特集／安全保障、経済安全保障関連政策の動向

〈3〉研究セキュリティの国際動向 ―発展過程と共通する基本的枠組み

合同会社デロイト トーマツ デロイト トーマツ戦略研究所 研究員
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 特任フェロー
鈴木　和泉

はじめに

国境を越えた共同研究、研究者自身の国際的な流動性、研究インフラの共有など、現代の研究活動において国際協力は不可欠な基盤となっている。科学技術の発展は、多様な専門性を持つ研究者が自由に意見を交わし、リソースや成果を共有できるオープンな研究環境の中で、研究の質を高めてきた。

一方、2010 年代後半以降、一部の国による組織的な技術獲得活動への懸念を背景として、欧米を中心に、研究成果や技術の外国への不正移転、助成審査や論文査読における情報漏洩・不正利用といった外国からの不当な影響、技術流出、サイバー攻撃、新興技術の軍事転用など､新たなリスクが顕在化した。

こうしたリスクへの対応として、日本を含む各国で研究インテグリティおよび研究セキュリティの強化が進められてきた。当初は、研究者や大学・研究機関の外国との関係性や資金源を可視化し、利益相反・責務相反を適切に管理する研究インテグリティの取組が中心であった。しかし、現在では、開示された情報を活用してリスクを特定・評価し、技術流出や不当な干渉を未然に防止するリスクベースアプローチへと発展している。すなわち、研究者個人の誠実性や透明性を重視する研究インテグリティを基盤としつつ、大学・研究機関や資金配分機関を含む研究コミュニティ全体で研究活動を取り巻くリスクを管理する「研究セキュリティ」[1] が新たな機能として確立しつつある。

本稿では、各国の研究セキュリティの取組を、問題の顕在化、対応策の形成、研究現場への導入という三つのフェーズに整理し、その発展過程と特徴を概観するとともに、各国で共通する研究セキュリティの基本的な枠組みについて紹介する。

1. 研究セキュリティが求められる背景

1.1　研究の開放性と国際化

国際共同研究など、国際的に開かれた研究環境を確保することは現代のアカデミアでの研究の前提とされている。研究者は先行研究を基盤として知識を発展させてきた。こうした再現・検証を可能にする

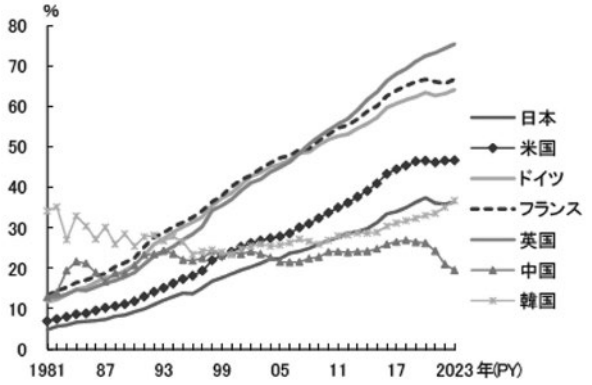
[1]「研究セキュリティ」は国によって表現が異なる。英国では「Trusted Research」、オーストラリアでは高等教育機関に対する外国干渉対策、カナダでは「Research Security」、オランダでは「Knowledge Security」として位置付けられている。日本では長らく研究不正防止を含む広義の「研究インテグリティ」の枠組みの中で扱われてきたが、2025 年の内閣府の「研究セキュリティの確保に関する取組のための手順書研究セキュリティの確保に関する取組のための手順書」において、研究セキュリティの定義が初めて明確化された。

ために、研究に用いた情報や材料へのアクセスを確保する開放性は、研究活動の根幹を成している[2]。また、科学的知識をオープンに利用可能、アクセス可能、かつ再利用可能にすることで、科学知識を公共財とし、研究の成果を社会に還元するという機能も期待されてきた[3]。

米国では、開放的かつ国際的な研究環境こそがイノベーションの原動力と考えられてきた。研究開発から商業化に至るプロセスは国際化し、科学研究活動も相互依存的なグローバル・イノベーション・エコシステムの中においては、研究環境のオープン性の確保は技術優位性を維持するためにも必要不可欠であると認識されている[4]。実際、国際共同研究の数は、コロナ禍に一時的に下がったものの増加傾向にあった（図表１）。

図表１　国際共著論文割合

（出典：文部科学省　科学技術・学術政策研究所、科学技術指標 2025、調査資料 -349、2025 年 8 月）



研究の世界では、国際共同研究が一般化し、クラウドを介したデータ共有の拡大、基礎研究と応用研究の境界の曖昧化といった研究環境の構造変化により、研究成果や知識が国境を越えて移転する速度と規模が大きく増大した。しかしその一方で、研究活動の国際化と開放性は、新たなリスクを生じさせた。研究成果や技術、人材、データが国境を越えて流動化するなかで、その開放性を悪用し、研究協力を通じて技術を獲得したり、研究成果を不適切に利用したりするリスクが顕在化したのである。

1.2　国際協力に伴う潜在的リスクの顕在化

アカデミアのオープンな研究環境に対するリスクが指摘され始めたのは 2010 年代後半頃からである。各国政府、議会やシンクタンクは、オープンな学術環境が国家戦略的に利用されるリスク、および先端技術や研究成果の不適切な移転が現実化しつつある点を指摘した[5]。2025 年時点においても米国では、米国の下院中国問題特別委員会が、国際共同研究における研究セキュリティ上の脆弱性や、国防総省の防衛研究においてすら外国からの不当な影響・関与を十分にチェックできていない点を指摘する報告書を発表しており[6]、オープンな研究環境が不当に利用される懸念は継続していると言える。

こうした懸念は、国際的な研究協力そのものを問題視するものではなく、研究者や研究機関の意図に反して研究成果が利用されるリスクが政策課題として認識されるようになったことを示している。

各国の政策文書や報告書で示されている具体的な懸念･リスクは、大きく 4 つに整理できる（図表 2）。ただし、研究開発の内容や研究のステージ、そして国際化の進展度合いによって、リスクの現れ方や影響の濃淡は大きく異なる。そのため、各国、大学・研究機関は、自国の制度環境や研究構造に応じて、リスクの把握と適切な管理が求められる。

---

[2] David B. Resnik (2023), *Openness in Scientific Research: A Historical and Philosophical Perspective*, Journal of Open Access Law.
[3] UNESCO (2021), *UNESCO Recommendation on Open Science*.
[4] Subcommittee on International Science and Technology Coordination, National Science and Technology Council (NSTC) (2024), *Biennial Report to Congress on International Science and Technology Cooperation*, February 2024, https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/2024-Biennial-Report-to-Congress-on-International-Science-Technology-Cooperation.pdf (2026 年 6 月 1 日アクセス), National Academy of Sciences (2022), *Protecting U.S. Technological Advantage*, National Academies Press, September 2022.
[5] JST-CRDS（2026）『各国の研究セキュリティの取組 ―研究の開放性と安全の両立に向けて―』（CRDS-FY2025-RR-10）、2.1「研究セキュリティの背景と問題の所在」, https://www.jst.go.jp/crds/pdf/2025/RR/CRDS-FY2025-RR-10.pdf, (2026 年 6 月 1 日アクセス).
[6] The Select Committee on the CCP(2025), *Joint Institutes, Divided Loyalties - How the Chinese Communist Party Exploits U.S. University Partnerships to Empower China's Military and Repression*, September 11, 2025, https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/jointinstitutesreportfinal.pdf（2026 年 6 月 1 日アクセス）, The Select Committee on the CCP(2025), *Fox in the Henhouse - The U.S. Department of Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research*, September 5, 2025, https://chinaselectcommittee.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fox-in-the-henhouse_report_final_04sep2025-compressed.pdf (2026 年 6 月 1 日アクセス)

図表 2：研究セキュリティの主要なリスク（著者作成）

意図しない技術移転	研究協力や人材交流を通じて、研究機関の意図に反して技術・知識が移転するリスク
外国からの影響力行使・干渉	外国政府・組織が研究活動や意思決定に政治的・経済的圧力を加えるリスク
制度的脆弱性の悪用	ガバナンスや制度上の不備・未整備を悪用することによって、情報・知的財産が流出するリスク
サイバー侵害・不正アクセス	サイバー攻撃による研究データ等の窃取

(1) 意図しない技術移転

オープンな研究環境では、研究者の交流や共同研究を通じて知識が自然に移転する。しかし、国家主体が意図をもって研究者・学生を派遣し、研究室内部での情報収集を行う場合や、高額報酬・研究費を用いたリクルート活動を通じて研究者に技術提供を求める場合、研究成果が大学・研究機関の意図に反して流出するリスクが生じる。また、共同研究先が外国政府と密接な関係を持つ場合、研究成果が軍事・監視用途へ転用される可能性もある。

(2) 外国からの影響力行使・干渉

外国政府やその影響下にある組織が、大学・研究機関の意思決定に対して政治的・経済的圧力を行使することで、研究活動の自由や独立性が損なわれるリスクである。具体的には、寄付・資金提供を通じた研究テーマの誘導、研究者の採用・配置への介入、研究成果（論文）の内容に対する修正要求などが含まれる。また、国家主体が国外にいる研究者・学生に対し、母国の家族への圧力、脅迫、監視を通じて情報提供や行動の変更を強制する越境弾圧（transnational repression）もある。

(3) 制度的脆弱性の悪用

大学・研究機関の制度・ガバナンスの不備や脆弱性が利用され、情報や知財が流出するリスクである。これらは制度の脆弱性が悪用される構造的リスクとして認識されている。

- **兼業等の申告漏れ**：研究者が外国機関での役職・報酬・人材採用プログラム参加を申告せず、研究費申請や成果利用において不透明な利益関係が生じる。これにより、外国側が研究成果を優先的に取得する構造が生まれる。
- **共同研究契約の不備**：知財の帰属や成果利用条件が曖昧な契約を悪用し、共同研究先が成果物を独占的に利用したり、国家主体に提供したりする。
- **研究データ管理の不備**：アクセス権限管理の不十分さやデータ保管の不備を利用し、共同研究者・学生がデータをコピーして持ち出す。
- **利益相反（COI）・責務相反（COC）の未申告**：外国企業・機関との契約や報酬を申告しないことで、研究テーマや成果利用が外国側の利益に誘導される。
- **査読者による未公開情報の流出**：査読制度の匿名性・非公開性を悪用し、未公開データや手法を自らの研究や外国機関に提供する行為。

(4) サイバー侵害・不正アクセス

研究データ、設計図、コード、実験記録などが、サイバー攻撃によって窃取されるリスクである。研究室ネットワークへの侵入、共同研究プラットフォームの乗っ取り、研究インフラへの攻撃などが含まれる。

1.3　研究インテグリティから研究セキュリティへ

上記のようなリスクへの対応として、各国では当初、研究者と外国機関との関係や外国資金の受入れ、兼業・兼職等の情報開示を求め、利益相反（COI）・責務相反（COC）の管理を中心とした研究インテグリティの強化が進められてきた[7]。

[7] 詳細は JST-CRDS『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 月を参照。