（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、金融分野ガイドライン第８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