６－６－１　自社内外への報告に関する手続は、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５条に定める「機微（センシティブ）情報」（生体認証情報を含む。）の取扱いについて

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５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　金融分野ガイドライン第５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　金融分野ガイドライン第５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

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扱いは、保管・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　金融分野ガイドライン第５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に規定する消去・廃棄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扱いは、消去・廃棄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２条第４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．⑵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ずることとする。

（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金融分野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。