ウクライナ座談会第 11 弾
――ウクライナ侵攻における宇宙・サイバー空間・電磁波領域――
（2022 年 5 月 13 日）

ウクライナ座談会第 11 弾では、ウクライナ侵攻におけるロシアとウクライナ双方による宇宙・サイバー空間・電磁波領域の活用について議論を行った。福島康仁グローバル安全保障研究室主任研究官、押手順一社会・経済研究室研究員、瀬戸崇志グローバル安全保障研究室研究員が座談会に参加した（司会は、菊地茂雄・企画調整課研究調整官）。

趣旨説明

齋藤：今般のウクライナ侵攻においてロシア軍は、宇宙・サイバー・電磁波の領域において目立った成果を上げていないようにも見受けられるが、その実態や背景にある思惑には不明な点が多い。そこで、ウクライナ座談会第 11 弾においては、ロシアとウクライナ、さらにはウクライナを支援する米国等が、宇宙・サイバー・電磁波においてどのような対策を行い、さらにこれらの領域における能力をどのように使用し、実際にどのような効果があったのかを議論したい。参加してもらうのは、福島グローバル安全保障研究室主任研究官、押手社会・経済研究室研究員、瀬戸グローバル安全保障研究室研究員の 3 名である。各位には、それぞれの専門分野の観点から議論を期待する。

1　ウクライナ侵攻における宇宙領域

福島：宇宙領域は、実際にはサイバー空間、電磁波領域と密接に関連していることに留意しながら何点かお話したい。まず、認知戦という観点では、商用衛星画像がロシア政府の言説を覆し、逆にウクライナ政府や米国政府などの主張を裏付けるという効果を発揮してきた。例えば 2 月 24 日の侵攻開始前、ロシア政府はウクライナ国境近くに集結させた部隊を撤収させていると主張したが、それをウクライナ政府や米国政府

などは否定した。マスメディアやシンクタンク、さらには個人も商用衛星画像の分析を通じて、ウクライナ政府や米国政府などによる主張の方が正しいということを確認し得た。

また、米国のスペース X 社が提供する衛星インターネットサービスのスターリンクは、ロシア軍による非人道的行為を明るみにするうえで重要な役割を果たしている。ウクライナでは、地上の通信インフラが破壊された場合でも、スターリンクを介して引き続きインターネットを利用できるようにする取り組みがなされている。これによりウクライナ市民は情報発信を継続でき、ロシア軍の侵攻に伴う惨状を世界に知らしめている。

宇宙領域はウクライナ軍の作戦においても重要な役割を果たしている。これは他国政府や企業の宇宙システムを直接あるいは間接的に活用することで実現している。現在運用されている地球観測衛星の撮像頻度では移動目標を追尾することは困難であるが、それでも衛星画像の分析を通じてロシア軍の部隊配置は大まかに把握できる。衛星通信もウクライナ軍の作戦に貢献している。とりわけスターリンクのユーザー端末は小型で持ち運びが容易であり、かつブロードバンドであることから、前線に展開したドローン部隊でも撮影した動画をリアルタイムで司令部や砲兵部隊と共有できている。

一方、ウクライナ侵攻におけるロシア軍の宇宙利用は見えてこない。2015 年に始まったシリアにおける軍事作戦ではロシア軍自身が宇宙利用をアピールしたが、ウクライナ侵攻ではそうした動きは顕著でない。当然、ロシア側も宇宙を作戦に利用していると推定できる。だが、ロシアは衛星測位システムであるグロナスを運用しているにも関わらず、Su-34 戦闘爆撃機のパイロットが米国の衛星測位システムである GPS のユーザー端末を携行していた例が報道されるなど、グロナスがどの程度、活用されているのか疑しい点もある。

そのうえロシア側はウクライナによる宇宙利用を効果的に妨害できていないようである。開戦当日にロシアは、米国のヴィアサット社が欧州で提供する衛星通信サービス網にサイバー攻撃を実施した。ウクライナ政府・軍も同社のサービスを利用していたことから一定の影響はあったと考えられるが、その後、ウクライナのフェドロフ副首相兼デジタル変革担当大臣がマスク氏に対してスターリンクのユーザー端末を提供するように要請した。その結果、一万機を超えるユーザー端末がウクライナ側に供給されている。マスク氏によれば、スターリンクのシグナルに対してジャミングが行われてきたが、ソフトウェアの改修を行うことでウクライナでのサービスを継続できている。

瀬戸：開戦前の大規模かつ迅速な米国のインテリジェンス公表政策は、商用衛星画像のような民間に拡散した情報源の存在と、撮像地点を一度把握すれば捕捉し易い国境線での大規模な陸上戦力の動員という二つの要素を無視できない。言い換えれば、インテリジェンス機関が自身の機微な情報源の喪失に繋がるリスクを低減しつつ分析を公表できたことが、今回の対応を支えてきた。質問として、商用衛星画像の技術的潜在性に鑑みたとき、米国政府の今回と類似の対応は、他の紛争でも再現性はあるだろうか。

福島：ロシアの行動が商用衛星画像で暴露されるということは今後も続くだろう。米国のマクサー・テクノロジーズ社のように、撮像した衛星画像を積極的に公表する企業も存在する。さらに、米国のホークアイ 360 社のように衛星により信号情報を収集し、ウクライナにおける GPS 妨害の発生状況を分析・公表する会社もある。

押手：スターリンクのソフトウェア改修による通信妨害への対応について、具体的にどのような手法を用いているのか関心を持った。電子防護の手段としては、まずは周波数の変更が考えられる。それ以上の手法としては、（世界的にサービスを展開するシステムに短期間で適用するのは現実的には困難だと思うが）理論上の想定として、誤り訂正符号の比率やインターバル比を増やして冗長性を高めたり、変調方式を変更する（例えば妨害の状況に応じて予め用意されたモードを切り替える）といったことが実現できるならば、優れた電子防護技術となる。

ここで、スターリンクへの通信妨害の難しさに話を広げたい。まず地上側について、衛星通信システムに一般的に言えることであるが、アンテナ面が上空に向いているため、少なくとも地上からの攻撃では利得の大きい方向からの妨害は難しく、地上に設置された多数のアンテナに向けた効果的な通信妨害は困難であると考えられる。加えて、衛星側について、スターリンクは、地上から見ると多数の衛星がコンステレーションとして上空の幅広い方位に拡散しており、そのすべての衛星を地上から同時に攻撃することは不可能であるため、衛星側に対する妨害も困難であると考えられる。

少なくとも現時点までの評価として、ロシアは電子攻撃において十分な効果を上げられていないとの指摘がある。その原因は特定できないが、一般的に、地理的に広く拡散した対象に向けて通信妨害を行うのは難しい。高い周波数帯における地上間の攻撃では、見通し線外の相手に対しては通信妨害が困難であるし、低い周波数帯で利得の小さいアンテナを用いる場合は、妨害電波が広範囲に及ぶため味方部隊への同士討ちが問題になる。

齋藤：ウクライナ侵攻はあらためて宇宙インフラの重要性を示している。１つは衛星画像に

より、ロシア軍の動きを丸裸にし、その戦争犯罪も明らかにしている。また、通信インフラとしても役割が大きい。また、地上の施設が破壊されてても、ウクライナ側からの発信を可能にしているなど、認知戦の面でも極めて重要である。また、スターリンクはウクライナ軍の指揮通信にも活用されている。

福島：宇宙の軍事利用は、もはや一部の先進国・大国に限られるわけではなくなった。ウクライナ軍によるスターリンクの活用が象徴するように、商用衛星を作戦に利用することが常態となるであろう。それに付随して、商用衛星への妨害もより深刻になると見込まれる。こうした問題への対応も課題となる。

菊地：米国防省宇宙開発庁が進める国家防衛宇宙アーキテクチャーもコンステレーション型のものを構想していると聞くが、ウクライナにおけるスターリンクの運用はコンステレーション側の強靭性を証明したかと思うか。

福島：米宇宙軍のトンプソン宇宙作戦副部長は 5 月 11 日の議会証言で、ウクライナにおいて、大規模衛星コンステレーションのレジリエンスが示されたと述べている。なお、2021 年 11 月にはロシア軍が地上発射型ミサイルで衛星を破壊する実験を行ったが、こうした兵器でスターリンクを構成する 2,000 機超の衛星を破壊することは困難である。

押手：指向性エネルギー兵器（DEW）が実用化されつつあり、例えば光学衛星に対するレーザによる撮像妨害も現実の脅威となってきた。しかし、コンステレーションでは多数の衛星が広い範囲に分散しているため、個々の衛星を攻撃してもシステム全体に影響を及ぼすのは難しいだろう。

2　ウクライナ侵攻におけるサイバー空間作戦

瀬戸：大前提として最初にお伝えしたいのは、ウクライナ侵攻におけるサイバー作戦をどのように評価するかは、現時点では正確かつ端的に答えるのが非常に難しい。一般的にサイバー作戦の動向は、インシデント対応やインテリジェンス機関の作戦に携わった関係者のみがアクセス可能な機微な一次情報でしか測れないことも多く、リアルタイムな状況把握が極めて困難である。ウクライナ本土での大規模な通常戦争の混乱もあるなかで、事実関係は常に遅れて明らかになっていく要素もある。また、今回の戦争は情報作戦(information operations：IO)や、通俗的には「認知戦」とも呼ばれる、情報空間を通じた言説と認識をめぐる競争も争点領域になっている以上、ロシア・ウクライナ双方の側に紛争の動態への情報統制の誘因もある。この点を割り引いたとき、紛争当事者ではない我々研究者や報道関係者は「現時点で観測可能な情報で何が言えるか（言えないか)」に意識的であらねばならず、状況を安易に一般化せず、じ後的に明らかに

なる情報を踏まえて分析を修正していく姿勢が求められる。

こうした前置きを踏まえて、現時点（注：2022 年 5 月 13 日）までに、各国政府発表・民間セキュリティ企業や研究機関が公表した分析を通じて確実に言えるのは、「開戦当初から、ロシア・ウクライナ双方による個々のインシデントは無数に存在してきたが、その個々のインシデントが、戦争全体の推移にもたらした影響度は依然未知数」という点だろう。

開戦当初は、ウクライナ側の通信網も完全にはダウンしないなかでロシアの大規模な通常戦力が投入された「力業」での戦争遂行をしており、欧米諸国の一部報道では、このドメインの状況把握の難しさを見落とし、特にロシアのサイバー作戦が「存在しなかった/上手くいなかったのではないか」とすら見るミスリーディングな議論もあった。しかし、2022 年 4 月に Microsoft 社が公表したレポートなどが明らかにするように、開戦当初からウクライナ全土の政府機関・民間目標に対するインシデントは、Microsoft 社が観測できる自社サービス経由のデータに限っても無数に存在してきた。また、福島主研が言及された事案だが、つい先日、米国や欧州連合がロシア軍参謀本部情報総局（GRU）に対するアトリビューションを公表したヴィアサット社が提供する衛星通信能をターゲットにした攻撃（ヴィアサット事案）のように、結果的に事なきは得たが、潜在的に軍事作戦に影響を与えうるインシデントが存在してきたことも事実である。したがって今回の戦争でも、サイバーは常に戦争遂行のなかのドメインの一部であったことは事実であり、サイバー作戦の「不在(missing)」という論調は事実に反している。

よって、今後の論争の焦点は、結果的にロシアのウクライナや第三国に対するサイバー作戦や、あるいは IT 軍を始めとするウクライナ側のロシアに対するサイバー攻撃が、結果的に個々の軍事作戦や戦争遂行に影響を与えたのか、という点にあろう。この点の全容の評価は、戦争の混乱のなかでデータの制約が大きい現時点では恐らく不可能だろう。

ただし、ここまでの公表データや、それを踏まえた各国の専門家の議論のコンセンサスを踏まえて暫定的に言える点は、サイバー作戦の軍事的または戦略的価値は、単発のインシデントのみならず、(1)他の戦力や戦争遂行計画との統合(integration)の視点と、(2)複数のインシデントが継続・反復（累積）する「キャンペーン(campaign)」の視点を踏まえて分析していかなければならない、ということだろう。

特に 2010 年代前半のこのドメインをめぐる議論は、例えば重要インフラに対する単一のサイバー攻撃が、それだけで戦争の帰趨に大きな影響を与え、かつそれは、通常戦力と比べて「即効性」があり「安価」との「神話」が形成されてきた要素は否めない。

しかし、サイバー作戦は有事にはあくまでも通常戦力や他の戦力を増幅する機能(force-multiplier)として真価を発揮するものとの議論に向かっており、そのためには、通常戦力とのターゲティング・攻撃のタイミングなどの面での統合が重要となる。ま

た、Advanced Persistent Threats(APT)とも称される高度な標的型攻撃は、情報窃取にせよ標的の破壊にしろ、標的のネットワーク・システムの脆弱性や構成情報の収集や攻撃ツール・インフラの調達などの一定の時間をかけた準備を要し、オペレーションの目的に応じては同一または異なる標的のネットワークへの幾度もの侵入を繰り返さなければ、最終目標の達成に繋がらないこともある。こうしたオペレーションは、喩えれば弾薬の事前配備のように（多くは平素からの）準備を必要とするため、通俗的に語られるほど「即効」でも「安価」でもない。

一方で、DDoS 攻撃のように技術的洗練度が低く、個々の攻撃の効力は一時的でも、その規模・頻度が累積による対応要員の消耗や、標的国社会への心理的な圧力が、軍事作戦や外交的な支援に与える影響などは、未知数であり、こうしたパターンも含めて、サイバー作戦の戦略的な含意はある程度長い目で見ていく必要がある。

この視点を踏まえ、特に米英両国の軍・インテリジェンス機関が懸念している点は、ロシアとウクライナの戦争が長期化し消耗戦の様相を呈するなかで、ロシア側の主たる標的が第三国の標的に推移することである。そのシナリオは、戦争遂行を支援するためのサイバー空間を通じた諜報活動(espionage)から、対ウクライナ支援の政治的意思を削ぐためのサボタージュ（破壊工作）まで多岐に渡りうるが、既に通常戦争での大規模な戦争状態に突入しているウクライナよりも、むしろ「平素からグレーゾーン」の事態での対応を要求される自由民主主義諸国の社会のほうが、事態の継続の社会的な影響に脆弱になりやすい。そのような紛争の動態の変化や、そこで各国政府が上手くリスク・コミュニケーションをできるか否かは今後とも注意を払う必要があるだろう。

福島：2014 年のクリミア半島併合作戦は、かなりの部分がサイバー攻撃の支援により達成されたという評価も聞くが、それは過大評価であったのだろうか。

瀬戸：あのオペレーションでのサイバー作戦は、戦域と投入兵力が限定されたクリミア半島周辺でのロシアの実力部隊との運用面での統合が機能したからこそ真価を発揮したと理解している。それについても、やはり現状変更を決定づけたのは物理空間での部隊の存在と、当時のウクライナ軍の即応能力の低さであり、サイバー作戦だけを切り離して考えるのは適切ではない。ただし、この議論は、あくまで軍事作戦での評価軸の話で、（法的な）平素からグレーゾーンの事態で続くサイバー作戦を梃とした知財窃取や影響工作などが繰り返され、累積的に標的国の国益を損ねる戦略的含意を持つとの議論はありうる。

押手：ウクライナ侵攻において、クリミア併合作戦のような電子戦とサイバー作戦のコンビネーションがみられないのはなぜか。

瀬戸：コンビネーション問題は、手に入る情報での評価が未だ難しい。例えば 4 月の Microsoft 社のレポートを見る限り、通常戦力の軍事作戦とサイバー攻撃の打撃目標にはある程度の重複が見られるが、それが意図的に統合された作戦だったのか、サイバー攻撃で上手く行かなかったから、よりシンプルな通常戦力で打撃したのか、どち

らかはよくわからない。なお防御側では、GRU によるヴィアサット事案は、ウクライナの軍・法執行機関の運用に影響を与えうる潜在性を持ちながら、最後はスターリンクの提供などもあり被害の局限に成功しているとみられる。このようなサイバー空間単体ではなく、他のドメインとの関係で優劣を見るのが重要かもしれない。

齋藤：ウクライナ侵攻においては、ウクライナ側が善戦しているが、世論戦を見るとウクライナ側が圧勝している。この世論戦での勝利は、国際的な支援の引き出しにつながっている。

瀬戸：冒頭に申し上げたように、まさに世論戦の観点から現地で観測可能なデータにバイアスが生じている可能性は否定できないため、実態としての善戦度合いは早期には結論付け難いと思う。ただ、確かに各国の民間のセキュリティ企業の有形無形の支援を取り付け、持続させるうえで、大きな含意があったのは事実だと思う。

3　ウクライナ侵攻における電磁波領域作戦

押手：ウクライナ侵攻における電磁波領域の作戦について特徴的な点を３つ指摘したい。1 つ目は、福島主研が指摘されたように、民生用の衛星通信システムであるスターリンクが効果的に利用されている点である。ロシアは携帯電話システムに対する妨害システムも有しているが、今回、スターリンクの活用により妨害を回避し通信を維持できることが実証された。

2 つ目は、ウクライナ市民がロシア軍の展開や攻撃の状況を捉えた写真や映像をインターネット上に投稿することで、民間人による事実上の ISRT 活動がなされている点である。SNS 上には、ウクライナ市民により投稿された、ロシア軍による攻撃の様子や部隊の展開状況を示す画像や映像が多数投稿されている。加えて、趣味用のドローンを保有する市民が、移動中のロシア軍車両の画像とその位置情報を、SNS を介してウクライナ軍に提供したとの報道もある。攻撃側から考えるならば、民間人による ISRT を効果的に妨害する手法は、スターリンクの実績もあり、見つけにくい状況にある。

３つ目は、ロシア軍がウクライナ軍のドローンに対する電子攻撃を実施しているが、少なくとも現時点では十分な効果が得られていないとされる点である。ロシア軍は、ドローンの遠隔操縦のための指揮統制(C2)リンクに対する妨害を行う R-330BMV、及び衛星測位システムの信号受信を妨げる R-330Zh ジテリを投入しているとみられる。これらの兵器が十分な成果を挙げられていないとすれば、その原因の一つとして、戦闘が行われている地域が地理的に拡散しており、また市街地が含まれることが挙げられるかもしれない。先に示したロシア軍の妨害装置はいずれも車両に搭載されたものであるが、車両を適切な場所に配置できなければ効果は発揮できない。まず、

電磁波は距離に応じて減衰するため、ドローンを射程内に捉えられる位置に車両を展開しなければならない。攻撃対象となるドローンが地理的に広い範囲で運用されているならば、これら全体をカバーするには一定数の車両が必要である。また、攻撃対象の SHF 帯は直進性が強いため、妨害装置からドローンまで障害物がなく見通せる位置に車両を配置する必要がある。高層の建築物が建ち並ぶ市街地では、地上に設置した装置からでは十分な見通し線を確保することは難しい可能性がある。車両が通行できない森や起伏の激しい場所では、車両搭載型ではなく携行型の妨害装置が有利であると考えられるが、こうした兵器は各国からウクライナ軍に提供され使用されている。ただし、車両搭載型の妨害装置は一般に射程が数十 km であるのに対し、携行型では数 km にとどまる。

そもそも、現在運用されている兵器はドローンに対する通信妨害を行うものであるが、ドローンの機体自体を物理的に破壊するわけではないため、ドローンが自律飛行する場合は効果を発揮できない。今後は、高出力マイクロ波や高エネルギーレーザによってドローンの外板や内部の電子機器を物理的に破壊する DEW の実用化が見込まれる。

瀬戸：ロシア軍の部隊の分散運用が、電子戦能力の現場への統合にネガティブに作用した可能性があった指摘が興味深かった。クリミア併合作戦を考えると、ロシアにとって、ウクライナ側部隊の通信妨害は、電子戦の運用構想の１つとしてありえたと思うが、そうした構想への防御側の取りうる対応はどのようなものがあるか。

押手：通信妨害に対抗することを考えるならば、送信電力や周波数、運用場所（地上、海上、航空機、成層圏、宇宙）の異なる複数のプラットフォームを確保することが重要だろう。

齋藤：新領域は相互に連関しているが、今後のインプリケーションについて問いたい。

福島：国家安全保障のために、民間が生み出す宇宙イノベーションをどれだけ効果的に活用できるかが重要となっている。民間のイノベーションを取り込むことできるか否かによって軍事的な優劣が左右される時代が到来している。

瀬戸：「新領域」というとドメインに焦点を当てた議論になりがちだが、その能力の整備・運用に要する「時間軸」を加味した議論が必要に思う。例えば今回のウクライナ政府の対応能力は、各国の CERT、軍・情報機機関、法執行機関同士の協力のほか、NATO の防衛・安全保障関連能力構築支援イニシアティブ(DCB Initiative)関連の事業を含め、2014 年以降の欧州・環大西洋地域でのウクライナとのサイバーセキュリティ協力の上に成り立っている。今回の侵攻前後で、ウクライナ政府やリトアニア政府が米国サイバー軍の支援要員を受け入れえたのも、2018 年以降の米国サイバー軍とウクライナを含む欧州の同盟・パートナー国政府との類似の任務経験が基盤にある。陸海空などの通常の防衛力と同じく、攻撃側と防御側の双方で、「平素」からの取組と準備が「有事」のパフォーマンスと相互に結びつく側面はもっと意識されるべきだろう。

押手：電磁波、宇宙、サイバーのドメイン間の重なり、結び付きを再認識し、この前提を踏

まえた全ドメインの効果的な活用が重要である。本座談会においても、民間人が画像や映像を、宇宙の衛星を経由して送信し、これがサイバー空間である SNS 上で拡散しているという状況が説明された。これは一例に過ぎないが、言うまでもなく、電磁波、宇宙、サイバーの各領域は互いに結びついたものであり、それぞれ個別に運用方法や作戦を考えていたのでは、効果を最大化できない。各領域を切り分けるのではなく、一体的に捉えるという視点が重要である。

齋藤：今回の座談会では、新領域の重要性を浮き彫りにすることができた。参加者からは貴重な話を聞くことができた。これだけの準備をしてくれた参加者に感謝したい。

（座談会で示された意見は参加者個人の見解であり、防衛研究所や防衛省の意見を代表するものではない）