［サイバー・ウォーズ］

③ 情報通信技術（ICT）と安全保障

佐藤丙午 | 拓殖大学

戦争と技術

安全保障と情報通信技術の間には，歴史的に密接な関係がある．戦争において，時間，距離，場所による制約を技術的に乗り越える試みは，人類の歴史とともに古い．たとえば，トロイの陥落を狼煙や篝火で連絡したエピソード，アラマダの海戦におけるプリマスからロンドンへの連絡，米国の南北戦争におけるテレグラフの活用，近い歴史の中では，第一次世界大戦時の軍事上の発見として，機械化とラジオ技術が挙げられることが多い☆1．

第二次世界大戦以降の戦争や国際関係では，特に情報通信技術の飛躍的進化が，その動向を大きく左右してきた．情報通信技術は Information and Communication Technology（ICT，日本では IT と呼ばれることが多い）と呼ばれるようになり，米国の第二次オフセット戦略の下で軍事面での活用が拡大した．ICT の軍事的意義が実証されたのは，1991 年の湾岸戦争である☆2．この戦争は，ネットワーク中心戦闘（Network Centric Warfare）の軍事的可能性が実証された戦争とされる．

さらに 90 年代以降，旧ユーゴスラビアをめぐる紛争，さらには同時多発テロ後の対テロ戦争やイラク戦争などにおいて，攻撃手段の効率化や拡大に加え，暗号技術や解析技術の活用による情報作戦の分野でも，ICT の活用が進んだのである．特に，映像技術，計算技術，衛星技術により，通信，指揮統制，偵察監視，兵力の効率化，ナビゲーション，そして気象分野などの分野で軍事利用は拡大した．21 世紀の戦争では，ICT によって獲得した情報を人工知能（Artificial Intelligence：AI）で処理し，兵器システムの自律化につなげる試みも見られる．

ICT と安全保障の関係を考察する上で，軍事技術革命（Revolution in Military Affairs：RMA）と社会の関係の分類および，その後の情報 RMA における議論が，基本的な思考枠組みとなる．RMA と社会の関係では，社会の変化が RMA をもたらす，もしくは RMA によって社会の在り方が変化する，など，軍事社会学的な議論が展開されてきた．そして，情報 RMA の議論では，アンドリュー・マーシャル（Andrew Marshal）が進めた ICT を使用した軍の作戦の効率化についての政策論が進められた☆3．

本稿では，1990 年代の RMA の議論を出発点として，国際関係論を基盤に，軍事社会学と政策論の双方で進化した ICT と安全保障の関係を振り返る．その上で，2020 年代の議論を展望し，ICT を含む新興技術の安全保障上の課題を説明する．

RMA 論と軍事技術開発

1990 年代の RMA の議論や，GW ブッシュ（G. W. Bush）政権期の軍事変革（Transformation），オバマ（Barack Obama）政権期の第三のオフセット戦略などに見られるように，科学技術の進化は戦争の在り方を変え，それが国家戦略や，軍事的な調達政

☆1 Krepinevich, A. F. Jr. : The Military-Technical Revolution : A Preliminary Assessment (CSBA, 2002).

☆2 クレピネビッチの評価は，最初 CSBA より 1992 年に発表され，その後更新版が 2002 年にまとめられた．Krepinevich, A. F. Jr. : The Military-Technical Revolution : A Preliminary Assessment (CSBA, 1992).

☆3 Davis, N. C. : An Information-Based Revolution in Military Affairs, in John Arquilla, David Ronfeldt, eds., In Athena's Camp: Preparing for Conflict in the Information Age (RAND, 1997).

策に影響を及ぼす．米国の各政権で語られた軍事技術と安全保障に関する政策は，それぞれ政治的用語は異なるが，実質的には類似の事象を扱ってきたものである．その本質は，技術の進化が国際社会をどのように変えるか，そしてその中で米軍が目指すべき状態は何か，である．

技術進化が見られる限り，戦争の進化も止まらない．歴史を振り返っても，火薬の発明，蒸気機関などの内燃機関の登場，通信技術の発達，そして原子力の活用も，技術進化が戦争を変えた例として考察できる．特に原子力の軍事利用では，戦争の目的を，戦闘による破壊ではなく，抑止（戦争を止めること）へと変化させた[☆4]．

このように，科学技術が国際システムを変革する潜在性があることは，多くの研究者によって指摘されてきた[☆5]．科学技術の成果を軍事面に適用し，それが革新的な成果につながるとすれば，各国にとって，科学技術は国際政治におけるパワーを補正する重要な手段となる．その際，科学（Science）と技術（Technology）のうち，科学的知見を国家として蓄積し，動員できるのが有効か，もしくは社会的に必要な機能を技術的に実現する能力が必要なのか，議論が分かれてきた．また，科学技術のオーナシップの問題は，さらに科学技術と国家の関係を曖昧にしている．政府主導で技術開発プロジェクトを推進した時代は終わり，今日の国際社会において，国家は技術開発の主導者ではなく，すでに存在するものの受益者に過ぎないとの主張も存在する．この場合は，科学技術を効果的に動員できた国が，国際社会でパワーを行使することが可能になる．

その際，科学技術が社会に及ぼす長期的なインプリケーションについて，社会の変化と科学技術の関係を説明する上で，社会の変化が科学技術の進化を促すのか，科学技術の変化に合わせて社会が適用するのか，という概念的な二分法で議論されることがある[☆6]．

たとえば，19 世紀の工業文明の到来とともに，内燃機関を中心とした軍事技術革命が進行した．この最大の受益者は近代海軍建設で先行した英国であった．英国は工業化を前提とする海軍を維持する上で，世界各地に拠点が必要となった．これが，植民地主義の 1 つの側面である．他の欧州諸国も世界規模の海軍建設に乗り出し，整備・修理・補給等の拠点を求めたため，帝国主義の拡大につながったと解釈される．つまり，軍事技術の革命が，国際社会に影響を与えた一例といえる．

戦略爆撃の歴史からも，技術が社会に大きく影響を与えたことが分かる．戦略爆撃は，戦略論との関係の中で社会を変えていった．戦略爆撃は，航空機の発達とともに考案された攻撃方法であるが，上空からの爆弾投下の精度は低く，反撃による被害と，付帯被害が大きいという欠点があった．しかし，作戦に関連する被害の軽減が必要という社会的要請に直面したとき，特に米軍は 3 つの選択肢に直面した．それらは，価値攻撃（戦略爆撃による都市攻撃），原爆（効率的に反撃の手段を奪う），そして精密誘導爆撃である[☆7]．

冷戦という特別な戦略環境の下，米国はソ連に対して科学技術の優越性を維持するとともに，ソ連の通常兵器による急襲に対抗するため，情報通信技術を活用した精密誘導兵器の開発と，それに合わせた戦略の採用へと進んだのである．この選択は，米軍が情報の優越の下でのみ作戦を実施するという特徴をもたらした．

ただし，米国によるこの戦略の採用は，1970 年代にソ連のオガルコフ（Marshal Nikolai V. Ogarkov）による軍事技術革命の議論に触発されたもの

☆4 Brodie, B. : Strategy in the Missile Age (RAND, 1959).
☆5 Weiss, C. : How Do Science and Technology Affect International Affairs?, Minerva, Vol.53, No.4, pp. 411-430 (2015).
☆6 Liaropoulos, A. N. : Revolutions in Warfare : Theoretical Paradigms and Historical Evidence," The Journal of Military History, Vol.70, No.4 (2006).
☆7 Sapolsky, H. M. eds. : US. Military Innovation since the Cold War: Creation without Destruction (Routledge, 2009).

であった．ソ連が考案し，米国が採用したこの「エア・ランド・バトル（Air-Land Battle）」の重要なポイントは，情報の優越の維持と，情報通信技術の活用である．後に 1991 年の湾岸戦争で国際社会が目撃したように，ステルス技術，各種センサ技術，GPS 誘導兵器，レーザ管制兵器，衛星通信，暗視装置等の活用による，戦闘の効率化と彼我の軍の被害の限定は，目に見える形で実現したのである☆8．

もちろん，湾岸戦争でこのトレンドが確定し，その後のトランスフォーメーションや第三のオフセット戦略へと，その後の軍事技術と戦略が自動的に転換したものではなく，伝統的な兵器を重視する勢力からの抵抗，予算の優先をめぐる兵種間の争い，特に陸軍からの抵抗などに直面している．さらに，2001 年 9 月の同時多発テロ後，軍の作戦に対する社会の要請も変化した．テロ組織や反体制勢力を壊滅するためには，航空戦力による精密爆撃ではなく，陸上兵力が，低強度能力しか持たない敵と低強度紛争を戦う必要が生まれた．

しかし，陸上における低強度紛争でも，また海上においても，ICT による戦闘の効率化は，技術進化の中で必要不可欠になっていった．特に位置情報の把握，偵察活動，部隊間の情報伝達など，作戦を促進する条件の部分で，ICT の活用は作戦運用を助けた．2003 年のイラク戦争において，ストライカー旅団を中核とする軽機動部隊がイラク国内に侵入して，ごく短期間にバグダッドを制圧できた理由の 1 つに，米国側の情報の優越があったことは言うまでもない．そして，ICT による作戦効率の追求は，戦争の進化の合理的な結論に至ることになる．

たとえば，2010 年代の後半に政策として確立する「マルチ・ドメイン戦略（日本ではクロス・ドメイン戦略）」は，各軍種間の統合作戦の推進，その一環として各軍種の作戦に対する相互の作戦協力が前提となる☆9．具体的には，地上部隊は近接して敵対勢力を撃破するのではなく，遠隔攻撃を行い，また別の部隊は特殊部隊化して精密誘導爆撃の着弾点の観測および連絡要員として活用する，などの戦い方が一般的になる．ICT は，これらの作戦を可能にする技術（Enabling Technology）と位置付けられる．

ICT を活用した戦争の変化が，そのまま国家関係の変化に直結するものではない．多くの科学技術は，戦闘方法の効率化に貢献するが，社会変革を企図していない．変革との関連では，たとえば，アメリカ革命やフランス革命以降進んだ自由主義および民主主義の世界的な普遍化が，国家動員を合理化して徴兵の制度化を促した面はある．一般的な兵役制度の下では大人数の兵員が確保可能とあり，特に陸上戦力が必要な戦争（占領戦）の遂行には有利となる．

しかし，ICT の活用が進み，占領戦の必要性が下がった戦略環境では，兵員の数は必要ではなく，個々の要員の技術的専門性が重要になる．サイバー空間まで戦闘領域を拡大するとすれば，そこにおける戦闘員は，ハッカーや SE，さらにはゲーマーなどが最適な「兵員」となる☆10．つまり，ICT と国家関係の変化に相関を見るとすれば，戦闘方法と戦争様相の変化が同時に発生した際に，特定の社会条件（社会の構造変化が発生している等）の下で発現すると理解すべきなのであろう．

そして，ICT を含む新興技術などを活用する戦争が，社会条件とは無関係に，社会の構造変化につながるかどうか，注目すべきなのであろう．

ICT と安全保障における文化的要因

一般的に社会の構造変化は，所定の社会条件に影響され，ICT と安全保障の関係では，それが文化

☆8 湾岸戦争によって，1980 年代に欧州で想定された戦略を中東地域で展開した米軍は，戦争の方法についても，陸上勢力と航空勢力のバランスの逆転をなし遂げた．この方法は，ボスニア（1995 年）およびセルビア（1999 年）における戦闘にも引き継がれた．戦略爆撃の歴史は，Pape, R. A. : Bombing to Win : Air Power and Coercion in War（Cornell, 1996）に詳しい．

☆9 Joint Doctrine Note（JDN）1-18, Strategy (Washington, DC: U.S. Government Printing Office, 25 April 2018).

☆10 Harris, S. : @ War : The Rise of Cyber Warfare (Headline, 2014).

的要因と，包括的な意味で，社会における技術の価値に左右される．

戦争において，各国が考案する選択肢の傾向は異なる．入手可能な技術レベルと，地理的および地政学的な戦略環境に応じて，各国はそれぞれ異なった戦術を採用する．さらに，その選択内容には，文化的な要素も存在する．たとえば，国際関係論の現実主義や，戦略論的に考えて，日本は核保有を選択しても不思議ではないとされる．しかし，被爆体験からくる反核感情の影響から，核兵器開発への道を歩んでいない☆11．

安全保障における文化的要因には，経験から導かれた教訓として蓄積されたものも存在する．本土に対する直接攻撃に過剰に反応する米国，戦争で獲得した領土を失うことを極端に嫌がる中国やロシアなども，文化的要因から自由ではない．このため，文化的要因による戦術選択を助けるものとして，科学技術の位置付けを考慮すべきである．

1970 年代後半以降，米国が欧州においてエア・ランド・バトル戦術を重視した理由の 1 つに，共産圏勢力が西ドイツに地上軍で急襲をかけた場合，防御線を突破されて西ドイツや NATO 軍の中核部分や，在欧の戦術核施設を破壊され，反撃手段が限定されることに対する恐怖があった．このような戦術的劣勢を挽回するためには，核兵器による反撃あるいは先制攻撃が考えられるが，それは世界規模での核戦争を覚悟する必要がある．全面核戦争を回避するためには，共産圏勢力の攻撃の兆候を早期に探知し抑止のメッセージを強化するか，攻撃を受けたとしても，少数の戦力で効果的に侵略を撃破する必要がある☆12．ここに，C4IR の強化の中核を担うものとして，ICT が重要な意味を持つのである．

この問題を文化的に見ると，可能な限り人的被害を限定したい米国の社会的要因が深く関係する．米国は 1960 年代から 1970 年代初頭までベトナムでの泥沼に苦しんでいた．北ベトナム軍や南部に侵入したベトコンと米軍との軍事力の差は明確であったが，北ベトナム側は非対称戦争で米軍に被害をもたらした．この結果，米兵の消耗は大きく，米国内においても可視化できる被害が続出したため，国民の世論は反戦に傾いたのである．民主主義国において，国民の支持が欠ける戦争を遂行するリスクは大きい．ベトナム戦争後の米国は，戦争において人的被害を最小限にする方策を模索してきた．

湾岸戦争を経て，1996 年 7 月に公表された Joint Vision 2010 では，米軍の将来は，大規模兵力ではなく，小規模で精強な兵力に依存し，長射程な精密誘導ミサイルなどの，遠隔地からの兵力投射能力を重視することになる，としている☆13．つまり，米軍への被害を限定し，個別の戦闘の行方が世論に与える影響を管理することを重視しているのである．ただし，1990 年代中葉に示された航空戦力重視の RMA は，米国内では大きな批判に直面した．戦争の最終的な結果を決めるのは陸軍であるとの主張は根強く，たとえ陸上戦闘で米軍に被害が出たとしても，航空優越では勝利を収めることができないため，航空作戦は陸上作戦に従属するとの主張が見られた☆14．

米国における技術開発は，人道的問題に起因するケースが多い．たとえば，イラク戦争後に米軍の兵站を担った PMC が反体制勢力に攻撃され，場合によっては残忍に殺害され，映像化されたことがある．この事件が米国の世論を硬化させた経験に基づき，兵站の自動化を目指す自動運転技術開発への投資が増大した．さらに，福島原発事故のように人間による作戦が不適な環境や，イラクでの反乱掃討作戦などで経験した，混乱した都市部での近接戦闘の回避などを目的に，ロボット開発も進められている．

☆11 岸　俊光『核武装と知識人：内閣調査室でつくられた非核政策』（勁草書房，2019 年）．

☆12 Skinner, D. W : Air Land Battle, Professional Paper 463 (CAN, 1988).

☆13 Joint Chiefs of Staff, Joint Vision 2010.　同様の点は，Joint Vision 2020 にも盛り込まれている．

☆14 Press, D. G : The Myth of Air Power in the Persian Gulf War and the Future of Warfare, International Security, Vol. 26, No.2, pp. 5-44 (Fall, 2001).

AIの開発は，自動運転技術やロボットなど，新興技術の軍事転用が進められ，戦略への影響が展望される中で，その可能性が追及されるようになった．

ICTは軍事作戦のすべての局面に関係するため，米国におけるRMA論議とは直接的に関係なく進展した．米国では2012年にパネッタ（Leon Panetta）国防長官が，「現在の戦争を戦いつつ将来の挑戦に準備する」との方針を発表し，陸軍対空軍の戦略爆撃論争に一応の終止符が打たれた．そして，将来への挑戦において，統合運用の下での作戦の効率化の追求が進められたのである．

この方針は2014年にヘーゲル（Chuck Hagel）国防長官により，第三のオフセット戦略として再確認され，トランプ（Donald Trump）政権も方針を引き継いだ☆15．2018年の国防戦略では，米軍の目標はテロ組織との戦いや小規模紛争を戦うことではなく，国家間の戦略競争を戦うことと規定し，特に中国やロシアを念頭において，米国の軍事的優越性の再確立を目標として掲げている☆16．この間の米国の技術政策における目標は明確である．それは，新興技術により，戦闘における目標探知や攻撃，さらにはその評価までを含めた「キル・チェーン」を効率化することで，新たな戦場のネットワークシステムを構築することと解釈できる．

「キル・チェーン」は攻撃サイクルとも呼ばれる．攻撃サイクルの効率化は，米国だけの問題ではなく，中国やロシア，また日本においても同じ方向を向いていた．たとえば，サイクルの中でAIを活用する方針は，（攻撃手段の自律化を含め）米国ではなく中国や韓国，さらにはイスラエルなどの方が効率的に実施している面がある．米国の比較優位が減退した理由は，米軍がRMA論争を繰り広げ，各軍が将来の挑戦に向けた必要な投資を制限したためである．したがって，米国が優越を再確立するためには，伝統的な軍を強化するのではなく（ICTの適用は，強化のための手段であるとする見方もある），新たな戦争の方法の確立が必要とされたのである．

このため，第三のオフセット戦略およびトランプ政権の安全保障政策の下では，新興技術の可能性を念頭に，新たな戦争の方法の模索が続けられてきた．この方法は，技術に合わせて兵器開発を行う，いわゆる「技術決定論」とは異なる．技術決定論は，先端的な技術の開発が実現した後に，それを活用した兵器開発を検討するものである．一般的には，「ある技術から兵器を作る」という方が理解しやすいかもしれない．これに対し，「兵器主導開発論」では，必要な兵器構想の下で技術開発が進むという形態を想定する．

技術決定論と兵器主導開発論は，兵器開発においていくつかの前提の下で成立する．技術決定論では，そもそも新興技術は開発されるものであり，技術へのアクセスを含めて，その兵器への技術の応用の程度が問題となる．兵器主導開発では，技術開発に必要な資金や人的資源の確保を兵器の発注側である政府が保証する形をとるため，閉鎖された環境の下で進められることになる．たとえば，米国の軍事産業は第二次世界大戦における政治経済体制の下で，生産態勢が規定され，兵器主導開発への適応が容易な構造になっている．

しかし，ICTを含めた新興技術の開発は民間企業主導で進められ，各国において，軍の側は技術開発の受益者になるという構図の下にある．このため，民間分野と軍事分野の協力が必要になっているのである．

新興技術と官民協力

社会的な意味を含め，技術により，戦争の方法が根本的に変化するかどうかは，新しくて古い，安全保障議論の重要なポイントである．恐らく安全保障

☆15 Ellman, J., Samp, L. and Coll, G. : Assessing the Third Offset Strategy, CSIS (March 2017).
☆16 https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

論の教科書には，防衛装備の基本的な機能として「動く」，「撃つ」，「交信する」を挙げて，それぞれの機能の進化の方向性を説明していくだろう．

「動く」機能には，自軍による兵器等の操作に加え，相手の行動を探知して突入する行動等が含まれる．この領域では，IoT などの利用範囲の拡大に助けられ，低コストで広範に存在する民間分野の技術を活用して，遠隔地での探索活動等も，新たな役割と規定される．さらに，治安活動目的で利用される顔認証技術や携帯電話の位置情報の活用，さらには決済ツールの利用など，ICT の活用により，広範なデータ収集と分析が可能になっている．これら広範なデータ収集の手段としては，宇宙における衛星，サイバー手段なども想定され，その解析には，将来的には量子計算機などが使用されると指摘される．

「動く」機能の高度化において，センサーなどを大量に配置してデータを収集して状況把握能力を高めることは，戦場における「マス」の復活を意味する．人的コストの削減と正確性を目的としてユビキタスに配置されたセンサーから収集されたデータは，人間では処理できない分量のため，必然的に AI の活用が進む．そして情報処理能力が高度化すれば，IoT を含めて，低コストで配置できるセンサの数は増加する．同時に，もし動力源の問題が改善されるとすれば，規模（小型化と大量生産）と速度の問題が解決され，自律兵器の開発は加速度的に進むことになる．

自律化された兵器の特徴と課題は，データ収集から判断に至るまで，「キル・チェーン」の下に分割された各種機能の自律化をシステムとして運用することになるため，戦闘自体は，システムの無力化を目的とすることに重点が置かれる．その意味で，戦争の進化において，「撃つ」機能は実態的には大きく変化することになる．安全保障論では，攻撃方法として対価値攻撃と対軍事攻撃という二分法を導入したが，システム自体の無力化が必要になるということは，攻撃対象としての価値と軍事とが区別困難になっていくことを意味する．

つまり，新興技術の発達により，「撃つ」機能がサイバー攻撃，通信妨害，電子戦闘，ソフトウェアに対する攻撃（書き換えや情報盗取など）などまで拡大することになり，それらがハードウェアに対する攻撃と同等の価値を持つことになる．さらに，「動き」と「撃つ」が高機能化することになると，探知から攻撃までの時間が短縮され，戦闘が軍事的合理性の下で高速化される可能性が生まれる．これは，戦争が外交と並ぶ政治の手段ではなく，それ自体に別の価値を持つことを意味する．それを，戦争の「ゲーム化」と呼ぶことも可能であろう．そして極端に言うと，「ゲーム化」され，政治性を失う戦争において，実態上，前線と後方の区分が曖昧になり，既存の国際法の適用は困難になる．そして，戦闘員同士ではなく，社会全体が軍事的なリスクに直面することにつながる．

さらに，「交信する」機能において，軍の指揮命令系統に特有の中央での管制ではなく，前線の部隊や「プラットフォーム」間の通信による，分散化されたネットワークの戦闘へと変化する．航空部隊におけるロイヤル・ウィングマンは，母艦となる戦闘機が複数の異なる機能を持つドローンを操作する戦闘システムである．同様のシステムは，潜水艦でも運用されており，陸上の戦車システムの無人化を含めると，戦場での情報収集・分析および作戦運用を分散化するのは，各軍種で進められていることが分かる．同時に，プラットフォームの小型化により，操作員が指揮統制するターミナルの数は増加傾向にある．人間が操作可能なターミナルの数を超える場合，そこでも自律化が進められることになる．

「交信する」機能の基礎インフラである通信関係の技術では，5G 通信の普及が進む．通信技術と計算技術（量子科学の発達が期待される）の先に，暗号化技術や脳計算インタフェース技術を含む，さまざまな製品開発と実用が期待されており，軍事面ではスウォームやロボット化技術への期待が大きい．これらは，技術に対する期待が先行し

ている例であり，実際に民間技術の軍事転用が円滑に進むとは限らない．

包括的な表現を使用するとすれば，この問題は，技術のオーナシップと官民の技術協力の問題と規定できる．

技術のオーナシップ問題について，新興技術などの技術の知的所有権は，一般的に特許や占有等で開発者に帰属しており，たとえ国内に存在する技術であったとしても，政府は自由に使用できるものではなく，ユーザの一人に過ぎないということである．官民の技術協力については，特に防衛装備開発には大学や研究開発機関を含む，民間分野の協力が不可欠であるにもかかわらず，技術的に先行する民間分野は，軍事研究に抵抗があったり，軍事分野への協力には経済的に魅力がないなどの理由で協力に抵抗する，という問題である☆17．

中国においては，この問題を「軍民融合」で乗り越えようとしている．中国のように，権威主義的な国家資本主義の下では，AI などの新興技術の開発と利用を，人民解放軍が選択的に利用することが可能である．そして，社会のデータを独占的に収集し，利用することも可能となる☆18．日米のような民主主義や自由主義を掲げる国家群は，ICT などの新興技術を活用した新しい戦争において，技術の活用に関する官民協力には制約が多く，なおかつ社会の体制は硬直的である．

では，新興技術を活用する新たな戦争は，国家資本主義勢力が有利になり，国際システムもパワーの変革に向かうのだろうか．多くの研究が，米中関係において，米国の通常抑止能力の浸食が，これまで米国が影響力を維持してきた世界の各地域を不安定にすると指摘している．地域の不安定化は，米国の抑止力の低下や限定と同時に，各国の経済政策や国際政策に対し，中国が影響を行使することで，それぞれの国内政治が不安定化することによっても出現する．中国の進める国家資本主義，もしくは「新中華圏」の構築に対して，米国が有効に対抗する体制を構築しない限り，米国の漸進的衰退の懸念は続くことになる．

自律兵器開発の課題

軍事力の近代化において，ICT をレガシー・システムに最適化し，その更新に資源を投入するのであれば，米国に限らず，ロシアであったとしても中国との量的な競争に勝利することはできない．中国はすでに AI を含めた新興技術への投資を拡大し，「新しい戦争」への体制を強化している．このため，日米両国は質的な競争により，パラダイムの異なる戦争での勝利を追求しなければ，既存の国際秩序の不安定化に直面することになる．

異なるパラダイムの戦争の構成要素である新興技術が「キル・チェーン」を効率化する上で，2 つの課題が生じている．1 つが，軍事システムの開発における民間部門と軍事部門の協力体制の構築である．2018 年の Project Maven をめぐる Google 社内の議論や，2019 年の Microsoft の全国防総省のクラウド受注問題を見る限り，民間企業と軍の関係には複雑な愛憎関係が存在する．この問題は，中国では表面化しにくい．今後，米中の間で，民間企業との協力関係をめぐる不均等な競争条件が，どのように変化するか，注目する必要がある．

第二の問題は，自律兵器開発をめぐる倫理の問題である．兵器の自律化による課題については，2014 年以降特定通常兵器使用禁止制限条約（CCW）の下で議論されており，2019 年には 11 項目の指導原則が合意されている．自律化された兵器はもたらす問題は，人間の意図を超えて自律的に攻撃を展開し，国際人道法が順守されない状態が生じるという懸念である．米国は 2020 年 2 月に，AI と軍事の関係を規定する 5 つの倫理原則に合意してい

☆17 What is Project Maven? The Pentagon AI project Google employees want out of, Global News, April5, 2018.
☆18 Kai-Fu Lee : AI Super-Powers : China, Silicon Valley and the New World Order (HMH, 2018).

る[☆19]．しかし，国際社会，米国，そしてそれ以外の国々との間で，倫理原則や遵守ガイドラインが異なるとすれば，それが緩い国が新興技術の兵器化で有利な立場を獲得することに対する懸念は大きい．

この2つの要素は，ICTなどの新技術を新たな戦争に向けて活用すべきかどうかという議論の現代的な本質になる．1991年の湾岸戦争後は，精密誘導に管制可能な戦略爆撃の利用が，戦争の革命かどうか議論され，陸上兵力に対する航空兵力の優位が主張された．米国社会としては，これは犠牲者ゼロ戦略として歓迎すべき方向性だったのであろう．しかし，米国が戦略的競争相手ではなく，テロ組織や反体制勢力を撃破し，掃討する「小さな」戦争や反乱鎮圧作戦も重視される過程で，1990年代に議論されたRMAではなく，ICT等を利用した効率的な小部隊や特殊部隊作戦の中に，新興技術の活用方法を模索するようになった．その成果の1つが，ビンラディン暗殺作戦であった．

しかし，中国やロシアなどのような戦略的競争相手の出現とともに，これら諸国との対抗手段として，新興技術の役割が再定義されていった．技術決定論と兵器開発論の枠内にとどまらない兵器開発の方法が検討され，そこで伝統的な兵器システムを前提とした戦争を前提とした安全保障戦略の非効率が強調されるようになった．量的および質的な優位を背景に，たとえ，敵対相手が米軍の脆弱な部分で一時的に優勢を確保したとしても，スピードを伴う展開能力と，相手の状況を正確に把握する能力によって反撃し，勝利することができる力は，米国の通常抑止の基盤を構成した．しかしその能力が，戦略的競争相手の登場とともに無効化され，勝利を実現できなくなった状況での戦略の在り方は，従来の安全保障政策の変更を迫るものとなったのである．

ICTなどの新興技術には，上記の2つの制約があったため，概念的には，パラダイムの異なる兵器システムを構築する方法と，伝統的な兵器システムにICTなどの新興技術を組み込んで能力更新を図る方法が存在した．後者の方法は，既存のドクトリンや組織運営を合理化する方法であり，過去，多くの軍で試みられ，多くの場合は失敗に終わった．前者の方法は，新たな戦略，ドクトリン，組織構成が必要になるため，軍の持つハードウェアだけでなく，作戦運用などのソフトウェアも更新する必要がある．成功が保証されていない手法の採用には，組織内の抵抗が大きい．

つまり，ICTの技術的状況や，新興技術の可能性を考慮し，米中の戦略バランスの問題を考えると，自律兵器の採用は不可避であるが，その採用の方法をめぐって，人道規範と軍事的効率性を共存させる方策を模索する必要があったのである．

将来の課題

過去に発生したと評価される軍事技術の革命が，国際システムの変革にまで至った例は少ない．たとえば，特定の武器弾薬や，それを利用した戦術の変更により，特定の国が大国の地位へと上昇した例は多いが，その地位が構造的に維持され続けた例は少ない．この理由として考えられるのは，技術は伝播・拡散するため，技術をベースにしたパワーは平準化されるためとされている[☆20]．

平準化は，国際的な技術移転に加え，軍事システムの維持コストによる長期的なパワーの低減によってももたらされる．さらに，その時点で優越した軍事システムを無効化する新兵器システムの開発も大きな影響を与える[☆21]．新興技術が出現する際，各国が常に神経質に反応する理由は，先行して行った軍事投資が無駄になるのではないかという恐怖があるためである．ICTを含む新興技術の作戦運用への

☆19 DOD, Release : DOD Adopts Ethical Principles for Artificial Intelligence (Feb. 24, 2020).

☆20 Schmid, J. : The Diffusion of Military Technology, Defence and Peace Economics, DOI: 10.1080/10242694.2017.1292203

☆21 Brodie, B. : Sea Power in the Machine Age, Princeton University Press, pp.105-23, 434 (1943).

適用において，それが「キル・チェーン」の中で可能性を高める技術であることから，伝統的な兵器システムの更新にも，さらには新しい戦争の方法においても使用される．新興技術による戦争の変革は，政治的な効果が伴う必要はない．

長期的に見ると，平準化の防止は困難であり，その速度を遅らせることで，比較優位を確保することが現実的な方策になる．もちろん，敵対国に欠ける技術を特定して管理する手法も存在する．たとえば，中国の軍民融合や攻撃的な技術獲得戦略，さらにはAI大国を目指す方針などは，国家政策として平準化を目指すとともに，それを超えて優位的な立場の獲得を目標とするものと解釈できる．このため，米国を中心とする西側諸国が，中国の技術政策に神経質な反応を示すのも，これまでの軍事技術の歴史を振り返ると，自然な反応である．

ICTを含む新興技術による軍事技術革命は，その中核技術が民間企業にあり，情報やデータ等も民間企業が保有しているため，それらを利用して他国がキャッチアップするのは容易である．この問題は，情報作戦（Information Warfare）において一層明確になる．もし双方が同じレベルの情報と技術を持っており，その平準化が不可避的に進むのであれば，重要な技術や情報を保護する側が，比較優位を持つことになる．中国の国家資本主義との競争が懸念される理由は，技術や情報の保護において，中国が不均等な条件を作り出しているためである．米国がオバマ政権の二期目以降，新興技術の管理方法を検討してきたのも，技術や情報の防護の戦略的意義を理解しているためであろう．

比較優位をもたらすもう1つの要素が，空間的制約である．各国は，その戦略的環境に合わせた兵器の採用を進める．国家間の係争地に物理的に近くで作戦活動を実施する場合，兵站や整備補給等の拠点に近い方が有利になる．その量的優位に対抗するために質的優位を追求するのが一般的な反応であるが，ICTを含む新興技術では，質的優位を実現するのが困難な事例が多く，場合によっては平準化の速度を加速することが想定される．

このように，ICTは各国の安全保障に，大いなる機会と課題を投げかけており，この問題を継続的に評価分析することが必要なのである．

（2020年4月2日受付）

佐藤丙午　hsatou@ner.takushoku-u.ac.jp
一橋大学大学院修了．防衛庁防衛研究所主任研究官を経て，2006年より拓殖大学海外事情研究所教授，2013年より国際学部教授．拓殖大学国際学部・海外事情研究所副所長（現職）．専門は，国際関係論，安全保障論．