て衛星を破壊することや、宇宙空間で他の衛星を衝突させて衛星の機能を奪う（いわゆるキラー衛星）といったことも可能である。こうした物理的な攻撃によって衛星の能力を奪うことは軍事戦略的に有効な手段と考えられており、中国だけでなく、アメリカ、ロシアも衛星撃墜の能力を持っている。さらに 2019 年 3 月にはインドが自国の衛星である MICROSAT-R を撃墜し、世界で 4 番目の ASAT 能力保有国となった。

こうした ASAT 実験は宇宙空間において極めて大きな問題を生み出す。それは物理的に衛星を破壊することで大量のデブリが発生するということである。既に述べたようにデブリは宇宙空間を高速で飛翔しており、デブリと衝突すれば衛星は大きく損傷することになるが、さらにその衝突によって多数のデブリが発生し、そのデブリが他の衛星の脅威となる、いわゆるデブリのカスケードが起こる。こうした現象を指摘した NASA の科学者であるケスラーの名を取って「ケスラー・シンドローム」と呼ぶ。このように連鎖的にデブリの衝突によって大量のデブリが地球軌道を汚染し、宇宙空間が安全に利用することのできない空間になってしまうという恐れがある。

しかし、衛星を破壊し、大量のデブリを発生させることは、その衛星を破壊した国にとってもデブリとの衝突リスクを高める行為である。ASAT 能力を持つ米中露印はいずれも安全保障目的でも社会経済目的でも宇宙を利用しており、多数の衛星を保有・運用している。そのため、自国の短期的な軍事的戦略であったとしても、長期的には自国の衛星をデブリ衝突リスクに晒すこととなるため、衛星を破壊するという行為は相当な状況にならなければ積極的に取り得る選択肢にはならないだろう。

むしろ、より懸念されているのは非物理的な衛星攻撃である。衛星と地上の間で通信を行う場合も、GPS 信号を受信する場合も、偵察衛星の画像を見るときも全て無線で地上局と衛星の間で電波のやり取りを行う。そのため、この電波を遮断すれば自らが保有し運用する衛星であってもアクセスできなくなり、その衛星の機能を奪うことができる。こうした妨害電波による工作を「ジャミング（Jamming）」と言うが、非物理的な攻撃はジャミングに限らない。GPS 信号のように衛星からのデータに基づき、自らの位置や必要な情報を取得する場合、その電波に偽りのデータを混ぜることで情報を誤認させ、相手を混乱させるという「スプーフィング（Spoofing）」と呼ばれる手段や、偵察衛星のカメラやセンサーに対して強い刺激を与え、その機能を麻痺させる「ダズリング（Dazzling）」といった手法も用いられる。また、こうした非物理的な攻撃は地上から衛星を狙うだけでなく、軌道上に配置した衛星から行うことも可能である。さらに、非物理的な攻撃として、衛星を管制するためのシステムにサイバー攻撃を行い、ハッキングをして衛星を乗っ取ることや、地上局の衛星を制御するシステムを無効にするという方法もある。

こうした攻撃に対して、防御する方法が極めて限られているだけでなく、その攻撃がどこから行われたものなのか、誰が損害に対して責任を持つのかということを明らかにすることが難しい。こうしたアトリビューション問題は宇宙システムの場合、宇宙状況監視（SSA）によってデブリの動きなどを監視していても、SSA で把握出来るデブリの大きさにも限りがあるため（直径約 10cm 以下のデブリは観測できない）、物理的・非物理的な攻撃によって衛星の能力が失われたとしても、それがデブリによるものなのか、それとも意図的な攻撃によるものなのかを判定することが難しい。紛争状態になった場合、宇宙システムは「おいしい」標的となり、攻撃の対象になりやすい。

さらに、宇宙空間は安全保障のための衛星だけでなく、社会経済活動のための衛星も数多く軌道上を周回している。近年に入って小型衛星の技術革新が進んだことで、廉価に衛星を開発・製造し、打ち上げることが可能になっている。そのため、宇宙空間にはこれまで宇宙開発に関わってこなかった途上国や大学、民間企業が続々と宇宙開発の分野に参入し、技術開発や教育や商業目的で宇宙利用を進めるようになっている（石田, 2017）。こうした新しく宇宙開発に参入してきた主体は、しばしば衛星を打ち上げて運用することを最優先とするため、宇宙空間が安全保障目的で利用されていることに対する意識が希薄であり、衛星管制のプログラムに対するサイバー攻撃からの防護や衛星管制のための電波の管理などが甘くなる傾向がある（Secure World Foundation, 2017）。そして、これらの民間衛星であっても、いったんハッキングされ乗っ取られた場合、その衛星を標的となる軍事衛星と衝突する軌道に乗せ、あたかも事故に見せかけた形で衛星を攻撃することができる。

宇宙空間は長い間、「平和の目的に限り」利用される「聖域」のように扱われてきたが、「安全保障のための宇宙」としての性格が強くなる一方、かつてのような数少ない技術先進国による寡占状態ではなく、途上国や大学までもが自由に参入できる空間となったため、極めて「混雑した」空間にもなってきており、それらを使って敵の宇宙システムを攻撃することが「おいしい」状況が生まれている。こうした変化を受けてアメリカでは、宇宙空間が「戦闘領域（War Fighting Domain）」になったという認識を持つようになり、「安全保障のための宇宙」を活用するためにも「宇宙空間の安全保障」が重要になってきたと考えられるようになってきたのである。

3. なぜ宇宙戦にならなかったのか

では、なぜロシアはウクライナ侵攻に際し、宇宙システムに対して攻撃せず、ウクライナがアメリカの衛星システムを使ってロシア軍の位置を確認し、的確な攻撃をすることを可能にしたのか。また、アメリカの民間企業である Starlink が提供する通信サービスを使うことが出来るようになったのか。もしロシアが本格的にウクライナに対して軍事侵攻を行い、戦場において優勢を獲得しようとするのであれば、宇宙システムを攻撃するのがセオリーではないのだろうか。

3.1.宇宙空間における抑止

宇宙システムが戦時において圧倒的優位性をもたらすものであれば、その衛星の機能を奪うことを目指すことになる。実際、ロシアは、ウクライナへの大規模侵攻を開始する前の、2021 年 11 月に ASAT 実験を実施し、ロシアが保有する衛星を撃墜している。これは、ロシアがウクライナに侵攻した際、アメリカを含む他国が介入するようなことがあれば、衛星を破壊することが出来ると脅すためのデモンストレーションであったと考えられる。

こうした ASAT 能力を誇示するロシアが宇宙戦を展開しなかったのは、宇宙空間における「抑止」が効いていたからだ、と理解するべきであろう。宇宙空間における抑止とは、A 国が保有する衛星に対して B 国による攻撃がなされた場合、耐えがたい損害を伴う報復を、最初の攻撃を B 国に対して行う、と言うものである。しばしば、宇宙における抑止は、例えば「衛星一機撃墜された場合、相手の衛星一機を撃墜する」するといった形の報復が想定されるが、これは有効な抑止ではない。なぜなら、衛星の役割や価値は国によって異なっており、多数の衛星を保有する国家であれば、衛星一機を失っても、他の衛星で代替出来る可能性があるが、限られた数の衛星しか持たず、その役割が大きい場合は過剰な反撃として受け止められるであろう。また、衛星を攻撃する能力は持つが、自らは衛星を保有しない国（例えば北朝鮮）のような国が衛星を攻撃した場合、報復として北朝鮮の衛星を撃墜しようとしても、対象となる衛星がない、という状態が起きる。

そのため、宇宙空間における抑止を論じるには、衛星への攻撃に対して、衛星に対する報復という形で抑止が成立するわけではない。では、どのような形で抑止が成立するのか。それは、衛星に対する攻撃に対して、あらゆる手段を使って報復する、ということになる。つまり、ロシアがアメリカの衛星に対して攻撃を行った場合、アメリカは核兵器を含むあらゆる手段によって報復する可能性がある。つまり、衛星に対する攻撃は第三次世界大戦を引き起こす恐れがある、と言うことである。こうしたエスカレーションの可能性がある限り、衛星を攻撃することは、慎重にならざるを得ないであろう。そのため、ロシアはウクライナ侵攻に対しても衛星を攻撃することはなかったのである。

3.2.　　「打ち上げ国」を巡る問題

しかし、宇宙条約では、衛星には「打ち上げ国」の管轄権が及ぶことになっており、衛星が「誰のものなのか」ということに関しては、法的には複雑な状況がある。打ち上げ国は「一般に宇宙物体登録条約に基づき宇宙物体の登録を行い、また、宇宙損害責任条約が宇宙物体により引き起こされる損害についての責任を負い、賠償を行うべき国」とされるが、衛星の所有権が移転した場合には、その打ち上げ国の概念が複雑化する。A 国に所在し、 B 国が保有する射場ＸからＢ国のロケットで C 国政府の所有する衛星を打ち上げた場合、 A 国が領域打上げ国、 B

国が施設打上げ国、 C 国は打上げを行わせる国となり、宇宙物体登録条約上は C 国が「打ち上げ国」となるが、A 国、B 国とも打ち上げ国として関与することになる。このように、宇宙空間における主権や管轄権の問題は、地上における領域的な規定を適用することが出来ない。

さらに、民間企業の運用する衛星であったとしても、宇宙条約の規定では、その衛星の運用にライセンスを与える国家が責任を負うことになる。Starlink も Maxar もアメリカ政府からライセンスを受けており、その意味では、これらの民間企業の活動もアメリカ政府の管理下にあると言える。もしロシアが何らかの形でこれらのアメリカの民間企業が運用する衛星に攻撃を仕掛けた場合、アメリカ政府に対する攻撃と受け取られる可能性もある。そうなれば、アメリカがウクライナへの侵攻に介入してくる可能性もあり、ロシアとしては望ましい結果とはならないだろう。宇宙空間における自衛権の問題は必ずしも確立した法理とはなっていないが、それでも、ルールがないだけに、アメリカが自衛権を主張して介入してくる可能性を排除できない限り、ロシアもこれらの衛星に対する攻撃には躊躇するであろう。その意味で宇宙空間においても「抑止」が成立しており、それゆえに宇宙システムが「武器」として活用できるのである。

なお、ロシアがウクライナへの軍事侵攻を始めた 2022 年 2 月 24 日に、アメリカの通信衛星会社である Viasat にサイバー攻撃がかけられたことが明らかにされている。Viasat は一般向けのほかに軍事用のブロードバンド通信サービスを提供する会社だが、この衛星会社にサイバー攻撃を仕掛けたのはロシアではないかと疑われているが、まだ攻撃主体を特定するには至っていない。また、このサイバー攻撃による被害は軽微であり、通常のサービスに影響することはなかったと Viasat も発表している。

4. 宇宙とサイバー

衛星に対するサイバー攻撃は、ASAT と異なり、明白な攻撃主体を示すことが困難であり、物理的な破壊を伴わないながらも、衛星の能力を奪うことが出来るという点で、衛星に対する攻撃としてより有効で、現実的な脅威となっている。

2022 年 2 月、ロシアのウクライナ侵攻が始まると同時に、ウクライナをはじめとするヨーロッパの多数の衛星モデムがサイバー攻撃を受け、使用不能となったと報告されている。また、グローバルな通信サービスを提供し、米軍も利用していると言われている Viasat はサイバー攻撃を受け、一時サービスが停止したが、ハードリセット（衛星を一度停止し、再起動を行うこと）を行い、隣国スロバキアのウクライナ難民向けの通信を含むサービスを再開した。

近年では、ソフトウェア定義型衛星の登場により、衛星の運用がより複雑になっている。衛星は常にシステムをアップデートし、サイバー攻撃に対する柔軟性と堅牢性を構築している。伝統的な衛星オペレーターは長い間、ハードウェアとネットワークのセキュリティに長けており、政府、軍事、石油・ガス、海運、金融など、厳しいセキュリティ要件が求められるセクターへのサービスを提供してきたことから、相当程度のサイバーセキュリティの水準にある。しかし、商業ベンチャー企業が多数登場し、衛星を通じたネットワークの数とチャンネルが増えているため、全ての衛星が堅牢であるとは限らず、脆弱性を抱えたサービスも少なからずあると見られる。また、衛星は打ち上げてから、そのハードウェアを 10 年単位で運用するため、システムのアップデートをする仕組みを持っていなければ、リスクは大きくなる。実際、老朽化した衛星を運用しているオペレーターも少なからずあると見られている。

この問題は、サードパーティ（衛星を使ったサービスプロバイダ）との関係で問題になってくる。最終使用者にとって、どの衛星を使っているかが必ずしも明確でないことが多く、そのインフラとして脆弱な衛星ネットワークを使っている可能性が排除出来ない。また「サプライチェーン脆弱性」の問題もある。サプライチェーン脆弱性とは、サイバーセキュリティの水準の高いプロバイダであっても、そのプロバイダが使っているハードウェアのサプライチェーンの中にリスクのあるサプライヤーが存在し、そこにセキュリティホールを設定する場合があり得る。そのため、最終的なサービスを提供するプロバイダは、サイバーセキュリティに関して、サプライチェーンを点検し、そうした脆弱性を回避することが求められる。しかし、ハードウェアメーカー、ソフトウェア開発者、衛星メーカー、事業者、商用ユーザーの全てを管理することは極めて困難であり、誰にどのような責任があるのかということを明らかにすることは不

可能に近い。
さらに大きな問題は、衛星そのもののサイバーセキュリティがしっかりしていても、地上局におけるセキュリティが脆弱な場合、衛星がハッキングされ、乗っ取られることで、上述したような、衛星自身が武器として使われるリスクが存在している。
こうした問題に対して、衛星のサイバーセキュリティに関する多国間のセキュリティセンターを構築し、サイバーインシデントの前、中、後の情報共有を支援する明確なコミュニケーションラインを構築する必要がある。そのためには、政府、衛星メーカー、オペレータ、ソフトウェア開発者、サービス利用者の間の協力が必要である。各領域からの教訓や経験の共有も含め、それぞれが果たすべき役割を担っている。地上システムと宇宙システムがこれまで以上に密接に統合され、その区別が曖昧になるにつれ、従来はサイバー脅威管理の別々の分野とみなされていたものが、協力的かつ情報交換することが必要である。

5. 宇宙アセットを持たないウクライナの宇宙利用

ロシアのウクライナ侵攻で宇宙戦にならなかったもう一つの理由は、ウクライナが宇宙アセットを持っていなかったことによる。ロシアは当初、電撃戦によりキーウを強襲して陥落させることを目指していた。そのため、制空権を得るためにアントノフ空港を占拠し、ウクライナの防空システムを攻撃した（結果的には防空ミサイルや航空機を移動させていたことで攻撃は成功しなかった）が、その過程でウクライナの衛星も攻撃することは視野に入っていたと思われる。しかし、ウクライナは独自で保有する衛星システムを持っておらず、宇宙を基盤とするシステムに依存していなかった。そのため、宇宙戦は起こらなかったと言える。
しかし、自らの衛星システムを持たないウクライナは、アメリカをはじめとする西側諸国によって訓練を受け、アメリカの商用衛星などを使ったシステムの活用については十分知悉していたと思われる。ゆえに、ロシアのウクライナ侵攻が始まった当初あるいはその前から、衛星の重要性は理解しており、それゆえウクライナのフェドロフ情報大臣（副首相）が Starlink のオーナーであるイロン・マスクにツイッターでメッセージを送り、その 10 時間後に Starlink が使えるようになる、といった状況が生まれた。

5.1. Starlink

Starlink は 2022 年の 4-5 月に主たる戦場となったマリウポリ攻防戦の拠点となったアゾフスターリ製鉄所の包囲戦で重要な役割を果たした。ここではアゾフスターリ製鉄所の地下に潜んでいたウクライナ軍（アゾフ大隊）とキーウの司令部との間の通信を確保することで、戦況の把握や補給の連絡、またロシア軍の包囲状況などの情報を提供したと言われている。
また、外国首脳がキーウを訪問する際、鉄道を使ってウクライナ国内を移動するが、ウクライナ鉄道の通信ネットワークは基本的に Starlink によるものである。列車内の移動体通信サービスだけでなく、鉄道運行のための連絡調整やロシア軍の攻撃による破壊と、その修復に関する情報も Starlink を通じてやり取りされている。
戦場においては、ドローンに Starlink のターミナルを搭載することは不可能であるが、ドローンを操縦する端末を Starlink に接続することで、ドローンが撮影した画像などの情報を伝達し、敵の位置や「戦場の Uber」と言われる GIS Arta に必要な情報を提供している。GIS Arta とはスマホ入力やレーダーなどによる索敵情報を統合するシステムであり、そこで統合された情報を元にウクライナ軍の装備のうち、最も効率的に攻撃する方法を選択し、瞬時にそれを伝達するシステムである。戦場においてこうした指令を伝達するシステムとして Starlink は不可欠なものとなっている。
しかし、Starlink は民間企業であり、このような形で軍事利用されることでロシアからの攻撃を受けるリスクが高まることに対する懸念も生まれている。Starlink のオーナーであるイロン・マスクは 2022 年 10 月に、無限にウクライナを支援し続けることは出来ない、とコメントしてゼレンスキー政権を困らせることがあった。イロン・マスク自身、しばしばロシア寄りの発言をすることが知られており、ロシアからの圧力を受けていた可能性もある。また、2023 年 2 月には Starlink の社長であり、その親会社である SpaceX の COO であるグウェイン・ショットウェルは、Starlink が「武器化」されていることを懸念していると発言している。これは商業衛星

が軍事的に用いられることで、ロシアの攻撃対象となることを懸念したものと考えられる。

5.2 GPS

現代戦において、自らの位置と敵の位置を知ることは絶対不可欠の能力である。それを可能にするのは GPS である。GPS には一般向けの P-code と呼ばれる信号と軍が使用する M-code があるが、アメリカは同盟国に対しても M-code は公開しておらず、共同作戦を実施する際にのみ M-code を提供すると言われている。そのため、アメリカの支援を受けつつも、ウクライナ軍が M-code を使っていると言うことは考えにくい。ゆえに、ウクライナ軍は P-code を使っているものと想定される。

しかし、P-code の問題は、その周波数が一般に知られており、それ故にその信号に対してジャミングをかけることが可能であり、実際、ロシアはコンスタントに GPS のジャミングを行っているとの報告もある。電波情報収集を民間企業として行っている HawkEye360 はウクライナとロシアの国境地帯で GPS のジャミング信号が出されていることを確認している。

こうしたジャミングはロシアに限らず、様々な場面で用いられている。GPS の P-code 信号は脆弱性が高く、実際の戦闘においてはその有効性には限りがある。しかし、こうしたジャミングを受けているにもかかわらず、ウクライナは各戦線において一定の成果を挙げており、その点では GPS のジャミングも恒常的なものではなく、一時的な戦術的利用しか出来ないということが示唆される。M-code が常時使える状況でなければ P-code を活用するしかないが、一定の限界と脆弱性を抱えつつも、そのオプションは完全に否定されるべきではないだろう。

5.3.商業衛星画像

商業衛星画像は、1990 年代から一般に利用可能になり、近年では Planet Labs や Spire のように小型衛星をコンステレーションとして運用し、数時間ごとに世界のあらゆる地域の画像を更新することが可能なサービスも登場している。また、伝統的に商業的な衛星画像は光学センサーを使った、写真のような画像が主流であったが、光学センサーは夜は使えず、雲がかかっている時も使えないため、情報収集の手段としては限界があった。しかし、合成開口レーダー（SAR）を使った衛星画像は曇りでも夜間でも使えるため、偵察などに使われるが、こうした SAR 画像も商業的に入手出来るようになっている。2006 年に 11 基だった商業用地球観測衛星の数は、2022 年には 500 基を超え、そのうち約 350 基が米国企業によるものである。

実際、ウクライナへの大規模侵攻が始まる前から、軍事アナリストなども SAR を使ってロシア軍の動きを把握しており、2 月 24 日の前から侵攻が始まることを見ることが出来ていた。当然、ウクライナ軍もこうした動きは掴んでいたと思われる。また、こうした商業衛星の画像はメディアでも活用され、New York Times がブチャでの虐殺を衛星画像を使って証明したことはよく知られている。

ただ、SAR 衛星の画像は電波の跳ね返りを捉えて地上の物体を判別する画像であるため、その画像を分析する能力やソフトウェアの存在が重要となる。既にそうしたソフトウェアも商業的に入手可能ではあるが、それでも分析者には一定の訓練が必要となる。また、闇雲にあちこちの画像を取得するだけでは情報として不十分であり、どこを見れば良いのか、どこに敵の動きがあるのかということを知るためには、一定のインテリジェンスが必要となる。そうした能力を高めていくことも民間データを利用する際には重要となる。

また、日本でも衛星画像の海外移転に関しては、リモートセンシング法といった規制がかかっているが、米国の商業衛星が他国に衛星画像を提供する場合も、様々な規制がかかっている。しかし、米国政府はウクライナを支援する立場から、ウクライナ向けの画像提供については規制を緩和している。また、ロシアも衛星画像を活用していると言われているが、ソ連時代から偵察衛星の開発には後れを取っていたロシアも商業衛星画像に依存していると見られている。ただし、米国企業の画像にアクセスすることが出来ないため、ロシアは中国から商業衛星画像を購入していると見られている。

また、軍による商業衛星画像の利用だけでなく、メディアがこれらの画像にアクセス出来るようになったことが大きい。いわゆる公開情報インテリジェンス（Open Source Intelligence: OSINT）として、商業衛星の画像を活用することで、戦況の変化を逐一確認し、戦場で何が起こっているかを正確に検証することが出来るようになった。そして、こうした画像の持つ影響力

は大きく、世論形成にも大きな影響を与えていると言える。こうした紛争の可視化は戦争の行方を大きく変えることになるだけでなく、西側諸国によるウクライナ支援の流れを作ったものと見て良いだろう。

6. 商業衛星の軍事利用の問題点

ロシアのウクライナ侵攻は、史上初の「商業宇宙戦争」とも言えるような、商業衛星が前面に出る戦いとなっている。しかし、こうした新しい状況は、これまでにない問題を生み出している。

伝統的に宇宙システムを軍事的に利用する場合、その秘匿性や技術的特殊性から、政府や軍が保有する衛星を使ったものに限られていた。民間企業の運用する衛星は軍が保有する精密な画像を取得したり、秘匿通信が出来ないものであった。しかし、ウクライナ軍が示したことは、そうした特殊性がない場合でも、民間企業が提供する衛星の能力は軍のそれと大きく変わることはなく、十分に軍事的な作戦を遂行する上で有効なものであるということであった。

こうした軍事的有用性が証明されたとなると、本章の冒頭で論じたように、相手の軍事的能力を引き下げるために軍事衛星だけでなく、商業衛星の能力も奪い取る必要が出てくる。軍事衛星であればその所属が明確であり、軍事衛星への攻撃は国家に対する攻撃として認知されるため、抑止戦略が可能となる。しかし、民間衛星はしばしば所有者の国籍が複数にまたがっていたり、様々な国から出資されている場合もある。宇宙条約に基づく「打ち上げ国」の登録も便宜的に第三国でなされる場合があり、どの国家が民間企業の活動に責任を持つのかがはっきりしない場合もある。そのため、商業衛星に対する攻撃に対して、抑止戦略を採ることは容易ではない。しかも、今回ウクライナ軍が使っている衛星は主にアメリカの企業が提供する衛星サービスであり、ウクライナ軍の活動を制限することを目的にアメリカの衛星を攻撃する可能性もある。まさに Starlink の社長であるショットウェルが懸念した通りの問題が起きうる可能性が出てきたのである。

では、誰が商業衛星を防護し、どのような形で抑止をすることが可能なのであろうか。まさにこの問題が現在、アメリカの国家宇宙評議会（議長はハリス副大統領）を中心に議論されている。この議論の答えはまだ出ていないが、一つの可能性として考えられるのは、民間企業の活動であっても、アメリカが防護するとコミットするサービスについては、アメリカが「打ち上げ国」であることを宣言し、その民間企業に対する攻撃はアメリカに対する攻撃であると宣言することである。そうすることで、民間企業にも軍事衛星と同様の位置づけを与え、抑止戦略を展開すると言うことである。これが国家宇宙評議会の結論になるかどうかは不明だが、商業衛星をどのようにして守るのか、ということは今後も大きな問題として議論が続くであろう。

7. ウクライナ侵攻からの教訓

最後に、本章で論じたロシアのウクライナ侵攻から得られる教訓をまとめてみたい。

7.1. サイバー攻撃への対抗

戦時において宇宙システムが使われることは自明という状況である。物理的な ASAT による攻撃は、抑止戦略によって止めることが出来る可能性はあるが、明確な攻撃の意図や形跡が残りにくいサイバー攻撃に対する防護は抑止戦略でも実現することはない。

となれば、サイバー攻撃に対する対抗は、第一に衛星だけでなく、地上局も含めたサイバーセキュリティを高めていくことである。これは既存のオペレーターでは実施されていることではあるが、新たに商業的サービスを展開する宇宙ベンチャー企業では必ずしも実施されているとは限らない。ゆえに、政府は戦時におけるサイバー攻撃を想定して、これらのベンチャー企業にもサイバー防衛を義務づけること、また必要であれば、サイバーセキュリティの専門家を育成するプログラムを展開し、サイバー攻撃に対抗できるような能力を構築していくことである。

7.2. GPSに対する妨害電波への対抗

戦場において、GPS ほど重要な情報を提供してくれる信号はない。しかし、GPS 信号は中軌道（MEO）の衛星から発せられているため、相対的に弱い信号であり、簡単にジャミングなどで妨害される恐れがある。そのため、GPS に対するジャミングに対抗する手段を持たなければならない。既に述べたようにGPSへの攻撃は恒常的に行われるものではないが、それでも重要な局面で使われることは想像に難くない。

GPS への対抗手段の一つは、周波数ホッピングなどを使い、ジャミングに対抗する M-code の信号を使うことである。ウクライナの場合は同盟国ではないため、M-code を使う可能性は低かったが、日本の場合、アメリカの同盟国として M-code が使える可能性はある。しかし、それはアメリカの判断によるものであり、常に使えるとは限らない。そのため、代替手段として考えられるのが、準天頂衛星に搭載されている公共信号を使うと言うことであろう。この点についてはまだ未確定のことが多いが、日本独自の測位衛星システムがある以上、これを活用することは十分に可能性がある。

また、GPS ジャミングに対抗するような受信機能の強化ということも一つの方法として考えるべきであろう。さらには、GPS のジャミング信号を出す機器に対して、その機能を奪うということも一つの方法である。物理的に攻撃することは、敵の主権の及ぶ範囲にある場合、なかなか難しいと思われるが、電磁波によってそうした機器に対して攻撃をかけることは可能であろう。今後GPSジャミングに対抗する手段としての電子戦の能力を向上させることが重要な問題と考えられる。

7.3. 独自のコンステレーションか商業サービスの利用か

本章で紹介したStarlinkやPlanet Labsは小型衛星を多数打ち上げ、それらを同期させて、一つの機能を獲得するものである。これらの小型衛星コンステレーションは民間企業で培われたものであり、政府はこうした技術を十分に習得しているわけではない。アメリカでも軍が極超音速滑空ミサイルを探知・追尾するために小型衛星のコンステレーションを構築しようとしているが、米国防総省も独自で開発するのではなく、民間の商業衛星オペレーターに発注してシステムを構築する方針を打ち出している。

他方、日本では国家安全保障戦略や国家防衛戦略の中でコンステレーションの構築が明記されているが、それを誰が構築するのかという点については書かれていない。アメリカと異なり、日本には小型衛星のコンステレーションによって衛星サービスをはじめようとするベンチャー企業がないわけではないが、まだ十分に成功するとは言えない状況にある。その中で、日本がコンステレーションを構築する際、政府が独自で開発するのか、民間の商業サービスを利用するのか、という問題が残る。

小型衛星コンステレーションは一つの機能を多数の衛星で実行するため、一つの衛星を破壊したり、無効化したとしても、他の衛星で機能をカバーすることが出来る。その意味では、小型衛星コンステレーションは敵の攻撃に対して攻撃されるリスクを分散するという効果を持っている。その意味でも、小型衛星コンステレーションを積極的に活用していくべきである。しかし、本論でも述べたように、商業衛星を軍事的活動に利用するとなると、その衛星をどう防護するのか、という問題が出てくる。それ故、日本では小型衛星コンステレーションの構築能力は政府ないし防衛省が持つべきであり、そうした技術開発を進めることによって民間企業にもスピルオーバーすることを期待することが出来る。日本の宇宙産業の競争力強化という観点からも、政府が独自のコンステレーションを構築することが望ましい。

7.4. 衛星画像取得にかかる能力

戦争において民間企業であれ、軍や政府の衛星であれ、宇宙から画像を取得することは極めて重要である。日本はこれまで内閣官房の衛星情報センターが情報収集衛星を運用して衛星画像を取得してきたが、これは防衛省や自衛隊に直結した画像ではないため、安全保障上の目的で十分に活用できるかどうかには疑義が残る。

日本では国家安全保障戦略、国家防衛戦略、防衛力整備計画でスタンドオフミサイル能力の構築のために、標的を発見し追跡する手段として衛星画像の取得が論じられている。その意味

でも、これまで防衛省・自衛隊が持たなかった画像取得能力を持つべきである。しかも、その主たる目的がスタンドオフミサイルの運用ということであれば、小型衛星コンステレーションによる撮像頻度が高いシステムにする必要があるだろう。

まとめ

安心・安全の観点からの宇宙利用を考えるに際して、ロシアのウクライナ侵攻から得られる教訓は多い。この侵攻における宇宙利用は今後も様々な形で広がって行くであろうが、防衛省・自衛隊はこれまで衛星の運用の実績がないだけに、世界が宇宙を利用した安全保障戦略を描き、それを実際の活動に応用していることを考えると、日本が出遅れているという感覚は否めない。それだけに、ここから得られる教訓に基づいて、どのような衛星を使った能力を、どのようなプライオリティとスピード感で構築していくのか、を早急に検討する必要があるだろう。