参考資料2

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（抜粋）平成19年3月　経済産業省

2-2-3-2.安全管理措置（法第２０条関連）

法第２０条

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない（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。その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。なお、クレジットカード情報については、別添の「クレジットカード情報を含む個人情報の取扱いについて」に掲げられた措置を講じることが望ましい。

【必要かつ適切な安全管理措置を講じているとはいえない場合】

事例１）公開されることを前提としていない個人データが事業者のウェブ画面上で不特定多数に公開されている状態を個人情報取扱事業者が放置している場合

事例２）組織変更が行われ、個人データにアクセスする必要がなくなった従業者が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従業者が個人データを漏えいした場合

事例３）本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失又はき損し、本人がサービスの提供を受けられなくなった場合

事例４）個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合

事例５）個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

【安全管理措置の義務違反とはならない場合（従業者の監督及び委託先の監督の義務違反ともならない場合）】

事例１）内容物に個人情報が含まれない荷物等の宅配又は郵送を委託したところ、誤配によって宛名に記載された個人データが第三者に開示された場合

事例２）書店で誰もが容易に入手できる市販名簿（事業者において全く加工をしていないもの）を処分するため、シュレッダー等による処理を行わずに廃棄し、又は、廃品回収に出した場合

組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という。）を整備運用し、その実施状況を確認することをいう。

【組織的安全管理措置として講じなければならない事項】

①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

②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

③個人データの取扱状況を一覧できる手段の整備

④個人データの安全管理措置の評価、見直し及び改善

⑤事故又は違反への対処

【各項目を実践するために講じることが望まれる手法の例示】

①「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」を実践するために講じることが望まれる手法の例示

・従業者の役割・責任の明確化

＊個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。

・個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））の設置

・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定

・個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定

・個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化

・監査責任者の設置

・監査実施体制の整備

・個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備

・個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備

＊個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第３１条を参照）。

・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備

・漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備

②「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」を実践するために講じることが望まれる手法の例示

・個人データの取扱いに関する規程等の整備とそれらに従った運用

・個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用

＊なお、これらについてのより詳細な記載事項については、下記の【個人データの取扱いに関する規程等に記載することが望まれる事項の例】を参照。

・個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用

・個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
・定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持
※保持しておくことが望まれる監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

③「個人データの取扱い状況を一覧できる手段の整備」を実践するために講じることが望まれる手法の例示
・個人データについて、取得する項目、明示・公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備
・個人データ取扱台帳の内容の定期的な確認による最新状態の維持

④「個人データの安全管理措置の評価、見直し及び改善」を実践するために講じることが望まれる手法の例示
・監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施
・監査実施結果の取りまとめと、代表者への報告
・監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善

⑤「事故又は違反への対処」を実践するために講じることが望まれる手法の例示
・以下の(ア)から(カ)までの手順の整備
ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。
(ア)事実調査、原因の究明
(イ)影響範囲の特定
(ウ)再発防止策の検討・実施
(エ)影響を受ける可能性のある本人への連絡
事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。
ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。
・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
・高度な暗号化等の秘匿化が施されている場合

・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）

(オ)主務大臣等への報告

a．個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合

認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。

ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。

・機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合

・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合

・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合

・その他認定個人情報保護団体が必要と考える場合

b．個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合

経済産業大臣（主務大臣）に報告を行う。

なお、認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。

(カ)事実関係、再発防止策等の公表

二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。

ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。

・影響を受ける可能性のある本人すべてに連絡がついた場合

・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合

・高度な暗号化等の秘匿化が施されている場合

・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）

【個人データの取扱いに関する規程等に記載することが望まれる事項の例】

以下、（1）取得・入力、（2）移送・送信、（3）利用・加工、（4）保管・バックアップ、（5）消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項の例を列記する。

（1）取得・入力

①作業責任者の明確化

・個人データを取得する際の作業責任者の明確化
・取得した個人データを情報システムに入力する際の作業責任者の明確化（以下、併せて「取得・入力」という。）

②手続の明確化と手続に従った実施

・取得・入力する際の手続の明確化
・定められた手続による取得・入力の実施
・権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）での入力作業の実施
・個人データを入力できる端末の、業務上の必要性に基づく限定
・個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする。）

③作業担当者の識別、認証、権限付与

・個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定
・個人データの取得・入力業務を行う作業担当者に付与した権限の記録

④作業担当者及びその権限の確認

・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と、権限外作業の有無の確認

（2）移送・送信

①作業責任者の明確化

・個人データを移送・送信する際の作業責任者の明確化

②手続の明確化と手続に従った実施

・個人データを移送・送信する際の手続の明確化
・定められた手続による移送・送信の実施
・個人データを移送・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆

回線を利用して個人データを送信する場合）
・移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）
・ＦＡＸ等におけるあて先番号確認と受領確認
・個人データを記した文書をＦＡＸ機等に放置することの禁止
・暗号鍵やパスワードの適切な管理

③作業担当者の識別、認証、権限付与
・個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。）
・個人データの移送・送信業務を行う作業担当者に付与した権限の記録

④作業担当者及びその権限の確認
・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と、権限外作業の有無の確認

（３）利用・加工
①作業責任者の明確化
・個人データを利用・加工する際の作業責任者の明確化

②手続の明確化と手続に従った実施
・個人データを利用・加工する際の手続の明確化
・定められた手続による利用・加工の実施
・権限を与えられていない者が立ち入れない建物等での利用・加工の実施
・個人データを利用・加工できる端末の、業務上の必要性に基づく限定
・個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする。）

③作業担当者の識別、認証、権限付与
・個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）
・個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

④作業担当者及びその権限の確認
・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と権限外作業の有無の確認

（4）保管・バックアップ
①作業責任者の明確化
・個人データを保管・バックアップする際の作業責任者の明確化

②手続の明確化と手続に従った実施
・個人データを保管・バックアップする際の手続※の明確化
※情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（ＯＳ）やアプリケーションのバックアップも必要となる場合がある。
・定められた手続による保管・バックアップの実施
・個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化
・暗号鍵やパスワードの適切な管理
・個人データを記録している媒体を保管する場合の施錠管理
・個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
・個人データを記録している媒体の遠隔地保管
・個人データのバックアップから迅速にデータが復元できることのテストの実施
・個人データのバックアップに関する各種事象や障害の記録

③作業担当者の識別、認証、権限付与
・個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。）
・個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

④作業担当者及びその権限の確認
・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管と権限外作業の有無の確認

（5）消去・廃棄
①作業責任者の明確化
・個人データを消去する際の作業責任者の明確化

・個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

②手続の明確化と手続に従った実施
・消去・廃棄する際の手続の明確化
・定められた手続による消去・廃棄の実施
・権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
・個人データを消去できる端末の、業務上の必要性に基づく限定
・個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に１回又は複数回上書きする。）
・個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）

③作業担当者の識別、認証、権限付与
・個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定
・ID とパスワードによる認証、生体認証等による作業担当者の識別
・作業担当者に付与する権限の限定
・個人データの消去・廃棄を行う作業担当者に付与した権限の記録

④作業担当者及びその権限の確認
・手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
・アクセスの記録、保管、権限外作業の有無の確認

人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

【人的安全管理措置として講じなければならない事項】
①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。）における委託者と受託者間での非開示契約の締結
②従業者に対する内部規程等の周知・教育・訓練の実施
なお、管理者が定めた規程等を守るように監督することについては、法第２１条を参照。

【各項目を実践するために講じることが望まれる手法の例示】
①「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。）における委託者と受託者間での非開示契約の締結」を実践するために講じることが望まれる手法の例示
・従業者の採用時又は委託契約時における非開示契約の締結

＊雇用契約又は委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。

＊個人情報に関する非開示の義務を、就業規則等の社内規程に規定することも考えられる。なお、社内規程に個人情報に関する非開示の義務を規定する場合には、特に、労働基準法第８９条及び第９０条などの労働関連法規を遵守する必要がある。

＊個人情報に関する非開示契約の締結の際に、営業秘密を対象とする秘密保持契約をあわせて締結する場合であっても、個人情報保護と営業秘密の保護はその目的・範囲等が異なるため、従業者の「納得感」の向上の観点からは、個人情報保護に関する契約と営業秘密に関する秘密保持契約は峻別する（別書面であるか否かは問わない）ことが望ましい。

・非開示契約に違反した場合の措置に関する規程の整備

＊個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

②「従業者に対する内部規程等の周知・教育・訓練」を実践するために講じることが望まれる手法の例示

・個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知

・個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施

・従業者に対する必要かつ適切な教育・訓練が実施されていることの確認

物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいう。

【物理的安全管理措置として講じなければならない事項】

①入退館（室）管理の実施

②盗難等の防止

③機器・装置等の物理的な保護

【各項目を実践するために講じることが望まれる手法の例示】

①「入退館（室）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

・個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施

・個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的

に保護された室内等への設置

②「盗難等の防止」を実践するために講じることが望まれる手法の例示
・個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止
・離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止
・個人データを含む媒体の施錠保管
・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③「機器・装置等の物理的な保護」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機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいう。

【技術的安全管理措置として講じなければならない事項】
①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤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
⑥個人データの移送・送信時の対策
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
⑧個人データを取り扱う情報システムの監視

【各項目を実践するために講じることが望まれる手法の例示】
①「個人データへのアクセスにおける識別と認証」を実践するために講じることが望まれる手法の例示
・個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証（例えば、ID とパスワードによる認証、生体認証等）の実施
＊ ID とパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗した ID を停止する等の措置を講じることが望ましい。

・個人データへのアクセス権限を有する者が使用できる端末又はアドレス等の識別と認証（例えば、MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施

②「個人データへのアクセス制御」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権限を付与すべき者の最小化
・識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施
・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 （一）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、受託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。

「必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれる。

なお、本人からの損害賠償請求に係る責務を、安全管理措置に係る責任分担を無視して一方的に受託者に課すなど、優越的地位にある者が委託者の場合、受託者に不当な負担を課すことがあってはならない。

また、委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要する。

【受託者に必要かつ適切な監督を行っていない場合】

事例１）個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合

事例２）個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合

事例３）再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

・委託者及び受託者の責任の明確化
・個人データの安全管理に関する事項
　・個人データの漏えい防止、盗用禁止に関する事項
　・委託契約範囲外の加工、利用の禁止
　・委託契約範囲外の複写、複製の禁止

・委託契約期間
・委託契約終了後の個人データの返還・消去・廃棄に関する事項
・再委託に関する事項
・再委託を行うに当たっての委託者への文書による報告
・個人データの取扱状況に関する委託者への報告の内容及び頻度
・契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれる。）
・契約内容が遵守されなかった場合の措置
・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項