第六章　ネットワーク社会化と紛争形態の変化
――ハードな安全保障からソフトな安全保障へ

矢澤　修次郎

１．はじめに

本稿は、以下の諸点を明らかにするものである。

(1) 1990年代初頭以来活発化した「ITと安全保障」に関する議論の流れの一つの基調。

(2) そうした議論は、単に新しい技術が紛争を変えたという形で、表層的には理解できず、より根底的な社会変動を踏まえて初めてその真意を理解できること。

(3) ネット(サイバー)ウォーの実態。

(4) そうした新しい紛争に対処するためには、単に高度なテクノロジーに依拠するだけではなく、テクノロジーと人間のコンビネーションが重要であること。

以下順を追って、これらの諸点を明らかにして行くことにしよう。

２．サイバーウォーからネットウォーへ

1990年代の前半、情報技術革命が戦争や社会におけるコンフリクトのあり方、さらには安全保障に限りなく大きなインパクトを与えるのではないかとの問題関心が多くの人々に共有されるようになったとき、まずはじめに多くの人々に用いられた概念は、サイバーウォーという概念だった。

サイバーウォーという概念は、情報技術革命が戦争をどのように変えるかということを、主にテクノロジーに力点をおいて考えるのには、適した概念であった。しかし研究を進めてみると、情報技術革命によって戦争や紛争、対立の担い手が従来の国家だけではなくて、テロリストや国際的な犯罪者や宗教集団などに広がりつつあること、さらには戦争や紛争の主体が従来のような官僚制的な、垂直的な組織ではなくて、ネットワーク型の水平的な組織であることが明らかになり、必然的に、サイバーウォーとは区別されて、ネットワークウォー、ネットウォーという概念が使われるようになった。すなわち「軍隊であったり、軍隊ではない行為者が関わる、戦争とは呼べないようなコンフリクト」(注1)が重要なものになり、それを議論するためにサイバーウォーとは区別されるネットウォーという概念が必要になったのである。

軍事的な用語を使ってそれを言い表せば、サイバーウォーは「高度な緊張を伴うコンフリクト」(HIC)「中程度のコンフリクト」(RIC)を意味し、フォーマルな軍事力の対峙を指すのに対して、ネットウォーは「低い緊張のコンフリクト」(LIC)「戦争というよりは作戦」を意味し、非国家的な準軍事的な不規則的な力を指すのである(注2)。また、二つの用語、さらにはサイバ

ーウォーからネットウォーへの変化の背後には、次のような二つの命題が潜んでいると判断される。一つは、情報技術革命が進展した時代の紛争は、いずれも情報とコミュニケーションを巡る紛争であり、時の経過につれて、コミュニケーション環境を巡る紛争に止まらず、共有された観念や知識を巡る紛争の様相を色濃くするというものである。もう一つの命題は、紛争はネットワークの形で組織され、ネットワークを駆使して闘われるということである。

要するに「ITと紛争、戦争」を巡る議論の背後には、情報社会、知識社会が成立したという認識、情報・知識社会においては、一切のものがネットワーク化されないと上手く機能しないという認識がある。この点を見落としては、多くの議論はその真意を理解できない。

３．ハードな安全保障からソフトな安全保障へ

1993年ごろから、情報が問題であることが誰の目にも明らかになってきた。そうなった理由の第一は、情報技術革命が進行して、インターネットだけではなくて、ケーブルシステム、通信衛星、携帯電話など、従来の「一対多」のメディアから「多対多」の新しい通信メディアが利用可能になったことである。第二の理由は、直接的にインフォーメーションやコミュニケーションのイシューに関わる沢山の組織―国家組織あるいは非国家組織を問わない―が群生してきたことである。しかもそれらの組織はネットワークされることによって、大きな影響力を持っていったのである。そして第三の理由は、情報と権力が益々相互依存関係にあるという認識が多くの人に認められたことである。さらにこれら３つのレベルにおいていずれも、ネットワーク効果が発揮されたことも忘れてはならないだろう。かくして情報に基盤をおいた領域が創造されると共に、その領域もネットワーク効果をともなって、ますます重要なものになっていったのである。

インフォーメーションによって規定される領域は３つあるとされる(注３)。それは、サイバースペース、インフォスフィア、ヌースフィアである。

これら３つの領域は多くの重なり合う側面を持つと同時に、相対的に独自の内容を持っている。サイバースペースは、３つの領域の共通部分であり、最小の領域であり、技術的なものである。それは、「インターネットで結ばれたコンピューター、コミュニケーション・インフラストラクチャー、オンライン・コンフェレンス・エンティティ、データベース、一般的にはネットとして知られるインフォーメーション・ユーティリティ」(注４)のことである。この領域は、一般的にはネットを指すという意味で、他の２つの領域よりも境界づけられたものである。しかしこの領域をより広く解釈して、パブリック・スイッチ・ネットワークや重要インフラを統御するサイバースペースを含むものと考えることもある。戦略的な情報戦争は、このようなサイバースペースのセキュリティと安全を確保しようとするものに他ならない。

インフォスフィアは、サイバースペースと同じ意味に使われることもある。しかしサイバースペースと異なるものとして概念化する場合には、サイバースペースを含んで、それよりももっと大き

な、ネットの部分ではないかもしれない情報システムの範域を意味する。民生面で事例を挙げれば、放送、印刷、その他のメディア、およびそれらに関係した制度を意味し、軍事面では、コマンド、コントロール、コミュニケーション、インテリジェンス、サベーランス、偵察システムを言う。要するにそれは、より広い形で規定された「情報環境」を表現している概念である。それは、「真にグローバルな情報インフラ、情報環境」(注5)を表現するのに相応しい概念であると言えよう。

ヌースフィアは、前二者を含んだ最も広汎な「地球大に広がった精神の領域」を指す。ヌーというのは、ギリシャ語で精神のことである。この概念は、はじめフランスの神学者ティヤール・ドゥ・シャルダンによって、地理的な領域、生物的な領域の次に来る進化の段階、精神の領域の意味で用いられたが、今日では情報時代の多くの思想家に受け継がれ、「精神の集合的有機体」(注6)を意味するものとされている。それは、サイバースペース、インフォスフィアを含み、それ自体、テクノロジーのレベル、組織のレベル、観念のレベルを持っている。とりわけ組織のレベルは重要で、そのレベルでネットワーク型の組織が支配的になり、それらがNGOなどの市民社会の行為者によって担われ、発展させられてゆくことが、ヌースフィアの発展に極めて大切である。

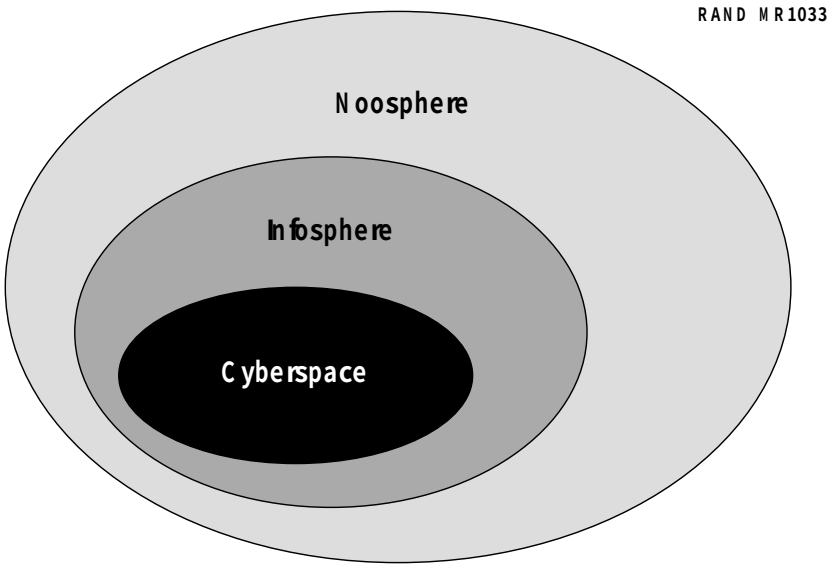

図１　インフォメーションの３つの領域［出典：注７］

表１　３つのレヴェルからみた情報領域［出典：注７］

	Cyberspace	Infosphere	Noosphere
Ideational tenets	Interconnectivity and democracy	Prosperity and interdependence	Sharing ideas
Organizational exemplars	Internet Society, EFF,CPSR	CNN,Disney, TimeWarner	Peace NGOs, universities, the UN
Technological conduits	Internet, the Web	Radio, TV, cable	Educational and training systems

図１は、サイバースペース、インフォスフィア、ヌースフィアの関係を、表１はそれら３つの領域の特徴を比較対照して明らかにしたものである（注7）。図１からは、３つの領域はビットと知識や知恵などの違いはあるものの、いずれも情報の領域である点で共通しており、従って「情報処理」の領域であることが分かる。そして表１からは、各領域の相対的に独自な特徴が浮かび上がってこよう。さらに図１と表１を関連付けて見ると、もう一つ重要な問題に気付く。それは、今３つの領域は全て情報処理の領域としては共通であると言ったが、ヌースフィアだけは情報処理の領域であると共に、情報の構造化にも関わる領域であるということである。情報は処理され伝達されるだけでは何にもならない。処理され伝達されると共に構造化されて、目的、価値、規範、実践に結び付けられて初めて意味を持つ。この意味で唯一構造化を受け持つヌースフィアは、最も重要な領域なのである。換言すれば、この領域は知識、知恵の領域でもあると言える。この領域の質によって、情報の時代が、知識・情報の時代として完成する。

今日、情報技術革命は世界の統合を推し進めると同時に、他方では世界に断片化をもたらしてもいる。さまざまな情報テクノロジーを使えば、独自の文書、イメージ、映像、音などを自分たち自身で作ることができ、その自分たちの作った世界のなかに閉じこもることが可能になるからである。この矛盾に直面して、われわれが世界の安定と平和を推進しようとするならば、どうしても、特別の重要性を持つヌースフィアの形成とその情報の構造化機能に注目しなければならない。これまでアメリカは、サイバースペース、インフォスフィアにおいては先導的な役割を果たしてきた。そこでアメリカは、このヌースフィアの領域においても主導的な役割を果たし、世界の安全を保障して行く責務を持っている。そのためには、情報の３つの領域、とりわけヌースフィアに重点を置いた、これまでの現実政治に代わるヌーポリティークの形成が不可欠である（注8）。そのような認識が一段と強まっている。勿論、アメリカ以外の国々や非国家的主体や諸勢力もこの課題を追求するだろうし、現にこの領域に関ってきている。また、テロリストや犯罪者集団もこの領域に介入しようとし、その領域を自己の目的の為に利用しようとしている。したがって、この領域が上手く連接・形成されないならば、この領域は新しいイズム(宗教的、エスノナショナリズムなど)によって利用されてしまう恐れなしとしない。そこで、先の課題は、このような諸勢力に対峙する形で進められなければならないのである。一例を挙げよう。イラクのサダム・フセイン体制の変革のためには、国家が主体となった戦争だけで十分だろうか。いやそのようには考えられない。国連やNGOなどとの連携が必要不可欠になるだろうし、それらを通じて初めて、その目的を実現することができるのではなかろうか。以上のような認識が、今日ほど必要とされている時はない。

４．情報社会における戦争

これまでの考察からも明らかなように、ITと安全保障の問題は、情報社会、ネットワーク社会における安全保障という包括的な視野をもって考えられなければならない。この問題は、情報技術が戦争、紛争を変えるという狭い文脈において、しかも新しい技術が何かを変えるといった技術決定論的な視角から考えるのは、却って問題の本質を捉え損ねることになりかねない。情報技術と経済、政治、社会、文化は、一方が他方を決定するといった単純な関係にはなく、両者が複雑に規定しあう複雑なインターフェースの関係にある。そこで以下では、今日における戦争、紛争の問題を情報社会、ネットワーク社会との関係において、しかも技術と戦争、紛争のインターフェースという視角を保持して解明する試みをトレースしておくことにしよう。

アメリカの社会学者Manuel Castellsによれば、情報技術革命と経済、政治、社会、文化とのインターフェースは、情報社会、ネットワーク社会の台頭とそこにおける経済、企業、労働、国家、政治、社会運動、文化などあらゆるもののネットワーク化をもたらした。情報社会、ネットワーク社会とは、ネットワークが主体の社会であり、情報や知識が社会の発展様式を第一義的に規定する、情報的発展様式を形成するようになる社会である(注9)。

従来の産業社会と情報社会、ネットワーク社会の関係に関しては、二つの連続性を強調する考え方と両者の断絶性を主張する立場とがある。しかし人間が、時間と空間という根源的な概念に支えられて身体を動かして生きているという原点にまで立ち返って考えてみれば、情報社会、ネットワーク社会は、やはり質的に新しい社会として把握されなければならないのではないだろうか。以下では、カステルの議論に従って、時間と空間という２つの概念を検討することによって、情報社会、ネットワーク社会が質的に新しい社会であることを明らかにしておくことにしよう。その新しい社会において、戦争、紛争も質的に新しいものへと変化していかざるを得なかったのである。

カステルによれば、「近代性とは、そのマテリアルな観点から見ると、空間と社会に対する時計時間の支配として認識される」(注10)。しかしこの単線的な、不可逆の、計測可能な、予測可能な時間は、ネットワーク社会という極めて重要な動向のなかで、壊れはじめている。

今、時間は極限にまで圧縮されつつあり、したがって時間が消滅していこうとしている。換言すれば、今、多くのものが時間から自由になり、時計時間から逃走しようとしており、結果として、人間存在のあらゆる領域で「新しい時間性の論理」が自らを明示しようとしているのである。その新しい時間性の首尾一貫したパターンは、タイムレスタイムと表現されている。

カステルに従って新しい時間性の論理、タイムレスタイムのさまざまな領域における明示をトレースしておくことにしよう(注11)。グローバルな資本市場においては、価値の源泉として時間が使われ、同時性、スピード、将来の時間さえも取り込んだ価値創造が行われ、グローバルな資本市場はグローバルカジノの様相を呈すると共に、「生産と報酬、労働と意味、倫理と富、それ

らの間の対応関係についての社会認識に根本的なダメージ」が与えられている。

情報社会、ネットワーク社会で支配的になっているネットワーク企業もフレックスタイムを明示している。ネットワーク企業の諸実践（柔軟な経営形態、固定資本の間断無き使用、業績評価、戦略的同盟、組織連関)は、時間の圧縮、破棄に基づいている。市場の要求や技術変化に対応できる時間の枠組みが、企業の競争力を支える原点であり、それを担うのは、熟練労働者のフレックスな時間管理による労働に他ならない。

情報社会、ネットワーク社会においては、人々の生活労働時間の圧縮と多様化・差異化が顕著である。近代社会においては、賃労働の時間が社会的時間を構造化してきた。また労働時間数、そしてライフサイクルの上で、年で、月で、週で、それをどう配分するかは、彼らが生活をどう感じ、どう楽しみ、どう経験するのか、その中心的な問題であった。この100年間は、一貫して、労働時間の短縮化の方向、生活労働時間の配分の画一化の方向が追求されてきた。しかし、この労働時間の短縮化、画一化傾向は、ここにきて、より複雑な、より変化に富むパターンに変容しつつある。その鍵を握るのが、企業、ネットワーク、業種、職業、労働者の特徴によってそれぞれ異なる、労働時間と労働スケジュールの多様化の増大傾向である。以上のような労働時間の新しい配置によって、労働時間はライフサイクルのなかで占めてきた伝統的な中心的位置を失うかもしれない状況に直面している。

こうした事態と関連して、平均寿命が伸張し、労働力化する年齢が高くなり、労働年数が減少する過程が進行する。世界的に見ると、50歳台前半で、男性労働力の３分の１から２分の１以上の人達が永続的に労働市場を放棄する事態になっている。結果として、労働が人生の中核に座ることがなくなり、さらには年金、医療システムに大きな問題をなげかけると共に、世代間の社会的連帯にもさまざまな問題が生じつつある。

今日の社会変動は、宇宙の法則に関連した生命リズム、それに即したライフサイクルを崩しつつある。今日の社会変動は、このライフサイクルを決定的に侵食しつつある。種の再生産をコントロールする能力が増大し、平均寿命が延びつづけている。さらに高齢者の社会的世界が一口に高齢者と一括することが出来ないほど多様化している。再生産の管理化が一段と進行し、再生産からも、親となることからも、年齢と生物学的条件を引き離してしまっている。社会制度と再生産の営みとの間のずれが増大し、生物学的時間の無効化が進行している。その結果、世俗的なリズムは、実存的な決定に委ねられることになっている。それにもかかわらず、現代人にとって、その実存的決定を支えるものはあまり提供されていない。ここに、現代の危機の最も重要な要因の一つがあると言えないだろうか(A．ギデンズ)。

さらに現代社会は、死を否定しようとしているかに見える。これまでは社会と生活における時間は死によって計られてきた。今まで死は否定されることはなかった。死を前提にし、気遣いをもって人間はその時間性を生きてきたのではないか(M．ハイデガー)。しかし、現在は、われわ

れの生活から死を追放する企てが行われている。現代人は、あたかも死が存在しないように生きている。生きつづける野望を抱き、脅迫的なまでに予防に力を入れ、終末と戦うのが現代人の生き方である。そこにおいては、死の時間的・空間的隔離が行われ、死者に対して喪に服することをも喪失しているのではないか。現代社会は、生から死を取り除こうとしている。要するに、人生の期間に永遠を構成しようとしているのである。

以上のようにカステルは、情報社会、ネットワーク社会における新しい時間性の論理のさまざまな領域における現れを捉えているが、彼はその同じ文脈において戦争をも捉え、新しい戦争を、新しい時間性を体現したものとして捉えている。彼は、新しい戦争をインスタントな戦争と呼び、先進諸国の間には、戦争を開始し、それを何らかの形で社会が受け入れるための条件に関して、３つの結論が急速に浸透したと考える(注12)。

> 一般市民を巻き込まないこと。戦争は専門の軍隊によって実行されるべきこと。そのために強制的な徴兵は、それが要請されるような環境が生じるまで保留されるべきこと。
>
> それは短期間、さらには一瞬であること。人間そして経済環境の消耗を減らし、軍事行動に対する正当性の問題が提起されないように、すばやく結果を出すこと。
>
> 敵を破壊する時でさえ、クリーンな、局所攻撃であること。そして十分な根拠を持った限度内で行い、イメージ構成や戦争場面の構成に関して厳密な情報操作を実行することで、可能な限り公衆の目から事態を隠すこと。

湾岸戦争からアフガン戦争にいたる過程を見ていると、カステルの情報社会における、ネットワーク社会における戦争、インスタント戦争の性格付けは、正鵠を射ていると判断されるであろう。そして新しい戦争への変化を確実に裏付け、支えてきたのは、情報技術の軍事技術への応用、軍事技術の飛躍的進歩である。その進歩は、生身の人間の存在がむしろ精密な兵器の使用の桎梏になるところにまで行き着いているという(注13)。また、人生で１度も戦争を経験しない最初の世代が育ちつつある。これは人類史でも新しい経験であり、少なからず社会に大きな影響を与えることになるであろう。これらのことを考え合わせると、情報社会、ネットワーク社会は、新しい戦争をもたらすと同時に、どうやら戦争を一つのデッドエンドに導きつつあるように思える。国家と国家の戦争、それはますます起こりにくくなりつつあるだろう。

かくして時間は消滅し、「時間を共有する実践を束ねる物質的なサポート」(注14)としての空間がわれわれの社会の時間を規定するようになり、したがって、近代性の歴史的トレンドを逆転する。この意味で、情報社会、ネットワーク社会は、質的に新しい社会として位置付けなければならないのではなかろうか。

５．ネット（サイバー）ウォーの実態

情報技術革命が兵器体系を根本的に変え、それが戦争の戦略、戦術、オペレーションその他をどのように変えていったのかは、重要な問題であるが、それをトレースするのは私の任務ではない。しかし、そうしたいわば表の戦争と同時並行して戦われるネット（サイバー）ウォーの実態に関しては若干の考察を行っておかなければならないだろう。

今日世界で起きている多くの紛争においては、現実世界で行われる紛争行為の背後で、それと平行して、サイバースペースにおける闘争が行われている。それが現代世界の行方を左右すると言っても決して過言ではない。アラブ－イスラエルの紛争を例に取ってみよう(注15)。この紛争においてネットウォーが本格化したのは、2000年10月、レバノンのシーア派のヒズボラ運動が３人のイスラエル兵士を誘拐した直後であった。プロイスラエルのハッカーがパレスチナ側のウェブサイトをクリッピングし、それに対抗してプロパレスチナのハッカーが報復に出て、イスラエル政府のウェブサイト、イスラエル外務省のウェブサイトをダウンさせた。これをきっかけにサイバーウォーは一気にエスカレートした。イスラエルのハッカーは、ダビデの星とヘブルー語のテキストをヒズボラのミラーサイトの一つに書き込むと、プロパレスチナのハッカーは、イスラエル銀行やテルアビブの証券取引所を攻撃した。この紛争に、南北アメリカのハッカーたちも参加し、100を越えるウェブサイトやインターネットサービスが使えなくなってしまった。この事件以降今日のサイバースペースは、「ハッキングという道具を使って抗議をし、より広い闘争に参加しようとする、反乱者、フリーダム・ファイター、テロリスト、その他の人々の、ディジタルな戦場として、ますます使われつつある」(注16)。

ドロシー・デニングは、以上のような活動を言い表すには、ハッキングとアクティビズムを組み合わせた「ハクティビズム」という用語が最も相応しい、と言う。従来このような活動は、サイバーテロリズムという用語によって表現されてきた。しかし厳密に言えば、彼も言うように、「ハクティビズム」がテロリズムの性格を持ってはじめてサイバーテロリズムと呼ぶのが妥当であるから、「ハクティビズム」をサイバーテロリズムから区別しておいたほうが良いのではないか。ホームページの改竄などはまだ良い。そうした活動を越えて、コンピューター制御で行われる電気、水道、ガスの供給、経済活動のインフラ、金融システム、そうしたものに混乱をもたらそうとする活動は、限りなくテロリズムに近い。

もっともドロシー・デニングは「テロリスト達は、テラーを誘発する手段としては、バイトよりは爆弾を好む」が故に、「ハクティビズムはリアルで広がっているが、サイバーテロリズムは理論のなかにだけ存在する」(注17)と主張しているが、それも行き過ぎた主張ではないだろうか。確かに今までのところ、９・11事件が示すようにテロリストはローテクによる破壊を主要な活動として選択する(注18)。しかしそのことは、ハッキングによるテロリズムの可能性を排除するものではないだろう。とりわけ我々の生活の基盤がコンピューター制御で整えられる度合いが飛躍

的に増大していることを考えれば、決してサイバーテロリズムが理論のなかで存在するだけであるとは言えないだろう。また、テロリストがローテクに依拠するのは、好みの問題でもありえない。

ハクティビズムは、インターネットの広がりにつれて増えつづけ、今後も益々ポピュラーになることは間違いない。では、どうしてハクティビズムはそんなに魅力的なものなのか。それは何よりもまず実行しやすく、物理的な攻撃よりも多くの利点を持っているからだろう。ドロシー・デニングは、ハクティビズムの魅力を以下の諸点に纏めている(注19)。

第１にハクティビズムは、実行者のメッセージを極めて広汎な聴衆に届けることができる。ハックされたサイトが多くの人々に見られるだけではなく、ハックされたサイトが元通りに直されても、ハックされたページは、いくつかのサイトに保存され、そのサイトはいつどこからでも見ることができる。さらにハッカーによってページが改竄されたことはメディアが大々的に取り上げ、その報道を通じてメッセージがさらに広げられてゆく。

第２にハクティビズムは、実行に際してほとんどコストがかからない。コンピューターをインターネットに繋げればできてしまう。ハッキングのツールは、インターネットの多くのサイトからダウンロードすることができる。

第３にハクティビズムは、地理や距離的な制約を越えることができる。いつどこからでも戦闘に参加することができる。WTOに対する抗議行動においては、イギリスに本拠を置くエレクトロニック・ヒッピー・コレクティブの推計によれば、422,000人がWTOのサイトへのシットインに参加した。いつでもどこからでも参加できるが故に、一定のコーディネートが行われれば、比較的短期間に多くの人が抗議行動に参加できるのである。

第４にハクティビズムは、匿名で危険を伴うことなく闘争に参加できる形態である(注20)。

ハクティビズムがこのようなものであってみれば、インターネットの普及にともなってますます広がり尽くしていくものであることは明らかであろう。その動機は、スリルを求めて、好奇心に駆られて、抗議行動としてなど、実にさまざまである。一体、サイバーウォーの隆盛は何を意味しているのだろうか？私見によれば、それは、これまでは国民国家がその枠組みの内部で情報や知識を監視、コントロールすることによって社会秩序を維持してきたのだが(注21)、それが最早不可能になりつつあることを意味しているのではないだろうか。人々が情報技術に支えられて国民国家の枠組みを超えて横に繋がることが容易にできるようになる。社会主義国民国家は、情報化の進行のなかで、逸早く消滅せざるをえなかった。暴力を使ってそれを阻止する選択もありえたが、ゴルバチョフはそれを選択しなかった。さらなる情報化の進展は、資本主義国民国家の再編を迫りつつある。人々はswarmingな戦略を取って権力のコントロールを取り除こうとする。勿論、国家も黙って手をこまねいているわけではない。国家も同じswarmingな戦略を取って、自らの枠組みの内部でなんとか知識、情報をコントロールして社会秩序を維持しようと試みる(注22)。

したがって今日における安全保障という問題の本質は、近現代国民国家の危機を踏まえて、新しいネットワーク国家を作ることであろう。情報社会、ネットワーク社会においては、国家権力の手段も目標も、コミュニケーションやネットワーキングに依存せざるを得ない。国家は消滅しないが、国家はその構造と実践を、根本的に転換して行かない限り、上手く機能しないのである(カステル)。そのことは、９・11事件を見るだけでも明らかであろう。アメリカは、必死に、ネットワーク国家を作り国民国家の枠組み内部で知識や情報を監視、コントロールすることによって、何とかして社会秩序を維持して行こうとしているのである。

サイバーウォーの実態を探る最後に、再びドロシー・デニングに依拠して、サイバーウォーにおけるさまざまな攻撃の形態を瞥見しておくことにしよう(注23)。

最も一般的なサイバー攻撃の形態は、ウェブの改竄やウェブのハイジャックである。ウェブの改竄は説明するまでもないが、これは1999年に3,700件行われ、2000年には5,000件を数えるようになり、その後も増えつづけている。ウェブハイジャックというのは、特定のサイトのドメインネームサービスを不正に書き換えてしまい、そのサイトにアクセスすると自動的に、自らの訴えたい内容の書かれたサイトが現れてくるようにしてしまうことである。

もう一つのポピュラーな攻撃形態は、ウェブシットインと言われるものである。これは、数千のウェブユーザーが時を同じくして目標のウェブサイトにアクセスして、通常のサービスを機能不全にしてしまうものである。シットインを効果的に実行するために、さまざまなテクノロジーが開発されてきた。シットインのオルガナイザーは、自動的なソフトウェアがセットされた特別のサイトを設置して、シットインの賛同者に参加を呼びかける。賛同者がそのサイトにアクセスすると、アクセスした人のブラウザーが自動的にセットされていたソフトをダウンロードし、そのソフトは数秒ごとに、攻撃の対象とされたサイトにアクセスすることを繰り返す。アクセスしたときに、メッセージを残すようにも工夫されている。

シットインは効果的なものになるまでには、少なくとも数千人の参加者を必要とするが、「サービスの否定」(denial of service, DoS)攻撃は、一人で、大きな効果を発揮することができる。この攻撃は、ハッカーが目標のサーバーに多くのネットワークメッセージを送りつけるソフトウェアを使用する。送られたメッセージがサーバーをクラッシュするか、サービスを妨害してしまう。この応用編としては、「配布されたサービスの否定」(DDoS)攻撃がある。これは、ハッカーが沢山のインターネットサーバー(ゾンビと名づけられている)に侵入してそこにソフトをインストールしておくものである。ハッカーはそのゾンビを全てのターゲットに１度に攻撃をしかけるようにするソフトを使用して攻撃を行う。

６．ネット（サイバー）ウォー、ネット（サイバー）テロリズムは防げるか

９・11事件以降、アメリカのインテリジェンスシステムは何故テロを防ぐことができなかったのか、あるいはどうすれば今後テロを防ぐことができるのかに関する議論が盛んに行われている。おびただしい議論が有る中で、興味深いことは、技術によってテロを防ぐことができるというよりは、テロを防止するために最も重要なものは人間的な要因であるという議論が多く展開されたことである。

テロと戦う技術の面で最もポピュラーなものは、エシュロンやカーニバルなどの監視システムである。エシュロンは、言うまでもなく、National Security Agencyのグローバルな監視ネットワークである。これは、毎日、30億個のアメリカ領域外のコミュニケーション(電話、e-mail、ファクス、放送など)をインターセプトするスパイ・システムである。またカーニバルは、FBIがインターネットサービス・プロバイダーの協力を得て、インターネットを通じて送られるデータのやりとりをインターセプトするもので、1996年以降使われている。

しかしこれら監視システムが如何に優れているとしても、われわれはテロリズムとの闘いにオプティミズムを持ち込むことはできないという。何故なのか。

ケビン・ホーガンによれば(注24)、それは第一に、今日地球上で作られる情報の量は監視システムの情報処理能力を遙かに凌駕してしまっているからである。必要なインテリジェンス情報を情報の洪水のなかから探し出すのは、極めて困難な課題である。このことは、セキュリティの専門家も認めている。また、たとえ通信を傍受できたとしても、暗号をかけられたメッセージを解読できる可能性はそれほど高くないと言われている。さらに最も先端的なスパイテクノロジーも、驚くほどプリミティブな対抗手段で妨害されてしまう。

以上のように攻撃される側が技術的に圧倒的に不利であるということに加えて、ケビン・ホーガンが挙げる第２の理由は、スパイや監視のためのテクノロジーを、開かれた民主主義社会と両立する形で使用することが極めて難しいということである(注25)。９月11日の衝撃的な事件の後でさえ、アメリカの市民達は政府がテロ対策の名の下に運動やコミュニケーショを詮索する力を増大させることを批判した。確かにカーニバルのような技術は、特定の個人にターゲットを絞る形での監視・諜報は有効であろうが、９月11日事件の後のように、電子メールを受け取ったり、ウェブサイトにアクセスしただけで400～500人が被疑者とされてしまうのは、多くの問題をはらんでいるように思われる。

かくしてアメリカにおけるテクノロジーの多くの専門家達は、ブッシュ政権のテロ対策はこれまで見たことのないような監視国家を作る可能性を持つものの、アメリカをより安全な場所にすることにはならないと主張している(注26)。また多くの専門家達は、「最先端のテクノロジーだけではわれわれを安全にすることはできない。人間的要素、とりわけ『暗黙知』といわれる経験と直観のコンビネーションがより一層重要である」(注27)とも述べている。

７．おわりに

史上第三の科学技術革命と言われる情報技術革命は、すべてのものとインターフェースしながら、大きくいろいろなものを根本的に変化させている。その革命の中核にあったのは、言うまでもなく、コンピューターである。コンピューターは、人間のもう一つの頭脳となるべく開発されたものである。現時点で、このことをもう一度想起しておくことは重要なことである。何故ならば、今日多くの人々は、新しい技術に依存して人間の頭脳、英知を発展させることを怠りがちであるからだ。いかに高度なテクノロジーでも、それは人間の細胞のイミテーションを越え出ていない。人間の頭脳、知識、知恵、英知と、テクノロジーが車の両輪となったとき、人間はより十全な社会を作ることができる。現在は、そのどちらが欠けても、われわれは十全に生きることはできない。安全保障の問題もその例外ではあり得ない。人間と自由な社会を消し去って、高度なテクノロジーに依拠して完全な監視社会を作るのは、真の解決の方向ではあるまい。二つのもののコンビネーション、不均等な発展、貧困、環境問題、文明の対話に真摯に取り組むこと、その過程を通じてグローバルな情報ネットワーク社会を作るべく努力すること、それこそが今後の安全保障の基盤ではないだろうか。

－　注　－

1．Arquilla，John，and David Ronfeld，*The Advent of Netwar*，Santa Monica，Calif.，RAND，1996．p.1.

2．*Ibid.*，p.3.

3．以下の３つの領域に関する議論は次の文献による。Arquilla John and David Ronfeld，*The Emergence of Noopolitik: Toward an American Information Strategy*，Santa Monica，Calif.，RAND,1999.

4．*Ibid.*，p.10.

5．*Ibid.*，p.12.

6．*Ibid.*，p.13.

7．*Ibid.*，p.16，p.17.

8．*Ibid.*，pp.20-25．このような議論は、すでにさまざまな議論のなかに取り入れられている。たとえば、ジョセフ・ナイの議論などはその代表的なものであろう。

9．Castells，Manuel，*The Internet Galaxy*，Oxford，Oxford University Press，2001．また情報社会、ネットワーク社会の総体的な分析に関しては、彼の以下の３巻本を参照のこと。Castells，Manuel，*The Rise of Network Society*，2nd edition，Oxford，Blackwell，2000，

The Power of Identity, Oxford, Blackwell, 2001, *The End of Millennium*, Offord, Blackwell, 1998.

10. Castells, Manuel, *The Rise of Network Society*, Oxford, Blackwell, 2000, p.463.
11. *Ibid.*, pp.465-499.
12. *Ibid.*, p.486.
13. この点は、加藤朗氏の研究会における発言に教えられた。
14. Castells, Manuel, *Ibid.*, p.441.
15. 以下のネットウォーの実態に関しては、以下の論文に依拠している。Denning Dorothy, "Cyberwarriors: Activists and Terrorists Turn to Cyberspace," *Harvard International Review*, Summer 2001, Vol.XXIII, No.2, pp.70-75. 以下の議論でデニングは、サイバーウォーという概念を使っているのでそれに従う。
16. *Ibid.*, p.70.
17. *Ibid.*, p.70.
18. Tenner Edward, "The Shock of the Old," *Technology Review*, December 2001, pp.50-51.
19. Denning Dorothy, *Ibid.*, p.71.
20. 勿論名前を明示して闘争に参加する運動もあることには注意しておきたい。
21. この点を十全な形で明らかにしたのは、Anthony Giddensである。Giddenns, Anthony, *The Nation State and Violence*, Oxford, Polity Press, 1985.
22. Swarmingというのは、小さな単位、集団、個人が、ネットワーク化されて、多面的、多方向的に展開されて行く紛争の様式をいう。以下の文献を参照のこと。Arquilla John and David Ronfeld, *Swarming and The Future of Conflict*, Santa Monica, Calif., RAND, 2000.
23. Denning Dorothy, *Ibid.*, pp.71-74.
24. Hogan Kevin, "Will Spywar Work?" *Technology Review*, December 2001, p.47.
25. *Ibid.*, p. 47.
26. Garfinkel Simon, "How not to Fight Terror," *Technology Review*, December, 2001, p.21.
27. Bennet, John, "Technology and Terror," *Technology Review*, December, 2001, p.9.