NIDS 防衛研究所
The National Institute for Defense Studies

ロシアのウクライナ侵攻と米英両国のインテリジェンス公表政策
―情報機関の「ジレンマ」と 2014 年以降の安全保障協力の「系譜」

政策研究部グローバル安全保障研究室 研究員 瀬戸 崇志

NIDSコメンタリー
第 224 号 2022 年 5 月 26 日

1. はじめに―米英両国のインテリジェンス公表政策の「ジレンマ」と「系譜」

2022 年 2 月 24 日に始まったロシアのウクライナ全土への軍事侵攻は、その前後での「インテリジェンス(intelligence)[1]」 の多様な機能に光を当てた。特に世界的に注目を集めたのは、米国と英国のインテリジェンス機関（以下：情報機関）の保持するインテリジェンス（機密情報）の一般公表（以下：インテリジェンス公表政策）であろう。2021 年 12 月から 2 月 24 日の開戦前にかけ、米英両国の政府が、ロシア軍の国境付近への集結状況からウクライナでの傀儡政権樹立計画まで、ロシアの軍事侵攻の兆候を続々と暴露した対応は、日本の報道でも、ロシアの偽情報を牽制する情報戦の手法の 1 つと紹介されている。

ただし、今回のロシアの軍事侵攻の前後での米英のインテリジェンス公表政策の機能や将来展望は、以下の 2 点に留意しながら議論する必要がある。第 1 に、米英両国の取組の是非は、各国の実務家・研究者の間でもなお議論が分かれる。それは、情報戦の遂行のための当該施策は、情報機関の伝統的な中核的任務である、情報収集と分析の提供による政策決定・軍の運用への支援の継続との間に「ジレンマ」を突きつけうるからである。米英両国がそのジレンマを緩和しつつ異例の規模・速度での対応を継続できた背景は、近年の先行研究と、ロシアの軍事侵攻を取り巻く作戦・情報環境を見る必要がある。第 2 に、そうした背景への理解は、インテリジェンス公表政策に留まらない米英両国の協力と、その基盤となった 2014 年以来の欧州・環大西洋地域での安全保障協力の「系譜」への目配せも要する。

以上の問題意識を踏まえ、本稿では、ロシアによる軍事侵攻前後での米英両国を軸とするインテリジェンス協力の概要を、2010 年代後半の米英両国と NATO 加盟国間の安全保障協力との連続性も意識しつつ概観する。その後、近年の先行研究を踏まえ、特に軍事侵攻の前段階で米英両国のインテリジェンス公表政策が果たした機能と限界を整理し、同時にインテリジェンス公表政策が各国政府とその情報機関に対して突きつけるジレンマの構造を確認する。最後に、そのジレンマを、米英両国が今回の共同対処のなかで緩和しえた背景を整理しながら、本稿の結論と含意に触れてむすびと代えたい。

[1] この用語は、伝統的には次の 4 つの意味で用いられうる。すなわち、(a)政府のインテリジェンス機関とその共同体（インテリジェンス・コミュニティ）、(b)(a)の任務・活動、(c)(b)の一部である情報収集・分析（任務）の成果物（インテリジェンス・プロダクト）、(d)(c)の成果物の生成・利活用のプロセス（インテリジェンス・サイクル）、である。本稿でもこの立場を踏襲しつつ、原則として政府の対応に焦点を当てる。また、報道などでは「機密情報」と訳される(c)については、後述の理由からインテリジェンスあるいは分析の成果物との表現を用いる。用語の多義性と外延をめぐる議論は以下を参照。川上高司、樋口敬祐、上田篤盛、志田淳二郎『インテリジェンス用語辞典』（並木書房、2022 年）91-93 頁；小林良樹 『なぜ、インテリジェンスは必要なのか』（慶應義塾大学出版会、2021 年）16-18 頁。

2. ロシアの軍事侵攻前後での米英両国のインテリジェンス協力—2021 年晩秋以降の 4 本柱の取組

今回の軍事侵攻をめぐる米英両国のインテリジェンス協力は、ロシアの侵攻計画の情報収集と分析面での連携から始まる。英国放送協会(BBC)の調査報道によれば、とある西側諸国の情報機関がロシアの政権内部での侵攻計画立案の兆候を掴んだのは 2021 年の夏頃であったとされる[2]。そのような兆候を踏まえて水面下で進展した米英連携の過程を経て、2021 年秋頃には、まず米国がロシアの軍事侵攻の蓋然性をめぐる評価を固め、ホワイトハウスを軸に対処方針検討と危機管理体制の構築を進めていく[3]。

その後、米英両国政府は、特に 2021 年の晩秋頃から他の NATO 加盟国や国際社会全体との関係も意識したインテリジェンス協力を加速させていく。一連の取組を、両国がインテリジェンスを共有する範囲と目的に応じて分類していくと、主に次の 4 本柱で整理することができる。

第 1 の柱は、「インテリジェンス外交」とも呼ばれる米英の同盟国との間での水面下でのインテリジェンスの共有と政策調整の試みである。例えば、2021 年 11 月の NATO 首脳会合の前後では、米国から各 NATO 加盟国に対して、ロシアの軍事侵攻計画をめぐる機微なインテリジェンスの共有が行われたとされる[4]。米英両国による NATO 加盟国に対する機微なインテリジェンスの共有と、これを梃とした対ロ政策の調整は、2018 年に発生した英国本土ソールズベリーでの化学兵器使用事案への対処や、その後の中距離核戦力(INF)全廃条約違反の認定に際しても、米英両国が NATO 加盟国との間で実践したロシアに対する国際共同対処の様式である[5]。今回の対応でも、米英両国は同様の様式を踏襲した[6]。

第 2 の柱は、ロシアの軍事侵攻をめぐる開戦の前後でのインテリジェンス公表政策である。その機能と論点は第 3 節以降で扱うため、以下では事実関係と留意点を見ておきたい。まず 2021 年 12 月 3 日に、米国の情報機関が、ウクライナ国境付近でのロシア軍の動員状況や集結拠点を示す衛星画像を含む分析資料を公表した[7]。これ以降も米英両国は、2 月 24 日の侵攻開始までの期間において、国境線での軍の動員状況や予想侵攻時期に加え、ロシアの情報機関によるウクライナ東部での偽旗作戦やウクライナの現政権転覆・傀儡政権樹立計画の存在などを、報道機関などを通じて矢継ぎ早に公表してきた（図表 1）。また 2 月 24 日の開戦後も、米英両国政府ともに記者説明やリークを通じ、戦況の推移を発信する取組を継続しているほか、例えば英国国防省の国防情報部（Defense Intelligence：DI）は Twitter などのソーシャル・メディアを通じて毎日の情勢分析を公表する取組にも着手している[8]。

なお、インテリジェンス公表政策は「機密情報」の公表や開示とも邦訳されるが、ここでは「機密情報」の含意に注意する必要がある。特に、この第 2 の柱のなかで米英両国が公表してきた「機密情報」とは、基本的に収集した 1 次情報(information)に対し、分析と加工を施した成果物(intelligence product)を指す。これは、後述する情報源の保全と分析の質の担保の要請もあり、公表に伴うリスク評価と内容

---

[2] Gordon Corera, “Ukraine: Inside the Spies’ Attempts to Stop the War,” *BBC News*, April 8, 2022, https://www.bbc.com/news/world-europe-61044063.
[3] Ibid.; Ellen Nakashima and Ashley Parker, “Inside the White House Preparations for a Russian Invasion,” *The Washington Post*, February 14, 2022, https://www.washingtonpost.com/national-security/2022/02/14/white-house-prepares-russian-invasion/.
[4] Corera, “Ukraine: Inside the Spies’ Attempts to Stop the War”; Julian E. Barnes, “U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion,” *The New York Times*, February 3, 2022, https://www.nytimes.com/2022/02/03/us/politics/russia-ukraine-invasion-pretext.html.
[5] この点は次を参照。The Intelligence and Security Committee of Parliament (ISC) “Intelligence and Security Committee of Parliament: Russia,” HC 632, July 21, 2020, 37-39, https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.；鶴岡路人「ポスト INF 条約の NATO と欧州安全保障」 日本国際問題研究所編『混迷する欧州と国際秩序』（平成 30 年度外務省外交・安全保障調査研究事業、2019 年 3 月）100-101 頁。
[6] Barnes, “U.S. Exposes What It Says Is Russian Effort to Fabricate Pretext for Invasion.”
[7] Shane Harris and Paul Sonne, “Russia Planning Massive Military Offensive against Ukraine Involving 175,000 Troops, U.S. Intelligence Warns,” *The Washington Post*, December 3, 2021, https://www.washingtonpost.com/national-security/russia-ukraine-invasion/2021/12/03/98a3760e-546b-11ec-8769-2f4ecdf7a2ad_story.html.
[8] Karla Adam, “How U.K. Intelligence Came to Tweet the Lowdown on the War in Ukraine,” *The Washington Post*, April 22, 2022, https://www.washingtonpost.com/world/2022/04/22/how-uk-intelligence-came-tweet-lowdown-war-ukraine/.

調整のうえで機密指定解除(declassification)を行っている[9]。つまり一連の対応は、決して五月雨式に 1 次情報を明らかにする訳でも、分析を裏付ける全ての証拠を詳らかに提示している訳でもない。公表された内容は、その根拠として米英両国が保持する一次情報や、「インテリジェンス外交」で同盟国と水面下で共有しているとみられる成果物と比較し、氷山の一角と理解しておくべきである[10]。

図表 1：2021 年 12 月から 2022 年 2 月 24 日までに米英両国政府が公表した主要なインテリジェンス

年月日	公表国	公表したインテリジェンス（分析の成果物）の概要
2021 年 12 月 3 日	米国	ロシア軍のウクライナ国境付近での動員状況や集結拠点を示した衛星写真を含む分析資料を公表。早ければ 2022 年初頭にも最大 17 万 5000 人規模の兵力を動員した多正面からの軍事侵攻の準備が完了するとの評価を提示。
2022 年 1 月 14 日	米国	ロシアがウクライナへの軍事侵攻の口実を作るため、東部地域での偽旗作戦実施に向けた工作員配備を進めている旨を公表。当該偽旗作戦が 1 月中旬から 2 月中旬に実施され、その数週間後にも軍事侵攻が始まりうるとの評価を提示。
2022 年 1 月 22 日	英国	ロシアによるウクライナの政権転覆工作・傀儡政権樹立計画の存在を公表。傀儡政権の首班候補のイーヴェン・ムラエフ（Yevhen Murayev）元議員を筆頭に、計 5 名のウクライナ側の関係者の実名を暴露。そのうち何名かが、ロシアの情報機関と侵攻準備のため共謀したとの評価を提示。
2022 年 1 月 28 日	米国	国境線に配備されたロシア軍部隊に対して、（動員が通例の軍事演習であるとすれば考え難い）輸血用血液などの医療用物資の配布が始まったとの分析結果を、複数の米政府高官が報道機関に対してリーク。
2022 年 2 月 3 日	米国	ロシアが軍事侵攻の正統化のため、ウクライナ東部におけるロシア系住民虐殺を演出するプロパガンダ映像の作成を進めている旨を公表。情報源の保全のため映像自体は未公表だが、国務省報道官によれば、映像には、ウクライナ政府軍の住民への攻撃を虚証する装備品（例：ウクライナ軍も採用するトルコ製ドローン Bayraktar TB2）、攻撃の跡地、犠牲者の遺体・遺族役などが含まれる。
2022 年 2 月 13 日	米国	米国大統領補佐官（国家安全保障担当）が、ロシアによる軍事侵攻が、北京五輪の閉会（2022 年 2 月 20 日）の前にでも始まりうるとの評価を表明。
2022 年 2 月 16 日- 2 月 17 日	米国 英国	ロシア政府による「国境線地域からのロシア軍の撤退」との声明につき、米英両国政府はそれぞれ、ロシア軍の国境線での動員は継続しており、撤退というロシア側の主張を裏付けうる情報は確認できていない旨の評価を提示。
2022 年 2 月 23 日	米国	48 時間以内にロシア軍の軍事侵攻が開始されることを、ウクライナ政府に対して警告した旨を、報道機関を通じて全世界に対して公表。

（注）米英両国に先駆け、2021 年 11 月にウクライナ国防省[11]が、ロシア軍の国境線での動員規模や予想侵攻経路などの分析を公表している。

（出典）米英両国政府の公刊情報・関連報道を基に筆者作成。

[9] Ken Dilanian et al., “The U.S. Is Using Declassified Intel to Fight an Info War with Russia, Even When the Intel Isn’t Rock Solid,” *NBC News*, April 6, 2022, https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014.
[10] Adam, “How U.K. Intelligence Came to Tweet the Lowdown on the War in Ukraine.”
[11] Howard Altman, “Russia Preparing to Attack Ukraine by Late January: Ukraine Defense Intelligence Agency Chief,” *Military Times*, November 20, 2021, https://www.militarytimes.com/flashpoints/2021/11/20/russia-preparing-to-attack-ukraine-by-late-january-ukraine-defense-intelligence-agency-chief/.

第 3 の柱は、ウクライナや NATO 加盟国のサイバー防衛に対してのインテリジェンスを駆使した支援である。例えば米国サイバー軍は、2018 年以来「ハント・フォワード・ミッション(hunt forward mission：HF 任務)」と呼ばれる、米国の競争国の近隣諸国（以下：接受国）の要請・同意に基づくサイバー軍要員の派遣と、接受国領域内での共同任務を世界各地で展開してきた[12]。

HF 任務は、接受国に対するネットワーク防衛支援の一面と、接受国領内のネットワークなどに残された、近年民間のサイバーセキュリティ産業では「脅威インテリジェンス([cyber]threat intelligence：CTI) 」と呼ばれる技術的情報の収集・分析の一面の双方を含む[13]。米国サイバー軍と国家安全保障局（NSA）は、2018 年以来、この HF 任務を含む海外展開や対外情報収集活動で獲得した CTI を米国の各省・産業界・同盟国の当局との水面下の情報共有や、機密指定解除と一般公表に振り向けることで、米国と同盟・パートナー国双方の官民での脅威状況把握・対処能力強化を支援してきた[14]。

特に HF 任務は、元々がロシアによる米国への選挙干渉対策の一環として始動した経緯もあり、従来からウクライナを含む欧州諸国との共同実施を重視してきた[15]。今回の米国サイバー軍の対応も、こうした欧州での過去の連携の基盤の上に成り立つ[16]。米国サイバー軍と国家安全保障局の要員は、この HF 任務の権限に基づき 2021 年内からウクライナ国内に派遣され、ウクライナ側の要員と共に、同国の重要インフラなどを標的とするサイバー攻撃の脅威の状況把握やネットワーク防衛を支援し、その後も 2 月の開戦前後に要員が増派され、国外からのウクライナと NATO 加盟国への支援を継続してきた[17]。その後にサイバー軍は、ウクライナ情勢に伴う脅威の増大を念頭に、2022 年 2 月から同年 5 月の 3 か月間で、リトアニア外務省や国防関係のネットワークを対象とした HF 任務を完遂した旨も公表した[18]。

第 4 の柱が、ウクライナ軍の通常戦遂行のための開戦後のインテリジェンス支援である[19]。特に、重要な役割を果たしたのが、米英両軍の情報収集・警戒監視・偵察(Intelligence, Surveillance and Reconnaissance：ISR)のアセットと、その NATO 東翼地域での前方展開・運用基盤（図表 2）である[20]。特に 2021 年末以降から、ウクライナと国境を接するポーランドやルーマニアの領空や黒海洋上での有人・無人機双方を含む米英両国軍または NATO が共同保有する航空 ISR アセットの運用の活発化が

---

[12] HF 任務の目的と、地理的な展開範囲は次を参照。Timothy D. Haugh et al., “Agile Collaboration in Defense of the Nation,” in *Ten Years In: Implementing Strategic Approaches to Cyberspace*, ed. Schneider, Jacquelyn G., Goldman, Emily O., Warner, Michael, Newport Papers (Newport, Rhode Island: Naval War College Press, 2020), 97–108; Julian E. Barnes, “U.S. Cyber Command Expands Operations to Hunt Hackers From Russia, Iran and China,” *The New York Times*, November 2, 2020, Online edition, https://www.nytimes.com/2020/11/02/us/politics/cyber-command-hackers-russia.html.

[13] HF 任務は、サイバー軍と接受国による「脅威ハンティング(threat-hunting)」の共同実施ともいえる。CTI と、脅威ハンティングを含むその収集・分析プロセスの類型は、特に次を参照。石川朝久『脅威インテリジェンスの教科書』（技術評論社、2022 年）2-172 頁。

[14] 次を参照。Haugh et al., “Agile Collaboration in Defense of the Nation,” 102–106; Michael Warner, *US Cyber Command’s First Decade*, Aegis Series Paper 2008 (Washington, DC: Hoover Institution/Stanford University, 2020), 18–21; The National Security Agency, “2021 NSA Cybersecurity Year in Review” (Fort Meade, Maryland, February 3, 2022), 3–4, 6, 10, https://media.defense.gov/2022/Feb/03/2002932462/-1/-1/0/2021_NSA_Cybersecurity_Year_in_Review_20220203.PDF.

[15] Sean Lyngaas, “Cyber Command’s Midterm Election Work Included Trips to Ukraine, Montenegro, and North Macedonia,” *CyberScoop*, March 14, 2019, https://www.cyberscoop.com/cyber-command-midterm-elections-ukraine-montenegro-and-north-macedonia/.

[16] Martin Matishak, “One-on-One with the Air Force’s Cyber Chief,” *Recorded Future*, April 18, 2022, https://therecord.media/one-on-one-with-the-air-forces-cyber-chief/.

[17] ナカソネ(Paul M. Nakasone) 米国サイバー軍司令官・国家安全保障局長官の 2022 年 4 月 5 日の米国上院軍事委員会での証言に基づく。次を参照。*Posture Statement of General Paul M, Nakasone Commander, United States Cyber Command Before the 117 th Congress Senate Committee on Armed Services,* 117 th Cong. (2021) *(*General Paul M. Nakasone, Commander, U.S. Cyber Command) 3.

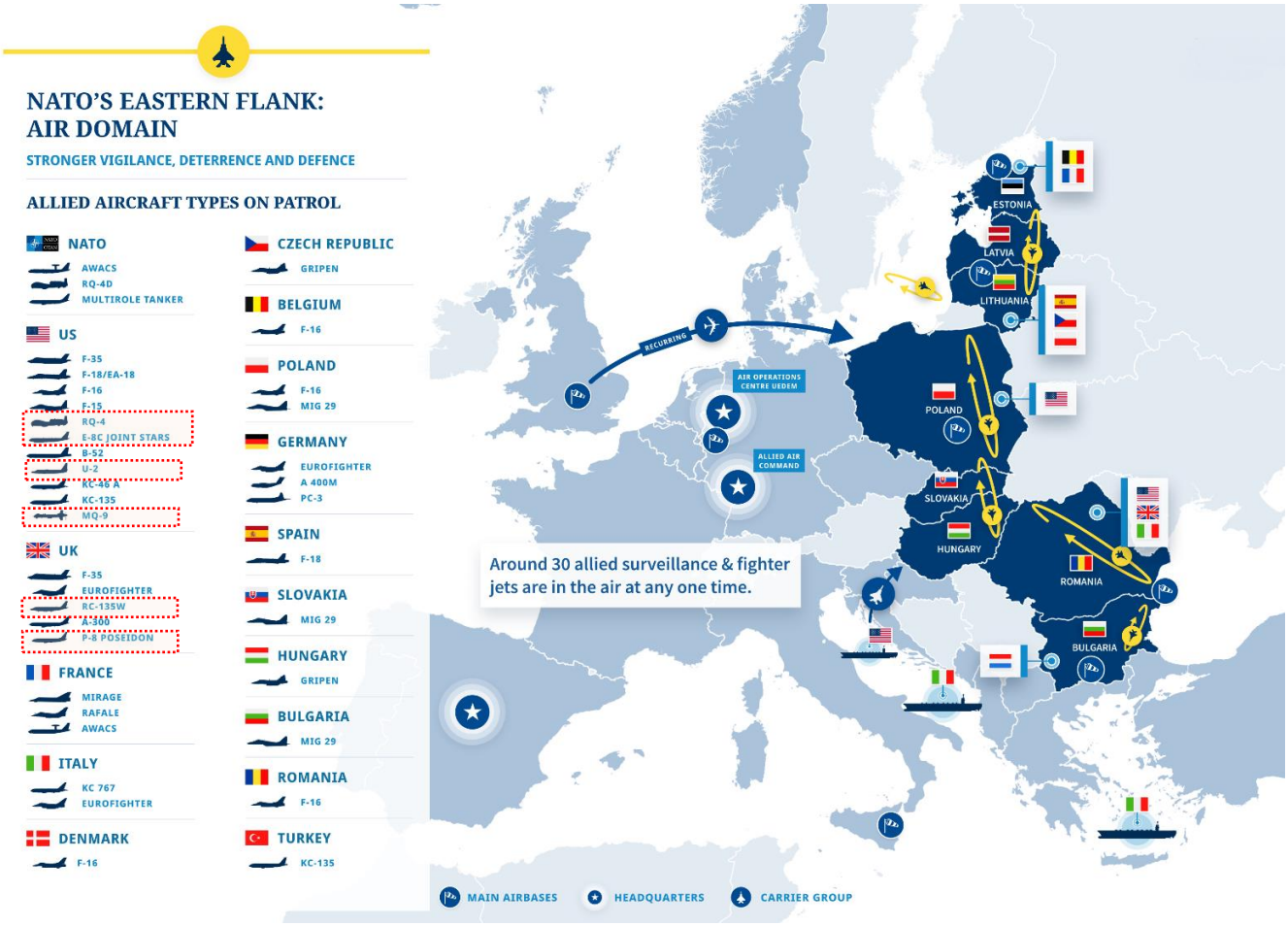
[18] “U.S. Conducts First Hunt Forward Operation in Lithuania,” The United States Cyber Command, May 4, 2022, https://www.cybercom.mil/Media/News/Article/3020430/us-conducts-first-hunt-forward-operation-in-lithuania/.

[19] 匿名の米軍の情報担当者は、特に 2022 年 2 月頃にかけてポーランドやルーマニアなどの NATO 東翼諸国への ISR アセットの増派が行われたと言及している。次を参照。Ken Klippenstein and Sara Sirota, “U.S. Quietly Assists Ukraine With Intelligence, Avoiding Direct Confrontation With Russia,” *The Intercept*, March 17, 2022, https://theintercept.com/2022/03/17/us-intelligence-ukraine-russia/.

[20] Ibid.　なお、NATO 東翼地域での NATO 加盟国の通常戦力の前方展開を支えた態勢と、2014 年以降における態勢強化の経緯は、次を参照。合六強「3 つの‘ショック’に揺れる NATO」日本国際問題研究所編『混迷する欧州と国際秩序』（令和元年度外務省外交・安全保障調査研究事業、2020 年 3 月）99-110 頁。

観測され[21]、一連の ISR 活動は、ロシア軍の位置情報や侵攻目標の把握に重要な役割を果たしてきた[22]。この ISR 活動の成果は、ここまで述べてきた取組での活用[23]は勿論のこと、報道によれば、米国は一連の ISR で収集・分析した情報をウクライナの防空任務支援などのために開戦当初から提供してきたとされる[24]。

図表 2：NATO 東翼地域での NATO 加盟国の航空戦力の前方展開態勢（2022 年 5 月 10 日時点）



（注）網掛けした機種は、2021 年末以降、NATO 東翼地域や黒海での運用が公開情報で確認された米英両国の ISR 関連アセット。
出典：以下 URL の NATO 空軍司令部の画像ならびに本文脚注 19、21、23 の文献をベースに筆者作成。
"Allies Stand Together to Bolster NATO's Eastern Flank," NATO HQ Allied Air Command, May 10, 2022, https://ac.nato.int/archive/2022/nato_eAV_air.

以上の 4 本柱の取組の共通の特徴を 1 つ挙げれば、その戦略的な公表であろう。報道でも取り上げられる第 2 の柱の取組は元より、それ以外の取組も、純粋な軍事的合理性の観点ではこれまで秘匿対象た

[21] こうした ISR アセットのウクライナ周辺国や黒海洋上での運用状況は、「Flightradar24」などを駆使した専門家による公開情報の分析で一定程度が可視化されてきた。アセットの種類や運用状況は次を参照。Thomas Newdick, "This Is The Armada Of Spy Planes Tracking Russia's Forces Surrounding Ukraine," *The Drive*, February 18, 2022, https://www.thedrive.com/the-war-zone/44337/these-are-the-planes-keeping-watch-on-russian-forces-around-ukraine.
[22] Kieran Devine, "Russia-Ukraine Crisis: What Are NATO Spy Planes Doing to Keep Tabs on the Russians?," *Sky News*, February 8, 2022, https://news.sky.com/story/russia-ukraine-crisis-what-are-nato-spy-planes-doing-to-keep-tabs-on-the-russians-12536567.
[23] Larisa Brown, "How Western Spy Planes Keep Tabs on Russian Tactics," *The Times*, March 11, 2022, https://www.thetimes.co.uk/article/how-western-spy-planes-keep-tabs-on-russian-tactics-8slcm0j22.
[24] ただし、当初米国政府・議会内では、ウクライナ政府軍へのターゲティング情報の提供により、米国がロシアから直接の交戦当事者とみなされる可能性への懸念が根強くあり、開戦以降の米国政府からの情報共有の粒度・速度の方針（の説明）は二転三転してきた。次を参照。Ken Dilanian et al., "U.S. Intel Helped Ukraine Protect Air Defenses, Shoot down Russian Plane Carrying Hundreds of Troops," *NBC News*, April 26, 2022, https://www.nbcnews.com/politics/national-security/us-intel-helped-ukraine-protect-air-defenses-shoot-russian-plane-carry-rcna26015.

りえた活動を、その一部とはいえど、ロシアや同盟国などの存在も意識しながら意図的に「見せて」きた一面をもつ[25]。この潮流をおさえつつ、第 3 節以降は第 2 の柱、すなわち、政府による、分析の成果物の機密指定解除と公表という狭義のインテリジェンス公表政策を軸に、その機能と論点を分析する。

3. 論争の出発点と終着点—情報機関の中核的機能と情報収集源・収集手法の保全の要請

インテリジェンス公表政策の議論は、そもそも情報機関の情報収集活動や分析の成果物とは、本来は一般に公表されるものではないとの原則から出発する必要がある。目下の米英両国の対応や将来的含意の評価も、最終的にこの原則との関係で議論されるからである。

公表を控えるべき最大の理由の 1 つは、分析の成果物や情報収集活動自体の一般公表を通じた、情報機関の「情報源と収集手法(sources and methods：以下：情報源)」の喪失への懸念である。分析の公表は、その内容を裏付ける証拠の開示はもとより、仮に結論の提示に留めた場合でも、その公表内容や時期の如何では、その情報源を監視対象や第 3 者が逆探知できてしまう。また、正確な情報源が特定できずとも、情報収集活動の存在の露見自体が、そこから逃れようとする監視対象の対策を通じて、水面下での情報収集活動の継続を破綻させる契機ともなる[26]。

情報機関の中核的機能を、情報収集と分析（の成果物）の提供を通じた、政策決定ならびに軍の運用の支援に見出す限り、インテリジェンス公表政策への慎重論は強くなる。元より分析の適切な共有・活用と情報源の保全による情報収集活動の継続には一定のジレンマがある[27]。しかし、共有範囲を限定せずに内容を誰もが把握可能な一般公表は、特に情報源の保全に対するリスクが高い。この情報源へのリスクは人的情報（human intelligence：HUMINT）ならば文字通り要員の生命を脅かし、そうでなくとも機微な情報源の喪失は、将来における情報収集活動と分析による支援の継続に悪影響を与える[28]。この中核的任務の要請から、情報機関はインテリジェンス公表政策を忌避する組織文化を培う傾向が強い[29]。

以上からインテリジェンス公表政策は、政策決定・軍の運用に対する客観的な情報分析の提供を通じた支援という情報機関の本来任務や行動規範と必ずしも整合的ではない、政治的動機に由来するとの発想が伝統的には通説的立場を占めてきた。

4. インテリジェンス公表政策の機能と限界—ウクライナ侵攻を取り巻く米英の対応の暫定的評価

しかし、近年のインテリジェンス研究は、以上の通説的立場を相対化しつつ、政治的動機に還元できない、よりボトムアップの実務的な動機に導かれた各国のインテリジェンス公表政策の存在を実証的に明らかにしてきた[30]。インテリジェンス公表政策を情報戦の手段とみる議論も、この系譜に位置づけること

---

[25] 第 3 の柱と第 4 の柱の取組の可視化の背後にある論理は、次を参照。Thomas G. Mahnken and Grace B. Kim, “Deterrence by Detection: Using Surveillance to Pre-Empt Opportunistic Aggression,” *NDC Policy Brief* (Rome,: NATO Defense College, January 14, 2021), 2–4; Erica D. Borghard, “U.S. Cyber Command’s Malware Inoculation: Linking Offense and Defense in Cyberspace,” *NetPolitics* (blog) (New York: Council on Foreign Relations, April 22, 2020), https://www.cfr.org/blog/us-cyber-commands-malware-inoculation-linking-offense-and-defense-cyberspace.

[26] 分析の公表と情報源の喪失リスクをめぐる一連の議論は、特に次を参照。Allison Carnegie and Austin Carson, *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation*, 1st ed. (Cambridge: Cambridge University Press, 2020), 28–39.

[27] Ibid., 6–8, 26–33; Jon R. Lindsay, “Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem,” *Intelligence & National Security* 36, no. 2 (February 23, 2021): 261; Timo Steffens, *Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage* (Weisbaden, Germany: Springer Vieweg, 2020), 174.

[28] Ofek Riemer and Daniel Sobelman, “Coercive Disclosure: Israel’s Weaponization of Intelligence,” *War on the Rocks*, August 30, 2019, https://warontherocks.com/2019/08/coercive-disclosure-israels-weaponization-of-intelligence/; Douglas London, “To Reveal, Or Not to Reveal: The Calculus Behind U.S. Intelligence Disclosures,” *Foreign Affairs*, February 23, 2022, https://www.foreignaffairs.com/articles/ukraine/2022-02-15/reveal-or-not-reveal.

[29] Lindsay, “Cyber Conflict vs. Cyber Command,” 269–71; Carnegie and Carson, *Secrets in Global Governance*, 31.

[30] 例えば、2010 年代のイスラエル政府のインテリジェンス公表政策の積極化をめぐる実証研究として次を参照。Ofek Riemer, “Politics Is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States,” *Contemporary Security Policy* 42, no. 4 (October 2, 2021):

ができる。そのような研究は、政府がインテリジェンスの公表によって働きかけたい「ターゲット・オーディエンス（target audience：以下：TA）」と、作用の機序が複数併存することを念頭に置く。この点を踏まえ、近年の先行研究が体系化してきたインテリジェンス公表政策の機能は次の通り整理できる。

第 1 に、現状変更を意図した敵対勢力を TA とみる場合、その目標達成までに保秘が不可欠な作戦の遂行を（一時的に）妨害する機能を持つ。例えば、情報機関の他国内での諜報活動や非公然な工作活動のアセット、偽情報の流布や偽旗作戦の計画、（国家が支援する）武装集団やサイバー攻撃グループの活動基盤など、能力・計画の保秘と政府の関与の否認可能性の喪失が、その作戦の有効性や関与する要員の安全を損ねてしまう場合、暴露による保秘の剥奪は、作戦実施の延期や計画の修正を迫りうる[31]。また、度重なる計画の漏洩や遅延は、政策決定者の自国の軍・情報機関の能力に対する疑義や内通者の存在への懸念を惹起し、作戦の関係者間の疑心暗鬼を誘発する。その結果として生じうる情報共有や意思疎通の混乱は、計画の迅速な再立案を更に困難にする[32]。

第 2 に、同盟国や、敵対者以外の第 3 国の政策当局者・国民世論を TA とみると、情報機関の分析の発出が、情勢認識の収斂や国際的なアジェンダ形成を支える機能を持つ。これは自国の発信した内容を TA に受容させることに加え、英国では「予防反駁（prebuttal）」とも表現される、敵対者の偽情報の流布を機先を制して暴露して潰し、相手方が意図する言説が情報空間を支配することを牽制する機能も含む[33]。

近年の先行研究は、今日の情報環境の特性が、政府がインテリジェンス公表政策という手段で第 2 の機能を追求する意義を強めていると指摘する。リーマー(Ofek Riemer)によれば、情報通信技術（ICT）の発展とメディア機能の拡散により、日々の情報量と流通速度が飛躍的に増大する情報環境下では、公的機関の情報発信ですらも、TA からの注目(attention)の獲得・維持が困難となる。インテリジェンス公表政策は、TA からの情報機関の専門性（実績・権威）に対する信頼や、機密指定を解除する行為自体の異例さを梃として、政府が発信した内容に突出した注目を導出する起爆剤として作用する[34]。

ここで創出された注目は、次の 2 つの機序を通じて分析の公表の効果を増幅する。１つは、ピーターセン（Karen Lund Petersen）が「知識共創（knowledge co-production）」と概念化した、政府の分析の共有・公表が、産業界や市民社会の専門家からの新たな情報提供・分析の呼び水となり、結果として社会全体での脅威状況把握の向上を促す作用である[35]。もう１つは、この知識共創のサイクルの副産物として、政府が公表した分析に対する信頼性が補強されうる。例えばリン・グリーンバーグ（Erik Lin-Greenberg）とミロノポウロス（Theo Milonopoulos）のサーベイ実験・実証研究は、商用衛星画像を駆使した民間企業や市民社会による政府の主張に対する第 3 者検証の提供が、当該分析の当否への信頼性を向上させると共に、世論からの政府（の主張）に対する支持強化を促す機能を示唆している[36]。

554–583.

[31] Ibid., 556–559, 566–570; Ofek Riemer, “Intelligence and the War in Ukraine: The Limited Power of Public Disclosure,” *INSS Insights* (Tel Aviv: The Institute for National Security Studies, March 27, 2022), 6, https://www.inss.org.il/wp-content/uploads/2022/03/no.-1577.pdf; Matthew Armelli et al., *Named but Hardly Shamed: The Impact of Information Disclosures on APT Operations*, SIPA Capstone Project 2020 (Washington, DC: Columbia University’s School of International and Public Affairs[SIPA], 2020), iii , 92-95; “Russian Spooks Are Being Kicked out of Europe En Masse,” *The Economist*, April 7, 2022, https://www.economist.com/europe/2022/04/07/russian-spooks-are-being-kicked-out-of-europe-en-masse.

[32] Riemer, “Intelligence and the War in Ukraine,” 4–5; J. D. Work, “Successful Counter-Cyber Operations Secure US Election,” *Janes Intelligence Review* (Jane’s Group UK Limited, January 28, 2021), 6.

[33] Dan Lomas, “To Brief, Or Not to Brief: UK Intelligence and Public Disclosure,” *RUSI Commentary* (blog) (London: Royal United Services Institute, February 2, 2022), https://rusi.org/explore-our-research/publications/commentary/brief-or-not-brief-uk-intelligence-and-public-disclosure.

[34] Riemer, “Politics Is Not Everything,” 557, 562–566.

[35] Karen Lund Petersen, “Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?,” *Intelligence & National Security* 34, no. 3 (April 16, 2019): 322–324.

[36] Erik Lin-Greenberg and Theo Milonopoulos, “Private Eyes in the Sky: Emerging Technology and the Political Consequences of Eroding Government Secrecy,” *The Journal of Conflict Resolution*, February 8, 2021, 6-8. 22-24.

インテリジェンス公表政策は、米国では古くは冷戦期のキューバ危機の対応にまで遡り、2010 年代のイスラエル政府の取組などを踏まえても、今回の軍事侵攻が世界史上初の事例ではない。しかし今回の米英両国の対応は、その公表の速度・規模・継続性などの面で歴史上類を見ないものであり、同時に、先行研究が理論化してきた機能が十二分に発揮されたものといえる。

まず何よりも、2021 年末からの絶え間ないロシアの侵攻計画の暴露と偽情報への予防反駁は、各国の関心をウクライナ情勢に向けさせ続け、ロシアによるウクライナ軍事侵攻のリスクや、ロシアの行為の正統性の乏しさを世界に印象付けた。この作用は、2014 年のクリミア併合のような電撃的な現状変更を妨害することで時間を稼ぎつつ、従来から対ロ姿勢に温度差がある欧州諸国の連帯を強め、開戦後の制裁措置や兵器供与などの対ウクライナ支援を導く政治的モメンタムの形成を導いてきた[37]。

また、分析の公表後の知識共創機能と信頼性の補完のメカニズムが、ソーシャル・メディアという媒体と結合して増幅された一面も指摘できる。2021 年 12 月の米国の分析資料の公表は、各国の調査研究機関やロシア・軍事専門家による様々な公開情報（open source intelligence：OSINT）による分析の呼び水となり、これらが米英両国の分析内容の妥当性を補完していく。こうした政府機関と、民間・市民社会のプレイヤーの相互作用も、ロシア側の偽情報と言説の優位を相対化する機能を支えたといえよう[38]。

以上の機能を念頭に、この取組の限界も確認したい。この政策の目標は、政策当局の説明や報道では、便宜的に「抑止(deterrence)」とも表現されやすい。しかし、研究者の間では、この用語を用いることへの慎重論は強い。その理由は、インテリジェンス公表政策の TA が敵対者に限定されないことに加えて、そもそもこの取組は、公然たる武力行使で現状変更が可能な能力と意思を持ちうる国家に、その軍事侵攻を躊躇させるコストを課しえないからである。

第 1 の機能としての敵対者への「妨害(disruption)」は、その源流を辿ると通常戦力・核戦力とエスカレーションのリスクを梃とする抑止・強要の論理よりも、どちらかといえば平素からの攻勢的なカウンターインテリジェンスの論理に近い。すなわち、大規模な武力攻撃には至らない敵対者の実力行使は完全にはゼロには出来ないにせよ、その実行に必要な相手方の能力と資源を削ぎ続け、実行を判断する政策決定者に対しても、将来も同種の活動が暴露される政治的リスクを突き付けることで、その烈度と頻度を抑制させる作用を念頭に置く[39]。そのため、防御側による暴露が相手方の戦略目標の達成に裨益しうる場合[40]や、敵対者が、平素からグレーゾーンの事態を超えて公然たる武力行使で現状変更を達しうる能力と意思を持つ場合、この施策単体で実力行使を躊躇させる機能は持ちえない[41]。

---

[37] Dan Lomas, “Weaponizing Truth： UK Intelligence Public Information and Ukraine,” *In-Depth Briefing* (Surrey: The Centre for Historical Analysis and Conflict Research[CHACR], April 22, 2022), 5; Riemer, “Intelligence and the War in Ukraine,” 3–4; London, “To Reveal, Or Not to Reveal.”

[38] Lomas, “Weaponizing Truth,” 3–4; London, “To Reveal, Or Not to Reveal.”

[39] カウンターインテリジェンス政策の文脈での「妨害（disruption）」の機序については次を参照。Hank Prunckun, *Counterintelligence Theory and Practice* (London, United Kingdom : Rowman and Littlefield, 2019), 223–225; Jon Bateman, “The Purposes of U.S. Government Public Cyber Attribution,” in *Managing U.S.-China Tensions Over Public Cyber Attribution*, ed. Ariel E. Levite et al. (Washington, D.C: Carnegie Endowment for International Peace, 2022), 14–24; Jason Healey, Neil Jenkins, and J. D. Work, “Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations,” in *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2020), 255–257.

[40] 特にロシアの情報機関とその隷下のグループは、物理空間・サイバー空間を問わず、その工作活動の目的は標的に対する恐怖と分断の創出であり、防御側の暴露がその戦略目標に裨益しうるゆえに逆効果となるリスクが指摘されてきた。次を参照。Chris Cruden and Nicholas Krohley, “Flunking the New York Times Test: Making Sense of Russian ‘Covert’ Action,” *Modern War Institute* (blog), February 21, 2022, https://mwi.usma.edu/flunking-the-new-york-times-test-making-sense-of-russian-covert-action/; Rory Cormac, Calder Walton, and Damien Van Puyvelde, “What Constitutes Successful Covert Action? Evaluating Unacknowledged Interventionism in Foreign Affairs,” *Review of International Studies* 48, no. 1 (May 24, 2022): 112–113, 126–127. 佐々木 勇人「ロシアを背景とするサイバー攻撃グループによるサボタージュ目的/偽情報作戦としての攻撃活動とその対策について」 『CISTEC journal』第 198 号（2022 年 3 月）68 頁。

[41] Riemer, “Intelligence and the War in Ukraine,” 4; Lomas, “Weaponizing Truth,” 5; Riemer and Sobelman, “Coercive Disclosure: Israel’s Weaponization of Intelligence.”

5. インテリジェンス公表政策のジレンマ―公表に伴う情報源の保全と信頼性の担保の緊張関係

政府によるインテリジェンス公表政策の最大の難問は、公表による情報源の喪失のリスクゆえに、インテリジェンスの公表と、情報収集・分析による政策・運用支援の継続という、2 つの異なる政策ないし任務の目標・要請の間でのジレンマが生じ易いことにある。情報機関の分析の公表は、既述の通り提示する証拠の性質や公表のタイミングにより機微な情報収集源の喪失を導き、その累積は、将来にわたり敵対者の能力と意図を探る重要な情報源の枯渇に繋がりうる。また、ハリントン(Jake Harrington)が指摘するように、情報機関が、以上のリスクを軽視した政策当局による無思慮な公表に不信感を覚えた場合、情報機関が自身の保持する機微な情報を出し渋る誘因を生む。そのため、成果物の公表は情報保全の要請への配慮を踏まえた政策調整が必要なプロセスとなる[42]。

その一方で、情報保全の要請に配慮した公表は、特に第 3 国の政策当局者や国民世論を TA として、脅威認識の共有を試みる第 2 の機能の追求には強い足枷となる。まず、情報保全の要請に配慮した機密指定解除は、公表のリスク精査に時間を要するため、公表の範囲や頻度を制約する。また、情報源の性質によっては、最終的に分析の根拠となった証拠を明かせず、結論のみを述べた成果物の公表に留めざるえないこともあるが、この場合、公表した分析の内容の客観的な検証が困難となり、その分析の妥当性を、情報機関の過去の実績・権威に依拠した TA からの信頼(trust)によってしか担保できない状況を導く[43]。

このような情報源の保全の要請と証拠開示の制約下での取組の継続は、取組の長期化につれて「オオカミ少年」の寓話のように、TA の情報機関に対する信頼と、取組の効果の低下を招く悪循環に陥り易い。情報源の保全と公表する分析の質の両立は、公表の速度と規模の増加につれ困難となるが、情報保全と速度を優先して分析の質（確度）や証拠の提示を犠牲にした公表は、TA からの不信感や、これを煽る敵対勢力の言説に脆弱性となる。その帰結として分析の内容に対する信頼が損なわれていくと、今度は分析の公表による注目の創出が困難となり、これを梃とする一連の効果の追求も難しくなるからである[44]。

6. 米英両国のジレンマの緩和要因―2014 年のクリミア併合以降の安全保障協力から連なる「系譜」

以上のジレンマは、特に 2017 年以降、各国の政府機関によるサイバー攻撃のアトリビューションの公表（パブリック・アトリビューション）などでも問題となってきた[45]。この近年の類例との対比で今回の米英両国の対応をみると、次の 3 つの要因が、両国のジレンマの緩和に寄与してきたといえる。

第 1 に、地理的・技術的・政治的条件が規定した作戦・情報環境自体が、機微な情報源の保全と公表の信頼性の担保のジレンマの緩和に適していた。特に今回の軍事侵攻は、ロシア側の意図をめぐる決定的証拠を示せずとも、侵攻の蓋然性の評価を支えるロシア軍の能力と即応態勢を裏付ける客観的証拠[46]を機微度の低い OSINT も含めて多種多様な情報源で把握し、かつ一部を公表できたことが大きい。

---

[42] 以上の点は、次を参照。Jake Harrington, “Intelligence Disclosures in the Ukraine Crisis and Beyond,” *War on the Rocks*, March 1, 2022, https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/.

[43] 証拠開示の制約に伴う公表した分析の信頼性の低下の問題は次を参照。Carnegie and Carson, *Secrets in Global Governance*, 37–39.

[44] この負の連鎖の問題は次を参照。Harrington, “Intelligence Disclosures in the Ukraine”; Amy Zegart, “The Weapon the West Used Against Putin,” *The Atlantic*, March 5, 2022, https://www.theatlantic.com/ideas/archive/2022/03/russia-ukraine-invasion-classified-intelligence/626557/.

[45] 特に次を参照。Steffens, *Attribution - How to Identify* , 175–176; William Hoverd, “Cyber Threat Attribution, Trust and Confidence, and the Contestability of National Security Policy,” in *Emerging Technologies and International Security*, ed. Steff, Reuben Burton, Joe Soare, Simona R. (London : Routledge, 2020), 221–239; Florian J. Egloff, “Contested Public Attributions of Cyber Incidents and the Role of Academia,” *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 55–81.

[46] 例えば米国は、輸血用血液などの医療物資配給という、軍事侵攻の準備以外では想定し難い挙動のインテリジェンスの公表を、ロシアの軍事侵攻の意図の存在を説得的に示す材料として用いた。ただし、ロシア側の意図の評価は、NATO 加盟国間も必ずしも当初から一枚岩ではなく、「インテリジェンス外交」の過程でも、特に米英両国とドイツ・フランスの間での情勢評価のすり合わせは極めて難航したとされる。以下を参照。Neveen Shaaban Abdalla et al., “Intelligence and the War in Ukraine: Part 1,” *War on the Rocks*, May 11, 2022, https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-1/.

そもそも、ベラルーシ領内を含めたウクライナとの国境地帯における大規模な戦力動員は、その集結拠点や兵站網の秘匿が困難であり、撮像地点を特定できれば、商用衛星画像などの民間への技術拡散が進んだ情報源でもロシア軍の位置情報を把握しやすい。同時に、ウクライナ軍・情報機関による通信傍受から現地住民によるソーシャル・メディアへの投稿まで、侵攻前後のロシア軍の動向を捕捉する様々な現地の情報源も存在した[47]。このように機微度が低い、または情報源が特定されてもロシア側に対策が困難な情報源を活用した米英両国の対応を梃に、世界各国の研究機関や専門家の OSINT での分析も続々と情報空間に流入した。この流れは、米英両国の分析の背後に存在しうる機微な情報源のカバーとなり、同時に分析の信頼性を補強したことで、取組の継続に伴うジレンマの緩和に優位に働いた[48]。

第 2 に、米英両国政府の能力の卓越性である。その中でも特に重要な点は、迅速な機密指定解除の能力基盤と、これを支えた政策当局と情報機関のコミットメントである。例えば米国のインテリジェンス・コミュニティは、今回の対応の中で、情報源の保全と分析の質の担保を両立しながら迅速に分析を公表していく離れ業を成し遂げるため、機密指定解除の専門家と資源を集中的に投下してきた[49]。この対応は、施策の目的や基準をめぐっての政策当局と情報機関の間での共通理解の形成が前提となる[50]。この点で、ロシアによる 2014 年のクリミア併合や 2016 年の米国大統領選挙干渉への対応の教訓などを通じ、米英両国の軍・情報機関でも取組への理解が形成されてきたことも今回の対応を支えた[51]。

最後に、第 2 の点との関連で、2014 年以降の欧州・環大西洋地域における、平素からの安全保障協力が培ってきた基盤を無視できない。2014 年 2 月のクリミア併合に始まり、その後も 2010 年代後半を通じて、ロシアの情報機関が各国で継続してきた非公然な破壊工作活動からサイバー攻撃を駆使した選挙干渉まで、平素からのハイブリッド脅威（hybrid threats）への対処の切迫性が、この 8 年間の NATO・EU 加盟国間での平素からの安全保障協力を深化させてきた[52]。その成果が、NATO 東翼地域での ISR 活動から、ロシアによる軍事侵攻の兆候やサイバー空間上の脅威まで含む様々な機微情報の同盟国との共有に至るまで、第 2 節で触れた残り 3 本柱の協力の基盤となった。そうした基盤は、米英両国が利用可能な情報源の多角化や、公表しうる分析の信頼性を水面下の「インテリジェンス外交」でも補完する共同対処方式[53]を導くことで、間接的に今回の米英両国のジレンマの緩和に寄与した[54]。

このように、今回の米英両国のインテリジェンス公表政策は、2014 年のクリミア併合以降の約 8 年間にわたる欧州・環大西洋地域の安全保障協力の系譜に連なる形で、その機能を発揮できたのである。

---

[47] 今回の軍事侵攻前後におけるウクライナ政府・住民が提供する現地からの情報や、商用衛星画像を始めとした OSINT の役割は次を参照。Neveen Shaaban Abdalla et al., “Intelligence and the War in Ukraine: Part 2,” *War on the Rocks*, May 19, 2022, https://warontherocks.com/2022/05/intelligence-and-the-war-in-ukraine-part-2/ ; Peter Aldhous and Christopher Miller, “How Open-Source Intelligence is Helping Clear the Fog of War in Ukraine,” *Buzzfeed* News, March 3, 2022, https://www.buzzfeednews.com/article/peteraldhous/osint-ukraine-war-satellite-images-plane-tracking-social.

[48] Lomas, “Weaponizing Truth,” 4.;“Expert Views on the War in Ukraine,” *King’s Intelligence and Security Group Blogposts* (blog), April 21, 2022, https://kisg.co.uk/blogposts/f/expert-views-on-the-war-in-ukraine.

[49] Corera, “Ukraine: Inside the Spies’ Attempts to Stop the War.”

[50] Harrington, “Intelligence Disclosures in the Ukraine.”

[51] 近年の米英両国の軍・情報機関における取組への姿勢は、次を参照。Besty Woodruff Swan and Bryan Bender, “Spy Chiefs Look to Declassify Intel after Rare Plea from 4-Star Commanders,” *POLITICO*, April 26, 2021, https://www.politico.com/news/2021/04/26/spy-chiefs-informtion-war-russia-china-484723; Adam, “How U.K. Intelligence Came to Tweet the Lowdown on the War in Ukraine.”

[52] この点の経緯や概要は、例えば次を参照。志田淳二郎『ハイブリッド戦争の時代―狙われる民主主義』（並木書房、2021 年）42-44, 151-170 頁。Peter Poptchev, “NATO-EU Cooperation in Cybersecurity and Cyber Defence Offers Unrivalled Advantages,” *Information & Security An International Journal* 45 (2020): 35–55.

[53] 公表可能な分析の証拠の限定性と信頼性の問題を補うため、同盟国との水面下の「インテリジェンス外交」を通じて分析への支持調達をはかる共同対処方式は、2017 年以降の米英両国による国際共同対処でよくみられた。次を参照。Florian J. Egloff, “Public Attribution of Cyber Intrusions,” *Journal of Cybersecurity* 6, no. 1 (September 14, 2020): 5–8.　瀬戸崇志 「国家のサイバー攻撃とパブリック・アトリビューション―ファイブ・アイズ諸国のアトリビューション連合と SolarWinds 事案対応」『NIDS コメンタリー』第 179 号（2021 年 7 月）4 頁。

[54] 今回の軍事侵攻に至るまでの過程での NATO 加盟国間の「インテリジェンス外交」による評価共有の問題や、2010 年代後半の NATO 加盟国における、ハイブリッド脅威に対するインテリジェンス公表政策での対応の発展は、それぞれ次の文献を参照。Lomas, “Weaponizing Truth,” 4–5; Poptchev, “NATO-EU Cooperation in Cybersecurity and Cyber Defence ,” 42–45.

7. おわりに―個別・具体的な文脈の重要性、1 つの普遍的論点

近年、国家安全保障における心理・認知領域の重要性や、いわゆる情報戦への対応強化が叫ばれるなか、米英両国のインテリジェンス公表政策はその革新性もあり注目を集めている。しかし、その効用にのみ着目した議論は、本稿が触れた施策の内在的限界やジレンマの問題を捨象してしまいかねない。また、今回のロシアの大規模な軍事侵攻を取り巻く作戦・情報環境や、これに影響を与えた 2014 年以降のクリミア併合以降の欧州・環大西洋地域での安全保障協力も、米英両国の空前の規模での対応を支えた要素として無視できない。米英の取組の評価や将来展望は、以上の点を踏まえて論ずる必要がある。

欧米の専門家の間でも、今回の軍事侵攻の前後での米英両国のインテリジェンス公表政策は一定の効果を挙げてきたと見る立場は強い。ただし、ここで留意すべきは、評価の念頭にある施策の目標設定である。米英両国はウクライナ情勢への通常戦力での軍事介入とロシアとの直接交戦の選択肢を排除しており、したがって両国に残るオプションは、2014 年 2 月のクリミア併合のようなロシアの電撃的な現状変更と既成事実化を妨害して時間を稼ぎ、ウクライナ軍の防衛戦を兵器供与などで支え、国際社会の対ロ制裁・圧力を維持・強化し続ける他にはない。今回の米英の政策対応に向けられた評価は、こうした制約条件下の戦略目標を達する手段としての有用性を念頭に置くものといえる[55]。

この点で、この取組の価値と費用対効果は、異なる地理的環境・形態・戦略目標を伴う危機や武力紛争に応じて変わりうる[56]。その分析は本稿の射程を超えるが、例えばインド太平洋地域や中東を含め、米国・英国が介在しうる異なる地域での同種の施策の意義は、各地域の平素からの安全保障協力の文脈や、想定されうる武力紛争の作戦・情報環境を踏まえた別個の議論が必要となろう。

その一方、現時点でウクライナをめぐる各国のインテリジェンス協力の事例に普遍的含意を見出すとすれば、それは「インテリジェンスとはかくあるべきか」という、インテリジェンス研究の根源的命題を、21 世紀の情報環境のなかで問うたことかもしれない。

例えば、今回のインテリジェンス公表政策を取り巻く一連の流れは、ICT の発展を基盤とした OSINT の有用性を示し、同時に、非営利の調査研究機関から Twitter 上で著名な軍事専門家に至るまで、伝統的な政府のインテリジェンス・サイクルの外側に居たプレイヤーが脅威状況把握や脅威認識の形成において果たす役割の大きさを印象付けた[57]。また、情報機関の機能・任務という側面に着目すると、確かに各国の情報機関は情報収集・分析による政策決定と軍の運用支援を一義的には担うにせよ、それを超えた任務の有無や、複数の任務の要請が競合した場合の優先順位は、米英両国を含めて歴史的に自明でも普遍的でもない[58]。この点で、今回の米英両国のインテリジェンス公表政策は、21 世紀の情報環境に適応しうるように、情報機関が自身の任務や秘密主義を規範とする組織文化の調整を迫られていることの証

---

[55] 本文で既述の通り、そもそも「（敵対国の）通常戦力による軍事侵攻の抑止」は、この施策には達成不可能なゴールポストといえる。また、仮に米英両軍の直接軍事介入が想定しえたのであれば、軍に対する運用支援の継続のための情報源の保全の要請から、今回と異なる対応に合理性が見出された可能性を指摘する声もある。次を参照。 Lomas, “Weaponizing Truth,” 5.

[56] 例えば、地理的作戦環境の差異に伴う情報源の多寡の問題を指摘するものとして、次を参照、Lomas, “Weaponizing Truth,” 5.

[57] この点は次を参照。Alexa O’Brien, “Open Source Intelligence May Be Changing Old-School War,” *Wired*, May 24, 2022, https://www.wired.com/story/open-source-intelligence-war-russia-ukraine/?utm_source=twitter&utm_medium=social&utm_campaign=onsite-share&utm_brand=wired&utm_social-type=earned
; Benjamin Strick, “Follow the Russia-Ukraine Monitor Map,” Bellingcat, February 27, 2022, https://www.bellingcat.com/news/2022/02/27/follow-the-russia-ukraine-monitor-map/.

[58] この点は次を参照。Mark Stout and Michael Warner, “Intelligence Is as Intelligence Does,” *Intelligence & National Security* 33, no. 4 (June 7, 2018): 517–526; James Lockhart and Christopher R. Moran, “Principal Consumer: President Biden’s Approach to Intelligence,” *International Affairs* 98, no. 2 (March 7, 2022): 552–554; Rory Cormac, *Disrupt and Deny: Spies, Special Forces, and the Secret Pursuit of British Foreign Policy*, 1st ed. (Madison Avenue; New York: Oxford University Press, 2018), 7–15.

左ともいえる[59]。同時に、当該施策をめぐる論争の構図自体が、任務とプレイヤーの多様化に伴う情報機関の役割の変容や、ICT の拡散によって透明性が増し続ける世界でなお残る政府機関の秘密性（secrecy）の役割をめぐる近年の専門家の論争とも一種の相似形をなす[60]。こうした、今回のロシアの軍事侵攻に限定されないダイナミックな論争も踏まえて、今回の米英の取組と展望を見ていくことは、インテリジェンスの機能と外延の議論が自明視されがちな日本では、実務的にも学術的にも重要な試みといえよう。

（2022 年 5 月 25 日脱稿）

プロフィール profile

政策研究部
グローバル安全保障研究室
研究員　瀬戸　崇志
専門分野：安全保障・インテリジェンス研究
サイバーセキュリティ

防衛研究所企画部企画調整課
直　通 ： 03-3260-3011
代　表 ： 03-3268-3111（内線 29177）
ＦＡＸ ： 03-3260-3034
※ 防衛研究所ウェブサイト：http://www.nids.mod.go.jp/

[59] 米英両国の近年の姿勢の参考としては、例えば次を参照。Jeremy Fleming, “Director GCHQ’s Speech on Global Security amid War in Ukraine” (Australian National University, March 31, 2022), https://www.gchq.gov.uk/speech/director-gchq-global-security-amid-russia-invasion-of-ukraine; Mathew J. Schwartz and Ron Ross, “Intelligence Agencies Seek Fast Cyber Threat Dissemination,” *Bank Info Security*, April 25, 2019, https://www.bankinfosecurity.com/intelligence-agencies-seek-fast-cyber-threat-dissemination-a-12415.

[60] このような情報機関の役割の変容（拡大）をめぐる問題は次を参照。Petersen, “Three Concepts of Intelligence Communication,” 322–325; Dennis Broeders, Sergei Boeke, and Ilina Georgieva, *Foreign Intelligence in the Digital Age. Navigating a State of “Unpeace,”* The Hague Program For Cyber Norms Policy Brief (Hague: The Hague Program for Cyber Norms/Leiden University, 2019); Jamie Collier, “Getting Intelligence Agencies to Adapt to Life Out of the Shadows,” *NetPolitics* (blog) (Council on Foreign Relations, April 5, 2017), https://www.cfr.org/blog/getting-intelligence-agencies-adapt-life-out-shadows; Harrington, “Intelligence Disclosures in the Ukraine.” また、NATO 加盟国間の「インテリジェンス外交」の例をはじめ、OSINT の価値が増大しても残る情報機関の機密情報共有の意義や、今回の軍事侵攻に留まらない文脈での、政府機関の取組の秘密性の機能をめぐる論争は、以下の各文献を参照。Joshua Rovner, “Intelligence and War: Does Secrecy Still Matter?” *War on the Rocks*, May 23, 2022, https://warontherocks.com/2022/05/intelligence-and-war-does-secrecy-still-matter/; Allison Carnegie, “Secrecy in International Relations and Foreign Policy.” *Annual Review of Political Science* 24, no.1(May 2021): 213-33.