個人情報の取扱いに関する最新動向

情報処理学会　電子化知的財産・社会基盤研究会 主査　原田 要之助
同運営委員　加藤 尚徳
同幹事　小向 太郎
同運営委員　板倉 陽一郎
同幹事　折田 明子
同運営委員　須川 賢洋

1. はじめに

この特集号では、情報処理学会 電子化知的財産・社会基盤研究会（EIP）[*1]の研究者、実務家が執筆を分担した。個人情報については、日本では2017年5月に改正個人情報保護法が施行され、EUでは2018年5月より一般データ保護規則（GDPR）が全面適用された。いずれも、改正事項は多岐に渡るが、データ主体（個人データの本人）の権利を強化する方向が含まれていることは共通する。一方、日本とEUでは、2019年1月23日より、相互に個人データの移転できる仕組みとして相互の認定（EUからの十分性認定、日本からの同等性認定）がなされた。本稿では、現状の個人情報に係る動向について述べるとともに、今後の動向については、法制度、十分性認定、情報銀行や死者のプライバシー問題にフォーカスして論じている。

（研究会主査　原田要之助）

2. 個人情報をめぐる現状

2.1 個人情報保護法制

我が国の個人情報保護法制を歴史的側面から眺めた場合、3つの源流がある。1つ目は、1975年に東京都国立市で制定された「国立市電子計算組織の運営に関する条例」である。我が国においては、電子計算組織（コンピューター）を利用する際の個人情報保護の必要性から、電子計算組織を導入する単位である自治体毎に条例が制定されてきた。続いて、2つ目は、1988年に制定された「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律（以下、行政機関電算機個人情報保護法）」である。国の行政機関における電子計算機処理（コンピューター処理）を対象とした我が国初の国レベルでの個人情報保護法が作られた。ただし、1つ目の源流である条例は併存する形で今日まで維持されており、国レベルでの制度に巻き取られることはなかった。最後に、3つ目として、2003年に制定された「個人情報の保護に関する法律（以下、個人情報保護法）」である。こちらが、今日、一般的に「個人情報保護法」と呼ばれているものである。個人情報保護法は、1つ目が自治体を、2つ目が行政機関を対象としていたのに対して、従来の個人情報保護法制を横断的に適用される形の基本法部分（第1章から第3章）と、民間分野を対象とした具体的義務を定める保護法部分（第4章以降）からなる。加えて、個人情報保護法の下には、各事業分野を所掌する省庁がガイドラインを制定し運用がなされてきた（主務大臣制）。合わせて、同年に、行政機関電算機個人情報保護法の全部改正としての「行政機関の保有する個人情報の保護に関する法律（以下、行政機関個人情報保護法）」ほか、いわゆる個人情報保護法関連五法が整備された。以上のように、個人情報保護法制の範囲は、長年にわたって拡張されてきたと説明できる。そして、このように個人情報保護法制といった場合、いわゆる個人情報保護法だけを指すのではなく、行政機関個人情報保護法のみでなく1700以上の自治体条例が含まれ、その数はおおよそ2000程度あるといわれている。これらの組織間で異なるルールが適用されることにより、様々な問題が生じていることは、「個人情報保護法2000個問題」と呼ばれることもある。以下、特に個人情報保護法に着目して解説を続ける。

*1　情報処理学会 メディア知能情報領域に設置された研究会で、デジタル情報革命によって引き起こされる情報処理とその社会的側面の境界領域に焦点を当てて研究しています。特に、技術的な課題を持った研究者と文科系の研究者が同じテーマを異なる側面で研究しています。ご興味のある方は、年4回開催している研究会にご参加ください。http://eip-ipsj.com/theme.html

個人情報保護法は「個人の権利・利益の保護」と「個人情報の有用性」のバランスを図るために作られた法律である。前述のとおり、個人情報保護法制全体としての基本理念を定めるほか、民間事業者の個人情報の取扱いについて規定している。個人情報保護法第1条にはその目的として「事業者の遵守すべき義務等を定める」こと、「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」こと、が明記されている。「個人情報」は、第2条第1項柱書において、「生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。」とされ、第1号で「当該情報に含まれる氏名、生年月日その他の記述等（･･･）により特定の個人を識別することができるもの（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。）」、第2号で「個人識別符号が含まれるもの（2015年改正によって追加）」と定義されている。また、個人情報をデータベース化等して検索可能な状態にしたものを「個人情報データベース等（第2条第4項）」、「個人情報データベース等」を構成する情報を「個人データ（第2条第6項）」、「個人データ」のうち事業者に修正・削除等の権限があり6か月以上保有するものを「保有個人データ（第二条第7項）」という。個人情報保護法では、民間事業者の個人情報の取扱いについて、①個人情報の取得・利用、②個人データの安全管理措置、③個人データの第三者提供、④保有個人データの開示請求、の4つの基本ルールを規定している。個人情報保護法には適用除外も設けられており、憲法が保障する基本的人権への配慮から、①報道機関が報道の用に供する目的、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、政治団体が政治活動の用に供する目的、で個人情報を取り扱う場合等には、事業者の義務は適用されない（個人情報保護法第76条第1項）。また、これらの者に個人情報を提供する行為には、個人情報保護委員会はその権限を行使しない（個人情報保護法第43条第2項）。個人データの漏えいについては「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」（告示）が定められており、①事業者内部における報告・被害の拡大防止、②事実関係の調査・原因の究明、③影響範囲の特定、④再発防止策の検討・実施、⑤影響を受ける可能性のある本人への連絡等、⑥事実関係・再発防止策の公表、が講ずべき措置とされている。個人情報保護委員会は上記民間事業者の取扱いを担保すべく、事業者に対して、必要に応じて報告を求めたり、立入検査を行うことができる。また、それらの結果等を受けて、指導・助言、勧告・命令を行うことができる。勧告に従わない場合には、罰則が適用される場合もある。命令に違反した場合は「6ヶ月以下の懲役又は30万円以下の罰金」、虚偽の報告には「30万円以下の罰金」、従業員が不正な利益を図る目的で個人情報データベース等を提供・盗用した場合には「1年以下の懲役又は50万円以下の罰金」が課せられる。

個人情報保護法は、2015年9月に大改正されている。2003年の個人情報保護法制定以来、「グレーゾーンの拡大」「ビッグデータへの対応」「グローバル化」への対応が必要となったことから、大幅な改正が行われたものである。改正のポイントは、①個人情報保護委員会の新設、②個人情報の定義の明確化、③個人情報の有用性を確保（利活用）するための整備、④いわゆる名簿屋対策、⑤その他、の5つに分けられる。①としては、個人情報取扱事業者に対する監督権限を各分野の主務大臣会から委員会に一元化した。これまでは各省庁から出されていたガイドラインについても、主に個人情報保護委員会から出されることになった。②としては、利活用に資するために個人情報の定義に身体的特徴等が対象となることを明確化したことと、要配慮個人情報（本人の人種、信条、病歴など本人に対する不当な差別または偏見が生じる可能性のある個人情報）の取得及び第三者提供について原則として本人の同意を得ることが義務化されたこと、が挙げられる。③としては、匿名加工情報の規定が新設された。④としては、個人データの第三者提供に係る確認記録作成等が義務化されたこと、個人情報データベース等を不正な利益を図る目的で第三者に提供し、または盗用する行為を「個人情報データベース等不正提供罪」として処罰の対象とすること、が挙げられる。⑤としては、取り扱う個人情報の数が5000以下である事業者を規制の対象外とする制度を廃止、オプトアウト規定を利用する個人情報取扱事業者の個人情報保護委員会への届出の義務付け、外国にある第三者への個人データの提供の制限・個人情報保護法の国外適用、個人情報保護委員会による外国執行当局への情報提供に係る規定の新設、が挙げられる。

（研究会運営委員　加藤尚徳）

2.2　GDPRの概要

（1）成立の経緯

「EU一般データ保護規則（GDPR：General Data Pro-

tection Regulation」は、欧州連合（EU：European Union）の個人情報保護に関する新しいルールである。欧州諸国では、1970年代から個人情報全般を保護する制度を整備し、専門の監督機関を設置するなど、規制の実効性を担保する取組みが行われてきた。1995年には、より実質的かつ統一的な個人情報の保護を図るために、EU個人データ保護指令（95年指令）が採択されている。これは個人情報全般についてEU域内で求められる個人情報保護のレベルを定めるものであった。

95年指令は、厳格な個人情報保護の制度として世界に知られていたが、データ利用の多様化と重要性の増大に伴い、個人データ保護強化の必要性が議論されるようになってきた。このような新たな状況に対応し、個人情報保護レベルを統一的に確保するために、2016年5月にGDPRが採択された（2018年5月効力開始）。

（2）規制内容

GDPRの導入に当たって特に重視されているのが、透明性の確保である。情報技術の進展によって人々の行動履歴の把握が容易になり、利用者等があまり意識することなく情報を収集されていることが多くなり、情報が思い掛けず使われる懸念も大きくなっている。これによって、自分の個人データがどのように利用されるのかをできるだけ把握できるようにすること、つまり「透明性」がより重要性を増している。こうした状況に対応するため、GDPRでは、本人にとっての透明性を高めることを制度設計の基本思想としている。

具体的な規定を見ると、まずGDPR第6条は個人データの処理の全ての過程について、その処理を適法化する根拠を求めている。個人データが適法とされるためには、（a）本人の同意、（b）契約等の履行のための必要性、（c）法的義務、（d）生命に関する利益、（e）公共の利益・公的権限の遂行、（f）適法な利益、のいずれかの適法化根拠が必要となる（この規定自体は、95年指令にもあった）。そして、適法化根拠は、各個人データについて利用目的ごとに明らかにしなければならない（GDPR 13条1項（c）等）。

GDPRには、個人データ保護に関する新たな懸念に対応するために、**表1**のような新たな制度が盛り込まれており、様々な方法で透明性を高め、本人によるコントロールを確保しようとしている。そして、どの適法化根拠に依拠しているかによって本人が行使できるコントロールや、個人データ管理者に求められる義務の内容が変わってくる。GDPR対応において、よく「情報資産の棚卸し」とか「データマッピング」が強調される。これは、データと利用目的ごとに、どのような根拠に基づいて処理をするのかを明確にして、必要な対応ができることを確認しなければならないからである（GDPR 30条）。

（3）日本への影響

GDPRは、本来であればEU域内だけのローカルなルールであるが、世界的な影響があると考えられている。これには、大きく分けて3つの理由がある。

まず、EUは個人情報保護政策をリードしてきた世界のトップランナーであり、他国の制度にも大きな影響力を持つ。EUがAIビッグデータに対応するために導入したこの制度を、無視することはできない。

次に、EUは以前から、個人情報保護が十分になされていない国への個人情報の移転を原則として禁止している。GDPR成立後は、より厳格にEU域外への移転が制限されることになる（「2.3 十分性認定」を参照）。

さらに、GDPRは、EU域外の者が、EU域内にいる人（EU市民等）の個人情報を取り扱う場合にも、広く適用される。

■表1. GDPRで新たに追加された制度の例

条文	規定	概要
第17条	消去権（忘れられる権利）	一定の場合に、データ管理者に対して自己に関する個人データの消去を求める権利
第20条	データ・ポータビリティの権利	データ管理者に提供した個人データを、他のデータ管理者に移す権利（SNSやクラウドを想定）
第22条	プロファイリング規制	法的効果を生じる決定や、本人にとって影響の大きな決定を、プロファイリング等の自動処理によって行われない権利
第33条 第34条	データ侵害通知	漏えい等のデータ侵害が生じた場合の規制機関に通知と、本人に高いリスクをもたらす場合の本人への連絡の義務付け
第35条	データ保護影響評価	高いリスクや影響が懸念される個人データの取扱いについて事前のデータ保護影響評価を義務付け
第83条	制裁金制度	2000万ユーロまたは前年度世界売上の4%のいずれか高い方を最高額とする行政制裁金

出典：小向太郎『情報法入門（第4版）デジタル・ネットワークの法律』NTT出版（2018年）210頁

日本企業がEU市民を相手に物品やサービスを提供したり、EUでの行動をモニタリングしたりする場合等には、これらに関連して取り扱われる個人情報についてGDPRの全規定を遵守することを求められる。これは、十分性認定に基づく個人データの域外移転とは別の話である。GDPRには、日本にはない制度が大量に盛り込まれている。主なものだけでも、個人データ処理の適法化根拠、データ保護影響評価、データ・ポータビリティ権、プロファイリングに関係する権利等は、日本にはない制度である。EU市民等の情報を扱う際には、これらについて遵守していなければ、いくら日本の個人情報保護法を遵守していても、違法行為として法執行の可能性があるというのがEUの立場である。

日本企業にも、GDPRのこのような特徴を理解して、どのように対応すべきかを、自身の問題として考え決断することが求められる。

（研究会幹事　小向太郎）

2.3　十分性認定

（1）十分性認定とは

欧州委員会による十分性認定とは、「第三国、第三国内の地域又は一若しくは複数の特定の部門、又は、国際機関が十分なデータ保護の水準を確保していると欧州委員会が決定」することによって、「当該第三国又は国際機関への個人データの移転」が適法となる手続きである（GDPR45条1項、3項）。GDPRは個人データの処理と移転（越境移転）を原則違法としているところ（移転につきGDPR44条）、移転の適法化事由のうち原則とされているものが、十分性認定ということになる。

十分性認定の制度はGDPR以前、EUデータ保護指令の頃から存在し、日本への十分性認定がGDPR全面適用後初の事例である。裏を返せば、現在の十分性認定は、ほぼ全てEUデータ保護指令下の十分性認定が経過措置で有効とされているものである（GDPR45条9項）。2019年4月19日現在、十分性認定がなされているのは日本を除くと、アンドラ、アルゼンチン、カナダ（民間事業者）、フェロー諸島、ガーンジー島、イスラエル、マン島、ジャージー島、ニュージーランド、スイス、ウルグアイ、米国（プライバシーシールドの枠組みに限定）の12か国・地域である。このうち、アンドラ及びスイスは欧州連合又は欧州経済地域には加盟していないものの、欧州の隣国であり、フェロー諸島（デンマーク領）、ガーンジー島（英領）、マン島（英領）、ジャージー島（英領）は、欧州連合加盟国の自治領である。アルゼンチン及びウルグアイは旧宗主国のデータ保護法制の影響を強く受けている。かくして、欧州と相当程度の差異を有するデータ保護法制に関して十分性認定を経たのは、イスラエル、ニュージーランド、カナダ（民間事業者）、米国（プライバシーシールドの枠組み）に限られ、その数は極めて少ないといってよい[*2]。

（2）日本の十分性認定までの経緯

十分性認定が認められない場合、原則として拘束的企業準則や標準データ保護条項といった例外的な移転手段を用いる必要がある（GDPR46条）。これらの利用は各事業者のコストとなるものであり、国として十分性認定が認められることは基本的に望ましい。初期に、日本がGDPR上の十分性認定について意識したことが表れているものとして、例えば2012年7月4日の高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議第30回会合において、「EUにおける個人情報の取扱いについて、従来は指令だったものを規則化する動きがある。規則化された場合、EUの中の個人情報を第三国へ持ち出すことが禁止されることとなり、ヨーロッパで事業展開している日本企業は、EU内の顧客情報を日本へ持ち出すことが禁止される。…日本の対応が遅れてしまうと、大きな問題となる可能性があるので、ご検討いただきたい。」との議事がみられる[*3]。十分性認定は個人情報の保護に関する法律（平成15年法律第57号、以下、個人情報保護法）の平成27年改正（平成27年法律第65号による）の議論でも意識されており、例えば、改正の議論が行われた『パーソナルデータに関する検討会』の中で、「十分性の基準をクリアするための法整備における課題を今回は検討する、そちらに集中するという理解でよいか」との新保史生委員からの質問に対し、事務局は「それについて対応できるような法制の整備を目指したい」と回答しているし（2014年3月27日）[*4]、実際に、平成27年改

＊2　十分性認定を得た国へのインタビューを経てまとめられた資料として、消費者庁『個人情報保護制度における国際的水準に関する検討委員会・報告書』（平成24年3月）が存する。十分性認定のプロセスは数年単位かかるのが通常であり、例えばイスラエルは2007年7月12日に審査を開始し、十分性認定がなされたのは2011年1月31日である（119頁以下）。

＊3　高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議第30回会合（平成24年7月4日）議事要旨。

＊4　高度情報通信ネットワーク社会推進戦略本部第6回パーソナルデータに関する検討会（平成26年3月27日）議事要旨。

正個人情報保護法の解説で立案担当者は、「十分性の認定を得ることを念頭に制度設計が行われて」いるとしている[*5]。同法により2016年1月1日には特定個人情報保護委員会が改組される形で、個人情報保護委員会が設置された。個人情報保護委員会のような独立した監督機関の設置も、十分性認定の要諦の一つである（GDPR45条2項（b））。

設置後の個人情報保護委員会は欧州との間で相互の円滑なデータ移転を図る枠組みを構築する方針を決定し（2016年7月）、欧州委員会は政策文書の中で、日本の十分性認定の優先順位が高いこと等を述べた（2017年1月）。個人情報保護委員会は欧州委員会（司法総局）と極めて頻繁な対話を実施した（2016年4月～2018年5月の間に53回）[*6]。その結果、2017年7月3日には、「双方が十分な保護レベルを同時に見いだすことを通して、相互の円滑なデータ流通をより一層促進する新しい機会を提供する」ことを合意するに至り[*7]、2018年7月17日には、「お互いの個人データ保護の制度が同等であると認識するための議論を成功裏に終了した」（最終合意）[*8]。2019年1月23日、合意に従い欧州委員会は、日本（個人情報保護法の適用範囲）について十分性認定を行い[*9]、日本は、欧州の31か国について個人情報保護法24条に基づき（個人情報の保護が）、我が国と同等の水準にあるものとして指定した。

（3）「補完的ルール」

さて、通常の十分性認定であれば、欧州から移転された個人データについては認定された国または地域の法制度に従って取り扱えば足りるはずであるが、日本の場合は、さらに「個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」（平成31年個人情報保護委員会告示第4号）の内容を遵守することが求められる。これは、例えば要配慮個人情報の内容をGDPR上の特別な種類の個人データに近づけようとしたり、欧州から日本に移転された個人データの再移転について個人情報保護法24条の移転方法のうち一部を認めないという内容を含むものである。

日本の十分性認定は、欧州との相互の認定である点で異例であり、移転後に上乗せ措置が求められる点でも異例であるが、GDPR下の初の十分性認定である。2年後に行われるレビューを含め、その趨勢は広く注目されている。

（研究会運営委員　板倉　陽一郎）

3. 今後の改正動向

3.1 法制度の見直し

現在、個人情報保護委員会を中心として、個人情報保護法の新たな改正の議論が行われている。改正には、大きく分けて2つの動機がある。1つは、個人情報保護法が持つ、いわゆる3年ごと見直し条項を根拠としたものである。2015年個人情報保護法改正の根拠になる平成27年法律第65号は附則第12条第3項として、「政府は、前項に定める事項のほか、この法律の施行後三年ごとに……新個人情報保護法の施行の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとする。」と定めている。2017年の全面施行から3年となる2020年を基準とした見直しが宿題となっている。もう1つは、2.3で解説された欧州からのGDPRに基づいた十分性認定への対応である。十分性認定では、欧州側からの定期的なレビューが求められているが、最初のレビューが2年後と目される。2020年から2021年頃にあるのではないかと予想されるところである。過去の例として、欧米間のデータ保護の枠組みであったセーフハーバー協定が欧州司法裁判所で無効であるとされたことがある（2015年）。米国は欧州との個人データのやり取りができなくなる危機に陥り、欧米間ではプライバシーシールドという新しい枠組みが策定された。日本の十分性認定も欧州司法裁判所に持ち込まれれば、無効と判断される可能性がある。これは、欧州からの十分性認定が後述のように告示による補完によるも

＊5　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）57頁（Q33）。
＊6　高度情報通信ネットワーク社会推進戦略本部第14回新戦略推進専門調査会・第10回官民データ活用推進基本計画実行委員会合同会議（平成30年5月11日）【資料2-2】個人情報保護委員会事務局「国際的な個人データの移転について」（2018年5月11日）。
＊7　熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント（2017年7月3日）。
＊8　熊澤春陽個人情報保護委員会委員、ベラ・ヨウロバー欧州委員会委員（司法・消費者・男女平等担当）による共同プレス・ステートメント（2018年7月17日）。
＊9　COMMISSION IMPLEMENTING DECISION (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information (notified under document C (2019) 304).

のであることや、欧州からの疑念が十分には払拭されていないことによる。今後の改正動向については、個人情報保護委員会による3年ごと見直しに加えて、日欧間の制度の差異に目を向ける必要がある。以下、それらについて解説する。

まず、個人情報保護委員会による3年ごと見直しはどのようなものになるのか。個人情報保護委員会は2019年4月25日に中間整理を公開したが、本稿執筆時点ではパブリックコメントに付されている。中間整理やその後の検討を見るに当たり参考になるのが、2019年1月28日の個人情報保護委員会において示された「いわゆる3年ごと見直しに係る検討の着眼点」である。7つの視点が示されており、それぞれ以下のとおりである。①「個人データに関する個人の権利の在り方（開示、利用停止・削除等の検証等）」としては、開示請求権の現状（改正法による開示請求権の明確化を踏まえた状況）、訂正、利用停止・削除等の現状オプトアウト規定（名簿屋対策）の現状、データ活用の多様化と個人の権利、諸外国の現状（制度、運用）、が含まれている。②「漏えい報告の在り方」としては、法執行の実効性、安全管理措置としての意義、事業者の負担、報告の対象・形式等、本人への通知等の在り方、諸外国の現状（制度、運用）が含まれている。③「個人情報保護のための事業者における取組みを促す仕組みの在り方」としては、認定個人情報保護団体制度の在り方、事業者による自主的取組みの状況、個人情報に関連する国際標準・認証等の動向（Pマーク、ISO/IEC 27001等）、PIA類似制度の現状（例：番号法における特定個人情報保護評価、生産性向上　特別措置法における革新的データ産業活用計画の実績）、が含まれている。④「データ利活用に関する施策の在り方」としては、匿名加工情報制度等の現状、AI・IoT等データを取り巻く技術の進展状況、クッキー・ソーシャルプラグイン等を活用したターゲティング広告の動向、情報銀行等個人データを活用したビジネスの現状、保護と利活用のバランス（規制とイノベーションとの関係）、国際的な議論の動向、が含まれている。⑤「ペナルティの在り方」としては、国内外事業者に対する抑止効果、法執行の実効性（モニタリングの在り方、調査・執行手段の在り方等）、事業者の法遵守状況、諸外国の現状（制度、運用）、参考となる国内法の現状（制度、運用）、が含まれている。⑥「法の域外適用の在り方」としては、外国事業者に対する執行態勢の状況、外国執行当局との連携状況、域外適用に係る他の国内法の状況、諸外国の現状（制度、運用）、が含まれている。⑦「国際的制度調和への取組みと越境移転の在り方」としては、国際的制度調和の動向、越境移転の現状、諸外国の現状（制度、運用）、データローカライゼーション・ガバメントアクセス等に関する議論の状況、が含まれている。一方で、データ・ポータビリティ、プロファイリング、削除権（忘れられる権利）等の具体的言及はなされていない（なお、中間整理では一定の記述が見られる）。

（研究会運営委員　加藤尚徳）

3.2　十分性認定のレビュー

次に、欧州から十分性認定の視点から、どのような改正が必要となると予想されるか概観する。十分性認定の観点からは、告示による暫定的状況の治癒が必要になることが予想される。「個人情報の保護に関する法律に係るＥＵ域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」を用いて、十分性認定において国内法制度で不十分な点について、個人情報保護委員会は法改正ではなく告示レベルでの対応を行っている。告示での対応は今後、執行可能性の観点から不十分であるとして、執行可能性を担保するために法改正が求められることがあり得る。「補完的ルール」は、具体的には、要配慮個人情報（法第2条第3項関係）、保有個人データ（法第2条第7項関係）、利用目的の特定、利用目的による制限（法第15条第1項・法第16条第1項・法第26条第1項・第3項関係）、外国にある第三者への提供の制限（法第24条・規則第11条の2関係）、匿名加工情報（法第2条第9項・法第36条第1項・第2項関係）について上乗せの規定をしている。十分性認定において欧州データ保護会議（EDPB）から付された意見書では、法執行（刑事法）分野に関しては欧州との本質的同等性が否定されており、個人情報保護委員会の執行（告示を上限とする法令の範囲内での委任）についてもその実効性に疑問が呈されている。プライバシー権が日本国憲法上で文言として触れられていない点等、個人情報保護法の改正だけにとどまらない論点もあり、情報法制全般としての対応が求められている。

（研究会運営委員　加藤尚徳）

3.3　死者のプライバシー

全ての世代において幅広くデジタルデバイスやインターネットが利用される現在、個人の死亡によって残されるものは、形あるモノに限られなくなった。かつての遺品や日記、手紙のようなものはデジタルデータとして、残されたデバイ

ス内にとどまらず、クラウド上にも存在する。そのデータには、写真や文章、各サービスのアカウント情報、他者とのやり取りの記録に加え、自身のライフログなど多種多様なものが含まれる。

故人の私的な遺品の扱いについては、その遺族や子孫、関係者に不利益があってはならないが、残されるものがデジタル情報であれば新たな課題が発生する。データは複製が容易であり、サービスによっては他者との交流自体のデータも残される。データは故人の追悼のために共有されることもあり、また、これまでも博物館の展示に私的なものが供されてきたように、後年貴重な史料になり得る可能性もあり、直ちに削除すれば解決するものではない。

本人の生存中であれば、これらのデータは個人情報保護法やEU一般データ保護規則（GDPR）等の制度によって、利用者本人の意向に基づいた保護がなされるのだが、死後のデータの扱いや、故人のプライバシー（post-mortem privacy）については，いずれの国・地域の法制度においても明確に概念化し保護するには至っていない。

現状の運用は様々である。2016年時点の日本国内では、都道府県の66.0%（31団体）並びに市区町村の57.0%（992団体）が、死者の名誉や人格的利益を守る目的や、保有している情報が生存する個人のものか死者のものかを分別することが困難なことを理由にして、個人情報保護条例上の「個人情報」の範囲に死者に関する情報を含めている[*10]。本人の意思を生前に確認し、死後反映させる動きもある。GoogleやFacebookでは、利用者は生前に、自分の死後のデータの扱いを決めておくことができる。例えばGoogle社が提供する「アカウント無効化ツール（Inactive Account Manager）」では、あらかじめ指定した期間（3〜18か月）にアカウントのアクティビティがなく、さらに設定された連絡先への連絡に反応がないことが判明した時点で、あらかじめ本人が設定したデータの削除や共有が実行される。Facebookでは、故人のアカウントを「追悼アカウント」に変更でき、その管理人は本人が生前に指定することができる。

故人が残したデータの扱いの現状は、三種類に分類することができる。(1) 生存する相続人や親族に決定を委ねるもの（ブルガリアやエストニアが採用）、(2) データ保護法制並びにプライバシー保護法制の適用対象を死者にも拡大するもの（フランスが採用）、そして (3) 財産権的な保護への転換を図るもの（アメリカのいくつかの週で採用）がある[*11]。

今後の課題を、本稿では二点提示しておきたい。

まず、インターネット利用における本人確認の問題である。サービス利用のアカウントは、必ずしも身分登録上（日本では戸籍上）の氏名で利用されているとは限らず、死亡証明書と氏名が一致しない可能性がある。Facebookでは別名併記という選択肢があるが、旧姓と戸籍姓を併記するよりも旧姓のみを表示している利用者の方が多いという調査結果もある[*12]。個人を特定できる情報を必要としないサービスや、一つのサービスで複数のアカウントを取得し使い分けることができるサービスの場合、本人及び死亡確認の困難さに加え、遺族がそもそもアカウントを把握しきれない可能性も高い。

もう一つは、ソーシャルメディアをはじめとする、他者との関わりを目的としたサービスにおけるプライバシーの扱いである。サービスによっては、利用者が自分の情報共有範囲を設定することができるため、例えば相続者が故人のアカウントにログインできてしまうと、故人に対して「他の利用者が」共有や開示していた情報を、相続者が目にすることとなり、生存する他の利用者のプライバシー侵害にもつながりかねない。2018年7月にドイツにおいて、相続者によるFacebookアカウントへのアクセスを認める判決が出た。故人の母親が、亡くなった娘のFacebookへのアクセスを求めたものであり、裁判所はアカウントを日記や手帳と同様の遺産に相当すると判断し、母親が亡くなった娘のアカウントにログインすることを許可した。これは「生存する相続人や親族に決定を委ねる」ケースと言えるが、故人の「友人」が故人「本人」との信用の上で共有した情報が、故人の「遺族」に開示されることにもなる。故人と相手との関わりや、故人が属する集団の観点からは、“Group Privacy”の概念の援用が考えられる。

（研究会幹事　折田明子）

---

*10　総務省. 地方公共団体が保有するパーソナルデータに関する検討会（第2回）資料3「個人情報の定義の明確化」http://www.soumu.go.jp/main_content/000455021.pdf

*11　湯淺墾道、折田明子：GDPR（一般データ保護規則）と死者の個人情報、情報処理学会研究報告、Vol. 2018-EIP-80, No. 6, pp. 1-6, 2018

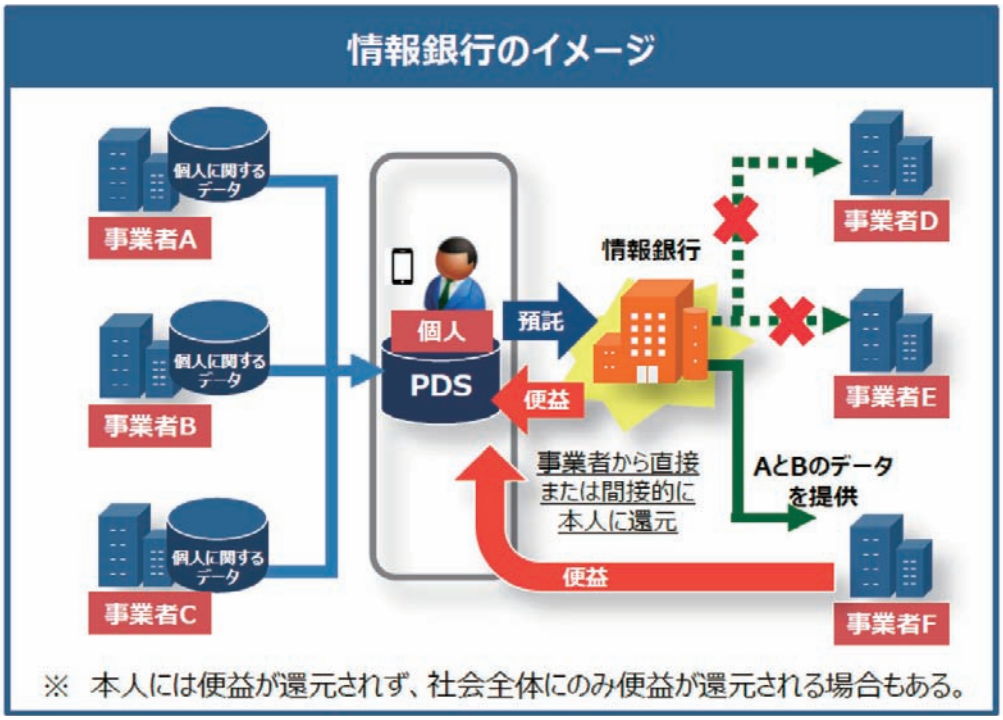
*12　折田明子（2017）オンライン・オフラインにおける名乗りと「本名」〜戸籍姓・生来の姓・家族の姓. 情報社会学会誌 Vo.12 No.1 pp.63-72

3.4　情報銀行

個人情報関連法制には、情報の保護のための制度と利活用のための制度の両面性があるが、『情報銀行』は、匿名加工情報などと同様に個人情報の利活用を念頭においた法律である。無論「利活用」といっても個人情報保護がなされた上でのことであることは言うまでもない。情報銀行では、自らの個人情報群の一部を機関に提供し、その情報を管理・運用してもらう代わりに便益を得るわけであるが、そのシステムがお金を寄託してもらい活用する金融機関に近いということで情報銀行と称される。この場合の情報の運用とは、マーケッティングや商品開発などのために自己の個人情報を先方に提供することである。管理・運用される個人に関する情報は、年齢、性別や購買歴といった従来型のものだけにとどまらず、スマホなどに蓄えられた運動や歩数の記録などといった生活行動歴になる場合もある。

まずは、以下の**イメージ図**と定義を参照していただきたい。これは『IT総合戦略本部 データ流通環境整備検討会「AI、IoT時代におけるデータ活用ワーキンググループ中間取りまとめ」(2017)』以降の政府の情報銀行に関する公開資料に繰り返し記載されているものである。情報銀行に類似した概念に「PDS (Personal Data Store)」というものがあるが政府の整理では「PDS」と「情報銀行」は異なる概念とされており、「データ取引市場」を合わせて、それぞれの定義が上記取りまとめ等にも記載されている。すなわち**『情報銀行（情報利用信用銀行）とは、個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。』**とされている。これに対して、PDSは仕組み（システム）の呼称とされており、情報銀行はその仕組みを備えている個人に関する情報の預託機関のことを指すという整理である（**表2**）。

総務省の予算による情報銀行の実証実験は既に2018年度から行われており、2019年中には本格的な実証が行われる予定である。また、既に大手金融機関や保険会社、IT企業、電力などのインフラ企業などは実ビジネスの開始を予定している。もっとも、情報銀行は新しい事業形態であり、当初から法的規制を及ぼすのは躊躇される。しかしながら、利用者の個人情報・個人データについて、指定された条件の中で裁量を持って第三者に提供するという事業は、本人のプライバシー等の権利利益へのインパクトが大きいため、民間において何らかの認定事業が行われること



出典：IT総合戦略本部データ流通環境整備検討会「AI、IoT時代におけるデータ活用ワーキンググループ中間とりまとめの概要」（2017）https://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/dai2/siryou1.pdf 7枚目より

■図．情報銀行のイメージ

■表2. PDS・情報銀行・データ取引市場の定義

PDS（Personal Data Store）	他社保有データの集約を含め、個人が自らの意思で自らのデータを蓄積・管理するための仕組み（システム）であって、第三者への提供に係る制御機能（移管を含む）を有するもの。
情報銀行（情報利用信用銀行）	個人とのデータ活用に関する契約等に基づき、PDS等のシステムを活用して個人のデータを管理するとともに、個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、データを第三者（他の事業者）に提供する事業。
データ取引市場	データ保有者と当該データの活用を希望する者を仲介し、売買等による取引を可能とする仕組み（市場）。

出典：総務省「情報通信白書」平成30年版17頁

は適切である。このような観点から、まず、総務省・経済産業省により『情報信託機能の認定に係る指針ver1.0』（2018年6月）が定められ、民間団体等が認定事業をする際には参照できるとされた。そして、2018年12月からは、一般社団法人日本IT団体連盟が、同指針に準拠した形で情報銀行の認定事業を開始している。

以上のように、GAFAに代表される米国一極集中のビッグデータ・ビジネスに対抗するための切り札の感もある情報銀行であるが、その成功の可否は現時点では全くの未知数と言えよう。ネットを利用する一般ユーザーは既に、個々のサービスを利用する際に様々な個人情報を提供しており、その情報提供の見返りとして便益を得ている。しかしながら、このことがすぐに情報銀行の普及へつながるかというと、そうはならないであろう。その理由の1つ目は、ユーザー側からすれば個人情報を提供した対価としてネットサービスを享受できているという意識がまだまだ希薄なこと。2つ目は、情報が1か所に集約されることへの利用者の不安である。この2つの意識改革ができるかどうかが、情報銀行の浸透への鍵と言える。

（研究会運営委員　須川賢洋）