ハッカー倫理と情報公開・プライバシー[É]

白田 秀彰

1998年 6月 12日

1 はじめに

クリントン政権が情報スーパーハイウェイ構想を掲げたことで、電子ネットワークは遽に一般の人々の注目を集めるようになっている。なかでも、全世界的情報基盤(Global Information Infrastructure)として事実上機能しているインターネットは、その本来の利用目的である研究者同士の情報交換のみならず、現在は商業利用の可能性が模索され、産業界のインターネット利用が増大しつつある[1]。

インターネットは1960年代末に研究者同士の情報交換のために実験が始まったARPAnetに起源を持つ[2]。それから、現代までの約30年間には、当初からの利用者たちによって独特の倫理、道徳、思想、慣習法とでもいえるような漠然とした規範が形成されている。こうした電子ネットワーク上の先住者たちとでも言えるような人々、すなわちハッカーたちの規範と、後から参入してきた現実社会の規範にはかなりの程度のずれが存在していおり、現在ネットワーク上で生じているコンピュータへの無権限アクセスや著作権侵害等の法律問題の原因として大きく影響している[3]。

しかしながら、法律学の領域でこの電子ネットワーク上の規範について正面から検討されたことはなく、また、一般の人々がネットワークに不慣れなことに起因して、ハッカーは常習犯罪者(outlaw)であるとい

[É]この論文では、次の方々に資料の提供や助言をいただいた。ここに感謝の意を表する。もちろん本論文の内容に関する責任はすべて筆者にある。著書"The Hacker Crackdown"をネットワークで公開され、私の質問に応えて下さった、小説家のBruce Starling氏。論文を送付して下さり、さらに、電子メールで私の誤解を正して下さったジョージタウン大学のDorothy Denning教授。編著書『Think GNU』をネットワークで公開され、私の質問に親切に対応して下さった引地 信之 氏。大量の文献をネットワークで提供し、さらにEFFに関する私の質問に答えて下さったEFFのStanton McCandlish氏。また、ネットワークにおける私の問い合わせに答えてくれた数多くのネットワーカーの方々に。なお、本論文では未刊行のネットワーク上の文書を多数参照している。それらの文書はUNIX等で使用される"ftp"というプログラムで手元に転送してくることができる。所在はすべて掲げてあるので、"ftp"でとり寄せ 参照して頂きたい。

[1] Internetの背景および問題点についての報告は、名和 小太郎, Internetをめぐる制度的課題, 1994 法とコンピュータ 75。また、同報告では、ネットワーク同士を結合する技術である"internet"とアメリカ国防省高等研究計画局(the U.S. Defense Advanced Research Projects Agency: [D]ARPA)、全米科学財団(National Science Foundation: NSF)およびアメリカ航空宇宙局(National Aeronautics and Space Administration: NASA)の援助によって活動している全世界的規模のネットワークである"Internet"を区別している。本論での「インターネット」は後者を指している。

[2] 1960年代、DARPAは大陸間弾道弾による核攻撃に耐えうる国防機構の研究を進めていた。その研究の成果の一つとして、パケット交換通信技術が開発された。それは、一部の基地が核攻撃で壊滅しても国防システム全体が破綻しないように、ネットワークの中心点を持たない分散的な構造になっていた。DARPAの研究活動を支援することを目的として開設されたARPAnetは、このパケット交換通信技術を採用した。採用の理由は、通信の効率性が優れていたからだったという。修羅, Historical Memorandum | コンピュータ・ネットワークとパケット交換網, 13 bit (1981)。ARPAnetは、国防ネットワークの実験線として開始されたとも思われるが、ARPAnetの利用者たちは、この分散的ネットワークが情報の共有を通じて人間の知的能力を大幅に増大させる効果に着目し、ARPAnetを情報伝達の道具として活用する方向性に進化させることになる。Howard Rheingold, 思考のための道具, 285{324 (栗田 昭平 trans., 1987)。このARPAnetにおける実験を通じて基礎づけられたパケット交換通信網が発展し、現在のインターネットの基幹となっている。Vinton G. Cerf 新ネットワーク技術, in コンピューターネットワーク, 18 (別冊日経サイエンス, No. 105, 1992)。この、ARPAnetはゼロックス社パロアルト研究所(Palo Alto Research Center: PARK)や、東西両海岸の大学等の研究機関を結合していたので、多数のハッカーたちがARPAnetに触れることになった。彼らは、ARPAnetの開放的で効率的な研究環境を経験することを通じてハッカー倫理を形成するに至ったと考えられる。Rhiengold, supra note 2, at 285{324。逆にARPAnetの構造がハッカー倫理の影響を受けていたとする見解もある。Steven Levy, ハッカーズ, 180 (古橋 芳恵 and 松田 信子 trans., 1987) (HACKERS: Heroes of the Computer Revolution (1984))。

[3] ネットワーク上の法律問題について、ネットワーク利用者の立場から書かれた要約的かつ包括的な論文として、Anne W. Branscomb 侵される著作権と知的財産権, in コンピューターネットワーク, supra note 2, at 104 がある。

う理解が一般的になっている。実際のネットワークの運用で慣習的に形成された彼らの規範を一切考慮せず、先のような法律問題を直ちに違法行為であると判断することは、ネットワーク上の法律問題を考えるときの態度としてはやや一面的だと思われる。そこで本稿では、「ハッカー倫理 (hacker ethic)」とも呼ばれうる考え方を彼らの主張をもとに整理し、それがアメリカ法に与えつつある影響について検討する。

2 ハッカー

2.1 ハッカーとは

まず、「ハッカー」という言葉は、「日本人」「アメリカ人」という語と同様に、それぞれに異なる個性を持った個人を包括的に指していることに注意する必要がある。したがって、ハッカーがすべて同じような人物であると一般化することは誤りである。次に、この語の指し示す対象が「技術に精通した人」であることについては、これまで参照してきたいずれの資料でも一致している。しかし、その対象が持っている属性については、肯定的なものから、否定的なものまでかなりの幅がある。コンピュータにそれほど精通していない人々が接する放送や出版物などの媒体では、「(特に電子工学的) 技術を悪用して不法な行為を行う人」であるという否定的認識が一般的なものである。一方、コンピュータの利用者の中でも特に早い時期からコンピュータに親しんできた人々 (彼ら自身が否定的意味におけるハッカーでないとしても) の間では、ハッカーという呼称は尊称として肯定的に用いられる場合がある[4]。

近年、コンピュータ・ネットワークが一般化するにつれて、否定的認識がますます大勢を占めるようになっているが[5]、早い時期からのコンピュータ愛好家たちは、ハッカーという呼称の本来の肯定的意味についての啓蒙活動を行い、否定的な意味におけるハッカーのことを「クラッカー (cracker)」と呼ぶように提唱している[6]。

ハッカーという言葉の由来について『ハッカーズ[7]』を見ると、そもそも「ハック」とは、工学系の技術を習得する場合の習得者の態度を示したものであることがわかる[8]。すなわち、その方法が学究的であるというよりも、むしろ情熱的で力任せである点で、しばしば通常の規範を逸脱していることを特徴とする。こうしたハックはしばしば結果において賞賛すべき成果を生み出す一方、その過程で「禁じられていることでも行う」という反社会的な態度を導く[9]。

また、ハッカーたちが大学で学生生活を送っていた時期が、ちょうどベトナム反戦運動およびヒッピー運動の時代と重なったことを原因として、本来政治的要素を持たなかったハッカーという言葉に反政府的、無政府主義的要素が結合することになった。この時期を境に現在まで続く否定的ハッカー象が形成されたものと思われる。特に、この時期、巨大産業に対するささやかな対抗意識と、単に電話料金を支払いたく

[4] 例えば、座談会 ハッカー談義, 19 bit 4 (1987) (出席者: Robert W. Scheiçer, Mark Crispin, Lynn Gold, 石田 晴久, 後藤 滋樹, 多田 好克)。

[5] 例えば、Michael Meyer and Anne Underwood, Crimes of the `Net', 1994 Newsweek 42 等。一方、Paul Wallich, Wire Pirates, 1994 Scientific American 90 等のように、「ハッカー」に代えて「クラッカー」を使用するものもある。また、我が国では「ハッキング」という用語が事実上、クラッカーが行う違法行為を指すものとして扱われている。例えば、堀部 政男 and 永田 眞三郎 and others, 情報ネットワーク時代の法学入門, Ch.6 山中 敬一 担当部分 (1989) や安冨 潔, 刑事手続とコンピュータ犯罪, (1992)。しかし、我が国およびアメリカの現行法規でハッキングという用語は使われていない。Computer Fraud and Abuse Act, 18 U.S.C. x1030 に頻繁に用いられている用法に従って、「無権限アクセス (access without authorization)」と呼ぶほうが適切だと思われる。

[6] ハッカーとクラッカーの区別については、Eric Raymond, The New Hacker's Dictionary, (1991) 参照。The New Hacker's Dictionary は、コンピュータのたち人たちの間の隠語集である。元データは電子的な辞書であり、hal.gnu.ai.mit.edu に置かれている。またやや古いが、坂村 健, ハッカーの研究, 15 bit 20, 21 (1983) に邦語訳された定義内容が紹介されている。またハッカーという語についての最近の客観的な議論は、Bruce Starling, ハッカーを追え!, 86{90 (今岡 清 trans., 1993)。

[7] Levy, Hackers, supra note 2。

[8] Id。

[9] ハッカーの一般的気質については坂村, supra note 6 参照。また、日本におけるハッカー気質についてはハッカーたちの BOF, 19 bit 65 (1987) (出席者: 深瀬 弘彦, 手塚 宏史, 酒匂 寛, 工藤 丈彦, 加藤 朗, 橘 浩志) が参考になる。一方、コンピュータ科学者からの、ハッカーの精神的態度への否定的見解としては、Joseph Weizenbaum, コンピュータ・パワー, 129{152 (秋葉 忠利 trans., 1979)。

ないという堕落した倫理観を背景にして、電話交換機を不正に動作させ、電話料金を免れる「フリーキング (phreaking)」が流行した。この電話交換機の不正利用を行う「フリーク (phreak)」とハッカーはしばしば同一人物だったため、ここでもまた、フリークとハッカーの混同が生じて、「ハッカー」に否定的属性を追加した[10]。

さらに、コンピュータへの無権限アクセスを行うクラッカーたちが自らを「ハッカー」と僭称することが、ハッカーの語義をますます否定的なものとしている。クラッカーたちが無権限アクセスの手法等について記述した電子的文書である \Phrack" で、「ハック」という言葉は無権限アクセスのための手法と同義に用いられた[11]。例えば、「UNIX をハックする」「電話回線をハックする」という場合、このハックは無権限アクセスのために必要な作業のことを指している。こうして、ハッカーは常習犯罪者と同義の言葉として広く認識されるに至った。

本論ではハッカーという語が二面性を持つことを踏まえながらも、あえて古典的かつ肯定的な意味でハッカーという語を用いる。このため、一般的な意味でのハッカーを指す語として、クラッカーを用いる。ジョージタウン大学のデニング (Dorothy Denning) 教授と筆者との電子メールでの議論で、同教授はハッカーが示す対象は「システム侵入者」にほかならないと主張し、ネットワーク社会における貢献者をなぜ素直に「プログラマ」と呼ばないのかと批判された。しかし、肯定的な面におけるネットワーク文化でさえ、いくらか治外法権的状況の下で発展してきたことを考慮すると、やはり、貢献者たちをハッカーと呼ぶのが適切だと思われる。

しかしながら、この両者が曖昧微妙な境界によって区別されていることに注意すべきである。例えば、後に紹介する著名なハッカーであり、Free Software Foundation (FSF) の代表であるストールマン (Richard Stallman) は次のように述べている。

> どのハッカーも権力には我慢することができないのだ。ハッカーの権力に対する反応はいつも、何人も自分を支配することはできないということである。私は賢い方法でそれをなんとかする。それゆえに、ハッカーはセキュリティを破ることを学んだのだ。というのは、セキュリティはある種の支配を意味するからだ。我々は他の人々にコントロールされたくはない。
>
> さて、セキュリティを破ることに魅せられている、幾人かのティーン・エイジャーがいるが、彼らが興味を持つのはそれだけだ。私は、そういうハッカーは良いハッカーだとは思わない。というのは、彼らが人生に対して良い姿勢を持っているようには思えないからだ。彼らは人生で、悪い面を強調しているのだと思う。
>
> むやみにセキュリティを破るのは時間の浪費であり、また何の意味があるのだろうか。もし私がある仕事をしたいが、セキュリティが私を立ち塞いでいるとする。そういう場合にのみ、私はセキュリティを破りたいと思うのだ。その意味では、私はセキュリティを破ったことがあるが。
>
> しかし、本当に私がしたいことは、有用なプログラムを書いて社会の役に立つことだ。私はセキュリティ破りには興味がないし、また、私が必要だと感じる時以外は、セキュリティを破ることについて考える暇もない。
>
> しかし、概してハッカーはセキュリティを破ることは、悪いことだとは思っていない。我々は、それが何を引き起こすかを考える傾向にある。セキュリティを破り、人々を傷つけるのは悪いことなのだ。

[10] ハッカーとヒッピーの関連については、Starling, supra note 6, at 74{78。また、伝説的なハッカーへのインタヴュー集である、Zachary Margulis and Carol Palecki, バークレイ・ハッカーズ, (広谷 渉 trans., 1992) を参照しても、彼らのヒッピー的性格がうかがわれる。また一方では、純粋に技術的なハッカーたちはむしろ政治的な問題について関与することを避けようとしていたこともわかる。Levy, Hackers, supra note 2, at 159{164。この政治的思想性の有無という違いは東海岸にある MIT のハッカーたちと西海岸にあるバークレイのハッカーたちの性格の違いにも原因があるとも思われる。

[11] \Phrack" の所在は、ftp://ftp.eff.org/pub/Publications/CuD/Phrack/以下。

たとえセキュリティを破ったとしても、害のないことをするのであれば悪いとは言えない。害のないことをするのは、悪いことではないだろう[12]。

2.2 ハッカー倫理

上記のハッカーが常習犯罪者であるとする一般的認識の一方で、特に、コンピュータの技術に長けた管理者や研究者、愛好家たちには最も古典的な意味でのハッカーという用法に執着する人々も数多く存在する。こうした人々の間では、ハッカーとは該博なコンピュータの知識を応用して優れたソフトウェアを作成する貢献者のことを意味する。例えば、「C 言語ハッカー」「TEX ハッカー」という用法は、それぞれ C 言語あるいは TEX 組版システムのたち人を意味している。

こうした貢献者たちの努力によって発展せられてきたコンピュータ・ネットワーク共同体の中には、独特の文化あるいは緩やかな倫理が存在している。この文化は時としてネットワーク文化などと呼ばれているが、明確に整理され定義されてはいない。しかし、この文化の基礎となった精神的態度は明確に文書化されている。それは、レヴィーが、著書『ハッカーズ』の第二章に整理して紹介した「ハッカー倫理」と呼ばれるものである。それは次のような内容である。

- è コンピュータへのアクセス、加えて、何であれ、世界の機能の仕方について教えてくれるものへのアクセスは無制限かつ全面的でなければならない。実地体験の要求を決して拒んではならない。
- è 情報はすべて自由に利用できなければならない。
- è 権威を信用するな | 反中央集権を進めよう。
- è ハッカーは、成績、年齢、人種、地位のような、まやかしの基準ではなく、そのハッキングによって判断されなければならない。
- è 芸術や美をコンピュータで作りだすことは可能である。
- è コンピュータは人生を良い方に変えうる。

実際には、ハッカー倫理という概念がすでに存在していたというよりも、むしろ同書による紹介によって、明確に意識されるようになったという見方が正しいものと思われる。これらの規範がレヴィーの創作だというわけではないが、ハッカーたちの共同体に存在する精神的態度の中でも、合法的で評価されるべき部分だけを彼が抽出したものだと理解するのが適当だろう。

レヴィーの記述によれば、これらの規範は、能力の乏しいコンピュータを効率的に動作させる手法を追求するマサチューセッツ工科大学 (MIT) の学生たちの共同作業の中から生じてきたものだった。また逆に、コンピュータを極限まで効率よく機能させるためには、上記の態度が必要とされた。現在、爆発的な勢いでコンピュータやネットワークの利用者が増大している。こうしたシステムで作業を行うとき、利用者がシステムに要求する能力はしだいに増大していく。一方、利用者が費すことのできる資源は有限である。この条件の下、個々の利用者は、自分の求める水準に応じて、システムを効率よく動作させるための手法について取り組まなければならなくなる。このとき、この利用者は、ある程度 MIT の学生たちと同様な考えを持つに至ると考えられないだろうか。

[12] 引地 信之 and 引地 美恵子, Think GNU | プロジェクト GNU 日記とソフトウェアの憂鬱 | , (1993) available online URL ftp://ftp.sra.co.jp/pub/gnu/sra/think-gnu-book.tar.gz。なお、この文献は後に述べる \copyleft" という一定の条件のもとに自由に複製して配布することが認められており、かつ、全文がコンピュータ・ネットワークを通じて、公開されている。本論文で参照したのはこのオンライン版である。オンライン版の所在は、ftp://ftp.sra.co.jp/pub/gnu/sra/think-gnu-book.tar.gz である。したがって、印刷版のページ数を示すことができないが、このストールマンの発言が記述されているのは、『第 2 部　GNU ソフトウェアの関連記事/ インタビュー (2)「「copyleft」は賢いジョークの王様だ」』の部分である。

また、現在のコンピュータ利用者が恩恵を受けているさまざまな技術の原形は、コンピュータ草創期に存在したハッカーたちの生み出したものであるという歴史的事実と、こうしたハッカーたちが強力な個性を発揮して、それぞれが伝説となっていることを背景にして、彼らの「良い目的のためには禁じられていることでも行う」という精神的態度は、コンピュータの研究家・愛好家たちに現在も影響を与え続けている[13]。また、ハッカーたちの精神的態度が、技術的合理性の立場から見た現実の社会に対する批判である一方で、こうした精神構造の持ち主が技術を再生産することを通じて、現在主流となっているネットワーク技術は彼らが好むシステムに親和的な構造、すなわち分散的で水平的な構造を持つようになっている。こうした構造を持つネットワークを一般の人々が活発に利用するようになれば、そのネットワーク構造が暗喩している精神のあり方が、直接にハッカー倫理に影響されていない人々にも影響を与えることになると思われる[14]。

さらに、このハッカー倫理は、特定の言語をもって唱道されているのではなく、日々利用されるシステムの構造として表現されているので、その影響は特定の言語圏に限定されるものではない。しかも、このネットワークは利用者層こそ特殊ではあるものの、先進国および一部の発展途上国を包含するものとなっており、影響力の地理的な広がりはこれまでにない規模だということができる。したがって、ネットワークにおける「情報の自由」を検討する場合の基礎として、このハッカー倫理を無視することはできない。

しかしながら、ハッカー倫理それ自体はアメリカ国内でも廃れたものとなっている。レヴィーの著書の中でも、すでにハッカー倫理の時代は終わったとして記述されているし、ストールマンもまた、それが失われたことを認めている。筆者は、後に紹介する Electronic Frontire Foundation (EFF) のマッキャンドリッシュ (Stanton McCandlish) と電子メールで議論したが、その中でも彼はハッカーが常習犯罪者として認識されていることを認めている。しかしながら、EFF や FSF がハッカー倫理を受け継いで、それを活動の中で具体化しているのではないかという筆者の指摘を肯定している。すなわち、ハッカー倫理は、EFF や FSF の活動の基礎として生き続けているのである。

3 情報の自由

3.1 政府情報の公開

クラッカーがなぜ他者のコンピュータに侵入するか、という点について考えてみると、それが単に面白く、自らの技術を誇示できるからであるというのが一番の目的であり、つづいて、他者のコンピュータに格納されている情報から、なんらかの経済的利益を獲得するのが二番目の目的だろう。しかしながら、さまざまな種類のクラッカー関連文書を読んでみると、コンピュータへの不正侵入を試みるような種類のクラッカーたちには共通した性向がある。それは、政府と、民間とを問わず巨大な官僚組織に対する反感と不信である[15]。彼らの反感の対象は集中管理された大型汎用コンピュータとこれを管理する組織に象徴される権力であり、彼らはそれらの組織を攻撃し、脆弱性を暴くことによって、こうした組織が持つ権威の破壊を狙う。

草創期のハッカーたちの目的は、管理者の裏をかいて大型汎用コンピュータを自由に使うことであり、自らの知的好奇心に忠実なだけだったといえる。しかし、ベトナム反戦運動の頃には、攻撃目標はもっと一般的な社会機構へと広がりを見せるようになる。当時の学生たちは政府と対立的な関係にあり、彼らが政府

[13] 例えば、坂村, supra note 6 もまた、ハッカーを良質のものと悪質のものにわけて把握しており、良質のハッカーを養成することが我が国の計算機科学の発展のために必要不可欠であると主張している。

[14] 「メディアはメッセージである」とする McLuhan の主張はこのことを指している。Marshall McLuhan, 人間拡張の原理: メディアの理解, Ch.1 (後藤 和彦 and 高義 進 trans., 1967)。

[15] 旧西ドイツからアメリカの軍事ネットワークに侵入し、国防情報を旧ソビエトのスパイに売却していたクラッカー集団を摘発することに大いに貢献したストール (Cliãord Stall) もまた、質問に応えるなかで官僚組織への批判をしている。参照 Interview with Cliãord Stoll, 7 UNIX Magazine 84, 85 (1992)。なお、このクラッカー追跡に関する詳細については彼の著作である、Cliãord Stoll, カッコウはコンピュータに卵を生む 池 央耿 trans., (1991) に詳しい。

の情報収集能力に対して妄想的な被害者意識をもっていたことを背景として、民衆の情報力の強化が模索された。その結果が電子掲示版システム (Bulletin Board System: BBS) であり、パーソナル・コンピュータだった[16]。彼らは、個人情報の保有という点で個人にはるかに勝る政府に、技術で対抗しようとした。政府機関の保有するコンピュータへの侵入についても、行政手続法から情報自由法を発展させるというような手続を踏まえた国民による政府監視ではなく、技術の力による直接的な政府情報の公開を狙ったものといえるかもしれない。

現在は、Computer Fraud and Abuse Act (CFAA) 18 U.S.C. x1030 et seq. により、コンピュータへの侵入は、試みただけでも違法となっており[17]、少なくともハッカーたちは法で禁止されるような種類の侵入行為を避けるようになっている。こうしたなかで、合法的な政府情報へのコンピュータによるアクセスを求める動きが起こるのは当然の動きといえるだろう。

ネットワークにおける市民活動団体として著名な Electronic Frontier Foundation (EFF) はその設立当時から、コンピュータによる政府情報の公開を主張して活動している[18]。

現在アメリカ政府が進めている政府組織のネットワーク化はこうした市民団体の圧力によるものというよりも、業務の効率化とサービスの向上を狙った自発的な改善とされている[19]。しかしながら、この政府組織のネットワークは、従来のように中央統制的で閉鎖的な機構構造を独自に構築したものでなく、ハッカーたちが育て上げてきた水平分散的で開放的な機構構造を持つネットワークの一部として整備されつつある。そこで、EFF は、NII 計画を積極的に支援する態度を表明している[20]。この水平分散的ネットワークを政府に導入することによる結果としては二つの筋書きが考えうる。一つは、ハッカー倫理にかなった形態でのこのネットワークはクラッカーの違法行為を減少させるだけでなく、違法行為に著手しようとするクラッカーをハッカーが抑制するという善の循環が達成されるというもので、もう一つは、政府情報への侵入の入り口を政府自ら拡大することで、一層の無権限アクセスの危険が増大し、重要な政府情報が流出するというものである。

この二つの筋書きのいずれが現実のものとなるかは、NII で提供される政府情報の程度に依存するものと思われる。「政府の情報は納税者のもの」という情報公開の原則に立てば、流通が制限されるべき情報は、プライバシーに該当するもののみということになる。政府情報への回路を十分に提供することは、無権限アクセスへの動機付けを減少させるとともに、無権限アクセスそれ自体を違法なものとするための基盤として必要不可欠なものである。民主主義が、国民による政府の監視を前提とする以上、政府が政府情報を過度に秘匿したまま、政府情報へのアクセスを禁止することは、違法者に正当化の口実を与えることになるだろう。

3.2 情報の自由の拡張: 知的財産権

「情報の自由」の主張と相対すると考えられている権利に著作権や特許権等の知的財産権がある。ハッカーの知的好奇心が人一倍強いこと、彼らが経済的にゆとりのない青年を中心として構成されていること、そして、ある程度は左翼運動の影響と思われるが、知識を「共有すべし」との信念を持っていたことから、

[16] BBS システムの最初の試みである Community-Memory については Levy, Hackers, supra note 2, at 197{235。また、パーソナル・コンピュータの発祥については Id. at 236{299。

[17] 18 U.S.C. x1030 (b).

[18] EFF の設立目的は、合衆国憲法の権利章典で保障されている諸原則が新しい通信技術の世界でも同様に保障されることを確保することである。彼らは、最終的には「電子的民主主義」の完成を目指しているという。この目的のために、1) 自由で開かれた通信のための政策を実現するように政策担当者に働きかけ、2) ネットワーク上の正当な自由と権利の確立のために、訴訟を支援し、3) ネットワーク利用者の市民的権利について啓蒙活動を行うとしている。Electronic Frontier Foundation, Inc., General Information About the Electronic Frontier Foundation (1994) ftp://ftp.eff.org/about.eff なお、国内における紹介記事として例えば、下條 真司, USENIX Summer '91 報告 コンピュータ、そして人間社会の未来, 6 UNIX Magazine 19, 23{24 (1991) がある。

[19] 参照、徹底検証 日米欧マルチメディア政策, 144{214 (マルチメディア研究会 ed., 1994)。

[20] Mitchell Kapor, The Case for a Jeãersonian Information Policy, 1993 WIRED available online URL ftp://ftp.eff.org/pub/EFF/Frontier_Files/EFF_Files/NII/highway_kapor.article 参照。また、EFF の NII 関連の文書については、ftp://ftp.eff.org/pub/EFF/Frontier_Files/EFF_Files/NII 以下。

個人用コンピュータの歴史の極めて初期の段階から知的財産権法上の問題が生じていたし、現在でも同様の問題は生じている[21]。

一般に批判されているように、ハッカーがなんらかの形で著作権法に違反する行為をしてきたことは間違いない。しかしながら、彼らが、著作権について一般の人々と比較して、顕著に順法意識や倫理観に劣っているともいえない。というのは、一般の人々の間でも、音楽CDやVTRテープの違法複製が広く行われていることは、周知のことだからである。ハッカーの著作権に対する無頓着さが強調されるのは、彼らが一般に馴染みのない著作物を馴染みのない機器を用いて複製しているからだと思われる。そうであるからこそ、彼らは、何か貴重な著作物を違法に複製しているという増幅された印象を与える。

ハッカーおよびクラッカーが行っている著作権法違反について詳細に検討することは、本論文の目的ではないので割愛し、こうした違法行為を回避するために、彼らがどのような活動をしているのかについて検討することにする。

ハッカーとは、すなわち、コンピュータに関する知的探求を行う者であるから、彼らは自分の（合法、違法を含めて）所有しているハードウェアおよびソフトウェアの解析を自由に行えて当然であると考えている。しかし、実際には解析が禁止されている場合が多い。このことが彼らを刺激する。彼らはハードウェアの細部まで解析を行い、その情報を公表することに大きな意義を見いだしているし、そのような行為はプログラムを書く上で必要不可欠な情報を共有することであるから、他のハッカーたちの賞賛を得ることになる[22]。

こうしたハードウェアの解析は時として、製造者の知的財産権を犯すこととなっている。しかし、ハッカーたちは、単に解析を行うだけでなく、そのハードウェアを効率的に動作させるためのソフトウェアや周辺機器を作成するので、製造者としては、彼らの行為を禁止することは、市場における優位性を低下させることになるため、黙認する場合がある。すなわち、彼らにハードウェアの解析を禁止したならば、彼らは、そのハードウェアを運用するときに生じた問題点の解決方法の公表を行わなくなり、その結果、それぞれの利用者で独自に問題を解決しなければならなくなるため、利用者全体で見た場合の運用に必要なコストが増大するからである[23]。

このことは、ソフトウェアについても同様であり、ハッカーは、法的な制限が設けられている商用ソフトウェアをできるだけ避け、自分たちが自由に複製、頒布、解析、改良ができるソフトウェアを作りだそうと努めている。こうして、彼らのネットワーク共同体に蓄積された、著作権に基づく排他的独占権がなんらかの形で放棄されているソフトウェア群が存在している。これらのソフトウェアに添附されている使用条件はさまざまであり、一概にまとめることはできないが、次のような種類に分類されている。

Public Domain Software (PDS) 著作者人格権の放棄が可能である法域で、著作権に基づくすべての権利行使を放棄したソフトウェア。また、すべての法域でその法域で定義される著作物の用件を満たさない程度に創作性を欠いている場合、また、その法域で認められた保護期間を満了したソフトウェアも含まれうると思われる[24]。アメリカ法では、1989年2月29日までに公表された著作物について、著作権表示を付加することでコピーライトを主張しない場合、その著作物は公的領域に含まれるもの

[21] Meyer & Underwood, supra note 5。

[22] 彼らの技術情報に対する態度を端的に示したのが、Apple社の製品であるコンピュータに内蔵された画面表示関係のマイクロチップを制御するために必要な非公開の技術情報を、NuPrometheus Leagueと名乗る集団がネットワーク上で公開したNuPrometheus事件である。Starling, supra note 6, at 328{329。

[23] 情報公開を市場での成功と結び付けた最初の試みが、1984年にIBM社が行った、PC/AT コンピュータの技術情報の公開である。この技術情報の公開によって、PC/AT互換機はパーソナル・コンピュータ市場のほとんどを占めることになった。逆に、IBM社がPC/ATの後継機種として送り出したPS/2は、技術情報が非公開だったため市場的に失敗したといわれている。また、Apple社も技術情報を公開しなかったために、広い市場を獲得することに失敗したといわれている。

[24] いずれの法域でも、著作物として保護を受けるための最小限の創作性の要件を置いている。この最小限の創作性を満たさないようなプログラム、例えば、誰が書いても同じコードでしか表現しえないようなものは、プログラムの目的とする機能と表現が融合しているために、著作権による保護を受けられない。また、法律による保護期間が終了しているプログラムが数十年後には表れはじめるはずだが、これらもまた、著作権による保護がないために、PDSと呼ばれうるだろう。なお、コンピュータ愛好者たちの間では、PDSとその他の自由なソフトウェアの違いについて必ずしも明確に認識されていない。このような広い意味での \PDS" については、大谷 和子 パブリックドメインソフトウェア, in コンピュータと法律, (犬伏 茂之 and others ed., bit別冊, 1992) に紹介がある。

と推定された[25]。最近まで、ネットワーク上で流通しているソフトウェアで、特に権利を主張しないものはすべてこの種類に分類されていた。

Free Software 著作者人格権の放棄ができないとされている法域、および著作者人格権の放棄が可能である法域で、ソース・コードを公開して、複製権、頒布権、使用権等の権利行使を放棄したソフトウェア。その他の権利については、著作権者がさまざまな権利を維持している。例えば、改変物の配布を禁止したり、頒布先に制限をおいたり、あるいは使用できる者の資格に制限をおいたりしているものもある。FSFが提唱しているcopyleftはこれに該当する[26]。

Freeware 著作者人格権の放棄ができないとされている法域、および著作者人格権の放棄が可能である法域で、ソース・コードの公開をせずに、複製権、頒布権、使用権等の権利行使を放棄したソフトウェア。その他の権利については、著作権者がさまざまな権利を維持している。例えば、改変物の配布を禁止したり、頒布先に制限をおいたり、あるいは使用できる者の資格に制限をおいたりしているものもある。

Shareware Freewareと同様の権利の主張を行うが、継続的に使用する場合には対価を支払うことを要求するもの。利用者の善意に頼るものから、対価を支払うと、機能がより優れた正式版を送付することによって対価支払いへの動機付けを行うことを狙ったものまである。

これらのソフトウェアによって、コンピュータ上での一般的な作業はすべてまかなわれており、ハッカーは、すべてのソフトウェアを上記のいずれかの種類のソフトウェアでまかなっていることが多い。この意味で、優秀なハッカーは自由なソフトウェアの利用と著作権法の制限の競合を回避している。ネットワークで流通しているソフトウェアの大部分はこのように、合法的に流通している自由ソフトウェアなのである。逆に、このような状況でなお、商用ソフトウェアの違法複製を行う利用者はハッカーたちによっても批判の対象となる。

ハッカーたちは、自ら作成したソフトウェアを自由に使用できるよう提供する代わりに、他者が作成したソフトウェアもまた自由なものとして公開してほしいと考えている。そこで、通常プログラムのソース・コードを公開しない商用プログラムに、対抗心を抱くことがある。例えば、ソース・コードを公開しないプログラムの作者が、自分の作成したソース・コードの一部を使うことは不当であると考えるし、また、ハードウェアのインターフェースを公開しない周辺機器製造者のハードウェアの制御に自分のソフトウェアが使用されるのを好まない場合がそうである。また、そのような閉鎖的な企業のハードウェアについて、それをより効果的に動作させることのできるソフトウェアを提供しないと宣言することによって、そのハードウェア会社がインターフェース情報を公開するように働きかけることもある。

このように、自らの信念を主張する手段として、自らのプログラムを使用するためには、完全に著作権を放棄するのでは不都合である。そこで、彼らは、彼らの考える情報の自由に従って行動する場合にのみソフトウェアの使用を自由とする、ある権利関係を設定した。それは、ネットワーク上で、コピーレフト(copyleft)として知られるGNU一般公有使用許諾(GNU General Public Licence: GPL)である。

---

[25] 1988年改正前のCopyright Act of 1976, 17 U.S.C. x101 et seq.のx401, x402では、著作権を主張するに当たって、著作権表示を行うことが要求されている。著作物がこの表示を欠いていた場合、善意の利用者は侵害行為について免責された(x405(b))。しかし、表示の欠落、あるいは誤記があった場合でも、権利者側が公表の前、あるいは後5年以内に登記を行い、その後頒布されるすべての複製物に著作権表示をする合理的な努力をした場合、著作権法の保護が与えられる。x405(a)-(2). したがって、一見PDSに見えるプログラムでも公表年から5年間は再び著作権が主張される可能性があった。一方、Berne Convention Implementation Act of 1988, Pub. L. 100-568(10/31/88)での改正によって、著作権表示が任意となり、1989年3月1日以降に公表された著作物については、著作権表示のない著作物にも著作権が存在する可能性が高くなった。この場合、利用者は善意かつ無過失でなければ侵害行為を免責されない。x401, x402. そこで、これに該当するプログラムについては明示的に著作権が放棄されない限りPDSとして扱うことは適切でない。

[26] FreewareとFree Softwareを区別しない場合が一般的であるが、FSFが両者を区別しているので分類してある。引地, supra note 12 『第2部　GNUソフトウェアの関連記事/インタビュー(2)「「copyleft」は賢いジョークの王様だ」』参照。

3.2.1　コピーレフト

コピーレフトは、ハッカーとして著名なストールマンによって提唱された「情報の自由」の一形態である。彼の主宰する Free Software Foundation (FSF) はすべてのプログラマが自由に使用、改善することができるソフトウェア群を提供するという GNU プロジェクトを推進している[27]。このプロジェクトによって作成された GNU プロダクツと呼ばれる一連のソフトウェアは、基本的でありながら、高度な内容のものであり、教育研究機関のみならず一般企業にまで広く利用されている。

ハッカーたちに人気の高い基本ソフトウェア (OS) である UNIX は、AT&T 社の研究機関であるベル研究所の 4 人の研究員によって 1969 年に開発された。それは、「スペース・トラベル」というゲームプログラムを、研究所ではあまり使用されていなかったコンピュータで動作させる過程の中で誕生したものだった。すなわち、UNIX は中心的な開発計画から外れた趣味的で周辺的なシステムとして誕生した[28]。UNIX は、非常に緩やかな使用許諾条件で配布された。AT&T 社は UNIX が商業的に成功するとは考えておらず、自由な利用と改善を通じて、よりよいコンピュータ環境が実現されれば良いと考えていたからである。このため、UNIX のライセンス料は非常に安く、また、1974 年からはソースコードも提供されていたので、教育・研究用 OS として広く普及した。また、UNIX は自由にソースコードを解析することができ、自由に改良を加えることができたために、さまざまな改良が非常な速度で進んだ[29]。この UNIX の普及と成功は、プログラミングにおける情報の自由の必要性の論拠を側面から助けている。

また、UNIX の発展における一支流であるバークレイ版 UNIX (BSD) は、現在のインターネットの基礎である ARPAnet の OS として改良された。このために、ネットワークを基本とした研究開発環境としての UNIX の地位が確立された[30]。したがって、自由な UNIX 文化とインターネットの自由さは一体不可分の関係として結びついていた[31]。インターネットが分散的で管理不能である構造を採用しているのは、それが核攻撃に耐えうる構造だったからという ARPAnet 時代の名残りというだけでなく、むしろ官僚主義や中央統制を嫌ったハッカー倫理の具体化のように思われる。

ところが 1983 年以降、AT&T は、広く普及したためプログラムの命令体系が混乱していた UNIX を商用 OS として整理統合し、使用者に AT&T 標準との互換性維持の厳格な義務を課し、これまでに比較すればかなり高額のライセンス料を請求するように方針を変えた[32]。そこで、UNIX を愛好する技術者たちの手によって、UNIX と同じ機能を提供するものの、AT&T が権利を保有するコードを含まない、自由な互換 UNIX が登場することとなっている。例えば、MINIX や FreeBSD や Linux と呼ばれる OS である。ストールマンも同様に AT&T の著作権からまったく独立に作成された、UNIX と同一の機能を提供する OS と、その OS 上で動作するソフトウェア群を作成する計画を 1984 年に開始した。これがプロジェクト GNU である。

このプロジェクト GNU を進めるに当たって、彼は、ソフトウェアをより自由な状態におくためには、単

[27] GNU に関する設立経緯や活動の概要について手軽な文献には、座談会 リチャード・ストールマン氏を囲んで, 19 bit 4 (1987) や引地, supra note 12 がある。また、GNU に関する資料は、日本では、ftp.iij.ad.jp/.0/GNU/GNUinfo/ 以下で入手できる。また、同資料の一次配布先は、prep.ai.mit.edu/pub/gnu/ 以下である。また、同様にプログラミングの自由を維持するために設立された団体として、The League for Programming Freedom (LPF) という団体も存在している。下條, supra note 18, at 24、および、prep.ai.mit.edu/pub/lpf/以下。

[28] Dennis M. Ritchie, UNIX の誕生, 15 bit 51, 51{54 (1983)

[29] 参照、希早, BSD のファイル・ワールド (5) UNIX の歴史, 2 UNIX Magazine 62, 62{63 (1987)、Doug McLloy, UNIX サクセス・ストーリー, 2 UNIX Magazine 17, 17{23 (1987)。なお、UNIX の開発と同時期 Multics というシステムが存在していた。これは、いわゆる中央集権的で官僚的なシステムとしてハッカーたちに忌み嫌われた。このため、ハッカーたちは Multics を停止させるためにあらゆる手段を講じた。UNIX と対照的なこの OS をみれば、彼らの感性に反するシステムがどのような末路を辿るかがうかがわれる。Levy, Hackers, supra note 2, at 143{146。

[30] 希早, supra note 29, at 64。

[31] バークレイ版 UNIX (BSD) の生い立ちと普及の様子については、Margulis, supra note 10, at 102{108。

[32] 1983 年まで、AT&T は独占禁止法の制限によって、電話事業における独占的な地位を認められる代わり、コンピュータ事業への参入が制限されていた。すなわち、AT&T は UNIX を公に商品として販売できないという立場にあった。これが、UNIX の法的位置づけが曖昧なまま大学にライセンスされた理由である。ところが 1982 年の AT&T に対する第 3 回反トラスト法訴訟の修正同意審決に従い、AT&T は 7 つの地域電話会社への解体と引き換えにコンピュータ事業へ参入することができることになった。このとき、UNIX が有望な収益事業の一つとして着目された。AT&T の解体については、舟田 正之 and 黒川 和美, 通信新時代の法と経済, 121{127 (1991)。

に著作権を放棄するだけでは不十分であり、むしろ作成者が著作権を主張し、ソフトウェアの使用条件として、「ソフトウェアの自由な使用を妨げる行為を禁ずる」という権利主張の方法を考案した。これがGNU一般公有使用許諾[33]である。

一部のコンピュータ利用者は、自分たちが使っているソフトウェアがこのような理念と配布条件のもと提供されていることを意識していないと思われるが、GNUプロダクツの浸透にともなって影響力を増すものと思われる。しかしながら、「ソフトウェアは自由であるべきである」とする一方、FSFの理念に疑問を表明するハッカーも存在する。その理由の一つとして、非常に高品質かつ高機能でありながら、無料あるいは非常に低廉なソフトウェアが提供されているために、ソフトウェアの多様性が損なわれていることを挙げている[34]。

4 プライバシー

本節では、電子ネットワークにおけるプライバシーの問題に関して検討する。プライバシーについて、ハッカーたちは、個人対個人の場合と、個人対政府の場合とで相反する態度をとることが多い。

個人対個人の場合、彼らは、開拓時代の西部のように、それぞれの個人が自らの情報力をもって他人を制するという状況を楽しんでいる[35]。この意味で彼らはやはり無法者としての自らを容認している。一方、個人対政府の場合、彼らの態度は一変する。彼らの観念では官僚的組織は対抗すべきものなのである。したがって、政府が彼らを取り締まるに当たって行う情報力の行使、すなわち、ネットワーク上での捜査については、合衆国憲法を盾に自らのプライバシー権の保護を主張する。これらの矛盾した態度は一個人それぞれについてみるならば、いずれかに統一されているのかもしれないが、ハッカーという集団で捉えたとき解決されていない。しかし、1990年に行われたハッカー一斉取締をめぐる諸事件をきっかけに一つの方向性がハッカーの側から提示されることになった[36]。

4.1 情報力の支配

クラッカーは、しばしば自らの技術力・情報力から得られる破壊的力を誇示する。いわく、「アメリカ中の電話交換機を停止することができる」あるいは「国防省の軍事機密情報を入手することができる」と。時として、これらの行為は現実に行われ、ハッカーに対する社会の恐怖を喚起する。また、一方で、彼らは、これらの違法行為を行うことの正当化理由として、「一般の人々が信頼して依拠しているコンピュータ・システムがいかに脆弱で不安定なものであるかを示すことによって、社会の注意を喚起している」という。摘発されたクラッカーたちが、社会復帰した場合、しばしばシステムの安全管理者として生計を立て

[33] Free Software Foundation, GNU General Public Licnese, Ver.2, 1991, 所在は ftp.iij.ad.jp /.0/GNU/GNUinfo/GPL。なお、引地, supra note 12 にも同文書の邦語訳が掲げられている。さらに、GNUプロダクツには必ず同文書が添附されている。また、現在流通しているフリーソフトウェアの中には、GNUと直接かかわりを持たないものの、このGPLに従う旨を宣言しているものもある。

[34] Margulis, supra note 10, at 105, 179, 223。

[35] クラッカーと個人情報提供サービス業者の活動によるプライバシー侵害について、ジャーナリストの視点から書かれた最近の報告として、Jeffrey Rothfeder, 狙われる個人情報, (大貫 昇 trans., 1993)。この報告のような、電子データベースを利用した個人情報の収集には、一般的な認識ではハッカーがかかわると考えられている。実際にそうした行為をする人物は、電子技術に堪能だろう。しかし、本来の意味での「ハッカー」の定義に従えば、ほとんどのハッカーたちは他人の個人情報について興味を示すことはあまりないと思われる。例えば、彼らは、ネットワーク上での知人が、実際にどのような人物であるかを知ることは少ない。Starling, supra note 6, at 141{142。 また、Dorothy E. Denning, Concerning Hackers Who Break into Computer Systems, (Washington, D.C., 1990, National Computer Security Conference) available online URL http://www.eff.org-/pub/Net_culture/Hackers/denning_hackers.speech でも、ハッカーは主としてコンピュータプログラムに興味を持つのであり、他人のプライバシーに興味を持つことが希であることが示されている。しかし、自らのネットワーク上における情報力と技能を示すために、例えば、有名人の秘密の個人情報を収集するようなことはあると思われる。

[36] このハッカー一斉取締を中心的に取り上げているのが、Starling, supra note 6。また、この一斉取締をきっかけとして提起されたネットワーク上の憲法問題についてネットワーク利用者の側から簡単にまとめられているのが、Mitchell Kapor 魔女狩りにあうハッカーたち, in コンピューターネットワーク, supra note 2, at 110。

ていることをみるとき[37]、先の正当化理由がまったく逃げ口上であるとは言えないように思われる[38]。実際、彼らはシステムの脆弱性をよく知っているし、彼らの目的は自らの技術的能力を他者に認めさせることにあるのであって、それを認めてくれる人々がシステムの管理者側であろうと、システムへの侵入者側であろうと、いずれでもかまわないからである[39]。

コンピュータを日頃から使用している人にとっては常識と思われるが、コンピュータは実に脆弱である。小さな個人用コンピュータから大型の汎用機に至るまで、わずかなトラブルによって致命的な破壊を招く危険を常に内包している。この脆弱性はシステムの機能についてのみならず、プライバシーについてもまったく同様に当てはまる[40]。コンピュータに記録されているすべての情報は、常に、なんらかの形で読み出しうる状態になっており、それはシステムの側から見て、記憶領域に格納された電磁気的記録である点では、国家機密も他愛ないおしゃべりの記録でも同様なのである。

さらに、近年進行しているネットワーク化によって複数のコンピュータが電気的に結合されるようになると、より脆弱な要素が増大する。ネットワークはコンピュータ相互の情報交換用に設置されるから、理論的には、ネットワークに接続されているすべてのコンピュータに侵入することができる。ネットワークの安全対策はソフトウェア的に達成されているものであり、ハードウェア的には無防備であると言っても過言ではない。したがって、ネットワークに接続された一台のコンピュータの脆弱性はネットワーク全体の脆弱性として拡大し、事故の起こる可能性は飛躍的に増大する。このことをプライバシーについて考えてみると、ハッカーたちには、コンピュータに収められたすべての情報が、あたかも幕が掛けられた掲示版に書き連ねてあるように見えるだろう。幕をめくればすべてがそこに記述してあるのであり、ただ、その幕をめくる方法を一般の人が知らないだけだということになる。

電子ネットワークによる情報通信は不可視であるがゆえ、電話のように通信内容の秘密が維持されていると思いがちであるが、実際には、電話でさえ盗聴されうることは周知の事実である。まして、コンピュータによる情報通信は、送り主と宛て先を付加されたパケットと呼ばれる情報単位に分割されて世界中に送り出されているのであり、そのパケットが通過するコンピュータの記憶領域には一時的にでも必ず格納される[41]。適切なプログラムを作成すれば、自分宛でないパケットを受信して、元の通信文を復元することも可能である。こうしてみると、コンピュータを用いて通信をするということは、葉書によって文書を送っているのに等しい[42]。

現在では、インターネットの商業利用について期待が大きいが、インターネットが分散的で開放的なシステムであるがゆえに、これまでになくプライバシー的に問題のあるシステムであることを再確認しなければならない。クラッカーたちが行使していた技術力、情報力とは結局のところ、システムの本質を理解し、発見された脆弱性を悪用していたに過ぎず、技術者の視点から見れば、むしろ幼稚なものである。その意味で、優秀なハッカーはクラッカーたちを軽蔑しているし、システムの破壊などというような単純な行為には興味を抱かない。

---

[37] アメリカの著名なクラッカー集団「破滅の軍団 (Legion of Doom: LoD)」は現在、クラッカーの侵入から顧客を守るためのコンサルタント業を営んでいる。コンピューターネットワーク 別冊日経サイエンス No. 105, 105 写真注記 (1992). また、\Control-C" と呼ばれるクラッカーは、訴追後ミシガン・ベル電話会社のセキュリティ担当に就職した。Starling, supra note 6, at 144。

[38] コンピュータ犯罪がコンピュータの安全対策上の欠陥を指摘してくれるとする考え方は、根強く主張されている。例えば、一松信, コンピュータ・セキュリティ (1), 17 bit 14, 15 (1985) や Steven Levy, ハッカーは愛すべき存在, 1995 Newsweek 日本版等。しかしながら、コンピュータ・システム自体が非常に複雑になっているので、単にシステムへの侵入行為によって欠陥を指摘するだけでは、問題の解決につながらなくなっており、そういう意味で、もはや侵入行為は正当化されないとする考え方もある。Eugene H. Spaãord, 特集ワーム・ストーリー (1) インターネット・ワーム事件の全容 | 危機とその余波, 21 bit 4, 16 (1989).

[39] 参照、Denning, Hackers, supra note 35。

[40] コンピュータ運営に当たってのハードウェア、ソフトウェア両面の脆弱性については、August Bequai, 情報犯罪, (堀部 政男 and 堀田 牧太郎 trans., 1986)。本書を参照すると、コンピュータ犯罪を行うに当たって、特殊な知識や技能が必要とされないことがわかる。「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」Id. at 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当てはまるし、それらの犯罪のほとんどは、ハッカーが仲間に誇れるほど特殊な技術を必要とするものではない。

[41] 参照、Martin E. Hellman 新しい暗号体系, in コンピューターネットワーク, supra note 2, at 126。

[42] インターネットが開放的なシステムであることを理由に、そもそも、インターネット上でプライバシーは存在しないとするような考え方も存在する。

法律や教育によって「できることではあるが、してはいけないこと」を知らしめることは重要な作業ではあるが、数知れず参入してくるだろう一人一人の利用者が、出気心を抱かないように期待することは困難だろう。そこで、ネットワークのプライバシーでは、最も現実的な解決法として技術的な解決、すなわち「暗号化」が議論の中心となる。誰でも覗ける掲示版に書かれていても、秘密の記号列ならば、宛て先の人物しか読むことができない。このことは、あたかも封書で文章を送ることに例えられるだろう[43]。

しかし、誰もが自由に暗号化技術を使うことを認めるべきかについては、個人対政府という局面で別の問題を生ずる。

4.2 ハッカー 対 政府

1989年から90年にかけて行われたハッカー一斉取締によって、いくつかの個人用コンピュータが押収された。そのうちのいくつかはネットワークの電子会議室システム(BBS)として使用されており、その中には利用者の私信や個人的なファイルが多数格納されていた。それらのファイルはBBS機材に格納されたまま、捜査官によって没収され、シークレットサービスの捜査官によって読まれることになった[44]。

このハッカー一斉取締によって押収されたBBSのうちには、捜査官の誤解によって押収されたものもあった。そのうちの一つ、スティーブ・ジャクスン・ゲームズ会社(Steve Jackson Games Inc.: SJG社)は、EFFの支援のもと、同社のBBSの中の電子メールや電子会議室記録をBBS機器ごと押収する行為が、電気通信プライバシー法(Electronic Communications Privacy Act, 18 U.S.C. x2510 et seq.: ECPA)にで禁止された通信の傍受(interception)を構成すること[45]、および、同社の出版物の原稿を押収する行為が、プライバシー保護法(Privacy Protection Act, 42 U.S.C. x2000aa et seq.: PPA)で禁止された公表前の文書(documentary materials)および職務活動の成果物(work product materials)の押収に該当すること[46]、を主張し、BBS機器の返還と損害賠償を求めて提訴した[47]。判決の中で裁判所は、PPAに関する部分について、シークレット・サービスが十分な事前調査を怠ったことで、プライバシー侵害がなされたことを認めた。すなわち、コンピュータに格納されている電子的記録が合衆国憲法修正第4条の保護を受けることが確認された[48]。一方、ECPAに関する部分について、コンピュータに格納された電子メールはECPAに規定されいてる意味での通信に該当しないと判断し、捜査員が通信の傍受を行ったとする原告の主張を退けた[49]。SJG社やEFFは、電子メールが通信であると認められなかったことを不服として上訴している[50]。

この判決は、電子ネットワークでの捜査で、取締側がプライバシーについて十分な配慮をしなければな

---

[43] ハッカーの中には、ネットワーク上のプライバシーに関して、プライバシーを維持したいと望む側に責任があるとする考え方をとる論者がいる。すなわち、プライバシーの侵害が生じた場合、十分な安全対策を行わない利用者の側に落ち度があると考える。

しかしながら、後述するスティーブ・ジャクスン・ゲームズ会社事件で、コンピュータに蓄積された電子メールにプライバシーが認められたことから合衆国憲法修正4条に規定された「合理的なプライバシーの期待」が電子ネットワークで存在することが、裁判所によって確認されたことになる。

[44] このハッカー一斉取締作戦 \Operation Sundevil" について全体像を把握するのに適したものとして、Starling, supra note 6, at 160{246。SJG事件に関する資料の所在は、ftp.eff.org/pub/EFF/Policy/SJG/以下。また、Sundevil作戦については、デニングによる報告の邦語訳がDorothy E. Denning, クレイグ・ニードルフ事件（前編）, 24 bit 12 (1992) で紹介されている。また、このデニングによる報告に対する7人の識者のコメントがDorothy E. Denning and others, クレイグ・ニードルフ事件（後編）, 24 bit 46 (1992) に掲載されている。ハッカーに対する関係者の認識の多様性を理解するのに好適な資料である。さらに、SJG事件についてはEdward A. Cavazos and Gavino Morin, Cyberspace and the Law: Your Rights and Duties in the On-line World, 22{25 (1994) にも紹介がある。

[45] 18 U.S.C. x2511

[46] 保護の対象となる文書の定義については、42 U.S.C. x2000aa-7。また禁止条文については、42 U.S.C. x2000aa。

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

[48] コンピュータに格納されている電子的記録に対する犯罪捜査におけるプライバシーについての検討は、安冨, supra note 5, at 14{64 で行われている。SJG社事件判決でBBSにおけるプライバシーが認められたということは、逆に裁判所がBBSという情報伝達手段において、プライバシーの合理的期待があると判断したことを意味する。したがって、前註のハッカーの主張は認められないことになる。

[49] 電子メールがコンピュータに記録されていることから、裁判所は、BBSが「電気通信記録および処理記録アクセス法(Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. x2701 et seq.)」のx2711に定義されている \remote computing service" に該当するとした。そしてBBSに捜査官がなしうる捜査は記録の開示のみであり、BBSの押収は同法x2703に違反するとした。

[50] BBSシステムへの捜査が通信設備に対する捜査であると認められた方が、通信記録への捜査であると考えられるよりも捜査令状の発給で、より慎重な態度が求められるからである。

らないことを示した点で、画期的なものであり、合衆国憲法が電子情報のプライバシーを保護していることを改めて認識させる事件だった。しかし、裁判所の令状に基づけばBBSへの捜査が可能であること、またそれが実際に行われていることも、ネットワーク利用者の間に強く印象づけられた。

そうしたなかで、個人の私信についても暗号化しようという動きが強くなるのも当然である。この私的暗号化の提唱は違法行為を司法権力の目から逃れさせようとするクラッカーの身勝手な主張というだけでなく、前節のネットワーク上のプライバシーの問題とも結合することになった。こうして、暗号化技術に長けた人物によって作成された、数種類の暗号化プログラムがネットワーク上で提供されることになった。こうした暗号化プログラムは、送信者と受信者しか、この暗号を復号化する方法を知りえないものだった。この意味では、ネットワーク上のプライバシーは完全であり、暗号化して送信している限り、第三者から送信内容を読まれる危険性は消失した[51]。

ところが、これらの私的暗号化について、治安および防衛上の観点から問題点が指摘されることになった。例えば、麻薬取引の連絡にこの暗号が使用された場合、捜査当局によっても通信文の解読が不可能であるため、ネットワークの普及は常習犯罪者たちにとって好都合となる。このように、暗号化技術はネットワークを真の無法地帯とする危険性をはらんでいる[52]。また、暗号化技術は国防上の観点から、国外持出禁止となっているのだが、一旦ネットワークで提供された暗号化プログラムが、国外に持ち出されるのを差し止める方法はない[53]。

こうした動きのなか、プライバシーとネットワークの治安という両方の問題を解決する案として、FBIは「デジタル電話通信に係るプライバシー促進法案(Digital Telephony and Communications Privacy Improvement Act)」を準備した。これは、送信者、受信者および司法権力の三者が通信内容を解読できる方式の暗号化技術のみを合法とするものである。同法案では、この暗号化方式を実行する"Capstone Chip"および"Clipper Chip"と呼ばれる暗号化回路を通信機器に装備することを義務づけ、これによって、ネットワーク上のプライバシーを維持したまま、ネットワークが無法地帯となることを回避しようとした[54]。

この案については、ハッカーおよび法学者の側から轟々たる非難が沸き起こった[55]。一部のハッカーは

---

[51]公開鍵暗号化方式については、Hellman, supra note 41。また、公開鍵暗号化方式をめぐる知的財産権等の問題については、Cavazos & Morin, supra note 44, at 28{31 に触れられている。

[52]ハッカー容認的な態度で知られていたデニングは、ネットワークにおける治安、すなわち司法力の執行可能性という観点から、第三者が通信内容を調査することができる、Escrowed Encryption Standard (EES) を確立しようとした政府の提案に賛同している。Dorothy E. Denning, Encryption and Law Enforcement, 1994 available online URL ftp://ftp.eff.org/pub/EFF-/Policy/Digital_Telephony/denning_wiretap.paper。しかし、EFFはデニングの提案に批判的である。EFFとデニングのネットワーク上における論争についての資料は、ftp.eff.org/pub/EFF/Policy/Digital_Telephony/以下。

[53]暗号化技術の輸出を禁止する根拠条文は武器輸出規制法(Arms Export Control, 22 U.S.C. x2751 et seq.)であり、直接的には同法x2778, Control of arms export and inports で、U.S. Arms Control and Disarmament Agencyの許可を得ない武器の輸出入を禁じている。同条(f)で、輸出入が制限されるdefence article and defence service に該当する軍需品一覧が、官報(Federal Register)に掲載されるとしている。官報で(Amendments to the International Traé c in Arms Regulations, 58 Fed. Reg. (1993) available online URL ftp://ftp.cygnus.com/pub/export/itar.in.full)暗号化技術は、"Category XIII-Auxiliary Military Equipment"に分類されている。"Information Security Systems and equipment, cryptographic devices, software, and components speciåcally designed or modiåed ...."

公開鍵方式暗号化技術を用いており、EFFが推奨しているプログラムが、Pretty Good Privacy (PGP)と呼ばれるものである。このプログラムは、世界中にある自由利用可能な公開書庫(anonymous FTP site)に事実上存在する。しかし、EFFはこのPGPが合法的に輸出可能であることが法的に確認されるまで、アメリカ国外の利用者がこれを転送して入手しないように呼びかけている。例えば、www.eã.org等。National Security Agencyによる、PGPの輸出禁止措置への反対者たちは、合衆国憲法修正第1条を根拠に「暗号化の自由」を主張している。なぜPGPの国外への輸出に合衆国憲法が関係するかといえば、暗号化プログラムは送信、受信の双方で使用しなければならず、国外へのPGPの輸出禁止のため、国外のネットワーク利用者との間の情報交換で、アメリカ人利用者もPGPが使えないことになるからである。

PGPは日本からでも入手可能ではあるが、仮に、日本の利用者が、PGPをEFFの警告に反して転送してくると、EFFは合衆国政府から訴追される危険がある。

[54]同法案の正式名称は、"To ensure continued law enforcement electronic surveillance access to the content of wire and electronic communications and call setup information when authorized by law, to improve communications privacy protection, ad for other purposes"である。法案の原文はJaleen Nelson, Sledge Hammers and Scalpels: The FBI Digital Wiretap Bill and Its Eãect on Free Flow of Information and Privacy, 41 UCLA L. Rev. 1139 (1994) の付録に収められている。また、ftp.eff.org/pub/EFF/Policy/Digital_Telephony/digtel94.billでも入手できる。

この法案の原文を見ると、103回議会に提出される法案として準備されたようだが、米国議会図書館のデータ・ベースで検索した結果、実際に提出された形跡は見つけられなかった。現在は104回議会が開かれているが、ここでも提出されていないようである。

[55]法学者の側からのこの立法に対する批判として、Id。ネルソンはFBI提案に対して、国際合意および合衆国憲法を基に批判している。第一に、同法案は合衆国内部を通過するすべての通信に適用されるので、国際電気通信協約(Internatianl Telecommunication

再び強力な暗号化プログラムをネットワークで提供するようになった。こうした私的暗号化技術を利用する運動、および賛同者たちは「サイファーパンク (Cypherpunk)」と呼ばれるようになった。ハッカーたちの本能的な政府嫌いという基本的態度が発揮されたわけである。このように、何種類かの暗号化プログラムが出まわってしまっている以上、政府が狙ったような犯罪抑止効果はすでに失われているように思われる。個人が政府と同等の情報力を獲得した場合に、個人と政府との力関係が変動することを実証した事例であると同時に、ネットワークの将来に大きな懸念材料を提供することになった。

5　まとめ

本論文では、常習犯罪者として一般に認識されているハッカーについて、その変遷を示すことで彼らの思考・行動様式について示した。そしてこれらを端的に整理したものとして「ハッカー倫理」を紹介した。このハッカー倫理はすでに廃れたとされているが、現在ネットワークの中でなされている「情報の自由」と「プライバシー」に関する市民活動や議論に強い影響を与えていることを示した。

情報の自由については、ネットワークが情報をより早く幅広く流通させることができる能力を持つという点で、情報公開にとって有利な環境である一方、知的財産権に脅威を与えていることが示された。しかしながら、ネットワーク環境の中で、ネットワークの性質に調和した、新しい知的財産権の形態が模索されていることも示された。

次に、ネットワークのもつ情報伝達能力の故に、コンピュータに格納されている情報について、プライバシーが否定されかねない状況にあることが示された。しかしながら、裁判でネットワークでも「合理的なプライバシーの期待」が存在すると認められたため、ネットワークにおけるプライバシーについて具体的に検討する必要が生じている。また、この問題を技術的に解決するために、暗号化技術が改善されたが、法の執行能力を維持したいと考える政府と暗号の利用者の間に摩擦が生じていることが示された。

これらの検討を終えて二つの提言をしておきたい。

第一は、ネットワークにおける一般規範の研究である。ネットワークが一部の研究者・愛好家のためのものではなく、一般社会の人々も参入するものとなってきている。こうしたなかでは古参者と新入者の間での軋轢が生じているという例を数多く目にする。かつては参入者の数が限定されていたので、古参者たちが新入者を個人的に指導するなかで秩序が維持されてきた。しかしながら、現在ではそのような指導が有効ではなくなってきている。そこで、なんらかの秩序維持に当たる主体が必要とされるかもしれない。しかしながら、ネットワークが国家の枠を越えて広がり、また、ハッカーたちが権力の介入を嫌い、さらに、ネットワーク技術自体が全体的な管理を不能とするような仕組みを採用しているために、国家が統制することは不可能だろうと思われる。こうしたとき、これまで自発的に維持されてきた秩序を維持し、発展させるために、法学者はネットワーク文化を正しく理解し、整理し、提示することでネットワークにおける一般規範の形成に寄与する必要があるだろう。ネットワーク文化と現実社会の法規範との冷静なすり合わせが求められるのであって、秩序維持の問題はハッカーやクラッカーを駆逐すればすむという単純な問題ではない。

第二は、ネットワークで生じつつある新しい価値の維持・発展である。本論で示したように、ネットワーク文化の一部は、人類普遍の自由や権利に基づいており肯定されるべきものである。また、これらの価値を具体化するための活動も活発に行われている。確かにこれらの活動は既存の法規範との摩擦を生じさせているかもしれないが、このことをもって直ちにそれが否定されるべきではない。我々が現在享受してい

Convention) 18条 22(1)条、世界人権宣言 (Universal Declaration of Human Rights) 12条 19条、市民的政治的権利に関する国際規約 (International Covenant on Civil and Political Rights) 17条 19(2)条等、数多くの国際合意に違反するとする。第二に、同法案は情報通信に利用することのできる媒体を広範囲に制限するので、合衆国憲法修正第1条で保障されている言論の自由を制限する場合に必要な標準的要件に合致していないことを批判し、それが言論の自由を脅かすものであることを批判する。第三に、同法案で政府が通信を傍受を正当化する理由として掲げられている「国家の安全保障」と「法の執行」の定義が曖昧であり、また、同法案の適用対象があまりに広範囲に渉るため、合衆国憲法修正第4条で禁止されている不当な捜査と押収に該当すると結論している。

る自由や権利は、長い過去の法規範との衝突の末に獲得されてきたものである。例えば、200年ほど前までは、世界のどの国家でも自分の考えを世に問うことは危険を伴う行為だった。ネットワークにおける新しい価値について検討する我々に求められているのは、近視眼的な違法合法の判断ではなく、いずれの価値が我々の幸福に寄与するのかを問う大局的な視点だろう。