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。

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　関係法令等の遵守、個人情報を目的外に利用しないこと及び苦情処理に適切に取り組むこと等、個人情報保護への取組方針の宣言
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　個人情報の取扱いに関する質問及び苦情処理の窓口

２　個人情報保護宣言には、消費者等、本人の権利利益保護の観点から、事業活動の特性、規模及び実態に応じて、次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。

①　保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止など、自主的に利用停止等に応じること。
②　委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めること。
③　事業者がその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したり、事業者が本人の選択による利用目的の限定に自主的に取り組むなど、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。
④　個人情報の取得元又はその取得方法（取得源の種類等）を可能な限り具体的に明記すること。

第19条　ガイドラインの見直し

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩、国際動向等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて、必要に応じ見直しを行うものとする。

○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定める件を次のように定め、個人情報の保護に関する法律及び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の一部を改正する法律（平成二十七年法律第六十五号）の施行の日（平成二十九年五月三十日）から適用し、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（平成十七年金融庁告示第一号）は、同日をもって廃止する。

平成二十九年二月二十八日

個人情報保護委員会委員長　堀部　政男
金融庁長官　森　信親

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

目次

Ⅰ．金融分野における個人情報保護に関するガイドライン第８条に定める安全管理措置の実施について
⑴　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
１－１　個人データの安全管理に係る基本方針の整備
１－２　個人データの安全管理に係る取扱規程の整備
１－３　個人データの取扱状況の点検及び監査に係る規程の整備
１－４　外部委託に係る規程の整備
⑵　個人データの安全管理措置に係る実施体制の整備
１）実施体制の整備に関する組織的安全管理措置
２－１　個人データ管理責任者等の設置
２－２　就業規則等における安全管理措置の整備
２－３　個人データの安全管理に係る取扱規程に従った運用
２－４　個人データの取扱状況を確認できる手段の整備
２－５　個人データの取扱状況の点検及び監査体制の整備と実施
２－６　漏えい事案等に対応する体制の整備