講じなければならない措置	手法の例示	中小規模事業者における手法の例示
⑴　個人データを取り扱う区域の管理	（管理区域の管理手法の例） ・入退室管理及び持ち込む機器等の制限等 なお、入退室管理の方法としては、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。 （取扱区域の管理手法の例） ・壁又は間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止	・個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる。
⑵　機器及び電子媒体等の盗難等の防止	・個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・個人データ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、当該機器をセキュリティワイヤー等により固定する。	（同左）
⑶　電子媒体等を持ち運ぶ場合の漏えい等の防止	・持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ・封緘、目隠しシールの貼付けを行う。 ・施錠できる搬送容器を利用する。	・個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、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。
⑷　個人データの削除及び機器、電子媒体等の廃棄	（個人データが記載された書類等を廃棄する方法の例） ・焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 （個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例） ・情報システム（パソコン等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用する。 ・個人データが記録された機器、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の手段を採用する。	・個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、責任ある立場の者が確認する。

8－6　技術的安全管理措置

個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。

⑴　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。

⑵　アクセス者の識別と認証

個人データを取り扱う情報システムを使用する従業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。

⑶　外部からの不正アクセス等の防止

個人データ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。

⑷　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データ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。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
⑴　アクセス制御	・個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ユーザーＩＤに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。	・個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
⑵　アクセス者の識別と認証	（情報システムを使用する従業者の識別・認証手法の例） ・ユーザーＩＤ、パスワード、磁気・ＩＣカード等	・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、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。
⑶　外部からの不正アクセス等の防止	・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。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。	・個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ・個人データ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し、自動更新機能等の活用により、これを最新状態とする。
⑷　情報システムの使用に伴う漏えい等の防止	・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。）。 ・個人データを含む通信の経路又は内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。	・メール等により個人データ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する。