

米国連邦政府によるインターネット上のプライバシー保護政策の変化

夏井高人

米国においては、インターネットのガバナンスに関し、インターネットに主体として登場する企業や個人が自律的な規範を形成するのが望ましいとする考え方（自由主義）が主流となっている。そのため、政府（特に連邦政府）によるインターネット上の法律問題への介入はできるだけ避けるべきであり、ネット上の中立性（*neutrality*）を維持すべきだとの考え方が強い¹。日本流の表現で言えば、「政府による規制」には反対する考え方だと言い換えても良い。

とはいえ、インターネット上で様々な法律問題が生じていることは事実であるので、連邦政府（特に FTC や FCC）が何らかのかたちで介入することによりインターネット利用者の権利保護を図るということが行われてきた。例えば、スパムメール（*unsolicited e-mail message*）に対する規制をその例としてあげることができる。本来、電子メールのタイトル（サブジェクト欄）や本文をどのような内容にするかは送信者の表現の自由に属することであるし、商業宣伝目的で電子メールを利用することは企業の経済活動の自由に属することだ。そのため、商業宣言目的の電子メールのタイトル（サブジェクト欄）に商業宣伝目的の電子メールであることを記載させるような法制を構築するということは、表現の自由や経済活動の自由に対する侵害行為になると考えられていた。とはいえ、スパムメールの被害がひど過ぎるため、FTC を中心として商業宣伝目的の電子メールを自動的に識別し、自動的に排除できるようにするための法制が構築されることになった。このことは、日本の政策に対しても、特定電子メール適正化法（特定電子メールの送信の適正化等に関する法律（平成 14 年 4 月 17 日法律第 26 号））の立法などにみられるように、強い影響を与えることになったことは周知のとおりだ²。

その後、インターネットの利用が更に拡大し、Facebook などの **Social Media** の利用が一般に普及するにつれ、その利用者のネット上の行動が追跡され、商業利用される事例が激増

¹ 何か問題が生じた場合には、被害者が自分で訴訟を提起して解決すべきだという考え方（サミュエル・スマイルズ『自助論』の「天は自ら助くる者を助く（*Heaven helps those who help themselves*）」と基本を同じくする思想）がベースになっていることを正しく理解しないと、米国流のやり方を正確に理解したことにはならない。日本では、個人が訴訟を続々と提起するという文化や精神風土に乏しく、「おかみ」にすがって保護してもらうという傾向が強いため、普通の日本人には米国流のやり方を理解しにくいかもしれない。このことは、一般市民だけではなく法学者でもそうであり、そのために米国流のやり方について誤った評価がなされることがしばしばある。

² ただし、これらスパムメール対策立法が功を奏したかどうかは疑問であり、日本では特定電子メール適正化法の改正（送信アドレス偽装の禁止や罰則強化）がなされてきたことも周知のとおりだし、また、現時点では、スパムメールに見せかけてマルウェア（トロイの木馬など）を仕組んだ電子メールが送信されることが非常に多くなっており、商業宣伝行為に対する規制という観点だけではほとんど何も対応していないことになってしまっていることも事実だと思われる。

した。このような状況に対しては、EFF や EPIC などのプライバシー保護団体から手厳しい批判が重ねられてきた。しかし、インターネットの利用は自由であるべきであり、「連邦政府はインターネットについて中立性を維持すべきだ」との考えかたが依然として強かったため³、強力な規制策が構築されることはなかった。

ところが、Facebook 利用者や Twitter 利用者の個人プロフィールデータが自動的に第三者に転送され商業利用されることへの批判が高まり、また、これらのシステムのバグや攻撃などによって防御措置も破られる事態が多発するに及んで、世論は、ネット上のプライバシー保護の方向へと大きく動いたようだ。米国連邦政府の関連省庁による調査や連邦議会による調査が重ねられ、連邦政府による介入によって問題を解決しようとする方向性が打ち出されることになった⁴。

2010年12月1日、FTCは、ネット上のプライバシー保護に関する報告書を公表した。

FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change

FTC: December 1, 2010

<http://www.ftc.gov/os/2010/12/101201privacyreport.pdf>

Preliminary FTC Staff Privacy Report: Remarks of Chairman Jon Leibowitz as Prepared for Delivery

FTC: December 1, 2010

<http://www.ftc.gov/speeches/leibowitz/101201privacyreportremarks.pdf>

[関連記事]

³ ネット利用者の行動履歴を収集・蓄積し、データベース化すること（いわゆるネットプロフィールやライフログなどを含む。）、そしてその分析結果を商業利用することをもくろむ事業者が、たとえその介入が消費者の権利を保護するための正当なものであったとしても政府による介入を嫌い、意図的または曲解的に「中立性」を強調してきた疑いがある。また、特定の企業をスポンサーとする評論家などがそのような企業に迎合し、「中立性」をことさら強調してきた疑いもある。EFF や EPIC などの厳しい批判は、そのような事業者側の利益追求の姿勢に対するいわばカウンターのようなものとして社会の中で機能してきたと理解することもできるだろう。なお、日本には EFF や EPIC に相当するプライバシー保護団体が存在しないため、国民や消費者が、その個人データやプライバシーデータを一方的に収奪・搾取されるだけの状況にあるということを正確に理解する必要がある。

⁴ このような動きについては、サイバー法ブログのバックナンバーを拾い読みしていただきたい。記事の「個人情報」タグをクリックすると、その一覧が表示されるので、その中から適宜関連記事を選択して読むか、または、ブラウザの検索機能で必要なキーワード検索をすることにより、過去記事を発見することができる。なお、米国の新聞記事等については相当古いものでもそのまま残されているが、日本の新聞記事等は数週間～1ヶ月程度で削除されるのが普通なので、リンク先の記事が消滅している可能性が高い。

FTC、Web ユーザー向け「ネットでの行動追跡拒否」システム提案

IT Media: 2010年12月02日

<http://www.itmedia.co.jp/news/articles/1012/02/news027.html>

FTC Chairman Jon Leibowitz On The Cyber-Stalkers Violating Our Privacy

Huffington Post: 12-14-10

http://www.huffingtonpost.com/2010/12/14/ftc-chairman-jon-leibowitz_n_796207.html

Who's Tracking You Online?

npr: December 17, 2010

<http://www.npr.org/2010/12/17/132141781/whos-tracking-you-online>

この FTC の報告書の中では、採用されるべき解決策として、次のような基本的な枠組みの重要性が指摘されている⁵。

- A. Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device
- B. Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services
 - 1. Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy
 - 2. Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services
- C. Companies should simplify consumer choice
 - 1. Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.
 - 2. For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data
 - a. General considerations regarding how choice is presented
 - b. A special choice mechanism for online behavioral advertising: Do Not Track
- D. Companies should increase the transparency of their data practices
 - 1. Privacy notices should be clearer, shorter, and more standardized, to enable better comprehension and comparison of privacy practices
 - 2. Companies should provide reasonable access to the consumer data they maintain;

⁵ この報告書の抄訳を会員に対するプレミアムサービスとして提供すべく検討中。

the extent of access should be proportionate to the sensitivity of the data and the nature of its use

3. Companies must provide prominent disclosures and obtain affirmative express consent before using consumer data in a materially different manner than claimed when the data was collected

4. All stakeholders should work to educate consumers about commercial data privacy practices

次いで、2010年12月16日、米国商務省（Department of Commerce）も同様の報告書を公表した。

RELEASED: Policy Framework for Protecting Consumer Privacy Online While Supporting Innovation

Department of Commerce: December 16, 2010

<http://www.commerce.gov/blog/2010/12/16/released-policy-framework-protecting-consumer-privacy-online-while-supporting-innova>

Green Paper: Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework (1.0 MB PDF file)

http://www.ntia.doc.gov/internetpolicytaskforce/index_test12162010.html

[関連記事]

ネット上のプライバシー保護強化を＝米商務省が報告書

Wall Street Journal: 2010年12月17日

http://jp.wsj.com/US/node_161526

米、ネット上の個人情報保護へ 消費者団体の懸念受け

共同通信: 2010/12/17

<http://www.47news.jp/CN/201012/CN2010121701000132.html>

これらの報告書に示されている方策の要点は、商業利用の目的で利用者の行動履歴を収集・蓄積することそれ自体については適法行為（企業活動の自由の範囲内）としつつも、ブラウザ上に設置したボタンをクリックするなどすれば行動履歴の追跡を拒否できるようにしなければならない（オプトアウトの一種）とするものだ。このようなやり方は、古くから電話による商業宣伝広告をブロックするために採用されている Do not call のやり方を応用したものだといわれ、Do not track と正式に命名されている。

このような動きを踏まえ、Microsoft 社は、IE 9 において Do not track 機能を実装するという方針を公表している。

IE 9 To Feature 'Do Not Track' Option

dark READING: Dec 7, 2010

[http://www.darkreading.com/security-](http://www.darkreading.com/security-monitoring/167901086/security/privacy/228600190/ie-9-to-feature-do-not-track-option.html)

[monitoring/167901086/security/privacy/228600190/ie-9-to-feature-do-not-track-option.html](http://www.darkreading.com/security/privacy/228600190/ie-9-to-feature-do-not-track-option.html)

このような動きが日本国の個人情報保護法の解釈・運用にどのような影響を与えるかについては未知数の部分が多い。

しかしながら、個人情報保護法に定めるオプトアウトが必要となる場合（保有個人データの第三者提供、目的外利用など）に該当しなくても、Do not Track によるオプトアウトが実装されていなければ（少なくとも米国では）違法とされることになるわけだから、日本でもそれに追随せざるを得なくなることが確実だと思われる。

現在の日本国の国会の状況から推測すると、個人情報保護法の一部改正は完全に不可能だと思われる。したがって、関連各省庁の個人情報保護ガイドラインの見直し、「電子商取引及び情報財取引等に関する準則」の改定によって当面の状況を乗り切るしかないだろうと思われる⁶。

⁶ 米国において、利用者履歴の収集・蓄積・商業利用がプライバシーの問題の一部として理解されているのは、プロッサーの学説をベースとするプライバシー理論に依拠していることによる。日本国では、「宴のあと事件」の判決等の判決理由を誤読した結果と思われる誤ったプライバシー理論が通説化しているため、この点が非常にわかりにくい。とりわけ、プロッサーの第3類型及び第4類型のプライバシー侵害が過去のドイツ法理論の影響を受けて別のもので扱われていることが非常に大きな要因となっている。そのドイツでの理論は、現時点では、かなりアメリカ風に変容してしまっている。日本の研究者がドイツにおける理論の基本的変化をきちんととらえていないことが多いため、ますますもって理論上の混乱が生じているものと思われる。