個人情報保護法
ハンドブック

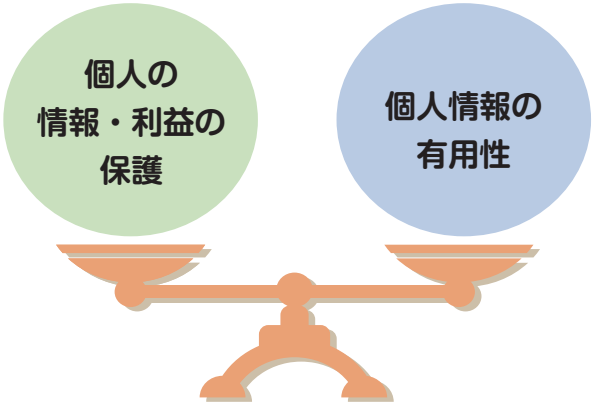
個人情報保護委員会

目　次

1 個人情報保護法

（1）個人情報保護法

個人情報の保護に関する法律（以下、個人情報保護法といいます。）は、利用者や消費者が安心できるように、企業や団体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です。（平成 15 年 5 月に公布、平成 17 年 4 月に全面施行されました。）



POINT!

個人情報保護法の下に、「個人情報の保護に関する法律施行令（以下「政令」といいます。）」や「個人情報の保護に関する法律施行規則（以下「規則」といいます。）」がありますが、これらを解説した資料として、「個人情報の保護に関する法律についてのガイドライン」を公表しています。

個人情報の取扱いについて詳しく確認したい場合には、ガイドラインをご参照ください。

（2）個人情報保護法の改正

情報通信技術の発展や事業活動のグローバル化等の急速な環境変化等を踏まえ、平成 27 年 9 月に改正法が公布され、平成 29 年 5 月 30 日から全面施行されました。

改正前の個人情報保護法では、5000 人以下の個人情報しか有しない中小企業・小規模事業者の方は適用対象外となっていました。

しかし、法改正によりこの規定は廃止され、個人情報を取り扱う「すべての事業者」に個人情報保護法が適用されることとなりました。

（3）「すべての事業者」って？

取り扱う個人情報の数に関わらず、例えば、紙やデータで名簿を管理されている事業者は、すべて「個人情報取扱事業者」となり、法の対象になります。

「事業者」には、法人に限らず、マンションの管理組合、NPO 法人、自治会や同窓会などの非営利組織も含まれます。

小規模の事業者の事業が円滑に行われるように配慮することとされており、安全管理措置については、従業員の数が 100 人以下の中小規模事業者（一部の事業者を除く。）に対して、特例的な対応方法が示されています。（「3 － 2　個人データの安全管理措置」を CHECK!）

2 個人情報

改正個人情報保護法に規定された、「個人情報」や「個人識別符号」などの用語について説明します。

☑「個人情報」とは

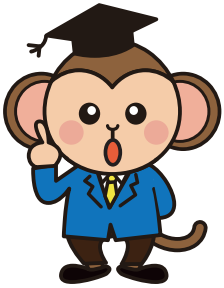
個人情報とは、生存する個人に関する情報であって、氏名や生年月日等により特定の個人を識別することができるものをいいます。

個人情報には、他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものも含みます。

POINT!

たとえば、「氏名」のみであっても、社会通念上、特定の個人を識別することができるものと考えられますので、個人情報に含まれます。また、「生年月日と氏名の組合せ」、「顔写真」なども個人情報です。

個人識別符号も個人情報に当たります。



☑「個人識別符号」とは

改正法においては、個人情報の定義の明確化を図るため、その情報だけでも特定の個人を識別できる文字、番号、記号、符号等について、「個人識別符号」という定義を設けました。個人識別符号は、政令や規則で限定的に列挙されています。

たとえば、以下のものが「個人識別符号」に当たります。

①生体情報を変換した符号として、DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋

②公的な番号として、パスポート番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証等

☑「個人情報データベース等」、「個人データ」、「保有個人データ」とは

個人情報をデータベース化したり、検索可能な状態にしたものを「個人情報データベース等」といいます。

「個人情報データベース等」を構成する情報が「個人データ」です。

「個人データ」のうち、事業者に修正、削除等の権限があるもので、6ヶ月以上保有するものを「保有個人データ」といいます。

「個人情報データベース等」を事業のために使っている者が「個人情報取扱事業者」であり、個人情報保護法の対象となります。また、個人情報取扱事業者は、本人から「保有個人データ」の開示請求を受けたときは、本人に対し、原則として当該保有個人データを開示しなければならないとされています。（3－4「保有個人データの開示請求」を CHECK ！）

③ 守るべき４つの基本ルール

個人情報保護法では、民間事業者の個人情報の取扱いについて、４つの基本ルールを規定しています。

③－１　個人情報の取得・利用

個人情報取扱事業者は、個人情報を取り扱うに当たって、利用目的をできる限り特定しなければならないとされています（個人情報保護法第 15 条第１項）。

その際、利用目的はできるだけ具体的に特定しましょう。

また、特定した利用目的は、あらかじめ公表しておくか、個人情報を取得する際に本人に通知する必要があります。

POINT!

個人情報を書面で取得する場合は、利用目的を本人に明示する必要があります（個人情報保護法第 18 条第２項）。

なお、取得の状況から見て利用目的が明らかである場合は、通知・公表する必要はありません（個人情報保護法第 18 条第４項第４号）。

例えば、商品配送のために配送伝票に氏名・住所等を記載してもらう場合は、利用目的が明らかなため、取得の際の通知・公表の必要はありません。

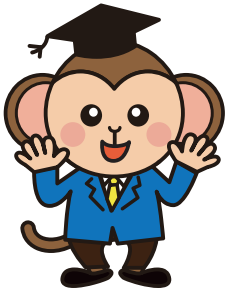
取得した個人情報は、特定した利用目的の範囲内で利用する必要があります。

特定した利用範囲以外のことに利用する場合は、あらかじめ本人の同意を得なければなりません（個人情報保護法第 16 条第 1 項）。

POINT!

個人データは、利用目的の達成に必要な範囲内において、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、当該データを遅滞なく消去するように努めなければならないとされています（個人情報保護法第 19 条）。

例えば、キャンペーンの懸賞品送付のために保有していた応募者の個人データは、懸賞品の発送が終わり、不着対応等のための合理的な期間が経過した場合は、利用する必要がなくなったときに該当すると考えられます。



☑「要配慮個人情報」とは

「要配慮個人情報」は、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要する情報として、法律・政令・規則に定められた情報です。

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、捜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します。

要配慮個人情報を取得する場合は、利用目的の特定、通知又は公表に加え、あらかじめ本人の同意が必要です。

また、要配慮個人情報は、オプトアウトによる第三者提供はできないので注意が必要です。（「３－３個人データの第三者提供」の「オプトアウト」を CHECK ！）

③-2　個人データの安全管理措置

個人情報取扱事業者は、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とされています（個人情報保護法第20条）。

POINT!

漏えい等が生じないよう、安全に管理するほか、業者・委託先にも安全管理を徹底する必要があります。

（1）安全管理の方法について

個人データの安全管理のため講じなければならない措置は、個人データが漏えい等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、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る必要があります。

POINT!

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、基本方針や個人データの取扱いに係る規定を策定することが重要です。

また、その他、具体的な講ずるべき措置は、以下のものがあります。

組織的安全管理措置	・組織体制の整備 ・個人データの取扱いに係る規律に従った運用 ・個人データの取扱状況を確認する手段の整備 ・漏えい等の事案に対応する体制の整備 ・取扱状況の把握及び安全管理措置の見直し
人的安全管理措置	・従業者の教育
物理的安全管理措置	・個人データを取り扱う区域の管理 ・機器及び電子媒体等の盗難等の防止 ・電子媒体等を持ち運ぶ場合の漏えい等の防止 ・個人データの削除及び機器、電子媒体等の廃棄
技術的安全管理措置	・アクセス制御 ・アクセス者の識別と認証 ・外部からの不正アクセス等の防止 ・情報システムの使用に伴う漏えい等の防止

（2）小規模事業者に対する特例について

小規模の事業者の事業が円滑に行われるように配慮することとされており、安全管理措置については、従業員の数が 100 人以下の中小規模事業者（一部の事業者を除く。）に対して、ガイドラインにおいて特例的な対応方法が示されています。

POINT!

取り扱う個人情報の性質や量等によりますが、例えば、

- 個人情報の取扱いの基本的なルールを決める
- 従業者を教育する
- 紙で管理している場合は、鍵のかかる引き出しに保管する
- パソコン等で管理している場合は、ファイルにパスワードを設定する
- パソコンにセキュリティ対策ソフトウェアを導入する

などの手法が考えられます。

③-3　個人データの第三者提供

個人情報取扱事業者は、個人データを第三者に提供する場合、原則としてあらかじめ本人の同意を得なければなりません（個人情報保護法第 23 条第 1 項）。

また、第三者に個人データを提供した場合、第三者から個人データの提供を受けた場合は、一定事項を記録する必要があります（個人情報保護法第 25 条、26 条）。

ただし、以下のような場合は例外的に、第三者提供の本人の同意が不要になります。

○法令に基づく場合（例：警察、裁判所、税務署等からの照会）

○人の生命・身体・財産の保護に必要（本人同意取得が困難）
（例：災害時の被災者情報の家族・自治体等への提供）

○公衆衛生・児童の健全育成に必要（本人同意取得が困難）
（例：児童生徒の不登校や、児童虐待のおそれのある情報を関係機関で共有）

○国の機関等の法令の定める事務への協力
（例：国や地方公共団体の統計調査等への回答）

○委託、事業承継、共同利用

POINT!

○基本的な記録事項は、以下のとおりです。
記録の保存期間は原則３年です。

（提供した場合）
「いつ・誰の・どんな情報を・誰に」提供したかについて記録しなければなりません。

（提供を受けた場合）
「いつ・誰の・どんな情報を・誰から」提供されたかの記録に加えて、「相手方の取得経緯」についても記録しなければなりません。
ただし、一般的なビジネスの実態に配慮して、例外規定があります。

○本人との契約等に基づいて提供した場合は、記録は契約書で代替ＯＫです。
○反復継続して提供する場合は、包括的な記録でＯＫです。
○例外規定に加え、以下の場合には記録義務はかかりません。

・本人による提供と整理できる場合（例：SNS での個人の投稿）
・本人に代わって提供していると整理できる場合（例：銀行振込）
・本人側への提供と整理できる場合（例：同席している家族への提供）
・「個人データ」に該当しないと整理できる場合（例：名刺１枚のコピー）　等

☑「オプトアウト」とは

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場合、本人の同意を得ることなく第三者に個人データを提供することができる制度です。（個人情報保護法第 23 条第 2 項）

POINT!

オプトアウトにより個人データを第三者に提供する場合は、必要な事項を委員会に届け出なければなりません。

委員会は、届け出のあった事項を公表することとなっており、委員会のウェブサイトで、オプトアウトを行っている事業者や、第三者提供されている個人データ項目などを確認することで、本人が当該第三者提供の停止を求めることができます。

POINT!

外国にある第三者に個人データを提供する場合は、次の①～③のいずれかを満たす必要があります（個人情報保護法第 24 条）。

①外国にある第三者に提供することについて、本人の同意を得る。
②外国にある第三者が、適切な体制を整備している（※）。
③外国にある第三者が個人情報保護委員会が認めた国に所在している。

（※）具体的には、以下が該当します。

○外国の第三者において、個人情報保護法の趣旨に沿った措置を実施することが、委託契約・共通の内規・個人データを提供する者が APEC 越境プライバシールール（CBPR）システムの認定を受ける等によって担保されていること
○外国の第三者が個人情報の取扱いに関する国際的な枠組み（例：APEC 越境プライバシールール（CBPR）システム）に基づく認定を受けていること

（※）APEC 越境プライバシールール（CBPR）システムとは、APEC 域内における個人データ越境移転を円滑にする仕組みです。

事業者が、自社の越境個人情報保護に関するルール、体制等に対して自己審査を行い、その内容について、予め APEC から認定された認証団体（アカウンタビリティ・エージェント）から審査を受け、認証を得ると、認証を受けた事業者は、APEC 域内で個人データ越境移転を円滑に行うことができます。日本は平成 26 年 4 月に CBPR システムに参加し、平成 28 年 1 月には、APEC CBPR システムの認証団体として我が国で初めて一般財団法人日本情報経済社会推進協会（JIPDEC) が認定されました。

③－4　保有個人データの開示請求

個人情報取扱事業者は、本人から保有個人データの開示請求を受けたときは、本人に対し、原則として当該保有個人データを開示しなければならないとされています（個人情報保護法第 28 条）。

また、個人情報の取扱いに関する苦情等には、適切・迅速に対応するよう努めることが必要です（個人情報保護法第 35 条）。

POINT!

一時的に保有しているにすぎない個人情報（＝半年以内に消去するもの）や、他の事業者からデータ編集作業のみを委託されて取り扱っているだけの個人情報（＝開示等の権限がないもの）は、対応は不要です。

以下の①～⑤について、「本人が知り得る状態」に置く必要があります。

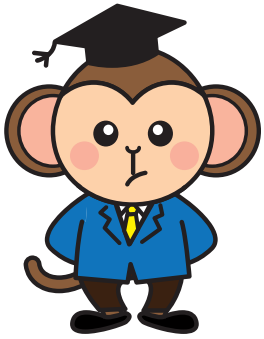
方法については、HP 公表、事業所での掲示等です。

また、それらを行わず、以下の事項に関する問合せに対して遅滞なく答えられるようにしておくことでもよいです。

①事業者の名称、②利用目的、③請求手続、④苦情申出先、
⑤加入している認定個人情報保護団体の名称・苦情申出先
（※⑤は認定個人情報保護団体に加入している場合のみ）

POINT!

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、対外的にわ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す。



4 匿名加工情報

☑「匿名加工情報」とは

匿名加工情報とは、個人情報を本人が特定できないように加工をしたもので、当該個人情報を復元できないようにした情報をいいます。個人情報の取扱いよりも緩やかな規律の下、自由な流通・利活用を促進することを目的に個人情報保護法の改正により新たに導入されました。

匿名加工情報の作成方法の基準は、個人情報保護委員会規則で定められています。これを最低限の規律とし、民間事業者の自主的なルールの策定が期待されます。

このような基準に則って匿名加工情報を作成した場合は、当該匿名加工情報に含まれる個人に関する情報の項目を公表する義務があります（個人情報保護法第 36 条）。

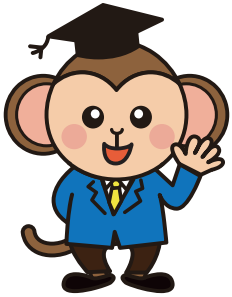
匿名加工情報を第三者に提供する場合は、あらかじめ、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供方法を公表するとともに、提供する情報が匿名加工情報である旨を明示する必要があります（個人情報保護法第 36 条第 4 項、第 37 条）。

POINT!

事業者において、匿名加工情報を再度識別することは禁止されています（個人情報保護法第 38 条）。

POINT!

匿名加工情報は、例えば、ネットワークにつながった車の走っている位置とワイパーの動きに関するデータを集めて分析し、ゲリラ豪雨など局地的な天候の変化をリアルタイムで把握することなど、様々な活用が期待されています。



5 認定個人情報保護団体

☑「認定個人情報保護団体」とは

認定個人情報保護団体とは、事業者の個人情報の適切な取扱いの確保を目的として、国の認定を受けた民間団体です。

認定個人情報保護団体は、業界の特性等に応じた自主的なルール（「個人情報保護指針」）を作成するよう努める義務があり、また、対象事業者が指針を遵守するよう指導・勧告を行う義務があります（個人情報保護法第 53 条）。

また、認定個人情報保護団体は、対象事業者の個人情報の取扱いに関する苦情を処理する義務があります（個人情報保護法第 52 条）。

6 適用除外

憲法が保障する基本的人権への配慮から、
①報道機関が報道の用に供する目的
②著述を業として行う者が著述の用に供する目的
③学術研究機関等が学術研究の用に供する目的
④宗教団体が宗教活動の用に供する目的
⑤政治団体が政治活動の用に供する目的
で個人情報を取り扱う場合には、個人情報取扱事業者の義務は適用されないこととされています(個人情報保護法第 76 条第 1 項)。

また、これらの者に個人情報を提供する行為には、個人情報保護委員会はその権限を行使しないこととされています（個人情報保護法第 43 条第 2 項)。

7 個人データの漏えい等

個人情報取扱事業者には、「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」（平成 29 年委員会告示第１号）に基づく措置が求められています。

個人データの漏えい等の事案が発覚した場合に講ずるべき措置としては、①事業者内部における報告、被害の拡大防止、②事実関係の調査、原因の究明、③影響範囲の特定、④再発防止策の検討・実施、⑤影響を受ける可能性のある本人への連絡等、⑥事実関係、再発防止策の公表があげられています。

また、内容によって、個人情報保護委員会等への報告が求められています。

POINT!

漏えい等とは、漏えい、滅失又は毀損のことをいいます。

8 罰則

国は事業者に対して、必要に応じて報告を求めたり立入検査を行うことができます。

また、実態に応じて、指導・助言、勧告・命令を行うことができます。

監督に従わない場合は、罰則が適用される可能性があります。

POINT!

国からの命令に違反	6 か月以下の懲役又は 30 万円以下の罰金
虚偽の報告	30 万円以下の罰金
従業員が不正な利益を図る目的で個人情報データベース等を提供・盗用	1 年以下の懲役又は 50 万円以下の罰金（法人にも罰金）

9 個人情報保護委員会

（1）個人情報保護委員会の監視・監督権限

個人情報保護委員会は、個人情報、匿名加工情報の適正な取扱いに向けた取組みを行っており、個人情報保護法に違反する、又は違反するおそれがある場合に、立入検査をし、指導･助言や勧告･命令をすることができます。

その場合、個人情報保護委員会の命令に従わなければ、罰則の適用もあり得ます。

（2）個人情報保護法相談ダイヤル

個人情報保護委員会では、個人情報保護法の解釈についての一般的な質問や、苦情あっせんのための個人情報保護法相談ダイヤルを設置しています。

個人情報保護法相談ダイヤル

☎ 03-6457-9849

受付時間　土日祝日及び年末年始を除く　9:30 ～ 17:30

POINT!

個人情報保護法について、もっと詳しく知りたい方は、

・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・外国第三者提供編・確認記録義務編・匿名加工情報編）

・金融分野における個人情報保護に関するガイドライン

・医療関連分野における個人情報の適切な取扱いのためのガイダンス

・匿名加工情報に関する事務局レポート「パーソナルデータの利活用促進と消費者の信頼性確保の両立に向けて」

・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

を個人情報保護委員会のウェブサイトに掲載していますのでご参照ください。

また、中小企業の方向けにわかりやすい資料を掲載した「中小企業サポートページ」、認定個人情報保護団体に関する資料を掲載した「認定個人情報保護団体ページ」もご活用ください。

詳しくは・・・　個人情報保護委員会
https://www.ppc.go.jp/