報保護宣言に盛り込むべき点**

| | 内容 | 例 |
|---|---|---|
| ① | 保有個人データについて本人から求めがあった場合は、自主的に利用停止に応じること | 本人の求めに応じてダイレクトメールの発送停止を行う |
| ② | 委託処理の透明化を進めること | 委託の有無、委託する事務の内容を明らかにする |
| ③ | 本人にとって利用目的がより明確になるようにすること | ・事業内容を勘案して顧客の種類ごとに利用目的を限定して示す<br>・本人の選択による利用目的の限定に自主的に取り組む |
| ④ | 個人情報の取得元またはその取得方法を可能な限り具体的に明記すること | 取得源の種類を明記する |

（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

また、策定した個人情報保護宣言に関して、例えば、図表 7 に掲げる内容をインターネットのホームページに常時掲載したり、事務所の窓口に掲示・備付け等する形で公表することとされている。

**図表 7　個人情報保護宣言に関して公表する内容の例**

| | |
|---|---|
| ① | 個人情報保護への取組方針の宣言<br>（関係法令等の遵守、個人情報を目的外に利用しないこと、苦情処理に適切に取り組むこと等） |
| ② | 個人情報の利用目的の通知・公表等の手続についての分かりやすい説明 |
| ③ | 個人情報の取扱いに関する諸手続についての分かりやすい説明（開示の手続等） |
| ④ | 個人情報の取扱いに関する質問、苦情処理の窓口 |

（出所）個人情報保護委員会・金融庁「金融分野における個人情報保護に関するガイドライン」より大和総研作成

## Ｑ７：個人情報保護法に準拠するときに金融分野で気をつけることは？

**Ａ７：保有する個人データの保存期間の設定、保有個人データに関する事項の公表の方法、個人情報等の漏えい事案等への対応など、金融ガイドラインに沿った対応を行うことが求められている。**

個人情報保護法では、個人情報取扱事業者は個人データを利用する必要がなくなったときは、個人データを遅滞なく消去するように努めなければならないが、特に金融分野の個人情報取扱事業者は、保有する個人データの利用目的に応じて保存期間を定めることとされている。例えば、預金者や保険契約者等の個人データの保存期間を契約終了後一定期間内とし、期間経過後は個人データを消去することとする。

また、個人情報取扱事業者は保有個人データに関して、原則として、**以下の事項を本人の知**

**り得る状態に置かなければならない**が、金融分野の個人情報取扱事業者は、その際は**自らの金融商品の販売方法等の事業の態様に応じて適切な方法による必要がある。**例えば、「個人情報保護宣言」と一体としてインターネットのホームページでの常時掲載、事務所の窓口等での常時掲示・備付けを行うこと等が考えられる。

| |
|---|
| **①個人情報取扱事業者の氏名または名称** |
| **②全ての保有個人データの利用目的** |
| **③保有個人データの利用目的の通知の求めの手続、手数料** |
| **④保有個人データの開示等の請求の手続、手数料** |
| **⑤保有個人データの取扱いに関する苦情の申出先** |

さらに、金融分野の個人情報取扱事業者は、個人情報等の漏えい事案が発生したときは、監督当局等に直ちに報告し、事実関係・再発防止策等を早急に公表するとともに、事案の対象となった本人に速やかに事実関係等の通知等を行うこととされている（**個人データの漏えい事案については義務規定**）。