2022.4.10 金融法務事情　掲載

# 金融分野における個人情報保護に関するガイドライン改正の概要


| | | |
|---|---|---|
| 個人情報保護委員会事務局 | 参事官補佐・弁護士 | 松本 亮孝 |
| 同 | 参事官補佐 | 今 拓久真 |
| 同 | 参事官補佐・弁護士 | 椎名 紗彩 |
| 金融庁企画市場局総務課 | 課長補佐 | 赤井 啓人 |


「個人情報の保護に関する法律」（平成15年法律第57号）をめぐっては、令和２年６月に「個人情報の保護に関する法律等の一部を改正する法律」（令和２年法律第44号。以下「令和２年改正法」という）が成立・公布され、また、令和３年５月には「デジタル社会の形成を図るための関係法律の整備に関する法律」（令和３年法律第37号。以下「令和３年改正法」という）が成立・公布されており、その後、同年10月29日には、令和３年改正法を踏まえ、「個人情報の保護に関する法律施行令等の一部を改正する等の政令」および「個人情報の保護に関する法律施行規則の一部を改正する規則」が公布され、また、同日に令和３年改正法を踏まえた改正後の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、外国にある第三者への提供編、第三者提供時の確認・記録義務編、仮名加工情報・匿名加工情報編、認定個人情報保護団体編）が公表されている（以下、令和３年改正法50条による改正後の個人情報の保護に関する法律を「法」、個人情報の保護に関する法律施行令を「施行令」、個人情報の保護に関する法律施行規則を「施行規則」、個人情報の保護に関する法律についてのガイドラインを「ガイドライン」という）。

この点、個人情報保護委員会および金融庁は、法６条等に基づき、金融庁が所管する分野（以下「金融分野」という）における個人情報の取扱いについて特に厳格な措置を求めるものとして、「金融分野における個人情報保護に関するガイドライン」および「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」を公表しているところ、令和２年改正法等を踏まえて同ガイドライン等も改正され、令和４年３月24日に公表されている（以下、改正後の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「金融分野ガイドライン」という）。

本稿では、金融分野ガイドラインの改正項目のうち主要なもの、具体的には、個人データ等の漏えい等の報告等（11条）、外国にある第三者への提供の制限（13条）、個人関連情報の第三者提供の制限等（14条）、個人情報保護宣言の表示の工夫（20

条）について、紙幅の許す限りその内容を解説することとしたい。[1]なお、文中意見にわたる部分は、あくまで筆者の個人的見解であって、筆者が所属する組織の見解ではないことをあらかじめお断りしておく。

## 1. 個人データ等の漏えい等の報告等

### ⑴　概　要

令和２年改正法により、漏えい等の報告等の規律が新設されたことを受け、金融分野ガイドラインにおいても、漏えい等の報告等の規律について、必要な改正を行っている。

### ⑵　漏えい等の報告

#### a　金融分野ガイドライン11条１項前段（法に基づく報告義務）

金融分野ガイドライン11条１項前段は、法26条１項に基づく規律である。

金融分野における個人情報取扱事業者は、施行規則７条各号に定める事態を知ったときは、ガイドライン（通則編）3-5-3に従って、個人情報保護委員会（法147条の規定により金融庁長官等が報告を受理する権限の委任を受けている場合にあっては金融庁長官等、法165条の規定により地方公共団体の長等が報告を受理する権限に属する事務を行う場合にあっては地方公共団体の長等）に報告しなければならない。

【施行規則7条各号に該当する事態】
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、また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、また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個人データの漏えい等が発生し、または発生したおそれがある事態
④ データに係る本人の数が1000人を超える漏えい等が発生し、または発生したおそれがある事態

[1] 令和２年改正法の概要については、小川智史「令和２年改正個人情報保護法の概要」本誌2144号24頁を参照されたい。また、令和２年改正法を踏まえた改正後の施行令、施行規則、ガイドラインの概要については、小川智史＝関口朋宏「令和２年改正個人情報保護法 政令・規則・ガイドラインの解説」本誌2170号51頁を参照されたい。

具体的な報告方法等については、ガイドライン（通則編）3-5-3を参照いただきたい。

また、報告先については、金融機関における個人情報保護に関するQ&A（以下「金融分野QA」という）および個人情報保護委員会のウェブページ[2]を参照いただきたい。

**b　金融分野ガイドライン11条1項後段（各業法に基づく報告義務）**

金融分野ガイドライン11条１項後段は、金融庁が所管する各業法（銀行法、保険業法等。以下「各業法」という）に基づく規律である。

金融分野における個人情報取扱事業者は、各業法およびその下位省令[3]（銀行法13条の3の2、同法施行規則13条の6の5の2等）に基づき、「その取り扱う個人である顧客等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（金融庁長官等）に報告を行う必要がある。

各業法に基づく漏えい等報告の報告対象事態については、以下の点に留意が必要である。

- 対象となるのは「個人である顧客等に関する個人データ」の漏えい等である。このため、法人顧客に関する個人データや、金融機関自身の雇用管理分野や株主情報の中に含まれる個人データの漏えい等は、各業法に基づく漏えい等報告の対象外である。
- 「個人である顧客等に関する個人データ」の漏えい等であれば、漏えい等した個人データに係る本人の数を問わず、報告義務が生じる。
- 「仮名加工情報である個人データ」の漏えい等も報告対象事態から除外されない。
- 「高度な暗号化措置その他の個人の権利利益を保護するために必要な措置」が講じられた個人データの漏えい等も報告対象事態から除外されない。

具体的な報告方法等については、金融分野 QA を参照されたい。原則として、「速やかに」監督当局に報告をする必要があるが、一定の場合には、四半期に1回程度にまとめて報告を行うこと等も許容されている。

なお、個人データの漏えい等について、法26条１項の定める漏えい等報告の報告対象事態（施行規則７条各号）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、双方の法に基づきそれぞれ報告を行う必要があるが、１つの報告書を監督当局に提出することで、双方の法に基づ

[2] https://www.ppc.go.jp/personalinfo/legal/kengenInin/

[3] 令和４年３月24日に、銀行法施行規則等の一部を改正する内閣府令等が公布されている。

く報告を一括して行うことも可能である。

**c 金融分野ガイドライン11条2項（努力義務）**

金融分野ガイドライン11条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かんがみ、「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る。

【金融分野ガイドライン11条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、また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41条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）また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、または発生したおそれがある事態

具体的な報告方法等については、金融分野 QA を参照されたい。

**⑶ 本人への通知等**

**a 金融分野ガイドライン11条3項前段（法に基づく通知等義務）**

金融分野ガイドライン11条３項前段は、法26条１項に基づく規律である。

金融分野における個人情報取扱事業者は、施行規則 7 条各号に定める事態を知ったときは、ガイドライン（通則編）3-5-4 に従って、本人への通知を行わなければならない。本人への通知が困難な場合には、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る。

**b 金融分野ガイドライン 11 条3項後段（努力義務）**

金融分野ガイドライン 11 条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かんがみ、「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」との努力義務を定めている。

【金融分野ガイドライン 11 条３項に定める「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、また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、また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また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、または発生したおそれがある事態 |
|---|

仮名加工情報である個人データおよび仮名加工情報である個人情報については、本人への通知等の努力義務の対象外とされている。

## 2. 外国にある第三者への提供の制限

### ⑴　概　要

令和２年改正法により、個人情報取扱事業者が外国に個人データを移転できる場合を一定の場合に制限する法28条の規定に関し、移転先の事業者やその事業者が置かれている外国の状況について本人への情報提供の充実等が義務付けられたことを受け、金融分野ガイドラインにおいても、必要な改正を行っている。

### ⑵　同意取得時における情報提供の充実

#### a　金融分野ガイドライン13条１項 第１段落・第２段落

令和２年改正法により、個人情報取扱事業者は、法28条１項の規定により外国にある第三者への個人データの提供を認める旨の本人の同意を得ようとする場合には、施行規則17条２項から４項までの規定により情報提供が求められる事項について、当該本人に情報提供することが義務付けられた（法28条２項）。

| 【施行規則17条２項の定める事項】<br>①　当該外国の名称<br>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<br>③　当該第三者が講ずる個人情報保護のための措置に関する情報 |
|---|

金融分野ガイドライン13条１項第１段落は、金融分野の個人情報取扱事業者が、施行規則17条２項から４項までの規定により情報提供が求められる事項に加えて、以下の事項について情報を提供することを努力義務として定めている。

| 【金融分野ガイドライン13条１項の定める事項】<br>①　個人データの提供先の第三者<br>②　提供先の第三者における利用目的<br>③　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13条１項第２段落は、本人の同意を取得する時点において、①個人データの提供先の第三者が特定できない場合にはそれに代わる本人に参考となるべき情報（例えば、提供先の第三者の範囲や属性に関する

情報）を当該本人に認識させた上で、同意を取得することを努力義務として定めている。

さらに、金融分野ガイドライン 13 条１項の規定により、金融分野における個人情報取扱事業者は、「本人の同意を得る際には、原則として、書面によること」（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。以下同じ）が求められており、また、「当該書面における記載を通じて」情報提供を行うことが求められている。すなわち、情報提供の方法については、口頭で説明する方法等ではなく、必要な情報を記載した書面を本人に示す方法により行うことが求められている。

**b　金融分野ガイドライン 13 条1項　第 3 段落**

金融分野ガイドライン 13 条１項第３段落は、金融分野における個人情報取扱事業者があらかじめ作成された同意書面を用いる場合には、文字の大きさおよび文章の表現を変えること等により、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等と明確に区別され、本人に理解されることが望ましいと定めている。具体的な方法については、金融分野QAを参照されたい。

**⑶　同意取得時に提供先の第三者が所在する外国が特定できない場合等の取扱い**

**a　金融分野ガイドライン13条2項前段**

金融分野ガイドライン 13 条２項前段は、法 28 条２項および施行規則 17 条３項に基づく規律である。

金融分野における個人情報取扱事業者は、法 28 条１項の規定により本人の同意を得ようとする時点において、個人データの提供先の第三者が所在する外国が特定できない場合には、特定できない旨およびその具体的な理由（提供先が定まる前に本人同意を得る必要性を含む）を情報提供するとともに、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場合には、当該情報を提供しなければならない。

**b　金融分野ガイドライン13条2項後段**

金融分野ガイドライン13条２項後段は、法28条２項および施行規則17条３項・４項に基づく規律である。

金融分野における個人情報取扱事業者は、（ⅰ）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、施行規則17条２項１号および２号に掲げる事項について、また、（ⅱ）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、同項３号に掲げる事項について、本人の求めに応じて情報提供を行う努力義務を負う。

金融分野ガイドライン13条２項後段は、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20条に定める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また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を努力義務として定めている。

また、本人から情報提供の求めがあった場合であっても、例えば、情報提供することにより金融分野における個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合等は、施行規則17条２項各号に定める情報の全部または一部について情報提供しないことができる。情報提供しない場合、金融分野における個人情報取扱事業者は、本人に対し、遅滞なくその旨を通知するとともに、その理由を説明することが努力義務として求められる。

**⑷　施行規則16条に定める基準に適合する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個人データを提供する場合に講ずべき措置等**

**a　金融分野ガイドライン13条3項　第　1段落**

令和２年改正法により、個人情報取扱事業者は、施行規則 16 条に定める基準に適合する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、当該第三者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じることおよび本人の求めに応じて当該必要な措置に関する情報を当該本人に提供することが義務付けられた（法 28 条３項）。

金融分野ガイドライン 13 条３項第１段落は、金融分野における個人情報取扱事業者は、施行規則 16 条に定める基準に適合する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および内容、当該制度がある場合においては、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、確認する必要があると定めている。

相当措置の実施に影響を及ぼすおそれのある制度としては、次に掲げる例が考えられる。

（例）
- 事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度
- 事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度

**b　金融分野ガイドライン 13 条3項　第2段落**

個人情報取扱事業者は、施行規則16条に定める基準に適合する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には、当該第三者による相当措置の実施状況等を、適切かつ合理的な方法により、定期的に確認する必要がある（法28条３項、施行規則18条１項１号）。

この確認方法について、金融分野ガイドライン13条３項第２段落により、金融分野における個人情報取扱事業者は、「個人データを取り扱う場所に赴く方法または書面により報告を受ける方法」により確認を行うこととするとされている。すなわち、口頭により確認するのではなく、書面により報告を受ける方法等により確認することが求められている。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および性質なら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る。

**c　金融分野ガイドライン13条3項　第3段落**

金融分野ガイドライン13条３項第３段落は、法28条３項および施行規則18条に基づき、本人の求めに応じて事後的に情報を提供する旨を金融分野ガイドライン20条に定める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また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を努力義務として定めている。

## 3. 個人関連情報の第三者提供の制限等

### ⑴　概　要

令和２年改正法により、個人関連情報の第三者提供の制限等の規律が新設されたことを受け、金融分野ガイドラインにおいても、個人関連情報の第三者提供の制限等に関する規律が追加されている。

### ⑵　金融分野ガイドライン14条1項

個人関連情報取扱事業者は、提供先の第三者が、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）を個人データとして取得することが想定される場合には、原則として、当該個人関連情報に係る「本人の同意」が得られていること等を確認する必要がある（法31条１項）。同項1号の「本人の同意」を取得する主体は、原則として、提供先の第三者であるが、例外的に、同等の本人の権利利益の保護が図られることを前提に、提供元の個人関連情報取扱事業者が同意取得を代行することも認められる（ガイドライン（通則編）3-7-2）。

金融分野ガイドライン14条１項は、金融分野における個人情報取扱事業者が、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個人データとして取得するにあたり、法31条１項１号の「本人の同意」を得る際には、「原則として書面による」こととし、また、「当該書面による記載を通じて、①対象となる個人関連情報の項目、②個人関連情報の提供を受けて個人データとして取得した

後の利用目的を本人に認識させたうえで同意を得ることとする」との努力義務を定めている。

また、金融分野における個人情報取扱事業者が、提供元の個人関連情報取扱事業者に同意取得を代行させる場合には、提供元の個人関連情報取扱事業者が上記の努力義務を負うことになる。

### ⑶　金融分野ガイドライン14条2項

個人関連情報取扱事業者は、施行規則16条に定める基準に適合する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関連情報を提供した場合には、法31条２項により読み替えて準用される法28条３項（施行規則18条１項１号）に基づき、当該第三者による相当措置の実施状況等を定期的に確認する必要がある（ガイドライン（通則編）3-7-3-2）。

金融分野ガイドライン14条２項は、金融分野における個人情報取扱事業者が、外国にある第三者による相当措置の実施状況を定期的に確認する際には、「個人データの内容や規模等に応じて個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法によることとする」との努力義務を定めている。

## 4. 個人情報保護宣言の策定

### ⑴　概　要

金融分野における個人情報取扱事業者は、事業者の個人情報保護に関する考え方及び方針に関する宣言（以下「個人情報保護宣言」という）を策定することが努力義務として求められていたところ、今般の金融分野ガイドラインの改正により、新たに個人情報保護宣言の表示に係る具体的な工夫に関する規定が追加された。

### ⑵　個人情報保護宣言の表示に係る具体的な工夫の例（【図表】参照）

金融分野ガイドライン20条１項は、金融分野における個人情報取扱事業者に対し、個人情報保護宣言を策定し、同項各号に例示する内容をインターネットのホームページへの常時掲載または事務所の窓口等での掲示・備付け等により、公表することを努力義務として求めている。

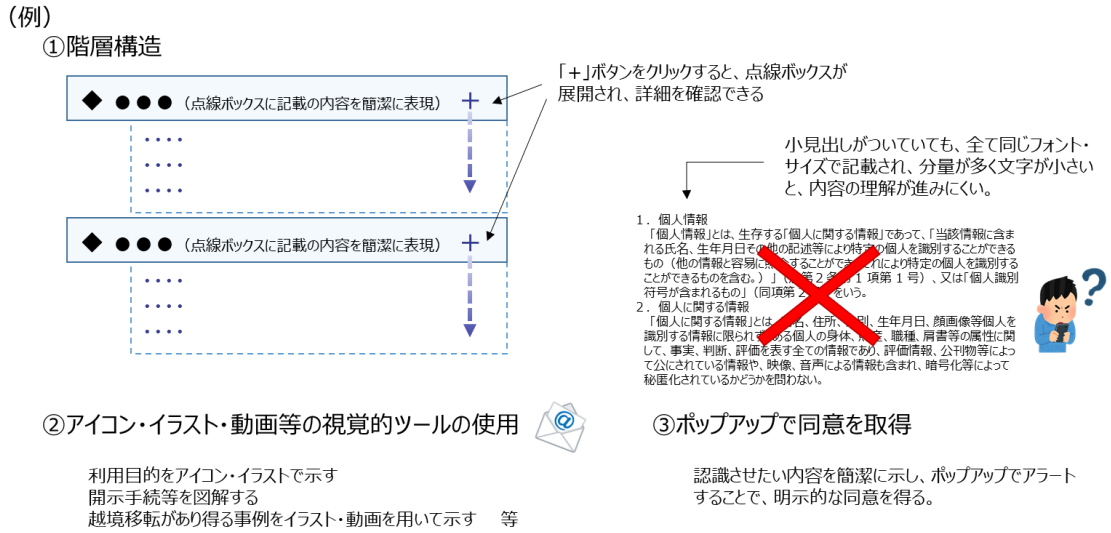
金融分野ガイドラインの改正により、20条３項の規定が追加され、個人情報保護宣言は、本人がこれを適切に理解した上で自らの判断により選択の機会を行使することができるような表示等により構成することが望ましいとされた。具体的な工夫としては、次に掲げる例が考えられる。

（例）
- 階層構造（要点を複数の項目にまとめ各項目を選択すると詳細な内容が見られる構造をいう。）

- アイコン、イラスト、動画等の視覚的ツールの活用
- ポップアップによる同意取得

**【図表】個人情報保護宣言の記載方法の工夫**

「個人情報保護宣言」（いわゆるプライバシーポリシー）については、利用者にとって内容を確認しにくい仕様となっている場合が多い。金融機関等には、本人が、個人情報保護宣言の内容を適切に理解した上で自らの判断により選択の機会を行使できるよう、表示等の工夫を求めることとする。




その他、文字の大きさ、**太さ**、字体、<u>下線</u>などにより、利用者が内容を確認しやすいようにする方法も可。

## 5. おわりに

令和２年改正法および令和３年改正法のうち50条による改正に係る部分（国・独立行政法人等・学術研究関係）は、令和４年４月１日に全面施行される。

金融分野における個人情報取扱事業者および個人関連情報取扱事業者においては、法、施行令、施行規則、ガイドラインのみならず、金融分野ガイドライン、実務指針、金融分野QA等も踏まえ、適正に個人情報等を取り扱う必要がある。

（まつもと　りょうこう／こん　たくま／しいな　さあや／あかい　ひろと）