改　正　案	現　行
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 ⑴　（略） ⑵　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。 ①～⑥　（略） （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。	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 ⑴　（略） ⑵　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。 ①～⑥　（略） （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。

２－１－１・２－１－２　（略）	２－１－１・２－１－２　（略）
２－２～２－４　（略）	２－２～２－４　（略）
（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　（略）	（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　（略）
２－５－１　（略）	２－５－１　（略）
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。	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。
２－６・２－６－１　（略）	２－６・２－６－１　（略）
２）　（略）	２）　（略）

３）実施体制の整備に関する技術的安全管理措置	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。 ①～⑦　（略）	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。 ①～⑦　（略）
４－１～４－４－２　（略）	４－１～４－４－２　（略）
（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<u>や操作を記録する</u>とともに、当該記録の分析・保存を行わなければならない<u>。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</u>。	（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<u>を記録する</u>とともに、当該記録の分析・保存を行わなければならない。
４－６　（略）	４－６　（略）
（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<u>、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</u>を４－５及び４－６により監視するとともに<u>、監視システムの動作の定期的な確認等</u>、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<u>。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</u>。	（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<u>及び個人データへのアクセス状況</u>を４－５及び４－６により監視するとともに、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。
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	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	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。	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。
５－１～５－２（略）	５－１～５－２（略）
（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。	（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
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。	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、定期的又は随時に委託先における委託契約上の安全管理措置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⑵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

（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⑵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

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　（略）	（利用・加工段階における取扱規程） ６－２　（略）
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	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

（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・６－２－２　（略）	６－２－１－１・６－２－２　（略）
（保管・保存段階における取扱規程） ６－３　（略）	（保管・保存段階における取扱規程） ６－３　（略）
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	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

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　（略）	６－３－２　（略）
６－４～６－６－１　（略）	６－４～６－６－１　（略）