（安全管理措置）

第12条　協会員は、その取り扱う個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備及び安全管理措置に係る実施体制の整備等の必要かつ適切な措置を講じなければならない。必要かつ適切な措置は、個人データの取得・利用・保管等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、「技術的安全管理措置」及び「外的環境の把握」を含むものでなければならない。

なお、当該措置は、個人データが漏えい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、個人データの取扱状況及び個人データを記録した媒体の性質等に起因するリスクに応じたものとする。

例えば、不特定多数者が書店で随時に購入可能な名簿で、協会員において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書細断機等による処理を行わずに廃棄し、又は廃品回収に出したとしても、協会員の安全管理措置の義務違反にはならない。

なお、保護法第23条における「その他の個人データの安全管理のために必要かつ適切な措置」には、協会員が取得し、又は取得しようとしている個人情報であって、当該協会員が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる。そのため、以下この条における「個人データ」には、当該個人情報も含まれることに留意する。

本条における用語の定義は、次のとおりである。

⑴　組織的安全管理措置

個人データの安全管理措置について役職員（協会員の組織内にあって、直接又は間接に協会員の指揮監督を受けて協会員の業務に従事する者等をいい、雇用関係にある従業者（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、協会員との間の雇用関係にない者（取締役、執行役、監査役、派遣社員等）も含まれる。以下同じ。）の責任と権限を明確に定め、安全管理に関する規程等を整備・運用し、その実施状況の点検・監査を行うこと等の協会員の体制整備及び実施措置をいう。

⑵　人的安全管理措置

役職員との個人データの非開示契約等の締結及び役職員に対する教育・訓練等を実施し、個人データの安全管理が図られるよう役職員を監督することをいう。

⑶　物理的安全管理措置

個人データを取り扱う区域の管理、機器及び電子媒体等の盗難の防止、電子媒体等を持ち運ぶ場合の漏えい等の防止並びに機器及び電子媒体等の廃棄等の個人データの安全管理に関する物理的な措置をいう。

⑷　技術的安全管理措置

個人データ及びそれを取り扱う情報システムへのアクセス制御及び情報システムの監視等の個人データの安全管理に関する技術的な措置をいう。

⑸　外的環境の把握

外国において個人データを取り扱う場合に、当該外国の個人情報の保護に関する制度等を把握することをいう。協会員は、外国において個人データを取り扱う場合には、外的環境を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じなければならない。

2　協会員は、個人データの安全管理に係る基本方針・取扱規程等の整備として、以下の「組織的安全管理措置」を講じなければならない。

⑴　規程等の整備

イ　個人データの安全管理に係る基本方針の整備
ロ　個人データの安全管理に係る取扱規程の整備
ハ　個人データの取扱状況の点検及び監査に係る規程の整備
ニ　外部委託に係る規程の整備

⑵　各管理段階における安全管理に係る取扱規程

イ　取得・入力段階における取扱規程
ロ　利用・加工段階における取扱規程
ハ　保管・保存段階における取扱規程
ニ　移送・送信段階における取扱規程
ホ　消去・廃棄段階における取扱規程
ヘ　漏えい等事案（漏えい等又はそのおそれのある事案をいう。以下同じ。）への対応の段階における取扱規程

3　協会員は、個人データの安全管理に係る実施体制の整備として、以下の「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」及び「技術的安全管理措置」を講じなければならない。

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　漏えい等事案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　物理的安全管理措置

イ　個人データの取扱区域等の管理
ロ　機器及び電子媒体等の盗難等の防止
ハ　電子媒体等を持ち運ぶ場合の漏えい等の防止
ニ　個人データの削除及び機器、電子媒体等の廃棄

⑷　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働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

（解説）
・　漏えい、滅失及び毀損の定義については、第15条参照
（参照条文：保護法23条、通則ガイドライン３－４－２、金融分野ガイドライン８条）