平成26年12月改正

「個人情報」の「取扱いのルール」が

（「個人情報の保護に関する法律について」の経済産業分野を対象とするガイドライン）

改正

されました！

経済産業省
Ministry of Economy, Trade and Industry

もくじ

もう一度確かめたい「個人情報」ってなに？

個人情報保護法では、保護が必要な情報を「個人情報」、「個人データ」、「保有個人データ」の３つの概念に分けています。
３つの概念ごとに、実施しなくてはならない義務が定められています。個人情報よりも個人データ、個人データよりも保有個人データの方が、守るべき義務が増えていきます。

❶個人情報

- 生存する特定の個人を識別できる情報
- 他の情報と容易に照合でき、その結果、特定の個人が識別できることとなる情報も含まれる

❷個人データ

- ❶のうち、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（個人情報データベース等）に含まれる個人情報

❸保有個人データ

- ❷のうち、開示、訂正、消去等の権限を有し、かつ、6ヶ月を越えて保有するもの

❶個人情報

- 利用目的の特定（15条）
- 利用目的による制限（16条）
- 適正な取得（17条）
- 取得に際しての利用目的の通知等（18条）
- 苦情の処理（31条）

❷個人データ

- データ内容の正確性の確保（19条）
- 安全管理措置（20条）
- 従業者の監督（21条）
- 委託先の監督（22条）
- 第三者提供の制限（23条）

❸保有個人データ

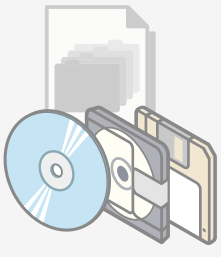
- 保有個人データに関する事項の公表等（24条）
- 開示（25条）、訂正等（26条）、利用停止等（27条）、理由の説明（28条）、開示手続（29条）、手数料（30条）

❶個人情報

名前：
住所：
年齢：
注文商品：
感想：
・・・・

例えば、ソフトに入力して、データベースにした場合

❷個人データ



開示等の権限を有し、かつ、6ヶ月を越えて保有する場合

❸保有個人データ

もう一度確かめたい「個人情報取扱事業者」って誰のこと?

個人情報保護法上の義務を負う「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者です。しかし、現実には、ほとんどの事業者がこの定義に該当すると考えられます。個人事業主や、NPO等の非営利組織であるからと言って、法律上の義務の対象にならないわけではありません。

個人情報保護法の義務を負うのは誰か?

「個人情報取扱事業者」

個人情報データベース等を事業の用に供している者(2条3項)

●情報処理やソフトウェア開発等をしている会社ばかりが対象ではない。

個人情報データベースに該当する事例	●メールソフトのアドレス帳、仕事で使う携帯電話の電話帳、ソフトウェア等でリスト化された従業者や顧客台帳 ●五十音順に整理し、インデックスを付してファイルしている、登録カード ●氏名、住所、企業別に分類されている市販の人名録

●上記を業務に使っている会社は「個人情報取扱事業者」となる。
●法人には限定されないので、「個人事業主」も個人情報取扱事業者。
●営利か非営利かも問われないので、「NPOなど」も個人情報取扱事業者。

【例外1】:個人情報取扱事業者に当たらない

個人情報データベース等に含まれ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ヶ月以内のいずれの日においても5,000を超えない者

【例外2】:義務規定の適用除外

①報道機関が報道活動の用に供する目的
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

経済産業分野
ガイドライン改正について

改正のポイントは、個人情報保護法における以下の規定に関し、それぞれ取組の充実・強化を図ります。

ガイドライン改正のポイント

① 法第17条 …… 第三者からの適正な情報取得の徹底

（適正取得）第17条

個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

② 法第20条 …… 社内の安全管理措置の強化

（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。

③ 法第22条 …… 委託先等の監督の強化

（委託先の監督）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。

④ 法第23条 …… 共同利用制度の明確な説明

（第三者への提供）第23条第1項

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。

（共同利用）第23条第4項第3号

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3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。

3 個人データを特定の者との間で共同して利用する場合であって、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。

第三者からの適正な情報取得の徹底

問題点

- 個人情報を取得した者は、提供元がそれを適法に入手したことを十分に確認しないまま（提供元から「誓約書」を取得するという形式的な対応）、当該情報を入手していました。

ガイドラインの主な改正事項

- 第三者から個人情報を取得する場合※には、
  - 提供元の選定に当たり、その個人情報保護法の遵守状況を確認すること。
  - 個人データの取得方法等について、例えば、取得の経緯を示す契約書等の書面を点検する等により、**適法に入手されていることを確認**すること。

※不特定かつ多数の者が購入することができるものから取得する場合、法令に基づき提供される場合、承継、共同利用、委託等の場合を除きます。

- 第三者から個人情報を取得する場合において、当該個人情報が**適法に入手されたことが確認できない場合**は、偽りその他不正の手段により取得されたものである可能性もあることから、その**取得を自粛することを含め、慎重に対応**すること。

社内の安全管理措置の強化（サイバー攻撃対策）

問題点

- 近年、外部からのサイバー攻撃により、大量の情報が漏えいする事案が発生しています。
- 従前のガイドラインでは、外部からの脅威について十分な対応が記載されていませんでした。

ガイドラインの主な改正事項

① 管理手法の追記

有効であると考えられる管理手法を望まれる手法として追記しました。

- データベースへのアクセス制御
- ワンタイムパスワード等
- 不要アカウントの無効化
- 管理者権限の分割
- アクセス記録
- ウイルス対策ソフトウェアの有効性確認
- データ移送時の秘匿化

② 既存の管理手法の修正

既に掲載されている管理手法であり、有効かつ一般的な手法であると考えられますが、実施していない事業者も相当程度存在する手法を、より周知を図る観点から、順番を入れ替えて冒頭に記載しました。

- ファイアウォールの設置
- ウィルスソフトウェアの導入

社内の安全管理措置の強化（内部不正対策）

問題点

大量の個人情報が漏えいする事案が発生しました。その原因は…

- 個人情報のダウンロードを監視するシステムが、設定されていませんでした。
- 個人情報を取り扱う部屋へ、私物であるスマートフォンを持ち込むことができました。また、個人情報のデータベースに、そのスマートフォンが接続できる状態になっていました。
- 個人情報のダウンロードのログ（記録）について、定期的な確認が行われておらず、長期間にわたり、漏えいの事実を把握できていませんでした。
- 「性善説」に立った、不十分な社内管理体制になっていました。

ガイドラインの主な改正事項

① 組織的安全管理

- **個人情報保護管理者**（CPO）への**役員の任命**など、社内体制を整備すること。
- 情報セキュリティ等に十分な知見を有する者による社内の監査体制を構築すること。
- スマートフォン等の**記録機能を有する機器の接続制限**を行う社内規程を整備すること。

② 物理的安全管理

- 業務上許可を得ていない**記録機能を有する媒体・機器の持ち込み・持ち出しの禁止**と検査を実施すること。
- カメラによる撮影や立ち会い等による記録又はモニタリングを実施すること。
- 個人情報を取り扱う部屋への入退室記録の保存をすること。

③ 技術的安全管理

- 個人情報の**監視システム**について、その動作を**定期確認**すること。
- 個人情報への**アクセスやダウンロードのログ**（記録）について、不正が疑われる異常な記録の存否を**定期確認**すること。

委託先等の監督の強化

問題点

大量の個人情報が漏えいする事案が発生しました。その原因は…

- システム開発・管理の委託先（子会社）における安全管理措置が十分でなく、そこから個人情報が不正に持ち出されていました。

- 委託業務の一部が、委託先から他の企業へ再委託、再々委託されていることを十分に把握できておらず、委託先等を適切に監督していませんでした。

ガイドラインの主な改正事項

① 委託先の監督

- 委託先の選定に当たり、**委託先の安全管理措置を確認**し、ＣＰＯ等が評価すること。
- **定期的**に、**委託業務の監査**を実施し、その結果について、ＣＰＯ等が評価すること。
- 委託契約等において、委託先で個人データを取り扱う者の役職又は氏名、損害賠償責任を盛り込むこと。

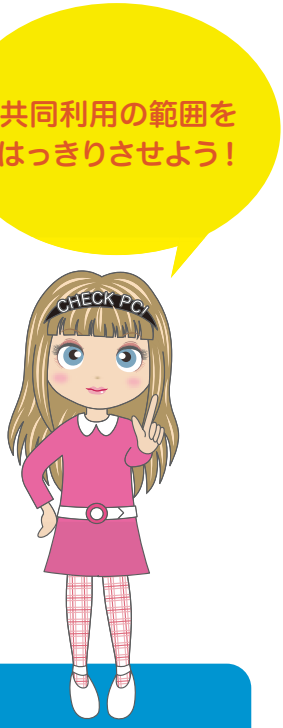
② 再委託先の監督

- 委託元は、委託先が**再委託**を行う場合には、委託先から、**事前報告又は承認**を求めること。
- 委託元は、委託先を通じて、又は必要に応じて自らが、**再委託先に対し、定期的な監査**を実施すること。
- 再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とすること。

共同利用制度の明確な説明

問題点

- 「企業ポイント等を通じた連携サービス」で共同利用を行う場合、共同利用者の範囲が明確でなくても共同利用が可能であると誤解を与えている可能性があります。
- 最新の共同利用者リストを本人が容易に知り得る状態に置いているだけで、共同利用者の範囲が明確でなくても共同利用が可能と誤解を与えている可能性があります。



ガイドラインの主な改正事項

① 共同利用の趣旨の明確化

- あらかじめ本人の同意が必要な第三者提供の例外の１つである共同利用について、制度の趣旨を明確に記載しました。
- 事業者が共同利用を円滑に実施するために、共同利用者における責任等を明確にする観点から、あらかじめ取り決めておくことが望ましい事項について趣旨が伝わりやすいよう明記しました。

② 共同利用者の範囲の明確化

- 共同利用者の範囲について、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で共同利用ができるのであり、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある旨追記しました。
- 共同利用者の範囲が明確である具体例を追記しました。

消費者等本人に対する分かりやすい説明の取組について

趣　旨

- 個人情報取扱事業者は、消費者等本人との信頼関係を構築する観点から、消費者等本人に対して、個人情報取扱事業者の個人情報保護を推進する上での考え方や方針等について、冗長で分かりにくい説明を避け、消費者等本人に誤解を与えることなく分かりやすい表現で説明することが望まれます。

- このことから、個人情報を利活用してサービスを行う事業者が、消費者からパーソナルデータを取得し利用する際に、消費者に対して行う情報提供や個人情報保護を推進する上での考え方や方針等を分かりやすく説明した文書等の内容の適切性を第三者が事前に評価する際のツールとして経済産業省が策定した「評価基準」を基に作成した、「分かりやすい説明の実施に際して参考とすべき基準」を追記しました。

「分かりやすい説明の実施に際して参考とすべき基準」

1. 記載事項

(1)必要十分な記載事項

1個人情報の取扱いに関する情報として、以下の7項目が記載されていること
- 1)提供するサービスの概要
- 2)取得する個人情報と取得の方法
- 3)個人情報の利用目的
- 4)個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先
- 5)消費者等本人による個人情報の提供の停止の可否、訂正及びその方法
- 6)問合せ先
- 7)保存期間、廃棄

2. 記載方法

(1)取得する個人情報とその取得方法に係る記載方法

2取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること

3取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること

(2)個人情報の利用目的に係る記載方法

4取得する個人情報の利用目的を特定し、具体的に記載していること

5個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること

6取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること

(3)第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法

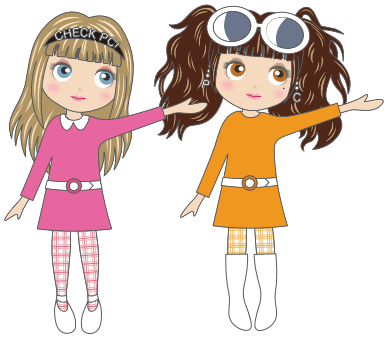
7個人情報取扱事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先(事後的に提供先を変更する場合は提供先の選定条件を含む)及び提供目的が記載されていること

8個人情報取扱事業者が取得した個人情報を加工したデータを第三者に提供する場合、その加工方法が記載されていること

(4)消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法

9消費者等本人が個人情報取扱事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載していること

個人情報保護法関連資料については、以下をご参照ください。



消費者庁（個人情報の保護）

http://www.caa.go.jp/planning/kojin/

経済産業省（ガイドライン）

http://www.meti.go.jp/policy/it_policy/privacy/index.html

保護法、ガイドラインのほか、民間事業者の優良取組実践事例、
社内啓発ビデオ等を掲載しております。

経済産業省　商務情報政策局　情報経済課