個人データの安全管理措置等に関する指針
（個人情報保護指針別冊）

全国銀行個人情報保護協議会

目次

Ⅰ．目的等

（１）目的

本指針は、「個人情報保護指針」（以下「保護指針」という。）の「Ⅳ．安全管理措置」の規定にもとづき、全国銀行個人情報保護協議会（以下「協議会」という。）会員（以下「会員」という。）が取り扱う個人データまたは個人番号および特定個人情報の安全管理措置に関して定めること、ならびに保護指針「Ⅰ．２．（６）機微（センシティブ）情報」および「Ⅱ．５．機微（センシティブ）情報の取扱い」に定める「機微（センシティブ）情報」の安全管理措置等に関して定めることを目的とする。

（２）指針の遵守

本指針において、「（金融分野指針〇―〇）」または「（特定個人情報安全管理措置〇）」などと示している事項は、「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」（以下「金融分野指針」という。）または「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の「（別添１）特定個人情報に関する安全管理措置」と「（別添２）特定個人情報の漏えい等に関する報告等（事業者編）」（以下「特定個人情報安全管理措置」といい、「金融分野指針」と併せて「金融分野指針等」という。）において求められ、または望ましいとされている措置である。

それ以外に本指針が規定している事項は、会員が金融分野指針を遵守し、必要かつ適切な措置を講じるための考え方や具体的措置の一例を示したものであり、金融分野指針の解釈を示したものではない。

その中で、「必須項目」として列挙している事項および「〇〇しなければならない」等と規定している事項（同等以上の効果が認められる方法を含む。）は、保護指針本文と同様に、会員が遵守すべき事項を示したものである。

また、「例示項目」として列挙している事項および「次のような例がある」、「こととする」、「（例：〇〇など）」等と規定している事項は、個人データの安全管理のために、会員が実務の実態に応じて遵守すべき事項の具体例を示したものである。

なお、金融分野指針が対象としない事業における個人データの安全管理措置については、本指針の安全管理措置の内容を参考としつつ、個人情報保護委員会の「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）」の「７（別添）講ずべき安全管理措置の内容」を遵守しなければならない。

また、会員のうち、特定個人情報安全管理措置における「中小規模事業者」に該当する者においては、同安全管理措置における特例的な対応方法を採ることでも差支えない。「金融分野における個人情報保護に関するガイドライン」所定の金融分野の事業者は「中小規模事業者」に該当しないとされている点に留意する。

（３）定義

本指針における用語の定義は、保護指針「Ⅰ．２．定義」の規定によるほか、次に定めるところによる。

Ａ.「規程等」

「規程等」とは会員の内部規程、作業手順書、マニュアル等の文書化された定めをいう。

Ｂ.「記録媒体」、「紙媒体」、「記録媒体等」

ａ.「記録媒体」とは、データを記録・保存するために使用されるコンピュータ（サーバー・パソコン等を含む。）の磁気ディスク、ＵＳＢメモリ、光ディスク、磁気テープ、ＤＡＴ等をいう。

ｂ.「紙媒体」とは、情報を記録するために使用される帳票等の紙をいう。

ｃ.「記録媒体等」とは記録媒体および紙媒体をいう。

Ｃ.「保管」、「保存」

ａ.「保管」とは使用頻度が高い記録媒体等を随時使用できるように室内に置くことをいう。

ｂ.「保存」とは使用頻度が下がった記録媒体等を必要な期限を満たすまで倉庫等業務スペース室内以外の場所に置くことをいう。

Ｄ.「漏えい等」、「漏えい等事案」

「漏えい等」とは、「漏えい（外部に流出すること）」、「滅失（内容が失われること）」、「毀損（内容が意図しない形で変更されたり、内容を保ちつつも利用不能な状態となること）」をいう。「漏えい等事案」とは、漏えい等またはそのおそれのある事案をいう。

Ⅱ．安全管理措置

１．基本方針・取扱規程等の整備

（１）個人データの安全管理に係る基本方針の整備

会員は、次の事項を定めた個人データの安全管理に係る基本方針を策定し、当該基本方針を公表するとともに、必要に応じて基本方針の見直しを行わなければならない（金融分野指針１－１）。

Ａ．個人情報取扱事業者の名称
Ｂ．安全管理措置に関する質問および苦情処理の窓口
Ｃ．個人データの安全管理に関する宣言
Ｄ．基本方針の継続的改善の宣言
Ｅ．関係法令等遵守の宣言

（２）個人データの安全管理に係る取扱規程の整備

会員は、個人データの各管理段階における安全管理に係る取扱規程を整備し、各管理段階に７．に規定する事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。

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、各管理段階に取扱規程を定めることに代えて、全管理段階を通じた安全管理に係る取扱規程において次の事項を定めることも認められる（金融分野指針１－２）。

Ａ．取扱者の役割・責任
Ｂ．取扱者の限定
Ｃ．各管理段階において個人データの安全管理上必要とされる手続

（３）個人データの取扱状況の点検および監査に係る規程の整備

① 会員は、個人データの取扱状況に関する点検および監査の規程を整備し、次の事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。

なお、個人データ取扱部署が単一である会員においては、点検により監査を代替することも認められる（金融分野指針１－３）。

Ａ．点検および監査の目的
Ｂ．点検および監査の実施部署
Ｃ．点検責任者および点検担当者の役割・責任
Ｄ．監査責任者および監査担当者の役割・責任
Ｅ．点検および監査に関する手続

② 会員は、定められた規程等に従って業務手続が適切に行われたことを示す監査証跡を保持しておかなければならない。

（４）外部委託に係る規程の整備

会員は、外部委託に係る取扱規程を整備し、次の事項を定めるとともに、定期的に規程の見直しを行わなければならない（金融分野指針１－４）。

Ａ．委託先の選定基準

Ｂ．委託契約に盛り込むべき安全管理に関する内容

２．組織的安全管理措置

（１）組織的安全管理措置

会員は、個人データの安全管理措置に係る実施体制の整備における「組織的安全管理措置」として、次の措置を講じなければならない（金融分野指針 １））。

Ａ．個人データの管理責任者等の設置

Ｂ．就業規則等における安全管理措置の整備

Ｃ．個人データの安全管理に係る取扱規程に従った運用

Ｄ．個人データの取扱状況を確認できる手段の整備

Ｅ．個人データの取扱状況の点検および監査体制の整備と実施

Ｆ．漏えい等事案に対応する体制の整備

（２）個人データ管理責任者等の設置

① 会員は、（１）Ａ．の「個人データ管理責任者等の設置」として次の役職者を設置しなければならない（金融分野指針２－１）。

Ａ．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個人データ管理責任者

Ｂ．個人データを取り扱う各部署における個人データ管理者

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、個人データ管理責任者が個人データ管理者を兼務することも認められる。個人データ管理責任者は、株式会社組織であれば取締役または執行役等の業務執行に責任を有する者でなければならない（金融分野指針２－１）。

② 会員は、①Ａ．の個人データ管理責任者に、次の業務を所管させなければならない（金融分野指針２－１－１）。

Ａ．個人データの安全管理に関する規程および委託先の選定基準の承認お

よび周知

Ｂ．個人データ管理者および５．（２）①に定める「本人確認に関する情報」の管理者の任命

Ｃ．個人データ管理者からの報告徴収および助言・指導

Ｄ．個人データの安全管理に関する教育・研修の企画

Ｅ．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

③　会員は、①Ｂ．の個人データ管理者に、次の業務を所管させなければならない（金融分野指針２－１－２）。

Ａ．個人データの取扱者の指定および変更等の管理

Ｂ．個人データの利用申請の承認および記録等の管理

Ｃ．個人データを取り扱う保管媒体の設置場所の指定および変更等

Ｄ．個人データの管理区分および権限についての設定および変更の管理

Ｅ．個人データの取扱状況の把握

Ｆ．委託先における個人データの取扱状況等の監督

Ｇ．個人データの安全管理に関する教育・研修の実施

Ｈ．個人データ管理責任者に対する報告

Ｉ．その他所管部署における個人データの安全管理に関すること

（３）横断的な組織体制

会員は、個人データ管理責任者を補佐し、個人データの安全管理の徹底を図るために、関係各部署店の聴取・連絡・調整・指示・点検・改善等を横断的に行うための組織体制を整備することができる。

その方法としては、横断的な委員会等を設置する方法と一元的に取り扱う部署を明確化する方法のいずれでも差し支えない。「関係各部署店の聴取・連絡・調整・指示・点検・改善等を横断的に行うための組織」は、次の業務を行うことができる。

例示項目

Ａ．個人データの利用、保管・保存、移送・送信、消去・廃棄の流れに沿った取扱いの実態の確認および必要な見直しの指示

Ｂ．個人データの取扱いに関係する全ての部署店の役割と責任の明確化

Ｃ．規程等の整備を含む対策の策定または策定状況の確認、その評価・見直しまたはその指示

Ｄ．個人データ管理責任者への報告連絡体制の整備

（４）就業規則等における安全管理措置の整備

会員は、（１）Ｂ．の「就業規則等における安全管理措置の整備」とし

て、次の事項を就業規則等に定めるとともに、従業者との個人データの非開示契約等の締結を行わなければならない（金融分野指針２－２）。

Ａ．個人データの取扱いに関する従業者の役割・責任

Ｂ．違反時の懲戒処分

（５）個人データの安全管理に係る取扱規程に従った運用

会員は、（１）Ｃ．の「個人データの安全管理に係る取扱規程に従った運用」として、個人データの安全管理に係る取扱規程に従った体制を整備し、当該取扱規程に従った運用を行うとともに、取扱規程に規定する事項の遵守状況の記録および確認を行わなければならない（金融分野指針２－３）。

（６）個人データの取扱状況を確認できる手段の整備

会員は、（１）Ｄ．の「個人データの取扱状況を確認できる手段の整備」として、次の事項を含む台帳等を整備しなければならない（金融分野指針２－４）。

Ａ．取得項目

Ｂ．利用目的

Ｃ．保管場所・保管方法・保管期限

Ｄ．管理部署

Ｅ．アクセス制御の状況

（７）個人データの取扱状況の点検および監査体制の整備と実施

① 会員は、（１）Ｅ．の「個人データの取扱状況の点検および監査体制の整備と実施」として、個人データを取り扱う部署が自ら行う点検体制を整備し、点検を実施するとともに、当該部署以外の者による監査体制を整備し、監査を実施しなければならない。

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、点検により監査を代替することも認められる（金融分野指針２－５）。

② 会員は、個人データを取り扱う部署において、点検責任者および点検担当者を選任するとともに、点検計画を策定することにより点検体制を整備し、定期的および臨時の点検を実施しなければならない。また、点検の実施後において、規程違反事項等を把握したときは、その改善を行わなければならない（金融分野指針２－５－１）。

③ 会員は、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

保するとともに、監査計画を策定することにより監査体制を整備し、定期的および臨時の監査を実施しなければならない。また、監査の実施後において、規程違反事項等を把握したときは、その改善を行わなければならない。

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（金融分野指針２－５－２）。

④ 会員は、新たなリスクに対応するための、安全管理措置の評価、見直しおよび改善に向けて、個人情報保護対策および最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者による、社内の対応の確認（必要に応じ、外部の知見を有する者を活用し確認させることを含む。）等を実施することが望ましい（金融分野指針２－５－２）。

（８）漏えい等事案に対応する体制の整備

① 会員は、（１）Ｆ．の「漏えい等事案に対応する体制の整備」として、次の体制を整備しなければならない（金融分野指針２－６）。

Ａ．対応部署
Ｂ．漏えい等事案の影響・原因等に関する調査体制
Ｃ．再発防止策・事後対策の検討体制
Ｄ．自社内外への報告体制

② ①Ｂ．において調査すべき事項としては次のような例がある。

Ａ．漏えい等があった個人データの関係部署店・関係者の特定
Ｂ．漏えい等が発生した日時やルート等の特定
Ｃ．漏えい等があった個人データの情報主体・項目・件数等の特定
Ｄ．個人データの漏えいの有無の確認（漏えいしていた場合は、漏えい先の特定）
Ｅ．漏えい等が発生した原因
Ｆ．他社で発生した漏えい等の原因・対応

③ ①Ｄ．の報告体制の整備としては、次のような例がある。

Ａ．個人データの取扱いに関する規程に違反している事実または兆候があることに気づいた場合、および個人データの漏えい等が発生した場合またはその可能性が高いと判断した場合における個人データ管理責任者等への連絡体制に関する事項

Ｂ．漏えい等の兆候が苦情処理窓口等を通じて外部からもたらされる可能性があること
Ｃ．監督当局等および協議会への報告体制に関する事項
Ｄ．漏えい等による影響を受ける可能性のある本人に対する情報提供体制に関する事項
Ｅ．二次被害の防止、類似事案の発生回避の観点から、可能な限り事実関係の公表を行う必要があること
Ｆ．個人データを含んだ記録媒体等を盗取される等の犯罪が発生した場合、警察への通報を行う必要があること

④　会員は、１．（２）Ｃ．または７．（６）②にもとづき、自社内外への報告体制を整備するとともに、漏えい等事案が発生した場合には、次の事項を実施しなければならない（金融分野指針７－６－１）。
Ａ．監督当局等への報告
Ｂ．本人への通知等
Ｃ．二次被害の防止・類似事案の発生回避等の観点からの漏えい等事案の事実関係および再発防止策等の早急な公表

３．人的安全管理措置

（１）人的安全管理措置
①　会員は、個人データの安全管理の徹底が図られるよう当該従業者に対して必要かつ適切な監督を行わなければならない。そのためには、規程等の遵守状況を監査することに加え、採用時等に非開示契約等を締結すること、従業者に対して適切な教育・研修を実施しなければならない。

②　会員は、個人データの安全管理措置に係る実施体制の整備における「人的安全管理措置」として、次の措置を講じなければならない（金融分野指針　２））。
Ａ．従業者との個人データの非開示契約等の締結
Ｂ．従業者の役割・責任等の明確化
Ｃ．従業者への安全管理措置の周知徹底、教育および訓練
Ｄ．従業者による個人データ管理手続の遵守状況の確認

（２）従業者との個人データの非開示契約等の締結
①　会員は、（１）②Ａ．の「従業者との個人データの非開示契約等の締結」として、採用時等に従業者と個人データの非開示契約等を締結するととも

に、非開示契約等に違反した場合の懲戒処分を定めた就業規則等を整備しなければならない（金融分野指針３－１）。

② ①の非開示契約等の締結に当たっては、次の事項に留意する。

必須項目

Ａ．会員は、従業者を個人データの取扱いに係る業務に従事させる場合には、当該従業者の採用時等に、当該従業者と、業務上知り得た秘密に関する守秘義務を含む非開示契約等を締結すること

Ｂ．非開示契約等の締結に当たっては、非開示契約等の内容の十分な説明を行うこと。また、非開示契約等の書面を管理・保管する部署を明確にしておくこと

Ｃ．派遣社員を個人データの取扱いに係る業務に従事させる場合には、派遣社員本人と契約、覚書、念書等（電磁的手段を含む。）により守秘義務を規定すること

Ｄ．非開示契約等には、従業者でなくなった後においても非開示義務を遵守する旨を規定すること。また、非開示義務に反した場合の責任についても規定すること

③ ①の就業規則等の整備に当たっては、会員は、業務上知り得た秘密に関する守秘義務およびこれに違反した場合に適用され得る処分を就業規則、社内規則等に定めなければならない。

また、守秘義務は、従業者でなくなった後においても同様とする。

（３）従業者の役割・責任等の明確化

会員は、（１）②Ｂ．の「従業者の役割・責任等の明確化」として、次の措置を講じなければならない（金融分野指針３－２）。

Ａ．各管理段階における個人データの取扱いに関する従業者の役割・責任の明確化

Ｂ．個人データの管理区分およびアクセス権限の設定

Ｃ．違反時の懲戒処分を定めた就業規則等の整備

Ｄ．必要に応じた規程等の見直し

（４）従業者への安全管理措置の周知徹底、教育および訓練

① 会員は、（１）②Ｃ．の「従業者への安全管理措置の周知徹底、教育および訓練」として、次の措置を講じなければならない（金融分野指針３－３）。

Ａ．従業者に対する採用時の教育および定期的な教育・訓練

Ｂ．個人データ管理責任者および個人データ管理者に対する教育・訓練

C．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
D．従業者に対する教育・訓練の評価および定期的な見直し

② ①D．の措置を講じるに当たっては、次の事項に留意する。
必須項目
A．会員は、個人データの安全管理の徹底を図るための教育・研修担当部門を明確化すること
B．会員は、個人データの安全管理に関する従業者の認識を確実なものとするために、当該従業者を対象とした教育・研修を計画的に実施できる体制を整備すること
C．会員は、従業者に対する教育・研修を計画的に実施し、実施状況を確認すること。また、新入社員や中途採用者であっても確実に教育・研修が受けられる体制にしておくこと
D．教育・研修は、個人データの安全管理の徹底が図られるように、これに関係する法令、保護指針および内部規程等を従業者に対して周知徹底できるような内容とすること

（５）従業者による個人データ管理手続の遵守状況の確認

会員は、（１）②D．の「従業者による個人データ管理手続の遵守状況の確認」として、１．（２）の個人データの安全管理に係る取扱規程に定めた事項の遵守状況について、２．（５）にもとづく記録および確認を行うとともに、２．（７）①にもとづき点検および監査を実施しなければならない（金融分野指針３－４）。

４．物理的安全管理措置

（１）物理的安全管理措置

会員は、個人データの安全管理措置に係る実施体制の整備における「物理的安全管理措置」として、次に掲げる措置を講じなければならない（金融分野指針　３））

A　個人データの取扱区域等の管理
B　機器及び電子媒体等の盗難等の防止
C　電子媒体等を持ち運ぶ場合の漏えい等の防止
D　個人データの削除及び機器、電子媒体等の廃棄

（２）個人データの取扱区域等の管理

会員は、（１）Ａ.の「個人データの取扱区域等の管理」として、次に掲げる措置を講じなければならない(金融分野指針４－１)。

Ａ 個人データ等を取り扱う重要な情報システムの管理区域への入退室管理等

Ｂ 管理区域への持ち込み可能機器等の制限等

Ｃ のぞき込み防止措置の実施等による権限を有しない者による閲覧等の防止

（３） 機器及び電子媒体等の盗難等の防止

会員は、（１）Ｂ．の「機器及び電子媒体等の盗難等の防止」として、次に掲げる措置を講じなければならない（金融分野指針４－２)。

Ａ 個人データを取り扱う機器等の施錠等による保管

Ｂ 個人データを取り扱う情報システムを運用する機器の固定等

（４） 電子媒体等を持ち運ぶ場合の漏えい等の防止

会員は、「電子媒体等を持ち運ぶ場合の漏えい等の防止」として、次に掲げる措置を講じなければならない（金融分野指針４－３）

Ａ 持ち運ぶ個人データの暗号化、パスワードによる保護等

Ｂ 書類等の封緘、目隠しシールの貼付等

（５） 個人データの削除及び機器、電子媒体等の廃棄

会員は、「個人データの削除及び機器、電子媒体等の廃棄」として、次に掲げる措置を講じなければならない（金融分野指針４－４)。

Ａ 容易に復元できない手段によるデータ削除

Ｂ 個人データが記載された書類等又は記録された機器等の物理的な破壊等

５．技術的安全管理措置

（１）技術的安全管理措置

① 会員は、個人データの安全管理措置に係る実施体制の整備における「技術的安全管理措置」として、次の措置を講じなければならない（金融分野指針 ４))。

Ａ．個人データの利用者の識別および認証
Ｂ．個人データの管理区分の設定およびアクセス制御
Ｃ．個人データへのアクセス権限の管理
Ｄ．個人データの漏えい等防止策
Ｅ．個人データへのアクセスの記録および分析
Ｆ．個人データを取り扱う情報システムの稼動状況の記録および分析
Ｇ．個人データを取り扱う情報システムの監視および監査

② 会員は、本指針を参照してリスクの所在を把握し、本指針により技術的安全管理措置を講じなければならない。ただし、紙媒体等物理的に技術的安全管理措置を講じることができない一部の例外は除く。

なお、本指針のほかに別途、「金融機関等コンピュータシステムの安全対策基準・解説書」（公益財団法人金融情報システムセンター（ＦＩＳＣ））等も参照して適切な安全管理措置を講じなければならない。

（２）個人データの利用者の識別および認証

① 会員は、（１）①Ａ．の「個人データの利用者の識別および認証」として、次の措置を講じなければならない（金融分野指針５－１）。
Ａ．本人確認機能の整備
Ｂ．本人確認に関する情報の不正使用防止機能の整備
Ｃ．本人確認に関する情報が他人に知られないための対策

② ①Ａ．の措置として、個人データの利用者が正当な権限を保有した本人かどうかの正当性を確認（以下「本人確認」という。）する機能を整備しなければならない。具体的な措置を講じるに当たっては、次の事項に留意する。

例示項目

Ａ．ＩＤとパスワードを利用する。
Ｂ．記録媒体上の個人データへのアクセス権限を有する各従業者が使用できる端末またはアドレス等の識別と認証（例：ＭＡＣアドレス認証など）を実施する。

③ ①Ｂ．の措置を講じるに当たっては、次の事項に留意する。

例示項目

Ａ．第三者による悪用を抑止するため、当該ＩＤによる前回アクセスの日時、状況等のログオン履歴情報が当該ＩＤのユーザーに提供される仕組みとする。
Ｂ．パスワードの有効期限を設定する。

Ｃ．一定回数以上ログインに失敗したＩＤを停止する。
Ｄ．自動ログオン処理（パスワードの自動入力）の使用を禁止する。

④　①Ｃ．の措置を講じるに当たっては、次の事項に留意する。
例示項目
Ａ．ＡＴＭ等顧客が端末画面を見ることを前提とする端末等について、他の顧客の覗き込み防止策等の対策を講じる。
Ｂ．本人確認機能にパスワードを使用する場合は、例えば次の対策を講じる。
ａ．パスワードが記載されたメモ等を第三者の目に触れる場所に貼付することを禁止する。
ｂ．入力したパスワードは画面上非表示、帳票上非印字とする。
ｃ．パスワードを書類で申請した場合はパスワード設定後、書類の当該パスワードを黒く塗りつぶす等、判読できない措置を講じる。
Ｃ．本人確認機能にパスワードを使用する場合は、推測されやすいパスワードを設定しない。推測されやすいパスワードとは、次のものが考えられる。
ａ．桁数の短いもの
ｂ．単純な文字列や英字のみのものまたは数字のみのもの
ｃ．よく使用される英単語
ｄ．ＩＤと同じもの
ｅ．氏名、生年月日、電話番号等の個人情報
Ｄ．パスワード文字数の最低限度を設定する。
Ｅ．同一または類似パスワードの再利用を制限する。

（３）個人データの管理区分の設定およびアクセス制御
①　会員は、（１）①Ｂ．の「個人データの管理区分の設定およびアクセス制御」として、次の措置を講じなければならない（金融分野指針５－２）。
Ａ．従業者の役割・責任に応じた管理区分およびアクセス権限の設定
Ｂ．事業者内部における権限外者に対するアクセス制御
Ｃ．外部からの不正アクセスの防止措置

②　①Ａ．の措置として、アクセス権限所有者を特定し、漏えい等の発生に備えアクセスした者の範囲が把握できるような対応をとらなければならない。

③　会員は、①C．の「外部からの不正アクセスの防止措置」として、次の措置を講じなければならない（金融分野指針５－２－１）。

A．アクセス可能な通信経路の限定

B．外部ネットワークからの不正侵入防止機能の整備

C．不正アクセスの監視機能の整備

D．ネットワークによるアクセス制御機能の整備

④　③B．の具体的な措置を講じるに当たっては、次の事項に留意する。

必須項目

A．インターネットと接続する場合はファイアウォール等を設置し、外部からの個人データへの不正アクセスから保護する措置を講じること。

（４）個人データのアクセス権限の管理

①　会員は、（１）①C．の「個人データへのアクセス権限の管理」として、次の措置を講じなければならない（金融分野指針５－３）。

A．従業者に対する個人データへのアクセス権限の適切な付与および見直し

B．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

C．従業者に付与するアクセス権限を必要最小限に限定すること

②　①A．の措置として、アクセス権限の付与方法を明確に定めなければならない。具体的な措置を講じるに当たっては、次の事項に留意する。

必須項目

A．アクセス権限の承認者および設定作業者を明確にすること。

B．アクセス権限の登録、変更、抹消の記録を管理簿等により管理すること。

C．担当者の役割に応じたアクセス権限が適切に付与されているかの定期的な見直しを行うこと。アクセス制限の見直しのタイミングとしては、次の時点が考えられる。

ａ．所属、職制、組織等の変更時

ｂ．長期出張、長期留学、休職、退職時

ｃ．新システム稼働時

ｄ．一定期間経過時

③　①A．およびC．の措置を講じるに当たっては、次の事項に留意する。

例示項目

Ａ．特権ＩＤ（管理者ＩＤ）を設定する場合は、管理者を限定し管理方法に特別の留意をする。

（５）個人データの漏えい等防止策

①　会員は、（１）①Ｄ．の「個人データの漏えい等防止策」として、個人データの保護策を講じることとともに、障害発生時の技術的対応・復旧手続を整備しなければならない（金融分野指針５－４）。

②　会員は、①の「個人データの保護策を講じること」として、次の措置を講じなければならない（金融分野指針５－４－１）。

Ａ．蓄積データの漏えい等防止策

Ｂ．伝送データの漏えい等防止策

Ｃ．コンピュータウイルス等不正プログラムへの防御対策

③　②Ａ．の措置として、ファイルの不正コピーや盗難等による漏えいを防止するため、ファイルの不正コピーや盗難の際にも個人データの内容が分からないようにするための措置を講じなければならない。具体的には次の事項に留意する。

例示項目

Ａ．保管・バックアップ時において不正コピー・盗難があった際の対策を講じる（例：記録媒体上の個人データが記録されたファイルへのパスワード設定や暗号化）。

Ｂ．移送時において不正コピー・盗難があった際の対策を講じる（例：記録媒体上の個人データが記録されたファイルへのパスワード設定や暗号化）。

④　②Ｂ．の措置として、個人データの伝送時に盗聴等による漏えいを防止するため、データ伝送時に盗聴された場合にもデータの内容が分からないようにするための措置を講じなければならない。具体的には次の事項に留意する。

例示項目

Ａ．個人データを通信（例：本人および従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送など）する場合には、個人データが記録されたファイルへのパスワードの設定または暗号化を実施する。

⑤　②Ｃ．の措置として、コンピュータウイルスの侵入や不正アクセスによるプログラムの改ざんがなされないための対策を講じなければならない。具体的には次の事項に留意する。

必須項目

Ａ．ウイルス対策ソフトウェアを導入すること。

例示項目

Ａ．オペレーションシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）を適用する。

Ｂ．不正ソフトウェア対策の有効性・安定性を確認する（例：パターンファイル、修正ソフトウェアの更新の確認など）。

Ｃ．無認可のソフトウェアの使用を禁止する。

⑥　会員は、①の「障害発生時の技術的対応・復旧手続の整備」として、次の措置を講じなければならない（金融分野指針５－４－２）。

Ａ．不正アクセスの発生に備えた対応・復旧手続の整備

Ｂ．コンピュータウイルス等不正プログラムによる被害時の対策

Ｃ．リカバリ機能の整備

（６）個人データへのアクセスの記録および分析

①　会員は、（１）①Ｅ．の「個人データへのアクセスの記録および分析」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（金融分野指針５－５）。

②　①のアクセスや操作の記録およびその分析・保存に当たっては、漏えい等（特に内部の悪意者による漏えい等）を防止する観点から必要な措置を講じなければならない。具体的には次の事項に留意する。

必須項目

Ａ．個人データを取り扱う情報システムにおいては、個人データへのアクセスや操作および個人データを取り扱う情報システムの稼動状況について記録・分析すること（例：ログインとログオフの状況、不正なアクセス要求、情報システムによって失効とされたＩＤ、システムログなど）。

Ｂ．個人データへのアクセスや操作および個人データを取り扱う情報システムの稼動状況の記録について、改ざん、漏えい等防止の観点から適切に安全管理措置を講じること。

Ｃ．個人データを取り扱う情報システムにおいては、取得した記録を分析

すること（特に、休日や深夜時間帯等、漏えいリスクの高い時間帯におけるアクセス頻度の高いケースを重点的に分析すること）。

（７）個人データを取り扱う情報システムの稼動状況の記録および分析

会員は、（１）①Ｆ.「個人データを取り扱う情報システムの稼動状況の記録および分析」として、個人データを取り扱う情報システムの稼動状況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（金融分野指針５－６）。

（８）個人データを取り扱う情報システムの監視および監査

会員は、（１）①Ｇ.「個人データを取り扱う情報システムの監視および監査」として、個人データを取り扱う情報システムの利用状況および個人データへのアクセス状況および情報システムへの外部からのアクセス状況を（６）および（７）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および監査を行わなければならない。また、セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策を行わなければならない（金融分野指針５－７）。

６．委託先の監督

会員は、個人データの取扱いを委託する場合は、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、個人データの取扱いを委託するとともに、委託先における当該個人データに対する安全管理措置の実施を確保しなければならない（金融分野指針Ⅲ.）。

（１）個人データ保護に関する委託先選定の基準

① 会員は、個人データの取扱いを委託する場合には、次の事項を委託先選定の基準として定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直さなければならない（金融分野指針６－１）。

Ａ．委託先における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

Ｂ．委託先における個人データの安全管理に係る実施体制の整備

Ｃ．実績等にもとづく委託先の個人データ安全管理上の信用度

Ｄ．委託先の経営の健全性

② 委託先選定の基準においては、①Ａ．の「委託先における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、次の事項を定めなければならない（金融分野指針６－１－１）。

Ａ．委託先における個人データの安全管理に係る基本方針の整備

Ｂ．委託先における個人データの安全管理に係る取扱規程の整備

Ｃ．委託先における個人データの取扱状況の点検および監査に係る規程の整備

Ｄ．委託先における外部委託に係る規程の整備

③ 委託先選定の基準においては、①Ｂ．の「委託先における個人データの安全管理に係る実施体制の整備」として、「２．組織的安全管理措置」、「３．人的安全管理措置」「４．物理的安全管理措置」、「５．技術的安全管理措置」および「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条第６項の外的環境の把握に記載された事項を定めるとともに、委託先から再委託する場合の再委託先の個人データの安全管理に係る実施体制の整備状況に係る基準を定めなければならない（金融分野指針６－１－２）。

④ ①Ｃに関連して委託先を選定する基準として次の事項が考えられる。

例示項目

Ａ．技術・運用等のレベル（業務内容の理解度、業界に関する知識、情報収集能力、管理能力等）

Ｂ．漏えい等の問題発生時の対応力

Ｃ．各種公的認証の取得状況

⑤ 会員は、（２）①にもとづき、委託契約後に委託先選定の基準に定める事項の委託先における遵守状況を定期的または随時に確認するとともに、委託先が当該基準を満たしていない場合には、委託先が当該基準を満たすよう監督しなければならない（金融分野指針６－２）。

（２）委託契約において盛り込むべき安全管理に関する内容

① 会員は、委託契約において、次の安全管理に関する事項を盛り込まなければならない（金融分野指針６－３）。

Ａ．委託者の監督・監査・報告徴収に関する権限

Ｂ．委託先における個人データの漏えい、盗用、改ざんおよび目的外利用の禁止

Ｃ．再委託における条件

Ｄ．漏えい等事案が発生した際の委託先の責任

② ①B．に関連して委託契約に盛り込む事項として次の事項が考えられる。

必須項目

A．委託業務に際して知り得た秘密に関する守秘義務（委託業務終了後においても同様とすること）。

B．委託先が漏えい等の防止その他の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るべきこと。

C．委託先が個人データの安全管理の徹底が図られるよう、従業者に対する必要かつ適切な監督を行うべきこと。

③ 会員は、①C．として、再委託の可否および再委託を行うに当たっての委託元への文書による事前報告または承認手続等を、委託契約に盛り込むことが望ましい（金融分野指針６－３）。

④ ①D．に関連して委託契約に盛り込む事項として次の事項が考えられる。

必須項目

A．契約違反・損害発生の場合における損害賠償および契約の解除等に関する事項

⑤ 会員は、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（金融分野指針６－３）。

（３）委託先における安全管理措置の遵守状況の確認、監督

① 会員は、（２）①にもとづき、定期的に監査を行う等により、定期的または随時に委託先における委託契約上の安全管理措置等の遵守状況を確認するとともに、当該契約内容が遵守されていない場合には、委託先が当該契約内容を遵守するよう監督しなければならない。また、会員は、定期的に委託契約に盛り込む安全管理措置を見直さなければならない（金融分野指針６－４）。

② ①の確認、監督に当たっては、次の事項に留意する。

必須項目

A．委託先の従業者が、委託業務を行う場合には、委託先においてセキュリティポリシーをはじめとした従業者が遵守すべきルールが明確にされ遵守されていることを確認すること。

B．委託契約期間中においても、次の事項に留意して継続的に委託先を評価すること。委託先の評価に当たっては、例えば、次の項目が考えられる。

ａ．委託業務に関する管理者を明確にする。

ｂ．委託業務の処理状況、機密管理状況等について定期的に報告を受ける。

ｃ．委託業務の処理体制・処理方法等に関する重要な変更がある場合には速やかに報告を受ける体制を整備する。

ｄ．委託業務の内容に応じ、定期的または必要に応じて委託先に対する監査を行う。

Ｃ．委託先において個人データの漏えい等事案が発生した場合または発生の可能性が高いと判断された場合に、速やかに委託元である会員に報告され、適切に対応できるよう、予め委託先との間で連絡体制等を整備すること。

③　再委託先に対する直接の監督は委託先が行うこととなるが、委託元である会員においても、例えば、再委託の実態や委託先による再委託先に対する監督の方法等を委託先から報告させ、委託先に対して必要に応じて指導等を行わなければならない。

７．各管理段階における安全管理に係る取扱規程

会員は、１．（２）にもとづき、各管理段階の安全管理に係る取扱規程において、次の事項を定めなければならない（金融分野指針別添１）。

（１）取得・入力段階における取扱規程

①　会員は、取得・入力段階における取扱規程において、次の事項を定めなければならない（金融分野指針７－１）。

Ａ．取得・入力に関する取扱者の役割・責任
Ｂ．取得・入力に関する取扱者の限定
Ｃ．取得・入力の対象となる個人データの限定
Ｄ．取得・入力時の照合および確認手続
Ｅ．取得・入力の規程外作業に関する申請および承認手続
Ｆ．機器・記録媒体等の管理手続
Ｇ．個人データへのアクセス制御
Ｈ．取得・入力状況の記録および分析

②　会員は、①Ｇ．として、次の事項を定めることが望ましい（金融分野指針７－１）。

Ａ．入館（室）者による不正行為の防止のための、業務実施場所および情

報システム等の設置場所の入退館（室）管理の実施（例：入退館（室）の記録の保存）

Ｂ．盗難等の防止のための措置（例：カメラによる撮影や作業への立会い等による記録またはモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止または検査の実施）

Ｃ．不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性にもとづく限定（例：スマートフォン、パソコン等の記録機能を有する機器の接続の制限および機器の更新への対応）

（２）利用・加工段階における取扱規程

①　会員は、利用・加工段階における取扱規程において、組織的安全管理措置および技術的安全管理措置を定めなければならない（金融分野指針７－２）。

②　利用・加工段階における取扱規程に関する組織的安全管理措置は、次の事項を含まなければならない（金融分野指針７－２－１）。

Ａ．利用・加工に関する取扱者の役割・責任
Ｂ．利用・加工に関する取扱者の限定
Ｃ．利用・加工の対象となる個人データの限定
Ｄ．利用・加工時の照合および確認手続
Ｅ．利用・加工の規程外作業に関する申請および承認手続
Ｆ．機器・記録媒体等の管理手続
Ｇ．個人データへのアクセス制御
Ｈ．個人データの管理区域外への持出しに関する上乗せ措置
Ｉ．利用・加工状況の記録および分析

③　②Ｆ．を定めるに当たっては、漏えい等のリスクを洗い出し、その防止のために必要かつ適切な措置を盛り込まなければならない。特に、自社における事例だけでなく、他社で発生した漏えい等事案も参考に必要な内容を盛り込まなければならない。具体的には次の事項に留意する。

必須項目

Ａ．個人データを取り扱う機器類（社内ＬＡＮ管理に係る通信機器等を含む。）に関する管理責任者を明確にすること。

Ｂ．機器類等の盗難防止策（例：離席時の個人データを記載した紙媒体や個人データを保存した携帯可能なコンピュータ等の机上等への放置の禁止、離席時のパスワード付きスクリーンセーバー等の起動、個人データを記録した記録媒体等の施錠保管、個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止など）を策定すること。

Ｃ．個人データを保存した持出しが容易な機器類（ノート型コンピュータ等）は、個人データのセキュリティが危険にさらされないような防御を確実にするために、特別な注意を払い、個別の盗難防止策等を採用すること。持出しが容易な機器類の盗難防止策としては次のような例がある。

ａ．ワイヤー等による設置機器類の固定

ｂ．鍵付ラックへの収納

Ｄ．紙媒体の業務中離席時の机上への放置を禁止すること（施錠箇所への保管等）。

例示項目

Ａ．個人データを取り扱う機器類を適切に管理するため、台帳等を作成する。

なお、営業店・本部取扱部署等に設置されている機器類を主管部署が一括管理する場合には、主管部署で作成した台帳を配付し、当該部署店においても識別管理できるようにしておく。

また、主管部署においては、システム構成図等を整備し、システム構成変更などに的確に対応できるようにしておく。

Ｂ．許可されていない機器類の移動が行われていないか、現場検査を定期的に実施し、その現場検査があることを従業者に認識させる。

Ｃ．記録媒体等は、利用目的に照らして必要な範囲内において作成（複写を含む。）するとともに、必要性がなくなった場合には確実に消去・廃棄することにより、可能な限りその量を減らす。

Ｄ．紙媒体の出力については、次の点に留意して不正防止および機密保護対策を講じる。

a. プリンタは、印刷後速やかに取り出せる位置に設置する。

b. 端末画面への長時間の継続表示は行わない。

c. 権限のない者による印刷、画面の覗き込み、コピー取得を禁止する。

d. 印刷を行う作業者を限定する。

e. 紙媒体のコピー取得はその利用目的に照らして必要な範囲内に限定するとともに、コピーを取得した場合は記録を残す。

Ｅ．記録媒体のバックアップまたはコピーを作成する場合は、依頼・承認、授受、廃棄等の手続とその管理方法を明確にしておく。

④　会員は、②Ｇ．として、次の事項を定めることが望ましい（金融分野指針７－２－１）。

Ａ．入館（室）者による不正行為の防止のための、業務実施場所および情報システム等の設置場所の入退館（室）管理の実施（例：入退館（室）の記録の保存）

Ｂ．盗難等の防止のための措置（例：カメラによる撮影や作業への立会い

等による記録またはモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止または検査の実施）

C．不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性にもとづく限定（例：スマートフォン、パソコン等の記録機能を有する機器の接続の制限および機器の更新への対応）

⑤　②G．を定めるに当たっては、次の事項に留意する。

必須項目

A．機器類の設置場所および管理に当たっては、従業者による不正使用の抑制とアクセスを許可されていない者からのアクセス防止を勘案すること。

B．重要な機器類は、入退館（室）の許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。接近防止策としては次のような例がある。

ａ．入室資格付与

ｂ．施錠による管理

⑥　②H．の「個人データの管理区域外への持出しに関する上乗せ措置」は、次の事項を含まなければならない（金融分野指針７－２－１－１）。

A．個人データの管理区域外への持出しに関する取扱者の役割・責任

B．個人データの管理区域外への持出しに関する取扱者の必要最小限の限定

C．個人データの管理区域外への持出しの対象となる個人データの必要最小限の限定

D．個人データの管理区域外への持出し時の照合および確認手続

E．個人データの管理区域外への持出しに関する申請および承認手続

F．機器・記録媒体等の管理手続

G．個人データの管理区域外への持出し状況の記録および分析

⑦　利用・加工段階における取扱規程に関する技術的安全管理措置は、次の事項を含まなければならない（金融分野指針７－２－２）。

A．個人データの利用者の識別および認証

B．個人データの管理区分の設定およびアクセス制御

C．個人データへのアクセス権限の管理

D．個人データの漏えい等防止策

E．個人データへのアクセス記録および分析

F．個人データを取り扱う情報システムの稼動状況の記録および分析

（３）保管・保存段階における取扱規程

① 会員は、保管・保存段階における取扱規程において、組織的安全管理措置および技術的安全管理措置を定めなければならない（金融分野指針７－３）。

② 保管・保存段階における取扱規程に関する組織的安全管理措置は、次の事項を含まなければならない（金融分野指針７－３－１）。

Ａ．保管・保存に関する取扱者の役割・責任
Ｂ．保管・保存に関する取扱者の限定
Ｃ．保管・保存の対象となる個人データの限定
Ｄ．保管・保存の規程外作業に関する申請および承認の手続
Ｅ．機器・記録媒体等の管理手続
Ｆ．個人データへのアクセス制御
Ｇ．保管・保存状況の記録および分析
Ｈ．保管・保存に関する障害発生時の対応・復旧手続

③ ②Ｅ．の事項を定めるに当たっては、次の事項に留意する。

必須項目

Ａ．紙媒体は業務終了後、施錠可能な場所へ保管すること。
Ｂ．ＵＳＢメモリ等の記録媒体の管理簿等により、定期的または随時に在庫管理を行い、保管・保存状況の点検を行うこと。

例示項目

Ａ．記録媒体の不正使用等を防止するため、ラベルへの内容表示は記号等により最小限の項目に留める。

④ 会員は、②Ｆ．として、次の事項を定めることが望ましい（金融分野指針７－３－１）。

Ａ．入館（室）者による不正行為の防止のための、業務実施場所および情報システム等の設置場所の入退館（室）管理の実施（例：入退館（室）の記録の保存）
Ｂ．盗難等の防止のための措置（例：カメラによる撮影や作業への立会い等による記録またはモニタリングの実施、記録機能を持つ媒体の持込み・持出し禁止または検査の実施）
Ｃ．不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性にもとづく限定（例：スマートフォン、パソコン等の記録機能を有する機器の接続の制限および機器の更新への対応）

⑤ ②Ｆ．の措置を講じるに当たっては、会員は、次の事項に留意のうえ、

個人データを取り扱う建物または室への入館（室）者を特定するため、重要度や建物の構造等に応じ、資格付与と鍵の管理を行わなければならない。

必須項目

Ａ．建物または室の入退館（室）者に対する資格審査のうえ、資格識別証等を発行し（例：写真入り入館許可証の発行、所属、立入場所等を判別できる識別章の発行、予め設定された入退資格を識別し、扉の開閉（施錠、解錠）を行う出入管理設備と資格の登録された磁気カード（ＩＣカード等を含む。以下同じ。）の発行および識別コードの付与など）、目に見える場所に入館許可証等の着用を義務付けるなど、入退館（室）を管理すること。また、資格喪失時には、資格識別証等を回収すること。

Ｂ．鍵管理に関する管理責任者を明確にすること。

Ｃ．建物（室）の施錠・解錠、鍵の保管および受渡し等の記録をとること。

⑥　②Ｆ．の措置を講じるに当たっては、会員は、次の事項に留意のうえ、不法侵入、危険物持込み、不法持出し等を防止するため、重要度や建物の構造等に応じ、厳格な入退館（室）管理を実施しなければならない。

なお、共同ビルを利用していることにより、入退館管理を行うことができない場合は、入退室において、入退館管理と同等の管理をしなければならない。

必須項目

Ａ．建物または室の入退館（室）に関する管理責任者を明確にすること。

Ｂ．不法侵入を防止するため、個人データを取り扱う機器類を設置した建物または室の出入口には警備員の配置や有人の受付その他の出入管理設備、防犯設備を設置すること。

Ｃ．営業時間外に利用する通用口にはインターホン、防犯ビデオ等の入館（室）者の識別設備を設置すること。

Ｄ．入退資格が付与されている者であっても、夜間、休日の入退館については、入退館者名を入館受付に事前通知するなど、手続を明確にしておくこと。

Ｅ．訪問者に対しては、身元および用件を確認のうえ、入退館を許可すること。

⑦　②Ｆ．の措置を講じるに当たっては、重要な機器類の設置場所について、特に厳格な入退室管理を実施しなければならない。

⑧　保管・保存段階における取扱規程に関する技術的安全管理措置は、次の事項を含まなければならない（金融分野指針７－３－２）。

Ａ．個人データの利用者の識別および認証

Ｂ．個人データの管理区分の設定およびアクセス制御
Ｃ．個人データへのアクセス権限の管理
Ｄ．個人データの漏えい等防止策
Ｅ．個人データへのアクセス記録および分析
Ｆ．個人データを取り扱う情報システムの稼動状況の記録および分析

（４）移送・送信段階における取扱規程

① 会員は、移送・送信段階における取扱規程において、組織的安全管理措置および技術的安全管理措置を定めなければならない（金融分野指針７－４）。

② 移送・送信段階における取扱規程に関する組織的安全管理措置は、次の事項を含まなければならない（金融分野指針７－４－１）。
Ａ．移送・送信に関する取扱者の役割・責任
Ｂ．移送・送信に関する取扱者の限定
Ｃ．移送・送信の対象となる個人データの限定
Ｄ．移送・送信時の照合および確認手続
Ｅ．移送・送信の規程外作業に関する申請および承認手続
Ｆ．個人データへのアクセス制御
Ｇ．移送・送信状況の記録および分析
Ｈ．移送・送信に関する障害発生時の対応・復旧手続

③ ②Ｄ．を定めるに当たっては、次の事項に留意する。

必須項目

Ａ．個人データをＦＡＸ等で送信する場合は、誤送信の防止および個人データの紛失等防止のための対策（例：宛先番号確認、受領確認等）を講じること。

例示項目

Ａ．記録媒体等の授受は、送付状、授受伝票、授受管理簿、発送管理表、媒体数・印刷枚数一覧表等により確認する。
Ｂ．記録媒体の授受は、不正使用、改ざん、紛失等を防止するため、次のような項目を明確にして行う。
ａ．使用目的
ｂ．使用日時
ｃ．使用者名
ｄ．責任者の承認
ｅ．入出庫日時
ｆ．入出庫担当者名

④　移送・送信段階における取扱規程に関する技術的安全管理措置は、次の事項を含まなければならない（金融分野指針７－４－２）。

Ａ．個人データの利用者の識別および認証
Ｂ．個人データの管理区分の設定およびアクセス制御
Ｃ．個人データへのアクセス権限の管理
Ｄ．個人データの漏えい等防止策
Ｅ．個人データへのアクセス記録および分析

（５）消去・廃棄段階における取扱規程

①　会員は、消去・廃棄段階における取扱規程において、次の事項を定めなければならない（金融分野指針７－５）。

Ａ．消去・廃棄に関する取扱者の役割・責任
Ｂ．消去・廃棄に関する取扱者の限定
Ｃ．消去・廃棄時の照合および確認手続
Ｄ．消去・廃棄の規程外作業に関する申請および承認手続
Ｅ．機器・記録媒体等の管理手続
Ｆ．個人データへのアクセス制御
Ｇ．消去・廃棄状況の記録および分析

②　①Ｅ．を定めるに当たっては、次の事項に留意のうえ、誤消去、漏えい等の適切な防止策を講じなければならない。

例示項目

Ａ．機器類を廃棄する場合およびリース契約期限切れに伴いリース会社へ機器類を返却する場合等は、機器内記録媒体上の個人データを適切な方法で消去する。
Ｂ．紙媒体の廃棄方法としては、次のような例がある。
　a．シュレッダー等による記載内容が識別不能までの裁断
　b．自社または外部の焼却場での焼却または溶解
Ｃ．記録媒体の消去・廃棄方法としては、次のような例がある。
　a．適切なデータ消去ツールを使用したデータの完全消去
　b．消磁気または裁断等による消去・破壊
Ｄ．外部委託して廃棄する場合には、守秘義務契約を締結したうえで、廃棄帳票等の授受帳簿を作成し、廃棄終了後は遅滞なく報告を受け、廃棄の事実を確認できる文書（焼却・溶解場の廃棄証明）等を受領する。
　また、廃棄時には自社の従業者が立ち会う。

（６）漏えい等事案への対応の段階における取扱規程

① 会員は、漏えい等事案への対応の段階における取扱規程において、次の事項を定めなければならない（金融分野指針７－６）。

Ａ．対応部署の役割・責任
Ｂ．漏えい等事案への対応に関する取扱者の限定
Ｃ．漏えい等事案への対応の規程外作業に関する申請および承認手続
Ｄ．漏えい等事案の影響・原因等に関する調査手続
Ｅ．再発防止策・事後対策の検討に関する手続
Ｆ．自社内外への報告に関する手続
Ｇ．漏えい等事案への対応状況の記録および分析

② ①Ｆ．の「自社内外への報告に関する手続」は、次の事項を含まなければならない（金融分野指針７－６－１）。

Ａ．個人情報保護委員会又は監督当局等への報告
Ｂ．本人への通知等
Ｃ．二次被害の防止・類似事案の発生回避等の観点からの漏えい等事案の事実関係および再発防止策等の早急な公表

なお、会員は、個人情報の保護に関する法律施行規則第７条各号に定める事態を知ったときは、個人情報の保護に関する法律第 26 条及び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）３－５－３及び３－５－４に従い、必要な措置を講ずる必要がある点に留意して上記取扱規程を定める。

Ⅲ．個人番号および特定個人情報に関する安全管理措置

１．安全管理措置の検討手順

会員は、個人番号および特定個人情報（以下併せて「特定個人情報等」という。）の取扱いに関する安全管理措置について、次のような手順で検討を行わなければならない（特定個人情報安全管理措置１）。

（１）個人番号を取り扱う事務の範囲の明確化

会員は、個人番号関係事務の範囲を明確にしておかなければならない（特定個人情報安全管理措置１Ａ）。

（２）特定個人情報等の範囲の明確化

会員は、「（１）」で明確化した事務において取り扱う特定個人情報等の範囲を明確にしておかなければならない（特定個人情報安全管理措置１Ｂ）。

（３）事務取扱担当者の明確化

会員は、「（１）」で明確化した事務に従事する事務取扱担当者を明確にしておかなければならない（特定個人情報安全管理措置１Ｃ）。

事務取扱担当者は、基本的には、個人番号の取得から廃棄までの事務に従事する全ての者が該当すると考えられる。この場合、当該事務のリスクを適切に検討し、必要かつ適切な安全管理措置を講ずることが重要となり、事務取扱担当者が担う役割に応じて講ずる安全管理措置が異なると考えられる。なお、社内管理上、定期的に発生する事務や中心となる事務を担当する者のみを事務取扱担当者と位置付けることも考えられるが、特定個人情報等の取扱いに関わる事務フロー全体として漏れのない必要かつ適切な安全管理措置を講ずることが重要である。

（４）基本方針の策定

特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である（特定個人情報安全管理措置１Ｄ）。

（５）取扱規程等の策定

会員は、上記「（１）～（３）」で明確化した事務における特定個人情報等の適正な取扱いを確保するために、取扱規程等を策定しなければならな

い（特定個人情報安全管理措置１Ｅ）。既存の個人情報の保護に係る取扱規程等がある場合には、新たに特定個人情報等の保護に係る取扱規程等を策定するのではなく、既存の個人情報の保護に係る取扱規程等に、特定個人情報等の取扱いを追記することも可能である。

２．講ずべき安全管理措置の内容

特定個人情報等の保護のために必要な安全管理措置については、次のとおりであり、当該措置の具体的な手法の例示は「例示」として記載している（特定個人情報安全管理措置２）。本例示は、これに限定する趣旨で記載したものではなく、会員の規模および特定個人情報等を取り扱う事務の特性等により、適切な手法を採用することが重要である。

（１）基本方針の策定

会員は、特定個人情報等の適正な取扱いの確保について組織として取り組むために、次の事項等を定めた基本方針を策定することが重要である（特定個人情報安全管理措置２Ａ）。

例示

・会員の名称
・関係法令・ガイドライン等の遵守
・安全管理措置に関する事項
・質問および苦情処理の窓口　等

（２）取扱規程等の策定

会員は、「１．（１）～（３）」で明確化した事務において事務の流れを整理し、特定個人情報等の具体的な取扱いを定める取扱規程等を策定しなければならない（特定個人情報安全管理措置２Ｂ）。取扱規程等は、次に掲げる管理段階毎に、取扱方法、責任者・事務取扱担当者およびその任務等について定めることが考えられる。具体的に定める事項については、「（３）～（６）」に記述する安全管理措置を織り込むことが重要である。

例示

①　取得段階
②　利用段階
③　保存段階
④　提供段階
⑤　削除・廃棄段階

※法定調書を作成する事務の場合、例えば、次のような事務フローに即して、手続を明確にしておくことが重要である。

・提出された書類等を取りまとめる方法
・取りまとめた書類等の法定調書の作成部署への移動方法
・情報システムへの個人番号を含むデータ入力方法
・法定調書の作成方法
・法定調書の行政機関等への提出方法
・法定調書の控え、提出された書類および情報システムで取り扱うファイル等の保存方法
・法定保存期間を経過した法定調書の控え等の廃棄・削除方法 等

（３）組織的安全管理措置

会員は、特定個人情報等の適正な取扱いのために、次の組織的安全管理措置を講じなければならない（特定個人情報安全管理措置２Ｃ）。

① 組織体制の整備

安全管理措置を講ずるための組織体制を整備する（特定個人情報安全管理措置２Ｃa）。整備項目としては次の事項が挙げられる。

例示

・事務における責任者の設置および責任の明確化
・事務取扱担当者の明確化およびその役割の明確化
・事務取扱担当者が取り扱う特定個人情報等の範囲の明確化
・事務取扱担当者が取扱規程等に違反している事実または兆候を把握した場合の責任者への報告連絡体制
・漏えい等事案の発生または兆候を把握した場合の従業者から責任者等への報告連絡体制
・特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担および責任の明確化

② 取扱規程等にもとづく運用

取扱規程等にもとづく運用を行うとともに、その状況を確認するため、システムログまたは利用実績を記録する（特定個人情報安全管理措置２Ｃb）。記録する項目としては次の事項が挙げられる。

例示

・特定個人情報ファイルの利用・出力状況の記録
・書類・媒体等の持ち運びの記録
・特定個人情報ファイルの削除・廃棄記録
・削除・廃棄を委託した場合、これを証明する記録等

・特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

③　取扱状況を確認する手段の整備

特定個人情報ファイルの取扱状況を確認するための手段を整備する。

なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない（特定個人情報安全管理措置２Ｃc）。取扱状況を確認するための記録等としては次の事項が挙げられる。

例示

・特定個人情報ファイルの種類・名称
・責任者、取扱部署
・利用目的
・削除・廃棄状況
・アクセス権を有する者

④　漏えい等事案に対応する体制の整備

漏えい等事案の発生または兆候を把握した場合に、適切かつ迅速に対応するための体制を整備する（特定個人情報安全管理措置２Ｃd）。当該体制整備は次の対応に係るものが考えられる。

・事業者内部における報告および被害の拡大防止
・事実関係の調査および原因の究明
・影響範囲の特定
・再発防止策の検討・実施
・影響を受ける可能性のある本人への通知等
・事実関係および再発防止策等の公表

なお、漏えい等事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、当該事案の内容等に応じて、事実関係および再発防止策等を早急に公表することが重要である。

また、特定個人情報の漏えい等事案が発生した場合、事業者には、番号法第 29 条の４、「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第 29 条の４第１項及び第２項に基づく特定個人情報の漏えい等に関する報告等に関する規則」及び「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の「（別添２）特定個人情報の漏えい等に関する報告等（事業者編）」に基づき個人情報保護委員会等への報告等が求められる。漏えい等事案が発生した場合の対応の詳細については、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」の「（別添２）特定個人情報の漏えい等に関する報告等（事業者編）」に従って対

応する必要がある。

⑤　取扱状況の把握および安全管理措置の見直し

特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直しおよび改善に取り組む（特定個人情報安全管理措置２Ｃe）。

例示

・特定個人情報等の取扱状況について、定期的に自ら行う点検または他部署等による監査を実施することが考えられる。
・外部の主体による他の監査活動と合わせて、監査を実施することも考えられる。

（４）人的安全管理措置

会員は、特定個人情報等の適正な取扱いのために、次の人的安全管理措置を講じなければならない（特定個人情報安全管理措置２Ｄ）。

①　事務取扱担当者の監督

会員は、特定個人情報等が取扱規程等にもとづき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う（特定個人情報安全管理措置２Ｄa）。

②　事務取扱担当者の教育

会員は、事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う（特定個人情報安全管理措置２Ｄb）。

例示

・特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行うことが考えられる。
・特定個人情報等についての秘密保持に関する事項を就業規則等に盛り込むことが考えられる。

（５）物理的安全管理措置

会員は、特定個人情報等の適正な取扱いのために、次の物理的安全管理措置を講じなければならない（特定個人情報安全管理措置２Ｅ）。

①　特定個人情報等を取り扱う区域の管理

特定個人情報等の漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）および特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、次のような物理的な安全管理措置を講ずる（特定個人情報安全管理措置２Ｅa）。

例示

・管理区域に関する物理的安全管理措置としては、入退室管理および管理区域へ持ち込む機器等の制限等が考えられる。
・入退室管理方法としては、ＩＣカード、ナンバーキー等による入退室管理システムの設置等が考えられる。
・取扱区域に関する物理的安全管理措置としては、壁または間仕切り等の設置および座席配置の工夫等が考えられる 。

② 機器および電子媒体等の盗難等の防止

管理区域および取扱区域における特定個人情報等を取り扱う機器、電子媒体および書類等の盗難または紛失等を防止するために、次のような物理的な安全管理措置を講ずる（特定個人情報安全管理措置２Ｅb）。

例示

・特定個人情報等を取り扱う機器、電子媒体または書類等を、施錠できるキャビネット・書庫等に保管することが考えられる。
・特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。

③ 電子媒体等の取扱いにおける漏えい等の防止

特定個人情報等が記録された電子媒体または書類等を持ち運ぶ場合、容易に個人番号が判明しないよう、安全な方策を講ずる（特定個人情報安全管理措置２Ｅc）。当該方策については、次のような措置が考えられる。

なお、「持ち運び」とは、特定個人情報等を管理区域または取扱区域から外へ移動させることまたは当該区域の外から当該区域へ移動させることをいい、事業所内での移動等であっても、特定個人情報等の紛失・盗難等に留意する必要がある。

例示

・特定個人情報等が記録された電子媒体を安全に持ち運ぶ方法としては、持ち運ぶデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段の利用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。
・特定個人情報等が記載された書類等を安全に持ち運ぶ方法としては、封緘、目隠しシールの貼付、追跡可能な移送手段の利用等が考えられる。

④ 個人番号の削除、機器および電子媒体等の廃棄

個人番号関係事務を行う必要がなくなった場合で、所管法令等において

定められている保存期間等を経過した場合には、個人番号をできるだけ速やかに復元不可能な手段で削除または廃棄する。

個人番号もしくは特定個人情報ファイルを削除した場合、または電子媒体等を廃棄した場合には、削除または廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除または廃棄したことについて、証明書等により確認する（特定個人情報安全管理措置２Ｅd)。

以上の個人番号の削除ならびに機器および電子媒体等の廃棄の手段等については、次の手段が考えられる。

例示

・特定個人情報等が記載された書類等を廃棄する場合、焼却または溶解、復元不可能な程度に細断可能なシュレッダーの利用、個人番号部分を復元不可能な程度にマスキングすること等の復元不可能な手段を採用することが考えられる。
・特定個人情報等が記録された機器および電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用または物理的な破壊等により、復元不可能な手段を採用することが考えられる。
・特定個人情報等を取り扱う情報システムまたは機器等において、特定個人情報ファイル中の個人番号または一部の特定個人情報等を削除する場合、容易に復元できない手段を採用することが考えられる。
・特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築することが考えられる。
・個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定めることが考えられる。

（６）技術的安全管理措置

会員は、特定個人情報等の適正な取扱いのために、次の技術的安全管理措置を講じなければならない（特定個人情報安全管理措置２Ｆ)。

①　アクセス制御

情報システムを使用して個人番号関係事務を行う場合、事務取扱担当者および当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う（特定個人情報安全管理措置２Ｆa)。アクセス制御を行う方法としては、次の事項が挙げられる。

例示

・個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。
・特定個人情報ファイルを取り扱う情報システムを、アクセス制御により

限定する。
・ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

② アクセス者の識別と認証

特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果にもとづき認証する（特定個人情報安全管理措置２Ｆb)。事務取扱担当者の識別方法としては、例えば、ユーザーＩＤ、パスワード、磁気・ＩＣカード等が考えられる。

③ 外部からの不正アクセス等の防止

情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護する仕組みを導入し、適切に運用する（特定個人情報安全管理措置２Ｆc)。当該保護の仕組みについては次の事項が挙げられる。

例示

・情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断することが考えられる。
・情報システムおよび機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入することが考えられる。
・導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認することが考えられる。
・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とすることが考えられる。
・ログ等の分析を定期的に行い、不正アクセス等を検知することが考えられる。

④ 漏えい等の防止

特定個人情報等をインターネット等により外部に送信する場合、通信経路における漏えい等を防止するための措置を講ずる（特定個人情報安全管理措置２Ｆd)。措置の内容としては次の事項が挙げられる。

例示

・通信経路における漏えい等の防止策としては、通信経路の暗号化等が考えられる。
・情報システム内に保存されている特定個人情報等の漏えい等の防止策としては、データの暗号化またはパスワードによる保護等が考えられる。

（７）委託の取扱い

① 委託先に対する必要かつ適切な監督

会員は、個人番号関係事務の全部または一部の委託をする場合には、「委託を受けた者」において、番号法にもとづき会員自らが果たすべき安全管理措置と同等の措置が講じられるよう、次の必要かつ適切な監督を行わなければならない。

Ａ．委託先の適切な選定

委託先の選定については、委託者は、委託先において、番号法にもとづき委託者自らが果たすべき安全管理措置と同等の措置が講じられるか否かについて、次の事項を予め確認しなければならない。

・委託先の設備
・委託先の技術水準
・委託先の従業者に対する監督・教育の状況
・委託先の経営環境　等

Ｂ．委託先に安全管理措置を遵守させるために必要な契約の締結

個人番号関係事務に係る委託契約には、契約内容として次の事項を盛り込まなければならない。

・秘密保持義務
・事業所内からの特定個人情報等の持出しの禁止
・特定個人情報等の目的外利用の禁止
・再委託における条件
・漏えい等事案が発生した場合の委託先の責任
・委託契約終了後の特定個人情報等の返却または廃棄
・従業者（※）に対する監督・教育
・契約内容の遵守状況について報告を求める規定

（※）「従業者」とは、事業者の組織内にあって直接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う。具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。

また、これらの契約内容のほか、特定個人情報等を取り扱う従業者の明確化、委託者が委託先に対して実地の調査を行うことができる規定等を盛り込むことが望ましい。

Ｃ．委託先における特定個人情報等の取扱状況の把握

委託先における特定個人情報等の取扱状況については、本指針の「６．（３）委託先における安全管理措置の遵守状況の確認、監督」を踏まえ適切に把握等を行う。

② 再委託

個人番号関係事務の全部または一部の「委託を受けた者」は、最初の委託者の許諾を得た場合に限り、再委託をすることができる。再々委託以降の場合においても、最初の委託者の許諾を得た場合に限り、同様である。なお、最初の委託者は、最初の委託先に対する監督義務だけではなく、再委託先である者に対しても間接的に監督義務を負うこととなる。

Ⅳ.「機微（センシティブ）情報」の取扱い

会員は、保護指針「Ⅰ．２.（６）機微（センシティブ）情報」および「Ⅱ．５．機微（センシティブ）情報の取扱い」に定める機微（センシティブ）情報について、保護指針を逸脱した取得、利用または第三者提供を行うことのないよう、本指針Ⅱ．に規定する措置に加えて、次に掲げる措置（１.（２）②、同（３）②、同（４）②および同（６）②を除く。）を実施しなければならない。また、機微（センシティブ）情報に該当する生体認証情報（機械による自動認証に用いられる身体的特徴のうち、非公知の情報。以下同じ。以下「生体認証情報」という。）の取扱いについては、次に掲げる全ての措置を実施しなければならない（金融分野指針別添２）。

１．各管理段階における安全管理に係る取扱規程

（１）各管理段階における安全管理に係る取扱規程

会員は、Ⅱ．１.（２）に定める「個人データの各管理段階における安全管理に係る取扱規程」において、機微（センシティブ）情報の取扱いについて規程を整備するとともに、情報通信技術の状況等を踏まえ、必要に応じて、当該規程の見直しを行わなければならない（金融分野指針８－１）。

（２）取得・入力段階における取扱規程

① 会員は、Ⅱ．７（１）に規定する取得・入力段階における取扱規程において、機微（センシティブ）情報の取扱いについては、Ⅱ．７（１）に規定する事項に加えて、次の事項を定めなければならない（金融分野指針８－１－１）。

Ａ．保護指針Ⅱ．５．①から⑨までに規定する場合のみによる取得

Ｂ．取得・入力を行う取扱者の必要最小限の限定

Ｃ．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および本人への説明事項

② 生体認証情報の取扱いは、取得・入力段階における取扱規程において、①に規定する事項に加えて、次の事項を含まなければならない（金融分野指針８－１－１－１）。

Ａ．なりすましによる登録の防止策

Ｂ．本人確認に必要な最小限の生体認証情報のみの取得

Ｃ．生体認証情報の取得後、基となった生体情報の速やかな消去

（３）利用・加工段階における取扱規程

① 会員は、Ⅱ．７．（２）①に規定する利用・加工段階における取扱規程において、機微（センシティブ）情報の取扱いについては、Ⅱ．７（２）②、⑥および⑦に規定する事項に加えて、次の事項を定めなければならない（金融分野指針８－１－２）。

Ａ．保護指針Ⅱ．５．①から⑨までに規定する目的のみによる利用・加工

Ｂ．利用・加工を行う取扱者の必要最小限の限定

Ｃ．利用・加工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および本人への説明事項

Ｄ．必要最小限の者に限定したアクセス権限の設定およびアクセス制御の実施

② 生体認証情報の取扱いは、利用段階における取扱規程において、①に規定する事項に加えて、次の事項を含まなければならない（金融分野指針８－１－２－１）。

Ａ．偽造された生体認証情報による不正認証の防止措置

Ｂ．登録された生体認証情報の不正利用の防止措置

Ｃ．残存する生体認証情報の消去

Ｄ．認証精度設定等の適切性の確認

Ｅ．生体認証による本人確認の代替措置における厳格な本人確認手続

（４）保管・保存段階における取扱規程

① 会員は、Ⅱ．７（３）①に規定する保管・保存段階における取扱規程において、機微（センシティブ）情報の取扱いについては、Ⅱ．７（３）②および⑧に規定する事項に加えて、次の事項を定めなければならない（金融分野指針８－１－３）。

Ａ．保管・保存を行う取扱者の必要最小限の限定

Ｂ．必要最小限の者に限定したアクセス権限の設定およびアクセス制御の実施

② 生体認証情報の取扱いは、保管・保存段階における取扱規程において、①に規定する事項に加えて、保存時における生体認証情報の暗号化を含まなければならないほか、サーバー等における氏名等の個人情報との分別管理を含まなければならない（金融分野指針８－１－３－１）。

（５）移送・送信段階における取扱規程

会員は、Ⅱ．７（４）①に規定する移送・送信段階における取扱規程において、機微（センシティブ）情報の取扱いについては、Ⅱ．７（４）②

および同④に規定する事項に加えて、次の事項を定めなければならない（金融分野指針８－１－４）。

Ａ．保護指針Ⅱ．５．①から⑨までに規定する目的のみによる移送・送信

Ｂ．必要最小限の者に限定したアクセス権限の設定およびアクセス制御の実施

（６）消去・廃棄段階における取扱規程

① 会員は、Ⅱ．７（５）①に規定する消去・廃棄段階における取扱規程において、機微（センシティブ）情報の取扱いについては、Ⅱ．７（５）①に規定する事項に加えて、消去・廃棄を行う取扱者の必要最小限の限定について定めなければならない（金融分野指針８－１－５）。

② 生体認証情報の取扱いは、消去・廃棄段階における取扱規程において、①に規定する事項に加えて、生体認証情報を本人確認に用いる必要性がなくなった場合は、速やかに保有する生体認証情報を消去することを含まなければならない（金融分野指針８－１－５－１）。

２．監査の実施

会員は、Ⅱ．２（７）③に規定する監査の実施に当たっては、生体認証情報の取扱いに関し、外部監査を行うとともに、必要に応じて、その他の機微（センシティブ）情報の取扱いについても外部監査を行わなければならない（金融分野指針８－２）。

以　上