はしがき

本報告書は、当研究所の平成 26 年度外務省外交・安全保障研究事業（調査研究事業）のひとつである「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」の研究成果として取りまとめたものです。

本プロジェクトでは、サイバー空間、宇宙、北極海という世界共通の課題（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・学を合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）を活かしながら果たすべき役割等を検討し、採るべき施策について提言を行っています。

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になっている一方で、国家及び犯罪グループによる攻撃の脅威に常にさらされています。また、宇宙空間は、かつての米ソ冷戦時代は 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って利用可能なものとしつつあります。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、これらの空間の安全を確保し、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。

日米同盟は過去 50 年以上の長きにわたって日米の安全、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、世界の中で日本がより積極的な役割を果たすべき課題でもあり、本報告書ではこうした議題に対する解決策についても議論がなされています。

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が、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 27 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	大阪大学副学長（海外展開担当）兼 大学院国際公共政策研究科教授
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	東京海上日動リスク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
	宮田　智之	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：「アクロス・ザ・ユニバース」の安全保障
－グローバル・コモンズにおける「普遍的な平和」とは－

星野　俊也

１．はじめに－「グローバル・コモンズ」を超える安全保障論

巨匠スタンリー・キューブリック監督と SF 界の重鎮アーサー・C・クラークが手を組んで製作し、1968 年に公開された映画『2001 年宇宙の旅（2001: A Space Odyssey）』で描かれた 21 世紀初頭の世界では、人類は月面基地を持ち、往還には地球の軌道上に建設途上の宇宙ステーションまでは民間航空会社がスペースプレーンを運航し、そこから宇宙船に乗り換えることになっている。さらに、人類は、宇宙の謎を解明するため、人工知能を備えた最新鋭のコンピューターを搭載した有人宇宙船ディスカバリー号で木星探査に乗り出していく。

現実の 21 世紀を迎えた我々は、宇宙ステーションまでは手にしていても、映画とは違い、そのなかに大手のホテル・チェーンが経営する宿泊施設もなければ、航空会社によるシャトル便もない。有人宇宙探査は繰り返されているが、人工冬眠をしながら銀河系の彼方に向かうミッションまでは実現できていない。しかし、我々にとって宇宙はもはや遠い存在ではない。テレビの天気予報や衛星放送、GPS（全地球測位システム）機能を持つスマートフォンやカーナビの例を出すまでもなく、大気圏外の宇宙を利用したサービスはすでに日常生活の一部になっている。もちろん値段は張るが、弾道飛行による宇宙旅行の予約を受け付ける企業も出始めた。他方で、ロケットや人工衛星の低価格化の動きもある。

科学技術の進歩は、我々の生活空間を確実に広げている。実際、物理的な活動領域は陸海空から宇宙に広がったのみならず、サイバー空間と呼ばれる仮想の領域でのコミュニケーションやトランザクションがなければ不便きわまりないほどにまでライフスタイルは変わってきている。

我々の活動する領域（ドメイン）の広がりは、生活を便利で豊かにしてくれる。他方、便利さへの過度の依存はそのシステムが不安定化した際のリスクの波及度に直結する。また、豊かさは、その資源が限られていればいるほど、利害は競合し、調整が必要となる。

本研究では、今日の世界で一般に「グローバル・コモンズ（global commons）」と認識されることの多い地球社会の公共領域に関し、特にそのなかでもサイバー空間、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、さらにこれらの領域において公共秩序を提供する「ガバナンス（governance）」の体制のあり方―特に「安全保障ガバナンス

（security governance）」の側面―を検討し、さらにその過程において日本は同盟国である米国とともにいかなる役割を果たすことができるのかについて考察することを目的としている。本章に続く各章では、サイバー空間、宇宙、北極海という個々のドメインにおける関係主体の動きやガバナンス形成に向けた状況、及び日米同盟が果たしうる役割が議論される。そこで、総論となる本章では、今日、急速にその利用が活発化している 3 領域をあえて「グローバル・コモンズ」と概括することによっていかなるものが見えてくるのか、サイバー空間、宇宙、北極海という 3 つの領域での動きを相互に関連させながら議論することによって見えてくる特徴や課題をあぶり出し、それを日米同盟の文脈に位置付けることを試みる。

２．「新たな戦略ドメイン」のリアル・ポリティーク

安全保障政策のディスコースのなかで「グローバル・コモンズ」という表現が使われ始めたのは、米国のオバマ政権が発表した『4 年ごとの国防戦略見直し（QDR）』（2010 年 2 月）[1]や『米国国家安全保障戦略（2010 年版）』（同年 5 月）[2]などであり、海洋と宇宙とサイバー空間を例に、新たな脅威に対応する米国の体制強化の必要が論じられた。かかる動きに呼応し、日本では第二次安倍政権が新たに取りまとめた『国家安全保障戦略』（2013 年 12 月）のなかで海洋、宇宙空間、サイバー空間を「グローバル・コモンズ」（同文書では「国際公共財」という訳語が付けられている）と位置づけ、新しいタイプのリスク要因に対し、これらの領域での法の支配の実現・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への努力の必要を指摘した[3]。

もっとも、海洋、宇宙、サイバー空間と並べたところで、これらを一括りにして「グローバル・コモンズ」と表現することの適否の問題がある。また、そもそも定義も明確ではない。したがって、何をもって「グローバル・コモンズ」とするのかについても決してコンセンサスがあるわけではない。実際、この概念を最初に提起した米国の『QDR』のさらに 4 年後の報告書（2014 年 5 月）を見ると、わずか 1 回、何の説明もなく結論部分で「グローバル・コモンズの保全」という言葉が出てくるほどにまでトーンダウンしている[4]。海洋や宇宙、サイバー空間をまとめて表現している場所が一か所だけあるが、それは「競合の度合いが高まっている戦闘空間（increasingly contested battlespace）」と、別のかたちで表現されている[5]。また、2015 年に刷新された『米国国家安全保障戦略』文書では、もはや「グローバル・コモンズ」という言葉自体は消え、サイバー安全保障、宇宙安全保障、及び航空及び海洋の安全保障については、世界を結び付ける「共有空間（shared spaces）」と呼び、米国として「これらの共有空間へのアクセスを確保する能力を保有する一方、責任ある行

為に向けたルール作りを促進していく」との方針を明らかにしている[6]。

こうした用法の変化を見る限り、似たようなグローバルな意味合いをもつ“共有空間”ではありながらも、サイバー、宇宙、海洋といった各ドメインにはそれぞれ独自の力学が働いているがゆえに、並べて論じるよりも個別に精査したほうが合理的で現実的と考える見方が復権しているように思われる。実際、宇宙や海洋は自然空間であるが、サイバー空間は人工的なものであり、質的に異なっている。また、これらの領域では「共有地」と言えるような条件は成立していない、あるいは所有権が競合・対立する領域と見る方が適切な状況もあるだろう。他方で、新たにその重要性がクローズアップされてきたこれらのドメインにおける政治過程を相互に比較・対照しながら検討することによってこそ見えてくるものもあるに違いない。なぜならば、「安全保障」の観点から見るならばなおのこと、これら3領域には、地球規模での波及効果を持つ3つのリスク要因―開放性、連結性、非対称性―を、ある程度共通して指摘できるからである。

第一に、開放性とは、コモンズ概念の最も基本的な特質である自由なアクセスの原則に関わるものである。当該ドメインにおいて、明確な所有権が確立している部分は別にしても、共用できる部分においては、資源やサービスや便益については誰もが自由にアクセスでき、誰もが排除されない環境が想定されている。仮に機会は均等に提供されていても、実際にそれを活用できるかどうか、そして、その活用において自己の利害と全体の利害とをいかにバランスさせるかは、行動する主体の能力と意思による。宇宙空間への参入障壁は低くなっているが、まだ海洋ほどではない。一方、海洋のなかでも北極海への関心の急速な高まりは、そこが行く手を氷が阻む難度の高い厳寒の海であったものが、気候変動による海氷面積の減少でより多くの主体の航行が予想されるようになってきたためである。そして、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、いかにその秩序を維持していくか（例えば、悪質な行動や、自由なアクセスを阻害する行動の制限など）が重要な課題となる。

第二の連結性とは、我々の社会生活がいまやグローバル・コモンズを構成する領域によって連結された世界のなかで成立していることを意味している。言い換えるならば、グローバル・コモンズと認識される領域には、自己と他の主体との間を連結する社会インフラとしての役割があるということである。ここから、悪意を持った主体が開放的で相互に連結されたドメインを通じて相手の安全保障の中枢に侵入してくるリスクや、安定的・恒常的な連結が作為・不作為によって遮断されるリスクなどを想定しておくことが重要となる。

第三の非対称性によるリスクとは、総合的な実力から言えばむしろ劣勢にある主体が、グローバル・コモンズの開放性や連結性を乱用ないし悪用し、より優勢な地位にある主体

の利益を脅かしうるような状況に関わるものである。最も象徴的なものは、テロリストや暴力的過激主義集団のような非国家主体がサイバー空間での攻撃を行うことで大国の社会インフラをかく乱しうるような状況や、海洋や宇宙において新規参入の後発主体の行動が、先行する主体の大規模投資を揺るがすような状況などが想定される。実力の非対称性や被害の非対称性は、いわゆる抑止を通じた安定の確保を困難にする。

以上の考察を踏まえるならば、グローバル・コモンズをいかに定義するにせよ、なぜいまそうした領域における安全保障ガバナンスの構築・整備・発展を進めていかなければならないかが理解できるのではないだろうか。

実際、サイバー空間や宇宙、北極海がその最も先鋭的な例となるわけだが、これらの領域が世界の安全保障環境に計り知れないほどのインパクトを与えうる「新たな戦略ドメイン」として注目を集めるなか、そこでの制度の整備状況との間には著しいギャップがあることがわかる。そのことは、とりもなおさず、一見新しい分野と思われがちなこれらの各ドメインで、関係主体間のリアル・ポリティーク（現実政治）が繰り広げられていることを意味しているのだろう。

３．グローバル・コモンズの制度ギャップと主体の責任

前述のようにグローバル・コモンズには明確な定義がなく、一般的には特定の主権国家のコントロールの及ばない公共の領域と考えられているが、そうした領域に秩序を提供することはかえって難しい。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、グローバル・コモンズは最もアナーキカルで脆弱かつデリケートな領域になりかねない。しかも、実力をつけた新興国家や国際ルールをものともしない非国家主体の台頭などもあり、状況はさらに複雑化している。しかし、サイバー空間にしろ、宇宙にしろ、北極海にしろ、そうしたドメインは、いまや我々の社会や生活に深く入り込み、“日常化”している一方で、制度構築においては決定的な遅れ（制度ギャップ）が生じている[7]。他方、それほどのインパクトのある戦略ドメインであれば、制度が未整備のうちに最大限の利得を得ようとする動きや、新制度を自らの都合により多く近づけようとする動きが出てきても不思議はない。グローバル・コモンズにおける安全保障ガバナンスを議論する理由がここにある。

では、いかにして安全保障ガバナンスの構築・整備・発展を進めていけばよいのだろうか。その出発点として、本稿では、サイバー空間や宇宙、北極海を含む海洋を念頭に、グローバル・コモンズをさしあたり「グローバルな開放性と連結性を持ち、国家・非国家の多様な主体の間で、共通の事項の管理（＝共通の利益の促進や相互の利害の調整）のため

の制度の構築・整備・発展が進められている公共性の高い領域」と操作的な定義をしておきたい。そのうえで、サイバー空間や宇宙、海洋といったそれぞれの分野で制度は形成途上だが、相互に参考にすべき規範や行動基準、ベスト・プラクティスを見出すことは不可能ではないだろう。ここでは、既存の国際法ルールを適用できるものもあれば、まったく新しいルールを編み出す努力が必要な場面もある。個々のドメインにおけるガバナンスの形成状況は他の章で議論されているが、ドメイン横断的にグローバルな公共領域における制度ギャップを狭めるための一連の公共政策（＝グローバルな公共政策 global public policy）の立案・形成・実施をしていくのであれば、当面、次のいくつかの点について着目していくことが重要である。

第一は、グローバルな開放性と連結性という固有の特質を持った公共のドメインにおいて基本となる「共通の事項の管理」とは何かを確認することである。総じて、それは、開放性や連結性がもたらす正の価値（＝公共善 public goods）を維持・拡大し、負の価値（＝公共悪 public bads）を軽減・除去していく政策努力であり、そのために関係主体（国家、民間事業者、さらには個人）間の共通の利益の促進と相互に重複する利害の調整を進めていく必要がある。

関係主体間の共通利益という観点からは、やはり「各ドメイン（宇宙、海洋、サイバー空間）内及び各ドメイン間での平和と安定の維持・前進」が出発点になる。そして、どのドメインにとっても共通する根源的な原則を改めて一つ打ち出すとするならば、それは、グローバル・コモンズの「平和利用」ということになるだろう。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合うグローバルな公共領域での、それは基本的な「マナー」に関わる姿勢である。自由なアクセスが担保されるかわりに「有害行動」を互いに禁止し合う原則を打ち立てていくことは、それが明文化されようと暗黙の理解にとどまろうと、最も基本的な要件である。宇宙、海洋、サイバーの各ドメインにおいて、何が有害行為であり、どこまでが無害の範囲内かは個別に議論されてしかるべきであるので、ここでは立ち入らない。他方、宇宙と海洋については、それぞれ国家間で権利・義務・責任を規定した国際条約がある。これに対し、サイバー空間においては個人や民間事業者の関与も大きいことから、国家に期待される役割と民間人・団体の果たすべき役割のバランスの問題から議論していかなければならない部分が多い。日本や欧米諸国が民間ベースのルール作りを支持しているのに対し、ロシアや中国がより国家の関与を強めた制度を求めていることはよく知られているところである。

もちろん、これらは新しい領域ではあっても、すでに主体の戦略的な利益が関わり、主体間のリアル・ポリティークが展開する世界である。グローバル・コモンズの当該ドメイ

ンにおける各主体の間では、公共善を伸ばそうとする政治的意志と、それとは逆に、公共悪につながるような政策オプションであってもそれを温存しようとする政治的意図とがない交ぜとなる現実のなかで、「安全保障ガバナンス」を構成する「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となっていく。「社会的なアレンジメントとしての責任」という言葉は、「共有地の悲劇（The Tragedy of the Commons）」と題する論文で、関係主体が互いに「共有地」として認識する場所で、それぞれが自らの利得を最大化しようとする合理的な選択を進める結果、全体としては共有地の荒廃という悲劇が生じるパラドックスを論じた際に用いたものである[8]。開放性と連結性がグローバルな公共領域の特性であるとするならば、主体の行動によっては、正の価値も負の価値もグローバルに波及する可能性がある。したがって、各主体が「責任」（道義や節度に裏付けられた責任）を自覚した行動をとれるかどうかが試されることになる。

個別の政策オプションについては、本章では論じないが、各ドメインにおいて問題の所在を的確に認識し、共通規範の形成や信頼醸成の促進、さらに万一、緊急の事態が発生してしまった場合の有効な対抗策を議論していくことが、ここでの作業となる。既存の国際ルールでいえば、有害行動の最も極端な例として、グローバル・コモンズにおける武力攻撃事態にいかに取り組むか、被害を受けた主体による個別的・集団的な自衛権の発動はいかなるかたちをとるのか、また、国際社会全体としての集団安全保障のメカニズムは用いられるのかなど、法の支配に基づく検討は深めていかなければならない。

特にサイバー空間においては、何をもって「武力行使」とするのか、そして武力行使事態が確認された際に、サイバー分野においての自衛権行使とは何を意味するのか、「集団安全保障」のメカニズムを適用することはできないのか、といった議論、さらには、「武力行使未満」のグレーゾーンでの行動であっても標的とされた主体に甚大な被害を及ぼすような事態が発生した場合、あるいは、民間事業者が管理・運営する重要なインフラへのサイバー攻撃が仕掛けられた場合、当該国としてどのように位置付けるのか、などの論点については、さらなる検討が求められるだろう。

４．おわりに－「アクロス・ザ・ユニバースの平和と安全」に向けた日米同盟の役割

本章では、サイバー空間や宇宙、北極海を含む海洋をあえて「グローバル・コモンズ」と見るマクロの観点から、それらの領域における安全保障ガバナンスの必要性や国際社会としての取り組みのあり方について論じてきた。グローバル・コモンズをさしあたり、「グローバルな開放性と連結性を持ち、国家・非国家の多様な主体の間で共通の事項の管理（＝共通の利益の促進や相互の利害調整）のための制度の構築・整備・発展が進められている

公共性の高い領域」と操作的な定義をし、そのなかで関係主体（国家、民間事業者、場合によっては個人）が互いに参画し、グローバルな公共政策を通じて「社会的なアレンジメントとしての責任」を発展させていく必要性も検討した。では、最後に、こうしたガバナンス形成のプロセスにおける日米同盟の役割についても概観したい。

今日の世界においては、宇宙、海洋、サイバーのどのドメインをとってみても米国がその実力（技術・規模・行動）において圧倒的に優勢な地位にあることは誰もが認めるところだろう。これだけをとっても、米国がグローバル・コモンズにおける「社会的なアレンジメントとしての責任」を踏まえ、リーダーシップをとっていくべき立場にあることが期待される。また、これらの各ドメインのなかで米国の存在が大きければ大きいほど、当該ドメインにおける平和と安定の維持（特に、ドメイン内での有害行動の排除を通じた平和利用の促進）において果たすべき役割も広がっていく。しかも、米国が、その存在感の大きさから、各ドメインにおいて挑戦を受けるケースも多いことを考え合わせれば、米国にとってもグローバル・コモンズにおける安全保障ガバナンスの発展は、国益につながるものである。

もっとも、グローバル・コモンズの最大の特徴は、たとえいかなる大国であったとしても一国のみでそれをコントロールできないほどの広がりをもつ領域であることだった。しかも、米国は深刻な財政危機を抱え、強制歳出削減によって国防支出にも一定の制限がかけられるようになると、同盟国や友好国との協力関係がクローズアップされるのは無理からぬことである。日本は、米国と同盟関係を組み、そのスコープは日本の防衛に加え、アジア太平洋地域の平和と安全や、さらに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」的な役割をも含むようになってきている。グローバル・コモンズにおける平和と安定に向けた努力は国際公益に向けた日本の貢献でもあるが、同時に、多くの場合、米国と協力していくことで効率的に伸ばすことのできる日本の国益に直結する活動とになっている。

では、日本は何がどこまでできるのか。宇宙、北極海を含む海洋、そしてサイバー空間という 3 つのドメインを見渡して日本の果たしうる役割を考えるならば、日本もこれら 3 つのドメインでは実力面で米国には依然はるかに及ばないとしても、世界有数の大国として、きわめて大きなステイク（利害）を有する国であることがわかるだろう。実際、日本の宇宙開発活動は急速に拡大している。島国・日本にとって世界の海洋は命綱でさえある。さらにサイバー空間の安定なしに日本の社会・経済基盤は成り立たなくなってきている[9]。これだけとっても、日本が米国と協力をしてグローバル・コモンズにおける平和と安定を実践していく意義がある。

日本は、自らの能力を過信すべきではないが、決して米国の優位を前に自らを卑下する必要はない。何よりも日本には、輝かしい技術力がある。極東の大陸の沖合に南北に伸びる地理的位置にあり、米軍の駐留を受け入れている役割も大きい。宇宙関連事業でも、先進的なロケット発射能力を含む優れた実績を持つ。とは言え、日本が国際社会の規範やルール形成のプロセスに機敏かつ柔軟に参画できていないケースも散見される（例えば、米欧の専門家がエストニアの首都タリンでサイバー空間の行動基準のあり方等についてまとめた「タリン・マニュアル」の作成過程に日本は十分に参加していない）。

日本と米国の立場が常に一致するとは限らない。しかし、日本は、軍事同盟であるとともに政治同盟であり、また価値の同盟でもある日米同盟の枠組みのなかで米国との意見調整を進め、さらに、官民一体の「オールジャパン」体制で立場を集約し、グローバル・コモンズに新しい制度の形成・実施・発展にダイレクトに参画し、リードする主要な一国として今後、存在感を高めていく必要がある。もちろん、米国のほか、英豪加といった国々との連携も重要である。そして、さらに日本としては、中国やロシア等、宇宙や海洋、サイバー空間での問題認識や行動様式において米欧諸国と時に立場を異にする国々とも前提条件なしに、率先して対話と協議を重ね、共通の理解を広げていくべきだろう。

21 世紀の世界はかつての SF が描いたほどには科学技術が進んでいるようには見えないが、人々の生活を取り巻く安全保障の地平は、陸上から海洋、空、宇宙といった自然空間のみならず人工的に構築されたサイバー空間にまで広がっている。しかも、バーチャルな情報空間を生み出すインターネットであっても、その実は地上や海底のケーブルによってつながっていたり、宇宙から送られてくる衛星情報が陸上や海上や航空の管制に用いられたり、インターネット空間を通じた情報のやり取りが経済や社会の基盤的なインフラを維持していたりと、各領域は我々が想像する以上につながっている。言い換えるならば、我々は、この地球に暮らしながら、宇宙空間や目に見えないサイバー空間の出来事とも不可分の、より大きな世界（ユニバース）の安全保障のデリケートなバランスのなかで生きているのである。

この世界に「グローバル・コモンズ」などという領域は存在しない、と切り捨てることは簡単である。しかし、仮にグローバル・コモンズと呼べるような戦略的な領域（ドメイン）が複数存在し、それらが相互に連結し合っていると仮定するならば、そこから安全保障の新しいヴィジョンを見出すことは決して無意味ではない。そのヴィジョンとは、個々の主体（国家・非国家の両方）が自らの安全を保障するためには、自らの力だけでは安全を確保できない公共の物理的・仮想的な領域の平和と安全をも確保するための共同の責任（＝相互に有益な行動を促し、相互に有害な行動は制御する責任）を認識することが必要

であり、さらに、そうした公共の領域の安全保障が地球と宇宙とサイバー空間といった境目を飛び越えたさらに大きな世界（ユニバース）における地政学と密接に結びついている、というものである。したがって、人間の行動のスコープが格段に広がった 21 世紀におけるより「普遍的な平和」を担保していくための制度を設計していくためには、主体ごと、あるいはドメインごとの安全保障に向けた体制づくりは当然だが、それにとどまらず、各主体やドメインの間の相互連結も十分に視野に入れ、我々を取り巻く世界全体の安全保障をより領域横断的に捉え直す―いわば「アクロス・ザ・ユニバース」で考える安全保障の―体制を整備していく視点にもしっかりと目を向けていくべきなのである。

－注－

1 U.S. Department of Defense, *Quadrennial Defense Review Report*, February 2010.
http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf
http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf

2 The White House, *National Security Strategy*, May 2010.
https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

3 『国家安全保障戦略について』（2013 年 12 月 17 日国家安全保障会議決定・閣議決定）
http://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-j.pdf

4 U.S. Department of Defense, *Quadrennial Defense Review Report*, May 2014, p.63.
http://www.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf

5 U.S. Department of Defense, *ibid*., p.III.

6 The White House, *National Security Strategy*, February 2015.
https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf

7 平成 25 年度の本調査研究事業の報告書のなかで筆者は、トーマス・ウィースらの「ガバナンス・ギャップ」論（Thomas W. Weiss, “The UN’s Role in Global Governance, “ *United Nations Intellectual History Project Briefing Note*, Number 15, August 2009, pp.2-5.）を援用し、グローバル・コモンズの安全保障の諸問題にひきつけて、知識・規範・政策・制度・順守の 5 つのギャップの可能性について検討している。星野俊也「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、宇宙空間、北極海を中心として―」日本国際問題研究所『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』（2014 年 3 月）、6-8 頁。

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

9 独立行政法人情報通信研究機構（NICT）の調査によれば、2014 年に国内外から日本の政府機関や企業等に向けられたサイバー攻撃関連の通信が約 256 億 6 千万件で、これまで最多だった 2013 年の約 128 億 8 千万件から倍増する勢いでサイバー空間の攻撃が激化しているという。共同通信「対日サイバー攻撃、256 億件 国内外から政府、企業に」2015 年 2 月 17 日。

第２章　サイバー攻撃と自衛権：重要インフラ攻撃とグレーゾーン事態

川口　貴久*

はじめに

グローバル・コモンズとしてのサイバー空間は人工的なドメインであり、その大部分は民間セクターに依拠している。サイバー空間は民間のインフラストラクチャや情報機器の集合体として存在すると同時に、サイバー空間自体が社会インフラや生活の基盤となっている。電力、上下水道、運輸、通信などの重要インフラはサイバー攻撃の脅威に晒され、医療機器や自動車などのコネクト化に伴いそのリスクは高まっている。

こうした環境をふまえて、日米の安全保障協力も変化しようとしている。現行の日米ガイドラインの見直しプロセスにおいても、「新たな戦略的領域における日米共同の対応」としてサイバー空間での安全保障協力が提起された。しかし、日米両国のサイバーセキュリティ政策の強化にもかかわらず、残された課題は大きい。さらにその課題は国際安全保障の核心に関わるもの、抑止や自衛権行使である。日米の安全保障協力の究極的な目的は、①平時においては第三国などからの武力攻撃を抑止し、②抑止が失敗し攻撃が発生する前後では実効的に対処することだが、サイバー空間ではここに問題が生じている。

こうした課題認識に基づき、平成25年度の研究プロジェクトとでは、前者の「抑止（deterrence）」について検討した。サイバー空間では、攻撃の発信源を特定しにくい点（いわゆる帰属問題）と攻撃優位のアーキテクチャにより、懲罰的な抑止メカニズムが機能しにくい。その一方で、アメリカの同盟ネットワークを中心に抑止力を整備しようとする試みも存在している[1]。

抑止が「平時」における安全保障メカニズムだとすれば、平成 26 年度研究プロジェクト（本稿）で扱う自衛権は抑止力の信頼性を担保し、実際の「有事」における対処能力向上に貢献するものである。

サイバー空間についても他のドメインと同様、ある一定の状況下でサイバー攻撃は自衛権行使の要件となり、それは同盟国のコミットメントを発動させることにもなる。しかし重要な問題は

（１）どういったサイバー攻撃が自衛権行使の対象となりうるのか

（２）そうしたサイバー攻撃に対して実効的に対処するための整備や日米協力は何なの

*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、筆者の所属する組織や団体の意見・見解を示すものではない。

か

である。

両方の問いに対して、本稿は**民間セクターに対するサイバー攻撃**を自衛権行使との関連で整理し、どういった体制整備が必要かを検討する。前述のとおり、コモンズとしてのサイバー空間が民間セクターに依拠し、また多くの社会基盤やインフラがサイバー空間に依存していることを踏まえると、こうした観点での検討は不可欠である。

サイバー攻撃への自衛権行使については既存の国際法体系から類推出来る領域はあるものの、重要インフラに対する破壊的攻撃への対処は難しい。更に言えば、既存の規範体系からは類推が難しく、純然たる有事とも平時ともいえないサイバー空間の「グレーゾーン事態」が生じている。

本稿では、まず第 1 節で昨今の日米両国におけるサイバーセキュリティ政策の強化、サイバー攻撃に対する自衛権行使の宣言政策について俯瞰する。その上で、第 2 節ではサイバー攻撃と自衛権に関する課題について整理し、第 3 節では、サイバー攻撃事態に対処するためのいくつかの提言を行う。

１．サイバー攻撃事態対処の強化

（１）日米におけるサイバー安全保障政策の進展

日本の外交・安全保障政策は転換期にある。2012 年 12 月に発足した第二次安倍政権は「積極的平和主義」や「セキュリティ・ダイアモンド[2]」といったコンセプトを打ち出し、国際的な安全保障環境の変化に適応しようとしている。実際、同政権は国家安全保障戦略の策定、国家安全保障会議の設置、武器輸出三原則の見直しなど次々と重要な決定を下し、2014 年 7 月 1 日には集団的自衛権行使容認を含む安保法制についての閣議決定を行った。

サイバー安全保障政策もこうした流れの中で強化されている。『国家安全保障戦略』や『防衛計画の大綱』でサイバー空間を「グローバル・コモンズ」と位置づけ、その重要性を確認している。また 2014 年 11 月にはサイバーセキュリティ基本法が成立し、同法は政府や重要インフラ事業者の責務を明らかにした。内閣に設置されるサイバーセキュリティ戦略本部は政策策定や重大事案対処では国家安全保障会議と連携していく予定である。

アメリカではサイバー空間を陸、海、空、宇宙に続く「第五の戦場」と位置づけ対策を強化してきた。サイバーセキュリティは緊縮財政および「強制削減（sequestration）」が進行する国防総省・米軍で、人員や予算などのリソースが増大している数少ない分野の 1 つである。

2014 年 3 月 28 日、米メリーランド州フォートミード陸軍基地でキース・アレグザンダー（Keith B. Alexander）大将の退役セレモニーが開かれた。アレグザンダーは国家安全保障局長官を約 9 年（2005 年 8 月 1 日～）、また初代サイバー軍（CYBERCOM）司令官として約 4 年（2010 年 5 月 21 日～）を務め、ロバート・ゲイツ（Robert M. Gates）国防長官の頃より、ウィリアム・リン（William J. Lynn）副長官とともに国防総省・米軍のサイバーセキュリティ対策を推進してきた。その退官セレモニーで、チャック・ヘーゲル（Chuck Hagel）国防長官は、CYBERCOM 要員を現行の約 1800 名から 2016 年までに 3 倍超（約 6000 名）に引き上げると宣言した。

もちろん手放しでサイバーセキュリティ政策の強化が歓迎されている訳ではない。アレグザンダーの後任であるマイケル・ロジャース（Michael Rogers）大将の指名にあたり、スノーデン事件の影響もあり、CYBERCOM 司令官と NSA 長官の兼務（dual-hatted）を解くべし、との意見も根強かった（結果的には兼務となった）。それでも前述のとおり、国防予算が縮小する中でのサイバーセキュリティへの投資増加はその重要性を示している。

（２）同盟とサイバーセキュリティ

こうした日米両国のサイバーセキュリティに関する認識は、日米安全保障協議委員会（Security Consultative Committee: いわゆる「２プラス２」）で確認される。2011 年 6 月の２プラス２でサイバーセキュリティが「共通の戦略目標」であると初めて明示され、2013 年 5 月からは局長級の日米サイバー対話が始まった。そして、現行の日米ガイドライン見直しのプロセスでも重要分野の 1 つとしても明示されている。

サイバー攻撃への対処は日米だけでなく、アメリカとその他の同盟国との間でも重要な政策課題となっている。特にサイバー攻撃への自衛権行使は主なアジェンダの 1 つである。アメリカは『サイバー空間の国際戦略』（2011 年 5 月）などで、サイバー攻撃に対して集団的な自衛権を行使することを宣言している。

> あらゆる国家は生来固有の自衛権を保有し、アメリカは、**サイバー空間を通じた特定の悪意ある行為が軍事的取極めを結ぶパートナーとのコミットメントを発動させる**ことを認識している。アメリカは、［筆者注：　サイバー攻撃および自衛権などに関連する］適応可能な国際法と矛盾のない形で、我々の国家、同盟国、パートナー、国益を守るために、外交、情報、軍事、経済的に必要なあらゆる措置（all necessary means）をとる権利を有している。[3]
> ［下線強調筆者］

実際、こうしたサイバー攻撃への対処が宣言されている。2014 年 9 月 5 日、ウェールズで開催された北大西洋条約機構（The North Atlantic Treaty Organization: NATO）サミットでは、「サイバー防衛は NATO 集団防衛（collective defence）の中核的任務の 1 つ」と明言された。その約 3 年前、2011 年 9 月 15 日、米豪の外交・防衛閣僚会議（２プラス２）は「領土保全、政治的独立性、米豪の安全保障を脅かすようなサイバー攻撃」は太平洋安全保障条約（ANZUS）の集団的自衛権行使の対象である点を確認した。

サイバーセキュリティが同盟や安全保障パートナーシップの主要アジェンダとして認識されつつある中、残された課題は大きい。その１つがサイバー攻撃への対処、自衛権の行使である。抑止が「平時」における安全保障メカニズムだとすれば、自衛権行使のための整備は抑止力の信頼性を担保し、実際の「有事」における対処能力向上に貢献するものである。だが、サイバー攻撃と自衛権について言えば、重要な点は（１）どういったサイバー攻撃が自衛権行使の対象となりうるのか、また（２）そうしたサイバー攻撃に対して自衛権を行使するための実効的な整備や日米協力は何なのか、である。

２．サイバー攻撃事態対処と残された課題

（１）サイバー攻撃と自衛権行使

サイバー攻撃に自衛権は行使可能か。この問題には、既存の国際法体系から類推できる領域と必ずしもそうでない領域（グレーゾーン）が存在する。

既存の国際法体系からの類推は比較的明快である。情報セキュリティ会議の外務省見解（2012 年 4 月 26 日）や安倍首相の国会答弁（2013 年 10 月 23 日、衆議院予算委員会）で示されているとおり、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」である。

より厳密に述べれば、国連憲章を含む既存の国際法体系をサイバー空間に適応できるならば、通常の武力攻撃に相当するサイバー攻撃は自衛権行使の要件となる。問題は、どの種類のサイバー攻撃が武力攻撃に相当するか、である。

NATO 加盟各国の研究者・実務家が作成した『タリン・マニュアル（Tallinn Manual on the International Law Applicable to Cyber Warfare）』によれば、「国際法上の戦争」「武力攻撃」に相当するサイバー攻撃とは、通常の動学的な（kinetic）軍事行動・武力攻撃に相当するもので、「規模」と「影響」を勘案し認定される[4]。米国務省の法律顧問クー（Harold Hongju Koh）は「直接的に死者、負傷者、重大な破壊行為を引き起こすサイバー攻撃は武力行使と見なしうる」とした上で、①原子力関連施設のメルトダウンを引き起こす攻撃、②ダムを開放

し、居住地域へ放水させる攻撃、③航空管制への攻撃を武力攻撃相当として列挙している[5]。

もちろん、こうした物理的被害の有無にかかわらず、電子戦に関する国際法体系から類推すれば、軍事目標に対するサイバー攻撃は自衛権行使の対象となりうる[6]。以上を整理すると、表 1、表 2 のように、サイバー攻撃は 4 つの象限で整理することが可能である。端的に言えば、物理的効果を伴うサイバー攻撃（分類 A、C）や軍事目標に対するサイバー攻撃（分類 A、B）は自衛権行使の対象となりうる。

既存の国際法体系からこのような整理は出来るものの、非軍事目標（民間の重要インフラなど）へのサイバー攻撃に対処することは難しい。**民間の重要インフラへの破壊的攻撃など（分類 C）**は物理的効果を伴えば、国際法上の自衛権行使が認定される可能性は高いものの、如何にして攻撃を抑止し、有事において対処するかは問題も多い。

更に言えば、**非軍事目標に対する物理的効果を伴わないサイバー攻撃（分類 D）**はそもそも自衛権行使との整理がつきにくい。具体的には、インターネット・サービス・プロバイダーに対する大規模な DDoS 攻撃、重要インフラのシステムの脆弱性を利用したエクスプロイテーション、経済システムの破たんを意図したサイバー攻撃などである。こうしたサイバー攻撃は「武力攻撃」「国際法上の戦争」とは言えず、純然たる有事とも平時とも言えない「グレーゾーン事態」に該当する。

表 1：サイバー攻撃の「対象」と「物理的効果」

		物理的効果	
		あり	なし
対象	軍事目標	分類 A	分類 B
	非軍事目標 （民間ｾｸﾀｰ）	分類 C 物理的効果を伴えば、自衛権行使の要件となる可能性は高いが、民間セクターへの攻撃を監視し、実効的に対処することが難しい。	分類 D 既存法からの類推では、自衛権行使の要件となる可能性が低く、サイバー空間の「グレーゾーン事態」といえる。

分類 A、B、C の攻撃は既存法からの類推で自衛権行使要件となる可能性が高い。一方、分類 D については必ずしも整理が明確ではない。

出典：　河野桂子「サイバー戦に適用される国際法と日米同盟：　『タリン・マニュアル』の評価」公益財団法人 日本国際問題研究所「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」研究会報告（2014 年 9 月 25 日）から、筆者作成。報告は、河野桂子「サイバー攻撃に対する自衛権の発動」、江藤淳一編『国際法学の諸相：　到達点と展望』（信山社、2015 年）、847-862 頁に基づくものである。

表 2：サイバー攻撃の具体例

前述の分類に基づく自衛権の認定可能性		サイバー攻撃の種類	具体例や備考
A B	既存法から類推	通常の軍事行動と一体のサイバー攻撃 （Cyber-Conventional Combination）	通常の軍事行動と一体化している軍事目標へのサイバー攻撃。イスラエルによるシリア空爆直前の防空レーダー網へのハッキング（2009）、中国による接近阻止・領域拒否（A2AD）戦略としてのサイバー攻撃など。
C	既存法から類推	制御システムへの破壊型攻撃 （destructive attack）	対象のシステムなどを破壊するサイバー攻撃（被害はサイバー空間外に及ぶ）。stuxnet によるイラン・遠心分離機の産業統制システムへの破壊工作（2009）、同種の標的型攻撃（Flame、Duqu、Gauss）など。
D	グレーゾーン	窃取型攻撃 （exploitation）	対象の情報を窃取するサイバー攻撃（スパイ活動）。「ゴーストネット［GhostNet］」（2009）、「タイタンレイン［Titan Rain］」（2003）など先端技術・防衛機密へのアクセスなど。
		妨害型攻撃 （disruptive attack）	対象のサービスやシステムを一時的に機能停止させるサイバー攻撃。エストニア（2007/4）、グルジア（2008/8）、ウクライナ（2014/3）への DDoS 攻撃など。
		データの破壊型攻撃 （destructive attack）	対象のデータやシステムを破壊するサイバー攻撃（被害はサイバー空間内にあるもの）。shamoon によるサウジ国営石油会社アラムコのデータ消去（2012/8）、韓国の金融・報道機関への攻撃（2013/3）など。

出典：筆者作成

（２）重要インフラへの破壊的サイバー攻撃：　制御システムへの攻撃

民間セクターに対する物理的効果を伴う攻撃（分類 C)、特に重要インフラの制御システムへの攻撃は、これまでも現実のものとなっている。

そもそも「重要インフラ」とは何だろうか。日米はそれぞれ、サイバー攻撃から特に防護すべき産業分野を定義している。

もっとも、日米ではサイバー関連の重要インフラの設定が異なる（表 3 を参照)。この差は日米の監督省庁の構成の影響もあるが、重要インフラ策定の経緯が異なっている。日本は内閣官房情報セキュリティセンター（NISC）が中心となり、情報セキュリティの観点で重要インフラを検討した。一方、アメリカは 9.11 テロ直後、より広範な国土安全保障の文脈で検討し、従来からの重要インフラを大統領政策指令（Presidential Policy Directive: PPD）21 号（2013 年 2 月 12 日）でサイバーセキュリティの観点で確認した結果である。こうした重要インフラなど制御システムへのサイバー攻撃は 10 年以上前から顕在化している。【表 4】

表 3：重要インフラの日米比較

日本 13 分野	アメリカ 16 分野
情報通信	情報技術
	通信
金融	金融
航空	運輸
鉄道	
物流	
電力	原子力関連
	ダム
	エネルギー
ガス	
水道	上下水道
政府・行政サービス	政府機能
	救急サービス
医療	医療・公衆衛生
化学 ＊	化学
石油 ＊	該当なし
クレジット ＊	
該当なし	重要製造業
	商業施設
	防衛基盤産業
	農林水産

出典：情報セキュリティ会議「重要インフラの情報セキュリティ対策に係る第３次行動計画」（2014 年 5 月)、Presidential Policy Directive 21: Critical Infrastructure Security and Resilience(February 12, 2013)を基に筆者作成。
日米の対応するセクターは正確な対比や一致ではなく、便宜上のものであり、さらに順序を変更している。
＊は第３次行動計画で新たに追加されたセクター。

さらに、これら重要インフラの中でもリスクや対応の優先度は異なっている。ホワイトハウスのサイバーセキュリティ調整官ダニエル（Michael Daniel）は「重要インフラのうち、特に電力、金融、輸送・物流、通信は脅威に直面している」と指摘する[7]。実際、2011 年 10 月から 2013 年 9 月にアメリカ国内で発生した産業統制システムのインシデント件数（軽微なものを含む）は 454 件だが、その内の 233 件（51%）は電力・エネルギーセクターで発生した。【図 1】　CYBERCOM 司令官兼 NSA 長官のロジャース大将は、「中国およびその他 1､2 の国はアメリカの電力網や航空管制システムを機能停止に追い込む能力を有している可能性」があり、そうした事態は「起こるかどうかではなく、いつ起こるか」と警鐘を鳴らす[8]。

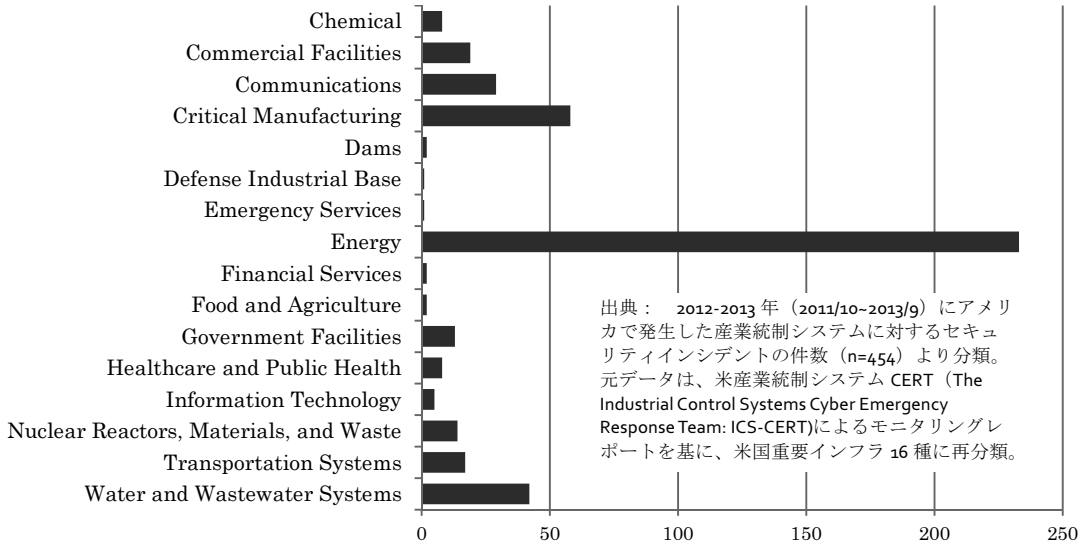
こうした重要インフラへの攻撃の中でもっとも有名なものは､「スタックスネット（Stuxnet)」であろう。2010 年夏、スタックスネットと呼ばれるマルウェアがイラン国内の核関連施設

表４　制御システムに対するサイバー攻撃・インシデント

時期	業界	国名	概要
1997 年	交通・運輸（航空）	アメリカ	ウォーセーター空港の電話サービス、管制塔の滑走路ライトを制御する送信機がシャットダウンされた。（犯行は 10 代の若者によるもの）
2001 年	水道	オーストラリア	上下水道の管理運営会社の制御システムが侵入を受け、結果、264,000 ガロンの未処理下水が放出された。（犯行は同社に採用されなかった者による報復）
2003 年	電力・エネルギー	アメリカ	ファーストエナジー社の管理する電力システムに不具合が生じ、管区内（東部・五大湖周辺）で停電が発生した。
2003 年	電力・エネルギー（原子力）	アメリカ	制御システムに Slammer が侵入し、システムが約 5 時間停止した。
2003 年	交通・運輸（鉄道）	アメリカ	東部の鉄道会社の信号管理システムが W32/Blaster に感染し、周辺の 3 路線で列車の運行停止とダイヤ乱れが発生した。
2005 年	製造業（自動車）	アメリカ	ダイムラークライスラー社の 13 の自動車工場が Zotob ワームにより一時的な操業停止に追い込まれた（自動車生産が約 50 分間停止）。感染の疑惑はサプライチェーン全体に及び、約 1400 万ドルの損失が生じた。
2008 年	交通・運輸（鉄道）	ポーランド	14 歳の少年がテレビのコントローラを改造し、鉄道の分岐点システムに侵入し、4 つの車両が脱線した。（12 人が怪我）
2009 年	交通・運輸（陸上）	アメリカ	カリフォルニア州などの交通信号システムのロックが解除されており（単純な人為的ミス）、侵入を受けた交通表示機に「ゾンビ注意（ZOMBIES AHEAD）」と表示された。
2010 年	電力・エネルギー（原子力）	イラン	Stuxnet に感染したウラン濃縮の遠心分離機に不具合が生じ、国内の遠心分離機が機能停止した。
2011 年	製造業（製鉄）	ブラジル	製鉄所工場内の発電所の制御システムが WORM_DOWNAD に感染し、発電機能が停止した。復旧に数カ月を要した。

出典：技術研究組合制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向および CSSC の研究概要について」（2014 年 9 月）、土屋大洋編著「サイバー攻撃の実態と防衛」 21 世紀政策研究所研究プロジェクト報告書（2013 年 5 月）、小林偉昭「制御システムの今あるセキュリティ脅威と対策について　～制御システムは、セキュリティ脅威とは関係ないと思っていませんか～」IPA グローバルシンポジウム 2012（2012 年 5 月 24 日）より筆者作成。

図１　重要インフラ 16 種別の産業統制システム・インシデント件数



の遠心分離機を一時的に機能停止に追い込んだ。フラッシュドライブ経由で持ち込まれたと見られるこのプログラムはクローズドの（インターネットなど外部に接続していない）産業統制システムを標的とした。Stuxnet は遠心分離機のローターの回転速度を僅かに狂わせ、オペレータの手元の制御画面では正常なデータを表示し続けた。結果、遠心分離機は破損し、イランの核開発計画が遅延した。『ニューヨークタイムズ』のサンガー（David Sanger）記者などの報道によれば、Stuxnet はアメリカとイスラエルによって企画された「オリンピックゲームズ」と呼ばれる作戦であった。社会インフラの制御システムが狙われたという意味で、この事件はサイバー戦争の大きな転換となった。それ以降、Flame、Duqu、Gauss といった同種の標的型攻撃が世界中で発見される。

現代生活のバックボーンとなる重要インフラだけでなく、「モノのインターネット」（Internet of Things: IoT）の進展に伴い身近な機器もリスクにさらされている。今後、医療機器や自動車などコネクト化がますます進展し、サイバー攻撃への脆弱性が高まるだろう。こうした状況をふまえて、デンプシー（Martin E. Dempsey）統合参謀本部議長は国家安全保障の観点からも自動車に対する攻撃（スピードメーターによる改ざん）について懸念を表明している[9]。

重要インフラへのサイバー攻撃（分類 C）はおおよそ「物理的効果」をねらったものであり、これは「国際法上の戦争」（自衛権行使の要件）と認定される可能性が高い。だが、実際に発生する攻撃を抑止し、危機において実効的に対処することは難しい。

（３）グレーゾーン事態：　物理的効果を伴わない民間セクターへのサイバー攻撃

一方で、物理的効果を伴わない民間セクターへの攻撃（分類 D）は明確に「国際法上の戦争」とは認定しにくく、「グレーゾーン事態」に該当する。このサイバー空間のグレーゾーン事態への対応も喫緊の課題である。

グレーゾーン事態とは、『国家安全保障戦略』や『防衛計画の大綱』といった最近の日本の安全保障政策文書が指摘する「純然たる平時でも有事でもない事態」である。今日の安全保障環境をふまえると、直面する有事は宣戦布告のある正規軍による衝突よりもグレーゾーン事態である可能性が高い。サイバー空間のグレーゾーン事態とは、安全保障上重要な施設への侵入、大規模かつ執拗な DDoS 攻撃、データ消去などが考えられる。実際に発生したグレーゾーンと考えられる攻撃をいくつか紹介する。

まず、証券取引所や中央銀行など、経済システムに壊滅的な打撃を与えるサイバー攻撃である。2013 年 4 月 23 日、ＡＰ通信（Associated Press）の Twitter アカウント（@ap）から、「ホワイトハウスで２度の爆破があり、バラク・オバマが負傷した」との発信がなされ

た[10]。この「つぶやき」は後にシリア電子軍によってアカウントが乗っ取られたためであることが分かったが、この偽の「つぶやき」は短期的にではあるが株式市場に影響を与えた。もちろんこうした乗っ取り行為を自衛権行使の対象とするのは不可能である。しかし、経済システムや市場への影響が大きくなれば、それは自衛権行使の要件と認定される可能性がある[11]。

重要施設のセキュリティシステムや機密情報に対するエクスプロイテーションも重大な脅威となっている。セキュリティ会社「Cylance」社の報告書によると、2012 年以降、イラン政府の支援をうけたハッカーグループが、世界 15 カ国 16 業種 30 事業者にハッキングを行ってきた。この「肉切り包丁作戦（Operation Cleaver）」と呼ばれる活動の攻撃対象は、アメリカ、カナダ、クウェート、UAE、トルコ、パキスタン、韓国などの 15 カ国にある航空会社・空港、病院、防衛関連企業などの重要インフラを含むものである。ハッカーグループは空港ゲートとセキュリティ・コントロール・システムへの完全なアクセスを獲得し、結果、ゲート通行資格を偽装できていた可能性があった[12]。マンディアント社の最高セキュリティ責任者（当時）のベトリッチ（Richard Bejtlich）が指摘しているように、こうした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[13]。それゆえ、こうしたエクスプロイテーションは物理的被害を伴う破壊攻撃の「第一手」と見るべきである。

2014 年の米ソニー・ピクチャーズ・エンターテインメントへのサイバー攻撃は国家間の対立が顕在化した例である。後に連邦捜査局（FBI）は、この攻撃は同社が作成する北朝鮮の最高指導者を暗殺するというパロディ映画『ザ・インタビュー』の上映中止を求めて、北朝鮮が行ったものであると結論づけた。度重なるサイバー攻撃や社員への脅迫を受け、同社は上映中止を決定した。米下院議長を務めたニュート・ギングリッチ（Newt Gingrich）は自身の Twitter 上で、「ソニーが屈したことで、アメリカは最初のサイバー戦争に負けたこととなった。これは極めて危険な先例となる」と述べる[14]。「戦争」という表現はレトリックと捉えることもできるが、実際、ホワイトハウスのアーネスト（Josh Earnest）報道官は本件を「深刻な安全保障問題」と位置づけ、オバマ大統領は報復措置をとる意向を示した。

現状、こうしたサイバー攻撃はいずれもただちに武力攻撃と認定することは出来ず、自衛権行使の要件とはならないだろう。その一方で、攻撃の影響を勘案すれば、それは純然たる平時のインテリジェンス活動の延長とも言い難い。こうしたサイバー空間の「グレーゾーン事態」に対応していく必要がある。

３．サイバー攻撃の実効的な対処のための整備と日米協力

こうした重要インフラへの破壊的攻撃と「グレーゾーン事態」に対処するため、平時の抑止力強化と自衛権行使を含む有事の対処メカニズムの構築が不可欠である。そのための整備と日米協力として、国際規範の強化と創造、民間セクターの防衛、日米共同対処のメカニズム構築を進める必要がある。

（１）国際規範の強化と創造

サイバー攻撃に対する自衛権行使には、まず既存の国際規範の強化と新たな規範創造が不可欠である。サイバー攻撃への自衛権行使の前提は、国連憲章第 51 条（自衛権）を含む既存の国際法体系がサイバー空間に適応されることである。アメリカは『サイバー空間の国際戦略』などで、サイバー空間の新たな条約や法の「再発明」は不要であり、既存の法体系を適用すべしとの立場をとっている[15]。一方で、中国やロシアはサイバー空間に新しい行動規範を構築すべきだと考え、対立が生じている。

だが、この問題は国連総会第一委員会のサイバーセキュリティに関連する政府専門家会合（Group of Governmental Experts:　GGE）の報告書（2013 年 6 月）で一定の決着をみた。同報告は「国連憲章を含む既存の国際法体系はサイバー空間に適応可能」という合意に至った[16]。国際法体系がサイバー空間にも適用されるということは、前述の分類 C（物理的効果を伴う民間セクターへのサイバー攻撃）のリスクに対応することとなる。日米はこうした規範をより強化していく必要がある。

前述のグレーゾーン事態への対処として、新たな国際規範の創造も必要である。サイバー攻撃の大規模化・深化をふまえて、国際規範も創造されなければならない。例えば、『タリン・マニュアル』策定にたずさわったシュミット（Michael N. Schmitt）は近い将来、経済的なサイバーインフラへの攻撃や経済システムを破綻させるようなサイバー攻撃は、武力攻撃と認定されるだろうと評価する[17]。ネットワーク化された世界では物理的効果を伴わないサイバー攻撃であっても、平和と安全を脅かすことを確認する必要がある。

日米はマルチ外交の場で、「既存の国際法体系がサイバー空間に適応され、物理的効果が伴えば民間セクターへの攻撃であっても自衛権行使の要件となる」ことを引き続き確認していくとともに（既存規範の強化）、物理的効果を伴わない攻撃や経済システムへの攻撃も「国際平和や安全を脅かす」という認識を拡げていく（新たな規範創造）必要がある。こうした規範形成は、普遍的なメンバーシップを有する国連などでなくとも、NATO や価値を共有する諸国でも十分効果的だろう。

（２）民間セクターの防衛：　ガイドライン構築と継続的モニタリング

次に、サイバー空間を構成する事業者や重要インフラ事業者の防衛である。そのためには､民間セクターの自主的なリスクマネジメント体制構築と政府による関与が必要である。

現状、重要インフラ事業者はサイバーセキュリティ基本法により事業継続のための努力義務が求められ、NISC や監督省庁が中心となって「重要インフラの情報セキュリティ対策に係る行動計画」の策定や分野横断的演習が実施されている。しかし、こうした行動計画や演習の基となるサイバーリスク対応の方針･考え方は必ずしも十分に示されていない。重要インフラ事業者をはじめとする民間セクターに対して、サイバー攻撃に対するリスクマネジメント体制の指針を提供することも必要である[18]。また、こうしたガイドラインや演習は重要インフラ事業者の事業継続性を意図したものだが、さらに事業者を絞って、有事における法執行機関や自衛隊、在日米軍の連携を明示すべきである。

民間セクターの自主的な防衛体制を奨励する一方で、安全保障に直結する事業者については政府が一定の負担をし、サイバー防衛の機能を提供すべきである。こうした政府（特に防衛省や自衛隊）による関与は、重要インフラの設定の見直しと日米の整合をはかる必要がある。例えば、農林水産業のサイバーセキュリティは重要だが、それが原子力関連施設と同程度ではないことは明らかである。日米それぞれの重要インフラをサイバーセキュリティ、特に有事における優先度で再定義し、どのセクターに防衛省・自衛隊、国防総省・米軍が関与するか、を検討すべきである。少なくとも電力や通信は残るだろう。

2014 年 3 月に発足したサイバー防衛隊は自衛隊ネットワークの防護がメインだが、一部の報道によれば、政府は原発や通信などの重要インフラへの防護に自衛隊アセットが展開できないか検討を始めた[19]。CYBERCOM が民間セクターの防衛を任務とする部隊（後述）を整備していることを踏まえ、日米連携の観点からもこうした検討は必要である。

民間セクター防衛の方法の 1 つは、サイバー攻撃の継続的なモニタリングである。ネットワークを監視し、攻撃を予見し、場合によっては相手方のアクセスを拒否することが必要である。この点について、既に『中期防衛力整備計画』（2013 年）でも「相手方によるサイバー空間の利用を妨げる能力」の保有の検討を示唆している。

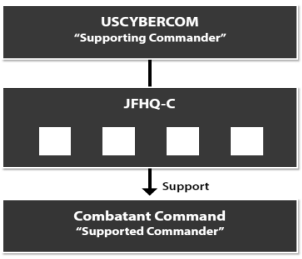
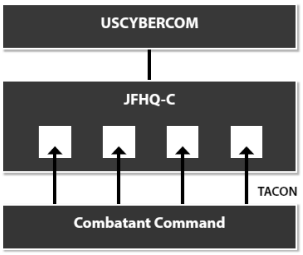
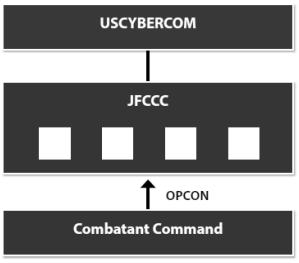
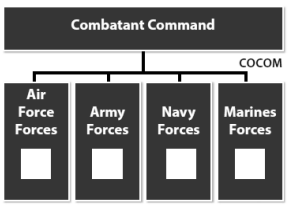
だが、こうしたネットワーク監視は憲法が保障する「通信の秘密」（第 21 条）との整合をはかる必要がある。総務省はこれまで厳密に運用してきた解釈を緩和し、悪意あるサイバー攻撃をモニタリングし､場合によっては攻撃を遮断できる環境を整える予定である。「コンテンツ」と「メタデータ[20]」を分け、政府や事業者が関与できる仕組みを整えていく。

（３）サイバー攻撃への日米共同対処

サイバー攻撃に実効的に対処するためには、自衛隊および米軍の連携が不可欠である。そうした連携の基礎となるのが「日米防衛協力のための指針」（ガイドライン）であり、これまでの日米連携の経験である。2011 年 3 月 11 日の未曽有の大災害における共同対処、意思疎通と運用調整の経験は、「将来のあらゆる事態への対応のモデル[21]」となるであろうと確認された。

しかし、サイバー空間の拡大と深化に伴い、どのようにサイバーオペレーションを日米共同対処に組み込むかはいまだ解決されていない。前述のとおり発足したサイバー防衛隊の役割は防衛省・自衛隊ネットワークの防護と監視であり、現状、民間セクターの防護や攻撃的なオプションにおける役割はない。一方で、国防総省・米軍のサイバーオペレーションについては、CYBERCOM 下の部隊が 3 つの機能を担う。それは、①重要インフラなどの民間セクターの防衛を担う国家防衛（National Mission Force）、②米軍のネットワークの防衛を担うサイバー防衛（Cyber Protection Force）、③全世界の統合軍をサポートする戦闘支援（Combat Mission Force）であり、2016 年までに 133 を超えるサイバー任務部隊の運用が開始される。

表 5　CYBERCOM と他の統合軍（Combatant Command）の指揮統制モデル

支援モデル	戦術統制（TACON）モデル	作戦統制（OPCON）モデル	戦闘指揮（COCOM）モデル
			
サイバー統合部隊司令部（Joint Force Headquarter-Cyber; JFHQ-C）は戦闘司令官の要求に基づき支援を行う。戦闘司令官はサイバー軍に対して指揮統制は行使しない。戦略軍の宇宙における作戦行動を統合軍と共同する場合と同様。	CYBERCOM は統合軍に対して、一時的にサイバー統合部隊司令部（Joint Force Headquarter-Cyber; JFHQ-C）への指揮統制を移譲する。戦闘統合軍の統制は割り当てられた部隊および付随する部隊に限定され、地理的な制約がある。戦略軍のグローバル・ストライクに関する作戦行動を統合軍と共同する場合と同様。	統合部隊サイバー部門司令官（Joint Force Cyber Component Commander: JFCCC）は、統合軍の全面的な指揮統制を受ける。戦闘司令官は JFCCC 指揮下の部隊を組織し、使用することができる（ただし、後方支援や教育・訓練、行政・人事は除く）。特殊作戦軍が統合軍と共同する場合と同様。	各地域の統合軍は、サイバー部隊に対して完全な指揮統制を有する。言い換えれば、独自のサイバー部隊を保有している状態であり、後方支援や教育・訓練、行政・人事に関する指揮統制を有する。電子戦（electric warfare）の場合と同様の形態。

出典：Ben FitzGerald and Lt Col Parker Wright, Digital Theaters: Decentralizing Cyber Command and Control, Disruptive Defense Papers (CNAS, April 2014)より筆者作成。

CYBERCOM の体制にも課題がある。最大の課題は、こうした CYBERCOM の部隊（サイバーオペレーションを担う部隊）と全世界の統合軍（Combatant Command）との関係、

特に指揮統制が明確でないことである。自衛隊・米軍での共同作戦となれば、指揮統制はより複雑な問題となる。このサイバー部隊－戦闘部隊、日米部隊間の指揮統制を整理しなければ、有事における自衛隊と米太平洋軍（PACOM）・在日米軍の共同対処に問題が生じる。この指揮系統の問題について、新アメリカ安全保障センター（Center for a New American Security: CNAS）は、CYBERCOM とその他統合軍との指揮統制モデルを整理する【表 5】。

さらに現在、アメリカでは CYBERCOM の位置づけについて議論がある。一部では、CYBERCOM の「格上げ」「大統領・国防長官への直接アクセス」が提起されている。現状、CYBERCOM は戦略軍（STRATCOM）隷下であり、CYBERCOM 司令官は戦略軍司令官を飛び越えることは出来ない。司令官はともに四つ星（大将）だが、こうしたアクセスの差は大きい[22]。前述の指揮統制モデルについても、こうした CYBERCOM 格上げ提案と密接に関連している。

こうした CYBERCOM の位置づけに関する議論を見据えながら、サイバーオペレーションを担う部隊と戦闘部隊の指揮統制を整理しつつ、防衛省・自衛隊のサイバー部隊を拡大・強化していく必要がある。特に、重要インフラ事業者のうちの特に国家安全保障に関わる事業者との連携は喫緊の課題である。

おわりに

日米でサイバーセキュリティ政策が強化され、NATO、米豪ではある特定のサイバー攻撃が同盟のコミットメントを発動させる要件であると確認されている。こうしたサイバーセキュリティ政策の高まりにもかかわらず、この分野に残された課題は大きい。さらにその課題は国際安全保障の核心、つまり抑止や自衛権行使に関するものである。抑止は平時における安全保障の中核的メカニズムであり、自衛権は抑止力の信頼性を担保し、実際の有事における対処能力向上に貢献するものである。

そして、有事におけるサイバー攻撃事態対処、自衛権行使の課題は、サイバー空間が人工的ドメインであり、民間セクターの資産の集合体であるという点と密接に関連している。法的な整理からすれば、既存の国際法体系からの類推から、①軍事目標に対する攻撃、②非軍事目標（民間セクター）であっても物理的効果を伴う攻撃は、自衛権行使の要件となりうる。

しかし、重要インフラなど民間セクターへの攻撃に、国家や政府が実効的に対処することは難しい。さらに、民間セクターに対する物理的効果を伴わない攻撃（重要システムへのエクスプロイテーション、経済システムの破綻を意図した攻撃など）は現状、直接的に自衛権行使の要件とはならず、サイバー空間の「グレーゾーン事態」に該当する。

日米両国はこうした課題を共有し、実効的な対処メカニズムを構築していく必要がある。それは国際規範の強化と創造、重要インフラ事業者への関与、日米のサイバー部隊間の調整である。

重要なことは、アメリカの影響力が相対的に低下する中で、コモンズとしてのサイバー空間を維持しなければいけないということである。確かに、アメリカの安全保障政策の中でサイバーセキュリティの優先度は高い。しかし、それは限られたリソースの中での優先順位であり、「強制削減」という言葉に象徴される緊縮財政下における安全保障政策である。日本は日米同盟を中心として、従来以上の役割と任務の中で、サイバー空間の国際安全保障に貢献しなければならない。

（2014 年 12 月 24 日）

－注－

1 川口貴久「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」、公益財団法人 日本国際問題研究所編『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 25 年度外務省外交・安全保障調査研究事業（2014 年 3 月）、11-26 頁。またサイバー抑止は、川口貴久「サイバー戦争とその抑止」、土屋大洋（監修）『仮想戦争の終わり：サイバー戦争とセキュリティ』角川インターネット講座第 13 巻（KADOKAWA、2014 年）、279-315 頁。

2 セキュリティ・ダイアモンドとは日米豪印など自由や民主制といった価値を共有する諸国による連携を指す。Shinzo Abe, “Asia’s Democratic Security Diamond,” Project Syndicate (December 27, 2012).

3 The White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), p.14.

4 Michael N. Schmitt, eds., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence(Cambridge University Press, 2013), p.54.

5 Remarks by Harold Hongju Koh, Legal Advisor U.S. Department of State, "International Law in Cyberspace," USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (September 18, 2012)

6 河野桂子「サイバー戦に適用される国際法と日米同盟 ―『タリン・マニュアル』の評価 」公益財団法人 日本国際問題研究所「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」研究会報告（2014 年 9 月 25 日）。報告は、河野桂子「サイバー攻撃に対する自衛権の発動」、江藤淳一編『国際法学の諸相：到達点と展望』（信山社、2015 年）、847-862 頁に基づくものである。

7 Bill Gertz, “White House cyber chief: future cyber attack to wipe out critical infrastructure,” Flash//CRITIC: Cyber Threat News (March 29, 2014).
http://flashcritic.com/white-house-cyber-chief-future-cyber-attack-wipe-critical-infrastructure/

8 2014 年 11 月 20 日に開催された米下院情報委員会での証言。Michael Rogers, "Cybersecurity Threats," at a House Select Intelligence Committee hearing on U.S. efforts to combat cybersecurity threats (November 20, 2014).
http://www.c-span.org/video/?322853-1/hearing-cybersecurity-threats

9 Gen. Dempsey's Remarks and Q&A at the Atlantic Council's Disrupting Defense Conference, WASHINGTON, D.C.(May 14, 2014).
http://www.jcs.mil/Media/Speeches/tabid/3890/Article/8919/gen-dempseys-remarks-and-qa-at-the-atlantic-councils-disrupting-defense-confere.aspx

[10] The Associated Press(AP), “Breaking: Two Explosions in the White House and Barack Obama is injured,” (April 23, 2013 at 1:07 PM), Tweet.　当該の「つぶやき」は、アカウント「乗っ取り」発覚直後、既にＡＰ通信自身により削除されている。

[11] 単に経済的損害だけでは認定可能性は低く、市場暴落などの大規模な経済的破綻の場合は見解が分かれる。コロンビア大学のワクスマン（Matthew Waxman）による見解。Ellen Nakashima, "When is a cyberattack an act of war?," *The Washington Post* (October 26, 2012).

[12] Cylance, Operation Cleaver (December 2014), p.14.
http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
Operation Cleaver の概要については WIRED 記事を参照。「イランの関与が疑われる、米国などの重要システムへのハッキング：Operation Cleaver」WIRED（2014 年 12 月 5 日）
http://wired.jp/2014/12/05/iran-backed-hackers/

[13] 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

[14] Newt Gingrich (newtgingrich), “No one should kid themselves. With the Sony collapse America has lost its first cyber war. This is a very very dangerous precedent.,” (December 18, 2014 at 7:04 AM), Tweet.

[15] *International Strategy for Cyberspace, p.9*.

[16] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* UN. Doc., A/68/98 (June 24, 2013), para.19.

[17] Michael N. Schmitt,“International Law and Cyber Warfare,” the Atlantic Council (March 28, 2013).
http://www.c-span.org/video/?311806-1/panelists-explain-new-cyber-warfare-manual

[18] アメリカの重要インフラ事業者向けの指針としては、「サイバーセキュリティ・フレームワーク」が挙げられる。2013 年 2 月 12 日、オバマ大統領は一般教書演説でサイバーセキュリティ強化を訴え、同日中に大統領令（Executive Order）13636 号および大統領政策指令（Presidential Policy Directive）21 号で具体的施策を指示した。その内の 1 つが同フレームワークである。National Institute of Standards and Technology(NIST), Framework for Improving Critical Infrastructure Cybersecurity, Version.1 (February 2014).

[19] 「サイバー攻撃時：自衛隊が原発防護 政府検討、民間に」『毎日新聞』（2014 年 5 月 9 日）

[20] 「コンテンツ」とは通信内容そのものであり、「メタデータ」とは通信に付随する情報である。電話を例にとると、メタデータとは発信元の番号、通話時刻、通話時間などである。監視の際には、コンテンツとメタデータを分けて議論されることが多い。メタデータは構造化されており、大量のデータ処理は容易である。

[21] 日米安全保障協議委員会文書「東日本大震災への対応における協力」（2011 年 6 月 21 日）

[22] 詳細は、土屋大洋「米サイバー軍と国家安全保障局の第二幕」『治安フォーラム』（2014 年 9 月）、48-51 頁。

第３章　グローバル・コモンズとしてのサイバースペースの課題

土屋　大洋

はじめに

サイバー攻撃やサイバー犯罪の多発により、サイバースペース全体が不安定になってきている。小説の題材としても取り上げられるようになっており、現実の事件に基づいて構成されているものも多い。人気作家のトム・クランシー（Tom Clancy）がマーク・グリーニー（Mark Greaney）の助けを借りて執筆した小説『米中開戦』においては、軍事的なサイバー攻撃のシナリオが示された[1]。また、マルク・エルスベルグ（Marc Elsberg）の小説『ブラックアウト』では、2001 年の対米同時多発テロ（9.11）、2008 年のリーマン・ショック、2010 年のイランの核施設に対するスタックスネット攻撃、2011 年の東日本大震災といった事件にヒントを得て、民間の重要インフラストラクチャへのサイバー攻撃が甚大な被害を及ぼす可能性を描いている[2]。

しかし、インターネットそのものがすぐに停止させられるというシナリオは必ずしも示されていない。他の社会的な機能の多くが失われるのに伴い、インターネットやその他の通信手段が失われる可能性は高いが、少なくともサイバー攻撃の初期段階においては、攻撃者側もインターネットに依存しているからである。インターネットがあるからこそ彼らは攻撃ができるのであり、初期段階でそれを使えなくしてしまっては、目的に達することができない。いわば、攻撃者や犯罪者を含めて多くの人にとってサイバースペースがコモンズ（commons）になっていることを示している。

本章では、コモンズとしてのサイバースペースを今一度捉え直し、その課題を検討したい。

１．土地としてのサイバースペース

コモンズは「共有地」と訳されることが多い。しかし、英英辞書の一つ（New Oxford American Dictionary）を見てみると、「コミュニティ全体に属したり影響を与えたりする土地や資源（land or resources belonging to or affecting the whole of a community）」とも書いてあり、必ずしも土地だけを意味するわけではない[3]。共有地の牧草が、家畜の過放牧で荒れてしまうというとき、問題なのは共有地の土地ではなく、共有地に生えている資源としての牧草であるともいえる。

そうすると、サイバースペースをグローバル・コモンズとして考える場合、世界各国の

人々によって共有されている「土地」としてのアナロジーと、「資源」としてのアナロジーの両面から考えることができるだろう。

無論、サイバースペースは、物理的な空間に存在する土地としては考えられない。それがどこにあるかと聞かれれば、世界各地に分散しているコンピュータの記憶装置の中であり、そうした装置が取り外されたり、新たに接続されたりすることで、絶えず縮小・拡大を繰り返していることになる。サイバースペースの利用者が増加傾向にある現在では、接続される装置のほうが多く、土地としてのサイバースペースは拡大基調にあるといえるだろう。しかし、やがては、世界人口に比してサイバースペースが飽和状態に陥ったり、人々が使わなくなったりすれば、それが縮小に転じることもあり得ないわけではない。

記憶装置が単に存在するだけではサイバースペースは構成されない。数多くの記憶装置が相互接続されるとともに、そこに収蔵されているさまざまなデータが処理・活用されなければ意味がない（そのデータこそが、サイバースペースの資源だが、これについては後述する）。記憶装置をつなぐのは多くの場合は各種の有線ケーブルであり、時には無線電波ということになる。

ますます多くの人が携帯電話を使ってサイバースペースにアクセスするようになっている。携帯電話は特定の周波数帯で電波をやりとりできる端末であり、固有の番号を振られ、特定の呼び出し番号にしか反応しないようにプログラムされている。

無線 LAN を使って携帯電話やパソコンなどからサイバースペースにアクセスすることも多くなっている。携帯電話とは違う周波数帯とプロトコル（通信規約）を使ってアクセスすることになるが、外形的にはあまり変わらない。

ラジオやテレビなどの放送も技術的・法的には通信の特殊形態であり、放送用アンテナから一方的に発せられる電波を専用端末が受信することで視聴可能になっている。

マイクロ波や短波を使った通信は、有線ケーブルが使いにくいところで広く使われてきたが、近年では光ファイバーが実用化され、電波に比べて通信容量が飛躍的に大きくなったため、有線ケーブルが優先的に使われるようになってきている。大海を越える国際通信は、19 世紀後半に海底ケーブルが発明されるまでは船舶に依存していた。海底ケーブルが大西洋や太平洋を越えてつながることで、地球の裏まで数時間、数分、数秒でメッセージを送ることができるようになった[4]。

1970 年代に人工衛星が使えるようになると、国際通信は無線に頼るようになったが、1980 年代後半に光ファイバーが実用化され、光ファイバーを使った海底ケーブル（光海底ケーブル）が敷設されるようになると、国際通信はふたたび有線ケーブルの時代に戻っている。

中長距離の陸線でもまた光ファイバーのケーブルが使われるようになっている。オフィスの中、家庭の中ではイーサネットと呼ばれる回線でコンピュータ同士をつなぐことが多い。

そして、ここで、データを収蔵する記憶装置とつながり（時には内包しながら）携帯電話やパソコンといった端末からの処理要請を処理する機械を「サーバー」としておこう。上記のような有線・無線の回線は、記憶装置＝サーバー＝端末の間の無数のチャンネルをつなぐことになる。この全体像が、土地としてのサイバースペースになる。

この土地としてのサイバースペースを攻撃するにはどうすれば良いか。それには、それらをつなげる有線・無線の回線を切断すること、あるいは、回線がつながっている装置・端末を破壊することになる。

回線の切断には、まず、それらの物理的な切断がある。海底ケーブルや陸上ケーブルを切断することは可能である。特定のオフィスにつながる回線を切断するために、電柱に架かる回線を切断したり、地下に埋設されているケーブルをマンホールなどからたどって切断したりすることも可能だろう。

無線回線の場合は、使われている周波数を妨害したり干渉したりする電波を出すこと（ジャミング）が考えられる。電波の利用は、場所、周波数、出力に依存している。同じ場所で同じ周波数で、ターゲットを上回る出力で妨害電波を出せば簡単に邪魔することができるだろう。

特定の個人のサイバースペースへのアクセスを邪魔したければ、その人の携帯電話やパソコンなどの端末を破壊したり、奪ったりすることがあり得る。不特定多数をターゲットとする場合には、事業者の装置や端末を破壊したり、不能にしたりすることもあり得るだろう。あるいは電力供給を止めるということも多大な影響を与える。バッテリーの充電がなくなれば、使えなくなる。

牧草地を使えなくするには、囲いを作ったり、武力で脅して近寄らせなかったりといったことが必要であり、かなりのコストを要することになる。しかし、多くの場合、土地そのものを消し去ることは、ほぼ不可能であろう。例えば、島を爆破して海上への露出部分をなくしたり、地形を変えてしまったりはできるだろうが、土地そのものを存在しない状態にするのは難しい。

それに対し、土地のアナロジーで考えるサイバースペースを存在しない状態にするのは比較的簡単である。回線を切断したり、装置・端末を破壊したりするだけで、すぐに消えてしまう。人工のスペースとしてのサイバースペースは、物理的なスペースよりもはるかに脆弱であるといえるだろう。

２．資源としてのサイバースペース

それでは、土地において提供される資源としてサイバースペースを考えるとどうなるだろうか。土地そのものを消し去るのは難しいとしても、牧草のような資源を使えなくするのは比較的簡単であろう。牧草を枯らすには、家畜に残らず食べさせてしまったり、適切な間隔で水をやらないようにしたり、毒薬をまいたり、アスファルトで舗装してしまったりすることができる。

土地利用は牧草ばかりではない。そこにオフィスビルや家屋を建てたり、商店街を設けたり、鉄道を敷設したりすることもできる。しかし、そうした利用法を妨害する方法はたくさん考えられるだろう。

サイバースペースの資源としてのデータはどうだろうか。サイバースペースで使われる資源としてのデータは無体物であり、デジタル情報である。牧草は再生可能な資源だが、化石燃料は有限の資源である。デジタル情報は、貯蔵・複製されていなければ、再生不可能な資源である。しかし、貯蔵・複製されていれば、簡単に再生可能な資源でもある。化石燃料のように使えば枯渇するものでもなく、電力や記憶装置の制約がなければ、無限の資源だといって良いだろう。

サイバースペースにおける資源としてのデータとは、具体的には何なのか。それは、電子メールのように個人間でやりとりされるメッセージでもあり、ウェブのように不特定多数によって共有・消費されるコンテンツでもある。

しかし、それらの中には有限のものもある。本研究プロジェクトの昨年度の報告書でも指摘したように[5]、ドメインネームやIP（インターネット・プロトコル）アドレスといった、サイバースペース上で一意に決まらなければならない文字列や数列は、共有しにくく、有限性を持つ資源である。apple.comというドメインネームを、コンピュータを作るアップル社や、レコードを作るアップル・レコード社、リンゴを作る農家が共有するのは難しい。

それ以外のデータは、サイバースペース上ではほぼ自動的にコピーされるといっても過言ではない。電子メールが送信されると、メッセージそのものは送信者のコンピュータにも残っているし、途中で経由するサーバーの中にも設定次第では残る。そして、受信者のコンピュータの中で複製される。ウェブページを閲覧するということは、ウェブサーバーの中にある情報を自分のパソコンや携帯電話の中に（一時的にせよ）コピーするという行為に他ならない。

グーグルのような検索エンジンは、世界中で生成されているウェブコンテンツを自動で複製し、それを自社のサーバーの中で保存しており、その複製・保存したコンテンツを参照しながら検索結果を表示し、それに基づいて検索者を元のウェブページに誘導している。

元のウェブページが更新・改変されていれば、中身が違ったり、行き着けなかったりすることもある。いずれにせよ、大量のコピーが自動的に生成されている。

無論、グーグル社が検索可能にしているコンテンツは、サイバースペース全体のコンテンツ資源の 4 割程度ではないかと見積もられている。検索エンジンを通じて行き着けないウェブページは、「ダークネット（darknet）」と呼ばれることがある。これらは例えば、ID とパスワードを使わないとたどり着けないページや、企業内のイントラネットのように外部からのアクセスを遮断しているコンテンツ、検索エンジンによる複製を拒否しているサイト、どこからもリンクされておらず孤立しているサイトなど、数多くある。個々人のパソコンはサイバースペースの一部でありながら、その中身を他者に自由に見せるようにしている人はまずいないだろう（ファイル共有［P2P］ソフトウェアによるファイル共有はその一つの例といえるかもしれない）。牧草地のアナロジーでいえば、柵で囲われてたどり着けない牧草、川があって渡れないところにある牧草、そもそも見えないところにある牧草といったところだろう。

そうすると、資源としてのサイバースペースを妨害するにはどうすれば良いだろうか。

まず、データそのものを破壊する行為があるだろう。端末に不正にアクセスして消去したり、改変したりすることが考えられる。最近ではデータをロックしたり、暗号化してしまったりして、本来の所有者がデータにアクセスできないようにし、金銭を要求する脅迫も行われるようになっている。

検閲、ブロッキング、フィルタリングなども、データへのアクセスを阻害する措置である。検閲は、政府当局者などがコンテンツの中身を政治的に判断し、出版・公開を差し止めたり、改変を求めたりする行為である。ブロッキングは、政府当局者や事業者が、あらかじめ決められたリストに基づいて、利用者に特定のコンテンツへアクセスさせないことである。フィルタリングは、利用者自身の判断によって特定のコンテンツへのアクセスを遮断する行為である。親が子供のアクセスするコンテンツをコントロールしたり、スパム・メールがメールボックスに入ってこないようにすることも含まれる。

あるいは、著作権法などを行使することによって、データの利用を阻止することもできる。ただし、この場合の強制力は、相手の法遵守規範のレベル次第であり、悪意を持った相手には意味をなさないだろう。

３．重要インフラストラクチャとしてのサイバースペース

上記の試論は、あくまでサイバースペースが単体のスペースとして存在しているという仮定の下にある。しかし、実際は、サイバースペースは現実のさまざまなスペースと切り

離すことはできない。電子商取引は、ソフトウェアやコンテンツの売買においてはサイバースペースだけで完結する場合もあるが、本や CD、その他の物品の購入にインターネットを使う場合には、物流のネットワークと結びついている。電気やガス、水道、輸送システム、工場などの制御システムと接続されている場合もある（現在ではなるべく切り離す方向になっているが)。軍隊でさえも、調達部門を中心に一般的なインターネットとつながっている。

サイバースペースは、陸、海、空、宇宙に次ぐ第五の作戦領域だと米軍は指摘しているが、実際には、軍事的に見れば、サイバースペースはそれら四つの自然のスペースをつなぐ神経系になっている。例えば、エア・シー・バトルという戦術概念が議論されつつあるが、空軍と海軍が連携するには通信が必要である。並んで歩きながら連携するならまだしも、現代における大規模な軍事作戦は、通信なくして成り立たない。

軍事ばかりでなく、ほとんど全ての社会システムが広義の（インターネットにつながっていないものも含む）サイバースペースに依存するようになっている。つまり、サイバースペースは重要インフラストラクチャそのものであり、その中心的存在でもある。

2001 年の対米同時多発テロ（9.11）を検証した結果、アルカイダが本当に狙っていたのは米国経済の神経網への攻撃であり、米国経済を麻痺させることであったとの見方がされるようになった。いわば、9.11 の数千人の犠牲者は「副産物」であり、本当の狙いは米国経済にあっただろうというのである[6]。

米国経済を日本経済やグローバル経済に置き換え、攻撃者をアルカイダ以外のアクターに置き換えることもできる。どこかのテロリスト・グループがグローバル経済を麻痺させることを狙ってサイバー攻撃を実施するとすれば、何を狙うだろうか。一つには、「土地」としてのサイバースペースの破壊である。先に述べた考えを敷衍すれば、その攻撃は物理的な設備に対する破壊となるだろう。海底ケーブルの回線や陸揚げ局、人工衛星そのものや通信回線、地上局が物理的破壊のターゲットとなる。個々の端末を狙うよりも手っ取り早いであろう。

「資源」としてのサイバースペースを攻撃するならば、ドメインネームや IP アドレスの管理システムを破壊することでかき乱すことができる。例えば、日本国際問題研究所の研究員に電子メールを送ろうとしても、「jiia.or.jp」というドメインネームがどの IP アドレスに対応するのか分からなくしてしまえば、メールは届かなくなる。メールだけなら良いが、サイバースペースに依存を深める金融取引には大きな打撃になるだろう。例えば、街中の銀行の店舗は、銀行業界の合併淘汰を経て減らされており、窓口業務はすべてのニーズをさばききれないだろう。各所に保管されているデータを破壊・改ざんすることができれば

大きな混乱がもたらされる。

土地に対する攻撃と資源に対する攻撃の両方を合わせた攻撃として EMP（電磁パルス）爆弾の可能性を完全には否定できない。EMP 爆弾はサイバー戦の前の電子戦の時代にはよく議論されたが、現在ではあまり意識されていない。しかし、現実に起こり得る問題である。1962 年に米軍が太平洋で核実験（Starfish Prime）を行ったが、それが EMP 爆弾と同じ効果を引き起こし、1445 km 離れたハワイの街灯が消え、盗難警報器を鳴らし、マイクロ波通信回線を不能にした。当時はまだパソコンが普及していない時代だったが、現代で同じことが起きれば各種コンピュータを不能にするなど広範な被害が出る可能性がある。

４．米軍と米インテリジェンス機関の動き

1991 年の湾岸戦争において米軍はハイテク兵器の圧倒的な威力を見せつけた。そして、ビル・クリントン（Bill Clinton）政権時代の軍事革命（RMA）や、ジョージ・W・ブッシュ（George W. Bush）政権時代のトランスフォーメーションの流れの中で、情報通信技術をいっそう積極的に軍事の中に取り入れてきた。

しかし、1997 年に米軍が行った「エリジブル・レシーバー」演習では、国家安全保障局（NSA）が地域別統合軍の一つである太平洋軍等をサイバー攻撃したところ、太平洋全域の作戦を担う米軍の指揮統制システムを損なうことができた。それ以来、米軍はサイバー攻撃の可能性を懸念し、徐々に対応を行ってきた。

もともとのインターネットの発想に従い、米軍内のネットワークも「自律、分散、協調」の影響を少なからず受けてきた。各軍・各部隊でそれぞれのニーズにあったシステムが構築されてきた。それは、一方では成功であった。米軍の一つのシステムが攻略されても、米軍全体に及ぶ可能性は低い。被害は一部にとどめることができる。しかし、他方では、バラバラのシステムは全体の防御のコストを上げることになる。個別のシステムに応じた防御を行えば、それだけ時間的なコストも金銭的なコストもかかる。一括して守ることはできない。もともと軍は、ヒエラルキー型の中央集権的統制を求める。そこで、米軍は徐々に、情報通信システムのアーキテクチャを変えようとしてきている。

そこでのキーワードが統合情報環境（JIE）である。

米国防総省の資料によれば、米軍の現役の軍人は 140 万人、それに加えて 78 万 3000 人の民間人が請負等で働いている。120 万人の州兵と予備役、550 万人以上の家族と退役兵もいる。それらの人々が世界 146 カ国以上に散らばり、拠点の数は 5000 を超える。ビルや建物の数にして 60 万を上回る。情報通信システムでみれば、システム数は 1 万を超え、データセンターは 1850 近くもある。サーバーの数は 6 万 5000 台弱、コンピュータその他の端

末は 700 万台以上ある。脆弱性は無数にあるといっても過言ではない。

インターネットにつながっていなくても、これだけの人間がいればミスをする。クランシーは『米中開戦』の中で、ウイルスを仕込んだ USB メモリを駐車場に落としておくという作戦を描いている。拾った人の何割かは中身を確かめようと自分のコンピュータにそれを差し込んでしまうだろう。あっという間にシステム全体に影響が及ぶ。実際、中東の基地で似たようなことが行われ、2008 年に米軍のネットワークに大規模な侵入が行われるという「バックショット・ヤンキー（Buckshot Yankee）」事件が起きている（バックショットは乱れ撃ちのこと）。

あるいは、自宅で使っている個人的なパソコンや iPad などを職場に持ち込むことを「ブリング・ユア・オウン・デバイス（略して BYOD）」と呼ぶが、BYOD は「ブリング・ユア・オウン・ディザスター（災厄の持ち込み）」だと揶揄する声もある。

そこで、米軍は、収拾が付かなくなっている情報通信システムを統合し、管理・防御しやすくするためのアーキテクチャ改造をし始めている。それが JIE である。

JIE のキーワードは、安全性（secure）、抗堪性（resilient）、統合性（consolidated）になる。バラバラに運用されていた各種システムを統合して数を減らし、安全かつ使いやすくする。攻撃されないのが一番だが、されてもすぐに回復できる抗堪性が求められる。

こうした改革は民間企業でも常に行われているし、米軍でもこれまでも求められてきた。そもそもブッシュ政権時代にドナルド・ラムズフェルド（Donald Rumsfeld）国防長官が求めたトランスフォーメーションは、冷戦時代の重厚長大型の米軍をポスト冷戦時代の機敏な軍隊に変えることであり、情報通信システム等のハイテクの導入も、まさにそのためであった。しかし、システムの肥大化はかえって作戦を困難にしつつあり、オバマ政権の国防予算カットの波の中で、システムのアーキテクチャ見直しは不可避になっている。

新しい環境への移行は、米軍だけではできない。当然のことながら民間の情報通信業界との連携が不可避になる。そこには昔の軍産複合体さながらのサイバー軍産複合体が形成されつつある。ワシントン・ポスト紙のデイナ・プリースト（Dana Priest）とウィリアム・アーキン（William M. Arkin）が『トップシークレット・アメリカ』で明らかにしたように、9.11 以降の米国は、湯水のように予算を情報通信システムに使ってきた[7]。

５．ハッカーたちの反応

サイバーセキュリティが問題になり、サイバースペースへの軍事的な影響が拡大する現状に対して、ハッカーたちはどう反応しているのだろうか。

毎夏、米国ラスベガスのカジノ併設巨大ホテルで「デフコン」が開かれる。軍事用語の「デ

フコン」は「ディフェンス・レディネス・コンディション」の略で、防衛準備態勢のレベルを示すが、ネット業界での「デフコン」といえば、1993 年から開かれているハッカーのための会議である[8]。2014 年 8 月 7 日から 10 日に開かれた 22 回目のデフコンには 1 万 4000 人が参加した。

ハッカーといっても、現在のマスコミで使われるハッカーとは違う。もともとハッカーは技術に精通した人たち一般を指す言葉で、必ずしも犯罪行為に携わる人たちではない。彼らの技能が常人離れしていたために、ハッカーは中世の魔女のような扱いを受け、いつの間にか悪人の代名詞になってしまった。実際、デフコンでさまざまなハッキングを実演し、「ほら」と結果を見せられると、素人には魔法を見せられている気がする。

しかし、デフコンに集うハッカーは、本来の意味のハッカーであり、公然と悪事を働く人はほとんどいない。むしろ、技術の脆弱性を公表・共有することがデフコンでは奨励されている。最初に見つけ、実演することを誇りとしている。

実はデフコンには少なからぬ政府職員が聴衆として参加している。連邦捜査局（FBI）や国防総省、州や市の警察関係者などである。彼らからすれば、最新の技術情報や犯罪に使われる可能性のある手法を学ぶことができる。ハッカーたちもそれをある程度受け入れてきたが、会場で「連邦政府職員を見分けろ（spot the fed)」というゲームが毎年行われ、見つかった職員は壇上に上げられ、さらし者にされてしまう。

NSA 長官であり、サイバー軍の司令官でもあったキース・アレグザンダー（Keith Alexander）がデフコンに登場したことがある。NSA の契約社員だったエドワード・スノーデン（Edward Snowden）が機密を暴露したのは 2013 年の 6 月だが、その前年の 2012 年のデフコンである。陸軍の大将として普段は軍服を着ているアレグザンダーが、この日は黒の T シャツにジーンズという姿で現れた。アレグザンダーは、第二次世界大戦中のドイツのエニグマ暗号や、日本のパープル暗号の話を持ち出し、政府と民間の協力が必要なのだと聴衆に呼びかけた。政府と民間は責任を共有しているというのが彼のメッセージであった。

しかし、ハッカーと NSA の蜜月は、翌年のデフコンでは消え失せた。2013 年 6 月にスノーデンの機密暴露が行われ、2 か月後に開かれたデフコンでは、「連邦政府よ、我々はしばらく離れている必要があるね」というかけ声が使われ、NSA／サイバー軍だけでなく、その他の連邦政府職員もデフコンから閉め出された。

米国の IT 企業は、米国政府と密接な関係を築いてきた。しかし、その関係はスノーデンの告発で変わり始めている。IT 企業は公然と政府を批判し始め、簡単には政府からの情報共有要請に協力しなくなってきている。今後、大手の IT 企業がどこまで政府からの要請を

突っぱねられるのかはまだ分からない。しかし、個人のハッカーたちの間では、再び政府への警戒感が高まってきている。

ハッカーたちはサイバースペースにおけるプライバシーを尊重している。しかし、彼らの技術がいったん「敵」に対して向けられれば、さまざまな情報の暴露（ウィキリークス事件やスノーデン事件のように）に向かったり、サイバー攻撃に使われたりする。米国政府だけでなく、各国政府にとってもハッカーたちとどう折り合いを付けるかが課題の一つになるだろう。

おわりに

コモンズとしてサイバースペースをとらえれば、それは単なる共有地というだけでなく、「土地」のアナロジーと、「資源」のアナロジーの両方を見なくてはならなくなる。サイバースペースの場合、物理的な土地は存在しないが、それは世界中の多様な設備の集合として見るべきであり、常に大きさを変えつつあり、むしろ複合主体ないし社会のアナロジーとして考えるほうが適切かもしれない。しかし、それ故に、脆弱なコモンズかもしれない。

サイバースペースの資源は、一般的にはデータやコンテンツといったデジタル情報だが、それと物理的な設備を支える法制度やルールも含めるべきだろう。法制度やルールは、インターネット・ガバナンスという言葉で議論が続けられている一方、データやコンテンツはプライバシーの文脈で議論されることが多い。しかし、セキュリティという面からもデータやコンテンツの保護を考えておく必要があるだろう。

グローバル・コモンズとして見た時、サイバースペースの今後の課題は、これまで注目されてきたような「資源」としてのコモンズに対する攻撃はいうまでもなく、「土地」としてのコモンズに対する攻撃、言い換えれば物理的な設備としてのコモンズに対する攻撃にいっそう備えるということになるだろう。電力設備、海底ケーブル、人工衛星といった重要インフラストラクチャを対象に含めた群発攻撃に備えなければならない。群発攻撃とは、物理的な設備に対する攻撃とデータ／コンテンツ／プログラムに対する攻撃の両方を含む、複数のターゲットを狙った同時多発的な攻撃である。

かつてのサイバー攻撃は、無料で入手できるツールを使って誰でもできた。しかし、サイバーセキュリティに対する意識が高まってきている現在、最前線のサイバー戦はプロ同士のものになりつつある。そうした争いが、サイバースペースというコモンズをさまざまな形で荒らし始めている。

－注－

[1] トム・クランシー、マーク・グリーニー（田村源二訳）『米中開戦 1〜4』（新潮文庫、2013 年〜2014 年）。

[2] マルク・エルスベルグ、（猪股和夫、竹之内悦子訳）『ブラックアウト（上・下）』（角川文庫、2012 年）。

[3] なお、「commons」は、「common」の複数形ではなく、「commons」という単数名詞として使われている。ギャレット・ハーディン（Garrett Hardin）の「共有地の悲劇」の論文でも、例えば「sharing a commons」という表現があるように、単数形で使われている。Garrett Hardin, “The Tragedy of the Commons,” *Science*, vol. 162, no. 3859 (December 13, 1968), pp. 1243-1248.

[4] 初期の電信では、人手を使ってメッセージを中継していたため、数時間を要することもあった。

[5] 土屋大洋「サイバースペースのガバナンス」日本国際問題研究所編（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」2014 年 3 月、27〜41 頁。

[6] ダン・バートン（星睦訳）『ブラックアイス―サイバーテロの見えない恐怖―』（インプレス、2003 年）106〜107 頁。

[7] デイナ・プリースト、ウィリアム・アーキン（玉置悟訳）『トップシークレット・アメリカ―最高機密に覆われる国家―』（草思社、2013 年）。

[8] 会議の創設者ジェフ・モス（Jeff Moss）は、友人の送別パーティーをカジノの街ラスベガスで企画していた。しかし、その主役の友人がパーティーに参加できなくなったため、ハッカーの友人たちを招いたのがデフコンの始まりである。1983 年に公開されたハッカー映画『ウォー・ゲーム』で核戦争のターゲットになるのがラスベガスだったことから、遊び心で会議をデフコンと名付けた。

第４章　安全保障分野における宇宙協力
―オバマ政権の取り組みと今後の日米協力―

福島　康仁（防衛研究所）[1]

はじめに

2010 年、オバマ（Barack Obama）政権は、大統領政策令第 4 号として「国家宇宙政策」（NSP）を発表した[1]。その策定に深く関与した米国政府高官によれば、国際協力の拡大こそ NSP の鍵であり基盤である[2]。ブッシュ（George W. Bush）前政権の NSP（2006 年）とは対照的に[3]、オバマ政権の NSP は全体が国際協力を念頭に記述されており、「目標」（Goals）の項では国際協力の拡大に高い優先順位が与えられている[4]。こうした方針は、2011 年にゲイツ（Robert Gates）国防長官とクラッパー（James Clapper）国家情報長官が共同署名した「国家安全保障宇宙戦略」（NSSS）にも反映されている[5]。実際、米国政府は安全保障分野における宇宙協力を深化・拡大させており、協力相手の増加と多様化もみられる[6]。本稿では、オバマ政権が安全保障分野における宇宙協力を重視する背景と具体的な取り組み状況を分析する。その上で今後の日米協力について考える。

１．協力を重視する背景

オバマ政権が安全保障分野での宇宙協力を重視する背景としては、つぎの 3 点を指摘できる。1 つ目は米国にとって協力に値する国家や非国家主体が増加していることである。これまで安全保障分野における同盟国との宇宙協力が限定的であった一因は、そもそも同盟国側が協力に値する能力を有していなかったことにあるといわれる[7]。だが、こうした状況には変化が現れている。欧州では通信や偵察、測位などの分野で軍事衛星や軍民両用衛星の整備が進んでいる。カナダも宇宙監視衛星の運用を始めている[8]。企業による通信衛星や地球観測衛星などの運用も拡大しており、その数は 400 機を超えている[9]。こうしたことから米国は宇宙で単独で行動することはできないし、その必要もないことを認識し始めたとロベロ（Douglas Loverro）米国防次官補代理（宇宙政策担当）は述べている[10]。

もっとも、オバマ政権が安全保障分野での宇宙協力を重視しているのは、単に増大する機会を活用するためだけではない。2 つ目の背景として、米国が宇宙利用を安定的に行っていくためには、他の宇宙利用者の協力が不可欠であるという認識の存在を指摘できる。こうした認識は前記の NSP や NSSS で明確に示されており、衛星破壊実験のような無責任

[1] 本稿の見解は執筆者個人のものであり、所属する組織を代表するものではありません。

な活動が全ての宇宙利用者に損害を与え得ることを考慮して、責任ある宇宙利用を各国に促していく方針が明記されている[11]。また、2009 年の米ロ衛星衝突のような事態が起きた場合、当事者のみならず他の衛星運用者にも多大な影響を与え得ることから、後述の宇宙状況認識（SSA）に関する協力を進めていく方針が示されている[12]。

同時に、米国政府、とりわけ米国防省には、安定的な宇宙利用を確保するために、他国や企業との協力を通じて、抑止や抗たん性（resilience）を強化したいという思惑がある。NSSS と 2012 年改訂の米国防省訓令「宇宙政策」では、責任ある宇宙利用を促す国際規範の醸成やコアリションの形成により、宇宙システムへの攻撃を抑止する方針が示されている[13]。国際規範の醸成は衛星破壊などを行った場合に国際的な非難を受ける状況を作り出すことで、コアリションの形成は敵対者が攻撃を行う場合に米国のみならずその協力相手とも対峙しなければならない状況を作り出すことで、潜在的な敵対者の意思決定を複雑化させることを狙ったものである[14]。米国防省はさらに抑止が失敗した場合でも引き続き作戦を継続できるように宇宙利用をめぐるアーキテクチャ全体の抗たん性を強化する方針を示しており、そのために他国政府や企業などが有する能力を活用する意向である[15]。

オバマ政権が安全保障分野での宇宙協力を重視する 3 つ目の背景としては、財政環境の悪化を挙げることができる。すでに米空軍宇宙コマンドは、2013 会計年度から 2014 会計年度にかけて 10 億ドル近い予算の削減を実施している[16]。さらに 2016 会計年度以降、予算の強制削減が再び実施される可能性があることに、ハイテン（John Hyten）米空軍宇宙コマンド司令官は強い危機感を表している[17]。こうした中、米国防省は同盟国や企業との協力に活路を見出そうとしている。クリンガー（Gil Klinger）米国防次官補代理（宇宙・戦略・情報システム担当）は、2014 年の議会証言において、現在および将来の財政環境を踏まえ、同盟国や企業の宇宙関連能力・サービスの活用を拡大する必要性を指摘している[18]。ロベロ米国防次官補代理も同じ議会証言の中で、現実の予算状況を考えると、米国による投資のみでは抗たん性を確保することは不可能であり、他国や企業の協力が必要であると述べている[19]。

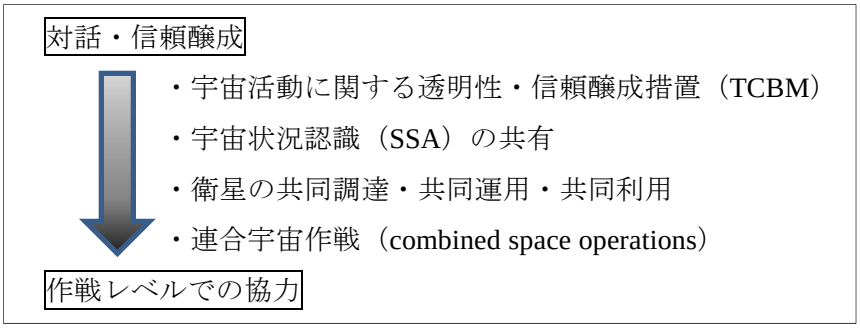
このようにオバマ政権が安全保障分野での宇宙協力を重視する背景には、増大する機会を活用したいという思惑に加えて、宇宙利用に対する脅威の顕在化と財政環境の悪化を受けて、協力を行う必要性に迫られているという事情がある。

２．具体的な取り組み状況

実際、2009 年 1 月のオバマ政権発足以降、安全保障分野における米国の宇宙協力は深化・拡大している。その内容は、他の宇宙活動国との対話・信頼醸成から緊密な同盟国・友好

国との作戦レベルでの協力まで幅広い。本稿では、下図に示す 4 つの代表的な取り組みを分析する。図内の矢印は、協力相手との安全保障面における緊密度を示している。おおよその傾向として、矢印の指す方向に向かうほど、より緊密な関係にあることを意味している。

図：米国が進める安全保障分野における宇宙協力



米国が進める安全保障分野における宇宙協力の 1 つ目は、宇宙における責任ある活動と平和的な宇宙利用を促すための透明性・信頼醸成措置（TCBM）の推進である[20]。オバマ政権の NSP は法的拘束力のある軍備管理措置について、公平で、効果的に検証可能であり、米国・同盟国の安全保障を強化するという基準にかなう提案・概念については「検討する」（consider）との方針を明記している[21]。こうした記述は前政権の NSP との明確な差異を示すものであるが[22]、実際には同基準に合致する案は存在しないとの立場をオバマ政権はとっている[23]。

かわりにオバマ政権が重視しているのが法的拘束力のない TCBM の推進である。2012 年にクリントン（Hillary Clinton）米国務長官（当時）は、宇宙活動に関する国際行動規範の策定に向けて、欧州連合（EU）やその他の関係国と協力していくとの声明を発表した[24]。前記のとおり米国防省も、国際規範の醸成を宇宙における抑止の向上につなげたいとの思惑から国際行動規範の策定を支持している[25]。

こうした多国間での TCBM に加えて、オバマ政権は中ロなどとの二国間 TCBM にも取り組んでいる。2014 年のウクライナ危機発生後は停滞を余儀なくされているものの、ロシアとの対話は比較的進んできた。宇宙安全保障に関する対話に加えて、ロシア軍関係者を米戦略軍の統合宇宙作戦センター（JSpOC）に招待するといった取り組みが行われてきた[26]。オバマ政権は中国との対話も重視しており、その拡大をはかっていく意向である[27]。2014 年の第 4 回米中戦略安全保障対話（SSD）では、新たに宇宙安全保障に関する議論が行われた[28]。米国側は、こうした対話を通じて、衛星破壊兵器の開発・実験に対する懸念を中

国側に伝達しているものと思われる[29]。

2 つ目は SSA をめぐる協力である。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[30]。前述のとおり米ロ衛星衝突のような事態が起きた場合、当事者のみならず他の宇宙利用者にも多大な影響を与え得ることから、オバマ政権は衛星を保有・運用する他国政府や企業等への SSA 情報の提供を強化している。現在、その中心を担っているのは米戦略軍である。同軍は 2009 年から SSA 共有プログラムを通じて、緊急、基礎、上級という 3 つのサービスを提供してきた[31]。

緊急サービスは他の衛星や宇宙ゴミとの衝突可能性について該当する衛星の保有・運用者に緊急通知するものである。こうした緊急通知は中国に対しても行われている。ローズ（Frank Rose）米国務次官補代理（当時）は、2007 年の衛星破壊実験で生じた宇宙ゴミが中国自身の衛星に接近していることを通知した逸話を紹介している[32]。中国への通知を行った理由についてローズ氏は、中国の衛星が宇宙ゴミと衝突し新たな宇宙ゴミが発生した場合、結果として米国の衛星が危険にさらされる恐れがあったためであると述べている[33]。中国側もこうした米国による緊急通知の価値を認識しているものとみられる。中国への通知は外交ルートを通じて行われてきたが、中国は 2014 年末に、今後は衛星運用機関に直接通知するように米側に要請した[34]。ハイテン米空軍宇宙コマンド司令官はこうした中国側の姿勢を高く評価しており、要請に応えるための作業が米側で進められている[35]。

つぎに基礎サービスは米戦略軍が運営するウェブサイト「Space-Track.org」を通じて基礎データの提供を行うものである[36]。2013 年 2 月時点で、ユーザー登録を行った 185 カ国の 8 万 8,000 人にデータの提供を行っている[37]。

そして上級サービスは、SSA 共有協定締結者への高精度データの提供である。米戦略軍は 2010 年から衛星の打上げビジネスや衛星の保有・運用を行う企業との間で、また 2011 年以降は他国政府等との間でそうした協定の締結を進めている[38]。2015 年 1 月時点で米戦略軍は、46 の企業と、8 つの政府（締結順に豪、日、伊、加、仏、韓、英、独）、2 つの政府間組織（欧州宇宙機関、欧州気象衛星機関）と協定を締結済みである[39]。こうした協定は、双方向でのデータ共有の基盤となるものであり、米国が一方的に SSA データを提供するのではなく、衛星の軌道位置や周波数に関する情報を提供してもらうことで、米国自身の SSA の精度向上をはかるという意味合いもある。米国は他国の追随を許さない圧倒的な SSA 関連能力を有しているが、それでも地理的・資源的制約から単独では全ての宇宙物体を精密に追跡できないと認識している[40]。

このような問題意識に基づいて、米国防当局は宇宙監視（space surveillance）に関する同盟国との協力拡大もはかっている。宇宙監視は地球を周回する人工物体を体系的に観測す

る活動であり、環境モニタリング（宇宙天気の観測など）や各種のインテリジェンス活動と並び、SSA を生成するための手段である[41]。英国とノルウェーはそれぞれ冷戦期と 2000 年代前半から地上レーダーで収集した情報を米国の宇宙監視ネットワーク（SSN）に提供してきたが[42]、カナダも 2014 年からサファイア宇宙監視衛星で収集した情報を SSN に提供し始めている[43]。さらに、手薄となっている南半球での宇宙監視を強化するために、米国は豪州への関連施設の移設を進めている。2016 年には米国から豪州に移設する宇宙監視レーダーと宇宙監視望遠鏡の共同運用を開始する予定である[44]。

3 つ目は衛星の調達や運用、サービスの利用をめぐる協力である。代表的なのは衛星通信に関する協力であり、前政権の取り組みを拡大する形で進んでいる。2007 年に米豪の国防当局は、米空軍の広帯域全地球衛星通信システム（WGS）6 号機の製造・打上げ・運用費を豪州側が負担する見返りとして、同通信衛星群の帯域に豪州側が一定のアクセスを得るという覚書を締結した[45]。2010 年にも米豪の国防当局は、商用通信衛星に相乗りしている豪軍のトランスポンダに米海軍のアクセスを認めるかわりに、米海軍の移動体衛星通信システム（MUOS）へのアクセスを豪州側が得るという覚書を結んだ[46]。さらに 2012 年には、カナダ、デンマーク、ルクセンブルグ、オランダ、ニュージーランドとの間で WGS の 9 号機に関して米豪間と類似の覚書を締結した[47]。こうした衛星通信をめぐる協力は、陸海空で連合作戦を行う際の相互運用性を確保するという目的に加えて、経費を節減し、かつ抑止力と抗たん性の向上をはかるという意味合いを有している。例えば WGS への攻撃を行う場合、米国のみならず WGS を利用する同盟国の反応も考慮に入れなければならない状況を作りだすことで、敵対者による攻撃の敷居を上げるという効果が期待されている。

米国防当局は測位・航法・時刻同期（PNT）の分野でも国際協力を進めている。全地球測位システム（GPS）に対するジャミング（電波妨害）の脅威が顕在化する中、他の PNT サービスを米軍が利用できるようにするための交渉を関係国と始めている[48]。これは EU のガリレオや日本の準天頂衛星など、衛星測位システムの整備が世界的に進んでいることを背景としたものである。この他、SSA の分野では、前述のとおりカナダの宇宙監視衛星を SSN に組み込んでいる。

さらに、衛星を保有・運用する企業との協力も新たな段階に入っている。2011 年から 2014 年まで米空軍は商用通信衛星に相乗りさせた赤外線センサー（CHIRP）の試験的運用を行った[49]。米軍はこれまでも軍事衛星にペイロードを相乗りさせてきたが[50]、商用衛星に相乗りさせたのはこれが初めてであった。米空軍宇宙コマンドは、商用衛星への相乗りは、経費の節減につながり、さらに敵対者が攻撃を行う際の計算を複雑にさせ得ると評価している[51]。

ただし、米空軍宇宙コマンドは設計面での課題や法的懸念などが存在するとしており[52]、実用ペイロードを商用衛星に相乗りさせるという段階には至っていない。だが、こうした取り組みは、衛星を保有・運用する企業を単なる下請けとしてではなく、より対等なパートナーとして位置付ける試みとして注目に値する。

4 つ目は、緊密な同盟国・友好国との作戦レベルでの協力である。象徴的なのは、宇宙監視に関する協力や衛星の調達・運用・利用に関する協力を基盤として進んでいる連合宇宙作戦（combined space operations）構想である[53]。2014 年に米豪加英の国防当局は、同構想に関する覚書を締結した[54]。連合宇宙作戦は、陸海空で一般化している連合作戦を宇宙に適用する試みである[55]。米戦略軍のレイモンド（John Raymond）宇宙統合機能構成部隊司令官によれば、連合宇宙作戦は同盟国・有志国と宇宙領域で作戦面での提携関係を構築せよという NSP ならびに NSSS の指示に対する戦略軍の回答である[56]。連合宇宙作戦の範囲には、宇宙システムへの脅威について警報・評価を提供したり、宇宙システムによって陸海空の部隊への支援を行ったり、宇宙システムを防護・防衛したりするための活動が含まれる[57]。まずは各国の宇宙作戦センターの相互接続を進めることで、より緊密な SSA 共有がはかられる見通しである[58]。また、米国防省は陸海空と同様、宇宙においてもコアリションを形成して作戦を行っていく方針を示しており[59]、今後、同構想への参加国の拡大が見込まれる[60]。

これまで見てきたとおり、オバマ政権は安全保障分野における宇宙協力を深化・拡大させている。その内容は対話・信頼醸成から作戦レベルでの協力まで幅広く、協力相手も多様である。個々の協力が今後どこまで進展するかは協力相手の意向にも左右される。だが、米国が協力を重視する背景には前記のとおり宇宙利用に対する脅威の顕在化や財政環境の悪化という切実な事情があるため、米国は今後も協力を重視していかざるを得ないであろう。

３．今後の日米協力

米国の視点に立った場合、2008 年の宇宙基本法成立を契機として安全保障分野を含めた宇宙利用の拡大をはかっている日本は、協力相手としての価値を急速に高めている[61]。日本にとっても、宇宙利用の安定性確保や財政上の制約は宇宙利用の拡大を進める上で直面している課題であり、米国との協力に共通の利益を見いだすことが可能である。

実際、日米は 2009 年 11 月の首脳会談を契機として安全保障分野での宇宙協力のあり方について協議を重ねてきた[62]。また日米宇宙協力を行動志向なものにするという目標を掲げ[63]、徐々にではあるが協力の具体化をはかってきた。本稿でとりあげた米国による 4 つ

の取り組みのうち、最初の 2 点について日本はすでに主要な協力相手となっている。

1 点目の TCBM については、クリントン国務長官（当時）が国際行動規範の策定に向けて関係国と協力する旨を発表した約 1 週間後に、当時の玄葉光一郎外務大臣が協議への積極参加を表明した[64]。2014 年には国際行動規範案への東南アジア諸国の理解を得るために、米国およびインドネシアと共催で、第 2 回 ASEAN 地域フォーラム（ARF）宇宙セキュリティワークショップを東京で開催した[65]。

2 点目の SSA 共有については、2013 年に「日米宇宙状況監視協力取極」を締結した[66]。これは米国が他国政府と結んだ SSA 共有協定の中では豪州に次いで早いものであった。日本側から米国側への SSA 情報の提供も徐々にではあるが始まっている[67]。

さらに 3 点目の衛星の共同調達・共同運用・共同利用についても、日本は主要な協力相手となる可能性が高まっている[68]。2015 年 1 月の新しい「宇宙基本計画」は、アジア太平洋地域における米国の抑止力を支える宇宙システムの抗たん性を向上させるために、米国との衛星機能の連携強化等を行うと明記している[69]。より具体的には、準天頂衛星と GPS の連携を一層強化することが盛り込まれている[70]。

今後、2 点目と 3 点目の協力がどこまで深化するかは、かなりの部分、日本側による能力整備の進捗にかかっている。そもそも日米間では、米国が能力を整備し同盟国側が資金等を提供するという協力形態（WGS 型）はほとんど念頭に置かれていない。少なくとも現時点で日米が重視しているのは、同盟国側が能力を整備した上で米国と共有するという協力形態（サファイア型）である。この点は、2014 年の宇宙に関する包括的日米対話第 2 回会合の共同声明に明確に表れている[71]。同共同声明には「日本の宇宙活動の活発化が日米双方の安全保障に不可欠な宇宙アセットの抗たん性の向上につながる日米宇宙協力の新しい時代が到来したことを確認した」との一文が盛り込まれた。これは、日本が自立的な宇宙活動能力を有する数少ない国家の一つであり、今後も自立性の維持と産業基盤の強化を行っていく姿勢を明確にしていることを考えれば、それほど驚くことではない。

SSA について新しい「宇宙基本計画」は、平成 30 年代前半までに関連施設と運用体制の構築を行うと明記している[72]。2014 年に改訂された防衛省の「宇宙開発利用に関する基本方針」も、宇宙監視機能の保持に向けて内閣府や文部科学省と具体的な検討を進めることや、専従組織の設置を検討していくことを掲げている[73]。また準天頂衛星について新しい「宇宙基本計画」の工程表は、2017 年度から 4 機体制の運用を始め、2023 年度には 7 機体制の運用を始めるとしている[74]。これらの能力整備が進捗するにつれて、日米協力はより双方向性の高いものとなる可能性を有している。

最後に、こうした個々の協力を基盤として作戦レベルでの協力をどのように進めていく

かという問題は、今後の日米協力の主要な論点となる可能性がある。2014 年 10 月発表の「日米防衛協力のための指針の見直しに関する中間報告」が、見直し後の指針で宇宙協力について記述すること、その中には「宇宙の安全かつ安定的な利用を妨げかねない行動や事象及び宇宙における抗たん性を構築するための協力方法に関する情報共有」を含むと明記した点は注目に値する[75]。

また日米の有識者からは、JSpOC への防衛省職員の派遣や、米国政府が主催する机上演習への日本の参加といった提言が発表されている[76]。すでに豪加英は JSpOC への交換将校の派遣や[77]、米空軍宇宙コマンド主催の「シュリーヴァー・ウォーゲーム」への定期参加を行っている[78]。2012 年には参加国を拡大した「シュリーヴァー2012 インターナショナル」も開催され、豪加英に加えてフランス、ドイツ、イタリア、オランダ、デンマーク、トルコが参加している[79]。

机上演習に加えて米軍主催の実動演習・訓練への参加や、既存の日米共同演習・訓練への宇宙の組み込みも検討に値するだろう。米南方軍主催の年次多国間共同演習「PANAMAX 2014」の宇宙関連部分には、ドミニカ共和国、ペルー、ブラジルが参加し、米空軍と共同演習を実施している[80]。日米はこうした先進事例を参考としつつ、徐々に作戦レベルでの協力を進めていくことができるだろう。

おわりに

本稿では、オバマ政権が安全保障分野における宇宙協力を重視する背景と具体的な取り組み状況を分析した上で、今後の日米協力について考察した。これまで見てきたとおり、米国が安全保障分野における宇宙協力を重視し始めたのは比較的最近のことである。特に同盟国等の能力活用や作戦レベルでの協力といった点は、未だ試行錯誤の段階にある。自立的な宇宙活動能力を有し、かつ米国の主要な同盟国である日本は、米国とともに、こうした協力上の課題克服に取り組んでいくものと考えられる。

－注－

1 White House, *National Space Policy*, Presidential Policy Directive-4, June 28, 2010.
2 Office of the Spokesman, U.S. Department of State, Briefing by Senior Administration Officials on the President’s National Space Policy Via Teleconference, June 28, 2010, http://www.state.gov/r/pa/prs/ps/2010/06/143752.htm.
3 White House, *National Space Policy*, National Security Presidential Directive-49, August 31, 2006.

[4] オバマ政権の NSP では 6 つの目標が掲げられており、そのうち国際協力の拡大には 2 番目に高い優先順位が与えられている。なお、同 NSP における記述の順序は、多くの場合、優先順位と無関係であるが、「目標」の項は優先度の高いものから記述されている。White House, *National Space Policy*, 2010, p. 4.

[5] U.S. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy - Unclassified Summary*, January 2011.

[6] 米国は民生分野での宇宙協力については長い歴史を有している。米航空宇宙局（NASA）は、過去半世紀の間に、100 以上の国家・国際組織と 3,000 超の協力協定を結んでいる。National Aeronautics and Space Administration, *International Partnerships*, http://www.nasa.gov/exploration/dio/partnerships.html.

[7] このため従来の協力は米国が能力を整備し、それを同盟国が利用するという形態にとどまることが多かった。Richard W. McKinney, “Military International Space Cooperation,” *High Frontier*, Vol. 6, No. 2, February 2010, p. 3.

[8] カナダは同国初の実用軍事衛星としてサファイア宇宙監視衛星を 2013 年に打上げ、2014 年から実運用を始めている。National Defence and the Canadian Armed Forces, *News Release – Sapphire Satellite System is Declared Fully Operational*, January 30, 2014, http://www.forces.gc.ca/en/news/article.page?doc=sapphire-satellite-system-is-declared-fully-operational/hr1thk2x.

[9] 2014 年 7 月末時点において、世界で運用されている衛星は官民あわせて 1,235 機存在し、そのうち 434 機が商用衛星であった。この他に、商業目的にも利用される政府の衛星が存在する。Union of Concerned Scientists, *UCS Satellite Database*, http://www.ucsusa.org/nuclear_weapons_and_global_security/solutions/space-weapons/ucs-satellite-database.html.

[10] Douglas L. Loverro, Deputy Assistant Secretary of Defense for Space Policy, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, April 3, 2014, p. 8.

[11] White House, *National Space Policy*, 2010, pp. 1-2; U.S. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy - Unclassified Summary*, pp. 5-6.

[12] U.S. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy - Unclassified Summary*, p. 6.

[13] Ibid., p. 10; U.S. Department of Defense, *Space Policy*, Department of Defense Directive 3100.10, October 18, 2012, p. 2.

[14] U.S. Department of Defense, *Fact Sheet: DoD Strategy for Deterrence in Space*, http://www.defense.gov/home/features/2011/0111_nsss/docs/DoD%20Strategy%20for%20Deterrence%20in%20Space.pdf.

[15] U.S. Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy - Unclassified Summary*, p. 11.抗たん性については下記も参照。福島康仁「安定的な宇宙利用の確保に向けた日米の取り組み：鍵を握る抗たん性の強化」日本国際問題研究所『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』分析レポート、2014 年 3 月、1－6 頁。

[16] Cheryl Pellerin, “Budget Cuts, Growing Threats Affect Space Operations,” *DoD News*, July 23, 2014, http://www.defense.gov/news/newsarticle.aspx?id=122737.

[17] Mike Gruss, “At Space Surveillance Conference, Hyten Sounds a Warning on a 2016 Sequestration Threat,” *Space News*, September 10, 2014, http://spacenews.com/41817amos-conference-hyten-sounds-a-warning-on-a-2016-sequestration-threat/.

[18] Gil I. Klinger, Deputy Assistant Secretary of Defense for Space, Strategic, and Intelligence Systems, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, April 3, 2014, p. 4.

[19] Loverro, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, p. 8.

[20] White House, *National Space Policy*, 2010, p. 7.

[21] Ibid.

[22] Office of the Spokesman, U.S. Department of State, Briefing by Senior Administration Officials on the President’s National Space Policy Via Teleconference.

[23] Robert A. Wood, Permanent Representative of the United States to the Conference on Disarmament (CD), *Ensuring the Long-Term Sustainability and Security of the Space Environment*, CD Plenary, September 9, 2014, https://geneva.usmission.gov/2014/09/09/ambassador-robert-wood-ensuring-the-long-term-sustainability-and-security-of-the-space-enviroment/.

[24] Hillary Rodham Clinton, U.S. Secretary of State, *Press Statement: International Code of Conduct for Outer Space Activities*, Washington, DC, January 17, 2012, http://www.state.gov/secretary/20092013clinton/rm/2012/01/180969.htm.

[25] なお、米国政府がこうした交渉に積極的に関与する背景には、米国の安全保障を損なうことがないように国際行動規範の内容を形成していくという狙いもある。U.S. Department of State, *Fact Sheet: International Code of Conduct for Outer Space Activities*, http://www.defense.gov/home/features/2011/0111_nsss/docs/FINAL_DoD_Fact_Sheet_International_Code-2012_1-17-12.pdf.

[26] Frank A. Rose, *2010 Space Symposium – Keynote*, Omaha, Nebraska, November 2, 2010, http://www.stratcom.mil/speeches/2010/55/2010_Space_Symposium_-_Keynote/.

[27] Frank A. Rose, *Strategic Stability in East Asia*, The Johns Hopkins-Nanjing Center for Chinese and American Studies, Nanjing, China, December 8, 2014, http://www.state.gov/t/avc/rls/2014/235384.htm.

[28] U.S. Department of State, Senior State Department and Treasury Officials on the U.S.-China Strategic and Economic Dialogue, Beijing, China, July 8, 2014, http://www.state.gov/r/pa/prs/ps/2014/07/228888.htm.

[29] Rose, *Strategic Stability in East Asia*.

[30] U.S. Joint Chiefs of Staff, *Space Operations*, Joint Publication 3-14, May 29, 2013, Ⅱ-1, http://www.dtic.mil/doctrine/new_pubs/jp3_14.pdf.

[31] これは米空軍が 2004 年から運用していた試験的なプログラムを受け継いだものである。Tiffany Chow, *Space Situational Awareness Sharing Program: An SWF Issue Brief*, Secure World Foundation, September 22, 2011, pp. 1-2.また、詳細は不明であるが、米戦略軍は 2014 年から新しい SSA 共有戦略を実施し始めている。日本宇宙フォーラム「宇宙開発利用の持続的発展のための“宇宙状況認識（Space Situational Awareness: SSA）”に関する国際シンポジウム」成果報告書、2014 年 3 月、221 頁；John W. Raymond, Commander Joint Functional Component Command for Space, U.S Strategic Command, Statement Before the House Committee on Science, Space and Technology, Space Subcommittee on Space Track Management, May 9, 2014, p. 5.

[32] 日本宇宙フォーラム「宇宙開発利用の持続的発展のための“宇宙状況認識（Space Situational Awareness: SSA）”に関する国際シンポジウム」成果報告書、2014 年、210 頁。

[33] 同上。

[34] John E. Hyten, Commander, Air Force Space Command, *Air Force Space Command: Accomplishments, Future Challenges and Opportunities*, Air Force Association Mitchell Institute for Aerospace Studies Friday Space Group Seminar on “Space Power for the Warfighter” – Washington, DC, December 5, 2014, http://www.afspc.af.mil/library/speeches/speech.asp?id=754.

[35] Ibid.

[36] https://www.space-track.org/auth/login.

[37] 日本宇宙フォーラム「宇宙開発利用の持続的発展のための“宇宙状況認識（Space Situational Awareness: SSA）”に関する国際シンポジウム」成果報告書、2013 年 3 月、129 頁。

[38] Courtland B. McLeod, U.S. Strategic Command, *Space Situational Awareness (SSA) Sharing*, http://www.oosa.unvienna.org/pdf/pres/stsc2012/tech-40E.pdf.

[39] U.S. Strategic Command, *USSTRATCOM, Germany Make Arrangement to Share Space Services, Data*, January 28, 2015, http://www.stratcom.mil/news/2015/534/USSTRATCOM_Germany_make_arrangement_to_share_space_services_data/.

[40] 日本宇宙フォーラム「宇宙開発利用の持続的発展のための“宇宙状況認識（Space Situational Awareness: SSA）”に関する国際シンポジウム」成果報告書、2014 年、101－102 頁。

[41] U.S. Joint Chiefs of Staff, *Space Operations*, Ⅱ-1.

[42] レーダーの運用は両国が行っているが、レーダーそのものは米国製である。U.K. Ministry of Defence, *UK Air and Space Doctrine*, Joint Doctrine Publication 0-30, 2013, pp. 7-8, 7-9; RAF Fylingdales, *History*, http://www.raf.mod.uk/raffylingdales/aboutus/history.cfm; Alan D. Scott, “Coalition Building in Space: Initial Technical Considerations and Potential Implementation Strategies,” Defense Threat Reduction Agency, U.S. Department of Defense, October 2011, p. 3.

[43] National Defence and the Canadian Armed Forces, *News Release – Sapphire Satellite System is Declared Fully Operational*.

[44] Minister for Defence, Australian Government, *Defence Space Cooperation - Space Situational Awareness*, November 15, 2012,

http://www.minister.defence.gov.au/2012/11/15/minister-for-defence-defence-space-cooperation-space-situational-awareness/; “US Space Radar at Exmouth,” *DMO Bulletin*, Issue 2, 2014, http://www.defence.gov.au/dmo/NewsMedia/DMOBulletin/US-Space-Radar-at-Exmouth; Minister for Defence, Australian Government, *Australia and the United States Agreement on Defence Space Cooperation*, November 22, 2013, http://www.minister.defence.gov.au/2013/11/22/minister-for-defence-australia-and-the-united-states-agreement-on-defence-space-cooperation/.

45 Memorandum of Understanding Between the Department of Defense of the United States of America and the Department of Defence of Australia Concerning Joint Production, Operations, and Support of Wideband Global Satellite Communications, November 14, 2007. 同機は 2013 年に打上げられ、すでに運用が開始されている。

46 John Faulkner, Minister for Defence, Australian Government, *Enhanced Communications for Deployed Forces*, April 28, 2010, http://www.defence.gov.au/minister/90tpl.cfm?CurrentId=10206.また、報道によれば、MUOS を製造するロッキード・マーチンは、米国防省と協力して、同盟国に MUOS への出資を呼びかけている。MUOS の 6 号機の製造費用を同盟国側が負担することで、同盟国は MUOS 衛星群の帯域全体にアクセスできるようになる。特にカナダが関心を有しているといわれる。Mike Gruss, “Lockheed Eyes Partnerships to Keep MUOS Production Lines Warm,” *Space News*, Vol. 25, Issue 7, February 17, 2014, p. 6; Stew Magnuson, “New Satellite Systems to Boost Communication Coverage in Arctic (UPDATED),” *National Defense*, August 2014.

47 National Defence and the Canadian Armed Forces, *Canada’s Participation in the Wideband Global Satellite Communications System*, January 17, 2012, http://www.forces.gc.ca/en/news/article.page?doc=canada-rsquo-s-participation-in-the-wideband-global-satellite-communications-system/hgq87xyn.

48 Loverro, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, pp. 8-9.

49 Los Angeles Air Force Base, *AF Commercially Hosted Infrared Payload Launches Successfully from French Guiana*, September 21, 2011, http://www.losangeles.af.mil/news/story.asp?id=123273052; Los Angeles Air Force Base, *Air Force Commercially Hosted Infrared Payload Mission Completed*, December 6, 2013, http://www.losangeles.af.mil/news/story.asp?id=123373357.

50 例えば GPS 衛星には核爆発探知センサーが相乗りしている。Federation of American Scientists, *United States Nuclear Detonation Detection System (USNDS) (U)*, October 1, 1997, http://www.fas.org/spp/military/program/nssrm/initiatives/usnds.htm.

51 Air Force Space Command, U.S. Air Force, *White Paper on Resiliency and Disaggregated Space Architectures*, August 21, 2013.

52 Ibid.

53 連合宇宙作戦構想については下記も参照。福島康仁「宇宙における連合作戦：米豪加英の取り組みと今後の見通し」日本国際問題研究所『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』分析レポート、2014 年 12 月、1－5 頁、http://www2.jiia.or.jp/pdf/research_pj/h25rpj06/20141205_fukushima_report.pdf。

54 Cheryl Pellerin, “Stratcom, DoD Sign Space Operations Agreement With Allies,” *DoD News*, September 23, 2014, http://www.defense.gov/news/newsarticle.aspx?id=123236.

55 連合作戦は同盟国が共に行う作戦を意味するが、米豪加英が進める連合宇宙作戦構想にはその他の有志国の参加も視野に入れられている。また「コアリションによる宇宙作戦」（coalition space operations）あるいは「宇宙におけるコアリション」（coalition in space）という用語も使われることがあり、その場合は同盟国にとどまらない有志国による宇宙作戦という意味合いが一層強いように思われる。連合作戦については下記を参照。U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, November 8, 2010, As Amended Through August 15, 2014, p. 44.

56 Raymond, Statement Before the House Committee on Science, Space and Technology, Space Subcommittee on Space Track Management, p. 6.

57 Pellerin, “Stratcom, DoD Sign Space Operations Agreement With Allies,” *DoD News*.

58 Ibid.

59 Loverro, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, p. 13. なお、宇宙作戦のためのコアリションは、時限的なものではなく恒久的な枠組みとすることが念頭に

置かれている。Donna Miles, “Stratcom Strives to Build Coalitions for Space Operations,” *American Foreign Press Service*, May 14, 2013, http://www.defense.gov/news/newsarticle.aspx?id=120029.

60 具体的な国名は明らかにされていないが、すでに 2013 年時点で米戦略軍は潜在的な候補国に対して連合宇宙作戦に関する説明を行っている。Loverro, Statement Before the House Committee on Armed Services, Subcommittee on Strategic Forces, p. 13; Pellerin, “Stratcom, DoD Sign Space Operations Agreement With Allies,” *DoD News*; Miles, “Stratcom Strives to Build Coalitions for Space Operations,” *American Foreign Press Service*.

61 加えて、米国がアジア太平洋におけるリバランスを進めていることも協力相手としての日本の価値を高めている。Frank A. Rose, *A Modern U.S.-Japan Alliance*, American Center, Tokyo, Japan, February 23, 2015, http://www.state.gov/t/avc/rls/2015/237918.htm.

62 外務省「日米首脳会談の概要」2009 年 11 月 13 日、http://www.mofa.go.jp/mofaj/area/usa/visit/president_0911/sk_gaiyo.html。

63 外務省「共同声明 宇宙に関する包括的日米対話 第 2 回会合」2014 年 5 月 9 日、http://www.mofa.go.jp/mofaj/files/000038507.pdf。

64 外務省「宇宙活動に関する国際行動規範案」2014 年 5 月 30 日、http://www.mofa.go.jp/mofaj/gaiko/space/kokusaikoudou.html。

65 外務省「『第 2 回 ARF 宇宙セキュリティワークショップ』の開催（概要）」2014 年 10 月 10 日、http://www.mofa.go.jp/mofaj/fp/sp/page22_001610.html。

66 外務省「宇宙の状況の監視に関する日本国政府とアメリカ合衆国政府との間の書簡の交換（日米宇宙状況監視（SSA）協力取極の締結）」2013 年 5 月 28 日、http://www.mofa.go.jp/mofaj/press/release/press6_000278.html。

67 外務省「宇宙状況監視に関する日米協力」2014 年 5 月 7 日、http://www.mofa.go.jp/mofaj/press/release/press22_000049.html。

68 ただし、日本による米軍事衛星の利用は 1980 年代から行われてきた。防衛省・自衛隊は 1985 年から米海軍の通信衛星フリートサット（FLTSAT）を、1993 年からは米空軍の GPS 衛星を利用してきた。また 1996 年からは米空軍の防衛支援計画（DSP）衛星などで収集した早期警戒情報を利用してきた。防衛庁『防衛白書（昭和 61 年版）』大蔵省印刷局、1986 年、資料 23；防衛省「防衛省における宇宙開発利用の取り組みについて」文部科学省宇宙開発利用部会国際宇宙ステーション・国際宇宙探査小委員会（第 8 回）、2014 年 10 月 17 日。

69 「宇宙基本計画」平成 27 年 1 月 9 日宇宙開発戦略本部決定、9 頁。

70 同上、13－14 頁。

71 外務省「共同声明 宇宙に関する包括的日米対話 第 2 回会合」。

72 「宇宙基本計画」平成 27 年 1 月 9 日宇宙開発戦略本部決定、20 頁。

73 防衛省宇宙開発利用推進委員会「宇宙開発利用に関する基本方針について（改訂版）」2014 年 8 月 28 日、7－8 頁。

74 「宇宙基本計画工程表」平成 27 年 1 月 9 日宇宙開発戦略本部決定、2 頁。

75 防衛省「日米防衛協力のための指針の見直しに関する中間報告（2014.10.8）」http://www.mod.go.jp/j/approach/anpo/sisin/houkoku_20141008.html。

76 The Maureen and Mike Mansfield Foundation, *U.S.-Japan Space Forum: Mid-Term Objectives and Near-Term Priorities for Japan-U.S. Space Cooperation*, http://mansfieldfdn.org/mfdn2011/wp-content/uploads/2014/08/USJSF-Objectives-Priorities-21.pdf.

77 T. M. Anderson, “Schriever V - A UK Perspective,” *High Frontier*, Vol. 5, No. 4, August 2009, p. 15.

78 Joseph D. Rouge and Dennis L. Danielson, “Coalition Space Operations: Lessons Learned from Schriever V Wargeme,” *High Frontier*, Vol. 5, No. 4, August 2009, p. 28; C. Robert Kehler, “Introduction,” *High Frontier*, Vol. 7, No. 1, November 2010, p. 2.

79 Headquarters, Supreme Allied Commander, Transformation, North Atlantic Treaty Organization, *Shcriever Wargame 2012 International*, p. 8.

80 Jessica Casserly, “AFSOUTH Strengthens Space Ties With Partner Nations,” Air Combat Command, August 19, 2014, http://www.acc.af.mil/news/story.asp?id=123421769.

第５章　日本の安全保障宇宙利用の拡大と日米同盟

鈴木　一人

はじめに

昨年度の本外交安全保障調査研究事業「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」において、宇宙空間のグローバル・ガバナンスのあり方と日米同盟を通じた日本の対応について論じたが、本年度では、日本の宇宙開発、とりわけ 2008 年の宇宙基本法の制定から 2015 年初頭に採択された新たな宇宙基本計画を検討し、日本の安全保障宇宙利用の政策転換が日米同盟にどのように寄与するのかを論ずる。

１．日本の宇宙開発における安全保障の位置づけ

1960 年代から始まった日本の宇宙開発は既に過熱していた米ソ宇宙競争によって月面着陸に至る高度な技術を開発していた先進宇宙開発国にキャッチアップすべく、技術開発を優先した政策決定を行ってきた。また 1969 年の「宇宙の平和利用国会決議」によって防衛当局による宇宙への投資、開発、運用、利用が制限されることとなったことで、より多くの人的・財政的資源を民生目的の技術開発に集中させることが出来た。そのため、日本の宇宙開発は、防衛当局が全く介入することなく、宇宙開発機関の技術者が中心となった政策決定システムが強固に根付くこととなった。

しかし 1990 年代からの日本を取り巻く安全保障環境の変化、とりわけ 1998 年の北朝鮮によるテポドン打上げによって、こうした民生目的の技術開発優先の宇宙政策に変化が生まれるようになってきた。その転換点の中心となったのが情報収集衛星の開発決定（1998 年）である。これにより、日本でも安全保障目的の宇宙利用が進むかのように思われたが、しかし、既存の政策決定システムとの整合性を取るべく、防衛当局の介入は排除され、開発、運用の主体は内閣官房（情報調査室）が行うこととなった[1]。こうしたことから、情報収集衛星の開発決定以降も、宇宙機関や技術者を中心とする政策決定システムは継続され、情報収集衛星を例外的な存在として扱うことで、宇宙開発をめぐる政策とそれに伴う言説は維持され続けたのである。

２．宇宙基本法制定への道程

しかし、日本周辺の安全保障環境の変化はさらに厳しいものへと変化していき、中国の

対日感情の悪化、中国の周辺地域への影響力の拡大、指導者の死亡に基づく北朝鮮政治体制の不安定化など、懸念される事項が増大していった。また、アメリカが 1990 年代から進めた軍の近代化、いわゆる RMA（Revolution in Military Affairs : 軍事上の革命）が起こり、防衛装備のあり方や運用方法、戦術・戦略の変化が起こっていた[2]。その中でも宇宙システムの重要性は極めて重要となっており、グローバルな C^4ISR（Command, Control, Communication, Computing, Intelligence, Surveillance and Reconnaissance）の要として位置付けられるようになった[3]。こうした流れの中で、日本だけがこれまでの宇宙開発政策を継続し、情報収集衛星を例外として安全保障利用を一切排除した政策決定システムを維持し続けることは困難との認識が高まった。こうした流れの中心人物となったのが、自民党の河村建夫であった。彼は 2003 年から文部科学大臣として、日本の宇宙政策の中枢に据わることとなったが、彼は 2003 年の情報収集衛星の打上げ失敗（H-IIA6 号機）にロケット開発の最高責任者として立ち会うことになったのである。文部科学大臣はあくまでも宇宙技術の開発を指揮する立場にあり、JAXA が開発した打上げロケットである H-IIA も、基本的な考え方は「技術開発を重視した」ロケットであった。しかし、そのロケットに搭載された情報収集衛星は広い意味での安全保障目的のために開発され、利用される衛星である。従って、H-IIA6 号機の失敗に対して、文科省／JAXA としては「技術開発の途上であるがゆえに事故は不可避である」という立場をとる一方で、情報収集衛星を運営する内閣官房は「国家の安全保障を担う衛星を失うことは許されない」という立場をとる。ゆえに、技術開発の責任者として状況を説明した河村に対し、内閣官房長官である福田康夫をはじめとする政府・与党関係者は激しく非難したのである。河村自身も内閣の一員として、このジレンマに悩まされることとなった。

この経験から、河村は宇宙政策の現状に対する疑問を強く持つようになり、内閣改造に伴って大臣の職を去った 2005 年に、一議員として私的な勉強会である「国家宇宙戦略立案懇話会」、通称「河村懇話会」を発足させ、文部科学省、経済産業省、外務省、防衛省などの副大臣をメンバーとして、宇宙政策の勉強会を定期的に開催することとなった。この河村懇話会での議論がきっかけとなり、自民党政務調査会の宇宙開発特別委員会を中心に、日本の宇宙開発のあり方を見直す議論が進められることになった。2006 年 3 月には同委員会は「平和利用」＝「非軍事」の解釈を変更し、自衛権の範囲での防衛目的による宇宙利用は可能とする法案を提出することが合意された。

こうして自民党の案として合意を得た「宇宙基本法案」は、議員立法として国会に提出されることになったが、そこで河村はさらにもう一つのユニークな提案を行う。それは、この法案を単に自民党の案とするのではなく、当時連立政権を組んでいた公明党、さらに

は野党である民主党にも働きかけ、超党派の法案として議員立法を進めようとしたのである。その背景には、河村が超党派の議員連盟「せんたく」など、民主党にも広くパイプを持っていたことが挙げられるが、それ以上に、河村が宇宙開発を党派的な利害の問題としてではなく、国家戦略の問題として取り組んできたことが挙げられる。これは、河村懇話会が H-IIA6 号機の失敗による、情報収集衛星 2 機の喪失ということをきっかけに始められたものであり、個別利害や省庁の利益といったことを超えて検討しなければならない課題であるとの強い信念があったからである。その結果、宇宙基本法は 2008 年 5 月に国会を通過し、成立した。

３．宇宙基本法の特徴

（１）政策決定システムの変更

これまでの日本の宇宙開発が技術開発一辺倒であり、テポドンショックによってもその政策の方向性が変化しなかったのは、科技庁（文科省）と NASDA（宇宙開発事業団。後の JAXA：宇宙航空研究開発機構）が宇宙開発の中心に据わり、宇宙開発を科学技術開発として性格づけていたことが大きいとの認識が強かった。そのため、「平和利用原則」の再解釈においても、文科省と JAXA が宇宙開発を仕切っている限り政策は大きく変化しないと考えられていた。したがって、宇宙基本法では「宇宙開発体制の一元化」を一つの目標にしており、これまで存在しなかった宇宙開発担当大臣のポストを設定し、総理大臣が本部長となってすべての大臣がメンバーとなる宇宙開発戦略本部を設置することが定められた。これは、文科省だけでなくすべての省庁が宇宙システムのユーザーとなるべきであり、利用官庁も宇宙政策の意思決定に参画することで主体的に宇宙の利用を広げていくというコンセプトに基づく措置であった。宇宙開発戦略本部が出来たことで、そのもとに宇宙開発戦略本部事務局が設置され、文科省からは切り離された、宇宙を戦略的に扱う行政組織が生まれ、宇宙開発担当大臣が宇宙開発戦略本部副本部長となることで一定の政治行政上の責任の所在を明確にしたことは大きい。また、麻生内閣で河村が官房長官（宇宙開発戦略本部副本部長）となり、実質的に日本の宇宙開発政策決定を主導したことも大きい。これによって文科省／JAXA が進めてきた技術開発中心の宇宙開発から、利用官庁を巻き込んだ宇宙開発へと大きくシフトすることが可能になったのである。

（２）宇宙政策に対する認識の変化

いずれにしても、宇宙基本法の制定は日本の宇宙開発のあり方に大きな変化をもたらした。その変化は単に「平和利用原則」の解釈を変更したことや、新たな制度的枠組みを導

入したということだけではない。その根源にある発想は、宇宙開発を「社会インフラ」として評価しなおし、日本が持つ技術を国内外の問題解決に用いるべきである、ということであり、このような発想に突き動かされる形で宇宙基本法は成立したのである。そこには、以前のままの技術開発中心の宇宙開発では、財政状況がひっ迫する中で一層の予算削減が迫られることが想定され、グローバル市場で競争力を持たなければ日本の宇宙産業や宇宙開発コミュニティは生き残れなくなる、という危機感があったことは確かである。また、これまで見てきたように、諸外国における宇宙開発は軍事も含めた政治的なコミットメントによって推進されてきた部分が大きいにも関わらず、日本では政治的なコミットメントがほとんどなく、省庁と宇宙機関という次元で宇宙開発が進められてきたことでグローバル市場での競争からは隔離されたような、いわゆる宇宙開発の「ガラパゴス化」が起きている、との認識があったともいえる。そのため、宇宙基本法は、政治家が宇宙開発にコミットし、単に技術力で勝負するのではなく政府が後ろ盾となる形で日本の宇宙開発を支援していかなければならない、という方向性が打ち出されたのである。そのためには「公共事業としての宇宙開発」ではなく、「社会インフラ」としての宇宙システムの構築、しかも、日本国内だけでは市場も地理的範囲も狭いため、アジア地域にまで拡大した社会インフラとしての宇宙システムを構築する、という認識になっていったものと考えられる。

（３）安全保障上の宇宙利用の変化

宇宙基本法を進める上で、大きな原動力の一つとなったのは、これまでの「宇宙の平和利用国会決議」に制約され、防衛当局が極めて限定的にしか宇宙開発に関与できない状況を変更することであった。宇宙基本法では平和利用原則の新たな解釈として「国際約束の定めるところに従い、日本国憲法の平和主義の理念にのっとり」という前提を第二条で示し、第三条で「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」ものとして宇宙開発が位置づけられている。これにより、「平和利用原則」で制約されていた防衛当局や自衛隊による宇宙システムの開発、保有、運用なども認められることになり、宇宙システムを軍事的なインフラとして位置づけることが出来るようになった。

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 に派遣される等、遠方に展開するようになっているが、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通信衛星を自らの衛星を調達するのではなく、PFI（Private Finance Initiative）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、民間企業の公募によって衛星の開発・運用を任せ、防衛省はあくまでも利用者として使う

という位置づけのものである。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。一つは長い間「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。とりわけ防衛省の技術研究本部にも宇宙を専門とするスタッフは限られており、その能力を新たに構築していくことのコストも大きい。さらに、限られた予算の中で、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。しかし、より重要な問題は、自衛隊がそもそもグローバルに展開することを前提とした部隊編成になっておらず、あくまでも日本の領域防衛が中心となっているため、宇宙インフラによって支援される必要性が他国に比べて低いことも考えられよう。確かに日本近海の警備などでは宇宙インフラが重要となるし、PKO などで海外に派遣された場合もそうなのだが、これまでも商用衛星や地上システムによって運用してきた実績があるため、新たに宇宙システムに依存する必要がない、という状況でもある。

４．2014 年の総理指示と新たな宇宙基本計画

このような状況の中で、宇宙基本法を推進した（主として自民党の）政治家が安全保障上の宇宙利用が進んでいないことを問題視し、問題点の分析を自民党内で行った。その結果、これまで「平和利用国会決議」によって防衛省・自衛隊の中に宇宙開発に関する知見の蓄積が十分でなく、防衛省防衛政策課内に宇宙政策班を設けたが、その活動は上述した PFI による通信衛星に関する事項に事実上限定されるような状況であった。また自衛隊の技術研究本部においても宇宙技術の開発や運用の検討がなされていたが、その規模は小さく、新たなプロジェクトの立ち上げや新技術開発に向けた取り組みを行える状況にはなかった。また、宇宙技術に関する知見を蓄積している文科省と JAXA は、これまでの政策決定システムからの脱却意識が乏しく、防衛省・自衛隊との連携が充分ではないという結論に至った。

そのため、宇宙基本法で新たに安全保障目的の宇宙利用が可能になったにも関わらず、そのポテンシャルは十分に生かし切れていないため、省庁レベルでの調整では不十分であり、政治的な介入が必要との判断に至った。そしてこの議題が宇宙開発戦略本部（本部長

は総理大臣）で取り上げられ、2014 年 9 月 12 日に安倍内閣総理大臣による指示が発せられ[4]、これに基づいて新たな宇宙基本計画が策定されることとなった。

既に宇宙基本計画は宇宙基本法制定後の 2009 年に第一回の基本計画が策定され、その 5 年後の 2013 年 1 月に第二回の基本計画が策定されていた。本来 5 年を目途に策定される基本計画であるにも関わらず、前回から 2 年も経たないうちに新たな宇宙基本計画を策定するという異例な形での総理指示であった。また、第二回基本計画の時と同じ内閣（第二次安倍内閣）であり、宇宙政策委員会のメンバーも同じという状況であり、新たな基本計画を策定する根拠が明確ではないとの見方も多い[5]。

このような異例な状況の下で出された総理指示ではあるが、この時期に総理指示を出す根拠として「我が国を取り巻く外交・安全保障環境は急速に変化しており、我が国の安全保障上、宇宙の重要性は著しく増大」しているという認識と、「宇宙関連企業の事業撤退・人員減少が相次ぐなど、自前で宇宙開発利用を行う産業基盤がゆらぎつつあり、その回復・強化が喫緊の課題」であることが挙げられている。この総理指示に対し、メディアは「安全保障に偏った宇宙政策」であるとの懸念を表明し厳しい批判が浴びせられているが[6]、総理指示を見る限り、より大きな問題として位置付けられているのは各省の連携の悪さを改善することと宇宙産業の持続的発展を可能とする産業基盤の強化と読むほうが適切であろう。

ここにメディアを含む世間一般の宇宙基本法・基本計画のイメージと実際の宇宙政策が抱える問題のズレを看取することが出来よう。宇宙基本法によって設置された内閣府宇宙戦略室を中心とした宇宙政策担当者のレベルでは、宇宙産業が直面する問題を解決することが喫緊の課題であり、安全保障の問題は必ずしも最重要課題という位置づけにはなっていない。それは総理指示文書の中でも明らかにされている。むしろ、安全保障分野への投資を活発にすることで日本国内の宇宙産業の受注機会を増やし、それによって実用に耐えうるロケット・衛星を開発することで産業界に資することが期待されているとみることが出来る。

このようにして進められた異例の宇宙基本計画の更新だが、2014 年中の成立は不可能となり、基本計画が宇宙開発戦略本部で採択されるのは 2015 年 1 月となった。公開された新しい宇宙基本計画[7]を見てみるとその方向性が見えてくる。第一に、2013 年 12 月に策定された「国家安全保障戦略」に適合的な宇宙インフラの構築が重要とされていること、第二に、日米同盟の強化において宇宙分野の協力が重要視されていること、第三に、昨年度の報告書でも論じた宇宙空間の安定的利用を妨げるリスクを軽減するグローバル・ガバナンスの仕組みが不可欠であり、日本もそれに積極的に参加することが目指されている。

こうした問題意識に基づいて、この 10 年で進められるべきプログラムとして、日本版 GPS と言われる準天頂衛星を現在の 1 機から自律的測位が可能となる 7 機体制へと拡大すること、情報収集衛星を光学衛星 2 機、レーダー衛星 2 機の体制として継続運用すること、海洋監視（Maritime Domain Awareness：MDA）に向けて陸域・海域観測のための光学衛星とレーダー衛星を 1 機ずつ継続運用すること、そして宇宙空間の状況監視（Space Situational Awareness：SSA）に向けてレーダー設備を強化することなどが定められた。また、懸念されていた安全保障への傾斜は必ずしも明確ではなく、技術試験衛星や宇宙科学・探査衛星なども推進されることが計画されており、全体としてはバランスが取れた宇宙基本計画になっていると言えよう。

５．新たな安全保障宇宙利用と日米同盟

宇宙基本法の成立、そして新たな宇宙基本計画で示された安全保障利用の強化は日米関係も大きく変えようとしている。2003 年に戦略国際問題研究所（CSIS）が発表した『日米宇宙政策』と呼ばれるポリシー・ペーパーでも 1969 年の「国会決議は全く時代遅れのものとなっており、地域における日本の安全保障政策の足かせとなっている[8]」と厳しい表現で日本の政策変更を迫っていた。欧州ではボスニアやコソボにおけるオペレーションを通じて、欧州における安全保障能力の欠如が強く認識され、1990 年代の後半から欧州能力向上アクションプログラム（ECAP）などが実施されており、その一環として宇宙開発が位置づけられていたが[9]、日本は「平和利用国会決議」が障害となっており、同盟間の協力関係を築くことが困難であるとの認識を示してきた。

故に、宇宙基本法の成立に伴う安全保障宇宙利用の再定義は歓迎すべきとの見方がアメリカでは広がり、将来的な日米同盟の礎として宇宙分野も貢献しうるとの認識が高まった[10]。しかしながら、宇宙基本法が成立したにも関わらず、上述したように防衛省が宇宙の開発利用に消極的であり大きな変化が生まれてこなかったことに苛立ちを見せるようになっていた。そのピークとなったのが 2012 年 4 月の日米首脳会談であろう。ここでアメリカ側は日米の宇宙対話を進め、国家安全保障、国際安全保障を含む様々な問題に取り組む「政府全体アプローチ（Whole-of-government approach）」を確保することが必要と訴えた[11]。これは、日本の宇宙政策に関連する省庁が個別に政策を展開し、各省ごとに目標を設定しプログラムを展開しているのでは、日米間の連携を強化することは困難であり、問題解決に結びつかないという認識のあらわれであった。しかし、当時の野田総理はこの問題に着手することなく政権を失い、しばらくは政策決定システムの抜本的な変更を実現することはできなかった。

野田政権を引き継いだ安倍政権も、2013 年 1 月の第二回宇宙基本計画の策定時には政権の優先課題が経済にあり、宇宙政策や宇宙分野における日米同盟の強化にまで目配りできるような状況ではなかった。それゆえ、第二回宇宙基本計画までは旧来型の政策決定システムが継続されていたとみるべきであろう。しかし、安倍政権が軌道に乗り、安定した政権運営が出来るようになってくることで宇宙政策にも変化がみられるようになってきた。その象徴となったのが、2014年5月に行われた第二回日米包括宇宙対話である。これは2012年 4 月の日米首脳会談での議論を踏まえ、日米が「政府全体アプローチ」に基づいて、個別省庁や宇宙機関同士ではなく、外務省・国務省が窓口となり統一的な協力を進める仕組みの二回目の会合であった。ここでは「日本の宇宙活動の活発化が日米双方の安全保障に不可欠な宇宙アセットの抗たん性の向上につながる日米宇宙協力の新しい時代が到来したこと」が確認され、宇宙状況監視（SSA）、海洋監視（MDA）、宇宙空間の国際行動規範（Code of Conduct in Outer Space）など、安全保障に関わる分野で多くの合意が示され、日米同盟が宇宙分野で大きく前進しているという認識が共有された[12]。

ここで特に注目すべきは「宇宙アセットの抗たん性の向上」という文言である。これは昨年度の報告書でも言及した、2007 年の中国による衛星破壊（ASAT）実験によって明示化された、宇宙アセットへの脅威への対処としての日米関係という構図を示している。すでに述べたように、現在の米軍は通信・偵察・測位など様々な分野で宇宙システムに依存しており、米軍の行動を支えるインフラの役割を果たしている。有事の際に他国が宇宙アセットである衛星などを攻撃することがあれば、米軍の戦力は圧倒的に低下し行動に大きな制約がかけられることとなる。そのため、宇宙アセットの抗たん性（resilience）は極めて重要な課題となっている。また、オバマ政権は就任当初から議会との関係が対立的で、宇宙関連予算も様々な形で制約を受けている。そのため、日本が積極的に宇宙分野に投資を行うことで日米同盟を強化する方針を歓迎しているのである。なぜならば、日本が独自の衛星を打上げ、その衛星によるサービスをアメリカに開放することとなれば、その分アメリカは予算を節約することができ、また有事の際に衛星攻撃によってアメリカの衛星が失われたとしても、日本の衛星が同等のサービスを提供することが出来れば、バックアップとして強力な支援を得ることが出来る。こうした側面から、日本が「政府全体アプローチ」を取り、安全保障分野における宇宙利用に積極的になることは、アメリカにとって、また日米同盟にとって大きな意味があると言える。

実際、2014 年の宇宙基本計画において示されている準天頂衛星の 7 機体制の構築は、アメリカの GPS と共通運用が可能な信号を利用しているため、もし GPS が衛星攻撃などで機能劣化した場合、一定のバックアップ機能を提供することが出来る。さらに、仮に GPS

が機能停止したとしても準天頂が 7 機あれば自律的な測位が可能になるため、日本を中心に東アジア、オセアニア地域では継続した測位が可能となる。また情報収集衛星の継続的運用や、陸域・海域の地球観測衛星から得られるデータは、米軍の持つ情報収集能力を補完し、情報共有のシステムが整えば日米双方にとって大きな資産となる。これらの衛星はアメリカが強い関心を持つ西太平洋、東シナ海、南シナ海の海洋監視（MDA）にも用いることが可能であり、中国の影響力が増している地域における情報収集に資するものとなるであろう。さらに、今回の宇宙基本計画で宇宙状況監視（SSA）体制の構築が進められることで、アメリカが持つグローバルな SSA ネットワークで手薄であったアジア地域から見た宇宙状況の監視が可能となり、宇宙空間の持続的利用可能性を高めることも期待される。

まとめ

日本の宇宙政策は長きにわたって「平和利用国会決議」によって安全保障面での利用が制限されてきた。2008 年の宇宙基本法によって法的な制約は大幅に緩和されたが、しかし歴史的経緯に伴う問題は現在も防衛省の宇宙に関する知見不足や JAXA の消極的な態度に見ることが出来る。しかし、防衛省は 2014 年 9 月に宇宙監視を専門とする部隊を設置し[13]、技術研究本部でも JAXA と協力しながら宇宙利用に関する研究を始めている。こうした日本の前向きな姿勢は日米同盟にも大きく貢献しており、日本がアメリカと対等な立場で情報共有を進め、宇宙アセットの運用を協議し、宇宙空間の持続可能な利用を目指すグローバル・ガバナンスにおいてパートナーとして活動するようになってきている。こうした変化を受けて、2014 年 9 月に総理指示が発出され、安全保障と産業振興を柱にした、新たな宇宙基本計画が策定された。

メディアではしばしばこうした動きに対して否定的な評価がなされるが、日本の外交及び安全保障から見ても、日本が安全保障分野における宇宙利用を進めることは積極的な意義を見出すことが可能である。また、その技術開発と運用においても宇宙基本法第二条に定められている「国際約束の定めるところに従い、日本国憲法の平和主義の理念にのっとり」という規定があり、一般に懸念されるような宇宙の（攻撃的な）軍事利用ということに結び付くとは考えにくい。しかし、こうした懸念を払拭する政治的なメッセージをどう表現していくかについては、今後の課題として残るであろう。

－注－

[1] 詳細は春原剛『誕生 国産スパイ衛星：独自情報網と日米同盟』日本経済新聞出版社、2005 年。

[2] Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle*. (Princeton, N.J.: Princeton University Press); John B. Alexander, *Future War: Non-Lethal Weapons in Twenty-First-Century Warfare*. (New York, Thomas Dunne Books/St. Martin's Griffin, 1999); Thierry Gongora and Harald von Riekhoff (eds.), *Toward a Revolution in Military Affairs?: Defense and Security at the Dawn of the Twenty-First Century* (Westport, CT: Greenwood Press, 2000); Donald H. Rumsfeld, Transforming the Military, *Foreign Affairs*, vol. 81, No. 3, May/June, 2002, pp. 20–32.

[3] Michael E. O'Hanlon, *Neither Star Wars Nor Sanctuary: Constraining the Military Uses of Space*. (Washington D.C., Brookings Institution Press, 2004)

[4] 安倍内閣総理大臣による指示（宇宙開発戦略本部会合（第８回））、内閣府、2014 年 9 月 12 日。<http://www8.cao.go.jp/space/comittee/dai27/siryou2.pdf> 2014 年 12 月 20 日アクセス。

[5] 例えば「宇宙開発はどこへ向かう?」NHK 時論公論、2014 年 11 月 25 日。<http://www.nhk.or.jp/kaisetsu-blog/100/204039.html> 2014 年 12 月 20 日アクセス。

[6] 「社説：宇宙基本計画―安保色が強すぎる」朝日新聞、2014 年 11 月 18 日;「社説:新宇宙計画案 安全保障に偏りすぎだ」毎日新聞、2014 年 11 月 8 日 ;「社説：宇宙基本計画 安全保障偏重でよいのか」西日本新聞、2014 年 11 月 20 日。

[7] 新「宇宙基本計画」（素案）、内閣府。2014 年 12 月 11 日。<http://www8.cao.go.jp/space/comittee/dai32/sankou1.pdf> 2014 年 12 月 20 日アクセス。

[8] Campbell K., Beckner C. and Tatsumi Y., *U.S.-Japan Space Policy: A Framework for 21st Century Cooperation*. CSIS, July 2003, p.26.

[9] 鈴木一人「欧州における軍民両用技術開発と安全保障貿易管理」『国際安全保障』第 32 巻第 2 号、2004 年 9 月、73-97 頁。

[10] Crystal Pryor, Strategic Imperatives for US–Japan Outer Space Cooperation, *Asia Pacific Bulletin*, Number 190, December 7, 2012.

[11] Office of the Press Secretary, Fact Sheet: United States-Japan Cooperative Initiatives, White House, April 30, 2012. <http://www.whitehouse.gov/the-press-office/2012/04/30/fact-sheet-united-states-japan-cooperative-initiatives> 2014 年 12 月 20 日アクセス。

[12] 宇宙に関する包括的日米対話 第２回会合共同声明、外務省、2014 年 5 月 9 日。<http://www.mofa.go.jp/mofaj/files/000038507.pdf> 2014 年 12 月 20 日アクセス。

[13] 「宇宙監視の新部隊 防衛省方針、ミサイルの兆候察知」『日本経済新聞』2014 年 8 月 29 日。<http://www.nikkei.com/article/DGXLASDE28H0R_Y4A820C1PP8000/> 2014 年 12 月 20 日アクセス。

第６章　北極海と日米同盟（その２）
－注目を要する安全保障・防衛面での懸念への対応－

金田　秀昭

はじめに

2013 年 12 月、JIIA「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」を命題とする調査研究事業における研究成果として、「北極海と日米同盟」と題するテーマで報告を行った。その際、わが国の官民における北極海問題に関する関心は、主として新たな海洋資源開発や国際海上交通路の利用といった点に向けられ、安全保障・防衛面での関心が極めて低いことに警鐘を鳴らし、幾つかの課題を提示した。

残念ながら、1 年が経過した今でも、北極海に関する安全保障・防衛、とりわけ日米同盟という視点での官民の関心が高まったとは言えない。安倍首相の第 2 次政権発足以来、安全保障・防衛問題への真摯な取り組みがなされ、制度や法整備などで大いなる進展を見せ、日米同盟に関しても、集団的自衛権の限定的な行使に道筋をつけ、日米防衛協力指針の改訂に関する両国当局間の協議が進展しているが、本研究の主テーマである「日米同盟の新しい課題」といった視点で北極海問題をとらえる動きは、十分とは言えない。

もっとも、現時点で北極海を巡る安全保障・防衛環境が、日本の安全保障・防衛面で喫緊の課題を提起しているという訳ではないのも事実であり、過敏になる必要はないが、的確な安全保障・防衛政策の遂行には、国際動向を踏まえた長期的視野に基づく先見的かつ周到な対応が必要であることは言を待たない。このような観点から、本稿では、前年報告後に生起した新たな事象を丹念に収集、分析しつつ、明白な事実となった北極海の変容がもたらす安全保障・防衛面への影響について、日米同盟という観点を主としつつ、現時点や近い将来にとるべき施策について幅広く提言する。

１．北極海変容の安全保障・防衛面の影響

前回と同様、北極海変容の安全保障・防衛面での影響についての分析に際しては、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、今回の報告でも、短期、中期、長期に分けて考察することとした。

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。いまだ国際的な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多く行われ始め、北極海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いる。

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得る。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・防衛問題に関与する意図を持つ国にとっては､戦略的な機動展開能力にかか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、今後の中国の海上核戦力の動向にもよるが、米国やロシアの拡大核抑止力の信頼性の低下が生じる可能性がある。更に、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も危惧される。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､北極海自体や､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、安全保障・防衛の側面においても、可能な限りの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

まずは、新たに重要な国際的海上交通路の誕生が及ぼす影響についてである。既に北極圏諸国のみならず、日本を含む欧亜の主要国が、この点について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、いまだ本格的とはいかないまでも、既にその航行実績は増加しつつある。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おり、北極圏に潜在する膨大な資源の開発への強い関心とも相まって、国際的な協力と競争が交錯し、行き着くところ、新たな国際的安全保障・防衛問題の生起に結びつく可能性がある。

一方、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。加えて、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課せられており、恒常的な利用には不確実性がある。その上、北極海は従来から「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、冷戦さなかの戦略原潜の活動を含む米ソ戦略核戦力の対峙という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ことに変わりはない。

（２）北極海を舞台とする軍事面の鍔迫り合い

他方、北極海を舞台とする関係国間の軍事面での鍔迫り合いは、既に生起している。しかも前回の報告以来、関係国間の緊張が緩和される方向での変化は見られず、むしろ高まる方向にある。特に 2014 年に入ってからの、ウクライナ問題を巡るロシアと米欧の対立に由来した緊張の高まりという側面もあり、こうした傾向は、ロシアによる北極圏での軍事力増強や軍事プレゼンスの急増に結び付いている。

前回報告と同様、北極圏諸国の中でもロシアの軍事面での動きは顕著である。ショイグ国防相は、北極が 2014 年の国防優先課題であるとして、北極海航路の利用における寡占的利益の確保のための立場を維持し、北極圏での国益確保のための北極圏領土保全機能を統合しつつ、北極圏に展開する部隊や基地（潜水艦基地や飛行場を含む）の新設、配備する兵力（特に潜水艦戦力）や砕氷艦船の増強などを進めている。2014 年 12 月には、北洋艦隊を主体として、西部軍管区の空軍や地上軍を統合し、北極海域と島嶼部を管轄する新たな「統合戦略コマンド」を創設した。一方、部隊運用においてもプレゼンスを高め、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、これを常続的に行う体制をとるとともに、原子力潜水艦の行動や対潜空中哨戒も活発化させている。2014 年 9 月には、北極圏を含む東部軍管区の全域で、冷戦終結後では過去最大となる複合戦闘訓練としての「ヴォストーク 2014」演習を実施した。

またロシアは、米国が核抑止力改善の一環として、北極圏での原子力潜水艦の活動を再活性化し、バレンツ海などにもイージス艦を配備するなど、海上核抑止体制を強化するとともに、BMD 機能を高めていく可能性が高いと見て、これに機先を制する形で、欧州への BMD 機能強化（EPAA）に対すると同様に、北極圏についても反対の意図を強く表明する一方、昨年は新型戦略原潜を北洋艦隊に配備し、2014 年 11 月には、新型 SLBM の発射を成功させている。この動きの中には、最近になって核兵器管理についての数多くの不備が指摘されている米国と同様、冷戦時代の遺物となりつつあった核戦力の、近代化による核抑止力の回復を目指す思惑もあるとみられる。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、更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み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。相互核抑止に関して、一定の信頼感が醸成されている米国に比し、意図や能力が不透明な中国の核戦力、とりわけ海上核戦力への警戒心が高まってきていると考えられる。

カナダは、ロシアとは異質ではあるが、ロシアと同様に北極に対しては高い軍事的関心を示し、「北方戦略：2009」では、北極における主権の行使を強調し、北極圏での哨戒、迎

撃、輸送、救難行動に適応する航空機やUAV兵力の整備を進めている。

米国は、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、2014年2月には、米海軍が「北極ロードマップ2014～2030」を発表し、短、中、長期の各期におけるロードマップを5年振りに更新した。短期（現在～2020年）では、水中・航空戦力による軍事プレゼンスを維持し、要員教育、戦略・政策・計画・所要等の策定を行い、中期（2020～2030年）では、更なる融氷が進むと見て水上艦の行動を増加させる一方、要員訓練・人員確保、定期的プレゼンスを持続的に行い、長期（2030年以降）では、北東航路や中央航路の航行可能域が増大すると見積もり、持続的作戦行動能力を保有し、前方展開部隊を維持するとしている。しかし米国は、大幅な国防予算の削減に直面しており、戦略核抑止や周辺海域防衛といった点で日本の安全保障・防衛に深くかかわる問題でありながら、北極海問題を最優先課題として取り扱わない可能性もあることから、日本として可能な限り、これを補完するための協力姿勢を示すことが肝要である。

欧州諸国の中では、ノルウェーの関心が高く、軍全体としての北極海での行動を意識した軍備の改善やロシアとの連携の強化が図られている。スウェーデンは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。デンマークは、中国のグリーンランドへの政治・経済的接近を警戒しつつ、同地に北極任務部隊を新編し、F-16戦闘機を配備し、北極海哨戒艦の建造にも着手している。アイスランドは、中国との関係を強化している。

アジア諸国では、中国は自らを「北極近傍国家」、「北極利害関係国」と自称し、政経産軍、硬軟織り交ぜて北極圏周辺環境の整備に力点を置いている。また、戦略・攻撃原潜の不透明であるが意欲的な増強を目指しており、米露を含む関係国の警戒心を呼んでいる。インドは気象観測装置を設置するなど関心を高めている。韓国は、北極圏に強い関心を向け、砕氷調査船の建造などでの中国との協力を進めている。

（３）北極海での資源獲得競争の激化

北極海での資源獲得競争は、ますます激化の方向にある。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。

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。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。しかし、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

しているが、計画策定や税制問題など未解決の問題が多く、開発計画は後倒しの状況となっている。

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、北極評議会加盟国への接近をあからさまにし始め、2012 年には、温首相がスウェーデン及びアイスランドを、胡主席がデンマークを訪問し、2013 年 12 月には、北欧 5 カ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た。

（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。この数字からは、北極海の航行が海運業的に経済的な効果をもたらすことへの期待に繋がるが、国内外の運行関係者の中には、期待するほどではないとの指摘もある。しかし、軍事戦略的に見れば、圧倒的なメリットが生まれ、グローバルな戦略環境に革新的な変化を与える。

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あらわれ、場合によっては、アジア・太平洋に振り向けられる米軍事力が若干縮小するといった可能性が生じ、これに伴い、日本の負担が増大することも起こり得る。

ロシアの関心は非常に高く、その海上戦略機動（欧亜間）能力改善に向けての意欲は顕著であり、北極圏での軍事優勢獲得に向けて特段の注力がなされている。特に前回報告以降では、北極圏への軍事基地（海上、航空、地上部隊）の改修や新設、北洋艦隊による北極海巡航や北極地域（ノボシビルスク諸島）での上陸演習など、北極圏での軍備の拡充や軍事演習が急速に行われている。

いずれにせよ、従来の地政学や軍事戦略では、全く顧みられる事がないか、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、北極圏諸国や日本など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

既に前（２）項で触れたように、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。米国国防省は、目下国防予算の大幅削減下、「中古となった」冷戦時代の核戦力の維持、近代化に苦慮している。このまま手をこまねいていれば、海上核戦力を含めた米核抑止力の信頼性の相対的な低下は、避け難くなる。これに加えて、米国を核戦力によって脅かす存在としてのロシア及び中国の相対的な核戦力の増強という現実がある。

まずは、ロシアであるが、北極海の変容により、戦略原潜の活動期間や哨戒範囲が拡大し、対米国戦略原潜兵力の北極圏における展開も容易化する。前回報告以来のロシアの動向を見てみると、戦略爆撃機（Tu-95MS）の北極圏哨戒飛行の強化、北極圏海軍基地網（水上・潜水艦）整備構想、航空宇宙防衛部隊の配備や早期警戒監視網・飛行場の再開、北極圏用ミサイル防衛システム（Pantsir-S1）の配備、SSBN/SSN の増強や対潜哨戒（Tu-142/Il-38）の拡大、戦略ミサイル軍のサイバー戦対処能力の強化など、核抑止力向上のための顕著な努力が傾注されている。

これに加え、中、長期的視点で見れば、そう遠くない将来、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）が北極圏や周辺海域（北部太平洋を含む）に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鍔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、北極海や周辺海域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ない。

となれば、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対露・対中核抑止能力の低下が起こり得る可能性が生じる。しかし、こういった点に関する米国の動きは、これまで比較的緩慢であり、北極圏での核抑止力低下に対する対策が十分にとられてきたとは言い難い。しかし 2014 年 8 月には、米下院が戦略核抑止について、北極海への関心を向けるよう勧告したり、大西洋艦隊の潜水艦部

隊指揮官が、ロシアのみならず中国の戦略原潜にも注意を払うよう促すなど、各方面からの警鐘が鳴らされるようになった。2014 年 10 月には、米国の有力紙 WSJ が、「中国の潜水艦隊：対米決定的抑止力」とする論評で、中国の戦略原潜の充実は、同国の「核先制不使用」戦略の維持にあいまいさを残すとの警戒心を米国内に呼ぶ結果となっている。

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。この点に関していえば、2014 年 4 月に米国の会計検査院の高官が、「日米同盟：重要性を増す日米海軍協力」と題して議会証言を行い、対潜戦（ASW）が 1980 年代同様、再び日米同盟の最前線となるであろうと予測したうえで、日米が共通のビジョンを持ち、あらゆるレベルでの戦略的関与を進めたうえで、来る日米防衛協力指針の改訂に加え、地域戦略に資する実行可能戦略議論を進めるべきであると指摘していることは見逃せない。

（６）周辺海域での多様な安全保障課題の生起

北極海そのものではなく、周辺海域において海洋を巡る多様な安全保障問題が生起する可能性が高ま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。日本周辺では、日本海やその出入り口となる３海峡（宗谷、津軽、対馬）、オホーツク海やベーリング海に繋がる北太平洋海域の航路が輻輳化する。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、益々、日本海や３海峡における海上交通が輻輳化する。また同時に、日本やロシアのみならず、中国や韓国（北朝鮮）による利用も増加することとなり、これらの海域において、海上保安や海洋安全保障面での問題が生起する可能性も高まることとなろう。最近、北朝鮮との国境線に近いロシア領ザルビノ港の中露共同による開発が報じられているが、このことを見越しての動きと見ることも出来よう。

一方、北極海や周辺の北方海域、日本海などでの海上交通が輻輳化すれば、海上における捜索救難、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についても、目に見える形で適切に関与することにより、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。

（７）北極海を巡る新国際ルール設定の必要性

繰り返しになるが、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は確立されていない。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。

最近の動きとして、北極条約の新規制定や国連海洋法条約の改訂を念頭に置き、国際的に開かれた公正な議論が必要になったとして、国際的なコンセンサス作りの機運が生じ、2014 年 11 月には、IMO（国際海事機関）が、北極海での国際ルール作りに乗り出した。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、日本がこの IMO による国際ルール作りに積極的に関与していくことが必要となる。この際 IMO が、北極評議会の意向を尊重することは想像に難くない。そのための日本にとっての現実的な選択は、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、北極評議会を通じて IMO 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。しかし米国には、国連海洋法条約を批准していないという弱点がある。最近、南シナ海での「航行の自由」問題に関連して、米国内にも同条約批准の動きを推す意見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ていくべきである。

２．日本の採るべき対応

これまで見てきたように、近年における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、今後わが国として如何なる対応を採るべきか。本稿では、「北極海と日米同盟」を主題におきつつ、短、中、長期的観点から、幅広く論究を進めていくこととする。

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は死活的に重要であり、「北極海の利用と国益に沿った外交政策」を推進すべきであろう。一方、中、長期的には、海洋立国たる日本としては、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」、更には「関係友好国との海洋安全保障協

力の見直し…海洋安全保障協盟の推進」を実現していくべきであろう。

（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るにつれ、北東アジア地域における海上交通のハブ港を国内に取り戻すことも可能となる。

日本は北極圏諸国ではないが､その生存と繁栄を海洋に大きく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、現時点では正確に見通すことは出来ないが、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、既述した IMO の動きにみられるように、北極海を巡る新たな国際法制定に関する協議には積極的に参加し、特に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。同時に、2013 年 11 月の日露「2＋2」の決定を遵守する形で、2014 年 10 月に日本海のウラジオストク方面で、日露合同海難事故訓練を実施したように、実力国ロシアとの信頼関係維持のための手立ても欠かしてはならない。

（２）防衛体制の見直し…自律防衛能力の強化

安倍内閣が昨年末に示した「国家安全保障戦略（NSS)」でも、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。既に述べてきたとおり、北極海を巡る安全保障・防衛環境の変化への対策が、喫緊の課題ではないとしても、見通し得る将来の課題として、わが国の中、長期的な防衛体制見直しに取り込まれるべきであることは明らかである。その方向性としては、北極海をも視野に捉えた形で、海洋安全保障に関する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や 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や周辺海域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 UUV の効果的利用が求めら

れよう。更に弾道ミサイル防衛能力の拡大、強化も必要となり、イージス艦の増勢に加えて、総合防空・ミサイル防衛（IAMD：Integrated Air and Missile Defense）の導入も必要となろう。一方、北極海や周辺海域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、北極海での通年行動能力の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）日米防衛協力態勢の見直し…日米同盟の深化

1997年制定の日米防衛協力指針については、2013年10月の日米外務・防衛閣僚による安全保障協議委員会（いわゆる「2＋2」）の決定により、2014 年末までに改訂することになっていたが、突然の衆議院解散、総選挙などの影響もあり、来春までに延期されることとなった。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。

また2014年10月には、日米防衛協力小委員会（SDC）により、日米防衛協力指針改訂の中間報告がなされ、日米両政府は、平時から緊急事態までのいかなる段階においても切れ目のない形で、日本に対する武力攻撃を伴う状況、あるいは日本と密接な関係にある国に対する武力攻撃が発生し、2014年7月1日の閣議決定（集団的自衛権の限定的な行使など）の内容に従って日本の武力の行使が許容される場合における、日米両政府間の協力について詳述する方針が示された。また日米同盟のグローバルな性質を反映するため、協力の範囲をグローバルに拡大する方針も述べられ、海洋安全保障や弾道ミサイル防衛などでの協力が示された。閣議決定や日米防衛協力指針の改訂に伴い必要となる法体系の改正案は、2015年春の通常国会に提出される運びとなっている。

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。しかし、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。米国の拡大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。この視点からは、まず、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洋領域把握（MDA：Maritime Domain Awareness）に関し、北極海や周辺海域においても協力していくことが必要となる。また、これを強化するための宇宙状況把握（SSA：Space Situational Awareness）での協力も同時に必要となる。

疑いもなく、日米防衛協力指針の改訂は、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（あるいは BMD を取り込む形での IAMD）、対潜水艦戦、掃海、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、日米同盟の更なる深化を図ることは、大いに意義がある。この際、北極海を巡る安全保障・防衛面での情勢の変化に即応し得る形で、日米防衛協力指針を、都度、改訂または一部修正していくことが求められよう。

一方、中露の極端な接近や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・防衛協力の実質的な強化は、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。

（４）関係友好国との海洋安全保障協力の見直し…海洋安全保障協盟の推進

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、安倍首相の進める「国際協調主義に基づく積極的平和主義」や「地球儀を俯瞰する外交」を具現化するため、欧米、インド洋・アジア太平洋地域の良識ある友好海洋国家（関係友好国）との海洋安全保障協盟（MSA: Maritime Security Coalition）の推進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・防衛面での関係友好国と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、北極海や周辺海域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を進めることにより、長大な海上交通路の安全保障を切れ目なく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

ちょうど1年前に、「北極海と日米同盟」という同様の趣旨で報告したが、1年を経て北極海を巡る状況、わが国の安全保障・防衛や日米同盟を巡る環境には、大きな変化が印されてきた。昨年報告した際の想定を超え、早いペースで北極海や周辺海域を巡る核を含む戦略環境の変化があらわれてきており、日本が一層、北極海問題に、安全保障・防衛上の観点から真剣に取り組むべきことを教えている。

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5月、ようやく他のアジア諸国と共に、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、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、更には関係友好国との海洋安全保障協盟の推進が求められている。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、更に集団的自衛権の限定的な行使を容認する閣議決定がなされ、日米防衛協力指針も日米当局間での合意・締結が間近いなど、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」や「地球儀を俯瞰する外交」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。また、先般の衆議院選挙では与党が大勝し、今後の政権運営基盤を確固たるものにした。ついては、ここに改めて「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、一連の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：米国の政策と日本の対応

池島　大策

はじめに

本稿は、「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」と称して日本国際問題研究所において 2 年間にわたって行われた調査研究事業における最終年度の報告書を構成するものである。本稿の主な問題意識は、グローバル・コモンズとはそもそも何か、北極海がサイバー空間や宇宙と同様にグローバル・コモンズを構成するものであるか、そして北極海はサイバー空間や宇宙空間と同様に日米同盟が作用するものといえるか否か、という点にある。その理由は、筆者の従来からの研究において、グローバル・コモンズの概念[1]や北極海をめぐる国際法（海洋法を含む）[2]上の論点、日本の安全保障と日米同盟との関連といった事項が法政策上それぞれ複雑に関連しながらも、その内実においては現在進行形の現実と法理論との相違や、近似的な関係にありながらも日本の置かれた状況や現在の国際事情に照らせば、これらの事項が本研究会の根本テーマとして適切に措定されうるか否かという疑問と無縁ではなかったからである。

既に、筆者は、同研究所における幾つかの研究会の報告書において、本研究会に関連する論点につき詳述している。まず、平成 24 年度（2012 年度）の調査研究・提言事業「北極のガバナンスと日本の外交戦略」において、報告書「北極のガバナンス：多国間制度の現状と課題」[3]の中で、北極(海)におけるより良いガバナンスのために既存の枠組みとしての北極評議会（AC）や、国連海洋法条約（UNCLOS）を中心とした海洋法など可能性と限界を踏まえて、北極圏諸国との連携を基礎に日本が従来行ってきた施策の拡充を行うような外交戦略を展開することが肝要である旨を述べた。

また、筆者は、同研究所の同年度の別のプロジェクト「米国内政と外交における新展開」では、報告書「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―」[4]において、米国が UNCLOS に加入できない国内的な事情と米国自体が UNCLOS の定立過程とその後において果たしてきた役割とその限界などを論じながら、安全保障や国益の観点から米国の内政と外交との関係を明らかにした。

続いて、筆者は、昨年度における本研究会報告書「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」[5]の中で、広義の非伝統型安全保障という概念においてこそ、北極海及びその沿岸諸国との関係において環境保護や持続可能な開発とが両立し得る分野で

あって、日本が現行の憲法の枠組みにおいて従来の外交政策・戦略を推進し得るとの考え方を示している。

以上の各種報告書を執筆する機会の前後やその期間中にも、筆者は、北極海に関する別の若干の論考[6]において、本稿に深く関連する論点につき概ね次のような内容の考察を行っている。つまり、(1) 北極海においては、環境保護と持続可能な開発を目指す AC が事実上の主要フォーラム兼レジームとなっているが、南極における南極条約体制とは異なることから可能性と限界を併せ持っているということ、(2) 北極圏諸国と非北極圏諸国は、北極海に特有かつ独自の安全保障とガバナンスに関する概念を理論と現実を踏まえて政策として実施する責務を国際協力によって果たすべきであるということ、そして、(3) 常任オブザーバーの地位を得た日本は自国の足場を踏み固めて北極海の有効なガバナンスと広義の安全保障に資することに貢献すべきであるということ、である。

さらには、ここ数年の間に参加した主な北極海関連の国際的な学術大会・研究会[7]においても、以上に述べた諸点を筆者は大なり小なり重ねて繰り返しつつ、また同様な感触を国内外の研究者や実務家からのフィードバックや意見交換を通じて、再確認することができた。

そこで、以下では、これまでの議論と検討を基礎にして、まず、日本の北極政策ともいうべきものを概観しつつ日米同盟の方向性との関連を論じ、次に米国の北極政策と安全保障に関する北極海の事情を検討したうえで、最後に日本の北極政策に関わる課題を述べることにする[8]。

１　日本の北極政策と日米同盟

（１）日本の北極政策[9]

日本の北極地域における観測や科学調査の研究は、早くは 1950 年代から行われているといわれている。しかし、地球の気候変動によって北極航路が開拓される可能性が高まることに日本で注目されだしたのは歴史的に浅く、日本の動きも他国に比べて後れを取っているといえる。

2013 年 4 月に定められた「海洋基本計画」[10]では、「気候変動がもたらす北極海の状態の変化等を受けて、我が国としても、海上輸送の確保や海上交通の安全確保、研究・調査活動の推進、環境の保全、国際的な連携や協力の推進等、検討・対応すべき多岐にわたる課題が生じている。このため、今後、これら諸課題について、総合的かつ戦略的な取組を進める。」[11]とされ、同年 7 月 30 日に設置された関係省庁連絡会議により、ようやく北極地域にかかわる国家政策の整備が始まったといえる。

また、2013 年の秋から 2014 年までに、北極観測船（砕氷船）の建造の具体的検討を政府が開始したことも報じられている[12]。2014 年 5 月 30 日には、「北極海航路に係る官民連携協議会」[13]の第 1 回会合も行われ、情報共有や意見交換等がなされた。特に、この官民連携協議会は、北極海航路の将来的な利活用に関して日本が国を挙げて政府機関と民間企業などとの連携を深める上での重要なフォーラムであり、国土交通省総合政策局海洋政策課が事務局となって関係省庁からの情報提供と参加企業との意見交換などを幅広く行っていることが活動状況からうかがえる。さらに、最近では、日本が北極海航路の将来的な利用を見据えて、官民（産官学）連携や学術交流を交えながら、より専門的な国際セミナーを開催する機会が増えつつある[14]。

こうした動きは日本の北極政策が主として従来からの観測・科学研究事業と今後の経済的活動を柱とするものであって、ここに科学（学術）や経済の視点はあったとしても、軍事（安全保障）の視点は皆無とは言えないまでも極めて乏しいことが分かる。

しかし、こうした動きからは日本の北極政策と安全保障との関係は必ずしも明らかではないし、憲法と日米同盟との関係が北極政策に及ぼす影響にも配慮する必要がある。

（２）日米同盟の方向

日米同盟を中心とする日本の安全保障に関して、安倍晋三政権下の近年の一連の動向が注目される。2013 年 12 月 17 日に決定された「国家安全保障戦略について」[15]や、2014 年 5 月 15 日の「安全保障の法的基盤の再構築に関する懇談会報告書」[16]においても日米同盟の強化や深化が謳われる一方で、同年 7 月 1 日に行われた閣議決定「国の存立を全うし、国民を守るための切れ目のない安全保障法制の整備について」[17]では、従来の内閣がとってきた集団的自衛権の行使に関して現行憲法下では禁じられているとされる解釈が変更されて、その行使が許される旨の解釈が採用されるに至った。

さらに、加速する日米同盟の深化は、2014 年 10 月 8 日に明らかとなった「日米防衛協力のための指針（ガイドライン）の見直しに関する中間報告」[18]の中でも、自衛隊の活動への地理的制約の除去、「周辺事態」の文言の削除、そして日米協力の拡大として「宇宙及びサイバー空間」まで対象とされたことで明確となってきた。もとより、この中間報告を経て、同年 12 月 19 日の「2+2」日米安全保障協議委員会（SCC）共同発表[19]では、日本の安保法制作業の「進展」を考慮して、「明年前半」、つまり 2015 年前半における「指針の見直しの完了」を待つこととなった。

もっとも、この「日米協力の拡大」の射程にはたして北極海が含まれるのか否かは明確でない。上述したように、本研究プロジェクトでは、宇宙空間、サイバー空間と共に、北

極海がはたしてこれらの空間と同様なグローバル・コモンズといえるか否かが問われる中で、当該中間報告におけるこれらの空間の位置付け（言及の有無を含む）を正確に読み解く必要がある。なぜなら、中間報告では、「同盟の文脈での宇宙及びサイバー空間における協力」が重要であることに日米両国間の共通認識があることが示され、その「VII.　新たな戦略的領域における日米共同の対応」の項では宇宙空間とサイバー空間における安全かつ安定的な利用を確保する政府の取組に自衛隊と米軍が寄与することや、これらの空間における両国間の協力が明記されたものの、北極海という文言の記載が見られないからである。その訳は不明であるが、「アジア太平洋及びこれを越えた地域」の安定や平和・繁栄のために日米の「切れ目のない」共同対応や「日米同盟のグローバルな性質」、そして「協力の範囲を拡大」した分野としての「海洋安全保障」といった文言に北極海が含まれるという考え方がはたして可能か否かは現状では疑問が残るであろう。見直し後の指針といえども、中間報告の「III.　基本的な前提及び考え方」にあるとおり、国際法の基本原則、国連憲章、日米各国の憲法、適用のある国内法令などに加えて、日本の行為が「専守防衛、非核三原則等の日本の基本的な方針に従って行われる」という制約を受けることを明記していることは興味深い。

そのうえ、この見直し後の指針は、日米同盟の根幹をなす日米安保条約との整合性の問題も生じるであろう。その時、同条約からの乖離が大きな焦点となる。日本および「極東」の範囲（同条約前文、5 条、6 条）との関係で、どこまで認められるのかが問題となる。

２　米国の北極海政策と安全保障に関する北極海事情

日米同盟を論じるうえで、やはり日本のパートナーである米国の北極政策を考察しておくことも必要である。はたして米国の北極政策と日本のそれとの間に齟齬がないかが問われるからである。

（１）米国の北極海政策[20]

そもそも、オバマ第 1 次政権はその北極政策について、前 G.W. ブッシュ政権下で 2009 年 1 月 9 日に出された「北極地域政策指令」（NSPD 66/HSPD 25）[21]を引き継ぎ、同指令に基礎を置いていた。その後、2010 年 5 月に出された「国家安全保障戦略」[22]において、北極に関して米国が「国家安全保障のニーズに見合うよう、環境保護を行い、責任を持って資源を管理し、原住民社会を考慮して、科学調査を支援し、かつ幅広いイシューに関して国際協力を強化する」[23]ことは明らかになったものの、政権としての明確な北極戦略は打ち出されなかった[24]。しかし、グローバル・コモンズへのアクセスの保持が軍事上重要であることを強調している点と、グローバル・コモンズを守る（セーフガード）との名目で

共有された海洋、空及び宇宙のドメイン（しかも、これらの場所は「排他的国家管轄権の外に存在する」と説明される）の利用を最大限にすることとは別の項目として、「北極海における利益」の中で上記の国際協力の強化が指摘されている[25]。

実際にオバマ政権が独自の北極政策を明確にしたのは、その第２次政権発足後の 2013 年 5 月 10 日の「北極地域国家戦略」[26]においてであり、その中で米国が「責任ある管理者の立場」(responsible stewardship)を取る方針が打ち出された。ほぼ同時期に沿岸警備隊(CG)の「北極戦略」[27]（同年 5 月）や、続いて国防総省（DoD）の「北極戦略」[28]がそれぞれ公にされた。2014 年 1 月にはホワイトハウスによる「北極地域国家戦略実施計画」[29]としてさらに具体的な方向性やプロセスが明らかになり、米国海洋大気庁（NOAA）が「北極行動計画」[30]を発表し、会計検査院（GAO）が予算措置関連について若干の見解（資源ガバナンス・レジームの強化、環境保護、北極大使等について）を示した点などが注目される[31]。

これらの諸文書等からうかがえる重要な共通点は、自国の安全保障、責任ある管理者の立場、そして国際協力の３点であると考えられる。特に注目すべきと思われる点は、最後の「国際協力」への言及である。示唆されているのは、米国だけの単独の施策を行う意図も能力・余裕にも事欠く状況下（予算上の制約、近隣諸国との関係、国内政策との優先順位の兼ね合いなど）で、むしろ関係諸国間との協力を通じた連携や取組を米国が重視するという方針であろうと推察される。

さらに、2014 年 2 月に発表された「米海軍　北極ロードマップ 2014-2030 年」[32]では、海軍の任務や役割という観点から中長期的なビジョンともいうべきものを読み取れることと、グローバル・コモンズへの言及が見られることが特筆される。とりわけ興味深い点は、まず、長い歴史を有する北米大陸における安全保障上のパートナーとしてはカナダを明示しているにとどまるということである。次に、気候変動による国際航路の実現可能性について、北極海が「安定的かつ紛争のない地域」であるとの認識に立ちつつ、その背景として信頼と協力の必要性が強調されている。また、沿岸警備隊(CG)、省庁間、北極圏パートナーとの間の協力が重要であることから、短期的（現在～2020 年）には現行のあり方で十分としつつも、中期的（2020 年～2030 年）には他の政府部署への支援の提供を必要とすることが述べられ、長期的（2030 年以降）には、当該支援を拡大していくことを予測する内容となっている。しかし、グローバル・コモンズという用語への定義や具体的な説明もなく、文脈上は北極海がグローバル・コモンズであるということが当然であるかのような記述の仕方で、「グローバル・コモンズ（すなわち北極海）へのアクセスと海洋の自由」は北極海において米国海軍によって確保されるという点がこのロードマップでは強調されている[33]。

ちなみに、2015 年 2 月 6 日の「国家安全保障戦略」[34]においても、「共有空間」(shared spaces)[35]と

位置付けられたサイバー、宇宙、空および海洋に対する自国のアクセスの確保が重視されており、過去数年間において「前例のない国際協力」（unprecedented international cooperation）を基礎に前進させる場所の一つとして、特に北極海が挙げられている点が注目される[36]。しかし、2015 年版の「国家安全保障戦略」においては、グローバル・コモンズという言葉は見られない。

以上のような米国の北極政策に関するいくつかの特徴以外に、留意しておくべき米国の国内事情として、厳しい財政事情から生ずる制約があり、そのほかに議会の理解を得る必要がある点を軽視することはできない。

日本の第２次安倍政権において安全保障に対する新しい方向性が出され始めた 2014 年 8 月には米国の議会調査報告書「北極海における変化：議会のための背景と争点」（CRS）[37]でも、北極海が「潜在的な、顕在化しつつある安全保障上の争点」であることが認められ、米国とカナダの間で北米航空宇宙防衛司令部（NORAD）による監視、情報共有、協力強化が謳われ、沿岸警備隊と海軍の役割強化を行う上で、財政課題とのバランス、他国等との（AC、国際海事機関（IMO）、イヌイット極域評議会等における）協力、環境上の対応や捜索救援活動の意義が示されている。

最後に、以下の点は、米国固有の国内事情として念頭に置いておく必要がある。すなわち、米国は、北極海の沿岸諸国（特に、アラスカ州の位置）の一つであり、石油や天然ガスなどの資源、エネルギー開発、漁業、環境保護、航行の自由などの点で利害関係が大きい国であると考えている[38]。とはいえ、国連海洋法条約（UNCLOS）にはまだ加入していないという事情から[39]、北極海の事項が UNCLOS に反映されている慣習国際法によって規律されるとの立場を米国は維持していると解される。AC の 2015 年の会期から議長国となる米国は、これまでは必ずしも有力な北極圏諸国の一つと目されていないのが実態であることから[40]、今後の会期でどのようなリーダーシップを発揮するのか、そして「国際協力・平和の空間としての北極海」をどういう方向へ誘うことになるかが注目されている[41]。米国の関心は、国際協力を推進すべき場所としての北極海にあると考えられる。他方、北極海をめぐるこれらの事情に対する米国議会の理解は依然としてローキーともいうべき低調なままで、財政上の裏付けを欠く北極政策からは具体像が浮かび上がりづらい状況に米国は置かれているというのが現状であろう。

（２）安全保障に関わる北極海の事情

それでは、次に、日本や米国以外における安全保障をめぐる国際的な環境はどのようになっているのであろうか[42]。日米同盟というバイラテラルな関係といえども、国際社会と

の関わり無しに存在するものではない以上、日米同盟が置かれた国際的な状況を若干振り返っておく必要があろう。

北極海沿岸諸国の間においては、たとえば、2010 年には米国、カナダおよびデンマークの間で海軍の共同軍事演習が行われているなど[43]、冷戦以後も、沿岸諸国相互に安全保障上の関心を維持し、平和と安定を維持するための努力が二国間または多数国間における合意や了解を通じた様々な形態の協力（環境、輸送、調査・研究、軍事を含む）として継続されている。AC 自体が安全保障上の問題を扱わないことを前提としているため、AC での具体的作業が比較的中立で合意を得やすいテーマである捜索救援（SAR）や油漏れ対応関連の課題に焦点を当てることになった。したがって、こうした経緯は、ある意味で自然な成り行きであったと言えよう[44]。

また、北極海における北大西洋条約機構（NATO）の関与に対して、北極圏諸国の間にはいわば温度差もあることに留意しておかなければならない。たとえば、カナダは NATO が北極海における安全保障関連の事項に関与することに強い懸念を有している。他方、沿岸国としてのロシアは、クリミア情勢、それに関わる各国の報道等から察するに、NATO の影響力や介入によって北極圏にクリミア情勢から生まれる危機感や緊張が拡散することを懸念し、その抑圧を欧州諸国ともども模索しつつある。

最後に、非北極圏諸国、中でも中国[45]の動きに対する評価は多様であって、また今後どう推移するかは定かでない[46]。成長と台頭の著しい中国が北極海におけるプレゼンスを増し、資源開発において関与の度合いを高めるにつれて、こうした非北極圏諸国の進出が持続可能な発展を目指す北極圏諸国にとって好機となるか、または脅威となるかは、各国・地域が抱える課題と無縁ではない。北極海以外の世界の海域における中国の果敢な進出として東シナ海や南シナ海における状況を例に、それに類似した、またはそうした状況を類推するような事態が北極海にも今後生起し得ると危惧する見解も少なくない。このように、非北極圏諸国の動きに対する評価に一致や収束が見られない以上、安全保障上の課題にも今後は慎重な精査と分析が必要になるという状況である。

こうした北極海における新たな動向という点で、日本の『平成 26 年版防衛白書』[47]によれば、「ロシアをはじめとした沿岸諸国の一部は、自国の権益確保や領域の防衛を目的に軍事力の新たな配置などを進める動きもある」とされ、北極圏は「将来的には、海上戦力の展開や、軍の海上輸送力などを用いた軍事力の機動展開に使用されることが考えられ、その戦略的重要性が高まっている」と認識されている。しかも、ロシア[48]は「他の沿岸諸国に比べて有力な軍事力の配備による軍事的優位性を背景に、沿岸諸国の中で最も活発な動きを見せている」一方で、中国も「北極圏に積極的に関与する姿勢を見せている」という

状況にある[49]。これらの点から、とりわけロシアと中国が、北極海における安全保障上の動向を注視すべき対象と日本側には映っているともいえる[50]。したがって、これらの二国を視野に入れて今後は北極海においても日本の安全保障を考えなければならないということが日本の立場であると推察される。要は、こうした見方を他の北極圏諸国とどの程度共有することができるのか、そして特に米国との間ではどのような認識を共有できるかが問われることになると思われる。

３　日本の今後の北極(海)政策の確立へ

日本が北極海と関わりを有するようになったのは、極域における科学調査・研究を通じてであり[51]、そうして得られた知見や経験を特に環境保護の分野において発揮するという過程において日本は定評を得てきたといえるであろう。その意味で、北極海における平和と安定の維持に加え、国際協力の促進という点で、非北極圏諸国の一つである日本の貢献度は広く知られ、実績の厚みにおいて一定の信頼を得られているといえる。

他方で、北極海への政治的・経済的な関与の歴史は比較的浅いと言わざるを得ず、日本は後発国としての立場に甘んじている。その分、不信感を買うような活動や意図が見られたわけでもなく、平和国家としての名声と経済大国としての足跡に照らしてみても、日本の関与に対して、北極圏諸国から得られた信頼は、日本が AC の常時オブザーバーの地位を 2013 年に付与されたことにも表れている[52]。もとより、日本には今後このオブザーバーの地位をどのように活用して、北極海の平和と安定に今以上の寄与をすることができるのかを至急検討し、そのための政策を実施していくことが必要になるであろう。

今後の経済的な関わりとして、北極海航路（NSR）の利用[53]、沖合資源の開発や利用において、日本の経済界の関心が低いわけではないし[54]、独立行政法人石油天然ガス・金属鉱物資源機構（JOGMEC）を始めとした開発分野での進出や、投資への参加を行っている企業も少なくはない[55]。ただ、航路の利用という点において、NSR が日本と欧州とを結ぶ南回りの航路に代替するようになるとの見通しまでには経済界全体がなっておらず、当分はせいぜいスポット利用に留まるとの予測もある[56]。世界的な原油安が今のままでは、特に船舶・海運・保険業者にとってコストやリスクが依然として負担となる NSR に対する今以上の経済的なインセンティブは生じにくい。この点は、専門家以外にもおそらく容易に理解されるであろう[57]。

であるとするならば、日本は科学・観測・調査[58]を中心とした活動以外での関与は限定的なものになると当面は予想される。もちろん、学術的な分野からすれば、いわば理系分野だけにとどまらず、幅広く人文・社会科学系の研究者や教育・研究機関の相互交流を促

進・発展させることが今後の大きな課題ともなるであろう。その意味では、2015 年 4 月に富山で行われる「北極科学サミット週間」[59]は、北極研究に関わる広範な科学・学術分野を取り扱うもので、産官民挙げて北極研究に関する日本の存在感を示すための大きな試金石となりうる。

ここで考察している日本の北極政策は、前項「1. 及び 2.」までに検討した日本と米国とのバイラテラルな関係、日本が国際社会で置かれた立ち位置、日本が AC およびその参加国・主体と結ぶ関係などと深く関連していることはいうまでもない。そのため、日本だけが独自に突出した言動を示すような事態は避けなければならないし、日米同盟の今後の拡大深化や日本の安全保障政策全体における整合性も同時に図ることが求められる。したがって、北極海における日本の関与と立場、それを示す北極政策という点で、安全保障を中心とする日米同盟のバイラテラルな関係を北極海関連の事項やイシューにまで拡張する必要性の有無､その際に他の諸国からありうる反応や要請の有無等を入念に勘案した上で、慎重な行動をとることが日本の将来にも有益であろうと考えられる。

おわりに

本研究会の大きなテーマは、グローバル・コモンズとしての宇宙、サイバー空間および北極海の平和・安定的な利用における日米同盟の役割である。そもそもグローバル・コモンズとは何か、また北極海が他の二つの空間のようなグローバル・コモンズかといった根本的な問題は、本稿の性格上、また紙幅の制約上、別の機会に譲らざるを得ず、筆者がそれに関して既に著したいくつかの論考を見ていただかざるを得ない。実は、北極海をどのような空間として位置づけるべきかによって、日米同盟との関わりや接点の有無が変わってくるわけで、その意味で北極海が冷戦後にあっても平和と安定が比較的成功裏に維持されてきた地球上の数少ない空間であるという事情は単なる偶然ではないであろう。しかも、この平和と安定のためにとりわけ北極圏諸国の中でも 5 つの沿岸諸国（Arctic 5）が果たしてきた広範かつ長期の真摯な努力は、AC の諸活動やガバナンス状況にも見られるように[60]、広く世界で共有されている。その際に、最も注目すべきは、軍事・安全保障の面をも含めて、あらゆる側面において北極圏諸国の多様な関係を中心に国際協力が進展してきた経緯とその意義であろうと考えられる。

次に、日米同盟が機能しうる地理的範囲や政治的意義についても、日本が憲法第 9 条下で取ることのできる集団的自衛権に基づく対応･措置に関する解釈の変更を 2014 年 7 月に閣議決定によって行ったことから、どのようなことが起こりうるかを予め検討しておく必要がある。北極海において日米同盟が作用する状況を日本国憲法の解釈上は想定できない

との立場を政府は本来なら取ってきたと推察されるが、それが近時の解釈変更やその後の一連の政府の動きから見れば、日米同盟が作用し得る事情が北極海に今後、生じ得るか否かは新たに日本に課された決して容易でない課題となるであろう。解釈変更に伴って必要となる国内法の整備・修正は、中長期的な視野の下に行われるべきものでもあり、実際の運用がいつになるかを予見することはできない。また、上述したような北極海をとりまく事情から、北極圏諸国の中で想定される相手国(ありうるのは米国の場合がほとんどと推察される)からの要請（または事前合意・了解）に基づく日本の関与（国家的な言動に基づく介入）にどれだけ自国の主体的な制約と抑制を日本自身が課すことができるか、また日本へのどのような期待が当該相手国にはあるか（またはないのか）などを予め想定して、理解しておく必要がある。日米同盟のバイラテラルな関係は、北極海をめぐる北極圏諸国相互のバイラテラルやマルチの関係にも影響を受けるし、日米と非北極圏諸国との関係にも場合によっては大きく左右されることになる。これらについての明確なビジョンとそのために有効な実施方法に基づいて、日本は北極政策を起案し、遂行することが肝要である[61]。

最後に、繰り返しになるが、国際社会における日本の立場を政策立案者が十分踏まえた上で、日米同盟の役割と働きの文脈を考えるべきであろう。とりわけ、日本と北極圏諸国または Arctic 5 との関係、日本と AC との関係、また日米同盟関係や日本の政策が国際社会の利益（公益）に及ぼしうる影響を十分に検討すべきであることはいうまでもない。

－注－

1　グローバル・コモンズの概念については、池島大策「1　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」、日本国際連合学会編『グローバル・コモンズと国連』(『国連研究』第 15 号)、国際書院、2014 年、21-56 頁およびそこで引用された文献を参照。

2　北極海に関する国際法の最近の文献について、たとえば、以下のものを参照。奥脇直也・城山英明(編著)『北極海のガバナンス』（東信堂、2013 年）（この英文書評として Taisaku Ikeshima, ‘Book Review’, *Japanese Yearbook of International Law*, Vol. 58 (2015)を参照）。Michael Byers, *International Law and the Arctic*, Cambridge University Press, 2013 (この英文書評として Taisaku Ikeshima, ‘Book Review *International Law and the Arctic’*, *Transcommunication*, Vol. 1 (2013).を参照).

3　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、63-78 頁（HP は＜http://www2.jiia.or.jp/pdf/resarch/H24_Arctic/06-ikeshima.pdf＞(accessed 31 January 2015)を参照）。

4　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―」、平成 24 年度報告書『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（HP は＜http://www2.jiia.or.jp/pdf/resarch/H24_US/09-ikeshima.pdf＞(accessed 31 January 2015)を参照）。

5　池島大策「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」、平成 25 年度報告書『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』、日本国際問題研究所、2014 年、77-89 頁（HP は＜http://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/08-ikeshima.pdf＞(accessed 31 January 2015)を参照）。

6　上記の注以外に、主なものとして以下を参照。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 巻、2013 年、46-53 頁；池島大策「グローバルコモンズとしての北極海と

安全保障：国際法の視点から」（分析レポート）、2013 年、＜ http://www2.jiia.or.jp/pdf/research_pj/h25rpj06/131204_ikeshima_report.pdf ＞(accessed 31 January 2015)；Taisaku Ikeshima, ‘China’s Interests in the Arctic: Threat or Opportunity?’, *Transcommunication*, Vol. 1 (2013), Waseda University Graduate School of International Culture and Communication Studies, 2014, pp. 73-83; Taisaku Ikeshima, ‘Arctic States and Asian States for Arctic International Governance and Security: A Japanese View-point’, *Transcommunication*, Vol. 2 (2014), Waseda University Graduate School of International Culture and Communication Studies, 2015, pp. 83-91.

[7] 主要な口頭発表等として以下のものが含まれる。Taisaku Ikeshima, ‘Cooperation in the Arctic: Some Lessons from the Antarctic Treaty System’, at the 3rd Meeting of the Japan-Canada-US Conference Series on Trilateral Cooperation in Washington, D.C., May 7-8, 2012, at < http://www.eventbrite.com/e/trilateral-cooperation-washington-dc-registration-3436545801 > (accessed 31 January 2015); Taisaku Ikeshima, ‘Arctic States, Asian States and Arctic International Governance and Security: A Japanese Perspective’, at Joint CRCLA & DIR Workshop: ‘Arctic Nexus in Asian-Nordic+ Relations’, Aalborg, Denmark, 5-7 November 2014, at < http://www.aau.dk/arrangementer/vis/workshop-on-arctic-nexus-in-asian-nordic--relations.cid141964 > (accessed 31 January 2015); 池島大策(討論者)による、国際セミナー「ロシア北極圏の持続的発展」セッションⅠ「北極圏の持続可能なガバナンスに向けて」におけるコメント、2015 年 1 月 31 日、虎ノ門 HILLS2 階ホール、＜http://src-h.slav.hokudai.ac.jp/jp/seminors/src/2014.html＞(accessed 31 January 2015)。

[8] 上記の諸文献以外に、本稿に関連する最近の北極海事情に関するものとして、以下のものを参照。『国際問題』627 号、2013 年の「北極海特集」として、國方俊男、西元宏治、北川弘光、原田大輔、石原敬浩の各氏による各論考。*The Politics of the Arctic*, Edited by Geir Hønneland, Edward Elgar, 2013; *Polar Geopolitics?: Knowledges, Resources and Legal Regimes*, Edited by Richard C. Powell & Klaus Dodds, Edward Elgar, 2014.

[9] 北極に関する日本の外務省の HP については、＜http://www.mofa.go.jp/mofaj/press/pr/wakaru/topics/vol107/＞（accessed 31 January 2015）を参照。文部科学省の北極研究に関する HP については、＜http://www.mext.go.jp/a_menu/kaihatu/kaiyou/gaiyou/1343292.htm＞（accessed 31 January 2015）を参照。北極観測に関する国立極地研究所の HP については、＜http://www.nipr.ac.jp/aerc/＞（accessed 31 January 2015）を参照。なお、これら以外にも、官邸や国土交通省、経済産業省がそれぞれの資料を作成した HP を掲出しているが、紙幅の都合上、ここでは割愛する。

[10] 海洋基本計画は、官邸の HP＜http://www.kantei.go.jp/jp/singi/kaiyou/kihonkeikaku/130426kihonkeikaku.pdf＞（accessed 31 January 2015）を参照。

[11] 「海洋基本計画」8 頁。

[12] 「北極観測船、政府が新造検討　航路活用、出遅れ挽回」MSN 産経ニュース、2014 年 1 月 26 日、＜http://sankei.jp.msn.com/life/news/140126/trd14012614110012-n1.htm＞ (accessed 21 October 2014)を参照。

[13] 国土交通省の「北極海航路に係る官民連携協議会」の HP＜http://www.kantei.go.jp/jp/singi/kaiyou/sanyo/dai14/siryou3.pdf＞(accessed 20 February 2015)を参照。

[14] たとえば、以下のものを参照。国立極地研究所の主催による GRENE 北極気候変動研究事業特別セミナー「北極海航路の利用実現に向けて」2014 年 11 月 17 日、＜http://www.nipr.ac.jp/grene/20141117seminar/＞(accessed 31 January 2015)、国土交通省海事局が米加露の専門家を交えて開催した「北極海航路の航行安全に関する国際セミナー～極海域における船舶の運航と船員の訓練～」2015 年 1 月 20 日、＜http://www.mlit.go.jp/report/press/kaiji04_hh_000063.html＞(accessed 31 January 2015)。特に、筆者も参加した後者は、「極海域綱領」（Polar Code）が国際海事機関（IMO）において審議・採択が大詰めを迎えたことに因んだものとして、船舶・保険業界を中心に関連業界にまで注目される最近の内容を反映した実務上重要なものと位置づけられる。

[15] 内閣官房の以下の HP＜http://www.cas.go.jp/jp/siryou/131217anzenhoshou.html＞(accessed 31 January 2015)にある文書等を参照。

[16] 報告書は、官邸の以下の HP＜http://www.kantei.go.jp/jp/singi/anzenhosyou2/dai7/houkoku.pdf＞(accessed 31 January 2015)を参照。

[17] 閣議決定の原文は、以下の HP＜http://www.cas.go.jp/jp/gaiyou/jimu/pdf/anpohosei.pdf＞(accessed 31 January 2015)を参照。

[18] この中間報告の原文は、防衛省・自衛隊の HP＜http://www.mod.go.jp/j/approach/anpo/sisin/houkoku_20141008.html＞(accessed 31 January 2015)を参照。

[19] 防衛省・自衛隊の HP＜http://www.mod.go.jp/j/approach/anpo/sisin/js20141219j.html＞(accessed 31 January 2015)を参照。

[20] オバマ政権以降を中心とする。なお、米国の北極政策について、米国政府の以下の HP＜http://www.arctic.gov/portal/policy.html＞(accessed 31 January 2015)を参照。
[21] 原文は、以下の HP＜http://www.fas.org/irp/offdocs/nspd/nspd-66.htm＞(accessed 31 January 2015)を参照。
[22] 原文は、以下の HP＜http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf＞(accessed 31 January 2015)を参照。
[23] 同 50 頁。
[24] なお、2011 年の 5 月における米国防総省の「北極海における軍事行動と北西航路に関する議会に対する報告書」において、将来、北極海において必要なインフラ整備のための評価を主として行うものである。原文は、以下の HP＜http://www.defense.gov/pubs/pdfs/Tab_A_Arctic_Report_Public.pdf＞(accessed 31 January 2015)を参照。
[25] 「2010 年国家安全保障戦略」49-50 頁。
[26] 原文は、以下の HP＜http://www.whitehouse.gov/sites/default/files/docs/nat_arctic_strategy.pdf＞(accessed 31 January 2015)を参照。
[27] 原文は、以下の HP＜http://www.uscg.mil/seniorleadership/docs/cg_arctic_strategy.pdf＞(accessed 31 January 2015)を参照。
[28] 原文は、以下の HP＜http://www.defense.gov/pubs/2013_Arctic_Strategy.pdf＞(accessed 31 January 2015)を参照。
[29] 原文は、以下の HP＜http://www.whitehouse.gov/sites/default/files/docs/implementation_plan_for_the_national_strategy_for_the_arctic_region_-_fi....pdf＞(accessed 31 January 2015)を参照。
[30] 原文は、以下の HP＜http://www.arctic.noaa.gov/NOAAarcticactionplan2014.pdf＞(accessed 31 January 2015)を参照。
[31] See Charles K. Ebinger, 'The Way Forward for U.S. Arctic Policy', *Planet Policy*, June 5, 2014, at <http://www.brookings.edu/blogs/planetpolicy/posts/2014/06/05-way-forward-us-arctic-policy-ebinger> (accessed 31 January 2015).
[32] 原文は、以下の HP＜http://www.navy.mil/docs/USN_arctic_roadmap.pdf＞(accessed 31 January 2015)を参照。
[33] 同 16 及び 17 頁。しかし、グローバル・コモンズへの言及は、これら 2 頁で各 1 箇所のみであり、その定義もない。
[34] 原文は、以下の HP＜http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf＞(accessed 31 January 2015)を参照。
[35] 同 12 頁。
[36] 同 13 頁。なお、北極海への言及は、アデン湾沖の海賊対処やカリブ海や東南アジアを跨ぐ麻薬の密輸対処と同様に、特に例示されたものとなっている。
[37] 原文は、Ronald O'Rourke, 'Changes in the Arctic: Background and Issues for Congress', August 4, 2014, CRS Report, Congressional Research Service, 以下の HP＜https://www.fas.org/sgp/crs/misc/R41153.pdf＞(accessed 31 January 2015)を参照。
[38] それでいながら、米国に関しては現在、自国の原子力砕氷船の建造を大至急望む声も少なくない。Milosz Reterski, 'Breaking the Ice: Why the United States Needs Nuclear-Powered Icebreakers', *Foreign Affairs*, December 11, 2014, at <http://www.foreignaffairs.com/articles/142516/milosz-reterski/breaking-the-ice> (accessed 31 January 2015).
[39] この論点の詳細については、池島・前掲注 4、「第九章　国連海洋法条約への参加をめぐる米国の対応」参照。
[40] See, for example, Victoria Herrmann, 'A Response to Admiral Robert J Papp, Jr: America is Not (Yet) an Arctic Nation', The Arctic Institute, Center for Circumpolar Security Studies, at <http://www.thearcticinstitute.org/2014/12/121514-Not-Yet-Arctic-Nation.html>　(accessed 31 January 2015).
[41] See Ebinger, 'The Way Forward', *supra* n. 31; Ross A. Virginia, *et al*., 'The US and a Peaceful Arctic Future', *The Hill*, August 08, 2014, at <http://thehill.com/blogs/congress-blog/energy-environment/214597-the-us-and-a-peaceful-arctic-future> (accessed 31 January 2015); Roman Kilisek, 'Upcoming US Arctic Council Chairmanship Should Not Focus on Military Security', *Breaking Energy*, October 09, 2014, at <http://breakingenergy.com/2014/10/09/upcoming-us-arctic-council-chairmanship-should-not-focus-on-military-security/> (accessed 31 January 2015).
[42] 北極海をめぐる安全保障の考え方には沿岸諸国が抱える国益の観点から、実は多様な見解が存在し、安全保障の概念そのものも伝統的及び非伝統的なものなど多岐にわたるため複雑である。以下のものを参照。*Arctic Security in an Age of Climate Change*, Edited by James Kraska, Cambridge University Press, 2011.

[43] たとえば、以下の HP 参照。See ‘International Arctic Partners’, at the Canadian Government’s HP at <http://www.international.gc.ca/arctic-arctique/partners-international-partenaires.aspx?lang=eng> (accessed 31 January 2015); ‘The Emerging Arctic: A CFR InfoGuide Presentation’, at <http://www.cfr.org/arctic/emerging-arctic/p32620#!/> (accessed 31 January 2015).

[44] なお、最近、完成間近に迫ったと報じられた国際海事機関（IMO）の「極海域綱領」（Polar Code）が北極海航路に関して与えるインパクトなどの論点は、ここでは触れない。

[45] 中国じたいの立場は、以下のものを参照。Tang Guoqiang, ‘Arctic Issues and China’s Stance’, China Institute of International Studies, at <http://www.ciis.org.cn/english/2013-03/04/content_5772842.htm> (accessed 31 January 2015).

[46] See Ikeshima, ‘China’s Interests in the Arctic’, *supra* n. 6; 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.

[47] 「<解説>北極海をめぐる安全保障上の動向について」『平成 26 年版防衛白書』、防衛省・自衛隊 HP＜http://www.mod.go.jp/j/publication/wp/wp2014/pc/2014/html/nc001000.html＞ (accessed 31 January 2015)参照。

[48] 北極海におけるロシアの安全保障につき、小泉悠「ロシアにおける海洋法制―北極海における安全保障政策に着目して―」『外国の立法』259 号、2014 年、85-98 頁。

[49] 特に中国の姿勢として、北極海を跨ぐ核攻撃を米国に対して南シナ海の自国潜水艦から弾道ミサイルによって行うことを中国の軍事計画としていることや、米中間の対立と中国の南シナ海や東シナ海における海洋進出とを結びつける記述に、以下のものがある。Tetsuo Kosaka, ‘Reality Intrudes on China’s Military Contingency Plans’, *Nikkei Asian Review*, December 20, 2013, at <http://asia.nikkei.com/print/article/9884> (accessed 31 January 2015).しかし、こうした見方がいかに誇張された一方的な見方であるかという考察については、Ikeshima, ‘China’s Interests in the Arctic’, *supra* n. 6, pp. 77-79.を参照。

[50] しかし、北極海における自国の立場に関するロシア側からの視点については、以下のものを参照。Valery Konyshev & Alexander Sergunin, ‘Russia’s Policies on the Territorial Disputes in the Arctic’, *Journal of International Relations and Foreign Policy*, 2014, Vol. 2, No. 1, pp. 55-83.

[51] たとえば、以下のものを参照。Jasmin Sinclair, ‘Japan and the Arctic: Not So Poles Apart’, 『石油・天然ガスレビュー』2014 年、48 巻 2 号、39-48 頁、特に 41-42 頁参照。

[52] 2013 年 5 月 15 日のキルナ宣言、AC の HP＜http://www.arctic-council.org/index.php/en/document-archive/category/425-main-documents-from-kiruna-ministerial-meeting＞ (accessed 31 January 2015)を参照。

[53] たとえば、「商船三井、北極海初の定期航路　コスト 3～4 割減」日本経済新聞電子版、2014 年 7 月 9 日＜http://www.nikkei.com/article/DGXNASDZ0809O_Y4A700C1MM8000/＞(accessed 31 January 2015)を参照。Mari Iwata & Wayne Ma, ‘Shipping Firms to Add Arctic LNG Route’, *The Wall Street Journal*, July 9, 2014, at <http://www.wsj.com/articles/china-japan-shippers-to-launch-arctic-lng-route-1404905617> (accessed 31 January 2015).

[54] たとえば、「北極海をめぐる動向で説明聞く」『週刊経団連タイムス』2013 年 11 月 28 日＜https://www.keidanren.or.jp/journal/times/2013/1128_06.html＞(accessed 31 January 2015)。

[55] 本村眞澄「姿を現した新資源地帯の可能性―日本のエネルギー安全保障を強化」『外交』22 巻、2013 年、36-41 頁。

[56] 2015 年 1 月 31 日に開催された国際セミナー「ロシア北極圏の持続的発展」（前掲注 7 参照）において合田浩之氏より得られたコメントより。ちなみに、合田浩之「北極海航路の経済性と日本の期待―南回りに比べ競争力、航海日数短縮で利点」『外交』22 巻、2013 年、42-45 頁も参照。

[57] なお、2014 年に北極海航路を利用した海運が諸般の事情から前年度を大きく下回ったことで報じられている。こうしたマイナスのイメージともいえる結果は、将来の航路の更なる利用について様々な憶測や懸念を呼び、今後思い描く青写真も変わってくることになる。The Associated Press, ‘Number of Ships Transiting Arctic Waters Falls in 2014’, *The New York Times*, January 5, 2015, at <http://www.nytimes.com/aponline/2015/01/05/us/ap-us-arctic-shipping.html?_r=0> (accessed 31 January 2015); Carl Bildt, ‘The Battle for the Arctic’s Resources Heats Up’, *The Japan Times*, January 13, 2015, at <http://www.japantimes.co.jp/opinion/2015/01/13/commentary/world-commentary/battle-arctics-resources-heats/#.VO31ivmsWSp> (accessed 31 January 2015).

[58] 北極圏における国際共同研究体制について、日本の積極的な姿勢につき、以下のもの参照。「北極圏、共同研究体制に」日本経済新聞、2014 年 8 月 26 日。 ‘Japan to Create International Framework for Arctic Research’, *Nikkei Asian Review*, August 26, 2014, at <http://asia.nikkei.com/print/article/47114> (accessed 31 January 2015).

[59] 2015 年 4 月 23～30 日の「北極科学サミット週間」については、以下の HP＜http://www.assw2015.org/japanese/＞(accessed 31 January 2015)を参照。
[60] See Ikeshima, ‘Arctic States and Asian States’, *supra* n. 6, pp. 84-85.
[61] Id., pp. 85-86.

第８章　政策提言

＊平成 25 年度及び平成 26 年度報告書の各章における政策提言の要約である。

秋山　信将・宮田　智之

はじめに

今日、「グローバル・コモンズ」と呼ばれる地球社会の新たな公共領域として、とりわけサイバー空間、宇宙、北極海は多くの関心を集めている。しかし、グローバル・コモンズを「人類共同の遺産」、あるいは「コモンズ（共有地）」の延長として捉え、平和的で安定した世界と認識することは好ましくないであろう。グローバル・コモンズでは、特定の主権国家によるコントロールこそ及んでいないものの、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せめぎ合う、「リアル・ポリティーク」が展開されている。同時に、グローバル・コモンズは、①開放性、②連結性、③非対称性という、３つのリスク要因を有していることも忘れてはならない。原則として誰もが自由にアクセスできるという開放さ故に、他の主体により自らのアクセスが妨害・拒否される恐れがある。また、我々の社会生活は以上の領域と密接に結び付きながら成立しており、そのため悪意をもった主体が侵入することで、我々の社会生活に大きな混乱を引き起こす恐れがある。さらに、経済や軍事といった通常の力関係では劣位にある主体がグローバル・コモンズの特性を悪用し、力関係において優位にある主体に打撃を加える恐れがあり、テロリストがサイバー空間の活用を通して大国の重要インフラに甚大な打撃を与える状況は容易に想像できる。

このような点を考えるならば、サイバー空間、宇宙、北極海の安全を確保し、それら秩序の形成発展を図っていくことは急務であり、このプロセスにおいて日本は主体的に行動し、日米同盟を軸に積極的な貢献を果たしていかなければならない。

日米の同盟関係は長年にわたり地域の安定に寄与してきたのみならず、国際社会の「公共財」として、アジア太平洋地域の平和と安定に向けた協力や、グローバルな次元でのパートナーシップを拡大させている。そして、この日米の連携はグローバル・コモンズにおける安全確保という新たな課題においても大きな役割を果たすことが期待される。

そこで、本研究はサイバー空間、宇宙、北極海の３つのドメインの安全を確保するために、安全保障とガバナンスの２つの視点から日米同盟が果たすべき役割について検討を重ねた。以下は、その研究成果として、昨年度報告書及び本年度報告書の各章において指摘された提言を取り纏めたものである。

１．サイバー空間

（１）サイバー空間における安全保障面

現行の日米ガイドラインの見直しプロセスが示す通り、日米両国はサイバー空間での安全保障協力の強化を推進している。しかし、こうした日米両国のサイバーセキュリティ政策の強化にもかかわらず、①平時においては第三国などからの武力攻撃を抑止し、②抑止が失敗し攻撃が発生する前後において実効的に対処すること、これらは依然としてサイバーセキュリティをめぐる大きな課題である。

（ｉ）平時の抑止力強化

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。

以下は、日米同盟によるサイバー抑止力強化のための提言である。

・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

日米はサイバー抑止強化を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。

・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。

・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。

（ⅱ）有事における実効的対処

サイバー空間は人工的なドメインであり、その大部分は民間セクターに依拠している。したがって、物理的効果を伴う民間セクターへのサイバー攻撃や、物理的効果を伴わない民間セクターへのサイバー攻撃（グレーゾーン事態）に対処する必要があり、それには平時における抑止力強化とともに、自衛権行使を含む有事の対処メカニズムの構築が不可欠である。具体的には、国際規範の強化と創造、民間セクターの防衛、日米共同対処のメカニズム構築の推進である。

・国際規範の強化と創造

2013 年 6 月、国連総会第一委員会のサイバーセキュリティに関連する政府専門家会合（GGE）は「国連憲章を含む既存の国際法体系はサイバー空間に適応可能」との報告書を発表した。これは、物理的効果を伴う民間セクターへのリスクに対応することを意味し、日米はこうした規範をより強化していく必要がある。同時に、グレーゾーン事態への対処として、新たな国際規範の創造も必要である。日米は、マルチ外交の場で物理的効果を伴わない攻撃や経済システムへの攻撃も「国際の平和や安全を脅かす」という認識を広げていくことが必要である。こうした規範形成は、普遍的なメンバーシップを有する国連などでなくとも、NATO や価値を共有する諸国でも十分効果的であろう。

・民間セクターの防衛：ガイドラインの構築と継続的モニタリング

民間セクターの自主的な防衛体制を奨励する一方、安全保障に直結する事業者について政府は一定の負担をし、サイバー防衛の機能を提供すべきである。こうした政府（特に防衛省や自衛隊）による関与は、重要インフラの設定の見直しと日米の整合が必要であり、日米それぞれの重要インフラをサイバーセキュリティ、特に有事における優先度で再定義し、どのセクターに防衛省・自衛隊、国防総省・米軍が関与するか、を検討すべきである。民間セクター防衛では、サイバー攻撃の継続的なモニタリングも欠かせない。ネットワークを監視し、攻撃を予見し、場合によっては相手方のアクセスを拒否することが必要である。ただし、こうしたネットワーク監視は憲法が保障する「通信の秘密」（第 21 条）との整合をはかる必要がある。

・サイバー攻撃への日米共同対処

サイバー攻撃事態に実効的に対処するためには、自衛隊および米軍の連携が不可欠であるが、どのようにサイバーオペレーションを日米共同対処に組み込むかはいまだ解決されていない問題である。2014 年 3 月に発足したサイバー防衛隊の役割は防衛省・自衛隊ネットワークの防護と監視であり、現状では民間セクターの防護や攻撃的なオプションにおける役割はない。CYBERCOM の体制にも課題があり、CYBERCOM の部隊（サイバーオペレーションを担う部隊）と全世界の統合軍との関係、特に指揮統制が明確でない。CYBERCOM の位置づけについての議論もあり、一部ではサイバー軍の「格上げ」や「大統領・国防長官への直接アクセス」が提起されている。こうした CYBERCOM の位置づけに関する議論を見据えながら、サイバーオペレーションを担う部隊と戦闘部隊の指揮統制を整理しつつ、防衛省・自衛隊のサイバー部隊を拡大・強化していく必要がある。

（２）サイバー空間におけるガバナンス面

（ⅰ）グローバル市民の活動拡大のためのサイバースペース

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。一方、中露は国家主導のサイバースペースの管理を求めているが、それ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。

（ⅱ）グローバル・コモンズとしてのサイバースペースの今後の課題

グローバル・コモンズとして見た時、サイバースペースの今後の課題はこれまで注目されてきたような「資源」としてのコモンズに対する攻撃はいうまでもなく、「土地」としてのコモンズに対する攻撃、言い換えれば物理的な設備としてのコモンズに対する攻撃にいっそう備えるということになるだろう。電力設備、海底ケーブル、人工衛星といった重要インフラを対象に含めた群発攻撃に備えなければならない。群発攻撃とは、物理的な設備に対する攻撃とデータ／コンテンツ／プログラムに対する攻撃の両方を含む、複数のターゲットを狙った同時多発的な攻撃である。

２．宇宙

（１）宇宙空間における安全保障面

オバマ政権は、協力に値する国家や民間宇宙活動の増大による調整の必要性、宇宙利用における脅威の顕在化、そして財政的制約といった理由から、安全保障分野での宇宙協力を強化している。こうした米国にとって、安全保障分野を含めた宇宙利用の拡大をはかっている日本は協力相手としての価値を急速に高めている。オバマ政権は主に①宇宙活動に関する透明性・信頼醸成措置(TCBM)、②宇宙状況認識（SSA）の共有、③衛星の共同調達・共同運用・共同利用、④連合宇宙作戦を推進しているが、このうち、①と②について日本はすでに主要な協力相手となっている。③についても、今後日本は主要な協力相手となる可能性がある。

（ｉ）宇宙状況認識（SSA）の共有、衛星の共同調達・共同運用・共同利用

今後②と③の日米協力がどこまで深化するかは、かなりの部分、日本側による能力整備の進捗にかかっている。そもそも日米間では、米国が能力を整備し同盟国側が資金等を提供するという協力形態（WGS 型）はほとんど念頭に置かれておらず、少なくとも現時点で日米が重視しているのは、同盟国側が能力を整備した上で米国と共有するという協力形態（サファイア型）である。2014 年の宇宙に関する包括的日米対話第 2 回会合の共同声明においても、「日本の宇宙活動の活発化が日米双方の安全保障に不可欠な宇宙アセットの抗たん性の向上につながる日米宇宙協力の新しい時代が到来したことを確認した」との一文が盛り込まれている。

SSA について新しい「宇宙基本計画」は、平成 30 年代前半までに関連施設と運用体制の構築を行うと明記している。防衛省の「宇宙開発利用に関する基本方針」も、宇宙監視機能の保持に向けて内閣府や文部科学省と具体的な検討を進めることや、専従組織の設置を検討していくことを掲げている。また準天頂衛星について新しい「宇宙基本計画」の工程表は、2017 年度から 4 機体制の運用を始め、2023 年度には 7 機体制の運用を始めるとしている。これらの能力整備が進捗するにつれて、日米協力はより双方向性の高いものとなる可能性を有している。

（ⅱ）作戦レベルでの協力

個々の協力を基盤として作戦レベルでの協力をいかに進めていくかという問題は、今後の日米協力の主要な論点となる可能性がある。2014 年 10 月発表の「日米防衛協力のための指針の見直しに関する中間報告」が、見直し後の指針で宇宙協力について記述すること、

その中には「宇宙の安全かつ安定的な利用を妨げかねない行動や事象及び宇宙における抗たん性を構築するための協力方法に関する情報共有」を含むと明記した点は注目に値する。

また日米の有識者からは、米戦略軍の統合宇宙作戦センター（JSpOC）への防衛省職員の派遣や、米国政府が主催する机上演習への日本の参加といった提言が発表されている。さらに、米軍主催の実動演習・訓練への参加や、既存の日米共同演習・訓練への宇宙の組み込みも検討に値するだろう。

（ⅲ）宇宙利用をめぐる懸念の払拭

メディアではしばしば否定的な評価がなされているが、日本の外交及び安全保障から見ても日本が安全保障分野における宇宙利用を進めることは積極的な意義を見出すことが可能である。また、その技術開発と運用においても宇宙基本法第２条に定められている「国際約束の定めるところに従い、日本国憲法の平和主義の理念にのっとり」という規定があり、一般に懸念されるような宇宙の（攻撃的な）軍事利用ということに結び付くとは考えにくい。しかし、こうした懸念を払拭する政治的なメッセージをどう表現していくかについては、今後の課題として残るであろう。

（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。

こうした中、今後のグローバル・コモンズとしての宇宙ガバナンスを考える上で、次の３点は大きな課題である。

（ⅰ）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。こうした中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。

（ⅱ）衛星の小型化に伴い、技術がより単純化し、陳腐化

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見られる。これは、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、という問題が提起される。

（ⅲ）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なのである。

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、今後わが国として如何なる対応を採るべきか。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は死活的に重要であり、「北極海の利用と国益に沿った外交政策」を推進すべきであろう。中・長期的には、海洋立国たる日本としては、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」、更には「関係友好国との海洋安全保障協力の見直し…海洋安全保障協盟の推進」を実現して行くべきである。具体的には下記のとおりである。

（ｉ）北極海の利用と国益に沿った外交政策の推進

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。また、日本は北極圏諸国ではないが、その生存と繁栄を海洋に大きく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(AC)の将来的意義について、現時点では正確に見通すことは出来ないが、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には積極的に参加し、特に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。同時に、2013 年 11 月の日露「2＋2」の決定を遵守する形で、2014 年 10 月に日本海のウラジオストク方面で、日露合同海難事故訓練を実施したように、実力国ロシアとの信頼関係維持のための手立ても欠かしてはならない。

（ⅱ）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、海洋安全保障に関する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や C4ISR 等の整備が求められる。将来的に、艦船や航空機などの北極海や周辺海域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、無人航空機（UAV）や無人水中ビークル（UUV）の効果的利用が求められよう。更に弾道ミサイル防衛能力の拡大、強化も必要となり、イージス艦の増勢を始め、一般防空と弾道・巡航ミサイル防衛を総合化した IAMD（Integrated Air and Missile Defense）の導入も必要となろう。一方、北極海や周辺海域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、北極海での通年行動能力の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。

（iii）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もつ。米国の拡大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であろう。この視点からは、まず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洋領域把握（MDA）に関し、北極海や周辺海域においても協力していくことが必要となる。また、これを強化するための宇宙状況把握（SSA）での協力も同時に必要となる。

疑いもなく、日米防衛協力指針の改訂は、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（あるいは BMD を取り込む形での IAMD）、対潜水艦戦、掃海、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、日米同盟の更なる深化を図ることは大いに意義がある。この際、北極海を巡る安全保障・防衛面での情勢の変化に即応し得る形で、日米防衛協力指針を、都度、改訂または一部修正していくことが求められよう。

一方、中露の極端な接近や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・防衛協力の実質的な強化は、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。

（iv）関係友好国との海洋安全保障協力の見直し…海洋安全保障協盟の推進

日本は戦略的な観点から、安倍首相の進める「国際協調主義に基づく積極的平和主義」や「地球儀を俯瞰する外交」を具現化するため、欧米、インド洋・アジア太平洋地域の良識ある友好海洋国家（関係友好国）との海洋安全保障協盟（MSC）の推進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・防衛面での関係友好国と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、北極海や周辺海域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を通じて、長大な海上交通路の安全保障を切れ目なく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

（ｉ）北極海の性格

そもそもグローバル・コモンズとは何か、また北極海が他の二つの空間のようなグローバル・コモンズかといった根本的な問題がある。実は、北極海をどのような空間として位置づけるべきかによって、日米同盟との関わりや接点の有無が変わってくるわけで、その意味で北極海が冷戦後にあっても平和と安定が比較的成功裏に維持されてきた地球上の数少ない空間であるという事情は単なる偶然ではないであろう。しかも、この平和と安定のためにとりわけ北極圏諸国の中でも 5 つの沿岸諸国(Arctic 5)が果たしてきた広範かつ長期の真摯な努力は、北極海評議会（AC）の諸活動やガバナンス状況にも見られるように、広く世界で共有されている。その際に、最も注目すべきは、軍事・安全保障の面をも含めて、あらゆる側面において北極圏諸国の多様な関係を中心に国際協力が進展してきた経緯とその意義であろうと考えられる。

（ⅱ）北極海と日本

日本政府は北極海において日米同盟が作用する状況を日本国憲法の解釈上は想定できないとの立場を本来なら取ってきたと推察されるが、それが近時の集団的自衛権に関する解釈変更やその後の一連の政府の動きから見れば、日米同盟が作用し得る事情が北極海に今後、生じ得るか否かは新たに日本に課された決して容易でない課題となるであろう。また、北極海をとりまく事情から、北極圏諸国の中で想定される相手国(ありうるのは米国の場合がほとんどと推察される)からの要請（または事前合意・了解）に基づく日本の関与（国家的な言動に基づく介入）にどれだけ自国の主体的な制約と抑制を日本自身が課すことができるか、また日本へのどのような期待が当該相手国にはあるか（またはないのか）などを予め想定して、理解しておく必要がある。日米同盟のバイラテラルな関係は、北極海をめぐる北極圏諸国相互のバイラテラルやマルチの関係にも影響を受けるし、日米と非北極圏諸国との関係にも場合によっては大きく左右されることになる。これらについての明確なビジョンとそのために有効な実施方法に基づいて、日本は北極政策を起案し、遂行することが肝要である

国際社会における日本の立場を政策立案者が十分踏まえた上で、日米同盟の役割と働きの文脈を考えるべきであろう。とりわけ、日本と北極圏諸国または Arctic 5 との関係、日本と北極評議会との関係、また日米同盟関係や日本の政策が国際社会の利益(公益)に及ぼしうる影響を十分に検討すべきであることはいうまでもない。