参考資料２

関連法令等

（民間ＰＨＲ事業者による健診等情報の取扱いに関する制度上の要求事項関連）

1. 情報セキュリティ対策

【個人情報の保護に関する法律（平成 15 年法律第 57 号)】

（安全管理措置）

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。

【個人情報の保護に関する法律についてのガイドライン　ー通則編ー】（個人情報保護委員会（平成 28 年 11 月（令和 2 年 10 月一部改正)))

3-3-2 安全管理措置（法第 20 条関係）

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、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、必要かつ適切な措置を講じなければならないが、当該措置は、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しなければならない。具体的に講じなければならない措置や当該項目を実践するための手法の例等については、「8（別添）講ずべき安全管理措置の内容」を参照のこと。

8　（別添）講ずべき安全管理措置の内容

法第 20 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。

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（※１）については、その他の個人情報取扱事業者と同様に、法第 20 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）「中小規模事業者」とは、従業員（※２）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

（※２）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。

8-1　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。

8-2　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。

8-3　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。

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）漏えい等の事案に対応する体制の整備

漏えい等の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、漏えい等の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、漏えい等の事案が発生した場合等の対応の詳細については、別に定める（4（漏えい等の事案が発生した場合等の対応）参照）。

（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。

8-4　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21条に基づき従業者に対する監督をしなければならない（3-3-3（従業者の監督）参照）。

○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。

8-5　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。

8-6　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）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。

【「中小企業における組織的な情報セキュリティ対策ガイドライン」（IPA（情報処理推進機構））

４．共通して実施すべき対策

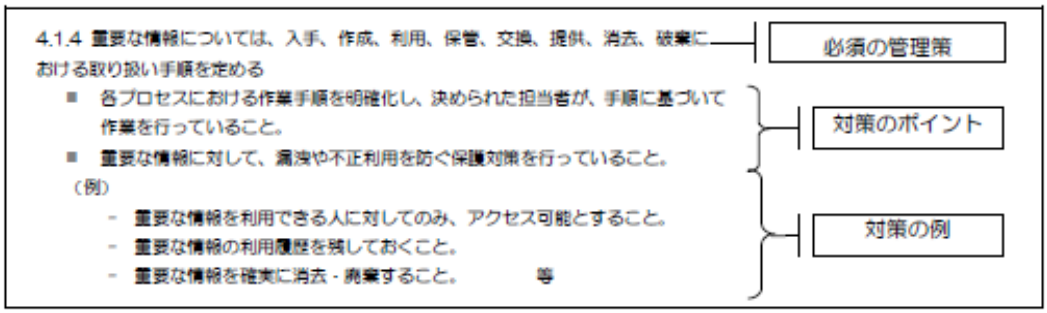
ここでは、中小企業であれば共通して実施すべき対策について示す。ここでは、規模や業種にはよらないが、中小企業の中でも企業として組織的な対策をとりうる企業を念頭においている。

共通して実施すべき対策では、以下の 5 つの分類に従って、管理策をまとめている。

1．情報セキュリティに対する組織的な取り組み：経営者あるいは経営管理者が整備すべき社内的体制や規程類の整備に関する項目
2．物理的セキュリティ：建物や記憶媒体など、物理的な物の管理に関する項目
3．情報システム及び通信ネットワークの運用管理：PC やネットワークなどの管理に関する項目
4．情報システムのアクセス制御の状況及び情報システムの開発、保守におけるセキュリティ対策：情報や情報システムに対するアクセス制御に関する項目と、情報システムの導入時に考慮すべき項目
5．情報セキュリティ上の事故対応：情報セキュリティに関する事故が発生した場合へ

の準備に関する項目

それぞれに記載された対策の読み方であるが、「必須の管理策」が項目番号の直後に記載されており、企業が共通して実施すべき管理策が示されている。ただし、ここで示された管理策を具体的にどのように実現するかは企業にまかされている。そのため、管理策を実現する上での「対策のポイント」を、「必須の管理策」の後に示した。「対策のポイント」が全て満たされないと、「必須の管理策」が実現しないというわけではないが、管理策の実効性を担保するためには、「対策のポイント」と同等程度の対策が実施される必要があることに留意すべきである。



なお、対策のポイントについて、具体的な「対策の例」を適宜示した。

4.1 情報セキュリティに対する組織的な取り組み

4.1.1 情報セキュリティに関する経営者の意図が従業員に明確に示されている

■ 経営者が情報セキュリティポリシーの策定に関与し、実現に対して責任を持つこと。

■ 情報セキュリティポリシーを定期的に見直しすること。

4.1.2 情報セキュリティ対策に関わる責任者と担当者を明示する

■ 責任者として情報セキュリティと経営を理解する立場の人を任命すること。

■ 責任者は、各セキュリティ対策について（社内外を含め）、責任者、担当者それぞれの役割を具体化し、役割を徹底すること。

4.1.3 管理すべき重要な情報資産を区分する

■ 管理すべき重要な情報資産を、他の情報資産と分類すること。

■ 情報資産の管理者を定めること。

■ 重要度に応じた情報資産の取り扱い指針を定めること。

■ 重要な情報資産を利用できる人の範囲を定めること。

4.1.4 重要な情報については、入手、作成、利用、保管、交換、提供、消去、破棄における取り扱い手順を定める

■ 各プロセスにおける作業手順を明確化し、決められた担当者が、手順に基づいて作業を行っていること。

■　重要な情報に対して、漏洩や不正利用を防ぐ保護対策を行っていること。

（例）

- 重要な情報を利用できる人に対してのみ、アクセス可能とすること。
- 重要な情報の利用履歴を残しておくこと。
- 重要な情報を確実に消去・廃棄すること。 等

4.1.5 外部の組織と情報をやり取りする際に、情報の取り扱いに関する注意事項について合意を取る

■　契約書や委託業務の際に取り交わす書面等に、情報の取り扱いに関する注意事項を含めること。

（例）

- システム開発を委託する際の本番データ利用時の際の情報管理、例えば管理体制や受託情報の取り扱い・受け渡し・返却、廃棄等について、注意事項を含めること。
- 関係者のみにデータの取り扱いを制限すること。
- 外部の組織との間で情報を授受する場合、情報受渡書を持っておこなうこと。
- 契約に基づく作業に遂行することによって新たに発生する情報（例：新たに作製された、金型・図面・モックアップ等々）の取扱を含めること。

等

4.1.6 従業者（派遣を含む）に対し、セキュリティに関して就業上何をしなければいけないかを明示する

■　従業者を採用する際に、守秘義務契約や誓約書を交わしていること。

■　従業者が順守すべき事項を明確にしていること。

■　違反を犯した従業員に対する懲戒手続きが整備されていること。

■　在職中及び退職後の機密保持義務を明確化するため、プロジェクトへの参加時など、具体的に企業機密に接する際に、退職後の機密保持義務も含む誓約書を取ること。

4.1.7 情報セキュリティに関するルールの周知と、情報セキュリティに関わる知識習得の機会を与える

■　ポリシーや関連規程を従業員に理解させること。

■　実践するために必要な教育を定期的に行っていること。

4.2 物理的セキュリティ

4.2.1 重要な情報を保管したり、扱ったりする場所の入退管理と施錠管理を行う

■　重要な情報を保管したり、扱ったりする区域を定めていること。

■　重要な情報を保管している部屋（事務室）又はフロアーへの侵入を防止するための対策を行っていること。

■　重要な情報を保管している部屋（事務室）又はフロアーに入ることができる人を制限し、入退の記録を取得していること。

4.2.2 重要なコンピュータや配線は地震などの自然災害や、ケーブルの引っ掛けなどの人

的災害が起こらないように配置・設置する

■　重要なコンピュータは許可された人だけが入ることができる安全な場所に設置すること。

■　電源や通信ケーブルなどは、他の人が容易に接触できないようにすること。

■　重要なシステムについて、地震などによる転倒防止、水濡れ防止、停電時の代替電源の確保などを行っていること。

4.2.3 重要な書類、モバイル PC、記憶媒体などについて、整理整頓を行うと共に、盗難防止対策や確実な廃棄を行う

（重要な書類について）

■　不要になった場合、シュレッダーや焼却などして確実に処分すること。

■　重要な書類を保管するキャビネットには、施錠管理を行うこと。

■　重要な情報が存在する机上、書庫、会議室などは整理整頓を行うこと。

■　郵便物、FAX、印刷物などの放置は禁止。重要な書類の裏面を再利用しないこと。

（モバイル PC、記憶媒体について）

■　保存した情報が不要になった場合、消去ソフトを用いるなど、確実に処分していること。

■　モバイル PC、記憶媒体については、盗難防止の対策を行うこと。

■　私有 PC を会社に持ち込んだり、私有 PC で業務を行ったりしないこと。

4.3 情報システム及び通信ネットワークの運用管理

4.3.1 情報システムの運用に関して運用ルールを策定する

■　システム運用におけるセキュリティ要求事項を明確にしていること。

■　情報システムの運用手順書（マニュアル）を整備していること。

■　システムの運用状況を点検していること。

■　システムにおいて実施した操作や障害、セキュリティ関連イベントについてログ（記録）を取得していること。

■　設備（具体例）の使用状況を記録していること。

4.3.2 ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行う

■　ウイルス対策ソフトを導入し、パターンファイルの更新を定期的に行っていること。

■　ウイルス対策ソフトが持っている機能（ファイアーウォール機能、スパムメール対策機能、有害サイト対策機能）を活用すること。

■　各サーバやクライアント PC について、定期的なウイルス検査を行っていること。

■　Winny 等、組織で許可されていないソフトウェアのインストールの禁止、あるいは使用制限を行っていること。

4.3.3 導入している情報システムに対して、最新のパッチを適用するなどの脆弱性対策を行う

■　脆弱性の解消（修正プログラムの適用、Windows update 等）を行っていること。

■　脆弱性情報や脅威に関する情報の入手方法を確認し、定期的に収集すること。

■　情報システム導入の際に、不要なサービスの停止など、セキュリティを考慮した設定を実施するなどの対策が施されているかを確認すること。

■　Web サイトの公開にあたっては、不正アクセスや改ざんなどを受けないような設定・対策を行い、脆弱性の解消を行うこと。

■　Web ブラウザや電子メールソフトのセキュリティ設定を行うこと。

4.3.4 通信ネットワークを流れる重要なデータに対して、暗号化などの保護策を実施する

■　必要に応じて、SSL 等を用いて通信データを暗号化すること。

■　外部のネットワークから内部のネットワークや情報システムにアクセスする場合に、VPN などを用いて暗号化した通信路を使用していること。

■　電子メールをやり取りする際に、重要な情報についてはファイルにパスワードを付ける、又は暗号化すること。

4.3.5 モバイル PC や USB メモリなどの記憶媒体やデータを外部に持ち出す場合､盗難、紛失などに備えて、適切なパスワード設定や暗号化などの対策を実施する

■　モバイル PC や USB メモリ等の使用や外部持ち出しについて、規程を定めていること。

■　外部でモバイル PC や USB メモリ等を使用する場合の紛失や盗難対策を講じていること。

■　モバイル PC や USB メモリ等を外部に持出す際は、利用者の認証（ID・パスワード設定、USB キーや IC カード認証、バイオメトリクス認証等）を行うこと。

■　保存されているデータを、重要度に応じて HDD 暗号化、BIOS パスワード設定などの技術的対策を実施すること。

■　PC を持出す場合の持出者、持出・返却管理を実施すること。

■　盗難、紛失時に情報漏えいの脅威にさらされた情報が何かを正確に把握するため、持ち出し情報の一覧、内容管理を行うこと。

4.4 情報システムのアクセス制御の状況及び情報システムの開発､保守におけるセキュリティ対策

4.4.1 情報（データ）や情報システムへのアクセスを制限するために、利用者 ID の管理（パスワードの管理など）を行う

■　利用者毎に ID とパスワードを割当て、その ID とパスワードによる識別と認証を確実に行うこと。

■　利用者 ID の登録や削除に関する規程を整備すること。

■　パスワードの定期的な見直しを求めること。また、空白のパスワードや単純な文字列のパスワードを設定しないよう利用者に求めること。

■　離席する際は、パスワードで保護されたスクリーンセーバーでパソコンを保護す

ること。

■　不要になった利用者 ID を削除すること。

4.4.2 重要な情報に対するアクセス権限の設定を行う

■　重要な情報に対するアクセス管理方針を定め、利用者毎にアクセス可能な情報、情報システム、業務アプリケーション、サービス等を設定すること。

■　職務の変更や異動に際して、利用者のアクセス権限を見直すこと。

4.4.3 インターネット接続に関わる不正アクセス対策（ファイアウォール機能、パケットフィルタリング、ISP サービス 等）を行う

(外部から内部へのアクセス)

■　外部から内部のシステムにアクセスする際、利用者認証を実施すること。

■　保護すべき重要な情報が保存されるシステムは、それ以外のシステムが接続しているネットワークから物理的に遮断する、もしくはセグメント分割することによりアクセスできないようにすること。

(内部から外部へのアクセス)

■　不正なプログラムをダウンロードさせる恐れのあるサイトへのアクセスを遮断するような仕組み（フィルタリングソフトの導入等）を行っていること。

4.4.4 無線 LAN のセキュリティ対策（WPA2 の導入等）を行う

■　無線 LAN において重要な情報の通信を行う場合は、暗号化通信（WPA2 等）の設定を行うこと。

■　無線 LAN の使用を許可する端末（MAC 認証）や利用者の認証を行うこと。

4.4.5 ソフトウェアの選定や購入、情報システムの開発や保守に際して、情報セキュリティを前提とした管理を行う

■　ソフトウェアの導入や変更に関する手順を整備していること。

■　システム開発において、レビューの実施と記録を残していること。

■　外部委託によるソフトウェア開発を行う場合、使用許諾、知的所有権などについて取り決めていること。

■　開発や保守を外部委託する場合に、セキュリティ管理の実施状況を把握できること。

4.5 情報セキュリティ上の事故対応

4.5.1 情報システムに障害が発生した場合、業務を再開するために何をすべきかを把握する

■　情報システムに障害が発生した場合の、最低限運用の必要な時間帯と許容停止時間を明確にしておくこと。

■　障害対策の仕組みが組織として効果的に機能するよう、よく検討していること。

■　システムの切り離し（即応処理)、必要なサービスを提供できるような機能（縮退機能)、情報の回復や情報システムの復旧に必要となる機能などが、障害時に円滑に

機能するよう確認しておくこと。

■　日常のシステム運用の中で、バックアップデータや運用の記録などを確保しておくこと。

■　障害発生時に必要な対応として、障害発生時の報告要領（電話連絡先の認知等）、障害対策の責任者と対応体制、システム切替え・復旧手順、障害発生時の業務実施要領等の準備を整えておくこと。

（例）

- 大容量データの復元には時間を要するため、復元に要する時間の事前見積りの実施。

■　関係者への障害対応要領の周知や、必要なスキルに関する教育や訓練などの実施を行っていること。

4.5.2 情報セキュリティに関連する事件や事故等（ウイルス感染、情報漏えい等）の緊急時に、何をすべきかを把握する

■　ウイルス感染や情報漏えい等の発生時、組織内の関係者への報告、緊急処置の適用基準や実行手順、被害状況の把握、原因の把握と対策の実施、被害者への連絡や外部への周知方法、通常システムへの復旧手順、業務再開手順などを整えておくこと。

（例）

- ウイルス感染の場合、ウイルス定義ファイルを最新の状態にしたワクチンソフトにより、コンピュータの検査を実施し、ワクチンソフトのベンダの Web サイト等の情報を基に、検出されたウイルスの駆除方法などを試すことが必要となる。
- 情報漏えいの場合、事実を確認したら速やかに責任者に報告し、対応体制を取ること、対応についての判断を行うため 5W1H の観点で調査し情報を整理すること、対策本部で対応方針を決定すること、被害の拡大防止と復旧のための措置を行うことが必要となる。また、漏洩した個人情報の本人、取引先などへの通知、監督官庁等への報告、ホームページやマスコミ等による公表についても検討する必要がある。

2. 個人情報の適切な取扱い

【個人情報の保護に関する法律（平成 15 年法律第 57 号）】

第 15 条　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

第 16 条　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない

2・3　（略）

第 17 条　（略）

2　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

五　当該要配慮個人情報が、本人、国の機関、地方公共団体、第七十六条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合

六　その他前各号に掲げる場合に準ずるものとして政令で定める場合

第 18 条　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

2　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

3・4　（略）

第 19 条　個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

第 22 条　個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

第 23 条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

2　個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

五　本人の求めを受け付ける方法

3・4　（略）

5　次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　特定の者との間で共同して利用される個人データが当該特定の者に提供される場合

であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

第 30 条　本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データが第十六条の規定に違反して取り扱われているとき又は第十七条の規定に違反して取得されたものであるときは、当該保有個人データの利用の停止又は消去（以下この条において「利用停止等」という。）を請求することができる。

2　個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

3～5　（略）

第 35 条　個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

2　個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

【令和 2 年 改正個人情報保護法（個人情報の保護に関する法律等の一部を改正する法律（令和 2 年法律第 44 号）。全面施行は交付日（令和 2 年 6 月 12 日）から起算して 2 年を超えない範囲内において政令で定める日。）】

第 30 条　1～4　（略）

5　本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データを当該個人情報取扱事業者が利用する必要がなくなった場合、当該本人が識別される保有個人データに係る第 22 条の 2 第 1 項本文に規定する事態が生じた場合その他当該本人が識別される保有個人データの取扱いにより当該本人の権利又は正当な利益が害されるおそれがある場合は、当該保有個人データの利用停止等又は第三者への提供の停止を請求することができる。

6　個人情報取扱事業者は、前項の規定による請求を受けた場合であって、その請求に理由があることが判明したときは、本人の権利利益の侵害を防止するために必要な限度で、遅滞なく、当該保有個人データの利用停止等又は第三者への提供の停止を行わなければならない。ただし、当該保有個人データの利用停止等又は第三者への提供の停止に多額の費用を要する場合その他の利用停止等又は第三者への提供の停止を行うことが困難な場合

であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

【個人情報の保護に関する法律についてのガイドライン　ー通則編ー】（個人情報保護委員会（平成 28 年 11 月（令和 2 年 10 月一部改正））

3-1-1 利用目的の特定（法第 15 条第 1 項関係）

個人情報取扱事業者は、個人情報を取り扱うに当たっては、利用目的をできる限り具体的に特定しなければならないが、利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報が個人情報取扱事業者において、最終的にどのような事業の用に供され、どのような目的で個人情報を利用されるのかが、本人にとって一般的かつ合理的に想定できる程度に具体的に特定することが望ましい。

なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的の特定に当たっては、その旨が明確に分かるよう特定しなければならない（3-4-1（第三者提供の制限の原則）参照)。

3-1-2 利用目的の変更（法第 15 条第 2 項、第 18 条第 3 項関係）

上記 3-1-1（利用目的の特定により特定した利用目的は、変更前の利用目的と関連性を有すると合理的に認められる範囲、すなわち、変更後の利用目的が変更前の利用目的からみて、社会通念上、本人が通常予期し得る限度と客観的に認められる範囲内（※１）で変更することは可能である。変更された利用目的は、本人に通知するか、又は公表しなければならない。

なお、特定された利用目的（法第 15 条第 2 項に定める範囲で変更された利用目的を含む。）の達成に必要な範囲を超えて個人情報を取り扱う場合は、法第 16 条第 1 項に従って本人の同意を得なければならない。ただし、本人の身体等の保護のために必要があり、かつ本人の同意を得ることが困難である場合等、法第 16 条第 3 項各号に掲げる場合には、あらかじめ本人の同意を得ることなく、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことができる（3-1-5（利用目的による制限の例外）参照)。

（※１）「本人が通常予期し得る限度と客観的に認められる範囲」とは、本人の主観や事業者の恣意的な判断によるものではなく、一般人の判断において、当初の利用目的と変更後の利用目的を比較して予期できる範囲をいい、当初特定した利用目的とどの程度の関連性を有するかを総合的に勘案して判断される。

3-1-3 利用目的による制限（法第 16 条第 1 項関係）

個人情報取扱事業者は、法第 15 条第 1 項により特定した利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければならない。

ただし、当該同意を得るために個人情報を利用することメールの送信や電話をかけること等は、当初特定した利用目的として記載されていない場合でも、目的外利用には該当しな

い。

3-2-4 直接書面等による取得（法第 18 条第２項関係）

【利用目的の明示に該当する事例】

事例１）利用目的を明記した契約書その他の書面を相手方である本人に手渡し、又は送付する場合

なお、契約約款又は利用条件等の書面（電磁的記録を含む。）中に利用目的条項を記載する場合は、例えば、裏面約款に利用目的が記載されていることを伝える、又は裏面約款等に記載されている利用目的条項を表面にも記載し、かつ、社会通念上、本人が認識できる場所及び文字の大きさで記載する等、本人が実際に利用目的を確認できるよう留意することが望ましい。

3-6 個人情報の取扱いに関する苦情処理（法第 35 条関係）

個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

また、苦情の適切かつ迅速な処理を行うに当たり、苦情処理窓口の設置や苦情処理の手順を定める等必要な体制の整備に努めなければならない（※１）。もっとも、無理な要求にまで応じなければならないものではない。

（略）

（※１）消費者等本人との信頼関係を構築し事業活動に対する社会の信頼を確保するためには、「個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等)」を策定し、それをホームページへの掲載又は店舗の見やすい場所への掲示等により公表し、あらかじめ、対外的に分かりやすく説明することや、委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めることも重要である。

【「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ】（個人情報保護委員会（平成 29 年２月 16 日（令和２年９月１日更新））

Ａ３－12－２

…現行の個人情報保護法では、個人情報取扱事業者は、保有個人データを法第 16 条の規定に違反して取り扱っている場合又は法第 17 条の規定に違反して取得した場合でなければ、当該保有個人データの利用の停止又は消去の請求に応じる義務はありませんが、顧客から寄せられた冊子や電子メールの送付の停止等の要求を苦情として扱った上で、適切かつ迅速に処理するよう努めなければならず（法第 35 条第１項)、令和２年改正法（未施行）において利用の停止又は消去の請求の要件が緩和されたことにより将来的には対応が必要

になる場合があることも踏まえ、適切に利用停止又は消去の請求に応じることが望ましいと考えられます。…

Ａ５－９

提供先を個別に明示することまでが求められるわけではありません。もっとも、想定される提供先の範囲や属性を示すことは望ましいと考えられます。

3. 健診等情報の保存・管理、相互運用性の確保

【個人情報の保護に関する法律（平成 15 年法律第 57 号)】

第 19 条　個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

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。

第 28 条　本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの開示を請求することができる。

2　個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。

一　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

二　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

三　他の法令に違反することとなる場合

【「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ】（個人情報保護委員会（平成 29 年２月 16 日（令和２年９月１日更新））

3-3-1 データ内容の正確性の確保 等（法第 19 条関係）

個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つよう努めなければならない 。

なお、保有する個人データを一律に又は常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すれば足りる。

また、個人情報取扱事業者は、保有する個人データについて利用する必要がなくなったとき、すなわち、利用目的が達成され当該目的との関係では当該個人データを保有する合理的な理由が存在しなくなった場合や、利用目的が達成されなかったものの当該目的の前提となる事業自体が中止となった場合等は、当該個人データを遅滞なく消去するよう努めなければならない。なお、法令の定めにより保存期間等が定められている場合は、この限りではない。

4. その他

【個人情報の保護に関する法律（平成 15 年法律第 57 号)】

（定義）

第２条　（略）

２　（略）

３　この法律において「要配慮個人情報」とは、本人の人種、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その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

４～12　（略）

【個人情報の保護に関する法律施行令（平成 15 年政令第 507 号)】

（要配慮個人情報）

第２条　法第二条第三項の政令で定める記述等は、次に掲げる事項のいずれかを内容とする記述等（本人の病歴又は犯罪の経歴に該当するものを除く。）とする。

一　身体障害、知的障害、精神障害（発達障害を含む。）その他の個人情報保護委員会規則で定める心身の機能の障害があること。

二　本人に対して医師その他医療に関連する職務に従事する者（次号において「医師等」という。）により行われた疾病の予防及び早期発見のための健康診断その他の検査（同号において「健康診断等」という。）の結果

三　健康診断等の結果に基づき、又は疾病、負傷その他の心身の変化を理由として、本人に対して医師等により心身の状態の改善のための指導又は診療若しくは調剤が行われたこと。

四　本人を被疑者又は被告人として、逮捕、捜索、差押え、勾留、公訴の提起その他の刑事事件に関する手続が行われたこと。

五　本人を少年法（昭和二十三年法律第百六十八号）第三条第一項に規定する少年又はその疑いのある者として、調査、観護の措置、審判、保護処分その他の少年の保護事件に関する手続が行われたこと。