

個人情報情報の適正な 取り扱いの徹底

令和7年3月27日（木）

令和6年度地域密着型サービス等集団指導

芦屋市高齢介護課

個人情報とは

生存する個人に関する情報であって、氏名や生年月日等により特定の個人を識別することができるもの

要配慮個人情報とは

個人情報のうち、不当な差別、偏見その他の不利益が生じないように取扱いに配慮を有する情報として、個人情報保護法・政令・規則に定められた情報
人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実等のほか、身体障害、知的障害、精神障害等の障害があること、健康診断その他の検査の結果、保健指導、診療・調剤情報、本人を被疑者又は被告人として、逮捕、搜索等の刑事事件に関する手続が行われたこと、本人を非行少年又はその疑いがある者として、保護処分等の少年の保護事件に関する手続が行われたことが該当する

個人情報保護に関する法律

利用者や消費者が安心できるように、企業や団体、国の行政機関等に個人情報をきちんと大切に扱ってもらった上で、有効に活用できるよう共通のルールを定めた法律

- 個人情報保護法

- ・第23条（安全管理措置）
- ・第26条（個人情報保護委員会への漏えい等の報告等）

⇒介護サービス事業者も遵守しなければならない

しかし、介護サービス事業者からの要配慮個人情報の漏えい等が見受けられる

第23条 安全管理措置

① 個人データの取扱いに係る規律の整備

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。

組織的
安全管理措置

人的
安全管理措置

物理的
安全管理措置

技術的
安全管理措置

組織的安全管理措置（１）

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 ・ 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。

組織的安全管理措置（2）

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に従った運用を確保するため、例えば次のような項目に関して、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の作成等を通じて、個人データの取扱いの検証を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）	・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。
(3) 個人データの取扱状況を確認する手段の整備	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 ・責任者・取扱部署 ・利用目的 ・アクセス権を有する者 等	・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。

組織的安全管理措置（３）

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
(4) 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、従業員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。
(5) 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について、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。	・ 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。

人的安全管理措置

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
○従業員の教育	・個人データの取扱いに関する留意事項について、従業員に定期的な研修等を行う。 ・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)

物理的安全管理措置（１）

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員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、封筒に封入し鞆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。

物理的安全管理措置（2）

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
(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又は物理的な破壊等の手段を採用する。	・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。

技術的安全管理措置（１）

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	・ 個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・ 情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ ユーザーID に付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。	・ 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 カード等	・ 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、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。

技術的安全管理措置（２）

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
(3) 外部からの不正アクセス等の防止	・ 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。 ・ 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、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により、ソフトウェア等を最新状態とする。 ・ ログ等の定期的な分析により、不正アクセス等を検知する。	・ 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。
(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。）。 ・ 個人データを含む通信の経路又は内容を暗号化する。 ・ 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。	・ 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。

第26条 漏えい等の報告

- 漏えい：個人データが外部に流出すること

（例）第三者に誤送付・誤送信、インターネット上での閲覧可能状態
書類・媒体等の盗難、不正アクセス等

- 滅失：個人データの内容が失われること

（例）帳票等の誤った廃棄、書類・媒体等の社内紛失等

- 毀損：個人データの内容が意図しない形で変更されることや、
内容を保ちつつも利用不能な状態になること

（例）内容の改ざん、個人データの復元キーの喪失または暗号化により
復元できなくなる等

漏えい等が発覚した場合の対応

(1) ～ (5) に掲げる事項について必要な措置を講じること

(1) 事業者内部における報告及び被害の拡大防止

(2) 事実関係の調査及び原因の究明

(3) 影響範囲の特定

(4) 再発防止策の検討及び実施

(5) 個人情報保護委員会への報告及び本人への通知

個人情報保護委員会への報告

●個人情報の保護に関する法律施行規則 第7条

法第26 条第1 項本文の個人の権利利益を害するおそれ大きいものとして個人情報保護委員会規則で定めるものは、次の各号のいずれかに該当するものとする。

- (1) 要配慮個人情報に含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下この条及び次条第1 項において同じ。）の漏えい、滅失若しくは毀損（以下この条及び次条第1 項において「漏えい等」という。）が発生し、又は発生したおそれがある事態
- (2) 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
- (3) 不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データ（当該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、個人 データとして取り扱われることが予定されているものを含む。）の漏えい等が発生し、又は発生したおそれがある事態
- (4) 個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

個人情報保護委員会への報告(具体例)

①要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生したおそれがある事態



例 1.

病院における患者の診療情報や調剤情報を含む個人データを記録したUSBメモリーを紛失した場合

例 2.

従業員の健康診断等の結果を含む個人データが漏えいした場合

②不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態



例 1.

ECサイトからクレジットカード番号を含む個人データが漏えいした場合

例 2.

送金や決済機能のあるウェブサービスのログインIDとパスワードの組み合わせを含む個人データが漏えいした場合

個人情報保護委員会への報告(具体例)

③不正の目的をもって行われたおそれがある当該個人情報取扱事業者に対する行為による個人データの漏えい等が発生し、又は発生したおそれがある事態



例 1.

不正アクセスにより個人データが漏えいした場合

例 2.

ランサムウェア等により個人データが暗号化され、復元できなくなった場合

例 3.

個人データが記載又は記録された書類・媒体等が盗難された場合

例 4.

従業員が顧客の個人データを不正に持ち出して第三者に提供した場合

④個人データに係る本人の数が1,000人を超える漏えい等が発生し、又は発生したおそれがある事態



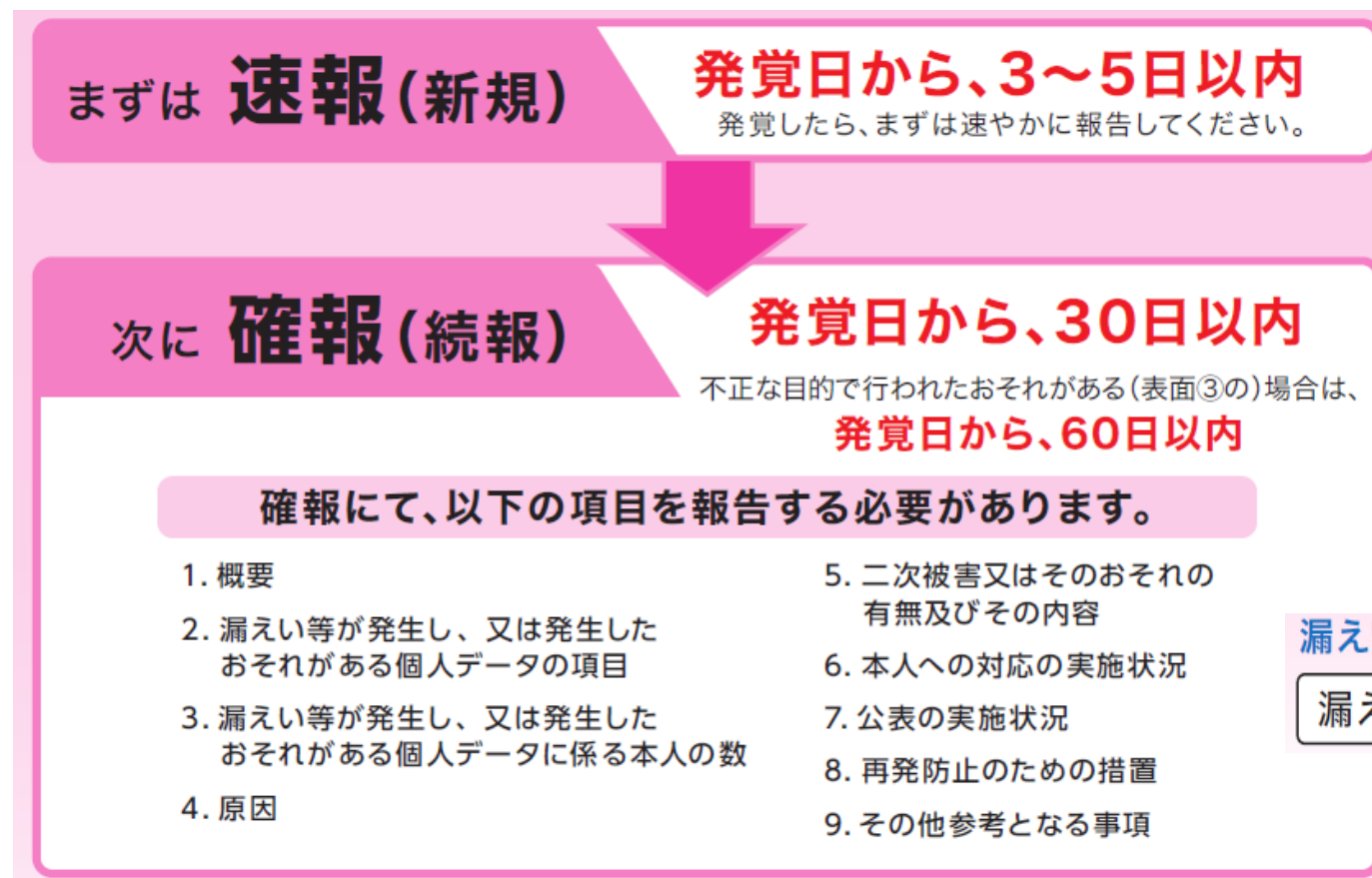
例 1.

システムの設定ミス等によりインターネット上で個人データの閲覧が可能となり、当該個人データに係る本人の数が1,000人を超える場合

例 2.

自社の会員(1,000人超)にメールマガジンの配信を行う際、本来メールアドレスをBCC欄に入力して送信すべきところをCC欄に入力して一括送信した場合

個人情報保護委員会への報告順序



漏えい等報告はHPで受け付けています

漏えい等報告 個人情報委



本人への通知