別紙１

コメントの概要及びコメントに対する金融庁の考え方

No.	該当箇所	コメントの概要	コメントに対する金融庁の考え方
金融分野における個人情報保護に関するガイドライン			
1	第 12 条第１項	「事業の規模」とは、委託先企業の事業規模ではなく、委託する事業自体の規模との理解でよいか。「委託する事業の規模」に関しては、一律の基準等はなく、各金融機関のリスクベース等で判断するものとの理解でよいか。	御指摘のとおりです。
2	第 12 条第３項①	「必要に応じて」の具体的内容や、「これに代わる合理的な方法による確認」の具体的確認方法には、一律の基準等はなく、各金融機関のリスクベース等で判断するものとの理解でよいか。	委託先選定時における、「実地検査等の要否」については、個人データが漏えい等した場合に本人が被る権利侵害の程度、委託する事業の規模や性質等に応じて、判断していただきたいと考えます。また、「これに変わる合理的な方法による確認」については、例えば「相手先からの書面による報告」が想定されます。
3	第 12 条第３項①	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とあるが、合理的な方法とは ISMS の取得等、第三者機関の規定取得証明で足りるか。	当該部分は、委託先選定に当たって、委託先の安全管理措置が個人情報保護法20条で求められるものと同等であることを確認するという観点から、実施することが望ましい措置として追加されたものです。このため、第三者機関による認定を取得していることは、委託先選定に当たっての判断材料の一つではありますが、「合理的な方法による確認」を満たすとはいえません。

4	第 12 条第 3 項①	例えば、委託開始前に、「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」の各項目の実施状況を確認する「個人データ取扱委託先の安全管理措置に関する確認書」等の書面を委託先から提出してもらう方法や、第三者による監査報告書を委託先から受け入れるといった方法は、「これに代わる合理的な方法による確認」として許容されるとの理解でよいか。	御指摘の方法も一つの方法であると考えられますが、「これに代わる合理的な方法による確認」の具体的な方法については、個別具体例毎に実態に即して判断していただきたいと考えます。
5	第 12 条第 3 項①	「個人データ管理責任者等」の定義は「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」に定義されているものと同義であるとの理解でよいか。また、「等」に含まれる具体的な範疇に特段の定めはなく、各金融機関が実務等を踏まえて判断するものとの理解でよいか。	「個人データ管理責任者等」の定義は「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」に定義されているものと同義です。「等」については、個人データ管理責任者に準ずる権限・責任を有する者を想定しております。
6	第 12 条第 3 項②	「定期的に監査を行う等により」とあるが、「監査」の方法は「現場への立入り」に限定されず、例えば「委託元が提示した項目に対する委託先からの報告」等、監督の実効性の確保という観点から委託元が適切と判断した方法により実施することも可能との理解でよいか。	委託先における安全管理措置等の遵守状況の具体的な確認方法については、御指摘の方法も一つの方法であると考えられますが、個人データが漏えい等した場合に本人が被る権利侵害の程度、委託先において取り扱う個人データの性質や量等に応じて、委託元による実地検査等も含めて、判断していただきたいと考えます。

7	第 12 条第 3 項②	「定期的に監査を行う等」には、例えば、「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」の各項目の実施状況を確認する書面を委託先から提出してもらい、個人データを取り扱う場所に赴いて、方針・規定・実施体制の整備状況や運用状況を確認すること、またはそれに代わる第三者による監査報告書を委託先から受け入れるといった方法等が含まれるとの理解でよいか。	委託先における安全管理措置等の遵守状況の具体的な確認方法については、御指摘の方法も一つの方法であると考えられますが、個人データが漏えい等した場合に本人が被る権利侵害の程度、委託先において取り扱う個人データの性質や量等に応じて、委託元による実地検査等も含めて、判断していただきたいと考えます。
8	第 12 条第 3 項②	委託先について「定期的に監査を行う等」には、委託先が所謂プライバシーマーク認定等を受けていることを定期的に確認することも含まれることを確認したい。	当該部分は、委託元においても、委託先における委託契約に定める安全管理措置等の遵守状況を把握するとする趣旨であることから、委託先がプライバシーマーク認定等を取得している場合でも、委託元が実地検査や書面による報告等を実施して、委託先における個人データの取扱状況を把握する必要があると考えます。
9	第 12 条第 3 項②	「金融分野における個人情報保護に関するガイドライン」の第 12 条第 3 項２号については、「定期的に監査を行う等により」を例えば「定期的に監査を行う又は個人データの取扱いの実情に見合った合理的な方法により」などと、一律に定期的な監査が求められるものではないことが明白となる表記をご検討いただきたい。	当該部分については、委託先における個人データの取扱状況の確認については、一律に定期的な監査を求めるものではありません。個人データが漏えい等した場合に本人が被る権利侵害の程度、委託先において取り扱う個人データの性質や量等に応じて、定期的な監査を中心に、実地検査や書面による報告等から、適切な措置を実施していただきたいと考えます。

10	第 12 条第 3 項②	「安全管理措置等」の「等」には、例えば、委託先が再委託を行う場合に、「委託先の事前報告または承認手続を求めること」や「直接また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」といったことも含まれるとの理解でよいか。	「等」は、委託契約に盛り込んでいる事項で、安全管理措置以外の事項を想定しております。個人データが漏えい等した場合に本人が被る権利侵害の程度、委託先において取り扱う個人データの性質や量等に応じて、判断していただきたいと考えます。
11	第 12 条第 3 項②	委託先を通して再委託先以降の管理が確認できればよく、再委託先以降を必ず直接監督しなければならない趣旨ではないとの理解でよいか。 加えて、委託先と再委託先の契約の見直しを求めるものではなく、委託先を通じて再委託先を監督し、問題があると判断した場合、「再委託先として許容しない」といった判断を、各金融機関がリスクベース等にもとづきそれぞれが判断するものとの理解でよいか。	再委託先の監督については、本人の個人データが漏えい等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い状況等に起因するリスクに応じて、委託先を通じた監督のみとせず、委託元による再委託先の監督も含めて、必要かつ適切な措置を講じていただきたいと考えます。 御質問の契約書の見直しの要否については、個別の事案に即して判断いただければと考えますが、例えば委託先が再委託先を適切に監督していることが確認できない場合等に、委託元が再委託先を直接監督することができる必要があると考えます。
12	第 12 条第 3 項②	「再委託先が法 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」には、例えば、再委託開始前や再委託中（1 年毎）に、「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」の各項目の実施状況を確認する書面（あるいはその写）や、第三者による監査報告書を、委託先から受け	再委託先の監督については、本人の個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、御指摘の方法のみとせず、委託元による再委託先の監督も含めて、必要かつ適切な措置を講じていただくことが望ましいと考えております。

		入れるといった方法等が含まれるとの理解でよいか。	
13	第 12 条第 3 項②	既に委託している委託会社との間でも新たに監査実施の要綱を追記のうえ、委託契約書を取り交わすことが必要となるのか。	御質問の契約書の見直しの要否については、個別の事案に即して御判断いただきたいと考えますが、例えば委託先が再委託先を適切に監督していることが確認できない場合等に、委託元が再委託先を直接監督することができる必要があると考えます。
14	第 7 条	登記簿謄本の情報をリスト化したものを第三者から取得する場合など、公表情報のみで構成された個人データを第三者から取得する場合において、適法に取得されたかどうかの確認方法として「公表情報（登記簿謄本等）との整合性の検証」が含まれるとの理解でよいか。	公表情報のみで構成された個人データを第三者から取得する場合における、適正取得の確認方法については、具体的なケースや場面に即して判断すべきであり、一概にお答えすることはできません。 なお、当該部分については、個人情報を取得する際に、当該個人情報が適法に取得されたことを確認した上で、個人情報を取得することが望ましいとしたものであり、個人情報を取得後に適正取得を確認するものではありません。
15	第 7 条	団体保険・団体年金保険における契約者（団体）からの所属員の個人情報の取得や、個人のお客さまからの家族の個人情報の取得のように、明らかに提供元が知り得るような個人情報を取得する場合には不正取得が想定されないため、「提供元の法の遵守状況」や提供元での「個人情報の取得方法」の確認を省略することが認められるとの理解でよいか。	明らかに提供元が知りうるような個人情報を取得することを以て、必ずしも適正に取得しているとは言い切れない可能性があります。一律に御指摘の対応を行うのではなく、個別具体的な状況に応じて、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、当該個人情報が適法に取得されたことを確認した上で、個人情報を取得することが望ましいと考えます。

16	第７条	「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」 とあるが、このうち、合理的な方法として個人情報の「取得ルート」（例示：ウェブ、イベント、アンケート等）ごとに、業務プロセスを段階的に作成させ、どの時点で　1.利用目的、2.開示手続、3.問合せ・苦情の受付窓口などを公表しているかを図示させたうえで誓約させるなどの手法で足りるか。	個人情報の適正に取得したか否かの具体的な確認方法については、具体的なケースや場面に即して判断すべきであり、一概にお答えすることはできません。
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			
17	２－１（注）	個人データの取扱いの点検・改善等の監督を行う「部署又は合議制の委員会」はどのような社内における位置づけを想定しているのか。専担である必要はなく、従来からある部署・委員会等が兼ねることも認められるのか。また、このような規定が提案された背景・理由を伺いたい。	今回の改正では、社内における個人データの取扱体制を拡充するという観点から、「個人データの取扱いの点検・改善等の監督を行う部署又は合議制の委員会（以下、「個人データの取扱いの監督を行う部署等」とする。）の設置を、「望ましい措置」として追加しております。その組織体制や社内における位置づけ等については、事業者の規模や特性等に応じて、御対応いただきたいと考えます。
18	２－１（注）	部署又は合議制の委員会の役割は、どのようなものを想定しているのか。	個人データの取扱いの監督を行う部署等は、個人データの取扱いの点検・改善等の監督を実施することを想定しております。なお、その具体的な運用方法等については、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、適切な措置を講じていただきたいと考えます。

19	２－１（注）	個人データ管理責任者、個人データ責任者等が、「個人データの取扱いの点検・改善等の監督を行う合議制の委員会」の構成員となるようにしていただきたい。また、「個人データの取扱いの点検・改善等の監督を行う部署又は合議制の委員会」による監査又は点検の結果等を踏まえ、個人データ管理責任者・個人データ責任者等は、個人データの取扱い状況を適切に評価し、必要があると認めるときは、その見直し等の措置を講ずるようにしていただきたい。	個人データの取扱いの監督を行う部署等の、具体的な運用方法等については、御指摘の方法も含め、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、適切な措置を講じていただきたいと考えます。
20	２－１（注）	外国銀行支店の場合、「個人データの取扱いの点検・改善等の監督を行う部署又は合議制の委員会」は、必ずしも在日支店に設置される必要はなく、例えば本店にかかる組織が有効に存在し機能していれば足りるとの理解でよいか。	今回の改正では、外国企業の在日支店においても、「個人データの取扱いの監督を行う部署等」を設置することが望ましいとしております。 なお、御質問にある国外の本店に個人データの取扱いの監督を行う部署等が設置されている場合において、国内の在日支店にも個人データの取扱いの監督を行う部署等を設置するか否かについては、個人データが漏えい、滅失又はき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い状況等に起因するリスク等に応じて、御判断いただきたいと考えます。
21	２－５－２（注）	「社内の対応の確認」の頻度については、一定の基準等はなく、各金融機関のリスクベース等で判断するもの	「情報セキュリティ対策に十分な知見を有する者に係る経験年数等の要件」や「社内の対応の確認の頻度」については、個人データ

		との理解でよいか。また、「情報セキュリティ対策に十分な知見を有する者」に係る経験年数等の要件に関しては、一定の基準等はなく、各金融機関が実情等を踏まえて判断し、要件を設定すべきものとの理解でよいか。	が漏えい、滅失又はき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い状況等に起因するリスクに応じて、御判断いただきたいと考えます。
22	４－５	「金融分野における個人情報取扱事業者は、「個人データへのアクセスの記録及び分析」として、個人データへのアクセスや操作を記録するとともに、当該記録の分析・保存を行わなければならない。また、不正が疑われる異常な記録の存否を定期的に確認しなければならない」とあるが、定期的に確認する頻度は、事業者の業態に応じて適宜設定することでよいか。	不正が疑われる異常な記録の存否を確認する（定期的な）頻度については、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、御判断いただきたいと考えます
23	４－５	個人データへのアクセスや操作は、外部からのアクセスだけでなく、事業者内部におけるアクセスや操作も記録されるのか。	御指摘のとおりです。
24	４－５	金融分野における個人情報取扱事業者は、「個人データへのアクセスの記録及び分析」として、個人データへのアクセスや操作を記録するとともにとあるが、操作の記録については具体的にどの程度までの操作履歴を記録すれば足りるのか、例示してほしい。	記録すべき操作の具体的な範囲については、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、適切な範囲を設定するものと考えます。

25	４－５	「異常な記録の存否の確認」は、これまでの個人データへのアクセス記録の分析においても、求められていたものと考える。本改正では、「また、不正が…」以降の下線部が追記されたことにより、「定期的に確認」することが追加的に求められているとの理解で良いか確認したい。	当該部分については、不正が疑われる異常な記録の存否を定期的に確認することを、明示的に規定したものです。
26	４－７	「監視システムの動作の定期的な確認」とは、監視システム等が問題なく作動していることなどを確認するといったことを意味しているとの理解でよいか。	御指摘のとおりです。
27	４－７	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情報システムの監視及び監査」として、個人データを取り扱う情報システムの利用状況、個人データへのアクセス状況及び情報システムへの外部からのアクセス状況を４－５及び４－６により監視するとともに、監視システムの動作の定期的な確認等、監視状況についての点検及び監査を行わなければならない」とあるが、定期的に確認する頻度は、事業者の実態に応じて設定することでよいか。	監視システムの動作の定期的な確認する頻度については、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、御判断いただきたいと考えます。
28	４－７	情報システムへの外部からのアクセス状況とあるが、システムに接続されている事業者内部の端末からのアク	御指摘の点については、既に「個人データへのアクセス状況」に含まれております。

		セス状況も含めていただきたい。	
29	５－３（注）	例えば、委託先において個人データを取り扱う者の氏名・役職または部署名を委託契約に盛り込むことが望ましいものの、実務的に困難な場合、個人データを取り扱う部署名と責任者（必ずしも全員の氏名を求めるものではない）を覚書・別表・別紙・別データ等で盛り込むといった対応も許容されるとの理解でよいか。	御指摘のとおりです。
30	５－３（注）	新たに委託契約を締結した後に、「委託先において個人データを取り扱う者の氏名・役職又は部署名」が変更される場合には、委託契約書またはその別紙を改定する必要はなく、例えば、委託先から定期的に報告するような対応、委託元が委託先に対する安全管理措置の遵守状況を確認する際等に通知書・報告書等により当該変更について把握するという対応、委託先における個人データを取り扱う者の氏名・役職または部署名等を一覧として委託先社内で管理し、それを委託元が確認するといった対応が、許容されるとの理解でよいか。	契約締結後、委託先において個人データを取り扱う者等が変更した場合には、委託契約書等を改訂する必要はありませんが、当該変更について、単に委託先において把握するだけでなく、委託元においても把握することが望ましいと考えます。 委託元による具体的な把握方法については、個人データが漏えい、滅失又はき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引状況等に起因するリスクに応じて、御判断いただきたいと考えます。
31	６－１（注） ６－２－１（注） ６－３－１（注）	規定する全ての措置を講じることが困難な場合には、他の措置と組み合わせるなどして、各事業者のリスクベース等にもとづいて判断し対応を行うことが可能との理解でよいか。また、例示されている事項については、あくまで手法の１つを示しているものであり、必ずしも例	取得・入力段階等における取扱規程に、「アクセス制御」として定めることが望ましいとされた措置の、具体的な実施方法については、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、御判断いただきたいと考えます。

		示されている手法を全て実施しなければならないものではなく、アクセス制御の手法は取り扱う個人データの性質・量に応じて、各事業者が適切に判断して対応すれば当該規定の趣旨を満たすとの理解でよいか。	なお、例示された事項については、例示以外の方法も含め、必要かつ適切な措置を講じていただきたいと考えます。
32	６－１（注）	「入退館（室）の記録の保存」が例示されているが、記録の保存期間は、事業者の実態に応じて設定することでよいか。	入退館（室）の記録の保存期間については、リスクと実態を踏まえて、御対応いただきたいと考えます。
33	６－１（注）	注書きにある例示は、預金等受入金融機関における個人顧客口座情報のように金融サービス利用者から幅広く取得されるデータの保護を意図した安全管理措置であると理解して良いか確認したい。	「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」は、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における個人情報取扱事業者の個人データの取扱いを対象としております。 なお、例示部分の具体的な実施方法については、個人データが漏えい、滅失又はき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い状況等に起因するリスクに応じて、例示以外の方法も含め、適切な措置を講じていただきたいと考えます。