

## ○ 金融分野における個人情報保護に関するガイドライン（平成29年個人情報保護委員会・金融庁告示第1号）の一部を改正する告示案

次の表により、改正前欄に掲げる規定の傍線を付し又は破線で囲んだ部分をこれに順次対応する改正後欄に掲げる規定の傍線を付し又は破線で囲んだ部分のように改め、改正前欄及び改正後欄に対応して掲げるその標記部分（連続する他の規定と記号により一括して掲げる規定にあつては、その標記部分に係る記載）に二重傍線を付した規定（以下「対象規定」という。）は、その標記部分が異なるものは改正前欄に掲げる対象規定を改正後欄に掲げる対象規定として移動し、改正前欄に掲げる対象規定で改正後欄にこれに対応するものを掲げていないものは、これを削り、改正後欄に掲げる対象規定で改正前欄にこれに対応するものを掲げていないものは、これを加える。

改 正 後	改 正 前
目次	目次
第1条 [略]	第1条 [同左]
第2条 利用目的の特定（ <u>法第17条</u> 関係）	第2条 利用目的の特定（ <u>法第15条</u> 関係）
第3条 同意の形式（ <u>法第18条、第27条、第28条及び第31条</u> 関係）	第3条 同意の形式（ <u>法第16条、第23条及び第24条</u> 関係）
第4条 利用目的による制限（ <u>法第18条</u> 関係）	第4条 利用目的による制限（ <u>法第16条</u> 関係）
第5条 [略]	第5条 [同左]
第6条 取得に際しての利用目的の通知等（ <u>法第21条</u> 関係）	第6条 取得に際しての利用目的の通知等（ <u>法第18条</u> 関係）
第7条 データ内容の正確性の確保等（ <u>法第22条</u> 関係）	第7条 データ内容の正確性の確保等（ <u>法第19条</u> 関係）
第8条 安全管理措置（ <u>法第23条</u> 関係）	第8条 安全管理措置（ <u>法第20条</u> 関係）
第9条 従業者の監督（ <u>法第24条</u> 関係）	第9条 従業者の監督（ <u>法第21条</u> 関係）
第10条 委託先の監督（ <u>法第25条</u> 関係）	第10条 委託先の監督（ <u>法第22条</u> 関係）
第11条 個人データ等の漏えい等の報告等（ <u>法第26条</u> 関係）	第11条 第三者提供の制限（ <u>法第23条</u> 関係）
第12条 第三者提供の制限（ <u>法第27条</u> 関係）	第12条 保有個人データに関する事項の公表等（ <u>法第27条</u> 関係）
第13条 外国にある第三者への提供の制限（ <u>法第28条</u> 関係）	第13条 開示（ <u>法第28条</u> 関係）

第14条 個人関連情報の第三者提供の制限等（法第31条関係）  
第15条 保有個人データに関する事項の公表等（法第32条関係）  
第16条 開示（法第33条関係）  
第17条 理由の説明（法第36条関係）  
第18条 開示等の請求等に応じる手続（法第37条関係）  
第19条 個人情報取扱事業者による苦情の処理（法第40条関係）  
第20条 個人情報保護宣言の策定（法第21条、第32条及び基本方針関係）  
第21条 ガイドラインの見直し

第1条 目的等（法第1条関係）

1 本ガイドラインは、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）、個人情報の保護に関する法律施行令（平成15年政令第507号。以下「施行令」という。）、個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。以下「施行規則」という。）及び個人情報の保護に関する基本方針（平成16年4月2日閣議決定。第20条において「基本方針」という。）を踏まえ、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）（平成28年個人情報保護委員会告示第6号。以下「通則ガイドライン」という。）を基礎として、法第6条及び第9条に基づき、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、及び当該分野における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

第14条 理由の説明（法第31条関係）  
第15条 開示等の請求等に応じる手続（法第32条関係）  
第16条 個人情報取扱事業者による苦情の処理（法第35条関係）  
第17条 個人情報等の漏えい事案等への対応  
第18条 個人情報保護宣言の策定（法第18条、第27条及び基本方針関係）  
第19条 ガイドラインの見直し

第1条 目的等（法第1条関係）

1 本ガイドラインは、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）、個人情報の保護に関する法律施行令（平成15年政令第507号。以下「施行令」という。）、個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号。以下「施行規則」という。）及び個人情報の保護に関する基本方針（平成16年4月2日閣議決定。第18条において「基本方針」という。）を踏まえ、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）（平成28年個人情報保護委員会告示第6号。以下「通則ガイドライン」という。）を基礎として、法第6条及び第8条に基づき、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、及び当該分野における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定めるものである。

本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）（平成28年個人情報保護委員会告示第7号。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）（平成28年個人情報保護委員会告示第8号）、同ガイドライン（仮名加工情報・匿名加工情報編）（平成28年個人情報保護委員会告示第9号）及び同ガイドライン（認定個人情報保護団体編）（令和3年個人情報保護委員会告示第7号）が適用される。

2 本ガイドライン中「～なければならない」と記載されている規定について、それに従わない場合は、法の規定違反と判断され得る。

また、本ガイドライン中「こととする」、「適切である」及び「望ましい」と記載されている規定については、金融分野における個人情報取扱事業者及び個人関連情報取扱事業者がその規定に従わない場合には、法の規定違反と判断されることはないが、当該規定は、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及び個人関連情報取扱事業者に特に厳格な措置が求められる事項として規定されており、金融分野における個人情報取扱事業者及び個人関連情報取扱事業者においては、遵守に努めるものとする。

3 [略]

を支援する具体的な指針として定めるものである。

本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）（平成28年個人情報保護委員会告示第7号）、同ガイドライン（第三者提供時の確認・記録義務編）（平成28年個人情報保護委員会告示第8号）及び同ガイドライン（匿名加工情報編）（平成28年個人情報保護委員会告示第9号）が適用される。

2 本ガイドライン中「～なければならない」と記載されている規定について、それに従わない場合は、法の規定違反と判断され得る。

また、本ガイドライン中「こととする」、「適切である」及び「望ましい」と記載されている規定については、金融分野における個人情報取扱事業者がその規定に従わない場合には、法の規定違反と判断されることはないが、当該規定は、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として規定されており、金融分野における個人情報取扱事業者においては、遵守に努めるものとする。

3 [同左]

4 金融分野における認定個人情報保護団体が個人情報保護指針を作成又は変更し、また、金融分野における事業者団体等が事業の実態及び特性を踏まえ、当該事業者団体等の会員企業等を対象とした自主的ルール（事業者団体ガイドライン等）を作成又は変更することもあり得るが、その場合は、認定個人情報保護団体の対象事業者や事業者団体等の会員企業等は、個人情報の取扱いに当たり、個人情報の保護に関する法令、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（認定個人情報保護団体編）及び本ガイドライン等に加えて、当該指針又はルールに沿った対応を行う必要がある。特に、認定個人情報保護団体においては、認定個人情報保護団体が対象事業者に対し個人情報保護指針を遵守させるために必要な措置をとらなければならないこととされていることを踏まえることも重要である。

5 金融分野における個人情報取扱事業者は、個人情報の漏えい、滅失又は毀損（以下「漏えい等」という。）等を防止等するため、個人情報の保護に関する法令、通則ガイドライン及び本ガイドラインのほか、関係法令等に従い、個人情報の適正な管理体制を整備する必要がある。

#### 第2条 利用目的の特定（法第17条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者が、法第17条に従い利用目的を特定するに際して、「自社の所要の目的で用いる」といった抽象的な利用目的では「できる限り特定」したものとはならな

4 金融分野における認定個人情報保護団体が個人情報保護指針を作成又は変更し、また、金融分野における事業者団体等が事業の実態及び特性を踏まえ、当該事業者団体等の会員企業等を対象とした自主的ルール（事業者団体ガイドライン等）を作成又は変更することもあり得るが、その場合は、認定個人情報保護団体の対象事業者や事業者団体等の会員企業等は、個人情報の取扱いに当たり、個人情報の保護に関する法令、通則ガイドライン及び本ガイドライン等に加えて、当該指針又はルールに沿った対応を行う必要がある。特に、認定個人情報保護団体においては、法改正により、認定個人情報保護団体が対象事業者に対し個人情報保護指針を遵守させるために必要な措置をとらなければならないこととされたことを踏まえることも重要である。

5 金融分野における個人情報取扱事業者は、個人情報の漏えい、不正流出等を防止等するため、個人情報の保護に関する法令、通則ガイドライン及び本ガイドラインのほか、関係法令等に従い、個人情報の適正な管理体制を整備する必要がある。

#### 第2条 利用目的の特定（法第15条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者が、法第15条に従い利用目的を特定するに際して、「自社の所要の目的で用いる」といった抽象的な利用目的では「できる限り特定」したものとはならな

い。利用目的は、提供する金融商品又はサービスを示した上で特定することが望ましく、次に掲げる例が考えられる。

(例)

- ・ 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
- ・ 当社又は関連会社・提携会社の金融商品・サービスの販売
- ・ 勧誘
- ・ 当社又は関連会社・提携会社の保険の募集
- ・ 当社内部における市場調査及び金融商品・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

[2～4 略]

5 法第17条第2項に定める「変更前の利用目的と関連性を有すると合理的に認められる範囲」については、次に掲げる例が考えられる。

(許容例)

「商品案内等を郵送」→「商品案内等をメール送付」

(認められない例)

「アンケート集計に利用」→「商品案内等の郵送に利用」

第3条 同意の形式（法第18条、第27条、第28条及び第31条関係）

以下の事項の他は通則ガイドラインの例による。

金融分野における個人情報取扱事業者は、法第18条第1項及び第

い。利用目的は、提供する金融商品又はサービスを示した上で特定することが望ましく、次に掲げる例が考えられる。

(例)

- ・ 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
- ・ 当社又は関連会社・提携会社の金融商品・サービスの販売
- ・ 勧誘
- ・ 当社又は関連会社・提携会社の保険の募集
- ・ 当社内部における市場調査及び金融商品・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

[2～4 同左]

5 法第15条第2項に定める「変更前の利用目的と関連性を有すると合理的に認められる範囲」については、次に掲げる例が考えられる。

(許容例)

「商品案内等を郵送」→「商品案内等をメール送付」

(認められない例)

「アンケート集計に利用」→「商品案内等の郵送に利用」

第3条 同意の形式（法第16条、第23条及び第24条関係）

以下の事項の他は通則ガイドラインの例による。

金融分野における個人情報取扱事業者は、法第16条、第23条及び

2項、第27条第1項、第28条第1項並びに第31条第1項第1号（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同項の規定による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場合に限る。）に定める本人の同意を得る場合には、原則として、書面（電磁的記録を含む。以下同じ。）によることとする。

なお、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、文字の大きさ及び文章の表現を変えること等により、個人情報の取扱いに関する条項が他と明確に区別され、本人に理解されることが望ましい。または、あらかじめ作成された同意書面に確認欄を設け本人がチェックを行うこと等、本人の意思が明確に反映できる方法により確認を行うことが望ましい。

#### 第4条 利用目的による制限（法第18条関係）

以下の事項の他は通則ガイドラインの例による。

法第18条第3項の場合の例としては、通則ガイドライン3-1-5（利用目的による制限の例外）に掲げている場合以外に、次に掲げる場合が考えられる。

[①・② 略]

#### 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、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

第24条に定める本人の同意を得る場合には、原則として、書面（電磁的記録を含む。以下同じ。）によることとする。

なお、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、文字の大きさ及び文章の表現を変えること等により、個人情報の取扱いに関する条項が他と明確に区別され、本人に理解されることが望ましい。または、あらかじめ作成された同意書面に確認欄を設け本人がチェックを行うこと等、本人の意思が明確に反映できる方法により確認を行うことが望ましい。

#### 第4条 利用目的による制限（法第16条関係）

以下の事項の他は通則ガイドラインの例による。

法第16条第3項の場合の例としては、通則ガイドライン3-1-5（利用目的による制限の例外）に掲げている場合以外に、次に掲げる場合が考えられる。

[①・② 同左]

#### 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、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、法第76条第1項各号若しくは施行規則第6条各号に掲げる者により公

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。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。

[①～④ 略]

⑤ 法第20条第2項第6号に掲げる場合に機微（センシティブ）情報を取得する場合、法第18条第3項第6号に掲げる場合に機微（センシティブ）情報を利用する場合、又は法第27条第1項第7号に掲げる場合に機微（センシティブ）情報を第三者提供する場合

⑥～⑨ [略]

2 [略]

3 金融分野における個人情報取扱事業者は、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、例えば、要配慮個人情報を取得するに当たっては、法第20条第2項に従い、あらかじめ本人の同意を得なければならないとされていることなど、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。

4 金融分野における個人情報取扱事業者は、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。なお、機微（センシティブ）情報のうち要配慮個人情報については、同項において、

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。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。

[①～④ 同左]

[号を加える。]

⑤～⑧ [同左]

2 [同左]

3 金融分野における個人情報取扱事業者は、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、例えば、要配慮個人情報を取得するに当たっては、法第17条第2項に従い、あらかじめ本人の同意を得なければならないとされていることなど、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。

4 金融分野における個人情報取扱事業者は、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23条第2項（オプトアウト）の規定を適用しないこととする。なお、機微（センシティブ）情報のうち要配慮個人情報については、同項において、

オプトアウトを用いることができないとされていることに留意する。

#### 第6条 取得に際しての利用目的の通知等（法第21条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者が行う法第21条第1項に定める「通知」については、原則として、書面によることとする。また、同項に定める「公表」については、自らの金融商品の販売方法等の事業の態様に応じ、インターネットのホームページ等での公表、事務所の窓口等への書面の掲示・備付け等適切な方法によらなければならない。

2 金融分野における個人情報取扱事業者は、与信事業に際して、法第21条第2項に従い、本人から直接書面に記載された当該本人の個人情報を取得する場合は、利用目的を明示する書面に確認欄を設けること等により、利用目的について本人の同意を得ることが望ましい。

なお、与信事業に際して、申込時に利用目的について本人の同意を得る場合、当該申込時に利用目的について同意を得た個人情報については法第21条第1項に基づく「通知又は公表」を要しないが、それ以降に取得する情報については、あらかじめ利用目的を公表していない限り、利用目的を本人に通知し、又は公表しなければならない。

3 法第21条第4項の場合の例としては、通則ガイドライン3-3-5（利用目的の通知等をしなくてよい場合）に掲げている場合

オプトアウトを用いることができないとされていることに留意する。

#### 第6条 取得に際しての利用目的の通知等（法第18条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者が行う法第18条第1項に定める「通知」については、原則として、書面によることとする。また、同項に定める「公表」については、自らの金融商品の販売方法等の事業の態様に応じ、インターネットのホームページ等での公表、事務所の窓口等への書面の掲示・備付け等適切な方法によらなければならない。

2 金融分野における個人情報取扱事業者は、与信事業に際して、法第18条第2項に従い、本人から直接書面に記載された当該本人の個人情報を取得する場合は、利用目的を明示する書面に確認欄を設けること等により、利用目的について本人の同意を得ることが望ましい。

なお、与信事業に際して、申込時に利用目的について本人の同意を得る場合、当該申込時に利用目的について同意を得た個人情報については法第18条第1項に基づく「通知又は公表」を要しないが、それ以降に取得する情報については、あらかじめ利用目的を公表していない限り、利用目的を本人に通知し、又は公表しなければならない。

3 法第18条第4項の場合の例としては、通則ガイドライン3-2-5（利用目的の通知等をしなくてよい場合）に掲げている場合



以外に、次に掲げる場合が考えられる。

[①・② 略]

#### 第7条 データ内容の正確性の確保等（法第22条関係）

[略]

#### 第8条 安全管理措置（法第23条関係）

- 1 金融分野における個人情報取扱事業者は、その取り扱う個人データの漏えい等の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じなければならない。必要かつ適切な措置は、個人データの取得・利用・保管等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」及び「外的環境の把握」を含むものでなければならない。

当該措置は、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、事業の性質、個人データの取扱状況及び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たものとする。

例えば、不特定多数者が書店で随時に購入可能な名簿で、事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、事業者の安全管理措置の義務違反にはならない。

以外に、次に掲げる場合が考えられる。

[①・② 同左]

#### 第7条 データ内容の正確性の確保等（法第19条関係）

[同左]

#### 第8条 安全管理措置（法第20条関係）

- 1 金融分野における個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じなければならない。必要かつ適切な措置は、個人データの取得・利用・保管等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」及び「技術的安全管理措置」を含むものでなければならない。

当該措置は、個人データが漏えい、滅失又は毀損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、事業の性質、個人データの取扱状況及び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たものとする。

例えば、不特定多数者が書店で随時に購入可能な名簿で、事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、事業者の安全管理措置の義務違反にはならない。

2 この条における「組織的安全管理措置」とは、個人データの安全管理措置について従業者（法第24条参照）の責任と権限を明確に定め、安全管理に関する規程等を整備・運用し、その実施状況の点検・監査を行うこと等の、個人情報取扱事業者の体制整備及び実施措置をいう。

3 [略]

4 この条における「物理的安全管理措置」とは、個人データを取り扱う区域の管理、機器及び電子媒体等の盗難の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止並びに機器及び電子媒体等の廃棄等の個人データの安全管理に関する物理的な措置をいう。

5 [略]

6 この条における「外的環境の把握」とは、外国において個人データを取り扱う場合に、当該外国の個人情報の保護に関する制度等を把握することをいう。金融分野における個人情報取扱事業者は、外国において個人データを取り扱う場合には、外的環境を把握した上で、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なければならない。

7 金融分野における個人情報取扱事業者は、個人データの安全管理に係る基本方針・取扱規程等の整備として、次に掲げる「組織的安全管理措置」を講じなければならない。

（組織的安全管理措置）

(1) [略]

(2) 各管理段階における安全管理に係る取扱規程

2 この条における「組織的安全管理措置」とは、個人データの安全管理措置について従業者（法第21条参照）の責任と権限を明確に定め、安全管理に関する規程等を整備・運用し、その実施状況の点検・監査を行うこと等の、個人情報取扱事業者の体制整備及び実施措置をいう。

3 [同左]

[項を加える。]

4 [同左]

[項を加える。]

5 金融分野における個人情報取扱事業者は、個人データの安全管理に係る基本方針・取扱規程等の整備として、次に掲げる「組織的安全管理措置」を講じなければならない。

（組織的安全管理措置）

(1) [同左]

(2) 各管理段階における安全管理に係る取扱規程

[①～⑤ 略]

⑥ 漏えい等事案（漏えい等又はそのおそれのある事案をいう。以下同じ。）への対応の段階における取扱規程

8 金融分野における個人情報取扱事業者は、個人データの安全管理に係る実施体制の整備として、次に掲げる「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」及び「技術的安全管理措置」を講じなければならない。

（組織的安全管理措置）

[①～⑤ 略]

⑥ 漏えい等事案に対応する体制の整備

（人的安全管理措置）

[①～③ 略]

④ 従業者による個人データ管理手続の遵守状況の確認

（物理的安全管理措置）

① 個人データの取扱区域等の管理

② 機器及び電子媒体等の盗難等の防止

③ 電子媒体等を持ち運ぶ場合の漏えい等の防止

④ 個人データの削除及び機器、電子媒体等の廃棄

（技術的安全管理措置）

[①～③ 略]

④ 個人データの漏えい等防止策

[⑤～⑦ 略]

第9条 従業者の監督（法第24条関係）

[①～⑤ 同左]

⑥ 漏えい事案等への対応の段階における取扱規程

6 金融分野における個人情報取扱事業者は、個人データの安全管理に係る実施体制の整備として、次に掲げる「組織的安全管理措置」、「人的安全管理措置」及び「技術的安全管理措置」を講じなければならない。

（組織的安全管理措置）

[①～⑤ 同左]

⑥ 漏えい事案等に対応する体制の整備

（人的安全管理措置）

[①～③ 同左]

④ 従業者による個人データ管理手続の遵守状況の確認

（技術的安全管理措置）

[①～③ 同左]

④ 個人データの漏えい・毀損等防止策

[⑤～⑦ 同左]

第9条 従業者の監督（法第21条関係）

1 金融分野における個人情報取扱事業者は、法第24条に従い、個人データの安全管理が図られるよう、適切な内部管理体制を構築し、その従業者に対する必要かつ適切な監督を行わなければならない。

当該監督は、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、事業の性質及び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。

[2・3 略]

#### 第10条 委託先の監督（法第25条関係）

1 金融分野における個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、法第25条に従い、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

当該監督は、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、委託する事業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。

2 [略]

3 金融分野における個人情報取扱事業者は、個人データを適正に取り扱っていると認められる者を選定し委託するとともに、取扱いを委託した個人データの安全管理措置が図られるよう、個人データの安全管理のための措置を委託先においても確保しなければならない。なお、二段階以上の委託が行われた場合には、委託先

1 金融分野における個人情報取扱事業者は、法第21条に従い、個人データの安全管理が図られるよう、適切な内部管理体制を構築し、その従業者に対する必要かつ適切な監督を行わなければならない。

当該監督は、個人データが漏えい、滅失又は毀損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、事業の性質及び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。

[2・3 同左]

#### 第10条 委託先の監督（法第22条関係）

1 金融分野における個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、法第22条に従い、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

当該監督は、個人データが漏えい、滅失又は毀損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、委託する事業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。

2 [同左]

3 金融分野における個人情報取扱事業者は、個人データを適正に取り扱っていると認められる者を選定し委託するとともに、取扱いを委託した個人データの安全管理措置が図られるよう、個人データの安全管理のための措置を委託先においても確保しなければならない。なお、二段階以上の委託が行われた場合には、委託先

の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行わなければならない。

具体的には、金融分野における個人情報取扱事業者は、例えば、以下を実施すること。

- ① 個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準を定期的に見直さなければならない。

なお、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方法（テレビ会議システム（映像と音声の送受信により相手の状態を相互に認識できる方法をいう。）） を利用する方法を含む。以下同じ。）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。

- ② 委託者の監督・監査・報告徴収に関する権限、委託先における個人データの漏えい・盗用・改ざん及び目的外利用の禁止、再委託に関する条件及び漏えい等事案が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的に監査を行う等により、定期的又は随時に当該委託契約に定める安全管理措置等の遵守状況を確認し、当該安全管理措置を見直さなければならない。

なお、委託契約に定める安全管理措置等の遵守状況については、個人データ管理責任者等が、当該安全管理措置等の見直し

の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行わなければならない。

具体的には、金融分野における個人情報取扱事業者は、例えば、以下を実施すること。

- ① 個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準を定期的に見直さなければならない。

なお、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。

- ② 委託者の監督・監査・報告徴収に関する権限、委託先における個人データの漏えい・盗用・改ざん及び目的外利用の禁止、再委託に関する条件及び漏えい等が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的に監査を行う等により、定期的又は随時に当該委託契約に定める安全管理措置等の遵守状況を確認し、当該安全管理措置を見直さなければならない。

なお、委託契約に定める安全管理措置等の遵守状況については、個人データ管理責任者等が、当該安全管理措置等の見直し

を検討することを含め、適切に評価することが望ましい。

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等について、委託先に事前報告又は承認手続を求め、かつ、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本条の委託先の監督を適切に果たすこと及び再委託先が法第23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。

#### 第11条 個人データ等の漏えい等の報告等（法第26条関係）

以下の事項の他は通則ガイドラインの例による（施行規則第7条各号関係に限る。）。

- 1 金融分野における個人情報取扱事業者は、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（法第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つては金融庁長官等、法第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つては地方公共団体の長等）に報告しなければならない。
- 2 金融分野における個人情報取扱事業者は、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に従い、本人への通知等を行わなければならない。

を検討することを含め、適切に評価することが望ましい。

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等について、委託先に事前報告又は承認手続を求め、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本条の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。

[条を加える。]

3 金融分野における個人情報取扱事業者は、漏えい等事案が発覚した場合は、当該事態の内容等に応じて、次に掲げる事項について必要な措置を講じなければならない。

- ① 事業所内部における報告及び被害の拡大防止
- ② 事実関係の調査及び原因の究明
- ③ 影響範囲の特定
- ④ 再発防止策の検討及び実施

また、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。

#### 第12条 第三者提供の制限（法第27条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者は、法第27条第1項に従い、個人データの第三者提供について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、当該書面における記載を通じて、

- ① 個人データの提供先の第三者
- ② 提供先の第三者における利用目的
- ③ 第三者に提供される個人データの項目

を本人に認識させた上で同意を得ることとする。

本人の同意を得ようとする時点において、①に掲げる事項が特定できない場合には、①に掲げる事項に代わる本人に参考となるべき情報を本人に認識させた上で、同意を得ることとする

#### 第11条 第三者提供の制限（法第23条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者は、法第23条に従い、第三者提供についての同意を得る際には、原則として、書面によることとし、当該書面における記載を通じて、

- 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

を本人に認識させた上で同意を得ることとする。

。当該情報としては、次に掲げる例が考えられる。

(例)

- ・ 提供先の第三者の範囲や属性に関する情報

## 2 個人信用情報機関に対する提供

個人信用情報機関に対して個人データが提供される場合には、個人信用情報機関を通じて当該機関の会員企業にも情報が提供されることとなるため、個人信用情報機関に個人データを提供する金融分野における個人情報取扱事業者が本人の同意を得ることとする。

本人から同意を得るに当たっては、本人が、個人データが個人信用情報機関を通じて当該機関の会員企業にも提供されることを明確に認識した上で、同意に関する判断を行うことができるようにすることとする。このため、事業者は、同意を得る書面に、前項に定める事項のほか、個人データが当該機関の会員企業にも提供される旨の記載及び当該機関の会員企業として個人データを利用する者の表示を行うこととする。

「当該機関の会員企業として個人データを利用する者」の表示は、「当該機関の会員企業として個人データを利用する者」の外延を本人に客観的かつ明確に示すものであることが必要であり、会員企業の名称を記載する方法若しくは当該機関の規約等及び会員企業名を常時公表しているインターネットのホームページ（苦情処理の窓口の連絡先等、第20条の内容を記載したもの）のアドレスを記載する方法等により、本人が同意の可否を判断するに足

## 2 個人信用情報機関に対する提供

個人信用情報機関に対して個人データが提供される場合には、個人信用情報機関を通じて当該機関の会員企業にも情報が提供されることとなるため、個人信用情報機関に個人データを提供する金融分野における個人情報取扱事業者が本人の同意を得ることとする。

本人から同意を得るに当たっては、本人が、個人データが個人信用情報機関を通じて当該機関の会員企業にも提供されることを明確に認識した上で、同意に関する判断を行うことができるようにすることとする。このため、事業者は、同意を得る書面に、前項に定める事項のほか、個人データが当該機関の会員企業にも提供される旨の記載及び当該機関の会員企業として個人データを利用する者の表示を行うこととする。

「当該機関の会員企業として個人データを利用する者」の表示は、「当該機関の会員企業として個人データを利用する者」の外延を本人に客観的かつ明確に示すものであることが必要であり、会員企業の名称を記載する方法若しくは当該機関の規約等及び会員企業名を常時公表しているインターネットのホームページ（苦情処理の窓口の連絡先等、第18条の内容を記載したもの）のアドレスを記載する方法等により、本人が同意の可否を判断するに足



りる具体性をもって示すことをいう。また、本人に表示する個人情報信用情報機関の規約等においては、機関の加入資格及び会員企業の外延が明確に示されるとともに、個人データの適正管理、情報の目的外利用の防止等の観点から、安全管理体制の整備、守秘義務の遵守及び違反に対する制裁措置等を明確に記載することが適切である。

なお、金融分野における個人情報取扱事業者は、個人情報信用情報機関から得た資金需要者の返済能力に関する情報については、当該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、慎重に取り扱うこととする。

#### 3 与信事業における法第27条第2項（オプトアウト）の規定の適用

金融分野における個人情報取扱事業者は、与信事業に係る個人の返済能力に関する情報を個人情報信用情報機関へ提供するに当たっては、法第27条第2項の規定を適用しないこととし、前項に従い本人の同意を得ることとする。

#### 4 法第27条第5項第3号に定める通知等（共同利用の際の通知等）

金融分野における個人情報取扱事業者は、法第27条第5項第3号に定める「通知」については、原則として、書面によることとする。

金融分野における個人情報取扱事業者による「共同して利用する者の範囲」の通知等については、共同して利用する者を個別に列挙することが望ましい。また、共同して利用する者の外延を示

りる具体性をもって示すことをいう。また、本人に表示する個人情報信用情報機関の規約等においては、機関の加入資格及び会員企業の外延が明確に示されるとともに、個人データの適正管理、情報の目的外利用の防止等の観点から、安全管理体制の整備、守秘義務の遵守及び違反に対する制裁措置等を明確に記載することが適切である。

なお、金融分野における個人情報取扱事業者は、個人情報信用情報機関から得た資金需要者の返済能力に関する情報については、当該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、慎重に取り扱うこととする。

#### 3 与信事業における法第23条第2項（オプトアウト）の規定の適用

金融分野における個人情報取扱事業者は、与信事業に係る個人の返済能力に関する情報を個人情報信用情報機関へ提供するに当たっては、法第23条第2項の規定を適用しないこととし、前項に従い本人の同意を得ることとする。

#### 4 法第23条第5項第3号に定める通知等（共同利用の際の通知等）

金融分野における個人情報取扱事業者は、法第23条第5項第3号に定める「通知」については、原則として、書面によることとする。

金融分野における個人情報取扱事業者による「共同して利用する者の範囲」の通知等については、共同して利用する者を個別に列挙することが望ましい。また、共同して利用する者の外延を示

すことにより本人に通知等する場合には、本人が容易に理解できるように共同して利用する者を具体的に特定しなければならない。

外延を示す具体例としては、

- ・ 当社及び有価証券報告書等に記載されている、当社の子会社
- ・ 当社及び有価証券報告書等に記載されている、当社の連結対象会社及び持分法適用会社

といった方法が適切である。

なお、法第27条第5項第3号は、同号に定める「個人データの管理について責任を有する者」以外の共同して利用する者における安全管理責任等を免除する趣旨ではないことに留意する。

#### 第13条 外国にある第三者への提供の制限（法第28条関係）

以下の事項の他は外国第三者提供ガイドラインの例による。

1 金融分野における個人情報取扱事業者は、法第28条第1項に従い、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際には、原則として、書面によることとし、当該書面における記載を通じて、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、

- ① 個人データの提供先の第三者
- ② 提供先の第三者における利用目的
- ③ 第三者に提供される個人データの項目

を本人に認識させた上で同意を得ることとする。

本人の同意を得ようとする時点において、①に掲げる事項が特定できない場合には、①に掲げる事項に代わる本人に参考となる

すことにより本人に通知等する場合には、本人が容易に理解できるように共同して利用する者を具体的に特定しなければならない。

外延を示す具体例としては、

- ・ 当社及び有価証券報告書等に記載されている、当社の子会社
- ・ 当社及び有価証券報告書等に記載されている、当社の連結対象会社及び持分法適用会社

といった方法が適切である。

なお、同号は、同号に定める「個人データの管理について責任を有する者」以外の共同して利用する者における安全管理責任等を免除する趣旨ではないことに留意する。

[条を加える。]

べき情報を当該本人に認識させた上で同意を得ることとする。当該情報としては、次に掲げる例が考えられる。

(例)

- ・ 提供先の第三者の範囲や属性に関する情報

また、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、文字の大きさ及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。

- 2 金融分野における個人情報取扱事業者は、法第28条第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、特定できない旨及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。例えば、本人の同意を得ようとする時点において、移転先となる外国の候補が具体的に定まっており、当該候補となる外国の名称等、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、同項及び施行規則第17条第3項に基づく適法な情報提供とは認められない。したがって、この場合、金融分野における個人情報取扱事業者は、同条第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を本人に改

めて提供した上で、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なければならない。なお、改めて情報提供するには、前項の規定による情報提供にも留意することとする。

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を特定できた場合は、本人の求めに応じて、施行規則第17条第2項各号に定める情報を提供することとする。また、このような情報提供の求めが可能である旨を前項に定める書面における記載を通じて本人に認識させるとともに、第20条に定める「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、公表することとする。ただし、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、同項各号に定める情報の全部又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であっても、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とする（情報提供により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の具体例については、外国第三者提供ガイドライン6-2-2参照）。

3 金融分野における個人情報取扱事業者は、個人データの取扱いについて法第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施行規則第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及び内容、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、確認しなければならない。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

その後、当該第三者に個人データを提供した場合に施行規則第18条第1項第1号の規定により当該第三者による相当措置の実施状況を確認する際には、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り確認を行うこととする。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。

また、金融分野における個人情報取扱事業者は、法第28条第3項及び施行規則第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第20条に定める「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、公表することとする。

- 4 金融分野における個人情報取扱事業者は、前2項の定めるところにより、外国にある第三者に個人データを提供した場合には、提供先の第三者が所在する外国（第2項の場合においては、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の当該外国）の名称をインターネットのホームページへの掲載等により、公表するとともに、定期的に更新することが望ましい。

第14条 個人関連情報の第三者提供の制限等（法第31条関係）

以下の事項の他は通則ガイドラインの例による。

- 1 金融分野における個人情報取扱事業者は、個人関連情報取扱事業者から法第31条第1項の規定による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当たり、同項第1号の本人の同意を得る（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を含む。）際には、原則として、書面によることとし、当該書面における記載を通じて、

- 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上で同意を得ることとする。

[条を加える。]

なお、金融分野における個人情報取扱事業者は、個人情報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した場合には、法第21条に従い、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならないとされていることに留意する。

2 金融分野における個人情報取扱事業者は、法第31条第2項において読み替えて準用する法第28条第3項に従い、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、必要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。

#### 第15条 保有個人データに関する事項の公表等（法第32条関係）

以下の事項の他は通則ガイドラインの例による。

金融分野における個人情報取扱事業者が、法第32条に従い、保有個人データに関する事項を本人の知り得る状態に置く際には、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り、継続的に公表を行う方法として、例えば、第20条に定める「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を行うこと（保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。）、又は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。

#### 第16条 開示（法第33条関係）

以下の事項の他は通則ガイドラインの例による。

#### 第12条 保有個人データに関する事項の公表等（法第27条関係）

以下の事項の他は通則ガイドラインの例による。

金融分野における個人情報取扱事業者が、法第27条に従い、保有個人データに関する事項を本人の知り得る状態に置く際には、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り、継続的に公表を行う方法として、例えば、第18条に定める「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を行うこと、又は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。

#### 第13条 開示（法第28条関係）

以下の事項の他は通則ガイドラインの例による。

法第33条第2項第2号の場合の例としては、通則ガイドライン3-8-2（保有個人データの開示）に掲げている場合以外に、次に掲げる場合が考えられる。

（例）

- ・ 与信審査内容等の個人情報取扱事業者が付加した情報の開示請求を受けた場合
- ・ 保有個人データを開示することにより評価・試験等の適正な実施が妨げられる場合
- ・ 企業秘密が明らかになるおそれがある場合

なお、開示すべき保有個人データの量が多いことのみでは法第33条第2項第2号の場合に該当しない。

#### 第17条 理由の説明（法第36条関係）

金融分野における個人情報取扱事業者は、法第36条に従い、法第32条第3項、第33条第3項（同条第5項において準用する場合を含む。）、第34条第3項又は第35条第7項の規定により、本人から求められ、又は請求された措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合において、本人に対しその理由を説明する際には、措置をとらないこととし、又は異なる措置をとることとした判断の根拠及び根拠となる事実を示すこととする。

#### 第18条 開示等の請求等に応じる手続（法第37条関係）

以下の事項の他は通則ガイドラインの例による。

- 1 金融分野における個人情報取扱事業者は、法第37条に従い、開

法第28条第2項第2号の場合の例としては、通則ガイドライン3-5-2（保有個人データの開示）に掲げている場合以外に、次に掲げる場合が考えられる。

（例）

- ・ 与信審査内容等の個人情報取扱事業者が付加した情報の開示請求を受けた場合
- ・ 保有個人データを開示することにより評価・試験等の適正な実施が妨げられる場合
- ・ 企業秘密が明らかになるおそれがある場合

なお、開示すべき保有個人データの量が多いことのみでは法第28条第2項第2号の場合に該当しない。

#### 第14条 理由の説明（法第31条関係）

金融分野における個人情報取扱事業者は、法第31条に従い、法第27条第3項、第28条第3項、第29条第3項又は第30条第5項の規定により、本人から求められ、又は請求された措置の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合において、本人に対しその理由を説明する際には、措置をとらないこととし、又は異なる措置をとることとした判断の根拠及び根拠となる事実を示すこととする。

#### 第15条 開示等の請求等に応じる手続（法第32条関係）

以下の事項の他は通則ガイドラインの例による。

- 1 金融分野における個人情報取扱事業者は、法第32条に従い、開



示等の請求等を受け付ける方法を定めた場合には、第20条に定める「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を行うこと、又は事務所の窓口等での掲示・備付け等を行うこととする。

2 法第37条第1項及び施行令第12条第3号に基づき、開示等の請求等をする者が本人又は施行令第13条に定める代理人であることの確認の方法を定めるに当たっては、十分かつ適切な確認手続とするよう留意することとする。

なお、施行令第13条第2号の代理人による開示等の請求等に対して、事業者が本人にのみ直接開示等することは妨げられない。

#### 第19条 個人情報取扱事業者による苦情の処理（法第40条関係）

以下の事項の他は通則ガイドラインの例による。

法第40条第2項に定める必要な体制の整備の例としては、通則ガイドライン3-9（個人情報の取扱いに関する苦情処理）に掲げているもの以外に、苦情処理に当たる従業者への十分な教育・研修が考えられる。

[条を削る。]

示等の請求等を受け付ける方法を定めた場合には、第18条に定める「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を行うこと、又は事務所の窓口等での掲示・備付け等を行うこととする。

2 法第32条第3項及び施行令第10条第3号に基づき、開示等の請求等をする者が本人又は施行令第11条に定める代理人であることの確認の方法を定めるに当たっては、十分かつ適切な確認手続とするよう留意することとする。

なお、施行令第11条第2号の代理人による開示等の請求等に対して、事業者が本人にのみ直接開示等することは妨げられない。

#### 第16条 個人情報取扱事業者による苦情の処理（法第35条関係）

以下の事項の他は通則ガイドラインの例による。

法第35条第2項に定める必要な体制の整備の例としては、通則ガイドライン3-6（個人情報の取扱いに関する苦情処理）に掲げているもの以外に、苦情処理に当たる従業者への十分な教育・研修が考えられる。

#### 第17条 個人情報等の漏えい事案等への対応

1 金融分野における個人情報取扱事業者は、個人情報の漏えい事案等又は匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに法第36条第1項の規定により行った加工の方法に関する情報の漏えい事案（以下「個人情報等の漏えい事案等」という。）の事故が発生した場合には、監督当局等に直ちに報告することとする。

第20条 個人情報保護宣言の策定（法第21条、第32条及び基本方針関係）

1 金融分野における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、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（いわゆるプライバシーポリシー、プライバシーステートメント等。本ガイドラインにおいて「個人情報保護宣言」という。）を策定し、例えば、次に掲げる内容を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、公表することとする。

- ① [略]
- ② 法第21条における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 法第32条における開示等の手続等、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
- ④ [略]

2 金融分野における個人情報取扱事業者は、個人情報等の漏えい事案等の事故が発生した場合には、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を早急に公表することとする。

3 金融分野における個人情報取扱事業者は、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。

第18条 個人情報保護宣言の策定（法第18条、第27条及び基本方針関係）

1 金融分野における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、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（いわゆるプライバシーポリシー、プライバシーステートメント等。本ガイドラインにおいて「個人情報保護宣言」という。）を策定し、例えば、次に掲げる内容を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、公表することとする。

- ① [同左]
- ② 法第18条における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 法第27条における開示等の手続等、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
- ④ [同左]

2 [略]

3 個人情報保護宣言は、消費者等、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のが望ましく、そのための工夫として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。）による表示
- ・ 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

第21条 [略]

2 [同左]

[項を加える。]

第19条 [同左]

備考 表中の [ ] の記載は注記である。