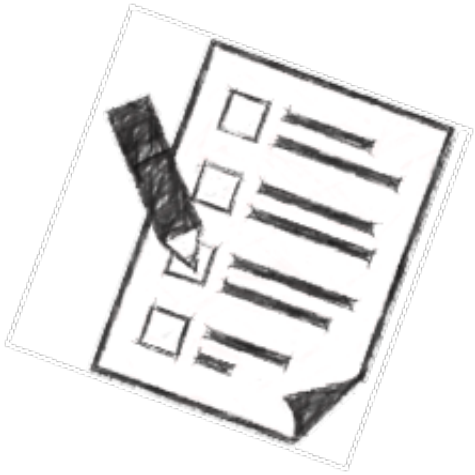
練馬区町会連合会
個人情報保護法に関する研修会

【中小規模事業者向け「これだけは！」10のチェックリスト付】

はじめての個人情報保護法

～シンプルレッスン～



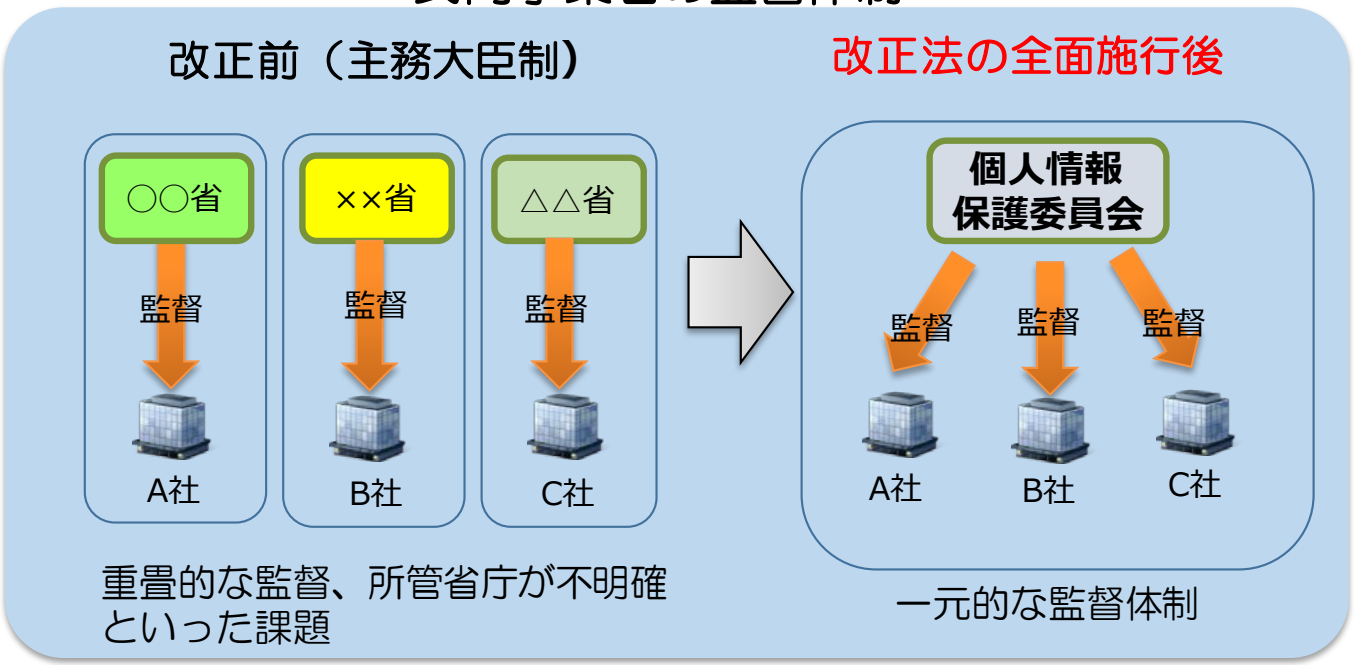
平成30年2月28日
個人情報保護委員会

目次

？ 個人情報保護委員会とは？　※赤字箇所は改正部分を示しています。

- ✓ 主務大臣が有していた監督権限を個人情報保護委員会へ一元化
- ✓ 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る
  また、実態に応じて、指導・助言、勧告・命令を行うことができる

民間事業者の監督体制



公的機関の監督体制*

- 行政機関個人情報保護法
  （対象：国の行政機関）
- 独立行政法人
  個人情報保護法
  （対象：独立行政法人等）
- 個人情報保護条例
  （対象：地方公共団体等）

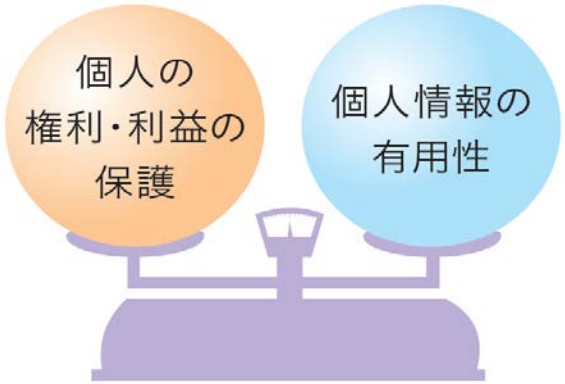
※公的機関の監督体制は、個人情報保護法の改正前後で変更はない。

(※)個人情報保護法の具体的な指針として定めた4つのガイドラインを規定
「通則編(個人情報保護法全体の解釈、事例)」「外国にある第三者への提供編」
「第三者提供時の確認・記録義務編」「匿名加工情報編」

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」が適用されています！

？ 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(社会生活やビジネス等への活用)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
- ✓ 従来は、取り扱う個人情報の数が5,000人分以下の事業者には適用されていませんでしたが、平成29年5月30日からは、すべての事業者に適用されています



2. 「個人情報」とは

【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

（※ その情報単体でも個人情報に該当することとした「個人識別符号」も個人情報に該当します。）

顧客情報だけでなく、従業員情報や取引先の名刺といったものも個人情報です。

？ 「個人識別符号」とは？

✓ 以下①②のいずれかに該当するものであり、政令・規則で個別に指定される
（政令第1条、規則第3、4条）

①身体の一部の特徴を電子計算機のために変換した符号
⇒DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋

②サービス利用や書類において対象者ごとに割り振られる符号(公的な番号)
⇒旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー等

3．事業者が守るべき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。（持ち運ぶ場合も要注意）

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！

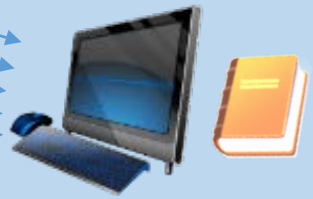
（※）②～④は個人情報をデータベース化（特定の個人を検索できるようにまとめたもの）した場合にかかるルールです。

3．事業者が守るべき４つのルール

個人データ　個人情報データベース等を構成する個人情報

個人情報データベース等

（特定の個人情報を検索できるように体系的に構成したもの）



パソコンの管理ソフト、台帳など

個人情報をデータベース化した場合、
②保管・管理、③提供に関する義務
が追加

保有個人データ　その事業者に開示等の権限のある個人データ（6ヶ月以内に消去するものを除く）

顧客情報、従業員情報など

その個人データに開示等の権限があれば、
④本人からの開示等の請求に応じる義務
がさらに追加

※他の事業者からデータ編集作業のみ委託されて渡された個人データなどは、保有個人データには該当しない

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。

（※）利用目的の通知・公表方法は、特に定めはありません。通知であれば、本人に口頭・書面・メール等で通知することが考えられ、公表であれば、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。なお、同意までの義務はありません。

「利用目的の特定」とは、何のために個人情報を利用するのか具体的に決めることです。

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案内のため」

✓ 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。

（※）なお、法令に基づいて取得する場合等は同意は不要です。

（例）労働安全衛生法に基づき健康診断を実施、これにより従業員の身体状況、病状、治療等の情報を健康診断実施機関から取得する場合

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（政令第2条、規則第5条）に定められた情報。

（例）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、身体障害等の障害があること等

！ 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（通則編P86～P98）。

※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。	• 個人データの取扱いを担当者任せにせず、責任者がチェックすることで不適切な取扱いを防ぐことができます。
（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。

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。

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。

第三者とは、個人情報の本人及び当該事業者以外の者を指します。

（※）本人の同意を得る方法は、特に定めはありません。口頭・書面で同意を得る方法のほか、ホームページで同意欄にチェックいただく方法も考えられます。

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　　等

3. （3）提供に関するルール（補足：確認記録義務）

！ 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、本規定は個人データの不正な流通の防止が目的であるため、一般的なビジネスの実態に配慮して、以下の通り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
- ✓ *例外規定として*、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

例外規定の詳しい内容はガイドライン（第三者提供時の確認・記録義務編）をご参照ください。

4. （3）提供に関するルール（補足：外国への提供）

！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か②のいずれかを満たさない限り、本人から「外国にある第三者に提供する」ことについての同意を得ることが必要です。
（単に「第三者に提供する」ということについて同意を得るだけでは足りません。また、委託や共同利用を行おうとする場合にも同意が必要です。）

①外国にある第三者が、適切な体制を整備している（※）
②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

★上記①か②のいずれかを満たす場合は、国内における第三者提供と同様の規律。

なお、外国のクラウドを利用する場合、当該クラウド事業者がサーバ内に保存された個人データを取り扱わない場合は、外国への第三者提供には当たりません。

（※）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。

「開示等の請求」とは、自分の個人情報について「見せてほしい」、「誤りを訂正してほしい」等の請求のことをいいます。

？ 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。

（参考2）事業者におい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（概要）

対象事案

- ✓ 個人データ（特定個人情報に係るものを除く。）の漏えい、滅失又は毀損
- ✓ 加工方法等情報（匿名加工情報の加工の方法に関する情報等）の漏えい
- ✓ これらのおそれ

望ましい対応

（1）事業者内部における報告及び被害の拡大防止

（2）事実関係の調査及び原因の究明

（3）影響範囲の特定

（4）再発防止策の検討及び実施

（5）影響を受ける可能性のある本人への連絡（事案に応じて）

（6）事実関係及び再発防止策等の公表（事案に応じて）

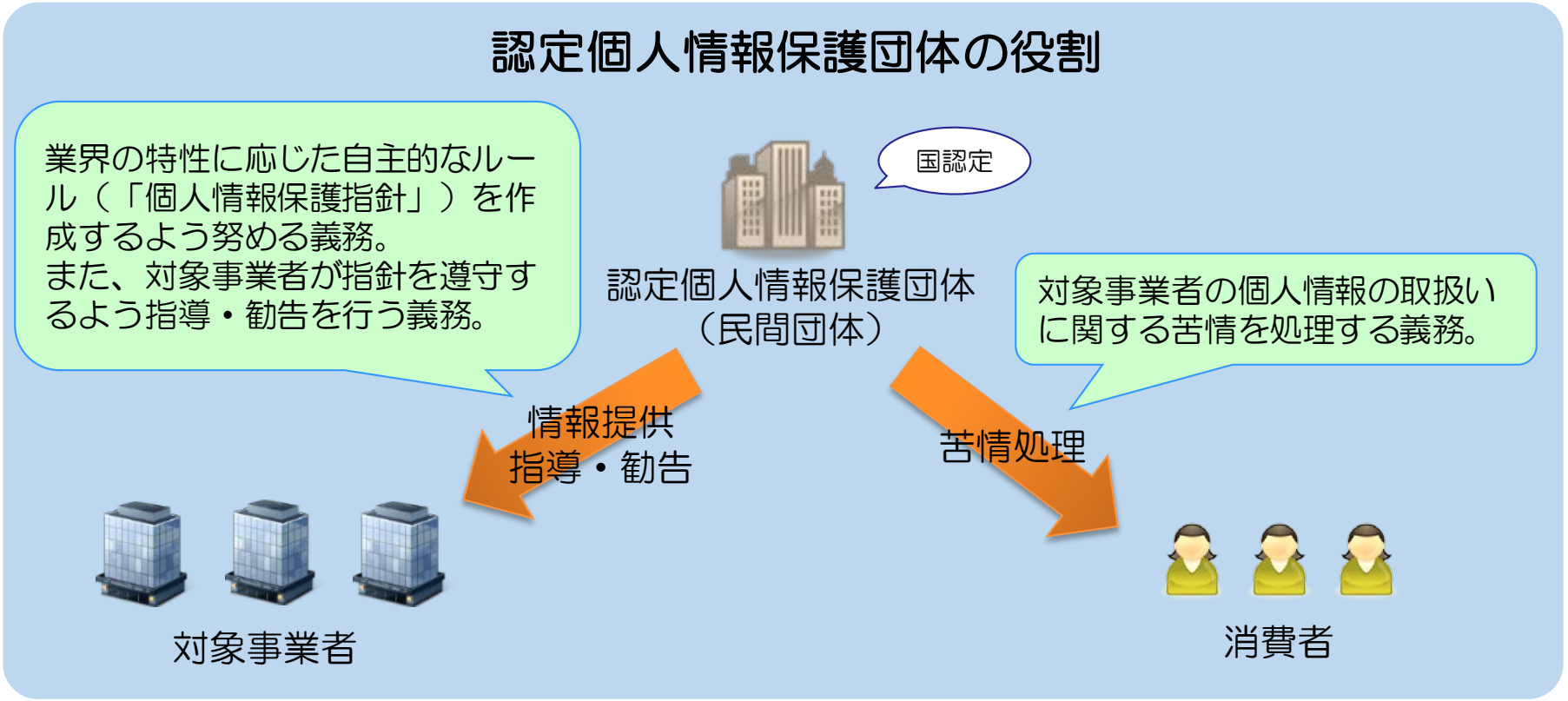
努力義務

個人情報保護委員会等への速やかな報告

※事業分野によっては、**認定個人情報保護団体**や権限の委任を受けた**事業所管大臣**が報告先となることがあります。
※なお、別途、業法等で監督当局への報告が義務付けられている場合もある為、注意が必要です。

●「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。



●個人情報保護法に関する質問・苦情相談

個人情報保護法の解釈についての一般的な質問や、事業者の個人情報の取扱いに関する苦情等は下記にご連絡ください。

個人情報保護法相談ダイヤル
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、以下の窓口でも受け付けています。

- 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等をご参照下さい。

〇個人情報保護委員会ホームページ
https://www.ppc.go.jp/
〇法令・ガイドライン等
https://www.ppc.go.jp/personal/legal/
〇中小企業サポートページ（個人情報保護法）
https://www.ppc.go.jp/personal/chusho_support/
〇政府インターネットテレビ「これだけは知っておきたい個人情報の取扱いルール　～名簿を作成する人必見！～　」
http://nettv.gov-online.go.jp/prg/prg16085.html

【巻末資料】中小規模事業者向け「これだけは！」10のチェックリスト

分類	No	チェック項目	ポイント	関連ページ
取得・利用	1	取り扱っている個人情報について、利用目的を決めていますか？	• 目的は具体的に。 ○「新商品のご案内の送付のため」 ×「当社の事業のため」	P7
	2	その利用目的は、本人に通知するか公表していますか？	• 取得の状況からみて利用目的が明らかなら、通知・公表は不要。	P7
保管	3	（組織的安全管理措置） 個人情報の取扱いのルールや責任者を決めていますか？	• 個人情報の保管場所や漏えい発生時の社内の報告先は決まってますか？	P9,10
	4	（人的安全管理措置・従業者監督） 個人情報の取扱いについて従業員に教育を行っていますか？	• 個人情報の保管場所等のルールは周知できていますか？	P9,11
	5	（物理的安全管理措置） 個人情報が含まれる書類や電子媒体について、誰でも見られる場所・盗まれやすい場所に放置していませんか？	• 不要になった情報は適切に廃棄・削除することも大切。	P9,11
	6	（技術的安全管理措置） パソコン等で個人情報を取り扱う場合、セキュリティ対策ソフトウェア等をインストールして最新の状態にしていますか？	• ログイン時にパスワードを要求したり、ファイルにパスワードをかけることも大切。	P9,12

※このチェックリストは、主に中小企業を対象に、個人情報保護法を遵守できているかどうか確認する際の参考に作成したものです。
個人情報保護法のルールの詳細は、本シンプルレッスンの関連ページや、個人情報保護委員会のガイドラインを参照してください。

【巻末資料】中小規模事業者向け「これだけは！」10のチェックリスト

分類	No	チェック項目	ポイント	関連ページ
保管	7	個人情報の取扱いを委託する場合、契約を締結する等、委託先に適切な管理を求めていますか？	• 委託先にも安全管理を徹底してもらうということ。	P9
提供	8	本人以外に個人情報を提供する場合、本人に同意をとっていますか？	• 法令に基づく場合（警察や裁判所からの照会等）や、委託に伴う提供には同意不要。	P13
	9	本人以外に個人情報を提供したり、本人以外から個人情報を受け取る際、相手方や提供年月日等について記録を残していますか？	• 法令に基づく場合（警察や裁判所からの照会等）や、委託に伴う提供には記録不要。	P13,14
開示請求等	10	本人から自分の個人情報を見せてほしいと言われたり、訂正してほしいと言われた際には、対応していますか？	• 開示等の請求に対応する人は決まっていますか？	P16

※このチェックリストは、主に中小企業を対象に、個人情報保護法を遵守できているかどうか確認する際の参考に作成したものです。
個人情報保護法のルールの詳細は、本シンプルレッスンの関連ページや、個人情報保護委員会のガイドラインを参照してください。