② 委託者の監督・監査・報告徴収に関する権限、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、再委託に関する条件及び漏えい等が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的に監査を行う等により、定期的又は随時に当該委託契約に定める安全管理措置等の遵守状況を確認し、当該安全管理措置を見直さなければならない。

なお、委託契約に定める安全管理措置等の遵守状況については、個人データ管理責任者等が、当該安全管理措置等の見直しを検討することを含め、適切に評価することが望ましい。

委託先が再委託を行おうとする場合は、委託元は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先に事前報告又は承認手続きを求める、直接又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、再委託先が法第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が望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。

（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一部改正）

第二条 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一部を次のように改正する。

２－１を次のように改める。

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。

㈱　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。

２－５－２を次のように改める。

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。

㈱　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。

４－５中「を記録する」を「や操作を記録する」に改め、「ならない」の次に「。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」を加える。

４－７中「及び個人データへのアクセス状況」を「、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」に改め、「ともに」の次に「、監視システムの動作の定期的な確認等」を、「ならない」の次に「。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」を加える。

５－３を次のように改める。

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

㈱

・　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中「基づき」の次に「、定期的に監査を行う等により」を加え、「委託契約上の安全管理措置」を「委託契約上の安全管理措置等」に改める。

６－１を次のように改める。

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

㈱　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