（二）利用目的を本人に通知し、又は公表することにより外務省関係事業者の権利又は正当な利益を害するおそれがある場合

（例）

・新規開発部門が収集した情報の種類が明らかになることにより、企業の健全な競争を害する場合

・暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、業務妨害行為を行う悪質者情報を取得したことが明らかになることにより、情報提供を受けた企業に害が及ぶ場合

（三）国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

（例）

・犯罪捜査への協力のため、被疑者等に関する情報を取得した場合

（四）取得の状況からみて利用目的が明らかであると認められる場合

（例）

・今後連絡を取り合うために名刺交換をした場合

・着信において相手方の電話番号が非通知でない場合で、同じ用件で当方から相手方に電話を掛け直す場合

第六　個人データの管理に関する義務

一　データ内容の正確性の確保【法第十九条関係】

外務省関係事業者は、利用目的の達成に必要な範囲において、個人データを正確かつ最新の内容に保つよう努めなければならない。

二　安全管理措置【法第二十条関係】

外務省関係事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

その際、外務省関係事業者において、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、事業の規模及び性質、個人データの取扱状況並びに個人データを記録した媒体の性質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。

特に、事業者の内部又は外部からの不正行為による個人データの漏えい等を防止するための手法として、例えば次のような措置を講じることが望ましい。

（一）責任の所在の明確化のための措置

（例）

・個人データの安全管理の実施・運用に関する責任及び権限を有する個人情報保護管理者の設置（例えば、役員などの組織横断的に監督することのできる者を任命する）

・事業者内の個人データの取扱いの点検・改善等の監督を行う部署の設置

・事業者内の個人データの取扱いの点検・改善等の監督を行う合議制の委員会の設置

（二）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。）

（三）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

（四）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

（五）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

・個人データの保管場所の施錠及び鍵の管理

（六）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

・個人データの事務所外への持出しの制限（個人データを持ち出す権限を付与する者の限定、持出し手段の限定等）

（七）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

（例）

・個人データへのアクセスにおける識別と認証（アクセス権者へのＩＤ・パスワードの付与）

・個人データへのアクセス制御（アクセス権限を識別・認証する機能の設定）

・個人データへのアクセス権限の管理（アクセス権限を付与する者の限定）

・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）

・個人データを取り扱うシステムのセキュリティレベルの高度化（外部からの不正アクセス防止の機能をもつソフトウェアを組み込むシステムの設定等）

・外部のネットワークからの個人データを取り扱うシステムの遮断

・外部のネットワークと接続しているコンピュータへのファイアウォールの設置

・外部のネットワークにより個人データを送受信する場合のデータの暗号化

（八）個人データの保護に関する内部規程の整備、個人データ取扱マニュアルの作成

（九）従業者に対する教育・研修等の実施

（十）個人データの委託先の選定基準の策定、委託契約における安全管理の条項の整備

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。

三　従業者の監督【法第二十一条関係】

外務省関係事業者は、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。

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じる必要がある。