

○現行の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）及び「個人情報の保護に関する法律についてのガイドライン」に関するQ＆Aの対応関係

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）		「個人情報の保護に関する法律についてのガイドライン」に関するQ＆A
講じなければならない措置		
10-3 組織的安全管理措置		
(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。	(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員及びその役割の明確化 ・上記の従業員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
(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。	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）
(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。	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
(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。	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
(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。	・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。

Q10-10 「個人データの取扱状況を確認する手段の整備」に関して、いわゆる「個人情報取扱台帳」のようなものを作成しなければいけませんか。

A10-10 この項目について、講じていただく必要があるのは、個人データの取扱状況を確認できるように手段を整備することであるため、いわゆる「個人情報取扱台帳」を作成することが義務付けられているわけではありません。

ただし、個人情報取扱事業者において取り扱っている個人データとしてどのようなものがあるかを明確化することは、個人データの取扱状況を把握するに当たって有効な取組であると考えられます。

Q10-11 「取扱状況の把握及び安全管理措置の見直し」について、手法の例示として「監査を実施する」とありますが、実施に当たって参考となるような規格はありますか。

A10-11 例えば、「マネジメントシステム監査指針 JIS Q19011（ISO 19011）」に準拠した監査を行うことが考えられますが、これに限られるわけではありません。

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）		「個人情報の保護に関する法律についてのガイドライン」に関するQ＆A	
講じなければならない措置	手法の例示		
10-4 人的安全管理措置			
○従業員の教育	従業員に、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。	・ 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。	Q10－12 「従業員の教育」について、研修の頻度はどの程度とすることが適切ですか。
		・ 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。	A10－12 研修の頻度は、事業者の規模や取り扱う個人データの性質・量等によっても異なり得るため、それらを踏まえて適切に判断いただく必要がありますが、適切な内容の研修であれば、年1回程度でも少ないとはいえないと考えられます。
			Q10－14 「従業員の教育」としての研修は、全従業員を一堂に集めて講義形式で行う必要がありますか。
			A10－14 個人データの安全管理に関して留意すべき事項は、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よって異なり得ますので、研修の形式も個人情報取扱事業者ごとに異なり得るものと考えられます。全従業員を対象とした講義形式による研修も含まれ得ますが、これに限られるのではなく、部署ごとに個人データの取扱いに関する責任者からの講話形式、eラーニング形式、標的型メールを疑似体験する形での訓練形式など、様々な形式が考えられます。

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）			「個人情報の保護に関する法律についてのガイドライン」に関するQ＆A
講じなければならない措置		手法の例示	
10-5 物理的安全管理措置			
（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。	（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	Q10－15 「個人データを取り扱う区域の管理」に関して、個人データを取り扱う場所は、全て厳格な入退室管理を実施する必要がありますか。 A10－15 個人データを取り扱う区域の管理として、常に入退室管理の実施が求められるわけではありませんが、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（管理区域）については、入退室管理の実施、承認されていない記録媒体やカメラ等の持込の制限等が有効な取組と考えられます。
			Q10－16 「座席配置の工夫」「のぞき込みを防止する措置」「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」とは、例えばどのような措置が該当しますか。 A10－16 具体的には、以下のような措置が該当すると考えられます。 ○ 個人データの取扱いを、個人データを取り扱う権限が付与されていない者の往来が少ない場所で実施すること ○ 個人データをパソコンで取り扱う場合、離席時にパスワード付スクリーンセーバーの起動又はコンピュータのロック等で閲覧できないようにすること ○ 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を机上、社内等に放置しないこと
（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。	・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。	
（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。	・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。	
（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。	（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）			「個人情報の保護に関する法律についてのガイドライン」に関するQ＆A
講じなければならない措置		手法の例示	
10-6 技術的安全管理措置			
(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。	・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。	Q10-18 「アクセス制御」を講じるための手法は、ガイドライン（通則編）で示されている以外にどのようなものが考えられますか。 A10-18 ガイドライン（通則編）に示した手法を具体的に記述したものも含めて、例えば、次のような手法が考えられます。 ○識別に基づいたアクセス制御の実施 ○アクセス権限を有する者に付与する権限の最小化 ○個人データを取り扱う情報システムへのアクセスが必要最小限となるような措置（当該情報システムの同時利用者数の制限、当該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機器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。） ○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、OS・ウェブアプリケーションのぜい弱性有無の検証等。） ○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、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定期的に審査し、その者だけが登録等の作業を行えるようにする等。）
(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。	(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	Q10-19 「アクセス者の識別と認証」を講じるための手法は、ガイドライン（通則編）で示されている以外にどのようなものが考えられますか。 A10-19 ガイドライン（通則編）に示した手法を具体的に記述したものも含めて、例えば、次のような手法が考えられます。 ○（ID・パスワードを利用する場合）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 ○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の実施（例えば、IPアドレス認証、電子証明書等）
(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。	・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。	Q10-20 「外部からの不正アクセス等の防止」を講じるための手法は、ガイドライン（通則編）で示されている以外にどのようなものが考えられますか。 A10-20 ガイドライン（通則編）に示した手法を具体的に記述したものも含めて、例えば、次のような手法が考えられます。 ○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（操作内容も含む。）、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監視（個人データへのアクセスや操作の成功や失敗の記録及び不正が疑われる異常な記録の存否の定期的な確認（当該記録の漏えい、滅失及び毀損並びに改ざん及び不正消去等からの適切な保護も含む）も含む。） ○導入したセキュリティ対策ソフトウェア等の有効性・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確認等。） ○端末及びサーバ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用修正ソフトウェアの適用 ○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の導入防止のための対策
(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。	・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。	Q10-21 「情報システムの使用に伴う漏えい等の防止」を講じるための手法は、ガイドライン（通則編）で示されている以外にどのようなものが考えられますか。 A10-21 ガイドライン（通則編）に示した手法を具体的に記述したものも含めて、例えば、次のような手法が考えられます。 ○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）による個人データの送信（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）時における、個人データの暗号化等の秘匿化（例えば、SSL/TLS、S/MIME 等） ○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等、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こと。 ○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こと ○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