NRI 未来創発
Dream up the future.

IT ソリューション フロンティア
IT Solutions Frontier

特集「パーソナルデータ」

09 | 2014 Vol.31 No.9
(通巻369号)

www.nri.com/jp

野村総合研究所
Nomura Research Institute

ITソリューションフロンティア
IT Solutions Frontier
09／2014

視　点

特　集　「パーソナルデータ」

NRI Web Site

社会を進化させるパーソナルデータ

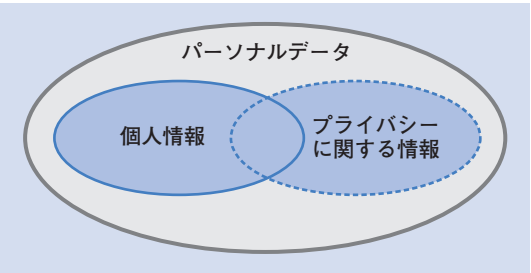
ITの進化は私たちの生活を便利なものにしてきた。その代表格がインターネットであり、Google社の検索サービスやAmazon.com社のネット通販は私たちの生活を一変させたといっていいだろう。インターネットへのアクセス手段もしかりである。1999年に登場したNTTドコモのi-modeによって、携帯電話でインターネットにアクセスできるようになったことは画期的だった。しかし、当時の小さな画面を見ながらの操作は、決して使い勝手がいいとはいえなかった。

この状況を一変させたのが、Apple社のスマートフォンiPhone（日本では2008年に販売開始）と、Google社などが開発したAndroidをOS（基本ソフト）に採用したスマートフォンの登場（日本では2009年）である。使い勝手のよいスマートフォンがITサービスの利用を拡大させ、それに合わせてさまざまなサービスが登場するという状況が続いている。これを支えているのは、クラウドコンピューティングやスマートフォンに代表される、処理能力の向上と処理の分散化である。

今後、社会を進化させるドライバーになると思われるのがビッグデータの活用である。中でも注目されるのがパーソナルデータである。パーソナルデータは、個人に関連する情報を指す最も大きな集合である。いわゆる個人情報は、特定の個人を識別できる情報であり個人情報保護法によって保護されるが、それはパーソナルデータの一部である。個人情報に該当しないパーソナルデータは、法令上は本人の同意なしに利用や提供ができる。そのため、個人情報を含まないパーソナルデータが注目を浴びているのである。

ただし、プライバシーに抵触するリスクがないわけではない。プライバシーに関する法令上の定義はないが、プライバシーは個人や家庭内の私事、私生活に関する情報全般であり、パーソナルデータの活用においては個人情報に加えてプライバシーへの配慮が必要となる。最近は、計画的なプライバシー対策のプライバシー・バイ・デザイン（Privacy by Design）や、事前にプライバシーへの影響を評価するPIA（Privacy Impact Assessment）などの取り組みも行われている。

政府がパーソナルデータの活用に期待していることを示したのが、2014年１月24日に閣議決定された「産業競争力強化に関する実行計画」である。これは、アベノミクスのいわゆる「第３の矢」である成長戦略の重点施策の実行を加速させるための計画である。「ビッグデータ時代におけるパーソナルデータの



野村総合研究所
常務執行役員
IT基盤イノベーション事業本部長
綿引達也（わたひきたつや）

利活用促進」が挙げられており、イノベーションの推進、IT活用の促進を通じた産業競争力強化という観点からパーソナルデータを含むビッグデータの活用が期待されている。

しかし現状では、広告業界のような一部の事例を除いて、ビッグデータの活用が成功しているとはいい難く、産業力強化に本当に寄与できるのかという懐疑的な意見も多い。例えば、顧客マーケティングや商品レコメンデーションにおけるビッグデータの活用に期待している企業は多いと思われるが、実際にビッグデータを分析してみると、「CRM（顧客関係管理）やBI（ビジネスインテリジェンス）の結果と大きく違わない」といった声が聞こえてくることも少なくない。当然であるが、データの量や、データを取得できるチャネルが増えたからといって、単純に効果が出るものではない。ここは一段の工夫が求められるところである。

産業競争力の強化を可能にするビッグデータ活用とは、ほかにどのようなものがあるだろうか。例えば、GPS（全地球測位システム）により得られた移動履歴データといったパーソナルデータを防災・減災対策に活用することが考えられる。それによって被害を抑えられれば、あらゆる産業において生産力の低下やサービスの中断を最小限にとどめ、災害からの復旧を早めることができるだろう。

また、ゲノム（遺伝子）の解析結果を病気の早期発見や健康管理に活用することも考えられる。家族の介護の負担を減らすばかりでなく（24時間の介護が必要なために、家族が仕事に就けなかったり、仕事を辞めざるを得なかったりするケースは非常に多い）、関連産業の雇用を拡大することにも貢献するだろう。この分野は海外の方が進んでいるが、世界一の超高齢社会の日本においてこそ、今後さらに重要になってくるといえるだろう。

問題は、移動履歴やゲノムといったパーソナルデータは、多くの人にとってプライバシーそのもののデータだということである。自分がどこに行っていたのか、どういう病歴があるのか、他人に知られたくないという思いは誰にでもあるだろう。その一方で、そのようなデータを大量に集めて分析し、活用することが新たな知見を生み社会を進化させることも事実である。この二律背反を解決するための何らかの仕組みが必要になってくる。

現在、プライバシー保護とパーソナルデータ活用を両立させるため、個人情報保護法改正の動きが進んでいる。欧米はこの分野でも先行しており、すでにパーソナルデータの取り扱いについて一元的に監督する第三者機関の設置が進んでいる。日本でも同様の第三者機関の設置が検討されているが、さまざまな課題もある。有効なデータ活用ができる社会にするために、事業者や利用者を巻き込んだ国民的な議論が進むことを期待したい。 ■

越境データ保護が企業に求める新たな対応
―世界同時進行のプライバシー保護規制強化―

データの活用によるイノベーションへの期待が強まる一方、パーソナルデータに関する制度の改正が世界で相次いでおり、日本でも2014年度の通常国会で個人情報保護法改正案の通過が目指されている。本稿では、世界に広がるこうした規制強化が企業にどのような影響を及ぼすか、また企業はどのような対策を取るべきかを考える。

注目される越境データ保護の動向

日本の企業にEU（欧州連合）の規制当局から何億円もの課徴金の支払い命令が突き付けられる、そうしたことが起こりかねない事態が進行している。個人情報保護に関する考え方は国や地域によって異なるが、EUでは、国境を越えて流通する個人情報を各国が協力して保護しようという機運が高まっている。これが越境データ保護である。

この越境データ保護に関する新たな規制はEUの加盟国以外へも域外適用される見込みである。これに対して米国は警戒感を大きく強めているが、日本も例外ではない。これらの動きに対応するため、今号の特集論文でも紹介されているように「プライバシー影響評価（Privacy Impact Assessment：PIA）」などに取り組む企業も現れている。

一方、企業は、自社が持つデータの取り扱いに関して法令順守のためのコストを引き上げられ、情報システムの設計や運用時に配慮すべき点も変わらざるを得ない。そのため、パーソナルデータを活用した企業の新ビジネスの展開意欲を損ねるのではないかと懸念する声もある。

時代や地域で異なるプライバシー保護の考え方

顔見知り同士がどこで何をしているかを承知して助け合って生活してきた日本では、西洋的な「プライバシー」の概念が育たなかったとされる。そうした相互信頼を基本とした社会であった時代を惜しむ声はいまだになくなっていない。

欧米で伝統的にプライバシー侵害とされてきたのは、住居への侵入や過度な訪問、のぞき見などであった。ホテルの部屋のドアノブに「Privacy Please（起こさないでください）」と書かれた札を掛けておく習慣はそのような考え方に基づいたものである。これは個人情報とは違い、個人が特定されていなくても、本人が望まない行為はプライバシーの侵害とされる。こうした「放っておいてもらう権利」という概念は、欧米でプライバシー保護が重視される背景となっている。

プライバシーに対する考え方が文化的背景によって多様であったにせよ、今日では都市化や情報化によって個人情報やプライバシーの問題は各国共通のものになっている。例えば、個人を特定する情報がソーシャルネット

野村総合研究所
IT基盤イノベーション事業本部
ビッグデータビジネス推進室
上席研究員
横澤　誠（よこざわまこと）
専門は社会情報学、国際情報通信政策

表1　パーソナルデータをめぐる近年の動向

国内	海外
・総務省「パーソナルデータの利用・流通に関する検討会」（2012年10月発足、2013年6月報告） ・経済産業省「IT融合フォーラム パーソナルデータワーキンググループ」（2012年11月発足、2013年5月報告） ・規制改革会議「創業等ワーキンググループ」（2013年3月発足、2013年5月報告） ・高度情報通信ネットワーク社会推進戦略本部「パーソナルデータに関する検討会」（2013年9月発足、2013年12月制度見直し方針発表、2014年6月大綱発表）	・EU（欧州連合）「一般データ保護規則案」（2012年1月公表） ・米国政府「消費者プライバシー権利章典」（2012年2月発表） ・米国FTC（連邦取引委員会）レポート「急速に変化する時代における消費者プライバシー」（2012年3月最終版発表） ・OECD（経済協力開発機構）「改訂版プライバシー・ガイドライン」（2013年9月発表） ・EU（欧州連合）「一般データ保護規則案修正案」（2013年10月市民的自由・司法・内務委員会（LIBE委員会）採択、2014年3月欧州議会採択）

出所）本庄智也修士論文（2014年3月。京都大学情報学研究科NRI連携ユニット）

ワークによって拡散することでプライバシー侵害が起きやすくなっている。また、小説のモデルとされた人物がプライバシー侵害で著者を訴える事件も発生している。プライバシーの侵害は、精神的な苦痛を引き起こすと同時に、口座番号やパスワードなどの情報が漏えいすれば、財産の侵害といった実害に結び付く。

一方で、国や自治体、企業が保有するデータを分析することで新たな価値を創造しようという動きも進んでいる。安倍政権が掲げる「世界最先端IT国家創造宣言」（2014年6月24日閣議決定により改定）においても「データ」という語が100回以上使われている。しかし、本特集でも触れられているように、移動履歴や走行データの分析などパーソナルデータの活用には課題も少なくない。

各国の越境データ保護の動向

越境データ保護を強めようとする動きの背景には、技術の進展によってデータ利用が質的にも量的にも広がったという世界共通の現象がある。そのため、これに対応して法制度を充実させる動きもほぼ同時期に相次いで起こった。

2014年に日本が加盟50周年を迎えた経済協力開発機構（OECD）では、各国の個人情報保護法制の基準となった1980年の「OECDプライバシーガイドライン」の改訂版を数年にわたる議論の末、2013年に公表した。新しいガイドラインとその付則は、新たな水準の国際協調と政府の主体的関与を促すものとなっており、インターネットやクラウドコンピューティング、データ活用を前提とした各国でのルール改正に拍車がかかる見込みである。

表1は、パーソナルデータをめぐる欧米の動向を簡単にまとめたものである。米国では一律の規制ではなく業務の特性に応じた自主規制を促しており、カリフォルニア州のように独自の取り組みを行うなど多様なアプローチが見られる。

これに対してEUでは、現行の「データ保

護指令」によって大枠での統一性を確保しながらも加盟国ごとに異なっていたデータ保護規制をさらに統一するため、GDPR（General Data Protection Regulation：一般データ保護規則）への改定作業が進行中である。

この改定は、いくつかの点で企業にとって大きな負担になると見られている。特に米国企業にとっては、これまでセーフハーバー協定（違法とならない範囲を規定した協定）で認められていた規制除外の取り扱いが、米国のNSA（国家安全保障局）による盗聴問題の影響もあって見直されるため、米国はEUと官民を挙げた交渉を行っている。

新しい規則案は、すでに2014年３月12日に欧州議会を通過し、今後、欧州理事会で審議された後、議会、委員会、理事会による三者協議のプロセスを経て2015年中の法案成立を目指している。

しかし、2014年５月に行われた欧州議会選挙の結果を受けて委員会の新メンバーが決まり、また欧州理事会の議長国が変わるなどの情勢変化があり、規制案全体が再審議され、すでに遅れている立法化がいつになるかは不透明である。

一方で、28カ国が加盟するEUよりも多くの加盟国（47カ国）を持つ欧州評議会では、「個人データの自動処理に係る個人の保護に関する条約第108号」（1981年）の改正案が2012年11月に採択された。スイス、ノルウェー、アイスランドなどのEU非加盟国については異なる基準となることに注意しなければならない。

アジアに目を転じると、2013年６月に日本がAPEC（アジア太平洋経済協力）の「CBPR（Cross Border Privacy Rules：越境プライバシールール）システム」に参加申請したことから、これまで日本国内で運用されていたプライバシーマーク制度との関係を整理して相互運用を図るための調整が進行する見込みである。また、オーストラリアでは2014年３月12日に13項目から成る「オーストラリアプライバシー原則」が施行された。台湾や韓国でも、ここ数年で個人情報に関連する法制度の改定が相次いでいる。

日本では、2014年６月25日に公表された高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）の「パーソナルデータの利活用に関する制度改正大綱（事務局案）」に従い、具体的な法律改正のための条文調整が行われている。世界の他の地域や国がさまざまな規制方針を示してくるなかで、日本もデータの保護と活用について明確な思想を持ち、矛盾のない執行体制で対応に当たることが求められる。

企業に求められる対応

2014年５月に、EU司法裁判所は重要な判断を示した。人には「忘れられる権利」があるとして、原告（EU市民）の過去の個人情報へのリンクを検索結果に表示しないことを

Google社に命じた。企業が提供するデータに対して、削除や利用停止にする権利を利用者に認めたことで、Google社も直ちに利用者からの請求を受け付けるためのシステム機能を提供し始めた。

このように、欧州の新しい規制案は企業に多くの対応を求めることになるが、特に重要なのは「第三国データ移転の扱い」「域外適用からの除外」「削除できる権利（忘れられる権利）」「本人同意原則」「監督機関による課徴金」「認証メカニズムとデータ保護シール」などである。

域外適用についてはやや緩和されたものの、欧州以外の国で運用されているインターネット上のサービスにも欧州規制が適用される可能性がある。また、日本企業が欧州の規制を十分に理解せず、自らが欧州での事業主体であるという認識を持たずにいると、世界連結売上高の５％または１億ユーロ（約140億円）を上限とする課徴金が課せられる条項が審議されている。

こうしたビジネス上の障害を避けるためには、リスク評価や、データを提供した個人の同意の確認、国際標準化に取り組むほか、まず欧州の規制議論の現場において日本でも個人情報保護について高い水準が保たれているということを当局に対して明確に示し、現行のスイス、カナダ、イスラエルなどのような「十分性認定国」としての扱いが受けられるようになることが望ましい。

また、企業が「拘束的企業準則（Binding Corporate Rules：BCR）」の承認を受けてグループ企業内でのデータの利用に影響がないようにするなど、官民協力の下で働きかけを行うべきである。

オーストラリアやニュージーランドは欧州より厳しい規制を大企業に対して課している。また、韓国や台湾、そしてASEAN（東南アジア諸国連合）にも欧州型の厳しい規制の基準が広がると、市場としてのみならず生産拠点としてのグローバルビジネス展開戦略は大きな影響を受けるであろう。特に情報システム分野でのオフショア生産、運用やBPO（ビジネスプロセスアウトソーシング）については深刻となる。

社会的要請に応える能力を競争力に

昨今の個人情報保護に関する事件を見ていても、適切なデータ保護を最終的に保証するためには、組織で働く人々の意識を高める必要があることを痛感する。技術やシステムとともに、データを取り扱う組織全体で品質管理に取り組む姿勢が重要である。

これは、製造業の品質管理について歴史的に海外に比して一日の長がある日本企業にとっては必ずしも苦手なことではない。これまで日本の工業製品が世界から信頼を得てきたように、それと同等の品質を、個人情報保護に強い日本のサービスとして展開する発想を持つことが重要である。 ■

データ保護からプライバシー保護へ
―パーソナルデータ活用の前提となる行動規範―

個人情報保護法改正の方向性を示す「パーソナルデータの利活用に関する制度改正大綱」が発表された。「大綱」は、これまでの形式的な「データ保護」から、個人への実質的な影響を重視する「プライバシー保護」へ向けた一歩を踏み出している。本稿では、「大綱」の概要と、プライバシー保護の枠組みとしての国際規格を紹介する。

パーソナルデータの活用に向けた検討

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）は、2013年12月20日に「パーソナルデータの利活用に関する見直し方針（案）」を発表した。これは、いわゆるアベノミクスの３本目の矢である成長戦略の１つとして、パーソナルデータ活用の重要性と、そのための制度見直しを訴えるものである。

具体的には３つの方向性を打ち出している。第１に挙げられたのが「ビッグデータ時代におけるパーソナルデータ利活用に向けた見直し」で、「個人データを加工して個人が特定される可能性を低減したデータに関し（中略）第三者提供における本人の同意を要しない類型、当該類型に属するデータを取り扱う事業者（提供者及び受領者）が負うべき義務等について、所要の法的措置を講ずる」としている。これは、一定の条件の下で本人の同意がなくてもデータの活用を可能とするべく制度を見直そうということである。

これを受けて、IT総合戦略本部に設置された「パーソナルデータに関する検討会」では、「準個人情報」と「個人特定性軽減データ」（いずれも仮称）を定義し、後者については同意がなくても流通できるようにしようという検討が開始された。なお「準個人情報」とは、個人が特定されていないものの特定される恐れのある情報、「個人特定性軽減データ」とは、個人が特定される蓋然（がいぜん）性が低くなるようにデータを加工して個人の特定を困難にしたものである。いずれも、個人情報でも非個人情報でもない「グレーゾーン情報」として定義し、取り扱い義務の内容を変更しようというわけである。

だがこのアプローチは委員からも、民間からの意見を通じても多くの批判を受けることになる。検討会でも、検討が始まって４回目の５月20日に行われた第９回会合あたりから、データを分類しそれに基づいて法規制を行う「データ種類別規制」一辺倒から、（これから始める）データの活用がどのようにプライバシーに影響を及ぼすかを勘案して事例ごとに扱いを決めていく「行為規制」（事業者の行為に対する規制）を取り入れる方向へ変わったように思われる。

制度改正に向けた「大綱」の決定

こうした検討を経て、法案作成の指針を示

野村総合研究所
IT基盤イノベーション事業本部
オープンソースソリューション推進室
上席研究員
崎村夏彦（さきむらなつひこ）
専門はID管理・プライバシー技術に関する国際標準化

した「パーソナルデータの利活用に関する制度改正大綱」が2014年6月24日に決定された。そこでは、制度改正に当たって以下の4つの課題が挙げられている。

①法解釈や事業者ルールの曖昧さが生じさせているグレーゾーンを解消して「利活用の壁」を取り払うこと。同時に、個人の権利利益の侵害を未然に防止すること。
②法律で定めるべき範囲と政省令や規則、ガイドラインなどで対応すべき範囲を分けるとともに、機動的な対応のための民間の自主的な取り組みを促進すること。
③確実な制度執行（公平な執行主体、公的機関による認定や普及啓発など）を担保すること。
④国際的に調和の取れた制度にすること。

そして、これらの課題を解決するための枠組みとして「本人の同意がなくてもデータの利活用を可能とする枠組みの導入等」「基本的な制度の枠組みとこれを補完する民間の自主的な取組の活用」「第三者機関の体制整備等による実効性ある制度執行の確保」を挙げている。以下、これを簡単に解説していこう。

(1)本人同意なしでのデータの活用

これは上記の1つ目の課題に対応するもので、「大綱」では「現行法の規律に加え、新たに一定の規律の下で原則として本人の同意が求められる第三者提供等を本人の同意がなくても行うことを可能とする枠組みを導入する」とし、具体的には「個人データ等から個人の特定性を低減したデータへの加工と、本人の同意の代わりとしての取扱いに関する規律を定める」としている。すなわち、現行法の本人同意原則をベースとして、その上でプライバシー侵害の実質的大きさを見積もり、所定の条件を満たした場合には同意原則の例外として扱おうということである。

このような枠組みは珍しいものではなく、英国の「データ保護法」でも、個人の同意がなくても個人データの活用が認められる5つのケースを定めている。

米国においては、連邦取引委員会（FTC）が2012年3月に公表した報告書の中で、企業が消費者のデータを利用する際の3つの条件（「FTC3要件」と呼ばれる）を挙げている（FTC「急速に変化する時代における消費者プライバシーの保護」）。

①当該企業は、データを合理的に非識別化（de-identify）するための措置を取ること。
②当該企業は、そのデータを再識別化（re-identify）しないことを公に約束すること。
③委託先・第三者にかかわらず、そのデータの移転を受ける者が再識別化することを当該企業が契約で禁止すること。

ここで重要なのは、「非識別化」は技術的対策というよりも、条件②および③を記述するための準備であるということだ。重要なのは条件②および③で、当該企業とデータを受け取る企業に「再識別しない」と宣言させること、すなわち「個人のプライバシーを侵害

するようなことはしない」と宣言させることが重要なのである。米国の場合、いったんこのように宣言すると、それに背くことをした場合にはFTC法第５条によって取り締まりの対象になる。そういう意味で、「FTC３要件」はプライバシー保護のための行為規制であり、データの種類による規制ではないことに注意する必要がある。

(2)基本的な制度の枠組みと自主的な取り組みの活用

プライバシー侵害のリスクの大きさは、人々のプライバシーに対する考え方や攻撃手法の巧妙化などによって変わっていく。そのため、プライバシー侵害を防ぐ手法に至るまで事前に法律で規定することは不可能である。従って、前述した「大綱」が挙げる２つ目の課題で示されているように、要件や執行体制などの大枠を法律で規定して、具体的内容は政省令や規則、ガイドラインなどで機動的に決めていく形にならざるを得ない。

また、制度の趣旨に則して「本人同意なしの利用」を考えるのであれば、それによって本人ないし社会が得られる利益が、プライバシー侵害による損失を上回ることを検証しなければならない。そのためには、当該業務に対する深い知識を基にケースバイケースで吟味することが必要で、業界ごとの検討が必要になる。「大綱」ではこれを「消費者等も参画するマルチステークホルダープロセス」によって実現するとしている。

(3)実効性ある制度執行の確保

制度や枠組みを考える際に重要なことは、それらの外側で何かをしようとする「悪者」にどう対処するかということである。「大綱」が挙げる３つ目の課題はこうしたことを指している。この課題を解決しないと、不良事業者の存在が優良な事業者の負担を大きくしてしまい、その結果「悪貨が良貨を駆逐する」ことになってしまう。

「大綱」ではこの対策として、現行の「特定個人情報保護委員会」を改組して、第三者機関として「パーソナルデータの保護及び利活用をバランスよく推進することを目的とする委員会」を設置し、立ち入り検査などの機能・権限を与えるとしている。

「プライバシーフレームワーク」の重要性

「大綱」が掲げる以上のような枠組みに従ってパーソナルデータの取得・利用・保持・開示をしようとした場合に、まず行わなければならないのが本人への影響を測ることである。それは具体的にはどうしたらよいだろうか。場当たり的な方策が役に立たず、全てを包括的に規定した仕組みが必要なのは自明である。それが「プライバシーフレームワーク」と呼ばれるものである。

プライバシーフレームワークは、言葉を定義し、行為者間のやり取りを整理し、プライバシーを尊重するためにはどのような原則に従い、どのような管理を行わなければならな

いかを整理するものだ。

国際標準規格としては2011年に制定された「ISO/IEC 29100 Privacy Framework」がある。ISO/IEC 29100は言葉の定義、プライバシー保護要件を定め、プライバシーリスク管理を行うことを求めている。そして、これは①法規制要因②契約要因③業務要因④本人のプライバシー選好などその他の要因－の４つの要因によって影響されるとしている。個人情報保護法といった単一の法律よりも広い範囲の考慮を求めていることに注目すべきであろう。

加えて、ISO/IEC 29100はパーソナルデータの取り扱いに関して満たすべき下記の11の原則を挙げている。

①同意と選択
②目的の正当性と規定
③収集の制限
④データ最小化
⑤利用、保持、開示の制限
⑥正確性と品質
⑦オープンさ、透明性、通知
⑧個人の参加とアクセス
⑨説明責任
⑩情報セキュリティ
⑪プライバシー法令の順守

詳細は誌面の都合で紹介できないが、ぜひ原文に当たっていただきたい。データを新しい目的で使い始める前に本人にその目的を知らせなければならないなど、何をすべきかが具体的に書かれている。ISO/IEC 29100を基本として、後続の「プライバシーアーキテクチャー（ISO/IEC 29101）」などの国際規格が生まれた。「大綱」に４つ目の課題として挙げられた「国際的に調和の取れた制度」とするためには、日本独自の規則を作るのではなく、各国の代表が集まって何年もかけて練り上げたこうした国際規格を取り入れていくべきであろう。

「プライバシー影響評価」から始める

プライバシーは、日本国憲法が規定する基本的人権の一部であり、第13条には「立法その他の国政の上で最大の尊重を必要とする」と書かれている。

従って、パーソナルデータの活用を正当化するには、まずそれが個人にどのような負の影響を与えるかを吟味し、プラスの影響がそれを上回ることを立証し、負の影響が上回ってしまう人にはどのように補償するかを決めなければならない。

このための第１ステップは、国際的に認められたプライバシーフレームワークに基づいた「プライバシー影響評価（Privacy Impact Assessment：PIA）」を行うことである。現在ISO/IECでは、PIAの手法の規格化が進行している（ISO/IEC WD 29134）。パーソナルデータの活用を目指した制度改正に当たっては、これらを参照しながら行っていくことが肝要である。 ■

プライバシー影響評価の重要な役割
―プライバシー保護とパーソナルデータ活用の両立―

「頭隠して尻隠さず」。名前や顔を分からなくするなど法令に形式的に対応するのみで、個人が隠しておきたい肝心なものを守れていないという点で、プライバシーをめぐる昨今の事件にはこのことわざがぴたりと当てはまる。本稿では、消費者への説明責任を果たし、パーソナルデータを円滑に活用するための「プライバシー影響評価」を紹介する。

なぜ非難や反発が相次ぐのか

スマートフォンやソーシャルメディアが普及し、そこから大量に生成される個人に関する情報（パーソナルデータ）を活用して、事業者は以前とは比べものにならないほどの精度で、個人の好みや未来の行動を推し量ることができる時代が到来した。

パーソナルデータには、プライバシーに該当する個人情報もあれば、そうでないデータも含まれている。2005年４月に個人情報保護法が全面施行されて以来、個人情報の保護は日本の社会の隅々にまで浸透し、誰もが個人情報は保護しなくてはならないものと理解するようになった。その一方で、データが個人情報に該当しなければどのような取り扱いをしてもいいという拙速な使い方をして消費者の非難や反発を招くケースも頻発している。また、上記のようにパーソナルデータにはプライバシーに属するのかそうでないのかが明白でない、いわゆるグレーゾーンがあることも、そうした問題の一因になっている。

そもそも、個人情報は何のために保護されなければならないのだろうか。それは、個人情報保護法の第１条に規定されているとおり、「個人の権利利益を保護すること」が目的である。そして、個人の権利利益の中心にプライバシーがある。すなわち、個人情報を保護する目的はプライバシーを守ることであり、個人情報の保護はその手段に過ぎない。しかし、従来型の個人情報保護ではプライバシーを守ることができなくなっており、それがパーソナルデータの活用に関する問題の原因なのである。今はプライバシーを守るための手段を見直さなければならない過渡期といえるだろう。

「プライバシー影響評価」とは

パーソナルデータの取り扱いを開始する前に、発生する可能性のあるプライバシー侵害リスクを評価し、そのリスクを回避・最小化する考え方を「プライバシー・バイ・デザイン（Privacy by Design）」（PbDと略記）といい、近年、世界的に注目されている。一般的なリスクマネジメントにおいても、事前対策は事後対策よりも効果的であると認識されており、その考え方をプライバシー保護分野に応用したものといえる。

PbDの考え方を、実際のプライバシー保護の業務プロセスに落とし込む代表的な手法

野村総合研究所
コンサルティング事業本部
ICT・メディア産業コンサルティング部
上級コンサルタント
小林慎太郎（こばやししんたろう）
専門はICT公共政策・経営

が「プライバシー影響評価（Privacy Impact Assessment：PIA）」である。

PIAそのものはそれほど新しい取り組みではない。すでに1990年代後半から米国、カナダ、オーストラリアなどでは、行政機関が個人情報を取り扱う情報システムを開発する場合に実施されてきた。しかし、PIAの実施方法は国によってさまざまであり、確立された方法はこれまでなかった。また対象は行政機関のみで、民間事業者には直接関係のないものであったため、これまでPIAはあまり普及してこなかった。

しかし、EU（欧州連合）が新しいプライバシー保護ルールである「EUデータ保護規則（案）」にPIAを取り入れたことで、一気に普及が加速する様相を見せている。同案において、一定の条件に当てはまるパーソナルデータを取り扱う行政機関・民間事業者に対して、PIAの実施を義務づけることになったからである。特に民間事業者におけるPIA義務化は世界で初めてとなる。なお、「EUデータ保護規則（案）」では、データ保護影響評価（Data Protection Impact Assessment：DPIA）と呼称しているが、意味するものはPIAと違わない。

日本においても、「社会保障・税の番号制度」（マイナンバー制度）において、「特定個人情報保護評価」という呼称でPIAが行政機関に義務づけられ、すでに運用が開始されている。さらに「パーソナルデータの利活用に関する制度改正大綱」（2014年6月24日IT総合戦略本部決定）ではPIAが継続検討事項となっており、今後検討が深められる見込みである。

PIAの実施手順

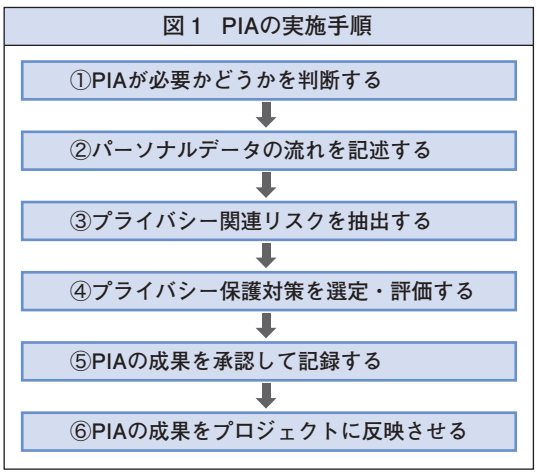
いまだ確立された標準的な方法はないものの、PIAはすでに多くの国で取り組まれ、実施手順の骨格は共通のものとなりつつある。国際標準化団体においても標準化が進められており、筆者もこの作業に日本から参加している。

ここでは、イギリスの第三者機関であるICO（Information Commissioner's Office：情報コミッショナー局）が定めたガイドライン「Conducting privacy impact assessments code of practice」（2014年2月25日公表）に基づいて、個人情報・プライバシー保護に関する筆者のコンサルティング経験や標準化作業の知見を踏まえ、PIAの実施手順の概要を紹介する。

ICOのガイドラインでは、PIAの実施手順を6つのステップに分けている（次ページの図1参照）。以下で順に見ていこう。

①PIAが必要かどうかを判断する

PIAを実施する必要があるのか、実施する場合は、どの程度の規模で実施すればよいのか、最初の段階でふるい分ける。パーソナルデータを取り扱う事案は多く、全てを対象に厳格なPIAを実施することは現実的ではなく



非効率でもあるからである。「予備評価」「しきい値判断（マイナンバー制度の「特定個人情報保護評価」における呼称）」などと呼ばれる。

②パーソナルデータの流れを記述する

このステップでは、誰が、誰から、何のパーソナルデータをどのように取得・利用し、誰と共有し誰に提供するのかといった基本的なデータの流れを整理し、さらにデータフロー図や業務フロー図などを用いてデータの流れを可視化する。この成果は、後続のステップであるリスク抽出のための基礎資料となる。また、データの取得から廃棄までの一連の流れを記述し、データのライフサイクル全般での保護を検討するための資料とする。

③プライバシー関連リスクを抽出する

パーソナルデータの流れが整理できたら、それを基にプライバシー関連リスクを抽出し、その影響を評価する。プライバシーの分野では、特定の領域を除いて、汎用的なリスク参照モデルはいまだ確立されていない。これは、プライバシー保護が比較的新しい分野であり、またパーソナルデータをどのような目的や状況で活用するかに依存する部分が大きいために、一般化できる部分が限られているからである。このため、「OECD（経済協力開発機構）８原則」（OECD理事会で1980年９月23日に採択された「プライバシー保護と個人データの国際流通についての勧告」に記された８つの原則）や「ISO/IEC 29100 Privacy Framework」といったプラバシー保護のフレームワークを用いて、先に整理したデータの流れに沿ってリスクの洗い出し作業を行う。

④プライバシー保護対策を選定・評価する

リスクを抽出した後は、それらがどのくらい影響があるか、発生確率はどの程度あるかを分析し、リスクに応じた対策を講じる。これは、リスクマネジメントにおける一般的なリスク評価手法と同じ考え方に基づいている。すなわち、PIAにおいても一般のリスクマネジメントと同じく、リスクは完全に排除するのではなく、リスクの影響度や発生確率を許容できるレベルにまで低減することを目的に対策を選定することになる。

⑤PIAの成果を承認して記録する

このステップでは、PIAの実施結果として、パーソナルデータの取り扱い、プライバシーリスク、リスクへの対策をレポートにまとめ、プロジェクトの実施責任者やプロジェク

トオーナーによる承認を得る。

先進諸外国の事例を見ると、公的機関の場合、PIAのレポートやその概要を公開することが一般に行われている。民間事業者では営業秘密やセキュリティを理由に、自発的にPIAレポートを公開することはあまりない。ただし、プライバシー保護当局から照会があった際に迅速に開示できるようにレポートを準備しておく事業者もある。

⑥PIAの成果をプロジェクトに反映させる

最後のステップは、PIAの実施結果を確実にプロジェクトに反映させることである。前述したとおり、PbDの思想に基づくPIAでは、事前にリスクへ対処することが目的であるため、サービスや情報システムの設計にPIAの結果を取り込めるタイミングである概念設計が終了するまでの間に行う。

本質はステークホルダー間の合意形成

プライバシー保護に対する意識は個人差が大きい。そのため、多くの消費者がメリットを認めてパーソナルデータの利用を容認する場合であっても、社会的な影響力を持つ企業や公的機関では、保護意識の強い一部の消費者の要求に合わせてデータの利用を控えたり、オプトイン（事前に許可を取ること）で本人同意を得られた場合のみ利用したりする傾向が見られ、パーソナルデータを活用したビジネスに踏み出せない企業もある。PIAは、こうした状況を打開する手段としても期待される。

例えば、行動ターゲティングを活用した新たなサービスを提供するためにパーソナルデータの利用が必要になったとする。このとき、サービス利用者から個別に同意を取得するか、オプトアウト方式（事前に利用者の明示的な同意を取得せずに個人情報を利用し、本人からの求めがあった場合に個人情報の利用を停止するやり方）にするかが問題となっているとする。この場合に、PIAの一環として、サービス利用者へのアンケートやヒアリングを通じてデータ利用に対する受容性を評価し、その結果に基づいて分かりやすい同意取得のインターフェースを開発して簡便にオプトアウト（利用停止の手続き）ができる方法を提供する、といったリスクの回避・軽減措置をステークホルダー（利害関係者）を集めて協議するのである。

このように、PIAは、ステークホルダーとの協議を通じてデータ活用の便益とプライバシー保護とのバランスを追求し、全体最適を求めるプロセスとして有効であり、PIAの実施は説明責任を果たすことになる。

PIAは発展途上にあり、今後もPIAの手法を洗練させる試みが各所で行われると思われる。PIAを義務づけるEUの新しいルールはその強力な追い風になるはずだ。プライバシー保護と両立するパーソナルデータ活用の道を切り開いていくために、今後PIAの役割はますます重要になるであろう。 ■

行動履歴データの活用とその課題
―利用者の理解と信頼を得るための方策とは―

企業のビッグデータ活用に際してプライバシー保護はどこまで必要かといった悩みをよく耳にする。特に、位置履歴や購買履歴のように個人の行動を把握できる行動履歴データは最も扱いが難しい情報の１つである。本稿では、この問題にどのように対応していくべきか、個人情報保護法改正の動向を踏まえて考察する。

ビッグデータ活用とプライバシー保護

ビッグデータを分析して、これまでは分からなかったことを発見し、新しい価値を生み出そうという取り組みが多くの企業によって行われている。その一方で、ビッグデータの中でも価値が高いと期待される、個人の位置履歴や購買履歴といったパーソナルデータの活用が、プライバシー上の問題があるとして社会的な批判を受ける事例が数多く発生している。パーソナルデータを活用したい企業にとって、どこまでのプライバシー保護策を講じるべきかが実務上の大きな悩みの１つとなっている。

もちろん、プライバシーの問題は以前から存在している。しかし近年は、SNS（ソーシャルネットワーキングサービス）やスマートフォンの普及によって、個人から取得できる情報の量が格段に増し、個人の行動や趣味、好みなどを知ることも以前よりはるかに容易である。例えば、利用者からGPS（全地球測位システム）によって情報を取得して地図アプリを提供する事業者が、自社で保有する利用者の位置情報と、FacebookやTwitterへの投稿時の位置情報を照合して、それが誰であるかを特定することも可能である。地図アプリのGPSの位置情報からは、個人の詳細な行動を長期間にわたって把握することが可能であるため、いったん個人が特定されると、利用者にとって知られたくない行動が第三者に知られてしまうリスクがある。

地図アプリから得られた位置情報は、名前や住所といった個人を直接特定できる情報が入っていないため、事業者によっては個人情報として扱わず、第三者に販売することも可能性としてあり得る。事業者はそんなことはしないと言うかもしれないが、利用者は自分の詳細な情報がどこかに売られるのではないかという不安を感じている。2011年には、スマートフォンから利用者の知らないところで定期的に位置情報が送信されていたことが報道され、Apple社やGoogle社がプライバシーを侵害していると非難されたが、このケースも、自分の情報の使われ方を利用者がいかに不安視しているかを示すものである。

こうしたことが起きる原因として、利用者が期待するプライバシー保護と、事業者の考えるプライバシー保護との間に大きなギャップがあることが考えられる。事業者の側では、「法律に違反していない」「利用者に実害

野村総合研究所
IT基盤イノベーション事業本部
ビッグデータビジネス推進室
上級コンサルタント
島　次志（しまつぐし）
専門はIT分野における調査・コンサルティング

表1　位置情報を取得する際に電気通信事業者が実施すべき対応

項目	内容
同意	位置情報の高いプライバシー性を踏まえ、原則として、その提供するサービスごとに、位置情報の取得・利用・第三者提供について、個別かつ明確に利用者の同意を得ることが必要である。
説明事項	同意を取得する前に、利用者から位置情報を取得されることに伴うプライバシー上のリスクについて利用者が理解できるように分かりやすく、容易参照できる場所に説明・表示を行うべきである。 説明事項：取得者、位置情報の種類（基地局情報、GPS位置情報、Wi-Fi位置情報等）、精度・取得頻度・追跡期間、利用目的、第三者提供の有無およびその提供先、保存期間、位置情報にひも付けて利用される他の利用者情報、利用者関与の仕組み　等
説明・表示の推奨方法	利用者が内容を理解した上で同意するためには、位置情報の種類、利用目的、第三者提供の有無といった特に重要な点について、概要として説明・表示し、詳細については別途誘導して説明する等の対応が推奨される。
同意内容の事後的変更	位置情報取得等の取り扱いでは、利用者が事後的に同意内容を変更できる（設定変更できる）機能が設けられることを原則とすべきである。

出所）総務省「位置情報プライバシー レポート～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～（案）」に基づき作成

はない」「利用者にとってもメリットがある」と考え、利用者の不信を買うかもしれないという観点からの評価を客観的かつ適切に行わなかった可能性がある。

以上のように、パーソナルデータを含むビッグデータの活用が進んできている状況においては、現行の個人情報保護法に対応して行われているプライバシー保護のレベルでは不十分だという声が高まっている。

データ活用の前提として必要なもの

今やビッグデータブームといえるような状況のなかで、行動履歴データ活用の議論も活発になっている。しかし、プライバシー保護の対策をどこまで実施すべきかの明確な基準がないため、冒頭でも述べたように企業の担当者は頭を悩ませているのが実情であろう。それでは、どうすればデータ活用とプライバシー保護を両立させることができるだろうか。

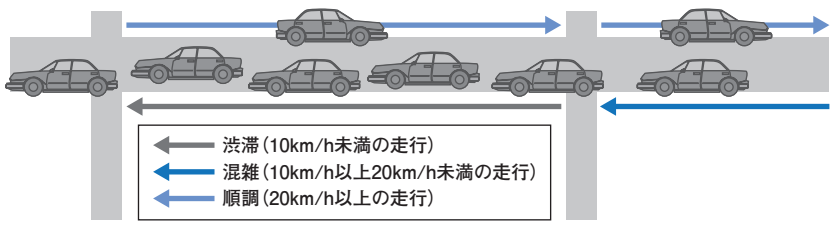
2014年5月に、総務省の「緊急時等における位置情報の取扱いに関する検討会」が「位置情報プライバシーレポート～位置情報に関するプライバシーの適切な保護と社会的利活用の両立に向けて～（案）」を公表した。表1は、このレポート中の「位置情報の取扱の在り方について」に記された、電気通信事業者に求められる対応を抜粋したものである。

簡単にいうと、利用者にとって分かりやすく、理解が得られるような方法で説明し同意を取得することがポイントとなる。一見、簡単そうだが、多くのケースで行われているような、長い文章で規約を示すやり方はほぼ否定されている。デザインや画面フローを含めて抜本的な見直しを行い、同意項目ごとに同意内容を変更する機能を実装することが必要である。

レポートには総務省情報通信政策研究所による「位置情報の利用に対する意識調査」の

結果も示されている。「広告マーケティングやサービス向上」に活用することは、半数近くの人が「どんな場合でも許容できない」と回答していることから、利用者の同意なく位置情報を広告マーケティングに活用すると大きな批判を招くことになりかねない。

図１　プローブデータを使った道路交通情報生成のイメージ



特定のドライバーの特異な行動を捉えないようにするため、複数の車両から情報を取得できる場合にのみ、交通情報の生成に利用する。また、プライバシーに配慮して主要幹線道路に限って情報を提供する場合がある（生活エリア内の道路の場合、走行する人が限定的である可能性があるため）。

明示的な同意なく位置情報を活用しているサービスの事例は、NTTドコモの有料サービス「モバイル空間統計」などいくつか存在する。しかし、それらはマスマーケティング以外では活用できないレベルに統計化したデータを使用するもので、プライバシーに配慮して個人を特定することはできないようになっている。プライバシーに配慮しつつ個々人の行動履歴をより詳細に取得して利用しようとすれば、分かりやすい説明をした上で１人１人から明示的な同意を得る以外にないというのが実情であるが、その際、利用者のメリットをうまく伝えることができないと、同意を得ることは難しい。

パーソナルデータ活用の成功事例

パーソナルデータ活用をサービスとして実用化している数少ない事例が、通信機能付きカーナビから取得できるプローブ情報（車のGPSの位置情報）を利用して道路交通情報を生成しドライバーに提供するサービスである（図１参照）。

GPS情報の取得自体はカーナビの利用にとって必須であるため、カーナビを利用する時点で同意が取れているといえるであろう。交通情報の生成にプローブ情報を利用することについては別途、同意が必要となるが、プローブ情報の提供により精度の高い交通情報を得ることができ、かつ他のドライバーの役に立つことにもなるので多くの人に同意してもらいやすい。また、交通情報を普段から利用していることで、同意していることを認識してもらいやすいというメリットもある。

このサービスは、複数の車両からGPS情報を取得して車の平均速度を計算し、その速度に応じて地図上の道路に「渋滞」「混雑」「順調」といった線を描くことによって道路交通情報を提供している。その車両が誰のものかということは分からないようになっており、事業者はプライバシー侵害を心配せずにパー

ソナルデータを活用したサービスを開発、提供することが可能となる。

これに対して広告分野では、誰が何をしているか、何を求めているかということが分かれば分かるほど、より広告の価値を高められるといわれる。しかし利用者からすれば、自分の行動が知られれば知られるほど、気持ちが悪いと考える人の割合が増えてくる。また、道路交通情報のようなデータ加工方法で一律にプライバシーに配慮することが難しく、どこまでであれば許容されるのかという基準を明確にしにくいこともあって、企業が踏み込みにくい分野になっている。

事業者と利用者のギャップを埋めるために

現在、2015年の通常国会への法案提出が目指されている個人情報保護法の改正をめぐって、プライバシーに配慮しつつパーソナルデータを活用できるようにするための方策についても議論されている。本稿執筆時点の2014年6月には大綱（「パーソナルデータの利活用に関する制度改正大綱」）が決定・公開されたが、購買履歴、移動履歴といった個人の特徴的な動きを把握できるデータの扱いについては、難しいテーマであるため引き続き検討されることになっている。

有力な案として出されているのは、業界の自主ルールの活用である。業界やサービスによってプライバシー保護の考え方や方法が異なるため、利用者の理解が得られやすいよう業界やサービスごとにルールを定めようというのである。これにより、匿名化によってデータの価値を低下させることなく行動履歴データをビジネスに活用できるのではないかと期待されている。

しかし、業界の自主ルールは利用者の理解を得ることが前提である。そのため、業界の意向を先行させるのではなく、利用者の意見を十分に取り入れ、第三者機関の認証・監査といった影響力の下で機能すること、すなわちプライバシーに関する「トラストフレームワーク」（信頼を醸成するための枠組み）に基づいたものであることが必要である。業界の自主ルールを守ると宣言し、かつルールを順守しているか定期的にチェックされている事業者であれば自分の情報を分析され利用されてもよいと考える人は増えると思われる。

業界の自主ルール以外にも、利用者の理解を得るために事業者にできることがある。利用者の理解を得るためには、データ提供によるメリットを示すことも有効な方法の1つである。利用者の信頼を醸成するために、得られたデータでどのような価値を創り出すことができるかを利用者や社会に示す活動を継続的に行っていくべきである。しかし、現状では利用者や社会にデータ活用のメリットを訴求できているケースは少ない。今後、これらの活動によって事業者と利用者のギャップを埋めていくことがデータ活用の拡大のために重要になっていくであろう。 ■

「走るセンサー」化する自動車
―パーソナルデータを活用した自動車サービスの課題―

スマートフォン、ウェアラブル端末、スマート家電など、利用者個人に寄り添い日常生活を便利にする最新機器はさまざまなセンサーを組み込んでいる。本稿では、そこから得られるパーソナルデータを活用した便利なサービスの提供とプライバシー保護はいかにして両立するのか、最新の自動車サービスを例にその課題と対策について考察する。

広がりを見せる自動車サービス

夢の技術として実用化が目指されている自動運転。その実現は、これまで人間が感じ、対処してきたさまざまな情報を機械がセンシングすることが前提である。すなわち、自動車がセンサーによって人間の目となり耳となり手となることを意味するのだ。事業者は、LTE（Long Term Evolution。携帯電話の新しい高速通信規格）などの通信技術の向上により、センサーデータを低コストで大量に収集することができるようになってきており、データ活用の巧拙が競争力を左右する状況となっている。

すでに自動車メーカーでは、トヨタ自動車の「G-BOOK」や本田技研工業の「インターナビ」のように、プローブ交通情報（実際に走行している自動車から得た位置や車速を基に生成された交通情報）を利用したカーナビゲーションサービスを提供している。「インターナビ」では、会員から収集した自動車の位置情報から、これまでVICS（Vehicle Information and Communication System。主要道路に設置したセンサーのデータを活用したリアルタイムの交通情報提供サービス）では捕捉できなかった細かい道路の情報も含めて、今どこで渋滞が起きているのかをリアルタイムに分析し、利用者に道路交通情報として提供している。パイオニアでは自社のカーナビにカメラを取り付け、リアルタイムにアップロードされる画像を基に車線ごとの混雑情報を提供するなど、利便性の高いナビゲーションサービスを提供しようとしている。

近年では、スマートフォンの普及に伴って携帯電話のデータ定額プランに加入する利用者が増えているため、カーナビとの通信を利用者個人の携帯電話を介して行うことにより、事業者はコストをかけずにデータを収集することが可能である。

このようにデータ収集のための環境が整うことにより、自動車に関するさまざまな事業者が、自動車を「走るセンサー」と捉え、そのデータの活用にビジネスチャンスを見いだそうとしている（表1参照）。

データ活用によるサービスの拡がり

現在、注目されている自動車のデータとしてCAN（Controller Area Network）データがある。CANとは自動車の内部で各機器をつなぐネットワークの規格であり、機器の状

野村総合研究所
コンサルティング事業本部
ICT・メディア産業コンサルティング部
コンサルタント
山崎浩平（やまざきこうへい）
専門は情報通信・放送メディア分野の事業戦略・マーケティング戦略

態を通信し合うことで、自動車内の各機器が制御されている。CANデータからは、エンジンの回転数、アクセルやブレーキの動作に加え、ワイパーの動きやウインカーの利用に至るまで、自動車の動作に関するあらゆる情報を入手することが可能である。

CANデータのように従来から自動車内に存在していたデータに加え、新たに自動車からデータを収集する動きも出てきている。例えば、シートにセンサーを内蔵することによってドライバーの心臓の鼓動を捉え、ドライバーが眠気を感じているかなどを把握して警告するサービスも始まっている。

まずは、これらのデータがどんなサービスを可能にするか考えてみよう。

(1) CANデータの活用

CANデータからはアクセルやブレーキの動作、ハンドル操作の様子などが入手でき、それらを解析することによってドライバーがどんな運転の仕方をしているかを把握することができる。このデータを自動車保険に利用すれば、安全運転をするドライバーに保険料を安くしたり、運転の仕方によって保険金の支払いを決めたりすることが可能である。実際に米国の大手自動車保険会社Progressive社では、加入者の自動車にCANデータを取得する端末を取り付け、急ブレーキの回数などを保険料に反映させる「Snapshot」と呼ばれるサービスを2010年から提供している。日本では、損保ジャパンが日産自動車の電気自動車「リーフ」から収集したデータを基に、走行距離に応じた保険サービス「ドラログ」を提供している。電気自動車は価格が高く保険料も高くなりがちだが、走行距離が短い人にとっては保険料が安くなるというメリットがある。

表1　センサーで取得可能な自動車のデータの例

センサー	取得可能なデータ
CAN	アクセルやブレーキの挙動、燃費、走行距離など
車載カメラ	周辺の映像・動画、車内の映像・動画
シートセンサー	ドライバーの心拍数
GPS	自動車の位置情報

また、CANデータは自動車内部の機器の状態を表しているため、ディーラーがエンジンオイルの交換時期のお知らせや修理のお勧めなど、自動車の状態に合わせたサービスを提供することも可能となる。

(2) 車載カメラの活用

近年は、テレビのニュースなどで生々しい自動車事故の画像や映像が紹介されることがある。それらは自動車に取り付けられた車載カメラが撮影したもので、交通事故の際の過失の有無を示す証拠として利用するため、法人車両をはじめ車載カメラを搭載する自動車は増加している。先に挙げたパイオニアの例のように、車載カメラの画像をリアルタイムで送信して利用することにより、道路状況を把握し、詳細な交通情報を生成することができる。また、急ブレーキが多い地点における車載カメラの画像を分析することによって、

子供の飛び出しが多い地点を把握したりすることも可能である。

(3) シートセンサーの活用

前述のように、シートセンサーによってドライバーの心拍数などを検知し、体調や眠気の状態を把握することができる。これを運送業者が利用すれば、眠気を感じやすいドライバーを把握したり、眠気が起きやすい運行ルートや時間帯を特定したりすることが可能となり、事故を未然に防げる可能性が高くなる。ドライバー自身も、継続して運転に集中できる時間の長さを把握するなど、自己管理を適切に行うことが可能となる。工業用ミシン大手のJUKIは、シートセンサーを用いた居眠り運転警告装置「スリープバスター」を2012年より発売している。

センサーデータ活用の課題と対応

このように、自動車から取得できる情報を活用したサービスは、事故の予防や修理コストの削減など大きな可能性を持っている。しかし、自動車に限らずセンサーから収集したデータは利用者個人と結び付いた情報であり、その人が思っていなかった利用の仕方をすると反発を招くこともある。こうしたリスクの把握と事前の対応は、これまでなかったような新しいサービスの提供に当たって大きな課題となる。例えば、Google社のGoogle Glass（眼鏡型のウェアラブル端末）の場合、顔認証機能を利用したサービスの開発・提供を禁止している。技術的には、目の前の人の顔認証データを他のパーソナルデータと照合して、その人が誰であるかを特定することは可能だが、Google社はこのような技術を利用したサービスがプライバシーを侵害することを懸念しているのである。

以下では、自動車メーカーが利用者からCANデータを取得する場合に考えられるプライバシーの課題とその対応について、サービスの各段階ごとに解説する（図1参照）。

(1) データの取得

自動車の位置情報やドライバーの運転特性は、個人にひも付くパーソナルデータである。それらのデータの取得は利用者の同意の上で行われなければならず、事業者はあらかじめ利用者にサービス内容を通知し同意を取得する必要がある。近年ではインターネットサービスを中心に、利用規約の分かりにくさ、利用者同意の形がい化が指摘されている。利用者にとって分かりやすい説明と、実効的な同意取得方法の提供が求められる。

サービスは使ってみないとそのメリットやデメリットが分かりにくいことが多く、サービス利用に同意したことを後悔する利用者も少なからず存在する。そのため、一度同意した利用者がサービスの利用を取りやめるオプトアウトの仕組みをサービスのWebサイトに実装しておくことも非常に重要である。

(2) データの利用

データの利用においては、事業者のデータ

図１　利用者のデータを使ったサービスにおけるプライバシーの課題と対策

	取得	利用	消去
サービス事例（自動車メーカーによるCANデータの取得と活用）	事前に利用者からデータ提供の同意を取得 CANデータを自社のサーバーに送信	自社の自動車開発に利用 保険会社に提供し自動車保険に利用 ユーザーに提供しCRM（顧客関係管理）に利用	サーバーからデータを消去
プライバシーリスク	利用者の同意の形がい化	目的外利用（利用者が想定していない、コンテキストに沿わない利用）	データの漏えい データの安全性の低下
対策	明確で分かりやすい説明・同意取得 利用者が自らサービスをやめられるオプトアウトの仕組み	利用者へのデータのフィードバック	データ保存期間の明示 データ削除が可能なシステム設計

利用の仕方をサービスの利用者が不自然に感じないこと、すなわちサービスの内容に則したデータ利用を行うことが重要である。JR東日本がSuicaの乗降履歴を外部の企業に販売して問題となったことは記憶に新しいが、その原因の１つとして、「まさか自分のデータが売られているとは思わなかった」という驚きが挙げられる。データの外部提供に納得してもらう手段の１つとして有効なのが、データのフィードバックである。前述の「ドラレコ」では、保険会社によって利用者に「エコドライブ」の点数が付けられる。自らのデータが取得されていることを常に意識してもらうことによって、利用者の反発を受けずにデータを活用することが容易になるだろう。

(3)データの消去

取得したデータの中には、時間が経過したことで意味がなくなっているものもある。そうしたデータをメンテナンスせずに使い続けることは、分析結果の信頼性を低下させるリスクがある。プライバシーを守る上では、データを提供したユーザーについて誤った分析をしないために、データの保存期間を適切に設定することも大切である。

事前対策を業務に根付かせる

パーソナルデータを活用したサービスには、さまざまなプライバシーリスクが潜んでいる。データの上手な活用は経験知であり、いったん消費者の信用を失ってデータ活用が止まってしまうと、それが致命的な遅れとなることも考えられる。「何か」があってからでは遅いのである。自由なサービスの発想とプライバシーへの配慮を両立させるために、プライバシーリスクを最小化するための「プライバシー影響評価（PIA）」など、事前対策の手法を仕組みとして業務に根付かせることが必要である。■

パーソナルデータのさらなる活用に向けて
―プローブデータを活用したサービスの動向―

パーソナルデータの活用に当たってプライバシーへの配慮は欠かせないが、それがサービス利用者にとっての利便性を低下させることもある。本稿では、自動車などから収集されるプローブデータを活用したサービスの事例を紹介し、プライバシーを保護しつつパーソナルデータの活用を拡大させるために必要な条件について考察する。

用途が拡大するプローブデータ

プローブデータとは、GPS（全地球測位システム）の発信機を搭載した自動車などから得られる移動軌跡情報のことである。現在は携帯電話もGPS発信機を搭載しているので、プローブデータを収集することは容易である。プローブデータは、移動体を識別するID、データの取得日時、緯度・経度の３つを基本項目とするシンプルなデータであるが、自動車の走行履歴として分析することでさまざまな活用が行われている。

プローブデータを活用した道路交通情報サービスは、トヨタ自動車、日産自動車、本田技研工業といった自動車メーカーや、パイオニアなどのカーナビメーカーからテレマティクスサービス（移動体通信システムを利用したサービス）として提供されている。また、プローブデータを分析して急ブレーキが多い地点を把握し、道路の問題点を改善するといった道路行政に活用したり、プローブデータから走行距離を把握して自動車保険の保険料を算定したりすることも行われている。

このようにプローブデータの用途は拡大しており、今後、プローブデータがますます必要とされることは間違いない。

野村総合研究所（NRI）でも、スマートフォン向けのナビゲーションサービス「全力案内！ナビ」（2013年11月にサービスを終了）の提供に当たり、プローブデータを使って道路交通情報を生成し利用者に提供してきた。

このサービスは、全国の政令指定都市を中心とした合計約11,000台（そのうちの約７千台は東京都内）の契約タクシー会社の車両と、位置情報の提供に同意したサービス利用者から得られるプローブデータを用いて自動車の走行スピードを算出し、渋滞している道やすいている道といった道路状況を把握し、渋滞情報や目的地への最短経路の情報をルート情報に加えて提供していた。プローブデータを活用することにより、自動車が通行する全ての道路の状況を把握できるため、VICS（Vihicle Information and Communication System）のように高速道路と主要幹線道路のみに設置された固定的なセンサーから得られる情報と比べてはるかに多くの道路をルート案内の対象とすることができた。

災害時のプローブデータ活用

プローブデータは、東日本大震災時の通行

野村総合研究所
IT基盤イノベーション事業本部
ビッグデータビジネス推進室
主任システムコンサルタント
北村雄騎（きたむらゆうき）
専門は情報通信分野の技術開発・コンサルティング

可能道路に関する情報の提供にも活用された。図1は、2011年3月19日からNRIのグループ会社ユビークリンク（当時）のWebサイトで提供されていた「通れた道路マップ」の一例である。3月12日以降に自動車の通行が可能であった道路の累積情報と、直近の過去3日間に通行できた道路が色分けされて表示されていた。このような災害時の情報提供は、走行する自動車そのものをセンサー化するプローブデータでなくては実現が困難であったといえよう。

震災時には、同じく通行可能な道路を示す「Google Crisis Response 自動車通行実績情報マップ」も提供された。これは、本田技研工業、パイオニア、トヨタ自動車、日産自動車の4社のデータを特定非営利活動法人ITS-Japanが集約したものである（当初は本田技研工業の「通行可能道路実績マップ」を利用）。4社の情報が統合されることで、情報の精度やカバー範囲は飛躍的に高まったといわれている。

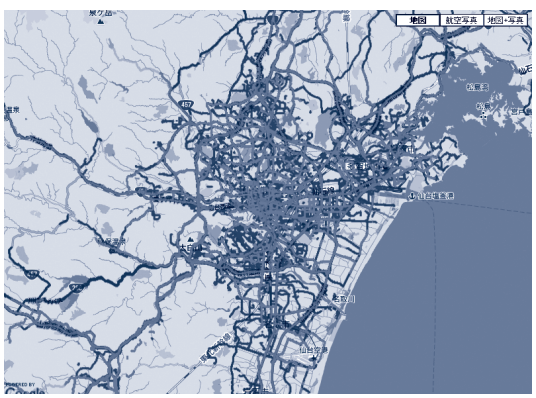


図1「通れた道路マップ」で表示された道路の状況

最近のプローブデータ活用事例

現在、市場ではさまざまな事業者がプローブデータを収集・分析してサービスを提供している。

(1) 国内の事例

次ページの表1は、プローブデータを活用した主なサービスをまとめたものである。冒頭に述べた基本的なデータ（ID、取得日時、緯度・経度）に加え、さまざまなセンサーから得られる情報が付加されたプローブデータを収集・分析することで、利用者にとってより利便性が高く、企業にとっては業務効率化が図れるサービスが生まれている。いずれも、データの利用目的についてサービス利用者の理解が得られやすいサービスといえるだろう。

2014年6月にトヨタ自動車が発表した新しいサービス「T-Connect」では、車両情報（位置・車速・燃費など）を利用した車載アプリケーションの開発を可能とする開発環境である「TOVA（Toyota Open Vehicle Architecture）」が公開された。これにより、プローブデータを活用したサービスの高度化が見込まれるが、同時に、車両情報の活用に対する利用者の理解をどう得ていくかも注目される。

(2) 海外の事例

海外に目を向けると、プローブデータを収集・分析する事業者と、その結果をサービス

表1　プローブデータを活用したサービス

サービス	サービス概要	サービス提供事業者	データ収集源
道路交通情報の提供	プローブデータを基にした道路交通状況の可視化、カーナビやスマートフォンを通じた情報提供	トヨタ自動車、日産自動車、本田技研工業、パイオニア、ナビタイムジャパン、ゼンリン・データコム、Google	自家用車、スマートフォン
E-Call（ヘルプネット）	自動車の事故時に、現在位置や走行軌跡のデータをセンターに送信し、速やかに救助機関と連携	トヨタ自動車、日産自動車、本田技研工業	自家用車、スマートフォン
カーシェアリング	レンタカー車両の現在位置のほか、急発進・急停止・燃料残量などを車両ごとに管理	タイムズ24	レンタカー
実走行距離連動型自動車保険	走行距離に応じて自動車保険の保険料を算出	あいおいニッセイ同和損害保険	乗用車
動態車両管理	自動車の位置情報と運転情報（燃料消費、エンジン回転数など）を専用車載機で取得し、車両管理業務を効率化	スマートバリュー	法人車両
道路パトロール	GPSなどのセンサー付き端末やスマートフォンを車両に搭載し、走行した道路の路面状況を診断	富士通	法人車両

として提供する事業者が分かれているケースが見受けられる。

米国のINRIX社は世界30カ国以上で1億台を超える車両からプローブデータを収集してリアルタイムの交通情報を事業者に提供している。海外の自動車メーカーだけでなく、日本の自動車メーカーが海外でテレマティクスサービスを行う際にも活用されている。また、イタリアのOcto Telematics社は30以上の保険会社にプローブデータを活用した自動車保険に関するソリューションを提供しており、それには車両情報を取得する専用機器やドライバーの運転特性を分析するサービスも含まれる。

この2つの事例は、いずれも広くさまざまなデータソースからプローブデータを収集・分析することで情報の価値を高めているものといえる。

プローブデータ活用時の注意点

プローブデータは特定の個人の走行履歴を示すことから、プライバシーが侵害されるリスクも有している。従ってデータの分析やサービスへの活用においてプライバシーへの配慮が欠かせないことはいうまでもない。この配慮の過程で、分析結果の精度の低下や分析手法の制限、あるいは使用できるデータの制限といった課題が発生する。

例えば、自家用車であれば、使用するプローブデータの起点や終点から、個人の自宅や通勤先といった情報が把握できてしまうことが考えられる。朝にプローブデータが発生し、どこかでデータが途絶えるという挙動が繰り返し行われれば、自宅と勤務先を高い確

度で推定することができるだろう。

こうしたことが行われないようにするためには、幹線道路などに限ってプローブデータを対象にした分析を行うといった工夫が求められるが、起点や終点付近の道路交通状況が反映されないというデメリットもあり、あらゆる道路の状況が把握可能だというプローブデータの強みが損なわれる。

また、タクシー車両の場合は、タクシーに乗っているのが誰かをプローブデータから知ることはできないが、スマートフォンなどから得られるプローブデータはサービスの利用者と結び付いた情報であり、特定の個人の移動履歴を示すものである。利用者にとっては、道路交通情報として提供される以外に、例えば特定の端末の動きを個別に分析されるといったことは、たとえ個人の特定につながらないとしても、意図した使われ方とは異なると感じられるであろう。このため、何らかの方法で同意が得られていない場合は、タクシー車両から得られるデータに限って分析を行うといった割り切りも必要になる。

さらなるデータ活用に向けて

プローブデータは、プライバシーが守られることを前提に、将来は利用者の属性情報と組み合わされ、事業者をまたいだ形での活用が進むと予想される。例えば、SNS（ソーシャルネットワーキングサービス）の利用履歴に基づいて、ナビゲーションサービスが個々人の趣味や好みに合った飲食店を推薦することも可能になるだろう。また、大規模災害の発生時に、被害の状況が把握できない、いわゆる情報空白域を発生させないために、行政側で不足する情報を事業者が提供するといった、官民の情報連携も期待される。

今後、パーソナルデータとしての活用も増えてくるプローブデータを含め、利用者の信頼を得ながらさまざまなサービスを運用するための条件として、特に以下の２点が求められる。

①サービス開始前のリスク対策

サービス提供を開始した後の対策では、利用者のプライバシー侵害リスクを回避できない恐れがある。サービス構築の段階から利用者のプライバシー保護に配慮し、かつ利用者がメリットを感じられるようなサービスを実現するための「プライバシー・バイ・デザイン」や、事前にプライバシーリスクを評価する「プライバシー影響評価（PIA）」の導入が対策として有効である。

②同意管理の仕組み

パーソナルデータを提供する側にしてみれば、自分が意図しない使い方をされないかが懸念されるが、一般にデータが適切に使用されているかどうかをデータの提供者が判断するのは難しいと考えられる。そのため、利用者個人が自分の情報をコントロールできる「プライバシーフレームワーク」といった枠組みを導入することも肝要である。 ■

NRI Web Site

NRI公式ホームページ　www.nri.com/jp

会社情報

NRIグループのCSR活動	www.nri.com/jp/csr	IR情報	www.nri.com/jp/ir

事業・ソリューション別のポータルサイト

コンサルティング	www.nri.com/jp/products/consulting	日本における先駆者として社会や産業、企業の発展に貢献してきたコンサルティングサービスを紹介
未来創発センター	www.nri.com/jp/souhatsu	アジア・日本の新しい成長戦略に関わるNRIの取り組み、研究成果の情報発信、政策提言などを紹介
金融ITソリューション	www.nri.com/jp/products/kinyu	金融・資本市場でのビジネスを戦略的にサポートするITソリューションの実績、ビジョンを紹介
NRI Financial Solution	fis.nri.co.jp	金融・資本市場に関わるNRIの取り組みについての情報発信、政策提言、ITソリューションを紹介
産業ITソリューション	www.nri.com/jp/products/sangyo	流通業やサービス業、製造業などさまざまな産業分野のお客さまに提供するソリューションを紹介
IT基盤サービス	www.nri.com/jp/products/kiban	産業分野や社会インフラを支えるシステム、システムを安全・確実に運用するためのソリューションを紹介
BizMart	www.bizmart.jp	企業間業務や生・配・販を中心とするさまざまな業種の業務効率化を支援するソリューションを紹介

サービス・ソリューション別のWebサイト

INSIGHT SIGNAL	www.is.nri.co.jp	マーケティング戦略の効果を科学的に“見える化”し、効果を最大化することを目的とした総合支援サービス
TrueNavi	truenavi.net	コンサルティング業務を通じて独自に開発したインターネットリサーチサービス
TRUE TELLER	www.trueteller.net	コールセンターからマーケティング部門までさまざまなビジネスシーンで活用可能なテキストマイニングツール
てぷらぱ	teplapa.nri.co.jp	テスト工程の効率化を実現するテスト自動実行支援ツール
OpenStandia	openstandia.jp	オープンソースソフトウェアにより高品質な業務システムを構築するワンストップサービス
Senju Family	senjufamily.nri.co.jp	ITサービスの品質向上とコスト最適化を実現するシステム運用管理ソフトウェア

グループ企業・関連団体のWebサイト

NRIネットコム	www.nri-net.com	インターネットシステムの企画・開発・設計・運用などのソリューションを提供
NRIセキュアテクノロジーズ	www.nri-secure.co.jp	情報セキュリティに関するコンサルティング、ソリューション導入、教育、運用などのワンストップサービスを提供
NRIデータiテック	www.n-itech.com	IT基盤の設計・構築・展開と稼働後のきめ細かな維持・管理サービスを提供
NRIサイバーパテント	www.patent.ne.jp	「NRIサイバーパテントデスク」など、特許の取得・活用のためのソリューションを提供
NRI社会情報システム	www.nri-social.co.jp	全国のシルバー人材センターの事業を支援する総合情報処理システム「エイジレス80」を提供
NRIプロセスイノベーション	www.nri-pi.com	中国でのオフショア業務などで培ったノウハウを活用した業務支援サービスを提供
NRIシステムテクノ	www.nri-st.co.jp	味の素グループに情報システムの企画・開発・運用サービスを提供
だいこう証券ビジネス	www.daiko-sb.co.jp	証券業務に関わるさまざまなミドル・バックサービスをワンストップで提供
野村マネジメント・スクール	www.nsam.or.jp	日本の経済社会の健全な発展および国民生活の向上のために重要な経営幹部の育成を支援する各種講座を開催

Worldwide

NRIグループ（グローバル）	www.nri.com	NRIアジア・パシフィック	www.nrisg.com
NRI Financial Solutions（英語）	fis.nri.co.jp/en	野村総合研究所（香港）有限公司	www.nrihk.com
野村総合研究所（北京）有限公司	www.nri.com.cn/beijing	野村総合研究所（台湾）有限公司	www.nri.com.tw
上海支店	shanghai.nri.com.cn	野村総合研究所ソウル	www.nri-seoul.co.kr
野村総合研究所（上海）有限公司	consulting.nri.com.cn		

『ITソリューション フロンティア』について

本誌の各論文およびバックナンバーはNRI公式ホームページで閲覧できます。
本誌に関するご意見、ご要望などは、it-solution@nri.co.jp宛てにお送りください。

おわびと訂正

前号（2014年8月号）に誤りがありました。おわびして下記のとおり訂正いたします。

19ページ筆者肩書き

（誤）システムコンサルティング本部

（正）システムコンサルティング事業本部

ITソリューションフロンティア

2014年9月号　Vol.31 No.9（通巻369号）

2014年8月20日　発行

発行人　嶋本　正

発行所　株式会社野村総合研究所　コーポレートコミュニケーション部

〒100－0005　東京都千代田区丸の内1－6－5　丸の内北口ビル

ホームページ　www.nri.com/jp

発　送　NRIワークプレイス株式会社　ビジネスサービスグループ

〒240－0005　横浜市保土ケ谷区神戸町134

電話（045）336－7331／直通　Fax.（045）336－1408