

## 「インターネット・サービスとプライバシー問題」

市川類@JETRO/IPA NY

### 1. はじめに

近年、インターネットの進展により、世界における情報の流れは、飛躍的に増大しつつある。これに伴い、個人に係る情報の流れにも大きく変化しつつあり、その結果、プライバシーに係る問題・懸念が、これまでになかった新たな側面において提起されつつある。

インターネットの進展により、個々の利用者は、検索エンジンを活用することにより、ウェブを通じて、コストをほとんどかけることなく情報を入手することが可能になりつつある。また、そればかりでなく、個々の利用者が、自らの情報を、ウェブを通じて世界全体に対して、発信することができるようになった。このような流れの中で、インターネット・サービスがビジネスとして急成長してきている。これらのビジネスでは、多くの場合、最新の技術を駆使して、個人情報を集積することにより、当該個人に最も適した情報提供などの各種サービスを提供している。

しかしながら、これらのサービス提供にあたって利用される個人情報に関しては、その取り扱いに対する基準や共通理解が必ずしも存在せず、その結果、プライバシーに係る懸念が、従来とは異なった新たな課題として提起されつつある。また、これらのビジネスはボーダレスなインターネットという環境で提供されることから、グローバルな問題としても議論の対象となる。さらに、特に米国においては、テロ対策等の国家安全保障の観点からのプライバシーを一定程度制限すべきとの議論もあり、問題を複雑にしている。

本報告においては、米国におけるこのようなインターネット・ビジネスとプライバシーに係る最新の現状を報告する。

### 2. プライバシーとインターネット・サービスの関係

#### (1) ビジネスにおける個人情報の利用とプライバシー問題

プライバシー問題とは、一般的には、個人に属する情報（個人情報）が、当該個人の望まれない形で利用され、あるいは、外部に提供される（漏洩される）ことによって生じる各種の問題であると考えられる<sup>1</sup>。一般的に、企業（ビジネス）

<sup>1</sup> 『Privacy Lost』の著者 David H. Holtzman は、プライバシーには3つの基本的な意味があるとしている。その3つの権利とは、a) Seclusion(隔離): 他人から認知されないように隠れている権利、b) Solitude(孤

にとって、個人情報に限らず情報を適切に入手しそれを効果的に活用することは、利益を生み出す源であるとともに、その利用者にとっても、利便性の高いものとなることが多いことから、その適切な範囲での利用が求められる。そのような観点から、企業（ビジネス）におけるプライバシーの問題を考えた場合、個人情報に係る利用あるいは外部提供の範囲に関し、以下のように分類されるものと考えられる。

- ① 個人から得た情報に関し、当該個人の理解の下、明示された目的の範囲内で利用する場合（企業内のみで利用する場合、限定された範囲内で他の特定企業で利用する場合）
- ② 上記で明示された以外の目的に、意図的に使用する場合（企業内で目的外に利用する場合、企業が意図的に他の企業等に対して当該個人情報の売買・取引を行う場合）
- ③ 非意図的に漏洩する場合（企業のミスにより漏洩する場合、外部からの悪意あるものにより漏洩する場合）

このような中で、企業が如何にプライバシーを保全するかについては、二つの視点が存在する。

一つ目は、企業として IT セキュリティを含めた企業における情報管理に対する信頼性の問題である。一般的には、企業における個人情報の管理としては、①の場合に限定して行うことが望ましいとされる。しかしながら、その場合でも、実態としては、他の企業など情報が拡散されるにつれ管理が甘くなったり<sup>2</sup>、あるいは、目的の範囲に関して認識の差が存在するなどにより、実態として、②の場合のように、情報が幅広く拡散すると、それだけ、個人が情報をコントロールできる可能性が低くなり、プライバシー問題に発展する傾向が強まる。さらに、この情報の拡散範囲が広がるにつれ、③にいたるリスクも高まっていく。実際にそのような問題が生じていることから、プライバシーが情報セキュリティとも言われるゆえんであり、また、企業に対する不信感と合わさって、プライバシーが問題となる。

このような観点から、企業においては、まずは、①の場合に限定すべく、プライバシー・ポリシーを作成し、当該個人の了承を得た上で、個人情報を利用するとともに、③の場合に至るリスクを最小限にすべく情報セキュリティ対策などの

---

独): 1人にしておいてもらう権利、c) Self-determination(自決): 自分自身の情報をコントロールする権利であり、これらが何らかの形で侵害されることによって、プライバシーの問題が発生すると見ている。本稿では、このうち、特に上記c)の観点から論ずる。

<sup>2</sup>しかし、限定された「特定企業」の定義が明確でないケースも多く、例えば Robert O' Harrow, JR. *No Place to Hide* (2005)に指摘されるように、パートナー企業という曖昧な情報共有の対象範囲を設定されることによって、広範に情報が流通する懸念もあり、結果として、上述の②、③になる可能性は否定できない。

取り組みを行っている。また、このような、企業における個人情報利用を規律付け、プライバシーに関わる問題を防ぐための法律も制定されている。例えば、米国連邦政府の中で、消費者の利益を保護する立場から消費者のプライバシー保護における中心的な役割を担っている機関 Federal Trade Commission (FTC)<sup>3</sup>のプライバシー推進イニシアティブ情報公開 Web ページに挙げられた、主な米国のプライバシー関連法は以下の通り<sup>4</sup>。

主な消費者プライバシー保護に関する法律

法律	概要
Federal Trade Commission Act <sup>5</sup>	同法に基づき、FTC は企業のプライバシー保護の保証を強化させることによって、企業による消費者情報の収集・利用及びその情報セキュリティ保持の方法に関する不正・詐欺を防ぐ。
Gramm-Leach-Bliley Act <sup>6</sup>	同法に基づき、FTC は個人の財務プライバシーに関する通知及び個人情報の管理面、技術面及び物理的な面での保護について規制を導入することで、不正に情報を入手する手法プレテクスティング (pretexting) を防止する。
Fair Credit Reporting Act <sup>7</sup>	同法は消費者に関するレポート (consumer reports) の正確性を向上させ、同時に同レポートに含まれる情報のプライバシーを保護することを目的とする。
The Children's Online Privacy Protection Act <sup>8</sup>	同法は、オンライン上で自分の子供について収集される情報及びその利用法について、親権者にそのコントロールの権利を与えるというもの。

二つ目は、個人情報管理に係る国家的な関与の問題である。国は、国家安全保障 (ナショナルセキュリティ) や治安の維持、公序良俗などの観点から、国家権力をもって、企業に集められた個人のプライバシーに関わる情報を取得し、場合によっては、その情報に基づき権力の行使を行う場合がある。もちろん、国家が取得した個人情報は必ずしも公開されるものではないが、利用者から見れば、特

<sup>3</sup> <http://www.ftc.gov/privacy/>

<sup>4</sup>なお、米国のプライバシー関連の法律は、不動産法などと対照的に最近になってやっと法律問題として認識されるようになった個人の保護されるべき権利と考えられている。

<http://www.rbs2.com/privacy.htm#anchor222222>

<sup>5</sup> <http://www.ftc.gov/ogc/ftcact.shtm>

<sup>6</sup> <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>

<sup>7</sup> <http://www.ftc.gov/privacy/privacyinitiatives/credit.html>

<sup>8</sup> <http://www.ftc.gov/privacy/privacyinitiatives/childrens.html>

に国家から監視されているという不安も含めて、プライバシーの維持に対する懸念に影響を与えることになる。したがって、国家的観点といえども、このような観点も含めて、どのような場合に、どの程度の国への情報の提供が認められるのかが大きな論点となる。

この点に関し、特に米国においては、2001年9月11日の同時多発テロ以降、テロ対策と引き換えに個人のプライバシーが警察・諜報機関などによって侵害されることをやむなしとする風潮などが出てきており、また、一方で、それに対する反発、あるいは、国民の危機意識としてプライバシー保護に対する関心が高まってきた。

## (2) インターネット・サービスとプライバシー問題（本稿の議論の範囲）

### <従来における米国のプライバシー問題：社会保険番号>

このようなプライバシーに係る問題は、インターネットが普及する以前から存在している。特に、これらのプライバシーに係る問題は、個人を特定する情報と、その当該個人の属性を示す情報がデータベースとして連結されることによって、電子情報として、利用面でも問題面でも強力なものとなるが、そのうち前者の個人を特定する情報基盤として、社会保障番号（Social Security Number: SSN）は、従来から、米国における個人情報の扱いにおいて高い関心を呼んできた。

SSN<sup>9</sup>は、本来、納税管理、社会保障等において個人を特定することが主たる目的だが、現実にはそれ以外にも多くの場所で利用されてきた。例えば、米国で生活するにあたり、電話サービスに加入するにも、クレジットカードを作成するにも、すべてこのSSNの記入が必要とされる。消費者からSSN番号を受け取った事業者は、信用調査機関（credit report bureaus）に対して、同番号を送り、当該消費者の信用調査を入手、それに基づき、サービス提供の可否を決定、利率の決定、サービス内容の決定等を行っている。この結果、SSNの番号を事業者に提供した場合、事業者においては、既に、個人の信用度等を示す各種情報とデータベースで連結されるに至っており、その意味でSSN自体が既に重要な個人情報であるとの位置づけになっているといえる。

この結果、SSNが、自らの管理の手が届かないところで利用されていることに多くの消費者はプライバシーを侵害されている危機感を感じており、約9割の米国市民が、州政府や連邦政府はSSNの利用可能性及び利用そのものを禁止・制限する法律を、成立させるべきだと考えているとの指摘がある<sup>1011</sup>。また、米国では、

<sup>9</sup>米国政府が発行するユニークな9桁の番号で、米国民だけではなく、永住権を持つ外国人及び永住権をもたないが米国で就業している外国人にも発行されている。

<sup>10</sup>[http://www.informationweek.com/story/showArticle.jhtml?articleID=201805228&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201805228&cid=RSSfeed_IWK_News)

<sup>11</sup> [http://www.consumersunion.org/pub/core\\_financial\\_services/004860.html](http://www.consumersunion.org/pub/core_financial_services/004860.html)

こうした「SSN の広範囲な利用によって、ID 窃盗が容易になっており、年間約 1 千万件の事件がおきて」と消費者団体 Consumer Union<sup>12</sup>の Jeannie Kenney は Information Week 誌にコメントしている<sup>13</sup>。このような中で、GAO は、事業者が SSN 情報を提供する場合の提供方法の標準化（SSN の提供桁数など）について、法制化すること及び SSA にその権限を与えることを議会に検討するように求めている。<sup>14</sup>

一方で、テロ対策等近年の国家安全保障面での関心の高まりを踏まえ、2005 年に、Real ID Act<sup>15</sup>が成立しており、これに基づき、国家安全保障省（Department of Homeland Security: DHS）は、新たに国民にバーコードを組み込んだ運転免許証（もしくは運転資格を持たない人に運転免許証の代わりに州政府が発行する ID カード）を発行するという国家 ID 計画「Real ID」を 2008 年 5 月から開始することとしている<sup>16</sup>。本計画は、SSN と切り離すことにより、現在のプライバシー保護を想定しているが、やはり、国家によるプライバシーの侵害をさらに強めるものとして反対も多い<sup>17</sup>。

<sup>12</sup><http://www.consumersunion.org/>

<sup>13</sup>[http://www.informationweek.com/story/showArticle.jhtml?articleID=201805228&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201805228&cid=RSSfeed_IWK_News) ;さらに情報化社会を象徴し、様々な分野で個人情報の利用が価値を生み出すことから、インターネットを使った SSN 情報提供事業者もかなりの数に昇っている。Government Accountability Office (GAO) が 2006 年 5 月に発表した調査報告書 (<http://www.gao.gov/new.items/d06495.pdf>)によれば、現在、154 のインターネット情報小売業者が SSN に関連したサービスを提供していることが判明した。こうしたサービスの多くは、個人の背景調査や犯罪歴を調べるために利用されている。

<sup>14</sup> <http://www.gao.gov/new.items/d06495.pdf>

<sup>15</sup> <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR01268:@@L&summ2=m&>

<sup>16</sup> [http://www.news.com/8301-10784\\_3-9771953-7.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://www.news.com/8301-10784_3-9771953-7.html?part=rss&subj=news&tag=2547-1_3-0-20); しかし、同計画も数え切れないほどのプライバシー及びセキュリティ上の不備があるという指摘が出ている。例えば、カード上の二次元バーコード情報を暗号化を義務付けられていないため、プライバシーの侵害を目的とする悪意ある者がカード情報を外部から読み取ることができるなどの問題が懸念されている。

<sup>17</sup>例えば、プライバシー問題を懸念する消費者団体などが中心となって結成している Privacy Coalition(<http://www.privacycoalition.org/>)は、Real ID 計画を阻止するためのキャンペーンを展開、2007 年 3 月 9 月付けで DHS が発表した立法提案通知 (Notice of Proposed Rule Making: NRPM) に対して、これに反対するコメントを提出するよう、働きかけを強めた。

同キャンペーンでは、「他の連邦政府機関と一緒に、DHS の権力が、この国の国民の日々の生活にまで手を伸ばすということはこれまで前例のないことだ。この機関 (DHS) は、ハリケーン・カトリーナ被害を受けた人々を助ける責任を負っていたにもかかわらず、そうした課題に対処できる状態にないことを自ら証明した機関である。国家 ID システムを作るということは巨大で複雑なプロジェクトであり、連邦政府機関においてこの大規模なプロジェクトを管理できると証明できることはない」とした<sup>17</sup>。同コアリションに参加する団体は 45 団体 (IT 関連では、[Center for Digital Democracy](http://www.centerfordigitaldemocracy.org/)、[Electronic Frontier Foundation](http://www.electronicfrontierfoundation.org/)、[Electronic Privacy Information Center](http://www.electronicprivacycenter.org/) など) で、同コアリションの活動と足並みをそろえて個別の活動を展開しているグループは 16 団体に上る。

<http://www.privacycoalition.org/>

Docket #DHS-2006-0030 Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes at

[http://www.dhs.gov/xlibrary/assets/nprm\\_realid.pdf](http://www.dhs.gov/xlibrary/assets/nprm_realid.pdf)

### <インターネットの普及に伴う新たなプライバシー問題>

このような個人を特定できる SSN という情報基盤を含む従来からの問題に加え、近年のインターネットの普及に伴い、プライバシー問題に関し、以下の2つの新たな変化が生じてきている。

#### ①検索技術の進展

近年のインターネットの普及、さらには Google をはじめとする検索エンジン技術の発展に伴い、それまで物理的に情報を入手する必要があった個人情報、ネットワークを通じて瞬時に得られるだけでなく、無料でインターネット上から入手できるような状況を生み出している。

これにより、以前は、「知る権利」が確保されつつも、実際に入手するには非常に手間暇が掛かり、入手されることがほとんどなかった情報が、インターネット上にアップされている限り、圧倒的に容易に入手が可能となった。特に、検索技術の向上により、従来であれば知られることができる可能性が極端に低かった情報までが、目的を持って情報を収集しようとする個人・組織が検索エンジン等を利用することにより、容易に見つけられるような世界になりつつある。

#### ②インターネット・サービスの進展

インターネット・サービスとは、基本的には、消費者である個人が、インターネット上で自ら情報を入力し、その情報に基づいて、インターネット上の情報や商品・サービスの販売などの各種サービスの提供を行う事業形態であると位置づけられる。具体的には、ポータル、検索による情報と広告を提供する Google や、Yahoo!、商品販売、オークションなどの Amazon、eBay などの事業であり、これらのサービス事業は、米国内を問わず、インターネット技術の発展に伴い、近年著しい伸びを示している。

このようなサービスにおいては、これまでになかった個人情報が事業者に蓄積され、あるいは公に公開されることになる。すなわち、まずは、これらのサービスでは、消費者が自らの情報を入力し、事業者としては、それらの情報を蓄積することにより当該消費者に最も適したサービスを提供することがビジネス・モデ

<http://www.privacycoalition.org/stoprealid/>

一方、IT 業界を代表する業界団体 Information Technology Association of America (ITAA) は、基本的には同プロジェクトに賛成しているものの、いくつかの課題があることを認識しており、上記 NRPM に対して、5月8日付けでコメントを提出している<sup>17</sup>。これによれば、Real ID 導入における2つの障害として、①適正なポリシー、手続き、トレーニングについて確立すること、②同カード導入の実施責任を負うことになる州政府に対して、その資金負担を連邦政府も負うことを挙げている。特に後者については、ITAA は議会にも働きかけを行っている。

[http://www.ita.org/es/docs/ITAA\\_RealID\\_Comments2007.pdf](http://www.ita.org/es/docs/ITAA_RealID_Comments2007.pdf)

[http://www.washingtontechnology.com/online/1\\_1/31487-1.html](http://www.washingtontechnology.com/online/1_1/31487-1.html)

ルとして求められる。また、事業者の情報提供サービスの一環として次々とインターネットに情報がアップロードされることになる。このような状況において、前者に関しては、これらのサービスの利便性と、消費者が入力した情報に関してプライバシーとのバランスをどう考えるか、また、後者においては、公開情報であれば個人情報であっても、全てアップロードして構わないのかといった点について論点となる。また、このように新たに蓄積される情報に関して、国家安全保障の観点等から国がどこまで傍受、検閲することが認められるのかといった問題も発生する。

#### <本稿での対象>

本稿においては、このような整理の下、特に、上述のインターネット・ビジネスの進展に伴って、近年新たに生じてきているプライバシーに係る新たな懸念をめぐる動向を中心に、それに加えて、9/11以降高まっている国家安全保障の観点から国家が個人情報を管理する動き等に係る議論を紹介する。

なお、プライバシーの侵害に関しては、いわゆるITセキュリティ問題（ID窃盗など）や企業のミスの結果生じた情報漏洩により、実際に被害として明確になる場合が多いと考えられるが、これらについては、本稿では扱わない。

### 3. インターネット・サービスにおいて生ずる新たなプライバシー問題

#### (1) 概要

前述のとおり、インターネット・サービスは、具体的には、利用者が入力する情報を活用して、ウェブ上での情報提供その他のサービスの提供を行うものであり、近年、そのサービスの内容は益々拡充され、それに伴い、個人が入力する情報の範囲も拡充する傾向にある。このようなインターネット・サービスへの移行は、従来のデスクトップ内でのソフトウェアでのサービスでは、原則として<sup>18</sup>物理的には情報が他者に流れることはありえなかったものに対し、情報をむしろ当然の前提として当該サービス提供会社に預けるという構造に変化していることを意味しており、したがって、当該サービス提供会社が、安心して情報を預けられるに足る企業なのかという視点が重要になる。

具体的な情報の内容としては、検索履歴、あるいは商品の購入履歴に加え、近年においては、ウェブ上でのメール・サービス、あるいは、文章、書類作成ツールを提供するウェブ・アプリケーション・サービスなどの普及により、これらによって入力される情報も、当該サービス提供企業に蓄積されることになる。これらの情報は、一般的には、個人に最も適したサービスを提供する等利用者の利便

<sup>18</sup> もちろん、これらの場合でも、CD-ROM等を通じた漏洩や、ハッキングなどを通じた漏洩はある。

性の観点からは、企業として保持することが望まれる一方で、その場合における企業における個人情報の保全が、従来にも増して必要となってくる。

また、さらに、インターネット・サービス企業においては、情報提供サービスの拡充の観点から、これまでウェブ上にはなかった情報を収集し新たにアップロードするなどの取り組みを進めたり、あるいはソーシャル・ネットワーク・サービス（SNS）などに見られるように、個人が自らの情報を、インターネット・サービス会社だけでなく、他者に対して提供することによって成り立つウェブサービスも急速に伸びつつある。これらのように意図的に公開される情報においても、一部個人情報を含む場合が存在し、このような情報に係る対応の検討が課題となってくる。

以下においては、前者の事例として、近年米国内等で議論になっている検索ログの事例、ウェブ上の文書作成サービス、また、後者の事例として、最近の地図検索における事例、SNS の事例を取り上げる。

## （２）インターネット・サービス利用に係る個人情報の扱い

### ①検索エンジン・サーバのログ<sup>19</sup>

インターネット・サービスとプライバシー問題で、現在、メディア等で大きな注目を集めているのが、検索エンジン・サーバのログに関する問題である。

#### 【問題のポイント】

Google、Yahoo!などをはじめとする検索エンジンは、ユーザが検索を行うたびに、検索クエリー、ユーザの IP アドレス、クッキーに保存された ID 情報などを含む各種情報を収集している。それと同時に、検索エンジンは、それらのデータを、特定のユーザ、Web ブラウザー及びコンピュータの種類に関連付けられた ID 情報との関連付けを行い、データベース化を行うという作業も自動的に行っている。一般的に、こうした情報を保存するという手法をとることによって、①検索結果の品質を向上させるだけではなく、②スポンサー広告の表示内容が検索結果

<sup>19</sup><http://japan.cnet.com/news/media/story/0,2000056023,20354535,00.htm>、  
[http://www.informationweek.com/story/showArticle.jhtml?articleID=201311113&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201311113&cid=RSSfeed_IWK_News)  
[http://www.news.com/How%20search%20engines%20rate%20on%20privacy/2100-1029\\_3-6202068.html?part=rss&tag=2547-1\\_3-0-20&subj=news](http://www.news.com/How%20search%20engines%20rate%20on%20privacy/2100-1029_3-6202068.html?part=rss&tag=2547-1_3-0-20&subj=news)  
[http://www.news.com/Competition%20is%20good%20for%20search%20privacy,%20report%20says/2100-1029\\_3-6201468.html?part=rss&tag=2547-1\\_3-0-20&subj=news](http://www.news.com/Competition%20is%20good%20for%20search%20privacy,%20report%20says/2100-1029_3-6201468.html?part=rss&tag=2547-1_3-0-20&subj=news)  
[http://www.informationweek.com/story/showArticle.jhtml?articleID=201200289&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201200289&cid=RSSfeed_IWK_News)  
[http://www.news.com/2100-1030\\_3-6198053.html?part=rss&tag=2547-1\\_3-0-20&subj=news](http://www.news.com/2100-1030_3-6198053.html?part=rss&tag=2547-1_3-0-20&subj=news)



とより適正に検索結果と結び付けられ、また③検索機能と広告メカニズムの不正利用の防止等に役立つと考えている<sup>20</sup>ものの、一方で、このように検索エンジンが収集・整理する情報には、多量のプライバシーに係る情報が含まれていることになる。

このような情報に係る収集・保存・利用等に関し、もちろん検索エンジンの運営会社は、一般的にプライバシー・ポリシーの公表を行っている。しかしながら、ユーザ側からみた場合、一般的に、必ずしも十分に当該プライバシー・ポリシーを認識せずに利用していることも多く、また、当該プライバシー・ポリシーを読んだだけでは、当該個人情報、実際にどのように管理・利用されているのかについて分からないとの指摘もある。最終的には、ユーザとして、当該企業によるこれらの情報管理が信頼できるか否かという判断になるが、実際には、これらの情報を検索エンジン会社が適正に管理せず、大量の個人情報がインターネット上に漏洩する事態が起こってはじめて認識が高まるとというのが現状であると考えられる。

この検索エンジン企業による個人情報に関して、問題意識を高めるきっかけとなった有名な事件は、2006年8月に起こったAOLによる情報漏洩事故である。これを報じた2006年8月9日付けNew York Times<sup>21</sup>によれば、同社の検索エンジンを使って収集された約50万ユーザによる検索クエリ・リスト約2千万件が、同社のインターネット上に公開された。目的は研究者コミュニティに広く利用してもらうことであり、悪意あるものではなかったが、これらの情報には社会保険番号（Social Security Number: SSN）などが含まれていたことなどが明らかになり<sup>22</sup>、同年9月には訴訟にも発展している。

#### 【利害関係者の意見、対応の方向】

このような検索ログに係る問題意識の高まりの中、本年春以降、各社においては、消費者のプライバシー・ポリシー保護を求める団体等の指摘や他社の動向を踏まえつつ、自らのプライバシー・ポリシーにおけるログ管理方法・期間等について、見直しを行ってきた。その結果、2007年8月8日に、インターネット上の自由を擁護する団体Center for Democracy and Technology（CDT）がまとめた、主要米インターネット検索エンジンにおけるプライバシー・ポリシーに関する評価に係る報告書「Search Privacy Practices: A Work In Progress CDT Report -- August」<sup>23</sup>においては、以下のとおりとなっている。

<sup>20</sup> <http://www.cdt.org/privacy/20070808searchprivacy.pdf>

<sup>21</sup> <http://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=print>

<sup>22</sup> <http://www.itworld.com/Man/2681/061207top10/>

<sup>23</sup> <http://www.cdt.org/privacy/20070808searchprivacy.pdf>

検索エンジンを通じて収集されたデータ保存期間<sup>24</sup>

		IP アド レス	クッキー ID	クエリ
Google		18 ヶ月	18 ヶ月	不明
Yahoo!		13 ヶ月	13 ヶ月	不明
Microsoft		18 ヶ月	18 ヶ月	不明
Ask.com	オプト・アウト 希望ユーザ	2-3 時間	2-3 時間	2-3 時間
	その他	18 ヶ月	18 ヶ月	不明
AOL		13 ヶ月	13 ヶ月	13 ヶ月

この結果によれば、Ask.com は唯一、ユーザが IP アドレス、クッキーID、検索クエリなどを長期間保存することを自らの意思で拒否できるオプト・アウトのツール「AskEraser」を提供しており、CDT はこれを、ユーザ自らが個人情報をコントロールできる手法として評価しており、他の検索エンジンに対してもこうしたツールを提供すべきという提言を行っている<sup>25</sup>。

なお、このような検索ログに係るプライバシー問題に対する認識の高まりに対し、グーグルは、対消費者向けに、オンライン用ビデオを作成、対外公表を行い、グーグル社としてどのような情報を収集しているのか、あるいはどのような対応を図っているのかについて、分かりやすく説明を行うなどの取り組みを行っている<sup>26</sup>。

②ウェブサービスによって入力・保存される情報

近年、様々なアプリケーションがデスクトップからウェブを通じた提供へと移行する中、このようなウェブ・アプリケーションとして保存される情報に関するプライバシー問題も浮上している。

【問題のポイント】

Microsoft 社のオフィス製品に対抗し、Google 社は、オンライン・アプリケーション・サービス「Google Apps」の一部として、文書、スプレッドシート等のアプリケーション・サービスである Google Docs を提供している。Google Apps のア

<sup>24</sup> CDT Search Privacy Practices: A Work In Progress CDT Report – August を基に作成

<sup>25</sup> CDT の報告書では、ユーザによる個人情報のコントロールを与えることを提案していることに加え、検索エンジン会社が集めたプライバシーに関わる情報を長期間に亘って保護すること、ユーザ・プライバシーの保護と広告目的での市場への情報提供のバランスを考慮すること、プライバシー保護実現のために、ユーザ間、検索エンジン間等のパートナーシップを促進すること、またプライバシー保護のように重要な権利は、競争原理の中で確保されるものではなく、法的な保護が必要であることを提言している。

<sup>26</sup> <http://blog.wired.com/business/2007/08/google-video-me.html>

アプリケーションは全て、ウェブベースで提供されており、ユーザは、自分が作成した文書をウェブ上で公開したり、共有することが可能となっている。同社は2007年9月、国際的なコンサルティング会社 Capgemini 社と提携し、企業ユーザを対象として、「Google Apps」の有料版である Premium Edition<sup>27</sup>を本格的に展開していくと発表している<sup>28</sup>。

このように、企業向けにオンライン・アプリケーション・サービス提供を本格化させていく中で、これらのオンライン・アプリケーションを利用して作成されたコンテンツの所有権の問題について、業界関係者が懸念を示している。具体的には、シリコン・バレーに拠点を置く企業アプリケーション・コンサルタントの Joshua Greenbaum 氏は、2007年8月、企業向け IT 関連情報のニュースサイトのブログ投稿（2007年8月27日）において、企業ユーザに対して、Google 社のオンライン・アプリケーション・サービス Google Docs を利用する際の危険性を呼びかけた<sup>29</sup>。すなわち、同利用規約の一節<sup>30</sup>には、同サービスを利用したコンテンツは全て Google 社によって利用されることが前提としていると解釈され、「一般のユーザには無視されがちなサービスの利用規約であるが、利用規約に十分注意を払わずに、企業が同社のサービスを利用した場合、Google 社のマーケティング・キャンペーンなどにおいて、企業の IP アドレスが公表される危険性がある」と指摘している。

#### 【利害関係者の意見、対応の方向】

このような懸念・指摘を受けて、2007年9月、Google 社の Australia 支局は、Google Docs を利用して作成された文書の所有権など、文書のコンテンツ全てに関する権利はユーザにあり、Google 社が同アプリケーションを使ったコンテンツ

<sup>27</sup> ユーザ 1 人当たり年間 50ドルの Premium Edition では、無料で提供されている Google Apps の Standard Edition と提供されるアプリケーションの種類は変わらないが、Gmail の保存容量が 25GB (Standard Edition は 2GB) と大幅に拡大されるほか、データ移行、ユーザ・プロビジョニング機能および年中無休の電話サポート・サービスを提供している。

<http://www.google.com/a/help/intl/en/admins/editions.html>

<sup>28</sup> <http://www.eweek.com/article2/0,1759,2180503,00.asp>

<sup>29</sup> <http://blogs.zdnet.com/Greenbaum/?p=130>

<sup>30</sup> <http://www.google.com/google-d-s/intl/en/terms.html>; 同条項の対象部分は次の通り。

「同サービスを利用して作成されたコンテンツの著作権およびその他の権利はユーザが保持するが、ユーザは、Google 社に対して、同サービスを通じて提出、投稿、表示したコンテンツの複写、翻案、修正、発行、公演、公表および配布を行うための権利を認めるものとする。同権利は、Google 社が同サービスを幅広く普及および推進していくことのみを目的とする」"You retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the Service. By submitting, posting or displaying the Content you give Google a worldwide, royalty-free, and non-exclusive license to reproduce, adapt, modify, translate, publish, publicly perform, publicly display and distribute any Content which you submit, post or display on or through the Service for the sole purpose of enabling Google to provide you with the Service in accordance with its Privacy Policy."

を、ユーザの意思に反して利用するようなことはない」と発表した<sup>31</sup>。すなわち、「Google 社のサービス利用規約では、ユーザが他者との共有を選択した文書に限り、ユーザが共有を認めた他ユーザが文書を閲覧できるように、共有を指定された文書の表示および異なるディスプレイに適応させて文書形式を変更することを保証している。Google 社は、ユーザの統制権利を超えてまで、ユーザの文書を利用はしないということを明確にしておきたい。同社は、ユーザが指定しない限り、豪州における作業文書やスプレッドシートを他ユーザに共有することはない」<sup>32</sup>と述べ、ユーザの意思に反して、Google 社が無断でコンテンツの共有や公表を行うことは一切ない」とし、ユーザの完全なコンテンツ所有権を保証するものだとしている。

この問題に関し、豪州のニューサウスウェールズ大学<sup>33</sup>のインターネット法律・政策センター（Cyberspace Law and Policy Centre）<sup>34</sup>のエグゼクティブ・ディレクターを務める David Vaile 氏は、Google 社が「公開（Public）」の定義を明確に提示し、ユーザがコンテンツを公開および非公開にするかページごとに選択できるようなインターフェースを提供していくべきだとしている<sup>35</sup>

### ③個人情報の収集範囲拡充による影響への懸念

このようにインターネット・サービスにおいて、多様なサービスを提供することにより、それに応じた多種の個人情報を入手し、それらに応じて、行動ターゲティング広告（Behavioral Targeting Advertising : BTA<sup>36</sup>）などを行うような事業が一企業によって独占的に行われることに関し、独占禁止法上の問題に加え、個人の広範なプライバシー情報が、当該個人ではなく、企業によってコントロールされる危険性が高まるという指摘も行われている。

### 【問題のポイント】

<sup>31</sup> Greenbaum 氏の記事は米国から発せられたものであるが、これに対して対応を発表したのは Google の本社ではなく、Google Australia であった。米国では、同氏のブログに対して、多くの意見が寄せられている。Google による公式発表ではないが、そのコメントの 1 つとして、Google Docs のエンジニアリング・ディレクターと称する人物のコメントでは、同氏の解釈は間違っており、「個人で利用しているか否かにかかわらず、Google は Google Docs & Spreadsheet で作成されたコンテンツの所有権を主張するものではなく」、ユーザの目的を超えたところで勝手に Google がこれらのドキュメントを使うことはない」と述べている。

[http://digg.com/tech\\_news/The\\_Content\\_in\\_Google\\_Apps\\_Belongs\\_to\\_Google?t=8848565#c8848565](http://digg.com/tech_news/The_Content_in_Google_Apps_Belongs_to_Google?t=8848565#c8848565)

<sup>32</sup> [http://www.news.com/Google%20denies%20ownership%20of%20users%20words/2100-1030\\_3-6207535.html?part=rss&tag=2547-1\\_3-0-20&subj=news](http://www.news.com/Google%20denies%20ownership%20of%20users%20words/2100-1030_3-6207535.html?part=rss&tag=2547-1_3-0-20&subj=news)

<sup>33</sup> <http://www.unsw.edu.au/>

<sup>34</sup> <http://www.bakercyberlawcentre.org/>

<sup>35</sup> [http://www.news.com/Google%20denies%20ownership%20of%20users%20words/2100-1030\\_3-6207535.html?part=rss&tag=2547-1\\_3-0-20&subj=news](http://www.news.com/Google%20denies%20ownership%20of%20users%20words/2100-1030_3-6207535.html?part=rss&tag=2547-1_3-0-20&subj=news)

<sup>36</sup> 「行動ターゲティング広告」とは、インターネットの利用者が関心を持つテーマ・内容について、検索履歴情報を基に分析、それによって、個人の好みに合った広告を配信する手法のこと。

本問題については、Google が 2007 年 4 月 13 日に発表された大手広告会社 DoubleClick の買収計画（31 億ドル<sup>37</sup>）に関し、新たに注目を浴びてきている。すなわち、本買収により、あらゆるオンライン広告のパイプラインを Google が独占してしまうことによる非競争的状态を生み出す可能性に加え、Google が DoubleClick のオンライン最大ユーザ情報データベースを手に入れることにより、膨大なプライバシー情報を入手することになり、オンライン上の過去に例を見ない規模のデータブローカーになりうる可能性を示唆しており、そのような中、ユーザのプライバシーがどのように扱われるのかが争点の一つにあがっている。

この問題に関し、Microsoft によるオンラインマーケティング会社 aQuantive（2007 年 5 月、60 億ドル）<sup>38</sup>の買収計画、Yahoo!による自動ネット広告取引所 Right Media（2007 年 4 月、6 億 8,000 万ドル）<sup>39</sup>の買収計画なども含めて、本件に関する公聴会が、2007 年 9 月 27 日には議会上院司法委員会の反トラスト、競争政策及び消費者権利に関する小委員会<sup>40</sup>にて開かれている。

#### 【利害関係者の意見、対応の方向】

本件合併に関し、消費者保護団体の 3 団体<sup>41</sup>は、FTC に対し、Google がプライバシー保護を保障しない限り、この合併を阻止するよう求めた<sup>42</sup>。これら 3 団体は、FTC に対して、「Google も DoubleClick も収集した個人データを保護する手段について、適切な処置を取っていない。さらに、今回提案された合併では、プライバシーについて特殊なリスクを生み出すとともに、オンライン広告の運営に関連してこれまでに同意された標準規格（OECD によるプライバシー・ガイドライン<sup>43</sup>などを含む）にも違反することになる」と主張している<sup>44</sup>。この背景として、特に、今回合併対象となった DoubleClick はこれまで、プライバシーを慎重に扱わない企業としてのレッテルを貼られてきた前歴があり、それが今回の吸収合併におけるプライバシー問題がクローズアップされる原因となっていると見方もある<sup>45</sup>。

<sup>37</sup> <http://itpro.nikkeibp.co.jp/article/NEWS/20070928/283195/>

<sup>38</sup> [http://www.infoworld.com/article/07/05/18/microsoft-to-buy-aquantive\\_1.html](http://www.infoworld.com/article/07/05/18/microsoft-to-buy-aquantive_1.html)

<sup>39</sup> [http://www.news.com/2100-1024\\_3-6180268.html](http://www.news.com/2100-1024_3-6180268.html)

<sup>40</sup> <http://judiciary.senate.gov/subcommittees/110/antitrust110.cfm>

<sup>41</sup> Electronic Privacy Information Center (EPIC)、Center for Digital Democracy (CDD)及び U.S. Public Interest Research Group (US PIRG)

<sup>42</sup> <http://www.itworld.com/Tech/2428/070420epic/>

<sup>43</sup> [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html)

<sup>44</sup> <http://www.itworld.com/Tech/2428/070420epic/>

<sup>45</sup> 具体的には、1999 年、DoubleClick が Abacus Direct というデータ収集会社 (data collecting agency) を 17 億ドルで買収したことに起因する。その際、DoubleClick が、Abacus のデータベース情報に含まれる個人情報 (氏名、住所、電話、電子メールなど) と、DoubleClick のウェブ検索プロファイル・データベースを統合し、個人を特定できるような状態にすることを発表した。これに対し、プライバシー保護団体から、大きな反対運動が起き、Abacus のシステムとの統合は行わないことを発表している<sup>45</sup>。同問題を契機に同社

また、専門家においても、本買収による広告市場へのインパクトを認めつつも、DoubleClickのこれまでの振る舞いが合併後もプライバシー保護を重視しないような姿勢が継続されるのではないかという疑念を抱く指摘がみられる<sup>46</sup>

このような指摘に対し、2007年9月27日に開かれた議会公聴会<sup>47</sup>においては、Googleは、消費者の信頼を得るためにプライバシー対策に取り組むと主張し、また、Microsoftは、競争こそがプライバシーを守ると主張した。本公聴会は、「消費者のプライバシーをリスクにさらし、競争を押しさえ込むようなオンライン広告ビジネス界における怪物を作り出すことになるか」否かを議論することを目的としたものであったと翌日付Washington Post紙は報じている<sup>48</sup>。

具体的には、GoogleのDavid Drummond (Senior Vice President, Corporate Development and Chief Legal Officer)は、同公聴会の中で、特にプライバシーに関して、同社はユーザのプライバシー保護について重要と考えており、プライバシー保護の手段やポリシーについて、継続的に改善するよう取り組んでいることを強調した。また、同社のビジネス・モデルはユーザの信頼あつてのものであり、同社が集めた個人情報の取り扱いについて、ユーザが不安を感じていれば、ユーザはすぐにも他の競争相手のサービスに移ってしまうことを認識しており、それを避けるためにプライバシー保護に、企業として非常に高い優先度を付けて取り組んでいるとした<sup>49</sup>。

一方、Microsoftからは、Senior Vice President and General CounselのBrad Smithが出席し<sup>50</sup>、GoogleがDoubleClickを買収することで、同社の独占状態が強まること、また、1つの巨大企業が、膨大な情報をコントロールする状況を生み、

はプライバシー保護への取り組みを強化し、オプト・アウトのオプションを提供しているとされるものの、これはクッキーのみに対するもので、オプト・アウトされてもIPアドレスのトラッキングは行われているという調査結果を指摘する声もある<sup>45</sup>。

<http://www.wired.com/politics/law/news/2000/02/34037>

<http://www.wired.com/politics//0,1283,34734,00.html>

[http://en.wikipedia.org/wiki/DoubleClick#\\_note-3](http://en.wikipedia.org/wiki/DoubleClick#_note-3);

<http://www.elvey.com/it/spr/SPR-2001-01-22.txt>

<sup>46</sup> 例えば、Privacy Forum 創設者兼 California Initiative for Internet Privacy 共同設立者である Lauren Weinstein は、IT 業界エキスパートである Frederick Lane<sup>46</sup>のインタビューに答えて、「検索履歴と Google によって集められたその他の情報と、DoubleClick 技術を使って集められた第三者サイトに関する情報を相互に関連付ける能力は、マーケティング・ツールとして、非常にパワフルで、潜在的に非常に魅力的なものである。(中略)事業開始当初から、DoubleClick は第三者 Cookie の看板男だった。そして、同社が幅広いソースから情報を引き出し、それを中央データベースに蓄積し始めると、今度は Cookie の対抗勢力を排除する支援をした」と応えている。

[http://www.sci-tech-today.com/story.xhtml?story\\_id=51313](http://www.sci-tech-today.com/story.xhtml?story_id=51313)

<sup>47</sup> <http://judiciary.senate.gov/hearing.cfm?id=2955>

<sup>48</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/27/AR2007092701191.html>

<sup>49</sup> <http://googlepublicpolicy.blogspot.com/2007/09/our-senate-testimony-on-online.html>

<sup>50</sup> <http://www.microsoft.com/Presspass/exec/bradsmith/09-27googledoubleclick.msp>

Google はユーザのオンライン上のほぼすべての行動を記録する方向に向かっていると指摘し、その対応に向けて、健全な競争環境を維持することが必要であると考えていると主張した。

このような流れの中で、上述の Washington Post 紙によると、議会の一部では、消費者保護のための新たな法律の必要との意見もあり、下院エネルギー商業委員会の商業・貿易及び消費者保護小委員会（Subcommittee on Commerce, Trade and Consumer Protection）の Bobby Rush 議長（民主党、イリノイ選出下院議員）は、FTC に対する書簡の中で、そのような観点からの新たな公聴会開催を望むと述べたことを報じている<sup>51</sup>。

## （２）インターネット・サービスでアップロードされる個人情報の扱い

### ①地図検索における画像表示

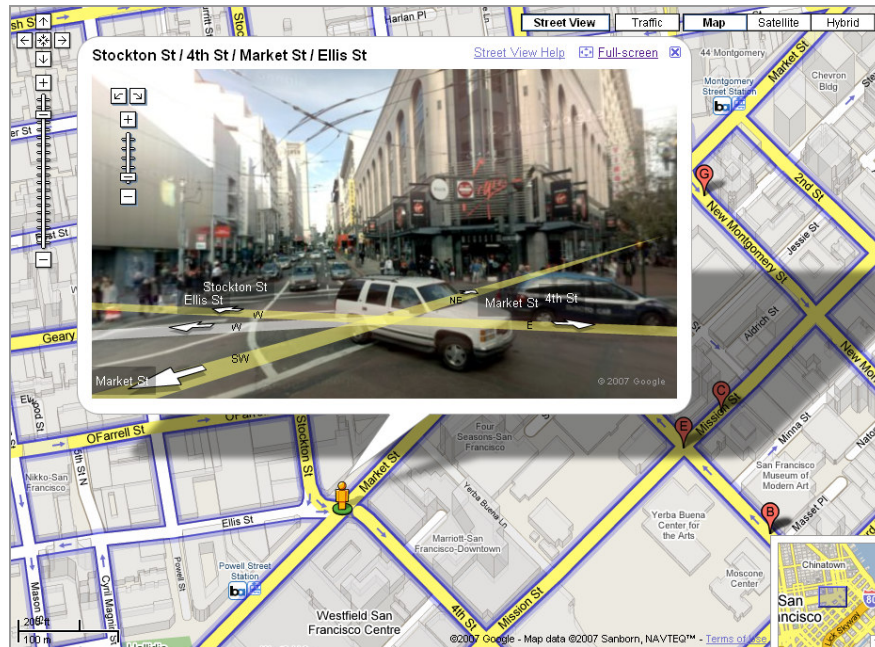
これまでの個人情報検索の基本は、文字情報をベースとしたものであった。しかし、画像・動画・音声検索といった検索技術の進展に伴い、画像を解したプライバシーの問題も浮上している。今日、カメラ付携帯電話が普及し、誰もが手軽に撮影した写真を、ブログをはじめとするインターネットに簡単に掲載できるようになってきた。しかし、写真というメディアには、背景情報として、他者やそれにかかわる個人情報が含まれている場合も多い。これを個人が自らの趣味として掲載しているうちは、大きな問題とはならなかったが、インターネット・サービス企業が、サービスの一環として、ひとつの都市の町並みを撮影、地図検索にこれを関連付けたとした場合、その背景に写された個人のプライバシー情報ほどのように扱われるのか—Google の新サービスを巡って、プライバシー侵害を懸念する声が上がってきている。

#### 【問題のポイント】

Google の提供する Google Map においては、2007年5月から、当初カリフォルニア州サンフランシスコ市とサン・ディエゴ市を皮切りに、新たに「Street View」と呼ばれる新機能によるサービス提供を開始した（2007年10月現在、米国内中西部・東海岸等の都市にも拡大され、対象都市は15都市に上る）。同機能を使うと、通りの風景が写真で映し出され、移動する方向を写真の中で選択（下図の矢印をクリック）すると、移動先の風景も次々と写真で表示されるというもの。また、ある地点での風景を360度映し出し、ズームも可能となっている。

Google Map 「Street View」 サンフランシスコ市マーケット通り交差点付近の様子

<sup>51</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/27/AR2007092701191.html>



これらの画像は、Googleが、高解像度撮影の可能なカメラを搭載した車で、これらの風景を撮影したものであり<sup>52</sup>、写真に写った個人及び個人の所有物等について、許可無く撮影し、これをインターネット上に掲載したものである<sup>53</sup>。これらの画像に含まれる通りを歩く人々や自動車などには、数多くのプライバシーにかかわる情報が含まれていると考えられ、このような情報の扱いの有り方が論点となっている。

#### 【利害関係者の意見、対応の方向】

カナダ・プライバシー・コミッショナーJennifer Stoddart 女史は、2007年9月、同機能は、カナダの個人情報保護を保護する法律である、Personal Information Protection and Electronic Documents Act (PIPEDA : 2004年1月1日施行)<sup>54</sup>に反するものだとする書簡を、Googleに送った<sup>55</sup>。すなわち、GoogleのStreet Viewでは、解像度の高い画像が利用され、クローズアップすることによって、個人の顔、自動車のナンバープレートの特特定が可能であること、また、同サービスでは、ある個人の身分を証明するような情報がオンライン上に流れた場合において、当該個人がその「被害」にあってることを認識し、かつ、Googleに対して

<sup>52</sup> [http://www.news.com/8301-10784\\_3-9764512-7.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://www.news.com/8301-10784_3-9764512-7.html?part=rss&subj=news&tag=2547-1_3-0-20)

<sup>53</sup> [http://www.news.com/8301-10784\\_3-9776962-7.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://www.news.com/8301-10784_3-9776962-7.html?part=rss&subj=news&tag=2547-1_3-0-20)

<sup>54</sup> [http://www.privcom.gc.ca/legislation/02\\_06\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_e.asp)

<sup>55</sup> PIPEDAは、「特定の状況において、収集、利用もしくは公開された個人情報を保護し、情報の交換・記録及び処理のための電子的手段の利用について規定し、Canada Evidence Act、Statutory Instruments Act及びStatute Revision Actを修正することによって、電子商取引を支援・促進するため」に作られた法律である。 <http://laws.justice.gc.ca/en/P-8.6/text.html>



その改善策を要請しない限りは画像の削除などがなされないという点についても、問題視された。

Googleは、こうした批判を受けて、Street Viewアプリケーションの提供について、カナダでは米国で提供している形態のまま提供するのではなく、個人の顔やその他個人情報に関連するものはぼかして表示することによって、個人を特定できないようにするとした<sup>56</sup>。また、米国におけるポリシーも変更され、「被害」にあった個人だけではなく、他人の顔や車のナンバープレートの番号がはっきり認識できる画像を発見した人からの通報を受けて、対処を行うこととしている<sup>57</sup>。

## ②ソーシャル・ネットワーキング・サービス（SNS）での情報<sup>58</sup>

MySpaceやFacebook、mixi（ミクシィ）などに代表されるソーシャル・ネットワーキング・サービス（SNS）は、ユーザがメールアドレスや所属団体などの個人情報を含めたプロフィールを作成し、友人とのコミュニケーションを深めたり、共通の価値観や興味を持っている者同士がグループを結成したりなど、友人・知人の輪を広げていく為に利用されている。

このSNSに関しては、SNSの人気の高まるのに比例し、SNSユーザをターゲットとした犯罪も増加していることに加え、最近問題になっているのは、こうしたSNSに登録されている個人情報がSNSサイト以外でもGoogleなどを代表する検索エンジンで容易に検索できるようになり、個人情報がさらに引き出しやすくなるという点も、問題点として指摘されつつある。

### 【問題のポイント】

Facebook社は2007年9月5日、Facebookにメンバーとしてアカウント登録をしなくても、同サイトを利用しているメンバーの検索ができる「public search listings」機能を追加すると発表した。FacebookのエンジニアであるPhilip Fung氏のブログによると、これまではFacebookのサイト上でのみ、メンバーの検索が行なえるようになっていたが、今後は、Google、MSN Live、Yahoo!などの主要検索エンジンでも検索できるよう拡張していくとしている<sup>59</sup>。なお、Facebook社

<sup>56</sup> <http://www.canada.com/nationalpost/news/story.html?id=a5052787-a013-4ed4-b9f7-44acc96f9858&k=81423>

<sup>57</sup> [http://www.news.com/8301-10784\\_3-9764512-7.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://www.news.com/8301-10784_3-9764512-7.html?part=rss&subj=news&tag=2547-1_3-0-20); 2007年10月現在、サンフランシスコの風景を写した写真を見る限りでは、まだかなりの顔が明確に識別できるレベルのまま掲載されている模様。

<sup>58</sup> [http://www.informationweek.com/story/showArticle.jhtml?articleID=201804345&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201804345&cid=RSSfeed_IWK_News)  
[http://www.mercurynews.com/ci\\_6814725?source=rss&nclick\\_check=1](http://www.mercurynews.com/ci_6814725?source=rss&nclick_check=1)

<sup>59</sup> ただし、外部から検索可能なプロフィールには、極めて限定された情報しか表示されないほか、プロフィールに掲載する内容はユーザーが自分で決定でき、プライバシー機能を使うことで、外部から検索できないように設定することもできる。

によって public search listing 機能が発表される以前から、Google などの検索エンジンを使ってメンバーのプロフィール検索は可能であった<sup>60</sup>。検索エンジンに関する様々な情報を取り扱っているサイト Search Engine Watch の Danny Sullivan 氏は、Facebook のプライバシーに関するデフォルト設定が、情報の「制限」から「公開」へと変更されただけだと述べている。

インターネット・セキュリティの専門家は、今回のメンバー検索拡張機能によって、Facebook ユーザの個人情報が悪用される可能性が高くなると懸念を示している。ウィルス対策ソフトウェアのベンダとして有名な Sophos 社が行った調査によると、41%の Facebook ユーザが、Eメールアドレス、生年月日、電話番号などの個人情報を友達以外に公開してもよいと設定していることが判明している<sup>61</sup>。特に、10代後半から30代前半の若者を中心とする SNS ユーザの多くは、SNS サイトの利用にあたり、プライバシー設定をよく考えずに行ったり、必要以上に写真を含めて個人情報を公開しているため、SNS サイトは、個人情報保護対策上のリスクが非常に高いものと考えられる。

実際に、この結果、実際に、多くの個人情報が流通し、また、人気 SNS サイトの利用者が低年齢層化する流れの中で、その個人情報を活用した18歳未満の子どもを狙った犯罪が増えている<sup>62</sup>。なお、SNS の多くは、18歳未満の利用者のサイト利用を禁じているが、利用者の年齢を確認する手段がないため、18歳未満の者でも簡単に登録ができてしまうのが実態である。

#### 【利害関係者の意見、対応の方向】

上記のような SNS サイトを悪用したインターネット犯罪から子どもたちを守るため、SNS における子どものプライバシー・個人情報の保護を巡って様々な動きが起こっている。2006年5月9日には、米下院で、SNS を利用する子どもを性的犯罪から守るための法案「Deleting Online Predators Act」(HR 5319)が提出された。同法案では、学校、図書館などから子どもが SNS サイトにアクセスできないように、セキュリティ・システムの実装を義務付けている。また、2006年6月28日には、米連邦取引委員会 (FTC) が米下院エネルギー・商業委員会監視調査小委

<sup>60</sup> <http://www.informationweek.com/industries/showArticle.jhtml?articleID=202200395>

<sup>61</sup> <http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html>

<sup>62</sup>例えば、2006年7月、当時26歳であった Jason Palmeira 容疑者は、人気 SNS サイト MySpace で知り合ったコネチカット州に住む15歳の少女に対して、性行為をはたらいととして逮捕された。米国司法省の発表したプレスリリースによると、15歳の少女は、年齢を偽らずに15歳としてプロフィールを公開しており、コネチカット州に住む18歳以下の男子と知り合いになりたいというメッセージを載せていたという。Palmeira 容疑者は、同15歳の少女に MySpace のサイト上のメッセージ機能を利用して連絡を取り、サイトのメッセージ機能や電話を使って頻繁にコミュニケーションを取り合うようになった。同容疑者は、性的な内容の会話を少女とするようになり、直接会う約束をし、直接あつて性行為に及んだとされている。このケースは無理にレイプしたケースではないが、米国では17歳以下の子供との性行為は違法行為とされている。  
<http://www.usdoj.gov/usao/ct/Press2006/20060801.html>

員会で、SNSにおける子どもの安全対策に関する証言を行い、FTCが複数のSNSサイトを対象に、コンプライアンス状況の調査を実施していると述べた。

#### (4) 論点の整理

上記のいずれの事案（例えば、検索ログやウェブサービスの情報や、SNSに登録される情報など）にせよ、基本的には、利用者が、どこまでプライバシー漏洩の危険性を認識した上で、当該インターネット・サービスを楽しんでいるのかという問題に帰着するものと整理される。また、このような認識ギャップが生じている原因は、インターネット・サービスは、近年急速に伸びている分野であり、プライバシー保護に係る社会的な認識や受容基準がまだ確立されていない分野であるためであるとも考えられる。

そのような意味で、インターネット・サービス会社においては、収集する個人情報の内容とその社内での管理体制に関し、利用者に対して説明責任を果たすとともに、自ら収集し公開する情報等（例えば、マップにおける画像情報、未成年者によるSNS情報など）に対してプライバシー保護の観点から一定の規律を確立することも含めて、その管理に対する責任を履行し、消費者の信頼を得ていくかという問題であると考えられる。これらについては、未成年者に対する配慮、教育なども含まれよう。逆にこのようにして、利用者との信頼関係が確立されることにより、プライバシー問題にも配慮した持続的なビジネスの発展がなされるものと考えられる。

また、本問題は、インターネットのボーダレスな性質を踏まえると、国際的な基準、ガイドラインが必要との指摘もある。例えば、(1)で議論したログ保存期間に関しては、米国内では、一方で、後述するように、国家安全保障の観点から、長くするべきとの議論もある。これは、欧州にあるログ保存期間を短くし、消費者のプライバシー保護強化に向けた方針と対立する考え方であり、インターネットを介したボーダレスなサービスだけに、国際的協調の必要性が求められる分野でもある<sup>63</sup>。

こうした中、インターネット・サービスを提供する企業からは、世界的なプライバシー標準策定を期待する動きが出ている<sup>64</sup>。Googleのグローバル・プライバシー担当顧問であるPeter Fleischerは、2007年9月14日、フランスで開催された国連教育科学文化機関の倫理と人権に関する会議で講演、アジア太平洋経済協力会議（APEC）のプライバシーフレームワーク<sup>65</sup>に沿ったプライバシー標準策定について提案している<sup>66</sup>。

<sup>63</sup> <http://www.itworld.com/Man/2681/061207top10/>

<sup>64</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/13/AR2007091302248.html>

<sup>65</sup> [http://www.apec.org/apec/news\\_media/fact\\_sheets/apec\\_privacy\\_framework.html](http://www.apec.org/apec/news_media/fact_sheets/apec_privacy_framework.html);

<sup>66</sup> <http://peterfleischer.blogspot.com/2007/09/need-for-global-privacy-standards.html>

#### 4. インターネット・サービスに係る国家による情報検閲とプライバシー問題

##### (1) 概要

インターネット・サービスにかかる個人情報については、企業においては、プライバシー保護の観点から、利用者等との関係でセキュリティ対策も含め適切な管理が求められる一方で、国家安全保障（ナショナルセキュリティ）などの観点から、国として必要と判断された場合には、プライバシーの一部を犠牲にしても、個人情報を国家が傍受あるいは検閲する場合がある。特に、インターネットに係る情報技術が発展し、インターネットを通じた情報のやりとりが国境を越えて増加し、大きな役割を担いつつある中、国家としては、既存の情報のルートのみならず、それらのインターネットでの情報を活用し、当該国益を確保すべきという意見が存在する。

特に、米国においては、一般的には、中国など外国の行う、表現の自由の抑制、思想の管理の観点等からの情報管理・検閲については、機微な感覚を有する一方、国内においては、特に、9/11以降、多くの議論をはらみつつも、国家安全保障（ナショナルセキュリティ）重視の観点からの個人情報の傍受に係る法制がいくつかなされてきている。当然ながら、このような国家（政府）による個人情報の傍受や検閲は、当然ながらインターネット・サービスにおける個人情報（プライバシー）の保護のあり方に対して、大きな影響を与えるものである。

本章においては、このような、米国における国家安全保障の観点からのプライバシーに係り得る情報検閲等の状況、及び、中国におけるインターネット検閲に係る米国内企業等の対応の状況について報告する。

##### (2) 米国における国家安全保障の観点からの情報検閲

###### ①愛国者法（Patriot Act）とデータマイニング

2001年9月11日に発生した同時多発テロを受け、米国連邦議会は、同年10月24日、Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001<sup>67</sup>、通称Patriot Act（愛国者法）を

<sup>67</sup> なお、このGoogleの提案に対して、これを後述するDoubleClick買収への批判をかわす目的とする見方や、APECフレームワーク自体が非常に生ぬるいものであり、ガイドラインとしてふさわしくないという意見もある。

<http://www.washingtonpost.com/wp-dyn/content/article/2007/09/13/AR2007091302248.html>

<sup>68</sup> <http://www.epic.org/privacy/terrorism/hr3162.pdf>

可決した。議会通過の2日後には、ブッシュ大統領が同法律に署名している。同法により、連邦政府諜報機関は、一部の場合には、裁判所の包括許可（礼状）を得ることなく、一般市民に対し、電話の盗聴や電子メールの傍受等ができるなど、これまで以上に個人情報収集することが容易になった<sup>69</sup>。

### 【問題のポイント】

愛国者法の成立当初から、政府によるプライバシー侵害の懸念が指摘されてきた。特に、インターネットなどに関連した懸念として、同法成立直後の2001年10月26日、CNET Newsは「愛国者法が招くプライバシーの懸念（Patriot Act draws privacy concerns）<sup>70</sup>」と題する記事を掲載した。この中で、Center for Democracy and Technology（CDT）のJerry Berman エグゼクティブ・ディレクターは、「司法長官はインターネットに対して全面的攻撃を仕掛けつつある。彼らはインターネット上で多数のデータマイニングや捜査を実施したいのだ。（中略）同法の心配の種は、同法が非常に広範なものであり、単にテロリスト容疑者だけに適応されるのではなく、合法的な活動に関わっている個人や組織にまでも適応できてしまうことだ」とコメントしている<sup>71</sup>。実際、上記の懸念は現実のものとなり、テロリストの容疑者だけではなく、同法が反戦運動家、中絶経験者、ホームレス等にも適用されるケースが起きてきている<sup>7273</sup>。

同法によって、政府の諜報機関が日常的に国民の動きを監視できるような環境が整ったとされる。例えば、データマイニングはそのための重要なツールのひとつとして利用されている。2004年5月にGAOが発表した連邦政府のデータマイニングに関する報告書<sup>74</sup>によれば、当時の時点で、連邦政府全体で、131のデータマイニング・プロジェクトが運用されていることが明らかになった（加えて、運用を検討しているプロジェクトが68件）。

<sup>69</sup>同法成立の背景について、『Privacy Lost』の中で、著者のDavid H. Holtzmanは「9/11同時多発テロは不適当な諜報活動及び諜報機関と法執行機関の欠陥のあるコミュニケーションゆえに起こったとするものであり、こうした不備によって、国家が保護すべき対象範囲の中にギャップが生まれ、テロリストが検知されることなく、我々のシステムを使って、我々攻撃することを許す事態になった」と述べている。David H. Holtzman *Privacy Lost* 2006 pg 223

<sup>70</sup> <http://www.news.com/2100-1023-275026.html>

<sup>71</sup> <http://www.news.com/2100-1023-275026.html>

<sup>72</sup>例えば、アイダホ大学の学生であったSami al-Hussayenは、Islamic Assembly of North Americaにおいてウェブマスターをしていたが、その仕事の一環として、同団体外のウェブサイトにあるイスラム系学者が書いた論文等にリンクを貼った行為がもとで、逮捕・起訴されている。

<http://www.npr.org/templates/story/story.php?storyId=4756403>

<sup>73</sup>また、12歳の少年が宿題のためにインターネットでワシントンDC付近にある橋について調査していたところ、それがFBIがセキュリティ対象であったために、これが危険信号として受け取られ、FBIが同少年の下に捜査員を送るというケースなども報告されている<sup>73</sup> David H. Holtzman *Privacy Lost* (2006)

<sup>74</sup> <http://www.gao.gov/new.items/d04548.pdf>

連邦政府機関別データマイニング利用目的<sup>75</sup>

Table 1: Top Six Purposes of Data Mining Efforts in Departments and Agencies and Number of Efforts Reported

Department or agency	Improving service or performance	Detecting fraud, waste, and abuse	Analyzing scientific and research information	Managing human resources	Detecting criminal activities or patterns	Analyzing intelligence and detecting terrorist activities
Department of Agriculture	8	1				
Department of Commerce						
Department of Defense	19	1	1	14	1	5
Department of Education	6	9			3	1
Department of Energy					3	
Department of Health and Human Services	4		1			1
Department of Homeland Security	5			2	2	4
Department of the Interior	1					
Department of Justice	1			1	3	3
Department of Labor	3	1				
Department of State						2
Department of Transportation		1				
Department of the Treasury	4	1			2	
Department of Veterans Affairs	5	5			1	
Environmental Protection Agency		1				
Export-Import Bank of the United States	1					
Federal Deposit Insurance Corporation	1					
Federal Reserve System		1				
National Aeronautics and Space Administration	1	1	21			
Nuclear Regulatory Commission	1					
Office of Personnel Management	1					
Pension Benefit Guaranty Corporation	2					
Railroad Retirement Board	1					
Small Business Administration	1					
<b>Total</b>	<b>65</b>	<b>24</b>	<b>23</b>	<b>17</b>	<b>15</b>	<b>14</b>

Source: GAO analysis of agency-provided data.

これらのデータマイニングの対象は、電子メール、ブログ等の内容まで含まれるものもある<sup>76</sup>。例えば、国家安全保障省（DHS）の Dissemination, Visualization, Insight, and Semantic Enhancement（ADVISE）というシステムは、2006年2月9日付 Christian Science Monitor 紙の記事によれば、オンライン上にある財務情報から CNN ニュースなどを含む広範な情報について収集、これを連邦政府諜報機関及び法執行機関の情報と相互参照させ、その上で、個人、場所、組織等とリンクさせたデータを保存するものであるとしている。

【利害関係者の意見、対応の方向】

GAOは同レポートの中で、特に、連邦政府機関では、9/11同時多発テロ以降、データマイニングをテロリストの脅威に対抗する重要なツールと認識、既知のテロリストについての捜査に使うだけではなく、膨大なデータを分析し、特定のパターンを発見することによって、潜在的テロリストとなる個人を見極めることに

<sup>75</sup> <http://www.gao.gov/new.items/d04548.pdf>

<sup>76</sup> <http://www.csmonitor.com/2006/0209/p01s02-uspo.html>

利用しようとしている利用法は、一般市民や議会のプライバシー侵害に対する懸念を招くものだとしている<sup>77</sup>。

さらに、2006年6月15日付け Washington Post 紙は、政府による民間データマイニング・サービスの利用が進められていることと、それに関連してプライバシー侵害の危険が高まっていることについて報じている<sup>78</sup>。同記事の中で、元政府関係者は、「何も隠さなければならないようなことをしていなければ、あなたがどんな映画を借りているかについて私が知っていても気にする理由はないだろう」とコメントしている。その一方で、こうした民間のデータが法執行のために収集されたものではなく、多くの誤りを含んでいるデータであり、そこから導き出された情報分析の結果が誤った推測を生み出す危険性について、CDTの政策ディレクターである Jim Dempsey 氏の意見も取り上げている。

なお、愛国者法によって改正された国際情報監視法 (Foreign Intelligence Surveillance Act: FISA) に関し、同法では盗聴・傍受が裁判所からの礼状が必要とされている機関において、ブッシュ政権は、法律に反して礼状を取らずに監視を行っていたことを契機に、最近、国家による監視行為のそもそもの合法性について、大きな議論になっている<sup>79</sup>。

## ②検索ログ等の保全義務

前章において、検索エンジンのログについては、CDTをはじめとする消費者団体から、その保存すべき期間を短くすべきとの議論があることを述べた。一方で、検索エンジンのログを捜査活動に役立てようとしている米国の警察・諜報機関は、検索エンジン会社のログの保存期間をできる限り長くしたいと考えており、これと関連し、司法省、議会共和党議員を中心として、ISP等にデータ保存を義務付ける法案の成立を目指している。「Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (Safety Act)<sup>80</sup>」として知られる同法案はオンライン上の児童ポルノを規制することを目的としているが、その目的の一環として、ISPは、インターネット上で顧客が何をしているか、トラッキングしなければな

<sup>77</sup> [http://www.news.com/Government-data-mining-lives-on/2010-1028\\_3-5223088.html](http://www.news.com/Government-data-mining-lives-on/2010-1028_3-5223088.html);

<http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html>

<sup>78</sup> <http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063.html>; この中で、国家安全保障省 (DHS) が導入したものの、失敗に終わった2億ドル規模の CAPPs II と呼ばれるデータマイニング・システムについて触れられている。同システムでは当初、民間から得たクレジット・ヒストリー情報などを基に、よく引越しをする人物やクレジット・ヒストリーが確立されていない人物などを潜在的危険人物とみなして、飛行機の搭乗の際に利用しようと考えたが、「危険度が高い」とされる人物が多すぎて、結局利用できなかったという関係者の証言が紹介されている。

<sup>79</sup> [http://ryumurakami.jmm.co.jp/dynamic/report/report5\\_184.html](http://ryumurakami.jmm.co.jp/dynamic/report/report5_184.html)

<sup>80</sup> <http://www.politechbot.com/docs/smith.data.retention.labeling.draft.020607.pdf>

らないとしている<sup>81</sup>。同法案では、Web ホスティング、ドメインネーム登録機関、検索エンジン会社、SNSについて、明言はされていないが、これらも対象にすべきと考える解釈も議会には存在している<sup>82</sup>。

データ保存を義務付ける Safety Act を巡る米議会・政府の動き<sup>83</sup>

時期	政府・議会の動き
2005年6月	米司法省当局者、密かにデータ保存ルールを提案。
2006年4月14日	コロラド州議会及び米国連邦議会において、データ保存に関する司法省提案が明るみに。
2006年4月20日	Alberto Gonzales 司法長官、データ保存は優先課題として取り組まなければならないと発言。
2006年4月28日	民主党、データ保存規制修正案を提出。
2006年5月26日	Gonzales 司法長官及び Robert Mueller FBI ディレクター、インターネット及びテレコム企業に対して、圧力行使。
2006年9月26日	Web ホスティング、ドメインネーム登録機関、検索エンジン会社も、同法を遵守しなければならないだろうと、政治家が提言。
2007年2月6日	共和党、Safety Act の一環として、データ保存を義務付ける法案を第 110 議会（2007-08）に提出。
2007年3月1日	米下院、犯罪、テロリズム及び国家安全保障小委員会（Crime, Terrorism, and Homeland Security）に付託 <sup>84</sup> 。

<sup>81</sup> [http://www.news.com/GOP-revives-ISP-tracking-legislation/2100-1028\\_3-6156948.html](http://www.news.com/GOP-revives-ISP-tracking-legislation/2100-1028_3-6156948.html)

<sup>82</sup> [http://www.news.com/Politicos-mull-data-retention-by-Web-hosts%2C-registrars/2100-1028\\_3-6119878.html](http://www.news.com/Politicos-mull-data-retention-by-Web-hosts%2C-registrars/2100-1028_3-6119878.html)

<sup>83</sup> [http://www.news.com/Justice-Department-takes-aim-at-image-sharing-sites/2100-1028\\_3-6163679.html?tag=st.ref.goo](http://www.news.com/Justice-Department-takes-aim-at-image-sharing-sites/2100-1028_3-6163679.html?tag=st.ref.goo)

<sup>84</sup> <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.00837:>



(4) 中国におけるインターネット検閲<sup>85</sup>

中国政府によるインターネット・コンテンツの検閲は、米国インターネット企業の協力の下に行われていることが明らかになり、表現の自由及びプライバシー保護を巡って、米国内で大きな論議を呼んだ。

【問題のポイント】

特に、近年、この問題が米国内でクローズアップされたのは、2006年2月15日、Yahoo!、Microsoft、Google、Ciscoの代表が呼ばれて開催された、連邦下院人権小委員会における中国のインターネット規制に関する公聴会である。同公聴会では、潜在的市場として期待の高い中国においてビジネスを行っていくために、同国の法律等に遵守するあまり、米国の象徴といえる表現の自由とそれを実現するために必要とされる個人のプライバシーを守ることを放棄することの是非が問われた。すなわち、①外国政府から要求があった場合、インターネット・サービス会社に個人情報を提供しなければいけないのか、②外国政府から要求があった場合、特定の情報を検索結果から、排除するような仕組みを設けてよいのかという問題である。なお、同公聴会における企業代表の発言は、各社はビジネスを行う国・地域における法律に遵守しているだけであるとする現状説明に留めている<sup>86</sup>。

前者(①)の具体的事例(中国政府がインターネット・サービス企業に対して、圧力をかけたことによって起こったプライバシー侵害の事例)としては、2004年、天安門事件15周年の報道に関連して機密漏洩罪で中国人ジャーナリスト、Shi Tao氏が10年の懲役刑に処せられた事件がある。これは、Yahoo!がTao氏のメールのログイン記録を中国政府に提供したためと言われている<sup>87</sup>。また、Yahoo!は2003年にも中国政府に情報提供し、この結果、中国人ライターのLi Zhi氏が投獄され、現在8年の刑に服しているとされる<sup>88</sup>。

<sup>85</sup>[http://www.informationweek.com/story/showArticle.jhtml?articleID=201806531&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201806531&cid=RSSfeed_IWK_News)

[http://www.mercurynews.com/ci\\_6809009?source=rss&nlick\\_check=1](http://www.mercurynews.com/ci_6809009?source=rss&nlick_check=1)

<http://www.nytimes.com/2007/08/12/business/worldbusiness/12security.html?ex=1344571200&en=df3f7b36de098b00&ei=5088&partner=rssnyt&emc=rss>

[http://www.news.com/Yahoo%20files%20to%20dismiss%20China%20human%20rights%20suit/2100-1030\\_3-6204746.html?part=rss&tag=2547-1\\_3-0-20&subj=news](http://www.news.com/Yahoo%20files%20to%20dismiss%20China%20human%20rights%20suit/2100-1030_3-6204746.html?part=rss&tag=2547-1_3-0-20&subj=news)

[http://www.informationweek.com/story/showArticle.jhtml?articleID=201001971&cid=RSSfeed\\_IWK\\_News](http://www.informationweek.com/story/showArticle.jhtml?articleID=201001971&cid=RSSfeed_IWK_News)

<sup>86</sup> <http://www.informationweek.com/news/showArticle.jhtml?articleID=178600547>;

[http://select.nytimes.com/2006/02/19/opinion/19kristof.html?\\_r=1&n=Top/News/Business/Companies/Yahoo!%20Inc.&oref=slogin](http://select.nytimes.com/2006/02/19/opinion/19kristof.html?_r=1&n=Top/News/Business/Companies/Yahoo!%20Inc.&oref=slogin)

<sup>87</sup> <http://news.bbc.co.uk/1/hi/world/asia-pacific/4221538.stm>

<sup>88</sup> <http://news.bbc.co.uk/1/hi/world/asia-pacific/4695718.stm>

また、後者(②)は、プライバシー侵害では必ずしもないものの、表現の自由を阻害する事例としては、米インターネット企業は中国当局の圧力を受け、ジャーナリストのブログを閉鎖したり、検索エンジンの自己検閲を実施したり、あるいは、「民主主義 (democracy)」、「中国における人権 (human rights in China)」、「法輪功 (Falun Gong)」、「ダライ・ラマ (Dalai Lama)」、「天安門広場 (Tiananmen Square)」に関するコンテンツを含む Web サイトを排除したりといったことを行なってきたとされる。例えば、Google は中国向けの検索エンジン<sup>89</sup>を開始したが、これは検閲 (自動フィルタリングなどを使用、特定の言葉の検索結果が出ないような仕組み) を提供している。

#### 【利害関係者の意見、対応の方向】

国境なき記者団 (Reporters Without Borders<sup>90</sup>)、その他米国主要メディアは、米国インターネット企業が中国におけるジャーナリスト糾弾に手を貸しているとして批判している。

しかし、インターネット関連企業は、中国におけるプライバシー侵害問題等について、これを政治的問題とする姿勢が強い。例えば、同公聴会開催に先立ち、下院の Human Right Caucus が中国の人権とインターネットに関する Briefing を開催、Cisco Systems、Google、Microsoft、Yahoo! に出席を求めたが、4社は米国政府が主導して中国政府やインターネットの制限を加えている他国の政府と政府間協議を行うことを期待するとの共同コメントを発表し、これに対する出席を拒否した<sup>91</sup>。さらに、Yahoo!香港が、Tao 氏及び Wang Xoapmomg 氏に関する情報を中国政府に提供したことによって、両氏が10年の懲役刑を受けたことについて、2007年4月、両氏と Yu Ling 女史 (Wang 氏の妻) は Yahoo! 及びその香港支社を相手取って、北カリフォルニア地方裁判所に訴えを起こした<sup>92</sup>。これに対し、Yahoo! 側は原告の訴えを棄却すべきとする申し立てを行った。同社のスポークスパーソンである Kelly Benander 女史は「同社は人権保護に対して強い信念を持っている企業であり、世界中で表現の自由と個人のプライバシーを尊重している」としながら、「本件は政治・外交問題であり、法的問題ではない」とするコメントを発表している<sup>93</sup>。

このような中、グーグルの CEO である Eric Schmidt 氏は、2007年8月に開催されたコンファレンスの中で、「表現の自由を守るために、各国政府はインターネット検閲を非関税障壁と捉えるべきだ」と呼びかけている<sup>94</sup>。すなわち、好ましくないコンテンツの基準は何か、国家間で法律がどう違うのかなど、いろいろな

<sup>89</sup> [www.google.cn](http://www.google.cn)

<sup>90</sup> [http://www.rsf.org/rubrique.php?id\\_rubrique=20](http://www.rsf.org/rubrique.php?id_rubrique=20)

<sup>91</sup> [http://news.com.com/2061-10811\\_3-6033949.html?tag=nl](http://news.com.com/2061-10811_3-6033949.html?tag=nl)

<sup>92</sup> [http://www.news.com/Yahoo-files-to-dismiss-China-human-rights-suit/2100-1030\\_3-6204746.html](http://www.news.com/Yahoo-files-to-dismiss-China-human-rights-suit/2100-1030_3-6204746.html)

<sup>93</sup> [http://www.news.com/Yahoo-files-to-dismiss-China-human-rights-suit/2100-1030\\_3-6204746.html](http://www.news.com/Yahoo-files-to-dismiss-China-human-rights-suit/2100-1030_3-6204746.html)

<sup>94</sup> <http://japan.cnet.com/news/media/story/0,2000056023,20355385,00.htm>

問題があるが、これは全世界を巻き込んだ現象なのだから整理する必要がある、としている。

なお、米国政府は、上述の公聴会に先立ち、2006年2月14日、ライス国務長官は「Global Internet Freedom Task Force (GIFT)」の設立、インターネットの規制問題について、外交政策として検討するため、政府部内及び関係者と協議を進めると発表している<sup>95</sup>。

このレポートに対するご質問、ご意見、ご要望がありましたら、tagui\_ichikawa@jetro.go.jp までお願いします。

なお、本レポートは、注記した参考資料等を利用して作成しているものであり、本レポートの内容に関しては、その有用性、正確性、知的財産権の不侵害等的一切について、執筆者及び執筆者が所属する組織が如何なる保証をするものでもありません。また、本レポートの読者が、本レポート内の情報の利用によって損害を被った場合も、執筆者及び執筆者が所属する組織が如何なる責任を負うものでもありません。

---

<sup>95</sup> <http://www.state.gov/r/pa/prs/ps/2006/61156.htm>;  
<http://www.informationweek.com/internet/showArticle.jhtml?articleID=180202242&pgno=2&queryText=>;  
しかし GIFT の最近の活動については、公開情報からは明らかになっていない。