

## NPO-ISEF 情報セキュリティレポート：2012-No.02

# ソーシャルネットワークサービスと 個人情報・プライバシー

情報セキュリティ大学院大学

湯浅 壘道 (Yuasa Harumichi)

### 【著者経歴】

1970年生まれ。青山学院大学法学部卒業、慶應義塾大学大学院法学研究科政治学専攻博士課程退学。2008年九州国際大学副学長。2011年情報セキュリティ大学院大学教授。2012年4月より同学長補佐・教授。情報法、選挙制度などを専攻。

## 1 個人情報とプライバシー

スマートフォンの普及と比例するかのようにして、近年、各種のソーシャルネットワークサービスの利用が急速に進みつつある。しかしこれに伴って、ソーシャルネットワークサービスにおける個人情報やプライバシーの保護のあり方も大きな問題となりつつある。

プライバシーの権利は当初、公権力やマスメディアから個人を保護するものとして形成されてきた経緯がある。公権力が個人に関する情報を大量に収集・蓄積してこれを利用したり、マスメディアが個人の「私生活をみだりに公開」したりすることから個人を保護することは、非常に重要であるとされた。

しかしソーシャルネットワークサービスにおける個人情報・プライバシーの保護は、これとは異なる側面を有している。ソーシャルネットワークサービスを利用するかどうかは、個人の自主的な判断に委ねられており、「ソーシャルネットワークサービスを使いこなさないとビジネスの潮流に乗り遅れる」というような社会的な動機があるとしても、公権力によって強制されているわけではない。また多くのユーザーは、ソーシャルネットワークサービスの上でプライバシーに属する事項を自ら公表している。「〇〇なう(now)」、「〇〇だん(done)」というような書き込みによって、居場所や行った事柄を自ら公表し、それを友人や知人が（場合によっては全く知らない他人も）知ることを期待しているのである。

それでは、ソーシャルネットワークサービスにおけるさまざまな情報は、個人が自主的に公表したものであるから、その保護は必要ないと考えてもよいのであろうか。ここには二つの問題点がある。一つは、かならずしも自主的に公表されたものとはいえない情報も少なくないということである。たとえば友人や知人と一緒に撮った写真を他の人が断りなく掲載し、そこに名前を書き込んで、顔と氏名を合致させてしまうという場合がある。Facebookではタグ付けという機能があり、写真の顔の部分などをクリックして、その箇所に表示されている部分に相当する人物の名前を設定することができ

る。この場合は、自分の知らない間に自分の顔と氏名を一致させて公開されてしまうことになるが、これは私人同士がプライバシーを侵害し合っているということになる。

さらに、ユーザーはプライバシーに属する事項を自ら公表したとしても、それが後になってどのような影響をもたらすのかを必ずしも理解していない可能性がある。社会的・経済的な悪影響が生じたり不利益を受けたりする可能性を事前に知らされていれば、公表することを控えたであろうという情報について、その保護は必要ないのであろうか。その一例として、最近「ソー活」と呼ばれるようになっている就職活動におけるソーシャルネットワークの利用の場面を考えてみたい。

## 2 「ソー活」とプライバシー保護

ソーシャルネットワークサービスが就職活動に利用されることは、学生・企業の双方にとって諸刃の剣になりかねない面がある。特に、身上調査の手段として利用されかねないという点については、十分に理解されているとはいえない。実際に、近年の調査結果によればアメリカでは約半数の企業が採用候補者のソーシャルメディア身上調査(Social Media Background Checks)を行っているという。

学生にとっては、就職活動を始める前に何気なくネットワーク上で書き込んだりつぶやいたりした内容が企業側から採用候補者として問題があると判断される可能性があり、就職活動の際に影響を与えることを恐れて自由な表現活動をすることができなくなるという萎縮効果が発生する恐れがある。逆に、そのことを意識した学生は、志望する企業について意図的にほめちぎったり、企業側からみて採用したいと思わせるような人材像を装った書き込みばかりしたりする可能性もあろう。後者については、企業が消費者に広告と気づかれないように客観的な記事を装って宣伝行為をする「ステマ(ステルス・マーケティング)」の逆のパターンという側面も有するが、これは経歴詐称や詐欺といえるのであろうか。

このような状況の下で、カナダのプリティッシュコロンビア州情報プライバシー・コミッショナー事務局(Office of the Information and Privacy Commissioner)が、いち早く2011年11月にソーシャルメディア利用に関するガイドライン(Guidelines for Social Media Background Checks)を公表したことは注目される。

ガイドラインの前文によれば、「今や企業やボランティアエージェンシー、その他の組織(政党など)は、あたかも信用情報や犯罪歴調査のように、将来従業員やボランティアスタッフや候補者となりうる人々のソーシャルメディア上での振る舞いをチェックしている。これらの調査は、対象となる人々の同意を得る場合もあれば、得ない場合もある。現在のところ、管轄司法機関や裁判所からの指針はほとんど存在しない。」(訳文は、情報セキュリティ大学院大学修士課程修了・同客員研究員の永野一郎氏の試訳による)という。

従来、このような個人情報やプライバシーに関する情報の取扱いについては、本人の同意を得ているかどうかというのが一つの基準となっていた。しかし、ソーシャルネットワークサービス上の個人情報やプライバシーに関係する情報は、本人が自主的に公表している場合もあれば無断で公表されている場合もあり、それらを「同意の有無」という観点から区別することは困難である。そこでガイドラインでは、次のように具体的にってはならない行為についての例を示している。わが国の「ソー活」

のあり方を考える上でも、示唆に富むものとなっているといえよう。

1. プライバシー法制に遵守しているかの評価を、調査実施後まで先延ばしにすること。
2. 調査が単独の個人に関する情報のみを対象とし、複数の個人に関する情報は含まれることはない  
と想定すること。
3. プライバシーの法規制を避けるため、個人のアカウントを用いて調査を行うこと。
4. プライバシー法規制上の義務を免れる目的で、外部機関を用いて調査を行うこと。
5. 調査の対象となった者が、そのことを知り得ないと想定して行動すること。個人であっても、自  
身の個人情報にアクセスした者の IP アドレスをチェックする等のアクセス解析は可能である。

### 3 位置情報とプライバシー・ビジネス

近時は、GPS機能を装備したスマートフォンの普及により、スマートフォンを携帯するひとりひとりの個人の位置情報を容易に取得できるようになり、位置情報が積極的に利用されるようになってきている。その反面、個人がどの位置にいるかという情報、位置の移動の追跡による個人の行動情報が収集され、本人の意図しないところで公開されたり利用されたりする機会が増大している。すでにアメリカでは、自動車のGPS装置から位置情報を送信しそのデータを使用することを保険会社に許諾すると、自動車保険の保険料が割安になる仕組み（走行した距離の分だけ自動車保険料を負担すればよいという仕組み等）が導入されはじめている。このような自動車保険は「pay as you drive」と呼ばれているが、カリフォルニア州ではこの仕組みの導入を保険会社に義務づけようとしたため、プライバシー保護に関する議論が起こっている。

しかしこのような位置に関する情報には、個人のプライバシーとしての側面のほかに、財産的価値があるか、財産的価値があるとすれば誰のものか、譲渡・売買の対象となりうるかという点が、法的問題点として浮上している。アメリカにおいても、位置に関する情報には個人のプライバシーとしての側面のほかに財産的価値があるか、何らかの価値があるとすればそれを収集した機器に属するものか、位置を収集された個人に属するものであるかについては、議論の最中である。

2012年1月にアメリカ連邦最高裁判所で判決が下された合衆国対ジョーンズ判決(United States v. Jones, 565 U.S. \_\_ (2012), 132 S. Ct. 945 (2012) (No.10-1259))では、9人の最高裁判所判事の見解が二つに割れ、位置に関する情報を財産権や所有権という観念に結びつけようとする法廷意見と、個人のプライバシーに属するという補足意見が対立した。法廷意見は、あくまでも古典的な有体物に対する法的保護を基礎としつつ、先端的な技術の進歩や進化するインターネット環境によって生じる多様な問題を、なるべく財産に対する保護のしくみである所有権の範疇で処理しようとした。これに対して補足意見は、そのようなアプローチを否定し、あくまでも合理的なプライバシーの期待の範疇で処理しようとした。法廷意見のアプローチに即すると、位置情報は、それを生成する機器、または取得する機器または機会の所有権的権利の一部として構成することが可能であると思われる。補足意見のアプローチでは、位置情報は属人的なものであり、ある自然人がどこにいる（いた）かという情報は、いつという時間情報と共にプライバシーの一部として取り扱わなければならないことになる。

個人のプライバシーに係る情報を処理することによって効率的なマーケティングを行う手法が開

発・利用されつつあることを踏まえると、位置情報を、譲渡・売買の対象にしたいというニーズが高まってくるであろうことは容易に想像できる。また個人の行動や特性等に関するデータを収集して利用する機会は急速に増えつつあり、それをどのような法的形態によって保護するかという問題が生じてきている。

仮に位置情報が属人的なものであり、位置情報と時間情報は共にプライバシーの一部であるとしても、アメリカではプライバシーをビジネスに展開することは比較的容易である。というのは、アメリカにおいては1974年プライバシー法等で本人がプライバシーを放棄（waiver）し、事業者に自由な第三者提供等を認めるということが規定されているためである。

しかしわが国では、プライバシーは人格権・自己決定権的な意味合いを色濃くして理解されてきた。個人の人格権としてのプライバシーの一部に財産権的価値を認め、それを譲渡・売買の対象とするということは、わが国で掲載されてきたプライバシーの権利とは親和性があるのかという問題が生じるであろう。また、位置の移動の追跡による個人の行動情報の収集は、憲法22条1項が保障する移動の自由を侵害しないかという観点からの検討も必要となつてこよう。

以上

2012年10月2日発行

特定非営利活動法人 NPO 情報セキュリティフォーラム 〒221-0835 神奈川県横浜市神奈川区鶴屋町 2-17 相鉄岩崎学園ビル TEL(045)311-8777 FAX(045)311-8747 E-Mail: isef@isef.or.jp URL: <a href="http://www.isef.or.jp">http://www.isef.or.jp</a>
---

当レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。

Copyright©2012. Not-for-Profit Organization of Information Security Forum All right Reserved