

デュアルユース・テクノロジーをめぐって

小林信一 こばやし しんいち

科学技術イノベーション政策アナリスト

今日のデュアルユース・テクノロジー(両用技術)の主役は、人工知能(AI)などの情報技術(IT)である。ITは軍事のみならず、民生分野でも重要かつ有望な技術であるだけに、IT分野の両用性は大学にとって避けて通れない問題である。今回は、軍事研究と民生研究との関係、両用技術の発展について整理したい。

1. 世界を駆け巡った日韓の軍事研究ニュース

2018年4月、奇しくも同時期に、日韓両国の科学技術と軍事研究にまつわるニュースが世界を駆け巡った。

2015年度に発足した防衛装備庁の「安全保障技術研究推進制度」を契機として、日本学術会議は2017年3月に「軍事的安全保障研究に関する声明」を発表し、「軍事目的のための科学研究を行わない」等の過去の声明を継承するとともに、「軍事的安全保障研究と見なされる可能性のある研究について、その適切性を目的、方法、応用の妥当性の観点から技術的・倫理的に審査する制度を設ける」ことを大学等に要請した。およそ1年を経て、審査制度の導入状況等についてアンケート調査を実施し、第1次集計結果を2018年4月3日の総会で公表した。集計結果によると、審査制度のある機関が約26%、検討中が約33%であり、必ずしも対応が進んでいない。また、検討していない機関が約41%あるが、その主たる理由は、軍事的安全保障研究を実施する可能性がほとんどないから審査制度は不要だということだった。

翌4月4日頃から、韓国科学技術院(KAIST)がAIを利用した自律型殺人ロボットを開発する可能性があるとして、世界の主要なAI研究者が連名でKAIST総長宛の公開書簡を発し、自律型殺人ロボットの開発をしないと明言しない限り、KAISTとの共同研究をボイコットすると宣言したというニュースが世界を駆け巡った。これは、2018年2月20日にKAISTが設立した国防人工知能融合研究センターが、韓国の有力な防衛企業、ハンファシステム(Hanwha Systems)の資金提供により運営されていることから、あるメディアがAI兵器を開発するのではないかと疑義を呈したことが契機だった。結局は、KAIST総長が、センターはAIの基礎技術の開発が目的だと表明したので、AI研究者たちは4月9日にボイコットを撤回した。

大騒ぎになった要因の一つは、AIを搭載した機械が自律的に判断して殺傷する「自律型致死兵器システム」を禁止すべきだという議論が、数年前から国連で、ホーキング博士を始めとする世界中の有力研究者たちの先導により進められていたことである。AIを利用した兵器であっても、殺傷などの判断は人間が下すべきだという考え方である。KAISTのセンターが自律型殺人兵器の開発を目指すのであれば、この原則に反する。もう一つの要因は、有力な兵器メーカーの資金を受け入れたことで、軍事研究をするセンターであると誤解されたことである。センターの名称が、AIの国防分野への応用を連想させたことは否定できない。また、センターの研究は基礎技術開発に止まるとする一方で、そこで開発された技術をハンファシステムが軍事技術へ応用してもKAISTの与

り知らないというスタンスも示された。

ほとんど同時期のニュースだったが、日本では大学が軍事研究へ参画することに躊躇する傾向がみられるのに対して、KAISTは防衛産業から資金を得て、センターの名称にも国防を冠するなど、両国の違いが目立つ。しかし近年、オーストラリア、EC(欧州委員会)などでも、大学研究者に対する防衛技術分野の研究資金助成が始まっており、大学と軍事研究の関係は世界的に議論的になっている。日本の大学の軍事研究の扱いが、次第に韓国のそれに近づく可能性も一概には否定できない。

2. 基本的概念の整理

まず、基本的概念を整理しておく。

(1) 軍事技術、民生技術、安全保障技術

技術開発の対象が、兵器の開発など軍事目的であるか、一般の人々の生活やそれに関連する産業に関わるものであるかの違いに着目して、軍事技術と民生技術とを区別する。国防技術、防衛技術、安全保障技術といった語も用いられるが、軍事技術、国防技術、防衛技術は、若干のニュアンスの違いはあるが、実質上は同じもののだとしても概ね問題はない。

一方、安全保障技術は曖昧な概念である。後述するように、冷戦後に米国は、産業技術の強化を通じた国際競争力の向上を経済安全保障と表現し、安全保障の一分野として位置づけた。また、「人間の安全保障」の概念も登場し、安全保障の概念は軍事的な意味を超える概念となった。しかし、民生分野の技術開発にまで範囲を広げて安全保障技術と言うことには違和感がある。日本学術会議は、軍事的手段による国家的安全保障を「軍事的安全保障」とした*1。混乱を避ける上で妥当な定

義だと思われる。

(2) 両用技術、スピノフ、スピノン

軍事技術と民生技術は明確に分けられるとは限らない。基盤的技術の中には、軍事技術としても民生技術としても応用できる技術が少なくない。そのような技術を両用技術と呼んできた。また、スピノフは、軍事技術を民生用に転用すること、スピノンは、民生技術を軍事技術に転用することを指す。スピノフ、スピノンは結果的に軍民両用の技術となることから、これらを含めて両用技術と呼ばれることがある。しかし、両用技術をあまりにも広義に捉えてしまうと、明らかな軍事技術、民生技術まで含んでしまうため、議論を混乱させる要因になる。

今日的な狭義の両用技術の概念は、冷戦終結後の米国の独特な歴史的な文脈の中で独自の意味を獲得した。それは、結果として技術が移転するスピノフやスピノンではなく、最初から軍民両用を目指して開発する、あるいは近い将来の軍事転用を狙いつつ、まずは民生用として開発する技術である。そのため、開発当初は、外形的に純粋な民生技術の開発と区別することが困難になる。だからこそ、大学での両用技術の扱いが問題になる。狭義の両用技術はスピノフ、スピノンと区別するべきであろう。

(3) スピノンと COTS

スピノンは、技術のレベルで民生技術を軍事技術に転用することを言うのに対して、製品のレベルで既存の民生品を軍事用に利用することもある。この民生品を COTS(Commercial-Off-the-Shelf)と呼ぶ。民生品であれば何でも利用できるというわけではなく、軍事用の納入品に対しては仕様(Mil-Specと呼ばれる)が微細に定められており、それを満たす必要がある。

(4) デュアルユース・ジレンマ、科学技術の両義性

軍事技術とは関係のない基礎研究であっても、あるいは人類の幸福を願って進められる研究でさ

*1—軍事科学という概念もある。軍事衛星等で収集した膨大なデータは、科学の材料としても貴重であり、それを一般の科学研究で用いることができれば、科学にとってもメリットがある。米国の場合は、国防総省が研究資金を提供し、そのようなデータの活用による基礎研究を支援してきた。このような活動を軍事科学と呼ぶが、国防部門の予算の制約のため縮小傾向にある。Sharon Weinberger, The changing face of military sci-

ence, *Nature*, vol. 477, pp. 386-387(2011).

え、ある種のものはテロや犯罪に悪用される危険性がある。科学技術のこのような性質を両義性と呼ぶ。病原菌の遺伝子改変などによるバイオテロなどが典型的な悪用のケースとして想定され、バイオテクノロジー分野を中心に発生する危惧がある。基礎研究は公開が原則であるが、悪用への懸念から公開しないように政治的な圧力がかかる可能性もある。このような科学技術の両義性は、デュアルユース・ジレンマ^{*2}と言われる。

デュアルユース・ジレンマの概念は、日本学術会議が「用途の両義性」という言葉で表現したものに近い^{*3}。もともと日本学術会議は dual use の日本語訳として「用途の両義性」を提唱した。その背景には、「科学技術の成果は、本来、それを用いる者次第で、人類の福祉の向上に使われる場合もあれば、悪用・誤用により、人類に害をなす場合もある」といった通念がある。この理解にもとづけば、軍事技術もスピノフ、スピノオンも、狭義の両用技術、民生技術も、すべて「用途の両義性」の概念の下で両用技術に含まれてしまう。日本学術会議が取り上げた主たる問題は、デュアルユース・ジレンマであり、「用途の両義性」はデュアルユース・ジレンマの日本語訳とするほうが適当だろう。

3. 両用技術の由来

冷戦後の米国で、最初から軍民両用を目指して技術開発を進めるといふ今日的な両用技術の概念が登場した。日本における軍事研究と大学との関係については杉山(参考文献参照)に譲り、ここでは両用技術の概念が米国で成立した経緯を紹介する。

なお、吉永(参考文献参照)も参照されたい。

*2—Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, National Research Council, *Biotechnology Research in an Age of Terrorism*, National Academy Press, p. 1(2004).

*3—日本学術会議「科学・技術のデュアルユース問題に関する検討報告」(2012).

3.1. 冷戦後の軍事研究

冷戦の終結は、米国において国防関連予算を削減させ、国防分野の装備品などの取得(acquisition)、研究開発(Research, Development, Testing and Evaluation: RDT&E)や調達(procurement)に大きい変化をもたらした。RDT&Eに関しては、1980年代前半に大きく増加したが、1987年以降は横ばいとなり、冷戦終結後減少に転じた。1991年の湾岸戦争の後には2000年まで、RDT&Eはほぼ横ばいで推移したが、米国同時多発テロ後には再び増加し、2010年以降は減少に転じている。調達は1977年以降1987年まで10年間にわたり大幅に増加するが、1987年以降10年間は急激に減少し、実質価格ベースで1997年の調達額は1987年の半分以下になった^{*4}。

冷戦終結に伴う国防予算の減少は、国防分野の支出のあり方を変えた。第1は、国防関連品の取得改革による経費削減である。1994年6月に国防総省(DOD)のウィリアム・ペリー長官は、経費削減のために、国防用の納入品に適用されるMilSpecの緩和とCOTSの取得を推進する方針を打ち出した。この方針は、クリントン政権下の国家安全保障委員会の1995年の「国家安全保障科学技術戦略」にも引き継がれた。

第2はスピノオンの推進である。歴史的には、第二次世界大戦後に、原子力の平和利用やロケットの宇宙開発への応用、コンピュータなど、軍事技術のスピノフが進んだ。1980年代には逆に、民生分野の半導体技術、材料技術などの発展の結果、先端技術のスピノオンの重要性が高まった。1990年代以降は、ソフトウェアを含むITの進展が速く、IT分野のスピノオンが重要になった。この傾向は現在も続いている。

第3は両用技術の推進である。冷戦後に、両用技術は最初から軍民両用を目指して開発を進めるといふ意味で使われるようになった。冷戦後に両用技術が重視されることになった最大の要因は

*4—Office of the Under Secretary of Defense (Comptroller), National Defense Budget Estimates for FY 2018, pp. 142-148 (2017)

国防予算の大幅な減少のために、国防産業とその研究開発基盤を従来のまま維持することが困難になった。国防産業の業界再編が進み、縮小した産業基盤、研究開発基盤の上で半導体技術、材料技術、ITに独自に対応することは困難になっていった。その上、1980年代以降、米国の産業界は国際経済競争にも直面していた。そこで「国家安全保障科学技術戦略」は、国防のための軍事技術基盤と民生向けの産業技術基盤とを別々に維持することは困難であることから、民間のほうに技術開発が進んでいる、または民間の技術開発のほうに速いと予想される技術分野に関しては、軍事技術の開発を民間の産業技術開発基盤に依存する方針を打ち出した。ここで提案された両用技術の要点は、産業技術開発基盤の上で国防用、民生用の技術開発を並行して推進するところにある。

3.2. 経済安全保障と両用技術開発

「国家安全保障科学技術戦略」は、新たに経済安全保障の概念を導入した。国際経済競争力強化を安全保障の新たなドメインとして国防政策の中に位置づけ、両用技術開発はこのための手段となった。これが、冷戦後の両用技術の新しい意義である。「国家安全保障科学技術戦略」は、両用技術開発を支援する施策も提示したが、民生用にも資する技術開発を支援する点で国防予算による産業技術政策とも言える。

国防用と民生用の両方に資する技術開発の支援策は1993年にすでに開始されていた。この両用技術開発プログラムの運営は、高等研究計画局(Advanced Research Projects Agency: ARPA)^{*5}が担当していた。ARPAの施策は、潜在的な軍用技術として期待される新興商業技術にテコ入れし、商用市場で育てることで、開発コストを低減するとともに、技術を温存することを狙った。ここに冷戦後における両用技術の意義が表されている。後に

*5—現在の国防高等研究計画局(Defense Advanced Research Projects Agency: DARPA)。設立当初はARPA、その後DARPAに改称し、1993年からARPAに戻ったが1996年には再びDARPAとなり、現在に至っている。

DARPAは類似のプログラムを継続的に実施し、今日に至るまで多様な両用技術開発プログラムを展開してきた。

両用技術の特徴は、それが最終的に軍事技術として利用されることになるとしても、もっぱら民間企業や大学などの研究基盤の上で開発が行われ、外形的には民生技術の研究開発の体裁をとることにある。その意味で、純粋な民生技術の開発と区別することは困難^{*6}で、また開発された技術が商業的成功を収め、社会に便益をもたらすこともあるので、両用技術か民生技術かの判断は容易ではない。とくに、21世紀に入って以来、IT関連分野ではその傾向が顕著である。

4. ポスト911の軍事・諜報技術研究

4.1. 軍事・諜報環境の変化

21世紀に入る頃から、国防・諜報^{*7}活動のあり方が大きく変わった。インターネットの普及に伴って、サイバーテロ、サイバー戦争が深刻になった。1990年代にはすでにハッカー集団が軍事機密を狙ってサイバー攻撃をしていた。重要機関、重要インフラを混乱に陥れ、また軍事機密などを狙ったサイバーテロも現実的問題になった。1990年代末のコンゴ紛争、中東紛争ではすでに国家間のサイバー戦争が起きていたと言われる。このような姿の見えない敵が組織的に行うサイバー攻撃から情報システムを防御し、情報の流出を防ぐサイバーセキュリティが安全保障の重要な課題となった。

2001年9月11日に発生した米国同時多発テ

*6—研究資金源が、政府の国防部門か基礎研究の支援部門かで、軍事技術と民生技術を区別することは妥当であるように思われる。しかし、大学研究者が民生技術開発を装った軍事研究費を迂回して得ることは容易で、その場合、大学の審査には限界がある。また日本の総合科学技術・イノベーション会議は、政策の対象として防衛技術研究開発を徐々に取り込んでおり、非防衛部門向けの研究開発予算の一部が「デュアルユース」の名の下に、防衛技術開発に回されているという現実もあり、研究資金源を単純に軍事、民生に分けることには限界がある。

*7—本稿ではintelligenceとinformationとを区別するために、それぞれ諜報、情報と記す。

口は、国防・諜報分野に衝撃を与えた。国内に潜むテロリストへの対応は、伝統的な軍事衝突とはまったく性質が異なる。戦車、戦闘機などの正面装備を中心とする軍事力はほとんど意味をもたない。インターネットが発達した現代社会においては、個人の足跡がインターネット上に残されることが多い。市民社会に潜むテロリストを発見するためには大量の情報を収集し、ITを駆使して分析し、テロリストやテロ計画を割り出し、予防する諜報活動が重要になる。

4.2. ポケモン GO の逸話

1999年に米国中央情報局(CIA)はIT分野を対象とする非営利のベンチャーキャピタル(VC)、In-Q-Telを創設した。後述するように、伝統的な調達や委託研究ではなく、VCという手法を用いて、ベンチャー企業を発掘、育成し、民生技術の開発を支援し、その中から軍事・諜報部門にも有効な技術を調達することを狙った。

典型的な事例が、2001年創業のKeyhole社である。In-Q-Telは2003年に衛星地図ソフトEarthSystemを開発するKeyhole社に投資した。EarthSystemは不動産や都市計画向けに、ユーザが衛星画像や航空写真の巨大データベースにアクセスし、インタラクティブにバーチャルな映像を作り出す3D可視化技術として開発されていた。当時は、アフガニスタン、イラクで戦争が行われていた。テレビ局はEarthSystemを利用して、飛行体が作戦地域を飛行しているかのような3Dデジタル映像をバーチャルに作成して放映した。DODもEarthSystemを導入して、専用衛星で取得した画像を用いて軍事作戦を支援するシステムを構築していたと言われる。

Keyhole社は2004年にグーグル社に買収され、EarthSystemはGoogle Maps、Google Earthに組み込まれて普及した。その後Google Earthの技術は、衛星画像、地図情報などを利用した3Dマッピングの基盤技術として、各種のシステムに応用されていった。Keyhole社のCEOジョン・ハンケ氏は、2004年のグーグル社によるKeyhole

社買収後、グーグル社のGoogle Earthなどの担当副社長となり、2011年に社内ベンチャーとしてNiantic Labsを設立し、2015年にはグーグルから独立したNiantic社のCEOとなった。同社が2016年7月から一般ユーザ向けにサービスを開始し、世界的なブームとなったのが、位置情報とマッピング技術などを利用したゲーム、ポケモンGOである*8。

4.3. IT時代の両用技術開発

Keyhole社の事例はIn-Q-Telの出資事業の典型的な特徴を示している。インパクトのある基盤技術を開発し、商業市場で大きい成功を収めると同時に、国防・諜報部門でも利用された、IT時代の典型的な両用技術開発である。画像認識、GPSなどの位置情報技術、AI、ビッグデータ解析などIT関連分野の技術は、民生技術として重要であるが、国防・諜報部門にとっても重要である。

In-Q-Telが出資した技術には、監視カメラなどの情報を用いて、不審者をリアルタイムで特定するNORA(Non-Obvious Relationship Awareness)と呼ばれる技術がある。この技術は、事前に収集した情報を蓄積したデータベースの分析から、事前には明らかにされていなかった共謀関係にある人間関係を識別したり、特定の人物についてデータベースと照合することで、既存の犯罪者などと同一人物であるか否かを推定したりする技術である。空港、鉄道の駅などで活用することで、犯罪者や不審者の抽出など、セキュリティ技術として使えるほか、同一人物の移動などを特定することで、犯罪者やテロリストを捜索するためにも利用できる両用技術である。類似の技術として、インターネット上の膨大なデータから不正行為、犯罪、テロなどの監視に結びつく情報を探索するデータマイニング技術や、その基盤となるビッグデータの処理に適

*8—技術の源泉を辿るとCIAが登場するため、一部ではCIAがポケモンGOの開発やサービスに関与している、世界中のユーザの情報がCIAに集約されて諜報活動に利用されると疑われたこともあった。

したデータベース管理システム、AI技術などがあり、In-Q-Telはこれらも支援してきた。こうした技術は民生用として有望であり、多く大学研究者が研究対象としている。一方で、国防・諜報部門でもこれらの基盤技術は重要で、典型的な両用技術となっている。

4.4. In-Q-Tel モデル

IT関連分野の技術発展のスピードは速く、またベンチャー企業による貢献が大きいため、国防・諜報部門が従来から有する内部の研究開発活動、国防関連企業などからの調達では、必要な技術やツールを適時に入手することが困難であった。そこでCIAが考案した方法がVCの設立だった。In-Q-Telは、ベンチャー企業のネットワークにつながり、有望な技術を有するベンチャー企業を発掘し、出資して育成し、市場での成功を支援するとともに、国防・諜報部門の需要に適した技術を調達しようとした。

生産、販売を行う事業会社が社内外にVCをもつ場合、それをコーポレート・ベンチャーキャピタル(CVC)と呼ぶ。そのうち、キャピタルゲインよりも、自社またはスポンサー企業の本業の長期的発展に寄与する可能性のある技術を探索し、出資により技術開発を支援し、将来的に製品の供給を受けたり、技術を導入しようとするものを戦略的CVCと呼ぶことがある。In-Q-TelはCIAの戦略的CVCである。In-Q-Telの出資は、CIAなどが直面する問題に対するソリューションの獲得にもつながる。換言すれば、In-Q-TelはVCの方式による両用技術の振興策である。

In-Q-TelはVCなので、ベンチャー企業、研究者らが、起業や研究開発のための資金獲得を目指して多数のビジネスプランや技術提案をIn-Q-Telへ持ち込む。これはIn-Q-Telにとって都合がよい。In-Q-Telは持ち込まれた提案を通じて、関連企業や研究者などの存在、公表前の最新の技術動向を把握することができる。さらに、大学や研究機関の研究者、他のVCなどとの間で形成されたネットワークを通じて、In-Q-Telは膨大で良質

な技術情報を蓄積できた。In-Q-Telは、この情報資産を活用して、技術調査を行い、特定の課題の解決に貢献しうる技術や研究者、ベンチャー企業等を特定し出資した。CIAの需要を満たす技術や製品が見つければ、CIAはそれを取得すればよいが、諜報部門の特殊な要求を満たすものはほとんどないため、In-Q-Telは有望なベンチャー企業に出資したり、CIAに仲介して、諜報部門向けの開発も支援する。

ベンチャー企業へ出資すれば、In-Q-Telは上場前のベンチャー企業やアイデア段階の技術情報にアクセスできるようになり、CIAの要求にかなう技術の早期の同定、CIAの要求にかなう方向への開発の誘導も期待できる。また、複数のVCが関与することで、In-Q-Telの出資額を上回る総出資額を確保するレバレッジ効果も期待できる。多数のVCが関わることで、投資先ベンチャー企業は技術的な支援を得るだけでなく、潜在的な需要が提示されることにより販路を見据えた開発が可能になるなど、マーケティング面での支援も受けることができる。

4.5. DARPAの懸賞金競争

21世紀に入って、DARPAは新しい両用技術開発施策を開始した。アマチュアの研究者や研究チーム、ベンチャー企業など、伝統的な研究助成では対象とならない潜在的な研究開発力をもつ人々の力を集約することを狙った懸賞金競争(Prize Competitions)^{*9}と呼ばれる政策モデルである。2004年にグランドチャレンジと呼ばれる自動走行車コンテストを実施して以来、AI、ロボットなどの分野で多数のコンテストを実施してきた。これらのコンテストで取り上げられた技術は、自動運転、AI、ロボット分野の基礎的技術として民生分野に大きいインパクトをもたらすと同時に、

^{*9}—懸賞金競争による科学技術の推進施策は古い。1714年に英国議会は、経度を一定の精度で計測する方法を開発した者に懸賞を出すという法律を制定したのが最初だと言われる。また、2004年以降、Xプライズ財団が実施する多数の懸賞金競争も有名である。

戦争にも革命的変革をもたらすと期待される両用技術である。

2010年アメリカCOMPETES再授權法は懸賞金競争を、財政支出の一つの方法として規定した。その結果、現在では政府全体で多様な懸賞金競争が実施されており、懸賞金競争の連邦政府横断的なポータルサイトChallenge.govも運営されており、すでに825を超える競争が実施されたと言う*10。

5. IT時代のイノベーション政策の新しいモデル

In-Q-Tel、懸賞金競争は、両用技術開発の観点を離れれば、IT関連分野のイノベーション政策の革新的なモデルと言える。米国では、IT関連分野の今後の重要技術の開発が、このような斬新な手法によって支援されている事実は注視すべきである。

新しい政策モデルとして注目すべき点はいくつかある。第1はイノベーションの担い手の変化に適應したことである。IT関連分野では、ベンチャー企業が新しい技術を開発し、それがプラットフォーム技術として成功し、多様な機器やシステムに組み込まれることがある。また、アマチュアの個人やチームが革命的な取組を行うこともある。このように、IT関連分野の研究開発では、ベンチャー企業やアマチュアなど、非伝統的な研究開発の担い手が大きい影響力をもっている。しかし、伝統的な調達や委託研究などの施策ではこれらの新しい担い手への接近は難しい。この障壁を乗り越える手法として登場したのがIn-Q-Telや懸賞金競争である。

第2は、資金の提供よりも、各種の情報の収集とイノベーションを促進するネットワークの形成に重点をおいた施策であるという点である。情報収集の点では、In-Q-Tel、懸賞金競争ともに、

アイデア段階や研究開発途上の技術情報や潜在的な研究者やチームに関する情報を集める仕掛けをもっている。ネットワーク形成の点では、In-Q-Telの場合は、他のVCやベンチャー企業、大学研究者などのネットワークに加わり、民間VCとの共同出資などを通じて、ネットワーキングを促進する。つまり、既存のネットワークを活用し、それを刺激することでイノベーションを促進する施策である。また、今日では政府がITの巨大需要家となり、政府の調達や投資がIT産業の成長を左右するようになってきているが、IT産業と政府とを結びつける能力をもつのがIn-Q-Telである。懸賞金競争は、やはりコンテストの主催者が広範な先端技術情報を獲得でき、多数の潜在的な開発チームを掘り起こして接触することができるという特徴がある。さらに、参加者にとっても、コンペに参加することで技術動向を把握でき、他のチームやベンチャー企業、VCなどのネットワーキング、商用化の機会の獲得、政府機関からの調達や委託研究が期待できる。このように、In-Q-Telも懸賞金競争も、研究開発を資金的に支援するというよりは、ネットワークを刺激してイノベーションを促進する施策である。そのため、委託研究や調達と比べて資金規模は小さく、コストパフォーマンスの点でもメリットがある。

第3は、「ネットワークの失敗」を克服するイノベーション施策だという点である。「ネットワークの失敗」とは、例えばベンチャー企業などがイノベーションを実現する上で適切な能力をもつ信頼すべきパートナーを見つけられない状況を指す。In-Q-Telや懸賞金競争は、技術シーズを発展させて商用化を目指す施策というより、技術の利用イメージを示して、それを実現する技術開発を促進するニーズ側からのアプローチである。こうして、多様な経済主体が協働するための公共空間を生み出そうとしている。

In-Q-Tel、懸賞金競争はIT分野の特性と、米国のベンチャー文化の上に成立している。そのため、同様の施策が日本で実現可能かはわからない。ただし、In-Q-Tel、懸賞金競争のコピーを作ると

*10—Challenge.gov website (<https://www.challenge.gov/about/>)参照(2018年4月22日現在)。

いう意味ではない。技術情報の収集、潜在的な研究者、チームの発掘、ベンチャー企業や VC を含むネットワークの活性化を実現する施策が日本でも可能か、が疑問の本質である。DARPA ロボティクスチャレンジに参加し、予選で最高得点を挙げた東京大学からのスピノフベンチャー SCHAFT 社が、2013 年にグーグル社に買収されたというニュースは、日本のベンチャー企業の優秀さを示すと同時に、その企業を発掘し、投資したのが米国のイノベーション政策と米国企業であったという現実を日本社会に突きつけた。最終的には 2017 年にソフトバンクが買収したが、優れた IT 関連ベンチャー企業へ接近する適切なチャネルと支援策がないために、日本政府はその成長を初期段階から支援する機会を逃した可能性がある。

日本でも、IT 系ベンチャー企業が CVC やベンチャーファンドを設定し、ベンチャー企業へ出資するケースがここ 2、3 年増えている。自ら事業を行うベンチャー企業が、本業との相乗効果を狙ったり、将来の買収候補となりうる技術やベンチャー企業を育成したり、技術情報やマーケット情報などを獲得することを目的として投資を行う戦略的 CVC を創設している。日本のベンチャー文化はすでに変容しつつある。

日本には、大規模な大学発ベンチャー支援ファンドも存在している。2012 年度補正予算で、東京、京都、大阪、東北の 4 国立大学に対して総額 1000 億円が出資された。例えば、東京大学への政府出資金総額は 417 億円だった。東京大学が政府出資金をもとに造成可能なファンドの総額は In-Q-Tel のこれまでの投資総額に匹敵すると見込まれる。In-Q-Tel は日本の大学がもつファンドと比較して決して大きくないにもかかわらず、顕著な成果を上げていることを直視すべきである。逆に言えば、日本の大学ファンドにも可能性はある。

6. オープンで継続的な議論を

両用技術に戻ろう。日本における安全保障技術研究推進制度の導入は、大学や学界で軍事研究や両用技術に関する議論を巻き起こした。多様な議論があるが、今日では IT 関連技術を中心に、多くの技術が両用技術としての潜在的可能性を有することから、軍事技術、両用技術の線引きは困難になってきている。各大学が研究計画を審査するとしても、研究資金の出所が問題の本質なのか、研究開発の意図や目的が問題の本質なのか、一般の基礎研究のように研究成果の公開が許されているか否かで判断するのか、定義上も実態上も明確ではない。

この点に関しては、米国の大学における軍事研究の扱いが、長い議論や試行錯誤を経て、次第に明確なルールとして定着した歴史がある。詳細は岡村(参考文献参照)に譲るとして、少なくとも、オープンな場で議論を継続することが大切であることは確かであろう。本稿は、大学における狭義の両用技術の扱いに関して、特定の立場を主張するものではない。それは、IT 技術が両用技術の重要な対象となった今日、大学における両用技術の是非を決定することは非常に困難であり、オープンな議論によってのみ、合意の可能性があると考えるからである。

参考文献

- 杉山滋郎『「軍事研究」の戦後史』ミネルヴァ書房(2017)。
小林信一「CIA In-Q-Tel モデルとは何か」『レファレンス』793号, pp. 25-42(2017). <DOI: 10.11501/10308612>
小林信一「ポスト冷戦, ポスト 911 の科学技術イノベーション政策」『冷戦後の科学技術政策の変容』pp. 5-20(2017). <DOI:10.11501/10314912>
吉永大祐「デュアルユース政策の誕生と展開」『冷戦後の科学技術政策の変容』pp. 79-98(2017). <DOI:10.11501/10314917>
岡村浩一郎「米国の大学における国防研究」『冷戦後の科学技術政策の変容』pp. 99-120(2017). <DOI:10.11501/10314918>