**資料3－3**

○　金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（平成29年個人情報保護委員会・金融庁告示第２号）の一部を改正する告示案

次の表により、改正前欄に掲げる規定の傍線を付し又は破線で囲んだ部分をこれに順次対応する改正後欄に掲げる規定の傍線を付し又は破線で囲んだ部分のように改め、改正前欄及び改正後欄に対応して掲げるその標記部分（連続する他の規定と記号により一括して掲げる規定にあっては、その標記部分に係る記載）に二重傍線を付した規定（以下「対象規定」という。）は、その標記部分が異なるものは改正前欄に掲げる対象規定を改正後欄に掲げる対象規定として移動し、改正前欄に掲げる対象規定で改正後欄にこれに対応するものを掲げていないものは、これを削り、改正後欄に掲げる対象規定で改正前欄にこれに対応するものを掲げていないものは、これを加える。

| 改　正　後 | 改　正　前 |
|---|---|
| 目次 | 目次 |
| Ⅰ．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条に定める安全管理措置の実施について | Ⅰ．　［同左］ |
| ⑴　［略］ | ⑴　［同左］ |
| ⑵　個人データの安全管理措置に係る実施体制の整備 | ⑵　［同左］ |
| １）実施体制の整備に関する組織的安全管理措置 | １）　［同左］ |
| ［２－１～２－５　略］ | ［２－１～２－５　同左］ |
| ２－６　漏えい等事案に対応する体制の整備 | ２－６　漏えい事案等に対応する体制の整備 |
| ２）実施体制の整備に関する人的安全管理措置 | ２）実施体制の整備に関する人的安全管理措置 |
| ３－１　従業者との個人データの非開示契約等の締結 | ３－１　従業者との個人データの非開示契約等の締結 |
| ３－２　従業者の役割・責任等の明確化 | ３－２　従業者の役割・責任等の明確化 |
| ３－３　従業者への安全管理措置の周知徹底、教育及び訓練 | ３－３　従業者への安全管理措置の周知徹底、教育及び訓練 |
| ３－４　従業者による個人データ管理手続の遵守状況の確認 | ３－４　従業者による個人データ管理手続の遵守状況の確認 |

| | |
|---|---|
| ３）実施体制の整備に関する物理的安全管理措置<br>４－１　個人データの取扱区域等の管理<br>４－２　機器及び電子媒体等の盗難等の防止<br>４－３　電子媒体等を持ち運ぶ場合の漏えい等の防止<br>４－４　個人データの削除及び機器、電子媒体等の廃棄 | |
| ４）実施体制の整備に関する技術的安全管理措置 | ３）実施体制の整備に関する技術的安全管理措置 |
| ５－１　個人データの利用者の識別及び認証 | ４－１　個人データの利用者の識別及び認証 |
| ５－２　個人データの管理区分の設定及びアクセス制御 | ４－２　個人データの管理区分の設定及びアクセス制御 |
| ５－３　個人データへのアクセス権限の管理 | ４－３　個人データへのアクセス権限の管理 |
| ５－４　個人データの漏えい等防止策 | ４－４　個人データの漏えい・毀損等防止策 |
| ５－５　個人データへのアクセスの記録及び分析 | ４－５　個人データへのアクセスの記録及び分析 |
| ５－６　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 | ４－６　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 |
| ５－７　個人データを取り扱う情報システムの監視及び監査 | ４－７　個人データを取り扱う情報システムの監視及び監査 |
| Ⅱ．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９条に定める「従業者の監督」 について | Ⅱ．　［同左］ |
| 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 | Ⅲ．　［同左］ |
| ６－１・６－２　個人データ保護に関する委託先選定の基準 | ５－１・５－２　個人データ保護に関する委託先選定の基準 |
| ６－３・６－４　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・５－４　委託契約において盛り込むべき安全管理に関する内容 |
| （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７項⑵に定める各管理段階における安全管理に係る取扱 | （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 | 規程について |
| ７－１　取得・入力段階における取扱規程 | ６－１　取得・入力段階における取扱規程 |
| ７－２　利用・加工段階における取扱規程 | ６－２　利用・加工段階における取扱規程 |
| ７－３　保管・保存段階における取扱規程 | ６－３　保管・保存段階における取扱規程 |
| ７－４　移送・送信段階における取扱規程 | ６－４　移送・送信段階における取扱規程 |
| ７－５　消去・廃棄段階における取扱規程 | ６－５　消去・廃棄段階における取扱規程 |
| ７－６　漏えい等事案への対応の段階における取扱規程 | ６－６　漏えい事案等への対応の段階における取扱規程 |
| （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 | （別添２）　［同左］ |
| ８－１・８－２ | ７－１・７－２ |
| （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 | （別添３）　［同左］ |
| ９－１　資格審査 | ８－１　資格審査 |
| ９－２　モニタリング | ８－２　モニタリング |
| ９－３　不適正使用に対する処分 | ８－３　不適正使用に対する処分 |
| ９－４　外部監査 | ８－４　外部監査 |
| Ⅰ．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条に定める安全管理措置の実施について | Ⅰ．　［同左］ |
| ⑴　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 | ⑴　［同左］ |
| （個人データの安全管理に係る基本方針の整備） | （個人データの安全管理に係る基本方針の整備） |
| １－１　金融分野における個人情報保護に関するガイドライン（ | １－１　金融分野における個人情報保護に関するガイドライン（ |

| | |
|---|---|
| 平成29年個人情報保護委員会・金融庁告示第１号。以下「金融分野ガイドライン」という。）第１条第１項に規定する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８条第７項⑴①に基づき、次に掲げる事項を定めた個人データの安全管理に係る基本方針を策定し、当該基本方針を公表するとともに、必要に応じて基本方針の見直しを行わなければならない。 | 平成29年個人情報保護委員会・金融庁告示第１号。以下「金融分野ガイドライン」という。）第１条第１項に規定する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８条第５項⑴①に基づき、次に掲げる事項を定めた個人データの安全管理に係る基本方針を策定し、当該基本方針を公表するとともに、必要に応じて基本方針の見直しを行わなければならない。 |
| ［①～⑤　略］ | ［①～⑤　同左］ |
| （個人データの安全管理に係る取扱規程の整備） | （個人データの安全管理に係る取扱規程の整備） |
| １－２　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８条第７項⑴②に規定する「個人データの安全管理に係る取扱規程の整備」として、同項⑵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を整備し、各管理段階ごとに別添１に規定する事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。<br>　なお、全ての管理段階を同一人が取り扱う小規模事業者等においては、各管理段階ごとに取扱規程を定めることに代えて、全管理段階を通じた安全管理に係る取扱規程において次に掲げる事項を定めることも認められる。 | １－２　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８条第５項⑴②に規定する「個人データの安全管理に係る取扱規程の整備」として、金融分野ガイドライン第８条第５項⑵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を整備し、各管理段階ごとに別添１に規定する事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。<br>　なお、全ての管理段階を同一人が取り扱う小規模事業者等においては、各管理段階ごとに取扱規程を定めることに代えて、全管理段階を通じた安全管理に係る取扱規程において次に掲げる事項を定めることも認められる。 |
| ［①～③　略］ | ［①～③　同左］ |
| （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） | （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） |
| １－３　金融分野における個人情報取扱事業者は、金融分野ガイ | １－３　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８条第７項⑴③に基づき、個人データの取扱状況に関する点検及び監査の規程を整備し、次に掲げる事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。<br>　なお、個人データ取扱部署が単一である事業者においては、点検により監査を代替することも認められる。<br>［①～⑤　略］ | ドライン第８条第５項⑴③に基づき、個人データの取扱状況に関する点検及び監査の規程を整備し、次に掲げる事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。<br>　なお、個人データ取扱部署が単一である事業者においては、点検により監査を代替することも認められる。<br>［①～⑤　同左］ |
| （外部委託に係る規程の整備）<br>１－４　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８条第７項⑴④に基づき、外部委託に係る取扱規程を整備し、次に掲げる事項を定めるとともに、定期的に規程の見直しを行わなければならない。<br>［①・②　略］ | （外部委託に係る規程の整備）<br>１－４　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８条第５項⑴④に基づき、外部委託に係る取扱規程を整備し、次に掲げる事項を定めるとともに、定期的に規程の見直しを行わなければならない。<br>［①・②　同左］ |
| ⑵　個人データの安全管理措置に係る実施体制の整備<br>１）実施体制の整備に関する組織的安全管理措置<br>　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８条第８項に基づき、個人データの安全管理措置に係る実施体制の整備における「組織的安全管理措置」として、次に掲げる措置を講じなければならない。<br>［①～⑤　略］<br>⑥　漏えい等事案に対応する体制の整備 | ⑵　［同左］<br>１）実施体制の整備に関する組織的安全管理措置<br>　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８条第６項に基づき、個人データの安全管理措置に係る実施体制の整備における「組織的安全管理措置」として、次に掲げる措置を講じなければならない。<br>［①～⑤　同左］<br>⑥　漏えい事案等に対応する体制の整備 |
| ２－１－１　金融分野における個人情報取扱事業者は、２－１①に規定する個人データ管理責任者に、次に掲げる業務を所管さ | ２－１－１　金融分野における個人情報取扱事業者は、２－１①に規定する個人データ管理責任者に、次に掲げる業務を所管さ |

| | |
|---|---|
| せなければならない。 | せなければならない。 |
| ①　［略］ | ①　［同左］ |
| ②　個人データ管理者及び５－１に規定する「本人確認に関する情報」の管理者の任命 | ②　個人データ管理者及び４－１に規定する「本人確認に関する情報」の管理者の任命 |
| ［③～⑤　略］ | ［③～⑤　同左］ |
| （漏えい等事案に対応する体制の整備） | （漏えい事案等に対応する体制の整備） |
| ２－６　金融分野における個人情報取扱事業者は、「漏えい等事案に対応する体制の整備」として、次に掲げる体制を整備しなければならない。 | ２－６　金融分野における個人情報取扱事業者は、「漏えい事案等に対応する体制の整備」として、次に掲げる体制を整備しなければならない。 |
| ①　［略］ | ①　［同左］ |
| ②　漏えい等事案の影響・原因等に関する調査体制 | ②　漏えい事案等の影響・原因等に関する調査体制 |
| ［③・④　略］ | ［③・④　同左］ |
| ［削る。］ | ２－６－１　金融分野における個人情報取扱事業者は、１－２③又は６－６－１に基づき、自社内外への報告体制を整備するとともに、漏えい事案等が発生した場合には、次に掲げる事項を実施しなければならない。<br>①　監督当局等への報告<br>②　本人への通知等<br>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 |
| ２）実施体制の整備に関する人的安全管理措置<br>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 | ２）実施体制の整備に関する人的安全管理措置<br>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８条第８項に基づき、個人データの安全管理措置に係る実施体制の整備における「人的安全管理措置」として、次に掲げる措置を講じなければならない。<br>［①～④　略］ | イン第８条第６項に基づき、個人データの安全管理措置に係る実施体制の整備における「人的安全管理措置」として、次に掲げる措置を講じなければならない。<br>［①～④　同左］ |
| ３）実施体制の整備に関する物理的安全管理措置<br>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８条第８項に基づき、個人データの安全管理措置に係る実施体制の整備における「物理的安全管理措置」として、次に掲げる措置を講じなければならない。<br>①　個人データの取扱区域等の管理<br>②　機器及び電子媒体等の盗難等の防止<br>③　電子媒体等を持ち運ぶ場合の漏えい等の防止<br>④　個人データの削除及び機器、電子媒体等の廃棄<br>（個人データの取扱区域等の管理）<br>４－１　金融分野における個人情報取扱事業者は、「個人データの取扱区域等の管理」として、次に掲げる措置を講じなければならない。<br>①　個人データ等を取り扱う重要な情報システムの管理区域への入退室管理等<br>②　管理区域への持ち込み可能機器等の制限等<br>③　のぞき込み防止措置の実施等による権限を有しない者による閲覧等の防止 | ［加える。］ |

（機器及び電子媒体等の盗難等の防止）

４－２　金融分野における個人情報取扱事業者は、「機器及び電子媒体等の盗難等の防止」として、次に掲げる措置を講じなければならない。

①　個人データを取り扱う機器等の施錠等による保管

②　個人データを取り扱う情報システムを運用する機器の固定等

（電子媒体等を持ち運ぶ場合の漏えい等の防止）

４－３　金融分野における個人情報取扱事業者は、「電子媒体等を持ち運ぶ場合の漏えい等の防止」として、次に掲げる措置を講じなければならない。

①　持ち運ぶ個人データの暗号化、パスワードによる保護等

②　書類等の封緘、目隠しシールの貼付等

（個人データの削除及び機器、電子媒体等の廃棄）

４－４　金融分野における個人情報取扱事業者は、「個人データの削除及び機器、電子媒体等の廃棄」として、次に掲げる措置を講じなければならない。

①　容易に復元できない手段によるデータ削除

②　個人データが記載された書類等又は記録された機器等の物理的な破壊等

４）実施体制の整備に関する技術的安全管理措置

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８条第８項に基づき、個人データの安全管理措置に係る

３）実施体制の整備に関する技術的安全管理措置

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８条第６項に基づき、個人データの安全管理措置に係る

実施体制の整備における「技術的安全管理措置」として、次に掲げる措置を講じなければならない。

［①～③　略］

④　個人データの漏えい等防止策

［⑤～⑦　略］

５－１～５－３　［略］

（個人データの漏えい等防止策）

５－４　金融分野における個人情報取扱事業者は、「個人データの漏えい等防止策」として、個人データの保護策を講ずることとともに、障害発生時の技術的対応・復旧手続を整備しなければならない。

５－４－１　金融分野における個人情報取扱事業者は、「個人データの保護策を講ずること」として、次に掲げる措置を講じなければならない。

①　蓄積データの漏えい等防止策

②　伝送データの漏えい等防止策

③　［略］

５－４－２～５－６　［略］

（個人データを取り扱う情報システムの監視及び監査）

５－７　金融分野における個人情報取扱事業者は、「個人データを取り扱う情報システムの監視及び監査」として、個人データを取り扱う情報システムの利用状況、個人データへのアクセス状況及び情報システムへの外部からのアクセス状況を５－５及

実施体制の整備における「技術的安全管理措置」として、次に掲げる措置を講じなければならない。

［①～③　同左］

④　個人データの漏えい・毀損等防止策

［⑤～⑦　同左］

４－１～４－３　［同左］

（個人データの漏えい・毀損等防止策）

４－４　金融分野における個人情報取扱事業者は、「個人データの漏えい・毀損等防止策」として、個人データの保護策を講ずることとともに、障害発生時の技術的対応・復旧手続を整備しなければならない。

４－４－１　金融分野における個人情報取扱事業者は、「個人データの保護策を講ずること」として、次に掲げる措置を講じなければならない。

①　蓄積データの漏えい防止策

②　伝送データの漏えい防止策

③　［同左］

４－４－２～４－６　［同左］

（個人データを取り扱う情報システムの監視及び監査）

４－７　金融分野における個人情報取扱事業者は、「個人データを取り扱う情報システムの監視及び監査」として、個人データを取り扱う情報システムの利用状況、個人データへのアクセス状況及び情報システムへの外部からのアクセス状況を４－５及

| | |
|---|---|
| び５－６により監視するとともに、監視システムの動作の定期的な確認等、監視状況についての点検及び監査を行わなければならない。また、セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策を行わなければならない。 | び４－６により監視するとともに、監視システムの動作の定期的な確認等、監視状況についての点検及び監査を行わなければならない。また、セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策を行わなければならない。 |
| 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 | Ⅲ．　［同左］ |
| 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。 | ［同左］ |
| ６－１・６－１－１　［略］ | ５－１・５－１－１　［同左］ |
| ６－１－２　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、同３）の物理的安全管理措置、同４）の技術的安全管理措置及び金融分野ガイドライン第８条第６項の外的環境の把握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。 | ５－１－２　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。 |
| ６－２　金融分野における個人情報取扱事業者は、６－３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 | 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）

６－３　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。

［①～③　略］

④　漏えい等事案が発生した際の委託先の責任

（注）

・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手続等を、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。

６－４　金融分野における個人情報取扱事業者は、６－３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

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。

［①～③　同左］

④　漏えい事案等が発生した際の委託先の責任

（注）

・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７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、７－１から７－６－１までの事項を定めなければならない。

７－１～７－２－１－１　［略］

７－２－２　利用・加工段階における取扱規程に関する技術的安全管理措置は、次に掲げる事項を含まなければならない。

［①～③　略］

④　個人データの漏えい等防止策

［⑤・⑥　略］

７－３・７－３－１　［略］

７－３－２　保管・保存段階における取扱規程に関する技術的安全管理措置は、次に掲げる事項を含まなければならない。

［①～③　略］

④　個人データの漏えい等防止策

［⑤・⑥　略］

７－４・７－４－１　［略］

７－４－２　移送・送信段階における取扱規程に関する技術的安全管理措置は、次に掲げる事項を含まなければならない。

［①～③　略］

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。

６－１～６－２－１－１　［同左］

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

［①～③　同左］

④　個人データの漏えい・毀損等防止策

［⑤・⑥　同左］

６－３・６－３－１　［同左］

６－３－２　保管・保存段階における取扱規程に関する技術的安全管理措置は、次に掲げる事項を含まなければならない。

［①～③　同左］

④　個人データの漏えい・毀損等防止策

［⑤・⑥　同左］

６－４・６－４－１　［同左］

６－４－２　移送・送信段階における取扱規程に関する技術的安全管理措置は、次に掲げる事項を含まなければならない。

［①～③　同左］

| | |
|---|---|
| ④　個人データの漏えい等防止策 | ④　個人データの漏えい・毀損等防止策 |
| ⑤　［略］ | ⑤　［同左］ |
| ７－５　［略］ | ６－５　［同左］ |
| （漏えい等事案への対応の段階における取扱規程） | （漏えい事案等への対応の段階における取扱規程） |
| ７－６　金融分野における個人情報取扱事業者は、漏えい等事案への対応の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。 | ６－６　金融分野における個人情報取扱事業者は、漏えい事案等への対応の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　［略］ | ①　［同左］ |
| ②　漏えい等事案への対応に関する取扱者の限定 | ②　漏えい事案等への対応に関する取扱者の限定 |
| ③　漏えい等事案への対応の規程外作業に関する申請及び承認手続 | ③　漏えい事案等への対応の規程外作業に関する申請及び承認手続 |
| ④　漏えい等事案の影響・原因等に関する調査手続 | ④　漏えい事案等の影響・原因等に関する調査手続 |
| ［⑤・⑥　略］ | ［⑤・⑥　同左］ |
| ⑦　漏えい等事案への対応状況の記録及び分析 | ⑦　漏えい事案等への対応状況の記録及び分析 |
| ７－６－１　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。 | 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　個人情報保護委員会又は監督当局等への報告 | ①　監督当局等への報告 |
| ②　［略］ | ②　［同左］ |
| 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等事案の事実関係及び再発防止策等の速やかな公表 | 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 |
| （注）　金融分野における個人情報取扱事業者は、個人情報の保護に関する法律施行規則（平成28年個人情報保護委員会規則第３号）第７条各号に定める事態を知ったとき | |

は、個人情報の保護に関する法律（平成15年法律第57号）第26条及び個人情報の保護に関する法律についてのガイドライン（通則編）（平成28年個人情報保護委員会告示第６号）３－５－３及び３－５－４に従い、必要な措置を講ずる必要があるため、この点に留意して上記手続を定めること。

（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、８－１、８－１－１、８－１－２、８－１－３、８－１－４、８－１－５及び８－２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。

８－１　［略］

８－１－１　金融分野における個人情報取扱事業者は、７－１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

（別添２）　［同左］

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　［同左］

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、７－１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。

［①～③　略］

８－１－１－１　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、８－１－１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。

［①～③　略］

８－１－２　金融分野における個人情報取扱事業者は、７－２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、７－２－１、７－２－１－１及び７－２－２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。

［①～④　略］

８－１－２－１　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、８－１－２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。

［①～⑤　略］

８－１－３　金融分野における個人情報取扱事業者は、７－３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、７－３－１及び７－３－２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

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。

［①～③　同左］

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。

［①～③　同左］

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。

［①～④　同左］

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。

［①～⑤　同左］

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。 | する。 |
| ［①・②　略］ | ［①・②　同左］ |
| ８－１－３－１　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、８－１－３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。 | ７－１－３－１　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。 |
| ８－１－４　金融分野における個人情報取扱事業者は、７－４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、７－４－１及び７－４－２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。 | 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・②　略］ | ［①・②　同左］ |
| ８－１－５　金融分野における個人情報取扱事業者は、７－５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、７－５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　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。 |
| ８－１－５－１　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、８－１－５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。 | ７－１－５－１　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。 |

| | |
|---|---|
| ８－２　［略］<br>（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<br>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、９－１から９－４までの措置を講ずることとする。<br>９－１～９－４　［略］ | ７－２　［同左］<br>（別添３）［同左］<br>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。<br>８－１～８－４　［同左］ |
| 備考　表中の［　］の記載は注記である。 | |