資料5

金融分野の個人情報取扱事業者の安全管理措置等について

＜安全管理措置等に関する基準＞	＜各基準において定められる内容＞	＜ 具 体 例 ＞
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：安全管理措置** **第11条：従業者の監督** **第12条：委託先の監督**	安全管理措置等の基本的枠組を定めるとともに、措置事項を明示する。	「技術的安全管理措置」の措置事項として「個人データ利用者の識別及び認証」を定める。
安全管理措置等についての実務指針（別冊）	金融分野における個人情報保護に関するガイドラインに規定された各措置事項について、求められる措置内容を明示する。	「個人データ利用者の識別及び認証」として、本人確認に関する情報が他人に知られないための対策を講ずること等を定める。
事業者自ら、もしくは関係団体が自主的に示す安全対策基準等	求められる措置内容に関し、各事業者で個々具体的に採用すべき管理手法等を定める。	本人確認に関する情報が他人に知られないための対策として具体的な方法を定める。 （例えば、(財)金融情報システムセンター「金融機関等コンピュータシステム安全対策基準・解説書」では、暗証番号・パスワードについて、非表示や非印字、媒体上にそのまま記憶させない対策、最低桁数の設定、有効期間の設定、予測可能な文字等の排除、等を定める。）

1．規程等の整備

(1) 基本方針の整備

①基本方針の策定
（基本方針に定める事項）
・安全管理への取組み宣言
・個人データ保護の取組み内容
等

②基本方針の公表

③実施状況を踏まえた基本方針の見直し

(2) 安全管理に係る取扱規程の整備

①安全管理に係る取扱規程の策定
・各管理段階毎に規程を策定(1-2参照)
（規程に定める基本的事項）
・各管理段階における責任・権限関係
・各管理段階における取扱者の限定
・各管理段階において必要とされる手続き
・各管理段階における違反時の懲罰規定

②実施状況を踏まえた規程の見直し

(3) 点検・監査に係る規程の整備

①点検・監査に係る規程の策定
（規程に定める事項）
・点検・監査の対象
・点検・監査の実施部署
等

②実施状況を踏まえた規程の見直し

(4) 外部委託に係る規程の整備

①外部委託に係る規程の策定
（規程に定める事項）
・委託先選定基準
・委託契約に盛り込むべき安全管理措置の内容

②実施状況を踏まえた規程の見直し

<u>生体認証情報等高度な管理が必要な情報及び、個人信用情報機関における信用情報管理等については、更に厳正な管理として、どのような措置が求められるか（以下の各項目に亘る共通課題）</u>

１－２．各管理段階における取扱規程の整備

＜漏えい･き損等の要因に対応し、重要な管理段階毎に盛り込むべき安全管理措置の内容を定める。＞

管理段階	１．取得･入力	２．利用･加工	３．保管･保存	４．移送･送信	５．消去･廃棄	６．漏えい事案等への対応
主な漏えい･き損等の要因		①利用持ち出し時の紛失、窃盗被害 ②目的外利用 ③外部からの不正アクセス〔ハッキング等〕 ④内部悪意者による持ち出し	①顧客情報の社内紛失、盗難被害	①メール･ＦＡＸ等の誤送信 ②輸送中の紛失、盗難		①漏えい原因の特定が困難なことによる再発 ②迅速な対応の遅れによる二次被害の拡大

2．安全管理措置に係る実施体制の整備（①組織的安全管理措置）

(1)個人データの管理責任者の設置

①管理責任者(総責任者)の設置

②各部署毎の管理者の設置

管理責任者・管理者に求められる役割・資質等として記載すべき事項は何か

- 教育・研修の企画・実施
- 点検・監査を受けた規程の見直し

等

(2)雇用・雇用契約における安全管理の整備

①職務規程の整備

②従業者との個人データ非開示契約の締結

職務規程に記載すべき事項は何か

- 個人データを漏えい・流出、不正利用した場合の懲罰規定

等

(3)個人データの安全管理に係る取扱規程に従った運用

①取扱規程等に従った体制整備

②取扱規程等に従った運用の実施

③実施状況の記録・確認

(4)個人データの取扱状況を確認できる手段の整備

個人データの取扱状況を確認できる手段として含むべき事項

- 取得項目
- 利用目的
- 取得方法
- 保管方法
- 所管部署・管理者
- アクセス権限の内容
- 保存・保管期限
- 廃棄方法

等

(5)個人データの安全管理の点検・監査体制の整備と実施

①点検体制の整備と実施

②監査体制の整備と実施

点検・監査体制の整備として記載すべき事項は何か

- 責任者・担当者の選任
- 点検・監査計画の策定
- 体制の定期的な評価・見直し

等

(6)漏えい事案等に対応する体制の整備

①対応部署の設置

②漏えい等が発生した場合の調査体制の整備

③対応策の策定

④再発防止策・事後対策の検討体制の整備

⑤対策評価制度の整備

⑥自社内外への報告体制の整備

2．安全管理措置に係る実施体制の整備（②技術的安全管理措置）

アクセス制御関連

(1) 個人データの利用者の識別及び認証

①本人確認機能を設けること

②本人確認に関する情報が他人に知られないための対策を講ずること

等

(2) 個人データの管理区分の設定及びアクセス制御

①アクセス区分の設定

②内部関係者からのアクセス制御

③外部からの不正アクセスの防止措置

(3) 個人データへのアクセス権限の管理

①個人データへのアクセス権限の適切な付与・見直し

②権限を付与する従業者数の最小化

③従業者に付与する権限の最小化

利用･移送関連

(4) 個人データの漏えい･き損防止策

①個人データ保護策の実施

（個人データの保護策として記載すべき事項は何か）

・暗号化
・パスワード設定
・コンピュータウィルス等不正プログラムへの対応

等

②障害発生時の技術的復旧・代替方法

（技術的復旧・代替方法として記載すべき事項は何か）

・障害箇所の切り分け機能の設定
・リカバリ機能の設定

等

記録･分析関連

(5) 個人データへのアクセス記録及び分析

①アクセス記録の採取

②アクセス記録の分析・保存

(6) 個人データを取扱う情報システムの稼動状況の記録及び分析

①情報システムの稼動記録の採取

②情報システム稼動記録の分析・保存

監視･監査関連

(7) 個人データを取扱う情報システムの監視及び監査

①情報システムの利用状況の監視

②アクセス状況の監視

③監視体制の実施状況についての点検・監査

2．安全管理措置に係る実施体制の整備（③人的安全管理措置）
3．従業者の監督に係る事項

(1) 従業者との個人データの非開示契約の締結

①採用時等及び一定期間毎の締結

②違反した場合の措置に関する職務規程の整備

(2) 従業者の役割・責任等の明確化

①個人データの安全管理に係る規程の整備

各管理段階において人的安全管理措置として定めるべき事項

- 従業者の責任・権限
- 利用・持出し時等における従業員の義務
- 個人データ管理区分の設定とアクセス権限
- 規程に違反した場合の懲罰規定

②実施状況を踏まえた規程の見直し

(3) 従業者への安全管理措置の周知徹底、教育及び訓練

①採用時の教育や定期的な教育・訓練の実施

②個人データ管理責任者及び個人データ管理者に対する教育・訓練の実施

③個人データの安全管理に係る取扱規程に違反した場合の措置の周知

④教育・訓練の評価及び定期的な見直し

(4) 従業者による個人データ安全管理に係る取扱規程の遵守状況の確認

①安全管理に係る取扱規程に従った実施状況の確認・記録

②安全管理に係る取扱規程に従った実施状況についての点検・監査の実施

4．委託先の監督に係る事項

（1）委託先選定基準の明確化

〔選定基準に定める事項〕

①委託先における個人データ保護の実施体制の整備状況

〔求められる安全管理措置として記載すべき事項は何か〕

（組織的安全管理措置）
- 安全管理に係る取扱規程の整備　等

（人的安全管理措置）
- 個人データ非開示契約の締結　等

（技術的安全管理措置）
- 個人データ管理区分の設定とアクセス制御　等

②委託先における安全管理措置に係る規程等の整備状況

③実績等に基づく委託先の信用度

④委託先の経営の健全性

（2）委託契約において盛り込むべき安全管理措置の内容

①委託者の監督・監査・報告徴収に関する権限

②個人データの漏えい・盗用・改竄及び目的外利用の禁止

③再委託に関する条件

〔求められる条件として記載すべき事項〕
- 再委託先に対する監督・監査・報告徴収に関する権限
- 個人データの漏えい・盗用・改竄及び目的外利用の禁止
- 漏えい等が発生した際の委託先及び再委託先の責任

等

④漏えい等が発生した際の委託先の責任

等