

第1章 総論：「アクロス・ザ・ユニバース」の安全保障 ーグローバル・コモنزにおける「普遍的な平和」とはー

星野 俊也

1. はじめにー「グローバル・コモنز」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、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なければいるほど、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نز (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)」の体制のあり方ー特に「安全保障ガバナンス

(security governance)」の側面一を検討し、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・ポリテイク

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」の観点から見ればなおのこと、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、そこに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

の利益を脅かしようとする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ようとする状況や、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、サイバー空間にしる、宇宙にしる、北極海にしる、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を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、サイバー分野における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. おわりにー「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いる⁹。これだけをとっても、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نز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نز」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نز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نز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نز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نز(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。