PACIFIC FORUM

21st Century Technologies, Geopolitics, and the US-Japan Alliance: Recognizing Game-changing Potential

Edited by Brad Glosserman, Crystal Pryor, and Riho Aizawa
Japanese translations by Harunari Soeda, Yu Inagaki, and Erika Hongo

ISSUES & INSIGHTS

SPECIAL REPORT

VOL. 21, SR1 | April 2021

Pacific Forum

Based in Honolulu, the Pacific Forum (www.pacforum.org) is a foreign policy research institute focused on the Asia-Pacific Region. Founded in 1975, the Pacific Forum collaborates with a broad network of research institutes from around the Pacific Rim, drawing on Asian perspectives and disseminating project findings and recommendations to global leaders, governments, and members of the public throughout the region. The Forum's programs encompass current and emerging political, security, economic, and maritime policy issues, and works to help stimulate cooperative policies through rigorous research, analyses and dialogues.

TABLE OF CONTENTS

ABOUT THE AUTHORS

Kathryn Ibata-Arens is Vincent de Paul Professor of Political Economy, DePaul University. A scholar of innovation and entrepreneurship, science and technology policy, and economic development, her most recent book published in 2019 by Stanford University Press, is Beyond Technonationalism: Biomedical Innovation and Entrepreneurship in Asia. Using the lens of venture start-up firms in China, India, Japan, and Singapore, Beyond Technonationalism finds a new "networked techno-nationalism" guiding national policy and firm-level strategy supporting competitive growth in frontier technologies. Her 2021 book Pandemic Medicine: Why the Global Innovation System is Broken and How We Can Fix It (Lynne Rienner Publishers) analyzes international competition in new drug discovery and access to essential medicines. Ibata-Arens is also researching emergent organizations supporting sustainability of natural medicine and the plant biodiversity upon which it depends. Ibata-Arens earned a doctorate in political economy from Northwestern University while a Fulbright Doctoral Fellow at the Research Center for Advanced Science and Technology (RCAST) at Tokyo University. She served on the METI-State Department Japan-US Innovation and Entrepreneurship Council, and serves currently on the Board of Directors of the Japan-America Society of Chicago, on U.S.-Japan bilateral advisory boards for the American Council on Education (ACE) and the Okinawa Institute of Science and Technology Graduate University (OIST) Foundation, and as a member of the U.S.-Japan Council (USJC).

キャサリン・イバタ＝アレンスは、デポール大学ヴァンサン・ド・ポール教授（政治経済学）です。イノベーションと起業家精神、科学技術政策、経済開発の研究者であり、2019 年にスタンフォード大学出版局から出版された最新の著書は『Beyond Technonationalism: Biomedical Innovation and Entrepreneurship in Asia』（邦題：科学技術立国の彼方に：アジアにおけるバイオメディカルイノベーションとアントレプレナーシップ）です。『Beyond Technonationalism』では、中国、インド、日本、シンガポールのベンチャー・スタートアップ企業の視点をもとに、フロンティア技術における競争的成長を支える国家政策や企業レベルの戦略を導く新しい「ネットワーク化されたテクノナショナリズム」を発見しています。2021 年に出版された『Pandemic Medicine: Why the Global Innovation System is Broken and How We Can Fix It』（邦題：パンデミック医学・薬剤：なぜ私たちの世界技術革新システムが壊れた？直せる方法へ）（Lynne Rienner Publishers）では、新薬開発における国際競争と必須医薬品へのアクセスについて分析しています。また、イバタ＝アレンスは、自然療法の持続可能性とそれが依存する植物の生物多様性をサポートする新興の組織についても研究しています。イバタ＝アレンスは、東京大学先端科学技術研究センター（RCAST）でフルブライト博士研究員を務める中、ノースウェスタン大学で政治経済学の博士号を取得しました。彼女は「経済産業省・米国国防省より日米イノベーション・アントレプレナーシップ・カウンシル（IEC）」に任命。現在はシカゴ日米協会の理事、アメリカ教育協会および沖縄科学技術大学院大学財団の日米諮問委員会委員、米日カウンシルのメンバーを務めています。

Akira Igata is currently the Executive Director and Visiting Professor at the Center for Rule-making Strategies, Tama University. He is also a Senior Adjunct Fellow at Pacific Forum, a US-based think tank. He advises the Japanese government, bureaucracy, and the private sector in various capacities. His research expertise includes: Economic statecraft; Influence operations; International Politics in the Indo-Pacific; and Japan-US relations.

井形彬
多摩大学ルール形成戦略研究所 事務局長・客員教授
多摩大学ルール形成戦略研究所客員教授・事務局長。米国シンクタンクのパシフィック・フォーラム Senior Adjunct Fellow や、国際議員連盟の「対中政策に関する列国議会連盟（IPAC）」経済安保政策アドバイザーを兼務。その他様々な立場から日本の政府、省庁、民間企業に対してアドバイスを行う。専門分野は、エコノミック・ステイトクラフト、インフルエンス・オペレーション、インド太平洋における国際政治、日米関係。

Keisuke Inoue
Director of FabLab KandaNishikicho
Part-time lecturer at Tama Art University
After working as a research assistant in Tama Art University, Inoue joined to FabLab Shibuya as one of its founding members. With a background in media art and installation skills, Inoue specializes in creation utilizing both digital and analog techniques. He is responsible for both Planning & Production and human resources development for Digital Fabrication Association (DFA).

井上恵介
ファブラボ神田錦町ディレクター
多摩美術大学非常勤講師
多摩美術大学で研究助手を務めた後、創立メンバーの一人としてファブラボ渋谷に参加。メディアアートとインストール技術の経験から、井上はデジタルとアナログの両方の技術を利用して作成することに特化している。主にデジタルファブリケーション協会（DFA）の企画・制作と人材育成の両方を担当。

Erick Nielson C Javier is a Defense Research Officer II of the National Defense College of the Philippines. Previously, he served as a Defense Analyst of the Office of Strategic Studies and Strategy Management, Armed Forces of the Philippines from 2015-2021. He completed his Master of Arts in Political Science, Major in Global Politics at the Ateneo de Manila University in 2017. His research interests include geopolitics, geoeconomics, great power competition, revolutions in military affairs and the future of warfare. His work experience includes Track II defense diplomacy, strategic studies research, scenario building and military wargaming.

エリック・ニールソン・C・ハビエルは、フィリピン国防大学の第二種防衛研究員です。以前は、2015 年から 2021 年まで、フィリピン国軍の戦略研究・戦略管理室の防衛アナリストを務めていました。2017 年にアテネオ・デ・マニラ大学でグローバル政治を専攻し、政治学修士号を取得。 研究テーマは、地政学、地経学、

大国間競争、軍事問題における革命、戦争の未来など。実務経験としては、トラックⅡ防衛外交、戦略研究調査、シナリオ構築、軍事作戦演習などがあります。

Elsa B. Kania is an Adjunct Senior Fellow with the Technology and National Security Program at the Center for a New American Security (CNAS) and a Research Fellow with the Center for Security and Emerging Technology at Georgetown University. Her research focuses on Chinese military innovation and technological development. At CNAS, she contributes to the Artificial Intelligence and Global Security Initiative and the "Securing Our 5G Future" program, while acting as a member of Digital Freedom Forum and the research team for the Task Force on Artificial Intelligence and National Security. Elsa was a 2018 Fulbright Specialist and is a Non-Resident Fellow with the Australian Strategic Policy Institute's International Cyber Policy Centre. Elsa has been invited to testify before the House Permanent Select Committee on Intelligence, the U.S.-China Economic and Security Review Commission, and the National Commission on Service. Currently, Elsa is a PhD student in Harvard University's Department of Government.

エルサ・B・カニアは新アメリカ安全保障センター（CNAS）テクノロジー・国家安全保障プログラムの Adjunct Senior Fellow。ジョージタウン大学セキュリティ・新興テクノロジーセンター（CSET）研究員も務める。専門は中国の軍事イノベーションと技術開発。CNAS では「人工知能とグローバルセキュリティ構想」や「アメリカの 5G の未来を守る」プログラムに参加する一方、「デジタルフリーダムフォーラム」や「人工知能と国家安全保障タスクフォース」の研究チームメンバーとしても活動している。2018 年のフルブライトスペシャリストであり、オーストラリア戦略政策研究の「国際サイバー政策センター」で非常駐研究員も務める。また「下院諜報活動常任特別委員会」「米中経済安全保障審査委員会」「軍事、国家、公共サービスに関する国家委員会」に招集され証言を行った実績がある。現在はハーバード大学政治学部博士課程に在学中。

Margaret E. Kosal is Associate Professor in the Sam Nunn School of International Affairs at Georgia Institute of Technology. Her research explores the relationships among technology, strategy, and governance. She focuses on two, often intersecting, areas: reducing the threat of weapons of mass destruction (WMD) and understanding the geopolitics of emerging technologies.

マーガレット・E・コサル博士は、ジョージア工科大学サムナン国際問題大学院の准教授です。彼女の研究は、技術、戦略、ガバナンスの関係を探るものです。特に、大量破壊兵器（WMD）の脅威の軽減と、新興技術の地政学的理解という、しばしば交差する 2 つの分野に焦点を当てています。

Edward Parker is an Associate Physical Scientist at the RAND Corporation, a nonprofit, nonpartisan public policy research organization. (He wrote this paper in his personal capacity; the views expressed here represent his own opinions and not the views of the RAND Corporation.) Dr. Parker's research focuses on the societal impacts of emerging technologies, with a particular focus on quantum technology and artificial intelligence. He received his Ph.D. in theoretical quantum physics from the University of California at Santa Barbara.

エドワード・パーカー博士は、非営利・無党派の公共政策研究機関であるランド研究所のアソシエート物理学者です。（本論文は個人の資格で執筆したものであり、ここで述べられている見解は、ランド研究所の見解ではなく、彼自身の意見を表しています）。パーカー博士は、新興技術の社会的影響を研究しており、特に量子技術と人工知能に焦点を当てています。彼はカリフォルニア大学サンタバーバラ校で量子理論の分野で博士号を取得しています。

Willem Thorbecke is a Senior Fellow at the Research Institute of Economy, Trade and Industry. Prior to this he was a Senior Research Fellow at the Asian Development Bank Institute and a professor at George Mason University. He has written many papers investigating the determinants of trade flows in Asia and the rest of the world and the spillovers that result from trade.

ウィレム・トルベッケは、独立行政法人経済産業研究所(RIETI)の上席研究員です。それ以前は、アジア開発銀行研究所のシニアリサーチフェロー、ジョージ・メイソン大学の教授を務めていました。アジアを始めとする世界中の貿易の流れの決定要因や、貿易から生じる波及効果について、多くの論文を執筆しています。

Mariko Togashi is a research assistant at the Edwin O. Reischauer Center for East Asian Studies and a second-year student at Johns Hopkins University School of Advanced International Studies, concentrating in Strategic Studies. She earned her undergraduate degree in International Law at Keio University, Tokyo. Previously, she worked as an equity analyst in the technology sector at Deutsche Bank and Bank of America Merrill Lynch. Her research interests include geoeconomics, economic statecraft, technology and security, and U.S.-Japan relations.

富樫真理子は、エドウィン・0・ライシャワー東アジア研究センターのリサーチアシスタント兼、ジョンズ・ホプキンス大学高等国際問題研究大学院修士課程所属（戦略研究専攻）。慶應義塾大学法学部法律学科にて学士号を取得。大学院以前には、ドイツ銀行とバンク・オブ・アメリカにてテクノロジーセクターの株式アナリストとして勤務。研究分野は、地経学、経済安全保障、テクノロジーと安全保障、日米関係等。

Takahiro Tsuchiya is currently an Associate Professor at Kyoto University of Advanced Science, Japan. He served as a researcher in the Consulate General of Japan in Hong Kong (2015-2017), Ministry of Foreign Affairs of Japan (2013-2015), and a lecturer in the department of Policy Management at Shobi University, Japan (2010-2014), where he taught the Chinese Economy, etc. Dr. Tsuchiya received his Ph.D. in Security Studies from the National Defense Academy, Japan. He earned the equivalent of a BA in Environmental Information from Keio University and an MA in Economics from University of Hitotsubashi. His research focuses on Industrial Policy on Advanced Science and Technology, Civil-Military relations, Foreign Policy, Security Studies, and International Relations. Areas of specialization include China and East Asia. His major written work is *Military System of Modern China: The party, the government, and the*

army relations involving national defense expenditure and military expenditure, Tokyo: Keiso Shobo, 2015 (in Japanese).

土屋貴裕
京都先端科学大学経済経営学部准教授。安全保障学博士。慶應義塾大学環境情報学部環境情報学科卒業。一橋大学大学院経済学研究科修士課程修了。防衛大学校総合安全保障研究科後期課程卒業。在香港日本国総領事館専門調査員などを経て現職。専門分野は、公共経済学、国際政治経済学、安全保障論など。近年は、中国の経済安全保障戦略、とりわけ先端科学技術および新興産業に関する産業政策を中心に研究。著書に、『現代中国の軍事制度：国防費・軍事費をめぐる党・政・軍関係』（勁草書房、2015 年）ほか多数。

Mason Venturo is an analyst for Delta Air Lines. After completing a Master's in International Policy at the University of Georgia, Mason went on to work in supply chain studies at BSI before moving to Delta's Methods team where he has spent the past several months working on safely distributing vaccines and vaccine precursors around the world. Mason additionally worked for the Pacific Forum on a project centering on the discovery of the real economic impact of trade controls on strategic economic sectors. Mason's passions include nonproliferation and photography.

メーソン・　ヴェンチュリオは、デルタ航空のアナリストです。ジョージア大学で国際政策の修士号を取得した後、BSI 社でサプライチェーン研究に従事し、その後デルタ航空のメソッドチームに移り、過去数カ月間、世界中にワクチンやワクチン前駆体を安全に流通させることに取り組んできました。また、パシフィックフォーラムでは、EXBS が資金提供したプロジェクトで、戦略的経済部門に対する貿易管理の実際の経済的影響を明らかにすることを中心に仕事をしました。情熱を傾けているのは、核不拡散と写真撮影です。

KEY FINDINGS

Throughout the month of October 2020, with support from the US Embassy Tokyo, the Pacific Forum cohosted with the Center for Rule-Making Strategies at Tama University, the Keio University Global Research Institute, and the Okinawa Institute of Science and Technology a series of virtual panel discussions on "Game Changing Technologies and the US-Japan Alliance." Over 280 individuals joined the 10 sessions – 7 closed door and 3 public panels – that examined issues such as artificial intelligence, autonomous vehicles, big data, cybersecurity, drones, quantum computing, robots, and 3-D printing. A conversation of this length and breadth is difficult to summarize, but the following key findings attempt to capture this rich and variegated discussion.

General landscape

Mastery of new and emerging technologies is key to success in 21st century economic competition and global leadership. There is much talk about those technologies' impact on "the balance of power," but a fundamental question remains: The power to do *what*?

Technological prowess is vital not only to national defense and dominance, but also to provide a bulwark against interference by authoritarian governments in domestic and personal affairs. Democracies are losing their historical influence over technology development, standard-setting, and limiting proliferation relative to the growing capacity of authoritarian competitors, but this can be corrected.

Japan has made national economic statecraft a priority but has considerable work to do to deal with the suite of issues associated with creating and effectively exploiting emerging technologies.

The ubiquity of many of these technologies and government initiatives like China's Military-Civil Fusion (MCF) erase historical distinctions between military and civilian use. Traditional export controls focus on protecting military and dual-use items. The growing difficulty in distinguishing between military and civilian end-use and end-users makes export controls challenging to apply, and ineffective in practice.

Emerging technologies

Despite growing attention to emerging technologies in the US and Japan and acknowledgement of the need for coordinated action to regulate their use, disparities between the two countries in terms of knowledge about, impact of, and proficiency in these technologies inhibit coordinated action.

Uncertainties inherent in the development of "emerging technologies" make regulation of their use and control of their dissemination difficult, if not impossible. Identifying the appropriate technology to control is also problematic, and there is agreement that "casting the net" too wide will inhibit innovation.

There is an inherent tension between a desire for international collaboration to spur innovation and the perceived need to control access to technologies to preserve economic and security-related advantages, particularly to prevent their diversion by or to other countries.

While there is an instinct in the US to decouple economic exchange from perceived adversaries to prevent technology leakage, connections afford the US and its allies a window into the work of perceived adversaries and prevent surprise – both economic and strategic.

Economic incentives to get new technologies to market as quickly as possible may undermine the readiness of entrepreneurs to build in safety, security, and ethics. The declining cost of new technologies and their increasing availability to the public democratize access to dangerous tools and create a leveling effect among nations.

Cyberspace

If data is "the new oil" – and there was little dissent about this – then the norms and regulations regarding its "ownership" and/or use will be vital to success in the 21st century economy. Coordination among governments that facilitate or inhibit sharing of such data is critical.

We are only beginning to understand how data processing outcomes can be influenced by the types of algorithms used. Ostensibly "neutral" algorithms can prejudice decision-making by incorporating subtle but important biases. Even nontechnical policy people should seek to shine light into the algorithm "black box" to understand what assumptions are being made.

The COVID-19 pandemic has accelerated demand for better cybersecurity practices – and made plain the alarming gap in both the capacity and the will to implement those practices. At the same time, the pandemic-triggered recession has forced companies to cut their cybersecurity budgets just as they have increased spending on IT capabilities to account for a surge in remote working arrangements.

Be wary of comparisons of who is "winning" cyber or technology races. Much depends on the metrics used and assumptions about the nature of the competition. The "race" metaphor also obscures the importance of international collaboration and reduces the equation to a zero sum.

Identifying and thinking about cyberspace as a separate military domain on par with air, sea land, or space encourages clarity in relevant decision making – whether civilian, military, government, or private. On the other hand, such a distinction risks obscuring the fact that cyberspace is intrinsic to, and fully permeates, the other domains.

As governments attempt to secure national cyber networks, small- and medium-size businesses continue to struggle to protect themselves from cyberattacks. Their shortage of cybersecurity resources makes them vulnerable to cyberattacks, and both government and industry-driven initiatives have been launched to help these smaller businesses enhance their cybersecurity.

There is a tension between resilience and deterrence in national security planning for cyberspace. While technology is often the focus of security concerns, the human factor must not be overlooked. Trust may be the key concept in developing secure cyber networks.

Robotics

While there is concern about the role of robots or autonomous weapons on the battlefield and their impact on human control and delivery of intended effects, advocates counter that autonomous weapons can be discriminating and more accurate than humans, creating less collateral damage.

Public sensitivity to (or aversion toward) the application of advanced technologies in the national security space has kept some researchers (many Japanese but also some American) from considering the military applications of their work.

Semiconductors, 3-D Printing, and Supply Chains

Japan is several years behind the world in adopting additive manufacturing practices like 3-D printing. While 3-D printing offers many advantages, problems persist in acquiring the necessary raw materials for printing at scale. Effective utilization of 3-D printing will require more and better education about this technology.

The US has much to learn from Asia about reviving its manufacturing sector and resourcing supply chains.

Given a 60-70% cost differential between manufacturing in the US and China, relocating low-cost production out of China makes little sense in a short-term analysis that relies solely on cost. Yet there are competing and sometimes compelling longer-term factors to consider, such as geopolitical relations, political risk, and the security of supply chains in a crisis. Establishing new supply chains demands close attention to these factors.

For the US, a "National Manufacturing Guard," modeled after the National Guard, may be one way to ensure the availability of manufacturing capacity in a crisis such as a global pandemic.

Quantum Technology

While impressive progress has been made, the world is a long way from a game-changing quantum computing capability. Small quantum computing capabilities may appear in the next three to five years, but the potential – and the hype – outpaces the technology.

It is too early to tell which quantum technologies will have an impact on national security, and different states are pursuing different lines of effort. Japan, China, and the EU are prioritizing quantum *communications*, which might improve the security of encrypted communications. The US and a few other countries are focusing on quantum *computing*, which could threaten the security of encrypted communication, as well as provide useful commercial applications.

It is also too early to set broad international standards for quantum technologies. Instead, it may make more sense to focus on limited cooperation among allies or like-minded countries.

Biotechnology

Biotechnology proliferation poses new security threats as nefarious actors will be able to access these capabilities soon.

While most of the focus of biotechnology is on medical and health-related products, it is estimated that more than 60% of physical inputs into the global economy can be replaced by biological production.

A shift to biological production can yield profound reductions in energy, water use, and land use, along with substantial cuts in "food miles" (the distance from production to the table).

For new types of food production, economies of scale are not everything: there is room for individual or startup competitiveness. However, supply capacity is a key limiter, particularly with regard to amino acids and water.

While Japan has been developing biotechnologies, gains have been limited by bureaucratic factionalism and stove-piping between government departments.

Areas of Cooperation

Technology can only be successfully managed through whole-of-government and whole-of-society approaches. Policymakers should promote coordinated action between allies, partners and like-minded states, where technology-generated impacts have their most far-reaching effects.

The US-Japan Cooperation Dialogue on the Internet Economy, which included discussions with private-sector representatives, is a best practice for US-Japan cooperation. The exchange of ideas among industry, government, and academia will create an open architecture highlighting the values of transparency, vendor diversity, and standardization, creating market opportunities for US and Japanese vendors and benefitting third countries by improving supply chain security.

The fundamental challenge the US and Japan face in 5G competition is a lack of attractive, alternative options to very cheap technologies offered by China to third countries. An area of focus for the US and Japan in 5G should be R&D collaboration to ensure multi-vendor interoperability on technology challenges. Our countries should also be thinking to develop 6G technology, in particular multilateral and bilateral industry consortiums for standard-setting.

One important lesson from the US-Japan trade and technology competition of the 1980s is that the US exaggerated the "threat" from a highly capable competitor to a point that it almost missed opportunities to work together for mutual benefit. (The allies should not lose sight of opportunities to do so with China.)

The US needs an accurate understanding of government involvement in industrial development. The vital role that Washington played in creating what came to be known as Silicon Valley is often downplayed to foster a myth of "entrepreneurial independence" and advance ideological positions that are not based on history.

Alignment between the US and Japan on trade, investment, and technology controls is necessary. Otherwise, attempts to address shared security concerns will generate friction between our two countries. One vital step Japan can make is developing more sophisticated procedures to handle classified information, including a security clearance system. As a first step, the US and Japan should update their science and technology agreement signed in 1988.

要旨

パシフィック・フォーラムは、2020 年 10 月、東京の米国大使館、多摩大学ルール形成戦略研究所、慶應義塾大学グローバルリサーチインスティテュート、沖縄科学技術大学院大学と共に「革新的技術と日米同盟」について約 1 ヶ月間に亘るバーチャル形式のパネルディスカッションを行った。280 名を超える参加者が、人工知能や自動運転、ビッグデータ、サイバーセキュリティ、ドローン、量子コンピューティング、ロボット、３D 造形技術等をテーマにした 10 回のセッション(7 つの非公開セッションと 3 つの公開セッション)に参加した。これだけ長期に亘る幅広い議論を要約することは困難だが、この豊かで多様な議論を総括する試みとして以下にその要点を示す。

昨今の国際情勢

21 世紀の経済競争や国際的なリーダーシップにおいて成功を収めるには、新技術及び新興技術を制することが極めて重要である。これらの技術が「バランス・オブ・パワー」に与える影響については多く語られてきた。しかし、根本的な問いは残ったままである。つまり、一体何をするためのパワーなのかという問いである。

技術力は、国防や覇権にとって重要なだけでなく、他国の内政や個人のプライバシー等の領域に対する権威主義国家による干渉及び介入行為への防壁にもなる。

権威主義的な競争相手の能力が増大しているのに対して、民主主義国家は技術革新や規格の設定、拡散の防止に対するその歴史的な影響力を失いつつある。しかし、この状況は是正することができる。

日本はエコノミック・ステイトクラフトを優先事項としてきたが、新たな技術の創造、効果的な運用に関連したこれらの問題に対処する為に一段の努力が必要である。

これらの技術の遍在性、中国の軍民融合のような政府の取り組みにより、軍事用と民生用の歴史的な区別が付かなくなっている。従来の輸出管理は軍事品目とデュアルユース品目を保護することに焦点を当てていた。しかし、最終的な使用用途とエンドユーザーを軍または民に区別することは困難になってきており、それにより輸出管理は適用することが難しく、実際運用上効果がないものとなっている。

新興技術

日米間においては、新興技術への注目が高まり、これら新興技術の利用を規制するために協調して行動することの必要性が認識されているにもかかわらず、両者の間にはこれら技術に対する認識、影響力、技術レベルに差があるため協調行動が妨げられている。

「新興技術」の開発に内在する不確実性により、「新興技術」の利用を規制しその普及を管理することが不可能ではないにしても困難なものとなっている。また、管理されるべき技術の選定も困難であり、「網を広げすぎる」ことはイノベーションを阻害するという合意がある。

イノベーションを促進するための国際的な協力が望まれる一方、経済及び安全保障上の優位を維持するために技術へのアクセスを制御し、特に他国による転用及び他国への流出を防ぐ必要があるという認識があり、そこには難しい釣り合いが存在する。

米国においては技術流出を防ぐために、敵対国と目される国家との経済的交流を分断しようとする傾向がある一方で、そのような国家間関係を維持することは、米国とその同盟国が敵対国と目される国家の動向を把握し、経済的及び戦略的な不意打ちを防止することを可能にする。

新たな技術をできるだけ早く市場に出したいという経済的インセンティブは、安全、安全保障、及び倫理的観点を勘案する意思を低下させる可能性がある。さらに、新技術のコストが低下し、危険なツールへのアクセス可能性が高まったことが国家間に平準化効果をもたらしている。

サイバー空間

もしデータが「新たな石油」であるとするならば（これに関しては参加者からほとんど異論がなかった）、その利用や「所有権」に関する規制や規範は 21 世紀の経済的成功に不可欠なものとなるだろう。このようなデータ共有の促進または抑制を行う政府間の調整が不可欠である。

私たちはデータ処理に関して、用いられるアルゴリズムの種類が結果にどのような影響を与えるかを理解し始めたばかりだ。微妙ではあるが重要なバイアスが組み込まれていることにより、表面上は「中立的」なアルゴリズムであっても、意思決定に影響をもたらしうる。技術分野ではない政策担当者であっても、アルゴリズムという「ブラックボックス」に焦点を当て、どのような前提のもとに組まれているのかを理解しようとする必要がある。

COVID-19 のパンデミックはより良いサイバーセキュリティの実装への要求をさらに高め、技術的な能力とそれら実装に対する意思との間における深刻な差があることを明らかにした。同時に、パンデミックに端を発した不況により、各企業はサイバーセキュリティのための予算を削減する一方、リモートワークの急増に対応するため情報通信設備への支出を増加させている。

サイバー分野や技術分野での競争において誰が「勝っている」のか、という比較については注意を払わなければならない。多くは使用している指標や競争に関する前提に依拠しているからだ。また「競争」という比喩は国際的な協力の重要性を不明瞭にし、ゼロサム的な考え方に至ってしまう。

サイバー空間を陸、海、空、宇宙と同様に独立した軍事領域として認識し、考えることは関連する事項の意思決定を明確にすることにつながる。これは文民、軍、政府、民間を問わない。一方でこのような区別のあり方は他の領域にもサイバー空間が内在し深く浸透しているという事実を不明瞭にしてしまいかねない。

政府が国家レベルでのサイバーネットワークの安全性を確保しようとしている一方、中小企業はサイバー攻撃から身を守るのに苦労し続けている。彼らはサイバーセキュリティに関するリソースが不足しているためサイバー攻撃に対して脆弱であり、これらの中小企業がサイバーセキュリティを強化できるように支援するための取り組みが、政府と産業界の両方によって立ち上げられている。

サイバー空間に関する国家安全保障計画においては、強靭性と抑止のどちらを重視するかについて議論がなされている。技術が安全保障課題の焦点となることが多いが、人的要因も見落としてはならない。安全なサイバーネットワークを構築する上で、信頼が鍵となるコンセプトかもしれない。

ロボティクス

戦場におけるロボット又は自律型兵器の役割や、人間による制御や意図した行為の実行に対する影響については懸念があるが、自律型兵器は人間よりも識別能力や精度において優れており、戦闘による副次的な被害が少ないという議論もある。

最先端の科学技術を国家安全保障へ応用することに対する世間の懸念（または嫌悪感）により、一部の科学者（多くは日本人であるが、一部の米国人も）は自らの研究の軍事利用を考慮していない。

半導体、3D 造形技術、サプライチェーン

日本は 3D 造形技術に代表されるようなアディティブ・マニュファクチャリング技術（原料を積層・付加することによって成型する技術―訳者註）の導入において、

世界から数年後れをとっている。3D 造形技術には多くの利点があるが、一方で大規模な造形を行う際の原料調達において依然課題が残る。将来的に 3D 造形技術を有効に活用するためには、本技術に関する教育が必要となるだろう。

米国は、製造業の復活とサプライチェーンの再構築について、アジアから学ぶべきことが多い。

製造業における米国と中国のコスト差が 60～70%であることを踏まえると、コストのみに立脚した短期的な分析では、低コストの製造拠点を中国から移転させることはほとんど意味を成さない。むしろ、地政学的関係、政治的リスク、危機的状況におけるサプライチェーンの安全性など、競争的で時に強制力のある、考慮すべき長期的な要因がある。新たなサプライチェーンを確立する際には、これらの要因に細心の注意を払わなくてはならない。

米国においては、地球規模のパンデミックのような危機的状況において製造能力を確保するために州兵のような「国家製造部隊」を立ち上げるのも一つの手かもしれない。

量子技術

目を見張るべき進歩があったとはいえ、現時点において革新的と言えるような量子技術には未だ遠く及ばない。小型の量子コンピューティング技術は 3～5 年後に登場するかもしれないが、現行技術はその潜在的な応用可能性（と誇大評価）に達していない。

量子技術におけるどの分野が国家安全保障に影響を与えるのかを判断することは時期尚早であり、各国は各々異なる分野に注力している。日本、中国、EU は暗号化通信の安全性を向上させる可能性のある量子通信を優先している。米国と他の数カ国は、暗号化通信のセキュリティを脅かすと共に、有用な商業利用ももたらす可能性のある量子コンピューティングに注目している。

また、量子技術の広範な国際基準を設定することも時期尚早である。それよりも同盟国や同志国との間での限定的な協力に焦点を当てることの方が有効かもしれない。

バイオテクノロジー

バイオテクノロジーの拡散は新たな安全保障上の懸念を引き起こしており、悪意を持ったアクターがこれらの技術を利用できるようになる日も近い。

今日、バイオテクノロジーにおける焦点の大部分は医療・健康関連製品であるが、世界経済における物理的に取引されるものの内 60%以上がバイオ関連の製品に置き換わると推定されている。

バイオ関連の製品へのシフトはエネルギー、水、及び土地の利用の大幅な削減を生み出すと共に、「フードマイル」（生産から食卓までの距離）を短縮することができる。

新しい食品の生産方法においては、規模の経済がすべてではない。個人やスタートアップの競争力にも余地がある。しかし、供給能力が主要な制限要因となる。特にアミノ酸と水に関して顕著である。

日本はバイオテクノロジー分野の開発を進めてきたが、その成果は省庁間における派閥主義と縦割り行政により限定的なものとなっている。

協力できる分野

技術は政府全体、そして社会全体的なアプローチによってはじめて有効に管理することができる。政策立案者は技術の生み出す効果が最も広範囲に行き渡るように、同盟国や協力国及び同志国との協力を促進しなくてはならない。

民間企業の代表者を含む「インターネットエコノミーに関する日米政策協力対話」は日米協力における最良の事例である。

産官学の意見交換は、透明性やベンダーの多様性、標準化の価値を重視した開かれた産業構造を作り出し、日米のベンダーに市場機会を創出し、サプライチェーンの安全性を向上させることで第三国に利益をもたらす。

5G 競争において米国と日本が直面している根本的な課題は、中国が第三国に提供している非常に安価な技術に代わるような魅力的な選択肢がないことである。5G において日米が焦点とすべきは、技術課題に対するマルチベンダーの相互運用性を確保するための共同研究開発である。日米はまた、6G 技術の開発、特に規格設定のための産業界での多者間及び二者間のコンソーシアムについて考えるべきである。

1980 年代の日米貿易及び技術競争からの重要な教訓の一つは、米国が有力な競争相手からの「脅威」を誇張しすぎて、協力して相互に利益を得るチャンスをほとんど見逃してしまったことである。（米国の同盟国は中国との協力という観点を見失うべきではない。）

米国は、産業開発における政府の関与について正しく理解しなくてはならない。「起業家の自助自立」という神話を維持し、史実に基づかないイデオロギー的な立場が推し進める為に、シリコンバレーの誕生において米国連邦政府が果たした重要な役割はしばしば過小評価されている。

貿易、投資、技術管理に関して日米間の調整が必要である。そうでなければ、共通の安全保障上の懸念に対処しようとする試みは、両国間の摩擦を生むことになる。日本ができる重要なステップの一つは、セキュリティ・クリアランス制度を含めた、機密情報を扱うためのより洗練された体制を構築することである。その第一歩として、日米両国は１９８８年に署名した科学技術協定を更新すべきである。

より詳しい情報についてはクリスタル・プライアー（crystal@pacforum.org）またはブラッド・グロッサーマン（brad@pacforum.org）に連絡してください。本書に記載された意見は各カンファレンスのオーガナイザーによるものであり、必ずしも全参加の意見を反映させたものではありません。

ECONOMIC SECURITY AND JAPANESE ECONOMIC STATECRAFT

By Akira Igata

The rise of "economic security" discourse in Japan

"Economic security" has become a hot topic in Japanese media, especially in the last year or so. There are a couple of reasons why this term, loosely used to describe almost every issue where economic and security issues overlap, has been the focus of attention in Japan.

China factors

Much of this relates to China. There are four strategic trends worth noting. First, there is a growing perception of China's rise and the relative decline of US power in international politics, which has led to an increase in the Chinese presence in Japanese discourse. Second, China has increasingly employed "economic statecraft," or the use of economic means to pursue geopolitical or security interests.[1] Democratic countries including the United States and Japan have been creating policies to deal with new challenges posed by China's economic statecraft. Third, Xi Jinping has raised the Military-Civil Fusion concept to the strategic level, raising concern that any technological cooperation with China may result in contributions to the modernization of the People's Liberation Army. Fourth is China's increasingly inward-focused economic policies, evident in measures such as "Made in China 2025," a policy that aims to create domestic champions in numerous critical industries, a government procurement list that prioritizes domestic information technology products, and the "dual circulation strategy," which calls for China to shift from its export-oriented economic strategy to one that focuses on the domestic market.

Three important Chinese domestic legal developments have contributed to the rise of economic security discourse in Japan. One is the establishment of the National Intelligence

[1] Numerous works detail Chinese economic statecraft, among them Robert D. Blackwill and Jennifer M. Harris. *War by Other Means: Geoeconomics and Statecraft*, The Belknap Press of Harvard University Press (2016) and William J. Norris. *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*, Cornell University Press, (2016).

Law, which stipulates that every Chinese company or individual shall cooperate with state intelligence gathering. The second is the Cyber Security Law, which prioritizes the Chinese government's access to data over protection of privacy. The third is the new Export Control Law, which identifies re-exports and deemed exports in ways that will be problematic for foreign companies in China that use emerging technologies. These newly enacted laws – especially the Export Control Law - are perceived as having transformed in a negative way the environment in which companies operate in China.

Media coverage of human rights violations in China has contributed to the rethinking of how to deal with China, especially in the private sector. Reports of forced labor in Xinjiang,[2] Tibet,[3] and elsewhere,[4] as well as population control of Uyghurs in Xinjiang[5] have led to heightened media scrutiny of global supply chains. As a result, numerous Japanese companies have been "named and shamed" for indirectly violating human rights by potentially using forced labor in their supply chains[6] or providing components to video surveillance companies that have been blacklisted by the US for human rights violations.[7]

Technological factors

In addition to these strategic, legal, and human rights concerns, economic security has become a focus because the nature of technology has changed. Previously, a limited number of technologies had both military and civil uses, were identified as "dual-use" and thus subject to control. Today, virtually all emerging technologies have some potential military use. Automated driving systems can be used for unmanned military aerial drones; biological weapons can be created through DIY biology; 3D printers can be used to fabricate weapons. These developments render the concept of "dual use" obsolete, as all emerging technologies are

[2] Bureau of International Labor Affairs, US Department of Labor. *Against their Will: The Situation in Xinjiang*. Accessed on Nov. 26, 2020.
https://www.dol.gov/agencies/Ilan/against-their-will-the-situation-in-xinjiang
[3] Adrian Zenz. "Xinjiang's Militarized Vocational Training System Comes to Tibet." *Jamestown Foundation China Brief*. Volume: 20 Issue: 17.
[4] Vicky Xiuzhong Xu, Danielle Cave, Dr Games Leibold, Kelsey Munro & Nathan Ruse. "Uyghurs for sale," *Australian Strategic Policy Institute*. March 1, 2020.
[5] Adrian Zenz. *Sterlizations, IUDs, and Mandatory Birth Control: The CCP's Campaign to Suppress Uyghur Birthrates in Xinjiang*. Jamestown Foundation. July 21, 2020.
[6] For instance, see: "Uyghurs for sale"; Erin Handley and Bang Xiao. "Japanese brand Muji and Uniqlo flaunt 'Xinjiang Cotton' despite Uyghur human rights concerns." *ABC News*, Nov. 4, 2019.
[7] "Sony, Sharp supply parts to U.S.-blacklisted China security video firm." *Kyodo News*. Nov. 25, 2019.

potentially "dual use." As a result, the economic activities of companies that once had nothing to do with the military have become highly relevant to security.

Japan's defensive economic statecraft

The critical question for Japan is how to think about economic statecraft in an era of heightened competition between the US and China. Japan has been pursuing various defensive policies for a year or so.

First, the Japanese government has strengthened its organizational structure for economic security. It created an Economic Division in the National Security Secretariat to deal with technology and security along with other economic security issues. The Ministry of Foreign Affairs created an Economic Security Policy Division; the Ministry of Economy, Trade, and Industry (METI) created the Economic Security Division; and the Ministry of Defense announced that it will create an economic security position to deal with emerging technologies. The Japanese government is also planning to create a comprehensive promotion law on economic security, which will include such items as strengthening economic intelligence gathering capacity, promoting cooperation with "Five Eyes" countries, and creating new restrictions on foreign land acquisition adjacent to sensitive areas.[8]

Second, Japan is implementing policies on technological innovation based on its Integrated Innovation Strategy[9]. This strategy has four pillars: (1) "Knowing" which technologies pose threats and what technologies exist to counter these threats; (2) "developing" these technologies; (3) "protecting" the intellectual property; and (4) "applying" the technologies in society.

The Japanese government is considering the creation of a "Japanese version of the RAND corporation" which will make the connection between emerging technologies and security and make it easier to "know" what an innovative technology is and how to "apply" it. This think

[8] "Dejitaru Tsuuka he Hou Kaisei Jyunbi wo: Jimin, Chuukan Torimatome [Prepare for legal amendment to create digital currency: Mid-term report by the Liberal Democratic Party]." *Nihon Keizai Shimbun*. October 5, 2020.

[9] For the most recent strategy, see: Japanese Cabinet. *Tougou Inobe-shon Senryaku 2020 [Integrated Innovation Strategy 2020]*. July 17, 2020.

tank will lead research into the state of R&D in industry, academia, and the government then make recommendations on how these technologies can be utilized for security purposes in areas such as quantum computing and artificial intelligence (AI).[10]

Japan has R&D subsidies for emerging technologies for FY2021 to "develop" these technologies. METI has requested nearly 100 billion yen for "creating an innovation ecosystem" that includes R&D promotion for AI, materials, and sensors.[11] The Ministry of Internal Affairs and Communications has asked for 73 billion yen for strategic investment in emerging technologies such as 5G, "Beyond 5G," quantum cryptography, AI, and space-related information and communications technologies (ICT).[12]

To "protect" technology, Japan must block four main routes of illicit technological transfer: people, products, money, and cyber attacks. On the "people" front, the Japanese government recently changed the rules for government research grants by mandating that those receiving monies disclose funding sources from foreign entities,[13] with potential next steps including the strengthening of visa controls to prevent illicit technological transfers through researchers.[14] On "products" and "money," the Foreign Exchange and Foreign Trade Act was revised to strengthen export control and investment screening. On "cyber," Japan has been strengthening cyber security for both the government and private sector.

Protection of technology is sought through international coordination as well. Japan is reportedly considering a call for a new international export control regime. While it will not

[10] "Seifu, Anpo de Shin Shinku Tanku: Minkan Gijyutsu wo Kenkyu [The government is considering a new thinktank in the area of security: Will research civil technology transfer]." *Nihon Keizai Shimbun*. January 19, 2020.
[11] Ministry of Economy, Trade and Industry. *Reiwa 3 Nendo Keizai Sangyoushou Kankei Gaisan Youkyuu no Pointo [Important points from METI-related budgetary request for the 3rd year of Reiwa]*. September 30, 2020.
[12] Ministry of Internal Affairs and Communications. *Reiwa 3 Nendo Soumushou Shokan Yosan Gaisan Youkyuu no Gaiyou [Overview of the budgetary request under Ministry of Internal Affairs and Communication's Jurisdiction for the 3rd year of Reiwa]*. September 30, 2020.
[13] "Sentan Gijyutsu no Kaigai Ryuusyutsu Boushi: Seifu Hojyo, Shikingen no Kaiji Jyouken [Preventing foreign leaks of emerging technology: Government funding will require disclosure of funding]." *Nihon Keizai Shimbun*. June 23, 2020.
[14] Dokuji - Ryuugakusei Biza no Shinsa Genkakuka e: Chuugoku Nentou, Anpo Gijyutsu wo Ryuusyutsu Boushi [Exclusive – Tightening visa for foreign students: With China in mind, preventing leak of security-related technologies]." *Yomiuri Shimbun*. October 5, 2020.

replace the Wassenaar Arrangement, the idea is to create a more agile group to control exports of emerging technologies such as AI, machine learning, quantum computing, biotechnology, and hypersonic among countries that have these capacities, such as Japan, the US, Germany, UK, and the Netherlands.[15]

Third, the private sector is waking up to this new geopolitical reality and is strengthening its capacity to collect and analyze economic security concerns that will affect them and shift its global management strategies accordingly. Most notable is Mitsubishi Electric, which in September 2020 created a new Corporate Economic Security Division to "comprehensively manage economic security risks throughout the entire company's business" and is tasked with "researching and analyzing the rapidly changing economic security policies and legal systems of countries worldwide."[16] This trend will likely spread to other companies and industries.

Japan-U.S. cooperation in economic security

Japan must continue developing its capacity to deal with new economic security challenges, while increasing cooperation with like-minded countries. This could take many forms. Since countries (including Japan) have only begun to establish economic security policies, this process would benefit from prioritizing bilateral discussions focused on economic security with countries that have emerging technologies before moving to a multilateral forum. A Japan-US economic security dialogue that included the government and private sector would greatly benefit future coordination between the two countries on this critical issue.

[15] "Sentan Gijyutsu no Yusyutsu Kisei, Bei nado ni Wakugumi Teian e Seifu Kentou [The government is considering calling for a framework on emerging technology export controls to countries like the U.S.]" *Nihon Keizai Shimbun*. September 26, 2020.
[16] Mitsubishi Electric Corporation Public Relations Division. *Mitsubishi Electric to Change Executive Officer's Duties and Organization*. September 16, 2020.

経済安全保障と日本のエコノミック・ステイトクラフト

井形　彬

日本における「経済安全保障」の台頭

ここ数年、「経済安全保障」が日本のメディアで取り上げられることが多くなってきた。経済及び安全保障分野が重なり合うほぼ全ての課題を表すものとして緩く用いられているこの用語が日本において注目され始めたのにはいくつかの理由がある。

中国要因

経済安全保障が台頭した背景の大部分は中国要因だ。まずは、中国に関する四つの重要な戦略的傾向が挙げられる。第一に、国際政治分野における中国の台頭と米国の相対的パワーの低下という認識が浸透し、日本国内の議論の中で中国の存在感が増していること。第二に、中国が「エコノミック・ステイトクラフト」、つまり地政学及び安全保障上の国益を追求するための経済的手段を用いるようになってきていること[1]。この中国のエコノミック・ステイトクラフトにより引き起こされている課題に対応するために、米国や日本を含む民主主義国家は新たな政策を策定してきている。第三に、習近平が「軍民融合」という概念を戦略レベルへと引き上げたことで、中国と技術協力を行うことが人民解放軍の近代化に寄与

[1] 中国によるエコノミック・ステイトクラフトについての著作は多数ある。Robert D. Blackwill and Jennifer M. Harris. *War by Other Means: Geoeconomics and Statecraft*, The Belknap Press of Harvard University Press (2016) and William J. Norris. *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*, Cornell University Press, (2016).

してしまうことに繋がるのではないかと、いう懸念が高まっていること。第四に、中国の経済政策の内向き傾向が強くなってきていること。この傾向は、多くの重要分野において国内産業を確立することを目指した「中国製造 2025」、国内の情報技術製品を優先する政府の調達リストである「安可目録」、輸出中心の経済戦略から国内市場中心の経済戦略への転換を求める「双循環戦略」等に明確に表れている。

ここ数年に中国で制定された三つの重要な国内法も日本の経済安全保障関連議論を加速させている。第一に、全ての中国企業及び中国人が国家の情報収集に協力することを定めた「国家情報法」の制定。第二に、中国政府によるデータへのアクセスが個人のプライバシー保護より優先されることを定めた「サイバーセキュリティー法」。第三に、中国において新興技術を使用する外資系企業にとって障害となる再輸出規制やみなし輸出制度を定めた「輸出管理法」。これらの新しく制定された法律（特に輸出管理法）は中国でビジネスを行う企業を取り巻く環境を悪化させているという認識が広まる理由となっている。

さらに、中国の人権侵害に関する度重なるメディア報道が、今後の中国との関わり合い方について、民間セクターにまでも再検討を促している。ウイグル[2]、チベ

[2] Bureau of International Labor Affairs, US Department of Labor. *Against their Will: The Situation in Xinjiang*. Accessed on Nov. 26, 2020.
https://www.dol.gov/agencies/Ilan/against-their-will-the-situation-in-xinjiang

ット[3]等における強制労働[4]や新疆でのウイグル人の人口抑制策に関する報道を受け[5]、グローバル・サプライチェーンへのメディアの詮索が強まっている。その結果、多くの日本企業もサプライチェーンにおいて強制労働をさせられている人々を利用している[6]、あるいは、人権上の理由から米国がブラックリストに登録している監視機器会社に対して部品を供給していることで人権侵害に間接的に関与している可能性がある、などと名指しで批判されている[7]。

技術要因

こうした戦略、法、そして人権といった中国に関する懸念に加え、技術自体の性質が変わってきたことも経済安全保障が注目されるようになった理由として挙げられる。以前は、軍事用にも民生用にも利用でき規制対象とされていたいわゆる「軍民両用技術」の数は限定的であった。しかし今日では、ほぼ全ての先端技術が軍事転用可能なものである。自動運転システムは軍用無人航空機に利用することができる。生物兵器は DIY バイオの一貫で製造することができる。3D プリンターは武器生産に利用可能である。全ての新興技術が潜在的に「軍民両用」であるため、「軍民両用」という概念自体が時代遅れのものとなっているとまでも言えるかもしれない。この結果、軍事とは無関係であると思われていた企業の経済

[3] Adrian Zenz. "Xinjiang's Militarized Vocational Training System Comes to Tibet." *Jamestown Foundation China Brief*. Volume: 20 Issue: 17.
[4] Vicky Xiuzhong Xu, Danielle Cave, Dr Games Leibold, Kelsey Munro & Nathan Ruse. "Uyghurs for sale," *Australian Strategic Policy Institute*. March 1, 2020.
[5] Adrian Zenz. *Sterlizations, IUDs, and Mandatory Birth Control: The CCP's Campaign to Suppress Uyghur Birthrates in Xinjiang*. Jamestown Foundation. July 21, 2020.
[6] For instance, see: "Uyghurs for sale"; Erin Handley and Bang Xiao. "Japanese brand Muji and Uniqlo flaunt 'Xinjiang Cotton' despite Uyghur human rights concerns." *ABC News*, Nov. 4, 2019.
[7] "Sony, Sharp supply parts to U.S.-blacklisted China security video firm." *Kyodo News*. Nov. 25, 2019.

活動が安全保障と非常に密接に関係するものとなってきている。

日本のエコノミック・ステイトクラフト

米中競争が激しさを増す中で、エコノミック・ステイトクラフトをどう考えるべきかが日本にとって重要な課題である。日本はここ数年、様々な防御的政策の立案に取り組んでいる。

第一に、政府は経済安全保障のための組織体制を強化してきた。例えば、国家安全保障局に技術、安全保障及び経済安全保障全般を担当する経済班が新設された。外務省では経済安全保障政策室を、経産省は経済安全保障室を設置したほか、防衛省も新興技術を扱う経済安全保障情報企画官を新たに設けることを発表した。また、「経済安全保障一括推進法案」という経済安全保障に関する包括的な法案制定や、経済関連情報収集能力の向上、「ファイブアイズ」諸国との協力強化、外国資本による安全保障上機微な土地の買収に関わる新たな規制等に向けた動きが現在動き始めている[8]。

第二に、日本は「統合イノベーション戦略」に基づき、技術革新のための政策を進めている[9]。この戦略は、（1）どの技術が脅威をもたらし、それら脅威に対抗するための技術としてはどのようなものがあるのか「知る」こと（2）こうした技術を「育てる」こと（3）知的財産を「守る」こと（4）その技術を社会に

[8] 「デジタル通貨へ法改正準備を　自民が中間とりまとめ」日本経済新聞　2020年10月5日
[9] 最新の戦略については、内閣府「統合イノベーション戦略2020」2020年7月17日

「生かす」こと、という四つの柱から構成されている。

「知る」と「生かす」に関しては、日本政府は現在「日本版 RAND」の創設を検討している。この日本版RANDの設立は、新興技術と安全保障分野の関連性を示し、何が革新的技術か、そしてそれをどのように活用すべきかについて把握することを容易にするだろう。このシンクタンクは、産・官・学の研究開発状況を調査し、量子コンピューターや人工知能（AI）等の分野における安全保障目的のためにこれらの技術がどのように利用可能かについて提言することとなるだろう[10]。

日本はこれらの技術を「育てる」ために、2021年度予算に新興技術のための研究開発の補助金が計上されている。経産省は、AIやマテリアル、センサーなどの研究開発推進を含めた「イノベーション・エコシステムの構築」に 1000 億円近くを要求している[11]。総務省は 5G や「Beyond 5G」、量子暗号、AI、宇宙関連の情報通信技術（ICT）などの新興技術への戦略的投資に730億円を要求した[12]。

技術を「守る」ために日本は、ヒト、モノ、カネ、サイバー攻撃という四つの不当な技術移転経路を遮断しなければならない。「ヒト」の面では、日本政府は公的研究費に関する規則を改正し、支援を受けるものに対し海外からの資金源に関する情報の開示を義務付けた[13]。次の段階として、研究者を通じた不正な技術移

[10] 「政府、安保で新シンクタンク　民間技術転用を研究」日本経済新聞　2020年1月19日
[11] 経済産業省「令和3年度 経済産業省関係 概算要求のポイント」2020年9月30日
[12] 総務省「令和3年度総務省所管予算概算要求の概要」2020年9月30日
[13] 「先端技術の海外流出防止　政府補助、資金源の開示条件」日本経済新聞　2020年6月23日

転を防ぐために入国管理を強化する可能性もある[14]。「モノ」と「カネ」の面では、輸出管理及び投資管理を強化するために外為法が改正された。「サイバー」の面では、日本は官民双方のサイバーセキュリティを強化している。

日本は国際協力を通じた先端技術保護も模索している。具体的には、日本は新たな国際的輸出管理のレジーム形成を推進することを検討しているという。これはワッセナー・アレンジメントに代わるものではないが、AI、機械学習、量子コンピューター、バイオテクノロジー、超音速などの新興技術の輸出を、日本、米国、ドイツ、英国、オランダ等、これらの技術を有する国家間で管理するために、より迅速な枠組みを構築しようとする試みである[15]。

第三に、民間セクターもこの新しい地政学的現実を直視しつつあり、彼らに影響を与えるであろう経済安全保障上の懸念に関する情報を収集及び分析し、それをグローバルな経営戦略の実行に反映させる能力を強化している。最も顕著な例としては、三菱電機が 2020 年 9 月に会社全体のビジネス上の「経済安全保障の観点から見たリスク制御を統合的に行う」ために経済安全保障統括室を新設した。この経済安全保障統括室は「各国の経済安全保障政策の急激な変化に対応して、政策動向や法制度を調査・分析」することを任務としている[16]。この傾向は他の企業及び産業にも広がりを見せるだろう。

---

[14] 「【独自】留学生ビザの審査厳格化へ…中国念頭、安保技術を流出防止」読売新聞 2020 年 10 月 5 日

[15] 「先端技術の輸出規制、米などに枠組み提案へ　政府検討」日本経済新聞　2020 年 9 月 26 日

[16] Mitsubishi Electric Corporation Public Relations Division. *Mitsubishi Electric to Change Executive Officer's Duties and Organization*. September 16, 2020.

経済安全保障における日米協力

日本は、有志国との協力関係を深めながら、新たな経済安全保障上の問題に対処する能力を強化し続けなければならない。これには様々な方策が考えられる。日本を含め各国は経済安全保障政策を立案し始めたばかりであるため、多国間フォーラムを志向する前に、これらの取り組みにおいて新興技術を有する国々と共に経済安全保障に焦点を当てた二国間協議を優先させることが有益となるだろう。官民合同の日米経済安全保障対話は、この重要な問題に関する今後の日米間の調整に大きな利益をもたらすだろう。

ECONOMIC SECURITY CHALLENGES AND EMERGING TECHNOLOGICAL OPPORTUNITIES IN THE US-JAPAN ALLIANCE

By Elsa B. Kania

The boundaries between economic and national security have been eroding. In particular, the intense disruption of the COVID-19 pandemic has highlighted the degree to which security depends on national resilience and the fundamentals of a country's economic foundations, including the capacity to secure critical resources and scale up production at a moment of crisis. In particular, the future trajectory of US-China rivalry will depend upon capacity to promote economic recovery and sustain development. For the United States and Japan as democracies, the relative openness of our innovation ecosystems can provide an important competitive advantage, especially in a world of globalized innovation. However, this openness can also be exploited and create vulnerability to the tactics of tech transfer that the Chinese government has often undertaken. As economic security comes to the forefront of the conversation, both governments have explored policy options to mitigate those risks. For the US-Japan alliance, these are critical challenges on which coordination and engagement will be critical.

Economic Security at the Forefront

US concern for economic security as a dimension of national security has intensified under the Trump administration. While economic security has long been a concern for US policymakers, its elevation as a core and central concern for US national security has become particularly prominent during the Trump administration. The 2015 *National Security Strategy* emphasized, "America's growing economic strength is the foundation of our national security." By contrast, the latest *National Security Strategy* directly declared, "Economic security is national security."[1] The policies and practices by China that are damaging US economic interests, such as those that undermine fair competition or pilfer intellectual property, are regarded as "economic aggression" to require a forceful response. US policy is to promote "free, fair, and reciprocal"

[1] "National Security Strategy of the United States of America," https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

relationships, such as those marked by equal levels of market access. While the next iterations of this strategy remain to be seen, there will likely be a degree of continuity in these concerns into and across future administrations.

However, there is not a single concept or coherent understanding of economic security in US policy in practice. Interestingly, the recent concern with economic security in US policy debates presents a useful comparison to parallel concepts in China. Within the "overall national security concept" that Xi Jinping has promoted, economic security is regarded as "the foundation."[2] PRC Science and Technology (S&T) plans have also concentrated on promoting indigenous innovation, including to overcome chokepoints or bottlenecks, such as semiconductors, where China remains dependent upon foreign technologies and has not yet developed an indigenous alternative. On the other hand, debates about economic security could be situated instead in relation to concerns about human security. In particular, the COVID-19 crisis highlights the importance of resilience and societal well-being as essential prerequisites of US strength. By most metrics, the United States has yet to dedicate adequate attention or resources to any of these issues.

These concerns about economic security have often been invoked in US policy debates in response to threats from and competitiveness relative to China. Certainly, the theft of intellectual property, as well as transfer of technology through licit means, at scale has imposed serious damage on US companies, and the aggregate impacts on the US economy have been severe. As described in the *National Security Strategy*, the United States must focus on domestic production of essential products and critical technology. In particular, there is renewed concern with protection of the "national security innovation base," a concept that encompasses not only the defense industry and traditional stakeholders in US national security, such as national laboratories, but also academia and the private sector. However, even as the US government starts to regard new players as critical to the national security innovation base, such as for their strengths in emerging technologies, these entities do not view their interests as aligned necessarily with those of the US government, nor are views on security the same across sectors.

[2] "Xi Jinping talks about the overall national security concept: people's security is the purpose of national security" [习近平谈总体国家安全金句：人民安全是国家安全的宗旨], *People's Daily Online* [人民网], April 15, 2019, http://cpc.people.com.cn/xuexi/n1/2019/0415/c385474-31030462.html

As debates continue about the prospects of "decoupling" from China, an underlying consideration is not simply the reduction of risk but also the rebuilding of industries that had been hollowed out. After decades in which much of that capacity for indigenous development had been lost within the United States because of globalization, the latest attempts to reverse that trend will be challenging and likely require significant investments to achieve. For the United States, assured supplies of critical resources, such as rare earths, and reorienting important industries, such as pharmaceuticals, are priorities that will only redouble in the wake of the pandemic, which demonstrated the dangers of failing to secure a reliable supply or being dependent upon another country for any vital resource. Whereas once economic interdependence was regarded primarily as a stabilizing influence in US-China relations, that dynamic is viewed today on both sides as creating a degree of mutual vulnerability that is dangerous as rivalry intensifies.

The measures intended to change the status quo ante between the US and Chinese economies have been pursued in parallel between both governments. Considering that the Chinese government has long blocked US companies from sensitive industries or critical infrastructure, including the expulsion of Google from China as early as 2010, for the US to respond reciprocally, recognizing similar concerns, appears reasonable, if not long overdue. The latest initiatives in China policy from Congress have introduced more restrictions. For instance, the reforms to the Committee on Foreign Investment in the United States (CFIUS) through the Foreign Investment Risk Review Modernization Act (FIRRMA) have expanded scope of purview and mandate, including to consider different types of investment and issues that encompass personal information. In particular, CFIUS has recently blocked Chinese companies from investments that might provide access to the personal information of US citizens.

Beyond the bombastic rhetoric from the Trump administration, several of the measures introduced have been relatively reasonable, despite messaging and implementation that have at times been lacking or confusing or haphazard. However, the failure to articulate a coherent rationale or create a generalized framework for these policies has meant that various actions taken to constrain the unwanted transfer of technology have at times appeared randomly targeted against Chinese companies in ways that have raised concerns about undue political

influence. For instance, the use of the "entity list" that the Department of Commerce maintains to impose restrictions on certain Chinese companies, such as to deny their access to chips, has occurred with greater frequency, including against companies alleged to be linked to the Chinese military or complicit in human rights abuses. Moreover, new rules from the Bureau of Industry and Security (BIS) have expanded understanding of "end user" and "military end user" for the purposes of transfer and licensing. In parallel, there has been increased screening and in some cases denial of visas to students linked to tech transfer and military-civil fusion, a policy that is reasonable yet raised concerns about fairness in approvals.

Emerging Industries and the Fourth Industrial Revolution

While the United States was once regarded as a leader and essentially unchallenged in innovation, China's rise as a powerhouse in science and technology has raised concerns about the competitive challenge. In particular, the US and Chinese governments have concentrated on artificial intelligence (AI), advanced manufacturing, quantum information science (AIS), and fifth-generation telecommunications (5G), which were deemed during the Trump administration as "industries of the future." In parallel, Chinese leaders concentrated on promoting the digital economy and the development of new-type infrastructure. At a moment of global economic slowdown in the aftermath of the pandemic outbreak, and as the fourth industrial revolution that is emerging as a result of these advances in disruptive technologies progresses, the capacity to achieve competitive advantage in these industries will be consequential.

Beyond defensive measures intended to block technology transfer, policymakers are starting to explore options to enhance US competitiveness. In particular, after years of shortfalls in funding for basic research, there are calls for greater government investment in promoting research and development in priority directions. At the same time, the US has had an aversion to measures that might be regarded as industrial policy, and in industries that are evolving so quickly there are reasons to consider carefully not only the benefits but also possible detriments to more directed governmental involvement. Efforts by governments to direct funding to fill gaps or address market failures, including in industries that are consequential but remain immature or relate to urgent concerns of national security, can be productively supported.

Economic Security in an Age of Pandemics

The United States and Japan must recalibrate and reevaluate their understandings of economic security in response to lessons learned from the pandemic and recognition of looming systemic threats. The global economy is facing severe economic consequences as the result of a pandemic for which preparedness proved inadequate. In its wake, efforts to promote resilience are especially consequential, as future pandemics and the threat of climate change, which will contribute to extreme weather and forced migration, will present urgent concerns for every country. Such systemic threats, especially climate change, necessitate a more global approach, including re-engagement with international institutions by the United States. The United States and Japan should continue to engage on concerns of economic security, sharing lessons learned, and explore options for joint action.

日米同盟における経済安全保障課題と先端技術の可能性

エルサ・B・カニア

経済安全保障と国家安全保障との境界は曖昧となってきている。特に昨今コロナウイルスがもたらした混乱は、国家の強靭性、そして危機における重要資源の確保や生産の拡大といった能力を含む国家の経済基盤に安全保障が依存していることを浮き彫りにした。特に今後の米中競争の展開は、景気回復や発展の持続といった能力に左右される。民主主義国家である米国及び日本にとり、イノベーションのエコシステムが比較的開かれていることは、特にグローバル化されたイノベーションの世界において重要な競争優位性をもたらす。しかし一方で、このエコシステムの開放性は悪用され、中国政府によってしばしば用いられる技術移転の手法に対する脆弱性を生じさせうる。経済安全保障が主要な議題となる中で、両国政府はそうしたリスクを軽減する政策を模索してきた。日米同盟にとり、これらは調整及び対応が必須となる重要な課題となるであろう。

経済安全保障の最前線

安全保障問題としての経済安全保障に対する米国の懸念はトランプ政権下で高まった。経済安全保障は長らく米国にとって懸念事項の一つであったが、それが米国の国家安全保障にとって中心的且つ重要な懸念事項であるとされるようになったのはトランプ政権下であった。2015 年の国家安全保障戦略は、「米国の経済成長力は国家安全保障の基盤である」としていた[1]。その一方で最新の国家安全保障戦略では「経済安全保障は国家安全保障そのものである」と明記された。公正競争の弱体化又は知的財産の窃盗といった米国の経済的利益を損なう中国の政策や手法は、強硬な措置を必要とする「経済侵略」とみなされている。米国の政策は、市場への平等なアクセス等といった「自由で、公正で、互恵的な」関係を促進す

[1] “National Security Strategy of the United States of America,” https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

るものである。この戦略の今後の在り方は不明瞭であるが、将来の政権においてもこれらの懸念事項は一定程度引き継がれるであろう。

しかし、実際の米国の政策には、経済安全保障に関する単一の概念や一貫した認識は存在しない。興味深いことに、近年の米国の政策議論における経済安全保障関連の懸念は、中国における懸念と類似性を有している。習近平が推し進める「総体国家安全観」の中で、経済安全保障は「基盤」とみなされている[2]。また、中国共産党政府の科学技術（S&T）計画は、中国が外国の技術に依存しており、自国で代替技術を開発できていない半導体などといった難点やボトルネックを解消することを含め、国内の技術革新を促進することに注力してきた。一方で経済安全保障の議論は、人間の安全保障に関する懸念との関連で議論することもできる。特にコロナ禍は、米国の国力に不可欠である強靭性と社会福祉の重要性を浮き彫りにした。しかし何れにおいても、米国はこうした課題に十分な注意を払ってきておらず、また十分な資源も充ててこなかった。

中国の脅威や競争力に対応するため、こうした経済安全保障に関する懸念は米国の政策論争の中でもしばしば議題として上った。確かに知的財産の窃盗や合法な手段での技術移転等は米国企業に深刻な被害を与え、米国経済への影響も計り知れないものとなってきている。国家安全保障戦略にも述べられているように、米国は重要製品や基幹技術の国産化に注力しなければならない。特に、防衛産業や国立研究所といった米国国家安全保障分野における従来の利害関係者だけでなく、アカデミアや民間セクターも含めた「国家安全保障革新基盤」の保護に関する懸念が再度高まっている。米国政府は、新興技術分野において強みを持つ新たな主体の重要性を認識し始めている一方で、これらの主体は自らの利益と米国政府の

[2] “Xi Jinping talks about the overall national security concept: people's security is the purpose of national security” [习近平谈总体国家安全金句：人民安全是国家安全的宗旨], *People’s Daily Online* [人民网], April 15, 2019, http://cpc.people.com.cn/xuexi/n1/2019/0415/c385474-31030462.html

利益が必ずしも一致しているとは考えておらず、また安全保障に関する考え方も部門によって異なっている。

中国との「分断」に関する議論が続く中で、根底にある問題は単なるリスクの軽減だけでなく、空洞化していた産業の再構築である。グローバル化の影響によりここ数十年米国は国内産業を発展させる能力を失っている。近年のこうした傾向を一変させる試みは困難であり、巨額の投資が必要となるだろう。米国にとり、レアアース等の重要資源の供給確保や医薬品などの重要産業における方針転換は優先事項であり、確実な供給を確保出来ないことや重要な資源を他国に依存することの危険性を示したコロナ禍により、その重要性がさらに明らかとなった。経済的相互依存関係は米中関係の安定化をもたらすものと考えられていたが、競争が激化するにつれてそうした関係は米中に危険な相互脆弱性をもたらしているとされている。

従来の米中経済関係を変えるための施作は両政府間でそれぞれ追求されてきた。2010 年には早くもグーグルが中国から締め出されるなど、中国政府が機微産業や重要なインフラから米国企業を長い間締め出してきたことを勘案すると、米国が同様の懸念を認識してようやくそれらに呼応した対応するようになったことは、合理的に見える。米国議会における対中政策の昨今の取り組みでは、さらなる制限措置を導入している。例えば、外国投資リスク審査現代化法（FIRRMA）を通じた対米外国投資委員会（CFIUS）の改革では、様々な投資の種類や個人情報を含む課題を検討するなど、その対象と権限の範囲を拡大した。特に、近年 CFIUS は米国市民の個人情報の入手を可能にしうる中国企業の投資を拒否している。

トランプ政権の大袈裟な主張は別にして、導入された措置のいくつかは、その広報や実施が不十分で、混乱しており、拙劣であったにせよ、ある程度合理的なものであった。しかしながらこれらの政策のための一貫した理論的根拠を示すことや、包括的な枠組みを構築することができなかったため、好ましくない技術移転を制限するための様々な施作が無差別に中国企業を標的としたものとなり、過度

な政治的介入ではないかと疑問視された。例えば、特定の中国企業に対し、チップの入手を拒否する等の規制を課すために商務省が管理している「エンティティ・リスト」は、人民解放軍との関係や人権侵害に加担しているとされる企業を対象とするものも含めて、頻繁に用いられている。さらに、商務省産業安全保障局は、技術移転及び供与において「エンドユーザー」や「軍事エンドユーザー」の定義を拡大させてきた。同時に、技術移転や軍民融合に関わっている学生へのスクリーニング、場合によってはビザの発給拒否が増加した。この方針は合理的でありながらも承認の公平性についての懸念を招いた。

新興産業と第四次産業革命

米国はかつて他の追随を許さないイノベーションにおける先駆者とみなされていたが、中国が科学技術大国として台頭してきたことで、中国との競争が懸念されている。特に、トランプ政権時代に「未来産業」とされていた人工知能（AI）、先端製造業、量子情報科学（AIS）、第 5 世代通信（5G）等に米国及び中国政府は注力してきた。同時に中国指導部はデジタル経済の推進と新型インフラの整備にも注力した。昨今のパンデミックを受け、世界的に景気は後退し、革新的技術における発展の結果による第四次産業革命が進展するにつれて、これらの産業における競争優位性を獲得する能力は肝要なものとなるだろう。

技術移転を阻止することを目的とした防御的な措置のみならず、政策立案者は米国の競争力強化のための対応策も模索し始めている。特に、基礎研究の資金不足が長年続いていることから、優先分野の研究開発を推進する為の政府投資の拡大が求められている。一方で、米国は産業政策とみなされるような施策を避けてきたこともあり、急速に発展する産業においては、政府のより直接的な関与のメリットのみならず、デメリットも十分に考慮する必要がある。このような資金不足解消の為の資金提供、市場の失敗への対処といった政府による取り組みは、重要ではあるが発展が遅れている産業や、国家安全保障上緊急の懸念がある産業等を効果的に支援することができる。

パンデミック時代における経済安全保障

パンデミックから学んだ教訓と、迫り来る構造的な脅威を受けて、米国と日本は経済安全保障に関する認識を見直し、再評価しなければならない。その備えが不十分であった昨今のパンデミックの結果として、世界経済は厳しい事態に直面している。このような事態を受けて、将来のパンデミックや気候変動の脅威は、異常気象や強制的な移住を引き起こすこととなるため、各国にとって強靭性を強化するための取り組みは特に重要である。このような構造的脅威、特に気候変動は、米国による国際機関への再関与を含め、よりグローバルなアプローチを必要としている。米国と日本は、経済安全保障に関する課題に引き続き取り組み、教訓を共有し、共同対応策を検討すべきである。

THE SEMICONDUCTOR INDUSTRY AND SUPPLY CHAINS: A HISTORICAL PERSPECTIVE

By Willem Thorbecke

Semiconductor devices are the most manufactured item ever, with more than 13 sextillion (1.3 x 10^{22}) metal-oxide silicon (MOS) transistors made so far.[1] They are vital not only for computers and smartphones but also for artificial intelligence, quantum computing, autonomous vehicles, the Internet of Things, cybersecurity, and countless other civilian and military applications.

America's Bell Labs invented the transistor in 1946 and the MOS transistor in 1959. Autonetics Corporation in the early 1960s placed several transistors on a microchip and sold these to the Pentagon to make intercontinental ballistic missiles. Hayakawa Electric (later renamed Sharp) asked Autonetics to produce for them microchips with more than a thousand transistors to be used to make calculators; it turned to the US company after every Japanese firm refused Hayakawa's request. As Johnstone recounts,[2] Hayakawa convinced Autonetics to supplement its high-margin work for the Pentagon with low-margin work in consumer electronics by invoking the learning curve. At first, profits would be small but as Autonetics gained experience, production yields would increase and profits would rise. Autonetics supplied the chips and Hayakawa used these to produce millions of battery-powered calculators. Japanese chipmakers that had refused to produce for Hayakawa now complained to the Ministry of Industry and Trade (MITI), and MITI forbade Hayakawa from buying more microchips from the US. This limited the learning-curve benefits for Autonetics.

Hayakawa, now renamed Sharp, asked RCA, another US company, to supply thin-film transistors to apply to liquid-crystal displays (LCD). RCA demurred and RCA and Westinghouse abandoned the market. Sharp then manufactured them itself and used them to

[1] Laws, D. 2018. Thirteen sextillion and counting: The long and winding road to the most frequently manufactured human artifact in history. Computer History Museum weblog, 2 April. Available at http://computerhistory.org.

[2] Johnstone, B. *We Were Burning: Japanese Entrepreneurs and the Forging of the Electronic Age.* New York: Basic Books, 1999, p. 52.

make not only calculators but also televisions. Sharp and Seiko also mastered the manufacturing process for the complimentary MOS (CMOS) transistors that RCA had developed. It profited from this while RCA and Westinghouse languished.

Bernard Vonderschmitt of RCA said that no one in Silicon Valley recognized the potential of CMOS technology until the late 1970s or early 1980s.[3] Thus, when the industry standard turned to CMOS, Japanese producers were far ahead. In 1980 no Japanese manufacturer was among the top 10 producers in the world but within six years Japan had become the world's leading semiconductor supplier. In 1979 US semiconductors companies had 60 percent of the world market and Japanese companies less than 30 percent. By 1985, they both had 45 percent of the market and then Japanese firms took the lead. In dynamic random access memory (DRAM), the US share fell from 70 percent in 1978 to 20 percent in 1986 while the Japanese share rose from less than 30 percent to 75 percent over this period.[4]

Congress responded by seeking trade protection, complaining that MITI had excluded US semiconductor firms such as Autonetics from the Japanese market. The US and Japanese governments negotiated a settlement. As part of the settlement, MITI pressured Japanese firms to lower export quantities and raise prices for semiconductor devices.

Samsung benefited from these restrictions on its Japanese competitors. In the 1980s, it had focused on DRAM chips. Its workers diligently acquired technology from Japanese and US engineers. In 1985 and 1986 most US producers exited the DRAM market and Japanese producers were constrained by the settlement with the US to limit supply and raise prices. Korean producers were not constrained by this agreement and were able to sell as much as they could produce at the higher prices charged by Japanese producers. Samsung channeled the resulting profits into capital formation and R&D, and as a result, in the early 1990s Samsung became the world's leading producer of DRAMs. It remains the leader in this technology today. The Korean company SK Hynix is now the second leading producer of DRAM and flash memory chips, while Micron, a US company, is third.

---

[3] Ibid., p. 74.
[4] Irwin, D. "The U.S. –Japan Semiconductor Trade Conflict," in Anne O. Krueger, editor, *The Political Economy of Trade Protection.* Chicago: University of Chicago Press, 1996, p. 7.

While Korean companies dominate the market for memory chips, Taiwan Semiconductor Manufacturing Corporation (TSMC) is the leading manufacturer of logic chips. In the 1970s, Taiwan was technically at war with China, had just left the United Nations, severed relations with a key source of technology and capital (Japan), and suffered a 47 percent increase in consumer prices from the first oil shock. Many overseas Chinese researchers, scholars, and engineers were eager to help Taiwan and joined a Technical Advisory Committee (TAC) to advise the government. The TAC identified integrated circuits as a key product to develop and located Chinese engineers working in the US to join the government-sponsored Industrial Technology Research Institute (ITRI). It recommended that Taiwan absorb 7.0 micron CMOS technology at a time when the state of the art was 3.0 micron technology. It also advised that within four years Taiwan should develop technology through local research.[5]

In 1976, Taiwan obtained 7.0 micron technology from RCA, recruited engineers, and provided them training from RCA. Thanks to learning by doing, by 1979 the percentage of ITRI wafers that worked properly surpassed yields at RCA.[6]

The ITRI then pursued very large scale integration (VLSI) technology. VLSI involves placing more than 100,000 devices on a chip. After developing the manufacturing capacity, ITRI employed it to spin off TSMC. As Lin and Rasiah discussed,[7] TSMC inaugurated a new business model. Previously, IC companies integrated design functions with manufacturing functions. TSMC was the first pure-play foundry that did not design its own microchips but instead manufactured them according to other companies' specifications. In 2020, it remains the largest pure-play semiconductor manufacturer, with $69 billion in assets and 50,000 employees. The rise of TSMC as a company that focused on the expensive and capital-intensive activity of producing chips frees other firms to focus on the brain-intensive work of designing chips.

[5] Lin, Y., and Rasiah, R. 2014. "Human capital flows on Taiwan's catch up in integrated circuit manufacturing." *Journal of Contemporary Asia* 44: 64-83.
[6] Breznitz, D. *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan, and Ireland.* New Haven: Yale University Press, 2007, pp. 97-145.
[7] Lin and Rasiah, op cit, note 5.

Many firms in the industry have thus opted for a "fabless" manufacturing model. They design the chips, outsource their production to companies such as TSMC, and then sell the chips under their own name. The US company Nvidia uses this model to produce graphics processing units and sells these to computer gaming companies, AI developers, self-driving car makers, cryptocurrency miners, and cloud service providers. Qualcomm uses it to produce chipsets for smartphones. Advanced Micro Devices, also from the US, uses TSMC to produce chips for PCs and data centers.

Intel has long been an integrated device manufacturer, combining design with manufacturing. However, in 2019 it encountered delays in developing the process technology to produce 10 nanometer (nm) chips and in 2020 it announced delays in developing 7 nm chips. This places Intel well behind TSMC in manufacturing cutting-edge chips. It may have to outsource more production to TSMC.

The supply chain for the semiconductor industry has many sophisticated firms located upstream. Much of the design architecture used to construct chips for smartphones, laptops, tablets, Apple computers, and data centers is licensed from a British company, ARM. Semiconductor manufacturing equipment is made by US companies such as Applied Materials, Japanese companies such as Tokyo Electron, and Dutch companies such as ASML. ASML is a key producer of photolithography equipment as it is the only one using extreme ultraviolet light.

Japan now focuses on producing inputs to the semiconductor industry where craftsmanship and advanced technology are crucial. These include not only semiconductor manufacturing equipment but also ceramic capacitors made by Murata Manufacturing, image sensors made by Sony, and the fluorinated polyimide, photoresists and etching gas made by JSR, Tokyo Ohka Kogyo, Shin-Etsu Chemical, Showa Denko, and Kanto Denka Kogyo.

Chinese firms such as Semiconductor Manufacturing International Corporation (SMIC) and Yangtze Memory produce 40 nm chips, but are working diligently to reach the 5 nm frontier. China's "Big Fund" supports spending on factories and equipment and pays to lure engineers

away from TSMC. Chinese workers in this industry view it as their patriotic duty to achieve self-sufficiency and kept working even in Wuhan during the coronavirus outbreak.

President Trump has restricted the sale of semiconductor manufacturing equipment, software, and chips made with US technology to SMIC, Huawei, and other Chinese companies deemed unreliable. US allies are also restricting sales: for instance, ASML has been unable to obtain a license to sell photolithography equipment to SMIC.

The US has lost its comparative advantage in manufacturing computer chips. Having chip-making centered in Korea, Taiwan, and China poses risks if there is a military conflict. Channeling money to the semiconductor industry and imposing protectionism is unlikely to recreate a vibrant domestic industry, however. During the Cold War, military funding helped US companies invent countless technologies. However, it was often Japanese rather than US companies that profited. Government largesse left US companies bloated, while market forces compelled Japanese companies to innovate. Protectionism in the semiconductor industry also backfired for both the US and Japan. If national security requires that chips be produced domestically, then the US should spend the minimum amount necessary to achieve this goal. If the US wants to revive its manufacturing sector, then it should reduce its budget deficit, expose its industries to the discipline of global competition, and glean lessons judiciously from Asia's manufacturing success.

半導体産業とサプライチェーン：歴史的な観点からの考察

ウィリアム・ソーベック

半導体デバイスはこれまでに最も多く製造されたものであり、13 セクスティリオン（1.3×10^{22}）個以上の金属酸化物シリコン（MOS）トランジスタが製造されてきた（Laws, 2018）。それらはコンピュータやスマートフォンにとって不可欠なだけでなく、人工知能、量子コンピューティング、自動運転、IoT、サイバーセキュリティ、その他の無数の民間および軍事への応用にとっても不可欠なものである。

米国のベル研究所は 1946 年にトランジスタを、1959 年に MOS トランジスタを発明した。1960 年代の初めには、オートネティクス社がいくつかのトランジスタをマイクロチップ上に配置し、大陸間弾道ミサイルを製造するために国防総省に売却した。早川電機（後にシャープと改名）は電卓の製造をするために、1000 個以上のトランジスタを搭載したマイクロチップの製造をオートネティックス社に依頼した。日本のどの企業も早川電機の依頼を断った為、米国企業に話を持ち掛けたのであった。Johnstone（1999）が回顧するように、早川電機は学習曲線の考え方からオートネティクス社に対して国防総省向けの利益率の高い仕事を、民間向け電子機器という利益率の低い仕事で補うよう説得した。即ち、初めは利益が低いものかもしれないが、オートネティクス社が経験を積むにつれて生産収率が上昇し、利益も上昇するだろうということだった。結果としてオートネティクス社はチップを供給し、早川電機はそれらを用いて何百万台もの電池式計算機を製造した。しかし、初めは早川電機に対するチップ製造を拒んでいた日本のチップメーカーは、今度は通商産業省（通産省）に対して苦情を申し立てた。それにより、通産省は早川電機に対して米国からマイクロチップをさらに購入することを禁じたのだった。この早川電機に対する通産省の措置によって、オートネティクス社の学習曲線によるメリットは限定的なものになった。

シャープという名前に変更した早川電機は、今度は液晶ディスプレイ（LCD）に応用するため、RCA という別の米国企業に対し薄膜トランジスタを供給するように依頼した。しかし、RCA はこの申し出に対し難色を示し、RCA とウェスティングハウスはその市場から撤退したのだった。その後、シャープはそれらを自社で製造し、電卓だけでなくテレビの製造にも用いた。シャープとセイコーはその他にも、RCA が開発した CMOS（Complimentary MOS）の製造工程もマスターし、RCA とウェスティングハウスが低迷する中、その恩恵を受けたのだった。

RCA のバーナード・ワンダーシュミット（Bernard Vonderschmitt）氏は 1970 年代後半から 80 年代の初めまで、シリコンバレーにおいて誰も CMOS 技術の持つ可能性に気付いていなかったと語る。(Johnstone, 1999）ゆえに業界の標準が CMOS へと移った時には、日本のメーカーははるか先を行っていた。1980 年には、どの日本のメーカーも世界トップ 10 には入っていなかったが、その後の 6 年間で日本は世界をリードする半導体供給者となった。1979 年には米国の半導体企業は世界シェアの 60 パーセントを占めており、日本企業は 30 パーセントにも満たなかった。それが 1985 年までに、両者とも 45 パーセントとなり、日本の企業がリードしたのだった。ダイナミック・ランダム・アクセス・メモリ（DRAM）に関しても、米国のシェアは 1978 年の 70 パーセントから 1986 年には 20 パーセントに低下した。一方で、同じ期間に日本のシェアは、30 パーセントにも満たない状態から 75 パーセントにまで上昇した。（Irwin, 1996）

米国議会は、通産省がオートネティクス社など米国の半導体メーカーを日本の国内市場から排除したことに不満を持ち、貿易保護を求めるという反応を示した。日米の両政府は和解交渉を行い、その一環として通産省は日本企業に対し、半導体の輸出量を減らし価格を引き上げるよう圧力をかけた。

サムスンは日本の競合他社が受けたこれらの制約から恩恵を受けた。1980 年代、サムスンは DRAM チップに注力していた。サムスンは日本と米国の技術者から熱心に技術を習得していた。1985 年、1986 年にはほとんどの米国メーカーは DRAM

市場から撤退し、日本のメーカーは供給量を制限し価格を引き上げるという、米国との和解案の制約を受けていた。韓国のメーカーはこの合意に制約を受けることなく、できるだけ多くの製品を、日本のメーカーが課したよりも高い価格で販売することができた。サムスンはその利益を資本形成と研究開発に当て、結果としてサムスンは、1990 年代の初めには世界をリードする DRAM メーカーとなった。サムスンは現在でもこの技術の先導者である。韓国の SK ハイニックス社は今や世界第 2 位の DRAM とフラッシュメモリチップのメーカーであり、米国のマイクロン（Micron）社は第 3 位となっている。

韓国企業がメモリチップ市場を独占する一方で、ロジックチップにおいては台湾積体電路製造（TSMC）が業界大手である。1970 年代において、台湾は厳密にはまだ中国と戦争状態にあり、国連を脱退したばかりで、技術と資本の重要な供給源であった日本との関係が断たれ、第一次オイルショックによる 47 パーセントもの消費者物価の高騰に苦しんでいた。多くの華僑の研究者、学者、エンジニアが台湾を支援することを熱望し、政府に助言を与える技術諮問委員会（TAC）に参加した。TAC は集積回路が開発すべき重要な製品だと判断し、政府出資の工業技術研究院（ITRI）への参加者として米国にいる中華系エンジニアを探し出した。当時の最先端が 3.0 ミクロンレベルである中で、台湾は７.0 ミクロンサイズの CMOS 技術を習得すべきとした。また、台湾は 4 年以内に国内での研究を通じて技術開発をすべきであると当委員会は提言した。(Lin and Rasiah, 2014)

1976 年、台湾は RCA から７.0 ミクロン技術を習得し、技術者を集め、彼らに RCA からの研修を受けさせた。これによって、1979 年までには ITRI の正常に作動するウェハーの歩留まりは、RCA のそれを上回るようになった。(Breznitz, 2007)

その後、ITRI は超大型集積回路（VLSI）技術を追求した。VSLI は一つのチップ上に 10 万個以上のデバイスを搭載する技術である。製造能力を開発した後、ITRI はそれを用いて TSMC を分社化した。Lin and Rasiah (2014)が論じるように、TSMC は新しいビジネスモデルを始めた。それまでの集積回路企業は集積回路の設計機能

と製造機能を統合していた。それに対し、TSMC は自社でマイクロチップの設計を行わない代わりに他社の仕様に合わせたチップを製造するという、初のピュアプレイファウンドリ企業（pure-play foundry）だったのである。2020 年の現在においても、TSMC は 690 億ドルの資産を持ち、5 万人の従業員を擁する世界最大のピュアプレイ半導体メーカーである。TSMC がチップ製造という高価で資本集約的な事業に特化した企業として台頭したことにより、他の企業はチップの設計という頭脳集約的な作業に注力できるようになった。

このように、チップ業界における多くの企業が「ファブレス」（企画設計・開発は行うが自社では製造しない）モデルで操業している。彼らはチップを設計し、その製造を TSMC のような企業に委託し、出来上がったチップを彼らの名で販売している。米国のエヌビディア（Nvidia）社はこのビジネスモデルでグラフィックス・プロセッシング・ユニット（GPU）を製造し、それをコンピューターゲーム企業や AI 開発者、自動運転車研究者、暗号通貨マイナー、クラウドサービスのプロバイダーなどに販売している。同様に、クアルコム（Qualcomm）社はスマートフォン用のチップセットを製造している。米国のアドバンスト・マイクロ・デバイセズ（Advanced Micro Devices）社も PC やデータセンター用のチップ製造に TSMC を利用している。

インテル（Intel）は長年設計と製造を組み合わせたデバイスメーカーであった。しかし、2019 年に 10 ナノメートル（nm）チップ製造のプロセス技術開発の遅れに直面し、2020 年には 7 nm チップ開発の遅れを発表した。これらによって、インテルは最新鋭のチップ製造において TSMC に大きく後れをとっている。インテルはより多くの製造を TSMC に外注しないといけないかもしれない。

半導体産業のサプライチェーンにおいては、たくさんの優良企業がその上流に存在している。例えば、スマートフォンやノートパソコン、タブレット、アップルのコンピュータ、データセンターに使われるチップの製造において用いられるアーキテクチャ設計の多くは、イギリスのアーム（ARM）社からライセンスを受け

ている。半導体の製造機器はアプライド・マテリアルズ（Applied Materials）社などの米国企業、東京エレクトロンなどの日本企業、ASML のようなオランダ企業によって製造されている。ASLM は唯一極紫外線を用いたフォトリソグラフィ機器を製造する重要なメーカーである。

現在の日本は、熟練した技術と先進的な技術が重要な半導体業界において必要な原料を生産することに注力している。これらは半導体生産機器といったものだけではなく、村田製作所によるセラミックコンデンサや、ソニーによるイメージセンサー、JSR や東京応化工業、信越化学工業、昭和電工、関東電化工業によって生産されているフッ化ポリイミド、フォトレジスト、エッチングガスなども含まれる。

中芯国際集成電路製造（SMIC）や長江存儲科技（Yangtze Memory）といった中国企業は現在 40 ナノメートルのチップを製造しているが、最先端の 5 ナノメートルサイズの開発に尽力している。中国「大資本」（”Big Fund”）は工場や設備への出資を支援し、技術者を TSMC から引き抜くために資金を投入している。この業界における中国人労働者は、これら技術を国内で自給自足することが愛国的な義務であるととらえ、コロナウイスが発生した武漢においてすら働き続けた。

トランプ大統領は米国の技術で作られた半導体製造機器やソフトウェア、チップなどを SMIC やファーウェイ、その他信頼できないと考えられている中国企業へ販売することに制限を課した。米国の同盟国も同様に制限を課している。例えば、ASML はフォトリソグラフィ装置を SMIC に対して販売するライセンスを取得できずにいる。

米国はコンピューターチップ製造における比較優位性を失ってしまった。チップ製造を韓国や台湾、中国に集中させることは、軍事的衝突があった場合のリスクを呈している。しかし半導体産業に資金を投入し、保護主義を押し付けても、国内産業を再び活気づけることができる訳ではない。冷戦時代においては、軍による資金援助によって米国の企業は多くの技術を開発したが、米国企業ではなく、

しばしば日本企業が利益を得ていた。政府による惜しげもない援助は米国の企業を肥大化させたが、一方で日本企業は市場原理の中で革新的に変化し続けた。また、半導体産業における保護主義は日米の双方にとって裏目に出た。国家安全保障上、チップの国内生産が必要ならば、米国はこの目標を達成するために必要最低限の出資に抑えるべきだろう。米国がチップの製造業を再び甦らせたいならば、財政赤字を減らし、自国の産業を国際競争の原理にさらし、アジアにおける製造業の成功から賢明に教訓を得るべきだ。

GAME-CHANGING BIOTECHNOLOGY: SECURITY, PROLIFERATION & GOVERNANCE CHALLENGES

By Margaret E. Kosal

Preventing the acquisition and use of biological weapons by hostile states, substate actors, or terrorists is among the highest international security priorities. Novel threats posed by the proliferation of advances in the life sciences and biotechnology have been recognized as potential game-changers. Understanding and anticipating the types of threats that may emerge from the life sciences and biotechnology; the potential consequences of those threats; and the motivation for others to seek, to intentionally pursue proliferation, and to obtain such weapons – all are necessary for preparing for the security of the nation and allies.

Using technical scholarship, social science methods, and current affairs, I explore how these game-changers may affect geopolitics and international relations to shape the future. The life sciences will offer novel offensive and defensive capabilities. How or if any of these might shift or reorder the existing balance of power is considered, along with potential governance approaches.

In the 21st century, both nation-states and nonstate actors are likely to have access to game-changing advances in the life sciences and new biotechnology-enabled capabilities.[1] This has been highlighted by prominent public figures,[2] policymakers,[3] international organizations,[4] and

[1] *Biotechnology Research in an Age of Terrorism*; (Washington, D.C: National Academies Press, 2004) and *Globalization, Biosecurity, and the Future of the Life Sciences*; (Washington, D.C: National Academies Press, 2006).
[2] "Bill Gates warns tens of millions could be killed by bio-terrorism," *The Guardian (UK),* February 18, 2017, https://www.theguardian.com/technology/2017/feb/18/bill-gates-warns-tens-of-millions-could-be-killed-by-bio-terrorism.
[3] For example, "Letter to the President," President's Council of Advisors on Science and Technology, Executive Office of the President, November 2016, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_biodefense_letter_report_final.pdf.
[4] "New scientific and technological developments relevant to the Convention: Some examples," BWC Preparatory Committee, Eighth Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, BWC/CONF.VIII/PC/WP.18, August 5, 2016.

other prominent voices.[5] From a security perspective, among the most notable was the inclusion of advances in gene editing in the list of threats posed by "weapons of mass destruction and proliferation" by then-US Director of National Intelligence (DNI) James Clapper in the DNI's 2016 annual Worldwide Threat Assessment Report.[6]

At the intersection of game-changing biotechnology and security, one of the most provocative areas is advances in genetic engineering. While one of these -- the CRISPR systems -- has garnered a great deal of attention, other, less well-known gene-editing techniques are also important. CRISPR stands for Clustered Regularly Interspaced Short Palindromic Repeats and is a bacteria-derived system that uses RNA molecules that recognize specific human DNA sequences and can make cuts and insertions in a programmable way.[7] In October 2020, the Royal Swedish Academy of Sciences announced that Drs. Jennifer A. Doudna and Emmanuelle Charpentier had been selected to receive the Nobel Prize in Chemistry. In the announcement, the Academy highlighted their work as being "one of gene technology's sharpest tools: the CRISPR/Cas9 genetic scissors. Using these, researchers can change the DNA of animals, plants, and microorganisms with extremely high precision. This technology has had a revolutionary impact on the life sciences, is contributing to new cancer therapies, and may make the dream of curing inherited diseases come true."[8] The initial work that led to realizing the game-changing nature of the CRISPR system was undertaken in pursuit of new ways to overcome antibiotic resistance. It illustrates that many of the most game-changing advances in science and technology occur when one is not specifically looking for the end result and that

[5] R. G. Reeves, et al., "Agricultural Research, or a New Bioweapon System?" *Science*, 362, no. 6410 (2018), 35-37; Malcolm Dando, "Find the Time to Discuss New Bioweapons," *Nature*, 535 (July 2016), 9. https://www.nature.com/news/find-the-time-to-discuss-new-bioweapons-1.20206; and

[6] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community,* Statement for the Record to the Senate Armed Services Committee, February 9, 2016, https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

[7] For an excellent overview of the CRISPR-Cas9 system, see, Jennifer A. Doudna and Emmanuelle Charpentier, "The new frontier of genome engineering with CRISPR-Cas9," *Science*, vol. 346, no. 6213 (Nov. 2014), pp. 1077-1088, https://science.sciencemag.org/content/346/6213/1258096.

[8] Royal Swedish Academy of Sciences, "The Nobel Prize in Chemistry 2020 to Emmanuelle Charpentier, Max Planck Unit for the Science of Pathogens, Berlin, Germany, and Jennifer A. Doudna, University of California, Berkeley, USA," 7 October 2020, https://www.nobelprize.org/prizes/chemistry/2020/press-release/.

these advances are most likely to occur at metaphorical seams or intersections of traditional technical disciplines.[9]

CRISPR is not the first type of gene-editing technology, but it is best known in national and international security debates. Such advancements now allow for easier and more tunable manipulation of the genetic code of life with implications for governance of science and technology and with international security significance in the context of proliferation, deterrence, and unconventional weapons. Scholars have written on the game-changing and potentially strategic nature of advanced biotechnology and its impact upon international security.[10] Biosecurity concerns range from resurrecting viruses like the causative agent of smallpox; increasing the lethality, duration, or ease of transmission of microbiological agents; and development of novel delivery methods that avoid detection or can overcome preventative measures like vaccines and other therapeutics.[11] Whether gene-editing techniques like CRISPR may enable capabilities that challenge nuclear weapons in terms of strategic stability is also being considered.[12] One of the factors that differentiates advanced biotechnology from earlier weapons is the greater level of uncertainty in terms of effect, capabilities, capacity, detectability, stealth, and offensive versus defensive intention.

---

[9] J. Rogers Hollingsworth, "High Cognitive Complexity and the Making of Major Scientific Discoveries," *in Knowledge, Communication, and Creativity,* Arnaud Sales and Marcel Fournier (eds), 2007, Sage Publications, pp 129-155.

[10] Thomas Preston, *From Lambs to Lions: Future Security Relationships in a World of Biological and Nuclear Weapons,* Boulder, CO: Rowman and Littlefield, 2007/2009; Kathleen M. Vogel and Sonia Ben Ouagrham-Gormley, "Anticipating Emerging Biotechnology Threats: A Case Study of CRISPR," *Politics and the Life Sciences,* 37, no 2 (Fall 2018), 203-219; Gigi Gronvall, "The Security Implications of Synthetic Biology," *Survival,* 60, no. 4 (2018), 165-180; Margaret E. Kosal, "Emerging Life Sciences and Possible Threats to International Security," *Orbis,* 64, 4, 2020, pp 599-614, https://doi.org/10.1016/j.orbis.2020.08.008; Greg Koblentz, "Pathogens as Weapons: The International Security Implications of Biological Warfare," *International Security* (2003) 28:84-122; Margaret E. Kosal, "Anticipating the Biological Proliferation Threat of Nanotechnology: Challenges for International Arms Control Regimes, pp.159-174, in Hitoshi Nasu and Robert McLaughlin (eds.), *New Technologies and the Law of Armed Conflict*, Springer, 2014; Jonathan B. Tucker, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies,* MIT Press, 2012.

[11] Margaret E. Kosal, *Nanotechnology for Chemical and Biological Defense*, (NY: Springer, 2009).

[12] Martin, Susan, "The Role of Biological Weapons in International Politics," *Journal of Strategic Studies* (2002) 25:63-98; Francisco Galamas, "Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution," *Comparative Strategy* (2008) 27:315-323; Margaret E. Kosal, "CRISPR & New Genetic Engineering Techniques: Emerging Challenges to Strategic Stability and Nonproliferation," *Nonproliferation Review,* in press.

The nature of biotechnology – and much of modern science and technology – adds further complications to governance, response, and risk mitigation. Biotechnology is a dual-use technology, meaning that the same or similar techniques, manufacturing elements, and processes used for beneficial purposes could also be misused for deleterious purposes.[13] Some basic and applied research is considered dual-use research of concern.[14] Advances in biotechnology and gene-editing specifically not only potentially pose security and proliferation concerns, but they also may enable new capabilities for defense, detection, and verification of biological agents, as well as diagnostic capabilities for emerging infectious diseases, like COVID-19,[15] and a plethora of other beneficial outcomes beyond therapeutic gene-editing, as was highlighted in the 2020 Chemistry Nobel Prize announcement.

A driving concern is that in the 21st century, both nation-states and nonstate actors may have access to new and potentially devastating dual-use biotechnology technology. Advanced technology is no longer the domain of the few. Biological weapons are perceived as (and in some cases, arguably are) relatively cheap and easier to produce, more widely available, and within the capabilities of an increasingly large number of people with access to minimal technical skills and equipment and more concealable dual-use technologies, especially when compared to obstacles in attaining and developing nuclear weapons. The potential synergies between biotechnology and other emerging technologies, such as nanotechnology, big data analytics, machine learning, and artificial intelligence, cognitive neurosciences, and all things cyber not only suggest tremendous potential promise for advancement in technologies for

[13] For this paper, dual use refers to the fact that almost all the equipment and materials needed to develop dangerous or offensive agents, particularly biological and chemical agents, have legitimate uses in a wide range of scientific research and industrial activity, including defensive military uses. Within this context, it does not refer to a demarcation between civilian or military uses.
[14] "United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern," 24 September 2015, http://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf and https://osp.od.nih.gov/biotechnology/dual-use-research-of-concern/ .
[15] "SHERLOCK Team Advances Its CRISPR-Based Diagnostic Tool," Broad Institute, October 4, 2019, https://www.broadinstitute.org/news/sherlock-team-advances-its-crispr-based-diagnostic-tool; "Enabling coronavirus detection using CRISPR-Cas13: An open-access SHERLOCK research protocol," McGovern Institute, February 14, 2020, https://mcgovern.mit.edu/2020/02/14/enabling-coronavirus-detection-using-crispr-cas13-an-open-access-sherlock-research-protocol/; and Sabbi Lall, "SHERLOCK-based one-step test provides rapid and sensitive COVID-19 detection," McGovern Institute, May 5, 2020, https://mcgovern.mit.edu/2020/05/05/sherlock-based-one-step-test-provides-rapid-and-sensitive-covid-19-detection/.

consumers and defense applications but also raise new security, privacy, and civil-rights concerns.

The Biological Weapons Convention and other international regimes create legal frameworks and norms that condemn the proliferation and use of biological agents. Alone, the current framework, which lacks any verification protocol, is an increasingly shaky deterrent. Challenges to the post-WWII international order from states like Russia, China, and DPRK further add to the perilousness of excessive reliance on any single governance tool.

Biosecurity and other emerging technologies require new models, not just extrapolations of Cold War or more recent deterrence (or nonproliferation) paradigms. Nonproliferation of biological weapons is a function of nation-states and the international community. In the late 20th and early 21st century, the international community and nation-states struggled – and continue to do so – to deal with technologically-enabled proliferation challenges. An underlying challenge of biological-weapons nonproliferation in the 21st century has been the tacit shifts in responsibility for nonproliferation from the international community and nation-states to individual researchers. This is primarily due to intransigence at the international level and domestically in some major states, like the US. The risks associated with traditional pathogenic bacterial and viral-based weapons have not diminished. At the same time, globalization and the information revolution have made new technological developments accessible and relatively inexpensive to many nations and put them within the grasp of more states and nonstate actors.

In the 21st century, limiting the proliferation of technologically enabled biological weapons necessarily involves the physical sciences, the life sciences, the medical sciences, and several engineering communities. Biotechnology has evolved to be an intrinsically interdisciplinary domain with the potential to bridge many disciplines. Notable examples are found in the design of sensors that use active complexes that bind DNA to carbon nanotubes; this was a joint effort by electrical engineers and computer scientists[16] in one case and originated in a physics and astronomy department research group in another.[17]

[16] C Dwyer, et al., "DNA Functionalized Singlewalled Carbon Nanotubes," *Nanotechnology,* 2002, 13, pp 601-604.
[17] C Staii, M Chen, A Gelperin, AT Johnson, "DNA-decorated Carbon Nanotubes for Chemical Sensing," *Nano Lett.* 2005, 5, pp 1774-1778.

The social sciences also need to be more fully integrated into technical-based nonproliferation efforts or the latter risk being technologically deterministic. Narrow demarcations of research into traditional disciplinary silos – literally 'old school thinking' – have become increasingly less likely to yield transformational technologies or policy approaches. Cutting-edge science is fundamentally interdisciplinary. That interdisciplinarity is messy when it comes to designing implantable policy and makes an already challenging problem even more complicated.

Flexible approaches to nonproliferation and counterproliferation are important policy elements to reduce the risk of malfeasant application of biotechnology. Practices and policies that do not account for the international nature and prominent commercial biotechnology sector are increasingly inadequate. The issue of a state (or a terrorist group) utilizing biological weapons against another state is a mounting concern since dangerous pathogens have been known to cause deadly effects, yet little weapons deterrence research addresses methods of dealing with the threat of biological weapons and even less with deterring bioterrorism. Bridging the gaps between the life sciences, the social sciences, and implementable policy is a crucial element in devising implementable and executable strategies that can lead to successful nonproliferation and deterrence of bioweapons. Similarly, thinking about verification and international arms control regimes can be explored as part of new approaches to strategic deterrence in the 21st century.

Reducing the risk of state-based misuse of biotechnology for biological proliferation will mean consideration of the highly transnational nature of biotechnology research and development, which is more likely to come from political scientists, science and technology studies scholars, and others. [18] Traditional and innovative new approaches to nonproliferation and counterproliferation are important policy elements to reduce the risk of malfeasant application of technology. Robust international agreements lower the risk of terrorist applications by eliminating legal routes for terrorists to obtain agents, precursors, or weaponization materials,

[18] E.g., Kathryn Ibata-Aren, *Beyond Technonationalism: Biomedical Innovation and Entrepreneurship in Asia,* April 2019, Stanford University Press; Roselyn Hsueh, *China's Regulatory State: A New Strategy for Globalization,* Cornell University Press, 2011; Kathleen Vogel, *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats,* Johns Hopkins University Press, 2013; Kobi-Renee Leins, *International Law Applicable to the Use of Nanomaterials in War,* 2019, http://hdl.handle.net/11343/238667.

and by minimizing transfers from state to nonstate actors through theft, deception, or other means. Efforts to strengthen the international regime to control transfers of dual-use materials and equipment are also important. The highly transnational nature of biotechnology research and development is a major consideration in reducing the risk of state-based misuse for biological (or chemical) weapons. Narrow demarcations of research into traditional divisions will decreasingly yield the strategies and results needed to govern our ingenuity in limiting the threats – while maximizing the benefits – from these game-changing advances in the life sciences and biotechnology.

革新的なバイオテクノロジーにおける安全保障、拡散とガバナンスの課題

マーガレット E. コーザル

生物兵器が敵性国家や準国家主体、テロリストの手に渡るのを阻止することは、国際安全保障上の最優先事項のひとつである。生命科学とバイオテクノロジー分野における発展の拡散によって引き起こされる新たな脅威は、潜在的なゲームチェンジャーとして認識されている。生命科学とバイオテクノロジーから出現するであろう脅威の種類、それらの脅威によって引き起こされる潜在的な事態、これら兵器を求め、意図的に拡散させ、取得する意図−これらのことを理解し予測することは、米国と諸同盟国がこれらの脅威から身を守る準備を行う上で必要である。

技術的な知見、社会科学のメゾット、時事問題を通じて、これらのゲームチェンジャーがどのように地政学や国際関係に影響を与え、未来を形作るのかについて私は研究を行っている。生命科学は新しい攻撃能力と防衛能力の両方を生み出すだろう。これらの技術が既存のパワーバランスを変えたり、再編成することはあるのか、どのようにしてそれが行われるのかを、新たなガバナンスのアプローチと共に検討する。

21 世紀においては国家主体と非国家主体の両方が、生命科学と新たなバイオテクノロジーが可能にする、革新的な進歩を利用しうる[1]。このことは社会的に大きな

[1] *Biotechnology Research in an Age of Terrorism*; (Washington, D.C: National Academies Press, 2004) and *Globalization, Biosecurity, and the Future of the Life Sciences*; (Washington, D.C: National Academies Press, 2006).

影響力を持つ人々[2]や政策立案者[3]、国際機関[4]、その他著名人[5]によって強調されている。安全保障の観点において最も注目されたのは、当時のアメリカ合衆国国家情報長官（DNI）ジェームズ・クラッパーによる DNI 2016 年次グローバル脅威評価報告書[6](DNI’s 2016 annual Worldwide Threat Assessment Report)において、「大量破壊兵器と拡散」（“weapons of mass destruction and proliferation”）によってもたらされる脅威を示したリストの中に遺伝子編集技術の発達が含まれていたことだ。

革新的なバイオテクノロジーと安全保障が交叉する部分において、もっとも挑戦的な分野の一つが、遺伝子工学の進歩である。その中の一つである CRISPR システムは特に注目を集めているが、それ以外のあまり知られていない遺伝子編集技術も重要である。CRISPR とは Clustered Regularly Interspaced Short Palindromic Repeats の略であり、細菌由来のシステムである。そのシステムは特定の人体の DNA に反応する RNA を用いており、操作可能な方法で遺伝子の切断・挿入を行うことができる[7]。2020 年 10 月、スウェーデン王立科学アカデミーはノーベル化学賞の受賞者として、ジェニファー・A・ダウドナ博士とエマニュエル・シャルパンティエ博士を発表した。発表において科学アカデミーは、彼らの研究成果をこ

---

[2] “Bill Gates warns tens of millions could be killed by bio-terrorism,” *The Guardian (UK),* February 18, 2017, https://www.theguardian.com/technology/2017/feb/18/bill-gates-warns-tens-of-millions-could-be-killed-by-bio-terrorism.

[3] その例として次があげられる： “Letter to the President,” President’s Council of Advisors on Science and Technology, Executive Office of the President, November 2016, https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_biodefense_letter_report_final.pdf.

[4] “New scientific and technological developments relevant to the Convention: Some examples,” BWC Preparatory Committee, Eighth Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, BWC/CONF.VIII/PC/WP.18, August 5, 2016

[5] R. G. Reeves, et al., “Agricultural Research, or a New Bioweapon System?” *Science*, 362, no. 6410 (2018), 35-37; Malcolm Dando, “Find the Time to Discuss New Bioweapons,” *Nature*, 535 (July 2016), 9. https://www.nature.com/news/find-the-time-to-discuss-new-bioweapons-1.20206

[6] James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community,* Statement for the Record to the Senate Armed Services Committee, February 9, 2016 https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

[7] CRISPR-Cas9 システムについての素晴らしい概要は次を参照されたい：Jennifer A. Doudna and Emmanuelle Charpentier, “The new frontier of genome engineering with CRISPR-Cas9,” *Science*, vol. 346, no. 6213 (Nov. 2014), pp. 1077-1088, https://science.sciencemag.org/content/346/6213/1258096.

う評した：「CRISPR/Cas9 という遺伝子のハサミは、遺伝子工学における極めて鋭利なツールの一つです。これによって、研究者は動物や植物、微生物の DNA を非常に高い精度で改変することができます。この技術は生命科学に革命的なインパクトを与え、新たながん治療に貢献し、遺伝子疾患の治療という夢を実現させるかもしれません。[8]」CRISPR システムの革新性を実証した最初の研究は、抗生物質耐性機構を克服する新たな方法を求めて行われた。科学と技術における革新的な進歩の多くは、特定の明確な研究結果を求めている時ではなく、比喩的なつなぎ目、言い換えれば伝統的な技術分野の交わるところで生まれやすいことをこの研究は示している[9]。

CRISPR は初めての遺伝子編集技術というわけではないが、国家安全保障、国際安全保障における議論の中では最もよく知られている。このような技術の進歩は、これまで以上に遺伝子コードの操作を簡単で調整可能にすると共に、科学技術のガバナンスと、拡散や抑止、非従来型兵器の文脈から国際安全保障上においても重要な意味合いを持つようになった。専門家は先進的なバイオテクノロジーの潜在的戦略性と、それらがゲームチェンジャーになりうること、国際安全保障に与える影響について喚起してきた[10]。バイオセキュリティは天然痘病原体のような

[8] Royal Swedish Academy of Sciences, "The Nobel Prize in Chemistry 2020 to Emmanuelle Charpentier, Max Planck Unit for the Science of Pathogens, Berlin, Germany, and Jennifer A. Doudna, University of California, Berkeley, USA," 7 October 2020, https://www.nobelprize.org/prizes/chemistry/2020/press-release/.

[9] J. Rogers Hollingsworth, "High Cognitive Complexity and the Making of Major Scientific Discoveries," *in Knowledge, Communication, and Creativity,* Arnaud Sales and Marcel Fournier (eds), 2007, Sage Publications, pp 129-155.

[10] Thomas Preston, *From Lambs to Lions: Future Security Relationships in a World of Biological and Nuclear Weapons,* Boulder, CO: Rowman and Littlefield, 2007/2009; Kathleen M. Vogel and Sonia Ben Ouagrham-Gormley, "Anticipating Emerging Biotechnology Threats: A Case Study of CRISPR," *Politics and the Life Sciences,* 37, no 2 (Fall 2018), 203-219; Gigi Gronvall, "The Security Implications of Synthetic Biology," *Survival,* 60, no. 4 (2018), 165-180; Margaret E. Kosal, "Emerging Life Sciences and Possible Threats to International Security," *Orbis,* 64, 4, 2020, pp 599-614, https://doi.org/10.1016/j.orbis.2020.08.008; Greg Koblentz, "Pathogens as Weapons: The International Security Implications of Biological Warfare," *International Security* (2003) 28:84-122; Margaret E. Kosal, "Anticipating the Biological Proliferation Threat of Nanotechnology: Challenges for International Arms Control Regimes, pp.159-174, in Hitoshi Nasu and Robert McLaughlin (eds.), *New Technologies and the Law of Armed Conflict*, Springer, 2014; Jonathan B. Tucker, *Innovation, Dual Use, and Security: Managing the Risks of Emerging Biological and Chemical Technologies,* MIT Press, 2012.

ウイルスの復活、細菌の致死性や持続性、感染力の上昇といったことから、検出の網をすり抜けるような又はワクチンやその他治療法などの予防法に対する耐性をつけるなどの新たな運搬方法の開発など多岐にわたる[11]。CRISPR のような遺伝子編集技術が、戦略的安定性の観点から核兵器に代わることができるのかどうかも検討されている[12]。先進的なバイオテクノロジーがそれ以前の兵器と異なる点の一つは、効果、能力、装備力、検出可能性、ステルス性、攻撃的か防御的なのかといった観点でバイオテクノロジーの方が、不確実性が高いことである。

バイオテクノロジーーそしてその他多くの現代科学技術ーはガバナンス、対策、リスク低減をさらに複雑なものにしている。バイオテクノロジーはデュアルユース技術である。即ち有益な目的のための技術、製造要素、プロセスはその類似のもの、または全く同じものが有害な目的のためにも利用されうるということである[13]。いくつかの基礎研究・応用研究はデュアルユースの問題が懸念されている[14]。バイオテクノロジーと遺伝子編集技術の進歩は潜在的に安全保障と拡散の懸念がある一方、2020 年のノーベル化学賞の発表で語られたように、生物学的物質に対する防衛、検出、検証を可能にしうるのみならず、COVID-19 のような新たな感染症の診断法[15]や医学的治療のための遺伝子編集を超えた、多くの有益な成果をもたらす可能性を有している。

---

[11] Margaret E. Kosal, *Nanotechnology for Chemical and Biological Defense*, (NY: Springer, 2009).
[12] Martin, Susan, "The Role of Biological Weapons in International Politics," *Journal of Strategic Studies* (2002) 25:63-98; Francisco Galamas, "Biological Weapons, Nuclear Weapons and Deterrence: The Biotechnology Revolution," *Comparative Strategy* (2008) 27:315-323; Margaret E. Kosal, "CRISPR & New Genetic Engineering Techniques: Emerging Challenges to Strategic Stability and Nonproliferation," *Nonproliferation Review,* in press.
[13] 本論文においてはデュアルユースという言葉が危険性のある物質、
または攻撃的な物質、特に生物学的・化学的な物質を製造する際に必要な設備、
材料のほぼすべてが防衛的な軍事用途を含む幅広い範囲の科学研究や産業活動で合法的に用いられていることを指す。この文脈では民生用と軍事用の境界について指摘しているわけではない。
[14] "United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern," 24 September 2015, http://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf and https://osp.od.nih.gov/biotechnology/dual-use-research-of-concern/ .
[15] "SHERLOCK Team Advances Its CRISPR-Based Diagnostic Tool," Broad Institute, October 4, 2019, https://www.broadinstitute.org/news/sherlock-team-advances-its-crispr-based-diagnostic-tool; "Enabling coronavirus detection using CRISPR-Cas13: An open-access SHERLOCK research protocol," McGovern Institute, February 14, 2020, https://mcgovern.mit.edu/2020/02/14/enabling-coronavirus-detection-using-crispr-cas13-an-open-access-sherlock-research-protocol/; and Sabbi Lall, "SHERLOCK-based one-step test

21 世紀においては、国家主体と非国家主体の両方が、新たなそして潜在的に破壊的なデュアルユースのバイオテクノロジー技術へアクセス可能となるかもしれないということが強く懸念されている。先端技術はもはや少数のアクターのよる領域ではない。生物兵器は（いくつかの場合においては議論の余地もあるが）比較的安価で、容易に製造でき、幅広く活用でき、最低限の技術と設備を持った多くの人々が利用できる、隠匿性の高いデュアルユース技術だと認識されている。特に核兵器の場合と比べると、獲得と開発の障壁は低い。バイオテクノロジーとその他ナノテクノロジーやビックデータ解析、機械学習、人工知能、認知神経科学、そしてサイバー技術など新しい技術との間の潜在的な相乗効果は、民生技術や防衛技術における進歩の多大な可能性を秘めているが、同時に新たな安全保障やプライバシー、市民の権利の問題などを提起する。

生物兵器禁止条約などの国際レジームは生物兵器の拡散や使用を非難する法的枠組みと規範を作っている。しかし現状の枠組みは検証プロトコルを欠いており、ますます不安定な抑止力となっている。中国やロシア、北朝鮮のような国家による、第二次世界大戦後の国際秩序に対する挑戦は、単一のガバナンスツールに過度に依存することの危険性を高めている。

バイオセキュリティや新たな技術については、冷戦時代や近年の抑止（または不拡散）パラダイムに何かを加えるのではなくて、全く新しいモデルが必要である。生物兵器の不拡散は国民国家及び国際社会と密接に関連している。20 世紀後半から 21 世紀はじめにかけて、国民国家と国際社会は技術的に可能になった拡散という課題をどうすべきか苦悩してきた。（そしてそれは依然として続いている。）21 世紀において、生物兵器不拡散の根底にある問題は不拡散の責任が国際社会と国民国家から個々の研究者に移ったことである。これは主に、国際的にも、そし

provides rapid and sensitive COVID-19 detection," McGovern Institute, May 5, 2020, https://mcgovern.mit.edu/2020/05/05/sherlock-based-one-step-test-provides-rapid-and-sensitive-covid-19-detection/.

てアメリカのような諸大国において国内的にも妥協に至ることができなかった為である。伝統的な細菌兵器やウイルス兵器と関連したリスクは未だ存在するが、それと同時にグローバリゼーションと情報革命によって新しい技術開発はより多くの国家と非国家主体にとってアクセス可能なものとなり、比較的安価になった。

21 世紀において、技術的に活用可能な生物兵器の拡散を防ぐためには、必然的に物理科学や生命科学、医学、いくつかの工学コミュニティの関与を必要とする。バイオテクノロジーは多くの分野間を横断する可能性を持ち、本質的に学際的な分野へと発展してきた。特筆すべき例としては、DNA をカーボンナノチューブに結合させる活性複合体を使ったセンサーの開発である。これは電気工学者とコンピューター科学者が協力した例であり[16]、物理学と天文学の研究グループから派生したものである[17]。

社会科学もまた、技術的な観点に基づく不拡散の取り組みにより深く組み込まれる必要がある。そうでなければ技術を後追いする形になってしまうリスクがある。伝統的な学問分野のサイロ−文字通り「古い考え方」−によって研究を狭い範囲で区分けすることは、技術的・政策的アプローチを変革することをますます難しくしている。最先端の科学は基本的に学際的であり、その学際性は実行可能な政策を立案する際には厄介なもので、すでに頭を悩ませている問題をより複雑にしてしまう。

不拡散、対拡散のための柔軟なアプローチは、バイオテクノロジーを不正に応用するリスクを減らすのに重要な政策要素である。国際社会の性質や台頭するバイオテクノロジーの商用部門を無視した取り組み・政策は、現実社会に対してはますます不十分なものになっている。ある国家（またはテロリスト）が他の国家に

[16] C Dwyer, et al., “DNA Functionalized Singlewalled Carbon Nanotubes,” *Nanotechnology,* 2002, 13, pp 601-604.
[17] C Staii, M Chen, A Gelperin, AT Johnson, “DNA-decorated Carbon Nanotubes for Chemical Sensing,” *Nano Lett.* 2005, 5, pp 1774-1778.

対して生物兵器を用いるという問題は、危険な病原菌が致命的な結果をもたらすということが知られて以来懸念事項であった。しかし、生物兵器の脅威に対処する方法について取り上げた兵器抑止の研究はほとんどなく、バイオテロへの抑止についての研究はより限られている。生命科学と社会科学、実行可能な政策との間のギャップを埋めることは、生物兵器の不拡散と抑止を達成できるような実施・実行可能な戦略を生み出すうえで非常に重要である。同様に、不拡散の検証や国際軍備管理レジームは、21 世紀における戦略的抑止に対する新たなアプローチの一部として検討されうる。

国家によるバイオテクノロジーの悪用と生物兵器を拡散させる行為のリスクを低減させることは、バイオテクノロジーの研究開発における高度に国際的（transnational）な性質を考えることであり、これはポリティカル・サイエンスの研究者や科学者・技術者、その他専門家によって行われるだろう[18]。伝統的かつ革新的な、非拡散・対拡散への新しいアプローチを考えることは、技術の悪用のリスクを低減する上で重要な政策要素である。堅牢な国際協定は、テロリストが薬剤や前駆体、武器化された物質を手に入れる合法的な手段を排除し、これらが国家主体から盗用、欺瞞、またはその他の手段によって非国家主体へ渡る可能性を最小化することによって、テロリストによる悪用のリスクを低減させる。同時に、国際的なレジームを強化することによって、デュアルユース可能な物質や装備の移転をコントロールする取り組みも重要である。国家による生物（または化学）兵器の悪用のリスクを低減する上で、バイオテクノロジーの研究開発における高度に国際的な研究体制は大きな懸念事項である。狭い学術的な区分を伝統的な区分けに取り入れることは、生命科学とバイオテクノロジー分野における

[18] E.g., Kathryn Ibata-Aren, *Beyond Technonationalism: Biomedical Innovation and Entrepreneurship in Asia,* April 2019, Stanford University Press; Roselyn Hsueh, *China's Regulatory State: A New Strategy for Globalization,* Cornell University Press, 2011; Kathleen Vogel, *Phantom Menace or Looming Danger? A New Framework for Assessing Bioweapons Threats,* Johns Hopkins University Press, 2013; Kobi-Renee Leins, *International Law Applicable to the Use of Nanomaterials in War,* 2019, http://hdl.handle.net/11343/238667.

革新的な発展から最大限の利益を引き出しつつ、脅威を最小限にするための工夫を生み出す戦略や結果をさらに創造しづらくさせてしまうであろう。

JAPAN AND THE UNITED STATES NEED TECHNONATIONAL SECURITY AND STRATEGIC POLICIES TARGETING BIOMEDICAL INNOVATION IN ASIA

By Kathryn Ibata-Arens

On the morning of June 24, 2016, I was chatting with a Chinese colleague who advises the Chinese government on science and technology issues. Earlier that morning, the results of the Brexit vote in the United Kingdom had been announced: Britain was to leave the European Union. My colleague started our conversation by referencing the vote, saying "the world is being handed to us [the Chinese] on a silver platter." As isolationism and populism led Western powers to retreat from the world stage, China was embracing the global political economy and asserting a new leadership role in such multilateral organizations as the World Trade Organization and among the global corporate literati at the World Economic Forum in Davos.

This newfound assertiveness was long in coming. Beginning in the 1970s under Deng Xiaoping, the Chinese state began to use the Chinese diaspora for technonational strategic investments in core technologies, some of which were discussed in previous sessions of the Pacific Forum conference series, "21st Century Technologies, Geopolitics and the U.S.-Japan Alliance: Recognizing Game Changing Potential": artificial intelligence and biotechnology. A new term was coined for technologists who ventured out into the world to draw from the intellectual property resources of Western countries, particularly the United States. They were "techno-warriors" guided by a strategic vision of technonationalism.[1] Until this time, Japan had been known as the archetypical technonationalist state.

The term "technonationalism" was coined in 1983 by Nakayama Shigeru, who used it to refer to building national strength through science and technology independence.[2] Less known is

[1] Feigenbaum, Evan A. *China's techno-warriors: national security and strategic competition from the nuclear to the information age*. Stanford University Press, 2003. See also Cao, Cong. "Chinese Technonationalism." *Metascience* 13, no. 1 (2004): 71-74.
[2] Nakayama, Shigeru. "Science in Japan," *Nature* 305: 214-20.

that Japan styled its technonationalism (*kagaku gijtsu rikkoku* 科学技術立国) on strategic policies in China, dating back to the consolidation of political and economic power behind the rise of the first Qin dynasty (221 – 206 BCE). It seems that techno-nationalism has returned to its original home in China, stronger than ever.

In the 20th century, Japan, and Asian economies that emulated Japan, through incremental innovation of Western technologies in automobiles and electronics, gained global market share and began competing head-to-head with US industry. These countries often succeeded and then surpassed their US competitors, thanks in part to state policies targeting these sectors of the economy. These countries did so under a vision of what has been called technonationalism. Technonationalism equated national security with technology independence (from Western countries in particular). Here I lay out the Asian and global competitive landscape within which strategic investment policy pursued by Japan and the United States must navigate.

As Pacific Forum's Crystal Pryor outlined in the opening session of the "Game Changing" series, key for the United States-Japan partnership is setting global standards in disruptive game-changing technologies, building on our complementary strengths in certain foundational and critical discoveries. In the 21st century, competition is over emerging technologies, including biomedicine. The biomedical industry comprises mainly pharmaceuticals and medical devices. Compared to the 20th century, the competitive landscape is more populated, and includes rising competition from China and India. Like Japan, such countries as China, India, and South Korea have made a strategic bet on biomedicals and have invested at the national level in stimulating innovation and entrepreneurship at the technological frontier.

Why biomedicals? First, as early as 2014 global revenue exceeded $2 trillion, while the global market for biomedical products had grown to surpass $10 trillion.[3] Second, global healthcare expenditure had risen to 10 percent of GDP and is expected to remain high. To date, more than half of global revenue in biomedicals is generated in the United States and Europe. Future growth is forecast to be driven by market opportunities in Asia. Further, it became evident

[3] "2015 Global life sciences outlook: adapting in an era of transformation," Deloitte Touche Tohmatsu Limited, 2014. See also "2020 Global life sciences outlook: creating new value, building blocks for the future," *Deloitte Insights*, 2020.

during the 2020 global race to develop a workable COVID-19 vaccine that much of the manufacturing capacity and control over the global supply of essential pharmaceutical active ingredients was held by China.

Consequently, the biomedical industry has become the "next big thing" for countries, promising global market dominance and the chance to set a generation of international industry standards. As a result of this fierce competition, national governments have turned to new technonational solutions. What is "new" about this technonationalism?

The challenge for Japan in the context of its Asian competitors is what I call "the Janus Paradox." The Janus Paradox is an analogy I developed that is inspired by the Roman God of gateways. The temple Janus is open only during times of war. Its god, Janus, has two faces. One looks out, open and engaged to the outside world. The other is turned in, closed to and protecting against that outside world. The paradox is that competing nation-states are compelled to be both open and exposed to draw technology and capital resources from the global economy, yet closed and protective of the domestic economy to nurture nascent entrepreneurs and innovators building technonational strength.

Japan's competitors in Asia, including China and India, have through their diaspora human capital and sometimes industrial espionage networks mastered the Janus Paradox. China in particular has made strategic investments in biotechnology, bio-pharmaceuticals, and medical devices and diagnostics in an explicit goal of setting global standards as they have done in such technologies as 5G and artificial intelligence.

Here is an example of how China has mastered the Janus Paradox. The Human Genome Project (HGP) was an open-source science initiative bankrolled mainly by the United States National Institutes of Health and Department of Energy from 1990 to 2003. Country teams from the US, UK, France, Germany, Japan, and China collaborated and competed in team "nodes" to map the entire human genome. China's team was able to use the HGP platform to map its assigned part months ahead of schedule. Japan, on the other hand, fell behind. Japanese scientists later said that "Japan had failed to establish a unified national program due to

bureaucratic sectionalism." [4] In other words, the inter-ministerial factionalism that has characterized Japanese innovation policies held Japan back on the global stage.

Meanwhile, in China, members of the HGP team went on to launch the venture company BGI (Beijing Genomics Institute), which has since moved to Shenzen, China. BGI is known for quickly mapping the SARS genome in 2003, which was critical in the development of diagnostics and treatments for that epidemic of severe acute respiratory syndrome.

The novel coronavirus is called SARS-CoV-2 as its genomic structure is very close to the 2003 SARS virus. So, connecting the dots from 1990 to 2020: First, in the 1990s China joins the Human Genome Project. Second, by 2003, it applies technology advancements drawn from the open innovation platform to its domestic human health crisis of SARS. Third, in 2020, when SARS2 hit, China's Janus face pivots to the outside, parlaying its COVID-19 vaccine discovery. China's manufacturing and global supply chain connectivity has enabled it to engage in global health diplomacy on a scale no other country has ever been able. But, significantly, this diplomacy was strategically deployed. Countries on the western frontier of the Belt and Road (BRI) infrastructure initiative -- Iran and Italy -- were the first to benefit by receiving personal protective equipment (PPE) and COVID-19 diagnostics.

Key to the new technonationalism in Asia is harnessing international diaspora networks. Japan defines its diaspora as "Nikkei" or all Japanese people who have relocated overseas on a permanent basis, including their descendants. By 2014, Japan's global diaspora numbered 3.5 million people. In contrast, conservative estimates indicate that India had 25 million and China at least 50 million. Those countries -- China in 1978 and India in 2004 -- established national units devoted to engaging with their global diaspora talent. Even Singapore, which has explicitly emulated Japan's developmental state, also established a national agency to engage foreign and diaspora talent (1998), even though its diaspora consists of a few hundred thousand. Viewing these trends through the lens of biomedical innovators and entrepreneurs, it is clear how the new networked technonationalism at the state level translates into innovation at the firm level.

[4] Sakaki, Yoshiyuki. "A Japanese history of the human genome project." *Proceedings of the Japan Academy, Series B* 95, no. 8 (2019): 441-458.

What has changed for Japan since the 1990s? First and foremost is the economic rise of China. This has come with an increase in economic participation at all levels, including high-growth new firm ventures with global reach. Rapid growth in China, followed by India, in part inspired the research for my current book on innovation in new drug discovery.[5] In this regard, Japan stands out for its leadership in global health diplomacy, which I examine below.

In *Beyond Technonationalism: biomedical innovation and entrepreneurship in Asia,* I explore connections between innovation capacity and entrepreneurial ecosystem development in China, India, Japan, and Singapore.[6] In *Beyond Technonationalism*, I propose a new framework of "networked technonationalism" to explain how countries have adopted a quasi-open, yet fundamentally technonationalist stance, in pursuing developmental goals. These countries harness global diaspora networks to make technology investments and entrepreneurial gains in the domestic economy.

What must be done to improve Japan's strategic innovation, and maintain leadership at the technological frontier? First, it should build on existing international network connections. An example discussed in *Beyond Technonationalism* are the US connections behind Japanese stem cell scientist and entrepreneur Yamanaka Shinya's research that led to the Nobel Prize-recognized innovations in iPS "induced pluripotent stem cells" that he and hundreds of lab members have since continued at Kyoto University. Similar dynamics can be found in cases of Japanese entrepreneurs in Singapore and on a much larger scale with Chinese diaspora returnees, known affectionately in China as *hai gui* (a homonym with "sea turtle"). The US has been the beneficiary of global diaspora talent, enhancing our US innovation and entrepreneurial ecosystems, even if these researchers eventually return "home," reinforcing international network synergies.

[5] Bosma, Niels, Stephen Hill, Aileen Ionescu-Somers, Donna Kelley, Jonathan Levie, and A. Tarnawa. "Global Entrepreneurship Monitor 2019/2020 Global Report." *Global Entrepreneurship Research Association, London Business School* (2020).
[6] Ibata-Arens, Kathryn C. *Beyond Technonationalism: Biomedical Innovation and Entrepreneurship in Asia*. Stanford University Press, 2019.

Building on international connections includes embracing international, foreign, and diaspora networks. While Japan will never be able to compete with the Chinese and Indians in sheer quantity of work and workers, it can compete on quality. Japan has many gems to be found in frontier science and technology (S&T) innovation capacity, as is demonstrated by the Kyoto University researchers in stem cells. In hindsight, it is clear that the 2012 Nobel Prize award to Yamanaka became a watershed moment for Japan's global science and technology policy. Japan's Temple Janus was open for business and it launched a series of new disruptive initiatives in biomedical innovation. In addition to providing more government funds for stem cell research (2012) and the launch in early-2013 of a new investment fund (discussed below), government officials began deliberating by mid-2013 the idea for a new agency. These and other initiatives culminated in the creation by 2015 of the Agency for Medical Research and Development (AMED). AMED was backed with government seed-funding of about $1.2 billion. AMED was modelled on the much larger roughly $30 billion-dollar National Institutes of Health (NIH). In 2015 Japan also launched a package of initiatives, dubbed the "Sakigake" （先駆けパッケージ戦略） to fast-track research and development in "pioneering" Japanese innovations in regenerative medicine and pharmaceuticals.[7]

Japan has launched other game-changing initiatives. Japan's public-private partnership Global Health Innovation Technology Fund (GHIT) was launched in 2013. GHIT is a joint effort in new drug discovery between partners that include leading Japanese pharmaceutical companies (Estellas, Eisai, Takeda), the Ministry of Health, Labor, and Welfare, and the Gates Foundation. I explore GHIT and other emergent organizations in new drug discovery in Japan and other countries in Asia in *Medicine in an Age of Pandemics: why the global innovation system is broken and how we can fix it.* In it, I offer a case study of Japan's recent disruptive emergent organizations. Instead of focusing on the domestic environment, the drugs and diagnostics under development in what I call innovation *sandboxes* and intellectual property *pools* would be for so-called neglected tropical diseases in the developing world. GHIT's globally connected international board would add synergies to the strong biomedical intellectual property held in Japan. Its innovation architecture took into account inter-ministerial factionalism – and surmounted it.

[7] 先駆けパッケージ戦略～革新的医薬品等の実用化促進～. Accessed October 26, 2020. https://www.mhlw.go.jp/seisakunitsuite/bunya/kenkou_iryou/iyakuhin/topics/tp140729-01.html,.

In the United States, strategic investment policies partnered with Japan's emerging game-changing technologies and exceptional scientific talent could, and should, build on past success. Together, Japan and the United States are poised to extend their strong bilateral security, investment, and trade partnership to a pan Asian and American innovation and entrepreneurial ecosystem.

日米が必要としているアジアにおけるバイオメディカル分野でのイノベーションのための技術国家安全保障と戦略的政策

キャサリン イバタ-アレンス

2016 年 6 月 24 日の朝、私は中国政府に科学技術的課題について助言を行っている中国人の同僚と話していた。その日の朝早く、ブレクジッドの是非を問うイギリスの国民投票の結果が発表された：イギリスが EU を離脱するという。選挙結果にふれながら、同僚は会話をこんな言葉で初めた：「世界は銀の大皿に乗って我々（中国人）に手渡されつつある。」孤立主義とポピュリズムによって西側の大国が世界の舞台から退場する中、中国はグローバルな政治経済を取り込み、世界貿易機関のような国際機関やダボスの世界経済フォーラムにおけるグローバル企業の知識人の中で、新たな指導的役割を主張している。

このような新たな主張はかなり前から行われていた。鄧小平指導下の 1970 年代初めから、中国はコア技術へのテクノナショナルな戦略投資のために中国人ディアスポラ(Chinese diaspora)を活用するようになった。これらコア技術のうちのいくつかは先日のパシフィック・フォーラムの「21 世紀における技術、地政学、そして日米安全保障条約：潜在的なゲームチェンジャーを考える」においても議論された人工知能とバイオテクノロジーである。米国を中心とした欧米諸国の知的財産を利用して、世界に打って出た技術者を表すための新しい言葉が生み出された。彼らはテクノ・ナショナリズムの戦略的ビジョンに導かれた「科学技術戦士(techno-warriors)」であった[1]。これまで日本は、典型的な科学技術立国として知られていた。

[1] Feigenbaum, Evan A. *China's techno-warriors: national security and strategic competition from the nuclear to the information age*. Stanford University Press, 2003. See also Cao, Cong. "Chinese Technonationalism." *Metascience* 13, no. 1 (2004): 71-74.

「テクノ・ナショナリズム」という言葉は 1983 年に中山茂によって造られ、科学と技術の独立性によって国力の増強を図るという意味で用いられた[2]。あまり知られてはいないが、日本はそのテクノ・ナショナリズム(科学技術立国)を、中国の戦略政策、それも秦朝（紀元前 221-206）の台頭の背後にあった、政治と経済力の統合にならって構築した。今日、テクノ・ナショナリズムは、かつてないほどの強力な形で、発祥地である中国に戻ってきたようである。

20 世紀に入ってから、日本や日本に倣ったアジア諸国は、自動車やエレクトロニクス分野における欧米技術の数々の漸次的なイノベーションを通じて、世界市場のシェアを獲得し米国産業界と競い合うようになった。これらの国々はしばしば成功し、米国の競合他社を凌駕したが、それは幾分かこれらの産業分野に焦点を当てた政府の政策の結果でもあった。これらの国々はテクノ・ナショナリズムと呼ばれるビジョンの下でこのような政策を行った。テクノ・ナショナリズムは、（特に欧米諸国からの）国家安全保障を技術的独立と同一視した。本稿では、アジアとグローバルな競争の展望と、その中で日本と米国がどのような戦略的投資政策を採っていくべきかを示す。

パシフィック・フォーラムのクリスタル・プライアー氏が「ゲームチェンジング」シリーズのオープニング・セッションで概説したように、基礎的かつ重要な発見における私たちの補完的な強みに基づいて、既存の価値基準を打ち砕くようなゲームチェンジング技術の国際基準を確立することは日米間のパートナーシップにとって重要である。21 世紀においては、バイオメディカル等の新興技術にまで、競争が激化している。バイオメディカル産業は主に医薬品及び医療機器によって構成される。20 世紀と比較すると、中国とインドからの参入者も増え、一層競争が激しくなった。中国、インド及び韓国は日本のようにバイオメディカル分野に

[2] Nakayama, Shigeru. “Science in Japan,” *Nature* 305: 214-20.

戦略的な期待を持ち、技術の最前線においてイノベーションと起業家精神を刺激するために、国家レベルで投資を行ってきた。

何故バイオメディカル分野なのかについてだが、第一に、当該分野は早くも 2014 年の時点で全世界の収益が 2 兆ドルを超え、バイオメディカル製品の市場は全世界で 10 兆ドルを超えるまでに成長していた[3]。第二に、世界の医療費は GDP の 10%にまで上昇し、今後も高い水準で推移していくと予想されている。今日に至るまで、全世界のバイオメディカルにおける収益の半数は、米国とヨーロッパにおいて生み出されてきた。だが今後の当該分野の成長は、アジアにおける市場機会に牽引されると予想されている。さらに、COVID-19 のワクチン開発における各国の競争の中で、製造能力の多くと重要な原薬の国際供給の管理を中国が担っていることが明らかになった。

その結果、バイオメディカル産業は各国にとって、国際市場における優位性と、新たな国際業界標準を設定する機会を授ける、「次なる大きなもの（next big thing）」となった。この激しい競争の結果、各国政府は新たなテクノ・ナショナルな発明に目を向けるようになった。

それでは、このテクノ・ナショナリズムにおける「新しさ」とは何だろうか。

アジアの競争相手が現れている状況の中で日本の課題としては、私が「ヤヌスのパラドックス（“the Janus Paradox”）」と呼んでいるものがある。ヤヌスのパラドックスとは、ローマ神話の扉の守護神から着想を得て私が考えたアナロジーである。ヤヌス神殿の門は戦時にしか開かない。神ヤヌスは二つの顔を持っており、その一つは外側を向いていて、外側の世界に対して開かれ関わりを持っている。もう一方は内側を向いており、外側の世界から閉じ自らを守っている。ヤヌスの

[3] “2015 Global life sciences outlook: adapting in an era of transformation,” Deloitte Touche Tohmatsu Limited, 2014. See also “2020 Global life sciences outlook: creating new value, building blocks for the future,” *Deloitte Insights*, 2020.

パラドックスとは、グローバル経済から技術と資本を得るために、競合する国民国家は開放的で国際競争にさらされなくてはならないが、それと同時に、テクノ・ナショナルな強靭性を構築する駆け出しの起業家やイノベーターを育てるため、国内経済を閉鎖的・保護的にすることを余儀なくされる、ということを指す。

中国とインドを含むアジアにおける日本の競合相手は、各国に存在する彼らの人的資源と、時には産業スパイ活動のネットワークを用いてこのヤヌスのパラドックスを克服してきた。特に中国は５G や人工知能などの技術分野において行ってきたように、国際基準を設定するという明確な目的を掲げて、バイオテクノロジー、バイオ医薬品、医療機器・診断などの分野に戦略的投資を行ってきた。

以下は中国がどのようにしてヤヌスのパラドックスを克服したのかについての一例である。

ヒトゲノム計画（HGP）は 1990 年から 2003 年にかけて、主に米国国立衛生研究所（National Institutes of Health）とエネルギー省（Department of Energy）から資金提供を受けて行われたオープンソースサイエンスの取り組みであった。米国、イギリス、フランス、ドイツ、日本、中国からの各国のチームが協力し、ヒトゲノム全体をマッピングするための「ノード」をチームごとに競い合った。中国のチームはHGPのプラットフォームを使用して、割り当てられた箇所を予定よりも数か月も早くマッピングすることができた。一方で、日本は後れを取った。後に日本の科学者は「日本は官僚的な縦割りシステムのために、国家レベルで統合されたプログラムの立ち上げに失敗した」と語った[4]。言葉を変えれば、日本のイノベーション政策を特徴づけてきた省庁間縦割りが、世界の舞台において日本の足を引っ張ったのである。

[4] Sakaki, Yoshiyuki. "A Japanese history of the human genome project." *Proceedings of the Japan Academy, Series B* 95, no. 8 (2019): 441-458.

一方で中国は、HGP のメンバーがベンチャー企業である BGI（Beijing Genomics Institute）を設立した（これは後に中国の深圳に移転された）。BGI は 2003 年に、SARS のゲノムを迅速にマッピングしたことで知られており、感染が拡大した SARS の診断法や治療法の開発に重大な役割を担った。

新型コロナウイルスは、2003 年の SARS ウイルスとゲノム構造が非常に近いことから、SARS-CoV-2 と呼ばれている。それでは、1990 年から 2020 年までを時系列で見ていこう：第一に 1990 年代、中国はヒトゲノム計画に参加した。第二に、2003 年までにはオープンイノベーションプラットフォームから得た技術発展を国内の健康危機であった SARS に応用した。第三に 2020 年、SARS２が襲った時、COVID-19 のワクチン開発を最大限利用して、中国のヤヌスの顔は外側を向いた。中国の製造業及び世界中とつながったサプライチェーンの連結性によって、中国は今までどの国もできなかったような規模で、保健外交（health diplomacy）を世界的に展開することが出来た。しかし重要なのは、この外交政策は戦略的に展開されたものである点だ。一帯一路政策（BRI）の最西端に位置するイランとイタリアは中国から個人用防護具（PPE）と COVID-19 診断キットを最初に受け取り、その恩恵を受けた。

アジアにおける新たなテクノ・ナショナリズムの鍵となるのは国際的なディアスポラのネットワークを活用することである。日本におけるディアスポラは「日系人」、即ち海外に永住した日本人とその子孫を指す。2014 年までに、世界における日本のディアスポラは 350 万人に上る。一方で、控えめに見積もってもインドのディアスポラは 2500 万人、中国は少なくとも 5000 万人に上るとされている。これらの国々は世界中に点在する彼らのディアスポラを活用するための国際団体を（中国は 1978 年、インドは 2004 年に）設立した。日本の発展に倣ったシンガポールでさえ、数十万人程のディアスポラしかいないにも関わらず、有能な外国人やディアスポラを活かすための国家機関を 1998 年に設立した。このような傾向をバイオメディカル分野のイノベーターや起業家の視点で見れば、国家レベルの

新たなテクノ・ナショナリズムのネットワークが、いかに企業レベルでのイノベーションに活かされているかは明らかである。

1990 年代以降、日本にとって何が変わったのか。何よりも第一に中国の経済的台頭である。これはグローバルに展開し急成長している新たなベンチャー企業を含め、あらゆるレベルで経済への参入が増加したことと関係している。急成長する中国に続くインドの成長は、新薬開発におけるイノベーションに関する、私の著作にもヒントを与えてくれた[5]。この意味で、以下に示すとおり日本はその世界的な保健外交におけるリーダーシップという点において抜きんでている。

著書「テクノ・ナショナリズムを超えて：アジアにおけるバイオメディカルイノベーションと起業家精神」(*Beyond Technonationalism: biomedical innovation and entrepreneurship in Asia*)において私は、中国、インド、日本、そしてシンガポールにおけるイノベーション能力と、起業家のエコシステムの発達との間にどのような関係があるかを考察した[6]。そして当著書において、開発目標を追求する中で、各国がいかに半開放的であり、それでいて基本的にはテクノ・ナショナリストのスタンスを採ってきたかを説明するため、「ネットワーク化されたテクノ・ナショナリズム」という新たな枠組みを私は提唱している。これらの国々は国内経済に技術的投資と起業家的利益をもたらすために国際的なディアスポラのネットワークを利用しているのである。

日本の戦略的イノベーションを向上させ、科学技術の最前線におけるリーダーシップを維持させるために、何をすべきか。第一に、既存の国際的なネットワークの繋がりを強化することである。先に示した著書では、日本の幹細胞研究者で起

[5] Bosma, Niels, Stephen Hill, Aileen Ionescu-Somers, Donna Kelley, Jonathan Levie, and A. Tarnawa. "Global Entrepreneurship Monitor 2019/2020 Global Report." *Global Entrepreneurship Research Association, London Business School* (2020).
[6] Ibata-Arens, Kathryn C. *Beyond Technonationalism: Biomedical Innovation and Entrepreneurship in Asia*. Stanford University Press, 2019.

業家である山中伸弥氏の研究を支えた米国との関係を一例としてあげた。ノーベル賞に輝いたこの iPS「人工多能性幹細胞」のイノベーションは、京都大学において彼と数百人もの研究室のメンバーによって続けられてきたものだった。同様のダイナミクスはシンガポールにおける日本人起業家の例や、よりスケールの大きな例としては、中国で hai gui（中国語の「海亀」とかけている）として親しまれている海外から中国に帰国した人材にもみられる。米国は国際的なディアスポラ人材の恩恵を受けており、米国におけるイノベーションと起業家のエコシステムを強化し、最終的に彼らが「祖国」へ帰ったとしても、さらなる国際的なネットワークの相乗効果を生み出している。

国際的な繋がりを構築することは、国際的なネットワーク、外国人ネットワーク、ディアスポラのネットワークの活用を含む。日本は中国人やインド人に対して、仕事量や労働者の数においては決して太刀打ちできないが、質の面では競合することができる。幹細胞研究における京都大学の研究者に代表されるように、日本は科学技術（S&T）分野の最前線において、多くの可能性を有している。今振り返ると、2012 年の山中教授のノーベル賞受賞が、日本のグローバルな科学技術政策の分水嶺であったことは明らかである。日本のヤヌス神殿はビジネスに門戸を開き、バイオメディカル分野のイノベーションにおける革新的な一連の取り組みを開始した。幹細胞研究のためにより多くの政府予算を配分し（2012 年）、2013 年の初頭に（後述するように）新たな投資ファンドを立ち上げただけでなく、政府関係者は 2013 年半ばまでには新たな機関の構想を開始した。これら取り組みとその他イニチアチブは 2015 年に頂点に達し、日本医療研究開発機構（Agency for Medical Research and Development: AMED）が設立された。AMED は政府による約 12 億ドルの設立資金援助を受けた。はるかに大規模な約 300 億ドルの予算を持つ米国国立衛生研究所（NIH）をモデルとして AMED は創設された。また 2015 年には、再生医療と製薬における「先駆的な」日本のイノベーションを迅速に研究・

開発するための、「先駆けパッケージ戦略」と名付けられた一連の取り組みを開始した[7]。

日本はその他にも画期的な取り組みを立ち上げている。2013 年には官民パートナーシップであるグローバルヘルス技術振興基金（Global Health Innovation Technology Fund: GHIT）が設立された。GHIT は、日本を代表する製薬会社（アステラス製薬、エーザイ、武田薬品工業）や、厚生労働省、ビル&メリンダ・ゲイツ財団等による新薬の共同開発の取り組みである。私は「パンデミック時代の医学：なぜ国際的なイノベーションシステムは破綻しているのか、そしてどうすれば改善できるのか」（*Medicine in an Age of Pandemics: why the global innovation system is broken and how we can fix it*）において、日本やアジアにおける新薬開発のための新興機関と GHIT を調査した。その中で私は、近年の日本における革新的な新興機関に関するケーススタディを紹介している。国内の環境に目を向けるのではなく、私がイノベーションのサンドボックス (sandboxes)と呼んでいるものや、知的財産のプール (pool)における開発途中の新薬・診断法は、発展途上国における「顧みられない熱帯病（neglected tropical diseases）」と呼ばれる病のためになるだろう。国際的な関係を有する GHIT の国際委員会は、日本に存在する優れたバイオメディカルの知的財産に更なる相乗効果をもたらすだろう。GHIT のイノベーション構造は省庁間の縦割りを考慮したうえで、それを克服したのである。

米国において、戦略的な投資政策と日本で生まれている革新的技術や並外れた科学人材とを合わせることで
更なる成功を築くことが可能でありまた望ましい。日本と米国は、これまでの安全保障、投資、貿易のパートナーシップから、全アジア・アメリカのイノベーションと起業家のエコシステムにまで、その強力な二国間関係を拡大する準備が十分にできている。

[7] 先駆けパッケージ戦略～革新的医薬品等の実用化促進～. Accessed October 26, 2020. https://www.mhlw.go.jp/seisakunitsuite/bunya/kenkou_iryou/iyakuhin/topics/tp140729-01.html,.

A DIGITAL FABRICATION PERSPECTIVE: REFLECTING ON THE PAST DECADE OF THE 'MAKER MOVEMENT' DIGITAL FABRICATION ECOSYSTEM AND ESTIMATING POTENTIAL FUTURES

By Keisuke Inoue

Executive Summary

3D printing and digital fabrication have brought massive changes to the production process over the past 10 years. The so-called democratization of manufacturing – supported by improvements in internet infrastructure and new intellectual property rights, such as open source and creative commons – has permeated all layers of life, from the personal to the industrial to the educational and governmental use of technologies.

History tells us that huge innovation will bring new risks, and digital fabrication is no exception. Concrete methods for risk management is required for this new technology after a decade of democratization. While digital fabrication users are both amateurs and professionals, both manufacturers and consumers need industrial institutions and literacy.

This presentation and accompanying paper will summarize the past decade of improvements in digital fabrication industry and aim to theorize on practical uses in the near future.

Looking back on the decade called Maker Movement (in the 2000s)

The history of 3D printers began with the invention of stereolithography[1] by Hideo Kodama at the Nagoya Municipal Industrial Research Institute in 1980. The early 3D printing industry was driven by leading companies such as 3D Systems and Stratasys, which continue to do so today. However, the implementation cost was high and unmanageable to the general public. In the late 2000s, as the basic patent protection period for 3D printing expired, various manufacturers began to sell inexpensive 3D printers. As of 2020, you can buy a 3D printer for less than $200 and build your own "desktop factory."

[1] https://ja.wikipedia.org/wiki/%E5%B0%8F%E7%8E%89%E7%A7%80%E7%94%B7

The 2000s laid the groundwork for the current "maker movement." Information infrastructure centered on the Internet developed and various information became sharable. The open-source model is a concept originally used in the fields of software development and programming. By being able to upload not only text but also information in various formats to the server, it became possible to share blueprints, schematics, or 3D data itself. Without such developments, hardware like 3D printers would not have been open-sourced.[2]

The Internet not only encouraged the development of 3D printers, but also encouraged users to share information. 3D data created by users all over the world are uploaded to 3D data sharing sites[3] such as Thingiverse and GrabCAD. On video sharing sites like YouTube, one can find many tutorials on creating 3D data and using 3D printers, reviews of new products, and so forth. Forums and SNS groups that are useful for exchanging opinions and troubleshooting also evolved in various languages. Although the quality of information varies, one can measure the current maker movement's enthusiasm from these exchanges on the Internet.

Fab Lab[4] was born from the practical connection of these features of the Internet and manufacturing. By opening the workshop equipped with various digital fabrications[5] such as 3D printers to the public, they aimed to share the issues in each region and solve them with the knowledge available throughout the world. They showed a way to solve individual problems by creating them themselves, especially in areas where physical infrastructure is not available. Because it is a digital fabrication that operates machine tools directly from digital data, exchanging data between Fab Labs via the Internet and share deliverables became possible.

[2] The RepRap project is considered one of the representative efforts of open-source hardware and has had a significant influence on developing the underdeveloped fused filament fabrication (FFF) 3D printer. https://reprap.org/wiki/RepRap
[3] https://www.thingiverse.com/ https://grabcad.com/
[4] https://fablabs.io/
[5] Industrial machine tools that operate and process digital data, such as machining centers and CNC routers, are already commonly used. Civilians have widely used industrial machine tools that have been used in such a closed environment through the maker movement, and the name "digital fabrication" has come to be used as a whole.

The essential advantage of digital is that it can be stored and duplicated without sacrificing quality. While this advantage has brought many benefits, it has created new challenges in terms of copyright protection. Under such circumstances, Creative Commons [6] significantly influenced the maker movement as an extremely democratic and constructive system in which the creators themselves can decide how to share.

The Internet is not the only foundation behind the maker movement.

Just like sharing information on the Internet, the sharing economy allowed one to share work and workspaces to equipment and human resources. Workshops that are open to the public are not limited to Fab Labs but have appeared in various operating forms (these workshops are generally called makerspace.) TechShop, which was founded in California in 2006, has since expanded to 10 workshops in the United States and has become a representative makerspace while expanding licenses overseas. The HAXLR8R (later renamed HAX), which was founded in Shenzhen, China, in 2012, has come to symbolize today's Shenzhen, a makerspace hub specializing in hardware startups.

Maker Faire,[7] which was first held in California, the USA, in 2006, has since been held worldwide as an event where makers from all over the region gather. The large-scale Maker Faire has become a symbol of the maker movement, with more than 100,000 people attending in just a few days. The emergence of an offline event like Maker Faire that anyone can easily attend has motivated the makers themselves. Moreover, as it grows in size, it became not only a gathering of hobbyists, but also worked as a trade fair for startups.

Looking back on the decade called Maker Movement (in the early 2010s)

As I mentioned, not only technological developments such as equipment and information infrastructure, but various factors that permeated in the 2000s, such as legal systems, values, and community formation of creators, laid the foundation for the current maker movement. As we entered the 2010s, the number of inexpensive 3D printers that are easy for general consumers to purchase has increased, and it has become popular in the media as a "revolution

[6] https://creativecommons.org/
[7] https://makerfaire.com/

in the manufacturing industry." Until then, 3D printing technology, which had been used in the polarized area, in the laboratories of large companies and universities, or DIY by individuals, has permeated the middle class such as small and medium-sized manufacturing industries, designers, and educational institutions.

At the same time, government agencies in each country also actively launched various support measures to support the utilization of new technologies. The startup support measure "French Tech," which was launched in 2013, has since created and attracted many startup companies within France and abroad.[8] In 2014, Maker Faire, as mentioned above, was held at the White House in the United States, and many implementation support measures were initiated, especially for educational institutions, to improve the competitiveness of the next-generation manufacturing industry.[9] The "Mass Entrepreneurship/Innovation by all" that started in China in 2015 is also a measure to support domestic startups and encourage innovation. In China, which has led the economy in a top-down manner under a huge bureaucracy, many start-up companies centered in Shenzhen were born through measures that can be described to be rather bottom-up.[10] As concrete efforts for new manufacturing technology are being promoted in each country, many maker spaces have been created in the private sector. The rise of the maker movement peaked in the first half of 2010 at all levels industry, government, academia, and the private sector.

Looking back on the decade called Maker Movement (in the late 2010s)

Fab Lab Kanda Nishikicho (formerly Fab Lab Shibuya), which I run, was born in 2012 as the third Fab Lab in Japan during such prosperity, and I have seen the trends of the maker movement to date from the perspective of an industry insider. In the late 2010s, the maker movement as a trend began to settle down, and success are failure started to appear in maker spaces, startups, and administrative measures in each country. No matter how fascinating the technology is, it is not a magical tool that promises success, and there are numerous failures behind spectacular success stories. News such as Techshop's bankruptcy filing (2017), the company I mentioned earlier, and Maker Media's suspension of operations (2019), which hosts

[8] https://lafrenchtech.com/en/
[9] https://makezine.com/2014/06/18/white-house-maker-faire-fact-sheet-has-been-released/
[10] https://spc.jst.go.jp/experiences/studylife/studylife_1910.html

Maker Faire in the United States, have shocked the maker community in no small measure. Also, hardware startups weren't born, unlike the dot-com bubble which created many IT startups. Even if ideas and working prototypes can be formed, completely different technologies are required for stable mass production. The high cost of mass production has made financing more difficult. Compared to software, it takes more time to develop, and it is not easy to change specifications. Human skills and technology have not caught up enough to solve these hardware-specific difficulties.

The late 2010s is positioned as the maker movement's maturity stage, where only select services remain while many services are eliminated. The trend of dazzlingly eliminated cases seem dark, but there are many cases of correct understanding of new technologies and adaptation to a changing society. In particular, the area of 3D printing is steadily taking root in society without being influenced by the rise and fall of the movement.[11]

The future led by 3D printing

After the Industrial Revolution, manufacturing technology evolved into a more systematic production system, resulting in a mass production/mass consumption society. This significant change in human history has enriched society. However, by the second half of the 20th century, it was seen as the main cause of rapid environmental destruction, and questions about the implications of affluence were raised. It may seem contradictory but digital fabrication, which has the advantage of preservation and replication, can alter the mass production/mass consumption production system.

First, data can be stored at a meager cost and with a low environmental load compared to the storage of material substances. If we can produce the required amount when necessitated, we could suppress excess production, and the seller will not bear the burden of inventory. For the new cycle of mass production/mass consumption, digital fabrication can be a means to enable "appropriate production/consumption."

[11] https://www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html?gclid=CjwKCAiAqJn9BRB0EiwAJ1Sztb4s0VHPGIqIP-y79e4rslj0sAZJM10iCMxTMv5hPUz5v320jMXkwhoCv2AQAvD_BwE

Second, many digital fabrications, including 3D printers, are not suitable for mass processing in a short time in the first place. Instead, its advantage is that it can expand into different variations with only minor changes to the data. Digital fabrication is beginning to be used as a practical means to meet diversifying consumer needs, such as "small quantity and wide variety" and "mass customization."[12] In addition, the manufacturing process of equipment for medical and professional sports, which required made-to-order, is digitized as the 3D scanning technology improves.

Third, it is used more and more by taking advantage of the high degree of freedom in shape that 3D printers can achieve. In most cases, 3D printing is possible even for shapes that cannot be formed by conventional manufacturing methods. Shapes that had to be divided into manufacturable shapes by the conventional manufacturing method can now be output as a single unit to omit the assembly process. Another significant advantage is that the cost of 3D printing is proportional to "volume" and is not easily affected by "shape complexity." In the past, it was essential to have an "easy-to-make shape" in order to reduce manufacturing costs. However, by replacing it with a quantified index such as "volume," introducing a new design process called generative design has progressed.[13] Since the volume and weight are proportional to each other, if the same material is used, the material cost can be decreased by designing a part to have the smallest possible volume (= lightweight) while maintaining its strength. Furthermore, the weight reduction of materials in the aerospace industry will lead to a reduction of operating costs and environmental load.[14]

---

[12] "Loft & Fab," which I operate in collaboration with Loft Co., Ltd., has been operating since November 2013 as a maker space specializing in mass customization. The store is equipped with facilities for shoppers to customize the products purchased at Loft freely, and staff assists the shoppers in shaping their ideas. http://andfab.jp/

[13] Generative design is a design method that allows the computer itself to design a shape that satisfies a specific constraint or condition that has been input and automatically derives multiple solutions. With the development of 3D printing technology, it is one of the fields that 3D CAD design software makers focus on developing. https://en.wikipedia.org/wiki/Generative_design

[14] Boeing is a company that is actively adopting 3D printing technology. The GE9X engine installed in the new 777X, connected to the 777 series, is equipped with more than 300 3D printed parts, achieving low fuel consumption and high thrust. The engine has already obtained FAA certification and is taking the first step towards mass production. In addition, the company has recently announced that it will open a 3D printing research and development facility in Scotland, and is actively investing in this technology. https://www.boeing.com/features/innovation-quarterly/2019_q4/btj-additive-manufacturing.page https://www.geaviation.com/commercial/engines/ge9x-commercial-aircraft-engine

Although its use in consumer products is still limited[15] due to high material costs and low production speed, development competition in the 3D printing industry is still heating up. Not only the development of the printer itself but also the development of materials is developing. New materials with various added values are being created one after another. There is also an increasing momentum for new products to be created by 3D printing, rather than as a substitute for conventional manufacturing methods. As the material can be supplied reliably and as its cost decreases, the utilization version will gradually spread. The 3D printer craze that broke out in many media in the early 2010s has subsided, but the progress has been much better since then, and there is still no sign that it will decrease.

Consideration on 3D printing and distribution

3D printers are currently roughly divided into inexpensive models for hobbyists and small businesses, and expensive models for the manufacturing industry. In either case, the production speed is slower compared to the conventional manufacturing technology, and at least as of now, it is not a substitute for injection molding machines. However, that is the case when looking at the equipment alone, and the situation is different when a large number of 3D printers are operated at the same time. Unlike injection molding machines, 3D printers that do not require expensive "molds" are easy to operate by arranging multiple printers parallel to one another. In fact, there are factories with dozens or hundreds of 3D printers lined up.[16] As a production system that utilizes 3D printers, such parallelization has great merits. Since the whole production can be operated with a small number of people and the initial cost of "mold" is not required, there is no lower limit to production. Different data can be handled in much the same way, and equipment can be set up at low labor costs. The 3D printing mega factory, which has strengths in on-demand production, will continue to be deployed according to needs.

On the other hand, such a "mega-factory conversion" has not been able to break away from the conventional mass production/mass consumption model from the viewpoint of

[15] Sports apparel brands such as Nike, Adidas, and Under Armor have already released consumer products that print the sole of sneakers with 3D printers. Some companies manufacture and sell prosthetics such as artificial arms and artificial legs with 3D printers.

[16] The on-demand 3D printing factory "Redeye," which Stratasys has been operating since 2005, is the world's largest 3D printer factory equipped with more than 100 industrial 3D printers. (Currently integrated into Stratasys Direct Manufacturing.) For more information on Redeye, see the following press documents. https://www.bbc.com/news/av/technology-25101388

transportation costs. It is better to send the data close to the product's consumption destination and produce it there so that the effect of the 3D printer can be truly utilized.

In the recent coronavirus pandemic, good examples of its effect have been demonstrated all over the world. As seen in the local hobbyists and small businesses' movement, with 3D printers, decentralized production promptly responded to consumer needs, such as producing and providing the parts of face shields and ventilators that medical institutions lacked, at low cost. These cases, which occurred under an unprecedented emergency, have a sufficient impact to consider future production, distribution, and consumption and not just as a temporary measure.

In the rapidly advancing 3D printing industry, the answer is not clear whether to centralize or disperse production; and if a dispersed production system is adopted, the appropriate density of each production area. As of now, it is unclear whether each municipality will have one base and a medium-sized factory, or whether it will be distributed one by one in the city like a copy machine at a convenience store in Japan. In any case, there are proven cases where 3D printing technology is effective in both centralized and distributed production systems. It is necessary to pay close attention to what kind of position 3D printing technology will take in the flow from production to consumption in the manufacturing industry in the future.

デジタルファブリケーションの視点:
「メイカームーブメント」の過去 10 年間を振り返る
デジタルファブリケーションエコシステムと
可能性がある未来の予測

井上恵介

メイカームーブメントと呼ばれた 10 年を振り返る（2000 年代）

1980 年、名古屋市工業研究所にて小玉秀男による光造形法の発明[1] から、3D プリンターの歴史は幕を開けた。初期の 3D プリント産業は、現在も続く 3D Systems 社や Stratasys 社といったリーディングカンパニーによって牽引されてきたが、まだまだ導入コストが高く、一般消費者が扱えるものではなかった。2000 年代後半に入り、3D プリンティングにかかる基本特許の保護期間が終了したことに伴い、様々なメーカーから安価な 3D プリンターが発売されるようになった。2020 年現在では、$200 以下で 3D プリンターを購入でき、自前の「デスクトップ工場」を構築できる。

2000 年代は、現在の「メイカームーブメント」に続く重要な下地を作った。インターネットを中心とした情報インフラが整備され、様々な情報を共有できるようになった。オープンソースは、本来ソフトウェア開発やプログラミング分野で用いられてきた概念だ。テキストだけではなく、様々なフォーマットの情報をサーバーにアップロードできるようになったことで、設計図や回路図、あるいは 3D データそのものを共有できるようになった。こうした背景がなければ、3D プリンターのようなハードウェアがオープンソース化されることはなかっただろう[2]。

[1] https://ja.wikipedia.org/wiki/%E5%B0%8F%E7%8E%89%E7%A7%80%E7%94%B7

[2] RepRap プロジェクトは、オープンソースハードウェアの代表的な取り組みに数えられ、後進の熱融解積層（FFF）方式の 3D プリンター開発に多大な影響を与えた。https://reprap.org/wiki/RepRap

インターネットは3Dプリンターの開発を後押ししただけでなく、ユーザー側の情報共有も促した。ThingiverseやGrabCADといった3Dデータ共有サイト[3]には、世界中のユーザーが製作した3Dデータがアップロードされている。YouTubeのような動画共有サイトでは、3Dデータの作り方から3Dプリンターの使い方、新製品のレビューなどが多く見られる。意見交換やトラブルシューティングに役立つフォーラムやSNSグループなども、様々な言語で展開されている。情報の質としてみれば玉石混交ではあるものの、インターネット上で交わされるこれらの交流から、現在のメイカームーブメントの熱量を測ることができるだろう。

Fab Lab[4]は、こうしたインターネットの利点とものづくりを実践的につなげることから生まれた。3Dプリンターをはじめとするデジタルファブリケーション[5]を備えた工房を一般に開放することで、地域ごとの課題を共有し、グローバルに点在するナレッジによって解決することを目指した。物理的なインフラが整わない地域では特に、個々の課題を自ら作ることで解決する道筋を示した。デジタルデータから直接工作機械を動かすデジタルファブリケーションだからこそ、インターネットを通じたFab Lab間のデータの交換が可能となり、成果物を共有できるようになった。

デジタルの本質的な利点は、質を落とすことなく保存し、複製できる点にある。この利点は多くの恩恵をもたらしたと同時に、著作権保護の観点では新たな課題を生み出した。そのような中でクリエイティブ・コモンズ[6]は、どのようにシェアするかを制作者自身が決められる極めて民主的かつ建設的な制度として、メイカームーブメントにも大きな影響を与えた。

---

[3] https://www.thingiverse.com/ https://grabcad.com/
[4] https://fablabs.io/
[5]マシニングセンターやCNCルーターなど、デジタルデータを元に操作し、加工する産業用工作機械は既に一般的に利用されてきた。そうした閉じた環境下で使われてきた産業用工作機械が、メイカームーブメントを通じて民間人にも活用の幅が広がったことにより、総じて「デジタルファブリケーション」という呼び名が用いられる様になった。
[6] https://creativecommons.org/

メイカームーブメントを下支えする背景は、インターネットだけではない。インターネット上で情報をシェアするように、仕事や職場、機材や人材に至るまで、あらゆるものがシェアの対象となりうるシェリングエコノミーが誕生した。一般に開放された工房は Fab Lab に限らず、様々な運営形態で各所に現れた（こうした工房を総じてメイカースペースと呼ぶ)。2006 年に米国カリフォルニア州から出発した Techshop は、その後米国内に 10 拠点展開し、海外にもライセンス展開するなど、代表的なメイカースペースとなった。2012 年、中国深圳に誕生した HAXLR8R（後に HAX に改名）は、ハードウェアスタートアップに特化したメイカースペースとして、現在の深圳を象徴する拠点となった。

また 2006 年に米国カリフォルニア州で初開催された Maker Faire[7] は、地域中のメイカーが集まるイベントとして、その後世界各地で開催されるようになった。大規模な Maker Faire では、わずか数日間の開催で 10 万人を超える動員となるなど、メイカームーブメントを象徴するイベントとなった。Maker Faire のように誰でも気軽に参加できるオフラインイベントが登場したことは、メイカー自身にとってモチベーションたり得たし、その規模が徐々に大きくなるに連れ、単なるホビイストの集いではなく、スタートアップのための見本市としても機能した。

メイカームーブメントと呼ばれた 10 年を振り返る（2010 年代前半）

この様に、機材や情報インフラなどの技術的発展だけでなく、法制度や価値観、作り手のコミュニティ形成など、2000 年代に浸透した様々な要素が、現在のメイカームーブメントの下地を整えた。2010 年代に入ると、一般消費者でも購入しやすい安価な 3D プリンターが増え、「製造業の革命」としてメディアでも盛んに取り上げられる様になった。それまで大企業や大学の研究室、もしくは個人による DIY という両極で活用されていた 3D プリント技術が、中小製造業やデザイナー、教育機関といった中間層にも浸透していった。

[7] https://makerfaire.com/

時を同じくして、各国の行政機関も積極的に新しい技術の活用を後押しする様々な支援策を打ち出した。2013 年から展開されたスタートアップ支援策”French Tech”は、その後国内外から数多くのスタートアップ企業を生み出し、また誘致した[8]。2014 年には米国ホワイトハウスで前述の Maker Faire が開催され、次世代の製造業の競争力向上のため、特に教育機関向けに多くの導入支援策が施行された[9]。2015 年から中国で始まった「大衆創業・万衆創新」も、国内スタートアップを支援し、イノベーションを喚起する施策である。巨大な官僚機構の下に、トップダウン型で経済を先導してきた中国にあって、むしろボトムアップ型といえる施策を通じて、深圳を中心に多くのスタートアップ企業が誕生した[10]。新しい製造技術に対する具体的な取り組みが各国で進められる中、民間でも数多くのメイカースペースが誕生し、産官学民のすべてのレイヤーで、メイカームーブメントの隆盛は 2010 年前半にそのピークを迎えた。

メイカームーブメントと呼ばれた 10 年を振り返る（2010 年代後半）

筆者が運営するファブラボ神田錦町（旧ファブラボ渋谷）もそうした隆盛の最中、国内 3 番目のファブラボとして 2012 年に誕生し、今日までのメイカームーブメントの動向を当事者目線で見てきた。2010 年代後半に入ると、流行としてのメイカームーブメントは落ち着きはじめ、各国のメイカースペースやスタートアップ、行政施策に成否が現れる様になった。いかに魅力的なテクノロジーであっても、成功を約束された魔法のツールということはなく、華々しい成功事例の陰に数多の失敗がある。前述の Techshop の破産申請（2017）や、米国の Maker Faire を主催する Maker Media 社の業務停止（2019）といったニュースは、メイカーコミュニティに少なからず衝撃を与えた。また、かつての IT バブルが多くの IT ベンチャーを生み出した様には、ハードウェアスタートアップは生まれなかった。アイデアからワーキングプロトタイプまでは形にできても、安定して量産化させるに

[8] https://lafrenchtech.com/en/
[9] https://makezine.com/2014/06/18/white-house-maker-faire-fact-sheet-has-been-released/
[10] https://spc.jst.go.jp/experiences/studylife/studylife_1910.html

は全く異なる技術を要する。量産にかかる過大なコストは、資金調達をより困難にした。ソフトウェアと比較して開発に多くの時間を要し、仕様変更も容易には行えない。こうしたハードウェア特有の難しさを解決するほどには、人のスキルもテクノロジーも追いついてはいなかった。

2010 年代後半は、数多のサービスが淘汰されるなか、残るべきサービスだけが残るメイカームーブメントの成熟期に位置付けられる。流行がまばゆいほど淘汰された例は暗く見えるものだが、新しいテクノロジーを正しく理解し、変化する社会に適応した事例も多い。特に 3D プリンティングの領域は、ムーブメントの盛衰にさほど左右されることなく着々と社会に根ざしてきている[11]。

3D プリンティングが導く未来

産業革命以降の製造技術は、よりシステマティックな生産体制へと発展し、大量生産/大量消費社会をもたらした。この人類史上でも大きな変革は社会を一層豊かにしたが、20 世紀後半に差し掛かる頃には、急速に進む環境破壊の主な原因と見なされ、豊かさのあり様について疑問が投げかけられるようになった。一見矛盾するようだが、保存と複製を利点とするデジタルファブリケーションは、大量生産/大量消費の生産体制に一石を投じ得る。

一つにはデータの保存が物質の保存に比べて極めてローコストに、低い環境負荷で行える点にある。必要な量を、必要な時に生産できたなら、過剰な生産を抑制し、売り手も在庫という重荷を抱えることがなくなる。大量生産/大量消費に変わる新たなサイクルについて、デジタルファブリケーションは「適量生産/適量消費」を可能にする手段となり得る。

第二に、3D プリンターをはじめとするデジタルファブリケーションの多くは、短時間での大量加工にそもそも向いていない。代わりに、データを少し変更するだ

[11] https://www.marketsandmarkets.com/Market-Reports/3d-printing-market-1276.html?gclid=CjwKCAiAqJn9BRB0EiwAJ1Sztb4s0VHPGIqIP-y79e4rslj0sAZJM10iCMxTMv5hPUz5v320jMXkwhoCv2AQAvD_BwE

けで様々なバリエーションに展開できるのが強みである。「少量多品種」や「マス・カスタマイゼーション」といった、多様化する消費者のニーズを叶える実践的な手段としての活用が進んでいる[12]。また、医療やプロスポーツ用の装備品など、これまでオーダーメイドで対応を迫られた用途も、3D スキャン技術の向上に伴い、製造工程のデジタル化が進んでいる。

第三に、特に 3D プリンターが叶える形状自由度の高さを活かした活用が進んできている点である。従来の製造方法では造形不可能な形状も、ほとんどの場合で 3D プリンティングは可能になる。従来の製造方法では製造できる形に分割する必要があった形状も、一体で出力できるようになったことで、組み立ての工程を省略できる。また、3D プリンティングにかかるコストは「体積」に比例し、「形状の複雑さ」からは影響を受けにくい点も大きなアドバンテージである。製造コストを下げるために、従来は「作りやすい形」であることが重要だったが、「体積」という数値化された指標に置き換わったことで、ジェネレーティブデザインという新たなデザインプロセスの導入が進んでいる[13]。同一素材であれば体積と重量は比例するため、強度を維持したまま可能な限り体積が小さい（=軽い）部材を設計すれば、材料コストを抑えられる。さらに航空・宇宙産業分野における部材の軽量化は、運用コストや環境負荷の低減にもつながる[14]。

---

[12] 筆者が株式会社ロフトと協働で運営する「Loft & Fab」は、マス・カスタマイゼーションに特化したメイカースペースとして 2013 年 11 月から営業を続けている。同店には買い物客がロフトで購入した商品を自由にカスタマイズするための設備が備わり、スタッフが購入者のアイデアを形にするサポートを行っている。http://andfab.jp/

[13] ジェネレーティブデザインとは、入力した特定の制約や条件を満たす形状の設計をコンピューター自身に行わせ、複数の解を自動的に導き出すデザイン設計手法である。3D プリント技術の発展に伴い、3DCAD 設計ソフトウェアメーカー各社が開発に注力している分野の一つである。
https://en.wikipedia.org/wiki/Generative_design

[14] 3D プリンティング技術を積極的に取り入れている企業の一つがボーイング社である。777 系に連なる新機体 777X に搭載された GE9X エンジンは、300 点を超える 3D プリント部品を装備し、低燃費・高推力を実現した。同エンジンは既に FAA 認証を取得しており、量産化に向けた第一歩を踏み出している。また、先ごろ同社は 3D プリンティング研究開発施設をスコットランドに開設することを発表するなど、同技術への投資を積極的に進めている。
https://www.boeing.com/features/innovation-quarterly/2019_q4/btj-additive-manufacturing.page
https://www.geaviation.com/commercial/engines/ge9x-commercial-aircraft-engine

材料コストが高く、生産スピードも劣ることから、コンシューマープロダクトへの活用は未だ限定的[15] ではあるものの、3D プリント業界における開発競争は今なお加熱している。プリンター本体の開発だけでなく、材料の開発にも拍車がかかっている。様々な付加価値をもつ新素材が次々と生まれ、従来の製造法の代替品としてではなく、3D プリンティングによる全く新しい製品が生まれる機運が高まっている。材料が安定的に供給でき、そのコストが下がるにつれて、徐々にその活用版図が広がってくるだろう。2010 年代前半に多くのメディア上で繰り広げられた 3D プリンター狂騒は落ち着いたが、その歩みは当時から格段に進んでおり、今なお収まる気配は見られない。

3D プリンティングと流通に関する考察

現在、3D プリンターは大きく分けてホビイストやスモールビジネス向けの安価な機種と、製造業向けの高価な機種に大別される。いずれの場合も、従来の製造技術と比較して生産スピードは遅く、少なくとも現段階では射出成形機の代替とはならない。ただし、それは機材単体で見た場合で、多数の 3D プリンターを並列運用した場合では状況が異なる。射出成形機のように高額な「金型」を必要としない 3D プリンターは、複数台を並べた運用がしやすい。実際に、数十台、数百台もの 3D プリンターを並べた工場も存在する[16]。3D プリンターを活用した生産体制として、こうした並列化には大きなメリットがある。少ない人員で全体をオペレートでき、「金型」というイニシャルコストを必要としないため、生産数に下限がない。異なるデータもほぼ同様に扱うことができ、機材のセットアップも低い労

[15] 既に Nike や Adidas、Under Armour といったスポーツアパレルブランドでは、スニーカーのソール部を 3D プリンターで出力したコンシューマー向けプロダクトをリリースしている。また、義手や義足といった補装具を 3D プリンターで製造・販売する企業も存在する。

[16] Stratasys 社が 2005 年から事業展開させているオンデマンド 3D プリンティングファクトリー「Redeye」は 100 台を超える産業用 3D プリンターを備えた、世界最大の 3D プリンター工場である（現在は Stratasys Direct Manufacturing に統合化）。Redeye に関しては以下の報道ドキュメントに詳しい。 https://www.bbc.com/news/av/technology-25101388

働コストで行える。今後もオンデマンド生産を強みにした3Dプリント・メガファクトリーは、ニーズに合わせて配備されていくだろう。

一方で、こうした「メガファクトリー化」は、輸送コストの観点で従来の大量生産/大量消費モデルから脱却できていない。製品の消費先の近くまでデータで送り、そこで生産する方が3Dプリンターのもつ効果を真に活用できる。昨今のコロナ禍において、その効果を示す好例が世界各地で示された。各医療機関で不足するフェイスシールドや人工呼吸器のパーツを、地域のホビイストや小規模事業者が自前の3Dプリンターで出力して提供するといった動きに見られる通り、分散型の生産によって速やかに、ローコストで消費ニーズに対応してみせた。未曾有の非常事態のもとに起こったこれらの事例は、単なる一時的な対処法としてではなく、今後の生産・流通・消費のあり方を考察するのに十分なインパクトがある。

日進月歩の3Dプリンティング業界にあって、生産体制を集中させるか、分散させるか、分散させるとした場合にどの程度の密度で分散させるのかは、未だ答えが出ていない。各自治体に 1 拠点、中規模のファクトリーができるのか、日本のコンビニエンスストアのコピー機のように、街に 1 台ずつ分散されるのかも、現段階では適性が定かではない。何れにせよ、3D プリンティング技術が集中生産体制・分散生産体制のいずれの場合でも効果を発揮する事例は示されている。今後3D プリンティング技術が、製造業における生産から消費までの流れの中で、どのようなポジションを取っていくのか注視が必要である。

SECURITY IMPLICATIONS OF QUANTUM COMMUNICATIONS AND COMPUTING

By Edward Parker

Executive Summary

Quantum technology is at an early stage of development, and the future applications and timelines are highly uncertain. Japan, China, and the EU are prioritizing the subfield of *quantum communications*, which might (or might not) greatly improve the security of encrypted communications. The US and a few other countries are focusing more on *quantum computing*, which could eventually *threaten* the security of encrypted communication, as well as providing useful commercial applications. Most international cooperation between the US and Japan in this area occurs informally through academic laboratories, but more formal cooperation may eventually become useful as quantum technology continues to mature.

Quantum physics describes the behavior of particles that are (roughly) at or below the size of individual atoms. New and counterintuitive phenomena occur at these tiny sizes, and physicists and engineers have recently begun to control this behavior with high precision. These phenomena could eventually unlock fundamentally new capabilities, some of which have implications for international security.

Quantum technologies are generally grouped into three broad categories: communications, computing, and sensing. Although quantum sensing has some defense applications,[1] this paper focuses on quantum communications and computing, which have the greatest potential long-term impacts on international security. It gives an overview of the technologies' possible applications, their timelines, and the different approaches taken by the US, Japan, and China.

Quantum communications and computing could both have major impacts on the security of encrypted information, but in opposite directions: quantum communications could *strengthen*

[1] C. Todd Lopez, "DOD Should Focus on Short-Term Goals in Quantum Science," DoD News (March 12, 2020). https://www.defense.gov/Explore/News/Article/Article/2110617/dod-should-focus-on-short-term-goals-in-quantum-science/

the security of encryption, while quantum computing could *threaten* it. Although these technologies will converge as they become more mature, today they are both in very early stages and being developed largely independently. Depending on which subfield becomes mature first (if either), the overall security of encrypted information could either strengthen or weaken.

Quantum communications

Quantum communications refers to physical mechanisms for information transmission that do not use electromagnetic waves, but instead individual microscopic particles of light called *photons*. The only application of quantum communications deployed today is known as *quantum key distribution* (QKD), a type of *quantum cryptography* that in principle enables extremely secure encrypted communication.

QKD works because, unlike with standard communications, the laws of quantum physics guarantee that an eavesdropper who intercepts a stream of photons *inevitably* leaves a signature of their eavesdropping directly on the signal itself. If the recipient detects that the signal has been intercepted, then they can abort the transmission until the intrusion ends.[2] QKD is sometimes referred to as enabling "unhackable" communication. However, it is important to note that QKD is only truly "unhackable" when implemented correctly, and actual commercial QKD devices have consistently demonstrated security vulnerabilities.[3]

QKD was first deployed commercially in Switzerland in 2007, and is still used in Europe to secure sensitive communications such as election results.[4] However, East Asia is now arguably at the forefront of the commercial deployment of QKD. Japan inaugurated a city-scale network of fiber-optic cables for QKD across Tokyo in 2010.[5] In January 2020, Toshiba Corporation and Tohoku University announced that they had set a QKD bandwidth record by transmitting

[2] Strictly speaking, QKD does not directly transmit messages, but instead *encryption keys*, which are very large numbers that used to encrypt messages. If an encryption key is intercepted by an eavesdropper, then it is discarded before any sensitive messages are encrypted.
[3] Nitin Jain et al., "Trojan-horse attacks threaten the security of practical quantum cryptography," *New Journal of Physics* 16 (2014).
[4] ID Quantique, "IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation," November 23, 2017. https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/
[5] Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Express* 19, 10387 (2011).

hundreds of gigabytes of encrypted genomic data in minutes, and Toshiba has announced that it soon intends to begin selling QKD devices in the United States.[6]

China appears to be even further ahead in the deployment of QKD. It has laid down a 2000-km cable connecting Beijing, Jinan, Hefei, and Shanghai.[7] Most impressively, the Chinese have also launched the world's only quantum communications satellite capable of performing QKD from space, known as Micius or *Mozi* (墨子). In 2017, this satellite enabled a heavy-encrypted intercontinental video teleconference between Xinglong, China and Graz, Austria.[8] QKD has therefore advanced to the point where small but useful amounts of data can be encrypted. If this significantly improves the security of highly sensitive communications, then the implications for national security are clear.

However, not all security experts are convinced that QKD will in fact improve communication security, at least in the short term. Some experts have expressed doubts that QKD will ever prove useful in practice,[9] and both the UK Government Communications Headquarters and the US Department of Defense's Defense Science Board have publicly stated that they believe that QKD has not yet been demonstrated to be secure enough for operational use.[10] Unlike Europe and East Asia, the US has not yet deployed QKD commercially, although a few startups are exploring the technology.

In the future, quantum communications may be used for applications beyond QKD. More technically sophisticated forms of quantum communication could eventually enable a full "quantum Internet," with end-to-end quantum encryption and (for example) distributed

---

[6] Toshiba Corporation, "World-first Demonstration of Real-time Transmission of Whole-genome Sequence Data Using Quantum Cryptography" (Jan. 14, 2020).
"Toshiba to launch quantum cryptography services this year," *Nikkei Asia* (Jan. 21, 2020).
[7] However, the Beijing-Shanghai line contains 32 signal repeaters that each represent a point of vulnerability to inception. Yiu, Yuen, "Is China the Leader in Quantum Communications?," *Inside Science* (Jan. 19, 2018).
[8] Philip Ball, "Intercontinental, Quantum-Encrypted Messaging and Video," *Physics* 11, 7 (2018). https://physics.aps.org/articles/v11/7
[9] Bruce Schneier, "Quantum Cryptography: As Awesome As It Is Pointless," *Wired* (Oct. 15, 2008).
[10] United Kingdom National Cyber Security Centre, "Quantum security technologies," (March 24, 2020). https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
Department of Defense Defense Science Board, "Applications of quantum technologies: Executive Summary" (Oct. 2019).
https://dsb.cto.mil/reports/2010s/DSB_QuantumTechnologies_Executive%20Summary_10.23.2019_SR.pdf

quantum computing. But these applications are still at very early stages of technological maturity, and it is not clear exactly how they will be used and over what timelines.[11]

Quantum computing

A quantum computer is a type of computer that operates on fundamentally different physical principles than standard computers that exist today. While the basic unit of information for a standard computer is a bit – a 0 or 1 stored in memory – the basic unit of information for a quantum computer is called a *qubit*, which can in some sense be thought of as representing both a 0 and a 1 at the same time. For certain calculations, quantum computers are believed to be exponentially faster (and therefore more powerful) than any classical computer could be.

Over the long term, the application of quantum computers with the most disruptive impact on international security is likely be their (future) use against cryptography. If executed on a large enough quantum computer, a quantum algorithm known as *Shor's algorithm* would be able to quickly decrypt algorithms currently used to encrypt internet traffic.[12] It is difficult to overstate the damage that a hostile actor capable of executing Shor's algorithm could inflict on both national and economic security if no safeguards are put into place. The many types of sensitive internet communications would all become insecure: email, financial transactions, personal health information, sensitive diplomatic or military communications – essentially anything that requires a password.

Moreover, quantum computing is no longer a completely fanciful technology. In October 2019, a team of Google researchers announced that they had built a quantum computer named "Sycamore" that had performed a certain calculation faster than the fastest standard supercomputer. Although the Sycamore computer's calculation has no known applications, it was an important proof-of-principle demonstration that quantum computers can in fact be qualitatively faster than standard computers, at least for certain tasks.[13]

---

[11] Stephanie Wehner et al., "Quantum internet: A vision for the road ahead," *Science* 362(6412), eaam9288 (2018).

[12] Strictly speaking, the most powerful quantum decryption algorithms only attack a class of cryptography known as *public-key cryptography*, but almost all internet encryption uses this class at some point.

[13] William D. Oliver, "Quantum computing takes flight," *Nature* 574, 487 (2019).

However, it is important to keep the significance of this demonstration in perspective. Quantum computers are still nowhere near the size and sophistication necessary to threaten encryption. Other Google researchers recently estimated that breaking commercial-grade encryption will require a quantum computer with approximately 20 million qubits. By contrast, Google's Sycamore computer had 53 qubits. Because of the huge number of required qubits and many other technical challenges that have yet to be overcome, most experts are confident that current encryption is safe from quantum computers for at least the next 10 years.[14] Researchers are already developing new cryptography algorithms which are believed to be resistant against attacks from quantum computers. These algorithms will hopefully arrive before quantum computers become sophisticated enough to threaten encryption, although the large-scale deployment of these new algorithms will pose their own challenges.[15]

Quantum computers are also believed to have applications other than decryption – for example, biochemistry simulation for the discovery of new medical drugs.[16] Many of these applications are believed to be less technically challenging than decryption, so they will become feasible sooner. These applications have positive commercial applications, so we should anticipate quantum computers with a sense of hope in addition to a sense of concern.

Unlike with quantum communications, the United States appears to be the clear world leader in the commercial deployment of quantum computing. Several private companies, from tech giants such as Google and IBM to small startups such as IonQ, have developed quantum computers with more than 50 high-quality qubits – the approximate threshold at which quantum computers become competitive with the world's best supercomputers for certain tasks. No other country has announced the complete integration of a potentially useful quantum computer. However, there are certain enabling technologies – for example, certain

[14] National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects.* Washington, DC: The National Academies Press (2019).
[15] Michael J.D. Vermeer and Evan D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," RAND Corporation, RR-3102-RC (2020).
[16] Katherine Bourzac, "Chemistry is quantum computing's killer app," *Chemical and Engineering News* 95(43) (2017).

quantum materials – of which Japan is the primary supplier, so the two countries' deployments of quantum technology remain somewhat interdependent.[17]

Conclusion

Quantum technology – particularly the communications and computing technologies that this paper focuses on – are still at a very early stage of development. As such, their future use cases and timelines for deployment are highly uncertain. But given the major technical challenges that need to be overcome, the most disruptive impacts of these technologies are probably still at least 10 years away. Policymakers should expect the unexpected – but not too soon.

Moreover, different nations are focusing their efforts on different technologies: China, Japan, and the EU are putting comparatively more effort into (and correspondingly leading in the deployment of) quantum communications, while the US, Canada, and the UK are leading in quantum computing. The combination of low levels of technological maturity and different focuses by different countries means that it is still too early to tell which quantum technologies will have the biggest impacts on national security, or which nations will be best positioned to capitalize on those technologies when they do become mature. Policymakers should carefully monitor new technological developments in this field, but should adopt a measured posture rather than overreacting to potential threats that are probably not yet imminent. If possible, nations should broadly invest across diverse areas of quantum technology, given the high uncertainty regarding which technologies will prove practical.

The US and Japan have strong ties in academic quantum research, with laboratories from both countries often co-authoring research papers. There are very few formal agreements or policies between the two countries regarding quantum technology. However, in December 2019, the governments of the US and Japan signed the Tokyo Statement on Quantum Cooperation pledging to jointly advance innovation in quantum technology,[18] and (as mentioned above) Toshiba Corporation has announced that it plans to begin exporting QKD devices to the US.

---

[17] National Academies of Sciences, Engineering, and Medicine. *Domestic Manufacturing Capabilities for Critical DoD Applications: Emerging Needs in Quantum-Enabled Systems: Proceedings of a Workshop.* Washington, DC: The National Academies Press (2019).

[18] US Department of State, "Tokyo Statement on Quantum Cooperation" (Dec. 19, 2019). https://www.state.gov/tokyo-statement-on-quantum-cooperation/

These developments may indicate that the technology is maturing to the point where formal economic policy cooperation becomes appropriate.

If the US does begin to deploy QKD at scale, then standards setting to ensure interoperability could be a fruitful area for international cooperation between the US and Japan (as well as the European Union and South Korea, who are also deploying this technology). International standards setting for quantum computing would probably be premature, as quantum computers are still at such an early stage that researchers have difficulty even characterizing the performance of their own computers, let alone synchronizing that performance with other computers'.

One possible exception is in the area of *post-quantum cryptography*. As mentioned, researchers at the National Institute of Standards and Technology are developing new cryptography algorithms that are believed to be resistant to attacks by quantum computers, with the initial standards planned to be released in 2022.[19] Transitioning to new cryptography standards will be very complicated and will require close cooperation between nations. Depending on how quickly nations move to adopt the new standards, this cooperation could begin within the next few years.

Quantum technology is still at an early stage, but is developing rapidly. Its potential impacts are difficult to predict, but they could be transformative. Technological leadership could still change hands – potentially several times – before the technologies become fully mature. Close cooperation between allied nations – particularly nations taking complementary technological approaches, such as the US and Japan – could be a useful hedge against the large uncertainties inherent to such a fundamentally new technology.

[19] National Institute of Standards and Technology. "NIST's Post-Quantum Cryptography Program Enters 'Selection Round'" (July 22, 2020). https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

量子コンピューティングと量子通信におけるセキュリティ

エドワード パーカー

要約：量子技術はまだ開発の初期段階にあり、将来的な応用や今後の流れは非常に不確実である。日本や中国、EU は、暗号化された通信の安全性に大きな発展をもたらすかもしれない（または、そうでないかもしれない）量子通信の分野を優先的に開発しており、米国や他幾つかの国々は、量子コンピューティング分野により注力している。量子コンピューティングは将来的に暗号化通信の安全性を脅かしうる一方で、有益な商業的応用ももたらしうる。当該分野における日米間の国際協力は、その多くが学術的な研究を通じて非公式に行われている。しかし量子技術が発展していくにつれて、よりフォーマルな二国間の協力が有用となるかもしれない。

量子力学は個々の原子と（ほぼ）同じか、それ以下の大きさを持つ粒子の物理現象を記述する学問である。新たな現象や反直感的な現象がこれらの微小なサイズにおいて起こるが、近年物理学者やエンジニア達は、高い精度でこれら粒子の行動をコントロールできるようになってきた。これらの現象は将来的に、根本的に全く新しい技術の開発を可能にするかもしれず、そのうちのいくつかの技術は国際安全保障に影響を与える。

量子技術は一般的に 3 つのカテゴリーに分類することができる：通信、コンピューティング、センシングである。量子センシングは防衛技術への応用ができることも事実だが[1]、本論文では国際安全保障に長期的な影響を与える可能性のある量子通信と量子コンピューティングに焦点を当てる。特に、技術の応用可能性、今後の流れ、米国、日本、中国のアプローチの違いについて概観する。

[1] C. Todd Lopez, “DOD Should Focus on Short-Term Goals in Quantum Science,” DoD News (March 12, 2020). https://www.defense.gov/Explore/News/Article/Article/2110617/dod-should-focus-on-short-term-goals-in-quantum-science/

量子通信と量子コンピューティングはどちらも暗号化された情報のセキュリティに大きな影響を与える可能性があるが、量子通信が暗号化の安全性を強化するかもしれない一方、量子コンピューティングはその逆、即ち暗号化の安全性を脅かす可能性がある。これらの技術が発達していくにつれてどこかに収束していくことになると予想されるが、今日において両技術は未だ非常に初歩的な段階にあり、別個に研究が進められている。どちらの分野が先に発達するかによって、（もしどちらか一方だけが発達すればだが、）暗号化情報のセキュリティ全般は強化されるか脆弱になるかのいずれかになる。

量子通信

量子通信とは、電磁波ではなく代わりにフォトンと呼ばれる微小な光の粒子を使って情報伝達を行う物理的機構を指す。今日において唯一の量子通信の応用例は、量子鍵配布（*quantum key distribution*: QKD）として知られており、量子暗号の一種で原理的には極めて安全な暗号化通信を可能にするものである。

QKD の仕組みはこうだ：標準的な通信とは異なり、QKD は量子力学の原理に従い、フォトンの流れに介入する傍受者が、信号そのものに傍受の証拠を直接残さざるを得ない。もし情報の受信者が、通信が傍受されたことを感知した場合、通信者はその傍受行為が終わるまで通信を切断することができる[2]。QKD は時々「ハッキング不可能」（“unhackable”）な通信手段を可能にするもの言及されることがある。しかし大切なのは、QKD は正しく実装された場合にのみ「ハッキング不可能」であり、実際の商用 QKD デバイスはセキュリティの脆弱性が絶えず指摘されていることに注意が必要である[3]。

---

[2] 厳密に言えば、QKD はメッセージを直接送信するのではなく、メッセージを暗号化するために使用される非常に大きな数字、暗号化キーを送信する。暗号化キーが傍受された場合、それは機密性の高いメッセージが暗号化される前に破棄される。

[3] Nitin Jain et al., “Trojan-horse attacks threaten the security of practical quantum cryptography,” *New Journal of Physics* 16 (2014).

QKD は 2007 年にスイスで初めて商業展開され、今日でもヨーロッパにおいて選挙結果などの機微な情報を安全に伝えるために用いられている[4]。しかし、QKD の商業展開の最前線を占めているのは今やおそらく東アジアであろう。日本では 2010 年、東京に都市規模の QKD 用光ファイバーケーブルを敷設した[5]。2020 年 1 月、東芝と東北大学は、数百ギガバイトの暗号化された遺伝子情報を数分間で伝達し、QKD の帯域幅の記録を樹立したと発表した。さらに、東芝は近く米国内で、QKD デバイスの販売を開始する意向であるとも発表した[6]。

中国は QKD の導入において、さらにその先を行っているようである。中国は北京、済南、合肥、上海を結ぶ 2000km のケーブルを敷設した[7]。最も驚くべきは、宇宙から QKD を実行できる、世界で唯一の量子通信衛星「墨子」を打ち上げたことだ。2017 年にはこの衛星が、中国の興隆とオーストリアのグラーツとの間で高度に暗号化された大陸間ビデオ電話を可能にした[8]。QKD は少量ではあるがそれでも有用な量のデータを暗号化できるところまで進んでいる。この技術により機密性の高い情報通信の安全性が大幅に向上する場合、国家安全保障へ与える影響は明らかである。

しかし、すべてのセキュリティ専門家が、少なくとも短期間で QKD が通信の安全性を向上させるだろうと考えているわけではない。一部の専門家は QKD の実際の有効性を疑問視しており[9]、英国の政府通信本部（Government Communications Headquarters）や米国の国防総省防衛科学委員会（Department of Defense's Defense

[4] ID Quantique, "IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation," November 23, 2017. https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/
[5] Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD Network," *Opt. Express* 19, 10387 (2011).
[6] Toshiba Corporation, "World-first Demonstration of Real-time Transmission of Whole-genome Sequence Data Using Quantum Cryptography" (Jan. 14, 2020).
[7] しかし、北京−
上海間の通信線は 32 信号リピーターがあり、それぞれがインセプションに対する脆弱性を示している。Yiu, Yuen, "Is China the Leader in Quantum Communications?," *Inside Science* (Jan. 19, 2018).
[8] Philip Ball, "Intercontinental, Quantum-Encrypted Messaging and Video," *Physics* 11, 7 (2018). https://physics.aps.org/articles/v11/7
[9] Bruce Schneier, "Quantum Cryptography: As Awesome As It Is Pointless," *Wired* (Oct. 15, 2008).

Science Board）も、QKD は実際の運用に耐えうるだけの安全性が実証されていないという判断を公に示している[10]。ヨーロッパや東アジアとは異なり、米国においてはいくつかのスタートアップが開発を試みているが、QKD の商業展開には至っていない。

将来的には、量子通信は QKD 以外にも応用されうる。より技術的に洗練された量子通信は初めから終わりまで量子暗号化されており、（例えば）分散された量子コンピューターで構成されている完全な「量子インターネット」を可能にしうる。しかし、これらの技術はまだ非常に初歩的な段階であり、どのようなタイミングで、またどのように用いられるかは明らかではない[11]。

量子コンピューティング

量子コンピューターは今日存在している一般的なコンピューターとは根本的に異なる物理的原理で作動するコンピューターである。一般的なコンピューターにおける情報の単位はビット—メモリに格納された 0 か 1—であるが、量子コンピューターにおいては量子ビットという単位が用いられる。これはある種 0 と 1 の両方を同時に表していると考えることができる。計算上は、量子コンピューターは古典的なコンピューターよりも指数関数的に高速（すなわち強力）であると考えられている。

長期的に考えると、国際安全保障に最も強力な影響をあたえる量子コンピューターの活用方法は、暗号技術に対する（将来的な）応用である可能性がある。もしも十分に大きな量子コンピューター上で、ショアのアルゴリズム（Shor's algorithm）として知られる量子アルゴリズムを実行すれば、現在インターネットのトラフィ

[10] United Kingdom National Cyber Security Centre, "Quantum security technologies," (March 24, 2020). https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies
Department of Defense Defense Science Board, "Applications of quantum technologies: Executive Summary" (Oct. 2019). https://dsb.cto.mil/reports/2010s/DSB_QuantumTechnologies_Executive%20Summary_10.23.2019_SR.pdf
[11] Stephanie Wehner et al., "Quantum internet: A vision for the road ahead," *Science* 362(6412), eaam9288 (2018).

ックで暗号化に使われているアルゴリズムを素早く解読してしまうだろう[12]。何も安全策が講じられていない場合、ショアのアルゴリズムを実行できる能力を持った敵対的なアクターが、国家安全保障と経済安全保障の双方に与える可能性のあるダメージは計り知れない。基本的にパスワードを必要とするもの全て、例えば E メール、金融取引、個人の健康情報、機密性の高い外交や軍事通信等、多種多様なインターネット上の機微なやり取りはすべて安全なものではなくなるであろう。

さらに言えば、量子コンピューティングはもはや空想上の技術ではない。2019 年の 10 月にはグーグルの研究チームが一般的な最速のスーパーコンピューターよりも速く特定の計算を実行する「Sycamore」と名付けられた量子コンピューターを構築したと発表した。この「Sycamore」の計算には既知の応用例はないが、少なくとも特定のタスクにおいては、量子コンピューターが標準のコンピューターよりも質的に高速である可能性を実際に示した、重要な概念実証であった[13]。

しかし、この実験の重要性を全体の中で位置づけることが重要である。量子コンピューターはまだ、暗号化を脅かすのに必要なサイズと技術の洗練さには未だ遠く及ばない。あるグーグルの研究者は最近、一般的な商用の暗号を解読するには約 2000 万量子ビットの量子コンピューターが必要であると推定した。対象的に、グーグルの Sycamore は 53 量子ビットであった。必要とされる膨大な量子ビット数と、その他のまだ解決されていない技術的課題ゆえに、多くの専門家は、現行の暗号技術は少なくとも今後 10 年間は量子コンピューターから安全である確信している[14]。また研究者はすでに、量子コンピューターからの攻撃に耐えうると考えられている新しい暗号化アルゴリズムを開発している。これらのアルゴリズムは

---

[12] 厳密に言えば、
最も強力な量子暗号解読アルゴリズムは公開鍵暗号と呼ばれるタイプの暗号化方式しか攻撃しないが、インターネット上のほぼすべての暗号化において、どこかの段階でこの方式が使われている。

[13] William D. Oliver, “Quantum computing takes flight,” *Nature* 574, 487 (2019).

[14] National Academies of Sciences, Engineering, and Medicine. *Quantum Computing: Progress and Prospects.* Washington, DC: The National Academies Press (2019).

量子コンピューターが暗号化技術を脅かすほど発展する前に開発されることが望ましいが、これらの新しいアルゴリズムの大規模な展開にはいくつかの課題を伴う[15]。

量子コンピューターは暗号解読以外の応用も考えられている—例えば、新薬を発見するための生化学シミュレーション等である[16]。これらの多くは暗号解読よりも技術的には容易であると考えられており、すぐに実用化されるだろう。量子コンピューターはこれらの応用例のように有用な商業的応用もあるので、我々は懸念だけでなく、希望も持って量子コンピューターを考える必要がある。

量子通信の時とは異なり、米国は量子コンピューティングの分野において明確な世界的リーダーであるように思われる。グーグルや IBM などのハイテク大手や IonQ などの小さなスタートアップなどの民間企業が高品質な 50 量子ビットを超えるコンピューターを開発してきた。特定のタスクにおいては、量子コンピューターは世界最高のスーパーコンピューターと肩を並べ始めている。米国以外のどの国も潜在的に利用価値のある量子コンピューターの完全なる統合を発表していない。とはいえ、そのために必要な特定の技術—例えば特定の量子材料など—は日本が主要なサプライヤーであり、両国の量子技術の展開は幾分か相互に依存している[17]。

結論

量子技術—特に本稿が焦点を当てた通信技術とコンピューティング—はいまだ開発の初期段階にある。そのため、それらの技術が将来的にどのように用いられるか、何年後にそれが実装されるのかといったことは非常に不確実なものとなって

[15] Michael J.D. Vermeer and Evan D. Peet, "Securing Communications in the Quantum Computing Age: Managing the Risks to Encryption," RAND Corporation, RR-3102-RC (2020).
[16] Katherine Bourzac, "Chemistry is quantum computing's killer app," *Chemical and Engineering News* 95(43) (2017).
[17] National Academies of Sciences, Engineering, and Medicine. *Domestic Manufacturing Capabilities for Critical DoD Applications: Emerging Needs in Quantum-Enabled Systems: Proceedings of a Workshop.* Washington, DC: The National Academies Press (2019).

いる。しかし、克服しなければならない主要な技術的課題があることから、これら技術が最も破壊的な衝撃を与えるのは、少なくともあと 10 年先である。政策立案者は予期せぬ事態に備えなければならないが、それはすぐに生じるわけではない。

さらに各国が異なる技術に開発に注力している：日本、中国、そして EU は比較的量子通信により注力している（そしてそれゆえにこの分野の展開をリードしている）が、米国やカナダ、イギリスは量子コンピューティングの分野をリードしている。技術がまだ十分に発展していないことや、それぞれの国が異なる分野の開発に注力していることから、どの量子技術が安全保障に最も多大な影響を与えるのか、技術が発展した暁にはこれら技術の商業利用からどの国が最も恩恵を受けるのかを現時点で判断するのは拙速である。この分野における技術的進歩を政策立案者は注意深く追っていかなければならないが、未だ然程差し迫っているわけではない潜在的な脅威に対して過剰に反応するのではなく、慎重な姿勢を取るべきである。もし可能であるならば、どの技術が実用化されうるのか不確実性が高いことを考慮し、量子技術の幅広い分野に各国は投資すべきである。

日本と米国は学術的な量子技術の研究において強い結びつきがあり、両国の研究室はしばしば研究論文を共同執筆している。量子技術に関して、二国間の公式な合意や政策はほとんど無いが、2019 年 12 月、日米両政府は量子技術革新を共同で促進していくことを誓約する、量子協力に関する東京声明（Tokyo Statement on Quantum Cooperation）に署名した[18]。さらに、（前述の通り）東芝は米国への QKD デバイスの輸出を開始する予定であると発表した。これらの進展は、正式な経済政策協力を適切となるまでにこの技術が発展したことを示しているのかもしれない。

[18] US Department of State, “Tokyo Statement on Quantum Cooperation” (Dec. 19, 2019). https://www.state.gov/tokyo-statement-on-quantum-cooperation/

もし米国が QKD を大規模に展開した場合、相互運用性を確かなものにするための規格の設定は、日米間の国際協力にとり実りの多いものとなるだろう（そしてそれは、この技術を開発している EU や韓国といった国々とも同様である）。量子コンピューターはまだ非常に初歩的な段階であり、研究者は自らのコンピューターの性能を正確に測ることも、他のコンピューターの性能と同期させるのも難しいことを踏まえれば、量子コンピューティングの国際標準の設定はおそらく時期尚早であろう。

一つの例外として考えられるのは、ポスト量子暗号の分野である。前述したように、米国国立標準技術研究所（National Institute of Standards and Technology）の研究者は量子コンピューターによる攻撃に耐えうると考えられている新しい暗号化アルゴリズム開発しており、**最初の標準規格が 2022 年に発表される予定である**[19]**。**新しい暗号化標準への移行は非常に複雑で、国家間の密接な協力が必要となるだろう。各国がどれだけ迅速に新たな規格を採用するかによっては、この協力は今後数年以内に開始される可能性がある。

量子技術はまだ初期段階にあるが、急速に発達している。量子技術の持つ潜在的な影響力を予見することは難しいが、変革をもたらす可能性はある。これらの技術が完全に成熟するまで、その技術的な主導権は他へ移る可能性があり、それは数回起こるかもしれない。同盟国同士、特に日米などの技術の補完的なアプローチをとる国々との密接な協力は、このような全く新しい技術に伴う多大な不確実性に対する有効なヘッジとなるかもしれない。

[19] National Institute of Standards and Technology. “NIST’s Post-Quantum Cryptography Program Enters ‘Selection Round’” (July 22, 2020). https://www.nist.gov/news-events/news/2020/07/nists-post-quantum-cryptography-program-enters-selection-round

CHINA'S AIM FOR QUANTUM HEGEMONY AND THE JAPAN-US ALLIANCE

By Takahiro Tsuchiya

China's ambitions for "quantum hegemony"

In an Oct. 16, 2020 group study session of the Political Bureau of the Chinese Communist Party (CCP) Central Committee, General Secretary Xi Jinping stressed the importance and urgency of advancing the development of quantum science and technology. Xi emphasized the need to strengthen strategic planning and systematic efforts to develop quantum science and technology, grasp general trends, and be "a first mover" in the industry. Xi also emphasized that cultivating high-level talent is critical, enabling innovation in disruptive technologies, collaboration among industries, universities, and research institutes, and enhancing international cooperation in the field of quantum science and technology. He also called for efforts to foster strategic emerging industries such as quantum communications to gain the upper hand in international competition and facilitate national development.[20]

Chinese research institutes and industries working on quantum

China has laboratories run by private companies such as Baidu, Alibaba, Tencent, and Huawei, as well as national priority laboratories run by governments and universities.[21] The Chinese University of Science and Technology is the most famous of these because Dr. Pan Jianwei, "the father of quantum" in China, works there.

Military-Civil Fusion (or Civil-Military Integration) has military companies and institutions working on the quantum key distribution (QKD) network; they include Beijing Puhui Civil-Military Integration Equipment Technology Center, Beijing Jintai Technology Co., Ltd., and Wuhan Maritime Communication Research Institute (a.k.a. the 722 Institute).

---

[20] "Observing the Global Battle for 'Quantum Hegemony'," *Xinhua*, February 14, 2018. <http://www.xinhuanet.com/science/2018-02/14/c_136972095.htm>, and Elsa B. Kania, John Costello, "Quantum Hegemony?: China's Ambitions and the Challenge to U.S. Innovation Leadership," Center for a New American Security, 12 September 2018. <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf>

[21] Strider Global Intelligence Team, "QUANTUM DRAGON," Strider, November 2019. <https://www.strider.tech/resources/quantum-dragon-report/>

In China, an industrial chain is being built along with a quantum network. The quantum communications industrial chain includes the manufacture of core devices for quantum communications; the manufacture of communications equipment; the construction and management of communications transmission networks; the operation of communications networks; and the provision of quantum applications such as generating encryption keys to securely transfer highly confidential information, such as government, financial, medical, and military information. Various companies and national organizations are involved in each stage of the industry chain.

China advances its QKD Network

China is ahead of Japan and the US in building and operating complex quantum networks using quantum communication satellites and optical-fiber networks. In August 2016, China successfully launched the world's first quantum science experimental satellite "Mò zi." China is also focusing on construction of a quantum cryptographic network by constructing a ground-based quantum communication trunk line. The QKD Network aims to protect critical infrastructure networks from cyber-attacks. For China, military use is also a main purpose: the QKD Network includes the headquarters of the People's Liberation Army (PLA) theater commands.

Construction and operation of this complex quantum network allows China to proceed with the verification of secure quantum protocols and the accumulation of knowhow on how large-scale quantum operate. This will give it an advantage in the development of the advanced Quantum Internet.

A quantum network that is secure and difficult to decipher makes it possible to protect confidential information from cyber-attacks. In the future, cloud quantum computing will deploy quantum computers in China and other countries to enable blind quantum computing and the quantum internet, a global network capable of more advanced quantum communications compared to today's cryptographic network. China intends to provide not only quantum computers but also global communication networks. If that happens, the world will depend on China for its satellite and communications network infrastructure.

Attacks on quantum devices alone don't necessarily expose information, but merely block communications. And while communication over quantum networks is secure, the infrastructure of quantum networks is not robust. It is difficult to identify the perpetrator of an infrastructure attack given the way quantum networks work.

There is a risk that terminal nodes will be isolated and disconnected from the network if a repeater is determined to be malicious or faulty. A quantum network's security could also be compromised if the quantum bit being transmitted Bell pair (entangled two qubits[22]) is stolen. The corresponding classical communications method (communication over the Internet) can also be identified and eavesdropped on[23].

Application of Quantum Technology for National Defense and Military

Quantum technology is being applied not just to computing, cryptography, telecommunications, and teleportation but also to radar and sensors. In China, universities, research institutes, and companies are conducting research and development in the fields of quantum radar and quantum sensors to acquire "quantum hegemony."

Chinese military universities and military industries are actively involved in the R&D of these technologies. A future single-photon quantum radar could detect and capture stealth platform targets in electronic warfare. Quantum inertial sensors may improve submarine navigation in deep waters. We should expect quantum communications using quantum cryptography to be developed to enhance the survival of conventional weapons.

In 2018, a group led by Pan Jianwei successfully conducted experiments related to interstellar quantum communications in China.[24] The paper from this experiment suggests that it is

[22] If Bell pairs are shared between two remote locations, we can perform quantum communication using those Bell pairs.
[23] T. Satoh, et al. "The network impact of hijacking a quantum repeater," *Quantum Science and Technology* 3.3 (2018): 034008.
[24] C. Yuan, et al. "Bell Test over Extremely High-Loss Channels: Towards Distributing Entangled Photon Pairs between Earth and the Moon," *Physical Review Letters* 120 (2018): 140405.

possible to place quantum satellites for interstellar quantum communication at L4 and L5 Lagrange points, following "Mò zi."

China has plans for manned exploration of the moon's surface and construction of a space station (a lunar base). A lunar base will enable fixed-point monitoring of the Earth and encrypted communications with the Earth via quantum satellites. It could be used for military purposes, such as cyber-attacks and remote control of missiles. There is also the possibility of using weapons of mass destruction (WMD) or antisatellite (ASAT) weapons to protect quantum satellites, raising concerns about China's use of quantum technology for military purposes. As John Raymond, director of US space operations, has pointed out, "The universe is no longer a peaceful space, but a combat zone."

China's Long-Term Plan for the Construction of Quantum Networks and the Military-Civil Fusion Development Strategy

China's plan to build a national quantum cryptography network is based on a medium- to long-term plan presented by Chinese scientists in 2014. China plans to introduce quantum password transmission between Asia and Europe later in 2020. This is part of the plan to build an intercontinental quantum network between Asia and Europe. Around 2030, China will build a globalized wide-area quantum cryptography communications network. This will yield a quantum network capable of safely transmitting information and an organized quantum communication industry chain.

China is enhancing R&D and military use of quantum technologies under the "military-civil fusion development strategy." A specialized communications command network (C4ISR) is the central nervous system of a modern military, and it requires encryption. China invested more than 100 billion Chinese yuan in 2018 to build such a network dedicated to military communications. China aims to secure absolute security through quantum cryptography.

As with other "game-changing" technologies, military-civil fusion in quantum technology has made it difficult to determine whether end users have consumer or military purposes. Therefore, quantum technology was designated as a "fundamental technology" and "emerging technology" that is essential for US national security in the "Export Control Reform Act 2018"

(ECRA) in the "National Defense Authority Act for Fiscal Year 2019." ECRA calls for review of the scope of licensing requirements for a "comprehensive arms embargo" and an assessment of licensing exceptions for exports to, re-exports to, and transfers to, the same country.

In September 2020, China's Ministry of Commerce issued its own regulations regarding an "unreliable entity list." On October 17, the "Export Control Law of the People's Republic of China" was adopted at the 22nd session of the 13th NPC Standing Committee, and it will go into force on December 1. The law implements export control measures and list regulations based on China's "overall national security view." The government has also begun to regulate the import and export of information technology, mainly through the Ministry of Industry and Information Technology and the Cyberspace Administration of China.

Japan-US Cooperation for the Quantum Internet

There are three areas in which Japan and the United States can or should cooperate. First, the most important thing is to overcome physical difficulties and connect the quantum networks of Japan and the United States. To communicate over long distances, it is necessary to send quantum entanglements while correcting for errors. However, due to the limitations of low-altitude satellites, it is impossible to link the quantum networks of Japan and the US through a single satellite as China does.

Therefore, many satellites should be connected, or many quantum repeaters[25] must be installed every few tens of kilometers in the sea. Japanese researchers have suggested physically transporting one side of the quantum entanglement in large quantities in containers. The key to challenging China's future hegemony over quantum physics is solving these technical problems between Japan and the United States.

Second, Japan and the United States, and other like-minded countries, must unite to protect core technologies and products of the quantum internet through export controls, in particular "Military End-Use and Military End-User Regulations."

[25] A node in the quantum internet which communicates and manages quantum states.

As noted, even if a third country has a quantum repeater or computer, the confidentiality of communications can be maintained. And, in today's Internet, there is no principle of not connecting with other countries in peace time because of a fear of attacks on networks, infrastructure, or devices. This doesn't mean we shouldn't use products from third countries or networks with other countries. To use them safely, the important thing is to design secure protocols and hardware.

Third, it is necessary to establish international rules to ensure the safety of quantum networks under the Japan-US alliance and install a security system for the quantum Internet era.

「量子覇権」を目指す中国と日米協力

土屋貴裕

「量子覇権」を目指す中国

2020年10月16日、中共中央政治局第24回全体学習会議を習近平が主宰した[1]。この学習会の目的は、「世界の量子技術の開発動向を理解し、中国の量子技術の開発状況を分析し、中国の量子技術の開発をより促進すること」である。

習近平は、「量子技術の発展は、重大な意義があることを深く認識し、量子技術の発展のための戦略的計画やシステムレイアウトを強化しなければならない」と述べた。そのためには、「中国の量子技術の開発をより促進すること、基礎研究を進めてコア技術を獲得すること、ハイレベル人材育成、産官学の共同研究によるイノベーション、国際協力を促進すること」などと強調した。

その上で、習近平は、「量子通信などの戦略的新興産業を育成し、量子技術の国際競争において圧倒的な高地（優勢）を押さえ、新しい開発の利点を構築せよ」と述べており、今後、中国の量子科学技術の研究開発および投資が一層加速すると見られる[2]。

[1] "Xi Focus: Xi stresses advancing development of quantum science and technology," Xinhua News Agency, 18 October 2020. <http://www.xinhuanet.com/english/2020-10/18/c_139448027.htm>

[2] 中国は「量子覇権」の争奪戦において「戦局」を主導することを目指している。
詳しくは、以下を参照。「全球“量子霸权”争夺战观察」新華網、2018年2月14日、
<http://www.xinhuanet.com/science/2018-02/14/c_136972095.htm>、
および Elsa B. Kania, John Costello, "Quantum Hegemony?: China’s Ambitions and the Challenge to U.S. Innovation Leadership," Center for a New American Security, 12 September 2018. <https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf>

中国における量子に関する研究機関と産業チェーン

中国の量子情報科学技術（量子技術）分野における研究機関としては、「BATH」と呼ばれるバイドゥ（百度）、アリババ（阿里巴巴）、テンセント（騰訊）、ファーウェイ（華為）といった民間企業の研究所のほか、政府や大学の研究機関として、中国を代表する「量子の父」潘建偉が所属する中国科学技術大学や、上述の学習会で報告を行った薛其坤・清華大学副校長が院長を務める北京量子情報科学研究院など、複数の国家重点実験室が存在している[3]。また、北京璞匯軍民融合装備技術中心 北京金泰衆和科技有限責任公司、武漢船舶通信研究所（722 所）など、量子鍵配送 (Quantum Key Distribution：QKD) による量子暗号通信ネットワークの分野でも、軍民融合によるいくつかの企業や研究機関が存在している。

中国では、量子通信ネットワークの構築に伴って、量子通信に関する産業チェーンも構築されつつある。量子通信の産業チェーンについては、量子通信コアデバイス製造、量子通信設備製造、量子通信伝送ネットワークの建設・管理、量子通信ネットワークのオペレーション、アプリケーションの提供といった上流から下流まで、各段階で様々な企業や国の機関が関わっている。

量子暗号通信ネットワークの構築を進める中国

少なくとも中国が日米に先行しているのは、量子通信衛星や光ファイバーネットワークを用いたセキュアな量子プロトコルの検証と量子暗号通信ネットワーク構築である。2016 年 8 月、中国は量子科学実験衛星「墨子号」の打ち上げに世界で初めて成功した。また、中国は地上における量子機密通信幹線を敷設することによる量子暗号通信ネットワークの構築も力を入れている。量子機密通信幹線は、国家の中枢を担う重要インフラ網を他国のサイバー攻撃から防御する狙いがある。

[3] Strider Global Intelligence Team, "QUANTUM DRAGON," Strider, November 2019. <https://www.strider.tech/resources/quantum-dragon-report/>

また、中国の場合は軍事利用も主目的の 1 つであり、この量子暗号通信ネットワークには中国人民解放軍の 7 大戦区の司令部などが含まれている。

安全かつ解読困難な量子通信ネットワークを構築することで、サイバー攻撃の脅威から機密情報を守ることが可能となる。未来のクラウド量子計算は、ブラインド量子計算と量子インターネット（現行の量子暗号通信ネットワークよりも高度な量子通信が可能な地球規模ネットワーク）によって、中国やその他の国の量子コンピュータであっても安心して使用することができるようになるだろう。ただし、中国はそうした量子コンピュータのみならず、量子通信ネットワークを国際的に提供することを意図している。もしそうなれば、中国に衛星やネットワークインフラ自体を依存することになるだろう。

量子インターネットでは、量子デバイスへの攻撃だけでは、セキュリティが破れないため、通信を阻害することしかできない。ただし、量子ネットワーク上の通信は安全性が確保されていても、量子ネットワークのインフラ自体は堅牢ではない。悪意のあるノードによるインフラ攻撃は、正常なノードが悪意ある、もしくは故障していると判断され、ネットワークから隔離されてしまう危険性がある。また、転送中の量子ビットが盗まれ、対応している古典通信（古典インターネットを介した通信）も特定・盗聴されている場合には、量子ネットワークのセキュリティも破られる可能性がある。しかも、そうした攻撃は、量子ネットワークのセキュリティを逆用しているため、犯人特定が難しく、古典通信よりも脅威が増大するかもしれない[4]。

量子技術の応用分野と安全保障利用

量子技術は、コンピューティングや暗号、通信・インターネット、テレポーテーションを用いた通信・量子インターネットのみならず、レーダーやセンサなどの分野にも応用可能性が広がっている。中国は、「量子覇権」を握るため、そうし

[4] T. Satoh, et al. "The network impact of hijacking a quantum repeater," Quantum Science and Technology 3.3 (2018): 034008.

た量子レーダーや量子センサの分野に関しても、大学・研究機関や企業で研究が進められている。特に注目すべきは、軍の大学や軍事産業が積極的に関わっている点である。将来的には、単一光子量子レーダーの開発によって、電子戦におけるステルス・プラットフォームの標的を検知・捕捉したり、量子慣性センサの開発によって、深海における潜水艦の航法を向上させたりするなど、解読が困難な量子暗号を用いた量子通信のみならず、通常兵器の生存に向けた応用シーンも想定されている。

また、2018 年、中国では潘建偉のグループが天体間量子通信関連の実験に成功している[5]。この実験に関する論文に基づけば、墨子に続き、天体間量子通信のための量子衛星を L4 と L5 のラグランジュポイントに置く可能性がある。中国は月面の有人探査や宇宙ステーション（月面基地）建設構想も有している。月面基地を建設することで、地球上の定点監視や地球との量子衛星を通じた暗号通信が可能になる。月面基地からのサイバー攻撃やミサイルの遠隔操作など、軍事利用も想定されるだろう。さらに、そうした量子衛星を保護するために、衛星破壊兵器（ASAT）を使用する可能性もあり、中国による量子技術を用いた宇宙の軍事利用が懸念される。ジョン・レイモンド米宇宙作戦部長が指摘するように、「宇宙はもはや平和的空間ではなく戦闘領域」になりつつあると言えよう。

中国の量子戦略と軍民融合発展戦略に基づくネットワークの構築

上述の通り、中国は、国内全土に量子暗号通信ネットワークを構築しようとしている。これは 2014 年に中国の科学者等によって提示された中長期的な計画に基づいている。中国は、2020 年中にアジア・欧州間の量子パスワード伝送を実現し、これによりアジアと欧州を結ぶ大陸間量子通信ネットワークを構築することを計画している。また、2030 年頃には、グローバル化された広域量子暗号通信ネット

[5] C. Yuan, et al. "Bell Test over Extremely High-Loss Channels: Towards Distributing Entangled Photon Pairs between Earth and the Moon," Physical Review Letters 120 (2018): 140405.

ワークを構築した上で、情報が安全に伝送できる量子ネットワークを構築し、整った量子通信産業チェーンを形成することを掲げている。

特筆すべきは、中国は「軍民融合発展戦略」の下で、量子技術の研究開発および軍事利用を進めようとしている点である。とりわけ、軍事用の通信指揮専門ネットワーク（C4ISR）は、現代の軍の神経中枢であり、暗号化が必要となる。こうした軍事用通信指揮専用ネットワークの構築のため、2018 年には 1,000 億人民元超を投入しており、将来的には、量子通信の暗号化を採用して絶対的な安全性の確保を目指していると見られる。

このように、量子技術は他のゲームチェンジャー技術と同様に、軍民融合の進展により、最終需要者（民間か否か）、あるいは最終用途（民生用か否か）に係る判断が困難になっている。そのため、量子技術については、米国の 2019 会計年度の「国防権限［授権］法」に盛り込まれた「輸出管理改革法」（ECRA：Export Control Reform Act of 2018）で、米国の国家安全保障上重要な技術である「基盤的技術」（Foundational Technologies）および先進的な「新興技術」（Emerging Technologies）の 1 つに指定された。ECRA では「包括的武器禁輸国」に対する輸出、再輸出、同一国内移転について、「軍事エンドユース、軍事エンドユーザー規制」の許可要件の範囲の検討、許可例外についての要件見直しを求めている。

一方、中国も、2020 年 9 月、中国商務部は「信頼できないエンティティリスト」に関する規定を公表した。また、10 月 17 日には、第 13 期全人代常務委員会第 22 回会議で「中華人民共和国輸出管理法」が可決、成立し 12 月 1 日に施行される。同法は、中国の「総体国家安全観」に基づいて、他国への輸出管理措置やリスト規制の実施するものである。さらに、工業情報化部インターネット弁公室を中心に、情報技術の調達に関する輸出入規制に着手している。

量子インターネット時代に向けた日米協力の必要性

そうした中で、特に日本と米国が協力できる、あるいは協力すべき点は、3 つある。

第 1 に、何よりも重要なのは、物理的な困難を乗り越えて、日米の量子通信ネットワークを接続することにある。長距離間の量子通信を行うためには、エンタングルメントのエラーを修正しながら送る（量子中継を行う）必要がある。しかし、低高度衛星の限界から、日米間の量子ネットワークを中国のように単一の衛星を介して繋ぐことはできない。そのため、多数の衛星同士を繋ぎ合わせるか、海中に数十キロメートルごとに多数の中継ノード（量子中継器）を設置することになるだろう。また、量子通信資源（エンタングルメントの片側）を大量・継続的にコンテナなどで物理的に輸送するという方法もあるだろう。こうした技術的問題を日米でいかにクリアしていくかが、今後の量子をめぐる中国の覇権に対抗する上で、最も重要であると考えられる。

第２に、安全保障輸出管理面で、量子インターネットのコア技術および製品に関する「軍事エンドユース、軍事エンドユーザー規制」を行うべく、日米をはじめ、同盟国や協力国による協力が必要である。

もちろん、上述の通り、量子中継器や量子コンピュータが第三国のものであったとしても、通信の機密性は保たれる。また、古典インターネットがそうであるように、ネットワークやインフラ、デバイスへの攻撃を恐れて、平時に他国と繋がないという原則はない。つまり、第三国の製品を使わなければよい、あるいは他国とのネットワークを接続しなければよいという訳ではない。そこで、第３に、日米同盟のもとで、量子ネットワークの安全性を確保するための国際的なルールを形成していくとともに、量子インターネット時代の安全保障体制を構築していく必要ことが望まれる。

LEVERAGING THE PRIVATE SECTOR IN JAPAN'S ECONOMIC SECURITY POLICY

By Mariko Togashi

Japan's economic security policy is becoming increasingly important due to the expanding intersection of economics and national security. In April 2020, Tokyo established an economic division in the National Security Secretariat (NSS) in light of China's rising influence, leveraging its economic tools to achieve strategic goals.[1] The ruling Liberal Democratic Party is currently planning to establish a comprehensive economic security policy and economic alliances with like-minded countries.[2] While Tokyo is making significant progress in this endeavor, a key area where it falls short is in addressing the private sector's concerns. The private sector's concerns include: balancing security and profits, the lack of budget, the shortage of expertise, and the lack of information protection standards. Although the private sector is not a traditional player in security, due to its critical role in the technology field, which is the key to Japan's economic security policy, its concerns must be considered. Therefore, the Japanese government should take steps to more thoroughly incorporate the private sector in its economic security policymaking.

The Importance of the Technology Sector in Economic Security Policy

Technology is at the core of Japan's economic security policy. The NSS's new economic division lists a number of focus areas that are strategically important for Japan, such as telecommunications, export controls on technology and strategic products, and digital currency.[3] Pushing Tokyo's development of an economic security strategy is China's rise and ambition in the technology field, evidenced by initiatives like "Made in China 2025" and "China

[1] "国家安保局に「経済班」発足　新型コロナ対応も急務," Nikkei, April 1, 2020, https://www.nikkei.com/article/DGXMZO57510630R00C20A4PP8000/

[2] "経済安保推進法制定を　国家戦略確立へ中間まとめ―自民、政府に年内提言へ," Jiji.com, September 28, 2020, https://www.jiji.com/jc/article?k=2020092700241&g=eco

[3] "経済安保、デジタル通貨・土地取引にも拡大　米には連携打診," Nikkei, March 18, 2020, https://www.nikkei.com/article/DGXMZO56920550X10C20A3PP8000/

Standards 2035."[4] China's research and development (R&D) spending surpassed that of Japan more than a decade ago and has almost caught up with the United States.[5] China has also increased the number of scientific papers: China released 19.9% of the global total between 2016 and 2018, surpassing the United States at 18.3%.[6]

In response to Beijing's rise and the U.S.-China competition, Tokyo is bolstering its efforts to develop and protect its technology through multiple approaches. The Cabinet Office announced a new guideline for universities and research institutions to stop the unintentional technology drain in 2019 and expanded the scope of disclosure obligations for funding sources to research labs.[7] Moreover, Tokyo revised the Foreign Exchange Law in November 2019 to increase the scrutiny placed on inbound foreign direct investments in the fields that relate to national security, including nuclear energy, electricity, and telecommunication.[8] On the research side, Tokyo is planning to establish a think tank to apply advanced commercial technologies, such as quantum technology and AI, to the national security field in FY 2021.[9]

Japan's Private Sector Plays a Critical Role in the Technology Field

Japan's private sector is at the forefront of strategic competition in the technology field, especially in game-changing technologies. AI, semiconductors, technologies related to Connected Industries, and personal technologies are all developed and possessed by private

[4] Kennedy, S., "Made in China 2025," Center for Strategic & International Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025; Kharpal, A., "Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech," CNBC, April 26, 2020, https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html

[5] OECD, Research and Development Statistics (RDS), https://www.oecd.org/sti/inno/researchanddevelopmentstatisticsrds.htm

[6] "China passes US as world's top researcher, showing its R&D might," Nikkei Asia, August 8, 2020, https://asia.nikkei.com/Business/Science/China-passes-US-as-world-s-top-researcher-showing-its-R-D-might

[7] "大学・国立研究開発法人の外国企業との連携に係るガイドライン―適正なアプローチに基づく連携の促進―（中間とりまめ）," Cabinet Office, June 21, 2019, https://www8.cao.go.jp/cstp/openinnovation/procurement/guideline.pdf; "外国の資金協力、科研費にも開示義務　経済安保で厳格化," Nikkei, September 29, 2020, https://www.nikkei.com/article/DGXMZO64345400Y0A920C2PP8000/

[8] "改正外為法が成立　安保上重要な企業への出資規制," Nikkei, November 22, 2019, https://www.nikkei.com/article/DGXMZO52473470S9A121C1MM0000/

[9] "政府、安保で新シンクタンク　民間技術転用を研究," Nikkei, January 19, 2020, https://www.nikkei.com/article/DGXMZO54579280Z10C20A1NN1000/

companies. Furthermore, the expansion of dual-use technologies makes the private sector even more important in Japan's technology sector.[10]

The significance of Japan's private sector in the technology field is clear in data as well. In R&D funding, Japan's private sector accounted for 78 percent of national R&D in 2017, which was the highest among G7 economies.[11] Moreover, Japan used 97 percent of its total national science and technology budget for commercial technologies in 2016-2018,[12] in contrast to the U.S., which spent 55% of the total science and technology budget on commercial technologies in 2019.[13]

Addressing the Private Sector's Concerns

The significance of the private enterprise in Japan's technology sector implies that effective economic security policy should address the private sector's concerns. From the Japanese business perspective, four major issues impact Japan's economic security agenda: profit vs. security, lack of adequate budget, lack of expertise, and lack of information protection standards.

First, one of the private sector's main concerns is the possibility of losing business opportunities. While aware of the growing need to better protect business data, companies nevertheless want to avoid losing foreign business opportunities due to overly tight economic security policy measures such as export controls, investment restrictions, and restrictions on production location.

While it may seem that private firms and Japan's government are working together to balance security and profits, the reality is that recent cooperation reflects needs arising from the

[10] Kanehara, N., "科学技術と安全保障　民生技術の管理・育成が急務," Nikkei, April 10, 2020, https://www.nikkei.com/article/DGXKZO57867440Z00C20A4KE8000/
[11] OECD, Research and Development Statistics (RDS), https://www.oecd.org/sti/inno/researchanddevelopmentstatisticsrds.htm
[12] National Institute of Science and Technology Policy, 政府の予算, https://www.nistep.go.jp/sti_indicator/2019/RM283_12.html
[13] American Association for the Advancement of Science, Historical Trends in Federal R&D, https://www.aaas.org/programs/r-d-budget-and-policy/historical-trends-federal-rd

COVID-19 pandemic. Japan announced to distribute subsidies for companies to re-shore operations, and the total amount of funds requested was 11 times the approved budget for the October round.[14] Although this suggests a certain level of consensus between the private and public sectors when addressing economic security, in fact, corporate decision-making reflected a desire to avoid supply chain disruption due to the pandemic rather than strategic calculations. The subsidy targeted health-related businesses and firms that have a high concentration of production in specific countries. Since the pandemic has obscured the potential conflict between security and profits, striking a balance between them will be even more critical in the future.

Second, companies may not have sufficient budgets to engage in economic security strategy-making, especially given a large number of small- and medium-sized enterprises (SMEs) in Japan. While the private sector is at the forefront of economic security threats, economic security is a new agenda for most companies and will require additional budgets. The surge in the cybersecurity budgets is one example of how they must deal with new threats.

Third, the lack of expertise in economic security is critical for Japanese companies. Most Japanese companies do not have sufficient government relations divisions nor economic security divisions. Moreover, the fundamental problem is that human resources in the economic security field are scarce in general. Recently, Mitsubishi Electric Corporation has established the Corporate Economic Security Division "to comprehensively manage economic security risks throughout the entire company's business, including exports, information security, investments and development."[15] Although the new division hints at a new trend of companies' paying greater attention to economic security, it does not necessarily mean that they can attain adequate expertise immediately. Furthermore, the lack of both expertise and budget may delay or stop the spread of this trend.

[14] "コロナで生産回帰 補助金競争率 11 倍　マスクや医薬品," Nikkei, September 8, 2020, https://www.nikkei.com/article/DGXMZO63583090Y0A900C2EE8000/
[15] "Mitsubishi Electric to Change Executive Officer's Duties and Organization," Mitsubishi Electric Corporation, September 16, 2020, https://www.mitsubishielectric.com/news/2020/pdf/0916.pdf

Finally, the lack of systems to protect sensitive data hinders Japanese companies from building business relationships with foreign partners. Economic security requires business-to-business partnerships based on the alliance of like-minded countries. However, the current lack of information-protection systems makes it difficult for companies to develop business partnerships in sensitive technology. Currently, Tokyo is moving toward establishing a security clearance system, including the private sector.[16]

Policy Recommendations

While making significant progress in the economic security field, Tokyo should address the concerns of the private sector to make economic security policy effective. Tokyo should communicate more with the private sector, increase its communication between bureaucratic divisions, incentivize the private sector to establish and develop their economic security division, build a knowledge-sharing network for the private sector, and provide a business base that companies can rely on through partnering with like-minded countries.

First, Tokyo should bolster its communication with the private sector in order to better understand the technology sector and to discuss economic security with them. Almost all advanced technologies are in the hands of companies. In addition to large companies, this communication should include SMEs and start-up companies since both possess many emerging or sensitive technologies, which can lead to game-changing technological breakthroughs. Continuous communication may generate a sense of responsibility in the private sector and may lead to a consensus between the public and the private sector in economic security policy-making.

Second, Japan should deepen its communication among ministries.[17] Although Tokyo recognizes the importance of knowing the overall science and technology field, stove-piping of government bureaucracy makes it difficult for Tokyo to understand the overall picture of the

[16] "先端技術者の信用度に資格新設へ　中国への警戒感にじむ," Asahi Shimbun, August 13, 2020, https://www.asahi.com/articles/ASN8D76FBN8DUTFK003.html
[17] Kanehara, N., "科学技術と安全保障　民生技術の管理・育成が急務," Nikkei, April 10, 2020, https://www.nikkei.com/article/DGXKZO57867440Z00C20A4KE8000/

technology field.[18] Especially given the expansion of dual-use technologies, deeper communication and collaboration are necessary to incorporate the private sector into economic security policy-making.

Third, the Japanese government should incentivize the private sector to take the initiative in economic security. While Mitsubishi Electric Corporation's establishment of the new economic security division shows the beginning of a new trend of the private sector's interest in the economic security field, not all companies have enough budgets and human resources. Since economic security policy has to cover numerous technologies, an effective economic security policy requires a proactive private sector. To achieve this, Tokyo must incentivize companies through measures such as subsidies and tax credits. In the long run, Japan should establish a sustainable system to ensure that companies can make changes needed to align with national economic security policy.

Fourth, Tokyo should facilitate discussions between companies to share basic knowledge of economic security within specific fields. Since each technology field has a different landscape, players, restrictions, and supply chains, it is unrealistic for the government to cover every detail. Therefore, Tokyo's goal should be to create a platform for companies to share basic information and find the optimal points of economic security policy enforcement. Tokyo should utilize organizations such as the Japan External Trade Organization (JETRO) to take initial steps.

Finally, Japan should work to ensure a friendly business environment for companies' overseas business through partnering with like-minded countries. Given the expansion of strategic competition, Tokyo should identify which technology sectors Japan can cooperate on with which country. Specifically, Japan should increase the number of specific technology sub-fields in which it can cooperate with the U.S. to provide a solid base for corporate decision making and to find the right balance between globalization and protectionism.[19] A blanket statement

[18] Integrated Innovation Strategy, Japan's Ministry of Education, Culture, Sports, Science and Technology, June 15, 2018, https://www.mext.go.jp/content/1414951_005.pdf
[19] Schoff, J. L., "U.S.-Japan Technology Policy Coordination: Balancing Technonationalism With a Globalized World," Carnegie Endowment for International Peace, June 29, 2020,

of identifying allies and enemies does not help companies make business decisions. For instance, the supply chain initiative that Japan launched with India and Australia, which intends to achieve supply chain resilience in the Indo-Pacific region in response to China's increasing influence, is a good example of specifying a sector and partner countries.[20]

Furthermore, deepening alliances requires that Tokyo ensure data protection through multiple approaches. Tokyo should maintain its timeline for the security clearance bill and prepare to provide companies with concrete operational guidelines in the interim. Japan should also focus on the implementation of measures to block technology leakage through universities and research institutions. Although METI required universities to establish new divisions dedicated to protecting technology, only around 60% of Japanese universities have complied so far.[21] In addition to the creation of the security clearance system and better protecting technology in universities, Tokyo should establish a new guideline for companies to protect technology.

Given the importance of the private sector in Japan's technology field, the government's ability to address the private sector's concerns may determine the effectiveness of Japan's economic security policy.

---

https://carnegieendowment.org/2020/06/29/u.s.-japan-technology-policy-coordination-balancing-technonationalism-with-globalized-world-pub-82176

[20] "Japan, Australia and India to launch supply chain initiative," Bloomberg, August 31, 2020, https://www.bloomberg.com/news/articles/2020-09-01/japan-australia-and-india-to-discuss-supply-chains-alliance

[21] "公私立大、輸出管理部署設置は６割　技術流出、対策進まず," Sankei Shimbun, October 14, 2020, https://www.sankei.com/life/amp/201014/lif2010140037-a.html

日本の経済安全保障政策における民間セクターの活用

富樫真理子

経済と安全保障との接点が拡大するにつれて、日本の経済安全保障政策が益々重要なものとなってきている。日本政府は、中国の影響力拡大、とりわけ、戦略的目標のための経済的手段の利用拡大を踏まえ、2020 年 4 月、国家安全保障局（NSS）に経済班を設置した[1]。自民党は、現在、包括的な経済安全保障推進法の制定、価値観を共有する国々との経済連携樹立を目指している[2]。経済安全保障分野での日本政府の取り組みが迅速に進む一方で、民間セクターが直面する課題への対応は十分ではない。民間企業は、安全保障と企業利益の均衡、経済安全保障分野の予算確保、専門知識の不足、情報保護基準の欠如といった課題に直面しよう。民間セクターは、従来、安全保障分野において主体的な役割は担ってこなかったが、日本の経済安全保障政策の鍵となる技術分野において中心的な役割を担っているため、民間企業の課題を考慮する必要があろう。日本政府は、経済安全保障政策の政策形成段階で、民間セクターをより積極的に取り込むべきである。

経済安全保障政策における技術分野の重要性

技術分野は日本の経済安全保障政策の中核を成している。NSS に新たに設置された経済班は、通信、技術や戦略的重要性を有する製品の輸出規制、デジタル通貨など、日本にとって戦略的に重要な分野を定めている[3]。日本の経済安全保障戦略の背景にあるのは、「Made in China 2025」や「China Standards 2035」等に見られる、

[1] “国家安保局に「経済班」発足　新型コロナ対応も急務,” Nikkei, April 1, 2020, https://www.nikkei.com/article/DGXMZO57510630R00C20A4PP8000/
[2] “経済安保推進法制定を　国家戦略確立へ中間まとめ―自民、政府に年内提言へ,” Jiji.com, September 28, 2020, https://www.jiji.com/jc/article?k=2020092700241&g=eco
[3] “経済安保、デジタル通貨・土地取引にも拡大　米には連携打診,” Nikkei, March 18, 2020, https://www.nikkei.com/article/DGXMZO56920550X10C20A3PP8000/

技術分野での中国の台頭と野心である[4]。中国の研究開発（R&D）費は十年以上も前に日本を上回り、今やアメリカに追いつこうとしている[5]。また、科学論文数も増加しており、中国は 2016 年から 2018 年の間に世界全体の論文数の 19.9%を発表し、アメリカの 18.3%を上回った[6]。

中国の台頭と米中競争に応じ、日本政府は様々なアプローチで技術の開発、流出防止に向けた取り組みを加速させている。内閣府は、2019 年に大学や研究機関による意図せざる技術流出を防ぐため、新たなガイドラインを発表するとともに、資金源の開示義務の適用範囲を研究機関にまで拡大した[7]。また、日本政府は 2019 年 11 月に外為法を改正、原子力、電力、通信などの安全保障分野に関わる企業への対日直接投資の規制を強化した[8]。研究開発に関しては、量子技術や AI 等先端民間技術を安全保障分野に応用することを目的としたシンクタンクを 2021 年度に設立する予定である[9]。

日本の技術分野において、中心的な役割を担うのは民間セクター

日本の民間セクターは、技術分野、特に革新的技術における戦略的競争の最前線にいる。例えば、AI、半導体、コネクテッド・インダストリーズ関連技術、個人

---

[4] Kennedy, S., "Made in China 2025," Center for Strategic & International Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025; Kharpal, A., "Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech," CNBC, April 26, 2020, https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html

[5] OECD, Research and Development Statistics (RDS), https://www.oecd.org/sti/inno/researchanddevelopmentstatisticsrds.htm

[6] "China passes US as world's top researcher, showing its R&D might," Nikkei Asia, August 8, 2020, https://asia.nikkei.com/Business/Science/China-passes-US-as-world-s-top-researcher-showing-its-R-D-might

[7] "大学・国立研究開発法人の外国企業との連携に係るガイドライン―適正なアプローチに基づく連携の促進―（中間とりまめ）," Cabinet Office, June 21, 2019, https://www8.cao.go.jp/cstp/openinnovation/procurement/guideline.pdf; "外国の資金協力、科研費にも開示義務　経済安保で厳格化," Nikkei, September 29, 2020, https://www.nikkei.com/article/DGXMZO64345400Y0A920C2PP8000/

[8] "改正外為法が成立　安保上重要な企業への出資規制," Nikkei, November 22, 2019, https://www.nikkei.com/article/DGXMZO52473470S9A121C1MM0000/

[9] "政府、安保で新シンクタンク　民間技術転用を研究," Nikkei, January 19, 2020, https://www.nikkei.com/article/DGXMZO54579280Z10C20A1NN1000/

用技術といった先端技術は、全て民間企業が開発、保有している。さらに、軍民両用技術の拡大により、民間セクターは日本の技術分野において従来以上に重要な役割を担っている[10]。

技術分野における、日本の民間企業の重要性はデータからも見て取れる。日本全体の研究開発費のうち、78%を民間セクターが占めており（2017 年データ）、これは G7 の中で最も高い比率である[11]。また、科学技術関連予算においては、日本は 97%を商用技術に充てており（2016—2018 年）[12]、アメリカの商用技術比率 55%（2019 年）とは対照的である[13]。

民間セクターの課題

日本の技術分野における民間セクターの重要性は、効果的な経済安全保障政策形成において民間セクターの課題が重要であることを示唆していよう。経済安全保障において、日本のビジネス界は、安全保障と利益の均衡、経済安全保障分野の予算確保、専門知識の不足、情報保護基準の欠如という、四つの課題に直面しよう。

第一に、民間企業は、経済安全保障政策の進展により、ビジネスの機会を失う可能性を懸念しよう。企業は、データ保護の必要性を認識する一方で、輸出、投資、生産地に関する規制が過度に厳しくなり海外での商業機会を失う可能性を懸念しよう。

---

[10] Kanehara, N., “科学技術と安全保障　民生技術の管理・育成が急務,” Nikkei, April 10, 2020, https://www.nikkei.com/article/DGXKZO57867440Z00C20A4KE8000/
[11] OECD, Research and Development Statistics (RDS), https://www.oecd.org/sti/inno/researchanddevelopmentstatisticsrds.htm
[12] National Institute of Science and Technology Policy, 政府の予算, https://www.nistep.go.jp/sti_indicator/2019/RM283_12.html
[13] American Association for the Advancement of Science, Historical Trends in Federal R&D, https://www.aaas.org/programs/r-d-budget-and-policy/historical-trends-federal-rd

国内生産回帰のための補助金の例から見るに、安全保障と企業利益の均衡に関し、民間企業は今のとこと政府方針と齟齬がないように見えるが、これはコロナ対策の必要性を反映したものである可能性があろう。政府は国内生産回帰促進のための補助金交付を発表したが、10月分の予算について、予算額の11倍にも上る申請があった[14]。この例からは、経済安全保障への取り組みにおいて、官民の間で一定のコンセンサスがあるように見えるが、実際には、企業の意思決定において戦略的な計算よりも、サプライチェーンの混乱回避が優先された可能性があるだろう。同補助金は、特定の国に生産拠点が集中している、もしくは国民の健康に重要である製品、素材が対象となっていた。パンデミックにより、経済安全保障における、安全保障と企業利益の潜在的な衝突が不透明となったため、今後は両者のバランスを取ることがより重要となろう。

第二に、経済安全保障関連予算の確保が民間企業の懸念事項となろう。特に、日本では中小企業の数が多いことを踏まえると、この点は重要である。経済安全保障は、民間企業が前線に立つ領域であるにも関わらず、企業にとっては新たな課題であり、新たな予算が必要となる。サイバーセキュリティ関連予算の増額は、民間企業がどのように新たな脅威に対処すべきか示唆している。

第三に、民間セクターにおける経済安全保障の専門知識は十分でないと考えられる。日本企業の多くは、十分な政府渉外部署や経済安全保障部署を設けていない。さらに言えば、根本的な問題は、経済安全保障分野の人材が全般的に不足していることである。今般三菱電機は「輸出、情報セキュリティ、投資、開発等に関わる経済安全保障の観点から見たリスク制御を統合的に行う」ために、経済安全保障統括室を設置した[15]。この経済安全保障統括室の新設は、企業が経済安全保障を重視する新たな傾向の兆候ではあるが、直ちに十分な専門家を揃えることは難

[14] “コロナで生産回帰 補助金競争率11倍　マスクや医薬品,” Nikkei, September 8, 2020, https://www.nikkei.com/article/DGXMZO63583090Y0A900C2EE8000/
[15] “Mitsubishi Electric to Change Executive Officer’s Duties and Organization ,” Mitsubishi Electric Corporation, September 16, 2020, https://www.mitsubishielectric.com/news/2020/pdf/0916.pdf

しいだろう。また、専門知識と予算の不足は、企業が経済安全保障分野に経営資源を注ぐ傾向の広がりの足かせとなりうる。

最後に、日本では機密情報を保護する枠組みが整っていないため、日本企業にとって、海外パートナーとの取引関係構築が難しい局面があろう。価値観を共有する国々との企業間パートナーシップは、経済安全保障において最重要であるにも関わらず、情報保護体制が整備されていない現状では、機微技術分野でのビジネス・パートナーシップの構築は困難である。現在、日本は民間を含めたセキュリティ・クリアランス制度設立に向けて動き出している[16]。

政策提言

日本政府は、経済安全保障政策を大きく進展させているものの、より効果的な政策形成のために、民間企業の課題に対応するべきである。日本政府は、民間セクターとのコミュニケーション強化、官庁間のコミュニケーション強化、民間部門の経済安全保障部署の設置及び強化の奨励、民間セクターの知識共有のためのネットワーク構築、価値観と共有する国々との提携を通じたビジネス基盤作りに注力すべきである。

第一に、技術分野への理解を深め、経済安全保障議論を深化させるため、日本政府は、先端技術の大部分を有する民間企業とのコミュニケーションを強化すべきである。日本には、企業規模に関わらず革新的技術につながりうる技術を有する企業が多く存在している。このため、大企業のみならず、中小企業やスタートアップ企業も含めたコミュニケーション強化が必要である。また、継続的なコミュニケーションにより、民間セクターに経済安全保障の観点からの責任感が生まれ

[16] “先端技術者の信用度に資格新設へ　中国への警戒感にじむ,” Asahi Shimbun, August 13, 2020, https://www.asahi.com/articles/ASN8D76FBN8DUTFK003.html

れば、経済安全保障政策形成段階における官民のコンセンサスを生み出すことも可能であろう。

第二に、日本は省庁間のコミュニケーションを強化すべきである[17]。日本政府は技術分野の全体像を把握することの重要性を認識している一方で、官僚の縦割り構造によりその全体像を把握することが困難となっている側面があろう[18]。特に、軍民両用技術の広がりを踏まえれば、より深いレベルのコミュニケーションと連携により、経済安全保障政策形成において民間セクターを取り込むことの必要性は高まろう。

第三に、日本政府は、民間企業が経済安全保障分野において積極的な役割を果たすよう促すべきである。三菱電機の経済安全保障統括室の新設は、民間の経済安全保障への関心の高まりを示すものではあるが、全ての企業が十分な予算と人材を有している訳では無い。経済安全保障政策は多様な技術分野を網羅しなければならないため、効果的な経済安全保障政策を実行するには、民間セクターの積極的な取り組みが不可欠である。そのためには、日本政府が補助金や税額控除などの措置を通じて民間企業にインセンティブを与える必要があろう。長期的には、企業が国の経済安全保障政策に呼応して必要な措置をとることが出来るような、持続可能な枠組みを構築すべきである。

第四に、日本政府は特定の分野における経済安全保障の基礎知識を共有するために企業間の議論を促進すべきである。特定の技術分野ごとに特徴、関係者、規制、サプライチェーンが異なるため、政府がすべての詳細を網羅することは非現実的である。したがって、日本政府が目指すべき目標は、企業が基本的な情報を共有し、経済安全保障政策の最適な実施方法を見出すためのプラットフォームを作る

[17] Kanehara, N., “科学技術と安全保障　民生技術の管理・育成が急務,” Nikkei, April 10, 2020, https://www.nikkei.com/article/DGXKZO57867440Z00C20A4KE8000/
[18] Integrated Innovation Strategy, Japan’s Ministry of Education, Culture, Sports, Science and Technology, June 15, 2018, https://www.mext.go.jp/content/1414951_005.pdf

ことである。日本政府は、まず日本貿易振興機構（ジェトロ）などの組織を活用して、これらの課題に取り掛かるべきである。

最後に、日本は、価値観を共有する国々との連携を通じて、企業の海外事業に好適な環境の確保に努めるべきである。戦略的競争の拡大を踏まえ、日本はどの技術分野でどの国と協力できるかを明確にすべきである。特に、企業の意思決定のための強固な基盤を提供し、グローバリゼーションと保護主義の均衡を取るために、日本がアメリカと協力できる技術範囲を拡大すべきである[19]。敵対国と同盟国、と分けるような単純な線引きは、企業の経営判断の助けにはならない。例えば、中国の影響力の拡大に対応するために、日本がインド及びオーストラリアと共同で開始したインド・太平洋地域でのサプライチェーンのレジリエンスを高めようとする取り組みは、協力国と協力分野を具体的に示した好例である[20]。

さらに、国家間連携を深化させるため、日本政府は複数のアプローチで、情報保護を確実にすることが必要である。日本は現在示されているタイムラインに沿ってセキュリティ・クリアランス制度の導入を進め、その間に企業に具体的な運用ガイドラインを提供する準備を進めるべきである。また、大学や研究機関を通じた技術流出防止策の実施にも注力すべきである。経済産業省は大学に技術流出防止のための専門部署の新設を求めたが、これまでに約 6 割の大学しか対応できていないことが明らかとなっている[21]。日本政府は、セキュリティ・クリアランス制度の導入や大学における技術流出防止に加えて、企業の技術流出防止に関するガイドラインを策定すべきである。

---

[19] Schoff, J., "U.S.-Japan Technology Policy Coordination: Balancing Technonationalism With a Globalized World," Carnegie Endowment for International Peace, June 29, 2020, https://carnegieendowment.org/2020/06/29/u.s.-japan-technology-policy-coordination-balancing-technonationalism-with-globalized-world-pub-82176

[20] "Japan, Australia and India to launch supply chain initiative," Bloomberg, August 31, 2020, https://www.bloomberg.com/news/articles/2020-09-01/japan-australia-and-india-to-discuss-supply-chains-alliance

[21] "公私立大、輸出管理部署設置は６割　技術流出、対策進まず," Sankei Shimbun, October 14, 2020, https://www.sankei.com/life/amp/201014/lif2010140037-a.html

日本の技術分野における民間セクターの重要性を踏まえれば、日本政府が、民間企業が有する課題に対応できるかどうかが、日本の経済安全保障政策の有効性を左右するといっても過言ではないだろう。

KEEPING THE LAST FRONTIER FREE AND OPEN: US-JAPAN SPACE COOPERATION AND PROSPECTS FOR GREATER ENGAGEMENT WITH SOUTHEAST ASIA

By Erick Javier

On 30 May 2020, the SpaceX Crew Dragon 2 spacecraft *Endeavor* lifted off from the Kennedy Space Center in Florida. Carrying two US astronauts to the International Space Station (ISS), the flight established several milestones, including being the first crewed flight carried by a private entity. This illustrates the rapid progress in the development and proliferation of space-based capabilities in the last 10 years. Space is increasingly accessible to multiple actors, both state and nonstate. Consequently, there is a growing concern that space is becoming "congested, contested and competitive."[1] This paper proposes that emerging US-Japan cooperation in space and space defense become an anchoring framework for space cooperation among like-minded states, particularly in Southeast Asia.

Challenges and Competition in Space

Space has been a securitized domain from the beginning of humankind's ascension to the stars.[2] Space provides significant advantages to national security and defense, being the ultimate "high ground." Many space technologies are dual-use, with major applications for both commercial and military offensive and defensive purposes.

Threats of kinetic space conflict have existed since the beginning of the Cold War. Despite best efforts to establish international norms to ensure peace in space, space has never been a "sanctuary" free from the risk of violent conflict. This can be seen in the development of counterspace capabilities, particularly anti-satellite (ASAT) weapons which overlap with missile

[1] Dickey, Robin. *The Rise and Fall of Space Sanctuary in US Policy*. The Aerospace Corporation. September 2020.
[2] Johnson, Kaitlyn. "What is Space Security and Why does it Matter?" *Georgetown Journal of International Affairs.* Fall 2020, Vol XX, p.81

defense.[3] Apart from kinetic means, electronic and cyber weapons including lasers and malware provide **viable and deniable means** to conduct counterspace operations, and have reportedly been deployed and used.[4]

These concerns have taken on new urgency with the resurgence of great power competition between the United States, the People's Republic of China, and the Russian Federation. In line with its Chinese Dream (*Zhōngguó Mèng*/中国梦), the PRC aims to surpass Russia as a space power by 2030, and the United States by 2045.[5] To defend their interests in space, states established dedicated military space organizations, such as the Russian Space Forces and the PLA Strategic Support Force in 2015, the United States' Space Force (USSF) in 2019, and the Japan Air Self-Defense Force Space Operations Squadron (JASDF-SOS) in 2020.

Competition in space also involves economic and normative dimensions. China has been very active in its space diplomacy, painting itself as a benevolent hegemon willing to provide developing states with space-related needs. China has been advocating for a Space Information Corridor (*Yīdài yīlù"kōngjiān xìnxī zǒuláng*/一带一路"空间信息走廊) as a space complement to its Belt and Road Initiative (BRI)[6] and has been selling satellites and space systems to partners across Eastern Europe, South and Southeast Asia, Africa, and Latin America.[7] China also launched the Asia-Pacific Space Cooperation Organization (APSCO) in 2008 to promote its brand of space cooperation. These initiatives support China's ambitions to shape norms and regimes in space.

---

[3] The United States' SM-3 ship-launched antiballistic missile demonstrated its potential as an ASAT in its 20 February 2008 intercept of satellite USA-193. Defensive missile systems such as the Russian S-500 *Prometey* and A-235, and the Israeli *Hetz* (Arrow) 3 have been claimed to be ASAT-capable.
[4] Rajagapolan, Rajeswari Pillai. "Electronic and Cyberwarfare in Outer Space." *Space Dossier 3*. United Nations Institute for Disarmament Research. May 2019. Accessed at https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf
[5] Pollpeter, Kevin et al. *China's Space Narrative: Examining the Portrayal of US-China Space Relationship in Chinese Sources and its Implications for the United States.* China Aerospace Studies Institute. 2020.
[6] Hu Jiang. *Programme and Development of the "Belt and Road" Space Information Corridor*. China National Space Administration. April 2019. Accessed at http://www.unoosa.org/documents/pdf/psa/activities/2019/UNChinaSymSDGs/Presentations/Programme_and_Development_of_the_Belt_and_Road_Space_Information_Corridor_V5.1.pdf
[7] Cheng, Dean. "How China has Integrated its Space Program with its Broader Foreign Policy." *2020 CASI Conference*. China Aerospace Studies Institute. September 2020.

Partnership and Convergence between US and Japan

Though the US will remain the preeminent space nation for the next two decades, maintaining security in space cannot be a unilateral affair. The United States will need partners and friends in space to help legitimize its position and values there. The US Department of Defense' International Space Cooperation Strategy 2017 set guidelines for harmonizing US and allies and partners' space defense. The 2020 Defense Space Strategy further affirmed the importance of US allies and partners in space, as well as opportunities for collaboration and inter-operability.

Japan is a natural partner for the US in space; it is a potent space power with its own suite of independent space capabilities. US-Japan cooperation has a rich history dating back to 1969, and has been steadily growing, with collaboration in a variety of projects such as the International Space Station (ISS).[8] Cooperation was further regularized with the annual Japan-U.S. Comprehensive Dialogue on Space, which began in 2013.[9] The most recent Dialogue, held on 25 August 2020, codified agreements on lunar exploration[10] and space defense operations.[11]

The importance of space to Southeast Asia

Southeast Asia's footprint in space has been growing,[12] commensurate with its growing economic and strategic importance. Seven of the 10 members of the Association of Southeast Asian Nations (ASEAN) have at least one satellite,[13] and many have established their own space

[8] Beckner, Christian. *US-Japan Space Policy: A Framework for 21st Century Cooperation*. Center for Strategic and International Studies. July 2003. Accessed at https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/taskforcereport.pdf

[9] Robson, Seth. "US, Japan pledge to work together on lunar exploration and space security." *Stars and Stripes.* 27 August 2020. Accessed at https://www.stripes.com/news/pacific/us-japan-pledge-to-work-together-on-lunar-exploration-and-space-security-1.642785?fbclid=IwAR3FuQh7fk-pqCTqqFCbyRXyuHzLaDrZgLI31LWeRLDhvQ1dF2EmN3-mkuY

[10] Patel, Neel V. "Why Japan is emerging as NASA's most important space partner." *MIT Technology Review*. 22 July 2020. Accessed at https://www.technologyreview.com/2020/07/22/1005546/why-japan-jaxa-nasas-most-important-space-partner-artemis-moon-gateway/?fbclid=IwAR0u-zcb_yEP84tgJOHTXB0ERuCXYR4Apgm0gzruB-48tlsz4XVgOG96iT8

[11] Areas for further cooperation may include: early warning, intelligence, surveillance and reconnaissance (ISR), space situational awareness, meteorological observation, command, control and communication, and ensuring resiliency of relevant space systems.

[12] Sarma, Nandini. ""Southeast Asian Space Programmes: Capabilities, Challenges and Collaborations." *ORF Special Report No. 82.* Observer Research Foundation. March 2019. Accessed at https://www.orfonline.org/wp-content/uploads/2019/03/ORF_SpecialReport_82_SEA-Space.pdf

[13] Indonesia, Laos, Malaysia, Philippines, Singapore, Thailand, and Vietnam all have at least one satellite as of 2020; Myanmar is planning to launch a satellite by mid-2021. Many of these satellites have been developed with foreign assistance. Japan is one of the largest partners in these space programs, providing

organizations.[14] Most of these programs have developmental and self-reliance objectives, and involve such space services as communications, meteorological, and geospatial information gathering. Several Southeast Asian states see space as an avenue to spur national development and boost technological capabilities.[15]

Space is also increasingly relevant for Southeast Asian states' security; satellite data was used by the Philippines to help fight insurgents during the Marawi crisis of 2017, and satellite imagery has been instrumental in observing Chinese reclamation and aggressive maritime activities in the South China Sea.

Prospects for Alliance Cooperation in Southeast Asia

US-Japan space collaboration can be the building block for initiatives with like-minded Southeast Asian states. The rationale for a joint US-Japan approach to Southeast Asia, as opposed to just US and Japan individually engaging Southeast Asian states, is due to the potential for:

- Increased trade: The space sector is expected to expand significantly, in part due to the increasing importance of space-based communications and data.[16] However, Southeast Asian states lack critical launch infrastructure to send payloads into space. Facilitating Southeast Asian space programs' access to both Japanese and US launch capabilities, including those from private-sector providers, can provide trade benefits such as reduced costs for Southeast Asian states, and thus allow them to better compete against Chinese

significant official development assistance to Vietnam, and Japanese institutions such as Hokkaido and Kyushu Universities assisting in the development of Philippine, Vietnamese, Myanmar, and Thai satellites.

[14] Space agencies were established by Indonesia (National Institute of Aeronautics and Space/LAPAN, 1962), Malaysia (National Space Agency/ANGKASA 2002, merged with the Malaysian Remote Sensing Agency to form the Malaysian Space Agency in 2019), the Philippines (Philippine Space Agency/PhilSA, 2019), Thailand (Geo-Informatics and Space Technology Agency/GISTDA, 2000), and Vietnam (Vietnam National Space Centre/VNSC, 2011).

[15] Vietnam has a stated aim of becoming one of the "leading countries in the region" in space technology. Indonesia, Malaysia, and the Philippines have identified space as potential growth engines for their economies. The Philippines in particular has identified the space sector as a strategic industry vital for national security and economic development. Singapore has encouraged and supported the growth of small satellite and space service start-ups to set up shop in the country.

[16] Bryce Space and Technology LLC. *Global Space Industry Dynamics*. Australian Department of Industry, Innovation and Science. 2019. Accessed at https://www.industry.gov.au/sites/default/files/2019-03/global_space_industry_dynamics_-_research_paper.pdf

space launch providers that rely on massive state subsidies to artificially lower costs.[17] Increasing demand for launch services also provides economic incentives for private-sector providers to maintain otherwise excess or "reserve" launch capabilities, to ensure resiliency for the US, Japan, and allies in event of any adversaries' attempts to degrade their space capability.[18]

- Space diplomacy and norm-building: Japan has been working extensively with Southeast Asian states' space programs. Japan has made space diplomacy and norm-building for space a key component of its foreign policy, including the creation and support of the Asia-Pacific Regional Space Agency Forum (APRSAF), which has been active since 1993.[19] Compared to the later APSCO, the APRSAF is looser and has less binding mechanisms, but is open to non-Asian states and includes international and nongovernment organizations.[20] The United States could learn from the Japanese experience in working with these states, or reinforce these ventures. Although Southeast Asian states are not interested in deep space exploration ventures such as the *Artemis* program due to the expense and modest ambitions of their current space programs, they may be willing to participate with the right economic incentives.

- Addressing common threats and space concerns: There is wide scope to leverage and co-develop space capabilities to help address traditional and nontraditional security threats. Space-based information can contribute to enhancing maritime security and defense, monitoring environmental, ocean health, and climate risks,[21] all of which are of great importance to the US, Japan, and several Southeast Asian states. The US and Japan can

---

[17] Smart, Benjamin. *Asian Responses to China's Space Power Strategy*. Naval Postgraduate School June 2019. Accessed at https://apps.dtic.mil/dtic/tr/fulltext/u2/1080404.pdf?fbclid=IwAR0e5CuEJ3zTz_tRTR3bgbG9687qwLZbh9rmfRp4DzFljcrXbC_Aejv32YE

[18] Markey, Michael. "Strengthening the US-Japan Alliance in Outer Space." *NIDS Visiting Scholar Paper Series* No. 4. National Institute for Defense Studies. 3 March 2020.

[19] Pekkanen, Saadia. "Japan's Space Power." Part of "Asia In Space: The Race to the Final Frontier." *Asia Policy*. Vol. 15. No.2. National Bureau of Asian Research. April 2020.

[20] Schrogl, Kai-Uwe and Giannopapa, Christina. "Europe in Space." Part of "Asia In Space: The Race to the Final Frontier." *Asia Policy*. Vol. 15. No.2. p.55 National Bureau of Asian Research. April 2020.

[21] An example is the United States' SERVIR initiative, which has been supplying geospatial data to Lower Mekong River Southeast Asian states to assist in land-use planning, agriculture risk management, and predicting and managing floods and other natural disasters in the area since 2014.

also provide capacity-building to counter common cybersecurity threats against space assets. ASEAN has expressed concerns about space debris,[22] and Japan issued a joint statement with the United Nations Office for Outer Space Affairs (UNOOSA) to raise awareness on space debris.[23] If Southeast Asian states back the Japanese advocacy, it could provide additional incentive for the United States to support or even initiate stronger measures against space debris.

Pursuing additional space cooperation will not be easy between the US and Japan, let alone with Southeast Asian or other partners. There is need for more discussion and harmonization of legal and scientific cooperation frameworks, as well as the appropriate safeguards to address private-sector and national concerns over intellectual property and data security. That last issue requires careful attention, as US export controls make direct collaboration and space trade difficult with other space-faring states,[24] and harm competitiveness against China, which has been working to position itself as a more open and less restrictive alternative supplier of space technology. Here, Japan, with extensive experience in co-developing satellites and other space assets with Southeast Asian states, can help bridge issues.

Conclusion

Cooperation is essential to preserve space as a domain for the benefit of all humankind. Great-power competition threatens this, and it does not seem possible to halt this competition given the clear intent of revisionist states to change the international order. To be better able to provide benefits to other states in a way that promotes the "rules-based international order," the United States and Japan must have a more deliberate and strategic convergence of interests in space. Given the collective advantages the US and Japan have, with the proper policies and coordination, they can ensure that space will continue to remain free and open for all.

---

[22] Penaranda, Ariel Rodelas. Statement on behalf of the Association of Southeast Asian Nations during the 2018 Session of the United Nations Disarmament Commission.
[23] "UNOOSA and Japan join forces to address space debris challenge." *SpaceRef.* 6 February 2020. Accessed at http://www.spaceref.com/news/viewpr.html?pid=55229&fbclid=IwAR1ymrHjEgRIX1YfpEzEZBAU8hOW4a2GVNWKuKfw1mxzQni92T21NTEF5as
[24] Solem, Erika. "The Emergence of China's Commercial Space Companies and Start-Ups." *2020 CASI Conference*. China Aerospace Studies Institute. September 2020. p.17

自由で開かれた最後のフロンティア：日米の宇宙協力と東南アジアとの関係強化についての展望

エリック・ハヴィエアー

2020年5月30日、スペースXの有人宇宙船クルードラゴン２、エンデバー号がフロリダのケネディ宇宙センターから打ち上げられた。国際宇宙ステーション（ISS）へ 2 名のアメリカ人宇宙飛行士の輸送を行なったこの飛行は、初めて民間団体によって実施された有人飛行であったことなど、幾つかの画期的な実績を打ち立てた。これは宇宙関連技術の発展と普及が過去10年間で急速に進んできたことを示している。官民を問わず宇宙は多くのアクターにとって益々利用可能なものとなっている。このことにより、宇宙は「混雑し、競合し、競争的」になりつつあるという懸念が高まっている[1]。本稿では拡大しつつある日米の宇宙及び宇宙防衛における協力関係が、東南アジアをはじめとした有志国家間での宇宙関連の中心的な協力枠組みになるべきであると提言する。

宇宙における課題と競争

人類が宇宙に進出した当初から宇宙は安全保障化された領域であった[2]。宇宙は究極の「高地」であり、国家安全保障及び防衛に大きな利点をもたらす。多くの宇宙技術はデュアルユースであり、商用にも軍用（攻撃、防御）にも利用される。

宇宙空間での武力紛争の脅威は、冷戦当初から存在していた。宇宙における平和維持の為の国際規範を確立する試みが為されてきたにもかかわらず、宇宙が紛争リスクのない「聖域」であったことは一度も無かった。こうした事実は、対宇宙

[1] Dickey, Robin. *The Rise and Fall of Space Sanctuary in US Policy*. The Aerospace Corporation. September 2020.
[2] Johnson, Kaitlyn. “What is Space Security and Why does it Matter?” *Georgetown Journal of International Affairs.* Fall 2020, Vol XX, p.81

能力、特にミサイル防衛とともに発展してきた対衛星攻撃兵器の開発にも見られる[3]。物理的な手段とは異なり、レーザーやマルウェアを含めた電子及びサイバー兵器は対宇宙作戦を行う上で有益且つ攻撃関与を否定しうる手段であり、既に配備及び使用されているようである[4]。

こうした懸念は、米中露の大国間競争の再燃により新たな緊急性を帯びてきた。中国は「中国の夢」に基づき、2030 年までにロシアを、そして 2045 年までにアメリカを超える宇宙大国になることを目指している[5]。宇宙における国益を守るために、2015 年にロシア宇宙軍と中国人民解放軍戦略支援部隊、2019 年にはアメリカ宇宙軍（USSF）、2020 年には日本航空自衛隊宇宙作戦隊（JASDF-SOS）と各国は宇宙領域を司る軍事組織を設立している。

宇宙をめぐる競争は経済的及び規範的側面も包含している。中国は積極的に宇宙外交を展開しており、発展途上国に宇宙関連支援を提供する良心的な覇権国と自らを称している。中国は宇宙情報回廊を、一帯一路を補完するものとし[6]、衛星や宇宙システムを東欧、南アジア、東南アジア、アフリカ、ラテンアメリカの友好国に販売している[7]。中国は中国流の宇宙協力を促進することを目的に 2008 年にはアジア太平洋宇宙協力機構（APSCO）を設立した。これらの取り組みは、宇宙における規範とレジームを形成するという中国の野心を下支えしている。

---

[3] 米国の船舶発射型対弾道ミサイル SM-3 は、2008 年 2 月 20 日の人工衛星 USA-193 の迎撃で、ASAT としての可能性を実証した。ロシアの S-500 プロメテーイや A-235、イスラエルのヘッツ（アロー）3 などのミサイル防衛システムは、ASAT としての能力を持ち合わせていると言われている。

[4] Rajagapolan, Rajeswari Pillai. “Electronic and Cyberwarfare in Outer Space.” *Space Dossier 3*. United Nations Institute for Disarmament Research. May 2019. Accessed at https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf

[5] Pollpeter, Kevin et al. *China’s Space Narrative: Examining the Portrayal of US-China Space Relationship in Chinese Sources and its Implications for the United States.* China Aerospace Studies Institute. 2020.

[6] Hu Jiang. *Programme and Development of the “Belt and Road” Space Information Corridor*. China National Space Administration. April 2019. Accessed at http://www.unoosa.org/documents/pdf/psa/activities/2019/UNChinaSymSDGs/Presentations/Programme_and_Development_of_the_Belt_and_Road_Space_Information_Corridor_V5.1.pdf

[7] Cheng, Dean. “How China has Integrated its Space Program with its Broader Foreign Policy.” *2020 CASI Conference*. China Aerospace Studies Institute. September 2020.

日米パートナーシップ

アメリカは、今後 20 年間は宇宙大国の地位を維持し続けるだろう。しかし、宇宙の安全保障は一国で達成されるようなものではない。アメリカは宇宙での地位及び価値を正当化するためにも友好国が必要である。2017 年に国防総省が策定した「国際宇宙協力戦略 2017」ではアメリカ、同盟国及び友好国間の宇宙防衛協力に関するガイドラインを定めた。2020 年の国防宇宙戦略では、宇宙におけるアメリカの同盟国と友好国の重要性、そうした国々との協力と相互運用性の機会が再確認された。

日本は宇宙分野におけるアメリカの適切なパートナーであり、日本は独自の宇宙能力を保持している有力な宇宙国家である。日米の協力の歴史は 1969 年にまで遡り、国際宇宙ステーション（ISS）をはじめとする様々なプロジェクトで協力し、着実に成長してきた[8]。2013 年に開催された「宇宙に関する日米包括的対話」を以って、協力関係はさらに制度化された[9]。2020 年 8 月 25 日に開催された直近の会議では、月面探査[10]と宇宙防衛活動に関する合意が成文化された[11]。

[8] Beckner, Christian. *US-Japan Space Policy: A Framework for 21st Century Cooperation*. Center for Strategic and International Studies. July 2003. Accessed at https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/taskforcereport.pdf

[9] Robson, Seth. "US, Japan pledge to work together on lunar exploration and space security." *Stars and Stripes*. 27 August 2020. Accessed at https://www.stripes.com/news/pacific/us-japan-pledge-to-work-together-on-lunar-exploration-and-space-security-1.642785?fbclid=IwAR3FuQh7fk-pqCTqqFCbyRXyuHzLaDrZgLI31LWeRLDhvQ1dF2EmN3-mkuY

[10] Patel, Neel V. "Why Japan is emerging as NASA's most important space partner." *MIT Technology Review*. 22 July 2020. Accessed at https://www.technologyreview.com/2020/07/22/1005546/why-japan-jaxa-nasas-most-important-space-partner-artemis-moon-gateway/?fbclid=IwAR0u-zcb_yEP84tgJOHTXB0ERuCXYR4Apgm0gzruB-48tlsz4XVgOG96iT8

[11] さらなる協力分野としては、早期警戒、情報、監視、偵察（ISR）、宇宙状況把握、気象観測、指揮統制及び通信、関連宇宙システムの強靭性確保などが考えられる。

東南アジアにとっての宇宙の重要性

東南アジアの宇宙におけるプレゼンスは、その経済的及び戦略的重要性の増大に応じて発展してきている[12]。東南アジア諸国連合（ASEAN）の 10 カ国のうち 7 カ国は、少なくとも 1 つの衛星を有しており[13]、多くの国々は独自の宇宙組織を設立している[14]。これらのプログラムのほとんどは、開発と自立を目的としており、通信、気象、地理空間情報収集等の宇宙サービスを含んでいる。東南アジアの数カ国は、宇宙を国の発展を促進させ、技術力を高めるための手段と考えている[15]。

宇宙は東南アジア諸国の安全保障においても重要性が増している。2017 年のマラウィ危機の際にはフィリピンは過激派掃討のために衛星からのデータを使用した。また衛星画像は、南シナ海における中国の埋め立て及び積極的な海洋活動を監視する上でも重要な役割を果たしている。

---

[12] Sarma, Nandini. ““Southeast Asian Space Programmes: Capabilities, Challenges and Collaborations.” *ORF Special Report No. 82.* Observer Research Foundation. March 2019. Accessed at https://www.orfonline.org/wp-content/uploads/2019/03/ORF_SpecialReport_82_SEA-Space.pdf

[13] インドネシア、ラオス、マレーシア、フィリピン、シンガポール、タイ、ベトナムは 2020 年時点で少なくとも 1 機の衛星を保有しており、ミャンマーは 2021 年半ばまでに衛星を打ち上げる予定である。これらの衛星の多くは、外国の援助を受けて開発されている。日本はこれらの宇宙開発計画の重要なパートナーであり、ベトナムに対して多額の政府開発援助を提供している。また、北海道大学や九州大学
がフィリピン、ベトナム、ミャンマー、タイの人工衛星の開発を支援している。

[14] インドネシア（インドネシア国立航空宇宙研究所/LAPAN, 1962）、マレーシア（マレーシア国立宇宙局/ANGKASA 2002 がマレーシアリモートセンシング庁と合併し、マレーシア宇宙庁を 2019 年に設立）、フィリピン（フィリピン宇宙庁/PhilSA, 2019）、タイ（タイ地理情報・宇宙技術開発機関/GISTDA, 2000）、ベトナム（ベトナム国家宇宙センター/VNSC, 2011）はそれぞれ宇宙関連機関を設立している。

[15] ベトナムは宇宙技術分野で当該地域における主導国の一つとなることを目指している。インドネシア、マレーシア、フィリピンは、宇宙を経済発展の潜在的な原動力として認識している。特にフィリピンは、宇宙を国家安全保障と経済発展に不可欠な戦略的産業分野として捉えている。シンガポールは小型衛星や宇宙サービスを提供する新興企業の成長を促進し、支援している。

東南アジアにおける同盟協力の展望

日米の宇宙協力は、東南アジアの有志国との取り組みのための土台となり得る。日米が個別に東南アジア諸国に関与するのではなく、日米が東南アジアに対し共同アプローチをとるべき理由は、以下のような可能性を秘めているからである。

● 貿易拡大：宇宙通信及び宇宙からの情報の重要性が増していることもあり、宇宙分野の大幅な成長が予想されている[16]。 しかし、東南アジア諸国は、十分なペイロードを宇宙に送るために必要なロケット打上げの為のインフラが不足している。東南アジア諸国の宇宙計画に対して、民間事業者のものも含めて日米の打ち上げ技術の利用を容易にすることによって、東南アジア諸国にコスト削減などの貿易の恩恵をもたらし、コストを削減するために国家からの巨額の補助金に依存している中国の宇宙打上げ事業者と競合しうるようにすることが可能である[17]。打上げサービスの需要の増大は、民間事業者に余剰又は「予備」と見做される打上げ能力を維持する経済的インセンティブを与えており、敵対国が宇宙能力の弱体化を試みた場合にもアメリカ、日本、その他同盟国の強靭性を確保しうる[18]。

● 宇宙外交と規範形成：日本は、東南アジア諸国の宇宙開発計画に積極的に協力してきた。日本は 1993 年に始まったアジア太平洋地域宇宙機関フォーラム（APRSAF）の設立と支援を含め、宇宙外交と宇宙に関する規範構築を外交政策の重要な要素としてきた[19]。APRSAF は、後の APSCO に比べて緩やかで拘束力に欠いているが、アジア以外の国々にも開かれ、国際機関や非政府組織も参加して

[16] Bryce Space and Technology LLC. *Global Space Industry Dynamics*. Australian Department of Industry, Innovation and Science. 2019. Accessed at https://www.industry.gov.au/sites/default/files/2019-03/global_space_industry_dynamics_-_research_paper.pdf

[17] Smart, Benjamin. *Asian Responses to China's Space Power Strategy*. Naval Postgraduate School June 2019. Accessed at https://apps.dtic.mil/dtic/tr/fulltext/u2/1080404.pdf?fbclid=IwAR0e5CuEJ3zTz_tRTR3bgbG9687qwLZbh9rmfRp4DzFljcrXbC_Aejv32YE

[18] Markey, Michael. "Strengthening the US-Japan Alliance in Outer Space." *NIDS Visiting Scholar Paper Series* No. 4. National Institute for Defense Studies. 3 March 2020.

[19] Pekkanen, Saadia. "Japan's Space Power." Part of "Asia In Space: The Race to the Final Frontier." *Asia Policy*. Vol. 15. No.2. National Bureau of Asian Research. April 2020.

いる[20]。アメリカは、これらの国々と協働してきた日本の経験から学ぶことやこれらの事業をさらに強化することができる。東南アジア諸国は、宇宙開発計画の予算と限定的な目標のため、アルテミス計画のような深宇宙探査事業には強い関心を示していないが、適切な経済的インセンティブがあれば参加する可能性もある。

- 共通の脅威と宇宙に関する懸念への対応： 伝統的安全保障及び非伝統的安全保障脅威に対応するための宇宙能力の活用及び共同開発は幅広い分野において可能である。宇宙からの情報は、海上安全保障と防衛の強化、そして環境、海洋健全度、気候リスクの監視に貢献することが出来[21]、これらはすべてアメリカ、日本、そして数カ国の東南アジアの国々にとって非常に重要なものである。また、日米両国は宇宙アセットに対するサイバーセキュリティの脅威に対処するための能力構築支援も提供しうる。ASEANはスペースデブリについて懸念を示しており[22]、日本も国連宇宙局（UNOOSA）と共にスペースデブリに対する意識啓発のための共同声明を発表した[23]。もし東南アジアの国々が日本の主張を支持した場合、アメリカがスペースデブリ対策を支援したり、より強力な対策を講じたりする更なるインセンティブとなる可能性がある。

宇宙協力をより深化させることは、東南アジアや他の友好国との間ではもちろん、日米間でも容易ではない。より議論を深めと法的及び科学的な協力枠組みの調和を図る必要があり、また知的財産やデータ・セキュリティに関する民間及び国家の懸念に対応するための適切な保護措置も必要である。アメリカの輸出規制は、

[20] Schrogl, Kai-Uwe and Giannopapa, Christina. “Europe in Space.” Part of “Asia In Space: The Race to the Final Frontier.” *Asia Policy*. Vol. 15. No.2. p.55 National Bureau of Asian Research. April 2020.
[21] 例えば、土地利用計画、農業リスク管理、洪水やその他の自然災害の予測と管理を支援するために、アメリカの SERVIR イニシアチブは 2014 年からメコン川下流の東南アジア諸国に対し地理情報を提供している。
[22] Penaranda, Ariel Rodelas. Statement on behalf of the Association of Southeast Asian Nations during the 2018 Session of the United Nations Disarmament Commission.
[23] “UNOOSA and Japan join forces to address space debris challenge.” *SpaceRef.* 6 February 2020. Accessed at http://www.spaceref.com/news/viewpr.html?pid=55229&fbclid=IwAR1ymrHjEgRIX1YfpEzEZBAU8hOW4a2GVNWKuKfw1mxzQni92T21NTEF5as

他の宇宙国家との直接的な連携や宇宙関連貿易を困難にしており[24]、またより開かれた宇宙技術の代替供給国としての地位を確立しようとしている中国に対する競争力を低下させているため、最後に述べた課題は特に注目に値する。この問題について、東南アジア諸国との人工衛星やその他の宇宙アセットの共同開発に豊富な経験を持つ日本が、橋渡し役を務めることができる。

結論

宇宙を全人類の利益のための一つの領域として維持するには、協力が不可欠である。大国間競争はこうした協力を脅かすものであり、修正主義国家の国際秩序を変更しようとする明白な意図を踏まえれば、この競争を止めることはできないように思える。「ルールに基づく国際秩序」を促進する形で他の国々により恩恵を与えられるようになるために、日米両国は計画的及び戦略的に宇宙における利益を共有しなければならない。日米両国が持つ優位性を鑑みれば、日米が適切な政策と調整を行うことで、全ての人々の為の自由で開かれた宇宙を維持することが出来るであろう。

[24] Solem, Erika. “The Emergence of China’s Commercial Space Companies and Start-Ups.” *2020 CASI Conference*. China Aerospace Studies Institute. September 2020. p.17

UNIFYING SMALL-SCALE UAV REGULATIONS: TRILATERAL COORDINATION TO COMBAT UAV TERRORISM AND PROMOTE CIVIL UAV DEVELOPMENT

By Mason Venturo

The drone economy will introduce a new era of innovation among entrepreneurs and nefarious nonstate actors. The accessibility, ease-of-use, and versatility of Small-scale Unmanned Aerial Vehicles (UAVs) will allow them to revolutionize how wars are fought, surveillance is conducted, and mail is delivered. While the possibilities for the use of UAVs by militaries are widely recognized, less attention has been given to the possibility of small-scale drone diversion. In Syria, Iraq, Venezuela, and Yemen, nonstate actors used widely available commercial drones to deliver conventional ordnance and perform reconnaissance. In Japan, an individual protesting nuclear energy policy landed a small drone carrying radioactive sand onto the roof of then-Prime Minister Abe Shinzo's office, prompting reform of Japanese civil drone regulation. The drones used in these attacks do not resemble the specialized UAVs employed by militaries; instead, nonstate groups use drones geared toward hobbyists, systems easily purchasable online.[1]

Just as planes, firearms, and explosives revolutionized the ability of radicals to inflict violence, UAVs possess the potential to revolutionize that potential for nonstate actors. This article explores the scope of this threat, including the economics of terrorism. It will discuss the fragmented world of state regulations pertaining to small-scale UAV systems. Given the relative 'newness' of drone technology and its numerous commercial applications, it is easy to understand the desire of governments to not overly burden this industrial sector with regulations. A lack of attention creates opportunities for violent nonstate groups.

Finally, this paper, after examining regulatory structures across the United States, European Union, and Japan, proposes a policy of international coordination by agencies responsible for

[1] Clover, Charles & Emily Feng. "Isis Use of Hobby Drones as Weapons Tests Chinese Makers." *Financial Times* (London, UK), December 10, 2017.

civil-UAV oversight. Given the size of these economies, their historical political/economic alignment, and the growth of their UAV industries, these three entities are particularly well-suited to introduce more complete drone regulations, and coordination will enable the sharing of best practices as the civil drone industry develops internationally, enabling multinational civil drone tech partnerships, and the creation of a drone 'California Effect' that will motivate drone technology developers to produce drones compliant with internationally coordinated regulations.

The use of drones in civil society is becoming ubiquitous. Over the past decade, UAV producers worked to produce more user-friendly UAV systems for hobbyists and private enterprises. Entrepreneurs continue to explore the myriad possibilities for legitimate UAV use, including urban firefighting, postal delivery, and landscape surveying. For instance, in Japan, Japan Airlines is currently studying drone parcel and medical supplies delivery capabilities.[2] Japan has instituted a four-stage roadmap aimed at coordinating drone technology and regulation development. According to *ICLG – Aviation Laws and Regulations*, coordinating new drone technological developments with regulatory reform will encourage commercial UAV utilization while also helping to address future Japanese labor shortages.[3]

However, as drones became more 'user-friendly 'and accessible, nonstate groups also began to employ these technologies. Actors such as the Houthi rebels, Islamic State, and Venezuelan antigovernment dissidents used drones to conduct reconnaissance or deliver conventional explosives. Nonstate actors use UAV systems for the same reasons state militaries do: use of drones increases the chance of operator survival while effectively performing reconnaissance or delivering ordnance.

For example, in August 2018, an assassination attempt on Venezuelan leader Nicolás Maduro occurred in which drones were used, injuring many.[4] In April 2015, Yamamoto Yasuo landed

[2] Bellamy III, Woodrow. "Japan Airlines Continues Effort to Enable Future Drone Delivery Operations." *Aviation Today* (US), September 25, 2020.
[3] Hayashi, Hiromi & Koji Toshima. "Regulations on Drone Flights in Japan: Aviation Laws and Regulations 2020." ICLG. Global Legal Group, March 2, 2020. Accessed on October 5, 2020. https://iclg.com/practice-areas/aviation-laws-and-regulations/6-regulations-on-drone-flights-in-japan.
[4] "Venezuela President Maduro Survives 'Drone Assassination Attempt." *British Broadcasting Corporation* (London, UK), August 5, 2018.

a drone carrying radioactive sand on the roof of the office of Japan's prime minister; authorities did not discover the drone until two weeks later.[5] In December 2018, dissidents used drones to shut down London's Gatwick airport, causing mass disruption of British air traffic and disrupting travel for thousands.[6] And Houthi rebels in 2019 disrupted Saudi Arabia's oil output via coordinated drone attacks on Saudi Aramco facilities, reportedly cutting the kingdom's oil output by nearly half."[7]

These attacks illustrate an increased willingness/capacity by nonstate groups to use drone tech, but also underscore an important fact: Terrorists are primarily economic actors. Their actions are aimed at producing maximum impact while using the fewest resources. Terror attacks require significant amounts of resources. Terror organizations, with limited resources, seek to inflict maximum damage on society with minimal investment. Drones are an increasingly cheap and efficient way to carry out attacks while not directly placing terror operatives in danger. The ability of drones to operate well away from their operators helps shield nonstate actors and dissidents from detection and arrest; this was made clear by the amount of time it took Japanese authorities to discover Yamamoto's drone/payload. This may help dissidents conduct a greater number of attacks before discovery by security forces. Extremist groups also recognize this feature of drone terrorism and will seek to incorporate this into their arsenals.

Civil drone regulations are uncoordinated. The EU possesses perhaps the most comprehensive system of small-scale UAV regulations, separating drones into three categories based on safety hazards: open, specific, and certified.[8, 9] For the open and specific categories, drone users must register themselves and attach their registration numbers to their drones; the certified category requires both the registration of the drone and the licensing of the pilot (separate from user registration). The specific and certified categories also require the notification of drone

[5] Murai, Shusuke. "Man Who Landed Drone on Roof of Japanese Prime Minister's Office Gets Suspended Sentence." *The Japan Times* (Tokyo, Japan), February 16, 2016.
[6] Burridge, Tom. "'Sustained' Drone Attack Closed Gatwick, Airport Says." *British Broadcasting Corporation* (London, UK), February 20, 2019.
[7] "Major Saudi Arabia Oil Facilities Hit by Houthi Drone Strikes." *The Guardian* (London, UK), September 14, 2019.
[8]" Civil Drones (Unmanned Aircraft)." European Union Aviation Safety Agency. Accessed October 5, 2020. https://www.easa.europa.eu/domains/civil-drones-rpas.
[9] "Drones (UAS)." European Union Aviation Safety Agency. Accessed October 5, 2020. https://www.easa.europa.eu/the-agency/faqs/drones-uas.

operation to relevant national authorities prior to use. The EU also maintains rules related to the maintenance of line of sight, maximum altitude, and other operation requirements as listed in Regulations (EU) 2019/947 and 2019/945).[10]

The United States, according to the FAA's 'Small Unmanned Aircraft Rule (Part 107), ' mandates pilot certification and drone registration, weight limits, and maintenance of line of sight among other rules.[11] So-called 'Recreational Flyers & Modeler Community-Based Organizations 'do not currently need to register themselves with the FAA, but must register their UAVs. In the future, this type of operator will also need to pass an aeronautics test.[12]

Japan instituted several reforms to its civil drone regulations after 2015. An amendment to the Japanese Aviation Act set new requirements concerning the operation of civil drones, primarily dealing with the proscribed operational envelope for civil UAV operators.[13] The Act on Prohibition of Flying UAVs over Important Facilities further introduced restrictions on UAV flight over governmental facilities and nuclear energy infrastructure.[14] Significantly, Japan currently does not require the registration or labelling of civil UAVs. Japan's Ministry of Land, Infrastructure, Transport, and Tourism (MLIT) does, however, require that drone operators request permission to fly small-scale UAVs; applications must be submitted 10 days prior to flight.[15] The EU, US, and Japan all make provisions for 'toy 'drones (≤250 grams for the EU

[10] "Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft" (2019) *Official Journal of the European Union* L152, p. 45.
[11] "Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems" (2019) *Official Journal of the European Union* L152, p. 1.
[12] "Recreational Flyers & Modeler Community-Based Organizations." Federal Aviation Administration. Accessed October 5, 2020. https://www.faa.gov/uas/recreational_fliers/.
[13] 航空法の一部を改正する法律案. Act to Partially Revise the Aviation Law. 189th Diet (2016). http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBDE56.htm.
[14] 国会議事堂、内閣総理大臣官邸その他の国の重要な施設等及び外国公館等の周辺地域の上空における小型無人機の飛行の禁止に関する法律案. Act on Prohibition of Flying UAVs over Important Facilities. 189th Diet (2016).
http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBDDC2.htm.
[15] "Japan's safety rules on Unmanned Aircraft (UA)/Drones." Ministry of Land, Infrastructure, Transport, and Tourism. Accessed October 5, 2020. https://www.mlit.go.jp/en/koku/uas.html.

and US, ≤200 grams for Japan). These drones, due to their small size and operational capacity, do not face the same operational restrictions or registration requirements as larger UAVs.[16, 17, 18]

In addition to its 2015 regulatory reforms, Japan set up the Council to Improve the Environment regarding UAVs, a private-public partnership council, aimed at facilitating discussion on drone regulation development in Japan. This council releases an annually updated document, the "Roadmap towards the Industrial Revolution in the Air," detailing a four-tiered plan for drone-use regulations. The first two tiers entail the operation of UAVs in civil society within visual range of UAV operators, while the third and fourth revolve around drone use beyond the line of sight of operators.

This system of public-private drone regulation partnership provides a venue for exploration of some of the best practices mandated in the US and EU regulatory systems, some of which are already being explored by Japanese policymakers, namely: drone/drone user registration. Japan's current regulatory structure does not provide Japanese civil society with adequate protection against the diversion of civil drone technology for nefarious purposes; adopting registration practices similar to the EU's will go a long way toward preventing drone attacks. While Japan's only major UAV incident did not result in any harm, the growing use of UAVs in violent attacks perpetrated by nonstate actors worldwide in addition to historical examples of dissidents and radicals in Japan disrupting infrastructure construction projects and releasing toxic chemicals should motivate more stringent regulation of this technology.

Additionally, Japan should use the momentum of its regulation roadmap to work with US and EU policymakers to bring about uniformity of international civil UAV regulation. While some level of uniformity exists -- exceptions for 'toy' drones -- additional efforts will produce economic benefits. Primarily, regulatory uniformity will allow for enhanced coordination between civil drone technology developers across borders, while potentially creating a drone

[16] "Civil Drones (Unmanned Aircraft)." European Union Aviation Safety Agency. Accessed October 5, 2020. https://www.easa.europa.eu/domains/civil-drones-rpas.
[17] "Summary of Small Unmanned Aircraft Rule (Part 107)." Federal Aviation Administration. Washington, DC. June 21, 2016.
[18] "Japan's safety rules on Unmanned Aircraft (UA)/Drones." Ministry of Land, Infrastructure, Transport, and Tourism. Accessed October 5, 2020. https://www.mlit.go.jp/en/koku/uas.html.

'California Effect.' The size of these markets, in conjunction with a more unified multinational drone regulatory system, will force manufacturers to build products that comply with regulatory constraints while allowing for international coordination in the development of the still largely unexplored opportunities the UAV revolution represents. As manufacturers find it increasingly economical to focus production on compliant UAV systems aimed primarily at markets of these three economic powerhouses, drone production outside Japan, the US, and the EU should increasingly align with internationally coordinated regulations. Coordination on UAV regulations may include common standards for drone payload, flying ceiling, and electronic tracking measures (although this raises questions regarding user privacy).

Coordination should seek the eventual inclusion of China, India, and Southeast Asia in an international regulatory superstructure; halting future UAV diversion will inevitably require the coordination of these actors as the possibilities of the drone economy are explored. When Japanese, US, and EU drone regulation policymakers work together to create rules aimed at encouraging civil drone technology development and dissuading illicit drone diversions, the result is a safer world in which for entrepreneurs to deliver new solutions without the risk of their products being used by violent extremists.

小型 UAV 規制の統一化：UAV テロリズムとの戦い及び民間 UAV 開発促進の為の三者間連携

メイソン・ヴェンチュロ

ドローン経済は、起業家と非道な非国家主体にイノベーションの新時代をもたらすであろう。小型無人航空機（UAV）の入手可能性、利便性、汎用性は、戦闘行為、監視、郵便物の配達方法に革命を起こすことが出来る。軍による UAV 使用の可能性は広く認識されているが、こうした小型ドローンの異なる用途の可能性はあまり注目されていない。シリア、イラク、ベネズエラ、イエメンでは、非国家主体が広く流通している商用ドローンを用いて、通常兵器の輸送や偵察を行った。日本では、原子力政策に反対していた個人が放射性物質を積載した小型ドローンを当時は安倍総理のオフィスであった首相官邸の屋上に着陸させる事件が発生し、この事件が日本における民間ドローン規制の改革を促進させた。これらの攻撃に用いられたドローンは、軍で使用されている特殊な UAV とは異なる。非国家主体は、オンラインで簡単に購入できる愛好家向けのドローンを使用しているのである。

飛行機、銃器、爆発物が過激派の攻撃能力に革命をもたらしたように、UAV も非国家主体の可能性に革命を起こす潜在力を秘めている。本稿では、テロリズムの経済学を含めて、こうした脅威について検証する。また、小型 UAV システムに対する国家規制の様相についても議論する。ドローン技術の相対的な「新しさ」と数多くの商業的用途を考えると、この産業分野に規制をかけすぎないようにしたいという政府の願望は理解しうる。こうした小型 UAV への関心の欠如は、暴力的な非国家主体に絶好の機会を与えてしまっている。

最後に、本稿では、アメリカ、EU 及び日本における規制構造を検討した上で、民間の UAV 管理を担う機関による国際協調政策を提案する。経済規模、歴史的な政治・経済

的連携、UAV 産業の成長を勘案すると、アメリカ、EU 及び日本は、より包括的なドローン規制を導入するのに適している。そしてこうした協調は、民間ドローン産業が国際的に発展する中でベストプラクティスの共有を促し、多国間の民間ドローン技術パートナーシップを可能にする。さらに、ドローン技術開発者が国際規制に準拠したドローンを生産する動機づけとなる「カリフォルニア効果」が生まれることも期待される。

ドローンの使用は市民社会のあらゆる場所で散見されるようになってきている。過去 10 年間、UAV の製造者は、愛好家や民間企業のために、より容易に使用可能な UAV システムの開発に取り組んできた。起業家は、都市の消防、郵便配達、土地の測量など、無数にある合法的な UAV の可能性を模索し続けている。例えば、日本では、日本航空がドローンによる小包や医療品の配送能力を研究している[283]。 日本は、ドローン技術と規制の発展を調整することを目的とした 4 段階のロードマップを策定している。ICLG（航空法規）によると、ドローンの新技術開発と規制改革を調整することは、UAV の商業的利用を促進すると同時に、将来の日本の労働力不足への対処にも資するという[284]。

しかしながら、ドローンがより「ユーザーフレンドリー」で容易に手に入るようになるにつれ、非国家主体も同様にこれらの技術を用いるようになった。フーシ反政府勢力、イスラム国、ベネズエラの反体制派は、偵察や爆発物の投下にドローンを用いた。非国家主体は、軍がドローンを利用するのと同様の理由、つまりドローンの使用が、効果的な偵察や武器の運搬を効果的に行うと同時に現場の人間の生存率を高めることができるという理由で UAV システムを用いている。

[283] Bellamy III, Woodrow. “Japan Airlines Continues Effort to Enable Future Drone Delivery Operations.” *Aviation Today* (US), September 25, 2020.
[284] Hayashi, Hiromi & Koji Toshima. “Regulations on Drone Flights in Japan: Aviation Laws and Regulations 2020.” ICLG. Global Legal Group, March 2, 2020. Accessed on October 5, 2020. https://iclg.com/practice-areas/aviation-laws-and-regulations/6-regulations-on-drone-flights-in-japan.

例えば、2018 年 8 月に起きたベネズエラの指導者ニコラス・マドゥロの暗殺未遂事件ではドローンが使用され、多くの人々が負傷した[285]。2015 年 4 月には山本泰雄が首相官邸屋上に放射性物質を積んだドローンを落下させる事件が発生し、事件から２週間が経過するまでドローンは発見されなかった[286]。2018 年 12 月には、反政府派がドローンを用いてロンドンのガトウィック空港を一時閉鎖に追い込み、イギリスの航空交通、数千人の旅行者に大きな混乱をもたらした[287]。そして2019年にはフーシ派がサウジアラムコの石油施設をドローンで攻撃し、サウジアラビアの石油生産にダメージを与えた。これにより、サウジアラビアの石油生産量はほぼ半分に削減されたといわれている[288]。

こうした事例は、非国家主体のドローンを使う意思、能力が向上していることと同時にテロリストが経済的なアクターであるという重要な事実を示している。彼らの行動は限られたリソースで最大の効果を得ることを目的としている。テロリストの攻撃には大量のリソースが必要である。限られたリソースしか持たないテロリストは最小限のコストで最大限のダメージを社会に与えようとしているのである。ドローンの利用は、テロ行為を行う者を直接の危険にさらすことなく攻撃を実行出来る益々安価で効率的な方法となっている。ドローンが操縦者から十分に離れた場所で動作できることは、非国家主体や反体制派が発見され逮捕されないようにする上でも有用である。これは山本が使用したドローンを発見するのに長い時間を要したことからも明らかである。さらにこのことは反体制派が治安部隊に発見される前により多くの攻撃を実行することを可能にするかもしれない。過激派グループもまた、こうしたドローンによるテロの特徴を認識し、彼らの武器として取り入れようとしているのだ。

[285] “Venezuela President Maduro Survives 'Drone Assassination Attempt.'” *British Broadcasting Corporation* (London, UK), August 5, 2018.
[286] Murai, Shusuke. “Man Who Landed Drone on Roof of Japanese Prime Minister’s Office Gets Suspended Sentence.” *The Japan Times* (Tokyo, Japan), February 16, 2016.
[287] Burridge, Tom. “‘Sustained’ Drone Attack Closed Gatwick, Airport Says.” *British Broadcasting Corporation* (London, UK), February 20, 2019.
[288] “Major Saudi Arabia Oil Facilities Hit by Houthi Drone Strikes.” *The Guardian* (London, UK), September 14, 2019.

現在、民間のドローン規制は画一的に調整がなされているわけではない。EU は、おそらく最も包括的な小型 UAV 規制のシステムを有しており、その中でドローンを安全上のリスクに基づいて、オープン(open)、特定(specific)、認定(certified)という 3 つのカテゴリーに分類している[289, 290]。オープンと特定のカテゴリーでは、ドローンの利用者はユーザー登録を行い、登録番号をドローンに付与しなければならない。認定のカテゴリーでは、ドローンの登録とパイロットのライセンス（ユーザー登録とは別に）の両方が必要となる。また、特定及び認定のカテゴリーでは、使用前にドローンの利用を国の関係当局に通知することが義務付けられている。また、EU では、規則（EU）2019/947 及び 2019/945 に記載されているように、照準線維持、最大高度、その他の運用要件を定めた規則がある[291]。

FAA の「小型無人航空機規則（パート 107）」によると、アメリカではパイロットの資格、ドローンの登録、重量制限、照準線維持、その他多くの規則を義務付けている[292]。「娯楽用模型飛行機コミュニティ団体 (Recreational Flyers & Modeler Community-Based Organizations)」は、現在、FAA へのドローン利用者登録を求めていないが、使用する UAV を登録する必要がある。将来的には、こうしたドローンの使用者は航空技術試験に合格する必要も出てくるだろう。

日本は 2015 年以降、民間ドローン規制の改革を行った。航空法の改正では、民間のドローン利用に関する新たな要件が定められ、主に民間 UAV 使用者の運用範囲が規制された[293]。 重要施設上空での UAV 飛行の禁止に関する法律では、政府施設や原子力施設

[289]“ Civil Drones (Unmanned Aircraft).” European Union Aviation Safety Agency. Accessed October 5, 2020. https://www.easa.europa.eu/domains/civil-drones-rpas.
[290] “Drones (UAS).” European Union Aviation Safety Agency. Accessed October 5, 2020. https://www.easa.europa.eu/the-agency/faqs/drones-uas.
[291] “Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft” (2019) *Official Journal of the European Union* L152, p. 45.
[292] “Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems” (2019) *Official Journal of the European Union* L152, p. 1.
[293] 航空法の一部を改正する法律案. Act to Partially Revise the Aviation Law. 189th Diet (2016). http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBDE56.htm.

上空での UAV 飛行の制限が導入された[294]。 驚くべきことに、日本では現在、民間 UAV の登録や表示を義務付けていない。しかし、国土交通省は、ドローン使用者が小型無人機の飛行許可を申請することを義務づけている（申請書は飛行の 10 日前までに提出されなければならない）[295]。 EU、アメリカ及び日本はいずれも「おもちゃの」ドローン（EU とアメリカは 250 グラム以下、日本は 200 グラム以下）についての規定を設けている。これらのドローンは、小型で運用能力も限られている為、大型の UAV と同様の運用上の規制や登録要件はない。

2015 年の改革に加え、日本は国内のドローン規制整備の議論を円滑に進めることを目的とした「小型無人機に係る環境整備に向けた官民協議会」を設置した。この協議会は、毎年更新される「空の産業革命に向けたロードマップ」を発表し、ドローン利用規制の 4 段階の計画を詳述している。レベル 1 と 2 では、市民社会における UAV の使用を UAV 使用者の目の届く範囲内で行うこと、レベル 3 と 4 では、使用者の目の届く範囲を超えたドローンの利用を対象としている。

この官民でのドローン規制パートナーシップのシステムは、米国や EU の規制システムで義務付けられている優れた実例を検証する場を提供し、そのうちのいくつか（例えばドローン/ドローン使用者の登録）は日本の政策立案者によってすでに検証されている。日本の現在の規制構造は、市民社会を民間ドローン技術の悪用から十分に保護する仕組みとなっていない。日本が EU と同様の登録方法を採用することは、ドローン攻撃の防止に大きく貢献するだろう。日本で発生した唯一の主な UAV 事件は大きな被害をもたらさなかったが、世界中で非国家主体による攻撃に UAV が使用されるようになってきているという事実や、反体制派や過激派がインフラ建設プロジェクトを混乱させ、有毒

[294] 国会議事堂、内閣総理大臣官邸その他の国の重要な施設等及び外国公館等の周辺地域の上空における小型無人機の飛行の禁止に関する法律案. Act on Prohibition of Flying UAVs over Important Facilities. 189th Diet (2016). http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/keika/1DBDDC2.htm.
[295] “Japan’s safety rules on Unmanned Aircraft (UA)/Drones.” Ministry of Land, Infrastructure, Transport, and Tourism. Accessed October 5, 2020. https://www.mlit.go.jp/en/koku/uas.html.

化学物質を放出した日本における過去の事例は、この技術に対する規制を厳格化する動機付けとなるだろう。

さらに、日本は規制ロードマップ作成を機に、アメリカや EU の政策立案者と協力して、国際的な民間 UAV 規制の統一を図るべきである。「おもちゃの」ドローンを除いて、ある程度の統一性は存在するが、さらなる統一化の努力は経済的利益も生むだろう。

規制の統一は、ドローンの「カリフォルニア効果」を生み出す可能性がある一方で、国境を越えた民間ドローン技術開発者間の協力を強化することを可能にするだろう。 これら三者の市場の規模、そしてそこにより統一された多国間のドローン規制システムが組み合わされば、製造業者は規制上の制約に準拠した製品を製造することを余儀なくされ、同時に、UAV 革命の中でまだ開発が然程進んでいない分野における国際的な協力を可能にするだろう。これら 3 つの大きな経済市場に準拠した UAV システムの生産に集中することが経済的であることを製造業者が認識するにつれ、日本、アメリカ及び EU 以外の国でのドローン生産も、国際的に調整された規制に沿ったものになっていくと予想される。UAV 規制の調整には、ドローンの積載量、高度、電子トラッキングなどの共通基準が含まれてくるかもしれない（ただしこれらはユーザーのプライバシーに関する課題を呈する）。

こうした協力は、最終的には中国、インド、東南アジアを国際的な規制構造に含めることを模索すべきである。将来的な UAV の悪用を阻止するためには、ドローン経済の可能性が探究される中で、必然的にこれらのアクター間の調整が必要となるであろう。日本、アメリカ及び EU のドローン規制に関する政策立案者が協力して、民間のドローン技術開発を奨励し、ドローンの悪用を阻止することを目的とした規則を定めれば、開発者が暴力的な過激派によって自らの製品を利用されるリスクを背負うことなく、新しいソリューションを提供することができる、より安全な世界の実現に繋がる。