第一章　サイバー空間における脅威と安全保障・危機管理のあり方

星野　俊也

１．はじめに

IT（情報技術）革命の積極的な側面が強調されるなか、コンピューターを用いた情報通信ネットワークの脆弱性とそれに対する依存度を高める社会の陥穽を突いたサイバーテロやハイテク犯罪など、新しいタイプの脅威は着実に個人や組織、国家の安全保障にとっての重要な挑戦となりつつある。物理的な空間での不正行為と異なり、「サイバー空間」でのそれに対し、われわれは予防・検知・対策のすべての面で発想の転換と新しい危機管理体制の整備を進めていく必要がある。そこで本委託研究は、IT革命がさまざまなレベルで人々の社会に及ぼすことになる影響を「安全保障」という観点から捉え直し、その脅威の実態や対応策の現状と今後のあり方について考えることを目的とする。

言うまでもなく、IT革命は極めて技術集約的な動きではあるが、本研究では、そうした技術の側面―すなわち、高度技術を用いた攻撃に対する高度技術による防衛という側面―のみに議論を限定せず、「IT革命と安全保障」をとりまく政治、軍事、経済、社会の諸側面まで検討していく。特にわが国の安全保障という観点からの議論に着目するが、その場合も、サイバー空間での不正行為が頻発する政治・軍事的な背景や技術・経済面での相互依存の現状、さらには社会・文明的な意味についても掘り下げていきたい。また、ITの技術的な発展は、「情報空間」の拡大をもたらすものである。ついては、問題は変化する情報空間における情報の収集・分析・活用の方法とも密接に結び付く。そして、これは、サイバー空間における攻撃に対する安全保障・危機管理の体制に関する議論を超え、より広い情報空間での外交の展開についても考察することにもつながるだろう。

本章は、この委託研究全体の総論として、まず初めにサイバー空間における安全保障上の脅威の実態について整理する。次にこれらの脅威に対する危機管理と安全保障のあり方や今後の方向性を打ち出すこととしたい。

２．サイバー空間における脅威

(1) サイバー空間とは何か？

「サイバー空間における脅威」とひと言で言っても、おそらく多くの場合、実感がわかないというのが現状なのではないだろうか。目に見える物理的な破壊と人々の生命や財産の喪失を伴う自然災害や武力衝突と違ってコンピューター・ネットを通じた電子的な世界での脅

威のことである。一体どれほどの被害が想定されるのか、にわかには捉えどころのないことがサイバー空間での不正行為の特徴であると言えるだろう。しかし、その空間は「バーチャルな（仮想の）」かたちでしかイメージできないかもしれないが、万一、破壊工作が行われるならば、その被害は決してバーチャルなものにとどまらない、現実的なものとして現れるはずである。しかも、もしも適切な防御措置をとっていなければ、被害の規模はほとんど計り知れないほど大きなものにまで波及する可能性がある。なぜなら、それは、「サイバー空間」がもつ広範な便利さと表裏一体の関係にあるからである。

「サイバー空間（cyberspace)」は、米国のSF作家ウィリアム・ギブソンの小説『ニューロマンサー』(1984年）で最初に使われた表現とされているが、一般には「コンピューター・ネットワークを通じて情報流通が行われる空間」と理解すればよいだろう。自然界の空間とは違い、これは人間が技術によって作り出した新たな空間である。では、それが持つ特徴とはどのようなものなのだろうか。

ごく単純化するならば、「端末間（end to end)」ネットワーク、双方向性、距離と時間の超越、という３つを指摘することができるだろう。第１は、これが、自らのコンピューター端末をもつ不特定多数のネットワーク利用者の間に構築される空間である、という事実にほかならない。一つ一つは独立したネット同士が結び付き―つまり、「インターネット」を形成し―、世界全体を文字通り「網羅」する。これは裏返すなら、世界の隅々（あるいは「末端」）までが結び付いていることを意味している。第２は、そうしたネットワーク上を動く情報が双方向性をもつこと。そして第３は、インターネットを通じた情報の流通が、瞬時に、距離と時間を超えるということである。

情報ネットワークは、媒体であると同時にそれ自体が重要なインフラを支える基盤になっている。このことは、「媒体としてのネット」を介した「基盤としてのネット」の攻撃が可能であることを意味している。ネットは、善意のメッセージの交換のためであれば極めて有用な媒体にとどまるが、万が一にも悪用された場合、便利さによって、結果はたちまち予想をはるかに越える社会基盤に対する脅威に様変わりする。

(2) サイバー空間の危機管理

本研究報告のなかで繰り返し強調されるように、サイバー空間を利用した犯罪や攻撃に対する危機管理(crisis management)においては、技術的な対応による予防措置を講じておくことが必要条件になるが、それだけでは十分とは言えない。外界と「つながっている」という現実がある限りは、双方向的な情報の流れが可能であることを意味し、さらに、防御技術は攻撃技術よりも宿命的に遅れをとらざるを得ない現実をも直視し、攻撃があり得ることをむしろ前提とした対応―これは、「結果管理(consequence management)」の側面―を強化

することが不可欠である。そして、ネットからの被害を避ける唯一の方法が、コンピューターに保存された情報で、完全な安全の確保を必要とするようなものはネットから隔絶する、という単純かつ明快な選択肢しかないことを理解する必要がある。(もっとも、その場合でも、内部に深く潜入している人物によるコンピューターへの侵入という問題は残るが。）その他の情報は、攻撃を前提に、リダンダンシーを確保することにより、波及を阻止し、バックアップを確実にするほかはない。

結論を先に言うならば、IT革命が安全保障に及ぼす影響を理解することが、抑止と対処を前提とする従来型の安全保障観から、抑止の効きようのない、必ず起こる（あるいは、すでに起こっている)「そこにある明白な危機(clear and present danger)」であるという考え方に転換すること、である。こうした情報セキュリティに対する意識の変革を促すことが、本研究を通じて導き出される役割の最も大きなものの一つと言えるだろう。

だが、サイバー空間を悪用した不正行為の被害を実感することは、ある意味で難しいことも事実だろう。なぜなら、現在、報道されているトラブルは、多くの場合、コンピューター・ウイルスの蔓延といったケースが多く、実害は大きいが、国家の重要インフラ（情報通信、金融、航空、鉄道、電力、ガス、上下水道、政府・行政サービスなど国民の生活に直接かつ死活的な影響を及ぼすインフラ）に対する遠隔的な攻撃はまだ発生していないためだが、これは単なる「幸運」にすぎない。わが国政府としても、「重要インフラのサイバーテロ対策に係る特別行動計画」の策定（平成12年12月15日付）を含む情報セキュリティ対策の推進に着手しているが、官民協力をはじめとし、各般の対策のさらなる具体化が急務となっている。この傾向は、今後、一般家庭のコンピューターがブロードバンド回線を通じ、外部のネットワークと常時接続されるようになり、コンピューター自体が家電になることでより深刻な問題をはらんでいくことに留意する必要がある。

３．サイバー空間の脅威の実態

(1) サイバー空間における脅威の４つのパターン

サイバー空間の脅威に対する認識を深めるためには、おそらく、現時点で顕在化している代表的なケースを見ていくことが有効である。なお、ここで「顕在化している」と断った理由は、後に論じるように、サイバー攻撃は、その攻撃相手(国家・企業・個人など)に対する物理的な攻撃を伴うが、より本質的には主体の機能と信頼性(つまり、脅威に対する強靭性)に対する攻撃であることから、現実に被害を受けてもその事実を公にしない場合がある(または、被害があったことにすら気づかないほどにシステムが脆弱な場合もある)からである。

本研究で取り上げるサイバー空間の不正行為はさまざまな形態をとるが、いずれも（程度の差はあれ）意図と目的を持った人為的な行為であることは間違いない。その観点から見る

と、加害者の意図・目的は大きく２つに分けられるだろう。一つは、サイバー空間によって結び付けられたコンピューター端末そのものの機能撹乱・破壊であり、もう一つは、サイバー空間を流通する情報自体への不正アクセスを狙ったものである。さらにこれらを、相手を特定して狙い撃ちにする場合と、不特定多数を無差別に対象にする場合に分けることができるだろう。こうして、４つの脅威のパターンが浮かび上がってくる。

第１は、不特定の相手のコンピューター端末に対する機能撹乱・破壊

第２は、特定の相手のコンピューター端末に対する機能撹乱・破壊

第３は、不特定の相手のコンピューター端末内の情報に対する不正アクセス

第４は、特定の相手のコンピューター端末内の情報に対する不正アクセス

以下では、それぞれのパターンについて、代表的なケースを取り上げて考えてみたい。

まず第１のパターンだが、不特定の相手のコンピューター端末に対する機能の撹乱･破壊としては、今日、日常的に発生している「マリシャス・コード」による攻撃がこのカテゴリーに入るだろう。

「マリシャス・コード」とは、文字通り「悪意をもった信号」であり、コンピューター上で発生するウイルスやワーム、トロイの木馬、ロジック爆弾などの総称である。これらの「マリシャス・コード」には当然、その作者がいる。優れた工学的知識をもつハッカーたちのなかで、その知識を悪用する者（「クラッカー」と呼ばれ、「ハッカー」一般とは区別される）が自らの腕を試すようにさまざまなかたちで悪意に満ちた信号をネットワークに送り込む。同一の手口で後述のように特定の相手を狙い撃ちすることもあるが、ここでは愉快犯的に不特定多数の相手のコンピューター端末の機能を無差別に撹乱し、ネットワーク社会の混乱を引き起こすことが自己目的化している場合に注目したい。子供のいたずらの場合さえある（注1）。

「ウイルス」という比喩が多用されるように、感染性が高く、感染条件が揃うまで潜伏し、いざ感染した場合、データの破壊、動作の不具合、他のコンピューター端末への攻撃をほぼ自動的に行うことになる。

ウイルスは現在５万種もあると言われ、その種類は増加し、同時に被害件数も年々増加の一途をたどっている。カーネギー・メロン大学コンピューター緊急事態対策センター（CERT）の「CERTコーディネーション・センター」に寄せられた2001年のセキュリティ・インシデント発生報告は５万6000件以上で、前年の160％増になっているという。最近では、特定のウイルスの発生に対する警告が発せられると、自分のメールの受信ボックスに感染源になり得ると懸念されるメールが知人からの着信メールとして入っている、といったケースも日常的に経験しているのではないだろうか。ウイルス検知・対策ソフトを導入し、明らかにされたセキュリティホールには修正プログラムでパッチをあてるような処理を怠ると、

取り返しのつかない結果を招くこともある。

第２のパターンは、特定の相手のコンピューター端末に対する機能撹乱・破壊を目指すものである。

マリシャス・コードが単なるいたずらとして用いられるのでなく、はっきりとした政治目的のために利用されるとすれば、もはやサイバーテロ、あるいはサイバー戦の領域に入っていると言っても過言ではないだろう。

今日、ネット上では、いわゆるDoS攻撃（Denial of Service Attacks）と呼ばれ、特定のコンピューターに処理能力以上の接続や処理要求を浴びせて負荷をかけ、サービス不能に追い込む手口も横行している。これがより巧妙になり、支配下におかれた不特定多数のコンピューターから特定の標的とされるコンピューターに、特定の時間に攻撃が行われるというDDoS攻撃（分散型DoS攻撃：Distributed Denial of Service Attacks）も試みられている。

なかでも2001年７月、米ホワイトハウスを狙ったDDoS攻撃は広く知られることになった。これは「コード・レッド(Code　Red)」と呼ばれるワームが多数のコンピューターからの集中的なアクセスによりホワイトハウスの公式ホームページをダウンさせようとしたものであった。ホワイトハウス側は「コード・レッドと呼ばれるコンピューター・ウイルスの影響を最小限に抑えるため、しかるべき予防策をとった」とのみコメントしているが、サイトのIPアドレスを変更することによって攻撃をかわしたと見られている。このほか、2001年中の出来事としては、日中間で歴史教科書問題を受けた日本の政府系ネットを狙った書き込みや改竄事件や、米中軍用機接触事件時に米中間のクラッカー同士で戦わされたネット上での攻撃合戦などは象徴的であり、米同時テロ後に見られた「E-ジハード（聖戦）」なども政治的色彩の強い行動であった。実際、事件直後に発生した強力なコンピューター・ウイルス「ニムダ（W32.Nimda）」の被害は世界中に広がり、これはサイバーテロではないか、ともっぱら懸念された。

ネットの世界に国境はない。しかし、さまざまなイシューで「クラッカー」と呼ばれる人々がナショナリスティックな対応を示している。相手国からの攻撃が国家的意思に基づくものなのかどうかは判定のしにくい問題ではあるが、ある特定の国から集団的で、同一的な攻撃が仕掛けられている場合、やはり相手国の関与のシナリオも検討の価値はある。

第３のパターンは、不特定の相手のコンピューター端末内の情報に対する不正アクセスであるが、これは上記のような不特定多数のコンピューター端末を動員してDoS攻撃をする前段階として、サイバーテロリストがポートスキャンなどをかけ、いつでも「踏み台」に利用できるセキュリティの甘いサーバーを監視し、ルート権限を奪取しておくなどといった行為は、こうした不正アクセス手段の結果といえよう。

最後に第４のパターンとして、特定の相手のコンピューター端末内の情報に対する不正ア

クセスの問題がある。これは、コンピューター端末の機能を麻痺させることが目的ではなく、端末の中に保存されている情報（データ）自体の価値に着目し、それを不正に窃取ないし改ざんするものである。

最近の深刻なケースの一例としては、日本でロケットや人工衛星の開発に携わる宇宙開発事業団でのコンピューターへの不正侵入事件がある。これは2001年の暮れ、事業団から衛星開発を受注したNEC東芝スペースシステム社の社員が、技術情報を記憶する事業団のコンピューターに不正アクセスしたうえ、ライバルの三菱電機の技術情報も盗み見していた、という事件であった。この場合、問題となったのは事業団のコンピューターにアクセスするためのパスワードであり、これが受注メーカーごとに事業団が割り当てていたのだが、それが自社のものから他社のものが推測できるほどの違いにとどまる、というお粗末な管理体制の結果でもあった（注2）。

今回の事件は2000年２月に施行された不正アクセス禁止法に抵触する可能性があったが、事業団側は「予備設計の段階で、致命的な機密情報はなかった」として、スペース社に指名停止１ヵ月の処分を科したのみで告訴は見送ったことから、知的財産保護意識の薄さや処分の甘さも指摘されている。

宇宙開発事業団のケースでは「機密情報ではない」ことが管理体制の甘さを生んだのかもしれないが、では、どの組織も機密情報に関しては保護が徹底しているのだろうか。サイバー空間で情報がいとも簡単にアクセスされ、窃取・改竄が行われている今日、ネットワークの保護による情報の保護がいかに重要かを改めて考える必要があるだろう。

(2) サイバー空間の脅威の特質

以上、４つに分類したサイバー空間のセキュリティ問題だが、これらを通して共通する特質に向けるならば、それらは次の５点にまとめられる。

第１は、不正行為を働こうとする主体の多様性と非対称性である。サイバー空間の「クラッカー」たちは、個人や非国家のグループであり、子供さえいる。そして、これらの個人やその集まりが非対称性を乗り越え、企業や国家を相手に攻撃をすることも多い。すなわち、個人レベルでのサイバー戦と国家レベルでのサイバー戦に本質的な差などなく、基本的には同一の手法・手口で行われていることがわかる。逆にいうならば、ITが個人と国家を同じ平面で対峙する空間を提供したわけである。ここでは、国家間で正規軍が互いに合理的な計算と選択をしながら安全保障利益の確保を求めるという、従来型の発想は通用しない。

第２は、匿名性である。サイバー空間でのテロ行為が発生し、犯行声明が出されたとする。しかし、それが真実かどうかを見極めることは極めて困難である。逆に、いたずらや犯罪を犯そうとする者は真っ先に偽装工作をするはずである。自らのIDを隠し、他人になりすま

すことも簡単にできる。ネットの中の迷宮で、匿名を通すことも可能なケースも多い。

第３は、サイバー空間の攻撃が、対象の物理的な破壊であるよりも、機能、あるいは信頼性に対する破壊であることを指摘できる。コンピューター端末が正常に機能しないようにすることは、ネットワークに依存している部分が重要であればあるほど、その機能不全によって失われる信頼は大きなものになるはずである。企業は、攻撃を受けたことが判明した場合、信頼・信用の失墜をおそれ、事件を公にしない可能性もある。重要インフラは、正常なコンピューター制御の下、機能するものである。それが不正侵入によって誤作動を起こしたとしたらどうだろうか。

第４は、こうした攻撃にかかる費用である。それが極めて低コストになっている。国家を防衛する軍隊がいかに強力で、堅牢で高価な装備を有していたとしても、民生用のコンピューターが鉄壁の守りをいとも簡単にすり抜けてしまうかもしれない。そうした現実は、1997年、米国防総省が実施した演習「エリジブル・レシーバー」の経験を思い起こせば容易に実感できる。「ハッカー」に扮した政府のスタッフは、民生用コンピューターと商用のインターネットを利用し、いとも簡単に米国の重要インフラや国防総省のネットワークシステムへのアクセスの痕跡を残すことができたという。この結果、国防総省の情報管理体制はかなり強化されたとされるが、いずれにしても、力による抑止の効かない新しい空間に対する理解を深めていかなければならない。

最後に第５には、これまでの４つの特質―それが従来型の安全保障問題の理解をいかに変えなければならないかを強調した―とは異なり、サイバー空間の問題でも、われわれのごく通常の政治空間と同様の視点で事態を理解する必要性があることを指摘しておきたい。というのも、たしかにサイバー空間を通じたコンピューター端末に対する機能撹乱や情報への不正アクセスなどはいずれも新しいタイプの攻撃ではあるが、上述のようにこれらが一定の政治目的をもった権威主体（体制）への反抗という動機によるものであれば、サイバー空間でのこともそうでない空間での行為も問題の図式に本質に変化はない。テロの首謀者たちは情報通信技術の高度化により、低コストで攻撃を実施できる手段を手にしたということである。したがって、防御する側としては、サイバー空間からの攻撃に対して技術的な対応をするのみならず、その攻撃を誘発している政治的な背景を理解し、それに対しても効果的な対応策を講じる必要がある。

もちろん、サイバー空間での不正行為のすべてに政治的な目的があるわけではない。むしろ、問題は「理由なき反抗」というべきか、政治性などなく、ただ単に自分が習熟した工学的技術の腕を誇示することだけが理由の、反社会的な行動がほとんどであることだろう。しかし、こうした反社会的な行動を封じる手がかりになるよう、首謀者に対し社会の秩序の維持を目指した法の支配を適用することはこれからの大きな課題になる。

４．サイバー空間の脅威への安全保障と危機管理

(1) 安全保障・危機管理思想の発想転換

これまでに見てきたように、サイバー空間での安全保障を脅かす主体は多様で、非対称的な性格をもつ上、身元を隠し、目に見えない攻撃によって標的となった相手のインフラの機能を破壊し、信頼を失墜させる、という特質がある。これがごく安価にできることから、事件は今日、日常的に発生してきている。これが今後、回線のブロードバンド化が普及し、インターネット人口が増加するとともに、IP（インターネット・プロトコル）バージョンも更新され、一般の家庭生活のほとんどの部分でコンピューター制御を受けることが可能になることにより、その裏面として社会の脆弱性も増すことになりかねない。このような状況下では、安全保障や危機管理のための従来の発想では限界があることも留意しておかなければならない。

では、通常の安全保障・危機管理思想ではどのような限界がありうるのか。これらについては、概ね次の３つを指摘できる。

第１は、リアリスト的「パワー（ハード・パワー)」の限界というべきものである。伝統的なリアリスト（現実主義）の観点は、軍事力に代表されるハードなパワーのバランスあるいは優越を達成することによって自らの安全を確保する、という思想が中心であった。この視点がまさに「現実主義」と理解され、法や社会制度の強化によって、いわば他律的に安全保障を考えることは理想主義的と考えられてきた。しかし、パワーのバランスや相対的な力関係というものは、国家対国家というように、対称的な主体間で、費用対効果の計算もある程度合理的にでき、優劣の差が歴然とする結果、紛争も起こるかもしれないが、その抑止も可能となる仕組みができていた。実際、核抑止の考え方は、決して好ましいものではなかったが、核戦争の回避には役立った。理想的には軍備の削減や軍縮の制度を確立することが有益だが、目の前にある軍備については、それをいかに効果的に使うか（そのなかには、実際に軍事力を使わずに相手を抑制・圧倒する、という発想も含まれる）を考えるのが、「現実主義」の立場であった。しかし、サイバー空間の発展によって、こうしたハードなパワーを用いる現実主義的な視点のみでは捉えられない「現実」が到来しているといえないだろうか。

第２は、技術的対応の重要性とその限界である。IT社会が技術集約的であるということは、そこに見出される多くの問題に技術的な観点からの対応策は不可欠だろう。しかし、それは必要条件であっても、十分条件にはなっていない。

技術的に不可欠な対応としては、暗号の利用、ファイアー・ウォールやウイルス対策ソフトの導入、OS・ソフトウェアの更新・修正などがある。これらの詳細は他に譲るとして、利用者の自己責任において、これらの手立ては最低限しておかなければならない。しかし、多くの技術者が指摘するように、技術面では攻撃技術と防戦・対策技術とでは、どうしても

後者が遅れをとることから、技術面以外の対応策についても講じる必要がある。

第３は、ネットにおけるレッセフェール（自由放任）型対応の限界である。これは、インターネットそのものが、レッセフェールを前提にした相互リンクの結果として生まれたことと大いに関係する。自発的な選択によってリンクを広げ、相互に便益を得ること基盤にした社会であり、そこには自然と「行動基準」や、あるいは、「ネチズン」(ネットワーク上の市民）としての自覚が一定の秩序（「ガヴァナンス」とも言うべきもの）を生み出している事実がある。結果的には自己責任の世界である。しかし、ネットワークが国家や社会の基盤を構成し、公的な利益をも脅かすほどの影響力を持つにいたった現在、すべてをレッセフェールと自己責任にまかせることは適切ではない。

こうして、「現実主義」の安全保障観も、技術集約的な対応も、レッセフェール型のインターネット社会の規律も、みな限界を迎えるなか、より広範な安全保障と危機管理の方策が求められることになる。次節では、それらについて検討する。

(2) 新しい安全保障と危機管理の方向性

誤解のないようにあえて指摘しておくならば、上記のような従来の安全保障や危機管理の体制について、これらの要素が今日その有用性をまったく失ったというわけではない。われわれをとりまく社会の脅威がサイバー空間からだけのことにとどまらず、通常の国際関係や国内での社会生活―インターネットの世界に浸っている人々の言葉を使えば「オンライン」ではなく「オフライン」の生活―での危機も多いこともあるが、ネット犯罪やサイバーテロ、サイバー戦の背景にナショナリズムや国際問題、政治目的がある場合もあることから、上記の対策は依然として有益に作用することを見落としてはならない。問題は、サイバー空間での脅威が拡大することにより、これまでの対応策に加え、新たな手法も追加しなければならないことである。ここでは、次の４点を取り上げたい。

第１は、「ハード・パワー」に加え、「ソフト・パワー」の有用性を再評価することである。「ソフト・パワー」とは、軍事力のような物理的・物質的な力ではないが、アイデア、価値観、規範、倫理観などが持つ力と言えるだろうか。これらは、社会制度ができるときの知的な基盤を提供するものであり、人間が生み出すものである。サイバー空間の安全保障と危機管理にあたっては、具体的にはサイバー攻撃やサイバーテロを「非正当化」する論理と、そうした反社会的な行動を「非合法化」する新しい発想を発展させていくべきだろう。「ソフト・パワー」は、そうした努力を促すダイナミズムを持っている。そして、「ソフト・パワー」の有用性をしっかりと再評価することは、新しい価値観に基づく制度―特に法制度―の構築をももたらすことだろう。こうして、サイバー空間にも「法の支配」が広がる糸口を作り出すことができる。

サイバー空間の「自由」が失われてよいわけではないが、過度の自由が混乱をもたらすのであれば、一定の規律は必要となる。合理的な範囲の法制度（あるいは法的に担保された防衛体制）が整備されるのであれば、いままで「レッセフェール」の紳士協定や行動基準にまかされていた部分でも、より公共性の高い分野については具体的な規制を作ることが不正行為の抑止や効果的な罰則につながるのではないだろうか。

もちろん、ネットを規律する法律がこれまでまったくないわけではない。わが国では、データの消去やホームページの書き換えなどには刑法の電子計算機損害等業務妨害罪や電磁的記録毀棄罪などを適用できるが、実際の被害がない段階で重大な犯罪行為の「予備」や「未遂」を罰する規定はないこと、2000年２月に施行された不正アクセス禁止法は、「ネットワークの信頼性」の保護が目的でもあるため、ネットワークにつながっていないシステムに侵入しても罰せられないこと、などの問題点はすでに指摘されている(注３)。韓国では重要インフラに対するサイバー攻撃を犯罪として取り締まる「重要インフラ保護法」の立法化も進められているという。また、欧州評議会は2001年11月８日にサイバー犯罪防止条約を採択しているが、わが国も引き続き国内の法的な体制整備を進めていく一方、日米やG８、OECD、国連など国際的な文脈での協力体制の強化といった努力もまた、早急に期待される。

第２には、結果管理としての危機管理体制の強化の必要性を取り上げたい。先に論じたように、高度技術を用いた攻撃に対し、技術本位の対応策（暗号やファイアー・ウォール、ウイルス対策ソフト、OS・ソウトウェアの更新・修正など）が不可欠である反面、それだけでは不十分であった。防御側の技術革新は決して怠ってはならないが、それと同時に、ネットワークが広く公開されている限りにおいて被害は不可避である、という認識に立ち、被害が発生した際にその結果を最小限にとどめる努力―結果管理―を導入することも見落してはならないだろう。これらは、リダンダンシーを確保し、被害の波及の阻止、バックアップ体制の強化などを行うことである。

第３は、ネットからの隔絶である。これは、ネットワーク社会に逆行する動きのように見られるが、真に大切な情報を何も公開の場においておく必要はない。サイバー空間を狙う不正行為の首謀者は、ある意味で民主的で開放的な社会の利点を最大限に悪用していると言えるだろう。こうした開放的な社会の脆弱性から自らを守る手立てとして、コンピューターを複数管理し、ネットワークにつながないものもしっかりと（しかも、リダンダントなかたちで）保護しておくべきだろう。(もっとも、ここでも内部犯の問題は避け得ないので、適切な対応は必要だが。)

IT革命は、われわれの社会に大きな便益をもたらしたが、その反面、ネット自体が社会基盤を構成し、われわれの生活がそこに大きく依存することによってさまざまなリスクや安全保障上の脅威がもたらされることになったことも否定できない。しかし、われわれにとって

「IT以前」の社会に後戻りするオプションが合理的でも現実的でもない以上、発想を柔軟にした対応策を講じていくほかはない。本研究は、サイバー空間の果たす役割の比重が高まるなかで顕在化しつつある脅威のパターンを分析し、危機管理のあり方について再検討するものであったが、ネットを用いる一人ひとりの意識変革と政府としての安全保障・危機管理政策の強化につながる問題提起ができたとすれば、幸いである。

－ 注 －

1．米トレンドマイクロ社の「トレンド・ワールド・ヴァイラス・トラッキング・センター」のサイトでは、常時、危険なウイルスのトップ10リストを発表している。http://wtc.trendmicro.com/wtc/

2．「不正アクセス―宇宙開発事業団で発覚、甘過ぎる先端技術の情報管理」『読売新聞』2002年２月21日。

3．杉浦美香「サイバーテロの脅威―日本の防御は十分か（４）越境するネット犯罪」『産経新聞』2001年10月６日。

－ 付 記 －

コンピューターやインターネットの世界は、専門の技術用語も多く、近づきがたい印象をわれわれに与えるが、比較的平易にパソコンの知識や情報セキュリティ関係の動きを理解を促進するものとして、筆者にとって有用だったサイトを参考までに次に列挙しておく。

もちろん、筆者は、これらのサイトの情報が常に正確であると保証する立場にはなく、これもサイトの管理者とそのサイトを利用するものの責任において利用していただくほかはないが、一般に有益と考えられる情報も多いと言える。

―「アスキー デジタル用語辞典」

基礎的なパソコン用語から難しい専門用語まで、コンピューターに関する用語を幅広く収録したインターネット上の用語辞典。収録されている用語は（株）アスキー発行の雑誌や書籍、Webサイトなどから集められているため、それぞれのジャンルに詳しい編集者がチェックしていることに自信をもっている様子。内容の更新も随時行われている。

URL：http://yougo.ascii24.com

―「ブロードバンドセキュリティ倶楽部」

ウイルス対策ソフトを開発・販売しているトレンドマイクロ社のサイト。ブロードバンド時代

のセキュリティ問題の解説、ウイルス警報、駆除･修復方法などを紹介している。

URL：http://www.trendmicro.co.jp/broadband/index.asp

―情報セキュリティ関係のニュースなどは、以下のところが詳しい。

iDEFENSE　URL：http://www.idefense.co.jp/　（日本）

http://www.idefense.com/　（米国）

HotWired Japan　URL： http://www.hotwired.co.jp/news/

CNET Japan　URL： http://japan.cnet.com/

－ 付　録 －

筆者は、2001年12月５日に外務省企画課主催（日本国際問題研究所共催）のシンポジウム「情報通信技術（IT）と外交」の第２セッション「ITと安全保障」にパネリストとして参加したが、そのシンポジウムでの議論や筆者の発言を次のエッセイにまとめた経緯があるため、ここに再録しておきたい。

なお、同エッセイは、『グローバル・ヴィジョン』誌（2001年２月号、東京経営経済出版社）に掲載されたものである。

「ＩＴとＲＭＡと外交」

IT革命といわれ、目覚しい進歩が続く情報技術は、国際関係にどのような影響を及ぼし、外交はそれにどう対応すべきなのだろうか。

米国では９･11同時テロ事件のあおりで急速な消費の冷え込みや失業率の増加が生じたが、もともと景気は事件前から減速傾向を見せ始めており、その主な要因にはITﾊﾞﾌﾞﾙの崩壊やIT不況が指摘されていた。だが、これは、コンピューター関連のハードやソフトが米国の生活のなかにすっかり浸透し、市場が飽和状態になっていることは意味しても、ITに対する社会の依存度が下がったことを指し示すわけではない。むしろ、テロ事件のあと、「次はサイバー攻撃か」と心配されたように、われわれは情報ネットワークが日常生活を支える重要インフラと切り離せない事実の重みをかみしめるべきときにあるといえる。

昨年（2001年）12月５日、外務省主催で「ITと外交」シンポジウムが開かれ、筆者もパネリストとして出席する機会を得たが、そこでは、中国やインドの動向を展望した「ITと21世紀のアジア」に関するセッションとあわせ、「ITと安全保障」に関しても活発な議論が行われた。

安全保障については、特に「情報RMAの現状」と「サイバー戦の脅威とその対策」の２つの観点から問題への接近が試みられた。

「RMA」とは「軍事革命（レボリューション・イン・ミリタリー・アフェアーズ)」の略で、技術の高度化が軍事戦略や作戦行動に及ぼす変革のこと。米国では技術革新の展望を組み込んだ軍事・安全保障政策の見直しがさかんになっている。ラムズフェルド国防長官らが中心となって推進するミサイル防衛構想などは、高度技術を統合的に用いるRMAの代表格と言える。そして、一連のRMAの原動力になったのが、情報関連技術の飛躍的な進展であった。

この問題についてシンポジウムで現状報告に立ったジャン・ローダル米ローダル社会長（元筆頭国防次官代理）は、精密誘導ミサイルの開発や通信分野での劇的な前進がもたらした変化を強調していた。実際、標的への命中精度は湾岸戦争のときよりも格段に向上してきているという。

この結果、味方の犠牲や相手方に対する付随的ダメージを極力抑えることが可能となった。また、センサー技術の発達により、作戦行動がとられている現場の状況をより正確に一人ひとりの米軍要員に伝えられるようになった、との話もあった。

このように米国が最先端の軍事革命を取り込み、有利に作戦を展開できるようになったため、正規軍同士による伝統的なイメージの戦争はもはや過去のものになった、とローダル氏は指摘した。

革命の裏側

しかし、とローダル氏が次に強調したことは、「９月11日」以来、技術面でのリードだけでは安全が確保できない現実もあるということだった。RMAがあれば何でもできるわけではなく、事実、アフガニスタンの山岳地帯の洞窟に潜むテロリストを見つけ出すことに米国はてこずっている。タリバン政権を物理的に破壊することはできても、テロリストを捕捉する能力にはかなりの限界がある。

さらに、情報技術の進歩がテロリストを利する側面があることも見逃せない。

ローダル氏に続き、サイバー戦をめぐる諸問題について報告した通信総合研究所の三輪伸介研究員が語ったように、インターネットがオープンなネットワークへのコンピューターシステムの接続を前提にし、しかも、われわれの生活を支えるライフラインも含め、多くのシステムがコンピューター制御されていることから、サイバー戦は、「いつでも起こりうる現実の脅威」になっている。

「戦争」という言葉を安易に用いることは好ましくないにしても、上述のように、「媒体としてのネット」を介し、「基盤としてのネット」を狙った攻撃は、いまや日常的になっている。その手口は、盗聴、改ざん、なりすまし、不正アクセス、サービス妨害、と多岐にわたる。

また、サイバー空間での脅威は、子供のいたずらからサイバー犯罪、サイバーテロ、情報戦とさまざまの可能性があるが、三輪研究員が指摘するように、インターネット上ではいたずら目的に使われるのと同じ手段がサイバーテロにも利用できるという特徴がある。これは、サイバー空間ならではで、ふつうの世界ではいたずら目的でミサイルが使われるようなことはまずないだろう。ネットが善用も悪用も可能な共通のインフラであることが、われわれの対応を難しくする。

もちろん、われわれとしてネットが不正に使用されるのを手をこまねいて見ているわけにいかない。暗号の利用や、不要な通信を排除する「ファイアー・ウォール」の設置、侵入検知システム（IDS)、ウィルスチェックシステム、セキュリティ監査ツール、OS・ソフトウェアの更新・修正など、技術面での対応は不可欠になっている。

だが、問題は、三輪研究員（通信総合研究所）も正しく指摘したように、これらの防御手段は

完璧ではないし、インターネット技術のみでは防げない攻撃もあることだ。そこで、「攻撃による被害を想定した危機管理」が重要となる。同研究員の報告では、インターネットにおける危機管理を、準備（情報セキュリティ対策)・対応（対応チームの設置)・復旧（バックアップ・システムなど)・防止（教育・啓蒙活動など）という４側面が紹介された。

世界貿易センタービルがテロ攻撃（これは物理的な攻撃だったが）で倒壊したとき、ビルに入居していた企業のなかには重要データをしっかりと他の場所でバックアップ保管をしていたものも多かったという。わが国では、危機の予防とともに、どれほど復旧のための手立てがとられているのだろうか。

情報危機管理については内閣官房情報セキュリティ対策推進室で一連のプランが進められているが、各個人や企業の努力もおろそかにできない。

「外交革命」へ

今回のシンポジウムは、サイバー空間の安全保障と今後の外交のあり方を検討するうえで有益な機会となった。IT革命と安全保障ないし外交の問題は、筆者も平素から強い関心をいだいている分野だが、国際政治の観点からシンポジウムのテーマとの関連で自分なりの考えをまとめると、概ね次の３点がある。

第１は、サイバー空間での「応酬」が国際政治においても日常化している現実を直視する必要性である。中国・天安門事件がたまたま現場に居合わせたCNNテレビが生中継をした最初のケースならば、コソボ紛争がネットで情報戦が展開された最初、という研究を見たことがあったが、これからはネットを抜きにした安全保障や外交は考えられない―逆にいえば、インターネットを外交により積極的に用いるべき―だろう。

第２は、テロリストのように非国家の主体が国家・非国家の区別のないネットを使って起こすさまざまな脅威に対し、わが国をはじめ、国家が国家だからこそ発揮できる能力を用いた対応を進める必要性である。ここでは、国際関係における「法の支配」の徹底が重要だ。技術的な防御に加え、ネット上の不正行為を具体的に取り締まる制度構築がこれからの急務である。

第３は、外交における「情報」面での優位性、という古くて新しい問題への再認識がある。「IT」というと、どうも技術の側面にばかり目が行きそうだが、（インテリジェンス情報の分析を含め）正しい情報の把握、バランスのとれた国益観や時代の要請に対応した新しい規範意識の醸成、文化・文明の壁を対立・対決の口実にさせない「文際的」理解の促進など、ソフトの部分こそ重要になる。

IT革命を軍事面でのハード・パワーの強化にとどめるのでなく、「情報力」を駆使した「外交革命」に用いる努力にもぜひとも期待したい。