「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（案）」への意見一覧

番号	条文	質問の概要	回答
1	全般（実務指針の位置付け）	「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等についての実務指針」（以下、実務指針）の位置付け等を明確にして頂きたい。特に、実務指針の位置付け（告示もしくは事務ガイドライン等）、「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、ガイドライン）との関係、実務指針違反時の罰則適用の有無について明確にして頂きたい。	実務指針は、ガイドライン第10条から第12条に定められた安全管理措置等について、事業者の講ずべき措置等を明らかにするものです。このため、安全管理措置に該当する実務指針に定められた規定のうち、個人情報の保護に関する法律（以下、保護法）第20条から第22条の解釈に係る内容は義務規定であり、これらに違反した場合には保護法第34条（勧告及び命令）、ひいては保護法第56条（罰則）の対象となります。
2	全般（義務規定又は努力規定）	実務指針のうち「義務規定」とされている項目については、各項目の実現に向け継続的に努力すべき「努力規定」としていただけないか。	実務指針の内容については、保護法第20条から第22条までの解釈に係る内容は義務規定となります。 なお、実務指針において事業者の講ずべき措置として定められた事項について、その具体的な対応方法は、各事業者の自主的な取組みを求めるものです。
3	全般（義務規定又は努力規定）	実務指針には、高度な基準のみを示すべきであり、具体的で詳細な安全管理措置義務を規定すべきではありません。実務指針には、「最も望ましい事例」を示すにとどめ、事業者が実務指針に規定されたすべての事項に応じた措置を講ずることが、法律上・行政上の義務ではないことを明記すべきです。	実務指針の内容については、保護法第20条から第22条までの解釈に係る内容であるか、個人情報の保護に関する基本方針の定める「格別の措置」に該当するかは、個々の規定の内容ごとに位置付けられるものであり、保護法第20条から第22条までの解釈に係る内容は義務規定となります。 なお、実務指針において事業者の講ずべき措置として定められた事項について、その具体的な対応方法は、各事業者の自主的な取組みを求めるものです。

番号	条文	質問の概要	回答
4	全般（実務指針の対象）	実務指針は、金融分野の個人情報取扱事業者の子会社・関連会社及び外部委託先（金融分野の個人情報取扱事業者でない）も適用対象となるのか。また委託先が金融分野の事業者のための事務とはいえないものを取扱うときも同様の安全管理水準が適用されるかを確認したい。	ガイドライン及び実務指針は、金融庁が所管する分野及び保護法第36条第1項に基づき指定を受けた分野（以下「金融分野」という。）における個人情報取扱事業者に加え、当該個人情報取扱事業者の委託先及びその再委託先が適用の対象となります。従って、金融分野における個人情報取扱事業者に該当しない委託先及びその再委託先においても、金融分野の個人情報に関する業務の受託先として、ガイドライン及び実務指針に基づき、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が求められることとなります。ただし、保護法第22条は委託先の監督の目的を「その取り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」と規定しているため、仮に受託された個人データの管理が事業部門や事業所単位で完全に遮断されているのであれば、当該事業部門や事業所単位で安全管理に係る基本方針・取扱規程の整備等の措置を実施することも認められます。また、子会社や関連会社については、当該事業者が金融分野における個人情報取扱事業者に該当しなければ、ガイドライン及び実務指針の適用対象とはなりません。
5	全般（事業者の裁量）	「実務指針」の記載事項が「個人データの内容や性質、利用の態様等に関わらず画一的な措置を求めるものではない」ことを確認したい。	実務指針では、事業者における個人データの安全管理に必要かつ適切な内容が各事業者における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に盛り込まれることを必要としておりますが、その具体的な対応方法については各事業者の自主的な取組みを求めるものです。
6	全般（事業者の裁量）	個人データの安全管理に係る規程等や運用体制整備の具体的な方法については、各事業者の自主的な取組みを求めるものであることを実務指針の前段等に明記頂きたい。	実務指針では、事業者における個人データの安全管理に必要かつ適切な内容が各事業者における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に盛り込まれることを必要としておりますが、その具体的な対応方法については各事業者の自主的な取組みを求めるものであり、この点はガイドラインに対する意見募集への回答としても明らかにしております。

番号	条文	質問の概要	回答
7	全般（事業者の裁量）	実務指針の遵守にあたっては、具体的な水準は事業者の判断に委ねられているという理解でよいか。	実務指針では、事業者における個人データの安全管理に必要かつ適切な内容が各事業者における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に盛り込まれることを必要としておりますが、その具体的な対応方法については各事業者の自主的な取組みを求めているものです。 但し、事業者の裁量は、あくまで保護法第20条が定める「個人データの安全管理のために必要かつ適切なもの」である限りにおいて認められるものであり、事業者の措置は「個人データの安全管理のために必要かつ適切なもの」に適合する必要があります。
8	全般（柔軟性の確保）	安全管理のための方針と手続きは技術変革に対応できるよう十分な柔軟性を持たせることが重要であり、広範な目的の下においてセキュリティ方針と手続きの設定を義務付けるべきである。	安全管理措置については、個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理を目的とし、技術革新等に対応したものとなるよう、ガイドラインにおいて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を定めており、ガイドライン及び実務指針に基づき、事業者等の自主的なルール策定及び措置の実施等が期待されます。なお、実務指針については、技術革新等に対応した見直しを行うよう検討してまります。
9	全般（個人情報・個人データの定義）	市販の人名録、会社情報書籍及びインターネットの検索ページ上の個人情報等については、ガイドライン及び実務指針が適用されないとの例外規定を設けて頂きたい。	実務指針は保護法に基づくものであるため、対象となる「個人情報」及び「個人データ」の定義についても、保護法に基づき定められたガイドラインの定義によるものです。

番号	条文	質問の概要	回答
10	全般（個人情報・個人データの定義）	個人として検索可能性がない個人情報は個人データに該当しないという理解でよいのか。個人情報と個人データを分ける基準である「検索可能性」は、「個人として検索可能な否か」で判断し、個人として検索可能性がない個人情報は個人データに該当しないという理解でよろしいか	安全管理措置の対象となる「個人データ」とは、保護法第2条第2項に規定される「個人情報データベース等」を構成する「個人情報」であり、一定の方式により検索可能な状態となっているものを指します。この検索可能性については、保護法第2条第2項第1号において「特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの」と規定されているほか、保護法第2条第2項第2号において「特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの」と規定されていることから、紙に個人情報が記録されたファイリングシステム等やコンピュータを用いていない場合であっても、氏名の50音順など個人情報を一定の方式によって整理・分類されていれば、一般的に容易に検索可能な状態にあるものと解されております。
11	1-2、1-3、1-4（規程の策定）	既に規程を策定している場合に、これを充実させて対応することも考えられるため、取扱規程の「策定」という文言を「整備」に統一すべき。	御指摘を踏まえ、修正致しました。
12	1-2（規程の要件）	実務指針において整備することが求められている「規程」は、各事業者においては「細則」「マニュアル」等、名称や形式を問われないこと、また、個々の規程等の構成が実務指針と一致せずとも、当該事業者で定めるルール全体として実務指針に規程する措置に対応していれば、事業者全体の「規程」としては問題ないことを確認したい。	実務指針で定める規程は、各管理段階ごとに措置内容等を明確化することを求めるものであり、「規程」の名称や形式の統一を求めるものではありません。従って、個々の規程等の構成を実務指針の記載と一致させる必要は必ずしもないほか、各管理段階ごとの取扱規程を、業務単位や商品単位ごとのように、実務に即して規程に盛り込むことも可能です。 但し、その際には、事業者全体として、①実務指針6-1から6-6-1において定められた事項が各管理段階ごとに全て盛り込まれていること、②事業者内の部署や商品ごとに定めた規程において盛り込まない規定がある場合には合理的な理由があること、が求められることとなります。
13	1-2（規程の要件）	各管理段階ごとに規程を定めることになっているが、各管理段階ごとに規定を定めるという要素が含まれていれば、実務に則してアレンジは可能という理解でよいか。	同上

番号	条文	質問の概要	回答
14	1-1、1-2、1-3、1-4、5-2、5-4（規程の見直し）	規程等の見直しの期間について、項目ごとに差異がある理由をうかがいたい。	「基本方針」（1-1）、「取扱規程」（1-2）及び「点検及び監査にかかる規程」（1-3）は、当該個人情報取扱事業者のみに係るものであるため、必要に応じて見直しを求めることとしています。一方、「外部委託に係る規程」（1-4、5-2、5-4）については、規程の内容の変更には委託先との交渉が必要であり、事業者のみの裁量により随時見直すことが困難な場合も想定されることから、「定期的な見直し」と規定しております。
15	1-1、1-2、1-3、1-4、5-2、5-4（規程の見直し）	「定期的に規程の見直しを行わなければならない」とした理由を確認したい。	同上
16	1-2（小規模事業者等の定義）	「全ての管理段階を同一人が取り扱う小規模事業者等」には「全ての管理段階を同一人が取り扱う個人情報取扱事業者内の業務又は部署」や「全ての管理段階を同一部署が取り扱う個人情報取扱事業者内の業務又は部署」が含まれ、これらについては各業務又は各部署ごとに全管理段階を通じた安全管理に係る取扱規程を定めることが認められると理解してよいのか。	各管理段階ごとの取扱規程を整備することを求めている趣旨は、漏えい事案等が発生した場合にどの管理段階における取扱いに問題があるかを検証し、適切な対応策を講ずることを可能とすることで、個人情報取扱事業者自らが取扱規程の有効性を高めていくことを可能とするものです。 但し、個人データ取扱部署が単一であり、「全ての管理段階を同一人が取り扱う」場合には、取扱部署が単一であるため、いずれの措置が不適切であっても問題点の特定が可能であることから、特例を設けております。 このため、個人データ取扱部署が複数ある個人情報取扱事業者については、「全ての管理段階を同一人が取り扱う小規模事業者等」には該当しません。

番号	条文	質問の概要	回答
17	1-2（小規模事業者等の定義）	「小規模事業者」の定義について具体的な要件を明らかにして頂きたい。	各管理段階ごとの取扱規程を整備することを求めている趣旨は、漏えい事案等に対応し、どの管理段階における取扱いに問題があるかを検証し、適切な対応策を講ずることを可能とすることで、事業者自らが取扱規程の有効性を高めていくことを可能とするものです。 仮に、個人データ取扱部署が単一であり、「全ての管理段階を同一人が取り扱う」場合には、管理段階は単一となるため、いずれの措置が不適切であっても問題点は特定が可能であると考えることができます。 このため、「常時使用する従業者の数が5人以下であり、物理的に各管理段階に担当者を分離することが不可能な場合」には「小規模事業者」の定義に該当し、例外規定の適用が認められることとなります。
18	1-2（小規模事業者等の定義）	「なお、全ての管理段階を同一人が取り扱う小規模事業者等においては・・・」の箇所の「等」は何を指すのか確認したい。	金融分野以外を主体とする個人情報取扱事業者であり、一部門のみが金融分野における事業を営み、当該金融分野における事業を営む部門が「小規模事業者」の定義に該当する個人情報取扱事業者を指します。
19	1-3（監査の特例）	「なお、個人データ取扱部署が単一である事業者においては・・・」の箇所で、「部署」の定義を明示していただきたい。	課やグループなど、個人情報取扱事業者における内部規程等に定められた分掌上の最小組織単位を指します。

番号	条文	質問の概要	回答
20	2-1-1（権限委譲）	個人データ管理責任者の業務とは統括責任を負うという意味であって、業務執行については権限委譲が可能と理解してよいか。	実務指針は、個人データ管理責任者が2-1-1に定めた業務を所管することを定めているのであり、全ての業務を個人データ管理責任者が実際に行うことを求めたものではなく、業務を行う権限を他の従業者に委譲することを妨げるものではありません。 但し、2-1-1①「個人データの安全管理に関する規程及び委託先の選定基準の承認及び周知」及び②「個人データ管理者及び4-1に規定する『本人確認に関する情報』の管理者の任命」についての決裁は、あくまで個人データ管理責任者の名義で行われる必要があります。 また、③「個人データ管理者からの報告徴収及び助言・指導」、④「個人データの安全管理に関する教育・研修の企画」及び⑤「その他個人情報取扱事業者全体における個人データの安全管理に関すること」についても、権限委譲の手続き等を規程等で明確化する必要があります。
21	2-1-1（本人確認に関する情報）	「本人確認に関する情報」の管理者はどのような業務を行うのか。	「本人確認に関する情報」とはID又はパスワード等を指します。このため、「本人確認に関する情報」の管理者はID又はパスワード等を付与及び管理する業務を行うこととなります。
22	2-2、3-1、3-2、3-3（懲戒処分）	現在の記載内容ですと、懲戒処分を前提に、主体的な労使協議による労働条件の決定に影響を与え、また、事業者が従業員に過度なロード・リスクを課した対処を進める虞があるため、組織全体として個人情報保護の体制整備を行うといった本来の趣旨と異なる運営が行なわれるのではないかとの懸念があります。また、これらの規定が主体的な労使協議による労働条件に影響を与えるのではないかと懸念しております。ついては、上記を踏まえた修正を行なうべきだと考えます。	御指摘の項目は、漏えい等の防止策の一環として、故意に漏えい等を行った従業者等に対する懲戒処分に関して就業規則等に規定を整備することを求めるものであり、本ガイドライン・実務指針をもって労働関係法令に反する行為を求めるものではありません。 また、就業規則等には内規等も含むことから、これらの規定は必ずしも「個人データの取扱に関する従業者の役割・責任」及び「違反時の懲戒処分」に関する全ての内容が就業規則又は労働協約に規定されることを求めているものではありません。 従いまして、原案を維持することと致しました。

番号	条文	質問の概要	回答
23	2-3（記録）	「取扱規程に定められた事項の遵守状況の記録」とは、各管理段階において作成される帳票類への各取扱者の捺印等により行うことと解釈して良いか確認したい。	実務指針では、個人情報取扱事業者における個人データの安全管理に必要かつ適切な内容が各事業者における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に盛り込まれることを必要としておりますが、その具体的な対応方法については各個人情報取扱事業者の自主的な取組みを求めています。このため、「取扱規程に定められた事項の遵守状況の記録」の具体的内容については、業務の実態に鑑み、個人情報取扱事業者が自ら設定することが求められるものであり、各取扱者の捺印を含め、必要かつ適切な方法によって頂く必要があります。
24	2-4（台帳等の作成単位）	2-4において「以下の事項を含む台帳等を整備しなければならない」とあるが、台帳は部署ごと、事業者ごと、あるいは顧客ごとのいずれの基準で整備するのこととなるのか。	2-4に定める台帳等の整備は、事業者ごとに整備を求めるものです。なお、台帳における各項目の記載については、対象が個人データであることから、基本的には「データベース」単位であり、紙媒体の場合には「同種の書類・帳票」単位で記載することが求められます。
25	2-4（台帳等の作成単位）	「個人データの取扱状況を確認できる手段の整備」として、「以下の事項を含む台帳等を整備しなければならない。」と規定され、「取得項目」等が挙げられている。「取得項目」等として記載する基準は、たとえば帳票単位という理解でよいか確認したい。また、可変式の書式の帳票については、それらに盛り込まれうる取得項目をすべて盛り込むことで、ひとつの「取得項目」とすることは問題ない事を確認したい。	2-4に定める台帳等の整備は、事業者ごとに整備を求めるものであります。台帳における各項目の記載については、対象が個人データであることから、基本的には「データベース」単位であり、紙媒体の場合には「同種の書類・帳票」単位で記載することが求められます。 なお、同種の書類・帳票で取得する項目が複数の形式となり得るものについては、一つの書類・帳票と整理し、「取得項目」の欄には盛り込まれ得る全ての項目を記載することで、本規定の要件を満たすものと考えられます。
26	2-4（アクセス制限）	2-4⑤の「アクセス制限」と6-1から6-5の「個人データへのアクセス制御」との違いは何か。両者に相違がない場合には、表現を統一願いたい。	御指摘を踏まえ、2-4⑤の「アクセス制限」を「アクセス制御」と修正致しました。
27	2-5-1（兼務の可否）	「点検責任者及び点検担当者を選任するとともに・・・」の箇所で、部署が少人数の場合などもあることから、点検責任者と点検担当者の兼務が可能であることを確認したい。	御指摘のとおりです。

番号	条文	質問の概要	回答
28	2-5-2（監査の定義）	「監査の実施に当たっては、監査対象となる個人データを取り扱う部署以外から監査責任者・監査担当者を選任し、監査主体の独立性を確保・・・」の箇所で、異なる部署が相互に監査する体制が可能であることを確認したい。	監査は、点検とは異なり、監査対象部署とは別個の立場から個人データの取扱状況を確認するものであり、単に各部署における個人データの取扱状況を確認するだけでなく、監査を踏まえて当該事業者全体としての個人データの取扱いの見直しが行われることが求められます。このため、監査部署は取扱状況の監督及び全体的見直し等の機能を持つ、監査部等の部署が一元的に行うことが望ましいものと考えられます。ただし、そうした一元化な機能を有する部署が存在しない場合には、監査結果を集約し事業者全体としての個人データの取扱いに関する適正な実施体制等を整備することを前提として、各部署が相互に監査を行うという手法は排除されるものではありません。
29	2-5-2（監査の定義）	「なお、監査部署が監査業務等により個人データを取り扱う場合には、当該部署における個人データの取り扱いについて、個人データ管理責任者が特に任命する者がその監査を実施しなければならない。」とあるが、ここで言う監査業務の監査者として個人データ管理責任者が特に任命する者は、監査の為に被監査部署に派遣された監査部署の監査チームのメンバー（主席者等）で構わないか。	監査は、2-5において「当該部署以外の者による」と規定されていることから、2-5-2に規定された「個人データ管理責任者が特に任命する者」は監査部署の従業者以外の者であることが求められます。
30	2-5-2（監査部署の監査）	「監査部署が監査業務等により個人データを取り扱う場合には、当該部署における個人データの取り扱いについて、個人データ管理責任者が特に任命する者がその監査を実施しなければならない。」とあるが、個人データ管理責任者だけが監査担当者の任命権を持つのではなく、社長や監査部長でも任命できるなど裁量の余地があってもいいのではないか。	当該規定は、個人データの取扱状況についての監査という事務について定めるものであり、2-1①において個人データ管理責任者が個人データの安全管理に係る業務遂行の総責任者であると規定されていることから、任命権については個人データ管理責任者に限定することと致します。
31	2-6、6-6（漏えい事案等の対応）	「漏えい事案等」についての対象情報は個人データであることを確認したい。また、条文には対象情報が個人データであることを明確に記載頂きたい。	実務指針2-6及び6-6は、ガイドライン第10条から第12条までに定められた安全管理措置についての内容を示すものであるため、ガイドライン第2条第4項に定める「個人データ」が対象となります。この点は、実務指針の位置付けにより、明確になっております。

番号	条文	質問の概要	回答
32	2-6、2-6-1（漏えい事案等の対応）	「漏えい事案等」の箇所の「等」とは漏えいの他に何を対象としているのか明示していただきたい。	保護法第20条に基づき、「滅失」及び「き損」を指します。
33	2-6（漏えい事案等の対応）	「①対応部署」の箇所で、専門部署を設けず既存の部署が担当することを可としていただきたい。	当該規定は、対応部署を明確化することを求めるものであり、既存部署が対応部署となることを排除するものではありません。
34	2-6-1（漏えい事案等の対応）	「①行政当局等」の箇所の「等」とは他に何を対象としているのか明示していただきたい。	御指摘を踏まえ、趣旨を明確化する観点から、ガイドラインとの平仄を合わせ、「監督当局等への報告」と修正致しました。なお、「等」には、警察等捜査当局が該当することとなります。
35	2-6-1（漏えい事案等の対応）	「②本人への通知等」の箇所の「等」とは他にどのような対応を対象としているのか明示していただきたい。	「等」とは漏えい等に関する謝意の表明又は原因の説明等が該当することとなります。
36	2-6-1（漏えい事案等の対応）	消費者金融業界では、漏えい事案の発生にともない事業者が直ちに本人に通知することは、借入の秘匿性ゆえに本人が望まないケースも有り得ることから、「公表」を原則とし、本人への通知については、当該本人の利益侵害が切迫している場合などに限定するよう修正して頂きたい。	御指摘のようなケースにおいては、本人への通知の際における情報の本人以外に対する秘匿性への十分な配慮が必要であるものの、本人への通知の必要性が否定されるものではないと考えられ、原案を維持することと致しました。
37	3-1（非開示契約等）	非開示契約等の締結は、全ての従業者ではなく、管理者に限定すべきではないか。管理者以外の従業者については、就業規則等の個人情報の保護に関する規則を定め、違反時の処分を明確化すれば十分ではないか。	就業規則等の作成・変更にあたっては、必ずしも各従業者の同意を必要としていない一方、個人データの漏えい・き損防止は、一従業者の誤った取扱いにより多大な被害が発生し得るため、各従業者における責任等の認識が不可欠であることから、従業者との個人データ非開示契約等の締結を別途求めることとしております。
38	3-3（教育及び訓練）	個人情報を実際に取扱う従業者に関しては、かかる研修を行うことを義務付けるとしても、その他の全従業者に関しては、かかる研修および継続的教育を行うことは「最も望ましい事例」と位置付けることを提案いたします。	従業者への安全管理措置の周知徹底、教育及び訓練は、保護法第20条及び第21条を根拠とするガイドライン第10条及び第11条の内容に関する規定のため、義務規定となります。

番号	条文	質問の概要	回答
39	3-3（教育及び訓練）	「個人データの安全管理に係る就業規則等に違反した場合の懲戒処分の周知」とは、教育の中で周知、徹底させるという理解でよいか確認したい。	御指摘のとおりです。
40	3-4（遵守状況確認の頻度）	「個人データ管理手続の遵守状況の確認」における程度・頻度について確認したい。	「個人データ管理手続の遵守状況等の確認」については、3-4に定めているとおり、「2-3に基づく記録及び確認」及び「2-5に基づく点検・監査」により確認することとされております。 なお、「2-3に基づく記録及び確認」及び「2-5に基づく点検・監査」における程度及び頻度については、事業者自身が自ら安全管理の観点から必要かつ適切と判断する内容を規程に定め、それに従った運用を行うことが求められます。
41	4-1～4-7（技術的安全管理措置全般）	紙に記載された個人データについては、技術的安全管理措置の対象外であることを念のため確認したい。	御指摘の紙媒体の個人データについては、当該個人データへの技術的安全管理措置の適用が物理的に不可能な場合に該当するのであれば、技術的安全管理措置の対象外となることがあるものと解します。
42	4-1～4-7（技術的安全管理措置全般）	実務指針が対象とするのは「個人データ」全般であるが、技術的安全管理措置は全ての個人データに一律に適用されるものではなく、記録媒体や取扱状況に応じ、事業者の判断によりいずれかの段階で適切な措置を講じればよいという理解でよいか。具体的には、紙媒体であるマニュアル情報や営業店のパソコン等にも、全ての技術的安全管理措置が必要ではないということでよいか確認したい。	実務指針では、安全管理措置は全ての個人データが対象となり、事業者における個人データの安全管理に必要かつ適切な内容が各事業者における規程等に盛り込まれることを必要としておりますが、その具体的な対応方法については各事業者の自主的な取組みを求めています。 御指摘の紙媒体の個人データについては、当該個人データへの技術的安全管理措置の適用が物理的に不可能な場合に該当するのであれば、技術的安全管理措置の対象外となるものと解します。 一方、事業者の管理下にある以上、当然に営業店のパソコン等においても「個人データへのアクセスの記録及び分析」等の技術的安全管理措置が必要となります。

番号	条文	質問の概要	回答
43	4-2-1、4-5、4-6、4-7（技術的安全管理措置全般）	本項目については、推奨（努力）項目とし個別企業の判断に委ねるべきと考える。	御指摘の項目は、保護法第20条から第22条の解釈に係る内容であるガイドライン第10条から第12条までに定められた安全管理措置についての内容であり、義務規定となります。但し、その具体的な対応方法については、関係団体が自主的に示す安全対策基準等の内容を踏まえ、各事業者の自主的な取組みによるものです。
44	4-1、6-2-2、6-3-2、6-4-2（利用者の識別及び認証）	金融審議会金融分科会特別部会議事録（平成16年10月15日）の中で有識者発言として、弊社などが製品化しております“虹彩”による本人確認方式が金融機関で採用できない生体認証方式例として述べられているが、この議事録記載の発言における“虹彩”認証方式の問題点は過去の海外事例によるもので、現時点では既に技術的に解決され、国内金融機関では既に導入実績もあります。こうした点を踏まえれば、実務指針では、生体認証として特定の方式を推奨するものでも、金融分野における生体認証として虹彩（アイリス）が否定されているものではないと考えているが、そうした認識でよいか。 また、このような誤解を避ける意味からも、情報通信技術の進展状況を良く了解した上で、適切に各種の措置を講じることが必要と考え、4-1については『4-1 金融分野における個人情報取扱事業者は、「個人データの利用者の識別及び認証」として、情報通信技術の進展状況を踏まえた上で、以下の措置を講じなければならない。』と修正するよう要望いたします。	ガイドライン第6条第1項第8号により機微情報に該当する生体認証情報については、本人の同意に基づき、本人確認に用いる場合を除き、取得・利用又は第三者提供を行わないこととなっております。実務指針においては、ガイドラインに定める措置を確保するために求められる技術的安全管理措置等の内容を定めており、生体認証情報の具体的な認証方式については、特定の認証方式の採用を推奨したり、否定するものではありません。 なお、実務指針は、あくまで現時点における実用化された技術や業務プロセス等を踏まえたものであり、将来的に更に進んだ技術等により業務プロセスの見直し等が行われた場合には、適宜・適切にその内容を見直すことが必要であることは、4-1だけでなく実務指針全体に該当するものであることから、原案を維持することと致しました。
45	4-2（管理区分の設定及びアクセス制御）	個人データに管理区分を設定するにあたり、役職別（支店長、役席、一般職員等）に設定するのではなく、例えば、部署別（融資担当、預金担当等）に設定することでも実務指針の定めに沿っていることになるのか。	個人データの管理区分は、業務の実態に鑑み、個人情報取扱事業者が自ら設定することが求められるものであり、その内容が保護法第20条が求める安全管理の観点から必要かつ適切であれば、部署別にアクセス管理区分を設定することも可能です。
46	4-3（アクセス権限の管理）	「個人データへのアクセス権限を付与する従業者数を必要最小限に限定すること」とあるが、当該個人データにアクセスをする必要性がある従業者を「必要最小限」により排斥するものでないことを確認したい。	御指摘の項目は、漏えい等の防止や発生時の漏えいルートの解明等の観点からアクセス権限を付与する従業者数を限定することを求めているものであり、業務上の必要性のある従業者による個人データへのアクセスを制限するものではありません。

番号	条文	質問の概要	回答
47	4-3（アクセス権限の管理）	4-2でアクセス権限の設定が示されたうえで、4-3②において従業者のアクセス権限を必要最小限に限定するとあるが、これは営業店においては業務遂行に必要な従業者へのアクセス権限の設定を排除するものではないと考えてよいか。	同上
48	4-4-1、6-4-1（個人データの保護策）	4-4-1②「伝送データの漏えい防止策」が暗号化のことであるならば、推奨（努力）項目とすべきと考える。	御指摘の項目は、保護法第20条から第22条の解釈に係る内容であるガイドライン第10条から第12条までに定められた安全管理措置についての内容であるため、義務規定となります。但し、その具体的な対応方法については、関係団体が自主的に示す安全対策基準等の内容を踏まえ、各事業者の自主的な取組みによるものであり、御指摘の手法のみを義務付けるものではありません。
49	4-4-1、6-4-1（個人データの保護策）	4-4-1③「個人データ保護策を講ずること」の措置として、コンピュータウイルスの防御をする場合、防御対策としてどのような対応が考えられるか。	4-4-1③の措置としては、不正プログラムからシステム及びデータを守るため、コンピュータウィルスの侵入又は不正アクセスによるプログラムの改ざん等を防止する対策を講ずることを求めるものです。その具体的な対応方法については、関係団体が自主的に示す安全対策基準等の内容を踏まえ、各事業者の自主的な取り組みによるものであり、御指摘の項目には、一般的に、①ウィルスソフト（ワクチンソフト）の導入、②ダウンロードしたファイル等のウィルス・チェックの厳格な実施、などが含まれます。
50	4-5（アクセスの記録及び分析）	「個人データへのアクセスの記録及び分析」について、「アクセスの記録及び分析」の対象に、個人情報を取扱う全てのシステムを対象としているわけではないことを確認したい。	安全管理措置は全ての個人データが対象となるものであるため、「個人データへのアクセスの記録及び分析」については、サーバーだけでなく、スタンドアローンのパソコンなどを含め、全てのシステムが対象となります。但し、御指摘の紙媒体の個人データについては、当該個人データへの技術的安全管理措置の適用が物理的に不可能な場合に該当するのであれば、技術的安全管理措置の対象外となることがあるものと解します。 なお、具体的な分析の手法については、「個人データのアクセスの記録及び分析」は保護法第20条が定める「個人データの漏えい、滅失又はき損の防止」の観点から求められているものであり、全ての個人データのアクセスの記録を悉皆的に分析することに代えて、漏えい等のリスクの高い個人データへのアクセスを重点的に分析するなどの方法も認められます。

番号	条文	質問の概要	回答
51	4-5（アクセスの記録及び分析）	「個人データへのアクセスの記録及び分析」とあるが、「分析」とは、漏えい等の防止が目的であり、漏えい等につながる可能性のあるアクセスを洗い出すことであることを確認したい。	御指摘のとおり、「個人データのアクセスの記録及び分析」は保護法第20条が定める「個人データの漏えい、滅失又はき損の防止」の観点から求められているものであり、具体的な方法として、全ての個人データのアクセスの記録を悉皆的に分析する以外に、漏えい等のリスクの高い個人データへのアクセスを重点的に分析する方法なども認められます。
52	4-5（アクセスの記録及び分析）	今後、システム手当が必要となるケースも想定されることから、システム対応の代替措置が可能であることの規定及び経過措置の規定を設けていただきたい。	御指摘の項目は、保護法第20条から第22条の解釈に係る内容であるガイドライン第10条から第12条までに定められた安全管理措置についての内容であり、義務規定となります。このため、御指摘の代替措置の内容が不明ですが、4-5に定める事項の実施が必要となります。
53	4-5、4-6、4-7（記録の保存期間）	「個人データへのアクセス記録を保存する期間」については、不正アクセスの分析等が済むまでの期間（当方では1年間）を想定しているがよいか。	「個人データへのアクセス記録を保存する期間」については、業の実態や情報の取扱状況等に鑑み、個人情報取扱事業者自らが安全管理の観点から必要かつ適切な期間を設定することが求められます。具体的な保存期間の設定に際しては、別途定められている記録・分析及び点検・監査が適切に実施されるよう、これらの周期と整合的な期間とすることが求められます。
54	Ⅱ（従業者の監督）及びⅢ（委託先の監督）	従業者に対する監督は、監督・訓練の手順及び個人情報保護上の適切な対策の義務付けに限定すべきであり、委託先に対しても監督を義務付けるべきではない。	保護法は、第21条において事業者は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と定めるとともに、第22条において事業者は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と定めています。実務指針も、保護法及びガイドラインに基づき、必要かつ適切な監督の内容を定めております。
55	5-1（委託先の選定基準）	「委託先選定の基準」として、「実績等に基づく委託先の個人データ安全管理上の信用度」が規定されているが、過去に漏えい事象がある委託先であっても、事後に適切な措置がなされていればそれらを一律に排除するものではないことを確認したい。	御指摘のとおりと解されます。 過去の漏えい事案等の発生後に適切な対応がとられ、現時点で必要かつ適切な安全管理措置が図られていると判断できるのであれば、本規定によってそうした事業者への委託が妨げられるものではありません。

番号	条文	質問の概要	回答
56	5-1（委託先の選定基準）	「委託先選定の基準」として、「委託先の経営の健全性」が規定されているが、当該基準は漏えい等の防止の観点から設けられているものであり、財務状況等が悪化している企業を一律に委託先から排除するものではないことを確認したい。	御指摘のとおりと解されます。 本規定は、委託先における適切な個人情報保護の遂行の視点から経営の健全性についての審査を求めるものであり、財務状況等が悪化している企業を一律に委託先から排除するものではありません。
57	5-1-2（委託先の選定基準）	委託先の選定基準としての委託先の実施体制については、各項目において委託元となる金融機関等と同様のレベルまで求めるものではないことを確認したい。	委託先の選定基準としての委託先の実施体制については、実務指針に基づき必要とされる全ての事項を満たす必要があります。なお、委託先において取扱う個人データの性質や量等により、具体的に講じられる手法に差異があることは許容されます。
58	5-1-2（委託先の選定基準）	本条文の趣旨は、銀行が求められている安全管理措置と同等の体制整備を、委託先・再委託先に対して強いるものではないことを確認したい。	同上
59	5-2（委託先の監督）	「委託先における遵守状況を定期的又は随時に確認する」とされているが、「委託先における遵守状況について定期的又は随時に報告等を求め確認する」等と明示できないか。	委託先の監督については、保護法第22条及びガイドライン第12条に基づき、「委託を受けた者に対する必要かつ適切な監督が行われること」が求められております。実務指針では、その遵守状況の確認方法については5-2において「5-3に基づき」と規定しており、報告徴収に関する権限だけでなく、監督・監査に関する権限に基づく確認も含まれております。 従いまして、原案を維持することと致しました。
60	別添1～3（義務規定又は努力規定）	別添1から別添3の位置付けおよび努力規定か義務規定かを明確化していただきたい。	保護法第20条から第22条の解釈に係る内容としてガイドライン第10条から第12条までに定められた安全管理措置は義務規定であることから、ガイドライン第10条から第12条に基づき、安全管理措置として行うべき内容を定めた部分は、実務指針の本編であるか別添であるかにかかわらず義務規定となります。

番号	条文	質問の概要	回答
61	別添1（取扱者の限定、個人データの限定）	各管理段階ごとに、「取扱者の限定」、「個人データの限定」を定めることになっている。例えば「取扱者の限定」は部署ごと（融資部、営業部等）、「個人データの限定」は帳票ごと（融資の帳票類、預金の帳票類等）に定めることは実務指針に沿っていることになるか。	「取扱者の限定」については、業務の実態に鑑み、個人情報取扱事業者が自ら設定することが求められるものですが、その内容が保護法第20条が求める安全管理の観点から必要かつ適切であれば、部署別にアクセス管理区分を設定することも可能です。 また、「個人データの限定」は、業務の実態に鑑み、個人情報取扱事業者が自ら設定することが求められるものですが、その内容が保護法第20条が求める安全管理の観点から必要かつ適切であれば、帳票ごとに設定することも可能です。
62	別添1（記録及び分析）	各管理段階ごとの取扱規程に定めなければならないとされている取扱状況の「記録及び分析」に関して、個人データの「記録」を行う規定の趣旨・目的を確認したい。	「個人データのアクセスの記録及び分析」は法第20条が定める「個人データの漏えい、滅失又はき損の防止」の観点から求められているものであります。従って、個人データの取扱いの記録は、漏えい事案等が発生した際に、原因及び漏えいルートの解明等を行い、個人データの漏えい、滅失又はき損を防止するために行う必要があります。
63	別添1（記録及び分析）	「各段階での記録及び分析」を定めることになっているが、指針ではどこまでのレベルの分析を想定しているのか。	「個人データのアクセスの記録及び分析」は保護法第20条が定める「個人データの漏えい、滅失又はき損の防止」の観点から求められているものであり、漏えい等の防止に有効であることを前提として、「各段階での記録及び分析」の具体的内容については、業務の実態に鑑み、個人情報取扱事業者が個人データの安全管理に必要かつ適切な内容を自ら設定することが求められるものです。
64	別添1（記録及び分析）	各管理段階における「記録・分析」については、従業員の労働実態に多大な影響を与えかねないことから、個人情報保護の実効性と実際の運用において生じるロード等をふまえ、適宜見直しを検討いただきたい。	同上

番号	条文	質問の概要	回答
65	6-1（取得・入力の定義）	経済産業省ガイドラインでは、個人情報を本人から受け取る段階を「取得」、個人情報を情報システムに入力する段階を「入力」と定義し、それぞれに責任者を置くとされているが同様と考えていいか、取得・入力の定義を明示して頂きたい。	実務指針においては、「取得」は個人情報取扱事業者が自ら保管するために個人情報を本人から受け取る段階を指し、「入力」は個人情報取扱事業者が個人情報を情報システムに入力する段階を指します。なお、個人データ管理者については、実務指針では部署ごとに定めるよう規定しておりますが、役割の明確化として管理段階ごとに作業責任者を置くことを排除するものではありません。
66	6-1（取得・入力時の照合・確認）	「④取得・入力時の照合及び確認手続き」とは、データが正確に入力されたかどうかの照合・確認手続きなのか、それとも、取得・入力の取扱者としての本人確認及び権限等の照合・確認手続きなのか。	「④取得・入力時の照合及び確認手続き」は、具体的には取得時の確認手続きと入力時の照合手続きからなります。前者は、取得時の取扱者としての本人確認及び権限等の確認手続きを指し、後者は入力データが正確かどうか照合する手続きを指します。
67	6-2-1-1（持ち出しに関する上乗せ措置）	「個人データの管理区域外への持ち出しに関する上乗せ措置」について、例えば個人データの社外持出しを日常的に行うコンサルティングセールス業務等においては、管理区域として社外も含めて規定できることを確認したい。	何をもってコンサルティングセールス業務と定義されているか明確ではありませんが、御指摘の件は個人データ管理者が「2-1-2③個人データを取り扱う保管媒体の設置場所の指定及び変更等」に基づいてアクセス管理区域を定め、その内容を「6-2-1⑥機器・記録媒体等の管理手続き」に基づき規程に記載し、それに基づいて事業者の敷地外で個人データを取扱うケースを指すのではないかと思われます。 これに対し、6-2-1-1は、規程に定められた以外での取扱いは例外的な作業であり、そうした規程に定められていない作業フローは漏えい事案等に繋がりやすいため、当該措置は特に慎重な取扱いを求めることとしているものです。 従って、管理区域に顧客先など事業者の敷地外を定める場合には、6-2-1-1⑤に規定された個別の申請及び承認等は求められないものの、事業者の敷地外への持ち出しに関する各種リスク要因を洗い出した上で、厳格な取扱いが求められることとなります。具体的には、取扱者及び対象となる個人データの限定のほか、アクセス制御及び機器・記録媒体等の管理手続きなどを規程に定め、その規程に従った運用を行うことなど、個人データの安全管理の観点から必要かつ適切な措置を講じることが求められます。

番号	条文	質問の概要	回答
68	6-2-1-1（持ち出しに関する上乗せ措置）	コンサルティング営業においては、営業所・顧客先等の通常の営業活動を行う範囲が「管理区域」であるとの理解で問題ないか。	同上
69	6-2-1-1（持ち出しに関する上乗せ措置）	来店できないお客様等に対して、得意先係が訪問して集金や融資の相談等を行っているが、こうした営業活動には個人データを管理部署から外へ持ち出すことが必要となる。 このような外訪における個人データの取扱い方は、6-2-1-1に定める上乗せ措置の対象にはならないと考えてよいか。	何をもって得意先係の業務と定義されているか明確ではありませんが、御指摘の件は個人データ管理者が「2-1-2③個人データを取り扱う保管媒体の設置場所の指定及び変更等」に基づいてアクセス管理区域を定め、その内容を「6-2-1⑥機器・記録媒体等の管理手続き」に基づき規程に記載し、それに基づいて事業者の敷地外で個人データを取扱うケースを指すのではないかと思われます。 これに対し、6-2-1-1は、規程に定められた以外での取扱いは例外的な作業であり、そうした規程に定められていない作業フローは漏えい事案等に繋がりやすいため、当該措置は特に慎重な取扱いを求めることとしているものです。 従って、管理区域に顧客先など事業者の敷地外を定める場合には、6-2-1-1⑤に規定された個別の申請及び承認等は求められないものの、事業者の敷地外への持ち出しに関する各種リスク要因を洗い出した上で、厳格な取扱いが求められることとなります。具体的には、取扱者及び対象となる個人データの限定のほか、アクセス制御及び機器・記録媒体等の管理手続きなどを規程に定め、その規程に従った運用を行うことなど、個人データの安全管理の観点から必要かつ適切な措置を講じることが求められます。
70	6-3（保管・保存の定義）	経済産業省ガイドラインでは、「保管・ﾊﾞｯｸｱｯﾌﾟ」と表記され、「保存」とは表現していない。ﾊﾞｯｸｱｯﾌﾟは、災害・障害時の復旧向けに直近最新のものの保管することと解釈しますが、「保存」の解釈は「ﾊﾞｯｸｱｯﾌﾟ」と同様と考えてよいか明示していただきたい。	「保存」は個人データを加工せず、そのままの状態でとっておくことを指すため、バックアップもその一形態と解されます。
71	6-4-1（移送・送信時の照合及び確認）	「移送・送信時の照合及び確認手続き」とは宛先の照合・確認であることを確認したい。	「移送・送信時の照合及び確認手続き」は、FAX及びメール等の誤送信による漏えい等を防止する観点から、宛先の照合・確認を求めるものです。

番号	条文	質問の概要	回答
72	6-5（消去・廃棄）	廃棄段階の取扱規程の整備に関連して、ガイドライン第9条の規定中「保有する個人データの利用目的に応じ保存期間を定め、当該期間経過後の保有する個人データを消去することとする」とあるが、個人情報データベースAと同Bにそれぞれ個人データC（利用目的が同じ）が共通して含まれるケースでは、データベースAとBについてそれぞれ異なる保存期間を定めることはできるか。	実務指針では、事業者における個人データの安全管理に必要かつ適切な内容が各事業者における規程等に盛り込まれることを必要としておりますが、その具体的な対応方法については各事業者の自主的な取組みを求めています。このため、「保存期間の設定」についても同一項目の個人データに関し、複数の異なる利用目的がある場合、各々の利用目的に応じて、異なった保存期間を設定することは可能です。
73	別添2（機微情報全般）	機微情報に関する規程は、「各管理段階における取扱規程」とは別に定めてもよいか。	7-1の規定は、機微情報に係る各管理段階ごとに取扱内容を明確化することを求めるものであり、機微情報に関する規程を「各管理段階における取扱規程」と別に定めることを排除するものではありません。
74	別添2（機微情報全般）	機微情報の取得、利用又は第三者提供については、本人の同意により、これを可能とするとともに、公共政策目的に基づくものも取得、利用又は第三者提供を可能とすべきである。	ガイドライン第6条第1項第7号に基づき、金融分野の個人情報取扱事業者は、事業の適切な業務運営の確保とは関係が認められない場合、又は、業務遂行上の必要がない場合には、本人の同意があることを理由として機微情報を取得、利用又は第三者提供することは認められないと考えます。なお、御指摘の「公共政策目的」が、ガイドライン第6条第1項各号のいずれかに該当する場合には、取得、利用又は第三者提供が認められます。
75	別添2（生体認証情報全般）	生体認証情報の特性や認証精度等についての重要情報の明示的な説明なしに取得・利用した預金者の生体認証情報を漏洩させた金融機関の経営者・管理責任者には、重い刑事罰を課す事も考慮すべきだと考えます。	「7-1-1③ 取得に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項」は、機微情報の取得にあたっての本人同意の取得に際して、ガイドライン第6条第1項第8号に基づき同意を得ることを説明する必要があることを定めているものです。なお、機微情報を適切な業務運営その他の必要と認められる目的として認められる目的以外に使用することの禁止について、個人顧客情報の管理について各業法の体系上もその実効性を確保する観点から、金融分野の個人情報取扱事業者に係る各業法施行規則に定めることを予定しております。

番号	条文	質問の概要	回答
76	別添2（生体認証情報全般）	事業者が生体認証情報を取得する場合のデータの保管に関する指針として、「事業者のサーバー等ではなく、本人が管理するカードのICチップ等に保管する方式」を推奨すべきと考えます。	機微情報に該当する生体認証情報については、ガイドラインに基づき、本人確認のみに用いられるための措置が必要であり、実務指針は、同ガイドラインに基づき必要となる安全管理措置を定めております。従って、生体認証情報の管理が実務指針を満たす限り、管理方式として特定方式に限定する若しくは特定方式を推奨するものではありません。
77	別添2（生体認証情報全般）	実務指針の7-1-1-1①③及び7-1-2-1①④の規定は、ガイドライン第１条の「個人情報の適正な取り扱いの確保に関して行う活動を支援する」にある策定目的の範囲外であると考えます。	ガイドライン第1条の目的に基づき、生体認証情報についてもガイドライン第10条に定められた適切な安全管理措置が求められております。 このため、生体認証情報における不適切な安全管理措置は、ガイドライン第10条に反し、第1条の目的に反するものとなります。 従って、7-1-1-1①③及び7-1-2-1①④の規定は、ガイドライン第1条に基づくものであります。
78	7-1-1（機微情報の取得・入力）	法人顧客の役職員等に係る機微情報を本人以外の第三者から会話の中で受動的に取得する可能性がないとは限りませんが、当該機微情報を業務に利用することが想定されない場合であっても、本人に事情を説明し機微情報の取得について事後的に同意を得るなどの対応が求められるのでしょうか？	仮に第三者から会話の中で受動的に機微情報を受け取ったとしても、保管しない場合には「取得」に該当せず、本人の同意を得る必要もありません。しかし、会話等で認識した機微情報を、氏名等により個人を識別できる個人情報として保存するのであれば、ガイドライン第6条の要件を満たす必要があります。
79	7-1-1（機微情報の取得・入力）	本人への説明事項では、生体認証情報についての本人拒否率と他人受入率及びその計測のベース（計測基準等）のほか、その計数の意味や特性、更には本人拒否時に使用する救済策等についてまで漏れなく説明することを義務付けるべきであると考えます。	機微情報に該当する生体認証情報の取得にあたっての本人同意の取得に際しては、ガイドライン第6条第1項第8号に基づき同意を得ることを説明する必要があります。
80	7-1-1（機微情報の取得・入力）	7-1-1③「取得に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項」は、ガイドラインにおいて安全管理措置について規定する第10条から12条までに基づくものではなく、機微（センシティブ）情報について規定する第6条に基づくものであることを確認したい。	御指摘のとおりです。

番号	条文	質問の概要	回答
81	7-1-1（機微情報の取得・入力）	機微（センシティブ）情報の取扱いに関して定める事項とされている、「本人への説明事項」の内容は、例えば生命保険契約の申込に際しては、金融庁ガイドライン第6条第1項第7号に定める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、利用等を行うことについて説明することであることを確認したい。	御指摘のとおりです。
82	7-2（外部監査）	機微（センシティブ）情報に該当する生体認証情報の取扱に関し、「外部監査」と特に限定する必要はないのではないか。	機微（センシティブ）情報に該当する生体認証情報については、プライバシー保護上特に適正な取扱いが求められること等から、安全管理措置として求められる内容については専門的な知見をもって中立公正な立場から監査が行われる必要があり、個人データの適切な取扱いを担保するためには、外部監査は必須であると考えております。
83	7-2（外部監査）	従業員の入退室等に、指紋・静脈認証等の生体認証情報を利用している場合について、当該生体認証情報については外部監査は不要としていただきたい。	保護法第36条第1項第1号に基づき、雇用管理における個人情報の取扱いについては、「雇用管理に関する個人情報の適正な取扱いを確保するための事業者が講ずべき措置に関する指針（平成16年厚生労働省告示第259号）」によることとなります。
84	7-2、8-4（外部監査）	機微情報の収集及び個人信用情報機関の会員管理に関する実務指針の別添2及び別添3では外部監査が規定されています。これらの別添において、「外部監査」という言葉の定義は明らかにされていません。外部監査の意味を明確にしてください。	外部監査とは、当該個人情報取扱事業者から独立した者が実施主体となり、当該事業者においてガイドライン及び実務指針に従った安全管理措置が実施されていることを確認するための監査を意味します。
85	8-1（資格審査）	「あらかじめ定めた入会資格基準に基き・・・」の箇所の「入会資格基準」の要件を明示していただきたい。	入会審査の基準については、①「5-1 個人データ保護に関する委託先選定の基準」を満たすこと、②会員となろうとする個人情報取扱事業者が個人信用情報を返済能力の調査以外の目的のために使用しないこと及びその確認のための個人信用情報取扱機関によるモニタリングに書面等により同意すること、が含まれます。

番号	条文	質問の概要	回答
86	8-1（資格審査）	「会員が入会基準を逸脱し、・・・」の箇所の「入会基準」とは前項8-1の「入会審査基準」を指しているのか、または別の基準なのかを明確にしていただきたい。	御指摘を踏まえ、趣旨を明確化する観点から、8-1の「入会審査基準」を「入会基準」と修正致しました。
87	8-2（モニタリング）	「モニタリング」の定義を明示していただきたい。	8-2に定める「モニタリング」は、会員である個人情報取扱事業者が個人信用情報を返済能力の調査以外の目的のために使用していないことを確認するため、会員による個人信用情報へのアクセス状況を分析すること等を意味します。
88	8-4（外部監査）	「外部監査」の定義、要件を明示していただきたい。対象となる「信用情報管理の適切な取り扱い」とは何を指すのか、明確にしていただきますよう要望します。	外部監査とは、当該個人情報取扱事業者から独立した者が実施主体となり、当該事業者においてガイドライン及び実務指針に従った安全管理措置が実施されていることを確認するための監査を意味します。 また、御指摘を踏まえ、趣旨を明確化する観点から、「個人信用情報機関における信用情報管理の適切な取り扱いを確認する」を「個人信用情報機関個人におけるガイドライン及び実務指針に従った安全管理措置が実施されていることを確認する」と修正致しました。
89	8-4（外部監査）	外部監査を受けるためには、準備段階として、①規程等の整備、②取扱手順書の整備、③規定及び手順書に則った運用、④証跡を残す、という期間が必要となるため、平成17年4月1日までに外部監査による監査報告を受けることは実務上困難である。このため、外部監査については、全面施行後に猶予期間を設けていただきたい。	実務指針は、保護法及びガイドラインと同様に、平成17年4月1日から施行されることとなります。 このため、外部監査については、法施行後における個人情報の取扱いについての適切性を確認するために行われることとなります。