（別紙）

全国銀行個人信用情報センターの会員における安全管理措置等に関する指針

全国銀行個人情報保護協議会

目　次

Ⅰ．目的等

（１）目的

全国銀行個人信用情報センターの会員における安全管理措置等に関する指針（以下「本指針」という。）は、全国銀行個人信用情報センターにおける個人情報保護指針（全国銀行個人信用情報センターにおける個人信用情報の保護と利用に関する自主ルール）（以下「センター保護指針」という。）第 18 条の規定にもとづき、センターの会員が取り扱う個人信用情報の安全管理、委託先の監督および目的外利用防止等の措置に関する具体的な指針を定めるものである。

情報通信技術の進展により、大量かつ高度に処理された情報の迅速かつ広範な流通と利用が可能となり、国民生活に多大な利便性の向上という恩恵をもたらしている一方で、個人情報の漏えい等が生じた場合に情報主体が受ける被害もより広範かつ深刻なものとなるリスクが高まっている。

そうしたなかで、個人信用情報機関への個人信用情報の登録とその利用は、与信業者における適正与信を図り、もって多重債務防止に資することを目的として、多くの会員が個人信用情報機関に個人情報を提供し、これを共同で利用するという特殊性を有しており、十分な安全管理措置に加え、目的外利用禁止その他のセンター保護指針等の決定事項の遵守徹底が図られなければならない。

本指針は、まず、基本方針・取扱規程等の整備に続いて、実施体制の整備に関する組織的・人的（従業者の監督を含む。）・技術的な安全管理措置、委託先の監督を規定している。

また、各管理段階における安全管理に係る取扱いおよび目的外利用防止策についても規定している。

センターの会員は、自己の個人信用情報の取扱いの実態を把握し、リスクの所在を認識し、基本方針・取扱規程等を整備したうえで、合理的な対策を講じ、さらにこれらの見直しを定期的に行うという一連の対応を継続的に行うことが求められる。

個々の対策は、センターの会員の組織体制、取扱場所の物理的な構造、業務フロー、記録する媒体の特性等に応じて講じられるべきものであり、一律に規定すべき性格のものではないため、本指針では、多くの項目が例示となっている。また、会員によっては、本指針に規定する対策の例が必ずしも適当とはいえない場合や、逆に本指針に規定のない対策が必要になる場合もあり得る。

重要なことは、本指針を参照してリスクの所在を点検し、リスクが認められる場合はその大きさや特性に応じた合理的な対策を検討することであり、適当な場合は本指針の規定に準じるまたは同等以上の効果が認められる方法によっても差し支えない。

（２）処分・罰則の適用

本指針において、「(金融分野指針○―○)」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についての実務指針」(以下「金融分野指針」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、センターの会員が金融分野指針を遵守し、必要かつ適切な措置等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「○○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、当該対策を実施していない場合は原則としてセンターによる処分･罰則の対象となることを示している。

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」、「(例：○○など)」等と規定している事項は、これを実施していなかったとしてもセンターによる処分・罰則の対象とはならないものの、漏えい等や目的外利用が生じた場合において処分・罰則を決定するに当たっては当該対策の実施状況（同等以上の効果が認められる方法を含む。）が勘案される。

（３）本指針の見直し

本指針は、情報通信技術の進展、センターの会員における安全管理措置の実施状況に加え、問題事案が発生した場合はその分析等を踏まえた見直しを行っていくものとする。

（４）定義

本指針における用語の定義は、センター保護指針「第 2 条（定義)」の規定によるほか、次に定めるところによる。

① 「センター」

「センター」とは、全国銀行個人信用情報センターをいう。

② 「規程等」

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

③ 「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、フロッピィディスク、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。

④ 「個人信用情報」、「個人信用データ」

A.「個人信用情報」とは、センターに登録・照会等を行うために提出すべく

記録媒体等に記録した個人情報、およびセンターへの照会によって取得した個人情報（紙媒体に出力したものを含む。）をいう。

（注）「個人情報」の定義は、個人情報保護法第２条による。

Ｂ．「個人信用データ」とは、個人信用情報のうち、記録媒体に格納されているものをいう。

⑤　「従業者」

「従業者」とは、センターの会員の組織内にあって直接間接にセンターの会員の指揮監督を受けてセンターの会員における個人信用情報の取扱いに係る業務に従事している者をいい、雇用関係にある従業員（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、取締役、執行役、理事、監査役、監事、派遣社員も含まれる。

⑥　「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（個人信用情報を取り扱うセキュリティが確保された領域）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。

⑦　「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．センター保護指針第 18 条第１項に定める安全管理措置の実施について

１．個人信用情報の安全管理に係る基本方針・取扱規程等の整備

（１）個人信用情報の安全管理に係る基本方針の整備

センターの会員は、次の事項を定めた個人信用情報の安全管理（目的外利用防止等を含む。以下同じ。）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．会員の名称

Ｂ．安全管理措置に関する質問および苦情処理の窓口

Ｃ．個人信用情報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）個人信用情報の安全管理に係る取扱規程の整備

センターの会員は、個人信用情報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「Ⅴ．各管理段階における安全管理に係る取扱規程について」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信用情報の安全管理上必要とされる手続

（３）個人信用情報の取扱状況の点検および監査に係る規程の整備

① センターの会員は、個人信用情報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、個人信用情報取扱部署が単一であるセンターの会員においては、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 センターの会員は、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

センターの会員は、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．実施体制の整備に関する組織的安全管理措置

（１）組織的安全管理措置

センターの会員は、個人信用情報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．個人信用情報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．個人信用情報の安全管理に係る取扱規程に従った運用

Ｄ．個人信用情報の取扱状況を確認できる手段の整備

Ｅ．個人信用情報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）個人信用情報管理責任者等の設置

① センターの会員は、（１）Ａ．の「個人信用情報の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．個人信用情報の安全管理に係る業務遂行の総責任者である個人信用情報管理責任者

Ｂ．個人信用情報を取り扱う各部署における個人信用情報管理者

なお、個人信用情報取扱部署が単一であるセンターの会員においては、個人信用情報管理責任者が個人信用情報管理者を兼務することも認められる。個人信用情報管理責任者は、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 センターの会員は、①Ａ．の個人信用情報管理責任者に、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．個人信用情報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．個人信用情報管理者および５．（２）「個人信用データの利用者の識別および認証」の①に定める「本人確認に関する情報」の管理者の任命

Ｃ．個人信用情報管理者からの報告徴収および助言・指導

Ｄ．個人信用情報の安全管理に関する教育・研修の企画
Ｅ．その他当該会員全体における個人信用情報の安全管理に関すること

③　センターの会員は、①Ｂ．の個人信用情報管理者に、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．個人信用情報の取扱者の指定および変更等の管理
Ｂ．個人信用情報の利用申請の承認および記録等の管理
Ｃ．個人信用情報を取り扱う保管媒体の設置場所の指定および変更等
Ｄ．個人信用情報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．個人信用情報の取扱状況の把握
Ｆ．委託先における個人信用情報の取扱状況等の監督
Ｇ．個人信用情報の安全管理に関する教育・研修の実施
Ｈ．個人信用情報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信用情報の安全管理に関すること

（３）横断的な組織体制

センターの会員は、個人信用情報管理責任者を補佐し、個人信用情報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．個人信用情報の利用、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．個人信用情報の取扱いに関係する全ての部署店の役割と責任（委託先の監督を含む。）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．個人信用情報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

センターの会員は、（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、従業者との個人信用情報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．個人信用情報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）個人信用情報の安全管理に係る取扱規程に従った運用

センターの会員は、（１）Ｃ．の「個人信用情報の安全管理に係る取扱規程に従った運用」として、個人信用情報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）個人信用情報の取扱状況を確認できる手段の整備

センターの会員は、（１）Ｄ．の「個人信用情報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．アクセス制限の状況

（７）個人信用情報の取扱状況の点検および監査体制の整備と実施

① センターの会員は、（１）Ｅ．の「個人信用情報の取扱状況の点検および監査体制の整備と実施」として、個人信用情報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、個人信用情報取扱部署が単一であるセンターの会員においては、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２－５）。

② センターの会員は、個人信用情報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 センターの会員は、監査の実施に当たっては、監査対象となる個人信用情報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信用情報を取り扱う場合には、当該部署における個人信用情報の取扱いについて、個人信用情報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　センターの会員は、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　センター会員は、（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．「漏えい等事案の影響等に関する調査体制」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信用情報の関係部署店・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信用情報の情報主体・項目・件数等の特定
Ｄ．個人信用情報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「自社内外への報告体制」における報告体制の整備としては、次のような例がある。

Ａ．連絡体制の整備

　個人信用情報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、および個人信用情報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信用情報管理責任者等への連絡体制に関する事項を予め定めること。

　なお、体制整備に当たっては、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に留意すること。

Ｂ．監督当局等およびセンターへの報告体制の整備

　監督当局等およびセンターへの報告体制に関する事項を予め定めること。

Ｃ．本人への情報提供体制の整備

　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を予め定めること。

Ｄ．事実関係の公表体制の整備

　事実関係の公表に関する事項を予め定めること。

なお、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に留意すること。

E．警察への通報

個人信用情報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　センターの会員は、１．（２）C.「各管理段階において個人信用情報の安全管理上必要とされる手続」またはⅤ．（５）「漏えい等事案への対応の段階における取扱規程」の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・類似事業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．実施体制の整備に関する人的安全管理措置

（１）人的安全管理措置

①　センターの会員は、個人信用情報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　センターの会員は、個人信用情報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．従業者との個人信用情報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．従業者による個人信用情報管理手続の遵守状況の確認

（２）従業者との個人信用情報の非開示契約等の締結

①　センターの会員は、（１）②A．の「従業者との個人信用情報の非開示契約等の締結」として、採用時等に従業者と個人信用情報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　センターの会員は、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．従業者を個人信用情報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．派遣社員を個人信用情報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（電子的手段を含む。）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守秘義務を遵守する旨を規定すること。また、守秘義務に反した場合の責任（損害賠償等）についても規定すること。

③　センターの会員は、①の就業規則等の整備に当たっては、センターの会員は、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・責任の明確化

センターの会員は、（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信用情報の取扱いに関する従業者の役割・責任の明確化

B．個人信用情報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　センターの会員は、（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．個人信用情報管理責任者および個人信用情報管理者に対する教育・訓練

C．個人信用情報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　センターの会員は、①D．の「従業者に対する教育・訓練の評価および定期的な見直し」を講じるに当たっては、次の事項に留意する。

必須項目

A．個人信用情報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．個人信用情報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．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、個人信用情報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、センター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）従業者による個人信用情報管理手続の遵守状況の確認

センターの会員は、（１）②D．の「従業者による個人信用情報管理手続の遵守状況の確認」として、１．（２）「個人信用情報の安全管理に係る取扱規程の整備」の個人信用情報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）「個人信用情報の安全管理に係る取扱規程に従った運用」にもとづく記録および確認を行うとともに、２．（７）「個人信用情報の取扱状況の点検および監査体制の整備と実施」の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．実施体制の整備に関する物理的安全管理措置

（１）物理的安全管理措置

センターの会員は、個人信用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．個人信用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．個人信用データの削除及び機器、電子媒体等の廃棄

（２）個人信用データの取扱区域等の管理

センターの会員は、（１）A．の「個人信用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．個人信用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

センターの会員は、（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．個人信用データを取り扱う機器等の施錠等による保管

Ｂ．個人信用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

センターの会員は、「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．持ち運ぶ個人信用データの暗号化、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）個人信用データの削除及び機器、電子媒体等の廃棄

センターの会員は、「個人信用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．個人信用データが記載された書類等または記録された機器等の物理的な破壊等

５．実施体制の整備に関する技術的安全管理措置

（１）技術的安全管理措置

① センターの会員は、個人信用情報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．個人信用データの利用者の識別および認証

Ｂ．個人信用データの管理区分の設定およびアクセス制御

Ｃ．個人信用データへのアクセス権限の管理

Ｄ．個人信用データの漏えい等防止策

Ｅ．個人信用データへのアクセス記録および分析

Ｆ．個人信用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．個人信用データを取り扱う情報システムの監視および監査

② センターの会員は、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）個人信用データの利用者の識別および認証

① センターの会員は、（１）①Ａ．の「個人信用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 センターの会員は、①Ａ．の「本人確認機能の整備」として、個人信用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．記録媒体上の個人信用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（例えば、ＭＡＣアドレス認証等）を実施する。

③ センターに会員は、①Ｂ．の「本人確認に関する情報の不正使用防止機能の整備」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 センターの会員は、①Ｃ．の「本人確認に関する情報が他人に知られないための対策」を講じるに当たっては、次の事項に留意する。

例示項目

Ａ．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。
Ｂ．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

C．本人確認機能にパスワードを使用する場合は、パスワード文字数の最低限度を設定する。

D．本人確認機能にパスワードを使用する場合は、同一または類似パスワードの再利用を制限する。

（３）個人信用データの管理区分の設定およびアクセス制御

① センターの会員は、（１）①B．の「個人信用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 センターの会員は、①A．の「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」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 センターの会員は、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 センターの会員は、③B．の「外部ネットワークからの不正侵入防止機能の整備」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、外部からの個人信用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）個人信用データのアクセス権限の管理

① センターの会員は、（１）①C．の「個人信用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信用データへのアクセス権限の適切な付与および見直し

B．個人信用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 センターの会員は、①A．の「従業者に対する個人信用データへのアクセス権

限の適切な付与および見直し」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、定期的な見直しを行うこと。アクセス権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　センターの会員は、①Ａ．「従業者に対する個人信用データへのアクセス権限の適切な付与および見直し」および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」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）個人信用データの漏えい等防止策

①　センターの会員は、（１）①Ｄ．の「個人信用データの漏えい等防止策」として、個人信用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　センターの会員は、①の「個人信用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　センターの会員は、②Ａ．の「蓄積データの漏えい等防止策」として、ファイルの不正コピーや盗難等による漏えい等を防止するため、ファイルの不正コピーや盗難の際にも個人信用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こと（例：記録媒体上の個人信用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など）。

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こと（例えば、

記録媒体上の個人信用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など)。

（注）センターの会員・センター間で授受する記録媒体は、センター所定の方法により暗号化すること。

④　センターの会員は、②Ｂ．の「伝送データの漏えい等防止策」として、個人信用データの伝送時に盗聴等による漏えい等を防止するため、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．個人信用データを通信（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、個人信用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こと。

(注)センターの会員･センター間の通信による個人信用データの授受は、センター所定の方法による。

⑤　センターの会員は、②Ｃ．の「コンピュータウイルス等不正プログラムへの防御対策」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．自社の取り決めに従った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・安定性を確認すること（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こと。

⑥　センターの会員は、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）個人信用データへのアクセスの記録および分析

①　センターの会員は、（１）①Ｅ．の「個人信用データへのアクセスの記録および分析」として、個人信用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 センターの会員は、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．個人信用データを取り扱う情報システムにおいては、個人信用データへのアクセスや操作および個人信用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．個人信用データへのアクセスや操作および個人信用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は、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．個人信用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）個人信用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

センターの会員は、（１）①Ｆ．の「個人信用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、個人信用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）個人信用データを取り扱う情報システムの監視および監査

センターの会員は、（１）①Ｇ．の「個人信用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、個人信用データを取り扱う情報システムの利用状況、個人信用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）「個人信用データへのアクセスの記録および分析」および（７）「個人信用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」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）。

Ⅲ．センター保護指針第 18 条第２項に定める「従業者の監督」について

センターの会員は、センター保護指針第 18 条第２項にもとづき、「Ⅰ．３．実施体制の整備に関する人的安全管理措置」に規定する措置を講ずることにより、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（金融分野指針Ⅱ）。

Ⅳ．センター保護指針第 18 条第３項に定める「委託先の監督」について

センターの会員は、センター保護指針第 18 条第３項にもとづき、個人信用情報の取扱いを委託する場合は、個人信用情報を適正に取り扱っていると認められる者を選定し、個人信用情報の取扱いを委託するとともに、委託先における当該個人信用情報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）個人信用情報保護に関する委託先選定の基準

① センターの会員は、個人信用情報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信用情報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信用情報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信用情報安全管理上の信用度
Ｄ．委託先の経営の健全性

② 委託先の選定基準においては、①Ａ．の「委託先における個人信用情報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信用情報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信用情報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信用情報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信用情報の安全管理に係る実施体制の整備」として、Ⅱ．２．の組織的安全管理措置、Ⅱ．３．の人的安全管理措置、Ⅱ．４．の物理的安全管理措置、Ⅱ．５．の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信用情報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の「実績等にもとづく委託先の個人信用情報安全管理上の信用度」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　センターの会員は、（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」の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　センターの会員は、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信用情報の漏えいの防止、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　センターの会員は、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　①B．の「委託先における個人信用情報の漏えいの防止、盗用、改ざんおよび目的外利用の禁止」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信用情報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．委託先が個人信用情報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。

④　センターの会員は、①C．の「再委託における条件」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）。

⑤　①D．の「漏えい等事案が発生した際の委託先の責任」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

（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　センターの会員は、（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」の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、センターの会員は、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　センターの会員は、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信用情報の漏えい等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センターの会員に報告され、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、委託元であるセンターの会員においても、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。

Ⅴ．各管理段階における安全管理に係る取扱規程について

センターの会員は、Ⅱ．１．（２）「個人信用情報の安全管理に係る取扱規程の整備」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）利用・加工段階における取扱規程

① センターの会員は、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信用情報の限定
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．個人信用データへのアクセス制御
Ｈ．個人信用データの管理区域外への持ち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 センターの会員は、②Ｃ．の「利用・加工の対象となる個人信用情報の限定」を定めるに当たっては、次の事項に留意する。

例示項目

Ａ．システムの開発、変更等に伴う動作確認時のテストデータとして、個人信用データを使用する場合は、使用前に個人が特定できないようにすること。なお、テスト終了後は、テストデータの廃棄を確認すること。

④ センターの会員は、②Ｆ．の「機器・記録媒体等の管理手続」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．個人信用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：離席時の個人信用情報を記載した紙媒体や個人信用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、個人信用情報を記録した記録媒体等の施錠保管、個人信用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．個人信用データを保存した持ち出しが容易な機器類（ノート型コンピュータ等）は、個人信用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。持ち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）。

例示項目

A．個人信用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、端末画面への表示については次の事項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印刷した紙媒体を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。

⑤　センターの会員は、②G．の「個人データへのアクセス制御」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）

⑥　センターの会員は、②G．の「個人信用データへのアクセス制御」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、従業者におけ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

⑦　②H．の「個人信用情報の管理区域外への持ち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．個人信用情報の管理区域外への持ち出しに関する取扱者の役割・責任

B．個人信用情報の管理区域外への持ち出しに関する取扱者の必要最小限の限定

C．個人信用情報の管理区域外への持ち出しの対象となる個人信用情報の必要最小限の限定

D．個人信用情報の管理区域外への持ち出し時の照合および確認手続

E．個人信用情報の管理区域外への持ち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．個人信用情報の管理区域外への持ち出し状況の記録および分析

⑧　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．個人信用データの利用者の識別および認証

B．個人信用データの管理区分の設定およびアクセス制御

C．個人信用データへのアクセス権限の管理

D．個人信用データの漏えい等防止策

E．個人信用データへのアクセス記録および分析

F．個人信用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

（２）保管・保存段階における取扱規程

①　センターの会員は、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信用情報の限定

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．個人信用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　センターの会員は、②Ｅ．の「機器・記録媒体等の管理手続」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．フロッピーディスク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を防止するため、ラベルへの内容表記は記号等により最小限の項目にとどめる。

④　センターの会員は、②Ｆ．の「個人データへのアクセス制御」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　センターの会員は、②Ｆ．「個人信用データへのアクセス制御」を講じるに当たっては、次の事項に留意のうえ、個人信用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者に対する資格審査のうえ、資格識別証等を発行し（例えば、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　センターの会員は、②F．「個人信用データへのアクセス制御」を講じるに当たっては、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、個人信用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　センターの会員は、②F．「個人信用データへのアクセス制御」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．個人信用データの利用者の識別および認証

B．個人信用データの管理区分の設定およびアクセス制御

C．個人信用データへのアクセス権限の管理

D．個人信用データの漏えい等防止策

E．個人信用データへのアクセス記録および分析

F．個人信用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）移送・送信段階における取扱規程

①　センターの会員は、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信用情報の限定

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．個人信用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 センターの会員は、②Ｄ．「移送・送信時の照合および確認手続」を定めるに当たっては、次の事項に留意する。

必須項目

Ａ．個人信用情報をＦＡＸ送信することは原則として回避すること。

やむを得ず個人信用情報をＦＡＸ等で送信する場合は、誤送信の防止および個人信用情報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．個人信用データの利用者の識別および認証

Ｂ．個人信用データの管理区分の設定およびアクセス制御

Ｃ．個人信用データへのアクセス権限の管理

Ｄ．個人信用データの漏えい等防止策

Ｅ．個人信用データへのアクセス記録および分析

（４）消去・廃棄段階における取扱規程

① センターの会員は、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．個人信用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 センターの会員は、①Ｃ．の「消去・廃棄時の照合および確認手続」を定めるに当たっては、次の事項に留意する。

例示項目

Ａ．システムの開発、変更等に伴う動作確認時のテストデータは、個人が特定できないようにしてあったとしても、テスト終了後はその廃棄を確認すること。

③ センターの会員は、①Ｅ．「機器・記録媒体等の管理手続」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う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信用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、守秘義務を含む委託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。

（５）漏えい等事案への対応の段階における取扱規程

① センターの会員は、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・原因に関する調査手続
Ｅ．再発防止策・事後対応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または監督当局への報告
Ｂ．本人への通知等
Ｃ．二次被害の防止・類似案件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、センターの会員は、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および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。

Ⅵ. 目的外利用防止措置

センターの会員は、個人信用情報の目的外利用を防止するためのチェック体制を整備しなければならない。

このチェック体制は、①照会の前提となる同意取得等の確認、および②照会作業者と確認者の分離を基本とすること。

（1）オンラインリアルタイム照会におけるチェック体制

① 営業店において照会を行う場合

センターの会員は、営業店において照会を行う場合のチェック体制として、次のいずれかによるチェック体制（適当な場合はこれに準じる方法）を講じなければならない（注１）。

チェック時点	チェック方法
照会前	照会作業者（端末操作者）とは別の者（確認者）が同意取得等を確認する書類（注２）を確認したうえでなければ照会できない仕組みとする。 ＊当該仕組みの例としては、照会作業者の入力するＩＤ・パスワードとは別の者（確認者）のＩＤ・パスワードが入力されなければ照会できないようにする方法、照会作業者とは別の者（確認者）が発行する承認番号等を入力しなければ照会できないようにする方法等が考えられる（注３）。
回答情報受領時	照会作業者とは別の者（確認者）でなければ回答情報を取得できない仕組みとし、確認者が回答情報と同意取得等を確認する書類（注２）を突合する。 ＊当該仕組みの例としては、照会作業者の入力したＩＤ・パスワードとは別の者（確認者）のＩＤ・パスワードを入力しないと回答情報を受信できないようにする方法、回答情報を社内便等で送付する場合において送付先を照会作業者とは別の者（確認者）とする方法等が考えられる（注３）。
照会日以降	照会後に日々の被照会者リストを出力し、照会作業者とは別の者（確認者）が同リストと同意取得等を確認する書類（注２）を突合する。 この方法による場合は、同リストは照会案件がない日についてもその旨を表示して出力し、照会がなかったことの確認を行うこと（注４）。 また、確認者による確認は、原則として照会日の翌営業日までに完了すること。

チェック時点	チェック方法
	照会後に日々の照会件数リストを出力し、照会作業者とは別の者（確認者）が照会件数と回答情報の件数の一致を確認したうえで、回答情報と同意取得等を確認する書類を突合する。 この方法による場合は、同リストは照会案件がない日についてもその旨を表示して出力し、照会がなかったことの確認を行うこと（注４）。 また、確認者による確認は、原則として照会日の翌営業日までに完了すること。

（注１）上記のチェックのほか、「Ⅱ．４．（６）個人信用データへのアクセスの記録および分析、（７）個人信用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」により、目的外利用防止措置を講じる必要があることに留意する。例えば、センターへの個人信用情報の照会および照会記録情報の取消・訂正等の処理の実績（照会依頼実績）をセンターに確認することができるので、照会依頼実績を確認することにより、照会端末の利用状況を定期的に監査するとともに、必要に応じて随時監査すること。

（注２）上記における同意取得等を確認する書類は次のとおり。

区分	同意取得等を確認する書類
新規与信判断を目的とする照会の場合	借入申込書等 ＊信用状況再調査または転居先調査を目的とする照会の場合は、センターに被照会者の取引情報が登録されていないとエラーにする仕組みをセンターにおいて講じている。
連帯保証人の場合	連帯保証人であることが確認できる書類（当該債務の主たる債務者に係る借入申込書、元帳等）
取引停止処分照会の場合	新規先：当座預金開設申込書 既存先:既存先であることを確認できる資料（元帳等）
官報情報照会の場合	新規先:借入申込書、当座預金開設申込書等 既存先:既存先であることを確認できる資料（元帳等）

（注３）照会作業者とは別のもの（確認者）のＩＤ・パスワードの管理は、前記「Ⅱ．４（２）個人信用データの利用者の識別および認証」に規定する措置を講じること。特に、確認者のＩＤ・パスワードの他人への貸与を禁止する等の「本人確認に関する情報が他人に知られないための対策」を講じるとともに、確認者のＩＤ・パスワードの利用状況を確認する等の「本人確認に関する情報の不正使用防止機能の整備」を行わなければならないことに留意すること。

（注４）照会案件がある日のみ出力することとすると、リストの出力を失念した場合やリストの破棄等があった場合に必要な確認ができないことに留意する。

② 営業店からの依頼を受けて本部が照会を行う場合

センターの会員は、営業店からの依頼を受けて本部が照会を行う場合のチェック体制として、次のいずれかによるチェック体制（適当な場合はこれに準じる方法）を講じなければならない（注１）。

照会を行う本部の対応	照会依頼を行う営業店におけるチェック方法
照会依頼を行った営業店に被照会者リストを還元する場合（注２）	照会作業者とは別の者（確認者）が同リストと同意取得等を確認する書類を突合する。 この方法による場合は、同リストは照会案件がない日についてもその旨を表示して出力し、照会がなかったことの確認を行うこと（注３）。 また、確認者による確認は、原則として照会日の翌営業日までに完了すること。
照会依頼を行った営業店に照会件数リストを還元する場合（注２）	照会作業者とは別の者（確認者）が同リストの照会件数と回答情報の件数の一致を確認したうえで、回答情報と同意取得等を確認する書類を突合する。 この方法による場合は、同リストは照会案件がない日についてもその旨を表示して出力し、照会がなかったことの確認を行うこと（注３）。 また、確認者による確認は、原則として照会日の翌営業日までに完了すること。
照会依頼を行った営業店に特に還元を行わない場合（注２）	営業店において照会日以降にチェックすることができないため、前記①の照会前または回答情報受領時の方法に準じて本部への照会依頼前または回答情報受領時にチェックを行う。 ＊照会依頼前のチェックの仕組みの例としては、照会作業者の入力するＩＤ･パスワードとは別の者(確認者)のＩＤ･パスワードが入力されなければ本部へ照会依頼できないようにする方法、照会作業者とは別の者（確認者)が発行する承認番号等を入力しなければ本部へ照会依頼できないようにする方法等が考えられる（注４）。 ＊回答受領時のチェックの仕組みの例としては、照会作業者の入力したＩＤ･パスワードとは別の者(確認者)

照会を行う本部の対応	照会依頼を行う営業店におけるチェック方法
	のＩＤ･パスワードを入力しないと本部から回答情報を受信できないようにする方法､本部からの回答情報を社内便等で送付する場合において送付先を照会作業者とは別の者（確認者）とする方法等が考えられる（注４）。

（注１）上記のチェックのほか､「Ⅱ．４．（６）個人信用データへのアクセスの記録および分析､（７）個人信用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」により、目的外利用防止措置を講じる必要があることに留意する。例えば、センターへの個人信用情報の照会および照会記録情報の取消・訂正等の処理の実績（照会依頼実績）をセンターに確認することができるので、照会依頼実績を確認することにより、照会端末の利用状況を定期的に監査するとともに、必要に応じて随時監査すること。

（注２）上記のほかに、照会を行う本部における不正を防止するために、本部において照会した合計件数と営業店からの照会依頼件数の合計とが一致していることを確認すること。

また、本部において、営業店からの照会依頼にもとづかない照会を行う場合には、前記①に準じてチェックを行うこと。

（注３）照会案件がある日のみ出力することとすると、リストの出力を失念した場合やリストの破棄等があった場合に必要な確認ができないことに留意する。

（注４）照会作業者とは別のもの（確認者）のＩＤ･パスワードの管理は､前記「Ⅱ．４（２）個人信用データの利用者の識別および認証」に規定する措置を講じること。特に、確認者のＩＤ・パスワードの他人への貸与を禁止する等の「本人確認に関する情報が他人に知られないための対策」を講じるとともに、確認者のＩＤ・パスワードの利用状況を確認する等の「本人確認に関する情報の不正使用防止機能の整備」を行わなければならないことに留意すること。

（２）バッチ照会におけるチェック体制

センターの会員は、ファイル転送によるバッチ照会を行う場合のチェック体制として、次のチェック体制（適当な場合はこれに準じる方法。）を講じなければならない。

① 業務担当部署における取扱い

Ａ．業務担当部署の依頼によりバッチ照会を行う場合は、予めファイル転送の要件定義書を作成し、業務担当部署内において複数名による精査を行う。

Ｂ．要件定義書作成に当たっては、システム開発部署と当該作成に係る調整を十分に行う。

Ｃ．業務担当部署が作成した要件定義書は、予め定めた十分な期間保存する。

② システム開発部署における取扱い

Ａ．システム開発部署は、要件定義書にもとづきシステム設計書を作成し、同部署内で複数名による精査を行う。

Ｂ．システム開発部署は、作成したシステム設計書またはテストデータを業務担当部署に回付し、業務担当部署内においても複数名により精査を行う。

Ｃ．システム開発部署は、テストを終了したプログラムの運用をシステム運用部署に依頼する。

③ システム運用部署における取扱い

Ａ．システム運用部署は、システム開発部署から依頼を受けたプログラムの運用を業務処理手順書にもとづいて行う。

なお、システム運用部署にはプログラム作成・変更等の権限を付与しない。

Ｂ．システム運用部署は、プログラムを予め定めた十分な期間保存する。

④ 同意取得等を確認する書類の確認

バッチ照会の場合も、オンラインリアルタイム照会の場合と同様に、同意取得等を確認する書類の確認が必要であるが、元帳等の既存顧客リストにもとづかなければ作成できない仕組みになっている等、システム的なチェックが可能な場合には、既存顧客の信用状況再調査を目的とした照会についてはシステム的に既存顧客であることをチェックする方法によっても差し支えない。

以　上