サイバー攻撃と関連法制度

橋　本　靖　明

はじめに

1998年５月、アメリカのクリントン大統領（当時）は大統領決定指令63を出し、サイバー攻撃に対するアメリカの脆弱性を克服するため、国内制度の構築を開始した[1]。翌年1999年１月には、同大統領は、全米科学アカデミーにおいて講演し、化学兵器と生物兵器によるテロリズムと並んでサイバー攻撃によるテロリズムの危険性を指摘し、コンピュータセキュリティと重要インフラストラクチャ防御のための対策が必要であると主張した[2]。現在では、アメリカ社会を支える重要インフラストラクチャの電子的防御に関して具体的なシステムが作られてきている。また、わが国においても、2000年以降は、高度情報通信ネットワーク社会推進戦略本部（ＩＴ戦略本部）を中心に、政府の情報セキュリティと社会の重要インフラストラクチャ防護のための対策を講じているところである[3]。2001年10月には、ＩＴ戦略本部は、サイバー攻撃に対応することを目的としたナショナルチームを2002年度中に内閣官房に設置することを決定した[4]。これは、サイバー攻撃が重要インフラストラクチャに対してなされる事態を想定し、その対処を官民一体となって行うために設けられるものである。

日米両国がこのようにサイバー攻撃への対応を進める背景には、近年の急速なネットワーク社会の発展とコンピュータシステムのネット依存拡大という現実がある。脆弱なネットワーク自体が攻撃を受け、ネットワーク経由で官民のコンピュータシステムがダメージを受けた場合、その影響は社会の広い範囲に及ぶことが懸念されている。こうした攻撃は、国家のみならず、テロリストや個人までが行う可能性があるため、その適切な対

---

[1] Presidential Decision Directive/NSC-63, May 22, 1998, The White House.

[2] Reuters, “Clinton Combats Cyberterrorism,” January 22, 1999. （http://www.wired.com/news/politics/0,1283,17494,00.html）

[3] アメリカの対応については、『軍事力としてのサイバー攻撃の形態及び諸外国の法的取り扱いに関する調査研究』（財団法人ディフェンスリサーチセンター、2000年）58-66頁。わが国の対応の経緯については、同上、16-19頁、およびＩＴ戦略本部議事録を参照。
（http://www.kantei.go.jp/jp/it/network/index.html）

[4] 『日本経済新聞』2001年10月10日。「サイバーテロ対策にナショナルチーム・IT戦略本部」（http://www.nikkei.co.jp/news/seiji/20011010CPPI009010.html）

『防衛研究所紀要』第５巻第１号（2002年８月）22～41頁。

処が必要とされるのである。また、サイバー攻撃は、インターネットのようなサイバー空間を経由して行われ、衝突力や爆発力のような実際の物理的エネルギーによる破壊をもたらすものではない。そのために、こうした攻撃を従来の武力攻撃の考え方と同様に捉え、対応することができるのかという問題も生じてくる。

本小論は、サイバー攻撃を巡る近年の事態進展を認識した上で、サイバー攻撃について、主に法的側面から検討を加えようとするものである。サイバー攻撃の内容を概観し、その法的性格をいかに捉えるか、どのような根拠によって対応できるかという問題を取り扱う。また、2001年９月11日に発生したアメリカにおける同時多発テロ事件が、サイバー攻撃への対処を行う際の法的根拠を巡る議論に影響を及ぼすと考えられるため、その点についても若干の分析を加えた。

１　サイバー攻撃とは何か

本節では、現在一般に用いられているサイバー攻撃という言葉が意味する内容について明らかにする。サイバー攻撃の明確な定義は定まっておらず、いくつかある定義についてもある程度の相違が見られる[5]。ただし、官民双方のコンピュータやネットワークへの侵入や攻撃を含む点でほぼ共通していると思われるため、本研究においても、サイバー攻撃を、サイバー空間を利用した、コンピュータシステム、ネットワークへのあらゆる不法な侵入や攻撃として捉えておく。サイバー攻撃は、技術への依存度が高いために、従来の武力攻撃とは異なるさまざまな特徴を有している。

（１）サイバー攻撃の実行者

まず、サイバー攻撃を行う可能性のある者は個人である。サイバー攻撃は技術に対する依存度が非常に高いため、一個人の能力によっても実施が可能である。また、同じような攻撃意図を持った複数の人間が一緒になって、グループとして行動することも考えられる。彼らは、ネットワークから特定のコンピュータシステムに侵入し、そのデータを盗み、改竄したりすることや、システムを破壊することなどを目的とする者たちで、ハッカーやクラッカーと呼ばれている。

5　いくつかの定義を簡潔に紹介するものとして『軍事力としてのサイバー攻撃の形態及び諸外国の法的取り扱いに関する調査研究』（前注３）２－５頁。

そのほかに、いわゆるテロリストもサイバー攻撃の実行者となるだろう。テロリストは、自らの要求を国際社会や特定の国家などに受け入れさせる目的で社会の脆弱な部分を狙うため、ネットワークへの依存を深める現代社会においてはサイバー攻撃は有効な攻撃手段となりうる。ただし、テロリストグループは、最終的な目標として国家建設を目指すものから、特にそのような目的は持たず、ある一定の要求を容認させることだけを目的として、特定の国から支援を受けつつ活動するグループまで多岐にわたっているため、それらをすべて同じように扱ってよいかという問題がある。

さらに、国家自身が他の国家への攻撃の一環として、サイバー攻撃を行うことも想定される。この種のサイバー攻撃は、実体的な武力攻撃の前段階として用いられることもあろうし、武力攻撃の最中に同時に行われることもあろう。加えて、武力を行使した実体的な攻撃を伴わずに、サイバー攻撃単独で実施されることも考えられる。

このように、サイバー攻撃という同じ用語を用いても、個人から国家までさまざまな実行者が考えられる。また、注意すべきは、こうした実行者の特定が困難であることも想定されるという技術的な現実である。サイバー攻撃は、ネットワーク管理者が存在しないインターネットを利用して行われ、しかも攻撃のためのデータが分割された上でそれぞれ別のルートを通る可能性がある。攻撃者は、ネットワーク端末であるコンピュータを操作しているだけであって、具体的な実体を攻撃対象者から見える位置に置いているわけではないために、所在地や攻撃者自身が何者なのかを判断することが難しい。

（２）サイバー攻撃の意図

次の特徴は、サイバー攻撃の意図も多様であるということである。たとえば、単純な悪戯心で行うコンピュータシステムの侵入や改竄、破壊も、武力攻撃と同様の意図をもって行われるコンピュータシステムへの深刻な侵入や改竄、破壊も、その外見上には差異が見られない。法的対応を行うためには、その意図の判断が重要であるが、その点が不明確な可能性があることがサイバー攻撃の特徴のひとつである。

実際にサイバー攻撃の背後にある意図としては、先に挙げた悪戯から、（特に外部からの侵入に対して強固に防衛されていると噂される）システムを征服したいという技術的な欲求、特定のコンピュータシステムからデータを盗み出すことによって金銭的な利益を得ようとする窃盗、システムの破壊やそれによってもたらされる社会不安を起こすことによってある要求を受け入れさせようとするテロリズム、さらにはある国家の他の国家に対する攻撃意図まで挙げることができる。

（３）サイバー攻撃の手法

サイバー攻撃は、インターネットやそれに接続したローカルネットワーク上において行われる攻撃である。従って、攻撃は物理的衝突や爆発によって引き起こされる実態的な破壊ではなく、コンピュータシステムの中におけるデータやプログラムの破壊といった形で引き起こされる。このようなサイバー攻撃が身近な危機となった背景には、コンピュータ性能の急速な向上とそれに伴うネットワークの発展がある[6]。サイバー攻撃は、こうした技術的進歩とネットワーク社会の構築を利用して実施されるのである。

具体的には、攻撃対象となるコンピュータシステムに侵入し、そのデータを盗む、または改竄する。また、目標とするシステムの提供するサービスを妨害する、また、あるシステムに侵入し、そのシステムを踏み台として別のシステムを攻撃するといったことが行われる。

攻撃対象となるコンピュータに侵入するために用いられるのが、パスワード・クラックと呼ばれる攻撃である。コンピュータシステムは、外部からの不当な侵入を防ぐために使用許諾者にパスワードを付与しているが、それを推測し、使用者になりすますことによって目指すシステムに侵入する。侵入後は、正規使用者になりすまし、システムから必要なデータを盗み出し、データやプログラムを改竄することが可能になる。ホームページ改竄などはこうした手法を利用して行われる。

攻撃対象のシステムのサービスを妨害するために使用される手法がDoS（Denial of Service:サービス不能）攻撃と言われる手法である。この手法に分類される攻撃方法にはいくつかの種類があるが、基本的には、対象となるコンピュータが処理しきれないほどの量のデータを送り込み、そのシステムを麻痺させて、以後のサービスを不可能にしてしまう。アメリカにおいてインターネットを利用した商用システム（ヤフーなど）が麻痺した事例、わが国において特定の組織のコンピュータシステム（歴史教科書問題に関連して扶桑社など）が麻痺した事例などは、この種の攻撃による被害である。

また、このように特定のコンピュータシステムを狙った攻撃だけがサイバー攻撃ではない。コンピュータネットワークそのものの脆弱化を図ったり、不特定多数のシステムを破壊、麻痺させることも考えられる。この攻撃は、コンピュータウィルスと呼ばれるプログラムをネットワーク上に走らせることによって引き起こされる。

---

[6] コンピュータスコープ社の集計では、世界のオンライン端末機器数は、1995年12月に1,600万台であったものが、2001年５月には４億6,200万台に、2002年５月には５億8,000万台にまで達している。（http://www.nua.com/surveys/how_many_online/world.html）

コンピュータウィルスによってもたらされる被害としては、たとえば、コンピュータそのものが全く起動できなくなることがある。他にも、あらゆる関係者に無断でウィルスに感染したメールを送信してしまうことも典型的な被害例である。また、無断で発信されるメールに、感染したコンピュータが保存していたデータを添付してしまう被害も生じる。機関や個人が保管していた各種のデータが、知らないうちに他者の手に渡ってしまう。さらに、ウィルスに感染したコンピュータを外部の攻撃者が乗っ取り、遠隔操作することが可能となることもある。ウィルスを使用した攻撃も、ネットワークへの依存度を拡大する社会全体にとっての大きな脅威となる[7]。

（４）サイバー攻撃によってもたらされる被害

サイバー攻撃という言葉自身まだ新しいものであり、我々自身もその攻撃によっていかなる被害がもたらされるかについて想像しにくいところがある。そのため、サイバー攻撃の危険性がさほどに重く考えられない可能性もある。たしかに、サイバー攻撃のみによって、対象とする国家を完全に破壊することは不可能である。しかし、以下のような実例を見れば、被害が決して無視できないことが認識できる。1997年６月、アメリカ軍統合参謀本部は、サイバー攻撃に関してアメリカのコンピュータシステムを防衛することができるかどうかを検討するため、「エリジブル・レシーバ」演習を実施した。外国に雇われたハッカーがアメリカを攻撃するというシナリオである。その結果生じうると判断された被害は甚大であった。ハッカーたちはアメリカの９主要都市の送電を停止させ、その地域の救急システムを破壊することができた[8]。さらに、ホノルルにあるアメリカ軍太平洋司令部の指揮・統制システムも麻痺させることにも成功した[9]。実際の演習はそうした被害を起こしうると判明した時点で終了したが、この結果によってサイバー攻撃の持つ危険性を窺い知ることができる。この演習中に攻撃チームが実際に使用したのは、市販のコンピュータと一般的なインターネットプロバイダが提供する通常の通信回線であった。またチームを構成した人数は35人であり、攻撃対象を選び、そのための手段を用意するなどの準備期間

7　コンピュータウィルスの蔓延は既に重大な問題として認識されつつある。政府関係機関である情報処理振興事業協会によると、ウィルスを発見した、またはシステムがウィルスに感染したという届出は、1999年に３千６百件であったが、2000年には１万１千件を越え、さらに2001年には２万４千件を越えた。ちなみに、1990年の届出数はわずかに14件でしかなかった。
(http://www.ipa.go.jp/security/index.htm)

8　James Adams, “Virtual Defense,” *Foreign Affairs*, vol.80 No.3 (2001), pp.100-101.

9　『日本経済新聞』2001年１月９日。「特集　技術創世記：未来と向き合う（８）見えない敵の脅威」（http://www.nikkei.co.jp/sp2/nt18/20010109eimi147909.html）

は３カ月。しかも、彼らが使用したシステム侵入用プログラムは、法律に違反することなくインターネット上で無料で入手したものであった。ちなみに、２年後の1999年10月には「ゼニス・スター」演習が実施された。ここでは前回の「エリジブル・レシーバ」演習で判明した防衛上の欠陥がその後どのくらい克服されているかを検証しようとしたが、ハッカーたちはいくつかのアメリカ軍基地に電力を供給している送電システムを攻撃し、地域救急システムを麻痺させることに成功した[10]。また、1998年には実際に、ソーラーサンライズと呼ばれるコンピュータシステム侵入事件が発生した。複数のハッカーが、航空宇宙局、国防省、幾つかの大学システムに侵入し、それらに侵入の証拠を残したのである。

さらに、サイバー攻撃の被害は、アメリカでの「エリジブル・レシーバ」「ゼニス・スター」両演習が示したような、電力供給停止や救急システム麻痺だけにとどまらない。鉄道管制システム、航空管制システム、海上交通管制システム、通信システムなどが機能を停止し、誤作動する危険性がある。大型旅客機の事故は、乗員乗客だけでも500名の死傷者を発生させる。新幹線のような高速鉄道の事故は、一編成だけで1,000名を越える乗客に相当の死傷者を出すだけでなく、その後の輸送業務を滞らせる。電力システムでは、原子力発電所の管理システムを誤作動させることによって、最悪の場合には原子炉のメルトダウンを招き、核爆発に近い被害をもたらす。水道や燃料のパイプラインの管理システムが誤作動させられると、バルブの急激な開閉によるパイプの破断などの被害が生じる。ダムや水門の急激な開放によって洪水を発生させ、死傷者を発生させ、土地利用に支障をきたさせることも懸念される。通信システムも、現在はコンピュータによって管理しているため、通信不可能となる可能性がある。さらに、金融システムの破壊も現代社会にとっては致命的である。各国の中央銀行は各商業銀行との間で決済システムを維持し、また、財務当局の指示を受けて為替介入を行うシステムを有しているが、これらのシステムが破壊されれば、一国の経済のみならず、世界経済が麻痺する[11]。

加えて、コンピュータウィルスの蔓延は、ネットワークに高度に依存している国家、社会においては経済を沈滞化させる要因となる。実際に、”I Love You”ウィルスやNIMDAウィルス、Gonerウィルスなどによって、官民を問わず世界中の多くのコンピュータシステムが汚染されたが、こうしたウィルス蔓延をサイバー攻撃の一部として計画するならば、その被害は甚大である。汚染された可能性のあるすべてのコンピュータシステムを検査し

---

[10] Adams, “Virtual Defense”（前注８）, pp.101-102.

[11] 発生する可能性のあるこれらの被害を簡潔に示すものとして、以下のものがある。Department of Defense Office of General Council, *An Assessment of International Legal Issues in Information Operations*, 1999, p.20; L.T.Greenberg, S.E.Goodman, K.J.Soo Hoo, “Introduction,” *Information Warfare and International Law*, National Defense University Press, 1998. (http://www.dodccrp.org/iwilchapter1.htm)

原状に復帰させるためには、多くの技術者の労力と時間とを必要とする[12]。その間、通常の業務は行うことができず、コンピュータシステムの信頼性が低下しているために、連続してサイバー攻撃が行われたときには十分に対処できないという問題が生じる。

また、安全保障面で見ても、たとえばアメリカ軍の場合、部隊等の間で行われる通信の多くが一般通信回線を経由して行われているために、通信システムが破壊されることで、以後の行動に著しい制約を課される危険性がある[13]。わが国においても、たとえばバッジシステムは気象情報を入手するために気象庁とリンクしており、そこから攻撃者の侵入を受けて誤作動する可能性がある。一般通信回線を利用したデータ通信が不可能となることで活動に支障をきたすことは、アメリカの場合と同様である。他にも、サイバー攻撃によって、自衛隊の燃料、交換部品、衣料品などの物資補給システムが機能せず、部隊の行動に制約が課されることも予測される[14]。電源も含めて完全に外部から遮断されて作動するシステム以外は、サイバー攻撃の被害を受ける危険性を基本的に有している。

（５）サイバー攻撃の特徴

以上のことから、サイバー攻撃の特徴には以下のような点が考えられる。

まず、一般にサイバー攻撃と言われるものの中には、サイバー空間における破壊や窃盗などの個人による犯罪行為から、サイバー空間における国家による他国への攻撃行為までのさまざまな形が考えられる。このように、その実行者や意図に多くのバリエーションがあることがサイバー攻撃の特徴であるが、こうした行為を厳密に峻別できないことがサイバー攻撃の問題の複雑さを示している。

問題の複雑さをもたらすのは、組織化の度合いと攻撃力との間にある従来からの比例関係がサイバー攻撃には当てはまらないという事実である。つまり、組織化が進んでいない集団（その究極にあるのは個人）による攻撃能力は、組織化が最大限に進んだ集団（その究極にあるのは国家）による攻撃能力に比べて圧倒的に劣っているという前提が、サイバー攻撃には該当しない。小さな組織であったとしても、大規模な被害をもたらすだけの

---

[12] たとえば、”I love you” ウィルスによる被害の場合、アメリカ労働省は1,600人時間と1,200時間の外注作業を復旧のために必要とした。このウィルスによってアメリカが蒙った被害は40億ドルから150億ドルと考えられ、これはアメリカの小規模都市が絨毯爆撃されたのと同等の被害規模であったという。Adams, “Virtual Defense,” （前注８）pp.106-107.

[13] 軍事通信の95パーセントが一般の交換機ネットワークを経由して行われている。The Staff Statement of the U.S. Permanent Subcommittee on Investigations (Minority Staff) Hearings on Security in Cyberspace, 5 June 1996, Section I.B.

[14] Department of Defense, *An Assessment of International Legal Issues in Information Operations,* （前注11）p.20.

攻撃力を行使することができる。そうした新しい攻撃形態がサイバー空間においては存在しうる。すなわち「１人の天才は、1,000人のエンジニアに勝る」のである[15]。たとえば、”I Love You”ウィルスの作成者はフィリピンの大学生であり、Gonerウィルスの場合はイスラエルの15歳と16歳の若者であった。また、深刻なコンピュータシステム侵入問題であったソーラーサンライズ事件の犯人は、カリフォルニアの高校生と中学生であったことがその好例である。これは、コンピュータの高性能化とインターネットやローカルエリアネットワークなどの急激な発達がもたらした状態であって、この状態を従来のような組織化と攻撃力との間にあった比例的関係に戻すことは、われわれが現在享受しているネットワーク社会の恩恵を捨てることになり、現代社会が受け入れることはできない。

さらに、このような技術発展がもたらした結果として、サイバー攻撃は国境をまったく意識せずに実施することができる。また、さまざまなネットワークの上をデータがいわば細切れに移動し（パケット通信）、かつその移動経路全体を管理している者が事実上存在しないために、ネットワーク管理の面からサイバー攻撃を行う者の取締まりを行うことも困難である。

つまり、サイバー攻撃は、現代の国際社会の特徴である情報流通の高速化、自由化がもたらす危機と言える。

２　サイバー攻撃対処と関連法規制

（１）サイバー攻撃は犯罪か、武力攻撃か

前節において検討してきたように、サイバー攻撃には、犯罪としての性格をもつ個人による攻撃と、国家や国家に準ずる団体によって行われる、従来の武力攻撃と同様の意図をもつ攻撃とがある。ここでは、サイバー攻撃の結果（被害）の同質性と原因の異質性について考察する。この問題が、実行者の違いを基準とした、犯罪と武力攻撃に対する法的対処の差異に関する従来の考え方を、根本的に覆す可能性があるためである。

サイバー攻撃が、コンピュータによってインターネットのようなネットワークを経由して行われるために、攻撃者にさまざまなバリエーションがありうることは既に明らかにした。しかも、攻撃が、急速に性能を高めたコンピュータの処理速度とネットワークの高速

[15] 2001年（平成13年）6月、防衛研究所において開催された研究会「サイバー攻撃の技術と対処」における講師（富士通システム統合研究所主席部長　山田永三氏）による。

大容量化という技術的要素に依存しているために、個人が悪戯で行うサイバー攻撃も、国家が攻撃の意図をもって実施するサイバー攻撃も、その結果として生じる被害の点においてはほぼ同質である。社会の重要インフラの麻痺や破壊といった重大な被害を、個人のパソコンによってもたらすことも可能なのがサイバー攻撃である。

ここに見られるのは、結果（被害）の同質性と原因の異質性である。原因は個人的な悪戯心や征服感の達成にあっても、結果としてもたらされる被害の程度は、従来の武力行使でいえば大規模攻撃に匹敵するだけの重大さ、広範さを持つことがある[16]。今までは、攻撃者の組織化の度合いと攻撃者が行使する攻撃力（破壊力）との間の比例関係が存在した。攻撃力の小さい攻撃者は、従来の社会では個人であり、少人数のグループである。彼（彼ら）の行使しうる攻撃力は小さく、社会全体の脅威となるには程遠いために、国家の対処としてもそれらを犯罪行為として認識し、警察力をもって抑止、逮捕、処罰することにしたと考えられる。

サイバー攻撃の場合、こうした従来からの比例関係が崩れてしまっている点に注目しなくてはならない。このような状況下では、犯罪としての個人的サイバー攻撃にも、時に大規模な組織による対処が必要となる。また、行為者が誰なのか判明するまでは、国家などによる攻撃と考えた上での対処と、犯罪としての対処との双方が、同時並行的に、時に協力して進み、行為者が明確となった時点で国家による反撃などの行為が実行されるか、警察行為としての犯人追求が行われるかが決定されるような事態も考えられる。サイバー攻撃とは犯罪でもありうるし、また武力攻撃でもありうるために、対応にも両面性が求められるのである。

（２）犯罪としてのサイバー攻撃

まず、サイバー攻撃が犯罪として認識される場合を考える。たとえば、テロリストが実施するサイバー攻撃は、従来からのテロ行為に対する国際的法規制と同様に対処するのであれば、犯罪としての取り扱いが相当である。また、個人によって行われるサイバー攻撃も、やはり同様に犯罪として把握することが相当であろう。

テロ行為に対しては国際法は、各種の反テロ国際条約を用意することによって対応してきた。さまざまなテロ行為を国際的な犯罪として認定し、犯人が世界中どこにいても逮捕され、引渡され、あるいは訴追されるような法制度が構築されている。各国は、テロ実行

[16] 前注12を参照。

者を逮捕し、自国において処罰するか、適当な国家へと引渡す義務を負っており、それによって、テロを行う者の安住の地を世界中からなくすことを狙っているのである[17]。

こうした犯罪としてのテロ活動に対する法的規制は、サイバー攻撃の一部に関しても有効であろうと考えられる。実際、そのための対応が模索されつつある。サイバー攻撃というよりもハイテク犯罪の一環として一般的に認識されるサイバー空間における攻撃行為は、いくつかの機会において検討されてきた。特に先進国間においては、デンバーサミット以来議論が活発化した。G８では、リヨングループ（国際組織犯罪上級専門家会合）にハイテク犯罪サブグループを作っている。また、欧州評議会はコンピュータ犯罪専門家会合を設けサイバー空間における犯罪の取締まりを検討し、サイバー犯罪全般に関わる国際条約を起草して、国際犯罪としての取締まりを開始しようとしている。その新しい制度が欧州サイバー犯罪条約[18]であり、日本、アメリカ、カナダおよび南アフリカがオブザーバとして参加しているため、これらのオブザーバ諸国が加盟すれば、北半球にあるネットワーク先進地域のかなりの領域を地理的にカバーする条約となることが期待される。この条約においては、違法アクセス、違法傍受、データ妨害、システム妨害などがサイバーテロに関連する規制対象活動として含まれている[19]。今までの対テロ条約と同様に、サイバー空間における各種犯罪を、国際的な犯罪として諸国に共通する利益を害するものとして捉え、各国に、引き渡しか国内における処罰を求めている[20]。

サイバー空間における犯罪を規制する上記のようなシステムと、従来から整備されてきた反テロ条約などを有効に組み合わせることによって、犯罪としてのサイバー攻撃を相当程度制限できる可能性がある。実体空間におけるテロ活動が、実際の行動からテロ活動を支援する経済行為まで制限され、禁じられてゆき、さらにサイバー空間においても同種の活動が困難となることにより、テロ行為一般の活動分野が狭められていくことになろう。

また、各国の国内法においても、サイバー犯罪を法的規制の枠内に取り込むことで、サイバー攻撃の芽を摘み取るような制度が作られてきている。日本においては、1999年（平成11年）に不正アクセス禁止法が制定され、サイバー空間を利用した第三者のコンピュー

17　国連では、現在までにテロを封じ込めるための条約が11作成されている。ハイジャックに関連する諸条約、外交使節等に対する犯罪に対する処罰条約、放射線物質の保管に関する条約、安全な航海を保護するための条約、大陸棚のプラットフォームの安全確保のための条約、プラスチック爆弾探知に関する条約、爆弾テロに対する条約、テロ支援のための資金を封じ込める条約などが作成された。

18　Convention on Cybercrime（サイバー犯罪条約）は、欧州委員会において作成され、2001年11月23日にブダペストで署名された。欧州委員会の３加盟国を含む５か国の批准によって成立する。

19　サイバー犯罪条約の第2条　違法アクセス、第3条　違法傍受、第4条　データ妨害、第5条　システム妨害、第6条　機器の不正使用。

20　同条約の第22条と第23条は、犯罪人の処罰や引渡し、そのための国際協力について定めている。

タシステムへの侵入を禁じているのがその一例である[21]。その他にも、アメリカ、カナダ、オーストラリア、中国、フランス、イタリア、オランダ、スイス、マレーシアなどがコンピュータ犯罪に関する国内法を定めている[22]。

ただし、問題点もある。テロ活動を含めたサイバー攻撃は、大規模な組織や資金を必要としないという点で従来の物理的攻撃と異なっている。サイバー攻撃は、インターネットというネットワーク管理者が存在しない環境で生起するために、実行者の追跡と特定が困難である。しかも、ネットワーク社会の急速な進展を見ると、攻撃の性格、内容によっては、一般市民を含む社会全体に対する大規模かつ広範な被害が発生する危険性が高い。このようなサイバー攻撃に対して、テロ活動に対して従来から行われてきたような犯罪としての国際的、国内的規制だけで十分なのかという問題が当然に提起されるであろう。

（３）武力攻撃としてのサイバー攻撃

（ア）自衛権

サイバー攻撃が武力行使として捉えられるのであれば、攻撃を受けた国家は、自衛権を用いて必要な反撃を行うことができる。現在の時点では、自衛権とは他国による武力攻撃の帰結として行使される権利である。たとえば、国際法学会が編集した『国際関係法辞典』によれば、自衛権とは、外国からの違法な侵害に対し、自国を防衛するため、それに反撃するために武力を行使しうる権利である[23]。ここでは、自衛権とは、国際社会における国家間関係において認められる権利として理解されている。

こうした解釈から明らかなように、個人またはグループによって行われる国家にとって有害な行為を防止するために、外国の領土や公海において取られた軍事行動は、自衛権の行使の範疇に入れられていない。古典的な国際法における、国家の自己保存のための権利、自存権の行使として行われた軍事活動がこれにあたる[24]。その後の国際社会は、こうした幅広い自存権概念を整理し、国家間の争いは平和的に解決することを義務付け、限定的な

---

[21] 不正アクセス行為の禁止等に関する法律。平成11年8月13日法律第128号、平成12年2月13日施行。

[22] 夏井高人教授（明治大学）による。（http://www.isc.meiji.ac.jp/~sumwel_h/doc/code/index.html）

[23]「自衛権」の項を参照、国際法学会『国際関係法辞典』（三省堂、1995年）374-375頁。

[24] たとえば、自衛権を巡る議論においてその典型的事例として引かれるカロライン号事件も、実際には、当事国であるアメリカとイギリスとの間での武力攻撃と反撃という関係で生じたのではなく、アメリカ領に潜んでイギリス領カナダにやってくるカナダ独立運動の活動家をイギリスがアメリカ領に侵入し軍事力をもって排除したことに端を発しており、国家間武力紛争における自衛権行使の例ではない。

場合にのみ自衛権行使を認めることで、国際的な武力行使が発生する可能性を極小化しようとした。ここでは、自衛権は、国家対国家の関係において、相手側の先制的な武力攻撃に反応するために国家に認められる権利とされる。しかも、国連憲章により、安保理事会が適切な処理を開始するまでの間だけ行使できる時限的な権利となったのである[25]。では、こうした自衛権概念は、サイバー攻撃にどのように適用されるのであろうか。

サイバー攻撃は、従来の武力攻撃の考え方に収まらない新しい攻撃形態である。国際法上の武力攻撃とは、たとえば山本教授によれば「陸海空軍その他のこれに準ずる軍事的手段を用い国境線を越えて行われる組織的な軍事行動をいい、武力行使のうち最も重大性をもつ方式である」[26]。この解釈では、直接に物理的攻撃を伴わず、行為者も多様なサイバー攻撃が、武力攻撃の範疇にそのまま入るとは考えにくい。

しかし、この考え方には修正の余地があると考えられる。軍事行動は今や、物理的破壊力によってのみ行われるとは限らない。意思と結果を重視して、攻撃の内容をより広く捉えることが可能である[27]。また、逆に、そのように解釈を適切に拡大しなければ、放置しておくことができないほどの損害を及ぼしうるサイバー攻撃への有効な対処が不可能となる[28]。そのようにして新しい攻撃形態であるサイバー攻撃も武力攻撃の一形態であるとした時点で、サイバー攻撃に対する自衛権行使が認められることになる[29]。ただし、サイバー攻撃には多様な行為者と目的が存在する可能性があるため、すべての攻撃に自衛権を利用した反撃が自動的に行えるとは考えられない。では、たとえば、テロリスト(グループ)が行ったサイバー攻撃に対して自衛権は援用できるのであろうか。

---

[25] 国際連合憲章の第51条は、「安全保障理事会が国際の平和と安全の維持に必要な措置をとるまでの間」に限って、各国が個別的または集団的自衛の固有の権利を行使することを妨げないことを規定している。

[26] 山本草二『国際法』(有斐閣、1994年) 733頁。

[27] 加藤朗「新たな兵器と新たな倫理－コンクリ爆弾の意味－」『新防衛論集』第27巻4号 (2000年) 39－56頁。M.R.Jacobson, *War in the Information Age: International Law, Self-defense, and the Problem of "Non-Armed" Attacks*, note63.(http://www.infowar.com/resource/warinfo.doc)

[28] サイバー攻撃のメカニズムよりもその結果を重視し、被害が大きければ、武力攻撃を受けたものと同様に考える可能性を示すものとして、Department of Defense, *An Assessment of International Legal Issues in Information Operations*, (前注11) pp.15-27.

[29] James Adams氏との意見交換 (2001年5月21日) において、Adams氏も武力行使の概念を拡張すべきであるとの同様の見解を表明していた。氏は、サイバー攻撃の対策分野で実績を持つアメリカのサービス提供企業iDefense社の設立者である。

（イ）自衛権概念の適用拡大可能性

2001年9月11日に発生した同時多発テロ事件に対応して、アメリカは自衛権によって軍事行動を開始した。この自衛権は、今回のテロ実行者と考えられたテロリストグループ、アルカイダとそのグループを支援しているアフガニスタンの実質的支配政権であったタリバンに対して行使されている。

テロの主な対象国とされてきたアメリカは、1983年のベイルートにおけるアメリカ軍海兵隊司令部の爆破テロ事件以来、テロを犯罪とみなす姿勢を改め、戦争として対処する方向へと転換した。たとえばアメリカは、1985年から86年にかけて発生したテロがリビアの関与によるものであるとして、同国のトリポリとベンガジを航空攻撃したが、その根拠を自衛権に求めていた[30]。今回の軍事行動も、こうした従来の主張の延長線上にあるものと考えられる。

注目されるべきは、このようなアメリカの自衛権行使に対する各国の反応である。同時多発テロに対して、NATOは、その成立後初めてNATO条約第５条に基づく集団的自衛権の行使を認めた[31]。つまり、アメリカに対する大規模テロは、アメリカに対する武力攻撃であり、これをNATO加盟国に対する武力攻撃と同等視すると認定したことになる。

従来、アメリカが自衛権を広範囲に適用してきたのに対し、アメリカ以外の西側諸国はむしろ抑制的な解釈を取ってきた[32]。しかし、今回はむしろ積極的にアメリカと同じ立場に立った。この変化は一体何がもたらしたのであろうか。

ひとつの理由は、ニューヨークのワールドトレードセンタービルがハイジャックされた民間旅客機によって破壊されたことが、アメリカ単独の問題ではなく、世界全体の問題として捉えられたためと推測される。その結果、アメリカの個別的自衛権だけにとどまらず、他の国家も集団的自衛権の行使を認めるに至ったと考えられる。

その背景には、すぐれて現代的な状況が存在している。それはメディアの発達である。メディアやインターネットを経由した情報の流通は、急速に現れ発展した現代社会の特徴であり、多くの情報がリアルタイムに世界中に伝播する。我々は、いながらにして、世界

30「テロリズム」、『国際関係法辞典』（前注23）570頁。また、事件の前後の経緯を簡潔に記すものとして三野正洋、田岡俊次、深川孝行『20世紀の戦争』（朝日ソノラマ、1995年）587-588頁。

31 事件の翌日（9月12日）に早くも、北大西洋理事会が、今回のテロ行為がアメリカに対する武力攻撃であると認定されれば北大西洋条約第5条の適用に同意する旨を決定し、さらに10月２日には、武力攻撃とするに足る証拠をアメリカから提示されたためか、第５条の適用を決定した。

32 たとえば、前述のリビア航空攻撃に際して、ヨーロッパの一部の国家（フランスおよびスペイン）はアメリカ軍機が自国領空を通過することを許可しなかった。

中のいろいろな場所で起こった出来事を画像や音声を通じてほぼ同時に見聞することができる。サイバー攻撃も、ネットワークの発展という、まさに現代社会の特性を利用して行われるのであるが、今回の同時多発テロの場合、対象となったのが世界で最も注目される都市のひとつであるニューヨークであり、しかも、アメリカの、そして自由主義経済の繁栄の象徴ともいうべきワールドトレードセンターに対して、２機のハイジャック機が連続して突入した事実が重要であった。この映像は世界中に中継されたはずである。テロリストは、リアルタイムな情報中継によって世界中に自らのテロの効果を見せることに成功したが、それは同時に、世界中の多くの人々がこのテロの被害を世界共通の痛みとして理解することにもつながった。今回の同時多発テロによって、我々は、自分達が一体化を強めた国際社会の一員であることを実感し、この意識のもとで危機意識の共有化が達成された[33]。

その危機意識は各国にも共有化され、その結果が、アメリカの対テロ活動への速やかな支持、すなわちアメリカの自衛権行使に対する同調へとつながった理由ではないかと想像される。自衛権行使に対するこのような国際的同調により、テロ活動に対しても自衛権に基づく対応が行われる可能性が生じた。この自衛権行使の可能性は、サイバー空間を経由して行われるサイバーテロに関しても生じることになる[34]。

（４）サイバー攻撃に対する新たなアプローチ　－集団安全保障－

すでに検討したように、サイバー攻撃を武力攻撃として捉えられるのであれば問題は生じにくい。つまり、サイバー攻撃には、自衛権による対処が理論的に可能となるのである。しかし、実際にはそのような単純化が難しいことがサイバー攻撃の特性である。サイバー攻撃と見なされる攻撃には、個人による犯罪としてのそれも含まれており、その攻撃を即時に峻別することは難しい。個人の犯罪に対してまで、国家の自衛権を適用することには無理がある。また、テロリストによるサイバー攻撃についても、それを自衛権をもって対処しようとする動きはあろうが、それですべてをカバーできるとは限らない。技術的特性として示したように、サイバー攻撃は、個人から国家に至るまで、さまざまなレベルの攻撃者が実施して、等しく重大な被害を生じさせることができるのである。

---

[33] 国際問題研究所「ＩＴ革命と安全保障」研究会（2001年（平成13年）11月12日）における矢澤修次郎教授（一橋大学大学院社会学研究科）との討論から。

[34] たとえば、アメリカNational Defense University, Institute for National Strategic StudiesのK.L. Thachuk客員フェローは、テロリストグループも今や、新たな国際法主体として自衛権行使の対象となりつつあると指摘する。著者によるThachuk客員フェローとのインタビュー（2002年６月、ワシントンDC）。

たとえ自衛権を援用してサイバー攻撃に反撃することが可能であるとしても、すべてのサイバー攻撃に有効に反撃できるかどうかは疑問である。たとえば、攻撃を受けた国家が反撃しようとする場合には、サイバー反撃と軍事力を用いた従来型の物理的反撃との双方が考えられる。サイバー反撃を行おうとする場合、攻撃してきた国がサイバー反撃に脆弱であるとは限らない。サイバー攻撃を行おうとする国家は、事前に自らのサイバー防御能力を強化しているはずである。さらに、ネットワーク化が遅れている国家がサイバー攻撃を行ってきた場合、サイバー上で反撃しようとしても、攻撃国側にはサイバー反撃の対象となる適切な目標が存在しない可能性さえある[35]。

また、サイバー攻撃に物理的に反撃しようとする場合にも問題がある。サイバー攻撃は、ネットワークを経由して行われるために、地球上のいかなる場所に対しても攻撃が可能である。その点で、サイバー攻撃は彼我の距離を極限にまで縮め、ゼロにしてしまう。一方で物理的攻撃（反撃）には距離の壁が存在する。サイバー攻撃国が判明しても、その国家に反撃するための十分な軍事能力を有しない国家にとっては、自衛権は利用することが事実上不可能な権利でしかない。実際に、世界のあらゆる地域にまで反撃能力を有する国家は殆んどないのが現実である。現在までの「攻撃－反撃」関係は極めて物理的で実際的なものであった。国家は、自国を攻撃するかもしれない国家を具体的に想定し、その攻撃内容を予測した上で、攻撃の内容、規模に応じた物理的反撃能力を整備してきたのである。

このように個別的自衛権でカバーしきれない反撃能力を、集団的自衛権によって補うことは可能である。しかし、世界的規模での反撃能力を有する僅かな数の国家が、サイバー攻撃を受けたすべての国家に対して、常に集団的自衛権を行使して反撃してくれるとは限らない。集団的自衛権とは、自動的にあらゆる国家に対して発動されるものではなく、また、たとえ発動されたとしてもその内容が自動的に決まるものでもない。そう考えると、集団的自衛権と個別的自衛権を組み合わせることによって、サイバー攻撃に有効に対処しきれると考えることには問題がある[36]。

以上のような考慮の上に、我々にはサイバー攻撃に対する対処の根拠を見出す努力が求められる。サイバー攻撃は、実行者が多岐にわたり、攻撃の内容によっては、もたらされる被害が、程度の差こそあれネットワーク化され、その依存度を深めつつあるあらゆる国

---

[35] Greenberg, Goodman & Hoo, “Chapter 3. Responding to Information Warfare Attacks: International Legal Issues and Approaches,” *Information Warfare and International Law.* （前注11）(http://www.dodccrp.org/iwilchapter3.htm)

[36] 自衛権行使には、攻撃を受けた国家の恣意的な判断と濫用も懸念される。安全保障理事会が適切な処置を行わない限り、自衛権を名目にして、行き過ぎた武力行使が行われることも考慮しなければならない。

家に波及する。サイバー攻撃を行う側は、ネットワーク化の進展と社会のネット依存という点を利用して行動するのであるが、防御、対応する側にも、そうした攻撃の実態に即した思考法が求められるはずである。たとえば、実際に攻撃を受けた一部の国家による個別自衛権、集団的自衛権によって対処するだけではなく、サイバー攻撃の潜在的対象がネットワーク化されたすべての国家であり、しかも被害が国際社会の広い範囲にまで波及することを考慮して、サイバー攻撃を国際の安全に対する阻害要因と捉え、対処することを考えるべきではないだろうか。サイバー攻撃から防御される対象は、ある特定の国家や国民ではなく、広く国際社会と人類である[37]。この考え方は、戦争を違法化する中で、国連憲章が採用した集団安全保障の概念に通じるものである[38]。

つまり、サイバー攻撃がもつ上記のような性質を踏まえて、それを国際の平和と安全への破壊行為として認めることを出発点として、各種の活動を複数の法的根拠(犯罪対処や武力攻撃への対処)の下に同時並行的に行い、最終的に実行者、攻撃対象などの要因が判明し、適用されるべき法が明らかになった時点で、適切な法的根拠のもとに以後の行動を進めるという形態を想定する、そのための法制度に不備があれば速やかに整備してゆく、こうした総合的アプローチをとることがサイバー攻撃への対処上考慮されるべきではないだろうか。このアプローチは、問題が世界的であることから、国連を中心として実施されることが望ましいと考える。

異なる法的根拠に基づく行動を全体として包括するのは、サイバー攻撃が、いずれの行為者によって、いかなる目的で、どのような対象に向かって実施されようとも、それは国際社会の安定性を損なう不正な行為であるという集団安全保障に通じる理念である[39]。こうした理解を行うことによって、集団安全保障概念の下で、個人によって行われるサイバー攻撃に対しても、国際犯罪としての法的扱いを行って、いずれの地域においても処罰されるようにしておくことができる。自衛権援用が困難である可能性のあるテロリストによるサイバー攻撃に対しても、国際的な追及、たとえば多国間協力による追及やその温床となっている国家への制裁、体制変更要求などが可能となる。テロリストの追及、

---

[37] 同じ主旨の考えを示すものとして、A.D'amato, “International Law, Cybernetics, and Cyberspace”, chapter in volume on computer network attack and international law (Naval War College International Law Studies “Blue Book”, Volume7, publication in 2000), Para.24. (http://www.infowar.com/law/00/law_052600b_j.shtml)

[38] 国連安保理がサイバー攻撃を平和の破壊として認定し、行動する可能性を指摘するものとして、D.J.DiCenso, “Information Operations: An Act of War?”, *Aerospace Power Chronicles*, 31 July, 2000.（http://www.airpower.maxwell.af.mil/airchronicles/cc/dicenso1.html）

[39] たとえばダマトは、社会状況の変化に応じて古い法解釈を柔軟に変化させるべきことを主張する。D'Amato, “International Law, Cybernetics and Cyberspace”（前注37）Para.3.

逮捕には、彼らのもつ実力に応じて適切な組織が選択される。軍隊が適切であると見なされれば、軍事活動として実施されることになる。また、武力攻撃として行われたサイバー攻撃にも、攻撃された国家のみならず、あらゆる国家によるさまざまなレベルでの国際的共同対処が可能となる。

（５）サイバー攻撃問題に関してわが国がとるべき方策

わが国はネットワークに対する依存度をますます深めつつある。現在においても、インターネットに接続された端末機器は5,100万台（2002年4月）に達している[40]。携帯電話の端末数は7,000万台を越え、国民の半数が携帯端末を所有していることになる。この端末は今後、音声通信からデータ転送へとその利用の重心を移していくことが予想される。また、金融、経済、産業の各分野でのネットワーク化が進み、通信業界の開放も進められている。防衛庁、自衛隊のネットワーク化も急速に進むはずであるが、その中にも一般のネットワークとのインターフェースが設けられることになる。各家庭に供給されるネットワークの情報伝達性能も急速に向上し、秒あたりのデータ転送速度も、キロ単位からブロードバンドと言われるメガ単位にまでなってきている。今や、家庭にまで光ケーブルによるデータ供給が開始されている時代である[41]。

産業界、経済界、そして個人家庭までが利用するネットワークは、その多くが開放型のインターネットであることも重要なポイントである。すなわち、ネットワークへの依存がますます深化する一方で、そのネットワーク自体の外部からの攪乱に対する脆弱性は一向に改善されない危険な状況が継続することになる。

このようなわが国の場合、サイバー攻撃を通常の武力攻撃と同様な意思を伴った武力行使の一部と捉えれば、わが国に向けられた武力行使に関する従来の対応と同様に、自衛権をもって反撃できることになる。そしてその際には、反撃力として適切な手段が用いられることになり、サイバー反撃、物理的反撃、およびその双方の組み合わせが可能である。ただし、サイバー反撃は地理的な限界なく技術的に可能であるが、攻撃側は反撃に備えた十分な対処をとっている可能性が高く、効果がどれほど上がるかは疑問である。さらに、物理的攻撃力が低い国家によってサイバー攻撃が行われる時、そうした国家の多くは自分

40　1997年９月には、接続端末数はわずかに800万台でしかなかった。５年弱の間に８倍を越えている。(http://www.nua.com/surveys/how_many_online/asia.html)

41　わずか10年ほどの間に、通信速度は、毎秒当りの情報送信量で、パソコン通信と言われた2,400バイトから、54Kバイト、ISDNの1.5Mバイト、ADSLの８～12Mバイト、そして光ケーブルの100Mバイトへと急速に上昇した。

自身のネットワーク化が遅れていることが多いと考えられるが、その場合も、サイバー反撃が反撃としての意味を持たない。他方、わが国の物理的反撃能力には地理的にも能力的にも限界がある。わが国は、自国の周辺を越える領域への反撃能力を有していないし、攻撃が大規模であった際の十分な物理的反撃力を保持しているわけではない。しかし、そうした事態に有効に対処するために日米安全保障体制が用意されており、不足する反撃力はアメリカによって補填されると考えられる。サイバー攻撃に対して、アメリカが日本と共同して物理的攻撃力使用を含めて反撃してくれるように、自衛権行使についての共通理解を確立しておく必要がある。さらに加えて、一国（この場合は日本）に対するサイバー攻撃を世界全体への攻撃と捉え、国際の平和と安全への脅威、破壊とすることで国際社会全体による対応を求める方策の有効性を考慮する価値もある。そうした行動を取ろうとする際には、サイバー攻撃が実施されたことを示す証拠の開示が求められることになるため、そのための技術開発は必須である。いずれにせよ、サイバー攻撃を武力攻撃とすることができれば、サイバー攻撃を行った者の側に違法性があることになり、反撃の合法性が確保されることになる。

以上のように考えた上で、わが国がサイバー攻撃に関してとるべき方策は、以下のようなものではないだろうか。

・犯罪と捉えられるサイバー攻撃に対しては、国際的な犯罪としての対応を行うべく、国際的法規制が実施されるように提起する。実際の行動としては、欧州評議会において起草されたサイバー犯罪条約の早期批准や、加盟国の増加促進、サイバー犯罪取締りのための技術移転などが考えられる。

・武力攻撃と同様の目的と効果を狙うサイバー攻撃に対しては、これを従来からの武力攻撃の範疇に入るものとして国際法上禁じられると主張し、そうしたサイバー攻撃に対しては、自衛権を根拠とした対処が可能であると国際社会に認知させる[42]。このような主張は、国連やサミットなどの国際的交渉の場においてなされることが望ましい。実際の自衛権行使の際には、サイバー攻撃の実態が外部からは容易に認識できないことを考え、できるだけ詳細な攻撃の証拠を収集しておくことが必要である。自衛権行使の判断は個別の国家が行うが、国際社会がその合理性如何を判断することになるため、攻撃に関する証拠の収集、分析と開示は重要な問題である[43]。このような任務を実施するために、自衛隊の内部にサ

---

[42] 定義を国際的に明確にすべきことが必要と主張するものに、Greenberg, Goodman & Hoo, "Conclusion," *Information Warfare and International Law.*（前注11）（http://www.dodccrp.org/iwilchapter4.htm）

[43] Jacobson, *War in the Information Age: International Law, Self-defense, and the Problem of "Non-Armed" Attacks,*（前注27）Part IV. Paradigm Shift.

イバー攻撃と防御を研究し、サイバー防衛を行うサイバー戦部隊の設置が必要である。
・さらに、わが国単独、またはわが国と他国の集団自衛権行使だけで対処しきれないケースを考慮し、加えて他の国家にも同様の事態が生じる危険性を考えて、サイバー攻撃を国際の平和と安全に対する脅威、破壊と認め、その認定の下で世界各国がそれぞれ対処を行うように、集団安全保障の概念をサイバー攻撃問題に適用するべく国際社会に働きかける。この働きかけは、集団安全保障機能を果たす機関である国連において行われるべきであると考える。そうした基本的理解の国際的な醸成が、ひいてはわが国の安全確保につながっていくはずである。
・国内においては、サイバー攻撃に対する脆弱性を限定化するため、公的部門と民間部門との協力を進める。また、公的部門においても、警察部門と防衛部門等、対応可能な能力を持つ機関の協力関係を強化すると共に、適切な対処を行うための共同化を進める必要がある。この協力は、被害情報の相互開示だけにとどまらず、対応の法的根拠を明確にするために必要な証拠収集、分析に関する技術協力も含む広範なものとなるべきである。具体的には、現在ＩＴ戦略本部が整備しつつある対処体制の構築を促進して、サイバー攻撃への対処情報の一元化を図ることが考えられる。その中には、サイバー攻撃に対する防御方法を研究し、実施するための組織を設けることが含まれる。たとえば、既に警察組織内に存在するサイバーポリスに、前述の自衛隊サイバー戦部隊と民間部門のサイバー防御技術開発者とを加えた組織などが想定される。
・さらに、こうした国内対応についての情報を他国にも提供し、国際的な技術交流と協力によって、より有効な各国間の対応協力に結びつける努力が必要である。実際には、それぞれの国が独自に構築しつつあるサイバー防御システムの相互接続などが考えられる。

ネットワーク依存大国であるわが国の場合、サイバー攻撃に関しては、これを犯罪としても武力攻撃としても認識し、法的対処が可能な行為として位置付け、対応のための制度を整えておくべきである。サイバー攻撃に関する法制度が形成されようとしている現在においては、サイバー攻撃のもたらす被害の甚大さと対処の困難さを明確に認識し、通常時から警告を発し続けると共に、事態の発生した際には積極的な行動を示すことが重要である[44]。

[44] 政策決定者や関係者の発言や行動がサイバー攻撃に関する法制度の発展に影響を与えると説くものに、Department of Defense, *An Assessment of International Legal Issues in Information Operations*,（前注11）pp.20-22, p.27 and p.52.

おわりに

本小論においては、これからの安全保障に重大な影響を及ぼす可能性のあるサイバー攻撃について、その技術的特性を考慮した上で、適用される法制度と問題点を検討してきた。

サイバー攻撃への対処は、サイバー空間における攻撃実行者が多様であること、攻撃の結果が広範かつ重大な社会的脅威になりうることを考えると、必然的に多面的、重層的なものとならざるを得ない。今日の社会は、社会への攻撃という行為に対して定義と対処の分担を明確にしてきたが、サイバー攻撃に関しては、従来とは異なり、より柔軟な対処が必要となってくる。逆に言えば、攻撃者が、対処に関するそうした柔軟性の欠如部分を、制度面からも技術面からも狙ってくるのがサイバー攻撃の特徴である。

実際には、国際レベルでは、犯罪や脅威としての共通認識に基づく国際協力を進めることが必要である。一方、国内レベルにおいては、ネットワーク化された社会の特性に注目して、官と民との間の協力や、官の中における各部門の協力関係構築が求められる。また、法規制を執行するに際しては、攻撃者の能力、実力に応じて、適切な対処能力を有する組織を選択することが必要である。我々がネットワーク化社会の只中にいる以上どうしても避けては通れないサイバー攻撃という問題に対しては、警察や軍、民間が国際的、国内的にさまざまに連携しつつ共同して対応することが重要であり、そうした体制を構築しない限り、サイバー攻撃への有効な対処は不可能である。