FOCUS　グローバル・コモンズ

拡大する安全保障領域をどう考えるか

技術の進歩に伴う人類の活動領域の拡大。しかしその華々しい成果は同時に、考慮すべき安全保障問題群の拡散をも招いている。

平和・安全保障研究所理事長
西原 正
にしはら　まさし
京都大学法学部卒業後、一九七二年にミシガン大学大学院 PhD 取得。防衛大学校教授、同校校長などを経て二〇〇六年より現職。著書に *The Japanese and Sukarnos Indonesia*、『戦略研究の視角』などがある。

冷戦終結後、米ソ超大国間の対立が消滅し、国際安全保障の領域は二つの分野で拡大している。一つは、気候変動、感染症、食料安全保障、災害対処など個人レベルの安全保障問題を非伝統的安全保障問題として重視するようになったため、国家の役割が増大したことである。もう一つは、中国などの台頭によって宇宙空間における米中軍備競争が進むのではないかという懸念や、サイバー戦争が起きるのではないかという懸念が生じて、宇宙空間およびサイ

バー空間における安全保障問題が重視されつつあることである。

テロ、麻薬取引、海賊行為なども、新しい非伝統的安全保障問題として扱われる傾向にあるが、これらの行為は歴史的に存在していた越境犯罪であり、非伝統的ではない。ただアルカイダなどのテロ行為やソマリア沖の海賊行為は規模が大きいがため、非国家主体による行為として注目を集めることになった。

右記の二つの拡大する国際安全保障の領域のうち、ここでは宇宙空間における開発競争やその陰にある勢力争い、またサイバー空間におけるテロなどの伝統的安全保障の領域の拡大に注目する（サイバーテロは伝統的なものではないが、伝統的安全保障の領域に入る）。

四つのグローバル・コモンズとその特徴

二一世紀に入って、海洋、大気圏、宇宙空間、サイバー空間などをグローバル・コモンズ（グローバル公共領域）として言及することが多くなった。一九八九年のソ連の崩壊によって、超大国ソ連の脅威は消滅したが、新たに台頭した中国などがグローバル・コモンズにおける「利用自由の原則」に挑戦し始めているからである。

グローバル・コモンズは、諸国が自由に利用できる領域をさす。歴史的には、船舶の発達とともに海洋が最初にグローバル・コモンズになり、ついで航空機の発達によって大気圏がグローバル・コモンズになった。同様に、宇宙空間は人工衛星が実際的目的に利用されるようになった一九五〇年代末以降に、そしてサイバー空間はインターネットが地球的規模で利用されるようになった九〇年代半ばに、それぞれグローバル・コモンズと考えられるようになったようだ。

このいずれの空間でも利用自由の原則が慣習法ないしは国際法となっている。海洋には、一般的に沿岸から一二カイリまでを領海、それより外側の海洋を「公海」とし、どの国も自由に利用できるという原則、つまり「公海の自由」原則が「公海に関する条約」（一九五八年）によって決められている。その原則には、公海における航行の自由、漁獲の自由などが含まれている。大気圏も国が管轄下におく領空以外の空域に関しては、「公海の上空を飛行する自由」が右記の公海条約で決められている。宇宙空間に関しても、「宇宙条約」（六七年）は、月その他の天体においてすべての国が、自由に探査し、利用することができるとし、領有権を凍結した。宇宙空間の利

用の自由が海洋および大気圏のそれと異なるのは、前者においては核兵器などの大量破壊兵器を配置しないこと、また軍事施設などの設置や軍事演習なども禁止したことである。

サイバー空間は以上の三つの領域とは質的に異なっていて、地理的な空間ではなく、仮想空間である。したがってサイバー空間はこの三つのそれぞれの領域の中にも存在する。コンピューターや情報機器をインターネットで結びつけ、コミュニケーションや情報サービスが地球的規模で行われる状況では、外国の軍組織や民間セクターが政府（国防組織を含む）関係情報に侵入するのを可能にしている。サイバー空間は、これを規制しながら利用の自由を確保することが必要であるが、その条約はまだできていない。しかしインターネットを通しての、正当な手段による情報取得、交換、意見表明は自由であるべきで、その自由が民主主義の健全な発展に不可欠だとする意見は強い。二〇一〇年一月にクリントン米国務長官は「インターネットの自由」について講演をしている。その意味でインターネット利用の自由に関する慣習法はできつつあると考えてよい。

「利用自由の原則」に挑戦する中国と対抗策

以上見たように、「利用自由の原則」の内容は四つの領域によって異なっている。海洋と大気圏は軍事活動を容認した利用自由の原則であるが、宇宙空間は軍事活動を禁止した利用自由の原則である。そしてサイバー空間は仮想空間における利用自由の原則である。しかしこれらの原則は現在、いずれも挑戦を受けている。その挑戦国の筆頭は中国である。

中国は海軍力（駆逐艦、潜水艦など）を増強して、台湾海峡や東シナ海、南シナ海に米海軍などが接近するのを阻止する能力をつけ始めた。二〇一〇年、中国は南シナ海を自国の「核心的利益」の海域であると主張し、米海軍の接近を牽制した。これは公海における航行自由の原則への挑戦である。中国はまた、公海上の空域において米軍が自国領空に接近するのを阻止し始めている。〇一年四月には中国の戦闘機が、海南島南の公海上を飛行していた米国の偵察機を妨害して事故を起こしたことがある。これも公海上の空域での飛行自由の原則に反する行為であった。さらにステルス戦闘機「殲二〇」や射程二〇〇〇キロの対艦弾道ミサイルが将来配備されれば、米軍にとっ

て脅威となる。これに対して、米国は「統合空海戦闘」（ジョイント・エア・シー・バトル）構想を具体化したり、豪州のダーウィンに海兵隊を配備する決定をしたりして、軍備費削減の圧力にもかかわらず、アジア太平洋の軍備増強で対抗しようとしている。

中国は宇宙空間においても宇宙法で謳う宇宙空間の非軍事化を前提にした利用自由に反する動きをしている。二〇〇七年一月、中国が予告なしに、古くなった自国の気象衛星を地上からの弾道ミサイルで破壊する実験を成功させた。これは中国が米国の衛星や有人宇宙船を撃墜できる衛星攻撃兵器（ＡＳＡＴ）を持つに至ったことを証明した。米国はソ連とともに一九八五年に宇宙空間での衛星攻撃兵器の使用を禁止することに合意したが、中国がこの慣行に挑戦していることに懸念を表明している。中国はさらに米国に依存しない独自のＧＰＳ（全地球測位システム）「北斗」を確立する計画を進めており、二〇三〇年には世界全域で高度の監視・識別能力により、米軍の動きをより正確に追跡することができるようになる。米国の偵察衛星、早期警戒衛星に対抗するものとなりそうである。

さらにサイバー攻撃の例を見ても、発信源が中国であることが多い。米議会は二〇一一年一月、米航空宇宙局（ＮＡＳＡ）の人工衛星二機が二〇〇七～〇八年に中国からのサイバー攻撃にあったことを公表した。人民解放軍には、総参謀本部の中にサイバー攻撃の主たる担当組織があり、各軍管区には技術偵察局や情報戦民兵隊が組織されている。また中国軍はすべての軍種と部隊レベルにおいてネットワーク戦訓練施設をおき、敵味方に分かれてサイバー戦の演習もしているという。さらに中国政府は約二五〇の民間ハッカー集団との連携を図って、サイバー攻撃やサイバースパイに活用しているとされる。米国は二〇一〇年二月の「四年ごとの国防戦略の見直し」（ＱＤＲ）報告で対抗組織の結成に言及し、同年一〇月にサイバー軍司令部を創設した。そして一二年七月、サイバー軍事戦略を発表し、サイバー攻撃には軍事報復をする方針を打ち出した。

法的整備に欠ける日本の対応策

こうした異なる空間での利用自由の原則に挑戦する国は今後中国以外にも出てくる可能性はある。日本はこうした事態に対してどんな対応策を持つべきであろうか。日本は外交的手段と軍事的手段を巧みに使った対応をすることが必要である。中国との二国間および多国間

協議を通して、グローバル・コモンズにおける国際慣習や国際法を順守することの重要性を認識するよう促すことに努めるとともに、自衛隊の能力、とくに海空の能力を一層向上させる必要がある。そして公海および大気圏における中国の接近阻止戦略に対しては、米国の対抗戦略である統合空海戦闘戦略を側面から支援する能力が必要になる。

日米同盟のもとで共同対処を進めるためには、日本は集団的自衛権を行使できるよう憲法解釈を修正する必要がある。この修正は韓国やオーストラリアなどの他のパートナー国との連携を強化する上でも不可欠である。日本は二〇〇八年に制定した宇宙基本法に「国際社会の平和・安全の確保、わが国の安全保障に資する」ことを明記して、防衛省が「情報収集衛星」をもつことを可能にした。これによって朝鮮半島などの動きがより正確に認識でき、より効果的な対応策を講じて地域の安定に寄与することができるようになった。同時に日本は、宇宙空間の軍事化の動きには強く反対すべきである。地上からの衛星攻撃兵器や地上の物体を破壊する地球周回軌道上の衛星を配備する動きをも多国間協力によって阻止するように努めるべきである。

サイバー攻撃はいつ仕掛けられるかわからないという特徴がある。これに対抗するには、日本は、サイバー攻撃があった場合ただちに発信源を突き止め破壊し甚大な影響を与えるソフトを開発していると報じられているが、早期に配備し、その事実を敵性国に事前告知しておくべきである。こうして相互抑止効果を狙うことができる。現在、防衛省が採っている専守防衛戦略はサイバー攻撃には効果がない。サイバー攻撃にはサイバー反撃をすることが重要である。しかし関係者は、「日本の現在の武力攻撃事態法では、サイバー攻撃が『武力攻撃』とは見なされないので反撃できない」との解釈になっているという。サイバー攻撃は武力攻撃ではないのであるから、むしろサイバー反撃をすることは問題がない筈である。

時代の変化とともに、国際安全保障が扱う領域も変化、拡大していく。主要国はパワーゲームの場を広げる半面、パワーゲームの場を制限する努力もしてきた。宇宙空間の非軍事化がそのいい例であるが、このほかにも南極大陸の領有権凍結、海底核兵器禁止条約、部分的核実験禁止条約などがある。日本をはじめ主要国は早期にサイバーへの不正な侵入を防止する方策を見つけることが緊要である。■