・アクセス権限を有する者に付与する権限の最小化
・個人データを格納した情報システムへの同時利用者数の制限
・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）
・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）
＊個人データを格納するためのデータベースを構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素であるデータベースへのアクセス制御を別に実施し、それぞれにアクセス権限を設定することが望ましい。
＊アクセス権限の設定を情報システム全体と別に実施する場合にあっては、無権限アクセスからの保護に係る機器等の設定として、特に不要アカウントの無効化や初期設定されている標準アカウントのパスワード変更を実施することが望ましい。
・個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等）
＊情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。
＊特権ユーザーに対するアクセス制御については、例えば、トラステッドＯＳやセキュアＯＳ、アクセス制御機能を実現する製品等の利用が考えられる。
・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ＯＳ・ウェブアプリケーションのぜい弱性有無の検証）

③「個人データへのアクセス権限の管理」を実践するために講じることが望まれる手法の例示
・個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）
＊個人データにアクセスできる者を許可する権限については、情報システム内において当該権限を含む管理者権限を分割する等して、不正利用を防止することが望ましい。
・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④「個人データへのアクセスの記録」を実践するために講じることが望まれる手法の例示
・個人データへのアクセスや操作の成功と失敗の記録及び不正が疑われる異常な記録の存否の定期的な確認
＊個人データへのアクセスや操作の成功と失敗の記録については、情報システムを構成する各システムへのアクセスや操作の成功と失敗等の記録を組み合わせ、各個人データへのアクセスや操作の失敗を全体として記録することが考えられる。
・採取した記録の漏えい、滅失及びき損からの適切な保護
＊採取した記録を漏えい、滅失及びき損から保護するためには、当該記録を適切に管理された外部記録媒体ないしログ収集用のサーバ等に速やかに移動することが望ましい。
＊システム管理者等の特権ユーザーのアクセス権限を用いても、採取した記録を改ざん・不正消去できないよう、対策することが望ましい。
＊個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤「個人データを取り扱う情報システムについて不正ソフトウェア対策」を実践するために講じることが望まれる手法の例示
・ウイルス対策ソフトウェアの導入及び当該ソフトウェアの有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）
・端末及びサーバ等のオペレーティングシステム（ＯＳ）、ミドルウェア（ＤＢＭＳ等）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
・組織で許可していないソフトウェアの導入防止のための対策

⑥「個人データの移送（運搬、郵送、宅配便等）・送信時の対策」を実践するために講じることが望まれる手法の例示
・個人データの移送時における紛失・盗難に備えるための対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化）
・盗聴される可能性のあるネットワーク（例えば、インターネットや無線ＬＡＮ等）による個人データの送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）時における、個人データの暗号化等の秘匿化（例えば、ＳＳＬ、Ｓ／ＭＩＭＥ等）
＊暗号を利用する場合には、復号に必要な鍵についても十分注意して管理する必要がある。

⑦「個人データを取り扱う情報システムの動作確認時の対策」を実践するために講じることが望まれる手法の例示
・情報システムの動作確認時のテストデータとして個人データを利用することの禁止（正確な動作確認を要する等、個人データの利用が不可欠な場合であっても、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換える等の措置を講じることが考えられる。）
・情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証

⑧「個人データを取り扱う情報システムの監視」を実践するために講じることが望まれる手法の例示
・個人データを取り扱う情報システムの使用状況の定期的な監視
・個人データへのアクセス状況（操作内容も含む。）の監視
＊個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。
＊特権ユーザーによる個人データへのアクセス状況については、特に注意して監視することが望ましい。
・個人データを取り扱う情報システムへの外部からのアクセス状況の監視（例えば、ＩＤＳ・ＩＰＳ等）
＊監視システムを利用する場合には、事業者等が業務で行う送受信の実態に合わせ、当該装置について適切に設定し、定期的にその動作を確認することが必要になる。

２－２－３－３．従業者の監督（法第21条関連）

法第21条
個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。