

改正個人情報保護法のポイントと 企業が対応すべき事項 第2回 要点整理編

アドバイザリー事業部 公認会計士 梅澤 泉

▶ Izumi Umezawa

公認情報システム監査人、公認不正検査士。金融機関、製造業、小売業、サービス業などの会計監査を経て、個人情報保護をはじめとする情報セキュリティ監査やデータセンター事業者・クラウドサービス事業者の顧客向けサービスに係る内部統制の保証業務に従事。(TEL: 03 3503 3500 E-mail: umezawa-zm@shinnihon.or.jp)

I 改正個人情報保護法への対応

2017年に施行される予定の改正個人情報保護法(以下、改正前の同法を「現行法」、改正後の同法を「改正法」)は、プライバシーの保護に配慮しつつパーソナルデータの利活用に向けて現行法を見直したものとなりました。本誌2016年7月号(Vol.112)「第1回概要編」では、現行法に比べて改正法で見直された主な変更点についてまとめており、本編ではその中から、企業が改正法に沿った対応を進める上でより正しく理解しておくべきポイントとして、「個人情報の定義の明確化による概念の整理」「個人情報の有用性の確保を通じた利活用の促進」「個人情報の保護強化に向けた規制の見直し」の三つの観点から解説します。

II 個人情報の明確化(改正法第2条1項・2項)

改正法では、保護対象を明確にするという観点から個人情報の定義が一部修正されています。具体的には新たに個人識別符号という用語が条文に加わり、従来曖昧であった概念が一部整理されることとなります。ただし、個人情報に該当するのかがどうか不明瞭な、いわゆるグレーゾーンの領域も依然として残っており、この点については今後制定される政令などを通じて可能な限り解消されていくことが望まれます。改正法による個人情報の概念を整理すると<図1>のとおりです。

▶ 図1 個人情報の分類

<個人情報に該当するもの>	
a. 一般的な個人情報(改正法第2条1項1号)	▶ 氏名、住所、生年月日など
	▶ 移動履歴、購買履歴など(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情報)
b. 個人識別符号①(改正法第2条2項1号)	▶ 指紋認証データ、顔画像データ、歩容認証データなど
c. 個人識別符号②(改正法第2条2項2号)	▶ 個人番号(マイナンバー)、運転免許証番号、パスポート番号、基礎年金番号、保険証番号など
d. 要配慮個人情報(改正法第2条3項)	▶ 人種、信条、社会的身分、病歴、犯罪の経歴など
<一概に個人情報とはいえないもの(グレーゾーン)>	
	▶ 携帯電話番号、クレジットカード番号、メールアドレス、会員IDなど
<個人情報にはあたらないもの>	
	▶ (携帯電話などの)通信端末ID
	▶ 匿名加工情報(改正法第2条9項)

* 今後制定される政令によって、上記の分類内容は一部変更となる可能性がある。

▶ 表1 匿名加工情報に関する規制事項

作成・提供側（個人情報取扱事業者）	提供を受け活用をする側（匿名加工情報取扱事業者）
匿名加工情報の作成方法の遵守	——
加工方法等の漏えい防止措置の実施	——
作成した情報の項目等の公表（作成時／提供時）	提供を受けた情報の項目等の公表（提供時）
匿名加工情報の再識別の禁止（個人を特定するために他の情報と照合してはならない）	
匿名加工情報の安全管理措置の実施（安全管理措置の内容につき、公表に努める）	

Ⅲ 利活用のための改正ポイント

1. 匿名加工情報（改正法第2条9項）

(1) 匿名加工情報の取扱規制

匿名加工情報は、特定の個人を識別できないように個人情報を加工し、当該個人情報を復元できないようにした情報です。個人情報には該当しないことから、本人の同意なしで第三者に提供することが可能で、これらをビッグデータとして活用することが期待されています。匿名加工情報の取扱いに当たっては、元の個人情報を加工して匿名加工情報を作成する立場（個人情報取扱事業者）と、それらの情報を受け取り活用する立場（匿名加工情報取扱事業者）のそれぞれの事業者に対し、規制事項が定められています（＜表1＞参照）。

(2) 匿名加工情報の性格

匿名加工情報に関しては、元の個人情報をどのように加工すれば「当該個人情報を復元できないようにした情報」となり得るのが論点となります。現時点では、通常、人の技術力等の能力をもって復元しようとしても当該個人情報に戻ることもないような状態が想定されており、技術的側面からの全ての復元可能性を排除するようなレベルが求められているわけではないと考えられています。

なお実務上の加工基準または方法については、個人情報保護委員会規則において最低限の規律が定められるとともに、具体的な内容は認定個人情報保護団体が作成する個人情報保護指針等の自主的なルールに委ねられる予定です。

(3) 匿名加工情報の作成方法の例

匿名加工情報の作成にはいくつかの方法が考えられますが、一例を挙げると以下の通りです。

- ▶ 作成のもととなる個人情報と個別に関連づけられている項目やID等の識別子を削除する。
→ 氏名、住所、生年月日などを削除する方法
- ▶ 分析対象のデータの平均から大きくかい離するデータ群をまとめる（トップコーディング）。
→ 早朝・深夜の入退室ログについて、「午前6時以前」、「午前1時以降」のようにくくる方法
- ▶ 詳細な項目を一定のまとまりや区分に置き換える。
→ 生年月日を年代に置き換え、グルーピングする方法
- ▶ 一定の誤差（ノイズ）を付加する。
→ 一定の金額や数量誤差を対象の情報に加える方法

なお、通常程度の手法によって復元できてしまうレベルの加工情報は改正法で定める匿名加工情報には当たらず、依然として個人情報のままということになるので、前記のどれか一つが実施されていれば直ちに匿名加工情報になるわけではない点に注意が必要です。

2. 利用目的制限の緩和

現行法では、利用目的を変更する場合には変更前の利用目的と相当の関連性を有すると合理的に認められた範囲内で実施しなければならないと定められていましたが、改正法ではこの「相当の」という文言が削除されました（改正法第15条2項）。これによって利用目的の変更が従来よりも柔軟に実施可能となり、企業にとってはすでに取得済みの顧客情報などを活用して新規の事業やサービスを機動的に展開できる可能性が広がります。

では、どこまでの変更が「利用目的と関連性を有すると合理的に認められた範囲」になるのでしょうか。その判断基準としては「本人が通常予期し得る限度内か否か」という観点で検討されることになります。すなわち、変更された目的が本人にとって想定外となるような事態は回避する必要があるため、企業としては現在通知または公表している利用目的を再確認の上、今後範囲を変更した場合に本人の誤解を招かない内容となっているかどうかについて、あらためて見直しを検討することが望ましいと言えます。

IV 保護のための改正ポイント

1. 要配慮個人情報の取扱い

要配慮個人情報は、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情報として改正法で新設されました（改正法第2条3項）。通常の個人情報とは異なり、以下の事項が定められている点が特徴です。

- a. 原則として、本人の事前同意がない取得は禁止（改正法第17条2項）
- b. オプトアウト^{※1}による第三者提供は認められない（改正法第23条2項）

実務上の観点から一例を挙げると、例えば従業員の健康情報のうち病気を推測、または特定できるような情報に関しては要配慮個人情報として取扱われる可能性が高く、その場合企業は、これらの情報を取得する目的を従業員本人に明らかにし、あらかじめ同意を得ることが必要となります。

なお、要配慮個人情報の具体的な内容は別途政令によって定められることになっていますが、他のガイドライン等で示されている類似の概念について参考までに比較すると、＜表2＞のとおりになります。

2. 第三者提供

(1) 第三者提供に係る記録等の義務

個人データを第三者に提供する際には、トレーサビリティ確保の観点から当該情報を提供する側と提供を受ける側それぞれに対して規制が強化されました。具体的には、原則として本人の同意を得る以外に、個人情報取扱事業者は以下の義務を負うことになります。

- ▶ 提供する側：提供年月日、提供先等に関する記録の作成、および当該記録の一定期間の保存（改正法第25条）
- ▶ 提供を受ける側：提供者の情報、および提供者が当該個人データを取得した経緯の確認、提供年月日、提供者情報およびその取得経緯に関する記録の作成、および当該記録の一定期間の保存（改正法第26条）

作成すべき記録の具体的な内容や保存期間等については、個人情報保護委員会規則で別途定められることになっていますが、これらはいわゆる名簿屋対策の一環として、個人情報の不正な流通や取得を阻止することを目的に今回の改正に至っています。

(2) 外国にある第三者への提供制限

現行法では、個人データの提供時には提供先である第三者が国内か海外かに関係なく、一律に本人同意を求めることが義務付けられていましたが、海外における当該第三者が日本の個人情報保護水準に比べて不十分な取扱いを行っている場合、本人の権利利益が侵害されかねないというリスクがありました。そこで改正法では、外国にある第三者に個人データを提供する場合、当該第三者に対して自分の個人データの提供を認める、という旨の本人同意を原則として得なければならないことが規定されました（改正法第24条）。

ここで注意しなければならないのは、従来の第三者提供制限とは異なり、個人データの委託時においても本人同意が不要にはならないという点です。例えば、海外のクラウド事業者に個人データの管理を委託している場合であっても、本規定は適用されることになり、事前の本人同意を取得する必要があります。

なお、当該第三者が以下に該当する場合は、例外として従来の本人同意が得られていれば足りるということになっています。

▶ 表2 要配慮個人情報の内容比較

改正法（第2条3項） （要配慮個人情報）	JISQ15001：2006「個人情報保護マネジメントシステム 要求事項」 （特定の機微な個人情報）	金融分野における個人情報保護に関するガイドライン （機微（センシティブ）情報）	EU一般データ保護規則 （特殊な種類の個人情報）
▶ 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 ▶ 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（政令で定められる個人情報）	▶ 思想、信条または宗教に関する事項 ▶ 人種、民族、門地、本籍地（所在都道府県に関する情報を除く）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項 ▶ 勤労者の団結権、団体交渉その他団体行動の行為に関する事項 ▶ 集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項 ▶ 保健医療または性生活に関する事項	▶ 政治的見解 ▶ 信教（宗教、思想および信条） ▶ 労働組合への加盟 ▶ 人種および民族 ▶ 門地および本籍地 ▶ 保健医療および性生活 ▶ 犯罪歴	▶ 人種、種族的出身 ▶ 政治的見解 ▶ 宗教、哲学的信念 ▶ 性的指向、性別認識 ▶ 労働組合の加入および活動 ▶ 遺伝子データ、生体データ、健康、性生活に関するデータ ▶ 行政的制裁、裁判判決、刑事犯罪、犯罪容疑、有罪判決に関するデータ

※1 個人に関するデータの第三者提供に関して、事後的に本人の求めに応じて第三者への提供を停止すること。



- ▶ 日本と同等の水準にあると認められる個人情報保護の制度を有している外国（具体的には個人情報保護委員会規則で定められる）
- ▶ 個人情報保護委員会規則で定める基準に適合する体制を整備している外国企業

海外のデータセンターを利用している企業や、従業員情報または顧客データについて海外子会社やグループ企業との間で共有している企業は、こうした規制への対応を検討し、業務への影響やサービスの低下といったビジネスリスクを回避するための方策を練ることが望ましいと言えます。

(3) 第三者提供のオプトアウトに対する規制強化

現行法において、オプトアウトで個人データの第三者提供を行おうとする場合には、以下の事項についてあらかじめ本人に通知し、または本人が容易に知り得る状態に置かなければならないと定められていました（現行法第23条2項）。

- a. 第三者への提供を利用目的とすること
- b. 第三者に提供される個人データの項目
- c. 第三者への提供の方法
- d. 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

改正法では、オプトアウトが認められるためには前記事項に「e. 本人の求めを受け付ける方法」を加えた5項目について個人情報保護委員会に届け出なければならず、かつ当該届出の内容は個人情報保護委員会によって公表されることになりました（改正法第23条2項、4項）。これは、情報主体である本人が、オプトアウトを行っている企業について適切に把握できるようにすることを目的として見直されたものです。

本人に対し、これまでオプトアウトの十分な通知・公表が実施できていなかった企業は、今後もオプトアウトによる第三者提供を継続するかどうかも含めて、提供の方針を再確認することが望まれます。

3. データベース提供罪（改正法第83条）

改正法によって新設されたデータベース提供罪（1年以下の懲役又は50万円以下の罰金）は、企業およびその従業者（元従業者を含む）が業務に当たり取り扱った個人情報データベース等を、不正な利益を図る目的で提供または盗用した時に科せられます。ここで

いう不正な利益とは、職務上の権限や地位を利用して入手した個人情報を他の事業者に販売して経済的利益を得る場合などを指しています。従って、例えば従業員が組織に対する嫌がらせや興味本位目的でこれらの情報を持ち出した場合は、当該規定は適用されない可能性が高く、またマイナンバー法^{※2}における同様のケース（マイナンバー法第68条、3年以下の懲役又は150万円以下の罰金）などと比べても、さほど重い量刑が科せられているとはいええない状況です。

このため、当該罰則による抑止効果は必ずしも十分に発揮されるとは限らないことから、企業としては個人情報データベース等の安全管理状況をあらためて確認し、必要に応じて追加のセキュリティ対策を講じるといった強化策の検討が望ましいと考えられます。

4. 個人データの廃棄規制

企業は個人データを利用する必要がなくなった場合、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という努力義務が定められました（改正法第19条）。これは、不要となった個人データを保持し続けることで生じる紛失または漏えいのリスクを、できるだけ回避するために図られた措置といえます。

なおマイナンバーに関しては、これらの事務処理の必要性がなくなり、所管法令による保存期間を経過した時点で、できるだけ速やかに廃棄または削除しなければならないという義務規定になっていることから、改正法における個人データに比べて規制が強化されている点に注意が必要です。

V おわりに

2回にわたって、改正個人情報保護法の内容と企業実務へのインパクトについて解説してきました。このあと施行令や個人情報保護委員会規則、ガイドライン等が公表される中で、企業はより具体的な対応方針を検討していくことが必要となります。またグローバル企業にとっては、国内法のみならずEUや米国、アジア太平洋経済協力（APEC）でのプライバシールールに関しても理解を深めつつ、海外諸国との間でのプライバシーデータの健全な流通と保護・利活用に向けて体制構築を進めていただきたいと思います。

※2 行政手続における特定の個人を識別するための番号の利用等に関する法律（2013年5月制定）