【中小規模事業者における対応方法】
○　特定個人情報等の取扱い等を明確化する。
○　事務取扱担当者が変更となった場合、確実な引継ぎを行い、責任ある立場の者が確認する。

C　組織的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。

a　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する。

≪手法の例示≫

＊　組織体制として整備する項目は、次に掲げるものが挙げられる。
・　事務における責任者の設置及び責任の明確化
・　事務取扱担当者の明確化及びその役割の明確化
・　事務取扱担当者が取り扱う特定個人情報等の範囲の明確化
・　事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制
・　情報漏えい等事案の発生又は兆候を把握した場合の従業者から責任者等への報告連絡体制
・　特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

【中小規模事業者における対応方法】
○　事務取扱担当者が複数いる場合、責任者と事務取扱担当者を区分することが望ましい。

b　取扱規程等に基づく運用

取扱規程等に基づく運用状況を確認するため、システムログ又は利用実績を記録する。

≪手法の例示≫

＊　記録する項目としては、次に掲げるものが挙げられる。
・　特定個人情報ファイルの利用・出力状況の記録
・　書類・媒体等の持出しの記録
・　特定個人情報ファイルの削除・廃棄記録
・　削除・廃棄を委託した場合、これを証明する記録等
・　特定個人情報ファイルを情報システムで取り扱う場合、事務取扱担当者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

【中小規模事業者における対応方法】
○　特定個人情報等の取扱状況の分かる記録を保存する。

c　取扱状況を確認する手段の整備

特定個人情報ファイルの取扱状況を確認するための手段を整備する。

なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。

≪手法の例示≫

＊　取扱状況を確認するための記録等としては、次に掲げるものが挙げられる。
・　特定個人情報ファイルの種類、名称
・　責任者、取扱部署
・　利用目的
・　削除・廃棄状況
・　アクセス権を有する者

【中小規模事業者における対応方法】
○　特定個人情報等の取扱状況の分かる記録を保存する。

d　情報漏えい等事案に対応する体制の整備

情報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する。

情報漏えい等の事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である。

≪手法の例示≫

＊　情報漏えい等の事案の発生時に、次のような対応を行うことを念頭に、体制を整備することが考えられる。
・　事実関係の調査及び原因の究明
・　影響を受ける可能性のある本人への連絡
・　委員会及び主務大臣等への報告
・　再発防止策の検討及び決定
・　事実関係及び再発防止策等の公表

【中小規模事業者における対応方法】
○　情報漏えい等の事案の発生等に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認しておく。

e　取扱状況の把握及び安全管理措置の見直し

特定個人情報等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む。

≪手法の例示≫

＊　特定個人情報等の取扱状況について、定期的に自ら行う点検又は他部署等による監査を実施する。
＊　外部の主体による他の監査活動と合わせて、監査を実施することも考えられる。

【中小規模事業者における対応方法】
○　責任ある立場の者が、特定個人情報等の取扱状況について、定期的に点検を行う。

D　人的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。

a　事務取扱担当者の監督

事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。

b　事務取扱担当者の教育

事業者は、事務取扱担当者に、特定個人情報等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う。

≪手法の例示≫

＊　特定個人情報等の取扱いに関する留意事項等について、従業者に定期的な研修等を行う。
＊　特定個人情報等についての秘密保持に関する事項を就業規則等に盛り込むことが考えられる。

E　物理的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。

a　特定個人情報等を取り扱う区域の管理

特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。