

## 【概要】

東日本大震災（東北地方太平洋沖地震）を契機として、各種のソーシャル・メディアの広報広聴手段としての意義が高く評価され、政府や自治体もソーシャル・メディアを本格的に利用するようになってきている。しかし、ソーシャル・メディア上で発信される政府・自治体の情報の法的位置づけは曖昧であり、情報公開の対象となるか等の問題がある。その背景にはそもそも情報や情報セキュリティの定義が困難であるという大きな問題があり、情報セキュリティの定義の手法について日米の比較を試み、日本型の定義手法の問題点を明らかとして、アメリカ法型の定義の可能性を検討する。

【キーワード】 ソーシャル・メディア 情報公開 公文書 行政文書

## 1 はじめに

東日本大震災（東北地方太平洋沖地震）を契機として、各種のソーシャル・メディアの広報広聴手段としての意義が高く評価されるようになった。政府や自治体もソーシャル・メディアを本格的に利用するようになっており、特に震災の後には自治体の利用が増えている。このことを背景として、経済産業省は2011年4月5日、内閣官房、総務省と共同で、国や地方公共団体などの公共機関がTwitter等のソーシャル・メディアを活用して情報発信をする際の留意点をまとめた「国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信についての指針」<sup>1</sup>（以下、「指針」と略。）を発表した。また同日、経済産業省は「公共機関向けのTwitterアカウントの認証スキーム構築について」を<sup>2</sup>公表し、公共機関がTwitterアカウントを運用する際の認証スキームを構築したとした。指針および認証スキームで問題とされているのは、主としてなりすましの問題である。2009年の年末に鳩山由紀夫首相（当時）を名乗る偽アカウント（@nihonwokaeyou）が作られるという騒ぎ<sup>3</sup>があった影響もあると思われる。指針で要求されているのは、なりすまし等の防止（アカウント運用者の明示、なりすましが発生した場合の注意喚起、短縮URLの原則

利用制限）と、アカウント運用ポリシーの策定・明示である。

しかし指針は、民間ソーシャル・メディアを利用して政府・自治体が発信した情報についてそもそもどのような性質を帯びるものであるのかについての記載を欠く。行政機関の保有する情報の公開に関する法律に基づく開示請求の対象となるのかどうか、公文書等の管理に関する法律にいう行政文書に含まれるのかどうか等の問題があると考えられるが、上記の指針や認証スキームには、特にこれらの問題への言及はない。

そこで本稿では、情報セキュリティについて法的にどのような定義が可能であるのかについて若干の検討を行い、それを手がかりとしてソーシャル・メディア上の政府情報の法的性質を考察することにしたい。

## 2 情報セキュリティの定義とその手法：日本法とアメリカ法

わが国の法体系においては、「情報」そのものに関する明確な定義は存在しない。情報それ自体の概念がきわめて多義的であり、経済学者、情報科学者などから多種多様な定義が試みられているが、「情報は物質でもエネルギーでもない。情報は情報である。」というノーバート・ウィーナーの定義<sup>4</sup>が結局のところ最も明晰かもしれない。しかしこの定義はたしかに明晰ではあるけれども、実務的には無意味である<sup>5</sup>。単なる文書上の文字の羅列から諜報の類までが「情報」としてひとく

<sup>1</sup> 経済産業省「国、地方公共団体等公共機関における民間ソーシャルメディアを活用した情報発信について」

<http://www.meti.go.jp/press/2011/04/20110405005/20110405005.html>

<sup>2</sup> 経済産業省「公共機関向けのTwitterアカウントの認証スキーム構築について」

<http://www.meti.go.jp/press/2011/04/20110405004/20110405004.html>

<sup>3</sup> 騒動の経緯については、次のサイトが詳しい。

<http://www.kotono8.com/2009/12/25nihonwokaeyou.html>

<sup>4</sup> NORBERT WIENER, CYBERNETICS (2<sup>ND</sup> ED.) 61-62 (1965).

<sup>5</sup> 名和小太郎『情報を商品にする方法』（東洋経済新報社、1988年）1頁。

くりにされていることも、定義を難しくしている一因であろう。また情報を法的に定義しようとするのとは逆に、情報科学によって法的推論の過程を「科学的に」明らかにして自動化しようとする試みが、第5世代コンピュータや人工知能がブームとなった時代に行われた<sup>6</sup>。しかし裁判官の推論過程のある程度の可視化に成功した<sup>7</sup>以外は、所期の成果を挙げたとは言い難い。

情報の定義がないため、情報セキュリティについても明確な定義はなく、情報セキュリティのCIAをそのまま受容し、それを所与の前提として法的概念を適合させようとするアプローチが一般的であるといえる<sup>8</sup>。「秘密保護のあり方こそ、情報セキュリティ法の基本概念」<sup>9</sup>であるとする、情報とは何かについて拘泥すること自体が無益かもしれない。ただ、情報化社会においてはそもそも法の正統性の根源である国家の「支配能力が低下したために、企業がアーキテクチャを駆使することによってそれを埋め合わせている」<sup>10</sup>であり、アーキテクチャだけではなくISMSのような一種のマニュアルやソフトローによって情報セキュリティが担保されている部分が多い。「セキュリティという概念は因果率にもとづいて組み立てられている」<sup>11</sup>とすれば、因果関係を明らかにするだけで足りるという見方もできる。また、定義が不明確なままに実態としても形式としても成立している事例として、「行政」それ自体の概念の定義が不明瞭なままに行政法体系が成立していることが挙げられ、情報セキュリティの法的概念が不明確であることがただちに重大な問題を惹起するわけではない。ただ、行政の概念についていえば、消極説のほか、積極説の各説においても法の下での公益の実現を目的とした能動的な作用という「最大公約数的な内容」<sup>12</sup>は成立している。情報セキュリティそれ自体の法的定義は難しくとも、それを構成する諸要素を柔軟に定義していくことによって何らかの情報

セキュリティの定義を導出することを試みるというアプローチはありえよう。

わが国の法体系は、明治維新後に継受したフランス法とドイツ法（特に後者）を基礎としている。第二次世界大戦後はアメリカ法の影響が強くなったものの、いまだにドイツ法の影響を色濃く残しており、それが日本法の強みとして認識される場合もある<sup>13</sup>。しかし、ドイツ法的な法体系の下では、「一般的確実性と具体的妥当性を調和」<sup>14</sup>という法に対する二つの要請のうち前者が重視されがちである。情報セキュリティに関係する技術がドッグイヤー的に発展する以上、それに対応する法律が後追いつ的になることはある程度やむをえず、またこれらのすべての技術に一般的に対応する法律を制定することも困難であるので個別領域において特別法を順次制定していく方向とならざるを得ないが、それは「なるべく特別法をつくらずに、主要法律に組み入れるべき」<sup>15</sup>という日本法の伝統的な要請には反することになる。

しかし、情報セキュリティに関係する領域では、法の体系性はかならずしも一般的確実性に結びつくとは限らないのである。

たとえば、実態としては行政活動に利用される個人情報であるのに、活動を担当する行政の組織が形式的に変更されただけで、法の網から漏れるという問題がある。わが国では、地方自治体の保有する個人情報については当該自治体の個人情報保護条例の適用対象となるが、地方独立行政法人、土地開発公社・地方道路公社・地方住宅供給公社のいわゆる地方3公社、指定管理者や一部事務組合・全部事務組合の保有する個人情報については実施機関には含まれない。このため行財政改革の一環として自治体の事務の一部を事務組合に移管すると、自治体の条例で明確に定めるか、当該事務組合等の条例で自治体条例の準用を規定しない限り、これらの保有する個人情報に情報主体がアクセスすることがとたんに難しくなる<sup>16</sup>。

また、わが国の個人情報保護の法体系においては、事業者にとっては負担が重くなっている反面で、情報主体である個人の権利性が曖昧なままとなっている。

<sup>6</sup> 吉野一編『法律エキスパートシステムの基礎』（ぎょうせい、1986年）、吉野一編『法律人工知能』（創成社、2000年）。

<sup>7</sup> 岡本浩一・太田勝造・村松良之「裁判官のエキスパートシステムとは何か：『スジ』『スワリ』をてがかりに」人工知能学会誌13巻2号（1998年）165-172頁。

<sup>8</sup> たとえば岡村久道『情報セキュリティの法律』（商事法務、2007年）。

<sup>9</sup> 林紘一郎『「情報セキュリティ法」の体系化の試み』情報ネットワーク・ローレビュー5号（2006年）88頁。

<sup>10</sup> 大屋雄裕「電子化された社会と制度」渡部明・長友敬一・大屋雄裕・山口意友・森口一郎『情報メディアの倫理』（ナカニシヤ出版、2008年）72頁。

<sup>11</sup> 名和小太郎『情報セキュリティ』（みすず書房、2005年）25頁。

<sup>12</sup> 原田尚彦『行政法要論（第2版）』（学陽書房、1989年）6頁。

<sup>13</sup> 上村達男「アメリカ・欧州・中国・日本の会社法制」季刊企業と法創造9号（2006年）119頁。

<sup>14</sup> 我妻榮『法律における理窟と人情』（日本評論社、1955年）6頁。

<sup>15</sup> 山田晟「特別法整理の必要」『立法学序説』（有斐閣、1994年）153頁。

<sup>16</sup> 宇賀克也「個人情報保護条例の現状と課題」ジュリスト1367号（2008年）47-48頁。

情報主体が民事訴訟によって個人情報の開示を請求することができるか（本人情報開示請求権の法的性格）という問題はその一例である（判例はこれを消極に解している）<sup>17</sup>。個人情報事業者から漏洩した場合に情報主体に事業者がこれを通知する義務はなく、個人情報を含むデータについても「滅失または毀損」の防止が定められているだけで、廃棄については具体的な手順や時期等についての規定がない。このことも情報主体が個人情報の漏洩に対して神経質となり、過剰反応を生む一因となっていると見ることができよう。

これに対してアメリカ法では「法について実際的な見方をする」ことから「問題が発生したときに救済が与えられることを重視する」ので、「どんなに実際上よく守られているルールであっても、違反があったときに法的制裁が加えられないものは、法の準則とは考えられない」し、「法違反の被害者に有効な救済を与え、将来の法違反を抑止するために必要ならば『理論』—少なくとも elementary な意味での理論—を無視してでも、裁判所の手を通じて法の実現を図るための手段が講じられる」<sup>18</sup>。救済を重視するためにいきおい法の規定は体系性を欠くことになり、たとえばプライバシーが侵害された場合の救済手段についてアメリカ法はいわゆるセクトラル方式を取っているので、連邦法には約 30 の法律に個別に散在している<sup>19</sup>。個人情報事

業者から漏洩した場合に情報主体に通知する義務については、連邦法上は存在しない（ただし連邦法制定に向けた動きはあり、2011 年 6 月の商務省の報告書では「政策勧告 B2a 連邦議会は電磁的記録に対して適用される商用データのセキュリティ侵害に関して通知規定を含む法律を制定すべきであり、これによって民間事業者が厳格なデータセキュリティ手順を実施することが期待されると同時に、各州が規定された方法以外の規制を行うことも可能となる。当該立法は、各州のセキュリティ侵害通知に関する法及び政策から生まれた効果的なデータ保護手段を踏襲すべきである。」としている）<sup>20</sup>、アラバマ、ケンタッキー、ニュー・メキシコ、サウス・ダコタ以外の州では州法で定められており（コロンビア特別区、プエルト・リコ準州、ヴァージョン諸島を含む）、半数の州ではデータの廃棄方法についても州法で規制を加えることによって情報主体を保護している。

このようなアメリカ法型の対応について「最終的にできあがった法律は、さまざまな妥協の産物以外の何物でもなく、ザル法的性格を色濃くしてしまっている」<sup>21</sup>という批判がある一方で、「誰が何を目的にどんな情報を取得・利用するかを絞り込むことで規制の必要性に応じたきめ細やかな立法」<sup>22</sup>になっているという評価もある。

アメリカ法では、重要な権利についての概念も変遷することがある。たとえば財産権の観念は、従来圧倒的に不動産を念頭に置いて構成され土地からの連想で物質的に定義されていたが、南北戦争の後に到来した資本主義社会・産業社会化を背景として 19 世紀末から 20 世紀初頭にかけて抽象的な法律関係からなるものであり物理的なものではないという観念に転換した。これによって著作権や特許権のような無体財産権の観念が生成された。同時にこれは、財産権は権利や権能、特権や免除からなる法律関係の束にすぎないという理解への革新的な変容であったとされる<sup>23</sup>。

またアメリカにおいては、言論という形式により公的に発信された情報は合衆国憲法修正 1 条<sup>24</sup>の保障を受けるが、「言論(speech)」について、プライベート・

<sup>17</sup> 東京地判平 19・6・27、判例タイムズ 1275 号 323 頁、判例時報 1978 号 27 頁。

<sup>18</sup> 田中英夫『英米法総論 上』（東京大学出版会、1980 年）21-22 頁。

<sup>19</sup> 主要なものとして、Administrative Procedure Act, 5 U.S.C. §551, 554-558, Cable Communication Policy Act, 47 U.S.C. §551, Census Confidential Statute, 13 U.S.C. §9, Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§6501, Communications Assistant for Law Enforcement Statute, 47 U.S.C. §1001, Computer Security Act, 40 U.S.C. §1441, Consumer Credit Reform Act of 1996, Pub. L. 104-208, Criminal Justice Information System Statute, 42 U.S.C. §3789G, Customer Proprietary Network Information Statute, 47 U.S.C. §222, Driver's Privacy Protection Act, 18 U.S.C. §2721, Drug and Alcoholism Abuse Confidentiality Statute, 21 U.S.C. §290dd-3, Electronic Communication Privacy Act, 18 U.S.C. §2701, Electronic Funds Transfer Act, 15 U.S.C. §§1693, Employee Polygraph Protection Act, 29 U.S.C. §2001, Employee Retirement Security Act, 29 U.S.C. §1025, Equal Credit Opportunity Act, 15 U.S.C. §1691, Equal Employment Opportunity Act, 42 U.S.C. §2000E, Fair Credit Billing Act, 15 U.S.C. §1666, Fair Credit Reporting Act, 15 U.S.C. §1681, Fair Debt Collection Practices Act, 15 U.S.C. §1692, Fair Housing Act, 42 U.S.C. §§3604, Family Educational Rights and Privacy Act, 20 U.S.C. §1232g, Freedom of Information Act, 5 U.S.C. §552, Gramm-Leach-Bliley Act, 15 U.S.C. §6801, Health Insurance Portability and Accountability Act, Pub. L. 104-191, Health Research Data Statute, 42 U.S.C. §242m, Mail Privacy Statute, 39 U.S.C. §3623, Paperwork Reduction Act of 1980, 44 U.S.C. §3501, Privacy Act, 5 U.S.C. §552a, Privacy Protection Act, 42 U.S.C. §2000aa, Right of Financial Privacy Act, 12 U.S.C. §3401, Tax Reform Act, 26 U.S.C. §§6103, Telephone Consumer Protection Act, 47 U.S.C. §227, Video Privacy Protection Act, 18 U.S.C. §2710, Wiretap Statutes, 18 U.S.C. §2510.

<sup>20</sup> DEPARTMENT OF COMMERCE INTERNET POLICY TASKFORCE, CYBER SECURITY, INNOVATION AND THE INTERNET ECONOMY 22-32 (2011).

<sup>21</sup> 阪本昌成『プライバシー権論』（日本評論社、1986 年）261 頁。

<sup>22</sup> 牧田潤一朗「アメリカのプライバシー保護法制の日本への示唆」Law & Practice 4 号（2010 年）212 頁。

<sup>23</sup> MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW 1870-1960: THE CRISIS OF LEGAL ORTHODOXY 151-156 (1992).

<sup>24</sup> U.S. CONST. amend. I.

スピーチとパブリック・スピーチ、または公的な性質（報道する意義）があるものとそうではないものとの伝統的に区分されている。私的な会話はプライベート・スピーチにあたるが、プライベート・スピーチに対する修正第1条の保障は強く、たとえば、急迫かつ具体的な違法行為の発生を伴わない限り違法行為や不法行為の談合をしたとしても政府はこれを罰することはできないとされる<sup>25</sup>。伝統的な区分をインターネット上のスピーチに適用することが適当ではないことは、すでに憲法学者の間で広く認められているが<sup>26</sup>、スピーチに対する合衆国憲法修正1条の保障は、スピーチが口頭でなされたか文書の上に表現されたかホームページ上のものかという形式的な基準で判断されるのではなく、営利的か名誉毀損的なものか公益性を有するかというような性質によって主として判断される<sup>27</sup>。だからこそ、スピーチ活動のために公共の場所を使用する権利もまたパブリック・フォーラムとして修正1条の保障の射程に入ってくるのである<sup>28</sup>。

このような英米法の柔軟性は、情報セキュリティの法的定義を試みる際には有用であると考えられる。英米法的な発想を導入することも、今後の日本では一つの手法として評価されるべきなのではないか。

付言すれば、わが国におけるプライバシーやアクセス権、自己情報コントロール権の法理の形成に当たっては、アメリカのプライバシー権理論に大きな影響を受けた。にもかかわらず、官・民・自治体の個人情報保護の基本法的な性格を持つ通則法として個人情報保護法を制定したことに見られるように、それに対応する法制度の構築にあたっては伝統的な立法手法に依った。このことも、今日の個人情報保護をめぐる混乱の一因になっていると思われる。

### 3 ソーシャル・メディア情報の法的地位

上述したような情報や情報セキュリティに関する法的定義の手法を手がかりとして、政府がソーシャル・メディア上で発信する情報の法的地位について検討してみたい。

公権力を発動して強制力をもって政策を実現しうる

<sup>25</sup> *Brandenburg v. Ohio*, 395 U.S. 444 (1969).

<sup>26</sup> Geoffrey Stone, *Privacy, the First Amendment, and the Internet*. IN SAUL LEVMORE AND MARTHA NUSSBAUM EDs, *THE OFFENSIVE INTERNET: SPEECH, PRIVACY AND REPUTATION* 186-189 (2010).

<sup>27</sup> JOHN E. NOWAK & RONALD D. ROTUNDA, *CONSTITUTIONAL LAW* (5TH ED.) 986-987 (1995).

<sup>28</sup> *Adderley v. Florida*, 385 U.S. 39 (1966); *Shuttlesworth v. City of Birmingham*, 394 U.S. 147, 152 (1969); *Grayned v. City of Rockford*, 408 U.S. 104, 115 (1972); *Carey v. Brown*, 447 U.S. 455, 460 (1980).

政府や自治体の情報発信は、その内容についてそれが直接国民の権利義務関係に影響を与えた場合の法的責任にとどまらず、内容の公正性や正確性についてのアカウントビリティを要求される。しかし、国民や住民が後になってそれらの情報にアクセスしようとする場合には、情報公開制度を利用する他はない。したがって、目下の喫緊の問題はこれらの情報が「行政文書」に該当するかどうかとなる。仮に行政文書に該当する場合には、情報公開請求の対象となり、公文書として一定期間保存する義務も生じる。逆に行政文書に該当しない場合には、行政は後になって発信した内容を公開する義務もなく、保存義務もないので、「言いつ放し」状態となる。後になって政府が国民に対してどのような情報を発信したのかを検証することも困難となってしまう。

行政文書にあたるかどうかは、行政機関の保有する情報の公開に関する法律2条2項の「行政機関の職員が職務上作成し、又は取得した文書、図画及び電磁的記録（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）であつて、当該行政機関の職員が組織的に用いるものとして、当該行政機関が保有しているもの」に該当するかどうかで判断される。

一般に、情報と文書の関係について、既存の法的枠組みからは、まず情報が「文書」に該当するかどうか問題となる。

民事訴訟法においては文書および準文書を規定しているが、前者は紙片等に文字その他の符号をもって何らかの思想を表示したものと解されており、後者は図面、写真、録音テープ、ビデオテープなど情報を表すために作成された物件をさす（民事訴訟法231条）。ここでいう文書と情報の関係は、後者は有形物としての媒体（前者）に記録すべき内容を指すものとなる。このため、ソーシャル・メディアにおける情報は、スマートフォンやコンピュータ・ディスプレイ上で視聴する限りにおいては文書とは言い難く、何らかの媒体に電磁的に保存して状態で準文書となりうる。

一方、ほかの領域では「書類」と情報の関係について規定している場合もあり、紙片等に文字その他の符号をもって何らかの思想を表示したものを常に「文書」と呼ぶわけではない。たとえば金融商品取引法附則第7条は、「新金融商品取引法第七十二条の三の規定は、（中略）記載対象事業年度（新金融商品取引法第八十五条の七第二十九項各号に掲げる書類又は情報の区分に応じ、（後略）」と定めている。ここでいう書類は

有価証券報告書、四半期・半期報告書等のことをさし、情報は開示用電子情報処理組織の用に供するため当該報告書類に記載すべき内容を電磁的に記録したものを指しており、ここでの書類と情報との関係は、民事訴訟法における文書と情報との関係に類似している。

ただし、公職選挙法は法定ビラ等以外の選挙運動のために使用する文書図画の頒布を禁じているところ（公職選挙法 142 条）、1996 年に新党さきがけが自治省（当時）選挙部長に対してインターネット上のホームページの開設と公職選挙法との関係について回答を求め、選挙部が公職選挙法の「文書図画」とは、文字若しくはこれに代わるべき符号又は象形を用いて物体の上に多少永続的に記載された意識の表示をいい、スライド、映画、ネオンサイン等もすべて含まれるのでディスプレイに表示された文字等は公職選挙法の「文書図画」に当たると回答したことから、公職選挙法の上ではこれらのソーシャル・メディア上の情報は「選挙運動のために使用する」のであれば文書に該当すると解されている。ここでいう文書と情報の関係は、文書＝情報となる。

以上をふまえて考えると、ソーシャル・メディア上の情報は、「行政機関の職員が職務上作成した」文書、図画及び電磁的記録には該当しよう。しかし、行政文書の保有・占有という問題がある。

情報公開法及び多くの自治体の情報公開条例においては、前述したように「当該行政機関が保有している」ものを開示請求の対象としており、一般的には行政機関が情報が記録されている媒体（紙、電磁的記録等）を占有している場合に「保有している」に当たると解されている。民間事業者の運用するソーシャル・メディアにおいて行政機関が発信した情報については、行政機関が保有しているといえるであろうか。ある程度の長文の情報については行政機関で下書きを作成し、それを保存している可能性もあるが、常識的に考えて Twitter のツイートの下書きは作成しない人が多いであろう。そうであるとすれば、ソーシャル・メディアの情報発信内容について情報公開請求を行ったとしても、不存在を理由として不開示とされる可能性が高い。

この問題は行政におけるクラウドの導入についても当てはまり、クラウドサービスを利用して保存されている行政の情報は、行政が「保有」または「占有」しているといえるのかという大きな論点が存在する。行政が収集、作成した情報であって「当該行政機関の職員が組織的に用いる」のであれば、保存先はクラウドであっても原則的に行政文書と見なすべきであり、行

政の保有するサーバをアウトソーシング等で外部に設置している状態と同じであるが、クラウドの場合は個別の行政情報がどのサーバに保存されているのかは行政機関側にも把握しきれず、支配力を行使することはできない（この点は民間事業者がユーザーとなっている場合も同様であるが）。この点を考えると、当該情報を行政が保有又は占有しているとはいえないことになる。

しかし、このように従来型の解釈で「当該行政機関の職員が組織的に用いるものとして、当該行政機関が保有している」かどうかを基準としてよいものであろうか。ツイッター等に書き込む際に草稿を作成・保存せずに直接書き込んでいる場合は、確かに電磁的記録として行政機関が保有しているとはいえない。しかし、これらの情報が記録されている民間ソーシャル・メディア上の情報について、当該自治体が ID とパスワードを所有して独占的に書き込みや削除を行っている場合には、不正アクセス行為の禁止等に関する法律 2 条の定義なども参酌しながら、物理的に行政が所有したり業務委託等で特定のサーバにアウトソーシングしたりしているサーバに記録していても、特定利用として「保有」していると解する余地があろう。このように解しないと、行政がクラウドを利用する場合に、クラウド上で保存されている情報は行政が「保有」しているとはいえない、ということになってしまう。

ただしこの場合にも問題となるのは、保存義務である。そもそもブログやツイッター等のソーシャル・メディアの時間軸については現在（「××なう」の類）や近い将来のことが基軸となっているのであるから<sup>29</sup>、これらのメディアにおける過去の情報の保存について本来あまり意味はないという見方もできるが、行政が保有する情報であるという立場からは一定期間の保有義務が生じることになる。それは誰が負うのであろうか。また、どのように担保することができるであろうか。

さらに、近時は大臣や自治体の首長等の記者会見内容については逐語的にホームページで公開する例も増えている。しかし、公務員の職務に関係する口頭の発言をすべて文書に記録して保存することが義務づけられているわけではないところ、ツイッターは「つぶやき」であるから口頭の発言に相当するものであり、公務員等のツイッターにおけるツイートは口頭の発言に相当する情報を即時的に公衆送信するために簡易的に

<sup>29</sup> GREG MYERS, THE DISCOURSE OF BLOGS AND WIKIS 75-76 (2010).

文字情報に置換して送信したに過ぎず、本質的には文書には当たらないという見方も可能である。

このようにして考えてみると、文字情報として画面上に表示される以上「文書、図画又は電磁的記録」として体系的に取り扱う、という既存の対応方法には、相当の無理がある。そもそもソーシャル・メディアが今日の形態で何年間通用するのかも不透明であるが、ソーシャル・メディアにおいて発信される情報の性質に応じて何らかの法改正で対応するほかはないのではあるまいか。

#### 4 おわりに

今回の輪講ではソーシャル・メディア上の政府情報の法的性質に対する考察を行ったが、情報セキュリティ法制の観点からはソーシャル・メディアには多くの問題点が山積しているといつてよい。

プライバシーが軽視されがちなことはその一例であり、Facebookの創設者であるMark Zuckerbergは「プライバシーはもはや社会的な規範ではない」と公言したと報じられている<sup>30</sup>。「憲法的プライバシー権が即コントロール権としてのプライバシー権ということにはならない」<sup>31</sup>にしても、ソーシャル・メディア上のプライバシーの期待が情報主体によってすべて放棄されているわけではないであろう。独占が生じやすいことはネットワーク上のビジネスの特性であるが<sup>32</sup>、ソーシャル・メディアもその例外ではなく、大量のユーザーが登録・利用するのは早くも少数のソーシャル・メディアに収斂しつつある。そのような環境の下で、ソーシャル・メディア側による一方的なプライバシー・ポリシー変更等に対するユーザー側の対抗手段は乏しく<sup>33</sup>、人々の生活がソーシャル・メディアに依存するようになればなるほどサービス提供中断・停止や提供内容の変更が利用者の権利利益に対する大きな侵害となりうる<sup>34</sup>。これらがいわゆる熟慮の民主主義に広く利用されるようになれば、政治的見解についての言論の保護の是非や、憲法の秘密選挙の自由は政治的意

思・見解を匿名で表現することに対する保障まで射程となるかも問題となる<sup>35</sup>。その一方で、利用者の権利利益の侵害の危険性を恐れる余りにプライバシーを含む情報の利活用について極度に警戒的になることは、ICT利活用の停滞のみならず社会全体の停滞を招く恐れもあり、「もしデジタル・ネットワーク社会がその変化を停滞させるものになるようなら、それは本来の情報社会とはいえ」<sup>36</sup>ないことになる。

またソーシャル・メディアにおける情報に対する人々の信頼度は誰からの発信かという点に大きく依存するといわれ<sup>37</sup>、市民が情報の信頼性を判断する際に「主に見ているのは、情報の中身ではない。見られているのは『発信者が信頼に値するかどうかである』」という<sup>38</sup>。そうであるとすれば、今回の東日本大震災と福島原発に係る情報発信について、なりすましを防止し情報の発信者が政府・自治体であることを明らかにすることは確かに一定の意義があったといえよう。ただし、その「一定」というのは、今回は発信者の身元が政府・自治体であることが明確であったものは、逆に国民に信頼されなかった、ということである<sup>39</sup>。

本校では紙幅の制限からアメリカにおけるEFOIAやソーシャル・メディア情報の法的位置づけに触れることができなかつたので、今後はそれも参酌しながらソーシャル・メディア上の政府情報の法的性質をさらに考察し、それを手がかりとして既存の権利義務関係の解釈や体系を見直し「情報セキュリティ」に何らかの法的定義を与える可能性について探求していきたい。

#### 参考文献

本文の各注に示すもの。

※本稿は、科学研究費補助金基盤研究C「熟議の民主主義の形成を実現する情報法制度」(研究代表:湯淺壘道)の研究成果の一部である。

<sup>30</sup> Bobbie Johnson, "Privacy No Longer a Social Norm, Says Facebook Founder" (Jan. 11, 2010), <http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy>.

<sup>31</sup> 堀部政男『現代のプライバシー』(岩波書店、1980年)118頁。

<sup>32</sup> 林紘一郎『ネットワークの経済学』(NTT出版)1989年。

<sup>33</sup> Ruben Rodrigues, *Privacy on Social Networks: Norms, Markets, and Natural Monopoly*, in SAUL LEVMORE AND MARTHA NUSSBAUM EDS, *THE OFFENSIVE INTERNET: SPEECH, PRIVACY AND REPUTATION* 255-256 (2010).

<sup>34</sup> EVAN CARROLL AND JOHN ROMANO, *YOUR DIGITAL AFTERLIFE: WHEN FACEBOOK, FLICKER AND TWITTER ARE YOUR ESTATE, WHAT'S YOUR LEGACY?* 74-83 (2011).

<sup>35</sup> Josh Halliday, "Twitter Unmasks Anonymous British User in Landmark Legal Battle" (May 29 2011), <http://www.guardian.co.uk/technology/2011/may/29/twitter-anonymous-user-legal-battle>.

<sup>36</sup> 松岡正剛『私が情報について語るなら』(ポプラ社、2011年)461頁。

<sup>37</sup> 藤代裕之「ソーシャルメディアの登場で風評の広がり方が変わった」宣伝会議814号(2011年)30頁。

<sup>38</sup> 三上直之「専門家の伝える『正しい知識』はなぜ市民に信頼されないのか」宣伝会議814号(2011年)51頁。

<sup>39</sup> 野村総合研究所「震災に伴うメディア接触動向に関する調査」(2011年)。 <http://www.nri.co.jp/news/2011/110329.html>