・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、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（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
・採取した記録の漏えい、滅失及びき損からの適切な保護
＊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
・オペレーティングシステム（ＯＳ）、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
・不正ソフトウェア対策の有効性・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）

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
・移送時における紛失・盗難が生じた際の対策（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）で個人データを送信（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）する際の、個人データの暗号化等の秘匿化

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
・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。

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。

個人情報取扱事業者は、法第20条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない（２－１－４．「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。

なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

【従業者に対して必要かつ適切な監督を行っていない場合】
事例１）従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合
事例２）内部規程等に違反して個人データが入ったノート型パソコン又は可搬型外部記録媒体を繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】
個人データの取扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング（以下「モニタリング」という。）を実施する場合は、次の点に留意する。

その際、雇用管理に関する個人情報の取扱いに関する重要事項を定めるときは、あらかじめ労働組合等に通知し、必要に応じて、協議を行うことが望ましい。また、その重要事項を定めたときは、労働者等に周知することが望ましい。

なお、本ガイドライン及び雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針（平成16年厚生労働省告示第259号）第三　九　㈠に規定する雇用管理に関する個人情報の取扱いに関する重要事項とは、モニタリングに関する事項等をいう。

・モニタリングの目的、すなわち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
・モニタリングの実施に関する責任者とその権限を定めること。
・モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。
・モニタリングの実施状況については、適正に行われているか監査又は確認を行うこと。