特集／大学の輸出管理／研究セキュリティ

〈2〉米国の研究セキュリティ強化の動向：研究の開放性と安全性への取組み

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

はじめに

前号において、研究コミュニティや大学・研究機関における研究インテグリティの強化や研究セキュリティの導入の背景と、米国、英国、豪州等の動向、さらにG7や経済開発協力機構といった国際協力枠組みの取組みを説明した[1]。

特に諸外国の動向として、研究インテグリティ・研究セキュリティの強化が、法律や大統領覚書のような形で方向付けられるケースもあれば、ガイドラインや支援枠組み設置のような形で研究コミュニティや大学等の自発的な取組みを支援する形も見られた。

研究インテグリティ・研究セキュリティ強化の背景には、一部の国によるオープンな研究環境の不当な利用や干渉、研究活動を通じた情報や技術の不正な移転の懸念がある。その一方、これらへの過度な対策が科学研究自体に影響することへの考慮もなされている。

前号で取り上げた研究インテグリティ・研究セキュリティの取組みを進めている諸外国の共通点は、研究現場とそこで生み出される成果・資源を守るだけでなく、研究の開放性や健全性も保護するという方向性にある。

そこで今回は、中でも米国の事例について取り上げ、研究セキュリティ強化の政策とその中での大学等の取組み、また連邦政府機関の施策を受けた研究コミュニティの対応について報告する。具体的には、情報開示、研究セキュリティリスクの評価・管理、研究セキュリティの体制整備やトレーニング拡充といった取組みを扱う。また、これらの取組みを支える関係者によるネットワークや情報共有についても言及する。

なお本稿は、国立研究開発法人科学技術振興機構（JST）研究開発戦略センター（CRDS）が2024年3月に公表した報告書作成にあたり調査した内容を元にしている[2]。

1. 研究インテグリティと研究セキュリティの概念整理と本稿での記述

そもそも研究インテグリティ、研究セキュリティはどのような意味を持つのか。まずは双方の概念整理を行う。

[1] 奥田将洋、鈴木和泉、菊地乃依留「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」『CISTEC Journal』No.210、2024年3月。
[2] 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（CRDS）『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。
https://www.jst.go.jp/crds/report/CRDS-FY2023-RR-08.html

研究インテグリティや研究セキュリティ、あるいはこれに類する取組みの用語は必ずしも各国で一般化されているわけではない。例えば英国では外国からの研究現場への不当な干渉への対策は“Trusted Research”と呼ばれている。また、日本では研究インテグリティという概念がセキュリティの側面を含むものへ拡大しているとの指摘がある[3]。

米国では、研究セキュリティに関連する政策文書や、その元となった学術界からの報告書があり、これらの中で研究インテグリティと研究セキュリティの概念整理が試みられている。

表1は、2022年1月に公表された米国大統領覚書33号（National Security Presidential Memorandum: NSPM-33）履行のためのガイダンス[4]、および2023年3月に公表されたJASON報告書に記載されている定義である[5]。同報告書は、米科学財団（NSF）が科学助言グループであるJASONに委託し作成した。NSFではNSPM-33の定義を公式に利用しており、米国内での一定程度の了解ができつつある。

一方で研究インテグリティと研究セキュリティを明確に区別することは難しく、国や文化の違いによって異なるとも同報告書は指摘されている。現在も国際的な概念統一はなされていない。

表1. 各種文書における研究インテグリティと研究セキュリティの定義
（各文書より筆者作成）

文書	NSPM-33 履行のためのガイダンス (2022.1)	JASON 報告書 “Research Program on Research Security”(2023.3)
研究 インテグリティ	研究開発活動の提案、実施、評価、報告において、客観性、公正性、透明性、公平性、説明責任、スチュワードシップなどの専門的な価値観や原則を遵守すること	客観性、公正性、開放性、説明責任、公平性、スチュワードシップといった研究活動の指針となり、資金配分機関、研究機関、研究コミュニティの期待として認識され、受容されている価値観や原則を遵守すること
研究 セキュリティ	国家または経済の安全保障を損なう研究開発の不正利用を目的とした行為、研究インテグリティの侵害に類する行為、そして外国政府からの不当な干渉から研究機関を保護すること	研究手法、ノウハウ、成果物について、研究プログラムのリーダーやセキュリティに関する他の関係者の承認により共有できる段階になるまで保護すること

これらの定義では、研究インテグリティは研究の客観性や公正性や開放性といった、研究者の責任ある行動として求められ原則とされている。これに対して、研究セキュリティとは、国家の経済や安全保障を損なう不当な干渉や研究インテグリティの侵害から、研究の成果やプロセスを保護することとして整理されている。

本稿で取り上げる米国の動向も、研究の国際化、オープン化が進展する一方で、研究現場を標的とした外国による不当な干渉や不正行為への懸念を背景として生じている。よって本稿の内容は、米国の研究セキュリティに係る動向が中心となる。

2. 米国の研究セキュリティの政策

近年、米国と中国の関係を中心に、技術や情報の獲得を巡る競争が激化している。その中で米国政府は、国内における研究開発活動を通じた技術の不正

[3] 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に必要となる対応」『CISTEC Journal』No.207、2023年9月。
[4] National Science and Technology Council, Joint Committee on the Research Environment, Subcommittee on Research Security, “Guidance for Implementing National Security Presidential Memorandum 33（NSPM-33）on National Security Strategy for United States Government – Supported Research and Development,” January 2022.
[5] JASON, The MITRE Corporation, “Research Program on Research Security,” March 2023, pp13-15, https://nsf-gov-resources.nsf.gov/2023-03/JSR-22-08%20NSF%20Research%20Program%20on%20Research%20Security_03152023_FINAL_1.pdf

な獲得や研究現場への不当な干渉に対して懸念を示している[6]。これらの中には、中国の人材採用プログラムである「千人計画」や、留学生の活動や共同研究を通じた技術・人材獲得についても言及がある。

こうした外国からの不当な干渉の懸念に対応するため、米国では技術管理の手段としてこれまで用いられてきた機密情報管理や輸出管理とは異なる形で、研究セキュリティとして情報管理やリスク管理といった取組みが展開されている。

以降、本稿ではトランプ政権下およびバイデン政権下で制定された「国防権限法」や「半導体・科学法」、「NSPM-33」等における研究セキュリティに関する動向を取り上げる。これらの法律や覚書は総じて資金配分機関を含む連邦政府機関に対する命令である。各連邦政府機関等は、研究資金の提供先等、支援対象となる大学等に対してセキュリティの強化を求める形となっている。

(2021 年度国防権限法)

トランプ政権下で成立した「2021 年度国防権限法」では、「研究開発費の申請時における情報開示」の規定が設けられた[7]。この規定では、年間 1 億ドル以上の外部向け研究開発費を支出する連邦政府機関を「各連邦研究機関 (each federal research agency)」と定義し、当該連邦政府機関が実施する研究開発資金提供の申請要件の一部として、申請者に対して情報の開示させることを要求している。

開示項目や要件には以下のものがある。

①開示項目として、現在及び申請中の研究資金提供等の金額・種類・提供元
②開示内容が最新・正確・完全であることの証明
③資金提供期間の前または期間中、連邦政府機関からの求めに応じた情報の更新

これらの要求の違反（violation）がある場合、連邦研究機関は資金提供申請の却下や助成の一時停止・終了、研究者の所属機関への研究資金提供の一時・恒久的な停止、所属機関の資格停止といった措置をとることができるとしている。

国防権限法のこの規定を背景として、連邦政府機関が支援する研究開発において情報開示の実施による研究セキュリティ強化がなされている。

(NSPM-33)

トランプ政権末期の 2021 年 1 月 14 日には、ホワイトハウスから「NSPM-33」として「米国政府支援による研究開発の国家安全保障政策」が発表された[8]。

この政策公表の背景には、一部の国が米国の開かれた研究開発環境を自国の利益拡大のために不正に利用しているとの問題意識がある。この不正の中には、研究開発成果の盗取や研究開発現場の意思決定への干渉等含まれる。こうした不正が問題になる前提には、連邦政府機関が支援した研究開発やその成果の公開が、米国のイノベーションや科学技術分野のリーダーシップ、延いては経済競争力や国家安全保障に係る能力の構築に貢献してきたことへの認識がある。

「NSPM-33」では研究開発に資金提供を行う連邦政府機関の長に対し、資金提供先の大学等への情報開示の要求、研究セキュリティ・研究インテグリティに関するリスクの特定と管理ポリシーの確立、そのための法執行機関との協力を命じている。

そして、当該連邦政府機関が資金提供する大学等については、連邦政府機関から年間 5000 万ドル以上の研究資金を受領する場合、以下を求めることとしている。

①情報開示要件とそのプロセスの強化

---

[6] このような懸念を喚起した米国政府の報告書として次のようなものがある、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. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF; 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. https://www.hsdl.org/?view&did=812268

[7] 2021 年度国防権限法セクション 223

[8] The White House, “Presidential Memorandum on United States Government-Supported Research and Development National Security Policy,” January 14, 2021. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/