⑵　新たなリスクに対応するための、安全管理措置の評価、見直し及び改善に向けた監査実施体制の整備
（例）
・　個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者による事業者内の対応の確認（必要に応じ、外部の知見を有する者を活用し確認させることを含む。）
⑶　漏えい等に早期に対処するための体制整備
（例）
・　漏えい等が発生した場合又は発生のおそれがある場合の連絡体制の整備
⑷　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
⑸　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
⑹　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
・　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
⑺　情報システムからの漏えい等を防止するための技術的安全管理措置
イ　加入者等の個人情報を取り扱う基幹システムに接続されたネットワーク（基幹系ネットワーク）とインターネットに接続されたネットワーク（情報系ネットワーク）を物理的又は論理的に分離をすること。また、基幹システムに保管されている個人情報を直接取り扱う作業は、インターネットに接続されたパソコン等では行わないこと。また、業務に応じて適切なアクセス権限を付与すること。
ロ　基幹システムにある個人情報データを外部の機関等へ電磁的方法により移送する場合は、暗号化・パスワードの設定等を必ず行い、原則として、インターネット等を介した電子メール等での送信は行わず電磁的記録媒体を使用する、又は専用線等のセキュリティが確保された通信を使用すること。また、作業に当たって一時的にパソコン等に個人情報を保存した場合は、作業終了後のデータ消去を徹底すること。
ハ　イ及びロについて運用上可能なものは直ちに実施するとともに、システム対応が必要となるものについては、システム改修を検討すること。なお、システム改修までの間、基幹システムにある個人情報を取り扱う場合、暗号化・パスワードの設定、作業終了後のパソコン等からの個人情報の消去等の安全管理措置を徹底すること。
（例）
・　個人データへのアクセスにおける識別と認証
・　個人データへのアクセス制御
・　個人データへのアクセス権限の管理
・　個人データへのアクセスや操作の記録及び不正が疑われる異常な記録の存否の定期的な確認
・　情報システムへの外部からのアクセス状況の監視及び当該監視システムの動作の定期的な確認
・　ソフトウェアに関する脆弱性対策（セキュリティパッチの適用、当該情報システム固有の脆弱性の発見及びその修正等）

なお、不特定多数者が書店で随時に購入可能な名簿で、事業者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、事業者の安全管理措置の義務違反にはならない。

3　従業者の監督【法第21条関係】

私的年金関係事業者は、その従業者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、当該従業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。

その際、個人データが漏えい、滅失又はき損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、個人データを取り扱う従業者に対する教育及び研修等の内容及び頻度を充実させるなど、必要かつ適切な措置を講ずる必要がある。

4　委託先の監督【法第22条関係】

⑴　私的年金関係事業者は、個人データの取扱いの全部又は一部を外部に委託する場合は、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（以下「委託先」という。）に対する必要かつ適切な監督を行わなければならない。

その際、個人データが漏えい、滅失又はき損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、委託する事業の規模及び性質並びに個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講ずるものとする。

⑵　私的年金関係事業者は、委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第20条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に応じて、確実に実施されることについて、委託先の体制、規程等の確認に加え、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行った上で、個人情報保護管理者等が、適切に評価することが望ましい。

⑶　私的年金関係事業者は、委託契約等において次に示す事項について定めることが望ましい。
イ　委託先の個人データの取扱いに関する事項
（例）
・　委託先において個人データを取り扱う者（委託先で作業する委託先の作業者以外の者を含む）を明確にすること
・　委託先において講ずべき安全管理措置の内容
ロ　委託先の秘密の保持に関する事項
ハ　委託された個人データの再委託に関する事項
（例）
・　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
ニ　契約終了時の個人データの返却等に関する事項
ホ　契約内容が遵守されなかった場合の措置
（例）
・　安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項

⑷　委託先における委託された個人データの取扱状況を把握するためには、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

委託先が再委託を行おうとする場合は、委託元は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先に事前報告又は承認手続を求める、直接又は委託先を通じて定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、再委託先が法第20条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。