第３章　サイバースペースのガバナンス

土屋　大洋

はじめに

インターネットを発展させてきた技術者たちの間では、インターネットの基本原理は「自律・分散・協調」であるといわれてきた。そこでは中心となる組織が存在せず、個別の目的に特化した組織が自律的な運営を行っている。全体としてみるとインターネットの各種の機能は分散的に維持されているが、しかし、それぞれは協調を前提としている。一般的な政治は代議員などに権限を託すという意味で「他律」的であり、権力の「集中」が前提となっている。そして、それに従うという「統制」が求められている。つまり、「他律・集中・統制」である。こうして対比的に考えれば、インターネットの「ガバナンス」は、既存の「ガバメント」とはずいぶん異なるものであることが分かる。

マサチューセッツ工科大学教授のデービッド・クラーク（David Clark）はかつて「われわれが拒否するもの：王、大統領、投票。われわれが信じるもの：ラフ・コンセンサスとランニング・コード」と述べたことがある。クラークはインターネットがアナーキーだといいたかったわけではないが、1970 年代の反権力的なヒッピー文化の影響もあり、インターネットでは独自のガバナンスが追求されてきた[1]。

ところが、インターネットが社会において重要なインフラストラクチャと見なされるようになると、そのセキュリティが問題となってきた。もともとインターネットは性善説に基づいて設計されており、悪だくみをする人間も含めて、これほど多くの人が使うことは想定されていなかった。そのため、政府が責任をもって管理すべきであるという声も日増しに強くなっている。そして、「サイバー戦争」ともいわれるような状況が視野に入ってくると、各国は「サイバー軍」を組織するようにもなっている。

その結果、インターネットを作り、運営してきた技術者たちのギーク（オタク）文化、政府の役人や企業人たちのスーツ文化、そして、軍服を着た軍人たちのユニフォーム文化が対立するようになってきている。

以下では、インターネット・ガバナンスをめぐる問題を、資源問題、デバイド問題、ガバナンス問題、フリーダム問題、セキュリティ問題に分けて整理した後、国連総会第一委員会での政府専門家会合とソウルでのサイバースペース会議を題材に、近年のサイバースペースのガバナンスについて、グローバル・コモンズを念頭に置きながら、検討していきたい。

１．サイバースペースにおけるガバナンスをめぐる諸問題

（１）資源問題

そもそも、インターネット・ガバナンスが問題となるきっかけとなったのは、インターネットにおける希少資源である IP アドレスとドメイン・ネームの問題であった。インターネットでも個別の機器を特定するために電話番号のような番号が振られており、これを IP アドレスといっている。初期の IP アドレスの配分はおおざっぱに行われており、インターネットの初期から中心的な役割を担ってきた米国のスタンフォード大学が保有していた IP アドレスの数は、遅れてインターネットに参入してきた中国一国よりも多かったといわれている。IP アドレスは数字の集合であり、桁数が限定されているため、それは有限の資源である。IP バージョン 4（約 42 億個）の IP アドレスはすでに在庫が尽きているため、既存のアドレスの再利用や IP バージョン 6（約 340澗(かん)個）への移行が必要になっている。これは想定を上回る数の機器・端末がインターネットに接続されるようになったためである。

ドメイン・ネームとは、「jiia.or.jp」や「amazon.com」といった人間にとって分かりやすい文字列である。本来なら電話と同じく IP アドレスだけですべてを運用することもできる。しかし、「jp」が日本を表し、「or」が非営利組織、「jiia」が日本国際問題研究所、「com」が商用サイト、「amazon」が社名といった具合に整理することで、人間にとってはウェブページや電子メールの相手の所属を容易に理解できるようになる。

ところが、ドメイン・ネームもまた有限である。例えば、リンゴ生産農家やアップル・レコード社はいずれも「apple.com」というドメイン・ネームを利用するインセンティブをもっているが、実際にはコンピューターのアップル社がそれを先に取得し、使い続けている。世界中でドメイン・ネームは一義に決まるようにしなくてはならないので、希少な文字資源の奪い合いという状況が起きた。

もともとこの IP アドレスとドメイン・ネームを管理していたのは米国の南カリフォルニア大学教授のジョン・ポステル（Jonathan Postel）であり、彼の組織 IANA（Internet Assigned Numbers Authority）であった。インターネットの利用者が 1990 年代後半に増加するにつれ、ポステルは IP アドレスとドメイン・ネームの管理業務を、1998 年に設立された ICANN（Internet Corporation for Assigned Names and Numbers）に移すことにした。

ところが、ICANN を維持・運営するのは誰かという点が問題になり、これがインターネット・ガバナンスをめぐる問題の端緒となる。ICANN は米国カリフォルニア州の NPO 法人となっていたが、グローバルな存在であるはずのインターネットの根幹機能を、国際機関ではなく、米国の NPO 法人が担うのはおかしいのではないかという批判が出てきた。さら

には、ICANN 設立時の理事選出過程が不透明であるという指摘もあった。

そこで、19 人の理事のうち 5 人が、世界 5 つの地域（北米、ラテン・アメリカ、アジア・太平洋、アフリカ、ヨーロッパ）から選ばれる形で改選されることになった。当初の想定では 5000 人ぐらいによるオンライン投票であったが、ふたを開けてみると各国のナショナリズムが吹き荒れ、投票しようとする登録者は 7 万人を超える事態となった[2]。

特に、登録者数が多かったのがアジア・太平洋である。北米が 1 万 694 人、ヨーロッパが 2 万 3519 人にとどまったのに対し、アジア・太平洋は 3 万 8397 人にのぼった。日本からは 19 人の理事のなかにすでに慶應義塾大学教授の村井純が入っていた。ところが、当時は日本のインターネット利用者数が中国の利用者数を上回っていたため、日本からもうひとりが理事会に入る見込みとなり、これに反発した中国が登録を呼びかけたため、日中で登録競争が始まり、ナショナリズムを刺激することになってしまった。結果的に富士通の加藤幹之が理事に当選するが、これが中国における ICANN 不信を高める一因となった。ICANN 側も一般投票による理事選挙は妥当ではないとして、これ以後行っていない。

中国がもうひとつ問題としたのは、ルート DNS（Domain Name System）サーバーの配置である。ドメイン・ネームが世界で重複することがないよう、ドメイン・ネームと IP アドレスの対応関係を収めたデータベースが DNS サーバーである。世界には無数といってよいほどの DNS サーバーが設けられているが、そのそれぞれにすべての情報が収められているわけではない。不明なドメイン・ネームの問い合わせが来ると、それぞれの DNS サーバーは階層的に上位の DNS サーバーに問い合わせを送る。水平的なネットワークをモットーとするインターネットの中で唯一といっても良いヒエラルキー構造が DNS である。そして、世界の 13 ヵ所に、最上位のルート DNS サーバーが設置されており、そのうち 10 ヵ所は米国、2 ヵ所がヨーロッパ、1 ヵ所が日本にある。中国は当初、すべてのインターネットの通信がルート DNS サーバーを通るものと誤解していたこともあり、この地理的な配置が問題だと指摘した。誤解が解けた後も、米国偏重や、利用者数拡大が見込まれる中国に置かれていないことを繰り返し指摘することになる。

（２）デバイド問題からガバナンス問題へ

こうした問題が繰り広げられていたのと並行して、2000 年 7 月には G8 の九州・沖縄サミットが開かれた。当時は 2001 年の対米同時多発テロ（9.11）も起きておらず、深刻な国際問題は顕在化していなかった。そのため、日本政府はグローバルなデジタル・デバイドの問題を議題に取り上げ、G8 首脳は「グローバルな情報社会に関する沖縄憲章」を打ち出した。単なる宣言に終わってはいけないとして、デジタル・オポチュニティ作業部会（ドッ

トフォース）が設置されることになった。

ドットフォースが画期的だったのは、政府代表、民間企業代表、NPO という 3 つのセクターからそれぞれ代表を出し、問題を討議するという「マルチステークホルダー・アプローチ（政府だけではなく民間企業や市民社会も参加すること）」をとったことだった。それまでの外交は、外務省が行うのが当然であり、特定の業界が絡む経済交渉などでは経済産業省（旧通商産業省）や総務省（旧郵政省）などが参加することもあった。しかし、民間だけでなく、NPO までもが、タスクフォースとはいえ、参加するのは異例であった。

ドットフォースは翌年の G8 ジェノバ・サミットまでに報告書をまとめ、首脳会議に提出した。しかし、報告書だけでは実現性を伴わないため、さらに 1 年間、実施計画をまとめることとされ、ドットフォースの活動は延長されることになった。ところが、この頃は世界的にグローバル化反対運動が盛んであり、ジェノバ・サミットではデモに際して死者まで出てしまった。さらに、サミット後の 9 月には 9.11 テロが起きてしまい、国際政治の様相が大きく変わってしまう。

2002 年にカナダで開かれた G8 カナナスキス・サミットは、厳重な警戒の下で行われ、参加者が極度に絞り込まれた。ドットフォースの実施計画書は提出されたものの、テロ対策にかき消されてしまった。

実は 2001 年 9 月 11 日当日、ニューヨークの国連本部で、国連 ICT タスクフォースの会合も開かれるはずだった。このタスクフォースは、G8 よりも大きな枠組みである国連を使い、その事務総長の主導で、デジタル・デバイド問題を検討しようというものであった。当然ながら、この会合はキャンセルされてしまったが、国連の枠組みの下でデジタル・デバイドを検討しようとする試みは、国連の専門機関である国際電気通信連合（ITU）に受け継がれることになった。

ITU は、国連自体よりも古い国際機関であり、19 世紀の万国電信連合に起源をもつ。ITU は国連の専門機関だから、民間の専門家が必要に応じて参加するものの、各国の政府代表が主導する枠組みである。そして、それが主管するのは電信・電話であり、新しい通信であるインターネットは含まれていなかった。インターネットは民間主導で草の根的に発展してきたものであり、各国政府の規制権限は各国でバラバラで、少なくとも米国のビル・クリントン政権とジョージ・W・ブッシュ政権は不介入の姿勢をとっていた。

しかし、ITU は、グローバルなデジタル・デバイドの解消を名目に、世界情報社会サミット（WSIS）を開催することとし、世界各地域での準備会合とともに、2003 年に ITU 本部のあるスイスのジュネーブ、2005 年にチュニジアのチュニスで本会合を開くこととした。

その WSIS は各地域の準備会合から波乱含みとなった。インターネット・ガバナンスに

国際機関や政府が介入してくることに対して、従来のガバナンスの担い手である技術者たちから強い反発が出てきた。上述のように、インターネットのガバナンスは自律・分散・協調的にいろいろな機関が行っており、それまで政府の介入なしで成立してきた。たとえデジタル・デバイドの解消が目的だとしても、介入は受け入れられないという声が強かった。それに対して、中国をはじめとする一部の国々は、インターネットはますます重要な社会的インフラストラクチャになりつつあり、政府が責任をもって管理すべきだと主張していた。

その結果、2003 年のジュネーブでの本会合では、デジタル・デバイド解消策よりも、インターネット・ガバナンスとはそもそもなんなのかという点が議論の焦点になってしまった。それを受け、インターネット・ガバナンスの定義を定めるためのワーキンググループとしてインターネット・ガバナンスに関するワーキンググループ（WGIG）が 2004 年 11 月に設置され、2005 年のチュニジア本会合に提言することになった。

2005 年になっても議論は収束せず、チュニジアの本会合でも同様の議論が行われ、一応のデジタル・デバイド解消が謳われたものの、インターネット・ガバナンスについてはインターネット・ガバナンス・フォーラム（IGF）が 2006 年 7 月から組織され、現在まで議論が続けられている。特に、ITU のインターネットに対する管轄問題は、2012 年 12 月にドバイで開かれた世界国際電気通信会議（WCIT）での規約改訂交渉でも議論されたが、事実上の決裂で終わった。

（３）フリーダム問題

インターネット・ガバナンスをめぐる議論のひとつの極となったのは中国である。中国は国内では「金盾」といわれる情報統制のシステムを構築し、海外との通信も政治的に規制している。それでも、成長する中国経済は、各国の企業にとっては将来的な収益源に見えた。そこで、マイクロソフトやグーグルといった米国の IT 企業も中国市場に参入した。その際、中国政府は、中国政府の規制に従うことを各企業に求めていた。

ところが、2010 年 1 月 12 日、突然、米国のグーグル社が中国政府に対しインターネットの検閲撤廃を求めることを明らかにし、同時に、グーグル社が提供する電子メール・サービスが中国からのサイバー攻撃を受けたことも発表した。そして、中国政府との交渉が決裂すれば、中国市場から撤退する可能性も示唆した。米国政府もすぐにこれに反応し、国務省の広報担当者が「すべての国はネットワークの安全を維持する義務がある。それには中国を含む。ネット上の不正行為は犯罪とすべきだ」と語ったという。

ヒラリー・クリントン（Hillary Clinton）米国国務長官（当時）もすぐに声明を出し、「非

常に深刻な懸念と疑念を抱く」と述べた。さらにクリントン長官は、1 月 21 日、米国の首都ワシントン DC のニュースに関する博物館「ニュージアム」で演説し、「情報ネットワークの拡散は、われわれの地球の新しい神経系を形成しつつある」と述べ、「権威主義体制の国々でも情報ネットワークは、人々が新しい発見をするのを手助けし、政府をより責任あるものにしている」と指摘した。そして、米国務省は外交的な課題としてインターネットの自由の問題に取り組んでいくことを表明した。

この問題は当初、クリントン長官の演説の効果もあって、情報の自由に関する問題と受け止められた。しかし、実際には、サイバー攻撃に関するセキュリティ問題の側面も強い。グーグルのニコール・ウォン（Nicole Wong）副社長（当時）は、（1）2009 年 12 月半ば以来、グーグル本社の企業インフラを標的とする中国からの高度のサイバー攻撃が急増した、（2）米国のインターネット、金融、技術、マスコミ、化学分野などの大企業 20 社以上が同様に標的となり、攻撃を受けている、（3）この種の攻撃の第一の目的はまず標的あるいは標的と関連のある G メールへの秘密の侵入だと思われる、（4）特に米欧在住を含む中国の人権活動家たちにかかわる G メール・アカウントは第三者により定期的に侵入されていることが判明したなどと証言した。

（４）セキュリティ問題

「サイバー攻撃」が何を意味するのかは、必ずしも確定していない。サイバー攻撃によって直接的な死者が出た事例もまだないだろう。しかし、2007 年のエストニア、2008 年のグルジアなどをはじめとして、各種のサイバー攻撃が知られるようになった。

特に近年では APT（Advanced Persistent Threat）と呼ばれる各種の情報窃取の手法が用いられ、攻撃されていることすら分からない形のサイバー攻撃が広く行われている。欧米や日本などに対するサイバー攻撃は日常茶飯事になりつつある。

米国は戦略軍の下にサイバー軍（USCYBERCOM）を設置し、防衛だけでなく攻撃も軍事作戦として行うようになっている。イランの核施設に対する STUXNET 攻撃は、米政府は認めていないものの、米国とイスラエルの共同作戦だったといわれている。

各種のサイバースペースをめぐる問題を議論すべく、英国のウィリアム・ヘイグ（William Hague）外相の呼びかけで、ロンドンでサイバースペースに関する国際会議が開かれ、60 ヵ国が参加した。この会議は何かを決めるための公式な会議ではないが、サイバーセキュリティをはじめとして活発な議論が展開される場となった。この会議の開幕に当たってウィキペディアの創設者のジミー・ウェールズ（Jimmy Wales）は、「インターネットへの最大の脅威はサイバー犯罪ではなく、政府のまちがった政策や行き過ぎた政策だ」と警告した

が、ヘイグ外相はサイバー攻撃の脅威について警告した。

これらの動きを受け、国連総会は、2011 年 12 月の決議で、安全保障を担当する第一委員会の政府専門家会合（GGE）において規範等について議論することを明確化した。

2012 年にはロンドン会議に続くブダペスト会議がハンガリーで開かれた。そして、2013 年 10 月には韓国でソウル会議が開かれた。

以下では、国連 GGE の報告書と、ソウルのサイバースペース会議について見ていこう。

２．国連 GGE

（１）国連を舞台にしたサイバーセキュリティ交渉

2011 年 9 月 12 日、中国、ロシア、タジキスタン、ウズベキスタンの４ヵ国は、国連に情報セキュリティ国際行動規範の案を提出した。この４ヵ国は、サイバースペースで各国が責任ある行動をとるという国際行動規範を作るため、国連総会がこれを議論すべきだとしていた。提案を受け取った国連の潘基文事務総長は、これを国連総会の第一委員会に付託した。国連総会の下には 6 つの委員会が設けられているが、第一委員会は軍縮・国際安全保障を扱っている。

国連総会第一委員会は 4 ヵ国の提案を受けて、15 ヵ国の代表による政府専門家会合（GGE）を開催し、検討を求めることにした。GGE とは、各国政府のなかから特定の専門家を集めた協議グループのことで、武器貿易条約や宇宙活動などでも招集されたことがある。

サイバースペースに関する GGE は、実は今回が 3 回目である。第 1 回が 2004 年から 05 年、第 2 回が 2009 年から 10 年、そして第 3 回が 2012 年から 13 年になる[3]。

このサイバーGGE を始めるきっかけは、1998 年の米露首脳会談にさかのぼる。この会談の共同声明において、ロシア側はサイバーセキュリティ（当時は「情報セキュリティ」といっていた）を大々的に取り上げようとしていた。ところが、米国側がこれに乗らず、全 15 段落の共同声明のうち、ようやく第 14 段落でこの問題が取り上げられた。そこでは、「われわれは、今起こりつつある情報技術革命のポジティブな側面を促進し、ネガティブな側面を軽減する重要性を認識する。それは両国の将来の戦略的安全保障利害を確かなものとする際の重要な挑戦である」とされ[4]、両国の対話を続けていくとされた。

（２）中露の求めるサイバーセキュリティ

当時は米国がビル・クリントン（Bill Clinton）大統領、ロシアがボリス・エリツィン（Boris Yeltsin）大統領の時代である。インターネットのドット・コム・ブームが始まろうとして

いた頃で、多くの人がまだ電話線によるダイヤルアップ接続でインターネットを使っていた。米国との協議が不調に終わったロシアは、国連を使って情報セキュリティを議論しようと画策し始めた。

この頃の構図は、米国を中心とする自由主義諸国と、上海協力機構（SCO）に参加する国々の対立になっていた。SCO は、ロシア、中国、カザフスタン、キルギス、タジキスタン、ウズベキスタンの 6 ヵ国による多国間協力組織であり、2001 年に成立しているが、前身となる上海ファイブ（ウズベキスタンを除く 5 ヵ国首脳会議）は 1996 年に成立している。

ロシアや SCO 諸国は情報セキュリティをインフラストラクチャと情報そのもの（あるいはコンテンツとしての情報）を含む広いものとして定義しようとしていた。ところが、米国等は、表現の自由を支持する点から情報を含むことに反対し、情報セキュリティはインフラストラクチャに限定すべきだとしていた。

従来のロシアの主張は、近年では中国に受け継がれている。ただし、中国は、ロシアのようにコンテンツを含めろと直接的にはいっていない。むしろ、定義の問題は回避しながらも、主として 2 つの主張をしている。第 1 に、欧米が主張するような民間に任せるインターネット・ガバナンスではなく、政府や国際機関がサイバースペースに責任をもつべきである。第 2 に、サイバースペースは新しい特殊な領域であり、既存の国際法を適用するのではなく、新しい条約等で対応すべきである。

これらの主張の背後にあるのは何なのだろうか。第 1 の点については、各国ごとの主権をサイバースペースで認めさせ、各国が独自の政策判断に基づき、規制や介入を可能にしたいということのようである。米国政府やインターネット・ガバナンスを担う技術者たちは、政府はサイバースペースに介入すべきではないと言い続けてきた。これをひっくり返したいというのが中国の第 1 の狙いである。

第 2 の点については、従来の国際法が適用されるとなると、言論の自由や通信の秘密などの人権がサイバースペースにも適用されることになり、仮に政府の介入が認められるようになったとしても、検閲や通信傍受がしにくくなる。それを各国の判断として行ったとしても、他国から非難を受けないようにするためには、「サイバースペースは特別であり、既存のルールはそのままでは適用されない」という認識を定着させる必要があり、そのためには、欧米主導ではなく、中露が積極的に参加する枠組みにおいて新たな条約等を作りたいという狙いである。

（３）前哨戦としての GGE

2013 年 9 月の国連総会を前に、第 3 回の GGE の報告書が国連のウェブページで 8 月に公開された。

交渉に参加した政府関係者によれば、6 月の最終交渉は難航したそうである。大きく分けて議論は、(1) 国際規範、(2) 信頼醸成措置、(3) 能力構築、の 3 点あった。このうち、最もスムーズにまとまったのは能力構築である。つまり、人材育成や技術開発、普及啓発といったことについては異論が出にくい。最も議論が分かれたのが国際規範であり、十分な議論ができずに終わったのが信頼醸成措置である。

今回の交渉では、オーストラリア代表が議長を務めた。1 月にスイスのジュネーブで行われた交渉の際、議長が報告書の文案を提出した。この議長案をめぐってさまざまなやりとりが行われた後、各国はこれを持ち帰って、議論することになった。

そして、最終案を決めるために 6 月に 15 ヵ国の代表がニューヨークに集まった。そこで特に問題となったのが、国際規範の構築における既存の国際法の扱いであった。日米欧豪は結束し、国連憲章を含む既存の国際法がサイバースペースにも適用されるという立場をとった。それに対し、中露は新たな枠組みが必要だとし、先述の 2011 年の 4 ヵ国からの提案をベースに設定しようとした。

しかし、最終日になっても、議論はまとまりそうになく、ロシアは比較的柔軟な姿勢を見せたものの、中国はかたくなに既存の国際法の適用に反対し続けた。業を煮やした議長が、決裂も辞さない覚悟で中国代表と談判し、「このまま決裂すれば、各国は中国のせいで決裂したという声明を出すだろう」と指摘し、妥協を迫った。中国代表は、交渉中も電話をかけ、おそらく本国と調整を図った。その結果、国際交渉ではよくあることだが、双方にとって都合の良い文言が選ばれることになった。

例を挙げてみよう。

> 【第 16 段落】国家による ICT［情報通信技術］利用にとって重要となる、既存の国際法から導き出される規範の適用は、国際的な平和、安全保障、安定へのリスクを減じるのに不可欠な措置である。（中略）ICT のユニークな特性に鑑みれば、追加的な規範がやがて発展し得る。

既存の国際法は不可欠だとする点で日米欧豪側の主張を入れながら、他方で追加的な規範がやがて発展し得るとすることで、新しい枠組みが必要だとする中露の主張にも配慮している。

【第 19 段落】国際法、特に国連憲章は、平和と安定を維持し、オープンで、安全で、平和的で、アクセス可能な ICT 環境を促進するために適用可能（applicable）であり、不可欠である。

国連憲章というユニバーサルな国際法が適用可能であるとする点で日米欧豪側の主張に近くなっているが、「適用される（applied）」という断定的な表現ではなく、「適用可能（applicable）」という含みをもたせた表現にすることで、中露が納得しやすくしたことになる。

また、信頼醸成措置については、意見交換、諮問枠組みの創設、情報共有、コンピュータ緊急事態対策チーム（CERT）間連携、事案協力、法執行協力に言及した。

第 3 回のサイバーGGE は、1990 年代末にロシアが提起し、中国が受け継いだ問題を解決するには至らなかった。むしろ、それについての 2 つの陣営の対立を確認し、結論を持ち越したと見るべきである。

３．ソウル・サイバースペース会議

（１）受け継がれる国連 GGE の議論

2013 年 10 月 17 日と 18 日、韓国の首都ソウルに世界 87 ヵ国から 1000 人以上が詰めかけた。第 3 回のサイバースペース会議に参加するためである。

初日の冒頭、韓国の朴槿恵大統領が登場し、ヘイグ英外相も挨拶をした。日本からは三ツ矢憲生外務副大臣が参加し、各国からも外務大臣やそれに準じる副大臣などが登壇した。

サイバースペース全般について論じる会議なので、ブロードバンド・アクセス技術の普及やデジタル・デバイド、人材育成・研究開発といった問題も論じられたが、主題はサイバーセキュリティとサイバー犯罪だったといってよい。大臣たちの発言も多くがその点に触れていた。

いくつかのパネル討論が設けられたが、そのなかでも最も注目されたのは「国際安全保障」と題するパネルである。司会は米国のシンクタンク CSIS（戦略国際問題研究所）のジェームズ・A・ルイス（James A. Lewis）である。パネルには、米国、ロシア、中国、オーストラリア、韓国の代表などが参加した[5]。

司会のルイスは、国連総会第一委員会の政府専門家会合（GGE）の調査委員としてかかわっていたため、必然的に話題は GGE 報告書を受け継いだものになった。ルイスは、パネルの冒頭で「GGE はサイバーセキュリティのランドスケープを変え」、そして、元米 CIA の職員で NSA による情報収集活動を暴露した「エドワード・スノーデン（Edward Snowden）

によってダイナミクスが変わった」と指摘した。サイバースペースにおける国際安全保障は、新しい局面に入ったというのである。

そこで、ルイスは、議論を始める前に韓国のインテリジェンス機関である国家情報院（NIS）の幹部を壇上に上げた。彼は、北朝鮮が数千人を使ってサイバー攻撃を企図しており、韓国のメディア、金融機関、企業、そして重要インフラストラクチャが狙われているという。しかし、サイバーセキュリティの世界では、攻撃者の特定が難しいため、制裁や抑止が働かない。そこで、国際協力が必要になっていると指摘した。インテリジェンス機関といえども、各国独自の活動だけでは成り立たなくなっていることを示唆したといえよう。

パネル討論に移ると、米国代表のクリストファー・ペインター（Christopher Painter）は、国連 GGE の報告書が発表されるなど、2013 年は画期的な年だったと評価した。GGE 報告書で国連憲章など既存の国際法の適用が確認され、国家はプロキシー（代理人）によるサイバー攻撃を禁じられ、信頼醸成措置によって予測性を高め、エスカレーションを回避するための枠組みの構築に合意することができたという。

ロシアのインターネット大使であるアンドレイ・クルツキフ（Andrey Krutskikh）は、一国主義的な対応ではグローバルな問題を解決できず、サイバースペースにおける軍拡競争は安定につながらないという。ロシアや中国は 2009 年に SCO で一定の合意を得ており、これを他国もモデルにすべきだと提言した。そして、国連に働きかけ、2014 年にもう一度 GGE を開くという。

中国の国際問題研究所の徐龍第（Xu Longdi）は、GGE の報告書で「国家による責任ある行動」とあるように、「責任ある（responsible）」という言葉が入ったことが重要であると指摘した。そして、サイバースペースにおける国家主権の概念を詰めて行く必要があると論じた。

一通りの議論の後、司会のルイスは、「GGE において各国はマルチステークホルダー・アプローチには合意できたが、しかし、軍事面については合意できなかった」とし、どこでこの問題を論じるべきかと問いかけた。中国の徐は、「将来のための議論には国連がベストな場所だ」と答えた。すると、すぐに米国のペインターが反応し、「国連の役割は誇張されている。インターネット・ガバナンスを国家だけが議論できるわけではない。そこにはたくさんの組織が関係している」と指摘した。

ロシアや中国は、国連において、国家主導でサイバーセキュリティの問題を収めようとしている。それに対し、米国や欧州、日本、オーストラリアなどは、これまでのインターネット・ガバナンスの在り方を尊重し、国連だけで議論を進めるのは不適切だと主張して

いる。インターネットないしサイバースペースは、国家による制約のないところで、民間の力で成長してきており、そのガバナンスを崩すべきではないとしている。

（２）タリン・マニュアル

結局のところ、サイバースペースを律するグローバルな法律やルールについて各国が合意できていないために、こうした議論が行われている。中露は新条約によってこれを解決すべきだとしているのに対し、日米欧豪などは、既存の国際法をサイバースペースに適用すべきだと主張している。

後者のひとつの試みが、タリン・マニュアルである。2007 年にエストニアに対する大規模なサイバー攻撃が行われた後、エストニア政府は首都タリンに北大西洋条約機構（NATO）の研究施設協調的サイバー防衛研究拠点（CCDCOE）を誘致した。ここには NATO 加盟国の軍人や政府職員、弁護士や研究者などが集まり、サイバーセキュリティに関する研究が行われている。そこでのひとつのプロジェクトとして「サイバー戦争に適用される国際法についてのタリン・マニュアル」が検討された。

タリン・マニュアルは 2013 年春に書籍の形で公開された[6]。そこには 95 個のルールと、その解説が収められている。作成に当たったのは 19 人の国際法学者であり、そのリーダーは米国海軍大学校教授のマイケル・シュミット（Michael Schmitt）である。

このタリン・マニュアルは、エストニア政府にも NATO にも公式にはオーソライズされていない。あくまでも CCDCOE の研究成果のひとつである。それでも、サイバー戦争に関する国際法解釈の重要なスタンダードになっている。

しかし、これが NATO の枠組みのなかで行われたために、ロシアや中国などは参加しておらず、これらの国々ももちろんオーソライズしていない。2001 年に締結されたサイバー犯罪条約と同じく、NATO で勝手に作ったものであり、中露が拘束される理由はないという見解である。中露は、中露やその他の国々も一緒になって国連で新しい条約を起案すべきだと主張する。

（３）ねじれた議論

中露の主張は、SCO 諸国を中心に、発展途上国でもそれなりの支持を集めている。世界の多くの国はインターネットなどのメディアを検閲下に置いており、日米欧豪などが主張する情報の自由な流通ではなく、情報の統制を正当化するような国際条約を欲しがっている。

しかし、議論がややねじれているのは、NATO の下で作られたタリン・マニュアルを見

ると、例えばルール 1 やルール 2 では、国家はサイバースペースにおいてもその領域のなかにおいて国家主権を行使できるとしていることである[7]。これはどちらかというと中露の主張に近い。

無論、どの国もサイバースペース全体に主権を行使することはできない。しかし、何らかの形でサイバースペースにおける領域を主張することができれば、そのなかでの主権の行使は可能になる。例えば、日本は島国であり、その国際通信の 95%以上は海底ケーブルに依存している。そうすると、少なくとも海底ケーブルの陸揚局より内側は、日本の主権の及ぶ範囲として差し支えないだろう[8]。

サイバースペースをデータの所在を基準にして考えるととたんに難しくなる。クラウド・サービスのように、利用者の所在国とデータの所在国が異なってくるからである。しかし、外国人であろうと、外国人の所有する端末であろうと、日本国内にある主体や物体には日本の主権が及ぶとすれば、それほど難しくはない。外国人が日本国内で罪を犯せば、日本法に基づいて処罰されるのと同じである。

ただし、日米欧豪などの政府は、サイバースペースにおける自由な情報の流通を重要な価値と考えている。それこそが、1990 年代半ば以降、インターネットが多くの人に受け入れられてきた最大の価値であり、それを損なってはいけないと主張している。それゆえに、あえて国連だけで議論をすることを避け、多様なアクターの参加を求めるマルチステークホルダー・アプローチを堅持しようとしている。

サイバースペース会議の第 4 回は、2014 年中には開催されず、2015 年の早い時期にオランダのハーグで開かれることになった。ハーグは国際法学者たちの中心地であり、「法律の世界首都」とも呼ばれている。2014 年には国連の GGE が再開されるが、ハーグのサイバースペース会議までにいかなる結論を得られるのか、それとも結論は先送りされるのか。それが当面の課題となるだろう。

むすび

米国政府は、各種の文書でサイバースペースはグローバル・コモンズであると主張している。グローバル・コモンズとは、「一国がコントロールはできないが、すべての国が依拠する領域や区域」であるとされている[9]。しかし、自然空間である宇宙や南極大陸と違い、サイバースペースは、情報通信端末、通信回線、記憶装置等の単なる集積でしかなく、従来と同じ意味でグローバル・コモンズと考えるのは必ずしも適切ではない。機器等の集積であるとしたら、サイバースペースはきわめて脆弱であり、部分的な破壊や分裂といった恐れもある。サイバースペースをグローバル・コモンズとしてとらえることができるとし

ても、それはきわめて脆弱であると見るべきである。

しかし、そうだとすると、なぜそこまで各国がこだわるのかといえば、軍事も経済もサイバースペースに強く依存するようになっているからである。サイバースペースは第 5 の作戦領域だといわれることがあるが、むしろ、それは、陸・海・空・宇宙という 4 つの作戦領域をつなぎ、人類の活動を円滑にする存在である。

サイバースペースのガバナンスは、もともとうまくいっていたところに、政府が介入しようとしたために政治的な問題となっているという点で特異である。技術者たちは、「壊れていないなら直すな（If it ain't broke, don't fix it）」という言い方をよくする。インターネット・ガバナンスは壊れているのかどうか、そもそもそれは何なのかを定義するために 10 年以上にわたって議論が続けられている。しかし、セキュリティ問題が深刻化する現在、議論を収束させ、安定的かつ安全なガバナンスが求められている。

日米両国は、現在のサイバースペースが生み出している便益を維持し、増大させることに共通の価値を見いだしている。「現状維持」という戦略が魅力に乏しいことは確かである。しかし、中露が求めているような国家主導のサイバースペースの管理は、これまでのガバナンスをガバメントに変えることになり、サイバースペースが生み出してきたダイナミズムを失わせることになる可能性が高い。いま一度、情報統制のためではなく、グローバル市民の活動拡大のためのサイバースペースという意味でサイバースペースをグローバル・コモンズであると規定し、それが非常に脆弱なものであることを確認しながら、そのセキュリティを確保すべきである。物理的なインフラストラクチャの確保とともに、コンテンツとしての情報の流通の自由を求め、それらをつなぐルールの整備を図るべきである[10]。

－注－

1　クラークとのインタビュー（2008 年 7 月 21 日）に基づく。

2　土屋大洋『情報とグローバル・ガバナンス―インターネットから見た国家―』（慶應義塾大学出版会、2001 年）107-124 頁。

3　Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace," Geneva: ICT for Peace, 2012, accessed December 23, 2013. http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

4　"Joint Statement on Common Security Challenges at the Threshold of the Twenty-First Century," 1998, accessed December 23, 2013. http://www.gpo.gov/fdsys/pkg/WCPD-1998-09-07/pdf/WCPD-1998-09-07-Pg1696.pdf

5　以下のパネリストの発言の引用は筆者のメモに基づく。

6　Michael N. Schmitt, ed., Tallinn Manual on the International Law Applicable to Cyber Warfare, New York: Cambridge University Press, 2013.

7　Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, pp. 15-21.

8　土屋大洋「非伝統的安全保障としてのサイバーセキュリティの課題―サイバースペースにおける領域

侵犯の検討―」渡邉昭夫編『2010 年代の国際政治環境と日本の安全保障―パワー・シフト下における日本』（防衛省防衛研究所、2013 年）2013 年 12 月 23 日アクセス。
http://www.nids.go.jp/publication/kaigi/studyreport/j2013.html

9 U.S. Department of Defense, Quadrennial Defense Review Report, February 2010, pp. 8-9.
http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf

10 下層に物理層、中層にコード層、上層にコンテンツ層を設定するのはローレンス・レッシグ（Lawrence Lessig）の考え方に基づく。Lawrence Lessig, The Future of Ideas: The Fate of the Commons in a Connected World, New York: Random House, 2001.