第 7 章　ロシアの GPS スプーフィング能力

小泉　悠

はじめに

本稿では、衛星 PNT システムに対する妨害能力を中心に、ロシアの宇宙作戦能力について考察する。

まずは議論の前提として、衛星 PNT システムとは何かについて簡単に定義しておく必要があろう。PNT とは、測位（Positioning）、航法（Navigation）、計時（Timing）の頭文字を取ったものであり、人工衛星を用いてこうした機能を提供するシステムとしては、米国の GPS（グローバル測位システム）がすぐに思い浮かぶ。この他にも、ロシアの GLONASS（グローバル航法システム）、EU（欧州連合）のガリレオ、中国の北斗といった GNSS（グローバル航法衛星システム）はいずれも PNT 機能を備える。カバー範囲を特定の地域に限る日本の QZSS（準天頂衛星システム）やインドの IRNSS（インド地域航法衛星システム）も同様である。

これらの衛星 PNT 機能が現代の社会生活に不可欠であることは、改めて述べるまでもあるまい。自動車やスマートフォンのナビゲーション機能といった身近な用途に始まり、大規模な経済活動や科学研究に至るまで、その応用範囲は極めて広い。

軍事面においても、衛星 PNT 機能は幅広く利用されるようになっており、軍事作戦のあり方を大きく変えている。冷戦期の軍事宇宙利用は、戦略偵察（大規模な軍事的動向や軍縮条約の履行状況などを観察する）や核兵器に対する指揮通信統制、敵弾道ミサイルに対する早期警戒などを主用途としており、要するに米ソの相互核抑止を支える基盤であった。それゆえに、宇宙空間は戦場から切り離された一種の「聖域」としておこうという考え方が冷戦期の米国では主流を占めていたが、近年では状況が大きく変わりつつある[1]。

1990 年代に米空軍が GPS を実用化したことはその顕著な画期であった。部隊・艦船・航空機が自らの位置を正確に把握してリアルタイムで共有したり、爆弾やミサイルを精密に目標へ指向させたりといった現代戦の基本的なスタイルは、もはや衛星 PNT 機能を抜きにして成立しない[2]。指揮通信、兵站、生物・化学・放射能防護といった地味な分野でも衛星 PNT 機能は大いに活用されている。宇宙空間を利用して大気圏内の軍事作戦を支援する能力を、米軍は「戦力強化（force enhancement）」と呼ぶが[3]、衛星 PNT システムはまさにこうした戦力強化の中核を成すものと言える。

裏を返すならば、衛星 PNT 機能が停止や誤作動に陥った場合、これに依存する社会活動や軍事作戦は大きな混乱を被ることが予想されよう。例えば衛星が故障・破損するといった事態はこれに該当しようし、それを人為的に引き起こそうとするのがいわゆる対衛星（ASAT）兵器である。他方、衛星自体が健全であっても PNT が機能不全に陥る可能性も想定できる。マルティンとバスティデによれば、衛星 PNT の持つこうした脆弱性は次の 4 つに分類することができる[4]。

- システム脆弱性（System vulnerabilities）
- 伝搬脆弱性（Propagation vulnerabilities）
- 偶発的脆弱性（Accidental vulnerabilities）

・ 意図的脆弱性（Deliberate vulnerabilities）

このうち、上から三番目までは、一種の不可抗力として、意図せずして発生する脆弱性と位置付けられよう。例えばシステム脆弱性は衛星が発信できる電波の出力[5]など物理的能力に由来するものであり、伝搬脆弱性はそのようにして発信された電波の伝搬環境（大気の状態等）に起因する。偶発的脆弱性はこれ以外の、予期し得ない事態によってもたらされた脆弱性をいう。

これに対して意図的脆弱性は、国家等の主体が明確な意図を持って作り出すものである。例えば人為的に衛星の電波を妨害（ジャミング）したり、偽の電波とすり替える（スプーフィング）といった方法であるが、この種の妨害・欺瞞能力は物理的に敵衛星を破壊する ASAT にない軍事的利点を有しており（後述）、それゆえに今後も対宇宙作戦能力の一つの柱になっていく可能性が高い。

ロシアはこの分野で実際に高い能力を持つとされ、中でも GPS をはじめとする衛星 PNT システムに対しては実際に度々妨害・欺瞞を実施してきたことが知られている。したがって、その実態を詳しく検証することは、ロシアの軍事戦略と今後の宇宙安全保障のあり方を考える上での一つの指針となろう。

1. ロシアの宇宙作戦能力概観

(1) 宇宙作戦組織と対衛星攻撃能力

ロシア軍において対宇宙作戦を担当するのは、軍種の一つである航空宇宙軍（VKS）である。より詳しく述べるならば、VKS は空軍（VVS）、防空・ミサイル防衛部隊（Voiska PVO-PRO）、宇宙部隊（KV）の 3 兵科部隊から構成されており、概ね次のように役割を分担している。

・ VVS：軍管区レベルでの防空及び戦術・戦域ミサイル防衛（S-300 シリーズ、S-400）
・ 防空・ミサイル防衛部隊：モスクワ周辺の防空（S-400）及び戦略ミサイル防衛（A-135 アムール）
・ KV：軍事衛星（攻撃衛星を含む）の打ち上げ・運用や弾道ミサイル警戒・宇宙状況監視（SSA）

このうち、防空・ミサイル防衛部隊の A-135 アムールは今後、A-235 ヌードリにアップグレードされて ASAT ミサイルを運用可能になるとされるほか[6]、開発中の次期防空システム S-500 も ASAT 能力を有すると見られる[7]。また、KV が運用する弾道ミサイル早期警戒レーダー網（近年配備が進むヴォロネジ・シリーズ等）や、アクノー光学衛星監視システム、レーザー衛星監視システムであるクローナ等は外国の軍事衛星を観測・追尾してカタログ化することで SSA 能力を提供する[8]。また、VKS は近年、MiG-31 戦闘機に搭載される ASAT ミサイル[9]やペレスウェート地上配備型対衛星レーザー妨害システムの開発を進めていると見られ、多様な ASAT 能力の保有を目指していることが伺えよう。ここでは詳細には立ち入らないが、米国や中国が保有ないし保有しつつある ASAT 能力と比較しても、ロシアのそれは規模・能力ともに格段に手厚い。

(2) 宇宙空間におけるロシアの劣勢

しかし、ロシアの高い ASAT/SSA 能力は、同国の宇宙作戦能力の高さを必ずしも意味するものではない。

世界初の人工衛星打ち上げと有人宇宙飛行を実現したソ連とその後継国家ロシアは、長らく宇宙開発のフロントランナーとされてきた。しかし、表 -1 に示すように、今やロシアが持つ宇宙能力は国際的に珍しいものではなくなっており、米国のスペース X 社のような再使用型打ち上げシステムも実現できていない。また、表 -2 からは、数の上でもロシアは世界第一級の宇宙大国とは呼べなくなりつつあることが窺われよう。独自の有人宇宙飛行能力を持つ点や、GNSS である GLONASS を保有している点など依然としてロシアは高い宇宙能力を持つが、その相対的地位は明らかに低下している。ロシアの経済力や科学技術力を考えるとき、こうした状況が予見しうる将来において変化することも考えにくい。

表 -1 主要国の宇宙能力

宇宙能力	米国	中国	ロシア	インド	EU	日本
有人宇宙飛行	○	○	○	（開発中）	-	-
静止衛星への打ち上げ能力	○	○	○	○	○	○
国際宇宙ステーションへの物資補給	○	○	○	-	○	○
再使用型打ち上げ手段	○	（開発中）	-	-	-	-
衛星 PNT システム	○	○	○	○	○	○
情報・監視・偵察・リモートセンシング	○	○	○	○	○	○
衛星通信	○	○	○	○	○	○

（出典）筆者作成

表 -2 主要国の衛星保有数

種別	世界全体	米国	中国	ロシア	その他
情報・監視・偵察・リモートセンシング衛星	・38 カ国 ・666 機	353 機	122 機	23 機	168 機
通信衛星	・45 カ国 ・790 機	391 機	38 機	81 機	280 機
PNT 衛星	・6 カ国 ・121 機	31 機	28 機	28 機	34 機
科学技術衛星	・38 カ国 ・303 機	94 機	62 機	11 機	136 機

（出典）The National Air and Space Center, *Competing in Space*, December 2018, p. 5. <https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF>

軍事的に見れば、宇宙を用いた作戦能力においてロシアは今後とも米国等に対して劣勢

であり続ける可能性が高いことを以上の状況は示唆している。他方、宇宙作戦能力が現代の軍事作戦において必須であることはすでに指摘した通りであり、この点はロシアにおいても変化はない。2015年に開始されたシリア作戦において、ロシアは偵察画像のリアルタイム伝送が可能なペルソナ偵察衛星を初めて実戦投入したほか、通信衛星やGLONASSを用いて地上部隊や航空部隊を支援する「戦力強化」を大々的に実施した。しかし、諸外国と同様にロシア軍が宇宙に依存しながら作戦を展開する場合（このこと自体は今後も不可避であろう）、宇宙戦力で劣勢のロシアは、大気圏内でも常に劣勢に立たされることが予想される。

2. 宇宙作戦に関するロシアの考え方

(1) 宇宙版「非対称措置」

このような状況にロシアがどのように対処しようとしているのかについて、「ロシア連邦軍事ドクトリン」をはじめとする公式政策文書は何も述べていない。他方、ロシア軍参謀本部アカデミーの紀要である『軍事思想』に掲載された論文「現代的条件下における宇宙優勢確保のためのアプローチ」[10]は、この点について一定の示唆を与えるように思われるので大要を紹介したい。

同論文はまず、「宇宙優勢」を「一方の軍事衛星が他方のそれに対して決定的な優位」を有する状態と定義し、このような環境下では「人工衛星に対する敵の妨害を受けることなく課題を解決することが可能となる」と述べる。だが、この定義に拠るならば現状で宇宙優勢を確保しているのは米国やその同盟国などの「西側」であり、ロシアが「宇宙劣勢」に置かれていることは上述の通りである。

そこで同論文は、自力で宇宙優勢を達成できないならば敵の水準を引き下げてやればよいというテーゼを掲げる。具体的な考え方は次のようなものだ。まず、敵は宇宙空間をどのような目的（偵察、通信等）で利用しようとしているのか、そのためにどのような種類の衛星をどのくらい軌道上に配備しているのかを分析するのがスタートである。前述のように、VKSは各種のSSA能力を有しており、この面ではロシアの能力は比較的高い。

こうして基礎的なデータが揃ったら、軌道上の衛星が何機以下になると所期の機能が発揮できなくなるのかを分析し、この水準まで敵の衛星数を減少させる手段についても検討する。その上で、ロシア側の攻撃手段とターゲットである外国衛星をモデル化してコンピュータ上で仮想戦闘を行い、実際に敵の衛星数が必要数を割り込むかどうかをシミュレーションしてみる。この結果、生き残った（あるいは機能を維持している）衛星の数が敵の宇宙利用を支えきれる最低数を割り込めば、ロシアの戦略は成功ということになる。

歴史的に経済力や科学技術力で優勢な相手に対抗することを常に余儀なくされてきたロシアは、より低コストかつローテクな方法に依拠することで均衡を維持する戦略を発達させてきた。米国の弾道ミサイル迎撃システム計画である「戦略防衛構想（SDI）」に対し、ソ連側が弾道ミサイルの多弾頭化や囮システムの搭載といった「非対称措置（асимметричные меры）」で対抗しようとしたことはその一例である。同様の考え方は冷戦後に米国が進めてきたグローバルミサイル防衛構想に際しても見られた[11]。米国の宇宙優勢を「引き下げる」という考え方は、こうしたアプローチを宇宙作戦に応用したものと理

解することができよう。

(2) 破壊的 ASAT と非破壊的 ASAT

では、敵の宇宙優勢を「引き下げる」方法とは、具体的にいかなるものであろうか。最も単純な方法は、敵の人工衛星を物理的に破壊することであり、ソ連はこうした能力を実用化した最初の国である[12]。また、現在においてもロシアが多様な対衛星攻撃能力を開発・保有していることについては少し前に触れた。

ただし、人工衛星の破壊は大量のデブリ（宇宙ゴミ）を生じさせる。ロシアは近年、ASAT 実験を行なっていないが、2007 年に中国が行なった ASAT 実験の場合は観測可能な分だけでも 3000 個、観測不能分も合わせると 3 万 2000 個以上とも言われる史上最多のデブリを発生させ、2010 年時点でもその 97% が軌道上に留まっていた[13]。2019 年にインドが実施した ASAT 実験では、デブリの大部分が大気圏に突入して消滅したが、それでも一部のデブリは軌道上に残留し、一部は高度 2200km 以上に到達してさらに長期間残留する見通しである[14]。

以上のような特性を考えるならば、ASAT 兵器による物理的な衛星破壊は宇宙利用環境を不可避的に悪化させ、ロシア自身による宇宙利用をも制約しかねないということになろう。大規模な国家間戦争時にはこのような宇宙作戦も許容されようが、冷戦後のロシアが主として念頭に置いているのは、旧ソ連諸国への軍事介入や、シリア紛争のような地域紛争における「限定行動戦略」である。こうした限定戦争においては、交戦相手は独自の宇宙アセットを持たないが限定的にしか保有していないのが普通であって、彼らは GPS やガリレオといった西側の衛星 PNT システムのユーザーに過ぎない。また、後述するように、ロシアは平時における重要政府施設や要人保護のためにも GPS 妨害を実施していると考えられるが、そのためにいちいち外国の衛星を破壊するのは全く論外であろう。

後先を考える必要のない大規模戦争時（「ロシア連邦軍事ドクトリン」が述べる通り、このような戦争の蓋然性は現在ではさほど高くない）を除けば、GPS をはじめとする西側の衛星システムを破壊することなく、その機能だけを妨害する手段が必要であるということになる。実際、ロシアはこうした手法をすでに一部実用化していると考えられ、多くの報告や研究結果も見られるようになってきたので、次節ではこの点について詳しく紹介してみたい。

3. ロシアによる衛星 PNT システム妨害

(1) 妨害手法

ひとくちに妨害といってもその形態は様々であるが、大きく分けてジャミング（電波妨害）とスプーフィング（なりすまし）の 2 種類を指摘することができる。ジャミングとは文字通り、妨害電波によって衛星 PNT システムの機能を阻害するものであり、スプーフィングは正常な信号を装った偽電波によって衛星 PNT システムの機能を混乱させる欺瞞手段を意味している。米国のシンクタンクである C4ADS はこれをさらに細かく定義し、次の 3 種類に分類した[15]。

・ ジャミング

衛星 PNT システムが用いる周波数に合わせて攻撃側がノイズ状の電波を発信し、受信機が信号を受信できないようにする方法。

・ サービス拒否型スプーフィング
攻撃側が衛星 PNT システムを装った偽の電波を発信したり、情報の含まれていない「空白」の電波を発信する方法。多くの場合、被攻撃側は妨害を受けていることに気づくことができる。「スマート・ジャミング」と呼ばれることもある。

・ 欺瞞的スプーフィング
攻撃側が衛星 PNT システムを装った偽の電波を発信することはサービス拒否型スプーフィングと同様であるが、欺瞞的スプーフィングでは被攻撃側は攻撃の事実に気づかずに誤った方向へ誘導される

(2) ジャミングの事例

以上のうち、最初に実戦使用が確認されたのは GPS に対するジャミングである。2003 年のイラク戦争において、イラクがロシア製の GPS ジャミング用電波妨害装置 6 基を投入し、米国の航空作戦を妨害しようと試みたとされる事例がこれに当たる[16]。もっとも、このシステムは、大出力の電波によって広域を妨害するというものであったために発信源が早々に特定され、空爆で破壊された。皮肉なことに、米軍はこれらの GPS ジャミング装置を破壊するのに GPS 誘導爆弾を使用したという。

ただし、その後もロシアは敵の衛星から発せられる電波を妨害するシステムを開発・配備しており、一部はクラスーハ -2 及びクラスーハ -4 としてロシア軍に制式採用されている（後述するように、前者はシリアでも実戦投入されていると見られる）。また、2017 年には防空システム・メーカーであるアルマーズ・アンテイ社が、さらなる新型システムの開発を受注したことが明らかになった[17]。

(3) 民生機器に対するスプーフィングの事例

2016 年以降、ロシア及びその周辺地域ではサービス拒否型スプーフィングの事例が相次いで報告されるようになった。その発端は、モスクワのクレムリン宮殿周辺においてタクシーアプリや「ポケモン GO」などのゲームアプリの位置表示が狂うという苦情が相次いだことである。ロシアの有力紙『ヴェドモスチ』によると、これは国家保安委員会（KGB）の要人・重要施設警護部門を引き継いだ連邦警護庁（FSO）によるスプーフィングであり、シポヴニク・アエロと呼ばれる移動式スプーフィング装置がクレムリン内の様々な場所から欺瞞電波を発信していると見られる[18]。2017 年以降には、黒海周辺やイスラエルの空港でも GPS の位置情報が狂う現象が報告されており、いずれもロシアによるスプーフィングが強く疑われている[19]。

以上のように、個別の GPS スプーフィングについてはすでに多くの報告が存在しているが、前述の C4ADS が米テキサス大学オースティン校と実施した大規模調査[20]は、その全容を統計的に把握したものとして興味深い。これは民生用 GPS への妨害を対象として、公開情報、衛星画像、自動船舶識別装置（AIS）のデータ、国際宇宙ステーション（ISS）に搭載された GPS 受信機のデータ等を総合したもので、その結果、ロシアの GPS スプーフィングは上記の地域に加えて地中海（シリア周辺）、バルト海（サンクトペテルブルグ周辺）

や極東（ウラジオストク周辺）でも実施されていることが明らかになった。また、2016 年から 2018 年までの期間における民間船舶への GPS スプーフィング事例は合計 9883 回にも及び、1331 隻が何からの影響を被ったとされている。ロシア周辺地域で広範な GPS スプーフィングが実施されていることが窺われよう。

これらの事例に共通しているのは、GPS 受信機の示す自己位置が空港に変更されてしまうという点である。モスクワの場合はクレムリン周辺に居ながら郊外のヴヌコヴォ空港やドモジェドヴォ空港が表示されてしまうことが早い段階から報告されており、C4ADS の調査によると、黒海上の船舶でも GPS 受信機はやはりモスクワ周辺の空港を示していた。その理由は定かでないが、C4ADS や前述の『ヴェドモスチ』は、ドローン対策を挙げている。多くのドローンは航空機の運航を妨害しないよう、空港付近に差し掛かると自動着陸したり、発進地点に引き返すように飛行制御プログラムが設定されており、したがって任意の地点を空港であるかのように誤認させることでドローンの侵入を防ぐことができるというものである。

ロシアでは 2016 年、メドヴェージェフ首相らの豪華な別荘やブドウ園上空にドローンが侵入し、反体制派がその映像をインターネット上で公開するなどして大きな反響を呼んだ。あるいはヴェネズエラではマドゥロ大統領の演説中に自爆ドローンが侵入し、同人の暗殺を図るという事案が発生している。GPS スプーフィンがクレムリンやノヴォ･オガリョヴォ、黒海周辺（沿岸の措置にはプーチン大統領の別荘がある）で実施されているのは、こうした事態を阻止するための保安措置である可能性が高い [21]。

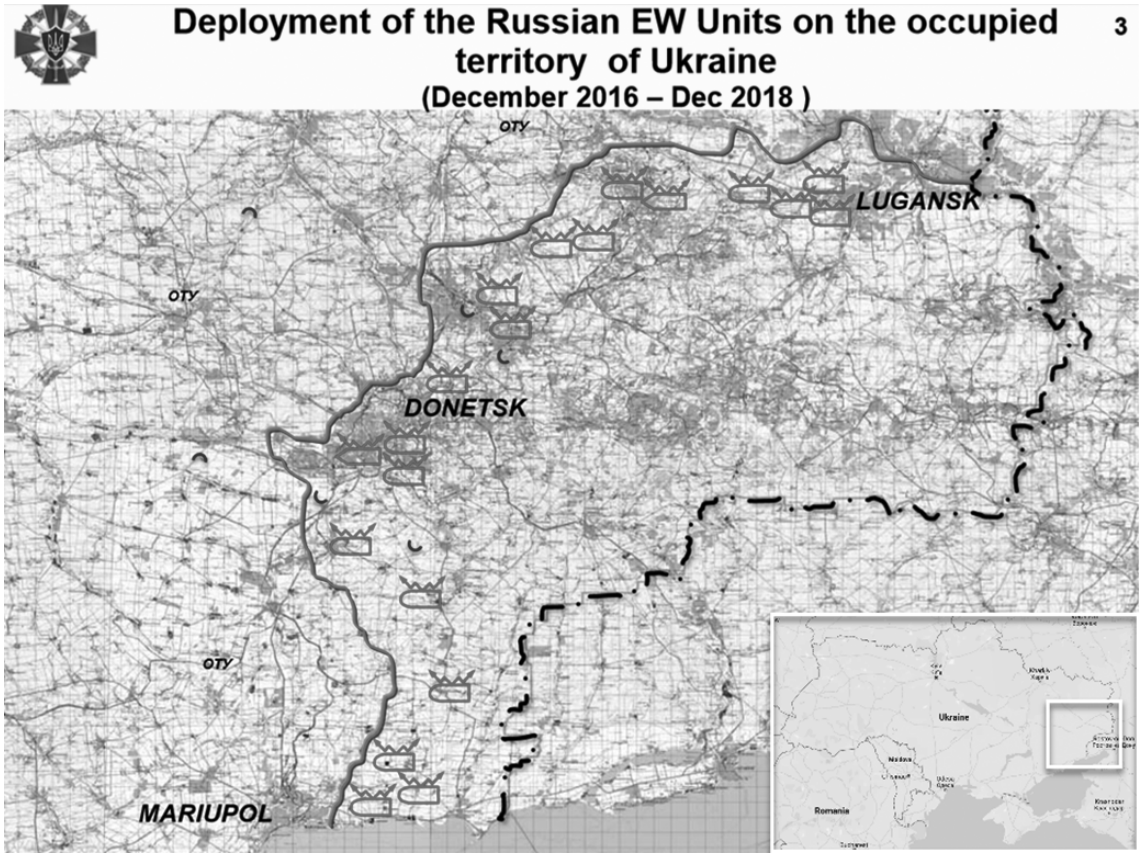
(4) 軍事活動に関連したスプーフィングの事例

ロシアによる GPS スプーフィングは、大規模な軍事的活動に付随しても報告されているので、以下、その代表的な事例を幾つか紹介したい。なお、これらの事例については、実施主体は前述の FSO ではなく、国防省電子戦総局所属の電子戦部隊であると考えられる。

最初の事例はウクライナ紛争である。ロシアは、現在も戦闘が続くドンバス地方に GPS スプーフィング能力を有する R-330Zh ジーチェリ電子戦システムを度々展開させてウクライナ軍や OSCE（欧州安保協力機構）のドローンを妨害してきたことが報じられている他 [22]、ウクライナ軍の評価ではクレムリン周辺でのスプーフィングに用いられているのと同じシポヴニク・アエロも投入されていると見られる [23]。図 -1 はウクライナ軍が作成したロシア軍の電子戦システムの推定展開位置であり、戦線全域に渡って幅広くロシアが電子戦を展開していることが読み取れる。

第 2 に、シリア紛争での事例が挙げられる。2015 年にシリア紛争に介入したロシアは、シリア西部のラタキア県にあるフメイミム飛行場を主要拠点としており、ここにジーチェリやシポヴニクのほか、偵察衛星や通信衛星の電波を妨害する能力を持ったクラスーハ -4 等の強力な電子戦システムを展開させている。C4ADS は ISS に搭載された GPS 受信機を用いてフメイミム飛行場から GPS スプーフィング電波が発信されていることを確認している他、シリアで活動する米軍の無人偵察機が継続的に GPS スプーフィングによる妨害を受けていると報じられていること [24] などを考え合わせると、ロシアがシリアで GPS スプーフィングを実施している可能性は高いと考えられよう。また、2018 年 1 月にフメイミム基地がシリア反体制のドローン 10 機による攻撃を受けた際には、ロシア軍の電子戦部隊が一部の

図 -1 ドンバス紛争におけるロシア軍電子戦システムの展開



（出典）Major General Borys Kremenetskyi, *op. cit.*

ドローンのコントロールを乗っ取って強制着陸させたと報じられている [25]。

第 3 に、ロシアは北極圏でも GPS スプーフィングを実施していると見られる。ウクライナやシリアの場合とは異なり、ロシアは北極圏で軍事紛争に関与しているわけではないが、同地域で大規模な軍事作戦が実施された際に GPS スプーフィング事案が発生することが多い。2019 年 4 月に米国の戦略国際問題研究所（CSIS）がまとめたところによると、主な事例は以下の 3 件である [26]。なお、以下の事例ではいずれも GPS 信号が「消失」したとされており、ジャミングがスプーフィングであるかは判然としない。ただし、CSIS の報告書はこれらの事例をいずれもスプーフィングと位置付けている。

・「ザーパド 2017」演習（2017 年 9 月）
　ロシア軍西部軍管区が 2017 年 9 月に実施した大規模演習「ザーパド（西方）2017」の期間中、ノルウェーの民間航空機パイロットが同国上空で GPS 信号を受信できなくなったことを報告しており、ノルウェー政府の調査の結果、ロシアから妨害電波が発信されている可能性が高いと結論づけられた。
・「トライデント・ジャンクチャー」演習（2018 年 10 月から 11 月）
　「トライデント・ジャンクチャー」は冷戦後に西側諸国が北極圏で実施した最大規模の軍事演習であり、NATO の全 29 カ国とフィンランド及びスウェーデンが参加した。この演習の期間中、ノルウェーの民間航空機や空港施設が GPS 信号を受信できない事

例が複数報告された。フィンランドでも民間航空機の運航が妨害を受け、同国政府がロシア政府によるものとして抗議した[27]。

・「クロックウォーク」演習（2019 年 1 月から 2 月）
英国軍が北極圏で実施した「クロックウォーク」演習の期間中、ノルウェーのロシア国境で操業していた建設会社が GPS 信号を受信できなくなり、業務に支障をきたした。

おわりに

以上をまとめるならば、衛星 PNT システムに対するロシアの妨害は次のように整理することができよう。

その第一は「平時の保安措置」であり、クレムリン、大統領公邸、大統領の出張先等において FSO が実施するドローン対策用スプーフィングが該当する。

第二に、「西側を直接の交戦相手としない軍事活動の支援」が挙げられる。これに該当するのはウクライナやシリアでの限定戦争や軍事演習等であり、いずれも西側諸国との直接交戦を回避しつつその衛星 PNT 機能を妨害することに主眼が置かれる。ただし、これらの事例でターゲットとなるのは軍事組織であり、それゆえにロシアのスプーフィングがどの程度の効果を挙げたのかは多くの場合、公表されない。

第三は「大規模戦争勃発時における宇宙優勢の獲得手段」であり、前述した『軍事思想』の論文が想定するのはこうした事態であろう。ただし、大国が互いの軍事衛星を破壊し合うという状況は幸いにして現在まで生起していない。

いずれにしても、GPS スプーフィングは平時や限定戦争下でも宇宙劣勢を補いうる妨害手法であり、それゆえに多用される傾向にある。また、ロシアや中国は高出力レーザー等を用いて衛星のセンサー部分やアンテナ部分のみを破壊する能力を追求していると言われるが、こうした限定的な破壊のみを伴う攻撃は、実行主体の特定の困難さゆえに在来型の ASAT 兵器に比べて使用の敷居が低くなる可能性が考えられよう。

現行の「ロシア連邦軍事ドクトリン」は、「ロシア連邦に対する大規模戦争が行われる蓋然性は低下したにもかかわらず、ロシア連邦に対する軍事的危険は増加している」という、一見矛盾した情勢認識を示している。しかし、本稿で見たような、大規模戦争に至らない範囲において行われる軍事活動の性質とこれを可能にする技術の進展を顧みる時、これはさほど奇異な認識とは言えないだろう。

破滅的な戦争を引き起こさないために大国間で戦略的な相互抑止が成立すると、多少の軍事的危機が発生しても簡単には全面戦争にエスカレートしないと考えられ、結果的に低強度紛争が発生しやすくなるという「安定・不安定パラドックス」は冷戦期から指摘されてきた。ウクライナ危機に際してロシアが用いた介入戦略はこのようなパラドックスを意図的に利用したものであることはすでに指摘されているが、スプーフィングに代表される衛星妨害も同様に理解できるのではないか。したがって、西側に対して一定の抑止力を有する（と考える）アクターはロシアと同様の対宇宙作戦能力を追求する可能性があるし、実際に中国、イラン、北朝鮮等はすでに各種の GPS 妨害能力を保有していると見られている[28]。

一方、米国はこのような「競合的環境」下においても宇宙優勢を確保し、PNT をはじめとする宇宙能力を維持する方法について検討を重ねてきた。それが 2011 年の「国家安全保

障宇宙戦略（NSSS）」に盛り込まれた「多層的抑止」の概念であり、①宇宙空間における行動の規範作り、②宇宙空間における責任ある国家連合の形成、③攻撃元を特定する能力及び攻撃による利益を失わせる能力の向上、④自衛のための反撃能力の保持から成っている[29]。

ただ、こうした抑止は大規模な衛星攻撃に対しては一定の効果を発揮するにせよ、GPS スプーフィングのような低コストかつ低強度の対宇宙作戦を抑止するには大掛かりかつ高コストすぎるように思われる。少なくともロシアの GPS スプーフィングは「多層的抑止」概念の出現からかなり時間を経てから出現したものであり、現実にその効果を発揮しているとは言い難い。

こうした低強度かつ非破壊的な衛星攻撃を抑止する方法は見いだせるのか、あるいは宇宙に依存しない PNT システムを実用化することができるのかは、今後の対露軍事戦略と宇宙安全保障全体の双方を考える上で焦点となろう。

―注―

1 米国における軍事宇宙利用の位置付けについては以下に詳しい。福島康仁「宇宙空間の軍事的価値をめぐる議論の潮流――米国のスペース・パワー論を手掛かりとして――」『防衛研究所紀要』第 15 巻第 2 号、2013 年 2 月、49-64 頁。

2 例えば米軍のアフガニスタン空爆では、全使用弾薬の約 3 割が GPS による誘導を受けていた。村野将「技術が変える宇宙の軍事利用」『「技術」が変える戦争と平和』芙蓉書房出版、2018 年、18 頁。

3 U.S. Joint Chiefs of Staff, *Space Operations*, 2013.5.29.

4 Jean-Christophe Martin and Frederic Bastide, “Positioning, Navigation and Timing for Security and Defense,” Kai-Uwe Schrogl, Peter L. Hays, Jana Robinson, Denis Moura and Christina Giannopapa eds., *Handbook of Space Security*, Vol.2, Springer, 2015, pp. 621-624.

5 GPS の場合、システムを構成する NAVSTAR 衛星は地球上 2 万 3000km 程度の中軌道（MEO）を周回しており、発信される電波の出力は 50W ほど、地表の受信機に到達する頃には 10^{-16}W まで減衰してしまう。このため、外的な擾乱に対して非常に脆弱となる。*Ibid*, p.621.

6 “Эксперт раскрыл подробности испытания ракеты для комплекса ПРО «Нудоль»,” *Федеральное агентство новостей*, 2019.6.4.

7 “Достанет и в космосе: Уникальная система ПВО может сбивать спутники на низкой орбите” *Российская газета*, 2019.4.25.

8 詳しくは以下の拙稿を参照されたい。「『ハード・キル』と『ソフト・キル』: 米国の宇宙優勢に対抗するロシアの「非対称措置」」『軍事研究』第 51 巻第 2 号、2016 年 2 月、208-221 頁。

9 Amanda Macias, “A never-before-seen Russian missile is identified as an anti-satellite weapon and will be ready for warfare by 2022,” *CNBC*, 2018.10.25.

10 А. Н. Ковальчук, Ю. И. Мушков, “Подходы к обеспечению господства в космосе в современных условиях,” *Военная мысль*, 2018, No. 5, pp. 65-68.

11 例えばソ連戦略ロケット軍アカデミーで教官を務めたイーゴリ・ベロウス少将（退役）は、弾道ミサイル発射地域の偽装、囮ミサイル、弾頭の機動化やステルス化などを米 MD 計画への対抗手段として挙げている。“Ответы на американские вызовы имеются,” *Независимое военное обозрение*, 2000.7.14.

12 ソ連／ロシアの ASAT システムについては前述の拙稿に加えて以下を参照されたい。Todd Harrison, Kaitlyn Johnson, Thomas G. Roberts, et. al., *Space Threat Assessment 2019*, CSIS, April 2019, pp. 17-24.

13 Brian Weeden, *2007 Chinese Anti-Satellite Test: Fact Sheet*, Secure Space Foundation, 2010.

14 Caleb Henry, “India ASAT debris spotted above 2,200 kilometers, will remain a year or more in orbit,” *Space News*, 2019.4.9.

15 C4ADS, *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*, 2019, p. 9.

16 “Military Wipes Out Iraqi GPS Jammers,” *FOX News*, 2003.3.25.

17 “Алмаз-Антей разрабатывает противоспутниковые системы РЭБ,” *РИА Новости*, 2017.4.24.

18 Елизавета Серьгина, “Телепортация из Кремля во «Внуково»: В Кремле действует специальная система, искажающая сигнал GPS,” *Ведомости*, 2016.10.21. また、C4ADS の報告書は、クレムリン周辺の建造物に多数のドローン妨害用固定式アンテナが設置されている可能性を指摘している（C4ADS, *op. cit.*, pp. 34-37.）。

19 Stan Goff, “Reports of Mass GPS Spoofing Attack in the Black Sea Strengthen Calls for PNT Backup,” *Inside GNSS*, 2017.7.24.; David Hambling, “Ships fooled in GPS spoofing attack suggest Russian cyberweapon,” *New Scientist*, 2017.8.10.; Matt Burgess, “When a tanker vanishes, all the evidence points to Russia,” *WIRED*, 2017.9.21.; “Israel blames Russia for GPS failure over Ben Gurion Airport,” *UAWIRE*, 2019.6.28.

20 C4ADS, *op. cit.*, pp. 5-8.

21 このほかの地域においても、プーチン大統領の訪問先と GPS の障害発生地域に強い相関があることを C4ADS の報告書は示している。*Ibid*, pp. 23-24.

22 “OSCE SMM withheld information about Russian EW systems in Donbas for two weeks,” *InformNapalm*, 2018.12.8.; “Russian GPS-Jamming Systems Return to Ukraine” *Medium*, 2019.5.23.

23 Major General Borys Kremenetskyi, *EW Lessons Learned: Russian Hybrid Warfare in Ukraine*, General Staff of Armed Forces of Ukraine, 2019.

24 Courtney Kube, “Russia has figured out how to jam U.S. drones in Syria, officials say,” *CNBC*, 2018.4.10.

25 “Атака с минометами на базу Хмеймим оказалась нападением дронов,” *РБК*, 2018.2.13.

26 Alexandra Coultrup, *GPS Jamming in the Arctic Circle*, CSIS, 2019.4.4. <https://aerospace.csis.org/data/gps-jamming-in-the-arctic-circle/>

27 Kati Pohjanpalo, “Finland Probes Russia for GPS Jamming,” *Bloomberg*, 2018.11.11.

28 一例として、北朝鮮は韓国の航空管制システムに対する GPS 妨害を度々実施していることが知られている。「航空機に GPS 障害、北の妨害と結論」『産経新聞』2016.6.24.

29 機密解除分については以下から閲覧できる。U.S. Department of Defense and U.S. Office of the Director of National Intelligence, *National Security Space Strategy: Unclassified Summary*, January 2011, p.13. <http://archive.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassified Summary_Jan2011.pdf>