≪手法の例示≫
＊　管理区域に関する物理的安全管理措置としては、入退室管理及び管理区域へ持ち込む機器等の制限等が考えられる。
＊　入退室管理方法としては、ＩＣカード、ナンバーキー等による入退室管理システムの設置等が考えられる。
＊　取扱区域に関する物理的安全管理措置としては、壁又は間仕切り等の設置及び座席配置の工夫等が考えられる。

**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。

≪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・書庫等に保管する。
＊　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　電子媒体等を持ち出す場合の漏えい等の防止**

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場合、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。

「持出し」とは、特定個人情報等を、管理区域又は取扱区域の外へ移動させることをいい、事業所内での移動等であっても、紛失・盗難等に留意する必要がある。

≪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。

**【中小規模事業者における対応方法】**
○　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場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。

**d　個人番号の削除、機器及び電子媒体等の廃棄**

個人番号関係事務又は個人番号利用事務を行う必要がなくなった場合で、所管法令等において定められている保存期間等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－(3)Ｂ「保管制限と廃棄」参照

個人番号若しくは特定個人情報ファイルを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。また、これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。

≪手法の例示≫
＊　特定個人情報等が記載された書類等を廃棄する場合、焼却又は溶解等の復元不可能な手段を採用する。
＊　特定個人情報等が記録された機器及び電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用する。
＊　特定個人情報ファイル中の個人番号又は一部の特定個人情報等を削除する場合、容易に復元できない手段を採用する。
＊　特定個人情報等を取り扱う情報システムにおいては、保存期間経過後における個人番号の削除を前提とした情報システムを構築する。
＊　個人番号が記載された書類等については、保存期間経過後における廃棄を前提とした手続を定める。

**【中小規模事業者における対応方法】**
○　特定個人情報等を削除・廃棄したことを、責任ある立場の者が確認する。

**Ｆ　技術的安全管理措置**

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

**a　アクセス制御**

情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う。

≪手法の例示≫
＊　アクセス制御を行う方法としては、次に掲げるものが挙げられる。
・　個人番号と紐付けてアクセスできる情報の範囲をアクセス制御により限定する。
・　特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する。
・　ユーザーＩＤに付与するアクセス権により、特定個人情報ファイルを取り扱う情報システムを使用できる者を事務取扱担当者に限定する。

**【中小規模事業者における対応方法】**
○　特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定することが望ましい。
○　機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定することが望ましい。

**b　アクセス者の識別と認証**

特定個人情報等を取り扱う情報システムは、事務取扱担当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する。

≪手法の例示≫
＊　事務取扱担当者の識別方法としては、ユーザーＩＤ、パスワード、磁気・ＩＣカード等が考えられる。

**【中小規模事業者における対応方法】**
○　特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定することが望ましい。
○　機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定することが望ましい。

**c　外部からの不正アクセス等の防止**

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、適切に運用する。

≪手法の例示≫
＊　情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。
＊　情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。