Title	「共有地の悲劇化」するネット社会に求められる情報環境倫理
Sub Title	Information environmental ethics needed in the network society falling into the state of the tragedy of the commons
Author	水元, 豊文(Mizumoto, Toyofumi)
Publisher	慶應義塾大学メディア・コミュニケーション研究所
Publication year	2002
Jtitle	メディア・コミュニケーション : 慶応義塾大学メディア・コミュニケーション研究所紀要 (Keio media communications research). No.52 (2002. 3) ,p.21- 45
JaLC DOI	
Abstract	
Notes	
Genre	Journal Article
URL	https://koara.lib.keio.ac.jp/xoonips/modules/xoonips/detail.php?koara_id=AA1121824X-20020300-0021

「共有地の悲劇化」するネット社会に求められる情報環境倫理

水元豊文

▶ 1　問題意識
――日常化するネット・情報環境問題にわれわれはどう立ち向かうべきか――

コンピュータおよびインターネットに代表される電子ネットワーク（以下では略して「ネット」と呼ぶ）は深くわれわれの生活に根づいてきている。その一方で，ここ数年の間に，クラッキング[1]，ウィルス，サイバー・テロなどの反社会的行為は，電子商取引などの「正当な」ネット利用を上回る勢いで急増し，それらのニュースがマスメディアを賑わさない日はないというような状況になってきている。

コンピュータ機器を介してバーチャルなコミュニケーション環境を提供するネットでは，リアルなコミュニケーションと異なり，匿名性を高めることが容易であり，そこで構築される人間関係は一時的，一方的，そして部分的なものになりやすい。そのように「浅い」コミュニケーションのツールであるネットでは，簡単かつ迅速に人間関係を創りあげることができる一方で，関係が不要になれば比較的簡単に離脱することができる。創りあげられた関係に対する帰属意識が低いため，担うことを期待されている役割をあまり深く自覚せず，反社会的行為を無責任にとってしまうことも少なくない。

環境に対する責任は，なかなか自覚されない。特に個人の自由を最優先にする社会では，環境に対する責任は軽視されやすい（本田，1998）。それは，環境を破壊するような行為をしたとしても，環境そのものが抗議することもないし，環境を利用する人々に直接被害が出るのには長い年月を要するからである。

しかし，反社会的行為をこのまま無秩序に放置しておくと，ネットという有益な情報メディア／コミュニケーション環境そのものが維持できなくなってしまう。ネットはわれわれの生活とって切っても切り離せないものになっており，われわれはもはやそれなしには生きられないほど強く依存している。それらが使えなかった状態に戻ることは不可能である。そのように重要な公共インフラであるネット・情報環境が混乱に陥ったり，破壊されることは非常に大きな問題である。しかし，越智・土屋・水谷らが（2000: ii-iv）

脚注

1．一般にコンピュータ・システムに不正侵入する者を総称してハッカーと呼ぶ場合も少なくないが，この論文では，倫理問題を扱ううえで動機の違いは非常に重要であると考えるので，インターネットの技術規約や安全に関する助言などが記されているインターネット標準文書（RFC）にしたがって，ハッカーとクラッカーを区別して扱う。すなわち，ハッカーとは殊にシステムやコンピュータ，ネットワークについて深く理解することに喜びを感じる人々を指し，クラッカーとはコンピュータ・システムに権限を持たずにアクセスしようとする人々を指す（RFC 1983）。

が強調するように，目下の問題解決だけに心を奪われると，えてしてそれを取り巻く背景や条件が見えにくくなる。トラブルの解決ばかりに目を向けると，その背後により本質的な問題が潜んでいることを忘れてしまう。いまわれわれが考えなければならないのは，そのようなネット・情報環境（情報生態系）の混乱や破壊行為にどう対処すべきか，ネット・情報環境を誰がどう維持するか，そしてそこでわれわれはどう生きるべきかという本質的な部分である。

ネット・情報環境問題を倫理的に考察するうえでの準拠枠となるのが，情報倫理学と環境倫理学という二つの学問分野を構成する基本的な考え方とそれぞれの分野で蓄積されてきた知見である。それら二つの分野は，たしかに応用倫理問題を扱うという点では共通であるが，問題を考えるうえで個人に重きを置くのか，それとも社会や環境に重きを置くのかという点で大きく考え方を異にしてきた。これまでの情報倫理学の基本的課題は，知的所有権やプライバシー問題に端的に見られるように，ある個人の自由や権利が他者の自由や権利と抵触する際にその利害関係をどう調整するかということであった。たしかにこれまでも情報倫理学でも，ネット・情報環境問題に関連する問題としてウィルスやシステムへの不正侵入問題は扱われてきた。しかし，そこで想定されていたのは「他者」の権利を侵害するかどうかという対個人問題が中心であり，環境そのものを混乱ないし破壊するというものではなかった。現在問題となっているクラッキング，ウィルス，サイバー・テロなどの反社会的行為は，環境そのものを破壊・汚染してしまう水準に達しており，これまでの情報倫理学の射程を超えている。

そのような環境そのものの混乱・破壊に対してわれわれがどう立ち向かうべきか，環境を誰がどう守るべきかという問題を考えてきたのがまさに環境倫理学であろう。自然環境の破壊や汚染が急速に進むなか，さまざまな知見が蓄積されてきた。ネット・情報環境問題を考えるうえでも，われわれは何をどう論じるべきか，どのような選択肢が可能かなど，環境倫理学で培われてきた知見はネット・情報環境問題を考えるうえでも非常に有益である。しかし，ネット・情報環境と自然環境には違いがあることも確かであり，それらの相違を念頭において両分野で発展させられてきた知見を適切に組み合わせることが必要であろう。

ネット・情報環境が自然環境ともっとも大きく異なる点は，ネット・情報環境があくまでも人間生活を維持するために意図的あるいは無意識的に創られた人工的な環境であるということである。人工的な環境であるネット・情報環境には，自然環境のような自己保全機能がもともと組み込まれているわけではなく，環境を利用する者がそのような機能を意図的に組み込まざるをえない。ネット・情報環境は環境をどのようなものにするかという利用する人々の意図と意欲に強く依存しているのである。もうひとつの大きな違いは破壊や汚染に対する環境の可逆性の高さである。自然環境では一度破壊が進むとそれらの被害を全面的に回復するのは非常に難しい。これに対して，そもそも人工的なものであるネット・情報環境は破壊や混乱が起きても，環境を保全しようとする人々がいる限り，それなりに機能させていくということが可能である。このような環境そのものの本質的な違いを念頭に置いたうえで，われわれはネット・情報環境にふさわしい環境倫理を築く必要がある。

ネット・情報環境の破壊や汚染が進むなか，環境倫理的発想を持ち込むことが必要であることは間違いない。しかし，環境保全をまっとうしようとするあまり環境全体主義（ファシズム）に陥ることが環境倫理学でも問題視されているように，環境倫理的発想が行き過ぎてしまうことは問題である。環境を保全しようとすればたしかに公共のために個人の自由をある程度制限せざるをえない。けれども，そのような制限を無制限に認

めてしまうと，公共のためという理由で個人の自由は圧迫され，「個人は環境のために存在する」という位置に置かれてしまう危険性をはらんでいる。

ネットは，表現の機会を増加させるということでは自由を拡大するものである。その一方で，ネットは，集権的管理を容易にするためにそもそも開発されたものであり，個人を特定し，その活動を監視することを容易にする。ネットは本来的に個人の自由を制約する要素をはらんでいるのである。特に最近，個人の自由を制約することにつながる技術の発展は著しい。集権的管理を必要としているのは，巨大組織，特に大企業や政府である。そのような巨大組織は，個人とは比較にならないほどの経営資源（人，物，金，情報など）を活用することが可能である。なかでも技術的な優位性は格段に高い。さらに最近では，Winner（2000: 176-186）が懸念するように，すでに権力を持った者がますます大きな権力を手にし，すでに支配力を持っている者がますますその支配力を集中させ，すでに富み栄える者がますますその富を増やしているように見える。たしかに民衆が低価格のコンピュータを手に入れることは，社会的影響力のひとつの次元である電子的次元において，民衆の力を増大させるものではあるが，権力を持つ者と民衆の力関係そのものを変えるほどのものではない。

多くの人々が，無差別同時多発テロなどをきっかけに，政府が安全を保障してくれるのであれば，プライバシーなど基本的な人権についてもかなりの程度までは放棄するのは仕方なく，政府に権限を委譲してもかまわないと思うようになってきている（Winner, 2000: 190）。問題は，安全という大義名分によって個人の自由が極端に制限されるようになってしまうことである。巨大組織にはすでに権力が集中しており，さらにどこまでどういう条件で権力を委ねるべきなのであろうかが問われている。

個人は，あくまでも環境と共存すべきものではあっても，環境に従属すべきものではない。目的が正当であれば従わない理由はないが，環境や公共のためという理由だけで個人の自由が制限されるのは不当である。たしかに，ネット・情報環境を維持するためにクラッキング，ウィルス，サイバー・テロなどバーチャルな世界で起きている反社会的行為を抑制することは必要である。そのような反社会的行為により環境そのものが維持できないほど破壊や汚染されてしまってから，環境を作り直すのは容易ではない。そのような破壊的な段階に進むことそのものを抑止することが求められている。

ネット・情報環境の破壊・混乱を抑止するためにもっとも重要なことは，その環境を利用する人々（ネット市民）それぞれがそのような反社会的行為を抑止するための責任を担っていることを自覚し，自分たちのネット・情報環境を創造・維持するための積極的な活動を実践していくことである。そこでは，自分たちにとって環境がどうあるべきか，自分たちはどのような環境を望むかという，環境に対する価値観が問われる。環境がそれなりに整備された段階で環境を利用するようになった人々は，その環境の創生に携わった人たちに比べて，環境に対する責任感が薄れがちである。ネット・情報環境に対する責任感が希薄化している現在，創生に携わった人々が持っていた価値観や精神をあらためて問い直してみる必要があるであろう。創生に携わった人々は，自助自立の精神をもって，コンピュータやネットワークの技術的可能性に魅せられ，その可能性を追求した。そのような技術的可能性の追求者が「ハッカー」と呼ばれた。現在ネット・情報環境を利用している人々の多くは，自分たちを環境の単なる消費者としてしか考えておらず，環境の汚染や混乱に対して無責任で「傍観者」的な態度しか示さなくなってきている。環境を破壊や汚染から守るためには，ネット・情報環境は自分たち自らが「創造」していくものであるとともに，自分たちの環境と自分自身はそれぞれが自ら守るしかないという自助自立の精神と責任感を涵養するしかない。たしかに法律など外的な制

裁を強めることも環境の破壊や汚染を抑止するうえで有益ではあるが，そのような外的強制を有効に機能させるためにも自助自立の精神と責任感の涵養のような内的サンクション（倫理的自己拘束）を自らに課すような人間を増やすことが重要である。

この論文では，ネット・情報環境に対する破壊的な反社会的行為にわれわれがどう立ち向かうべきか，そして，そのもっとも有力な実践主体として期待されている政府の関与はどこまでどのような条件で認めるべきかなどという問題など，ネット社会における自由とその限界の問題について考える。それらの問題は，ネットが本格的にわれわれの生活の中に浸透した現在，ネット・情報環境はいかにあるべきかというあり方そのもの，そしてそのような環境でわれわれはどう生きるべきかということに深く関わっている。

▶ 2　日常化するネット・情報環境の破壊・汚染
――クラッキング，ウィルス，サイバー・テロはネット・情報環境の常態的構成要素であり，自助自立の精神をもって，共生の道を模索するしかない――

2-1　クラッキング，ウィルス，サイバー・テロなどの横行により増幅される社会的混乱と不安

現在，ネット・情報環境の破壊や汚染が問題になっている。なかでも大きな問題となっているのが，クラッキング，ウィルス，サイバー・テロなどの反社会的行為であり，そのような行為が日常的に行われるようになっている。関連するニュースがメディアを賑わさない日はないほど，それらの反社会的行為は日常化しており，ネット利用者の多くが混乱するとともに不安感を強めている。

ネット・情報環境の破壊・汚染問題でまず第１に挙げられるのが，不正にコンピュータ・システムおよびネットワークに侵入する「クラッキング」である。この１，２年，ネットのセキュリティをめぐるトラブルがニュースでひっきりなしに伝えられるようになっており，必ず毎日のようにどこかのWebサイトが攻撃されている。クラッキングにより，強力なセキュリティ対策が施されているはずの政府機関や大手民間企業でさえ，システムが簡単に乗っ取られ，何度となく業務が混乱に陥っている。

ネット・情報環境にとって本当に脅威なのは，Webを不正に書き換えるネット上の「落書き犯」というよりも，ニュースの見出しを飾っていない組織的あるいはプロのクラッカーたちである。Web不正書き換えのように被害が目で見て明らかな場合はそれなりに対策を講じることは可能である。しかし，組織的あるいはプロのクラッカーたちは自分たちが不正に侵入し，犯行に及んだことそのものを隠してしまうので，被害にさえ気づかないことも少なくない。そのようなクラッカーたちが，政府や産業界の機密ネットワークに侵入して，情報を盗難・破壊したり，銀行口座に侵入したり，クレジット・カードの請求額を激増させたり，あるいはコンピュータ・ウィルスをばらまくと脅して金を強請ったりするようなことも増えている（Wired News, 1999.1.22）。さらに，政府機関や企業が保有している価値ある情報を盗むのではなく，後で述べるが，それらの組織が有するネットそのものを破壊してしまおうとするサイバー・テロに発展する場合も増えてきている。

価値の高い情報を盗むことを目的にしているプロのクラッカーたちにとっては，悪戯目的の少年ハッカーたちが残す目に見える犯行声明が，自分たちの存在そのものを隠すためのいい煙幕になっている（ZDNet, 2000.9.13）。「サイバー・スペースの防衛に関する最大の誤解は，脅威となっているのは少年ハッカーたちという考え方である。たしかに少年ハッカーたちはヘッドライン・ニュースを飾る。捕まってしまうからだ。だが，プ

ロは捕まることはない」と言われている。

ネット・情報環境を破壊・汚染するサイバー犯罪は，電子商取引のようなネットの正当な利用と比べても，より速く成長しているとさえ言われる。特に爆発的に成長しているのがクラッキングを利用したスパイ（情報の窃盗や改ざんなど）活動である。ネットにつながっていれば，侵入する意志と能力さえあれば，離れた場所であってもどこでも侵入できてしまう。グローバルに張り巡らされたネットのおかげでスパイ活動は非常にやりやすくなった。クラッキングを受けたという報告は急増しているが，クラッキングを受けたこと自身に気づいていない企業も少なくない。

第２の問題は「ウィルス」である。現在，ウィルスやワームは鼠算式に増え，その破壊力は飛躍的に強力になってきている（ZDNet, 2001.4.2）。特に，ここ１，2年，ウィルスが振るっている猛威は凄まじく，ネット・情報環境そのものを危うくさせる危険さえはらんでいる。さらにネット化が進むこれからの時代には，より強力な新種のウイルスがわれわれを襲うことになるであろう。軽い悪戯心で作られたウィルスやワームも少なくないが，自然界のウィルスと同じく適切な処置を施していないと猛威を振るう危険性は高い。

第３の問題は，ネット・情報環境そのものを破壊してしまう危険性をはらんでいる「サイバー・テロ」である。マスコミで取り上げられるクラッカーやウィルスの製作者たちの多くは，ネット・情報環境を破壊することを目的としているというよりも，生じる社会的混乱によって自分たちの存在を誇示したいために，そのような反社会的行為にはしってしまういわゆる「威嚇攻撃者」である。そのようなクラッカーたちがネットを攻撃する動機は「退屈さ」であり，攻撃そのものも行き当たりばったりのものが少なくない（Wired News, 2000.6.27）。問題なのは，ネット・情報環境だけでなく，電力網や交通網などの社会・公共インフラの破壊を目的としているサイバー・テロリストたちである。現在，組織的なサイバー・テロも少なからず出始めている。ネットは社会・公共インフラを制御するために必要不可欠なものであり，それが寸断されるとほとんど制御できなくなってしまう。社会・公共インフラが破壊されると，戦争で爆撃を受けたのと同じぐらいの死傷者が出るなど，非常に大きな被害が出る可能性が高い。

これまでの戦争は正規の軍隊を戦わせるというものであった。しかし，ネット上での戦争では，むしろ国家とは関係のない準軍事的で非正規の武力が使われる（Wired News, 1999.4.20）。ネット化が進めば進むほど，サイバー・テロリストは以前は不可能だったところまで侵入できるようになる。ネットとその窓口であるコンピュータ端末は，過激派の兵器庫の中でも最も重要な機器となったといわれる。彼らはそれによって，メンバーを集めたり組織を拡充させたりできるばかりか，10年前なら存在すら知らず，簡単に話もできなかったような人々やグループと協力できるようになっている。

現在，サイバー世界と実世界は密接に連動するようになっており，一方の世界で起きたことはもう一方の世界にそのまま波及する。特にサイバー世界ではテロや戦争行為を素早くかつ容易に実行することが可能である。最重要な社会・公共インフラであるネット・情報基盤は現在，戦争遂行上の生命線となっており，それを破壊することが最も効率的かつ効果的な戦略である。国際紛争が実世界で発生すると必ず，激しいサイバー・テロ攻撃が応酬される。サイバー戦争から実世界の戦争に発展した事例は今のところないが，ネット上で繰り広げられるプロパガンダ合戦は紛争地の人々の感情を煽り立てるには十分である。ここ１，２年の間にも，イスラエルとパレスチナ，米国と中国の間で，サイバー・テロないしサイバー戦争が繰り広げられたことに見られるように，ネットが新たな戦場になるサイバー・テロおよびサイバー戦争の脅威は現実化している（Wired

News, 2000.11.8, 2001.5.1)。各国とも,「将来各国が,爆弾ではなくてサイバー攻撃で,互いのインフラを破壊する能力を共に持つことになること」を非常に懸念しており,いわゆる「ならず者」的な国家やテロリスト・グループ,犯罪カルテルなどが,ネットに「計画的,全世界的に侵入」して,第二次世界大戦時のインフラに対する戦略爆撃にも比肩し得る被害を与える可能性があるとされている(Wired News, 1999.1.22)。グローバルにネットが張り巡らされている現在,サイバー・テロやサイバー戦争のようなネット・情報環境そのものに対する破壊行為は,関係当事国だけの問題ではなく,世界的な問題である。

サイバー・テロないしサイバー戦争に関連して,ひとつ大きな問題になっていることがある。ネットの普及により,個人が政治的活動を展開することは容易になったことは確かである。しかし,問題もある。これまでは開戦および戦争遂行の決断は,国家権力の中枢にいる権力者と一部の集団を媒介することによって行われてきた。そのような政治的決定を行うことで,普通の市民が直情的に戦争に突入することを抑制してきた。しかし,サイバー戦争になると,私人でも敵国の政府機関に戦争を仕掛けることもできるようになる。そのような個人による恣意的なサイバー戦争への参戦に頭を悩ませている政府も増えてきている(Wired News, 1998.9.22)。サイバー戦争とはいえ,血気盛んな市民が外交や軍事紛争に直接参加するのは大きな問題である。政治的に非常にアクティブでクラッキングなどサイバー戦争を遂行するのに十分な技術力を持った一般市民が行う,「ハクティヴィズム」と呼ばれる電子的政治活動も増えてきている。そのような直情的に戦争行為にはしってしまいやすい個人を政府が統御することは非常に難しい。

現代の社会には,社会を根本から変えてしまうような力,特に技術的な力が蔓延している。しかし,そのような力にともなう役割や責任が意識され,果たされる可能性はかえって望みがたい状況になっている(品川, 2001b)。クラッカーやウィルス製作者の行為も,個々人が単独で行う場合には影響はそれほど大きくないかもしれない。しかし,それらが組織的かつ集中して行われると,ネット・情報環境そのものを破壊してしまうほどの結果を引き起こしてしまう場合もある。

2-2 自助自立の精神をもって,共生の道を模索するしかない,ネット・情報環境の常態的構成要素としてのクラッキング,ウィルス,サイバー・テロ

クラッキング,ウィルス,サイバー・テロなどの反社会的行為は,たしかにネット・情報環境にとって破壊的な混乱を引き起こしかねない撹乱因子ではある。しかし,自然の生態系ないし環境においても,どんな時代であっても病気の原因となるウィルスや破壊活動などがなくなったことはない。そのような生態系および環境にとって撹乱因子を一定レベルに抑制することはできなくはないが,根絶することは不可能に近い。それから,本質的にそれらを根絶することが環境にとって本当に有益なのであろうか。環境に対する「悪」を廃絶することはまず不可能である。また,そのような「悪」なる要素を取り除くと,その環境を利用する者は安全を当然のものとして受け取ってしまい,環境の劣化が起きてもそれに気づかず,適切な対応が迅速にできなくなってしまいやすい。われわれに必要なのは,「悪」なる要素が存在することを前提に,個々人が環境の劣化に敏感になるとともに,環境の劣化に対して迅速かつ適切な対応ができる基礎体力をつけることではなかろうか。

ネット・情報環境にも,自然環境とまったく同じく「悪者」も「ウィルス」も存在する。それらの悪なる者を廃絶することは不可能であり,それらとうまく共生していかざるを得ない。「コンピュータが世界に接続されているとき,静かな時間帯というものは存

在しない。ネットは眠らない」と言われるように，誰もが接続された世界は，誰もが危険にさらされる世界である（Wired News, 2000.9.11）。そういう世界こそ，われわれが慣れていかざるを得ない厳しい現実なのである。クラッキング，ウィルス，サイバー・テロについても，そのような行為があることを前提として，それらとうまく付き合っていくしかない。

たしかにそういう厳しい環境に適応できない人々もいる。そのため，そういう人々は誰かが保護すべきではないかという議論も出てくる。個人にとっても組織にとっても，たしかに保護も福祉もある程度は必要である。福祉国家政策や国際援助は，いっけん利他的な行動として賞賛されるべきもののように見える。しかし歴史を見れば分かるとおり，援助された者は援助を受けることを当然のものと思ってしまい，「自らが何とかする」という精神を失い，「他者依存症」に陥ってしまいやすい。自助自立の精神を失うことこそが環境適応力の低下の大きな源泉である。保護や福祉を提供する場合，個々人が「自らのことは自らが守るしかない」という意識をもたざるを得ないような程度に留めるべきではなかろうか。ネット・情報環境での反社会的行為に対する対策を社会全体（特に政府が中心となるが）で実行することについても，その環境を利用する人々が自らのことは自らが守るしかないと思う程度のものであることが必要であろう。

次では，共有地としてのネット・情報環境ではなぜ「悲劇化」が進んでいるのかあるいは進みやすいのか，その誘因を探る。

▶ 3　進行するネット・情報環境の「共有地の悲劇化」とその誘因

ネット・情報環境はそもそも「共有地の悲劇化」を招きやすい要因を内包しているが，最近は特に悲劇化の度合いを強めている。ネット・情報環境は，そもそも管理権限も権利・責任関係も複雑で不明瞭な共有地である。共有地では，それを利用する個々人が自らの利益を最大化するために利己的な行為をとることは避けられない。個々人の行為はそれぞれの人にとっては合理的な行為であっても，それらが全体として集積されると共有地である環境そのものを破壊してしまうことになる。特に共有地の扶養能力が限界に達してしまった場合は破滅的になる（Hardin, 1977; 竹内, 1989: 217-218）。現在，このような「共有地の悲劇化」がネット・情報環境で急速に進んでいるのである。現在，多くの人々は，自分たちが活動している情報生態系ないしネット・情報環境に対して強い責任感はもっていない。自分のことだけしか考えず，自分だけが何をしても無駄だと感じている。無責任と無力感が蔓延しているのである（本田, 1998などを参照）。ここでは，なぜそのような無責任と無力感が蔓延しているのかを考えてみることにする。

ネット・情報環境が持っている反倫理的行動への誘因のまず第一が，匿名性の高さである。匿名性の高さは，プライバシーの確保，広くいえば個人の自由を保障するために非常に重要な要件である。匿名性が確保されていることで，自由な発言ができるのである。しかし，自由に発言できるということは，デマや誹謗中傷など無責任な行動を許してしまう危険性をそもそもはらんでいる。プライバシーの概念があまりにも拡張されて，「自分に関する情報をすべてコントロールする権利」として理解されると，それは自由権の領域を超えて，逆に他の人々の自由を制約することになる（森村, 2001: 42）。現在，ネットでは，匿名性を高める技術の開発が急速に進んでいる。プライバシーの確保と匿名性の高さを保持するための技術の進歩は，たとえば政府機関が「強力で解読できない暗号製品が続々と発売され，広く使用されるようになっている。これは，犯罪に立ち向かい，テロ活動を防止し，国家の安全保障を守るわれわれの能力をそぐことになるだろう」

（Wired News, 1999.2.9）と懸念を表明するぐらい激しい。そのような技術は，犯罪をおかそうとする者や他人に迷惑をかけようとする者にとってはかっこうの隠れ蓑を提供し，犯人の識別を難しくさせ，捕捉も捕縛も難しくさせる。

第２がバーチャル性である。加害者は，被害者および被害の実状をリアルな形で知ることはできず，大きな被害が発生していても誰にも迷惑をかけていないと思ってしまう。他者の権利を侵害しても，被害対象物を特定したり損害額を見積もることが難しく，責任感が非常に希薄になる。情報そのものが盗まれているのを現実としてリアルに「見る」というのは難しい。リアルな窃盗行為であれば何かが目に見えてなくなる。しかし，情報は複製が可能な唯一の財であり，盗すまれても何かがなくなっているようには見えない。盗まれると情報の持つ価値そのものはなくなってしまうが，情報ないし記号の集合自体は依然として盗まれた者の手元に残る。ほとんどのハッカーやクラッカーは，他人のWebページに悪戯をすることは違法ではあっても破壊活動ではなく，大した被害もないと思っている。ネット上にはそのような活動を支援する「ハッカー・ツール」が多数提供されており，スキルのない者でもWebサイトを簡単にハッキングしたりウィルスを作ったりすることができる。そのような反社会的行為を支援するようなツールそのものの開発や公表そのものは現在のところ違法ではない。また，ハッカーたちの多くは，攻撃される企業に多大の被害が生じたとしても，そのようなセキュリティ・ホールを放置していたのは組織の責任であり，それをそのまま放置して利用者に不当な不利益を与えてしまうことのほうが問題であり，それを指摘できるツールを開発することは社会貢献にさえなると思っているのである（ZDNet, 1999.6.3）。

第３が，技術的参入障壁の低下である。コンピュータおよびネット技術の進歩は，それまでは考えられなかったようなさまざまな技術的可能性を作り出した。ネットが産業活動や生活に深く浸透するとともに，技術はより扱いやすいものに改良され，それらの技術を利用するだけであれば高度な専門的知識を要求されなくなった。技術的参入障壁は低下し，ネット・情報環境を混乱ないし破壊しようとする者と彼らを捕まえる側との技術格差はほとんど無くなってしまい，「ITは悪い奴らにえこひいきをしている」（ZDNet, 2001.8.21）とも言われるほどである。そして，そのような技術的な可能性の増大と参入障壁の低下は，専門職だけでなくそれらの技術を利用する一般の人々にも，反社会的行為への誘惑を与えている（Kizza, 2001: 70）。技術的参入障壁は低下し，ネット・情報環境を撹乱しようとする者たちがクラッキングをしたりウィルスを作ったりすることは本当に簡単かつ容易になったと言える。ネットに不正侵入したり，ウィルスを作ったりしようと思えば，ネット上にそのための技術情報やノウハウとともにそれを支援するさまざまなハッキング・ツールが公開・提供され，それらを使えばそれほど専門的な知識がなくても簡単に実行に移すことができるのである。技術的参入障壁が低くなったことが反社会的行為を助長していることについていえば，ネット・情報環境の破壊行為として非常に大きな問題であるサイバー・テロないしサイバー・テロリストに対する影響は特に大きい。サイバー・テロはテロリズムと呼ぶにはあまりにも容易に実行可能な行為であるが，それが生み出す結果ないし被害はネットに依存しきった社会にとっては甚大である。サイバー・テロの増加に技術的な参入障壁の低下が影響を与えていることについては，Vladimir （2000: 111）が次のように適切に表現している。「ネットを利用したサイバー・テロは，テロ実行者が生命を賭する行為ではない。テロリストとしての人間としての倫理を，決壊寸前に至らしめる情念の不在は，そのままこの行為を実行することへの容易さを直結する。サイバー・テロは技術的な問題を除けば，気軽なのだ。用意周到で手の込んだ悪戯とその手法において変わることがない。だから，冒険心あふ

れる子供がお小遣い目当てで，パソコンからいとも簡単に実行できる類のものである。その悪戯に毛の生えたような行為でさえ，ネットに依存した社会にとっては重大な結果を引き起こす」。

第４が，サンクション（倫理的自己拘束と外的規範による強制）の無力さである。ネットの世界は，「良心」という内的サンクション（倫理的自己拘束）も，物理的，政治的，道徳的，宗教的強制といった外的サンクション（外的規範による強制）も機能しにくい世界であり，外部的な強制が弱ければ倫理に反する行為を平然と犯してしまう「合理的利己主義者」が増えてしまいやすい世界である（越智, 2000: 206-207）。合理的利己主義者にはそもそも良心という内的サンクションは機能しない。外的なサンクションが有効に機能しているときには彼らも倫理的に振舞うが，そのような外的強制力が無力であると感じると倫理にもとる行為を平然としてしまう。ネットは，「非対面性」と「匿名性」を基本とし，相手を目の前にしなくてすむし，自己の固有名や社会的属性を隠すことも容易である。合理的利己主義者にとって，そのようなサンクションの働きにくい世界は非常に住み心地がいい。ネットのおかげで犯罪者は国境を越えられるようになったが，国家というものが前提とされている限り捜査当局には国境という限界が常につきまとう。しかし，犯罪者には国籍も国境も関係ない。そもそも，グローバルな広がりをもつネットを介して行われる犯罪に対して，従来の国家を前提としたサンクション枠組みのままで制御しようとするのは無理がある。

第５が，ハッカー・コミュニティにおける共同体意識とハッカー倫理の喪失である。ネット創生の頃のハッカーたちは，利用者集団の規模が限定されていたので，自らがネット・情報環境を創造するとともにそれを守っていく役割を担っているという「ハッカーの倫理」を多くの人々が共有し，それに反する行動に出たものには制裁を加えることで秩序を維持するという連帯的共同体を形成していた。しかし，利用者集団の規模が飛躍的に増大するとともに，多様な価値観を持った人々が参入し，ハッカー倫理を共有する共同体は少数派になってしまい，影響力を失ってしまいつつある。昨今のクラッカーやウィルスの製作者は，ネットの普及を加速した閲覧ソフト「モザイク」出現以前の「正義の騎士」としてのハッカーたちとは異なる倫理観をもった人々である。悪意ないし行き過ぎた悪戯心を持った人々も少なくない。このハッカー・コミュニティにおける共同体意識とハッカー倫理の喪失を加速しているのが，ハッキングの「資本主義化」である。ハッキングは金銭的対価を得られる手っ取り早い手段になっている。特に最近は，侵入が起きている原因は「そこに金があるからだ」とも言われるように，「利益至上主義」という新たな局面を迎え，その様相は急激に悪化しつつある（ZDNet, 2001.1.1）。ハッカーは，「正義の味方」だろうが「悪者」だろうが，ソフトウェア業界の中でもエリートの一群に属しており，その多くが大手のソフトウェア企業に勤務しているといわれる（ZDNet, 1999.6.3）。有名ソフトメーカーでさえ，優秀なエンジニアを確保することは難しいため，ハッカーを意図的に採用する場合も少なくない。セキュリティ上の欠陥を指摘すれば，どんな優れた履歴書を出すよりも，能力の高さを認めてもらえる傾向がある。企業としてもハッカーを雇わざるを得ないというのが実情である。そのように企業のなかにハッカーが自然に増えているなかで，個人ハッカーよりも脅威を増しているのが，組織的かつ日常的にクラッキングやウィルスの製作を行う，ホワイトカラー・ハッカーである（Wired News, 1999.4.19）。ホワイトカラーの犯罪者たちは，「名声が欲しいだけ」のハッカーよりも，もっと密かに，そして巧妙に犯罪を行なう。巧妙な攻撃者たちは，直接のターゲットではないコンピュータ・システムにまず不正侵入し，そこを足場に本当のターゲットに攻撃を行なう。その後，攻撃のベースとしたシステムの侵入記録を消

去して，自分たちが攻撃したことの痕跡を消し去るのである。

第６が，ハッカーを正義の戦士としてもてはやす，マスメディアの風潮である。ハッカーたちは，システム侵入にはコンピュータ・ネットワークのセキュリティ・ホールを明らかにする積極的役割があると主張する。欠陥を指摘するのは善意に基づくものであり，それにより罪もない多くの人々がこうむる社会的被害を防ぐことができるという。たしかにセキュリティ破りという行為は侵入された組織にとっては不正なものであるが，社会全体の利益から見れば推薦すらされるべきものであるというのである。マスメディアに取りあげられるハッカー像のほとんどは，ハリウッド映画に登場するように，邪悪な権力に抵抗する「正義の戦士」というクリーンなイメージである。クラッキングそのものも，そのイメージの延長で見られ，後ろめたさが消し去られている。理想なり目的が正当化されればどんな手段も許されると考える傾向が肯定されているのである。

最後が，ハッカーを隠れ蓑にした組織的な責任回避である。ネットは，市場と同じく多種多様な行為主体によって構成され，基本的に管理権限と責任があいまいである。現在のところ，誰がどこまで責任を負うか，責任の切り分けが十分に確立されていとは言いがたい。責任が不明確なため，問題が起きた際に当事者間で責任の擦り付けあいが起きることもまれではない。その端的な例がデータ漏洩である。ネットの普及や電子商取引の拡大に伴い，データ漏洩の危険性が確実に高まっている。データ漏洩のもっとも大きな要因は，データを管理する側が基本的な安全対策を講じていないことである（ZDNet, 2001.8.3）。攻撃にあった政府機関，企業，サービス・プロバイダーのほとんどは，ハッカーをスケープ・ゴートにして，自らのセキュリティ対策に問題があったことに対する責任を回避しようとする事例も少なくない。自らは十分なセキュリティ対策を施していたが，ハッカーが予想を超えるぐらい強力であったから防ぎきれなかったと弁護したりする。新聞やテレビなどのマスメディアを騒がせている「ネットにおける反社会的な，もしくは犯罪色の強い情報」は，Vladimir（2000: 43）が言うように，「ハッカー」の仕業とステレオタイプ化して短絡的に呼ぶことで，一般ユーザが抱くさまざまなネットに対する不安感を煽り，問題の現実的な解決を阻害している。

次に，ネット・情報環境で進みつつある「共有地の悲劇化」を阻止するために，われわれは何をなすべきかを論じる。

▶ 4　情報環境倫理的発想の必要性とネット・情報環境問題を倫理的に考える際の基本指針

――リバタリアニズムを基本とし，内的サンクションを優先し，外的サンクションは最小に――

これまでに述べてきたように，われわれの社会は高度で複雑なネットワークに強く依存しており，ネット・情報環境が破壊ないし混乱させられることはわれわれの社会にとって致命的である。そして，そのネット・情報環境はそもそも「共有地の悲劇化」を招きやすいものであり，このまま何もせず放置すれば環境そのものの崩壊を招きかねない。それでは，ネット・情報環境を混乱や破壊から守るためにわれわれは何をしなければならないであろうか。具体的に利用できる手段としては，技術，法律，そして倫理などが挙げられるであろう。ここでは，目的そのものを取り扱う倫理が，技術と法律という手段に優先されるべきであることを論じる。

まず，ネット・情報環境問題に対して技術がすべて答えを提供することができるのであろうか。たしかに技術的に解決できる問題は少なくない。しかし，たとえば，どんな技術を用いて安全対策を強化したとしても，安全性を100％保証することは誰にもできな

い。基本的に環境問題を技術的な方法だけで解決することはできない（蔵田, 1998を参照）。それから，技術にはもうひとつ大きな落とし穴がある。技術は便利になればなるほどそれに依存せざるを得なくなる。技術や他者（特に政府など）をあまりにも頼りにすると，自分たちが抱えている問題を認識しそれを解決する意欲は自然に減退していくだけでなく，問題に対処するためのノウハウもまったく蓄積されないため，実際に問題が発生すると自分たちでは何も解決できないというような状況に陥ってしまいやすくなる。技術依存症および他者依存症に陥らないようにするためには，常日頃から問題を自分の問題として考えたり，技術や他者の存在がない状態を仮定した場合に自分が具体的にどう対応すればいいかを考えることが不可欠であろう。利用する者それぞれがネット・情報環境に対する責任を自覚し，自ら積極的に行動するが求められている。

では，法律を整備すれば問題が解決するのであろうか。ネット・情報環境問題に対しては法律による解決にも限界がある。法律はその社会で是認されている倫理的価値観を体現したものであり，日々新たな問題が発生しているネット・情報環境問題については十分に整備されているという段階には達していない。倫理は法律を支える基盤であり，倫理的な基盤が存在しない限り法律の執行力は弱まる。法律は基本的に技術の進歩とそれに対する倫理的価値観の変化がある程度確定された段階で整備されるものであり，法制度と現実の問題には時間的なずれが生じることは致しかたない。ネットに関連して発生しているさまざまな問題は，これまでの社会的な枠組みに大きな転換を迫るものであり，法律がそれらの問題にある程度対応できるようになるためにはかなりの時間が必要である。加えて，ネットに関連して発生しているさまざまな問題を法律だけで解決することには，もうひとつ大きな問題がある。国境という明確な適用範囲を前提として整備された近代法制度をそのまま，地理的境界線がそもそも存在しないネットに適用することには無理がある。たとえばある国が特定の反国家的思想集団のネットでの活動を排除しようとしても，国内だけでの活動であればそれなりに規制することは可能であるが，国外での活動に対してはほとんど無力である。

技術や法律はそもそも，実現したい「目的」が設定されていることを前提にして，その目的を実現する最適な解を探そうとするものである。ネット・情報環境問題についても，環境はどうあるべきか，それに対してわれわれはどう関与するべきかという，目的に対する価値観の一致があれば，技術や法律はそれなりに適切な回答を出すことができよう。しかし，目的を規定する価値観そのものは多様かつ相対的である。問題が各論になればなるほど多様化の傾向は強まり，目的について意見の一致を見ることは容易ではない。倫理は，共同生活を維持するために自発的に守られる規則であり（加藤, 1996: 79），目的に関する議論を整理・調整し，目的に関する合意および手段の選択に対する指針を提供しようとするものである。技術的および法律的な選択が本質的に有効になるためには，目的そのものについて一定の合意と手段選択のための指針がそれなりに作り上げられなければならない。問題の解決を急いで手段の議論に集中しすぎると，誤った方向に社会を導いてしまう。重要なのはわれわれはどのような環境に住みたいかであって，手近にある手段の問題にすりかえてはならない。

それから，技術も法律も，Winner（2000: 26-31）が述べているように，人間の活動と意味を再構成するように作用する強い力をもつものであり，いったん導入されると「公」の合意となり，その存在そのものを疑ったり，否定することは非常に難しいということを忘れてはならない。実際に導入の効果が出るのは後のことであり，その効果を導入の時点で正確に評価することは非常に難しい。

また，技術や法律が必要とされるのは問題が社会的に非常に大きくなったときであり，

問題が大きくなると正確にそれを理解することは難しく，反応は過剰な方向に流れてしまうやすいことも忘れてはならない。ネット・情報環境を守らなければならないと誰もが思っている。しかし，それは大変な作業であり，ほとんどの人は進んで最優先課題に取りあげたいとは思わない。何か問題が起こり非常に大きな影響が生じるまでは，ほとんど何の対策もとられないというのが実状である。その反動で，いったん事件が起きて問題になると，ネット・情報環境を守るためであれば，たとえば強力な法律を作り，徹底的な監視や盗聴までも許容するというように，過剰に反応してしまいやすい。そのように，いったん高度な監視を許容する技術や法制度が導入されると，それを撤去ないし廃止することはかなり難しいであろう。最も基本的な権利のひとつである自由を守るという名のもとに自由の基盤を掘り崩すようなことがあってはならない。

また，技術や法律は，今述べたように一度導入してしまうと本質的な改変は難しいということに関連するが，「最初に選んだものに大きく制約されてしまう」ということを忘れてはならない。最初に選んだ技術や法律の内容そのものがその後の環境のあり方に強く影響するのである。それゆえ，技術や法律の導入にあたっては，あくまでも慎重に時間をかけた論議をできるだけ多くの場で行い，問題の本質がそれぞれの個人に理解される段階まで待つべきであろう。最初の選択の段階で最も議論しなければならないのは，何度も述べているが「目的」と「価値観」に関する倫理問題である。

この論文の最初にも述べたが，これまで情報倫理学では環境そのもの破壊や混乱という問題を本格的には扱ってこなかったが，ネット・情報環境問題が深刻化している現在，われわれはそのような問題にどのようにアプローチすべきかという「準拠枠」としての情報環境倫理を提示することが求められている。次では，応用倫理問題としての情報環境倫理を扱ううえでの基本的注意事項について少し述べる。

まず第１は，避けることができない価値観や権利の対立を前提にしながら，できる限り建設的な価値観の妥協を追及するのが，倫理，特に応用ないし実践倫理の課題であるということを理解することである。倫理問題とは，基本的に，拮抗する価値観と権利の対立をどう調整するか，いかにうまく調和させるかという問題である。価値観は人それぞれ異なるだけでなく，それぞれが有する価値観でさえ，状況に大きく左右されるし，時間とともに変化する。価値観も権利も相対的であり，他者との関係性において規定されるものである。人はそれぞれ自らの有する権利を確保するためにさまざまな努力を重ねている。人が存在する限り，価値観と価値観，権利と権利が相互に対立することは避けられない。権利はただその主張を繰り返し続けたとしても自然に認められるわけではなく，権利を主張するものの間で一定の合意を勝ち取らないと何も得られず，紛争状態が維持されるだけになってしまう。自分の主張する権利を相手方に認めてもらうためには自らの主張もある程度譲歩せざるを得ない。主張する権利の内容は人それぞれ異なるし，主張する権利の優先順位も同じではない。権利を認められるためには，主張する当事者がそれぞれの権利の限界を認めて，相互の調整をはかることが要求される。加藤（1994: 28）が述べているように，価値観が違って，当事者に通約可能なルールが何もないという主張には何の意味もなく，むしろ違った価値観の持ち主が共生するための作法こそが「正義」なのである。

第２が，それにも関連するが，応用倫理問題を考えるうえで重要なことは「不一致の中で一致を求める」ことであることを肝に銘じなければならないということである。倫理や道徳，そして価値観の不一致は，危機や混乱ではなく自然なことである。重要なのは，平石（2001）が強調するように，不一致の中で社会的問題の解決を求め，何かを社

会的に決めて実行していくこと，つまり不一致の中で一致（よりよい妥協）を求めていく姿勢である。価値観に違いがあることを認め，誰の価値観が正しいか間違っているかは棚上げにして，お互いがこれなら合意できることを決めることが大事である。結論で合意ができれば十分であって，結論を導くための理由づけに違いがあっても，それは許容すべきである。多様な価値観を有する人々や組織が社会を円滑に機能させていくためには，そのような合意できる小さな結論を積み重ねていく以外にとるべき道はないであろう。大きな結論や理想的な合意を目指して失敗するよりも，小さな合意ではあっても，無いよりはましである。個々の具体的事例に限定したところで合意を求めるべきであろう。

第３に，合意に当たっては性急な答えを求めてはならないということに加えて，一度作られた合意も絶対的なものではなく常に改善に向けて議論を継続すべきであるということである。たしかに合意を形成するのは重要ではあるが，それが行き過ぎ，合意を形成することが目標となり，内容そのものが疎かになると逆に問題である。合意形成への志向が極端に強くなると，多数意見に目を向けやすく，少数意見を軽視するようになってしまいやすい。また，社会変動の真っ只中にいる人々にとって，Winner（2000: 168）が言うように，自分自身の活動の歴史的意義を熟考する時間はほとんどない。合意形成のための議論に十分な時間をとり，そのやり取りを通じて政策の再検討や修正を繰り返しながら合意に反映させるというような，着実な積み重ねが重要である。時間的な制限を含め使える資源には自ずと限界があるとともに，問題そのものが時間の経過によって変動していく，応用倫理問題にあっては，完璧な答えが得られることはほとんどない。Whitbeck（2000: xv）が強調するように，何が重要かを認識する智恵と想像力をもって，分析と総合を繰り返すしかない。それに加えて，ひとたび合意ができてもそれを絶対視することなく，新たな合意を継続的に積み重ねていける信頼関係を築き上げていく必要がある。どのような合意や解決策も完全なものはなく，改善の余地がなくなることはない。継続的な改善こそが求められている（Whitbeck, 2000: 67-93）。

第４が，アリストテレスが強調した「中庸」の精神が重要であるということである（Urmson, 1988）。中庸とは，対立する価値があった場合に，その中間を採れということではなく，どちらか一方の価値に過度に偏らないということである。性急な解決を求めすぎたり，一部の人々にしか受け入れられないような極端な解決を他者に押し付けるようなことがあってはならない。倫理問題においては対立する価値の間の微妙なバランスを保つことこそが実践的な解決に近づく道である。

最後に述べておかなければならないことは，倫理問題，特に応用倫理問題は，議論そのものも重要であるが，実践はそれ以上に重要であるということである。クラッキング，ウィルス，サイバー・テロなどネット・情報環境で起きている反社会的行為は，リアルな世界と同じく，排除することは不可能である。重要なことは，そのような反社会的行為をどこまで許容するのか，そしてその許容できる水準に抑えるためには具体的に何をどうすればいいかということを考え，それらを実際に実行に移すことである。実践知とは，Norman（2001: 66-67）が強調するように，普遍的なものではなく個別的なものに関わるもので，「今ここで何をすべきか」を知ることである。それは，一般的な規則や抽象的な原理原則に訴えることではないし，論理的議論や知的能力の問題でもない。ある個別の状況で，「それが私のすべきことだ」と知ることにある。実践知は，理論的原理を学ぶことによってではなく，道徳的訓練によって，すなわち道徳面で洗練された共同体の中で適切に育てられることによって，獲得されるものである。倫理，特に応用倫理が実践知であるということで，もうひとつ強調しておかなければならないことは，倫理に関

して議論するときにわれわれが実際に行っていることは，価値を発見することではなく，価値を創造することであるということである（Norman, 2001: 352）。倫理問題は，Whitbeck（2000: 80）が述べているように，選択問題のように存在するいくつかの答えの中からどれかひとつを選ぶものではなく，問題に直面したわれわれ自身が「自由記述」形式で答えを模索，創造していくものであるということである。

続いてここでは，情報環境倫理としてどのようなスタンスを採るのが望ましいかを論じる。情報環境倫理のスタンスを決定する重要な論点は，目的（対象）と，手段とりわけ行為主体についてどう考えるか（人間観）であろう。第１が，われわれが「何を」守るべきかということである。具体的には，守るべき対象であるネット・情報環境はどのような特性をもっていて，それにふさわしいアプローチとはどのようなものであるかということである。第２が，「誰」がどう関わっていくべきかということである。そこでは，行為主体であるわれわれはどのような特性をもっていて，それにふさわしいアプローチとはどのようなものかが具体的に問題となる。そのような問題を勘案すると，結論としては，情報環境倫理が依拠すべきスタンスは，他者に危害を加えない限り，個人の自由を最大限に尊重する「リバタリアニズム」であると考える（森村, 2001: 198-201）。

まず，守るべき対象であるネット・情報環境はどのような特性をもっていて，それにふさわしいアプローチとはどのようなものであるかという問題について考えてみよう。ネット・情報環境と自然環境のもっとも大きな違いは，冒頭にも述べたがネット・情報環境はあくまでもそれを利用する者が創りあげていく人工物であるということである。自然環境については，自然そのものが環境を利用する者の行動を強く規定するので，行為者の自由意志は部分的にしか反映されない。これに対して，人工物であるネット・情報環境は，それを利用する人々の自由意志と，その発現として連続的になされる政策の選択と実行に依存している。ネット・情報環境は，たしかに事前に選択・実行された政策に拘束されるが，利用する者がかなり自由に改変していくことが可能である。適切な政策が選択・実行され続ければ，環境そのものを守り続けていくことは自然環境よりも容易である。しかし，ネット・情報環境は自然環境のような自己保全機能をもっていないので，選択・実行される政策が適切なものかどうかに環境そのものの存在がかかっている。ネット・情報環境は，必要に応じて一つ一つ自己保全機能を意図的に組み込んでいかない限り，環境を維持することができない。不適切な政策が選択・実行されると環境そのものが壊れてしまうので，ネット・情報環境については自然環境に対する政策にもまして慎重な政策の選択と実行が望まれる。ネット・情報環境では，どのように技術や制度が進んでも，それらを生成する個々人が環境を維持ないし創造するための責務を自覚し，環境を破壊しようとする動きなどに自ら立ち向かう「自助自立の精神」が強く求められる。行為主体の主体的な取り組みしか，環境を存在せしめる基盤はないのである。リバタリアンが強調するのは，基本的に「自分が自ら何かを行わない限り誰も助けてくれない」ということである。そういう自助自立の精神をもった個体が自律的に活動することで，互いに尊重しあい，社会という協同活動が成り立つとするのである。ネット・情報環境を自らが創造していくという精神が求められている。

第２の行為主体であるわれわれはどのような特性をもっていて，それにふさわしいアプローチとはどのようなものかという問題ついては，先にも述べたが，基本的に人は合理的利己主義者であり，それにふさわしいサンクションを課すべきであると考える。聖人君子のような利他的な行動を自分に強いることはできる。しかし，他人に誰か他の人々のために自分を投げ出す利他的行動を期待することはできないし，またそのような

行動を他人に強制すべきでもない。管理権限も責任も複雑かつ不明瞭で「共有地の悲劇化」に向かいやすいネット・情報環境では利他的な行動を期待することはできず，そのような行動を前提に選択・実行される政策は結局「絵に描いた餅」にしかならない（加藤, 1997: 216）。では，ネット・情報環境の住人は完全に利己的な行動だけしか採らないかといえば，そうではない。他者との協同を強く欲しているネット・情報環境の住民たちは，そのような協同を実現するためには利己的な行動を慎まなければならないことは理解している。しかし，そこに適切な内的および外的サンクションが存在しないために，利己的な行動を慎まないだけである。サンクションにもいろいろあるが，社会ないし環境の秩序を維持するためには何がしかのサンクションが不可欠である。

最低限の秩序を維持するためには，内的サンクションと外的サンクションを適切に設定して，それらをうまく組み合わせて使う必要がある。内的サンクションは外的サンクションの基盤であり，その指針となるものである。内的サンクションは個々人に内在化されて個々の行為そのものを律するものであるが，内的サンクションが設定する目標以上の行為はほとんど期待できない。環境を破壊するための行動を阻止するように個々人を動機づけるためには，現実には実現しないけれども「理想とすべき目標」を掲げる必要があるであろう。情報倫理は，「何々をしない」という反社会的行為を抑制するように仕向けるという意味で「消極的」な倫理であるという向きもある。しかし，そうではない。われわれが内的サンクションとして設定すべきなのは，「このような行為をすべき」というようなことを説く「徳」の倫理である。

内的サンクションについては理想主義的なアプローチが必要であるのに対して，外的サンクションについては，われわれのほとんどは合理的利己主義者であるという現実主義の立場に立ち，ほとんどの人が許容できる最低限のもので満足せざるを得ないし，それがもっとも適切なものである。この外的サンクションの適正水準をどこに置くべきかという問題を考えるうえで役に立つのが，市場メカニズムのそれであろう。ネット・情報環境と同じ人工構成物である「市場」メカニズムでも，その環境を混乱ないし破壊する行為が発生する。しかし，環境そのものを破壊しないのであれば，そのような反社会的行為はかなりの程度まで許容せざるを得ない。環境そのものを破壊しない程度の行為ならば許容するレベル，すなわち最低限の秩序が維持できる程度のサンクションがあれば十分であり，それ以上を期待することは難しい。すなわち，合理的利己主義者たちを反社会的行為にいざなわない程度のサンクションにすべきである。また，そのような最低限のサンクションの設定こそが環境全体の利得を最大にするものであり，行き過ぎたサンクションは逆に環境全体の利得を引き下げることになってしまう。環境を維持するために必要な最低限のサンクション以上のものを課すためには，結局は全体主義（ファシズム）に近い強制が必要になるであろう。市場メカニズムは，個人の自由を最大限に保障しながら社会共同生活を成り立たしめる術を，その環境を利用してきた人々がその叡智を出し合い，長い時間をかけて創りあげられてきた。ネット・情報環境についても，市場メカニズムの形成発展と同じく，環境利用者が長い時間をかけてじっくりと創りあげていくしかないのである。

▶ 5　内的サンクションとして必要な「ハッカー精神」の復活
――自助自立の精神と社会的告発者としてのノブレス・オブリージュ――

内的サンクションの具体的な中身を検討するためには，ネット・情報環境の創生者たちがもっていた「ハッカー精神」といわれる理想像を見直す必要があるであろう。創生者た

ちは，他人に危害を加えない限り個人の自由を最大限に尊重し，自分たちの環境は自分たちが創りあげていくというリバタリアンたちが目指している自助自立の精神をもつとともに，社会全体の利益に適うならば反社会的行為でもあえて実行するという高貴な社会的責任（ノブレス・オブリージュ）を担おうとしていた。現在，そのような理想像としてのハッカー精神は，先にも述べたが，資本主義によって骨抜きにされようとしているのが実状であろう。「本質的に価値相対化と個人主義を際限なく促しつづける土壌」（Vladimir, 2000: 205）であるネット・情報環境であるからこそ，内的サンクションとしてハッカーの精神のような高い理想像を掲げるべきなのではないかと考える。

ハッカーとはもともとは，「創造的行為とその結果がインターネットという世界に即時的に反映し，世界的に使われ，プログラムを開発しようとする若者たちの心を躍らせる楽しい行為」（Vladimir, 2000: 20）を追求する人々のことであった。そういう技術的楽しみを追求することを目的にしていた人々の中から，「ネット・情報環境は自らが創造していくしかないし，誰も助けにはならない」と自らの社会的な責任の大きさを感じる人も少なからず出てくるようになっていった。そのようなハッカーたちは，ネット・情報環境に自生するアナーキストとして，個々人の自由を最大限に尊重しながら，不当な支配や権力の横暴には徹底的に抵抗するリバタリアン文化を徐々に創りあげていったのである。その創生期のハッカーたちは，悪意を持ったクラッカーと自分たちを区別するために，自らを「倫理的ハッカー（Ethical Hacker）」と呼び，高貴な倫理観を失わずに好奇心を満足させる「ノブレス・オブリージュ」の体現者と位置づけた。

しかし，そのような高貴な倫理観をもった人々は環境利用者の全体から見れば限られた一部であった。そして，すでに環境ができあがった後にその環境に入ってきた環境消費者が増えるにつれ，ハッカーの精神を持った人々は少数派となった。環境消費者は，自らが環境を創りあげようというような責任感はない。また，自分たちが何をしようとその環境を変えることは不可能であり，その環境をうまく使い，いかにそこからたくさんのものを収奪できるかということしか考えなくなっている。

ハッキングは，結果的には社会的告発として賞賛すべき成果をもたらす場合もある。しかし，その過程で行われる行為そのものは特にハッキングされる当事者にとっては自らの権利が侵害されるわけであり犯罪的なものである。現在，ハッカーの多くは，社会の利益に供するためにハッキングをしているのではなく，あくまでも個人的な欲望の追求をしている。自分たちが行ったハッキング行為の結果がどうなるかについてはまったく関心がないし，自分たちには大した責任があるわけではないと考えている。

個々人の自由を最大限に尊重するリバタリアニズムの立場の基本にあるのは，「他人に危害を加えない限り，個々人は何をしてもいい」ということである。ネット社会の構成主体であるわれわれは，「他者に危害を加えない」というもっとも基本的な責任から逃れることはできない。ネット・情報環境では，先にも述べたが，環境全体としてみれば大きな被害を与えているにも拘らず，被害そのものは分散化され，一人一人にすれば大した被害として意識されないだけでなく，被害そのものの現実感が薄いので，他人に危害を加えていると思わない場合が少なくない。しかし，被害が明確に意識されていないにしても，後で述べる社会的告発者のように目的が正当化されるような条件が満たされない限り，そのように社会的被害が大きい反社会的な行為に対しては厳格な罰（外的サンクション）が適用されてしかるべきである。他人に迷惑をかけなければ満たされない好奇心は罰せられて当然である。特に他者の権利を「不当に」侵害しないという社会的責任は，内的サンクションの中でも最優先に取りあげられるべきものであろう。

内的サンクションとして，自助自立の精神とともに，ネット・情報環境の住民に涵養しなければならないのが，「住みやすい環境を自らが創造していく」という積極的な社会貢献の精神であろう。住みやすい環境とは何かが問題になる。住みやすい環境とは，多種多様な価値観を有する人々がそれなりに共生できる環境である。共生が成り立つためには，谷本（2001）も強調するように，互いが他者の価値観に「寛容」になり，権利が不当に侵害されない限り個々人の自由を最大限に尊重することが必要であろう。このような関係こそが，創生期のハッカーたちを含めリバタリアンが目指してきたものである。環境の汚染や破壊の被害は，公害問題で明らかになったように（丸山, 1998: 27），平等には起こらない。ネット・情報環境においても被害は，生物的な意味および社会的な意味での弱者にまず起こり，そこに集中する。ハッカーのように優れた能力を有する者には，そのような社会的弱者に不当な被害が及ばないようにするノブレス・オブリージュがあるであろう。

住みやすい環境を創るなかでハッカーが担ってきたひとつの役割が，ネット・情報環境に存在する社会的な不正や欠陥を告発するということである。たとえば，セキュリティ・ホールは秘密にしておくべきものか，それとも万人に知らせるべきものなのか。1999年8月に「ハッカーズ・ユナイト」と呼ばれるハッカー集団が，マイクロソフトの「ホットメール」のセキュリティ・ホールを公にした（Wired News, 1999.8.30）。そのハッカー集団は，ハッキングは破壊のためにやったのではなく，市場で独占的な地位にある企業が提供しているソフトに，5000万前後のプライベートな電子メール・アカウントが，誰からでも覗ける状態にあったというようなセキュリティ上の「ずさんさ」があると指摘したかったからであると主張する。このようなハッカーによる社会的告発は増えている。

たしかに社会的告発は，倫理的に正当な理由がある限り進んで行われるべき行為であり，住みやすいネット・情報環境を構築するために必要なものである。ネット・情報環境で個人と組織がもっている情報の質と量，そしてそれらの情報を創造ないし加工する能力には格段の差がある（加藤, 1994: 139-140）。特に大企業や政府機関が組織的に自らの不正や欠陥を隠蔽することは比較的容易である。組織や集団に強く帰属してしまうと，属する組織や集団を守るために，倫理的に正しいことができなくなってしまうことが少なくない。不正や欠陥のような反社会的問題の組織的隠蔽を暴くためには基本的に内部告発が必要不可欠である。ハッカーの中には，自分たちが持っている技術的能力を生かして，そのような不正を暴こうとする者も少なくないこともたしかである。

告発は良心に基づく場合と復讐や仕返しに基づく場合があるので，慎重に対応する必要がある。しかし，社会的な告発をしようとする者は自らの身の危険を省みず行為をするわけであり，社会的に保護する仕組みが制度化されていないと守りきれない（Kizza, 2001: 74）。告発者が誰かということが特定されると危険をともなうので，匿名性の確保は告発にとって非常に重要な条件である。これまでも，匿名性を確保するために，ありとあらゆる手段が使われてきた。告発しようとする者は，匿名性が確保できるかどうか事前に十分に注意する必要がある。また，告発をしようとする者は，他者が納得できる証拠を収集するとともに，揉み消しなどの可能性がないのであれば告発する前にまず内部で解決を試みるとともに，告発する場合は異常な社会的混乱を引き起こさないような時期や発表手段に十分な注意が必要である。このように，必要な場合には社会的告発を進んで行うことを奨励する内的サンクションを課すとともに，それを支援する社会的制度の確立が必要である。

その一方で，逆に自分たちの反社会的行為を正当化するために，大義名分をつけるハッカーも少なからずいる。社会的告発はたしかに住みやすいネット・情報環境を構築するために必要なものであるが，他者の権利を侵害することは避けられないので，無秩序に行われるべきではない。目的が正当なものであればどのような手段を使ってもよいというわけ

ではない。社会的告発はたしかに必要なものではあるが，それが行き過ぎた自由主義や自己満足の道具に成り下がってはいけないのである。たとえば人権侵害に対して抗議するというような，大義名分を立てればなんでもありというような状況を作り出してはいけない。そこには，内的サンクションを設けることが不可欠である。特に社会的告発は人々が倫理的にディレンマに陥る問題であり，そのような問題に対しては具体的な行為指針（ガイドライン）を，環境を利用する人々が議論し，自ら設定することが重要である。

具体的に準拠すべき行動指針になるのは，何をどう報道すべきかというジャーナリストの職業倫理や企業倫理学で提唱されている内部告発が倫理的に正当化される条件，すなわち自分の利益のためではなく他者の利益のための緊急避難であるかどうかであろう（加藤, 1996: 33; DeGeorge, 1995: 第10章を参照）。具体的には，①社会ないし公衆に対して深刻かつ相当な被害を及ぼす明白かつ現在の危機が存在すること，②被害を及ぼすということについて合理的で公平な第三者を確信させるだけの証拠を入手する最大限の努力を行うこと，③極力関係当事者で内部的な解決を試みることである。気まぐれで誤った告発は，それ自体が危険である。告発する前に，その問題のすべての側面について徹底的に事前評価しなければならない。曖昧な状況を他者に報告する場合，Whitbeck（2000: 80）が強調するように，事実を自分でつかんでいるとおりに明確に述べ，自分の解釈を最小限に抑えて伝えるべきである。また，特にリスクと責任に対する評価については，Kizza（2001: 32）も言うように，信頼に足るものでなければならないので，他の専門家からの助言を求めることが不可欠である。

最後に内的サンクションを涵養するうえで重要なことは，ハッカーを日陰者にもスターにしてもいけないということである。ハッカーという単純なラベルを貼って最初から排除しようとするのではなく，その活動を自然なものとして社会的に認め，活動を地下に潜らせてはならない。ハッカーといっても多様な人々がいるわけであり，ひとくくりにして「悪人」として扱ってはならない。多くのハッカーたちがその才能のはけ口を求めており，建設的な「はけ口」を求めているハッカーも少なくない。最初から悪意をもって技術を利用しようとする者に対しては，犯罪として外的サンクション（厳罰）を適用するのが妥当である。しかし，建設的なはけ口を求めているようなハッカーたちを増やし，そのような人々を善用するというのが内的サンクションとして必要であろう。Def Con[2]のようなハッカーの自主的な研鑽活動は取り締まるのではなく，積極的に支援すべきである。ハッカーの活動に関する情報が公開されることで反社会的行為や反倫理的行為を容易に発見することができるだけでなく，ハッカー・コミュニティが自らの社会的責務を認識することができるからである。

ハッカーを，日陰者扱いしないのと同様に，スターにしてもいけない。メディアではハッカーを正義の騎士と描くことが少なくないが，そのように描くことで反社会的な行為を助長してしまうことは否めない。われわれに求められているのはハッカーという言葉でイメージを作り上げることではなく，具体的にどのような行為がどのような条件なら許されるかを自分たちで決め，それを実行するように仕向ける内的サンクションの明確化であろう。

脚注

2．ハッカー，クラッカー，セキュリティー専門家，連邦政府の捜査官，メディアなどが一堂に会するセキュリティ関連の一大イベントである。

▶ 6　外的サンクションの担い手として期待される政府による関与とその限界

ここでは，外的サンクションの担い手である政府はどのような役割を担うべきか，そのような関与に対してわれわれはどのように向き合うべきかを論じる。外的サンクションを本格的に議論する必要があるのは，サイバー・テロやサイバー戦争のような環境そのものを破壊してしまう危険性をはらんだ行為であろう。その危険性は急激に増大している。テロリストたちはすでに最新のサイバー・テロやサイバー戦争の技術に精通しており，現実の破壊活動よりも容易なうえに影響の大きい，ネットを利用した破壊活動を積極的に行うようになってきている。確固とした強力な行動をとらなければ，テロリスト，犯罪者，敵対する体制が命綱ともいえるシステムを侵略し，混乱させる危険がある（Wired News, 1998.5.22）。そのような環境そのものを混乱ないし破壊する反社会的行為に対しては，内的サンクションだけでは不十分であり，外的サンクションが必要不可欠である（森村, 2001: 91-92）。

しかし，外的サンクションがあまりにも行き過ぎてしまうことは逆に問題である。不必要な外的サンクションは，それが防止しようとする害悪よりもいっそう大きな害悪をもたらす（加藤, 1997: 184）。外的サンクションはリバタリアンとしてのわれわれが住みやすい環境を実現するに足りる程度のものでなければならない（加藤, 1997: 58-60）。その場合，権力が集中しやすい政府によるサンクションよりも，個々人ないし民間による自己規制を常に優先するということが重要である。共有地であるネット・情報環境を混乱や破壊から守っていくためにはその環境を利用していく者それぞれが個人的な責任を果たすとともに，環境そのものに対する責任を果たすように他者の行動を監視し，行き過ぎた行動を他者がとる場合自ら阻止する努力を行わなければならない。それぞれ異なった利害を持つ人々が共存できるのは，政府や国家によるよりも，人々の自発的な相互行為によるところが大きい（森村, 2001: 87-110）。秩序は，政府や国家によって上から与えられ守られるというよりも，自由な個々人の行動によって下から実現されるべきものである。権利侵害に至らないインフォーマルな社会的制裁があるからこそ，政府が強制的に介入しなくても個人の規律や社会の秩序が保たれるのである。自主的な監視活動こそがまず第一に重要なものである。

環境全体に対する脅威を追跡するためには，潤沢な資金のほか，きわめて多様な視点を持ち，高度な技術を備えた，強固な組織が必要である。外的サンクションの担い手として政府に期待されている役割は大きくなる一方である。しかし，政府によるサンクションは何もしなければ次第に増強されていくものであり，常にその権限が不必要に拡大していないかどうかを監視する必要がある。犯罪との果てしない戦いを続けている政府にとって，犯罪活動やスパイ活動との関係が疑われる情報のやり取りを自らのコントロール下に置くことができればいうことはない。ネットの場合，正当な利用者を識別するために多くのプライバシー情報が必要であり，ほとんどのサーバはすべてのアクセスについてそれらのプライバシー情報を記録として残している。サーバを管理するインターネット・サービス・プロバイダー（ISP）に情報を収集するための機器を設置することができれば，政府は捜査活動や諜報活動をより容易に行うことができる。そのために導入されたシステムで有名なのがたとえばFBIが導入した「カーニボー」である。政府は，「社会は自由と安全を秤にかけなければならない。まったく監視をしないというのも結構なことだ，もし誰もが法を守るなら。ところがそうではない」（Wired News, 1999.4.7）

と，安全のために自由はそれなりに制限されるべきであると監視の必要性を強調する。また，それまでプライバシー擁護派であった人々も，ニューヨークとワシントンDCで起きた無差別同時多発テロ以降，サイバー・テロと正面から向き合うためには政府が本腰を上げる必要があり，安全を守るためであればプライバシーが制限されても仕方ないと考えるようになってきている。

安全のためにはそのような政府の個人ないし民間の活動に対する積極的関与も甘受するという傾向を受けて，多くの政府が程度の差こそあれネットの検閲・監視手段を導入しようとしている[3]。政府が検閲を導入しようとしている理由は，テロリズムだけでなく，社会的，政治的，経済的，文化的なものなど多様である。ネットの検閲は実際に実行しようとすると非常に難しく費用のかかるものであり，これまで多くの政府や検閲機関が導入しようとしたが，ネットがあまりにも急激に成長したためにほとんど成功していない（Kizza, 2001: 253）。政府ないし検閲機関が急激に成長するネットでの犯罪行為に対処するには，システムを高度化するだけでなく，大量の検閲・監視官を継続的に雇用し続けなければならず，莫大な費用がかかってしまうのである。

われわれは，「権力は腐敗する。絶対権力は絶対的に腐敗する」（森村, 2001: 104-105）ということを肝に銘じなければならない。自分たちが権限を委譲した政府ないし国家が腐敗・暴走することを防ぐためには，政府とは何か，政府の任務とは何かという基本的な問題について継続的な問いかけが必要である。国家や政府は諸個人の基本的権利を保護するといった道具的役割しか持たない。それ以上の価値を認めることは個人の自由だが，それを他人にまで強いるのは不当な介入である。政府の干渉が正当化されるのは，加藤（1994: 10）が主張するように，「他者危害」の可能性がある場合に限るとすべきであろう。そのようなリバタリアンの立場に立ち戻り，それ以上の権限の拡大がないかどうかを常に監視する必要がある。

それに加えて，個々人の自由と権利の再確認し，それを実行あるものとするための法律の制定が不可欠である。さらに，権限の不要な拡大を防ぐためには，対抗権力として，個々人の自由と権利を保障するための独立機関を設置することも考えなければならないであろう。Hayek（1992: 59）が強調するように，現代の分業社会が複雑であればあるだけ，競争こそが，唯一，調整を適切に実現する手段であり，特定の機関に権限を集中するべきではない。

では，もっとも外的サンクションの担い手として絶大な権限を委託されている政府の関与は，具体的にどこまで，そしてどのような条件なら許容されるであろうか。問題は，社会の安全と個人の自由をどううまく天秤にかけるかである。たしかに個人の自由を確保するためには，プライバシーを保護するとともに，匿名性を高めることは必要である。表現の自由および「自己に対するアクセス権を自ら制御する権利」であるプライバシーは，絶対不可侵の権利ではないが，個人の自由を守るために必要不可欠な基本的権利で

脚注

3．政府は，関与の度合いに差はあるが，ネット利用に関するさまざまな政策を実行に移し始め，とりわけ社会問題の増加をくい止めるために検閲や監視を強化する政策の立案と実施に積極的に取り組んでいる。具体的に実行に移されているのは次のような手段である（Kizza, 2001: 256-258）。

①ネット利用者として「やってよいこと」と「やってはならないこと」のガイドラインを明示する。
②ユーザ・グループによる自己検閲の促進する。
③コンテンツを格付ける。
④不適切と思われるコンテンツを選別（フィルタリング）する。
⑤国そのものがインターネット接続サービスを提供し，コンテンツを規制する。
⑥不適切と思われるコンテンツが流れた場合，自動的に遮断プログラムを開発・導入する。
⑦通信品位法など子供のような社会的弱者を保護するための法律を制定する。

ある（水谷, 2000）。匿名性の高さは，それらの権利を確保するためにはある程度認められなければならないのである。しかし，そのような十分なプライバシー保護とか匿名性の高さは，普通の人々よりも，犯罪者の方に有利に働き，反社会的行為を誘発するものでもある。現実世界とサイバー・スペースでは匿名性の高さに大きな差がある。サイバー・スペースではなろうと思えば自分がなりたい者になることが容易である。自分で正体を明かそうとしない限り，隠れたままでい続けることも難しくはない。テロ事件を受けて，われわれの多くが，プライバシーの有難みは，それを享受するための十分に安全な社会があってこそ，味わえると思うようになっている（ZDNet, 2001.9.13）。

今後われわれがネット・情報環境を混乱や破壊から守るために外的サンクションとして政府の関与をどこまで，そしてどのような条件で許容すべきかという問題を考えるうえで重要なのは，「極端にはしらない」ようにすることである。われわれはテロなどネット・情報環境そのものの破壊という脅威を前にして，長い年月をかけて勝ち取られてきた「自由」を放棄する誘惑に負けてはならない。そもそもネット技術は，利用者の活動を集権的に管理するために開発されたものであり，利用する側が責任を持って自ら監視していないと，社会そのものを集権管理的なものに暴走させてしまう危険性をはらんでいる。サイバー・テロのようなネット・情報環境の破壊行為の脅威を完全に無視してもいけないが，それに対してあまりにも過敏に反応し，過去の世代が苦労して勝ち取ってきた自由を放棄するようなことがあってはならないのである（Hayek. 1992: 17-18）。どちらの行き過ぎも間違った道に導く。先にも述べたが，何に対しても極端にはしることを戒めたアリストテレスの「中庸」の精神こそが重要である。無差別同時多発テロという社会不安をまともに受けているわれわれに今必要なのは，われわれが過度に安全志向へ振れていること，そしてその強い安全志向が非常に巨大な権力機関である政府に責任を押し付け，さらにその権力を巨大なものにしようとしていることを自覚し，一度放棄すると取り戻すのは容易ではない自由の大切さについて冷静に判断・行動することである。

情報社会は本質的に集権管理型に向かいやすい社会であり，プライバシーに関わる情報は集権的に蓄積管理されるようになる。プライバシー情報が集権管理されることはたしかに便利な側面を持っているが，その一方で個人の自由にとっては大きな脅威となる可能性は高い。個人はそのようなプライバシー情報が単に組み合わされたものとして扱われるようになる。個人のプライバシーに関わる多くの情報が現在デジタル化され，政府機関や民間企業のさまざまなデータベースに蓄積されている。さらにネット化が進むことにより，個人を特定するために不可欠な情報のマッチングがこれまでとは比べ物にならないほど容易にできるようになる。それまでばらばらにしか利用できなかった情報を結合して利用できるようになることで，個人個人のニーズに応じた財やサービスの提供が行われるようになるであろう。その反面，結合されたプライバシー情報が悪用されるとその被害はこれまでとは比べ物にならない。たとえば民間企業にとって顧客のニーズや消費性向といったプライバシー情報は最も重要な経営情報資源になってきている。そのため，企業は，倫理的には問題が多いが，顧客に見えない形で顧客のプライバシー情報を収集するツールを積極的に導入するようになっている。また，従業員に対しても，その生産性を向上させるという目的で，どこで何をしているかを監視できるツールの導入を図っている。プライバシー情報の集中管理を求めているのは政府機関も同じであるが，技術的にも権力的にも絶大であり，安易な権限の委譲は社会的な不利益となる。

特に権限の乱用が懸念されているのが政府機関である。電子メール傍受装置「カーニボー」や，世界的な傍受網の「エシュロン」をはじめ，高度な諜報・監視システムが張り巡らされた現代社会では，情報はそのようなシステムの設置者である政府機関の特定

の人々に集まることになる。社会の安全を確保するために導入されたそれらのシステムが設置目的のとおり使用されるなら問題はない。しかし，米国では盗聴された通信の８割が犯罪に無関係であるといわれている。また，日本では警察が捜査や差し押さえなどの礼状を請求して，裁判所が却下する例はほとんどなく，加藤（2001: 159）が指摘するように，プライバシーを保護するための機関，たとえば裁判所のチェック機能が有効に働くがどうか疑わしい。また，ネット化により，情報はネットワーク上に存在し，アクセス権さえあれば入手することができるようになった。十分な情報セキュリティ対策が施されなければ，情報が流失する可能性は非常に大きくなる。政府の関与が安易に認められれば，たとえばFBIのフーバー長官が政治的実権を握ったことからも分かるように，特定の権力機関に意思決定および情報が集中することになり，問題が起きる。政府関与はある程度は必要であるが，最小限に留めるべきである。政府機関の暴走を避けるためには，情報の公開と相互交換の法律による明確な制度化が不可欠である。

プライバシー保護と社会の安全とセキュリティは本質的にトレードオフ関係にある。社会は個人から構成されるが，それぞれの個人が完全なプライバシーを持つとするならば，全体としての社会が安全ないしセキュリティを確保することは難しい。まったくセキュリティをもたないことになる。もちろんいかなる社会，そしてその安全を確保するために権限を委譲された機関である政府も，完全なプライバシーということを認めることはない。社会の安全を保つためには，誰かのプライバシーが犠牲にされることはある。「個人のプライバシー」と「社会の敵に対する防御の必要性」をどのように調和すべきか，個人の自由と社会の安全をどのように調和すべきか，個人の自由を確保しながら社会の安全を維持できる「第三の道」を模索しなければならない。そのためにもっとも必要なのは，プライバシー保護で最も問題となる捜査当局の権限がどこまであるかに関して，明確な法律を定めることである。

政府による情報の収集・利用と監視はどのような場合にどの程度まで許されるべきか，プライバシーの侵害はどのような条件でどこまで許されるか。情報を利用される本人が承認した目的の範囲で利用されるのであれば，個人情報が収集・利用されることは悪いことではない。問題は承認されていない目的や範囲で情報が収集される場合である。政府機関が個々人から収集してきたあるいは収集している情報は膨大であり，それらが不正に利用されると，非常に大きな不利益が個々人にふりかかることになる。さらに，それらの集められた情報が本人の知らないうちに結合されるとより大きな権利侵害に発展する。自分の個人情報を開示するのは必然性がある場合に限り，その場合でも可能な限り最小限にするように注意すべきである。政府の関与を許容する場合も解釈の余地のない厳密なルールを策定し，それを厳格に遵守させなければならない。政府機関が情報を収集する場合も，情報を結合したり，加工したりする場合には，厳格な制度的な手続きに従って，第三者機関の管理の下に行われる必要がある。第三者機関としては，裁判所だけでなく，個人のプライバシーを保護するための独立の第三者機関を設置し，その両者の管理下におかれるべきである。たとえばカナダのプライバシー・コミッショナーのような，個人データ保護のための公的な役職に民間人の登用を検討すべきであろう。

プライバシーを確保するうえで重要なことは，情報の利用をきちんと管理すること，そして何よりも，ユーザに自分たちのデータがどのように外部に提供される可能性があるかを通知することといった情報の公正な取り扱いである。情報の公正な取り扱い方針は，通常，公開性とユーザの同意の原則を掲げている。つまり，個人データのすべての記録とデータバンクは公開され，個人によってアクセス可能になる。アマゾン社がやっているように，サイトは，データを収集する目的と使用方法を明示し，ユーザが誤った

情報を訂正・削除できるようにする必要があるであろう。

▶ 7　結　論――情報環境倫理のあるべき姿――

ネット・情報環境を含め環境はそれが一度破壊されてしまうと復元することができないか，できたとしても膨大な時間と資源を必要とする。それゆえ，環境問題に対する解決で重要なのは，原因となる行為が行われないようにする「予防策」である。また，環境問題はグローバルな形で考えない限り，有効な答えとはならない。われわれは，そのようなグローバルな予防策について着実な合意を積み上げていくしかないのである。

環境問題の解決には，私たち一人一人に犠牲を強いる面があることは否定できない。ネット・情報環境問題についても，どこまで犠牲を払うべきかということについて議論は分かれるであろうが，何も犠牲を払わずに問題が解決されるということはありえない。

蔓延しているのは，Winner（2000: 5-7, 95）が述べているように，狭く設定された問題に巧妙な答えを出すための探求や，より多くの利潤や市場シェアを得るための探求である。こうした関心の持ち方が，公正な社会と呼びうる社会を創造することへの関心を，はるかに凌駕している。われわれは自分自身および将来の世代のために，よりよき未来を実現するよう行動する必要がある。単なる手段的な選択に過ぎないと思われるものでも，ある社会が建設する社会的，政治的生活の形式についての選択，われわれがどんな種類の人々になりたいかについての選択としてみたほうがよい。

われわれは日常生活のさまざまな場面で，いかに行為すべきか，いかに生きるべきかという問いに直面する。多くの場合，われわれは，それについてどのように考えればよいのか分からず，つい手近なところに答えを求めてしまいがちである。われわれにとって，いかに行為すべきか，いかに生きるべきかという問いが出発点であり，終着点である。手近な答えはない。われわれにできるのは，新田（2000: i-iii）が強調するように，カントが示した次の３つの思考原則，すなわち，「偏見にとらわれず自分で考えること」，「視野を広くもち，自分を他人の立場において考えること」，「首尾一貫して考えること」を実践することである。

画面を通じた交流の場であるネット・情報環境では，自分が相対しているのは「バーチャルな人」であって，またそこで生じる人間関係も部分的で抽象的なものになりやすく，他者に危害を加えたり，他者の尊厳を軽視したりすることになりやすい。

クラッキング，ウィルス，サイバー・テロなどバーチャルな世界で起きている反社会的行為は，リアルな世界と同じく，排除することは不可能であり，問題はそのような反社会的行為をどこまで許容できるかどうか，その許容できる水準に抑えるためには具体的に何をどうすればいいかということである。

ネット社会は本質的に「共有地の悲劇化」を招きやすい要素を内在しており，ネット・情報環境における自分の権利だけでなく，環境そのものを自ら責任を持って守っていくという精神を広め，根づかせることが必要である。自分たちはネット社会の「お客」ではなく，責任主体である。

ネット・情報環境を破壊から守るために，社会，特に政府の介入は，それなりに必要ではあるが，最小限であるべきである。情報生態系にすむ個々の住民に比べて，組織体が有するパワーや能力は大きい。

情報通信技術は集権化を助長する特性を持っているので，強力な権力をもともと持っている組織や集団がその権力的な優位性を高めることは否めない。とくに権力が集まり

やすい組織や集団に対しては，その優越的な地位に見合った責務を課し，明確に権限するだけでなく，権限の乱用を抑制するための対抗組織を設立し権限の監視を義務付ける必要があるであろう。

ネット社会は制度的にも技術的にも集権管理型に向かいやすく，特に政府には権力が集中しやすい。ネット市民自らが自分たちの自由が不当に侵害されるのを防御すべく行動しなければならない。それに加えて，個人の自由は一度失われると取り戻すことが難しいため，組織，特に政府の権力の過剰な行使から個々人の自由，具体的には表現の自由，匿名性およびプライバシーの権利を守るための第三者機関を設置する必要があるであろう。解釈の余地のない厳格なルール作りと対抗的な権力機関を作り相互に監視させることが重要である。

●参 考 文 献

Floridi, Luchiano（1999）"Information Ethics: On the Theoretical Foundations of Computer Ethics," *Ethics and Information Technology*, 1（1）: 37-56.

Gavison, Ruth（198）"Privacy and the Limits of Law," *Yale Law Journal*, 89（3）: 421-471（奥田太郎訳（2000）「プライバシーと法の限界」www.fine.bun.kyoto-u.ac.jp/tr1/03okuda2.html）

Hardin, Garrett（1977）*The Limits of Altruism: An Ecologist's View of Survival*, Indiana Univ. Press（竹内靖雄訳（1983）『サバイバル・ストラテジー』思索社）

Harris, Charles E., Michael S. Prichard, and Michael J. Rabins（1995）*Engineering Ethics: Concepts and Cases*, Wadsworth（日本技術士会訳編（1998）『科学技術者の倫理――その考え方と事例――』丸善）

Heiner Hastedt（2001）"How is an ethics of information possible?"（忽那敬三訳 「情報の倫理はいかにして可能か？」,「情報倫理の構築」プロジェクト第２回 国際ワークショップ（FINE2001），２月27－28日，広島，www.fine.lett.hiroshima-u.ac.jp/fine2001/Hastedt_j.html）

Hine, Christine, and Juliet Eve（1998）"Privacy in the marketplace," *Information Society*, 14: 253-262.

平石隆敏（2001）「道徳的な不一致と合意」加茂直樹編『社会哲学を学ぶ人のために』世界思想社，43-52.

本田裕志（1998）「消費者の自由と責任――対環境的に健全な社会を築くために――」加藤尚武編（1998）『環境と倫理――自然と人間の共生を求めて――』有斐閣, 187-205.

Introna, Lucas D.（2001）"Justice and responsibility: on（not）teaching computer and information ethics,"（林芳紀訳「正義と責任：コンピューターと情報の倫理を教える（教えない）ことについて」,「情報倫理の構築」プロジェクト第２回 国際ワークショップ（FINE2001），２月27－28日，広島，www.fine.lett.hiroshima-u.ac.jp/fine2001/introna_j.html）

Johnson, Deborah（1995）"Professional Ethics," in Deborah Johnson and Helen Nissenbaum, Computers, *Ethics and Social Values*, Prentice Hall（岸田功平訳（2000）「専門家倫理」www.fine.bun.kyoto-u.ac.jp/tr1/03kishida.html）

加藤尚武（1991）『環境倫理学のすすめ』丸善

加藤尚武（1994）『応用倫理学のすすめ』丸善

加藤尚武（1996）『現代を読み解く倫理学――応用倫理学のすすめII――』丸善

加藤尚武（1997）『現代倫理学入門』講談社

加藤尚武編（1998）『環境と倫理――自然と人間の共生を求めて――』有斐閣

Kizza, Joseph M.（1998）*Ethical and Social Issues in the Information Age*, Springer-Verlag.（大野正英・永安幸正監訳（2001）『IT社会の情報倫理』日本経済評論社）

蔵田伸雄（1998）「「未来世代に対する倫理」は成立するか――世代間の公正の問題――」加藤尚武編（1998）『環境と倫理――自然と人間の共生を求めて――』有斐閣, 85-104.

前田義郎（1994）「技術と有用性――人と自然を「つなぐ」もの――」加茂直樹・谷本光男編『環境思想を学ぶ人のために』世界思想社，36-57.

Masters, Brian（1996）*The Evil That Men Do*, Doubleday（森英明訳（2000）『人はなぜ悪をなすのか』草思社）

Miller, Arthur R.（1991）"Computers and Privacy," in R. Dejoie, G. Fowler and D. Paradice, eds., *Ethical Issues in Information Systems*, Boyd and Fraser（鶴田尚美訳（2000）「コンピューターとプライバシー」www.fine.bun.kyoto-u.ac.jp/tr1/03tsuruta.html#f1）

水谷雅彦（2001）「「高度情報化時代」における技術と倫理」『思想』926: 108-120.

Moor, James H.（2001）"The Importance of Virtue in Teaching Computer Ethics,"（坪井雅史・上村崇訳「コンピュータ倫理教育における徳の重要性」,「情報倫理の構築」プロジェクト第２回 国際ワークショップ（FINE2001），２月27－28日，広島，www.fine.lett.hiroshima-u.ac.jp/fine2001/moor_j.html）

森村進（2001）『自由はどこまで可能か――リバタリアニズム入門――』講談社

村田　純一（2001）「技術と倫理――技術の本性と解釈の柔軟性――」,「情報倫理の構築」プロジェクト第２回 国際ワークショップ(FINE2001)，２月27－28日，広島，www.fine.lett.hiroshima-u.ac.jp/fine2001/murata_j.html.
Norman, Richard（1998）*Moral Philosophers: An Introduction to Ethics*, 2nd. ed., Oxford Univ. Press（塚崎智・石崎嘉彦・樫則章監訳（2001）『道徳の哲学者たち――倫理学入門――』ナカニシヤ出版）
越智貢（2000）「「情報モラル」の教育――倫理学的視点から――」越智貢・土屋俊・水谷雅彦編（2000）『情報倫理学――電子ネットワーク社会のエチカ――』ナカニシヤ出版，188-217.
越智貢・土屋俊・水谷雅彦編（2000）『情報倫理学――電子ネットワーク社会のエチカ――』ナカニシヤ出版
Raab, Charles D., Colin J. Bennett（1998）"The distribution of privacy risks: Who needs protection?" *Information Society*, 14: 263-274.
品川哲彦（2001a）「環境，所有，倫理」『思想』923: 69-88.
品川哲彦（2001b）「組織と責任」加茂直樹編『社会哲学を学ぶ人のために』世界思想社，87-97.
竹内靖雄（1989）『経済倫理学のすすめ――「感情」から「勘定」へ――』中央公論新社
谷本光男（1998）「生物多様性保護の倫理――「土地倫理」再考――」加藤尚武編（1998）『環境と倫理――自然と人間の共生を求めて――』有斐閣, 127-147.
谷本光男（2001）「寛容――自由な社会を保障するもの――」加茂直樹編『社会哲学を学ぶ人のために』世界思想社，109-120.
土屋俊（2000）「情報処理技術の特徴とその倫理的意義――とくにインターネット技術について――」www.fine.bun.kyoto-u.ac.jp/tr1/02tutiya.html.
Urmson, J. O.（1988）*Aristotle's Ethics*, Blackwell（雨宮健訳（1998）『アリストテレス倫理学入門』岩波書店）
Vladimir（2000）『スーパーハッカー入門――超黒客入門――』データハウス
Whitbeck, Caroline（1998）*Ethics in Engineering Practice and Research*, Cambridge Univ. Press（札野順・飯野弘之訳（2000）『技術倫理１』みすず書房）
Winner, Langdon（1986）*The Whale and the Reactor: A Search for Limits in an Age of High Technology*, Univ. of Chicago Press（吉岡斉・若松征男訳（2000）『鯨と原子炉――技術の限界を求めて――』紀伊國屋書店）
Winner, Langdon（1992）"Citizen virtues in a technological order," *Inquiry*, 35: 341-362（河野哲也訳（2001）「テクノロジー社会における市民の徳」『思想』926: 58-81）
Wolfe, Christopher, John Hittinger, eds.（1994）*Liberalism and the Crossroads: An Introduction to Contemporary Liberal Political Theory and Its Crisis*, Rowman and Littlefield（菊池理夫ほか訳（1999）『岐路に立つ自由主義――現代自由主義論とその批判――』ナカニシヤ出版）

（水元豊文　慶應義塾大学メディア・コミュニケーション研究所助教授）