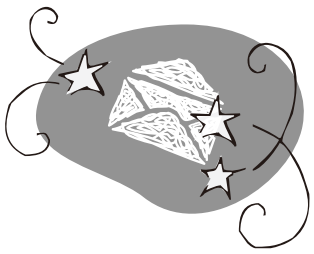
特集

パーソナルデータの利活用における技術および各国法制度の動向



編集にあたって

中川 裕志　東京大学 情報基盤センター

パーソナルデータと個人情報

ビッグデータの利活用が重視されているが，その中でもとりわけパーソナルデータすなわち個人に関する情報が広告をはじめとする種々のビジネスで有用である．日本のパーソナルデータにかかわる法制度は個人情報保護法であり，後に日本の状況の節で述べるように改正作業が進行している．しかし，その作業における検討の中で用語の意味解釈がインターネット隆盛の現代においては不適当なものになっていることが明らかになった．そこで，本特集の諸解説を読んでいただくにあたって基礎となる用語についてまず説明させていただくことにする．

パーソナルデータと個人情報あるいは個人データが同じ意味を持つということは現状でも正しい．しかし，現在の個人情報保護法の運用と解釈の中では，個人情報の意味を「個人を識別する情報」（以下では個人識別情報と呼ぶ）として捉えるような慣行になっていた．個人識別情報とはインターネットが普及する以前には（氏名，住所，年齢，性別）とほぼ一致すると考えられてきた．一方，インターネットとビッグデータに誰でも触れることができる現在においては，この一致性は再考を要する．たとえば，現在はネットワーク上の ID であるメールアドレスやソーシャルメディアの自身に関する記述が公開されている．また，ビッグデータの例である鉄道会社の保有する利用客の乗降履歴には，自宅と勤務先の最寄りの駅名が毎日のように集積している．あるいはスマートフォンの GPS による移動履歴には，自宅や勤務先の位置を示す情報が累積している．つまり，これらの位置情報，移動履歴を使えばほぼ個人を特定できる．ということは，これらのビッグデータ中の情報も個人識別情報としてのステータスを持つと考えるべきである．2013 年に JR 東日本が Suica の乗降履歴をインターネット以前における個人識別情報を削除しただけで売却しようとして批判に晒された．このことは，人々が上記の意味での個人識別情報の拡大を直感的に感じていたからではないだろうか．

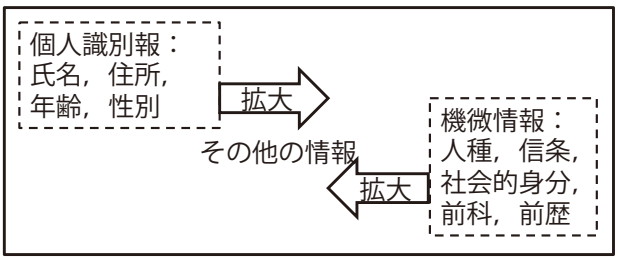


図 -1　個人情報の区分け

さらに購買履歴は一見個人にとって脅威になるような情報ではないが，集積されれば個人識別情報になりかねない．つまり，個人にかかわるすべての情報すなわちパーソナルデータを区分けする必要が生じた．以下のその区別について説明する．

(1) 個人情報は，個人識別情報と機微情報とその他の情報に区分けされる．

(2) 機微情報とは，従来から（人種，信条，社会的身分，前科・前歴）が列挙されていたが，購入履歴にしても運転者の脱法ハーブの購入や教師のアダルトビデオ購入は機微情報になる可能性が十分ある．つまり，機微情報の定義は状況依存的であり困難である．

(3) 個人識別情報とその他の情報の線引きも上記の例から推察されるように実に難しい．

この区分けの概略を**図 -1** に示した．

日本の個人情報保護法改正作業におけるこれらの

線引きに関しては，森氏の解説に詳細に説明されている．

パーソナルデータの利活用における各国法制度の動向

個人情報にかかわる法制度は日本と欧米の間でかなり大きな差があり，EU から個人データを輸入できないなど好ましいとはいえない状況にある．そこで本特集では，現在の海外および日本の法制度の動向，さらに制度，社会，技術との関係についての解説記事を各分野の専門家の方々にご執筆いただいた．

たとえばゲノム情報を創薬に利用するには人種による差異があるため，国内で採取できる日本人のデータだけでは不十分である．このようにパーソナルデータにおけるプライバシーが国内問題に閉じていないので，日本の状況を世界的レベルで位置づけることが必要になる．

はじめに，米国や EU での最近の法制度の動向の根底にあるプライバシー・バイ・デザイン（以下 PbD と略記する）の考え方を紹介しておく[1]．PbD は以下の 7 つの原則よりなる．

1. プライバシー保護に関しては，事後の対策ではなく，事前に予防措置をとるべし
2. プライバシー保護はデフォルトであるべし
3. プライバシー保護の仕組みは制度やシステムの設計時に組み込むべし
4. データ事業者，サービス利用者の双方の利益になるのでプライバシー保護対策をしっかりやるべし
5. プライバシー保護は個人データの生成から廃棄までの全期間において実施すべし
6. プライバシー保護の仕組みを可視化，透明化すべし
7. プライバシーは利用者中心の仕組みにすべし

このうち，原則 6. はサービス利用者の自己情報について公開，訂正，削除などを求める自己情報コントロール権につながるものである．

■ EU の動向

EU では，2014 年 6 月に検索エンジンにおける個人の過去の履歴の削除を Google 社に求めた裁判で同社の敗訴が確定した．その結果，同社は EU 内の利用者から要望があれば同社の検索エンジンからその利用者の過去の履歴の削除依頼を受け付けるようになった．このように事態は流動的であるが，法制度の改定も急速に進んでいる．すなわち 1995 年制定のデータ保護指令は，2009 年より改正作業が始まり，2014 年 3 月に改訂されたデータ保護規則が EU 議会で可決され，理事会の承認を待っている．新規則では自己情報コントロール権が明記されるなど PbD の考え方が色濃く反映されている．さらに，指令から規則になったことによって，各国での立法は不要になり，EU 全域で新規則が有効な法律となる．このような事情は高崎氏の解説が現状を詳細に説明している．

■ 米国の状況

米国においては以下の連邦取引委員会：FTC の 3 要件がよく知られている．

1. データ事業者はデータから個人識別ができないように合理的な措置を講ずること
2. データ事業者は，データを個人識別できない形態で保有および利用し，そのデータから再度の個人識別を試みないことを公に約束すること
3. データ事業者が個人識別を不可能にしたデータを他の事業者に提供する場合は，それがサービス提供事業者であろうとその他の第三者であろうと，その事業者がデータの再度の個人識別化を試みることを契約で禁止すること

この FTC の 3 要件に加え，自己情報コントロールの権利を取り込んだ消費者プライバシー権利章典もよく知られている．さらに PbD の考え方やサービス利用者保護を取り入れた法制度策定へ向けての種々の動き[2]がある．これらおよび最近の動向について石井氏の解説が詳しく述べている．

■日本の状況

成長戦略の一環としてビッグデータの利活用促進の目的で政府 IT 総合戦略本部によって 2013 年より「パーソナルデータに関する検討会」が立ち上がった．検討会では，プライバシーの重要度が認識されて個人情報保護法への改正に向かっての検討が 2014 年 6 月まで続けられ，法案作成の元になる「改正大綱」と呼ばれる報告書が公開された．この動きについて上記の検討会の委員であった森氏に執筆いただいた．

詳細は森氏の解説をお読みいただきたいのだが，無視できないのは個人データが国境を越えて移動する越境移転の問題である．特に重要なのは十分性と通称される次の問題である．すなわち，EU は EU 内で採取されたゲノムなどの個人データを個人情報保護法制が十分でない国には越境移転を許さない．残念ながら日本はこの点で十分ではない国とみなされており，EU からデータを入手することができない．EU から問題とされたのは，政府から独立したプライバシー保護を監督する第三者機関が存在しないことであった．これについては 2014 年 1 月 1 日に特定情報保護委員会が設置されたが，十分性を満たすために，これを発展させた第三者機関の設置が課題である．さらに十分性のない第三国へのデータ越境を禁止する法律が必要になる．このように日本の現状においてプライバシーにかかわる法制度および外国との関係に関する状況は簡単ではない．課題が多いため規制緩和と規制強化の両面から取り組むべきである．詳細については森氏の解説はぜひご一読いただきたい．

さて，「改正大綱」では個人情報から個人を特定できないようにすることの必要性について触れている．「改正大綱」では個人特定不可能な方法が存在しないとされた．そこで，個人特定の可能性を程度問題と捉え，個人特定性低減データというキーワードを導入した．実際，「改正大綱」では個人特定性低減の方法として主に k- 匿名性が念頭におかれているので，以下に簡単に説明する．

k- 匿名性[3] とは，個人データが

a. 個人 ID：たとえば氏名，
b. 疑似 ID：たとえば住所，年齢など，
c. 機微情報，その他の情報

というレコード構造を持つデータベースにおいて，

(1) 個人 ID を削除，
(2) 疑似 ID の精度を落とす，たとえば住所を市区町村までにする，年齢を 10 歳刻みにする，

というような変更が行われた結果，データベース中に同じ疑似 ID の個人が k 人以上存在するような状態である．k- 匿名性によって個人の機微情報が確定的には知られないようにできる．しかし，たとえばスマートフォンの GPS データのように長大な移動履歴が得られる場合，このデータ自体が疑似 ID となってしまうため，k- 匿名性を満たすには位置の精度を大幅に落とさざるをえない．よって，情報の価値が大きく損なわれることが「改正大綱」の検討過程で示された．このことから個人特定性低減に関しては技術的課題が山積していると言える．なお，位置情報の個人特定性低減ついては本特集の高橋氏の解説に詳述されている．

個人情報のコントロール

佐古氏が解説するパーソナル・データ・エコシステム（以下 PDE と略記）は PbD のアイディアを基礎にしており，プライベート企業のコンソーシアムのような枠組みである．具体的には，個人が自己情報についての全権を持つシステムである．佐古氏が解説中に紹介されているように Respect Network 構想として開発が進んでいる．端的に言えば，消費者の個人データはパーソナルクラウドと呼ばれる格納庫に管理し，このデータを利用したいデータ事業者は当該の消費者に申請し，許可された場合にだけ利用できるというシステムである．これは，個人データ管理の主導権をベンダーすなわち企業から消費者に取り戻す Vender Relation Management[4] という大きな流れの中で位置づけられる．PDE は個人的なプライバシーの重要さが高い医療分野での情報共有などで有望だと言われている．これは主として

IT 事業者がプライバシー保護を念頭におきつつ個人データの利活用を図る場合に適用される法制度とは方向性が異なる．

プロファイリングの問題

「改正大綱」では事業者が収集した膨大な個人データからサービス利用者個人の特性を推定するプロファイリングの扱いは先送りになっている．実際は上記の EU における個人プロファイルにかかわる履歴削除の裁判で Google が敗訴するなど注目すべき事態が発生している．この特集では，プロファイリングにおける技術的な 2 つの側面について神嶌氏に解説いただいている．

第 1 のテーマは公正性である．これはパーソナルデータ利用が，たとえば奨学金の採用判断などにおいて，個人の不利益をもたらさず，公正性が保たれるためのデータ利用方法に関する話題である．

第 2 のテーマは，自分の検索エンジンなどの閲覧履歴などがプロファイルされた結果，ソーシャルメディアや検索エンジンで表示される情報にバイアスが生じ，適切な情報が得られなくなるフィルタバブルの現象である．

移動履歴

個人の滞在した位置情報および移動履歴は，出店場所，商品の揃え方，さらには公共交通システムの設計などの参考になる基礎データであるため，有用性がきわめて高い．しかし，自宅住所や勤務先などのプライバシー情報が含まれている．したがって，この情報が漏洩した場合の危険性の把握，漏洩の起こり方の整理と対策が重要である．たとえば，個人の行動履歴から自宅や勤務先にかかわる部分の削除を行う方法が提案されている．このテーマに関して高橋氏が詳しく解説している．

将来の課題

最後にこういった制度やシステムを実現する技術について述べる．EU の現在のデータ保護指令の作業部会 WIP216 では 2014 年 4 月に k- 匿名化，差分プライバシーなどの匿名化に関する多数の技術が分析検討されている [2]．また暗号化したデータを復号せずに加算などの演算ができる準同型公開鍵暗号を用いて，個人情報を暗号化したままで処理する秘密計算プロトコルはプライバシー保護が完璧な重要技術である．残念ながら日本の法制度検討ではこれらの技術の検討は十分でない．研究レベルではいくつかの技術的成果が出始めているが，研究者層，研究成果とも薄く，この分野の拡大が望まれる．また，匿名化を破るためのコア概念である名寄せの実態解明と対策も今後の課題である．今後，公的機関に限らずプライバシーにかかわる技術者，事業者は，上記の技術動向に注意を払い，制度と技術が結びついてプライバシー保護とデータ活用が両立する方向性を模索する時期に来ている．なお，本特集では取り上げなかった医療データ，ゲノムデータはデータの性質上，プライバシー保護に関して異なる扱いが必要になることを留意しておく必要がある．

なお，デジタルプラクティス 21 号（Vol.6 No.1）「プライバシーフレンドリーシステム」特集には，この特集で扱ったテーマのうち佐古氏の解説に関連ある論文の掲載が予定されており，実社会での具体的応用に関してはそちらも参照されることをお勧めする．

参考文献

1) Cavoukian, A. : Privacy by Designand the Emerging, Personal Data Ecosystem, Information and Privacy Commissioner Ontario, Canada (2012). http://privacybydesign.ca/content/uploads/2012/10/pbd-pde.pdf
2) 石井夏生利 : 個人情報保護法の現在と未来，勁草書房 (2014).
3) Sweeney, L. : Achieving k-anonymity Privacy Protection using Generalization and Suppression, International Journal of Uncertainty Fuzziness and Knowledge-Based Systems, Vol.10, No.5, pp.571-588 (2002).
4) ドク・サールズ（栗原潔　訳）：インテンション・エコノミー顧客が支配する経済，Harverd Business School Press（和訳：翔泳社）(2013).

（2014 年 9 月 26 日）