「コンピュータ・ネットワークへの規制に対する社会学的考察」

安倍　尚紀† ‡
東北大学情報科学研究科†

１．はじめに

2003 年 11 月 17 日、ブッシュがサイバー犯罪条約を上院に批准勧告し、世界中の注目を集めた。ヨーロッパ協議会（Council of Europe）によるこの条約に、日本ではすでに署名しており、関連法案を準備中である。この動向は、コンピュータ・ネットワークの脱国境的な特性にあわせて、国際的に犯罪対策の足並みをそろえていくことを意図している（また現在、米国に渡航するすべての人は、入国時にもれなく顔と指紋のデータをとられる）。翻って、こうした動向に対するわれわれ一人一人の感情には、複雑なものがあろう。本稿の目的は、おこなわれる議論を不毛なものにしないためにも、現在の文脈において「規制」についてとらえなおすことである。

そもそも従来からこうした規制への反応にはいくつかの論調がみられる。が、ただし、それらの議論の前提として強調しておきたいのは、コンピュータ・ネットワークをめぐる議論が、もはや、いわゆるネット社会の住人だけの問題ではないことだ。たとえば、街頭の監視カメラやユビキタス社会の現状を考えあわせれば、ネットワークを媒介しない行為は少なくなってきている。したがって本稿では、「規制」を巡る従来の議論に、こうした現状分析を重ねて議論する。

まず、規制を巡る議論を整理し（2 節）、われわれのセキュリティ観の《変容》について述べる（3 節）。最後に、そうしたセキュリティ観の《変容》に重ねて、規制を巡る議論を捉えなおしたい（4 節）。

２．原理的考察－サイバー・リバタリアニズム VS 規制主義

「無法者と自由という新しい発想にとっての理想的な飼養場」（P.バーロウ）であるインターネットの匿名性などを論拠にして、われわれの日常生活に何らかの規制を設けようという立場がある。典型的には、1996 年の通信品位法(Communication Decency Act)だ。バーロウの『サイバースペース独立宣言』はこれに応えるものだったが、P.ボルソック[3]は彼らを「技術リバータリアニズム」として批判し、論争を呼んだ。

彼女の言うリバータリアニズム（自由至上主義）は、シリコン・バレーの技術者たちを指しており、二つの類型がある。「大文字の L」（Big L）と呼ばれる人々は、「社会契約と統治の価値に対する、お手軽な明瞭さ」をもち、他方、「小文字の I」（Small I）と呼ばれる人々は、「人とのつながり欠き、人間らしさといわれる大事な部分が覚束ない」。これらをまとめて、**サイバー・リバータリアニズム**と呼んでおこう。「どんな政府もインターネットの富なしに生き残れないけど、でもどんな政府もインターネット上で起こることをコントロールできない」[1]。

こうして、サイバー・リバタリアニズム VS 規制主義という二者による、能天気な自由主義と、ことなかれ主義の対立は続いてきた[1]。以下では、このことを念頭に考察を続けよう。

３．ポスト 9.11 の構図――「匿名性」・プライバシーの変容

ポスト 9.11 のいまや、上記のそれぞれの立場が追求するセキュリティやプライバシーといった概念がテクノロジーの発展とそれにともなう動機付けによって、根本的に変容している。（IPTS の提出した報告書[2]も述べるように、）ポスト 9.11 のセキュリティ・システムの思想は、**reactive（事後作用的）なモードから pro-active（事前作用的）なモードへ**と移行した（[6]も参照）。

従来の **reactive なセキュリティ**では、再度問題が生じた際のケアをどうするかということが念頭に置かれる。例えば、法律は基本的には問題が生じた後、事後作用的に効力を発揮する[1]。この意味で、法が問題にするのは**個別具体的な問題に対するアプローチ**である。

が 9.11 以降、あらゆる危機対処において、**pro-active なセキュリティ**が強調されるようになってきた。これを可能とする前提条件は、言語も貨幣も含めて、コンピュータネットワークというものがあらゆるものを媒介するようになってきたことである。現実世界の人間が地球上の大気や重力の制約を免れ得ないように、すべての行為もまたアーキテクチャの制限を受ける[1]。事前のフィルタ

Sociological Study on Regulation in Computer Network
† ABE Naoki(Graduate School of Information Science, Tohoku University)
‡ 当初、佐々木寛太郎氏が共著者となる予定だった。

[1] ただし同時に、法は、問題を起こそうとする輩に対する抑止の《動機づけ手当て》としても働く側面もある。

リング等によって個人データを管理しリスクを未然に防ごうというのが、この事前作用的なセキュリティのモードである。このような観点から、RFID や認証絡みの技術（bio-methorics など）／位置検索システム等、いわゆるユビキタスの技術すべてが、このとき reactive なモードから pro-active なモードへの移行に重ねて捉えなおされる。

４．考察

街頭の監視カメラと個人情報のデータベースによって、「何時、誰が、どこで、何を」しているか、していたかということが、今現在の法的／技術的状況においては事後的に極めて明瞭に指摘できるわけだが、これが法や慣習における re-active なセキュリティの層を、より細かく pro-active なセキュリティの層で補強した状況である。つまり、常時人々は「責任」を追わされる可能性を持っている。これは以前の reactive なセキュリティにおいては極めてグレーゾーンであった部分に権力の網が侵入してきて、新たなる「主体」を構築したというフーコー的な状況でもある。が、繰り返せば問題はより複雑であり、結局フーコー的な「内面を規律によって統治／制御する」というシステムから、「身体を直接管理する」という次元にセキュリティが移行した。つまり、reactive なセキュリティから pro-active なセキュリティへの以降は、これまでのような責任の問題には回収できない。

ここにおいて新たに、たとえば「匿名性」などの利益を擁護しえないという立場がありうる。なぜなら、身体に直接危害を与えるリスクがない限り、内面、信仰、価値観、政治的心情はある程度自由にできるはずであるから。したがって、以上の前提において、２節のサイバー・リバータリアニズム VS 規制主義の図式は、再度、以下のように言い換えられよう。ネットワーク使用の政治的な妥当性(legitimacy)を疑問視する《監視社会憂慮派》と、妥当性を認める《リスク管理社会肯定派》である。

これら二つの立場は、リスクが「確率的」に生じるという事実に対する、全か無かという二つの極端な反応である。リスクが「確率的」に生じるという事実をネガティブに捉える立場は、この「確率的」な事実をできるだけ回避しようという立場に立つ。つまり、「ネットワーク管理」によって「確率的」な事実を可能な限りトラッキングしようとするであろう。「確率的」にしか生じないリスクをポジティブに捉える立場は、いかに管理を追求しようとも、リスクが「確率的」にしか生じえない限り、完全なるコントロールは不可能である。「ネットワーク管理」は過剰な監視体制であるとして批判する。この差異は、legitimacy を巡る差異にも絡んでくる。例えば、これまでの法や規範を元にした制度の legitimacy とは、ありきたりの言葉で言えば、構成員相互間の信頼や予期を媒介として生じた行為の結果を法や規範の範疇において処理できるという前提の下において構築されてきた。この状態とは、つまり、構成員の「予期」、並びに行為を裏打ちする reactive なセキュリティ（法／規範）が legitimacy を持つ状態であるといえる。それに対し、コンピュータネットワークの媒介によって、これまで「予期」と呼ばれていたコスト計算の選択肢が可視化されることになり、つまりこの選択肢を管理すれば、実際には「確率的」にリスクが生じる事は事実であるが、少なくともこの選択肢を通過して生じるリスクについては事前に回避可能であり、あるいは事が生じたとしても責任の所在を明らかにすることが出来るというのが pro-active なセキュリティであるといえる。

以上、ネットワークの全面化を前提に考えれば、法という次元において担保されていた legitimacy は、まさに技術（アーキテクチャ）の次元に移行したということができよう。同時に、この変容を後押しする力となったのは、他ならぬ公衆(public)による危機意識であることが重要である。「身体の安全」を掲げる議論に対して疑義を投げつけるという立場は、確保不能であるからだ。2 節の議論の背景では、セキュリティとプライバシー（や言論の自由）のトレードオフが想定されており、「規制」が紋切り型に捉えられているのである。

参考文献

[1] Lessig, L. 1999 *Code and other laws of cyberspace*, Basic Books（＝柏木・山形訳、2001、『CODE?インターネットの合法・違法・プライバシー』, 翔泳社）

[2] CLEMENTS, B.,et.al. 2003 “Security and privacy for the citizen”, IPTS: http://www.jrc.es/home/publications/publication.cfm?pub=1118

[3] Borsook, P. 2001, *Cyberselfish*: Public Affairs

[4] Langdon, W. 1997 “CYBERLIBERTARIAN MYTHS AND THE PROSPECTS FOR COMMUNITY”, http://www.rpi.edu/~winner/cyberlib2.html

[5] D., R., Koepsell 2000, *The Ontology of Cyberspace*, Open Court（＝田畑訳、2003、『ネット空間と知的財産権』、青土社）

[6] 東浩紀・大澤真幸 2003、『自由を考える』、NHK ブックス