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。また、特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

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分野における個人情報保護に関するガイドライン第10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。

２－２－３－４．委託先の監督（法第22条関連）

法第22条

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた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、個人データの取扱いの全部又は一部を委託する場合、法第20条に基づく安全管理措置を遵守させるよう、委託を受けた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、委託する業務内容に対して必要のない個人データを提供しないようにすることは当然のこととして、取扱いを委託する個人データの内容を踏まえ、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た、必要かつ適切な措置を講じるものとする。特に、中小企業者においては、自ら又は委託先の事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

「必要かつ適切な監督」には、委託先を適切に選定すること、委託先に法第20条に基づく安全管理措置を遵守させるために必要な契約を締結すること、委託先における委託された個人データの取扱状況を把握することが含まれる。

なお、優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

①委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第20条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、個人情報保護管理者（ＣＰＯ）等が、適切に評価することが望ましい。

㈠組織的安全管理措置
・個人データの安全管理措置を講じるための組織体制の整備
・個人データの安全管理措置を定める規程等の整備と規程等に従った運用
・個人データの取扱状況を一覧できる手段の整備
・個人データの安全管理措置の評価、見直し及び改善
・事故又は違反への対処

㈡人的安全管理措置
・雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結
・従業者に対する内部規程等の周知・教育・訓練の実施

㈢物理的安全管理措置
・入退館（室）管理の実施
・盗難等の防止
・機器・装置等の物理的な保護

㈣技術的安全管理措置
・個人データへのアクセスにおける識別と認証
・個人データへのアクセス制御
・個人データへのアクセス権限の管理
・個人データのアクセスの記録
・個人データを取り扱う情報システムについての不正ソフトウェア対策
・個人データの移送・送信時の対策
・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
・個人データを取り扱う情報システムの監視

②委託契約の締結

委託契約には、当該個人データの取扱いに関する、必要かつ適切な安全管理措置として、委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を合理的に把握することを盛り込むことが望ましい。

③委託先における個人データ取扱状況の把握

委託先における委託された個人データの取扱状況を把握するためには、定期的に、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者（ＣＰＯ）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。