アメリカにおけるインターネットへの司法権力の介入

白田 秀彰

1997年 10月 17日

1　はじめに

本報告を依頼される直前に、あるシンポジウムでネットワークにおける倫理綱領について討議するセミナーに参加した。前の講演まで満席に近かった会場が、とたんに閑散とした様子をみて、法律や規範といったものがサイバースペース[1]に関わってくることに対する、技術者の方々の声無き反発を聞いた思いをした。また、このIAJ News 96年1月の石田教授の記事においても、「インターネットには規制を持ち込まれたくない」という率直な記述があった。こうした法律や規制に対する警戒感は健全なものであるが、そうした警戒が単に法律や規制に抵抗すればよいというのでは、敵を知らずして戦うのに似て、百戦危うしということになろう。

法が存在しない状態とは、逆に言えば法による保護を受けられない状態を意味する。例えていうなら、荒野における自由である。そこでは自分の行動によって生じる結果を全て自らの責任で処理しなければならない。法は我々の行動を規制するが、法に則って行動する限り、我々は法により保護される。合理的かつ明確な基準により、ある行為が禁止されているならば、我々はその行為をしていないことを立証することで、法によって保護されることになる。問題は、法律に携わるものの無知によって、しばしば不合理かつ不明瞭な規制が設定されることにある。そうした場合、我々は萎縮してしまい、禁止行為を必要以上に広く想定して、本来行うべき活動を制限してしまうことになる。

たとえば、いまアメリカのサイバースペースを沸騰させている1996年電気通信法による合衆国法典47巻223条の改正(いわゆる通信品位法)に対する批判点も、この改正が曖昧な「品位を欠く表現」という基準で通信内容を規制することにあるのであり、この改正に抵抗しているネットワーク市民団体(EPIC、CDT、EFF等)も、サイバースペースにおける表現が全くの野放しでよいとしているわけではない。それら団体は、法において禁止される表現をより明確かつより限定的にしようと活動しているのである。

サイバースペースへの法の過剰な侵入を警戒するならば、技術者もまた法を知り、立法者、法曹に対する継続的な指導と警戒をつづけなければならない。アメリカにはこうした団体が多数存在する一方で、我が国にはそうした団体がまだ見られない。これが筆者が最も懸念し警戒するところである。このことは、日本のサイバースペースにおける政策や法律上の欠陥を生む要因となるだろう。

本論は、アメリカのサイバースペース政策の背景にある一貫した姿勢について解説するものである。詳細については、出版予定の原稿があるゆえ、そちらを参照して頂きたい。刊行の詳細についてはfj.soc.lawに告知を出す予定である。

[1]この言葉は、アメリカではコンピュータ・ネットワークを「空間」として把握する場合に一般的に使用されており、法律論文でもこの領域を取り扱うものでは定着している。

2　もう一つのインフラ整備

NII行動計画[2]では、薔薇色のNIIの未来が語られるなかで、繰り返し「security」「privacy」「law enforcement」が重点課題として掲げられていることに気が付いただろうか。技術者の方々は、前二者については、直ちに対応する技術について思い到るだろう。しかし、最後の「law enforcement」についての具体的なイメージを思い浮かべることは難しいと思われる。実はこの「law enforcement」を一本の縦軸として、サイバースペースに対するアメリカ政府のさまざまな介入を整理することができるのである。

1980年代からコンピュータ犯罪が司法当局の関心を引くようになった。それらは、いわゆるホワイトカラー犯罪と呼ばれる類型が、単にコンピュータを使って行われているに過ぎないのであるが[3]、司法当局がコンピュータ技術に不慣れなため過剰に警戒されることになった。戦後のアメリカ政府は、国防や治安維持を、合衆国憲法によって設定された国民の権利よりも優先させる傾向があるが、コンピュータがまさに国防や治安機構の要となっていたことも背景となっていた。とくに、FBIやCIAは冷戦時代を通じてアナログ通信の盗聴や傍受を継続して行ってきており、この電子的監視(electronic surveillance)の能力がデジタル通信時代において失われることを怖れていた。

これに対応して、司法当局と諜報当局による三つの対策が始められた。第一に、 政府がサイバースペースの電子的監視を行うことの必要性を正当化ために、具体的な事例について宣伝すること。第二に、法律を制定し、通信の内容を傍受できるように電話回線や他の通信回線を設計させること。第三に、通話に用いられる暗号の種類をあらかじめ司法当局が解読できるものに限定するような法律を制定することである[4]。

2.1　電子的監視

第一の電子的な監視の例としては、1989年から90年にかけて行われたハッカー一斉取締、すなわちサンデビル作戦(Operation Sundevil)が挙げられる。詳細は、「ハッカーを追え![5]」という手軽な読みものになっているのでそちらを参照して頂きたい。この取締の目的は、ハッカー[6]という反社会的集団が存在しており、社会がその脅威にさらされていることを一般にアピールすることにあった。

この一斉取締では、刑事告発された人物が一人もいなかったのみならず、ある出版社のコンピュータをまるごと押収するといった過剰捜査も行われるなど、ずさんなところが見られた[7]。しかし、この事件によって、EFF等のネットワークにおける市民の権利を擁護するNGOの設立が加速されたのは、良い副産物であったといえる。

この事件によって、サイバースペースにおいても電子的監視が行われていることが、一般に意識されるようになった。こうした動きへのサイバースペース利用者側の対応として暗号通信が注目されるようになり、さまざまな暗号化プログラムが開発される原動力のひとつとなった。ところがPGPに代表されるような強力な暗号化プログラムが野放しに使用されると、司法当局の電子的監視の能力は実質的に失われることになる。こうしたことから、司法当局は寄託鍵暗号規格(Escrowed Encryption Standard: EES)[8]を開発

[2] The National Information Infrastructure: Agenda for Action, Federal Register, vol.58, (1993) 49,025 available online URL ftp://ftp.apple.com.

[3]「皮肉にもコンピュータは、ホワイト・カラー犯罪を民主化した」August Bequai, 情報犯罪, 堀部 政男 and 堀田 牧太郎 trans., (啓学出版, 東京, 1986) 70
という言葉によって指摘されているように、コンピュータ犯罪それ自体はほとんどの場合、古くから存在した犯罪類型にあてはまる。

[4] A. Michael Froomkin, The Metaphor is the Key: Criptography, the Clipper Chip, and the Constitution, U. Pa. L. Rev., vol.143, no.3,(1995) 743.

[5] Bruce Starling, ハッカーを追え!, 今岡 清 trans., (アスキー出版局, 東京, 1993).

[6] 筆者は「ハッカー」と「クラッカー」を使い分けている。これらの語義については、
Eric Raymond, The New Hacker's Dictionary, (1991) 参照。また、拙稿、ハッカー倫理と情報公開・プライヴァシー in 「高度情報化社会の法体系と社会制度」, 重点領域研究103 情報化社会と人間 研究成果報告書, (1995) においてハッカーについて検討している。この原稿は、http://srv.cc.hit-u.ac.jp/usr/hideaki/indexj.htmlにて参照可能。

[7] Steve Jackson Games Inc. et al v. United States Secret Service, 816 F.Supp 432 (W. D. Tex. 1993).

[8] 技術的内容については、Froomkin, supra note 4, at 758{759 に簡単な紹介がある。

し、必要に応じて司法当局が暗号通信を解読できる暗号システムのみを合法としようと図ったのである。司法当局は、まず議会での立法を経ず、電話会社に対してこうした機構を任意に採用するように働きかけたが失敗。ついで1992年より議会の制定法でEESを強制することを試みた。この一連の試みが、クリッパー騒動である。アメリカでは、このEESの強制に対してネットワーク市民団体や利用者からの轟々たる非難があがったため、議会に法案が提出されることさえなかった。

EESは、政府による強制的な規格とはならなかったが、任意に採用されうる規格としては存続した。そして、1994年のはじめには、第三の暗号鍵を保有する寄託機関が民間に設立され、商用化・実用化が始まった。これらは、商用暗号鍵寄託 (Commercial Key Escrow) と呼ばれている。

こうした民間の寄託機関を利用すること自体は任意であるから、なんら問題は生じない。ところがこの任意性が操作されているのである。具体的にいえば、政府がEESを民間に推奨し、また、政府が内部的に使用する通信機器にクリッパーと同じ仕組みを仕様として定め、これを大量購入するならば、EES型の暗号化機構は他の暗号化機構に比較して市場で優位に立つことになる[9]。この市場機構を利用した、事実上の標準としてのEESを目指す手法は、アメリカ市場のみならず、他国の市場でも有効に作用するものと思われる。

国立科学技術院 (NIST) は、連邦情報処理基準 (FIPS) を示すことで、政府内で使用する情報技術とコンピュータの基準や仕様を決定する権限を持っている。さらにFIPSは、産業界が利益を得ることができるとNISTが判断した領域の国家的な規範を示すためにも用いられる。公式には、FIPSに拘束されるのは連邦行政府の機関だけであるが、しかしながら、実際の影響力は、しばしば、国家的な事実上の標準を決定する力を持っている[10]。

通常の場合、FIPSは明確な納入基準を示す。しかしながら、EESに関しては、「国家安全保障局 (NSA) の技術基準に適合した」暗号化機構を要求するのみである。ところが、EESの基幹技術、すなわちスキップジャック・アルゴリズムは機密とされているから、政府からスキップジャックの使用を許可された一部企業しか実際には納入できないのである[11]。行政手続法 (Administrative Procedure Act) 第553条[12] では、政府が行う決定に関する詳細な告知の手続が規定されているが、このFIPSは政府納入に必要な情報を意図的に公にしていない点で、正当な告示とはいえないとも指摘されている[13]。また、こうした脱法的な手続で通信機器の購入を行うにあたって、予算面における議会からの追及を避けるために、違法品の押収から上がった収益である、"Asset Forfeiture Super Surplus Fund" を用いて9000台のクリッパーを組みこんだ通信機器の購入計画が立てられている。この資金の使用には議会の承認が不要だからである[14]。「政府は、このような大量購入に由来する市場への影響力を通じて、事実上EESへ補助金を与えているのに等しい[15]。」

また、合衆国政府は、武器輸出規制からEES製品を除外しようと考えていることを発表している。もしこれが実現すれば、EES適合品は唯一の輸出可能な高度暗号化機構ということになる。これは、アメリカ国内の競合する通信機器製造企業への大きな打撃になるだろう。このように合衆国政府は、政府基準決定能力、連邦政府の購買力、また輸出規制の制御を通じて、事実上の標準としてEESを定着させようとする意図を隠さない。そこには、制定法による承認も、議会による予算の制御も及ばないのである。

以上のように、暗号および電子署名すなわち「security」や「privacy」のためとして推進されている技術が「law enforcement」と結合する形で計画されていることがうかがわれるのである。クリッパーをめぐる一連の動きは直接的だったため、明確にその意図が透けてみえた。同様に、昨年注目を集めたエクソン法案と呼称される「通信品位法 (CDA)」の騒動も、この文脈からみると、単に猥褻や下品な通信内容が禁

[9] Jaleen Nelson, Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Eãect on Free Flow of Information and Privacy, UCLA Law Review, vol.41, no.4,(1994) 1141.
[10] Froomkin, supra note 4, at 765.
[11] Id. at 766.
[12] 5 U.S.C. x553(b){(d).
[13] Froomkin, supra note 4, at 767.
[14] 28 U.S.C. x524(c)(4). 参照、Id. at 770 n.244.
[15] Id. at 770.

止されたという表層的な把握とは全く異なった様相を見せるのである。

2.2 通信内容規制

アメリカ社会が最重視する価値の一つに、未成年者の保護がある。成人の行動や選択に関しては、かなり寛容なアメリカ社会であるが、未成年者を健全に育成するという目的のためには、かなり大胆な施策が容認される雰囲気があるように思われる。裁判所は、放送内容の制限をするにあたって、未成年者の健全な育成に根拠をおいてきた。サイバースペースへの政府の介入を正当化する理由として、1990年前後にハッカーの脅威が強調されたことは先に述べたが、次いで1995年には、ネットワーク内部を流通する危険文書や猥褻文書の存在に矛先が向けられることになった。

エクソン上院議員は1994年秋に上院で検討されたものの結局廃案となった「1994年通信法改正法案[16]」の頃から、サイバースペースに存在する情報内容の道徳的品位を維持するために、サイバースペースに連邦通信委員会(FCC)による内容規制を適用することを主張してきた。このため、サイバースペースへの政府の介入を嫌う古参の利用者たちの間では、彼の新しい法案は要注意とみられていたが、それが上院を通過するに到り、政府の介入が具体的になり出したわけである。

エクソン法案は、州を越えて放送や電話で伝送される内容を規制する合衆国法典47巻223条の規定[17] を、コンピュータ・ネットワークで伝達される全ての形態の通信内容に拡張し、猥褻あるいは下品であると判断されうる内容を、ネットワーク上で保有あるいは伝達することを禁じるものである。1996年電気通信法による改正以前の第223条は、あくまでも電話を念頭において作成されていた。そこで、エクソン法案2条(a)項以下では、旧第223条の \telephone" という記述を全体的に \telecommunication" と置き代えることで[18]、FCCによる迷惑電話規制に関連して適用されてきた法理をサイバースペースに拡張しようとしていた。この改正の結果、改正後の第223条では、電話を含む広い意味での電気通信設備をもちいて、禁止されている内容を伝達することに関与した全ての当事者が、25万ドル以下の罰金あるいは2年以下の懲役、またはその両方に服さなければならないことになる[19]。

端的にいえばこの法案は、ネットワークの伝送路に関与している全てのコンピュータ管理者に通信内容に関する責任を課するものである。これによって、刑事罰を避けたいと考える管理者は、自発的に通信内容の閲読と管理を行うよう動機付けられることになる。司法当局は、かつて通信内容の開示を電話会社に直接的に請求して失敗したことを教訓に、間接的なものへと戦略を変更しているのである。

しかしこの法案は、ネットワークの運用形態についての配慮を欠き、あまりにも欠陥の多いものであるために、2月の上程時からサイバースペースでは多数の批判が表明され、同法案の廃案を呼びかける警告がニューズグループなどに掲載された。そこでは、専門家から素人までを含む幅広い人々が修正第1条（言論の自由）に関する議論を戦わせ続けている。このエクソン法案と合衆国憲法修正第1条との間の法律論は、複雑かつ紙幅を必要とするので割愛し、ここでは、このエクソン法案に固有の問題点を述べるに止める。

批判者たちは、この法案の文言に従うと、情報伝達経路の途中に位置するコンピュータの管理者までが、実際に猥褻的な情報内容を提供するコンピュータにおいて生じた法的責任までも、負担しなければならないことをとくに問題とした。インターネットは、多数のコンピュータが境目なく結合して運用されるので、この法案のもとでは、同法で禁止される種類の情報内容の作成者だけでなく、これが伝達されて行く経路として使用されたコンピュータ管理者までが訴追されることになる。ところがこうした情報の伝達はほとんどが自動的に行われているので、コンピュータ管理者はどのような内容が伝達されているのかを知ることは困難なのである。また商業通信事業者は、この法案に従うならば、自らのネットワークの中に存在する全ての通信について検閲を行わなければならなくなる。しかも、「猥褻」や「下品」の定義について明確な

[16] Telecommunications reform bill of 1994, 103rd Congress, S.1822, Sec. 801{804.
[17] 47 U.S.C. x223.
[18] S.314 x2 (a).
[19] 47 U.S.C. 223(d)(2)

基準が存在しないので、最も広い基準においてこれらの内容に該当するものと思われる通信を排除しなければならない。これらの規制はネットワークで提供される議論の内容を著しく制限することになるだろう。

エクソン法案の批判者たちも、サイバースペースで流通している情報の中には未成年者にふさわしくないものがあることを認めている。そこで、彼らの主張する言論の自由と未成年者の保護という両方の目的を両立させるために、未成年者についてアクセス規制を行うべきであるという主張が批判者の側から出された。彼らは、コンピュータやモデムは、電話やテレビよりも閲覧される素材についてより大きな制御能力を両親に与えているという。ネットワークでは、利用者の認証やアクセス制限が既存のマスメディアに比較して容易に達成され得るので、利用者の側で望まない情報を受信しないように設定すべきであるというわけである[20]。

結果的には、こうしたサイバースペースにおける組織的反対運動にもかかわらず、1995年6月にエクソン法案は上院を通過し、1995年通信法改正法案(Communications Act of 1995)の一部に組みこまれ、1996年2月には、1996年電気通信法(Telecommunications Act of 1996)第5編「電気通信設備による猥褻、嫌がらせ及び悪用(Obscene, Harrassing, and Wrongful Utilization of Telecommunications Facilities)」として成立するに到ったのである。

この成立した法では、ネットワーク利用者たちの批判にある程度応え、自らの制御(control)の及ばないことに関して、訴追されないとする条項が盛り込まれた[21]。しかし、この条項での「制御」は、放送事業者が放送内容に関して責任を負う場合の前提である「編集上の制御(editorial control)」よりも広い概念であることに注意する必要がある。

この法案成立前後には、「ネットワークにおける検閲が始まる」と警告するおびただしい電子メールが複数のネットワーク市民団体から筆者のもとに届いた。また、法案成立の日にEFFは、この電気通信法第5編への抗議を示すために、ホームページを黒く塗り潰したり、抗議運動のシンボルである「青いリボン」の画像を表示することを呼びかけた。また、直ちにこの法律の違憲性を申し立てる訴訟がペンシルバニア州東部連邦地裁に提起された[22]。被告となった連邦法務総裁は、連邦地裁の判断が示されるまで、合衆国法典47巻223条の適用を指し控えることに合意している[23]。

これまでの合衆国連邦最高裁の言論の自由に関する判例をみるならば、1996年電気通信法で設定された内容規制の枠組みは、ネットワーク通信が実質的に放送と同じものとして認められない限り容認されない。逆に言うならば、1996年電気通信法第5編が合憲とされるならば、ネットワーク通信が実質的に放送と同じ規制枠組みのもとに入ること意味することになる。同法による改正で挿入された合衆国法典47巻223条(e)項では、電気通信に関与する者が、同条に規定された罰則から免責されるための条件が示されている。しかし、いかなる行為を行えばこの条件に合致したとされるかについては、裁判所に判断を預けてしまった同項の(5)と、FCCがその基準を定めるとする(6)があるにとどまる。コンピュータ・ネットワークに関する223条についての判例が存在しない現状においては、事業者はFCCが定めるだろう基準に依拠して運営を行う他ない。そうであるならば、たとえ(5)の後段において、FCCがコンピュータ・ネットワークについて監督権限を持たないことを強調したところで、意味を持たないのである。

このようにして見るならば、猥褻の規制と未成年者の保護(広い意味での「privacy」「security」としてアメリカでは把握されている)を経由して、サイバースペース全体を政府の監督下に置く(「law enforcement」)というのが、エクソン法の本質なのが理解されるだろう。

---

[20] 例えば、Testimony of Regarding \The Protection of Children from Computer Pornography Act of 1995", (Washington, D.C., 1995, Hearing of the Senate Judiciary Committee available online URL `http://www.cdt.org/cda.html` 等。

[21] 47 U.S.C. 223(e).

[22] American Civil Liberties Union et al v. Janet Reno, Attorney General of the United States, Civ. No. 96-963 (E. D. Penn., 1996).

[23] Id., Stipulation, 4.

3　結びに代えて

彼の国の法律が我が国にどのような影響を及ぼすのかは、筆者には予測の及ばないところであるが、サイバースペースにおけるアメリカの存在の大きさを見ると、対岸の火事として傍観するにはあまりにも大きな問題である。法意識が高く、多数のNGOが存在するアメリカにおいても、巧みな戦略によって、着々とサイバースペースへの政府介入は強化されている。もちろん、こうした政府介入は、直ちに否定されるべきものでなく、サイバースペースが新しい市民社会の基盤として、適切に整備されるべきものである以上、こうした制度面からのインフラ整備がNIIの重点項目であることはむしろ歓迎すべきということができる。

翻って我が国の取り組みはどうだろうか。不必要あるいは過剰な規制に抵抗する効果的な方法は、やみくもに抵抗することではなく、市民の側から積極的に法や政策を理解して、法の手続に従って抵抗することである。くり返しになるが、サイバースペースへの法の過剰な侵入を警戒するならば、技術者もまた法を知り、立法者、法曹に対する継続的な指導と警戒をつづけなければならない。そのための取り組みが未整備なのが懸念される。