ビッグデータ社会におけるプライバシー
「個人情報」から「プライバシー」の保護へ

小林慎太郎　八代　拓　伊藤智久　奥見紗和子




CONTENTS

要約

1　スマートフォン（高機能携帯電話端末）やソーシャルメディアの普及、ビッグデータビジネスの台頭によって、これまで非個人情報とされていた情報から特定の個人を識別しやすくなり、既存の個人情報保護法ではプライバシーの保護が困難になりつつある。

2　プライバシー侵害事件は国内外で生じている。国内はスマートフォンの急速な普及に伴う過渡的な問題であるのに対し、グーグルなどのグローバル企業の活動は、個人情報・プライバシーの保護のあり方への挑戦であり、制度的・社会的な仕組みが問われている。

3　日本の消費者は、自身の個人情報がネット上を流通していることをあまり認識していないなど、プライバシー侵害に対する自衛意識が低く、企業や社会の保護対策に委ねる傾向が見られる。

4　米国、EUともに2012年初にプライバシー法制の改正案を発表した。米国が自主規制、EUは法制の強化を指向するものの、同様の問題意識に基づき対処を模索している。①行動ターゲティング、②自動プロファイリング・個人データ売買、③子どものプライバシー保護――の規制案は日本への影響も大きい。

5　到来しつつあるビッグデータ社会に対応するには、「プライバシー・バイ・デザイン」の実践など、「個人情報」から「プライバシー」の保護へと対応を見直す必要がある。マイナンバー法の施行はその試金石となる。

スマートフォン（高機能携帯電話端末）やソーシャルメディアの普及とともに、個人に関するデータが日々大量に生成されるようになった。ビッグデータビジネスが推進される一方で、データの不正利用をはじめとするプライバシー侵害事件が頻発し、ネット社会への不安が高まっている。

ビッグデータは、次代の成長領域と目されるものの、プライバシー問題への対処が大きな課題の一つである。個人に関する情報を安心して利用・提供できる「ビッグデータ社会」に向けて、消費者の意識変化や欧米の政策動向を踏まえ、「個人情報」の範囲に収まらない「プライバシー」をめぐる課題について指摘し、それへの対処のあり方を提起する。

本稿では「個人に関する情報」「個人情報」「プライバシー」を明確に区別して用いるため、最初にその定義と相互の関係を整理する（図1）。

「個人に関する情報」は、個人に関連する情報の最も広い集合を意味する用語として用いる。

「個人情報」は、個人情報保護法で定義されているとおり、「生存する個人に関する情報であって、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）」である。

「プライバシー」は、法令上の定義はないが、一般に、個人や家庭内の私事・私生活、または個人の秘密を指すものであると理解されている。プライバシーは、個人に関する情報（個人情報を含む）の一部の私事・私生活に関する情報が該当し、個人情報と１：１の関係にはない。

図1 「個人に関する情報」「個人情報」「プライバシー」の関係

Ⅰ 個人情報の保護では守れないプライバシー

1 解消されない個人情報保護への不安

2005年に施行された個人情報保護法は、当初こそ、学校の連絡網が作成できなくなったなどのいわゆる「過剰反応」を引き起こしたものの、その後、次第に理解が進み、現在ではわれわれの社会生活にとって重要な制度の一つとして定着した感がある。事実、消費者庁の調査[注1]によると、個人情報にかかわる苦情相談件数と個人情報の漏えい事案件数は、いずれも減少傾向にある。

ところが、消費者の個人情報保護への不安は大きいままである。総務省の調査[注2]によ

ると、インターネット利用で感じる不安の内容として、「個人情報の保護に不安がある」と回答した消費者の割合は７割を超えており、増加傾向にある。また事業者における個人情報保護対策の位置づけについては、経済産業省の調査[注3]によると、重要性がますます高まるか、高いまま維持されていると回答した事業者の割合が８割を超えている。では、いったい何が消費者の個人情報に関する不安を助長し、事業者の対応を要請しているのであろうか。

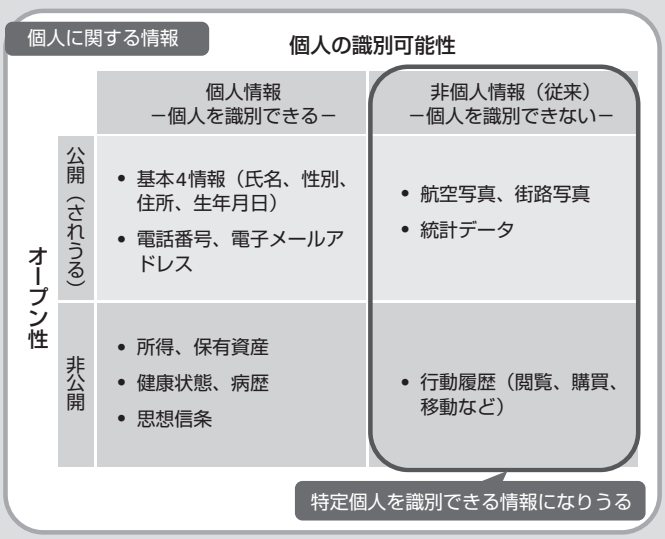
2　ネットを取り巻く３つの環境変化

この消費者の不安心理や事業者の高い個人情報保護対策への意識の背景には、ネットを取り巻く３つの環境変化があると考えられる。

(1)　スマートフォンの急激な普及

スマートフォンは、2011年度の携帯電話端末の出荷台数で初めて従来のフィーチャーフォン（一般型携帯電話端末）を上回り、国民生活に急速に普及しつつある。スマートフォンを利用するとインターネットの利便性が格段に向上するため、まさにいつでもどこでもネットサービスを利用できることに加え、GPS（全地球測位システム）が標準搭載されており、ユーザー自身の居場所を取り込んだサービスも多数提供されている。この結果スマートフォンには、電話帳などの個人情報が、Webサイトの利用履歴、さらにはリアルな移動履歴といったプライバシーにかかわる情報とともに大量に蓄積されることになり、次章で述べるように、不適切なアプリ（ソフトウェア）によるプライバシー侵害事件が頻発する状況にある。

図2　個人情報と非個人情報（従来）の例示



(2)　ソーシャルメディアの利用拡大

ソーシャルメディアは、スマートフォンの普及に伴って若年層を中心に急速に利用が拡大している。10億人以上のユーザーを抱える世界最大のSNS（ソーシャル・ネットワーキング・サービス）「Facebook（フェイスブック）」は実名での利用を義務づけているため、個人情報そのものが日々大量に生成され、友人・知人間を流通している。

SNSでは登録情報の種別に応じて公開範囲を、「友人」「友人の友人」「インターネット全体」といったように細かく設定できるのが一般的である。しかし、初期の公開設定では「インターネット全体」となっているケースがあり、内緒話で書き込んだつもりの情報が公になってしまう事態も生じている。

(3)　ビッグデータビジネスの台頭

整理されていない非構造の大量データを処理することで事業に有意な知見を取り出そうというビッグデータビジネスも、個人情報・プライバシー保護にとっては大きな脅威とな

りうる。

個人情報保護法では、「容易照合性」（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できるかどうか）を判断基準に、個人情報と非個人情報を区別している。しかし、これまで非個人情報とされていた情報であっても、個人に関する情報がネット上に大量に流通するようになり、さらにビッグデータビジネスによって個人の識別が容易にできる社会となりつつある（図２）。

たとえば、ニュース記事に掲載された事件現場の写真を、「グーグルマップ」などのインターネット上の地図情報提供サービスの航空写真と照合することで住所を特定できたり、匿名化処理をした行動履歴のデータを市販データベースと照合することで、特定個人の行動履歴データを識別できたりする事例が報告されている[注4]。また、ネット上を流通するさまざまな情報を収集して特定個人の人物像を描き出す（プロファイリング）サービスも登場している。

個人情報保護法は、「個人情報を保護することで、個人の権利利益を保護する」ことを謳っており、ここでいう「個人の権利利益の保護」にはプライバシーの保護も含まれている[注5]。しかし、

- 個人情報と非個人情報との明確な区別は難しいこと
- ネットビジネスで収集されるデータは、非個人情報であってもプライバシーの侵害につながる可能性があること
- 非個人情報は、本人の知らぬ間にネット上を流通し、本人の行動追跡や人物像が描かれるプロファイリングに利用されていること

――から、既存の個人情報保護法では、ビッグデータ社会におけるプライバシー問題に対処することは困難である。「個人情報」から「プライバシー」の保護へと、民間事業者、行政機関ともに対応が求められている。

Ⅱ ビッグデータ社会で生じるプライバシー侵害事件

1 近年のプライバシー侵害事件の類型

スマートフォンやソーシャルメディアの急速な普及により、新たなプライバシー侵害事件が数多く発生している。近年の主なプライバシー侵害事件の発生要因を、事業者の意識

表1　ビッグデータ社会で生じた主なプライバシー侵害事件とその類型

	日本		米国	
サービス名	ビューン	AppLog（アップログ）	Google Buzz（グーグルバズ）	フェイスブック
事業者	ビューン	ミログ	グーグル	フェイスブック
問題点	ユーザーのページ閲覧履歴を無断で収集し、サーバーに送信する機能がついていた点	同意を取得していない、または取得時の説明が不十分であった点と、送信される情報がユーザーにとって不透明である点	ユーザーの事前同意を取得せずに、「Gmail」の情報を「Google Buzz」の初期設定時のユーザー名などに利用したこと	ユーザーに通知することなく、非公開に設定していた情報の公開設定を変更した点
問題の類型	事業者の認識不足やセキュリティ対策が不十分だったことによる問題		法制度の規範が曖昧な領域に対する事業者の挑戦による問題	
	スマートフォンの急速な普及に伴って**過渡的に生じている**。セキュリティ対策の普及などによって次第に解消されうる		個人情報やプライバシーの保護について、**本質的な制度的・社会的仕組みが問われている**	

面の特徴から整理すると、大きく２つに類型化できる（前ページの表１）。

１つ目の類型は、スマートフォンなどの新たな情報端末の急速な普及と、サービス提供事業者のプライバシー保護への認識不足から生じた事件である。スマートフォン向けアプリを提供している事業者にはベンチャー企業も多く、プライバシーに対して十分な配慮が行き届いていないことがある。さらに、急速に普及した新たなサービスであるため、ガイドラインなどの各種制度が未整備な状態であることも事件発生の要因の一つである。ただし、事業者の認識不足によって生じたこれらの事件に対しては、スマートフォン向けの不正アプリを検出するセキュリティ対策ソフトが普及しつつあり、法制度の整備も検討されている。すなわち、これらは過渡的に生じている事件であり、次第に解消されうる。

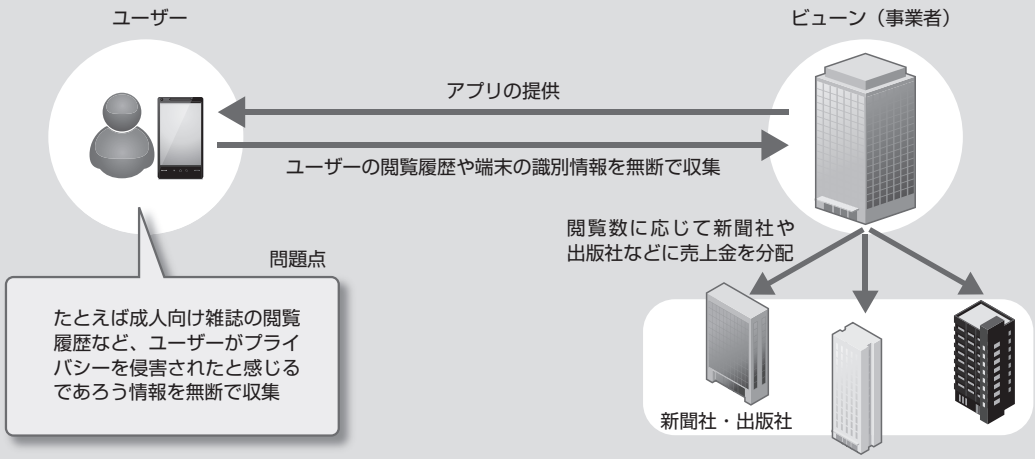
もう１つの類型は、ビッグデータ社会におけるプライバシーという曖昧な領域に対する事業者の挑戦によって生じた事件である。グーグルやフェイスブックなど米国の大手プラットフォーマーは、自らが提供した新たなサービスに対して法的な訴訟が発生していたとしても、プライバシーという曖昧な領域に向けて果敢に挑戦するサービスを提供している。これらのサービスに対しては、個人情報やプライバシーの保護のための本質的な制度的・社会的仕組みづくりが求められる。

2　類型１：事業者の認識不足によるプライバシー侵害事件

事業者の認識不足によって発生した主なプライバシー侵害事件として、「ビューン」と「AppLog（アップログ）」を取り上げる。両事件とも、既存の個人情報ではなく、非個人情報の取得によってプライバシーを侵害したという点で、ビッグデータ社会における特徴的な事件である。

ビューンとは、ビューン（事業者）が「iPhone（アイフォーン）」や「iPad（アイパッド）」「Android（アンドロイド）」の情報端末向けに提供する、電子新聞・雑誌を定額料金で購読できるアプリである。問題となったのは、2011年11月にビューンが公開したアプリに、ユーザーの閲覧履歴や端末識別情報を無断で収集する機能がついていたことであった[注6]（図３）。

図3　ビューンが提供するアプリ「ビューン」の問題点



出所）bizmash!「電子新聞・雑誌に落とし穴、ビューンや産経にユーザー情報の収集機能」（2012年1月）をもとに作成

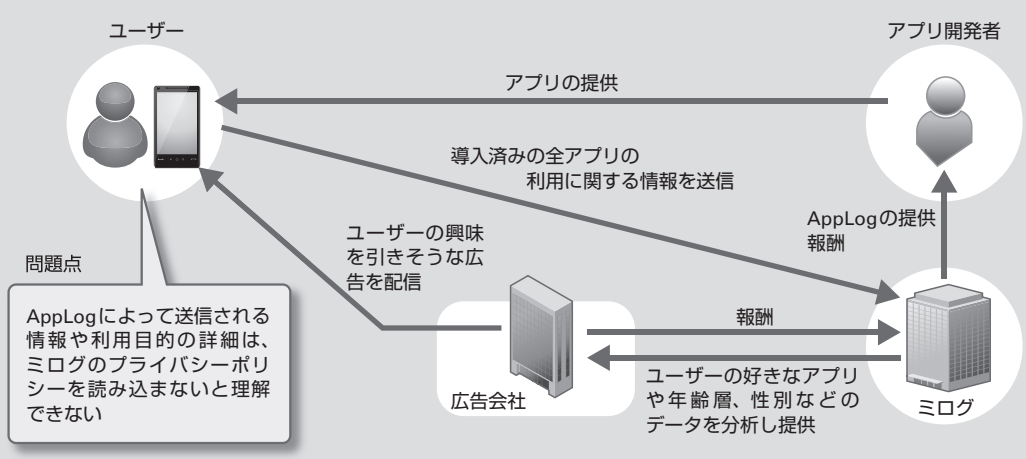
ビューンは、記事を掲載している新聞社・出版社への売上金分配のために閲覧履歴を取得し、特典適用の有無を確認するために端末識別情報を収集していた。取得した情報から個人は識別できないため、ビューンは個人情報には当たらないと認識していた。確かに、閲覧履歴から個人を特定することは困難である。しかし、ユーザーは自分が他人に知られたくないような雑誌（たとえば成人向けの雑誌）などの閲覧履歴を無断で取得された場合、プライバシーが侵害されたと感じるであろう。閲覧履歴の無断取得についてネット上で指摘を受けたため、ビューンは利用規約を変更し、現在では閲覧情報などを取得することを明記している。

一方、AppLogの事件[注7]は、ユーザーの同意を取得する際に十分な説明がされなかった点が問題であった。ミログのAppLogは、Android携帯端末にインストールされたアプリの利用状況を監視・取得するプログラムで、アプリ開発者はこのAppLogを組み込んだアプリを配信し、ユーザーのダウンロード数に応じてミログから報酬が得られる。一方ミログは、広告会社にユーザー情報を分析して提供することで報酬を得る仕組みである（図４）。なおミログは、このプライバシー侵害事件の影響により、2012年４月に会社を解散・精算した。

AppLogの問題は、AppLogが組み込まれたアプリの利用開始時に、「端末情報を送信して広告配信の最適化などに利用する」という旨の簡単な説明のみが表示される点であった。実際には、端末にインストールされているすべてのアプリの利用に関する情報を取得することや、ユーザーの年齢層や性別などのデータと合わせて分析される点については、ミログのプライバシーポリシーを読み込まないとわかりにくい。ユーザーは、すべてのアプリの利用に関する情報が取得されることを想定しておらず、プライバシーを侵害されたと感じた。

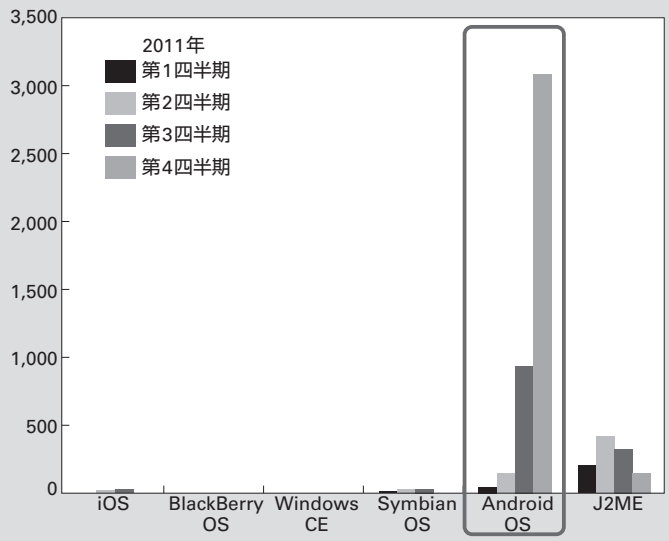
以上のように、ビッグデータ社会では、非個人情報の取得においてプライバシー侵害事件が生じている。特に上述の事件は、スマートフォンなどの新たな情報端末の急速な普及と、サービス提供事業者のプライバシー保護への認識不足から生じた事件である。ユーザ

図4　ミログの「AppLog（アップログ）」の問題点



出所）「アプリ利用時間や回数丸わかり『アップログ』に批判」（2011年10月5日付『朝日新聞』）をもとに作成

図5　モバイル向けマルウェア数



注）マルウェア：悪意のある不正ソフトウェアや不正プログラムの総称
出所）日本スマートフォンセキュリティ協会「マルウェア対策WG活動報告」2012年

ーがプライバシー侵害と感じる方法でスマートフォンなどから情報を取得するアプリは、ビューンやAppLogにとどまらず数多く存在している。特にAndroid端末向けの不正アプリは、2011年の後半から急増しており、11年で4000件以上も確認されている（図５）。

これらの事件は大きな問題ではあるものの、スマートフォン向けの不正アプリを検出するセキュリティ対策ソフトの普及や、官公庁、業界団体などによる法制度の整備が進むことによって次第に解消されうる。

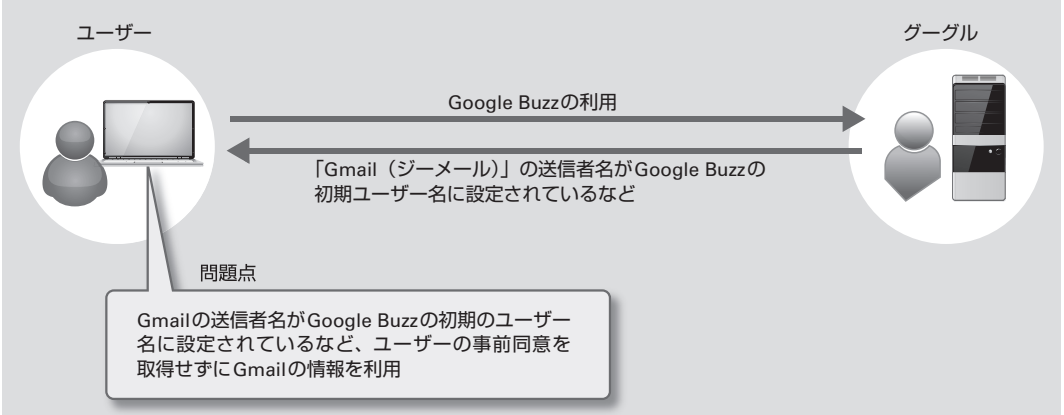
3　類型２：事業者による法制度への挑戦

法制度に対する事業者の挑戦として、グーグルの「Google Buzz（グーグルバズ）」とフェイスブックの事件を取り上げる。

Google Buzzは2010年２月、グーグルのメールサービス「Gmail（ジーメール）」の機能として組み込まれたソーシャルサービスである。Google Buzzの問題は、ユーザーの事前同意を取得することなく、Gmailで収集した情報をグーグルが利用した点である[注8]。グーグルは、「Gmailで収集した情報をGmailのみに用いる」という利用目的を提示しており、他に利用する場合は事前に同意を取得するというポリシーを掲げていたにもかかわらずGoogle Buzzで利用し、それにユーザーがプライバシーを侵害されたと感じた（図６）。

また、フェイスブックは2009年12月、ユーザーが非公開に設定していた可能性のある「Friends List（友だちリスト）」などの情報を、ユーザーの事前同意を取得することなく、すべてのユーザーから閲覧可能とした。フェイスブックはそのほかにも、外部のアプリケーションソフト提供者が必要以上の個人データにアクセスできる状態にするなどしており、同社のこうした複数の行為に、ユーザ

図6　グーグルの「Google Buzz（グーグルバズ）」の問題点



ーはプライバシーを侵害されたと感じた[注9]。

米国連邦取引委員会（FTC）は、Google Buzzやフェイスブックのサービスが、消費者に損害を及ぼす「不公正または欺瞞的行為」に該当すると判断し、両社に対して今後20年間にわたって総合的なプライバシー保護プログラムを実施し、第三者による隔年の監査等を義務づけるなどの是正措置を命じた。

しかしグーグルは、FTCによる是正措置が命じられているにもかかわらず、プライバシーという曖昧な領域に対して果敢に挑戦するサービスを提供している。たとえば、同社は2012年３月に、これまではサービスごとに策定していたプライバシーポリシーを一元化し、各サービスにおけるユーザーのデータを統合して、よりパーソナライズしたサービスを提供することを宣言した。

グーグルと同様にFTCから是正措置を命じられているフェイスブックも、ユーザー情報の初期設定時の公開範囲を年々拡大するなど、プライバシー保護とは逆行するとも取れるビジネスを展開している。

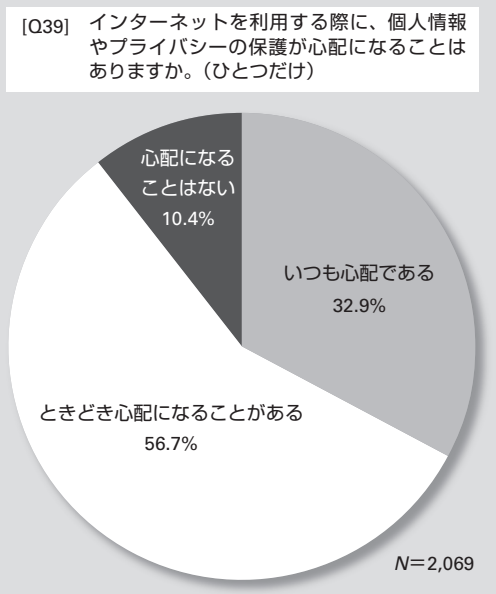
プライバシーという領域に挑戦するグーグルやフェイスブックのような事業者に対しては、個人情報やプライバシー保護についての本質的な制度的・社会的仕組みづくりが求められると考える。

Ⅲ プライバシーに対する消費者の意識

1 具体的な被害に対する認識が不十分な日本の若年層

前章に示したとおり、プライバシー侵害につながりかねない事件が多数発生している。

図7 インターネット利用における個人情報・プライバシー保護に対する消費者の意識



出所）野村総合研究所「情報通信サービスに関するアンケート」2012年7月

頻発するこうした事件に対し、消費者はどのような意識を持っているのだろうか。

野村総合研究所（NRI）が2012年７月に実施した「情報通信サービスに関するアンケート」調査では、インターネット利用の際に個人情報・プライバシー保護に対して、「いつも心配である」「ときどき心配になることがある」と感じている消費者は、合計すると約９割に上ることが明らかとなっている（図７）。

一方、情報処理推進機構（IPA）によると、個人情報の外部利用に対する日本の消費者（特に若年層）の意識は、欧州諸国の消費者に比べて低いという結果が出ている。2010年にIPAが日本の15～25歳の若年層を対象に実施したインターネット調査の結果と、IPTS（Institute for Prospective Technological Studies）[注10]が同様に、EU（欧州連合）に加盟する英国、ドイツ、フランス、スペイン

の４カ国の若年層を対象に実施した調査結果とを比較した（図８）。その結果、「私の個人情報が、私の知らないところで使われている」という項目に対して、「非常に懸念している」「いくぶんか懸念している」と回答した人の割合は、日本の若年層が65%、EUの若年層が82%であり、日本のほうが自分の個人情報の外部利用に対する認識が約20ポイント低かった。

オンライン上に掲載した個人情報が、自分の知らないところで利用されていること自体は認識しつつも、具体的にどのように利用されうるかについての認識が低いということは、被る可能性のある被害の大きさを十分に想像できていないと考えられる。

2　保護対策の実施率が低い日本の若年層

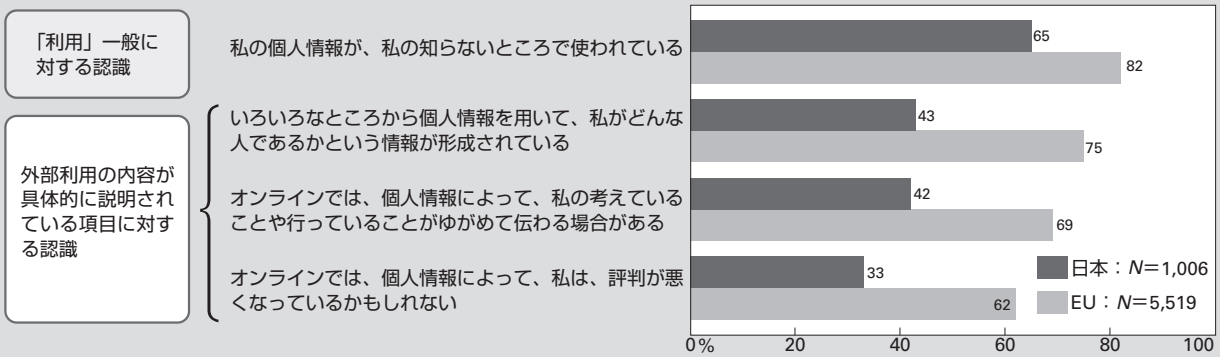
また、外部利用の内容が具体的に説明されている項目「いろいろなところから個人情報を用いて、私がどんな人であるかという情報が形成されている」「オンラインでは、個人情報によって、私の考えていることや行っていることがゆがめて伝わる場合がある」「オンラインでは、個人情報によって、私は、評判が悪くなっているかもしれない」については、日本の若年層の認識はEUの若年層に比べて約30ポイント低い。この結果から、日本の若年層はEUの若年層に比べて、自分がオンライン上に掲載した個人情報を他者が利用する場合の具体的な影響範囲を、十分に想像できていないことがうかがえる。

さらに、自らが個人情報の保護対策を実施しているかどうかの状況は、日本の若年層はEUの若年層に比べて全体的に低い（図９）。

具体的には、「ウェブサイトのプライバシーポリシーを読む」「自分を特定されないように偽の電子メール・アカウントを使用する」「クッキー[注11]を消去する」「個人情報を少しアレンジする」「プライバシーを確保するためにブラウザのセキュリティ設定を変える」「コンピュータから個人情報を収集するのを制限するツール（例えばファイアウォール、クッキー・フィルタリング）を使用する」などの対策ついて、「常にする」「頻繁にする」と回答した日本の若年層の割合は、EU若年層に比較して低かった。

日本の若年層がEUの若年層に比べて唯一高かったのは、「重要な個人情報を入力する前に、取引が保護されている、あるいは、サ

図8　個人情報の利用に対する若年層の認識度合い（日本・EU〈欧州連合〉比較）



注）「非常に懸念している」「いくぶんか懸念している」と回答した人の割合
出所）IPA（情報処理推進機構）「eIDに対するセキュリティとプライバシに関するリスク認知と受容の調査報告」（2010年8月）、IPTS "Young People and Emerging Digital Services: An Exploratory Survey on Motivations, Perceptions and Acceptance of Risks"（2009）より作成

イトが安全であるという表示を持っていることを確認する」であり、自衛策ではなく第三者による安全性の保障を示した項目である。

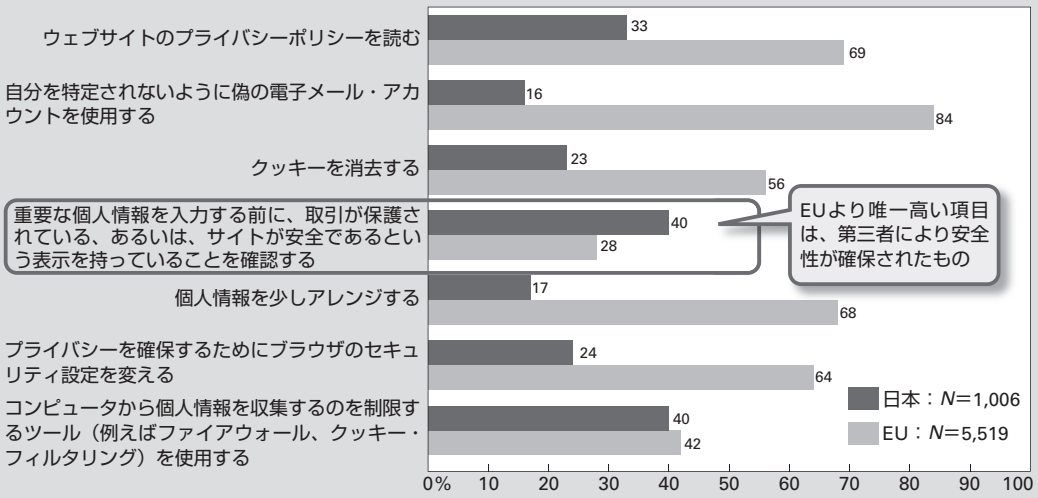
3　他者に保護を期待する日本の若年層

そもそも、EUの若年層に比べて日本の若年層の個人情報保護対策の実施率はなぜ低いのか。

要因の１つと考えられるのが、EUに比べ日本の若年層は、個人情報保護の責任の所在を企業に委ねる傾向が強いことである。図10に示したように、個人情報保護の責任の所在がどこにあるかを、企業、個人、社会全体、政府、警察・検察・裁判所それぞれについて聞いたところ、「企業が責任を持つべき」に「全くそのとおりだ／そのとおりだ」と回答した割合は40％と、EUの若年層に比べて10ポイント以上高かった。

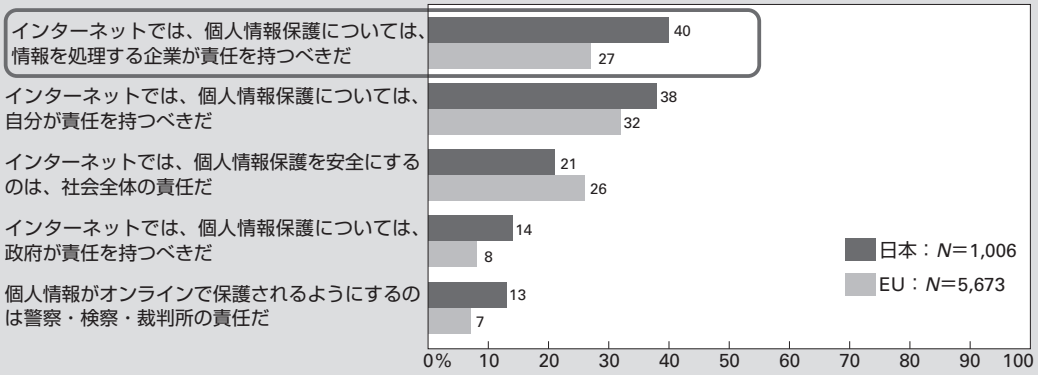
以上から日本の若年層は、オンライン上の個人情報保護についての自衛意識がEUの若年層に比べると低く、企業による保護施策に期待しているのが比較的大きいことは明らか

図9　若年層による個人情報保護対策の実施状況（日本・EU比較）



出所）IPA「eIDに対するセキュリティとプライバシに関するリスク認知と受容の調査報告」（2010年8月）より作成

図10　オンライン上の個人情報保護責任の所在に対する意識（日本・EU比較）



注）「全くそのとおりだ」「そのとおりだ」と回答した人の割合
出所）IPA「eIDに対するセキュリティとプライバシに関するリスク認知と受容の調査報告」（2010年8月）より作成

表2　米国の「消費者プライバシー権利章典」で示されている権利の概要

個人によるコントロール	消費者は、事業者が収集する自身の個人データおよび利用目的について、コントロールする権利を有する
透明性	消費者は、事業者によるプライバシーおよびセキュリティ遵守に関する情報について、容易にアクセスし理解できる権利を有する
脈絡（コンテクスト）の尊重	消費者は、自身が意図したコンテクスト（脈絡）に沿って、事業者による個人データの収集･利用･開示が行われることを期待する権利を有する
セキュリティ	消費者は、個人データが安全に管理され、責任を持って扱われる権利を有する
アクセスおよび正確性	消費者は、機微情報や不正確なデータが本人にリスクを与えるような場合、適切かつ利便性の高い方法で、本人のデータにアクセスし修正する権利を有する
適切な範囲の収集	消費者は、事業者が収集および保持する個人データを適切な範囲にとどめる権利を有する
説明責任	消費者は、個人データが、本権利章典に沿って取り扱われる権利を有する

出所）米国の消費者プライバシー権利章典より作成

である。プライバシー侵害事件が急増しつつあることや、サービス提供者には国内法の及ばない外国企業が多いことなどに鑑みると、危機的な状況であると認識すべきであろう。

Ⅳ 米国、EUそれぞれの規制強化の動き

海外に目を転じると、プライバシー保護は焦眉の課題となっており、米国、EUともに法制の見直しの動きが活発化している。どちらも規制強化の方向では一致しているものの、あくまでも自主規制を基調とする米国と、行政による厳格な法制執行を指向するEUとでは、アプローチの方法が大きく異なっている。本章では、米国、EUそれぞれの新しいプライバシー法案の主なポイントを比較しながら、わが国にも対処が求められる3つの論点について解説する。

1　米国：プライバシー保護と産業振興の両立を模索

米国の個人情報保護法制は、業種や分野別に個別法を定める「セクター形式」を取っており、わが国の個人情報保護法に相当する一般法はない。主な個別法には、

①信用情報分野における公正信用報告法（FCRA）

②医療分野における医療保険の相互運用性と説明責任に関する法律（HIPAA）

――などがある。

一般法がないことから、対応する個別法のない業種・分野における個人情報・プライバシー保護は事業者の裁量に委ねられている。すなわち一般法のあるわが国やEUよりも、米国は個人に関する情報の利用は比較的自由な環境にあり、このことから、産業振興を優先する同国の姿勢がうかがえる。

しかし、第Ⅱ章で述べたグーグルとフェイスブックの事例に見られるように、個人に関する情報を活用するビジネスが興隆する一方で、消費者のプライバシーを侵害する事件が頻発し、規制強化を要請する機運が高まっていた。こうした状況のもと、オバマ政権は2012年２月に「消費者プライバシー権利章典」を取りまとめ、消費者のプライバシー権をこれまでよりも明確にし、事業者の自主規制を促すこととした[注12]。これは、プライバシー保護を強化するための議員立法の提出が相次ぐ状況下にあって、法的拘束力のない消費者の権利章典を定めることで、新たな義務規制を事業者に課すことを回避する策と見ることもできる。

同章典では消費者の権利を７つ定めている（表２）。それには、

①消費者には、事業者が収集する消費者自身の個人データおよび利用目的をコントロールする権利を有する「自己情報コントロール権」

②消費者自身が意図した脈絡（コンテクスト）で、事業者による個人データやプライバシーにかかわる情報の取り扱いがなされることを期待する権利

――などがあり、消費者自らがプライバシー保護に積極的に関与することを奨励しつつも、事業者の自主的な取り組みを促す内容となっている[注13]。

2 EU:「人権」としてのプライバシー保護を強化

EUでは、1995年施行のEUデータ保護指令に基づいて、EU構成国がそれぞれ国内法を制定し、個人情報およびプライバシーの保護措置を講じている。しかし、同指令はインターネットの普及以前に策定された内容であり、めまぐるしく進化するネット社会に対応するため、かねてより改正の議論が重ねられてきた。

その成果として、欧州委員会は2012年１月に、EUデータ保護指令を全面的に見直したEUデータ保護規則（General Data Protection Regulation[注14]）案（以下、新EU規則案）を公表した。EUデータ保護指令が、各国に国内法化する際の裁量を残すルールであったのに対し、新EU規則案はEU全域を拘束する統一ルールに位置づけられる。背景には、急速な変化に適応するため国ごとの差異をなくし、EUが一体となってプライバシー保護を推進しなければならないという強い危機感がある[注15]。

「プライバシーは重要な人権の一つである」との基本認識[注16]に立脚する新EU規則案では、「忘却される権利」や「自動プロファイリングされない権利」などの個人の新たな権利が創設される。併せて、罰則をはじめとする事業者への規制も大幅に強化されている。同規則案では、EU域内に事業所がなくとも、EU市民を対象としたサービスを展開する事業者も規制対象にしており、わが国の事

表3　EUデータ保護規則案で示されている権利の概要

名称		EUデータ保護規則案
基本思想		人権保護
同意取得のあり方		オプトイン（本人の事前同意の取得を義務化）
特徴	「自己情報コントロール権」	透明なプライバシーポリシー（11条）や明示的な同意の取得（7条）、自己情報への容易なアクセスの保証（15条）に加え、「忘却される権利」（17条）等を通じ、消費者の自己情報コントロール権を強化
	セキュリティ	プライバシー強化技術（30条）やプライバシー認証制度（39条）の促進に加え、同規則違反時における、24時間以内の監督機関への届け出義務（31条）等を明示
	データ管理者の責任	プライバシー侵害の予防対策をサービス設計段階から講じる「プライバシー・バイ・デザイン」原則（23条）や機微情報にかかわるデータ保護影響評価（33条）等を通じて、データ管理者の説明責任を強化
	異議申し立ての権利	自動プロファイリングをされた異議申し立てを行う権利（19条）、および「自動プロファイリングのみに依拠して評価されない権利」（20条）を規定
	子どものプライバシー	13歳未満の子どものデータの取り扱いについては、親権者の事前同意を義務づけ（8条）
	非EU地域への言及	EU内に事業所がなくとも、EU市民を対象としたサービスを展開する事業者を規制対象と規定（3条）

出所）EUデータ保護規則案より作成

業者にとっても看過できない内容となっている（前ページの表３）。

3　対処が求められる３つの論点

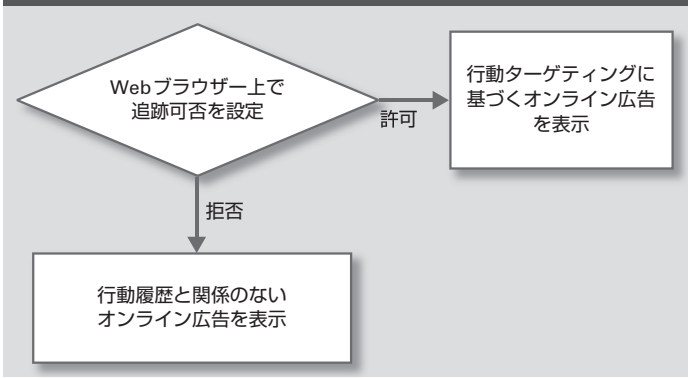
欧米のプライバシー保護政策の見直しを踏まえ、わが国への影響が大きいと想定される３つの論点、①行動ターゲティング、②自動プロファイリング・個人データの売買、③子どものプライバシー保護――についてそれぞれ述べる。いずれもわが国の個人情報保護法には収まらない領域にあり、国際協調の観点からも対処が必要と考えられる。

（1）行動ターゲティング

行動ターゲティングとは、広告配信事業者などが、クッキーやビーコン[注17]などを用いて、ネット上の個人の行動履歴を収集・分析し、個人の嗜好に合わせたオンライン広告表示やサービスを提供するための行為のことで、多くの関連ビジネスが展開されている。

しかし、この行為はプライバシーを侵害するものである[注18]として、米国の消費者団体やEUのデータ保護機関から規制強化を要請する機運が高まってきた。その際に論点となったのは、個人の嗜好に合わせたオンライン広告表示を「希望するユーザー」と「希望しないユーザー」のそれぞれの意思をどのようなメカニズムを通じて尊重するかという点であった。

図11　米国の「Do Not Track（追跡禁止）」の仕組み



こうした要請を踏まえ米国では、「Do Not Track（追跡禁止）」という仕組みによる「オプトアウト[注19]」を基調とする自主規制が推進されてきた。Do Not Trackは、ユーザー本人がWebブラウザー上で追跡の可否を設定できる仕組みを導入することで、行動ターゲティングに基づくオンライン広告表示やサービス提供を「希望しないユーザー」の意思を尊重するものである（図11）。

しかしFTCは、Do Not Trackにかかわる自主規制が必ずしも十分な効果を生んでいないとの認識のもと、Do Not Trackの監督を強化することを表明した[注20]。その後マイクロソフトは、同社のWebブラウザー「インターネットエクスプローラー」の初期設定でDo Not Trackを有効にすると表明している。なおオンライン広告業界は、マイクロソフトのこの決定に反対の姿勢を示している[注21]。

一方、EUでは、本人の自己情報コントロールを尊重し、事業者がクッキーなどを用いて行動ターゲティングを行う場合は、ユーザーから事前に明示的な同意を取得することを義務づける（オプトイン）政策を取っている[注22]。しかし、クッキーはインターネット利用に欠かせないツールとなっており、すべてをオプトインにすると利便性が損なわれ、運用に支障を来すため、オプトアウトがそのまま運用されているサイトも一部残っている。

（2）自動プロファイリング・個人データ売買

自動プロファイリングとは、クッキーなどを用いて個人の行動を追跡・推測したり、

Webサイト上に掲載されている個人情報を収集したりして、個人のプロファイルを自動作成する行為である。たとえば、SNSやブログなどに書き込んだプライベートな情報がプロファイリング事業者によって収集され、正確性が担保されないまま個人の「歴史」として公表されてしまうこともありうる。

問題は、「本人の意思に関係なく」「自動でプロファイリングされ」「正確性が担保されないまま」「公開される」ことにある。また、プロファイリングされたデータの蓄積に伴って、そうしたデータを売買するデータブローカーも多数存在し、誤った人物像が流通してしまう状況にもある。

米国は2000年初から、プロファイリングの可否を本人が決定できるよう、また、収集されたデータへの本人からのアクセス性、データの安全性を担保するよう推進してきたが[注23]、こうした自主規制では不十分であるとして、FTCは2012年３月、データブローカーを規制する立法を示唆している[注24]。実際、すでに2012年６月には、プロファイリングデータを販売したSpokeoがFTCから80万ドルの罰金を科される[注25]など、プロファイリング事業者の規制強化が始まっている（図12）。

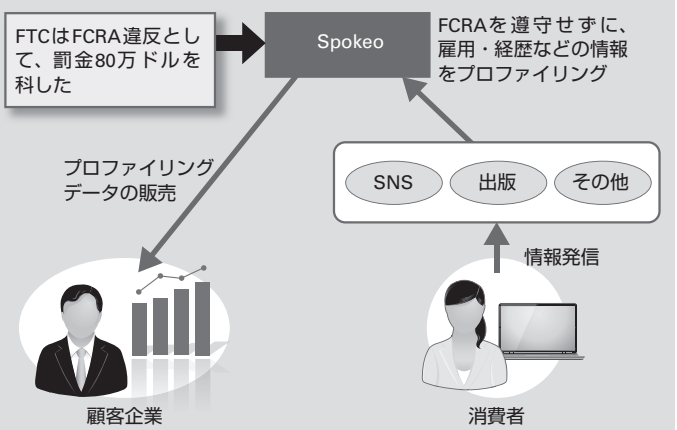
一方、EUは新EU規則案で、本人の個人的側面の評価や業績、経済状況、所在する場所、健康、趣味嗜好、信頼性、行動などがプロファイリングされない権利を創設し、権利を侵害しかねないプロファイリングサービスを牽制している。

すでにフランスでは、プロファイリングデータの購入者が罰せられる事件が発生した。本事件では、オンライン広告などの閲覧履歴をもとにデータブローカーが不動産所有者の個人情報を収集し、不動産調査会社にそのデータを販売していた。不動産調査会社は、購入データを利用して不動産所有者に向けて、事前同意を取得しない状態で広告を配信した。これに対してフランスのプライバシー監督機関であるCNILは、データの購入者である不動産調査会社に対し、２万ユーロの罰金を科したのである（図13）[注26]。

（３）子どものプライバシー保護

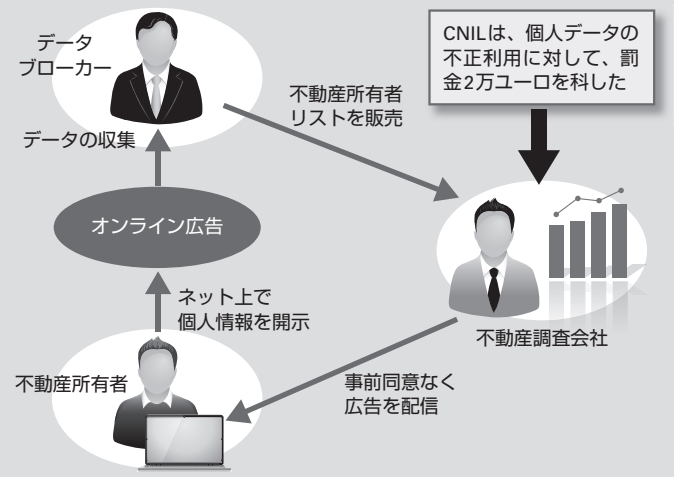
SNSをはじめ、若年層がユーザーの中心を

図12　米国でのプロファイリング事業者への罰則付加



注）FCRA：公正信用報告法、SNS：ソーシャル・ネットワーキング・サービス
出所）FTC（米国連邦取引委員会）のWebサイトより作成

図13　フランスでのプロファイリングデータ購入者への罰則付加



注）CNIL：フランスのプライバシー監督機関
出所）Privacy and Information Law Blogより作成

占めるオンラインサービスが普及するなか、子どものプライバシー保護が、米国、EUともに重要な課題として認識されている。オンラインサービスをゲーム感覚で利用する子どもは、習熟が早い一方で、社会経験や言語能力が乏しいため、私生活を不用意にネット上に公開してしまうことが多い。書き込んだ内容が、後に不適切であったと思って消去しようとしても、ネット上にいったん拡散してしまった情報を消去することは非常に困難である。

米国では、子どもオンラインプライバシー保護法（COPPA）によって、13歳未満の子どもがオンラインサービスを利用する際には親権者の同意を義務づけてきた。しかし、この法令が事業者によって十分に遵守されていないことから、監督が強化される見込みである[注27]。

EUも米国と同様に、新EU規則案では13歳未満の子どもの個人データの処理には親権者の同意取得を新たに義務づけた。これによりEUと米国の、子どものプライバシー保護にかかわる足並みがそろったことになる。また、創設される忘却される権利は子どものプライバシー保護を念頭に置いており、ソーシャルメディアなどの個人データを公開している事業者は、本人からの求めに応じて、当該データのリンクやコピーをネット上から削除することに責任を負うこととしている。

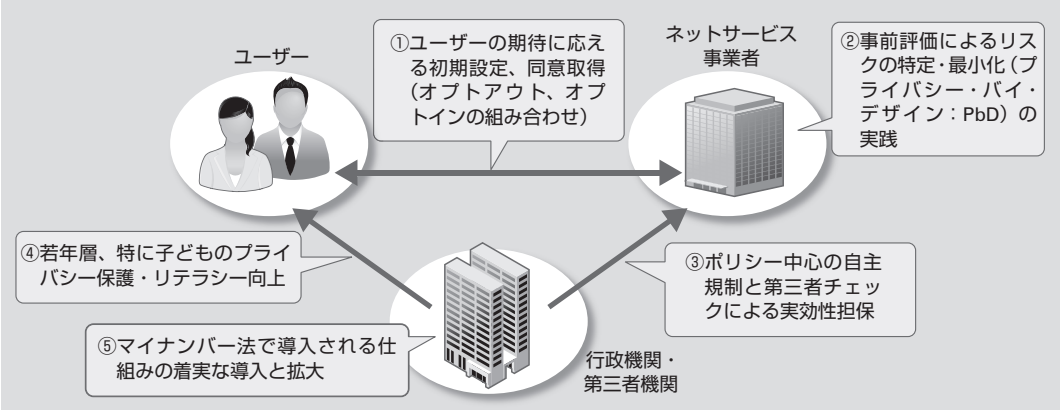
V ビッグデータ社会で求められるプライバシー保護のあり方

前章までに見たとおり、到来しつつあるビッグデータ社会に向け、わが国でもプライバシー保護への対処は急務である。本章では、「ユーザー」「ネットサービス事業者」「行政機関・第三者機関」の３つの主体が相互に関係し合うプライバシー保護のポイントを５つ提示し（図14）、それぞれの対処のあり方を考える。

1 ユーザーの期待に応える初期設定、同意取得（オプトアウト、オプトインの組み合わせ）

本人の意思を尊重して個人情報を取得・利用することは原則であるものの、EUのように、Webサイトを閲覧する際に挿入されるクッキーなどに対して必ず同意を求めていては利便性が低下するため、多くの日本人は欲していないであろうと推測できる。一方で、クッキーを通じて事業者が収集する閲覧履歴

図14　ビッグデータ社会におけるプライバシー保護を実現させるための5つのポイント



などの行動履歴情報を、複数の事業者の間で共有されることについては不快と感じることもあろう。

このため、コンテクストに沿って、ユーザーが期待する、すなわちユーザーが想定できる情報の取得、利用・提供の範囲を評価し、その結果に基づいて、情報の公開に関する初期設定や同意取得すべき場面を設定するよう提案する。

たとえば、多くの日本人は氏名や顔写真の提供を忌避する傾向にあることから、SNSでの個人情報の公開範囲は「友人」までを初期設定とする、軽微なポリシー変更（管理者名の変更など）はオプトアウトとし、当該サイト以外へ情報を提供するときは、本人の同意をオプトインで取得するといったものである。また、同意を取得するための通知文に、「アフターサービスに利用する」などの一般的に受容される内容は省略し、本当に伝えたい内容だけに絞り込むことも重要である。

ただしこのような取り組みが、競争の激しいネット業界で自発的に生まれることを望むのは困難である。事業者が利害を超えてビジネスの健全な発展に向かうには、まず公的機関が指針を明確にし、業界団体などにおいて各事業者が協調して対策を図る環境を整備することが不可欠であろう[注28]。

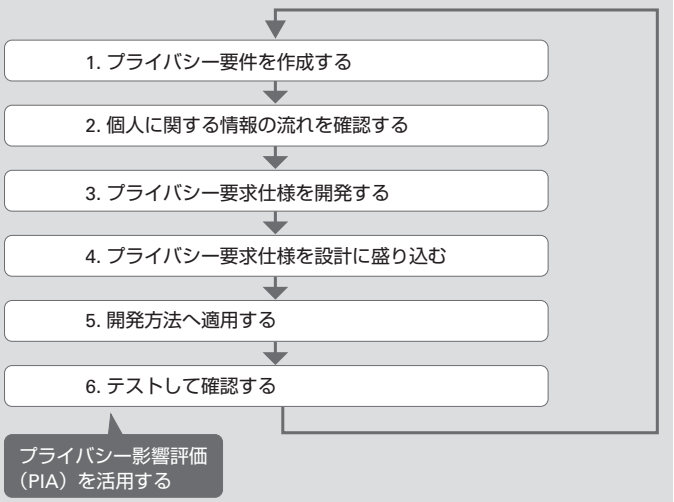
さらに、米国のFTCが推進するDo Not Trackのように、ユーザーのプライバシー設定を情報システムが判読して自動的に対処する仕組みも、今後の発展が期待される。たとえば、本人が希望するプライバシー保護のレベルを高・中・低の３段階で設定しておくと、アクセス先のサイトが初期設定を自動的にチューニングし、オプトインが必要なサービスを絞り込むことができれば、ユーザーの安心および利便性向上に寄与すると考えられる[注29]。

2　事前評価によるリスクの特定・最小化（プライバシー・バイ・デザイン：PbD）の実践

ビッグデータ社会では、これまで非個人情報と見なされていた情報であっても、特定の個人が識別される蓋然性が高くなる。このため個人に関する情報を収集する場合は、サービス開始に当たって発生する可能性があるプライバシー侵害を事前評価して、リスクを特定し最小化する取り組みである「プライバシー・バイ・デザイン（Privacy-by-Design、以下、PbD）」の実施（図15）が望まれる。

PbDを実施する手法としては、「プライバシー影響評価（Privacy Impact Assessment：PIA）」があり、米国、カナダ、オーストラリアなどでは電子政府プロジェクトに伴って行政機関に義務づけられ、定着している。またEUの新EU規則案では、PIAの実施が官民問わず要請されている。わが国のマイ

図15　プライバシー・バイ・デザイン（PbD）の実施プロセス



出所）Ann Cavoukian,“Privacy by Design Curriculum”より作成

ナンバー法では、「情報保護評価」として行政機関に義務づけられる予定である。

このPIAの実施時には、経済的損失リスクを定量把握することを提案する。サービスの期待収益とプライバシー侵害による経済的損失リスクとを比較衡量すれば、プライバシー保護対策に投資すべき予算を正当化することができ、PbDを円滑に進めることにつながる。

3 ポリシー中心の自主規制と第三者チェックによる実効性担保

第Ⅱ章のグーグルやフェイスブックの事例で見たように、米国では、プライバシーポリシーを、事業者による顧客とのプライバシー保護に対する約束事であるとして、運用実態に不正や欺瞞行為が認められたときは、FTCがFTC法５条に基づいて是正措置を命じることができる。また、前述のようにEUの若年層は、自身のプライバシーを守るために、Webサイトに掲載されたプライバシーポリシーを読む割合が高く（45ページの図９）、同ポリシーは、事業者のプライバシー保護を律するツールとして機能している。

わが国でも、個人情報保護法に収まらないプライバシーへの対処は、事業者自らがプライバシーポリシーを掲げて自主的に取り組むことが望まれる[注30]。このためには、まず公的機関や業界団体が、プライバシーポリシーで表示すべき事項を定める必要がある。

また、プライバシーポリシーの実効性を高めるには、第三者による監視の仕組みが必要である。わが国は米国やEUのようなプライバシー保護の監督機関を有しないため、民間の監査事業者や認定個人情報保護団体などの民間団体を活用することが考えられる。

4 若年層、特に子どものプライバシー保護とリテラシーの向上

若年層は、新しい技術への適応能力に優れている一方で、社会経験が乏しいためにプライバシーへの配慮が不足し、攻撃対象となりやすい。事実、若年層を標的にした不適切なアプリが急増しつつあり、特に子どものプライバシー保護は、焦眉の課題となっている。13歳未満の子どものネットサービス利用については、米国、EUとも保護者の同意を義務づけることで一致していることは前述のとおりで、わが国でも早晩、同等の対応が求められると考えられる。

また、EUの提唱する忘却される権利は、特に若年層を意識して議論されており、最近ではカナダの連邦プライバシーコミッショナーが、「今日の若者が犯した多くの過ちの電子的記録が何十年も残り続けることは深刻な懸念のもととなる」[注31]と表明している。ただし、忘却される権利を実現するための方法はいまだ模索段階にある[注32]ことから、まずはプライバシー教育などを通じて、若年層のプライバシーリテラシーを育成することから着手するのが適切であろう。

5 マイナンバー制度で導入される仕組みの着実な導入と拡大

社会保障・税の番号（マイナンバー）制度では、個人情報保護に関する特別法としてマイナンバー法[注33]が施行される予定である（図16）。同法は、マイナンバーに関係する情報に限定しているものの、明確にプライバシー保護を射程にしており、前述のPIAに相当する情報保護評価が導入されるとともに、個人番号情報保護委員会という個人の権利利益

を保護する第三者機関が設置される予定である。わが国でプライバシー保護を推進するには、その第一歩としてマイナンバー制度を着実に運用することが重要であると考えられる。

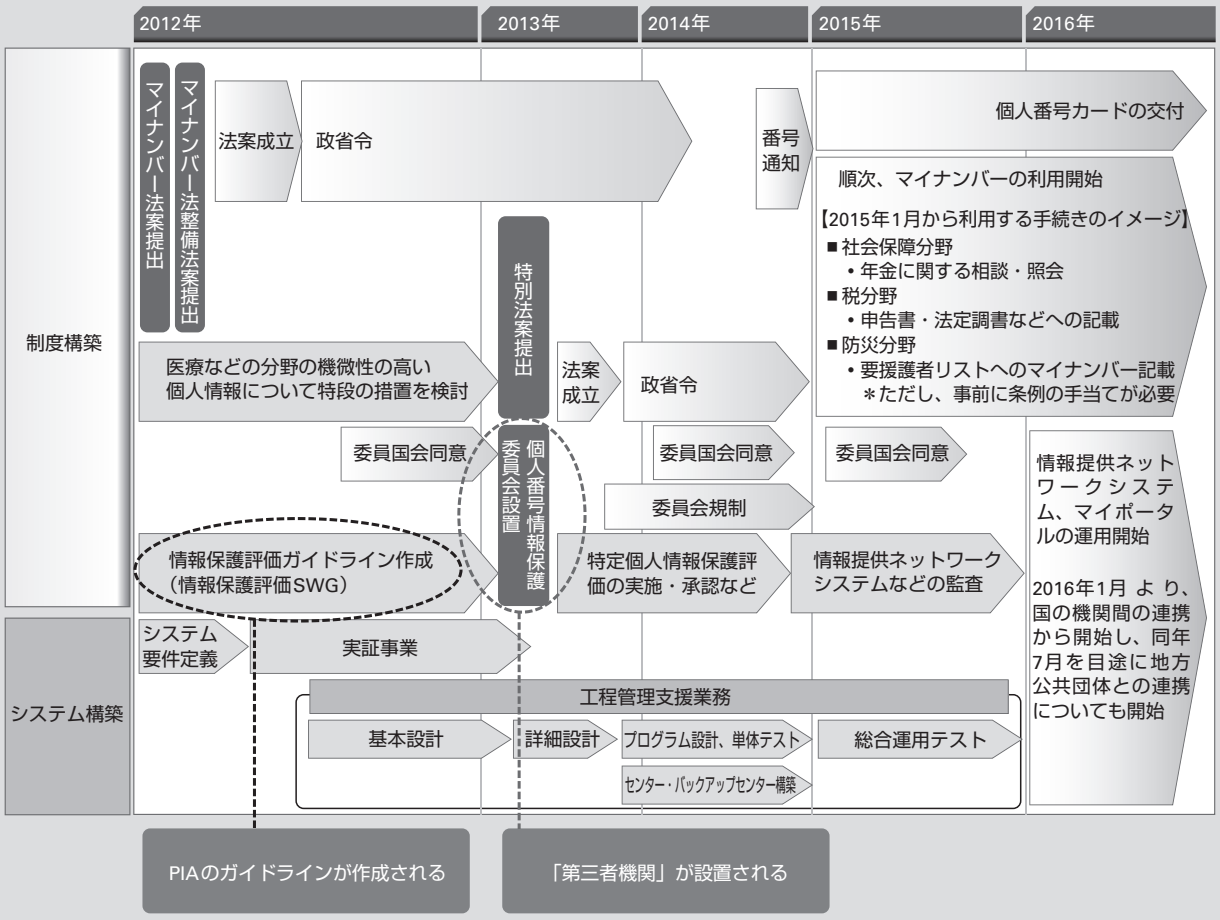
2012年上期は、米国、EUともにプライバシーに関する法規制の見直し案の発表が相次いだ。わが国もマイナンバー制度によってプライバシー保護へ動き出している。まさに「プライバシー元年」といった様相である。

到来しつつあるビッグデータ社会に向け、「個人情報」から「プライバシー」の保護へ踏み出す覚悟が、官民ともに求められている。マイナンバー法の施行はその試金石となろう。

注

1 消費者庁「平成22年度個人情報の保護に関する法律施行状況の概要」2011年８月
2 総務省「平成18年通信利用動向調査」2006年、総務省「平成22年通信利用動向調査」2010年
3 経済産業省「平成23年度　個人情報の保護に関する取組実態調査」2011年３月
4 Paul Ohm,“Broken Promises of Privacy：Responding to the Surprising Failure of Anonymization,”*UCLA Law Review*, Vol. 57, 2009
5 宇賀克也『個人情報保護法の逐条解説』（有斐閣、2005年）による個人の権利利益の解説では、「個人の人格的な権利利益と財産的な権利利益の双方を含む」とされている
6 「『ビューン』サービスに関わる閲覧履歴等のデ

図16　社会保障・税の番号（マイナンバー）制度の導入に向けたロードマップ（抜粋）



出所）内閣官房（2012年5月）

ータの取り扱いについて（2012年１月12日）」ビューンのWebサイト（http://www.viewn.co.jp/news/20120112_01.html）

7 「株式会社ミログ 第三者委員会報告書 2011年12月16日」

8 Federal Trade Commission, “FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network,” March 30, 2011（http://www.ftc.gov/opa/2011/03/google.shtm）

9 Federal Trade Commission , “Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises,” November 29, 2011（http://ftc.gov/opa/2011/11/privacysettlement.shtm）

10 IPTS（Institute for Prospective Technological Studies）は、EU政策に対して科学的な視点で評価する仕組みを構築することで、EU政策立案プロセスに対して消費者の視点によるサポートを提供することをミッションとして設立された科学機関

11 Webサイトの提供者が、Webブラウザーを通じて訪問者のパソコンなどに一時的にデータを書き込んで保存させる仕組みで、利用者に関する情報や最後にサイトを訪れた日時、そのWebサイトの訪問回数などを記録しておくことができることから、認証など利用者の識別に使われる

12 The White House, “We Can't Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consumers Online,” February 23, 2012（http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights）

13 Federal Trade Commission, “Protecting Consumer Privacy in an Era of Rapid Change,” FTC REPORT, March, 2012（http://ftc.gov/os/2012/03/120326privacyreport.pdf）

14 EUROPEAN COMMISSION, “Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data（General Data Protection Regulation）” Jan. 25, 2012

15 欧州委員会副議長の発表時のコメント（European Commission, “Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses,” January 25, 2012）

16 欧州人権（保護）条約（1950年）の８条１項において、「すべての者は、その私生活、家族生活、住居および通信の尊重を受ける権利を有する」と規定されている

17 Webサイト等に埋め込まれた、小さな容量の画像で、ユーザーがWebサイト等へアクセスしたという事実を、把握するために用いられる

18 “Self-Regulatory Principles For Online Behavioral Advertising,” FTC Staff Report, February 2009

19 ユーザーの明示的な同意を事前に取得せずに、ユーザーの個人情報を利用し、本人からの求めに応じてその個人情報の利用を停止するルール。ただし、オプトアウトを採用する場合は、個人情報の利用目的を事前に通知・公表することが前提となる

20 Bloomberg, “FTC Calls for Laws to Boost Consumer Privacy Protections,” Mar 27, 2012（http://www.bloomberg.com/news/2012-03-26/ftc-calls-for-laws-to-boost-consumer-privacy-protection-online.html）

21 “Microsoft Windows 8 includes default Do Not Track privacy feature” *The Washington Post*, May 31, 2012（http://www.washingtonpost.com/blogs/post-tech/post/microsoft-windows-8-includes-default-do-not-track-privacy-feature/2012/05/31/gJQAQ8N74U_blog.html）

22 Directive 2009/136/EC（Cookie Directive）

23 Federal Trade Commission , “Online Profiling：A Report to Congress,” JUNE , 2000

24 Federal Trade Commission , “Protecting Consumer Privacy in an Era of Rapid Change,”

FTC REPORT, March, 2012（http://ftc.gov/os/2012/03/120326privacyreport.pdf）

25 Federal Trade Commission, "Spokeo to Pay $800,000 to Settle FTC Charges Company Allegedly Marketed Information to Employers and Recruiters in Violation of FCRA," JUNE 12, 2012（http://ftc.gov/opa/2012/06/spokeo.shtm）

26 Privacy and Information Law Blog, "France: Sending of direct marketing communications: list brokers and clients: CNIL finds liability on both sides," February 13, 2012（http://privacylawblog.ffw.com/category/sanctions）

27 Thompson Coburn LLP, "United States: FTC Strengthens Law Protecting Children's Personal Information," 12 March, 2012（http://www.mondaq.com/unitedstates/x/168174/Privacy/FTC+Strengthens+Law+Protecting+Childrens+Personal+Information）

28 総務省では、利用者視点を踏まえたICTサービスに係る諸問題に関する研究会を組織して「スマートフォンを経由した利用者情報の取扱いに関するWG　最終取りまとめ・スマートフォンプライバシー イニシアティブ（案）」（2012年6月）を策定。同案には、プライバシー保護のための基本原則が示されている

29 類似のコンセプトにP3P（The Platform for Privacy Preferences Project）プロジェクトがある。P3Pは、Webサイトの運営事業者がプライバシーポリシーを、サイトを訪問する個人のコンピューターのツールが自動的に解読できるよう、記述方式を標準化した仕様である。実装が難しく普及していない

30 わが国では、プライバシーポリシーは、一般に「個人情報保護方針」と呼称されている。個人情報保護法では、個人情報保護方針の規定はないが、第24条（保有個人データに関する事項の公表等）において、公表すべき項目が提示されている

31 カナダ連邦プライバシーコミッショナーWebサイト（2012年6月）

32 グーグルは、「ダッシュボード」というツールで、個人に関する情報が検索結果に表示されないようにするサービスを提供している

33 正式名は、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案

著者

小林慎太郎（こばやししんたろう）
ICT・メディア産業コンサルティング部兼未来創発センター金融・社会システム研究室上級コンサルタント
専門はIT公共政策・経営

八代　拓（やしろたく）
公共経営コンサルティング部副主任研究員
専門は情報法、開発金融政策、東南アジア政治経済情勢など

伊藤智久（いとうともひさ）
経営情報コンサルティング部副主任コンサルタント
専門は情報通信・金融・消費財・サービス分野における事業戦略、マーケティング、IT戦略。また、情報通信分野における法制度の構築支援など

奥見紗和子（おくみさわこ）
金融コンサルティング部コンサルタント
専門はクレジットカード業界における業務改革・システムPMO、個人情報保護政策など