10　（別添）講ずべき安全管理措置の内容

法第 23 条に定める安全管理措置として、個人情報取扱事業者が具体的に講じなければならない措置や当該措置を実践するための手法の例等を次に示す（※1）。

安全管理措置を講ずるための具体的な手法については、個人データが漏えい等をした場合に、本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる例示の内容の全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。

なお、中小規模事業者（※2）については、その他の個人情報取扱事業者と同様に、法第 23 条に定める安全管理措置を講じなければならないが、取り扱う個人データの数量及び個人データを取り扱う従業者数が一定程度にとどまること等を踏まえ、円滑にその義務を履行し得るような手法の例を示すこととする。もっとも、中小規模事業者が、その他の個人情報取扱事業者と同様に「手法の例示」に記述した手法も採用することは、より望ましい対応である。

（※1）法第 23 条に定める「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」には、個人情報取扱事業者が取得し、又は取得しようとしている個人情報であって、当該個人情報取扱事業者が個人データとして取り扱うことを予定しているものの漏えい等を防止するために必要かつ適切な措置も含まれる。そのため、次に掲げる措置及び例示における「個人データ」には、当該個人情報も含まれる。

（※2）「中小規模事業者」とは、従業員（※3）の数が 100 人以下の個人情報取扱事業者をいう。ただし、次に掲げる者を除く。

・その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去 6 月以内のいずれかの日において 5,000 を超える者

・委託を受けて個人データを取り扱う者

（※3）中小企業基本法（昭和 38 年法律第 154 号）における従業員をいい、労働基準法（昭和 22 年法律第 49 号）第 20 条の適用を受ける労働者に相当する者をいう。ただし、同法第 21 条の規定により同法第 20 条の適用が除外されている者は除く。

10-1　基本方針の策定

個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。

具体的に定める項目の例としては、「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等が考えられる。

10-2　個人データの取扱いに係る規律の整備

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等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
○個人データの取扱いに係る規律の整備	取得、利用、保存、提供、削除・廃棄等の段階ごとに、取扱方法、責任者・担当者及びその任務等について定める個人データの取扱規程を策定することが考えられる。なお、具体的に定める事項については、以降に記述する組織的安全管理措置、人的安全管理措置及び物理的安全管理措置の内容並びに情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）は技術的安全管理措置の内容を織り込むことが重要である。	• 個人データの取得、利用、保存等を行う場合の基本的な取扱方法を整備する。

10-3　組織的安全管理措置

個人情報取扱事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。

（1）組織体制の整備

安全管理措置を講ずるための組織体制を整備しなければならない。

（2）個人データの取扱いに係る規律に従った運用

あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。

個人データの取扱状況を確認するための手段を整備しなければならない。

（3）漏えい等事案に対応する体制の整備

漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。

なお、漏えい等事案が発生した場合、二次被害の防止、類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である（※）。

（※）個人情報取扱事業者において、漏えい等事案が発生した場合等の対応の詳細については、3-5（個人データの漏えい等の報告等）を参照のこと。

（4）取扱状況の把握及び安全管理措置の見直し

個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
（1）組織体制の整備	（組織体制として整備する項目の例） • 個人データの取扱いに関する責任者の設置及び責任の明確化並びに責任部署の設置及び役割の明確化 • 個人データを取り扱う従業者及びその役割の明確化 • 上記の従業者が取り扱う個人データの範囲の明確化 • 法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実又は兆候を把握した場合の責任者及び責任部署への報告連絡体制 • 個人データの漏えい等事案の発生又は兆候を把握した場合の責任者及び責任部署への報告連絡体制 • 個人データを複数の部署で取り扱う場合の各部署の役割分担及び責任の明確化	• 個人データを取り扱う従業者が複数いる場合、責任ある立場の者とその他の者を区分する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(2) 個人データの取扱いに係る規律に従った運用	（個人データの取扱いに係る規律の明確化と周知） 個人データの取扱いに係る規律を明確化し、従業者に周知する。 （個人データの取扱いに係る規律に従った運用の確保） 個人データの取扱いに係る規律に従った運用を確保するため、あらかじめ整備された個人データの取扱いに係る規律に従って個人データが取り扱われていることを、責任者又は責任部署が確認する。例えば、次のような項目を確認し、あらかじめ整備された個人データの取扱いに係る規律と照らし合わせることが考えられる。 • 個人情報データベース等の利用・出力状況 • 個人データが記載又は記録された書類・媒体等の持ち運び等の状況 • 個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。） • 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ログイン実績、アクセスログ等） （個人データの取扱状況を確認する手段の整備） 上記確認のため、システムログその他の個人データの取扱いに係る記録の整備や業務日誌、個人情報取扱台帳を作成等することが考えられる。これらの記録等においては、例えば次のような項目をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とすることが考えられる。 • 個人情報データベース等の種類・名称 • 個人データの項目 • 個人データを取り扱う部署・当該部署の責任者	• あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	• 利用目的 • アクセス権を有する者 等	
(3) 漏えい等事案に対応する体制の整備	漏えい等事案の発生時に例えば次のような対応を行うための、体制を整備することが考えられる。 • 事実関係の調査及び原因の究明 • 影響を受ける可能性のある本人への通知 • 個人情報保護委員会等関係機関への報告 • 再発防止策の検討及び決定 • 事実関係及び再発防止策等の公表 等	• 漏えい等事案の発生時に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認する。
(4) 取扱状況の把握及び安全管理措置の見直し	(個人データの取扱状況の把握) • 個人データの取扱状況について、上記(2)による把握に加えて、定期的に自ら行う点検又は他部署等による監査を実施する。 • 外部の主体による監査活動と合わせて、監査を実施する。 (安全管理措置の見直し) • 個人データの取扱状況、情報技術の進歩等を踏まえて、講じた安全管理措置について、定期的に評価及び見直しを行い、必要に応じて改善をする。	• 責任ある立場の者が、個人データの取扱状況について、定期的に点検を行う。

10-4　人的安全管理措置

個人情報取扱事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。また、個人情報取扱事業者は、従業者に個人データを取り扱わせるに当たっては、法第 24 条に基づき従業者に対する監督をしなければならない（3-4-3（従業者の監督）参照）。

〇従業者の教育

従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
〇従業者の教育	• 個人データの取扱いに関する留意事項について、従業者に定期的に（少なくとも年 1 回程度）適切な内容の研修等を行う。 • 従業者に対する定期的な研修等の内容、実施方法等を評価、見直し及び改善する。 • 個人データについての秘密保持に関する事項を就業規則等に盛り込む。	（同左）

10-5　物理的安全管理措置

個人情報取扱事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。

(1) 個人データを取り扱う区域の管理

個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（以下「管理区域」という。）及びその他の個人データを取り扱う事務を実施する区域（以下「取扱区域」という。）について、それぞれ適切な管理を行わなければならない。

(2) 機器及び電子媒体等の盗難等の防止

個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。

(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止

個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。

なお、「持ち運ぶ」とは、個人データを管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、事業所内の移動等であっても、個人データの紛失・盗難等に留意する必要がある。

(4) 個人データの削除及び機器、電子媒体等の廃棄

個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。

また、個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(1) 個人データを取り扱う区域の管理	（管理区域の管理手法の例） • 入退室管理及び持ち込む機器等の制限等 なお、入退室管理の方法としては、IC カード、ナンバーキー等による入退室管理システムの設置等が考えられる。 （取扱区域の管理手法の例） • 間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止	• 個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる。
(2) 機器及び電子媒体等の盗難等の防止	• 個人データを取り扱う機器、個人データが記録された電子媒体又は個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 • 個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。	（同左）
(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止	• 持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 • 封緘、目隠しシールの貼付けを行う。 • 施錠できる搬送容器を利用する。	• 個人データが記録された電子媒体又は個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞄に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
(4) 個人データの削除及び機器、電子	（個人データが記載された書類等を廃棄する方法の例） • 焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。	• 個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄したことを、責任ある立場の者が確認する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
媒体等の廃棄	（個人データを削除し、又は、個人データが記録された機器、電子媒体等を廃棄する方法の例） • 情報システム（パソコン等の機器を含む。）において、個人データを削除する場合、容易に復元できない手段を採用する。 • 個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用、暗号化消去、物理的な破壊等の手段を採用する。	

10-6　技術的安全管理措置

個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取り扱う場合（インターネット等を通じて外部と送受信等する場合を含む。)、技術的安全管理措置として、次に掲げる措置を講じなければならない。

（1）アクセス制御

担当者及び個人データを取り扱う情報システムの範囲を限定するために、適切なアクセス制御を行わなければならない。

（2）アクセス者の識別と認証

個人データを取り扱う情報システムを使用する者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。

（3）外部からの不正アクセス等の防止

個人データを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

（4）情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。

（5）不正アクセス等の検知等

個人データを取り扱う情報システムに対する不正アクセス等が発生した場合に早期に検知等するための措置を平時から講じ、組織内ネットワークにおける被害拡大を防止できるよう適切に運用しなければならない。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
(1) アクセス制御	(情報システムの限定) • 個人データを取り扱う情報システムを限定する。 • 個人データを取り扱う情報システムへのアクセスを最小化する。例えば、事前に許可した特定の IP アドレスからのみに限定する方法が考えられる。 (アクセスできる者の限定) • 個人データを取り扱う情報システムを使用できる従業者については、ユーザーID に付与するアクセス権限を最小化することにより限定する。 • 特権アカウントを割り当てる従業者、利用する端末、利用する場面等を最小限に限定する。 • 組織体制に変更が生じた場合(例えば、人事異動、従業者の退職等)等に、アクセス権限の変更を適切に行う。 • アクセス制御が適切に行われているか確認する。例えば、アクセス権限について定期的に監査する、アクセス権限の棚卸しを行う等の方法が考えられる。 • 組織内外からのアクセスについて、アクセス要求ごとにアクセス元の場所、アクセス時間、デバイスのセキュリティ状態等の動的コンテキストを評価し、リスクに応じてアクセスの可否を判断する仕組みを導入する。	• 個人データを取り扱うことのできる機器及び当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
(2) アクセス者の識別と認証	(情報システムを使用する従業者の識別・認証手法の例) • ユーザーID、パスワード、磁気・IC カード、指紋認証・静脈認証・顔認証等の方法が考えられる。	• 機器に標準装備されているユーザー制御機能(ユーザーアカウント制御)により、個人データを取り扱う情報シス

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	• ユーザーID・パスワードを利用する場合には、同一のユーザーID・パスワードの使い回しの原則禁止及び類似パスワードの使い回しの制限、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 の停止等を行う。 • 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についての識別と認証を実施する。例えば、IP アドレス認証、電子証明書等の方法が考えられる。 • 組織外ネットワークからのアクセスや、管理者権限でのアクセス、重要な個人データへのアクセスにおいては、識別・認証手法を複数組み合わせる多要素認証（フィッシングに耐性のあるものを含む。）を導入する。 （情報システムを使用する従業者以外の者の識別・認証手法の例） • 従業者以外の者を適切に識別・認証する方法を採用する。例えば、同一及び類似パスワードの使い回しをしないよう周知、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 の停止、多要素認証（フィッシングに耐性のあるものを含む。）の導入等が考えられる。	テムを使用する従業者を識別・認証する。
（3）外部からの不正アクセス等の防止	• 個人データを取り扱う情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 • 個人データを取り扱う情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入して適切に運用（パターンファイルや修正ソフトウェアの更新確認等を行うことを含む。）し、不正ソフトウェアの有無を確認する。 • 機器やソフトウェア等に標準装備されている自動更新機能等の活用、端末、サーバ、VPN 機器等のオペレーティングシステム、ミドルウェア、	• 個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 • 個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	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の適用により、ソフトウェア等を最新状態とする。 • 個人情報取扱事業者において許可していないソフトウェア等の導入を防止する。例えば、ソフトウェアの導入時の確認のほか、定期的な監査などの方法が考えられる。 • 組織が許可し、セキュリティ基準を満たしたデバイスからのみ個人データへのアクセスを許可する。	
(4) 情報システムの使用に伴う漏えい等の防止	(情報システムの開発、維持・管理、変更等における安全性確保) • 個人データを取り扱う情報システムの設計時に安全性を確保し、継続的に見直す(情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む。)。 • 個人データを取り扱う情報システムの動作確認を行う際に、テストデータとして利用する個人データを必要最小限とする。例えば、テストデータとして個人データを利用することを禁止したり、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などの方法が考えられる。 • 個人データを取り扱う情報システムの変更時に、当該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を検証する。 (通信の経路又は内容の暗号化) • 個人データを含む通信の経路又は内容を暗号化する。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、本人又は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、個人データの暗号化等の秘匿化(例えば、SSL/TLS、S/MIME 等)を行うなどの方法が考えられる。	• メール等により個人データの含まれるファイルを送信する場合に、当該ファイルへのパスワードを設定する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	• 移送する個人データについて、パスワード等による保護を行う。 （クラウドサービスを利用した情報システムの更改・廃棄） • クラウドサービスのサーバ上に保管された個人データを消去する際は、クラウドサービス提供事業者が提供する方法、暗号化消去等、容易に復元できない手段を採用する。	
（5）不正アクセス等の検知等	（定期的な分析） • 個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、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等のログ（例えば、認証ログ、アクセスログ、操作ログ、通信ログ等）等を一定の期間保管する。 • 当該ログ等の漏えい、滅失及び毀損並びに改ざん、不正消去等からの適切な保護を行う。 • 当該ログ等の定期的な分析により、不正アクセス等の発生又は兆候を早期に検知する。 （常時監視による早期検知） • 不正アクセス等の発生又は兆候を早期に検知等するための仕組み（例えば、IDS/IPS、EDR 等）等を導入する。 （組織内ネットワークでの被害拡大の防止） • 不正アクセス等が発生した場合でも個人データを取り扱う情報システムの被害が広がらないよう、必要な対策を講ずる。例えば、侵害を受けた又はそのおそれがある情報システムの停止・隔離、アカウントの無効化	• 個人データを取り扱う情報システムの使用状況、個人データへのアクセス状況、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等のログ等を一定の期間保管する。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
	などの方法が考えられる。その他必要な対策については、10-6 技術的安全管理措置(1)から(4)の手法の例示も参照されたい。	

10-7　外的環境の把握

個人情報取扱事業者が、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、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。