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１条　目的（法第１条関連）

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。）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。平成 20 年４月 25 日一部変更。平成 21 年９月１日一部変更。以下「基本方針」という。）を踏まえ、金融庁が所管する分野及び法第 36 条第１項により指定を受けた分野（以下「金融分野」という。）における個人情報取扱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ため、金融分野における個人情報の性質及び利用方法にかんがみ、事業者が講ずべき措置の適切かつ有効な実施を図るための指針として定めるものである。

２　金融分野における各認定個人情報保護団体（法第 37 条第１項の認定を受けた団体をいう。以下同じ。）及び個人情報取扱事業者等においては、本ガイドライン等を踏まえ、各事業の実態等に応じて個人情報の適正な取扱いを確保するための更なる措置を自主的なルールとして定め、対象とする事業者等に遵守させること、及び自らが遵守することが重要である。

３　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、法、施行令、基本方針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。

４　金融分野において個人情報データベース等を事業の用に供している者のうち、法第２条第３項第５号の規定により「個人情報取扱事業者」から除かれる者においても、本ガイドラインの遵守に努めるものとする。

５　本ガイドラインにおいて記載した具体例については、これに限定する趣旨で記載したものではなく、また、個別ケースによって別途考慮すべき要素があり得るので注意を要する。

第２条　定義等（法第２条、施行令第１条、施行令第２条、施行令第３条及び施行令第４条関連）

１　「個人情報」とは、生存する個人に関する情報であって、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ものを含む。）をいう。

「個人に関する情報」とは、氏名、性別、生年月日、住所、年齢、職業、続柄等の事実に関する情報に限られず、個人の身体、財産、職種、肩書等の属性に関する判断や評価を表すすべての情報を指し、公刊物等によって公にされている情報や、映像、音声による情報も含まれる。これら「個人に関する情報」が、氏名等と相まって「特定の個人を識別することができる」ことになれば、それが「個人情報」となる。

なお、生存しない個人に関する情報が、同時に、遺族等の生存する個人に関する情報に当たる場合には、当該生存する個人に関する情報となる。

また、企業名等、法人その他の団体に関する情報は、基本的に「個人情報」には該当しないが、役員の氏名などの個人に関する情報が含まれる場合には、その部分については、「個人情報」に該当する。

さらに、「個人」には外国人も当然に含まれる。

2　「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、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う。

3　「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う。なお、個人情報データベース等から記録媒体へダウンロードされたもの及び紙面に出力されたもの（そのコピーを含む。）も含まれる。

4　「個人情報取扱事業者」とは、次に掲げる者を除いた、個人情報データベース等を事業の用に供している者をいう。ここでいう「事業の用に供している」の「事業」とは、一定の目的をもって反復継続して遂行される同種の行為であって、かつ、社会通念上事業と認められるものをいい、営利事業のみを対象とするものではない。

①　国の機関

②　地方公共団体

③　独立行政法人等（独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号）第２条第１項に規定する独立行政法人等をいう。）

④　地方独立行政法人（地方独立行政法人法（平成15年法律第118号）第２条第１項に規定する地方独立行政法人をいう。）

⑤　その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ない者

⑤の規定にいう者とは、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても5,000を超えない者とする（施行令第２条）。5,000を超えるか否かは、他人が管理している個人情報データベース等であっても、それを事業の用に供する場合には、当該個人情報データベース等を構成する個人情報によって識別される特定の個人の数も含めて判断する。例えば、個人信用情報機関の個人情報データベース等を利用する場合がこれにあたる。

また、個人情報データベース等の全部又は一部が他人の作成に係る個人情報データベース等であって、次のいずれかに該当するものを編集し、又は加工することな

くその事業の用に供するときは、それを構成する個人情報によって識別される特定の個人の数は、5,000 の数に数えない。

イ　氏名、住所・居所、電話番号のみが掲載された個人情報データベース等（例えば、電話帳やカーナビゲーション）

ロ　不特定かつ多数の者に販売することを目的として発行され、かつ、不特定かつ多数の者により随時に購入することができる又はできた個人情報データベース等（例えば、自治体職員録や弁護士会名簿）

５　「本人」とは、個人情報によって識別される特定の個人をいう。

６　「保有個人データ」とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、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すべてに応じることのできる権限を有する個人データであって、その存否が明らかになることにより公益その他の利益が害されるものとして次に掲げるもの以外のもの及び６か月以内に消去すること（更新することを除く。）となるもの以外のものをいう。

①　存否が明らかになることで、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの

②　存否が明らかになることで、違法又は不当な行為を助長し、又は誘発するおそれがあるもの

（例）

・　不審者情報やクレーマー情報、総会屋情報

・　暴力団等の反社会的勢力情報

③　存否が明らかになることで、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの

（例）

・　要人の行動予定情報

④　存否が明らかになることで、犯罪の予防、鎮圧又は捜査その他の公共の安全と秩序の維持に支障が及ぶおそれがあるもの

（例）

・　警察などから受けた捜査関係事項照会の対象情報

・　犯罪収益との関係が疑われる取引（疑わしい取引）の届出の対象情報

・　振り込め詐欺に利用された口座に関する情報

７　「個人信用情報機関」とは、個人の返済能力に関する情報の収集及び与信事業を行う個人情報取扱事業者に対する当該情報の提供を業とするものをいう。

８　前各項に定めるもののほか、本ガイドラインにおける用語は、他に特段の定めのない限り、法及び施行令の定義に従う。

第３条　利用目的の特定（法第 15 条関連）

１　金融分野における個人情報取扱事業者は、法第 15 条に従い、個人情報の取扱いに当たっては、個人情報がどのような事業の用に供され、どのような目的で利用されるかを本人が合理的に予想できるようできる限り特定しなければならない。

具体的には、「自社の所要の目的で用いる」といった抽象的な利用目的は、「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　金融分野における個人情報取扱事業者は、特定の個人情報の利用目的が、法令等に基づき限定されている場合には、その旨を明示することとする。

３　金融分野における個人情報取扱事業者が、与信事業に際して、個人情報を取得する場合においては、利用目的について本人の同意を得ることとし、契約書等における利用目的は他の契約条項等と明確に分離して記載することとする。この場合、事業者は取引上の優越的な地位を不当に利用し、与信の条件として、与信事業において取得した個人情報を与信業務以外の金融商品のダイレクトメールの発送に利用することを利用目的として同意させる等の行為を行うべきではなく、本人は当該ダイレクトメールの発送に係る利用目的を拒否することができる。

４　金融分野における個人情報取扱事業者が、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には、その旨を利用目的に明示しなければならない。さらに、明示した利用目的について本人の同意を得ることとする。

５　金融分野における個人情報取扱事業者は、法第 15 条第２項に従い同条第１項の規定により特定した利用目的を変更する場合には、変更後の利用目的が変更前の利用目的からみて、社会通念上本人が想定できる範囲を超えて行ってはならない。

（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」

なお、本人が想定できない変更を行う場合には、法第 16 条第１項の規定により、本人の同意を得なければならない。

第４条　同意の形式について（法第 16 条及び法第 23 条関連）

金融分野における個人情報取扱事業者は、法第 16 条及び法第 23 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のできない方式で作られる記録を含む。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。

なお、本人が未成年者、成年被後見人、被保佐人及び被補助人であって、個人情報の取扱いに関して同意したことによって生ずる結果について判断できる能力を有していない場合などは、親権者や法定代理人等から同意を得る必要がある。

第５条　利用目的による制限（法第 16 条関連）

１　金融分野における個人情報取扱事業者は、法第 16 条に従い、あらかじめ本人の同意を得ないで、法第 15 条の規定に従い特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

ただし、あらかじめ本人の同意を得るために個人情報を利用することは、当初特定した利用目的にない場合にも、目的外利用には当たらない。

２　金融分野における個人情報取扱事業者は、合併その他の事由により他の個人情報取扱事業者から事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

ただし、あらかじめ本人の同意を得るために個人情報を利用することは、承継前の利用目的にない場合にも、目的外利用には当たらない。

３　前二項の規定は、次に掲げる場合については、適用しない。

①　法令に基づく場合

（例）

・　国税通則法（昭和 37 年法律第 66 号）第 74 条の２から第 74 条の６に基づいて税務当局が行う質問検査及び国税犯則取締法（明治 33 年法律第 67 号）第１条等に基づいて収税官吏又は徴税吏員の行う犯則事件の任意調査に応じる場合

・　刑事訴訟法（昭和 23 年法律第 131 号）第 197 条に基づく捜査関係事項照会に応じる場合

・　犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号。以下「犯罪収益移転防止法」という。）第８条第１項に基づき疑わしい取引を届け出る場合

・　金融商品取引法（昭和 23 年法律第 25 号）第 210 条、第 211 条等に基づく証

券取引等監視委員会の職員による犯則事件の調査に応じる場合

・　弁護士法（昭和 24 年法律第 205 号）第 23 条の２第２項に基づく弁護士会の照会に応じる場合

なお、当該法令に、第三者が個人情報の提供を求めることができる旨の規定はあるが、正当な事由に基づきそれに応じないことができる場合には、金融分野における個人情報取扱事業者は、当該法令の趣旨に照らして目的外利用の必要性と合理性が認められる範囲内で対応するよう留意する。

②　人の生命、身体又は財産（法人の財産を含む。）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。

（例）

・ 暴力団等の反社会的勢力情報、業務妨害行為を行う悪質者情報、振り込め詐欺に利用された口座に関する情報を企業間で共有する場合

③　公衆衛生の向上又は児童の健全な育成の推進のために特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。

（例）

・ 病気の予防、治療に関する研究等を目的とする情報交換を行う場合

④　国の機関若しくは地方公共団体又はその委託を受けた者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であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（例）

・　税務当局の任意調査に応じる場合

・　警察の任意調査に応じる場合

・　振り込め詐欺に利用された口座に関する情報を警察に提供する場合

・　一般統計調査に回答する場合

なお、金融分野における個人情報取扱事業者は、任意の求めの趣旨に照らして目的外利用の必要性と合理性が認められる範囲内で対応するよう留意する。

第６条　機微（センシティブ）情報について

１　金融分野における個人情報取扱事業者は、政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報（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　法令等に基づく場合

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

③　公衆衛生の向上又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　国の機関若しくは地方公共団体又はその委託を受けた者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・宗教等の団体若しくは労働組合への所属若しくは加盟に関する従業員等の機微（センシティブ）情報を取得し、利用し、又は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（センシティブ）情報を取得、利用又は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（センシティブ）情報を取得し、利用し、又は第三者提供する場合

⑧　機微（センシティブ）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

２　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、前項に掲げる場合に取得し、利用し、又は第三者提供する場合には、同項に掲げる事由を逸脱した取得、利用又は第三者提供を行うことのないよう、特に慎重に取り扱うこととする。

第７条　適正な取得（法第 17 条関連）

金融分野における個人情報取扱事業者は、法第 17 条に従い、偽りその他不正の手段により個人情報を取得してはならない。事業者は、第三者から個人情報を取得するに際しては、本人の利益の不当な侵害を行ってはならず、個人情報の不正取得等の不当な行為を行っている第三者から、当該情報が漏えいされた個人情報であること等を知った上で当該情報を取得してはならない。

第三者からの提供（法第 23 条第 1 項各号に掲げる場合並びに個人情報の取扱いの委託、事業の承継及び共同利用に伴い、個人情報を提供する場合を除く。）により、個人情報（施行令第 2 条第 2 号に規定するものから取得した個人情報を除く。）を取得する場合には、提供元の法の遵守状況（例えば、オプトアウト（第 13 条第 4 項の規定（法第 23 条第 2 項・第 3 項）参照）、利用目的、開示手続、問合せ・苦情の受付窓口を公表していることなど）を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得の経緯を示す契約書等の書面の点検又はこれに代わる合理的な方法により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

第８条　取得に際しての利用目的の通知等（法第 18 条関連）

１　法第 18 条第１項においては、個人情報取扱事業者は、個人情報を取得した場合、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。

「通知」の方法については、金融分野における個人情報取扱事業者は、原則として、

書面によることとする。

「公表」の方法については、金融分野における個人情報取扱事業者は、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　法第 18 条第２項においては、個人情報取扱事業者は、同条第１項の規定にかかわらず、本人との間で、契約を締結することに伴って契約書その他の書面に記載された個人情報を取得する場合は、あらかじめ利用目的を明示しなければならないとされている。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１項から第３項までの規定は、次に掲げる場合については、適用されない。

①　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

（例）

・　暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、振り込め詐欺に利用された口座に関する情報、業務妨害行為を行う悪質者情報の提供者が逆恨みを買うおそれがある場合

②　利用目的を本人に通知し、又は公表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権利又は正当な利益を害するおそれがある場合

（例）

・　開発中の新サービス、営業ノウハウが明らかになることにより、企業の健全な競争を害する場合

・　暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、振り込め詐欺に利用された口座に関する情報、業務妨害行為を行う悪質者情報を取得したことが明らかになることにより、情報提供を受けた企業に害が及ぶ場合

③　国の機関又は地方公共団体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であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（例）

・　犯罪捜査への協力のため、被疑者等に関する情報を取得した場合

④　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

（例）

・　電話等での資料請求に対して、請求者が提供した住所及び氏名に関する情報を請求された資料の送付のみに利用する場合

・　今後連絡を取り合うために名刺交換をした場合

・　着信において相手方の電話番号が非通知でない場合で、同じ用件で当方から相手方に電話を掛け直す場合

第９条　データ内容の正確性の確保（法第 19 条関連）

金融分野における個人情報取扱事業者は、法第 19 条に従い、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

このため、事業者は、預金者又は保険契約者等の個人データの保存期間については契約終了後一定期間内とする等、保有する個人データの利用目的に応じ保存期間を定め、当該期間を経過した個人データを消去することとする。

ただし、法令等に基づく保存期間の定めがある場合には、この限りでない。

第 10 条　安全管理措置（法第 20 条及び基本方針関連）

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 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　この条における「人的安全管理措置」とは、従業者との個人データの非開示契約等の締結及び従業者に対する教育・訓練等を実施し、個人データの安全管理が図られるよう従業者を監督することをいう。

4　この条における「技術的安全管理措置」とは、個人データ及びそれを取り扱う情報システムへのアクセス制御及び情報システムの監視等の、個人データの安全管理に関する技術的な措置をいう。

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）

⑴　規程等の整備

①　個人データの安全管理に係る基本方針の整備

②　個人データの安全管理に係る取扱規程の整備

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

④　外部委託に係る規程の整備

⑵　各管理段階における安全管理に係る取扱規程

①　取得・入力段階における取扱規程

②　利用・加工段階における取扱規程

③　保管・保存段階における取扱規程

④　移送・送信段階における取扱規程

⑤　消去・廃棄段階における取扱規程

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　個人データの管理責任者等の設置

②　就業規則等における安全管理措置の整備

③　個人データの安全管理に係る取扱規程に従った運用

④　個人データの取扱状況を確認できる手段の整備

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

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　従業者との個人データの非開示契約等の締結

②　従業者の役割・責任等の明確化

③　従業者への安全管理措置の周知徹底、教育及び訓練

④　従業者による個人データ管理手続きの遵守状況の確認

（技術的安全管理措置）

①　個人データの利用者の識別及び認証

② 個人データの管理区分の設定及びアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データの漏えい・毀損等防止策
⑤ 個人データへのアクセスの記録及び分析
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及び分析
⑦ 個人データを取り扱う情報システムの監視及び監査

第 11 条　従業者の監督（法第 21 条及び基本方針関連）

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　この条における「従業者」とは、個人情報取扱事業者の組織内にあって直接又は間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、事業者との間の雇用関係にない者（取締役、執行役、理事、監査役、監事、派遣社員等）も含まれる。

３　金融分野における個人情報取扱事業者は、次に掲げる体制整備等により、従業者に対し必要かつ適切な監督を行わなければならない。

① 従業者が、在職中及びその職を退いた後において、その業務に関して知り得た個人データを第三者に知らせ、又は利用目的外に使用しないことを内容とする契約等を採用時等に締結すること。
② 個人データの適正な取扱いのための取扱規程の策定を通じた従業者の役割・責任の明確化及び従業者への安全管理義務の周知徹底、教育及び訓練を行うこと。
③ 従業者による個人データの持出し等を防ぐため、社内での安全管理措置に定めた事項の遵守状況等の確認及び従業者における個人データの保護に対する点検及び監査制度を整備すること。

第 12 条　委託先の監督（法第 22 条及び基本方針関連）

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　「委託」には、契約の形態や種類を問わず、金融分野における個人情報取扱事業者

が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。

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きを求める、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。

第 13 条　第三者提供の制限（法第 23 条関連）

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、次に掲げる場合を除くほか、あらかじめ本人に同意を得ることなく、個人データを第三者に提供してはならない。

①　法令に基づく場合

②　人の生命、身体又は財産（法人の財産を含む。）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。

③　公衆衛生の向上又は児童の健全な育成の推進のために特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。

④　国の機関若しくは地方公共団体又はその委託を受けた者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であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（注）上記①～④の具体例は、第５条第３項①～④における例示と同じ。

なお、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。

２　「第三者」について

「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ものをいい、自然人、法人その他の団体を問わない。

３　個人信用情報機関に対する提供について

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、第１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 23 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。

4　法第 23 条第２項（オプトアウト）について

法第 23 条第２項においては、個人情報取扱事業者が、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、同項各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、当該個人データを第三者に提供することができるとされている。

「本人が容易に知り得る状態」とは、本人が知ろうと思えば、時間的にも、その手段においても、容易に知ることができる状態をいい、金融分野における個人情報取扱事業者は、自らの金融商品の販売方法等の事業の態様に応じた適切な方法により、継続的な公表を行う必要があり、例えば、事務所の窓口等での常時掲示・備付け、インターネットのホームページへの常時掲載などが考えられる。

5　与信事業における法第 23 条第２項の適用について

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信用情報機関へ提供するに当たっては、法第 23 条第２項を用いないこととし、本条第３項に従い本人の同意を得ることとする。

6　法第 23 条第４項（「第三者」に該当しないもの）について

法第 23 条第４項に従い、次に掲げる場合において、当該個人データの提供を受ける者は、第三者に該当しない。

①　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合

②　合併その他の事由による事業の承継に伴って個人データが提供される場合

③　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

7　法第 23 条第４項第３号に規定する通知等（共同利用の際の通知等）について

金融分野における個人情報取扱事業者は、法第 23 条第４項第３号に定める「通知」は、原則として、書面によることとする。

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、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。

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」（以下「管理責任者」という。）は、共同して利用する者において、第一次的に苦情を受け付け、その処理を行うとともに、開示、訂正等及び利用停止等の決定を行い、安全管理に責任を有する者をいう。なお、同号は、管理責任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。

８　経過措置

法の施行前に第三者提供されている個人データについては、法施行前に法第 23 条第１項の規定による本人からの同意に相当する同意があれば、施行後においても引き続き第三者への提供を行うことができることとされている（法附則第３条）。金融分野における個人情報取扱事業者が法施行前に行った与信事業に際して、個人信用情報機関への提供についての同意を本人から得ている場合、加入資格に関する当該機関の規約等及び会員企業名の公表は法の施行前に実施されることが適当である。

第 14 条　保有個人データに関する事項の公表等（法第 24 条及び施行令第５条関連）

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、保有個人データに関し、利用目的、開示等の手続等の同条第１項各号に掲げる事項を本人の知り得る状態に置かなければならない。

「本人の知り得る状態」とは、本人が知ろうと思えば知ることができる状態をいい、事業者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、継続的な公表として、例えば、第 23 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。

なお、利用目的に第三者提供が含まれる場合には、法第 24 条第１項第２号に定める「すべての保有個人データの利用目的」の内容として、その旨を記載しなければならない。

第 15 条　開示（法第 25 条関連）

金融分野における個人情報取扱事業者は、法第 25 条に従い、本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、書面の交付による方法（開示の求めを行った者が同意した方法があるときは、当該方法）により、遅滞なく、保有個人データを開示しなければならない。ただし、同条第１項各号に従い、次のいずれかに該当する場合には、その全部又は一部を開示しないことができる。

①　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

②　当該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

（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②に該当しない。

③　他の法令に違反することとなる場合

（例）

・　犯罪収益移転防止法第８条第２項（顧客への届出事実の漏えい）

金融分野における個人情報取扱事業者が法第 25 条第１項各号の規定に基づき、求められた保有個人データの全部又は一部について開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知しなければならない。また、その決定の理由について、根拠とした法の条文及び判断の基準となる事実を示して遅滞なく説明を行うこととする。

第 16 条　訂正等（法第 26 条及び施行令第６条関連）

金融分野における個人情報取扱事業者は、法第 26 条に従い、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除（以下「訂正等」という。）を求められた場合には、利用目的の達成に必要な範囲内において、遅滞なく、事実の確認等の必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

訂正等を行った場合、又は訂正等を行わないこととした場合は、本人に対し、遅滞なくその旨（訂正等を行った場合は、その内容を含む。）を通知しなければならない。

なお、金融分野における個人情報取扱事業者が訂正等を行わない場合は、訂正等を行わない根拠及びその根拠となる事実を示し、その理由を説明することとする。

第 17 条　利用停止等（法第 27 条関連）

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、本人から、当該本人が識別される保有個人データが法第 16 条の規定に違反して取り扱われているという理由又は法第 17 条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

２　金融分野における個人情報取扱事業者は、法第 27 条第２項に従い、本人から、当該本人が識別される保有個人データが法第 23 条第１項の規定に違反して第三者に提

供されているという理由によって、当該保有個人データの第三者への提供の停止を求められた場合であって、その求めに理由があることが判明したときは、遅滞なく、当該保有個人データの第三者への提供を停止しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

３　金融分野における個人情報取扱事業者は、法第 27 条第１項の規定に基づき求められた保有個人データの全部若しくは一部について利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき又は同条第２項の規定に基づき求められた保有個人データの全部若しくは一部について第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨（本人から求められた措置と異なる措置を行う場合には、その措置内容を含む。）を通知しなければならない。

第 18 条　理由の説明（法第 28 条関連）

金融分野における個人情報取扱事業者は、法第 24 条第３項、法第 25 条第２項、法第 26 条第２項又は法第 27 条第３項の規定により、本人から求めら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は、本人に対し、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し、その理由を説明することとする。

第 19 条　開示等の求めに応じる手続（法第 29 条、施行令第７条及び施行令第８条関連）

１　金融分野における個人情報取扱事業者は、法第 29 条に従い、開示等の求めを受け付ける方法を定めた場合には、第 23 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 29 条第３項及び施行令第７条第３号に基づき、開示等の求めをする者が本人又は施行令第８条に規定す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８条第２号の代理人による開示等の求めに対して、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 20 条　手数料（法第 30 条関連）

金融分野における個人情報取扱事業者は、法第 30 条に従い、手数料を徴収する場合には、同様の内容の開示等手続の平均的実費の予測に基づき、合理的な手数料額を算定する等の方法により、実費を勘案して合理的であると認められる範囲において手数料の額を定めなければならない。

第 21 条　個人情報取扱事業者による苦情の処理（法第 31 条関連）

１　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、個人情報の取扱いに関する苦情を受けたときは、その内容について調査し、合理的な期間内に、適切かつ迅速に処理するよう努めなければならない。

２　金融分野における個人情報取扱事業者は、苦情処理手順の策定、苦情受付窓口の設置、苦情処理に当たる従業者への十分な教育・研修など、苦情処理を適切かつ迅速に行うために必要な体制の整備に努めなければならない。

第 22 条　漏えい事案等への対応（基本方針関連）

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の事故が発生した場合には、監督当局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、漏えい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、個人情報の漏えい事案等の事故が発生した場合には、漏えい事案等の対象となった本人に速やかに漏えい事案等の事実関係等の通知を行うこととする。

第 23 条　個人情報保護宣言の策定（法第 18 条、法第 24 条及び基本方針関連）

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かんがみ、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 24 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 24 条　「勧告」、「命令」及び「緊急命令」についての考え方（法第 34 条関連）

１　法第 34 条の金融庁長官の「勧告」（第１項）、「命令」（第２項）及び「緊急命令」（第３項）については、金融分野における個人情報取扱事業者が本ガイドラインに沿って必要な措置等を講じたか否かにつき判断して行うものとする。

２　本ガイドライン中「～ならない」（「努めなければならない」を除く。）と記載されている規定について、それに従わない場合は、法第 16 条から第 18 条まで、第 20 条から第 27 条まで又は第 30 条第２項の規定違反と判断され得る。違反と判断された際、実際、「勧告」を行うこととなるのは、個人の権利利益を保護するため必要があると認めるときである。

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、法第 16 条から第 18 条まで、第 20 条から第 27 条まで又は第 30 条第２項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かんがみ、個人情報の取扱いに関して、金融分野の個人情報取扱事業者等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等においては、遵守に努めるものとする。

３　「命令」は、単に「勧告」に従わないことをもって発することはなく、正当な理由なくその勧告に係る措置をとらなかった場合において個人の重大な権利利益の侵害が切迫していると認めるときに限られる。

「緊急命令」は、金融分野における個人情報取扱事業者が法第 16 条、第 17 条、第 20 条から第 22 条まで又は第 23 条第１項の規定に違反した場合において、個人の重大な権利利益を害する事実があるため緊急に措置をとる必要があると認めるときに、「勧告」を前置せずに行うこととする。

第 25 条　ガイドラインの見直しについて

本ガイドラインについては、社会情勢の変化、国民の意識の変化、技術動向の変化等諸環境の変化を踏まえ、必要に応じ見直しを行うものとする。