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

Ⅰ．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１０条に定める安全管理措置の実施について

（１）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

（個人データの安全管理に係る基本方針の整備）

１－１　「金融分野における個人情報保護に関するガイドライン」（平成１６年金融庁告示第６７号。以下「ガイドライン」という。）第１条第１項に規定する金融分野における個人情報取扱事業者は、ガイドライン第１０条第５項（１）①に基づき、次に掲げる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。

①　個人情報取扱事業者の名称
②　安全管理措置に関する質問及び苦情処理の窓口
③　個人データの安全管理に関する宣言
④　基本方針の継続的改善の宣言
⑤　関係法令等遵守の宣言

（個人データの安全管理に係る取扱規程の整備）

１－２　金融分野における個人情報取扱事業者は、ガイドライン第１０条第５項（１）②に規定する「個人データの安全管理に係る取扱規程の整備」として、ガイドライン第１０条第５項（２）に規定す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を整備し、各管理段階ごとに別添１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、各管理段階ごと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に掲げる事項を定めることも認められる。

①　取扱者の役割・責任
②　取扱者の限定
③　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き

（個人データの取扱状況の点検及び監査に係る規程の整備）

１－３　金融分野における個人情報取扱事業者は、ガイドライン第１０条第５項（１）③に基づき、個人データの取扱状況に関する点検及び監査の規程を整備し、次に掲げ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、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。

①　点検及び監査の目的
②　点検及び監査の実施部署
③　点検責任者及び点検担当者の役割・責任
④　監査責任者及び監査担当者の役割・責任
⑤　点検及び監査に関する手続き

（外部委託に係る規程の整備）

１－４　金融分野における個人情報取扱事業者は、ガイドライン第１０条第５項（１）④に基づき、外部委託に係る取扱規程を整備し、次に掲げる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。
① 委託先の選定基準
② 委託契約に盛り込むべき安全管理に関する内容

（２）個人データの安全管理措置に係る実施体制の整備

１）実施体制の整備に関する組織的安全管理措置

金融分野における個人情報取扱事業者は、ガイドライン第１０条第６項に基づき、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、次に掲げる措置を講じなければならない。
① 個人データの管理責任者等の設置
② 就業規則等における安全管理措置の整備
③ 個人データの安全管理に係る取扱規程に従った運用
④ 個人データの取扱状況を確認できる手段の整備
⑤ 個人データの取扱状況の点検及び監査体制の整備と実施
⑥ 漏えい事案等に対応する体制の整備

（個人データ管理責任者等の設置）
２－１ 金融分野における個人情報取扱事業者は、「個人データの管理責任者等の設置」として次に掲げる役職者を設置しなければならない。
① 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
② 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又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。

（注） 金融分野における個人情報取扱事業者は、「個人データの管理責任者等の設置」として、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を設置することが望ましい。

２－１―１ 金融分野における個人情報取扱事業者は、２－１①に規定する個人データ管理責任者に、次に掲げる業務を所管させなければならない。
① 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
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
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
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

２－１―２ 金融分野における個人情報取扱事業者は、２－１②に規定する個人データ管理者に、次に掲げる業務を所管させなければならない。
① 個人データの取扱者の指定及び変更等の管理
② 個人データの利用申請の承認及び記録等の管理
③ 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
④ 個人データの管理区分及び権限についての設定及び変更の管理
⑤ 個人データの取扱状況の把握
⑥ 委託先における個人データの取扱状況等の監督
⑦ 個人データの安全管理に関する教育・研修の実施
⑧ 個人データ管理責任者に対する報告
⑨ 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

（就業規則等における安全管理措置の整備）

２－２　金融分野における個人情報取扱事業者は、「就業規則等における安全管理措置の整備」として、次に掲げる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。

①　個人データの取り扱いに関する従業者の役割・責任

②　違反時の懲戒処分

（個人データの安全管理に係る取扱規程に従った運用）

２－３　金融分野における個人情報取扱事業者は、「個人データの安全管理に係る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及び確認を行わなければならない。

（個人データの取扱状況を確認できる手段の整備）

２－４　金融分野における個人情報取扱事業者は、「個人データの取扱状況を確認できる手段の整備」として、次に掲げる事項を含む台帳等を整備しなければならない。

①　取得項目

②　利用目的

③　保管場所・保管方法・保管期限

④　管理部署

⑤　アクセス制御の状況

（個人データの取扱状況の点検及び監査体制の整備と実施）

２－５　金融分野における個人情報取扱事業者は、「個人データの取扱状況の点検及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。

２－５―１　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部署において点検責任者及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、定期的及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。

２－５―２　金融分野における個人情報取扱事業者は、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、定期的及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。

（注）金融分野における個人情報取扱事業者は、新たなリスクに対応するための、安全管理措置の評価、見直し及び改善に向けて、個人情報保護対策及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。

（漏えい事案等に対応する体制の整備）
２－６　金融分野における個人情報取扱事業者は、「漏えい事案等に対応する体制の整備」として、次に掲げる体制を整備しなければならない。
①　対応部署
②　漏えい事案等の影響・原因等に関する調査体制
③　再発防止策・事後対策の検討体制
④　自社内外への報告体制

２－６－１　金融分野における個人情報取扱事業者は、１－２③又は６－６－１に基づき、自社内外への報告体制を整備するとともに、漏えい事案等が発生した場合には、次に掲げる事項を実施しなければならない。
①　監督当局等への報告
②　本人への通知等
③　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事案等の事実関係及び再発防止策等の早急な公表

２）実施体制の整備に関する人的安全管理措置

金融分野における個人情報取扱事業者は、ガイドライン第１０条第６項に基づき、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、次に掲げる措置を講じなければならない。
①　従業者との個人データの非開示契約等の締結
②　従業者の役割・責任等の明確化
③　従業者への安全管理措置の周知徹底、教育及び訓練
④　従業者による個人データ管理手続の遵守状況の確認

（従業者との個人データの非開示契約等の締結）
３－１　金融分野における個人情報取扱事業者は、「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。

（従業者の役割・責任等の明確化）
３－２　金融分野における個人情報取扱事業者は、「従業者の役割・責任等の明確化」として、次に掲げる措置を講じなければならない。
①　各管理段階における個人データの取り扱いに関する従業者の役割・責任の明確化
②　個人データの管理区分及びアクセス権限の設定
③　違反時の懲戒処分を定めた就業規則等の整備
④　必要に応じた規程等の見直し

（従業者への安全管理措置の周知徹底、教育及び訓練）
３－３　金融分野における個人情報取扱事業者は、「従業者への安全管理措置の周知徹底、教育及び訓練」として、次に掲げる措置を講じなければならない。
①　従業者に対する採用時の教育及び定期的な教育・訓練
②　個人データ管理責任者及び個人データ管理者に対する教育・訓練
③　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
④　従業者に対する教育・訓練の評価及び定期的な見直し

（従業者による個人データ管理手続きの遵守状況の確認）
３－４　金融分野における個人情報取扱事業者は、「従業者による個人データ管理手続きの遵守状況の確認」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、２－３に基づく記録及び確認を行うとともに、２－５に基づき点検及び監査を実施しなければならない。

３）実施体制の整備に関する技術的安全管理措置

金融分野における個人情報取扱事業者は、ガイドライン第１０条第６項に基づき、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、次に掲げる措置を講じなければならない。

① 個人データの利用者の識別及び認証
② 個人データの管理区分の設定及びアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データの漏えい・毀損等防止策
⑤ 個人データへのアクセスの記録及び分析
⑥ 個人データを取り扱う情報システムの稼動状況の記録及び分析
⑦ 個人データを取り扱う情報システムの監視及び監査

（個人データの利用者の識別及び認証）

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、次に掲げる措置を講じなければならない。

① 本人確認機能の整備
② 本人確認に関する情報の不正使用防止機能の整備
③ 本人確認に関する情報が他人に知られないための対策

（個人データの管理区分の設定及びアクセス制御）

４－２　金融分野における個人情報取扱事業者は、「個人データの管理区分の設定及びアクセス制御」として、次に掲げる措置を講じなければならない。

① 従業者の役割・責任に応じた管理区分及びアクセス権限の設定
② 事業者内部における権限外者に対するアクセス制御
③ 外部からの不正アクセスの防止措置

４－２－１　金融分野における個人情報取扱事業者は、「外部からの不正アクセスの防止措置」として、次に掲げる措置を講じなければならない。

① アクセス可能な通信経路の限定
② 外部ネットワークからの不正侵入防止機能の整備
③ 不正アクセスの監視機能の整備
④ ネットワークによるアクセス制御機能の整備

（個人データへのアクセス権限の管理）

４－３　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権限の管理」として、次に掲げる措置を講じなければならない。

① 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及び見直し
② 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
③ 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

（個人データの漏えい・毀損等防止策）

４－４　金融分野における個人情報取扱事業者は、「個人データの漏えい・毀損等防止策」として、個人データの保護策を講ずることとともに、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。

４－４－１　金融分野における個人情報取扱事業者は、「個人データの保護策を講ずること」

として、次に掲げる措置を講じなければならない。
① 蓄積データの漏えい防止策
② 伝送データの漏えい防止策
③ コンピュータウイルス等不正プログラムへの防御対策

４－４－２　金融分野における個人情報取扱事業者は、「障害発生時の技術的対応・復旧手続の整備」として、次に掲げる措置を講じなければならない。
① 不正アクセスの発生に備えた対応・復旧手続の整備
② 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
③ リカバリ機能の整備

（個人データへのアクセスの記録及び分析）
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。

（個人データを取り扱う情報システムの稼動状況の記録及び分析）
４－６　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稼動状況の記録及び分析」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。

（個人データを取り扱う情報システムの監視及び監査）
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。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。

Ⅱ．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１１条に定める「従業者の監督」について

金融分野における個人情報取扱事業者は、ガイドライン第１１条に基づき、「Ⅰ．（２）２）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。

Ⅲ．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１２条に定める「委託先の監督」について

金融分野における個人情報取扱事業者は、ガイドライン第１２条第３項に基づき、個人データを適正に取扱っていると認められる者を選定し、個人データの取り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。

（個人データ保護に関する委託先選定の基準）

５－１　金融分野における個人情報取扱事業者は、個人データの取り扱いを委託する場合には、ガイドライン第１２条第３項①に基づき、次に掲げる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。

① 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
② 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
③ 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
④ 委託先の経営の健全性

５－１－１　委託先選定の基準においては、「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、次に掲げる事項を定めなければならない。

① 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
② 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
③ 委託先における個人データの取扱状況の点検及び監査に係る規程の整備
④ 委託先における外部委託に係る規程の整備

５－１－２　委託先選定の基準においては、「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、Ⅰ（２）１）の組織的安全管理措置、同２）の人的安全管理措置及び同３）の技術的安全管理措置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。

５－２　金融分野における個人情報取扱事業者は、５－３に基づき、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又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。

（委託契約において盛り込むべき安全管理に関する内容）

５－３　金融分野における個人情報取扱事業者は、委託契約において、次に掲げる安全管理に関する事項を盛り込まなければならない。

① 委託者の監督・監査・報告徴収に関する権限
② 委託先における個人データの漏えい、盗用、改ざん及び目的外利用の禁止
③ 再委託における条件
④ 漏えい事案等が発生した際の委託先の責任

（注）

・ 金融分野における個人情報取扱事業者は、「再委託における条件」として、再委託の可否及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又は承認等を、委託契約に盛り込むことが望ましい。

・ 金融分野における個人情報取扱事業者は、委託先において個人データを取り扱う者の氏名・役職又は部署名を、委託契約に盛り込むことが望ましい。

５－４　金融分野における個人情報取扱事業者は、５－３に基づき、定期的に監査を行う等により、定期的又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、金融分野における個人情報取扱事業者は、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。

（別添１）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１０条第５項（２）に定める各管理段階における安全管理に係る取扱規程について

金融分野における個人情報取扱事業者は、１－２に基づき、各管理段階ごとの安全管理に係る取扱規程において、６－１から６－６－１までの事項を定めなければならない。

（取得・入力段階における取扱規程）

６－１　金融分野における個人情報取扱事業者は、取得・入力段階における取扱規程において、次に掲げる事項を定めなければならない。

① 取得・入力に関する取扱者の役割・責任
② 取得・入力に関する取扱者の限定
③ 取得・入力の対象となる個人データの限定
④ 取得・入力時の照合及び確認手続き
⑤ 取得・入力の規程外作業に関する申請及び承認手続き
⑥ 機器・記録媒体等の管理手続き
⑦ 個人データへのアクセス制御
⑧ 取得・入力状況の記録及び分析

（注）金融分野における個人情報取扱事業者は、取得・入力段階における取扱規程について、「個人データへのアクセス制御」として、次に掲げる事項を定めることが望ましい。

① 入館（室）者による不正行為の防止のための、業務実施場所及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

② 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又はモニタリングの実施
（例）記録機能を持つ媒体の持込み・持出し禁止又は検査の実施

③ 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、業務上の必要性に基づく限定
（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及び機器の更新への対応

（利用・加工段階における取扱規程）

６－２　金融分野における個人情報取扱事業者は、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及び技術的安全管理措置を定めなければならない。

６－２－１　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、次に掲げる事項を含まなければならない。
① 利用・加工に関する取扱者の役割・責任
② 利用・加工に関する取扱者の限定
③ 利用・加工の対象となる個人データの限定
④ 利用・加工時の照合及び確認手続き
⑤ 利用・加工の規程外作業に関する申請及び承認手続き
⑥ 機器・記録媒体等の管理手続き
⑦ 個人データへのアクセス制御
⑧ 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
⑨ 利用・加工状況の記録及び分析

（注）金融分野における個人情報取扱事業者は、利用・加工段階における取扱規程について、「個人データへのアクセス制御」として、次に掲げる事項を定めることが望ましい。
① 入館（室）者による不正行為の防止のための、業務実施場所及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
② 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又はモニタリングの実施
（例）記録機能を持つ媒体の持込み・持出し禁止又は検査の実施
③ 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、業務上の必要性に基づく限定
（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及び機器の更新への対応

６－２－１－１　「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」は、次に掲げる事項を含まなければならない。
① 個人データの管理区域外への持ち出しに関する取扱者の役割・責任
② 個人データ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
③ 個人データの管理区域外への持ち出しの対象となる個人データの必要最小限の限定
④ 個人データの管理区域外への持ち出し時の照合及び確認手続き
⑤ 個人データの管理区域外への持ち出しに関する申請及び承認手続き
⑥ 機器・記録媒体等の管理手続き
⑦ 個人データの管理区域外への持ち出し状況の記録及び分析

６－２－２　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、次に掲げる事項を含まなければならない。
① 個人データの利用者の識別及び認証
② 個人データの管理区分の設定及びアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データの漏えい・毀損等防止策
⑤ 個人データへのアクセス記録及び分析
⑥ 個人データを取り扱う情報システムの稼動状況の記録及び分析

（保管・保存段階における取扱規程）
６－３　金融分野における個人情報取扱事業者は、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及び技術的安全管理措置を定めなければならない。

６－３－１　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、次に掲げる事項を含まなければならない。
① 保管・保存に関する取扱者の役割・責任

② 保管・保存に関する取扱者の限定
③ 保管・保存の対象となる個人データの限定
④ 保管・保存の規程外作業に関する申請及び承認手続き
⑤ 機器・記録媒体等の管理手続き
⑥ 個人データへのアクセス制御
⑦ 保管・保存状況の記録及び分析
⑧ 保管・保存に関する障害発生時の対応・復旧手続き

（注）金融分野における個人情報取扱事業者は、保管・保存段階における取扱規程について、「個人データへのアクセス制御」として、次に掲げる事項を定めることが望ましい。

① 入館（室）者による不正行為の防止のための、業務実施場所及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

② 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又はモニタリングの実施
（例）記録機能を持つ媒体の持込み・持出し禁止又は検査の実施

③ 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、業務上の必要性に基づく限定
（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及び機器の更新への対応

６－３－２ 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、次に掲げる事項を含まなければならない。
① 個人データの利用者の識別及び認証
② 個人データの管理区分の設定及びアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データの漏えい・毀損等防止策
⑤ 個人データへのアクセス記録及び分析
⑥ 個人データを取り扱う情報システムの稼動状況の記録及び分析

（移送・送信段階における取扱規程）

６－４ 金融分野における個人情報取扱事業者は、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及び技術的安全管理措置を定めなければならない。

６－４－１ 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、次に掲げる事項を含まなければならない。
① 移送・送信に関する取扱者の役割・責任
② 移送・送信に関する取扱者の限定
③ 移送・送信の対象となる個人データの限定
④ 移送・送信時の照合及び確認手続き
⑤ 移送・送信の規程外作業に関する申請及び承認手続き
⑥ 個人データへのアクセス制御
⑦ 移送・送信状況の記録及び分析
⑧ 移送・送信に関する障害発生時の対応・復旧手続き

６－４－２ 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、次に掲げる事項を含まなければならない。
① 個人データの利用者の識別及び認証
② 個人データの管理区分の設定及びアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データの漏えい・毀損等防止策

⑤　個人データへのアクセス記録及び分析

（消去・廃棄段階における取扱規程）

６－５　金融分野における個人情報取扱事業者は、消去・廃棄段階における取扱規程において、次に掲げる事項を定めなければならない。

①　消去・廃棄に関する取扱者の役割・責任
②　消去・廃棄に関する取扱者の限定
③　消去・廃棄時の照合及び確認手続き
④　消去・廃棄の規程外作業に関する申請及び承認手続き
⑤　機器・記録媒体等の管理手続き
⑥　個人データへのアクセス制御
⑦　消去・廃棄状況の記録及び分析

（漏えい事案等への対応の段階における取扱規程）

６－６　金融分野における個人情報取扱事業者は、漏えい事案等への対応の段階における取扱規程において、次に掲げる事項を定めなければならない。

①　対応部署の役割・責任
②　漏えい事案等への対応に関する取扱者の限定
③　漏えい事案等への対応の規程外作業に関する申請及び承認手続き
④　漏えい事案等の影響・原因等に関する調査手続き
⑤　再発防止策・事後対策の検討に関する手続き
⑥　自社内外への報告に関する手続き
⑦　漏えい事案等への対応状況の記録及び分析

６－６－１　自社内外への報告に関する手続きは、次に掲げる事項を含まなければならない。

①　監督当局等への報告
②　本人への通知等
③　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事案等の事実関係及び再発防止策等の早急な公表

（別添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第６条に定める「機微（センシティブ）情報」（生体認証情報を含む）の取り扱いについて

金融分野における個人情報取扱事業者は、ガイドライン第６条に基づき、機微（センシティブ）情報について、同条第１項各号に掲げられた場合を除き、取得、利用又は第三者提供を行わず、同条第２項に基づき、同条第１項各号の事由を逸脱した取得、利用又は第三者提供を行うことのないよう、本実務指針Ⅰ～Ⅲに規定する措置に加えて、７－１、７－１－１、７－１－２、７－１－３、７－１－４、７－１－５及び７－２に規定する措置を実施することとする。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）の取り扱いについては、別添２に規定する全ての措置を実施しなければならない。

７－１　金融分野における個人情報取扱事業者は、１－２に規定する「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）情報の取り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うこととする。

７－１－１　金融分野における個人情報取扱事業者は、６－１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）情報の取り扱いについては、６－１に規定する事項に加えて、次に掲げる事項を定めることとする。
①　ガイドライン第６条第１項各号に定める場合のみによる取得
②　取得・入力を行う取扱者の必要最小限の限定
③　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

７－１－１－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、取得・入力段階における取扱規程において、７－１－１に規定する事項に加えて、次に掲げる事項を含まなければならない。
①　なりすましによる登録の防止策
②　本人確認に必要な最小限の生体認証情報のみの取得
③　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

７－１－２　金融分野における個人情報取扱事業者は、６－２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）情報の取り扱いについては、６－２－１、６－２－１－１及び６－２－２に規定する事項に加えて、次に掲げる事項を定めることとする。
①　ガイドライン第６条第１項各号に定める目的のみによる利用・加工
②　利用・加工を行う取扱者の必要最小限の限定
③　利用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
④　必要最小限の者に限定したアクセス権限の設定及びアクセス制御の実施

７－１－２－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、利用段階における取扱規程において、７－１－２に規定する事項に加えて、次に掲げる事項を含まなければならない。
①　偽造された生体認証情報による不正認証の防止措置
②　登録された生体認証情報の不正利用の防止措置
③　残存する生体認証情報の消去
④　認証精度設定等の適切性の確認
⑤　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き

７－１－３　金融分野における個人情報取扱事業者は、６－３に規定する保管・保存における取扱規程において、機微（センシティブ）情報の取り扱いについては、６－３－１及び６－３－２に規定する事項に加えて、次に掲げる事項を定めることとする。

①　保管・保存を行う取扱者の必要最小限の限定

②　必要最小限の者に限定したアクセス権限の設定及びアクセス制御の実施

７－１－３－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、保存段階における取扱規程において、７－１－３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むこととする。

７－１－４　金融分野における個人情報取扱事業者は、６－４に規定する移送・送信における取扱規程において、機微（センシティブ）情報の取り扱いについては、６－４－１及び６－４－２に規定する事項に加えて、次に掲げる事項を定めることとする。

①　ガイドライン第６条第１項各号に定める目的のみによる移送・送信

②　必要最小限の者に限定したアクセス権限の設定及びアクセス制御の実施

７－１－５　金融分野における個人情報取扱事業者は、６－５に規定する廃棄・消去における取扱規程において、機微（センシティブ）情報の取り扱いについては、６－５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ることとする。

７－１－５－１　機微（センシティブ）情報に該当する生体認証情報の取り扱いは、消去段階における取扱規程において、７－１－５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。

７－２　金融分野における個人情報取扱事業者は、２－５－２に規定する監査の実施に当たっては、機微（センシティブ）情報に該当する生体認証情報の取り扱いに関し、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）情報の取り扱いについても外部監査を行うこととする。

（別添３）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３条第３項に規定する個人信用情報機関における会員管理について

個人信用情報機関は、その会員が適正に個人信用情報（信用情報機関に登録される資金需要者の返済能力に関する情報。以下同じ）を登録・照会し、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を確保するため、本実務指針Ⅰ(2)に規定する措置に加え、８－１から８－４までの措置を講ずることとする。

（資格審査）

８－１　個人信用情報機関は、入会申込時においては、適正な事業者のみが会員となるよう、あらかじめ定めた入会基準に基づき、厳正に入会審査を行うこととする。

（モニタリング）

８－２　個人信用情報機関は、入会後においては、会員が入会基準を逸脱し、また返済能力の調査以外の目的のために個人信用情報を使用しないよう、会員による個人信用情報へのアクセスに対する適切かつ継続的なモニタリングを行うこととする。

（不適正使用に対する処分）

８－３　個人信用情報機関は、個人信用情報の不適正な使用があった場合、あらかじめ定めた会員管理に関する規程に基づき、利用停止、退会その他の処分を実施するとともに再発防止策を講じることとする。

（外部監査）

８－４　個人信用情報機関は、個人信用情報機関におけるガイドライン及び本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、外部監査を受けることとする。