Ⅲ．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10条に定める「委託先の監督」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10条第３項に基づき、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、個人データの取扱いを委託するとともに、委託先における当該個人データに対する安全管理措置の実施を確保しなければならない。

（個人データ保護に関する委託先選定の基準）

５－１　金融分野における個人情報取扱事業者は、個人データの取扱いを委託する場合には、金融分野ガイドライン第10条第３項①に基づき、次に掲げる事項を委託先選定の基準として定め、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さなければならない。

①　委託先における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
②　委託先における個人データの安全管理に係る実施体制の整備
③　実績等に基づく委託先の個人データ安全管理上の信用度
④　委託先の経営の健全性

５－１－１　委託先選定の基準においては、「委託先における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、次に掲げる事項を定めなければならない。

①　委託先における個人データの安全管理に係る基本方針の整備
②　委託先における個人データの安全管理に係る取扱規程の整備
③　委託先における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
④　委託先における外部委託に係る規程の整備

５－１－２　委託先選定の基準においては、「委託先における個人データの安全管理に係る実施体制の整備」として、Ⅰ．⑵１）の組織的安全管理措置、同２）の人的安全管理措置及び同３）の技術的安全管理措置に記載された事項を定めるとともに、委託先から再委託する場合の再委託先の個人データの安全管理に係る実施体制の整備状況に係る基準を定めなければならない。

５－２　金融分野における個人情報取扱事業者は、５－３に基づき、委託契約後に委託先選定の基準に定める事項の委託先における遵守状況を定期的又は随時に確認するとともに、委託先が当該基準を満たしていない場合には、委託先が当該基準を満たすよう監督しなければならない。

（委託契約において盛り込むべき安全管理に関する内容）

５－３　金融分野における個人情報取扱事業者は、委託契約において、次に掲げる安全管理に関する事項を盛り込まなければならない。

①　委託者の監督・監査・報告徴収に関する権限
②　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
③　再委託における条件
④　漏えい事案等が発生した際の委託先の責任

㈱

・金融分野における個人情報取扱事業者は、「再委託における条件」として、再委託の可否及び再委託を行うに当たっての委託元への文書による事前報告又は承認等を、委託契約に盛り込むことが望ましい。
・金融分野における個人情報取扱事業者は、委託先において個人データを取り扱う者の氏名・役職又は部署名を、委託契約に盛り込むことが望ましい。

５－４　金融分野における個人情報取扱事業者は、５－３に基づき、定期的に監査を行う等により、定期的又は随時に委託先における委託契約上の安全管理措置等の遵守状況を確認するとともに、当該契約内容が遵守されていない場合には、委託先が当該契約内容を遵守するよう監督しなければならない。また、金融分野における個人情報取扱事業者は、定期的に委託契約に盛り込む安全管理措置を見直さなければならない。

（別添１）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８条第５項⑵に定める各管理段階における安全管理に係る取扱規程について

金融分野における個人情報取扱事業者は、１－２に基づき、各管理段階ごとの安全管理に係る取扱規程において、６－１から６－６－１までの事項を定めなければならない。

（取得・入力段階における取扱規程）

６－１　金融分野における個人情報取扱事業者は、取得・入力段階における取扱規程において、次に掲げる事項を定めなければならない。

①　取得・入力に関する取扱者の役割・責任
②　取得・入力に関する取扱者の限定
③　取得・入力の対象となる個人データの限定
④　取得・入力時の照合及び確認手続
⑤　取得・入力の規程外作業に関する申請及び承認手続
⑥　機器・記録媒体等の管理手続
⑦　個人データへのアクセス制御
⑧　取得・入力状況の記録及び分析

㈱　金融分野における個人情報取扱事業者は、取得・入力段階における取扱規程について、「個人データへのアクセス制御」として、次に掲げる事項を定めることが望ましい。

①　入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館（室）管理の実施
（例）入退館（室）の記録の保存
②　盗難等の防止のための措置
（例）カメラによる撮影や作業への立会い等による記録又はモニタリングの実施
（例）記録機能を持つ媒体の持込み・持出し禁止又は検査の実施
③　不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性に基づく限定
（例）スマートフォン、パソコン等の記録機能を有する機器の接続の制限及び機器の更新への対応

（利用・加工段階における取扱規程）

６－２　金融分野における個人情報取扱事業者は、利用・加工段階における取扱規程において、組織的安全管理措置及び技術的安全管理措置を定めなければならない。

６－２－１　利用・加工段階における取扱規程に関する組織的安全管理措置は、次に掲げる事項を含まなければならない。

①　利用・加工に関する取扱者の役割・責任
②　利用・加工に関する取扱者の限定
③　利用・加工の対象となる個人データの限定
④　利用・加工時の照合及び確認手続
⑤　利用・加工の規程外作業に関する申請及び承認手続
⑥　機器・記録媒体等の管理手続
⑦　個人データへのアクセス制御
⑧　個人データの管理区域外への持出しに関する上乗せ措置
⑨　利用・加工状況の記録及び分析

㈱　金融分野における個人情報取扱事業者は、利用・加工段階における取扱規程について、「個人データへのアクセス制御」として、次に掲げる事項を定めることが望ましい。

①　入館（室）者による不正行為の防止のための、業務実施場所及び情報システム等の設置場所の入退館（室）管理の実施
（例）入退館（室）の記録の保存
②　盗難等の防止のための措置
（例）カメラによる撮影や作業への立会い等による記録又はモニタリングの実施
（例）記録機能を持つ媒体の持込み・持出し禁止又は検査の実施
③　不正な操作を防ぐための、個人データを取り扱う端末に付与する機能の、業務上の必要性に基づく限定
（例）スマートフォン、パソコン等の記録機能を有する機器の接続の制限及び機器の更新への対応