（役職員の監督）

第13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係る取扱規程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取扱状況の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12条参照
（参照条文：保護法24条、通則ガイドライン３－４－３、金融分野ガイドライン９条）

（委託先の監督）

第14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、取扱いを委託する個人データの安全管理が図られるよう、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、委託先における漏えい等の防止及び目的外利用の禁止、再委託に関する条件並びに漏えい等事案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等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25条、通則ガイドライン３－４－４、金融分野ガイドライン10条）

（漏えい等の報告等）

第15条　協会員は、その取り扱う個人データの漏えい等その他の個人データの安全の確保に係る事態であって個人の権利利益を害するおそれが大きいものとして次の各号のいずれかに該当するものが生じたときは、次項以下の定めに従って、当該事態が生じた旨を個人情報保護委員会（保護法第150条の規定により金融庁長官等が報告を受理する権限の委任を受けている場合にあっては金融庁長官等、保護法第170条の規定により地方公共団体の長等が報告を受理する権限に属する事務を行う場合にあっては地方公共団体の長等。第11項において同じ。）に報告しなければならない。ただし、協会員が、他の個人情報取扱事業者から当該個人データの取扱いの全部又は一部の委託を受けた場合であって、当該事態が生じた旨を当該他の個人情報取扱事業者に通知したときは、この限りでない。

⑴　要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下第１項各号及び次項において同じ。）の漏えい等が発生し、又は発生したおそれがある事態

⑵　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

⑶　不正の目的をもって行われたおそれがある当該協会員に対する行為による個人データ（当該協会員が取得し、又は取得しようとしている個人情報であって、個人データとして取り扱われることが予定されているものを含む。）の漏えい等が発生し、又は発生したおそれがある事態

⑷　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

2　前項の規定による報告をする場合には、前項各号に定める事態を知った後、速やかに、当該事態に関する次の各号の事項（報告をしようとする時点において把握しているものに限る。第５項において同じ。）を報告しなければならない（この時点での報告を「速報」という。以下同じ。）。

⑴　概要

⑵　漏えい等が発生し、又は発生したおそれがある個人データ（前項第⑶号に定める事態については、同号に規定する個人情報を含む。次号において同じ。）の項目

⑶　漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数

⑷　原因

⑸　二次被害又はそのおそれの有無及びその内容

⑹　本人への対応の実施状況

⑺　公表の実施状況

⑻　再発防止のための措置

⑼　その他参考となる事項

3　前項の場合において、協会員は、当該事態を知った日から30日以内（当該事態が第１項第⑶号に定めるものである場合にあっては、60日以内）に、当該事態に関する前項各号に定める事項を報告しなければならない（この時点での報告を「確報」という。以下同じ。）。

4　第１項による報告は、次の各号に掲げる場合の区分に応じ、それぞれ当該各号に定める方法により行うものとする。

⑴　個人情報保護委員会に報告する場合
施行規則第８条第３項第１号に定める報告書を提出する方法

⑵　保護法第150条第１項の規定により、第１項の規定による権限の委任を受けた事業所管大臣に報告する場合
施行規則第８条第３項第２号に定める報告書を提出する方法

5　協会員は、第１項ただし書の規定による通知をする場合には、同項各号に定める事態を知った後、速やかに、第２項各号に定める事項を通知しなければならない。

6　協会員は、その取り扱う個人である資金需要者等に関する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、関係法令に従って、監督当局に報告しなければならない。

7　協会員は、次の各号のいずれかの事態（第１項及び前項に規定する事態を除く。）を知ったときは、第１項及び前項の規定に準じて、監督当局に報告することとする。

⑴　その取り扱う個人情報の漏えい等が発生し、又は発生したおそれがある事態

⑵　その取り扱う仮名加工情報に係る削除情報等（保護法第41条第１項の規定により行われた加工の方法に関する情報にあっては、その情報を用いて仮名加工情報の作成に用いられた個人情報を復元することができるものに限る。第９項において同じ。）又は匿名加工情報に係る加工方法等情報の漏えいが発生し、又は発生したおそれがある事態