ソーシャルメディアにおけるプライバシーリスクの盲点：リスク逓減に向けた論点整理

鈴木英男* 遠藤真紀* 神野 建*
松下孝太郎* 安岡広志* 新島典子**

LINE、Twitter、Facebookなどのソーシャルメディアが急速に普及している。これらソーシャルメディアの普及とともに、プライバシーの暴露・漏えいが社会問題となっている。筆者はソーシャルメディアにおけるプライバシーを考える上で、ソーシャルメディアをクローズドなソーシャルメディア（LINEなど）とオープンなソーシャルメディア（Twitter、Facebookなど）に分類している。そのうえで本論文では、オープンなソーシャルメディアにおけるプライバシーリスク、実名を晒すプライバシーリスク、クローズドなソーシャルメディアを信用し過ぎるリスクについて、その盲点も含め複数の論点を提示した上で、意図してのみならず意図せずして生じたリスク逓減に向けた整理を行っている。プライバシー漏えいによる犯罪も増えている。特にソーシャルメディア利用率が急増している高校生や若い世代が犯罪に巻き込まれないためにも、本論文はプライバシーリスクを考える複数の材料を提供するものである。

キーワード：プライバシー、ソーシャルメディア、SNS、情報モラル教育、高校生、携帯電話

To Eliminate Blind Spots: On the Issues of Privacy Risks in Social Media

Hideo SUZUKI*, Maki ENDO*, Ken JINNO*,
Kotaro MATSUSHITA*, Hiroshi YASUOKA* and Noriko NIIJIMA**

Social media, as LINE, Twitter, Facebook, rapidly spread and grow in our daily life. These social media cause a divulgation of personal privacy information. The authors categorize social media into the closed social media like LINE and the open social media like Twitter and Facebook. In this paper, we discuss the blind spots related to privacy risks on the open social media services, revealing real name, too much trusting the closed social media services, in particular. An intentional/unintentional divulgation of personal privacy information has actually caused murders and crimes towards younger generation. We summarize the issues, hopefully to eliminate both blind spots of social media users this paper and their future troubles and related problems.

Keywords: privacy, social media, SNS, information morals education, high school student, cellular phone

*東京情報大学 総合情報学部
Tokyo University of Information Sciences, Faculty of Informatics
**ヤマザキ学園大学 動物看護学部
Yamazaki Gakuen University, Faculty of Veterinary Nursing

2014年12月12日受理

1．まえがき

平成26年度版の情報通信白書[1]によればいまや８割の日本人がインターネットを利用する生活を送っており、ICT総研[2]によれば、ソーシャルメディアを利用する人が増えている。ソーシャルメディアとは、Safko[3][4]によれば、「人々が社会的であらんがために使用するメディア」のことである。「ソーシャルメディア」という用語が日本語論文（CiNii全文検索[5]）で最初に使用されたのが2006年であることから、日本の一般社会に浸透したのはこの数年のことであることが推測される。

ソーシャルメディアの社会への浸透とともに、プライバシー暴露・漏洩の社会問題も増えている。例えば、2011年３月Twitterは、ユーザのプロファイルやツイートの保護措置が不十分で、漏洩しうる状態にあり、一方で、Web上では個人情報保護措置を講じていると明示していたため、米国FTC法第５条に基づき改善の執行命令を受けた[6]。2011年11月Facebookは、ユーザの事前同意を取得することなく、友達リストをすべてのユーザから閲覧可能に設定を変更したため、米国FTC法第５条に基づき改善の執行命令を受けた[6]。

これまで、ソーシャルメディア利用時のプライバシーリスクは、個別に断片的に述べられるにとどまり、網羅的に分析・提示するものは見受けられない。

そこで、本論文では、ソーシャルメディア利用に際して生じるプライバシーリスクの盲点を網羅的に提示し、ソーシャルメディア利用時のリスク逓減に向けた整理分析を行う。

ソーシャルメディア利用が社会で加速する理由として、従来の携帯電話機よりもソーシャルメディアを利用しやすいスマートフォンの所持率が上がっていることが挙げられる。MMD研究所の「2014年４月携帯端末購入に関する定点調査」[7]によれば、15～19歳の携帯電話所持者のうち、スマートフォン比率は84.5％であり、内閣府の「平成25年度青少年のインターネット利用環境実態調査」[8]によれば、高校生のスマートフォン所持率は、2010年3.9％、2011年7.2％、2012年55.9％、2013年83.4％と急激に伸びている。

そして、携帯やスマートフォン利用の目的の大半は、ソーシャルメディア利用であることが以下のように明らかになっている。内閣府の調査[8]によれば、高校生の96.7％が携帯電話やスマートフォンでインターネットを利用し、中学生の82.1％、小学生の44.3％が同様に利用している。高校生の利用目的は、メールが81％、調べものが73％、音楽や動画などの閲覧が60.1％、ゲームが51.5％、SNSサイトなどコミュニケーションが51.3％、チャットなどコミュニケーションが46.6％であった。これらは、２章で述べるSafko[3]の12分類によれば、ほとんどがソーシャルメディアの利用となる。

スマートフォンの利用が急伸していることと、ソーシャルメディアの利用がともに急伸していることは、いわば卵とニワトリの関係で、どちらが先（＝要因）か後（＝結果）かはわからないが相互に助長しあう関係性にあることが考えられる。

スマートフォンとソーシャルメディアは便利さから急速に普及はしているものの、実際のところ、どちらも操作が複雑である。したがってソーシャルメディア利用初心者には特に、リスクを意識する余力がない恐れがあり、初期設定のままプライバシーを守る方策を怠りながら利用するユーザも少なからず存在することが懸念される。

筆者らは2004年より各地の高校で、「携帯電話の危険性」という情報モラル教育講演を6,700名超の受講者を対象に実施してきた。携帯電話の本人追跡性を題材にした情報モラル教育の例は、文献[9]に示したとおりである。

だが、これまでの講演への反応や反響を見る限り、高校生が理解できていないリスクが多々あることがわかっている。また、前述のように、

高校生にもスマートフォンが高い比率で普及し、ソーシャルメディア利用率も急速に高まっているとともに、ソーシャルメディア利用に際してのリスクも多様化や拡大化しているため、ソーシャルメディアに関する情報モラル教育は常に見直す必要がある。

ソーシャルメディアは、前述した「人々が社会的であらんがために使用するメディア」という定義からもわかるように、情報を受信するだけでなく発信できる仕組みとなっている。受信するばかりの利用も可能であるが、YouTubeで観た動画に視聴者側からコメントできたり、ブログの記事に読者がコメントできたりと、双方向、さらにはマルチ方向への情報発信が可能である。

では、ソーシャルメディア利用に際して、いかなる場合にいかなるリスクが生じうるだろうか。情報を受信する場合には、メール受信時のウイルス感染によるスパムメール送信などを除きリスクが発生する恐れはほとんどないが、情報を発信する場合には、細心の注意が必要となる。注意を怠ることで人間関係を損ねたり、プライバシー漏洩などのリスクが生じるためである。特にプライバシーのリスクは住所・行動履歴・写真などをはじめとした個人情報が第三者にわかってしまう等の重大な問題に発展しかねず、一層の注意が必要である。

そこで本稿では、ソーシャルメディアにおいて、情報を発信する場合の代表的プライバシーリスクを分類し、リスク逓減に向けた方策について論じるものである。ここで、「情報を発信する」とは、記事、日記、ツイートを書いたり、写真、動画、音声、音楽をインターネット上に掲載したり、コメントを残したり、コメントへのレスポンスを記入するなど、特定もしくは不特定の他者へ向けたあらゆる発信する行為を表すこととする。

2．ソーシャルメディアの分類

2．1 Safkoによる分類

1章で述べたようにソーシャルメディアを定義したSafko[3]は、ソーシャルメディアを次の12種類に分類している。(1) ソーシャルネットワーク（Facebook、mixi、google＋、Ello[10]−[13]）、(2) 写真共有（Instagram、Tumblr[14][15]）、(3) 音楽、音声（YouTube[16]）、(4) 動画（YouTube[16]）、(5) マイクロブログ、ブログ（Twitter、Ameba、FC2、Yahoo、livedoor[17]−[21]）、(6) 放送（nicovideo、Ustream、Podcast[22]−[24]）、(7) 仮想現実（second life[25]）、(8) ゲーム、(9) RSSと情報収集、(10) 検索（google、Yahoo[26][27]）、(11) モバイル、(12) インターパーソナル（＝個人間通信：メール、LINE、WhatsApp、微信（WeChat）、Skype、kakao、Viber[28]−[33]）。上記の（ ）内は、筆者が代表例をあげたものである。

文献[34]では、主要ソーシャルメディアのMAUを報告している。MAU（Monthly Active Users）とは、月間アクティブユーザ数のことで、月1度でもサービスにログインするユーザの数を表す。Safkoの分類する（1）ソーシャルネットワークに該当するFacebookのグローバル（全世界）におけるMAUは12.8億人[35]と世界総人口の約18％、日本におけるMAUは、約2,100万人[36]と日本の総人口の約17％が月に最低1度はログインしていることが分かる。Safkoの分類する（5）マイクロブログ、ブログに該当する例がTwitterであるが、Twitterのグローバルにおける MAUは約2億7,100万人[37]で世界総人口の約3％と少な目だが、日本におけるMAUは、約2,175万人[38]と日本の総人口のやはり約17％が月間アクティブユーザである。全世界ではFacebookはTwitterの約6倍のMAUを擁するが、日本国内では両者のMAUが近い値である点に特徴がある。

次に、Safkoの分類する（12）インターパーソナルに該当する例には、LINE、WhatsApp、

微信（WeChat）などがある。文献[39]によれば、LINEのグローバルにおけるMAUは１億7,000万人、WhatsAppと微信（WeChat）がそれぞれ、６億人と４億3,800万人であり、それぞれ世界総人口の約２％、約８％、約６％となる。

LINEの公式発表[40]によれば、グローバルにおける総ユーザ数は4.9億人、日本における総ユーザ数は5,200万人（人口比率40.9％）、DAU（Daily Active Users、日間アクティブユーザ数）は、3,400万人。WhatsAppと微信（WeChat）の日本におけるDAUは不明であるが、LINEの日本における総ユーザ数の人口比率40.9％より、日本では、インターパーソナルに関して、LINEが一番ユーザ数が多いと考えられる。これらを踏まえ、３章以降では、日本におけるMAUやDAUの大きい、Facebook、Twitter、LINEに主たる焦点をおいて検討してゆく。

２．２　鈴木による分類（クローズドなソーシャルメディアとオープンなソーシャルメディア）

ソーシャルメディアにおけるプライバシーを考える際、鈴木はソーシャルメディアを「クローズド」なソーシャルメディアと「オープン」なソーシャルメディアに分類している[42]。「クローズド」なソーシャルメディアとは、発信する情報の届く範囲が、電話帳や友達リストに掲載されているユーザだけに限定されているソーシャルメディアであると定義する。Safkoの分類する（12）インターパーソナル（＝個人間通信：メール、LINE、WhatsApp、微信（WeChat）、Skype、kakao、Viber[28]−[33]）は、「クローズド」なソーシャルメディアの代表例である。これに対し「オープン」なソーシャルメディアとは、発信する情報の届く範囲が、電話帳や友達リストに掲載されているユーザだけに限定されず、インターネット全体に公開されるソーシャルメディアであると定義する。Safkoの分類する（12）インターパーソナル以外はすべて「オープン」なソーシャルメディアに該当する。例えば、Twitter、Facebookなどは、インターネットに公開し、誰にでもどこからも見られる設定だけでなく、それ以外に、友達リスト、フォロワーリスト、フォローリストに掲載されているユーザ限定で公開する設定も可能である。このような場合でも、公開設定がデフォルト（基本設定）である特徴を有している点で、それらは「オープン」なソーシャルメディアであると定義することとする。

３．情報公開の範囲設定の違い

ソーシャルメディアにおける情報公開の範囲は、各メディアで、大まかに「友達」、「友達の友達」、「全世界に公開」といった数段階を設定している場合が多い。これを筆者は、この先での議論のために抽象化し、便宜上以下の７レベルに細分化する。

（1）家族
（2）信頼できる友達、親友、恋人
（3）ふつうの友達（リアルの面識あり）
（4）ふつうの友達（リアルの面識なし）
（5）友達の友達
（6）そのサービスにログイン中のユーザに一般公開
（7）インターネット上の全ユーザに一般公開

この（1）「家族」から（5）「友達の友達」までの５段階が「クローズド」、すなわち「限定公開」で、それ以外の二段階は「オープン」、すなわち「一般公開」と分類できる。

LINEは、「クローズド」なソーシャルメディアに分類され、友達リストまたは、最大でも電話帳の中でLINEを使用している人全員とのやりとりに限定される。そのため、上記（1）「家族」から（7）「インターネット上の全ユーザに一般公開」のうち（1）「家族」から最大でも（4）「ふつうの友達（面識なし）」までの公開に限られる。

これに対し、Twitterおよびgoogle＋は「オープン」なソーシャルメディアに分類される。そ

れは、これらがいずれも友達という形式を取らず、承認なしのフォローという形をとるためである。いずれにおいても、自分がフォローしている人たちのことをフォローリストと呼び、自分をフォローしている人たちのことをフォロワーリストと呼ぶ。

Twitterでは、発信する情報（140字以内）が届く範囲を「一般公開」か「非公開」のいずれかに設定できるが、初期設定では「一般公開」で、インターネットに接続された全世界の不特定多数のユーザに到達するので注意が必要である。https://twitter.com/ にアクセスすると、ログインしてるユーザ限定の一般公開で、ユーザ登録しないと閲覧できないような印象を受けるが、実際は、https://twitter.com/asahiのように、実在するユーザを一度表示させれば、閲覧でき、検索もできる。

Twitterを用いる際、Privatter[43]を使えば、より多くの情報を細かく範囲を区切って公開することが可能となる。Privatter利用時には、Twitter公開範囲を「全体公開」、「ログイン限定公開」、「フォロワー限定公開」、「相互フォロワー限定公開」、「リスト限定公開」、「非公開」の六段階に分けて設定することが可能になる上、50,000文字程度までの長めの文章が投稿可能となり、画像は2,000KB程度までアップロード可能となる。

Facebookも「オープン」なソーシャルメディアに分類される。そして、発信する情報が届く範囲は「一般公開」、「友達限定」、「友達の友達限定」、「特定の友達限定」、「非公開」の五段階に設定できるが、Twitter同様に初期設定では「一般公開」になっているため、設定変更をしないまま情報を発信すると、インターネットに接続された全世界の不特定多数に到達するので注意が必要である。

また上記範囲のうち（5）「友達の友達」限定は「クローズド」なソーシャルメディアと「オープン」なソーシャルメディアの境界（ボーダー）に位置するとみなせるため、利用には注意が必要である。文献[44]では、仮に各Facebookユーザにそれぞれ100名の友達がいるとすると、「友達の友達」限定で情報発信したとしても、100名の「友達の友達」100名ずつに、つまり合計１万人に対して記事を送信することになり、「インターネット上の全ユーザに公開」とあまりかわりがなくなってしまうので注意が必要であることを指摘している。したがって、プライバシーを確保するためには、「友達の友達限定」で情報発信することは控えて、「友達限定」で情報発信することが望ましい。

さらに注意すべきなのが「シェア」の仕組みである。「オープン」なソーシャルメディアの場合、たとえ自分では「友達限定」で情報発信した場合であっても、受信した友達がその記事を「シェア」という形で「一般公開」してしまうことも仕組上は可能である点が問題となる。そこで、「シェア」して欲しくない場合は、「シェアしないで下さい」と忘れずに都度注意書きを入れる必要がある。

４．若者のソーシャルメディアの使い方

Boydは自身の著書[45]において、米国のティーンエイジャー（若者）によるソーシャルメディア利用の生態について詳しく述べている。彼女によれば、米国のティーンエイジャーには以下のような特徴があるという。

（1）ソーシャルメディアを初期設定のまま使用しているユーザが多い。
（2）初期設定のまま使用しているので、「友達限定」にせず、「一般公開」で情報発信するユーザが多い。
（3）「一般公開」で情報発信しているからといって、プライバシーを気にしていない訳ではない。
（4）一般の目を気にするよりも、家族、特に親の監視による親からのプライバシー侵害を気にしている。
（5）プライバシー確保の目的で、限定された友達にだけ解読可能な隠語をサブリミナ

ルに記事に入れ込むこともあるという。このような行為を「ソーシャルステガノグラフィ（social steganography）」と呼ぶ。

(6) 親の監視は煩わしいが、親が自分のためを思って監視していることは理解している。

少なからぬティーンエイジャーは、一方ではソーシャルメディアを初期設定、つまり「一般公開」のまま使用する無頓着さを有しつつも、他方では、親や周囲の大人の監視からだけは逃れようと、彼らからのプライバシーは上手に確保しているのだ。たしかに、反抗期を迎えたティーンエイジャーは、親の監視は煩く感じるので合点のいく現象である。一般には、３章で述べた７つの情報公開の範囲：「家族」から「一般公開」までは、単一方向的に公開範囲の制限が緩くなってゆくものと考えられる。だが、ティーンエイジャーの場合には、例えば「一般公開」にして誰に見られても良いが、「家族」だけには自分の感情を隠したいというユーザが存在するというBoydの報告[45]は斬新な指摘であったといえよう。

また、複数のソーシャルメディアを同時に器用に使い分けたり、要領よく乗換えや使い捨てが出来るのもティーンエイジャーユーザの特徴である。これまで愛用していたソーシャルメディアの居心地がひとたび悪くなると、気兼ねなく未練なく別のソーシャルメディアに簡単に移行する点も世代的特徴の一つと考えられる。

このような世代的特徴を理解せずして、ティーンエイジャーユーザをリスクから守ることは出来ない。だが世代間で異なる特徴については得てして盲点となりがちなので留意する必要がある。

５．ソーシャルメディアが人間関係を壊すリスク

ソーシャルメディアは人間関係を作ったり、繋いだり、強化するために用いられるものであるが、それは同時に、人間関係を壊す凶器にもなりうる点が盲点となりやすい。ソーシャルメディアに投稿した自分の記事に対し、他者から勘違いをされたり、自分の意図に反したコメントをもらって驚いた経験者は少なからずいることだろう。自分の記事が他人を傷つけたり、思わぬ誤解を抱かせてしまったこともあるだろう。リアル（実世界）の人間関係が複雑で難しいのと同様に、ソーシャルメディアの中での人間関係もまた複雑で難しいものである。

このような誤解や、意図せぬ反応を極力避けるためにも、記事を投稿する際は、自分の記事を様々な角度から検討した上で、慎重に投稿する必要がある。これを怠ると、予測不能なトラブルに巻き込まれる可能性があるためだ。

その極端な例として以下が挙げられる。2008年４月千葉県内の中学３年の男子生徒が、どこからか入手し、格好いいと思った服を着て撮った写真を、某プロフィールサイトに何も考えずに気軽に載せたことがきっかけで、暴走族メンバーらの怒りを買い、かれらに金属バットで殴られ、意識不明となる殺人未遂事件があった[46]−[48]。写真を載せた本人は、その服がある暴走族グループのユニフォームであることは知らなかったという。ただ気に入って載せただけであって、よもやそんなことになるとは想像すらしていなかったという。

もう少し一般的な事例は無数にある。例えば、リアルでも仲の良い高校の同級生同士が、あるブログでお互いの記事にコメントをしあう関係であった。だが、あるとき、自分の記事がその同級生を悲しませてしまった。そのような意図はなく書いた記事であったことを、誤解を解くべく何度も説明して、ようやく仲直りができた。このような経験談はよく聞かれる。

このように、ソーシャルメディアにおける情報発信（自己表現）は、ときに他人を不快にさせることもあるので、充分な注意が必要である。ここで、「情報発信（自己表現）」とは、記事、日記、ツイートを書いたり、写真、動画、音声、音楽をインターネット上に掲載したり、

コメントを残したり、コメントへのレスポンスを記入することである。

自分の記事に、反感をもったユーザからコメントをもらった際、それに対して敵意を抱き、火に油を注ぐようなレスポンスを返すと、自分のソーシャルメディアページ（サイト）が「炎上」しかねないので注意が必要である。「炎上」とは、ソーシャルメディアで発信した自分の投稿に対して、批判的なコメントが殺到する状況を指す。

6．GPSの位置情報提供システムから生じるリスク

最近の携帯電話（スマートフォンを含む）やカメラでは、初期設定でGPSによる位置情報を記録することができるものが多くなってきている。写真では、画像ファイル内のEXIF領域にGPSの緯度、経度情報を記録することで位置情報が書き込まれる。文献[49]は、EXIF、GPS、geotagに詳しい。

ここで、GPS（global positioning system）とは、米国が軍事目的で打ち上げている衛星群のシステムで、民間にも利用が開放されている。GPSでは、４個以上の衛星を同時受信することで、緯度・経度・高度・時間を知ることができるもので、携帯電話やカーナビゲーションシステムなどで利用されている。

ソーシャルメディアにおいては、発信する記事・文章に、発信時のGPSの位置情報を記録できるメディアがある。その代表例は、Facebook、Twitterである。

携帯電話自体や、携帯電話内のアプリで位置情報を利用するメリットには以下があり、便利に利用できる。

(1) 携帯電話の紛失時に、GPSを用いて現在の携帯電話のおよその場所を知ることができる。
(2) 自分の行動履歴に位置情報を追加することで、自分の日記やライフログとして記録でき、旅行の思い出づくりができる。

一方で、写真やソーシャルメディアの情報発信時に位置情報をつけるリスクには、以下がある。

(1) 閲覧者が写真の撮影・投稿場所を確認できてしまう。
(2) 記事・文章を読んだ人が、投稿者の自宅や行動履歴などを把握できてしまい、ストーカー被害や、空き巣被害にあった例がある。被害にあわなくても、自宅や行動履歴が知られてしまう。

このように危険なプライバシーリスクを冒さないためには、常にGPS位置情報を利用しない設定に変更するか、普段はGPS位置情報を記録しておくが、ソーシャルメディアに情報発信したり、写真を他人に送信するときに限ってGPS情報を記録されたEXIFデータを削除・管理する必要がある。スマートフォン向けのEXIFデータを削除・管理アプリは以下が推奨される[50][51]。

ソーシャルメディアに発信する際、「友達」限定にしておけば、GPS位置情報を削除しなくても安心という考え方もあるが、その写真を受信した人が、写真を気に入って２次利用する可能性もあるので、注意が必要である。

7．実名利用と匿名利用の長短

Facebookの利用は実名に限定されている。これに対し、Google＋は、2014年７月実名ルールが撤廃され、ニックネームなど匿名での利用も解禁された[52]。Twitter、Elloは、匿名利用がもとから可能である。Elloは、匿名利用可能なだけでなく、広告も表示されないのが特徴である。

Facebookの実名利用には、メリットもある。出身校を登録しておくと、連絡先を知らない昔の懐かしい旧友と再び連絡を取ることができるなど便利な一面がある。このような使い方は中高年世代ユーザに重宝がられ、Facebookの利用が浸透しているようである。学校に通う現役学生世代ユーザには、このようなニーズは当然な

がら少ないようである。このような世代間のニーズの違いから、若者はFacebookから離れていき、今やFacebookは中高年に人気があるようだ[53][54]。なお、Facebookでは、本名、出身校、住所、出身地、生年月日、友達リストを公開できるが、それが同姓同名の別人である可能性が0ではない。そのため、旧友と再び連絡を取る目的に利用する際は、プライバシーリスクが高まるので住所、出身地、生年月日、友達リストを公開しないことが推奨される。

8．ソーシャルメディア広告のリスク

Facebookなどで自分の好きな映画などの「趣味嗜好」を公開すると、同じ趣味を持つ同好の士と意気投合できるメリットがあるため、公開するユーザは多い。他方で、Facebookを利用しているとユーザの気を引きそうな広告が表示されるが、これは、そのユーザが公開している「趣味嗜好」項目に合わせて、広告を表示する機能である[55]。実は、ここに大きなプライバシーリスクが潜んでいる。ユーザは様々な機能を含むFacebookを無料で利用できているが、Facebookが無料で運営出来ている背景には、このようなユーザの趣味嗜好の個人データを広告業者の第三者に販売している事実があるのである。

2014年10月7日、Facebookは、広告主が広告配信のためにユーザのデータを使用できる「Audience Network」を発表した[56][57]。だが、このシステムを利用すると、Facebook広告がどこまでもユーザを追いかけてくるようになる恐れが危険視されていており、Facebook離れが加速する可能性がでている。

2013年にサービスを開始したElloは、広告を表示しない数少ないソーシャルメディアとして、2014年9月頃から爆発的な人気がでている[58][59]。Elloの人気からも、人々のプライバシー意識が顕著に向上していることが推察される。

9．検索結果の盲点

Amazon[60]、Rakuten[61]、Yahoo shopping[62]は、商品検索ができ、購入者の評価コメントを書き込めるので、ソーシャルメディアの一種であり、Safko[3]の分類では、(10) 検索に該当する。

だが、Amazon[60]、Rakuten[61]、Yahoo shopping[62]の商品検索には、プライバシーリスクが潜んでいる。例えば、Amazonには、「この商品を検索した人は、次の商品も検討しています」、「この商品を購入した人は、次の商品も購入しています」といった一見すると便利な機能がある。この機能で、ユーザは自分の検索商品と類似の別商品を知ることができる上、評価コメントを読んで、商品を比較できるという大きなメリットがある。

しかしながら、商品名と、自分の商品購入リストや検索リストが自動的に紐づけ（リンク）されていると考えると、ある種の薄気味悪さが感じられる。商品名と自分の購入の紐付け（リンク）は避けることができないが、検索のみ行う場合は、次の手順でクッキーを削除することで紐づけリスクを回避できる。

1．Amazonで商品検索前に、ブラウザのAmazonと関係のあるクッキーをすべて削除する
2．Amazonで商品検索する
3．検索後も、クッキーを削除する

ほとんどのPCブラウザでは、クッキーが削除できる。スマートフォンのブラウザアプリでも、多くの場合クッキーが削除できるので、プライバシーに留意するなら、クッキーを削除できるブラウザアプリの使用が推奨される。

このように、クッキーとプライバシーは紐づけされ、個人情報は日々関係付けられ、保存され、その量は拡大し続けている。PC用ブラウザmozilla Firefox[63]のaddonソフトのLightbeam[64]を使用すると、ブラウザを立ち上げて、ある1サイトを閲覧しただけでも、

サードパーティの多数のクッキーが即座に保存され、自分がトラッキング（追跡）されている事実が視覚的に確認できる。

ヨーロッパEUでは、次なるプライバシー保護の課題はWeb上のクッキーによるトラッキングであるとして、行政監督権限が強化される方向で議論されている[65][66]。だが、日本では、このようなトラッキングへの行政監督権限強化が即座に実行化されるわけではない。

クッキーを使うことには長短ある。商品購入時に一度訪れたサイトを再度訪問する際、ログイン処理をしなくてよいなどの便利さがある反面、自分が追跡されているというプライバシーリスクはつきまとう。そこで定期的にクッキーを全削除することが推奨される。

10. Facebookアプリのリスク

Facebookには、「Facebookアプリ」と呼ばれるアプリケーション（略してアプリ）が存在する。ゲームから実用的なツールまで様々なアプリがある。

Facebookアプリを利用するには、使用開始の条件として、Facebook内の自分のすべてのパーソナル情報（登録されている電話番号、メールアドレス、生年月日、友達リスト、友達とのやりとり、趣味嗜好）へのアクセスを要求しているものが多い。

Facebookアプリの中には、悪意のあるアプリの存在が確認されている。例えば、個人情報の収集、個人情報の外部への送信、ユーザになりすましての投稿などである。悪意のあるアプリは、スパムメール（迷惑メール）のような動きをするものもあるので、「スパムアプリ」[67]と呼ばれるものもある。

友達から紹介されたFacebookアプリを承認すると、悪意のあるFacebookアプリを知らずにインストールするリスクにさらされる。

特にスマートフォンでのFacebookアプリ利用時には、スマートフォン内部のメールアドレス、電話帳、各種サービスにログインするIDやパスワード、Webの閲覧履歴等、保存された様々な情報を外部に漏洩させる恐れのあるアプリも数多く確認されている[67]。

友達に紹介されたFacebookアプリを気軽に「承認」する前に、信頼性を確認することが必須である。プライバシーリスク逓減の観点からは、Facebookアプリは極力利用すべきでないと考えられる。また、友達をFacebookアプリに勧誘しないことが好ましい。

11. スマートフォンアプリのリスク

スマートフォンの便利さは、無数に存在する便利なアプリのお陰と言っても過言ではないであろう。スマートフォンは、一種のコンピュータなので、アプリはOS（operating system、基本ソフト）の上で動く。スマートフォンのOSには、iOS、Android、BlackBerry、Symbian、Windows Phone、Palmなど、様々なものがある。日本では、iOSとAndroidの合計が99.2％という圧倒的シェアを占めている[68]ので、以下では、iOSを搭載するiPhoneと、Androidスマートフォンについて述べる。

Androidスマートフォンにアプリをインストールするには、Google Playにアクセスして、アプリをダウンロードする。ダウンロードする過程で様々な問いかけ、すなわち「アプリの設定」が表示され、「同意」しないとダウンロードが開始されない。

iPhoneにアプリをインストールするには、App Storeにアクセスして、アプリをダウンロードする。iPhoneの場合、「アプリの設定」はダウンロード後、利用開始時に行うことになっている。一つ一つ個別に許可することが可能であり、確認しながら利用できる点においてAndroidより安全性が高いと言える。

AndroidとiPhoneの「アプリの設定」は、アプリに情報を読み取る権限を与えるものであるため、それぞれの確認が表示される都度、それが何を意味しているのかを理解して判断すべきである。6章で述べたGPS位置情報へのアク

セスも安易に許可すべきではない。カメラアプリでない場合は、カメラの利用は許可すべきではない。

不必要な権限を求めてくるアプリや、悪意のある危険なアプリをダウンロードしないためには、ダウンロード前の確認が必須である。確認の方法は、アプリの名称とアプリ開発者名で検索することで、「レビュー記事の評判」、「アプリ開発者がほかに公開しているアプリの評判」などを調べることである。

悪意のあるアプリが多数報告されている[69]。一例として、「けいおん-K-ON!動画」を含む16のアプリは、人気ゲームを動画で紹介するアプリで、ユーザの電話帳に登録されていた名前やメールアドレス、電話番号などの個人情報を勝手に外部に送信するものであった。これらアプリをインストールした人はおよそ6万6,000人から最大で27万人余りに上る。インストールした人たちの電話帳が漏洩しているので、場合によっては延べ数十万人から数百万人の大量の個人情報が流出した可能性があるとのことである[70]。その他、ウイルスを含むアプリも報告されている[71]。

単にダウンロードランキングに入っているからといって、よく調べもせずダウンロードするのは危険なので注意が必要である。

12. 人物画像に名前を付けるリスク

Facebookに集合写真を掲載して、顔にマウスを当てると、「名前を入力してください」と表示される（図1参照）。

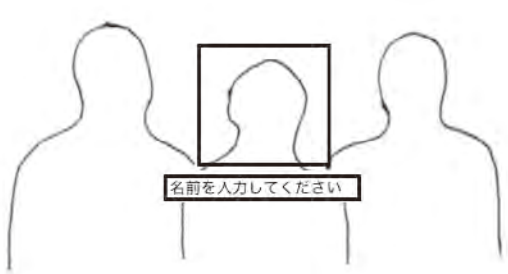

図1．Facebookの顔認識

ここで、指示されるまま名前を入力すると、それ以降、その人物写真と名前が紐付け（リンク）されて保存されることになってまう。一度、保存されると、以降似たような顔の写真すべてに、名前がリンクされることになり、大きなプライバシーリスクを招く。したがって、「名前を入力してください」という問いかけに安易に応じることは回避すべきである。

このように、Facebookで顔認識が可能になったのは、2012年6月、Facebookが顔認識テクノロジーのスタートアップ企業Face.com[72]を買収したからである[73][74]。

文献[73][74]では、8章で述べた、趣味嗜好のサードパーティ広告業者への売り渡しと同様に、Facebookは顔認識情報をサードパーティに開放するシステムの開発を呼びかけているので、人物画像のプライバシーリスクが侵食される恐れが高まっている。

これに対しては、ユーザからの批判もあって、最近Facebookは、この機能をオフ（無効化）できる設定を追加している[75]。オフにするかどうかはユーザ本人の判断によるが、他人の人物写真に名前を記入するのは、他人に上述のようなプライバシーリスクを高めることにつながり、その人に迷惑をかける恐れがあるのでやめるべきである。

13. 写真から個人情報が漏れるリスク

個人情報の保護に関する法律[76]において、個人情報とは、「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。）」と定義されている。この意味で、人物写真そのものが個人情報となる。

前章に書いたタグ付け画像に名前を付けることさえしなければ、人物写真に名前はリンクしないと錯覚しがちであるが、それこそが次なる

盲点である。

GoogleのChromeブラウザ[77]では、図２のように、「この画像をGoogleで検索」という機能があり、同じ画像が掲載される他のサイトを検索できる機能がある。この機能を使うと、同じ画像を使っている他のサイトを調べることが出来るのだ。

許可無く他人の写真や著作物を使用してはいけないが、この画像検索は、自分の写真が盗用されていないかを発見するのにも役立つものである。

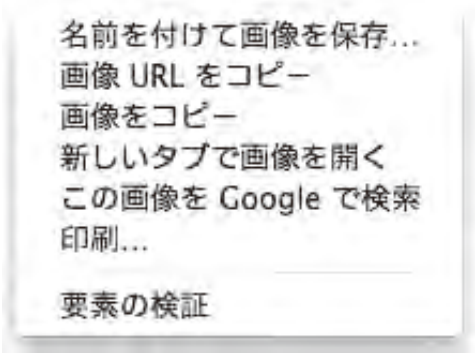

図２．Google Chromeブラウザの画像検索

しかしながら、この機能によりプライバシーリスクが発生するという盲点がある。うまく撮れた写真や、お気に入りの写真には誰しも愛着があるものである。一般的なブログ・サイトであるAmebaとFacebookの両方に、同じ写真を公開していたら、匿名で隠れて使っていたAmebaのブログが実名のFacebookとリンクして、実名が知れてしまうこともあり得る。すなわち、人物写真そのものが個人情報であることを覚えておく必要がある。

14．やり取りの相手を信用し過ぎるリスク（リベンジポルノ）

信頼できる人であっても、ソーシャルメディア上でやり取りする相手を信用し過ぎてはいけない。

LINEなど、「クローズド」なメディアにおけるやり取りは、第三者である他者にやりとりが見えないからといって、安心してしまいがちな点が盲点となる。お互い信頼しきった間柄の恋人同士で猥褻な写真を撮ったことがある人は、ある日突然自分の恥ずかしい写真を公開されてしまう、リベンジポルノという事件に巻き込まれかねない。相手が信用できると現段階で思っていても、将来にわたり、信頼し続けられる間柄でいられる保証はないと考えて行動しなければならない。安川雅史氏主催の全国webカウンセリング協議会[78]の調査によれば、子どもからのリベンジポルノ被害相談の件数が、2013年第４四半期から毎四半期80件を超えている。

このようなリベンジポルノの対策には政府も動き出し、2014年10月の国会で、公表罪法案（仮称）を審議している。公表罪[79]とは、性交やそれに似た行為の電子画像などを本人の同意なしに「第三者が撮影対象者を特定できる方法で、不特定多数に提供」した場合、３年以下の懲役、または50万円以下の罰金を課すというものである。

15．発信済み情報が削除できないリスク

オープンなソーシャルメディアでは、一度ネット上に発信した情報は簡単には削除できない。キャッシュと呼ばれる形でアーカイブサイトに残ったり、検索サイトのリストに半永久的に残ってしまうためである。アーカイブサイトは複数存在する。その１つに、https://archive.org/がある[80]。このサイトでは、図３の真ん中に、調べたいWebページのURLを入力する

図３．archive.orgの検索画面

だけで、過去のページが、更新された数だけ多数記録され、容易に閲覧できるものである。

現在の法律では、これらを削除したり、検索サイトのリストから削除するには、大変な手間と時間がかかる。ヨーロッパEUで議論されている「忘れられる権利（The right to be forgotten）」とは、本人に特定の検索エンジンにある自分のパーソナルデータを消す自己コントロール権を与えようというものである[81][82]。日本においては、まだこのような法律は存在しないので、削除には大変な困難を伴う。日本では、誹謗中傷などがあった場合にのみ、民法により削除できる場合があるが、削除依頼自体が大変な作業となってしまう。このように、オープンなソーシャルメディアで、一度ネット上に発信した情報は簡単に削除できないので、発信内容は発信前に時間をかけて何度も見直す習慣を身につける必要がある。

16. ソーシャルメディア運営会社を信用し過ぎるリスク

LINEなどの「クローズド」なソーシャルメディアであっても、その管理会社は内容を閲覧できる可能性がある。

そのような心配を解消するために、クローズドなビジネスメッセンジャーが登場した。株式会社L is B[83]が提供するビジネスメッセンジャーがその一例である。チャット、写真／動画の共有、位置情報、会議の時間調整機能などが搭載され、価格は10名6,480円から最大1,000名までの利用が可能であるという。これにより、企業秘密を保ちつつ、社員間でいわば秘密のLINEのような機能を利用可能であるという。

Dropbox[84]という、写真や文書ファイルなどのデータをインターネット上に保存しておけるサービスを提供する企業が、Dropbox business[85]という、暗号化でセキュリティ保護されたファイル共有、ストレージソリューションのビジネス向け有償提供を開始した。

LINEやFacebookやTwitterはあるとき突如として約款や設定を変更したり、断りなしにデータを利用することがある[6]。2014年6月Facebookがニュースフィードと呼ばれる部分を意図的に操作して、ユーザーの心理調査を行っていたことが発覚した。その後、Facebookは被験者への事前説明がなかったことを謝罪するも、データ利用ポリシーの範囲内のことだと主張している[86][87]。

このように、社内の企業秘密や個人のプライバシー保護のためには、ソーシャルメディア運営会社といえども信用し過ぎるとリスクが高まる点が盲点となりがちである。

17. 匿名用メールアドレス利用のメリット

LINE、Facebook、Twitterなどのソーシャルメディアにおいて、メールアドレスは重要な意味をもっている。同じメディアを使用している知り合い同士を、メールアドレスで紐付けする機能があるのが一般的だからである。

しかしながら、自分のメールアドレスを知っている人には、親しくない人も親しくしたくない人もいるだろう。そうであれば、ソーシャルメディアを使用し始めるときの、登録メールアドレスは、通常は使用しない、誰にも教えていない匿名用メールアドレスを使用するのが最善の策である。使用料フリーでメールアドレスを提供してくれるサイトもあるので、それらを使うことが推奨される。

メールアドレスと同様に匿名用携帯電話番号の確保も、格安simを利用すれば可能な時代となっている。

18. むすび

以上、本稿では、ソーシャルメディアに伴うさまざまなプライバシーリスクを先行研究や調査結果、筆者らが教育現場で収集した事例などを活用して整理し、ユーザが陥りやすい複数の盲点を示してきた。ユーザが無意識無自覚ながらも日常的に利用しているソーシャルメディア

について、その種類ごとの利用方法やリスクの差異、世代ごとに異なるニーズが存在することを明示することで、ソーシャルメディアが潜在的に抱えるプライバシーリスクの全容がある程度明示出来たと思われる。

インターネット上のソーシャルメディアは本来人とのつながりを無限に広げ、無数の情報と繋がることができる大変便利なコミュニケーションツールである反面、盲点になりがちな種々のリスクも包含する点で油断できないツールでもあることが改めて確認された。

インターネット上にひとたび拡散した情報は、それが隠したい情報であれ、誤報であれ、現在の日本社会では簡単には取り下げることが出来ない。そのため、特にその情報がプライバシーにかかわる内容である場合には、知らぬ間に犯罪のターゲットにされたり、日常生活に差し障るリスクにさらされるおそれもある。ソーシャルメディアの利用が手軽に気軽に便利になった半面、様々に気づきにくいリスクも増していることを十分に理解し、その長所を上手に活用するユーザが増えることを期待したい。

謝　辞

査読者に有益なコメントをいただいた。ここに記して感謝申し上げる。

【参考文献】

［1］総務省：『平成26年版情報通信白書』，インターネットの利用状況，http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/html/nc253120.html（accessed 2014. 12. 10）.
［2］日本のSNS利用者，4,965万人でネット利用者の過半数超え……ICT総研によるSNS利用動向調査，http://www.rbbtoday.com/article/2013/05/30/108575.html
［3］Lon Safko: The social media bible, 3/e, Hoboken, N. J.: Wiley, 2012.
［4］増田良文：ソーシャルコンピューティング入門，サイエンス社，2013. 3. “第7章ソーシャルメディア”，pp. 105-118.
［5］CiNii http://ci.nii.ac.jp/
［6］小林慎太郎：パーソナルデータの教科書，日経BP，2014. 8. p. 100.
［7］MMD研究所：「2014年4月携帯端末購入に関する定点調査」，2014. 4.
［8］内閣府：「平成25年度青少年のインターネット利用環境実態調査」，2014. 2.
［9］鈴木英男，安岡広志，圓岡偉男，神野建，新島典子：「本人追跡性を基礎とする携帯電話の情報モラル教育」東京情報大学研究論集，Vol. 16，No. 1，pp. 23-32（2012）.
［10］Facebook http://www.facebook.com/
［11］mixi http://mixi.jp/
［12］google＋ http://plus.google.com/
［13］Ello http://ello.co/
［14］Instagram http://instagram.com/
［15］Tumblr http://www.tumblr.com
［16］YouTube http://www.youtube.com
［17］Twitter https://twitter.com/
［18］Ameba http://ameblo.jp
［19］FC2 blog http://blog.fc2.com
［20］Yahoo blog http://blogs.yahoo.co.jp
［21］livedoor blog http://blog.livedoor.com
［22］nicovideo http://live.nicovideo.jp
［23］Ustream http://www.ustream.tv
［24］Podcast https://www.apple.com/jp/itunes/podcasts/
［25］secondlife http://secondlife.com
［26］google http://www.google.co.jp
［27］Yahoo http://www.yahoo.co.jp
［28］LINE http://line.me/ja/
［29］WhatsApp http://www.whatsapp.com/
［30］微信（WeChat）http://www.wechat.com/
［31］Skype http://www.skype.com/ja/
［32］kakao http://www.kakao.co.jp
［33］Viber http://viber.co.jp
［34］「5大ソーシャルメディアのユーザー数まとめ！Facebook，Twitter，LINE，Google＋，YouTube」2014. 5. 16. http://news.mynavi.jp/news/2014/05/16/324/（accessed 2014. 12. 10）.
［35］Facebook Reports First Quarter 2014 Results,（accessed 2014. 12. 10）, http://investor.fb.com/releasedetail.cfm?ReleaseID=842071
［36］2013年9月末ad:tech TOKYOにてFacebook Japan代表取締役社長　岩下充志氏による発表.
［37］Twitterを利用している人，https://business.twitter.com/ja/whos-twitter（accessed 2014. 12. 10）.

［38］2013 Japan Digital Future in Focus by comScore, 2013. 10. 14, http://www.comscore.com/jpn/Insights/Presentations-and-Whitepapers/2013/2013-Japan-Digital-Future-in-Focus（accessed 2014. 12. 10）.
［39］LINE 2014年10月－2015年３月期　媒体資料,（accessed 2014. 12. 10）, http://linecorp.com/ads/pdf/FE76CFE8-2904-11E4-9C1C-6FEF6D90A4FF
［40］「LINE登録ユーザー数，5.6億人突破　実際利用は1.7億人」，日本経済新聞電子版，2014. 10. 9. http://www.nikkei.com/article/DGXLASDZ09H5D_Z01C14A0000000/
［41］2014. 10. 9開催，LINE事業戦略発表会「LINEカンファレンス」にて発表.
［42］井関，金光，金，鈴木，花田：『情報ネットワーク概論』，コロナ社，2014. 10. p. 124.
［43］privatter http://privatter.net/
［44］Facebookを利用する上での注意，Facebookの危険性についてまとめ，http://matome.naver.jp/odai/2130720299046181301（accessed 2014. 12. 10）.
［45］Danah Boyd: It's Complicated, the social lives of networked teens, New Haven: Yale Univ. Press, 2014.“chap 2 Privacy,”pp. 54-76.（翻訳）野中モモ訳：つながりっぱなしの日常を生きる，草思社，2014. 10.“２章　プライバシー”，pp. 87-123.
［46］毎日新聞　2008年４月24日　東京朝刊：千葉・柏の中３重体：少年らプロフに「やっちゃうか」書き込み，https://web.archive.org/web/20080517231722/http://mainichi.jp/select/jiken/news/20080424ddm041040177000c.html（accessed 2014. 12. 10）.
［47］毎日新聞　2008年５月14日　東京朝刊：千葉・柏の中３重体：プロフ巡り殴打，17歳を殺人未遂で家裁送致－地検支部,（accessed 2014. 12. 10），https://web.archive.org/web/20080517051515/http://mainichi.jp/select/jiken/news/20080514ddm012040024000c.html
［48］柏プロフ殺人未遂事件について，http://d.hatena.ne.jp/dacs/20080517（accessed 2014. 12. 10）.
［49］水谷正大：写真に埋め込まれたGPSデータ，（accessed 2014. 12. 10），http://www.ic.daito.ac.jp/~mizutani/gps/gps_in_photo.html
［50］写真の位置情報・Exif情報を管理/削除するiPhoneアプリ，http://app-liv.jp/hobbies/images/1875/（accessed 2014. 12. 10）.
［51］写真の位置情報・Exif情報を管理／削除するAndroidアプリ，http://android.app-liv.jp/hobbies/images/1875/（accessed 2014. 12. 10）.
［52］Google＋の実名ルールが撤廃，ニックネームなど匿名での利用も解禁，2014. 07. 16，http://appllio.com/20140716-5478-google-plus-goes-real-name-rule（accessed 2014. 12. 10）.
［53］J-CASTニュース2013/11/25，フェイスブック，世界中で「若者離れ」「おじさん世代」のSNSになってしまうのか，http://www.j-cast.com/2013/11/25189977.html（accessed 2014. 12. 10）.
［54］若者のフェイスブック離れ！衰退する危険すぎるフェイスブック！，http://matome.naver.jp/odai/2139139933148483501（accessed 2014. 12. 10）.
［55］日本経済新聞2013/8/14電子版，フェイスブック，国内利用者2,100万人にスマホ広告強化へ,（accessed 2014. 12. 10），http://www.nikkei.com/article/DGXNASDD130C2_T10C13A8TJ0000/
［56］Facebook's Audience Network: Open for Business,（accessed 2014. 12. 10）, https://developers.facebook.com/blog/post/2014/10/07/audience-network
［57］フェイスブック広告がどこまでもユーザーを追いかけてくるようになる？，http://readwrite.jp/archives/14752（accessed 2014. 12. 10）.
［58］利用者急増SNS「Ello」とは？フェイスブック難民が殺到する新サービス，http://matome.naver.jp/odai/2141208002740151901（accessed 2014. 12. 10）.
［59］「反フェイスブック」の新SNSに入会希望が殺到，（accessed 2014. 12. 10），http://www.afpbb.com/articles/-/3027440
［60］http://www.amazon.co.jp/
［61］http://www.rakuten.co.jp/
［62］http://shopping.yahoo.co.jp/
［63］http://www.mozilla.jp/
［64］Lightbeam https://www.mozilla.org/ja/lightbeam/
［65］夏井高人：EU：Web上の行動追跡に対する規制強化の方向へ，2014. 11. 29，http://cyberlaw.cocolog-nifty.com/blog/2014/11/euweb-4e70.html（accessed 2014. 12. 10）.
［66］Europe's next privacy war is with websites silently tracking users, the Guardian, 2014. 11. 28, http://www.theguardian.com/technology/2014/nov/28/europe-privacy-war-websites-silently-tracking-

users（accessed 2014. 12. 10）.
［67］日立ソリューションズ，http://securityblog.jp/fb_guide/page04.html, http://securityblog.jp/dailylife/u_vol2.html（accessed 2014. 12. 10）.
［68］カンター・ジャパン，http://kantar.jp/whatsnew/2014/03/03/NewsRelease_140304_ComTech.pdf（accessed 2014. 12. 10）.
［69］【注意喚起】危険なスマホアプリ一覧，http://matome.naver.jp/odai/2133433099258226201（accessed 2014. 12. 10）.
［70］スマホアプリ　情報大量漏洩か，NHK NEWSweb, 2012. 4. 13, https://web.archive.org/web/20120413082637/http://www3.nhk.or.jp/news/html/20120413/t10014429731000.html（accessed 2014. 12. 10）.
［71］IPA最近のスマートフォンのウイルス事情，http://www.ipa.go.jp/files/000008930.pdf（accessed 2014. 12. 10）.
［72］http://face.com/
［73］Facebook Scoops Up Face.com For $55-60M To Bolster Its Facial Recognition Tech（Updated）, http://techcrunch.com/2012/06/18/facebook-scoops-up-face-com-for-100m-to-bolster-its-facial-recognition-tech/（accessed 2014. 12. 10）.
［74］Facebook，１億ドルでモバイル顔認識テクノロジーのFace.comを買収，http://jp.techcrunch.com/2012/06/19/20120618facebook-scoops-up-face-com-for-100m-to-bolster-its-facial-recognition-tech/（accessed 2014. 12. 10）.
［75］Facebook写真のタグ付けに関するヘルプ，https://www.facebook.com/help/463455293673370（accessed 2014. 12. 10）.
［76］個人情報の保護に関する法律，http://law.e-gov.go.jp/htmldata/H15/H15HO057.html（accessed 2014. 12. 10）.
［77］http://www.google.co.jp/chrome/
［78］全国webカウンセリング協議会，http://webcounseling.biz/page18（accessed 2014. 12. 10）.
［79］リベンジポルノ防止へ「公表罪」自民案，最高懲役３年，朝日新聞デジタル，2014. 10. 9,（accessed 2014. 12. 10），http://www.asahi.com/articles/ASGB94K0RGB9UTFK003.html
［80］https://archive.org/
［81］Factsheet on the “Right to be Forgotten” ruling（C-131/12）, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf（accessed 2014. 12. 10）.
［82］瀧口範子：「忘れられる権利」の行使にグーグルがしっぺ返し，2014. 7. 8，http://www.newsweekjapan.jp/column/takiguchi/2014/07/post-861.php（accessed 2014. 12. 10）.
［83］http://www.dropbox.com/
［84］https://www.dropbox.com/ja/business
［85］https://direct4b.com/ja/
［86］米フェイスブックが謝罪，投稿操作し心理実験論文で発覚，日本経済新聞，2014. 7. 2,（accessed 2014. 12. 10），http://www.nikkei.com/article/DGXNASGM0100I_S4A700C1000000/
［87］フェイスブックの心理実験は「逸脱」，米当局に苦情申し立て，AFP，2014. 7. 4，http://www.afpbb.com/articles/-/3019685（accessed 2014. 12. 10）.