

2018年11月8日 全13頁

今さら聞けない個人情報保護法のQ & A②

個人情報の取得や利用はどう行えばいいの？

金融調査部 研究員
藤野 大輝

[要約]

- ここもと、個人情報の保護に関する制度改正が、国内外で相次いでいる。わが国では、2015年9月に個人情報保護法が改正され、2017年5月30日から全面施行されている。個人の医療情報に関しては、別途、次世代医療基盤法が2017年5月に公布され、2018年5月11日から施行されている。海外ではEUでGDPR(EU一般データ保護規則)が2018年5月25日から施行されている。
- 本シリーズでは、改正された個人情報保護法に関する基本的な事項をQ & A形式で紹介する。
- 今回は、個人情報取扱事業者が個人情報を取り扱うに当たってしなければならないことや、匿名加工情報の作成・利用、個人情報の管理の委託、個人情報が漏えいした場合の対応等について取り上げる。

【目次】

- Q1：個人情報は自由に取得してもいいの？
- Q2：個人情報を取得したら何をしなければならないの？
- Q3：個人情報は一度取得したらずっと保有していてもいいの？
- Q4：個人データに関して何かしなければならないことはあるの？
- Q5：保有個人データの本人に請求されたらしなければならないことって？
- Q6：匿名加工情報はどうやって作るの？取扱いで気を付けることは？
- Q7：個人データの取扱いを業者に委託してもいいの？
- Q8：もし個人データが漏えいしてしまったらどうすればいいの？

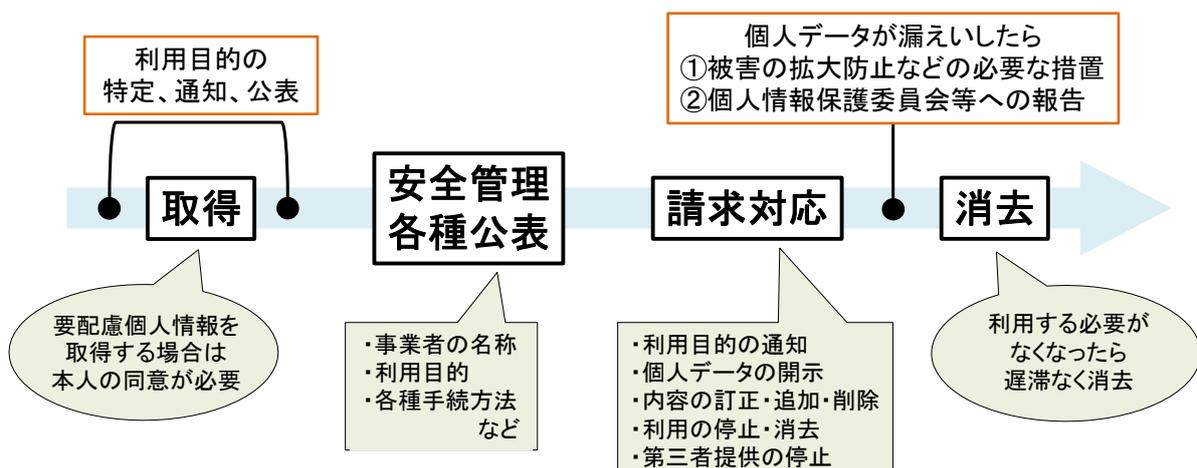
はじめに

昨今、情報技術の発展に伴い、個人情報¹を取得・利用する企業が増えている。さらに、いわゆる IoT によってあらゆる製品がネットワークにつながるようになり、そこから企業がデータを取得することが増えていくと考えられる。また、企業が取得した大量のデータ（ビッグデータ）を分析し、活用する事例も多く見受けられるようになってきている。

ただ、個人情報の取得・利用が拡大している一方で、個人情報の不正な取扱いや漏えいが決して少なくない頻度で報道されているように思われる。個人情報は法令に従って適切に取得・利用をする必要があり、また、漏えいした際には迅速かつ的確な行動が求められる。

今回は、個人情報取扱事業者が個人情報を取り扱うに当たって行わなければならないことや、匿名加工情報の作成・利用、個人情報の管理の委託、個人情報が漏えいした場合の対応等について取り上げる。

図表 1 個人情報の取得・利用のフロー



(注) このほか、個人情報の第三者提供を行う、もしくは受ける場合は別途対応が必要とされる。詳しくは本シリーズの次回以降のレポートで扱う。

(出所) 大和総研作成

Q 1 : 個人情報は自由に取得してもいいの？

A 1 : 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」が、それ以外の規定はない（個人データを他の事業者等の第三者から提供される場合は除く²）。ただし、要配慮個人情報は原則として本人の同意なしで取得してはならない。

¹ なお、「個人情報」「要配慮個人情報」「個人情報取扱事業者」「匿名加工情報」等の用語の定義については、藤野大輝「今さら聞けない個人情報保護法のQ&A①」（2018年8月27日付 大和総研レポート）参照。

https://www.dir.co.jp/report/research/law-research/law-others/20180827_020289.html

² 個人データの第三者提供については、本シリーズの次回のレポートで取り扱う。

個人情報取扱事業者は偽り等の不正の手段により個人情報を取得してはならない³。ここで言う不正の手段による取得としては、図表2のような例が挙げられる。

図表2 個人情報の不正な取得の例

①	十分な判断能力のない子供や障害者から、取得状況から考えて関係のない家族の個人情報を家族の同意なしに取得する場合
②	第三者提供制限に違反するよう強要して、個人情報を取得する場合
③	取得する主体や利用目的等について、意図的に虚偽の情報を示して個人情報を取得する場合
④	他の事業者に不正の手段で個人情報を取得させて、その情報を当該事業者から取得する場合
⑤	第三者提供制限違反がされようとしていることを知り、もしくは容易に知りうるにもかかわらず、個人情報を取得する場合
⑥	不正の手段で個人情報が取得されたことを知り、または容易に知りうるにもかかわらず、当該個人情報を取得する場合

(出所) 個人情報保護委員会「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）」より大和総研作成

一方、要配慮個人情報については、不正な取得が禁止されているだけではなく、取得するには原則として本人の同意を得なければならない。本人の同意なしで要配慮個人情報を取得することができるのは、図表3のような場合に限られる。

図表3 本人の同意なしで要配慮個人情報を取得することができる場合

場合		例	
①	法令に基づく場合	労働安全衛生法に基づき健康診断を実施し、従業員の身体状況等を健康診断実施機関から取得する場合	
②	人の生命等または財産の保護のために必要がある	本人の同意を得ることが困難	急病等の事態で本人の病歴等を医師等が家族から聴取する場合
③	公衆衛生の向上または児童の健全な育成の推進のために特に必要がある		保険者等が実施する健康診断等の結果判明した病名等につき、疫学調査等のために提供を受けて取得する場合 児童虐待のおそれのある家庭情報のうち被害を被った事実に係る情報を、他の関係機関から取得する場合
④	国の機関等の法令の定める事務の遂行に事業者が協力する必要がある	本人の同意を得ることで事務の遂行に支障を及ぼすおそれがある	事業者が警察の任意の求めに応じて個人情報を提出するために、当該個人情報を取得する場合
⑤	要配慮個人情報を本人や国の機関等が公開している場合		—
⑥	本人を目視または撮影することでその外形上明らかな要配慮個人情報を取得する場合		身体の不自由な方が店舗に設置された防犯カメラに映りこんだ場合
⑦	委託、事業承継又は共同利用等によって取得する場合		合併、分社化により、新会社等が個人データを取得する場合

(注) ⑦について、詳しくは本シリーズの次回レポートにて解説予定。

(出所) 個人情報保護委員会「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）」より大和総研作成

³ なお、例えばインターネット等で公開されている情報をただ閲覧するだけの場合（転記等を行わない場合）は、ここで言う「取得」には当たらないと考えられている。

Q 1 - a : 本人の同意って具体的にはどうやって得ればいいのか？

A 1 - a : 本人の同意を得るには、事業の性質や個人情報の取扱い状況に応じて、本人が同意に関する判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。

「本人の同意を得る」とは、本人の個人情報が、個人情報取扱事業者に示された方法によって取り扱われることの承諾を認識することをいう。本人の同意を得るには、事業の性質や個人情報の取扱い状況に応じて、本人が同意に関する判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない。本人の同意を得る方法としては、以下のような場合が挙げられる。

- ・ 本人からの口頭による意思表示
- ・ 本人からの書面（電磁的記録を含む）の受領
- ・ 本人からのメールの受信
- ・ 本人による確認欄へのチェック
- ・ 本人によるホームページ上のボタンのクリック
- ・ 本人による音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

また、未成年者など、個人情報の取扱いについて同意したことによって生じる結果を判断する能力を有していない等の場合は、親権者や法定代理人等から同意を得る必要がある。

Q 2 : 個人情報を取得したら何をしなければならないのか？

A 2 : まず、個人情報取扱事業者は個人情報を取り扱うに当たっては、利用目的をできる限り特定しなければならない。また、個人情報を取得したときは、原則として、速やかにその利用目的を本人に通知し、または公表しなければならない（あらかじめ公表している場合を除く）。

個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用⁴の目的をできる限り具体的に特定しなければならない。どの程度特定する必要があるかという点については、その個人情報がどのような事業にどのような目的で利用されるかが、本人に一般的かつ合理的に想定できる程度に具体的に特定することが望ましい（図表 4）。

⁴ 「利用」には取得と廃棄以外の取扱い全般が該当すると考えられ、保管しているだけでも利用に当たる。

図表4 利用目的の特定の例

良い例	〇〇事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします
悪い例	事業活動に用いるため マーケティング活動に用いるため

(注) 良い例は利用目的を具体的に特定しているが、悪い例は具体的に特定していないと考えられる。

(出所) 個人情報保護委員会「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）」より大和総研作成

個人情報取扱事業者は、あらかじめその利用目的を公表していない場合は、個人情報を取得した際に、速やかにその利用目的を本人に通知するか、もしくは公表しなければならない。

また、契約書や懸賞応募はがきによる記載等によって、直接本人から個人情報を取得する場合は、あらかじめ本人に利用目的を明示⁵しなければならない（人の生命、身体または財産の保護のために緊急に必要がある場合を除く）。

ただし、図表5に該当する場合は、個人情報を取得するときに利用目的を本人に通知、公表、明示する必要はない。

図表5 個人情報取得時に利用目的を通知・公表・明示しなくてよい場合

場合		例
①	利用目的を通知・公表することで	本人または第三者の生命、身体、財産等を害するおそれがある
		個人情報取扱事業者の権利等を害するおそれがある
②	本人または第三者の生命、身体、財産等を害するおそれがある	児童虐待への対応で、児童相談所等が加害者本人に個人情報の利用目的を通知・公表すると、虐待が悪化等するおそれがある場合
③	国の機関等の法令の定める事務の遂行に事業者が協力する必要がある	本人等から取得したことが明らかになると情報取得事業者に害が及ぶ場合
④	かつ 利用目的を通知・公表することで事務の遂行に支障を及ぼすおそれがある	警察が非公開で被疑者の個人情報を限られた事業者提供した場合で、事業者が被疑者本人に利用目的を通知・公表すると捜査に支障を及ぼす恐れがある場合
⑤	取得の状況からみて利用目的が明らかであると認められる場合	商品等の販売・提供のみを確実にを行うための利用目的で個人情報を取得する場合（今後の連絡のために名刺の交換をする場合等）

(出所) 個人情報保護委員会「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）」より大和総研作成

Q 2 - a : 特定した利用目的以外の目的で個人情報を利用することはできないの？

A 2 - a : 個人情報取扱事業者は、特定した利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことは原則としてできない（あらかじめ本人の同意を得た場合を除く）。

⁵ 「明示」とは本人に利用目的を明確に示すことをいい、利用目的を明記した書面を手渡し、または送付すること等を指している。

個人情報取扱事業者は、あらかじめ本人の同意を得ていない場合は、利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことはできない（図表 6 に該当する場合を除く）。

例えば、合併等によって他の個人情報取扱事業者から個人情報を取得した場合も、合併等の前の当該個人情報の利用目的の達成に必要な範囲外での利用はできない。

図表 6 本人の同意なしで個人情報の利用目的外利用が可能な場合

場合			例
①	法令に基づく場合		税務署の調査や警察の捜査に応じる場合
②	人の生命等または財産の保護のために必要がある	かつ	本人の同意を得ることが困難
③	公衆衛生の向上または児童の健全な育成の推進のために特に必要がある	かつ	
④	国の機関等の法令の定める事務の遂行に事業者が協力する必要がある	かつ	
			急病等の事態で本人の血液型や家族の連絡先を医師等に提供する場合 保険者等が実施する健康診断等の結果等にかかる情報を、疫学調査等に利用する場合 児童虐待のおそれのある家庭情報を児童相談所等が共有する必要がある場合 事業者が税務署または税関の職員等や警察の任意の求めに応じて個人情報を提出する場合

（出所）個人情報保護委員会「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）」より大和総研作成

Q 2 - b : 利用目的を変更することはできるの？

A 2 - b : 利用目的の変更は、変更前の利用目的と関連性を有すると合理的に認められる範囲ならば、行うことができる。ただし、利用目的を変更した場合は、変更後の利用目的等を本人に通知し、または公表しなければならない。

利用目的の変更は、変更前の利用目的と関連性があると合理的に認められる範囲で許されている（図表 7）。この「合理的に認められる範囲」とは、一般人の判断において、当初の利用目的と変更後の利用目的を比較して予期できる範囲をいい、当初の利用目的との関連性を総合的に勘案して判断される。

利用目的を変更した場合は、変更された利用目的について、本人に通知するか、もしくは公表しなければならない（図表 5 に該当する場合を除く）。

図表 7 変更前の利用目的と関連性を有すると合理的に認められる範囲の例

	変更前	変更後
認められる例	フィットネス事業者が顧客の食事メニューの指導サービスを行うため	フィットネス事業者が顧客に当該食事メニューに関する食品の販売サービスを行うため
認められない例	会員カード等の盗難・不正利用発覚時の連絡のため （第三者提供を含まない目的）	当該企業が提供する商品・サービスに関する情報のお知らせのため オプトアウトにより第三者提供をするため

（出所）一部（認められる例）は、瓜生和久編著『一問一答 平成 27 年改正個人情報保護法』（商事法務、2015 年）を参考に、大和総研作成

Q 3 : 個人情報是一次取得したらずっと保有していてもいいの？

A 3 : 個人情報取扱事業者は、利用する必要がなくなったときは、個人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。

個人情報取扱事業者は、不必要に個人データを保有し続けるのではなく、利用する必要がなくなったときは、遅滞なく消去するように努めなければならない。また、個人データは、利用目的の達成に必要な範囲内で、正確かつ最新の内容に保つよう努めなければならない。

利用する必要がなくなったときの例としては、個人データの利用目的が「商品の修理やサポート等」であり、そのサポート等の期間が終了したとき等が考えられる⁶。

このほかに個人データを消去等しなければならない場合として、保有個人データの本人から Q 1、Q 2、Q 2-a における取得・取扱いの方法に違反しているから消去等してほしいという請求があった場合は、当該保有個人データの消去等を原則として行わなければならない（詳しい対応等については Q 5 にて解説する）。

Q 4 : 個人データに関して何かしなければならないことはあるの？

A 4 : 個人情報取扱事業者は、①取り扱う個人データの安全管理のための各種措置・監督、②当該事業者の名称・保有個人データの利用目的・各種請求に応じる手続き等の公表を行わなければならない。

個人情報取扱事業者は、取り扱う個人データについて、漏えい・滅失・毀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行わなければならない。また、従業者⁷に個人データを取り扱わせる場合や個人データの取扱い（全部または一部）を第三者に委託する場合は、安全管理が図られるように従業者・委託先に対して必要かつ適切な監督を行わなければならない（委託に関しては Q 7 で詳述する）。

安全管理の手法の例としては、規律の整備、従業員の教育、機器等の盗難の防止、アクセス制御等が考えられるが、講ずべき措置は事業者によって異なるため、「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）」の「講ずべき安全管理措置の内容」を参考に、事業者ごとに検討することが望ましい。

また、個人情報取扱事業者は保有個人データに関して、図表 8 に掲げた項目について、本人

⁶ 瓜生和久編著『一問一答 平成 27 年改正個人情報保護法』（商事法務、2015 年）より。

⁷ 個人情報取扱事業者の指揮監督を受けて業務に従事している者等をいい、派遣社員等も含む。

の知り得る状態（本人の求めに応じて遅滞なく回答する場合も含む）にしておく必要がある。

「知り得る状態」とは、例えば事業所の窓口で書面で掲示したり、事業者のホームページ上のわかりやすい場所（トップページから 1 クリックで到達できる場所等）に掲載することで、本人が知ろうとすれば確実に認識できるようにしておくことを指す。

図表 8 保有個人データに関して公表すべき項目

①	個人情報取扱事業者の氏名または名称
②	全ての保有個人データの利用目的
③	保有個人データの利用目的の通知の求めの手續、手数料
④	保有個人データの開示等の請求(Q5参照)の手續、手数料
⑤	保有個人データの取扱いに関する苦情の申出先

(注1) ②については図表5の①～③の場合は除く。

(注2) 個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合は、その団体の名称及び苦情解決の申出先も公表すべき項目となる。

(出所) 個人情報保護委員会「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）」より大和総研作成

Q5：保有個人データの本人に請求されたいらなければならないことって？

A5：個人情報取扱事業者は、保有個人データの本人から、図表9の請求があった場合は、原則として、その請求に応じなければならない。また、請求に応じないことを決定した場合は、本人に遅滞なくその旨を通知しなければならない（図表9の③～⑤の請求の場合は、応じることを決定したときも通知の必要がある）。請求に応じない場合（請求された措置と異なる措置をとる場合も含む）は、本人にその理由を説明するように努めなければならない。

個人情報取扱事業者は、保有個人データの本人から図表9の請求があれば、原則、その請求された措置をとる必要がある。請求された措置の全部または一部について、その措置をとらない場合は、その旨を本人に通知する必要があり、かつ、その理由を説明するように努めなければならない。

また、個人情報取扱事業者はこうした請求を受け付ける方法を定めることができ、請求を行う本人はその方法に従わなければならない⁸。ここで定めることができる方法とは、①請求の申出先、②請求の方式（請求に際して提出する書面の様式等）、③請求者が本人または代理人⁹であることの確認方法、④手数料の徴収方法（手数料については後述）の4点である。

なお、請求を受け付ける方法を定めた場合は、その方法を本人の知り得る状態（本人の求め

⁸ 請求を受け付ける方法が定められていない場合は、本人は任意の方法で請求をすることができるため、事業者は個別に相談しながら対応を行うこととなる。

⁹ 図表9の請求は、代理人が行うことができる。ただし代理人として認められるのは、①未成年者または成年被後見人の法定代理人、②請求をすることにつき本人が委任した代理人のいずれかに限られる。

に応じて遅滞なく回答する場合も含む) にしておく必要がある (図表 8)。

請求があった場合は、個人情報取扱事業者は、本人に請求の対象となる保有個人データを特定するに足りる事項を提示してもらうことができる。例えば、本人が「貴社が保有する私の情報の全てを開示せよ」という請求をしてきた場合は、その本人に開示を請求する保有個人データの範囲を特定してもらうことができる。個人情報取扱事業者は、その特定された保有個人データを開示すれば事足りる¹⁰。

図表 9 個人情報取扱事業者が対応すべき本人からの請求

	保有個人データに対する請求	請求に応じなくてもよい場合
①	利用目的の通知	事業者がQ4のように公表をしていることで、利用目的が明らかである 図表5の①～③に該当する
②	開示	本人または第三者の生命、身体、財産等を害するおそれがある 事業者の業務の適正な実施に著しい支障を及ぼすおそれがある 他の法令に違反することとなる
③	内容の訂正、追加または削除 (内容が事実でないときに限る)	利用目的からみて訂正等が必要ではない 保有個人データが誤りである旨の指摘が正しくない
④	利用の停止または消去 (保有個人データがQ1、Q2、Q2-aの規定に違反して取得・利用されている場合に限る)	違反である旨の指摘が正しくない 利用停止等を行うことが困難(多額の費用を要する等)であり、本人の権利利益を保護するための代替りの措置をとる
⑤	第三者への提供の停止 (規定に違反して提供されている場合に限る)	違反である旨の指摘が正しくない 提供の停止を行うことが困難(多額の費用を要する等)であり、本人の権利利益を保護するための代替りの措置をとる

(注1) ここでいう「保有個人データ」は、請求を行う本人が識別される保有個人データに限られる。

(注2) 開示の請求に応じる場合、本人と同意した方法が別にない限り、書面の交付により開示を行う。

(注3) ③の請求があった場合は、遅滞なく必要な調査を行い、その結果に基づき対応を行う必要がある。

(注4) ⑤の第三者への提供の詳細と規定については、本シリーズの次回のレポートで取り扱う。

(出所) 個人情報保護委員会「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)」より大和総研作成

Q5-a : 本人の請求に応じる場合は手数料はとっていいの？

A5-a : 個人情報取扱事業者は、図表9の①(利用目的の通知)、②(開示)の請求を受けたときは、この実施に関して手数料を徴収することができる。

¹⁰ ただし、このような場合は、個人情報取扱事業者は本人が容易かつ的確に請求ができるように、請求の対象となる保有個人データの特定に資する情報の提供等の措置をとる必要がある。

個人情報取扱事業者は、保有個人データの利用目的の通知、開示の請求を本人から受けたときは、この実施に関して手数料を徴収できる。ただし、手数料の額は、措置にかかる実費を勘案して合理的であると認められる範囲内に定めなければならない。また、定めた手数料の額は、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合も含む）にしておく必要がある（図表 8）。

Q 6 : 匿名加工情報は どうやって作るの？ 取扱いで気を付けることは？

A 6 : 匿名加工情報は、特定の個人を識別したり、作成に用いた個人情報を復元することができないように、図表 10 の基準に従って作成しなければならない。
また、匿名加工情報を取り扱うときは、その作成に用いられた個人情報の本人を識別するために、当該匿名加工情報を他の情報と照合したり、加工方法等の情報を取得してはならない¹¹。

図表 10 匿名加工情報作成時に従うべき基準（個人情報保護委員会規則）

基準		例
①	特定の個人を識別することができる記述等の全部または一部	を削除すること
②	個人識別符号の全部	を元の記述等を復元できないように他の記述等に置き換えること
③	情報を相互に連結する符号（個人情報の管理用ID等）	を元の記述等を復元できないように他の記述等に置き換えること
④	特異な記述等	を元の記述等を復元できないように他の記述等に置き換えること
⑤	①～④以外の適切な措置	を元の記述等を復元できないように他の記述等に置き換えること

(注) 仮 ID に置き換えるときは、元の記述を復元できる規則性を有しないように、乱数等の他の記述を加えた上でハッシュ関数等を用いるなどの手法を検討することが考えられている。

(出所) 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」より大和総研作成

個人情報取扱事業者は、匿名加工情報作成時には、特定の個人の識別や個人情報の復元ができないよう、図表 10 の基準に従う必要がある（詳細は個人情報保護委員会規則 19 条等を参照）。

また、作成時には、作成に用いた個人情報から削除した記述や個人識別符号、加工方法等の漏えいを防止すべく、安全管理のための措置をとる必要がある。そのとき、図表 11 の基準に従わなければならない（詳細は個人情報保護委員会規則 20 条等を参照）。これに加え、作成した

¹¹ なお、匿名加工情報の第三者提供等については、本シリーズの次回のレポートで取り扱う。

匿名加工情報の安全管理に必要な措置や苦情の処理等の措置を自ら講じ、その内容を公表するように努めなければならない。

図表 11 匿名加工情報の安全管理で従うべき基準（個人情報保護委員会規則）

		構すべき措置	例
①	加工方法等情報	を取り扱う者の権限および責任の明確化	安全管理措置を講ずるための組織体制の整備
②		の取扱いに関する規程類	の整備 規程等の整備
		に従った適切な取扱い	規程等に従った運用、従業員の教育
③		の取扱い状況の評価、それに基づく改善措置	取扱状況の確認手段の整備、取扱い状況の把握、安全管理措置の評価・見直し・改善
		を取り扱う権限のない者による加工方法等情報の取扱いの防止	機器、電子媒体等の盗難等の防止 加工方法等情報へのアクセス制御

（出所）個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）」より大和総研作成

さらに、作成時には、作成した匿名加工情報に含まれる個人に関する情報の項目を、インターネット等により遅滞なく公表しなければならない。例えば、「氏名・性別・生年月日・購買履歴」という情報から、図表 10 の適切な措置を講じた上で「性別・生年月日・購買履歴」を匿名加工情報として作成した場合、この「性別」「生年月日」「購買履歴」という項目を公表する必要がある¹²。

匿名加工情報を取り扱う場合、①本人を識別するために他の情報と照合すること、②当該匿名加工情報の加工方法等の情報を取得することは禁止されている。

①について、例えば匿名加工情報を個人と関係のない気象情報等とともに統計的に分析をすることは識別のための照合には当たらない。しかし、保有する個人情報と匿名加工情報の共通する記述等を選別して照合したり、自ら作成した匿名加工情報を作成の元となった個人情報と照合すること等は、識別のための照合に当たるため、禁止されている。

Q 7 : 個人データの取扱いを業者に委託してもいいの？

A 7 : 委託することは可能だが、適切な委託先の選定、委託契約の締結、委託先の個人データ取扱い状況の把握等、委託先の必要かつ適切な監督を行う必要がある。

個人データの取扱いを業者等に委託¹³する場合は、委託された個人データの安全管理を図るた

¹² ただし、個人に関する情報の項目が同じである匿名加工情報を、同じ手法で反復・継続的に作成する場合は、最初の作成時にその旨を明らかにすれば、その後作成される匿名加工情報に係る公表については最初の公表により行われたものと解される。

¹³ ここでいう「委託」とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱い

めに、委託先に対する必要かつ適切な監督を行わなければならない。

例えば、「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）」の「講ずべき安全管理措置の内容」に従って安全管理措置が確実に実施されている業者を委託先として選定するようにすることが考えられる（適切な委託先の選定）。また、委託先と委託元の合意内容等を盛り込んだ委託契約の締結も行うべきであろう。さらに、定期的な監査・調査等による委託先の個人データ取扱い状況の把握が求められる。

また、利用目的の達成に必要な範囲内で個人データの取扱いを委託する委託先は、個人情報保護上の「第三者」には当たらず、委託先に個人データを提供するときには第三者への提供の際の規制を受けない¹⁴。ただし、委託先が外国の事業者である場合、「外国にある第三者」への提供として規制を受ける点には注意が必要である。

Q 8 : もし個人データが漏えいしてしまったらどうすればいいの？

A 8 : 保有する個人データ等が漏えいしてしまった、もしくはそのおそれがある場合は、図表 12 に掲げる必要な措置を講ずることが望ましい。また、原則として、漏えいの実関係や再発防止策等を、個人情報保護委員会等に速やかに報告するよう努めなければならない。

図表 12 個人データ漏えい時に必要とされる措置

①	責任ある立場の者へ直ちに報告
②	被害の拡大防止
③	事実関係の調査・原因究明
④	影響範囲の特定
⑤	再発防止策の検討・実施
⑥	影響を受ける可能性のある本人への連絡等
⑦	事実関係・再発防止策等の公表

(出所) 個人情報保護委員会「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」より大和総研作成

個人情報取扱事業者は、保有する個人データや匿名加工情報の加工方法等が漏えいしてしまった、もしくはそのおそれがあることが発覚した場合は、図表 12 の必要な措置を講ずることが望ましい。

を行わせることをいい、例えば個人データの入力や編集、分析を委託することが当たると考えられている。ただし、配送事業者を利用して個人データに含まれる「相手の名前、住所」宛てに荷物を送る場合等は、特別に合意があった場合を除き、配送事業者に個人データの取扱いの「委託」をしたとはみなされないと考えられている。

¹⁴ 第三者への提供、海外との関係については、本シリーズの次回以降のレポートで取り扱う。

例えば、②被害の拡大防止として、外部からの不正アクセスによる漏えいが疑われる場合は、ネットワークからの切り離し（LAN ケーブルを抜く等）といった対応が考えられる。また、④影響範囲の特定では、漏えいした個人データの内容、本人の数、漏えい手段、原因等を踏まえて特定を行うべきだろう。⑥影響を受ける可能性のある本人への連絡等については、漏えいの事実関係等について、速やかに本人に連絡するか、本人が容易に知り得る状態に置く（本人がアクセスできるホームページへ掲載する等）ことが求められる。

また、個人情報取扱業者は、漏えいの事実関係や再発防止策等を個人情報保護委員会等に速やかに報告するよう努めなければならない。ただし、漏えいした個人データ等を第三者に見られる前に全て回収した場合や、メールの誤送信等のうち軽微なものの場合には報告の必要はない。

報告先は、基本的には個人情報保護委員会だが、金融庁所管業者は金融庁、情報通信業等は総務省、不動産業等は国土交通省と、業種によっては報告先が異なることには留意する必要がある。

【今後のシリーズレポートタイトル予定】

今さら聞けない個人情報保護法のQ & A③

～個人情報を第三者に提供するときに気を付けることは？～

今さら聞けない個人情報保護法のQ & A④

～個人情報保護法と海外の個人や企業との関係は？（GDPR との関係は？）～

今さら聞けない個人情報保護法のQ & A⑤

～金融関連分野での扱いはどうなっているの？～