「情報戦は地政学」ロシアの偽情報戦略を解く

ネットニュースや動画を使ったサイバー戦は一般人を巻き込み、時には「駒」にする危険を孕む。ロシアは情報空間を「地政学」として見ており、ウクライナは世界に共感を呼ぶメッセージに腐心する。かつてない展開の「情報戦」。どうなっているのか。

笹川平和財団
安全保障研究グループ研究員
長迫智子
ながさこ　ともこ　東京大学大学院人文社会系研究科修士課程および情報セキュリティ大学院大学情報セキュリティ研究科修士課程修了。近著に"Global Disinformation Campaigns and Legal Challenges", *International Cyber Security Law Review*, Vol. 1. Springer. など。

二月二四日、「特別軍事作戦」と称してロシアがウクライナへ軍事侵攻を開始した。情報空間では、軍事侵攻以前からサイバー攻撃が行われるとともに、ロシア側のナラティブ（物語）を中心としたディスインフォメーション（偽情報）の拡散も観測されている。ロシアによる情報戦とそれに対するカウンターとしてのウクライナによる情報戦が、ハイブリッド戦という新しい戦争の様相として注目を浴びている状況であるが、情報戦や影響工作、ディスインフォメーション、フェイクニュースといった単語が日本の各種メディアで交錯しており、その実像は整理されていない。さらに、このウクライナ侵攻における情報戦では、ＳＮＳなどのサイバー空間にペルソナを持つわれわれ一人一人も、戦争の当事者である。しかし、そうした当事者意識が希薄なまま、兵器化するＳＮＳを用いてサイバー空間に「参戦」することは、非常に危ういといえる。

ロシアの情報戦、その三つのレイヤー

この軍事侵攻で、ロシアが影響工作を試みている情報のレイヤーは三つある。①国際世論に向けたロシアの侵攻を正当化するナラティブ、②相手側のウクライナ市民を混乱に陥れ政府への信頼を失墜させるディスインフォメーション、③軍事戦略上の欺瞞作戦、である。②や③がナラティブの役割を果たす場合や、①がロシアの正当化だけでなく西側諸国の社会の信頼失墜を狙う機能をもつ場合もあり、

複合的である点に注意が必要である。

安全保障の文脈における「ナラティブ」とは、北大西洋条約機構（ＮＡＴＯ）最高司令部戦略的コミュニケーション担当チーフであったマーク・ライティによれば、単なる物語ではなく、イデオロギー、理論、信念に沿った事象の説明であり、相手に将来の行動を促すものである。このナラティブは物語形式で表現され、われわれの認知に影響を与える戦略の行使といえる。安全保障上の戦略的なナラティブは、戦略と物語を整合させ、相互に支援し、統合する。そこには戦略を支えるための偽の情報も含まれる。

一方で「ディスインフォメーション」は、社会、公益への攻撃を目的とした害意のある情報で、情報自体が偽であるだけでなく、情報自体は真であるが誤った文脈や操作された内容で拡散されるものなど、真偽どちらもありうる、と欧州連合（ＥＵ）の報告書や各種先行研究から定義される。国家勢力によるディスインフォメーションは民主主義の毀損や社会の分断、不安定化を目的に用いられる情報操作型のサイバー攻撃であることから、戦略的ナラティブや一部の軍事上の欺瞞作戦をも広く包含する概念として、現在は認識されている。

①については、今回の軍事侵攻の淵源である二〇一三年のユーロマイダン、一四年のクリミア危機以降、「ウクライナ政府はネオナチであり東部親ロ派地域で虐殺を行っている」、「ウクライナとロシアは歴史的に一体である」、「ＮＡＴＯはロシアの安全保障を脅かしている」といったナラティブが典型的である。これらを素地に、ロシアは、ドネツクおよびルハンスク人民共和国をウクライナの侵略から守ることを今回の軍事作戦の目的と謳っている。

次に②について典型的であったのは、二月一五日にウクライナ国防総省および国立銀行二行に対して行われたサイバー攻撃と、それに関連するディスインフォメーションの流布である。銀行のウェブサイトにＤＤｏｓ攻撃が行われサイトがダウンし、その前後には当該銀行を詐称して「ＡＴＭが使用不能となった」という偽の情報がＳＭＳ（ショートメッセージサービス）を使ってウクライナ市民に送りつけられた。このディスインフォメーションの流布で、一時、市民の間に混乱が広がったが、実際にはＡＴＭが機能していることを市民ら自ら確認しＳＮＳ上で反論を行った。一連の攻撃について、米セキュリティ大手のMandiant社は、「一般利用者が銀行のウェブサイトを確認するように誘導しアクセス数を急増させ、疑似的ＤＤｏｓ攻撃に加担させる」、「市民の恐怖を煽り、政府への信頼を毀損する」とい

う二つの目的があったと分析している。

③については、同じく二月一五日にロシア国防省が行った「ロシア軍部隊が演習を終えて撤収を始めた」という発表が代表例だろう。「特別軍事作戦」を電撃的に成功させるための欺瞞的な情報であったが、欧米のメディアが商用の衛星画像やSNS上の投稿画像、動画等を分析して反論を行った。さらには一八日、バイデン米大統領が演説で、米国のインテリジェンス情報をもとに「ロシアのプーチン大統領がウクライナ侵攻を決断したと確信している」と否定した。

ロ・ウ間の緊張が高まった年明け以降、こうしたディスインフォメーションの発信は、ロシアによる虚偽情報の拡散に対処するためEUが二〇一五年に設置した作業部会「イースト・ストラトコム・タスクフォース（East StratCom Task Force）」において二六三件が確認されている（四月三〇日現在）。設置以降、ウクライナに関わるディスインフォメーションは五二九〇件が確認されており、ロシアが継続的にこうした影響工作を行っていることが伺える。工作活動には、ロシア政府系メディアのRTやスプートニクといったウェブメディアとそのSNSアカウント、クレムリンとつながりのあるオリガルヒ、エフゲニー・プリゴジンが資金提供する民間組織であるインターネット・リサーチ・エージェンシー（Internet Research Agency：IRA）によってSNS上に大量生産されたアカウントが活用されている。今年一月の米国財務省による制裁発表、同年四月のマイクロソフトおよびメタの報告書によれば、ロシア連邦保安庁（FSB）、ロシア連邦軍参謀本部情報総局（GRU）、ベラルーシの国家保安委員会といった政府機関が、こうした影響工作に関係していることも報告されている。

活発な戦時下ウクライナのカウンター

こうしたロシアの動きに対し、ウクライナ側も情報戦におけるカウンターとして影響工作を行っている。

二月二四日の侵攻と同時に、「首都キーウからゼレンスキー大統領とウクライナ軍が逃亡した」といった情報が、フェイスブックをはじめとしたSNS上でロシア関係アカウントから発信された。これに対し、ゼレンスキー大統領は即座にキーウから動画を発信し、逃亡が嘘であると反論した。このように、ウクライナ政府側はロシアの発信するナラティブやディスインフォメーションには的確に反論を行ってきた。現地情報の発信によるカウンターという点で

は、ウクライナ市民も積極的に画像や動画をSNS上にアップロードしていることが有効な動きとなっている。一例としては、演習と称して参戦させられたと話す若いロシア兵捕虜の動画がSNS上で数多く拡散され、国際世論に対して、ロシア軍のあり方に疑問を投げかけた。ただし、捕虜の待遇に関するジュネーブ条約一三条では、「(捕虜は)侮辱及び公衆の好奇心から保護しなければならない」とされており、人心に訴える効果的な手法であったとしても、こうした動きすべてを許容すべきではないだろう。

ナラティブの発信という点でも、ウクライナ政府の各種発信は非常に奏功している。ゼレンスキー大統領の各国議会でのオンライン演説について、東京海上ディーアールの川口貴久主席研究員は、米国では「パールハーバー」、日本では「原発事故」や「サリン」など、相手国民の歴史感情に訴えるようなキーワードや文脈で語りかけたことを認知戦の一環と評価している。

「悪辣なロシアに抗戦するウクライナ」、というナラティブ形成は非常に巧みに実行されているが、それが正しい情報ばかりから構成されるものではないことには注意が必要だ。二月二四日のズミイヌイ島の戦闘では、「ウクライナ国境警備隊が降伏を拒否し玉砕した」というウクライナ側の発表がある種の華々しい悲劇として国際社会でもてはやされた。しかしロシア政府は、警備隊が自発的に降伏をした後捕虜になったと発表し、ウクライナの情報に反論した。後にウクライナ国家国境警備局およびウクライナ海軍は国境警備隊全員の生存とロシア海軍による拘束を認めており、警備隊の通信途絶だけをもってして「玉砕」と演出されたのである。しかし「ロシアの軍艦よ、くたばれ!」という国境警備隊の最後の通信は、ウクライナ人とその支持者のための各国の集会でスローガンとなった。これは、一九世紀テキサス革命のアラモ砦の戦いにおける「アラモを忘れるな」というフレーズと比較引用され、歴史記憶を刺激する典型的なナラティブ形成といえる。

ウクライナ政府は、サイバー空間上の対処だけでなく、フェイクニュースを流していた五つのボットファームを突き止めて閉鎖し、設備を没収するなど、物理的な対処もあわせて行っている。ロシア側のボットファームによる工作活動を明らかにすることは、親ウ反ロのナラティブの後押しにもなっている。

情報対立を「地政学」とみなすロシア

では、こうした工作活動は、ロシアのどのような戦略に

起因するものなのか。

ロシアの「情報」に対する見方は、西側のそれとは大きく異なる。ロシアの国家安全保障戦略や軍事ドクトリンでは、「情報対立」(Информационное противоборство (informatsionnoe protivoborstvo))という概念が援用されている。ロシア国防省は、情報対立を「国益と思想の衝突」と表現する。敵の情報インフラを標的とし、自国を同様の影響から守ることを最優先事項としている。

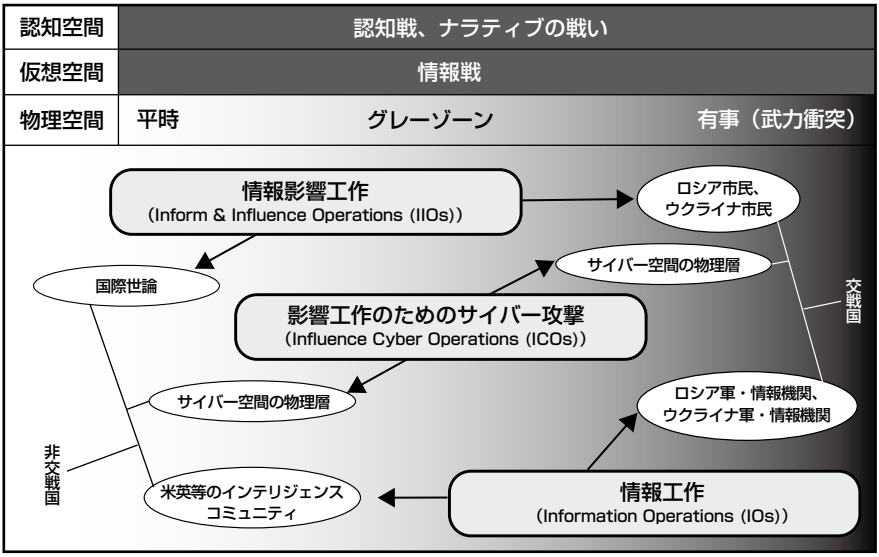
この「対立」では心理的権限も重要と考えられ、行為者は情報資源だけでなく、敵対国の軍人と住民全般の心理にも影響を与えようとする。そして、ロシアが規定する「情報空間」は、情報を形成し、変換し、保存する活動、および個人と公衆の意識、情報インフラ、情報そのものに影響を与える空間を指している。よって、そのための「情報セキュリティ」は、デジタル・ネットワークの保護だけでなく、社会の認知的完全性をも包含する。

そこで用いられる「情報兵器」という概念は、定義上は「情報戦のために使用する情報技術、手段、方法」と規定されるが、実際は、心理的影響を重視し、ディスインフォメーションの流布、電子戦、心理的圧力、敵のコンピュータ能力の破壊など、さまざまな活動が含まれている。二〇二一年のNATOによるロシア戦略分析レポートによれば、ロシアは、情報対立を大国、政治・経済体制、文明の間の絶え間ない地政学的ゼロサム競争であるとみなしている。平時と有事を明確に区別する国際法秩序に基づく西側の国家間紛争観とは異なり、ロシアの「情報対立」はわれわれの心理や認知までも当然のように射程として、常に進行中であることに留意せねばならない。

このように非軍事的な手段により相手国の政治上、軍事上の意思決定に影響を及ぼそうとする活動は「影響工作」とみなされる。SNSの活用で影響工作は安価かつスピーディな工作となり、その準備となる平時からのサイバー攻撃が組み合わされ、平時有事の区分が失われた。

NATOの影響工作の分類では、「情報影響工作」、「影響工作のためのサイバー攻撃」、「(軍事的な)情報工作」の三つに影響工作は大別される。「情報影響工作」は多様な情報発信を通じて大衆に影響力を行使するもので、メディアやSNSでの情報流布が中心となる(先述の工作例で①が中心)。「影響工作のためのサイバー攻撃」は、敵対国にハッキングをして情報をリークしたりウェブサイトをダウンさせたり、ディスインフォメーションの流布に必要なアカウントを乗っ取るといった活動である(先述の例で

図　ウクライナ戦争における情報戦と影響工作の関係性



(P. Brangetto and M. A. Veenendaal, "Influence Cyber Operations: The use of cyberattacks in support of Influence Operations," 2016, p117 をもとに筆者作成)

は②が該当）。「（軍事的な）情報工作」については、相手の軍やインテリジェンス機関に対し、軍事的な意思決定を混乱させ能力簒奪を図る（先述の例では③が該当）。これらを今回のウクライナ侵攻にあてはめたものが、上の図となる。

絶え間ない情報戦にどう備えるか

こうしたロシアの情報戦は、実際に成功しているといえるのだろうか。各国のインテリジェンス情報の公表、ファクトチェックやウクライナ側のカウンターが成果を上げ、軍事上の情報工作も、ネオナチに対する戦いといったロシアのナラティブも、いずれも国際社会において説得力を有しているとは言い難い。国際世論上は、ロシア＝悪、ウクライナとそれを支援する西欧諸国＝正義という構図が支配的である。しかし、これによりロシアの影響工作が無力であるとするのは皮相な見方である。日本国内でも、親ロ的な言説は一定の拡散力を有しているからである。

インターネットセキュリティ会社 Solacom や東京大学の鳥海不二夫教授の分析では、ＳＮＳ上で米国の極右系陰謀論「Ｑアノン」に共鳴した内容や新型コロナウイルスのワクチンをめぐる誤情報を発信していたクラスターが、ウ

クライナ侵攻では親ロ的な投稿を拡散しているということが判明した。各調査によれば、「ウクライナには米国主導の生物兵器研究所がある」という投稿が九〇〇万件以上拡散され、「ウクライナ政府はネオナチ」という二二八件の投稿は、約一万九〇〇件のアカウントにより三万回以上リツイート（転載）されていた。過去には、二〇一六年のブレクジットに係る英国国民投票のディスインフォメーションの流布に関与していたロシア系アカウントが米国大統領選に再利用されていた事例もある。今、ロシアのナラティブに親和的なアカウントが、今後、日ロ関係に影響を及ぼすような効力を発揮する可能性があることに留意すべきである。

それでは、われわれはどのようにこうした情報戦、認知戦に対処していけばよいのだろうか。

日本は平時の段階でのディスインフォメーションへの対策が遅れている。すでに欧米諸国が対策に取りかかっている、「外国からのディスインフォメーションのモニタリングと分析を行う情報収集センターの設置」、「外国からの選挙干渉規制を目指した公職選挙法と国民投票法の改正」、「選挙をサイバーセキュリティ上の重要防護対象とするため選挙インフラを重要インフラに指定する」、「外国からの情報操作型攻撃に対して、積極的サイバー防御を行える体制を整備」、「政府とプラットフォーマーによるディスインフォメーションを防ぐ協同規制の体制を整備」、「メディアリテラシー環境とファクトチェック体制を整備し、外部の影響工作に抗堪性のある国民意識を醸成」といった項目から取り組むべきだ。笹川平和財団では、二〇二二年二月に、こうした対策を織り込んだ「外国からのディスインフォメーションに備えを！」という政策提言を公表しており、政府や官界の対応が待たれる。また、今回、西側諸国ではRTやスプートニクといったロシア政府系メディアの締め出しが各SNS上から行われた。言論の自由とのバランスが難しいところではあるが、有事に限り行う対策として、こうした強い措置も検討の余地はある。

そして、ナラティブの戦いについては、まずは情報環境のリスク分析を行うことがNATOをはじめとした各種レポートで指摘されている。われわれ日本人がどのようなナラティブを持っており、どのようなナラティブに弱いのか、情報戦への備えとして見直しを行う必要がある。

ウクライナ侵攻は対岸の火事ではない。われわれも常に情報戦、認知戦下にいることを認識して備えを進めるべきである。●