平成25年度外務省外交・安全保障調査研究事業（調査研究事業）

グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題

平成26年3月

公益財団法人日本国際問題研究所
The Japan Institute of International Affairs

はしがき

本報告書は、当研究所の平成 25 年度外務省外交・安全保障調査研究事業（調査研究事業）「グローバル・コモンズ（サイバー空間、宇宙、北極海）における日米同盟の新しい課題」の成果として取りまとめたものです。

本プロジェクトは、サイバー空間、宇宙、北極海という世界各国に共通する課題（グローバル・コモンズ）の現状を分析し、これら「コモンズ」の安全を確保するための日米同盟・日米連携のあり方、また日本が産・官・学をあわせた総合的な強み（経済力、技術力、外交・国際的な影響力、自衛隊の能力等）を生かしながら果たすべき役割等を検討し、とるべき施策を提言しています。

安全保障空間は、技術革新や国際社会の構造変化により、大きな変容を遂げつつあります。サイバー空間は、今や経済活動と軍事オペレーションの双方にとって不可欠の領域である一方で、国家及び犯罪グループによる攻撃の脅威にさらされています。また、宇宙空間は、米ソ冷戦時代は 2 つの超大国が軍事利用を独占していましたが、近年では台頭著しい中国がこれにチャレンジする状況に至っています。さらに、近年における地球温暖化の進行は、従来「未到の海域」であった北極海を経済および軍事の両面にわたる現実の活動領域としつつあります。これらの空間は、世界の平和と繁栄のために必要不可欠な公共圏である「グローバル・コモンズ」としての重要性を増してきており、これら領域の安全を確保し、脅威を防ぎ、国際的なガバナンスを確立することがますます喫緊の課題となってきているという点で、共通する性格を有しています。

日米の同盟関係は過去 50 年以上の長きにわたって日本の安全、世界の平和と安定の確保に貢献してきましたが、上記のような戦略環境の変化に伴い、新たな課題に直面しています。「グローバル・コモンズ」の安全を確保し、世界の繁栄に貢献することは、日米共通の責務であると共に、世界において日本が積極的に役割を果たすべき課題でもあります。

なお、ここに表明されている見解はすべて参加された各研究者のものであり、当研究所の意見を代表するものではありません。しかし、個々の研究成果が今後の日本外交を巡る議論に資することを心より期待するものであります。

最後に、本研究に積極的に取り組まれ、報告書の作成に尽力いただいた執筆者各位、ならびにその過程でご協力いただいた関係各位に対し改めて深甚なる謝意を表します。

平成 26 年 3 月

公益財団法人　日本国際問題研究所

理事長　野上　義二

研究体制

主　査：	星野　俊也	大阪大学国際公共政策研究科科長・教授
委　員：	池島　大策	早稲田大学国際教養学部教授
	金田　秀昭	日本国際問題研究所客員研究員
	川口　貴久	東京海上日動コンサルティング株式会社主任研究員
	鈴木　一人	北海道大学大学院法学研究科教授
	土屋　大洋	慶應義塾大学大学院政策・メディア研究科教授
	福島　康仁	防衛研究所政策研究部グローバル安全保障研究室教官
委員兼幹事：	飯島　俊郎	日本国際問題研究所副所長
	秋山　信将	一橋大学大学院法学研究科教授
		日本国際問題研究所客員研究員
	松本　明日香	日本国際問題研究所研究員
担当助手：	松井　菜海	日本国際問題研究所研究助手

（敬称略、五十音順）

目　　次

第１章　総論：グローバル・コモンズにおける安全保障ガバナンスのあり方と日米同盟の課題
－サイバー空間、宇宙、北極海を中心として－

星野　俊也

はじめに

「グローバル・コモンズ（global commons)」と呼ばれる地球社会の公共領域がいま、主要国を中心とする多様な主体の権力と利益が錯綜する新たな国際安全保障のステージとしてかつてないほどに大きな注目を集めるようになっている。

「コモンズ（commons)」とは、本来、所有者を特定することができず、それがゆえに不特定多数の主体の自由なアクセスが可能な「共有地」を意味する。コモンズの原風景は、かつて米国の生態学者ギャレット・ハーディンが『サイエンス』誌に寄稿した論文「コモンズの悲劇」で紹介したように、農民だれもが自由に使える放牧地である[1]。そして、ハーディンは、農民たちが家畜の放牧を通じて自らの利得を最大化しようとする合理的な選択の結果、全体としてのコモンズの荒廃という悲劇が生じるというパラドックスを論じている。

21 世紀の世界でグローバル・コモンズを論じる我々にとって、ハーディンの議論は２つの意味で示唆的と言えるだろう。第一は、科学技術の長足の進歩により、いまやグローバルな観点でもコモンズと呼びうる領域（ドメイン）を活用できる時代となっており、その賢明な活用のためにもコモンズの特質をしっかりと理解することが求められているということ。そして第二には、グローバル・コモンズにおける悲劇をまさに回避するための方策を周到にデザインする必要があることである。ハーディンは、アクセスの自由原則そのものの見直しも選択肢に入れている。また、道義や節制といった態度も、あるいは人々が相互に強制することをも認め合う「社会的なアレンジメントとしての責任」の概念にも触れている。これらは、コモンズに関する「ガバナンス」のあり方の議論に通じる。

本研究は、今日の世界でグローバル・コモンズと認識されている地球社会の公共領域のなかでも特にサイバー空間、宇宙、北極海での動向を安全保障の観点から分析するとともに、これらの領域における公共秩序を提供するガバナンス体制のあり方を検討し、さらにその過程における日米同盟の役割について考察していくことを目的にしている。そこで、総論となる本章では、まず、グローバル・コモンズの概念整理を行うとともに、それが今日、国家の安全保障政策のなかで一定の注目を集めるようになった背景を分析する。続い

て、グローバルな公共領域のガバナンスに関わるメカニズムの理論的な枠組みを概観する。そして最後に、日米同盟の文脈において、グローバル・コモンズに関するガバナンスの構築プロセスにおいていかなる協力が求められ、また、可能であるのかを考えることとする。サイバー空間や宇宙、北極海という各ドメインにはそれぞれに特有の政治力学や課題が存在する。それらの詳細は本章に続く各章の議論に譲ることとする。

１．グローバル・コモンズの概念と特質

1−1　グローバル・コモンズにおけるリアル・ポリティーク

一般にグローバル・コモンズという場合、我々は、人類が共有する、あるいは共有すべきと考えられている空間や領域をイメージし、今日では、海洋や宇宙空間に加え、サイバー空間もその範疇で論じられるようになった。海洋においても公海や深海底にとどまらず、地球温暖化の影響で海氷面積が減少している北極海への関心が急速に高まっている。

科学技術の進歩により、人類の歴史は、人類の活動するフロンティアの拡大の歴史と言ってもよいだろう。グローバル化とは、そうした人類の活動が全地球を網羅するまでに広がったこと、さらには、宇宙空間から全地球を俯瞰できる視点までも我々が手に入れたことを意味している。それはまた、我々の活動が、日常の生活も含め、グローバル・コモンズと呼ばれる領域で相互に分かち難く、つながり合っていることもあらわしている。

もっとも、グローバル・コモンズを「人類共同の遺産（Common Heritage of Mankind：CHM）」とひとくくりにまとめることはできない。たしかに、月協定（1979 年）は月などの天体やその資源を、そして国連海洋法条約（1982 年）は深海底とその資源を、「国家管轄権の範囲を越えた地域」として、それぞれ人類共同の遺産と規定している。しかし、国際法は、基本的にはそれに署名した国家間での約束事に止まる。また、南極に関する条約や一連の勧告や措置（いわゆる「南極条約システム」）でも特徴的だが、一見、人類共同の遺産と考えられる地域でも、その実は領有権や鉱物資源をめぐる暗闘が展開している。

さらに言えば、グローバル・コモンズを、「コモンズ（共有地）」の延長としてイメージすることもまた誤解を招くことになりかねない。なぜなら、こうした領域は、特定の主権国家のコントロールが及んでいないものの、各国が権益を主張する動きには事欠かないからである。また、世界政府が存在しないという意味でアナーキカルな国際社会においては、そこを「共有地」であると容易に断言することも難しい。強いて言えば、グローバル・コモンズとは、多様な主体のアクセスが可能であるがゆえに、「互いの利害の相違の調整や共通の利益の促進のための合意形成が求められるグローバルな公共領域」と捉えるほうが適切である。

それが海洋であれ、宇宙空間であれ、サイバー空間であれ、グローバル・コモンズが多様な主体に開かれた公共領域であるということは、こうした領域がもはや国際関係において何ら特別な場所ではなく、むしろ我々の日常生活の一部に組み込まれていることを意味している。したがって、個々の主体がそれぞれの固有の権力と利益の極大化を目指して競争する「リアル・ポリティーク」は、グローバル・コモンズにおいても繰り広げられることになる。希少な価値の権威的な配分という政治のエッセンスが、グローバル・コモンズと呼ばれる領域でごく自然に見出されるようになった現実に、我々はいま向き合っているのである。

1－2　グローバル・コモンズにおける安全保障とは

今日の世界でグローバル・コモンズという表現が安全保障政策の見地からことさらに注目を集めるようになった一つの大きなきっかけとして、米国のオバマ政権が 2010 年 2 月に発表した『4 年ごとの国防戦略見直し（QDR）』文書がある。同政権は、この文書において、海洋と宇宙とサイバー空間を引き合いに、グローバル・コモンズのドメインでの多様な脅威に対して機動的かつ柔軟に対応し得る米軍の再構築の必要性を提起した[2]。この方針は同年 5 月に発表された『米国国家安全保障戦略（2010 年版）』文書においても引き継がれ、米国は「主要なグローバル課題における広範な協力を維持する」として、気候変動への対応、平和維持・紛争管理、感染症対策、国境を越える犯罪への対処とともに「グローバル・コモンズの保全」の重要性を強調している[3]。同文書で米国は自らが「北極圏の一国」であると明言し、安全保障上のニーズへの対応、環境の保護、資源の責任ある管理、先住コミュニティへの配慮、多岐にわたる問題に向けた国際協力の強化、といった利益を追求する姿勢も明らかにしている[4]。こうした動きは、単独行動が目立った前任のブッシュ共和党政権と異なるものであり、ここに国際協調を通じ、共通の課題に対する集団的な行動によって国際秩序を形成していくことに利益を見出すオバマ外交の特徴の一端を見出すことができるだろう。

同様の視点は、第二次安倍政権の下、新たに国家安全保障会議（日本版 NSC）を設置し、初めて『国家安全保障戦略』文書を打ち出した日本政府の動きにも見出すことができる。同文書では、日本が「国際協調主義に基づく積極的平和主義」の理念を踏まえ、海洋、宇宙空間及びサイバー空間といったグローバル・コモンズ（ここでは「国際公共財」という訳語が用いられている）におけるリスク要因を指摘し、これらの領域における法の支配の実現・強化、関心国との政策協議を通じた国際規範の形成や信頼醸成の促進、開発途上国の能力構築などに一層の努力をする、との姿勢を示している[5]。

ところで、前述のように、グローバル・コモンズだからといって、主体間のリアル・ポリティークという行動様式に何ら大きな違いがないのであれば、なぜ我々はことさらにグローバル・コモンズの安全保障に新たに注目をする必要があるのだろうか。それは、海洋、宇宙空間、サイバー空間というドメインの新規性によるものではなく、これらの広大なドメインの「グローバル性」に基づくリスクの深刻さが現実の世界で実感されるようになったためにほかならない。そうしたリスク要因は、開放性、連結性、非対称性という、いわばグローバル・コモンズを特徴づける３つの要素に直結する。そして、我々の日常生活がグローバル・コモンズの活用に依存すればするほど、その領域で発生するトラブルの深刻さに気付かされることになる。

第一に、グローバル・コモンズの開放性とは、原理的にコモンズ概念の最も基本的な定義である自由なアクセスの均等性に関わるものである。当該ドメインでは、明確な所有権を確立できる主体がおらず、その結果、原則として、誰もが自由にアクセスでき、誰も排除されない状況が成立している領域だからこそ、その資源や機会や便益が有効に活用できる公共性が主張される。このことは、もちろん、あらゆる主体に機会の平等を担保するものではない。海洋に比べ、宇宙空間への参入障壁はいまでも格段に高くなっている。他方で、サイバー空間にはほとんど誰もが参入しうる開放性がある。しかし、開放性が前提とされる領域においては、他の主体により自らのアクセスが妨害・拒否されることほど大きな損害はない。作為によらず、たとえ不作為の結果であったとしてもグローバル・コモンズの開放性への挑戦に対し、我々はまっさきに備えを固めていく必要がある。

第二のグローバル・コモンズの連結性とは、我々の社会生活がいまやこうした領域に連結された世界のなかで成立していること、あるいは、我々と他の主体との間を連結するインフラとしてグローバル・コモンズが介在していることを意味している。ここから、悪意を持った主体がグローバル・コモンズの各ドメインを通じて自らの安全保障の中枢に侵入してくるリスクや、安定的な連結が作為・不作為によって遮断されるリスクが予想される。

第三の非対称性のリスクもまたグローバル・コモンズ特有の力学を反映したものといえる。最も象徴的なのは、テロリストの個人や集団がサイバー空間を用いることで大国の重要インフラにさえも甚大な被害を与えうるような状況だが、海洋や宇宙空間においても、通常の経済関係や軍事関係であれば劣勢にある主体が、グローバル・コモンズの特性を乱用ないし悪用し、実力からいえば優勢な地位にある主体の利益を脅かすことが可能となっている。グローバル・コモンズの脅威に対する抑止が一般に限定的な効果しか期待できない理由も、こうした主体間の非対称的な関係に由来する。

1-3　グローバル・コモンズにおけるパワー・トランジション

もっとも、今日の米国や日本の例を挙げるまでもなく、グローバル・コモンズの使用頻度の高い大国の方が安全保障上の脅威をより切実に感じている現状にも目を向ける必要がある。言い換えるならば、グローバル・コモンズにおけるリスクの高まりは、海洋や宇宙空間、サイバー空間のどれをとっても、以前であればこれらの領域で支配的・独占的な地位を確立できていた大国において、より新興の国家や非国家の主体の参入により、その地位が侵食されるなかで発生していることが多い。かつて七つの海を支配できるのは大国の証であり、宇宙空間は米ソ両超大国に事実上独占されていた。そもそもサイバー空間を創造したのは米国である。こうした大国は、多大な投資を一方的に行ったことでそれぞれのドメインで圧倒的な地位を確立したわけだが、やがて、それらのドメインが超大国であったとしても独占状態を維持することができないほどに広大で、他の新規参入をさまたげられない公共領域に変質していくことになる。実際、グローバル・コモンズにおける問題は、後発の先進国や新興国、さらには非国家主体の実際の参入の過程で顕在化してきたものが多い。

グローバル・コモンズの安全保障とは、したがって、グローバルな公共領域におけるパワー・トランジションを反映したものと理解することができる。なかでも、新興国、特に中国の躍進と非国家主体の台頭が顕著である。グローバル・コモンズにおけるリアル・ポリティークが結局は「中国問題」であり、「非国家主体対応」になる理由がここにある。

こうした新興勢力の台頭は、米国からはそのパワー・プロジェクションを制約する要因として映る。事実、中国は海洋においても、空域においても、いわゆる「接近阻止・領域拒否（Anti-Access/Area Denial：A2/AD)」戦略を採用しているが、こうした発想はグローバル・コモンズにおける米国の優位の切り崩しにも応用できる。

また、米国はもとより世界全体を震撼させた 9・11 事件は、非国家のテロ組織が大国でさえも恐怖に陥れ、また、テロとの闘いに多大なコストを支払わせる方法論を最も衝撃的なかたちで見せつけた。そして、テロ組織が大量破壊兵器の獲得に触手を伸ばす脅威も広く認識されている。しかし、サイバー空間を活用し、「大量攪乱兵器」というべきサイバー攻撃を実行する動きはすでに現実の問題となっている。もちろん、こうしたサイバー攻撃は、公然と犯行声明を打ち出すテロ組織ばかりではなく、個人から法人、団体、さらに国家までもが、匿名性を隠れ蓑に、激しい攻防戦を繰り広げている。互いの情報通信端末がネットワークでつながり、いまや政治、経済、社会、文化に関わる活動のかなりの部分がこの仮想空間でのデータのトラフィックに依存している今日、従来と異なるパワー行使の現実が進んでいることになる。

グローバルな公共領域における新たな秩序、すなわちガバナンスの仕組みがいま求められているのは、こうした現実の課題により体系的・効果的に対応するためである。

２．グローバル・ガバナンスの概念と実践

2-1　グローバル・ガバナンスとは

国際社会の秩序形成の文脈でガバナンスを議論した研究としては、ジェームズ・ローズナウとエルンスト・オットー・ツェンピエルの『政府なき統治』論（1992 年）がその先駆けとして注目される[6]。彼らは、国際社会には中央に政府（government）が存在しないなかでも主体間の政治を通じて統治（governance）の機能をもつ制度が形成されている現象に着目した。こうした考えを背景に、中央政府のないアナーキカルな世界で、グローバルな広がりをもつ多様な課題が持ち上がるなか、これらの予防や対処のためにいかなる制度的な取り組みが可能かを追求する動きとしてグローバル・ガバナンス論が生まれてきた。

グローバル・ガバナンスの定義としては、山本吉宣が紹介するように、グローバル・ガバナンス委員会によるそれが最も包括的で実践的と言える[7]。同委員会は、「グローバル・ガバナンスは公私を問わず、個人そして機構が彼らの共通の事項を管理する多くの方法の全体である。それは、対立するあるいは多様な利益を調整し、あるいは協力的な行為がとられる継続的な過程である。それは、順守を強制することを付与されたフォーマルな機構やレジームを含むとともに、人々や機構が合意したか、彼らの共通の利益となると考えたインフォーマルな枠組みをも含むものである」と定義する。そして、山本は、国際法や国際レジームなど関連する概念との比較のなかで、グローバル・ガバナンスの基本的な要素として次の４つをすくい取っている[8]。

① 目的（共通の事項の管理、「共通の事項」という範囲には多くの問題領域が含まれよう）
② 主体（公私を問わない－国家、非国家主体の両方を含む）
③ 方法（多くの方法、フォーマル・インフォーマルなレジーム、機構を含む）
④ 行動規範（利益を調整し、協力的な行為に基づいたもの）

である。一般に国際法や国際機構が国家間のハードな取り組みであり、国際レジームがよりルースでインフォーマルな取り決めも含むとはいえ基本的に国家間の制度であるのに対し、グローバル・ガバナンスでイメージされる秩序が、主体の多様性と課題の包括性と制度の柔軟性に着目したものであることがわかるだろう。

では、こうしたガバナンスの概念をグローバル・コモンズの管理に応用することは可能なのだろうか。そして、可能であるとすればどのような努力が求められるのだろうか。

2-2　グローバル・コモンズにおけるガバナンス

グローバル・コモンズの悲劇を回避し、あるいはそうした悲劇に対処するためにも一定の秩序が必要であることは議論を俟たない。ハーディンが「社会的なアレンジメントとしての責任」に言及したことも、個々の主体の行動が社会全体の利害に直結するなかで「ガバナンス」の必要性を十分に認識していたからであり、十分に議論を掘り下げてはいないものの、その根底に主体の「責任」（道義や節制に裏付けられた責任）の体系を指摘している点はきわめて示唆的である。グローバル・コモンズにおける秩序形成の出発点であり終着点の一つは、やはり各主体が責任ある行動をとるように相互に自制し、牽制し、場合によっては強制をする制度的な基盤を整備することに行きつく。別の表現を用いるならば、グローバル・コモンズにおける共通の事項の管理－すなわち、グローバルな公共領域における主体間の利害の調整や共通利益の促進のための合意形成－に向けたグローバルな公共政策（global public policy）の立案・形成・実施が求められていることになる。

ところで、グローバル・ガバナンスが政策である限り、重要なポイントは、ガバナンスの有無ではなく、その効果である。そこで、いかに効果的に課題の予防や解決を実現できているかが問われることになる。その意味で、トーマス・ウィースらが複雑で多様なグローバルな課題に対応するためにガバナンスの仕組みが乗り越えるべき５つのギャップを論じている点は参考になる。それらは、知識、規範、政策、制度、順守のギャップである[9]。

グローバル・コモンズの安全保障の諸課題にひきつけてこれら５つのギャップを考えるならば、次のようになるだろう。まず、知識ギャップとは、グローバル・コモンズで発生する諸課題の性質・原因・深刻度等に関する知識の不在や違いであり、これらに関する共通の理解が得られるかどうかが第一の関門である。規範ギャップとは、ある特定の問題に対応する上で大多数が倫理的に適切と認識したり、互いの合意に基づき社会的に受け入れられたりした考えをどれだけ共有できているかに関するもので、これが第二のテストになるだろう。政策ギャップとは、課題に対する知識や課題解決のための規範を国際協定や国連決議などの文書でどれほど政策に落とし込むことができるかに関するものである。続く制度ギャップとは、ハード、ソフトなど制度化の度合いは異なるにしても、合意された知識・規範・政策が安定的・持続的な制度として主体の行動の管理に作用しているかを見る視点である。そして、最後の順守ギャップとは、合意された制度の履行・監視・強制により、主体の不順守をどれほど抑制することができるのかをチェックするものである。

サイバー空間や宇宙、海洋など、グローバル・コモンズを構成するドメインごとに異なる問題の性格や力学が働くことから、それぞれの領域でガバナンスの制度が整備されていくことも有益である。他方、グローバル・コモンズの開放性、連結性、非対称性といった

共通の特質の正の側面（＝公共善 public goods）を維持・拡大し、負の側面（＝公共悪 public bads）を除去していく努力は必要である。

どのドメインに関しても共通する根源的な原則を一つ打ち出すとすれば、グローバル・コモンズの「平和利用」があるだろう。多様な主体の利害が相互に錯綜し、主体の大小にかかわらずその活動が互いの利害に作用しあうグローバルな公共領域での活動である。自由なアクセスが担保されるかわりに「無害」行動の原則を明示していくことは、それが明文化されようが暗黙の理解に止まろうが、最も基本的な要件と言えるのではないだろうか。もちろん、そこはリアル・ポリティークの世界である。我々にとっては、公共善を伸ばそうとする政治的意図と、公共悪であってもその余地を技術的にも人為的にも排除できない現実のなかで「社会的なアレンジメントとしての責任」の体系を整備していくことが急務である。

３．おわりに－グローバル・コモンズの「平和」秩序と日米同盟の役割

過去 60 年を超す日米同盟の特徴は、冷戦型の共同防衛の仕組みで始まったものが時代とともにその性格を変え、冷戦が終結しグローバル化が進む時代にあっては、アジア太平洋地域の平和と安全や広くグローバルな秩序の形成・維持・発展という、きわめて「公共財」的な役割を持つ点である。もとより、日本がホスト国となることで可能となっている米軍の前方展開を不利益と考える国にとってみれば、日米同盟が公共財であるとの議論は容易には受け入れられないに違いない。しかし、日米ともに、国内の財政事情が厳しいなか、自らの防衛のみならず、地域の安定やグローバルな社会の平和に向けた経費をも織り込んで負担している点は、評価されてよい。

日米両国が連携し、物理的な軍事プレゼンスを維持することにより、地域の秩序の安定材料を提供している点が一つの大きな役割である。この関係では、特に中国のグローバル・コモンズへの進出を受けて、いかにこれを国際ルールの体系のなかに取り込んでいくかは、日米同盟協力の効果が最も直接的に試されることになるだろう。また、匿名性のヴェールの下でつばぜり合いが続くサイバー空間における安全保障利益の追求も具体的な取り組みが求められる分野である。

こうした物理的・直接的な同盟協力のみならず、グローバルな公共領域の秩序の形成・維持・発展に向けたルールづくりにおいて、日米両国が法の支配に基づき、他の国々や非国家の主体も巻き込み、リーダーシップをとっていくことも極めて重要だろう。その際のポイントは、サイバー空間や宇宙、北極海を含む海洋といったドメインごとの固有の課題に対応しつつ、グローバル・コモンズを包括的に理解し、その「平和利用」を促進すると

いう横断的な観点から、先に提示したグローバル・ガバナンスの５つのギャップ、すなわち、知識、規範、政策、制度、順守のそれぞれの分野での共通の認識の拡大に向けた提案を積極的にしていくことである。そうした交渉や協議のプロセスで、日米協力が技術革新を進め、技術的なエッジを広げていくことは外交上の大きなテコになるだろう。

日米同盟は、軍事同盟や政治同盟であるとともに価値の同盟でもある。両国が共有する普遍的な価値をベースにアジェンダを設定し、グローバル・コモンズにおける責任あるガバナンスの体系を主流化させていくことが期待される。

－注－

1 Garrett Hardin, “The Tragedy of the Commons,” *Science*, Vol.162, No.3859 (December 13, 1968), pp.1243-1248. http://www.sciencemag.org/content/162/3859/1243

2 U.S. Department of Defense, Quadrennial Defense Review Report, February 2010. http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf

3 The White House, National Security Strategy, May 2010, pp.49-50. なお、オバマ大統領は、新たな国家安全保障戦略文書を 2014 年初頭に発表することを予定しており、同文書でのグローバル・コモンズの取り扱いが注目される。http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

4 Ibid., p.50.

5 『国家安全保障戦略について』（平成 25 年 12 月 17 日国家安全保障会議決定・閣議決定）、7-8 頁及び 25 頁。なお、同文書では、グローバル・コモンズに「国際公共財」という和訳を充てている。http://www.kantei.go.jp/jp/kakugikettei/2013/__icsFiles/afieldfile/2013/12/17/20131217-1_1.pdf

6 James N. Rosenau and Ernst-Otto Czempiel, *Governance without Government: Order and Change in World Politics* (Cambridge: Cambridge University Press, 1992).

7 ブラント元西独首相が提唱し、1992 年に設立された国際委員会。2000 年の世界に向けた国連改革や国際制度の在り方を提言した。報告書は “Our Global Neighbourhood: The Report of the Commission on Global Governance” (Oxford: Oxford University Press, 1995)（日本語版は、京都フォーラム監訳『地球リーダーシップ－新しい世界秩序をめざして-グローバル・ガバナンス委員会報告書』日本放送出版協会、1995 年）として発表された。

8 山本吉宣『国際レジームとガバナンス』有斐閣、2008 年、169 頁。

9 Thomas W. Weiss, “The UN’s Role in Global Governance,” *UN Intellectual History Project Briefing Note*, Number 15 (August 2009), pp.2-5.

第２章　サイバー空間における安全保障の現状と課題
－サイバー空間の抑止力と日米同盟－

川口　貴久*

はじめに

サイバー空間へのアクセスとその安定的利用は各国の安全保障や社会・経済的な繁栄に不可欠である。同時に、サイバー空間は国家の排他的管轄権の外にあるため、「グローバル・コモンズ」としての性格を有している[1]。それゆえ、サイバー空間では諸国家や民間組織による自律的な秩序が求められている。

抑止力（deterrence）は自律的な秩序形成・維持に貢献する。抑止とは、相手にネガティブなメッセージを送ることで「相手が本来したであろう行為を思いとどまらせる」ことであり、その一般的モデルは武力による報復を示唆しながら相手方行為を思いとどまらせる「懲罰的抑止」である。冷戦期、核および通常戦力によって構成される抑止メカニズムが米ソ対立構造に一定の安定性を与え、ある歴史家はこれを「長い平和」とさえ呼んだ。

しかし、従来の国際安全保障の中心であった抑止メカニズムはサイバー空間で大きな問題に直面している。同時に、直面する課題を超えて、サイバー空間で抑止力を整備する動きもある。

そこで本章では、近年のアメリカのサイバー防衛・安全保障政策を中心に、サイバー空間での抑止力の限界性と可能性を検討する。特に議論の焦点となっているのは、攻撃元を特定し、報復や懲罰を示唆する抑止メカニズム（懲罰的抑止）が機能するか否かである。

結論からいえば、従来、アメリカの防衛・安全保障コミュニティでは、いくつかの理由によって懲罰的抑止力の構築は難しいと考えられてきた。しかし、現在ではサイバー攻撃の発信源を特定し、報復を示唆するような抑止力が整備されつつある。こうしたサイバー空間の防衛・安全保障政策の変化、つまり懲罰的抑止力の追求を前提に、日米同盟も適応していく必要がある。

まず、サイバー空間の抑止論の現状を俯瞰し（第 1 節）、サイバー空間で伝統的な抑止が機能しにくい理由を論じたい（第 2 節）。そうした限界性を踏まえて、アメリカの防衛・安全保障コミュニティで抑止論がどのように変化したかを論じ（第 3 節）、最後に日米同盟の課題について触れたい（第 4 節）。

* 東京海上日動リスクコンサルティング株式会社 主任研究員、慶應義塾大学ＳＦＣ研究所 上席所員（訪問）。本稿の内容は、筆者の個人的見解であり、所属する組織や機関の意見を代弁するものではない。

１．サイバー空間における安全保障

1-1．サイバー空間の抑止論

安全保障政策におけるサイバーセキュリティの優先度が高まっている。アメリカはサイバー空間を陸、海、空、宇宙に続く「第 5 の戦場」ととらえ、『米国家安全保障戦略』(2010 年 5 月）では「デジタル・インフラストラクチャーは戦略的な国家資産であり、この防衛は…中略…国家安全保障上の優先事項[2]」と位置づけた。また、ホワイトハウスや国防総省が中心となって、サイバーセキュリティに関する戦略・方針をたて続けに発信している（表 1)。

2010 年 10 月には、米軍のネットワークを防護するためサイバー軍司令部（Cyber Command: CYBERCOM）の運用が開始された[3]。今後数年で、CYBERCOM は要員を 5 倍に増やし、重要インフラの防衛、国防総省ネットワーク防護、海外での戦闘任務支援の部隊を整備する予定である[4]。連邦予算の「強制削減（sequestration)」下であっても、サイバーセキュリティ分野への投資は増えている。

表 1　サイバー安全保障にかかわる主な政策文書・スピーチなど（アメリカ）

年月	タイトル
2008 年 1 月	ホワイトハウス「包括的国家サイバーセキュリティ・イニシアティブ (Comprehensive National Cybersecurity Initiative)」　※公表は 2010 年 3 月
2009 年 3 月	ホワイトハウス「サイバー空間政策レビュー（Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure)
2010 年 1 月	クリントン国務長官「インターネットの自由」演説
2010 年 10 月	CYBERCOM 本格運用開始
2010 年 2 月	国防総省「4 年毎の国防報告 2010（Quadrennial Defense Review Report: QDR)」議会報告
2010 年 5 月	ホワイトハウス「アメリカ国家安全保障戦略（National Security Strategy)」
2011 年 5 月	ホワイトハウス「サイバー空間における国際戦略（International Strategy for Cyberspace)」
2011 年 7 月	国防総省「サイバー空間における作戦行動についての国防総省戦略」(Department of Defense Strategy for Operating in Cyberspace)
2011 年 11 月	国防総省「国防総省サイバー空間政策報告 (Department of Defense Cyberspace Policy Report)」
2012 年 10 月	パネッタ国防長官「国家安全保障についてのビジネス経営者向けサイバーセキュリティ」演説

一方で、サイバー安全保障政策の中での抑止の位置づけは不明瞭であり、模索が続いている。ブッシュ政権下で作成（2008 年 1 月）され、オバマ政権誕生後に公表（2010 年 3 月）された「包括的国家サイバー安全保障イニシアティブ（Comprehensive National Cybersecurity Initiative: CNCI)」は、その具体的取り組みの 1 つとして「揺るぎない抑止戦略およびプログラムの構築・発展」を掲げたが、体系的な政策を明示するに至ってはいな

い[5]。

そして、サイバー空間の抑止についての政策・研究[6]の多くは、冷戦期の懲罰的抑止モデルはサイバー空間で機能しない、という見方を示している。国防総省・米軍でのサイバーセキュリティ対策の推進者であり、オバマ政権で国防副長官を務めたリン（William J. Lynn, Ⅲ）ははっきりという。

> 一度のクリックは 0.3 秒で地球を 2 周する。その一方で、攻撃元を特定するのに必要な捜査は数カ月を要する。ほぼリアルタイムでサイバー攻撃者を特定しなければ、我々の抑止プログラムは破綻する。ミサイルは「返信先」を明らかにしてやってくるが、サイバー攻撃の多くはそうではない。こういった理由で、抑止についての既存モデルは、サイバー空間では全く当てはまらない[7]。

ブッシュ・オバマの両政権でサイバーセキュリティ政策に携わったクラーク（Richard A. Clarke）曰く、「戦略的核戦争防止の必須条件である抑止理論は、現段階では、サイバー戦争を阻止する上では何ら重要な役割を果たさない[8]」。抑止研究の第一人者であるモーガン（Patrick M.Morgan）も「その（冷戦期の）抑止の最も顕著な特徴の多くは、今日ではほとんど使いものにならない。現在のサイバー攻撃の問題は規模と特徴の面で全く異なっている。冷戦期の抑止から最も適用されうるいくつかの教訓は本質的にネガティブなものである。つまり、適用しない理由や避けるべき根拠といったものだ[9]」という。

しかし、こうした見方は変化しつつある。端的にいえば、2013 年 12 月現在、アメリカの安全保障政策はサイバー空間において攻撃元を特定し、報復や懲罰を示唆する抑止メカニズム（懲罰的抑止力）を模索し、一定程度の能力を有している。この変化は、2011 年 11 月に議会に提出された「国防総省サイバー空間政策報告（Department of Defense Cyberspace Policy Report）」に反映されている。詳細は後述するが、その前に抑止のメカニズムに触れたい。

1-2. 抑止のメカニズム

抑止の概念は第二次世界大戦以前にも存在したが、その理論化・精緻化は核戦略の発展と密接に関連していた。というのは、核兵器の誕生により、防衛・安全保障政策の目的（あるいは軍組織の役割）は「戦争に勝つ」ことから「戦争を起こさない」ことに変化したからである。こうした事情もあり、抑止といえば、冷戦に象徴される報復を示唆しながら相手方行為を思いとどまらせる「懲罰的抑止」が想像されるだろう。しかし、核兵器であれ

サイバー兵器であれ、「抑止は複雑で、単なる報復（retaliation）より多くのものを伴う[10]」。安全保障政策で想定される抑止はより広い概念である。

抑止とは、相手にネガティブなメッセージを送ることで、「相手が本来したであろう行為を思いとどまらせる」ことである。このように抑止を定義するならば、その形態は様々である[11]。特に注意すべきは抑止のメカニズムである。2 つのアクター間で抑止が成立するのは、攻撃失敗のコストの期待値が攻撃成功の利益の期待値を上回る場合である[12]。このような抑止メカニズムを成立させるためには、2 つの方法がある。1 つは相手の利益を否定する拒否的抑止（deterrence by denial）であり、もう 1 つは相手にコストを課す懲罰的抑止（deterrence by punishment）である。そして、サイバー空間の抑止論で議論の焦点となっているのは後者である。

２．サイバー空間における抑止力の限界性:「帰属問題」と「攻撃優位」

しかし、サイバー空間では従来的な抑止メカニズムは機能しないと考えられてきた[13]。いくつか理由はあるが、ここでは①サイバー攻撃の発信元の特定が困難である点、②インターネット空間では防御に対して攻撃が有利な点に焦点を絞りたい[14]。すなわち、サイバー空間の現状は、防御に対して攻撃が優勢であり、その攻撃の発信源の特定は難しい。こうした状況では懲罰による抑止メカニズムは機能しない。

2-1.「帰属問題（attribution problem)」

サイバー空間では攻撃の発信源を即座に断定することができない、少なくとも困難である。サイバーセキュリティの専門家はこれを「帰属問題（attribution problem)」と呼ぶ[15]。“attribution”とは「行為の原因・因果関係を特定すること」と定義されうるが、サイバー空間では攻撃が行われた物理的場所、使用されたコンピュータ端末、サーバの所有者、実際の攻撃者が国境を超えるため、帰属が複雑化する。

帰属問題の所在はインターネットの構造、アプリケーションやプログラムの設計、攻撃者の社会的属性（特に国家との関係）と多岐にわたる。ここでは帰属問題の階層性をある程度、単純化して、①技術的な帰属問題、②社会・政治的な帰属問題について検討してみたい。

技術的な帰属問題は、インターネットの構造と密接に関連している。インターネットとは、相互接続されたコンピュータ間で、情報を小分けにし、これらを任意の宛先に届ける世界大のネットワークである。そこでは、データを正確に届ける仕組み（通信プロトコル）が必要となる。データの送受信を保障する標準的規格が TCP/IP（Transmission Control

Protocol/Internet Protocol）であり、端末ごとにふられた固有の識別番号が IP アドレス（Internet Protocol Address）である。

だが、サイバー攻撃では発信元の IP アドレスが偽装されるケースが多い。この問題は、2013 年初頭の米セキュリティ会社マンディアント（Mandiant）による報告書と中国の対応でも顕在化した。同社の報告書によれば、中国政府および人民解放軍はアメリカの公的機関・民間企業に対して恒常的なエクスプロイテーション（exploitation）を行っている[16]。しかし、中国国防部はこうした攻撃に彼らが関与していないとした上で、「インターネットの世界では周知のことであるが、IP アドレスを根拠にサイバー攻撃の発信源を特定することはできない。IP アドレスの偽造は毎日のように起こっている[17]」と述べている。

さらに、ここ 10 年で顕在化したボットネットと呼ばれる攻撃手法も帰属問題を複雑にする。ボットネットとは、ウイルス感染等により“乗っ取られた”コンピュータの集合体を指す。ボットネットは、攻撃者からの指示をいくつかの中継サーバを経由して受信し、対象に攻撃を仕掛ける。ボットネットの規模は数万の IP アドレスに及ぶ。2009 年 5 月に発覚したボットネット「mariposa」（スペイン語で「蝶」の意味）は全世界で 1200 万以上の IP アドレスが感染する史上最大規模のボットネットであった。サイバー攻撃の帰属は、ボットネットの興隆により以前にも増して複雑化した。

このように、攻撃元の偽装やボットネットにより、技術的な階層で帰属が複雑化している。しかし、技術的なレベルよりも政治・社会的なレベルの帰属問題の方が深刻である。「インターネットの父」の 1 人とされるマサチューセッツ工科大のクラーク（David D. Clark）は断言する。「帰属問題とは全くもって技術的なものではない…中略…その解決は、技術的領域の外にある[18]。」　つまり、帰属問題は端末の前でクリックする人間の社会・政治的属性を特定しなければならず、それは政策的な解決を要する。

そして、サイバー攻撃の行為者と責任ある主権国家の関係を立証できなければ、抑止は機能しない。仮に攻撃者（個人や端末）を特定したとしても、攻撃者と責任ある国家・組織の関係を断定することは難しい。時間をかけて外国からのサイバー攻撃を特定したとしても、その外国政府との関連は明らかにされない。例えば、ロシアからエストニアへのサイバー攻撃（2007 年）、グルジアへのサイバー攻撃（2008 年）の背景には愛国的な青年組織が存在したと報道される。しかし、彼らのような「サイバー民兵」「クレムリン・キッズ」によるサイバー攻撃とロシア政府の関係を証明することは難しい[19]。

しかし、こうした見方は社会的帰属問題を過大視しているといえる。大西洋評議会（Atlantic Council）のヒーリー（Jason Healey）によれば、サイバー抑止はサイバー攻撃の実行者を特定する必要はない。彼は、1999 年の駐中米大使館への投石事件（NATO による

駐ユーゴ中国大使館への誤爆が原因）から教訓を導き出す。それは大使館の安全確保には実際の投石者を特定する必要はなく、投石事件の責任（この場合、投石を看過した所管警察と中国政府）を追及すれば事足りるということである。つまり、「誰がやったか」ではなく「誰が責任をもつのか」が重要である[20]。

実際、こうしたモデルに近いのは、民間の ISP（Internet Service Provider）事業者や CSIRT（Computer Security Incident Response Team）[21]による国際的連携・調整メカニズムであろう。インシデント発生時、さらなる被害を食い止めるために CSIRT 間で連携し、特定の IP アドレスをインターネットから切り離すなどの処置を行う。この過程は「誰がやったか（attribution）」ではなく、「誰が対処すべきか（responsibility）」という点で連携が行われ、これは一般的に機能しているといわれる[22]。もちろん過大な期待はすべきではない。CSIRT はあくまでも調整機関であり、法的強制力や執行機能はないし、昨今の国家主導（state-sponsored）の攻撃に対処できるかは分からない。

いずれにせよ、帰属問題が抑止メカニズムに与える影響は大きい。攻撃元を即時に断定できないため、報復による懲罰的抑止が冷戦期ほど機能しない。

2-2.「攻撃優位」のアーキテクチャ

もう 1 つの大きな問題は、サイバー空間は「攻撃優位」のアーキテクチャが形成されている点である。この「攻撃優位」の問題は、「帰属問題」と密接に関連している。

サイバー空間、特にインターネット空間[23]は情報を容易かつ自由に伝達・拡散することを目的として設計された。こうしたインターネットの「自由」「効率性」といった設計思想は必ずしもリスクマネジメントや安全保障を最優先事項とはせず、結果、攻撃者が有利なアーキテクチャが形成された。オバマ政権発足後、ハサウェイ（Melissa Hathaway）が中心となり、それまでのサイバーセキュリティ政策の見直しを行った。その成果文書は『60 日レビュー』と呼ばれ、現状に警鐘を鳴らした。

> デジタル・インフラストラクチャーのアーキテクチャは、**セキュリティよりも相互運用性や効率性を考慮して、設計された**。その結果、国家および非国家アクターが情報を危険にさらし、盗み、改竄し、破壊している。そして、アメリカのシステムに重大な破壊を引き起こしうるものになっている[24]。（強調筆者）

利便性とセキュリティはトレードオフであり、インターネット空間は利便性を求めた設計である。インターネット空間を行きかう情報（パケット）は善悪の価値判断が下されな

いどころか、識別番号さえない。ヴィントン・サーフ（Vinton G. Cerf）とともに、TCP/IP プロトコルを開発し、「インターネットの父」として知られるロバート・カーン（Robert E. Kahn）もインターネットの脆弱性の 1 つとして、「優先取極めのないコミュニケーションの自由」を挙げる。現状では、あらゆるコミュニケーションは基本的には同じ重要性として扱われる。したがって、許容できるコミュニケーションと不明・望ましくないコミュニケーションを区別することは難しい[25]。

「自律・分散・協調」を基本原理とするインターネット空間[26]では、結果的に、攻撃者による優位性が形成されてきた。端的にいって、サイバー空間の競合は「攻撃優位をめぐる競合であり、攻撃者と防衛者に等しく資源が与えられれば、攻撃側が勝つ[27]」のである。実際には、攻撃側は少ないコストや資源で防衛側に打ち勝つことができる。攻撃側は無数のプログラムから 1 つまたは複数の脆弱性を探し出せば目的を達成するが、防衛側は全ての脆弱性を網羅・検証し、アップデートし続けなければいけない。そのコスト差はあまりに大きい。例えば、1000 万行のセキュリティプログラムに対して、わずか 125 行の強力なマルウェアが作成されることもある[28]。

そして攻撃側が有利な環境では、「先制」は魅力的なオプションであり、現状変更を試みる者による侵攻のリスクが高まる[29]。このような世界では、既存の防衛・安全保障政策は変化を迫られる。日本でいえば、「専守防衛」に基づく政策体系は通用しないかもしれない。リン前国防副長官の言葉を借りれば、「要塞主義のメンタリティ（a fortress mentality）は通用しない」し、「ファイヤーウォールというマジノ戦線の後ろへ下がることはできない」のである[30]。攻撃優位の世界における抑止はきわめて困難な課題として浮上する。

３．サイバー空間における抑止力の模索

サイバー空間は攻撃者優位であり、攻撃元を特定することが難しい。それゆえ、アメリカの防衛・安全保障コミュニティでは、冷戦期のような懲罰的な抑止力は機能しないと考えられてきた。しかし、現在では、サイバー空間において懲罰的抑止力を追求する安全保障政策が形成されつつある。

3-1．リンの抑止論と「積極的防衛」

冷戦期に確立された懲罰的な抑止政策は、サイバー空間に適応できない。これが、2010 年末頃までのサイバー抑止に関する米国防総省の見解であった。CYBERCOM 司令官・アレクサンダー大将（Keith B. Alexander）は、2010 年 9 月の上院公聴会でサイバー抑止の困難さについて率直に述べている。「サイバー分野の抑止はその他分野とは異なるものである。

冷戦期のような機能は担えない。…中略…我々は幅広い観点で抑止を刷新する研究をしなければならない[31]。」

冷戦期の懲罰的抑止に代わって強調されたのが、拒否的抑止力である。つまり、サイバー空間では報復によりサイバー攻撃者にコストを課す「懲罰的抑止力」は難しいが、サイバー攻撃者の利益を否定する「拒否的抑止力」は実現可能である。こうした考え方は、リン国防副長官が『フォーリンアフェアーズ』誌に寄せた論説「新しいドメインの防衛」に反映されている[32]（もともとアメリカは懲罰的抑止政策を明示的に展開しようとしたが[33]、「サイバー空間における作戦行動についての国防総省戦略」等の政策文書では報復や攻撃的オプションは明示されなかった）。

サイバー空間の拒否的抑止力は、政策文書の中では「積極的防衛（active defense）」と表現される[34]。これは、CYBERCOM が掲げる重点分野の 1 つである[35]。「サイバー空間における作戦行動についての国防総省戦略」によれば、国防総省は「同省のネットワークとシステムへの侵入を予防し、侵入した敵対行為を打破する積極的なサイバー防衛（active cyber defense）を展開する」とした上で、積極的なサイバー防衛を「脅威と脆弱性を発見し、検知し、分析し、被害を低減するためのシンクロナイズドされた、リアルタイムの能力」と定義する[36]。つまり、積極的防衛とはサイバー攻撃を事前に検知し、リアルタイムに分析・検出し、ネットワークを防衛すること、およびそのための一連の投資と更新である。

積極的防衛の考え方は、防衛大綱に示される「動的抑止力」（2010 年）や「統合機動防衛力」（2013 年）に近い。核兵器はその強力さ故に、存在するだけで抑止力を有している（実存的抑止）とされた。しかし、サイバー空間の抑止力は「存在」することではなく、常に「運用」されることに意味がある。早期警戒やセキュリティシステムの更新といった運用がサイバー抑止の核心である。

しかし、そもそも拒否的抑止力のメカニズムには本来的に制約がある。というのは、どれほどサイバー攻撃の利益や成功確率を極小化しようとも（仮にそれらが限りなくゼロに近くとも）、サイバー攻撃によるコストがゼロであれば、攻撃のインセンティブが常に存在する。それゆえ、アメリカのサイバー抑止政策が拒否的抑止力だけでなく、懲罰的抑止力を追求することとなる。

3-2. パネッタ演説と懲罰的抑止力

こうした事情もあって、攻撃元の特定能力を備えた懲罰的抑止力が模索されてきた。統合参謀本部副議長［当時］のカートライト海兵隊大将（James E. Cartwright）をはじめ、かねてより米国は懲罰的抑止と攻撃オプションの必要性を訴えてきた。彼によれば、「21 世

紀の抑止は、それが核兵器であれ、生物兵器であれ、サイバーであれ、広義では匿名性（anonymity）と帰属（attribution）に関するもの」である。そして、効果的な抑止力は防衛的なオプションだけでは不十分であり、攻撃的なオプションが必要である[37]。

こうした見方が支配的となっていく。国防総省が議会に提出した「サイバースペース政策報告」（2011 年 11 月）では、サイバー空間における 2 つの抑止メカニズムを強調した。つまり、「サイバー空間での抑止は、他のドメインと同様に 2 つの基本的メカニズムに立脚する。つまり、敵の目的を否定することであり、必要であれば侵攻する敵対者にコストを課すことである[38]。」従来、焦眉の課題であった「帰属問題」についても、一定の方向性がみえているようである。2012 年 10 月のパネッタ国防長官（Leon E. Panetta）のスピーチはサイバー抑止を考える上で、大きな転換点となった。

> 国防総省のネットワークを防衛するために、我々は攻撃者への抑止を支援する。我々がサイバー攻撃者をたどることができる、あるいはサイバー攻撃は強固な防衛能力によって失敗する、と攻撃者が認識していれば、彼らが我々を攻撃する可能性は低くなる。
> 国防総省はサイバー攻撃の抑止を複雑にしている問題、つまり攻撃元を特定するという問題を解決する点で非常に進展を続けている。
> この 2 年間で国防総省は特定問題を解決するためのフォレンジック（forensics）に大きな投資をしてきた。そして我々は投資にみあう成果をつかみつつある[39]。

パネッタがいう「進展」の具体的内容については不明だが、国防総省「サイバースペース政策報告」で取り組みの方向性や一端が垣間見える。具体的には、攻撃の物理的な発信源を追跡する手法、ふるまいを基にしたアルゴリズム（behavior-based algorithms）による攻撃者評価、サイバーフォレンジック（cyber forensics、サイバー攻撃が行われた場合にコンピュータやネットワークなどのログを通じた証拠保全と攻撃元調査）、インテリジェンス・コミュニティと CYBERCOM を中心とする専門家育成、国土安全保障省との連携などである[40]。また、省庁間や国家間で新しいマルウェアのインディケーターを交換することも効果的であろう。

サイバー空間では攻撃元を特定することが難しい。しかし、こうした問題を超えて、懲罰的抑止力が形成されつつある。重要な点は、積極的防衛（拒否的抑止力）と懲罰的抑止力は相当程度、重なる部分が多いということである。冷戦期は攻撃用と防御用の核兵器・ミサイルが区別できたかもしれないが、サイバー空間では拒否的抑止力・懲罰的抑止力、攻撃・防御を明確に分けることはできない。サイバー「兵器」は 1 つのシステムの中で、

複数の要素を兼ね備えたものである。それゆえ、サイバー空間での「抑止は攻撃的であり、防衛的であり、インテリジェンス・オペレーションであり、これらを融合させたもの[41]」が求められる。

3-3. ドメイン横断型の抑止とエスカレーション・コントロール

サイバー空間の抑止力はサイバー空間だけに限定されず、攻撃に対する報復や懲罰行為は「ドメイン横断（cross-domain)」的である[42]。実際、アメリカはサイバー攻撃に対して、陸・海・空・宇宙で動力学的（kinetic）な方法による報復を示唆している。「国防総省サイバー空間政策報告」では、次のような見解が示されている。

> サイバー空間の悪意ある行為から、合衆国、同盟国、パートナー、国益を守るために、合衆国大統領は必要なあらゆる手段（all necessary means）を用いて対応する権利をもつ…中略…大統領の指示に基づき、対応オプションは国防総省によって提供されるサイバー能力および物理的能力（kinetic capabilities）のいずれか、あるいは双方を含む[43]。

こうした物理的能力には核戦力を含むという見方もある。国防総省の諮問機関である国防科学委員会（Defense Science Board）は最近の報告書の中で、「効果的な国防総省のサイバー戦略には抑止の要素が不可欠である」とした上で、サイバー攻撃への抑止として核戦力を維持すべし、と勧告している[44]。それは核兵器システムが最もサイバー攻撃に強く、抗堪性が高い（resilient）という評価に起因すると推察される。

しかし、物理的な軍事行動を示唆することで、危機がエスカレートするリスクが常に存在する。これを防ぐためにはエスカレーション・コントロール、「対象」と「手段」を考慮した段階的オプションが求められる。検討する際の視点としては、攻撃対象が軍事関連施設か民生用の社会インフラを含むか[45]、サイバー第一攻撃および報復攻撃がどの程度可視化されているかという点が挙げられる[46]。

４．サイバーセキュリティと日米同盟

サイバー空間の安全保障政策は変化の渦中にある。それは、サイバー脅威の顕在化というだけでなく、対抗する安全保障メカニズムの観点でも変化している。こうしたサイバー空間の防衛・安全保障政策の変化、つまり懲罰的抑止力の追求を前提に、日米同盟も変化する必要がある。

2013 年 10 月に開催された日米の外務相・防衛相による「２＋２」（Security Consultative

Committee: SCC）で、1997 年に改定された日米防衛ガイドラインを 2014 年末までに見直すことに合意した。サイバー空間での協力も新たな課題として認識され、作業部会を設置する。サイバー空間に関する日米協力の具体化が進む中、ここでは日米同盟によるサイバー抑止力強化にあたっての課題を検討したい。

4-1．政策：中国発のサイバー攻撃を“フルスペクトラム”で評価する

日米同盟におけるサイバー抑止を検討する場合、日米同盟の“本丸”の議論から外れるわけにはいかない。それは、「力による現状変更」を試みているとみられる中国との関係である。加えて、平時から有事、そしてそれらの「中間領域」「グレーゾーン」のリスク管理について検討する必要がある。つまり、中国発のサイバー攻撃をフルスペクトラムで評価し、抑止力の適応範囲を示す必要がある。

2013 年 6 月のアジア安全保障会議で、ヘーゲル（Chuck Hagel）米国防長官は、「アメリカを狙ったサイバー攻撃に中国政府および人民解放軍が関与し、その攻撃対象は米政府機関や軍だけでなく、米産業や民間企業にも及んでいる」と指摘し、続く米中首脳会談でもオバマ（Barack H.Obama）大統領が習近平（Xi Jinping）国家主席に同様の懸念を伝えた。

だが重要なことは、こうした中国発のサイバー攻撃は平時のエクスプロイテーションとしてだけでなく、有事におけるアクセス拒否・接近阻止（Anti-Access, Anti-Denial: A2AD）戦略の要としても位置づけられている。マンディアント社の最高セキュリティ責任者のベトリッチ（Richard Bejtlich）が指摘しているように、エクスプロイテーションと破壊的・攻撃的活動はシステムの脆弱性を探しだすという点で共通していて、両者は表裏一体である[47]。米中経済安全保障検討委員会に提出された中国のサイバー戦能力に関する報告書（2009 年、2012 年）は、東アジアでの紛争時、中国は平時のエクスプロイテーション活動で得られた脆弱性を活用し、アメリカにサイバー攻撃を行うことはほぼ間違いないと結論づける。攻撃は米軍の指揮統制・兵站ネットワークに対するオペレーショナルな妨害活動であると同時に、アメリカ政府の（介入するか否かの）意思決定を遅延・複雑化する狙いがある[48]。

サイバー空間の拡大抑止は、平時から有事および中間領域における中国発のサイバー攻撃のリスクを評価し、抑止力による対処の範囲を設定することが必要である。

4-2．法的基盤：“どの時点で”武力攻撃を認めるのか

次に法的基盤の整備である。サイバー空間の懲罰的抑止力の法的基盤を整備する上で、集団的自衛権に関する議論を決着させる必要がある。実際、第 2 次安倍政権下で設置され

た「安全保障の法的基盤の再構築に関する懇談会」で、集団的自衛権の見直しが進んでいる。2013 年 8 月、「懇談会」座長代理の北岡伸一は集団的自衛権の見直しを従来の「四類型」にとらわれず、シーレーンや宇宙、サイバー空間への攻撃対処を含む全面解禁とする方向性を示した。

もちろん個別自衛権の議論も進んでいる。2012 年 4 月 26 日、情報セキュリティ政策会議において、外務省は既存の国際法体系がサイバー空間に適応可能とした上で、サイバー攻撃が外国からの「武力攻撃」とみなせるのであれば、「サイバー攻撃に自衛権行使可能」という見解を表明した。2013 年 10 月 23 日の参議院予算委員会では、安倍首相もサイバー攻撃に自衛権行使可能との旨を述べた。

個別であれ、集団的であれ、サイバー空間における自衛権行使の要件は「通常の武力攻撃と同程度の損害を与えるか否か」という点に収斂するだろう。しかし、これは不十分である。2010 年のイランの遠心分離機制御システムへの攻撃（Stuxnet）であれ、2012 年のサウジアラビアの国営石油会社のデータ消去（Shamoon）であれ、結果的にあるサイバー攻撃が「武力攻撃」相当かどうかは判断・認定できるだろう。しかし、どの時点で「武力攻撃」相当と認定するかは難しい問題である。サイバー空間での対応はスピードが求められる。『ワシントンポスト』紙の国家安全保障問題担当記者のナカシマ（Ellen Nakashima）がいうように、結局のところ、「どのようなサイバー攻撃が戦争行為なのか」を決めるのは政治的判断であり、それは軍事的決定や法的決定以上に重要である[49]。そうした権限を予め決めておく必要がある。

4-3. 運用：2 つの“世界と言語”が理解できる人材を確保する

最後は日米同盟のサイバー抑止力を維持するための運用、そのための人材確保である。

東日本大震災における日米協力は有事の協力モデルとなった。震災直後、市ヶ谷、横田、仙台に日米調整所を設置し、米軍および自衛隊のコミュニケーションと運用調整を行った。2011 年 6 月の「２＋２」では、こうした経験を「将来のあらゆる事態への対応のモデル」と評価した。2014 年のガイドライン再改定では、日米の調整・協力メカニズムがより具体化されるだろう。

サイバーセキュリティ分野の協力がどういったスキームで構築されるかは定かではないが、いずれにせよ、日米同盟のサイバーセキュリティ強化には「スーツ」と「ギーク」、2 つの世界と言語を理解する人材が必要とされている[50]。「スーツ」、つまり防衛・安全保障政策の形成者たちには独特の価値体系や専門性がある。一方で「ギーク」、つまりサイバーセキュリティの世界や言語も同様である。

両者の価値体系（世界）と専門性（言語）を理解しなければ、サイバー攻撃対処の日米連携は困難であろう。教育や研修プログラムを通じて、「2 つの世界」を同時に理解する人材を輩出するのは難しい。現実的には、「スーツ」あるいは「ギーク」がもう一方の分野に歩み寄るしかないだろう。

またサイバーセキュリティの専門家、特に外交・安全保障分野で活躍する「ギーク」は不足している。業界団体や政府主導のワークショップ型ハッキング大会(いわゆる Capture The F1ag:CTF)などを通じて、有能な人材を積極的に登用していく必要がある。

おわりに

サイバー空間は「開かれ、グローバル（open & global）」であるが故に脅威にさらされている。リスクを管理し、「安全で強靭（secure & resilient）」な空間を構築しなければならない[51]。だが、「グローバル・コモンズ」としての性格を有するサイバー空間は単一の国家の統制下にあるわけではなく、諸国家による自律的な秩序が必要とされる。

一般的にいえば、抑止メカニズムは国際安全保障・秩序を構成する重要要素だが、サイバー空間の抑止メカニズムは問題に直面している。サイバー空間では、防御に対して攻撃が優勢であり、その攻撃の発信源の特定は難しい。「帰属問題」と「攻撃優位」のアーキテクチャにより、サイバー空間で懲罰的な抑止力は機能しないと考えられてきた。

しかし、ここ数年で、アメリカの防衛・安全保障政策はサイバー攻撃者を特定し、報復を示唆するような抑止力（懲罰的抑止力）を模索している。そして、サイバー抑止力は各国によるサイバー空間へのアクセスと安定的利用を保証する。日本そして日米同盟もこうした動きに呼応し、日米によるサイバー抑止力を整備していく必要がある。

－注－

1 The White House, *National Security Strategy of the United States* (Washington D.C.: White House, May 2010), pp.49-50.

2 The White House, *National Security Strategy of the United States*, pp.27-28.

3 CYBERCOM は戦略軍司令部（Strategic Command: STRACOM）隷下だが、司令官は他の統合軍司令部と同様に大将が務める。また、CYBERCOM 司令官アレクサンダー大将（Keith B. Alexander）は国家安全保障局（National Security Agency: NSA）長官を兼務する。

4 Ellen Nakashima, “Pentagon to boost cybersecurity force,” *The Washington Post* (January 28, 2013).

5 The White House, *Comprehensive National Cybersecurity Initiative* (Washington D.C.: White House, March 2, 2010)。

6 サイバー抑止に関する研究・考察として、Martin C. Libicki, *Cyberdeterrence and Cyberwar* (RAND, 2009); Richard L. Kugler, “Deterrence of Cyber Attacks,” in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security: Cyberpower and National Security* (Washington, D.C: National Defense University and Potomac Books, 2009), pp.309-340; Thomas J. Mowbray, “Solution Architecture for Cyber Deterrence,”: SANS Institute (April 12, 2010); Patrick M. Morgan, “Applicability of Traditional

Deterrence Concepts and Theory to the Cyber Realm," in National Academy of Sciences, eds., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options of U.S. Policy* (National Academies Pr., 2010), pp.55-76; William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol.89, No.5 (September/October 2010), pp.97-108; David C. Gompert, and Phillip C. Saunders, "Mutual Restraint in Cyberspace," in *The Paradox of Power： Sino-American Strategic Restraint in an Age of Vulnerability* (Washington D.C.; Institute for National Strategic Studies, National Defense University, 2011), pp.115-151;　Charles L. Glaser, "Deterrence of Cyber Attacks and U.S. National Security," Report GW-CSPRI-2011-5, Cyber Security Policy and Research Institute, The George Washington University (June 1, 2011); Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol.5, No.4 (Winter 2011), pp.18-38; Andrew F. Krepinevich, *Cyber Warfare: A "Nuclear Option"?* (Center for Strategic and Budgetary Assessments, 2012); Martin C.Libicki, *Crisis and Escalation in Cyberspace* (Ca: Santa Monica: RAND, 2012); Jason Healey, eds., *A Fierce Domain: Cyber Conflict, 1986 to 2012* (Vienna: Cyber Conflict Studies Association, 2013); Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst & Company, 2013).

[7] William J. Lynn, III, Deputy Secretary of Defense, Remarks at STRATCOM Cyber Symposium, Omaha, Nebraska (May 26, 2010).

[8] リチャード・クラーク、ロバート・ネイク（北川知子ほか訳）『核を超える脅威　世界サイバー戦争：見えない軍拡が始まった』（徳間書店、2011 年）、228 頁。

[9] Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," pp.75-76.

[10] Nye,"Nuclear Lessons for Cyber Security?," p.33.

[11] 例えば、誰を抑止するか（自国抑止 central deterrence,　同盟国を含める拡大抑止 extended deterrence）、いつ抑止するか（有事抑止 immediate deterrence、平時抑止 general deterrence）などが想定される。Lawrence Freedman, *Deterrence* (London; Polity, 2004).

[12] ①敵対者がある行為をとった場合に得られる利益［Benefits: B］、②ある行為が達成される確率［Probability: P］、③ある行為をとった場合に生じるコスト／抑止する者が課すコスト［Costs: C］とすると、抑止が成立するのは **C*(1-P)> B*P** の場合である。より詳細は、土山實男『安全保障の国際政治学：焦りと傲り』（有斐閣、2004 年）、178-179 頁。

[13] 抑止成立の条件は諸説あるが、端的にいえば、それは抑止をする「意思」と「能力」、抑止する側とされる側の「相互認識」の三要素が不可欠である。ただし、抑止成立の要件は論者により微妙に異なる。例えば、ポール（T.V. Paul）によれば、伝統的な抑止が成立する要件は、①抑止を成立させるべく、抑止する側に十分な能力があり、②その抑止が信頼性・信憑性があるものであり、③それが敵対者に伝達されること、である。 T. V. Paul, "Complex Deterrence: An Introduction," in T. V. Paul, Patrick M. Morgan & James J. Wirtz, ed., *Complex Deterrence: Strategy in the Global Age* (Chicago: University of Chicago Press, 2009), pp.2-3.

[14] 本稿で掲げる課題以外に、①サイバー空間の「戦争」「武力攻撃」についての共通認識がない点、どの時点で「戦争」「武力攻撃」となるか判断が難しい点（閾値問題 threshold problem）、②サイバー空間における「二重の非対称性」（アクターやパワーの非対称性、サイバーインフラへの依存度・脆弱度の非対称性）、がサイバー空間の抑止を困難にしている。

[15] Attribution についての詳細分析は、米下院科学技術委員会・技術とイノベーション小委員会のテーマ「将来のサイバー攻撃の帰属をプランニングする」（2010 年 7 月 15 日）、2010 年に開催された米国科学アカデミー（National Academy of Sciences）によるプロジェクトの分科会での検討『サイバー攻撃の抑止についてのワークショップ報告書』を参照。特に、Robert K. Knake, "Untangling Attribution: Moving to Accountability in Cyberspace," Prepared Statement Before the Subcommittee on Technology and Innovation, Committee on Science and Technology, United States House of Representatives(July 15, 2010); David D. Clark and Susan Landau, "Untangling Attribution," in National Academy of Sciences, eds., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options of U.S. Policy* (National Academies Pr., 2010), pp.25-40; W. Earl Boebert, "A Survey of Challenges in Attribution ," in *Proceedings of a Workshop on Deterring Cyberattacks*, pp.41-52.

[16] 報告書によれば、人民解放軍は単一の攻撃目標から 6.5 テラバイト（TB）のデータを入手した。これは、新聞紙朝刊の約 12 万年分の情報量に相当する。Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Feburary 2013) 。また、報道によれば、高高度ミサイル防衛（THAAD）、F-35 統合打撃戦闘機、新型オスプレイなど最先端の防衛機密情報がサイバー攻撃によって剽窃された可能性がある。"Pentagon aircraft, missile defense programs target of China cyber threat," *The Washington Post* (May 28, 2013).

[17] Chinese military never supports cyberattacks: defense ministry, Ministry of National Defense, The People's Republic of China (February 20, 2013)
http://eng.mod.gov.cn/Press/2013-02/20/content_4433574.htm

[18] Clark and Landau, "Untangling Attribution," p.39.

[19] Noah Shachtman, "Kremlin Kids: We Launched the Estonian Cyber War," Danger Room: What's Next in National Security, the Blog by *Wired* (March 11, 2009).

[20] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," Issue Briefs, Atlantic

Council (January 2012).

[21] CSIRT とは、インターネットを媒介とするサイバー攻撃やインシデントの状況監視、攻撃・インシデント発生時の対処、その他組織との調整を行う組織体の一般名称である。日本では一般社団法人 JPCERT コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center: JPCERT/CC）などが代表的である。

[22] 国内 CSIRT 関係者へのヒアリング。

[23] インターネットとサイバー空間は同議ではない。前者は個別のネットワークやシステム同士をつなぐネットワークである。後者はインターネットを含め、クローズド・ネットワークや周辺デバイスを含むものである。

[24] The White House, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington D.C.: White House, May 2009), iii.

[25] Robert E. Kahn, “The Role of Architecture in Internet Defense,” in Kristin M. Lord and Travis Sharp, eds., *America’s Cyber Future: Security and Prosperity in the Information Age*, Vol.2 (Washington, D.C.: The Center for New American Security, June 2011) pp.208-209.

[26] 土屋大洋「サイバースペースのガバナンス」、公益財団法人 日本国際問題研究所（外務省外交・安全保障調査研究事業）、平成 25 年度研究プロジェクト「グローバル・コモンズにおける日米同盟の新しい課題」分析レポート（2013 年 8 月）。

[27] Krepinevich, *Cyber Warfare,* p.40.

[28] William J. Lynn , III,　Remarks on Cyber at the RSA Conference, San Francisco, California (February 15, 2011).

[29] 国際政治学・安全保障研究では、攻撃と防御の区別と優劣は国家間の安定性（戦争と平和）に大きな影響を与えていると考えられてきた。安全保障研究では、攻撃と防御の区別がつかないほど、安全保障のジレンマが発生する。そして、防御に対して攻撃が優勢であるほど、侵攻のリスクが高くなる。前述のとおり、サイバー空間は攻撃有利であり、攻撃と防御は区別が難しい。それゆえサイバー空間は「二重のリスク」（doubly dangerous）を抱えている。Robert Jervis, “Cooperation Under the Security Dilemma,” *World Politics*, Vol. 30, No. 2 (January 1978), pp. 167-214.

[30] Lynn, “Defending a New Domain,” p.99.

[31] Statement of Gen. Keith B. Alexander, Commander, United States Cyber Command, before　the House Committee on Armed Services(September 23, 2010).

[32] Lynn, “Defending a New Domain,” pp.99-100.

[33] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War: Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force," *Wall Street Journal* (May 31, 2011).

[34] 安全保障研究では、抑止（deterrence）と防御（defense）を区別する場合がある。抑止は敵対者に攻撃を思いとどまらせることであり、防御は抑止が失敗した際に攻撃の被害を抑えることである。Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961). しかし、サイバーセキュリティは攻撃・防御、抑止力・防衛力は峻別できず、両者を一体的に扱っている。

[35] CYBERCOM の 5 つの戦略（a five-pillared strategy）とは、(1)サイバー空間が戦争・防衛の新たなドメインであると認識すること、(2)積極的・能動的な防衛、(3)死活的に重要なインフラの保護、(4)集団的防衛、(5)技術的優位の確保と活用である。Statement of Gen. Keith B. Alexander, Commander United States Cyber Command, Before the House Committee on Armed Service (September 23, 2010).

[36] Department of Defense, Department of Defense Strategy for Operating in Cyberspace (July 2011), p.7.

[37] Developments in China's Cyber and Nuclear Capabilities, Hearing Before the U.S.-China Economic and Security Review Commission, One Hundred Twelfth Congress Second Session (March 26, 2012), pp.11-13. Aliya Sternstein, “U.S. must strut cyber might to stop attacks, Cartwright says,” *Nextgov* (May 15, 2012).

[38] Department of Defense, *Department of Defense Cyberspace Policy Report*, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934 (November 2011), p.2.

[39] Secretary of Defense Leon E. Panetta, Remarks on Cybersecurity to the Business Executives for National Security, New York City (October 11, 2012).

[40] Department of Defense, *Department of Defense Cyberspace Policy Report*, pp.4-5. なお、同様のプログラムは防衛省も開発を進めている。「防衛省が対サイバー兵器、攻撃を逆探知し無力化」『読売新聞』（2012 年 1 月 1 日）。また、日本国内でもサイバー空間における攻撃オプションの検討が始まった。中期防衛力整備計画（2013 年）では、「攻撃側が圧倒的に優位であるサイバー空間での対処能力を確保するため、相手方によるサイバー空間の利用を妨げる能力の保有の可能性についても視野に入れる」としている。

[41] Lynn, Remarks at STRATCOM Cyber Symposium.

[42] James A. Lewis, “Cross-Domain Deterrence and Credible Threats,” Center for Strategic and International Studies (July 2010).

[43] Department of Defense, *Department of Defense Cyberspace Policy Report*, p.4.

[44] Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat* (January 2013), pp.40-43.

[45] グレイサーは「対価値サイバー攻撃（countervalue cyber attacks）」と「対軍事施設サイバー攻撃（counter-military cyber attacks）」という概念で、リビッキは「戦略的なサイバー戦争（strategic cyberwar）」と「作戦行動としてのサイバー戦争（operational cyberwar）」という定義で攻撃対象についての議論を進めている。Glaser, Deterrence of Cyber Attacks and U.S. National Security,”　Libicki, *Cyberdeterrence and Cyberwar*.

[46] リビッキは「公然たる（overt）攻撃／報復」「明白な（obvious）攻撃／報復」「秘密裏の（covert）攻撃／報復」という観点でリスク評価を行う。Libicki, *Crisis and Escalation in Cyberspace*, pp.155-158.

[47] Richard Bejtlich, “Don‘t Underestimate Cyber Spies: How Virtual Espionage Can Lead to Actual Destruction,” Snapshots on *Foreign Affairs* (May 2, 2013).
http://www.foreignaffairs.com/articles/139357/richard-bejtlich/dont-underestimate-cyber-spies

[48] Bryan Krekel, Patton Adams, *George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, Prepared for the U.S.-China Economic and Security Review Commission (McLean, VA: Northrop Grumman Corporation, March 2012), p.15［公益財団法人 防衛基盤整備協会訳「情報優位の獲得：コンピュータ・ネットワーク作戦及びサイバースパイ活動のための中国の能力」（公益財団法人 防衛基盤整備協会、2012 年 9 月）、10 頁］; Bryan Krekel [Principal Author], *Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* Prepared for The US-China Economic and Security Review Commission (McLean, VA: Northrop Grumman Corporation Information Systems Sector, October 2009)［財団法人 防衛調達基盤整備協会訳「中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力」BSK 保全小冊子、第 22-5 号（平成 22 年 9 月）］。

[49] Ellen Nakashima, “When is a cyberattack an act of war?” *The Washington Post* (October 26, 2012)　ナカシマによれば、判断基準の 1 つは、サイバー攻撃が通常の「武力攻撃」と同様の「耐え難い」損害を与えるのかどうかである。「耐え難い」損害とは、物理的または動的な（kinetic）な損害を指す。それゆえ、経済的損害のみが発生するサイバー攻撃や情報収集目的のサイバー・インテリジェンス活動は「戦争行為」「武力攻撃」とはみなしにくい。

[50] ギーク（geek）とは元々「オタク」「変人」の意味であり、情報技術の専門家を指す。スーツ（suits）とは官僚や軍人などの政策形成者を指す。土屋大洋『情報による安全保障：ネットワーク時代のインテリジェンス・コミュニティ』（慶應義塾大学出版会、2007 年）、3-13 頁。

[51] John D. Negroponte and Samuel J. Palmisano, Chairs, Adam Segal, Project Director, *Defending an Open, Global, Secure, and Resilient Internet*, Independent Task Force Report No.70(New York: Council on Foreign Relations, 2013).

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.

第４章　宇宙利用をめぐる安全保障
－脅威の顕在化と日米の対応－

福島　康仁

はじめに

近年、宇宙利用をめぐる安全保障（space security）への関心が世界的に高まっている。宇宙と安全保障の結びつき自体はすでに半世紀を超えており、冷戦期から米ソを中心とする各国は地球上での軍事活動を支援するために人工衛星を利用してきた[1]。それにもかかわらず宇宙利用をめぐる安全保障にあらためて注目が集まっている背景には、軍民両面で宇宙システムへの依存が世界的に深化する一方で[2]、安定的な宇宙利用を揺るがす脅威が顕在化しつつあるという事情がある。宇宙空間の利用を当然視することができた時代は終わりつつあり、宇宙空間そのものが安全保障上の争点となり始めている。

本稿では宇宙利用をめぐる安全保障を主題として取り上げ、宇宙システムへの依存が深まる中、どのような脅威が顕在化しつつあり、それに対して日米はどのように対応しようとしているのかを分析する。

１．深まる宇宙システムへの依存

そもそも宇宙利用をめぐる安全保障の重要性が高まっている背景には、宇宙活動が世界的に活発化し、宇宙システムへの依存が深まっていることがある。衛星を保有・運用する国家や政府コンソーシアムの数は、冷戦後の 20 年間で倍増し 60 カ国近くに達している[3]。また各国政府の宇宙関連支出と企業の宇宙関連収入の合計額は、2012 年までの 5 年間で 37 パーセント拡大し、約 3,043 億 1,000 万ドルに達している[4]。

こうした中、宇宙システムへの依存が世界的に進んでいる。宇宙利用は日々の経済・社会活動に浸透しており、その用途も通信・放送から地球観測（陸域、海域、大気）、測位・航法・時刻同期（PNT）まで幅広い。PNT に着目した場合、1995 年に GPS の完全運用が始まり、その民生用シグナルは世界中で利用されるようになっている[5]。その応用分野は農業、航空、環境、海洋、治安・災害救援、鉄道、レクリエーション、道路、宇宙（衛星の測位・航法等）、測量・地図作成、時刻同期と幅広い[6]。このうち時刻同期は各 GPS 衛星が搭載する原子時計を活用するものであり、通信システムや送電網、金融ネットワークといった重要インフラの多くが同機能に依存するようになっている[7]。

軍事的な観点においても宇宙システムへの依存は世界的に深化しており、情報・監視・

偵察（ISR）からミサイル警戒、環境モニタリング（気象、海洋、宇宙環境）、衛星通信、PNT にいたる多様な用途で衛星が利用されている。軍事目的の宇宙利用自体は米ソを中心に冷戦期から活発に行われていたが[8]、あくまで核抑止や軍備管理への貢献といった戦略レベルでの利用が中心であった。これに対して冷戦後は作戦レベルや戦術レベルにおける宇宙利用が活発化しており、実際の軍事作戦との結びつきが強くなっている。

このような宇宙の軍事利用をめぐる新たな潮流の形成を主導してきたのが米国である。同国は 1991 年の湾岸戦争を契機として軍事作戦への宇宙の組み込みを本格化させ、その後に従事したバルカン半島やアフガニスタン、イラク等での戦闘作戦において活発に宇宙を利用してきた[9]。各作戦における衛星通信の需要は、プレデターやグローバルホークといった滞空型無人機の登場などによって顕著に増大している。イラク戦争では湾岸戦争に比して約 40 倍の帯域が使用されたとの見積もりも存在する[10]。GPS の作戦利用も一層顕著となっている。1990 年代にイラクやバルカン半島での作戦で米国が使用した誘導弾の大半はレーザー/光学式のものであった。対照的に 2001 年に開始されたアフガニスタンでの作戦で米国が使用した誘導弾の半数以上は GPS を利用したものとなった[11]。また 2002 年以降、GPS を用いて自己や友軍等の位置を自動表示する BFT が南西アジアに展開する米軍車両に配備されるようになった[12]。同装置は実際にアフガニスタンやイラクでの作戦で活用され、戦場認識を飛躍的に向上させたといわれている[13]。

こうしたことから宇宙システムは作戦上、欠くべからざるものであるとの認識が米国内では広がってきている。例えば、米空軍宇宙コマンド司令官のウィリアム・L・シェルトン（William L. Shelton）大将は、人道作戦から主要な戦闘作戦にいたるまで、米国の軍事作戦は宇宙に依存しているとの認識を明らかにしている[14]。また PNT に関する米大統領令において、GPS は米国の安全保障にとって決定的に重要であり、実質的に同国の軍事作戦のあらゆる側面で利用されるようになっているとの認識が示されている[15]。

宇宙の軍事利用を拡大しているのは米国だけではない。冷戦期から宇宙の軍事利用を継続してきたロシアに加えて中国やインド、オーストラリア、カナダ、フランス、ドイツ、日本、イスラエル、イタリア、スペインなどが、軍事衛星もしくは軍事利用も可能な多目的衛星を開発・運用するようになっている[16]。フランス軍統合参謀本部副作戦部長のベルナール・ロジェ（Bernard Rogel）海軍中将は、偵察や気象、通信、航法、ミサイル防衛などにおいて、宇宙は作戦上のアセットを提供する強力で不可欠な存在であると述べている[17]。GPS 誘導弾を例にとると、フランスは AASM と呼ばれるキットを導入し 2008 年から実戦投入している[18]。また、GPS 誘導弾の代名詞ともいえる JDAM は米海空軍以外でも利用されるようになっており、2012 年時点で航空自衛隊を含む 26 の海外顧客に輸出されている[19]。

このように宇宙活動の世界的な活発化に伴い宇宙システムへの依存が深まる傾向にあるが、このことは同時に宇宙利用に伴う脆弱性の増大をもたらしている。宇宙システムへの依存が深まるほど､いったん宇宙システムを利用できなくなった際の影響も大きくなる。この脆弱性問題はこれまで潜在的なものにとどまってきた。だが、後述のとおり宇宙利用をめぐる脅威が顕在化するにつれて、同問題も顕在化しつつある。

２．宇宙利用をめぐる脅威の顕在化

陸海空あるいはサイバー空間と異なり、宇宙空間は長らく戦争のない聖域（sanctuary）であるとみなされてきた[20]。前述のとおり宇宙の軍事利用は冷戦期から活発に行われてきたものの、その目的はあくまで地球上での軍事活動を支援することにあった。だが、宇宙利用をめぐる脅威の顕在化によって、そうした状況には変化が表れつつある。

とりわけ世界最大の宇宙利用国である米国は[21]、こうした戦略環境の変化に強い危機感を抱いている。2011 年に米国防長官と国家情報長官が議会に提出した「国家安全保障宇宙戦略」（NSSS）では、宇宙空間はますます軍事的な挑戦を受ける領域（contested domain）になっており、宇宙システムとその支援インフラは多様な人為的脅威に直面しているとの認識が示されている[22]。

このような認識の背景には、意図と能力の両面において宇宙利用をめぐる脅威が顕在化しつつあるという事情がある。前者については「暗黙の了解」（tacit agreement）に頼ることの限界が米国内で認識されるようになっている[23]。冷戦期、米ソ間には、一方が他方の宇宙利用を妨害しない限り、もう片方も宇宙利用の妨害を行わないという不文律が存在していたといわれる[24]。これは相互核抑止や戦略的安定に果たす偵察衛星等の役割を米ソが互いに認識していたことによる。実際、1972 年の SALT I 合意以降、米ソ間の軍備管理条約には、偵察衛星等を念頭に置いて、「自国の検証技術手段」（NTM）への妨害禁止が明記された[25]。また他者の宇宙利用を妨害することを目的とした対衛星（ASAT）兵器等の配備も限定的なものにとどめられた[26]。だが、このような「暗黙の了解」は米ソ冷戦という特定の文脈において存在し得たものであり、現在および将来、米国が直面する潜在的な敵対者はそうした文脈を共有していない。むしろ、宇宙システムへの依存を米国の脆弱性としてとらえ、重要な攻撃目標として宇宙システムを位置づける可能性が指摘されている[27]。

加えて、能力面においても宇宙利用をめぐる脅威は顕在化しつつある。宇宙利用を妨害する手段は多様であり、軌道上の衛星を物理的に破壊する ASAT 兵器以外にも、衛星のセンサー等を狙ったレーザー照射、衛星や地上局の電子機器を狙った電磁パルス（EMP）攻撃、データリンクへのジャミング、地上局や支援インフラへの攻撃・妨害工作、宇宙シス

テムへのサイバー攻撃などが想定され得る[28]。

これらの脅威はこれまで潜在的なものにとどまってきたが、2000 年代に入り実際の使用事例が散見されるようになっている。最も顕著なのは GPS シグナルや衛星通信・放送に対するジャミングである[29]。2003 年のイラク戦争において、イラクは GPS シグナルへのジャミングを試みた[30]。これは米国が戦闘作戦中に GPS 利用への妨害を受けた初の事例であったといわれる[31]。北朝鮮は 2010 年から 2012 年にかけて、GPS シグナルへのジャミングをたびたび実施し、南北境界線付近の航空機や船舶、車両の測位・航法に影響を与えたといわれる[32]。衛星放送に対するジャミングも日常的にみられるようになっており、イランやリビア、エチオピアなどでの事例が報告されている[33]。

衛星の物理的破壊については、2007 年に中国が実施した事例が有名である。中国は DF-21 準中距離弾道ミサイルを改良した SC-19 を用いて、自国の古い気象衛星を高度 865 キロの低軌道上で破壊したと考えられている[34]。衛星の物理的破壊を伴う ASAT 実験に成功したのは米ソに次いで 3 番目であり、冷戦後では初めてのことであった[35]。この他、レーザー照射については、2006 年に中国が米国の偵察衛星に対して地上から実施したといわれている[36]。サイバー攻撃についても 2007 年と 2008 年に米国の宇宙システムが攻撃を受けたといわれている[37]。

このように宇宙利用に対する妨害はそれほど珍しいものではなくなりつつある。妨害を行い得る主体も上記のとおり多様である。特に、宇宙利用への依存度が低い一方で、他者の宇宙利用を妨害する能力を保有する主体は、宇宙利用への依存度が高い主体に比べて攻撃の敷居が低い場合が考えられる。例えば、核爆発によって宇宙空間に EMP を発生させた場合、その影響は付近の衛星に無差別に及ぶことになるが、宇宙利用への依存度が低い北朝鮮等の主体はその影響をそれほど考慮する必要がない可能性が指摘されている[38]。こうした非対称の脅威の存在は、宇宙利用への依存度が高い主体にとっては共通の課題であるといえる。

３．日米の対応

宇宙システムに深く依存する日米は宇宙利用をめぐる脅威の顕在化を受けた対応を進めている。まず、米国の対応は多層的なアプローチによる攻撃の抑止と、抑止の失敗に備えたレジリエンス（強靱性あるいは抗たん性）の強化を柱としている。このうち宇宙システムに対する攻撃の抑止は 4 層構造となっている[39]。第 1 層は外交的手段を通じた規範の醸成である。これは宇宙ゴミの発生を伴う ASAT 兵器の使用などを無責任な行為とみなす国際的な規範を形成していくことで、敵対者が攻撃を実施する際の計算を複雑にすること

を意図したものである。現在、米国が進めている透明性・信頼醸成措置（TCBMs）もこうした点を考慮に入れながら進められている。2012 年には当時のヒラリー・R・クリントン（Hillary R. Clinton）国務長官が、宇宙活動に関する国際行動規範の策定に向けて各国と協力することを表明した[40]。

多層抑止の第 2 層は宇宙利用をめぐるコアリションを構築することである。これは敵対者が宇宙システムを攻撃する場合、米国のみならず当該宇宙システムを利用する全ての国家と対峙せざるを得ない状況を作り出すことで、敵対者による攻撃の敷居を上げることを狙ったものである。例えば、米空軍の WGS と呼ばれる通信衛星群については、オーストラリアが 6 機目、カナダとデンマーク、ルクセンブルク、オランダ、ニュージーランドが 9 機目の衛星の費用を負担することで、これらの国に同衛星群の通信帯域へのアクセスを認める取り組みが進められている[41]。

第 3 層は後述するレジリエンスの強化である。個々の衛星ではなく宇宙利用に関するアーキテクチャ全体のレジリエンスを強化し、かつ宇宙利用がある程度妨げられた環境下でも作戦を継続できる態勢を構築することが目指されている。これは攻撃によって敵対者が得られる効果を限定し､攻撃のインセンティブを低下させることを意図したものである。

最後の層は攻撃に対する対応能力・態勢の保持である。米国あるいは同盟国が利用する宇宙システムを攻撃した場合、相応の対応を行う姿勢を明確にしておくことで、敵対者による攻撃を抑止することを狙っている。米国は攻撃に対して比例的に対応するとしている一方で、実際の対応は必ずしも対称的な形でなされるわけではなく、対応する領域は宇宙に限定されず、その手段も軍事力に限定されないことを明確にしている[42]。

このように米国は 4 つの層を積み重ねることで宇宙システムに対する攻撃を可能な限り抑止する一方で、抑止の失敗に備えたレジリエンスの強化も進めている[43]。その際、一つの中核となりつつあるのが、分散された宇宙アーキテクチャを構築していくことである[44]。具体的には、単一の衛星が果たしている機能を複数の衛星に分割することや、衛星の余剰スペースに副次的ペイロードを搭載すること[45]、利用する軌道を多様化すること、宇宙のみならず陸海空といった他領域への分散を進めることなどが検討されている[46]。

さらに、これらの多層抑止やレジリエンス強化の基盤として位置付けられているのが宇宙状況認識（SSA）であり、米国はその向上に取り組んでいる。具体的には宇宙監視能力の増強に加えて[47]､戦略軍の SSA 共有プログラムを通じた他国や企業との情報共有の推進[48]、フランスやカナダ、オーストラリア、日本といった同盟国との SSA 協力を進めている[49]。

米国と歩調をあわせる形で、日本も宇宙利用をめぐる脅威への対応を進めている。具体的には外交的手段を通じた規範の醸成や、衛星の抗たん性の強化を進めていく方向性が示

されている。2012 年にはクリントン国務長官の声明にあわせる形で、当時の玄葉外務大臣が国際行動規範案に関する国際的な議論に参加することを表明した[50]。2013 年末に公表された「国家安全保障戦略」においても、国際行動規範の策定に向けた取り組みに積極的に参加することが明記されている[51]。

加えて、「国家安全保障戦略」と同時期に公表された「平成 26 年度以降に係る防衛計画の大綱」と「中期防衛力整備計画（平成 26 年度～平成 30 年度）においては、SSA 等を通じて衛星の抗たん性を高めていく方針が打ち出された[52]。これと連動する形で、防衛省の平成 26 年度予算案においては、SSA システムの導入可能性調査や、衛星等に対する固定式警戒管制レーダー（FPS-5）の探知・追尾能力等の技術的検証、衛星通信システムの通信妨害対策に関する研究、防衛省・自衛隊の衛星防護のあり方に関する調査研究などが盛り込まれている[53]。

おわりに

本稿では宇宙利用をめぐる安全保障を主題として、宇宙利用への依存が深まる中、どのような脅威が顕在化しつつあり、それに対して日米がどのように対応しようとしているのかを分析した。日米はともに主要な宇宙活動国であり、安定的な宇宙利用の確保を必要としているという点で利害を共有している。また、上述のとおり、宇宙利用をめぐる基本的な戦略環境認識とそれに基づく対応は共通点が多く、同分野における協力も進み始めている。

他方、宇宙利用をめぐる脅威への対応は米国においても緒に就いたばかりであり、日米で検討していかなければならない課題も多い。そうした課題としては、例えば、宇宙監視にとどまらない SSA 協力の推進、日米の宇宙活動能力を活用したレジリエンスの強化、宇宙と抑止の結びつきに関する検討（特に日本側）といったことが挙げられるだろう。

現状において日米 SSA 協力の中核となっている宇宙監視（space surveillance）に加えて、各種インテリジェンス活動を通じて得られた各国の宇宙活動に関する情報を緊密に共有していくことが重要となってくるだろう[54]。SSA とは宇宙作戦が依存する宇宙環境および作戦環境に関する知識（knowledge）のことであるが[55]、日本側はこうした知識の蓄積を始めたばかりである。今後は米国等との情報交換を通じて、各国の宇宙活動や宇宙利用をめぐる脅威などに関する認識の向上をはかっていく必要がある。

またレジリエンスの強化は米国のみならず日本にとっても主要課題となりつつあることから、将来的には SSA と並ぶ日米協力の柱となる可能性がある。日本は数少ない自立的宇宙活動国の一つであり、実際に多数の衛星を製造し打ち上げてきた実績を有している。

この点は、これまで米国が安全保障分野における宇宙協力を緊密に進めてきた国々にはない日本の強みであり[56]、これらの国々とは異なる形での対米協力もあり得るだろう。

最後に、宇宙と抑止の結びつきについては、特に日本側における検討を加速させる必要がある。すでに米国においてはレジリエンスと並ぶ柱として抑止が位置付けられており、抑止の強化に向けた取り組みが行われている。日本が進めている外交的手段を通じた規範の醸成や衛星の抗たん性の強化も、宇宙システムに対する攻撃を抑止する手段として位置付け直すことが可能である。こうした点については米国との緊密な意見交換を進めながら概念整理を進めていく必要があるだろう。

－注－

1 米国は 1960 年 6 月に信号情報収集衛星「Grab 1」の打ち上げに成功し、同衛星は世界初の偵察衛星となった。さらに同年 8 月に画像情報収集衛星「Corona」が撮影したフィルムの回収に初成功した。Bruce Berkowitz, “The National Reconnaissance Office At 50 Years: A Brief History,” Center for the Study of National Reconnaissance, National Reconnaissance Office, September 2011, pp. 9, 11, accessed December 10, 2013, http://www.nro.gov/history/csnr/programs/NRO_Brief_History.pdf.ソ連も 1962 年には同国初の偵察衛星を打ち上げたといわれる。Thomas Graham Jr. and Keith A. Hansen, Spy Satellites and Other Intelligence Technologies That Changed History (Seattle: The University of Washington Press, 2007), p. 38.

2 宇宙システムには軌道上の人工衛星のみならず、地上局やデータリンク、打ち上げシステム、その他の支援インフラなども含まれる。U.S. Air Force, Space Operations, Air Force Doctrine Document 3-14, June 19, 2012, p. 4, accessed December 20, 2013, http://static.e-publishing.af.mil/production/1/af_cv/publication/afdd3-14/afdd3-14.pdf.

3 U.S. Department of Defense and Office of the Director of National Intelligence, National Security Space Strategy, Unclassified Summary, January 2011, p. 2, accessed December 20, 2013, http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.ただし、衛星を自力で製造し打ち上げる能力を有する自立的宇宙活動国の数は依然として 10 カ国程度にとどまっている。その他の国は衛星の製造や打ち上げを他国に依存している。

4 Space Foundation, The Space Report 2013 (Colorado Springs, 2013), p. 26.

5 GPS は米国防省によって運用されているシステムであるが、軍用サービスに加えて民生用サービスを提供している。その契機となったのは 1983 年の大韓航空機撃墜事件であり、同事件を受けてロナルド・W・レーガン（Ronald W. Reagan）大統領が当時、整備途上にあった GPS の民間開放を決定した。Statement by Deputy Press Secretary Speaks on the Soviet Attack on a Korean Civilian Airliner, September 16, 1983, accessed December 19, 2013, http://www.reagan.utexas.edu/archives/speeches/1983/91683c.htm.米国の GPS 以外にも、ロシアのグロナス（GLONASS）がグローバルな PNT サービスを提供している。また欧州のガリレオ（Galileo）と中国の北斗もグローバルな PNT システムとして、さらに日本の準天頂衛星システム（QZSS）とインドの IRNSS は地域的なシステムとして、それぞれ整備が進められている。Ibid., pp. 86-87.

6 National Coordination Office for Space-Based Positioning, Navigation, and Timing, “GPS.GOV: GPS Applications,” U.S. Government, accessed December 20, 2013, http://www.gps.gov/applications/.

7 National Coordination Office for Space-Based Positioning, Navigation, and Timing, “GPS.GOV: Timing,” U.S. Government, accessed December 20, 2013, http://www.gps.gov/applications/timing/.

8 例えば米国が 1958 年から 1990 年までに打ち上げた軍事衛星の数は計 668 機であり、同時期における民生衛星の打ち上げ数（492 機）を上回っている。下記をもとに筆者集計。なお、民生衛星には軍事ペイロードを搭載したものが含まれている。Tamar A. Mehuron, “2009 Space Almanac: The US Military Space Operation in Facts and Figures,” Air Force Magazine, vol. 92, no. 8 (August 2009), p. 59.

9 詳細は下記を参照。福島康仁「戦闘作戦における宇宙利用の活発化とその意義―1990 年代以降の米国における議論」日本国際政治学会 2013 年度研究大会報告ペーパー（2013 年 10 月）。

10 Dan Dia-Tsi-Tay, “COMM-OPS-Major Trends in the Tactical Use of MILSATCOM,” MilsatMagazine, May

2009, accessed December 21, 2013, http://www.milsatmagazine.com/story.php?number=1820534170.

11 同データは開戦からの 90 日間に関するものである。Joseph Rouge, “Air and Space Integration- In a Contested Environment,” National Security Space Office, slide 7, accessed December 22, 2013, http://airpower.airforce.gov.au/UploadedFiles/General/Day1_Rouge.pdf.GPS 誘導弾の利用が顕著となったのは、JDAM の登場によるところが大きい。JDAM は無誘導の自由落下爆弾に装着するキットである。誘導に慣性航法装置とともに GPS を利用することからレーザー/光学式誘導弾のように天候の制約を受けることがない。加えて 1 キットあたり約 2 万 2000 ドルと安価であるため頻繁に用いられるようになった 。“Fact Sheet: Joint Direct Attack Munition GBU-31/32/38,” U.S. Air Force, June 18, 2003, accessed December 10, 2013, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104572/joint-direct-attack-munition-gbu-313238.aspx. なお、JDAM が初めて実戦投入されたのは 1999 年にバルカン半島で展開された同盟の力作戦である。B-2 ステルス爆撃機との組み合わせによって大きな戦果を挙げた一方で、製造開始から間がなかったため使用可能な数量は限られていた。Boeing, “Joint Direct Attack Munition (JDAM),” January 2012, accessed December 10, 2013, http://www.boeing.com/assets/pdf/defense-space/missiles/jdam/docs/jdam_overview.pdf.

12 Richard J. Dunn,Ⅲ, “Blue Force Tracking: The Afghanistan and Iraq Experience and Its Implications for the U.S. Army,” Northrop Grumman, accessed January 23, 2014, http://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/BFT-Afghanistan-and-Iraq-Exper.pdf.

13 Ibid.

14 Air Force Space Command, “2013 AFA Pacific Air & Space Symposium General William L. Shelton, Commander, Air Force Space Command, Los Angeles, Calif. – Nov. 21, 2013,” U.S. Air Force, accessed December 10, 2013, http://www.afspc.af.mil/library/speeches/speech.asp?id=744.

15 President of the United States of America, Fact Sheet: U.S. Space-Based Positioning, Navigation, and Timing Policy, National Security Presidential Directive-39, December 15, 2004, accessed December 15, 2013, http://www.gps.gov/policy/docs/2004/.

16 Spacesecurity.org, Space Security Index 2013 (Ontario: Pandora Print Shop, 2013), p. 68.日本の防衛省は平成 27 年度に次期 X バンド通信衛星を打ち上げる予定である。防衛省編『平成 25 年版　日本の防衛―防衛白書―』（日経印刷株式会社、2013 年）123 頁。

17 Bernard Rogel, “Operational Benefits from Space, ” Space For Operations, 2011, p. 61.

18 “AASM: From Precision Guided Munitions to Smart Weapons,” Sagem, Safran, accessed December 24, 2013, http://www.sagem.com/spip.php?rubrique80.

19 Boeing, “Joint Direct Attack Munition (JDAM),” January 2012.航空自衛隊への JDAM の納入は 2007 年に開始されている。ボーイング・ジャパン「Made with Japan: A Partnership on the Frontiers of Aerospace」（2013 年）5 頁、2013 年 12 月 25 日アクセス。http://www.boeing.jp/BoeingJapan/media/BoeingJapan/Boeing%20in%20Japan/Made%20with%20Japan/1122_boeing_jcb13_final.pdf.

20 冷戦期の議論については下記を参照。David E. Lupton, On Space Warfare: A Space Power Doctrine (Alabama: Air University Press, 1988).

21 米国政府による宇宙関連支出は、2012 年時点で、各国政府による関連支出の 61 パーセントを占めていると見積もられている。Space Foundation, The Space Report 2013, p. 37. また全世界で運用中の衛星（2013 年 8 月 31 日時点で 1084 機）のうち、半数近く（同 461 機）は米国のものであると考えられている。“UCS Satellite Database,” Union of Concerned Scientists, September 13, 2013, accessed December 26, 2013, http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html.

22 この他にも NSSS では、宇宙空間がますます混雑するようになっており、宇宙ゴミとの衝突や電波干渉の危険性が増大しているとの認識が示されている。U.S. Department of Defense and Office of the Director of National Intelligence, National Security Space Strategy, pp. 1-3.こうした認識は日本の「国家安全保障戦略」でも共有されており、国際公共財（グローバル・コモンズ）に関するリスクの一つとして、宇宙ゴミの増加や対衛星兵器の開発などによって、持続的かつ安定的な宇宙空間の利用が妨げられる可能性が指摘されている。「国家安全保障戦略について（平成 25 年 12 月 17 日国家安全保障会議決定、閣議決定）」首相官邸、8 頁、2014 年 12 月 20 アクセス。http://www.kantei.go.jp/jp/kakugikettei/2013/__icsFiles/afieldfile/2013/12/17/20131217-1_1.pdf.

23 例えば、下記のゲアリー・ペイトン（Gary Payton）米空軍副次官（当時）の発言を参照。“Gary Payton, Deputy Undersecretary For Space Programs, U.S. Air Force,” Defense News, May 17, 2010, accessed December 15, 2013, http://www.defensenews.com/article/20100517/DEFFEAT03/5170306/Gary-Payton.

24 こうした暗黙の了解を米国の歴史家ジョン・L・ギャディス（John L. Gaddis）は「偵察衛星レジーム」と名付けている。ジョン・L・ギャディス『ロング・ピース―冷戦史の証言「核・緊張・平和」』五味

俊樹他訳（芦書房、2002 年）345－374 頁。ソ連側もこのような認識を共有していたか否かについては一層の検証が必要であるが、本稿の主眼は米国の脅威認識の変化を説明することにある。

[25] Graham Jr. and Hansen, Spy Satellites and Other Intelligence Technologies That Changed History, pp. 130-135.

[26] ただし、冷戦中、米ソはさまざまな ASAT 兵器等の研究・開発・実験を行い、その一部を配備した。詳細については下記を参照。Paul B. Stares, The Militarization of Space: U.S. Space Policy, 1945-1984 (New York: Cornell University Press, 1985).

[27] U.S. Department of Defense and Office of the Director of National Intelligence, National Security Space Strategy, p. 3.

[28] U.S. Air Force, Space Operations, June 19, 2012, pp. 40-41.

[29] 米国政府は、GPS が意図的・非意図的な干渉の影響を受ける可能性を認めており、全ての GPS 利用者に対して代替手段を維持するように促している。National Coordination Office for Space-Based Positioning, Navigation, and Timing, “GPS.GOV: Frequently Asked Questions,” U.S. Government, accessed December 25, 2013, http://www.gps.gov/support/faq/#jamming.

[30] Jim Garamone, “CENTCOM Charts Operation Iraqi Freedom Progress,” American Foreign Press Service, March 25, 2003, accessed December 15, 2013, http://www.defense.gov/News/NewsArticle.aspx?ID=29230.

[31] US Air Force, Space Operations, Air Force Doctrine Document 3-14, November 27, 2006, Incorporating Change 1, July 28, 2011, p. 33.

[32] “‘North Korea Jamming’ Hits South Korea Flights,” BBC News, May 2, 2012, accessed December 10, 2013, http://www.bbc.co.uk/news/world-asia-17922021; “Massive GPS Jamming Attack by North Korea,” GPS World, May 8, 2012, accessed December 10, 2013, http://gpsworld.com/massive-gps-jamming-attack-by-north-korea/.

[33] “Iran’s Attacks on the BBC,” Index on Censorship, February 18, 2013, accessed December 10, 2013, http://www.indexoncensorship.org/2013/02/iran-bbc-censorship-jamming/; Roy Greenslade, “Iran Targets BBC Persian Service By Jamming Signals and Harassing Staff,” The Guardian, February 22, 2013, accessed December 10, 2013, http://www.theguardian.com/media/greenslade/2013/feb/22/bbc-world-service-censorship; “Thuraya Satellite Telecom Says Jammed By Libya,” Reuters, February 24, 2011, accessed December 10, 2013, http://www.reuters.com/article/2011/02/24/libya-satphone-thuraya-idAFLDE71N2CU20110224; “ESAT Accuses China of Complicity in Jamming Signals,” ESAT News Release, June 15, 2011, accessed December 10, 2013, http://ethsat.com/2011/10/08/esat-accuses-china-of-complicity-in-jamming-signals/.

[34] 中国は 2010 年に SC-19 を用いて弾道ミサイル迎撃実験を実施したと考えられている。また 2013 年にも類似の実験を行った可能性が指摘されている。Brian Weeden, “Anti-Satellite Tests in Space-The Case of China,” Secure World Foundation, August 29, 2013, accessed December 10, 2013, http://swfound.org/media/115643/China_ASAT_Testing_Fact_Sheet_Aug2013.pdf.さらに中国は 2013 年中に、DN-2 と呼ばれる SC-19 よりも長射程の ASAT 兵器の発射実験や、衛星による衛星の捕獲実験を行ったとの報道もある。Bill Gertz, “China Conducts Test of New Anti-Satellite Missile,” The Washington Free Beacon, May 14, 2013, accessed December 10, 2013; Bill Gertz, “China Testing New Space Weapons,” The Washington Free Beacon, October 2, 2013, accessed December 10, 2013, http://freebeacon.com/china-testing-new-space-weapons/.

[35] 加えて、同実験は史上最多の宇宙ゴミを発生させたことから、世界の軍関係者のみならず宇宙利用コミュニティ全体の関心を集めることとなった。“Chinese Anti-satellite Test Creates Most Severe Orbital Debris Cloud in History,” Orbital Debris Quarterly News, vol. 11, issue 2 (April 2007), pp. 2-3, accessed December 10, 2013, http://orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv11i2.pdf.

[36] Warren Ferster and Colin Clark, “NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft,” Space News, October 3, 2006, accessed December 10, 2013, http://www.spacenews.com/article/nro-confirms-chinese-laser-test-illuminated-us-spacecraft.

[37] Nicole Blake Johnson, “Report: Cyber Attacks Targeted U.S. Satellites,” Defense News, October 28, 2011, accessed December 10, 2013, http://www.defensenews.com/article/20111028/DEFSECT01/110280301/Report-Cyber-Attacks-Targeted-U-S-Satellites.

[38] Independent Working Group on Missile Defense, the Space Relationship, and the Twenty-First Century, 2009 Report (Washington, DC: The Institute for Foreign Policy Analysis, 2009), appendix k:87.

[39] “Fact Sheet: DoD Strategy for Deterrence in Space,” U.S. Department of Defense, accessed January 7, 2014, http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Strategy%20for%20Deterrence%20in%20Space.pdf.

[40] Hilary R. Clinton, “Press Statement: International Code of Conduct for Outer Space Activities,” U.S. Department of State, January 17, 2012, accessed January 7, 2014, http://www.state.gov/secretary/rm/2012/01/180969.htm.

[41] Mike Gruss, “Australia-Funded WGS-6 Seen as Model for Future U.S. Military Constellations,” Space News, July 24, 2013, accessed January 7, 2014, http://www.spacenews.com/article/military-space/36452military-space-quarterly-australia-funded-wgs-6-seen-as-model-for-future.

[42] 宇宙空間以外での対応としては、例えば、地上に配備されたジャミング装置やASAT兵器への攻撃が考えられる。実際に2003年のイラク戦争においては、イラクが配備したジャミング装置を空爆によって破壊している。Garamone, “CENTCOM Charts Operation Iraqi Freedom Progress,” American Foreign Press Service.他方で、アシュトン・B・カーター（Ashton B. Carter）国防副長官（当時）が2013年の講演において、潜在的な敵対者による宇宙利用に対抗するためのオプションを策定中であると述べている点に留意する必要がある。Ashton B. Carter, “Remarks at National Press Club,” U.S. Department of Defense, May 7, 2013, accessed January 7, 2014, http://www.defense.gov/speeches/speech.aspx?speechid=1775.

[43] “Fact Sheet: Resilience of Space Capabilities,” U.S. Department of Defense, accessed December 10, 2013, http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Fact%20Sheet%20-%20Resilience.pdf. なお、レジリエンスの強化は宇宙ゴミの増大といった非人為的脅威への対応という側面も有している。Air Force Space Command, “White Paper: Resiliency and Disaggregated Space Architectures,” U.S. Air Force, 2013, accessed January 7, 2014, http://www.afspc.af.mil/shared/media/document/AFD-130821-034.pdf.

[44] Ibid.

[45] これは「hosted payloads」と呼ばれる取り組みである。2011年には米空軍の赤外線センサーを搭載した商業用通信衛星の打ち上げが行われ、同センサーは2013年末まで運用された。“Air Force Commercially Hosted Infrared Payload Mission Completed,” U.S. Air Force, December 6, 2013, accessed January 7, 2014, http://www.losangeles.af.mil/news/story.asp?id=123373357.

[46] 他領域への分散は宇宙システムへの依存緩和を意味しているが、宇宙利用の放棄まで視野に入れられているわけではない。シェルトン米空軍宇宙コマンド司令官は、短期的・中期的な観点において宇宙システムに対する現実的な代替物は存在せず、より長期的な観点においてもそうしたものを開発し得るかは定かではないとの認識を示し、脅威の存在を前提とした宇宙システムを整備していく必要性を指摘している。Air Force Space Command, “2013 AFA Pacific Air & Space Symposium General William L. Shelton, Commander, Air Force Space Command, Los Angeles, Calif. – Nov. 21, 2013,” U.S. Air Force.

[47] Mike Gruss, “Lockheed Martin, Raytheon Get Space Fence Bridge Contracts,” Space News, December 27, 2013, accessed January 7, 2014, http://www.spacenews.com/article/military-space/38844lockheed-martin-raytheon-get-space-fence-bridge-contracts.

[48] Tiffany Chow, “Space Situational Awareness Sharing Program: An SWF Issue Brief,” Secure World Foundation, September 22, 2011, accessed January 7, 2014, http://swfound.org/media/3584/ssa_sharing_program_issue_brief_nov2011.pdf.

[49] 例えばオーストラリアとの間では、宇宙監視用の望遠鏡とレーダーを同国に移設する計画が進められている。Office of the Spokesperson, “Australia-United States Ministerial Consultations (AUSMIN),” U.S. Department of State, November 20, 2013, accessed January 7, 2014, http://www.state.gov/r/pa/prs/ps/2013/11/217794.htm.

[50] 「外務大臣会見記録（要旨）（平成24年1月）」外務省、2014年1月7日アクセス。http://www.mofa.go.jp/mofaj/press/kaiken/gaisho/g_1201.html#7-C.

[51] 「国家安全保障戦略について（平成25年12月17日国家安全保障会議決定、閣議決定）」首相官邸、25頁。

[52] 「平成26年度以降に係る防衛計画の大綱について（平成25年12月17日国家安全保障会議決定、閣議決定）」防衛省、18頁、2013年12月20日アクセス。http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/20131217.pdf.「中期防衛力整備計画（平成26年度～平成30年度）について」防衛省、9頁、2013年12月20日アクセス。http://www.mod.go.jp/j/approach/agenda/guideline/2014/pdf/chuki_seibi26-30.pdf.

[53] 「我が国の防衛と予算（案）平成26年度予算の概要」防衛省、2013年12月24日、16頁、2013年12月25日アクセス。http://www.mod.go.jp/j/yosan/2014/yosan.pdf.

[54] 米統合参謀本部のドクトリンではSSAの情報源として、宇宙監視に加えて各種のインテリジェンス活動が挙げられている。U.S. Joint Chiefs of Staff, Space Operations, Joint Publication 3-14, May 29, 2013, Ⅱ-3, accessed January 24, 2014, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

[55] Ibid., Ⅱ-1.

[56] これまで米国は通称「ファイブ・アイズ」（Five Eyes）と呼ばれるインテリジェンス協力の枠内で安全保障分野における宇宙協力を緊密に進めてきたといわれている。同協力枠組みには米国の他にイギリス、カナダ、オーストラリア、ニュージーランドが参加しているといわれる。Roger W. Robinson, Jr. and Andrew K. Davenport, “Advancing Space Security Through The Trilateral U.S.-Europe-Japan Partnership,” Prague Security Studies Institute, July 2012, accessed January 24, 2014, http://www.pssi.cz/download/docs/158_pssi-space-security-report.pdf.

第５章　グローバル・コモンズとしての宇宙におけるガバナンス構築と日米同盟

鈴木　一人

はじめに

人類が宇宙空間を利用し始めてから 50 年がたち、その間、宇宙空間は人間が持ち込んだ、さまざまな「異物」によって使いづらい空間になりつつある。これまで、宇宙に衛星や宇宙船を打ち上げ、それを利用することだけを考えてきた結果、地球周辺の軌道上にはロケットの残骸や機能しなくなった衛星、そして衛星の破片など、さまざまな物体が周回している。これらの「異物」は宇宙デブリ（ごみ）と呼ばれ、高度 300－600km の軌道であれば､秒速 7－8km のスピードで地球を周回している｡このデブリが衛星に衝突すれば、当然のことながら、衛星は損壊するか、機能停止せざるを得ない状況となり、多額の費用をかけて開発し、打ち上げた衛星が利用できなくなるという問題が生じる。

また宇宙空間は軍事戦略的インフラとしての価値を高めている。遠隔地から兵器システムを操作し､的確な位置にナビゲートするためには通信衛星や測位衛星が不可欠となった。また、途上国における大量破壊兵器の開発やテロリストキャンプの監視などは、いきなり無人航空機（UAV）を飛ばすよりも、長期的な変動を偵察衛星から監視する方が効率的である。このように、現代における安全保障上の懸念に対応するためには、宇宙システムが重要な役割を果たしている。

しかし、地球上とは異なり、「人間が利用する」宇宙空間においては、すべての物体が常に移動しているため、ある特定の空間を実効的に支配することは困難であり、地球上で用いられる、主権国家によって分割された空間管理による秩序の維持、という方法をとることはできない。つまり、国家が自国の領域の域内に責任をもち、その秩序を安定させることで国際秩序を維持する、という仕組みをとることができない。言い換えれば、宇宙空間は「グローバル・コモンズ（グローバルな共有地）[1]」であり、宇宙空間を利用するすべての国や企業・個人が「グローバル・コモンズ」に依存している状況のなかで、ある特定の国家のみがその管理に責任を負うのではなく、宇宙空間を利用する者すべてが責任をもたなければならない空間なのである。

とはいえ、宇宙空間で何が起こっているかを直接目にすることは難しい。また、各国や企業が運用している衛星のなかには軍事的な目的で利用されているものも多く、それらの衛星はどの軌道を周回しているのかという情報を開示していない。また、現在、軌道上を

回る物体は 10cm 以上の大きさのものであれば、レーダーなどで探知することが可能であるが、それを下回るサイズの物体（それでも衛星に衝突すれば大きなダメージとなる）の探知は困難であるため、「人間が利用する」宇宙空間の物体をすべて把握することは極めて難しい。したがって、「グローバル・コモンズ」としての宇宙空間を持続的に利用するためには、それを利用する主体がすべての情報を開示するとともに、地球軌道上を周回する物体を可能な限り多く探知することができる能力を、グローバルにもつことが必要となってくる。つまり、一言で言えば、「グローバル・コモンズ」である宇宙空間の、グローバルなガバナンスの仕組みが必要となっている。

１．軍事力の近代化と宇宙利用

冷戦後の世界では宇宙インフラの役割が格段に増大し、伝統的な通信、情報収集、測位の手段では代替できないほどの死活的な役割を担うようになっている。宇宙インフラを活用した、近代化された軍事力は 1990 年代の旧ユーゴ紛争におけるアメリカを中心とした NATO 軍の介入で、さらにその重要性への認識が高まった。アメリカ軍が旧ユーゴ紛争に介入したのは、国内世論の高まりに押された結果であった[2]。1990 年代の初頭にアメリカがソマリアに介入し、海兵隊員が殺害されて死体がテレビカメラの前にさらされた経験から、アメリカ政府は米兵の死傷者を出すことに対して極めてセンシティブであった。そのため、旧ユーゴ紛争では地上部隊を出さずに航空機による攻撃を主体とする作戦となり、新聞にも取り上げられるような「ピンポイント爆撃」や「ゼロカジュアリティー（死傷者ゼロ）作戦」といった概念が登場した。これらの作戦は偵察衛星による正確な敵地情報の入手、GPS やレーザーで誘導された爆撃、部隊間の緊密な通信など、近代化された軍隊が宇宙インフラを駆使して行うものであり、アメリカ以外の NATO 軍として参戦した国々は、こうした宇宙インフラを活用する能力（capability）が欠けていたため、アメリカ軍とともに作戦行動を取ること自体が困難であった[3]。

2000 年代に入ると、軍事力の近代化は「軍事上の革命（RMA: Revolution in Military Affairs）」と呼ばれ、IT 技術を積極的に導入した装備の調達を加速化させていった。そのなかで宇宙インフラは C4ISR（Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance）部門で死活的に重要な役割を果たすようになった。たとえば UAV を操縦し、そこから得られる画像・音声情報をリアルタイムで伝達するための衛星プログラムや、次世代電子光学衛星の開発など、新たな宇宙インフラの能力向上が進められている。

こうしたアメリカが中心となって進める軍事能力の近代化は、他の地域にも大きく影響

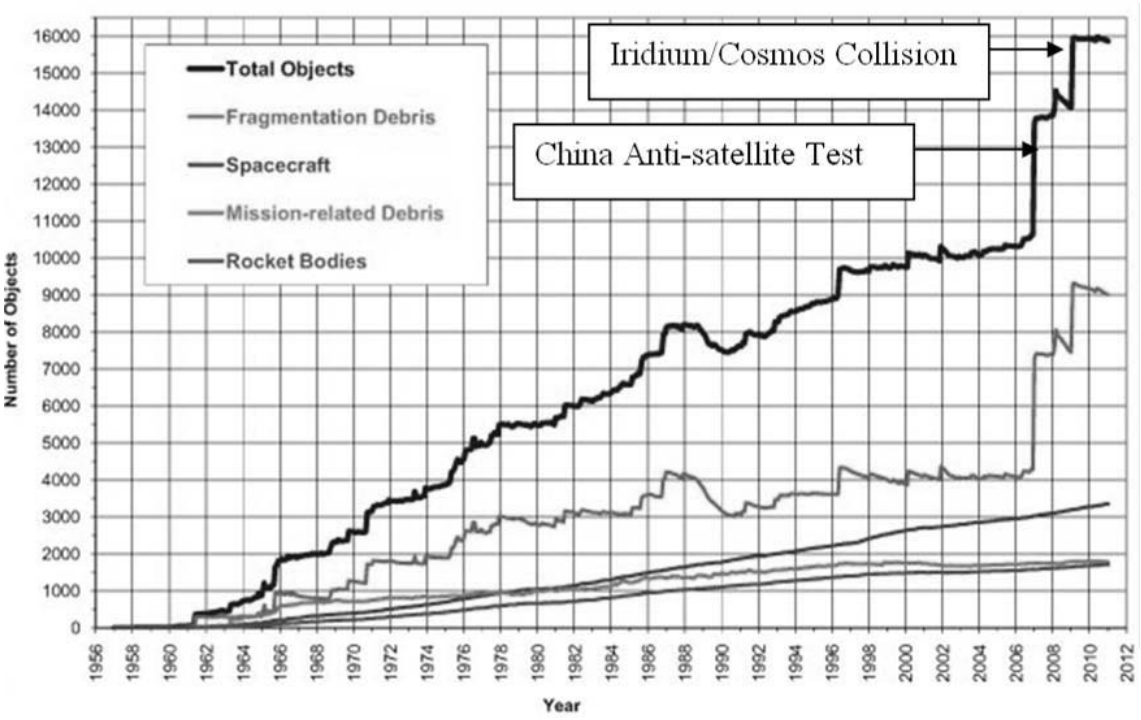
している。とりわけ、大きなインパクトを与えたのは中国と言えよう。1996 年の台湾総選挙に伴う台湾海峡の緊張の高まりにアメリカが介入したことをきっかけとして、中国の軍の近代化が急速に進んでいった。そのなかで、中国は宇宙インフラの拡充にも注力しており、通信衛星、偵察衛星はもちろんのこと、これまでアメリカの GPS の民間向け無料信号に依存していた測位システムも、アメリカとの関係悪化によってその信号を受けられなくなる可能性を懸念し、独自の測位衛星システムである「北斗（Beidou/Compass）」の開発を進め、2012 年には実用化している。

このように、冷戦後の軍事宇宙利用は、湾岸戦争をきっかけに軍の近代化が進み、それが世界的に波及することで、アメリカはもちろんのこと、ロシア、欧州、中国においても、宇宙インフラの軍事的重要性が飛躍的に増大した。これは、従前の地上系システムの補完という段階を超え、宇宙インフラなしには作戦行動を取ることが著しく困難となる段階に入ったと言える。このように、宇宙インフラが各国にとって死活的に重要なインフラとなることは、作戦領域の拡大という観点からみると、新たな局面に入ったことを意味する。それは、宇宙インフラが極めて脆弱な存在であり、その脆弱さにもかかわらず、宇宙インフラが死活的に重要になっているため、いかにしてその脆弱なインフラを保護するのか、という命題が生まれたということである。

２．宇宙空間の現状

その脆弱性を如実に示す事件となったのは、1997 年の中国による衛星破壊（Anti-Satellite: ASAT）実験であった。これにより、大量の宇宙デブリが発生し、軌道上にあるさまざまな衛星や国際宇宙ステーションなどの構造物にとって、極めて大きな脅威となった。中国（人民解放軍）は、自らの戦略的・政治的エゴによって衛星破壊実験を行ったことは間違いないが、それは巡り巡って、中国が利用する衛星にも影響しうるものであり、自分で自分の首を絞めるような行為となっている。さらに、2009 年にはアメリカの商業通信衛星であるイリジウム 33 号機とロシアのコスモス 2251 号機（退役済みだが軌道に残っていた）がシベリア上空の低軌道上で衝突し、衛星同士の衝突としては最初の、そして最大規模の事故が起こり、さらにデブリを大量発生させる事態を起こしている（図）。

図　確認されている軌道上物体の数



（出典：Nature ブログニュース
http://blogs.nature.com/news/2011/09/report_nasa_orbital_debris_off.html）

（１）デブリへの対処

このように大量発生したデブリは、現時点では回避するしか宇宙システムを守る方法はない。その際、重要になるのが宇宙状況監視（Space Situational Awareness: SSA）である。SSA とは、宇宙環境（太陽風などの宇宙気象や地球近傍小惑星＝Near Earth Objects: NEO の接近など）の理解と宇宙空間の人工物の追跡を通して、接近・衝突を監視することである。SSA によって各国は自らが運用する宇宙システムにどのようなリスクがあるのか、またそのリスクを回避するための手段はどのようなものになるのかを判断することができる。この SSA は、宇宙システムに大きく依存しているアメリカ軍が、自らの軍事宇宙システムを保護することを目的として提唱したものであり、宇宙監視ネットワーク（Space Surveillance Network: SSN）と呼ばれるレーダーや光学の監視局を世界各地に配置し、全天球を監視することを目指している。また、デブリを監視する衛星（Space Based Surveillance Satellites: SBSS）も打ち上げ始めており、デブリに関する情報を誰よりも多くもっている。とはいえ、アメリカの SSN は地域的な偏りがあり、とくに南半球でのカバレッジが低いため、2010 年にオーストラリアと協定を結び、監視局を置くことが決められた。しかし、そ

れでもまだ十分なカバレッジがないため、SSA の国際協力を進める方針を固めている。また、ロシアも宇宙監視の能力はもっているが、主としてロシア上空の状況しか監視するネットワークをもっていない。最近では、欧州でもフランスとドイツを中心に SSA の重要性への認識が高まっている。アメリカの SSN は 10cm 級のデブリまで監視する能力をもっており、活動中の衛星だけでなく、サイズの大きなデブリに関しては、それを把握し、カタログ化している。このカタログは軌道要素（Two-Line Element sets: TLE）と呼ばれ、一般に公開されているが、その精度は低く、かなりの誤差が出るため、TLE だけに依存してデブリを回避することは難しい。ちなみにアメリカ軍（正確には北米航空宇宙防衛司令部：NORAD）はより正確なカタログをもっており、関係国にデブリの接近情報などを提供しているが、これはあくまでもアメリカの自発的な行為であり、協定などに基づいた取り決めではないため、アメリカには通報義務があるとはみなされていない。

（２）軍事的合理性とグローバル・ガバナンスのジレンマ

では、なぜアメリカは正確なカタログをもっているにもかかわらず、それを公開しないのか。それはアメリカの運用する軍事衛星の情報が白日の下にさらされることとなり、アメリカの安全保障に支障をきたすと考えられているからである。軍事衛星の軌道が明らかになってしまえば、それを撃墜することも容易になるし、なによりも、偵察衛星が自国の上空を通過する時間帯がわかってしまえば、その時間だけカモフラージュを展開するなど、偽装工作が可能になるからである。また、デブリの軌道計算は膨大な人員とコンピューター能力が必要とされるため、NORAD は国際宇宙ステーション、スペース・シャトル、アメリカの軍事衛星システムの 3 つに接近するデブリの計算を最優先にしており、それ以外の物体については、監視をしていても軌道計算までしていないという状況にある。これがイリジウム衛星とコスモス衛星の衝突につながったとして、NORAD においても、監視と軌道計算の対象を広げる方向で修正が加えられていると伝えられているが、それがどの範囲まで広がるのかは定かではない[4]。

なお、日本も岡山県の上齋原（かみさいばら）町にレーダー観測施設、同じく岡山県の美星（びせい）町に光学観測施設をもっているが、主として NEO の観測が目的であり、宇宙航空研究開発機構（JAXA）ではなく NPO 法人の日本スペースガード協会という国立天文台と関係の深い団体が運営主体となっている[5]。米欧においては宇宙システムを保護するということから、軍や宇宙機関が主体となっているのとは大きく異なっているが、それは、日本における宇宙開発が技術開発を中心としており、それを「社会インフラ」として使うという発想が乏しかったため「守るべき対象」として宇宙システムを認識してこなかっ

たからに他ならない。こうしたグローバル・コモンズとしての宇宙空間のガバナンスを考える上で、日本の宇宙開発が他の国々と異なる発展をしてきたことで、ガバナンス体制の構築に関与できていないことは興味深い点である。

３．宇宙ガバナンスの枠組み

では、いかにして安全保障上の目的で衛星を破壊するような行為を止めることはできるのであろうか。一般的に対衛星（ASAT）攻撃は、移動性宇宙物体（キラー衛星）、宇宙地雷、地上配備のミサイルなどによって衛星を物理的に破壊するというもののほか、指向性エネルギー兵器や地上からのレーザー攻撃、ジャミング、衛星センサーの目くらましなど、さまざまな方法で衛星の能力を奪い、その機能を停止させることを目的としている[6]。これらの攻撃は必ずしもデブリを生み出すものばかりではないが、いずれにしても、有事の際に衛星を破壊することが技術的に可能であることを示唆している。

こうしたASATは、現時点では国際法上、違法とされていない。宇宙空間のガバナンスの基礎となる宇宙条約では、月などの天体における軍事的な活動は否定されているが、宇宙空間（軌道上）には大量破壊兵器を配置することは禁じられていても、通常兵器を配置することは禁じられていないためである。また、地球上から宇宙空間に向かって攻撃を行うことも、宇宙条約では直接言及されていないが、宇宙システムにはその運用主体の主権が宇宙空間にも及ぶため、他国による宇宙システムに対する攻撃は自国の主権に対する侵害として認めることができる。つまり、他国によってASATが行われた場合、自衛権を発動することができる、という解釈となる[7]。しかし、これもASATを抑止する効果は一定程度あるとしても、ASAT そのものを禁止するということではないため、たとえばかつて米ソが行い、2007年に中国が行ったように、自国の衛星を破壊することは違法にはならない。

（１）中ロ提案の条約案

このような状況に対して、近年に入り、法的規制をかけるような動きがみられるようになっている。国連の軍縮会議（Conference on Disarmament: CD）では、「宇宙空間における軍備競争の防止（Prevention of an Arms Race in Outer Space: PAROS）」と呼ばれるアドホック委員会が設置されており、1980年代から宇宙空間の軍事利用に関する議論がなされてきた。ここで最初に宇宙空間の非軍事化を目指す条約案を提出したのは、実は中国である。中国はPAROSにおいて、2000年に「宇宙空間における軍備競争防止問題に関する中国の立場と提案」、2001 年には「宇宙空間における兵器化（Weaponization）防止条約の要点に関する構想」を提出した。また、ロシアとともに2002年に、「宇宙空間への兵器配備およ

び宇宙空間物体に対する武力による威嚇または武力の行使防止に関する将来の国際協定のための要素」と題する作業文書を提出している[8]。これらの文書では、通常兵器も含めた兵器を宇宙空間および天体上に配備せず、宇宙空間の物体に対して武力行使・武力による威嚇はしないことが提案された。これらに基づき、2008 年に「宇宙空間への兵器配置および宇宙空間物体に対する武力による威嚇または武力の行使の防止に関する条約（Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects Treaty: PPWT）」案を国連軍縮会議に提出した。2007 年の中国による衛星破壊実験の直後に提出されたこともあり、この PPWT は国際的な注目を集めたが、中国はこれまでも軍縮会議において宇宙の兵器化を禁ずる提案を行っており、その意味では PPWT が唐突に出されたわけでも、中国の立場を正当化するために出されたわけでもない。ただ、この条約案をみてみると、中国の立場を否定するものでもないことは明らかである。というのも PPWT では、ASAT 兵器を「宇宙空間に配備する」ことを禁ずるものであり、地球上からの攻撃を禁じているわけではない。そのため、仮に PPWT が成立した場合でも、大量のデブリを発生させる衛星破壊攻撃を阻止することはできない。さらに、PPWT では自衛権の行使としての ASAT を否定しているわけではないため、地球上での紛争の延長として衛星破壊を行う可能性はある。

さらに大きな問題は「宇宙空間における兵器」とは何か、という定義の問題である。他国の宇宙システムの機能を奪うことを目的とするのであれば、兵器でなくてもデブリを衛星に衝突させるだけでその目的は達成される。そのため、民生目的と偽って衛星を操作し、他国の衛星に衝突させることも可能であり、いかなる人工物も兵器となり得るのである。PPWT では宇宙空間における兵器を「いかなる物理的原理に基づくものであれ、宇宙空間、地球上、および地球大気圏内の物体の通常の機能を破壊し、損害を与え、または妨害するために、もしくは人間あるいは人間の生存に不可欠な生物圏の構成要素を壊滅させ、または損害を与えるために、特別に製造または転換され、宇宙空間に配置された（place）あらゆる装置[9]」と定義しているが、この定義から民生目的の衛星は排除されるため、形式的な要件で宇宙の兵器化を防ぐことはできないと考えられる[10]。

（２）EU 提案の「宇宙の行動規範」

中国とロシアの PPWT が条約という強制力をもつ「ハードロー」であるのに対し、EU は「行動規範（Code of Conduct）」と呼ばれる提案を行い、「ソフトロー」による宇宙の兵器化を制限するという方向を模索している。2007 年の中国による衛星破壊とデブリの大量発生を受け、当時国連宇宙空間平和利用委員会（UNCOPUOS）の議長であったブラシェ

（Gérard Brachet）が宇宙活動の長期持続性（Long-term Sustainability）を提唱し、自らが主導したデブリ低減ガイドラインの策定をモデルに、宇宙空間における「行動規則（Rule of the Road）」を 2013 年までに策定するという提案を行った。これを踏まえ、宇宙の兵器化に関する議論に関しても言及することを求めたが、UNCOPUOS は平和利用の問題に限定され、安全保障にかかわる議論は行わないことが原則になっていることもあり、ブラシェ議長のイニシアチブを受けたフランスと、それに同調する国々が EU としての提案として、国連軍縮会議に問題提起をすることとなった。2007 年には国連第 1 委員会で EU の議長国であったポルトガルが「行動規範」の概略を説明し[11]、2008 年にフランスが主導する形で EU 加盟国間の意見の調整が行われ、2008 年末に EU の閣僚理事会で採択され、現在、この行動規範に賛同する国を集め、事実上の（de facto）宇宙活動ルールとして定着させる努力が続けられている。

４．日本の宇宙開発と安全保障

（１）「宇宙の平和利用原則」による制約

日本は長期にわたって「宇宙の平和利用原則」を堅持し、宇宙開発と安全保障を切り離して考えてきた。1969 年の国会決議で、日本の宇宙開発は「平和の目的に限り」行うことが定められ、その「平和の目的」が意味するところは、原子力の平和利用から類推される形で、防衛省・自衛隊が宇宙システムを開発・保有・運用・利用しない、ということを意味していた。しかし、宇宙システムは気象予報や衛星放送のように一般にも利用されるものであることから、1985 年に「一般化原則」が定められ、防衛省・自衛隊が商業的に利用可能な宇宙システムないしはそれと同等の機能をもつものを「利用」することは認められたが、それでも開発・保有・運用は認められなかった。

それが大きく変わる可能性があったのは、1998 年の北朝鮮によるテポドンの発射と、それが日本列島を超えて太平洋に着水した事件であった。これをきっかけに日本も北朝鮮をはじめとする近隣諸国の軍事的な活動を監視する必要性が認められ、情報収集衛星が開発されることになったが、「宇宙の平和利用原則」が存在しているため、防衛省・自衛隊が衛星を保有し、運用することは認められなかった。そのため、情報収集衛星は内閣官房の内閣情報調査室に「内閣衛星情報センター」を創設し、内閣官房の予算で開発・保有・運用するという仕組みになった。

しかし、この仕組みはかなりいびつな制度運用を迫られ、日本の安全保障における実効的な仕組みとは言い難かった。このような経験から、2008 年に成立した宇宙基本法では「国際社会の平和及び安全の確保並びに我が国の安全保障に資する」宇宙開発を行うことが定

められ、1969 年の「宇宙の平和利用原則」の解釈に縛られることはなくなった。また、宇宙基本法では、安全保障を狭義の軍事的手段による領土防衛にとどめることなく、「国民生活の向上、安全で安心して暮らせる社会の形成、災害、貧困その他の人間の生存及び生活に対する様々な脅威の除去」といった国民の生命・財産を守るという広義の安全保障の概念も取り入れている。

（２）安全保障利用の低迷の原因

しかしながら、日本の安全保障目的の宇宙利用は宇宙基本法が成立してからもあまり進んでいない。すでに自衛隊がアデン湾の海賊対処や国連 PKO に派遣されるなど、遠方に展開するようになったことをうけて、防衛省はこれまで使っていた商用衛星による通信を代替する、新たな防衛専用通信衛星を PFI 方式で発注することとなった。これは、防衛省が自ら衛星を開発し、運用するのではなく、あくまでも利用者として使うという位置付けのものである。また、偵察衛星については、すでに情報収集衛星が稼働していることもあり、防衛省としては独自に開発、運用する予定はない。

こうした消極的とも言える防衛省の対応の背景にはいくつかの理由があるだろう。ひとつは長い間「平和利用原則」に拘束され、宇宙開発利用が制限されてきたため、宇宙インフラが無い状態で作戦行動を検討するという思考が定着していることが考えられる。これまでのやり方を大きく変えるコストを考えれば、宇宙インフラを導入して新たな体制を作ることに消極的になるのも無理はないであろう。また、宇宙開発利用に関与してこなかった結果、宇宙技術に対するノウハウや理解が十分でないことも考えられる。さらに、限られた予算のなかで、新たに宇宙への投資を進めることは既存のプログラムに対する圧迫にもなるため、積極的になりにくいであろう。このように、日本は宇宙の軍事的重要性が増してきたとしても、宇宙インフラの開発、保有、運用、利用に対して必ずしも積極的にならないという状況にある。

（３）日米同盟の重要性

しかし、そのなかで近年重要性を増しているのは、宇宙空間の安全保障における日本の役割である。SSA を実施するためには、地球のあらゆる地点から宇宙空間を監視する必要があり、国際的な協力体制が不可欠であるが、現在、東アジア地域における SSA のネットワークは不十分である。すでに論じたように、これまではシビリアンの機関である JAXA やスペースガード協会が日本での SSA を担ってきたが、SSA ネットワークを担う各国軍との情報共有は困難である。そのため、2013 年度から防衛省がミサイル防衛用のレーダーで

ある FPS5 を活用してデブリ観測を行うこととなった。しかし、SSA のグローバルなカバレッジ構築を急ぐアメリカは 2013 年 10 月の 2＋2（日米外務・防衛閣僚会議）で、防衛省の能力構築を待たずに JAXA による SSA 情報提供を求め、日本側もそれを了承した[12]。シビリアンの機関が SSA 情報を提供するのは例外的措置ではあるが、グローバル・ガバナンス体制を構築するなかで、日米同盟が効果的な役割を果たす上で、そうした例外的な措置を取ってでも、SSA 構築を進めることが重要と判断した結果とみるべきであろう。

また、日米同盟は EU が提案した「宇宙の行動規範」を巡る国際ルール作りにおいても重要な役割を果たしている。当初、EU がこの行動規範を提唱した際、多くの国、とりわけ途上国から、EU が決定したルールを強制するのは「宇宙における植民地主義」の発露だとして強い反発があった。アメリカは、ブッシュ政権時代には宇宙活動を制限する国際的取り決めには全面的に反対してきたが、オバマ政権では「合衆国は安全で責任ある宇宙での活動を推進する国内・国際措置、宇宙物体の衝突回避の情報収集・共有の改善、死活的な宇宙システムの保護、軌道上のデブリ低減措置の強化を通じた宇宙の安定性の強化を目指す[13]」と、まったく異なる姿勢をみせるようになった。そこにすかさず日本とオーストラリアが協力姿勢をみせ、EU が提案した「宇宙の行動規範」をたたき台としながらも、国際的に開放されたフォーラムで議論を再開し、EU のものとは異なる「宇宙の国際行動規範」を構築するという方向性を打ち出すことに成功した。このフォーラムには 60 ヵ国近くが参加し、2013 年 5 月にキエフで、11 月にバンコクで開催され、2014 年内に最終的な取りまとめがなされる予定である。日本とアメリカは、EU、豪州とともに議長支援グループ（Friends of Chair（議長は EU））を構成し、「宇宙の国際行動規範」策定の中核をなし、議論をリードしている。

このように、新しい宇宙ガバナンスの構築に向けて、日米が協調して活動することで、国際ルール作りの中心が形成され、宇宙空間の持続的利用可能性の向上に資する役割を担っている。これは一方で 2007 年に ASAT 実験を行った中国や、中国と共に PPWT を提唱するロシアを国際ルール作りの周辺に配置することとなり、より軍事的重要性を増した宇宙空間の利用に関する国際社会の規範作りにおける影響力を巡る競争にも強い影響を与えている。今後、グローバル・コモンズである宇宙空間を利用し、そこから社会経済的な利益を享受し、安全保障上のシステムを安心して運用できるようにするためには、このグローバル・コモンズを管理するガバナンス構築における影響力競争において有利な立場にいることが重要である。それによって宇宙利用の主導権を握るだけでなく、広く社会経済的、安全保障上の利益も確保することになるからである。そのためにも、日米同盟が有効に機能し、自らの利益に即したルール作りを進めている現状を継続していくことが重要である。

むすび

最後に、今後のグローバル・コモンズとしての宇宙ガバナンスに対する課題を論じておこう。第 1 は、技術革新による環境の変化である。これまでは宇宙空間へのアクセスの困難さとコストから、寿命の長い衛星で多機能な衛星、すなわち大型衛星を打ち上げることに合理性があり、そのサイズは年を追うごとに大型化していった。しかし、大型衛星に多くの機能を搭載することは、デブリに衝突し、衛星が機能を失ったときのリスクが大きくなることも意味する。そのため、大型衛星の技術開発が継続される一方、小型衛星に機能を分散させ、より多くの頻度で打ち上げることによってリスクを分散させるという方向性が出てきている。こうした衛星の小型化は軌道上の物体が増加し、軌道がいっそう混雑することも意味している。こうしたなかで衛星同士の衝突を回避するためにも、SSA 体制の構築と情報共有の仕組みの構築がより重要となる。

第 2 に、衛星の小型化に伴い、技術がより単純化し、陳腐化していくという傾向がみられる。これはこれまで高い技術をもつ国のみがもち得た宇宙利用の可能性を、より技術力の低い国にも広げることとなり、大学レベルでも衛星の開発・運用が可能になることを意味する。それはすなわち、これまでの少数によって構成される「宇宙クラブ」のルールである「宇宙の国際行動規範」を、新規参入してくる多くの主体に認知させ、宇宙空間のガバナンスを徹底することを必要とする。しかし、そうした役割を誰が担うのか、また、法的拘束力のない「行動規範」で十分なのか、といった問題が提起される。

第 3 に、宇宙空間における兵器化の進展が挙げられる。2007 年の中国による ASAT 実験は物理的な破壊を伴うものであり、それによって多数のデブリが発生し、中国も含めた宇宙利用国すべてに不利益になることが明らかになった。したがって、今後、こうした物理的な破壊へのインセンティブは下がるだろう。しかし、すでに述べたように ASAT の手法は物理的な攻撃に限定されない。ジャミングや電子的な攻撃、さらには自然現象としての太陽風による障害といった問題もある。これらの攻撃や自然現象によって衛星の機能が停止したとしても、それがどのような原因で行われ、誰にその行為の責任が帰するのか、といった判定をすることは極めて難しい。衛星自身の故障による不具合という可能性も常に残る。

これらの問題についての解決はまだ明らかになってはいない。しかし、これらの問題に対処するためにも、国際的なルール作りと、SSA による宇宙状況の把握は極めて重要であり、これらを実現するためには強固な日米同盟を軸にしつつ、グローバル・ガバナンスの構築に向けた各国との協力が不可欠となるのである。

－注－

1 グローバル・コモンズに関する議論は近年急速に増えているが、さしあたり Abraham M. Denmark and James Mulvenon (eds.), *Contested Commons: The Future of American Power in a Multipolar World*, Center for a New American Security, January 2010 がよくまとまっている。

2 高木徹『戦争広告代理店 ： 情報操作とボスニア紛争』講談社、2002 年。

3 その結果、コソボ紛争後には欧州の能力向上（capability improvement）に関する動きが加速化し、欧州防衛機関（EDA）が設立されるなど、軍事技術開発や軍事調達の側面で大きな変化を生み出した。拙稿「欧州共同防衛調達と戦略産業政策」『新しい米欧関係と日本』国際問題研究所、2004 年 3 月、87-110 ページ参照。

4 Michael A. Earl, The Iridium 33 - Cosmos 2251 Collision: Creating Liability Awareness for Space Property / Contemplating the Future of Space Surveillance, Canadian Satellite Tracking and Orbit Research. May 2009

5 日本スペースガードに関しては http://www.spaceguard.or.jp/ja/index.html を参照。

6 Laura Grego, ―A History of Anti-Satellite (ASAT) Programs, Union of Concerned Scientists, October 20, 2003（http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/a-history-of-anti-satellite.html）

7 この点に関しては、青木、前掲書、第四章を参照。

8 日本国際問題研究所軍縮・不拡散促進センター『宇宙空間における軍備管理問題』（平成 19 年度外務省委託調査）2008 年 3 月。

9 この訳は佐藤雅彦・戸﨑洋史「宇宙の軍備管理、透明性・信頼醸成向上に関する既存の提案」日本国際問題研究所　軍縮・不拡散促進センター『新たな宇宙環境と軍備管理を含めた宇宙利用の規制――新たなアプローチと枠組みの可能性――』（平成 21 年度外務省委託研究）2010 年 3 月、85 ページに従った。

10 Wolfgang Rathgeber and Nina-Louisa Remuss, Space Security: A Formative Role and Principled Identity for Europe, *ESPI Report*, no.16, January 2009

11 Transparency and Confidence-building Measures in Outer Space Activities, A/62/114/Add.1, 17 September 2007

12 日米安全保障協議委員会共同発表「より力強い同盟とより大きな責任の共有に向けて」2013 年 10 月 3 日（www.mofa.go.jp/mofaj/files/000016027.pdf）

13 White House, National Space Policy of the United States of America, 28 June 2010

第６章　北極海と日米同盟

金田　秀昭

はじめに

近年、地球温暖化の影響を受けて、夏季においては北極海の万年氷が融氷するという変化が生じ、砕氷能力の無い船舶の航行が可能となった。この結果、北極海に関しては、欧州とアジアを短距離で結ぶ国際的な海上交通路としての利用や､海洋･海底資源の開発などに展望が開けることとなった。一方、北極海の急激な変容に起因する安全保障・防衛面への影響も見逃せなくなっている。早くも、米国、ロシア、カナダといった北極圏諸国が、北極海を巡る安全保障上の問題に関して敏感になっているのに加え、海洋への侵出傾向の著しい中国などの諸国が、北極海を巡って安全保障面でのつば迫り合いを始めている。

こういった状況を目の当たりにして、日本の官民も遅ればせながら北極海への関心を強め始めたが、その視点は、未だ海運や資源開発といった側面が主となっており、安全保障・防衛面での関心は未だ低調である。折しも安倍政権下、2013 年末に国家安全保障会議（JNSC）が創設され、JNSC により初となる国家安全保障戦略を始め、見直しを進めていた防衛計画の大綱や中期防衛力整備計画が採択、承認された。2014 年夏には、集団的自衛権の行使等に関する憲法解釈の変更、政策の転換も行われ、2014 年末には日米防衛協力指針が改定される運びとなっている。本稿では、こういった国内外の変化を捉えつつ、北極海変容の及ぼす安全保障・防衛面での影響を分析し、今後の北極海を巡る日米同盟のあり方を中心として提言する。

１．北極海変容の安全保障・防衛面の影響

北極海変容の安全保障・防衛面での影響を分析するに際しては、北極海の自然環境的な変化といった比較的進展の緩やかな現象と、北極圏諸国や関係国の安全保障・防衛上の関心の変化という比較的反応の速やかな事象を同時に捉えていくという異なった側面があるため、短期、中期、長期に分けて考察することが適当であり、本稿ではこの視点で考察を進める。

短期的には、新たに国際的に重要な海上交通路が誕生しつつあるということである。この面に関しては、未だ商業用航路としては本格的な段階にはないが、既に北極圏諸国や関係国において、開発、利用が進むようになり、現実に商業目的の海上輸送も行われ始めており、北極海域の経済面での利用という点に、国際的な関心が高まりを見せるようになっ

てきた。

中、長期的には、北極海での北極圏諸国や関係国間の資源獲得競争が激化すると予測され、今後の資源開発の成り行きによっては、欧亜の新規参入国が開発競争に殺到する可能性も生じよう。また大西洋と太平洋を最短距離で結ぶ新たな海上交通路の開設という事実は、単に経済面での影響だけではなく、グローバルな安全保障・防衛問題に関心を持つ国にとっては、戦略的な機動展開能力に係わる重大な変化を意味することになる。またこれに関連して、米国やロシアの拡大核抑止力の信頼性の低下や、日本周辺海域を含む北極海周辺海域や航路での、多様な安全保障課題が生起することが危惧される。こうしたことから、北極海を巡る安全保障上の視点も含めた新たな国際ルールを設定する必要性が生じている。

長期的には、北極海自身や、地球規模での環境変化の悪影響に拍車が掛かる懸念があり、この問題に対する国際的枠組み作りが求められる。

（１）新たな国際的海上交通路の誕生の及ぼす影響

新たに国際的に重要な海上交通路が誕生するという点については、既に、北極圏諸国のみならず、日本を含む欧亜の関係国が強い関心を示している。近年、これら諸国には、北極海の北東航路（ロシア沿岸)、北西航路（カナダ沿岸)、中央航路の利用への強い期待を背景として、未だ本格的とはいかないまでも、既にその航行実績も増加しつつある。とりわけ中国や韓国に加え、インドやシンガポールなどの新興海洋国家が積極姿勢を示していることが特徴的であり、そのことにより本問題は、必然的に資源開発問題へと繋がり、行き着くところは安全保障・防衛問題と関連付けられる傾向にある。

しかし現状では、北極海の海上交通路としての利用は、通年とはいかず夏季に限定されている。これに加え、北極圏諸国による国内法の適用や通航料の賦課（北東航路でのロシア）や自国内水との宣言（北西航路でのカナダ）といった形で通航には何らかの制約や制限があり、恒常的な利用には不確実性がある。その上、北極海は従来「万年氷に閉ざされた海」として広く認識され、学術目的以外には、海上交通路としての利用や、冷戦さなかの米ソ戦略原潜の活動以外では軍事作戦の舞台として顧みられることはほとんどなかったため、そもそも北極海の利用やルールに関する国際条約や協定が存在せず、現実に経済的に成り立つ海上交通路として、あるいは軍事目的での利用に関しては、容易には解決できない課題が山積しているのが実情である。

（２）北極海を舞台とする軍事面のつば迫り合い

北極海を舞台とする軍事面でのつば迫り合いを見てみると、一つには北極圏諸国間の領土確定問題が背景となっており、従来は具体的な政治的対立には至らなかったケースでも、現実に国家主権や領域確定問題として認識されるようになったという側面がある。それ以上に、今後深刻化すると思われる問題は、米露間の戦略核抑止態勢への影響であり、今後は、中国が本問題に参入する可能性があることである。

北極圏諸国の中でもロシアは、北極海航路の利用確保、北極圏での国益確保のための北極圏国境警備機能の統合のため、北極軍の創設や基地の新設など、軍事的な関心を増大させつつある。冷戦終結以降中断していた北極圏での監視哨戒飛行を再開し、原子力潜水艦の行動も活発化させるとともに、新たに北極旅団を新設し、砕氷艦船の増強にも着手した。2013 年には、北極海にあるノボシビルスク諸島付近で水上機動部隊が演習を実施し、20 年ぶりで同諸島の陸上基地の整備にも着手している。また米国が、核抑止力強化の一環として、バレンツ海など北極圏にもイージス艦を配備するなど、今後弾道ミサイル防衛（BMD）機能を高めていく可能性があると見て、機先を制する形で、欧州への BMD 機能強化（EPAA）に対すると同様に、北極海についても反対の意図を強く表明する一方、2013 年には新型戦略原潜を北洋艦隊に配備した。また最近では、中国の砕氷船「雪龍」が、宗谷海峡を経由して、ロシアにとっての軍事上の聖域であるオホーツク海ルートを利用し、さらにロシアの管轄外となる北極海の中央航路を航行するなどの動きを見せていることに対しても、強い警戒心を持って敏感な反応を見せるようになった。

カナダは、ロシアとは異質ではあるが、同様に高い軍事的関心を示しており、北極圏での哨戒、迎撃、輸送、救難行動に適応する航空機や無人航空ビークル（UAV）兵力の整備を進めている。また砕氷能力を持った哨戒艦艇等の更新を進めているほか、局地陸軍の能力も増強中である。

米国は、今までのところ、露加両国に比べれば、北極海での軍事的関心は高くないように見受けられるが、遅ればせながら、海軍を中心に北極海への安全保障・防衛面での関心を増大させており、2013 年 11 月には、国防省が北極戦略（Arctic Strategy）を発表し、「敵意をもった存在の侵入」に備え、海洋での探知・追尾能力の向上を図るとともに、北極圏の安全保障に関して、長期的な視点をもって関係国と連携する必要性を強調している。海軍は、2014 年中を目処に、ロードマップの策定に取り掛かっており、その結果に注目が集まっている。

欧州諸国の中では、ノルウェーの関心が最も高く、軍全体としての北極海での行動を意識した軍備の改善が図られており、ロシアとの連携の強化が図られている。スウェーデン

はグリペン戦闘偵察機や潜水艦など、海空軍を中心に北極行動を意識した軍備の拡充を図っている。またデンマークは、グリーンランドに、北極任務部隊を新編し、F-16 戦闘機の配備を開始した。

（３）北極海での資源獲得競争の激化

北極海には、世界の未発見天然ガスの 30%、石油の 13%が存在すると見られており、その大部分がロシアの管轄領内の浅海域に集中しているが、ロシアの現有する技術力での開発は難点があり、ノルウェーなどとの提携を模索している。しかし、計画策定や税制問題など未解決の問題が多く、開発計画は後ろ倒しの状況となっている。

北極圏諸国は、北極海の資源に関して大幅な主権的権限を主張し、開発に注力する姿勢を強めている。取り分けロシアは、北極海の大陸棚での資源開発と関連させた形で、シベリアでの陸上交通網の開発、ロシア～アラスカ間の大陸間トンネルの開設までも視野に入れている。

中国、韓国、インドなどは、北極海の資源に狙いを定めつつある。特に顕著なのは中国であり、近年は、北極評議会の加盟国への接近をあからさまにし始め、2012 年には、温家宝首相（当時）がスウェーデンおよびアイスランドを、胡錦濤中国国家主席（当時）がデンマークを訪問、2013 年 12 月には、北欧 5 ヵ国の北極研究機構との間で、「中国－北欧北極研究センター」を上海に設置することで合意した。中国は特にアイスランドに関心を強めており、同国のレイキャビックに大使館を設置するなど、同市港湾を、中国が独占的に利用し得る北極海運のハブ港として位置づけ､その開発を期しているのではないかとして、他の関係国からの反発を買っている。また中国はこの戦略の一環として、前述したように夏季の融氷期には、砕氷船「雪龍」を北極海に周航させ、レイキャビク港にも寄港させている。

（４）戦略的な機動展開能力の変化

北極海ルートを利用することが可能となった場合の、軍事面に及ぼす影響は多種多様であるが、中でも、欧州とアジアを結ぶ戦略的な機動展開能力の改善は顕著となる。海運業的視点から、オランダのロッテルダムから釜山までの航海日数を計算すると、北極海を経由する場合と、スエズ運河を利用する場合とでは、距離にして約30%（苫小牧では約40%、横浜では約34%）削減できるとの試算がある。この数字は海上運行日数という点からは、大きな差となり、海運業的に経済的な効果をもたらすことが期待できるが、それ以上に軍事戦略的に見れば、圧倒的なメリットが生まれることとなる。

このことはグローバルな戦略環境に革新的な変化を与えることとなる。まずはNATOの関心領域が増大し、北極海への常続的なプレゼンスを示す傾向が生じる。米国単独で考えれば、大西洋と太平洋を連結する海上戦略機動能力の改善が顕著となり、また北極海を基盤とするパワープロジェクションが可能となる。これらの変化により、北極地域を担当する地域軍の性格にも変化が生じるであろう。特段の担当の無かった北極海地域担当軍の区分は、カナダ側が北方軍、ロシア側が欧州軍と分割されることとなり、実兵力を持たない北方軍に太平洋軍が兵力を提供するという形を取る可能性があり得る。仮にそうなった場合には、アジア・太平洋における軍事バランスに少なからぬ影響を与え、日本の負担が増大することとなろう。

何れにせよ、従来の地政学や軍事戦略では、全く顧みられることがないか、ほとんど慮外とされていた北極海を取り込んだ形での海洋軍事戦略の構築が、北極圏諸国や関係国に必要となってくる。

（５）米国拡大核抑止力の信頼性の低下

北極海の変容がもたらす軍事面でのもう一つの大きな影響は、米国の拡大核抑止力の信頼性の低下の可能性が生じるということである。まずは、間違いなくロシアの戦略原潜の活動期間や哨戒範囲が拡大する。一方、米国の戦略原潜や攻撃型原潜の活動期間や哨戒範囲の拡大も同時に生じ得るわけであるが、米国の戦略原潜や攻撃型原潜の活動に対するロシアの攻撃型原潜の活動期間や哨戒範囲の拡大もあり得る。一般に、原潜の性能面では、米国がロシアに勝っているが､対潜兵力の展開を含め地の利を得ているのはロシアであり、このことは、米原潜の行動制約という意味ではロシアに有利に作用するであろう。

これに加え、中、長期的視点で見れば、そう遠く無い将来、中国の戦略原潜の哨戒（晋級またはポスト晋級戦略原潜）や攻撃型原潜（商級またはポスト商級原潜）が展開することも想定しておかねばならない。冷戦中を最盛期として、米ソの戦略原潜の哨戒活動やそれを常時追従する攻撃型原潜の活動に関して、平素からの息詰まるようなつば迫り合いが行われてきたのは周知のとおりである。現代においても、この点に関する米露の関係は、基本的には不変であると思われる。これに加え、中国がその戦略原潜に搭載する弾道ミサイルの開発に最終的に成功して、実戦化が可能となれば、その実用射程によっては、北極海での中国戦略原潜の哨戒活動が、日常的に行われるようになっても不思議では無い。

いずれにせよ、今後の米中露間の戦略原潜による戦略核第2撃力の推移によっては、北極海の変容に起因した米国の核抑止能力の低下が起こり得る可能性が生じる。こういったことも踏まえ、米国は宇宙、空中、陸上、海上配備型のBMD網の展開を強化すると思わ

れるが、このことは日本にとって他人事ではなく、米国の核拡大抑止力に大きく依存する日本にとって、今後は、北極海での戦略原潜の展開を巡って生じ得る各種の軍事問題への強い関心を払うとともに、この点に関する米国へのなし得る限りの協力が必要となることを銘記しなければならない。

（６）周辺海域での多様な安全保障課題の生起

北極海の変容に起因し、北極海には直接の関係は無くとも、周辺海域において多様な安全保障問題が生起する可能性があることも重要な点である。北極海での航路利用が増加すれば、北極海に連接する周辺海域の航路も輻輳することは当然の結果として起こる。日本周辺で考えても、日本海やその出入り口となる３海峡（宗谷、津軽、対馬）が輻輳化する。これに加えて、ロシアの東シベリアにおける原油や天然ガスの開発と日本などへの海上供給路の設定が軌道に乗れば、日本海を経由したエネルギーの重要な海上交通路が現出したこととなり、ますます、日本海や３海峡における海上交通が輻輳化する。同時に日本のみならず、中国や韓国（北朝鮮）による利用も増加することとなり、輻輳化した日本海や 3 海峡において、海上保安や安全保障面での問題が生起する可能性が高まるものと考えられよう。

また、北極海や北方海域での海上交通が輻輳化すれば、捜索救難、人道支援、災害救援といった面が新たに地域の課題となり、北極圏諸国や周辺国は、それらに対する新たな国際的責任を負うこととなる。日本は、こういった点での貢献を目に見える形で適切に行うことにより、今後の北極海利用に関する国際的協議を有利に進めるカードを持ち得ると認識すべきである。となれば、同方面での緊急事態や有事に備え、北極海や北方海域での活動をも念頭に置いた艦船・航空機などの防衛装備品の開発や取得などが、今後の具体的な課題となってくるであろう。

（７）北極海を巡る新国際ルール設定の必要性

現状では、北極海の航行、資源開発といった経済的側面のみならず、安全保障・防衛面での国際的ルールが確立されているとはいえない。現行の海洋法条約や国際的な航行に関する各種の国際合意や、南極の平和的な利用についての国際合意に基づく南極条約などは存在するが、北極に関してはほぼ存在しないといってよい。確かに北極評議会が存在し、グループ内での幾つかの取極めは存在するが､少なくとも現状における同評議会の性格は、北極海の利用などに関する寡占的な協議体であり、北極圏諸国としての既得権の維持を第一に置いており、国際的に見て、全ての国に開かれた公平な組織体として機能することを

期待することは、当面困難と見ざるを得ない。

そういう意味からは、北極条約の新規制定や国連海洋法条約の改定を念頭に置いた国際的に開かれた公正な議論が必要となるが、そういう点での国際的なコンセンサス作りの機運は目下現れていない。現状では北極評議会にそれを期待することは望み薄であるとすれば、国際政治、経済産業、国際海運、安全保障・防衛という観点から、日本の安定的な地位を確保するためにも、日本が主導的な位置を確保しつつ国際ルール確立のための議論を展開していくことが必要となるが、そのための日本にとっての現実的な選択は、同盟国米国との提携である。北極評議会の有力な加盟国である米国との協議を密にし、両国間の安全保障・防衛面の利害関係を調整した上で、米国を通じて、北極評議会での議論を有利に進めていくことが、当面の日本にとっての選択肢となろう。しかし、米国は国連海洋法条約を批准していないという弱点がある。南シナ海での「航行の自由」問題に関連して、米国内でも同条約批准の動きが強まってきたことは日本にとっても好ましいことであり、日本としては、この意味からも米国に同条約の速やかな批准を促した上で、当面は、北極評議会の有力メンバーである米国を直接､間接に強力に支援する形をとることが､日本にとって最善の選択となるものと考える。

（８）環境変化の悪影響に拍車の懸念

長期的課題として、北極海の変容が環境に及ぼす影響を無視することはもはやできない。北極海航路の輻輳や資源開発競争の激化による環境悪化への懸念を共有し、国際的に何らかの持続可能で有効な対策を採らねばならない。北極海の利用は、如何なる形態にせよ温暖化をますます助長するものと思われ、生態系への悪影響は避けて通れない。このため環境悪化に備えた新たなルール作りが望まれることになる。例えば、航行の資格として北極海仕様の船舶や航空機に限定し、運用者には氷洋運行資格等の取得を義務付けることが求められることとなろう。この点に関しては、軍艦・軍用機、公船や公用機も含むことも検討材料となろう。さらに言えば、艦船用燃料の使用制限までも視野に入れる必要が生じる可能性もある。

２．日本の採るべき対応

それでは、北極海の変容に伴う国際情勢の変化に対し、安全保障・防衛面の視点から、今後わが国として採るべき対応は何か。

短期的には、北極海航路の利用について、国際潮流を見定めつつ、海上交通路の利用を積極的に推進する方向で政策を進めていくべきであろう。また世界有数の海洋国家として、

国際的ルール作りへの参画も死活的に重要となる。すなわち「北極海の利用と国益に沿った外交政策の推進」が、短期的に日本の採るべき対応となる。一方、海洋立国たる日本が、安全保障・防衛面の視点から、中、長期的に採るべき対応としては、北極海を視野に捉えた安全保障・防衛政策の見直し、すなわち、「防衛体制の見直し……自律防衛能力の強化」、「日米防衛協力体制の見直し……日米同盟の深化」さらには「関係友好国との海洋安全保障協力の推進……海洋安全保障協盟の構築、拡大」を行うべきである。

（１）北極海の利用と国益に沿った外交政策の推進

わが国の安全保障・防衛面の視点からは、北極海を最大限に利用することが得策である。このためにはまず、生存と繁栄を海洋に全面的に依存する国家として、国際潮流を見定めつつ、わが国の国益に沿った形で北極海を通じた海上交通路の利用を推進すべきである。北極海を利用する海上交通が盛んになれば、わが国が失った北東アジア地域における海上交通のハブ港を国内に再設定することも可能となる。

一方、北極仕様の商船の建造や北極航路に適した教育を受けた船員の養成も必須となる。このためには、南極観測支援での経験を有する海自砕氷艦の乗組経験者の活用や砕氷艦建造技術の活用が可能となる。しかし、砕氷貨物船や、タンカー等の建造については、利害得失を慎重に検討する必要がある。より直截に安全保障・防衛面の視点からは、米海軍がグローバルに進めている国際テロや海賊対策のための海上状況把握（MSA：Maritime Situational Awareness）に関し、北極海においても協力していくことが必要となる。

何れにせよ、日本は北極圏諸国ではないが、その生存と繁栄を海洋に依存する海洋国家として、国際間で行われる北極海のルール作りには、早い段階で参画し、適切な外交手段により、日本の国益に合致する成果を得るように努めなければならない。北極評議会の将来的意義について、現時点では容易に見通すことはできない中で、同評議会が、現状において公正な国際ルール作りの中心となるとは想定し難いが、日本の関心が高いことを示すために、2013 年 5 月に得た非北極圏諸国（Non-Arctic States）という恒久的オブザーバーの資格を活用して、定常的に存在表明を続けることは重要である。そして、北極海を巡る新たな国際法制定に関する協議の機運が、北極評議会自身や、同評議会を発展する形で、あるいは別の何らかの形で生まれた場合には、海洋立国として積極的に参加する必要がある。それまでの間は、前述したとおり、北極評議会の加盟国である同盟国米国と協調しつつ、わが国の国益に沿った形でのルール作りへの参加を進めていくことが得策である。

（２）防衛体制の見直し……自律防衛能力の強化

安倍内閣が 2013 年末に示した国家安全保障戦略では、国際公共財（グローバル・コモンズ）に関するリスクの一つとして、北極海問題が特記されている。また、同時に採択された新防衛計画の大綱においては、北極海とは特記されていないが、グローバルな安全保障環境の改善への取り組みの一つとして、海洋安全保障の確保があげられている。このことは日本政府が、北極海問題を、わが国の海洋安全保障に直結する防衛体制見直しの、中、長期的課題として捉えるようになったと解することができよう。

中、長期的な北極海を視野に捉えた防衛体制見直しの方向性としては、自律防衛能力の強化を図ることが適当である。具体論としてはまず、北極海方面をもカバーする戦略情報収集能力強化のための監視衛星、UAV、C4ISR 等の整備が求められることになろう。将来的に、艦船や航空機などの北極海での行動海域が拡大することに伴い、戦略、戦域対潜能力の拡大、強化が必要となり、その能力を有する艦艇や航空機の増勢に加え、UAV や無人水中ビークル（UUV）の効果的利用が求められよう。さらに弾道ミサイル防衛能力の拡大、強化も必要となり、イージス艦の増勢なども検討の必要性が生じよう。一方、北極海での艦船や航空機の行動を念頭に置けば、砕氷救難機能確保のため、砕氷救難艦や氷洋救難機の整備、北極海や北方海域仕様の艦船、航空機の整備、同方面での海象・気象情報の収集、分析機能の保有も必要となろう。

また既述のとおり、日本海や 3 海峡防衛体制の強化はもとより、北海道周辺海域、北方海域、北極海での行動能力強化が必要となるため、同方面での自衛隊の情報収集体制の強化、C4ISR の整備、北方行動に適した艦船や航空機の装備、後方支援や運用面での改善、強化といった対策の検討も必要となろう。

（３）日米防衛協力体制の見直し……日米同盟の深化

安倍政権は、2014 年末を目処として日米防衛協力指針の改定作業を進めている。2013 年 10 月に東京で開かれた日米外務・防衛閣僚による安全保障協議委員会（いわゆる「2＋2」）において、1997 年の日米防衛協力指針について、2014 年末までに見直し作業を完了することが決定された。見直しの方向性としては、日米防衛協力の中核的要素である日本に対する武力攻撃への対処能力の確保、地域のパートナーとのより緊密な安全保障協力の促進、効果的・効率的・シームレスな対応を確保するための緊急事態における防衛協力の指針となる概念の評価といった、短、中期的課題に加え、同盟のグローバルな性質を反映する協力範囲の拡大や同盟強化を可能とする追加的な方策の探求といった、中、長期的課題が含まれている。「2＋2」では、それ以外にも、二国間の安全保障および防衛協力の分野として、

BMD 協力、サイバー空間や宇宙における協力、共同 ISR、防衛装備・技術協力などに加え、拡大抑止の協議の進展についても特記された。

これらを敷衍すれば、北極海を視野に捉えた、中、長期的な安全保障・防衛面の課題に対する日米同盟体制の見直しや日米防衛協力のあり方についても、今般の日米防衛協力指針の改定作業の中で、検討されるものと解すべきである。このことは当然のことながら集団的自衛権の行使についての議論の行く末とも深く関連する。

既に米海軍は、2009 年には北極海問題に対応するためのロードマップを作成する方針を打ち出し、2014 年を目処に、対応計画を作成する予定である。この計画には、戦略、政策、任務、計画が含まれ、作戦、教育訓練、武器、母体、センサー、C4ISR 等の兵力整備、戦略通信および展開、環境評価およびその予想が含まれる。対応計画で想定される任務としては、海洋安全保障、捜索救難、人道支援、災害救援、他官庁協力、戦略機動、戦略抑止、BMD などが含まれている。

現行の日米同盟体制では、北極海問題は想定外となっているが、北極評議会の加盟国米国との密接な関係構築は、安全保障・防衛面においても日本の北極海利用にとって大きな意義を持つことになる。米国の核抑止力を含む北極海安全保障体制強化への多角的な支援を、日本が行うことが可能となれば、日米安全保障体制の双務性向上に大きく寄与するという側面もある。

また、これに関連していえば、中露の関係強化を阻むためにも、核抑止を中心とした日米露の３国安保・防衛協力の強化も、以前に比べ現実味を増し、格段とその意義を深めていくこととなろう。

日米防衛協力指針の改定は、それ自身で大きな抑止効果を発揮するものと考えられ、取り分けこの中で、戦略情報共有、C4ISR、BMD、対潜水艦戦、捜索救難、人道支援、災害救援といった側面で、北極海の安全保障に関連する防衛協力の強化を含めていくことは、重要な意味を持つことになり、これらの関係強化を通じ、日米同盟のさらなる深化を図っていくことは、大いに意義を持つこととなる。この際、北極海を巡る安全保障・防衛面での情勢の変化に適応する形で、日米防衛協力指針を、都度、改定または一部修正していくことが求められる。

一方、指針の改定または一部修正に伴い、新指針の実効性を確保するための、日米防衛協力指針に直接関連する法体系である周辺事態安全確保法や船舶検査法の改定など、国内関係法の改定が必要となる可能性がある。またいうまでも無く、安倍政権により新設された国家の安全保障司令塔として期待される国家安全保障会議（JNSC）の指導、監督の下、関係省庁間の情報共有や運用面での協力の強化が必要となる。

（４）関係友好国との海洋安全保障協力の推進……海洋安全保障協盟の構築、拡大

2013 年 10 月の日米「2＋2」では、日米同盟の「地域への関与」として、能力構築、海洋安全保障協力、人道支援・災害救援、3 カ国協力や多国間協力についても論及された。その意味で、日本が自身の国益に沿う形で戦略的な観点から、「国際協調主義に基づく積極的平和主義」を具現化するため、欧亜の関係友好国との海洋安全保障協盟（有志連合：コアリション）を構築し、拡大を図っていくことが重要である。その中で、北極海問題に関しても、安全保障・防衛面での協調路線をとっていくことが求められる。

取り分け、遠隔の地にある関係友好国に対し、北極海での捜索救難などでの可能な範囲での積極的な協力を約束し、その見返りに、日本にとっての遠隔海域での海洋安全保障協盟の参加国との連携による広域かつシームレスな海洋安全保障協力により、長大な海上交通路の安全保障を確保することが可能となるよう、これら関係友好国との協調関係を維持していくことが得策である。

おわりに

北極海に関しては、日本自身は北極圏諸国という立場ではなく、2013 年の 5 月、ようやく他のアジア諸国とともに、北極評議会の「非北極圏諸国」という形の恒久的オブザーバーという資格を手に入れた。北極海航路の利用は、日本にとってのメリットは大いにあるものの、北極評議会の加盟国による寡占的性格、中国などによるあからさまな自己中心的な覇権外交活動、日本の出遅れなど、国際政治的に必ずしも日本に有利な状況が作られてはいない中で、航路としての利用や資源開発、関心の激化に伴う環境保護、安全保障・防衛といった面での国際的ルール作りが求められており、日本としては、わが国の国益に沿った形で、この動きに能動的に参画していく必要がある。

その一方で、中、長期的に北極海を視野に入れた自律防衛能力の強化、日米同盟の深化、さらには関係友好国との海洋安全保障協盟の構築、拡大が求められている。現安倍政権になって、国家安全保障戦略の初の採択をはじめ、新たに防衛計画の大綱や中期防が策定され、さらに集団的自衛権行使などの憲法解釈見直し作業が進み、日米防衛協力指針も日米当局間での検討作業が開始されるなど、わが国の安全保障・防衛政策の見直しが、「国際協調主義に基づく積極的平和主義」の具現化という明確な方針の下、推進されていることは大いに頼もしいことである。ついては「北極海問題」が、短期的な海運や資源開発という経済的側面だけではなく、中、長期的には、安全保障・防衛面に重要な意味を持つことに留意した形で、これら政策見直しが強力に進められていくことを期待する。

第７章　グローバル・コモンズとしての北極海に相応しい安全保障

池島　大策

はじめに――プロジェクトの目的との関連で

本研究会では、「グローバル・コモンズとしての北極海」を考察対象の一環に組み入れている。今日の米国や日本における特に安全保障関連の議論の際には、北極海がグローバル・コモンズ（Global Commons）の一つであるという考え方が暗黙の了解となっているように見受けられる。しかし、この考え方が前提として成熟しているかは、実は大きな論点の一つである。グローバル・コモンズという概念自体、軍事中心の安全保障上の観点に基づく一般的な呼称は別として、まだ曖昧な部分を多々残しており、国際法上または国際関係論の分野では厳格にいえば、明確に定義されているわけではない。

また、このプロジェクトが日米同盟の役割という文脈からグローバル・コモンズの安定利用を検討しているなかで、北極海のガバナンスが日米の二国間関係とどのような関連にあり、しかも安全保障[1]に関わる内容をどのように分析すべきかなどについても様々な角度からの考察が必要である。日米同盟といういわば日本と米国との二国間の政治・経済・軍事などの幅広い包括的な関係が、北極海の現状や今後の在り方とどのような関係を持つようになるのかを検討することも必要とされている。通常、軍事同盟である点が強調されがちな日米同盟が北極海周辺諸国を含む北極（圏）における安全保障の状況に、どの程度またどのような形態で関与すべきかが問われてもいる。

最後に、日本の役割とその強みを活かすことが日本外交の将来にとって重要であり、この点の検討・分析を行うことがこの研究会の究極のテーマである。したがって、北極海周辺諸国と日本という多数国間関係（場合によっては、北極周辺の各国と日本との二国間関係を含む）、日本と米国との二国間関係などの他にも、北極に関与する他の諸国（非北極諸国（non-Arctic states））と日本との関係をも考慮した上で、日本の立ち位置を見極め、将来の課題に対処することが求められているといえる。

したがって、本稿ではこれらの三つの問題意識を中心に、特に北極（海）に相応しい安全保障の概念に焦点を絞って、関連のある若干の論点に対する現段階で可能な検討と、それに対する暫定的な対応の概略だけを述べておく。なお、北極海に関するガバナンス上の論点や類似するイシューについての検討は、別稿を参照していただきたい[2]。

１．グローバル・コモンズとしての北極（海）という概念

グローバル・コモンズとは、国際法上、必ずしも定義の明確な概念とは言えず、一般に、国家の管轄外にある場所、空間、物などを総称して使われるようになった比較的新しい概念である。国際法上の類似の概念として議論は尽きないが、公海のような万民共有物（*res communis*）、深海底及びその資源に代表される人類の共同の財産（Common Heritage of Mankind: CHM）のようなほぼ定着したものがあげられるが、厳密にはこれらの概念とも同じではない[3]。

また、グローバル・コモンズという用語は、近時、とりわけ米国及び（米国における最近の流儀に倣った）日本で安全保障の文脈で多用されるようになった印象があるが、元来、環境保護と国際化の動きの中で、国際社会において共通の利益のために広く開放された空間や場所とその資源を一般的に指すことが多かったものである。

たとえば、2013 年末に閣議決定された「国家安全保障戦略について」[4]では、「海洋、宇宙空間、サイバー空間といった国際公共財（グローバル・コモンズ）」という書き方によって、グローバル・コモンズが国際公共財の言い換えであるようなニュアンスが感じ取れる。もっとも、この一節では、これらの国際公共財に対する「自由なアクセス及びその活用を妨げるリスクが拡散し、深刻化している」との指摘があるにとどまる。言い換えれば、こうした使い方が最近では多くなっていて、一般化しつつあることがうかがえる[5]。そして、この「国家安全保障戦略について」では、「北極海では、航路の開通、資源開発等の様々な可能性の広がりが予測されている」ため、「国際的なルールの下に各国が協力して取り組むことが期待されている」反面、「国家間の新たな摩擦の原因となるおそれもある」と警鐘を鳴らしている[6]。しかし、どういう理由で「国家間の新たな摩擦の原因」が生じるかは直接触れられていない。その前の記述にある「力を背景とした一方的な現状変更を図る動き」や、「資源の確保や自国の安全保障の観点から、各国の利害が衝突するレジームが増えて」いることなどが想定されているように見受けられるが[7]、はたして北極海では本当にそうなのかを検証しなければならない。

たしかに、北極海という海洋空間が国際社会（international community）において関係諸国にとって環境・生態系の保護を始めとした何らかの共通の利害関係を有する場所であるとすれば、もともとの意味におけるグローバル・コモンズと称される面があることは否定できない。しかし、半閉鎖海にあたる北極海の沿岸諸国として直接的な利害関係にあるカナダ、デンマーク、ノルウェー、ロシア及び米国の 5 か国（北極 5 か国）がはたして北極海を元来の意味における「グローバル・コモンズ」であると共通して考えているか否かには大きな議論のあるところである。彼らの真意とは別に、最近の国際世論や研究の動向などを見ると、北極海をグローバル・コモンズの一つに位置づけ、国際社会が関心を寄せるとともにグローバルな影響を有する場所であると捉えなおそうとする見解が徐々にではあるが勢いを増してきているようにも見える。こうした「北極海の国際化」ともいうべき

動きが徐々に進みつつある現状に鑑みると、できれば北極海の沿岸諸国の内々の問題としておきたい北極５か国の思惑と、グローバルな視野と対応を望む国際社会の動向とが、今後の持続可能な開発、環境保護、平和と安定の確保などにおいて必ずしも一致しないか、場合によっては相反するときに、北極海の将来が不透明感を増すことになる。

２．北極のよきガバナンスとは

地球温暖化の影響で生じつつある北極海における環境変化は、北極海沿岸諸国に多大な影響を及ぼし、北極海における地域の安定と持続可能な発展を大きく左右する。そうした中で、はたしてどのようなガバナンスが北極海には必要でありかつ望ましいのかという点が今問われている[8]。

北極に関するガバナンスとして北極評議会（AC）の設立趣旨や役割[9]が、南極に関するガバナンスを担う南極条約体制と異なることは言うまでもない。他方、現行の AC だけが北極海の「よきガバナンス」を担っているわけでもない。北極海を規律する法的枠組は、国連海洋法条約（LOSC）を中心とした海洋法、国際海事機関（IMO）のような国際組織・機関等で採択される関連規範などのほか、各沿岸国法令などの網の目により複層的に成り立っている[10]。

北極海では、沿岸国の対内的及び対外的な利益の調整が当面の重要な課題であることは変わらないが、これに沿岸付近の諸国、北西及び北東を含む北極海航路の利用国（船舶の旗国だけに留まらない）など以外にも、何らかの利害関係を有する国が経済や環境の分野を始めとした様々な要因から、ステークホルダー（利害関係者）として関与する度合いが増している。それにつれて、何らかの法的秩序に基礎を置く安定した「よきガバンナンス」が国際社会では広く期待されるようになっている。ただ、問題は、そのガバナンスの方向性が必ずしも明確になってはいないことであり、特に AC の北極 5 か国（Arctic 5）や北極海周辺諸国の間で重視する力点を国際協力に置くか、軋轢を覚悟の上で国家主権に置くかで意見の収斂が必ずしも見られないことにある[11]。この点は、安全保障（セキュリティ）の分野では特に顕著なイシューであり、そもそも北極海における安全保障の概念がいかに多様かつ複雑であるかを物語るものである[12]。

一般に北極海における安全保障を論じる際に、従来の軍事的対立や軍拡競争を扱う安全保障の問題以外にも、気候変動の結果生じる環境問題、汚染に由来する環境問題、天然資源開発に伴って生じるエネルギー問題、人間の生存に関する人間の安全保障（human security）なども含めて、多様な安全保障の概念とそれに対する対応が今世紀の国際社会全体で問われていることに留意しなければならない[13]。しかも、AC 内部でも安全保障に関する発想の根源は同じとは言えず、北極 5 か国が自国の国家主権と国家安全保障を中心に考えている傾向があるのに対して、その他の AC の 3 か国はより広義の安全保障とそのための国際協力に主眼を置いていると考えられることが指摘されている[14]。言い換えれば、AC の原加盟国である 8 か国（Arctic 8）でさえ、経済

的にも、政治的にもまた軍事的にも単一・同一の国際的な組織に加盟しているわけではなく、安全保障に関する共通の基盤を必ずしも持っていない以上[15]、北極海の地域特有の事情を織り込んだより包括的な安全保障観（軍事に限定されない）とそれを実施するための枠組みや仕組みがいずれ必要となるということである。

したがって、北極における安全保障では、主権国家の存立に関わる安全保障という従来の考え方以外にも、地球全体の利益に関わるグローバルな安全保障、北極海周辺の地域に特有のリージョナルな安全保障といったものまでも現在では、関係諸国すべてを巻き込んで考慮しなければ対応しきれない状況となっている。前者の従来型の安全保障については、冷戦後も続く米ロ両核大国の対峙という現実に伴って、おそらくは当分の間今後も続くものであり、伝統的な安全保障観を基礎に対応することが中心となるであろう。他方で、後者のより広範で複雑なグローバル及びリージョナルな安全保障については、北極海における越境環境侵害や捜索・救助のようなイシューに対しては国家主権の壁を越えた国際協力を必要とし、いずれの国にとっても直接・間接に様々な影響があることになるため、対話と協力の実施のための機会の確保・増大がますます喫緊の課題となっている。実は、こうした広い意味における安全保障（セキュリティ）という考え方こそ、グローバル・コモンズとしての北極（海）を考えるうえで不可欠な発想であるにもかかわらず、日本における最近の各種見解では、比較的疎んじられているように見受けられる。

以上より、北極海のよきガバナンスのためには、各関係国の安全保障と国際社会全体・地域全体にも及ぶ安全保障という両者を加味した仕組みの整備とその実施の確保に向けた国際協力が必要となるであろう。

３．沿岸諸国や関係諸国の動向

（１）沿岸諸国の動向の概略

北極海における沿岸諸国の中でも、米国は唯一、LOSC の締約国にはまだなっていない[16]。米国は、アラスカ州が地理的には最も関係があるにすぎず、これまで他国に比べて国家戦略自体が手薄な印象があった。そのため、米国は特にオバマ政権になってから北極地域に関わる外交政策をより明確にし始めたが、航行の自由のほかに自国安全保障上の利益を確保するため、下記に述べるように 2013 年にはその具体的な施策へとつなげるための方針をいくつか示し始めた。

他方、沿岸諸国として長く自国の沿岸における規律を強化してきたカナダとロシアには、環境と開発の点で対照的ともいえる興味深い姿勢が見られる。カナダは、環境保護の観点から北西航路の水域を厳格な規制に服する内水として扱い、環境保護の点を重視した沿岸管轄権の行使を厭わず、自国の「北極主権」（Arctic sovereignty）の保護こそが第一の国益と考える立場から、安全保障上の観点でも伝統的及び非伝統的な安全保障を併せて確保する道を考えている[17]。

北極 5 か国の中でも最長の海岸線で北極海に面するロシアは、北極海航路の開発と利用に積極的で、独自の管理方式により沿岸への支配を自国権益に直結させている反面、新規の 2013 年版「2020 年までの間のロシア連邦の北極地帯の開発及び国家安全保障の確保のための戦略」においては 2008 年版の「2020 年まで及びそれ以降の北極におけるロシア連邦の政策の基盤」よりもさらに軍事的な意味における安全保障政策を推し進める姿勢を見せている[18]。

非北極諸国である中国や韓国は、2013 年に日本などと同時に北極評議会（AC）から常任オブザーバーの地位を付与され、近年の北極海航路への積極的な関与に見られるように、いわゆる北極外交を推進する積極的な姿勢が顕著である。日本は、北極担当大使を配置するなど漸く北極外交を進めるのに本腰を入れ始めたようだが[19]、やや出遅れた感を払拭するには得意の科学調査や環境保護技術などの分野で貢献を進める以外の道を、総力戦で具体的に探らねばならない。

以下では、特に最近になって北極に関わる国家戦略を具体化させつつある米国の動きと、北極開発に積極的に進出してきている中国の動向を概観しておく。これにより、米国の北極政策を吟味したうえで、日米安保条約を核とする日米同盟下において、北極をめぐり顕著な動きを見せる中国の立場をどうとらえるべきかを考察しながら、同時にグローバル・コモンズとしての北極海の置かれた安全保障環境をどうとらえるべきかを考えるための素材を整理しておくことにする。

（２）米国の立場

まず、米国は、2013 年 5 月にオバマ大統領の政権下における「北極地域のための国家戦略」を公にしているが[20]、その中で北極をめぐる事項に関して順位付けを行い、国内的に統一した施策をとりながら国際的な対応を進めることを示した[21]。この「北極地域のための国家戦略」は、2010 年 5 月の「国家安全保障戦略」[22]を具体化し、気候変動に伴って生じる北極の新たな環境に対処すべく、(1)安全な商業・科学活動から国防に及ぶ広範な安全保障上の国益を推進すること、(2)北極地域の管理責任を全うすること、及び(3)二国間関係や多数国間機関を通じて国際協力を強化することを努力目標に、海・空の双方における航行・飛行の自由に基づく地域の平和と安全の確保、入手可能な最善の情報を利用した意思決定、関係方面との連携強化などを指針とすることなどを主な内容としている。

この戦略自体は総花的で具体性に欠けるともいえ、従来米国自体が北極に対して一層積極的な姿勢を示すことを望む声も少なくなかっただけに[23]、国益の確保と国際協力を念頭に置いていることが当該戦略に示されていることは理解できる。同時に、この戦略の中でオバマ大統領が「北極は平和で安定しており、争いのない地域である」と冒頭に述べていることを受けて、国防総省（ペンタゴン）が 2013 年 11 月に公にした「北極戦略」[24]は、現在の北極の状況に照らして国家の

安全保障を確保するには、自国だけでは不可能であって国際法に従って同盟国やパートナー国との連携が必要であることを率直に認め、人間の安全保障と環境安全保障との間にバランスがとれた取組みを推進していく旨、述べている。そして、官民のセクターを問わず、アラスカ州や連邦政府が一体となって共同で対処していくことを模索する内容となっている[25]。

さらに、北極に関する米国の国防戦略上も、同盟国やパートナーとの連携と協力の促進強化によって、多様な課題に対応する体制を整えておくことが謳われ、北極における今後の気候変動の度合いや経済状況などの不確定要因を十分考慮し、国家財政状況、国内世論の動向に注意を払って、透明性と情報共有を通じた信頼醸成に基づく国際協力を強調している点に特徴がある。

この「北極戦略」では、やや落ち着いたトーンによる国際協力に向けた取組みを重視する姿勢は、「軍事的な脅威が比較的低いレベルにある」北極という地域的特性にあり、2008 年のイルリサット宣言で LOSC 以外の包括的な法的枠組みを新たに必要としないことを確認したという点を繰り返しながら、軍事関連の安全保障に止まらない人間の安全保障や環境安全保障のような「ソフト・セキュリティ」のイシューに AC が対処できることも認めている[26]。したがって、北極の安全保障状況を過剰なまでに軍事や軍備競争の視点だけで捉えることは米国の現行の北極戦略に合致しないし、むしろ米国が回避しようとする見方であることが読み取れるのである[27]。

（３）中国の立場

次に、中国の動向に目を向けてみたい。ライジングパワーとも、リターニングパワーとも称される中国は、北極における航路開発や資源エネルギー探査に強い関心を示し、そのための北極外交を展開しているともいわれている[28]。そのため、中国の動向自体が北極海における安全保障環境を左右する大きなファクターであると見るような立場は少なくない[29]。中国自身にどのような思惑や外交方針があるのかについては、公式見解に近いと解されるものもないわけではないが[30]、北極に関する自国の政策を公にしていないため、確たるものはないといえる。その理由として国の政策自体が確定していないからであるとする見解が多い[31]。また、北極に関する中国の姿勢は、南極において早くから科学調査に専念してきた姿勢とも同じではないように見える[32]。はたして、中国の北極海への進出は、安全保障上の脅威となるのであろうか。

中国の北極への強い関心は、1980 年代初頭から主に南極における科学調査が本格的に始まったのからはやや遅れて、90 年代になってから徐々に本格化していたが、2010 年ごろになってようやく世界の注目を集めるようになったにすぎないようである[33]。確かに、中国は 2004 年にノルウェーのスヴァルバール島に科学調査基地を初めて設立する以前から、科学調査隊を派遣してきた結果、これまで既に 5 次（1999 年、2003 年、2008 年、2010 年及び 2012 年）にわたる調査隊の派遣という実績も積んでいる[34]。中国の砕氷船・雪龍の活躍が注目を浴びると同時に、中国の習近

平国家主席や李克強首相といった国家の首脳らによる近年の北欧諸国への訪問は、北極圏開発の利益をめぐる自国の足場を二国間外交によって固めつつ、AC を始めとした多数国間によるルール作り等の場での発言権の確保や影響力の強化に資するものともいえようが、話はそう単純ではない。こうした中国の進出を、気候変動などの環境要因、航路やエネルギー・資源開発に伴うビジネス機会の到来[35]、そして、既存の法規範（LOSC を中心とした）に基づくガバナンスの維持の諸点を主たる動機づけとする立場もあるが、その動向を脅威と見るか、好機と見るかにつき評価が分かれているのが現状である。

2010 年 3 月 5 日に中国の尹卓海軍少将が「国連海洋法条約に照らして、北極点及びその付近の地域は、いずれの国家にも属さないものであって、全世界の人民の共同の財産である」と述べたことが報道された[36]。そのため、この発言は様々な憶測を呼び、北極周辺国を含む関係国にとって中国の「野望」や「脅威」と受け止められたフシがある。中国が、日本と同時に AC への常任オブザーバー参加の資格を認められたことや、領土紛争のある東シナ海・南シナ海[37]などの周辺海域において近隣諸国との軋轢を増している近年の状況から、北極海についてもその野心や積極的な姿勢ばかりが強調されて伝えられるようにもなっている。

しかし、中国の北極に対する姿勢の現状は、必ずしも周辺諸国が警戒すべきものではないという冷静な見方が少なくない[38]。上記の科学調査協力などにおける実績、北欧諸国やロシア・カナダなどの北極周辺諸国との経済開発におけるバイラテラルな連携の強化、AC や LOSC といった法秩序に基づくガバナンスへの参加とその態様などに照らしてみると、その積極的にも見える姿勢に脅威だけを読み取る必要もなく、リアリズムの視点に立った別の冷めた見方も各種あって興味深い。

たとえば、中国がノルウェー、カナダ、アイスランド等との科学調査協力や経済的連携を強めていくにしても、中国の主に経済・技術力に対するこれらの国々の需要があるからであって、世界第 2 位の経済大国となっている中国の現状をみれば、至極当然の結果ともいえる[39]。むしろ、諸般の理由から、中国の野心や利益を上手く汲み取って中国をACの中に組み込むことで、安全保障上の過剰反応を回避し、北極における不安定要因を増幅させないように国際協力を進めることの利益を説く論調もあながち不合理ではない[40]。また、中国外交部の胡正跃（Hu Zhengyue）部長助理がその発言の中で、北極海の沿岸諸国が自国の大陸棚の延伸を過大に行うことに対して注意を喚起して、中国などの非北極諸国も北極海の深海底部分（CHM）に対してLOSCで認められた正当な利益を有することを唱えている[41]。しかし、この発言が LOSC の遵守を関係国に迫ると同時に[42]、発展途上国の立場を「代弁」したものであるとの解釈もあり、他の主要国が行っていないグローバル・コモンズとしての北極海を際立たせることになったという点で、中国は北極海のよきガバナンスを志向することをアピールするといった独特の役回りを演じている[43]ともいえる。さらに、北極

海における沿岸諸国の管轄権の拡張や大陸棚の延伸申請による権利行使などの状況を危惧するように見える中国の立場からすれば、この状況を南シナ海に擬して中国が権利を主張しようとしているという見方は両者のまったく異なる法的状況を混同している点で的外れであると評することもできる[44]。より突き詰めていえば、国際法上は、中国の、北極海に関わるこれまでの言動が非北極圏諸国に認められた各種の権利の範囲を逸脱するものであるという証拠はないという立場[45]の方に客観的で説得力があるといえる。

以上の検討から、中国自身が自国の北極に関する外交政策や戦略を公にしているか否かや、また意図的に曖昧な立場をとっているか否かに関わらず、また中国の論者がどのような形で中国の立場を表明しようと[46]、安全保障上の脅威や軍事的な緊張に繋がるような見方だけを強調することはバランスを欠くものであって、米国自身が抱く戦略や方針とも見比べたうえで、やはりもう少し視野の広い展望を持つことが関係諸国には必要となろう。

４．よきガバナンスの具体化に向けて

北極海を規律する国際的な法制度の中心は LOSC であると考えられるが、北極海の5沿岸諸国はイルリサット宣言[47]で確認したように、LOSC 以外の何らかの国際的な制度作り（北極の国際化）には今のところ消極的である。実際、北極海に関わる国際的な枠組みには、AC 及びその内部でコンセンサスによって採択される勧告などの他にも、各国の国内法令や、各種国際組織・機関によるソフトローとも呼ぶべき規範が存在している。たとえば、国際海事機関（IMO）や国際船級協会連合（IACS）のような国際機関・団体による船舶航行関連のガイドライン[48]や国内規則を調和させるための調整協議のような方式が相当関わっており、AC 主導で採択された捜索救助協定（2011 年）[49]や海洋油汚染準備対応協力（2013 年）[50]以外にも幾つかの法規範の整備がさらにこれからも必要とされている。その意味では、IMO における極域行動規範（Polar Code）が早期に妥結されることが当面は重要な課題であるが[51]、オタワ宣言により軍事・安全保障の分野を扱わないことになっている AC にとって、環境保護と持続可能な開発を両立させる取組みが今後ますます迅速に具体化されることが望まれよう。

しかし、安全保障上の課題が北極海のよきガバナンスの上で全くないわけではなく、米国、カナダ、デンマークなどの友好国間における共同演習の実績は徐々に蓄積されており、この分野で個別の対応が見られるのも事実である。北大西洋条約機構（NATO）[52]の関与について北極沿岸諸国の中でも温度差はあって、たとえば、カナダは他の北極圏諸国とは異なり、NATO の肩入れを好まない[53]。ロシアの圧倒的な存在や中国の海洋進出の本格化が見られる昨今、安全保障の概念自体も多様化、多角化している。ちなみに、中国は当初から北極海がグローバル・コモンズであるとの認識の下に、北極海をめぐる外交政策を遂行してきたとの見解もある。

北極特有の自然環境や地理的状況のせいもあって、災害や遭難などへの対処のために沿岸国の海軍や沿岸警備隊が協力・連携し、訓練、通報、情報交換などを通じて対応する実行も積み重ねられ、上記のように AC 主導の下で捜索救助や海洋油汚染への緊急対処といったソフトな安全保障関連の仕組み（多数国間合意）は徐々にではあるが蓄積ができてきている。その意味では、北極海における安全保障の概念は、必ずしも軍事関連の狭いセキュリティだけを意味するものではなく、広義のセキュリティとして捉える余地が十分にあるといえる。むしろ、グローバル・コモンズとしての北極海のよきガバナンスのためには、この広義のセキュリティという概念を通じて関係諸国間で調整を進める方が共通利益を見出しやすい面があることに留意すべきである。

５．日米同盟との関連性

以上のような北極の事情に鑑みて、日米同盟が今後いかなる意味を持ちうるかという点を検討しておくことは、たとえ理論上のことであっても有意義であろう。日米両国が何らかの認識を共有しておくことでバイラテラルな関係を、多数国間の共同利益が深く関わるグローバル・コモンズとしての北極における事項にどのように活かせるかが今後問われる可能性もある。ただし、日米同盟下で必要とされる集団的自衛権の行使が、現行憲法下で認められる自衛権の行使とどの程度、整合性をとることができるかは、非常に大きな論点となる。

日本における集団的自衛権の行使の議論はようやく内実のあるものとなってきたとも言われるが、それだけにより慎重な議論が行われることが期待される[54]。特に、これまで述べてきたような北極の状況に照らしてみれば、日米同盟の文脈でも議論に上がる集団的自衛権の行使といった軍事的・国防上のイシューが理論的なものであったとしても、こうしたハードな軍事的なイシューを避ける努力をしてきた北極圏諸国や関係諸国にとって歓迎されるものかは疑問である。したがって、グローバル・コモンズとしての北極海の事案に日米同盟というバイラテラルな関係を結び付けることが必要となるか否か、検討を深めていくにしても、安全保障の議論でも非伝統的な形態において行われる方が現状に違背しない。

たとえば、集団的自衛権の行使に関して「安全保障の法的基盤の再構築に関する懇談会」（安保法制懇）[55]でも議論された四類型の一つにあたる公海上での米軍艦の防護のケースとして、このケースでいう「公海上」に北極海の公海部分は入るのかが問われることにもなる。またこの四類型の二つめにあげられる米国に向かう弾道ミサイルの迎撃のケースとして、北極海上空を含む北極圏を経由するミサイルを迎撃する場合もはたして想定されるのかといった疑問も理論上は生じよう。

安保法制懇で 2013 年 10 月に新たに示された事例の中には、日本に向かうタンカーが通過する海峡（シーレーン）で攻撃国が敷設した機雷を有事においても除去できるか否かといったケース

がある[56]。これに関連して、将来、北極海における航路の利用が本格化してベーリング海峡が「ベーリング門」（Bering Gate）と称されるようなチョーキングポイントとして[57]、ここでいうシーレーンに該当するか否か、そしてもし該当するということになれば、この機雷除去のケースとして検討する必要があるかどうかという仮定の問題も浮上することがないわけではないであろう。

しかしながら、これらのケースは、我が国の置かれた現況から、技術的にも、法理的にも、戦略的にも無理と困難を伴い、極めて慎重に対応すべき事態ということになろう。北極海においては、バイラテラルな日米同盟を基礎とした集団的自衛権をも含むような安全保障の概念を北極海にまで拡張して考えたり、この二国間関係を全面的にまたは中心に安全保障を捉えたりするよりも、むしろ非伝統型安全保障のための国際協力として、AC を始めとした多数国間の枠組みを中心に、既存の海洋法や、捜索救助、緊急対応に関連する多数国間合意に基づいた対応として、日本の国際協力として現行法制下で可能な範囲を探ることをまずは検討する方が現実的なのではないであろうか。そして、上記の検討内容が、米国自身が日本に期待する日米同盟のあるべき姿とも合致するか否かをよく見極める必要がある。

おわりに

このように、より広い視野から見た安全保障（日米同盟の役割や機能をも含めて）の文脈においてグローバル・コモンズとしての北極海を捉えなおすと、環境保護や持続可能な開発といった視点だけでは把握しきれない国際法にも関連する様々な論点がいくつも見えてくることがわかる。しかも、この広義の非伝統的安全保障の概念こそ、冷戦後の状況や地球温暖化の将来を勘案して、北極海においては詳細に検討してみる価値があるのではないかと思われる。これらの論点の中には、日本国憲法の解釈適用上の論点にとどまらず、憲法の精神を活かす外交政策・戦略を模索するという課題とともに、中長期的な視野において検討されるべきものが少なくない。

したがって、北極海をめぐる広義の安全保障（セキュリティ）について、同沿岸諸国だけでなく、EU や NATO なども広く関心を有していることから分かるように、非北極諸国の一つである日本には何が可能で何が不可能か、何をすべきで何をすべきでないかをよく吟味しておかなければならないであろう。なぜなら、こうした広義の安全保障は、日本が北極に関わる外交政策を早急に固めて今後展開できるよう早期に検討しておくべき重要な課題だからである。

－注－

[1] しかも、この安全保障（security）の用語ですら、多様な意味を含んでおり、後に述べるように、伝統的な意味と非伝統的な意味、または広義と狭義の概念があるので、「セキュリティ」とカタカナで書いておく方が文脈上は相応しいこともある。

[2] さしあたり最近のものとして、池島大策「第６章　北極のガバナンス:多国間制度の現状と課題」平成24年度外務省国際問題調査研究・提言事業報告書『北極のガバナンスと日本の外交戦略』（日本国際問題研究所、2013 年 3 月）及び、池島大策「北極圏ガバナンスの課題――法秩序の生成と発展を求めて」『外交』22 号（時事通信社、2013 年 11 月）46-53 頁、をそれぞれ参照せよ。

[3] こうした概念の分類については、池島大策「公共圏におけるグローバル・コモンズの安定的利用と国連の役割」『国連研究』第 15 号（2014 年）（近刊）参照。

[4] 「国家安全保障戦略について」2013 年（平成 25 年）12 月 17 日国家安全保障会議決定、閣議決定、7 頁以下参照（http://www.kantei.go.jp/jp/kakugikettei/2013/__icsFiles/afieldfile/2013/12/17/20131217-1_1.pdf）（インターネットサイトの引用は、以下すべて 2014 年 1 月 15 日付）。

[5] この点の指摘は、池島論文・前掲注 3 を参照。

[6] 「国家安全保障戦略について」前掲注 4、8 頁参照。

[7] 同上、7 頁参照。

[8] 北極（海）におけるガバナンスについては、池島論文・前掲注 2 にあるもの以外に、以下を参照。奥脇直也・城山英明編著『北極海のガバナンス』（東信堂、2013 年）；西元宏治「北極海のガバナンスとその課題：海域の法的地位・国家間協力の枠組みを中心に」『国際問題』627 号（2013 年）5-21 頁。

[9] AC の設立時に安全保障の事項を扱うべきでないとの宣言が行われている。1996 年 9 月 19 日のオタワ宣言参照。

[10] 池島論文・前掲注 2「北極のガバナンス」63-66 頁及び同「北極圏ガバナンスの課題」49-52 頁。

[11] この点で、国際協力重視の論調が増えつつあるが、各国の戦略や政策を広範に比較検討するものとして、以下のものを参照。Ian G. Brosnan, Thomas M. Leschine & Edward L. Miles, ‘Cooperation or Conflict in a Changing Arctic?,’ 42 *ODIL* 173 (2011).

[12] この点を指摘する次の論考を参照。Lassi Heininen, ‘Arctic Security – Global Dimensions and Challenges, and National Policy Responses,’ 5 *The Yearbook of Polar Law* 93 (2013).

[13] この指摘につき、以下のものを参照。Oran Young, ‘Foreword - Arctic Futures: The Politics of Transformation,’ *Arctic Security in an Age of Climate Change*, Edited by James Kraska, Cambridge University Press, 2011, pp. xxi-xxvii, at p. xxvi.　ほかに、日本のもので以下を参照。石原敬浩「北極海と安全保障」『国際問題』627 号（日本国際問題研究所、2013 年）49-59 頁。

[14] See Heininen, *supra* note 12, p. 115.

[15] 8 か国のうち、5 か国が北大西洋条約機構（NATO）に、別の 5 か国が北欧理事会（Nordic Council）に、3 か国が欧州連合（EU）に、それぞれ加盟しているという具合であることから、足並みが揃っているわけではない。Heininen, *supra* note 12, pp. 100-101.

[16] この点についての詳細な検討は、以下のものを参照。池島大策「第九章　国連海洋法条約への参加をめぐる米国の対応――米国単独行動主義の光と影――」『米国内政と外交における新展開』（日本国際問題研究所、2013 年）147-164 頁；都留康子「アメリカと国連海洋法条約：“神話”は乗り越えられるのか」『国際問題』617 号（日本国際問題研究所、2012 年）42-53 頁。

[17] Rob Huebert, ‘Canada and the Newly Emerging International Arctic Security Regime,’ *Arctic Security in an Age of Climate Change*, *supra* note 13, pp. 193-217, at pp. 194-196.

[18] たとえば、以下のものを参照。秋山昌廣「北極圏めぐる安全保障の課題――資源と新航路が潜在的紛争要因に」『外交』22 号（時事通信社、2013 年 11 月）20-26 頁；John Drennan, ‘Russia’s Persistent Arctic Ambitions,’ 11 December 2013, at the following site:
http://www.iiss.org/en/militarybalanceblog/blogsections/2013-1ec0/december-e71c/russia-in-the-arctic-b038

[19] 以下の最近のものを参照。加藤喜久子「第 6 章　日本の北極問題への取り組みの現状と展望」、前掲注 8『北極海のガバナンス』97-115 頁；國方俊男「北極海問題と日本」『国際問題』627 号（日本国際問題研究所、2013 年）1-4 頁；内閣官房総合海洋政策本部事務局「第 14 回参与会議：資料 3　北極海に関する取組について」（2013 年）（http://www.kantei.go.jp/jp/singi/kaiyou/sanyo/dai14/siryou3.pdf）。

[20] ‘National Strategy for the Arctic Region’, 10 May 2013. See the following site:
http://www.whitehouse.gov/sites/default/files/docs/nat_arctic_strategy.pdf　なお、これを受けて出された米国沿岸警備隊の「北極戦略」（Arctic Strategy）については、次のサイトを参照。
http://www.uscg.mil/seniorleadership/DOCS/CG_Arctic_Strategy.pdf

[21] ちなみに、この国家戦略が公になる前（2013 年 4 月 25 日付）とその後（8 月 8 日付）に、議会向けに出された各報告書には、とりわけ北極海における米国の海軍と沿岸警備隊のプレゼンスの意義を指摘する箇所がある。Ronald O’Rourke, ‘Changes in the Arctic: Background and Issues for Congress,’ *CRS*

Report for Congress, 8 August 2013 (https://www.fas.org/sgp/crs/misc/R41153.pdf).また、米国のシンクタンク（CSIS）による提言が同年 3 月にも出ていた。Heather A. Conley *et al.*, 'The New Foreign Policy Frontier: U.S. Interests and Actors in the Arctic,' March 2013 (http://csis.org/files/publication/130307_Conley_NewForeignPolFrontier_Web_0.pdf).

22 'National Security Strategy,' May 2010. See the following site: http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

23 2009 年 1 月 9 日にブッシュ政権下で、「国家安全保障大統領指令／国土安全保障大統領指令」（NSPD-66/HSPD-25）において、「北極地域政策」（http://www.fas.org/irp/offdocs/nspd/nspd-66.htm）が出されていたが、特別な意味を有する安全保障上の議論が行われているとは一般に考えられておらず、北極の国家政策に関してむしろ米国の受け身的なまたは消極的な姿勢が表れていることがしばしば指摘されてきた。また、2009 年 10 月には、「米国海軍北極ロードマップ」（U.S. Navy Arctic Roadmap）も出来上がり（http://www.navy.mil/navydata/documents/USN_artic_roadmap.pdf）、北極の環境変化が及ぼす影響下で国連海洋法条約に基づく行動の重要性が記されている。なお、米国の北極安全保障における消極性につき、以下を参照。Siemon T. Wezeman, 'Military Capabilities in the Arctic,' *SIPRI Background Paper*, March 2012, pp. 1 & 10 (http://books.sipri.org/product_info?c_product_id=442).

24 'Arctic Strategy,' November 2013. See the following site: http://www.defense.gov/pubs/2013_Arctic_Strategy.pdf なお、ペンタゴンによる議会向けの 2011 年報告書では、人間の安全保障と環境安全保障とのバランスあるアプローチを促進する国際連携のための好機と捉える趣旨も見られる。Department of Defense, 'Report to Congress on Arctic Operations and the Northwest Passage,' May 2011 (http://www.defense.gov/pubs/pdfs/tab_a_arctic_report_public.pdf).

25 同戦略を公にしたヘーゲル国防長官は、「多数国間による安全保障協力が優先事項である」ことを別の機会でも述べている。'Pentagon Releases Strategy for Arctic,' *The New York Times*, 22 November 2013, at http://www.nytimes.com/2013/11/23/world/pentagon-releases-strategy-for-arctic.html?_r=0

26 'Arctic Strategy', *supra* note 24, pp. 4 & 7.

27 'Arctic Strategy', *supra* note 24, p. 13.

28 以下のものを参照。Linda Jakobson, 'China Prepares for an Ice-Free Arctic,' *SIPRI Insights on Peace and Security*, No. 2010/2, March 2010; Aldo Chircop, 'The Emergence of China as a Polar-Capable State,' 7 *Canadian Naval Review* 9 (2011); David Curtis Wright, 'The Dragon Eyes the Top of the World: Arctic Policy Debate and Discussion in China,' Naval War College, China Maritime Studies Institute, No. 8, August 2011 (http://www.usnwc.edu/Research---Gaming/China-Maritime-Studies-Institute/Publications/documents/China-Maritime-Study-8_The-Dragon-Eyes-the-Top-of-.pdf); Linda Jakobson & Jingchao Peng, 'China's Arctic Aspirations,' *SIPRI Policy Paper* 34, November 2012.

29 たとえば、以下のものを参照。Jamse Kraska, 'The New Arctic Geography and U.S. Strategy,' *Arctic Security in an Age of* Climate *Change*, *supra* note 13, pp. 244-266, at pp. 257-258; Lee Willett, 'Afterword: A United Kingdom Perspective on the Role of Navies in Delivering Arctic Secuirty,' *Arctic Security in an Age of Climate Change*, *supra* note 13, pp. 281-298, at pp. 295-296. 石原敬浩「極北のパワーゲーム　対立と協調の構図――中国の進出と米国の動向」『外交』22 号（時事通信社、2013 年 11 月）27-31 頁。

30 たとえば、以下のものから著者の役職・立場上、また掲載されたサイトなどを理由に、公式の見解に繋がる要素が汲み取れると思われる。その趣旨は、北極海周辺諸国が既存のルールに従って国際協力を通じた平和、安定、持続可能な発展をめざして北極の開発を行うということであろう。 News on Ambassador Tang Guoqiang's speech on the Arctic, Chinese Embassy in Norway, at http://no.china-embassy.org/eng/zngx/t654759.htm; 'China's View on Arctic Cooperation', 30 July 2010, Ministry of Foreign Affairs of the People's Republic of China (http://www.fmprc.gov.cn/eng/wjb/zzjg/tyfls/tfsxw/t812046.htm); Tang Guoqiang, 'Arctic Issues and China's Stance', 4 March 2013 (http://www.ciis.org.cn/english/2013-03/04/content_5772842.htm).

31 David Curtis Wright, 'The Panda Bear Readies to Meet the Polar Bear: China Debates and Formulates Foreign Policy Towards Arctic Affairs and Canada's Arctic Sovereignty', March 2011, p. 2 (http://www.cdfai.org/PDF/The%20Panda%20Bear%20Readies%20to%20Meet%20the%20Polar%20Bear.pdf) ; Chircop, *supra* note 28, p. 9; Jakobson & Peng, *supra* note 28, p. 22; Olga Alexeeva & Frédéric Lasserre, 'China and the Arctic', *Arctic Yearbook 2012*, pp. 80-90, at p. 83.中国が国家としてまだ確たる北極政策を有していないことを認めたうえで、昨今の中国における言論が北極関係において活発となっている背景には学界、評論家、軍関係者などが政府に政策の作成を迫る意図があると分析するものもある。Caitlin Campbell, 'China and the Arctic: Objectives and Obstacles,' *U.S.-China Economic and Security Review Commission Staff Research Report*, 13 April 2012, pp. 3-4 (http://origin.www.uscc.gov/sites/default/files/Research/China-and-the-Arctic_Apr2012.pdf).

32 ちなみに、中国の北極に関する外交と南極に関する外交との関係について、これまで参照したもの以外に、以下のものを参照。Zou Keyuan, 'Chapter 12 Chinese on the Poles,' in Zou Keyuan, *China's Marine Legal System and the Law of the Sea*, Martinus Nijhoff Publishers, 2005, pp. 312-337, at pp. 335-337.

33 Alexeeva & Lasserre, *supra* note 31, p. 82.

34 詳細は、以下のものを参照。Kai Sun, 'China and the Arctic: China's Interests and Participation in the Region,'

East Asia-*Arctic Relations: Boundary, Security and International Politics*, Paper No.2, 2013, pp. 2-3.

35 中国にとっては、北極航路の開発による海運の発展があっても、既存の南回り航路等のルートやシーレーンに取って代わるような「新たなシルクロード」にはなりえないという経済データを示す立場もある。Malte Humpert, 'The Future of Arctic Shipping: A New Silk Road for China?', The Arctic Institute, Center for Circumpolar Security Studies, November 2013 (http://issuu.com/thearcticinstitute/docs/the_future_of_arctic_shipping_-_a_n).

36 彼の発言は、「世界人民的共同財富」という言葉で伝えられている。中国語の原文は以下のサイト参照。http://www.chinanews.com/gn/news/2010/03-05/2154039.shtml　尹卓少将の発言の全体は、正確な英文や日本語に翻訳されてきたとは言えない。たとえば、以下のサイトの英文は中国語原文に近いと考えられるが、他の論考で英訳された彼の発言は正確なものとは言えないものも多く、誤解を招きやすいものとなっている。http://chinascope.org/main/content/view/2391/105/

37 南シナ海紛争における断続線の意義について、以下のものを参照。Taisaku Ikeshima, 'China's Dashed Line in the South China Sea: Legal Limits and Future Prospects,' 10 *Waseda Global Forum* (2014) (in press).

38 Alexeeva & Lasserre, *supra* note 31, pp. 83-84.とその中に紹介された文献を参照せよ。

39 Chircop, *supra* note 28, p. 14. カナダとしては、中国との協力関係の増進は好機であり、中国に AC へ関与させることを支持する立場として、以下を参照。Frédéric Lasserre, 'China and the Arctic: Threat or Cooperation Potential for Canada?,' Canadian International Council, *China Papers* No. 11, June 2010, p. 11 (http://www.opencanada.org/wp-content/uploads/2011/05/China-and-the-Arctic-Frederic-Lasserre.pdf).

40 Shiloh Rainwater, 'Race to the North: China's Arctic Strategy and Its Implications,' 66 *Naval War College Review* 62, 77-78 (2013).

41 「中国対北极事务的看法」『世界知识』55 巻 15 号（2009 年）55 頁。

42 日本が 2008 年に国連の大陸棚限界委員会（CLCS）に申請を提出した際に、中国は、申請国が深海底の範囲を尊重し国際社会全体の利益に影響を及ぼさないようにすることを主張する内容の口上書 (http://www.un.org/Depts/los/clcs_new/submissions_files/jpn08/chn_6feb09_c.pdf) を提出している。この口上書に見られる深海底に対する中国の立場は、北極海での沿岸諸国による大陸棚の延伸申請に懸念を示すものと相通ずるところがあるかもしれない。

43 Chircop, *supra* note 28, p. 14.

44 Chircop, *supra* note 28, p. 14; Alexeeva & Lasserre, *supra* note 31, pp. 85-86.南シナ海をめぐる領土権と北極海におけるそれとは、異なるアプローチによるものとされる。 Wright, *supra* note 28, pp. 37-38.

45 Olya Gayazova, 'China's rights in the Marine Arctic,' 28 *IJMCL* 61, 95 (2013).この論考は、本稿では取り上げることができなかった論点の中でも国際法上の重要なものを幅広く詳細に検討している。

46 たとえば、以下のものを参照。Tang Guoqiang, 'Arctic Issues and China's Stance', China Institute of International Studies, 4 March 2013 (http://www.ciis.org.cn/english/2013-03/04/content_5772842.htm); Kai Sun, *supra* note 34.

47 原文は、以下のサイト参照。http://www.oceanlaw.org/downloads/arctic/Ilulissat_Declaration.pdf

48 IMO における 2009 年採択のガイドラインについて、以下のサイトを参照。
http://www.imo.org/blast/blastDataHelper.asp?data_id=29985&filename=A1024(26).pdf

49 原文は、以下のサイト参照。
http://www.arctic-council.org/index.php/en/document-archive/category/20-main-documents-from-nuuk

50 原文は、以下のサイト参照。
http://www.arctic-council.org/eppr/agreement-on-cooperation-on-marine-oil-pollution-preparedness-and-response-in-the-arctic/

51 詳細は、以下の IMO のサイト参照。http://www.imo.org/MediaCentre/HotTopics/polar/Pages/default.aspx

52 NATO の最近の北極海をめぐる安全保障については、以下を参照。Ragnheidur Arnadottir, 'Security at the Top of the World: Is there a NATO Role in the High North?,' Assemblée parlementaire de l'OTAN (http://www.nato-pa.int/default.asp?SHORTCUT=2082).

53 NATO の介入につきカナダの消極的な対応と、沿岸諸国の二国間関係や AC/LOSC といった枠組みの活用を支持する姿勢について、以下を参照。Ibid., p. 11.

54 さしあたり、最近の議論を踏まえたものとして、以下を参照。松竹伸幸『集団的自衛権の深層』（2013 年、平凡社）。

55 安保法制懇によって当時の福田首相に提出された 2008 年の報告書は、以下のサイトを参照。
http://www.kantei.go.jp/jp/singi/anzenhosyou/houkokusho.pdf

56 「記者ブリーフィング要旨」として、以下を参照。
http://www.kantei.go.jp/jp/singi/anzenhosyou2/dai3/yousi.pdf

57 Rainwater, *supra* note 40, p. 76.ほかに、北極海におけるベーリング海峡の安全保障上の意義について、以下のものを参照。Alicia Cerretani, 'US Senate Hearing: "Protecting U.S. Sovereignty: Coast Guard Operations in the Arctic," ' at (http://larouchepac.com/node/20628).

第８章　政策提言

＊各章における政策提言の要約である。

秋山　信将・松本　明日香

０．グローバル・コモンズの「平和」秩序と日米同盟の役割

日米同盟は、世界史的にみて非常に興味深い特色がある。先の大戦で真っ向から対決し、国連憲章が「言語に絶する悲哀を人類に与えた戦争の惨害」と表現した戦争の悲劇とその記憶をもちながらも、戦後においては価値観と利害を共有し、きわめて緊密な同盟関係へと転換したことは、特筆される。また、世界最大の軍事大国といわゆる「平和憲法」を掲げる経済大国との組み合わせで、同盟のパートナーとしての役割が非双務的であることも両者の関係のユニークさを示している。だが、さらに注目されることは、この２つの大国が、同盟を通じ、双方の直接的な国益を追求するだけにとどまらず、アジア太平洋地域の平和と安定に向けた協力やグローバルな視野でのパートナーシップへとスコープを広げ、たったの２ヵ国でいわば国際社会の「公共財」を提供する役割を自認している点である。日本が寛大な接受国になることで、米軍がアジア太平洋地域に相当規模の物理的な軍事プレゼンスを維持することが可能となり、これが地域の秩序の安定材料になっている。そして、日米の連携は、「グローバル・コモンズ」における秩序の形成・維持・発展にも大きな役割を果たすことが期待される。

グローバル・コモンズとは、一般に「どの主権国家のコントロールの下にも入らない公共の領域」と理解され、海洋や宇宙やサイバー空間などが取り上げられている。本研究の焦点は、海洋のなかでも特に地球温暖化による解氷で新たな航路や資源開発の可能性に大きな関心が寄せられている北極海について検討するとともに、宇宙とサイバー空間での新たな動きを分析する。その際、出発点となるのは次の２つの見方である。まず第１は、グローバル・コモンズが、たとえ大国であっても自らのコントロールの下に置くことができないほどの新たな国際政治のフロンティアであることから、このグローバルな公共領域において、多様な主体の間で、互いの利害の相違の調整や共通の利益の促進のための公共秩序－グローバル・ガバナンス－が求められていることである。そして、第２には、グローバル・コモンズが新たな国際政治のフロンティアであったとしても、そこで繰り広げられる活動は、きわめてクラシックなリアル・ポリティークの延長である場合も多い、という点である。グローバル・コモンズの制度設計には、新興国、特に台頭する中国をいかに取り込んでいくかが重要な課題となるだろう。同時に、数多くの非国家の主体も加わり、匿

名性のヴェールの下でつばぜりあいが続くサイバー空間における安全保障のためにも具体的な取り組みが求められる分野である。

実際、いまほど、日米両国が、他の国々や非国家の主体も巻き込み、グローバルな公共領域の秩序の形成・維持・発展において主導的な役割を果たすことを求められているときはない。これは、とりもなおさず、グローバル・コモンズにおける「平和」を確保しようとする営みにほかならない。すなわち、日米両国は、一方でグローバル・コモンズにおける自由な活動を擁護しつつ、そうした自由を乱用し、有害な活動をしようとする主体の動きを制限する仕組みづくりに取り組む必要がある。

グローバル・コモンズにおける公共秩序を提供するガバナンスの制度は、国家と非国家の主体が共に参加し、フォーマルなものからインフォーマルなものまで多様な形態をとらざるを得ないだろう。しかし、その際のボトムラインとなる考え方は、サイバー空間や宇宙､北極海を含む海洋といったドメインごとの固有の課題に対応する場合でも､あるいは、グローバル・コモンズを包括的・横断的に理解し、その「平和利用」を促進するという場合でも、グローバル･ガバナンスを促進するうえで不可欠の 5 つの要素、すなわち、知識、規範、政策、制度、順守のそれぞれの分野における共通の認識の拡大に向けて積極的に提案をしていくことである。日米両国は、同盟関係を最大限に活用し、さらに最先端の技術的なエッジを外交上のテコとして、こうした秩序形成のための交渉や協議のプロセスのかじ取りにおいて大きな役割を有していることを改めて認識すべきだろう。

以下は、本研究でとりあげるグローバル・コモンズの各ドメインにおける安全保障およびガバナンスの推進と日米同盟の役割に関する主な政策提言として本報告書の各章で指摘されたものをとりまとめたものである。

１．サイバー空間

（１）サイバー空間における安全保障面

従来、アメリカの防衛・安全保障コミュニティでは、いくつかの理由によって懲罰的抑止力の構築は難しいと考えられてきた。しかし､現在ではサイバー攻撃の発信源を特定し、報復を示唆するような抑止力が整備されつつある。こうしたサイバー空間の防衛・安全保障政策の変化､つまり懲罰的抑止力の追求を前提に､日米同盟も適応していく必要がある。

日米同盟のサイバー抑止力強化のため、3 つの政策提言がある。

a) 政策：中国発のサイバー攻撃を「フルスペクトラム」で評価する

サイバー抑止強化に向けた同盟変革は日米同盟の中核機能、つまり対中抑止の文脈で検

討する必要がある。中国発のサイバー攻撃、すなわち平時におけるスパイ活動（exploitation）から有事における兵站・指揮通信システムへの攻撃をフルスペクトラムで評価し、抑止力による対処の範囲を設定することが必要である。

b) 法的基盤：「どの時点で」武力攻撃を認めるのか

個別であれ、集団的であれ、サイバー空間における自衛権行使の要件は「通常の武力攻撃と同程度の損害を与えるか否か」という点に収斂する。あるサイバー攻撃を結果的に「武力攻撃」相当と認定できるかもしれない。しかし、どの時点で「武力攻撃」相当と認定するかは難しい問題である。結局のところ、「どのようなサイバー攻撃が戦争行為なのか」を決めるのは政治的判断であり、それは軍事的決定や法的決定以上に重要である。そうした権限を予め決めておく必要がある。

c) 運用：2 つの「世界と言語」が理解できる人材を確保する

最後は日米同盟のサイバー抑止力を維持するための運用である。日米同盟のサイバーセキュリティ強化には「スーツ」と「ギーク」、2 つの世界と言語を理解する人材が必要とされている。「スーツ」、つまり防衛・安全保障政策の形成者達には独特の価値体系や専門性がある。一方で「ギーク」、つまり情報セキュリティの世界や言語も同様である。両者の価値体系と専門性を備えた人材を育成する必要がある。

（２）サイバー空間におけるガバナンス面

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出している。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。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ーの確保とともに、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。

２．宇宙

（１）宇宙空間における安全保障面

宇宙利用をめぐる脅威への対応は米国においても緒に就いたばかりであり、日米で検討していかなければならない課題も多い。そうした課題としては、例えば、宇宙監視にとどまらない宇宙状況監視（Space Situational Awareness: SSA）協力の推進、日米の宇宙活動能力を活用したレジリエンスの強化、宇宙と抑止の結びつきに関する検討（特に日本側）といったことが挙げられるだろう。

現状において日米 SSA 協力の中核となっている宇宙監視（space surveillance）に加えて、各種インテリジェンス活動を通じて得られた各国の宇宙活動に関する情報を緊密に共有していくことが重要となってくるだろう。SSA とは宇宙作戦が依存する宇宙環境および作戦環境に関する知識（knowledge）のことであるが、日本側はこうした知識の蓄積を始めたばかりである。今後は米国等との情報交換を通じて、各国の宇宙活動や宇宙利用をめぐる脅威などに関する認識の向上を図っていく必要がある。

またレジリエンスの強化は米国のみならず日本にとっても主要課題となりつつあることから、将来的には SSA と並ぶ日米協力の柱となる可能性がある。日本は数少ない自立的宇宙活動国のひとつであり、実際に多数の衛星を製造し打ち上げてきた実績を有している。この点は、これまで米国が安全保障分野における宇宙協力を緊密に進めてきた国々にはない日本の強みであり、これらの国々とは異なる形での対米協力もあり得るだろう。

最後に、宇宙と抑止の結びつきについては、特に日本側における検討を加速させる必要がある。すでに米国においてはレジリエンスと並ぶ柱として抑止が位置づけられており、抑止の強化に向けた取り組みが行われている。日本が進めている外交的手段を通じた規範の醸成や衛星の抗堪性の強化も、宇宙システムに対する攻撃を抑止する手段として位置づけ直すことが可能である。こうした点については米国との緊密な意見交換を進めながら概念整理を進めていく必要があるだろう。

（２）宇宙空間におけるガバナンス面

今後、グローバル・コモンズである宇宙空間を利用し、そこから社会経済的な利益を享受し、安全保障上のシステムを安心して運用できるようにするためには、このグローバル・コモンズを管理するガバナンス構築における影響力競争において有利な立場にいることが重要である。それによって宇宙利用の主導権を握るだけでなく、広く社会経済的、安全保障上の利益も確保することになるからである。そのためにも、日米同盟が有効に機能し、自らの利益に即したルール作りを進めている現状を継続していくことが重要である。

たとえば、日米同盟は EU が提案した「宇宙の行動規範」を巡る国際ルール作りにおいても重要な役割を果たした。一方で 2007 年に衛星破壊（Anti-Satellite: ASAT）実験を行った中国や、中国と共に「宇宙空間への兵器配置および宇宙空間物体に対する武力による威嚇または武力の行使の防止に関する条約（Treaty or the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects : PPWT）」を提唱するロシアを国際ルール作りの周辺に配置することとなり、より軍事的重要性を増した宇宙空間の利用に関する国際社会の規範作りにおける影響力を巡る競争にも強い影響を与えている。

「グローバル・コモンズ」としての宇宙空間を持続的に利用するためには、それを利用する主体がすべての情報を開示するとともに、地球軌道上を周回する物体を可能な限り多く探知することができる能力を、グローバルにもつことが必要となってくる。「グローバル・コモンズ」である宇宙空間の、グローバルなガバナンスの仕組みが必要である。

今後のグローバル・コモンズとしての宇宙ガバナンスには 3 つの課題がある。

a）技術革新による環境の変化

大型衛星の技術開発が継続される一方、小型衛星に機能を分散させ、より多くの頻度で打ち上げることによってリスクを分散させるという方向性が出てきている。こうした衛星の小型化は軌道上の物体が増加し、軌道がいっそう混雑することも意味している。こうしたなかで衛星同士の衝突を回避するためにも、SSA 体制の構築と情報共有の仕組みの構築がより重要となる。

b）衛星の小型化に伴い、技術がより単純化し、陳腐化

高い技術をもつ国のみが持ちえた宇宙利用の可能性を、より技術力の低い国にも広げることとなり、大学レベルでも衛星の開発・運用が可能になることを意味する。それはすなわち、これまでの少数によって構成される「宇宙クラブ」のルールである「宇宙の国際行動規範」を、新規参入してくる多くの主体に認知させ、宇宙空間のガバナンスを徹底することを必要とする。しかし、そうした役割を誰が担うのか、また、法的拘束力のない「行動規範」で十分なのか、といった問題が提起される。

c）宇宙空間における兵器化の進展

物理的な破壊へのインセンティブは下がるだろう。しかし、ジャミングや電子的な攻撃、さらには自然現象としての太陽風による障害といった問題もある。これらの攻撃や自然現

象によって衛星の機能が停止したとしても、それがどのような原因で行われ、誰にその行為の責任が帰するのか、といった判定をすることはきわめて難しい。衛星自身の故障による不具合という可能性も常に残る。

これらの問題についての解決はまだ明らかになってはいない。しかし、これらの問題に対処するためにも、国際的なルール作りと、SSA による宇宙状況の把握はきわめて重要であり、これらを実現するためには強固な日米同盟を軸にしつつ、グローバル・ガバナンスの構築に向けた各国との協力が不可欠となるのである。

３．北極海

（１）北極海における安全保障面

北極海の変容に伴う国際情勢の変化に対し、安全保障・防衛面の視点から、今後わが国として採るべき対応は何か。短期的には、北極海航路の利用について、国際潮流を見定めつつ、海上交通路の利用を積極的に推進する方向で政策を進めていくべきであろう。また世界有数の海洋国家として、国際的ルール作りへの参画も死活的に重要となる。即ち「北極海の利用と国益に沿った外交政策の推進」が、短期的に日本の採るべき対応となる。

一方、海洋立国たる日本が、安全保障・防衛面の視点から、中、長期的に採るべき対応としては、北極海を視野に捉えた安全保障・防衛政策の見直し、即ち、「防衛体制の見直し……自律防衛能力の強化」、「日米防衛協力体制の見直し……日米同盟の深化」さらには「関係友好国との海洋安全保障協力の推進……海洋安全保障協盟の構築、拡大」を行うべきである。具体的には下記の通りである。

a) 防衛体制の見直し……自律防衛能力の強化

中、長期的な北極海を視野に捉えた防衛体制見直しの方向性としては、自律防衛能力の強化を図ることが適当である。まず、北極海方面をもカバーする戦略情報収集能力強化のための監視衛星、無人航空機（UAV）、C4ISR などの整備が求められることになろう。将来的に、艦船や航空機などの北極海での行動海域が拡大することに伴い、戦略、戦域対潜能力の拡大、強化が必要となり、その能力を有する艦艇や航空機の増勢に加え、UAV や無人水中ビークル（UUV）の効果的利用が求められよう。さらに弾道ミサイル防衛（CBMD）能力の拡大、強化も必要となり、イージス艦の増勢なども検討の必要性が生じよう。一方、北極海での艦船や航空機の行動を念頭に置けば、砕氷救難機能確保のため、砕氷救難艦や氷洋救難機の整備、北極海や北方海域仕様の艦船、航空機の整備、同方面での海象・気象情報の収集、分析機能の保有も必要となろう。

また、日本海や3 海峡防衛体制の強化はもとより、北海道周辺海域、北方海域、北極海での行動能力強化が必要となるため、同方面での自衛隊の情報収集体制の強化、C4ISR の整備、北方行動に適した艦船や航空機の装備、後方支援や運用面での改善、強化といった対策の検討も必要となろう。

b) 日米防衛協力体制の見直し……日米同盟の深化

現行の日米同盟体制では北極海問題は想定外となっているが、北極評議会の加盟国である米国との密接な関係構築は、日本の北極海利用における安全保障・防衛面にとって意義がある。米国の核抑止力を含む北極海安全保障体制強化への多角的な支援を、日本が行うことが可能となれば、日米安全保障体制の双務性向上に寄与するだろう。核抑止を中心とした日米露の 3 ヵ国安保・防衛協力の強化も、以前に比べ現実味を増し、重要となろう。

日米防衛協力指針の改定のなかで、戦略情報共有、C4ISR、BMD、対潜水艦戦、捜索救難、人道支援、災害救援といった側面で、北極海の安全保障に関連する防衛協力の強化を含め、日米同盟のさらなる深化を図ることは大いに意義があろう。この際、北極海を巡る安全保障・防衛面での情勢の変化にあわせ、日米防衛協力指針を、都度、改定または一部修正することが求められる。集団的自衛権の行使とも深く関連する。

一方、指針の改定または一部修正に伴い、指針に直接関連する法体系である周辺事態安全確保法や船舶検査法の改定など、国内関係法の改定が必要となる可能性がある。また、国家安全保障会議（JNSC）の指導、監督の下、関係省庁間の情報共有や運用面での協力の強化が必要となる。

c) 関係友好国との海洋安全保障協力の推進……海洋安全保障協盟の構築、拡大

日本は戦略的な観点から、「国際協調主義に基づく積極的平和主義」を具現化するため、北極海問題に関しても、安全保障・防衛面での協調路線をとっていくことが求められる。遠隔の地にある関係友好国に対し、北極海での捜索救難などでの可能な範囲での積極的な協力を約束し、その見返りに、日本にとっての遠隔海域での海洋安全保障協盟（有志連合：コアリション）の参加国との連携による広域かつシームレスな海洋安全保障協力により、長大な海上交通路の安全保障を確保することが可能となるよう、これら関係友好国との協調関係を維持していくことが得策である。

（２）北極海におけるガバナンス面

北極海周辺諸国と日本という多数国間関係（場合によっては、北極周辺の各国と日本と

の二国間関係を含む)、日本と米国との二国間関係などの他にも、北極に関与する他の諸国（非北極諸国：non-Arctic states）と日本との関係をも考慮した上で、日本の立ち位置を見極め、将来の課題に対処することが求められている。

北極海においては、バイラテラルな日米同盟を基礎とした集団的自衛権をも含むような安全保障の概念を北極海にまで拡張して考えたり、この二国間関係を全面的にまたは中心に安全保障を捉えたりするよりも、むしろ非伝統型安全保障のための国際協力として、北極評議会（AC）を始めとした多数国間の枠組みを中心に、既存の海洋法や、捜索救助、緊急対応に関連する多数国間合意に基づいた対応として、日本の国際協力として現行法制下で可能な範囲を探ることをまずは検討する方が現実的である。そして、上記の検討内容が、米国自身が日本に期待する日米同盟のあるべき姿とも合致するか否かをよく見極める必要がある。