第８章　「新領域」と日本の安全保障

高橋　杉雄

はじめに

2018 年 12 月に策定された「平成 31 年度以降に係る防衛計画の大綱」（以下、2018 年防衛大綱）および「中期防衛力整備計画（平成 31 年度～平成 35 年度）」において、我が国は「多次元統合防衛力」を構築していく方針を打ち出した。これを 2018 年防衛大綱の前に策定された「平成 26 年度以降に係る防衛計画の大綱」（以下 2013 年防衛大綱）において打ち出された「統合機動防衛力」と比較すると、大きな特徴として、宇宙・サイバー・電磁波領域を「新領域」とし、この「新領域」を重視していく方向が鮮明に打ち出されたことを指摘できる。

ただ、この「新領域」とは、完全に新しいものというよりも、むしろ「古くて新しい」と呼び得るものである。宇宙空間の軍事利用は、冷戦期の 1950 年代末に始められていたし（最初の偵察衛星が打ち上げられたのは 1959 年）、電子戦に至っては第二次世界大戦の時にすでに行われている。サイバー空間については相対的に新しいが、それでも 1990 年代後半にはサイバー戦をめぐる問題についての議論が真剣に行われるようになっていた。

それを改めて「新領域」と名付けたことの背景としては、2018 年防衛大綱において、「宇宙・サイバー・電磁波といった新たな領域の利用の急速な拡大は、陸・海・空という従来の物理的な領域における対応を重視してきたこれまでの国家の安全保障の在り方を根本から変えようとしている」という認識をベースに、「宇宙・サイバー・電磁波といった新たな領域については、我が国としての優位性を獲得することが死活的に重要となっており、陸・海・空という従来の区分に依拠した発想から完全に脱却し、全ての領域を横断的に連携させた新たな防衛力の構築に向け、従来とは抜本的に異なる速度で変革を図っていく」および「全ての領域における能力を有機的に融合し、その相乗効果により全体としての能力を増幅させる領域横断（クロス・ドメイン）作戦により、個別の領域における能力が劣勢である場合にもこれを克服し、我が国の防衛を全うできるものとすることが必要である」との考え方を示したように、「新領域」を戦力増幅要素（フォース・マルチプライヤー）として活用し、仮に在来領域において劣勢に立たされたとしても、「新領域」によってその劣勢を相殺するという戦略構想を打ち出したことがあると考えられる。ただし、自衛隊においてはこれらの領域に対する本格的な取り組みがなされてこなかったため、自衛隊の取り組みとしては実際に「新しい」ということについても指摘しておく必要があろう。

本稿では、この「新領域」と日本の安全保障の関係について、「新領域」の特徴、その活用に伴って生まれる論点、さらに政策上の課題について議論することとする。

１．新領域の特徴

（1）宇宙

前述した通り、米国は冷戦初期にすでに宇宙空間の軍事利用を始めており、宇宙は決して「新しい」領域ではない。しかしながら、冷戦期においては、宇宙空間の軍事利用は戦略核戦力の運用と密接に結びついていたため、同じく大規模に宇宙空間を利用していたソ連との相互核抑止関係の中で、宇宙空間はある種の「聖域」として認識されていた。特に早期警戒衛星は核抑止において不可欠な要素であると認識されていたため、これを攻撃することは全面核戦争を始める意思があるのと同義であると捉えられていたのである。その結果として、米ソ双方にとって、宇宙空間においても相互抑止が成立し、核戦争へのエスカレーションの覚悟がなければ、相手側の宇宙能力を直接攻撃することはできないような状況が形成された。

引き続くポスト冷戦期においては、ソ連が崩壊したため、米国に対抗するレベルで宇宙空間を利用できる国家は存在せず、米国は事実上宇宙空間を独占的に利用することができた。

中国の宇宙空間利用が進んだことによって、この状況が変わった。中国は、米国の軍事行動が宇宙空間に依存していることを踏まえ、自らの宇宙空間利用を進めるだけでなく、対衛星兵器など、米国の宇宙空間利用を物理的に妨げる能力を整備してきたのである。こうした状況を踏まえ、米国においても、宇宙空間をこれまでのように安定的かつ独占的に利用することが難しくなっているとの認識が形成されており、これまで整備してこなかった宇宙空間に関連する戦闘能力についても整備していくべきとの指摘もなされるようになっている[1]。

宇宙空間の利用については、大きく分けて、情報収集（ISR）、衛星通信、精密航法・タイミング（PNT）、宇宙状況把握（SSA）、戦略抑止の 5 つの機能に分類することができる。情報収集は、光学望遠鏡や合成開口レーダーなどのセンサーによって地上の情報を収集するためのものである。この場合、地上との距離が近い方がより精密な監視ができることから、衛星は低い軌道を飛翔することになり、必然的に多数の衛星を必要とすることとなる。PNT も、米国の GPS システムが典型であるが、複数の衛星からの電波をとらえて地上の座標を精密に測定すると同時に、精密に時刻を同期させるものであるから、やはり相対的に低い軌道を飛ぶ多数の衛星を必要とする。

一方、衛星通信は、静止衛星軌道に置かれた通信衛星によって地球の曲面を越えて通信をするためのものである。静止軌道は 36,000 ㎞もの上空にあるので、ISR や PNT と異なり、3-4 個の衛星で全地球をカバーすることができる。SSA は、宇宙空間の衛星や宇宙ゴミの監視をする機能である。これは地上からのレーダーや光学望遠鏡によっても行われるが、宇宙空間から衛星などを直接監視するのも有効である。ただこれを宇宙空間から行う場合には、地上から距離が離れた高軌道衛星に対して行うことが相対的に有効であると考えられるから、やはりそれほど多くの衛星は必ずしも必要とされない。最後の戦略抑止は、核ミサイルの発射を探知するための早期警戒衛星や、将来の BMD（弾道ミサイル防衛）システムの構想にあるような、飛来するミサイルの軌道を詳細に把握し、キューイングを行う衛星などが含まれる。

こうした宇宙空間利用を妨害する手段として、物理的攻撃と非物理的攻撃がある（ほかに衛星を管制する地上局を攻撃する方法もあるが、ここでは除外する）。物理的攻撃は、文字通り物理的に相手の衛星を破壊しようとするもので、地上からミサイルを発射する直接上昇式（direct ascent）ASAT（対衛星攻撃兵器）や、人工衛星として軌道を飛翔し、目標の衛星に近接してロボットアームなどを用いて攻撃する同軌道（co-orbit）ASAT などがある。非物理的攻撃は、物理的な破壊を伴わず相手の衛星の機能を妨害しようとするもので、電波による妨害であるジャミング、光学センサーにレーザーを当てて妨害する幻惑などが含まれる。

上述の通り、衛星はその機能によって必要な数や軌道高度が異なるため、使用される攻撃手段も変わってくる。例えば GPS 衛星であれば、約 30 も数があるため、これを物理的攻撃によって撃破するには手間がかかる。逆に地上において妨害電波を放射し、GPS 衛星からの電波の受信を困難にすれば、測位ができなくなるので、攻撃側としては十分目的を達成できる。逆に通信衛星であれば数が限られるので、いくつかの衛星を撃破できれば大きく相手の機能を低下させることができる。他方静止軌道に対して直接上昇式の ASAT で攻撃するのは容易ではないので、あらかじめ静止軌道に配備した同軌道 ASAT による攻撃を行うことが効率的であろう。

（２）サイバー

サイバー空間における攻撃は、大きく 3 つに分けることができる。第 1 が DDos（分散型サービス拒否）である。これは、特定のサーバーにアクセスを集中させることによってそのサーバーを機能不全に追い込むための攻撃であり、比較的容易に実施することができる。しかしながら、通常のインターネットに接続されているサーバーに対してしか行うことは

できないため、エアギャップ（インターネットとの物理的な離隔）が通常設けられている軍事用のネットワークに対する攻撃を行うことはできない。ただし、DDos 攻撃はマルウェアを世界中のコンピュータに仕込むことで実行可能であるから、攻撃発信源を一定期間隠匿することは困難ではない。そのため、民間の重要インフラを攻撃し、相手の社会全体を混乱させる上では有効な手段となりえる。第 2 がクラッキングであり、回線を通じてターゲットとなっているサーバーに侵入し、情報を窃取したり遠隔操作したりするものである。これもまた、エアギャップが設けられているシステムに対する攻撃は困難になる。

第 3 はマルウェアであり、不正な動作をするプログラムをあらかじめ目標に仕掛けておき、一定のトリガーを満たしたときに作動させる。この有名な例が、イランに対して行われた「スタックスネット」による攻撃である。広く知られているとおり、スタックスネットは、USB ドライブを使用してエアギャップを越えて仕掛けられ、イランのウラン濃縮装置の制御プログラムを書き換え、それらを破壊した。軍事的なネットワークは通常エアギャップを施されていると考えると、安全保障の面から見て特に重要なのはマルウェアによる攻撃と考えることができる。ただしマルウェアは一度作動した場合その存在が露見してしまう。マルウェアの存在が判明すれば、それは駆除されてしまうため、エアギャップを越えて仕掛けられたマルウェアは一度しか使えないという制約がある。

（３）電磁波

電磁波領域においては、電子戦（Electronic Counter Measures: ECM）とそれに対抗する対電子戦（Electronic Counter-Counter Measures: ECCM）があり、ジャミングなど、相手側の通信やレーダーを妨害するのが ECM、それに対抗して自分たちの通信やレーダーの機能を維持しようとするのが ECCM となる。また最近では、高周波電磁波の放射により相手のセンサーを破壊する RF（高周波）兵器についても議論されるようになっている[2]。

なお、電磁波領域は、宇宙における非物理的 ASAT との重複がある。特に、非物理的 ASAT の 1 つであるジャミングは、衛星に対する指令電波などを妨害するアップリンクジャミングと、衛星から地上への電波を妨害するダウンリンクジャミングとがあるが、このうち、GPS に対するジャミングを含むダウンリンクジャミングは、地上での受信アンテナに対して行われるものであるから、地上におけるジャミングと本質的な違いはない。実際、2018 年防衛大綱においては、「相手方の指揮統制・情報通信を妨げる能力」についての言及があるが、これは主として電磁波領域におけるジャミングを指しているように思われる。

２．政策上の論点と課題

宇宙・サイバー・電磁波によって構成される新領域は、基本的にはC4ISRという言葉によってカバーされる分野全てに関わるものである。ただこれは、陸海空軍力のような意味で、物理的空間において使用されるものではない。新領域の作用の中心にあるのは、陸海空軍力のような物理的な能力を増幅する作用や相手の物理的能力の効果を低減する作用であり、その意味でまさにフォース・マルチプライヤーとして位置づけられることになる。

また、新領域においては物理的な破壊を伴わない攻撃が可能であるといった特徴もあり、この点はグレーゾーンにおいて特に重要な意味を持つ可能性がある。本節では、こういった点を踏まえながら政策上の課題を検討する。

（１）グレーゾーンと新領域

新領域は、フォース・マルチプライヤーとして陸海空といった在来領域の能力・効果を増幅すると同時に、非物理的使用を通じて、グレーゾーンにおいても大きな効果を発揮する可能性が高い。グレーゾーンにおいては、海上保安庁や警察など、軍隊ではない、法執行機関が中心的な役割を果たす。これに対し、特に海洋におけるグレーゾーンにおいて、現状打破側がGPSジャミングを行った場合、現状維持側のアセットは自己位置の測定が困難になり、また領海線やEEZの境界線も不明になってしまうため、適切な対応を行うことが極めて難しくなる。また、グレーゾーンにおいては、エスカレーションコントロールを精緻に行う必要があるため、時には中央からのマイクロマネージメントを行うことが不可欠になると考えられるが、通信衛星に対するアップリンクジャミングや地上におけるジャミングを行い、中央とのコミュニケーションを絶つことができれば、やはり現状打破側が優位に立つことができるであろう。

特に、一般的に見て、法執行機関はジャミングへの耐性が軍事組織よりも脆弱であることが予想される。そのため、グレーゾーンにおける新領域の非物理的使用は非常に大きな効果をもたらす可能性があるのである。

また、こうしたジャミングだけでなく、海上保安庁の指揮システムや補給システムに対してマルウェアによるサイバー攻撃を行った場合でも、同様の効果が期待できる。これも物理的破壊をもたらすものではないが、海上保安庁の適時適切な対応を困難にすることによって、現状打破側がグレーゾーンの事態を有利な形で展開させていくことを可能とするのである。

現在の日本の安全保障において、グレーゾーンの重要性が極めて大きく、そしてグレーゾーンにおいては警察や海上保安庁などの法執行機関が重要な役割を果たすことを考える

と、新領域に関する能力の充実が必要とされるのは自衛隊だけではない。警察および海上保安庁においてもその能力を高めていくことは不可欠である。加えて、新領域における自衛隊と法執行機関との連携の強化も進めていかなければならない。その意味で、2018 年防衛大綱で謳われた多次元統合防衛力の、「多次元統合」には、自衛隊のみならず、国内で安全保障に関わる法執行機関をも包含していく必要がある。

さらに、グレーゾーンにおいて新領域の非物理的使用が有効だとすれば、我が国もそうした能力を整備し、具体的な使用を想定した体制整備を進めていく必要がある。我が国がそうした能力を有効に整備できれば、ある種の相互抑止的な効果も期待できるし、実際に使用される局面になった場合には、現状打破側の行動を大きく混乱させることができるであろう。それに関連して法的な整理を行う必要もあるため、法的な議論も並行して進めていくことが望ましい[3]。

（２）新領域とエスカレーション

新領域とグレーゾーンに関連するもう１つの論点は、グレーゾーンからのエスカレーションに関連して、新領域が加わることによってエスカレーションのダイナミクスがどう変わるか、あるいは変わらないかである。これは、グレーゾーンから紛争への在来領域におけるエスカレーションと、非物理的使用を含む新領域におけるエスカレーションとの関連性をめぐる問題である。比喩的な意味でいえば、「エスカレーションラダーは在来領域に立っているのか、あるいは新領域に立っているのか」という問いであるともいえよう。特に、サイバー攻撃においては、重要インフラに対する物理的攻撃も可能であると考えられているから、グレーゾーンから事態がエスカレーションしていくプロセスの中で、どのような形、タイミングで新領域を利用した物理的攻撃が行われるかは、エスカレーションをコントロールするうえで重要な論点になる。

新領域の特徴を考慮すると、この点については以下のような仮説が成立しうると考えられる。まず、グレーゾーンにおいては、グレーゾーンにおいて優位に立つことを目的に、在来領域における現状変更の試みと連動する形で、新領域の非物理的使用が多用される可能性が高い。グレーゾーンにおける非物理的使用に限って言えば、エスカレーションは容易に発生するのである。

しかしながら、新領域であっても、物理的攻撃を行う場合には、現状打破側としてもより大きなリスクを覚悟する必要がある。例えばサイバー攻撃によって物理的ダメージを与えた場合、それを武力攻撃と解釈し、現状維持側が対応をエスカレートさせ、法執行機関に代わって軍事組織によって当該グレーゾーンへの対応を行うようにすることが考えられ

るからである。仮に法執行機関同士の対応において優位に立てる公算が高いのであれば、あえて相手側の軍事組織の投入を誘引するような物理攻撃を行う必要はない。

また、マルウェアは一度使用すればその存在が発覚し、駆除されてしまう可能性が高い。そのため、仕掛けられたマルウェアは最大の効果を発揮するタイミングで発動させることが有効であるが、そのタイミングとはおそらく在来領域で決定的な行動を取るタイミングになることが予想される。

よって、新領域の物理的使用へのエスカレーションは、在来領域のエスカレーションの効果を最大化させるために、それと連動して行われる可能性が高いと考えられるのである。この場合、在来領域のエスカレーションと新領域におけるエスカレーションが同時並行的に展開することになる。グレーゾーンにおいては、現状打破側においては新領域の物理的使用は抑制されると考えられるが、ひとたびグレーゾーンから紛争へとエスカレーションさせることを一方が決断した段階で、新領域を含めたエスカレーションが急激に発生することが考えられる。特にこの新領域におけるエスカレーションは、現状維持側の状況把握能力を少なくとも一時的には著しく低下させる可能性が高い。今後の我が国の危機管理体制は、こうした点を考慮しながら手直ししていく必要がある。

（３）防衛力整備上の課題

2018 年防衛大綱においては、新領域の防衛戦略上の位置づけとして、「個別の領域における能力が劣勢である場合にもこれを克服し、我が国の防衛を全うできるものとする」と記述されている。すなわち、在来領域において劣勢になったとしても、新領域においてそれを克服していくという考え方である。そのためには、相手に対して、新領域において相対的に優勢にある必要がある。しかしながら、例えば中国は、米軍のハイテク兵器の威力を見せつけた湾岸戦争やコソボ空爆を踏まえ、「ハイテク条件下の局地戦」概念を打ち出し、20 年以上にわたってこうした新領域の能力を大幅に強化させてきた[4]。一方、自衛隊のこの分野における取り組みは近年ようやく本格的に始まったものであり、中国と比べた場合、自衛隊の新領域の能力は大幅に遅れを取っているのが現状であると考えざるを得ない。

実際、2018 年防衛大綱と同時に策定された中期防衛力整備計画における整備計画を見ると、宇宙領域であれば SSA に関する宇宙設置型光学望遠鏡やレーザー測距装置、X バンド衛星通信網、電磁波領域と連携しての相手方の指揮統制・情報通信を妨げる能力の構築など、具体的な進展を見て取ることができる。しかしながら、サイバー領域においては、やはりサイバー攻撃を含意するとみられる「相手方によるサイバー空間の利用を妨げる能力を保持し得るよう」という記述があるが、具体的な進展は定かではない。電磁波領域に至っ

ては、データリンクやステルス戦闘機 F-35 の導入といった既存事業が中心であり、電子戦分野については、調査や研究開発を迅速に進めると記述されているだけで、具体的な進展を見て取ることはほとんどできない。この現状では、特に中国と比べた場合、まずはこれ以上能力的に引き離されないこと、ついでキャッチアップすることが精いっぱいであると考えざるを得ず、在来領域における劣勢を克服するというレベルにはまったく至っていない。次期防衛大綱、次期中期防に向けて、この分野を具体的に進展させていくことが急務である。

（４）日米同盟における論点

前述した通り、グレーゾーンにおいて新領域は重要な影響をもたらす可能性が高い。それは GPS ジャミングや通信衛星に対するジャミング、情報収集衛星に対する光学的な幻惑といった非物理的攻撃によって行われるであろう。こうした分野においては、日本一国だけでなく、米国とも協力して対抗していくことが有効である。例えば宇宙分野においては、他国のセンサーやアンテナを積むホステッド・ペイロードという協力形態がある。具体的には、日本の通信アンテナを米国の衛星に積むとか、その逆といったことである。

こうした協力を進めていくと、グレーゾーンにおけるミッション・アシュアランスが容易になっていく可能性がある。例えば、日中のグレーゾーンの事態において、中国が日本の衛星を妨害したとしても、米国の衛星によって宇宙関連の任務が遂行できることとなる。これに対し、もちろん中国は米国の衛星を妨害すれば、日本の宇宙空間の利用を妨害することができるが、それは米国を巻き込む水平的エスカレーションとなるため、中国としても慎重にならざるを得ないであろう。そして結果として米国の衛星によって関連する任務が遂行できるとすれば、そもそも日本の衛星に対する妨害も無意味であるとの結論に至る可能性もある。

逆に、日本の衛星が米国の宇宙機能の一部についてホステッド・ペイロードによる補完を行うとすれば、バルト海でロシアと NATO との間に危機が発生し、ロシアが米国の衛星に対する妨害を行ったとしても、日本の衛星を利用して任務を遂行することができる。この場合、ロシアが日本の衛星を妨害するならば、それは日本を巻き込む水平的エスカレーションとなってしまうため、ロシアとしても慎重にならざるを得ないことが予測できるのである。現状、アジアとヨーロッパの双方でグレーゾーンが懸念されていることを考えれば、こう言った形でホステッド・ペイロードを進めていくことによって、アジア・ヨーロッパ双方におけるグレーゾーンの対応能力を強化していくことが期待できる。

サイバー分野についてはこれまでも情報共有が進められているのであろうから、それを

継続していくことが重要である。電磁波領域については、米国はこれまで豊富な経験を有しているから、日本側がこれから本格的に導入していくにあたっての支援を期待することになろう。

終わりに

現在の安全保障の在り方を議論するうえで、新領域の問題は無視することができない重要性がある。その意味で、2018 年防衛大綱は、在来領域に加えて新領域を重視し、特に在来領域における劣勢を克服する手段として位置づけた点で画期的な防衛大綱であったということができる。ただし現在のところその取り組みは十分ではない。大きく以下の 2 点の課題を指摘することができる。第 1 は、同時に策定された中期防衛力整備計画に示された具体的な事業を見る限り、実際の取り組みとしては、在来領域における劣勢を相殺するにはまったく十分ではないと考えざるを得ないことである。特に中国はこの分野における取り組みが日本より 20 年は先行しているという現実を認識したうえで、危機感を持って取り組んでいく必要がある。

第 2 は、新領域は在来領域における戦闘との関連だけではなく、グレーゾーンにおいても重要な役割を果たすと考えられることである。特にグレーゾーンにおいては、自衛隊ではなく警察や海上保安庁のような法執行機関が中心となるが、新領域において非物理的攻撃が行われているような環境において、それらの組織が自衛隊よりも高い行動能力を持っているとは考えにくい。グレーゾーンにおける新領域の非物理的攻撃の効果を考えれば、自衛隊のみならず、警察・海上保安庁を含めた新領域の能力強化と、法的論点の検討を進めていくことが急務である。

－注－

1 Elbridge Colby, “From Sanctuary to Battlefield: A Framework for a U.S. Defense and Deterrence Strategy for Space,” (Center for New American Security, 2016).

2 Bryan Clark, Mark Gunzinger, and Jesse Sloman, “Winning the Gray Zone: Using Electromagnetic Warfare to Regain Escalation Dominance,” (Center for Strategic and Budgetary Assessments, 2017).

3 Jon R. Lindsay and Eric Gartzke, *Cross-Domain Deterrence: Strategy in an Era of Complexity,* (Oxford University Press, 2019).

4 Tai Ming Cheung, Thomas Mahnken, Kevin Pollpeter, Deborah Seligsohn, Eric Anderson, Fan Yang, “Planning for Innovation: Understanding China’s Plans for Technological, Energy, Industrial, and Defense Development,” (Institute on Global Conflict and Cooperation, 2016)