

第2章 核抑止と軍備管理 ——新領域・新興技術の視点から——

有江 浩一

はじめに

今日、陸海空の伝統的な戦闘領域は、宇宙・サイバー・電磁波・認知などの新たな領域との結びつきをますます強めつつある。2022年2月に始まったロシアによるウクライナ侵攻では、ウクライナの衛星通信がサイバー攻撃や電磁波による攻撃に晒され、インターネットなどの通信サービスが途絶する被害が出ている¹。また、軍事作戦ではないが、2024年1月の台湾総統選に際して、中国がディープフェイクや偽情報などによる大規模な認知戦を展開して選挙干渉を行ったと報じられている²。

こうした新領域の影響は核の領域にも及びつつある。2024年2月、ロシアが宇宙空間で人工衛星を攻撃するための新たな核兵器を開発しているとの疑惑が報じられた³。もともと宇宙領域は冷戦の時代から核の領域との関わりが強かったが、近年では様々な技術の進展と相まって両者の関連が更に強くなっているように思われる。また、サイバー領域も核の領域に影響を及ぼしつつあり、その代表例としては2010年に公表されたスタックスネット事案が挙げられる。スタックスネットはイランのナタンズにあるウラン濃縮施設の遠心分離機の制御システムに侵入し、遠心分離機1,000基以上に物理的損害を与えたマルウェアで、インターネッ

¹ Juliana Suess, “Jamming and Cyber Attacks: How Space is Being Targeted in Ukraine,” RUSI, April 5, 2022; James Pearson, “Russia Downed Satellite Internet in Ukraine – Western Officials,” *Reuters*, May 11, 2022.

² Helen Davidson, “Cognitive Warfare and Weather Ballons: China Accused of Using ‘All Means’ to Influence Taiwan Vote,” *Guardian*, January 9, 2024.

³ Johnny Franks, “Russia to Deploy Space-Based, Nuclear Anti-Satellite Weapon,” *Warrior Maven*, February 18, 2024.

トに接続されていない端末に USB メモリを用いて仕掛けられたとされている⁴。さらに、電磁波領域についても、近い将来に指向性エネルギー兵器を使用して戦域レベルの核兵器の誘導システムや通信を機能不全に陥らせ、これらの核兵器を無力化することも可能になるかもしれないと指摘されている⁵。

新領域の影響を考える上で見逃せないのが、人工知能 (AI) や極超音速兵器、量子技術などの新興技術の進展である。今後 AI が宇宙領域での戦いに導入される可能性があるとは指摘されているように⁶、新興技術は新領域での戦いのイネーブラーとして作用するという側面を有し、新領域の動向に少なからぬ影響を及ぼすものと考えられる。AI はサイバー領域にも導入されていくとみられており、AI を活用した高度なサイバー攻撃によって核ミサイルを搭載した戦略原子力潜水艦 (SSBN) がハッキングされる可能性も将来的には否定できないという⁷。

このように、新領域・新興技術の影響が核の領域にも及びつつあることに鑑みて、かかる動向が核抑止を安定化させるのか、それとも不安定化させるのかを本稿で検討してみたい。その上で、新領域・新興技術が核抑止の不安定化を招く場合には、その安定化を図るための政策課題は何かを考察し、最後に新領域・新興技術に係る軍備管理について付言する。

新領域・新興技術は核抑止を安定化させるか？

核保有国の核兵器システムのうち、早期警戒や指揮・通信といった中核的な機能を果たすのは核指揮統制通信 (nuclear command, control, and communications: NC3) と呼ばれるシステムであるが、NC3の機能の多くは人

⁴ Bishr Tabbaa, “Zer0 Days: How Stuxnet Disrupted the Iran Nuclear Program and Transformed Computer Security,” *Medium*, July 17, 2020.

⁵ Justin Anderson and James R. McCue, “Deterring, Countering, and Defeating Conventional-Nuclear Integration,” *Strategic Studies Quarterly*, Spring 2021, p. 48.

⁶ Charles Beames, “AI in Space and Its Future Use in Warfare,” *Forbes*, December 21, 2022.

⁷ James Johnson, “The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability,” *Journal of Cyber Policy*, vol. 4, no. 3, 2019, p. 448.

工衛星に依存している⁸。これらの衛星は物理的な攻撃や電磁波・レーザーによる妨害などに脆弱であり、サイバー攻撃の標的にもなりやすい。衛星のみならず、NC3を構成する様々なコンピュータシステムや通信ネットワークもサイバーや電磁波などの新領域における攻撃に脆弱である。

他方で、現在まで核保有国のNC3に対する重大な攻撃は行われていない。その要因として、宇宙やサイバーなどの新領域においてNC3への先制攻撃を行えば、何らかの重大な報復を受けることは避けられないと関係国が認識していることが挙げられよう。例えば、米国と中国がともに宇宙・サイバー領域での軍事能力を増大させた結果、これらの領域における攻撃に対して相互に脆弱な状態になりつつあることから、両国がこうした攻撃を相互に自制することはあり得ると指摘されている⁹。つまり、新領域において関係国の間に一定の相互脆弱性(mutual vulnerability)が成立しているとするならば、これが関係国に慎重さを促し、危機の安定性を高めているとも考えられる¹⁰。

新領域における攻撃手段が、攻撃側にとって意外と使いづらいものであることも攻撃を自制させる要因となり得る。例えば、宇宙領域における先制攻撃の手段として、標的となる衛星と同一軌道に電磁波放射装置を搭載した衛星を配備し、これを標的衛星に近接させて電磁波攻撃を行わせることが考えられる。ただし、こうした衛星による電磁波攻撃は、対衛星攻撃手段としては技術的なコストや制約が大きい上に、標的衛星への特異な近接行動が宇宙状況把握(SSA)活動によって捕捉される蓋然性も高いため¹¹、攻撃の準備及び実行には相当の困難を伴う。

⁸ Marie Villarreal Dean, "U.S. Space-Based Nuclear Command and Control: A Guide," Center for Strategic and International Studies, January 13, 2023, pp. 1-5.

⁹ David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, D.C.: National Defense University Press, 2011), pp. 2-7.

¹⁰ Jacek Durkalec, Paige Gasser, and Oleksandr Shykov, "Multi-Domain Strategic Competition: Rewards and Risks," Workshop Summary, Center for Global Security Research, Lawrence Livermore National Laboratory, November 2018, p. 12.

¹¹ Sitki Egeli, "Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability," *Journal for Peace and Nuclear Disarmament*, vol. 4, no. 1, 2021, pp. 124-125.

また、サイバー攻撃についても、攻撃の効果を正確に判定することが難しい上に、2010年のスタックスネット事案や2017年のNotPetya事案のようにマルウェアが標的衛星のみならず攻撃側を含めた世界中のネットワークに侵入する事態を引き起こす恐れがある¹²。

新興技術をNC3に導入することにより、相手国の核兵器システムに対する情報収集・監視・偵察 (ISR) 能力及び収集した情報の分析能力が向上し、核使用の判断をより適正に行うことが可能になるかもしれない。例えば、AIをNC3の早期警戒システムに導入して相手国の核態勢に係る動向を正確に把握することができるようになれば、相手国は秘密裏に核攻撃の準備を行うことが難しくなる。そうなれば、相手国による核使用の脅しが本物なのか否かを正しく見極めることが可能になるため、抑止の信頼性が高まり、危機の際に偶発的なエスカレーションの危険を減らすことにつながるであろう¹³。また、量子技術を応用した高感度なセンサーにより、潜航中のSSBNによって引き起こされる磁場や重力などの変化を計測して探知・追跡を容易にすることも考えられる¹⁴。このように、量子センサーによって相手国のSSBNの動向を事前に探知することが可能になれば、相手国による核使用の脅しにも冷静に対応することが可能になり、核使用判断の適正化に寄与するであろう。

新領域・新興技術は核抑止を不安定化させるか？

一方で、新領域での攻撃は、核保有国の報復第二撃能力を脆弱化させ、核抑止を不安定化させる側面を有する。前述のように、報復第二撃能力を担保するNC3は新領域での攻撃に脆弱であり、NC3を構成する各種の衛星が攻撃を受

¹² James Timbie and James O. Ellis Jr., “Technology, Complexity, Uncertainty, and Deterrence,” Kissinger Center Papers, May 2023, p. 18.

¹³ Edward Geist and Andrew J. Lohn, “How Might Artificial Intelligence Affect the Risk of Nuclear War?” RAND Corporation, 2018, p. 21.

¹⁴ Katarzyna Kubiak, “Quantum Technology and Submarine Near-Invulnerability,” European Leadership Network, December 2020, pp. 3-9.

けて破壊され、あるいは機能不全に陥った場合は核報復を実行できなくなる恐れがある。また、サイバー攻撃によって NC3 の早期警戒システムが攪乱される、通信が遮断されて核攻撃命令を受信できなくなる、若しくは核運搬システムのソフトウェアが破壊されて発射できなくなるといった事態は、核保有国の報復第二撃能力を脆弱化させるであろう¹⁵。

新興技術の導入も核抑止の不安定化を招く恐れがある。AI・極超音速兵器・量子技術などの新興技術は、核兵器を探知・追跡し、これを精密に打撃して破壊する能力を向上させ、報復第二撃能力の脆弱化に寄与することで核抑止の不安定化を招くものと考えられる。ある研究によれば、AI やクラウドコンピューティング、データアナリティクスなどの新たな技術の導入によって核保有国の報復第二撃能力、特に地上移動式の核ミサイルを容易に探知・追跡できるようになると、核抑止の不安定化につながるという。具体的には、ある核保有国が、AI などで強化された相手国の ISR システムで探知・追跡されないようにするために核ミサイルを移動・分散しようとし、その動きを探知した相手国が核戦争も辞さないというシグナルだと誤解してしまうことによって、第一撃の誘因が高まるというわけである。また、AI の導入による報復第二撃能力の脆弱化を恐れた核保有国が核戦力の増強に乗り出し、核軍備競争を引き起こすリスクもあるという¹⁶。

新領域での攻撃が攻撃側の意図しない形でエスカレーションを起し、あるいは被攻撃側の誤認によって核兵器が使用されかねない事態に発展する可能性もある。特に、米中露の3か国は相互の NC3 を標的とし得る対宇宙能力やサイバー攻撃能力を高めつつあり、これらの能力による自国の NC3 への奇襲攻撃が戦略的安定を損なうとの認識を互いに共有している。国際危機の際には、3か国の軍隊は自国の核兵器システムに対する攻撃の兆候を見逃すまいと監視態勢を強化するであろう。こうした状況下で、米中露が関わる局地的な非核（通常）戦争が生

¹⁵ Eva Nour Repussard, “Cyber-Nuclear Nexus: How Uncertainty Threatens Deterrence,” Project on Nuclear Issues, CSIS, May 10, 2023.

¹⁶ Paul Bracken, “The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race,” Foreign Policy Research Institute, September 21, 2020.

起した場合、非核作戦の効果を高めようとして相手国の非核作戦を支援している指揮統制システムを標的とする対宇宙あるいはサイバー手段による攻撃が行われることが考えられる。しかし多くの場合、米中露の非核作戦用の指揮統制システムは NC3 と両用となっている¹⁷。このため、意図的に NC3 を外して非核作戦用の指揮統制システムだけを攻撃しようとしても、結果的に NC3 への攻撃となってしまうことで、核へのエスカレーションを招くリスクが高まることになる。

新興技術が核兵器システムに導入されていけば、誤解、誤認、誤算あるいは事故などによる意図しない核兵器使用のリスクが高まると懸念されている¹⁸。特に、NC3 への AI の導入は核抑止を不安定化させる点でより深刻である。AI は NC3 の通信、早期警戒、意思決定支援、報復攻撃の自動化の 4 分野に導入されると考えられる¹⁹。このうち特に論争的なのは意思決定支援と報復攻撃の自動化である。意思決定支援については、AI の意思決定のアルゴリズムが意図しない行動をもたらし、偶発的な核戦争にエスカレートするリスクを高めることが懸念される²⁰。また、報復攻撃の自動化では、ロシアがソ連時代に整備したとされる自動核報復システムが例として挙げられる。これは、核攻撃を受けてロシアの指導部が壊滅する事態に備えたシステムであるが、同システムのセンサーが隕石の落下などの自然現象を核攻撃と誤認する可能性があり、これによって意図しない核使用が行われるかもしれないと指摘されている²¹。

¹⁷ Benjamin Bahney and Anna Peézei, “The Role of Nuclear-Conventional Intermingling on State Decision-Making and the Risk of Inadvertent Escalation,” NSI, November 2021, pp. 7-8.

¹⁸ 戸崎洋史「新興技術と核抑止関係」日本国際問題研究所、2021年3月30日。

¹⁹ Jill Hruby and M. Nina Miller, “Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems,” NTI, August 2021, pp. 12-25.

²⁰ Amber Afreen Abid, “Artificial Intelligence in the Nuclear Age,” Strategic Vision Institute, October 4, 2023.

²¹ Anthony M. Barrett, “False Alarms, True Dangers? Current and Future Risks of Inadvertent U.S.-Russian Nuclear War,” RAND Corporation, 2016, p. 11.

核抑止の安定化を図るための政策課題

新領域・新興技術が核抑止を不安定化させる可能性があるのであれば、その安定化を図る上での政策的課題は何かを考えてみたい。

まず、直接抑止 (direct deterrence) の安定化について考察する。第一に、新領域をめぐる抑止について、関係国の間で認識の共有を図る必要がある。特に、新領域でのいかなる活動が許容されるのか、あるいは許容されないのかについての関係国相互の理解を暗黙のうちに得ていく努力が重要になる。ただし、こうした暗黙の相互理解がまだ十分でないうちは、例えばサイバー領域においてある国々が著しく破壊的な攻撃の実行を正当化しようとする潜在的可能性がある。また、許容し得るサイバー攻撃とは具体的にいかなる種類のものなのかに関する関係国の理解が曖昧で不明確になりがちであるために、意図しない偶発的なエスカレーションが起り得る。さらに、新領域での関係国相互の競争的な活動が長く続いた結果、相対的なパワーシフトが生じて力関係が不安定化し、武力紛争に至る可能性もある²²。このため、新領域において比例性を担保し得る攻撃は何か、またどのような攻撃がエスカレーションを招きやすいのかを判断するための共通の枠組みを潜在的敵対国との間で共有すべきであろう²³。

第二に、新領域での脅威の出現状況を継続的に把握し、NC3への脅威を早期に発見し得る体制を整えることも重要な政策課題である。既に米軍は宇宙・サイバー領域の監視体制を整え、SSA活動やサイバー領域の監視活動などを継続的に行っている。しかし、NC3に対する全ての脅威を把握できるわけではない。SSAについては、宇宙デブリなどの宇宙物体を監視し、これらが衛星に衝突するのを回避するための能力は向上しており、衛星に対する物理的な攻撃を把握することもある程度可能と思われるが、非物理的な攻撃の把握は難しいであろう。サイバー領域についても、サイバー攻撃に対する鑑識技術が発達してきてはいるも

²² Michael P. Fischerkeller and Richard K. Harknett, "What Is Agreed Competition in Cyberspace?" *Lawfare*, February 19, 2019.

²³ Vincent Manzo, "Deterrence and Escalation in Cross-Domain Operations: Where Do Space and Cyberspace Fit?," *Strategic Forum*, no. 272, December 2011, pp. 3-7.

の、サイバー攻撃の技術も常に進化していることから鑑識にも限界がある²⁴。これらの問題を克服するには大きなコストがかかると予想されるが、新領域におけるNC3への様々な脅威を早期に発見し、核抑止の不安定化を防ぐためには必要な投資と考えるべきであろう。

第三に、核抑止の不安定化への対策として、NC3のレジリエンス向上を図っていかなければならない。特にNC3の衛星など宇宙アセットのレジリエンス強化は喫緊の課題であり、拒否的抑止の態勢を整える上でも重要である。具体的な方策として、デコイ衛星や護衛手段を軌道上に配備するほか、衛星の数を増やすことなどが挙げられる²⁵。

次に、拡大抑止 (extended deterrence) の安定化への課題について、米国の拡大核抑止の供与を受ける「核の傘」国に焦点を置いて考察する。第一に、新領域における攻撃が米国ではなく、「核の傘」国に指向された場合の対応を考えておく必要がある。考え得る事態としては、「核の傘」国の宇宙アセットがジャミングなどの非物理的攻撃を受けた場合、あるいは「核の傘」国の指揮統制システムがサイバー攻撃を受けた場合などが挙げられる²⁶。いずれの場合も、拡大抑止の不安定化を招かないためには、同盟として抑止・対処すべき事態と「核の傘」国が独力で対応する事態について役割分担をできる限り明確にしておく必要がある。

第二に、新興技術が核抑止を不安定化させる可能性について、「核の傘」国として米国と認識を共有しておくことも重要であろう。例えば、AIを米国のNC3に導入する場合、NC3のいかなる機能にAIを活用するのか、導入によって核抑止が不安定化することはないのかなどの点について米国と協議し、認識を一致させておくことができれば望ましい。また、非核作戦を支援するシステムにAIが導入され、その非核システムとNC3が接続された場合の核抑止上の課題についても協議しておく必要がある。現在、米国は米軍の全てのセンサーとシューターをリア

²⁴ 鈴木一人「安全保障の空間的変容」『国際問題』no. 658 (2017年1・2月) 10頁。

²⁵ Michael P. Gleason and Peter L. Hays, “Getting the Most Deterrent Value from U.S. Space Forces,” Center for Space Policy and Strategy, October 2020, pp. 4-5.

²⁶ Dean Cheng, “Prospects for Extended Deterrence in Space and Cyber: The Case of the PRC,” Heritage Foundation, January 21, 2016.

ルタイムで接続して戦う能力を目指す「統合全ドメイン指揮統制 (JADC2)」構想を推進中である²⁷。将来的に JADC2 構想が米軍の非核作戦を支援する新たな指揮統制システムに収斂していき、そのシステムに AI が導入され、それが NC3 と接続されていく可能性は否定できない²⁸。先述したように、そもそも非核作戦用の指揮統制システムは NC3 と両用となっていることから、JADC2 システムへの AI 導入は NC3 にも影響を及ぼし得るものと理解すべきであろう。この点も踏まえつつ、「核の傘」国は新領域をめぐる拡大核抑止のありようについて米国と協議を深めていくべきと考える。

第三に、「核の傘」国の立場から、新領域・新興技術をめぐる拡大核抑止のアジェンダを提起し、同盟の核政策に反映させていく取組を進めることも考えられよう。このための場として、NATO には加盟国のほぼ全てが参加する NATO 核計画グループ (NPG) による核協議の枠組みがある。インド太平洋地域においては、NATO の NPG のような多国間の枠組みは存在しないものの、米国との二国間同盟における核協議の中で「核の傘」国が新領域をめぐる拡大核抑止のアジェンダを提起することは可能であろう。

新領域・新興技術に係る軍備管理

新領域・新興技術が核抑止を不安定化させる可能性に鑑みて、いかなる軍備管理を追求すべきであろうか。まず、宇宙領域をめぐるのは、対衛星攻撃能力が NC3 の宇宙アセットに対する脅威となっていることから、核抑止の不安定化を防止する観点からは、当該能力の規制が宇宙における軍備管理上の焦点と考えられる。これについて、中国とロシアが宇宙における兵器配置を規制するための軍備管理条約を目指す姿勢を堅持しているのに対して、米国など西側諸国は宇宙

²⁷ 菊地茂雄「中国の軍事的脅威に関する認識変化と米軍作戦コンセプトの展開——統合全ドメイン指揮統制 (JADC2) を中心に——」『安全保障戦略研究』第 2 巻第 2 号 (2022 年 3 月)。

²⁸ Michael Klare, “The Military Dangers of AI Are Not Hallucinations,” *Foreign Policy in Focus*, July 14, 2023.

の安全保障に対する最大の脅威は特定の兵器などではなく軌道上における「行動 (behavior and actions)」であると考えており、宇宙における責任ある行動の規範を目指すアプローチを採っている²⁹。西側諸国がこうした行動規範アプローチを追求する背景には、宇宙における「兵器」とは何かを定義することが難しいため、中露が追求するような特定の兵器の規制・管理を目指した従来の軍備管理のアプローチでは実効性に欠け、検証が事実上不可能になるとの認識がある。

次に、サイバー領域をめぐっては、宇宙と同様に、サイバー領域における「兵器」とは何かを定義することは困難であり、従来の軍備管理アプローチでは実効性や透明性を確保できない恐れがある。このため、「サイバー兵器」の禁止あるいは規制を目指す従来のアプローチではなく、例えば NC3 を標的とするサイバー攻撃といった「行動」を規制の対象とするように、核抑止を不安定化させる「行動」に対して規制をかけることが軍備管理上意味のある方策だということができる。

電磁波領域についても、指向性エネルギー兵器が戦域以下のレベルの核兵器システムを無力化し得る潜在的可能性があることに鑑みて、これらの核兵器システムに対する指向性エネルギー兵器の使用を規制する枠組みを検討することが望ましい。特に、NATO 加盟 5 か国への配備が進められている米国の B61-12 戦術核爆弾には命中精度を高めるための慣性誘導装置が搭載されており³⁰、この誘導装置が指向性エネルギー兵器の影響を受ける恐れがあるとすれば、こうした枠組みは NATO の核抑止の安定化に寄与すると思われる。ただし、指向性エネルギー兵器そのものに規制をかける従来のアプローチではなく、核抑止を不安定化させる恐れのある指向性エネルギー兵器の使用という「行動」を規制の対象とする規範的アプローチを追求することが望ましいであろう。

新興技術が NC3 に導入された場合の核抑止上のリスクに鑑みて、これを規制するための軍備管理も必要である。とりわけ AI について、AI は核保有国が自信を持って NC3 に組み込めるだけの技術的成熟度に至っていないとして、核抑

²⁹ Victoria Samson, “Breaking the Impasse over Security in Space,” Arms Control Association, September 2022.

³⁰ “B61-12 Nuclear Bomb,” *Airforce Technology*, November 6, 2020.

止を不安定化させて核使用の可能性を高める恐れのあるAIの活用を規制するよう核保有国間で早期に合意すべきだとの指摘がある³¹。この指摘のように、AIを「兵器」として規制をかける従来の軍備管理のアプローチではなく、核抑止を不安定化させる恐れのあるAIの使用という「行動」を避けるべきとする規範的アプローチが有意義であると思われる。また、AIを実装した核兵器システムに対してサイバー攻撃が行われ、AIの訓練データが書き換えられて核兵器システムが無力化される可能性もある³²。このように核兵器システムに実装されたAIを標的とするサイバー攻撃という特定の「行動」も避けるべき対象とするかどうかも検討すべきであろう。

なお、新興技術のうち、極超音速兵器については従来の兵器規制アプローチを適用できる余地がある。ロシアとの戦略核兵器削減交渉を有利に進めるとともに、中距離核戦力の上限を再確立するための手段として、米国が極超音速兵器の制限をロシアに持ち掛けることにより米露間の核軍備管理協定への道筋をつけ、ゆくゆくはこれに中国を引き込んでいくことができれば望ましいと指摘されている³³。ただし、こうした交渉に際して、中露が米国のミサイル防衛システムを規制の対象に含めるように求めてくる可能性が高いことに留意する必要がある。もともと中露が極超音速兵器の開発を始めた背景には、中露に対する米国のミサイル防衛能力の優位性に直面した両国が、ミサイル防衛システムを回避できる報復第二撃能力の確保を目指したことがあり、その意味で米国のミサイル防衛の規制は中露両国にとって極超音速兵器の規制と引き換えにしても利益の方が大きいと判断されるかもしれない。このため、今後の米露(中)軍備管理のアジェンダに極超音速兵器の規制が含まれるとすれば、米国のミサイル防衛の規制とセットで議論されるようになるとと思われる。

³¹ Lauren Kahn, “Mending the ‘Broken Arrow’: Confidence Building Measures at the AI-Nuclear Nexus,” *War on the Rocks*, November 4, 2022.

³² Zachary Kallenborn, “AI Risks to Nuclear Deterrence Are Real,” *War on the Rocks*, October 10, 2019.

³³ Spenser A. Warren, “Avangard and Transatlantic Security,” Center for Strategic and International Studies, September 23, 2020.

おわりに

新領域・新興技術をめぐる動向は、今後の核抑止と軍備管理に少なからぬ影響を及ぼしていくであろう。米中露3か国は大国間競争の文脈において新興技術の開発にしのごを削っており、それが新領域での戦いのイネーブラーとして作用する形で、核抑止の安定性を動揺させつつある。このような新領域・新興技術による核抑止の不安定化を抑えるための軍備管理として、本稿では行動規範アプローチの可能性を模索したが、規範順守の検証をどのように行うのかといった課題が多いことはいうまでもない。

こうした中、米国のサリバン国家安全保障担当補佐官は2023年6月に、中国を軍備管理交渉に引き入れる取組を再開する一方で、米国の現有戦略核戦力を非核精密攻撃兵器などの新技術によって補いつつ核抑止を維持すると述べた。ただし、軍備管理の観点から、AIを意思決定における人間の介在 (human in the loop) なしには核使用の許可に用いないとするグローバルな合意の確立を目指すとした³⁴。こうした米国の姿勢は、新興技術に係る軍備管理の在り方の一端を示すものとして注目すべきであろう。

³⁴ Julian E. Barnes and David E. Sanger, “U.S. Will Try to Bring China into Arms Control Talks,” *New York Times*, June 2, 2023.