はじめての個人情報保護法

～シンプルレッスン～

平成29年3月
個人情報保護委員会事務局

目次

はじめに

１．「個人情報」とは

２．基本的な４つのルール

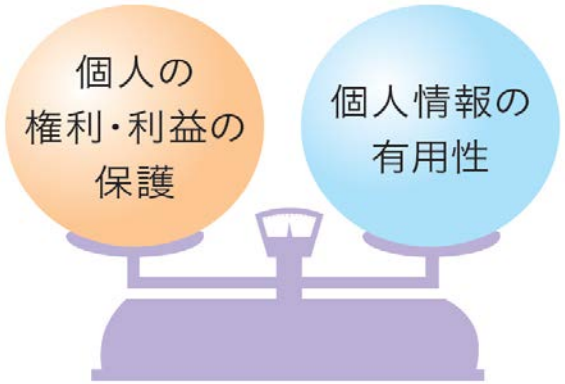
３．（１）取得・利用に関するルール
（２）保管に関するルール
（３）提供に関するルール
（４）本人からの開示請求等に関するルール

（参考）　罰則
匿名加工情報
認定個人情報保護団体
個人情報保護法質問ダイヤル等

平成29年5月30日から、すべての事業者に「個人情報保護法」が適用されます！

？ 個人情報保護法とは？

- ✓ 個人の権利・利益の保護と個人情報の有用性とのバランスを図るための法律
- ✓ 民間事業者の個人情報の取扱いについて規定
- ✓ 法律の下に政令や規則があるが、ガイドラインを確認すればOK



【個人情報】
生存する個人に関する情報で、
特定の個人を識別することができるもの

（例）「氏名」、「生年月日と氏名の組合せ」、「顔写真」等
（※「個人識別符号」も個人情報に該当します。）

？ 「個人識別符号」とは？

- ✓ その情報だけで特定の個人を識別できる文字、番号、記号、符号等
  （例）指紋データ、パスポート番号、免許証番号、マイナンバー等

2．基本的な４つのルール

①取得・利用

- 利用目的を特定して、その範囲内で利用する。
- 利用目的を通知又は公表する。

勝手に使わない！

②保管

- 漏えい等が生じないよう、安全に管理する。
- 従業者・委託先にも安全管理を徹底する。

なくさない！
漏らさない！

③提供

- 第三者に提供する場合は、あらかじめ本人から同意を得る。
- 第三者に提供した場合・第三者から提供を受けた場合は、一定事項を記録する。

勝手に人に渡さない！

④開示請求等への対応

- 本人から開示等の請求があった場合はこれに対応する。
- 苦情等に適切・迅速に対応する。

お問合わせに対応！

個人情報の「取得・利用」に当たって守るべきこと

- 利用目的を特定して、その範囲内で利用する。
- 利用目的を通知又は公表する。

（※）利用目的の公表方法は、特に定めはありませんが、HPの分かりやすい場所や店舗等の事業所への掲示、申込書等への記載等が考えられます。

？ 利用目的はどのように特定すればよいですか？

✓ 例えば、以下のように特定することが考えられます。
「当社の新商品のご案内の送付のため」
「当社の商品の配送及びアフターサービスのご連絡のため」

✓ なお、取得の状況から、利用目的が明らかであれば、利用目的の通知又は公表は不要です。
（例：配送伝票の記入内容を配送のために利用することは明らか）

✓ また、利用目的を変更（追加）する場合は、原則本人の同意が必要です。
（関連性のある範囲内での変更なら通知又は公表のみで可）

！「要配慮個人情報」の「取得」に当たって守るべきこと

- 「要配慮個人情報」を取得する場合は、あらかじめ本人の同意が必要。
（利用目的の「特定」「通知又は公表」も必要）

（※）なお、法令に基づいて取得する場合等は同意は不要です。
また、本人から直接書面や口頭で取得する場合は、同意があったものとみなされるため、あらためて同意をとる必要はありません。

？「要配慮個人情報」とは？

- ✓ 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他、身体障害等の障害があることや、健康診断結果等も該当します。

個人情報の「保管」に当たって守るべきこと

- 漏えい等が生じないよう、安全に管理する。
- 従業者・委託先にも安全管理を徹底する。

「安全に管理」するための手法とは？

✓ 取り扱う個人情報の性質及び量等によりますが、例えば、以下のような手法が考えられます。

- 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で保管する。
- 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。
  また、セキュリティ対策ソフトウェアを導入する。　　等

✓ なお、ガイドラインでは、小規模事業者（※）向けの手法例を掲載していますので、併せてご参照下さい（次ページ参照）。

※従業員数が100人以下の事業者（ただし、5,000人分を超える個人情報を取り扱う事業者や、委託を受けて個人情報を取り扱う事業者を除きます。）

3. （2）保管に関するルール（補足：安全管理措置）

小規模事業者向けの安全管理措置の手法例とヒント①

講じなければならない措置	手法例	ヒント
1 基本方針の策定	※この項目は、義務ではありません。	• 義務ではありませんが、策定しておくことで、従業員教育に役立ちます。
2 個人データの取扱いに係る規律の整備	● 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。	• 既存の業務マニュアル・チェックリスト・フローチャート等に個人情報の取扱いの項目を入れるのも一案。
3 組織的安全管理措置		
（1）組織体制の整備	● 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。	• リスク分散の観点から、誰かがチェックできると良いということです。
（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。	• 業務日誌やチェックリスト等を活用し、確認を。
（3）個人データの取扱状況を確認する手段の整備		
（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時に備え、従業者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。	• 「ほう・れん・そう」の中に、個人情報の漏えい事案を。
（5）取扱状況の把握及び安全管理措置の見直し	● 責任ある立場の者が、個人データの取扱状況について、定期的に確認を行う。	• （1）～（4）のプロセスで気づいたリスクがあれば、改善を。

3. （2）保管に関するルール（補足：安全管理措置）

小規模事業者向けの安全管理措置の手法例とヒント②

講じなければならない措置	手法例	ヒント
4 人的安全管理措置		
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。 ● 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。	• 集合研修に限らず、朝礼等の際に定期的に注意喚起を。
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を講ずる。	• 誰でも見られる場所に放置しない。
（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、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。	• 書類や電子媒体をきちんと管理。
（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、封筒に封入し鞄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。	• 電子媒体にはパスワードを。置き忘れ等にも注意を。

小規模事業者向けの安全管理措置の手法例とヒント③

講じなければならない措置	手法例	ヒント
5 物理的安全管理措置		
（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、電子媒体等を廃棄したことを、責任ある立場の者が確認する。	• 書類であれば、焼却、シュレッダー処理を、機器・電子媒体等であれば、データ削除ソフトウェアの利用や物理的な破壊等を。
6 技術的安全管理措置		
（1）アクセス制御	● 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。	• 必要のない者の個人情報へのアクセスを制限するため、個人情報を含むファイルにパスワードを。
（2）アクセス者の識別と認証	● 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。	
（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。	• セキュリティ対策ソフトウェアを最新の状態に。
（4）情報システムの使用に伴う漏えい等の防止	● 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。	• それほど難しい操作ではないので、メール送信時にはパスワードを。

！ 個人情報の「提供」に当たって守るべきこと

- 第三者に提供する場合は、あらかじめ本人から同意を得る。
- 第三者に提供した場合・第三者から提供を受けた場合は、一定事項を記録する。

？ 本人同意や記録が不要となる例外はありますか？

- ✓ 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

！記録事項・保存期間について

- 基本的な記録事項は、以下のとおり（保管期間は原則3年）。
  （提供した場合）　「いつ・誰の・どんな情報を・誰に」提供したか？
  （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？
  ＋「相手方の取得経緯」
- 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。

？何でも記録義務がかかるのですか？例外はありますか？

- ✓ 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
- ✓ 反復継続して提供する場合は、包括的な記録でＯＫ
- ✓ 前ページの各種例外の他、以下の場合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

外国にある第三者に提供する場合に守るべきこと

● 次の①～③のいずれかを満たす必要があります。

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。
〇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

〇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）システムについて、ご興味のある方は、当委員会のウェブサイトに説明資料を掲載していますので、是非ご覧ください。

URL：http://www.ppc.go.jp/files/pdf/CBPR_ppc.pdf

！ 個人情報の「開示請求等への対応」に当たって守るべきこと

- 本人から開示等の請求があった場合はこれに対応する。
- 苦情等に適切・迅速に対応する。

？ 開示請求等への対応に当たっての留意点は？

✓ 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。
（例：HP公表、事業所での掲示等。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OK）
①事業者の名称、②利用目的、③請求手続、④苦情申出先、
⑤加入している認定団体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）

●罰則について

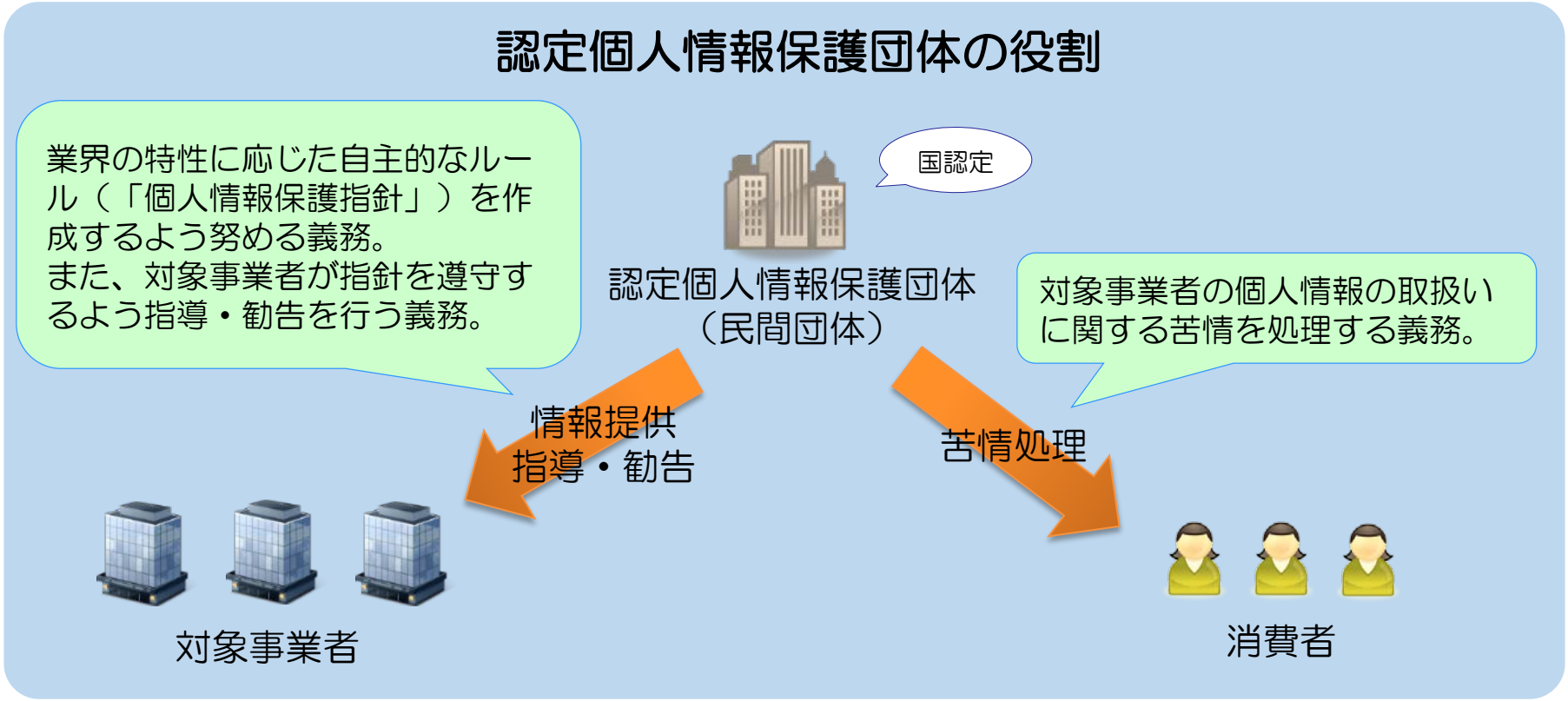
- ✓ 事業者の法遵守の状況は、個人情報保護委員会が監督します。
- ✓ 必要に応じて、報告を求めたり立入検査を行い、実態に応じて指導・助言、勧告、命令を行います。
- ✓ 罰則
  - ・国からの命令に違反・・6か月以下の懲役又は30万円以下の罰金
  - ・虚偽の報告・・・・・・30万円以下の罰金
  - ・従業員が不正な利益を図る目的で個人情報データベース等を提供・盗用
    ・・・・・・1年以下の懲役又は50万円以下の罰金（法人にも罰金）

●「匿名加工情報」について

- ✓ ビッグデータの活用を推進するための制度。
- ✓ 「匿名加工情報」とは、特定の個人を識別できないように個人情報を加工し、その個人情報を復元できないようにした情報（利用目的や第三者提供の制限なく、一定の取扱いルールの下、自由な流通・利活用を促進）。
- ✓ 匿名加工情報の加工基準や取扱いルールについては、ガイドラインや事務局レポートをご参照ください。

●「認定個人情報保護団体」について

- ✓ 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。
- ✓ 対象事業者への情報提供、個人情報に関する苦情の処理等を行う。



（参考2）　認定個人情報保護団体

対象事業等分野	名称
警備業	一般社団法人　全国警備業協会
指定自動車教習所業	一般社団法人　全日本指定自動車教習所協会連合会
証券業	日本証券業協会
保険業	一般社団法人 生命保険協会
保険業	一般社団法人 日本損害保険協会
保険業	一般社団法人 外国損害保険協会
銀行業	全国銀行個人情報保護協議会
信託業	一般社団法人 信託協会
投資信託委託業	一般社団法人 投資信託協会
証券投資顧問業	一般社団法人 日本投資顧問業協会
貸金業	日本貸金業協会
金融先物取引業	一般社団法人 金融先物取引業協会
放送	一般財団法人 放送ｾｷｭﾘﾃｨｾﾝﾀｰ
電気通信事業	一般財団法人 日本ﾃﾞｰﾀ通信協会
プライバシー付与認定事業者が行う事業	一般財団法人 日本情報経済社会推進協会
製薬業	日本製薬団体連合会
医療	公益社団法人 全日本病院協会
医療	一般社団法人 日本病院会
医療・介護	特定非営利活動法人 医療ﾈｯﾄﾜｰｸ支援ｾﾝﾀｰ
医療・介護・福祉	特定非営利活動法人 検定協議会
介護・福祉	社会福祉法人 沖縄県社会福祉協議会

対象事業等分野	名称
介護・福祉	社会福祉法人 岐阜県社会福祉協議会
手技療法	特定非営利活動法人 日本手技療法協会
医療・介護事業、ソフトウェア事業及び 冠婚葬祭事業を営む個人及び団体の事業者	一般社団法人 日本個人情報管理協会
ギフト用品に関する事業	一般社団法人 全日本ｷﾞﾌﾄ用品協会
クレジット事業	一般社団法人 日本ｸﾚｼﾞｯﾄ協会
印刷・グラフィックサービス工業	公益社団法人 東京ｸﾞﾗﾌｨｯｸｻｰﾋﾞｽ工業会
小売業	一般社団法人 日本専門店協会
経済産業分野	特定非営利活動法人 日本個人・医療情報管理協会
経済産業分野	公益社団法人 日本消費生活 ｱﾄﾞﾊﾞｲｻﾞｰ・ｺﾝｻﾙﾀﾝﾄ・相談員協会
経済産業分野	長野県個人情報保護協会
結婚情報サービス業	一般社団法人 結婚相談業ｻﾎﾟｰﾄ協会
結婚情報サービス業	結婚相手紹介ｻｰﾋﾞｽ協会
結婚情報サービス業	株式会社ＩＢＪ(日本結婚相談所連盟)
結婚情報サービス業	ﾅﾉﾗｲｾﾝｽ結婚専科ｼｽﾃﾑ協議会
新聞販売業	大阪毎日新聞販売店事業協同組合
葬祭業	ＪＥＣＩＡ 個人情報保護協会
葬祭業	全国こころの会葬祭事業協同組合
経済産業分野	一般社団法人　ビジネスコンプライアンス
自動車販売業	一般社団法人 日本自動車販売協会連合会
自動車登録番号標交付代行業	一般社団法人 全国自動車標板協議会
賃貸住宅管理業	公益財団法人 日本賃貸住宅管理協会

認定個人情報保護団体は42団体あります。（平成29年2月1日現在）

●個人情報保護法に関する質問

個人情報保護法の解釈についての一般的な質問は下記にお問合せください。
（※苦情相談窓口ではなく、ご質問等をお受けしています。）

個人情報保護法質問ダイヤル
０３－６４５７－９８４９
くわしく

受付時間　　土日祝日及び年末年始を除く　9:30～17:30

●事業者の個人情報の取扱いに関する苦情相談

事業者の個人情報の取扱いに関する苦情相談は、以下の窓口にお問合せください。

- 事業者の苦情受付窓口
- 消費生活センター等の地方公共団体の窓口
- 認定個人情報保護団体　　など

- 本資料は、改正個人情報保護法の概要をまとめたものであり、事業者の義務や例外規定の全てを記載したものではありません。

- より詳細な内容については、個人情報保護委員会のガイドラインをご参照下さい。
（個人情報保護委員会HP）http://www.ppc.go.jp/personal/preparation/

Thank You