参議院常任委員会調査室・特別調査室

論題	新興技術の規制に関する国際的議論の動向 －ＡＩ兵器、サイバー攻撃、極超音速兵器－
著者 / 所属	寺林　裕介 / 外交防衛委員会調査室
雑誌名 / ISSN	立法と調査 / 0915-1338
編集・発行	参議院事務局企画調整室
通号	469 号
刊行日	2024-9-20
頁	48-61
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20240920.html

新興技術の規制に関する国際的議論の動向

― ＡＩ兵器、サイバー攻撃、極超音速兵器 ―

寺林　裕介
（外交防衛委員会調査室）

１．はじめに

ロシアによるウクライナ侵略では両国の無人機が大量に投入され、それらは戦車や艦艇を攻撃し、戦場でその優位性を示した。ＡＩ（人工知能）搭載型の無人機の研究が急速に進み、ウクライナはＡＩ兵器の実験場になっているとも言われる。

近年では、ＡＩ、サイバー技術、極超音速技術などの新興技術（Emerging Technologies）が軍事分野で応用されており、これらは各国の安全保障に直接、そして広範囲に渡って影響を及ぼすことから注目されている。例えば、人間の関与なしに完全に自律したＡＩ兵器、他のコンピュータを乗っ取りそれを踏み台として一斉攻撃するサイバー攻撃、従来のミサイル防衛を回避して接近する核弾頭搭載可能な極超音速兵器などを競争相手国が使用可能になれば、自国に対する脅威の度合いは一段と高まることになる。

ウクライナやパレスチナ・ガザ地区での使用例から、これら新興技術の戦争への応用を目の当たりにして、その軍事利用を規制もしくは制限する必要性が強く認識されるようになった。しかし同時に、その有効性が実証されるにつれて、戦場を一変させる兵器を競争相手国より早く確保しようと各国は開発ペースの加速を余儀なくされている。新興技術に関する軍拡競争がすでに始まっているとも言えよう。

こうした新興技術の軍事利用については、いくつかの特徴を指摘することができる。第一に、これらの技術は戦闘の様相を一変させる、いわゆるゲーム・チェンジャーになり得るほど強力である。完全に自律したＡＩ兵器が実用化されれば、火薬、核兵器の登場に次いで第三の軍事革命を引き起こすとの指摘もある。第二に、その多くが民生用として機械、医療、科学分野など社会の広範に渡って活用されていることから、技術開発そのものを止めることはできない。サイバー空間はすでに我々の日常の一部であり、ＩＣＴ（情報通信技術）も生活に浸透している。第三に、新興技術の軍事利用には、非人道的なマイナス面だけでなくプラス面の主張も存在し、例えばＡＩによる正確な識別が文民への被害を減らす可能性が指摘されている。また、それらの技術への理解は防御面でも必要となり、サイバーセキュリティの強化、ミサイル防衛システムの更なる開発などにつながっていく。第四に、これらの新興技術は実際の戦闘の場面だけでなく、指揮官の意思決定や軍事計画の策定などあらゆる場面に関与して状況を複雑化させる。実際には戦時平時を問わずにこれらの技術を考慮する必要に迫られている。

このような新興技術が戦争に大きなインパクトを与え、戦闘のあらゆる場面が一変したとき、既存の軍備管理に関する国際法や国際制度に多くの課題を提起することになるだろう。一例としては、既存の軍備管理、もしくは抑止関係に存在しているエスカレーション・ラダーの想定の妥当性、戦略的曖昧性の計算の不確実性、相手の意図の不可知性といったリスクを増幅させることになる[1]。こうして新興技術の特徴を含めて複雑化した環境下では、軍備管理の形成やその規制についての各国間の合意は一層困難になることが予想される。

現在進行形である新興技術の進展により、その軍事利用がもたらす影響や規制の必要性、各国間における軍備管理の可能性について、近年、国際社会で多くの議論が起こっている。本稿では、①ＡＩ兵器、特にその最たる進化型である自律型致死兵器システム（ＬＡＷＳ）、②サイバー攻撃、③極超音速兵器を取り上げて軍事的な特徴と国家安全保障との関わりを解説し、その規制や軍備管理に関する国際社会の議論の動向を概観する。

２．ＡＩ兵器の規制に関する議論

（１）ＡＩの軍事利用の拡大

軍事兵器は、急速に進展したＡＩ技術を組み込むことにより、兵器の無人化、自律性の進歩を可能とし、兵器としての優位性を向上させている。ＡＩは、実際の戦場において兵器に組み込まれるだけでなく、サイバー空間でも利用されるなど、戦時及び平時のあらゆる場面ですでに軍事利用が進められている。例えば、ＡＩを搭載した無人航空機（ＵＡＶ、

[1] 秋山信将「新興技術の規制可能性：軍備管理の視点からの論点整理」日本国際問題研究所『研究レポート』（2021.3.30）

ドローン）は、戦場で敵の戦車を他の車両と区別して発見し、そこにミサイルで攻撃することが可能である。また、サイバー空間においては、敵からのサイバー攻撃に対抗し、ＡＩを利用したセキュリティ対策が追求されている。

ＡＩ技術の軍事利用については、米国では以下の分野において研究開発が進められている。

表１　軍事分野におけるＡＩの応用（米国）

研究分野	主な具体例
情報収集、監視、偵察	ドローンで撮影した映像の分析の自動化、関連データのない画像の地理的位置の特定、生活パターン分析に基づく建物機能の推測
ロジスティクス	部品交換や点検時期の予測、物資配送のコスト削減
サイバー作戦	ソフトウェアの脆弱性を自律的に検出・修正
情報操作、ディープフェイク	ディープフェイクの検出・評価（フォレンジック）、個人の行動履歴の作成
指揮・統制	最適な戦力構成の決定、実行可能な行動メニューの提供
半自律型・自律型車両	戦闘機、無人機、地上車両、艦艇へのAI搭載、環境・障害物の認識、ナビゲーション、通信等
LAWS	標的の識別、手動で制御なしに標的を破壊

（出所）米国議会調査局のレポート[2]を基に筆者作成

表１は米国の例であるが、同様に各国も研究開発を進めており、競争相手国がＡＩ兵器に関する優位性を獲得した場合には、自国の安全保障に及ぼす影響は甚大なものとなる。そのため、敵国との開発競争に関しては、人道や人権の観点についてどの程度考慮する必要があるのか、又はそれが研究開発を自発的に抑制する理由となるのか、という論点を顧みる動機が弱くなる。ＡＩの開発競争とその軍事利用について、各国の全面的な武器競争に発展する可能性が指摘されている[3]。特に自律型致死兵器システム（ＬＡＷＳ）をめぐる問題は、軍事的な効果のインパクトに加え、それが引き起こすリスクも大きく、国際社会で議論が重ねられてきた。

（２）ＬＡＷＳの特徴と課題

自律型致死兵器システム（ＬＡＷＳ：Lethal Autonomous Weapons Systems）は現時点で実在していない兵器システムであり、これをどのようなものとして定義するか、未だ国際的な合意が得られていない。日本政府は、国際社会で議論されているＬＡＷＳについて、「一度起動すれば、操作者の更なる介入なしに標的を識別し、選択し、殺傷力を持って交戦することができるという特徴を備えている兵器システム」と定義している[4]。なお、Ｌ：

[2] Kelley M. Sayler, “Artificial Intelligence and National Security,” CRS Report R45178, Updated November 10, 2020, pp.9-16.
[3] 佐藤丙午「ＡＩと安全保障：ＬＡＷＳ規制に向けた国際社会の議論について」『国際開発学研究』Vol.22-2（2023.3.31）70頁
[4] 外務省ウェブサイト〈https://www.mofa.go.jp/mofaj/dns/ca/page24_001191.html〉（以下、ＵＲＬの最終ア

Lethal（致死）を外し、対物破壊兵器を含めた自律型兵器システム（ＡＷＳ）の用語を使用する例も増えている。定義は、その規制の対象をどの範囲に定めるのかといった論点に関わることから、すでに各国の立場の相違が存在する[5]。

ＬＡＷＳの特徴として、人間がいつ、どこまで関与できるのか、すなわち機械の自律性（autonomy）をめぐる問題が、ＡＩの進化に伴って注目されている。自律性の観点について、①目標の選定や攻撃を人間の命令を受けて実行する兵器、②目標の選定や攻撃を自ら決定できるが人間がこれを無効にできる兵器、③一度起動すれば人間の命令を受けずに目標を選定して攻撃できる兵器、として大きく３つに分類した場合、前記②のように人間の関与によって攻撃を中止できることが不可欠とする立場や、③であっても起動するまでに人間の判断が介在するので十分許容できるとの立場があり対立している[6]。

ＬＡＷＳが兵器として支持される理由としては、戦闘機などの有人兵器やミサイルと比べて製造コストを削減できること、また、無人であることから死傷者を出さずに作戦を遂行でき、その分の人的コストを削減できることが挙げられる。作戦遂行時にはヒューマンエラーを減少させることができ、それは戦闘員と文民とを精緻に区別することも可能にすると言われる。しかし、このように人的・物的コストが削減され、正確な攻撃が可能であれば、かえって各国が攻撃を実施しようとする誘因となり、紛争解決のために実力行使の選択肢を採用する敷居を下げることとなる。

また、ＬＡＷＳが誤作動などによって被害を引き起こした場合、又はＬＡＷＳが自ら選択して人道法違反の攻撃を行った場合、その責任の所在がどこにあるのか明らかでなく、それは人間の判断がどの程度介在していたかによっても評価が分かれる。国際人道法からの要請としては、ジュネーブ条約第一追加議定書第36条において、締約国は新兵器等の研究、開発、取得又は採用に当たり、その使用が議定書又は他の国際法の諸原則により禁止されているか否かを決定する義務を負っている。ＬＡＷＳが攻撃を行った場合に、人間と同等のレベルで国際人道法の諸原則（区別原則、比例性原則、予防原則等）の要請に技術的に応えることができるのかについては結論が出ていない。加えて、機械に殺傷されるのは非倫理的であるため、兵器使用のいずれかの段階で人間の関与がなければならないという議論がある[7]。機械の意思で、機械に殺害されることは人間の尊厳が害されるのか否かという倫理的な問題が提起されている。

さらに、このようなゲーム・チェンジャーにもなり得る兵器をテロリストが獲得し、拡散させ、使用する危険性が拭えない。その技術が拡散した場合、人的・物的コストがかからない兵器は、テロリスト集団にとって格好の武器となり、国家の安全保障を脅かすものとなる。

クセス日は、いずれも2024.9.5）

[5] ＬＡＷＳの定義については、福井康人『通常兵器軍縮論』（東信堂、2020年）188～190頁を参照。

[6] 自律性をめぐる人間の関与の在り方の対立点については、岩本誠吾「ＡＩ兵器をどう規制するか」『世界』（2019.10）111頁を参照。

[7] 黒﨑将広ほか『防衛実務国際法』（弘文堂、2021年）543頁

（３）ＬＡＷＳ規制の国際的議論の動向

ＬＡＷＳに関しては、まず2013年４月、国際ＮＧＯヒューマン・ライツ・ウォッチが完全自律型兵器開発の禁止を目的として、世界規模の「キラーロボット反対キャンペーン」を開始した。同時期に国連では、2013年５月、国連人権理事会のクリストフ・ヘインズ特別報告者が自律型致死性ロボットの問題を提起する報告書[8]を提出し、その中で、こうした兵器の危険性を指摘し、各国に対してハイレベル・パネルを設置して議論するよう求めた。これらの問題提起を受け、特定通常兵器使用禁止制限条約（ＣＣＷ）の下で、2014年からＬＡＷＳに関する非公式会合が開始された。2016年の非公式会合では、ＣＣＷ締約国会議に対し、全ての締約国で構成されるＬＡＷＳに関する政府専門家会合（ＧＧＥ）を設置して議論を開始するよう勧告された。翌2017年からＧＧＥが開催され、2018年11月、ＧＧＥは「指針となりうる原則」を定め、ＣＣＷ締約国会議に提出した。さらにＧＧＥは、この原則に１項目を追加したＬＡＷＳに関する11項目の「指針」（表２を参照）を採択し、2019年11月、ＣＣＷ締約国会議にこれを報告した。

表２　ＬＡＷＳに関する11項目の「指針」の概要

(a) LAWSを含め全ての兵器に国際人道法が適用される
(b) 兵器使用に当たり人間の責任を確保する
(c) 兵器のライフサイクルの各段階で、人間と機械の相互関係は国際人道法に従う
(d) 新兵器の開発、配備及び使用の説明責任は、人間の指揮統制系統内を含めて国際法に従う
(e) 新兵器について、国家が国際法で禁止されているか否かを判断する
(f) 新兵器の開発・取得において、物理的防護、サイバーセキュリティを含む安全措置、テロ集団の取得リスク、拡散リスクを考慮する
(g) リスク評価と緩和措置を兵器の設計、開発、実験、配備の一部とする
(h) LAWS関連の新興技術の使用の際に、国際人道法及びその他の国際法の義務を遵守する
(i) LAWS関連の新興技術を擬人化しない
(j) CCWでの議論や政策は、自律型技術の進展や平和利用へのアクセスを妨げない
(k) CCWは、軍事的必要性と人道的考慮のバランスを追求し、LAWS関連の新興技術の問題を扱う適切な枠組みを提供する

（出所）CCW/GGE.1/2019/3（25 September 2019）Annex Ⅳを基に筆者作成

その後もＧＧＥは議論を重ねて2022年８月に報告書[9]を採択した。ここでは、今後の可能な措置と選択肢に関して、①ＣＣＷの枠組みの下で法的拘束力のある文書を作成する、②法的拘束力のない文書を作成する、③国際法、特に国際人道法の下で既存の義務の実施を明確化する、④国際人道法に基づき禁止・規制する、⑤さらなる法的措置は必要ない等の

[8] UN Doc. A/HRC/23/47 (9 April 2013)
[9] CCW/GGE.1/2022/2 (31 August 2022)

オプションを含む提案が議論されたことが報告された。基本的にＡＩ兵器の開発国は法規制に消極的であり、逆に非開発国は法規制に積極的な立場をとる。ロシア、イスラエルは前者、オーストリア、パレスチナは後者の例である。日本を含む米英加豪韓の６か国は、法的拘束力のある文書を作成することは意見の相違から困難と判断し、ＧＧＥにおける議論を踏まえた成果文書を志向して歩調を合わせている。

2023年５月に採択されたＧＧＥ報告書[10]では、国際人道法の遵守の観点から、ＬＡＷＳの開発と使用に国際人道法を適用することが再確認され、さらに、ＬＡＷＳ関連の新興技術を用いた兵器システムについて、国際人道法を遵守できないものは使用禁止であることが明記された（para.21）。また、国際法の遵守を確保するために、国家は必要に応じて、その兵器システムの標的の種類、運用期間、地理的範囲、規模を制限すること、人間のオペレーターに適切な訓練と指示を提供することを行うべきであるとされた（para.22）。

ＣＣＷのほかにも国連では、2023年７月にアントニオ・グテーレス事務総長が「平和のための新アジェンダ」を発表し、その中で国連加盟国に対し、ＬＡＷＳを禁止する法的拘束力のある文書を2026年までに採択するよう呼びかけを行った。2023年12月、国連総会で初めてとなるＬＡＷＳに関する決議が賛成152、反対４（ベラルーシ、インド、マリ、ロシア）、棄権11（中国、北朝鮮、イスラエル等）で採択された[11]。この決議では、自律型兵器システム（ＡＷＳ）がグローバルな安全保障と地域的・国際的な安定に及ぼす負の影響と結果について懸念を表明するとともに、国際法、特に国連憲章、国際人道法、国際人権法がＡＷＳに適用されることが確認された。さらに、国連事務総長に対し、ＬＡＷＳが提起する課題や懸念に対処する方法等について、国連加盟国の意見を求めるよう要請している。例えば、日本はこの決議に従って2024年５月、作業文書[12]を国連に提出し、その中で人間の関与が及ばない完全自律型の致死性を有する兵器システムを開発する意図はないことを表明した。また、今後の議論により作成されるべき成果物に求められるのは法的拘束力ではなく、実効性のあるルールであることを強調し、ＣＣＷ下での議論の継続を主張した。

この他にも、ＡＩの軍事利用について各国での議論が進んでおり、2023年２月にオランダで開催された「軍事領域における責任あるＡＩ利用（ＲＥＡＩＭ）サミット」において、米国が公表した「ＡＩと自律性の責任ある軍事利用に関する政治宣言」[13]に係るイニシアチブもその一つである。同政治宣言は、ＡＩの軍事利用について各国が実施すべき措置を示したものであり、2024年５月時点で日本を含む54の国・地域から支持が得られている。

以上のように国際社会ではＬＡＷＳの規制を中心に議論が行われてきた。しかし、ＬＡＷＳとされる兵器に対し、国際人道法を適用し、各国もそれを遵守すべきことでは一致しているものの、その規制の範囲や手段については、各国の安全保障上の要請に従い、意見が乖離している。この間、生成ＡＩをはじめとする技術開発が急速に進展しており、上述したように、ＬＡＷＳに限らずＡＩの軍事利用の射程も広がっている。今後、指揮・統制

---

[10] CCW/GGE.1/2023/2 (24 May 2023)
[11] UN Doc. A/RES/78/241 (22 December 2023)
[12] 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/files/100687670.pdf>
[13] 外務省ウェブサイト <https://www.mofa.go.jp/mofaj/files/100580933.pdf>

や作戦立案など様々な軍事の分野やタイミングでＡＩが活用されるだろう。そのとき、規制の必要性や範囲、手段についての認識を各国で共有することはますます困難となり、その議論は一層複雑化していくと考えられる。

３．サイバー空間の規制に関する議論

（１）サイバー攻撃の被害例

近年、サイバー空間を利用して特定情報を窃取したり、コンピュータ・システムを停止・破壊したりする侵害行為（サイバー攻撃）が国際社会で常態化している。そのような攻撃は時に甚大な被害を引き起こす。2007年にエストニアが受けたサイバー攻撃は、政府機関、銀行等のウェブサイトを停止させ、数日間、社会機能を麻痺させた。また、同年のイスラエルによるシリア核施設空爆作戦では、イスラエル側戦闘機のシリア領域侵入の前に、シリアの防空システムにサイバー攻撃が仕掛けられたとされる。多くの国家が、政治、経済、軍事的側面からサイバー空間を利用し、競争相手国に対して優位性を得ようとしてサイバー能力を強化している一方、これに対抗するためにサイバーセキュリティの重要性も認識されており、国家の安全保障課題としてサイバー攻撃への対応が急務となっている。

表３　被害の種別によるサイバー攻撃の一例

被害の種類	主な具体例(時期)
ウェブサイト閲覧障害	ハッカー集団KillnetのDDoS攻撃による日本の行政機関等のウェブサイト閲覧障害（2022.9）
偽情報の流布	米国大統領選における米国有権者向けロシアによる偽情報の流布（2016）
業務の妨害	韓国の金融機関等でマルウェア感染によるシステム障害（2013.3）、北朝鮮ラザルスのサイバー攻撃によるソニー・ピクチャーズエンタテインメント(SPE)の映画公開中止（2014.11）
金銭の獲得	北朝鮮ラザルスによるバングラデシュの銀行からの不正送金（2016.2）、ワナクライと呼ばれるランサムウェア攻撃(2017.5)、北朝鮮ラザルスによる約6億ドルの暗号資産の盗取（2022.3）
個人情報、知的財産を含む機密情報の窃取	欧州医薬品庁へのサイバー攻撃による新型コロナワクチンの承認申請文書の窃取・改ざん（2020.12）、ロシア関連組織による米国企業SolarWinds製ソフトウェアを利用した米国等政府機関へのサイバー攻撃(2020.12)、中国による日本の外務省公電システムの情報漏えい（2020）、内閣サイバーセキュリティセンターの電子メール関連システムへの侵入（2023.6）
政府機関への攻撃	イラン組織のサイバー攻撃によるアルバニア政府機関の公共サービスの一時停止（2022.7）
重要インフラへの攻撃	水道水の有毒化を企図した米国の浄水場へのサイバー攻撃（2021.2）、オーストラリアの医療機関へのランサムウェア攻撃によるシステム停止、緊急度の低い手術の延期（2021.3）、米国の石油パイプライン企業コロニアルへのランサムウェア攻撃による操業停止（2021.5）、名古屋港ターミナルへのランサムウェア攻撃による操業停止（2023.7）

（出所）報道等により筆者作成

表３は、平時におけるサイバー攻撃によって引き起こされた主な被害について、その種類ごとに整理したものである。

これらの多くは犯罪行為であり、その場合、基本的には各国の国内法が適用される。しかし、それが国家もしくは国家が命じた攻撃者によるサイバー攻撃であり、一定の条件を満たした場合、武力の行使と見なし得る場合も出てくる。この点に関して米国のハロルド・ホンジュ・コー元国務省法律顧問は、死者、負傷者、又は重大な破壊を直接的に引き起こすサイバー活動は、武力の行使と見なされる可能性が高いとし、具体的には、①原子力発電所のメルトダウンを引き起こす作戦、②人口密集地にダムを開放して破壊を引き起こす作戦、③航空機の墜落事故につながる航空管制を無効にする作戦を例として掲げた[14]。これらの例のように、サイバー攻撃が爆発物やミサイルと同様に物理的損害を与えるのであれば、そのサイバー攻撃も武力の行使と見なすべきと説明されている。

米国における2018年２月の「核態勢の見直し（ＮＰＲ）」では、米国の核指揮・統制・通信（ＮＣ３）施設に対するサイバー攻撃の脅威が認識され、そのような脅威の発生を回避するための核兵器使用も示唆した。また、重要インフラへの攻撃では、例えば、2021年２月、米国フロリダ州オールズマーの水道システムがハッキングされた。水酸化ナトリウムの濃度が100倍以上に引き上げられたが、すぐに職員が気づいて正常値に戻された。このような重要インフラへのサイバー攻撃は多大な損害を引き起こす可能性がある[15]。単なる情報の窃取であっても、米英韓３か国が2024年７月に共同で発表した北朝鮮による核関連施設へのサイバー攻撃については、核兵器開発を支援するための情報を標的としており、核拡散は各国の安全保障への脅威となり得る。サイバー攻撃はその対象や目的により国家安全保障上の脅威に結びつくことがある。

（２）サイバー攻撃の特徴

サイバー攻撃の特徴としては、その攻撃者の帰属（attribution）、すなわち誰がそのサイバー攻撃を実行しているのかについて、特定することが困難なことが挙げられる。さらに、たとえ実行犯が特定できたとしても、それが国家の行為として実行されたものなのか、政府の意を受けた代理人によるものなのか、政府とは関係のない私人によるものなのか、について判断することが難しい。国際的な事象に関連して、一定の思想的・社会的背景を持つ非国家主体によるサイバー攻撃も発生している。自然発生的に攻撃者が集団化し、同じ対象や同じ目的のためにサイバー攻撃を仕掛けていた場合、防御側の認識は一層混乱を招く可能性がある。

このような匿名性は、攻撃側を圧倒的に優位な立場に置くため、安易に攻撃を仕掛けようとする動機を与えることになる。サイバー空間を舞台にしていることから、敵対国との地理的な距離は関係が薄く、世界のどの場所からも攻撃は可能であり、国境を容易に越え

---

[14] Remarks by Harold Hongju Koh, Legal Advisor U.S. Department of State, “International Law in Cyberspace,” September 18, 2012. <https://2009-2017.state.gov/s/l/releases/remarks/197924.htm>

[15] 重要インフラに対するサイバー攻撃と安全保障については、森秀勲「サイバー攻撃の脅威とサイバー安全保障」『立法と調査』No.462（2023.12.18）115～118頁を参照。

ていく。サイバー攻撃により、敵国の防御能力を低下させることができた場合、これに続けて従来の兵器による攻撃を仕掛ける敷居も低くなる。

防御側にとっては、攻撃側のサイバー攻撃の手法は広範多岐に渡り、それらを個別に対処する必要がある。攻撃側は防御側システムの脆弱な部分を狙うことから、防御側は全ての面において最新のセキュリティ対策が求められ、コストは高まる。また、サイバー攻撃の把握が遅れ、システムに侵入されてから実際の被害が出るまでに時間差があった場合、気がついたときには対応が不可能になることもある。産業分野などＩｏＴ機器が浸透していることで、サイバー攻撃の被害は経済社会活動に広く、そして瞬時に拡散する。防御側は、そのサイバー攻撃の目的や意図を特定できず、状況認識を見誤り、エスカレーションを誘発する可能性が高まる。

（３）サイバー空間の規制と国際法の適用

サイバー攻撃が各国の経済・社会に大きな影響を及ぼすことから、サイバー空間をどのように管理していくのか、国際ルールや一定の行動規範の検討が求められている。しかし、サイバー空間について、国家が責任を持って管理すべきとする立場から、サイバー空間の利点である情報の自由な流通を確保し、国家による過度な統制は望ましくないとする立場まで、国際社会で統一した考え方は確立できていない。ロシアや中国、新興国は前者の立場をとり、サイバー空間の特徴を考慮した新しい条約等の策定を検討する必要性を訴えている。米欧諸国や日本は後者の立場をとり、サイバー空間においても既存の国際法が適用されるべきとする考えを検討している。

2004年に発効した欧州評議会の「サイバー犯罪に関する条約」（ブダペスト条約）は、コンピュータ・システムを攻撃する犯罪行為やコンピュータ・システムを利用して行われる犯罪行為について犯罪化することを締約国に求めている。現在、全てのＧ７諸国を含む76か国が締約国となっているが、中国、ロシア、インド等は未締結である。しかし、この条約は、サイバー攻撃を各国の法制度の下で犯罪化することを目的としており、さらに犯罪の処罰、犯罪人引渡しなど国際刑事分野における国際協力を規定したものであり、国家によるサイバー攻撃を対象としたものではない。なお、2024年８月には、国連において新たなサイバー犯罪条約の交渉が妥結した[16]。

サイバー空間における国際法の適用については、各国の専門家により作成されたタリン・マニュアルが参照され、議論の際の検討材料となっている。タリン・マニュアルでは、サイバー攻撃に対する自衛権の行使について一定の条件下では可能とする見解が示された[17]。例えば、重要インフラへの攻撃として、2010年にスタックスネットと呼ばれるマルウェアが、イランのウラン濃縮施設で使用されていた遠心分離機に損害を与えた例について、当該攻撃が国連憲章第２条４が禁止する「武力の行使」に当たることで専門家たちの意見は一致したが、同第51条の自衛権発動要件である武力攻撃に該当するか否かについては意見

---

[16] 外務省ウェブサイト〈https://www.mofa.go.jp/mofaj/gaiko/soshiki/cyber/index.html〉

[17] 中谷和弘、河野桂子、黒﨑将広『サイバー攻撃の国際法―タリン・マニュアル2.0の解説―』増補版（信山社、2023年）87～88頁

が分かれた。

国連では、安全保障分野におけるサイバー空間での責任ある国家の行動の進展に関するサイバーセキュリティに関する国連政府専門家会合（国連サイバーＧＧＥ）が、2004年から設置されて議論が行われている。国連サイバーＧＧＥ第３会期報告書（2013年）[18]では、サイバー空間に国際法、特に国連憲章が適用可能であることが明記された。具体的には、同第４会期報告書（2015年）で、国家主権、平和的紛争解決、内政不干渉の原則及び人権・自由の尊重についてサイバー空間に適用可能とされ、同第６会期報告書（2021年）[19]では、国際人道法（武力紛争時のみ）が適用されることが言及された。しかし、自衛権の行使についての議論はコンセンサスが得られていない。サイバー技術を十分保有していない国からは、正当な理由なく自国がサイバー攻撃の加害国とみなされ、他国の自衛権行使の対象になるとして懸念が示されている。コンセンサスの回避については、このような自衛権行使の対象になることを回避したいという考えと、国際法の適用の各論をできる限り未整理にしておき新条約交渉につなげようとする意図が指摘されている[20]。

この他に、国連サイバーＧＧＥ第４会期報告書では、サイバー空間における責任ある国家の行動に関する「11の行動規範」で一致した。

表４　サイバー空間における「11の行動規範」の概要

(a) 国際の平和及び安全の維持を含む国連の目的に沿って各国は協力する
(b) ICTの事案はあらゆる情報を考慮する
(c) 自国の領域がICTを用いた違法行為に利用されることを了知しながら許すべきではない
(d) ICTを利用したテロ行為や犯罪を訴追し、そのような脅威に対処するため協力する
(e) ICTの安全な利用のために人権を保障すべきである
(f) 重要インフラに故意に損害を与えるICT活動を行ってはならない
(g) 重要インフラをICTの脅威から保護するための適切な措置を講じる
(h) 重要インフラが悪意あるICT行為の対象となっている他国からの支援要請に応じる
(i) サプライチェーンの完全性を確保するため合理的な措置を講じる
(j) ICTの脆弱性の責任ある報告を奨励し、情報を共有する
(k) 他国の緊急対応チームのシステムに危害を加える活動をしない

（出所）UN Doc. A/70/174 (22 July 2015) Ⅲ.を基に筆者作成

国連サイバーＧＧＥは既存の国際法、特に国連憲章が適用可能とすることを確認し、米

[18] UN Doc. A/68/98 (24 June 2013)
[19] UN Doc. A/76/135 (14 July 2021)
[20] 赤堀毅「サイバーセキュリティと国際法―第６次国連政府専門家グループ報告書の成果を中心に―」『国際法外交雑誌』第120巻第４号（2022.1）43～45頁

欧諸国や日本の立場を反映した形で進められている。これに対し、国家がサイバー空間を管理する新条約の策定を目指すロシアは、2018年12月の国連総会に決議を提出し、全ての国連加盟国を参加可能とするサイバーセキュリティに関する国連オープン・エンド作業部会（ＯＥＷＧ）の設置を求めた。新たにＯＥＷＧで議論が進められる一方、さらに米欧諸国や日本は、行動計画（ＰｏＡ）と呼ばれる新たな枠組みを導入しようと議論している。こうしたサイバー空間における国際規範を形成しようとする複数のプロセスについて、自国側にとってより望ましい場で議論しようとして主導権争いとなっていることが指摘されている[21]。

上記の国際社会における議論に加え、二国間でサイバー攻撃の重大性について認識を共有する事例がある。2013年６月の米国カリフォルニア州における米中首脳会談では、バラク・オバマ大統領から習近平国家主席に対して中国のサイバー攻撃について問題提起があり、両国間でサイバーセキュリティに関する協議を行うワーキンググループが設置された。その後、2015年９月の米中首脳会談でも再び議論となり、両政府がサイバー攻撃による機密情報を含む知的財産の窃取に関与しないことや故意に支援しないことで合意した。また、2021年６月にスイスのジュネーブで開催された米露首脳会談では、ジョー・バイデン大統領からウラジーミル・プーチン大統領に対し、特定の重要インフラはサイバー攻撃やその他の手段による攻撃を受けないようにするべきと提案し、具体的に16の重要インフラのリスト[22]を提示したとされる。

重要インフラに対するサイバー攻撃が、どのような損害を引き起こすのか計算することは、防御側あるいは場合によっては攻撃側にとっても困難であり、これに対応しようとした国家が判断を誤れば、望まないエスカレーションを生む危険性がある。サイバー空間における責任ある国家の行動について、国家間で認識の差異があったとしてもできる限り合意形成を図るとともに、重要インフラへの攻撃を抑制することなど一定の共通理解を取り付ける努力が必要となる。

４．極超音速兵器の軍備管理

（１）極超音速兵器の開発

従来からミサイルは、発射後に目標に向かって飛翔し、標的を破壊する無人の兵器として、各国の安全保障上の脅威となってきた。こうしたミサイルは、核・生物・化学兵器など大量破壊兵器（WMD）の運搬手段として使用される。特に大陸間弾道ミサイル（ＩＣＢＭ）、潜水艦発射弾道ミサイル（ＳＬＢＭ）は、戦略爆撃機とともに戦略三本柱を形成してきた。これらのミサイルへの防御手段として、各国はミサイル防衛システムを整備し、特に高速で飛来する弾道ミサイルを迎撃するために特別に開発された弾道ミサイル防衛（ＢＭＤ）システムを配備してきた。しかし、新興技術の開発ペースが加速することによ

---

[21] 原田有「サイバー国際規範をめぐる戦い―国連を舞台とした日米欧諸国と露中等との対立」防衛研究所『ＮＩＤＳコメンタリー』第322号（2024.5.21）

[22] 化学、商業施設、通信、重要な製造業、ダム、防衛産業基盤、緊急サービス、エネルギー、金融サービス、食料・農業、政府サービス・施設、医療・公衆衛生、ＩＴ、原子炉・核物質・核廃棄物、輸送システム、上下水道

り、こうした各国の防衛網を突破することを企図して、通常の弾道ミサイルとは異なる低い軌道をとり、マッハ５を超える極超音速で飛翔する極超音速兵器の開発と配備が進んでいる。

極超音速兵器は、極超音速滑空体（ＨＧＶ：Hypersonic Glide Vehicle）と極超音速巡航ミサイル（ＨＣＭ：Hypersonic Cruise Missile）の２つに分類される。極超音速滑空体（ＨＧＶ）は、弾道ミサイルと同様にロケットブースターで打ち上げられるが、その後に弾道軌道を離れて大気圏内を飛翔し、高速で目標に向かって突入する。極超音速巡航ミサイル（ＨＣＭ）は、空気の圧縮を利用して超音速で作動するラムジェットやスクラムジェットを使用したエンジンにより、マッハ５以上での飛翔が可能となる。

これらＨＧＶやＨＣＭは、米国、ロシア、中国を中心に開発・配備が進められている。米国では、2000年代初頭から「通常兵器による迅速なグローバル打撃（ＣＰＧＳ）」構想を開始し、地域紛争で使用可能な核兵器を搭載しない極超音速兵器の技術開発を進めた。ロシアが開発したアヴァンガルドは、核弾頭が搭載可能とされるＨＧＶであり、2019年12月に実戦配備が公表された。中国は、複数の種類のＨＧＶ、ＨＣＭを開発しているとされ、実験を繰り返している。

その他の国でも、極超音速技術の開発とその応用に関心が高まっている。表５は極超音速兵器の主な開発国とその開発する兵器の種類を掲げたものである。

表５　極超音速兵器の主な開発計画

開発国 注1	主な開発計画（HGV, HCM）
米国	海軍: CPS [HGV], HALO [HGV]　空軍: ARRW [HGV], HACM [HCM] 陸軍: LRHW [HGV]　DARPA: TBG [HGV], HAWC/MOHAWC [HCM]
ロシア	アヴァンガルド [HGV], （キンジャール [HGV] 注2）, ツィルコン [HCM]
中国	DF-ZF(東風ZF) [HGV], Starry Sky-2(星空2) [HCM], Lingyun-1(凌雲1) [HCM]
インド(/ロシア)	Brahmos Ⅱ [HCM]
フランス	V-max [HGV]
韓国	Hycore [HCM]
北朝鮮	Hwasong-8(火星8) [HGV]
日本	極超音速誘導弾 [HCM], （島嶼防衛用高速滑空弾 [HVGP] 注3）

注１：この他にドイツ、イラン、イスラエル、ブラジルなど研究開発を実施している国がある。
注２：ロシアはキンジャールを極超音速兵器と呼んでいるが、ＨＧＶではないと評価されている。
注３：Hyper Velocity Gliding Projectile
（出所）米国議会調査局のレポート[23]を基に筆者作成

[23] Kelley M. Sayler, “Hypersonic Weapons: Background and Issues for Congress,” CRS Report R45811, Updated February 9, 2024, pp.4-21.

（２）極超音速兵器の特性と軍備管理の可能性

極超音速技術の進展は、従来の軍備管理の考え方に関してその変数を増大させ、国際社会の平和と安定を揺るがしている。極超音速兵器の最大の特徴は、マッハ５以上とされるその高速性能であるが、速さだけなら落下速度がマッハ10から20に達するこれまでの弾道ミサイルも同等の性能を持つ。極超音速兵器が各国の安全保障に新たな脅威を引き起こしている理由はその機動性にある。極超音速兵器は、弾道ミサイルに比べて低い高度を飛翔する。防御側から見れば、地球の水平線から突如として姿を現すことになり、地上配備レーダーでの探知が遅れ、迎撃が困難になる。そのため極超音速兵器は、迅速に相手の防空レーダー、航空基地、指揮統制施設などを狙って攻撃できることから、戦闘の初期段階で有用であると指摘される。

極超音速兵器の配備により先制攻撃の選択肢が増えること、もしくは増えたように見えることは、既存の大国間の戦略的安定性を脅かす可能性がある。防御側は、ＨＧＶを探知してから短時間でその弾頭にWMDが搭載されているか否かの判断を迫られる。また、防御側の核戦力の配備場所に攻撃が向かっている場合、最悪の事態を想定して反撃し、意図しないエスカレーションを誘発する可能性がある。防御側は多様で複雑な経空脅威に対応するため、ミサイル防衛を追求するが、それがまたその防衛網を突破しようとして新興技術によるミサイル開発を助長し、軍拡競争が起こる。

新興技術による兵器のカテゴリーの拡大は、将来の軍備管理交渉に複雑さを提供することになり得る。ＨＧＶやＢＭＤといった戦略的含意を持つ兵器システムの推進に積極的な米中露３か国が保有あるいは開発する核・非核能力について、対象を限定すれば実際の戦略バランスとの乖離が生じ、逆に拡大すれば軍備管理の成立に必要な戦略バランスにかかる計算が複雑化するといったジレンマが生じる[24]。

極超音速兵器の開発は新たな脅威を生み出すことになり、これを克服するために国際社会、もしくは各国間において、どのような措置が必要かを検討することが急務である。第一に、これまでの新戦略兵器削減条約（新ＳＴＡＲＴ）の後継条約の議論の中でどのように極超音速兵器が位置付けられるのかが注目される。新興技術の開発状況を踏まえれば、米国とロシアに加え、中国を含めて軍備管理交渉を進める必要がある。戦略兵器を規制する枠組みに極超音速兵器が含まれることが望ましいが、大国間の現在の緊張関係を考慮すると、短期的には、協調的な対外政策について進展を見込むことはできないだろう。

まずは極超音速兵器の使用に係る誤解のリスクを軽減するための措置を講じつつ、米中露の極超音速兵器規制交渉への機運を高めていくことが望ましいとする意見がある[25]。その際に、透明性を向上させることは、その後の軍備管理交渉を支える役割を果たす。開発・配備状況やその運用のための方針を明らかにしていくことは、予見可能性を高め、誤解のリスクを軽減させるだろう。そして、その後に協議のテーブルに着き、極超音速兵器の特

---

[24] 戸崎洋史「第３章 ポストＩＮＦ時代の軍備管理」森本敏・高橋杉雄編『新たなミサイル軍拡競争と日本の防衛』（並木書房、2020年）123頁

[25] 有江浩一「極超音速兵器をめぐる米中露の取り組み―核抑止・核軍備管理への含意」『安全保障戦略研究』第３巻第２号（2023年３月）36～38頁

性や安全保障上の潜在的リスクについて、各国が定期的な意見交換を実施し、信頼醸成を図っていくことが求められる。

第二に、現状の国際社会においては、弾道ミサイル、巡航ミサイルに関する各国の開発・生産に対して法的義務を課す国際約束は存在しないが、既存の国際規範や輸出管理の取組について、新興技術を踏まえた議論を進めていく必要がある。例えば、「弾道ミサイルの拡散に立ち向かうためのハーグ行動規範」（ＨＣＯＣ）における事前発射通報の制度は、弾道ミサイルで打ち上げられた地上配備型ＨＧＶにも当てはまると考えられる[26]。また、各国の研究活動の進展とともに、極超音速技術に関する知識が予期しない形で拡散する可能性があり、輸出管理の強化を目指すべきである。そのためにも、ミサイルの開発に寄与し得る関連汎用品・技術の輸出を規制する「ミサイル技術管理レジーム」（ＭＴＣＲ）は重要な枠組みであるが、レジームの参加国でない中国を極超音速兵器の開発国として取り込んでいく必要がある。極超音速兵器が米中露を超えて拡散すれば、安定性への懸念が悪化する可能性が指摘されている[27]。米中露３か国をはじめ極超音速兵器の開発国はその技術の不拡散に注力すべきであろう。

５．おわりに

日本政府が策定した国家防衛戦略（2022年12月、閣議決定）では、戦略環境の変化が指摘され、科学技術の急速な進展が安全保障の在り方を根本的に変化させ、各国は将来の戦闘様相を一変させる、いわゆるゲーム・チェンジャーとなり得る先端技術の開発を行っていると言及された。実際の戦場にあっては、ＡＩ、サイバー技術、極超音速技術などの新興技術は、その他の既存の兵器システムと組み合わさることによって活用される。また、局地的な戦闘に供するだけでなく、戦争の大義、正当性への認識など国際政治的な優位性を確保するために情報操作等の場面でも活用され、これらの技術は軍事的な手段にとどまらない「ハイブリッド戦」の様相を引き起こしている。

そのため、国際的な安全保障環境に大きなインパクトを与え得るこのような新興技術の開発、利用には適切な軍備管理が要請され、場合によっては規制や制限が求められる。しかし、これらの新興技術については各国の安全保障に与える影響が大きいが故に、それに伴って戦略関係が複雑化し、合意を得ることが一層難しくなっている。新興技術に関する軍拡競争が、取り返しのつかない被害を生む前に、国際社会で議論を深化させることが期待される。

（てらばやし　ゆうすけ）

---

[26] Emmanuelle Maitre, “Arms Control and Delivery Vehicles: Challenges and Ways Forward,” *Journal for Peace and Nuclear Disarmament*, March 10, 2022, p.134.

[27] Kingston Reif, “Hypersonic Advances Spark Concern,” *Arms Control TODAY*, January/February 2018, p.30.