令和７年度内閣府委託事業

令和 7 年度科学技術基礎調査等委託事業

研究セキュリティ・インテグリティ
(Research Security and Research Integrity)
に係る調査・分析及び
Ｇ７オンラインプラットフォーム
「バーチャルアカデミー」の運営支援・分析

報告書

令和８年２月

公益財団法人
未来工学研究所
INSTITUTE FOR FUTURE ENGINEERING

本報告書は、内閣府 科学技術・イノベーション推進事務局の令和７年度科学技術基礎調査等委託事業による委託業務として、公益財団法人未来工学研究所が実施した「研究セキュリティ・インテグリティ（Research Security and Research Integrity）に係る調査・分析及びＧ７オンラインプラットフォーム「バーチャルアカデミー」の運営支援・分析」の成果を取りまとめたものです。

― 目　　次 ―

― 図 目 次 ―

― 表 目 次 ―

略語表

国・地域	略語	英語等	日本語名称
米国	AOR	Authorized Organizational Representative	組織の権限ある代表者
	ARO	Army Research Office	陸軍・研究室
	ASCE	Academic Security and Counter Exploitation	学術セキュリティと悪用対策
	BRO	Basic Research Office	基礎研究室（国防省）
	CCP	Communist Party of China	中国共産党
	CETPP	Critical and Emerging Technology Protection Program	重要新興技術保護プログラム（テキサス A&M 大学システム）
	CHIPS and Science Act	Creating Helpful Incentives to Produce Semiconductors and Science Act	CHIPS 科学法
	CoSSaR	Center for Collaborative Systems for Safety, Security and Regional Resilience	安全保障・地域レジリエンス協力システムセンター（ワシントン大学）
	CRSO	Chief Research Security Officer	研究セキュリティチーフオフィサー（ワシントン大学）
	CUI	Controlled unclassified information	管理された非機密情報
	DoD	Department of Defense	国防省
	DOE	Department of Energy	エネルギー省
	DPID	Digital Persistent Identifier	デジタル永続識別子
	EAGER	Early-concept Grants for Exploratory Research	探索的研究への初期概念の助成金
	FFDR	Foreign Financial Disclosure Reporting	外国資金開示報告
	FFRDC	Federally Funded Research and Development Center	連邦資金研究開発センター
	FTRP	Foreign Talent Recruitment Program	海外人材採用プログラム
	GAO	Government Accountability Office	政府説明責任局
	GSR	Global Support Resources	グローバル支援リソース（MIT）
	IAC	International Advisory Committee	国際助言委員会（MIT）
	ICC	International Coordinating Committee	国際調整委員会（MIT）
	IIC	Informal International Collaborations	非公式国際協力（MIT）
	LOI	Letter of Intent	意向表明書
	MFTRP	malign foreign talent recruitment program	悪性海外人材採用プログラム
	MIT	Massachusetts Institute of Technology	マサチューセッツ工科大学
	MOA	Memorandum of Agreement	合意書
	MOU	Memorandum of Understanding	了解覚書
	NDAA	National Defense Authorization Act	国防授権法
	NIH	National Institutes of Health	国立衛生研究所
	NIST	National Institute of Standards and Technology	米国国立標準技術研究所
	NSF	National Science Foundation	米国科学財団
	NSPM-33	National Security Presidential Memorandum 33	国家安全保障大統領メモ第 33 号
	OCRSSP	Office of the Chief of Research Security Strategy and Policy	研究セキュリティ戦略・政策室（NSF）
	ORSP	Office of Research Security and Policy	研究セキュリティ・政策局（NSF）
	OSTP	Office of Science and Technology Policy	大統領府科学技術政策局
	OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering	国防省本省の研究・工学担当国防次官室
	PI	Principal investigator	研究室主宰者
	RISC Institute	Research and Innovation Security and Competitiveness Institute	研究イノベーションセキュリティ・競争力研究所

国・地域	略語	英語等	日本語名称
米国	QIS	Quantum Information Science	量子情報科学
	RoRS	Research on Research Security	研究セキュリティについての研究
	RSI-ISAO	Research Security and Integrity Information Sharing and Analysis Organization	研究セキュリティ・インテグリティ情報共有分析組織
	RSO	Research Security Office	研究セキュリティ室（テキサスA&M大学システム）
	RSP	Research security program	研究セキュリティ・プログラム
	RST	Research security training	研究セキュリティ研修
	SECURE Center	Safeguarding the Entire Community of the U.S. Research Ecosystem Center	米国研究エコシステム全体コミュニティ保護センター（SECUREセンター）
	SRG	Senior Risk Group	シニアリスクグループ（MIT）
	SVE	Shared Virtual Environment	共有バーチャル環境
	TRUST	Trusted Research Using Safeguards and Transparency	安全対策・透明性による信頼できる研究（TRUST）
	URSPA	University Research Security Professionals Association	大学研究セキュリティ専門家協会
	UW	University of Washington	ワシントン大学
	VPR	Office of the Vice President for Research	研究担当副学長室（MIT）
カナダ	CCA	Council of Canadian Academies	カナダアカデミー評議会
	CFI	Canada Foundation for Innovation	カナダ・イノベーション財団
	CIHR	Canadian Institutes of Health Research	カナダ保健研究機構
	CoP	Community of Practice	実践コミュニティ
	CSIS	Canadian Security Intelligence Service	カナダ安全保障情報局
	EDI	Equity, Diversity and Inclusion	公平性、多様性、包摂性
	ISED	Innovation, Science and Economic Development Canada	カナダイノベーション・科学経済開発省
	NRO	Named Research Organizations	指名研究機関
	NSERC	Natural Sciences and Engineering Research Council of Canada	カナダ自然科学・工学研究評議会
	NSGRP	National Security Guidelines for Research Partnerships	研究パートナーシップのための国家安全保障ガイドライン
	OSINT	Open Source Intelligence	オープンソースインテリジェンス
	OVPRI	Office of the Vice-President, Research & Innovation	研究イノベーション担当副学長室（トロント大学）
	PSC	Public Safety Canada	公共安全省
	RAF	Risk Assessment Form	リスクアセスメントフォーム
	RCR	Responsible Conduct of Research	責任ある行動規範
	RPSID	Research Partnership Security Information Document for International Partnerships	国際パートナーシップに関する研究パートナーシップ・セキュリティ情報文書（トロント大学）
	RSC	Research Security Centre	研究セキュリティセンター
	RSCO	Research Security + Compliance Office	研究セキュリティ＆コンプライアンス室（マギル大学）
	RSF	Research Support Fund	研究支援資金
	SRO	Safeguarding Research Office	研究保護室（アルバータ大学）
	SSHRC	Social Sciences and Humanities Research Council of Canada	カナダ社会科学・人文科学研究評議会
	STRA	Sensitive Technology Research Areas	機微技術研究領域
	STRAC	Policy on Sensitive Technology Research and Affiliations of Concern	機微技術研究および懸念される提携に関する方針
	TAHSN	Toronto Academic Health Science Network	トロント学術医療科学ネットワーク
英国	NPSA	National Protective Security Authority	国家保護安全保障局
	UKRI	UK Research and Innovation	英国研究・イノベーション機構
	UUK	Universities UK	英国大学協会
オーストラリア	ARC	Australian Research Council	オーストラリア研究評議会

国・地域	略語	英語等	日本語名称
オーストラリア	ANU	Australian National University	オーストラリア国立大学
	UWA	University of Western Australia	西オーストラリア大学
EU	ALLEA	All European Academies	全欧州アカデミー
	EU	European Union	欧州連合
	ERA	European Research Area	欧州研究圏
	EUA	European University Association	欧州大学協会
オランダ	KNAW	Royal Netherlands Academy of Arts and Sciences	オランダ王立芸術科学アカデミー
	NWO	Dutch Research Council	オランダ科学研究機構
	UNL	Universities of the Netherland	オランダ大学協会
	UvA	University of Amsterdam	アムステルダム大学
	VU Amsterdam	Vrije Universiteit Amsterdam	アムステルダム自由大学
ドイツ	ATB	Leibniz Institute for Agricultural Engineering and Bioeconomy	ライプニッツ農業工学・バイオエコノミー研究所
	BAFA	Bundesamt für Wirtschaft und Ausfuhrkontrolle	連邦経済輸出管理局
	BfV	Bundesamt für Verfassungsschutz	連邦憲法擁護庁
	BMBF	Bundesministerium für Bildung und Forschung	連邦教育研究省
	BMFTR	Bundesministerium für Forschung, Technologie und Raumfahrt	連邦研究技術宇宙省
	DAAD	Deutscher Akademischer Austauschdienst e.V.	ドイツ学術交流会
	DFG	Deutsche Forschungsgemeinschaft	ドイツ研究振興協会
	DLR-PT	DLR Projektträger	ドイツ航空宇宙センター・プロジェクト管理機関
	HRK	Hochschulrektorenkonferenz	大学学長会議
	KEF(s)	Ethikkommission für sicherheitsrelevante Forschung	安全保障関連研究倫理委員会
	MPG	Max Plank Gesellschaft	マックス・プランク協会
	RPTU	Technischen Universität Kaiserslautern-Landau	カイザー・スラウテルン＝ランダウ工科大学
	TUM	Technische Universität München	ミュンヘン工科大学
	UFZ	Helmholtz Centre for Environmental Research	ヘルムホルツ環境研究センター
イタリア	ACN	Agenzia per la cybersicurezza nazionale	サイバーセキュリティ局
	CoPER	Consulta dei Presidenti degli Enti Pubblici di Ricerca	公的研究所所長評議会
	CRUI	Conferenza dei Rettori delle Università Italiane	イタリア大学学長会議
	DIS	Dipartimento delle Informazioni per la Sicurezza	情報安全局
	MUR	Ministero dell'Università e della Ricerca	大学・研究省
その他	SIGRE	Security and Integrity of the Global Research Ecosystem	グローバルな研究エコシステムにおけるセキュリティとインテグリティ

第1章　調査の概要

1.1　調査の目的

研究活動の国際化、オープン化に伴う新たなリスクにより、開放性、透明性といった研究環境の基盤となる価値が損なわれる懸念や、研究者が意図せず利益相反・責務相反に陥る危険性が指摘されている。このような中、研究環境の基盤となる価値を守り、国際的に信頼性のある研究環境を構築すること、また、そのための取組を推進することが不可欠となっている。

本業務は、我が国の大学・研究機関、研究資金配分機関における研究セキュリティ・インテグリティに関する取組の進展に資することを目的として、具体的には、以下の調査・整理・分析等を行った。

（1）研究セキュリティ・インテグリティに関する大学・研究機関等、研究資金配分機関等による取組等の調査

（2）日本の大学・研究機関等のための研究インテグリティと研究セキュリティについての意見交換会の企画・運営

（3）Ｇ７オンラインプラットフォーム「バーチャルアカデミー」の運営支援・分析

1.2　調査の内容、方法等

1.2.1　研究セキュリティ・インテグリティ（Research Security and Research Integrity）に係る調査・分析

(1)　研究セキュリティ・インテグリティに関する大学・研究機関等、研究資金配分機関等による文書の調査・分析の実施

①海外主要国の大学・研究機関等及び研究資金配分機関等、並びに国内の大学・研究機関等及び研究資金配分機関等における研究セキュリティ・インテグリティに関する取組について、文献調査を実施した。更に、政府機関や関連団体により発出された文書についても調査を行い、大学・研究機関等、研究資金配分機関等が発出した文書との関係性を調査した。

②ヒアリング調査を実施した。

③文献調査、ヒアリング調査の結果に基づき、分析を行い、我が国の大学・研究機関等、研究資金配分機関等が研究セキュリティ・インテグリティに関する取組を各機関で推進する上で参照できるように事例を整理した。

(2)　日本の大学・研究機関等のための研究インテグリティと研究セキュリティについての意見**交換会の実施**

研究インテグリティと研究セキュリティについての意識醸成、課題等の抽出・整理、関係者のネットワーク形成を目的に、日本の大学・研究機関等のための意見交換会の企画・運営を実施した。

1.2.2　Ｇ７オンラインプラットフォーム「バーチャルアカデミー」の運営支援・分析

Ｇ７オンラインプラットフォーム「バーチャルアカデミー」の運営を支援した。

①日本国内の政府機関、大学・研究機関等、研究資金配分機関に対し、オンライン説明会（ウェビナー形式）を実施した。
②日本国内の政府機関、大学・研究機関等、研究資金配分機関からのユーザー登録依頼に対する認証業務等を実施した。
③日本国内のユーザーからのコンテンツ（原則として英語）の掲載依頼に対する認証業務を実施した。
④日本国内の政府機関、大学・研究機関等、研究資金配分機関からの問い合わせに対する対応を実施した。
⑤登録機関リスト、登録ユーザーリスト、掲載コンテンツリスト、問い合わせリストを都度提出した。

1.3　調査の実施時期

2025 年 8 月～2026 年 2 月

1.4　調査の体制

以下の者が本調査を実施した。

依田 達郎　　公益財団法人未来工学研究所 政策調査分析センター 主席研究員
多田 浩之　　公益財団法人未来工学研究所 政策調査分析センター 研究参与
衛藤 幹子　　公益財団法人未来工学研究所 政策調査分析センター シニア研究員
大竹 裕之　　公益財団法人未来工学研究所 政策調査分析センター 主任研究員
多喜沢 操児 公益財団法人未来工学研究所 政策調査分析センター 研究員
板垣 真吾　　公益財団法人未来工学研究所 政策調査分析センター 客員研究員

調査の全体取りまとめは依田が、意見交換会の企画・運営は依田・大竹が、各国・地域の調査は依田・多田・衛藤・大竹が担当した。報告書作成については、海外取組（米国・カナ

ダ）・意見交換会について依田が、海外取組（英国・オランダ）について多田が、海外取組（欧州連合、ドイツ、イタリア）について衛藤が、海外取組（オーストラリア）・バーチャルアカデミー運営支援等について大竹が担当した。

本調査の実施に当たっては、意見交換会に参加いただいた有識者の方々、研究セキュリティ・インテグリティ関連業務の担当教員・職員の方々、内閣府の調査担当者にご協力を頂いた。また、海外取組の調査に当たっては、Jacqueline Littlewood 様（アルバータ大学）、Scott Willoughby 様、Andy Hondrez 様（アデレード大学）、Zoe Naden 様（オーストラリア研究評議会）、Sergiu-Matei Lucaci 様（欧州大学協会）、Pawel Mariusz Rowinski 様、Matthias Johannsen 様（全欧州アカデミー）、Barbara Sturm 様、Ewa Adamkiewicz 様、Dominik Brunch 様、Maike Schroeder 様（ライプニッツ農業科学・バイオエコノミー研究所）にヒアリングにご協力いただいた。ここに記して謝意を表する。

本報告書は委託業務の成果として未来工学研究所が取りまとめたものである。本文中の見解は、ヒアリング協力者および関係機関の公式見解を示すものではない。

第2章　各国・地域における研究セキュリティ・インテグリティに関する大学・研究機関等、資金配分機関等による取組

研究活動の国際化、オープン化に伴う新たなリスクの軽減や管理に、各国の政策やガイダンス等を受けて、大学・研究機関、研究資金配分機関がどのように取組んでいるのか等に関して調査した。以下、調査の結果を、米国、カナダ、英国、オーストラリア、欧州連合、オランダ、ドイツ、イタリアの順に説明する。事例等の比較・分析は第 5 章で行った（231 頁以降参照）。

2.1　米国

2.1.1　研究セキュリティ・インテグリティ関連政策動向

米国の研究セキュリティ政策は、①研究者レベルの「透明性（ディスクロージャー）」強化と、②組織レベルの「研究セキュリティ・プログラム（Research Security Program）」整備等を、National Security Presidential Memorandum -33（NSPM-33）（2021 年）と CHIPS and Science Act（2022 年）（CHIPS 科学法）で制度化[1]し、連邦政府機関、資金配分機関等が実装を進めることで骨格が形づくられている（図 2-2・図 2-3 を参照）。米国科学財団（National Science Foundation: NSF）が公開する共通様式（Common Forms）に代表されるように[2]、標準化（「経歴・実績」（Biographical Sketch）、「現在・申請中の（その他の）研究支援」(Current & Pending (Other) Support)）が進み、外部支援・活動の開示や、悪性海外人材採用プログラム（Malign Foreign Talent Recruit Program: MFTRP）への関与がないことの自己証明が、提案・採択後の双方で要求される方向が明確になっている。[3]

米国の研究セキュリティ・インテグリティに関する主な法律・連邦指針

- 2018 年　National Defense Authorization Act (NDAA)（国防授権法）[4]（以降、毎年度）
- 2021 年　National Security Presidential Memorandum -33（NSPM-33）
- 2022 年　CHIPS and Science Act（CHIPS 科学法）
- 2024 年　OSTP「Guidelines for Research Security Programs at Covered Institutions」

組織側の実装要件は、2024 年 7 月の大統領府科学技術政策局（Office of Science and

[1] これらの制度の内容については、2.1.2、2.1.3 を参照。
[2] NSF. NSPM-33 Implementation Guidance　https://www.nsf.gov/policies/nspm-33
[3] NSF　https://www.nsf.gov/research-security　など
[4] 国防権限法（NDAA）は、米国軍隊、国防省及びその他重要な防衛優先事項に対する予算配分の水準を承認し、権限を付与する連邦法である（実際の支出金額は国防支出法（Defense Appropriations Act）で決定される）。US Senate Committee on Armed Service. “Fiscal Year 2025 National Defense Authorization Act Executive Summary” https://www.armed-services.senate.gov/imo/media/doc/fy25_ndaa_executive_summary.pdf

Technology Policy: OSTP）「Guidelines for Research Security Programs at Covered Institutions」（対象機関における研究セキュリティプログラムガイドライン）で具体化された。連邦政府からの研究資金受領が年 5,000 万ドルを超える「covered institutions」（対象機関）は、研究セキュリティ・プログラム（(1)サイバーセキュリティ、(2)海外渡航セキュリティ（教育・報告）、(3)研究セキュリティ研修、(4)（必要に応じた）輸出管理研修）を整備していることについて、資金配分機関に対して認証（certification）することが求められる[5]。

連邦政府研究資金受領が 5,000 万ドル以下の大学等でも、PI（研究室主宰者）とシニア・キーパーソン（covered individuals[6]）単位で開示や研修、MFTRP 不関与の証明が実務上の標準になりつつある。例えば国立衛生研究所（National Institutes of Health: NIH）は、研究セキュリティ研修（直近 12 か月以内の受講）[7]や、MFTRP に現に関与する者を研究プロジェクトのシニア／キーパーソン（主要研究者）にできないこと等を、申請・人選プロセスに組み込む方針を段階的に明確化している。さらに、研究者識別の強化（ORCID 等のデジタル永続識別子の活用）も NSPM-33 実装の一部として、各省庁の要件化が進んでいる。

また、国防分野では、NDAA（2018 年）に基づく国防省（Department of Defense: DoD）[8]の“Section 1286”リスト公表など、リスク情報の提示を継続している。

加えて、ナショナルアカデミーは、高等教育における研究セキュリティの取組の評価・論点整理を進めるとともに、オープンな国際協力と不当干渉対策の両立について、関係者（政府、資金配分機関、大学・研究機関等）が議論する場となっている。

---

[5] OSTP. Guidelines for Research Security Programs at Covered Institutions. July 9, 2024. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf

[6] PI と主要研究者が複数いる場合には covered individuals、単独の場合には covered individual になるが、以降は特に両者を区別しない。

[7] Research Security Training Requirements for NIH. Notice Number: NOT-OD-26-017. December 2, 2025 https://grants.nih.gov/grants/guide/notice-files/NOT-OD-26-017.html

[8] 2025 年 9 月 5 日の大統領令で、国防長官・国防省が「Department of War」「Secretary of War」などの追加の二次的（secondary）な呼称を、非法令文書や対外広報などで使えるようになったが、現在（2026 年時点）の法令上の正式名称は基本的に「Department of Defense」である。（Restoring the United States Department of War. Executive Orders. September 5, 2025. https://www.whitehouse.gov/presidential-actions/2025/09/restoring-the-united-states-department-of-war/）

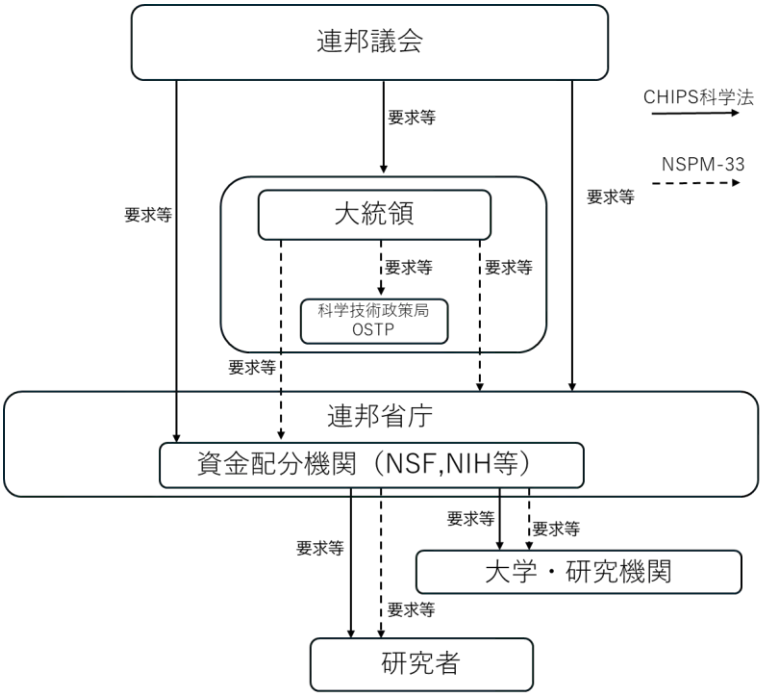


図 2-1　米国の研究セキュリティ確保のための施策等の関係機関

(1)　2024 年度までの経緯

表 2-1 は、一部、上記の繰り返しになるが、米国における研究セキュリティ・インテグリティ関連の連邦レベル文書を、時系列に整理したものである。2019 年の JASON レポート「Fundamental Research Security」[9]で問題認識・論点整理が行われ、大統領府による政府横断の基本方針（NSPM-33）の提示、現場実装に向けた推奨実務・実施ガイダンスの策定、CHIPS 科学法による法的裏付けの強化を経て、2024 年 OSTP ガイドラインにより、対象機関（covered institutions）に求められる研究セキュリティ・プログラムの要件が明確化される、という段階的な制度化の流れが確認できる。研究者個人の活動の透明性確保（開示等）と、大学・研究機関としての組織的管理体制の整備を、連邦政府全体で標準化していくプロセスを示していると言える。

表 2-1　近年の研究セキュリティ・インテグリティ関連文書（大統領府、連邦政府省庁）

発行年	文書名	発行元
2019	JASON レポート（Fundamental Research Security）	JASON The MITRE Corporation（NSF 委託調査）
2021.1.14	National Security Presidential Memorandum – 33 (NSPM-33)（Presidential Memorandum on United States Government-Supported Research and Development National Security Policy）	ホワイトハウス（第 1 次トランプ政権）
2021.1.19	Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise （出典 2）	Subcommittee on Research Security, Joint Committee on the Research Environment, National

[9] JASON. Fundamental Research Security. JSR-19-2I. MITRE Corporation. December 2019.

発行年	文書名	発行元
		Science & Technology Council
2022.1.4	Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33). (出典 3)	ホワイトハウス
2022 年 8 月	CHIPS and Science Act	連邦議会
2024 年 7 月	「対象機関における研究セキュリティプログラムガイドライン」（Guidelines for Research Security Programs at Covered Institutions）	OSTP

出典 1)「研究インテグリティ（Research Integrity）に係る調査・分析報告書」（未来工学研究所、2023 年 3 月、7 頁）を更新。
2)https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf
3)https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf

(2) 最近の主な動き（2025 年 3 月以降）

2025年3月以降に公表された主要文書群は、NSPM-33およびCHIPS科学法、さらに2024年OSTP研究セキュリティプログラムガイドラインで示された、連邦政府省庁横断の研究セキュリティ方針を、各機関が運用要件として定着させる段階（実装の深化）に入ったことを示している（「米国の研究セキュリティ関連の公表文書（2025年3月～2026年2月）」については44頁以降を参照）。特徴は、（1）資金配分機関による申請・管理プロセスへの要件組込み、（2）国防分野での基礎研究を対象とした対策強化、（3）議会・監査機関・ナショナルアカデミーによる監督・評価・制度調整、の三層が同時進行している点にある。

第一に、資金配分機関（NSF、NIH等）では、NSPM-33、CHIPS科学法等の要件の助成金公募プロセスへの実装を更に進めた。NSFの「重要通知」（2025年7月公表）[10]は、NSFM-33とCHIPS科学法の枠組みを踏まえ、NSFとしての研究セキュリティ関連ポリシーを更新・整理するものであり、大学・研究機関にとっては、何が変わり、何が継続要件なのかを把握する参照点となる文書である。NIHにおいては、Other Support（その他支援）の開示に関する研修義務を新たに明確化し、申請時点からのコンプライアンス確保を重視している[11]。また、研究者の「経歴・実績」（Biosketch）と「現在及び申請中の（その他の）研究支援」（Current & Pending（Other）Support）について連邦政府省庁で統一された共通様式（Common Forms）を採用し、提出様式・提出手順の整合を図っている[12]。これらは、研究者の開示・研修・様式を巡る運用を、機関ごとのばらつきがある状態

[10] NSF Important Notice No. 149「Updates to NSF Research Security Policies」（2025 年 7 月 10 日発出、11 月 24 日更新）
https://www.nsf.gov/notices/important/important-notice-no-149-updates-nsf-research-security/in149
[11] NIH Announces a New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements. Notice Number: NOT-OD-25-133. Release Date: July 17, 2025. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-133.html
[12] NIH's Implementation of Common Forms for Biographical Sketch and Current and Pending (Other) Support for Due Dates on or after January 25, 2026. Notice Number: NOT-OD-26-018. Release Date: December 2, 2025. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-26-018.html

から、政府横断の統一運用へ近づける動きであり、大学・研究機関側の事務・管理プロセスにおいて、研究セキュリティ・インテグリティに関し、研究者への周知、年次研修、様式点検、記録保持等を平時から実施することを促している。

第二に、国防省（DoD）の文書「国防省基礎研究ガイダンス」（2025年8月公表）[13]は、基礎研究（fundamental research）の位置づけを確認しながら、研究セキュリティ要求がどのように適用され得るのかを整理することで、学術的自由・公開性と安全保障上の要請の間で運用上の予見可能性を高める狙いを持つ。加えて、国防省の「セキュリティ施策と実施」文書（2026年1月公表）[14]では、悪性外国影響、知財窃取、研究成果の搾取といった脅威に対し、（i）特定リスト掲載企業への助成資金供与を行わないこと、（ii）国防省の省内横断のリスク審査情報を集約・共有するリポジトリを新設すること等の措置が示されている。

第三に、議会・監査機関（GAO）・ナショナルアカデミー等が公表する報告書等には、研究セキュリティに関して、監督（アカウンタビリティ）の一層の強化を求める動きと、制度の副作用の抑制を模索する動きの両方がみられる。例えば、下院中国特別委員会等の報告書（2025年12月公表）[15]は、中国との関係を軸に、国防・エネルギー分野を含む政府機関の研究セキュリティ対応の不備や、大学との連携形態（Joint Institutes等）、さらには人の移動（ビザ政策）まで論点を拡張し、行政機関に対して改善を強く求めている。他方、ナショナルアカデミー主催のワークショップ（2025年5月開催）では、大学における研究セキュリティ対策が実際にどの程度効果を上げているのかという実効性評価の観点を提示するとともに、研究規制・ポリシーの断片化が大学側に過大な事務負担と不確実性を生んでいる点を整理し、規制領域を俯瞰した最適化・簡素化の議論を進めた[16]。さらに政府説明責任局（Government Accountability Office: GAO）報告書（2026年1月公表）[17]は、研究セキュリティ強化が特定の人種・民族・出身（中国系／アジア系研究者等）を不当に標的化し得るという懸念に焦点を当て、主要助成機関における差別防止策の整備・運用状況を点検した。

米国の研究セキュリティ政策が、①資金配分機関における申請・管理の標準化（共通様式、研修義務、開示の厳格化）を通じて大学・研究機関の管理運営実務、研究者の研究資

---

[13] 国防省（DoD）「Department of Defense Fundamental Research Guidance」（2025 年 8 月 4 日）https://basicresearch.defense.gov/Portals/61/Documents/Research%20Security/Fundamental%20Research%20Guidance.pdf

[14] Department of War. The War Department Strengthens Measures to Protect DOW-Funded Research. Jan. 8, 2026. https://www.war.gov/News/Releases/Release/Article/4373247/the-war-department-strengthens-measures-to-protect-dowfunded-research/

[15] Select Committee on China, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence. Containment Breach: The U.S. Department of Energy's Failures in Research Security and Protecting Taxpayer-Funded Research from Foreign Exploitation. December 17, 2025. https://files.constantcontact.com/f0eecb46901/92d4c0a9-93b3-463d-a212-fa82a9e229e4.pdf

[16] National Academies of Sciences, Engineering, and Medicine, Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop, Washington, DC: The National Academies Press, 2025. https://www.nationalacademies.org/publications/29241　など

[17] GAO. Research Security: Agencies Should Assess Safeguards Against Discrimination. GAO-26-107544. Published: Jan 21, 2026. Publicly Released: Jan 22, 2026. https://www.gao.gov/products/gao-26-107544

金受領プロセスに深く組み込まれ、②国防分野では基礎研究を対象に開放性を維持しつつ、より効率的・効果的にリスク情報基盤や助成制限等の執行力を高め、また、③議会・GAO・ナショナルアカデミー等が、一方では更なるリスク・脅威対応の強化を求めつつ、他方で実効性評価、規制の断片化による負担、差別的運用の防止といった面からの調整を模索するという状況である。米国において、研究セキュリティは方針の提示段階を越えて、運用の細部（手続・教育・データ・審査インフラ）と、その副作用（負担・不確実性・公平性）まで含めた制度成熟の局面に入ったと考えられる。

2.1.2　大学・研究機関における取組

米国の連邦レベルの研究セキュリティ確保のための制度の骨格は、既に説明したように、大統領令 NSPM-33（2021 年）[18]で示され、CHIPS and Science Act（CHIPS 科学法）で法定化され、OSTP の 2024 年研究セキュリティプログラムガイドラインが連邦研究費の受領金額が大きな（年間 5000 万ドル超）研究大学に対して何を「研究セキュリティ・プログラム」として備えればよいかを標準要件として具体化した。

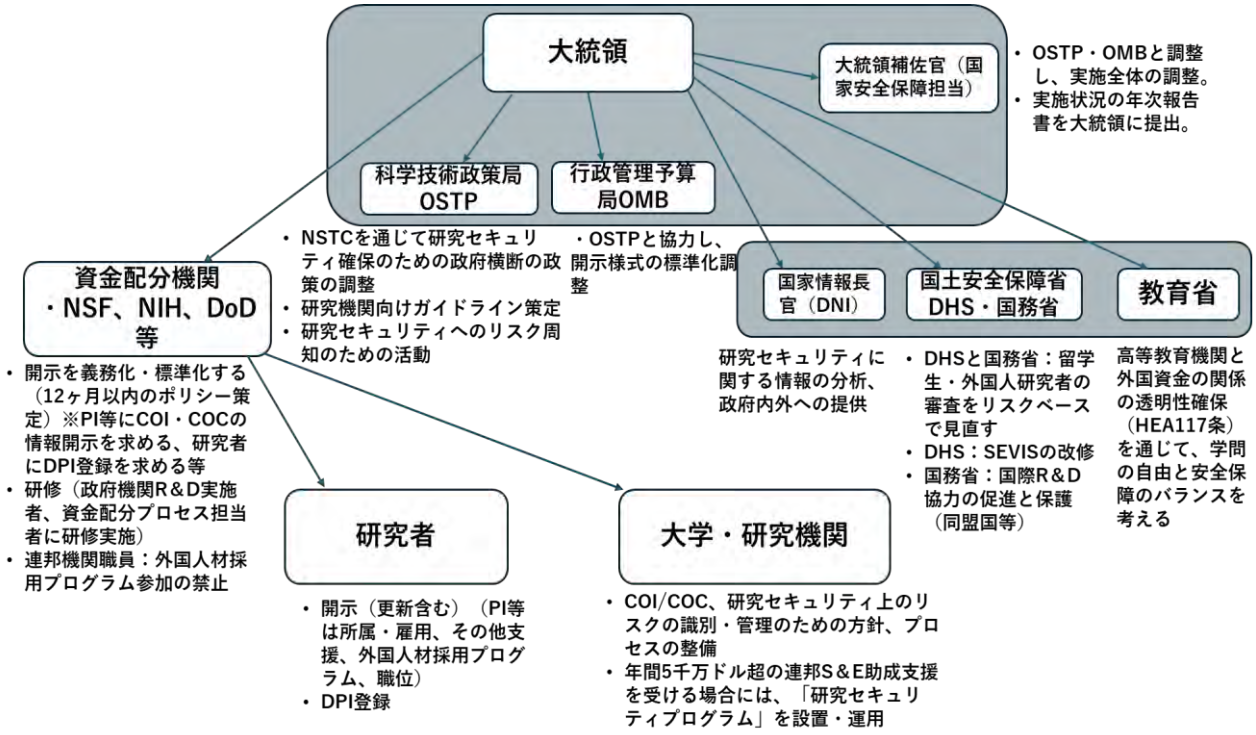
NSPM-33 は主として資金配分機関への指示として書かれており、大学・研究機関への要求は、実務上は助成の申請・受領条件（認証（certify）、開示（disclose）、研修（train））として資金配分機関を通じて行われる。

- 研究者・審査関与者に求める「開示（disclosure）」の標準化：NSPM-33 は、連邦助成に関わる人々（特に PI（Principal investigator（研究室主宰者））や senior/key personnel 等）に対して、以下を申請時と年次更新で開示させ、訂正機会も確保するよう求める。
  - ✓ 所属・雇用（affiliations/employment）
  - ✓ Other support（国内外・金銭/非金銭を含む研究支援）
  - ✓ 外国政府スポンサーの人材採用プログラム（海外人材採用プログラム）等への参加
  - ✓ 職位・兼職（国内外、無報酬の称号職等も含む）
- 個人識別の基盤としてデジタル永続識別子（Digital Persistent Identifier: DPID）：例として ORCID 等を想定）の登録・利用を助成条件に組み込む。

NSPM-33 は、年 5,000 万ドル超の連邦研究助成金支援を受ける大学・研究機関に対し、研究セキュリティ・プログラム（RSP）を整備・運用している旨の認証（certify）を求めることを、資金配分機関に指示している。RSP の中身として、サイバー、外国渡航、インサイダー脅威、（必要に応じ）輸出管理研修等を含む。OSTP ガイドライン（2024 年 7 月）は、これを実装するために covered institution の定義を明確にし（高等教育機関

[18] Presidential Memorandum on United States Government-Supported Research and Development National Security Policy. January 14, 2021. National Security Presidential Memorandum-33 https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

（IHE）、連邦資金研究開発センター（FFRDC）または非営利研究機関で、連邦 R&D 資金受領金額の過去 3 年平均が年 5,000 万ドル超〔FY2022 ドル換算〕等）、RSP に最低限含めるべき要素を(1)サイバー、(2)外国渡航、(3)研究セキュリティ研修、(4)輸出管理研修として標準化した（その他の NSPM-33 の要件等については図 2-2 を参照）。



注：矢印は NSPM-33 において、ポリシー策定、開示等を要求する関係を示す。
出典；National Security Presidential Memorandum-33 の内容に基づいて図を作成。

図 2-2　NSPM-33 の内容と主要アクターの役割

また、CHIPS 科学法では、「悪性海外人材採用プログラム」（Malicious Foreign Talent Recruitment Program: MFTRP）に関して、資金配分機関が助成制度に禁止・認証要件を組み込むことを求めた。申請書に記載される covered individual（対象者）が MFTRP の当事者でないことを申請時と、その後毎年認証し、大学・研究機関側も、対象者に要件を周知し遵守させている旨を機関として認証することが求められる。

CHIPS 科学法は、資金配分機関に対し、covered individual が「過去 1 年以内に研究セキュリティ研修を修了」したことを認証させ、大学・研究機関も同様に所属する対象者の修了を認証させる制度設計を義務づけている。研修内容は、サイバー、国際連携・渡航、外国からの介入、資金の適正使用、開示、利益相反・責務相反などを含む。また、研究セキュリティの実装が人種・民族・出身国に基づく差別を生まないようにするという明示的要請がある。（その他の CHIPS 科学法の要件については表 2-2 と図 2-3 を参照）

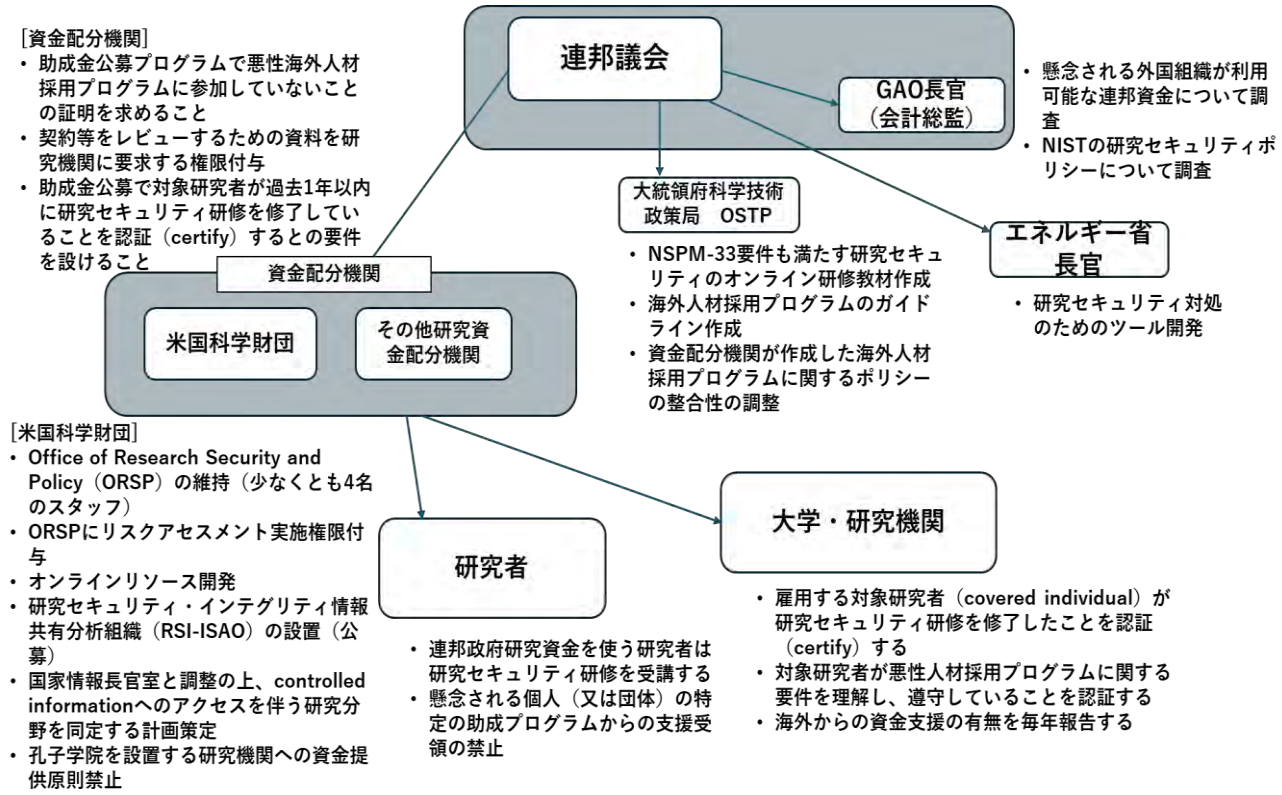
表 2-2　The CHIPS and Science Act of 2022 の研究セキュリティ関連の規定の概要

※青は要求事項（連邦省庁・資金配分機関に対する要求）、橙色は支援事項（研究組織・研究者への支援関連（係る支援についての、連邦省庁に対する要求を含む））。

大統領府科学技術政策局（OSTP）への要求項目	海外人材採用プログラム（Foreign Talent Recruitment Programs）のガイドライン作成（Sec.10631） ・（FY2020 NDAA 1746 条に基づき設立された）省庁間ワーキンググループと連携し、「連邦研究機関」（注参照）に対し、海外人材採用プログラムに関する統一したガイドラインを配布することを OSTP に要求。ガイドラインは、各連邦研究機関のすべての職員が海外人材採用プログラムに参加することを禁止し、海外人材採用プログラムの特徴を定義して説明する。21 年度 NDAA のセクション 223 に従い、covered の個人は、海外人材採用プログラムの契約、協定、または取り決めの当事者である場合、情報開示しなければならない。covered の個人は、悪性海外人材派遣プログラムに参加することはできない。 *注）本法律では、連邦研究機関（Federal research agency）は年間 1 億ドル以上の研究開発費を支出する連邦省庁を指す（資金配分機関を含む）。*
資金配分機関等への要求項目 （一部は、資金配分機関から研究者・研究機関への要求項目）	悪性海外人材採用プログラム（Malign Foreign Talent Recruitment Program）の禁止（Sec.10632） ・各連邦研究機関に対し、研究助成金提案プロセスの一環として、提案書提出時又はその後毎年、助成期間中、対象個人が悪性海外人材採用プログラムに参加していないことを証明するよう求める方針を確立することを要求する。
	契約等をレビューするための資料を研究機関に要求する権限付与（Sec.10633） ・各連邦研究機関は、要請に応じて、研究開発助成の申請書に記載された全ての対象者について、海外人材採用プログラムへの参加に特有の契約書、補助金、又は外国人の任命、外国機関への雇用、その他の合意書の写しを含む、補足書類を提出するよう機関に求める権限を有している。研究機関と協議の上、契約、助成金、協定が、機関が支援する活動の能力を阻害する、または機関が支援する活動との重複を生じさせると判断された場合、研究機関と機関は、対象者の代替または助成からの除外、助成額の削減、助成の停止/終了を開始することができる。各連邦機関は、最終的な行政措置が取られる前に、全ての対象者のプライバシーを保護し、措置の正当な理由を提供し、対象者にコメントや反論を提供し、上訴する機会を与えるために必要な措置を講じるべきである。
	連邦政府研究資金を使う研究者：研究セキュリティ研修要件（Sec.10634） ・　連邦研究機関は、研究資金の公募申請の一部として、申請書に記載された各対象者は研究セキュリティ訓練の修了（過去 1 年以内）を certify するという要件を設ける。 ・　大学・研究機関は、雇用されている各対象者がそのような訓練を修了していることを certify する。 ・　研究セキュリティ研修の内容は、サイバーセキュリティ、国際共同研究、海外渡航、海外からの介入、資金の適切な使用に関する規則、情報開示、コミットメント相反、利益相反に焦点を当てる。
Comptroller General への要求項目	研究資金の会計（Sec.10635） ・Comptroller General（※GAO の長官）に対し、研究のために懸念される外国組織が利用できる連邦資金に関する調査を実施することを要求する。この調査は、研究のために懸念される外国組織が利用できる連邦資金の量、種類、要件に関する評価を含むものとする。
NSF への要求項目 （一部は、NSF から研究者・研究機関）への要求項目	Office of Research Security and Policy と Chief of Research Security の維持（Sec.10331-10332） ・NSF に、NSF 長官室内に少なくとも 4 名のフルタイムスタッフを擁する Research Security and Policy オフィスを維持することを要求。
	Office of Research Security and Policy にリスクアセスメントの実施権限を付与（Sec.10336） ・NSF の監察官室（OIG）と連携して、NSF Office of Research Security and Policy が、研究開発助成の申請と NSF への情報開示について、オープンソースの分析・解析ツールの利用を含むリスク評価を実施する権限を付与する。
	オンラインリソースの開発（Sec.10334） ・NSF に対し、研究組織および個人の研究者向けに、最新情報を含むオンラインリ

	ソースを開発するよう要請。
	研究不正等についての研究の公募継続（Sec.10335） ・NSF に対し、研究不正や研究インテグリティの侵害、有害な研究行為に関する研究を含む、研究行為や研究環境に関する研究を支援するための研究助成を継続することを要求。
	責任ある研究実践についての研修（Sec.10337） • 責任ある研究実践についての研修に関する 2007 年 America COMPETES Act の Sec.7009 を修正。ポスドク研究者、教員、上級職員を含めるよう要件を拡大。 • プログラムは、メンター（研究指導者）の訓練、メンターシップ、潜在的な研究セキュリティの脅威に対する認識を高めるための訓練、連邦輸出管理・情報開示・報告要件に関する訓練を含むことを明記。
	Research Security and Integrity Information Sharing Analysis Organization の外注（Sec.10338）
	機密情報（Controlled information）へのアクセスを持つ研究分野を同定する計画作成（Sec.10339） ・NSF に対して、国家情報長官室（Office of the Director of National Intelligence: ODNI）及び他の連邦機関と協議の上、主要技術重点分野を含む NSF が支援する研究分野で、管理された非機密情報（controlled unclassified information: CUI）または管理された機密情報（controlled classified information）へのアクセスを伴う可能性のあるものを特定する計画を策定するとともに、研究助成に関して働く NSF 職員または NSF 研究開発助成の対象者に CUI または controlled classified information へのアクセスを適宜付与するにあたりデュー・ディリジェンスを行うことを要求。
	孔子学院を設置する研究機関への資金提供の原則禁止（Sec.10339A）
	研究倫理・社会的影響について公募提案書への記載を求める（Sec.10343） ・NSF に対し、利害関係者からの意見を踏まえ、助成金提案の指示書（instruction）を改訂し、研究開発費の支給に先立ち、倫理的・社会的配慮を提案の一部として含めることを義務付けることを要求する。利害関係者の意見を考慮し、NSF は何をもって「容易に予見可能または定量化可能なリスク（readily foreseeable or quantifiable risk）」とするかについて明確なガイダンスを作成する。
エネルギー省長官への要求項目	研究セキュリティに対処するツールの開発（Sec）10114） ・エネルギー省長官に対し、国家情報長官室が特定した脅威を反映した科学技術リスクマトリックスなど、研究セキュリティリスクを管理・軽減するためのツールやプロセスを開発・維持し、対象となる支援の下で実施される活動がもたらす米国の知的財産喪失のリスクや米国の国家安全保障への脅威を判断しやすくするよう要請。
GAO への要求項目	GAO（Government Accountability Office）に対して国立標準技術研究所（National Institute of Standards and Technology: NIST）の研究セキュリティポリシー、プロトコル等についての調査研究を行うよう要求（Sec. 10247）
大学等研究機関への要求項目	NSF に海外からの資金支援の有無を毎年報告（Sec.10339B） ・研究機関は、毎年 NSF に対し、贈与や契約を含め、当該機関が懸念される外国（foreign country of concern）に関連する外国資金源から直接または間接的に受ける 5 万ドル以上の現在の資金援助について、要約文書の形で報告しなければならない。
研究者等への要求項目	懸念される個人または団体の禁止。（Sec.10636） ・新設の NSF Directorate for Technology, Innovation and Partnerships を含む、特定のプログラムに対する grant、award、プログラム、支援、その他の活動を受けること又は参加することを、懸念事項とされた人物又は団体（persons or entities identified as a concern）に禁止する。

出典：AAU. The CHIPS and Science Act of 2022 (H.R. 4346): Research Security Provisions. Last updated August 8, 2022. https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf 等に基づき作成。（未来工学研究所「研究インテグリティ（Research Integrity）に係る調査・分析」（内閣府委託調査）（2023 年 3 月））



注：矢印は CHIPS and Science Act において、ポリシー策定、開示等を義務付ける等の関係を示す。
出典；CHIPS and Science Act の内容に基づいて図を作成。

図 2-3　CHIPS 科学法の研究セキュリティ関連の内容と主要アクターの役割

本セクションでは、上記の連邦政府レベルで整備された研究セキュリティ要件（NSPM-33、CHIPS 科学法、2024 年 OSTP ガイドライン等）が、大学・研究機関において、研究者の開示・研修、海外渡航、輸出管理、国際連携管理等の実務にどのように実装されているかを確認するため、マサチューセッツ工科大学（MIT）、テキサス A&M 大学システム、ワシントン大学を事例として取り上げる。これら 3 大学を選定した理由は、(i) 大規模な連邦研究資金[19]を背景に研究セキュリティ要件対応が組織運営上の主要課題になりやすいこと、(ii) NSF 資金で設置・運営がされている SECURE Center について、ワシントン大学が中核拠点として事業を主導し、Texas A&M 大学が分析機能（SECURE Analytics）を主導する[20]など、政府・学術コミュニティ横断の取組に深く関与していること、(iii) MIT は連邦政府の方針等の出る以前から研究セキュリティ関連の取組を開始しており参考になるであろうことである。

[19]連邦資金による R&D 支出は UW（Seattle）が約 11.89 億ドル、MIT が約 5.60 億ドル、Texas A&M（College Station 等）が約 5.46 億ドル（2023 会計年度）。National Center for Science and Engineering Statistics | NSF 25-314. Table 24 (Federally financed higher education R&D expenditures, ranked by FY 2023 R&D expenditures: FYs 2010–23). https://ncses.nsf.gov/pubs/nsf25314/assets/data-tables/tables/nsf25314-tab024.pdf

[20] NSF. NSF-backed SECURE Center will support research security, international collaboration. July 24, 2024. https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research

(1) マサチューセッツ工科大学（Massachusetts Institute of Technology）

マサチューセッツ工科大学（Massachusetts Institute of Technology: MIT）は、米国マサチューセッツ州ケンブリッジに所在する私立研究大学であり、工学・理学を中心に高い研究能力を有する。2019-2020 学年の在籍学生は合計 11,520 人（学部 4,530 人、大学院 6,990 人）で、学位課程の留学生は 3,331 人（学部 458 人（学部学生の約 10%）、大学院 2,873 人（大学院学生の約 41%））である。2019-2020 年には 118 の国から留学生が来ている[21]。MIT は国際的研究活動の規模が大きく、2020 年 3 月 1 日時点で、海外からの資金で実施する研究プロジェクトは約 2,000 件（72 か国と協力）とのことである[22]。

こうした国際的な研究資金、国際共同研究、海外との人材交流の厚みは MIT の研究力を支える一方、研究セキュリティ（開示、研修、輸出管理、海外渡航、外国からの不当干渉リスク管理等）の観点では、連邦政府要件への適合を含む組織的な取組が求められることとなる。

MIT は、以下に説明するように、研究活動の開放性を維持しつつ、国際研究交流のリスクを管理するため、1）中国戦略報告に基づく方針整理、2）高リスク・プロジェクト審査（Elevated-risk）、3）「10 のキーポイント」（Ten Key Points）による現場ガイド、4）「非公式国際協力ツール」（Informal International Collaborations (IIC) tool）による非公式連携の早期相談等の各種の取組を実施している。

(a) 背景・経緯等

MIT では、国際連携の拡大に伴うリスク管理を個別案件対応ではなく、大学全体のガバナンスとして早い段階から制度化してきた流れの中で、研究セキュリティ確保の取組が形成されてきた。2012 年に国際活動の調整・支援を担う国際調整委員会（International Coordinating Committee: ICC）が設置され[23]、2015 年に初代の国際活動担当副学長（Associate Provost for International Activities）として Richard Lester 教授（MIT School of Engineering）が任命された。さらに、2017 年に公表された報告書「A Global Strategy for MIT」では、国際活動の統治強化が提言され、国際助言委員会（International Advisory Committee: IAC）を学内の常設委員会として再構成した。IAC は、主要な国際関与に対して独立した教員の観点から助言・評価を行う[24]。

こうした体制整備を進める中で起こった 2018 年のカショギ事件[25]後に、学内の対サウジ関係を全学的に再点検し、国際的な研究連携は大学の価値・評判・人権等の論点と不可分

---

[21] MIT Facts 2020. https://facts.mit.edu/wp-content/uploads/2020/11/MIT-Facts-2020-Accessible-with-Cover-and-Map.pdf
[22] Richard Lester. On the Risks and Benefits of New International Engagements MIT Faculty Newsletter. Vol. XXXII No. 5., May/June 2020. https://fnl.mit.edu/may-june-2020/on-the-risks-and-benefits-of-new-international-engagements/
[23] MIT. International Coordinating Committee (ICC) https://globalsupport.mit.edu/about/international-coordinating-committee-icc
[24] MIT. A Global Strategy for MIT. Richard K. Lester (Associate Provost). May 2017. https://web.mit.edu/globalstrategy/A_Global_Strategy_For_MIT_May2017.pdf
[25] 2018 年 10 月、サウジアラビアのジャーナリストであるジャマル・カショギ氏がトルコのサウジアラ

であることを踏まえた意思決定が必要との見解が示された[26]。その後 2019 年 4 月、特定国等との案件を対象に「elevated-risk project review（高リスク案件審査）」を導入し、ICC による実務・コンプライアンス面の審査に加え、必要に応じて IAC によるレビュー、さらに最終判断を行う Senior Risk Group（SRG：国際担当、研究担当、法務の幹部で構成）へ付議する多層的プロセスを導入することとなった[27]。また、2018～2019 年頃に Huawei 社等との研究関係を打ち切り、対中案件を含む国際協力について慎重に審査し、必要に応じ SRG で最終判断をすることとなった[28]。

2022 年には、学内の China Strategy Group による検討を経て報告書「University Engagement with China: An MIT Approach」を公表し、「選択的関与」と「ターゲットを絞ったリスク評価・管理」を原則とすることを明文化した[29]。同報告書では、中国との大学間関与をめぐる原則・手順を整理し、ポスドク受入れ等では「国防七校」や軍・治安機関雇用者の受入れ回避など、具体的な線引きを示した。この報告はその後の大学実務への実装（Ten Key Points など（後述））の土台となった。連邦法令順守（コンプライアンス）とともに、それを超えた大学独自のリスク判断の枠組みを示している。報告書作成は Richard Lester 教授が主導した。

(b) 主な取組

i) 学内体制の整備

MIT では、研究セキュリティ（研究資産の保護、輸出管理・契約等のコンプライアンス、海外渡航・安全管理、不当な外部影響リスクへの対応等）を、個別部局の判断に委ねず、国際活動を横断的に支える統治体制として組み込んでいる。その中核が、上記のように、ICC である。ICC は、MIT における国際活動の規模と複雑性の増大を背景に、案件ご

ビア領事館で殺害された事件。BBC. “Jamal Khashoggi: All you need to know about Saudi journalist's death” 25 February 2021. https://www.bbc.com/news/world-europe-45812399

[26] Letter to the MIT community regarding engagement with Saudi Arabia. MIT News Office. February 6, 2019. https://news.mit.edu/2019/letter-regarding-mit-engagement-saudi-arabia-0206
Review and Reassessment of MIT’s Relationships with the Kingdom of Saudi Arabia: A Report to President L. Rafael Reif. Professor Richard K. Lester. Associate Provost. January 31, 2019. https://orgchart.mit.edu/system/files/reports/20190206-Lester-Report-13119.pdf

[27] Richard Lester. On the Risks and Benefits of New International Engagements. MIT Faculty Newsletter. May/June 2020Vol. XXXII No. 5. https://fnl.mit.edu/may-june-2020/on-the-risks-and-benefits-of-new-international-engagements/
New review process for 'elevated-risk' international proposals. April 3, 2019. https://orgchart.mit.edu/letters/new-review-process-elevated-risk-international-proposals

[28] Maria T. Zuber Written Testimony for House Committee on Science, Space and Technology Subcommittee on Investigations and Oversight March 5, 2025. https://democrats-science.house.gov/imo/media/doc/Zuber%20Testimony2.pdf

[29] University Engagement with China: An MIT Approach Final Report. November 2022. The MIT China Strategy Group (Richard Lester and Lily Tsai (co-chairs), Suzanne Berger, Peter Fisher, M. Taylor Fravel, David Goldston, Yasheng Huang, Daniela Rus). https://global.mit.edu/wp-content/uploads/2022/11/FINALUniversity-Engagement-with-China_An-MIT-Approach-Nov2022.pdf
未来工学研究所「研究インテグリティ（Research Integrity）に係る調査・分析」報告書（2022 年度内閣府委託調査）．74～78 頁.

とに生じ得るリスクや安全保障、法務・税務・財務コンプライアンス、文化的論点等に対応するため、教職員・学生の相談や国際交渉の促進、学内手続の改善を担う[30]。

ICC は、国際活動担当副プロボスト室（Office of the Vice Provost for International Activities）が事務局機能を担い、法務（Office of the General Counsel）、研究支援（Research Administration Services）、産学連携・技術移転（Office of Strategic Alliances, Transactions and Translation、Technology Licensing Office）、財務（Office of the Vice President for Finance）、研究統括（Office of the Vice President for Research）等、主要な大学事務管理部門の長で構成される。国際連携案件を大学運営の複数機能を束ねてレビューできる体制である。

また、MIT は、教員の視点から大学執行部へ助言する IAC を、学内の常設委員会（President 任命、Provost に報告）として位置づけている。IAC は、MIT の主要な国際的関与について、考案中・計画中・継続中・完了後の各段階でレビューを行い、国際的関与のポートフォリオが MIT の中核的使命（教育・研究・社会貢献）を実質的に前進させるかを検討する[31]。さらに、ICC 議長が IAC の ex officio メンバーとなっており、管理部門のデュー・ディリジェンスに、教員による学術的・価値的観点のレビューが加わるガバナンス構造となっている。

ii) ウェブサイトでの研究セキュリティの取組についての情報提供、説明

MIT では、研究担当副学長室（Office of the Vice President for Research: VPR）のウェブサイトページ「Research Security and Foreign Engagement」（研究セキュリティと海外関与）で、国際連携を原則支持しつつも、不当な外国影響（undue foreign influence）に関する注意喚起と、迅速な開示と透明性を軸とした学内プロセスを周知している[32]。助成金審査等、国際出張・会議、非公式な国際協力、提案書での開示、発明・知的財産の保護、機微な個人データ・政府関連データへのアクセス制限、関連規制・参照情報などについても詳しく説明している。

また、VPR のウェブサイトページ「Assessing and Mitigating Risk」（リスクの評価と軽減）では、1）海外人材採用プログラムへの関与、2）非公式な国際共同研究、3）米国外からの学生・研究者・訪問者受入れ、4）寄付受領、5）MIT 関連目的での海外渡航、6）国際的な会議・セミナー等への参加、といった場面別に、懸念国等による追加リスク、必要な開示、相談先等を説明している[33]。例えば、非公式な国際協力については、書面契約や資金授受がない場合でも輸出管理等の法令順守が必要であり、学内ツール（Informal International Collaborations tool）を用いたリスク評価を推奨する。

---

[30] MIT “International Coordinating Committee (ICC)”. https://globalsupport.mit.edu/about/international-coordinating-committee-icc/
[31] “International Advisory Committee” https://facultygovernance.mit.edu/committee/international-advisory-committee
[32] MIT “Research Security and Foreign Engagement” https://research.mit.edu/security-integrity-and-compliance/research-security-and-foreign-engagement
[33] MIT “Assessing and Mitigating Risk” https://research.mit.edu/security-integrity-and-compliance/assessing-and-mitigating-risk

さらに MIT は、国際活動の計画・運用を支える横断的支援として、MIT Global Support Resources（GSR）のウェブサイトページを作成している。GSR は国際担当組織と ICC の協働により、海外渡航の安全・手続、国際プロジェクト計画、プロジェクト・リスク管理（elevated-risk review を含む）、ビジター受入れ、学生派遣、国際合意、フィールド訪問など、国際活動の実務リソースを集約して提供している[34]。

iii） 研修の実施等

MIT では、連邦研究資金による研究活動に従事する PI、Co-PI、Senior/Key Personnel 等（NSPM-33 上の“covered individuals”）を対象に、研究セキュリティ研修の受講を義務化している。同研修は CHIPS 科学法（42 U.S.C. 19234 条）および NSPM-33 に基づく連邦要件に適合しており、MIT コミュニティ向けに学内学習基盤（Atlas Learning Center、Touchstone 認証）で提供される[35]。研修は合計約 90 分（1～1.5 時間）で、1）研究セキュリティ概論、2）開示（Disclosures）、3）リスクの管理・緩和（Manage and Mitigate Risk）、4）原則に基づく国際協力（Principled International Collaboration）の 4 モジュールで構成される（学外非公開）。研究提案書提出時には、過去 12 か月以内の受講がない限り MIT 内の審査プロセスに進めず、締切の少なくとも 5 営業日前までの研修受講完了を求めるなど、研究事務手続と直結させている[36]。

また、一回限りの研修受講で学習を終わらせない工夫として、MIT は PI 向けに、研究グループや指導学生等との対話を支援する「Research Security and Compliance Discussion Guide」（2024 年 3 月）を作成した。研究セキュリティ・インテグリティの基本概念、透明性、輸出管理、サイバーセキュリティ、国際渡航等の主要論点を、研究室内で共有・点検するための教材として利用可能である[37]。

iv） リスク判断支援ツールの作成

国際連携のうち、書面の合意や資金移転、成果物の提出義務を伴わない非公式な共同研究（informal collaborations）は、MIT 学内の通常の審査プロセスは経ないが、法的・財務的ペナルティや評判リスクを招き得る。このため、特に「追加リスクのある国」（elevated-risk countries）との協力を開始する前に、Informal International Collaborations（IIC）tool の利用を促している[38]。

IIC tool は、研究者が非公式連携について基本情報を入力すると、VPR のコンプライアンスチームが内容をレビューし、追加確認や懸念点があれば研究者に連絡する。さらに、

---

[34] MIT Global Support Resources. https://globalsupport.mit.edu/
[35] MIT “Research Security Training” https://research.mit.edu/security-integrity-and-compliance/training-courses/research-security-training
[36] Required training on research security for federal funding. September 10, 2025. Ian A. Waitz, Vice President for Research https://orgchart.mit.edu/letters/required-training-research-security-federal-funding
[37] MIT. Discussion Guide on Research Security and Compliance. March 2024. https://research.mit.edu/document/research-security-and-compliance-discussion-guide
[38] MIT. “Informal Collaborations” https://research.mit.edu/security-integrity-and-compliance/foreign-engagement/informal-collaborations

非公式連携であってもデータや研究資材の授受が発生する場合には、秘密保持契約・データ利用契約・MTA 等の必要性を学内ポータルの情報に基づいて検討すること、連邦助成による研究であれば資金配分機関ごとの開示ルールに従って活動を開示すること等が案内されている。なお、IIC tool 自体は MIT の証明書（MIT certificate）による認証が必要で、詳細手順は学内向けである一方、導入趣旨とフロー（入力→コンプライアンス審査→照会・助言）は MIT の学内宛レター（対外的に公開されている）で示されている[39]。

v） 高リスクプロジェクトレビュープロセス（Elevated-risk project review process）

MIT は、国際連携を推進する一方で、特定の国・案件については通常の国際プロジェクトの審査に上乗せする追加レビュー（elevated-risk project review）を行う。現在、中国（香港を含む）・ロシア・サウジアラビアとの関与について、追加のレビューを行うことでリスクを同定・管理し、国際協力の成功確率を高める旨を明示している[40]。大学としての価値観に基づき、人権・評判・安全まで含めたデュー・ディリジェンスを行う。

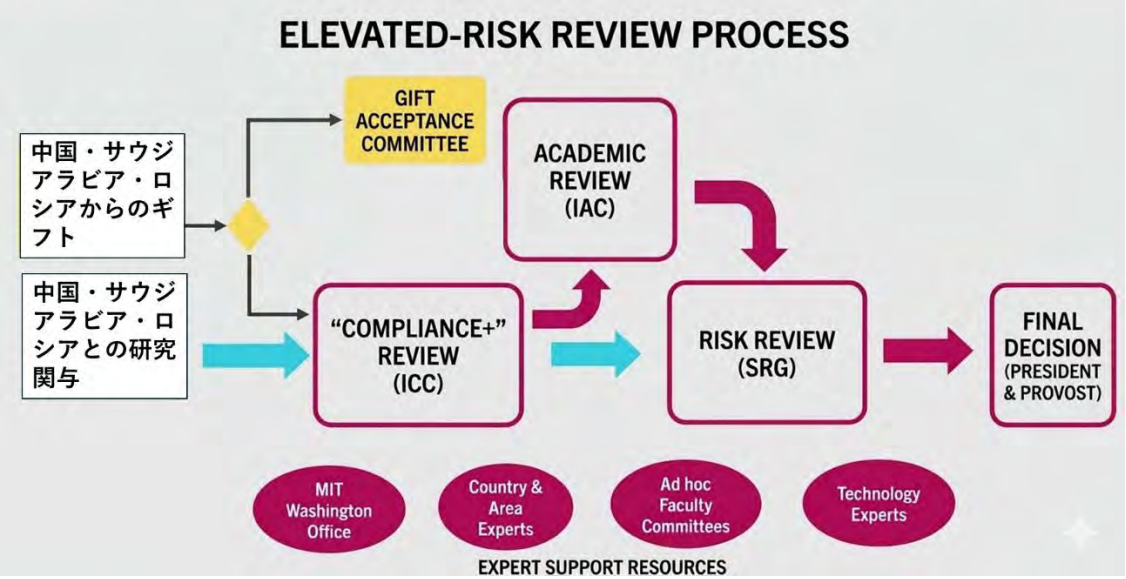
追加レビューの対象は、これら 3 か国の個人・組織から資金提供を受けるプロジェクト、MIT の教職員・学生が当該国で活動するプロジェクト、当該国の個人・組織との共同プロジェクトである。「プロジェクト」とは MIT が正式な契約関係・合意に拘束される関与（formal MIT contractual relationships and agreements）を指し、非公式・アドホックな協力は含まれない。当該 3 か国からの寄付（gifts）にも適用され、Gift Acceptance Committee の審査に付される。3 か国に限らず ICC が高度のリスクがあると判断した案件が追加レビュー対象となることがある。国際情勢の変化に応じて対象国・対象案件が変更され得ることも明記されている。

審査で評価されるリスクは、1）米国の国家安全保障、2）政治・市民的自由・人権、3）米国の経済競争力（経済安全保障）、4）MIT コミュニティの価値・学術的使命との整合（差別の誘発や不当な外部影響の許容を含む）、5）知的財産・輸出管理・データセキュリティ／アクセス・評判リスク等に加え、6）「受けないこと」に伴う MIT 側のリスク（代替困難な実質的利益の有無を含む）まで含めて多面的に点検する設計である。

運用プロセスは、まず、ICC が財務・法務・税務・輸出管理・運用等の観点からデュー・ディリジェンスを行い、PI（研究代表者）に対して想定リスクと緩和策を助言する（反復的に案件を磨き、承認可能性を高める設計）。次に、必要に応じて教員主導の常設委員会 IAC が、MIT の中核的学術的使命（教育・研究・社会貢献）を前進させる観点からレビューする。さらに、なお重要な残余リスクがある場合、国際担当副プロボスト（Vice Provost for International Activities）、研究担当副学長（VPR）、法務責任者（Vice President and General Counsel）で構成されるシニアリスクグループ（Senior Risk

[39] MIT. A new resource for informal international collaborations
January 18, 2023. Maria T. Zuber, Vice President for Research, 2013–2024 | Ian A. Waitz, Vice Chancellor for Undergraduate and Graduate Education, 2018–2024.
https://orgchart.mit.edu/letters/new-resource-informal-international-collaborations
[40] MIT Global Support Resources. “Elevated-risk project review process”
https://globalsupport.mit.edu/managing-project-risk/elevated-risk-project-review-process/ 等

Group: SRG）が最終判断を行い、「リスク管理計画付きで承認」または「不承認（実施不可）」を決定する。SRG の審査は MIT Washington Office や国・地域専門家等の支援も必要に応じて受けて行われる（図 2-4 を参照）。



出典：MIT. “Elevated -risk review process”に基づき作成。https://globalsupport.mit.edu/wp-content/uploads/2024/10/elevated-risk-review-process-1-slide-10-03-2024.pdf

図 2-4　MIT の高リスクレビュープロセス

vi)　国際関与に関する「10 のキーポイント」行動指針の作成

MIT は、前述の学内の対中関与に関する報告書（MIT China Strategy Group 報告、2022 年）の提言のうち教員・PI の行動を要する点を、参照シート「Ten Key Points for MIT Faculty & PIs When Engaging Internationally」（MIT の教員および PI が国際的な活動を行う際の 10 の要点）に整理して周知している。「中国への対応として有用である一方、他国との国際協力にも概ね当てはまる」点を明確にし、国際連携を萎縮させるのではなく、便益を最大化しつつリスクを最小化することが意図されている[41]。

10 項目行動指針では、1）正式な国際連携（契約・合意に基づくもの）については、研究便益とリスクを初期段階から見積もり、必要に応じて、MIT の追加レビュー（elevated-risk review）を受けること、2）審査の外に置かれがちな非公式な国際協力については、開始前に IIC tool を通じて連邦法令・機関要件に関する助言を得ることとし[42]、そのうえで、3）研究室内で情報共有・対外共有の規範を定期的に確認し、学生が独自に国際連携に入る前に PI へ相談する運用を徹底し（上記の PI 向けディスカッションガイド等も活用）、4）海外渡航時（特に高リスク国）には端末・データ保護、輸出管理、通関・ビザ等の論点を踏まえ事前準備を行い（安全な貸与端末の活用も推奨）、5）高リスク国からの短

[41] MIT. ”10 key points to consider when engaging internationally” June 5, 2023. Maria T. Zuber, Vice President for Research, 2013–2024 | Richard Lester, Associate Provost for International Activities, 2015–2023　https://orgchart.mit.edu/letters/10-key-points-consider-when-engaging-internationally
[42] MIT. “Mitigating risk”　https://globalsupport.mit.edu/managing-project-risk/mitigating-risk/

期訪問者を招へいする際は IIC tool 等で事前助言を得る、といった、運用上のボトルネックを具体的な行為レベルで説明している。

さらに、6）外国主体からのコンサル等の報酬を受ける前に利益相反・学外活動・スポンサー向け開示義務を点検すること、7）技術移転や情報提供の見返りとして便益供与が行われ得る悪性海外人材採用プログラムへの関与を回避すること、8）卒業生を高リスク国の職へ誘導することを目的としたプログラムに組織的に関与しないこと、9）有償の活動と引き換えに推薦状を書くような“quid pro quo”（交換条件、取引条件）を避けること、10）迷った場合は研究コンプライアンス部門に相談することを含む。研究セキュリティを法令遵守だけでなく、人材・渡航・訪問者・利益相反・人材採用等を横断する実務規範として定着させることを意図した内容となっている。

(c)　特色・注目点等

MIT の研究セキュリティ対応の注目点は、国際連携を萎縮させるのではなく、活動の透明性を開示で確保し、実務プロセスとして安全に回す方針を前面に出している点にある。研究担当副学長室（VPR）は、対外関与に伴う論点（開示、データ、知財、渡航等）を整理し、研究者が迷ったときの相談先も含めて学内に周知している。

その実装は体制面でも整っている。2012 年設置の ICC が法務・財務・研究管理・技術移転等を束ねて国際活動を支援し、教員の常設委員会 IAC が大学執行部に学術的観点から助言している。さらに、中国（香港含む）・ロシア・サウジなどを対象に、通常審査に上乗せする elevated-risk review を制度化し、国家安全保障・人権・経済安保・価値観・知財/輸出管理/データ・評判まで含めて判断する。

一方で審査の網から漏れがちな「非公式の国際協力」には IIC ツールで事前助言の窓口を設け、加えて、連邦要件に合わせて研究セキュリティ研修を提案申請事務プロセスに組み込み、PI 向け「10 のキーポイント」において研究セキュリティ面で気を付けるべき点等を行動指針として示している。

(2)　テキサス A&M 大学システム（The Texas A&M University System）

テキサス A&M 大学システム（The Texas A&M University System）は、米国でも有数の大規模な高等教育・研究システムであり、研究セキュリティ対応を個別大学の対応ではなくシステム全体の統合的な運用として進めている点で注目される。同システムは 12 大学・8 州機関、学生約 17.5 万人、年間運営予算約 81 億ドル、年間研究費約 16 億ドル規模を有しており[43]、R1 大学に加え、複数の R2 大学[44]や「歴史的黒人大学」（Historically black colleges and universities）を含む多様な構成を持つことが特徴である。

---

[43] The Texas A&M University System. “About” https://www.tamus.edu/system/about/

[44] R1 大学・R2 大学は、米国の Carnegie 分類で使われる研究活動（研究力）の区分名である。Carnegie の 2025 年更新では、R1/R2 は研究費と博士号授与数による基準である。
・R1（Research 1）：年間研究開発費が平均で少なくとも 5,000 万ドル かつ 研究博士号が年 70 件以上
・R2（Research 2）：年間研究開発費が平均で少なくとも 500 万ドル かつ 研究博士号が年 20 件以上

(a) 背景・経緯等

テキサス A&M 大学システムでは、国際連携や研究活動の規模が大きいことを背景に、研究セキュリティ対応を個別案件ごとの対処ではなく、システム全体の運営課題として段階的に制度化してきた。まず、2021 年には既存の国際協定を全件精査し、過去に締結された協定を含めて、研究セキュリティ、法令遵守、相手方リスク等の観点から棚卸し・再点検を進めた。これを踏まえ、2022 年には新規案件だけでなく、国際的関与全般を対象とする事前審査の枠組み（High Risk Global Engagements and High Risk International Collaborations）を制度化し、研究開始前の確認・助言・必要な是正措置を組み込む運用へ移行した[45]。こうした流れは、連邦レベルでの研究セキュリティ要件強化（NSPM-33、CHIPS 科学法等）への対応であると同時に、大学システムとしての説明責任とリスク管理能力を高める取組として位置づけられる。

その後、2023 年には、これらの対応を恒常的な機能として発展させるため、2016 年以降の Academic Security and Counter Exploitation（ASCE）プログラムの実務経験を基盤に、研究セキュリティについての教育・サービス・研究を束ねる中核拠点として Research and Innovation Security and Competitiveness（RISC）Institute 設立の構想が理事会に提示された[46]。研究セキュリティを競争力（competitiveness）や研究推進支援とも関連し検討するための組織である。さらに、NSF の SECURE Center（中核拠点：ワシントン大学）において、テキサス A&M 大学は SECURE Analytics を担う分析ハブとして参画[47]し、地域の大学・研究機関への支援機能も担っている。

(b) 主な取組

テキサス A&M 大学システムにおける研究セキュリティの取組は多岐にわたるが、とりわけ制度設計と実務運用の両面を把握しやすい 4 点、①既存の国際研究協定のリスク評価と見直し、②全ての国際的関与を対象とする事前リスク評価制度（High Risk Global Engagements / High Risk International Collaborations）の導入、③研究・教育・実務支援を束ねる中核拠点としての RISC Institute の発足、④NSF の SECURE Analytics への関与、について説明する。

（いずれも「単年」または「3 年移動平均」の“高い方”で判定）
Carnegie Classification of Institutions of Higher Education. “2025 Research Activity Designations” https://carnegieclassifications.acenet.edu/carnegie-classification/classification-methodology/2025-research-activity-designations/

[45] National Academies of Sciences, Engineering, and Medicine. 2025. National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop. Washington, DC: National Academies Press. https://doi.org/10.17226/27976. Chapter 5: University and National Lab Responses on Research Security. p.32.

[46] “Texas A&M System Regents Approve Research and Innovation Security and Competitiveness Institute” Dec. 14, 2023 https://news.tamus.edu/stories/texas-am-system-regents-approve-research-and-innovation-security-and-competitiveness-institute/

[47] “NSF-backed SECURE Center will support research security, international collaboration” July 24, 2024. https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research

i） 既存の国際研究協定のリスク評価と見直し

テキサス A&M 大学システムでは、2021 年にシステム全体で既存の国際協定の棚卸し・精査を実施した。この見直しは「懸念国（countries of concern）」に関係する協定を対象に、研究協定、学術協力協定、MOU、意向表明書（Letter of Intent: LOI）など約 100 件を対象として行われ、各協定について個別にリスク分析が実施された[48]。結果として、多数の協定は終了され、継続する案件については緩和措置を付した上で管理する方針が採られた。

この取組では、研究費を伴う契約だけでなく、無償の協定や交流枠組みもリスクを持ち得ることを、組織として可視化した点が特徴的である。交換留学等に関わる無償協定が、リスク認識の十分でない担当者により締結されていた事例が相当数あったことが指摘された。

ii） 全ての国際的関与についてリスク評価するシステムの導入（High Risk Global Engagements and High Risk International Collaborations）

上記の 2021 年の協定見直しを踏まえ、テキサス A&M 大学システム規程（System Regulation 15.05.04）[49]では、システム研究セキュリティ室（System Research Security Office: SRO）を中心とし、システム構成大学側の審査・法務確認・研究担当幹部が関わって、国際的関与を審査することとされている。2021 年の棚卸しを通じて把握された課題（協定種別の多様性、無償協定の見落とし、署名権限・審査体制の不統一等）に対応することを意図している。

この仕組みが 2022 年に導入された「High Risk Global Engagements and High Risk International Collaborations」である。提案された国際的関与を大学側で審査し、法的リスク、外国からの影響リスク、機関運営上のリスク、評判リスク等を評価した上で、承認・条件付き承認・不承認を判断しており、週当たり約 20 件を審査している。[50]。

テキサス A&M 大学システム規程（15.05.04）では、各構成大学に対し、ハイリスク国際関与の審査・承認権者、利益相反・責務相反や輸出管理・不当な外国影響への対応、研修、監視・懲戒の手順を定める補足ルールの整備を求めている。審査フローとしては、まず各構成機関の権限者（Empowered Official）が案件を確認し、その後、SRO がリスク審査を行い、Office of General Counsel（OGC）の法令適合性審査を経て、研究担当副学長（Vice Chancellor for Research）が最終承認を行う。また、承認後の案件でも契約・活動内容に変更があれば再審査を要し、対象者には 2 年ごとの輸出管理研修が求められる[51]。

---

[48] National Academies of Sciences, Engineering, and Medicine. 2025. P.32.
[49] The Texas A&M University System, Regulation 15.05.04 High Risk Global Engagements and High Risk International Collaborations (revised 2025/11/4) https://policies.tamus.edu/15-05-04.pdf
[50] National Academies of Sciences, Engineering, and Medicine. 2025. P.32.
[51] The Texas A&M University System, Regulation 15.05.04 High Risk Global Engagements and High Risk International Collaborations (revised 2025/11/4) https://policies.tamus.edu/15-05-04.pdf

iii) RISC Institute（Research and Innovation Security and Competitiveness Institute（研究イノベーションセキュリティ・競争力研究所））の発足

テキサス A&M 大学システムにおける研究セキュリティの取組の中核として位置づけられるのが、RISC Institute の設置である。州・連邦レベルで強化される研究セキュリティ要件への対応を進め、大学・産業界・政府の知見を結集する協働拠点（collaborative hub）として機能させることを意図している[52]。

RISC Institute の役割は、研究セキュリティ分野の教育・人材育成、研究セキュリティ政策・プログラム運用の技術的支援、国内外へのアウトリーチ、重要・新興技術（critical and emerging technologies）の研究開発の安全保障面の分析等である。活動の柱は「Education and Training」「Service」「Outreach」「Research」の 4 領域であり、教育・実務支援・政策連携・知見創出を束ねる研究セキュリティの中核拠点であることを目指している。

RISC Institute は既に 2010 年代から活動を継続している ASCE プログラムを、RISC Institute のサービス機能の中核とする。ASCE は、知的財産・管理対象情報・重要人材・重要技術の保護、ならびに不当な外国影響への対処を目的とし、大学間のベストプラクティス共有や連邦機関との対話の場として運用されてきた[53]。毎年会議を開催しており、米国を中心に、世界各国（25 か国以上）から 600 人以上の政府職員、大学関係者が参加している[54]。

ASCE の発展形として URSPA（University Research Security Professionals Association）が形成されつつあり、RISC Institute がその事務局的な拠点（administrative home）となり、研究セキュリティ専門職の資格認証の推進も担う構想を持っている。これは、NSPM-33 や CHIPS 科学法を受けて大学側に求められる実務が高度化する中、研究セキュリティ人材の専門職化（professionalization）を人材育成面から支える動きである[55]。

RISC Institute は重要・新興技術の保護については、CETPP（Critical and Emerging Technology Protection Program）を通じて、研究組織に対しデュー・ディリジェンス、対諜報（counter-intelligence）・対拡散（counter-proliferation）・サイバーセキュリティの専門的知見を提供し、技術の不正取得リスクを低減する支援を行う。対象はテキサス A&M 大学システム内にとどまらず、他大学・産業界にも広げる構想を持っており、地域・全国レベルでの支援拠点化を志向している[56]。

iv) NSF の SECURE Center／SECURE Analytics への関与

上記の RISC Institute の外部連携プログラムとして SECURE Analytics が掲げられてい

---

[52] The Texas A&M University System, Board of Regents Agenda Item No. 6.18 (Aug. 17, 2023), “Establishment of the Research and Innovation Security and Competitiveness Institute” https://wtaw.com/wp-content/uploads/2023/11/BOR_Nov23_RISCinstitute.pdf
[53] RISC Institute. “Programs and Partners” https://risc.tamus.edu/programs-and-partners/
[54] Academic Security and Counter Exploitation ASCE Program https://risc.tamus.edu/wp-content/uploads/2025/10/ASCE-Promo-One-Pager.pdf　第 10 回 ASCE 会議（2026 年 2 月）は、会場参加約 500 人、オンライン参加約 150 人（29 か国から参加）だった。
[55] The Texas A&M University System, Board of Regents Agenda Item No. 6.18 (Aug. 17, 2023)
[56] Critical and Emerging Technology Protection Program CETPP. https://risc.tamus.edu/wp-content/uploads/2025/10/CETPP-Final-August-2025.pdf

る。SECURE Center はワシントン大学を中心とする全米コンソーシアムであるが、テキサス A&M 大学は米国の南西地域ハブとしても参画している。[57]。

SECURE Center は NSF の公募プログラムで選定されたワシントン大学が主導し、研究セキュリティの情報共有・訓練等を担う全国拠点である[58]。テキサス A&M 大学は SECURE Analytics を主導（NSF 予算 1700 万ドル（5 年間））し、リスクの同定・モデリング・ランドスケープ分析・データ報告で SECURE Center と研究コミュニティを支える。SECURE Analytics のパートナー機関は、フーバー研究所（Hoover Institution）、Parallax 先端研究所である[59]。

(c) 特色・注目点等

以上説明したように、テキサス A&M 大学システムは大規模な研究・教育基盤（複数大学・州機関を含む）を前提に、2021 年に既存の国際協定をシステムワイドで精査し、終了・緩和措置を含む見直しを実施した。さらに 2022 年には、渡航や共著を含む国際的関与を事前審査する仕組みを導入し、RSO、法務部門、研究担当副学長が関与する審査体制を制度化した。さらに、RISC Institute を設置して、教育・訓練、サービス、アウトリーチ、研究を統合的に推進し、ASCE や CETPP 等を通じて人材育成、デュー・ディリジェンス支援、技術保護の機能を発展させている。NSF の SECURE Center（ワシントン大学主導）に対して SECURE Analytics として関与しており、学内対応の充実にとどまらず、他機関支援や全国的な研究セキュリティ基盤整備にも寄与しようとしている点が注目される。

(3) ワシントン大学（University of Washington）

ワシントン大学（University of Washington: UW）は、1861 年創設のシアトル所在の公立研究大学である[60]。ワシントン大学は米国の公立大学の中でも連邦研究資金の受給額が大きく（約 11.9 億ドル（2023 会計年度）[19]）、研究集約型大学としての性格が明確である。2025-26 年度の公式在籍者数は、3 キャンパス合計 63,727 人、留学生は 3 キャンパス合計 7,893 人であり[61]、国際的な研究・教育ネットワークを有する大規模大学である。

同大学は CHIPS 科学法等を踏まえ、学内横断の「Research Security」プログラムを整備しており、輸出管理、国際渡航、情報開示・報告、情報セキュリティ、研修等を統合的に運用することで、研究の開放性と研究セキュリティ確保の両立を図っている。さらに

---

[57] Research and Innovation Security and Competitiveness Institute. https://risc.tamus.edu/
[58] NSF website. “NSF-backed SECURE Center will support research security, international collaboration” July 24, 2024. https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research
[59] Parallax Advanced Research はオハイオ州を拠点とする非営利の民間研究開発機関である。https://parallaxresearch.org/
[60] “The UW in Seattle” https://www.washington.edu/about/seattle-campus/
[61] “Washington residents make up nearly three-fourths of incoming class as enrollment increases across all three UW campuses” Dana Robinson Slote. UW News. October 30, 2025. https://www.washington.edu/news/2025/10/30/washington-residents-make-up-nearly-two-thirds-of-incoming-class-as-enrollment-increases-across-all-three-uw-campuses/

NSF が 2024 年 7 月に発表した研究セキュリティ全国基盤「SECURE Center」の中核機関（lead institution）であり、5 年間・総額 6,700 万ドルの投資のうち 5,000 万ドルがワシントン大学に配分された。同センターは、研究コミュニティ向けの情報集約（clearinghouse）、研修提供、資金配分機関との橋渡し機能を担う構想を有している。

このようにワシントン大学は研究セキュリティの学内の取組と全米向け支援提供の双方を担うことを目指しており、先行事例として位置づけられる。

(a) 背景・経緯等

ワシントン大学における研究セキュリティの取組は、NSPM-33，CHIPS 科学法、OSTP の研究セキュリティ・プログラム指針への対応として、学内の既存機能を統合・再編する形で進展してきた。OSTP の 2024 年ガイドラインは、一定規模以上の連邦研究費を受ける対象機関（covered institutions）に対し、研究セキュリティ・プログラムの整備・認証を求める標準要件を示しているが、ワシントン大学の説明でも統合的な研究セキュリティ・プログラムを備える必要があると説明している[62]。

(b) 主な取組

i) 大学内における研究セキュリティ関連の取組：体制整備等

ワシントン大学は「Research Security at UW」として、研究セキュリティ関連の機能を学内横断で整理した上で運営している。具体的には、輸出管理（Export Control）、国際渡航（International Travel）、開示・報告（Compliance, Disclosures, and Reporting）、情報セキュリティ・プライバシー、研究セキュリティ研修、役割別ガイダンスを単一のプログラム枠組みとして提示している。特に、連邦科学技術資金を年 5,000 万ドル超受ける「covered institution」として、対象者（covered individuals）の海外渡航記録管理や外国渡航セキュリティ訓練が必要であること、また NSF・DOE 等の要件に沿って提案前の研究セキュリティ研修受講確認を行うことが明記されており、CHIPS 科学法、NSPM-33 上の要件を学内実務に反映している。また、ワシントン大学は「Research Security by Design」を掲げ、オープンな研究環境を維持しつつ、研究セキュリティを重視する文化を育てるとしている[63]。

組織体制面では、ワシントン大学は Chief Research Security Officer（CRSO）を「研究セキュリティに関する学内単一窓口（single point of contact）」として位置づけ、相談受付・情報提供・不遵守の通報・進捗確認等の連絡先を明確化している[64]。

---

62 “Research Security at UW” https://www.washington.edu/research/compliance/research-security-at-uw/

63 “Federal Research Security by Design” https://www.washington.edu/research/compliance/foreign-interests-in-sponsored-programs/federal-research-security-by-design/

64 “Research Security at UW” https://www.washington.edu/research/compliance/research-security-at-uw/

ii） 研究セキュリティについての研修教材等の作成

ワシントン大学の「Federal Research Security by Design」ページ[65]では、連邦資金付き研究に関与する研究者（Senior/Key Personnel 等）向けに、短編の解説動画「Disclosures（情報開示）」および「International Collaborations（国際共同研究）」を公開している。これらは必須訓練を代替するものではなく、必須訓練を補完するためのものである。研究室や研究グループの日常運用の中で、要件を事前に確認し、計画段階から組み込む（by design）という考え方も明示されている。

また、各動画には「Action Items Checklist」（行動項目チェックリスト）が付されており、例えば「Disclosures」（開示）では、証憑書類の準備、自身や業績のセルフサーチ、ORCID（永続的識別子）の取得、SciENcv（Science Experts Network Curriculum Vitae）を用いた経歴・実績（Biosketch）・「その他の研究支援」（Other Support）の作成、開示ツールの確認、学内の SFI（Significant Financial Interest（重要な経済的利益））・兼業届等の内部開示の確認といった実務手順が、研究者の行動単位で示されている。「International Collaboration（国際研究協力）」でも、懸念国関与時の追加対応、SAM.gov[66]での資格確認、ITA スクリーニングリスト確認、輸出管理部門との相談、スポンサー固有要件の確認、NIH（国立衛生研究所）の国際サブレシピエント対応（データアクセス確保・レター文言）などが整理されており、抽象的な注意喚起ではなく、提案準備・共同研究実施時のチェックポイントとして機能する構成となっている[67]。

iii） SECURE センターの運営

ワシントン大学における研究セキュリティの取組として、特に注目されるのが、SECURE Center の運営である[68]。SECURE Center は、CHIPS 科学法の要請を受けて整備された全国的な実装基盤であり、NSF は 2024 年 7 月、5 年間・総額 6,700 万ドル（うちワシントン大学に 5,000 万ドル、テキサス A&M 大学に 1,700 万ドル）を投じて、研究コミュニティ全体の研究セキュリティ対応力を高めるために立ち上げた。NSF は同センターを、研究セキュリティ上のリスク情報の「研究セキュリティ情報の共有拠点（clearinghouse）」、訓練提供の拠点、そして大学等の研究現場と連邦資金配分機関をつなぐ橋渡し機能として位置づけている[69]。

ワシントン大学の CoSSaR（Center for Collaborative Systems for Safety, Security and Regional Resilience）が中核を担っている。CoSSaR はワシントン大学の Human Centered Design and Engineering 部門に属し、もともと安全保障・レジリエンス分野で協働システムの設計・運用を専門としてきた組織である。SECURE Center の設計思想に

---

65 Ibid.
66 連邦政府の契約・補助金など連邦資金の手続をまとめたポータルサイト。
67 “Checklist: Federal Research Security by Design” https://www.washington.edu/research/policies/checklist-federal-research-security-by-design/
68 “UW awarded $50M to lead U.S. research security center” Leah Pistorius. July 24, 2024. https://www.hcde.washington.edu/news/article/2024-07-24/nsf-secure
69 “NSF-backed SECURE Center will support research security, international collaboration” July 24, 2024” https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research

もこの強みが反映されており、単なる規制遵守のための情報提供ではなく、研究現場の実務担当者（研究セキュリティ担当、コンプライアンス担当等）が学び、相互に調整しながら運用を改善する「共創型」の仕組みとして構築されている。

この「共創型」運営の中核が、SECURE Center の「共有バーチャル環境」（Shared Virtual Environment: SVE）である。SECURE Center は SVE を、研究セキュリティ専門職がオンラインでつながり、協働し、ツールを利用しながら実装知見を蓄積する場として設計している。SECURE Center の公開情報によれば、SVE は 2026 年にローンチされ、研究セキュリティの実務者向けに提供が開始されている[70]。。

また、SECURE Center は SVE だけでなく、実務ツール群の整備も進めている。公開されている Products には、海外渡航向けチェックリスト（通常版・高リスク版）、研究セキュリティ担当者向けのリスク評価フレームワーク、NIH・NSF・DOE・DoD の要件差異を整理した Federal Risk Matrix Reference Guide、参照資料ライブラリ（Reference Library）等が含まれている[71]。

さらに、最近の動向として、SECURE Center は研修教材の作成に力を入れている。Training ページでは、統合トレーニング・モジュール（Consolidated Training Module）が 2025 年 9 月にベータ版として開始されたこと、また同モジュールが連邦研究セキュリティ訓練要件への対応を支援する目的で設計されていることが示されている[72]。Briefings ページでは、研究セキュリティをめぐる最新の出来事、報告書、インシデント、政策更新等を毎週配信する運用が明示されている[73]。

(c)　特色・注目点等

以上説明したように、ワシントン大学の特色は、研究セキュリティを「個別の規制対応」ではなく、研究実施プロセス全体に織り込む“Research Security by Design”として制度化している点にある。学内では Chief Research Security Officer（CRSO）を単一窓口として配置し、相談・通報・運用支援の接点を一元化しているほか、輸出管理・開示・国際連携・訓練を横断的に扱う運用が整理されている。

もう一つの大きな特色は、ワシントン大学が学内対応にとどまらず、NSF の全国拠点 SECURE Center の中核として、大学コミュニティ全体の研究セキュリティ基盤づくりを担っている点である。SECURE Center は、研究セキュリティ情報の共有拠点（clearinghouse）となり、訓練提供、大学と政府資金配分機関の橋渡しを担う設計で、地域拠点の一つ（SECURE West）もワシントン大学が担っている。

---

[70] NSF Secure Center. “Our Timeline” https://www.secure-center.org/milestones
[71] NSF Secure Center “Products” https://www.secure-center.org/products
[72] “CTM 1.2 NSF SECURE Center Consolidated Training Module” https://www.secure-center.org/products
[73] “NSF SECURE Center Briefing” https://www.secure-center.org/briefings

2.1.3　資金配分機関等における取組

米国の連邦研究資金配分機関（NSF、NIH、DOE、DoD 等）に対する研究セキュリティ上の要求は、既に説明したように、近年、①NSPM-33、②CHIPS 科学法、③OSTP「Guidelines for Research Security Programs at Covered Institutions」（2024 年）等により段階的に具体化・標準化されてきた。

NSPM-33 に基づく資金配分機関への要求

NSPM-33 は、資金配分機関に対し、研究セキュリティ確保のための基本的な管理責務を広く課している。具体的には、研究者・審査関係者等に対する利益相反・責務相反等の開示要件の整備・運用（初回、年次更新等）、デジタル永続 ID（digital persistent identifier）要件の方針整備、開示様式・定義の標準化、監察官・法執行機関等との連携強化、違反時の対処（助成停止、資格停止等を含む）、研究セキュリティ研修（配分実務に関与する連邦職員向け）の実施、および一定規模以上の研究機関に対する研究セキュリティ・プログラム認証の要求が含まれる。あわせて、重要・新興技術分野について追加要件の要否を検討することも求めている。

NSPM-33 は実装に当たり、過度な事務負担の回避、訂正・救済の機会確保、標準化における明確な説明といった運用上の配慮も明記しており、研究の開放性を維持しながらリスク管理を強化する設計となっている。

CHIPS 科学法に基づく資金配分機関への要求

CHIPS 科学法（Subtitle D）は、NSPM-33 の方向性を法的義務として補強・具体化した（表 2-2 参照）。資金配分機関に対しては、特に以下の点が重要である。第一に、海外人材採用プログラムに関する統一ガイドラインを踏まえた機関ポリシーの策定が求められる。第二に、悪性人材採用プログラム（MFTRP）不参加の認証を助成申請・継続管理に組み込む（研究者側の認証に加え、申請機関側の認証も含む）。第三に、受給機関に対し、対象者（covered individuals）向けのリスク研修の提供を助成要件として課すことである。

さらに CHIPS 科学法は、資金配分機関に対し、必要に応じて申請機関へ外国人の雇用・任用、海外人材採用プログラム参加等に関する契約文書の提出要求や、申請機関側による契約・合意文書の適合性レビューを求め得る権限を明示している。また、研究セキュリティ研修の修了認証（研究者・機関双方）を申請要件にすることも法定化している。Subtitle D の実施に当たっては、人種・民族・国籍等に基づく標的化・差別の防止を求めている。

OSTP「研究セキュリティプログラムガイドライン」（2024 年）に基づく資金配分機関への要求

OSTP の 2024 年研究セキュリティプログラムガイドライン（Guidelines for Research Security Programs at Covered Institutions）[74]は、NSPM-33 Section 4(g) と CHIPS 科学法の要請を受け、資金配分機関が研究機関に求める研究セキュリティプログラム（RSP）要件を機関横断で標準化した文書である。資金配分機関は、一定要件を満たす「対象機関（covered institution）」（高等教育機関、FFRDC、非営利研究機関で、連邦研究開発資金が年 5,000 万ドル超）に対し、RSP の認証を求めなければならない。

RSP の標準 4 要素は、(1)サイバーセキュリティ、(2)海外渡航セキュリティ、(3)研究セキュリティ研修、(4)輸出管理研修である。特に 2024 年 OSTP ガイドラインは、資金配分機関に対し、研究セキュリティ研修および輸出管理研修について、政府提供教材（例：NSF 共通モジュール）と、要件を満たす機関独自研修の双方を許容することを求めており、標準化と大学・研究機関の裁量を両立させようとしている。

また、資金配分機関には、RSP 要件の実装において非差別（non-discrimination）の確保と、研究者・学生・研究支援職員の権利保護を大学側に認証させることが求めている。

以上を踏まえると、米国の連邦研究セキュリティ政策は、資金配分機関に対して、開示・認証・研修・情報共有等を含む実装責務を大学・研究機関に対して体系的に課し、同時に差別にならないように配慮することを求めていると解釈できる。

(1) 米国科学財団（National Science Foundation）

米国科学財団（National Science Foundation: NSF）は、1950 年に連邦議会により設立された独立連邦機関であり、全米 50 州および米領域における科学技術研究を支援する研究資金配分機関である。NSF はその任務を主として競争的資金（grant）によって遂行しており、米国の大学等における基礎研究に対する連邦支援の相当部分を担う中核的な資金配分機関である。[75]

NSF の FY2024（2024 年度）歳出法上の予算は 90.6 億ドルである[76]。幅広い分野を対象にしながら（医科学を除く）、外部専門家レビューを用いた競争的審査を基本とし、資金配分を行う。NSF は年間平均で約 11,000 件の競争的助成を行い、約 1,900 機関、約 35 万人（研究者・起業家・学生・教員等）の研究活動を支援していると説明しており [75]、大学・研究機関に対する裾野の広い配分構造を有している。

[74] Office of Science and Technology Policy. Guidelines for Research Security Programs at Covered Institutions. July 9, 2024. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/OSTP-RSP-Guidelines-Memo.pdf
[75] NSF. “About NSF” https://www.nsf.gov/about
[76] NSF. “Fiscal Year 2024 Appropriations” https://www.nsf.gov/about/budget/fy2024/appropriations

(a) 背景・経緯等

NSF における研究セキュリティ対応の強化は、2010 年代後半以降、米国の大学研究において、外国機関との関係、海外人材採用プログラム参加、他機関からの支援等に関する未開示・不十分開示が連邦政府全体の政策課題として顕在化したことを背景として進展した。NSF の対応は、研究の開放性を維持しつつ、透明性確保・説明責任・リスク管理を強化する方向で制度化されてきた。

この流れの基盤となったのが、2019 年の JASON 報告書（Fundamental Research Security）である[77]。同報告書は、基礎研究のオープン性の維持を前提としながら、研究セキュリティ上の懸念への対応として、開示の実効性向上、連邦機関間の整合的運用、過度な事務負担の回避、違反時の対処を重視する考え方を示した。NSF のその後の制度整備は、開放性を損なわないリスク管理という方向性に沿って進められた。

NSF は 2020 年、長官室（Office of the Director）直下の体制として、研究セキュリティを統括する Chief of Research Security の職を設け[78]、あわせて研究セキュリティ戦略政策室（Office of the Chief of Research Security Strategy and Policy: OCRSSP）を設置した。これにより、研究セキュリティ対応は、戦略・政策、分析、研修、対外連携を担う本部機能として位置づけられるようになった。[79]

その後、2021 年の NSPM-33 および 2022 年の CHIPS 科学法（Subtitle D）により、連邦研究資金配分機関に対する研究セキュリティ上の要件は一段と具体化された。NSF はこれらの要件に対応し、研究者向けガイダンス、受給機関向け実務案内、研修資源、審査・分析支援機能の整備を進めてきた。

さらに、2024 年 7 月の OSTP ガイドラインにより、資金配分機関が研究機関に求める RSP 要件の標準化が示され、NSF を含む各機関の実装フェーズが本格化した。NSF においては、2024～2025 年にかけて、Important Notice No.149[80]による実務要件の更新に加え、研究機関側の実装支援・審査支援を補強する仕組み（TRUST、SECURE Center 等（後述））の導入・運用が進展している。

---

[77] JASON, Fundamental Research Security (JSR-19-2, 2019).
https://nsf-gov-resources.nsf.gov/files/JSR-19-2IFundamentalResearchSecurity-12062019FINAL.pdf
[78] NSF. NSF creates new research security chief position. March 2, 2020.
https://www.nsf.gov/news/nsf-creates-new-research-security-chief-position
[79] NSF. Research Security at the National Science Foundation: Office of the Chief of Research Security Strategy and Policy. https://www.nsf.gov/research-security
[80] U.S. National Science Foundation, Important Notice No. 149
https://www.nsf.gov/notices/important/important-notice-no-149-updates-nsf-research-security/in149

(b) 最近の主な取組

i) CHIPS 科学法、NSPM-33 への対応

NSF は、CHIPS 科学法および NSPM-33 に沿って、研究セキュリティ上の透明性向上・説明責任を強化するための実務要件を段階的に整備しており、以下を含め、取組の現状を周知するための文書が Important Notice No.149（2025 月 11 月 24 日改正）である[81]。

研究セキュリティ・アセスメントと証拠書類の保持（2025 年 12 月施行）

NSF は提案・アワードに対し分析ツールを用いたリスク評価（未開示情報の有無等の確認）を行う権限を明示し、提案者・受給機関に対して、シニア／キー人員の外国での任用、外国機関との雇用、海外人材採用プログラム参加、現在および保留中の（その他の）支援（Current and Pending (Other) Support）などに関する裏付け文書の保持を求めている。

研究セキュリティ研修義務化（2025 年 12 月施行）

次に、研究セキュリティ研修について、NSF は CHIPS 科学法に対応し、提案時点でシニア／キー人員が過去 12 か月以内に所定の研究セキュリティ研修を修了していること、及び組織の権限ある代表者（Authorized Organizational Representative: AOR）がその修了を認証することを求めている。研修内容は、サイバーセキュリティ、国際共同研究、外国干渉、資金の適正使用、開示、利益相反・責務相反等を含む。さらに、NSF・NIH・DOE・DOD 等が共同利用可能な研修モジュール（SECURE Center の凝縮版を含む）を認めつつ、2024 年 OSTP ガイドラインが求めるとおり、各機関独自の研修教材の利用も認める。

悪性海外人材採用プログラム参加禁止

悪性海外人材採用プログラム（MFTRP）への対応として、NSF は CHIPS 科学法に基づき、MFTRP の当事者をシニア／キー人員として提案・受給させない方針を実施している（2024 年 5 月 20 日以降の NSF アワードに適用）。提案時には AOR および各シニア／キー人員による不参加認証、採択後には PI/Co-PI の年次自己認証（Research.gov 経由）を求めており、NSF は今後この年次認証の対象を全シニア／キー人員へ拡大する意向も示している。

外国資金開示報告

外国資金開示報告（FFDR: Foreign Financial Disclosure Reporting）について、CHIPS 科学法に基づき、NSF 資金の直接受給機関である高等教育機関に対し、懸念国に関連する外国資金（贈与・契約等、年間累計 5 万ドル以上）を年次報告させる制度を運用している。Important Notice No.149 では、対象範囲（関連財団・関連団体、仲介者経由を含む）、報告期間（初回は 2024 年 7 月～2025 年 6 月）等について記載されている。

---

[81] NSF. Important Notice No. 149: Updates to NSF Research Security Policies. July 10, 2025 https://www.nsf.gov/notices/important/important-notice-no-149-updates-nsf-research-security/in149

孔子学院（Confucius Institute）条項（2025 年 12 月施行）

CHIPS 科学法に基づき、孔子学院（Confucius Institute）と契約・協定を維持する高等教育機関には原則として NSF 資金を交付しないことが明確化された（2025 年 12 月施行）。ただし、学問の自由の保護、外国法の不適用、大学側の完全な管理権等の条件を満たす場合には、NSF 長官による免除（waiver）の余地がある。

ii） SECURE センターの設立

経緯・背景

NSF は、CHIPS 科学法に基づく研究セキュリティ・インテグリティ情報共有機能の整備要請を受け、2024 年 7 月、研究コミュニティ向けの新たな支援基盤として SECURE Center（Safeguarding the Entire Community of the U.S. Research Ecosystem）の立上げを公表した[82]。外国からの不当な干渉等に対する研究コミュニティの対応力強化を目的とするものである[83]。SECURE Center は、非政府・独立の組織体として位置づけられ、ワシントン大学主導で運営されており、資金期間は 2024 年 9 月 1 日から 2029 年 8 月 31 日までである。（ワシントン大学とテキサス A&M 大学の取組について、それぞれ 27 頁と 24 頁を参照）

主な取組

運営方式の特徴として、SECURE Center は全国分散型（mostly virtual）の体制を採用しており、National Center、Regional Centers、Expert Areas、Value Areas から成る構造で運営される。SECURE Center 自身は、この体制を通じて、各地域・各機関の事情（地理的、組織的、社会経済的な差異）を踏まえつつ、共通に使える実務改善策を「共創（co-creation）」していく方針を示している。特に Regional Centers は「co-design hub」として、地域の研究機関とともに課題設定・試作・改善を行う役割を担う。[84]

また、SECURE Center の提供基盤として「共有バーチャル環境」（Shared Virtual Environment: SVE）が整備されており、大学、非営利研究機関、中小企業等の関係者が、研究セキュリティ上の課題に関する情報共有、議論、ツール利用を行うための共通のデジタル環境として位置づけられている。[85]

iii） TRUST（Trusted Research Using Safeguards and Transparency）

NSF は 2024 年 6 月、研究提案に対する新たなリスク緩和プロセスとして、TRUST を公表した[86]。これは、NSF のミッションである学術研究支援を前提にしつつ、助成提案に

[82] “NSF-backed SECURE Center will support research security, international collaboration” July 24, 2024. https://www.nsf.gov/news/nsf-backed-secure-center-will-support-research
[83] SECURE Center. “Mission Statement” https://www.secure-center.org/mission
Award Abstract # 2403771. Center: SECURE - Collaborative Research Security & Integrity National Environment. https://www.nsf.gov/awardsearch/showAward?AWD_ID=2403771
[84] SECURE Center. “Overview of Our Approach” https://www.secure-center.org/approach
[85] SECURE Center. “Shared Virtual Environment” https://www.secure-center.org/secure-sve
[86] NSF enhances research security with new TRUST proposal assessment process

含まれ得る国家安全保障上のリスクを評価する枠組みであり、研究の国際協力を不必要に萎縮させないこと、公正性・適正手続（fairness and due process）を確保することを明示している。TRUST の制度設計は、CHIPS 科学法（Section 10339）および FY2023 歳出報告（FY23 Appropriations Report）の要請、ならびに JASON 報告書（2019）の問題提起を踏まえて進められた[87]。

TRUST の評価枠組みは、①現時点の兼職・任用・研究支援の把握、②開示義務違反の特定、③当該研究の予見可能な国家安全保障上の考慮事項の 3 点から構成される。NSF の説明資料では、①に関して BIS Entity List、EO 14032 関係リスト、NDAA（国防授権法）の 1260H リスト・1286 リスト等を参照し得ること等の運用が示されている。さらに、TRUST プロセスでは OCRSSP（Office of the Chief of Research Security Strategy and Policy）のデータ分析担当が主として①・②を評価し、必要時には大学・研究機関側とともにリスク緩和策を作成・実装する。③については、第 10 回 ASCE 会議（2026 年 2 月）での NSF 関係者の説明によれば、評価はとても労力を要するものであり、今後は現在の decision tree model から、DoD のような risk matrix model（40 頁参照）による評価に移行するとのことである（risk matrix 公開で透明性が高まるとのメリットもあるとのこと）。

適用は段階的に進められており、FY2025 に量子関連提案（Quantum Information Science: QIS）を対象とするパイロットから開始された。NSF は当初から、同パイロットで得られた知見を踏まえて、CHIPS 科学法上の主要技術分野へ拡大し、その後さらに対象を広げる 3 段階展開を示している。公開資料上、量子分野以降の全面展開の確定時期までは明示的ではないが、NSF の FY2025 Agency Financial Report では、量子パイロットの実装状況を評価し、他の主要技術分野への拡大可能性を検討している旨が示されており[88]、TRUST は試行から横展開判断の段階に移行しつつあると考えられる。

iv） 研究セキュリティについての調査研究の実施

NSF は、研究セキュリティそのものを学術的・実証的に分析するための研究基盤づくりを進めている。2022 年度の JASON グループによる検討を踏まえ、2023 年度に「Research on Research Security（RoRS）」の研究資金プログラムを設置する方針が示され、RoRS の設計に向けた取組として、NSF による関連ワークショップへの資金措置がなされた。[79]

その後、NSF は 2025 年に RoRS の公募を開始（PD 25-275Y（Research on Research Security Program）し、研究セキュリティ分野の「範囲・可能性・課題・性質」を学術的

June 5, 2024 https://www.nsf.gov/news/nsf-enhances-research-security-new-trust-proposal

[87] New NSF Proposal Review Process: Trusted Research Using Safeguards and Transparency (TRUST). Presentation for the Federal Demonstration Partnership - May Meeting. Sarah Stalker-Lehoux Deputy Chief of Research Security Strategy and Policy. National Science Foundation May 22, 2024. https://thefdp.org/wp-content/uploads/NSF-TRUST-Process-for-FDP-05.23.2024.pdf

[88] NSF FY2025 Agency Financial Report. Other Information 2A: Memorandum on FY 2026 Management Challenges Challenge 3: Mitigating Threats to Research Security. https://nsf-gov-resources.nsf.gov/files/FY-2025-Agency-Financial-Report_0.pdf

エビデンスによって明らかにする提案を募集した。RoRS プログラムの目的は、研究セキュリティ上のリスク・実務・政策に関する理解を深め、米国の研究基盤を保全するとともに、研究セキュリティを一つの学術分野として育成することと説明している。[89]

RoRS は、分野横断的（interdisciplinary）かつエビデンスベースの研究を重視しており、STEM 研究者、研究セキュリティ研究者、実務担当者の協働を促す設計となっている。採択対象となる提案類型として、①会議・ワークショップ開催、②プランニング助成金、③探索的研究への初期概念の助成金（Early-concept Grants for Exploratory Research: EAGER）を示し、脅威の実態把握、リスク同定・緩和手法、政策の含意、組織文化・制度変容、分野別・国際的文脈における研究セキュリティなど幅広い研究テーマを想定している。

NSF は RoRS の初回アワードを公表[90]しており、10 州の 12 受給者に対して、EAGER、Planning proposals、Workshops and conferences の 3 類型にわたる採択が行われた（表 2-3）。

表 2-3　Research on Research Security（RoRS）公募採択プロジェクト

研究タイトル（日本語 / 英語）	PI 所属機関	研究内容	金額(ドル)
NSPM-33 支援のための機関サイバーセキュリティ準備計画 Planning: RoRS: Planning Institutional Research Cybersecurity Readiness: Mapping Gaps and Maturity in Support of NSPM-33	アリゾナ州立大学	NSPM-33（国家安全保障指針）への対応状況をマッピングし、各大学のセキュリティ成熟度を評価する手法の開発。	$199,999
高等教育における RoRS ニーズ特定ワークショップ Conference: Workshop to Identify Research on Research Security (RORS) Needs in Higher Education	ミシガン工科大学	大学現場における研究セキュリティ上の喫緊の課題と研究ニーズを特定するための全米規模の会議開催。	$99,745
HPC 悪用の解明：メタデータからの AI グラフ推論 EAGER: Unmasking HPC Abuse: AI Graph Inference from Scheduling Metadata	イリノイ大学	スケジューリングデータから AI を用いて、高性能計算機（HPC）の不適切な利用や不正アクセスを検知する研究。	$274,654
量子情報科学（QIS）の研究コミュニティ特定と流出リスク EAGER: Time Aware Research Community Identification of Critical & Emerging Technologies: Global Multi-sector QIS	ミシガン大学	量子技術分野のグローバルな研究ネットワークを可視化し、技術流出の潜在的な経路を時間軸に沿って分析。	$299,840

[89] NSF. “The Research on Research Security Program (RoRS)” https://www.nsf.gov/funding/opportunities/rors-research-research-security-program
[90] NSF SECURE Center Research Security Briefing Vol. 1 No.11: September 11, 2025. https://76c77598-c030-4f60-96f6-d1d7f613ea5b.usrfiles.com/ugd/76c775_9010cc0fd5df46bfa7f7bdfabe080852.pdf

研究タイトル（日本語 / 英語）	PI 所属機関	研究内容	金額(ドル)
神経技術システムと新興ツールの国家安全保障評価 EAGER: SENSE: National Security Evaluation of Neurotechnology Systems and Emerging tools	セントラルフロリダ大学	神経技術（ブレイン・マシン・インタフェース等）分野における特有のセキュリティ脅威と安全保障上のリスク評価。	$299,414
情報スパイにおける漏洩パターン解明のグラフ分析 EAGER: A Graph Analytics Approach to Understanding Leakage Patterns in Information Espionage	カリフォルニア大学サンディエゴ校	グラフ分析技術を用い、研究情報の漏洩がどのような構造・パターンで行われるかを解明する。	$300,000
AI 研究の保護：ライフサイクルに基づく脅威の類型化 EAGER: Securing AI Research: Developing and Validating a Lifecycle-Based Typology of Threats	バージニア工科大学	AI 研究の着想から公開までの各工程（ライフサイクル）に潜む脅威を分類し、その対策を検証する。	$300,000
リソースが制約されたキャンパスのセキュリティ計画 Planning: Security Planning for Assessment-driven Resource-constrained Campuses	STEM RESOURCES LLC	予算や人員が限られた中小規模の大学等でも実施可能な、効率的な研究セキュリティ対策モデルの策定。	$197,286
安全な共同研究のためのゲーミフィケーション行動実験 EAGER: Gamified Behavioral Experiments for Responsible and Secure Collaboration	クレムソン大学	ゲーム形式の実験を通じ、研究者がどのようなインセンティブがあれば安全な情報共有を行うかを行動科学的に分析。	$300,000
研究ソフトウェア・サプライチェーン保護（共同研究） Collaborative Research: Planning: CROSS: Building a Community aROund Securing the Research Software Supply Chain	アラバマ大学	研究用ソフトウェアのオープンソース環境における脆弱性や改ざんリスクを防ぐためのコミュニティ構築。	$44,891
研究ソフトウェア・サプライチェーン保護（共同研究） Collaborative Research: Planning: CROSS	パデュー大学	（同上のプロジェクトの分担。）	$105,113
研究ソフトウェア・サプライチェーン保護（共同研究） Collaborative Research: Planning: CROSS	ロヨラ大学シカゴ	（同上のプロジェクトの分担。）	$49,996

出典：NSF. Search Results. https://www.nsf.gov/awardsearch/search-results?BooleanElement=Any&BooleanRef=Any&ProgEleCode=275Y00

(c) 特色・注目点等

NSF の研究セキュリティ対応の特色は、規則遵守、研究の開放性・国際協力の維持、研究現場の実装支援、個別案件のリスク審査、政策効果の検証までの多面的な取組を総合的に設計している点にある。CHIPS 科学法・NSPM-33 への対応を通じて制度要件を明確化するだけでなく、SECURE Center によって研究機関側の実務対応力の底上げや研修教材の作成に取り組み、TRUST による審査段階のリスク把握の高度化を図る。さらに RoRS を通じて研究セキュリティ政策そのものを実証的に検証する知識基盤の育成に努めている。

(2) 国防省（Department of Defense）（附置機関を含む）

米国国防省（DoD）は、大学・研究機関等への単一の研究資金配分機関というよりも、国防省全体の研究開発ミッションの下で、複数の国防省の構成機関（DoD Components）[91]が分担して資金配分を行っている。国防長官部局の基礎研究室（DoD Basic Research Office: BRO）が国防省全体の研究助成政策の総合調整を所管し、各種基礎研究プログラムを管理する[92]。一方、実際の大学・研究機関等向けの公募・審査は、例えば ONR（海軍研究局）、ARO（陸軍研究局）、AFOSR（空軍科学研究局）等の研究オフィスを通じて実施されている[93]。

DoD は、DoD 資金で行われる、大学等での fundamental research（基礎・応用研究のうち、通常は広く公表・共有される研究）の開放性を維持する考え方を明確にしつつ、研究セキュリティ上のリスクには別途、リスクベースで対応するという立て付けを採っている。DoD の学術研究セキュリティ（Academic Research Security）の検討でも、対象は主として大学における fundamental research であり、CUI（管理対象非機密情報）や機微・秘密指定研究に対する追加的な保護措置とは区別されている[94]。また、DoD の Fundamental Research Guidance（2025 年）[95]では、NSDD-189（National Security Decision Directive-189、国家安全保障決定指令 189 号）[96]等に基づき、fundamental research は原則として公表・共有することを前提とし、輸出管理上の制約を伴う事前の出版審査等を安易に課すべきでないことが改めて強調されている。

その上で DoD は、NSPM-33 および NDAA 第 1286 条等を踏まえ、2023 年に fundamental research 提案に対するリスクベースのセキュリティ審査の方針を整備[97]し、採択候補となった提案について、開示情報（利益相反（COI）・責務相反（COC）に関わる情報を含む）や公開情報等を用いた審査、必要に応じたリスク低減措置、DoD 構成機関の間での運用整合、スポットチェック等を求める枠組みを導入している。さらに DoD は、問題のある外国機関リストや国家安全保障上脅威となる海外人材採用プログラムのリ

---

91 Army Research Office（ARO）、Air Force Office of Scientific Research（AFOSR）、Office of Naval Research（ONR）、Defense Advanced Research Projects Agency（DARPA）、Defense Threat Reduction Agency（DTRA）などの fundamental science への助成金配分機関を含む。

92 Basic Research | Research Directorate. Office of the Under Secretary of Defense for Research & Engineering. https://basicresearch.defense.gov/

93 Office of Naval Research. “Fiscal Year (FY) 2026 Department of Defense (DoD) Defense University Research Instrumentation Program (DURIP) N0001425SF001” https://www.onr.navy.mil/work-with-us/funding-opportunities/fiscal-year-fy-2026-department-defense-dod-defense-university

94 “Academic Research Security” https://basicresearch.defense.gov/Programs/Academic-Research-Security/

95 Department of Defense. Fundamental Research Guidance. August 4, 2025. https://basicresearch.defense.gov/Portals/61/Documents/Research%20Security/Fundamental%20Research%20Guidance.pdf

96 NSDD-189（国家安全保障決定指令 189 号）は、1985 年にレーガン大統領によって署名された、米国の基本方針を定めた指令であり、基礎研究（Fundamental Research）の成果は、最大限、制限なく公開・配布されるべきであると規定している。

97 Department of Defense. Policy for Risk-based Security Reviews of Fundamental Research. June 8, 2023. https://media.defense.gov/2023/Jun/29/2003251160/-1/-1/1/COUNTERING-UNWANTED-INFLUENCE-IN-DEPARTMENT-FUNDED-RESEARCH-AT-INSTITUTIONS-OF-HIGHER-EDUCATION.PDF

ストを更新・公表[98]し、大学・研究者に対して注意喚起を行っている。こうした点から、DoD の研究セキュリティ政策は、「fundamental research の開放性の維持」と「資金配分段階でのリスク審査・低減」の両立を中核に設計されていると考えられる。

(a) 背景・経緯等

DoD の研究セキュリティに関する取組を理解する上では、まず、1980 年代に形成された米国政府の fundamental research（基礎研究）に関する基本方針を踏まえる必要がある。レーガン政権下で発出された NSDD-189（National Security Decision Directive 189, 1985）[99]は、大学等で行われる基礎研究の成果について、原則として最大限公開・共有されるべきであり、国家安全保障上の理由から制限が必要な場合には、原則として分類（classification）によって対応すべきである、という考え方を示した。

その後、冷戦後の 1990 年代から 2000 年代以降にかけて、技術流出、輸出管理、外国からの不当な影響等への懸念は強まったが、連邦政府は一方で、NSDD-189 の基本原則を繰り返し再確認してきた[100]。研究セキュリティ上の懸念が高まる局面においても、米国政府は「基礎研究の公開性」を直ちに否定するのではなく、開放性の維持とリスク管理の両立という整理を維持してきた点に特徴がある。こうした政策的蓄積は、近年の研究セキュリティ政策（研究者の開示義務強化、利益相反・責務相反管理、海外人材採用プログラム対応等）の制度化においても、重要な前提となっている。

DoD においては、こうした歴史的な方針の上に、2010 年代後半以降の安全保障環境の変化（戦略的競争の深まり、技術・知的資産流出への警戒）を受け、研究セキュリティ対応を具体化している。特に、NDAA 第 1286 条[101]は、DoD 資金による大学等の研究に関し、不当な外国影響への対応強化を求める法的根拠となり、さらに NSPM-33 は、連邦政府全体としての研究セキュリティの標準化を進める契機となった。

DoD は、2023 年に「fundamental research 提案に対するリスクベース安全審査方針」（Policy for Risk-Based Security Reviews of Fundamental Research）を公表[97]し、NDAA 第 1286 条及び NSPM-33 を踏まえた全省横断の審査運用を明確化した。DoD 内の各資金配分主体においても、この共通方針への統合が進められている。例えば Defense Advanced Research Projects Agency（DARPA）では、従来の対外国影響対策（CFIP）に関する運用を、DoD 共通のリスクベース審査プロセスへ統合・置換する運用に移行[102]し

---

98 Introduction to Fiscal Year 24 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232), as amended. June 24, 2025. https://basicresearch.defense.gov/Portals/61/Documents/Academic%20Research%20Security%20Page/FY24%20Section%201286%20List%20for%20public%20release_V2.pdf

99 NSDD-189 (National Security Decision Directive 189, 1985) https://irp.fas.org/offdocs/nsdd/nsdd-189.htm

100 Federation of American Scientists. “DoD Affirms Policy on Open Research”. Steven Aftergood. 2006.03.10. https://fas.org/publication/dod_research/

101 John S. McCain National Defense Authorization Act for Fiscal Year 2019. 443-444 頁. https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf

102 Defense Advanced Research Projects Agency (DARPA) Fundamental Research Risk-Based Security Review Program (FRRBS) Frequently Asked Questions (FAQs). Pp.10-11. https://www.darpa.mil/sites/default/files/attachment/2025-01/darpa-fundamental-research-risk-based-

ている。DoD 全体としての審査の一貫性・透明性を高める流れの一環として位置づけられる。

⑹ 主な取組

i) リスクベース・セキュリティ審査プロセス

上記のように、DoD の研究セキュリティ上の中核的な取組の一つは、fundamental research（基礎研究）を対象とした「リスクベース・セキュリティ審査プロセス」の整備である。この枠組みの制度的な骨格は、2023 年 6 月 8 日付の DoD メモ「Policy for Risk-Based Security Reviews of Fundamental Research」[97] で示された。同文書は、NDAA 第 1286 条および NSPM-33 に基づく方針であることを明記し、DoD 全体での一貫的な（consistent）審査運用を目的として、OUSD(R&E)（研究・技術担当国防次官室）が DoD の各構成機関の審査プロセスを監督する構造を定めている。また、審査は、技術的評価により採択候補となった fundamental research 提案を対象に実施し、研究機関・研究者の開示情報等から研究セキュリティ上のリスク（特に利益相反・責務相反に関わる事項）を把握し、必要なリスク低減措置につなげる設計となっている。

運用面では、後述のように、DoD は各構成機関のプログラム担当者向けに Decision Matrix（判断マトリックス）を公表し、審査判断の標準化と透明性向上を図っている。さらに、2026 年 1 月 7 日付の「Fundamental Research Security Initiatives and Implementation」メモ[103]は、既存の 2023 年リスクベース審査方針を強化する追加措置を示している。同メモは、DoD 資金による研究（特に fundamental research）を、悪意ある外国の影響、知的財産窃取、研究成果の搾取から守る必要性を前面に掲げた上で、①NDAA Section 1260H（中国軍事企業関連）リスト掲載企業等への基礎研究支援アワード（fundamental research assistance award）資金供与の禁止、②部内横断の基礎研究リスク審査リポジトリ（Fundamental Research Risk Review Repository）の新設、③年次スポットチェックの強化、④研究セキュリティ人材の訓練強化、⑤自動化された審査・継続監視能力の検討等を指示している。特にリポジトリ新設は、国防省の構成機関間の情報収集・共有を制度化し、審査の再現性・追跡性を高める措置として重要である。

また、前述のように、2025 年 8 月 4 日公表の「Department of Defense Fundamental Research Guidance」[104]は、こうした研究セキュリティ審査の強化が、fundamental research 本来の性格（公開・共有を前提とする研究）を不必要に損なわないようにする観点を明確化している。

---

review-faqs.pdf

[103] Department of War. The War Department Strengthens Measures to Protect DOW-Funded Research. Jan. 8, 2026
https://www.war.gov/News/Releases/Release/Article/4373247/the-war-department-strengthens-measures-to-protect-dowfunded-research/

[104] Department of Defense. Fundamental Research Guidance. August 8,2025.
https://basicresearch.defense.gov/Portals/61/Documents/Research%20Security/Fundamental%20Research%20Guidance.pdf

ii) 「基礎研究のためのリスクベース決定マトリックス」の作成

DoD における研究セキュリティ対応の取組として重要なのが、fundamental research（基礎研究）提案の審査判断を標準化するための「Decision Matrix（決定マトリックス）」の作成・公表である。DoD の Academic Research Security サイト[94]では、同マトリックスを関連文書として公開しており、2025 年版（2025 年 5 月 9 日以降の提出提案に適用）が現行の運用文書となっている。2025 年版[105]は、2023 年版の更新として、問題行動の審査基準の簡素化・明確化および議会による新要件の反映を目的としている。

同マトリックスは、国防省の構成機関およびプログラム担当者が、採択候補となった基礎研究提案に対して、どの程度のリスク低減措置を求めるかを判断するための判断補助（decision aid）を行うためのものである。2023 年版の導入説明では、同文書は利益相反・責務相反の潜在的問題を確認するためのガイドであり、①法令上禁止される行為、②緩和措置が必要・推奨される条件を整理するものと説明されている。DoD はこの文書を公開する理由として、問題視する行為類型を透明化し、DoD 資金を申請する研究者・大学が自らの提案がどのように審査されうるかを理解しやすくする点を挙げている。

DoD はマトリックスを単なる参考資料ではなく、全省的な審査の一貫性確保のための共通基盤として運用している。2023 年の方針文書では、各 DoD 構成機関に対し、マトリックスに整合した審査プロセスの整備、スポットチェック、OUSD(R&E)への審査要約の提出等を求めている。2023 年版マトリックスでは審査要約の提出頻度は「半期ごと（semiannual）」とされていた一方、2025 年版では「年次（annual）」提出を基本としつつ、OUSD(R&E)が必要に応じて更新頻度を調整できる形に改められている。
OUSD(R&E)は法令・政策の変更、運用上の教訓、他省庁との整合性を踏まえてマトリックス自体を更新するとされている。

以上のように、DoD の Decision Matrix は、研究セキュリティ審査の判断基準を可視化・段階化することで、部内の運用一貫性を高めると同時に、大学・研究者側にとっても「どのような行為・関係性が問題となり得るか」を事前に把握するためのガイドとして機能している点に特徴がある。

iii) 「中国・ロシア等の機関リスト」（NDAA 1286 リスト）の作成

国防省における研究セキュリティの取組の一つとして、NDAA（2019 会計年度国防権限法）第 1286 条に基づく機関リストの作成・更新が位置付けられている[101]。DoD の説明では、このリストは、①問題行為への関与が確認された外国機関（institutions）と、②米国の国家安全保障上の脅威となる海外人材採用プログラムを特定するための法定リストである。

---

[105] DOD. “Introduction to the 2025 DoD Component Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions” May 2025. https://basicresearch.defense.gov/Portals/61/Documents/Academic%20Research%20Security%20Page/2025%20DoD%20Decision%20Matrix%20to%20Inform%20Fundamental%20Research%20Risk%20Decisions.pdf

リスト掲載対象となる機関の判断基準として、①不適切な技術移転・知財窃取・サイバー／人的スパイ活動の履歴、②当該国の軍・情報機関の指揮下にあること、③軍事・情報目的の知識移転のための人材勧誘や関係隠蔽、④未公表・非公開の研究データ等の不適切移転に関する重大なリスクを列挙している[106]。また、同条は、リストを商務省産業安全保障局（BIS）、国家情報長官（DNI）、DoD 研究を多く実施する米国内大学、その他の適切な個人・組織との協議により作成・継続更新することを求めており、DoD はこの枠組みに沿って情報を集約している。

DoD は FY2024 版の 1286 条リストを公表しており、同文書の冒頭で、「問題行為に関与する外国機関リスト」の更新版であること、また国家安全保障上の脅威となる海外人材採用プログラムのリスト（FY2023 版）を再確認するものであることを説明している。DoD は、更新を継続的な取組とし、外国の懸念国への望ましくない技術移転（unwanted technology transfer）への対処の一環としている。本リストは制裁リスト的な性格のみを持つものではなく、基礎研究における相手機関・関係性のリスクを可視化し、案件ごとの審査・緩和措置判断を支える基盤情報としての性格が強い。

前述の DoD 共通 Decision Matrix では、1286 条リストは「Entity Lists」要素の一つとしている。

(c) 特色・注目点等

DoD の研究セキュリティ施策の最大の特徴は、基礎研究（fundamental research）の公開性を原則として維持しつつ、資金配分段階でリスク審査を制度化している点にある。これは、NSDD-189 が示した原則を土台にしつつ、近年は NSPM-33、CHIPS 科学法等への対応として、利益相反・責務相反を中心とするリスク審査を重ねる設計に進化したものである。

DoD は 2023 年の方針文書で、各 DoD の構成機関に共通のリスクベース審査プロセスを求め、OUSD(R&E)が全体の一貫性を監督する枠組みを導入した。審査は、技術評価で採択候補となった基礎研究提案を対象とし、研究内容そのものよりも、研究者・機関の関係性や開示情報に基づくリスク要因を確認する構造である。直近の 2026 年 1 月公表の措置では、部内横断リポジトリ整備が打ち出されており、審査・情報共有・継続監視の一体運用が強化されている。

運用面で特に注目されるのは、Decision Matrix（決定マトリックス）を公開している点である。2025 年版決定マトリックスは、海外人材採用プログラム、資金源、特許、エンティティ・リストとの関連で、助成金供与の禁止、リスク緩和策必須（Mitigation measures required）、リスク緩和策推奨（Mitigation measures expected/suggested）、リスク緩和策不要（No mitigation needed）となる要因（助成金申請者の悪性海外人材採用プログラムへの参加、懸念国からの資金受領等）を段階的に示している。

---

[106] SEC. 1286. Initiative to Support Protection of National Security Academic Researchers from Undue Influence and Other Security Threats. https://rt.cto.mil/wp-content/uploads/2025/03/Sec-1286-of-FY2021-NDAA.pdf

2.1.4 まとめ

(1) 大学・研究機関

本節で取り上げた３大学（MIT、テキサス A&M 大学システム、ワシントン大学）は、いずれも大規模な連邦研究資金を有する研究大学であり、研究セキュリティ対応が大学運営の近年の大きな課題となっている点で共通している。本事例比較からは、連邦政府が示す要件（NSPM-33、CHIPS 科学法、OSTP 2024 ガイドライン等）が、大学現場では規制遵守だけではなく、研究推進・国際連携・リスク管理を統合する運用設計へと各大学の特色ある方法で実装されている点が確認できる。

事例調査の結果と示唆をまとめると以下のとおりである。

第一に、大学の規模・構造に応じて、実装のモデルが単独の研究大学型（MIT 型）、複数大学・研究機関を束ねるシステム型（テキサス A&M 大学システム型）、そして全国支援基盤を担う中核拠点型（ワシントン大学/SECURE 型）で機能とガバナンスの構造が異なる。日本において、例えば、大規模大学型、大学群・地域連携拠点型、中小規模大学型等、類型別に実装のモデルを示す方法が考えられる。

第二に、研究者向けの実装支援については、MIT のツール等、ワシントン大学の補助教材では、研究現場の行動単位に落とし込んだツール群が整備されていた。

第三に、研究セキュリティ人材と、機関横断の基盤としてテキサス A&M 大学システムの RISC Institute、ASCE、URSPA、ワシントン大学の SECURE Center（SVE、リスクマトリクス、訓練モジュール（共通研修教材）、週次ブリーフィング）等の取組は、その他個々の大学の経営基盤だけでは対応しきれない研究セキュリティ・研究インテグリティの確保に関する実務負担を支えている。日本において、例えば、情報集約機能や、標準教材等の整備が有効である可能性がある。

(2) 資金配分機関

連邦レベルの研究セキュリティの枠組み（NSPM-33、CHIP 科学法等）に対し、本節で取り上げた２資金配分機関（NSF と、資金配分機関としての DoD）は共通する取組をしているとともに、同じ研究セキュリティ対応であっても、組織の性格・配分構造・ミッションの違いに応じて、相違点もみられる。

事例調査の結果と示唆をまとめると以下のとおりである。

第一に、現場実装支援について、NSF では、ルールの大学・研究機関への通知に加え、SECURE Center 型の共通支援基盤（研修、ツール、相談、実装知見の共有）に対する支援が行われていた。これらは、大学規模・体制差による現場実装による格差を埋めることに対して効果があると考えられる。

第二に、審査基準について、DoD の Decision Matrix では、海外人材採用プログラム、資金源等との関連で、助成金支出に関して、禁止、緩和策必須、緩和策推奨となる要因

（懸念国からの資金受領等）等を示しており、研究者、大学・研究機関、審査担当者の認識差や判断のばらつきを減らす効果があると考えられる。

第三に、研究の開放性の原則とリスク管理の示し方について、DoD では、fundamental research の公開性を上位原則として再確認しつつ、資金配分段階で COI（利益相反）/COC（責務相反）や関係性のリスクを審査している。研究セキュリティへの対応による過度な萎縮が懸念される場合には、両者を明文化することで安全保障上の懸念に対応できる可能性がある。

第四に、制度検証のための対応として、NSF の RoRS は、研究セキュリティそのものを研究対象としている点は注目される。これは、施策の効果検証・実務知見の蓄積等のための試みと考えられる。

【米国の研究セキュリティ関連の公表文書（2025 年 3 月～2026 年 2 月）】

(a) NSF

NSF Important Notice No. 149「Updates to NSF Research Security Policies」（2025年7月10日発出、11月24日更新）[107]

米国科学財団（NSF）が2025年7月10日に発出したImportant Notice No. 149「Updates to NSF Research Security Policies」は、CHIPS and Science ActおよびNSPM-33の要請を受けて、NSFが実施する研究セキュリティ政策の更新内容を示した重要通知である。

(b) NIH

共通フォームの作成、研修受講義務についての規定発出など。

NIH Announces a New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements（2025年7月17日公表）[108]

NIHは、NIH資金の受領機関（recipients）に対し、申請書等でシニア／主要人員（Senior/Key Personnel）に該当する研究者について、“Other Support（その他支援）”の開示要件に関するトレーニングを実施することを新たに義務づける。

NIH’s Implementation of Common Forms for Biographical Sketch and Current and Pending (Other) Support for Due Dates on or after January 25, 2026（2025年12月2日公表）[109]

NIHは、OSTP（大統領府科学技術政策局）の「共通開示様式（Common Disclosure Forms）」方針に沿って、Biosketch（経歴・実績）とCurrent and Pending (Other) Support（現在および保留中の（その他の）支援）について、政府横断で整合した共通様式（Common Forms）を採用し、NIH向けの補足（NIH Biographical Sketch Supplement）や提出方法を示した。

Research Security Training Requirements for NIH（2025年12月2日公表）[110]

この通知の趣旨は、CHIPS and Science Act of 2022（同法の研究セキュリティ研修要件）に基づき、NIHがResearch Security Training（RST）要件をNIHの助成金申請（extramural）に実装することを通知している。NIHでは、法が定める「対象研究者（covered individual）」はシニア／主要人員（Senior/Key Personnel）として扱われる。現時点ではRSTは任意だが、2026年5月25日以降の締切（due date）で提出される申請から、RST修了および各種「認証（certification）」が有効（＝実質的に

[107] https://www.nsf.gov/notices/important/important-notice-no-149-updates-nsf-research-security/in149
[108] NIH Announces a New Policy Requirement to Train Senior/Key Personnel on Other Support Disclosure Requirements. Notice Number: NOT-OD-25-133. Release Date: July 17, 2025. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-25-133.html
[109] NIH’s Implementation of Common Forms for Biographical Sketch and Current and Pending (Other) Support for Due Dates on or after January 25, 2026. Notice Number: NOT-OD-26-018. Release Date: December 2, 2025. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-26-018.html
[110] Research Security Training Requirements for NIH. Notice Number: NOT-OD-26-017. Release Date: December 2, 2025. https://grants.nih.gov/grants/guide/notice-files/NOT-OD-26-017.html

要件化）になる。申請提出日の過去12か月以内にRSTを修了したことを認証する必要がある。

(c) 国防省（DoD）

「Department of Defense Fundamental Research Guidance」（2025年8月4日）[111]

2025年8月4日に公表された「Department of Defense Fundamental Research Guidance」（国防省基礎研究ガイダンス）は、国防省が支援する基礎的・基盤的研究（fundamental research）について、研究セキュリティ要求と学術的自由・オープンな成果公開の両立を図ることを目的としたガイダンスである。

「Fundamental Research Security Initiatives and Implementation」（2026年1月8日）[112]

国防省資金による研究、とりわけfundamental research（基礎研究）を、悪意ある外国の影響（malign foreign influence）、知的財産の窃取、および研究成果の搾取から守るための、部内横断の対策強化。以下の措置を含む。

・NDAA（国防権限法）Section 1260Hに基づく「中国軍事企業（Chinese military companies）」リスト掲載企業に対し、基礎研究の助成（assistance award）資金を供与しないこと
・省内の全部局にまたがる、Fundamental Research Risk Review Repository（リスク審査リポジトリ）を新設し、情報収集・共有を改善すること。などを規定。

(d) 議会の動向

連邦議会（上院、下院）の様々な委員会で、中国と研究セキュリティ、政府省庁や公的研究機関における研究セキュリティへの対応状況、「2025年米国研究保護法案」等について討議が行われている。以下の報告書を公表している。

House Select Committee on the CCP. Fox in the Henhouse: The U.S. Department of Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research.（2025年9月5日）[113]

米国国防省の研究・技術担当国防次官室の研究セキュリティ体制の欠陥を集中的に批判したレポートである。国防省の研究資金による研究論文を約1,400本洗い出し、その半数以上が、中国の防衛研究・軍需産業基盤（国防7大学（Seven Sons）、国家国防科技工業局（SASTIND）系大学、軍関連企業）の研究者との共著であり、AI、量子、半導体、先端材料、宇宙・ミサイル、軍事用センサー等、重要・新興技術が中心であると指摘している。

---

111 https://basicresearch.defense.gov/Portals/61/Documents/Research%20Security/Fundamental%20Research%20Guidance.pdf

112 Department of War. The War Department Strengthens Measures to Protect DOW-Funded Research. Jan. 8, 2026 https://www.war.gov/News/Releases/Release/Article/4373247/the-war-department-strengthens-measures-to-protect-dowfunded-research/

113 The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. Fox in the Henhouse: The U.S. Department of Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research. September 2025. https://selectcommitteeontheccp.house.gov/media/reports/fox-in-the-henhouse

House Select Committee on the CCP. Joint Institutes, Divided Loyalties: How the Chinese Communist Party Exploits U.S. University Partnerships to Empower China's Military and Repression（2025年9月11日）[114]

2024年の報告書CCP on the Quad（2024年9月、下院中国特別委員会＋教育労働委員会）で示した「米国防省・DOE・NSFの資金が中国軍事技術の進展に寄与している」との問題提起を引き継ぎ、「Joint Institutes」や中外合作学部・ダブルディグリー等の共同教育・研究拠点に焦点を当てたフォローアップ報告である。

House Select Committee on the CCP. From Ph.D. to PLA: How Visa Policies Enable PRC Defense Entities to Tap U.S. Higher Education（2025年9月19日）[115]

米国のビザ・学生受入れ政策と、中国人民解放軍（PLA）/中国国防産業による人材・知識獲得の関係を分析している。国防7大学（Seven Sons of Ordnance／Arms Industry）や国家国防科技工業局（SASTIND）共管58大学など、軍民融合の中核となる中国大学群を整理し、それらの出身者・在籍者が米大学の博士課程やポスドクとして受け入れられている実態を、複数大学のケーススタディとして提示している。

Select Committee on China, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence. Containment Breach: The U.S. Department of Energy's Failures in Research Security and Protecting Taxpayer-Funded Research from Foreign Exploitation（2025年12月17日）

本報告書は、米国エネルギー省（DOE）が資金提供・支援する研究が、中国の軍事・防衛産業基盤や技術移転エコシステムに結び付く組織と広範に協働してきた実態を、出版物データ・助成記録・中国語資料等の分析、およびDOE内部から得た説明等を用いて示し、DOEの研究セキュリティ・研究インテグリティ上の統治不全を構造問題として批判するものである。

(e) ナショナルアカデミーにおける議論

ワークショップが定期的に開催（連邦政府機関、大学・研究機関から研究セキュリティの業務担当者、専門家等が出席）され、大学・研究機関における研究セキュリティについての対策等について討議されている。また、研究セキュリティに関連する報告書が策定されている。

---

[114] The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party and the Committee on Education and the Workforce. Joint Institutes, Divided Loyalties: How the Chinese Communist Party Exploits U.S. University Partnerships to Empower China's Military and Repression. September 2025. https://selectcommitteeontheccp.house.gov/media/reports/joint-institutes-divided-loyalties

[115] The Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. From Ph.D. to PLA: How Visa Policies Enable PRC Defense Entities to Tap U.S. Higher Education. September 2025. https://selectcommitteeontheccp.house.gov/media/reports/from-phd-to-pla

Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop（ワークショップ開催：2025年5月22–23日）[116]

このワークショップ報告書は、近年の対外脅威に対する懸念の高まりのなかで、「高等教育機関における研究セキュリティ対策は、実際どの程度効果を上げているのか」を評価することを目的としている。

Simplifying Research Regulations and Policies: Optimizing American Science（2025年9月）[117]

報告書は、連邦レベルの研究規制・ポリシーを「7つの規制領域」に整理し、それぞれについて、行政機関・議会・大学等が取り得るオプションを提示するメニュー型の提言となっている。その中で、研究セキュリティや輸出管理、サイバーセキュリティ、研究データ管理などを一括して扱う領域が「Regulatory Area 4: Protecting Research Assets」として独立に位置づけられている。この領域について報告書は、近年、規制の重要性が増した一方、規制体系は相変わらず断片的で、各省庁が重複・矛盾した要件を課しているため、大学側に過大な事務負担と不確実性をもたらしていると指摘している。

National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop – Highlights（2025年10月）[118]

この4ページのハイライト資料は、2020～2024年にわたって活動した「National Science, Technology, and Security Roundtable（NSTSR）」の最終ワークショップ（2024年7月16-17日開催）の議論を要約したものである。NSTSRは、連邦研究機関、情報・法執行機関、大学、産業界のリーダーを一堂に集め、「米国の科学技術力と国家・経済安全保障をいかに同時に維持するか」を巡る課題を継続的に議論する場として設置された。ハイライトでは、ラウンドテーブルの全体像を振り返るとともに、特に研究セキュリティに関する議論と含意が整理されている。

(f) 議会調査機関等

Congressional Research Service (CRS). Federal Research Security Policies: Background and Issues for Congress.（2025年5月）[119]

連邦レベルの研究セキュリティ政策を体系的に整理し、議会が検討すべき論点を提示している。まず、

---

116 National Academies of Sciences, Engineering, and Medicine, Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop, Washington, DC: The National Academies Press, 2025. https://www.nationalacademies.org/publications/29241

117 National Academies of Sciences, Engineering, and Medicine, Simplifying Research Regulations and Policies: Optimizing American Science, Washington, DC: The National Academies Press, 2025. https://www.nationalacademies.org/projects/PGA-POLICY-25-05/publication/29231

118 National Academies of Sciences, Engineering, and Medicine, National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop – Highlights, Policy and Global Affairs, 2025 年 10 月。
https://nap.nationalacademies.org/resource/27976/Highlights_Science_Technology_and_Security_Roundtable.pdf
ベースとなる本編報告書：National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop, National Academies Press, 2025 年 1 月 28 日.
https://www.nationalacademies.org/publications/27976

119 Congressional Research Service. Federal Research Security Policies: Background and Issues for Congress. May 20, 2025. R48541. https://www.congress.gov/crs-product/R48541

研究セキュリティを、軍事スパイ行為だけでなく、外国政府やその関連組織による不透明な研究支配、知的財産・未公開成果の不適切な移転、そして場合によっては研究インテグリティの侵害を含む概念として位置づけている。そのうえで、2010年代後半以降の主要な政策の流れを説明し、どの法律・覚書・ガイドラインが、どの主体（大学・FFRDC・連邦研究機関など）にどの義務を課しているかを整理している。副作用として、開示フォームやコンプライアンス要求の複雑さによる行政負担、外国出身研究者への萎縮効果や差別的取り扱いの懸念、機関ごと・省庁ごとのバラバラな運用による混乱、といった点を挙げ、これらをどう緩和しつつリスクを管理するかが今後の「Issues for Congress」として提示されている。

GAO. Research Security: Agencies Should Assess Safeguards Against Discrimination（2026年1月）[120]

本報告書は、連邦政府の研究助成における研究セキュリティへの対策が、特定の人種・民族・出身（特に中国系／アジア系研究者）を不当に標的化しないよう、各省庁がどの程度の差別防止の防止策を整備・運用しているかを点検した。GAO は、研究セキュリティは納税者資金の不正や研究成果の不正流出を防ぐ上で重要である一方、審査・調査の過程が差別的になり得るとの懸念があるため、差別が起きにくい設計になっているかに焦点を当てている。大学・研究機関への研究資金配分が大きい 5 機関―国防省、エネルギー省、航空宇宙局、NIH、NSF―を対象に、文書調査・文献レビュー・関係者（大学・市民社会組織等）への聞き取りを実施した。加えて、人口統計データ（人種等）を用いて差別の兆候を点検できるかを見るため、データが得られた NIH について統計分析も行った。防止策の採用状況は機関ごとにばらつきがあり、特に人口統計データの活用は多くの機関で未導入であった。

[120] GAO. Research Security: Agencies Should Assess Safeguards Against Discrimination. GAO-26-107544. Published: Jan 21, 2026. Publicly Released: Jan 22, 2026. https://www.gao.gov/products/gao-26-107544

2.2 カナダ

2.2.1 研究セキュリティ・インテグリティ関連政策動向

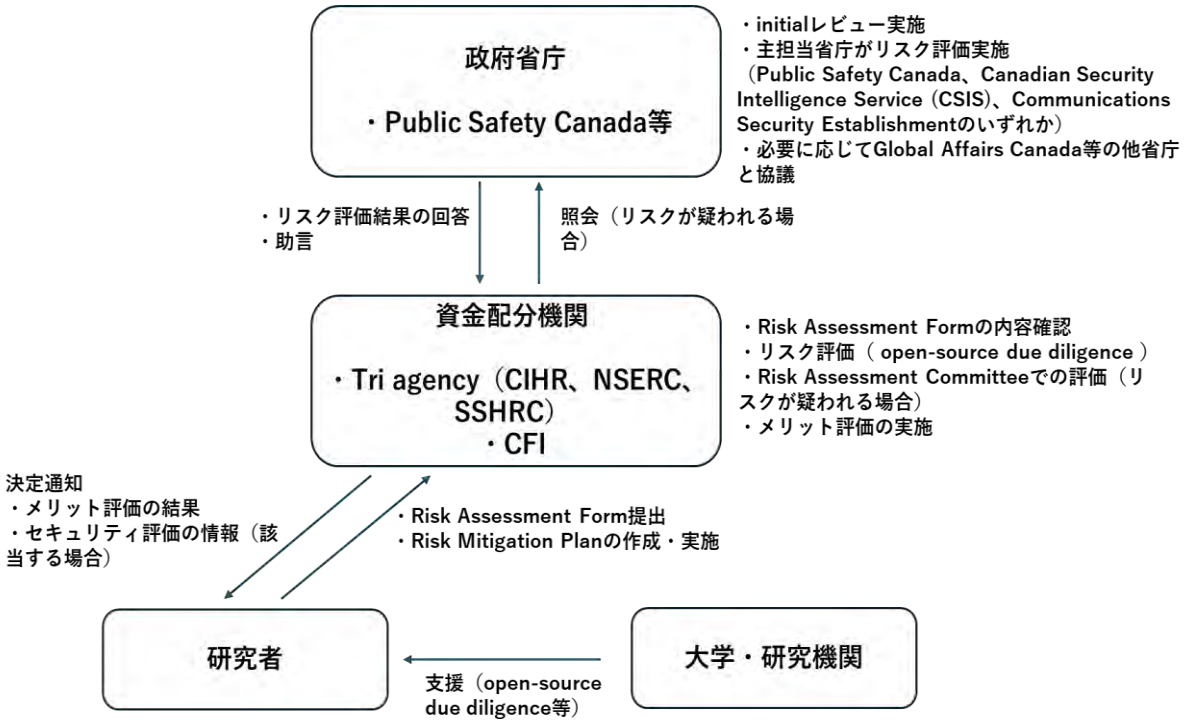
カナダ政府の研究セキュリティ政策は、近年、①「研究パートナーシップのための国家安全保障ガイドライン」（National Security Guidelines for Research Partnerships: NSGRP）（2021 年）に基づく、研究パートナーシップ案件に対するリスクベース審査と、②「機微技術研究および懸念される提携に関する方針」（Policy on Sensitive Technology Research and Affiliations of Concern: STRAC）（2024 年）の二本柱で制度化が進んでいる。

連邦研究助成の実施主体である資金配分機関（カナダ保健研究機関（Canadian Institutes of Health Research: CIHR）、自然科学・工学研究会議（Natural Sciences and Engineering Research Council of Canada: NSERC）、社会・人文科学研究会議（Social Sciences and Humanities Research Council: SSHRC）の 3 資金配分機関（「Tri-Agency」と呼ばれている）およびカナダ・イノベーション財団（Canada Foundation for Innovation: CFI））は、政府が策定したこれらの政策・ガイダンスを共通枠組みとして実装しており、研究の公開性・国際連携を維持しつつ、国家安全保障上のリスク判断を助成審査に組み込む構造となっている。

第一の柱である NSGRP[121]は、2021 年 7 月に導入された。導入当初は NSERC の Alliance Grants（民間連携機関（企業等）を含む案件が対象）で必須化され、申請者には「リスク評価票」（Risk Assessment Form）の提出と、リスクに応じた緩和計画の作成が求められる。政府は当初から、大学との共同ワーキンググループを通じて制度を設計しつつ、将来的に他の助成機関への展開も示していた（図 2-5 参照）。

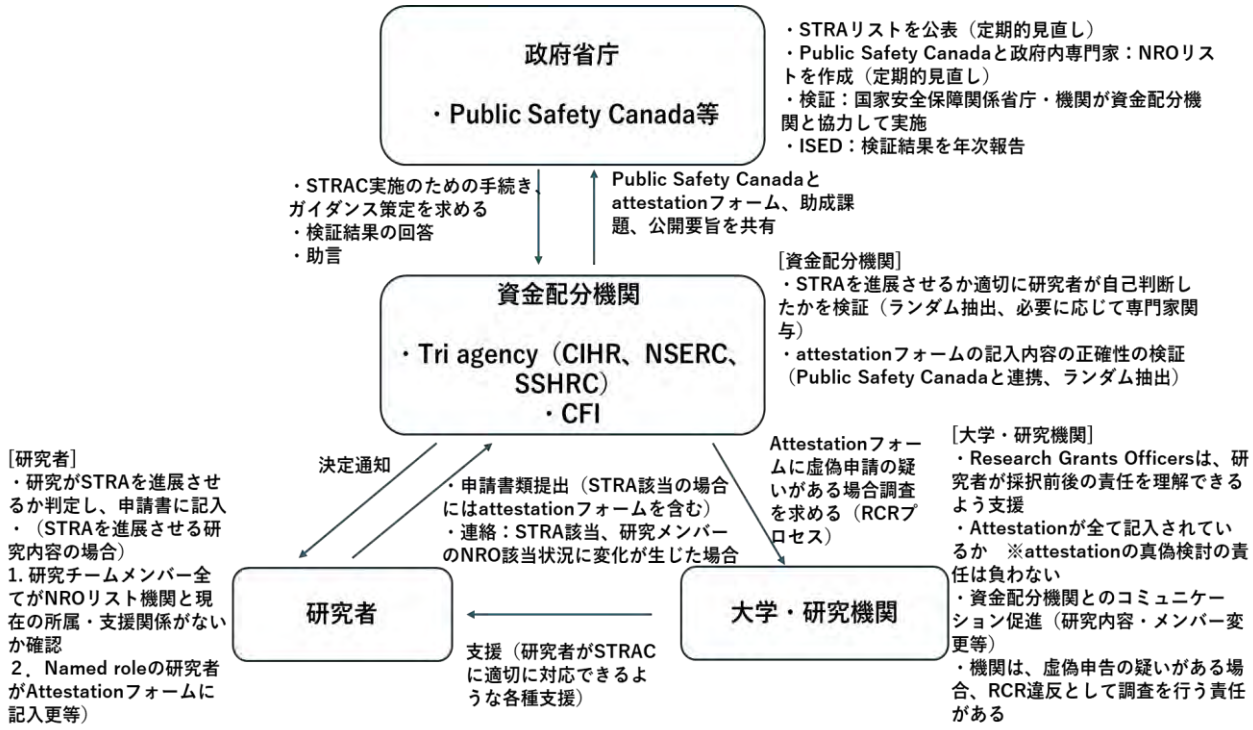
第二の柱である STRAC[122]は、2024 年 1 月に政策として公表され、2024 年 5 月 1 日以降に公募開始される対象制度から Tri-Agency で実施されている。STRAC では、「機微技術研究領域」（Sensitive Technology Research Areas: STRA）を「前進（advance）」させる研究を対象に、研究チームの関係者が「指名研究機関」（Named Research Organizations: NRO）に現在所属している、または資金・現物支援を受けている場合、当該申請は原則として不採択となる。政府はこの運用のために、STRA リストと NRO リストを公表し、申請段階では研究者による「誓約」（attestation）の提出を求めている（図 2-6 参照）。

121 National Security Guidelines for Research Partnerships
https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships
122 Sensitive Technology Research and Affiliations of Concern
https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern



出典；National Security Guidelines for Research Partnerships の内容に基づいて図を作成。

図 2-5　NSGRP の内容と主要アクターの役割



出典；Policy on Sensitive Technology Research and Affiliations of Concern の内容に基づいて図を作成。

図 2-6　STRAC の内容と主要アクターの役割

(1) 2024 年度までの経緯

カナダにおける研究セキュリティ政策は、2019 年頃からの政府主導の啓発・情報提供を起点として、2021 年以降は資金配分過程に国家安全保障上の審査を組み込む制度へと段階的に発展してきた。初期段階では、公共安全省（Public Safety Canada: PSC）による学術界向けの安全保障意識向上文書[123]や、政府・大学共同ワーキンググループにより整備された「Safeguarding Your Research Portal」[124]などを通じて、研究者・大学向けのリスク認識と実務的対策の底上げが図られた。

その後、2021 年 3 月の 3 大臣（イノベーション・科学・経済開発省（Innovation, Science and Economic Development Canada: ISED）、公共安全省、保健省の大臣）による研究セキュリティ政策声明[125]を経て、同年 7 月に NSGRP が導入された。NSGRP は、研究者・研究機関・連邦資金配分機関が一貫したリスクベースのデュー・ディリジェンスを行うための枠組みであり、対象となる公募では、民間パートナー（企業等）を含む申請に対してリスク評価フォームと、リスクに応じた緩和計画の提出を求める点に特色がある。また、運用指針上、リスク緩和は特定集団への差別につながってはならないことも明示されている。

2023 年 2 月には、3 大臣声明により、カナダ政府は研究セキュリティについて「強化された姿勢（enhanced posture）」をとる方針を示し、機微な研究領域に関する申請について、外国の軍・国防・国家安全保障機関に結びつく機関との関係を持つ研究者が関与する場合の資金配分制限を打ち出した[126]。これを受け、2024 年 1 月 16 日には STRAC が公表され、併せて STRA リストおよび NRO リストが提示された [122]。政府はこれを、NSGRP とは別個だが補完的な制度として位置づけ、2024 年 5 月から施行された。

---

123 Public Safety Canada. Building security awareness in the academic community. 2020. https://publications.gc.ca/collections/collection_2021/sp-ps/PS4-261-2020-eng.pdf
Research Security Information Update. May 2021. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx

124 “Introducing the Safeguarding your Research Portal” https://www.canada.ca/en/research-coordinating-committee/news/updates/2020/09/safeguarding-your-research-portal.html

125 “Government of Canada announces next steps in safeguarding research” From: Innovation, Science and Economic Development Canada. March 24, 2021. https://www.canada.ca/en/innovation-science-economic-development/news/2021/03/government-of-canada-announces-next-steps-in-safeguarding-research.html

126 Statement from Minister Champagne, Minister Duclos and Minister Mendicino on protecting Canada’s research. Innovation, Science and Economic Development Canada. February 14, 2023. https://www.canada.ca/en/innovation-science-economic-development/news/2023/02/statement-from-minister-champagne-minister-duclos-and-minister-mendicino-on-protecting-canadas-research.html

表 2-4　近年のカナダにおける研究セキュリティ・インテグリティ関連文書

時期	内容
2019年	公共安全省が「学術界における安全保障意識の醸成（Building Security Awareness in the Academic Community）」文書を発表。
2020年9月	カナダ政府は、カナダ政府・大学共同ワーキンググループが開発した「あなたの研究を保護するためのポータルサイト（Safeguarding Your Research Portal）」を開設し、研究コミュニティが研究と知的財産を保護するためのガイダンス、情報、ツールを提供することを開始した。
2020年9月	カナダ・サイバーセキュリティ・センターは、「研究開発におけるセキュリティの考慮事項（Security Considerations for Research and Development）」に関する出版物を発表した。
2021年1月	カナダ政府は、カナダの研究コミュニティ及びイノベーション・科学・経済開発相と緊密に連携し、世界をリードするカナダの研究を引き続き保護することを公共安全相に義務づけた。
2021年3月	・「研究セキュリティ政策声明（Research Security Policy Statement）」 イノベーション・科学・経済開発相、公共安全相、保健相は、カナダの研究事業のインテグリティ、国家安全保障、長期的な経済競争力と繁栄を守ると同時に、オープンで協力的な研究環境を支援する声明を発表した。
2021年7月	・「研究パートナーシップのための国家安全保障ガイドライン」（NSGRP） カナダ連邦政府は、カナダ政府・大学共同ワーキンググループから協力を得た上で、本ガイドラインを作成・公表した。
2023年2月	・3大臣声明（イノベーション・科学・経済開発大臣、保健大臣、公安大臣）
2024年1月	・3大臣声明（イノベーション・科学・経済開発大臣、保健大臣、公安大臣） ・「機微技術研究および懸念される提携に関する方針」（STRAC）の公表。
2024年3月	Tri-Agency Guidance on the STRAC Policy
2024年5月1日	STRACの施行と具体運用

出典：「研究インテグリティ（Research Integrity）に係る調査・分析報告書」（未来工学研究所、2024年3月）37～38頁などから作成。

(2)　最近の主な動き

2025年3月以降のカナダの研究セキュリティをめぐる動きは、①連邦政府による制度運用の継続、②大学・研究機関側の体制整備・取組みへの政府財政支援、③州・大学セクターによる制度化の進展、④オープンサイエンスとの両立をめぐる政策的整理の深化、という4つの層で捉えることができる。[127]

第一に、連邦政府レベルでは、研究セキュリティ施策の運用状況を年次で可視化する枠組みが定着しつつある。ISEDの研究セキュリティ・ポータル上では、三資金配分機関およびCFIにおける実施状況を整理した年次報告書（2023–2024年版）が公開されている

[127] このセクションに関係する文書については、【カナダの研究セキュリティ関連の公表文書（2025 年 3 月～2026 年 2 月）】を参照。

[128]。

第二に、実装能力（implementation capacity）の強化という点では、公共安全省のResearch Security Centre（RSC）に関する2025年評価報告[129]が重要である。同報告によれば、RSCは2024年1月に正式発足し、大学コミュニティに対する政府サービスの窓口として、助言・ガイダンス提供、連邦内外の調整、研修・アウトリーチを担う。体制規模は「2022年予算」で措置された今後5年間1,260万カナダドル、以降は年280万カナダドル、職員数12人（フルタイム換算）であり、評価報告自身も、現時点の需要には概ね対応している一方、将来的な追加リソースの必要性を指摘している。RSCは小規模なハブ（調整・助言・能力構築の核）として機能し、実際の実装は各資金配分機関・大学・関係省庁に分散して担われる構図と考えられる。

第三に、大学・研究機関側の実装を支える財政面では、Research Support Fund（RSF）の「研究セキュリティ」枠の制度化が進んでいる。連邦政府は、研究セキュリティをRSFの第5の重点分野として位置づけ、5年間で総額1.25億カナダドル（その後は年間2,500万カナダドル）を措置しており、一定規模以上の研究費を受ける大学等に対し、研究セキュリティ体制整備を資金的に支援する。2025年には、機関別のノーティナル額（見込額）と実支給額の双方が公開され、大学側が人員配置・研修・審査体制整備を計画しやすい運用となっている。実際に公表された実支給額一覧からは、大規模研究大学に数百万ドル規模、小規模大学に数万〜十数万ドル規模の支給金額であり、機関規模に応じた配分が確認できる。[130]

第四に、州・大学セクターの動きとして、オンタリオ州では2025年のBill 33（Supporting Children and Students Act, 2025）[131]により、州の研究資金を受領する大学等に対し研究セキュリティ計画の策定・実装を求める規定が法制化された。また、Council of Ontario Universitiesは2025年6月に、研究の開放性・国際協力・EDI[132]を維持しつつ、合理的かつリスクベースで研究保護を進める「共通コミットメント」を公表している。

また、カナダアカデミー評議会（Council of Canadian Academies: CCA）の報告書Balancing Research Security and Open Science（2025年10月）[133]は、カナダの研究セキ

---

[128] Government of Canada. Annual Report on the Implementation of Research Security Policies within the Federal Granting Agencies and the Canada Foundation for Innovation 2023-2024 https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/additional-resources/annual-reports/annual-report-2023-2024

[129] Public Safety Canada. Evaluation of the Funding to Build Canada's Research Security Capacity. July 2025. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-fndng-bld-cnds-rsrch-scrty-cpcty/index-en.aspx

[130] https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-eng.aspx#8
Research Security notional amounts for 2025-26（ノーティナル額：2025 年 8 月 20 日）
https://www.rsf-fsr.gc.ca/apply-demande/grants-subventions/rs2025-eng.aspx
Research Security Funding Awarded in 2025-26（実際の支給額：2025 年 10 月 22 日）
https://www.rsf-fsr.gc.ca/apply-demande/notional/research_security-2025-eng.aspx

[131] Bill 33, Supporting Children and Students Act, 2025. Legislative Assembly of Ontario. 新設の 20.1 条 "Research security plan" https://www.ontario.ca/laws/statute/s25012

[132] EDI（Equity, Diversity and Inclusion）：公平性、多様性、包摂性

[133] CCA (Council of Canadian Academies). (2025). Balancing Research Security and Open Science.

ュリティ確保の取組の現状を俯瞰した文書として重要である。同報告書は、カナダ国防研究開発省（Defense Research and Development Canada）およびカナダ公衆衛生庁（Public Health Agency of Canada）の要請に基づく独立評価として作成され、従来の生命科学中心の「デュアルユース性が懸念される研究」（Dual Use Research of Concern: DURC）概念より広い「懸念される機微研究」（sensitive research of concern）という概念で、機微性の判断と保護措置を分野横断で検討している。また、研究セキュリティを「研究者だけの責任」ではなく、研究者・大学執行部・資金配分機関・政府・情報機関・民間部門を含む研究エコシステム全体の「責任の共有」（shared responsibility）として位置づけている。

このように、2025年以降のカナダの研究セキュリティ政策は、NSGRPとSTRACという既存制度の単純な強化ではなく、①RSCを中心とした実装支援、②RSFによる大学側能力構築の財政的支援、③州レベルでの研究セキュリティ確保策、④CCAによる概念整理などの動きがみられる。

2.2.2　大学・研究機関における取組

カナダの研究セキュリティ制度は、連邦レベルでは主として研究資金申請・執行の要件として実装されており、研究者（申請者・研究チーム）に対する申告・確認・継続的遵守の要求が中心である。他方、大学・研究機関には、これを支える申請管理・所属研究者への周知・手続支援の役割が明示される。加えて、一部の州（例：オンタリオ州）では、州独自の研究資金制度において、大学・研究機関（Applicant）自体に対する要件をより直接的に課している。

前述のとおり、まず、連邦レベルの NSGRP で、対象となる連邦研究パートナーシップ助成において、民間パートナーを含む申請に対してリスク評価フォーム（Risk Assessment Form）の提出を求め、申請者にリスク軽減計画（mitigation plan）の策定・実施を求める。軽減策は差別につながってはならない旨も明記されている。

次に、STRAC では、STRA を前進させる研究については、研究チームの関係者が NRO に現に所属・支援関係を有する場合、当該申請は資金供与の対象外となる（ただし、過去の関係は問わない）。そのため、研究者側には、①自らの研究が STRA に該当するかの判定、②該当する場合の Attestation 提出、③採択後の継続的遵守（研究内容・研究チーム変更時の対応を含む）という、明確な義務・責任が課されている。

大学・研究機関の役割は、STRAC では「研究者の代わりに内容の真偽を審査し、正確性を保証すること」ではなく、制度遵守を支える管理機能として整理されている。NSERC の Tri-agency ガイダンスでは、研究助成担当（Research Grant Officers）等に対し、研究者への周知、必要な Attestation の完全性確認[134]（completeness check）、研究内

Ottawa, ON: Expert Panel on Sensitive Research of Concern, CCA. https://doi.org/10.60870/fmt9-9559.

[134] 記入すべき箇所がすべて記入されているかを確認するということである。

容や研究チーム変更時の資金配分機関との連絡支援が求められる一方、Attestation の正確性の検証自体は研究者本人の責任とされている。また、虚偽申告等が疑われる場合には、Tri-agency の「責任ある研究行動規範」（Responsible Conduct of Research: RCR）の枠組みに基づき、大学・研究機関が照会・調査（inquiry、investigation）を担う構造になっている。

また、州レベルの研究セキュリティ規則では、オンタリオ州の「Research Security Guidelines for Ontario Research Funding Programs」（2024 年 6 月版）[135]は、州の研究資金制度について、Applicant（主たる申請機関＝大学等）自体に手続要件を直接課す設計がより明確である。

以上を踏まえると、カナダの大学・研究機関の研究セキュリティ実装をみる際には、①連邦制度（NSGRP/STRAC）への対応としての研究者支援・申請管理・コンプライアンス運用と、②州制度（オンタリオ州など）への対応としての機関としての申請統制・リスク管理体制を分けて把握することができる。

(1) アルバータ大学（University of Alberta）

アルバータ大学（University of Alberta）は、カナダ・アルバータ州エドモントンを拠点とする研究集約型の総合大学であり、カナダの主要研究大学群（U15）の一角を占める。学生数は約 4.6 万人、職員数は約 1.2 万人、5 キャンパス 17 学部を擁する大規模大学である[136]。アルバータ大学の外部資金による研究収入（Sponsored Research Income）は約 6.21 億カナダドル（FY2023）でカナダ国内第 5 位に位置づけられており[137]、カナダ有数の研究拠点としての地位が確認できる。AI、ナノテクノロジー、移植医療、糖尿病研究などの研究面の強みを有し、国際連携も広く展開している[138]。

高い研究開放性と国際共同研究の厚みを前提に、同大学は研究セキュリティ対応を全学的に位置づけており、「Safeguarding Your Research」[139]の考え方を説明している。また、Safeguarding Research Office（SRO）が研究セキュリティ要件への実務支援等の機能を担い、Responsible Open Source Due Diligence Protocol（2025 年）で、オープンソース情報に基づくデュー・ディリジェンスを透明性・一貫性・公正性をもって実施する運用枠組みを示している[140]。

---

135 Ontario Ministry of Colleges and Universities. Research Security Guidelines for Ontario Research Funding Programs https://forms.mgcs.gov.on.ca/dataset/875d7629-9ddc-4545-a1c3-881ece0cb3a3/resource/6219fff3-aa2e-49ae-955c-0ebbd21059f1/download/on00708e.pdf
136 University of Alberta “University of Alberta Facts” https://www.ualberta.ca/en/about/facts.html
137 Canada's Top 50 Research Universities 2024 https://researchinfosource.com/cil/2024/top-50-research-universities/list
138 U15 Canada “University of Alberta” https://u15.ca/members/university-of-alberta/
139 University of Alberta “Safeguarding Your Research” https://www.ualberta.ca/en/research/services/safeguarding-your-research.html
140 “Responsible Open Source Due Diligence Protocol” https://www.ualberta.ca/en/research/media-library/services/2025_07-23_protocol_framework_external.pdf

(a) 背景・経緯等

2021 年の NSGRP の導入以降、アルバータ大学は、研究の開放性を維持しつつ安全性を確保するという考え方を明確化し、全学的な支援体制を整備してきた。2021 年に学内横断の調整機能として Safeguarding Research Working Group を置き[141]、2023 年に SRO を設置し[142]、SRO を中心にデュー・ディリジェンスやリスク評価の運用を支える体制が採られた。2024 年には SRO の初回の Impact Report が公表され[143]、2025 年にはアルバータ大学におけるデュー・ディリジェンスの運用文書である Responsible Open Source Due Diligence Protocol が公表された。

(b) 主な取組

i) 学内の体制整備（SRO の設置等）

アルバータ大学では、連邦政府の研究セキュリティ強化策（Budget 2022）で措置[144]された研究機関向けの能力構築支援（Research Support Fund（RSF）内の一区分）を活用し、学内の実施体制を整備してきた。具体的には、SRO を 2023 年に設置し、研究者・職員が研究セキュリティ要件に対応するための相談・実務支援機能を担わせている。大学公開資料でも、SRO は連邦資金（RSF 経由）により運営されていることが示されており、国の資金支援と大学内の実装体制が連動している点が特徴である。[142]

ii) Responsible Open Source Due Diligence Protocol

2025 年公表の Responsible Open Source Due Diligence Protocol[145]は、SRO が実施するオープンソースインテリジェンス（Open Source Intelligence: OSINT）によるデュー・ディリジェンスを、法令・学内方針・倫理要件に適合させつつ、透明・一貫・公正に運用するための実務プロトコルである。同プロトコルは、SRO のデュー・ディリジェンス活動を大学の研究イノベーションエコシステムを研究セキュリティ上のリスクから守るための支援と位置づける。連邦・州の要件（NSGRP、STRAC、アルバータ州の対中パートナーシップ方針等）への対応と、大学の意思決定支援（リスク特定・評価・緩和）を接続する枠組みとして整理している。特に、アルバータ大学の Due Diligence for Safeguarding

---

141 “Alberta's major universities hit pause on new research initiatives with China” Mark Lowey. December 22, 2021. https://researchmoneyinc.com/article/albertas-major-universities-hit-pause-on-new-research-initiatives-with-china

142 University of Alberta. Safeguarding Research Office. https://www.ualberta.ca/en/research/media-library/services/2023-vpri-sro-handout-three-pager.pdf

143 Impact Report: Engage, Educate, Support. Safeguarding Research Office. Office of the Vice-President (Research & Innovation). University of Alberta. https://www.ualberta.ca/en/research/media-library/services/2024-safeguarding-research-office-impact-report.pdf

144 Research security. https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-eng.aspx
Archived - Chapter 2: A Strong, Growing, and Resilient Economy. Securing Canada’s Research from Foreign Threats https://www.budget.canada.ca/2022/report-rapport/chap2-en.html

145 University of Alberta, Responsible Open Source Due Diligence Protocol, Version 2.0 (July 2025; Approved by PEC-S on January 15, 2025) https://www.ualberta.ca/en/research/media-library/services/2025_07-23_protocol_framework_external.pdf

Research Program の下で、①研究連携・契約（Category A）、②国家安全保障上の懸念ある所属（Category B）、③責任ある研究活動に関する照会・調査支援（Category C）の3類型を明示している。

本プロトコルの特徴は、手順を示すだけでなく、情報の収集・利用・開示・保存・アクセス・廃棄までを包括的に説明している点にある。アルバータ州のプライバシー法等を根拠に、個人情報の収集権限を明示し、目的外利用の制限、開示条件、アクセス制限、保存期間（最低１年）、記録廃棄の考え方を定めている。運用面では、Kharon ClearView や Dimensions Research Security 等のツール利用を認め、単一情報源に依拠しない裏取り（corroboration）、情報の正確性・バイアス評価、必要性・比例性に基づく調査範囲の限定を求めている。類型ごとの承認権限を定め、年１回以上の見直しも明記しており、研究セキュリティ実務を標準化された手続きとして示している。

iii） Alberta Research Security Community of Practice

アルバータ大学における研究セキュリティの特徴的な取組として、学外・州内連携による実務コミュニティ形成が挙げられる。具体的には、アルバータ大学はカルガリー大学（University of Calgary）と共同で、州内の高等教育機関を対象とする Alberta Research Security Community of Practice（CoP）を立ち上げ、運営に関与している。研究セキュリティに関する情報・ベストプラクティスの共有、能力構築支援、州内機関間の実務連携を目的とする枠組みである。

CoP は、2023 年の研究セキュリティ会議および関連ワークショップを契機として形成が進んだ。初期段階にはアルバータ大学とカルガリー大学が、州内の大学・カレッジ向けにデュー・ディリジェンス、リスク評価研修（カルガリー・エドモントン開催）を共同で実施した。2024 年には 2 回の対面ワークショップに延べ 175 名（17 機関）が参加し、2025 年 6 月の年次総会・ワークショップ（カルガリー大学開催）には 20 加盟機関から 64 名が参加し（現在は 22 機関が加盟）[146]、単発の研修活動ではなく、州内の研究セキュリティ実務を支える継続的な能力形成・横展開の場として機能している[147]。運営要領（Terms of Reference）が作成され、月例会合、共有ポータルの設置、対面ワークショップの開催などが継続的に実施されている。[148]

[146] Aug. 11, 2025. “Do you know if your research is secure? Community of practice responds to growing need for awareness” Beatrice Yeung, Faculty of Arts. https://ucalgary.ca/news/do-you-know-if-your-research-secure-community-practice-responds-growing-need-awareness

[147] Progress on UCalgary Research Security Project Objectives – 2023/24 report https://research.ucalgary.ca/sites/default/files/teams/1/RSF-IPG/2023-24-Research-Security-Performance-Objectives-Report.pdf

[148] General Faculties Council Agenda May 8, 2025. https://www.ucalgary.ca/secretariat/sites/default/files/teams/1/GFC/GFC%20Meetings/GFC%20Materials/all-docs-in-one%20GFC%202025-05-08%20-%20for%20post-meeting%20upload.pdf

iv） アルバータ州の研究セキュリティ確保に関する要求への対応

アルバータ大学の研究セキュリティ実務に関する公開文書上、州要件は連邦要件と並んで遵守すべき要件として位置づけられている。Responsible Open Source Due Diligence Protocol では、アルバータ州政府による対中連携に関する方針について、提携先が州方針の対象に該当するかを確認するためにオープンソース・デュー・ディリジェンスを行うこととされている。

v） Podcast（Power Plant Sessions）放送や Research Security Day の開催

アルバータ大学では、SRO による研究セキュリティ実務の整備に加えて、研究者・職員向けの周知と能力構築にも力を入れている。その一つの例が、SRO 制作の podcast “Power Plant Sessions”である[149]。同番組は、研究セキュリティに関する知識・実務能力の向上を、大学内だけでなく州内・全国レベルにも広げることを目的としており、2025 年以降に継続的に配信されている。内容面でも、研究セキュリティと研究インテグリティの接続、研究セキュリティのコミュニティ形成（Communities of Practice）、大学に対する国家的脅威事例（英国事例）など、研究者・大学実務者にとって理解しにくい論点を、他大学の研究セキュリティの実務者等を招き、対話形式で扱う構成となっている。

また、SRO は Research Security Day を開催（毎年開催予定）し、対面・双方向型の周知機会も設けている。2025 年 3 月 21 日に開催された第 1 回 Research Security Day[150]では、専門家講演、情報テーブル、オープンハウス、ブリーフィング・パネル討論などを実施し、100 名を超える参加登録があった[151]。参加者は、アルバータ大学の 5 キャンパスの学生・研究者・事務職員に加え、Alberta Research Security Community of Practice の関係者や、カナダ各地の実務者であり、同大学の周知活動が学内啓発にとどまらず、州内・全国の実務ネットワーク形成にも接続していることがうかがえる。こうした podcast やイベントは、研究セキュリティを規制対応だけでなく、日常的な研究支援・学習機会として定着させるための実践的活動と考えられる。

(c) 特色・注目点等

アルバータ大学における研究セキュリティ確保のための取組については、第一に、連邦政策・州政府方針・学内運用を接続する体制設計が注目される。SRO を中核として、連邦・州の要件への対応支援、デュー・ディリジェンス、相談、研修・アウトリーチのための機能を集約しており、研究セキュリティ対応を研究者任せにしない構造を明確にしている。加えて、カナダ政府側では Budget 2022 以降、RSF を通じた研究セキュリティ能力構築への財政的支援が制度化されており、アルバータ大学も継続的な資金配分を受けている。

---

149 Power Plant Sessions. https://power-plant-sessions.cohostpodcasting.com/
150 Research Security Day 2025. Mar. 21, 2025. https://www.ualberta.ca/en/events/research-innovation/research-security-day-2025.html
151 “Research Security Day 2025” https://www.ualberta.ca/en/research/media-library/services/rs-day-report-external.pdf

第二に、「Responsible Open Source Due Diligence Protocol」にみられるが、リスク判断を実施する上での、法的根拠、個人情報の取扱い、利用・保存、精度検証、比例性、EDI 等を事前に明文化し、学内外に公開することで、研究の開放性と安全性の両立を説明可能な形にしている点に特色がある。これは、カナダ連邦側が示す「as open as possible, as secure as necessary（可能な限り開放、必要な範囲で安全確保）」という原則と整合的であり、大学現場での実装モデルとして評価できる。

第三に、学内周知にとどまらない能力構築（capacity building）の外向き展開の取組も注目点である。カルガリー大学と連携して Alberta Research Security Community of Practice の形成に関与しており、州内機関を横断した研修・共有資源整備・実務者育成を進めている。さらに、SRO によるポッドキャスト（Power Plant Sessions）や Research Security Day の開催を通じて、研究セキュリティを一部の管理部門の業務ではなく、研究者・学生・事務職員が参加する共通課題として可視化している。こうした取組は、制度遵守だけでなく、研究コミュニティの理解と納得を伴う形で運用を定着させるうえで有効とみられる。

(2) マギル大学（McGill University）

(a) 背景・経緯等

マギル大学（McGill University）は、ケベック州モントリオールに拠点を置く研究集約型大学である。国際共同研究を重視してきた一方、近年は外国干渉や研究成果・知的財産の不適切な取得への対応を大学横断課題として位置づけ、研究の開放性と安全性の両立を図る方向で体制整備を進めている[152]。

こうした流れの中で、同大学では 2020 年に学内の「Foreign Interference Workgroup」を設置し、研究者への周知・助言を強化してきた。その後、2023 年 8 月には研究・イノベーション部門内（Innovation + Partnerships）に研究セキュリティ＆コンプライアンス室（Research Security + Compliance Office: RSCO）を設置[153]（4 名の専任体制で発足）し、連邦方針（NSGRP、STRAC 等）への対応、研究リスク評価、学内支援の中核機能を担っている。

[152] Global Research a Team Effort. Meaghan Thurston. 19 May 2022. https://www.mcgill.ca/research/article/global-research-team-effort

[153] Research Security + Compliance Office. https://www.mcgill.ca/research/about/research-security-compliance; McGill boosts research security, compliance, with new office. Junji Nishihata. November 12, 2023 https://healthenews.mcgill.ca/mcgill-boosts-research-security-compliance-with-new-office/

(b) 主な取組

i) 研究セキュリティ特設サイトによる制度・手順の説明

マギル大学は、研究・イノベーション部門のウェブサイトページに「Research Security」セクションを設け[154]、連邦研究セキュリティ政策（STRAC、NSGRP）、FAQ、外部リソース、問い合わせ先、州レベルの要件整理ページ[155]等へアクセスできる構成となっている。また、CFI の研究セキュリティ対応ページ[156]も作成されており、申請時のみならず採択後・事業期間中を通じて研究セキュリティ上の義務が継続すること、ならびに要件・様式の確認先を示している。

ii) 研究費申請オペレーションへの組込み（Research Funding Checklist の eRAP 化）

学内の研究費申請実務では、Research Funding Checklist を 2025 年 3 月 31 日付で eRAP 上のオンライン様式へ移行し、PDF 版を廃止した。加えて、同チェックリストは全ての外部資金による助成・プロジェクト契約に適用されることとなり、研究セキュリティ、利益相反、輸出管理、機微情報取扱い等の確認を、個別案件ベースで申請フローに埋め込む運用となっている。[157]

iii) 研修・啓発リソースの拡充

マギル大学では、研究セキュリティについての啓発・研修活動にも取り組んでいる。具体例として、2022 年には公共安全省の職員を講師として「Safeguarding Science Against Foreign Interference」ワークショップが学内で開催され、外国干渉への対応に関する認識向上が図られたことが大学側の発信で確認できる。[152]

また、学内オンライン教材として「Phishing 101」等が提供されており、動画・クイズ等を用いた継続受講型の形式で、データ保護・フィッシング対策・サイバー衛生に関する基礎的な理解を促す内容となっている。[158]

iv) リスク評価・輸出管理・問い合わせ窓口の整備

RSCO は、研究リスクの同定、リスク緩和の支援を担う組織として位置づけられており、研究者からの照会対応、研究資金関連書類のレビュー、学内の他部門（例：IT、法務等）との連携を通じた実務支援を行う。[153]

輸出管理については、研究セキュリティセクション内に専用ページを設け、カナダ法だけでなく米国輸出管理規制の域外適用にも触れつつ、デュアルユース技術を含む研究実務

---

[154] McGill University “Research Security” https://www.mcgill.ca/research/research/researchsecurity
[155] McGill University “Provincial research security policies” https://www.mcgill.ca/research/research/researchsecurity/provincial-research-security-policies
[156] McGill University “Canada Foundation for Innovation (CFI) approach to research security” https://www.mcgill.ca/research/research/researchsecurity/cfi-approach-research-security
[157] McGill University “Forms and Resources” https://www.mcgill.ca/research/research/forms-resources
[158] McGill University “Cybersecurity Essentials Training” https://www.mcgill.ca/cybersafe/training-and-resources/cybersecurity-essentials-training

上の留意点を説明している。問い合わせ先メールアドレスも明示されており、研究者が案件ごとに事前相談可能としている。[159]

(c) 特色・注目点等

マギル大学の特徴は、①連邦制度（NSGRP、STRAC）への適合を、単なる申請時の書類対応にとどめず、学内の申請フロー（Research Funding Checklist/eRAP）へ組み込んでいる点、②研究セキュリティを RSCO の専管機能として明確化しつつ、IT・法務・研究支援等との連携で運用している点である。

(3) トロント大学（University of Toronto）

(a) 背景・経緯等

トロント大学（University of Toronto）では、研究の国際性・開放性を維持しつつ、連邦政府の研究セキュリティ要件（NSGRP、STRAC）およびオンタリオ州の研究資金要件に対応するため、学内の研究支援サイト（Safeguarding Research）[160]に、制度別の実務ガイダンスを示している。研究者が研究提案書の応募先機関（NSGRP[161]、STRAC[162]、オンタリオ州[163]）に応じて必要な手続を確認できる構成になっている。

(b) 主な取組

i) 連邦要件（NSGRP、STRAC）の学内実装と研究者支援

上記のように、トロント大学は、STRAC および NSGRP それぞれについて専用ページを設け、研究者が申請前に確認すべき事項（適用有無の判定、提出フォーム、継続的義務）を明確化している。STRAC では、研究者の attestation 提出、研究チーム変更時・研究内容変更時の通知義務、助成期間中の継続遵守などを整理し、NSGRP では、リスク評価フォームと軽減計画の作成・実施を案内している。

そのうえで、研究イノベーション担当副学長室（Office of the Vice-President, Research & Innovation: OVPRI）の研究セキュリティチーム（Research Security Team）が、

---

159 McGill University “Export Controls” https://www.mcgill.ca/research/research/researchsecurity/export-controls
160 University of Toronto. ”Research Security: Safeguarding Research“ https://research.utoronto.ca/safeguarding-research/research-security-safeguarding-research
161 University of Toronto. “National Security Guidelines for Research Partnerships (NSGRP) – Federal Programs” https://research.utoronto.ca/safeguarding-research/national-security-guidelines-research-partnerships-nsgrp-federal-programs
162 University of Toronto. “Sensitive Technology Research and Affiliations of Concern (STRAC) Policy – Federal” https://research.utoronto.ca/safeguarding-research/new-requirements-STRAC
163 University of Toronto. ”Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects - Government of Ontario” https://research.utoronto.ca/safeguarding-research/mitigating-economic-andor-geopolitical-risks-sensitive-research-projects

attestation やリスク評価、パートナー審査に関する相談窓口として明示されており[160]、研究者個人に課される要件を、学内の支援体制で補完する運用になっている。

ii) 国際共同研究の事前審査（RPSID）とパートナー・デュー・ディリジェンス

トロント大学のウェブサイトページ「Minimize Risk When Establishing Partnerships」[164]では、外部パートナーとの連携前に、公開情報を用いたオープンソース・デュー・ディリジェンスや、制裁リスト・STRA/NRO 該当性の確認等を行うよう研究者に促している。国際研究パートナーシップについては、具体案件に進む前に「Research Partnership Security Information Document for International Partnerships（RPSID)」ツールを用いて、相手先の適格性・潜在リスクの評価を支援する運用となっている。

同ページは、研究セキュリティ観点の相談先として研究セキュリティチーム、国際連携設計・協定面の相談先として国際担当副学長室（Office of the Vice-President, International）やイノベーション連携室（Innovations & Partnerships Office）を示している。

iii) 州要件（オンタリオ州）への対応

大学ウェブサイトページで、州の対象研究資金プログラム、必須フォーム（Application Attestation Form、Mitigating Economic and Geopolitical Risk Checklist)、および高リスク案件に対する追加の Risk Mitigation Form 対応を、研究者向けに説明している。特に、州審査で懸念が示された場合に、大学側（研究セキュリティチーム・OVPRI）が研究者・部局と連携してリスク軽減フォームを作成し、州へ提出する流れを明示している。[163]

iv) TAHSN 等との実務ツールの共有

トロント大学の研究セキュリティ確保の取組は、学内に閉じたものではなく、トロント学術医療科学ネットワーク（Toronto Academic Health Science Network: TAHSN）の実務ガイド（国際共同研究・パートナーシップの研究セキュリティ指針）[165]と関係している。TAHSN のガイドでは、連邦・州要件を補完する目的が明示され、トロント大学の RPSID や「Minimize Risk」ページ等が参照先として挙げられている。

(c)　特色・注目点等

トロント大学の研究セキュリティ確保の取組の特色・注目点としては、国際共同研究の入口段階に「Research Partnership Security Information Document for International Partnerships（RPSID)」ツールを置いている点である。申請時のフォーム対応だけでな

164 University of Toronto. “Minimize Risk When Establishing Partnerships” https://research.utoronto.ca/safeguarding-research/minimize-risk-when-establishing-partnerships
165 General Guidelines for the Process of Mitigating Security Risk in Research across TAHSN. https://tahsn.ca/sites/default/files/assets/files/tahsn-rps-wg-guidelines.pdf

く、提携形成前のデュー・ディリジェンスをルーチン化することで、後段の資金審査・契約・知財管理とも接続しやすい構造になっている。

2.2.3　資金配分機関等における取組

カナダの研究セキュリティ政策は、研究者、大学・研究機関、資金配分機関、政府の間での「責任の共有」（shared responsibility）として設計されており、CIHR、NSERC、SSHRC の 3 資金配分機関（Tri-Agency）に加えて CFI も、政府の研究セキュリティ関連方針を実装する主体として位置づけられている[166]。

NSGRP については、資金配分機関（主として Tri-Agency、CFI も同枠組みの実装対象）は、対象助成におけるリスク審査プロセスを運用することが求められる[167]。NSGRP の Tri-Agency ガイダンスによれば、資金配分機関は、申請者に対して Risk Assessment Form と必要に応じてリスク軽減計画の提出を義務づけ、提出された様式について、①様式の完全性確認（記載が全て埋まっているか）、②オープンソースインテリジェンス（OSINT）によるリスク検証、③必要時の内部委員会（リスク評価委員会（Risk Assessment Committee））での審査、④必要に応じ、公共安全省の Research Security Centre（RSC）への照会、⑤その結果を踏まえた資金配分判断、という一連の審査プロセスを、メリット審査（学術的審査）と分離して実施する[168]。

STRAC については、資金配分機関は、対象公募において機微技術研究領域（STRA）と指名研究機関（NRO）の組合せを資金配分段階で判定し、排除する運用が求められる。すなわち、Tri-Agency ガイダンス[169]によれば、STRA を前進させる研究について、研究チームに NRO との所属、資金・現物支援関係がある場合は、Tri agency および CFI に提出された申請は資金供与しない。また、資金配分機関には、対象公募の範囲設定、attestation 提出要件の運用、採択案件の一部に対する事後的なランダム検証（validation）を実施する役割が課されている。

州レベルでは、州ごとに制度差があるが、オンタリオ州は州の研究資金プログラム向けに独自の Research Security Guidelines を策定しており、同ガイドラインは連邦 Tri-Council の要件・プロセスとは「別個・独立」（separate and distinct）であることを明示している[170]。オンタリオ州の研究資金配分当局は、州独自の審査基準・審査実務を運用する責務がある。

---

166 Tri-agency guidance on research security　https://nserc-crsng.canada.ca/en/funding/research-partnerships-and-collaborations/inter-agency/tri-agency-guidance-research-security
167 Tri-agency guidance on the National Security Guidelines for Research Partnerships (NSGRP) https://nserc-crsng.canada.ca/en/funding/research-partnerships-and-collaborations/inter-agency/research-security/tri-agency-guidance
168 Ibid.
169 Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)　https://nserc-crsng.canada.ca/en/funding/research-partnerships-and-collaborations/inter-agency/research-security/tri-agency-0
170 Ontario Ministry of Colleges and Universities. Research Security Guidelines for Ontario Research Funding Programs　https://forms.mgcs.gov.on.ca/dataset/875d7629-9ddc-4545-a1c3-881ece0cb3a3/resource/6219fff3-aa2e-49ae-955c-0ebbd21059f1/download/on00708e.pdf

(1) 自然科学・工学研究会議（Natural Sciences and Engineering Research Council of Canada）

自然科学・工学研究会議（NSERC）は自然科学・工学分野の資金配分機関であり、年間資金配分規模（2024 年度）は約 14 億カナダドルである[171]。

カナダは研究セキュリティを Tri-agency の枠組みで実装しており、NSERC はその中核として申請審査にリスクアセスメントを組み込んでいる。NSGRP、STRAC が適用される。必要に応じ申請は公共安全省で国家安全保障レビューに付され、助成可否・緩和条件に反映される。

(a) 背景・経緯等

カナダにおける研究セキュリティ施策は、連邦政府が 2021 年 3 月の「Research Security Policy Statement」において、研究環境の開放性を維持しつつ、外国からの干渉・知財流出等への警戒を明確化し、政府・大学・研究者の協働による対策強化を打ち出したことを起点として具体化が進んだ[172]。政府は大学とのワーキンググループに対し、研究パートナーシップの審査・資金配分に国家安全保障上の観点を組み込むためのガイドライン策定を要請し、連邦研究資金配分機関の運用見直しも進める方針を示した。

この流れを受けて、NSERC を含む連邦資金配分機関は、2021 年 7 月導入の NSGRP の実装を進め、研究パートナーシップ助成におけるリスク評価・緩和措置を制度化した。三資金配分機関の NSGRP ガイダンス[173]では、NSGRP を「as open as possible, as secure as necessary（可能な限り開放、必要な範囲で安全確保）」という考え方のもとで、研究者・大学・資金配分機関が一体で行うリスクベースのデュー・ディリジェンス枠組みとして位置づけている。

さらに、2023 年 2 月の連邦政府発表（研究セキュリティの強化姿勢）を経て、2024 年 1 月には STRAC が公表され、同年 5 月 1 日以降に開始する対象公募から、三資金配分機関および CFI で調和的に実装されることとなった。NSERC の STRAC ガイダンス[174]は、研究者の所属・資金関係（NRO との関係）と、STRA を組み合わせた新たな適格性・遵守要件を明確化している。

---

171 “2024–25 Departmental results report” https://nserc-crsng.canada.ca/en/plans-priorities-and-performance/2024-25-departmental-results-report/2024-25-departmental-results

172 Innovation, Science and Economic Development Canada. Research Security Policy Statement – Spring 2021. https://www.canada.ca/en/innovation-science-economic-development/news/2021/03/research-security-policy-statement--spring-2021.html

173 Tri-agency guidance on the National Security Guidelines for Research Partnerships (NSGRP) https://nserc-crsng.canada.ca/en/funding/research-partnerships-and-collaborations/inter-agency/research-security/tri-agency-guidance

174 Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy) https://nserc-crsng.canada.ca/en/funding/research-partnerships-and-collaborations/inter-agency/research-security/tri-agency-0

(b) 主な取組

i) NSGRP の実装（研究パートナーシップ型助成におけるリスク評価・緩和）

NSERC における NSGRP 実装の中核は、民間（private sector）パートナーを含む対象助成への申請時に、リスク評価フォーム（Risk Assessment Form）提出を必須化し、申請者に対してリスク評価とリスク軽減計画（mitigation plan）の作成を求める点にある。Tri agency ガイダンスでは、当該フォームは申請書の一部として扱われ、軽減策は助成期間を通じて実施すべきものとされる。

対象範囲については、NSGRP は選択された研究パートナーシップ型プログラムに適用される仕組みであり、NSERC 関係では Alliance grants や Idea to Innovation（Phase II）が明示されている。NSERC は自然科学・工学分野の産学連携助成を中心に、研究セキュリティ審査を運用に組み込む役割を担っている。

運用面では、NSERC を含む資金配分機関は、提出された Risk Assessment Form を用いて、メリット審査（学術的評価）とは独立したリスク審査プロセスを実施する（国家安全保障上の追加評価が必要な場合には公共安全省への照会）。

採択後も、申請時に提示した軽減策（および通知書で求められた措置）の実装は助成条件として扱われ、通常の報告プロセスの中で実施状況の確認が求められる。この点は、NSERC の実装が申請時のチェックにとどまらず、助成期間中の継続的な管理を前提としていることを示している。

ii) STRAC の実装（機微技術と懸念組織との関係の審査）

STRAC について、NSERC の Tri agency ガイダンスは、STRA を前進させる研究を対象に、研究者の NRO との関係を確認する仕組みを定めている。対象研究で、助成対象活動に関与する研究者が NRO との現時点の所属または資金・現物支援関係を有する場合、当該申請は資金供与されない。これは、研究テーマ（技術領域）と研究者の関係性（所属・支援元）を組み合わせて適格性を判断する設計である[175]。

申請時の実務は、概ね二段階で整理されている。第一に、申請者は自らの研究が STRA を「前進（advance）」させるか否かを判定し、申請書上で明示する。第二に、STRA 該当（Yes）の場合、申請書上の named roles（申請者、共同申請者、collaborator 等）に該当する研究者が、各自 Attestation Form を提出する。採択後は、研究の性質変化や研究チーム構成変更時の通知・対応を含め、助成期間を通じた遵守が求められる。

大学・研究機関の役割については、NSERC ガイダンス上、研究助成担当（Research Grant Officers）が、研究者への周知、必要書類の completeness check（形式的な提出確認）、助成期間中の変更連絡の橋渡し等を担う一方、Attestation の内容の真偽そのものを検証する責任までは負わない。検証（validation）は資金配分機関側が担い、ランダム抽出、NSGRP 案件との並行検証、アドホック検証等の複線的な運用が設けられている。

---

[175] Ibid.

NSERC における STRAC の適用範囲も比較的広く、NSERC ガイダンスでは、Alliance grants、Idea to Innovation、Discovery Grants（補助含む）、DND/NSERC Discovery Grant Supplements、Discovery Horizons、Research Tools and Instruments 等が、対象公募として列挙されている[176]。STRAC は産学連携系のみならず、基盤的・競争的研究助成の一部にも実装される枠組みとなっている。

(c) 特色・注目点等

NSERC の研究セキュリティ実装の特色は、第一に、NSGRP（研究パートナーシップのリスク評価）と STRAC（機微技術と懸念組織の適格性管理）という二つの仕組みを、相互補完的に運用している点にある。

第二に、役割分担の設計が比較的明確である点が注目される。研究者は自己申告・フォーム提出・継続遵守の一次的責任を負い、大学・研究機関は主として支援・形式確認・連絡調整を担い、資金配分機関（NSERC 等）は独立した審査・検証プロセスを運用する。審査・検証プロセスでは必要に応じて、政府の公共安全省の支援を受ける。この設計は、大学側に過度な実体審査責任を負わせず、他方で資金配分段階での統一的な管理を確保する仕組みとなっている。

第三に、開放性・学術的自由との両立を前面に出した実装である。NSERC の Tri agency ガイダンスは、研究セキュリティを「オープンサイエンス」「学術的自由」「差別の禁止」「機関の自律性」と両立させる原則の下で位置づけており、NSGRP や STRAC においても、メリット審査との分離、差別・プロファイリングの禁止、透明な手続・FAQ を充実させることなどを通じて、研究者コミュニティの予見可能性を高める設計が採られている。

(2) カナダ・イノベーション基金（Canada Foundation for Innovation）

カナダ・イノベーション基金（CFI）は、カナダの大学・カレッジ・研究病院・非営利研究機関における研究インフラ（設備・施設等）への投資を担う資金配分機関であり、研究費（運営費）中心の Tri-agency（NSERC、SSHRC、CIHR）とは、資金配分の対象・審査実務が異なる。Tri agency では研究者が申請者であるのに対して、CFI の公募助成では大学等の機関が申請者である。CFI は 1997 年以降、研究インフラ整備を通じて研究基盤の強化を担ってきた[177]。年間資金配分規模（2023 年度）は約 3.8 億カナダドルである[178]。

176 Ibid.
177 Canada Foundation for Innovation “About us” https://www.innovation.ca/about
178 “2024–25 Departmental Plan: Supplementary information” https://ised-isde.canada.ca/site/planning-performance-reporting/en/departmental-plans/2024-25-departmental-plan-supplementary-information

(a) 背景・経緯等

CFI において、近年の連邦政府の研究セキュリティ政策に対応し、研究セキュリティ要件（NSGRP と STRAC）の実装が求められるようになった[179,180]。

また、2025 年には Tri-agency の STRAC 実装ガイダンスが更新され、研究者・機関・資金配分機関の役割分担を明確化しつつ、CFI についても専用ガイダンスを参照すべきことが示されている。CFI は研究インフラ助成の申請・審査・採択後管理の各段階に研究セキュリティ要件を組み込む運用を整備している。

(b) 主な取組

i) NSGRP 対応と「研究セキュリティ＋知的財産」枠組みの整理

CFI では、民間パートナーを伴う案件に関する研究セキュリティ対応（NSGRP）が実装対象となっている。CFI 申請において研究セキュリティ設問への回答結果に応じて、民間パートナー関連様式（Private-Sector Partner Identification Form）等の提出が必要となる[181]。これは、CFI が研究インフラ助成であっても、研究パートナーシップ由来のリスクを申請段階で把握・管理しようとしていることを示す。

ii) STRAC の制度実装

CFI の実装において中核となるのが、STRAC 対応である。連邦の統一方針上、STRA を前進させる場合、研究チームの関係者に NRO との該当関係があると資金供与対象外となる（不交付）という枠組みが適用される。これは Tri-agency だけでなく、CFI を含む連邦資金配分機関に共通する考え方である。

iii) CAMS（CFI Awards Management System）への組込みによる運用実装

CFI の特徴は、上記の研究セキュリティ要件を CAMS（CFI アワードマネジメントシステム）上の申請プロセスに組み込んでいる点である。CFI の研究セキュリティについての説明では、研究セキュリティ関連様式を CAMS で提出する仕組みが示されている。[182]

また、CFI の CAMS 利用ガイドや公募書類（Innovation Fund[183]等）では、研究セキュリティ・モジュールが申請フォーム内に実装され、回答内容に応じて必要書類（STRAC アテステーション、リスク評価関連資料等）を提出する運用が示されている。つまり、

---

179 Canada Foundation for Innovation “Research Security” https://www.innovation.ca/apply-manage-awards/resources-apply-manage-award/research-security
180 Tri-agency guidance on the National Security Guidelines for Research Partnerships (NSGRP); Tri-agency guidance on the Policy on Sensitive Technology Research and Affiliations of Concern (STRAC Policy)
181 University of British Columbia. “Before you apply” https://ipo.ubc.ca/before-you-apply
182 Canada Foundation for Innovation “Research Security”
183 Canada Foundation for Innovation “Innovation Fund” https://www.innovation.ca/apply-manage-awards/funding-opportunities/innovation-fund

CFI は研究セキュリティ要件を申請システムそのもののワークフローとして実装している。

(c) 特色・注目点等

CFI における実装の特色は、研究セキュリティ要件を CAMS（CFI アワードマネジメントシステム）上の申請プロセスに組み込んでいる点である。研究インフラ資金配分機関としての性格に即して、大学等の機関申請者からの申請・管理実務に研究セキュリティ要件を埋め込んでいる。この点が、研究者中心の申請プロセスである NSERC とは異なる。CFI では CAMS を通じた機関側の申請統制・確認実務が相対的に重要となっているのである。

2.2.4 まとめ

(1) 大学・研究機関

調査対象としたカナダの 3 大学の事例（アルバータ大学、マギル大学、トロント大学）からは、各大学が同じ連邦制度に対応しながらも、大学の規模、既存の研究支援体制の違いに応じて、実装方法を工夫していることが確認できる。また、アルバータ大学はアルバータ州、マギル大学はケベック州、トロント大学はオンタリオ州にあるが、州政府の研究資金受領について州ごとに研究セキュリティ面の要件が異なることへの対応もカナダでは求められている。

事例調査の結果と示唆をまとめると以下のとおりである。

第一に、カナダでは、連邦政府が研究セキュリティ要件を課すだけでなく、大学の実装能力（人員、運用、研修、リスク評価体制）向上のための政府資金（Research Support Fund）を配分している。ガイドライン・様式整備に加え、大学の事務・支援部門の能力構築に使える恒常的財源支援であり、各大学における取組が積極的に進められている特徴がある。

第二に、研究者本人に申告・アテステーションの責任を置きつつ、大学は適用判定の支援、手続支援、相談、必要時調査を担う、という役割分担が比較的明確であった。

第三に、申請時対応だけでなく、連携形成前のデュー・ディリジェンスについて、トロント大学の RPSID、アルバータ大学の OSINT プロトコルは、いずれも応募直前ではなく、連携形成の前段階で確認を始めるとされている。共同研究契約・MOU・受入れ・知財協議の前に使える簡易な事前確認ツールの標準化により審査期間の短縮などに効果があると考えられる。

第四に、アルバータ大学の Podcast や Research Security Day、マギル大学の研修・教材では、研究セキュリティを継続的な学習・対話の場として運用していた。研究者・URA・事務職員が同じ土俵で学べる設計としていたことが特徴的であった。

第五に、アルバータ大学とカルガリー大学による Community of Practice（CoP）は、大学ごとの試行錯誤を共有資産に変える仕組みを構築していた。各大学が個別に悩むのではなく、地域ブロックや大学群、研究支援ネットワーク単位で、様式・FAQ・事例・研修を共同化する枠組みは特に、中小規模大学の実装力を底上げする効果があると考えられる。

(2) 資金配分機関

カナダの研究セキュリティ政策は、連邦レベルにおいて、研究者、大学、資金配分機関、政府の「責任の共有」（Shared Responsibility）として設計されている。この枠組みにおいて、資金配分機関は研究セキュリティ審査の運用、基準の適用、そして研究者や大学との連携を含む実施責任を負う主体として位置づけられている。

カナダの連邦資金配分機関である三機関（Tri-Agency：CIHR、NSERC、SSHRC）とカナダ・イノベーション基金（CFI）は、いずれも政府の研究セキュリティ関連方針を実装する主体である。Tri-Agency は主に研究費を支援するのに対し、CFI は研究インフラ（設備・施設等）への投資を担うという特徴を有する。共通の基盤として、民間パートナーとの連携に伴うリスクを評価する NSGRP と、機密技術研究における懸念組織との関係を管理する STRAC が、両機関の運用に組み込まれている。

事例調査の結果と示唆をまとめると以下のとおりである。

第一に、大学等職員の責任を形式確認に限定し、実体的な検証責任は資金配分機関が負うという明確な境界がある設計は、大学側の事務負担を適正化し、研究推進を阻害しないために有効であると考えられる。

第二に、カナダ政府は、公共安全省の下に「研究セキュリティセンター（RSC）」を設置し、NSERC 等の資金配分機関に対する専門的な助言提供体制を構築している。研究者や大学が直接政府の公共安全省とやり取りするのではなく、より高度な国家安全保障上の判断を要する案件については、資金配分機関が、公共安全省の RSC に照会を行い、追加的な評価を依頼する仕組みとなっている。

第三に、全ての案件のリスク判断を公共安全省に委ねるのではなく、資金配分機関がまず OSINT 等の公開情報を活用して行政的な検証を行うことで、政府の情報機関のリソースを真に機微な案件に集中させている。どの段階で、どのような情報を当局と共有し、その助言をどう配分判断に用いるのかがガイドラインで透明化されていることが、制度の受容性を高めていると考えられる。

【カナダの研究セキュリティ関連の公表文書（2025 年 3 月～2026 年 2 月）】

(a) 連邦政府機関等

Public Safety Canada. Evaluation of the Funding to Build Canada's Research Security Capacity（2025年7月4日）

[184]

本報告書「研究セキュリティ能力構築資金に関する評価」は、公共安全省（Public Safety Canada）がプログラム評価報告書（対象期間：2022–23年度～2023–24年度）として、連邦予算2022で創設された「Research Security Centre（RSC）」および関連資金（5年間1,260万ドル＋その後恒常的経費）のパフォーマンスを、財務・成果の両面から評価するために作成された。

Government of Canada. Research Security Notional Amounts / Funding Awarded in 2025-26（2025 年 8 月 20 日）、Research Security Funding Awarded in 2025-26（2025 年 10 月 22 日）[185]

連邦予算 2022 において、研究セキュリティ関連の間接経費を支援するため、Research Support Fund（RSF）に「研究セキュリティ」を第 5 の重点分野として位置づけ、5 年間で 1 億 2,500 万ドル、以後恒常的に年間 2,500 万ドルを配分することが決定された。RSF の研究セキュリティ枠は、年間 200 万ドル以上の RSF 対象研究費を受け取る大学・研究機関に対して、研究セキュリティ体制の構築・強化（専任人材、トレーニング、リスクアセスメント体制など）に必要なコストを支援することを目的としている。

「Research Security notional amounts for 2025-26」（2025 年 8 月）は、各機関が 2025–26 年度に受け取り得る研究セキュリティ資金の見込額（ノーティナル額）を一覧表で公表したものである。トロント大学、UBC、マギル大学、マクマスター大学など大規模研究大学には数十万～数百万ドル規模の配分が示されており、地方大学や規模の小さい大学には数万ドルから十数万ドル程度の配分が示されている。これにより各大学は、翌年度に向けた研究セキュリティ体制（人件費・システム整備・研修等）の計画を立てる際の財政見通しを把握できるようになっている。

「Research Security Funding Awarded in 2025-26」（2025 年 10 月）は、実際に承認・支給された金額を機関別に示すもので、ノーティナル額との差異（申請内容や報告状況による調整）を含めた最終的な配分結果を示している。

---

[184] Public Safety Canada. Evaluation of the Funding to Build Canada's Research Security Capacity. July 2025.
https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/vltn-fndng-bld-cnds-rsrch-scrty-cpcty/index-en.aspx

[185] https://www.rsf-fsr.gc.ca/apply-demande/research_security-securite-recherche-eng.aspx#8
Research Security notional amounts for 2025-26（ノーティナル額：2025 年 8 月 20 日）
https://www.rsf-fsr.gc.ca/apply-demande/grants-subventions/rs2025-eng.aspx
Research Security Funding Awarded in 2025-26（実際の支給額：2025 年 10 月 22 日）
https://www.rsf-fsr.gc.ca/apply-demande/notional/research_security-2025-eng.aspx

Government of Canada. Annual Report on the Implementation of Research Security Policies within the Federal Granting Agencies and the Canada Foundation for Innovation 2023-2024（2025年10月29日）[186]

本年次報告書は、カナダ連邦政府が連邦研究資金配分機関（三機関：CIHR・NSERC・SSHRC）およびCFIにおいて実施している研究セキュリティ政策の運用状況を整理したものであり、特にNSGRPの実施結果と、それを支える取組を中心に取りまとめている。

(b) 州政府

オンタリオ州. Bill 33, Supporting Children and Students Act, 2025（2025年11月20日）[187]

Bill 33は、オンタリオ州内の公的支援大学（publicly-assisted universities）と応用芸術・技術カレッジ（colleges of applied arts and technology）を対象に、各機関が研究セキュリティ計画（research security plan）を策定し実装することを求める。

(c) ナショナルアカデミー

CCA (Council of Canadian Academies). (2025). Balancing Research Security and Open Science.（2025年10月21日）[188]

本報告書は、カナダの研究エコシステムが重視してきたオープンサイエンス（開放性）と、近年強まる研究セキュリティ（悪用・不正流出・外部干渉等への備え）の緊張関係を、「守るべき研究」と「開くべき研究」を二者択一にしない形で整理し、“sensitive research of concern（懸念を要するセンシティブ研究）”をどう同定し、研究ライフサイクル全体でどう保護するかを、利用可能なエビデンスに基づいて検討した。

186 Government of Canada. Annual Report on the Implementation of Research Security Policies within the Federal Granting Agencies and the Canada Foundation for Innovation 2023-2024 https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/additional-resources/annual-reports/annual-report-2023-2024

187 Bill 33, Supporting Children and Students Act, 2025. Legislative Assembly of Ontario. 新設の 20.1 条 “Research security plan” https://www.ontario.ca/laws/statute/s25012

188 CCA (Council of Canadian Academies). (2025). Balancing Research Security and Open Science. Ottawa, ON: Expert Panel on Sensitive Research of Concern, CCA. https://doi.org/10.60870/fmt9-9559.

(d) その他調査機関等

Council of Ontario Universities. A Shared Commitment by Universities to Protect Ontario's Research（2025 年 6 月）[189]

本書は、オンタリオ州の大学が、研究の国際性（開放性、共同研究、EDI＝公平性・多様性・包摂）を維持しつつ、機会損失・知財流出・研究の悪用を防ぐための「合理的でリスクベース」の研究セキュリティ実装を、大学セクターとして共通フレームに落とし込んだ実務ガイドである。

[189] Council of Ontario Universities. A Shared Commitment by Universities to Protect Ontario's Research. June 2025. https://ontariosuniversities.ca/wp-content/uploads/Research-Security-Booklet-June-2025-Final.pdf

2.3　英国

2.3.1　研究セキュリティ・インテグリティ関連政策動向

(1)　2024 年までの経緯

英国は、世界中から投資を集める活気ある研究・イノベーションセクターを有しており、英国の研究成果の半数以上は国際的なパートナーシップによって生み出されている[190]。このような状況を踏まえて、2019 年 9 月に、英国政府の国家安全保障機関である国家防護安全保障局（National Protective Security Authority: NPSA）が、「Trusted Research」というキャンペーンを全国展開した[191]。

Trusted Research は、英国が築いてきた研究・イノベーションセクターの成功を維持・向上させるため、英国の大学・研究機関が、国際共同研究に関して十分な情報を得た上で意思決定を行い、その際に自国の研究者および学術的価値を保護できるよう支援することを目的としたイニシアチィブである。NPSA はこの一環として、大学・教育機関向けに、研究セキュリティに関する理解を促すためのガイダンスとして、Trusted Research Guidance for Academia を公表[192]した。

図 2-3 に、Trusted Research を推進する関係機関および Trusted Research における機関間の関係を示す。表 2-5 に、2024 年までに発行された Trusted Research に関する主な公的文書を示す。

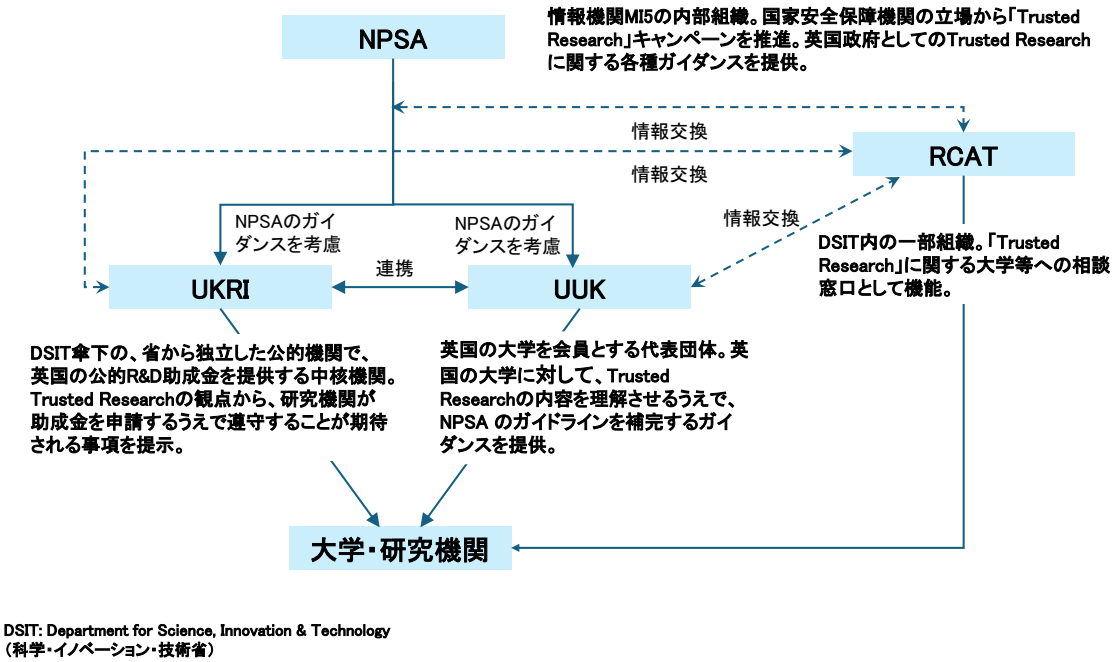


図 2-7　Trusted Research を推進する関係機関および Trusted Research における機関間の関係

190 Trusted Research Guidance for Academia. https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-academia
191 Trusted Research. https://www.npsa.gov.uk/specialised-guidance/trusted-research
192 Trusted Research Guidance for Academia. https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-academia

表 2-5　2024 年までに発行された Trusted Research に関する主な公的文書

発行年月	文書名	発行元
2019 年 9 月	Trusted Research Guidance for Academia	National Protective Security Authority（NPSA）
2020 年 10 月	Managing risks in Internationalisation: Security related issues	Universities UK (UUK)
2021 年 3 月	Export controls applying to academic research	Export Control Joint Unit and Department for International Trade
2021 年 6 月	National Security and Investment Act: guidance for the higher education and research-intensive sectors	Department for Business, Energy & Industrial Strategy (BEIS)
2021 年 8 月	Trusted Research and Innovation Principles	UKRI
2022 年 6 月	Managing risks in international research and innovation: An overview of higher education sector guidance	UUK / UKRI / NPSA
2024 年 1 月	Implementation – collaboration checklist: Evaluating research proposals	NPSA
2024 年 3 月	Evaluation Framework	NPSA
2024 年 5 月	National Security and Investment Act: guidance for the higher education and research-intensive sectors（更新）	Cabinet Office

2020 年 10 月、英国大学協会（Universities UK: UUK）は、NPSA の「Trusted Research」キャンペーンを踏まえて、英国の大学に対して、Trusted Research の内容を理解させるうえで、NPSA のガイドラインである「Trusted Research Guidance for Academia」を補完することを目的としたガイドラインである「Managing risks in Internationalisation: Security related issues」を公表[193]した。

2021 年 6 月、「Trusted Research」に対応して、英国の国家安全保障を脅かす可能性のある産業等に対する出資を規制することを目的とした国家安全保障・投資法（National Security and Investment Act: NSI 法）[194,195]が制定された。2022 年 1 月に、英国政府は、大学等の研究機関における NSI 法の適用ルールを提示したガイドライン「National Security and Investment Act: guidance for the higher education and research-intensive sectors」を公表（2024 年 5 月更新）[196]した。

[193] Universities UK, “Managing risks in Internationalisation: Security related issues,” October, 2020. https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation

[194] 取得者の国籍を問わず、英国政府が審査・介入できる制度である。一定要件の下、17 の機微分野に関する特定の取得は政府への事前届出が義務付けられる。

[195] National Security and Investment Act 2021. https://www.legislation.gov.uk/ukpga/2021/25/contents

[196] National Security and Investment Act: guidance for the higher education and research-intensive sectors. https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors

英国政府は、こうした動きに並行して、2021 年 5 月、「Trusted Research」を踏まえて、大学・研究機関に対して、国際的な研究に関連する国家安全保障上のリスクに関する公的なアドバイスを提供する最初の窓口となる組織（法的権限は無い）として、Research Collaboration Advice Team (RCAT)[197]を設立した。

一方、英国の R&D 資金配分機関である英国研究・イノベーション機構（UK Research and Innovation: UKRI）は、Trusted Research に基づき、国際共同研究のデュー・ディリジェンスに関して、UKRI のファンディングを受ける機関への要求事項（原則）を定めた文書である、「Trusted Research and Innovation Principles」を、2021 年 8 月に公表[198]した。UKRI から資金提供を受けている組織は、同文書に示された原則を採用し、これらの原則に合致する管理および対策を実施したことを証明できるようにすることが必要になった。

NPSA、UUK および UKRI の 3 機関は、大学が国際的な研究・技術革新におけるセキュリティリスクを管理するために、既存ガイドラインをどのように導入すればよいかを示すことを目的として、これまでこれらの機関が作成したガイドラインや主要原則をハイレベルでまとめたガイダンスである「Managing risks in international research and innovation: An overview of higher education sector guidance」[199]を、2022 年 6 月に共同で公表した。

NPSA は、2024 年 1 月に、研究者および研究支援部門が、共同研究に伴うリスクのレベルを判断する際に利用することができるチェックリストである「Implementation – collaboration checklist: Evaluating research proposals」[200]を公表した。この文書は、共同研究開始時に、研究者と研究支援部門が役割分担しつつ、共同研究に伴うリスクを俯瞰的に点検するための実務ツールである。これは、チェックリストを用いることで、①軽減が必要なリスクの特定、②遵守すべき法的義務の特定、③機関内の承認プロセスへのエスカレーションの要否、④ 機関を規律する方針や機関の価値観との整合性、⑤資金配分機関を含む既存の提携関係および遵守すべき契約上の義務、といった観点から検討を進めることを支援することを狙いとしたものである。

また、NPSA は、2024 年 3 月に、大学・研究機関が自機関の研究セキュリティに取組む体制・実践状況を自己評価し、改善に結び付けることを目的とした成熟度自己診断ツール「Evaluation Framework」[201] を公表した。これは、大学が自らの研究セキュリティの成熟度を自己評価することを支援する枠組みであり、評価領域として以下の 7 項目を提示した。

---

197 RCAT. https://www.gov.uk/government/organisations/research-collaboration-advice-team
198 UKRI, “UK Research and Innovation: Trusted Research and Innovation Principles,” August 2021. https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf
199 UUK/NPSA/UKRI, “Managing risks in international research and innovation: An overview of higher education sector guidance,” June 2022. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf
200 NPSA, “Implementation – collaboration checklist: Evaluating research proposals,” January 2024. https://www.npsa.gov.uk/system/files/npsa_tr_checklist_final_web.pdf
201 NPSA, “Evaluation Framework,” March 2024. https://www.npsa.gov.uk/resources/tr-evaluation-framework

- 上級管理者の関与とガバナンス
- コミュニケーション（周知・発信）
- 研修
- 機関としてのリスクと共同研究の管理
- 人・プロセス・ガイダンス（高リスクの共同研究に関する懸念・事案の記録及び報告プロセス、リスク発生時の対応、デュー・ディリジェンスのレビュー・プロセス、職員の入職・離職時の手続き等）
- データ・デバイスの管理
- 影響度の測定（理事会等での議論・意思決定の証跡（議事録等）、高リスクの共同研究の内部判断プロセスへの付議とリスク登録簿、RCAT 等の監督機関との関与記録、輸出管理ライセンス申請やエンドユーザーチェックの実施・記録等）

(2) 最近の主な動き

表 2-6 は、2025 年以降に発行・更新された Trusted Research に関する主な政府の公的文書である。

表 2-6 2025 年以降に発行・更新された Trusted Research に関する主な公的文書

発行年月	文書名	発行元
2025 年 6 月	UKRI Trusted Research & Innovation Principles and Expectations	UKRI
2025 年 7 月	Trusted Research Guidance for Academics（更新）	NPSA
2025 年 7 月	Trusted Research Guidance for Senior Leaders（更新）	NPSA
2025 年 7 月	Trusted Research Countries and Conferences Guidance（更新）	NPSA

以下、上記した3つのNPSA文書の概要を示す。なお、UKRIの文書「UKRI Trusted Research & Innovation Principles and Expectations」[202]の概要について、2.2.3「資金配分機関等における取組」で説明する。

Trusted Researchは、英国の研究・イノベーションセクターの持続的な成功に不可欠な国際研究協力システムの健全性を支援することを目的としており、特にSTEM分野、デュアルユース技術、新興技術、商業的に機微な研究領域の研究者に関連性の高い内容であるとしている。

NPSAは、以上を背景として、Trusted Research 関連のガイダンス文書を体系的に整備・更新を進めており、最近、表2-7に示した主要ガイダンス文書（大学・研究機関向け）が発行あるいは更新されている。

[202] UKRI Trusted Research and Innovation: principles and expectations. https://www.ukri.org/publications/ukri-trusted-research-and-innovation-guidance/ukri-trusted-research-and-innovation-principles-and-expectations/

表 2-7　NPSA が発行した Trusted Research に関する主なガイダンス文書

文書名	主な内容
Trusted Research Guidance for Academics[203]（2025年7月更新）	大学研究者が国際共同研究のリスクを理解し、共同研究パートナーの選定や情報保護・法令遵守を実務的に管理し、研究の安全性とオープン性の両立を図るための実践的なガイダンスである。本文書では特に、①潜在的な共同研究・資金パートナーに関するデュー・ディリジェンスの強化、②輸出管理、国家安全保障投資法、一般データ保護規則（General Data Protection Regulation: GDPR）等のTrusted Researchに関連する法規制の理解、③研究者の安全確保対策、等が強調されている。
Trusted Research Guidance for Senior Leaders[204]（2025年7月更新）	大学の上級リーダーが、Trusted Researchに関する重要な問題や質問事項について、迅速に把握できるように設計された文書である。本文書では以下等について言及されている。 ・ 研究協力を防護する責任を負う上級管理職レベルのリーダーの特定 ・ 最も機密性の高い研究の特定、貴重な研究資産に対する潜在的な脅威の特定 ・ デュー・ディリジェンスのプロセスにおけるレピュテーション・倫理・国家安全保障上のリスクの考慮 ・ リスク管理アプローチの採用（リスクと、海外の資金や研究能力から得られる利益とのバランス） ・ リスクを特定するためのポリシーとプロセスの整備と責任の理解、リスク軽減策（組織が許容できるレベルまで） ・ 単一の資金源に過度に依存することによる財務リスク ・ 国際研究協力者が活動する現地の法的枠組みを考慮したプロセスと監督体制の確立 ・ 職員の保護（外国人職員、客員研究者及び学生の採用と維持を支援するための適切なシステムの整備に関する確認 ・ Trusted Research 文化の創出
Trusted Research Countries and Conferences[205]（2025年7月更新）	国際的共同研究に携わる研究者を対象とし、海外での勤務や旅行時に直面する主な課題に関する助言とガイダンスを提供。海外での勤務や旅行時には、以下等を考慮することを提示している。 ・ 旅行前にリスクアセスメントを実施する。 ・ 共同研究相手の国の法律や規制に関する要件を認識しておく。 ・ ITデバイスを海外に持参する場合のサイバーセキュリティ対策を確認にする。 ・ 海外の国際会議に出席する場合の、ホスト国の法律や習慣を理解し、会議の場での情報提供等を慎重に行う。

[203] NPSA, “Trusted Research Guidance for Academics,” July 2025. https://www.npsa.gov.uk/system/files/NPSA%20TR%20Guidance%20for%20Academics_2025.pdf
[204] Trusted Research Guidance for Senior Leaders. https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-senior-leaders
[205] Trusted Research Countries and Conferences Guidance. https://www.npsa.gov.uk/specialised-guidance/trusted-research/trusted-research-countries-and-conferences

2.3.2　大学・研究機関における取組

英国に関しては、4 つの大学（インペリアル・カレッジ・ロンドン（Imperial College London）、オックスフォード大学（Oxford University）、アストン大学（Aston University）、ウォーリック大学（University of Warwick））を対象として、公開情報に基づき、Trusted Research に関する取組について調査し、整理した。

うち、ウォーリック大学については別途ヒアリングを実施し、先方の許可を得て、ヒアリング情報の一部を含めて、同大学の Trusted Research に関する取組について整理した。

(1) インペリアル・カレッジ・ロンドン（Imperial College London）

(a) 大学における Trusted Research の定義と位置づけ

インペリアル・カレッジ・ロンドンでは、Trusted Research を、「国際的な研究協力者や資金提供者との連携に伴うリスクレベルを評価し、科学的進歩を阻害することなく責任を持ってこれらのリスクを管理するために必要な、研究セキュリティの主要分野に関連する考慮事項を統合したもの」として捉えている[206]。

同大学では、「研究セキュリティは、英国政府の Trusted Research キャンペーンを踏まえた英国政府の戦略的優先事項であり、大学を含む研究基盤の資源が敵対的な国家・非国家主体によってアクセス・悪用されることを防ぐことを探求するものとし、非同盟軍事能力の向上、大量破壊兵器計画、人権侵害への貢献など、国家安全保障を損なうことなく、大学全体の国際協力の健全性を維持することを目的とする」としている[207]。

(b) 主な文書・ツール

インペリアル・カレッジ・ロンドンの教職員・学生を支援するため、Trusted Research に対応して、研究セキュリティおよび新規・既存の国際協力における潜在リスクを考察する方法に関する各種文書やツールを提供している。以下にその例を示す、

(i) Trusted Research チェックリスト

インペリアル・カレッジ・ロンドンでは、研究者自身が、共同研究者に対する初期のデュー・ディリジェンスを実施する必要があるとして、共同研究パートナーが、特に、見知らぬ相手の場合のリスクを認識するためのチェックリスト（Trusted Research Checklist）を作成している（表 2-8 参照）。

---

[206] Research Security. https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/
[207] Ibid.

表 2-8　共同研究パートナーのリスクを認識するためのチェックリスト
（出典：インペリアル・カレッジ・ロンドンのホームページ情報[208] を基に、未来工学研究所が和訳・編集）

チェック項目	考慮事項
新しいパートナーの特徴	・ パートナーが共同研究を望んでいる理由は何か？ ・ 資金提供パートナーが、資金援助の見返りに何を求めているのか？ ・ パートナーの所属機関に関連する国家は英国に敵対するとみなされているのか？または、英国とは異なる民主主義的なあるいは倫理的な価値を持っているのか？ ・ パートナーのデュー・ディリジェンスにより、敵対的な国家とのつながりがある軍隊あるいは警察に代わって行われた研究への関与が確認されたか？ ・ パートナーと共同研究を実施していくうえで、法的・規制上の制約あるいは大学ポリシー上の制約があるか？
共同研究におけるパートナーの関係性	・ 関係構築のため、覚書（MoU）への署名を求められていないか？ ・ 既存の知的財産（IP）、研究データ、機密情報または個人識別可能なデータをプロジェクトに提供するか？提供する場合は、どのように保護されるか？ ・ 生成される知的財産権の帰属先はどこか？ ・ 研究成果として生じる知的財産権を保護する計画は整っているか？ ・ 保護したい活動上の権利や利益（例：出版権、成果へのアクセス権など）を検討し、適切な実現方法について助言を求めること。 ・ 研究パートナーが結果やデータに必要とする、あるいは与えるべきアクセス権限を検討すること。これらは大学ネットワーク上に保存されているか？どのレベルのアクセス権限を提供すべきか？安全なアクセスを提供する他の手段はあるか？ ・ あなたや同僚は、他のパートナーや資金提供者と同様の研究を行っているか？これらの研究領域の間には、十分な物理的分離や保護が確保されているか？
研究者本人が実施しようとする研究の特徴	・ デュー・ディリジェンスで得られた情報の文脈において、研究が誤用されたり、意図しない悪影響を及ぼす用途に利用される可能性はあるか？ ・ 研究内容の全てまたは一部が、英国または他国の輸出許可規制の対象となる可能性はあるか？ ・ 保護すべき機微なデータや個人識別情報が存在するか？ ・ 研究の応用に関して倫理的・道徳的な懸念があるか？

[208] Trusted Research Checklists. https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/trusted-research---protecting-your-work/trusted-research-checklists/

チェック項目	考慮事項
	・ 研究から商業的または特許取得可能な成果が生じる可能性があるか？ ・ あなたのアイデアは盗まれる価値があるか？ ・ あなたの研究はどのように利用されているか？
研究者本人の特徴	・ あなたは標的にされているか？ ・ あなたの研究は不適切な者を引き寄せてはいないか？ ・ あなたの研究成果は不正な者の手に渡る可能性があるか？ ・ あなたの評判の価値はどの程度あるか？

(ii) 第三者機関の関係性レビュー質問票（デュー・ディリジェンス）

インペリアル・カレッジ・ロンドンでは、第三者（英国および海外）と協働する場合、助成金の受諾前にリスク評価を実施することが重要であり、大学当局は契約締結前に、財務的・倫理的・法的・国家安全保障上の考慮事項を含むデュー・ディリジェンスを実施するとしている。

同大学は、この一環として、研究責任者（PI）が、共同研究の関係の構築に伴う財務的リスク、評判的リスク、倫理的リスク、安全面でのリスク、地政学的リスク等、広範囲のリスクを検討することを支援するための、「第三者機関の関係性レビュー質問票」（Research Third Parties: Relationship Review Questionnaire）を作成している[209]（外部からは本質問票にアクセスできない）。

本質問票は、PI と所属部門は、第三者機関の直接的な協力を得て記入する必要があるとしている。本質問票では、プロジェクトの詳細を求めるとともに、以下等のリスク領域を検討するとしている[210]。

・ 第三者機関の財務健全性
・ 第三者機関との関係性および研究等遂行能力
・ 第三者機関の行動基準と誠実性
・ 第三者機関が所在する国の政治的・経済的・地政学的リスク

第三者機関との関係性に関するレビュー・プロセスの一環として、関係する第三者機関がどの程度適切かについて、以下の点を説明することが重要であるとしている[211]。

・ 第三者機関との関係性がどのようにして構築されたのか？
・ なぜ当該機関が、務遂行に最も適した第三者機関なのか？

[209] Undertaking Research Third Party Due Diligence and FAQs. https://www.imperial.ac.uk/research-and-innovation/research-office/preparing-and-costing-a-proposal/identifying-partners/research-third-party-due-diligence/undertaking-research-third-party-due-diligence-and-faqs/
[210] Ibid.
[211] Ibid.

・ 第三者機関との関係性をどのように発展させ、プロジェクトの成果物を監視する予定であるか？

(iii) 第三者機関に関するリスク評価

インペリアル・カレッジ・ロンドンでは、Research Office（研究事務局）により、上記の「第三者機関の関係性レビュー質問票」に基づいて、第三者機関のリスク評価を行うとされる[212]。

Research Office が、当該質問票に設定されている質問項目ごとにリスクスコアを算出し、総合的なリスク評価（低・中・高）を決定する。リスクの影響度と発生可能性のスコア判定には、同大学が設定しているリスク評価クライテリア（外部からはアクセスできない）が適用されるとしている。特定されたリスクの概要と推奨される軽減策は、PI、所属学部、学部研究サービス部門及び学部契約部門に提供されるとしている[213]。

第三者機関が非常に高いリスクと評価された場合には、当該案件は、研究事務局長（Director of the Research Office）、学部運営責任者、そして学部長にエスカレートされる。問題が解決できない場合には、当該案件は副学長（研究・企業担当）に判断が委ねられる[214]。

(iv) 国外出張・国際会議

インペリアル・カレッジ・ロンドンでは、業務目的で海外渡航する際の保護措置のレベルは、計画している活動によって異なるとしている。例えば、海外への短期出張（国際会議への出席など）と海外への長期派遣では、一般的に必要な手続きがより複雑になるとしている。

また必要な保護措置は渡航先の国によっても異なるが、これは、準備すべきセキュリティリスクのレベル（存在する場合）を明らかにするだけでなく、受入国の民主的・倫理的価値観が、学術的自由、研究インテグリティ、および業務の安全性に懸念を生じさせる可能性があるか否かを浮き彫りにすることになるからであるとしている[215]。

同大学では、以上の観点から、同大学の Web サイト[216]で、研究者自身、研究業務及び大学を守るため、業務目的の国際出張計画を申請する前に、以下の事項を検討・確認する必要性を示している。

・ 出張期間および計画する活動内容
・ 訪問の目的と意図する成果、ならびに英国および訪問先の両国における法的考慮事項の有無

---

212 Ibid.
213 Ibid.
214 Ibid.
215 International travel and conferences. https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/trusted-research---protecting-your-work/international-travel-and-conferences/
216 Ibid.

- 訪問予定国の政治状況および潜在的な安全保障上のリスク
- 合意書（あらゆるもの）への署名の要請があるか
- 訪問中に共有する予定の業務内容と情報の性質、および潜在的に機密性の高い質問や会話への対応策

(v) 輸出管理

インペリアル・カレッジ・ロンドンでは、機密性の高いテーマ、材料、情報等に関わる活動を行う職員や英国外の貿易業関係者は、研究セキュリティ自己評価記録（Research Security Self-Assessment Record）フォーム[217]と呼ばれるものを提出することが求められている。

これにより、研究セキュリティ要因（輸出管理リスクを含む）への考慮が記録され、同大学が、責任ある輸出への取り組み姿勢を示すと同時に、後述する同大学の研究セキュリティを支援する Research Office が、必要に応じて法的遵守に基づく適切な対応のための追加の助言や支援を提供できるようになるとしている[218]。

(vi) その他

インペリアル・カレッジ・ロンドンでは、同大学の Web サイトで、Trusted Research に関連する法令・規制（輸出管理、国家安全保障・投資法（NSI 法）等）に関する説明、英国政府から提供されている Trusted Research に関するガイダンスやビデオを案内している[219]。

(c) Trusted Research の支援体制

インペリアル・カレッジ・ロンドンにおいては、Research Office（研究事務局）が、機密指定対象機関・輸出先国の確認、輸出許可申請書の作成、英国輸出管理局（Export Control Joint Unit: ECJU）[220]との連携、米国輸出管理規制、その他の輸出管理・研究セキュリティ関連事項について、個別対応の助言を提供している[221]。また、Research Office には Research Security Team が設置され、研究者への一次窓口として、研究セキュリティに係る質問や相談に対する体制を組んでいる[222]。

なお、同大学においては、Research Office が、研究者が共同研究プロジェクトの助成を受けている期間中、PI、学術部門等と連携して、第三者機関との関係を監視・評価すると

---

217 大学内部のみアクセス可能。
218 Do I need an export license? https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/research-security-legislation/export-controls/do-i-need-an-export-licence
219 External Trusted Research Resources. https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/trusted-research---protecting-your-work/external-trusted-research-resources/
220 英国の軍事・デュアルユース製品の輸出管理・ライセンスを担当するビジネス・通商省（Department for Business and Trade: DBT）内の機関。
221 Further help. https://www.imperial.ac.uk/research-and-innovation/research-office/research-security/research-security-legislation/export-controls/further-help
222 Ibid.

ともに、必要に応じてプロジェクト終了時の第三者機関関係評価を実施するとしている[223]。

(d) 教育・研修

インペリアル・カレッジ・ロンドンでは、研究および学術的責任を有する全職員は、Trusted Research に関する e ラーニングモジュール（Trusted Research e-learning module）を受講し、修了することが求められる。博士課程の学生にも、当該モジュールを受講し、修了することが推奨されている[224]。

当該モジュールでは、研究セキュリティの概要を紹介し、法的順守、契約上の義務、保護措置といった中核的原則に関する知見が提供される。

なお、当該モジュールは、大学の研究セキュリティに関するサイトから提供されているが、外部からのアクセスは不可である。

(2) オックスフォード大学（Oxford University）

(a) 大学における Trusted Research の定義と位置づけ

オックスフォード大学においては、同大学の Trusted Research に関するホームページで、「国際協力に携わる研究者は、潜在的なセキュリティ関連の問題を考慮し、あらゆる潜在的なリスクを管理するために必要な措置を講じるべきである」と述べている[225]。

同大学の研究コミュニティは国際的であることから、世界中から集まった最も優秀な科学者や研究者が在籍し、世界中の多くの個人や組織が同大学との協働を望んでいるとしている。また、グローバルな研究活動においては、国際協力に伴うリスクの一部が動的で複雑化していることを認識することも重要であるとし、これらのリスクには以下が含まれるとしている[226]。

- 研究者・機関の評判リスク
- 学術的自由の制約または学術的議論への干渉
- 法的・規制要件（例：輸出管理規制違反は刑事犯罪）または資金提供契約条項の違反
- 特定資金提供者からの資金受領禁止
- 研究結果・データ・知的財産またはサイバー／物理的インフラの喪失・侵害

[223] Undertaking Research Third Party Due Diligence and FAQs. https://www.imperial.ac.uk/research-and-innovation/research-office/preparing-and-costing-a-proposal/identifying-partners/research-third-party-due-diligence/undertaking-research-third-party-due-diligence-and-faqs/
[224] Early Career Researcher Noticeboard, New Trusted Research Training e-learning module. https://blogs.imperial.ac.uk/early-career-researcher-noticeboard/2024/09/27/new-trusted-research-training-e-learning-module
[225] Trusted Research. https://test-researchsupport.web.ox.ac.uk/trusted-research?
[226] Ibid.

(b) 主な文書・ツール

オックスフォード大学においては、国際共同研究に携わる研究者は、あらゆる潜在リスクを管理するために必要な措置を講じるべきであるとして、検討すべき事項として以下の4つを挙げている。

- 国際共同研究におけるデュー・ディリジェンスの実施
- 法令・規制の遵守
- 知的財産の保護
- 海外での会議におけるセキュリティ対策

同大学においては、以上に関連して、海外パートナーとの共同研究を行う際の考慮事項、国際共同研究におけるデュー・ディリジェンス、法令・規制の遵守、および海外での会議におけるセキュリティ対策に関する解説、文書、ガイダンス等が提供されている。
以下に、これらを示す。

(i) 海外パートナーとの共同研究を行う際の考慮事項

オックスフォード大学においては、同大学のホームページ上で、以下の観点から、海外パートナーとの共同研究を行う際の助言を提供している[227]。

- 国際研究プロジェクトを開始する前に考慮すべき事項
- 国際研究プロジェクトの開始時の留意事項（契約、研究倫理、コスト、データ管理等）
- 国際研究プロジェクトの管理の留意事項（海外のスタッフの雇用、海外のスタッフへの支払い、海外でのサプライの購入、輸出・輸入管理等）

これらに関連して、国際共同研究チェックリストが提供されているが、内部資料のため、外部からはアクセスできない[228]。

また、同大学においては、研究サービス部門は、Strategic Partnership Scorecard（戦略的パートナーシップ・スコアカード）と呼ばれる、表形式の評価シートを作成している。これは、大学が国際研究パートナーシップを締結する前に、その候補となる機関間パートナーシップが徹底的かつ厳格な審査を受けることを保証するために使用されるとされる。本評価シートも内部資料のため、外部からはアクセスできない[229]。

(ii) 国際共同研究におけるデュー・ディリジェンス

オックスフォード大学では、Trusted Research の一環として、研究協力を行う際には、同大学の利益を守るために、デュー・ディリジェンスを実施することが求められる。また、

227 International Toolkit. https://globalresearch.admin.ox.ac.uk/international-toolkit?
228 Ibid.
229 Strategic Partnership Scorecard. https://globalresearch.admin.ox.ac.uk/strategic-partnership-scorecard?

資金提供者の契約条件において、オックスフォード大学が資金を受領し、それを外部機関に再配分・管理するすべての共同研究についてデュー・ディリジェンスの実施が求められている場合には、大学は所定のデュー・ディリジェンスの手続に従う必要があるとしている。

研究者が研究パートナーのデュー・ディリジェンスについて考慮すべき事項として、以下を示している[230]。

- 組織、機関、または団体について、懸念材料となり得る公開情報が存在するか？
- 協力関係あるいは研究パートナーは、倫理的または国家安全保障上の懸念事項を引き起こす可能性があるか？
- 提案されている研究パートナーは、軍や国家、特に我々の民主主義的・倫理的価値観とは異なる国家と関連しているか？
- 研究パートナーが所在する国の自由度や法の状態について、どのような情報が得られるか？
- 提案されている提携関係は、研究者または大学にとって利益相反を生じさせる可能性があるか？
- 学術訪問者や学生について、訪問や学生支援を行っている雇用主や資金源の身元を把握しているか？

デュー・ディリジェンスの手続きに関しては、ガイダンス、フローチャート等が提供されているが、これらは内部資料であり、外部からはアクセスできない[231]。

(iii) 法令・規制の遵守

オックスフォード大学では、Trusted Research の一環として、法令・規制の遵守に関する留意事項として、以下等をあげている[232]。

- 研究協力により、物品の物理的な移動、またはソフトウェア・データ・技術・ノウハウの英国から国外への移転が生じる可能性があるか？ 該当する場合、英国輸出管理規制の対象となる可能性があるか？
- 規制対象物品の輸出に関して適切な許可を取得しないことは刑事犯罪である。
- 米国輸出管理規制（第三者との資金提供契約や研究契約に含まれる可能性のあるものを含む）など、その他の制限対象となる情報・物品・資料を共有する予定があるか？
- 学生ビザの申請は、学術技術承認制度（Academic Technology Approval Scheme: ATAS）[233,234]の適用範囲に該当するか？

---

230 Trusted Research. https://test-researchsupport.web.ox.ac.uk/trusted-research?#tab-2697206
231 Due Diligence Guidance. https://globalresearch.admin.ox.ac.uk/diligence?
232 Trusted Research. https://test-researchsupport.web.ox.ac.uk/trusted-research?#widget-id-2697386
233 英国政府が運用する学術技術承認制度で、安全保障上機微な分野を学ぶ、あるいは研究する海外（主にビザ対象国籍）研究者・学生に対し、入国・在籍前に事前承認を求める制度。
234 Academic Technology Approval Scheme (ATAS). https://www.gov.uk/guidance/academic-technology-approval-scheme

・ 外国影響力登録制度(Academic Technology Approval Scheme: ATAS)[235,236]の影響を受けるか？

なお、同大学では、大学における輸出管理法令順守の手順や役割責任を規定した、「研究における輸出管理ポリシー（Export Control in Research Policy）」[237]を作成・公表しているが、その中で、輸出管理法令の適用・運用が特定の国籍・民族・宗教等に不均衡な影響を与える、あるいはそのように受け止められる可能性を認識している。

そのため、研究における輸出管理ポリシーの導入に際し、平等への影響を体系的に評価することを目的とした、Equality Impact Assessment（EIA）文書（Equality Impact Assessment（EIA）- Export Control in Research Policy）[238]を作成・公表し、潜在的影響の明示、緩和措置の設定、定期的レビュー体制等について示している。

(iv) 知的財産の保護

オックスフォード大学では、Trusted Research の一環として、研究者に対して、共同研究における知的資産の保護に関する留意点を示している[239]。以下にこれを示す。

・ 共同研究は、オックスフォード大学が保有あるいは生成した成果、情報及び知的財産を保護する契約の対象となるか？
・ 共同研究は、研究成果の公表能力を維持し、通常の学術的自由や議論を制限または妨害することはないか？
・ 当該プロジェクトは、他の研究プロジェクト（第三者との共同実施または第三者資金によるものを含む）から分離することが可能か？
・ 共同研究者（訪問者を含む）がアクセス可能な情報および研究成果は、プロジェクト遂行に必要な範囲に限定されるか？
・ 研究グループにおいて、適切な情報セキュリティおよびサイバーセキュリティ対策が実施されているか？

(v) 海外での会議におけるセキュリティ対策

オックスフォード大学では、Trusted Research の一環として、研究者に対して、海外での会議におけるセキュリティ対策に関する留意点を示している。以下に、これに関する主な

---

235 外国の勢力による英国政治や国家安全保障への秘密裏の干渉を監視・透明化するための制度で、2025年７月１日から施行された。この制度は、特定の外国の力やその支配下にある組織のために活動する個人・組織に対し、政治的影響活動やその他の活動の登録を義務付けるもので、違反者には罰則がある。
236 Academic Technology Approval Scheme (ATAS). https://www.gov.uk/guidance/academic-technology-approval-scheme
237 University of Oxford, “Export Control in Research Policy,” March 2025. https://compliance.admin.ox.ac.uk/sitefiles/export-control-in-research-policy.pdf
238 Equality Impact Assessment – Export Control in Research Policy. https://compliance.admin.ox.ac.uk/sitefiles/export-control-policy-equality-impact-assessment.pdf
239 Trusted Research. https://test-researchsupport.web.ox.ac.uk/trusted-research#tab-2697401

例を示す[240]。

- 英国の貿易制裁または武器禁輸措置の対象国へ渡航する場合、公式な協議や学術関係者との非公式な会話において共有する情報は、すべて既に厳密に公開情報（会員資格、有料壁、機密指定などの制限なく一般に公開されている情報：購読誌での掲載だけでは不十分）であることを確認すること。
- 会議を主催する場合は、学部 IT 部門及び大学本部情報セキュリティ部門と連携し、訪問者滞在中に許可する IT アクセス・インターネットアクセスの種類を検討する。
- 会議を主催する場合は、英国の貿易制裁または武器禁輸措置の対象国からの個人の参加、およびオックスフォード内外で開催される会議への参加を支援するために当該個人に送金される奨学金・資金に関する規則について協議すること。
- 学者の間で交わされる様々な会話（夕食時の非公式な会話等）は公的な領域に留めるべきであり、それらの会話から将来の共同研究につながる結果が生じた場合は、必ずTrusted Research Team（下記（c）参照）による審査を受けること。
- 出張から戻った際は、新たな人脈から生まれた共同研究について、適切なデュー・ディリジェンスを実施すること。
- オックスフォード大学主催の会議で発表を行う者は、講演中の全ての情報を公開情報として扱うよう通知を受ける必要があること。

(c) Trusted Research の支援体制

オックスフォード大学では、研究サービス部門（Research Services）の Trusted Research Team が、国際共同研究のコンプライアンス遵守と完全な保護を支援するとしている[241]。

この一環として、研究サービス部門では、各学部が「Trusted Research 」の変容する環境に対応できるように、定期的に「信頼される研究と保証に関する相談会（Trusted Research & Assurance Surgeries)」を開催している。この相談会は、研究者、学部支援スタッフ、学部長、研究サービス部門職員が参加可能であり、輸出管理、国家安全保障・投資法、国際共同研究におけるデュー・ディリジェンスを含む「信頼される研究と保証」の全側面について議論するとされる[242]。

(d) 教育・研修

オックスフォード大学においては、Trusted Research に関連する e ラーニング研修モジュールとして「Trusted Research and Export controls」が提供されている。これは、同大学の全大学教職員・学生が受講可能であるとされているが、具体的な内容は公開されていな

240 Trusted Research. https://test-researchsupport.web.ox.ac.uk/trusted-research?#widget-id-4936076
241 Oxford Talks, Research Briefing for MSD. https://talks.ox.ac.uk/talks/id/ad6d833e-3247-460c-a62b-d659fc305144
242 Oxford Talks, Trusted Research and Assurance Surgery. https://talks.ox.ac.uk/talks/id/30e02775-2879-4273-8bd0-a55b4e707a95/

い[243]。

(3) アストン大学（Aston University）

(a) 大学における Trusted Research の定義と位置づけ

アストン大学では、Trusted Research を、「研究者、英国の大学、産業界のパートナーが国際的な共同研究を行う際に情報に基づいた判断を下すことができるように支援するキャンペーン」であると説明し、これは、「研究の盗用や悪用から保護し、研究者自身の評判とアストン大学の評判の両方を守ることを目的とする」としている[244]。

同大学では、あらゆる研究にはリスクが伴うが、共同研究や応用研究は特に脆弱であるとしており、共同研究及び応用研究に関しては、以下のような注意点を示している[245]。

- 共同研究は、自国とは利益や倫理観が異なる国家に拠点を置く組織・機関によって歪められる可能性がある。共同研究は、敵対的な意図を持つ個人に専門知識、IT、研究、ネットワークへのアクセスを許す恐れがある。
- 応用研究は、特に明確な問題解決や商業的応用を目的とする場合、悪用されやすい。応用研究における危害の可能性は大きく、知的財産の喪失や、非倫理的な方法、あるいは国家安全保障を脅かす手段による技術の悪用といった結果を招きかねない。

同大学は、上記を踏まえて、当大学の研究者に以下を遵守することを求めている[246]。

- 個人データ保護、サイバーセキュリティ、輸出管理、デュー・ディリジェンスなど専門分野に関連するモジュールを含む研修の受講を維持すること。
- 同大学のホームページに掲載されている 4 つのサブセクション（デュー・ディリジェンス、輸出管理、国家安全保障、国家安全保障・投資法（NSI 法））で公開されているガイダンスを熟知すること。
- 共同研究を検討する際には、安全保障関連リスクを考慮すること。
- 国際的な個人・組織との共同研究・資金提供・提携については、資金の有無にかかわらず開示すること。
- 利益相反（実在または潜在的なもの）がある場合は申告すること。
- 不明点がある場合や国際共同研究を開始する際には、助言を求めること。

[243] Research Practice Training. https://www.ox.ac.uk/research/support-researchers/research-practice/research-practice-training
[244] Trusted Research and Innovation. https://www.aston.ac.uk/research/integrity-ethics/trusted-research
[245] Ibid.
[246] Ibid.

(b) 主な文書・ツール

アストン大学では、Trusted Research に関連するトピックスとして、同大学の Web サイトで、デュー・ディリジェンス、輸出規制、国家安全保障・投資法等について、手順書を含め、研究者に、共同研究の申請の手続き等に関する必要な情報を提供している[247]。

(i) デュー・ディリジェンス

アストン大学では、デュー・ディリジェンスとは、「合理的な事業体または個人が、他者と合意または契約を結ぶ前に実施すべき調査、あるいは注意義務」であるとしている。これは、共同研究等に関連する倫理的、法的、財務的及び国家安全保障上の問題、並びに、学術的状況を考慮に入れ、コスト、便益、リスクを理解した上での適切な意思決定を支援するものであるとしている。

同大学は、2022 年 6 月に、外部の研究者や関係者と共同研究を行う際のデュー・ディリジェンス手順書（Outside Party Due Diligence Procedures）[248]を作成・公開している。これは、大学における外部者とのあらゆる関係（研究、寄付、配置[249]、ビジネス等を含む）などを対象にした共通のデュー・ディリジェンスの手順を示したものであることから、同大学では、別途ホームページ上で、海外パートナーとの共同研究を検討している研究者向けに、デュー・ディリジェンスのプロセスを解説している[250]。

研究・イノベーションプロジェクトにおける海外協力者のデュー・ディリジェンスに関する確認は、以下の場合に限定されるとしている[251]。

協力対象となるプロジェクトが、公的資金または慈善団体資金によるものである場合で、協力者が以下のいずれにも該当しない場合：
- 英国、EU、米国、カナダ、オーストラリア、ニュージーランドに所在する大学
- 英国の公的機関（英国地方自治体、英国政府省庁等）
- 英国慈善委員会に登録された英国の慈善団体
- 協力契約またはその他の契約に基づく英国の産業協力者

表 2-9 に、海外パートナーとの共同研究を検討している研究者向けに説明されているデュー・ディリジェンスのプロセスの要点を示す。

247 Ibid.
248 Aston University, “Outside Party Due Diligence Procedures,” June 2022. https://www.aston.ac.uk/sites/default/files/Outside%20Party%20Due%20Diligence%20Procedures%20-%20June%202022.pdf
249 大学と外部組織との間で人が一定期間「物理的または組織的に入り込む形の関係」を意味する。
250 Due Diligence. https://www.aston.ac.uk/research/integrity-ethics/trusted-research/due-diligence
251 Ibid.

表 2-9　アストン大学における海外パートナーとの共同研究に関する
デュー・ディリジェンスのプロセス
（出典：アストン大学のホームページ情報[252]に基づき、未来工学研究所が作成）

海外共同研究に関するデュー・ディリジェンスの主な項目		概要
デュー・ディリジェンスの目的		・ 国際共同研究に関するデュー・ディリジェンスは、国際共同研究の可否を判定するものではなく、助成金授与前の段階で潜在的なリスクを早期に特定する。 ・ 研究者に対して、海外パートナーとの議論や意思決定の記録を保持することを求める。
デュー・ディリジェンスの手順	ステージ１：申請前の段階	・ 申請前の段階で、ステージ１のデュー・ディリジェンス質問票[253]を使って、早期に潜在リスクを特定することを目的として、デュー・ディリジェンス・チェックを行う。必要であれば、提案書提出前に、上位管理者にエスカレーションすることができる。 ・ デュー・ディリジェンス・チェックの結果は、レッド／アンバー／グリーンで判定され、レッドの場合は、大学理事会の書面承認なしに進めることができない。
	ステージ２：採択後～契約前	・ 採択された場合、契約署名前に、関係するパートナーに対して、ステージ２のデュー・ディリジェンス質問票[254]を使ったデュー・ディリジェンス・チェックを行う。
	ステージ３：契約後～研究期間中	・ 相手先の所有権の変更や合併、財務状況の変化、業務水準に関する重大な懸念等があった場合に、デュー・ディリジェンスを実施する。

なお、同大学のパートナーシップ関係委員会（Partnership Relations Committee）が、同大学における全てのデュー・ディリジェンスの決定についての判断を監督する。同委員会は、デュー・ディリジェンスに関する各判断の過程および根拠を後から検証可能な形で記録するため、月次で会合を開催する。特定のプロジェクトに対して実施されたデュー・ディリジェンス関連書類は、すべて大学内の研究管理システムの申請記録に保存される[255]。

(ii) 輸出規制

アストン大学は、輸出管理を、「特定の物品、技術、ソフトウェア及び知識を、英国から国外へ移転する際の一連の法的制限」として説明し、海外渡航時の PC 持ち出しなども輸出に該当し得るとしている[256]。

[252] Ibid.
[253] アストン大学の web ページ上では、ステージ１のデュー・ディリジェンス質問票の内容に関する説明がされていない。
[254] アストン大学の web ページ上では、ステージ２のデュー・ディリジェンス質問票の内容に関する説明がされていない。
[255] Due Diligence. https://www.aston.ac.uk/research/integrity-ethics/trusted-research/due-diligence
[256] Export Controls. https://www.aston.ac.uk/research/integrity-ethics/trusted-research/export

また、同大学は、2021 年 4 月にアストン大学輸出管理・貿易制裁ポリシー（Aston University Export Controls and Trade Sanctions Policy）[257]を作成・公開し、違反が刑事罰・重大な制裁につながり得る点を明確化している。

(c) Trusted Research の支援体制

アストン大学では、研究ガバナンス受信箱（Research Governance inbox）（電子メールでの連絡口）が設置されている。大学の研究倫理チームが、それを毎日確認しており、必要に応じて担当者や主要な関係者と連携するとされる[258]。

同大学の戦略的資金調達管理者（Strategic Funding Manager）は、研究応募書作成と承認プロセスの一環として、研究者がデュー・ディリジェンスの手続きを完了することを支援する重要な役割を担っているとされる。可能な限り、研究応募書作成のプロセスの早い段階で、関連する学部の戦略的資金調達マネージャーに連絡し、応募書の提出前にデュー・ディリジェンスのプロセスのステージ 1（表 2-9 参照）を完了する時間を確保することが推奨されている[259]。

同大学の事業開発管理者（Business Development Manager）は、産業界からの直接資金調達、Innovate UK 等への申請において、研究者がデュー・ディリジェンスのプロセスを完了するための支援を行うことができるとされる。可能な限り、研究応募書作成のプロセスの早い段階で、関連する学部の事業開発マネージャーに連絡し、応募書の提出前にデュー・ディリジェンスのプロセスのステージ 1（表 2-9 参照）を完了する時間を確保することが推奨されている[260]。

(d) 教育・研修

アストン大学では、デュー・ディリジェンス研修システム（Aston University online Due Diligence Training）がネットワーク上で提供されている。このシステムでは、以下のような学習メニューから構成されている。学習所要時間は 20～30 分とされる[261]。

- 学習の目的
- デュー・ディリジェンスとは？
- UUK のガイダンスの内容
- いつデュー・ディリジェンスを実施すべきか？
- アストン大学のデュー・ディリジェンスのプロセス
- 新たなパートナーシップに関する意思決定プロセスの一環として検討する必要のある事項

[257] Aston University, “Export Controls and Trade Sanctions Policy,” April 2021. https://www.aston.ac.uk/sites/default/files/Export-Controls-and-Trade-Sanctions-Policy.pdf
[258] Trusted Research and Innovation. https://www.aston.ac.uk/research/integrity-ethics/trusted-research
[259] Ibid.
[260] Ibid.
[261] Due Diligence. https://rise.articulate.com/share/dua1nBM4ON3L4eldawVV8rGh3b74W8Uo

・ パートナーシップで起きる可能性のあるリスク
・ 輸出管理における留意事項
・ 理解確認テスト

(4) ウォーリック大学（University of Warwick）

(a) 大学における Trusted Research の定義と位置づけ

2020 年 1 月に、英国が EU を離脱した後、英国の高等教育機関セクターにおける輸出管理への注目度が著しく高まった。これを受けて輸出管理への関心が増大し、Trusted Research への注目が高まり、ウォーリック大学もこの流れに従った[262]。

ウォーリック大学では 研究の安全確保、機微情報の保護、研究者の努力の成果が盗用・悪用・歪曲されるといったリスクを回避するために、Trusted Research を、研究を安全に進めるための規制・対策・グッドプラクティスとして位置づけている。これには、輸出管理関連法令、国家安全保障・投資法（National Security & Investment Act）、名古屋議定書等の遵守が含まれる。

ウォーリック大学では 、研究者に対して、自身の研究にアクセスし、利用し、利益を得る可能性のある者（研究者自身が認識しているか否かを問わず）を常に把握しておくことが重要であるとし、特に、以下のいずれかを行う際には注意を促している[263]。

・ 機微技術または国家的に重要な技術[264]を扱う場合
・ 英国国外のパートナーと共同作業を行う場合（特に民間企業や軍事禁輸措置対象地域のパートナーとの共同作業）
・ 電子メール、ファイル共有、ビデオ通話、電話、または物理的な送付により、技術・情報・データを英国国外の機関と共有する場合
・ 英国国外の研究者と共同出版する場合
・ 業務文書や業務用端末を携行して英国国外へ渡航する場合（アクセス権限が本人以外にない場合も含む）

(b) 主な文書・ツール等

ウォーリック大学では、全職員に適用される輸出管理方針[265]を策定している。共同研究パートナーの管理や共同研究の開発・支援を管理する各部門では、パートナーデュー・ディリジェンス、輸出管理、国家安全保障・投資法、名古屋議定書、その他関連法規など、

[262] 関係者への聞き取り調査による。
[263] Trusted Research. https://warwick.ac.uk/services/ris/research-compliance/trusted_research/
[264] 国家安全保障・投資法では、経済安全保障の観点から 17 の重要技術分野（先端材料、先進的ロボティクス、通信、民生用原子力、AI、コンピューティング・ハードウェア、暗号認証、データインフラ、防衛、量子技術、エネルギー、デュアルユース、衛星・宇宙技術、合成生物学、輸送等）の事業体の買収（いわゆる「届出義務のある買収」）について、政府に報告することが義務付けられている。
[265] Export Controls. https://warwick.ac.uk/services/ris/research-compliance/export-controls/

Trusted Research の主要分野に関する標準的な運用方針（Standard Operating Policy）とプロセスを定めている[266]。

これらの方針とプロセスについては、各種活動の承認または最終決定前に、チェックと審査を導入し、リスク評価の完了を義務付け、実務担当職員に対し、追加審査やエスカレーションを必要とする要素に関するガイダンスを提供するとしている[267]。

(i) 国際研究プロジェクトに関するガイダンス

ウォーリック大学では、英国国外で研究を実施または共同研究を行う場合、英国に拠点を置く研究者は、「国際研究に関する手続きと方針（University processes and policies for international research）」[268]に従い、英国および研究実施国の法的・倫理的要件（特に Trusted Research の要件）を遵守する必要があるとしている。

研究者は、自国および外国の研究者・参加者の民事・法的・財政的立場の違いを認識し、他国での研究実施に影響を及ぼし得る複数の国内法が存在し得ることを理解し、現地のデータ保護法に則り、個人データの収集・移転について配慮すべきであるとしている。

特に発展途上国が関与する場合、公平な研究パートナーシップの構築に留意し、以下の事項に配慮する必要があるとしている[269]。

- 当該国の特性や文化を尊重しつつ、研究者が関与する参加者の権利と利益を軽視してはならないこと。
- 研究実施の理由は、通常、研究が行われる地域社会のニーズとの関連性に基づくべきであること。
- 倫理審査は可能な限り英国と実施国双方で実施すること。
- 研究に関わる全ての関係者の貢献を適切に認めること。

同大学のホームページでは、国際研究の計画と実施には追加的な複雑性を伴うことから、研究コミュニティを支援する一環として、プロジェクトのライフサイクル全体を通じて国際パートナーと協働する際に考慮すべき事項を案内し、主要連絡先の詳細を提供するガイダンスページを作成したと述べている。しかし、その具体的な内容については、外部からアクセスできない。また、当該ホームページ上には、国際研究チェックリスト（International Research Checklist）のリンクが示されているが、外部からはアクセスできない[270]。

---

266 Trusted Research. https://warwick.ac.uk/services/ris/research-compliance/trusted_research/
267 関係者への聞き取り調査による。
268 Collaborative Working and International Research. https://warwick.ac.uk/services/ris/research-integrity/research_code_of_practice/collaborative_internationalresearch/
269 Ibid.
270 Guidance on International Research Projects. https://warwick.ac.uk/services/ris/international-research/

(ii) デュー・ディリジェンス

ウォーリック大学では、研究・インパクトサービス（Research & Impact Services: R&IS）が、研究助成金・契約、研究戦略・開発、インパクト・イノベーション、倫理・研究ガバナンス等において、専門的な実務者支援を提供している。

同大学では、研究コンプライアンスの枠組みで、輸出管理、外国影響力登録制度（FIRS）、国家安全保障・投資法、名古屋議定書、ヒト組織法（Human Tissue Act 2004）等の遵守を確保する過程で実施されるチェックについて説明する一環として、資金提供者、協力者、パートナーおよび関連プロジェクトに対するデュー・ディリジェンスの必要性について言及している[271]。

R&IS は、期待される資金提供者、共同研究者、パートナー及び関連プロジェクトに関するデュー・ディリジェンス審査を実施する際、大学の運営や評判に対する予期せぬ、あるいは未特定リスクの可能性を最小限に抑えることを目指すとしている。

デュー・ディリジェンス審査の具体的な内容は、対象となる組織やプロジェクトごとに異なるが、潜在的なパートナー、協力者、資金提供者に関して、以下を含む（ただしこれらに限定されない）複数の事項を検討することが一般的であるとしている[272]。

- 法人登記状況および公開財務諸表
- 信用情報報告書
- 学術的信頼性及び研究上の信頼性
- 共同・連携する組織の実態、組織に係る問題点、組織の対応等に関する否定的な報道や論争記事
- 制裁リスト掲載の有無、または高リスク地域における活動の有無

プロジェクト自体を審査する際には、特定法令（輸出管理など）に基づく申告・申請の要否に加え、業務内容の性質を精査し、大学価値観との整合性を確認するための追加の内部審査が必要になるか否かを判断するとされる[273]。

(iii) リスク評価

ウォーリック大学では、資金提供者、共同研究者の経歴・所在地、研究の種類、研究者の経歴などを確認するため、一連のリスク要因とトリアージ質問[274]を用いてすべての研究活動を審査する。リスク評価を行うため、オンライン検索に加えて、デジタルツールを活用し、大学でのベストプラクティスや先例を参照するとともに、必要に応じて RCAT と協議する[275]。

---

271 Due Diligence. https://warwick.ac.uk/services/ris/research-compliance/due-diligence/
272 Ibid.
273 Ibid.
274 トリアージ質問とは、提案されたプロジェクトの技術的領域を主に扱う初期段階のスクリーニング質問を指す。これらは非常に早い段階で用いられ、新たな提案をより厳格な審査プロセスに付すべきか否かを判断するために用いられる（ヒアリングによる）。
275 関係者への聞き取り調査による。

Trusted Research のリスク評価においては、規制違反の起こり易さおよびそれに伴う財務的損失、コンプライアンス維持に伴う業務負担、潜在的な信頼・評判の損失、必要な緩和策の比例性等を考慮する。これらは、共同研究を実施することによる評判・学術的・財務的利益、及び共同研究を実施しない場合に失われる機会費用と相対的に評価される[276]。

同大学では、初期審査で高リスクを示す一つ以上の要因（プロジェクトが機微な技術分野に属する等）が確認された案件は、RG&C Team に回付される。同チームは、関連する企業のプロファイル、研究プロジェクトの目的と適用法令との関連性、大学の内部方針やリスク許容度について詳細な調査を実施する。これには、専門家の視点からリスクと便益に関する見解を理解するために、研究責任者との協議が含まれる。一つ以上の領域で重大なリスクがあると判断された場合、研究者と協力して、最終決定を行う上級管理職に対してプロジェクトのバランスの取れた説明を行う[277]。

研究助成および契約の承認は、R&IS の承認なしには進められない。R&IS の承認を得るには、リスク評価プロセスの満足のいく完了が求められる。これにより全てのプロジェクトが、リスクの性質および大きさに応じた比例原則に基づき審査されることが保証される[278]。

(iv) 倫理原則

ウォーリック大学は、研究、資金調達、教育パートナーシップなどの分野に、倫理原則を適用している[279]。

ウォーリック大学では、評判や倫理の観点から、Trusted Research をより広範に捉えている。合法性や規制上の許容性は、同大学の Trusted Research に関する評価の重要な要素ではあるが、対象とする行為や活動が合法的で許容される場合であっても、それが合理的か否かを問うことを妨げるものではないとしている[280]。

同大学では、研究パートナーに対するデュー・ディリジェンス審査に加え、共同プロジェクトに対する倫理原則を適用しているが、同大学では、共同研究等の活動がもたらす評判への影響やその道徳的・倫理的価値を含め、より広範な文脈で精査する。大学がこれらの点で問われた場合、「規制で許可されていた」という形で弁明するだけでなく、判断したことの正当性を説明できるようにしている[281]。

(c) Trusted Research の支援体制

ウォーリック大学では、R&IS が、Trusted Research に関連する大学のガイドラインおよびポリシーの大部分を管理・策定しているが、これらは委員会レベルで承認される[282]。

---

[276] Ibid.
[277] Ibid.
[278] Ibid.
[279] Ibid.
[280] Ibid.
[281] Ibid.
[282] Ibid.

R&IS には、研究ガバナンス・コンプライアンス・チーム（Research Governance & Compliance Team: RG&C Team）があり、研究、活動のあらゆる側面におけるコンプライアンスの日常的な責任を管理するとともに、大学全体にわたる規制分野における責任の一部を担っている。これには、プロジェクト審査、規制対応（登録申請やライセンス取得など）、研修実施、リスク管理、品質保証などが含まれる[283]。

この他、R&IS には、パートナーシップ構築・支援を担う助成金・契約チーム（Grants and Contracts Team）、国際戦略チーム（International Strategy Team）、財務チーム（Finance Team）等の実務チームがある。R&IS 内のチームが、研究環境における全ての提案パートナーおよび活動について、最初の段階で一時審査と選別（リスクに応じて審査を行う深さを振り分ける）を実施する。また R&IS 内の別のチームが、必要に応じて複雑または高リスクが懸念されるケースについて詳細な審査と評価を行う。特に複雑なケースは R&IS の上位組織へエスカレーションされ最終承認を受ける場合があるが、その判断の根拠となる評価と審査は R&IS が主導する[284]。

R&IS およびその他の専門職サービス部門の本部はリスク管理の基盤を維持しているが、各学部および個々の研究者は、リスク管理において積極的であること、必要に応じて助言を求めることが推奨されている[285]。

潜在的または現在の共同研究者の経歴や活動内容が不明な場合、自身の研究が誤用または不正流用される可能性がある場合、自身の研究または研究で使用するものが不明または危険な場所から提供される可能性がある場合、研究の一環として開発するものがそのような場所へ送られる可能性がある場合等には、RG&C Team に相談することとしている[286]。

(d) 教育・研修・意識向上

学部指導層および個々の研究者は、RG&C Team による研修および啓発活動を通じて、Trusted Research の全体像、ならびに発展的なリスクをもたらす可能性のある主要な課題や問題について、常に認識し情報を得ている[287]。

ウォーリック大学では、画一的な必須研修プログラムを設けておらず、研究分野や国際連携の状況等に応じて研修内容を調整している。RG&C Team は、複雑な事例や問い合わせに対して対話的な支援を提供し、先行的なリスク評価を実施して、研修等の介入が必要な領域を判断している[288]。

同大学では、Trusted Research に関連する分野について、学部で、定期的に対面及びオンライン研修を実施している。研修の具体的な内容や頻度は、各学部の特性に応じて調整されている。大学本部は参加を義務付けることは多くはないが、学部が、職員の研修参加の義務化を希望する場合には、大学本部がそれを支援する[289]。

---

283 Ibid.
284 Ibid.
285 Ibid.
286 Contact Us. https://warwick.ac.uk/services/ris/research-compliance/contact/
287 関係者への聞き取り調査による。
288 Ibid.
289 Ibid.

追加支援を必要とする研究グループがある場合（RG&C Team に問い合わせしたグループ、または RG&C Team が自ら特定したグループ）には、RG&C Team が個別のニーズに応じた研修を実施することが多い[290]。

R&IS は、リスクの高い学部向けに定期的な研修を実施し、高等教育輸出管理協会（Higher Education Export Controls Association: HEECA）[291]が運営するオンライン研修モジュールへのアクセスを管理している[292]。

現在の研修対象は、主に R&IS 職員、技術職員、研究者、そして最近では博士課程の学生に焦点を置いている。今後は他の管理・専門職サービス部門や学部支援スタッフ（施設管理、資材倉庫等の担当者）にも、研修を拡大する必要性を認識しており、これを推進する予定であるとしている[293]。

(e) 研究のオープン性とのバランス

ウォーリック大学の Trusted Research に関する基本的なアプローチは、大学や個々の研究者を不当なリスクに晒すことなく、学術的自由とオープンな協働を可能な限り尊重し、柔軟に対応することであるとしている[294]。

同大学は、研究活動を阻止する理由を探すのではなく、原則として支援する立場から出発し、必要に応じてリスク管理と軽減策を講じる姿勢であるとしている。RG&C Team にとって重要なのは、高リスク分野で活動する研究者が、自らの研究に関わるリスクを管理し、リスクに対処するために、RG&C Team からその支援と権限を与えられていることであるとしている[295]。

2.3.3 資金配分機関等における取組

公開情報に基づき、英国研究イノベーション機構（UKRI）における Trusted Research に関する取組について整理した。

(1) 英国研究イノベーション機構（UKRI）

UKRI は、2021 年 8 月に、UKRI のファンディングを受けようとする機関が、UKRI としての研究の信頼性・安全性・開放性を同時に確保するための横断的枠組みである、TR&I（Trusted Research & Innovation）の観点から理解すべき原則を示した「Trusted Research and Innovation Principles」[296]を公表した。

---

290 Ibid.
291 HEECA は、英国高等教育セクター全体における輸出管理コンプライアンスのベストプラクティスを開発・維持・促進するための全国ネットワークである。
292 Trusted Research. https://warwick.ac.uk/services/ris/research-compliance/trusted_research/
293 関係者への聞き取り調査による。
294 Ibid.
295 Ibid.
296 UKRI, “UK Research and Innovation Trusted Research and Innovation Principles,” August 2021. https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf

UKRI は、2025 年 6 月に、上記文書を踏まえて、UKRI の助成金を申請するうえで、UKRI が TR&I に適用する原則および、UKRI が支援する研究組織（企業、研究所等）に対する一般的な期待事項を示した「Trusted Research & Innovation: Principles and Expectations」を公表した[297]。

なお、UKRI は、以下のニーズに応えるため、「Trusted Research and Innovation (TR&I) Shared Capability Team」を設立した[298]。

- 共同研究活動が安全かつ確実に実施されるよう、管理、指導及び支援を行うこと。
- グローバルな研究・イノベーション・エコシステム内で活動する際のリスクを最小限に抑えつつ、機会を最大限に活用すること。

同チームは UKRI 全体を横断して活動し、TR&I に関する取り組みを統合しており、英国全土のパートナーと緊密に連携しているとされる。また、国際的なステークホルダーに対しても同様のアプローチを採用しており、知識と優良事例の共有を通じて、強固で信頼できるグローバルな研究・イノベーション・エコシステムの促進と構築に協力して取り組んでいるとしている[299]。

以下に、「Trusted Research & Innovation: Principles and Expectations」の主要事項を示す。

(a) Trusted Research and Innovation（TR&I）の定義

TR&I とは、英国の知的財産、機微な研究、人材およびインフラを、潜在的な窃盗・悪用・搾取から保護することを指す。

(b) 原則

- UKRI は TR&I に関してリスクベースのアプローチを採用している。すなわち、リスクが高いと見なされたプロジェクトには、追加の緩和策や管理策の実施が求められる場合がある。
- UKRI は、合理的に可能な限り、以下等を確保することを目指している。
  - TR&I に関する方針が、UKRI の組織としての公平性・多様性・包括性（Equality, Diversity and Inclusion: EDI）の目標を十分に支えるものであること。

297 UKRI Trusted Research and Innovation: principles and expectations. https://www.ukri.org/publications/ukri-trusted-research-and-innovation-guidance/ukri-trusted-research-and-innovation-principles-and-expectations/
298 Trusted research and innovation. https://www.ukri.org/manage-your-award/good-research-resource-hub/trusted-research-and-innovation/
299 具体的な情報は示されていない。

- 助成金公募において、申請時に求められる可能性のある、または審査プロセスの一部となる TR&I 関連の追加要件が明確に示されていること。
- 助成の一環として要求される追加のリスク緩和策や管理策が、具体的かつ適切な範囲のものであり、理解可能で、助成金受給者が実行可能なものであること。
- 同様のレベルのリスクがあると評価されたプロジェクトには、同様の TR&I 要件が課されること。

・ UKRI は、研究とイノベーションが、誠実さをもって強固な倫理的枠組みの中で行われるよう確保すること（「責任ある研究とイノベーション（Responsible Research and Innovation）」と呼ばれる概念）についても、同等の重きを置いている。

(c) 期待事項

(i) プロジェクトパートナーの TR&I に関する評価

・ UKRI は、支援先の組織が研究パートナーシップ、共同研究契約、商業契約に関与する他組織に対して、適切なデュー・ディリジェンス（相手先の慎重な事前調査）評価を実施することを期待している。UKRI は、これらの評価におけるリスク許容度や実施方法の詳細は、機関によって異なることを承知している。

・ UKRI は、リスクベースのアプローチで評価されたプロジェクトの内容を踏まえ、助成を決定する前に様々なチェックを実施する。これには、助成の予定受領者と直接協議を行うことも含まれる場合がある。

・ プロジェクトパートナーが拠点とする国の民主的・倫理的価値観や法的枠組みを理解していることが重要である。

・ UKRI は、助成金の受領者がパートナー組織のガバナンスや所有構造、および当該組織と外国の政府機関や部局（民間・軍事問わず）との公式な連携の有無について調査を行っていることを期待する。こうした関係性が、プロジェクトの情報や成果物の取り扱いに関して潜在的なリスクをもたらす場合には、相応の管理策が講じられることを期待する。

・ 研究機関は、すべてのプロジェクトパートナーと正式な共同研究契約を締結し、データや資産（知的財産権等）が適切に管理されなければならない。その契約には、プロジェクトパートナーが関連する英国の法令を遵守する必要性を認識していることを確認する文言を含める必要がある。なお、共同研究契約には、いかなる条件下で、プロジェクトから得られた商業的に重要なデータや成果を公開できるかを明記すべきである。

(ii) サイバーセキュリティ

・ UKRI は、サイバー攻撃のリスクを最小限に抑えるため、研究機関が以下を備えていることを期待する。

- 十分に整備された管理策によって支えられた、強固なサイバーセキュリティ文化

- 職員や学生に十分周知されたガイダンスを含む、サイバーセキュリティに関する意識向上および研修プログラム

(iii) 知識および施設の共有

- 共同研究プロジェクトでは、相互の透明性と開放性が、研究とイノベーションの成功および利益の最大化にとって重要になる。UKRI は、研究組織がこの要件と商業上の要請、法令上の要件、および英国の国家安全保障上の要請とのバランスをとることを期待する。
- 研究組織は、プロジェクトパートナーと共有する情報や知識に十分注意を払うべきである。これは、他所で生成されたデータを解釈する際に研究者に提供する支援、研究組織が開発した施設、新しい技術の利用などにまで及ぶ。

(iv) データの取扱いとアクセス

- 情報交換に共有プラットフォームを使用する場合には、不正アクセスを防止するためアクセス制御を実施すべきである。
- データへのアクセスは、それを明確に必要とする者に対してのみ、必要とされる期間に限って付与すべきである。データの取扱いおよび利用の条件は、情報共有前に全ての当事者によって明確に定められ、理解・合意されていなければならない。特に、海外のパートナーに適用される現地法の中には、当局が全当事者の同意なく情報にアクセスできることを許すものがあるため、研究組織はそのような法令についても把握しておくことが期待される。

(v) 輸出管理

- 英国の輸出管理制度は、各種の技術・知識・戦略物資の輸出および伝達を制限する目的で設計されており、学術コミュニティにも他のいかなる輸出業者と同様に適用される。
- 各組織は、自身のプロジェクトや活動に適用されうる輸出管理について理解していることを確認すべきである。その際、以下の点に留意する。
  - 輸出管理規制は製品やサービスだけでなく、データやアルゴリズムにも適用される場合がある。
  - 「輸出」の概念には、英国外へのメール送信といった一見日常的な行為も含まれる場合がある。
  - 基礎的な科学研究に対する免除規定であっても、エンドユース（最終的な使用目的）やエンドユーザー、輸出先に懸念がある場合には適用されない。

2.3.4 まとめ

(1) 英国の大学における Trusted Research の取組に関する特徴

英国の 4 大学（インペリアル・カレッジ・ロンドン、オックスフォード大学、アストン大学、ウォーリック大学）における Trusted Research への取組は、調査した範囲では、以下のような共通の特徴が認められる。

(a) 強化されたデュー・ディリジェンス審査

4 つの英国の大学の事例から、共同研究先に関する質問票やトリアージ質問に基づく一次審査、段階毎の審査（国際共同研究の申請前、採択後～契約前、契約後～研究期間中）といった、しっかりとしたデュー・ディリジェンス審査が実施されていることを確認することができる。

以下、各大学におけるデュー・ディリジェンス審査の特徴を整理する。

(i) インペリアル・カレッジ・ロンドン

同大学におけるデュー・ディリジェンス審査の特徴として、①特に共同研究パートナーが見知らぬ相手の場合、研究者にチェックリスト（Trusted Research Checklist）を用いて共同研究を行う際のリスクについて認識させ、②共同研究の関係の構築に伴う広範囲のリスクを考慮して、研究責任者に「第三者機関の関係性レビュー質問票」に回答させ、③Research Office（研究事務局）が、「第三者機関の関係性レビュー質問票」に基づき、共同研究を行う第三者機関のリスク評価を行う、という 3 段階のアプローチを採用していることが挙げられる。

(ii) オックスフォード大学

同大学におけるデュー・ディリジェンス審査の特徴として、国際共同研究を行う場合にはデュー・ディリジェンスを実施することを義務化し、大学が国際研究パートナーシップを締結する前に、Strategic Partnership Scorecard（戦略的パートナーシップ・スコアカード）と呼ばれる評価シートを用いて、候補となる機関間パートナーシップについて徹底的かつ厳格な審査を受けることを保証していることが挙げられる。

(iii) アストン大学

同大学におけるデュー・ディリジェンス審査の特徴として、ステージ 1（国際共同研究の申請前）、ステージ 2（国際共同研究の採択後～契約前）、ステージ 3（契約後～研究期間中）の 3 段階で実施していることが挙げられる。

(iv) ウォーリック大学

同大学におけるデュー・ディリジェンス審査の特徴として、大学の運営や評判に対する予期せぬ、あるいは未特定のリスクの可能性を最小限に抑えることを狙いとして、資金提供者、共同研究者の経歴・所在地、研究の種類、研究者の経歴などを確認するために、研究者に向

けたトリアージ質問[300]等を用いてすべての研究活動について審査することが挙げられる

(b) 研究支援部門の役割

４つの英国の大学においては、以下に示すように、研究支援部門を中心とした、研究者が共同研究を行う際の研究セキュリティに関する幅広い支援体制が確立されている。

(i) インペリアル・カレッジ・ロンドン

同大学においては、Research Office（研究事務局）が、機密指定対象機関・輸出先国の確認、輸出許可申請書の作成、英国輸出管理局（ECJU）との連携、米国輸出管理規制、その他の輸出管理・研究セキュリティ関連事項について、個別対応の助言を提供している。また、Research Office には Research Security Team が設置されており、研究者への一次窓口として、研究セキュリティに係る質問や相談に対する体制を組んでいる。

(ii) オックスフォード大学

同大学においては、Research Service（研究サービス部門）内に、Trusted Research Team が設置されており、同チームが国際共同研究のコンプライアンス遵守を支援している。

また、Research Service は、研究者、学部支援スタッフ、学部長、研究サービス部門職員が参加できる「Trusted Research 」に関する相談会を定期的に開催している。

(iii) アストン大学

同大学においては、研究ガバナンス受信箱（Research Governance inbox）（電子メールでの連絡口）が設置されている。大学の研究倫理チームが、それを毎日確認しており、必要に応じて担当者や主要な関係者と連携する。

研究応募提案書の作成と承認プロセスの一環として、戦略的資金調達管理者（Strategic Funding Manager）が、研究者がデュー・ディリジェンスの手続きを完了することを支援する重要な役割を担っている。また、事業開発管理者（Business Development Manager）は、業界からの直接資金調達、Innovate UK 等への申請において、研究者がデュー・ディリジェンスのプロセスを完了するための支援を行うことできる。

(vi) ウォーリック大学

同大学においては、 R&IS（研究・インパクトサービス部門）が、Trusted Research に関連する大学のガイドラインおよびポリシーの大部分を管理・策定 している。また、同部門が、研究助成金・契約、研究戦略・開発、インパクト・イノベーション、倫理・研究ガバナンス等において、研究者に対して専門的な支援を提供している。

R&IS には、RG&C Team（研究ガバナンス・コンプライアンス・チーム）があり、研究、活動のあらゆる側面におけるコンプライアンスの日常的な責任を管理するとともに、大学

[300] 技術分野に関する質問で、非常に初期の段階で、新しいプロジェクトの提案が来た際、より堅牢なプロセスにかける必要があるか否かを判断することを目的とする。

全体にわたる規制分野における責任の一部を担っている。

(2) 英国の資金配分機関における Trusted Research の取組に関する特徴

英国の資金配分機関である UKRI は、TR&I（Trusted Research and Innovation）を、英国の知的財産、機微な研究、人材およびインフラを、潜在的な窃盗・悪用・搾取から保護する枠組みとして定義し、大学・研究機関が助成金を申請する際に、期待されるべき事項を示した「Trusted Research & Innovation: Principles and Expectations」を公表している。

UKRI は、TR&I はリスクベースで判断するものとし、助成先機関に対しては、リスクが高いと見なされたプロジェクトには、追加の緩和策や管理策の実施を求めること、助成の一環として要求される追加のリスク緩和策や管理策が、具体的かつ適切な範囲のものであり、理解可能で、助成金受給者が実行可能なものであること等といった原則を示していることが、大きな特徴として挙げることができる。

(3) 日本の大学にとって参考になると思われる点

英国の大学の事例から、日本の大学にとって参考となる点は以下のとおりである。

(a) 共同研究の申請に関する審査体制

英国の大学では、共同研究の申請については、研究支援・コンプライアンス部門が一次審査を担い、高リスク案件は上位決裁へエスカレーションする体制が整備されている。日本の大学においても、研究者による自己判断・自己申告のみに依拠するのではなく、研究支援部門が中心となる審査体制を明確化することが有効である。

(b) リスクに応じた段階的審査の導入

英国の大学では、全案件に一律の厳格手続を課すのではなく、リスクの程度に応じて審査の深度を調整する運用（例えば、簡易確認→追加確認→高リスク案件の深掘り）が採用されている。日本の大学でも、国際共同研究の申請・審査を効果的に行ううえで、想定されるリスクの大きさを踏まえた段階的審査の考え方を検討していく必要がある。

(c) デュー・ディリジェンスの実務化と記録の確保

例えば、アストン大学では、共同研究パートナーのデュー・ディリジェンスを実務手順として組み込み、判断根拠や手続を記録として残す仕組みを重視している。日本の大学においても、デュー・ディリジェンスを「実施した／実施していない」の確認に留めず、どの情報を参照し、どの基準で判断し、どの部署が関与したかを記録するといった仕組み作りを検討していく必要がある。

(d) 研修の体系化

例えば、ウォーリック大学においては、研究者だけではなく、研究支援職員、技術職員および博士課程の学生に焦点を置いて、研究セキュリティに関する研修・啓発を実施している。

日本の大学においても、研究者だけでなく、URA、研究支援職、契約担当等を含めた対象別研修を体系化し、「研究セキュリティ文化」を根付かせる取組を検討していく必要がある。

(4) 日本の資金配分機関にとって参考になると思われる点

英国の資金配分機関の事例から、日本の資金配分機関にとって参考となる点は以下のとおりである。

(a) 助成先機関が満たすべき研究セキュリティに関する期待事項の明確化

UKRI は、Trusted Research & Innovation の枠組みを「原則」と「期待事項」として提示し、助成先機関が組織として体制整備を進めることを促している。日本の助成機関においても、研究セキュリティを助成制度と接続させるため、助成先が満たすべき最低限の期待事項を明確にすることが必要である。

(b) リスクベース・比例原則の明示（研究の自由との均衡）

UKRI は、共同研究プロジェクト提案の応募に関して、リスクベースの考え方に基づき審査を行うが、リスク許容度や実施方法が応募機関によって異なることを踏まえて、リスクが高いと見なされたプロジェクトには、追加のリスク緩和・管理策の実施を求める考え方を示している。日本の資金配分機関においても、特定国の一律排除ではなく、想定されるリスクの大きさとリスク緩和・管理策を踏まえた評価に基づいて案件を採用する考え方について検討することが重要である。

2.4 オーストラリア

オーストラリアにおいては、研究セキュリティ・インテグリティに係る政策は、外国からの干渉リスク（Countering Foreign Interference：CFI）の文脈で展開されている。オーストラリアの特徴は、政府機関と大学機関等が共同して外国干渉からのリスクに対応するためのハブ機能である「University Foreign Interference Taskforce（大学外国干渉タスクフォース）」（以下、UFIT）を設置し、政府と大学機関・研究機関等との情報共有とガイドライン、実践事例等の蓄積を図っている。

オーストラリアの研究セキュリティ・インテグリティに係る主管省は、教育省（Department of Education）、内務省（Department of Home Affairs）を中心に、法務省（Attorney-General's Department）、国防省（Depart of Defence）および国防省傘下のオーストラリア通信情報局〈Australian Signals Directorate：ASD〉、外務貿易省（Department of Foreign Affairs and Trade：DFAT）である。

中心的な役割を担う内務省は、省内の外国干渉対策調整センター（Counter Foreign Interference Coordination Centre: CFICC）が UFIT の運営事務局として実務全般を支えている[301]。また、情報機関であるオーストラリア安全情報機構（Australian Security Intelligence Organisation: ASIO）、オーストラリア通信情報局（Australian Signals Directorate: ASD）と大学セクターの情報共有を図る役割を担っている。

また、教育省は、大学セクターのカウンターパートとして UFIT が策定するガイドライン等の運用を支え、リスク環境の理解を深めるため関係団体との協働、オーストラリアの大学セクターにおける外国干渉対策ガイドラインの実施状況の監視、大学の緩和策の支援に向けたリソースと指針の開発等を担っている[302]。2022 年 10 月に政府は、TEQSA（オーストラリア高等教育質・基準機構）内に Higher Education Integrity Unit（高等教育インテグリティユニット）を新設した[303]。同ユニットは、大学セクターおよび政府機関と連携し、大学セクター内で生じる新たなインテグリティリスクを特定・対応する能力を強化するもので、アカデミックインテグリティ、入学基準・情報、学生の安全、詐欺・汚職等の注力分野に加え、サイバーセキュリティ、外国干渉、研究インテグリティ等の高等教育に関連するインテグリティの脅威に対して、主要な責任を有する政府機関との協働を図っている[304]。

---

[301] オーストラリア内務省（2024）「Countering Foreign Interference in Australia - Working together towards a more secure Australia」(https://www.homeaffairs.gov.au/nat-security/files/cfi-australia.pdf)

[302] オーストラリア教育省「Countering Foreign Interference in the Australian University Sector」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector)

[303] オーストラリア TEQSA Higher Education Integrity Unit (https://www.teqsa.gov.au/about-us/teqsa-overview/higher-education-integrity-unit)

[304] オーストラリア TEQSA は、国内の全ての高等教育機関を監視・規制する連邦政府の独立機関（教育省に属する非法人連邦政府機関〈Non-corporate Commonwealth entity〉）である。2024 年 2 月に「Guidance Note: Academic and Research Integrity-Version 2.0.（ガイダンスノート：学術的研究インテグリティ-バージョン 2.0.）」では、学術不正、研究不正、第三者の提供／委託を含むガバナンス、訓練、記録管理等が中心であり、外国干渉リスクのガイダンスの記載はない。他方、高等教育機関が自ら高等教育基準の枠組みを遵守しているか体系的に評価する「自己保証報告書（Self-assurance report）では、サイバーセキュリティ、外国干渉についてオーストラリア通信情報局の「Strategies to mitigate cyber security incidents（サイバーセキュリティインシデント軽減戦略）」、TEQSA の「Compliance in

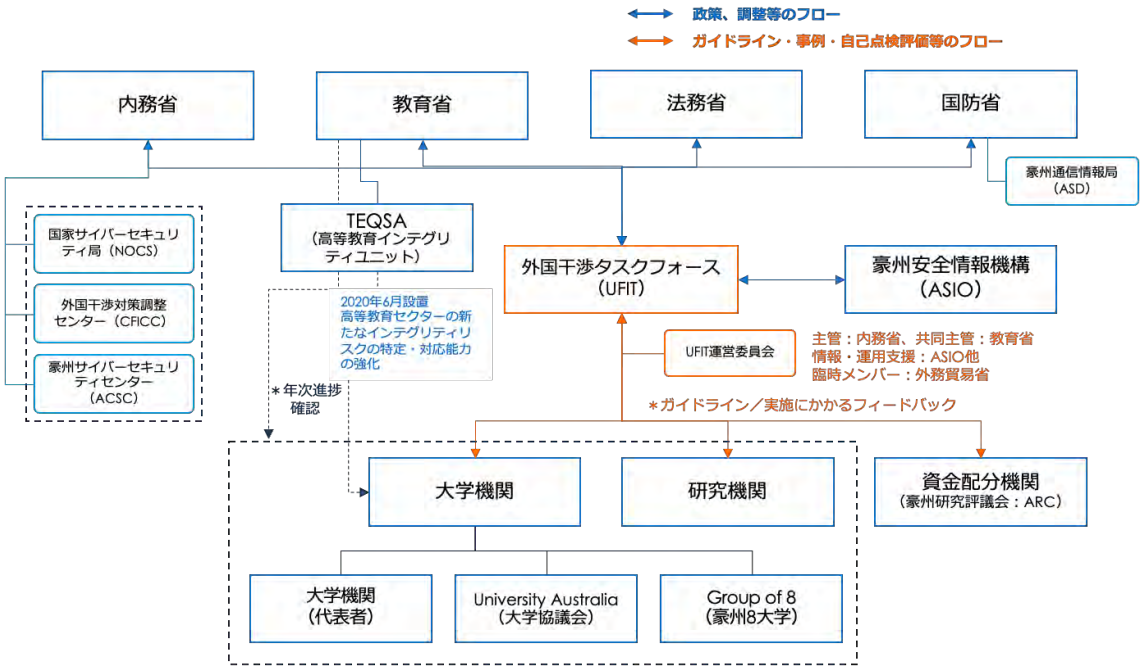


図 2-8　オーストラリアの研究セキュリティ・インテグリティ関係機関間の関連性と文書等のフロー

出典：オーストラリア内務省、オーストラリア教育省、UFIT の情報を元に未来工学研究所作成.

2.4.1　研究セキュリティ・インテグリティ関連政策動向

(1)　2024 年度までの経緯

オーストラリアでは、研究セキュリティ・インテグリティについて、高等教育機関や研究機関が直面するサイバー上でのスパイ活動、外国からの干渉、情報盗取、意思決定への影響、中国の大学と防衛研究、防衛科学者との関係について懸念され、教育大臣ダン・ティーハン氏が外国干渉リスクに関する政府と大学の連携強化を目的に、2019 年 8 月 28 日に大学外国干渉対策タスクフォース（UFIT）の設置を正式に公表した。前述のとおり UFIT[305,306]の運営委員会は、内務省委員長と連携し、政策策定を含む政府と大学間の対外外国干渉関連問題（Countering foreign interference）の主要な窓口として機能し、当該問題における政府と大学セクター間の連携・協力モデルの維持を担当している。

UFIT は、政府、大学、研究機関が参加するタスクフォースであり、学術協力と学問の自由を維持しつつ、大学が外国干渉のリスクを特定・評価・軽減するために、ガイドライン等を

focus: Cyber security」を検討することを推奨している。

[305] UFIT は、政府と大学・研究機関が共同で設立した組織（共同イニシアチブ）であり、サイバーセキュリティ、研究と知的財産、国際協調、文化とコミュニケーションの 4 つを戦略分野としてガイドライン等を検討している。UFIT 運営委員会は、内務省の外国干渉対策政策の担当（オーストラリア安全情報機構：ASIO）が主導する。組織の位置付けは、法定外諮問機関であり、教育大臣が設置主体となっている。ガイドラインの公開、大学との連携、教育分野における政策対応は、教育省が担っている。

[306] Australian government Directory「University Foreign Interference Taskforce」（https://www.directory.gov.au/portfolios/home-affairs/university-foreign-interference-taskforce）

策定している。

〈研究セキュリティ・インテグリティの 2024 年以前の取り組み〉

- 2019 年 8 月：University Foreign Interference Taskforce（UFIT）の設置
- 2019 年 11 月：UFIT「Guidelines to Counter Foreign Interference in the Australian University Sector」[307]の策定〔UFIT ガイドライン〕　※2021 年 11 月、改訂ガイドラインの公表
- 2023 年 8 月 : 教育省「Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector（UFIT ガイドライン実施状況報告書）」
- 2024 年 4-5 月：教育省「Pulse Check on the implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector」（オーストラリア大学セクターにおける外国干渉対策ガイドラインの実施状況に関する進捗確認）

教育省（2023）の「UFIT ガイドライン実施状況報告書」[308]では、大学の成功事例と障壁を把握するため、UFIT ガイドラインで大学部門が実施した広範な取り組みについての年次の実施状況を取りまとめたものである。同報告書では、大学のリスク管理フレームワークの強化とそれを支える内部ガイドライン等の資料の開発状況の報告、ガイドラインの評価を行った。ガイドラインの評価では、他大学との連携とコミュニケーション強化の推進要因、大学におけるサイバーセキュリティの重要性の認識の向上、外国干渉に対抗する課題に対して協調的なアプローチを実施するためのロードマップを提供したことをあげた。

[307] オーストラリア教育省, UFIT ガイドライン（https://www.education.gov.au/countering-foreign-interference-australian-university-sector/guidelines-counter-foreign-interference-australian-university-sector）
[308] オーストラリア教育省「Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector」（https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/report-implementation-guidelines-counter-foreign-interference-australian-university-sector）

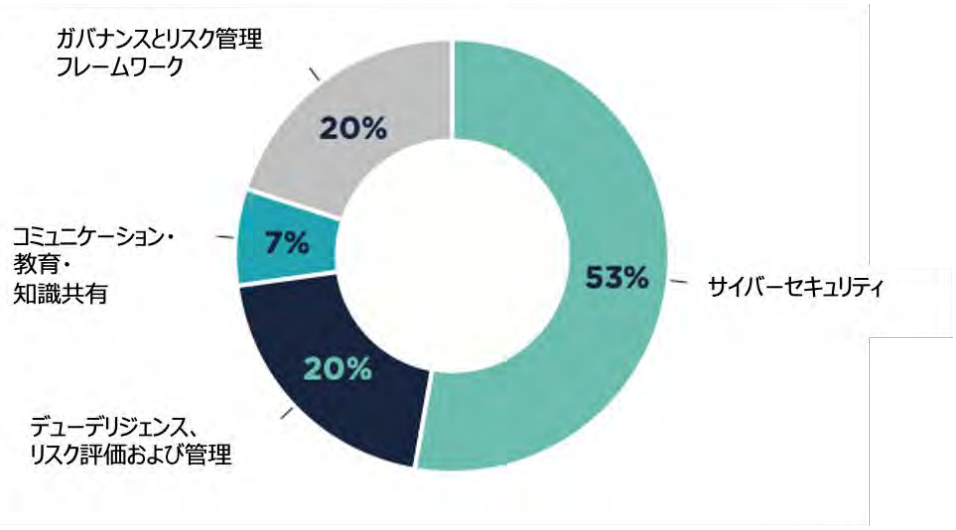


図 2-9　ガイドラインの最も重要な柱（投資額の割合）
出典：オーストラリア教育省「Consultation on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector」<https://www.education.gov.au/download/18010/consultation-implementation-guidelines-placemat/36841/document/pdf>

教育省（2024）の「オーストラリア大学セクターにおける外国干渉対策ガイドラインの実施状況に関する進捗確認」[309]は、2023 年 8 月に公表された「UFIT ガイドライン実施状況報告書」（上記）を踏まえ、本報告では教育省は全 42 のオーストラリアの大学に対して、過去 12 ヶ月間のガイドラインの実施状況に関する調査〈年次進捗確認調査〉（各大学の自己申告形式）[310]を実施し、リスク環境への理解の深化を目的とした「外国干渉対策ワークショップシリーズ」を全国で開催した。年次進捗確認調査では、調査回答機関の約半数（49%）で、ガイドライン実施における新たな障壁・顕在化した課題を経験したとし、具体的には、大学がデュー・ディリジェンス実施の困難さ（情報・専門知識へのアクセス、時間・リソースの負担、提携機関の方針への対応）が 28%、規制や報告要件の進化に伴うコンプライアンス負担の拡大が 26%、より多くのリソースの必要性（ガイドラインの運用実施を導くための研修、ブリーフィング、事例研究等）が 26%であった。また、政府による追加ガイダンスを必要とする部分として、デュー・ディリジェンスとリスク評価に関する追加ガイダンスが最も多く、次いで外国干渉脅威ブリーフィングであった。また、教育省は、大学セクターを対象に「外国干渉対策ワークショップシリーズ」を実施し、ブリスベン、メルボルン、

309 オーストラリア教育省「Pulse Check on the implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector」（https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/pulse-check-implementation-guidelines-counter-foreign-interference-australian-university-sector）
310 年次進捗調査は、2023 年 4 月から 2024 年 4 月までのガイドライン実施進捗を評価したものである。調査では、ガイドライン実施に関する大学からのフィードバックを得るため、A）外国干渉リスクへの対応策・主要な措置、B）ガイドライン実施上の新たな障壁・顕在化した課題、C）投資面におけるガイドラインの最も重要な柱（大学が最も多くの資源を投入した分野）、D）実践コミュニティを含む政府による追加手段、E）大学が政府に更なるガイダンスを求めている分野からなる。39 大学から回答が寄せられた。

パース、シドニー、およびオンラインで実施した[311]。本ワークショップシリーズは、内務省内の国家サイバーセキュリティ局（NOCS）、外国干渉対策調整センター（CFICC）、オーストラリアサイバーセキュリティセンター（ACSC）と連携して実施している。ワークショップでは、教育省が作成する事例研究の参考となるよう、大学機関は外国干渉リスク管理に対する独自の視点やアプローチを共有し、国家安全保障の枠組みを運用する経験に基づくフィードバックを提供した。

【「外国干渉対策ガイドラインの実施状況に関する進捗確認」で得られた主な知見】

- 過去 12 ヶ月間、92%の大学が外国干渉リスク（Foreign interference risk）への耐性を強化する主要施策を新設または改良した。
- 52%の大学が過去 12 ヶ月間で最も多くの資源を投入したガイドラインの柱としてサイバーセキュリティを挙げた。
- 大学は他大学や政府との連携強化によるベストプラクティス共有を歓迎し、97%が省庁主導の「実践コミュニティフォーラム」への関心を表明した。
- 大学から、さらなるデュー・ディリジェンスとリスク評価のガイダンスを求める声が一般的であり、政府助言がガイドラインの実施において有益であるとする意見も 26%占めると報告された。
- 49%の大学が、ガイドライン実施において、新たな障壁や課題に直面していると報告されており、その多くはリソース面が挙げられた。

(2) 最近の主な動き

(a) UFIT における各種文書の公表

UFIT は、2025 年 2 月に大学がガイドラインの各構成要素を実施する際に役立つよう、ガイドラインの項目別（ガバナンスとリスク管理の枠組み、コミュニケーション・教育・知識共有、デュー・ディリジェンス・リスク評価・管理）にガイドラインノート、ケーススタディ、自己評価報告書を公表した。

311 本ワークショップシリーズには、招待された 42 大学のうち 36 大学を代表する大学関係者 113 名が参加した。

表 2-10　UFIT ガイドラインの実施のための補足資料等

項目	資料の位置づけ	資料種類	資料概要
ⅰ）ガバナンスとリスク管理の枠組み	大学が外国干渉に関する考慮事項を既存の枠組み、方針、手続きに統合できるよう設計された資料	ガイダンスノート（2025 年 2 月）	大学が外国干渉リスクを管理するために必要となる要素を整理し、外国干渉の典型例や外国干渉がもたらすリスクと結果等を示し、大学機関での実装に向けた補足資料
		事例研究（2025 年 2 月）	大学における運用と意思決定者が具体的な状況でどのような判断・対応を行うべきかの参考事例
		自己評価（2025 年 2 月）	大学内の組織的・実務的な実装状況を点検するための設問集（質問形式）
ⅱ）コミュニケーション、教育、知識共有	大学が自由な意見交換を促進しつつ、外国干渉への認識を高める文化を支援することを推奨するための資料	ガイダンスノート（2025 年 2 月）	外国干渉リスクに対して、知識共有・効果的なコミュニケーション・教育支援により、ポジティブなセキュリティ文化を醸成するための資料
		自己評価（2025 年 2 月）	大学の実装状況を自己点検するための設問集。周知計画・教育プログラム、高リスク層への研修、知識共有の３テーマで整理
ⅲ）デュー・ディリジェンス、リスク評価および管理	包括的なリスク評価により、国際的な関与における外国干渉への曝露と発生可能性を低減できる。本ガイドラインは大学が継続的な開示と透明性の文化を育むことを推奨するための資料	ガイダンスノート（2025 年 2 月）	大学がどのように制度設計・運用すべきかを理解するための補助資料。リスク管理、デュー・ディリジェンス実施を支えるツール／情報源、技術・研究内容の評価からなる
		事例研究（2025 年 2 月）	想定事案として「国家安全の保護」（群制御研究事案）、「利益相反の申告」（先端電池）、「強化デュー・ディリジェンスの実施」（投資家候補の紹介事案）等をもとに大学が行ったデュー・ディリジェンス／リスク評価・管理を提示
		自己評価（2025 年 2 月）	相手先・関係者の評価、技術・研究内容の評価、包括的リスク評価と緩和策、承認・監査・継続的評価からなる
		デュー・ディリジェンス支援フレームワーク（2021 年 11 月）	グローバルな研究協力の潜在的機会のデュー・ディリジェンス評価を実施する際に、潜在的な外国干渉リスクを認識するためのプロセスマップ（「パートナーを検討する」、「技術を検討する」からなるチェックリストとフレームの提示）
		オープンソース情報ファクトシート（2021 年 9 月）	大学が公開情報または「オープンソース」情報の収集と分析を通じて、既存のデュー・ディリジェンスプロセスを強化する方法を概説。

項目	資料の位置づけ	資料種類	資料概要
ⅳ）サイバーセキュリティ	本ガイドラインは、情報システムを不正アクセス、改ざん、妨害、損害から保護する強固なサイバーセキュリティ対策の重要性を示した資料	ガイダンスノート（2025 年 2 月）	大学がサイバーセキュリティ対策を整備・実装するための助言資料。デジタル資産の把握と重要度の理解、サイバー脅威のモデリングの実施、大学全体のサイバー戦略の実装、研究者・学生・職員への意識向上、研究コミュニティへの参加等のアプローチを提示
		事例研究（2025 年 2 月）	「オーストラリア大学に在籍する博士課程学生の専門分野の海外学会への参加招待」に対して大学が検討すべき事項を提示（ナラティブな事例を提示し、学内においてコミュニケーション、リモートアクセスの慣行・ポリシー、アクセスと出張、システム管理、輸出管理、出張承認の検討・見直しを促す）
		サイバーセキュリティ強化報告書（2023 年 4 月）	サイバーセキュリティ脅威に対するオーストラリア大学セクターの能力を高めるため、サイバーセキュリティフォーラム（TCSF）における議論、ベストプラクティス・ガイドラインと青写真の策定、各大学における脅威インテリジェンスの共有と大学セクターのサイバーセキュリティ実践と態勢に関するベースラインおよび成熟度調査等を実施した。

出典：UFIT ガイドライン HP より未来工学研究所作成.（https://www.education.gov.au/countering-foreign-interference-australian-university-sector/guidelines-counter-foreign-interference-australian-university-sector）

ガイダンスノート（大学意思決定者向け点検項目）

ガイダンスノートは、大学意思決定者向けの点検項目を示したもので、UFIT ガイドラインの解釈や実装支援に向けた補足資料である。

「ガイダンスノート：ガバナンスとリスク管理の枠組み」（Guidance note: Governance and risk frameworks）[312]では、ガバナンス・リスク管理の枠組みを導入する際の基本的な要素として、①外国干渉がどのように発生し得るかの認識（Awareness）、②大学活動に関連する潜在的リスクと結果の特定（Consequences）、③大学リスク対策への責任の所在（Accountable authority）、④リスク軽減のための方針・手続きの整備（Policies and procedures）、⑤透明性のあるエスカレーション（escalation）・報告（reporting）体制の構築の５つに整理している。

また、外国干渉の発生可能性のある事例として、ⅰ）外国代表団、セミナー、共同研究、財政支援等を通じて学生や教職員から機密情報や機微情報等の情報を不正に入手する試み、ⅱ）外国主体の利益を促進するため、大学院研究課程の学生を含む学生・教職員を不適切に

[312] オーストラリア教育省「Guidance note: Governance and risk frameworks」（https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/governance-guidance-note）

標的とし勧誘すること、iii）学術的自由や大学の価値観・行動規範に反する外国関係者の行為（学術プログラムの変更の要求・誘導行為等）、iv）大学の研究計画を特定の研究分野に変更・誘導しようとする不適切な試み、v）資金提供や共同研究、個人を対象とした金銭的・その他誘因を通じた特定人物・活動領域・研究成果への不適切なアクセスや影響力を求める行為、vi）ネットワーク脆弱性の悪用や不正アクセスによるサイバー標的化等を挙げた。大学の外国干渉リスクの例では、研究・機密データ・個人データの望ましくないアクセス及び干渉の可能性、将来のパートナーシップ・共同研究・人材誘致の喪失、法的義務の違反、知的財産・商業化の機会の喪失、情報収集目的での大学コミュニティの育成、授業内外における特定の課題への不当な影響力等とした。

これらは、機関・研究者・研究チームの評判に損害を与えるとともに、研究結果やデータの信頼性・公正性に対する公衆やパートナーの信頼喪失等をもたらし、潜在的な収益の喪失や将来の資金調達機会の不適格化等の結果をもたらす。このため、大学の外国干渉リスク対策を担う責任当局には、副学長、最高情報セキュリティ責任者、その他上級職員、大学レベルの上級委員会等による執行機関を挙げており、大学の執行会議・プロジェクト委員会などで外国干渉を常設議題（standing agenda item）にすることを推奨している。

また、規程・ポリシーに盛り込むべき推奨要素として、キャンパス内の個人に対する嫌がらせや威圧等の行動規範に違反する行為から全ての学生及び教職員を保護する大学行動規範（言論の自由／学問の自由との整合性、学術的貢献を理由とした個人情報の暴露・標的化等の活動への対応）、学外・海外・国際的な教育提供に特有の問題への配慮、大学の方針に沿った外国干渉に関する申し立ての慎重な管理、学生・教職員双方の不当な影響力・嫌がらせ・威圧から保護する仕組み（機微なテーマを扱う際の学術成果物・評価の匿名化）、大学がリスクのある情報・資産へのアクセス権を付与する前に学生・教職員が外国干渉リスクと軽減策を理解しているかを確認する仕組み等を挙げた。

「ガイダンスノート：コミュニケーション、教育、知識共有」（Guidance note: Communication, education and knowledge sharing）[313]では、大学の意思決定者が自大学におけるコミュニケーション、教育、知識共有の実施状況を評価するための一連の質問を提示した。大学が外国干渉リスクに対処し、安全とウェルビーイングを支援するには、知識共有プログラムの確立、効果的なコミュニケーションの確立、教育支援の提供が必要となる。本資料では、「コミュニケーション計画と教育プログラム」、「外国干渉リスク対象者向け研修」について行動例や検討事項を提示している。「コミュニケーション計画と教育プログラム」では、外国干渉への認識を高めるために大学が実施できる行動例として、i）学生・教職員が外国干渉と大学への含意を学ぶ機会の提供、ii）授業内でセンシティブな議論や個人への嫌がらせ・威圧の軽減について扱えるよう教員へのトレーニング、iii）苦情申立プロセスや機密事項の相談を含む大学の苦情処理手順の情報について全学生・教職員が容易にアクセスすることを可能にすること、iv）学生・教職員に対する嫌がらせ、威圧、脅迫の申し

313 オーストラリア教育省「Guidance note: Communication, education and knowledge sharing」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/communication-guidance-note)

立てに対し、担当局の苦情・インシデント・対応を追跡すること、ｖ）外国干渉を論じる資料において言論の自由及び学問の自由の方針を関連付けること（科学的方法の基盤となる厳密な議論や思想対立と外国干渉の試みを区別）、vi）大学執行部と学生代表等との定期的対話を行い、外国干渉に関連する懸念事項や情報を議論すること、vii）学生・教職員の理解度の測定を提示した。

「外国干渉リスク対象者向け研修」では、研究者が自身の研究活動や国際共同研究が外国干渉の標的となり得る点を考慮するため、ｉ）研究者自身の研究活動や国際共同研究の結果が影響を与える対象とは何か、ii）どのような影響が考えられるか、iii）研究分野ゆえに標的となりうる対象は何か、iii）研究者自身の研究や外国との共同研究について他に考慮すべき事項は何かを論点に研修を行うことを提示した。大学セクターには、これらの取組を通じて、セクター全体の専門性を高めるため、セクター全体のフォーラム、ワークショップ、実践コミュニティへの参加により外国干渉対策に関する知識体系への積極的な貢献を推奨している。

「ガイダンスノート：デュー・ディリジェンス・リスク管理」（Guidance note: Due diligence, risk assessments and management）[314]は、大学がデュー・ディリジェンス、リスク評価および管理をどのように策定・実施できるかの理解を支援するための資料である。大学のデュー・ディリジェンス、リスク評価・管理は、リスクを特定したからといって活動を中止すべきとは限らず、国際的な関係や部局から申告しやすい文化・仕組みを整え、リスクを管理・緩和することを主眼とすべきとしている。デュー・ディリジェンスの実施を支えるツールとして、オーストラリア政府側の各種リソース[315]を活用して、大学が国際的な連携相手、活動のリスクを見極めることを推奨している。また、大学のデュー・ディリジェンスを学内情報だけで完結させずに、政府の制度、データベース、枠組み等と接続させることを強調している。

「ガイダンスノート：サイバーセキュリティ」（Guidance note: Cybersecurity）[316]では、大学がサイバーセキュリティを実践できるよう整備・実装するための助言資料であり、デジタル資産の把握と重要度（criticality）の理解、サイバー脅威のモデリングの実施、大学全体のサイバー戦略の実装、研究者・学生・職員への意識向上、実務コミュニティへの参加等のアプローチを提示している。また、参考としてオーストラリアの国家戦略やオーストラリアの「Australian Cyber Security Strategy 2023-2030」、「ACSC Annual Cyber Threat Report 2023-24」等の脅威レポートを理解することの有用性を示している。ガイダンスノートでは、サイバー対策の出発点として、資産の重要度の理解と比例的な投資・実装計画、脅

314 オーストラリア教育省「Guidance note: Due diligence, risk assessments and management」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/due-diligence-guidance-note)

315 「ガイダンスノート：デュー・ディリジェンス・リスク管理」では、オーストラリア政府機関が提供するツールとして、ASIO のデュー・ディリジェンス・インテグリティツール、UFIT のデュー・ディリジェンス支援フレームワークやファクトシート、外国影響力透明性スキーム（FITS）、オーストラリア制裁対象者・団体リスト、防衛輸出管理（DEC）等を挙げている。

316 オーストラリア教育省「Guidance note: Cybersecurity」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/cybersecurity-guidance-note)

威モデリングに基づく資産–脅威主体–攻撃手法を結び段階的な介入を可能にすること、大学の全体戦略の進捗・測定の重要性、セクター横断の情報共有を通じた共通課題への対処の必要性を挙げた。

事例研究（各大学が外国干渉リスク対策を開発するための参考事例）

UFIT では、大学が「ガバナンスとリスク管理の枠組み」[317]、「デュー・ディリジェンス、リスク評価および管理」[318]、「サイバーセキュリティ」[319]をどのように開発・実施できるかを理解するための事例を提供している。各事例研究は、多くの事例が提示されているものではなく、様々なタイプの事例を提示し、大学が外国干渉リスクを検討していく上での参照情報の位置づけである。各事例研究のうち、研究セキュリティに係る事例を下表に示す。

表 2-11　UFIT ガイドライン補足資料（事例研究〈研究活動に関する事例〉の概要）

項目	事例	大学の対応
ｉ）ガバナンスとリスク管理の枠組み	**事例 4：不当な影響力の報告** オーストラリアの大学教員が、外国の COVID-19 対応に関する論文を発表し、深刻な状況を予測した。当該外国の領事館は、より高位の同国人教員を大学に派遣し、論文が外国政府を批判し恥をかかせたとして、論文の撤回と公的な謝罪を要求するよう働きかけた。大学は領事館の撤回・謝罪要求を拒否。言論の自由と学問の自由を強く重視し、研究と論文は厳格な査読を経ていると判断した。 当該研究者が 1 週間後、大量の誹謗中傷メッセージを受け取り、個人情報や連絡先がオンラインで拡散。大学の SNS にも当該研究者への苦情を寄せられた。	• 研究者はサイバー虐待を大学のセキュリティチームと eSafety コミッショナーに報告。指導のもと証拠保全措置を講じ、警察への通報可能性を検討。不要な接触を遮断し、ソーシャルメディアプラットフォームに内容を報告。自身の SNS プライバシー・セキュリティ設定を更新し、大学ウェブサイトから研究者の連絡先情報を一時削除した。 • 大学は法執行機関を含む適切な政府機関と連携し、専門的な助言と支援を要請した。 • 大学のソーシャルメディアページにおける当該教員への苦情を受け、大学はソーシャルメディアプラットフォーム上で声明を発表。言論の自由と学問の自由へのコミットメントを表明するとともに、サイバー虐待は容認できず、大学がこうした事案を調査することを明言した。

317 オーストラリア教育省「Case studies: Governance and risk frameworks」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/governance-case-studies)
318 オーストラリア教育省「Case Studies: Due diligence, risk assessments and management」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/due-diligence-case-studies)
319 オーストラリア教育省「Case Study: Cybersecurity」(https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/case-study-cybersecurity)

項目	事例	大学の対応
iii）デュー・ディリジェンス、リスク評価および管理	**事例１：国家安全保障の保護** あるオーストラリア大学教授（工学・情報技術）は、群衆システムを専門とし、同大学にて公的資金による農業応用向け群衆システムプロジェクトに従事している。教授は長年同大学に在籍してきた。	大学によるデュー・ディリジェンス調査を実施し、本研究を特に高リスクと評価し、研究内容・大学の評判・オーストラリアの国益を保護するため、既存のリスク軽減策の強化措置を講じた。 • 大学が定める利益相反申告プロセス（全職員が副業及び外国政府との関連を申告義務） • 参加の教職員・学生の職歴及び経歴調査 • 研究へのアクセス管理強化（リモートアクセスを含む） 大学のデュー・ディリジェンス評価の実施（当該教授が海外人材招へいプログラムに参加し、現在、外国軍事大学の教授職にあること、学部長または教授が予定通り海外出張から帰国していないこと） ⇒大学は規定違反と判断
	事例２：利益相反の申告 クリーンエネルギー向け先進電池を専門とするオーストラリアの大学の教授が、外国の大学から再生可能エネルギーセンターの名誉教授就任の打診を受ける。外国大学は、教授が研究プロジェクトに参加し講義を行うこと、および年間３ヶ月分の旅費を負担することを提案した。 当該大学の副業規定では、利益相反を考慮した全ての副業について承認が必要とされている。	大学は、副業申請審査を実施。申請審査では以下の点が考慮された。 • 先進電池技術は同大学が世界をリードする分野であり、国際的なパートナーから高い関心を集めている • 防衛輸出管理部門と連携し、先進電池技術の輸出管理上の地位及び物理的輸出ならびにオーストラリア外への技術電子供給の許可が必要な事例の把握 • 当該外国は先進電池研究において世界をリードしており、同大学との連携は本学の先進電池技術における地位向上に寄与する。 • 外国大学との提案契約にデータ共有・開示に関する包括的条項が含まれている • 関連知的財産の所有権・保護を含む強固な契約上の取り決め • 教授は本学の利益相反ポリシーに沿って、利益相反の特定・申告・管理の義務を負っている ⇒大学は教授の海外活動による利益が、研究の公表・保護・商業化に関する大学の権利が損なわれるリスクを上回ると判断し客員教授職を受諾した。
iv）サイバーセキュリティ	**事例：研究の保護** オーストラリアの大学に在籍する博士課程の学生が、専門分野の海外学会への参加を招待された（ニュージーランドの大学と共同で進めている農業用ドローンの新機能に関する研究）。研究は最終試験段階で特許作成中。	大学は以下の事項を検討し優先順位をつける必要がある。 • システムへの公開リンクがもたらす敵対的なサイバーセキュリティ脅威 • 大学内の研究チームとの連絡調整 • ニュージーランドの大学およびその研究パートナーとの連絡管理 • 大学の評判への損害

項目	事例	大学の対応
	渡航費は会議主催者（外国政府機関）が負担し、博士課程学生の航空券・宿泊費・食事代・諸経費が全額支給される。学生は発表資料を持参し、現在の研究のライブ実演を行うよう要請された。 学生は第三国へ渡航し、大学のノートパソコンを持ち込み、プレゼンテーション中にリモートアクセスカードで自身のアカウントにログインする。その際、外国の工作員がリモートアクセス情報を盗み取り、大学のシステムと学生の研究データへの恒久的なアクセス経路を確立する。 帰国後 1 ヶ月以内に、学生の研究は複製されプロトタイプが開発され、一般市場に出回る。	• ニュージーランドの提携大学の評判への損害 • 輸出管理対象技術が物理的または電子的にオーストラリア国外へ持ち出されたか、またオーストラリアの輸出管理法が違反された可能性があるか • 大学への商業的損失 オーストラリア安全情報機構（ASIO）及びオーストラリアサイバーセキュリティセンター（ACSC）に支援を要請。リモートアクセスサービスの停止。（※リモートアクセスサービスの停止は、学内の数百名の教職員と数千名の学生に影響した） ニュージランドの大学の学長、パートナー企業へのセキュリティ侵害と結果の報告。侵害可能性の調査依頼。 ⇒大学の手順の見直し（コミュニケーション、リモートアクセス、アクセスと出張、システム管理、輸出管理、出張承認）

(b) 政府機関の取組

オーストラリア政府は、先に述べた通り、研究セキュリティを確保するための取組みとして、2019 年に大学外国干渉対策タスクフォース（UFIT）を設立し、UFIT ガイドラインを策定した。同ガイドラインは、2021 年に脅威の評価の進展とセクターの実践的な教訓を反映した改定ガイドラインを公表した。UFIT ガイドラインの実施状況については、教育省により進捗確認（Pulse check）が行われ、大学セクター、政府機関等との協議を通じて得られたものの蓄積を図るとともに、外国からの干渉に対応するためのワークショップシリーズ等を展開している。

大学の研究セキュリティに係る政府の制度については、外務貿易省（DFAT）が「Foreign Arrangements Scheme（外国関係手配制度）」（以下、FAS）を制定している。同制度は、「Australia's Foreign Relations (State and Territory Arrangements) Act 2020（2020 年対外関係（州・準州協定）法）」[320]に基づくもので、オーストラリアの外交関係を保護・管理するため、FAS の下、特定の「外国機関」との全ての協定は、外務大臣への登録が必要としたものである。同制度は、DFAT が管理する法定通知・審査プロセスとして実施され、オーストラリアの全ての公立大学に適用されている。外国との取り決めの種類は、①大学間の研究協力、②学生交換・移動プログラムの設立、③ワークショップや学会発表における学者の共同研究、④文化活動の手配にわたる。

[320] Australia's Foreign Relations (State and Territory Arrangements) Act 2020 は、オーストラリアの州・準州政府、地方自治体、公立大学が外国政府（機関を含む）と締結する取り決め（MOU 等）について、連邦政府が審査し、「国の外交政策と矛盾する」、「外交関係二悪影響を与える」と判断した場合は無効化・破棄できる権利を外務大事に与える制度である。2021 年１月に施行.
(https://www.legislation.gov.au/F2020L01569/asmade/text)

FAS 以外では、連邦政府は、外国との取り決め、外国主体との特定の活動に対する透明性の確保として、2018 年には「Foreign Influence Transparency Scheme Act 2018（外国影響力透明性制度法 2018）」に基づき、「Foreign Influence Transparency Scheme（外国影響力透明性制度）」（以下、FITS）が施行された[321]。FITS は、「外国主体」と特定された個人又は組織に代わって特定の活動を行う（行うことに合意する者）に対し、登録義務その他の義務を課す制度である。関連する活動や取り決めはオンライン登録簿に掲載され一般に公開される。制度の対象者は、例えば、大学での業務が外国の学者、組織、機関、政府と関わる場合、FITS に基づく登録が必要な活動に従事している可能性がある。また、FITS に準拠するためには、オーストラリア政府に活動または取り決めを登録する必要がある場合がある。具体的には、活動実施者の身元、外国委託者の身元、外国委託者と活動実施者との関係性の性質、活動内容と目的等を登録する。

2.4.2 大学・研究機関における取組

(1) オーストラリア国立大学（Australian National University）

(a) 背景・経緯等

オーストラリア国立大学では、2019 年 11 月に公表された UFIT ガイドラインを踏まえ、2020 年 4 月に学内の UFIT ガイドラインへの対応作業を開始した。同大学の外国干渉対策の整備に向けて、研究・イノベーション担当副学長（DVC Research & Innovation）、最高情報セキュリティ責任者（Chief Information Security Officer：CISO）が主導し、大学研究委員会（University Research Committee：URC）が監督している。2020 年 6 月には、URC は外国干渉諮問委員会（Foreign Interference Advisory Committee： FIAC）の設置を承認し、2020 年 12 月に学術委員会（Academic Board）に進捗報告が行われ、研究サービス部門と国際戦略・パートナーシップチームが FIAC への案件付託を担当することが確認された[322]。

オーストラリア国立大学では、研究・イノベーション担当副学長であるラクラン・ブラックホール（Lachlan Blackhall）教授をサポートするため、研究情報サービス部（Office of Research and Information Service）にて、大学の戦略的目標をサポートするため、研究サービスの運営と管理におけるリーダーシップ、助言、サポートを提供している。研究情報サービス部では、ブラックホール教授をサポートし、研究・イノベーションポートフォリオの他の副学長室（大学院研究担当および研究イニシアティブ・インフラストラクチャー担当）や研究パートナーシップ・トランスレーション室（ANU エンタープライズを含む）と緊密

321 Foreign Influence Transparency Scheme (https://www.dfat.gov.au/international-relations/Pages/foreign-influence-transparency-scheme#:~:text=Australian%20Volunteers%20Program,matching%20them%20with%20skilled%20Australians.)

322 オーストラリア会計検査院（ANAO）「Australian National University's Governance and Control Framework」, pp.50-51, 2021. (https://www.anao.gov.au/sites/default/files/Auditor-General_Report_2021-22_11.pdf)

に連携している。研究情報サービス部は、獣医サービスチーム、研究システムチーム、研究倫理チーム、研究データ品質室、研究契約室、研究コンプライアンス・インテグリティ室、研究分析室からなり、研究セキュリティに係る取組みは、研究コンプライアンス・インテグリティ室が担っている。コンプライアンスチームでは、防衛輸出管理、外国干渉、外国との取決め、研究インテグリティに関する事項について、ANU の研究者への支援と助言を提供している。

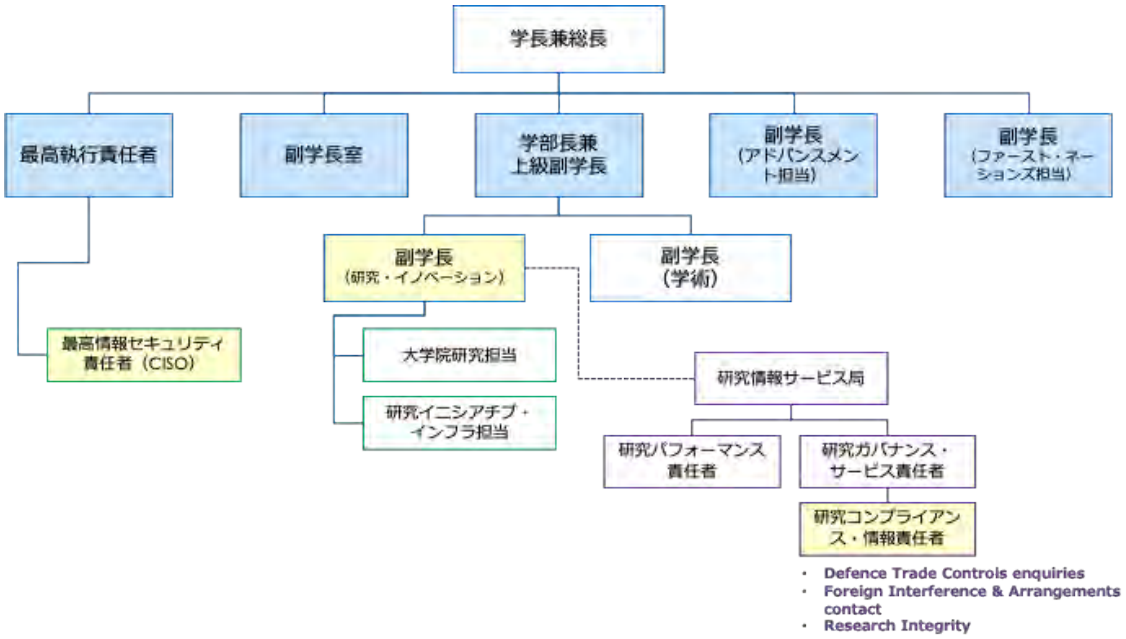


図 2-10　ANU のガバナンス体制と外国干渉対応部署 [323,324]
出典：ANU ホームページより未来工学研究所作成.

(b)　主な取組

i）　UFIT ガイドラインへの対応

ANU では、UFIT のガバナンス提言を運用化するために、外国干渉フレームワーク[325]と外国干渉諮問委員会（FIAC）を設置している。FIAC は、外国干渉リスクの可能性がある共同研究・提携・資金提供契約の審査を担っている。また、UFIT が求めるデュー・ディリジェンスについては、提携締結前に外国関与評価（REMS システム経由）を義務付けている。これにより正式契約と非公式な協力関係の双方を把握可能になる。

[323] オーストラリア国立大学 University Executive (https://www.anu.edu.au/about/university-executive)
[324] オーストラリア国立大学 研究情報サービス局（https://services.anu.edu.au/files/business-unit/RIS%20Org%20Charts_May24.pdf）
[325] 本フレームワークは、オーストラリア国立大学を外国干渉から保護し、国家安全保障上のリスクに対する大学の防御体制を強化することになる。具体的には、大学の評判を守り、学生と教職員を保護し、国際協力による継続的な恩恵を確保するため、外国干渉リスクを管理・軽減する大学のアプローチをフレームワークで概説した。(https://foreign-interference.anu.edu.au/files/2024-01/Foreign%20Interference%20Framework-v7.pdf)

サイバーセキュリティについては、2018 年にデータ侵害事件を経験したことから、サイバーレジリエンスの強化に多額の投資を実施している。ANU 情報セキュリティ室は、国家機関と連携している。

上記以外では、UFIT ガイドラインにある「セキュリティ文化の定着」に向けて、職員に対して外国干渉の定義と報告義務を理解できるよう、啓発活動に取り組むとともに FAQ やリソースの提供を行なっている。

ⅱ） 防衛輸出管理

コンプライアンスチームは、大学を代表して全ての防衛輸出管理許可を申請するため、国防省に登録されている。防衛輸出管理（DEC）は、軍事用及びデュアルユース物品・技術の輸出と供給を規制している。DEC 許可申請方法の詳細は、研究コンプライアンスチーム〈Defence Trade Controls enquiries〉が担当している。

ⅲ） 外国干渉

外国干渉リスクを横断的に監督・管理するのが、ANU 外国干渉諮問委員会（FIAC）である。FIAC の業務は、研究コンプライアンスチームが支援している。研究コンプライアンスチームの役割は、FIAC が日常業務（外国干渉リスク管理に関する評価・監視・助言・保証の提供を含む）を遂行するための事務局業務を提供している。FIAC では外国との共同研究について判断を下し、必要に応じて学長に勧告を行う。FIAC はその運営と活動について、大学研究委員会（URC）に定期的に報告している。

FIAC の評価審査プロセスは、開かれた研究文化の促進、学問の自由、および ANU の博士課程学生・教職員・研究に対する外国干渉リスクの均衡を図ることを目的としており、UFIT ガイドラインに基づいている。

外国機関との協働（正式なもの：法的拘束力のある研究契約、賞・資金受領、教職員・学生交流、名誉職任命等／非公式なもの：学生指導の受諾、共同研究助成申請等）は全て、FIAC へ提出する。

【外国干渉・外国との取り決めスキーム】

- 海外協定制度（Foreign Arrangements Scheme）は、2020 年 12 月 10 日に開始され、大学は、外国政府、外国政府の省庁・機関、または機関としての自律性を欠く外国の大学と取決めを結ぶ場合、外務貿易省（Department of Foreign Affairs and Trade）に通知する必要がある。外国の大学は、実質的に外国政府の管理下にある場合、機関としての自律性を有しないとみなされる[326]。
- 外国との取決めは、必ずしも契約を伴うものだけでなく、正式、非公式を問わない。軽微な行政・運営上の取決めは、本制度の対象外であるが、研究成果に関する二大学間の共同研究、文化活動の企画、学生交換・移動プログラムの設立、奨学金プログラ

[326] 外国干渉の定義は、「オーストラリア大学セクターにおける外国干渉対策に関する DESE ガイドライン」に示されている。

ムの設立、ワークショップ・発表会・会議セッションにおける共同運営は対象となる。コンプライアンスチームは、外国機関との関与評価フォーム提出プロセスの一環として、当該取り決めが本スキームに基づく届出対象か否かを審査する。本スキームでは取り決めの文書証拠（メール、覚書、契約書など）が要求されるため、外国機関との関与評価フォーム提出時にこれらの情報をアップロードすることが求められる[327]。

ⅳ） 研究インテグリティ

ANU は、知的な強さを備えた研究環境を育成・維持し、学問の自由を守り、誠実さ、高潔さ、そして学術的・科学的な厳密さをもって行動することを目指しており、この目標を支援するため、大学の「責任ある研究行動」方針では、ANU の全スタッフおよび客員/名誉職の任命者が「2018 年オーストラリア責任ある研究行動規範」[328]を遵守することが期待されている。コンプライアンスチームは、本規範の違反に関する苦情を審査・調査し、ANU の研究倫理担当責任者であるアン・エヴァンス教授を支援している。

(2) アデレード大学（Adelaide University）

(a) 背景・経緯等

2026 年 1 月にアデレード大学（University of Adelaide）と南オーストラリア大学が統合し、新大学としてアデレード大学（Adelaide University）が開校した。新大学は、両校の統合により学生数が約 7 万人規模となり、オーストラリアの最大級の大学となっている。外国干渉リスク対策については、新大学は研究の柱の一つに「防衛・宇宙」を掲げている。

統合大学では、外国とのコンプライアンス義務を管理する原則として「Foreign Compliance Policy（外国コンプライアンス・ポリシー）」[329]を定め、外国との取り決め、外国からの影響力、および外国による干渉に関連するリスクを特定、評価、管理するためのガバナンスレベルの責任を確立した。この方針は、「Foreign Compliance Review（外国コンプライアンス審査）」（[330]以下、FCR）を維持する権限を付与するものである。FCR は、最高セキュリティ責任者（Chief Security Officer：CSO）が主導している。一方で、CSO はセキュリティリスクの高い研究活動に対して、拒否権・統制権を有するものの、研究活動の実施の可否等は単独で判断することはなく、研究内容・研究価値は、研究担当副学長室（DVC Research）が所掌し、契約・法務的事項は法務部門等が担っている。

アデレード大学は、グローバルな文脈において自らの自律性と評判を積極的に守ること、また政府からはオーストラリアの高等教育セクターに対する全ての国際的関与及び重要技

---

[327] ANU における外国関係協定は、「Australia's Foreign Relations (State and Territory Arrangements) ACT 2020（オーストラリア外国関係（州・準州協定）法 2020）」に基づき、全ての外国関係協定を外務大臣に届け出る義務を負っている。

[328] Australian Code for the Responsible Conduct of Research, 2018（通称 *2018 Code*）(https://services.anu.edu.au/research-support/research-ethics-integrity-compliance/research-integrity)

[329] アデレード大学（2026）「Foreign Compliance Policy（外国コンプライアンス・ポリシー）」(https://adelaideuni.edu.au/about/policies/foreign-compliance-policy/)

[330] アデレード大学（2026）「Foreign Compliance Review Procedure」(https://adelaideuni.edu.au/about/policies/foreign-compliance-policy/foreign-compliance-review-procedure/)

術に関わる全ての研究に対して追加的な警戒を適用するように推奨されている。前述のFCR 制度では、特定の対外活動は FCR 承認後でないと進められない設計としている。具体的には、研究・イノベーション担当副学長および国際・外部連携担当副学長に対し、それぞれの担当分野における外国契約評価プロトコル、関連する外国コンプライアンスプロトコルを維持すること許可するものである。制度の適用対象は、大学職員、学生、称号保持者、請負業者・コンサルタント・客員研究者、外国関与の文脈においてアデレード大学を代表して行動するあらゆる者である。運用主体は Office of the Chief Security Officer であり、不承認時の不服申立てルートについても、副学長級（DVC）へ整理され、研究活動は DVC (Research & Innovation) が関与する仕組みである。非遵守の場合は 刑事罰や懲戒に繋がり得る旨が明示されている。

【オーストラリアにおける関連法規の遵守】

- Foreign Relations (State and Territory Arrangements) Act 2020（2020 年外交関係（州および準州間の取り決め）法）
- Defence Trade Controls Act 2012（2012 年防衛貿易管理法）/ Amendment Act（2024 年改正法）：デュアルユース・技術移転管理
- Autonomous Sanctions Act 2011（2011 年自主制裁法）：自主制裁
- Foreign Influence Transparency Scheme (FITS) Act 2018（2018 年外国影響透明性制度〈FITS〉法）：対外影響の透明化

また、大学における研究セキュリティ対応として、デュー・ディリジェンス義務も含まれる。「国家の利益」に関する懸念に伴い、法的保護が整備されている場合は、重大な罰則が適用される可能性がある。これらの義務を認識することは、リスクを特定・管理し、悪影響を回避するのに役立つと提示している。

(b) 主な取組

i） UFIT ガイドラインへの対応

アデレード大学の Research Integrity Policy の「関連文書」として UFIT ガイドラインが明示的に挙げられている。また、「Interim Foreign Compliance Policy and Procedure」[331]では、外国コンプライアンスポリシーの原則において、当該大学の活動は、UFIT ガイドラインに準拠することを明示している。全職員および外国人大学院研究学生は UFIT ガイドラインに従い、外国の所属関係、関係性、金銭的利害を含むあらゆる利害関係を申告する必要があると定めている。

FCR では、国家安全保障関連法（外交関係法／防衛貿易管理法／自主制裁法／外国影響透明性制度〈FITS〉 等）を束ね、CSO 主導で審査する設計で、UFIT ガイドラインが推奨する「対外連携のリスク評価・デュー・ディリジェンス・管理強化」と整合的な運用基盤を

[331] アデレード大学「Interim Foreign Compliance Policy and Procedure」
<https://adelaideuni.edu.au/about/policies/interim-foreign-compliance-policy-and-procedure/>

整理している。

ⅱ） 外国コンプライアンス審査（Foreign Compliance Review）

アデレード大学は、関連する国家安全保障法への遵守を確保するため、外国コンプライアンス審査（FCR）プロセスを策定している[332]。大学において、職員、学生、または職位保持者が関与する下記の活動は、最高保安責任者室が管理する外国コンプライアンス審査プロセスを得た後にのみ実施できるとした。

- アデレード大学内のいかなる役職への外国人市民の採用
- 外国の団体との個別の職員契約
- 外国の団体との個別の職員による「専門分野の実践」活動
- 提案された国際パートナーを含むあらゆる助成金申請または契約（助成金、契約研究、コンサルティング、共同研究、合弁事業、パートナーシップ、提携、会員資格、提携関係を含む）
- 海外在住の個人／団体を大学に招待する招待状
- アデレード大学の大学院研究プログラムを履修中または履修を希望する外国人大学院研究学生および外国人大学院研究学生候補者
- 外国の団体からの物品および／またはサービスの調達
- 新規の外国契約を進めるための承認申請
- 既存の外国契約（過去に FCR 承認済み）を更新するための承認申請

(3) 西オーストラリア大学（UWA）

(a) 背景・経緯等

西オーストラリア大学（University of Western Australia: UWA）は、1911 年創立の公立大学であり、海洋科学、農学、鉱業工学等の分野で世界的に評価され、同大学の防衛・セキュリティ研究所（DSI）を通じて、国防関連の研究も強化している。研究セキュリティへの対応については、UFIT ガイドラインに基づき、大学運営における外国の干渉に関連するリスクに対処し、軽減するための包括的な枠組み（政策策定、ガバナンス構造、教職員・学生の義務、支援システム）を整備している。これらの検討にあたっては、UWA は、上級職員 1 名を 3 か月間専任で配置し、大学の国家安全保障及び外国干渉リスクに関する包括的な見直しを実施している。これには、UFIT ガイドラインで指摘されたリスク、制裁遵守、Defence Trade Controls Act 2012 （DTCA）遵守[333]が含まれる。包括的な見直しの結果、

---

[332] FCR 制度は、統合前の旧アデレード大学期より、FCR と FCRP を運用しており、2025 年 2 月には、暫定 Foreign Compliance Policy and Procedure を承認している。2025 年 12 月に暫定文書を原則・責任・全体枠組み等のポリシー（Foreign Compliance Policy）、FCR の具体手順となる手続き（Foreign Compliance Review Procedure）に分割し、FCR を独立した手続きとして明確化した。これらは、2026 年 1 月 1 日に正式制度として試行した。(https://adelaideuni.edu.au/about/policies/foreign-compliance-policy/)

[333] DTCA の遵守（DTCA compliance）とは、オーストラリアの 2012 年防衛貿易管理法に従って、研究・共同研究・教育活動の中で取扱う「防衛・戦略物資／技術（DSGL 掲載）」を無許可で海外や外国人に提供・公開・仲介しないようにする一連のコンプライアンス対応のことである。
(https://www.legislation.gov.au/C2012A00153/latest/text)

28 の提言を含む報告書が UWA 執行部に提出された[334]。

(b) 主な取組

ⅰ） UFIT ガイドラインへの対応

ガバナンス／リスク枠組みでは、UWA は、「Foreign Interference Advisory Committee（外国干渉諮問委員会：以下、FIAC)」を設置した。FIAC の構成員は、上級副学長、研究担当副学長、教育担当副学長、グローバル連携担当副学長、最高デジタル情報責任者、ガバナンス・法務顧問で構成され、外国干渉リスク対応を統括している[335]。

デュー・ディリジェンス／リスク評価・管理では、防衛貿易管理、制裁措置及び外国干渉に対して、外国干渉のリスクと軽減策、表現の自由と学問の自由、国際的な研究・教育協力に伴うリスク、防衛貿易管理法／外国取り決めスキーム／制裁措置等の法的義務への体制とシステム整備を図っている。西オーストラリア大学（UWA）の全教員および実務経験等を有するシニアの専門職・一般職員は、該当する義務を理解していることを示す年次申告書の提出が義務付けられており、リスクの高い特定の国際的関与を開示する必要がある。また、研究学生の場合、研究に関連する制裁措置や防衛貿易管理上の問題については、指導教員が管理、研修することとなっている。このように教職員・学生には義務がある一方、権利も存在する。特に UWA は、外国政府による干渉のない安全な環境で教職員・学生が活動・学習する権利を支持している。具体的には、学生または教職員による他の学生・教職員への威嚇、UWA 内で活動する外国人学生団体による不適切な活動、学生・職員の個人情報の不適切な特定又は共有（“doxxing”）、同僚の教職員・学生を外国政府機関に通報する、または通報すると脅す行為等が想定されている。

また、研究インテグリティポリシー（UP20/6）はオーストラリア研究倫理規範に準拠している。これには、IT 適正利用ポリシー、サイバーセキュリティポリシー、プライバシーポリシー、知的財産ポリシー等の遵守を義務付けている。UWA の研究インテグリティの取組では、サイバーセキュリティ、データ保護に係るガイドラインを提供するとともに、AI 導入原則を提唱した。

ⅱ） 外国干渉対策方針（Foreign Interference）：Policy Number. UP22／2[336]

UWA の「外国干渉」に係る文書は、ポリシー番号（U22/2）にて公表されている。「外国干渉方針（Foreign Interference Policy)」は、①外国干渉ガバナンス枠組みの確立、②報告及び申告要件の実施、③国際協定に関するセキュリティの提供からなる。本方針の目的は、a）大学が外国による干渉から受けるリスクを軽減する行動及び慣行を明示すること、b）外

[334] 「Appendix 3: Measures taken by the Go8 to mitigate the threat of foreign interference in alignment with the UFIT Guidelines」(https://go8.edu.au/wp-content/uploads/2020/12/Appendix-3-Go8-actions-against-the-Guidelines.pdf)
[335] 西オーストラリア大学「Foreign Interference」(https://www.uwa.edu.au/about/leadership-and-governance/integrity-and-standards/foreign-interference)
[336] UWA「Foreign Interference Policy」(https://www.uwa.edu.au/policy/-/media/project/uwa/uwa/policy-library/policy/partnerships/internationalisation/foreign-interference/foreign-interference-policy.doc)

国による干渉に対抗する大学の取組を確約すること、c）大学及び大学コミュニティに有益な国際活動を促進し保護することを掲げた。UWA における外国干渉ガバナンス枠組みは、大学の評判を守り、学術的自由、価値観、研究協力関係を保護するため、外国干渉ガバナンス枠組みの責任を担うことである。責任の担い手には、外国干渉諮問委員会（FIAC）の大学執行部への以下の報告が求められる。

【FIAC への報告事項】
- FIAC が大学執行部が管理に関与する必要があるほど十分に深刻な性質であると判断した外国干渉事案
- 国際活動申告書の遵守状況
- 重大な外国干渉リスク及びそれらを軽減するための大学の体制と知識の適切性
- 年次外国干渉対策計画の進捗状況

外国干渉デュー・ディリジェンスについては、「International Partnerships Guideline（国際パートナーシップ構築ガイドライン）」[337]を策定・管理し、大学コミュニティに公開することになっている。国際パートナーシップ構築ガイドラインとは、大学コミュニティが締結する各種国際協定に関する高レベルの責任を説明するものであり、大学役員は外国干渉政策に沿って国際機関と協力する際、デュー・ディリジェンスを履行することが求められる。当該ガイドラインは、各国際協定に関連する国際パートナーシップの責任者を規定している。

2.4.3　資金配分機関等における取組

(1)　オーストラリア研究評議会（Australian Research Council）

(a)　背景・経緯等

オーストラリア研究評議会（Australian Research Council：ARC）は、基礎研究から応用研究までの幅広い分野の科学技術研究を支援・資金提供を行なっている資金配分機関である。代表的な資金プログラムとして、競争的助成プログラム（National Competitive Grants Program: NCGP）は全ての研究助成プログラムを統括する傘に相当するもので、NCGP は目的別に「Discovery」と「Linkage」の２つのサブ・プログラムに分かれている。ARC は全体で年間 10 億豪ドル規模の資金を運用し、その多くが NCGP に割り当てられる。研究開発プログラムについては、2026 年以降に 15 種類以上の助成スキームを、６～7 つの新スキームへと段階的に整理・統合する動きがある。

[337] UWA「Establishing International Partnerships Guideline」(establishing-international-partnerships-guideline. ...uwa.edu.auhttps://www.uwa.edu.au › foreign-interference › e...)

NCGP	主な目的	代表的な資金配分プログラム	プログラムの対象	助成規模
Discovery Program	基礎研究、個人のキャリア、知のフロンティアの拡大	Discovery Projects (DP)	個人またはチームによる基礎・応用研究。ARCの基幹プログラム	年間3万～50万豪ドル（最長5年間）
		DECRA	博士号取得後5年以内の若手研究者プログラム	年間約12.7万ドルの給与補助＋研究費最大5万ドル（3年間）
		Future Fellowships（FT）	中堅研究者（Mid-career）の国内留置・海外招聘	4年間の給与＋年間最大6万ドルの研究費
		Laureate Fellowships (FL)	世界トップレベルのシニア研究者	5年間の給与＋研究費＋ポスドク・大学院生雇用費
Linkage Program	産学連携、国際協力、社会課題解決、インフラ整備	Linkage Projects (LP)	産業界や政府、国内外の団体と連携する共同研究	年間5万～30万豪ドル（2～5年間），パートナー機関からの現金・現物出資が必要。
		Centres of Excellence (CE)	国際的なハブとなる大規模な研究センターの設立	2026年開始分として大規模な予算が配分され、分野を超えた長期的な共同研究を支援
		Industrial Transformation Research Program（ITRP）	産業界の課題解決に直結する研究拠点の形成	数百万ドル規模の大型投資。Training CentresとResearch Hubsがある

図 2-11　ARC における代表的な資金配分プログラム
出典：ARC の HP より未来工学研究所作成.

ARC の研究セキュリティに係る取組みでは、2021 年 11 月に「重要技術のための青写真と行動計画」（Blueprint and Action Plan for Critical Technologies）を発表し、国家利益のために重要技術を保護・促進するビジョンと戦略を提示した。2023 年 12 月には、ARC Countering Foreign Interference Framework（ARC CFI フレームワーク）を公表し、UFIT ガイドラインと、UFIT デュー・ディリジェンスフレームワークに基づき、リスク評価の実施を求める文書を公表した。

CFI フレームワークは、NCGP 全体の国家安全保障リスクを管理するためのアプローチであり、ARC は研究が重要な技術に関連しているかどうかを特定することに加えて、次に示すリスクの可能性について考慮している。

- 現在または最近の外国の財政支援、教育または研究関連の活動／現在または最近の海外人材採用プログラムへの関与または外国の大学への義務／外国政府、軍隊、警察、または諜報機関との現在または最近の関係／オーストラリアが制裁を課している政権、個人、または組織との最近の関係
- 評価では、研究者の研究管理システム（Research Management System: RMS）のプロファイル内で提供された情報を考慮に入れる。外務貿易省（DFAT）の制裁体制や統合リストなどのオープンソース情報も検討される。ARC がリスクが存在する可能性があると判断した場合、国家安全保障機関および/または外部の独立したプロバイダーに、懸念がある場合はレビューとアドバイスを依頼することができる。

研究セキュリティに係る要件の強化に沿って、2024 年 7 月に ARC 法が改正され、国家安全保障、防衛、国際関係に関連する要件を強化した（法的要件を満たすため、ARC は政府機関や研究機関と緊密に連携し、研究セキュリティ体制の強化）。改正 ARC 法では、研究セキュリティの審査プロセスが強化された。2026 年開始の「ARC Centres of Excellence 2026」や「Discovery Projects 2026」では、この最終的なデュー・ディリジェンス確認のために採択発表が延期されるケースも出ているとの情報がある（ARC の関連ページへのアクセスは不可となっている）。

- 早期セキュリティスクリーニング／より広範なオープンソース証拠の使用／外国の所属と資金開示の要件の明確化・申請時及び資金提供プロジェクト過程で一貫的なリスク評価を支援（完全な開示）／リスク軽減に関する具体的な保証（UFIT ガイドラインに沿ったデュー・ディリジェンスの実施の証明）
- 選考プロセスの最終段階で実施していたセキュリティチェックの評価プロセスの初期段階に統合

(b) 主な取組

i) ARC プロセス

議会情報安全保障合同会議（Parliamentary Joint Committee on Intelligence and Security: PJCIS）の「オーストラリア高等教育・研究セクターに影響を及ぼす国家安全保障リスクに関する調査」（2022 年）[338]、UFIT ガイドラインの戦略的方向性に基づき、ARC プロセスを策定・改善を図っている。

主な変更点 : 研究セキュリティ審査の早期化及び強化、実施機関とのより詳細な連携、外国関連団体の開示に関する期待事項の更新、研究セキュリティ／助成金受給資格／助成金遵守メカニズム間の連携強化

ii) UFIT ガイドラインに伴う機関の取り組み

UFIT が 2021 年に策定した「Guidelines to Counter Foreign Interference in the Australian University Sector（オーストラリアの大学セクターにおける外国からの干渉に対抗するためのガイドライン）」に沿って、ARC プロセスは運営されている。当該ガイドラインは意思決定者が外国干渉によるリスクを評価・管理する支援を目的とし、オーストラリア大学における既存のリスク管理方針およびセキュリティ慣行を基盤としている。

iii) その他関連の取り組み

国家競争助成プログラム（NCGP）及びその他のプログラムにおける国家安全保障リスク管理に必要な事項は、ARC Countering Foreign Interference Framework（ARC 外国干渉枠組み）で提供されている。

[338] Parliamentary Joint Committee on Intelligence and Security. Inquiry into national security risks affecting the Australian higher education and research sector. 2022. https://nla.gov.au/nla.obj-3053145503/view

【審査プロセスの対応例】

対応項目	概要
助成金審査プロセスにおけるセキュリティ審査の変更	審査段階の変更（セキュリティ審査を最終段階から前倒し）、審査内容の詳細化（研究者の所属機関、外国資金、外国人材プログラム、外国政府・情報機関・軍・警察等との関連性）、データ活用（リスク評価の制度の向上のため、オープンソース情報の活用）
審査	申請者及び研究者の RMS プロファイルに記載された情報を考慮
参照情報	外務貿易省（DFAT）の制裁対象リスト、統合リスト等の公開情報も参照
内部監査の実施	外国干渉/国家安全保障リスクに関するプロセスがどの程度機能しているかを評価するため、内部監査の実施
外国干渉リスク対策	ARC は、助成金申請における外国干渉リスクの評価・軽減方法を定義するフレームワークを有する
大学機関との連携	大学／管理機関は独自の方針とリスク管理慣行を有することが期待される。ARC はこれらを適切に機能させるため連携する

2.4.4 まとめ

オーストラリアの研究セキュリティは、外国干渉リスクに対応するために、政府機関と大学・研究機関等でガイドラインを策定し、併せて、大学・研究機関内で、外国干渉リスク対策（体制整備や規程の策定）が行えるよう補足資料を作成している。2025 年 2 月には、ガイドラインの項目に沿って、ガイダンスノートや事例研究、自己評価のための資料を公開した。

オーストラリアの外国干渉リスクは、研究者のみならず、学生の対応も含まれている。事例研究によると、研究上の外国干渉リスク（例えば、共同研究における外国政府からの意図を持った資金提供や研究プロジェクトの要請等）以外にも、学内で生じる排外的な活動から生じる学内の学生・教職員、外国政府からの脅迫等から、学生・教職員を守るための大学執行部の対応方針例を提示している。外国干渉リスク対策は、幅広く研究活動の自由を確保するための取組と考えられる。

オーストラリア大学における外国干渉リスク対応としては、本事例で取り上げた大学機関では、大学の執行部レベルで外国干渉諮問委員会を設置するとともに、外国干渉リスクに対応するために必要な報告手順等をとりまとめている。これらは、政府機関と大学・研究機関等で策定したガイドラインに基づき、整備しているものであり、我が国の大学機関等の取組の参考となる。また、オーストラリアでは、外国干渉に係る法整備も進んでおり、大学機関及び大学機関に関わる教職員・学生等も法の枠組みの中で、必要な報告等を行っていることも特徴である。

2.5　欧州連合（EU）

欧州連合（以下、EU）[339]の統治組織は、図 2-12 のように欧州理事会（European Council）、欧州連合議会（European Parliament）、EU（閣僚）理事会（Council of EU）及び欧州委員会（European Commission）から構成され、欧州議会と EU 理事会が共同で意思決定を担う。欧州委員会は、行政執行機関として政策案の策定と提案、政策の実施と運営、EU 法遵守の監視及び予算配分を担当する[340]。また、後述するように、資金配分機関であり、欧州最大の研究資金のホライズン・ヨーロッパ（Horizon Europe）を運営する。

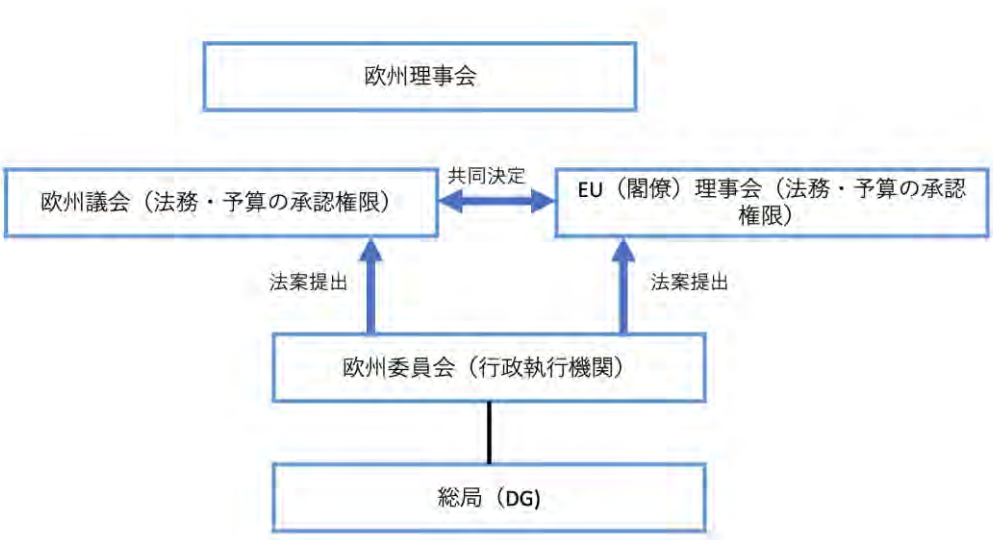


図 2-12　EU の意思決定の仕組[341]

EU の取組には大きく二つの地政学的な出来事（incident）が影響を及ぼしている。一つは、2019 年 3 月の対中政策の転換である。EU は、中国を「体制的ライバル（a systemic rival）」と定義し、技術流出への警戒を強めた[342]。そのため、研究セキュリティと研究インテグリティ（以下、研究セキュリティ・インテグリティ）のアプローチでは、デュアルユース技術の中国への移転防止が重視された。

二つ目は 2022 年 2 月のロシアによるウクライナ侵攻である。2023 年 6 月欧州委員会は、欧州議会、EU 理事会及び欧州理事会に対する共同通信「European Economic Strategies（欧

[339] 欧州連合（European Union, 以下 EU）は、経済・通貨同盟のほか、外交・安全保障、刑事・警察などの幅広い分野で協力する政治と経済の統合、経済通貨同盟、共通外交・安全保障政策や警察・刑事司法などより幅広い分野での協力を進め、欧州連合条約によって統治される政治・経済の共同体で、加盟国は現在 27 カ国である（駐日欧州連合代表部「EU とは」、https://www.eeas.europa.eu/japan/eutoha_ja?s=169）。
[340] 欧州委員会、https://eumag.jp/article/basicinfo0524/
[341] CRDS「研究開発の俯瞰報告書　主要国・地域の科学技術・イノベーション政策動向（2025 年）」（https://www.jst.go.jp/crds/pdf/2024/FR/CRDS-FY2024-FR-09.pdf）所収の図を基に未来工学研究所が作成した。
[342] European Commission “EU-China: A Strategic Outlook,”12 March 2019, https://commission.europa.eu/publications/eu-china-strategic-outlook-commission-and-hrvp-contribution-european-council-21-22-march-2019_en

州の経済安全保障戦略)」[343]を発表し、経済安全保障と研究セキュリティは不可分であるとの見解を示した。すなわち、EU の研究・開発（R&D）政策は、2023 年を境に、それまでの「openness in scientific research（科学研究の開放性)」や「academic freedom（学問の自由)」に加え、「安全な secure」研究を追求するアプローチへと変化した。

EU の R&D 政策は、2000 年に創設された European Research Area（欧州研究圏、以下 ERA）に基づいて計画される。ERA は EU 全域の研究・技術・イノベーション（以下 STI）の単一領域の形成を目指し、加盟国間の研究に関する政策と事業の調整を目的にしている[344]。ホライズン・ヨーロッパは、ERA の STI に関するビジョンや枠組を実現するための研究プログラムである。

EU の STI 政策に利害関係を有するステークホルダーは、加盟国のほか域内の大学・研究機関、研究者、学術団体であり、EU とステークホルダーとの関係は図 2-12 のように表すことができる。

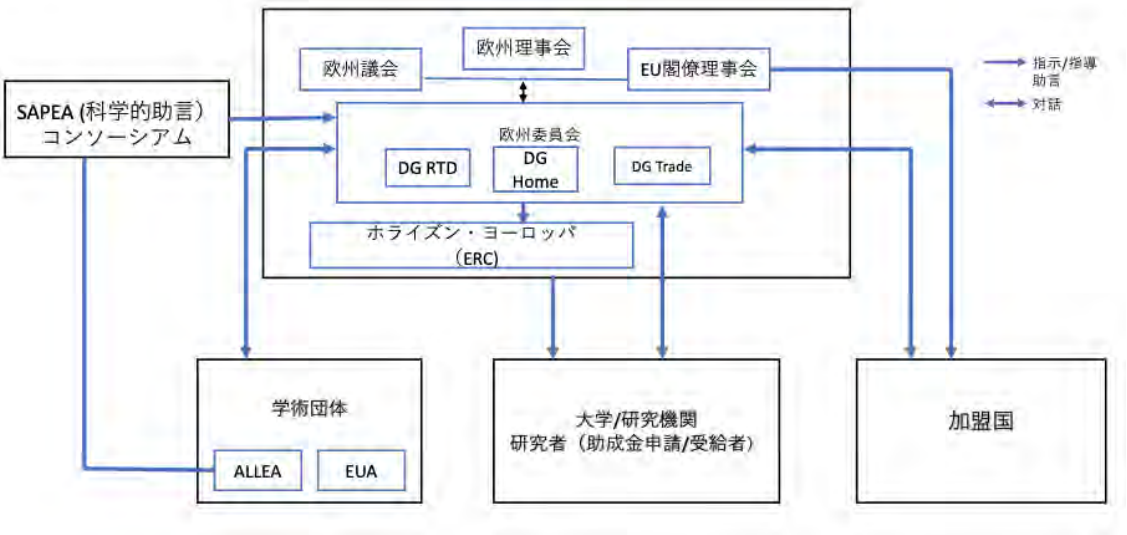


図 2-13　EU の研究セキュリティ・インテグリティに関する EU 機関とステークホルダーの関連性

欧州委員会は研究セキュリティ・インテグリティ関連文書（草案を含む）の策定とそれに伴う EU 組織内及び域内ステークホルダーとの調整等の役割を担う。同委員会には 41 の総局（日本の省庁に相当）[345]があり、これらのうち本案件に関与するのは、図 2-13 の向かって左手より、ホライズン・ヨーロッパに関する政策を担当する「研究・イノベーション総局(Directorate-General for Research and Innovation、DG RTD)」、対諜報リスク、外国から

[343] Joint communication to the European Parliament, the European Council and the Council on European Economic Strategies (20/06/2023), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020
[344] European Research Area, https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/our-digital-future/european-research-area_en
[345] European Commission, Departments and Executive Agencies, https://commission.europa.eu/about/departments-and-executive-agencies_en?page=0

の干渉、重要技術の保護等担当の「移動と内務総局（Directorate-General for Migration and Home Affairs、DG Home)」、そして研究成果のデュアルユースを含む輸出管理を担う「通商総局（Directorate-General for Trade、DG Trade)」である。研究セキュリティ・インテグリティ、デュアルユースに関連した課題は研究・イノベーション総局が所管する。

2.5.1　研究セキュリティ・インテグリティ関連政策動向

(1)　2024 年度までの経緯[346]

2024 年度までの EU の研究セキュリティ・インテグリティに関する主要な文書を表 2-12 及び 2-13 にまとめた。既に述べたように、EU のセキュリティ認識は 2023 年を境に変化が見られる。2023 年以降の文書では問題意識がより明確になり、リスクの特定や対応など具体的なアプローチが提示されて、セキュリティシステムのガバナンスとコンプライアンスの構築が志向されるようになった。

表 2-12　EU の近年の研究セキュリティ・インテグリティ関連文書（2024 年度まで前半）

発行年	文書の名称	発行組織
2021年5月18日	(a) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The Global Approach to Research and Innovation Europe's strategy for international cooperation in a changing world （欧州議会、EU理事会、経済社会評議会及び欧州地域委員会への欧州委員会通信：研究とイノベーションへの世界的接近）	欧州委員会
2021年9月28日	(b) Council Conclusion on Global approach to R&I; Europe's strategy for international cooperation in a changing world （研究とイノベーションへの世界的接近に係る決議：変化する世界における国際協力のための欧州戦略）	EU理事会
2022年1月	(c) Tackling R&I foreign interference: Staff working document （研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書）	欧州委員会
2022年6月10日	(d) Council conclusions: Principles and values for international cooperation in R&I （研究とイノベーションにおける国際協力のための原則と価値に係る決議）	EU理事会
2023年3月1日	(e) Code of Practice on the management of intellectual assets for knowledge valorisation （知識価値化のための知的資産管理に関する実践規範）	欧州委員会

(a)　Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The Global Approach to Research and Innovation Europe's strategy for international cooperation in a changing world （欧州議会、EU 理事会、経済評議会及び欧州委員会、

[346] ここで取り上げた文書のうち 2025 年 2 月 28 日のものを除いて、令和 5 年度科学技術基礎調査等委託事業「研究インテグリティ（Research Integrity）に係る調査・分析報告書」及び令和 6 年度科学技術基礎調査等委託事業「研究インテグリティ（Research Integrity）に係る調査・分析及び G7 オンラインプラットフォーム『バーチャルアカデミー』の運営支援・分析」調査報告書を参考にした。

通信：研究とイノベーションへの世界的接近）[347]

EU の研究とイノベーションの戦略を示した文書（2021 年 5 月 18 日）である。学問の自由や研究倫理などの分野で EU の利益と基本的な価値を保護することを目指した研究インテグリティの観点からのアプローチである。

(b) Council Conclusion on Global approach to R&I; Europe‘s strategy for international cooperation in a changing world（変化する世界における国際協力のための欧州戦略）[348]

欧州の研究とイノベーションについてホライズン・ヨーロッパを枠組として、国際的な協力を促進すると同時に、リスクの軽減と戦略的自律性を通じて EU の利益を保護するための措置を論じ、研究セキュリティに一歩踏み込む内容と言える。2021 年 9 月 28 日に発出された。

(c) Tackling R&I foreign interference: Staff working document（研究・イノベーションにおける海外からの干渉に対処するためのスタッフ作業文書）[349]

2022年1月発出の本文書は、外国による干渉（FI）は、外国の国家主体もしくはその代理による活動が、強制的かつ秘密裏に行われ、その結果欺瞞的な行為や腐敗を招き、さらにEUの主権、価値観及び利益に反するような事態を引き起こすとの注意を促す。価値観、ガバナンス、パートナーシップ、サイバーセキュリティの4つのカテゴリーに分類される重点分野を網羅した包括的な外国干渉対策戦略はEU域内の大学と研究機関にとって有益である。本文書では、大学・研究機関が自らのニーズに合わせた包括的戦略を策定するのに役立つと考えられる緩和策の非網羅的なリストを提示している。

(d) Council conclusions: Principles and values for international cooperation in R&I（研究とイノベーションにおける国際協力のための原則と価値に係る決議）[350]

本決議（2022 年 6 月 10 日）は、協力の開放性、多国間主義、民主的価値の遵守によって欧州の研究とイノベーションを強化する一方、戦略的自律性と研究セキュリティの重要性を指摘した。

---

[347] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The Global Approach to Research and Innovation Europe‘s strategy for international cooperation in a changing world (18.05.2021), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52021DC0252

[348] Council Conclusion on Global approach to R&I; Europe‘s strategy for international cooperation in a changing world (18.09.2021), https://www.consilium.europa.eu/en/press/press-releases/2021/09/28/council-agrees-on-a-global-approach-to-research-and-innovation/

[349] Tackling R&I foreign interference: Staff working document (17 Jan 2022), https://european-research-area.ec.europa.eu/documents/tackling-ri-foreign-interference-staff-working-document-2022

[350] Council conclusions: Principles and values for international cooperation in R&I, https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/multilateral-dialogue-principles-and-values_en

(e) Code of Practice on the management of intellectual assets for knowledge valorisation（知識価値化のための知的資産管理に関する実践規範）[351]

本書（2023 年 3 月 1 日発出）は、研究・イノベーション（R&I）の成果を社会的・経済的価値へ転換する「知識の価値化 knowledge valorisation」を改善するための EU の取組の一環として位置付けられ、2008 年の欧州委員会による知識移転における知的財産に関する勧告を基盤としつつ、一般的な定義の知的財産権を超えたより広範な知的資産を含む内容となっている。すなわち、本規範における「知的資産」には、知的財産権（特許、著作権など）だけでなく、データ、ノウハウ、プロセス、ソフトウェア、プロトタイプ、実践方法、その他の研究成果が含まれる。また、拘束力のある法律ではなく、指針であり、研究機関、大学、企業、知識移転機関、その他の R&I エコシステム関係者を想定した提言である。効率的な知的資産管理のための戦略策定、共同の研究やイノベーションの活動における知的資産の管理、知的資産の創出から市場(商業利用)への橋渡しの 3 点を提言する。

表 2-13　EU の近年の研究セキュリティ・インテグリティ関連文書（2024 年度まで後半）

発行年	文書の名称	発行組織
2023年6月20日	(f) Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy （EU理事会、欧州理事会への欧州の経済安全保障戦略に関する共同通信）	欧州議会、
2023年10月3日	(g) Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States (EUの経済安全保障における重要技術分野に関する欧州委員会勧告：加盟国とのさらなるリスク評価を目指して)	欧州委員会
2024年1月24日	(h) New tools to reinforce the EU's economic Security (EUの経済安全保障を強化するための新しいツール)	欧州委員会
2024年1月24日	(i) Council Recommendation on Economic Security Package (研究セキュリティに関する委員会勧告：経済安全保障パッケージ)	欧州委員会
2024年1月	(j) Factsheet on Research Security: Building blocks for risk appraisal (研究セキュリティのリスク評価の基盤概要書)	欧州委員会
2024年5月23日	(k) Council Recommendation on Enhancing Research Security（研究セキュリティ強化に関するEU理事会勧告）	EU理事会

(f) Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy（欧州の経済安全保障戦略に関する欧州議会、EU 理事会及び欧州理事会への共同通信）[352]

2023 年 6 月 20 日に出されたこの共同通信は、経済活動を安全保障のリスク要因と定義

[351] Code of Practice on the management of intellectual assets for knowledge valorisation, https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/eu-valorisation-policy/knowledge-valorisation-platform/guiding-principles-knowledge-valorisation-and-implementing-codes-practice/code-practice-management-intellectual-assets-knowledge-valorisation_en

[352] Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy, https://eur-lex.europa.eu/legal-

し、４つに分けられたリスクのカテゴリーの一つに技術の安全保障と漏洩を挙げた。研究セキュリティを経済安全保障の一部とする見解を明示した重要文書である。

(g) Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States （EU の経済安全保障における重要技術分野に関する欧州委員会勧告：加盟国とのさらなるリスク評価を目指して）[353]

上記の共同通信に続き、研究セキュリティをより広範な 欧州の経済安全保障の部分と位置付け、さらに 4 分野の重要な技術、すなわち先進半導体、人工知能（AI）、量子技術、バイオテクノロジーについてリスク評価を実施することを加盟国に促した。2023 年 10 月 3 日に出された本文書の内容は、R&I 関係者向けに簡潔に整理され、(i)と(j)で述べる 2 冊のファクトシートとして発出された。

(h) New tools to reinforce the EU's economic Security（EU の経済安全保障を強化するための新しいツール）[354]

貿易と研究分野に関する新しい措置に関する 2024 年 1 月 24 日付の概要記事である。研究セキュリティについては、例えば高度な電子機器のようなデュアルユース物品の悪用の防止、第三国による EU の高度技術の軍事力強化への悪用への対応措置が検討されていることが紹介された。記事に述べられた措置が、(k)で述べる 2024 年 5 月 23 日の勧告である。

(i) Council Recommendation on Economic Security Package（研究セキュリティに関する委員会勧告：経済安全保障パッケージ（ファクトシート 1））[355]

本文書（2024 年 1 月 24 日発行）も、同じく勧告「加盟国との更なるリスク評価を目指して」の考え方を域内のステークホルダー向けに分かりやすく示した概要書（ファクトシート）である。加盟国および研究・イノベーション分野の関係機関（者）を支援し、欧州全域における研究セキュリティの強化を図り、第三国による重要技術の望ましくない移転、悪意のある影響力、倫理的・誠実性の侵害といったリスクの管理を目的にしている。他方で、「可能な限りの開放性と必要な限りの閉鎖性」という原則に従い、国際協力と開放性の重要性も強調する。リスク管理施策を政府機能、研究資金配分機関の役割、大学・研究機関が実施可能な施策、そして欧州委員会の役割の 4 つのレベルから示している。

content/EN/TXT/?uri=celex:52023JC0020

[353] Commission recommendation on critical technology areas for the EU‘s economic security for further risk assessment with Member States, https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

[354] New tools to reinforce the EU’s economic Security, https://commission.europa.eu/news-and-media/news/new-tools-reinforce-eus-economic-security-2024-01-24_en

[355] Council Recommendation on Economic Security Package, https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en

(j) Factsheet on Research Security: Building blocks for risk appraisal（研究セキュリティのリスク評価の基盤概要書（ファクトシート 2））[356]

上記の欧州委員会勧告「加盟国との更なるリスク評価を目指して勧告」を広範なステークホルダーに周知するために 2024 年 1 月に刊行された文書である。研究セキュリティにおけるリスク評価とは国際的な研究・イノベーション協力において発生し得る複数のリスクを考慮に入れることとし、リスク評価のアプローチについて詳細に論じた。

欧州委員会は、研究セキュリティに関する理事会勧告の提案において、欧州全域での意識向上とレジリエンス強化のため、関連するあらゆるレベルでの複数のガイダンス及び支援措置を提示している。本ファクトシートは、あらゆる研究セキュリティアプローチの核心的な要素を詳細に扱い、リスク評価を対象と方法の両面から論じ、リスク評価のための質問項目参考案を提示している。

(k) Council Recommendation on Enhancing Research Security（研究セキュリティ強化に関する EU 理事会勧告）[357]

2024 年 5 月 23 日に発出された本勧告は EU の今後の方針を提示する重要文書である。発出に先立ち、EU 圏内のステークホルダーに「意見募集の呼びかけ（call for evidence）」が 2023 年 12 月 6 日から 2024 年 1 月 3 日まで実施され、56 の機関及び個人からフィードバックがあった[358]。

欧州委員会、加盟国、域内の資金配分機関及び大学・研究機関が研究・イノベーションの国際協力から生じる研究セキュリティ上のリスクに対処するためのガイドラインで、次のような事項が盛り込まれている。すなわち、協力の開放性を維持しつつ、望ましくない知識移転及び技術漏洩、外国の干渉、倫理及びインテグリティの侵害等のリスクの可能性を認識し、学術の自由と機関の自律性の維持、リスクを基礎にしたバランスの取れたアプローチの適用、差別の禁止、基本的権利の尊重、「可能な限りの開放性と必要最小限の閉鎖性」の比例原則という基本方針を示し、各ステークホルダーに求められる対応措置が挙げられた。

欧州委員会に対しては、無形技術移転を含む輸出管理、査証、知的財産管理等の EU 規則適用に関する解釈指針の提供、システム構築のための支援を検討し、加盟国との対話によって安全保障措置の整合性を図ることが求められた。支援措置の中には「欧州研究セキュリティ専門センター（European Centre of Expertise on Research Security）」の設立が含まれている。

加盟国には研究・イノベーション関係者のためのガイドライン及び支援サービスの構築、教育、R&I、貿易、外交、情報、安全保障等の政府部門間の調整、脅威・サイバー評価など

356 Factsheet on Research Security: Building blocks for risk appraisal, https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en
357 Council Recommendation on Enhancing Research Security, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510
358 European Commission, Boosting Research Security in the EU (guidance), About this initiative, Call for evidence, Feedback, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance-_en

エビデンスの基盤の強化、レジリエンステストとインシデントシミュレーションの実施、情報機関との情報交換の促進が提案された。なお、措置を講じるに際しては、特定国を想定するのではなく、中立性を維持すべきことが明示されている。

(2) 最近の主な動き

2025年4月以降のEUの研究セキュリティ・インテグリティをめぐる動向を時系列により表2-14にまとめた。

表 2-14 EU の最近の研究セキュリティ・インテグリティ関連動向（2025 年 4 月～）

発行年	文書の性質・表題	行為主体
2025年6月25日	(a)-i) New publications on dual use provide strategic input for future EU R&I policies (デュアルユースに関する新しい出版物が将来のEU研究・イノベーション政策に向けた戦略的考え方を提供)	欧州委員会（ニュース）
2025年9月8日	(a)-ii) 2025 Update of the EU Control List of Dual-Use Items (デュアルユース物品のEU管理リストの2025年)	欧州委員会（ニュース）
2025年9月30日	(b)-i) Conclusions on the importance of research and innovation for the EU Startup and Scaleup Strategy (EUのスタートアップとスケールアップ戦略のためのR&Iの重要性に関する決議)	EU競争力(研究)理事会（ニュース）
2025年10月28日～30日	(c)-i) European flagship conference on research security for responsible, open and secure research and innovation (責任・開放・安全なR＆Iのための研究セキュリティ欧州旗艦会議)	欧州委員会 EUA, ALLEA他 (パンフレット)
2025年10月28日	(a)-ii) Commission announces new measures to strengthen research security (研究セキュリティ強化のための新措置)	欧州委員会（告知）

(a) 欧州委員会

i) New publications on dual use provide strategic input for future EU R&I policies （デュアルユースに関する新しい出版物が将来の EU 研究・イノベーション政策に向けた戦略的考え方を提供）[359]

本文書は、欧州委員会がデュアルユースの研究・イノベーション（R&I）に関する二つの独立した専門家報告書を公表したことを紹介した 2025 年 6 月 25 日付の記事である。民生用と防衛用の両方に利用可能な技術への理解を深め、次世代 EU 資金プログラムに関する議論と情報に基づいた意思決定に貢献することを目指すとしている。

一つ目の報告書は、R&I の経済的・社会的影響に関する専門家グループ（ESIR）が作成した政策提言「EU の R&I 投資を最大限活用する：デュアルユースの再考」である。安全保障、戦略的自律性、競争力、持続可能性を促進する上での「デュアルユース R&I 資金」の戦略的役割を強調し、設計段階からデュアルユースを明示的に考慮した「設計によるデュアルユース」アプローチの採用を推奨する。デュアルユース R&I は研究生産性の向上、防衛と民間研究の相乗効果を促進、倫理的配慮とガバナンスへの対応の必要性と認知度の向上、研究成果移転、科学者と防衛専門家間の連携強化などのメリットがあり、デュアルユー

[359] New publications on dual use provide strategic input for future EU R&I policies, https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/new-publications-dual-use-provide-strategic-input-future-eu-ri-policies-2025-06-25_en

スの可能性を高める新戦略の検討の必要性が述べられている。

一方、二つ目の報告書「デュアルユース研究開発の可能性を解き放つ」では、デュアルユース研究開発が実際に機能する具体的な事例を挙げてケーススタディを行い、民間と防衛の相乗効果に関連する機会と課題に関する証拠を提供する。研究実施機関、中小企業、スタートアップ及びスケールアップ企業の視点からデュアルユース R&I の実践的な実施を明らかにし、世界各国の研究・開発（R&D）政策、戦略、資金プログラムの事例とベンチマークを示すものとなっている。

ii） 2025 Update of the EU Control List of Dual-Use Items （デュアルユース物品の EU 管理リストの 2025 年更新）[360]

2025 年 9 月 8 日付の欧州委員会ニュースの記事である。この更新により、リストは 2024 年に多国間輸出管理体制であるワッセナー・アレンジメント（Wassenaar Arrangement: WA）、ミサイル技術管理レジーム（MTCR）、オーストラリア・グループ（AG）、核供給国グループ（NSG）において採択された決定に整合するものとなった。この中には、加盟国がワッセナー・アレンジメントのメンバーとして受け入れた追加品目を統一的に管理する公約も含まれる。これに伴い、新技術に対する EU レベルでの効果的な管理がさらに強化され、2024 年輸出管理白書に沿ったデュアルユース物品取引の安全保障が担保される。また、EU レベルでの統一管理は、効果と透明性の保証と同時に、EU の競争力と経済事業者間の公平な競争環境の維持に寄与する。今回リストに追加されたデュアルユース物品は量子技術関連コントールシステム、半導体の製造・試験装置及び材料、高度なコンピューティング集積回路および電子アセンブリ、高温用途向けコーティング、積層造形装置並びに関連材料である。

iii） Commission announces new measures to strengthen research security（研究セキュリティ強化のための新措置発表）[361]

2025 年 10 月 28 日付の欧州委員会の記事によると、後述する研究セキュリティ欧州旗艦会議の席上、スタートアップ・研究・イノベーション担当の Ekaterina Zaharieva（エカテリーナ・ザハリエワ）欧州委員会委員が、EU 全域における研究セキュリティ強化に向けた新たな取組を発表した。この取組は、欧州研究セキュリティ専門センターを欧州委員会内に設置、研究者が国際協力のリスクを評価するためのデュー・ディリジェンスプラットフォームの構築、加盟国が研究実施機関のレジリエンスを検証するための新たな共通手法の開発の 3 点からなる。これらは欧州委員会が提案予定の欧州研究圏法（European Research Area Act）に盛り込まれ、研究セキュリティの法制化が見込まれる。

---

[360] 2025 Update of the EU Control List of Dual-Use Items, https://policy.trade.ec.europa.eu/news/2025-update-eu-control-list-dual-use-items-2025-09-08_en
[361] Commission announces new measures to strengthen research security, https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-announces-new-measures-strengthen-research-security-2025-10-28_en

(b) EU 競争力理事会（EU Competitiveness Council）

i) Conclusions on the importance of research and innovation for the EU Startup and Scaleup Strategy （EU のスタートアップとスケールアップ戦略のための R&I の重要性に関する決議）[362]

2025 年 9 月 30 日、EU 研究閣僚は次期ホライズン・ヨーロッパの枠組（2028-2034 年）の一環としてデュアルユース・安全保障・防衛分野における EU の研究・イノベーションに関する研究担当大臣討議による政策討論を行い、R&I がデュアルユース及び安全保障目標をより効果的に支援すべき点を強調した理事会決議を採択した。

(c) 欧州委員会と EU 域内ステークホルダー

i) European flagship conference on research security for responsible, open and secure research and innovation（責任・開放・安全な R&I のための研究セキュリティ欧州旗艦会議（以下、欧州旗艦会議）の開催）[363]

2025 年 10 月 28 日～30 日に開催された当会議には、欧州の研究・イノベーション関係の 12 団体が欧州委員会の呼びかけに応じて共催者になり、ボトムアップな組織化によって開催が実現された。先進的な取組、大学や研究資金配分機関の役割、政府のアプローチとサポートなどが議論された。研究セキュリティに関する欧州のアプローチを開発することを目的に、欧州全域および国際パートナー国から政策立案者、専門家、実務者 500 名が参加した。

2.5.2 大学・研究機関等における取組

EU は、欧州大学院（European University Institute） と 欧州大学（College of Europe という２つの大学の運営に関与しているが、いずれも人文・社会科学系の大学で、研究セキュリティとの関連性が希薄であり、実際関連文書が出された形跡もない。そこで、EU 域内の大学を代表して EU の方針について見解を表明し、研究セキュリティに積極的に取組む二つの学術団体に注目した。

(1) 欧州大学協会（European University Association）

(a) 背景・経緯等

2001 年に設立された European University Association（EUA）は、欧州 48 カ国の大学と全国大学学長会議を代表する組織で、ベルギーのブリュッセルにある。ボローニャ・プロセス[364]及び高等教育・研究・イノベーションに関する EU 政策において重要な役割を担う

[362] Conclusions on the importance of research and innovation for the EU Startup and Scaleup Strategy, https://www.consilium.europa.eu/en/meetings/compet/2025/09/30/
[363] European flagship conference on research security for responsible, open and secure research and innovation, https://euresearchsecurityconference.service-facility.eu; EUA, The Voice of Europe's Universities, https://eua.eu
[364] 1999 年 6 月 19 日にイタリアのボローニャで、欧州 29 か国の高等教育担当大臣が調印した宣言。2010 年までの欧州高等教育圏（European Higher Education Area: EHEA）の確立に向けて諸課題の達

とともに、高等教育・研究分野における独自の専門的情報を発信し、大学間におけるアイデアや優れた事例交換の場を提供している。研究セキュリティについても、EU の有力なステークホルダーとして積極的に関与している。

およそ 900 の会員を擁し、加入は大学と全国的な学長団体を単位とし、個人は認めていない[365]。約 40 名の専任スタッフを抱え、専門的な観点から提言を行うために、研究・イノベーション、高等教育政策部門、大学資金調達部門など様々なユニットに分かれて調査研究を行っている。研究セキュリティは研究・イノベーション（R&I）ユニットのテーマの一つとして取り組まれている[366]。R&I ユニットは、研究セキュリティのアプローチの開発について議論するため大学のリーダーや専門家を招集する[367]。運営は会費によって賄われているが、プロジェクトの運営に際しては、EU の研究助成に応募して、資金を得ることもある[368]。

ここでは、欧州委員会の提案に対する当団体の見解を述べた 2 文書を取り上げる。EU の政策形成に影響力を有する学術団体のスタンスと考え方を取り上げることは、我が国の学術界との関係を考える上で参考になると考えられる。

(b) 主な取組

i) Research and innovation as drivers of open international cooperation （開放的な国際協力のドライバーとしての研究・開発）[369]

2021 年 6 月 15 日に刊行された本文書は、EU が同年 9 月 28 日に欧州委員会発出の通知文書「Global Approach to Research and Innovation: Europe's strategy for international cooperation in a changing world (R&I への世界的接近：変化する世界における国際協力に対する欧州の戦略)」に対し EUA の考えを表明したものである。EUA は、EU の考え方に自らの意見が反映されたとし、ルールに基づく構造と共通の価値に基づいて構築されたグローバルな研究とイノベーションの協力を促進する EU の方針を歓迎した。同時に、研究とイノベーションにおける国際協力は、単なる外交政策の手段ではなく、何よりもまず知識の創造を目的とすべきだとし、学術組織としての立場も強調する。

EUA は、研究の責任あるオープン化の包括的アプローチの重要性を訴え、特定の国の研究とイノベーションのオープン化の原則からの排除は、重大な脅威が存在する場合に限って例外的に適用されるべきだとの見解を示した。

成に努力することに合意した。なお、本宣言から始まった欧州における高等教育システムの改革に向けた動きを「ボローニャプロセス」と言う（QA UPSATES、 https://qaupdates.niad.ac.jp/bologna/）。

365 EUA, https://www.eua.eu

366 EUA, Project, https://www.eua.eu/our-work/projects.html

367 関係者への聞き取り調査による。

368 関係者への聞き取り調査による。

369 EUA Policy Inputs, Research and innovation as drivers of open international cooperation, https://www.eua.eu/publications/policy-input/research-and-innovation-as-drivers-of-open-international-cooperation.html

ii） Policy input: enhancing research security in Europe （政策提言：欧州における研究セキュリティの強化）[370]

2024 年 1 月 15 日刊行の本文書は、欧州委員会による「EU の研究セキュリティを高める（boosting research security in the EU）」への意見募集（call for evidence）に対する EUA の回答である[371]。EUA は、学問の自由、大学の自治、倫理とインテグリティが欧州の研究・教育システムの中で堅持されることが国際的な研究コミュニティにおいて欧州の地位を維持するために極めて重要であり、責任ある形で広範な国際協力を継続するためのリスク管理が求められると指摘し、欧州委員会の研究セキュリティに関するイニシアティブを歓迎した。

EUA によると、この EU のイニシアティブは EU の「経済安全保障戦略と開放的な戦略的自律性」方針の一環であり、開放的で責任ある協力に重点が置かれている点を評価でき、健全かつ責任ある国際化に資するものである。その上で、オープンで責任ある協力を重視した研究セキュリティ政策を一貫して適用し、研究と教育における EU のグローバルな役割についての政策と齟齬のないものにするために、リスク対象における均衡性（proportionality）の原則、対話と自治、協働体制の構築を提案した。

(c) 特色・注目点等

EU 本部のあるブリュッセルに本拠を置く、欧州の大学を代表する学術団体である EUA は、EU と良好な関係を築き、研究セキュリティに関してもその政策策定に一定の影響力もある[372]。2024 年 5 月 23 日の「研究セキュリティ強化に関する EU 理事会勧告」はその策定に先立ってステークホルダーに意見の提出を呼び掛け、EUA もそれに応じて「政策提言」を提出し、EUA が表明した懸念や提案は勧告の中に反映された。EUA の意見は欧州の大学と学長団体の代表するものであり、その内容は専門家を交えた議論に基づく高い専門性を備えていたためと考えられる。

EUA では、欧州委員会から新しいイニシアティブや政策が提案されると、スタッフはタスクフォースを立ち上げ、異なる国々から数名の専門家の参加を募り、時間をかけて議論をして対応や意見をまとめる。国毎に事情が異なるため、必ずしも意見が一致するわけではないが、時間をかけた丁寧な議論が進められる。

EU には同じような学術関係のステークホルダーは数多く存在しているが、EUA は組織力や代表性、そして政策形成力において秀で、ロビー団体として EU 域内の大学の利益を代表するだけでなく、欧州委員会の政策パートナーとして EU の研究セキュリティ政策に

---

370 Policy inputs, enhancing research security in Europe, https://www.eua.eu/publications/policy-input/enhancing-research-security-in-europe.html

371 募集は 2023 年 12 月 6 日～2024 年 1 月 3 日まで実施され（European Commission, Boosting Research Security in the EU (guidance), About this initiative, Call for evidence, Feedback, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance-_en）、56 の機関及び個人よりフィードバックがあった（Boosting research security in the EU, Showing results, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14056-Boosting-research-security-in-the-EU-guidance-/feedback_en?p_id=17675）。

372 関係者への聞き取り調査によると、欧州委員会は EUA を含むステークホルダーの声をその政策アプローチに反映させようとしていると評価できるという。

貢献している点は注目される。

(2) 全欧州アカデミー（All European Academies）

(a) 背景・経緯等

All European Academies（ALLEA）は、ヨーロッパと国際社会における発信力を高め、科学を世界的な公共財として、国境を越えた科学的協力を促進することを目的に 1994 年に設立された。約 40 の EU 及び非 EU 諸国の約 60 の学術団体から構成される自然科学と人文科学の学術連盟である。ここで言う学術団体とは、例えばイギリス学士院やドイツ国立科学アカデミー（Leopoldina）のような、それぞれの国の学術を代表するアカデミーである[373]。なお、国によっては類似の団体が複数加盟しているため、加盟団体数が国数よりも多くなっている。ドイツのベルリンを本拠とし、ブリュッセルにプロジェクト事務所、ワルシャワに連絡窓口を置く。

欧州議会及び欧州理事会が重要とみなす政策課題に対しては、欧州委員会に設置された科学的助言機構（Scientific Advisory Mechanism: SAM）が独立した立場から科学的根拠を提示して政策提言を行う。SAM は 7 名の著名な科学者から構成される科学的助言者中核グループ（Chief Scientific Advisors Group）、SAPEA（Science Advice for Policy by European Academies、欧州の学術界による政策のための科学的助言）及び SAM 事務局から構成される。SAPEA は欧州の学術機関とアカデミーの意見や考え方を結集して、エビデンスを検討し、見解を統合する。その証拠や見解を根拠に、助言者中核グループが政策提言を行う[374]。

ALLEA は SAPEA（Science Advice for Policy by European Academies、欧州アカデミーの政策のための科学的助言）コンソーシアムの 6 つの学術団体の一つである[375]。EU の立法・政策の優先度の高い課題に対し、自然科学、工学技術、医学・健康科学、農業科学、社会科学、人文科学の各分野から卓越した専門家を結集して科学的な検証、助言をする SAPEA への参加は、ALLEA の旗艦的活動の一つである[376]。

研究セキュリティに関して、2024 年 12 月に声明書を発表した。2025 年 4 月には研究セキュリティへの対処のためのタスクフォース設置を準備し、その後発足した。研究の自由・研究者の自立を重んじるアカデミアと研究セキュリティには緊張が生じやすい。本団体も、研究セキュリティに対する EU の提案には理解を示しながらも、やはり学問の自由への懸念を示し、研究セキュリティを研究における原則（学問の自由、オープンサイエンス、国際協力）に統合するためのあり方を模索している。ALLEA の研究セキュリティに関連した取組を表 2-15 に示した。

---

373 ALLEA, https://allea.org/allea-in-brief/
374 European Commission, Scientific Advisory Mechanism, https://scientificadvice.eu/about-us/scientific-advice-mechanism/who-we-are/
375 他の 5 団体は、Academy of Europe (AE), European Academies' Science Advisory Council (EASAC)、European Council of Academies of Applied Sciences, Technologies and Engineering (Euro-CASE)、 Federation of European Academies of Medicine (FEAM) 、Young Academies Science Advice Structure (YASAS)である（ALLEA, Science advice, https://allea.org/science-advice/）。
376 関係者への聞き取り調査による。

表 2-15　全欧州アカデミー（ALLEA）の研究セキュリティ関連文書と取組

発行年	文書名
2024年12月18日	i) ALLEA Statement on research Collaboration and research Security in a Shifting Geopolitical Landscape（声明書：変わりゆく地政学的状況下における研究の協力とセキュリティ）
2025年 4月 16日～29日	ii) Call for Nominations: Task Force for Integrating Research Security and Academic Freedom（研究セキュリティと学問の自由の統合のためのタスクフォース候補者募集）
2025年~2027年	iii) Task Force: Integrating Research Security and Academic Freedom（タスクフォース：研究セキュリティと学問の自由の統合）
2025年9月10日	iv) ALLEA Response to the Call for Evidence on the ERA Act（ERA法制定に向けた意見募集への応答）

(b)　主な取組

i)　ALLEA Statement on research Collaboration and research Security in a Shifting Geopolitical Landscape（声明書 : 変わりゆく地政学的状況下における研究の協力とセキュリティ）[377]

2024 年 12 月 18 日に刊行された本文書は、近年の科学活動は、地政学的緊張の影響を受け、機密技術の急速な発展により研究成果のデュアルユースが可能になる中で行われることが増えており、研究と研究者自身の安全や研究パートナーシップの健全性に対する懸念が高まる現状において、知識、データ、インフラ、人材の保護を含む研究セキュリティへの対応の緊急性が増しているとの認識を示す。そして、研究セキュリティの課題は、欧州の学術機関にとって特に重要であるとし、研究者と研究機関は、科学が依存する開放性と国際協力を維持しつつ、複雑な規制環境を乗り切らねばならないと指摘する。特に政治的に不安定または制限的な状況下では、研究者の安全や研究パートナーシップの健全性に対する懸念が高まっていると述べる。

従って、新たな安全保障上の懸念への対処は必要だとする。だが、他方で、国際研究協力における開放性、研究の誠実性、学術的自由を保護する緊急の必要性があると訴え、EU 及び各国の政策立案者、研究資金提供者、学術機関に対し、責任ある国際化、欧州研究圏（ERA）の研究能力の構築、研究セキュリティと自由及び責任の統合のための調和的アプローチの採用を求める。すなわち、①研究の開放性とセキュリティのバランス、②欧州研究圏（ERA）全体での統一枠組み 、③共同研究におけるリスクを効果的に管理できるようなツールの開発と研修への投資 、④学問の自由や研究機関の自律性が十分に尊重されない環境下での共同研究を支援するためのガイドライン構築を提案した。

[377] ALLEA Statement on research Collaboration and research Security in a Shifting Geopolitical Landscape, https://allea.org/portfolio-item/allea-statement-on-research-collaboration-and-research-security-in-a-shifting-geopolitical-landscape/

ii） Call for Nominations: Task Force for Integrating Research Security and Academic Freedom（研究セキュリティと学問の自由の統合のためのタスクフォース候補者募集）[378]

新しい委員会とタスクフォースに参加する専門家を募集したが、タスクフォースの一つに「研究セキュリティと学術の自由の統合 」が含まれ、学術的価値と国際協力という基本的価値の維持を保証するための研究セキュリティ対策についての検討に入った。なお、募集期間は 2025 年 4 月 16 日～29 日であった。

iii） Task Force: Integrating Research Security and Academic Freedom（タスクフォース：研究セキュリティと学問の自由の統合）[379]

上記の募集の後、10 人のメンバーからなるタスクフォースがスタートした。高まる地政学的緊張と EU の研究政策の変化の中で、研究をセキュリティ上の脅威から保護しつつ、研究の開放性とインテグリティ、学問の自由を維持する方法を検討し、研究セキュリティ対策が国際協力を制限するのではなく支援するものとなることを目指す提言をまとめる。2025 年から少なくとも 2027 年まで、機関向けガイダンスの策定、均衡のとれたコンプライアンス枠組の推進、研究セキュリティと学問の自由に関する会議への意見提出などの活動を行い、学術的価値と国際協力が欧州の研究エコシステムの中核であり続けるよう支援するとしている。

iv） ALLEA Response to the Call for Evidence on the ERA Act （ERA 法制定に向けた意見募集への応答）[380]

既述の欧州委員会による ERA 新法制定に向けた意見募集に応じた文書において、2025 年 9 月に ALLEA は研究セキュリティに関する次のような見解を述べた。すなわち、新しい ERA 法は、加盟国の国際研究・イノベーション協力政策における整合性を高めると同時に、責任ある姿勢でグローバルな連携を推進すべきであり、研究セキュリティについては比例原則に基づく調和的な最低基準を策定し、EU 域内の正当な研究活動の開放性を維持しつつ、機微な知見を適切に保護すべきである。

(c) 特色・注目点等

EU 域内の大学の利益を代表してロビー団体的な性格を持つ EUA とは異なり、ALLEA は SAPEA のメンバーであり、また ERA フォーラムにおけるアカデミアの代表として EU の科学政策形成に助言をする諮問組織（advisory association）のような役割を担っている。そのため、エビデンスに基づいた提案を追求し、EU の政策形成に貢献することを目指している。つまり、EU の政策決定に直接的な影響力を行使するのではなく、欧州委員会が担う勧告やガイドラインの作成に科学的根拠のある情報と知見を提言して、より望ましい草案

[378] ALLEA, Taskforce, https://allea.org/task-forces/
[379] https://allea.org/task-forces/#toggle-id-2
[380] Feedback from ALLEA, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14608-European-Research-Area-Act/F3714470_en

が形成されるように支援する。このような形で、ALLEA も欧州委員会と欧州議会に影響力を与えていると言える[381]。

研究セキュリティについては、欧州旗艦会議の共催者となり、またタスクフォースを立ち上げて具体的な検討を進めるなど積極的な取組がみられる。研究セキュリティは現代の科学研究に関連した避けて通ることのできない課題だと認識する一方で、学問の自由、研究のオープン化、国際協力の原則について科学は妥協できないとの立場も堅持する[382]。EU の研究セキュリティの議論では、セキュリティと学問の自由の均衡を図るアプローチとして比例原則が提起されている。しかし、可能な限りの開放性とはどこまでを指し、必要最小限の閉鎖性の範囲は何か、具体的な物差しはなく、ケースバイケースとしている。

2.5.3　資金配分機関等における取組

(1)　欧州委員会

(a)　背景・経緯等

欧州委員会は、既述のように研究プログラム「ホライズン・ヨーロッパ」を運営する欧州最大の研究資金配分機関である。

ホライズン・ヨーロッパは、図 2-14 のように「卓越した科学」、「グローバルチャレンジ・欧州の産業競争力」、「イノベーティブヨーロッパ」の３つの柱と「参加拡大と欧州研究圏（ERA）強化」及び「欧州防衛基金（EDF)」から構成される。

図 2-14　欧州委員会 ホライズン・ヨーロッパの構成[383]

[381] 関係者への聞取り調査による。
[382]「優れた研究と科学への公共の信頼にとって学問の自由と制度的自律が不可欠だ」とする見解を示し、その擁護を ALLEA の主要な活動に掲げる（ALLEA, Activities: Academic Freedom, https://allea.org/academic-freedom/）。また、2025 年度に関係者へ実施した聞取り調査でも同様の発言があった。
[383] 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）「海外調査報告書：EU の研究・イノベーション枠組みプログラム・Horizon Europe」（2021 年）、https://www.jst.go.jp/crds/report/CRDS-FY2021-OR-02.html を基に未来工学研究所が作成した。

原子力分野の研究・イノベーション研究への資金提供を目的とした「Euratom」は、その補完的プログラムとして機能している。ただし、EDF はホライズン・ヨーロッパとは異なる規則と予算措置によって運用されており、ホライズン・プログラムとは 3 本柱及び「参加拡大と ERA 強化」と理解して良い[384]。

プログラムは 7 年毎に更新され、現在 2021 年から 2027 年を期間とした 955 億ユーロ規模の事業が執行中で、次期プログラムは 2028 年～2034 年に予定されている。助成金の募集は 2 年ごとに行われ、応募資格のある国/地域は、EU 加盟国（27 ヵ国）、アソシエイト国（22 ヵ国）及び低/中所得国である。これらに該当しない国（例えば米国、中国など）は、参加は可能ながら資金は自己調達しなければならない。ただし、作業計画並びに公募要項において、当該国が資金援助対象国として明示されている場合や資金助成機関が当該国の受益者としての参加がプロジェクト実施に不可欠だと判断されている場合には参加できる[385]。

(b) 主な取組

資金配分機関としての欧州委員会が発出するのは、助成申請者及び受給者向けの文書で、表 2-16 に示した。

2021 年 2 月「ホライズン・ヨーロッパ 2021 年~2027 年」の開始が発表され、同年 6 月には募集プログラム（ワーク・プログラム）が公開された。申請は 10 月より始まったが、それに先立って、研究セキュリティに係る 3 つの文書が相次いで発出された（表 2-16 参照）。

表 2-16 欧州委員会 ホライズン・ヨーロッパ: プログラム申請/受給者向け文書

発行年	文書名
2021年4月28日	i) Regulations （ホライズン・ヨーロッパ プログラム規則）
2021年7月1日	ii) EU Grants: How to handle security-sensitive projects （EU助成：安全保障上機密性の高い研究プロジェクトの取扱指針）
2021年9月14日	iii) Guidance note — Potential misuse of research （留意点：研究悪用の可能性, ガイダンス書①）
2021年9月14日	vi) Guidance note — Research with an exclusive focus on civil applications （留意点：民生用途のみに絞った研究、ガイダンス書②）

[384] 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）「海外調査報告書：EU の研究・イノベーション枠組みプログラム・Horizon Europe」（2021 年）、https://www.jst.go.jp/crds/report/CRDS-FY2021-OR-02.html

[385] List of Participating Countries in Horizon Europe（1 11/07/2014）, EU Funding Portal, https://eufundingportal.eu/horizon-europe-associated-countries/; https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_v3.1_en.pdf

i) Regulations（ホライズン・ヨーロッパ プログラム規則）[386]

本規則（2021 年 4 月 28 日発出）は、2021 年から 2027 年までの期間における EU の研究・イノベーション（R&I）枠組プログラムである「ホライズン・ヨーロッパ」を確定することを目的に、その参加規則、成果の普及、及び R&I プロジェクトに対する EU 資金援助を統括する一般原則を定めている。これに伴い、ホライズン・ヨーロッパ 2020 年の規則は廃止された。規則は、プログラムの一般的かつ具体的な目的を定義し、EU 資金が貢献し得る主題別優先事項と広範な「活動分野」を特定した後、参加資格のある主体と参加者（機関）の義務、資金形態と資金受領義務、ガバナンスと倫理及びインテグリティに関する規定が述べられている。補遺において、ホライズン・ヨーロッパの下で 9 つの共同事業体（官民パートナーシップ）の設立とその枠組構築に対する支援が盛り込まれている。

参加主体（大学、研究機関、産業、中小企業など）には、オープンアクセス、データ共有、知的財産、ライセンスを含む成果の普及に関する義務、そして費用償還、監査、財務チェックといった資金に関する規則に準ずることが求められる。ガバナンスと倫理及びインテグリティは、ヒト被験者、デュアルユース、環境影響などの倫理要件及びそのチェック体制及び監視規定、EU の広範な財務規則に沿った健全な財務管理、不正防止措置、監査及び統制を確保する義務から構成される。また、「オープンサイエンス」とオープンデータに重点が置かれ、成果の早期共有と再利用、透明性の促進が謳われている。

本文書では、デュアルユース関連条項と「安全保障 security」が重要である。ただし、ここでは「デュアルユース」という用語は使われていない。それに相当する内容が第 7 条「プログラムの基本原則」第 1 項に明示されている。すなわち、防衛研究プロジェクトへの参加規則を定める欧州議会及び欧州理事会規則における「欧州防衛基金」の下で実施される活動は防衛研究開発にのみ焦点を当てるべきである一方、「イノベーティブ・ヨーロッパ」と「参加拡大と欧州研究圏（ERA）強化」によって実施される R&I に関する活動は専ら民生用途（civil applications）に限定される必要があるとする。

「安全保障 security」（第 20 条）が対象とするのは、「研究セキュリティ」だけではなく、EU の外交や防衛、経済など幅広い安全保障法規に係る事柄で、表 2-17 のような留意すべき項目が列挙されている。

386 Regulations, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0695

表 2-17　欧州委員会 ホライズン・ヨーロッパ規則第 20 条「安全保障（security）」が列挙する留意事項

条項	概要
第1項	・本プログラムの下で実施される活動は、安全保障規則、特に 機密情報の不正開示防止に関する規則に準拠すること。 ・EU域外で機密情報を使用または生成する研究を行う場合は、これらの要件の遵守に加え、研究が実施される第三国とEUとの間で安全保障協定が締結されていること。
第2項	・提案書には安全保障自己評価を含め、あらゆる安全保障上の課題を特定し、関連するEU法及び国内法に準拠するための課題に対処する方法を詳細に記述すること。
第3項	・必要に応じて、欧州委員会または関連する資金提供機関は、安全保障上の問題を生じさせる提案について、安全保障審査手続を実施すること。
第4項	・本プログラム下で実施する活動は、EU（もしくはEuratom）の実施規則に準拠すること。
第5項	・活動に参加する法人は、当該行動で使用または生成される機密情報の不正開示に対する保護を確実にすること。 ・関係者は活動開始前に、個人保安審査または施設保安審査の証明を、関連する国家保安当局から取得すること。
第6項	・独立した外部専門家が機密情報を取り扱う必要がある場合、当該専門家を任命する前に適切な保安審査の実施が求められる。 ・欧州委員会または関連する資金配分機関は機密情報を取り扱う提案に対して保安審査手続きを実施すること。
第7項	必要に応じて、委員会または関連する資金配分機関は保安審査を実施できる。
第8項	本第20条に基づく保安規則に準拠しない活動はいつでも却下または終了させられる可能性がある。

ii)　EU Grants: How to handle security-sensitive projects　（EU 助成：安全保障上機密性の高い研究プロジェクトの取扱指針）[387]

本指針（2021 年 7 月 1 日発出）は、セキュリティ自己評価を EU の資金配分機関がセキュリティ上機密性の高い助成契約を締結する前に実施すべきセキュリティ審査プロセスの一部と位置付ける。その目的は、申請者および受益者のプロジェクトに機密情報もしくはそれに分類される情報が関与する場合に従う必要がある追加手続きの概要を示し、提案段階におけるセキュリティ自己評価および助成金準備中に提出を求められる可能性のある特別なセキュリティ文書の作成、さらにプロジェクト実施期間中の機密性のあるプロジェクトの取扱に関する指示への対応を支援することである。

主にホライズン・ヨーロッパ、デジタル・ヨーロッパ、欧州防衛基金を対象に作成されているが、資金承認にセキュリティ審査を必要とする可能性のある他の助成金プログラムにも適用可能である。研究プロジェクトの提案（申請）、助成金準備（採択）及び実施のそれぞれの段階において要請される可能性のある事項が説明されている。

EU 機密情報（EU classified information: EUCI）の分類やその他のセキュリティ上の推奨事項が必要になる可能性について特定し、機密レベル扱いとなった提案書は正式な安全保障審査（国家安全保障当局の専門家が参加する場合あり）を受け、適用すべき機密指定レベルが決定されることになる。

表 2-18、2-19、2-20 に申請書作成と応募、採択からプロジェクト開始まで、プロジェクトの実施までの各段階毎にセキュリティ自己審査手順を示した。

[387]EU Grants: How to handle security-sensitive projects,
https://www.euresearch.ch/en/app/core/action/service/table/section_asset/id/499/service/app_euresearch_inputtype_file_service_protectedfilesystemproxy/inputtype/file/lang/en/derivative/original/lm/1629980316/

表 2-18　欧州委員会 ホライズン・ヨーロッパの提案段階（申請書の作成と応募）におけるセキュリティ自己審査手順

提案段階：申請書の作成と応募		
総論		提案段階では、セキュリティに係る問題の一覧表に記入し（提出システム上で直接、または紙媒体で）、問題があった場合にはその対応方法を説明するセキュリティ自己評価を合わせて提出すること。
細目	非EU国家の参加者のEUCI取扱	・当該プロジェクトが不正開示に対する保護を必要とする情報及び/もしくは資料（EUCI）を伴い、その機密が背景（background）情報として用いられる場合、EUが機密指定するフォアグラウンド情報が成果に含まれる予定で、当該プロジェクトに非EU国の関与があり、機密扱いの背景情報を使用する場合には、事前に情報作成者（すなわち、当該情報の作成及び機密指定を行った権限を有する機関）には、正式な書面による承認の取得が求められる。 ・EU域外国のプロジェクト参加者（受益者、関連団体、連携パートナー、下請け業者など）のEUCIへのアクセスは、その参加者が所在するEU域外国がEUと情報保護協定を締結している場合にのみ可能である。非締結の場合は、当該業務をEUCIへのアクセス可能な参加者に割り当てること。
	誤用	悪意ある目的に悪用される可能性のある材料、方法、技術または知識を伴う、もしくはそれらを生成する活動に関与するプロジェクトで、個人、集団または国家の安全保障に重大な直接的影響を及ぼす可能性があり、当該プロジェクトが加盟国の利益を損なう恐れのある結果をもたらす場合は、機密指定される。
	その他のセキュリティ上の問題	プロジェクトが想定外のセキュリティ上の問題や懸念を引き起こす場合、国家安全保障上の制限（悪用以外のもの）とその例外の問題の両方を対象に、問題点と対処法の説明義務が生じ、状況を分析、問題解決のための適切な支援の提供を受けることができる。

この手順では EUCI、機密背景（background）情報、機密フォアグラウンド情報が用語として重要で、それぞれ次のように定義されている。

EUCI とは、プロジェクトの結果として生成され、不正開示からの保護が必要な情報（文書、成果物、資料）で、当該プロジェクトが安全保障に機微な主題に関わる、もしくは安全保障に機微な活動類型に該当する場合に必要となる。機密背景情報は、EU 機関、EU 加盟国、非 EU 国または国際機関によって既に機密指定され、プロジェクトの期間中及び目的のために使用されることが想定されるあらゆる情報（文書、成果物、資材）である。そして、機密フォアグラウンド情報は、EU 機関、EU 加盟国、非 EU 国または国際機関によって既に機密指定され、プロジェクトの期間中及び目的のための使用が想定されるが、EU によって機密指定されていない情報（文書/成果物/資材）である。

表 2-19　欧州委員会 ホライズン・ヨーロッパ 助成金準備段階：採択からプロジェクト開始までのセキュリティ自己審査手順

助成金準備段階：採択からプロジェクト開始まで		
細目	機密情報:SAL及びSCG	・プロジェクトがEUCIを扱う場合、採択後に助成金契約書にセキュリティ面の書簡（Security Aspects Letter、SAL）及びセキュリティ分類ガイド（Security Classification Guide、SCG）を付属書に追加することが求められる。 ・SALにはEUCIに関連するプロジェクト固有の保安要件（例えば、機密指定レベル、国際機関であるコンソーシアムメンバーによるアクセス、EU域外国の組織・団体など）の記載では、SCGは補助金契約の機密要素（成果物）とその保安機密指定レベルの説明をしなければならない。SAL及びSCGは、保安審査手続（SecSR）の結果に適合させること。 ・SCGにおいて、機密背景情報とフォアグラウンド情報に関しては、いずれも当該プロジェクトの遂行において把握しておくべき全ての組織を記載すること。未記載組織はたとえプロジェクトコンソーシアムに属していても、記載された機密情報へのアクセス権限はない。
	その他のセキュリティ推奨事項	・SALおよびSCGに加えてその他にもセキュリティ推奨事項に関する情報、例えば機密情報へのアクセスに関する推奨事項、セキュリティ担当者、ITシステムへのアクセスなどの記入が求められる。 ・プロジェクトが機密扱いの背景情報またはフォアグラウンド情報を含む場合には、セキュリティクリアランスの資格を持つプロジェクトセキュリティ担当官（PSO）を１名任命すること。 ・プロジェクトが機密扱いの背景情報またはフォアグラウンド情報、もしくは機密扱いのセキュリティ勧告を伴う成果物を含む場合、セキュリティ諮問委員会の設置が必要になる。

表 2-20　欧州委員会 ホライズン・ヨーロッパ プロジェクト実施段階のセキュリティ自己審査手順

プロジェクト実施段階	
細目	・プロジェクト実施中のセキュリティ問題はPSO及び/もしくはセキュリティ諮問委員会が管理する。 ・セキュリティ勧告が付された機密情報またはEUCIは、機密指定された権限を有する機関（作成者）の事前の書面による同意なしに、機密指定の解除、機密解除、またはさらなる配布を行ってはならない。 ・EUプロジェクトで生成されたEUCIについては、原則として欧州委員会が情報作成主体になる。 ・機密情報については、「Funding & Tenders Portal」の電子交換システムでの使用は禁止され、質問はEUプロジェクト担当官に直接連絡 すること。

iii)　Guidance note—Potential misuse of research（留意点：研究悪用の可能性（ガイダンス書①））[388]

2021 年 9 月 14 日発出の本文書は、安全保障上の懸念を引き起こす可能性のある情報の使用もしくは生成を伴うプロジェクトにおいて、研究の潜在的な悪用を特定し適切に対処するための助けになることを意図している。ここで言う安全保障は、経済、外交など広範に及ぶ一般的に用いられる概念を指し、また「悪用」とは犯罪／テロ活動に転用可能な知識、材料、技術を創出する可能性のある行為、そして化学・生物・放射性物質・核（CBRN）兵器及びその運搬手段の開発につながる可能性のある行為である。なお、安全保障面に関連しない研究不正行為（研究結果の改ざん、科学的証拠の捏造、剽窃等）は、倫理セクションの

[388] Guidance note — Potential misuse of research, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-potential-misuse-of-research-results_he_en.pdf

問題として除外される。デュアルユースに係る悪用の特定と対処に関する事項を表 2-21 に示した。

表 2-21　欧州委員会 ホライズン・ヨーロッパ 留意点（ガイダンス書①） デュアルユースに係る悪用の特定と対処

項目	説明事項
潜在的悪用とは	・犯罪やテロ目的で利用可能な知識・材料・技術の創出 ・化学、生物、放射性物質。核及びCBRNによる兵器またはその運搬手段の開発につながる可能性 ・人権や市民的自由を制限する監視技術の開発への関与 ・社会的・行動的・遺伝的プロファイリング技術の開発によって、少数派や脆弱な集団に関連、もしくはその集団の人々に烙印を押したり、差別や嫌がらせ、もしくは威嚇を行う可能性のある技術 ・ 流通、改変、増強によって人間、動物、環境に危害を加える可能性のある材料、方法や技術或いは知識の開発
悪用可能性特定のための質問例	・対象となる材料・手法・技術または知識それ自体または改変・強化された状態で、物理的またはその他の方法で、人・動物・環境に危害を及ぼす可能性はないか？ ・物理的またはその他の方法で、個人・集団・国家の安全保障に直接的な悪影響を及ぼす可能性はないか？ ・それらの不正開示によってEUまたはその加盟国の利益を損なう可能性はないか？ ・監視技術の開発を伴わないか？ ・それらが悪意ある者の手に渡った場合、何が起こるのか？ ・それらは意図された目的以外の用途に供される可能性はないか？ ・当該活動は、少数派や脆弱な集団に関わるものではないか？ ・社会的・行動的・遺伝的プロファイリング技術の開発を伴う、犯罪やテロ目的で使用され得る知識・材料・技術を生み出したり、化学、生物、放射性物質、核及びCBRNによる兵器の開発、製造、使用、輸送、発射、またはその他の方法による使用を可能にしたりする技術の開発に繋がるなどの可能性はないか？
潜在的な悪用への対応 （例）	・追加のセキュリティ対策（例：物理的セキュリティ対策、特定の成果物の機密指定、機密情報の拡散制限な）の実施 ・セキュリティ上の推奨事項に基づき、研究成果の一部のみの公開 ・プロジェクト関係者に対するセキュリティクリアランスの実施 ・追加的な安全対策（例：職員への安全研修の義務化）の実施 ・ダミーデータの活用など研究の設計上の工夫 ・輸出規制適用 ・提案書内の「セキュリティ課題表」及び、または「倫理課題表」への記入
義務違反	以上の義務のいずれかに違反した場合、助成金の減額または打切りになる可能性がある。

iv） Guidance note — Research with an exclusive focus on civil applications（留意点：民生用途のみに絞った研究（ガイダンス書②））[389]

ガイダンス書①とセットで発行された本文書において、ホライズン・ヨーロッパの資金提供は、民生用途に焦点を当てた R&I プロジェクトのみを対象とし、軍事用途での使用を意図した研究は対象外であることが明記された。本文書は申請予定の研究がこの基準を満たしているのか、判断するための指針を提供している。民生用途の判断基準において「デュアルユース」の取扱いが説明されており、その要約は次の通りである。

軍事用途を意図あるいは軍事目的とする研究は資金提供の対象とはならない。しかし、防衛産業や軍事組織が関与するプロジェクトが自動的に資金提供から除外されるわけではなく、研究活動が専ら民生用途に焦点を当てている場合に限って参加が可能である。しかし、多くの技術や製品は汎用性があり、民生ユーザーと軍事ユーザー双方のニーズに対応可能な場合には、「デュアルユース物品・技術」と呼ばれる。デュアルユース技術・物品の開発・改良を目的とする研究であっても、当該物品・技術が民生用途を意図している限り、資金提供の対象となり得る。

申請書では、「民生用途」について、2 点を確認しておく必要がある;

[389] Guidance note — Research with an exclusive focus on civil applications, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/guidance-note-research-focusing-exclusively-on-civil-applications_he_en.pdf

① 提案の研究活動が専ら民生用途に焦点を当てていること
② 提案の研究活動が民生と軍事両用物品、またはその他の認可が必要な物品を扱う場合、これらの物品の使用・輸出入に先立ち、関連する法的義務（輸出入許可など）を遵守すること

(c) 特色・注目点等

以上のホライズン・ヨーロッパ助成金の申請者及び受給者向けの 4 文書は、中国を「体制的ライバル」と見做し、同国への技術流出への警戒を強めた 2 年後の 2021 年に発出された規程とガイダンス書である。いずれも焦点はデュアルユース技術の流出防止措置で、手順が詳細に説明されている。2021 年開始のホライズン・プログラムは 2027 年で終了し、2028 年より次期プログラムが開始される予定である。

2.5.4 まとめ

欧州委員会は、勧告や提案などを一方的に発信するのではなく、「意見募集の呼びかけ（call for evidence）」を実施して、加盟国、域内の大学・研究機関、学術団体、研究者等ステークホルダーから意見を聴取し、アイデアや要望を取り入れる対話型の手法を採用しており、ボトムアップな意思決定が試みられている。加盟国の上位組織として全体的方向性や政策を提示し、各国にそれらに準拠した施策を立て、実施することを推奨する。

EU の決定事項は、①規則（regulation）、②指令（directive）、③決定（decision）、④勧告・意見（recommendation）の 4 つのレベルに分けられ、加盟国への強制力は①が最も強く、順次低下する[390]。研究セキュリティ関連文書に一般的である勧告に強制力はないものの、加盟国の対応を左右し、一定の影響力を持ち、加盟各国は勧告や通知を受けて国内施策を確立する。しかし、加盟 27 カ国の対応はまちまちで、違いがみられる。加盟国の事情は個々に異なるため、加盟国ごとに効果的な方法論やアプローチは違ってくるはずで、加盟国を網羅する統一的な方向性を示すことは困難な作業だと考えられる。

こうした問題の解決の一手段として欧州委員会が取り入れていると考えられるのが、ステークホルダーとの対話であり、有識者の助言である。国家の枠を超えて、研究セキュリティの課題に利害関係を持つ大学・研究機関の代表者、そして深い学識を持つ専門家集団の意見を聞き、議論することによって、勧告やガイドラインの内容をより現場に即した実効性のあるものにできる。一方、対話によってステークホルダーには課題を共有し、研究セキュリティを自らの課題として取組む機運が生じ、市民レベルからの協力が生じ、それは加盟国の取組にも影響する。

研究セキュリティの取組において鍵となるのがステークホルダーとの課題の共有であり、その協力である。今回取り上げた学術団体は、いずれも EU と歩調を合わせて、協力と協働の姿勢を示す。また、研究セキュリティ欧州旗艦会議には EU 域内の 12 の学術団体が共催者となって、「欧州のアプローチ」を検討した。欧州研究セキュリティ専門センターが設立

390 総務省、欧州連合（EU）通信、https://www.soumu.go.jp/g-ict/international_organization/eu/pdf_contents.html

され、より厳格なリスク管理が制度化されることになるが、ステークホルダーとの協力関係の構築や対話、ボトムアップな取組は EU の特徴であり、また学ぶべき点であると考えられる。

2.6 オランダ

2.6.1 研究セキュリティ・インテグリティ関連政策動向

(1) 2024 年度までの経緯

オランダにおいては、「研究セキュリティ」に関する用語として、機密性の高い知識や技術の好ましくない移転を防ぐことを意味する「知識セキュリティ」（Knowledge Security）という用語を使用している。

2022 年 1 月 31 日、オランダ政府は、オランダ大学協会（Universities of the Netherland: UNL）、オランダ科学研究機構（Dutch Research Council: NWO）、オランダ王立芸術科学アカデミー（Royal Netherlands Academy of Arts and Sciences: KNAW）等の協力を得て、「National Knowledge Security Guidelines」[391]を発表した。このガイドラインは、国際共同研究を推進するうえで、機密性の高い知識や技術の好ましくない移転のリスクを検討することが求められる大学・研究機関の管理者のための指針である。

また、同時期に、オランダ政府省庁間の共同で、「National Contact Point for Knowledge Security」（知識セキュリティ国家連絡窓口）を設置し、「Knowledge Security Desk」を立上げた。これは、大学・研究機関が、気軽に国際共同研究に関連する機会とリスク、実務的な事項等に関連する質問をすることができる中央窓口として意図されている[392]。

2023 年 4 月、資金配分機関であるオランダ科学研究機構（NWO）は、「知識セキュリティ」をさらに強化するため、資金調達プロセスにおける新たな方針を導入した。大学・研究機関が申請書を提出する際は、申請者は、「National Knowledge Security Guidelines」を遵守することが必須となった。申請者は助成金の申請時に、当該大学・研究機関が同ガイドラインの要求事項に従って運営されていること、及び申請書が本ガイドラインに準拠していることを確認することが要求されることになった[393]。

2024 年 4 月 19 日、オランダ大学協会（UNL）はオランダの大学に対して、知識セキュリティポリシーの設計・実施を支援し、自大学の知識セキュリティの「成熟度」について内部評価し、段階的に改善することができるように、「Capability Maturity Model Knowledge Security」[394]を公開した。

以上を踏まえて、図 2-15 に、知識セキュリティ政策に関与する関係機関の役割と機関間の関係を示す。また、表 2-22 に、オランダで、最近発行された知識セキュリティに関連する公的文書を示す。

---

391 Government of the Netherlands, “National knowledge security guidelines: Secure international collaboration,” January 2022. https://english.loketkennisveiligheid.nl/site/binaries/site-content/collections/documents/2022/04/07/national-knowledge-security-guidelines/National+Knowledge+Security+Guidelines.pdf

392 Loket Kennisveiligheid. https://www.loketkennisveiligheid.nl/

393 Knowledge security. https://www.nwo.nl/en/knowledge-security

394 Universities of the Netherlands, “Capability Maturity Model Knowledge Security,” April 19, 2024.

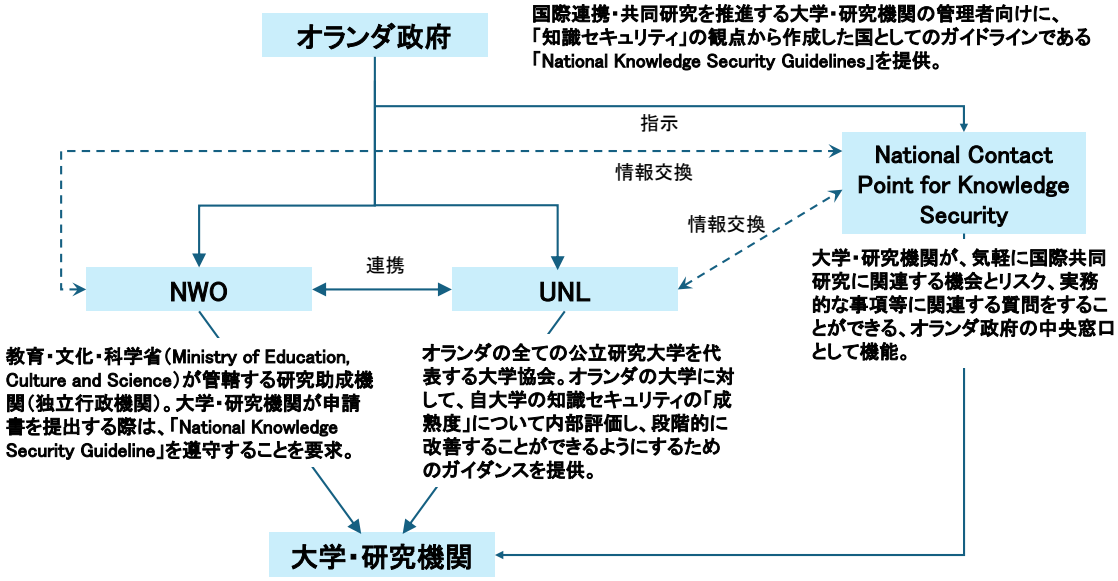


図 2-15　知識セキュリティ政策に関与する関係機関の役割と機関間の関係

表 2-22　2024 年までに発行された Knowledge Security に関連する主な公的文書

発行年月	文書名	発行元
2022 年 1 月	National Knowledge Security Guidelines	オランダ政府
2024 年 4 月	Capability Maturity Model Knowledge Security	UNL

(2)　最近の主な動き

(a)　Knowledge Security Screening Bill（知識セキュリティ・スクリーニング法案）[395]

2025 年 4 月 7 日、教育・文化・科学大臣（Minister of Education, Culture and Science）と司法・安全保障省大臣（Minister of Justice and Security）との共同で、「機微な知識又は技術」を扱う研究大学、応用科学大学などの研究機関の研究者および修士課程学生を対象として政府によるスクリーニング（審査）を義務付ける「Knowledge Security Screening Bill」（知識セキュリティ・スクリーニング法案）が、オランダ議会下院に提出された[396]。同法案により、審査（スクリーニング）の対象となるのは、国家安全保障やデュアルユースへの応用が懸念される以下の 21 の分野[397]である。

---

[395] Regels tot invoering van een screening om ongewenste kennis- en technologieoverdracht via onderzoekers, studenten en technisch ondersteunend personeel van kennisinstellingen te voorkomen en daarmee risico's voor de nationale veiligheid te verminderen (Wet screening kennisveiligheid) https://www.internetconsultatie.nl/screeningkennisveiligheid/document/13882

[396] Screening for researchers wising to handle sensitive knowledge. https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-sensitive-knowledge

[397] 概ね、米国の CETs リスト（Critical and Emerging Technologies）(White House, "Critical and Emerging Technologies List Update," A Report by the FAST TRACK ACTION SUBCOMMITTEE ON CRITICAL AND EMERGING TECHNOLOGIES of the NATIONAL SCIENCE AND TECHNOLOGY COUNCIL, February 2024.)に対応している。

- ハイパフォーマンス・コンピューティング・システム
- AI
- 高度データ分析（予測分析、処方的分析）
- バイオテクノロジー
- 化学技術（マイクロ／ナノリアクター）
- 通信・ネットワーク技術
- サイバーセキュリティ技術
- エネルギー技術（ガスタービン、エネルギー貯蔵、水素技術）
- 先端材料
- 半導体技術
- 極超音速技術
- 量子技術
- 軍事応用技術
- ナノテクノロジー
- 原子力技術（原子力エネルギー技術、原子力および推進技術、核物質の検出・特性評価技術等）
- 光学及びフォトニクス技術（先進的イメージング技術、高出力レーザー、光学センサー／フォトニックセンサー等）
- 測位・航法・タイミング（PNT）技術
- ロボティクスおよび自律システム
- 宇宙技術
- センサー技術（ソナー、レーダー、センサー融合・アレイ技術等）
- シミュレーション技術（デジタルツイン技術、拡張現実、仮想現実、複合現実等）

大学・研究機関は、専門的知識や技術を扱う部門・研究部門のリスト化、報告義務、適切な知識セキュリティ措置を講じる義務などが課される。

この法律が施行されると、機密性の高い知識や機微技術を取り扱う環境で働きたいと考える研究者（博士課程の学生を含む）や修士課程の学生は、経歴に関わらず審査を受ける必要がある。政府機関（司法機関等）が審査の実施主体[398]とされており、研究者の警察に関する記録や過去の学歴・職歴に加え、家族背景や特定政権との接触歴など、より徹底的な調査が可能になるとされる。オランダ情報機関が収集した情報もリスク評価に活用される[399]。

この法律が施行された場合、年間約 8,000 件程度の審査の実施が見込まれている。同法案は審議中であり、2027 年半ばの法施行を目標としている[400]。

398 Screening for researchers wising to handle sensitive knowledge. https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-sensitive-knowledge
399 The Netherlands to screen academics to stop knowledge leaks. https://www.dutchnews.nl/2025/04/the-netherlands-to-screen-academics-to-stop-knowledge-leaks
400 Screening for researchers wishing to handle sensitive knowledge. https://www.government.nl/latest/news/2025/04/07/screening-for-researchers-wising-to-handle-

2.6.2　大学における取組

オランダに関しては、公開情報の枠組みで２つの大学（アムステルダム大学（University of Amsterdam: UvA）及びアムステルダム自由大学（VU Amsterdam））における知識セキュリティに関する取組について整理した。

なお、アムステルダム自由大学については、別途聞き取り調査を実施したが、本報告書における記述は、公開情報のみに基づいて整理した。

(1)　アムステルダム大学（UvA）

(a)　大学における知識セキュリティの位置づけ

UvA は、現在の世界における地政学的情勢の激動を踏まえ、安全で強靭な社会構築への大学の役割がますます注目されているとし、同大学として、こうした複雑な社会的課題やテーマに関する知識の構築に取り組む責任を負っていると述べている[401]。

同大学は、知識セキュリティを、他機関等とのパートナーシップにおける知識の悪用、転用、不適切な移転等を念頭に置いた、「安全保障リスク管理」として位置づけている。その中で、同大学の活動は、適用される法的枠組みと外部機関との連携に関する倫理的枠組みの範囲内で行われるとしている[402]。

UvA は、同大学の貢献についての透明性を重視していることから、同大学が参加する可能性のあるプロジェクトについては、知識セキュリティに加え、倫理面及び社会面への配慮を行い、それらを厳しく評価するとしている[403]。

(b)　知識セキュリティの考え方、ガイドライン、ツール等

UvA は、自由な学術交流はより優れた科学を生み出すとしており、世界的に共有される科学的手法は、政治的相違よりも強力であると考えている。しかし、同大学は、国内外の多くのパートナーと協力している中で、この自由は無制限では無いと考えている[404]。

同大学は、学術機関としての基本原則の一つは、人権侵害や戦争犯罪に関与しないことである[405]として、共通の価値観に基づくプロジェクトにおいて協力することを目指して、外部との連携の可否を判断する評価ガイドライン（Assessment Guidelines）[406]を作成している[407]。このガイドラインは、外部との連携に関する倫理的リスクを特定し、適切なフォローア

sensitive-knowledge

401 How the UvA contributes to a safe and resilient society. https://www.uva.nl/en/research/research-environment/third-party-collaborations/defence-sector-police-and-others/how-the-uva-contributes-to-a-safe-and-resilient-society.html

402 Assessment guidelines. https://www.uva.nl/en/research/research-environment/third-party-collaborations/assessment-guidelines/ethical-assessment-of-collaborations.html

403 Ibid.

404 Ethical assessment: Conflict zones and human rights violations. https://www.uva.nl/en/research/research-environment/third-party-collaborations/conflict-zones-and-human-rights-violations/conflict-zones-and-human-rights-violations.html

405 Ibid.

406 内部資料であるため、外部からはアクセスできない。

407 Assessment guidelines. https://www.uva.nl/en/research/research-environment/third-party-collaborations/assessment-guidelines/ethical-assessment-of-collaborations.html

ップ措置の決定を支援するとしている。

外部連携の評価に関しては、個別の協力関係（共同論文、学会発表、ゲスト講義、学生インターンシップなど）は対象外であるが、交換留学生、企業・非営利団体・政府との共同研究、データ共有契約、UvA の活動への単独資金提供等といった正式な協力関係は、大学の承認がないとプロジェクトを開始することができない。この評価では、特に以下の問いに焦点を置いている[408]。

- プロジェクトが武力紛争や人権侵害に寄与するリスクが存在するか？
- 知識の安全保障へのリスク、または望ましくない軍事・テロ目的での知識悪用のリスクが存在するか？
- プロジェクトが、環境、生物多様性、人間の健康、文化遺産・動物福祉等への不可逆的損害に寄与するリスクが存在するか？

外部連携の評価は、以下に示すように個別対応であり、「第三者との協力に関する諮問委員会」（Advisory Committee on Collaboration with Third Parties: ACEC）の助言を必要とする[409]。

- 既存および将来の協力関係に対し、必要に応じて評価、助言、及び決定を提供する。
- 研究協力に加え、教育協力、患者ケア、研究成果の社会還元・事業化プロジェクト等も、「第三者との協力に関する諮問委員会」に助言を依頼することが可能。
- 評価、助言および決定は常に個別対応であり、特定の合意・時期・形式にのみ適用される。
- 大学として、特定の国や機関を協力・連携対象から全面的に排除することはない。

(c) 外部連携プロジェクトに関する評価手順

UvA は、研究者が共同研究パートナーを選択する際の支援を目的として、2021 年に、前述した「第三者との協力に関する諮問委員会」を設置した[410]。

同諮問委員会は、同大学の全学部の経験豊富な研究者と政策担当官で構成され、研究者、研究責任者、その他同大学に関連する機関から提出された外部機関との共同研究を含む外部機関との連携に関する課題について定期的に協議を行うとしている。

同大学における外部連携プロジェクトの評価手順は、以下のとおりである[411]。

- 新規・既存のプロジェクトの評価にあたり、職員は段階的計画、質問票及び行動計画を

408 Ibid.
409 Ibid.
410 Advisory committee for academics. https://www.uva.nl/en/research/research-environment/third-party-collaborations/advisory-committee-for-academics/advisory-committee-for-academics.html
411 Assessment guidelines. https://www.uva.nl/en/research/research-environment/third-party-collaborations/assessment-guidelines/ethical-assessment-of-collaborations.html

含む一連のガイドライン[412]を活用するためのフローチャート（Flowchart external collaborations）（図 2-16 参照）を使用する。必要に応じて、職員は評価結果について、彼らの所属長、学部連絡担当者、または学部長と協議する。

- 執行委員会（Executive Board）または学部長は、プロジェクトを「第三者との協力に関する諮問委員会」の専門家に付託することを決定できる場合がある。同委員会は、関係する執行委員会または学部長に対し追加情報の提供を求める場合がある。
- 「第三者との協力に関する諮問委員会」は執行委員会または学部長に助言を行うものであり、プロジェクトに関する決定権は持たない。
- 「第三者との協力に関する諮問委員会」の助言を受けた後、学部長または執行委員会が当該プロジェクトに関する決定を行う。
- 上記の段階的計画は、学部または学科の手続きおよび合意事項を補完するものである。

412 具体的な内容に関する説明は記載されていない。

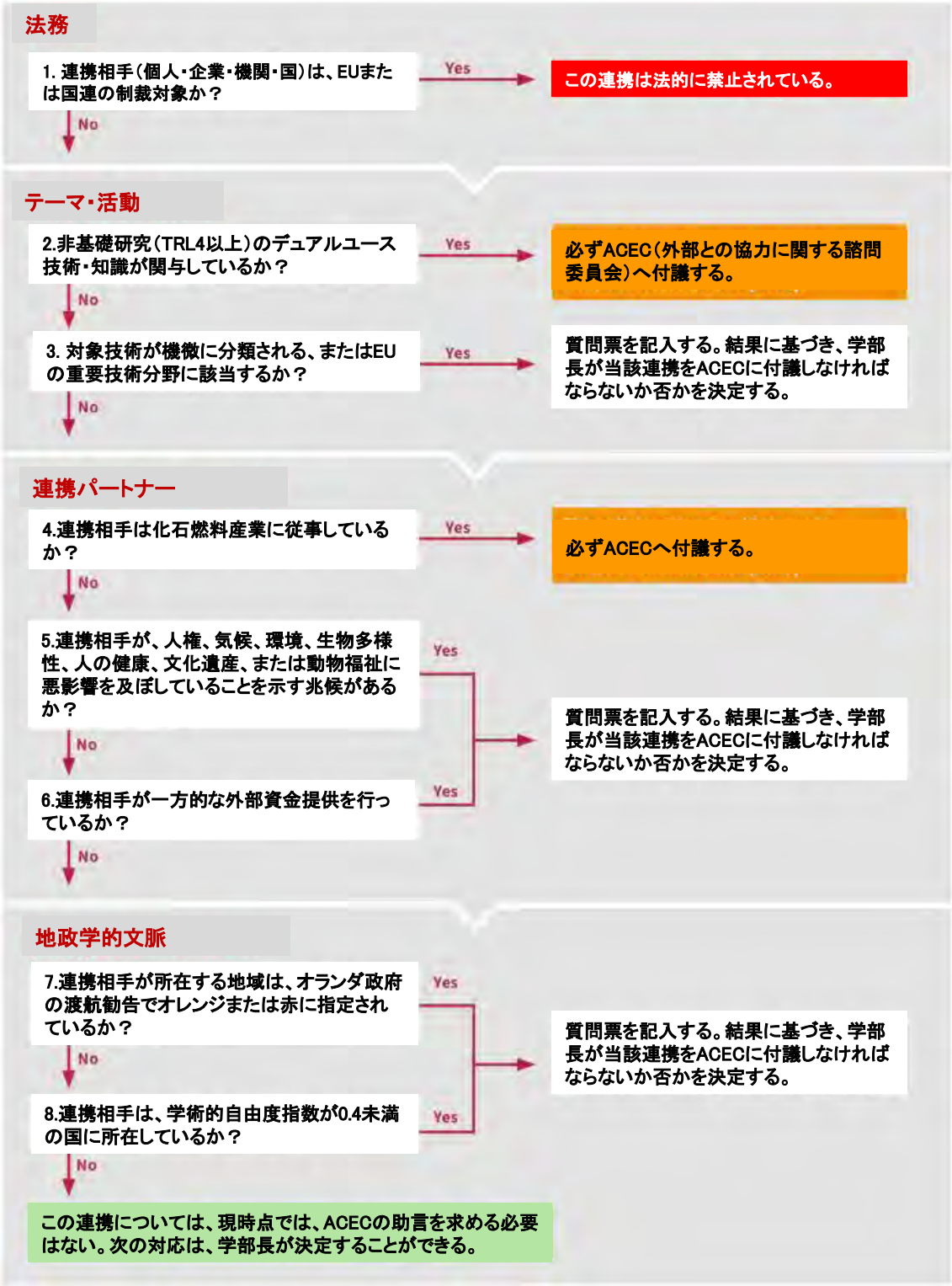


図 2-16　外部連携を評価する流れを示したフローチャート

（出典：UvA ホームページの図[413]に基づき、未来工学研究所が和訳・編集）

[413] Assessment guidelines. https://www.uva.nl/en/research/research-environment/third-party-collaborations/assessment-guidelines/ethical-assessment-of-collaborations.html

(2) アムステルダム自由大学（VU Amsterdam）

(a) 大学における知識セキュリティの定義と位置づけ

VU Amsterdam による知識セキュリティの定義は、以下のとおりである[414]。

- 知識セキュリティは、国際協力（国際共同研究・国際連携）が「安全に」行えるようにするための取組であり、これには、国際協力を取り巻く安全リスクを認識することを含む。これは、学問の自由と科学的インテグリティ（Scientific Integrity）という大学の中核の価値に立脚する。

同大学は、原則として、知識セキュリティとは、「機微な知識や技術の望ましくない移転を防ぐこと」としている。同大学は、知識セキュリティに関連して考慮すべき他の側面には、他国による教育・研究への隠れた影響があり、このような干渉は学術的自由と社会の安全に対する脅威になるとしている[415]。

また、同大学では、基本的人権を尊重しない国々との協力において、倫理的問題が知識セキュリティに対して大きな影響を与えるとしている。知識セキュリティは静的な概念ではなく、協力関係のある国の地政学的な態度の変化により、（継続中の）協力パートナーシップの見方に影響を与え得るとしている[416]。

(b) 主な取組

近年、VU Amsterdam は知識セキュリティに関して、以下の措置を講じている[417]。

- 知識セキュリティ諮問グループ（Knowledge Security Advisory Group）を設置。
- 拘束力のある「VU Knowledge Security Framework」を作成（2023 年 9 月 1 日）[418]。
- 知識セキュリティに関する質問は、職員が関連学部またはサービスの知識セキュリティ担当者に連絡することができる。担当者は、知識セキュリティ諮問グループによる研修を受けており、必要に応じて同グループに助言を求めることも可能である。
- オランダ国内の知識交流ネットワークに参加。
- VU Amsterdam 内のネットワークに職員向け情報ページを設置。継続的な意識啓発を実施。

知識セキュリティは、いわゆる高リスク国（ロシア、イラン、中国、北朝鮮など）に所属する博士課程学生やその他の研究職員を採用する際、特に重要な課題になるとし、こういった国々からの人材を採用するには、知識セキュリティチェックの実施が義務付けられてい

414 Knowledge Security Beta. https://vu.nl/en/employee/research-support-portal-science/knowledge-security-beta?
415 Knowledge security. https://vu.nl/en/about-vu/more-about/knowledge-security
416 Ibid.
417 Knowledge security. https://vu.nl/en/about-vu/more-about/knowledge-security
418 外部から「VU Knowledge Security Framework」にアクセスできない。

る。

学術的自由度指数（Academic Freedom Index）で低評価（0.4 未満）の国々、または高リスク国での研究活動にも知識セキュリティチェックを必要とする。VU では、知識セキュリティに関する取り組みを継続すること、また、可能な限り大学のプロセスに定着させることが重要であるとし、このため今後数年間は、「VU Knowledge Security Framework」の実装（新規提携の締結や既存提携の拡大）や意識啓発の継続、そして知識セキュリティ方針の継続的発展の一環としてガイドラインと対策の策定を進めていくとされている[419]。

(c) 主な文書・ツール

VU Amsterdam では、「VU Knowledge Security Framework」、職員採用前審査方針（Pre-employment screening）、知識セキュリティ・フローチャート等の文書が作成されている。うち、職員採用前審査方針および知識セキュリティ・フローチャートは公開されているが、「VU Knowledge Security Framework」は公開されていない。

(i) VU Knowledge Security Framework

「VU Knowledge Security Framework」は、同大学の学術的自由という中核的価値観、オランダ政府の「National Knowledge Security Guidelines」[420]及び研究インテグリティに基づくものとし、それらを遵守することが求められている。

当該フレームワークは、同大学における必要な知識セキュリティのプロセスを導くことを目的とし、国際協力の実施の可否または人材採用の可否を判断するためのものであるとされる[421]。同大学では、「VU Knowledge Security Framework」の中で、以下の事項を考慮することを求めている[422]。

- 科学分野の人材の採用
- 客員研究者の招聘
- 雇用や在籍関係を伴わない研究上の便宜供与[423]
- 代表団の受け入れ
- 寄付講座教授の任命
- 協力契約（秘密保持契約（NDA）、基本合意書（MoU）、意向表明書（LoI）等）の作成
- 共同教育プログラムの設立
- 機関間協定の作成

---

419 Knowledge security. https://vu.nl/en/about-vu/more-about/knowledge-security
420 Government of the Netherlands, “National knowledge security guidelines: Secure international collaboration,” January 2022. https://english.loketkennisveiligheid.nl/site/binaries/site-content/collections/documents/2022/04/07/national-knowledge-security-
421 Knowledge Security Responsibilities. https://vu.nl/en/research/portal/research-impact-support-portal/knowledge-security-responsibilities?
422 Pre-employment screening. https://vu.nl/en/employee/start-employment-contract/pre-employment-screening
423 雇用や正式な在籍関係を伴わずに、外部者（ゲスト）に対して大学の研究環境や研究資源への限定的アクセスを認める行為を指す。

- 共同施設の設立または外国投資誘致の計画
- 研究コンソーシアムにおけるプロジェクトコーディネーターや事務局の役割を担うこと
- 外国機関の研究者との共同研究や学術論文執筆

(ii) 職員採用前審査方針

VU Amsterdam では、新規職員採用者に対する採用前審査に関する大学全体としての方針の必要性が認識され、2021 年 8 月 1 日より、同大学全体で、採用前審査方針（Pre-employment screening）が採用・実施されている（2023 年 1 月に改正）[424]。

同大学においては、新規採用者に対する採用前審査に関する大学全体の中央方針の必要性が認識された。この方針の目的は、学外からの応募者の審査をどのように扱うべきか、また大学職務プロファイルに対して、どの採用前審査方法（学位証明書確認、参考身元照会（Reference Check）[425]及び犯罪経歴証明書（Certificate of Conduct：CoC））を実施すべきかを管理することにある。

この目的のために、大学職務プロファイル・リスクマトリクス（外部からはアクセス不可）が用意されている。大学職務プロファイル・リスクマトリクスを通じて、大学職務プロファイルに適用すべき採用前審査の方法が決定されるとしている。

この審査のポイントは、以下のとおりである[426]。

- 採用リスクの対象領域は、情報、金銭、物品、サービス、取引、プロセス、組織管理、人物管理等を網羅する。
- 上記リスクに起因する財務に与える影響度（低、高）と職員が機密情報を扱う権限のレベル（低、高）の組み合わせによって、採用前審査で求められる確認・検証事項が決定される（表 2-23 参照）。

表 2-23　大学職員の採用前審査で求められる確認・検証事項

（出典：VU Amsterdam のホームページ情報[427]に基づき、未来工学研究所が和訳・編集）

影響度	影響度と権限のレベル	採用前審査で求められる確認・検証事項
低	影響度低＋権限低	関連学位証明書確認
	影響度低＋権限高	関連学位証明書確認＋ 参考身元照会
高	影響度高＋権限低	関連学位証明書確認＋参考身元照会
	影響度高＋権限高	関連学位証明書確認＋参考身元照会＋犯罪経歴証明書

[424] Pre-employment screening. https://vu.nl/en/employee/start-employment-contract/pre-employment-screening
[425] 応募者が応募している職務に関連する情報を得るため、1 人以上の推薦者と連絡を取ることを指す。この照会は、推薦者が、応募者の知識・経験に関する主張や、応募者の能力について記述している内容を確認するか否かを検証することを目的とする。
[426] Pre-employment screening. https://vu.nl/en/employee/start-employment-contract/pre-employment-screening
[427] Ibid.

参考身元照会や学位証明書の確認の結果が肯定的でないことが判明した場合は、応募者に速やかに通知される。事前審査の結果が肯定的でないことが判明した場合、管理者は直ちに人事アドバイザーに連絡する。

採用前スクリーニングでは、職員（または応募者）が「本人が主張する人物であること」および「申告された能力を有すること」を検証するため、複数の手段が用いられる。これにより、大学が誠実さを欠く人物や関連する犯罪歴を持つ人物を採用するリスクを低減することができるとされている。

(iii) 知識セキュリティ・フローチャート

VU Amsterdam では、共同研究を行う予定の外部機関もしくは個人が認められるか、否かを判断するためのフローチャート（Flow Chart Knowledge Security）[428]を作成・公開している。

表 2-24 に、このフローチャートにおける質問の流れを示す。

以下の 2 つのカテゴリーを構成する複数の質問に対して Yes/No を選択することで、共同研究の可否を判断する構成になっている。

- 法的枠組み
- リスク管理

表 2-24　Flow Chart Knowledge Security における質問の流れ

（出典：VU Amsterdam のホームページ情報[429]に基づき、未来工学研究所が和訳・編集）

すべての質問に「いいえ」と回答した場合、その連携には障壁がありません。それでもなお、国際連携相手のリスク評価には「Partnering Tools」[430]を確認することが望ましいです。

【法的枠組み)】

1a. 連携を希望する企業または機関は、EU もしくは国連の制裁リストに掲載されていますか？

Yes：当該組織との連携は禁止されます。
No：次の質問 1b に進んでください。

1b. 連携を希望する個人（研究者など）は、EU もしくは国連の制裁リストに掲載されていますか？

Yes：当該個人との連携は禁止されます。
No：次の質問 2 に進んでください。

2. 当該研究は、EU のデュアルユース規制で定められた技術や知識を扱っていますか？（技術成熟度（Technology Readiness Level, TRL）が高い研究ほど、当該研究は「基礎的な科学研究」と見なされない可能性が高くなります）

428 Is collaboration with an organization or individual permitted and desirable? https://assets-us-01.kc-usercontent.com/d8b6f1f5-816c-005b-1dc1-e363dd7ce9a5/39efc2d5-52ca-460b-8b48-0fa7ca4b9f31/Flow%20Chart%20Knowledge%20Security%20VU.pdf
429 Ibid.
430 外部からはアクセス不可。

No：次の質問 3 に進んでください。
Yes：その研究は基礎的な科学研究に該当しますか？
　Yes：次の質問 3 に進んでください。
　No：研究で使用する製品・ソフトウェア・技術（およびそれに関する知識）は、誰もが利用可能なもののみですか？（研究成果を最終的に公開する予定であっても、その過程で使用する製品・ソフトウェア・技術（またはそれらに関する知識）が既に一般に公開・入手可能であるとは限りません）
　　Yes：次の質問 3 に進んでください。
　　No：輸出許可が必要となる可能性があります。学内の渉外・法務担当部署にお問い合わせください。

【リスク管理】

3. 連携相手の組織（または当人の過去の所属組織）は、EU 圏外の軍事組織と関係がありますか（または過去に所属していたことがありますか）？

Yes：所属学部の知識セキュリティ担当者に相談し、リスク評価のための包括的な質問票に記入してください。
No：次の質問 4 に進んでください。

4. 今回の連携は、機微な研究（安全保障上機微な研究領域）に該当しますか？

Yes：所属学部の知識セキュリティ担当者に相談し、包括的な質問票に記入してください。
No：次の質問 5 に進んでください。

5. 研究内容に倫理的に問題となり得る行為や論点が含まれており、なおかつ連携相手（組織または個人）の所属国が学術的自由度指数でスコア 0.4 以下となっていますか？

Yes：所属学部の知識セキュリティ担当者に相談し、包括的な質問票に記入してください。
No：次の質問 6 に進んでください。

6. 受け入れる研究者または共同研究が、相手方からの一方的な外部資金によって支援されていますか？

Yes：パートナー側が当該研究または人材に資金提供する理由・背景を確認してください。連携相手の所属国の学術的自由度指数（スコアが 0.4 以下の場合、以下の制限事項が適用されます。

- 2 年未満の短期受入（母国から指導を受ける）による奨学金留学生は受け入れ不可。
- デュアルユース技術分野および機微な研究領域の研究者は受け入れ不可。
- 質問 3 で言及された「極めてリスクの高い国」に所属する研究者は受け入れ不可。

上記のいずれかに該当する場合は、所属学部の知識セキュリティ担当者に連絡してください。なお、一方的な外部資金による奨学金留学生であっても、VU Amsterdam が提案した研究テーマに対して VU Amsterdam が選抜した人材である場合（博士課程の場合は学位取得先が VU Amsterdam となること）、受け入れが認められます。

No：特段の制限事項はありません。

結論：上記の質問すべてに「No」と回答した場合、その連携には何ら問題はありません。

(d) 組織体制・ガバナンス

VU Amsterdam は Knowledge Security Advisory Group を置き、各部局に知識セキュリティ担当者（contact persons）を配置している。知識セキュリティに関する質問は、職員が、関連学部またはサービスの知識セキュリティ担当者に連絡することができる。
知識セキュリティ担当者は 知識セキュリティ諮問グループにより訓練を受け、必要に応じて同グループに相談できる体制であるとされる[431]。

2.6.3 資金配分機関等における取組

(1) オランダ科学研究機構（NWO）

NWO は、2022 年 1 月下旬にオランダ政府が公表した「National Knowledge Security Guidelines」の策定に関与した。

2023 年 4 月、資金配分機関である同研究機構は、前述したように、「知識セキュリティ」をさらに強化するため、資金調達プロセスにおける新たな方針を導入した。研究機関が申請書を提出する際は、申請者は、「National Knowledge Security Guidelines」を遵守することが必須となった。申請者は助成金の申請時に、当該大学・研究機関が同ガイドラインの要求事項に従って運営されていること、及び申請書が本ガイドラインに準拠していることを確認することが要求されることになった[432]。

なお、2024 年 8 月 30 日発行のオランダ王国官報[433]によると、2024 年 2 月 21 日の通達「NWO Grant Scheme, Netherlands Organisation for Scientific Research」（原文はオランダ語）で、「NWO の助成金を受領する（サブ）プロジェクトリーダー及び受益者は、当該プロジェクトやそれによって生み出されたプロジェクト成果が、テロ活動、人権侵害、知識セキュリティにリスクに晒すこと、また、その他の違法活動に寄与しない（または寄与し得ない）ことを確保するために必要な措置を講じなければならない。」と記している。

同研究機構は、「National Knowledge Security Guidelines」の公表を受け、知識セキュリティに関する評価手順および同研究機構傘下の研究所における対策実施に取り組んでいるとされる。また、同研究機構全体（資金調達プロセスに関わる全職員および同研究機構の 9 つの研究所勤務者全員）を対象に、知識セキュリティ意識向上の取り組みを推進しているとされる[434]。

同研究機構は内部に、知識セキュリティに関する 2 つのアドバイザリーチームを設置している。1 つは資金調達プロセス担当職員向け、もう 1 つは研究所向けであり、両チームは政策実施と知識構築を支援し、内部職員の知識セキュリティ関連質問の窓口となり、知識セキュリティに関する懸案事項や事例に対処するとされる。これにより、同研究機構は高リスク国、機微な知識分野および潜在的高リスクのある関係者についての認識の向上、また、知

431 Knowledge security. https://vu.nl/en/about-vu/more-about/knowledge-security
432 Knowledge security. https://www.nwo.nl/en/knowledge-security
433 Staatscourant van het Koninkrijk der Nederlanden. https://zoek.officielebekendmakingen.nl/stcrt-2024-28067.html
434 Knowledge security. https://www.nwo.nl/en/knowledge-security

識セキュリティに関する兆候を感じた際の対応策の周知に努めているとされる[435]。

同研究機構は、助成金申請者が所属研究機関の知識セキュリティ方針を遵守することを求めており、提案書または採択プロジェクトに知識セキュリティに関するリスクが存在する可能性が示された場合、申請者またはプロジェクトリーダーに対し、リスク軽減策に関する説明を求めることがあるとしている。同研究機構は、さらに知識セキュリティ保護のため交付決定通知書に追加条件を付すことを決定し得るとしている[436]。

2.6.4 まとめ

(1) 大学の知識セキュリティの取組に関する特徴

調査した 2 つの大学における知識セキュリティの取組の特徴として、以下を挙げることができる。

アムステルダム大学（UvA）は、知識セキュリティを独立した安全保障問題とするのではなく、軍事・テロ目的での知識悪用を含め、武力紛争、人権侵害、環境問題、生物多様性、文化遺産等への損害等と並列する倫理評価項目の一つとして位置づけている。また、同大学と連携する国家・機関のスタンス（民主主義的、権威主義的等）に係わらず、個別案件ごとの評価を原則としており、価値基盤を明確にしつつ比例原則を重視する姿勢が見られる。

一方、アムステルダム自由大学（VU Amsterdam）は、知識セキュリティは静的な概念ではなく、協力関係のある国の地政学的な態度の変化により、協力関係にあるパートナーシップの見方に影響を与え得るとしている。また、リスクマトリクスを用いた職員採用前審査の仕組みを開発する等、非常に先進的な取り組みが行われており、人材採用と研究協力を同一フレームで扱っている。これは「研究セキュリティ」と「人的リスク管理」を統合的に扱うアプローチと言うことができる。

なお、両大学とも、複数の質問を設定し、回答者が各質問について Yes/No で回答することで、共同研究や連携する機関の可否を評価する流れを示した、わかり易いフローチャートを作成していることも大きな特徴と言うことができる。

(2) 資金配分機関の知識セキュリティの取組に関する特徴

資金配分機関としてのオランダ科学研究機構（NWO）における知識セキュリティの取組の特徴として、以下を挙げることができる。

- 大学・研究機関が、助成金の申請時に、国のガイドラインである「National Knowledge Security Guidelines」を遵守することの確認を義務化していること。
- 提案書または採択プロジェクトに知識セキュリティに関するリスクが存在する可能性が示された場合、リスク軽減策に関する説明を求める場合があること。
- 知識セキュリティに関する 2 つのアドバイザリーチーム（資金調達プロセス担当職員

[435] Ibid.
[436] Ibid.

向け、傘下の研究所向け）を設置し、内部職員の知識セキュリティ関連質問の窓口となっていること。

これは、知識セキュリティを「大学の自主的努力」に委ねるのではなく、資金配分プロセスに組み込むという強い意思を表すものと言うことができる。

(3) 日本の大学にとって参考になると思われる点

オランダの大学の事例から、日本の大学にとって参考となる点は以下のとおりである。

(a) 研究セキュリティに倫理審査と人権配慮を含めること

イスラエルのガザ攻撃や中国のウイグル問題など、国際的にも倫理的・人権的な重大な問題が生じていることから、オランダの大学は、大学としての国際的な名声と価値を維持するうえでも、外部連携の評価を行う場合には、こういった倫理的・人権的な問題を重要視している。今後、日本の大学が一層国際化していく流れの中で、研究セキュリティを、経済安全保障や国家安全保障の観点だけではなく、倫理的・人権的な問題を含めて対処していく考え方は、日本の大学としても参考になると考えられる。

(b) 職員採用前審査の仕組み

特に国外から大学の職員（事務系職員、研究系職員）を新規に採用する場合、候補者の身元、学位、犯罪歴等を正確に確認することは必ずしも容易ではない。このため、アムステルダム自由大学による、「大学の部署で扱う領域（情報、金銭、物品、サービス、取引、プロセス、組織管理、人物管理等）のリスクに起因する財務に与える影響度（低、高）」と「職員が機密情報を扱う権限のレベル（低、高）」との組み合わせ（表 2-23））で、採用前審査で求める確認・検証事項を決定する考え方は、研究セキュリティにおけるリスク管理の観点から極めて理に適っており、日本の大学としても非常に参考になると考えられる。

(4) 日本の資金配分機関にとって参考になると思われる点

オランダの資金配分機関の最大の特徴は、助成金を申請する大学・研究機関が国のガイドラインの要求事項に従って運営されていること、及び申請書が本ガイドラインに準拠していることを確認することが条件になっていることである。日本でも、資金配分機関の助成金の申請段階で同様の条件を課すことについて検討を進めていく必要がある。

2.7　ドイツ

2025 年 5 月連邦教育研究省（Bundesministerium für Bildung und Forschung、以下 BMBF）は、メルツ政権の行政組織改革により研究開発及び高等教育を中心的に担う連邦研究技術宇宙省（Bundesministerium für Forschung, Technologie und Raumfahrt、以下 BMFTR）に改組された[437]。研究セキュリティ・研究インテグリティの主管省は BMBF/BMFTR であるが、連邦経済輸出管理局(Federal Office for Economic Affairs and Export Control/Bundesamt für Wirtschaft und Ausfuhrkontrolle, 以下 BAFA)がデュアルユース、諜報機関の連邦憲法擁護庁(Bundesamt für Verfassungsschutz、BfV）はスパイ行為や機密情報漏洩等について助言や監督を行っている。

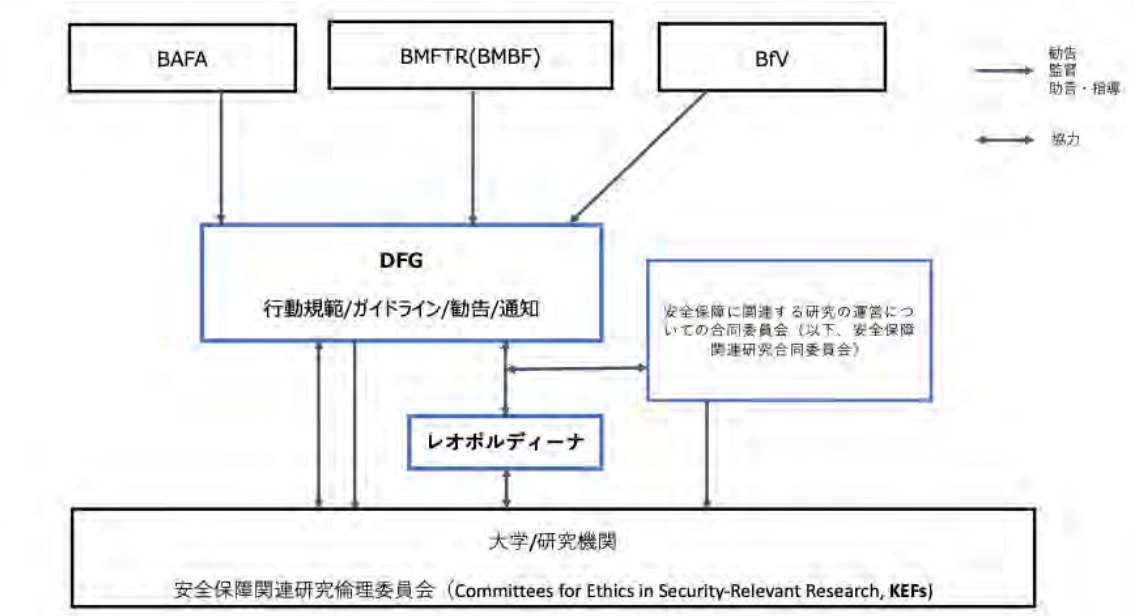


表 2-25 ドイツの研究セキュリティ関連機関と相互関係

ドイツの研究セキュリティ・研究インテグリティ（以下、研究セキュリティ・インテグリティ）では、非政府・非営利の研究資金配分機関であるドイツ研究振興協会（Deutsche Forschungsgemeinschaft、以下 DFG）が国立科学アカデミー・レオポルディーナ（Nationale Akademie der Wissenschaften: Leopoldina、以下レオポルディーナ）[438]との協力の下、ガイドラインの作成、大学・研究機関におけるルールづくりや関連委員会設置への助言・指導、規程やガイドライン作成の勧告と実施状況の監督などドイツにおける研究セキュリティ・インテグリティの中心的な役割を担ってきた。DFG とレオポルディーナは言わば学術界を

[437] 初・中等教育については、BMBFSFJ（Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend、連邦教育・家族・高齢者・女性・青年省）に移管された（参考：https://crds.jst.go.jp/dw/20250604/2025060442050/）。

[438] レオポルディーナは、1652 年に設立された世界最古にして国内最高峰の学術団体であり、科学及び科学政策について政財界に助言するなど影響力も大きい。この他に、ドイツ学術交流会（Der Deutsche Akademische Austauschdienst、略称：DAAD）ドイツ学長会議（Hochschulrektorenkonferenz、略称： HRK） などがある。

代表する立場であり、そのため一方的に勧告や指導・助言を行うのではなく、大学・研究機関との意思疎通が図られている。ドイツの研究セキュリティ・インテグリティのステークホルダーとその関係を図 2-26 に示した。

2014 年 6 月に DFG とレオポルディーナは共同で「Scientific Freedom and Scientific Responsibility: Recommendations for security-relevant research（学問の自由と科学的責任：安全保障に関連する研究への対応に関する勧告）」[439]を出し、これに基づいて 2015 年「Joint Committee on the Handling of Security-Relevant Research/Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung（安全保障に関連する研究の運営についての合同委員会、以下安全保障関連研究合同委員会）」を設立した[440]。当合同委員会は著名な科学者など学術界の有識者をメンバーに組織される。各大学・研究機関の自主規制の意識を高めるために、デュアルユースや安全保障関連研究について責任を持って取扱うよう個別に安全保障関連研究倫理委員会（KEFs）の設置と規約の策定、その学内もしくは機関内での承認、そして研究の適正な実践を保護するための行動規範（ガイドライン）の制定が推奨された。

DFG は、安全保障関連研究倫理委員会の監督組織として、その設置や規約策定の助言・指導を行う一方、行動規範（ガイドライン）について 2019 年に大学・研究機関の手本となる模範文書を発行した。各大学・研究機関は規則、規程、ガイドラインなど名称は異なるものの、行動規範の策定を進めている。DFG の勧告事項は、義務ではなく、民間団体の推奨にすぎない。とはいえ、大学・研究機関に対するその影響力は決して小さくない。例えば安全保障関連研究倫理委員会（KEF(s)）については、約 120 の大学・研究機関が設置済みである[441]。

ドイツでは、「研究セキュリティ」よりも「安全保障に関連する研究（security-relevant research、以下安全保障関連研究）」という用語が一般的である。安全保障関連研究は、先の合同委員会によると「第三者によって直接悪用され、人間の尊厳、生命、健康、自由、財産、環境、平和的共存に重大な害を及ぼす可能性のある知識、製品、または技術に関連する科学的研究」と定義されており[442]、 研究セキュリティの中でも「デュアルユース」に焦点を当てたものである。同委員会は専用のホームページを開設し、安全保障関連研究に係る最新の知見や情報を発信している[443]。

ところが、ウクライナ戦争の終結が見通せないなかで、こうしたデュアルユースに焦点を当てたあり方に変化が生じ始めた。2024 年 3 月、BMBF は「Position Paper on research security in light of the Zeitenwende（歴史的転換点の研究セキュリティに関する声明書、

439 Scientific Freedom and Scientific Responsibility: Recommendations for security-relevant research, https://www.security-relevant-research.org/publication-scientificfreedom2022/
440 Joint Committee on the Handling of Security-Relevant Research, https://www.dfg.de/en/basics-topics/basics-and-principles-of-funding/security-relevant-research/joint-committee
441 Joint Committee on the Handling of Security-Relevant Research, Should Research be used to, https://www.security-relevant-research.org
442 Frequently asked questions about security-relevant research and the KEFs, https://www.security-relevant-research.org/faq-eng/
443 Security-relevant research org, Should Research be used to, https://www.security-relevant-research.org

以下ポジション・ペーパー)」を発出し、G7 諸国で共有される研究セキュリティ[444]、すなわち外国政府やその代理人による諜報活動やスパイ行為によって生じるリスクを含む問題とする明確な認識が示され、これを契機にドイツの取組は新たな段階に入ったということができる。

2024 年は、スパイ事件も相次いで発覚した。4 月 22 日、中国の情報機関と連携し軍事転用が可能な技術情報を中国に提供した疑いで、ドイツ人 3 人が逮捕された[445]。ドイツの大学と協力協定を締結して中国国家安全省に情報提供する準備を進めていたとされる本事件については、事件の舞台になった大学の取組の記述において改めて述べる。翌 23 日には、極右政党の議員スタッフが中国への情報提供容疑で逮捕され[446]、さらに 10 月 2 日航空や貨物、乗客に関するデータのほか、軍事装備の輸送やドイツの武器会社とつながりのある人物に関する詳細を中国情報機関員に流した容疑で中国人の女が逮捕された[447]。

2.7.1　研究セキュリティ・インテグリティ関連政策動向

(1)　2024 年度までの経緯[448]

表 2-26　2024 年までのドイツの研究セキュリティ・インテグリティ関連の政府と関連機関の動向（１）

発行年	文書・取組の表題	発行・行為組織
2017年	(a) China: Daten & Analysen zum Hochschul- und Wissenschaftsstandort（中国：大学および科学拠点に関するデータと分析）	ドイツ学術交流会 (DAAD)
2019年9月/2024年9月改定	(b) Guidelines for Safeguarding Good Research Practice: Code of Conduct （行動規範：研究の適正な実践を保護するためのガイドライン）	DFG/レオポルディーナ
2020年4月6日	(c) Guidelines and Standards in International University Cooperation（大学の国際協力に関するガイドラインと基準）	大学学長会議（HRK）
2020年9月9日	(d) Guiding Questions on University Cooperation with the People's Republic of China（中国との大学間協力における疑問への指針）	大学学長会議（HRK）
2020年12月	(e) Compass, No Redline: Academic Cooperation within Complex Legal and Regulatory Environments（レッドラインはない：複雑な枠組み条件の下での学術協力羅針盤）	DAAD KIWi
2022年11月1日	(f) Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research （科学における自由と責任：安全保障に関連する研究の取扱についての勧告）	DFG/レオポルディーナ

444 内閣府「研究セキュリティと研究インテグリティに関する G7 共通の価値観と原則（日本語仮訳）、https://www8.cao.go.jp/cstp/kokusaiteki/integrity/g7_sigre_values_jpn.pdf
445 Reuters、「ドイツ、中国に軍事転用技術提供の疑いで 3 人逮捕　海軍強化の恐れ」（2024 年 4 月 23 日）、https://jp.reuters.com/world/security/GRHEUSNN4FOCPDTZXEN5U3PLAY-2024-04-22/
446 Reuters,「スパイ容疑で極右政党議員スタッフ逮捕　独検察　中国に情報提供」（2024 年 4 月 23 日）、https://jp.reuters.com/world/security/VVEQF3LZ4JM3ZH7PA2W6H4YJIY-2024-04-23/
447 Reuters、「独検察、中国スパイ容疑で女を逮捕　情報機関員に情報提供の疑い」（ 2024 年 10 月 2 日）、https://jp.reuters.com/world/security/3UG2TRINERKQXDUPIXUDCDOL5U-2024-10-02/
448 一部、令和 5 年度科学技術基礎調査等委託事業「研究インテグリティ（Research Integrity）に係る調査・分析報告書」を参考にした。

既述のように、ドイツでは学術界の自発性が尊重され、非政府・非営利の学術団体や研究機関、そして学術界メンバーが研究セキュリティ・インテグリティに積極的に関与し、本課題に関する勧告、ガイドラインやリポートなどの文書を発刊してきた。2024 年度までの動向をこれらのうち本調査において重要と考えられる文書及び報道を表 2-26 と 2-27 に示した。表に沿って概観する。

(a) China: Daten & Analysen zum Hochschul- und Wissenschaftsstandort（中国：大学および科学拠点に関するデータと分析）[449]

ドイツ学術交流会（Deutscher Akademischer Austauschdienst e.V.、以下、DAAD）が 2017 年に発行した文書で、ドイツの大学・研究機関及びその関係者を対象に中国との学術交流を行うにあたっての情報提供と注意喚起を目的に、中国の大学教育制度や研究のあり方（財政、政府の関与、国際交流など）、中国の大学・研究機関のドイツへの関心と学術交流の実態など基本情報から中国との交流や協力を行う際の注意事項まで詳細な説明を記載した文書である。

(b) Guidelines for Safeguarding Good Research Practice: Code of Conduct（研究の適正な実践を保護するためのガイドライン：行動規範）[450]

DFG/レオポルディーナが 2020 年発刊した本文書である。デジタル化の普及に伴う研究環境、研究機関の構造や協力形態の変化、また出版形態の新しいあり方に対応するため、2018 年に告発者の保護と無罪推定原則の促進を目的に「科学的不正行為への対応に関する手続規則」が改定された。その翌年の 2019 年 9 月に発行された本文書は、研究の誠実性を保証する枠組を提供すると同時に、改定規則の速やかな実施のための政策とガイドラインを確立することを目的に、6 項目の一般原則と研究プロセス全体における良質な実践のための 11 のガイドラインから構成される。本規範は研究倫理とインテグリティのための文書であるが、ドイツの文脈では安全保障関連研究と呼ばれるデュアルユースの課題を一部含んでいる。2024 年 9 月に改定された。

(c) Guidelines and Standards in International University Cooperation（大学の国際協力に関するガイドラインと基準）[451]

2020 年 4 月 6 日に大学学長会議（Hochschulrektorenkonferenz、以下、HRK）が発行した本文書は、ドイツの大学の国際パートナーシップのために、「戦略とガバナンス」、「共同教育と学習」、「共同研究」、「国境を越えた場としての大学」の 4 側面からなる包括的なガイドラインとその基準を定めている。

---

[449] China: Daten & Analysen zum Hochschul- und Wissenschaftsstandort, https://www2.daad.de/medien/der-daad/analysen-studien/bildungssystemanalyse/china_daad_bsa.pdf
[450] Guidelines for Safeguarding Good Research Practice. Code of Conduct, https://zenodo.org/records/14281892
[451] HRK, Guidelines and standards in international university cooperation, https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guidelines-and-standards-in-international-university-cooperation/

(d) Guiding Questions on University Cooperation with the People’s Republic of China（中国との大学間協力における疑問への指針）[452]

同じく HRK が発刊した本指針（2020 年 9 月 9 日）は、中国との学術協力における重要事項への認識を高め、中国大学・学術機関との強靭なパートナーシップ構築・発展に向けた支援を提供し、有益な発展経路を特定して、ドイツ側参加者に機会とリスクを認識させることを目的に書かれた。

(e) Compass, No Redline: Academic Cooperation within Complex Legal and Regulatory Environments（レッドラインはない：複雑な枠組み条件の下での学術協力羅針盤）[453]

本文書は、ドイツ学術交流会（Der Deutsche Akademische Austauschdienst: DAAD）によって 2020 年 12 月に発刊されたが、KIWi（学術交流センター）[454]によって作成された。国際化に関与する利害関係者に、複雑な条件の下で国際的パートナーとの学術協力を遂行するための体系的なアプローチを提供することを目指し、協力の機会とリスクを評価するために使用できる安全状況、広範な政治的責務、立憲的かつ政治文化的枠組、各学術システムの機会とリスク、パートナー機関の学術的な質、戦略の制度化への統合からなる 6 つの基準を示した。

(f) Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research（科学における自由と責任：安全保障に関連する研究の取扱についての勧告）[455]

本文書は、2022 年 11 月 1 日に DFG/レオポルディーナによって発行された。デュアルユースの問題に対して大学・研究機関及び研究者が対処すべきアプローチについての推奨策を提示している。ドイツにおいて、研究の自由は憲法に明記されているが、自由な研究にはリスクも伴い、しかも有用な研究成果ほど悪用される危険性も高く（「デュアルユースのジレンマ」）、境界の曖昧なリスクは法律で完全に規制することは難しい。そのため、個々の研究者に法的義務を超えた特別な倫理的責任を課すほかなく、本文書は学術界の自主規制の手段となる勧告である。

勧告は個々の研究者を対象にしたセクション(1～8)と大学・研究機関のためのセクション（9～11）から構成される。前者にはリスク分析、リスク軽減策、研究成果の公表評価、最終手段としての研究中止といった考慮事項が示され、一方、後者では安全保障関連研究の取扱に関する倫理規則の策定と安全保障関連研究倫理委員会（KEFs）の設置が推奨された。

---

[452] Guiding Questions on University Cooperation with the People’s Republic of China, https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guiding-questions-on-university-cooperation-with-the-peoples-republic-of-china/

[453] https://www.daad.de/kiwi-kompass/no-red-lines/

[454] KIWi は国際的な学術協力を支援し、DAAD のグローバルネットワークからの最新の情報発信するための DAAD のアドバイスセンターの一つである。

[455] DFG, Dealing with risks in security-relevant research, https://www.dfg.de/en/basics-topics/basics-and-principles-of-funding/security-relevant-research

リスク分析、リスクの最小化、出版（公表）の判断、最終手段としての研究の断念、リスクの文書化と伝達、訓練と情報、責任者、法的規定とコンプライアンス部門の各事項について説明されている。

表 2-27　2024 年までのドイツの研究セキュリティ・インテグリティ関連の政府と関連機関の動向（２）

発行年	文書・取組の表題	発行・行為組織
2023年6月22日	(g) Espionage in Science and Research （科学と研究における諜報活動）	連邦憲法擁護庁 (BfV)
2023年9月	(h) Dealing with Risks in International Research Cooperation: Recommendations （国際研究協力上のリスクへの対処に関する勧告）	DFG/レオポルディーナ
2024年1月	(i) Academic Cooperation with China: A Realistic Approach, Recommendations to German Higher Education institutions（中国との学術交流に対する現実的アプローチー国内大学への勧告）	DAAD
2024年3月	(j) Position Paper on Research Security in Light of the Zeitenwende （歴史的転換点の研究セキュリティに関する声明書/ポジションペーパー）	BMBF
2024年10月11日	(k) 研究セキュリティセンター創設に向けたキックオフ会議	BMBF
2024年11月	(l) Scientific Freedom and Security Interests in Times of Geopolitical Polarization: Report（地政学的二極化の時代における科学研究の自由とセキュリティへの関心）	DFG/レオポルディーナ

(g)　Espionage in Science and Research（科学と研究における諜報活動）[456]

2023 年 6 月 22 日の連邦憲法擁護庁（BfV）が発出した本文書によると、外国政府による科学スパイ活動の主目的は、知識面で一歩先を行くため、あるいは既存の知識の空白を埋めるために情報を入手することで、スパイ行為者は膨大な人的・財政的資源を有し、体系的かつ巧妙に、長期的に活動する。セキュリティ面やスパイ活動によるリスクに十分な注意を払わない傾向にある学術界は標的になり易いと警告し、特に危険に晒される研究分野、科学スパイ活動の手口とその防止策について、図式を用いて平易に説明した科学分野の研究者向けの諜報・スパイ活動に備えるための解説書である。

本文書が発出された同じ時期、科学・産業研究スパイ事件が発覚した。2023 年 6 月初め、フリードリッヒ・アレクサンダー大学エアランゲン・ニュルンベルク（Friedrich-Alexander Universität Erlangen-Nürnberg, FAU）は、 中国教育部の対外支援部門の中国国家留学基金管理委員会（CSC）から資金援助を受けていた同大の中国人研究者の活動を停止すると発表した。 CSC 奨学金受給者となる中国市民には「中国共産党への支持を誓約し、正しい世界観、人生観、価値観体系を持つこと」が要求される。FAU の公式発表では、ドイツで実践されている学問の自由および教職員の表現の自由の原則に違反するというのが活動停止の理由であった。しかし、大学の内部メールを入手したメディアは、 大学当局者は中国政

[456] Espionage in Science and Research, https://www.verfassungsschutz.de/SharedDocs/publikationen/EN/economic-and-scientific-protection/2023-06-23-espionage-science-research.pdf?__blob=publicationFile&v=2

府が当該研究者を介して FAU の科学・産業研究をスパイし、同大学のデータセキュリティや知的財産管理を侵害する可能性を懸念していたと指摘している[457]。

BfV は、その庁内報において「ドイツの大学には、スパイ活動によって集積してきた研究成果を失う高いリスクを認識し、そのための適切な保護措置を正しく評価する感度が欠如している」と指摘した[458]。本庁内報の発行月は不明であるが、本文書よりも早い時期だと考えられる。

FAU のスパイ事件では、大学当局の発表を受けて、BMBF の Bettina Stark-Watzinger（ベッティーナ・シュタルク＝ヴァッツィンガー）大臣は FAU の決定を支持し、「ドイツの大学や研究機関にはスパイ活動から自らを守る責任がある」と述べた。ドイツの他の大学も、FAU に倣って CSC 資金からの中国人研究者受入れ中断の検討を開始した。[459]

表 2-28 ドイツにおける研究セキュリティ関連インシデントと文書発行等のタイムライン

	2019年	2021年	2022年	2023年	2024年
事件	①宇宙技術ロシア人スパイ事件2019年～21年	6月16日現行犯逮捕			
			②デュアル・ユース事件 2022年7月～23年3月、ドイツ人3人が**ケムニッツ工科大学**に平軸受の研究を依頼、デュースブルク・エッセン大学とシュトゥットガルト大学も研究協力について協議し、前者の教授が会議の開催支援を受ける		4月22日軍事転用可能な技術情報を中国に提供した疑いで逮捕
				③科学・産業研究スパイ事件 2023年6月フリードリッヒ・アレクサンダー大学（FAU）が中国政府の資金援助を受けている研究者の活動を停止すると発表した	
関係機関の文書発行などの動き				☆ 連邦憲法擁護庁(Bundesamt für Verfassungsschutz, **BfV**）庁内報「ドイツの大学は、スパイ活動の危険性と専門知識を失う高いリスクを認識し、そのための適切な保護措置を正しく評価する感度を欠く」と指摘 ☆担当大臣は「ドイツの大学や研究機関にはスパイ活動から自らを守る責任がある」と指摘 ☆6月 **BfV** ファクトシート「科学と研究における諜報活動」発行 概略：科学研究におけるスパイ行為のリスクにどのようなものがあるのか、具体例を示して注意喚起し、その対応策を解説 ☆9月 **DFG/レオポルディーナ** 勧告「国際研究協力上のリスクへの対処」発行 概略：研究員採用や研究遂行上に起こり得るリスクとその対応方法を提示	☆ 6月 **マックス・プランク協会**「国際協力発展のための指針」発行 概略：研究の自由とリスクの認識・特定し、最小化を図るためのアプローチを提示 ☆ 7月 **ドイツ航空宇宙センター・プロジェクト管理機関**（DLR Projektträger）「科学におけるデューディリジェンス：評価プロセス、科学の保護、科学協力のためのマニュアル」刊行 ☆ 8月 **ケムニッツ工科大学**「安全保障関連研究および『デュアル・ユース』の側面に関するプロジェクトの取り扱いに関するガイドライン」を発行 ☆ 10月 **BMBF**「研究セキュリティセンター創設に向けたキックオフ会議」開催

以下の(h)と(i)で述べる DFG/レオポルディーナと DAAD がそれぞれ発行した文書も、この FAU における事件が影響していることが推測される。ドイツの研究セキュリティに関して文献調査で確認できたインシデントは 3 件であった。表 2-28 に事件と関連性が推測される政府と大学・研究機関の動きを時系列で表した。こうした事件が研究セキュリティ強化に及ぼした影響を明確な証拠を以て示すことはできないが、その後政府及び大学・研究機関が発行した文書や談話、会議の開催などから関連性を推測することはできる。

457 Joseph Fitsanakis “Leading German university suspends Chinese state-funded researchers,” IntelNews (August 1, 2023), https://intelnews.org/2023/08/31/01-3304/
458 Science/Business, Chinese scientific espionage in Germany: what next? (02 May 2024), https://sciencebusiness.net/universities/chinese-scientific-espionage-germany-what-next.
459 World University News, Yojana Sharma, German university ends ties with China scholarship scheme (20 July 2023), https://www.universityworldnews.com/post.php?story=20230720113914406

(h) Dealing with Risks in International Research Cooperation: Recommendations（国際研究協力上のリスクへの対処に関する勧告）[460]

2023 年 9 月に DFG/レオポルディーナが発行した本勧告の目的は、海外との研究協力に伴うリスク、特に海外からの人材採用や協力パートナーの選定におけるリスクを研究者が認識し、有意義な措置を講じることである。研究者および機関のデュー・ディリジェンスは、法的拘束力のある外国貿易規制を超えて拡大され、国際研究協力に関わるすべての個人および機関に安全性を提供すべきだとする。地政学的課題に柔軟に対応できる研究文化の模範を示すことを目指し、リスクと便益の評価、評価と検討における推奨ポイントが記されている。

(i) Academic Cooperation with China: A Realistic Approach, Recommendations to German Higher Education institutions（中国との学術交流に対する現実的アプローチ：国内大学への勧告）[461]

DAAD 発行の本文書（2024 年 1 月）は、ドイツ連邦政府が 2023 年 7 月に採択した中国戦略の新指針[462]が提示する戦略を起点として、中国との学術協力に関する現在の議論を整理し、中国との学術協力のあり方について具体的な提言を行うことを目的に、中国とのパートナーシップを設計する際に考慮すべき 3 つの指針を提起した。

(j) Position Paper on Research Security in Light of the Zeitenwende（歴史的転換点の研究セキュリティに関する声明書、以下ポジション・ペーパー）[463]

2024 年 3 月に BMBF が発出した本文書は、ロシアによるウクライナ侵攻を契機とした地政学的・戦略的状況の変化を受け、国際安全保障における「時代の転換点（Zeitenwende）」を認識したことが背景にある。技術、データ、デュアルユース分野における研究は、諜報活動、悪用、外国の影響力により大きなリスクに晒されているとし、学問の自由を保持しつつ、研究をより強固に保護する必要を述べた。論点は、安全保障と科学的自由の均衡、研究の機密性および潜在的な危害に見合ったリスクベースかつ比例原則（「可能な限り開放的に、必要な限り閉鎖的に」）に基づくアプローチ、新たな課題を踏まえて従来の民生研究と軍事研究の厳格な分離（「民生条項」）の見直しの必要性の 3 つであった。そして、リスクと脅威への対策について具体的な措置が示された。

---

460 https://www.dfg.de/resource/blob/289704/risiken-int-kooperationen-en.pdf
461 Academic Cooperation with China: A Realistic Approach, Recommendations to German Higher Education institutions, https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/der-daad/240307_daad_perspektive_china_en.pdf
462 The Federal Government,“Strategy on China of the Government of the Republic of the Federal Republic of Germany,” issued on 13 July 2013, https://www.auswaertiges-amt.de/resource/blob/2608580/49d50fecc479304c3da2e2079c55e106/china-strategie-en-data.pdf
463 BMBFTR, Position Paper on Research Security in Light of the Zeitenwende, https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf?__blob=publicationFile&v=4

(k) 研究セキュリティセンター創設に向けたキックオフ会議[464]

ポジション・ペーパーの内容を精査し、その実施の見通しについて、産官学のステークホルダーを交えた参加型の議論が進められることになり、そのキックオフ会議が 10 月 11 日にベルリンの BMBF で開催され、共同覚書の作成が目指された。議論には、ポジション・ペーパーで提案されている研究セキュリティを一元的に取扱う戦略的な組織となる研究セキュリティ・センターの創設も含まれた。

研究セキュリティ・センター構想について、DFG 会長 Katja Becker 氏は、Science/Business 誌のインタビューの中で、「ドイツの科学システムの全プレーヤーが利用できる独立の中央機関の必要性」を指摘し、センターについて「政治、国家安全保障組織、資金提供機関、大学・研究機関が対話によって合意が形成できるような各分野の専門知識を取り入れた効率的な機関であるべきだ」と述べた[465]。

(l) Scientific Freedom and Security Interests in Times of Geopolitical Polarisation: Report（地政学的二極化の時代における科学研究の自由とセキュリティへの関心）[466]

2024 年 11 月に DFG/レオポルディーナが発行したこの文書は、BMBF の「ポジション・ペーパー」を学術界の立場から捉え直し、学術的に補完することを目的に、主に安全保障関連研究合同委員会の活動実績を基にまとめられた報告書である。A から D までの 4 章から構成され、まず A 章は合同委員会の第 5 回報告書を紹介する。安全保障関連研究及び研究協力の取り扱いにおけるドイツの科学分野における自主規制の進展を述べた B 章に続いて、C 章では合同委員会委員及び事務局が公の場で提起してきた議論が取り上げられ、これらを踏まえた大学・研究機関の安全保障関連研究倫理委員会（KEFs）および合同委員会の任務と目標及び展望が D 章に提示された。

ポジション・ペーパーと同様、地政学的変化による時代の転換点（Zeitenwende）のために研究・イノベーションと国家安全保障（競争力、自律性）およびリスク（スパイ活動、悪用、デュアルユース）が切り離せないものになり、研究セキュリティの緊急性が高まっているとの認識に立つ。研究の自由は科学における根本の価値である一方、自由には責任を伴い、大学・研究機関と研究者にはこの新たなリスクと文脈を認識すべきとの見解を打ち出す。研究の国際協力が益々重要になっており、研究セキュリティのための措置が科学の自由、研究の完全性、オープンサイエンス、透明性の基盤だと強調する

ポジション・ペーパーが政府としての方針、すなわち研究セキュリティ政策のあり方を示したのに対し、本報告書は学術と研究の現場に即した論述が志向された。科学研究を取り巻

---

464 Peace Research Institute Frankfurt/Leibniz-Institut für Friedens- und Konfliktforschung (PRIF), Malte Göttsche involved in the BMBF's stakeholder process https://www.prif.org/en/about-us/news/details/forschungssicherheit-im-lichte-der-zeitenwende による。
465 Science/Business, Germany mulls new research security organization (29 Aug. 2024), https://sciencebusiness.net/news/germany-mulls-new-research-security-organisation
466 Scientific Freedom and Security Interests in Times of Geopolitical Political Polarisation: Report, https://www.sicherheitsrelevante-forschung.org/wp-content/uploads/2025/03/Progress-Report-Joint-Committee-2024.pdf

く現状分析に基づいて、各機関が安全保障関連研究倫理委員会（KEFs）の設置、ガイドラインやチェックリストの作成などの自発的取組を提案するとともに、比例原則（「可能な限り開放的に、必要な限り閉鎖的に」）の必要性を強調し、国際協力や学問の自由を損なう可能性のある過剰規制を戒めた。

(2) 最近の主な動き

(a) 政府（BMFTR）

i) National Platform for Research Security（「研究セキュリティ国家プラットフォーム」創設）[467]

2025年12月18日、BMFTRは研究と知識のセキュリティを体系的に強化して、知識や技術の望ましくない漏洩、違法な干渉、研究成果の不適切な使用等のリスクを予測し、管理することを目的にした「研究セキュリティ国家プラットフォーム（以下、プラットフォーム）」の創設を発表した。プラットフォームは、調整、情報提供、ガイダンスの3つの中核的な任務を持ち、調整運営委員会と支援サービスセンターから構成される。

本プラットフォームは国家安全保障会議に帰属し、運営は調整運営委員会が担う。委員会は、BMFTRを中心に外務省、内務省、国防省、経済エネルギー省などの連邦省庁、科学機関連合、各州の科学研究省、そして安全保障局のそれぞれの代表者から構成される。支援サービスセンターはBMFTRに設置され、主に大学・研究機関の担当あるいは組織に対して情報提供と指導業務を行う。

2026年1月より、入念な準備を始め、同年秋よりプラットフォームの運用とサービスセンター業務の一部を開始し、2027年1月から全面運用を目指す予定である。財源はBMFTR予算に計上され、また2028年秋には中間評価が計画されている。

ii) プラットフォーム創設に向けた関係者合意[468]

プラットフォームの創設が発表された翌日の2025年12月19日、BMFTR、科学組織連合、州科学省は、研究セキュリティの強化とプラットフォームの創設に向けた主要事項について合意した。ドイツ科学・人文科学評議会（German Science and Humanities Council, WR）のWolfgang Wick（ヴォルフガング・ヴィック）議長は、「このプラットフォームは政治と科学の空白を埋め、リスク評価において科学関係者に迅速かつ非官僚的な支援を提供し、国際共同研究における重要パートナーとの対応指針を示すものだ」と評価し、「科学界と政治界の対話」の必要性を強調した[469]。

---

[467] BMFTR, Key points for strengthening research security and establishing a National Platform for Research Security (18.12.2025), https://www.bmftr.bund.de/SharedDocs/Downloads/EN/2025/key-points-research-security.pdf?__blob=publicationFile&v=1

[468] WR News, National Platform for Research Security to be established (19. 12.2025), https://www.wissenschaftsrat.de/EN/Home/Buehne/_Inhalte/Inhalte_Online/2025_12_Research-Security

[469] WR News, National Platform for Research Security to be established (19. 12.2025), https://www.wissenschaftsrat.de/EN/Home/Buehne/_Inhalte/Inhalte_Online/2025_12_Research-Security

(b) 大学

i) 調査報告書「安全性を高めてイノベーションを促進：大学が安全関連の研究を評価する方法に関する大学バロメーター 2024/2025 の結果」[470]

2025 年 7 月に刊行された当報告書は、Stifterverband für die Deutsche Wissenschaft（ドイツ学術振興財団、以下 Stifterverband）という非営利団体[471]が、ドイツの大学経営陣に対して、ドイツにおける安全保障関連研究の取組をどのように評価するのかを質問した大学バロメーター調査の結果をまとめたものである。大学の経営陣の半数以上が、安全保障関連研究（研究セキュリティ）の重要性が高まっていると回答した。大学はこの問題にもっと貢献したいと考えているが、回答者の 3 分の 2 が大学の官僚主義や構造上の問題、インフラの不足などの問題点を挙げた。さらに、民生と軍事の研究が分断されている現状は、イノベーションの可能性を狭め、経済や社会にとっても安全保障への投資を民間で幅広く活用するのを妨げているとの指摘もあった。研究セキュリティにおいて大学が積極的な役割を果たすためには、明確な倫理的ガイドライン、近代的なインフラ、信頼性の高い支援メカニズムなどにより、大学が取組む上での構造的な能力強化が求められるとの見解が示された。

2.7.2 大学・研究機関における取組

ドイツの大学は総合大学（120 校）、応用科学大学（208 校）、芸術系大学（57 校）、その他（41 校）に分類され、設置主体別では国立 273 校、私立 115 校、宗教法人 38 校である（2023 年 12 月現在）[472]。大学を除く主要な研究機関のうち、代表的なものとしてマックス・プランク協会、ドイツ研究センターヘルムホルツ協会、ライプニッツ協会、フラウンホーファー研究機構などがある。

大学・研究機関には、既述のように安全保障関連研究倫理委員会（KEF(s)）の設置とともに、DFG/レオポルディーナが発出した「行動規範：研究の適正な実践を保護するためのガイドライン」（2019 年）に則って、それぞれ研究の適正な実践を保護するための行動規範またはガイドラインを作成することが推奨されている。そのため、DFG とレオポルディーナの指導と助言のもと、各大学の安全保障関連研究倫理委員会規約と行動規範/ガイドラインは、構成や文言に多少の違いはあっても、基本的な枠組みは共通する傾向にある。大学における行動規範は主に研究倫理や研究インテグリティに関する規程であり、研究セキュリティに当たる安全保障関連研究（デュアルユース）はその一部として盛り込まれており、研究セキュリティに焦点を当てた独立の文書については、少なくとも公開はされているものは見当たらない[473]。そこで、大学に関しては、本調査研究の目的に沿って「安全保障関連研究

[470] Mit Sicherheit zu mehr Innovationen: Hochschulen sehensichalszentrale Akteure bei sicherheitsrelevanterForschung,2024/2025,https://www.stifterverband.org/medien/mit_sicherheit_zu_mehr_innovationen
[471] Stifterverband は、社会の長期的なイノベーション能力の強化のための、教育と科学を再構築することを目的に、ドイツのビジネス、科学、市民社会の分野から集まった約 3,500 の個人、企業、団体等より構成されている（ABOUT THE STIFTERVERBAND, https://www.stifterverband.org/english）
[472] 文部科学省「国・地域別留学ガイド」、https://tobitate-mext.jasso.go.jp/countryguide/germany/
[473] イントラネットによって内部者のみアクセス可能な関連文書はあるとみられる。

（security-relevant research）」に関する箇所に絞って述べる。

研究機関も大学と同じように、DFG/レオポルディーナの勧告に応じて、行動規範の策定と KEFs の設置を進めているが、より先進的な取組を行なっている機関もみられ、ここではそうした独自の取組を進める研究機関を取上げる。

(1) カイザー・スラウテルン＝ランダウ工科大学（Technischen Universität Kaiserslautern-Landau: RPTU）[474]

(a) 背景・経緯等

RPTU は、1970 年創立のカイザー・スラウテルン工科大学が 2023 年に文系のランダウ大学と合併して誕生した。ラインラント＝プファルツ州で 2 番目に大きく、ドイツでは最も新しい大学の一つである。約 2 万人の学生と 300 人の教授陣を擁し、160 の学位プログラムを展開する。大学院教育に力を入れ、多数の授業が英語で行われている。

先の DFG/レオポルディーナの勧告に従って、安全保障関連研究倫理委員会（KEF）を設置し、その規約と行動規範を策定している。いずれも、DFG/レオポルディーナの設置基準や模範文書に則っており、従って RPTU の取組はドイツの大学の平均的な取組を表していると考えられる。

(b) 主な取組

i) Satzung zur Sicherung guter wissenschaftlicher Praxis an der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau（優れた科学的実践の確保に関する規約）[475]

2023 年 7 月 18 日発行された本書は、優れた科学的議論と実践を促し、科学的不正行為の防止を図ることを目的に掲げる。DFG/レオポルディーナの行動規範に準拠し、3 章、23 節から構成される。主に研究倫理とインテグリティに関する内容であるが、第 1 章第 7 節「法的及び倫理的枠組み：利用権」において、安全保障関連研究、すなわちデュアルユースを取り上げている。

ii) 安全保障関連研究倫理委員会規約（Satzung der Kommission für Ethik sicherheitsrelevanter Forschung）[476]

2024 年 7 月 31 日発行の本文書は、RPTU における安全保障関連研究倫理委員会（KEF）の任務と活動の基本原則、その構成と委員、委員の法的地位、審査の申請から決定までの一連の手続、費用から構成される。その任務は安全保障関連研究に関する倫理的および法的側面の助言と評価を行い、その啓発を推進することとしている。

---

474 DWIH Tokyo, https://www.dwih-tokyo.org/ja/supporter/rptu/
475 Satzung zur Sicherung guter wissenschaftlicher Praxis an der Rheinland-Pfälzischen Technischen Universität Kaiserslautern-Landau, https://rptu.de/fileadmin/ha-1/Rechtsvorschr_Ext/GWP_-_Satzung.pdf
476 Satzung der Kommission für Ethik sicherheitsrelevanter Forschung, https://rptu.de/fileadmin/foref/Satzung_KEF_unterzeichnet.pdf

(c) 特色・注目点等

RPTU の安全保障関連研究（デュアルユース）の取扱いを含む規約と委員会の設置や構成、審議手続などが定められた安全保障関連研究倫理委員会（KEF）規約は、いずれも DFG/レオポルディーナの勧告と指導に従い、内容もそれに準拠したものである。

(2) ミュンヘン工科大学 （Technische Universität München: TUM）[477]

(a) 背景・経緯等

1868 年に創立され、これまで 19 人のノーベル賞学者を輩出してきたドイツで最も高い評価を受け、また世界の大学ランキングでも上位を占めるエリート大学である。650 名弱の教授を含む約 8,300 名のアカデミックスタッフを擁し、学生数 51,954（うち院生 10,868）名、177 の学位プログラムを展開している。学生のうち留学生が 45%を占める。TUM では、大学レベルの包括的戦略関係、学部レベルにおけるパートナーシップ、さらに研究所や個々の教授や研究者のレベルでの協働プロジェクトと共同研究など多様な国際的な研究・教育活動が盛んである。

(b) 主な取組

i) TUM Global Engagement Principles: Building Resilient International Relations（ミュンヘン工科大学の世界的活動原則：強靭な国際関係の構築）[478]

2022 年 11 月発行に発行された本文書の目的はこの活動をさらに推進し、TUM の研究コミュニティを支援することにある。しかし、本書は意思決定プロセスの指針となる原則を示すものであり、より具体的な詳細については国際ネットワーク構築に関わる関係者向けの質問集、TUM の中央支援サービス案内、先に挙げた HRK と DAAD の文書を含む巻末の資料によって補完される。質問例では、パートナーシップを管理するための助けとなる指針が例示されているが、これらは HRK 発刊の「Guidelines and Standards in International University Cooperation（大学の国際協力に関するガイドラインと基準）」に依拠している。

(c) 特色・注目点等

本文書は、文中でも指摘されているように、大学学長会議（HRK）が発行した上記の「Guidelines and Standards in International University Cooperation」及びドイツ学術交流会（DAAD）の「Compass, No Redline: Academic Cooperation within Complex Legal and Regulatory Environments（レッドラインはない：複雑な枠組み条件の下での学術協力羅針盤）」を模範に作成されている。先行の 2 文書と同じように、リスクには備えなければならないが、オープンサイエンスと国際協力の推進も目指す。しかし、両者の均衡をいかに図るのか、具体的な方法は、TUM でも、また模範になった先行 2 文書でも提示されていない。

---

[477] TUM Global Engagement Principles: Building Resilient International Relations, https://www.tum.de/en/

[478] https://www.international.tum.de/fileadmin/w00bwe/www/Das_TUM_G_A_Office/TUM_Global_Engagement_Principles.pdf

(3) ケムニッツ工科大学（Technische Universität Chemnitz）[479]

(a) 背景・経緯等

1836 年に旧東ドイツのザクセン州に創設された、同州で 3 番目に大きい研究大学である。工学、コンピュータサイエンス、自然科学の他、経済学、人文科学、社会科学の 8 学部から構成される。200 人弱の教授陣を擁し、学生数は 8,500 人ほどで、外国人がその 32%を占める。

ケムニッツ工科大学は、2024 年 4 月に報じられたデュアルユース事件の舞台となった大学である（表 2-28 参照）。2022 年 7 月から 23 年 3 月まで、ドイツ人夫婦が関係する会社の依頼を受けて、機械の可動部品を導くために使用される平軸受の研究を実施した。だが、この平軸受の研究はデュアルユースの可能性があった。もっとも、同大学は「強制的な行政審査が行われたが、当該技術は外国貿易法に照らして疑念はないものであった」との見解を公表した[480]。

デュースブルク・エッセン大学（Universität Duisburg-Essen）とシュトゥットガルト大学（Universität Stuttgart）も同社と研究協力の協議をしたと指摘された。デュースブルク・エッセンでは、自動運転に関する会議が容疑者の会社の後援で開催され、さらに同大教授の 1 人が容疑者の関係する会社に関与していた[481]。 2024 年 4 月 22 日、当該夫婦を含む 3 人が軍事転用可能な技術情報を中国に提供した疑いで逮捕された[482]。

(b) 主な取組

i) Leitfaden zum Umgang mit Projekten in Bezug auf die Ethik sicherheitsrelevanter Forschung und “Dual-Use” Aspekte（安全保障関連研究および「デュアルユース」の側面に関するプロジェクトの取り扱いに関するガイドライン）[483]

2024 年 8 月 12 日付の本ガイドラインは、国際的な学術協力（研究プロジェクト、出張、会議への出張、協力協定など）を申請および計画する際のチェックリストである。当該研究が安全保障関連研究に関係するか否か、関係する場合にはどのように対処すべきかを検討するための質問票から構成されている。

例示の質問項目のうち、研究者向けの質問では、計画されている事業（研究プロジェクト、出張、会議、協力協定など）のデュアルユースとの関連性、協力パートナーが追加的な研究安全保障上のリスクを引き起こす可能性、協力パートナーのバックグラウンド調査（本拠地に対する EU 及び米国の輸出管理法上の禁輸措置、軍事研究との関わり、機密性の高い情

[479] ドイツの工学系大学：留学生のためのガイド 2025、https://www.mygermanuniversity.com/universities/Chemnitz-University-of-Technology；Chemnitz University of Technology, Facts and Figures、https://www.tu-chemnitz.de/tu/fakten.php.en
[480] Science/Business, Chinese scientific espionage in Germany: what next? (2024/05/02), https://sciencebusiness.net/universities/chinese-scientific-espionage-germany-what-next
[481] Chinese scientific espionage in Germany: what next? (2024/05/02), https://sciencebusiness.net/universities/chinese-scientific-espionage-germany-what-next
[482] Reuters,「ドイツ、中国に軍事転用技術提供の疑いで 3 人逮捕　海軍強化の恐れ」（2024 年 4 月 23 日）、https://jp.reuters.com/world/security/GRHEUSNN4FOCPDTZXEN5U3PLAY-2024-04-22/
[483] Leitfaden zum Umgang mit Projekten in Bezug auf die Ethik sicherheitsrelevanter Forschung und “Dual-Use”Aspekte, https://www.tu-chemnitz.de/forschung/dokumente/Leitfaden_KEF.pdf

報やセキュリティに関連する情報が漏洩する可能性など）が列挙されている。これらの項目のうちいずれかに該当する場合は、安全保障関連研究倫理委員会（KEF）に問い合わせる。

KEF が申請を処理する際には次のような追加質問が課される、①研究者、その委託者/資金提供者の当該プロジェクトにおける目標と目的、②研究作業に関する潜在的なリスク評価を行うために必要な専門知識の有無、③現在の知識レベルで研究結果の利点とリスクの比較検討の可能性、④デュアルユースに関係する事項が含まれる研究成果が公表された場合、その直接的な悪用が発生する可能性、⑤第三者が意図的に結果を悪用した場合の潜在的な損害の程度と適切な対策の有無、⑥研究計画を中止にした場合の悪影響の可能性等の質問が課される。

そして、KEF による最終評価および協議は、①法的利益に重大な損害を与えるために悪用する可能性が高い知識、製品、または技術を生み出す可能性、②当該研究の目標および目的の憲法上の基本原則、基本秩序、およびケムニッツ工科大学の行動規範と適合性、③安全に関連するリスクの軽減の可能性などの質問の検証に基づいて行われ、KEF は学長に対して最終的な勧告を行う。

(c) 特色・注目点等

ケムニッツ工科大学では、DFG/レオポルディーナの勧告に従い、2022 年 6 月 16 日に既に「Ordnung zur Sicherung guter wissenschaftlicher Praxis der Technischen Universität Chemnitz（ケムニッツ工科大学の優れた科学的実践の確保に関する規律）」[484]という名称の行動規範を発行していた。上記のガイドラインは言わば二つ目の行動規範である。同じく 2022 年に安全保障関連研究倫理委員会（KEF）も設置されていたが、ガイドライン発行と同時期に KEF を補完する「研究および若手科学者の育成のための委員会（KFF）」が設置された。この 2024 年に相次いで行われた取組とデュアルユース事件との関連性を示す明確な証拠はない。しかし、表 2-28 に示したように、これらの取組が逮捕報道から数ヶ月後に行われた点、さらに国際学術協力におけるリスクに関するチェックリストという内容から、事件が多かれ少なかれ影響を及ぼしていると考えることもできる。

(4) マックス・プランク協会（Max Plank Gesellschaft/Society: MPG）[485]

(a) 背景・経緯等

1948 年にカイザー・ヴィルヘルム協会の後継組織として設立され、国内に 84 の研究所と施設を擁し、さらに国外に 4 研究所、また米国プリンストン大学、フランス・パリ政治学院（Sciences Po）、英国ユニバーシティ・カレッジ・ロンドン、東京大学など 11 カ国の大学・研究機関と共同で 19 のマックス・プランク・センターを運営するドイツ科学の国際的な研究組織である。現在 130 以上の国から約 9,000 人の研究者が当研究所で働いている。

[484] Grundsätze zur Sicherung guter wissenschaftlicher Praxis und für das Verhalten bei Verdacht auf wissenschaftliches Fehlverhalten, https://www.tu-chemnitz.de/forschung/sicherung.html
[485] Max Plank Gesellschaft, About Us, https://www.mpg.de/max-planck-centers

2022 年 11 月に DFG/レオポルディーナが発行した「Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research（科学における自由と責任：安全保障に関連する研究の取扱についての勧告：安全保障関連研究取扱）」は当協会の 2010 年 3 月 19 日付文書「Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research（研究の自由と研究リスクに対する責任ある取組に関するマックス・プランク協会の指針と規則）」を基にしている[486]。

(b) 主な取組

i) Guidelines and Rules of the Max Planck Society on a Responsible Approach to Freedom of Research and Research Risks（研究の自由と研究リスクに対する責任ある取組に関するマックス・プランク協会の指針と規則）[487]

当会の科学会員、従業員、博士課程学生を対象に、2017 年 3 月 17 日に発行された本文書は、基礎研究の成功には透明性、自由な情報交換、研究成果の公表が必要であるが、自由で透明な研究にはリスクも伴うことを提起する。リスクは必ずしも研究者の過失や故意の不正行為から生じるわけではなく、それ自体は中立的または有用であっても、第三者による成果の有害目的での悪用、すなわち「デュアルユース」のように間接的に生じる危険性もあり、民生研究と軍事研究、防衛研究と攻撃研究、「平和維持」目的と「テロ」目的の研究の明確な区別は困難を極めるようになっている点に注意を促す。

本文書は MPG の科学評議会および協会評議会によって承認されたものであるが、強制力のある規程ではなく、科学者たちが倫理的不安をより良く解決し、リスクの見逃しや不備による非難を回避できるようにする手続きの確立によって、研究の悪用を防止し、自己規制を通じてリスクを回避することを目指す。総括的な目的と範囲、研究の法的制約、倫理的に責任ある研究の原則、組織的責任の 4 つのパートから構成され、リスク分析、リスク最小化措置、成果の出版がもたらすリスクの可能性、手段としての無責任な研究の放棄、リスクの文書化と伝達、責任の所在について説明されている。

ii) Guidelines for the development of international collaborations of the Max-Planck-Gesellschaft（国際協力発展のためのマックス・プランク協会ガイドライン）[488]

2024 年 6 月 13 日付の本文書は、DFG/レオポルディーナ発行の 2023 年 9 月「国際研究協力上のリスクへの対処勧告」に沿って策定された。国際的な科学協力は科学的進歩の基盤であるが、パートナー国の特定の構造的・規制的・政治的、さらには倫理的・文化的条件によって課題も引き起こされるとして、研究の自由とリスクの認識・特定・最小化との調和を図るためのアプローチが提示されている。

MPG に所属する科学者を対象に研究の自由と規制遵守及び個人責任との均衡を図り、潜

[486] Scientific Freedom and Scientific Responsibility Recommendations for Handling of Security-Relevant Research, https://www.security-relevant-research.org/publication-scientificfreedom2022/
[487] Max Plank Gesellschaft, Procedures and Regulations, https://www.mpg.de/about_us/procedures
[488] Max Plank Gesellschaft, Procedures and Regulations, https://www.mpg.de/about_us/procedures

在リスクへの認識を高め、適用される法的規則と内部要件を理解させ、助言を得ることができる既存の選択肢とともに、リスクや衝突発生時の解決策を提示する。国際協力事業に従事する科学者に新たな義務の追加や規制の導入を意図するものではなく、国際共同研究を設計するための既存の規制をまとめた文書だと位置付けられている。

リスク最小化には、MPG の科学者が潜在的なリスクへの認識を持ち、適用される法的規則と内部要件を理解し、助言を得るための既存の選択肢を熟知して、リスクや衝突が生じた場合の解決策を提案できるか否かにあるとする。

(c) 特色・注目点等

多数の研究機関を抱える分散型研究機関である MPG では、各研究所や施設における研究の品質保証のために規則や規制を細かく定め、遵守を求めている[489]。最初に挙げた 2017 年発行の MPG 指針と規則は、こうした規則の一つである。2010 年に発刊された本書の初版は、DFG/レオポルディーナが 2022 年 11 月に発行した「科学における自由と責任：安全保障に関連する研究の取扱についての勧告（安全保障関連研究取扱）」のモデルになった。ドイツの研究セキュリティ・インテグリティの取組をリードする研究機関の一つである。

(5) ヘルムホルツ環境研究センター（Helmholtz Centre for Environmental Research: UFZ）[490]

(a) 背景・経緯等

1991 年 12 月、ライプツィヒを拠点に設立された。環境研究の分野で世界をリードする研究センターであり、複雑な環境問題に対処するために、自然科学、工学、社会科学の間の専門性の境界を乗り越えて、統合環境研究を志向する。革新的な科学的インフラと国内及び国際協力によって問題解決を図ることを目指す。UFZ はヘルムホルツ協会[491]の傘下にあり、協会の国内 18 ヵ所の研究センターの中の一つであるが、組織や運営は独立している。研究セキュリティに関しても「InHand@UFZ」と呼ばれる UFZ 独自の取組を展開する。

(b) 主な取組

i) Rules for safeguarding good scientific practice at UFZ（科学の適正な実践を保護するための規則）[492]

2023 年 3 月 24 日に発行された行動規範である。DFG/レオポルディーナの行動規範に準じつつも、独自の見解を盛り込む。科学的誠実さ、法的および倫理的基準の遵守、優れた科学的実践の保護を目的に、研究の計画から実施、成果発表までのルールを示し、不正が疑われるケースへの対応手続きを示す。特に、研究やその成果の不正使用、特に「デュアルユー

489 Max Plank Gesellschaft, Procedures and Regulations, https://www.mpg.de/about_us/procedures
490 UFZ, Our Vision; Our Mission, https://www.ufz.de/index.php?en=34258
491 The Mission of the UFZ, https://www.helmholtz.de/en/about-us/helmholtz-centers/centers-a-z/centre/helmholtz-centre-for-environmental-research-ufz/
492 Rules for safeguarding good scientific practice at UFZ, https://www.ufz.de/export/data/2/278322_Rules%20for%20Safeguarding%20Good%20Scientific%20Practice%20at%20the%20UFZ_22.06.2023.pdf

ス」に対する研究者の責任を明示する。

ii） InHand@UFZ（インハンド・アット・UFZ）[493]

国際協力に伴うリスクへの認識を高めることを目的に、UFZ の科学者に対し実践的なツールを提供し、これらのリスクに責任を持って対処するための手順の開発を目指す取組である。具体的には、既存の手順を改善し、科学者が容易にアクセスできるようなツールとプロセスの統合化を図ることである。

(c) 特色・注目点等

InHand@UFZ は、ヘルムホルツ協会（本部）のイニシアチブ・ネットワーキング基金の資金提供を受けた 3 年間のプロジェクトとして取組まれている。本プロジェクトの主要な業務は、計画中のプロジェクトにおける機会と潜在的なリスクの検討、意思決定プロセスの構築、相談サービスの提供である。運営主体や運営方法などの詳細については、不明である[494]。

(6) ライプニッツ協会（Leibniz Association/Gemeinschaft）[495]

(a) 背景・経緯等

ライプニッツ協会は、1700 年にゴットフリート・ヴィルヘルム・ライプニッツがベルリンに科学会を設立し、後に科学アカデミーとなって発展を遂げてきた。自然科学、工学、環境科学から経済学、空間科学、社会科学、人文科学まで多岐にわたる分野を網羅する 96 の独立系研究機関が所属する。科学・工学分野には宇宙物理学、農業工学、地域開発、神経生物学、新素材、免疫療法が含まれ、異なる専門分野の研究者が協力する学際的なライプニッツ・リサーチ・アライアンスを通して基礎研究及び応用研究を行う一方、世界各国の大学や産業界、他のパートナー機関との連携にも力を注ぐ。傘下の研究博物館を中心に、知識移転にも積極的で、研究者、産業界、一般市民に研究成果などの情報を提供し、政策立案者にも助言を行う。12,170 人の研究者を含む約 21,400 人を雇用し、連邦及び州政府が半額ずつ負担する費用の年間規模は 23 億ユーロである。7 年ごとに外部評価を受け、研究の質と効率性の維持に努める。

(b) 主な取組

i） Leibniz Code for Good Research Practice（適正な研究実践のためのライプニッツ行動規範）[496]

DFG/レオポルディーナの 2019 年発行の「行動規範：研究の適正な実践を保護するため

---

493 InHand@UFZ, Research Security in International Cooperation, https://www.ufz.de/index.php?en=50875

494 公開情報では得ることができなかった。

495 DWIH Tokyo, https://www.dwih-tokyo.org/ja/supporter/the-leibniz-association/ , Leibniz Association website, https://www.leibniz-gemeinschaft.de/en/about-us/history/history-of-the-leibniz-association

496 Leibniz Code for Good Research Practice, https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/Über_uns/Gute_wissenschaftliche_Praxis/Leibniz_Code_for_Good_Research_Practice.pdf

のガイドライン（Guidelines for Safeguarding Good Research Practice」に準拠して 2021 年 11 月 18 日に発行された行動規範で、ドイツの他の大学・研究機関と横並びの取組と言える。傘下の研究機関を束ねる本部（拠点）としての文書であり、悪用リスクに機関横断的に対処する包括的ガバナンスを示す。

「安全保障関連研究（security-relevant research」を研究倫理と研究インテグリティにおけるセキュリティ上のリスクと位置付けるが、このセキュリティ上のリスクとは、研究結果や関連する知見の悪用（特にデュアルユース）を指す。

ii） Risk management in international scientific cooperation: points to consider（国際科学協力におけるリスク管理の考慮すべき要点）[497]

2021 年 10 月付の本文書は、文中で明示するように、2020 年 12 月発行のドイツ学術交流会（DAAD）「レッドラインはない：複雑な枠組み条件の下での学術協力羅針盤（KIWi compass, No redline: Academic cooperation within complex legal and regulatory environments）に準拠している。

協力パートナー側による研究成果の不正流用や不適切な使用のリスクを最小化するため、各機関内で個々のパートナーや国との協働をケースバイケースで標準的・実用的・非官僚的に評価できる内部プロセスを開発・確立することを推奨し、本文書はその実施を促し、ライプニッツ協会の研究所全体における問題意識の向上を目的にしたものである。

共同研究プロジェクトのリスクと便益（初期リスク評価、費用便益分析）、デュー・ディリジェンス 、EU およびドイツの輸出管理規制枠組、健全な科学実践の確保のためのパートナーシップ構造、内部評価および国際協力に関連するリスク最小化のための既存のガイド、指針となる質問票、チェックリストを活用すること、及び情報サイトリストが盛り込まれている。

iii） Geschäftsbericht 2024（2024 年度年次報告）[498]

本文書は 2023 年 10 月から 2024 年 9 月までの研究セキュリティに関する取組を含むライプニッツ協会の活動を総括した報告書である。連邦政府（BMFTR）、また DFG/レオポルディーナを中心とした学術界の研究セキュリティに関する議論を反映しつつ、ライプニッツ協会独自のアプローチを提示している。

研究セキュリティを研究インテグリティ、国際協力、情報セキュリティに組込むとともに、これらを横断するガバナンス課題として位置付ける。また、研究セキュリティは国際共同研究における責任ある研究ガバナンスとリスク認識の問題であり、ライプニッツ協会が組織的に取組むべき活動だとの認識を示す。特に積極的にアプローチする分野として国際協力、地政学上の機微な状況、情報・データセキュリティが挙げられている。

---

[497] Risk management in international scientific cooperation: points to consider, https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/Über_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf

[498] Geschäftsbericht 2024, https://www.lobbyregister.bundestag.de/media/d4/bd/581104/Geschaeftsbericht_2024.pdf

アプローチの具体的な実施ツールは、①中央集権的管理ではなく、各研究所の対応能力を上げるための情報交換フォーマット作成、ワークショップやイベントの開催、②研究所間の経験の交換と機微な分野の研究協力に関する議論、③個別的な助言による研究所への支援、 ④研究セキュリティ Wiki（ポータルサイト）の構築、⑤情報セキュリティイニシアチブである。

iv） Leibniz Institute for Agricultural Engineering and Bioeconomy（ライプニッツ農業工学・バイオエコノミー研究所、以下 ATB）の取組事例[499]

ライプニッツ協会は、自然科学から人文・社会科学までの幅広い分野を扱う 96 の研究所から構成される集合型研究機関である。そのため、協会本部が 96 研究所を統制する中央集権的かつコンプライアンス型ではなく、本部は総括的ガイダンスを示し、助言や情報を提供する知識インフラを整備して、各研究所の自発的な取り組みを促す分権型のアプローチを実践する。そこで、それらの研究所の一つである ATB を一例に個々の研究所における取組[500]を簡単に紹介する。

各研究所は、多くの場合研究セキュリティや輸出管理に関する最終的な責任を担う。特に所長は法的責任を負う立場にあり、リスク判断や対策決定に直接関与する。そのため、研究所は高度に組織化されたコンプライアンス主体として機能する。例えば ATB の場合は、BAFA（連邦輸出管理局）のガイドラインに基づき、次のような要素から構成される内部コンプライアンス・プログラムを整備している。

・研究協力機関の信頼性審査
・客員研究者・採用時のバックグラウンドチェック
・制裁リスト確認
・デュアルユース該当性評価
・材料・試料の輸出手続き管理
・出張・技術移転の管理

リスクの特定と分析、評価、対策は各研究所がその裁量によって実施し、本部はこのリスク管理の過程を支援する。

(c) 特色・注目点等

ライプニッツ協会は 96 の法的に独立した研究所から構成される研究連合体であり、本部を入れて 97 の組織は、組織の規模に関わらずそれぞれ１票を持ち、等しく協会の意思決定に関与している[501]。研究セキュリティの取組についても、各研究所がリスク管理に責任を持ち、本部の役割はガイドラインの策定、情報共有の推進、助言や指導に留まる。このような分権的な運営が採用されているのは、多数の研究所を抱える分散的な組織ゆえと考えられる。しかし、ドイツの同様の大規模分散型研究機関において、本部が統制する中央集権的な

499 ATB, About Us, https://www.atb-potsdam.de/en/
500 この ATB の取組に関する部分は関係者への聞き取り調査による。
501 同上。

運営する組織もある[502]。規模の問題よりも、ライプニッツの運営哲学と言えるかもしれない。

各研究所の自律性は高いが、研究所横断的な研究活動もあり、研究セキュリティに関しても研究所間のネットワークがある。2025 年 11 月にライプニッツ平和・紛争研究所の主催により「ライプニッツ研究ネットワーク中国」が組織された。このネットワークの目的は中国のパートナーとの協力に関する経験を交換することによってライプニッツにおける研究セキュリティの強化を図ることである。15 のライプニッツ機関の研究者、行政部門と科学コミュニケーション部門の専門家が参加し、地政学とシステム競争、安全保障、貿易と平和、イノベーション、教育と技術政策、気候、環境と公正、開発とインフラについて議論する[503]。人文・社会科学の研究所を傘下に持つ当協会ならではの取組であると同時に、人文・社会科学分野の研究セキュリティへの関心と関与を示唆している。

研究セキュリティ上のリスクは、人文・社会科学にも起こりうる。地政学的に機微な地域での現地調査には高い危険が伴い、国益が絡むような外交や国際関係の重要資料が悪意ある人物によって利用される可能性は否定できない。さらに、人文・社会科学の研究セキュリティの取組への貢献も見逃せない。極地研究や海洋研究、宇宙研究では、自然科学分野に加え、国際法や国際関係論の知見が求められ、データや知識の移転においては法律の遵守が欠かせない[504]。ライプニッツ協会内における分野横断的ワークショップの知見が期待される。

2.7.3　資金配分機関等における取組

(1)　ドイツ研究振興協会（Deutsche Forschungsgemeinschaft: DFG）

(a)　背景・経緯等

DFG は、科学の振興を目的に 1920 年に設立された。大学及び公的研究機関の基礎研究支援を行い、助成プログラムの資金は政府（58%）と州政府（42%）によって賄われている。研究費助成のほか研究者間の協力・交流支援、若手研究者の支援、議会等への科学的助言を行っている。BMFTR（2025 年 4 月まで BMBF）を始め省庁の研究助成が個人ではなく、プロジェクトへの資金提供であるのに対し、DFG は個人研究者（ドイツ国内の大学或いは公的研究機関に所属する博士号を保持するもの）を対象に行う[505]。

既述のように、DFG はドイツの研究セキュリティの取組を主導する役割を担い、ドイツの全ステークホルダー向けの関連文書をレオポルディーナと共同で発行してきた。それらの文書については、(1)の「2024 年度までの経緯」で述べた通りである。ここでは、資金配分機関として DFG 助成金申請/受給者を対象にした文書を取り上げる。

---

502 同上。
503 China-Kompetenzen bündeln und ausbauen, https://www.leibniz-gemeinschaft.de/ueber-uns/neues/forschungsnachrichten/forschungsnachrichten-single/newsdetails/china-kompetenzen-buendeln-und-ausbauen-1
504 研究セキュリティと人文・社会科学の関係については ATB に関する聞取り調査から示唆を受けた。
505 当該プロジェクトの管理運営を行う機関を公募にて選定し、そのプロジェクト・エージェンシーが戦略やプログラムを運営する（CRDS「研究開発の俯瞰報告書 主要国の研究開発戦略：５ドイツ」2021 年、https://www.jst.go.jp/crds/pdf/2020/FR/CRDS-FY2020-FR-05/CRDS-FY2020-FR-05_50100.pdf）。

(b) 主な取組

i) Security-relevant aspects in DFG-funded research projects （DFG 資金提供研究プロジェクトにおけるセキュリティの側面）[506]

本文書（2025 年 3 月 27 日付）は、ホームページ上で DFG の研究プログラム申請者に対してデュアルユースと外国貿易法について注意喚起を行った通知文である。これらの事項はいずれも、次に述べる申請書作成説明書で詳しく述べられており、本文書はその簡単な要約で、特定の研究成果の悪用が疑われる国の研究者と協力する場合、研究パートナーや研究条件を検討項目として協力に伴う利益とリスクを比較した上で、慎重に判断を下し、リスクを最小限に抑えるための対策を計画することが重要だと指摘する。

ii) Proposal Preparation Instructions: Project Proposals（研究プロジェクト申請者のための申請書作成説明書）[507]

表 2-29 DFG 研究助成申請者に対する研究セキュリティに関する注意点の概要

デュアルユースと外国貿易法	・計画中の研究プロジェクトにおいて、研究成果が重大な有害目的のために直接悪用され得る知識、製品、技術を産み出す可能性が「ある」場合には、申請書にリスクと便益の比率の評価、リスクを最小限に抑えるための対策の計画を記述し、安全保障関連研究倫理委員会（KEFs）に諮る。意見書が出されたら添付すること。 ・プロジェクトは、対外貿易規制、特に戦争兵器管理法（Kriegswaffenkontrollgesetz）、EC規則第428/2009号（ECデュアルユース規制）、対外経済・支払法（Außenwirtschaftsgesetz）、対外経済・支払令（Außenwirtschaftsverordnung）、または禁輸規制を遵守すること。
国際協力におけるリスク	・特定の研究成果の悪用が疑われる国の研究者との協力では、悪用の潜在的な機会を真剣に受け止め、当該協力の利益とリスクを相対的に評価し、十分な情報に基づいたトレードオフの決定を行わなければならない。 ・該当する場合は、研究対象、研究パートナー、研究条件に関してリスクと便益の比率をどのように評価するか、またリスクを最小限に抑えるためにどのような対策を計画しているかを申請書に添付すること。
申請者及び研究協力者に関する情報	・申請書には申請者の雇用状況を記載 ・ドイツ在住の外国人研究者と共同でプロジェクトを行い、プロジェクト実施の責任を共有する場合、これらの個人の氏名を共同研究者として申請書に記載すること。 ・ドイツ国外の研究者と緊密に連携して当該プロジェクトを実施する場合、申請書に協力パートナーについても記載すること。ドイツ国外の協力パートナーによる重要なプロジェクト貢献が計画され、外国パートナーによる承諾書が署名されている場合には協力パートナーとみなし、申請書と共に承諾書を提出すること。
技術移転プロジェクト	DFG資金による研究プロジェクトで得られた成果を検証、または基礎研究の知見をプロトタイプや実証的応用へと発展させるプロジェクトにおいて、申請パートナーとの協力を計画している場合には補足指示に注意すること 。

本文書（2025 年 9 月付）は、ウェブサイトに掲載された通知で、DFG の研究プロジェクト助成申請者が申請書を作成するための手引きが述べられている。当該研究テーマに関する現状と先行研究、目的と作業計画、プロジェクト及びテーマに関する業績リスト、研究の背景に関する補足情報の 4 セクションから構成される。

最後の第 4 セクションの中に「安全関連の可能性のある側面に関する説明」として、 デュアルユースと外国貿易法、国際協力におけるリスク、申請者の雇用状況に関する情報、ドイツ国外の研究者と緊密に連携して当該プロジェクトを実施する場合、技術移転プロジェ

[506] Security-Relevant Aspects in DFG-Funded Research Projects, https://www.dfg.de/en/basics-topics/basics-and-principles-of-funding/security-relevant-research/proposals
[507] Proposal Preparation Instructions: Project Proposals, https://www.dfg.de/resource/blob/168314/54-01-en.pdf

クトへの民間企業協力、科学機器の取扱が取上げられている。研究セキュリティに関する注意点の主な項目とその概要を表 2-29 に整理して、示した。

(c) 特色・注目点等

DFG の研究助成は、機関を対象にした助成と個人対象のそれとに分けられる。ドイツ国内および海外のドイツの大学・研究機関、そしてそれらに所属する研究者であれば、外国人であっても助成を申請し、また海外の外国人は共同研究者として参加できる[508]。

プログラムの種類によっては、2 段階審査方式が採用されており、予備申請（draft proposal）が行われ、その通過者のみが本申請（full proposal）に進むことができる。この 2 段階方式が適用されるのは、協働研究センター（Sonderforschungsbereiche: SFB）、共同研究グループ（Forschungsgruppen）、重点プログラム（Schwerpunktprogramme）、卓越した戦略に基づく卓越クラスター（Exzellenzcluster）、研究ユニット（Forschungsgruppen）の他、海外の若手研究者にも門戸を開く大学院性向けのプログラムである研究訓練グループ（Research Training Groups）並びに国際研究訓練グループ（International Research Training Groups, IRTG）である。国際研究訓練グループについては、日本の学術振興会も連携事業として共同採択を行なっているが、予備申請書はドイツ側の共同研究者が行わなければならない[509]。海外在住の外国籍申請者に予備申請を求めることは、審査の効率的を意図したものであると考えられるが、同時に初期スクリーニングの役割を果たし、結果的にリスクの抽出に寄与する可能性がある。

(2) ドイツ航空宇宙センター・プロジェクト管理機関（DLR Projektträger: DLR-PT）[510]

(a) 背景・経緯等

ドイツの研究資金助成において、特定課題について BMFTR（旧 BMBF）や経済エネルギー省（BMWi)など連邦各省が公募する公的資金は、大学、研究機関もしくは類似の機関を対象とし、個人は応募できない。助成に当たっては「プロジェクト・ファンディング」という方式で実施される。担当省は、対象プロジェクトの管理運営を行う機関（プロジェクト・エージェンシー）を公募により選定し、選定されたプロジェクト・エージェンシーがプログラムの運営を担当する[511]。DLR-PT は、このプロジェクト・エージェンシーの一つである。組織的には、その名称が示すように、ドイツ航空宇宙センター（DLR）の一部署であるが、取扱う分野は航空宇宙に限らず、教育、健康、社会、技術、環境、持続可能性、国際協力など多岐に渡り、クライアントも国内すべての大学・研究機関である。

主な業務は、連邦省庁、欧州委員会、科学機関からの委託を受け、研究開発資金プログラ

[508] DFG が提供する助成は、プロジェクトのドイツ国内での実施部分に対してのみ適用される（DFG, Funding in an international context, https://www.dfg.de/en/research-funding/funding-opportunities/funding）。
[509] 日本学術振興会・日独共同大学院プログラム、https://www.jsps.go.jp/j-jg_externship/04_download.html
[510] DLR Projektträger, Research, Education, Innovation (About us), https://projekttraeger.dlr.de/en/about-us/about-the-dlr-projekttraeger
[511] CRDS「主要国・地域の科学技術・イノベーション政策動向（2024 年）」、https://www.jst.go.jp/crds/report/CRDS-FY2023-FR-01.html

ムに関する専門的な助言、プログラムの計画と運用の管理、適切な実施を保証するプログラム運営、資金管理、研究成果の知識移転支援、プログラムやイニシアチブの効果の分析・評価である。およそ 1,600 人に従業員を擁し、2024 年は 13,500 件以上のプロジェクトに対し、約 19 億ユーロの資金を調達した[512]。

2021 年 6 月航空宇宙技術の流出によりロシア人スパイ事件が発覚した（表 2-28 参照）。バイエルンのアウクスブルク大学（Universität Augsburg）で機械工学の博士号を取得し、アウクスブルク・イノベーション・パーク（Augsburg Innovation Park）の材料研究所で助手をしていたロシア人の Ilnur Nagaev（イルヌール・ナガエフ）は、逮捕された 2019 年ごろから同年 6 月 18 日まで、ロシアの諜報機関のハンドラーと定期的に会い、情報を提供していた。当地には欧州の宇宙開発を担う基地の一つである宇宙開発ドイツ航空宇宙センターがあり、材料研究所はその中にあった。2021 年 6 月 16 日に逮捕されたイルヌール・ナガエフは、「航空宇宙技術分野の研究プロジェクト、特にヨーロッパのロケットランチャー「Ariane（アリアン）」のさまざまな開発段階に関する情報を渡した」と供述した[513]。

既述のように、2024 年 4 月には中国への軍事転用可能な技術情報が中国に提供されたとされるドイツ人の逮捕報道があった。以下に述べるデュー・ディリジェンスに関するマニュアルは、報道から数ヶ月後の 2024 年 7 月に発行された。

(b) 主な取組

i) Due Diligence in Science: Manual for an assessment process: safeguarding science and scientific cooperation（科学におけるデュー・ディリジェンス：評価プロセス、科学の保護、科学協力のためのマニュアル）[514]

当マニュアルは、序論、評価プロセス、範例を示した付記の 3 章から構成され、大学/研究機関（以下、機関）に「科学におけるデュー・ディリジェンス（以下、デュー・ディリジェンス）」の概念を紹介し、各機関のニーズに合わせたデュー・ディリジェンスの評価プロセスの構築と実施を支援することを目的としている。まず、前提として、デュー・ディリジェンスの実施は、その努力に見合うものでなければならず、この考え方が研究者に支持されるためにはそれが研究協力活動を阻害するものではなく、協力関係を支援するような設計でなければならないと説く。

当マニュアルは、序論、評価プロセス、範例を示した付記の 3 章から構成される。表 2-30 にデュー・ディリジェンスのための評価の概要をまとめた。

---

[512] DLR Projektträger, About us, Research, Education, Innovation, https://projekttraeger.dlr.de/en/about-us/about-the-dlr-projekttraeger

[513] Matthias von Hein “Russian scientist stands trial for espionage in Germany,” DW (July 17, 2022), https://www.dw.com/en/russian-scientist-stands-trial-for-espionage-in-germany/a-60804917 ; Joseph Fitsanakis “Germany arrests Russian PhD student on suspicion of spying for Moscow,” IntelNews (June 22, 2031), https://intelnews.org/2021/06/22/01-3025/

[514] Safeguarding Science, Our Publications, https://www.safeguarding-science.eu/resources/publications/

表 2-30　DLR-PT デュー・ディリジェンスの評価の概要

誰が、いつ、何を評価し、評価を判断するのは誰か	協力のパートナー、研究の背景、 テーマに関連するあらゆる側面を協力の正式締結前に実施し、決定の最終責任は組織の長であるが、評価プロセスの調整など全体の運営は一人の担当者が担うこと。
協力パートナー、パートナー関係者、客員研究者等の評価	①制裁対象国及び禁輸対象国リストへの記載の有無、②学歴、職歴やスキル、資格、業績、特許出願、③現在の所属先と雇用主、過去の所属先及び雇用主、④個人資金調達履歴、資金調達に成功した活動への参加履歴、⑤民間部門との専門的な結び付きや活動歴とその可能性、民間部門への投資、⑥軍事関連組織（予備役を含む）への所属歴、⑦テロを目的にした団体や組織との関係の有無、該当する場合には犯罪歴•認識可能な依存関係の有無、⑧利益相反の可能性の有無、⑨差別や犯罪行為の賛美、法律違反行為や所属機関の倫理違反になる発言の有無
研究テーマと研究対象に関する評価	①輸出管理体制への適合性、大量破壊兵器に関する情報等の拡散リスク、②デュアルユースの側面、③人権等優先的価値観の潜在的な侵害リスク、④自組織の競争力に対するプラスとマイナスの影響、⑤自組織のイノベーション基盤に対するリスク
協力機関に対する評価	①所在地の制裁対象国及び禁輸対象国リストへの記載の有無、②その他の関連リストへの掲載の有無、③科学分野における研究・教育歴、評判、業績、④主な資金提供者、学界における会員資格、⑤軍事機関や組織との繋がりの可能性、⑥デリケートな話題や危険な話題との潜在的な関わりの有無
評価のフィルター	組織固有のフィルターの基準を策定する必要がある。利用可能なフィルターとして、原産国一覧、機微技術リスト、施設での予定滞在期間、関連予算、学術レベル（学位レベル、博士課程在学中、研究経験）、所属組織内での専門的な活動など。
評価プロセスと実施者	最初のステップは、新規採用者や客員研究員の受入れや海外の研究機関や研究者との共同事業に際して、当該人物や事業について評価が必要かどうかを判断することで、当該案件の申請者が責任を負う。評価結果が得られたら、責任者または担当部署が結果を分析し、計画案件のリスクと機会を含む決定書を作成する。

(c)　特色・注目点等

DLR-PT は、ドイツ航空宇宙センターに属する研究プロジェクト管理機関である。研究のセキュリティ強化を目的に「Safeguarding Science（科学の安全対策）」というプラットフォームを運営し、研究セキュリティ・インテグリティに関する調査を実施し、その報告書を公開している[515]。これまで、研究セキュリティに関する詳細な分析と実践的なガイドラインをまとめた文書を 9 種発刊しており、ここで取り上げたデュー・ディリジェンスのマニュアルはこれらのうちの一つである[516]。

デュー・ディリジェンスに焦点を絞って詳細に論じたマニュアルは、ドイツにおいて初の試みと考えられる。当該マニュアルの発行とロシアや中国が関与したスパイ事件との直接的な関連を示す証拠はないが、こうした安全保障上の脅威が背景にある可能性は否定できない。

2.7.4　まとめ

ドイツの研究セキュリティは最近まで「安全保障関連研究（security-relevant research）」と呼ばれ、主としてデュアルユースに焦点を当てた取組であった。「ポジション・ペーパー」が発出された 2024 年を契機に、外国政府の干渉やスパイ行為などの外的な脅威に視野を拡大する取組へと舵を切った。2025 年 12 月には、国家研究セキュリティプラットフォームの設立が発表され、2026 年秋には一部が試行される予定であり、2027 年 1 月より本格的な運用が始まる。BMFTR がプラットフォームの実施を主導し、また設置予定の支援サービ

515 Safeguarding Science, Home, https://www.safeguarding-science.eu
516 Safeguarding Science, Our Publications, https://www.safeguarding-science.eu/resources/publications/

スセンターも BMFTR の中に置かれる。この転換の背景には、EU の政策転換とともに、ウクライナ戦争による欧州の地政学的リスク、そして相次ぐスパイ事件があると考えられる。

「安全保障関連研究」においては、研究資金配分機関である DFG が科学アカデミーであるレオポルディーナと連携し、これまで研究セキュリティに関する取組を主導してきた。、しかし、本プラットフォームの設立により、イニシアティブは学術界から BMFTR へと移行するものと考えられる。この新しい仕組において、DFG やレオポルディーナがどのように位置付けられ、またいかなる役割を果たすのか、現時点では不明である。しかしながら、本プラットフォームの設立に当たっては、参加型の議論が行われた。また、本プラットフォームの調整運営委員会には、学術界の代表が参画する予定とされている[517]。ステークホルダーとの対話と同意を重視するドイツのアプローチは今後も維持される可能性が高い。

本調査では、大学および研究機関をそれぞれ 3 ヵ所取上げた。研究機関については、独自のアプローチを含む、積極的な取組が確認された。他方、大学においては、デュアルユース事件の当事者となったケムニッツ工科大学を除き DFG およびレオポルディーナの勧告や学術団体の提案に準じた取組が中心であった。事例数が限られているため断定はできないものの、組織体制や文化的背景の相違が、大学と研究機関との間に取組の温度差を生じさせていることが示唆される。Stifterverband（ドイツ科学振興寄付者連盟）が大学経営陣を対象に行った調査（大学バロメーター）において、大学経営陣の研究セキュリティに対する意識は必ずしも低いものではなく、本課題に取組む意志も確認された。しかしながら、官僚的手続、組織構造上の制約、そしてインフラ不足といった要因により、その推進に困難が伴っていることが明らかとなった。加えて、研究と教育に関して個々の教員および研究者が広範な裁量を有し、自律的に行動するという大学教授職および研究者に特有の文化や学問の自由に対する強固な信念も研究セキュリティの取組における制約要因の一つと位置づけられる[518]。

517 関係者への聞取り調査による。
518 同上。

2.8　イタリア

イタリアにおける研究セキュリティ及び研究インテグリティ（以下、研究セキュリティ・インテグリティ）の主管省は、大学研究省（Ministero dell'università e della ricerca: MUR)[519]である。研究インテグリティと研究倫理に関連した委員会の設置やガイドラインの発行は、MUR 直属の国の研究機関である国立研究評議会（National Research Council/ Consiglio Nazionale delle Ricerche、以下 CNR)[520]が担ったが、研究セキュリティについては、情報安全局（Dipartimento delle informazioni per la sicurezza: DIS）とサイバーセキュリティ局（Agenzia per la cybersicurezza nazionale: ACN)の協力のもと、MUR が中心的な役割を果たしている。DIS はイタリア国内外の諜報活動を統括する首相直属の治安機関で、学術における海外からの干渉や安全保障上の脅威について助言を行い、ACN は大学・研究機関のデジタルインフラの整備とサイバーセキュリティへの対応に当たる。

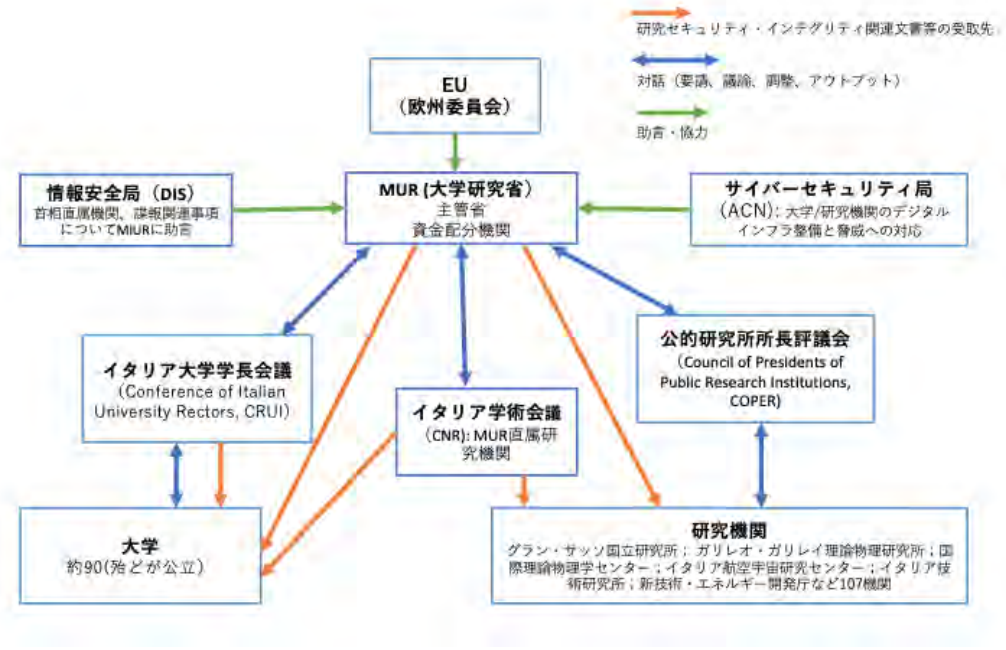


図 2-17　イタリアにおける研究セキュリティ及び研究インテグリティの関係機関相互の関連性と文書等のフロー

図 2-17 に MUR と研究セキュリティ・インテグリティのステークホルダーとの間の関係及び文書の発出等のフローを示した。加盟国は多かれ少なかれ EU の勧告や助言に対応して取組を進めるが、イタリアが研究セキュリティに関する政府の取組を公式に発表したのは 2024 年 11 月であった。本調査が取上げた他の EU 加盟国のオランダ、ドイツに比べると遅いスタートである。

519 2020 年に教育大学研究省（MIUR)は教育部門を分離する改組が行われた。
520 Consiglio Nazionale delle Ricerche のホームページ「About us」、 https://www.cnr.it/en/about-us

大学は 90 強を数え、その殆どが公立である。また、107 の研究機関があり、在籍者には海外からの研究者も多く、国際共同研究が盛んである[521]。

図 2-16 に示したように、大学と研究機関はそれぞれの代表組織であるイタリア大学学長会議（Conferenza dei Rettori delle Università Italiane、以下 CRUI）と公的研究所所長評議会（Consulta dei Presidenti degli Enti Pubblici di Ricerca、以下 CoPER)の傘下にある[522]。CRUI と CoPER は、研究セキュリティの方針確定やガイドラインの策定に参画し、政府と学術界の対話の回路が確保されている。

研究資金配分は MUR が一元的に担い、研究費は国家研究計画（PNR）のガイドラインに基づいて配分される。MUR が取扱う研究資金は、表 2-31 のように大きく 4 つのプログラムに分類される。大学及び研究機関が対象となるのは、基礎研究投資ファンドと国益に資する研究プロジェクトで、MUR が管理する研究資金の大部分を占める[523]。

表 2-31　イタリアにおける研究資金プログラム[524]

プログラム名	対象機関/組織	概要
基礎研究投資ファンド（FIBR）	大学及び公的研究機関のみ	知識の獲得や競争力の向上に資する ような国際的に高い科学技術レベルの基礎研究活動への資金配分
研究助成ファンド（FAR）	①製品/サービス生産企業 ②輸送業（陸海空） ③職人企業 ④コンソーシアム企業 ⑤MUR傘下のサイエンスパーク	問題解決型の研究成果や提案ができる研究、あるいは知的財産の保護や革新的な起業家精神が含まれる実装的な研究が対象で、場合によっては競争前段階の開発や訓練活動も包摂
国益に資する研究プロジェクト（PRIN）	大学や大学の機関、公立中等学校やMUR管轄下の公的研究機関	MURの法令に基づく運用
国家運用プログラム（NOP）		欧州構造・投資基金（ESIF）を通じて実施され、目的は欧州レベルにおいて経済・社会・地域の融合の促進と不均衡の是正

イタリアの対外関係における重要なアクターの一つは中国である。2019 年 に「一帯一路」構想に参加したものの、2023 年 12 月に離脱した。しかし、2024 年 7 月 Giorgia Meloni 首相が訪中し、関係改善と経済協力の再構築を目指した。中国とは研究・教育分野で強い協力関係を築いており、欧州と中国の学術交流の現状を追跡している「China-Europe Academic Engagement Tracker」が 2025 年 7 月 8 日に公開した調査によると、イタリア国内の 72 の大学及び公的研究機関のうち 65 ヵ所が研究・教育協力を実施し、全部で 758

521 研究開発戦略センター（CRDS）　「科学技術・イノベーション動向報告・イタリア編（2016 年度版）」、https://www.jst.go.jp/crds/report/IT20170404.html
522 学術団体には、他にもイタリアの大学の国際化を目的にしたユニ・イタリア協会（Uni-Italia Association）、学術的移動と均衡のための情報センター（Information Centre on Academic Mobility and Equivalence）全教育機関と学界の国際化を目指す国際教育協会（EDUITALIA: International Education）等がある。
523 研究開発戦略センター（CRDS)「科学技術・イノベーション動向報告イタリア編（2016 年度版）」、https://www.jst.go.jp/crds/report/IT20170404.html
524 本表は、研究開発戦略センター（CRDS)「科学技術・イノベーション動向報告イタリア編（2016 年度版）」、https://www.jst.go.jp/crds/report/IT20170404.html#sec4 に基づいて作成した。

の共同プロジェクトが展開されていた[525]。

研究セキュリティ上のインシデントに関して、イタリアでは少なくとも報道されたものはない。だが、政府高官の発言の中に脅威の実態や警告に関するものがみられる。例えば、Decode39 というイタリアにおける地政学的考察を提供する情報サイトが 2024 年 11 月 7 日に公開した記事は、情報問題を統括する Alfredo Mantovano 首相府政務次官が外国の干渉問題が長年イタリア情報機関の最優先課題であるとの認識を示し、イノベーション力の高いイタリアが特に標的となり易く、長年にわたる外国スパイの高度化する戦略を観察できると述べたことを明らかにした。Mantovano 氏は、高リスク分野として生物医学、ロボット工学、半導体を挙げた[526]。同氏は特定の国を名指してはいないが、Il Messaggero 紙によると、イタリア政府の懸念は中国、ロシア、イランなどに向けられている[527]。

一方で、研究者自身に危害が及んだ重大な事件があった。2016 年、イタリア人大学院生がフィールド調査地のエジプトでスパイ容疑を掛けられて諜報員に殺害された。このため、在外での研究・教育活動に従事する学生と教員・研究員の生命と人権を保護するためのガイドライン作成への切実なニーズが高まり、CRUI が個々の大学の取組や考えを踏まえてガイドラインを作成するに至った。

2.8.1　研究セキュリティ・インテグリティ関連政策動向

表 2-32　イタリアの研究セキュリティ・インテグリティ関連の政府と関連機関の動向（現在まで）

発行年	文書等の名称	発行組織
2015年（2029年改訂）	Guidelines on Research Integrity(研究インテグリティに関するガイドライン)	国立研究評議会（CNR）
2023年	Cybersecurity: Research & Innovation Agenda, 2023-2026 (サイバーセキュリティ：研究とイノベーション行動指針 2023-2026)	サイバーセキュリティ局（ACN） 大学研究省（MUR）
2024年7月24日	研究セキュリティに関するラウンドテーブルの開催	MUR
2024年11月7日	Piano d'azione nazionale per tutelare l'università e la ricerca italiane dalle ingerenze straniere（イタリアの大学と研究を外国の干渉から保護するための国家行動計画）の策定を発表	政府
2025年8月	National Framework for the Integrity and Security of Research（研究のインテグリティとセキュリティに関する国家枠組）	MUR
2025年8月	Guidelines for Research Institutions for the Integrity and Security of Research（研究のインテグリティとセキュリティに関する研究機関のためのガイドライン）	MUR

表 2-32 に、現在までのイタリアにおける研究セキュリティ・インテグリティに関する取組をまとめて示した。

2024 年 6 月にイタリア・プーリア（Puglia）で G7 サミットが開催されたが、7 月の科

[525] Italy: Transparency gap and collaborations under scrutiny, https://ceias.eu/italy-transparency-gap-and-collaborations-under-scrutiny/
[526] How Italy plans to tackle foreign interference in research（7 November 2024, Decode 37, https://decode39.com/9677/how-italy-plans-to-tackle-foreign-interference-in-research/
[527] Italy's spooks combat Chinese and Russian espionage in universitiesI,6 November 2024, The Italian Insider, https://www.italianinsider.it/?q=node/12919: “Foreign influence prompts Italy to shield universities, research”, The NRI Nation, https://www.mynrination.com/italy/2024/11/07/foreign-influence-prompts-italy-to-shield-universities-research

学技術大臣会合では研究セキュリティが議題に上り、その重要性が確認された。また、イタリアはより洗練された脅威に晒されている国の一つであり、なかでもバイオメディカル、ロボット工学、半導体はそのターゲットにされているとの認識が、政府高官の間で共有されるようになった。イタリアの研究分野における外国から干渉に対する懸念が高まり、対応を図ることが急務になった。2024 年 7 月 24 日、MUR は研究セキュリティに関するラウンドテーブルを開催し、議論を始めた[528]。

(1) 2024 年度までの経緯

(a) Guidelines on Research Integrity（研究インテグリティに関するガイドライン）[529]

国立研究評議会（CNR）内に研究倫理と生命倫理委員会が設置され、併せて研究インテグリティ及び研究倫理に特化して議論する小委員会も設けられた。2015 年、小委員会の議論を基礎に、研究における不正行為の防止に関する「研究インテグリティに関するガイドライン」が作成された。

(b) Cybersecurity: Research & Innovation Agenda, 2023-2026（サイバーセキュリティ：研究とイノベーションのための行動指針）[530]

ACN と MUR の共同文書である本指針は、重要セクターのサイバー脅威からの保護、非 EU 技術への依存を減らし、地政学的リスクを管理するための強力な欧州初のテクノロジーセクターの育成、学術界と研究開発から得られた研究成果を商業的に実装し、教育とトレーニングを含むサイバーセキュリティエコシステムの支援を目的に、投資とイノベーションのための優先分野を特定する。そして、情報通信デバイスを保護するための方法とツールの開発、クラウドセキュリティとデータ保護、量子コンピューティングの導入、安全なソフトウェアサプライチェーンの構築、サイバーレジリエンスとインシデント対応の強化を提案した。

(c) Piano d'azione nazionale per tutelare l'università e la ricerca italiane dalle ingerenze straniere（イタリアの大学と研究を外国の干渉から保護するための国家行動計画の策定）を発表[531]

イタリア政府は学術・研究分野の安全保障強化の枠組として国家行動計画を策定することを発表した。発表の記者会見が Palazzo Chigi（パラッツォ・チジ）で開催され、MUR の Bernini 大臣、Mantovano 次官、CRUI 会長の Giovanna Iannantuoni 氏、CoPER 会

528 Formiche Net, "Sicurezza della ricerca. Ecco il modello a cui pensa il governo Italiano"(07/11/2024), https://formiche.net/2024/11/piano-nazionale-anti-ingerenze-straniere-universita/#content
529 Guideline for Research Integrity, https://www.cnr.it/en/ethics
530Cybersecurity: Research & Innovation Agenda, 2023-2026, https://www.acn.gov.it/portale/documents/20119/87266/ACN_ResearchInnovationAgenda_EN.pdf/e8b2b315-b3db-fab4-be32-293422266986?t=1704453743342
531 Presidenza del Consiglo dei Ministri, "Piano d'azione nazionale per tutelare l'università e la ricerca italiane dalle ingerenze straniere " (7 Novembre 2024), https://www.governo.it/it/articolo/piano-d-azione-nazionale-tutelare-l-universit-e-la-ricerca-italiane-dalle-ingerenze

長の Antonio Zoccoli 氏が出席し、策定される文書に盛り込まれる基本方針、内容の概要などが説明された[532]。

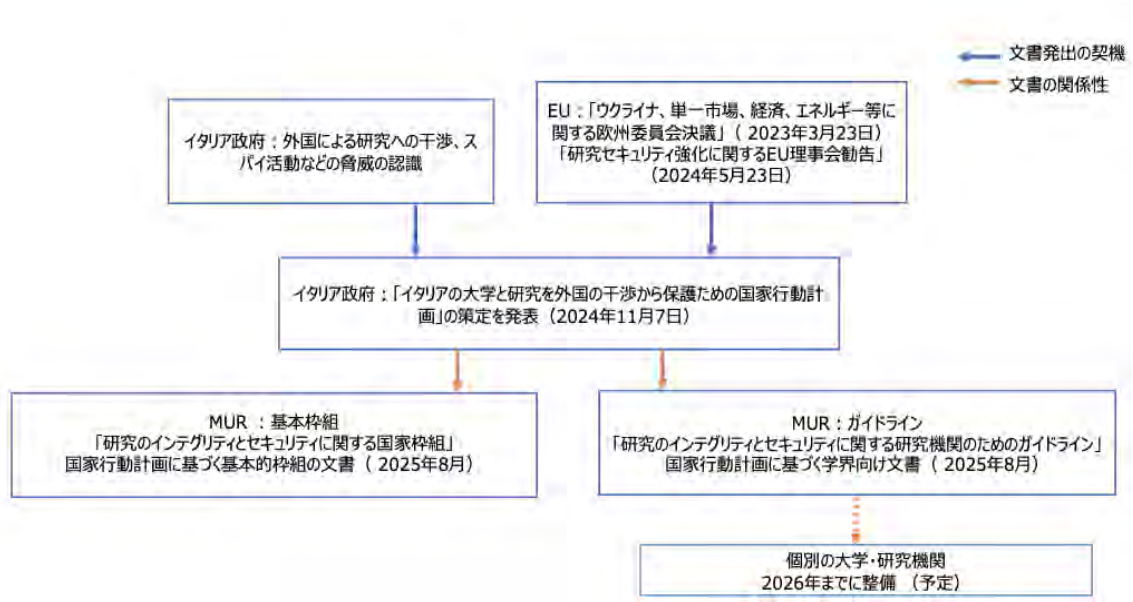


図 2-18　イタリア・MUR の研究セキュリティ関連文書作成の過程

図 2-18 にこの取組の契機となった事項、そして本計画がどのような文書に結実したのか、その過程を示した。

EU は、2023 年 3 月 23 日「European Council conclusions on Ukraine, single market and the economy, energy, and other items（ウクライナ、単一市場、経済、エネルギー等に関する欧州委員会決議）」を発出し、「欧州全域の研究者・学者の意識向上とレジリエンス構築が急務」との見解を示した[533]。さらに、2024 年 5 月 23 日には、「Council Recommendation on Enhancing Research Security（研究セキュリティ強化に関する EU 理事会勧告）」を上梓した[534]。本行動計画の策定は、この相次ぐ EU の取組に歩調を合わせ、また勧告を遂行したものだと言える[535]。2024 年 12 月に開催されたグローバル研究エコシステムのセキュリティとインテグリティに関する G7 会議（イタリア・プーリアの州都バーリ Bari）に合

532 会見では計画の中身が議論されたが、その内容を記述した政府文書を見つけることはできなかった。新聞報道では、その内容が次のように説明されている。「本案は、欧州各国との協調のもと、研究機関の日常業務への影響を最小限に抑えつつ、効果を発揮する包括的かつバランスの取れたモデルを目指している。省庁横断的な連携、特に MUR と首相府及び DIS の水平的な連携によって、制裁よりも予防、研究それ自体ではなく機関に照準を合わせ、EU 方針との整合性を図ること、そして法制化はしないことを方針に打ち出した。国家ガイドライン、対象別研修モジュール、教育リソース、様々なシナリオに対応したリスク軽減戦略の柱から構成され、リスクアセスメントは、自己評価用信号機システムを採用する。すなわち、緑信号なら脅威度は低く、黄信号は注意と追加審査を要する状態で、赤信号の場合には業務を直ちに停止し、DIS に通報して徹底的なリスク評価が必要になり、MUR への報告義務も生じる。」（DECODE39 (Geopolitical Insights from Italy), “How Italy plans to tackle foreign interference in research”, 7 Nov. 2024, https://decode39.com/9677/how-italy-plans-to-tackle-foreign-interference-in-research/）

533 European Council conclusions, 23 March 2023, https://www.consilium.europa.eu/en/press/press-releases/2023/03/23/european-council-conclusions-23-march-2023/

534 Council Recommendation on Enhancing Research Security, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510

535 The Italian Insider, “Italy's spooks combat Chinese and Russian espionage in universities”(6 November 2024) , https://www.italianinsider.it/?q=node/12919

わせて正式に提示され、2025 年の試験運用を経て、2026 年までに全ての大学・研究機関で本格的に導入するとされた[536]。

記者会見で、Bernini 大臣は「この計画は特定の国を敵視するものではなく、我々の研究を守るための措置だ」と述べ、本質的に善悪のある国など存在せず、善悪の分かれる行為のみが存在するとの中立的立場を強調した[537]。2024 年 12 月 4 日にバーリで開催された全国公開会議において策定案が提示された。

(2) 最近の主な動き

上記の提案は、2025 年 8 月に、以下に述べる 2 文書として MUR より発出された。前者は政府の取組を示し、後者は大学・研究機関向けのガイドラインである。いずれの文書も、MUR が設置した研究セキュリティ作業部会が策定を担ったが、この部会には専門家に加え、CRUI と CoPER の代表者が参加した[538]。

(a) MUR

i) National Framework for the Integrity and Security of Research（研究のインテグリティとセキュリティに関する国家枠組、以下、国家枠組）[539]

本文書は、既述のように 2024 年 11 月 7 日に政府が策定を発表した「国家行動計画」を根拠に発出された 2 本のうちの一つで、政府が責任を持って取組むべき事項が書かれている。提案事項を「イタリア（研究セキュリティ）モデル」と称し、その目的はオープンサイエンスと学問の自由の原則を守るための最も効果的な保護策として機能することにあるとする。表紙や目次を除いて本文は 5 頁で、研究インテグリティ及び研究セキュリティの定義と政府の取組の方向性の 2 章から構成されている。要点を簡潔に列挙する体裁になっている。

文書は、EU レベルの合意事項に沿って、効果的な対策を設計・実施するためには、協調的な集団的取組が不可欠だとの認識を示す。その背景には、研究セキュリティをめぐる強い危機感がある。本文書は、その序文の中で「イタリアの大学・研究機関の約 80%が参加した専用調査で得られた結果によれば、国内研究機関が直面するリスクは増加傾向にあり、多様な形態で顕在化する可能性がある」と指摘した。イタリアの研究システムは政府機関や独立機関などの多様なステークホルダーが情報や経験を共有する対話によって支えられており、この研究セキュリティに関しても、リスクを特定し、軽減するために共通の責任を負うことが求められている。すなわち、研究従事者と資金配分機関が、当該研究の潜在的なリスクを認識し、両者が資金提供を決定する前に対話を開始してリスクを軽減できるようにすることである。

---

536 Formiche,"Sicurezza della ricerca. Ecco il modello a cui pensa il governo italiano'(07/11/2024), https://formiche.net/2024/11/piano-nazionale-anti-ingerenze-straniere-universita/#content
537 Formiche,"Sicurezza della ricerca. Ecco il modello a cui pensa il governo italiano'(07/11/2024), https://formiche.net/2024/11/piano-nazionale-anti-ingerenze-straniere-universita/#content
538 それぞれの文書の要約ページの脚注参照のこと。
539 National Framework for the Integrity and Security of Research, https://www.sicurezzaricerca.mur.gov.it/wp-content/uploads/2025/08/National-Framework.pdf

政府の取組には、上記の「Council Recommendation on Enhancing Research Security（研究セキュリティ強化に関する EU 理事会勧告）」（2024 年 5 月 23 日）に準拠して、（各レベルの）政府関係者及び各組織の調整主体を含む研究機関の結集の下、National Center for Research Security and Integrity（国立研究セキュリティ・インテグリティセンター、仮称）の創設が掲げられて。このセンターには各レベルの政府機関と大学・研究機関が結集する。

大学・研究機関には研究セキュリティ・インテグリティに関する連絡窓口の設置を促す。一方、政府は技術作業部会及びタスクフォースの調整を通じ、不当な干渉の特定、外部契約・共同研究における最低限のデュー・ディリジェンスの推奨、データセキュリティ・倫理・インテグリティを保護する措置の特定・適用促進を目的にガイドラインと手順書を確定し、かつ定期的に更新する責務を負う。そして、標準化されたリスク評価ツールを開発し、大学・研究機関の要請に応じて支援をしなければならない。さらに、大学・研究機関や研究資金提供及び実施機関と管轄政府当局との円滑な連携を促進するために、予備的自己評価システムの効果的かつ効率的なモデルを開発することも挙げられた。

このイタリアモデルを導入する上で大学・研究機関には、研究セキュリティ・インテグリティに関連する事項について組織内で周知徹底し、研修を実施すること、現地訪問時の潜在リスクを最小化するために訪問者プロトコルの策定、進行中の外部連携に関するデータの収集と定期的な更新の確保などが求められた。

ii) Guidelines for Research Institutions for the Integrity and Security of Research（研究のインテグリティとセキュリティに関する研究機関のためのガイドライン、以下、ガイドライン）[540]

「国家行動計画」に基づく 2 本の文書のもう一つが、大学・研究機関の責務について論じた本書である。本ガイドラインは、「国家枠組」文書で定義される大学及び研究機関（以下、機関）に対し、研究セキュリティ強化のための運用指針を提供し、機関の意識向上、研究システムのレジリエンス強化、効果的な保護対策の開発・実施支援を図ることを目的にしている。機関では何をどのようにアプローチするのが望ましいのか、各機関に求められる事項が列挙されている。国家行動計画と同様、表紙と目次を除くと、5 頁、8 項目の短い文書で、研修モジュールや記入すべきフォーム、対象アイテムの列挙、参照などのより具体的な指示事項については、専用サイトのリンクが貼られており、アクセスして確認できるようにされている。

機関に要請される主要な取組として、自覚とコミュニケーション、研究活動責任者の責務の明確化、データ保護とサイバーセキュリティ、潜在的なデュアルユース物品の管理が挙げられ、それぞれにおいて以下のような 6 事項が提起されている。

[540] Guidelines for Research Institutions for the Integrity and Security of Research, https://www.sicurezzaricerca.mur.gov.it/wp-content/uploads/2025/08/Guidelines.pdf

① 自覚とコミュニケーション

ここでは、スタッフおよび学生へのタイムリーな情報伝達、セキュリティに関するニュースレターおよびプレゼンテーション、機関ウェブサイト内の専用ページの開設、研究コミュニティ内での意見交換の促進、研究インテグリティとセキュリティ、サイバーセキュリティ及び海外旅行に関する研修の実施が盛り込まれている。

特に、機関ウェブサイト内の専用ページについては、機関の広報資料・情報資料、ガイドライン、国家機関（政府・省庁等）が定める要件に基づき、省庁が特別に開発したウェブサイトのリンクを掲載することが必須とされ、このリンクには ACN 及び DIS が含まれ、これらの機関に直ちに接触できるようになっている。

② 活動責任者の任務

研究活動の責任者は、「インテグリティとセキュリティ」フォームの確認、リスクの予備的自己評価、当該研究の科学分野と海外との協力関係及び資金調達に関する分析、報告書（軽減策および担当者によるサポートを含む）の作成、自己評価シートの定期的な更新を行わなければならない。

③ 評価シートによる自己評価

評価シートを用いて、リスクを計算し、報告書を作成して、指摘された問題点を緩和するための対策を実施しなければならない。また、必要に応じて所属機関の研究セキュリティとインテグリティに関する担当者もしくは最高責任機関に相談を行い、各項目を評価することも求められる。

④ データ保護とサイバーセキュリティ

研究活動保護におけるサイバーセキュリティの影響に関する研修、サイバーリスクの分析と管理、ACN と GPDP（Garante per la protezione dei dati personali、情報保護局)及び AGID（Agenzia per l'Italia Digitale、デジタル庁)など関連当局との協力、規制および慣行に関する継続的な最新情報の提供、重要な情報資産の特定とデータ保護並びにアクセス制御を行う。

⑤ デュアルユースの物品および技術

デュアルユースに関する実施事項は、その物品および技術（民生用途と軍事用途の両方に使用できる特性を持つもの）の EU 並びに米国や英国など各国レベルでの規制、関連物品や技術の盗難や無許可輸出のリスクの自覚、平和的な研究目的とは無関係な個人や組織による情報・知識・科学資料の収集への関心に対する注意喚起、デュアルユース製品に関する研究の管理に関する内部コンプライアンスプログラムの採用、利益相反ポリシーの見直し・更新・適用である。

⑥ その他

利益相反、海外旅行の安全対策（旅行ガイドブックと旅行記録簿の作成・カスタマイズされた安全ブリーフィング・ 情報モジュール）、海外旅行・滞在の基本ルール、外部スタッフの訪問に関する注意事項（訪問に関するベストプラクティスの定義、身元・目的・滞在時間など訪問者記録の定式化）等について触れられている。

2.8.2　大学・研究機関における取組

イタリアにおける大学の取組は、一般的に研究倫理と研究インテグリティに関する行動規範の発行に止まっており、研究セキュリティに関するものはあまりない[541]。これは政府（MUR）の取組が始まったばかりであるためだと考えられる。それでも、大学や学術団体による独自の取組がみられる。

(1)　ローマ・ラ・サピエンツァ大学（Sapienza – Università di Roma）

(a)　背景・経緯等

首都ローマに位置する国立大学である。1303 年に創設された中世大学として欧州でも有数の伝統を持ち、学生数はイタリア最大規模の約 12 万人である。自然科学から人文・社会科学まで幅広い分野からなる 11 学部 65 学科から構成される。学術水準は、特に古典・古代史の分野において世界でもトップを争うとされ、考古学や物理学、法学でも高いレベルにある。これまで 10 人のノーベル賞受賞者を出してきたイタリアを代表する大学である。

(b)　主な取組

i)　Guidelines on compliance for dual-use research activities within collaboration outside the European Union （EU 域外での協力におけるデュアルユースの研究活動のコンプライアンスに関するガイドライン）[542]

2024 年 11 月 12 日発行の本ガイドラインは、2021 年 9 月 15 日の欧州委員会の勧告「Commission Recommendation on internal compliance programmes for controls of research involving dual-use items under Regulation（デュアルユース物品を伴う研究の輸出管理に関する内部コンプライアンスプログラム）」[543]に準拠し、EU 域外におけるデュアルユース技術に関する共同研究活動のための内部コンプライアンスプログラム（ICP）を定め、その理解を促すことを目的にしている。コンプライアンスのための体制と運営、デュアルユースとその関連用語の定義、研究費申請における注意事項の３つのパートからなる。

① 運営組織

2021 年に設置された学際研究倫理委員会（CERT）を 2024 年に改正して、デュアルユースに関する規定を定めた。これにより、当委員会には少なくとも 1 名のデュアルユースに関する専門家が加わることになった。

② デュアルユース研究に関する委員会の任務

本委員会は、デュアルユース関連活動の支援、欧州のデュアルユース規制の実施・適用支援、博士課程学生・研究者・学術職員・管理職員を対象とした、これらのテーマに関する研修の提案と支援について、学内における国内（MUR、CRUI）および EU 承認のガイドライン・規制の実施、促進を行う。

---

[541] 英語及びイタリア語によるインターネット検索による。
[542] Guidelines on compliance for dual-use research activities within collaboration outside the European Union, https://www.uniroma1.it/en/pagina/sapienza-dual-use-research-guidelines
[543] EUR Lex, https://eur-lex.europa.eu/eli/reco/2021/1700/oj/eng

③ 作業計画

デュアルユース研究に関する意識向上のための情報提供、学術コミュニティを対象としたデュアルユースに関するキャンペーン実施、研究管理のための運用ツールの提供、研究倫理研修の強化、中央管理部門および学部部門における研究管理に携わる事務職員を対象とした研修、欧州のデュアルユース規制に関連する技術・科学的な責任の連携体制の確立が盛り込まれている。

(c) 特色・注目点等

デュアルユースに関する研究のコンプライアンスのガイドラインは、イタリアの他の大学には見られない取組である。本文書の策定は、EU の勧告に準拠した自発的なものである。当大学は国際的に高い評価を受け、国際的な学術交流も活発であり、本ガイドラインはこうした国際的な地位に対応したものだと考えられる。

(2) イタリア大学学長会議（Conferenza dei Rettori delle Università Italiane: CRUI）

(a) 背景・経緯等

1963 年に設立されたイタリアの国公立大学および一部の私立大学の学長で構成される学術団体である。イタリアの高等教育機関の自主性を尊重しつつ、教育・研究の質の向上並びにイタリアの大学制度の発展を目的に活動している。2001 年、管理・執行機能を担う CRUI 財団が設立された。CRUI 財団は、社会・文化の発展を目的とした活動やプロジェクトの推進事業を受託し、大学と社会をつなぐ架け橋の役割も果たしている[544]。

2016 年 1 月、ケンブリッジ大学博士課程のイタリア人学生の Giulio Regeni（ジュリオ・レジーニ）氏が調査でカイロに滞在中、エジプトの諜報員にスパイ容疑で拘束され、惨殺された[545]。

この Giulio Regeni 事件は、イタリアの大学に大きな衝撃を与え、在外での研究・教育活動に従事する学生、教員・研究員の生命と人権の保護が急務となり、イタリアの複数の大学が対策に取り掛かった。例えば、Università degli Studi di Trieste（トリエステ大学）が学生・教職員の在外活動のための研修コースを実施し、Università degli Studi di Ferrara（フェラーラ大学）は安全に関する会議を開催した。また、ピサの Sant'*Anna* School of Advanced Studies（サンタ・アンナ高等学院）は「注意義務」と研究者の安全についての検証を行い、Dipartimento di Culture Politiche e Società dell'Università di Torino（トリノ大学政治文化社会学部）は学生の海外での安全をテーマとした研究プロジェクトを立ち上げた[546]。

CRUI は、全大学共通の指針を作成すべく作業部会を組織し、個々の大学の実践や議論をベースに、2023 年 2 月に次のような国外おける研究・教育活動の安全を図るガイドライン

544 The Conference of Italian University Rectors (English version), https://www.crui.it/the-conference-of-italian-university-rectors.html
545 法務省「エジプト人権報告書 2020 年版」、https://www.moj.go.jp/isa/content/001380808.pdf
546 CRUI, “Sicurezza nelle missioni all’estero: le Linee guida” (Febbraio 2023), https://www.crui.it/highlights/sicurezza-nelle-missioni-all’estero-le-linee-guida-4947.html

を作成した。

(b) 主な取組

i) Linee guida per la sicurezza nelle missioni all'estero in zone a rischio geo-politico e socio-sanitario del personale delle Università（大学の教職員/学生の地政学的・社会保健上のリスク地域における海外派遣安全ガイドライン、以下 CRUI 海外派遣ガイドライン）[547]

本ガイドラインの作成にあたっては、CRUI（イタリア大学学長会議）の指示に基づき、CUCS（開発協力のための大学調整機構）内に、Università degli Studi di Trieste（トリエステ大学）が調整役を務める作業部会が設置され、Università degli Studi di Torino（トリノ大学）、Università di Pisa（ピサ大学）、Università degli Studi di Urbino（ウルビーノ大学）、Università degli Studi di Verona（ヴェローナ大学）、Università degli Studi di Napoli, L'Orientale（ナポリ大学ロレンツァーノ）、Università Cattolica del Sacro Cuore（サクロ・クオーレ・カトリック大学）が参加し、2023 年 2 月に発行された。

教員、研究者、博士課程の学生、研究奨学生、言語専門家、技術・管理スタッフなど、仕事や研究のために、地政学的、社会・健康上のリスクのある地域に海外出張するイタリアの大学関係者に、手軽に参照できるツールを提供することを目的にする一方、各大学の自主性を最大限尊重し、自由に採用し、各大学の事情に応じて変更もできるようなものが目指された。

表紙と目次を除いて 16 頁から構成され、リスク分析、リスク評価、リスク回避の３つのパートに分けられ、詳述されている。ここでは、各パートの要点は以下の通りである。

① リスク分析

リスクの認識は常に主観的なものであり、個人の「観察力、人物や状況の分析力、予期せぬ出来事に対する即興力」に基づく個人の判断が重要な役割を果たすため、科学的謙虚さ、現地の文化に対する理解の深化、適応能力の向上が求められる。地政学的および社会衛生上のリスクは、個人または状況の脆弱性が著しいと悪化する場合がある。そのため、環境的、文化的、物流的、社会政治的要因のほか、官僚手続きの不適切な履行に起因する要因など、あらゆる要因を考慮に入れる必要がある。

目的地国に関する最新情報や考慮すべき緊急事態に関する情報は、外務・国際協力省（Ministero degli affari esteri e della cooperazione internazionale, MAECI）のウェブサイトの他、関連情報サイトを広く参照して入手したり、渡航先国に関する有用情報を掲載する Unità di Crisi della Farnesina（外務・国際協力省の危機対策ユニット）[548]のアプリ[549]を携帯電話にダウンロードしたりするなど、リスク分析は入念に収集された情報に基づか

[547] Linee guida per la sicurezza nelle missioni all'estero in zone a rischio geo-politico e socio-sanitario del personale delle Università, https://www.crui.it/highlights/sicurezza-nelle-missioni-all'estero-le-linee-guida-4947.html

[548] Farnesina は Ministero degli affari esteri e della cooperazione internazionale（外務・国際協力省）の別名である。

[549] 海外旅行者向けに安全情報や緊急連絡サービスをまとめた無料アプリで、https://www.viaggiaresicuri.it/download-app よりダウンロードできる。

なければならない。

② リスク評価

リスク評価は、実践を通じてリスクの有無とその程度を学ぶ作業であり、その過程でリスクに対する自己の認識の程度を知り、潜在的なリスクに関する知識の不足に対し事前に対処することができる。

③ リスク回避

リスクを回避、もしくは遭遇してもできるだけ軽減するための方法として最も重要なのが出発前の研修である。研修は、単なる情報提供ではなく、ケースバイケースで活用できる有用な知識を提供する。

(c) 特色・注目点等

本ガイドラインは、Giulio Regeni 事件を受けて、イタリア国内の大学が個別に行ってきた対策を参考に、作業委員会を設置して議論を重ねて完成したこともあり、想定を容易にする例示や有用情報提供先の紹介などを含めて、詳細かつ具体的な内容からなる実践書である。例えば、最新の現地状況を把握する場合、治安、政治情勢、社会・文化事情、衛生状態について、項目ごとにより正確な情報を入手するための方法と関連機関及びそのアクセスのリンク先が分かり易く掲載されているので、問題発生時や疑問が生じた時に直ちに役立つものと考えられる。

(3) トレント大学国際研究大学院（University of Trento/Università di Trento, School of International Studies: SIS）

(a) 背景・経緯等

トレント大学は 1962 年に開校した新興大学であり、本大学院は 2001 年に国際研究学部として設立された。2012 年には関係学部間の連携によって経済学、政治学、法学分野の教育と研究を担う大学院に再編された。授業は全て英語で行われ、イギリスの University of Glasgow（グラスゴー大学）、アイルランドの Dublin City University（公式名 Ollscoil Chathair Bhaile Átha Cliath、通称ダブリン・シティ大学）、チェコ共和国の Univerzita Karlova v Praze（プラハ、カレル大学）と共同の博士課程プログラムを実施するなど、国際化が推進されている。下記の取組にも、こうした学生と教職員の頻繁な国際移動が影響していると考えられる[550]。

(b) 主な取組

i) Guidelines for carrying out research activities in risk areas（リスクのある地域で研究活動を遂行するためのガイドライン）[551]

2025 年 3 月に刊行された本文書も、CRUI 海外派遣ガイドラインと同じく海外における

[550] SIS, “About Our School,” https://www.sis.unitn.it/60/about-our-school
[551] Guidelines for carrying out research activities in risk areas, https://corsi.unitn.it/sites/cds/files/2025-03/guidelines-reasearch-risk-areas-sis_1.pdf

研究・教育活動上のリスクへの対応を示したものである。だが、CRUI ガイドラインに比べると、「序」を入れてわずか 5 頁と短く、内容的にも簡素である。地政学的リスクと衛生状況および生物学的・化学的・物理的要因への曝露可能性の 2 点から現地研究開始前に取るべき措置が説明され、現地調査中の緊急事態発生時の対応手順へと続き、最後に現地調査終了時の対応が、それぞれ要点を絞って短く説明されているだけである。

(c) 特色・注目点等

本文書が簡素なのは、すでに詳細な CRUI のガイドラインがあるためと考えられる。ただ、CRUI のガイドラインはイタリア語で書かれており、英語でしかも要約版のような体裁は留学生や海外からの客員研究員などには便利であると考えられる。

2.8.3 まとめ

イタリア政府は、大学・研究機関をめぐるリスクの脅威が増す中で、2024 年の欧州理事会勧告を採択し、国家行動計画を策定することを発表した。MUR は、この提案に基づいて２つの文書を同時に発出した。「国家枠組」は文字通り研究セキュリティ・インテグリティに関するイタリアの取組のフレームワーク（モデル）を示したものである。「ガイドライン」はその運用ツールであり、大学・研究機関及び研究者の責務、省庁間の責任分担等が述べられている。だが、リスク特定化のための文書や手順に関しては関連するサイトを参照するように指示され、併せてそのリンクが示されているのみで、各大学・研究機関が実際に取組を進めていくための具体策についての記述はなく、今後の作業に委ねられている。

2024 年 7 月に「国家行動計画」策定提案が発表された際、Italian Insider 誌は、本案について、外国勢力による不正な影響から守られた安全な学術環境を速やかに構築するために、情報安全局（DIS）とサイバーセキュリティ局（ACN）による迅速な介入の道筋を定めている点で他の欧州諸国の取組とは一線を画するとコメントした[552]。確かに「国家枠組」と「ガイドライン」のいずれにおいても、この考え方が反映されている。例えば、前者で創設が提案されているセキュリティセンターの政府関係機関にはこれら 2 機関が含まれ、また後者では DIS 及び ACN のリンク先が明示され、迅速な関与の可能性が示唆されている。

しかしながら、これら 2 文書の策定には、CRUI と CPER という大学と研究機関を代表する団体が参画しており、情報機関の迅速な関与は学術界も合意の上の取決めである。こうした学術界の協力姿勢は取組の推進に貢献するものと考えられる。

一方、大学や学術団体には、政府（MUR）の働きかけではなく、独自の取組を行う組織もみられた。ローマ・ラ・サピエンツァ大学は EU の勧告に従って、EU 域外との国際的研究協力におけるデュアルユースに関するコンプライアンスのためのガイドラインを作成した。また、政情不安定地域における現地調査中の院生殺害事件の後、CRUI は地政学的リスク地域での研究・教育活動におけるガイドラインを作成し、トレント大学国際研究大学院でも同様の取組が見られた。

[552] Italy's spooks combat Chinese and Russian espionage in universitiesI,6 November 2024, The Italian Insider, https://www.italianinsider.it/?q=node/12919 の記事による。

CRUI のガイドラインは研究セキュリティの取組みだけでなく、研究者自身の生命や健康への脅威、さらに人権侵害等の課題も含め、研究者を取り巻く今日の課題への包括なアプローチであり、我が国の大学でも参考にできる取組だと考える。

第3章　研究インテグリティと研究セキュリティについての意見交換会の実施

3.1　意見交換会の実施概要

研究インテグリティと研究セキュリティの確保に関連するこれまでの政府方針、大学における取組についての講演を行うとともに、参加者（大学・研究機関等における研究インテグリティに関連する業務の担当者）を交えて意見交換会を 2025 年 12 月～2026 年 1 月に 3 回開催した。

開催要領は以下のとおりである。意見交換や関係者のネットワーク作りを促進するために対面での開催とし、日本全国から参加可能とするように、東京・大阪の 2 か所で開催した（東京で 2 回、大阪で 1 回開催）。

＜対象＞

・大学、研究機関等における研究インテグリティと研究セキュリティの確保のための取組に関係のある業務の担当者（大学の教職員、研究機関・企業の研究者・事務担当者等）

＜定員＞

各回 45 名程度

＜開催日時・場所＞

第 1 回　2025 年 12 月 4 日（木）13:30～17:00　東京開催

第 2 回　2025 年 12 月 12 日（金）13:30～17:00　大阪開催

第 3 回　2026 年 1 月 29 日（木）13:30～17:00　東京開催

＜主催者・事務局＞

主催：内閣府

事務局：公益財団法人未来工学研究所

3.2　意見交換会のプログラム構成

上記のように、3 回の意見交換会はいずれも 13 時 30 分から 17 時までの開催とし、プログラムは以下のように、前半は講演、後半はグループ討議を行う構成とした。

＜プログラム＞

13:30-13:35　主催者挨拶・説明　内閣府　科学技術・イノベーション推進事務局
企画官　吉田和久

13:35-14:40　講演と質疑応答

・「研究インテグリティと研究セキュリティの確保に関する取組」
内閣府 科学技術・イノベーション推進事務局　上席政策調査員　河野祐子

・各意見交換会で以下有識者 1 名からの講演
第 1 回　「三重大学における研究インテグリティ・研究セキュリティに関する

取組」　三重大学学長補佐（危機管理担当）　研究・社会連携統括本部 准教授、知財ガバナンス部門 部門長　研究インテグリティ部門 副部門長
狩野幹人

第２回　「アカデミックフリーダムを守る研究セキュリティ–過度な自主規制を防ぐために必要な視点–」　九州大学　法務統括室 室長補佐・特任教授
佐藤弘基

第 3 回　「大学・研究機関における研究インテグリティ・研究セキュリティ確保の考え方と実効的取組」　東北大学 副理事（研究公正担当）、
金属材料研究所所長・教授　佐々木孝彦

・「研究セキュリティ・インテグリティに関する調査・分析」
公益財団法人未来工学研究所　依田達郎

14:40-16:00　グループ討議

※参加者が少人数のグループに分かれ、講演内容、研究インテグリティの取組等について意見交換。

・対話 A：話題提供を踏まえた課題の共有
講演内容を踏まえ、気になったこと（課題認識・問題意識）の共有

・対話 B：話題提供を踏まえた取組の共有
講演内容を踏まえ、研究セキュリティ・インテグリティに関するリスクに備えて、所属する機関で取り組んでいることの共有

・対話 C：今後所属組織で取組む上での解決策の検討（注）
対話 B を踏まえ、所属する機関・組織における課題等の解決策・アクションの検討

・グループ間での共有のための準備
グループの対話結果の発表のポイントを検討

16:10-16:55　グループ討議結果の情報共有と全体討議、及び講評　各回有識者

16:55-17:00　閉会挨拶　内閣府　科学技術・イノベーション推進事務局
企画官　吉田和久

注）第１・２回の意見交換会では、対話 C の討議テーマは「今後所属組織で取組む上での課題の共有」（対話 B を踏まえ、研究インテグリティ・研究セキュリティに関するリスクに備えて、所属する組織で今後取組む上での課題の共有）とした。

グループ討議は参加者が 4～7 名程度のグループに分かれ、各グループに事務局からモデレータが 1 名加わり、司会進行等を行って実施した。グループ分けは、機関種別（国立・公立・私立大学、国立研究開発法人）、研究大学であるかどうか等で分類することなく、多様な大学・研究機関がグループ討議できるように、事前に事務局で行った。

なお、グループ討論等における発言については、自由な意見交換が可能となるように、意見交換会後に、参加者は発言者の所属機関・名前を明らかにしないことをルールにして行った（チャタムハウスルール）。

3.3　意見交換会への参加状況

上記のように、意見交換会の対象者は、「大学、研究機関等における研究インテグリティ確保のための取組に関係のある業務の担当者」とし、ウェブサイトから募集した。一つの大学、研究機関からの参加者は 2 名までとし、先着順で定員に達した時点で募集を締め切った。

3 回の意見交換会のそれぞれへの参加状況は表 3-1・図 3-1（機関種別）、表 3-2・図 3-2（地域別）に示すとおりである。第 1 回は 20 人、第 2 回は 23 人、第 3 回は 42 人が参加した。東京で開催した第 1 回と第 3 回は国立研究開発法人等からの参加者がそれぞれ 6 人、16 人と比較的多く、大阪開催の第 2 回は大学関係者の参加が多かった。大学は国立大学、公立大学、私立大学のいずれの機関種別からも各回の意見交換会への参加があった。

また、地域別に見ると、第 1 回と第 3 回（東京開催）は関東から、第 2 回（大阪開催）は近畿からの参加者が多かった。全国からの参加も見られ、北海道、東北、中国、四国、九州・沖縄地方からの参加者もあった。

大学の規模別には大規模の研究大学や総合大学から、中・小規模の大学まで、さまざまな参加があった。また、参加者は、研究インテグリティ、安全保障輸出管理・利益相反等に関連する部署の職員や、担当の教員が多かった。

表 3-1　意見交換会への出席者人数：機関種別

	国立大学等	公立大学	私立大学	国立研究開発法人等	合計
第1回（東京、12月4日）	7	2	5	6	20
第2回（大阪、12月12日）	8	1	11	3	23
第3回（東京、1月29日）	13	1	13	16	42
合計	28	4	29	25	85

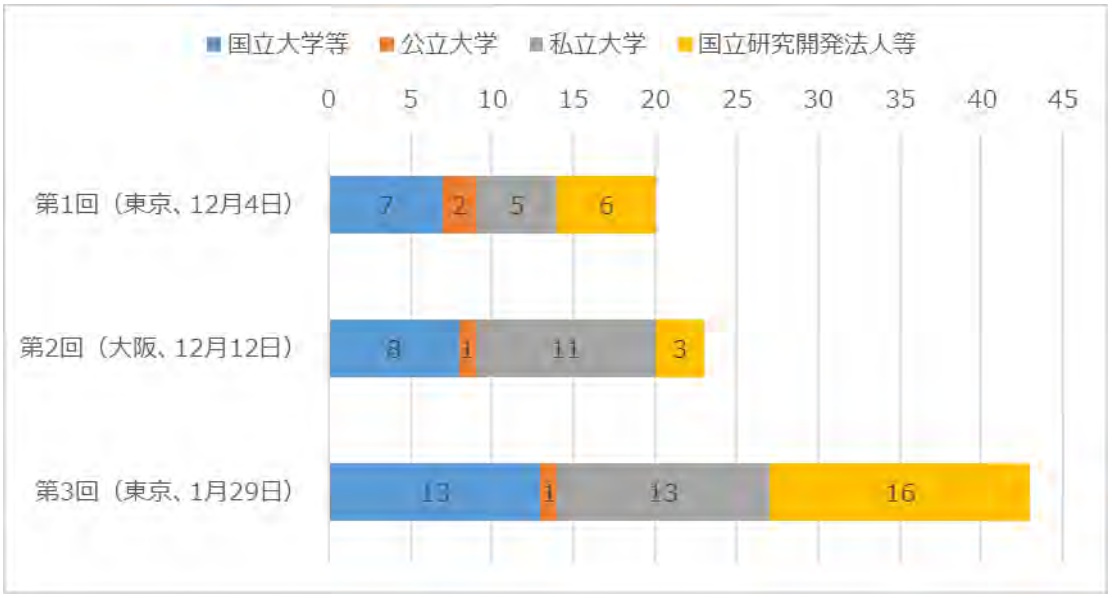


図 3-1　意見交換会への出席者人数：機関種別

表 3-2　意見交換会への出席者人数：地域別

	北海道	東北	関東	中部	近畿	中国	四国	九州・沖縄	合計
第1回（東京、12月4日）	1	1	11	3	2	1	1	0	20
第2回（大阪、12月12日）	2	0	2	3	15	1	0	0	23
第3回（東京、1月29日）	0	0	28	5	4	3	0	2	42
合計	3	1	41	11	21	5	1	2	85

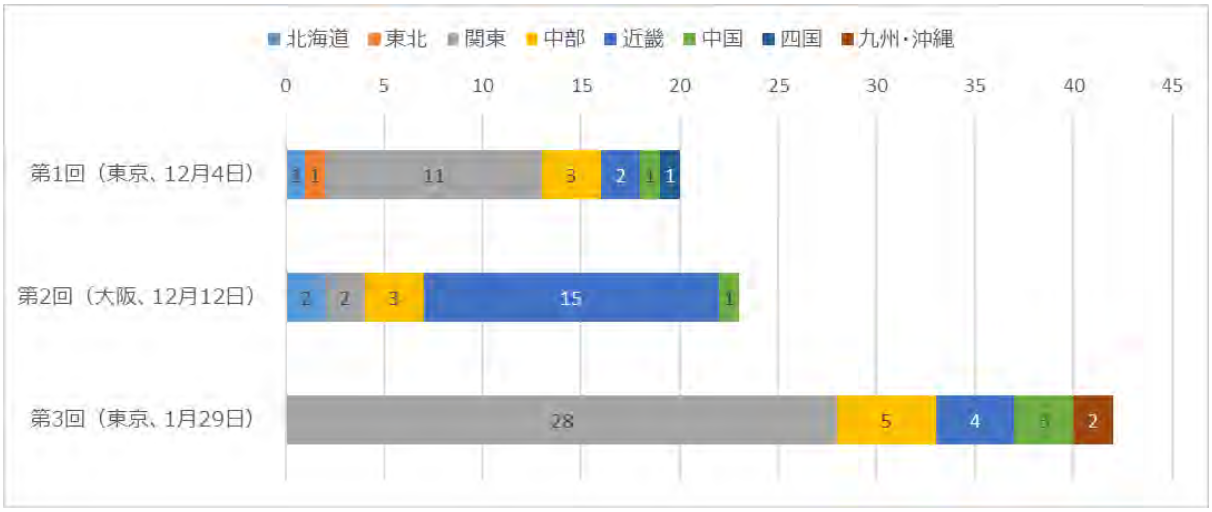


図 3-2　意見交換会への出席者人数：地域別

3.4　意見交換会についての感想・意見等

各回の意見交換会の終了後に参加者を対象に事後アンケートを行った。アンケートの設問は以下のとおりである。

1）内閣府からの講演について（参考になったかどうか（選択肢）、自由意見・コメント）、
2）有識者からの講演について（参考になったかどうか（選択肢）、自由意見・コメント）、
3）未来工学研究所からの講演について（参考になったかどうか（選択肢）、自由意見・コメント）、
4）グループ討議について（参考になったかどうか（選択肢）、自由意見・コメント）、
5）意見交換会全体について（自由意見・コメント）

各回のアンケート結果について、回答率の高かった第２回を例として以下に示した。

1）内閣府講演について

約 26%の回答は「とても参考になった」、約 74%の回答は「参考になった」だった。

コメント（抜粋）

- 各機関での人材負担やコストを軽減し、対応の公平性を確保するため、政府がデュー・ディリジェンス支援チーム（専門家派遣や教材整備）を設置することを提案する。（国立大学、大学職員）
- 研究インテグリティと研究セキュリティの違いがよく分かった。（私立大学、大学職員）
- デュー・ディリジェンスなどのリスク評価を研究者がどのようにしていけばよいのか、研究者がとても分かりやすい格好で今後の「研究セキュリティの確保に関する取組のための手順書」に示してほしい。（私立大学、大学職員）
- 現在の政府の動きや今後の動きなど知ることができた。（私立短大、大学職員）

2）有識者講演について

約 37%の回答は「とても参考になった」、約 63%の回答は「参考になった」だった。

コメント（抜粋）

- 研究セキュリティ・インテグリティに対する過剰反応、というのは新たな視点であった。（国立大学、大学職員）
- 特に、『青信号にする』ための実務を担うという点に共感した。契約条件を整えたうえで実施した場合であっても、相手方による契約違反が生じた際の対応方法については、さらなる工夫が必要であると感じている。（国立大学、大学職員）
- 「恐れ」を気にするあまり、研究活動が「委縮」してしまわないよう、相手を「理解」することが必要であるとの提言に共感した。（私立大学、大学職員）
- 実例に基づいた、わかりやすい内容であったため大変参考になった。（私立短大、大学職員）

3) 未来工学研究所講演について

約 16%の回答は「とても参考になった」、約 74%の回答は「参考になった」、約 10%の回答は「あまり参考にならなかった」だった。

コメント（抜粋）

- MIT の話は参考になったので、国内の事例とか国内で進んでいる機関の情報・取り組みなどの紹介を聞きたかった。（国立大学、大学教員）
- MIT が特定の国に対してリスクを設定している点は印象的である。（国立大学、大学職員）
- 内容が難しく、理解が追いつかなかった。先端的な理想的な大学を紹介したと理解したが、頑張れば手が届きそうな大学の事例も併せていただけると取り組む上での励みとなる。（私立大学、大学職員）
- 研究インテグリティと研究セキュリティについて、共通的土台部分と高リスク対応部分に分けて考えることが参考になった。（私立大学、大学職員）

3.4.1 グループ討議についての感想・意見等

このうち、意見交換会開催の主たる目的であったグループ討議についての質問に対するアンケート結果は表 3-3、図 3-3 のとおりである。事後アンケートの回答率は約 7 割であり[553]、参加者の意見を概ね反映しているとみられる。約 5 割の参加者は「とても参考になった」、約 9 割の参加者は「とても参考になった」「参考になった」のいずれかの選択肢を選んでおり、満足度は高かったと考えられる。

表 3-3 意見交換会の事後アンケート結果：グループ討議について

	とても参考になった	参考になった	あまり参考にならなかった	参考にならなかった	分からない	合計
第1回（東京、12月4日）	7	4	1	0	1	13
第2回（大阪、12月12日）	9	7	2	0	0	18
第3回（東京、1月29日）	13	14	3	0	0	30
合計	29	25	6	0	1	61

[553] 事後アンケートの回答率は、第 1 回 65%、第 2 回 78%、第 3 回 71%で、合計では 72%だった。

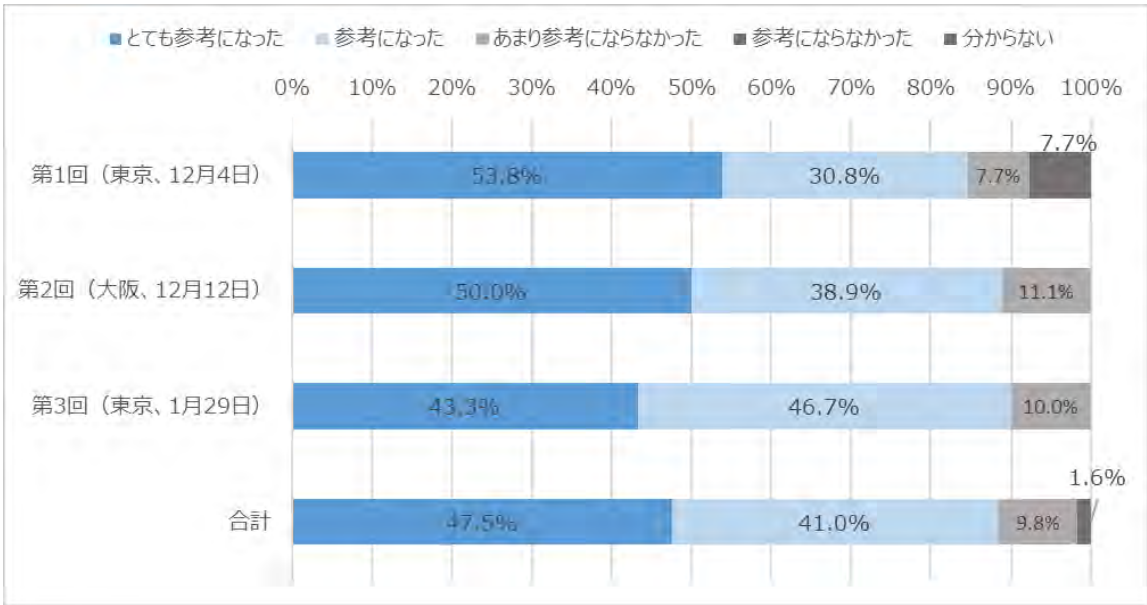


図 3-3　意見交換会の事後アンケート結果：グループ討議について

グループ討議についての自由記入の意見では、第一に、各機関が研究セキュリティ・研究インテグリティに関する取組を進める上で抱えている課題や悩みが、機関間で広く共通していることが確認できたとの指摘があった。自機関だけでは把握しづらい他機関の実務上の工夫や悩みを知ることができ、参考になった、学びが大きかった、という評価が多数を占めた。また、明確な取組内容が十分に示されないと感じられる状況や、各組織が不安を抱えながら個別に対応を進めている実態、担当者の理解度・関与度、取組の成熟度に大きな差が存在することが、討議を通じて可視化されたとの指摘が複数みられた。特に、想定以上に他機関でも同様の悩みを抱えていることを認識できたことにより、担当者としての孤独感が軽減された、現場が資金不足・人手不足の中で奮闘している様子に勇気づけられた、といった心理的効果を含むネットワーキング面での効用も報告されている。

一方で、得られた情報の具体性や実務への転用可能性という観点では、一定の限界も指摘された。特に組織規模やセクター（大学・研究開発法人等）が大きく異なる参加者同士では、制度・体制の前提の違いが大きくなっており、取組にも濃淡が生じているとのコメントがあった。討議の中でベンチマークとなるような具体的な情報や、すぐに導入可能な参考事例を十分に得られなかったという声もあり、より細かい議論を行うには、取組の深さに応じた議論が可能となるような工夫も必要であることが示された。

運営面では、討議時間の不足を指摘する意見が複数あり、論点の深掘りや具体策の検討に十分な時間を確保しにくかった可能性がうかがえる。さらに、付箋紙と模造紙を用いた KJ 法的な運用については、手法自体は否定されないものの、効率性や、後日の共有や分析への活用といった面で改善要望が挙げられている。

参加者グループ構成に関しては、異なるセクターや組織間の取組の違いや担当者の負担の大きさが実感として共有されたとの声があった。また、成熟度に応じたレベル分け、同セクターと異セクターが適度に混在するグルーピング、あるいは共通課題意識を持つ参加者

で編成することで連携を強める、といった編成上の工夫が提案されている。

議論の中では、国による支援の重要性があらためて認識されたとの指摘や、リスクマネジメントにおける判断の難しさ、人材不足等の課題が示された。また、それらの課題に対し、小規模大学等に対する共通ツールの提供、地域コンソーシアム等の枠組みを活用、人材不足の課題に対しインセンティブとしての資格の設置などの解決策の提案があった。

以下は意見の例である。

・とてもいいネットワーキング・意見交換の場となった。（国立研究開発法人、研究機関の職員）
・他機関の実務担当者と課題や解決案等を協議・共有できたことはとても参考になった。思った以上に他機関でも自機関と同じ悩みを抱えていることを知り、孤独感が薄れた。（独立行政法人、研究機関の職員）
・他大学・研究機関の事情や抱える悩みを共有し、同じ悩みを抱えていたり、こういう方法で解決・対応しているという対応例を知ることができ、非常に参考になった。（国立大学、大学職員）
・専門人材の少なさや研修内容等、各組織で困っていることを知ることができた。今回得られた気付き（利益相反の自己申告書や研究資料の改訂など）を、できるところから改善していきたい。（国立研究開発法人、研究機関の研究者）
・明確な取組方針が明示されていない中で各組織がそれぞれに取組を不安を持ちながら進めていることが理解できた。（国立大学、大学職員）
・様々な組織が参加していたため、組織間での温度差や担当されている職員の苦労がよく分かった。「国益」を守ることが目的であるならば、あらためて国による支援が重要と思った。（国立大学、大学職員）
・「全国大学コンソーシアム研究交流フォーラム」や各地域にある大学コンソーシアムの部会といった枠組みを活用して連携させて地元の大規模大学である国立大学にすべての負担がいかぬようにできないか。（私立大学、大学職員）
・実務担当者向けセミナーということだったが、実際に実務に取り組んでいる人でも取り組み方に濃淡があり、細かな点まで議論するのは難しかった。深く実務に取り組んでいたとしても、話せる範囲に限界があり、抽象的な話になってしまうこともあるのではないか。（国立研究開発法人、研究機関職員）
・もう少し議論する時間が欲しかった。（私立大学、大学職員）
・討議時間がやや不足しているように感じた。また、取り組み状況には機関間で差があることも見受けられたので、今後、レベル分け等を検討したらどうか。（大学共同利用機関法人、研究機関の職員）

3.4.2　意見交換会全体についての感想・意見等

図 3-3 について説明したように、参加者は概して、意見交換会は、啓発的で有益な会合であったと感じている。本意見交換会の事後アンケート自由記述からは、第一に、研究インテ

グリティ・研究セキュリティに関する意見交換の機会が継続的に設けられていること自体への評価が多く示された。特に、他機関の取組状況や悩みを共有し、現場の感覚や判断の背景を相互に理解できる点が有益であり、今後も同様の場への参加を希望する声が複数確認された。また、対面で議論することにより、教材や資料だけでは得にくい「人がどのように考え、どのように行動しているか」といった実務上の知見が得られるとの指摘もあり、ネットワーキングと相互学習の場としての価値が再認識された。地理的観点からは、東京開催のみでは参加機会が限定される可能性があるため、地方でも今後も開催してほしいという要望が挙がった。

第二に、研究セキュリティ・インテグリティの理解・浸透を進める上での課題として、重要性は理解しているが、具体的にどう取り組むべきかが難しい、定義や全体像が十分に腑に落ちていないといった声がみられた。このため、現場の研究者・実務担当者が理解しやすい資料や、各機関が体制整備を進める上で参考となる具体的事例の提示を求める意見が複数挙がった。特に、専門家が十分でない組織においては、リスク判断に必要な情報の収集、収集情報の評価、意思決定に至るプロセスの設計が難題であるとの声があった。

第三に、国による支援の必要性を指摘する意見もみられた。たとえば物理的セキュリティ（入退室管理等）は研究セキュリティ確保の前提であるにもかかわらず脆弱な施設が多い可能性があること、特定の枠組みに限らず公的資金による研究一般に対して研究セキュリティ確保が望ましいとされるのであれば、国が新たな取組を求める際に継続的な予算措置を伴わなければ実効性を欠く、といった問題提起がなされた。また、地政学的変化に応じて研究セキュリティの論点が変動することを踏まえ、節目での開催により中央の方針を理解しやすくしてほしいという意見もあった。

以下は意見の例である。

・このような場を設けていただくのは非常にありがたいし、必要であると思う。継続した取り組みを期待する。（国立大学、大学職員）
・現場の研究者が理解しやすい資料があると、もっと浸透すると思う。（国立大学、大学職員）
・研究インテグリティに関し、委員会を立ち上げたもののまだまだ体制整備が不完全な部分もあると感じている。それ以上にリスクへの対応が一番頭を悩ませる問題である。リスク判断は、組織として判断するのが最終的な方法である一方で、専門家不在の自組織では、判断材料の収集、収集した材料を基にどう判断するかがとても難しい。今回の意見交換会において、同じ悩みを持つ機関や先行されている機関の事例などを伺うことができ大変ためになった。今後もこうした機会を活用していきたい。（国立大学、大学職員）
・最近似たような勉強会（意見交換会）が多い。今回は参加者の事前の理解度が広いことを想定しての会であったと理解するが、今後は参加対象者を多少絞った議論の場があっても良いのかなと思った。（国立大学、大学職員）
・研究インテグリティ、研究セキュリティの重要性は理解しているが、どのように取り組むべきなのか具体的な内容の理解が難しい。各々の機関に適した体制を整えやすくな

るようにより具体的な事例紹介等の機会があればありがたい。機関の規模や研究分野によっても取り組みの内容は変わってくると思うので、機関規模別、研究分野別の情報交換の機会等があればよいのではないか。（私立大学、大学職員）

・研究インテグリティと研究セキュリティの定義が、自分も含めてきちんと理解できていないのではないかと感じた。この部分の図解などがあるとなお良いと思う。（私立大学、大学職員）

・関西在住のため、意見交換会が東京でのみ開催された場合は他機関の運用を知ることができる貴重な機会に参加できなかった。今後も大阪でも開催いただけると有難い。（独立行政法人、研究機関の職員）

・地政学的な変化で研究セキュリティが変化するので、そのタイミングで今回のようなセミナーの開催があれば政府方針が理解しやすいと思った。（国立大学、大学教員）

・グループ討議で大学と研究機関をまとめること、大学でも国立と私立をまとめるのは現実的でないように感じた。自律的な取り組みの実施率に国立と私立で差があるのにも理由がある。それぞれの属性の特徴に配慮して、取り組みやすい枠組としてほしい。（私立大学、大学職員）

・対面でやることの意義を改めて感じた。教材を見れば知識は得られるが、人間がどのように考えどのように行動していくかを知ることが、現場対応型の管理を進める中で、大変有用であることを再認識した。（国立研究開発法人、研究者の研究管理職員）

3.5　意見交換会グループ討議の概要

本セクションでは、内閣府や有識者からの講演を踏まえ、大学・研究機関の現場がどのような課題認識を持ち、どのような体制整備や実務対応を進めているかを、意見交換会でのグループ討議結果を整理し、紹介する。

意見交換会には、計 62 機関（国立大学等〔大学共同利用機関法人を含む〕20、公立大学 4、私立大学 23、国立研究開発法人等〔独立行政法人を含む〕15）が参加しており、大学・研究機関の種別をまたぐ多様な実務担当者の声を把握することができた。他方で、本意見交換会への参加機関は任意参加を前提とするものであり、日本の大学・研究機関全体を統計的に代表するものではない。このため、以下では、全国的な実態の「推計」ではなく、制度導入・運用の現場で共有されている論点（体制整備、人材・専門性、リスク判断、研究者への周知・研修、国際共同研究対応等）を把握するための質的な知見として位置づけて記述する。

3.5.1　研究インテグリティと研究セキュリティの確保についての課題認識

対話 A において、第 1～3 回の意見交換会を通じて、共通して認識されたのは、研究インテグリティと研究セキュリティの定義・対象範囲・位置づけを理解するのが難しいとの課題であった。現場では、省庁・機関・担当者によって説明の仕方が異なり、研究者に対して「何を守るための取組か」「なぜ必要なのか」を十分に言語化できていないとの認識が示された。

次に挙げられたのは、リスク評価・判断基準が不足しているという課題である。エンティ

ティ・リスト等の参考情報はあるものの、実務担当者が個別案件において「どこからをリスクとして対応すべきか」「どの条件なら進めてよいか」を判断するための具体的基準が不足しており、結果として「念のため止める」「安全側に倒れる」といった過度に慎重な運用に陥りやすい構造が共有された。特に第 2 回では、単に「止める」判断ではなく、研究活動を萎縮させないための“青信号化”（条件整理により進める判断設計）の必要性が認識された。

加えて、人員・専門性・継続性の不足は、全回を通じてボトルネックとして認識された。多くの大学・研究機関では専任部署や専任者が十分に置かれておらず、兼務・少人数体制で対応している実態が共有された。とりわけ小規模機関では、制度・方針を整備しても運用まで手が回らないという声が多かった。また、担当者の異動・短期交代により、判断ノウハウや案件対応の知見が属人的に失われることへの懸念も強く、標準化・ナレッジ継承の必要性が広く認識されている。

さらに、組織体制・ガバナンス設計の難しさも指摘された。中央集権型（委員会中心）と部局分散型（拠点責任型）のいずれにも課題があり、どのような体制が自組織に適切かが見えにくいという問題意識が共有された。実際には、輸出管理、契約、研究支援、国際、IT・サイバー、利益相反管理等の関連機能が縦割りで分散しており、研究インテグリティ／研究セキュリティの担当部署を設けても、横断的な情報共有・連携がなければ実効性を確保しにくいという認識が強かった。

このほか、研修・浸透の難しさも重要な課題として挙げられた。現場では講習会や e-learning を実施していても、研究者にとって「自分ごと」として理解されにくく、分野差（理系・文系・医療系等）や立場差（研究者・事務・理事層）により受け止め方が異なることが課題とされた。学生についても、大学院生は一定程度対象化されつつある一方、学部生や共同研究に関与する学生の位置づけが曖昧であり、法的責任の範囲と実務上の管理の必要性の間にギャップがあることが議論された。

第 3 回意見交換会では、デュー・ディリジェンス（DD）の「深度」や手順書・チェックリストの運用負担についての課題の指摘があった。すなわち、「何をどこまで調べるべきか」「自己申告にどこまで依拠してよいか」「誰がどの価値観で最終判断するのか」が曖昧なまま、制度や対象範囲だけが拡大すると、現場の負担が増大するのではないかということである。特定研究開発課題・プログラム等への指定時には、急激な対応要求が発生し得ることも、実務上の課題として示された。

3.5.2　研究インテグリティと研究セキュリティの確保のための取組内容

対話 B において、各グループから共有された取組内容としては、まず規程・体制整備の着手・進展が広く確認された。多くの機関で、研究インテグリティ関連規程の整備、相談窓口・事務局の設置、連絡会・委員会・ワーキンググループの設置など、基礎的な体制構築が進められている。研究インテグリティ・マネジメント委員会や WG を通じて、個別案件の検討や情報共有を行う枠組みを設けている例も複数示された。

また、研修・啓発の実施はほぼすべての機関で共通する取組である。具体的には、説明会、e-learning、年複数回のセミナー、学内ホームページでの情報発信などが実施されており、

研究公正研修の既存枠組みに研究インテグリティ／研究セキュリティの内容を取り込む動きも見られた。また、教育・研修においては単なる制度説明にとどまらない継続的啓発の必要性が共有された。

実務面では、チェックリスト・申告書・自己申告ベースの運用が現時点の主流であることが示された。共同研究、兼業、出張、外部資金、契約等に関連して、チェックリストや申告書を用いた確認プロセスを整備し、必要に応じて個別相談・個別案件対応を行う事例が紹介された。利益相反管理、研究倫理審査、モニタリング、自己点検等の既存制度と組み合わせながら運用している機関も多かった。

さらに、情報収集と外部情報の活用も重要な取組として挙げられた。各大学・研究機関は、内閣府・文部科学省の会議や研修、有識者会議、関連セミナー等から情報を収集し、自機関にフィードバックしている。加えて、国内外の研究セキュリティ・インテグリティに関する情報を継続的に収集し、機微技術情報の特定や、学内向け資料作成に活用している機関の事例も紹介された。

研修資料に関しては、研究者向けに具体的なリスク場面を可視化する工夫が報告された。例えば、リスク場面をポンチ絵やナラティブ形式で示し、レピュテーションリスクなど抽象的表現にまとめず、技術流出、人材流出、不当な外国からの干渉・影響、サプライチェーンリスク等に分解して説明する取組は、研究者の理解を促進する実践例として共有された。

ツール・システム面では、外部ツールの導入・活用も一定程度進み始めている。従来利用していた大学・機関情報確認ツールの有料化により簡便なチェック手段が失われたという課題が共有された一方、外部ツールを導入し、比較的安価かつ円滑に運用できている事例が紹介された。また、AI 活用への関心が高まる一方で、具体的な使い方については課題として残る状況が共有された。

組織運用の工夫としては、関連部署間の連携・情報集約の試みが挙げられる。兼業情報、出張情報、外部資金情報など、部署横断で分散する情報を一元的に扱う必要性が強く認識され、情報共有・集約の仕組みづくりに着手している機関もみられた。統合 DB やワークフロー整備の必要性、情報の一元管理の重要性について議論された。

学生・研究者への対応に関する個別運用として、学生への誓約書取得、特定場面での説明・確認強化、共同研究参加時の管理強化などの対応例が共有された。特定研究開発課題等における学生参画の扱いや、研究者・技術職員に当事者意識を持ってもらうための働きかけが実務上の重点として議論された。

外部連携の面では、大学間・地域間ネットワークや外部相談先の活用も取組として現れ始めている。地域の国立大学による小規模大学向け相談窓口構想の共有、地域単位の支援体制への期待、他大学の対応事例を相互参照したいという声があった。

総じて、現時点での取組は、規程・体制・研修・情報収集・個別案件対応・一部ツール活用を中心に進展している一方、なお基礎整備から実効運用への移行期にあり、機関間で成熟度の差が大きいという状況が読み取れた。

3.5.3　今後の取組・解決策の方向性についての認識

対話Ａ・Ｂにおける課題認識・現在の取組の意見交換を踏まえた上で、対話Ｃにおいて、今後の取組・解決策の方向性について討議された。まず、組織横断型の実効的ガバナンスの構築が挙げられた。委員会の設置それ自体よりも、実務層が機能する横断体制、すなわち研究支援・契約・国際・輸出管理・IT/サイバー・法務等をつなぐ運用体制が重要との認識が強かった。また、上位者中心の形式的委員会ではなく、現場で案件を扱える実務委員会や相談・予防対応の窓口を整備する必要性が提案された。学長直下等の強い位置づけも議論に上った。

人材の育成と継続性確保が、今後の重要課題として議論された。ツールやAIの活用余地は大きいものの、最終的に判断を下すのは人であり、デュー・ディリジェンスやリスク評価を実施できる専門性を持った人材が不足しているという認識は共通していた。研修プログラムの充実に加え、担当者のキャリア形成に資する資格制度・公的認証のようなインセンティブ設計、異動・退職を前提としたナレッジ継承の仕組み（判断ログ、事例蓄積、標準手順、引継ぎ資料等）の整備が提案された。

運用面では、判断事例・好事例の蓄積と共有が有効な解決策として提案された。相談案件の判断を逐次記録し、後から参照可能にするログ化の提案が出され、単なるヒヤリハット共有だけでなく、情報収集・判断・対処の一連のプロセスがうまく機能した好事例の共有が相互学習に資するとの認識が示された。

また、現場では、判断基準が曖昧なために念のため止める運用に寄りやすいが、研究セキュリティ確保のための取組の本来の目的は研究活動を不必要に萎縮させることではない、という認識が共有された。そのため、何がリスクかを一律に否定的に扱うのではなく、ケース別に条件を整理し、実施可能な形に落とし込む“青信号化”の設計が必要である、という認識が共有された。

この前提として、定義・基準・参照枠の明確化が重要との参加者の声があった。具体的には、研究インテグリティ／研究セキュリティの概念整理（両者の関係、輸出管理との関係、対象範囲の違い）を明確化し、研究者にも説明可能な言葉で示すこと、さらに、どの場面で何を確認し、どの条件なら可／不可／要追加確認となるかを示すQ&A、ケース集、判断基準、行動規範（Code of Conduct）的な共通参照枠を整備することが必要との認識があった。

また、研修・啓発の再設計（ユーザビリティ重視）も今後の方向性として示された。従来の研究公正研修が形骸化しやすいとの指摘を踏まえ、研究インテグリティ／研究セキュリティの定義、考え方、具体的なテクニック、場面別リスク、相談先、判断の流れなどを組み込んだ、より実務に即した研修が必要との指摘があった。加えて、研究者・技術職員・学生・事務・理事層など対象別にメッセージを変えること、研究者側の協力者（研究者リーダー）を巻き込んで浸透させること、研究室・大学院生まで情報が届く仕組みを作ることが重要と認識された。

機関間連携については、大学間・地域間ネットワークの整備と外部支援機能の構築が、特に小規模機関支援の観点から重要だと認識された。各機関が単独でツールや専門人材を抱えることには限界があるため、地域の中核大学をハブとした相談窓口、外部のコンサル的支

援組織、率直な情報交換が可能な人的ネットワークの形成が有効とされた。

最後に、国による支援強化への期待として、共通のリスク確認ツール、分かりやすいQ&A・ケース集、国際的にも説明可能な判断基準、政府方針の継続的な情報提供に加え、特定研究開発プログラム等で対応要件が増す場合に備えた予算措置が必要との認識が多く示された。研究セキュリティは個別機関の課題にとどまらず、国益・国家安全保障にも関わるとの見方から、国家レベルでの支援（予算・標準ツール・人材育成枠組み）を求める声が多かった。

第4章　Ｇ７オンラインプラットフォーム「バーチャルアカデミー」の運営支援・分析

4.1　G7 バーチャルアカデミーの運営概要

「G7 Virtual Academy on Research Security and Integrity（以下、G7 バーチャルアカデミー）」は、G7 科学技術大臣会合の枠組みで設置された会員制のウェブサイトであり、G7 各国等の研究関係者が、研究セキュリティと研究インテグリティに関する実務情報を共有・参照するためのオンラインプラットフォームである[554,555]。

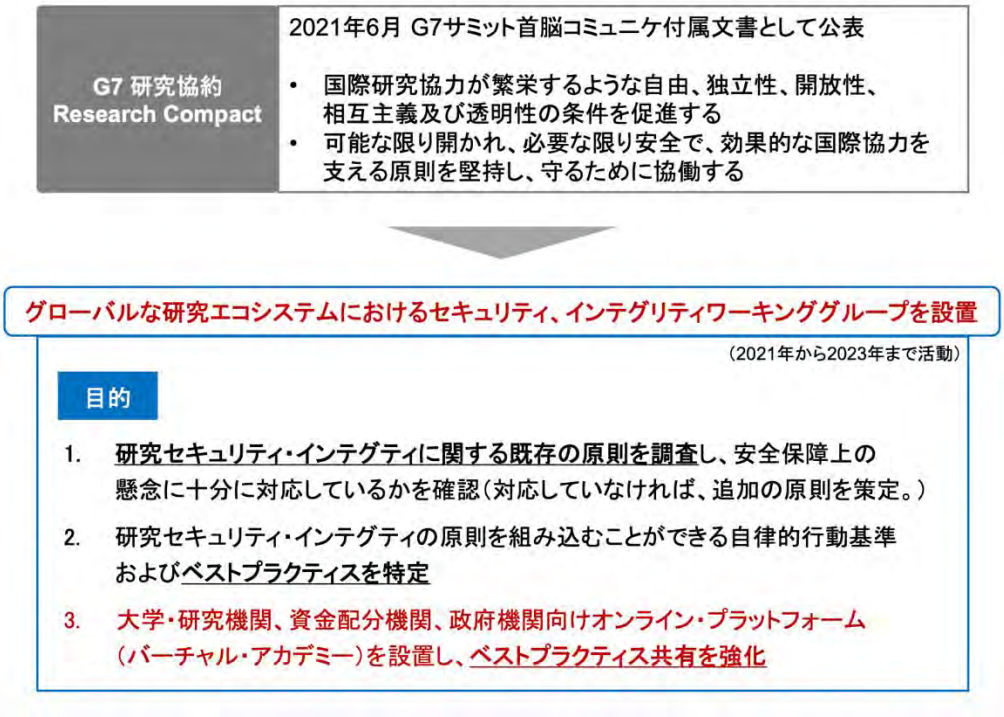


図 4-1　G7 バーチャルアカデミーの設置経緯

出典：内閣府科学技術・イノベーション推進事務局「G7 バーチャルアカデミー登録方法説明会」資料, 2025 年 11 月 5 日.

G7 バーチャルアカデミーは、「G7 グローバルな研究エコシステムにおけるセキュリティとインテグリティ（SIGRE）WG」の直下に、バーチャルアカデミーとツールキットに関す

554 G7 Virtual Academy: Research Security & Integrity (https://europa.eu/sinapse/sinapse/community/0505f60a-287b-11ed-b6d0-0050568bf5be/login)

555 G7 バーチャルアカデミーの目的は、研究エコシステムのセキュリティとインテグリティに関連する課題について、G7 やその他の国の研究コミュニティの間で認識を高め、研究関係者（政府、研究資金提供者、研究機関、研究者）が、それぞれの観点から、研究セキュリティ・インテグリティに関する共通の理解とより深い知識を発展させ、自信を持って国際協力を継続できるよう支援するものである。また、地域および/または世界的な研究エコシステムのセキュリティとインテグリティを保護するため、不正行為の共通のリスクと形態、バランスのとれた適切な措置について、研究関係者間の情報共有を促進することにある。（内閣府「G7 バーチャルアカデミー登録方法説明会」資料より）

るサブ作業部会が設置された（英国、イタリアが議長）。バーチャルアカデミーの設計・開発のため、国内有識者、ステークホルダーとのワークショップを実施し、バーチャルアカデミーとツールキットのコンセプト計画が合意され、「バーチャルアカデミー管理委員会」が設立され、2023 年 5 月が利用開始した[556]。

G7 バーチャルアカデミーは、ⅰ）ディスカッションとサーベイ、ⅱ）文書ライブラリー、ⅲ）リンクライブラリ、ⅳ）カレンダー、ⅴ）掲示板、ⅵ）ツールキット、ⅶ）ケーススタディ、ⅷ）メッセージの送信からなる[557]。文書ライブラリーについては、政府機関、大学・研究機関等が自身のコンテンツを掲載できるため、本業務では、日本側のコンテンツのアップロードの手順についても整備した（後述）。

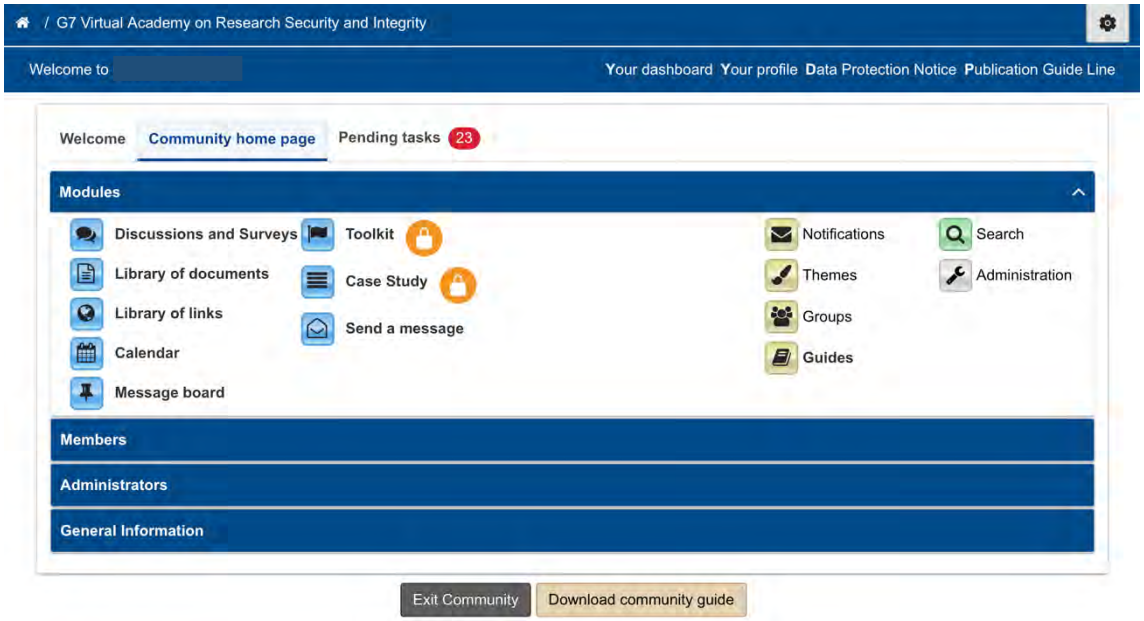


図 4-2　G7 バーチャルアカデミーの機能

出典：G7 バーチャルアカデミーのログイン後の画面例（2026 年 2 月 20 日現在）

本業務では、2024 年度に開始した「G7 バーチャルアカデミー」の日本側の運営業務として、2024 年度の登録ユーザーに対する登録継続意向の確認調査を行うとともに、2025 年度の新規登録機関の窓口担当者およびユーザーの募集と認証業務を行った（図 4-3）。

まず、2024 年度の登録機関の窓口担当者、ユーザー等の登録者を対象に、Web アンケートフォームで継続確認調査を実施した。同時に 2024 年度ユーザー登録者のうち「G7 バーチャルアカデミー」のプラットフォームである SINAPSE[558]の未登録者（G7 バーチャルア

[556] 内閣府科学技術・イノベーション推進事務局「G7 バーチャルアカデミー登録方法説明会」資料, 2025 年 11 月 5 日.

[557] G7 バーチャルアカデミーの機能のうち、ツールキット、ケーススタディについては、メンバーによりアクセス制限がある。（2026 年 2 月 20 日現在）

[558] SINAPSE（Scientific INformAtion for Policy Support in Europe）とは、欧州委員会が運営する政策形成のための知見共有プラットフォームである。科学コミュニティの知見と EU の政策担当者や関連ステークホルダーをつなぎ、政策立案・ガバナンスで専門知をより良く使うためのウェブ型のコミュニケーション基盤である。G7 バーチャルアカデミーは、SINAPSE 上に設けられたコミュニティ領域でホストさ

カデミーの承認プロセスに至っていない者)、2025 年度の新規ユーザー登録者に向けて、2025 年度の「SINAPSE 登録−G7 バーチャルアカデミー」の登録マニュアルの更新を実施した。その後、継続確認調査（機関窓口担当者）や 2025 年度新規窓口登録を希望する機関を対象に、「G7 バーチャルアカデミー」登録説明会を開催した。2025 年度の G7 バーチャルアカデミーの日本側の登録業務は、登録説明会を持って開始し、機関の窓口担当者の登録は 2026 年 1 月末まで登録を実施した（ユーザー登録は 2 月 13 日まで)。説明会後に 2024 年度登録継続意向のユーザーのうち、SINAPSE 未登録者と 2025 年度新規ユーザー登録者を対象に、登録マニュアル一式を送付し、「G7 バーチャルアカデミー」のバリデーション業務を実施した。

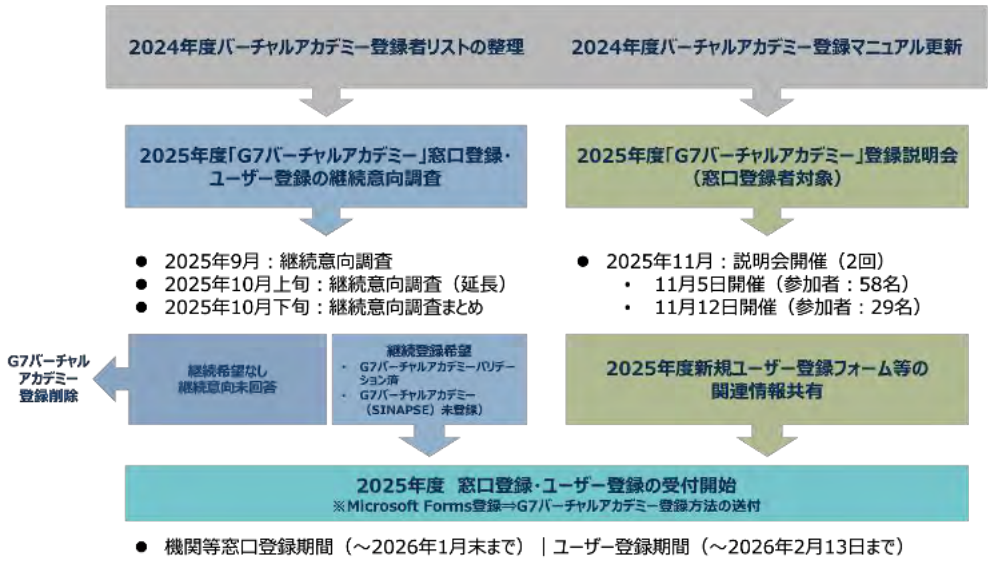


図 4-3 「G7 バーチャルアカデミー」日本側の運営手順

出典：未来工学研究所作成.

4.2 継続意向調査

4.2.1 調査概要

本業務では、前述のとおり、2024 年度ユーザー登録者を対象に、2025 年度ユーザー登録の継続意向に関する調査を実施した。2024 年度のユーザー登録者の状況は、SINAPSE−G7 バーチャルアカデミーの登録済が 64 名、未登録者が 71 名であった。

継続意向調査は、Web アンケートフォーム（Microsoft Forms）を活用し、「2024 年度ユーザー登録者」、「2024 年度窓口登録担当者」のそれぞれを対象に実施した。

《実施時期：ユーザー登録者、窓口登録者》

- 調査実施期間：2025 年 9 月 18 日から 9 月 30 日（一次締切）

れている。G7 バーチャルアカデミーの日本側の運営では、運営事務局の登録（機関窓口担当者、ユーザー登録者）⇒SINAPSE 登録⇒G7 バーチャルアカデミーの登録申請⇒日本側運営事務局によるバリデーション（登録情報の検証・承認）を実施している。(https://europa.eu/sinapse/sinapse/)

2025 年 10 月 1 日から 10 月 6 日（二次締切）

質問票は、ⅰ）「G7 バーチャルアカデミー」の 2025 年度の継続登録の可否や登録の確認に係る質問、ⅱ）登録を継続する方への質問（登録者の氏名、所属機関・部署、連絡先情報）、ⅲ）今年度登録を継続しない方に対する後任者に係る質問を調査した。

表 4-1　継続意向調査の質問票（2024 年度ユーザー登録者用）

Ⅰ）研究インテグリティ「G7 バーチャルアカデミー」の 2025 年度の継続登録についてお伺いします	1. あなたの氏名（日本語）を入力してください。 2. 昨年度「G7 バーチャルアカデミー」に登録したメールアドレスを入力してください。 3. 今年度（2025 年度）も、引き続き、研究インテグリティ「G7 バーチャルアカデミー」の国内登録を継続しますか。（登録を継続する／登録を継続しない） 4. 所属機関の G7 バーチャルアカデミーの窓口メールアドレスを入力してください。※ご所属情報について、機関の窓口に照会させていただくことがありますので、正確に入力するようお願いいたします。※機関の窓口が不明である場合、機関内でお問合せください。
Ⅱ）登録を継続する方に伺います【登録情報の変更のある方】	5. 【登録ユーザー情報の変更等】あなたの氏名（日本語）を入力してください。 6. 【登録ユーザー情報の変更等】あなたの氏名（ローマ字）を入力してください。 7. 【登録ユーザー情報の変更等】所属機関を入力してください。 8. 【登録ユーザー情報の変更等】所属部署を入力してください。 9. 【登録ユーザー情報の変更等】役職を入力してください。 10. 【登録ユーザー情報の変更等】連絡先（E-mail）を入力してください。
Ⅲ）「今年度登録しない」と回答された方に伺います　【後任者の連絡】	11. 「今年度登録しない」と回答された方に伺います。後任の方がいる場合、後任の方の氏名をお知らせください。 12. 上記で記載された方の連絡先（E-mail）をお知らせください。

表 4-2　継続意向調査の質問票（2024 年度機関の窓口登録者用）

<table>
<tr><td colspan="2"> 
</td></tr>
<tr><td>Ⅰ）研究インテグリティ「G7 バーチャルアカデミー」の 2025 年度の継続登録についてお伺いします</td><td>1. あなたの氏名（日本語）を入力してください。
2. 昨年度「G7 バーチャルアカデミー」の窓口メールアドレスを入力してください。
3. 今年度（2025 年度）も、引き続き、研究インテグリティ「G7 バーチャルアカデミー」の機関窓口担当者として継続しますか。※「登録は継続しない」と回答された機関のうち、「G7 バーチャルアカデミー」のユーザー登録者がいる場合、機関の窓口担当者の登録を別途お願いすることになります
（登録を継続する／登録を継続しない→後任の方のご紹介）</td></tr>
<tr><td>Ⅱ）登録を継続する方に伺います
【登録情報の変更のある方】</td><td>4. 【窓口登録者の情報の変更】所属機関の G7 バーチャルアカデミーの窓口メールアドレスを入力してください。※窓口メールアドレスは、登録ユーザーの確認等の照会をさせていただくことがあります。(E-mail の入力)
5. 【窓口登録者の情報の変更】あなたの氏名（日本語）を入力してください。
6. 【窓口登録者の情報の変更】あなたの氏名（ローマ字）を入力してください。
7. 【窓口登録者の情報の変更】所属機関を入力してください。
8. 【窓口登録者の情報の変更】所属部署を入力してください。
9. 【窓口登録者の情報の変更】役職を入力してください。
10. 【窓口登録者の情報の変更】電話番号を入力してください。</td></tr>
<tr><td>Ⅲ）「今年度登録しない」と回答された方に伺います
【後任者の連絡】</td><td>11. 「今年度登録しない」と回答された方に伺います。後任の方がいる場合、後任の方の氏名をお知らせください。
12. 上記で記載された方の連絡先（E-mail）をお知らせください。</td></tr>
</table>

4.2.2　調査結果

（1）機関窓口の継続意向

機関の窓口登録の継続意向調査では、2024 年度の 59 の登録機関のうち、登録継続意向の機関が 36 機関、登録非継続意向の機関が 9 機関であった。この 9 機関のうち、ユーザー登録者がいる機関が 7 機関である（無回答の窓口登録機関のうち、11 機関も同様にユーザー登録者がいる機関であった)。これらの機関は、ユーザー登録者がいるため、窓口登録は継続となる。

表 4-3　機関の窓口登録の継続意向調査結果

機関種別	登録継続	登録非継続	無回答	総計
国公立大学	17	4	4	25
私立大学	11		8	19
大学共同利用機関		1		1
研究開発法人	8	4	2	14
総計	36	9	14	59

表 4-4　機関の窓口登録の継続意向調査結果（ユーザー登録者の有無）

登録機関ユーザーの状況	登録継続	登録非継続	無回答	総計
ユーザー登録者がいる機関	29	7	11	47
ユーザー登録者がいない機関	7	2	3	12
総計	36	9	14	59

（2）登録ユーザーの継続意向

2024 年度の G7 バーチャルアカデミーの登録ユーザーの継続意向については、登録者 135 名のうち、82 名が登録継続の意向であり、全体の 60.2%を占める。登録非継続者は 13 名であり、全体の 9.6%に留まる。また、ユーザー登録の継続意向者（82 名）のうち、「SINAPSE−G7 バーチャルアカデミー」の登録済とする者は 47 名（登録継続者の 73%を占める）である一方、登録非継続とする者は 6 名、無回答者は 11 名に留まる。「SINAPSE−G7 バーチャルアカデミー」の登録済のユーザーの方が登録継続の意向が強い（登録継続者の割合が 73%）。他方、「SINAPSE−G7 バーチャルアカデミー」未登録のユーザーのうち、登録継続意向の者は 35 名であり、全体の 49%に留まり、無回答の割合が 41%を占める。このように「G7 バーチャルアカデミー」の登録継続の意向は、「SINAPSE−G7 バーチャルアカデミー」登録済のユーザー集団の方が登録継続の意向が高い。

表 4-5　2024 年度ユーザー登録者の継続意向状況および登録者の認証状況

ユーザー登録者	登録継続	登録非継続	無回答	総計
全体	82(60.7%)	13(9.6%)	40(29.6%)	135(100%)
SINAPSE／G7VA 登録済	47(73.4%)	6(9.4%)	11(17.2%)	64(100%)
SINAPSE／G7VA 未登録	35(49.3%)	7(9.9%)	29(40.8%)	71(100%)

4.3　説明会の実施

「G7 バーチャルアカデミー」登録説明会は、2025 年 11 月に 2 回にわけて開催した。説明会では、ⅰ）G7 における研究セキュリティ・インテグリティの議論の経緯、ⅱ）G7 バーチャルアカデミーの説明、ⅲ）「バーチャルアカデミー」への登録方法、ⅳ）「バーチャルアカデミー」における文書等の公開方法について、内閣府より説明を行った。「バーチャルアカデミー」の登録方法は、①大学・研究機関等の窓口登録、②国内でのユーザー登録手続

き、③ユーザー自身によるサインアップの流れを説明し、国内の登録手続き後、ユーザー登録を希望するものは自ら EU ログインを取得し、SINAPSE との紐づけ、G7 バーチャルアカデミーの登録申請を行うことを示した。国内でのユーザー登録手続きは、機関窓口の担当者、ユーザー登録者のどちらが実施しても良いとした。

図 4-4　「バーチャルアカデミー」への登録方法（大きな流れ）

出典：内閣府科学技術・イノベーション推進事務局「G7 バーチャルアカデミー登録方法説明会」資料, 2025 年 11 月 5 日.

また、「バーチャルアカデミー」のユーザー登録条件として、ｉ)大学・研究機関、資金配分機関または政府機関のメールアドレスを持っていること、ii）大学・研究機関、資金配分機関または政府機関において、職務として研究セキュリティ・インテグリティ確保の検討・実施または政策立案に関わっていることの両方の条件を満たす個人とした。想定されるユーザー像は、職務として研究セキュリティ・インテグリティ確保の検討・実施に関わっている（研究インテグリティ関連部門にお勤め）、かつ、所属機関が、国際共同研究を推進していること、研究インテグリティに関する外国政府や機関の情報収集、関係者とのネットワーキングに関心があることを掲げている。

各回の申し込み状況および参加者との質疑応答の概要を下記に示す。

表 4-6　説明会開催概要および質疑応答

説明会	概要	説明会時の質疑応答
第1回 説明会	・ 日時：2025年11月5日（水）17時から17時30分 ・ 事前参加登録者：80名 ・ 当日参加者：58名	・ 機関窓口のアカウントでバーチャルアカデミーの参加は可能か？ ➢ ユーザー登録のメールアドレスは機関が発行する個人のメールアドレスでお願いします。もし、機関窓口の登録も個人のメールアドレスでということであれば併用していただくことも可能。ただ、窓口のメールアドレスについてはできる限り共有のメールアドレスでお願いしている。実用上は問題ない。
第2回 説明会	・ 日時：2025年11月12日（水）17時から17時30分 ・ 事前参加登録者：49名 ・ 当日参加者：29名	・ 昨年度機関の窓口登録した大学であるが、アカウントはそのまま使えるか。今年度新規ユーザー登録をする場合の手順は？ ➢ ユーザー登録の手順②から進めてください。 ・ 昨年度、機関登録と何名か個人登録を済ませていますが、組織再編等があり、機関登録済みの内容（メールアドレス等）を変更することは可能でしょうか？ ➢ 組織再編があるということですので、前回まで使用していた窓口のメールアドレスを一旦使用しないとしていただき、新しく窓口登録のメールアドレスを登録していただく。そのうえで元々ユーザー登録されている方と新規で登録する方の紐づけを行っていただく。

4.4　申請・登録状況等

4.4.1　窓口登録状況

機関の窓口登録については、2025年度は新たに5機関が登録した。大学機関が2機関であり、研究開発法人が3機関であった。2024年度登録機関については、継続意向調査後、1機関から登録継続の回答があり、前年度からの登録継続機関は36から37機関となった。

表 4-7　機関の窓口登録状況

区分	2025年度新規登録	2024年度登録機関（意向調査後）		総計
		登録継続	登録非継続	
国公立大学	1	18	4	23
私立大学	1	11		12
大学共同利用機関			1	1
研究開発法人	3	8	3	14
総計	5	37	8	50

4.4.2　ユーザー登録状況

2025年度のユーザー登録状況については、新たに20名がユーザー登録した。2024年度の登録継続意向のユーザーと合わせると日本の事務局にユーザー登録申請を実施した者は102名である。このうち、「SINAPSE−G7バーチャルアカデミー」登録申請・認証

に至っている者は、2024 年度ユーザー登録者で 48 名、2025 年度ユーザー登録者で 11 名の全体 59 名（登録者の 57.8%）である。

表 4-8　ユーザー登録の状況（登録の継続意向者＋新規登録者）

	SINAPSE／G7VA 登録済	SINAPSE／G7VA 未登録	総計
2024 年度ユーザー登録者	48	34	82
2025 年度ユーザー登録者	11	9	20
総計	59	43	102

4.5　その他（文書のアップロード手順の整備）

バーチャルアカデミーに登録したユーザーは、研究セキュリティ・インテグリティ関連の文書（原則英語であるが、日本語でも可（英語の要約文があることが望ましい））やリンクなどをバーチャルアカデミーにおいて公開することができる。文書等をアップロードし公開する際の申請について手引を整備した。手順は、申請期間中（2025 年度は 2 つの申請期間を設定[559]）に、申請 Web フォーム（Microsoft Forms）を通じて、ユーザーからシステム管理者に対して事前申請する手続きとした。

図 4-5　「バーチャルアカデミー」への文書等のアップロード手続き

出典：内閣府科学技術・イノベーション推進事務局「G7 バーチャルアカデミー登録方法説明会」資料, 2025 年 11 月 5 日.

管理者は申請された文書等が以下の 3 点を満たすかを確認し、公開の可否を申請者に通知する。

・　所属機関の策定した研究セキュリティ・インテグリティに関連する規則、方針・ガイド

[559] 申請期間については、第 1 次申請期間が 2025 年 11 月 5 日～2025 年 12 月 15 日まで、第 2 次申請期間が 2025 年 12 月 16 日～2026 年 1 月 31 日までとした。

ライン、計画、ツール（ガイド、チェックリスト等）等であるか。

・　文書等のバーチャルアカデミーにおける公開を、文書を策定した機関または策定者は許可しているか。

・　バーチャルアカデミーへの掲載が適切であるか等

なお、2025 年度は、ユーザー登録者からの事前申請はなく、文書等のアップロードは行わなかった。

第5章　調査のまとめ・分析と注目点

5.1　各国・地域の大学研究機関、資金配分機関における研究セキュリティ・インテグリティに対する取組状況の調査

第２章で、米国、カナダ、英国、オーストラリア、EU、オランダ、ドイツ、イタリアの大学・研究機関における研究セキュリティ・インテグリティの取組[560]を調査した。各国・地域に共通する課題認識は、研究の開放性・国際協力の推進と、安全保障、デュアルユース、外国干渉等のリスクへの対応をいかに両立させるかという点にあると考えられる。また、研究セキュリティ・インテグリティの確保は、政府、資金配分機関、大学・研究機関、研究者の共同責任であるとの考え方もみられる。

他方、政府方針・法令の指示の強弱、大学・研究機関の自律性の程度、中間的な支援・調整組織の有無、政府による体制等整備のための資金支援の有無等に応じて、大学・研究機関や資金配分機関が担うべき役割、体制の整備状況、取組の内容には国・地域ごとに相違もみられた。

5.1.1　大学・研究機関における研究セキュリティ・インテグリティの確保のための取組

本事例調査を通じて確認できるのは、各国・地域の大学・研究機関における研究セキュリティ・インテグリティ対応は、重点の置き方や取組の進展の程度に差はあるものの、概して、①政府方針、法令、資金配分条件等を学内の規程、手順及び体制に具体化する機能、②国際共同研究の検討、研究者・訪問者受入れ、機微技術に該当するか等に関する個別案件について、デュー・ディリジェンス、確認及び必要な判断を行う機能、③研究者及び関係職員に対する周知、教育及び研修を行う機能、④研究者からの相談対応、手続支援及び学内調整を通じて実務運用を支える機能を組み合わせたものとして展開している点である。加えて、一部の大学・研究機関では、⑤他大学等との連携・情報共有を通じて知見の共有や対応能力の向上のための機能、⑥大学・研究機関としての価値観や研究理念を踏まえ、国際研究交流に伴うリスクを主体的に判断する機能も確認された。

(1)　各国の大学・研究機関における研究セキュリティ・インテグリティの取組

米国

米国では、NSPM-33、CHIPS and Science Act（CHIPS 科学法）、OSTP 研究セキュリティプログラムガイドライン等の連邦政府から求められる要件が、資金配分機関の公募要件を通じて、大学・研究機関の実務（開示、研修、国際連携、輸出管理、渡航、情報セキュリティ等）に実装されている。連邦政府からの研究資金受領が年 5,000 万ドルを超える大

[560] 調査対象国・地域において調査対象としたのは、”research security”等についての取組であり、研究不正対応等を含む研究公正についての取組は除く（以下同様）。

学・研究機関は、研究セキュリティ・プログラム（サイバーセキュリティ、海外渡航セキュリティ、研究セキュリティ研修、輸出管理研修の 4 項目）を整備することが求められる。5,000 万ドル以下の大学等でも、PI とシニア・キーパーソン単位で開示や研修、「悪性人材採用プログラム」（MFTRP）不関与の証明が連邦研究資金を受領するためには必要となっている（5 頁以下を参照）。

研究資金配分機関は連邦政府研究資金の受領要件を課し大学・研究機関における取組を促すとともに、NSF は研究セキュリティに関して大学・研究機関間の情報共有・訓練・政府との橋渡しの機能を担う中間機関として SECURE Center を構築した。

事例調査を行ったマサチューセッツ工科大学（MIT）、テキサス A&M 大学システム、ワシントン大学は、年間 5,000 万ドル以上の連邦政府研究資金を受領する研究大学である。これらの大学では、NSPM-33 と CHIPS 科学法の遵守にとどまらず、デュー・ディリジェンスの仕組み導入、研究セキュリティに特化した研究所の設置や大学内外を対象とした研修など、各大学で特色のある取組がみられた。

カナダ

カナダの研究セキュリティ確保のための制度は、連邦政府の 2 種類のガイドライン（National Security Guidelines for Research Partnerships と Policy on Sensitive Technology Research and Affiliations of Concern）に基づき、主として研究資金申請・執行の要件として実装されている。研究者（申請者・研究チーム）に対する申告・確認・継続的遵守の要求が中心であり、研究者は正しく申告する義務がある。他方、大学・研究機関には、これを支える申請管理・周知・手続支援といった支援的役割が求められている。ただし、研究者の申告内容に不正の疑いがあった場合に不正調査を実施する責任は研究者が所属する大学・研究機関にある。加えて、一部の州（例：オンタリオ州）では、州独自の研究資金制度において、大学・研究機関に対する要件をより直接的に課している。

カナダでは Budget 2022 以降、Research Support Fund（RSF）を通じ、連邦政府研究資金を受領する大学等における研究セキュリティ確保のための能力構築支援が制度化されている。大学等は政府資金を活用し継続的に体制整備を進めている。

また、カナダでは U15 研究大学連盟のワーキンググループなど、大学間の横連携による実務調整の動きも見られ、各大学の自律性を維持しつつ、知見の共有を進めている。

事例調査を行ったアルバータ大学、トロント大学、マギル大学は、いずれも U15 のメンバーである研究大学であり、政府研究資金の受領額は上位であり、上記の RSF を活用し、研究セキュリティ確保のための体制整備や様々な取組を実施している。

英国

英国では、NPSA による Trusted Research イニシアティブの下、NPSA による Trusted Research に関する各種ガイダンス文書が強い政策的参照点となっており、これらのガイダンスに従って、各大学で実務的なガイドラインやツールの実装を進めている。

インペリアル・カレッジ・ロンドンでは、研究者向けに、国際協力における潜在リスクを

考察する方法に関する各種文書やツール（第三者機関の関係性をチェックするための質問票等）を整備している。オックスフォード大学では、国際共同研究におけるデュー・ディリジェンス、法令・規制の遵守、海外での会議におけるセキュリティ対策等に関する解説、文書、ガイダンス等を提供している。アストン大学では、デュー・ディリジェンス、輸出規制、国家安全保障・投資法等について手順書を含め、研究者に、共同研究の申請の手続き等に関する必要な情報を提供している。ウォーリック大学では、デュー・ディリジェンス、輸出管理、国家安全保障・投資法等の Trusted Research の主要分野に関する標準的な運用方針とプロセスを策定している。英国の大学の事例は、安全保障上の要請への対応と、学問の自由、平等、大学の価値規範の保護を同時に制度設計に組み込んでいる。

オーストラリア

オーストラリアでは、UFIT ガイドラインに加え、外国関係・輸出管理・制裁等の法制度群を背景に、大学が具体的な審査フローを構築している。ANU では FIAC（外国干渉諮問委員会）と外国干渉フレームワークを設け、REMS 経由の外国関与評価を運用し、研究・国際・情報セキュリティ機能を連携させている。アデレード大学では、外国コンプライアンス審査（FCR）を設け、採用、契約、共同研究、調達、留学生受入れ等まで広く審査対象を定めている。UWA では外国干渉方針（FIAC 報告を含む）と国際パートナーシップ・ガイドラインを整備し、研究インテグリティ、サイバー、プライバシー等の関連政策と接続している。

欧州連合

EU 事例は、大学現場の個別運用というより、欧州大学協会（EUA）・全欧州アカデミー（ALLEA）のような学術団体が、欧州委員会や ERA（欧州研究圏）関連の政策形成に対して、大学側・学術側の立場から原則を提示している点に特色がある。EUA は、約 900 会員を擁する大学団体として、研究セキュリティを研究・イノベーション政策の一部として扱い、EU 政策への意見提出を行っている。

EUA・ALLEA 双方に共通するのは、研究セキュリティを否定せず、むしろ必要性を認めた上で、比例性（proportionality）・最小限性（minimum standards）・大学自治・国際協力の開放性を重視している点である。ALLEA は ERA 法関連の議論において比例原則を明示し、過度に広い規制が研究を萎縮させることへの懸念を示している。EUA も、大学の国際連携を前提とした上で、リスクに応じた運用の必要性を主張している。これは、国家安全保障上の要請と学術の国際性を両立させる「上位原則」の提示という意味で、各加盟国の大学運用にも間接的に影響を与える。

オランダ

オランダでは、国の Knowledge Security Guidelines が全体方針として策定されており、各大学がそれを踏まえて知識セキュリティに関するガイドラインの実装を進めている。

アムステルダム大学は、「第三者との協力に関する諮問委員会」を設置し、外部連携の可

否を判断する評価ガイドラインを用いて、質問事項に Yes/No で答えることで可否を評価している。アムステルダム自由大学は、「知識セキュリティ諮問グループ」を設置し、大学としての知識セキュリティ・フレームワークを策定し、職員採用前審査方針等も策定しており、参考になる。

ドイツ

ドイツでは、研究セキュリティの制度化が、法令主導というよりも、ドイツ研究振興協会（DFG）・レオポルディーナ等の学術界の勧告・行動規範を核に進められている。政府が包括的な法令を設けて一律統制するのではなく、学術コミュニティの自己統治と学術機関の自律的運用が中心にあると言える。

この枠組みの下で、カイザー・スラウテルン＝ランダウ工科大学の KEF（安全保障関連研究倫理委員会）規約は、委員構成、申請手続、審議方法、外部専門家意見の活用を含めて明文化され、DFG/レオポルディーナの勧告に準拠した「平均的モデル」として位置づけられている。一方、ミュンヘン工科大学（TUM）では「世界的活動原則（Global Activity Principles）」を策定し、国際協力の開放性を前提にしつつ、リスク対応を組織の目的・価値と整合的に運用する考え方を打ち出している。つまりドイツでは、デュアルユース・研究倫理型の委員会運用と、国際協力リスク管理の原則運用が並行して発展している。

加えて、ライプニッツ協会の事例は、集合型研究機関群における研究セキュリティ運営の一つのモデルを示す。本部はガイドライン・情報共有・助言を担い、各研究所が個別リスク管理に責任を持つ分権方式であり、連邦輸出管理局（BAFA）等の公的情報も参照しつつ、研究協力機関審査、採用時チェック、制裁リスト確認、輸出・技術移転管理等を各研究所が実施する。これは、日本のように大学間の規模差が大きい環境で、中央集権一択ではない設計の参考となる。

イタリア

イタリアは、包括的な国家法制がまだ十分に整っていない中で、大学側・大学団体側の実務形成が先行している点が特徴である。大学学長会議（CRUI）は 2025 年に研究セキュリティ作業部会を設け、研究、国際化、人的資源、輸出管理、サイバーセキュリティ等を含むガイドラインを策定しており、各大学の自律的取組を束ねる横断的基盤として機能し始めている。サピエンツァ大学はデュアルユース・輸出管理・金融制裁対応を含む窓口と実務支援を整備しており、大学単位での制度整備も進んでいる。イタリアの大学・研究機関では、包括的法令の不在下でも自律的に取組が進展している点が注目できる。

表 5-1　各国・地域の大学・研究機関における研究セキュリティ・インテグリティの取組

① 米国

大学・研究機関の役割・義務等
NSPM-33 によるもの ・年間 5 千万ドル超の連邦 S&E 助成支援を受ける場合には、「研究セキュリティプログラム」を設置・運用 ・COI/COC、研究セキュリティ上のリスクの識別・管理のための方針、プロセスの整備 CHIPS 科学法によるもの ・雇用する対象研究者（covered individual）が研究セキュリティ研修を修了したことを認証（certify）する ・対象研究者が悪性人材採用プログラムに関する要件を理解し、遵守していることを認証する ・海外からの資金支援の有無を毎年報告する
大学等における研究セキュリティ確保に関する取組の特色（3 大学の事例調査に基づく）
・連邦政府の研究セキュリティに関する法令、ガイドラインによって課される義務等を果たすための取組を実施している：担当のセクション・委員会等の設置等の体制整備、リスク判断の学内プロセス等の導入、研修等） ・要件を満たすことに加え、大学独自の取組にも取り組んでいる（中国の関与についての大学としての方針を検討し報告書を作成等）
参考となる点
・全国的又は地域的な連携・情報共有への大学等の関与（ワシントン大学：SECURE Center 運営、テキサス A&M 大学：SECURE Analytics 運営、RISC Institute 設置、ASCE 会議の毎年開催等） ・全学的なデュー・ディリジェンスプロセスの仕組みの導入と関与 ・大学等の主体的な研究セキュリティへの関与と検討（MIT：懸念国との関与をどうすべきかの検討など）
大学における研究セキュリティ確保のための主な取組（3 大学の事例調査に基づく）
【体制整備】 ・「国際調整委員会」「国際助言委員会」「シニアリスクグループ」を設置（MIT） ・「Chief Research Security Officer」を任命（ワシントン大学）など 【学内の情報提供】 ・「研究セキュリティと国際的関与」等のウェブサイトを作成（MIT）など 【デュー・ディリジェンス】 ・「非公式国際協力ツール」を開発（MIT） ・「ハイリスクレビュープロセス」を導入（MIT）（⇒次節の注目事例参照） ・国際関与に関する「10 のポイント」作成（MIT） ・既存の国際協定のリスク評価、見直し（テキサス A&M 大学システム） ・行動項目チェックリスト（ワシントン大学）など 【教育・研修】 ・約 90 分の研究セキュリティ研修教材作成（MIT） ・PI 向けの小冊子作成（研究室の学生等との討議用）（MIT）など ・解説動画作成（ワシントン大学） 【他大学等との連携・情報共有】 ・RISC Institute の設置（テキサス A&M 大学） ・ASCE 会議の毎年の開催（テキサス A&M 大学） ・SECURE Center の運営（ワシントン大学） ・SECURE Analytics の運営（テキサス A&M 大学） 【その他】 ・「中国への関与」についての学内委員会で検討し報告書作成（MIT）

② カナダ

大学・研究機関の役割・義務等
NSGRP によるもの ・研究者への支援の提供（open-source due diligence 等） STRAC によるもの ・研究者への支援の提供（研究者が STRAC に適切に対応できるような各種支援） ・大学等の研究助成金担当者は、研究者が採択前後の責任を理解できるよう支援 ・attestation が全て記入されているかを確認（※attestation の真偽検討の責任は負わない） ・資金配分機関とのコミュニケーション促進（研究内容・メンバー変更等） ・機関は、虚偽申告の疑いがある場合、RCR 違反として調査を行う責任がある 一部の州政府によるもの ・一部の州政府は、州の研究資金制度について、申請期間としての大学等に対して要件を直接課している（例：オンタリオ州）。
大学等における研究セキュリティ確保に関する取組の特色（3 大学の事例調査に基づく）
・連邦政府資金を利用して、体制整備に取り組んでいる ・連邦政府、州政府の両方の要件がある点で複雑であり、所属研究者への周知のために学内 Web サイト等で情報提供に努め、研究者の理解を助けている ・Community of Practice で有力大学が地域の中小大学の情報共有を主導している
参考となる点
・連邦政府資金を利用して、体制整備に取り組んでいる ・Community of Practice で有力研究大学が主導し地域の大学等と情報共有が行われている
大学における研究セキュリティ確保のための主な取組（3 大学の事例調査に基づく）
【体制】 ・Safeguarding Research Office を設置し、デュー・ディリジェンス等の対応（アルバータ大学） ・Research Security + Compliance Office を設置（マギル大学） ・Research Security Team が研究者支援を担当（トロント大学） 【学内の情報提供】 ・Research Security ウェブサイト作成等（マギル大学） ・Safeguarding Research Web サイトの作成（トロント大学）など 【デュー・ディリジェンス】 ・Responsible Open Source Due Diligence Protocol を制定、文書をして公表（アルバータ大学）（⇒次節の注目事例参照） ・Research Funding Checklist を研究管理電子システム上に統合（マギル大学） ・Research Partnership Security Information Document for International Partnerships (RPSID)ツールの作成（トロント大学） 【教育・研修】 ・Research Security Day イベントを年 1 度開催（アルバータ大学） ・ポッドキャスト番組の作成（アルバータ大学） ・公共安全省職員を講師とする学内セミナーの開催（マギル大学） ・学内オンライン教材作成（マギル大学） 【他大学等との連携・情報共有】 ・研究セキュリティ Community of Practice を地域で作り、メンバーの地域の大学等との情報共有を主導（アルバータ大学） ・地域の大学付属病院との連携（トロント大学） ・U-15（カナダの 15 研究大学から構成）における実務調整・知見共有

③ 英国

大学・研究機関の役割・義務等
Trusted Research Guidance for Academia によるもの ・大学として守るべき機微領域の把握、新規共同研究・資金提供先に対するデュー・ディリジェンスの実施、利益相反の管理と大学内外の研究関係の可視化、機微な研究・知的財産権・個人データへのアクセスを必要最小限に制限、契約・輸出管理・データ保護などの法的枠組みへの適切な対応、研究成果の公開前に特許化や保護の要否を検討すること、海外研究者・訪問研究者・海外出張者の適切な管理等を行う必要がある（義務ではない）。 National Security and Investment Act: guidance for the higher education and research-intensive sectors によるもの ・National Security and Investment Act（英国の国家安全保障を脅かす可能性のある産業等に対する出資を規制した法律）に対応して、17 の重要技術（AI、量子技術、合成生物学等）に係る、装置、知的財産等を取得する場合には、政府に届出を行う義務がある。
大学等における研究セキュリティ確保に関する取組の特色（4 大学の事例調査に基づく）
・Trusted Research Guidance for Academia 等の政府のガイドラインに基づき、大学としての研究セキュリティに関する各種ガイドラインやツールを作成。特に、共同研究先に対して、しっかりとしたデュー・ディリジェンス審査を実施。 ・研究支援部門を中心とした、研究者が共同研究を行う際の研究セキュリティに関する幅広い支援体制を確立。
参考となる点
・共同研究の申請については、研究支援・コンプライアンス部門が一次審査を担い、高リスクの案件は上位決裁へエスカレーションする体制を整備。 ・全案件に一律の厳格な手続を課すのではなく、リスクの程度に応じて審査の深度を調整する運用方法（例えば、簡易確認→追加確認→高リスク案件の深掘り）を採用。 ・共同研究パートナーのデュー・ディリジェンスを実務手順として組み込み、判断根拠や手続を記録として残す仕組みを重視（アストン大学）。 ・研究者だけではなく、研究支援職員、技術職員および博士課程の学生に焦点を置いて、研究セキュリティに関する研修・啓発を実施（ウォーリック大学）。
大学における研究セキュリティ確保のための主な取組（4 大学の事例調査に基づく）
【体制】 ・Research Office に Research Security Team を設置（インペリアル・カレッジ・ロンドン） ・Research Services に Trusted Research Team を設置（オックスフォード大学） ・Research & Impact Services に Research Governance & Compliance Team を設置（ウォーリック大学） 【学内の情報提供】 ・Trusted Research に関するウェブサイトを設置 【デュー・ディリジェンス】 ・「第三者機関の関係性レビュー質問票」を作成（インペリアル・カレッジ・ロンドン） ・Outside Party Due Diligence Procedures を策定・公開（アストン大学）（⇒次節の注目事例参照） 【教育・研修】 ・研究および学術的責任を有する全職員に Trusted Research に関する e ラーニングモジュールの受講を義務化（インペリアル・カレッジ・ロンドン） ・e ラーニング研修モジュールとして「Trusted Research and Export controls」を提供（オックスフォード大学） ・学内ネットワーク上で Aston University online Due Diligence Training を提供（アストン大学） ・定期的に対面及びオンライン研修を学部で実施し、リスクの高い学部向けに定期的な研修を実施（ウォーリック大学） 【その他】 ・研究ガバナンス受信箱（Research Governance inbox）（電子メールでの連絡口）を設置（アストン大学）

④ オーストラリア

大学・研究機関の役割・義務等に関連する文書
UFIT ガイドライン（大学外国干渉タスクフォースによるガイドライン） ・UFIT は、政府、大学、研究機関が参加するタスクフォースであり、学術協力と学問の自由を維持しつつ、大学が外国干渉のリスクを特定・評価・軽減するために、2019 年 11 月にガイドラインを策定し、2021 年 11 月には改訂版が公表された。 ・教育省は、2023 年 8 月に「UFIT ガイドライン実施状況報告書」を、2024 年 4 月から 5 月にかけて、「外国干渉対策ガイドラインの実施状況に関する進捗確認」に関する報告書等を公表し、各大学における実施状況の把握が行われている。 ・ガイドライン補足資料として、「ガバナンスとリスク管理の枠組み」においてガイダンスノート、事例研究、自己評価の各報告書・資料を公表。「コミュニケーション、教育、知識共有」ではガイダンスノート、自己評価資料を、「デュー・ディリジェンス、リスク評価および管理」では、ガイダンスノート、事例研究、自己評価、デュー・ディリジェンス支援フレームワーク、オープンソース情報ファクトシート等を、「サイバーセキュリティ」ではガイダンスノート、事例研究、サイバーセキュリティ強化報告書等を公表した。
大学等における研究セキュリティ確保に関する取組の特色（3 大学の事例調査に基づく）
・UFIT ガイドラインに基づき、外国干渉対策の整備を行っている。 ・学内の研究セキュリティ（外国干渉リスク対策）は、大学内の内部資金で体制整備やリスク評価活動を実施している。 ・学内のガバナンス体制として、外国干渉に係る諮問委員会（オーストラリア国立大学〈ANU〉、西オーストラリア大学〈UWA〉）等を設置し、外国干渉リスクに対する多面的な評価を実施。アデレード大学では、外国コンプライアンス審査プロセスを策定し、外国との契約に関する承認プロセスを整えている。
参考となる点
・UFIT は政府と大学が共同で外国干渉からのリスクに対応する取組であり、UFIT ガイドラインに基づき各大学が内部の実施体制を整備している。 ・防衛技術の研究開発に関わる大学では、UFIT ガイドラインの関連項目の学内規程の遵守に加え、オーストラリアの外交関係法、防衛貿易管理法、自主制裁法、2018 年外国影響透明性制度法への対応も、外国干渉リスクとして必要とされている。
大学における研究セキュリティ確保のための主な取組（3 大学の事例調査に基づく）
【体制】 ・外国干渉諮問委員会（FIAC）設置（オーストラリア国立大学、西オーストラリア大学） ・外国コンプライアンス審査（FCR）の策定（最高保安責任者室が審査） 【学内の情報提供】 ・教職員・学生が外国政府による干渉のない安全な環境で活動・学習する権利を支持する観点から外国干渉リスク対策を実施。大学により、全教員およびシニアの専門職・一般職員に該当する義務を理解しているかを示す年次報告書の提出を義務付けている機関もある。 【デュー・ディリジェンス】 ・UFIT ガイドラインでは、デュー・ディリジェンスについて、提携締結前に外国関与の評価を義務付けている。アデレード大学では外国コンプライアンス審査にあたり、国家安全保障法への遵守を確保するため、UFIT ガイドラインのデュー・ディリジェンスとの整合的な運用基盤を整理している。 【教育・研修】 ・UFIT ガイドラインの「コミュニケーション、教育、知識共有」の項目に沿って、各大学で実施方法を検討している（ウェブサイト上の教育・研修動画の提供等）。学内での審査プロセス（外国との契約〈共同研究、協定、研究者の受入等〉）を通じて、研究申請者に相当する者を対象に教育を進めている例もある。 【他大学等との連携・情報共有】 ・UFIT では、オーストラリアの 8 大学が参加し、ガイドラインを策定してきた。

⑤ オランダ

大学・研究機関の役割・義務等
National Knowledge Security Guidelines ・大学内の機微な知識領域の特定、案件ごとのリスク評価、大学内への知識セキュリティ・ガバナンスの設置、人事・来訪者・出張管理におけるリスク管理、知識セキュリティ文化の継続的な取組み、国際連携・契約・調達への知識セキュリティの組込み、サイバーセキュリティに関する最低限措置の実装等を行う必要がある（義務ではない）。
大学等における研究セキュリティ確保に関する取組の特色（2 大学の事例調査に基づく）
・National Knowledge Security Guidelines に基づき、大学としての知識セキュリティに関する各種ガイドライン、ツール等を作成し、研究者に提供。
参考となる点
・知識セキュリティに倫理審査と人権配慮を含める。 ・回答者（研究者）が各質問について Yes/No で回答することで、共同研究や連携する機関の可否を評価する流れを示したわかりやすいフローチャートを作成。 ・大学職員（事務系職員、研究系職員）採用前審査のガイダンスを作成し、リスクマトリクスを用いた職員採用前審査の仕組みを開発（アムステルダム自由大学)。
大学における研究セキュリティ確保のための主な取組（2 大学の事例調査に基づく）
【体制】 ・Advisory Committee on Collaboration with Third Parties を設置（アムステルダム大学)。 ・Knowledge Security Advisory Group を設置（アムステルダム自由大学)。 【学内の情報提供】 ・知識セキュリティに関するウェブサイトを設置。 ・学内ネットワークに、職員向けに知識セキュリティに関する情報サイトを設置（アムステルダム自由大学)。 【デュー・ディリジェンス】 ・外部との連携の可否を判断する評価ガイドラインを作成（アムステルダム大学）（⇒次節の注目事例参照） ・大学職採用前審査のガイダンスを作成（アムステルダム自由大学)。 【他大学等との連携・情報共有】 ・オランダ国内の知識交流ネットワークに参加（アムステルダム自由大学)。 【その他】 ・研究者向けに、共同研究や連携する機関の可否を評価する流れを示したフローチャートを作成。

⑥ ドイツ

大学・研究機関の役割・義務等に関連する文書
Position Paper ・研究は諜報活動、悪用、外国の干渉などより大きなリスクに晒されているという認識の下、研究の強固な保護の必要性を論じた政府の研究セキュリティに関する新しい方向性を提示。 ・デュアルユースの取扱を中心にした対策からスパイ行為や外国の干渉などより広範なリスクを網羅する政策への政策転換を明示。 Espionage in Science and Research ・科学と研究における諜報活動という観点から科学分野の研究者向けのスパイ活動や外国政府とその代理人による干渉に備えるための BfV 発出の解説書。 Scientific Freedom and Security Interests in Times of Geopolitical Polarisation ・DFG とレオポルディーナが刊行した Position Paper を大学や研究者に向けに整理した解説書。
大学等における研究セキュリティ確保に関する取組の特色（6 大学等事例調査に基づく）
・DFG/レオポルディーナの勧告に基づいて、大学では安全保障関連研究倫理委員会を設置し、あわせてデュアルユース取扱を含むガイドラインもしくは行動規範に関する規程を整備。 ・デュアルユース関連のスパイ事件が起きた大学では、リスク評価に関する特別規程を定め、また新組織を追加で設置。 ・研究機関では、研究セキュリティ問題を個別に相談できるウェブ上のアクセス窓口の開設、内部コンプライアンス・プログラムの開発と運用など独自の取組を展開。
参考となる点
・学問の自由、研究の開放性、大学の自律など大学が従来より尊重してきた研究活動の理念と研究セキュリティの均衡に配慮。 ・DFG/レオポルディーナが関連文書の発行や大学・研究機関への助言・指導を行うなどの中心的な役割を果たし、また施策に関する議論には学術界代表者の参加を推進して研究者の自発的性を尊重。
大学における研究セキュリティ確保のための主な取組（6 大学等の事例長調査に基づく）
【体制】 ・安全保障関連研究倫理委員会（RPTU） ・研究の安全確保と若手科学者の育成のための委員会（ケムニッツ大学） ・マックス・プランク科学評議会（MPG） ・InHand@UFZ（ヘルムホルツ環境センター） 【学内の情報提供】 ・ウェブサイト（RPTU、ミュンヘン工科大学、ケムニッツ大学、MPG、ヘルムホルツ環境センター、ライプニッツ協会） 【教育・研修】 ・96 の研究所の集合体であるライプニッツ協会では、本部が各研究所が活用できる情報交換フォーマットを作成し、全所横断的なワークショップやイベントを開催 【他大学等との連携・情報共有】 ・ライプニッツ協会は、傘下の 96 研究所間の中国に関する情報共有と知見を創出するための協力体制構築を目的に「ライプニッツ研究ネットワーク中国」を設立（⇒次節の注目事例参照）

⑦ イタリア

大学・研究機関の役割・義務等に関連する文書
Cybersecurity: Research & Innovation Agenda ・ACN は国家のサイバーセキュリティに責任を有するが、研究におけるサイバーセキュリティに関しては MUR と協力して行動指針を作成。 National Framework for the Integrity and Security of Research ・MUR 発出による研究セキュリティに関する政府方針。 ・政府としての取組を網羅的に提示。 Guidelines for Research Institutions for the Integrity and Security of Research ・MUR が National Framework と同時に発出した大学・研究機関向けの研究セキュリティに関するガイドライン。 ・大学・研究機関が取組む事項を提示。
大学等における研究セキュリティ確保に関する取組の特色（3 大学等の事例調査に基づく）
・欧州委員会の勧告に準拠して EU 域外での協力に際してのデュアルユースの研究活動のコンプライアンスに関するガイドラインを作成（ローマ・ラ・サピエンツァ大学）。 ・海外フィールド調査中の事件を契機に、研究者の生命と人権保護のためのガイドラインを作成（CRUI、トレント大学国際研究大学院）。
参考となる点
・政府による取組が進んでいない状況下において、大学等が自発的に取組む。 ・ACN と DIS との連携体制を強化し、リスクに迅速に対応できる体制を構築。
大学における研究セキュリティ確保のための主な取組（3 大学等の事例調査に基づく）
【体制】 ・開発協力のための大学調整機構内作業部会（CRUI）の設置。 【他大学等との連携・情報共有】 ・CRUI による大学間協力と情報提供。

(2) 注目事例

本調査から抽出できる参考事例・注目事例は、以下のとおりである。大学・研究機関にとっては、これらの事例の参考となる点を組み合わせて参照することが有効である。

(a) 米国 MIT：高リスク案件のリスク審査

米国の MIT の「高リスクプロジェクトレビュープロセス」（19 頁参照）は、国際連携を一律に制限するのではなく、通常審査に加えて、特定の高リスク案件に対して追加的なレビューを行う仕組みである。資金提供、共同研究、現地活動など、MIT が正式な契約・合意関係を伴う案件について、教員と管理部門が多面的なデュー・ディリジェンスを実施する。

(b) カナダ・アルバータ大学：学内デュー・ディリジェンス方法のマニュアル作成

カナダのアルバータ大学の「Responsible Open Source Due Diligence Protocol」（56 頁参照）は、オープンソース情報（OSINT）を用いて行うデュー・ディリジェンスを、カナダの法令・学内方針・倫理要件に適合させつつ、透明・一貫・公正に実施するための実務プロトコルである。

(c)　英国アストン大学、オランダ・アムステルダム大学：実務フローの可視化

英国のアストン大学（88 頁参照）、オランダのアムステルダム大学（155 頁参照）のように、フローチャートや質問票により確認項目を標準化し、懸念がある案件は担当部署・委員会に付議して助言・判断を得る運用は、導入容易性と再現性の点で有効である。

(d)　ドイツ・ライプニッツ協会：分権型モデル

ドイツのライプニッツ協会の分権型モデル（184 頁参照）は、各研究所の多様性を前提にしつつ、ガイドラインと情報共有で全体を支える点で、複数機関を束ねる研究機関ネットワークにも参考になる。

(e)　英国・EU：安全保障対応と価値保護の同時設計

英国（インペリアル・カレッジ・ロンドン（78 頁参照）、オックスフォード大学（83 頁参照）等）や EU（欧州大学協会（EUA）（137 頁参照）、全欧州アカデミー（ALLEA）（140 頁参照））では、研究セキュリティを進める際に、学問の自由、平等、大学自治、国際協力の開放性といった価値を明示的に守る設計がみられる。これは、制度の正当性確保にとって重要であり、規制を課すだけでなく、守るべき価値を同時に宣言することの必要性を示している。

5.1.2　資金配分機関における研究セキュリティ・インテグリティの確保のための取組

本事例調査を通じて確認できるのは、各国・地域の資金配分機関における研究セキュリティ対応は、重点の置き方や取組の進展の程度に差はあるものの、概して、①政府方針・法令を助成条件や審査実務に具体化する機能、②個別案件に対するリスクベースの確認・審査機能、③大学・研究機関におけるデュー・ディリジェンス及びコンプライアンス体制の整備を促す機能、④制度運用を支える支援・能力構築機能、⑤制度運用の評価・検証・知見形成機能、を組み合わせた制度設計として展開している点である。もっとも、これらの機能のうち何を資金配分機関が自ら担うかという役割分担や重心の置き方は各国で、また資金配分機関の間で異なっている。

(1)　各国の資金配分機関における研究セキュリティの取組

米国

米国では、NSPM-33、CHIPS and Science Act（CHIPS 科学法）等を土台として、連邦研究資金配分機関が、大学・研究機関に対する研究セキュリティ・プログラム要件や、研究者に対する研修、開示、利益相反・責務相反（COI/COC）対応等の共通要件を実装する枠組みが整備されている。米国科学財団（NSF）（30 頁参照）は、SECURE Center を通じた大学・研究機関への支援、TRUST を通じたリスクベース審査の高度化、Research on Research Security (RoRS)を通じた研究セキュリティ政策・実務に関する知見形成を進めている。他方、国防省（DoD）（37 頁参照）は、fundamental research の公開性を重視しつつ、DoD の構成機関（DoD Components）によるリスクベース審査の判断枠組みとして Decision Matrix を公表し、判断要素の明確化と運用の一貫性向上を図っている。このように、NSPM-33 等に基づく連邦横断的な共通要件の下でも、各資金配分機関の実装には差があるが、大学・研究機関及び研究者にとっては、複数資金配分機関に共通して利用可能な研究セキュリティ研修モジュールの整備に加え、経歴・実績（Biographical Sketch）及び現在及び保留中のその他支援（Current and Pending (Other) Support）に関する共通様式の導入にみられるように、申請・開示実務の負担軽減の取組も進められている。

カナダ

カナダの資金配分機関における研究セキュリティ対応の特色は、連邦政府の共通指針を基盤としつつ、資金配分機関が審査、検証及び資金配分判断の中核を担っている点にある。自然科学・工学研究会議（Natural Sciences and Engineering Research Council of Canada: NSERC）（64 頁参照）を含む Tri-Agency の資金配分機関は、NSGRP 及び STRAC をそれぞれの助成審査に組み込んでおり、NSGRP では、対象申請において、Risk Assessment Form の提出と、その中で特定されたリスクに対応する Risk Mitigation Plan の作成・記載を求めるとともに、採択後には、当該計画及び採択通知等に示されたリスク緩和措置の実施を求めている。STRAC については、機微技術研究領域（Sensitive Technology Research

Areas）と指名研究機関（Named Research Organizations）との関係に着目し、attestation の提出を求めるとともに、その妥当性及び不適格性判断を資金配分機関側で運用している。

カナダ・イノベーション財団（Canada Foundation for Innovation: CFI））（66 頁参照）は研究インフラ資金助成を担当する資金配分機関であり、CAMS（CFI Awards Management System）上で、機関単位の申請・管理実務の中に研究セキュリティ対応を組み込んでいる。このように、カナダでは、共通の連邦指針の下で、資金配分機関が審査・検証・判断を担いつつ、その具体的な実装は資金の性格に応じて異なっている。

英国

UKRI の取組は、国家・政府レベルの研究セキュリティ・対外リスク管理の方向性を、UKRI の TR&I（Trusted Research and Innovation）として制度運用に埋め込んでいる点に特徴がある（97 頁参照）。TR&I Principles and Expectations は、単なる注意喚起ではなく、UKRI の制度・運用・資金配分の中に埋め込まれた行動期待として位置づけられ、大学・研究機関におけるガバナンス、デュー・ディリジェンス、人材・データ・契約管理等を横断的に扱う。同時に、英国の事例では、政府方針を資金配分機関が、原則→期待事項→助成条件・運用という形で段階的に落とし込み、研究機関側の責任ある自律的管理を促している点が特徴と考える。

オーストラリア

オーストラリア研究評議会（Australian Research Council）は、UFIT ガイドライン（大学セクター向け外国干渉対策）を土台に、ARC CFI フレームワークを通じて競争的助成（NCGP）の審査フローに研究セキュリティを統合している（124 頁参照）。特に、外国資金・外国人材プログラム・外国政府／軍・警察等との関係、制裁対象との関係などを、研究管理システム（Research Management System: RMS）情報とオープンソース情報（DFAT 制裁・統合リスト等）で確認し、必要時には国家安全保障機関や外部プロバイダーの助言につなぐ設計は、審査実務として具体性が高い。

また、2024 年の ARC 法改正により、国家安全保障・防衛・国際関係に関する要件が法的に強化され、審査の前倒し・厳格化が進んだ。このように、政府方針・法令の改正が資金配分機関の審査運用に直結していた。オーストラリアは、政府による戦略・UFIT ガイドライン・法改正を、ARC の審査プロセスの変更（前倒し審査、開示強化、OSINT 活用、大学連携）として実装している。

欧州連合

EU（欧州委員会）は、ホライズン・ヨーロッパにおいて、研究の開放性・国際協力を基本としつつ、規則（例：参加制限、セキュリティ関連要件）と助成手続文書を通じて、研究セキュリティ審査を段階的に実装している（143 頁参照）。具体的には、申請時の自己評価（security self-assessment）、必要に応じた security scrutiny/review、採択後の助成契約上の義務である。EU では、研究内容・参加者・機微性に応じて必要な範囲で比例的

（proportionate）に審査・管理を行い、一律規制としない。

オランダ

NWO では、国の Knowledge Security Guidelines（2025）や知識セキュリティ関連制度（法制化の動向を含む）に基づき、申請フォーム上で研究者・機関に対し、知識セキュリティ上の論点の有無だけでなく、その法的根拠・機関内の判断枠組みを明示させる設計であり、研究機関側のガバナンス責任を可視化している（164 頁参照）。

NWO の特色は、資金配分機関がリスクに対する審査を全面的に引き受けるのではなく、大学・研究機関の内部審査・ガバナンスを前提にしつつ、その説明責任を申請段階で担保する点にある。これは、大学側の能力形成を促す設計として参考となる。

ドイツ

ドイツでは、DFG と DLR-PT に共通して、研究セキュリティを既存の法制度（輸出管理、デュアルユース、制裁・禁輸、軍事関連規制等）や研究管理実務に接続する形で実装している。DFG は、申請者向けに安全保障関連の留意事項や法令参照を示しつつ、採択審査の一部として研究セキュリティを織り込み、特に申請準備段階での自己点検を重視している（187 頁参照）。

一方、DLR-PT は、研究プロジェクト管理機関として、BMBF 等の政策要請の下で、申請・採択・実施管理の各段階に研究セキュリティを組み込み、ハンドブックや作業補助資料、相談機能等を用いて実務支援を行う構造が特徴である。これは法令順守と現場運用の橋渡し役としての性格が強いと考えられる（189 頁参照）。

表 5-2　各国・地域の資金配分機関における研究セキュリティ・インテグリティの取組

① 米国

資金配分機関の役割・義務等
NSPM-33 によるもの ・公募申請者（PI 等）に利益相反・責務相反の情報開示を求める等 ・政府機関 R&D 実施者、資金配分プロセス担当者に研修実施 ・連邦機関職員に対して、外国人材採用プログラム参加の禁止 ・年間 5 千万ドル超の連邦 S&E 助成支援を受ける大学・研究機関に対して「研究セキュリティ・プログラム」の設置・運用を求める CHIPS 科学法によるもの ・助成金公募で悪性海外人材採用プログラムに参加していないことの証明を求める ・助成金公募で対象研究者（covered individual）が過去 1 年以内に研究セキュリティ研修を修了していることを認証（certify）するとの要件を設ける （以下は特に NSF に対して） ・Office of Research Security and Policy の維持（少なくとも 4 名のスタッフを置く） ・研究セキュリティについてのオンラインリソース開発 ・研究セキュリティ・インテグリティ情報共有分析組織（RSI-ISAO）の設置（公募） ・国家情報長官室と調整し、管理情報へのアクセスを伴う研究分野を同定する計画を策定 ・孔子学院を設置する研究機関への資金提供原則禁止
資金配分機関における研究セキュリティ確保に関する取組の特色（NSF、DoD の事例調査に基づく）
・NSF で NSPM-33、CHIPS 科学法で課された取組等を計画的に実施（体制整備、審査プロセス、公募要件、研修教材、SECURE Center 設置等）。（⇒次節の注目事例参照） ・DoD では fundamental research の研究結果について原則公開であるとの原則を明確にしつつ、研究セキュリティについてリスクベースで評価するとの明確な方針を出している ・NSF の TRUST、DoD のリスクベース・セキュリティ審査プロセスなど資金配分機関内での審査体制、審査のプロセス等を整備してきている
参考となる点
・SECURE Center を設置し、全国的な情報共有のための組織を整備（地域拠点を含む） ・DoD では、Decision Matrix を公表。リスク審査判定の標準化と透明性向上を図っている ・Research on Research Security で研究セキュリティ政策のデータに基づき実証的検討（⇒次節の注目事例参照）
資金配分機関における研究セキュリティ確保のための主な取組（NSF、DoD の事例調査に基づく）
【体制整備】 ・Office of the Chief of Research Security Strategy and Policy の設置（NSF） 【大学等・研究者への情報提供】 ・”Research Security at NSF”等の web サイトを通じた大学等・研究者への情報提供 【デュー・ディリジェンス】 ・TRUST プロセスの導入（NSF） ・Decision Matrix の作成・公表（DoD）（⇒次節の注目事例参照） 【公募要件の追加等（共通フォーム作成を含む）】 ・研究者等の情報開示（悪性人材採用プログラム参加等含む）、研究セキュリティ研修受講等の公募要件への反映（NSF） ・研究セキュリティ・プログラムについてのガイドライン作成、要件の実装（NSF） 【教育・研修】 ・研修教材の作成（大学に委託）。資金配分機関間で共通の研修教材の作成（NSF） 【大学・研究機関間の連携・情報共有】 ・SECURE Center 等設置の公募（NSF） 【その他】 ・JASON 報告書の作成と公表。Research on Research Security 公募プログラム（NSF）

② カナダ

資金配分機関の役割・義務等
NSGRP によるもの ・公募申請者（研究者）に対して、Risk Assessment Form 提出、必要に応じて Risk Mitigation Plan の作成・実施を求める ・提出された Risk Assessment Form の内容確認、リスク評価（open-source due diligence） ・Risk Assessment Committee での評価（リスクが疑われる場合） STRAC によるもの ・公募申請者（研究者）に STRA（機微技術研究領域）該当の場合には attestation フォーム提出を求める ・STRA を進展させるかを研究者が適切に自己判断したかを検証（ランダム抽出、必要に応じて専門家関与） ・attestation フォームの記入内容の正確性の検証（公共安全省と連携、ランダム抽出） 一部の州政府のガイドライン等によるもの ・一部の州政府は、州の研究資金制度について州レベルの Research Security ガイドラインの遵守等を求める（オンタリオ州等の研究資金配分部門）
資金配分機関における研究セキュリティ確保に関する取組の特色（2 資金配分機関（NSERC と CFI）の事例調査に基づく）
・STRAC では STRA の申告内容の適切性、attestation の正確性等について、ランダム抽出で、必要な場合には、公共安全省とも連携して検証をしている（⇒次節の注目事例参照）
参考となる点
・STRAC では機微技術、指名研究機関に該当するかを研究者が適切に判断し、提出書類に記入しているのかを政府（公共安全省）の支援も必要に応じて受け、判断をする仕組み
資金配分機関における研究セキュリティ確保のための主な取組（NSERC、CFI 等の事例調査に基づく）
【体制】 ・担当部署の受付窓口のメールアドレスを web サイトに記載している（NSERC） 【情報提供】 ・NSGRP と STRAC の Tri Agency ガイダンス作成（Tri agency） ・”Research Security: Resource”の web サイトなど（NSERC） 【デュー・ディリジェンス】 ・研究者から提出された attestation の内容について妥当性、正確性の確認（NSERC） 【助成金公募等への実装（共通フォーム作成等）】 ・NSGRP 対象公募プログラムでリスク評価フォーム提出を求める等（NSERC） ・STRAC 対象公募プログラムで attestation 提出を求める等（NSERC） ・CAMS（CFI awards management system）への研究セキュリティ様式、module を組み込み、管理 【教育・研修】 ・Webinar 実施（CFI）

③ 英国

資金配分機関の役割・義務等
Trusted Research & Innovation: Principles and Expectations によるもの ・研究とイノベーションが、誠実さをもって強固な倫理的枠組みの中で行われるよう確保すること。 ・公平性・多様性・包括性（Equality, Diversity and Inclusion: EDI）を確保すること。 ・公募申請者に対して、リスクが高いと見なされたプロジェクトには、追加の緩和策や管理策の実施を求める。 ・公募申請者に対して、研究パートナーシップ、共同研究契約、商業契約に関与する他組織に対して、適切なデュー・ディリジェンス（相手先の慎重な事前調査）評価を実施することを期待。 ・公募申請者に対して、研究とイノベーションが、誠実さをもって強固な倫理的枠組みの中で行われるよう確保することを期待。 ・公募申請者に対して、共同研究プロジェクトにおける相互の透明性と開放性に加え、商業上の要請、法令上の要件、および英国の国家安全保障上の要請とのバランスをとることを期待。 ・公募申請者に対して、情報交換に共有プラットフォームを使用する場合には、不正アクセスを防止するためアクセス制御を実施することを期待。
資金配分機関における研究セキュリティ確保に関する取組の特色
・UKRI が、Trusted Research and Innovation（TR&I）を、英国の知的財産、機微な研究、人材およびインフラを、潜在的な窃盗・悪用・搾取から保護することと定義し、UKRI が助成金を提供する研究組織（企業、研究所、研究技術機関を含む）に対する一般的な期待事項を示した「Trusted Research & Innovation: Principles and Expectations」を公表。
参考となる点
・助成の可否の判断において、リスクベースのアプローチを採用していること。 ・公募申請者に対してプロジェクトパートナーが拠点とする国の民主的・倫理的価値観や法的枠組みを理解していることを求めていること。 ・公募申請者に対して、申請時に求められる可能性のある、または審査プロセスの一部となる TR&I 関連の追加要件を明確に示すことを求めていること。 ・公募申請者に対して要求される追加のリスク緩和策や管理策が、具体的かつ適切な範囲のものであり、理解可能で、助成金受給者が実行可能なものであることを求めていること。
資金配分機関における研究セキュリティ確保のための主な取組（UKRI の事例調査に基づく）
【体制】 ・UKRI 内部に TR&I Shared Capability Team を設置。 【情報提供】 ・UKRI“Trusted research and innovation”の web サイトを通じて、大学等研究者に「Trusted Research & Innovation: Principles and Expectations」について情報提供。（⇒次節の注目事例参照） 【デュー・ディリジェンス】 ・非公開 【助成金公募等への実装（共通フォーム作成等）】 ・共通フォームはないが、UKRI の公募別に、「Trusted Research & Innovation: Principles and Expectations」にて期待される事項の記載を求めている。 【教育・研修】 ・非公開

④ オーストラリア

資金配分機関の役割・義務等に関連する文書
重要技術のための青写真と行動計画」（Blueprint and Action Plan for Critical Technologies） ・国家利益のために重要技術を保護・促進するビジョンと戦略を提示 オーストラリア研究評議会 外国干渉対策フレームワーク（ARC Countering Foreign Interference Framework：CFI フレームワーク） ・NCGP 全体の国家安全保障リスクを管理するためのアプローチを概説。ARC は、研究が重要な技術に関連しているかどうかを特定することに加えて、次のような他のリスクが存在する可能性があるかどうかも考慮。 オーストラリア研究評議会法改正（改正 ARC 法） ・改正 ARC 法では、強化された研究セキュリティ審査が導入され、早期セキュリティスクリーニング／より広範なオープンソース証拠の使用／外国の所属と資金開示の要件の明確化・申請時及び資金提供プロジェクト過程で一貫的なリスク評価の支援（完全な開示）／リスク軽減に関する具体的な保証（UFIT ガイドラインに沿ったデュー・ディリジェンスの実施の証明）等を実施することになった。（⇒次節の注目事例参照）
資金配分機関における研究セキュリティ確保に関する取組の特色（ARC の事例調査に基づく）
・オーストラリア研究評議会（ARC）は、科学技術研究の競争的資金配分機関であり、競争的助成プログラムは、ARC 外国干渉対策フレームワークに沿って国家安全保障上のリスク管理を行っている。
参考となる点
・UFIT ガイドラインに沿って、ARC プロセスは管理・運営されている。資金配分機関として、助成金の審査プロセスにおいて、セキュリティ審査の前倒しや審査内容の詳細化、データ活用（オープンソース情報）を行っている。
資金配分機関における研究セキュリティ確保のための主な取組（ARC の事例調査に基づく）
【体制】 ・非公表 【情報提供】 ・ARC では、オープンソース情報のみを使用し、リスクレベルの決定を行っている。他方、オープンソース情報からリスクを発見・検証しているのは、情報収集のノウハウを有するセキュリティの専門家である。 【デュー・ディリジェンス】 ・2026 年開始の「ARC Centres of Excellence 2026」や「Discovery Projects 2026」では、最終的なデュー・ディリジェンス確認のために採択発表が延期されるケースも出ている。 【助成金公募等への実装（共通フォーム作成等）】 ・ARC は、助成金申請における外国干渉リスクの評価・軽減方法を定義するフレームワークを有する。 【教育・研修】 ・資金配分先の大学教員もしくは ARC の内部職員向けの教育・研修は現在実施していない。

⑤ 欧州連合

資金配分機関の役割・義務等に関連する文書
ホライズン・ヨーロッパプログラム規則 ・欧州最大の研究資金プログラム「ホライズン・ヨーロッパ」の運営、資金、申請と受給などの手続並びに申請者と受給者の責務を定めた規程。 EU 助成申請取扱指針 ・ホライズン・ヨーロッパ助成の申請者向けの指針。 ガイダンス書 ・規則や指針の具体的な取扱いに関する説明書。
資金配分機関における研究セキュリティ確保に関する取組の特色
・2021 年から 27 年までの 7 年間のプログラムに関する諸規定は、2019 年に対中政策の転換直後に定められ、重要技術の移転防止やデュアルユースの取扱を重点的に規制
参考となる点
・欧州委員会は研究セキュリティ施策に関して全般的な責任を持つが、その策定ではステークホルダーとの対話を重視 ・新しい方針や施策の策定時にはステークホルダーに対する意見募集を行う ・研究セキュリティと学問の自由の均衡維持を考慮
資金配分機関における研究セキュリティ確保のための主な取組
【体制】 ・研究・イノベーション総局（DG RTD）が担当も、対諜報リスク/外国からの干渉/重要技術の保護等担当の「移動と内務総局（DG Home)）並びに研究成果のデュアルユースを含む輸出管理を担う「通商総局（DG Trade)」と連携 【助成金公募等への実装（共通フォーム作成等)】 ・セキュリティに係る問題の一覧表に記入し（提出システム上で直接、または紙媒体にて)、問題があった場合にはその対応方法を説明するセキュリティ自己評価を合わせて提出 ・安全保障上の懸念を引き起こす可能性のある情報の使用もしくは生成を伴うプロジェクトにおいて、研究の潜在的な悪用を特定し適切に対処するための手順書を提示、申請者にはそれに沿う責務あり。 【他大学等との連携・情報共有】 ・EU 域内の大学と学術団体のそれぞれ代表する EUA と ALLEA との情報交換や情報共有を行い、またその連携によって研究セキュリティに関する欧州旗艦会議を開催

⑥ オランダ

資金配分機関の役割・義務等
NWO Grant Scheme, Netherlands Organisation for Scientific Research によるもの ・申請者は助成金の申請時に、当該大学・研究機関が「National Knowledge Security Guidelines」の要求事項に従って運営されていること、及び申請書が本ガイドラインに準拠していることを確認することを求める。 ・提案書または採択プロジェクトに、知識セキュリティに関するリスクが存在する可能性が示された場合、申請者またはプロジェクトリーダーに対し、リスク軽減策に関する説明を求める。
資金配分機関における研究セキュリティ確保に関する取組の特色（NWO の事例調査に基づく）
・「National Knowledge Security Guidelines」の公表を受け、知識セキュリティに関する評価手順および同研究機構傘下の研究所における対策実施に取り組んでいるとされる。 ・NWO 全体（資金調達プロセスに関わる全職員および同研究機構の 9 つの研究所勤務者全員）を対象に、知識セキュリティ意識向上の取り組みを推進しているとされる。
参考となる点
・助成金申請者による提案書または採択プロジェクトに知識セキュリティに関するリスクが存在する可能性が示された場合、申請者またはプロジェクトリーダーに対し、リスク軽減策に関する説明を求めることがあること。（⇒次節の注目事例参照） ・知識セキュリティ保護のため、助成金申請者に対して、助成金交付決定通知書に追加条件を付すことができること。
資金配分機関における研究セキュリティ確保のための主な取組（NWO の事例調査に基づく）
【体制】 ・知識セキュリティに関する 2 つのアドバイザリーチーム（資金調達プロセス担当職員向け及び研究所向け）を設置。 【情報提供】 ・NWO の Knowledge Security web サイトで、助成金申請者は「National Knowledge Security Guidelines」を遵守することを説明。 【デュー・ディリジェンス】 ・非公開 【助成金公募等への実装（共通フォーム作成等）】 ・各公募要領のサイトで 、公募申請用の添付書類として 「National Knowledge Security Guidelines」に遵守していることを確認するための、「Declaration knowledge security」という文書が設置されている。 【教育・研修】 ・非公開

⑦ ドイツ

資金配分機関の役割・義務等に関連する文書
資金提供研究プログラムのセキュリティ側面 ・ドイツ国内の大学或いは公的研究機関に所属する博士号の保持者を対象にした研究費の助成プログラムにおける注意事項に関する概説。 申請書作成説明書 ・研究プログラム申請者/受給者に対してデュアルユース取扱と外国貿易法の遵守を周知し、申請と受給時のチェックリストを提示し、その遵守を指示。
資金配分機関における研究セキュリティ確保に関する取組の特色
DFG ・資金提供機関だけでなく、ドイツの研究セキュリティ（デュアルユース中心）に関する取組を主導。 DLR-PT ・研究資金の運営等を担う研究プロジェクト運営機関であるが、関連文書やリポートを発行し、大学、研究者に情報を提供。
参考となる点
・DFG は単に資金配分機関とし資金配分業務を担うにとどまらず、研究セキュリティ関連文書の作成、模範文書の提示や大学とへの助言指導など、幅広い活動を担い、研究セキュリティにおける学術界主導モデルを提示。（⇒次節の注目事例参照）
資金配分機関における研究セキュリティ確保のための主な取組（DFG と DLR-PT の事例調査に基づく）
【情報提供】 ・ウェブサイト 【デュー・ディリジェンス】 ・DLR-PT は、評価のプロセスと範例からなるマニュアルを発行。 【助成金公募等への実装（共通フォーム作成等）】 ・DFG：申請書作成のための詳細な手順書の配布の他、ウェブ上で説明文を公開。 ・DFG：研究プロジェクトのドイツ国外在住の外国籍申請者の場合、二段階審査方式を導入。

(2) 注目事例

以下は資金配分機関の研究セキュリティ確保のための取組についての参考事例・注目事例である。

(a) 米国 NSF：規制、実装支援、能力構築、制度学習・評価の一体設計

CHIPS 科学法・NSPM-33 へ対応し、研究助成金支給の要件を明確化するだけでなく、SECURE Center 設立によって大学等の実務対応力の底上げや研修教材の作成、TRUST による審査段階のリスク把握の高度化を図り、さらに Research on Research Security 公募プログラム（RoRS）を通じて研究セキュリティ政策そのものを実証的に検証する知識基盤の育成に努めている。(30 頁参照)。

(b) 米国国防省：Decision Matrix 公開（透明性・予見可能性の向上）

米国国防省（DoD）は、国防省の構成機関およびプログラム担当者が、採択候補となった基礎研究提案に対して、どの程度のリスク低減措置を求めるかを判断するための実務上の

判断補助（decision aid）として Decision Matrix（決定マトリックス）を公開しており、審査判断基準の透明性と予見可能性が高い。（40 頁参照）

(c) カナダ NSERC：研究セキュリティ確保のための役割分担の明確化等

研究者は自己申告・フォーム提出・継続遵守の一次的責任を負い、大学・研究機関は主として支援・形式確認・連絡調整を担い、資金配分機関は独立した審査・検証プロセスを運用する。NSERC における審査・検証は研究者から提出された書類の中からサンプル抽出の上で行われ、必要に応じて、政府の公共安全省の支援を受けて行われる。（64 頁参照）

(d) 英国 UKRI：Trusted Research に関して原則の提示

UKRI は、TR&I（Trusted Research and Innovation）を、英国の知的財産、機微な研究、人材およびインフラを、潜在的な窃盗・悪用・搾取から保護する枠組みとして定義している。大学・研究機関が助成金を申請する際に、期待されるべき事項を示した「Trusted Research & Innovation: Principles and Expectations」を公表している。（97 頁参照）

(e) オーストラリア研究評議会（Australian Research Council）：ARC 法改正への対応

ARC に関しては、研究セキュリティに係る要件の強化に沿って、2024 年 7 月に ARC 法が改正され、国家安全保障、防衛、国際関係に関連する要件を強化した。法的要件を満たすため、ARC は政府機関や研究機関と緊密に連携し、研究セキュリティ体制を強化する。（124 頁参照）

(f) オランダ科学研究機構（NWO）：知識セキュリティの資金配分プロセスへの組み込み

NWO では、大学・研究機関が助成金の申請時に、国のガイドラインである「National Knowledge Security Guidelines」を遵守することの確認を義務化し、提案書または採択プロジェクトに知識セキュリティに関するリスクが存在する可能性が示された場合、リスク軽減策に関する説明を求める場合がある。（164 頁参照）

(g) ドイツ研究振興協会（DFG）：学術界の自己規律としての制度化

DFG の研究セキュリティ対応の特徴は、学術界の自己規律として制度化している点にある。DFG は国立科学アカデミー・レオポルディーナ（Leopoldina）と共同で、学問の自由と学術的責任を両立させる勧告を示し、Joint Committee を通じてその実装を支えている。（187 頁参照）

5.1.3　政府等の研究セキュリティ・インテグリティに関する方針・法令と、大学・研究機関の取組、資金配分機関の取組の関係

(1)　先行研究等

表 5-3 は、政府等の研究セキュリティ・インテグリティに関する方針・法令と、大学・研究機関の取組、資金配分機関の取組の関係などに関する先行研究や検討の結果を示す。

先行研究等の知見からは、研究セキュリティ・インテグリティの確保は、政府のみ、又は大学・研究機関のみが担うものではなく、政府、資金配分機関、大学・研究機関、学協会、研究者等の複数主体に責任が分散した形で進められるべきものとして理解されていることが分かる。国・地域によって異なり一概に言うのは難しいが、政府等は法令やガイドラインを通じて基本的枠組みを示し、資金配分機関はそれを助成条件、申請時のデュー・ディリジェンス、リスク開示、審査実務等に反映する媒介主体として機能し、大学・研究機関はこれを学内の体制、手順、研修、相談支援等として具体化していく構図が確認される。

また、先行研究は、効果的な制度設計として、比例的かつ体系的なリスク管理を重視するとともに、差別、国際共同研究の萎縮といった負の副作用や、過度な事務負担を抑制する必要性を指摘している。さらに、大学・研究機関においては、シニア・リーダーシップの関与、リスク管理枠組み、研究協定レビュー、物理・サイバー面の対応、組織横断的な体制、研修・教材整備等が主要な実装形態として指摘されている一方、何が実際に有効かを検証する評価研究はなお十分に蓄積されておらず、今後の重要な課題であることも示されている。

表 5-3　政府等の研究セキュリティ・インテグリティに関する方針・法令と、大学・研究機関の取組、資金配分機関の取組の関係に関連する先行研究等の主な知見

知見の内容	文献
研究セキュリティ・インテグリティの責任は、政府・資金配分機関・大学・研究機関・学協会などに分散している。	OECD (2022), p. 9.
効果的な制度は、比例的（proportionate）・体系的（systematic）なリスク管理であることが重要である。また、副作用としての差別、エスニック・プロファイリング、国際共同研究の萎縮を監視すべきである。	OECD (2022), pp. 12.
政府・資金配分機関は、研究セキュリティ措置による追加的な事務負担を最小化し、既存の申請・審査・報告プロセスを活用するのが望ましい。	OECD (2022), pp. 13-14.
資金配分機関は、政府方針を大学実務に反映する媒介装置として重要であり、申請時の due diligence、リスク開示、対象を絞った要件設定等を通じて、政策を実装する。	G7 (2023), p. 8; EU Council Recommendation (2024), pp. 6-7.
政府の役割は、大学・学協会に対して責任ある自己管理（responsible self-management）を促し、能力構築を支えることにある。	OECD (2022), p.12.
政府は枠組みを示すが、大学・研究機関には senior leadership レベルの責任者、リスク管理枠組み、研究協定レビュー、物理・サイバー面の機関的対応が求められる	G7 (2023), p. 9.
大学・研究機関は、政府の研究セキュリティ要求を、キャンパス横断の working groups / task forces、リスク評価委員会、国際活動やコンプライアンスを束ねる調整オフィスへと実装し対応する傾向がある。	AAU/APLU (2020), p.2.
政府方針に対する大学の対応は、研究公正研修への組込み、学内ウェブページや教材整備、研究者向けの重点研修、政府の安全保障機関との連携、輸出管理・訪問者管理・渡航支援等などとして現れる。	AAU/APLU (2020), p.2-7.
研究セキュリティ分野の制度は急速に整備されている一方で、何が本当に効果的かを測る評価研究はまだ弱い。現状では、研究者・研究活動への直接的影響、文化変化、負の副作用まで測る指標が十分に確立していない。	NASEM workshop highlights (2025), p. 3.

出典：1) OECD. Integrity and Security in the Global Research Ecosystem. OECD Science, Technology and Industry Policy Papers. June 2022. No. 130. https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/06/integrity-and-security-in-the-global-research-ecosystem_2bd8511d/1c416f43-en.pdf; 2) Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group. G7 Best Practices for Secure & Open Research. May 2023. https://www8.cao.go.jp/cstp/kokusaiteki/g7_2023/2023_bestpracticepaper.pdf; 3) Council of the European Union. Council Recommendation of 23 May 2024 on enhancing research security (C/2024/3510). 30.5.2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ%3AC_202403510; 4) Association of American Universities (AAU) and Association of Public & Land-grant Universities (APLU). University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus Updated. May 2020. https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/2020-Effective-Science-Security-Practices-Summary.pdf; 5) National Academies of Sciences, Engineering, and Medicine. 2025. Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop: Highlights, Washington, DC: The National Academies Press. /https://nap.nationalacademies.org/resource/29241/Highlights_Assessing_Research_Security_Efforts_in_Higher_Education.pdf

(2) 政府等の研究セキュリティ・インテグリティに関する方針・法令と、資金配分機関の取組、大学・研究機関の取組の関係

(a) 研究セキュリティ・インテグリティ確保と、政府、資金配分機関、大学・研究機関の果たす機能

表 5-4 では、研究セキュリティ・インテグリティに関する制度を、まず横軸として、①規範・規則設定機能、②リスク判断機能、③決定機能・決定権限、④支援・能力構築機能の四つに分けて整理している。これは、研究セキュリティ対応を規制の有無や、誰が担当するかといった整理にとどめず、制度の制定・運営においては、ルールを定める段階、個別案件を評価する段階、採否や条件付与等を決定する段階、さらにそれを現場で運用可能にする支援や能力形成の段階から構成されることを明確にするためである。とりわけ、②リスク判断機能と③決定機能・決定権限は、同一主体が担う場合もあれば分かれる場合もあるため、両者を区別して捉えることにより、制度の実際の構造をより精緻に把握することができると考えられる。

その上で、本表は、これら四つの機能が、政府等[561]、資金配分機関、大学・研究機関の各主体にどのように配分され得るかについて、本調査の事例調査（大学・研究機関、資金配分機関）における取組等を参考とし、概念的に整理したもの[562]である。先行研究で見たように、一般的には、政府等は、法令、政府方針、基本ガイドライン等を通じて制度全体の規範的枠組みを設定し、高リスク分野の提示や法令上の禁止・許可等を通じて大枠の判断及び決定を担う。他方、資金配分機関は、これを公募要領、申請様式、審査基準、条件付与等として具体化し、個別申請の審査、採択・不採択、資金停止等を通じて、政府方針を研究費配分の実務へ接続する媒介主体として機能する。これに対し、大学・研究機関は、学内規程、審査手続、契約審査ルール、訪問研究者管理、データ管理等を整備し、個別案件の一次評価や共同研究先のデュー・ディリジェンス、学内承認や条件付与等を通じて、研究現場に最も近い水準で制度を運用する主体である。さらに、研究者研修、相談窓口、事例集、ひな形整備、部局支援等の支援・能力構築機能は、制度を単なる規制にとどめず、実際に回る仕組みとして定着させる上で不可欠である。研究セキュリティ・インテグリティの確保は、各主体が、それぞれ異なる機能を担い、それらが相互に効果的に接続することによって成り立つものとして理解することが適切である。

なお、研究セキュリティの取組実施に関する政府と資金配分機関の関係と、政府と大学・研究機関の関係は、制度上同一ではない。一般に、資金配分機関は政府方針・法令に比較的近い位置にあり、助成条件、公募要領、審査手続等を通じてこれを具体化しやすいのに対し、大学・研究機関は数が多く、規模、研究分野、国際研究交流の態様等において多様であり、かつ学問の自由や機関自治が前提となるため、政府が一律に細部まで義務づけることには

561 国によっては、上位の規範・規則設定機能は政府とアカデミー、大学コミュニティ等とが共同で担うこともあり得る。

562 国・地域によって、あるいは同じ国・地域内においても資金配分機関、大学・研究機関の特色や考え方によって、各主体間の役割分担等は異なるものである。本表は概念的枠組みにより、取組等について一つの整理を試みたものであり、この限りではない。

限界がある。このため、大学・研究機関に対しては、政府は一定の枠組み、原則、期待事項を示しつつ、各機関が自らの状況に応じて具体的な体制、手順及び判断を構築する余地を残す傾向が強いと考えられる。他方、資金配分機関に対しては、政府方針・法令が助成条件や審査実務に比較的直接的に反映されやすく、政府の制度目的を具体的な制度運用へとつなぐ媒介主体としての性格が強いとみられる。

表 5-4　研究セキュリティ・インテグリティについての政府等、資金配分機関、大学・研究機関の機能と、取組例（概念的整理）

主体	① 規範・規則設定機能	② リスク判断機能	③ 決定機能・決定権限	④ 支援・能力構築機能
政府等	法令、政府方針、基本ガイドライン、対象分野・対象主体の設定等	高リスク分野の提示、情報提供、必要に応じた助言・照会対応等	法令上の禁止・許可、制裁、公的資金制度上の大枠決定等	全国向け教材、政府窓口、情報共有、大学等向け支援制度・支援組織設置等
資金配分機関	公募要領、申請様式、開示要件、審査基準、リスク緩和条件の設定等	個別申請の審査、追加資料要求、外部助言の取得、条件付けの検討等	採択・不採択、条件付き採択、資金停止、報告義務、リスク緩和措置付与等	申請者向けガイド、FAQ、研修、相談対応、実務コミュニティ形成等
大学・研究機関	学内規程、審査手続、契約審査ルール、訪問研究者管理、データ管理規程等	個別案件の一次評価、共同研究先のデュー・ディリジェンス、学内委員会審査等	連携実施の可否、条件付与、契約修正、学内承認・停止等	研究者研修、学内相談窓口、事例集、ひな形整備、部局支援、地域機関連携等

出典）未来工学研究所が作成。

(b)　政府等の研究セキュリティ・インテグリティに関する方針・法令と、大学・研究機関の取組の関係

表 5-5 は、大学・研究機関における研究セキュリティ・インテグリティ対応を、まず縦軸について、事例調査を通じて確認された 6 つの機能（231 頁参照）に基づいて概念的に整理したもの[563]である。すなわち、政府方針等を学内の規程・体制に具体化する機能、個別案件に関するデュー・ディリジェンス及び判断機能、周知・教育・研修機能、相談対応・手続支援等の運用支援機能に加え、一部の大学・研究機関でみられる、他機関との連携・情報共有機能、研究理念・価値観を踏まえた主体的判断する機能の 6 つである。

その上で、本表は横軸について、各機能に対応する取組を、a. 義務として課される取組、b. 実施が期待される取組、c. 大学・研究機関が自主的に行う取組の三つに区分している。これは、大学・研究機関の対応が、すべて一律に法令や政府方針によって決まるものではなく、法的・制度的に必ず実施すべき事項、政府や資金配分機関が望ましい実務として示す事項、さらに各機関が自らの判断で主体的に行う事項とが組み合わさり構成されていることを示すためである。

563 国・地域と大学・研究機関の特色や考え方によって、研究セキュリティ・インテグリティについての大学・研究機関の機能と、対応する取組例（義務的取組、期待される取組、自主的取組）は異なるものである。本表は概念的枠組みにより、取組等について一つの整理を試みたものであり、この限りではない。

このように整理すると、政府等の研究セキュリティ・インテグリティに関する方針・法令と大学・研究機関の取組の関係は、単なる規制と遵守の関係としてではなく、政府等が示す法令、ガイドライン、資金配分条件等（これらは国・地域、あるいは資金配分機関によって異なる）を基礎としつつ、多様な特性（規模、学問分野、国際研究協力の大小等）を有する大学・研究機関がこれを学内の規程、手順、教育、支援、個別案件判断等として具体化し、必要に応じて自主的な補完を加える関係として捉えることができる。

表 5-5　研究セキュリティ・インテグリティについての大学・研究機関の機能と、取組例（義務的取組、期待される取組、自主的取組）（概念的整理）

大学・研究機関の機能	a. 義務として課される取組の例	b. 実施が期待される取組の例	c. 大学・研究機関が自主的に行う取組の例
① 政府方針・法令・資金配分条件等を学内の規程、手順及び体制に具体化する機能	法令、政府方針、資金配分条件に基づき、必ず整備すべき規程、届出手順、担当部署、審査手続等	政府・資金配分機関が望ましい実務として示す体制整備、手順整備、責任者配置等	他の参考事例や自大学の方針を踏まえ、自主的に整備する規程、委員会、体制等
② 個別案件についてデュー・ディリジェンス、確認及び必要な判断を行う機能	申請時確認、相手先確認、輸出管理確認、機微技術該当性確認など、義務として実施すべき案件審査等	高リスク案件に対する追加確認、外部照会、条件付対応など、実施が期待される審査・判断等	自大学独自の高リスク基準、追加レビュー、倫理・価値判断を含む案件判断等
③ 研究者及び関係職員に対する周知、教育及び研修を行う機能	必修研修、法令遵守教育、申請者向け義務的周知等	研究者・職員向け啓発・説明、テーマ別研修など、推奨される教育等	独自教材、ケーススタディ、部局別研修、理念共有のためのプログラム等
④ 研究者からの相談対応、手続支援及び学内調整を通じて実務運用を支える機能	必須窓口、申請支援、学内報告・連絡調整など、制度運用上必要な支援等	相談体制、FAQ、事前相談、案件伴走支援など、期待される支援等	研究者に寄り添ったハンズオン支援、契約支援、国際連携支援の独自拡充等
⑤ 他大学等との連携・情報共有を通じて知見共有や対応能力向上を図る機能	政府施策・枠組みに基づく情報共有、通報、共同対応等	政府・大学団体・地域ネットワーク等を通じた知見共有、共同研修等	大学間コミュニティ形成、独自ネットワーク、実務者会合、相互学習等
⑥ 大学・研究機関としての価値観や研究理念を踏まえ、国際研究交流に伴うリスクを主体的に判断する機能	（人権、倫理、安全保障上の法的禁止・制約への適合）	政府等が示す価値原則や責任ある国際連携の考え方を踏まえた判断	学問の自由、開放性、研究理念、大学のミッションに基づく独自の判断基準や意思決定、重要テーマの調査研究等

注）どのような取組が義務として課されるか、期待されるのかは国・地域、政府・資金配分機関の示す方針、ガイドライン、公募要件等によって異なり、それら自体の優劣について判断するものではない。

出典）未来工学研究所が作成。

(c) 政府等の研究セキュリティ・インテグリティに関する方針・法令と、資金配分機関の取組の関係

表 5-6 は、資金配分機関における研究セキュリティ・インテグリティ対応を、5 つの機能（243 頁参照）に分けて同様に概念的に整理したもの[564]である。政府方針・法令を助成条件や審査実務に具体化する機能、個別案件に対するリスクベースの確認・審査・判断機能、大学・研究機関におけるデュー・ディリジェンス及びコンプライアンス体制の整備を促す機能、制度運用を支える支援・能力構築機能、制度運用の評価・検証・知見形成機能の 5 つである。

また、本表では、これら 5 つの機能に対応する取組を、上表と同様に、a. 義務として課される取組、b. 実施が期待される取組、c. 資金配分機関が自主的に行う取組の 3 つに区分して例示している。ここで示した取組内容は、各機能がどのような形で現れ得るかを示すための例であり、各国・地域の方針、資金配分機関の性格や権限に応じて、その具体的内容や重心の置き方は異なり得る。

表 5-6 研究セキュリティ・インテグリティについての資金配分機関の機能と、取組例（義務的取組、期待される取組、自主的取組）（概念的整理）

資金配分機関の機能	a. 義務として課される取組の例	b. 実施が期待される取組の例	c. 資金配分機関が自主的に行う取組の例
① 政府方針・法令を助成条件や審査実務に具体化する機能	法令、政府方針、ガイドライン等に基づき、助成条件、申請様式、開示要件、審査手順等として必ず反映すべき事項等	政府等が望ましい実務として示す事項を踏まえ、公募要領、FAQ、内部手順等に組み込むこと	独自の審査基準、補足ガイダンス、内部ルール等
② 個別案件に対するリスクベースの確認・審査・判断機能	特定案件について、法令・制度上求められる確認、追加資料徴求、リスク審査、条件付与、不採択判断等	高リスク案件への重点審査、外部助言の活用、追加的な確認プロセス等	独自のリスク指標、分析ツール、審査手法、重点分野の追加レビュー等
③ 大学・研究機関におけるデュー・ディリジェンス及びコンプライアンス体制の整備を促す機能	受給機関に対し、必要な体制整備、責任者配置、認証、報告、手続整備等を求める等	望ましい体制整備、学内手順、デュー・ディリジェンス実施、内部統制の強化を促す等	大学・研究機関の体制整備を後押しするため、独自の要件、モデル、支援枠組み等を設けること等
④ 制度運用を支える支援・能力構築機能	制度上必要な説明、問い合わせ対応、必須研修、提出支援等を行うこと	ガイダンス、研修、ワークショップ、相談窓口、事例共有等を通じて運用支援等	独自教材、コミュニティ形成、専門支援チーム、伴走支援、実務者ネットワーク等
⑤ 制度運用の評価・検証・知見形成機能	政府等から求められる制度実施状況の年次報告、点検、監査対応、データ提出等	制度の運用状況の把握、改善提案、効果検証、知見の整理等	自主的に評価研究、外部評価、ケース分析、知見の蓄積・公表等

注）どのような取組が義務として課されるか、期待されるのかは国・地域、政府の示す方針、ガイドラインによって異なり、それら自体の優劣について判断するものではない。

出典）未来工学研究所が作成。

[564] 国・地域と資金配分機関の特色や考え方によって、研究セキュリティ・インテグリティについての資金配分機関の機能と、対応する取組例（義務的取組、期待される取組、自主的取組）は異なるものである。本表は概念的枠組みにより、取組等について一つの整理を試みたものであり、この限りではない。

(3) まとめ

先行研究の知見及び事例調査に基づき、政府等の研究セキュリティ・インテグリティに関する方針・法令と、大学・研究機関の取組、資金配分機関の取組の関係を整理した。政府、資金配分機関、大学・研究機関が、それぞれ異なる機能を担いながら相互に接続することによって成立する事が分かる。政府等の方針・法令と各主体の取組の関係は、規制と遵守の関係というより、それぞれに応じた役割分担と責任を伴う関係として捉えることができる。また、大学・研究機関及び資金配分機関の取組は、いずれも、義務として課される取組、実施が期待される取組、自主的に行う取組が重層的に組み合わさることによって構成されている。

このように、研究セキュリティ・インテグリティに関する制度の比較に当たっては、政府の方針・関与の強弱をみるのではなく、どの主体がどの機能を担い、それが義務、期待、自主的取組のいずれとして構成されているかを多面的に把握することが重要と考える。さらに、何が実際に有効かを示す評価研究はなお十分ではなく、今後は制度運用の評価・検証を通じて知見を蓄積していくことが課題である。

5.2　研究インテグリティと研究セキュリティについての意見交換会の実施

意見交換会の実施概要

本調査では、研究インテグリティと研究セキュリティに関する政府方針や大学・研究機関の取組に関する講演と、実務担当者による意見交換を行うため、2025 年 12 月～2026 年 1 月に計 3 回の意見交換会を開催した。意見交換とネットワーク形成を重視し、対面形式（東京 2 回、大阪 1 回）で実施した。

対象は、大学・研究機関・企業等において研究インテグリティ確保に関係する業務の担当者（教職員、研究者、事務担当者等）であり、各回 45 名程度を定員として募集した。主催は内閣府、事務局は未来工学研究所である。

プログラム構成

3 回とも、前半を講演、後半をグループ討議とする共通構成で実施した。講演では、内閣府から政策動向、有識者から大学・研究機関の実務事例、未来工学研究所から調査分析結果を共有した。

グループ討議では、①課題認識の共有、②各機関の取組の共有、③今後の解決策・アクションの検討（第 1・2 回は主に課題共有）を行い、最後に全体共有・講評を実施した。討議は 4～7 名程度の少人数グループで行い、各グループに事務局モデレータを配置した。自由な発言を確保するため、チャタムハウスルールを適用した。

参加状況

参加者は計 85 人、参加機関は計 62 機関（国立大学等 20、公立大学 4、私立大学 23、国立研究開発法人等 15）であった。地域別では、東京開催回は関東、大阪開催回は近畿からの参加が中心であったが、北海道、東北、中国、四国、九州・沖縄からの参加もあり、全国的な広がりが確認された。

意見交換会に対する評価（事後アンケート）

各回終了後の事後アンケートでは、内閣府講演、有識者講演、未来工学研究所講演、グループ討議、意見交換会全体について評価を把握した。講演 3 件（内閣府・有識者・未来工学研究所）は、いずれも理解促進や論点整理に有益であったとの評価が多く、全体として概ね好評であった。

特に、主目的であるグループ討議については、回答率約 7 割のうち、約 5 割が「とても参考になった」、約 9 割が「とても参考になった」又は「参考になった」と回答し、満足度は高かった。他機関の担当者と課題や対応策を共有できたこと、同様の悩みを抱える機関が多いことを確認できたことなど、ネットワーキングと相互学習の効果が評価された。

意見交換会全体としては、継続開催への期待が強く、対面開催による実務的知見の共有や人材ネットワーク形成の意義が再確認された。他方、国による継続的支援（予算・情報提供・共通ツール等）等の課題も抽出された。

グループ討議の概要と主な示唆

（1）課題認識

研究インテグリティ・研究セキュリティに関して、研究者に「何を守るための取組か」「なぜ必要か」を伝えにくいという問題意識が共有された。また、個別案件でのリスク評価・判断基準も課題であり、結果として「念のため止める」といった過度に慎重な運用に傾きやすい。加えて、人員・専門性・継続性の不足、情報分散、研修の浸透の難しさ、学生の位置づけの曖昧さなども共通課題として示された。

（2）各機関の取組

各機関では、規程整備、相談窓口・委員会の設置、研修・e-learning・学内周知など、基礎的な体制整備が進められている。実務面では、チェックリスト、申告書、自己申告に基づく確認運用が主流であり、共同研究、兼業、出張、外部資金、契約等の場面で個別相談・個別対応を行う体制が整えられつつある。

また、外部会議・セミナー等からの情報収集、リスク場面を図解等で示す教育資料の工夫、外部ツールやAI活用への関心、部署横断での情報集約（兼業、出張、外部資金等）などの取組も共有された。他方で、機関間の成熟度には大きな差があり、多くの機関はなお「基礎整備から実効運用への移行期」にある。

（3）今後の方向性

今後の方向性として禁止・抑制中心ではなく、条件整理により研究を前に進めることが示され、概念整理、Q&A、ケース集、判断基準、行動規範などの必要性、ベースライン提示への期待が示された。

また、実装の鍵として、研究支援、契約、国際、輸出管理、IT／サイバー、法務等をつなぐ組織横断型の実務ガバナンス、デュー・ディリジェンスを担う人材の育成、判断ログや事例蓄積によるナレッジ継承の仕組みが示された。あわせて、ユーザビリティを重視した研修・啓発の設計、対象者別のメッセージ設計、地域の中核大学等をハブとした機関間ネットワークの整備、小規模機関向け支援機能の構築が有効な方策として示された。

参考文献

全般

Association of American Universities (AAU) and Association of Public & Land-grant Universities (APLU). *University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus*. Updated. May 2020.

Council of the European Union. *Council Recommendation of 23 May 2024 on enhancing research security* (C/2024/3510). 30.5.2024.

National Academies of Sciences, Engineering, and Medicine. 2025. *Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop: Highlights*, Washington, DC: The National Academies Press.

OECD. *Integrity and Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers. June 2022. No. 130.

Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group. *G7 Best Practices for Secure & Open Research*. May 2023.

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）「研究開発の俯瞰報告書 主要国・地域の科学技術・イノベーション政策動向（2025 年）」

未来工学研究所「研究インテグリティ（Research Integrity）に係る調査・分析報告書」2022 年度内閣府委託調査．2023 年 3 月．

未来工学研究所「研究インテグリティ（Research Integrity）に係る調査・分析報告書」2023 年度内閣府委託調査．2024 年 2 月．

野村総合研究所「研究インテグリティ（Research Integrity）に係る調査・分析及び G7 オンラインプラットフォーム「バーチャルアカデミー」の運営支援・分析」調査報告書．2024 年度内閣府委託調査．2025 年 2 月．

米国

Congressional Research Service. *Federal Research Security Policies: Background and Issues for Congress*. May 20, 2025. R48541.

Department of Defense. *Fundamental Research Guidance*. August 4,2025.

Department of Defense. *Policy for Risk-based Security Reviews of Fundamental Research*. June 8, 2023.

Department of Defense. *Introduction to Fiscal Year 24 Lists Published in Response to Section 1286 of the National Defense Authorization Act for Fiscal Year 2019* (Public Law 115-232), as amended. June 24, 2025.

Defense Advanced Research Projects Agency (DARPA) Fundamental Research Risk-Based Security Review Program (FRRBS) Frequently Asked Questions (FAQs).

GAO. *Research Security: Agencies Should Assess Safeguards Against Discrimination*. GAO-26-107544. Jan 21, 2026.

JASON, *Fundamental Research Security*. JSR-19-2. 2019.

Massachusetts Institute of Technology. *MIT Facts 2020*. January 2020.

Massachusetts Institute of Technology. *A Global Strategy for MIT*. Richard K. Lester. May 2017.

Massachusetts Institute of Technology. *Review and Reassessment of MIT's Relationships with the Kingdom of Saudi Arabia: A Report to President L. Rafael Reif.* Professor Richard K. Lester. January 31, 2019.

Massachusetts Institute of Technology. *University Engagement with China: An MIT Approach Final Report*. November 2022. The MIT China Strategy Group

National Academies of Sciences, Engineering, and Medicine. *Assessing Research Security Efforts in Higher Education: Proceedings of a Workshop*. Washington, DC: The National Academies Press, 2025.

National Academies of Sciences, Engineering, and Medicine. 2025. *National Science, Technology, and Security Roundtable Capstone: Proceedings of a Workshop*. Washington, DC: National Academies Press.

National Academies of Sciences, Engineering, and Medicine. *Simplifying Research Regulations and Policies: Optimizing American Science*. Washington, DC: The National Academies Press, 2025.

National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022.

National Science Foundation. FY2025 Agency Financial Report. Other Information 2A: Memorandum on FY 2026 Management Challenges Challenge 3: Mitigating Threats to Research Security.

NSF SECURE Center. *Research Security Briefing* Vol. 1 No.11: September 11, 2025.

Office of Science and Technology Policy. *Guidelines for Research Security Programs at Covered Institutions*. July 9, 2024.

Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. *Fox in the Henhouse: The U.S. Department of Defense Research and Engineering's Failures to Protect Taxpayer-Funded Defense Research*. September 2025.

Select Committee on the Strategic Competition between the United States and the Chinese Communist Party and the Committee on Education and the Workforce. *Joint Institutes, Divided Loyalties: How the Chinese Communist Party Exploits U.S. University Partnerships to Empower China's Military and Repression*. September 2025.

Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. *From Ph.D. to PLA: How Visa Policies Enable PRC Defense Entities*

to Tap U.S. Higher Education. September 2025.

Select Committee on China, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence. *Containment Breach: The U.S. Department of Energy's Failures in Research Security and Protecting Taxpayer-Funded Research from Foreign Exploitation*. December 17, 2025.

Texas A&M University System, *Regulation 15.05.04 High Risk Global Engagements and High Risk International Collaborations* (revised 2025/11/4)

Texas A&M University System, *Board of Regents Agenda Item No. 6.18* (Aug. 17, 2023), "Establishment of the Research and Innovation Security and Competitiveness Institute"

US Whitehouse. Presidential Memorandum on United States Government-Supported Research and Development National Security Policy. Issued on: January 14, 2021. National Security Presidential Memorandum – 33

Zuber, Maria T. *Written Testimony for House Committee on Science, Space and Technology Subcommittee on Investigations and Oversight.* March 5, 2025.

カナダ

Council of Canadian Academies (CCA). *Balancing Research Security and Open Science*. October 2025.

Council of Ontario Universities. *A Shared Commitment by Universities to Protect Ontario's Research*. June 2025.

Government of Canada. *National Security Guidelines for Research Partnerships*. 2021.

Government of Canada. *Annual Report on the Implementation of Research Security Policies within the Federal Granting Agencies and the Canada Foundation for Innovation 2023-2024*. October 2025.

Government of Canada. Innovation, Science and Economic Development Canada. *Policy on Sensitive Technology Research and Affiliations of Concern.* January 2024.

Government of Canada. Innovation, Science and Economic Development Canada. *Sensitive Technology Research Areas*. January 2024.

Government of Canada. Innovation, Science and Economic Development Canada. *Named Research Organizations.* January 2024.

Public Safety Canada. *Evaluation of the Funding to Build Canada's Research Security Capacity*. July 2025.

英国

Universities UK, "Managing risks in Internationalisation: Security related issues," October, 2020.

UUK/NPSA/UKRI, "Managing risks in international research and innovation: An overview

of higher education sector guidance,” June 2022.

NPSA, “Trusted Research Guidance for Academics,” July 2025.

UKRI, “UK Research and Innovation Trusted Research and Innovation Principles,” August 2021.

オーストラリア

Department of Education, Australian Government *Guidelines to Counter Foreign Interference in the Australian University Sector*. October 2021.

Department of Education. *Due Diligence Assistance Framework*. 2021.

Department of Education. *Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector*. August 2023.

University Foreign Interference Taskforce Transnational Education Working Group. *Guidance Note on Due Diligence*. June 2023.

University Foreign Interference Taskforce Transnational Education Working Group. *Guidance Note：Governance and risk frameworks*. February 2025.

University Foreign Interference Taskforce Transnational Education Working Group. *Guidance Note：Communication, education and knowledge sharing*. February 2025.

University Foreign Interference Taskforce Transnational Education Working Group. *Guidance Note：Cybersecurity*. February 2025.

University Foreign Interference Taskforce Transnational Education Working Group. *Case studies: Governance and risk frameworks*. February 2025.

University Foreign Interference Taskforce Transnational Education Working Group. *Case studies: Due diligence, risk assessments and management*. February 2025.

University Foreign Interference Taskforce Transnational Education Working Group. *Case studies: Cybersecurity*. February 2025.

欧州連合

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）「研究開発の俯瞰報告書　主要国・地域の科学技術・イノベーション政策動向（2025 年）」

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）「海外調査報告書：EU の研究・イノベーション枠組みプログラム・Horizon Europe」（2021 年）

JST 研究開発戦略センター「諸外国における研究セキュリティの取組み」（2024 年 10 月 17 日）

Emma Leenders, Duncan Liefferink & Sandrino Smeets “Leadership in EU policy-making：a deep dive into the extension of the EU emissions trading system,” Journal of European Public Policy, Volume 32, Issue 7 (2025)

ドイツ

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）「研究開発の俯瞰報告書　主

要国・地域の科学技術・イノベーション政策動向（2025 年）」

JST 研究開発戦略センター「諸外国における研究セキュリティの取組み」（2024 年 10 月 17 日）

Nicolas V. Rüffin, Katharina C. Cramer, Maximilian Mayer, Philip J. Nock, “Research Security” in Germany and the United States: Shifting Governance of Scientific Collaboration Under Geopolitical Pressure,” Global Policy (12 November 2025)

Katarina Zimmer “A structured system: the secrets of Germany’s scientific reputation,” Nature (27 November 2025)

オランダ

Government of the Netherlands, “National knowledge security guidelines: Secure international collaboration,” January 2022.

Universities of the Netherlands, “Capability Maturity Model Knowledge Security,” April 19, 2024.

イタリア

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）「科学技術・イノベーション動向報告・イタリアの研究開発システムの概要」（2009 年 4 月）

Daniel Pizzalato, “Bad apples or systematic problem? Is Italy struggling with maintaining high level of research integrity?” Ethics, Integrity and Policy, Vol. 32, Issue 4 (2025)

内閣府 科学技術・イノベーション推進事務局委託調査
令和７年度科学技術基礎調査等委託事業

「研究セキュリティ・インテグリティ（Research Security and Research Integrity）に係る調査・分析及びＧ７オンラインプラットフォーム「バーチャルアカデミー」の運営支援・分析」報告書

2026 年 2 月

公益財団法人　未来工学研究所
〒135-8473　東京都江東区深川 2-6-11　富岡橋ビル 4F
電話：03-5245-1015（代表）