講演録　法的側面から見たサイバーテロ

橋本　靖明
防衛庁防衛研究所
第１研究部第２研究室主任研究官

注：本章は、2001年11月12日に日本国際問題研究所において開催された研究会での講演内容を収録したものである。

１．はじめに

テロリズムとは一般的に、政府や革命団体が第三者に恐怖状況をつくりだし、その恐怖感をもって政治的目的を達成しようとする手段である。ある意味、政治活動だが、暴力的なものと言えよう。また、100年以上の歴史を持つ国際法学会が、つい最近編集した『国際関係法辞典』では、この他に「特定の私人、人や団体に資金、武器、サンクチュアリ（聖域）を提供することによって国家が支援するテロ活動もテロリズムの中に含まれる」という定義づけをしている。国家テロという言葉で表現されるようなことも、今ではテロに含まれている。

９月11日の米国同時多発テロでは、もし飛行機の代わりにコンピューターとネットワークが使われていればサイバーテロとなるが、その主体が誰かという問題が生じる。９.11事件の場合には、犯人だと見られているテロリスト・グループのアルカイダが、アフガニスタンのタリバン政権の支援を受けていると考えれば、まさに『国際関係法辞典』が定義するところの「国家が支援するテロ活動」になる。そうなればアフガニスタンはテロ支援国家として国際法上も責任を問われるということになる。

国際法は良くも悪くも国家の視点から見るせいもあるが、国家テロは基本的に、ある国家が特定の政治的効果をもたらすための手段としてテロを用いることを指すのであって、主体はあくまでも国家である。つまり、国家が自分たちの政治的主張を行うためにテロリストを支援して雇っているという発想に基づいている。これに対し、今回のアフガニスタンのタリバン政権とアルカイダの関係は今までとやや異なり、主と従が逆転しているのではないかと一般に言われている。そうすると、従来の捉え方で言う国家テロと、今回のアルカイダの行ったとされるテロが同じなのか。同じでないとするならば、国際法がこれまで考えていたテロと同列で議論できるものなのか。対応のための法的根拠も同じでいいのか、という問題が出てくる。こうした意味で、今回の９月11日以降、概念の動揺が見られつつあるのではないかと思う。

２．サイバーテロ

従来のテロは、大規模なテロをしようとすればするほど、まず組織化が必要であった。単発的な、例えば暴漢が誰かに襲いかかる程度のものでは恐怖感を植えつけられないし、特定の政治目的は達成できない。それに対し、サイバーテロは、近年急速に発達してきたコンピューターとインターネットというネットワーク技術に専ら依存し、また、肉体的訓練も必要としないので、机上で実行可能である点が注目に値する。

また、サイバーテロは、小規模な資金で済むことも特徴の１つである。アルカイダがやったと言われる今回の問題に関しては、航空機操縦のためのトレーニングに費やした時間も費用も大きなものだが、サイバーテロの場合にはそれが不要となる。

防衛研究所で実施した研究会で聞いた富士通の技術者の話では、サイバーテロを行うには、１人の天才エンジニアを雇えばよいということだった。天才であることは条件なようだが、アイデアを出せる人間が１人いれば、何千人の凡庸なエンジニアがいる守備側にも勝る攻撃力を持つことができる。これがサイバーの最大の特徴となる。また、今回のような実体的なテロであったとしても、そのための資金をサイバー犯罪によって調達していることもあり得る。ただ、これはいわゆるサイバー犯罪によってお金を上手に転がしていることとなり、サイバーテロではないかもしれないが、付随した問題としてもこういうものがある。

そして、サイバーテロの対象も多様である。例えば、特定の国家の軍事施設を守っている、もしくは軍事施設を動かしているコンピューター・ネットワークのシステム部分を破壊することも、あるいは社会のインフラ一般に対して攻撃をかけることも、サイバーテロの対象となるだろう。そのためには、攻撃をかけようとしているシステムに侵入したり、データやプログラムを改ざんしたり、さらにその改ざんがチェックできないように隠す手段を取ることにもなるはずである。ある技術者に聞いたところでは、今やコンピューターの技術も進んでいるので、定期的もしくは不定期的にプログラムのチェック（指紋照合）をするという。これにより、テロリストやハッカー、クラッカーたちがプログラムに侵入すると、指紋が違っているのですぐ分かってしまう。しかし、その傷口を上手く覆う指紋のマスクの様なものがあれば見た目は同じなので、機械が機械的にチェックする限りは改ざんされているように見えない、ということもあり得る。

また、特に国家を限定せずに、世界中のネットワークを混乱に陥れることも可能である。大学生がやったと言われるフィリピン発のI Love Youウイルスがその一例だが、この事件では、何か具体的な犯行目的があるというわけではなかった。もし事件が何かの政治目的を達成するために世界中を混乱に陥れるというものであったならばテロ活動と言える内容だったかもしれない。さらに、今回の同時多発テロ直後に蔓延したNimdaウイルスも、同様に世界中のコンピューター・システムを、官・民、官の軍事部門・民事部門を問わず、ひたすらつぶして回った。復旧に

ある程度の時間と費用が必要となるので、それに煩わされている間に何かを起こすこともできる。つまり、テロリストの目的は、ネットワークを麻痺させ、特定のデータベースを改ざん・破壊することにある。そしてこれらの結果、軍事システムの中心機能やコントロール機能といった軍事のハードに関わる部分を麻痺させることも、社会インフラの最も基本的な部分にある、例えば交通管理システムや金融システムを破壊することもできる。もしくはその兆候をちらつかせるだけでも、彼らは全てのシステムをチェックし直すことになるので、脅しの効果が非常に高い。さらに言えば、金融システムを不法にデータ改ざんすることにより、当面の活動費を他人の口座から入手したり、無いはずの金をつくり出すことも、場合によっては可能である。

その他、サイバーテロの特徴には、攻撃からだいぶ時間が経った後でテロの被害が明らかになる危険性もあると思う。例えば、製鋼所の高炉温度調整のコンピューターを操作して高炉の温度を変えると、鉄の特性が微妙に変わり、設計された強度に達しないことがあり、地震で曲がったり、あるいはこれが圧延されて軍艦の一部として利用されたら、波などで曲がることも起こり得る。そのように、サイバーテロは、目的は同じだったとしても、結果が曖昧で広範な点は今までのテロの比ではない。政治的効果という意味では、攻撃を受けたことが判明した時点でその政治効果の達成は終わっているかもしれないので、それが密接にリンクしているかどうかは別だが、しかし、我々がその辺までは気がついていない部分が問題だと言えるだろう。

もう１つの特徴は、それが見えないことだ。決して仮想ではなく実体としてネットワークがあるのだが、あくまでもサイバー空間と言われるネットワーク上で起こるために、見えない恐怖が社会的にもたらされるのがサイバーテロの特徴である。

３．サイバーテロと法制度

(1) 犯罪としてのサイバーテロ

国際法上は、基本的にはサイバーテロもいわゆるテロの一種であり、テロ犯罪としての取り組みを行うことになろう。テロに関しては、国連を中心として、ハイジャック等を含めて10を超えるテロ対策条約がつくられ、最近のマネーロンダリングに関する条約についても、今度、日本が入ることになっている。世界中どこにいてもテロ活動をした者は犯罪者であり、逮捕されればその国で裁判を受けて処罰されるか、もしくは行為を行った土地ないし身柄を要求する国に引き渡され、刑務所に収監される。政治的な主張はテロ活動によってではなく、あくまでも民主的に行ってほしいというのが、今までの取り組みだった。

９月11日の事件に戻ると、これはサイバーテロの話と別なのだが、そこに本当は矛盾がある。今までのハイジャッカーにはそれなりの仁義があり、ハイジャック機とその乗員・乗客の人命とを引き換えに政治的要求を行い、その結果、お金を手に入れたり、捕らえられていた活動家が解放されれば人質を解放していた。しかし、今回の場合は、ハイジャッカーであってハイジャッカ

ーではない。すなわち、人質が解放される可能性は皆無で、かつ、犯罪者が自ら死んでしまっては刑を適用することもできず、今までのテロ対策の条約ではカバーできない。そういう意味では今回のテロは、今まで国連が30年以上努力してきたテロ対策の条約システムに対する、挑戦であった。

サイバーテロについても、国際社会は基本的には、これを犯罪扱いしようとしていたのではないかと思う。今年、サイバー犯罪を国際的に取り締まるため、欧州評議会が欧州サイバー犯罪条約をつくっている。(この会議には日本、アメリカ、カナダ、南アがオブザーバー参加。)欧州各国と日本・カナダ・アメリカが入ると、北半球のインターネット先進国とも言える国々をカバーできる。これにロシアが加われば、北半球の国はカバーできるくらいの条約案である。この条約は、違法アクセスや違法傍受、データ妨害、システム妨害などが規制対象で、これらを犯罪として扱おうとしている。欧州が主体だが、今まで国連を中心に行ってきた犯罪に関するテロ条約の思想的延長上にある。

国内においても法的にサイバー犯罪を規制しようとする動きはあり、結果としてサイバーテロにも繋がるようなことは許さないという網ができてきている。日本でも平成11年に不正アクセス禁止法ができて、サイバー・ネットワークを利用して第三者のコンピューター・システムに侵入したり、書き換えたりすることは法的に禁じられ、各システム管理者はそのためのシステム構築をせよ、その能力がない場合には都道府県や国が協力せよということが決まっており、各国とも同様のことを行っている。米国は今回のテロ事件を受けて、FBIによる通信傍受が許されたが、先進国であるほどサイバー犯罪に対する法的システムが国内的にできているということは、一般論として正しいと思う。

しかし問題点もある。そもそも、インターネットにはシステム管理者がおらず、それ故に急速に広がることができるという矛盾した性質を持っている。また、技術的にはパケット方式といって、１つのデータであってもその都度小分けにし、空いた回線を通しているので、どの国を通ってどう回っているかが分からない。したがって、システム管理者がいない中では、犯罪がどこをどう経由してきたのかも分かりづらい。ネットワーク犯罪者は各々のコンピューターが持つ固有の番号、IPアドレスを詐称することが多いので、そのアドレスを突き止めても犯罪者逮捕には繋がらない場合もあり、法律をつくったところでどの程度カバーできるかについては常に問題となる。

さらに、サイバーテロのもたらす被害や効果が一国の経済や社会をひっくり返す程大規模であるにもかかわらず、今までのような犯罪という扱いでいいのか、犯罪だけで取り締まれるのかという問題が出てくる。

(2) サイバーテロと国際法

（ア）自衛権

ここで「自衛権」という言葉に注目したい。当初、私はこの言葉を持ち出すことに非常に懐疑的だったが、米国同時多発テロ以後、ポピュラーなテロ対策の用語になってしまったこともあり、再検証する必要があると考えている。

国際法学会の『国際関係法辞典』は冷戦終結直後に出版されたので、改訂後まだ10年も経っていないが、そこでは基本的に、自衛権は国対国の関係だと規定している。もちろん国対準国家のようなものはある。例えば反乱団体、国家に準じる団体の場合にはそれが適用されるが、基本的には国対国である。この概念をテロリスト・グループにも適用できるかという点は、長い間問題ではあった。例えば米国の場合には、1980年代の半ばごろから、テロリストにしばしば米国の在外公館などが攻撃される事態が続いた。最初は米国も国際法に鑑み、これを犯罪として扱おうとしていたが、それでは埒があかず、戦争ということにしてしまった。それ以降、米国はテロを戦争だと考えて対策を取っている。このため、今回の同時多発テロに対しても米国は、サイバーテロではないが、ストレートに自衛権という言葉を持ち出した。一方、米国が自衛権を持ち出すことについて、他の国（例えば、欧州各国）は今まで積極的な肯定も否定もしていなかった。例えば、在アフリカの米国大使館数カ所が、アルカイダに自爆テロを含む爆弾で攻撃され、負傷者が2,000人に上る事件があったが、これに対し米国が自衛権を援用してトマホーク・ミサイルを撃った際も、欧州各国の反応は冷ややかだった。しかし、今回の同時多発テロの場合、テロの首謀者が同一（アルカイダ）であるにもかかわらず、NATO諸国がすぐに自衛権を容認してしまった。そこが１つの大きな転換であり、注目すべき点であると思う。

大使館はテロの対象として常に狙われる立場にあるので、米国は海兵隊員を各大使館に張り付けている。ところが今回の場合、世界貿易センターという民間の、しかも約80カ国という様々な国籍の企業が入ったビジネス施設が攻撃されたにもかかわらず、当初は犯人も目的も分からなかった。つまり、無防備な我々にもいつ何が起こるか分からないという、まさにテロリストが狙った以上の恐怖が、米国のみならず世界中の国々に広がったという特徴がある。その結果、各国とも、何が理由かはしかとは分からないが、気に入らないと思われた国は、民間人が無差別に攻撃されるかもしれないという一種の恐怖感を持たされた。その恐怖感が自衛権を容認させた理由ではないだろうか。

そこで１つ注目すべきは、事件の翌日に国連安保理で緊急に採択された決議である。これは前文で、「個別的集団的自衛権の存在」に触れている。ただ、湾岸戦争時の決議のように、それに基づいて何かを行うことを各国にオーソライズ（授権）するとは言っていないが、それをもとに活動することもあり得るということを国連安保理もいち早く認めたことになる。もちろん、米国が安保理の常任理事国の１つということもあるだろうが、いずれにしてもそれを主要各国が認め

たことは一つの変化だろう。動揺の意識が反映されたのではないか。

その後も、アナン国連事務総長は総会で、これは人類社会全体に対する攻撃だと、ことある毎に強調している。それは本件は国連に関与させよという気持ちの表れかもしれないが、何にしても、これは米国だけの問題ではないと国際社会全体が認めてしまったことが、米国の個別的自衛権の行使を、初めてNATO条約を使って西欧諸国が認めたことに繋がったのだと思う。

サイバーテロに関しても、同様の判断がなされると思う。それはなぜかと言うと、サイバーテロの特徴として、特定の目的があったとしても、特定の相手だけに限定された被害を及ぼすこともできれば、その被害を社会インフラや一般に広げることもできる。それくらい変幻自在に使い得る危険性を孕むのがサイバーテロなので、今回の様なテロ事件が起こった場合に、自衛権も使えない、犯罪として取り上げてもあまり効果があるとは思えない、では何ができるのだという問題が出てくる。だから、今回の９月11日の事件は実は非常に重要だったし、その後、集団的自衛権をヨーロッパ諸国が認めたことも非常に重要な意味を持つと思う。

（イ）集団安全保障体制の適用は可能か？

自衛権の行使についてどこかで考える必要があるのではないだろうか。なぜなら、自衛権は基本的には国家対国家、もしくは国家と国家に準ずる間の話であって、今まで日本も有してきたように、自衛権は相手が組織的かつ継続的に武力行使を行ってきた時にそれを排除しようとする、国家に与えられた権利である。それを、例えばある国から独立しようと活動しているわけでもない、アルカイダのようなテロリスト・グループに対して当てはめるのは、やはりどこかに違和感がある。

また、国際法が自衛権をどう扱ってきたかというと、カロライン号事件（注1）のような古い時から、国家間の紛争は話し合いで解決せよ、戦争に訴えてはいけない、ということになっている。かつては、例えば自国民保護のために自衛権を主張して軍隊を派遣したこともあった。それが本当に自国民保護のためだけでなく、それを理由に居座ってしまって相手の国をどうこうすることにも使われてきた歴史があったので、それらを排除していった。そして第２次世界大戦後、自衛権は、相手が武力行使をしてきた時にそれをはねのけるという、まさに日本が認めている個別的自衛権と同じことになった。しかも自衛権を行使した場合には、すぐ国連安保理に報告せよ、国連安保理がそれに代わる手段を取り始めたら、そこでやめよ、とされている。つまり対象も限定されているし、時間的にもある意味、限定されている。そうした歴史を考えれば、そこまで100年以上かけて自衛権の適用範囲を狭めてきたのに、他に手段がないからといってまた曖昧に広げるのは、法律家側からするとちょっと悔しいという部分がある。その結果、では何らかの法的手当てが必要になるかどうかを検討してみようとなるわけである。

そこで、今回の集団的自衛権に関して欧州諸国が容認したのと同様の理由が使えるかと思う。

自衛権とはあくまでも個別または一部の国家に集団的自衛権として認められるものであることを考えると、より広範にテロを国際犯罪として扱ったのと同様の、国際的な「平和に対する脅威」であるという方向から手当てが取れないだろうか。これはサイバーテロのように、今回のテロ以上に広範な被害が及ぼされるような場合には（例えばI Love You ウイルスのように国境を越え広がってしまうものがテロと結びつくような場合には)、これらを今度は国際犯罪ではなくて国際的な「平和に対する破壊」行為であると認定し、各国がある何らかの権威づけを得て、軍をもってそのテロリスト・グループに対抗する手段を取っても、それは自衛権に基づくのではなく、あくまでも国際の平和を維持するために認められる特殊な軍事活動であると言えないだろうか。

非常に回りくどい言い方だが、ある部分、これは警察的な活動にもなると思う。犯罪者が一国の軍隊に匹敵するような暴力を行使している時には、警察だけでは対応しかねる。しかも、一国だけの話ではないので、国際的に権威づけられた、場合によっては軍隊を使った軍事活動を含む対テロ活動ということで言えないだろうかと思う。

ここまでの議論で分かるように、私が個人的に想定しているのは、自衛権によってどこまでも突っ走らせるべきではなく、安保理なりがこれに関して各国に活動をとってよいと承認すべきだということである。そうなれば、各国協調して、できる国とできない国がもちろんあるだろうが、それぞれの国がそれぞれの範囲内で、犯罪対策の面からも、軍事的能力を使うという面からも、最大限の努力を発揮して、テロを封じ込める活動ができるのではないか。

この発想によって、集団安全保障体制が再生できるのではないかと思っている。国連自身は集団安全保障体制をつくりたかったが、いきなり冷戦、東西対立が始まってしまった。今回の９.11事件や今後起こるかもしれないサイバーテロは、むしろ国際的な関心事項であるはずで、これに対して集団的自衛権のような、基本的にはブロック対立の中で出てきたものではなく、集団安全保障というものの発想をもう一度思い出し、それについて各国がどこまで統一された行動を行い得るかは別問題だが、理念づけとしてそこから出ていくとすれば、それぞれの国がそれぞれできる範囲で、ある部分は資金の流れを止める。ある部分は出入国管理を厳しくして、不審な人間が入って来ないようにする。実力を行使できる国同士で協調しながら、テロリスト支援国家に対して何らかの強制的な手段を取る。その強制的な手段は単純につぶすという意味ではなくて、その後その国にテロリストを支援する状況が起きないように、後の国家建設も含めた形のものが一連の流れとしてある。縦横に、時間的・活動的・地理的にも広くという意味では、集団安全保障という考え方の基本に帰って活動することが必要ではないか、できるのではないかと考えている。

何にしても自衛権には、それを使いたいと思うとどこまでも使えてしまうかもしれない恐れがあって、しかも国連安保理が動かない限りは続いてしまう。特に米国のように安保理常任理事国だと、安保理を動かさないために拒否権を使うとちらつかせ、差し当たって自衛権の行使しかな

いことを認めさせた上で、無理を通してくるのではないかという懸念がある。

４．まとめ

まとめると、サイバーテロの特徴の一つには、実行者が多様であって、しかもその区別がつかないことがある。天才のいたずらっ子が、テロではないけれども、いたずら心からどこかのシステムを麻痺させてしまうことも可能である。そのときにシステム管理者は必ず、テロリストかもしれないと疑う。国もそう疑うはずである。しかし、調べてみたらどこかの10歳そこそこの少年だったという可能性はあるわけだが、結果として多大な被害が発生している。そういう意味では、実行者の意図も、それから実行者そのものも多様で、結果として莫大な損害が出るのがサイバーテロである。

こうした多様性を考えると、サイバー空間における犯罪という問題と、サイバー空間のテロという問題と、サイバーテロではなくて国家が行うサイバー攻撃、ミサイルを同時に撃つとか、ミサイルは撃たずとも、ある国を壊滅させようという攻撃意図を持ってサイバー上で何かをすることもあり得るわけだから、犯罪があり、テロがあり、武力攻撃に匹敵するサイバー攻撃もある。今後、そうしたものがすべて無秩序なサイバー空間の中では起こり得るわけだから、それらをすべて同時並行的に捉えて制度的にも技術的にも対応していかないと、結局その対応のどこかが空いていると、その空いたところにサイバーテロが行われた時には対処不可能であって、被害だけが残ることになる。

とはいえ、その対応のためのマトリクスをいくら組んだところで、そのマトリクスを重箱の隅を突くようにして調べ、見つけた穴から突っ込むのがテロリストである。だからテロの対策はサイバーも含めて、迂遠のようだけれども可能性を一つ一つ潰していって、テロリスト側に、これを突き崩すのはなかなか大変だぞと思わせることしかないかもしれない。実効的な対応はそういう形で縦横斜めに、できるだけのものを組み合わせてやっていくことになろうかと思う。

－　注　－

１．カロライン号事件（1837年)：英領カナダが英国からの独立を目指して英国と交戦中、カナダ独立の運動家は米国に拠点をおき、米国の民間船であるカロライン号を雇い、カナダと米国間を行き来していた。そのカロライン号を、英国が米国領水内で攻撃し、ナイアガラ滝に落とした事件。英国は自衛権と自己保存権を援用して弁護に努めたが、結局、英国が米国に陳謝する形で双方が納得して落着した。

＜以下質疑応答＞

（問）９.11事件に関し、NATO諸国が、米国の自衛権行使を容認したのは、今回の攻撃が米国本土に対するものだったことと関係あるか？

（答）あるかもしれない。以前、アルカイダが、米国の在外公館を攻撃した場合とは違う、と考えた可能性もある。自衛権そのものの容認云々という問題については、「急迫不正な侵害」をするのは基本的には国だけなのかという話に戻る。今回の場合は相手が国ではないが、国が攻撃したのと同じくらいの被害があったのに、自衛権が使えないからとして何をもっても反応できないのは、まさに「憲法を守って国が滅ぶ」のと同じことにもなりかねないのでおかしい、という議論になると思う。

米国は従来、自衛権はいわゆる他の国際法上の権利とは別であって、国家が存続する以上、行使して当然のものという発想をしている。つまり、米国が考える自衛権は、むしろ自己保存だと思う。かつて自存権といっていた権利に近い。米国はその時代から、この権利については必要があれば行使すると言っていたので、今回もその連続になるわけである。

（問）正当防衛の要件は、急迫不正の侵害に対してやむことをえざる行為が云々とあるが、自衛権の要件もやはりそういうパラレルなものなのか。

（答）基本的には同じで、まさに急迫不正の侵害があってやむを得ない場合だ。ただ、国内における正当防衛でも過剰防衛が禁じられているように、均衡性を保たなければいけない。それからその急迫不正の侵害に対して取る自衛権行動は、これで大丈夫だという時点でやめなければいけない。ただ、それを判断するのが個々の国家であり、国際法の社会では国家の上に立つ国家はないので常に問題になるわけだ。

（コメント）９.11事件との関連で１つだけつけ加えると、急迫不正の脅威は確かにあったと思うが、米国が攻撃を受けたのは９月11日で、実際に軍事行動を起こしたのは10月８日であり、かなりの時間差があった。急迫不正の脅威に対してすぐに対応を取るのが正当防衛とか本来の自衛権に基づく活動のはずだが、１カ月も待って攻撃するのがいいのかという疑問点が残る。米国としては「オン・ゴーイング・スレット(脅威の継続)」がある。つまり９月11日の攻撃はあくまでも最初のものであって、これからも起こり得るかもしれないという脅威感を維持しておかねばならない。そこで「オン・ゴーイング・スレット」の話が出てくるのだと思う。

（問）NATOが間髪を入れずに集団的自衛権を発動したが、これは米側と裏でのすり合わせがあったのか。

（答）詳細はわからないが、米国と欧州各国との間で何らかのやり取りがあったとは思う。また、

アメリカに対する連帯の気持ちの表明という政治的な意図もあっただろう。NATO条約自身はできると言っているだけで、自動的に全部反応しろとは言っていない。つまり、各国ができる範囲のことはやるという姿勢を表明した点では、政治的な意味合いが強いと思う。

（問）世界の人々が、ほぼ同時に９.11事件をテレビを通して目撃し、身体で感じたとも言えると思うが、ごく普通の人にもグローバル・ソサエティが認識されたことは、文化的・社会的に非常に意味が大きかったと思う。

なぜNATOがすぐに自衛権行使を認めたかについては、政治的な問題や、民間が無差別に攻撃されるのではという恐怖に加え、あれを許しておくと大変なことになるという思いがあるだろう。

（答）おっしゃるとおり、負の意味合いで、世界貿易センターに旅客機が激突し、数時間後にビルが崩れ落ちるのを多くの人々がテレビで見たことにより、否応なしに世界中が一体となり、自分の五体がまさに傷ついていくのを各国の普通の人たちが感じたのではないかと思う。

NATO諸国が政治的な意味ですぐ同意した背景にも、それが実はあるのではないかと思った。米英間の特殊な関係ゆえに、英国政府だけはそういうことがなくてもすぐ動いたかもしれないが、その他の国が何も対応せずにいたら、グローバル・ソサエティに対する共通した痛みを、各国の政権は全く分かっていない、という方向に批判されるという直感が働けば、やはり即座のレスポンスが必要である。幸いにしてNATOの場合、政治的なレスポンスと、行動のレスポンスは条約上では必ずしも一致しないので、とにかくすぐにポリティカルな意味でのレスポンスはしよう、という考えはあったのかもしれない。

（問）今の話に非常に共感する。自分は、1998年の爆破事件の３カ月位前に、ダルエスサラームとケニアの両方、その同じビルに行っていた。日本のニュースで知った時は勿論がく然としたが、９.11事件の衝撃の比ではない。目に見えてしまったことは、身体感覚に対する恐怖の度合いが全然違う。それがNATOを反射的に集団的自衛権に走らせた背景だという気がする。

（答）そこからサイバーテロのほうに引っ掛ければ、コンピューター・ウイルスを上手に使うとか、クリティカル・インフラを上手に壊すと、サイバー上で何が起こったかは見えないが、結果としては、みるみるうちに社会的な麻痺が起こる。それこそ自分の指が動かないと思ったら手全体が動かなくなり、そういえば心臓も動かなくなってきた気がする、というような恐怖感を、ネットワーク化された社会であればあるほど、身近で視覚的に感じるかもしれない。９.11事件は、１カ所の出来事が世界中にブロードキャストされるという意味でまさにブロードだった。サイバーの場合には、個別の被害が燎原の火のごとく広がるという、ブロ

ードの意味合いが違うのだろうが、ブロード性があるかもしれない。そうすると、それに対する反応としても、ぼおっとしていていいのかという今回のような発想が起こったり、全世界的な社会のセキリュティ問題だということで反応がある可能性がある。

（問）まずNATOのコミットメントの話で、政治的意味合いが強い背景には、欧州諸国はテロリストを匿っているとか、自由にさせていると絶えず批判されていることが挙げられよう。アルカイダのグループも、英・仏・独などにセルを持っていると思われており、今までも親米のアラブ諸国から引き渡し要求があったが、欧州は自由を尊重しているから渡せないと言っていた。今回もし対応が遅くなれば、それをテロ支援とは言われずとも、テロを見逃していたと言われかねない、という負の意味での政治的コミットメントの必要があったのではないか。

また、９.11事件を世界中の人が見たとはいえ、すべての国の人が同じように思ったかは疑問であり、「グローバル」が誰を指すかを吟味する必要があるのではないか。

２つ目は、橋本先生がおっしゃる自衛権、あるいは新たな集団安全保障体制の下での新たな活動、抑止行動とか防止行動になるが、これは自衛権の場合や国内法での自己防衛の場合、均衡の原則とか相当の手段という考え方がある。例えばNimdaウイルスやI Love Youをばらまくことに対する相当の手段は具体的に何かあるのか。

（答）２点とも正しいご指摘だと思う。NATOの話も、確かにシェンゲン条約等で事実上、地域がだぶっているので、人も物も自由に動くことができ、それをもって欧州の統一性を保とうとしている。しかし、どこか空いているところを探して突っ込むのがテロリストだから、いくらでも逆手に取れる。パスポートもノーチェックだからこそ、ドイツにアルカイダのメンバーがいたのだ。ただ、逆手にばかり取らせはしない、という意思表示をし、批判をかわそうとしたと言えるかもしれない。

また、「グローバル」という時の言葉は、その意味づけと軽重は確かに重要だと思う。今回のテロ事件を歓迎した人々もグローバル・サイドにいたはずで、もしかするとその人数の方が多かったかもしれない。

集団安全保障体制下で取り得る抑止行動については、例えばコンピューター・ウイルスの場合には、その背後にいるのがテロリストであれ、いたずらな子供であれ、日本でも始まったいわゆるサイバー・ポリスのような形での捜査になると思う。基本的には、法制度等を含めた国際的なネットワークにより最後には逮捕されるので、やはり従来型の犯罪としての国際捜査、司法共助という形になるのではないか。今でもある程度、警察的側面、軍事的側面、お金の側面、技術的に協力可能な部分など、あらゆる組み合わせによる対応を取ることができるだろう。

（問）少しレベルが上の、例えば国防システムに入り込もう、あるいは実際入り込んで麻痺させることに対する相当の手段や、クリティカル・インフラを麻痺させるものに対する対応手段について、何か具体的なお考えをお持ちか。

（答）被害によるものではない、相手の実力に合わせた比例性ということになるかと思う。まず相手を探すことが第１の手段で、あらゆる機関が最大限の努力をする。そして見つけた相手が少年であれば警察が対応するだろうし、違うとなれば、それに相当する実力を持ったところが対応する。それがいわゆる比例性になっていくのだと思う。今までの国際法上の自衛権の比例性（均衡性）は、受けた攻撃・被害に対する比例性（均衡性）だった。つまり、ミサイルならミサイルに相当する位の反撃は許されるという具合に。しかし、サイバーテロの特徴として、少年のいたずらかもしれないものと、意図的・計画的なものとの被害規模が同じ場合、被害規模の比例性でいってしまうと、少年にミサイルを撃つのか、サイバーに実力で反撃していいのか。そういう意味では、今までの均衡性ともやや違う発想であって、まだ精緻には詰めてないが、やはり自衛権はそこでも引っ掛かりがあるのではないかと思う。

（問）今回の事件ではサイバーテロは同時に起こっていないが、サーバーテロというか、トレーディングルームのトップが落とされたので、国債引受も社債販売もできず、銀行間の資金決済も止まっている。これに加えて取り付け騒ぎが起こっていれば、世界がみんな見ていたという相乗効果もあり、金融社会が崩壊していたかもしれない。金融に対する不安を駆り立てる点では、最初の物理的な攻撃に意味があったと思うが、もし取り付け騒ぎが実際に意図どおり起きて、それを増長するために東京の金融システムを落とすとなれば、東京はサイバーに対する防御が弱いので可能だろう。よく、電力・空港を押さえるというが、これらのサーバーを落とすのは比較的初歩的と言われており、もしそこまで考えていたとすれば、今の日本では比較的あり得るシナリオだったのかと思う。

（答）サイバーテロは、恐らくテロリスト側にとって有効なやり方だと思う。今後は技術面での対処も当然なされていくし、必要だろう。システム自体に不安があるので、常にバックアップシステムを取っているのだが、それごと攻撃を受けるとなると、バックアップのバックアップが必要になる。ハード的及びソフトウエア的な意味で、サイバー上での自由な動きを少し制限しても、そのセキュリティをワンランク上げようという動きは今後出てくると思う。そういう意味では、今後、日本でもネットワーク・セキュリティの問題が出てくる時に、プロバイダに自由の侵害だとは言われるが、一定期間ちゃんと通信記録を控えておけとか、何かあった時には然るべき令状が出てくればそれを見せろといった形の協力で、コントロールされた自由はあり得るし、バックアップをもっと安定化させることもあると思う。

（問）これは加藤先生がご報告された際に学んだことで、サイバー攻撃とは物理的な破壊ではなくて機能に対する破壊だというご指摘があったが、さらにいうと、レピュテーション（名声）や信用に対する攻撃になると思う。だからここでは、そういう大きな被害の広がりを考える必要があるかもしれない。

（答）それがあるからサイバーテロが成り立つというジレンマだと思う。便利さを利用してサイバーテロが起こるのだ。便利さと、その便利さ故に生じるセキュリティの問題をどうバランスさせるか。恐らく、今までのような野放図な自由ではなく、これからは制限された自由となるだろう。

（問）攻撃手段が防御手段よりもどうしても早く進んでしまうらしく、このギャップが対策を難しくしているのかと思う。暗号作成と解読の関係も同様だ。

（答）守る側の富士通の技術者曰く、基本的にはいたちごっこだが、常に守る側が弱いらしい。なぜならば、こちらが気付かないような所を見つけるために彼らはすべての努力を傾けているからだ。

（問）技術を進めるためにハッカーは必要だという話もある。

（答）ハッキング自体は正しいことではないが、然り。見たという印だけを残すのは本来のハッカーで、クラッカーになると、コンピューターの中をいじくり回すとか、そこから先でお金を転がして懐に入れるなど、どんどん犯罪化していくが、そこは両刃の剣だ。ただ、その両刃の剣を使いながら我々がネットワークを拡大してきたことも確かで、インターネットも、本当はサイバー犯罪条約では禁じられているようなサイトの方がアクセスが多く、認めてはいけないが、その存在は認識せざるを得ない。しかしどこかで、これを越えたら実際に世の中の仕組みが動き出すという線を見せおく必要がある。そのための努力は、なかなか追いつかないが、追いつかないなりに努力すべきだと思う。

（問）サイバーテロの犯人がテロリストかいたずらな子供かを突き止めるのに時間を要する中、国際社会が一致して、サイバーテロに対抗する機運を高めるには、難しい面もあるのではないか。

（問）責任能力の問題も出るのではないか。中学生の天才集団が出て、それもやはり戦争なのかと言われるとよく分からない。

（答）そのとおりで、サイバー上のテロかは分からないが、被害はテロリストが意図したものと同様の被害がもたらされている場合の問題点だと思う。今までは、法律は基本的に１対１対応をしており、ある行為に対応するための法律や社会制度ができていた。だから国際法は国

対国で済んでいたし、サイバー犯罪は「個人がサイバー犯罪をする」で済んでいた。そこがクロス、もしくはミックスしてしまう。さらにいえば、ミックスしているかクロスしているか開けてみないと分からない時には、対応方法も多様に組み立てるしかない。ただ、今回の米国同時多発テロ事件の時のように、世界中が共に立ち上がらねばという意識が急激に高まるまでには至らないかもしれない。「見た」という意味での一体感はあるけれども、自分の身にすぐには降りかかっていないからだ。

逆にサイバーの場合には、コンピューター依存度が高い個人がいれば、身近であるが故に、かえって危機感があるかもしれない。

（問）日本の中枢に対して、敵国と思われるところから明確に目に見える形でのサイバーテロがあった場合も、日本は自衛権を発動できるか。

（答）発動できると思うが、実際に日本に何ができるかは特に難しい問題だと思う。なぜならば日本は物理的な打撃能力を十分に持っていないからである。国家の意思として武力攻撃と同等の意識でサイバー上での攻撃を受けた場合は、個人的にはそれは武力攻撃と見なしてよいと考える。なぜならばそれを武力攻撃と見なさなければ、何のために自衛権まで用意してそれぞれの国は武力攻撃から自分の国を守れるのか分からなくなるからである。

今までの武力攻撃はあくまでも、現在我々が想定できる武器をもとに、武力攻撃の範囲を決めていた。それから言えば、武力攻撃の範囲は時代と時期で内容は変わり得ると思う。国家の意思として、サイバー攻撃という形で武力攻撃と同じように攻撃がなされるならば、サイバー攻撃は攻撃であって、それに対して反応ができるのではないか。

（問）そうかもしれないが、例えば日本の政治状況、学問的な概念の整理の仕方と、政治の世界での話は分ける必要があると思う。侵略だと整理できたとして、具体的に何ができるのか、例えば国会でそのための法律が通るのか。その定義は何かという一連の長い議論があって、実は廃案になるのではないか。最終的に自衛権の話になっても、今の憲法の下で何ができるのかについては悲観的だ。

（問）個別的自衛権も行使できないのだろうか。

（答）私はできるのではないかと思う。ミサイル１発も撃たれないまま、実際にミサイルに撃たれるのと同様の状況で日本がつぶれてしまう。反撃もできない。先ほど日本は特につらいと言ったのは、要は長い議論もあった後にサイバーが武力攻撃だと見なせるとして、日本は何ができるかというと、日本は近隣国にすら届くミサイルを持っていないので、実際に行くしかない。行く間に向こうは対艦ミサイルを撃ってくるだろうし、飛行機は復路の燃料がない

ので帰って来られない。そうなると、今度はサイバーにはサイバーでできるのだろうかということになると思う。

ただ、ここで問題になるのは、そのようにサイバー攻撃を仕掛けようとする側は、巧妙に防御をしておく。もしくは通信のラインを切ってサイバー攻撃をされない状態にしてから、限られたサイトから相手（日本）のサイトをサイバー攻撃するだろうから、反撃手段が技術的にない。そうすると、やられ放しとなる危険性はあると思う。本来の正当に反撃できる権利と実際の技術・手段を持っていない限り、反撃できないのである。

（問）その点に関して、５年前に米国のシンクタンクで話した際、サイバー攻撃に対してサイバー防御、もしくはカウンターアタックができるのは米国しかない、との意見に彼らは特に反応を示さなかったが、その頃米国は「やってくれるか」という日本の要請を期待していたのを私は覚えている。その後どれほど日米間の協力が進んだのかに興味がある。

（答）日米安保条約の基本的なロジックからすれば、米国本土がサイバー攻撃されても日本が米国を守ることにはならないが、日本本土がサイバー攻撃された時に、日米双方がサイバー攻撃を武力攻撃と見なすと一致して解釈すれば、米国は自らが攻撃されたのと同様に、集団的自衛権を行使してくれるのではないか。

（コメント）新安保は義務規定ではないと思う。まず発動の要件の有無があり、あったとしてもやるかやらないかは、また判断の問題がある。