○個人情報保護委員会告示第　　号

個人情報の保護に関する法律（平成十五年法律第五十七号）の規定に基づき、個人情報の保護に関する法律についてのガイドライン（通則編）（平成二十八年個人情報保護委員会告示第六号）の一部を次のように改正する。

令和八年○月○日　　個人情報保護委員会委員長　手塚　悟

個人情報の保護に関する法律についてのガイドライン（通則編）の一部改正

個人情報の保護に関する法律についてのガイドライン（通則編）（平成二十八年個人情報保護委員会告示第六号）の一部を次のように改正する。

次の表により、改正前欄に掲げる規定の傍線を付し又は破線で囲んだ部分をこれに順次対応する改正後欄に掲げる規定の傍線を付し又は破線で囲んだ部分のように改め、改正前欄及び改正後欄に対応して掲げるその標記部分に二重傍線を付した規定（以下「対象規定」という。）は、その標記部分が同一のものは当該対象規定を改正後欄に掲げるもののように改め、その標記部分が異なるものは改正前欄に掲げる対象規定を改正後欄に掲げる対象規定として移動し、改正前欄に掲げる対象規定で改正後欄にこれに対応するものを掲げていないものは、これを削り、改正後欄に掲げる対象規定で改正前欄にこれに対応するものを掲げていないものは、これを加える。

改　　正　　後	改　　正　　前
個人情報の保護に関する法律についてのガイドライン （通則編） 目次 ［略］ 【凡例】 ［略］ ※　なお、特に断りのない限り、本ガイドラインにおいて示す法令の条番号は、令和９年○月○日時点の条番号を示すものとする。 １～９　［略］ 10　（別添）講ずべき安全管理措置の内容	個人情報の保護に関する法律についてのガイドライン （通則編） 目次 ［同左］ 【凡例】 ［同左］ ※　なお、特に断りのない限り、本ガイドラインにおいて示す法令の条番号は、令和８年６月 14 日時点の条番号を示すものとする。 １～９　［同左］ 10　（別添）講ずべき安全管理措置の内容

［略］

10－１・10－２　［略］

10－３　組織的安全管理措置

［略］

(1)　［略］

(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。

［削除］

(3)　漏えい等事案に対応する体制の整備

［略］

(4)　取扱状況の把握及び安全管理措置の見直し

［略］

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	［略］

［同左］

10－１・10－２　［同左］

10－３　組織的安全管理措置

［同左］

(1)　［同左］

(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。

なお、整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。

(3)　個人データの取扱状況を確認する手段の整備

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。

(4)　漏えい等事案に対応する体制の整備

［同左］

(5)　取扱状況の把握及び安全管理措置の見直し

［同左］

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	［同左］

	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 ・［略］ ・［略］ ・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 ・［略］	
(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	［略］

	責任者の設置及び責任の明確化 ・［同左］ ・［同左］ ・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 ・［同左］	
(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	［同左］

	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消去・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）	

	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 ・利用目的 ・アクセス権を有する者　等				

［削除］	［削除］	［削除］
(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。 ・［略］ ・［略］ ・個人情報保護委員会等関係機関への報告 ・［略］ ・［略］	［略］
(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	［略］

(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。
(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。 ・［略］ ・［略］ ・個人情報保護委員会等への報告 ・［略］ ・［略］	［同左］
(5)取扱状況の把握及び安全管理措置の見直し	［新設］ ・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	［同左］

	は他部署等による監査を実施する。 ・［略］ （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。	

10―４　人的安全管理措置

［略］

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。	［略］

	る。 ・［同左］ ［新設］	

10―４　人的安全管理措置

［同左］

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、従業者に定期的な研修等を行う。 ［新設］	［同左］

	・［略］	

10―５　物理的安全管理措置

［略］

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
［略］	［略］	［略］
(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） ［略］ （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） ・［略］ ・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。	［略］

10－６　技術的安全管理措置

	・［同左］	

10―５　物理的安全管理措置

［同左］

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
［同左］	［同左］	［同左］
(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） ［同左］ （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） ・［同左］ ・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。	［同左］

10－６　技術的安全管理措置

［略］

(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)・(4)　［略］

(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	［略］

［同左］

(1)　アクセス制御

担当者及び取り扱う個人情報データベース等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従業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)・(4)　［同左］

［新設］

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	［新設］ ・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	［同左］

	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			タベース等を限定する。 ［新設］ ・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。 ［新設］ ［新設］ ［新設］	

	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。	
(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。 ・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。	・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テムを使用する従業者を識別・認証する。

	［新設］	
(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 ［新設］	・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。

	・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、			［新設］ ［新設］ ［新設］	

	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。				
(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、アプリケーション等に対するセキュリティ対策	［略］	(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。	［同左］

	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。 ［削除］ ・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。			・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。 ［新設］ ［新設］	
(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。）。	［略］	(4) 情報システムの使用に伴う漏えい等の防止	［新設］ ・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。）。	［同左］

	・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。			［新設］	
	・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。			［新設］	
	（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			［新設］ ・個人データを含む通信の経路又は内容を暗号化する。	

	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。 ・［略］ （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。		・［同左］ ［新設］		
(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	・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	［新設］	［新設］	［新設］

	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	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。			

	トの無効化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　［略］ 【付録】　［略］			10－７　［同左］ 【付録】　［同左］		
備考　表中の［　］の記載は注記である。					

附　則

この告示は、令和九年〇月〇日から施行する。