

NII Interview

パーソナルデータ利活用とプライバシー保護の両立、
欠かせない技術と法制度の連携

That's Collaboration 1

個人情報保護法の改正に向けて

NII Special 1

柔軟性ある個人情報保護と活用へ

NII Special 2

パーソナルデータの制御権を自らの手に!

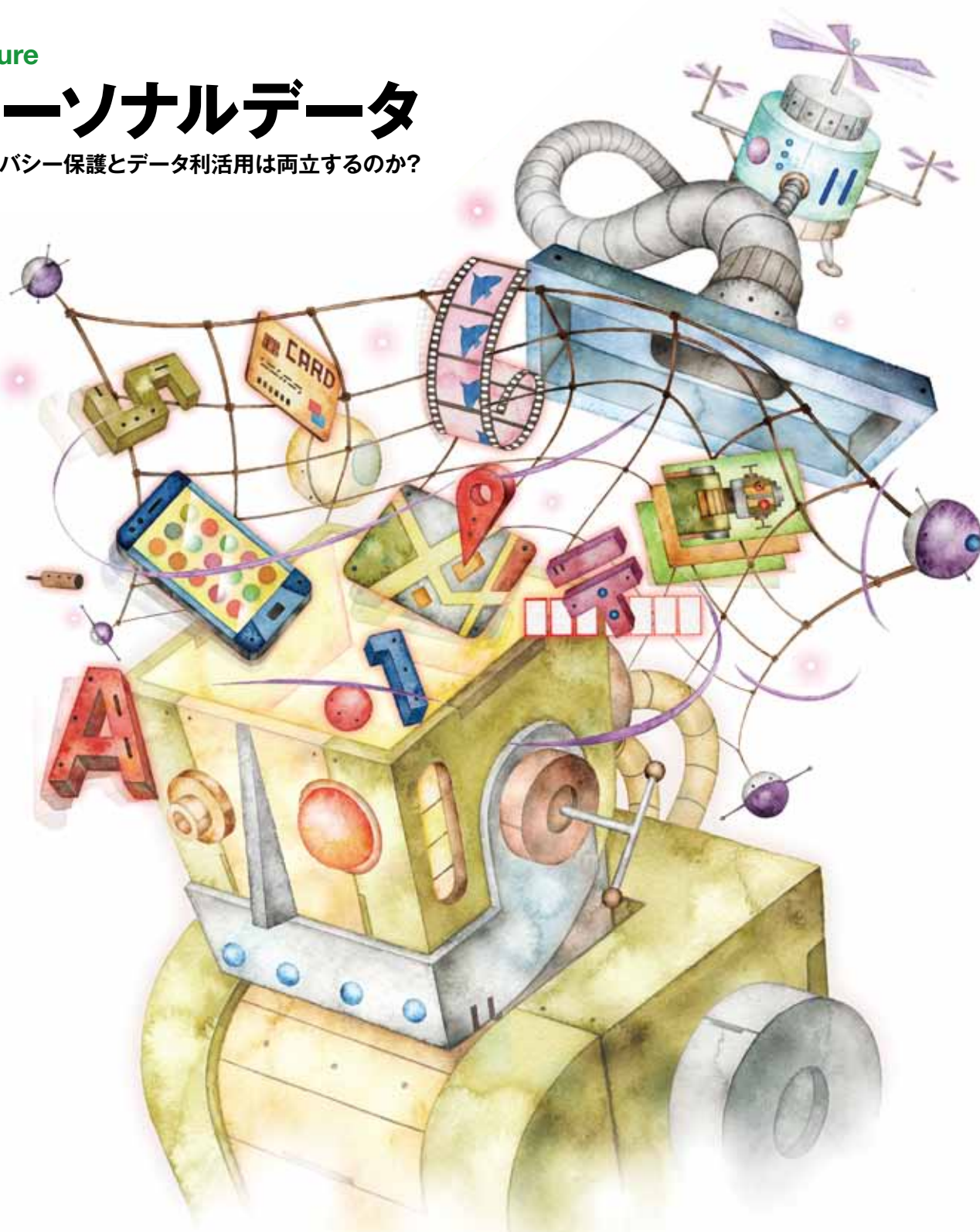
That's Collaboration 2

匿名化技術の最新動向とその課題

Feature

パーソナルデータ

プライバシー保護とデータ利活用は両立するのか?



パーソナルデータ利活用と プライバシー保護の両立、 欠かせない技術と法制度の連携

佐藤一郎

Ichiro Satoh

国立情報学研究所 アーキテクチャ科学研究系 教授
総合研究大学院大学 複合科学研究科 情報学専攻 教授

ビッグデータによる新たな価値創出に注目が集まっている。なかでも、個人の行動などの情報を含む「パーソナルデータ」は価値が高いが、その半面、プライバシー保護との両立という難しさをはらむ。政府IT総合戦略本部「パーソナルデータに関する検討会」（以降、検討会）の技術検討ワーキンググループ（以降、技術WG）では、技術的な立場から新たな制度を議論した。その主査を務めている佐藤一郎教授に、パーソナルデータ利活用を取りまく状況、問題意識について聞いた。

星 まず、検討会委員及び「技術WG」の主査を務めている経緯を教えてください。

佐藤 検討会は、パーソナルデータに関わる制度を設計する委員会です。パーソナルデータを保護するにせよ、利活用するにせよ、情報学を含む技術と密接に関わります。このため情報学を専門とする私が委員に加わりました。同時に技術WGという技術面をサポートする部会にも関わりました。

星 なぜ、パーソナルデータに関するルールを作り直すことになったのでしょうか。

佐藤 パーソナルデータに関して基本となる法律は2003年に制定された個人情報保護法（現行法）です。2008年に見直すことが付帯決議で盛り込まれていましたが、見直しがされていなかったこともあります。その他に2つの理由があります。1つは、現行法が技術の進歩についていっていないと言いが点。当時もインターネットやWeb検索はありましたが、その情報量や検索能力は格段に上がっています。もう1つは海外との関係。当初こそ、日本の個人情報の取り扱いは厳しいものでしたが、欧州はもちろん、その他の国でも法制度が整い、日本の取り扱いが緩くなってしまった。このままでは欧米で活動する日本企業が、顧客データベースを日本に置けなくなるなどの問題が出る恐れがありました。これは明らかに日本の国益に反します。

星 特に今回の法改正で議論されている「第三者への提供」により何が可能になるのか、お聞かせください。

佐藤 情報の利活用の際、事業者が必要な情報のすべてをもっているとは限りません。他事業者の情報を利用したいことも多いでしょう。その情報には個人情報が含まれる可能性があります。

例えば通販サイトでは、その事業者の他の利用者の購買行動を利用して商品推奨をしています。利用者にとっても、「自分が欲しい商品」を素早く見つけられるメリットがありますね。データの第三者提供が可能になると、メーカーに対して通販サイトの利用者の行動を教えて、メーカーの商品改良を促すこともできるでしょう。一方で第三者提供は個人情報の保護の観点では問題があります。

星 「技術WG」で議論された「匿名化」について、教えてください。

佐藤 匿名化というのは、情報を加工して個人を特定を難しくする技術です。第三者にパーソナルデータを提供する場合、匿名化により個人を特定する情報を適切に加工することが求められています。最近、EUは匿名化された情報は利用可能との法律を作りました。日本でも、匿名化について法律で規定していく方針です。

星 匿名化には一般的な方法がありますか。

佐藤 例えばデータから、個人の名前と電話番号を削除すればそれでいいのか、という

「技術開発の段階から、

法制度の専門家と協力して、

技術が普及したときの制度を考えるべき」



と、そう簡単ではありません。生年月日、性別、郵便番号が残っていれば、外部情報との突き合わせで7～8割がた、誰だかわかってしまう。しかも、データの種類や特性（パラッキ具合など）、突き合わせ得る外部データに依存するため、一般的な匿名化方法はなく、一律の基準を定めることはできません。また、厳重に匿名化を進めるほどデータの利活用は難しくなります。

星 匿名化において留意すべきことはありますか。

佐藤 匿名化には、データの分析よりも高度な知識、技術が必要になります。データ分析と匿名化は矛と盾の関係にあって、データ分析手法を知らないと、データを守る匿名化は難しいのです。しかし、こうした人材を育てるには時間がかかることから、人材が潤沢ではないことを前提に対策を考える必要がある。技術WGの第三者提供モデルはそれを前提にしています。

星 今後さらにパーソナルデータの利活用が活発になると、どのような新たな課題が出てきますか。

佐藤 顔識別とゲノム（遺伝子）を特に心配しています。技術が高度になり、どちらも識別の速度、精度が飛躍的に高まっているからです。例えば、街角の監視カメラや、ソーシャルネット上の顔写真などを突き合わせれば、

他のデータをいくら匿名化してもプライバシーがほとんどわかってしまう場合もあるでしょう。かといって、監視カメラなどを規制しすぎると安全を脅かす可能性もあります。

星 今後のプライバシーはどのように守るべきでしょうか。

佐藤 ビッグデータと呼ばれる技術が話題になっています。ビッグデータでは相違のデータを組み合わせることで、新しい知見を導き出してくれます。一方で、そのビッグデータによりデータの突き合わせが新しいプライバシー問題を引き起こします。例えば、水道とガスの使用量の両方を見比べれば、お風呂に入っている時間などがわかります。

星 どのようにしてパーソナルデータを守るべきでしょうか。

佐藤 技術者としては、この現実を認めるしかありません。パーソナルデータに限らず、技術が引き起こした問題を技術だけでは解決できないことが多くなっています。実際、ビッグデータや顔識別などの技術の発展が、新しいプライバシー問題を作っている部分があります。それを抜本的に防ぐ技術があるとは限らない。そうすると技術以外の方法、例えば規律を含む制度で問題を解決するしかない。技術WGが提案したパーソナルデータの第三者提供では、提供されるデータに完全な匿名化を求めない代わりに、提供元及び提供先がそのデータから個人の特定などをしない

規律を課すなど、技術と制度を組み合わせるパーソナルデータを守ろうとしています。

星 将来の技術と制度の関係はどうなると思いますか。

佐藤 今後は技術と制度は不可分として考えていくべきです。つまり、技術開発の段階から、法制度の専門家と協力して、技術が普及したときの制度を考えるべきです。逆に制度自体が技術に依存することも増えており、技術者が制度設計に参加する機会も増えていくでしょう。例えばウェアラブルカメラが話題になっていますが、単に製品を売るだけではなく、製品の利用に伴う社会的な問題を予想して、問題を最小化する法制度も一緒に提案すべきです。徴税も、犯罪捜査もITに依存しています。情報学の研究者には、将来の技術発展を予測して、技術にあった制度設計や社会設計を図ることが求められるでしょう。その意味では情報学を扱う研究機関であるNIIの役割はますます大きくなるはずで

インタビューの一言



議論中の新制度では、第三者へのパーソナルデータ提供では「匿名化」を義務付け、第三者機関の監視下に置く。産業界の負担が増えるとの見方もあるが、佐藤教授は世界的な流れに取り残されるわけにはいかない、と指摘する。パーソナルデータ利活用のメリットとプライバシー保護にはトレードオフ（相反）の関係がある。今や情報技術は社会の隅々まで深く食い込んでいる。一般の市民・消費者にとっても、技術と制度の知識はますます必要となってきたと感じた。

星 暁雄

Akio Hoshi
IT ジャーナリスト

早稲田大学大学院理工学研究科を修了。日経 BP 社で『日経エレクトロニクス』記者、オンラインマガジン『日経 Java レビュー』編集長などの経験を積み2006年に独立。半導体からOS、プログラミング言語、インターネットサービスに至る幅広い取材経験をもつ。

個人情報保護法の改正に向けて

識別性の明確化と独立第三者機関の設立がカギを握る

That's Collaboration 1

現在、2005年から全面施行されている個人情報保護法を改正する取り組みが進められている。その背景には、技術の急激な進展に伴い、より現実に対応したかたちで制度を見直すことに加え、プライバシーを保護しつつパーソナルデータを利活用したい、という狙いがある。本稿では、インターネットや情報セキュリティに関する法律問題の第一人者であり、個人情報保護法の権威として知られる法律家の岡村久道教授に、現行法の問題点と法改正への期待と課題について話を聞いた。

過剰反応、技術の進展、 主務大臣制などの問題

佐藤 現行法の問題点をお聞かせいただけますか？

岡村 施行当初、問題となったのは過剰反応でした。例えば、JR福知山線脱線事故では、被害者のご家族からの安否確認を搬送先の一部の病院が拒否したため、大きな混乱が起きました。なかには死に目に会えなかったご家族もいらしたのではないのでしょうか。またこのとき、被害者の携帯電話の中身を知りたいというご遺族が多くいらしたのですが、憲法の定める「通信の秘密」に阻まれた。一方で、守られるべき情報が漏洩する事件が後を立ちません。私は、こうしたちぐはぐな状況を是正し、個人情報の保護と流通のバランスを図っていきいたいという思いで、この問題に取り組んでいます。

佐藤 そうしたなか、岡村先生は中央省庁の政

策立案に関与されたり、NIIの客員教授として市民講座やメディアでご講演されていますね。

岡村 情報分野の法制度に関わる研究者は少ないですからね。ましてや、法律の立案から現状まで俯瞰して話せる法律家はほとんどいない。こうした新たな問題と法制度の関係性を一般にわかりやすく説明するのも私の役目だと思っています。

佐藤 先ほどの過剰反応のほかに、現行法にはどんな問題点があるのでしょうか？

岡村 大きく分けて、3つあります。1つ目は、技術の進展に対して社会制度が追いついていない、という点。2つ目は、この法律が主務大臣制^{*1}を採用していて、分野ごとに指針が縦割りになっている点。OECDの国際会議^{*2}でも、日本からはコミッショナー（責任者）ではなく、オブザーバー（傍聴者）として出席するにとどまり、国益に添った発言が難しい。また、縦割りでは対応できないような新たな技術も生まれています。例えば、携帯電話会社に対しては総

岡村久道

Hisamichi Okamura

国立情報学研究所 客員教授
弁護士



務省の指針が適用されますが、携帯電話の一機能である「おサイフケータイ」については金融庁、モバイルSuicaについては国土交通省といった具合で、すべての指針が重複されて適用されてしまうのです。やはり、核となる監督機関として第三者機関をつくる必要があるでしょう。そして3つ目の問題点は、「個人識別性」という概念が非常にわかりにくいこと。これを明確化することにより、先の過剰反応といった問題にも対応できると考えています。

曖昧な「識別性」の概念を どう定義し直すか

佐藤 識別性については、私が主査を務めた「パーソナルデータに関する検討会」の「技術検討ワーキンググループ」でも焦点となりました。識別性は技術の進展によって変化することから、都度、概念を見直す必要があるのでしょうか？

岡村 重要なご指摘です。ただし、識別性についてはOECDガイドラインやEU指令の概念を踏襲したものであり、現代のようにデータが国際間でやり取りされる時代においては、国際的な視点から概念定義を明確化する必要があります。さらに、国内の情報公開制度の不開示事由^{※3}や番号法^{※4}など、膨大な条例や法令が個人情報保護法の概念を踏襲している点を踏まえると、整合性を見ながら慎重にことにあたる必要があります。

また、法律というのは、一審で有罪でも二審で無罪となることがあるように、見方次第で結果が変わるという側面をもっています。あるいは、1つの法律だけで閉じているわけではなく、個人情報保護法ではOKだけど、プライバシー権には違反する、といったこともあり得る。法改正では、個人情報保護法とプライバシー権の間に齟齬が生じないように整備すると同時に、「自己情報コントロール権」が侵害された場合にどういう実害が生じるのか、もう少し踏み込んで考えていく必要があると思います。

独立第三者機関への期待と 人材育成

佐藤 法改正に伴い第三者機関の設立が検討さ



れています。そのメリットと組織のイメージをお聞かせください。

岡村 メリットは、分野横断的な問題に対処できるという点。現状は各省庁ごとに四十数種類ものガイドラインが林立していますが、実際のビジネスはもはや縦割りでは対処できません。また、データの海外移転などを踏まえて、日本の「プライバシーコミッショナー」として諸外国に日本の立場を主張できる点も大きなメリットでしょう。組織のイメージとしては、現在、内閣府に置かれている「特定個人情報保護委員会」^{※5}を拡張、発展させた形がふさわしいかと。国際調和の観点から、公的機関に対する監督機関を、より公共性の高い機関にするのか、権限をどこまで付与するのか、違反した場合のペナルティ（課徴金）をどうするのか、人員確保をどうするのかなど、課題は山積みです。

いずれにしても、改訂OECDガイドラインを踏まえて、初めて日本が国内法の改正をするわけですから、大綱をまとめるにあたっては、国際的に先陣を切るという気概をもって取り組んでもらいたい。ただ、技術はどんどん進歩していきますから、一気に決めるのではなく、将来の見直しも視野に入れておくべきです。日本版プライバシーコミッショナーの誕生に、大いに期待したいですね。

佐藤 技術の問題を技術で解決できないことに技術者として歯がゆい思いを抱えていますが、やはり、これからは技術者と法律家が協力して、制度との両輪で解決していかなければなりませんね。

岡村 保護する技術と破る技術は、つねにイタ

チごっこで開発されていますから、やはり、制度面でフォローすることが不可欠でしょう。しかしながら、技術の進歩の速度に対して、どうしても法律はその性格上、後手に回ってしまう。そうした意味からも、法律家と技術者が共同で対策を立てていかなければならないと思います。

一方、法律家でも、専門が違えば、隣のことはわからないという状況がある。個人情報保護の根底には、判例上認められてきたプライバシー権があり、このプライバシー権は、憲法上の「表現の自由」と対になるものです。本来、公的空間における情報の流通の自由と、閉じた私的空間における自己情報のコントロールの両立を目指すべきだと思いますが、個人情報を知っている、それ以外の法制度には疎い法律家がいちりする。全体に目配せしながら制度設計ができるような人材の育成が急務でしょう。そうした意味でNIIにおいても、法律のわかる技術者、技術のわかる法律家とともに育て、両者が前向きに議論を交わすことのできる貴重な「空間」として発展していく必要があるのではないのでしょうか。（聞き手＝佐藤一郎、構成・文＝田井中麻都佳）

※1 主務大臣制 各主務大臣が所管の個別分野において当該分野の実情に応じて指針を示すなどして監督すること。

※2 OECDの国際会議 OECD（経済協力開発機構）において、1980年、「プライバシー保護と個人データの国際流通についてのガイドラインに関するOECD理事会勧告」が採択された（2013年に改訂）。このガイドラインに記された八原則が、OECD加盟国の個人情報保護法制のスタンダードとなっている。

※3 情報公開制度の不開示事由 情報公開法・各情報公開条例のなかで、不開示情報として個人に関する情報が規定されている。

※4 番号法 「行政手続における特定の個人を識別するための番号の利用等に関する法律」の略称。

※5 特定個人情報保護委員会 個人番号その他の特定個人情報の有効性に配慮しつつ、その適正な取扱いを確保するために必要な措置を講ずることを任務とする内閣府外局の第三者機関。

柔軟性ある個人情報保護と活用へ コンジョイント分析で人々の姿勢を浮き彫りに

個人情報の活用や保護に関して、人々の意識はさまざま。個人情報は保護されるべきだという基本的な考え方は共通するものの、個人によって、どこまで情報を出すのかといった意識は大きく異なり、その対価で何を得られるのか、といったことで姿勢は大きく変わる。これを、コンジョイント分析手法を用いて浮き彫りにするのが、岡田仁志准教授が取り組む研究テーマの1つ。この研究成果は、個人情報保護に関するルールづくりにも応用されようとしている。

個人情報保護・活用には、 柔軟な取り組みが必要

個人情報の活用および保護に関する議論が活発化している。

企業からの個人情報の漏えいや、それを利用した企業情報や電子マネーの詐取といったサイバー犯罪が発生。ITの普及に伴って、個人情報を巡る課題は、世界的な関心事になっているのは周知のとおりだ。

だが、「単純に個人情報を保護すべきか、すべきでないかという議論に終始するのは意味がない」と、NIIの岡田仁志准教授は警鐘を鳴らす。

個人情報に対する考え方は、人によってさ

まざまだ。

まったく個人情報を出したくないという人もいれば、氏名、年齢はいいが、それ以外は公開したくない、あるいは、購買履歴情報、位置情報まで公開しても構わないという人もいる。そして、その考え方は、提供されるサービスなどによっても大きく異なる。

個人情報を提供したくないという利用者が、ソーシャルメディアを通じて、自らが食事をしている様子などを広く公開するといったように、サービスを楽しむ上で意識せず個人情報を提供してしまっているという例も少なくない。個人情報に対する意識と行動が乖離しているケースだといえよう。

一方で、制度の上で、個人情報の保護ばかりを優先すると、活用といった面での制限が増え、情報を活用した新たなサービスの創出

を阻む要因にもなりかねない。企業においては、余計な個人情報を取得することはリスクにしかならないが、適正な情報を収集し、それを活用することで、革新的なサービスの創出や、企業競争力を高めることができるのは明らかだ。保護とのバランスをとりながら、活用においても前向きな議論が必要である。

岡田准教授は、「個人情報の活用や保護についての議論やルールづくりは、択一的な観点での議論だけでは危険である。柔軟性をもった捉え方が必要である」とする。

ユーザの本音を引き出す コンジョイント方式とは

こうした個人情報の保護と活用において、

コンジョイント調査画面の例。9枚のカードをインターネット画面に一覧で表示、回答者が選好順にクリックしていくと、カードの選好順が記録される仕組みになっている。

購買履歴 開示しない	購買履歴 開示しない	購買履歴 開示しない	購買履歴 利用店名	購買履歴 利用店名	購買履歴 利用店名	購買履歴 店名+品名	購買履歴 店名+品名	購買履歴 店名+品名
位置情報 通知しない	位置情報 市区町村	位置情報 店舗・建物	位置情報 通知しない	位置情報 市区町村	位置情報 店舗・建物	位置情報 通知しない	位置情報 市区町村	位置情報 店舗・建物
クーポン 割引なし	クーポン 5%割引	クーポン 15%割引	クーポン 5%割引	クーポン 15%割引	クーポン 割引なし	クーポン 15%割引	クーポン 割引なし	クーポン 5%割引

① 購買履歴 開示しない 位置情報 通知しない クーポン 割引なし	② 購買履歴 利用店名 位置情報 市区町村 クーポン 15%割引	③ 購買履歴 利用店名 位置情報 通知しない クーポン 5%割引
---	--	--

①何も開示したくない人が1位に選ばれるカード
②なんらかのメリットがあれば積極的に通知してもよい人が1位に選ばれるカード
③購買履歴は提供してもよいが、位置情報の提供には抵抗がある人が1位に選ばれるカード

個人の意識を研究するために、岡田准教授が用いているのが、コンジョイント分析手法である。

コンジョイント分析とは、複数の評価対象を示し、それを繰り返し回答者にたずねることで、トレードオフの関係にある要素との相関関係を捉えながら、人々の考え方や行動を浮き彫りにしようというものだ。

岡田准教授が取り組んでいる研究では、インターネットを活用し、無作為に選ばれた対象者が、画面上に表示される9種類のカードを見比べて、そのなかから順に、自らの個人情報に対する姿勢に合致したものを選択することになる。2010年から研究を開始し、設定する項目を変えながら、さまざまな角度からの分析を行っているという。多いときには月1回のペースで情報を収集している。

一般的な調査では、「個人情報は保護すべき」と質問すれば、ほぼ100%に近い人が「はい」と答えるだろう。そして、個人情報をむやみに出したいとする回答も多いはずだ。

だが、仮に、「個人情報を提供する」という項目に加えて、「災害時の政府の支援対象となる」、「一定期間を過ぎれば情報を破棄」という項目が加われば、多くの人が個人情報の提供に同意すると考えられる。つまり、コンジョイント分析では、さまざまな要素を組み合わせたカードを対象者に見せ、どちらのカードに書かれたものを優先するかということを繰り返し調査することで、人々の姿勢を明らかにしていくことになる。

「個人情報は提供したくないと考えている人でも、個人情報を提供することによって、ポイント還元などのメリットを得られるとなれば一定の情報を提供すると答える。また、ソーシャルメディアで個人情報ともいえる写真の掲載や記述をすることは、そのサービスを楽しむというメリットを感じているためである。さらに、研究では、交通系カードの利用に際しては、個人情報を提供したくないという回答が多かったのに対して、流通系カードでは個人情報を提供したいという答えが多

岡田仁志

Hitoshi Okada

国立情報学研究所 情報社会相関研究系 准教授
総合研究大学院大学 複合科学研究科
情報学専攻 准教授

く、メリットを期待していることがわかる。場面や用途、どんなメリットを得られるのかということによって、個人情報の提供に関して提供者の姿勢は大きく変化する」

岡田准教授は、これを「コストとメリットのトレードオフ」と表現する。

「どこまでの個人情報を出せば、どれだけのサービスが得られるのかということ、消費者は強く意識している。個人情報をコストとして捉え、そのコストに見合ったサービスをメリットとして受け取るという仕組みが構築されはじめています」

コストとメリットを明らかにし、 ルールづくりに活かす

個人情報を提供する側と、それを受け取り、活用する側とが、コストとメリットのトレードオフの関係を理解することは、個人情報を有効活用する社会環境の構築において近道となる。

岡田准教授は、「個人は、どこまでのメリットを得られれば、どこまでの個人情報を

提供するのかという目安を理解すること。それに伴って、企業側はどこまでのサービスを提供するのかということ、お互いに理解した上で、それぞれの当事者間の契約が成り立つという仕組みが構築されるべき」とし、択一的な個人情報保護の考え方は適切ではないと指摘する。

現在、政府では、2014年6月を目標に、個人情報保護法改正案の大綱をまとめ、パブリックコメントを経て、2015年初めには、通常国会へ改正案を提出する予定である。

このなかでは個人情報（パーソナルデータ）の取り扱いに関して、いくつかの新たなルールが盛り込まれることになるが、当事者間での契約をベースとすることなどが前提となる柔軟性をもったものへと進化する。

コンジョイント分析手法は、もともと法律や条例などの新たなルールづくりを行う際に採用されることが多い。岡田准教授による個人情報に関するコンジョイント分析を活用した研究成果は、択一的にはならない個人情報保護のルールづくりの実現にも貢献することになりそうだ。

（取材・文＝大河原克行）

パーソナルデータの制御権を自らの手に！

恣意的な顔認識へ議論を投げかける「プライバシーバイザー」

ビッグデータ収集と解析技術の発展により、パーソナルデータが予想もつかない目的に利用される危険性が指摘されるようになった。SNSに登録・投稿されるコンテンツから、写真に写った人物の氏名や住所などの個人情報が、本人の意思とは無関係に丸裸にされてしまう事態が現実のものになったのだ。サイバー空間のパーソナルデータは本人の手で制御できないものなのか？ NIIの越前功教授が開発する顔検出防止ツール「プライバシーバイザー」が、ビッグデータ活用とプライバシー保護の議論に新たな一石を投じている。

顔認識の問題点

カメラ付き携帯電話やスマートフォンの普及とSNSの利用拡大に伴い、街角や施設内のスナップ写真が気軽にインターネットに公開されることが多くなっている。被撮影者にはその許可を得ていたとしても、背後にたまたま映り込んだ人は、自分の写真が公開されることが想像してもいないに違いない。ところが現在の顔認識技術によれば、その写真

に映り込んだ顔の特徴から、同一人物を探し出すことが簡単にできてしまう。さらに、写真に付帯する情報から、日時と位置情報まで公開されてしまうこともある。人物が同定できれば、インターネット上にある数々の情報源から関連する情報を検索・収集することは難しくないだろう。つまり、たった1枚の写真への映り込みから、自分がいつ、どこで、何をしていたかを見知らぬ誰かの知るところとなり、リンクをたどればどんな仕事をし、どんな仲間がいるのかといった情報まであかさまになってしまうのだ。

さらにGoogle Glassに代表されるカメラ

搭載ウェアラブルデバイスの実用化が目前になっており、こうしたデバイスを通して見た人物のパーソナルデータが、その場でリアルタイムにわかる時代がすぐそこまで来ている。

「自分の情報がサイバー空間に拡散し、商用にも利用されてしまう現実に対して、個人が自分自身のプライバシーを守るために何ができるかを考えてほしい」と、NIIの越前功教授は語る。「例えば、米カーネギーメロン大学が匿名で写真撮影に同意した人の顔写真をもとにFacebookに照合して人物同定ができるかを実験したところ、被験者の1/3の同定に成功、個人的な興味関心事や社会保障番号の一部も判明してしまいました。顔写真だけでプライバシーが暴かれる時代がすでに到来しているのです」※

顔検出を無効化する「プライバシーバイザー」

ビッグデータが活用可能な時代だからこそ生じているプライバシー侵害への懸念から、越前教授が急ピッチで研究・開発を続けているのが「プライバシーバイザー」だ。「プライバシーバイザーは、パーソナルデータである『顔』画像を恣意的に利用されないように自衛するための試みです。情報を収集する側の仕組みがどのようなものであれ、被撮影者の側でこれを装着することにより、顔認識の前処理である顔検出を無効化して、プライバシー侵害



越前 功

Isao Echizen

国立情報学研究所
コンテンツ科学研究系 教授
総合研究大学院大学 複合科学研究科
情報学専攻 教授

を防ぐことができます」と越前氏は言う。

いまや一般的なデジタルカメラでも、映像の中から人の顔だけを検出する技術が搭載されている。代表的な顔検出手法としてViola-Jones法が採用されていて、顔の特徴量として主に目の周辺と鼻筋、および鼻の周囲の輝度（明暗）の差を抽出し、蓄積・学習した顔の特徴データと照合して顔を検知する。

この手法はかなり精度がよく、越前教授の実験では22m離れた場所からの撮影でも顔検出ができるばかりか、デザインの異なる5種類のサングラスで変装してみても、顔が正しく検出できたという。この顔検出を失敗させるための対策として、これまでは特殊な顔面着色や髪型、あるいは顔面を蔽うマスクの着用が提案されてきたが、現実世界の対面コミュニケーションに支障をきたすという弱点があった。もっと自然に利用できる顔検出防止ツールとして開発されたのが、ゴーグル型のプライバシーバイザーだ。

越前教授は目の周辺領域を蔽う形状のゴーグルに11個の近赤外LEDを取り付け、顔検出されたくない時にLEDを点灯できるようにした。人間の可視域を超える波長の光なので、点灯状態でも対面する人には光は見えないが、民生用のカメラは赤外領域まで感知するため、LEDの光はノイズとして映る。その結果、目の周囲の輝度差が検出できなくなり、顔検出に失敗するというのがプライバシーバイザーの仕組みだ。

カメラの前に10人の被験者を並べて撮影した実験によると、バイザーを装着しない場合には、20m離れたところの被験者のうち7～8人の顔検出に成功した。バイザーを装着しただけでは顔検出率にあまり差はなかったが、LEDを点灯した場合には、22m以内に

いる人物は誰ひとり顔検出ができなかった。

電源不要でファッショナブルな 新プライバシーバイザー

ただし、この試作品ではLEDを点灯するために電池を要するところに難があった。また、プロ用のカメラでは赤外領域を感知しないの



プライバシーバイザーのプロトタイプ



で効果がない。そこで越前教授は昨年末から眼鏡製造で世界的に有名な福井県鯖江市の眼鏡メーカー数社と共同で、LED不要の新しいプライバシーバイザーの開発を進めている。

新プライバシーバイザーは、顔検出器が暗いと判断する目の周囲などの窪んだ領域に可視光を反射する素材を採用し、逆に顔検出器が明るいと判断する鼻上部などの出っ張った領域には可視光を吸収する素材を採用。試作品は白を基調に、細かいドットや文様を透明部分に散りばめた。これなら、サングラスのように持ち歩きにも装着にも比較的違和感や負担感は少なそうだ。デザイン上の工夫も加えながら、年内にはプロトタイプ出荷を目指しているという。

情報の利活用とプライバシー 保護のバランスが重要

一方、懸念されるのは、プライバシーバイザーが犯罪を助長しはしないかという点だ。

「例えば空港の監視カメラでテロリストを発見するといった目的で顔認識が使われていますが、そうした場所でのプライバシーバイザーの着用は禁止するなど、制度面での対策が必要でしょう。公益とプライバシー保護のバランスが大事です」と越前教授。プライバシーバイザーは、こうした課題への問題提起でもあるのだ。

さらに越前教授は、プライバシーバイザーの着用が個人画像の利用を拒否するサインとなる可能性を指摘する。人の装着物（アクセサリ、バッジなど）によって、自分のパーソナルデータの利用範囲を表明し、その条件に基づいてデータの利活用が図れるようにする仕組みの提案も視野に入れているのである。

ビッグデータ時代の今日、自分のパーソナルデータの何を守り、何を公開すればリスクを最小にして最大の利益が得られるのか、自衛方法も含めてよく考える必要がありそうだ。

（取材・文＝土肥正弘）

※ Facebook の顔認識機能については、2012 年に欧州連合（EU）からの要請を受けて、欧州に限って提供しないことが決まった。Google Glass も顔認識機能は搭載しないことを表明している。しかし、このような技術が実用レベルにある以上、両社が提供しなくても新たなサービス業者やアプリケーション開発業者が開発、提供しないとは言い切れない。

データ活用の利便性と安全性を両立させる

匿名化技術の最新動向とその課題

That's Collaboration 2

パーソナルデータの活用に際して、プライバシー保護を実現していくために不可欠となる匿名化技術。現在、匿名化技術はどこまで進化しているのか。そして、実運用にあたり、どのような課題が浮上しているのか。本稿では、匿名化技術の最新動向と、実用化に向けた展望と課題について、政府IT総合戦略本部「パーソナルデータに関する検討会」技術検討ワーキンググループ（以降、技術WG）のメンバーであるNTTセキュアプラットフォーム研究所の高橋克巳氏に、NIIの佐藤一郎教授（技術WG主査）が話を聞いた。

ビッグデータ時代の匿名化とは

佐藤 まず、今後のビッグデータの利活用の鍵となる「匿名化」についてお聞かせください。

高橋 匿名化の基本的な定義ですが、データに含まれる名前や生年月日、住所といった情報を削除したり、変更を加えたりすることで、個人を特定できないようにすることを言います。つまり、データの「匿名性」を高めるための技術や手法、あるいはそれらの組み合わせを匿名化と呼ぶわけですね。しかしビッグデータ時代を迎え、世に多くの情報が蓄積されるようになったなか、単に名前や住所を削除しても、他のデータとの突き合わせを行うことで個人が特定されてしまうといった問題が指摘されています。

ビッグデータ活用で匿名化が必要とされるのは法制度解釈上の事情からで、その背景には、

さまざまな制約を伴う個人情報を匿名データにして自由に使いたい、というニーズがあります。しかし、個人情報を個人情報でない状態に加工することは技術的には容易ではないケースが多々ある。匿名化技術を使えばいいじゃないかと言われるが、そこには匿名化技術への理解不足があります。データに含まれる名前を削除するなど、「単純な」匿名化は比較的簡単にできる。これが世の中でよく言われている「匿名化」ですが、それだけではデータに含まれる個人が誰であるかわかってしまうリスクは排除できないのです。

佐藤 匿名化というのは単純かつ一律にできるわけではない、ということですね。

高橋 ええ。一方、データに含まれる個人性をほぼ無くしたような状態に加工することは可能です。統計データがこれに相当しますが、これだとデータの抽象度が高くなりすぎて、分析対象データにはならない場合がある。これが、パーソナルデータの匿名性と有用性のジレンマです。

データの利用価値を損なうことなくプライバシーを確保する技術

佐藤 ジレンマの克服のためには、何を目標せばいいのでしょうか？

高橋 分析目的に応じて、必要最小限の情報だけを残すことが理論上の目標になります。「技術WG」では、匿名化の基本的な考え方として、「汎用的な匿名化は存在しない。種類・特性・利用目的等に応じケースバイケース」と表現しました。

このような状況においては、個人情報であるか否かということは、必ずしも根源的なことではなくなるでしょう。むしろパーソナルデータ



佐藤一郎

Ichiro Satoh
国立情報学研究所
アーキテクチャ科学研究所 教授
総合研究大学院大学
複合科学研究科 情報学専攻 教授

高橋克巳

Katsumi Takahashi
日本電信電話株式会社
NTT セキュアプラットフォーム研究所
情報セキュリティプロジェクト
プロジェクトマネージャ
主席研究員 博士（情報理工学）

〔図1〕k-匿名化の例

会員番号	生年月日	住所	年齢	購買品
1001	1979.04.01	東京都中央区A町	34	パン
1002	1986.12.10	神奈川県横浜市A町	26	漫画
1003	1974.10.10	東京都渋谷区B町	38	アイス
1004	1991.05.05	神奈川県鎌倉市B町	22	文庫
1005	2006.11.10	埼玉県川越市A町	17	コーラ
1006	1990.02.06	神奈川県厚木市C町	23	時刻表
1007	2003.08.15	埼玉県浦和市B町	19	牛乳
1008	2000.09.30	埼玉県大宮市C町	9	お茶
1009	1983.01.01	東京都練馬区C町	30	弁当
1010	1994.07.07	埼玉県与野市D町	18	水

↓ k-匿名性 (k=3) を満たした状態

会員番号	生年月日	住所	年齢	購買品
1001	1979.04.01	東京都	30代	食品
1003	1974.10.10	東京都	30代	食品
1009	1983.01.01	東京都	30代	食品
1002	1986.12.10	神奈川県	20代	書籍
1004	1991.05.05	神奈川県	20代	書籍
1006	1990.02.06	神奈川県	20代	書籍
1005	2006.11.10	埼玉県	未成年	飲料
1007	2003.08.15	埼玉県	未成年	飲料
1008	2000.09.30	埼玉県	未成年	飲料
1010	1994.07.07	埼玉県	未成年	飲料

の性質と行いたい分析の目的に応じて、最善のデータ処理方法をとることが重要になります。そしてプライバシー上のリスクを情報の提供者に正確に表現して、活用側への制度的な担保も含め、安全なデータ処理ができるようにする必要があります。

佐藤 技術としては、どのような方法があるのでしょうか？

高橋 例えば、分析の目的として個人情報のまま取り扱いたいのであれば、暗号が役に立ちます。我々は、プライバシーの保護と安全管理措置を実現できるよう、暗号化したままデータ処理を行う「秘密分散・秘密計算技術」に関する研究開発を進めてきました。これらの技術群はデータの正確さを損なうことなく、その秘匿性を極限まで追求するものです。

一方、匿名化をとるのであれば、プライバシーのリスクの表現パラメーターである「k-匿名性」があります。k-匿名性とはデータの匿名性を評価する指標で、「同じような属性の人が、必ずk人以上いる状態」のこと。例えば、年齢が20代でも、30代でも、対象とする属性に含まれる人が少なくとも10人以上いる場合、このデータの匿名性は「k=10」と表現されます。つまり、kの数値が大きいくほどプライバシーリスクは小さくなります。なお、k-匿名性を実現するパーソナルデータの加工技術がk-匿名化です。同じ属性の組み合わせをもつレコードを少なくともk個存在するよう、属性の値を粗くする一般化や、希少な人のデータの削除によって「k-匿名化」が実現できます(図1)。

佐藤 NTTセキュアプラットフォーム研究所では、さらに進んだ取り組みをされていますね。

高橋 我々のチームが新しく開発したのが、「Pk-匿名化」という手法です。Pk-匿名化は、個々のデータを確率的に変化させる処理である「ランダム化」※1を行って、データが誰のものであるのかをわからなくします。本手法のランダム化は誰のレコードであるか1/k以上の確率で当てることができないように制御するというものです。この性質をPk-匿名性(確率的なk-匿名性)と呼んでいます。その後、「ベイズ推定」※2と呼ばれる機械学習の手法を用いることで、データの元の状態を推定する処理を行います(図2)。このことで、実用的な分析が

可能な有用な匿名データが作成できます。これは、実パーソナルデータに基づく疑似パーソナルデータとも言えるでしょう。Pk-匿名化はk-匿名性と同様の性質をもちながら、ビッグデータの匿名化に有効だと私たちは考えています。

佐藤 Pk-匿名化は、どんなデータにも活用できるのですか？

高橋 とくに、多数の項目をもつ「長い」パーソナルデータの匿名化に有効です。長いデータの匿名化では、データの必要な項目を選択して匿名化を行う「オーダーメイド匿名化」が繰り返されることが多いと思いますが、複数の匿名化データを突き合わせることでk-匿名性が損なわれる可能性が指摘されていました。対して、Pk-匿名化はそうしたk-匿名性の喪失にも耐性をもつため、繰り返しオーダーメイド匿名化ができ、多項目のパーソナルデータに関しても、プライバシーを保護しつつ利用価値の高い分析用データに加工できるのが特長です。

技術と制度の両面で プライバシーを保護

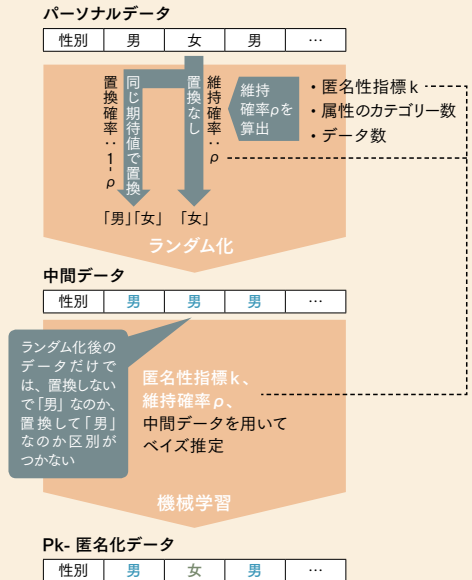
佐藤 今後、個人情報保護法の改正等に伴い、さまざまな場面でk-匿名性が大きく関わってくると考えています。データの第三者提供の許諾等に際して、k-匿名性がその判断の指標の1つとなるのでしょうか？ その場合、kの値がいくつだったら、安全になるということと言える

〔図2〕Pk-匿名化の概念図

Pk-匿名化はk-匿名性と等価な安全性をもつ世界初のランダム化法

ランダム化▶ データの確率的な置換だけでk-匿名性を確保(数学的に保証)

機械学習▶ ランダム化のパラメータを使い分析に適したデータを推定し補正



のでしょうか？

高橋 それは難しい問題ですね。実際にkの値だけで安全性を判断できるのかという面もありますし、k=1でもリスクがほとんどないケースもあるでしょう。kの数値の妥当性は、今後、法制度の整備を含めた社会的な運用によって定まっていくでしょう。

佐藤 これからの匿名化データの適正な利活用に当たっては、技術だけでなく制度も含めた両輪で回していくことが必要というわけですね。

高橋 個人情報については、法制度に基づき取り扱えばいい。また、明らかに特定の個人と切り離されたデータは、第三者も含め自由に使うことができる。これからの課題は、この2つ以外の「匿名化データ」の扱いです。その提供や利用に際して、社会的なルールを策定していくことで、プライバシー保護が可能になると考えています。プライバシー上のリスクがあるデータは、信頼できる相手にしか提供できません。すなわち、定められたルールを守っている相手であれば許可するけれども、ルールを守れなかった場合には、許可を取り下げたり罰したりするといった法制度を策定、運用していくことで、匿名化データを取りまく課題も徐々に解決していくのではないのでしょうか。

(取材・文=伊藤秀樹)

※1 ランダム化 データ分析に影響を与えない程度に元データにノイズデータを付加する匿名化手法。
※2 ベイズ推定 観測された事象から、その原因となる事象の確率を推定するための確率論的方法。

過去からの教訓

岡村久道

Hisamichi Okamura

国立情報学研究所 客員教授
弁護士

誰にでも忘れられない日があるはずだ。筆者にとって2005年4月25日が、それにあたる。

この日の朝、大阪市内に向かう通勤電車に乗っていた。うららかな春の陽が降り注いでおり、日頃と変わらぬ平凡な朝の光景だった。ところが、その直後から大事故発生の報道で埋め尽くされていった。JR尼崎駅の手前で快速電車が脱線し、107名が死亡するという未曾有の列車事故が発生したからだ。皮肉にも自分が乗った電車の直後を走る快速だった。

その日の午後、近畿大学で法科大学院の講義を終え、会議のために法学部長室に入ると、学部長がせわしなく携帯電話を掛けていた。法学部生の保護者から、「この電車に本人が乗っていたおそれがあり、携帯に何度電話しても連絡が取れないので、授業に出席していないか確かめてほしい」という連絡があり、確認させたが学生は出席していなかったという。保護者から聞いた学生の携帯番号宛に、学内関係者は何度も電話を掛け続けたが、つながることはなかった。建物の外に出ると、いつしか冷たい霧雨に変わっていた。その学生は最悪の結果となったことが後日判明した。

当時の報道によれば、事故現場では、被害者の携帯宛に、かけがえのない人の安否を気遣う家族からの

呼び出し音やメール着信音が、気が遠くなるほど繰り返し鳴り響いており、受話器の向こうで明暗が分かっていた。

その一方、数百人に及ぶ負傷者は、神戸から大阪にかけて広域の病院に搬送されていた。被害者の家族は安否を気遣って収容先病院を回ったが、収容の有無すら教えてもらえないケースが多発していた。つい25日前に施行された個人情報保護法（保護法）違反に問われることを怖れた病院側が、委縮して収容者の氏名公表を躊躇したことが原因だった。そのため最後の言葉を交わせなかった家族もいたようだ。これを皮切りに、保護法への「過剰反応」が社会問題となった。

この事故から9年の歳月が流れた現在、保護法の改正に向けた検討作業が進められている。情報通信技術の発展に伴う新たなパーソナルデータの利活用に対応するためのものだ。しかし、今も「過剰反応」には抜本的な対策が講じられないままだ。

過去を起点に未来は扇状に続くが、過去の出来事は常に未来への貴重な教訓を残している。我々はそれを、ときどき振り返ることによって、どのようにして保護と利活用の適正な調和を図るべきか、在るべき姿を常に問い続けなければならないはずだ。