各国の研究セキュリティ対応と JSTの取り組み方針

JST理事長・内閣官房 科学技術顧問
橋本 和仁

「研究セキュリティ確保」に対する問題意識

- 基礎研究成果の社会に与える影響の拡大、国際共同研究の重要性の増大、さらに地政学的緊張の高まり、といった目下の研究を取り巻く状況から、研究セキュリティ確保の対応は国際社会における喫緊の課題。

- 研究コミュニティにおいては、研究インテグリティの確保の取組を行ってきた。一方、新たな研究セキュリティの取組は、研究成果・研究者を適切に保護し、開かれた研究環境を守るためのものであり、さらに国の経済安全保障上の要請に応えるものである。

- よって国際的な政策や研究コミュニティの動向をしっかり踏まえた上で、対応を行っていくことが大切。

欧米主要国（米、英、加、仏、独）の共通認識

1. 研究セキュリティ確保の取組が、国際活動を制限・阻害するためのものであってはならない。可能な限りアカデミアの自由・透明性・開放性を尊重し、研究セキュリティ確保との両立を目指し、バランスを取ることが重要。また、特定の国・国籍に対する差別は回避しなければならない。

2. 研究セキュリティ対応を進めるにあたって、政府とアカデミアの対話によりアカデミアの認識・理解を醸成し、研究現場で実行可能なルールや取組の策定・推進が必須。

3. 研究セキュリティ対応は、①リスクベースで評価を行い、②リスクがあると判断された場合は、真に保護すべき研究領域を特定の上、「Small yard & High fence」、「As open as possible, as closed as necessary」の原則により、リスクを軽減。

以上の認識を共有しつつも、各国の政府の構造、研究システム、歴史的背景等により研究セキュリティ確保のアプローチは異なる

欧米主要国の研究セキュリティ対策

1. 2021年、第1次トランプ政権時に研究セキュリティ確保の国家的対応を指示。各機関の具体的な取組はアカデミアとの対話を重視しながら段階的に推進。
2. 米国科学財団（NSF）でも、リスク評価プロセス（TRUST）の開始を発表（2024年6月） 量子科学分野から試行。申請書のキーワード検索等でリスクが高いとされた採択候補は、レビューチーム（必要に応じて安全保障部局もオブザーバーとして参画）でさらにリスク評価。リスク緩和策を研究機関と検討し、その妥当性はNSFが判断。

1. 国家安全保障・輸出管理の法制度に沿い、研究セキュリティ確保の取組を推進。政府の国防・安全保障部局と研究大学幹部は、長年、信頼関係を構築しており、頻繁に脅威やリスクを共有。
2. 政府機関は、大学に向けてガイドラインや相談窓口を提供。大学は政府と密に連携しつつ、最終意思決定は独立機関として大学の責任で行うことを強調。

1. 大学の研究セキュリティ部門に国家安全保障部門出身者が在籍。政府は、機微な研究分野リスト、懸念される研究機関リスト、各種ガイドラインを公開。研究セキュリティ確保のための資金（年間約27億円程度）や相談窓口を提供。
2. カナダ自然科学・工学研究会議（NSERC）の公募プログラムでリスク評価を試行。申請者はリスク評価フォームを提出。必要に応じて国家安全保障部門が追加の評価や助言。リスクが特定された場合にはリスク軽減策を策定し、妥当性はNSERCが判断。

1. 2012年より、安全保障、経済的な観点から「科学技術潜在力の保護制度」の運用を開始。
2. 関係府省がすべての研究機関の研究チーム/研究室のリスク評価を実施。リスクが高いと特定された場合、研究テーマや研究参加者の管理、研究成果の保護をトップダウンで行う。

国際枠組みの動向

各国の対応が異なることで国際連携を阻害しないよう、関係国間で価値観と原則を共有する動き。

1. G7 科学技術大臣会合コミュニケ（2024年7月、ボローニャ）にて「国際的な協力における研究セキュリティ・インテグリティを促進することの重要性が増大していることを強調」、「G7は、共通の価値観と原則、及びベストプラクティスを議論し、促進し、普及するための重要なフォーラムと考える」と合意。
2. G7作業部会の成果として、「研究セキュリティ・インテグリティに関するG7共通の価値観と原則」等の文書の公表と、バーチャルアカデミー※の設立を評価。※ベストプラクティスの相互学習プラットフォーム

1. OECD・CSTP（科学技術政策委員会）の閣僚級会合（2024年4月、パリ）では、閣僚宣言に研究セキュリティ・インテグリティなどの国際協力における共有価値の強化を盛り込んだ。
2. 2025年2月、OECD科学技術イノベーション局（科学技術政策委員会（CSTP）・グローバルサイエンスフォーラム（GSF））は、研究セキュリティに関する新たな調査・分析プロジェクトを開始。

1. Horizon Europe等のEU域内の共同研究を阻害しないために、加盟国の研究セキュリティ確保の共通理解が必要であるとの認識のもと、鋭意調整中。
2. 2024年5月、EU理事会で加盟国に対して「研究セキュリティ強化に関する勧告」を採択。学問の自由の考慮、非EU加盟国との連携は「可能な限りオープンに、必要な限りクローズド」の原則遵守、非差別や基本的権利尊重、政府内の分野横断的な協力強化、支援組織新設等を勧告。

我が国としても、研究のオープン性を重視しつつ、研究セキュリティ確保により健全に研究に取り組む対応を進め、関係国との連携を進めていくことが重要

JSTとしての「研究セキュリティ確保」の考え方

- 研究の自由、透明性、開放性の確保は、知の探求の営みや人類の発展のために普遍的に重要なものであり、いわば研究の本質ともいえるもの。

- 他方、オープンな研究システムの不当な利用により、研究システムの健全性、公正性の毀損、研究成果の悪用、技術流出のリスクの高まりが懸念されている。

- 研究のオープン性の重要性は何ら変わらないが、そうした動きからアカデミアを守ることが重要。ただし、特定の国の排除や国籍等による差別をするものではない。アカデミアに注意喚起を促し、その上でお互いに信頼感を持って健全に研究に取り組む文化を醸成するため、研究セキュリティ確保に取り組む。

研究セキュリティ確保の対応状況

- **国際共同研究への適用開始**

先端技術分野の国際共同研究（先端国際共同研究事業（ASPIRE））において、相手国側と連携して「リスク評価」や「リスク緩和」などの取組を試行中
(日英バイオ、日独量子）

- **ファンディング申請時のセキュリティ確保システム導入**

米国（NSF）が試行的に実施中の研究セキュリティ取組（TRUST（Trusted Research Using Safeguards and Transparency））を参考に、日本版TRUST(JST-TRUST) を試行的に実施していく。試行を通じて、プロセスは柔軟に再検討。

※**「次世代エッジAI半導体研究開発事業」**（文科省、経産省、JST連携による半導体の先端研究開発プロジェクト）においても、研究セキュリティ対応を含め、制度設計を進めていく。

- **アカデミア（研究者個人、大学等執行部）との対話**

本シンポジウムなど、様々な機会を通じて実施。
（文科省科学技術・学術政策局は「大学等の研究セキュリティ確保に向けた文部科学省関係施策における具体的な取組の方向性」を昨年12月に公表。今後とも政府における検討を注視。）