特集／研究インテグリティ

〈1〉研究インテグリティ・研究セキュリティ：対応の背景と諸外国の動向

国立研究開発法人科学技術振興機構　研究開発戦略センター
フェロー　奥田　将洋
フェロー　鈴木　和泉
フェロー　菊地　乃依瑠

はじめに

研究インテグリティ・研究セキュリティの問題については、CISTEC Journal 誌上でも扱われており、上田（2022）による日本の取組の紹介や[1]、上野、張、山田（2023）による大学に求められる対応の検討[2]がなされてきたほか、双方の論考においては研究インテグリティ・研究セキュリティ対応が求められる国際的な背景についても触れられてきた。また、科学技術振興機構研究開発戦略センター（CRDS）においても、研究のオープン化・国際化の進展に伴う現行システムの揺らぎと研究インテグリティの見直しの必要性、我が国の課題ととるべき方策といった観点から、各国の動向を含め報告書としてまとめてきた（CRDS 2020, 2022, 2024）[3]。

これらで紹介されてきたように、今日の研究システムを支える研究の国際化とオープンな科学研究、その一側面にまつわる安全保障や研究環境の健全性へのリスクに対応した研究インテグリティ・研究セキュリティの取組は各国で展開している。また、近年は G7 や経済開発協力機構（OECD）といった枠組みでの国際協力も進展している。

本稿では、研究インテグリティの取組の拡大、あるいは研究セキュリティの導入が求められている背景について改めて整理すると共に、各国の現在の取組、また G7 と OECD での国際協力について概説する。また、次回以降研究セキュリティの観点から政府支援の基盤的研究（fundamental research）領域を含むリスク評価や情報開示といった取組を進める米国の事例について取り上げる。

1. 背景と問題の所在：技術管理を取り巻く環境の変化と科学研究の開放性

今日、多くの研究活動は世界中の知性・ノウハウ・才能・資金・インフラを合わせて活用する相互に関連した学際的で国際的なエコシステムの中で行われている。研究活動における開放性と国際協力は科学の進歩の基礎となるものであり、科学的な情報やデータのオープンで透明性の高いコミュニケーショ

[1] 上田光幸「研究活動の国際化・オープン化に伴う新たなリスクに対する研究インテグリティの確保に関する取組」『CISTEC Journal』No.199、2022 年 5 月。
[2] 上野一英、張壮壮、山田怜央「大学・研究機関における研究インテグリティに関して新たに必要となる対応」『CISTEC Journal』No.207、2023 年 9 月。
[3] 国立研究開発法人科学技術振興機構研究開発戦略センター『オープン化、国際化する研究におけるインテグリティ』（CRDS-FY2020-RR-04）2020 年 5 月『オープン化、国際化する研究におけるインテグリティ 2022- 我が国研究コミュニティにおける取組の充実に向けて -』（CRDS-FY2022-RR-01）2022 年 5 月、『米国における研究セキュリティの取組み－研究の開放性と安全の両立に向けて－』（CRDS-FY2023-RR-08）2024 年 3 月

ンと普及、研究成果の共有、人材の交流は、グローバルな科学エコシステムが効果的に機能する上で不可欠である。

その一方で、一部の国によってオープンな研究環境が自らの利益のために不当に利用されるリスクも2010年代後半頃からより認識されるようになっている。本稿で取り上げる国や国際的な枠組みの中では、公的研究における不正な情報の移転や外国の不当な干渉を国家と経済に対する重大な安全保障上のリスク、そして科学研究の開放性に対する脅威と捉えるようになっている。

こうしたリスクの懸念は2010年代中頃から安全保障のコミュニティを中心に認識され、高額の報酬や研究費の提供、留学生による技術情報の収集等を通じた技術流出が安全保障上の問題として認知され始めた。例えば、2018年に米国の通商代表部、大統領府の通商製造政策室、国防総省は、中国の貿易慣行への懸念や技術・知的財産の侵害、中国の技術移転戦略を懸念する報告書を公表し、不正な手段での知財、人材、技術獲得について、米国の国防及び経済的競争力のリスクになりうると懸念を示し始めた[4]。また、2018年にオーストラリア戦略政策研究所（Australia Strategic Policy Institute: ASPI）が発表したレポート“Picking flowers, making honey[5]”は、2007年に中国が海外の研究機関へ研究者を派遣し、先端技術の獲得を通じて軍事力の強化を行っていると指摘している。各国の政府や研究機関は中国の軍事関連機関や研究者へ技術提供する際に一定のチェック体制や管理メカニズムを確立すべきだとし、外国からの科学システムへの干渉に懸念を示した。

このような一部の国による研究開発活動を通じた不当な技術獲得の懸念はしばしばマスメディア等社会の広範において目に触れるような媒体でも取り上げられるところである。一方でこうした外国からの不当な干渉は、研究成果の公開や利用、大学・研究機関・研究者等の意思決定への影響、利益相反や責務相反の発生という観点から、安全保障のみならず研究システム自体の健全性を脅かすことにもつながりうるものである[6]。

また、技術管理の手法や枠組みという観点からもいくつかの背景を考慮する必要がある。

その一つが、技術管理を取り巻く前提の変化である。安全保障上の重要技術や機微技術は輸出管理や機密情報、あるいはこれらに準ずる情報[7]として、刑事罰等を含む法律の下で管理されてきた。大学や研究機関がこうした情報を利用、生産する場合にこれらのルールを遵守することは、研究インテグリティや研究セキュリティの一部という見方もできよう。こうした手法は、技術ないし技術の提供先といった主体が分類、ラベリングされることが前提となる。換言すれば、これまでは何を、あるいは誰に渡してはならないかを政府の権限で特定した上での管理が主であった。とりわけ輸出管理の観点では、政府としても国際輸出管理レジームという国際的な指針や規範を管理対象の技術やリスクの特定の背景とすることができた側面があった。

これに対して、近年注目される新興技術分野の中には、その軍事・安全保障目的での用途やリスク、これらに必要なスペックが必ずしも明らかになっていないものがある。また、経済安全保障の文脈に見られるような「経済的な手段を通じて国の安全保障を確保」するという観点は、技術のもたらす可能性とリスクを軍事用途のみならずより広範に評価する必要性を示している。こうした背景から、輸出管理で行われてきたような政府からの所与の管理基準やリスクの提示が以前ほど行き渡らない中で、外国からの不当な技術獲得の懸念に向き合わなければならない状態となっている現状がある。

もう一つの重要な背景として、科学技術・研究開発におけるオープンな環境がある。特に欧米諸国に

---

[4] Office of the United States Trade Representative Executive Office of the President, “*Report on China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation,*” March 22, 2018. White House Office of Trade and Manufacturing Policy, “*How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and The world,*” June 2018. Defense Innovation Unit Experimental, *China's Technology Transfer Strategy*, January 2018.

[5] Joske, Alex, *Picking flowers, making honey -The Chinese military's collaboration with foreign universities-*, Australian Strategic Policy Institute, 2018.

[6] 研究システムの健全性の問題については、CRDS『オープン化、国際化する研究におけるインテグリティ2022』（2022年5月）。

[7] 例えば米国における管理された非機密情報（Controlled Unclassified Information）とよばれる機密情報に至らない情報管理の枠組みでは、政府が持つ一部の科学技術情報等が含まれる場合がある。

おいては、開かれた研究活動から得られた成果が安全保障や経済に貢献してきたことは幅広く認識されている。研究開発に限らず、経済・産業も含めた活動への制限を最少化した技術管理はレーガン政権下の1985年に公表された国家安全保障決定指令第189号のようにかねてから追求されてきたところであり、これは現下の研究インテグリティ・研究セキュリティをめぐる取組においても同様である[8]。

例えば、米国科学財団（National Science Foundation : NSF）は2019年に、安全保障に関する問題の諮問組織JASONグループへ、外国からの干渉についてどのような方針をとるべきか諮問を行った。諮問に対してJASONグループが作成した報告書“Fundamental Research Security[9]”では、まず世界中の人材が協働する開かれた研究環境を維持することが米国の科学技術力の優位を保証するとの認識を前提として示した。その上で、外国の影響に対しては、研究上の責務相反や利益相反の開示を研究不正の防止のような既存の研究インテグリティのための措置に含め、完全な開示のための透明性の向上と条件の明確化等の措置を早急にとるべきと提言した。

NSFは2020年3月に前掲のJASONの報告書を踏まえた対応方針[10]を公表した。対応方針では責務相反・利益相反の開示については「研究提案の提出・採択方針及び手続ガイド」の改訂版に新たな申請フォーマットを導入し、透明性及び情報開示を明確化することが示された。また、NSFに新たに首席研究安全保障戦略政策官（Chief of Research Security Strategy and Policy）を配置して、研究インテグリティに対するリスク評価と対処、ステークホルダーとの協力等に取組むこととされた。これを端緒として、現在まで政府、ファンディング機関、研究機関の連携した取組が進められてきている。

英国においても、ほぼ同時期にアカデミアや産業界が行う研究活動を通じた技術流出が国家安全保障に重大なリスクを与えることが認識されており、英国政府の国家安全保障機関である国家インフラ保護センター（Centre for Protection of National Infrastructure: CPNI）と国家サイバーセキュリティセンター（National Cyber Security Centre: NCSC）は、2019年9月に“Trusted Research Guidance for Academia[11]”を公表した。また、英国大学協会（Universities UK, UUK）は、2020年10月に英国の高等教育体制が外国による敵対的な干渉を防ぐアプローチを示したガイドライン”Managing risks in Internationalisation: Security related issues[12]”を公表した。ガイドラインでは、外国の不当な干渉から高等教育体制を保護するために、英国大学協会に加盟している英国の大学や研究機関に個々の状況に合わせた適用を要請している。

研究インテグリティ・研究セキュリティの強化が求められてきた今日の背景には、国際関係の変化とこれを受けた経済安全保障といった問題の顕在化があり、またその中での科学技術の幅広い役割が再認識されたことがある。その一方で、技術管理を取り巻く前提の変化と、かねてから追求されてきた開かれた科学研究の維持という二つの背景は、各国における研究インテグリティ・研究セキュリティの政策とその下での取組にも大きな影響を与えている。次項以降、各国で進む取組について概説していく。また、研究インテグリティ・研究セキュリティに係る議論や検討はG7やOECDといった国際枠組みにおいても行われていることから、その動向についても扱う。

2. 各国の状況の概要

（1）米国

前述の通り、米国では2018年頃以降の動向として、外国からの不当な干渉への懸念を背景とした研究インテグリティ・研究セキュリティ確保のための取組強化が見られる。これらは、国防権限法や半導体・科学法といった法律や大統領による連邦行政機関への国家安全保障に係る命令である国家安全保障

[8] *National Policy on the Transfer of Scientific, Technical and Engineering Information*（National Security Decision Directive No.189）（NSDD-189）。当該指令では、「可能な限り、基盤的研究の成果を制限の外に置くことを維持する」ことを連邦政府の方針とした。
[9] JASON, *Fundamental Research Security*, The MITRE Corporation, 2019.
[10] National Science Foundation, *National Science Foundation Response to the JASON Report ‘Fundamental Science and Security’*, 2020.
[11] Centre for Protection of National Infrastructure & National Cyber Security Centre, *Trusted Research Guidance for Academics*, 2019.
[12] Universities UK, *Managing risks in Internationalisation: Security related issues*, 2020.