

2020 年改正個人情報保護法の解説

～EUの一般データ保護規則(GDPR)との比較も含めて

ニッセイ基礎研究所 保険研究部 松澤 登

要 旨

1. 2003年に制定された個人情報保護法については3年ごとに見直しがなされている。最終2015年改正(2016年1月以降順次施行)後3年経過したことから、個人情報保護委員会で2019年1月より審議が開始され、2019年12月に改正大綱が公表された。
2. これを受け、2020年通常国会に改正案が付議され、6月5日に可決成立、6月12日に公布された。改正法は一部を除き、公布より2年以内に施行される。改正のポイントは以下のとおりである。
3. まず、情報加工事業者が、クッキーなどのオンライン識別子だけを利用して、匿名のままデータを加工するが、その加工データの提供先では個人情報に該当することとなる場合には、提供先が、本人からあらかじめ個人情報の取得についての本人同意を得なければならないこととされた。
4. 次に、個人情報取扱事業者において、個人データが適切に取り扱われることを確保するための前提としての、本人からの開示請求について、電子的に提供するように求めることができることとした。また、個人データの利用停止等の請求ができる場合を拡大した。そして、重大な漏洩事案が発生した場合、個人情報保護委員会への報告と本人への通知を義務付けることとした。漏洩事案発生時に、これらの対応が求められることを踏まえた事前の準備が欠かせない。
5. また、オプトアウト方式(本人からは事後に提供停止を請求できる)による個人データの第三者提供について、提供できるデータの範囲を限定するなどの改正が行われる。さらに、すでに個人情報取扱事業者間で個人データのやり取りを行った場合に記録をすることが求められているが、改正法ではその記録について本人が開示請求できることとした。
6. 最後に、仮名加工情報という新たな個人データの利用方法を認めることとした。個人データから個人を識別できる情報を削除することで、個人情報保護法の一定の規制を受けず、データを利活用できるとするものである。経営戦略策定にあたってデータをより活用できることが期待される。
7. EUの個人情報保護法制であるGDPRほど厳格ではないが、個人データ保護に関する規律が強化される一方で、仮名加工情報を認めるなど、バランスの取れた改正法となっている。

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。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。

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月から法改正の検討がなされ、2020年通常国会の審議を経て、6月5日に成立、6月12日に公布されている。改正法の主な規定は公布から2年以内に施行される²。以下、公布された改正個人情報保護法については改正法という。

本稿では、この(1)～(3)についての法の内容と改正法の内容、および、改正法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³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）。

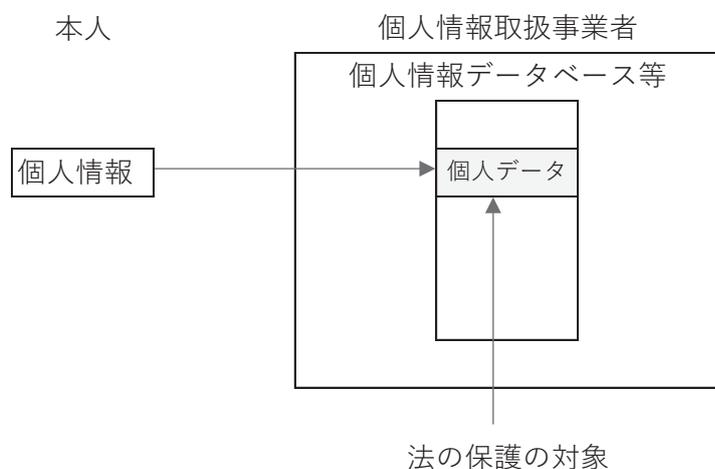
たとえばスポーツクラブ入会の申込書に住所・氏名等記入をした場合に、住所・氏名等を申込書に記

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、改正法ではこのような限定はなくなった。

² 個人情報保護委員会の命令違反などへの罰則の引き上げは2020年12月12日から施行される。

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⁴。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 | 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定義について改正はされていない。

今回、改正されたのは、オンライン識別子に関する規定である。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。

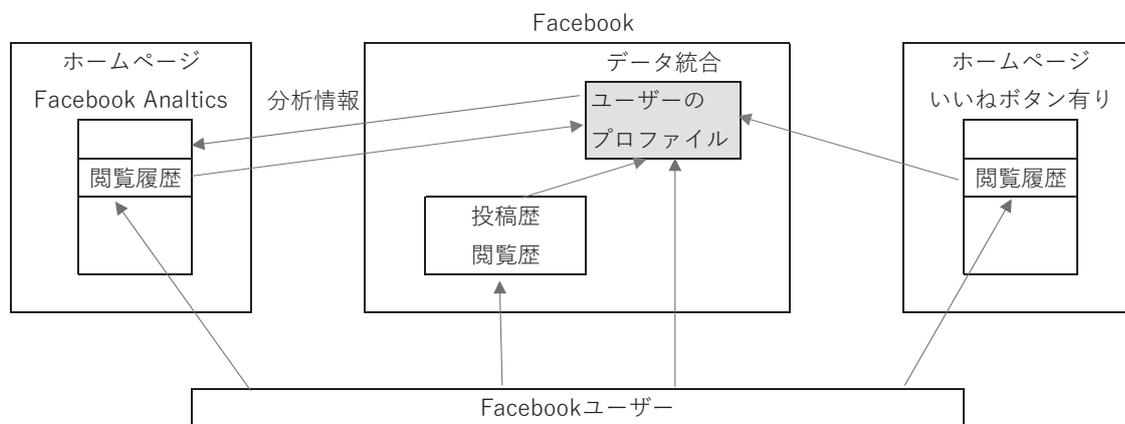
ところが、このような技術により、問題が発生することとなった。ドイツの連邦カルテル庁が、Facebook に対してデータ統合を禁止した旨を公表した⁵。具体的には、Facebook が、Facebook の閲覧履歴だけではなく、他のサイトで Facebook のシェアボタンが埋め込まれているサイトや、Facebook

³ 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

⁴ 誤解がないように補足すると、個人データになると個人情報保護法の保護対象となる。他方、個人情報の段階では、その不当な利用等について不法行為による保護が受けられる。

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】



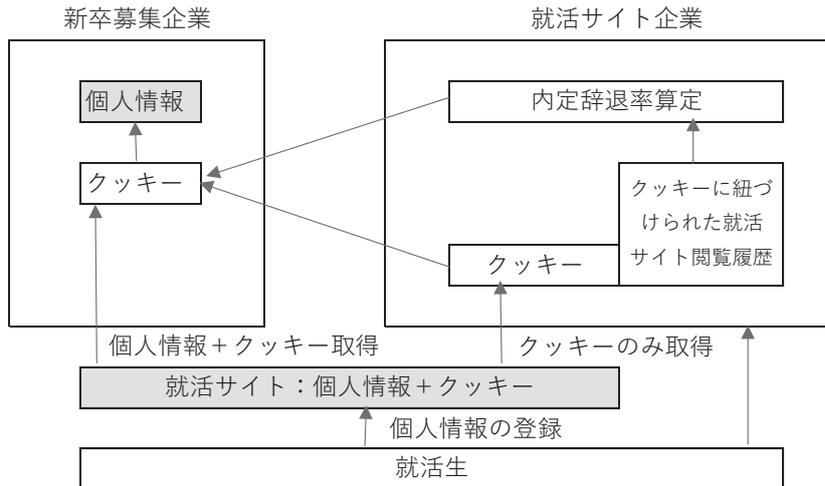
この事例が興味深いのは、ドイツにおける個人情報保護に関する規律（EU域内では、EUの規則であるGDPR（General Data Protection Regulation：一般データ保護規則）が直接適用される）に関してではなく、市場における企業の競争ルールである競争法違反とした点である。この点、日本でも同様の議論がある。すなわち、デジタル・プラットフォーム事業者は、その提供するサービスと交換に個人情報を取得するという取引を行っているとする。この取引において、正常な商慣習に反して不当に個人に不利益を与えることは優越的地位の濫用に該当するおそれがある。そのため、個人情報の不正な取得は、独占禁止法上問題となりうるとする公正取引委員会の見解がある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、新卒募集企業の就活サイトにおいて、就活生にエントリーシート等の個人情報の登録を求めている。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。就活サイト企業はそこで得たクッキーにより閲覧された自社サイトの履歴に基づいて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、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クッキーと内定辞退率を取得することで、内定辞退率を個人情報とを紐づけることができ、就活生の個人データとして取得した（図表 3）。

⁵ 公正取引委員会の HP 参照<https://www.iftc.go.jp/kokusai/kaigaiugoki/sonota/2019others/201903others.html>

⁶ 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.iftc.go.jp/houdou/pressrelease/2019/dec/191217_dpfgl_11.pdf 参照。

【図表 3】

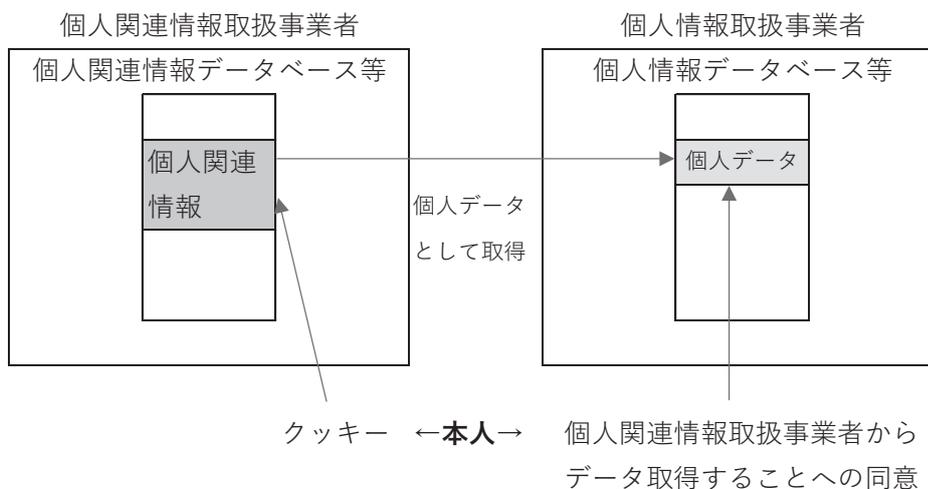


この案件では、就活サイト企業においては、内定辞退率を含む情報はクッキーだけに紐づけて管理しており、個人名とは紐づいていなかった。そのため、就活サイト企業では個人データには該当しなかった。しかし、就活生がエントリーシートを提出した先の新卒募集企業において、個人名に統合される仕組みになっていたため、実質的に見れば、個人データの第三者提供とも考えうる案件であった。

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から生じたものと捉えられている（提供元基準）⁷。そこで、今回の改正法においては、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場合は、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（改正法第 26 条の 2。図表 4）。

【図表 4】



⁷ 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>

この改正により、次のようなケースに注意が必要である。すなわち、事業者が個人に関連する情報を他社から取得する場合に、その情報そのものには氏名などが含まれず、したがって個人情報に該当しないものとする。しかし、その場合であっても、取得した情報を、事業者自身がすでに保有する個人データと照合させて利用するのであれば、本人から同意を改めてとる必要がでてくる。

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⁸。

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って、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。

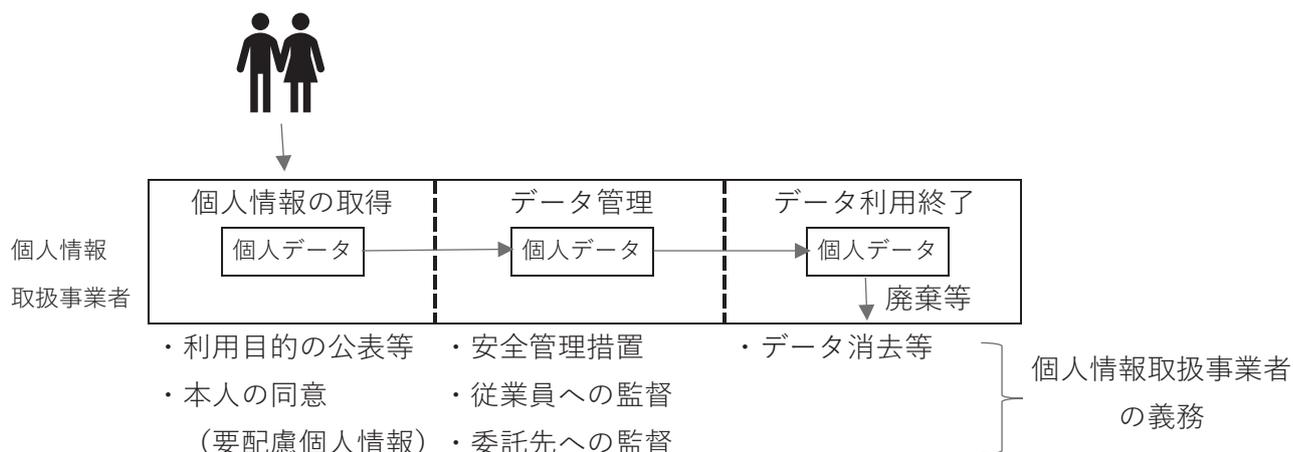
3——個人情報取扱事業者に対する本人の権利

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、本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ない（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)

⁸ GDPRでもオンライン識別子は個人データとされているが、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

【図表 5】



2 | 開示請求をはじめとする本人権利の強化

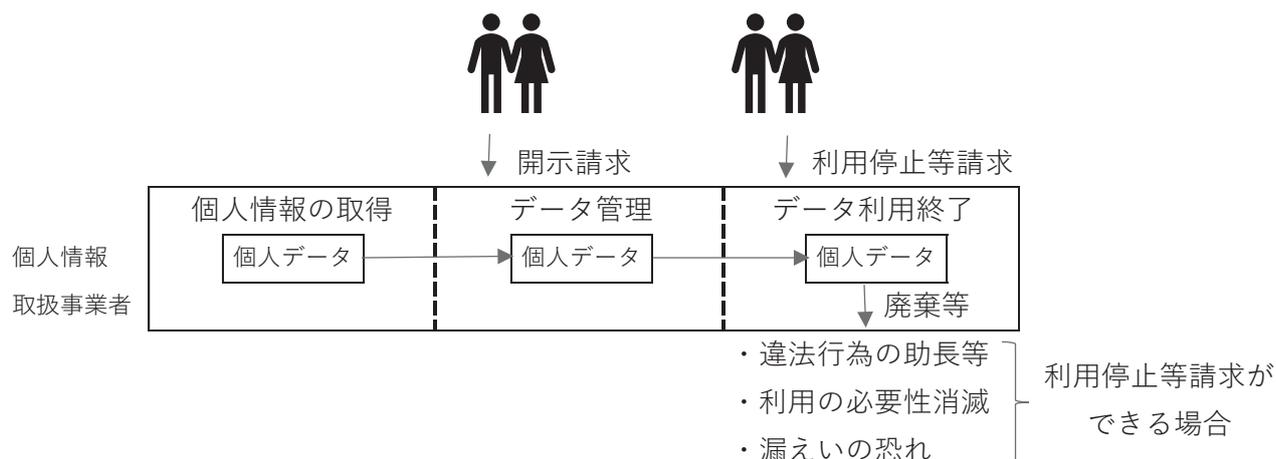
改正法は、本人からの開示請求および利用停止請求についての権利を強化した。要配慮個人情報以外の個人情報は、必ずしも本人の同意を得て取得されたものではない。また、仮に同意のもとで取得されたものとしても、個人情報提供後に個人情報取扱事業者による情報管理等が適切に取り扱われることの確保が必要である。

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。今回の改正法では、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、本人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（改正法第 30 条第 5 項）。（図表 6）

統一化する。

【図表 6】



この改正により、たとえば事業者で情報漏洩の事故が発生した場合に、保有個人データの利用停止を本人から求められることが考えられる。利用停止の範囲が広がったことも踏まえて、改めて顧客対応窓口の明確化や対応手順等を検討しておく必要がある。

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⁹。

令和元年度の個人データの漏洩は 4520 件であり、その多くが書類及びインターネットの誤送付、書類及び電子媒体の紛失である¹⁰。個人情報漏洩案件の多くが、単純ミスに基づくものようである。この観点から、たとえば要配慮個人情報が含まれる書面やメールの送付などについては、ダブルチェックを徹底するなどの対策をとることが望ましい。また、サイバー攻撃による情報流出も同様に、委員会への報告・本人への通知が必要となる。

ところで、本人へ通知するときには、賠償の話は避けて通れない。そもそも本人宛通知のための対応要員確保や、コールセンターの設置費用なども想定される。損害保険会社の提供するサイバー保険への加入も一考しておく必要があるだろう¹¹。

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

⁹ 前掲注 7 改正大綱 p 15 参照。

¹⁰ 個人情報保護委員会「令和元年度 年次報告」p 14 https://www.ppc.go.jp/files/pdf/020612_annual_report_r1.pdf

¹¹ 日本損害保険協会 HP <https://www.sonpo.or.jp/cyber-hoken/about/> 参照。

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。

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¹²。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。

また改正法はデータポータビリティの権利は認めていない。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¹³。

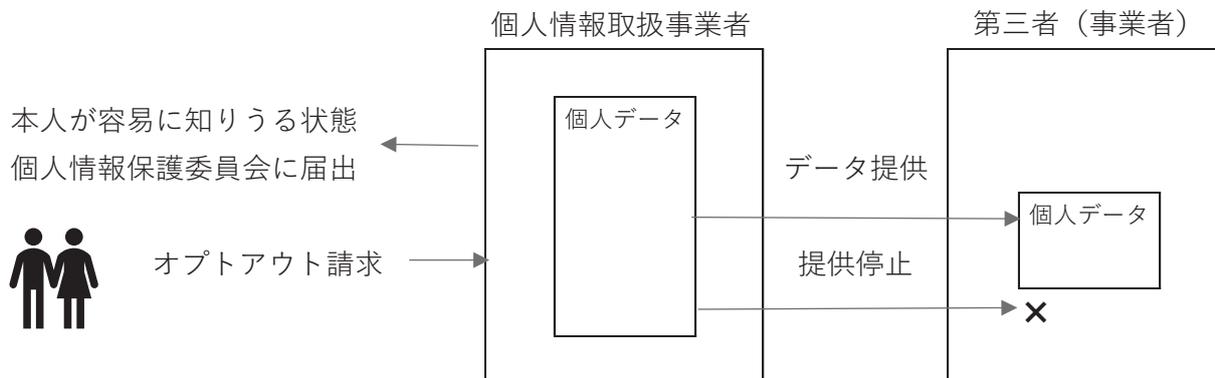
次に、②あらかじめ本人の同意を得ることはせず、オプトアウトでの個人データを第三者提供する方法である。オプトアウトとは、本人の請求があれば第三者提供を停止することを前提として、本人からあらかじめ同意を取得せず、個人データを第三者に提供するものである。このことを可能とする条件としては、一定の個人データを第三者に提供することを本人が容易に知りうる状況に置くとともに、個人情報保護委員会に届け出を行うことである

¹² 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

¹³ 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

(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罹患しており、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たものである¹⁴。

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になった（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い（改正法第 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。

オプトアウトの規定に則って提供されていない名簿の取得は、個人データの不正取得となる可能性が高い。個人データの単なる不正取得には罰則はない（本人から利用停止等は求められうる）ものの、言うまでもなく、出所不明の名簿を事業に利用することは厳に慎まなければならない。このことは経営陣が認識するだけでなく、従業員まで徹底しておく必要がある。

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

提供されたうえでの任意の同意ということがむづかしいケースが散見される。

¹⁴ 前掲注 7 改正大綱 p12 参照。

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¹⁵。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で、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、データがある程度丸めないといけないなど、法的な安定性に向け、使い勝手が悪いとの評価があった¹⁶。

また、社内で利用するにあたって、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仮名加工情報とすることで、個人データとしての規制を受けず、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。改正法も仮名加工情報は第三者提供してはならない(改正法第 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 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。経営戦略策定の基礎データともなりうる仮名加工情報の活用については検討に値すると思われる。

6——おわりに

今回の改正法は、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

¹⁵ 前掲注 7 改正大綱 p 13 参照。

¹⁶ 前掲注 7 改正大綱 P 21 参照。

れたものになっていると思われる。

注意すべきは、改正法は利活用のバランスをとりつつも、個人データの不正利用については厳格な立場をとっていることである。たとえば法人の役職員が個人情報保護委員会の命令に違反した場合や、個人情報データベースの不正提供を行った場合には、法人に1億円以下の罰金が科せられることとなった(改正法第83条、84条、87条1項1号)。

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の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

1718。

¹⁷ 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7改正大綱p29参照)。

¹⁸ なお、報道によれば、自治体の個人情報保護条例のルールを共通化するという議論が今後進められていくとのことである(2020年10月13日日本経済新聞朝刊第5面参照)。