NO.240 | 2022.4.25
政策オピニオン

一般社団法人
平和政策研究所
Institute for Peace Policies

サイバーグレートゲーム

―― データをめぐる大国間の争いと日本の対応 ――

土屋 大洋　慶應義塾大学大学院政策・メディア研究科教授

Contents

はじめに

イギリス人で初めてノーベル文学賞を受賞したラドヤード・キプリングが 1901 年に『少年キム』という小説を発表した。物語では少年キムが大英帝国と帝政ロシアの間のスパイゲームに巻き込まれていく。国際政治色が強い小説というわけではないが、物語の背景にはロシアとインドの間にある中央アジアをめぐる覇権争い「グレートゲーム」という考え方があった。この考え方はその後、欧米の戦略家に引き継がれた。

中央アジアを含むユーラシア大陸の内陸部は地政学者たちによりハートランドと位置づけられた。ハートランドを取るものが世界島（ユーラシア大陸とアフリカ大陸）を支配し、世界島を支配するものが世界を支配するという論理が使われた。

冷戦の最中、1979 年にソ連が実際にアフガニスタンへ侵攻した。第二次世界大戦後、英国に代わってソ連に対抗することになった米国がその阻止に動いた。

2001 年には 9･11 同時多発テロの報復として米国がアフガンへ侵攻したが、21 年夏に撤退した。現代にもグレートゲームの構図が少なからず残っているということができる。

一方で、現代はサイバーグレートゲームが激しく展開している。サイバースペースにおけるハートランドの一つはデータセンターである。デジタル・ハートランドをめぐるサイバーグレートゲームにおいて、日本の果たすべき役割は大きい。

土屋 大洋｜つちや・もとひろ

慶應義塾大学大学院政策・メディア研究科教授

1999 年慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士（政策・メディア）。国際大学グローバル・コミュニケーション・センター（GLOCOM）主任研究員などを経て、2011 年から現職。21 年 7 月まで総合政策学部学部長、21 年 8 月から慶應義塾常任理事。兼任として、内閣府宇宙政策委員会宇宙安全保障部会委員、GLOCOM 上級客員研究員、国際社会経済研究所研究アドバイザーなど。主著に『暴露の世紀』（角川新書）、『サイバーセキュリティと国際政治』（千倉書房）、『サイバーグレートゲーム：政治・経済・技術とデータをめぐる地政学』など多数。

1. 2016 年米国大統領選挙とロシアの介入

2016 年 6 月頃、「GUCCIFER2.0」というウェブサイトが現れた。これはロシアのスパイ機関と言われており、当時米国大統領選挙の候補者

だったヒラリー・クリントンと民主党全国委員会の情報を暴露した。元祖の GUCCIFER とはジョージ・ブッシュ大統領（息子）のアカウントをハッキングしたルーマニア人である。

GUCCIFER2.0 がハッキングした情報は、ウィキリークスにも掲載された。このとき、ロシアのプーチンとウィキリークスのジュリアン・アサンジと大統領候補だったトランプが共謀したのではないか、つまり、プーチンがデータを盗んでウィキリークスで暴露させてトランプ候補を当選させたのだ、という話さえ出回った。

プーチンにはヒラリーを落選させたい動機があった。ヒラリーが大統領選挙前に出版した本には「ロシアには報道の自由がない」など、ロシアやプーチンに関する批判が多かった。

2016 年に公表されたパナマ文書にプーチンの友人（音楽家）が載っていたことで、プーチンが友人を通して資金洗浄していると批判された。同年のリオオリンピックや 2018 年平昌オリンピック、東京 2020 ではロシア選手のドーピングが暴露された。

これらをプーチンの側からみれば「情報戦で攻撃の的になっている」という認識になる。プーチンは以前から、インターネットは CIA のおもちゃだと批判していた。ロシアによる米国大統領選挙への介入についても、プーチンは「仕掛けたのはあくまで米国」という認識であり、「米国の報道の自由には“偽情報を流す自由”も含まれており、ロシアは脅威にさらされている」と考えているのだろう。

ロシアの情報工作組織 IRA について、日本経済新聞が興味深い記事を載せたことがある。日経記者が IRA のビルに張り付いて、ビルから出てくる人たちに仕事内容を確認して回った。彼らは貿易業などと応えていたそうだが、やがてイライラした警備員がやってきて「俺達のボスは大統領だ」と言い放ったという。IRA が大統領の影響下にあることを明言した、世界的スクープだったのではないか。

私も IRA のビルに行ったことがあり、日経記者のように突撃取材を試みた。しかし、一階のテナント一覧はすべて剥がされており、内装工事が始まっていた。ビルの外側には「リース募集中」とあり、私は IRA が移転したのだと思った。帰国後にそれをコラムで書いたところ、国内の某報道機関から「リース募集中こそフェイクニースだ」と指摘された。その報道機関は「二階ではフェイスブック、三階ではツイッターに投稿している」という IRA ビルに勤務する若者の証言を報じた。

ロシアが IRA を使って 2016 年米国大統領選挙に介入していた証拠は徐々に明るみになった。それでもトランプ大統領はロシアがやったことを認めず、「中国や北朝鮮、イランもやっている」などとはぐらかしていた。

その後の報道によれば、バラク・オバマ大統領はロシアの選挙介入を 2015 年夏の時点で把握していた。中国で G20 サミットが行われたときに、オバマはプーチンをにらみつけて選挙介入をやめるように警告したが、プーチンはしらを切った。オバマはロシアの介入があろうとも、当選するのはヒラリーだと思っていたので、あえて公表しなかった。しかし、トランプが当選したことでオバマは公表しなかったことを後悔したという。

2. 新たなサイバー戦略で臨んだ 2020 年米国大統領選挙

オバマ大統領は 2017 年 1 月大統領退任の二週間前に、国土安全保障省に命じて選挙インフラを重要インフラのサブセクターに認定した。これを受けて、連邦軍が選挙を守れるようになった。

2017 年 8 月にはトランプ大統領が、機能別統合軍のひとつである戦略軍の下にあったサイバー軍を最上位の統合軍に昇格させると発表し、2018 年 5 月に実施した。同年 9 月には国防総省がサイバー戦略の概要を発表した。その中で「前方で防衛する（defend forward）」という言葉を四度使用した。

米軍は元来、米国本土での戦闘を回避するために在日米軍や在韓米軍、中東の米軍基地のように、戦力を前方に展開してきた。2018 年の発表では、サイバースペースでも同様に前方展開すると宣言したことを意味する。前方防衛という言葉は 2015 年 4 月のサイバー戦略にはないので、国防総省は 3 年間でサイバー戦略のコンセプトを大きく変えた。

サイバースペースにおける前方防衛とは、具体的には平時から中国・ロシア・イラン・北朝鮮等のネットワークに侵入して、米国に対するサイバー攻撃の兆候を見つけたらそれを阻止することを意味する。

同年 11 月、中間選挙が行われた。サイバー軍は防衛策として、実際にロシア IRA のネット回線を遮断した。また工作員がフェイスブックやツイッターにフェイクニュースを流す兆候を見つければ、「お前がやろうとしていることはわかっている」という主旨のメッセージを送りつけ、デスクトップに表示させた。日本の自衛隊では容易にできることではない。サイバー軍の努力の甲斐もあり、米国は 2018 年中間選挙を無事に乗り切ることができた。

サイバー軍の司令官は 2018 年 5 月から三代目のポール・ナカソネである。ナカソネは 2019 年 8 月に記者会見を行い、2020 年大統領選挙が最優先課題だとし、絶対に防衛すると発表した。

しかし、実際の大統領選挙はサイバー攻撃と関係なく、すでに混乱していた。討論会では非難合戦を繰り広げ、トランプはジョー・バイデンの議論を何度となく妨害した。

トランプ陣営はバイデンに対するレッテル貼りにも力を入れた。議会でよく居眠りをするバイデンを指して、トランプは“スリーピー・ジョー”とよんだ。トランプ支持者からは「バイデンは高齢だから、もうボケている」「アルツハイマー病に違いない」など、ネガティブメッセージが発信された。

同じような印象操作を狙ったフェイクニュースは SNS に溢れていた。バイデンが演説する舞台の文字を書き換えることで、バイデンがフロリダで「ハロー、ミネソタ！」と話しているような動画がツイッターに投稿され、100 万回再生された。フェイクニュースとしてはチープなレベルだが、騙される人もいる。

偽アカウントも数多く作られた。ある黒人男性が共和党支持をほのめかしたツイートには、リツイートが 1 万回以上、いいねが 4 万回以上押された。現在、このアカウントは凍結されている。

ゲイリー・レイと名乗る黒人男性の写真のツイッターアカウントはトランプ支持を表明していた。しかし実際の写真の男性が「私はゲイリー・レイではない」と名乗り出て、偽アカウントだと判明した。

大統領選挙期間中に、Black Lives Matter 運動が全米に広がった。BLM を取り扱った“BLMNews.com”というニュースサイトが登場したが、これはイランによる偽サイトだと判明した。現在このサイトにはアクセスできない。

他にも、有権者にトランプへの投票を迫るメールが送られた。国家情報長官がこれら脅迫メールはロシアとイランによるものだと発表した。脅迫メールの中には、イランが米国の極右団体「プラウドボーイズ」を装ったものもあった。

今回の選挙介入で目立ったのはロシアよりもイランだった。サイバー軍は国外からの不穏な動きなどをいち早く見つけて混乱を食い止めることに努めた。実際に選挙の大勢に関わるような選挙介入はなかったと言われている。

選挙後、ロシアがサイバースパイ活動を行っていたことが報じられた。具体的にはソーラーウィンズというサイバーセキュリティ会社のシステムをハッキングして多くのデータを盗んでいた。

一方、中国が選挙介入した証拠はあまり見つかっていない。どちらの候補が中国に利するのかわからなかったからだ、とサイバー軍の前司令官を務めたマイク・ロジャースはその理由を述べた。中国は通常、民主主義国家における選挙を見下して、自国の体制の優位性を強調するプロパガンダに力を入れる。今回の大統領選挙はすでに混沌としていたので、あえて介入する必要性を見いだせなかったのだろう。

3. サイバースペースの実態とケーブル通信の脆弱性

従来の作戦領域は陸海空であり、各領域に陸軍、海軍、空軍が対応してきた。近年は第四の作戦領域として宇宙、第五の作戦領域としてサイバースペースが挙げられている。

ただし、サイバースペースは他の四つの作戦領域とは違い、人工的な領域である。サイバースペースは雲（クラウド）のように浮かんでいるものではな

く、通信端末とそれらをつなぐ有線・無線の通信回線、サーバーなどが集積されたデータセンターなどで構成される、物理的な存在である。

サイバースペースはインターネットの外にも広がっている。多くの通信では光ファイバーの有線ケーブルを使っている。東京の地下には洞道というケーブル回線用の大きな穴が通っている。

もし何らかの目的で通信を遮断したい場合、手の込んだサイバー攻撃をする必要はない。標的周辺の洞道に侵入してケーブルを切ればいい。もちろん洞道に入るのは簡単ではないが、武装勢力などがその気になれば侵入は可能である。

私が懸念しているのは、日本全体の通信が同じ脆弱性を抱えているという点である。島国日本は国際通信の 99％を海底ケーブルに依存している。海底ケーブルの安全性は日本にとって死活問題である。

海底ケーブルは沖合では海底にそのまま置いてあり、陸地に近いところでは見えないように砂浜に埋められている。2015 年にニューヨーク・タイムズは、米国沿岸に現れたロシアの潜水艦がどの海底ケーブルを切れば米国経済にダメージを与えられるかを探っているのではないかと報じた。退役した米国海軍の提督ジェイムズ・スタヴリディスによれば、中国もロシアと同じことを考えているという。海底ケーブルには高電圧がかかっているため、直接触ると感電死してしまうが、爆発物などによって破壊することは可能である。

また、海底ケーブル陸揚局は局所的に集まっている。日本では千葉の千倉と三重の志摩など、韓国では釜山の近郊、台湾では南北に一箇所ずつ、中国では上海と汕頭と香港に集中している。イギリスのコーンウォールやシンガポールのチャンギ空港付近にも陸揚局を確認することができる。具体的な場所は公開情報だけでほとんど明らかになる。

くわえて重要なのが、陸揚局でケーブルの信号処理を行う SLTE（端局装置）である。ケーブルそのものは光ファイバーをコーティングしているだけのものなので、情報に細工を施すことはできない。経済安全保障の視点では SLTE の製造元にも十分注目すべきであるが、見逃されやすい。

4. 海底ケーブルと経済安全保障

アフリカのカメルーンと南米のブラジルをつなぐ SAIL という海底ケーブルがある。全長 5800km の中距離程度のケーブルで、所有者はカメルーンのカムテルとチャイナユニコムという通信会社である。中国企業が本土とまったく関係ない地域で海底ケーブルを所有していることには驚かざるをえない。

戦略的な要衝であるジブチには日本を含む様々な国が拠点を作っている。同時に、アジアとヨーロッパをつなぐ多くのケーブルも敷設されている。2016 年には中国も、ジブチにデータセンターや海底ケーブル陸揚局を開設した。すでにケーブルの引き揚げが始まっており、日米の関係者は非常に警戒している。

海底ケーブルの製造では米国のサブコム、日本の NEC、欧州の ASN という三社が 9 割以上のシェアを握っている。四番手につけてシェアを伸ばしているのが元ファーウェイの HMN テックである。

トランプ政権以来、米国は中国企業の排除を強化しているが、海底ケーブル産業でも同様である。

南米とアジアを海底ケーブルで結ぶチリ政府の計画について、中国はチリから中国を直接結ぶルートを提案した。トランプ政権はこれを警戒し、日米豪が連携して中国を妨害した。その結果、チリ政府は日本が提案したチリからニュージーランド・オーストラリアを経由して日本につながるルートを承認した。

同じ頃に注目されたのが PLCN（Pacific Light Cable Network）の差止めである。PLCN はグーグルとフェイスブック、中国のドクターペンが出資し、ロサンゼルスと香港を結ぶケーブルで 9 割ほど完成していた。米国司法省は 20 年 6 月、香港での陸揚げを認めないと発表した。17 年までは中国と直接つながる海底ケーブルの敷設は許可され、既存ケーブルの使用は続いている。PLCN の差止めは米中対立を象徴した。

20 年 8 月にはマイク・ポンペオ国務長官がクリーンネットワーク計画を発表した。これはアプリやクラウドサービス、海底ケーブルなどから中国企業を

排除し、同盟国の企業だけでネットワークをつくる構想である。中国外交部は強く反発したが、その後米国の政治的動きは加速した。同年 10 月には太平洋の島国パラオが 2 本目の海底ケーブルを敷設する計画に対して、日米豪の外相が揃ってインフラ支援を発表した。

東ミクロネシアにおける海底ケーブル敷設プロジェクトでも、日米豪は結束した。東ミクロネシアケーブル敷設はナウル、キリバス、ミクロネシア連邦における通信環境改善を目的とし、当初は三社が応札した結果、HMN テックが 2 割以上低い価格で落札した。

東ミクロネシアはグアムに近いこともあり、米国は敏感にならざるをえない。ナウルは台湾と国交をもっているが、ミクロネシア連邦は 1989 年から中国と国交を持っており、キリバスは 2019 年に台湾から中国に切り替えた。地政学的に危ういこともあり、米豪はこの地域にファーウェイのケーブルが敷設されることを強く警戒した。その結果、キリバスとナウルは応札した三社ともに必要な条件を満たしていなかったとし、入札を無効にした。

5. 日本のサイバーセキュリティ強化

サイバーセキュリティという点で、2021 年の東京五輪は日本にとって一つの正念場だった。サイバー防衛にあたって、わが国は米国の NSA や英国の政府通信本部(GCHQ)と協力した。実際のサイバー攻撃の回数は 4 億 5 千万回程度で、2012 年のロンドン五輪の 2 倍以上の規模ではあったが、想定したほどではなかった。この数を聞いた中国の専門家はその少なさに驚いていた。

日本がサイバーセキュリティ強化に舵を切ったのは 2018 年からである。同年 1 月の国会における施政方針演説で、安倍晋三総理は防衛大綱の見直しについて言及した。同年 3 月の防衛大学校の卒業式では「サイバー空間と宇宙空間など新たな領域で優勢を持つことが、わが国の防衛に死活的に重要になっている」と語った。

同年 8 月には安全保障と防衛力に関する懇談会が開かれ、議論の結果は同年 12 月に閣議決定された防衛大綱の中で「多次元統合」という言葉でまとめられた。

多次元統合の原案は、米国のオバマ政権時代に出てきた「クロスドメイン」である。陸・海・空・宇宙・サイバーに、日本は電磁波という領域も含める。これら領域を横断的に作戦活動が行われることを目指す。

防衛大綱で注目されたのはサイバー反撃能力の保有を明記した点である。これにより、敵のサイバー攻撃に対抗措置を取ることができる。今までの防戦一方からみれば、大きな前進である。

さらに大綱では次の一文がある。「全ての領域における能力を活用して、我が国周辺において広域にわたり常時継続的な情報収集・警戒監視・偵察活動を行うとともに、柔軟に選択される抑止装置等により事態の発生・深刻化を未然に防止する」。これはサイバースペースも含む全ての領域でサイバーインテリジェンスができるようになる、と読むことができる。実際に、自衛隊はハイレベルなサイバー訓練を実施している。

6. サイバーグレートゲームと日本の役割

サイバーグレートゲームでは、様々な国々がデジタル・ハートランドへのアクセスを競っている。デジタル・ハートランドは以下の二つである。

一つはデータセンターである。たとえば我々の資産はもはや硬貨や紙幣ではなくデジタル化された情報である。銀行の預金はデータセンターの中にデジタル信号として保管されている。このデータを紛失すれば、我々は資産を失うということになりかねない。

データの重要性は国家レベルでも同様である。データセンターをいかに防備するかは死活的に重要である。

もう一つのハートランドは、我々の頭の中にある。老若男女を問わず、我々は根拠が疑わしい情報を簡単に信じてしまうことがある。たとえば新型コロナワクチンには深刻な副作用があると、SNS を通して

信じた人は少なくなかった。メッセンジャーRNAの仕組みを理解すれば、ワクチンの働きを科学的に理解できるはずである。2020年の米国大統領選挙では、Qアノンを本気で信じる人たちが議会で暴動を起こすまでに至った。

これらの現象を説明する上で、「ナラティブ（物語）の木」という話を紹介したい。ツイッターやフェイスブック、インスタグラムなどで受け取るメッセージは枝葉の部分に該当する。それらのメッセージ（枝葉）を流す人が、明確な価値観（根）に基づく物語（幹）をもっている場合がある。その価値観が我々の価値観と相容れなかったとしても、我々がメッセージに踊らされていれば気づかないうちに洗脳されてしまうかもしれない。

これは民主主義がもつ、オープンであるがゆえの脆弱性である。我々の頭の中へのアクセスに、政府が検閲を行うことはできない。民主主義社会に生きる我々は自由にいろいろな情報にアクセスできる。しかし、その情報源がSNSなどに偏るのは危険である。

民主主義の脆弱性は物理的なアクセスという面にも当てはまる。データセンターや海底ケーブル陸揚局の場所なども、オープンゆえに簡単に把握することができる。

旧大英帝国で構成されるファイブアイズに日本も入るべきという議論を度々耳にする。五カ国はインテリジェンスを共有していると言われるが、この枠組みはアナログの無線通信を主流としていた時代のものである。今はデジタルの有線通信が主流の時代であり、インテリジェンスには陸上と海底の光ファイバーケーブルにおける通信傍受が欠かせない。

日本は今の時代に適した新しい枠組みを提案すべきである。サイバー攻撃の発信源である中国・ロシア・北朝鮮・イランに対抗するために、日米豪印によるクワッドという枠組みに英国を加えた新しいサイバー同盟（JAIBU：Japan, Australia, India, Britain, and United States）を提唱したい。

とくに米国の立場から見れば、大西洋側のパートナーは英国である。一方の太平洋側のパートナーがどこかといえば、おそらく日本しかない。

日本は憲法21条第2項に「検閲は、これをしてはならない。通信の秘密は、これを犯してはならない」とあるため、他国のような諜報活動ができない。しかし、米国の同盟関係国の中で、日本に期待される役割は非常に大きい。

（2021年11月24日に開催されたメディア有識者懇談会における発題内容を整理して掲載）

〈参考文献〉

土屋大洋、2020年、『サイバーグレートゲーム：政治・経済・技術とデータをめぐる地政学』、千倉書房

政策オピニオン　NO.240

サイバーグレートゲーム

―― データをめぐる大国間の争いと日本の対応 ――

2022年4月25日発行

発行所　一般社団法人平和政策研究所

代表理事　林 正寿（早稲田大学名誉教授）

一般社団法人
平和政策研究所
Institute for Peace Policies

住所　〒169-0051 東京都新宿区西早稲田 3-18-9-212
電話　03-3356-0551　　FAX　050-3488-8966
Email　office@ippjapan.org　　Web　https://www.ippjapan.org/