（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、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「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９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、金融分野ガイドライン第９条に基づき、「Ⅰ．⑵２）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。