Ⅱ．法令解釈指針・事例

２．個人情報取扱事業者の義務等

（３）個人データの管理（法第１９条～第２２条関連）

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（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、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。

【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事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、その従事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

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個人データの取扱い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

【各項目について講じることが望まれる事項】

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をする上で望まれる事項

・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する上で望まれる事項

・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］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しい監査証跡としては、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する上で望まれる事項

･個人データについて、取得する項目、通知した利用目的、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、見直し及び改善をする上で望まれる事項

･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する上で望まれる事項

･事実関係、再発防止策等の公表

･その他、以下の項目等の実施

ア）事実調査、イ）影響範囲の特定、ウ）影響を受ける可能性のある本人及び主務大臣等への報告、エ）原因の究明、オ）再発防止策の検討･実施

【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】

以下、（ⅰ）取得・入力、（ⅱ）移送・送信、（ⅲ）利用・加工、（ⅳ）保管・バックアップ、（ⅴ）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を列記する。

（ⅰ）取得･入力

ⅰ）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。）

ⅱ）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。）

ⅲ）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

ⅳ）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

（ⅱ）移送・送信

ⅰ）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

ii）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（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

iii）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

iv）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

（iii）利用・加工

ｉ）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

ii）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。）

iii）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

iv）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

（iv）保管・バックアップ

ｉ）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

ii）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

・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

iii）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

iv）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

（v）消去・廃棄

ⅰ）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

ⅱ）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。）

ⅲ）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

ⅳ）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雇用契約時及び委託契約時における非開示契約の締結

②従業者に対する教育・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。

【各項目について講じることが望まれる事項】

①雇用契約時及び委託契約時における非開示契約の締結をする上で望まれる事項・

・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。

・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。

人的安全管理措置

②従業者に対する周知･教育･訓練を実施する上で望まれる事項

･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

【各項目について講じることが望まれる事項】

①入退館（室）管理を実施する上で望まれる事項

･個人データを取り扱う業務上の、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盗難等を防止する上で望まれる事項

･離席時の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

・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

物理的安全管理措置

③機器・装置等を物理的に保護する上で望まれる事項

・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

【各項目について講じることが望まれる事項】

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項

・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アクセス権限を有する従業者本人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各従業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行う上で望まれる事項

・個人データへのアクセス権限を付与すべき従業者数の最小化

・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。）

・従業者に付与するアクセス権限の最小化

・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、業務上必要となる従業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行う上で望まれる事項

・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行う上で望まれる事項

・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施する上で望まれる事項

・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）・送信時の対策の上で望まれる事項

・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）

・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

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の上で望まれる事項

・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行う上で望まれる事項

・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。