・　特定個人情報ファイルの利用目的
・　特定個人情報ファイルに記録される項目及び本人として特定個人情報ファイルに記録される個人の範囲
・　特定個人情報ファイルに記録される特定個人情報等の収集方法

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

e　取扱状況の把握及び安全管理措置の見直し

監査責任者（地方公共団体等においては相当する者）は、特定個人情報の管理の状況について、定期に又は随時に点検又は監査（外部監査を含む。）を行い、その結果を総括責任者（地方公共団体等においては相当する者。以下同じ。）に報告する。総括責任者は、点検又は監査の結果等を踏まえ、必要があると認めるときは、取扱規程等の見直し等の措置を講ずる。

D　人的安全管理措置

行政機関等及び地方公共団体等は、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

総括責任者及び保護責任者（地方公共団体等においては相当する者。以下同じ。）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

総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適正な取扱いについて理解を深め、特定個人情報等の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。また、特定個人情報等を取り扱う情報システムの管理に関する事務に従事する職員に対し、特定個人情報等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

総括責任者及び保護責任者は、事務取扱担当者に、特定個人情報等の適切な管理のために、教育研修への参加の機会を付与する等の必要な措置を講ずる。

E　物理的安全管理措置

行政機関等及び地方公共団体等は、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。

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。）を明確にし、物理的な安全管理措置を講ずる。管理区域において、入退室管理及び管理区域へ持ち込む機器等の制限等の措置を講ずる。

行政機関等は、管理区域のうち、基幹的なサーバー等の機器を設置する室等（以下「情報システム室等」という。）を区分して管理する場合には、情報システム室等について、次の①及び②に掲げる措置を講ずる。地方公共団体等は、次の①及び②に掲げる項目を参考に、適切な措置を講ずる。

①　入退室管理

・　情報システム室等に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。また、情報システム室等に特定個人情報等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。
・　必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。
・　必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。

②　情報システム室等の管理

・　外部からの不正な侵入に備え、施錠装置、警報装置、監視設備の設置等の措置を講ずる。

b　機器及び電子媒体等の盗難等の防止

管理区域及び取扱区域における特定個人情報等を取り扱う機器、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、物理的な安全管理措置を講ずる。また、電子媒体及び書類等の庁舎内の移動等において、紛失・盗難等に留意する。

≪手法の例示≫

＊　特定個人情報等を取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット、書庫又は必要に応じて耐火金庫等へ保管する。
＊　特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定すること等が考えられる。

c　電子媒体等の取扱いにおける漏えい等の防止

許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。

取扱規程等の手続に基づき、特定個人情報等が記録された電子媒体又は書類等を持ち出す必要が生じた場合には、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる。

≪手法の例示≫

＊　特定個人情報等が記録された電子媒体を安全に持ち出す方法としては、持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等が考えられる。ただし、行政機関等に法定調書等をデータで提出するに当たっては、行政機関等が指定する提出方法に従う。
＊　特定個人情報等が記載された書類等を安全に持ち出す方法としては、封緘、目隠しシールの貼付を行うこと等が考えられる。

d　個人番号の削除、機器及び電子媒体等の廃棄

特定個人情報等が記録された電子媒体及び書類等について、文書管理に関する規程等によって定められている保存期間を経過した場合には、個人番号をできるだけ速やかに復元できない手段で削除又は廃棄する。

→ガイドライン第４－３－(4)Ｂ「保管制限と廃棄」参照