

安全管理措置の例

講じなければならない措置	内容	小規模事業者における手法の例示
＜個人情報の取扱いにかかる規律の整備＞		
個人情報の取扱いに係る規律の整備	取り扱う個人情報の漏えい等の防止その他の個人情報の安全管理のために、個人情報の具体的な取扱いに係る規律を整備しなければならない。	・個人情報の取得、利用、保存等を行う場合の基本的な取扱い方法を決める。
＜組織的安全管理措置＞		
組織体制の整備	安全管理措置を講ずるための組織体制を整備しなければならない。	・組織全体での責任者、若しくは個人情報ごとに責任者を決める。
個人情報の取扱いに係る規律に従った運用	あらかじめ整理された個人情報の取扱いに係る規律に従って個人情報を取り扱わなければならない。	・決定した取扱方法に従って個人情報が取り扱われていることを、責任者が確認する。
個人情報の取扱い状況を確認する手段の整備	個人情報の取扱状況を確認するための手段を整備しなければならない。	・あらかじめ整備された基本的な取扱方法に従って個人情報が取り扱われていることを、責任者が定期的に確認する。
漏えい等の事案に対応する体制の整備	漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。	・漏えい等の事案の発生時に備え、個人情報取扱者（個人情報を利用する者）から責任者に対する報告連絡体制等をあらかじめ確認する。
取扱状況の把握及び安全管理措置の見直し	個人情報の取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。	・個人情報の取扱状況について、責任者が確認した結果を踏まえ、必要に応じてルールの見直し、個人情報取扱者への指導を行う。
＜人的安全管理措置＞		
個人情報取扱者の教育	組織として、個人情報取扱者に、個人情報の適正な取扱いを周知徹底するとともに、適切な教育を行わなければならない。	・個人情報の取扱いに関する留意事項について、個人情報取扱者に定期的な研修等を行う。 ・個人情報についての秘密保持に関する事項を会則等に盛り込む。
＜物理的安全管理措置＞		
個人情報を取り扱う区域の管理	個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域及びその他の個人情報を取り扱う事務を実施する区域について、それぞれ適切な管理を行わなければならない。	・個人情報取扱者及び個人情報の対象者本人以外が容易に個人情報を閲覧等できないような措置（コンピュータ端末やキャビネット・書庫等に近づけないようにするなど）を講ずる。
機器及び弟子媒体等の盗難等の防止	個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。	・個人情報を取り扱う機器、個人情報が記録された電子媒体又は書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人情報を取り扱うコンピュータ端末等機器をセキュリティワイヤー等により固定する。
電子媒体等を持ち運ぶ場合の漏えい等の防止	個人情報が記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人情報が閲覧されないよう、安全な方策を講じなければならない。	・個人情報が記録されたＵＳＢメモリやパソコン等に保存された電子ファイルはパスワード設定や暗号化をする。 ・紙文書は封筒に封入し鞆に入れて手から離さないようにして搬送する。
個人情報の削除及び機器、電子媒体等の廃棄	個人情報を削除し又は個人情報が記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。	・ＵＳＢメモリを使用できないよう破壊して廃棄する。 ・紙はシュレッダー等で細かく刻んで廃棄する。 ・廃棄結果を責任者が確認する。
＜技術的安全管理措置＞		
アクセス制御	担当者及び取り扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。	・個人情報を取り扱うことのできる機器及び当該機器を取り扱う個人情報取扱者を限定し、その者しか利用できないようルールを定める。
アクセス者の識別と認証	情報システムを使用する個人情報取扱者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。	・責任者から情報システムで使用する ID・パスワードを許可した個人情報取扱者にのみ伝え、他者には教えないようにさせる。
外部からの不正アクセス等の防止	個人情報を取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。	・個人情報を取り扱う機器等のオペレーティングシステム（OS）を最新の状態に保持する。 ・個人情報を取り扱う機器等にセキュリティ対策ソフトウェア等を導入する。
情報システムの使用に伴う漏えい等の防止	情報システムの使用に伴う個人情報の漏えい等を防止するための措置を講じ、適切に運用しなければならない。	・メール等により個人情報の含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定し、暗号化する。

※注）…安全管理措置を講ずるための具体的な手法については、個人情報が漏えい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、個人情報の取扱状況（取り扱う個人情報の性質及び量を含む。）、個人情報を記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。