安全保障の空間的変容

鈴木 一人
Suzuki Kazuto

はじめに

人類の歴史は戦争の歴史であり、戦争のあり方は科学技術の変化に伴って変化してきた。とりわけ第1次、第2次世界大戦では戦車や航空機、空母や毒ガス、さらには核兵器の登場によってその戦争の行方を大きく左右され、兵器体系のあり方や軍編成にまで影響する進化がみられた(1)。冷戦期にも兵器の進化は続いたが、1990年代以降、いわゆる「サードオフセット（第3の相殺戦略）」と呼ばれる、新たな安全保障戦略がアメリカで議論されるようになり、これまでの人類の歴史にはない、安全保障の空間的変容が生まれている。

「サードオフセット」については本特集の神保論文、森論文で議論されているので詳細は割愛するが、簡単にまとめれば、先端技術の導入によって軍事的優位を維持し、アメリカの戦略を遂行する能力を確保することを意味する。なかでも重要になるのが、これまで伝統的に安全保障戦略の中心であった陸、海、空の3つの領域に加え、宇宙空間とサイバー空間を活用していることである。これまでも非物理的空間における安全保障問題として、例えば情報戦といったプロパガンダや情報操作などのオペレーションは想定されてきたが、サイバー空間という、主として民間活動によって発達した非物理的空間における安全保障問題が取り上げられるようになったのは、これまでの安全保障の考え方のなかでも大きな変化である。また、宇宙空間もこれまでミサイルが通過する空間でもあり、また、軍事的な通信や偵察といった活動にも用いられていたため、まったく新しい安全保障領域とは言えないが、その重要性は急速に高まっており、2007年の中国による衛星破壊（ASAT）実験にみられるように、宇宙システム（詳細は後述）そのものが攻撃対象となりうるようになったのは大きな変化である。

本稿は、果たしてこのような変化が、安全保障の空間的変容をもたらし、これまで人類が経験したことのない、新たな時代を迎えようとしているのか、それとも、これらの変化は単なる戦術的な変化にすぎず、その重要性は限られたものであるのかを分析し、評価するものである。この空間的変容が本格的に起こっているとすれば、日本を含め多くの国において、その安全保障戦略を見直さざるをえなくなり、宇宙・サイバー空間を含めた、まったく新しい安全保障戦略の構築を進めていかなければならないであろう。さらに言えば、こうした新しい安全保障戦略を支えるための技術的な能力をいかに確保し、既存の陸、海、空の戦力と統合できるかが問われることとなる。

1　宇宙・サイバー空間で何が起きているのか

宇宙空間もサイバー空間も直接目に見える空間ではなく、それゆえにそれらの空間における脅威が過剰に評価されたり、見過ごされたりしている。ここではやや詳しく宇宙・サイバー空間がどのようなかたちで安全保障にかかわっているのか整理してみたい。

(1)　宇宙空間

2007年の中国によるASAT実験は、宇宙空間が新たな「戦場」になりうる可能性を示したという点で大きな出来事であった[2]。ASATは冷戦期にもアメリカとソ連によって実施されており、まったく想定されていなかったわけではないが、冷戦期にはその効果が限定的であり、米ソ両国において、その安全保障上の価値は重視されてこなかった。その理由は定かではないが、正確に衛星を攻撃するだけの状況監視能力の限界や、核戦略のバックボーンとなる宇宙システムを攻撃することで核抑止のバランスが失われることを懸念した可能性が考えられる[3]。

しかし1990年代以降、状況は大きく変わってきている。ひとつには、兵器の高度化が進み、核戦略だけでなく、通常兵器の運用に関しても宇宙システムが広範に使われるようになったことが挙げられる。いわゆる「ネットワーク中心戦（NCW）」と呼ばれる、ネットワークによる兵器体系の接続により、偵察衛星のセンサーなどによって得られた情報を、通信衛星を介して配信し、それが戦場の情勢認識を高め、司令部と前線で情報を共有し、迅速な意思決定を可能にするようになった。また、無人偵察機・攻撃機は衛星システムによって遠隔地から操作され、それらの機材から得られる情報も衛星システムによって配信されている。こうしたNCWの発達により、宇宙空間は、現代の戦闘行為に不可欠なインフラを提供し、その能力の有無は安全保障の趨勢に決定的な影響を与える状況となっている[4]。

宇宙システムの重要性が増せば増すほど、敵対勢力にとって、こうした宇宙システムを攻撃するインセンティブが高まる。衛星は打ち上げ時に最も効率的になるよう限界まで軽量化されており、外部からの攻撃に対応できるような防御システムを備えてはいない。そのため、宇宙システムは軽度の衝撃に対しても脆弱で、その機能を失う可能性がある。そうした状況を逆手にとり、敵対的な勢力は相手の能力を剥奪し、自らの軍事的優位性を確立するため、宇宙システムを攻撃の対象とするインセンティブが高いのである。

また、宇宙空間での活動は直接目に見えるわけではなく、誰がどのタイミングで宇宙システムに対して攻撃を加えたのかを明確にすることが難しい。その行為の帰属（attribution）を証明することができなければ、攻撃に対する反撃を正当化することも難しく、反撃される可能性が低いとみられれば、よりいっそう、紛争時に宇宙システムを攻撃するインセンティブが高まる。さらに言えば、宇宙空間での戦闘行為では直接死傷者を出すことなく相手の軍事的能力を劣化させることができるため、紛争が始まった初期の段階で宇宙システムを攻撃することで最も大きな効果を得ることができるため、戦況の展開いかんにかかわらず、宇宙システムを攻撃の対象とする可能性も高い。つまり、宇宙における奇襲攻撃（Space Pearl Harbor）が起きる可能性が高いとアメリカではしばしば議論される[5]。

とりわけアメリカは世界で最も宇宙システムに依存した兵器体系をもっており、宇宙システムへの攻撃によってその能力を失うと、核戦力はもちろんのこと、通常兵器による戦闘遂行能力も激減する。そのため、現在の米国防総省では宇宙システムの抗堪性（resilience）の議論が大きな注目を集めている(6)。仮に宇宙システムが攻撃を受けたとしても、その機能が失われないようにするためにアメリカでは現在、大型衛星に多くの機能を搭載してそれへの攻撃によって機能を一気に喪失するリスクを避け、小型衛星に機能を分散させて、それらをコンステレーション（多数の衛星を同期させて運用すること）として運用することなどが検討されている。とりわけ民間企業が小型衛星のコンステレーション技術を進化させていることから、これまでのように特定の軍需産業に依存するのではなく、広く民間企業と国防総省・米軍が共同で技術開発を進め、新たな状況に対処することが想定されている。これは伝統的な軍事調達の仕組みを大きく揺るがすものであるが、伝統的な軍需産業と言われるボーイングやロッキード・マーチンもこうした変化に対応した技術開発や投資をしており、アメリカの軍需産業と政府の関係もまたダイナミックに変化している。

宇宙システムへの攻撃は2007年の中国によるASAT実験のイメージから、物理的な攻撃によって衛星を破壊することが想定されることが多い。しかし、物理的な破壊は宇宙空間に多くの宇宙デブリ（ゴミ）を撒き散らすことになる。2007年のASAT実験では3500以上の感知できるデブリ（直径10cm以上の大きさ）が発生し、それ以下の細かいデブリも含めると数万の破片が地球軌道を周回していることになる。地球軌道を周回する物体は第1宇宙速度、すなわち秒速7.9km（時速2万8500km）のスピードで飛翔しているため、ごく小さな破片であっても、それが他の衛星に衝突した場合、大きなダメージを与えることになる。確率的には地球周回軌道で最も多くの衛星を稼働させているアメリカ（約540機）にとって大きなリスクとなるが、中国も急速に軍民両面で宇宙システムを活用するようになっており、特に中国は軍の近代化に伴って宇宙システムへの依存を強めるようになっている。現在、中国が保有している稼働中の衛星は軍民合わせて170機程度とみられているが、宇宙デブリの密度が高まれば、当然ながら中国にも相当なリスクとなる。そのため、仮に中国が紛争状態に突入し、相手国の宇宙システムを攻撃するとしても、2007年の時のような物理的な攻撃を行なうことは可能性として低いとみられている（宇宙システムに依存していない北朝鮮のような国の場合はその限りではないため、将来にわたって衛星に対する物理的攻撃がなくなるというわけではない）。

しかし、ASATは物理的攻撃に限定されるものではない。衛星を破壊せずに衛星の機能を奪うことも可能である。その代表的な方法としては、衛星からの信号を妨害するジャミング、衛星からの情報に同期させた偽情報を流して受信者を混乱させるスプーフィング（spoofing）、また衛星に接近して衛星から発せられる信号を傍受したり、妨害電波を発したりする寄生衛星、偵察衛星などに対してレーザー光線を当て、そのセンサーの機能を奪う「目潰し（dazzling）」などの方法がある(7)。これらの手段はすでに活用されており、例えば北朝鮮は38度線付近にGPS（全地球測位システム）の測位信号を妨害するジャミング機器を配置し、仁川空港などの韓国国内のインフラを麻痺させるという活動を複数回にわたって実施している(8)。

このように、宇宙空間はすでに現代の安全保障に深く組み込まれており、平時において宇

宙空間における能力の有無が国家の軍事的優位性に大きく影響するようになっているだけでなく、有事においては、その軍事的能力を劣化させるために真っ先に攻撃の対象となりうる存在となっている。この意味で宇宙空間は現代の安全保障の空間的変容の一翼を担っていると言えるだろう。

(2) サイバー空間

サイバー空間も宇宙空間と同様、現代の安全保障の作戦領域として認識され、陸、海、空に続く「第4（ないし第5）の作戦領域」と呼ばれるようになっている。とりわけ「ネットワーク中心戦（NCW）」が現代の兵器体系の基盤となっているなかで、兵器システムだけでなく、C4ISR（指揮・統制・通信・コンピュータ・情報・監視・偵察）と言われる指揮命令系統や情報収集の仕組みまですべてネットワーク化され、サイバー空間抜きに軍事的行動をとることは事実上不可能な状況となっている。しかし、宇宙空間同様、サイバー空間は伝統的な作戦領域とは異なり、目に見える物理的空間ではなく、あくまでも仮想空間における作戦領域であり、その安全保障の考え方はサイバー空間特有のものがある。

第1にサイバー空間における脅威は物理的な攻撃ではなく、特定のプログラムやネットワークそのものに対して行なわれ、その結果、軍事的に枢要なシステムや経済社会に不可欠なインフラを機能不全にし、何らかのかたちで経済的、社会的、軍事的な損害を与える行為となる。サイバー攻撃とは、大量のコンピュータによって一斉に特定のネットワークを狙い撃ちにして通信容量を超える接続要求を出して機能麻痺させるDDoS（distributed deniel of service）攻撃から、意図的に相手のコンピュータにウィルスを忍び込ませ、それを通じて情報を掠め取ったり、内側からネットワークを機能不全にするといった攻撃まで、さまざまなタイプの攻撃形態をとりうる。もちろん、サイバー空間といえども、コンピュータとケーブルによる物理的なインフラは必要であり、これらに対する直接的な物理的攻撃もありうるが、一般にサイバー攻撃とは、遠隔地からネットワークをサイバー空間上で機能不全にさせることを意味する。

また、宇宙空間における安全保障と共通する問題として、帰属（attribution）をめぐる問題がある。サイバー攻撃の主体を特定するためには、その攻撃を行なったコンピュータのIPアドレス（サイバー空間におけるコンピュータの認識番号）を特定する必要がある。しかし、このIPアドレスは複数のコンピュータやサーバを経由することで容易に偽装することが可能であり、実際の攻撃を行なったコンピュータを特定するまでには長い時間がかかる。そのため、実際の攻撃が誰によって行なわれ、その行為の責任が誰に帰属するのかを判別することが非常に難しい。ゆえに、攻撃に対する報復を行なうにしても、即時に対応することは難しく、攻撃する側にきわめて有利な状況となる。実際にIPアドレスが特定できなくとも、サイバー攻撃が特定の国からなされたことは相対的に判断しやすい。しかしながら、その国から攻撃が行なわれたとしても、それが国家の行為として行なわれたものなのか、それとも政府とは関係ない個人によって行なわれたのかを特定することはできない(9)。

宇宙空間と大きく異なるのは、サイバー空間への参入障壁がきわめて低いことである。宇宙空間で何らかの攻撃を行なう場合、宇宙空間にミサイルや寄生衛星を打ち上げるか、地上

からジャミングやスプーフィングを実行することになり、そのための設備や人材を確保し、その攻撃を有効なものにするための投資や準備が非常に難しい。他方、サイバー空間での攻撃は、特殊な設備や機器を必要としておらず、日常的に使っているパソコンやすでに使われなくなった旧式のパソコンであっても実行可能である。また、マルウェア（悪意のあるソフトウェア）のプログラムを書くことができれば、それを多数のパソコンに忍び込ませ、そこからボット攻撃（プログラムによって機械的に同じ攻撃を繰り返す）を展開することもできる。こうしたプログラムは多少のコンピュータ言語の知識があれば書くことができ、理論的には誰でも攻撃に参加することができる。

攻撃への参入障壁が低く、帰属問題があるために攻撃側に非常に有利な構造となっているサイバー空間では、日常的に何らかのかたちでサイバー攻撃が行なわれている。当然ながら、そうした攻撃に対して、防御側も常に攻撃に対して備えがなされており、その脆弱性は宇宙システムと比較するとはるかに低いと言えよう。しかしながらサイバー空間では、特定の標的だけでなく、その標的にネットワークで繋がっているさまざまなサブネットワークが存在する。サイバー攻撃を避けるために、基幹的なインフラに関するネットワークは外部から遮断され、スタンドアローン（stand alone）にしているケースが多い。しかしながら、アメリカとイスラエルが開発したと言われるスタックスネット（Stuxnet）によって2010年にイランの核施設が攻撃された事件は、そうしたスタンドアローンのネットワークでも攻撃の対象になることが証明された。このスタックスネット事件はインターネット経由でコンピュータに感染し、そのコンピュータに兆候をみせることなく潜伏し、そのコンピュータにUSBメモリを挿すとUSBにワーム（コンピュータウィルス）が感染し、そのUSBをスタンドアローンのネットワークに接続しているコンピュータに挿すことで侵入した。この結果、イランのナタンズにある遠心分離機の制御装置が異常を起こし、稼働できなくなった。また同じくイランの民生用原子力発電所であるブシェール原発でもスタックスネットの被害があったと言われている(10)。

このように、サイバー空間における攻撃は、帰属問題と防御の難しさから日常的に行なわれているが、その攻撃は最も脆弱なポイントを標的にして行なわれる。これは、軍事的に枢要なシステムだけでなく、経済社会に不可欠なインフラを運営している企業や組織に対しても日常的に攻撃が行なわれ、それらの企業や組織に属する人物やコンピュータが常に標的になることを意味している。また、日本年金機構のネットワークが攻撃されたように、それらの企業や組織に属している人物の個人情報を得るために、直接的には関係ないネットワークまで攻撃の対象となっている。こうした「鎖の中の最も弱い環（weakest link）」を狙ったサイバー攻撃も日常化しているということを社会の構成員があまねく理解しておくことがサイバー攻撃に対する適切な防御となる。

2　宇宙・サイバー空間における抑止

宇宙空間、サイバー空間がともに新たな作戦領域となり、安全保障の空間的変容が常態となるのであれば、その空間における安全保障戦略も検討されなければならない。そこでまず

確認しておかなければならないのは、宇宙・サイバーは伝統的な安全保障の概念がきわめて適用しにくい空間である、ということである。

その際、とりわけ重要になるのは、宇宙・サイバー空間とも、物理的に支配することが不可能な空間であるということである。伝統的な安全保障戦略は、必然的に地理的空間の概念を前提にして立てられてきた。国土防衛や勢力圏といった概念は、ある特定の地理的空間を支配し、そこに軍事的な優位性を確立することで他者の影響を排除するということが大前提となっている。また、そのための手段として陸域においては占領や排他的支配、海域では制海権、空域では制空権といった、地理的な空間において外敵を排除する概念として表現されている。日本における周辺事態法などの国会論戦でも、その安全保障が及ぶ範囲として「地理的概念」が大きな議論になったことも合わせて考えておく必要があるだろう。

しかし、宇宙・サイバー空間では、地理的に排他的な支配を確立することは不可能である。中国などでは制宙権ないし制天権といった概念が用いられ、宇宙空間を支配するといった軍事戦略上の概念がみられるが、現実的に宇宙空間の特定の部分を支配し、外敵を排除することはできない。地球周回軌道を飛翔する物体は常に時速2万8500kmのスピードで移動しており、一箇所にとどまっているわけではない。静止軌道上の衛星も、地球の自転と同じ速度で移動しているから静止しているようにみえるのであり、人類社会からみれば、一定の空間的な属性と排他的な利用が可能であるが（国際電気通信連合〔ITU〕における国際合意に基づいて通信衛星などによる静止軌道のスロットの排他的利用は認められている）、物理的にその宙域を支配しているわけではない。また、国際宇宙ステーションや中国の有人宇宙実験室である天宮2号も同様に軌道上を周回しており、その構造物のなかで排他的な支配圏を維持しているにすぎない。海洋のアナロジーで言えば、有人宇宙構造物は海に浮かぶ船であり、船舶のなかでは排他的な支配圏をもっているとしても、それを制海権とは呼ばないのと同様に、宇宙ステーションを運用しているからといって宇宙空間を支配することはできない。もし排他的な支配圏を確立するのであれば、宇宙空間に物体を打ち上げようとするあらゆる試みを排除し、撃墜する能力をもたなければならないが、それは現実的に困難であるし、同時に宇宙条約（「月その他の天体を含む宇宙空間の探査及び利用における国家活動を律する原則に関する条約」）第1条に規定された、全人類に認められた宇宙空間の利用を否定する行為であり、条約違反となる。

また、サイバー空間も同様に仮想の空間であり、特定の領域を支配することが困難な空間である。もちろん、IPアドレスは各国ごとにドメインが振られており、その意味では一定の地理的な属性は備えている。また、物理的に国境を越えるケーブルを切断すれば、国内のネットワークを排他的に利用することは可能である。また中国やアラブ諸国などが国内の政治的・宗教的理由から特定のサービスを禁止し、国外にあるサーバーにアクセスすることを禁じたり、国内でそうしたサービスを展開することを阻んだりすることは可能である。しかし「自律・分散・協調」を基本原理とするサイバー空間[11]では、こうした排他的な支配は異常であり、不適切な状況を生み出す。それはサイバー空間を利用することによって得られる便益を著しく引き下げ、排他的になればなるほどサイバー空間を利用する効用が下がるという問題を抱える。実際、「アラブの春」後の混乱のなかでエジプトのインターネット・サービ

ス・プロバイダ（ISP）がサービスを停止したことでエジプト全体がサイバー空間から切り離された状態になったが[12]、電話回線などを通じてネットワーク上の通信を可能にするなど、さまざまな方法がとられて効果が出なかったこと、また、サイバー空間から切り離されることで失う便益があまりにも大きかったことから、数日で復旧した。

このように、地理的空間を支配することが難しい宇宙・サイバー空間においては、他の作戦領域のような安全保障戦略を練ることは大変困難であるが、なかでも難しいのは「抑止」の概念をいかにこれらの新しい作戦領域に導入するか、という問題である。

宇宙・サイバー空間における抑止は、帰属問題や宇宙・サイバー空間における排他的な支配が困難なことから、「懲罰的抑止」すなわち攻撃に対して報復があることを想定させることで相手の攻撃を抑止するのではなく、「拒否的抑止」すなわち相手の攻撃の効果を極限まで低めることで、攻撃することのコストを高め、攻撃そのものの意味をなくすという考え方が中心であった[13]。すでに論じたサイバー防御を機動的に運用することや、宇宙空間における抗堪性の強化といった方法が「拒否的抑止」にあたる。

しかしながら、宇宙・サイバー空間が第4、第5の作戦領域となり、仮に「拒否的抑止」が機動的に運用されているとしても、それに対する攻撃が相手の交戦能力を劣化させることが明らかになった今、「拒否的抑止」だけでは抑止として不十分であるという認識が高まっている。そのため、何らかのかたちでの「懲罰的抑止」の方法の模索が続けられている。

宇宙・サイバー空間で決定的に重要になってくるのは帰属問題を解決することである。宇宙においては宇宙空間監視（SSA: Space Situational Awareness）の重要性がきわめて高まっている。SSAとは、地上や宇宙空間にレーダーや光学望遠鏡を配置し、そこから地球軌道を周回する物体を監視し、宇宙物体をカタログ化していくことである。現在、米国防総省を中心に、日本やオーストラリア、欧州各国がもつSSA能力を連携させ、直径10cm以上の大きさの宇宙物体であれば識別できるだけの能力をもつと言われている。こうした宇宙物体の監視により、稼働中の衛星に異常接近する物体や地上からの攻撃がいかにして行なわれたのかを把握することができる。また、宇宙デブリが国際宇宙ステーションや稼働中の衛星に衝突する可能性がある場合も、その可能性を衛星の運用者に通達し、衝突を回避することができる。しかし、SSAはあくまでも物理的な接近や衝突に対して警告を発したりすることができるにとどまり、非物理的な攻撃については十分な監視能力をもっているわけではない。

サイバー空間においては、サイバー鑑識（cyber forensics）と言われる技術が発達し、サイバー攻撃やサイバー空間における犯罪を明らかにする作業が進められるようになった。しかし、この分野は常に新しい技術が開発され、サイバー鑑識をすり抜けるプログラムやウィルスが開発され、帰属問題を完全に解決することはできない状況にある。

また、宇宙・サイバー空間で抑止戦略を実行する場合、同じ作戦領域で抑止を実施することは困難である。核抑止戦略の中心には核攻撃に対して、核攻撃で報復することがあり、通常兵器の攻撃に対して、核攻撃で報復するという戦略を明示的にもっている国はない[14]（北朝鮮のように、どのような核戦略をもっているのかが曖昧な国はあるが）。しかし、宇宙・サイバー空間においては、その作戦領域において発生する被害の差が非対称的であるため、抑止の

効果が得られない、という問題がある。すでに述べたが、アメリカのように宇宙システムに大きく依存している国家は、ASATなどによって衛星機能が失われた際の損害はきわめて大きくなるが、その敵対的行為を行なう主体が北朝鮮のように宇宙システムに強く依存していない場合、宇宙システムへの攻撃に対する報復として相手の宇宙システムに攻撃を加えても抑止にはならない。同様に、サイバー空間においても、例えば金融システムのような国家の基幹的インフラのネットワークに対して攻撃が行なわれたとしても、その敵対的行為を行なった国家（ここでも北朝鮮を想定するとわかりやすい）の基幹的インフラがネットワークに依存していない場合、同じドメイン（作戦領域）での抑止が成立しない。

そのため、宇宙・サイバー空間における抑止は必然的に「ドメイン横断型」の抑止となる。つまり、宇宙・サイバー空間に対して行なわれた攻撃に対し、通常の武力による報復がなされる、ということである。この問題は、2007年のエストニアに対するサイバー攻撃を受けて、北大西洋条約機構（NATO）がサイバー攻撃に対する軍事的対処の可能性について議論し、国際法上とりうる措置を論じた「タリン・マニュアル」が制定された頃から定式化されてきた。タリン・マニュアルでは国家主権の侵害が認められた場合、あるいは深刻な損傷や人的被害が出る場合にのみ、国がサイバー攻撃に対し通常兵器を用いる権利があると定められているが[15]、これはあくまでもNATO加盟国の国際法学者の見解であり、NATOの公式なサイバー抑止の概念ではない。宇宙空間においては「タリン・マニュアル」に相当するものはまだないが、宇宙物体には主権が及び、それに対する攻撃に対して武力による報復がなされることは「国家に固有の権利（inherent right of states to individual or collective self-defence）」であるという認識が、現在議論されている「宇宙空間の国際行動規範」に含まれている[16]。

この際、安全保障戦略上重要となってくるのが、いかにして紛争のエスカレーションをコントロールするか、という問題である。宇宙・サイバー空間における攻撃に対し報復する場合、どの程度の損害が生まれたときに報復が正当化されるのか、また実際に物理的な武力行使をする場合、何を対象とし、どのような手段が認められるのか、といったことに関し、まだ国際的な合意は成立していない。そのため、物理的な武力行使による報復が実際に行なわれた場合、それが紛争の激化につながらないようにするために、その意図を明確化し、宇宙・サイバー空間への攻撃に対する限定的な報復であるということを明示していかなければならないであろう[17]。こうしたルール作りはこれからの大きな課題である。

まとめ

宇宙空間とサイバー空間は間違いなく新しい作戦領域となり、それによって安全保障の空間的な構造は大きく変容した。宇宙空間もサイバー空間も元々は軍事的な目的を含んだかたちで技術開発が進んだが、宇宙空間は宇宙の探査や通信、放送、気象、測位など経済社会的な役割も多くもつようになり、そのインフラは国家や国際社会にとって基幹的なものとなっている。同様に、サイバー空間も民間の研究者のネットワークから商業的なネットワークの広がり、そして今ではサイバー空間に接続することなく日常生活を過ごすことは不可能になるほど、経済社会のなかに深く組み込まれている。そうした技術が、今度は軍事的にスピン

オンするかたちで現代の安全保障に不可欠なドメインとなっている。

そのため、有事においては宇宙・サイバー空間は陸、海、空といった伝統的な作戦領域よりも先に攻撃しなければならない対象になりつつあり、また、宇宙・サイバー空間での戦闘は直接目に見えず、直接死傷者を出すものではないだけに、攻撃を仕掛ける敷居も低い。また、国家の経済社会に深く組み込まれているからこそ、宇宙・サイバー空間での攻撃は小さな攻撃でも大きな成果を上げることができ、また、他者を排除することが困難であるという物理的・システム的構造は攻撃へのインセンティブを高めている。そうした攻撃を抑止するための方策もさまざまに考えられているが、今のところは攻撃を避け、防御能力を高めていく「拒否的抑止」しか有効な手段はない状況である。

宇宙・サイバー空間が加わった現代の安全保障は間違いなく第2次大戦後の安全保障の流れを大きく変えている。そろそろ日本でも70年前の戦争イメージから脱却し、新たな安全保障の空間的構造を踏まえた議論と対処に本格的に取り組むべきである。

（1） 科学技術の発展と戦争の変化についての研究は多数あるが、ここではさしあたりW・H・マクニール（高橋均訳）『戦争の世界史――技術と軍隊と社会』、刀水書房、2002年などを参照。

（2） 中国の軍事戦略と宇宙戦略についての最新の研究として、草稿ではあるが公開されているものとしてAnthony H. Cordesman, *Chinese Space Strategy and Developments*, Center for Strategic and International Studies（CSIS）, August 2016〈https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160819_Chinese_Space_Strategy_Developments.pdf〉を参照。

（3） Sven F. Kraemer, *Inside the Cold War From Marx to Reagan: An Unprecedented Guide to the Roots, History, Strategies, and Key Documents of the Cold War*, University Press of America, 2015, esp. Chapter 13.

（4） Karl Ginter, *Space Technology and Network Centric Warfare: A Strategic Paradox*, U.S. Army War College, 2007〈http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA469763〉.

（5） 2007年の中国によるASAT実験の前からこの問題が議論されてきた。とりわけ2001年に米国議会の宇宙安全保障管理・組織特別委員会（通称ラムズフェルド委員会）によってこの問題が指摘されたことが嚆矢となっている。*Report of the Commission to Assess United States National Security Space Management and Organization: Pursuant to Public Law 106-65*, January 2001〈http://www.dod.gov/pubs/space20010111.pdf〉.

（6） Office of the Assistant Secretary of Defense for Homeland Defense & Global Security, *Space Domain Mission Assurance: A Resilience Taxonomy: A White Paper*, September 2015〈https://fas.org/man/eprint/resilience.pdf〉.

（7） 『ナショナル・インタレスト』誌では中ロが非物理的な宇宙攻撃兵器を開発していると報じている。Malcolm Davis, “Russia and China are Developing Some Very Powerful Weapons That Can ‘Kill’ Satellites,” *The National Interest*, November 9, 2016〈http://nationalinterest.org/blog/the-buzz/russia-china-are-developing-some-very-powerful-weapons-can-18347〉.

（8） “North Korea ‘jamming GPS signals’ near South border,” BBC News, 1 April 2016〈http://www.bbc.com/news/world-asia-35940542〉.

（9） しかし、コロンビア大学のサイバー安全保障の専門家であるヘイリーは、政府の関与が明確でなくても、その国家から行なわれた攻撃であれば政府が責任をとるべきであるとの議論を展開している。Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks,” Issue Briefs, Atlantic Council, January 2012〈http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF〉.

（10） Caroline Baylon, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, Chatham House, Septem-

ber 2015〈https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstoneUpdate.pdf〉.

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

（12） 「インターネットが“消えた”：グラフで見るエジプトのネット遮断」、ITメディアニュース、2011年1月31日〈http://www.itmedia.co.jp/news/articles/1101/31/news044.html〉.

（13） 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」、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。

（14） 核の先制不使用を宣言していれば、核兵器は核攻撃に対する抑止にしか使われないが、先制不使用を宣言していない場合は、通常兵器に対する核の報復がありうる。だが、それを明示的に示している国はない。

（15） Michael N. Schmitt（ed.）, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, March 2013.

（16） DRAFT International Code of Conduct for Outer Space Activities, VERSION 31 March 2014〈https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf〉.

（17） この点に関して幅広く論じた文献として、Martin C. Libicki, *Crisis and Escalation in Cyberspace,* RAND Corporation, 2012〈http://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1215.pdf〉を参照。

すずき・かずと　北海道大学教授
http://lex.juris.hokudai.ac.jp/~kazutos/
kazutos@juris.hokudai.ac.jp