組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（法第21条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

①個人データの安全管理措置を講じるための組織体制の整備
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データの取扱状況を一覧できる手段の整備
④個人データの安全管理措置の評価、見直し及び改善
⑤事故又は違反への対処

【各項目を実践するために講じることが望まれる手法の例示】

①「個人データの安全管理措置を講じるための組織体制の整備」を実践するために講じることが望まれる手法の例示

・従業者の役割・責任の明確化
＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。
・個人データの安全管理の実施及び運用に関する責任及び権限を有する者として、個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））を設置し、原則として、役員を任命すること
・個人データの取扱いを総括する部署の設置、及び個人情報保護管理者（ＣＰＯ）が責任者となり、社内の個人データの取扱いを監督する「管理委員会」の設置
・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定
・個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定
・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化
・監査責任者の設置
・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が社内の対応を確認すること（必要に応じ、外部の知見を有する者を活用し確認することを含む）などによる、監査実施体制の整備
・個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備
・個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備
＊個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第31条を参照）。
・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備

②「個人データの安全管理措置を定める規程等の整備と規程等に従った運用」を実践するために講じることが望まれる手法の例示

・個人データの取扱いに関する規程等の整備とそれらに従った運用
・個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用
＊なお、これらについてのより詳細な記載事項については、下記の【個人データの取扱いに関する規程等に記載することが望まれる事項の例】を参照。
・個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
・個人データの取扱いを委託する場合における委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用
・定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持
※保持しておくことが望まれる監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

③「個人データの取扱い状況を一覧できる手段の整備」を実践するために講じることが望まれる手法の例示

・個人データについて、取得する項目、明示・公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備
・個人データ取扱台帳の内容の定期的な確認による最新状態の維持

④「個人データの安全管理措置の評価、見直し及び改善」を実践するために講じることが望まれる手法の例示

・監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施
・監査実施結果の取りまとめと、代表者への報告
・監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善

⑤「事故又は違反への対処」を実践するために講じることが望まれる手法の例示

・以下の㋐から㋔までの手順の整備

ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。

㋐事実調査、原因の究明
㋑影響範囲の特定
㋒再発防止策の検討・実施
㋓影響を受ける可能性のある本人への連絡

事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。

ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。

・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
・高度な暗号化等の秘匿化が施されている場合（ただし、㋔に定める報告の際、高度な暗号化等の秘匿化として施していた措置内容を具体的に報告すること。）
・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合。ただし、㋔に定める報告の際、漏えい等をした事業者以外では特定の個人を識別することができないものと判断できる措置内容を具体的に報告すること。）