基礎研レポート

2020年個人情報保護法改正法案の解説

EUの一般データ保護規則（GDPR）との比較も含めて

保険研究部 取締役研究理事　松澤　登
(03)3512-1866　matuzawa@nli-research.co.jp

1――はじめに

従前から、個人情報（プライバシー）については、第三者による個人情報利用が本人の受忍限度を超える場合、人格権の侵害として、不法行為による損害賠償の対象となるという法律上の保護法益であるとされてきた。

個人情報保護法（以下、法という）は、上記のような認識のもと、2003年に、民間事業者による個人情報の利用と保護について定めた法律である（2015年最終改正）。法はおおむね以下のような構成となっている。なお、個人情報保護法等を施行するための公的監督機関として、個人情報保護委員会が設置されている（法第59条以下）。

(1)　個人データを利用する事業者への規制適用

特定の個人を識別できる情報、または個人識別符号が含まれる情報を個人情報と定義する。この個人情報をデータベース化（データベースに含まれる個人情報を個人データという）して利用する事業者を、個人情報取扱事業者として規制の対象とする[1]。

(2)　個人情報取扱事業者に対する本人の権利

個人データは、公表または本人に通知された目的内でのみ利用ができる。また、個人データの本人は、個人情報取扱事業者に対して、自己の情報の開示を請求することができ、情報が誤っている場合などには訂正や利用停止を求める権利がある。

(3)　個人データの第三者提供に関する規律

個人データを第三者に提供する場合は、①あらかじめ本人から同意を取得する、②申し出により提供を中止することを条件として、一定の手続きを経て第三者に提供する。あるいは③匿名加工をすることで個人データに該当しないようにしてから提供するという方法がある。

[1] なお、本論で述べないが、開示対象となる保有個人データには取得後六か月以内に消去される個人データを含まないとされていたが、改正法案ではこのような限定はなくなった。

個人情報保護法は 3 年ごとに見直しがされることとなっており、2015 年改正（施行は 2016 年 1 月以降順次）より 3 年経過した 2019 年 1 月から改正の検討がなされ、現在、改正法案が国会に付議されている。

以下、この（1）～（3）についての現行法の内容と改正法案の内容、および、改正法案で新たに導入される仮名加工情報について解説を加えたい。

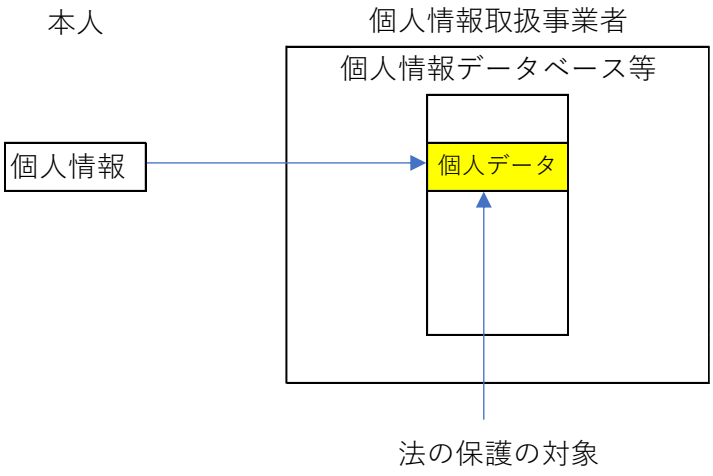
2――個人データを利用する事業者への規制適用

1｜個人情報取扱事業者の定義

個人情報取扱事業者は、個人情報データベース等を事業に利用している事業者と定義されている（法第 2 条第 5 項）。個人情報データベース等とは、電子計算機やファイリングシステムにより、特定の個人情報を検索[2]できるように体系的に構成したものをいい（法第 2 条第 4 項）、個人情報データベース等を構成するデータを個人データという（法第 2 条第 6 項）。

たとえばスポーツクラブ入会の申込書に住所・氏名等記入をした場合に、住所・氏名等を申込書に記入した段階では個人情報ではあるが、法が定義している個人データではない[3]。住所・氏名等がデータベースに入力され、あるいは検索しやすいようにファイリングされた場合に個人情報データベース等を構成することになり、個人データとなる。この段階で法の規制対象となる（図表 1）。

【図表 1】



2003 年の法制定当初においては、個人情報データベース等の個人データ数が 5000 件以下の小規模事業者は法の適用外（旧法第 2 条第 5 項）であったが、2015 年改正により、小規模事業者も規制対象となった。この改正の影響は意外と大きく、小規模事業者は営利業者のみならず、非営利の団体も含むことから、自治体やマンション管理組合の名簿も規制対象に含まれるようになった。

[2] 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こととなるものを含む
[3] 誤解がないように補足すると、個人データとなると個人情報保護法の保護対象となるが、個人情報の段階では不法行為による保護が受けられる。

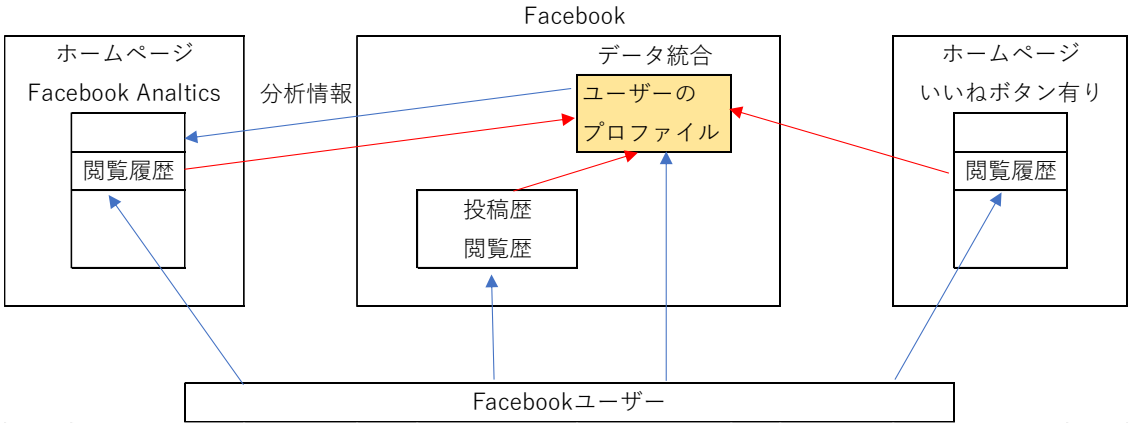
2｜個人情報の範囲とこれまでの議論

個人データのもととなる個人情報には、住所・氏名等の文字情報（紙や電子データで記載されたもの）のみならず、音声や動画などであっても、特定個人が識別できるものであれば該当する（法第 2 条第 1 項第 1 号）。したがって、例えば職場内を撮影している防犯カメラの映像であっても、データベース化されるのであれば、個人データとなる。もう一つは個人識別符号であり（同第 2 号）、これは保険証番号や免許証番号など公的な符号が対象となる。今回の見直しでは、個人情報そのものの範囲についての改正提案はない。

今回、議論になったのは、オンライン識別子である。典型的には、いわゆるクッキーと呼ばれる技術がある。これは、たとえばＰＣやスマホなどの端末で、サイトを閲覧した場合に、サイト側から閲覧した端末を特定できるように、短い情報を閲覧者の端末に書き込むといったことが行われる。そうすると同じ端末が同じサイトを再度閲覧した時には、サイト側はクッキーにより過去の閲覧履歴が追跡できる。この技術により、閲覧者は前回見たサイトページから続きを読むことができるなどのメリットがある。

ところが、このような技術により、問題が発生した。まずドイツの連邦カルテル庁が、Facebook に対してデータ統合を禁止した旨を公表した[4]。具体的には、Facebook が、Facebook の閲覧履歴だけではなく、他のサイトで Facebook のシェアボタンが埋め込まれているサイトや、Facebook Analytics の契約をしているサイトから閲覧履歴を収集したうえで、Facebook のアカウントに連動・統合させていた。この結果、Facebook は個人の閲覧履歴を幅広く収集することが可能となっていた。しかし、データ主体はそのことを理解していなかったことが、市場の濫用行為であるとした（図表 2）。

【図表 2】



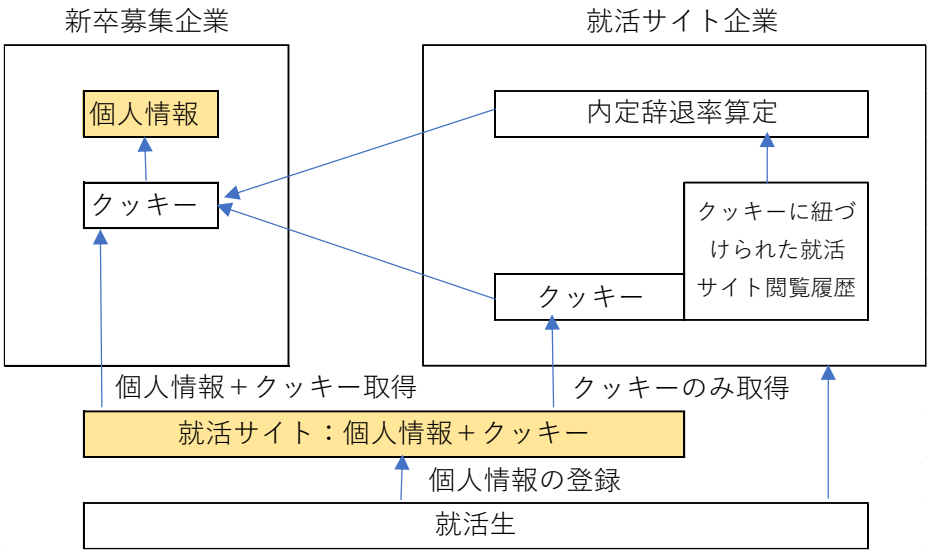
この事例が興味深いのは、ドイツにおける個人情報保護に関する規律（ＥＵ域内では、ＥＵの規則であるＧＤＰＲ （General Data Protection Regulation：一般データ保護規則）が直接適用される）に関してではなく、市場における企業の競争ルールである競争法違反とした点である。この点、日本でも同様の議論がある。すなわち、デジタル・プラットフォーム事業者は、その提供するサービスと交換に個人情報を取得するという取引を行っているとされる。この取引において、正常な商慣習に反

[4] 公正取引委員会の HP 参照 https://www.jftc.go.jp/kokusai/kaigaiugoki/sonota/2019others/201903others.html

して不当に個人に不利益を与えることは優越的地位の濫用に該当するおそれがある。そのため、個人情報の不正な取得は、独占禁止法上問題となりうるとする公正取引員会の見解がある[5]。

また、日本においては、就活サイト企業における個人情報の取り扱いが問題視された案件があった。具体的には、まず、就活サイト企業が設置した、特定の新卒募集企業の就活サイトにおいて、就活生からエントリーシート等の個人情報の登録を求めることとしていた。ここで、就活サイト企業は、氏名等の情報は自身では取得せず、クッキーのみを取得していた。就活サイト企業は当該クッキーによる自社サイトの閲覧履歴に基づく内定辞退率を算定し、その結果をクッキー情報とともに、新卒募集企業に提供していた。新卒募集企業においては、エントリーシート登録時に就活生の情報登録時にクッキーと個人情報の双方を取得していたため、就活サイト企業から内定辞退率とクッキーを取得することで、内定辞退率を個人情報とを紐づけ、個人データとして取得することができた（図表 3）。

【図表 3】



この案件では、就活サイト企業においては、内定辞退率を含む情報はクッキーだけに紐づけて管理しており、個人名とは紐づいていなかった。そのため、就活サイト企業では個人データには該当しなかった。しかし、就活生がエントリーシートを提出した先の新卒募集企業において、個人名に統合される仕組みになっていたため、実質的に見れば、個人データの第三者提供とも考えうる案件であった。

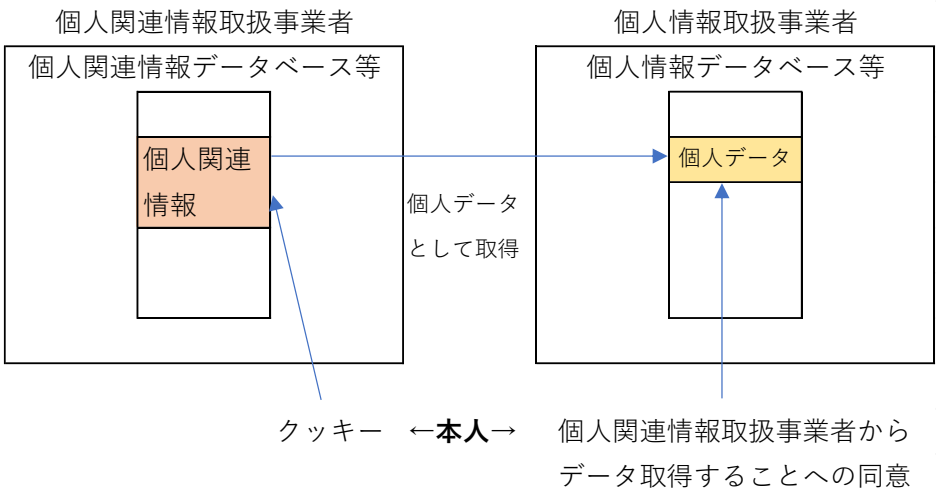
3｜提供先で個人情報になるデータ提供規制の導入

この問題は、提供元で個人データに該当しない場合は、個人データの第三者提供に該当しないこと

[5] 公正取引委員会「デジタル・プラットフォーム事業者と個人情報等を提供する消費者との取引における優越的地位の濫用に関する独占禁止法上の考え方」
https://www.jftc.go.jp/houdou/pressrelease/2019/dec/191217_dpfgl_11.pdf 参照。

から生じたものと捉えられている（提供元基準）[6]。そこで、今回の改正案においては、個人データに該当しない情報のデータベース（個人関連情報データベース）を利用する個人関連情報取扱事業者が提供するデータが、提供先の第三者（個人情報取扱事業者）において個人データとなるときは、その第三者が本人からあらかじめ同意を得ていなければならないとされた（改正法案第 26 条の 2。図表 4）。

【図表 4】



4｜残された課題:オンライン識別子の取り扱い

上記 3 に関連して、ＧＤＰＲではクッキーなどのオンライン識別子が、直接的に個人データであるとしている（ＧＤＰＲ第 4 条（1））。日本でも最近増加してきたが、海外のサイトを閲覧すると「このサイトではクッキーを取得するが、同意するか」との表示が出るものがある。これは、クッキーが個人情報とされるために、その取得に同意を要するからである[7]。

今回の法改正では、端末の同一性自体が個人データであるとの改正はなされなかった。確かに、家族で共有する端末､インターネットカフェや会社の端末などもあり｡一律に個人データといいにくい。

ところで、昨今のデジタル・プラットフォームでは、端末の閲覧情報を収集し、属性や行動を推測したうえで､それらに適した広告を表示させている｡たとえば出張先のホテルを検索すると､その後､どのサイトを見ても、その地域のホテルの広告が掲載されているのは、そのためである。

このような点に鑑みて、ＧＤＰＲのようにオンライン識別子まで個人情報と見るような規制まで踏み込むかであるが、具体的個人に直接的に結びつく情報に限り、個人情報と考える日本の方式は必ずしも否定されるものではないと考える。例えば、単なる広告を超え、具体的な取引を勧奨するような場合においては、多くの場合には、端末の同一性情報のみの利用ではなく、本人情報と結びつけられて活用される（したがって個人情報として規制対象となる）ものと思われる。また、先の就活サイト

[6] 個人情報保護法いわゆる 3 年ごと見直し制度改正大綱 p 25 参照。https://www.ppc.go.jp/files/pdf/seidokaiseitaiko.pdf
[7] ＧＤＰＲでもオンライン識別子は個人情報とされているが、より具体的には EU の e-Privacy 指令で同意取得が求められている。https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN　参照。なお、ＥＵ規則は直接的に規則が各国内で効力を有するが、ＥＵ指令はその内容に沿った法律を各国が立法することでルールを統一化する。

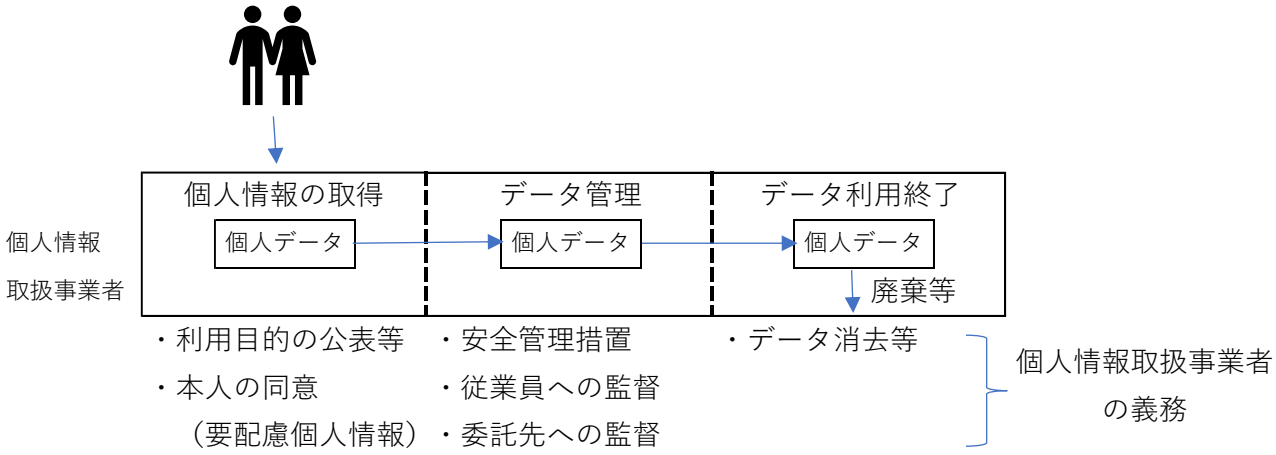
のような事例は、今回の改正で対応ができる。したがって、今後、さらに具体的な弊害事由が生じた場合に、改めて規制の見直しを考えるということでよいと考える。

3――個人情報取扱事業者に対する本人の権利

1｜個人情報取扱事業者の現行法における責務

個人情報取扱事業者の責務としては、まずは①個人情報の適正な取得である。適正な取得とは、利用目的を限定（法 15 条）し、個人情報の取得に当たっては、あらかじめ利用目的を公表するか、当人に通知しなければならない（法 18 条）。また、人種、信条、社会的身分などの要配慮個人情報（法第 2 条第 3 項）については、取得に当たって本人の同意を得なければならない（法第 17 条第 2 項）。②個人データ保護のための安全管理措置を講じなければならず（法第 20 条）、従業員や委託先を適切に監督しなければならない（法第 21 条、第 22 条）。また、③個人データは正確かつ最新の内容に保つとともに、利用の必要性がなくなった時は消去するよう努めなければならない（法第 19 条）。（図表 5）

【図表 5】



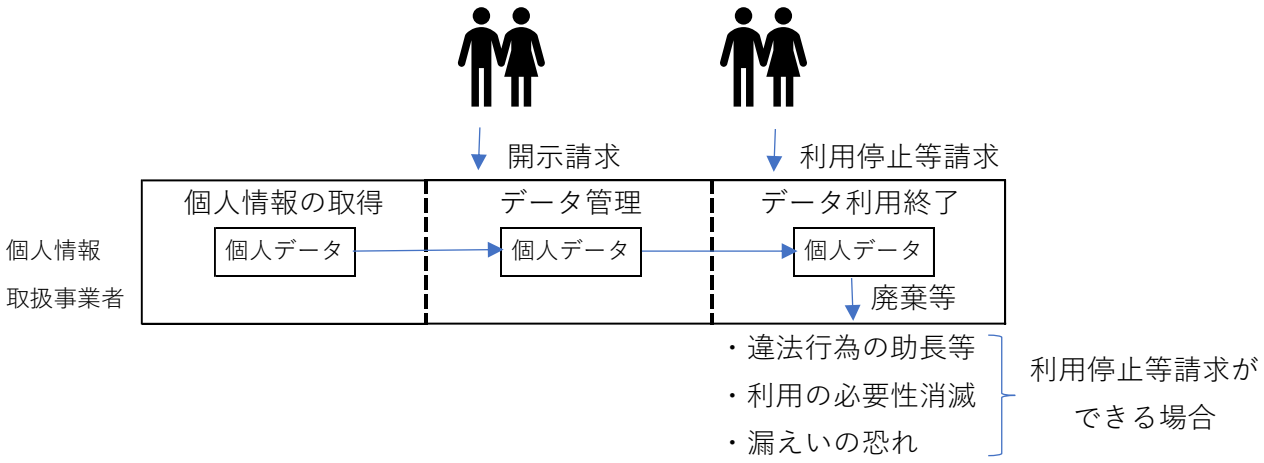
2｜開示請求をはじめとする本人権利の強化

改正法案は、本人からの開示請求および利用停止請求についての権利を強化した。要配慮個人情報以外の個人情報は、必ずしも本人の同意を得て取得されたものではない。また、仮に同意のもとで取得されたものだとしても、個人情報提供後に個人情報取扱事業者による情報管理等が適切に取り扱われることの確保が必要である。

この観点から、本人が利用停止請求などの権利を行使する前提となる、個人データ開示請求権が重要となる。今回の改正では開示請求の方法について改正がなされた。現行法では書面による提供を求めることが原則とされているが、改正法案では電磁的方法で開示を求める方法も明示的に認め、本人が開示の方法を指定できることとした（改正法案第 28 条第 1 項）。ただし、本人の指定した方法では多額の費用を要する場合などには、個人情報取扱事業者は書面によりデータを提供することができる（同条第 2 項）。

事業者の保有する個人データの利用停止または消去（利用停止等）を求められる場合も拡大した。個人情報は違法または不当な行為を助長し、誘発するおそれがある方法により利用してはならない（改正法案第 16 条の 2）として、これに反する個人データの利用停止を求めることができることとした（改正法案第 30 条第 1 項）。また、個人情報取扱事業者が、保有個人データを利用する必要がなくなったとき、あるいは、個人データの漏洩等により本人の利益が害されるおそれがあるときは、個人データの利用停止、または第三者への提供停止（後述）を求めることができる（改正法案第 30 条第 5 項）。（図表 6）

【図表 6】



3｜個人データ漏洩時の事業者の責務の強化

個人データの漏えい、滅失、毀損その他の個人データの安全確保にかかる事態であって、個人の権利・利益を害するおそれが大きいものとして、個人情報保護委員会規則に定める事態が発生した場合は、個人情報保護委員会へ報告する（改正法案第 22 条の 2 第 1 項）とともに、原則として、本人に通知しなければならない（同条第 2 項）とされた。

個人の権利・利益を害するおそれがあるとして報告・通知の対象となるのは、一定数以上の個人データ漏洩、あるいは要配慮個人情報の漏洩等が定められることが想定されている[8]。

4｜残された課題：同意の撤回とデータポータビリティ

ＧＤＰＲでは、合法的な個人データの取得方法はいくつか定められている（ＧＤＰＲ第６条第１項）。仮に、個人データの取得が本人の同意によるものであった場合には、本人はいつでも同意の撤回が可能である（ＧＤＰＲ第 7 条第 3 項）。同意が撤回された場合には、事業者はデータを利用停止・削除しなければならない。そのため、事業者は、契約の締結や履行に必要な情報であることを根拠として取得、あるいは事業者の正当な利益のためという根拠に基づいて取得（ＧＤＰＲ第 6 条第 1 項（ｂ）（ｆ））するなど、同意以外にも取得根拠をもって個人情報を取得することが多い。

[8] 前掲注 6 改正大綱ｐ15 参照。

また、本人が事業者の保有する個人データを、類似サービス業者などに移転する権利も保有する（ＧＤＰＲ第 20 条。データポータビリティの権利）。この権利が行使されると、事業者は他の事業者にデータを電子的に移転しなければならない。

このようにＧＤＰＲでは、個人データを本人が事業者にあたかも預託しているような法的構成になっている。個人データを保有する事業者は、自己の正当な利益に基づくか、あるいは契約履行上必要といえなければ、個人データを本人の意に反して保有し続ける権利はない。

改正法案は、本人が利用停止請求できる場合を拡大するなど権利強化を行ったが、同意の撤回という考え方を導入しなかった。そもそもＧＤＰＲでは同意取得自体が明確な説明に基づいて、自由に与えられるものでなければならないとされ（ＧＤＰＲ第７条第２項、第４項）、自由に与えられた同意と認められるかどうかについて、厳格な姿勢をとっている[9]。このあたり、日本でも今後の課題となる可能性はある。

ただ、ＥＵでの議論にもみられるが、同意のみに依存した個人情報の利用というのは、どこまで行っても限界がある。同意取得に当たって、事業者が詳細に内容を説明しようとすればするほど、本人の理解は進まず、同意の有効性の程度が下がる（＝説明文を読むのが面倒であり、読まずに同意にチェックしてしまう）ことが想定される。同意要件を突き詰めるのではなく、不適正な個人情報利用を具体的に制限していく方向性のほうが望ましいと思われる。

また改正案にはデータポータビリティの権利は認められていない。実務的には、データベースに登録されている個人データを、他の事業者に移転するというのは事業者間で共通のデータベースシステムがない以上、個人情報取扱事業者サイドに大きな障害あるいはコストの発生が容易に想定される。そのため、現状においては、慎重に議論すべきであると思われる。

なお、日本においても情報銀行構想など、情報を本人のコントロールする財産として取り扱う考え方はすでに導入されているともいえる。

4――個人データの第三者提供に関する規律

1｜現行法で第三者提供を行うための三つの方法

個人情報取扱事業者がその保有する個人データを第三者に提供するには、三つの方法がある。まずは①本人の同意を得る方法である。たとえば企業グループ内で個人データを相互に提供しあい、総合的なサービスを提供しようとする場合など、個人情報取得時に本人より同意を取得することが行われている。このように同意した人のデータのみが提供されることをオプトインという[10]。

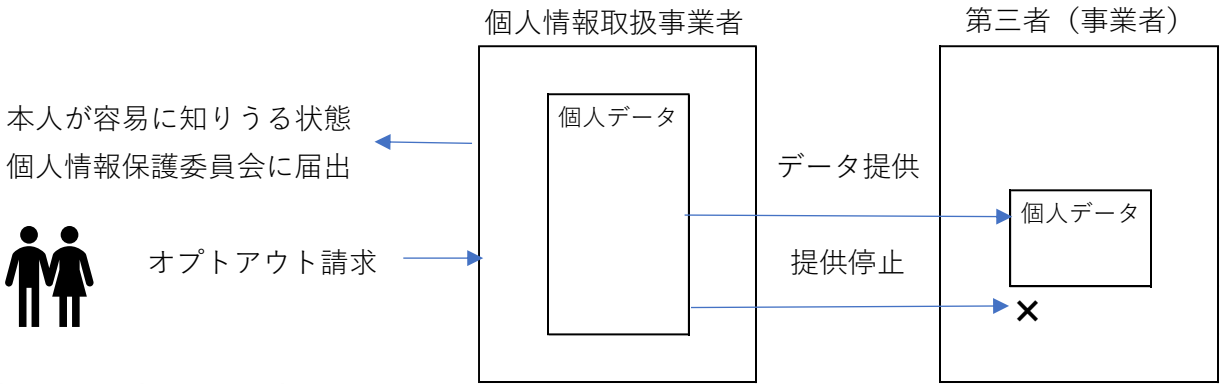
次に、②あらかじめ本人の同意を得ることはせず、オプトアウトでの個人データを第三者提供する方法である。オプトアウトとは、本人の請求があれば、第三者提供を停止することを前提として、本人からあらかじめ同意を取得せず、個人データを第三者に提供するものである。このことを可能とする条件として、一定の個人

9 消費者委員会のＨＰでは、ＥＵのＧＤＰＲの同意取得の要件についてのガイドラインおよび仮訳が閲覧可能である。
https://www.ppc.go.jp/files/pdf/doui_guideline.pdf

10 ただし、日本における同意取得は、現実的に拒否できる選択肢がないなど、ＧＤＰＲが要求するような、本人が情報提供されたうえでの任意の同意ということがむつかしいケースが散見される。

データを第三者に提供することを本人が容易に知りうる状況に置くとともに、個人情報保護委員会に届け出を行うことである（法第 23 条第 2 項。図表 7）。なお、要配慮個人情報については、オプトアウトの方法による第三者提供はできない。

【図表 7】



そして、③匿名加工情報を利用する場合である。匿名加工情報とは、個人を特定できる情報を削除するとともに、個人識別符号を削除すること、および特殊な情報（例えば数の少ない難病にり患しており、その情報だけで個人が特定できる情報）は分類項目を大きくするか、数字を丸めるなどなどを通じて、特定の個人を識別ができないように加工し、個人情報として復元できないものをいう（法第 2 条第 9 項）。このように加工された情報はすでに個人情報と見ることはできないため、そもそも個人データの第三者提供制限の枠外となる。

匿名加工情報はビッグデータを第三者に提供するために考えられ、2015 年改正で導入された規律である。

2｜オプトアウトの規制強化

今回の法改正では上記二つ目の方法である、オプトアウトについての規律が変更された。これは主に、いわゆる名簿屋に関して、業界内で個人データが転売されたり、また、名簿屋の主体が濫用的に営業停止したり、居所が不明になったりと不適正な取り扱いが確認されたため、それらの弊害に対応するための規制改正が行われるものである[11]。

まず、オプトアウトできる個人データは、偽りその他不正の手段により取得したものであってはならない（法第 17 条、改正法案第 23 条第 2 項）。オプトアウトにより取得した個人データを、再度オプトアウトにより第三者提供することも禁止されることなった（同項）。このことにより、名簿屋間の名簿の転売は禁止される。

また、オプトアウトしようとする個人情報取扱事業者は、氏名・名称、住所、法人にあっては代表者の氏名を個人情報保護委員会に届け出しなければならなくなった（改正法案第 23 条第 2 項）。これらを変更したときも届け出が必要である（同第 3 項）。また、オプトアウトする個人データを取得した方法も届け出事項とされた。

[11] 前掲注 6 改正大綱 P12 参照。

3｜第三者提供にかかるトレーサビリティの確保

現行法では、個人データの第三者提供にあたって、提供をする側の記録（法第 25 条第 1 項）、提供を受ける側の記録（法第 26 条第 3 項）の作成が求められてきた。しかし、これは個人情報保護委員会にとってのトレーサビリティであって、本人のトレーサビリティではないとの批判があった[12]。そのため、改正法では、本人がこれらの記録について開示請求ができることとした（改正法案第 28 条第 5 項）。

また、上述の個人データの利用停止等の事由（利用に必要性がなくなる、あるいは本人の正当な利益が害される等）が、第三者提供情報について認められる場合には、利用停止等を求めることができる（改正法案第 30 条第 5 項）。

5――新たに導入される仮名加工情報

1｜仮名加工情報の意味・定義

個人データから、氏名等を削除することによって、個人データの規律がかからないようにする方法としては、すでに匿名加工情報の制度がある。匿名加工情報は上述の通り、第三者提供を前提としており、氏名等の削除のほか、データをある程度丸めないといけないなど、法的な安定性にかけ、使い勝手が悪いとの評価があった[13]。

また、社内で利用するにあたっても、上述の開示の対象になったり、安全管理措置を講じたりするなどの負荷が重いとの問題意識もあった。そこで、個人データから氏名や個別識別符号を削除し、データを特定個人に紐づけられない形にすることで、仮名加工情報として法の定める規制を受けず、利活用を行えることとした。このように個人の識別を要しない場合に簡易な取扱を認めることは、すでにGDPRでも採用されている（GDPR第 11 条）。

匿名加工情報は第三者に提供するに際して加工が行われるが、仮名加工情報は社内利用を前提として加工が行われる。改正法案も仮名加工情報は第三者提供してはならない（改正法案第 35 条の 2 第 6 項）とする。

仮名加工に当たっては、識別できないように氏名等の情報を削除するとともに、復元するために必要となる削除情報等は　必要な安全措置をとらなければならない（改正法案 35 条の 2 第 1 項第 2 項）。

2｜仮名化による規制適用除外

まず①個人データについては収集時の利用目的から目的を変更した場合、個人への通知が必要となるが、仮名加工情報については公表のみでよい（改正法案第 35 条の 2 第 3 項）。そのほか、漏洩時の本人への報告（改正法案第 22 条の 2）、保有個人データにかかる一定の事項（個人情報取扱事業者の氏名等）の公表、本人からの開示請求（法第 28 条）、本人からの訂正請求（法第 29 条）、利用停止（法第 30 条）などの規律は仮名加工情報には適用がない。

したがって、顧客動向の分析を担当するマーケティング部署などが、個人データ管理部門である事

[12] 前掲注 6 改正大綱 p 13 参照。
[13] 前掲注 6 改正大綱 P21 参照。

務所管から仮名加工情報としてデータを受け取れば、本人からの開示請求や利用停止請求とはかかわりなく、分析の基礎データとして利用することができる。

6――おわりに

今回の改正案は、本人からの開示請求から始まる自分の個人データに関する権利を強化するなど、個人情報保護の規律を強化する一方で、仮名加工情報といったデータの利活用にも配慮したバランスの取れたものになっていると思われる。

ところで、今回の新型コロナ感染対策に当たっては、位置情報等の活用が話題となった。携帯会社や店舗等の保有する位置情報や基地局情報、屋外あるいは店内の映像情報を、一部の国の政府が取得・活用して、感染者の濃厚接触者を見つけだし、検査を受けさせ、陽性であれば隔離するということが行われた。

このことはかなりの難問を我々に突き付けている。位置情報という生活の行動、特定の場所にいたということによる趣味趣向、あるいは特定のデモに参加したといった情報すら、防疫という理由があれば、政府に渡してしまうということでよいのかという問題である。日本では、現在までのところ、新型コロナ感染により、欧米ほどの死者を出すことはなかったが、たとえば米国並みの死者が出たとしたならどうなのか。様々な状況を想定しつつ、十分に時間をかけて議論すればよいと思う。海外で成功したからという理由のみで、それに倣うべきという単純な議論ではない。日本の現状にあった考察が求められる。

日本では、駅前の人出の通常時からの減少具合を伝えるとき、ニュースでは必ず「同意を得た個人から取得した位置情報」であることを明確にしてから報道していた。その意味で個人情報がよく守られているのではないかと考える。

片方で、ＥＵのＧＤＰＲやカリフォルニア州の消費者プライバシー法など厳格な個人情報保護法制を入れる国・地域があり、もう片方で、国家や大企業が個人情報を自由に利用できる国・地域がある。どの方向に向かうのか、どこかでバランスをとるのか、新型コロナ禍後の世界がどうなるかは予断を許さないが、グローバル化が止められないとするならば、重大な課題として議論をしていくべきものと思う[14]。

14　今回改正では、法の適用対象となるのが、日本国内にある個人の情報を取り扱う事業者を対象とすることとしている（改正法案第 75 条）。海外にある事業者が日本国内にいる個人に関する個人情報保護法違反の場合の執行の問題は残るが、海外当局との協力が求められる（前掲注 6 改正大綱 p 29 参照）。

