ハックティヴィズムとクラックティヴィズムの概念的差異に関する考察
:アノニマスを事例に

A study on difference of a notion between hacktivism and cracktivism

塚越　健司（Kenji TSUKAGOSHI）

一橋大学大学院社会学研究科　博士後期課程[i]

［Abstract］
The object of this article is Hacktivism that is a coined word.It is conbined hack and activism. Hacktivism is a kind of political movement, utilizing information technology as a tool. Recently, there are some words such as cyberterrorism, cyberactivism that is similar to hacktivism. To define moreprecise the notion of hacktivism,, I compared it with these words, then also compared with ‘policy circumvention’ . By referring to the argument of other studies, this paper demonstrates that hacktivism　differs from cracktivism, and hacktivism is classified into political crackting, political coding, and performative hacktivism.

［キーワード］
ハックティヴィズム、クラックティヴィズム、アノニマス、アクティヴィズム、市民的不服従

1. はじめに

近年、情報技術の利用によってその政治的目的を達成せんとする「ハックティヴィズム」の動きが盛んである。ハックティヴィズムとは英語の hack と activism を掛けあわせた造語であり、hack は hacker の語源でもある。情報技術の発達が十分ではなかった 90 年代における情報技術は、メールやインターネット掲示板の利用といった、従来のアクティヴィズム（積極的行動主義）の補助的な役割を担うツールに過ぎなかった。

しかし情報技術の発達とインターネットユーザーの爆発的増加を伴う 2000 年代に突入すると、ハックティヴィズム運動もその激しさを増し、政府や企業に対する分散型サービス拒否攻撃(Distributed Denial of Service attack）、いわゆる DDoS 攻撃の規模や頻度は現在に至るまで拡大傾向にある。従って 2000 年代以降の社会は、情報技術を単にアクティヴィズムの補足ツールと位置づけるだけでは不適切な時代に突入したことになる。サミュエル（Samuel）はハックティヴィズムの定義を「政治的目的遂行における、違法な、もしくは法律的に曖昧なデジタルツールの非暴力的使用」とする[Samuel, 2006, p. 2.]。

これまでの先行研究においては、ハックティヴィストによるウェブサイトの改ざんや DDoS 攻撃を市民的不服従(civil disobedience)と捉えられることもあった[Denning, 2001, p. 263.]しかしその一方で、ハックティヴィストの抗議行為は年々その規模を加速化させる傾向にあり、既存の定義ではその多様なハックティヴィズムを捉えることが困難となっている。ハックティヴィズムは合法活動と違法活動の両方が内包された概念であったが、サミュエルはより違法性の強いものをクラックティヴィズムとし、ハックティヴィズムに対置させた。しかし、具体的なハックティヴィズムの事例としてアノニマスの活動を参照すると、組織の内部構造と大義の問題が提起され、ハックティヴィズムとクラックティヴィズムのどちらにも重なる曖昧な部分が指摘できる。

本稿の目的は、語の整理とより精確な位置づけによって、ハックティヴィズムの持つ魅力とその危険性に関する判断基準をより厳密化することであり、以上の考察と行う。その上で、今後の研究に必要な要素を書き加えたい。

2.ハックティヴィズムとは

2.1 hack＋activism=hacktivism

ハッカーの起源は 1950 年代後半、マサチューセッツ工科大学（MIT）の鉄道模型クラブのメンバーの中から生じた。鉄道模型を動かす配線の改良から「単に建設的な目標を達成するだけではなく、それにかかわること自体がスリリングな喜びであるような作品や計画は「ハック」と呼ばれた」[レビー, 1987, p. 11]。コンピュータを改良し、そこに快楽を感じ、それを追求する人々こそがハッカーであり、彼らの実践がハックである。しかし、ハックおよびハッカーという言葉は後に、コンピュータ・システムに無断で侵入し、故意にプログラムの改ざん等を行う犯罪者、といったイメージが世間に浸透してしまう。そこでハッカー達は自らそうした犯罪者をクラッカーと呼び、ハッカーとの差別化を目指した（注 1）。

他方、アクティヴィズムは積極的行動主義ないし政治的行動主義と呼ばれ、政治的目的を達成するための運動の総称として用いられる概念であり、その行動は政治制度や法の変更を強く訴えるために存在する。運動手段としては、選挙投票や言論活動の他に、デモや、ボイコット等、数多くの手段が存在する。あえて違法行為を行うが決して敵対勢力に物理的暴力を振るうことを禁じたガンディーの非暴力主義は、市民的不服従の一例である。このように、平和的であっても法に反する行為が存在することもまた、アクティヴィズムの特徴の一つである。

ハックティヴィズムは、このハックとアクティヴィズムを掛けあわせた言葉であり、ハックの力を政治的に利用する思想あるいは実際の活動そのものを指す。しかし他方、情報技術に関する言葉を既存の用語に組み合わせた造語は近年益々増加傾向にあり、ハックティヴィズムもそのひとつである現状を鑑みれば、それらハックティヴィズムに類似した言葉とハックティヴィズムの比較をする必要がある。そのうえでハックティヴィズムの個別論点を論じなければ、問題の所存が不明確になることが危惧されるからだ。そこで、次節では主にサイバーテロリズム、サイバーアクティヴィズムとハックティヴィズムの比較を行う。

2.2 サイバーテロリズムとサイバーアクティヴィズム

デニングはアクティヴィズム、ハックティヴィズムとサイバーテロリズムを区別した。それによれば、サイバーテロリズムとは、「政治的な動機からハッキングを用いることで深刻なダメージを与えるもの」である[Denning, 2001, p. 241]。深刻なダメージとは曖昧な言葉であるが、デニングは人の生命に危害を与えるかどうかを深刻性の基準とする。デニングは例として、飛行機の管制システムへの介入による飛行機の意図的な衝突事故を挙げている。人命を考慮することのない身体的被害を行う政治的行為は、テロの名に値する。さらにデニングはもうひとつ、国家や行政機関、あるいは社会的影響力の高いシステム、インフラ等への攻撃もまたサイバーテロリズムと呼ぶ。例としては、水道システムや交通システムにサイバー攻撃を仕掛けることでこれらのインフラを使用不可能にする行為である。生活インフラに対する攻撃は社会的、経済的に相当な規模の支障をきたし、病院など、場合によっては生命を危険に晒すことも考えられる。

デニングの主張する深刻性とは、主として人の死に関わるものを指し示し、その他生活インフラや国家の威信に関わるものである。本稿では他の概念との区別を明確にするために、サイバーテロリズムの定義を、「情報技術の利用の結果、他者の生命に危害を加えることも厭わない政治運動」とする。

次にサイバーアクティヴィズムであるが、これは時に「インターネットアクティヴィズム」あるいは単に「アクティヴィズム」とも呼ばれるが、その間に特質すべき概念的差異はない。故に、デニングがアクティヴィズムとして定義しているものを本稿ではサイバーアクティヴィズムの定義とする。デニングの定義は、「インターネットをシンプルに利用する」である[Denning, 2001, p. 241]。具体的には、インターネットを用いた情報収集、ウェブサイトの立ち上げ、電子メールでのやり取りやメーリングリスト、ネット上での活発な議論やデモのお知らせ等であり、実際にインターネットが本格的に浸透してきた 90 年代後半から 2000 年代前半にかけては、インターネットを利用したアクティヴィズム運動の事例がいくつも報告されている[井口他, 2001][ウィン, 2009]。それら 2000 年代前半におけるサイバーアクティヴィズムに関する事例の大半は、情報技術を用いることで、より多くの人々を

デモや集会に動員することに重きが置かれていた。

したがってサイバーアクティヴィズムにとって情報技術とは、従来のアクティヴィズムの活動を一層円滑にするためのツールとして用いられていることがわかる。Web2.0 時代を迎えた現在においても、サイバーアクティヴィズムは政治的目的達成のためのツールとしての SNS 利用や、情報伝達のスピードの向上、情報の相互発信性等、政治目的達成の手段としてデニングが定義した通りの活動を継続している。実際に 2011 年に生じた一連の「中東革命」では、SNS を利用した情報伝達が有効に機能した。

ただしサイバーアクティヴィズムの主たる実践は、デモや法廷闘争といった従来の政治運動となんら変わらない。近年の情報技術の結晶たるインターネットは、あくまで政治運動に便利なツールとして位置づけられるに留まる。例えば、1999 年に行われた大規模な反グローバリゼーション運動「シアトルの乱（バトル オブシアトル）」においては、世界中の人々がネット上で議論を交わし、シアトルで開催された世界貿易機関（WTO）会議への大規模な反対デモが行われた。このデモはインターネットなしには実現不可能な運動であったが、これをサイバーアクティヴィズムの側面からみれば、ネットはリアルの現場に人々を動員するための補助的ツールであったといえる。それはインターネット、あるいは広く情報技術単体によって政治活動を実践するものではない。この点が次のハックティヴィズムとの概念的差異に連なる。

後述するように、ハックティヴィズム活動の実践は、リアルの現場に人を集めること以上に、ネットの中だけで、すなわち情報技術によってのみ抗議活動を行うものが中心である。もちろん、サイバーアクティヴィズムの名を冠した活動にも DDoS 攻撃が目撃されることがあり、他方ハックティヴィズムと呼ばれる活動においても、デモや集会が行われることもしばしばある。ただし本稿ではそうした活動を考慮しない。というのも、類似した語の分類に際しては、両者の類似性ではなく差異、つまり両者の活動の主たる実践こそに着目し、その主たる実践を軸にした分類作業こそが必要とされるからである。そこで本稿では、サイバーアクティヴィズムの定義を、「情報技術を人々のコミュニケーションツールとして用いることで、リアルの場に動員する政治運動」と定義しよう。

2.3 ハックティヴィズムの定義

では、ハックティヴィズムは上記の二つと何が異なるのだろうか。デニングはハックティヴィズムを、「サイバーテロリズム同様にハッキング技術を政治に応用するものだが、深刻なダメージを与えるものではない」と定義する[Denning, 2001, p. 241]。例としては、ウェブ上での座り込み（シットイン）、コンピュータウイルスの拡散、ウェブサイトへのハッキングによる一時的な閉鎖等であり、近年では DDoS 攻撃などがメディアでも注目を浴びている。ハックティヴィズム活動は主にウェブ上において実行するものであり、サイバーアクティヴィズムのようにその身体をリアルの場に集合させる必要はない。人々が集合するのはウェブ上であり、そこでは個人の身体は情報に還元される。抗議行為としての DDoS 攻撃は、まさにウェブ上の身体である情報を膨張させ、抵抗対象に突入する行為だと言えるだろう。

したがって、身体を現実の場に集合させるか否かが、サイバーアクティヴィズムとハックティヴィズムの間にあるひとつの差異だと言える。そしてもちろん、情報は生身の身体ではないが故に、リアルの場で誰かが死ぬことはない。従って、情報技術によって人の生命を奪うサイバーテロリズムとハックティヴィズムの差異もここにみられる。時にメディア報道などにおいて、ハックティヴィズム活動の根本を誤解し、ハックティヴィズムをサイバーアクティヴィズムやサイバーテロリズムの概念を用いて論じることが多々みられるが、これらの概念と区別してハックティヴィズムを捉える必要があるだろう。

2.4 Policy circumvention

ハックティヴィズム活動の特徴として、「policy circumvention」と呼ばれる方法が挙げられる（注 2）。policy circumvention を訳すとすれば、「政策回避」あるいは「法の目をかいくぐる」と呼べるものであり、特定の政策を技術によって実質的に無効にするものである。

サミュエルは policy circumvention をより詳細に定義している。それによれば
①まず policy circumvention は既存の政策、法、規制、裁判決定に反対し、なぜそれらが不当であるかを明確にする。さらに反対するだけでなく、政策変更案などを訴える。
②次に、policy circumvention は決定された政策や法、規制、裁判決定を無効化することに重きを置き、問題のより根本的な部分を議論の遡上にあげる。その際、声をあげて反対する代わりに、政策の無能さを示すことで抗議行為に代える。後述する Winny による著作権侵害行為は法律においては違法であったが、実際に Winny が流布されることで、しばしば法はその実質的な効力を失った。それが危険な行為であったとしても、ハックティヴィストの攻撃は止まらない。policy circumvention とは、そのような法制度に対する危険を孕んだ概念である。
③最後に、policy circumvention は特定の個人や組織にだけ作用する利益を供給することはない。policy circumvention の結果得られるものは、非排他的な利益である。policy circumvention と違法行為の差異は、行為の結果が個人の参加によってもたらされる利益をはるかに超え出ることにある。ウィキリークスによるリークは社会悪を世界中に公表することにより情報の透明化や不正の撲滅の一歩を踏み出した。しかし、主義主張に基づくことのない単独犯の犯行の場合であれば、リーク情報が企業恐喝に利用され得る場合すらあろう。policy circumvention は個人にとって利益をもたらすだけでなく、人々に問題点を喚起させ、政策や法を廃止させ、あるいは変化させることを可能にする。
さらに policy circumvention は、個別の政策・法に反対するという意味では従来の市民的不服従行為等との関連性も指摘できる。寺島は市民的不服従を「自らの行為の正当性の確信のもとに行われる非合法行為」と定義する[寺島, 2004, p. 15.]。これは国家が定めた法や政策に対し、自分の良心に照らして我慢しがたいと感じる市民が、国家に対して抵抗する際の手段である。確信的な違法行為、あるいはそれに準ずる行為という意味で両者に類似性が認められる。しかし policy circumvention においては、市民的不服従行為が身体的暴力や逮捕の危険性があるのに対し、それらのコストが驚くほど少ない。また、匿名性を保ったまま活動に参加可能な policy circumvention は、情報技術が有する身体性に対する優位性を獲得し、さらに活動への参加が容易なために、しばしばネット上での大規模な動員を可能にする。
では実際にいくつかの policy circumvention 事例をみてみよう。

2.5 DeCSS

DeCSS とは、DVD-Video のアクセスコントロール技術（Content Scramble System）を解除するプログラムである。1999 年当時、Linux 等のオープンソース OS ではアクセスコントロールにより商用 DVD を観賞することが不可能だった。そこでノルウェーの当時 15 歳であったヨン・レック・ヨハンセンは、アクセスコントロールの解除に成功すると、そのプログラムを DeCSS という名で公開した。ヨハンセンは純粋に Linux 上での DVD 観賞のためだけに開発したのだが、情報の暗号解除を伴うため、その公開は単に DVD を観賞することを可能にするだけでなく、DVD の複製を可能にした。そのため、2000 年にヨハンセンは著作権侵害を理由に米映画協会（MPAA）に訴えられた。ただし、一審では有罪判決を受けたものの、2004 年に彼は無罪が確定している。
DeCSS は、ヨハンセンが政治的意図をもって実行したことではないが、DVD のコピー技術は多くのユーザーたちが利用することになった。また DeCSS の配布が一時的に有罪に問われた際には、数多くのユーザーが DeCSS のコードを T シャツに書いて販売するなど、多種多様な手段で裁判判決に対する反対活動をするだけでなく、コード公開の禁止が言論の自由に抵触するとの批判も寄せられた。ヨハンセンの無罪が確定した最終的な裁判では、合法的に入手した DVD を、製作者の想定を超えた使用方法（Linux 上で作動させること）は合法との判断を下すと同時に、如何に DVD コピーが行われたとしても、その技術を開発した者が製作によって罪に問われることはないとの判断も下された。
当時のヨハンセンは自覚的に法への反対意識をもって DeCSS を公開したのではない。しかし、彼の行為は多くのユーザーを巻き込み、法を実質的に変更させたのである。

2.6 Winny

日本において Policy circumvention に関連した事例としては、P2P 技術を利用し開発され、2002 年か

ら公開が開始されたファイル共有ソフト Winny がある。開発者の金子勇は 2004 年に逮捕されたが、2011 年に最高裁において無罪が確定している。判決理由は DeCSS と類似しており、違法行為が想定可能なものであっても、技術的な開発のみによって罪に問われることはないということである。

Winny は著作権を有するコンテンツを実質的に無料ダウンロードを可能にするなど、多くの問題が指摘されているが、事件の詳細は本稿では割愛する。本稿において重要なことは、金子が 2 ちゃんねるにおいて以下のような書き込みをしたことにある。

「個人的な意見ですけど、P2P 技術が出てきたことで著作権などの従来の概念が既に崩れはじめている時代に突入しているのだと思います。お上の圧力で規制するというのも一つの手ですが、技術的に可能であればだれかがこの壁に穴あけてしまって後ろに戻れなくなるはず。最終的には崩れるだけで、将来的には今とは別の著作権の概念が必要になると思います」[佐々木, 2006, pp. 85-86.]。さらに金子は、著作権制度が崩れた後の具体的な制度も考えていた(注 3)。

Winny 事件は、金子が意図的に著作権制度の崩壊を意図した部分があることからもわかるとおり、ハックティヴィズムの要素が多々みられる。金子の望む新たな著作権が現れることはなかったが、最終的に金子は Winny 製作については法的に無罪とされた。

本稿では続けて、現在もその活動を継続中のハックティヴィスト団体、アノニマスの戦略について考察しよう。

3. ハックティヴィスト集団「アノニマス」

3.1 アノニマスとは

ハックティヴィスト団体「アノニマス」は、「ネットの自由」を標榜し、政府や企業等に主にネット上で抗議を繰り返す団体である。彼らの起源は 4chan という巨大画像掲示板であるが、そこに集うネットユーザーの一部が、「情報の自由」という大義が掲げ、これを侵害する者たちに抵抗するための運動が生じた。彼らは Internet relay chat(IRC)システムを利用し、抗議活動（彼らはオペレーションと呼ぶ）ごとにその戦略をチャットを介して議論する。2006 年頃からすでにアノニマスとして緩やかな団体性を獲得していた彼らは、2008 年にアメリカの宗教団体「サイエントロジー」に抗議行動を開始したことで世界から注目を浴び始めた。当時の活動の大半は平和的なデモ活動であったが、2008 年 2 月 10 日に行われたデモでは、世界 93 都市で 7000 人が参加したとアノニマスは主張する。

アノニマスは「情報の自由」を守るという「大義」を共有しており、大義への賛同を暗黙の条件に、出入り自由な IRC を介し緩やかな組織形態を形成してきた。大義とは何を意味するのか。彼らは市民的不服従と同様に、法に従うのではなく、自らの倫理的な良心に従うことで違法行為を正当化する。ただし、彼らの大義は非常に抽象的であり、ネットの自由に対する侵害といった抗議活動の大義名分も、アノニマス内の各派閥でその内容が異なるため、抗議活動に一貫性が見えない。そのため、世論には受け入れられないような違法活動も多い。

なぜそのように抽象的な大義のみを彼らは掲げるのかについては理由がある。まず、アノニマスメンバーは国境・階級の壁を超えて世界中にメンバーが拡散しているが故に、メンバーの活動に対する意識も多様であり、それらをまとめるために解釈多様で抽象的な目的を設定するしかないのである。また IRC を利用した戦略会議の場などの交流では、実際の抗議に関する戦略に関するきめ細かな詳細の設定は可能であるが、共通の政治意識の醸成といった時間と議論を要する問題には対応が困難である。

このような理由故に、アノニマス内部の派閥ごとに決定された作戦には過度な犯罪的行為も少なくない。これらを考慮すれば、彼らの主張する大義とは、「違法行為を正当化し、動員を可能にするために設定された、多様な解釈可能性を有した抽象的概念」であるといわざるを得ない。同時に彼らは、特定の集団内において決定された価値観を、全世界に普遍的に共有されるべきものであると認識している。アノニマスの過激な抗議活動は、2010 年頃からそれまで以上に大規模な DDoS 攻撃や、特定企業の機密情報を盗み、公開するといったものへの変化していく。

2011 年 4 月、ソニーの個人情報漏洩事件においてアノニマスが日本でも注目された。事件は、ジョージ・ホッツという当時 21 歳の若手ハッカーが PS3 のハッキングに成功し、PS3 のプロテクト情報等を公開したことに端を発する。ソニーはすぐさまホッツを提訴したが、加えて米連邦裁判所にホッツ

の Twitter アカウント情報や、彼の HP に訪れたユーザーの IP アドレスの公開を求め、許可された。それはホッツと付き合いのあるユーザーばかりでなく、全く関係ないユーザーの個人情報までを開示することに等しく、これに対して多くのユーザーから批判が生じた。アノニマスはすぐさまソニーに対し「情報の自由」に対する侵害行為だとして、これらの処遇の不正を主張。ソニーの運営するオンラインネットワークサービス「プレイステーションネットワーク（PSN）」に対する攻撃を宣言し、実際に DDoS 攻撃を仕掛け PSN の運営を一ヶ月以上も機能停止に追いやった。その後も不正アクセスが続き、結果的にソニー関連企業を合わせて計 1 億件以上の個人情報流出という大規模な情報流出事件へと発展した。

ただしアノニマスは DDoS 攻撃に関しては認めたものの、その後も続けられた不正アクセスと個人情報流出に関しては関与を否定している。個人情報の不正取得は、大義に反するとアノニマスは主張する。これは個人情報の不正取得は、アノニマスではないか、いたとしても一部のメンバーや、またアノニマスの攻撃以後に便乗した金銭目的のハッカー集団の仕業だと想定できる。

もちろんアノニマスの活動は DDoS 攻撃に限定されない。アノニマスの名で合法的なデモを行うこともあれば、ネット検閲に厳しい中東各国のネットユーザーに向けて、検閲回避を行うツールの配布を行うこともある。とはいえ、本稿では近年その活動の量・質ともに顕著になった DDoS 攻撃をアノニマスのハックティヴィズム活動の中心に据えて考察する。

4. ハックティヴィズムとクラックティヴィズム

アノニマスの活動が「政治的目的遂行における、違法な、もしくは法律的に曖昧なデジタルツールの非暴力的使用」するハックティヴィズムに合致していることは言うまでもない。同時に policy circumvention 戦略を取っていることからも、ハックティヴィスト団体としての立場を明確にしていることが確認された。以下本稿では、さらにハックティヴィズムの定義において曖昧な、法的合法性・非合法性の箇所を明確にするために、クラックティヴィズムをハックティヴィズムの比較対象とする。

4.1 ハックティヴィズムの 3 分類

現状において、ハックティヴィズムが内包する合法活動および非合法活動は、いずれもハックティヴィズム活動のひとつとして捉えられている。実際にアノニマス内部には、自らの抗議活動を合法的活動に限定すべきだと主張し、デモや言論活動等の合法活動中心の「チャノロジー」と呼ばれる一派も存在する。彼らもまた情報の自由を標榜する限りにおいてアノニマスメンバーの一員ではあるが、その活動は近年の DDoS 攻撃とは性質を異にする。彼らからすれば、ハックティヴィストを無法者集団であると名指しされることには抵抗がある。また、かつてその違法性の側面ばかりが注目を浴びたことから、ハッカーが自らをクラッカーと区別し、違法行為を行う者をクラッカーと名付けたことは既に述べた。だとすれば、ハックティヴィズムもまた同様に、自らをクラックティヴィズム（cracktivism）と区別すべきである。

ここでもサミュエルの図式に従おう。彼はハックティヴィズムを、ポリティカルコーディング(political coding)とポリティカルクラッキング(political cracking)、パフォーマティヴハックティヴィズム(performative hacktivism)に分類している。ポリティカルコーディングとポリティカルクラッキングは両者共にハッカー・プログラマー文化の影響下にある。ポリティカルコーディングは、そのプログラミング技術を中国の検閲システムである金盾に典型的にみられるように、インターネット検閲が厳格な国家において検閲の目をかいくぐるプログラムの開発など、政治目的に対する抗議行為の一環である。DeCSS や Winny は、現状に満足することなく、新たなコードの製作＝技術開発が、既存のコード＝規則を超え、新たなコード＝規則の形成に寄与したとも解釈できる。それらは単純な破壊活動とは区別されるべきであるとサミュエルは主張する。

他方ポリティカルクラッキングはアウトロー的性格を有した個人主義的、匿名的活動を行う。しばしばポリティカルクラッキングは政治秩序を鑑みず、規制なきクラッキングを行うという、最も非合法的な活動である。サミュエルが念頭に置くのは、クラッキングによって入手した社外機密情報をもとに行う企業恐喝等である。そしてサミュエルは DDoS 攻撃もポリティカルクラッキングとする。

最後にパフォーマティヴハックティヴィズムは、暴力を伴うことのない、政治的にリベラルな考えをもったアーティスト志向のあるアクティヴィストであり、ウェブサイトのパロディ化や反グローバライゼーション運動に関わるという。上記のサミュエルの定義を著者の議論に当てはめれば、パフォーマティヴハックティヴィズムはむしろサイバーアクティヴィズムに近い概念である。

まとめると以下のようになる。ハックティヴィズムは

①ポリティカルコーディング→領域侵犯的、規則重視（ハックティヴィズム）
②ポリティカルクラッキング→個人主義的、アウトロー的（クラックティヴィズム）
③パフォーマティヴハックティヴィズム→領域侵犯的、ポストモダン左派的（サイバーアクティヴィズム）
に分類が可能である。先の DeCSS や Winny の事例は、①のポリティカルコーディングに分類可能である。両プログラムの作者は、意図的にせよ無意識的にせよ、技術開発によって制度の変革に間接的に関与している。その場合、その行為は犯罪性と同時にその思想性や目的において理解されるべきである。本稿では参照しなかったウィキリークスもまた、内部告発システムの開発によって、ポリティカルコーディングを行っていると判定できる。

それに対して、アノニマスの活動はサミュエルの分類では区分が困難である。DDoS 攻撃は匿名的であっても個人主義的な活動ではない。また上述のようにアノニマスの名で行われるデモやその他多くの活動は、サミュエルの分類のすべてに該当する。すなわち、アノニマスの活動は現状の分類において括ることが不可能であるばかりか、個々の活動ごとにその犯罪性や思想性を考慮しなければ理解し難い状況にある。

5. おわりに

本稿はハックティヴィズムと関連する語彙との差異を明らかにすることを目的とし、サイバーアクティヴィズムとサイバーテロリズムとの差異を示した後、ハックティヴィズムに関連する 3 つの用語を整理した。そこで、近年最も活動的なハックティヴィスト団体であるアノニマスの活動が、サミュエルの図式では分類不可能であることを指摘した。

ハックティヴィスト団体としてのウィキリークスやアノニマスは、前者はその創設者ジュリアン・アサンジのカリスマ性によって、後者はその印象的な仮面を被ることで、匿名でありながらキャラクター性を発揮している。いずれの組織も大衆動員戦略に優れており、またハックティヴィズム活動は参加が容易なため、その活動は今後もますます増加することが予想される。しかしそれが意味することは、違法行為がこれまで以上に蔓延することでもある。現にアノニマスの活動に参加する若者は多く、毎年ティーンエイジャーが数人～数十人の規模で逮捕されている。ハックティヴィズムは情報技術とその具体的方法である policy circumvention により、従来のアクティヴィズムに比べ、より強力な法・政策に対する抗議、および政策提案能力を有した。だが裏を返せばそれは、一部のユーザーの意見が大衆動員を可能にし、多大な不正を世界中に蔓延させながら統治機構との争いを繰り広げることにもなりかねない。

このように、ハックティヴィズムに関する評価は難しい。現状の制度を更新する可能性もあれば、単に巨大な犯罪行為として扱うことも可能だからである。ハックティヴィズム・クラックティヴィズムに限らず、違法性を伴う活動をどのように評価するべきかについては、まだまだ多くの議論が必要とされるだろう。ハックティヴィズム運動をより包括的に議論するためには、ハックティヴィズム運動を社会運動の観点から考察する必要がある。その際、市民的不服従に見られるような法的違法性と個人の良心に照らした正当性との兼ね合いの中で、ハックティヴィズムをどのようにとらえるかについては、今後の研究の課題としたい。

[注]

（1）詳しくは RFC1392 を参照のこと。http://tools.ietf.org/html/rfc1392 日本語訳は以下を参照 http://www.nic.ad.jp/ja/translation/rfc/1392.html。なお、このハッカーとクラッカー（あるいはハッキングとクラッキング）の差異に関する議論は、技術の専門家の間で今も議論の的になる問題でもあり、本稿では扱わない。本稿においてはハッカーという言葉を、コンピュータに詳しく、その改

良に快楽を感じる人々、といった元々の意味で用いる。この問題の参考文献としては、白田秀彰「ハッカー倫理と情報公開・プライバシー」『高度情報化の法体系と社会制度』 科学研究費補助金・重点領域研究報告書, 1995 年 3 月、がある。
（2）なお、policy circumvention については、2011 年 8 月に行われ著者も登壇した、慶應義塾大学 SFC 研究所 プラットフォームデザイン・ラボ主催のシンポジウム『ソニーの個人情報流出事件をどう考えるか-サイバー攻撃に対する政府・企業・個人の対応-』の中で八田真行氏が言及している。当日の資料が八田氏の HP からダウンロード可能である。www.mhatta.org/mhatta-keio-20110829.odp
（3）金子は著作権制度がいずれにせよ近い未来に崩壊することを予感し、新たな制度を構想していた。それは「デジタル証券によるコンテンツ流通システム」と呼ばれるものである。詳しくは、佐々木, 2006, p. 90. を参照。

[文中の参考文献]

[1]Samuel, W ,Alexandra, *Hachtivism and the Future of Political Participation*, Ph. D. Dissertation. Harvard Universiiry, May 10, 2006. (http://alexandrasamuel.com/dissertation)
[2] Denning, E Dorothy,, “ACTIVISM, HACKTIVISM, AND CYBERTERRORISM:THE INTERNET AS A TOOL FOR INFLUENCING FOREIGN POLICY” *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Rand Corp, 2001.
[3]スティーブン・レビー著、古橋芳恵、松田信子訳『ハッカーズ』、工学社、1987 年。原著は 1984 年出版。
[4]井口秀介・井上はるお・小西誠・津村洋著『サイバーアクション』、社会評論社、2001 年。
[5]ウィン・ファン・デ・ドンク他、尾内達也訳『サイバープロテスト』、皓星社、2009 年。なお原著は 2004 年出版。
[6]寺島俊穂著『市民的不服従』、風行社、2004 年。
[7]佐々木俊尚著『ネット vs リアルの衝撃――誰がウェブ 2.0 を制するか』、文春新書、2006 年。

[その他参考文献]

[1]Fleckenstein S Kristie, 2009, *Vision, Rhetoric, and Social Action in the Composition Classroo* ,Southern Illinois University Press.
[2]浜野喬士著『エコ・テロリズム』、洋泉社新書 y、2009 年。

[i] Kenjitsukagoshi32@gmail.com

(2012 年 4 月 29 日受理)