⑴　組織的安全管理措置
　イ　個人データの管理責任者等の設置
　ロ　就業規則等における安全管理措置の整備
　ハ　個人データの安全管理に係る取扱規程に従った運用
　ニ　個人データの取扱状況を確認できる手段の整備
　ホ　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
　ヘ　漏えい事案等に対応する体制の整備
⑵　人的安全管理措置
　イ　役職員との個人データの非開示契約等の締結
　ロ　役職員の役割・責任等の明確化
　ハ　役職員への安全管理措置の周知徹底、教育及び訓練
　ニ　役職員による個人データ管理手続きの遵守状況の確認
⑶　技術的安全管理措置
　イ　個人データの利用者の識別及び認証
　ロ　個人データの管理区分の設定及びアクセス制御
　ハ　個人データへのアクセス権限の管理
　ニ　個人データの漏えい・き損等防止策
　ホ　個人データへのアクセスの記録及び分析
　ヘ　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
　ト　個人データを取り扱う情報システムの監視及び監査

（参照条文：保護法20条、金融分野ガイドライン10条）

（役職員の監督）

第12条　協会員は、その役職員に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、適切な内部管理体制を構築し、その役職員に対する必要かつ適切な監督を行わなければならない。

2　協会員は、前項の役職員に対する「必要かつ適切な監督」を以下の体制整備等により行うこととする。

⑴　役職員が、在職中及びその職を退いた後において、当該協会員の業務等に関して知り得た個人データを第三者に知らせ、又は利用目的外に使用しないことを内容とする契約等を採用時等に締結すること

⑵　個人データの適正な取扱いのための取扱規程の策定を通じた役職員の役割・責任の明確化及び役職員への安全管理義務の周知徹底、教育及び訓練を行うこと

⑶　役職員による個人データの持出し等を防ぐため、社内での安全管理措置に定めた事項の遵守状況等の確認及び役職員における個人データの保護に対する点検及び監査制度を整備すること

（解説）
・　役職員の定義については、第11条参照

（参照条文：保護法21条、金融分野ガイドライン11条）

（委託先の監督）

第13条　協会員は、個人データの取扱いの全部又は一部を委託（契約の形態や種類を問わず、協会員が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。）する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

なお、当該監督は、個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じたものとする。

2　協会員は、個人データを適正に取り扱っていると認められる者を選定し委託するとともに、取扱いを委託した個人データの安全管理措置が図られるよう、個人データの安全管理のための措置を委託先においても確保しなければならない（二段階以上の委託が行われた場合には、委託先の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行うものとする。）。

具体的には、以下の対応等が必要である。

⑴　個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準に従って委託先を選定するとともに、当該基準を定期的に見直すこと。

⑵　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、定期的又は随時に当該委託契約に定める安全管理措置の遵守状況を確認し、当該安全管理措置の見直しを行わなければならない。

（解説）
・　委託先には外国の委託先も含まれる。

（参照条文：保護法22条、金融分野ガイドライン12条）

（第三者提供の制限）

第14条　協会員は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ることなく、個人データを第三者（個人データを提供しようとする協会員及び当該個人データに係る本人のいずれに該当しないものをいい、自然人、法人その他の団体を問わない。以下同じ。）に提供してはならない。

⑴　法令に基づく場合
⑵　人の生命、身体又は財産（法人の財産を含む。）の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき
⑶　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき
⑷　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき

2　協会員は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項にかかわらず、当該個人データを第三者に提供することができる。

⑴　第三者への提供を利用目的とすること
⑵　第三者に提供される個人データの項目
⑶　第三者への提供の手段又は方法
⑷　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること

3　協会員は、前項第２号又は第３号に掲げる事項を変更する場合は、変更する内容について、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置くものとする。

4　次に掲げる場合において、当該個人データの提供を受ける者は、第三者に該当しない。

⑴　協会員が、利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合
⑵　合併その他の事由による事業の承継に伴って個人データが提供される場合
⑶　個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者（共同して利用する者において、第一次的に苦情を受け付け、その処理を行うとともに、開示、訂正等及び利用停止等の決定を行い、安全管理に責任を有する者をいう。第６項において「管理責任者」という。）の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき

5　協会員が前項第３号の規定により行う通知は、原則として書面によることとする。協会員による「共同して利用する者の範囲」の通知等については、共同利用者を個別列挙するよう努めなければならない。

6　協会員は、第４項第３号に規定する利用者の利用目的又は管理責任者の氏名又は名称を変更する場合は、変更する内容について、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

（解説）
⑴　個人データを提供する場合の留意事項

協会員が取得した個人データを第三者に提供する場合には、あらかじめ本人の同意を得ることが必要となるが、本人の同意を得ることなく個人データを提供しようとするときは、次のいずれかに該当するかどうかを確認し必要な対応をとる。

①　法令に基づく場合等の適用除外の場合（第１項第１号～第４号）
②　オプトアウトによる場合（第２項）
③　委託の場合（第４項第１号）
④　合併等の事業承継の場合（第４項第２号）