令和５年度内閣府委託事業

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

令和６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５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「研究インテグリティ（Research Integrity）に係る調査・分析」の成果を取りまとめたものです。

― 目　次 ―

― 図 目 次 ―

― 表 目 次 ―

エグゼクティブ・サマリー

近年、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おり、Ｇ７をはじめとする我が国と価値観を共有する国において、リスクへの対策は進展してきている。

こうした中、我が国としても研究環境の基盤となる価値を守りつつ国際的に信頼性のある研究環境を構築することが、必要な国際協力及び国際交流を進めていくために不可欠となっており、2021 年 4 月には「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティの確保に係る対応方針について」（統合イノベーション戦略推進会議）が決定された。同対応方針では、政府は、研究者及び大学・研究機関等における研究の健全性・公正性（研究インテグリティ）の自律的な確保を支援すべく、研究者、大学・研究機関等、研究資金配分機関等と連携しながら、研究者による適切な情報開示に関する取組、研究者の所属機関における対応に関する取組、研究資金配分機関等における対応に関する取組等について着手することとされており、さらに、その際には、諸外国の動向を踏まえ適時必要な検討を実施すること、大学・研究機関等と対話を継続的に行い情報提供を行う等に留意することとされている。

このような状況を背景として、本委託事業では、第 1 に、各国・地域における研究インテグリティに対する取組状況を調査・分析し、適宜我が国の取組と比較・分析するとともに、第 2 に、大学・研究機関の研究インテグリティの確保に係る取組の現状・課題・要望を把握することを目的に、7 大学と 3 国立研究開発法人に対してヒアリングを実施し、第 3 に、日本における研究インテグリティに対する意識醸成、課題等の抽出・整理、関係者のネットワーク形成をすることを目的に、大学・研究機関の教員・研究者・職員を対象に研究インテグリティについての意見交換会を 3 回実施した。

なお、政府では、研究インテグリティを、従来明示的に対応してきた不正行為や、産学連携における利益・責務相反に対する適切な対応や安全保障貿易管理等の法令順守などに加え、研究の国際化やオープン化に伴う新たなリスクに対して新たに求められる研究者や研究組織としての「規範」、すなわち新たに確保が求められる研究の健全性・公正性のこととしている。本調査では「研究インテグリティ」は、特に断りがない場合には、「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティ」を意味する用語として用いており、また、研究不正行為の防止・対応、産学連携活動に伴う利益相反、安全保障輸出管理に関連する取組等に関しては、調査の範囲とはしていない。

他方、「研究セキュリティ」、すなわち外国や非国家による研究への干渉を防ぐことは「研究インテグリティ」を強化することになり、また、透明性を高め、潜在的な利益相反や責務相反を開示し、リスクを管理することで「研究インテグリティ」を強化することは「研究セキュリティ」を守ることになるという相互関係にある[1]ことから、研究の国際化、オープン

[1] OECD. *Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers. June 2022 No. 130. p.12

化に対するリスクへの対応について、国際的には研究セキュリティ・研究インテグリティというトピックとして議論されており、本報告書では「研究セキュリティ」の内容も調査の対象としている。

１．各国・地域における研究インテグリティに対する取組状況

各国・地域における研究インテグリティに対する取組状況を、米国、英国、オーストラリア、カナダ、欧州連合（EU）、ドイツ、フランス、スウェーデン、ノルウェー、フィンランド、デンマーク、オランダ、チェコ共和国、ニュージーランド、韓国、台湾、イスラエル（17 国・地域）について調査した。

なお、昨年度までに実施した内閣府委託調査で調査を既に行った国については、本委託調査は特に 2023 年度以降の動きを把握することに主眼があるが、対象国における研究インテグリティ確保のための取組を把握する上で必要な場合には 2022 年度までの動きについても適宜記述している。また、特に、研究活動の国際化、オープン化に伴うリスクの管理に関して公表されている文書等（リスクの分類、リスクの判断基準、リスク判断のフロー、事例・想定事例等が記載されている文書等)を詳細に調査した。研究インテグリティについての昨年度までの内閣府委託調査で調査対象としなかった国・地域については、これまでの動きも含めて記述した。

1.1　米国における研究インテグリティ確保のための取組

米国では、トランプ前政権が政権交代直前の 2021 年 1 月 14 日に「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」（*National Security Presidential Memorandum-33*（NSPM-33））を発出した。

バイデン大統領は、2021 年 1 月の大統領就任後に NSPM-33 を追認する一方で、トランプ政権下の 2018 年に司法省で始まった、大学・研究機関の中国のスパイ研究者の摘発キャンペーンである「China Initiative」については 2022 年 2 月に終了させた。

2022 年 1 月 4 日、大統領府科学技術政策局（OSTP）は、「NSPM-33 実施ガイダンス」（*Guidance for Implementing National Security Presidential Memorandum 33*（NSPM-33））を発表した。同文書の目的は、「連邦省庁に対し、NSPM-33 の実施に関する指針を提供すること」であり、各機関がその実施努力に適用すべき一般的なガイダンス（general guidance）に続き、NSPM-33 で取り上げられた、研究セキュリティの確保に関連する 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の結果、4. 情報の共有、5. 研究セキュリティプログラム）についての詳細なガイダンスが含まれている。

このように、米国では研究セキュリティの確保のために大統領覚書（NSPM-33）が大統領から、その実施ガイダンスが大統領府 OSTP が事務局を務める委員会から発出され、それらとともに 2020 年度国防権限法（2019 年 12 月）、2021 年度国防権限法（2021 年 1 月）、

CHIPS and Science Act（2022 年 8 月）に関連する条項が規定されている。このように、法令面では「研究セキュリティ」の確保について、法律や連邦政府大統領府レベルで規定されており、また、体制面では米国科学財団（NSF）、国立衛生研究所（NIH）等の資金配分機関や、CIA や FBI といった情報機関を含む関連する連邦省庁が一体となって、研究者、大学・研究機関、資金配分機関に対して、研究セキュリティ確保のための様々な要求や支援を行うことが大きな特色である。[2]

その後、上記の大統領覚書（NSPM-33）の実施ガイダンスや、CHIPS and Science Act（2022年8月）の関連条項で政府が実施を求められていることなどが順次実施されてきている。NSFにおいて研究セキュリティ担当課の設置、「研究セキュリティプログラム」のドラフト策定、「研究セキュリティ・インテグリティ情報共有分析組織」の設置準備、研究セキュリティについてのオンライン教育モジュールの開発などが行われている。

1.2　英国における研究インテグリティ確保のための取組

英国においては、「Trusted Research」という統一的な枠組みで、政府機関、大学機関及び R&D 資金配分機関が一体となって、大学・研究機関における研究インテグリティの取組を支援してきた。本年度においては、特に目立った動きはないが、内閣府から、RCAT（Research Collaboration Advice Team）の 2022 年から 2023 年にかけての活動状況に関する情報を中心として、RCAT に関する情報がアップデートされている。また、UUK（Universities UK）が、2020 年 10 月に公表した「Managing risks in internationalization: Security related issues」に関連して、大学が直面する安全保障上の脅威、安全保障の脅威に対処するために多くの大学が講じている措置、大学で安全保障ガイダンスを実装する方法、大学全体で安全保障を重視する文化を根付かせる方法等について纏めたものが、UUK のウェブサイト上に公開されている。

1.3　豪州における研究インテグリティ確保のための取組

豪中関係の悪化を背景に、豪州では 2019 年 8 月に、政府と大学・研究機関が共同してタスクフォース（University Foreign Interference Taskforce: UFIT）を設置した。政府側は教育省だけでなく内務省や国防省などが入っているのが特徴である。

UFIT は 2019 年 11 月、外国干渉を排除するための通称・UFIT ガイドライン（Guidelines to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表した。２年後の 2021 年 11 月に改定されている。豪州の大学・研究機関における外国干渉セキュリティの一連の審査は、同ガイドラインに基づいて行われている。

UFIT を構成するアクターの中では、とりわけ豪州研究評議会（Australian Research

[2] 以上の説明については、「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）に基づく（pp.viii~xi）。

Council: ARC）の役割が大きいが、ARC では 2018 年 7 月以降、教育省の指示のもとで主要な国家安全保障機関と協力し合い、政府資金による研究の申請プロセスに対する監視を強化するようになった。

また、2022 年 3 月には、豪州連邦議会のインテリジェンスとセキュリティに関する議会合同委員会（PJCIS）は大学・研究機関の安全保障上のリスクに対し 27 の勧告をした。

2023 年 8 月には、UFIT ガイドラインの制定後の大学における外国干渉リスクへの対応の取組状況についての報告書が公表された。取組状況の調査には 42 のオーストラリアの大学、8 つの関連団体、9 政府機関が参加した。外国干渉を管理するための万能の戦略は存在しないこと、大学はサイバー攻撃のリスクを認識し UFIT ガイドラインで言及されている以上の防護策に取り組んでいること、政府からの頻繁で具体的な情報共有がガイドラインの継続的な実施を支援すること、などが指摘されている。

1.4　カナダにおける研究インテグリティ確保のための取組

2020 年 9 月にカナダ政府は、カナダ政府・大学共同ワーキンググループ（Government of Canada-Universities Working Group）が開発した「Safeguarding Your Research Portal」[3]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。

2021 年 7 月に、カナダ政府は、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、「国際研究協力に対する国家安全保障ガイドライン（National Security Guidelines for Research Partnerships）」を作成・公表した。同ガイドラインは、外国政府や関係者に関連する潜在的な国家安全保障上のリスクからカナダの研究エコシステムを守ることの重要性を強調している。研究パートナーシップの開発、評価、資金提供におけるデューディリジェンス、リスク評価、リスク緩和に焦点を当てている。ガイドラインは、カナダの安全保障を脅かしたり、経済や社会を混乱させたりする可能性のある、外国からの干渉、スパイ活動、望ましくない知識の移転からカナダの研究を守ることを目的としており、NSERC のような資金配分機関への助成金申請に際し外国影響についてのリスクアセスメントが要請されている。

2024 年 1 月 16 日の 3 大臣声明（イノベーション・科学・産業大臣、保健大臣、公安大臣）で、カナダの研究を外国の影響や国家安全保障上のリスクから守るための新たな措置を紹介している。これらの措置には、「機微技術研究と、懸念される提携に関する政策」（*Policy on Sensitive Technology Research and Affiliations of Concern*）、「研究セキュリティセンター」（Research Security Centre）の設立、「研究支援ファンド」（Research Support Fund）を通じた高等教育機関への 5,000 万ドルの投資が含まれている。「機微技術研究と、懸念される提携に関する政策」は、研究助成金申請のガイドラインを定めるものであり、機微技術

[3] カナダ政府ウェブサイト” About the Government of Canada – Universities Working Group”<https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/about-government-canada-universities-working-group>

分野において、リスクをもたらす可能性のある海外の軍事・国家安全保障に関係する組織と提携することを警戒しており、機微技術分野のリストと、懸念すべき海外大学・研究機関のリストを合わせて公表した。この方針は、カナダの研究を保護し、その協力的でオープンな性質を維持することを目的としている。

2024 年初頭から、大学または関連研究機関が、連邦資金配分機関およびカナダ・イノベーション財団（Canada Foundation for Innovation）に機密技術研究分野を発展させる研究についての研究助成金申請書を提出した場合、その助成金で支援される活動に関与する研究者のいずれかが、カナダの国家安全保障に危険をもたらす可能性のある軍、国防、または国家安全保障機関と関係のある大学、研究機関、研究所に所属している場合、またはそこから資金や現物支援を受けている場合は、資金提供されなくなる。

1.5　欧州連合（EU）における研究インテグリティ確保のための取組

2021年5月、欧州委員会は、国際的な研究・イノベーション政策のための新たな欧州戦略の概要を示した「研究・イノベーションへのグローバルなアプローチに関するコミュニケーション」を発表した[4]。これを受けて、欧州理事会は2021年9月、研究セキュリティに共同で取り組むことを政治的使命とする理事会結論を採択した。

続いて、2022 年 1 月に欧州委員会は、「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」（Tackling R&I foreign interference staff working document）を発表した[5]。この文書は「スタッフ作業文書」というタイトルであり、欧州連合加盟国や大学・研究機関に対して法的拘束力を持つものではないが、外国からの干渉を防止し、対処するために大学・研究機関がどのような行動を取ることができるかを具体的に記述しており、チェックリストとして利用することが可能である。また、「海外からの干渉」（foreign interference）への対応策については、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つの類型に分けてリストアップし、それぞれ詳しく説明している。

2024年１月には、欧州委員会は「研究セキュリティ向上に関する理事会勧告の提案」（Proposal for a COUNCIL RECOMMENDATION on enhancing research security）を発表した[6]。文書の位置づけとしては、欧州理事会が「理事会勧告」を決定することができるのに対し、欧州委員会はその理事会勧告についての提案を作成する権限を持つ。2024年の第1四半期中に欧州理事会において勧告を採択することを目指すとしている。

本文書は研究活動を安全保障上の脅威から守るための指針を示しており、「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」の内容に基づい

[4] Commission communication on the Global approach to research and innovation: Europe's strategy for international cooperation in a changing world, COM(2021) 252 of 18.05.2021
[5] European Commission. Directorate-General for Research and Innovation. *Tackling R&I Foreign Interference. Staff Working Document* (2022/1)
[6] European Commission. “Proposal for a COUNCIL RECOMMENDATION on enhancing research security.” Brussels, 24.1.2024. COM(2024) 26 final.2024/0012 (NLE)

て作成されている。リスクの特定と評価、セキュリティ方針と手順の策定、研究者やスタッフの意識改革の重要性を強調している。さらに、安全保障上の課題に対処するための国際協力と情報共有の必要性も強調されている。

また、欧州委員会は2023年6月に「欧州経済安全保障戦略」（European Economic Security Strategy）を公表しているが、2024年1月に公表された、経済安全保障強化に向けた政策パッケージ「経済安全保障の推進：５つの新たなイニシアティブの導入」では、5つのイニシアティブの１つとして研究セキュリティ強化が位置付けられている

1.6　フランスにおける研究インテグリティ確保のための取組

研究活動の国際化、オープン化に伴うリスク管理について、フランスでは 2011 年から政府主導で「国の科学・技術可能性保護（PPST[7]）」という省際間プログラムの政策が採られてきた。これは主に軍事や経済の保護の視点でのアプローチで進められてきたものである。海外からの干渉、影響から自国の利益となる科学技術研究やその成果を守るための策が施され、法的裏付け、行政上での制度化が行われてきた。

また、2021 年、研究活動を行っている機関、場所への外国からの脅威は無視できなくなっているという状況について、上院議員アンドレ・ガトランが主導する調査部会が「我々の科学資産と学術の自由をより良く保護するために[8]」と題される報告書を発表した。同報告書は、フランスの科学技術に関する知識やノウハウの安全保障についての状況について調査分析し､起こり得る危険へ注意喚起し､今後について 5 つの目標と 26 の勧告を提言した。

1.7　ドイツにおける研究インテグリティ確保のための取組

ドイツにおいて研究活動の国際化、オープン化に伴うリスク管理の議論は、2010 年代終盤、連邦情報局（BND[9]）が中国からのリスクについて警戒が必要であると報告したことをきっかけに、連邦政府側からさらに大きく取り上げられることになり[10]、2020 年以降、それが学協会、研究機関にも拡がっていった。

学協会、研究機関の動きでは、ドイツ学長会議 HRK[11]の「大学の国際協力に関するガイドラインと基準[12]」や、マックス・プランクの「マックス・プランク協会の国際協力の発展のためのガイドライン（2021）[13]」などが挙げられる。

---

7 PPST：Protection du Potentiel Scientifique et Technique de la nation
8 Sénat. "Mieux protéger notre patrimoine scientifique et nos libertés académiques - Rapport d'information n° 873 (2020-2021)". septembre 2021
9 BND：Bundesnachrichtendienst
10 BfV. "BfV annual report 2020 - Brief summary 2020 Report on the Protection of the Constitution (Facts and Trends)". June 2021
11 HRK：Hochschulrektorenkonferenz
12 HRK. "Guidelines and standards in international university cooperation". April 2020
13 MPG. "GUIDELINES for the development of international collaborations of the Max-Planck-Gesellschaft". March 2021

このようにドイツでの当案件についての対応は、連邦政府からの関連知識の開発と普及を促進・支援し、意識を向上させるための施策に加え、ドイツ学長会議（HRK）、やマックス・プランク（MPG）など大学以外の大規模研究機関を通じて、学術界が強力に関与していることが特徴的である。

1.8　スウェーデンにおける研究インテグリティ確保のための取組

スウェーデンにおいて「研究インテグリティ」、すなわち新たなリスクへの対応は「責任ある国際化」と呼ばれている。取組は学界と資金配分機関が主導し、「責任ある国際化：国際的学術交流のためのガイドライン（以下、ガイドライン）」（2020 年）、「責任ある国際化によっていかに業務を遂行するかに関する高等教育機関への助言（以下、助言）」（2022 年）及び「世界に責任を持つ関与：チェックリスト(以下、チェックリスト)」（2023 年）の 3 つの文書から構成される。

いずれの文書も一般論として記述されている。しかし、一連の取組に先立って外務省が政府通信「中国に係る問題へのアプローチ」（2019 年）を発行し、また対中協力に従事する研究者が実際にどのような困難や課題に直面したのか、その具体的内容を検証する実態調査も行われており、近年スウェーデンの科学技術分野の研究において大きな影響力を持つようになった中国との協力関係が念頭に置かれているのは明らかである。もっとも、取組に関連した全ての文書には繰り返し「好機と挑戦」という言葉が登場する。国際協力は恩恵をもたらす一方、問題も引き起こすと、メリットとデメリットの両面を等しく強調する。

ガイドラインは責任ある国際化を担保する上で注意を要する領域に焦点を当て、大学・研究機関が考慮すべき事柄を認識し、自らリスクを発見し、解決の方向性を見出すための提案であり、スウェーデンの取組の中心に置かれている。助言とチェックリストはガイドラインを基礎に、前者は大学における実践事例を通して、実際の運用を示すのに対し、後者は個々の研究者が国際協力に入る前に検討すべき項目を平易に整理したものである。

スウェーデンにおける取組の鍵となる行為者は、大学・研究機関とそこに所属する研究者であるが、それらへの対応は個々の大学・研究機関に一任されているため、実施にばらつきが生じており、この点が課題と言えよう。

1.9　ノルウェーにおける研究インテグリティ確保のための取組

「責任ある国際協力」と称されるノルウェーの取組は、外務省が「知識移転管理」のために大学・研究機関への規制を強化する「研究セキュリティ」を打ち出し、教育研究省がそれを踏まえてガイドラインを作成するという手順で進められてきた。外務省は、2020 年に知識を取扱う大学等の教育機関における外国人の入学や雇用を輸出管理規制の対象にする「知識移転管理のためのガイドライン」を発表し、2022 年には大学等が知識を外国人に移転する場合には、移転前に政府の許可を必要とする「事前免許制」を導入した。免許制の対象となるのは、外国人の大学院課程の入学、外国人の雇用、外国人のポスドクや訪問研究員などで、対象となる国に定められたリストはなく、ケースバイケースで査定が行われる。

学問の自由を侵害しかねない「事前免許制」の導入に際しては、学界に意見聴取がなされた。学界からは当然反対の声が上がったが、大きな混乱はなかった。また、ノルウェー研究評議会の協力の下に 2023 年夏に公表された教育研究省の「責任ある国際知識協力のためのガイドラインとツール」も外務省の知識移転管理の考え方を前提に策定された。

教育研究省ガイドラインは、大学組織の指導部及び事務方が考慮すべき要点と手続きに焦点を当て、国際学術協力におけるリスクを管理し、安全を強化するための手段を提示する内容で、6 つの章からなり、それぞれの課題の背景、関連法やガイドラインなどを説明した上で、考慮すべき事項が列挙されている。特に第 1 章では学問の自由が取上げられ、その価値を保護し、かつ推進することの重要性が詳細に論述され、安全保障が学問の自由を犠牲にするものではないことが強調されている。

ノルウェーの基幹産業の一つが軍事産業で、学界もその発展の一翼を担ってきた。なかでも、アメリカ合衆国が主導する「F-35 統合打撃戦闘機計画（F-35 Joint Strike Fighter Program）」に参加し、先端複合部品、電気系統や機械部品の製造等を担う。しかも、2022 年 10 月にはトロムソ北極大学でロシア人と見られる訪問研究員がスパイ行為で摘発される事件が起こった。こうしたことが知識移転の安全保障管理を厳格化する政策の背景にあると考えられる。

1.10　フィンランドにおける研究インテグリティ確保のための取組

フィンランドは同国の科学技術の発展に中国は不可欠との認識の下、中国との学術交流を強く推進してきたが、2019 年の EU の対中政策の転換により見直しを図ることになった。そのため、フィンランドの取組は専ら中国に焦点を当て、外務省「政府対中アクションプラン」（2021 年）と教育文化省「中国との学術協力のための勧告」（2022 年）のように、中国との研究協力への対応策となっている。とはいえ、中国の重要性が大きく変わるわけではなく、中国との協力がもたらす恩恵とリスクの均衡を保つことがフィンランドの取組の基底をなす。しかしながら、中国との摩擦を避け、引き続き良好な関係を維持しようとする姿勢は、その取組を曖昧かつ具体性を欠いたものにしている。

外務省アクションプランは中国をフィンランドの研究開発にとって重要なパートナーと

位置づけ、協力関係を今後も発展させていくという方針を確認する内容である。教育文化省の勧告も外務省プランの基本方針に沿って作成されており、中国を重要な国際的パートナーと位置付けている。すなわち、中国との研究協力を推進させることを前提に、フィンランドの学界の重要価値である学問の自由と誠実さ、グッドプラクティスに配慮し、安全保障に対する注意を促す。

「勧告」は、個々の大学や研究者がどのように運用していくのか、具体性の乏しい提言に留まるが、この公表された文書を補う非公式の取組が行われている。「中国ラウンドテーブル」と称される政府（関係省）と現場（研究やビジネスにおいて中国と関係を持つ人・機関）の対話組織である。ラウンドテーブルはテーマ別に 5 つのワーキンググループに分かれて議論を積み上げ、政府（教育文化省）の対策づくりに現場の中国研究や関連事業の関係者（研究者や研究機関、企業関係者、法律家）が意見や考えを反映する一方、彼らの疑問や問題を政府が受け取り、解答や解決策を提示する実践型の仕組みである。参加と退場は自由であり、また自由かつ闊達な議論を保障するため、会議は非公開とされ、参加者の発言内容も公表されない。情報共有は出席者の間に限られる。そのため、より広範な研究者や大学等の関係者が共有し得ないという課題が残る。

1.11　デンマークにおける研究インテグリティ確保のための取組

デンマークでは、2020 年以降、高等教育・科学省、安全保障・情報局を中心に、研究・イノベーションにおける国際共同研究に対するガイドライン等を作成している。背景には、国防情報局、警察情報局等の機関から中国、ロシア等との研究・イノベーション協力における懸念事項が指摘されたことによる。デンマークは、国の規模が小さく、開放的な経済を推進するには、国際協力により、海外の高度な研究施設や知識へのアクセスを必要と考えている。一方で、世界トップクラスの研究環境を有する中国等との共同研究は、デンマーク、EU、同志国の研究機関や企業にとって有益な点があるものの、デリケートな技術分野では中国の研究能力の強化に貢献するといったジレンマを抱えている。

これらの環境変化を認識し、2022 年 5 月に高等教育・科学省が設置した「国際研究・イノベーション協力指針委員会」にて、「国際的な研究・イノベーション協力指針〈ガイドライン〉」（Afrapportering: Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde）を公表した。同ガイドラインは、教育・研究機関の経営陣を対象としたものであり、国際的な研究・イノベーション協力において、リスク管理に重点を置き、①倫理的、財政的、安全保障上のリスクへの組織的な意識向上、②リスク管理のための組織的な枠組みと手順、③全国的な共通アプローチと知識共有の強化の必要性に係る提言を行い、ガイドラインを提示した。教職員向けには、2021 年 5 月に安全保障・情報局と高等教育・科学省が『Is your research at risk?』を公表し、職員に対する外国からの干渉をどのように防止するか、研究の安全確保のためのヒントを提示している。

1.12　オランダにおける研究インテグリティ確保のための取組

オランダは、知識の移転が、国の安全保障を損なうようなものであれば、それは望ましいものではないとして、「研究インテグリティ」に関する用語として、「知識セキュリティ」という用語を使用している。オランダ政府は、国際共同研究に対処し、機会と安全上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、「知識の安全保障に関する国家ガイドライン」（National knowledge security guideline）を作成・公開している。この一環として、大学等が気軽に国際共同研究に関連する機会とリスクや実務的な事項に関連する質問をすることができる中央窓口「National Contact Point for Knowledge Security」を設置している。なお、大学・研究機関が R&D 資金配分機関に対して資金の申請を行う場合には、同ガイドラインを遵守することが要求されている。

1.13　チェコ共和国における研究インテグリティ確保のための取組

チェコ共和国は、旧東欧国であり、OECD（1995 年加盟）・NATO（1999 年加盟）・EU（2004 年加盟）の加盟国である。ロシアからの脅威（偽情報、ハイブリッド脅威等）への対抗のため、2010 年代後半から「外国からの干渉」に対抗するための措置が制定されている。2014 年のクリミア併合以後では、チェコにおけるロシアの干渉に対する懸念が高まり、様々な対抗措置が取られてきた。

2017 年 1 月に、「ハイブリッド脅威対策センター（Centre Against Hybrid Threats）」（2022 年 7 月までは「テロ・ハイブリッド脅威対策センター（Centre Against Terrorism and Hybrid Threats）」）が、2017 年末の総選挙を妨害するロシアの偽情報キャンペーンを防ぐために内務省に設立された。2021 年にハイブリッド脅威対策センターは、「チェコの学術セクターのための外国からの干渉対策マニュアル」（Counter Foreign Interference Manual for the Czech Academic Sector）を策定した。

また、2021 年には、ロシアからのハイブリッドの脅威に対抗するため、「ハイブリッド干渉に対抗するための国家戦略」（National Strategy for Countering Hybrid Interference）を国防省が策定した。ただし、この文書は科学的知識の安全保障の問題には特に触れていない。

1.14　ニュージーランドにおける研究インテグリティ確保のための取組

ニュージーランドでは、英国と同様に「Trusted research（信頼される研究）」として、研究インテグリティ（研究セキュリティ）の取組を実施している。「Trusted research」は、知的財産、機密性の高い研究、個人情報を保護しながら、国際的な科学協力を最大限に活用できるよう支援することにある。

2021 年 12 月に英国国際大学協会（UKKi）の「Joint statement from convening higher education associations（高等教育協会の会合からの共同声明）」にて、安全、安心、そして

持続的な国際化を支える取組を連携して実施することを共同で宣言するとともに、2023 年 8 月には、セキュリティ・クリアランスを管轄する Protective Security Requirements（特殊法人）が、研究機関、大学協会とともに、「Trusted Research: Guidance for Institutions and Researchers」を公表した。同ガイダンスでは、研究者、大学機関、研究機関、産業界のパートナーが潜在的リスクに対して決断できるよう、①研究の保護、②ニュージーランドの研究に対するアプローチ（国際的な研究・イノベーション活動における評判の低下、知的財産の損失、国益の損害にも留意）、③研究の保護の理由、④研究を守る方法を提示した。

また、2022 年 9 月には、大学協会が中心になって、大学の執行部向けに「TRUSTED RESEARCH - Protective Security Requirements - GUIDE FOR Senior University Leaders in Aotearoa New Zealand」のガイドラインを策定している。本ガイドラインでは、大学機関が抱える研究インテグリティに係るリスクを可視化するため、検討ツールもあわせて作成している。

1.15　韓国における研究インテグリティ確保のための取組

韓国では、研究活動の国際化の進展に応じて、研究成果等の海外への遺漏防止のための対策は、産業部門を主たる対象として実施されてきた。他方、近年では、海外から韓国の大学や研究機関に対する共同研究の申し出が増加しているため、セキュリティ上の懸念の声が挙がっていること、加えて諸外国において研究インテグリティへの対策が進んできていることから、大学・研究機関における対策が取り組まれるようになった。

韓国は、半導体など高度の科学技術力を持ち、中国の隣国であると同時に、米国の同盟国として、科学技術セキュリティを確保するための政策に取り組んでいる。2023 年 6 月には「国家研究開発事業におけるセキュリティ対策規則」（국가연구개발사업 보안대책）を科学技術情報通信部など 8 省庁の共同告示基準として定めた。また、諸外国における研究インテグリティ確保のための取組についての事例調査等も政府研究所で実施されている。

1.16　台湾における研究インテグリティ確保のための取組

台湾は半導体、エレクトロニクスなど高度の科学技術力を持つ。台湾にとって、知識の安全保障と経済の安全保障の確保は極めて重要であり、科学技術を保護し、中国の干渉のリスクを軽減するための措置は、台湾の政策、法律、社会的イニシアティブの自明な要素となってきた。結果として、研究インテグリティや研究セキュリティ[14]は自明の取組であるため、台湾では概念としてはあまり知られてこなかった。唯一の公式ガイダンス文書は、「国家基幹科学技術研究プログラム安全管理運用マニュアル」（国家安全委員会、2019 年、更新 2022 年）である。

その代わりに、経済安全保障や外国からの干渉、特に偽情報への対処を目的とした、より

[14] 言葉としては「學術倫理與安全」（「学術の倫理と安全」）が該当する。

広範な政策の一環として措置が取られている。台湾は中国からの強力かつ広範な干渉に苦しんでいるため、ほとんどの法律や措置は、中国によってもたらされるリスクの軽減に焦点を当てている。[15] 国家安全法（National Security Act、1987 年制定、最終改正 2022 年）、台湾地区及び大陸地区人民関係条例（The Act Governing Relations between the People of the Taiwan Area and Mainland Area、1992 年制定、最終改正 2022 年）という 2 つの法律が国家中核的重要技術やハイテク産業の保護について規定している。

さらに、上記のように、2019 年 1 月に、政府出資の国家基幹科学技術研究プロジェクトの従うべき手順（政府出資の国家基幹科学技術研究プログラム安全管理運営マニュアル）が策定され、国家安全保障会議の科学技術チームによって運営されるなど、近年は大学・研究機関において法令遵守が特に、厳しくなってきている。[16]

1.17　イスラエルにおける研究インテグリティ確保のための取組

イスラエルの「研究のオープン化、国際化に伴う新たなリスクへの対応」としては、国家レベルでは従来、中国を牽制する米国の意向を受けながら、主に投資や輸出管理規制の強化等の手法の中で進められてきた。最近では、2023 年 8 月にイスラエル国防軍（Israel Defense Forces: IDF）から安全保障に係る研究・イノベーションに IDF が関与する枠組みの取りまとめが示され、オープンユニバーシティの協力の下 IDF および防衛コミュニティのパートナーに様々な分野の研究や規範に関する学術教育を行い、安全保障状況の変化・変革に専門的・実践的に対応できる人材を育成すること等が挙げられている。また、同年 12 月にイノベーション科学技術省（Ministry of Innovation, Science and Technology）から、民間部門の AI 分野の主要課題として説明責任等を挙げた上で、政策調整やマルチステークホルダーの議論の場を確保する等の方針が示された。2024 年 1 月には、いわゆる外国干渉や技術戦略といった国家的課題のあり方について、国内研究機関からの考察や提言が示された。

1.18　各国・地域における研究インテグリティに対する取組状況の調査における注目点のまとめ

以上、17 カ国・地域の研究インテグリティ政策は、オープンかつ倫理的な研究環境を育成すると同時に、国際的な共同研究、スパイ活動、外国からの干渉に関連するリスクから学術的・科学的活動を保護することの重要性への共通した認識を反映している。以下は、これらの多様な地政学的背景の中で共通して観察されたポイントである。

- 共通の目標：どの国・地域も、自国の安全保障上の利益、知的財産、技術的進歩を、特に経済的・軍事的安全保障に不可欠とみなされる分野において、潜在的な外国の脅

[15] Ingrid d'Hooghe, and Jonas Lammertink (2022). *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden Asia Centre. pp.37-40.
[16] Ingrid d'Hooghe, and Jonas Lammertink (2022).

威から守ることに力を注いでおり、特に近年取組は強化されてきている。

- ガイドラインと枠組み：英国やニュージーランドの「Trusted Research」やカナダの「Safeguarding Your Research Portal」、また北欧の「responsible research」など、国際共同研究におけるリスク管理について、大学・研究機関や研究者に明確な指針を示すことを目的とした具体的なガイドラインや枠組みを策定している国が大半である。
- 政府と大学・研究機関の協力：政府機関、大学・研究機関間の連携を促進し、研究インテグリティ、研究セキュリティの総合的な強化を図る傾向が顕著である。例えば、オーストラリアの UFIT や英国の Universities UK、カナダのカナダ政府-大学ワーキンググループは、マルチステークホルダーアプローチを強調している。
- リスクの高いパートナーシップや技術への焦点（risk-based なアプローチ）：スウェーデン、ノルウェー、フィンランド、デンマークなどは、国際協力、特に中国やロシアなど急速に進展する研究協力や地理的隣接に伴う脅威のためにリスク管理を重視している。カナダの新方針では、機微技術とリスクの高い海外大学・研究機関をリストで指定している。他方で、EU では「国を問わないアプローチ」（country-agnostic approach）をとり、特定国をターゲットと明示せずに、特定国や地域の出身者への差別を防止するための配慮も見られる。
- 法律および規制措置：一部の地域では、研究セキュリティ確保の取組について法的強制力を与えるために法律が制定され、また、近年の国際情勢の緊迫を背景として議会における法律制定の動きが見られる。例えば、米国の国防授権法や Chips および科学法、フランスの PPST プログラムがその例である。
- サイバーセキュリティとデジタル保護措置：サイバーセキュリティ対策は、研究セキュリティ戦略の重要な要素であり、機密データや研究成果をサイバー脅威や不正アクセスから保護する必要性に対処するものである。研究インテグリティ、研究セキュリティの確保のための取組においては、大学・研究機関におけるサイバーセキュリティ対策が含まれていることが多い。例えば、欧州委員会の「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」である。
- 教育と意識向上：研究インテグリティとセキュリティの重要性に関する研究者や研究機関のスタッフの認識を高め、ベストプラクティスに関するトレーニングを提供することは、共通のテーマである。これは、研究コミュニティ内に責任と警戒の文化を醸成することを目的としている。政府資金でオンライン研修教材を開発したり（米国）、大学・研究機関間で共有するなどの動きがみられる。
- モニタリングとコンプライアンス：各国は、研究活動を監視し、セキュリティプロトコルの遵守を確保するための仕組みを導入または強化している（カナダの新ポリシーなど）。これには、国際的なパートナーシップや資金源を吟味する際のリスク評価やデューディリジェンスが含まれる。
- 国際研究協力の重要性：安全保障が重視される一方で、国際的な研究協力の利点も認識されている。政策では、リスクの軽減と国際的な科学協力の利点の活用のバランス

をとることを目指している（EU のオープンサイエンス重視など）。

- 各国独自の事情：各国のアプローチは、その国特有の地政学的背景、技術的強み、戦略的優先事項の影響を受けている。例えば、イスラエルが国防と民生研究部門の統合に重点を置いていることや、台湾が機密技術の知識移転の防止に重点を置いていること、さらに軍事産業が学界との協働で発展し、基幹産業の一つをなすノルウェーでは軍事先端技術の移転防止を図っていることは、国家安全保障上の独自の懸念を反映している。

また、調査対象とした国・地域の中では以下のような進んだ取組も見られた。カナダの政策は明確で先進的であり、カナダ固有のニーズに効果的に対応しているが、米国と EU は、その政策、インフラ、世界的影響力が、世界の研究インテグリティ・セキュリティ基準に広範な影響を与えるベンチマークと実践を設定しているという意味で、主導的である。

・カナダは、特に "Safeguarding Your Research Portal "と "National Security Guidelines for Research Partnerships"、「機微技術研究と、懸念される提携に関する政策」の開発・策定により、研究インテグリティ・研究セキュリティの確保のための積極的かつ体系的なアプローチを示している。これらの措置は、「研究セキュリティセンター」の設立や機密技術研究に焦点を当てた政策の導入と相まって、特に研究コミュニティに実用的なガイドラインやリソースを提供するという点で、カナダのアプローチが先進的であることを示唆している。研究セキュリティ対策をより広範な国家安全保障の枠組みの中に統合する一方、国際的な協力を促進する環境を整備している。

・米国と欧州連合（EU）は、いくつかの理由から、研究インテグリティ・研究セキュリティ政策の分野でリードしていると考えられる。米国は、NSPM-33 のようなイニシアティブと、それに続く科学技術政策局（OSTP）のガイダンスを通じて、研究インテグリティと研究セキュリティを守るための強固な枠組みを築き、国際的なリーダーシップも取ってきた。このような努力は、法的・規制的手段（Chips and Science 法、国防授権法）によって補完されている。米国の指導的地位は、その広範な連邦研究インフラと研究機関の世界的影響力によってさらに強固なものとなっている。

・EU もまた、「研究とイノベーションへのグローバルなアプローチに関するコミュニケーション」や、「研究セキュリティ向上に関する理事会勧告の提案」に見られるように、外国からの干渉に対処するための包括的なアプローチにより、研究セキュリティにおけるリーダーとしての地位を確立している。EU の戦略は、加盟国間の集団行動を重視し、EU 圏の規制的枠組みを活用して、研究セキュリティとインテグリティに関する課題に取り組む一方、オープンサイエンスや研究協力といった価値観を推進している点で注目に値する。

表 1 において、調査対象国・地域における研究インテグリティに関する主な規則・ガイドライン等（名称、制定年月、担当機関、内容・特徴）をまとめた。

表 1：調査対象国・地域における研究インテグリティに関する主な規則・ガイドライン等

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
米国	国家安全保障大統領覚書-33(NSPM-33)【大統領令】	2021 年 1 月	大統領府科学技術政策局（OSTP）	米国政府が支援する研究開発（R&D）を、外国政府の干渉や搾取から守るための行動を指示。研究セキュリティの確保に関連する 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の結果、4. 情報の共有、5. 研究セキュリティプログラム）。
米国	NSPM-33 実施ガイダンス【連邦政府規則】	2022 年 1 月	大統領府科学技術政策局（OSTP）	連邦省庁に対し、NSPM-33 の実施（上記の 5 分野）に関する詳細な指針を提供。
米国	FY2020 国防授権法【連邦法】、FY2021 国防授権法【連邦法】	2019 年 12 月、2021 年 1 月	連邦議会	すべての連邦政府の資金配分機関に対して、研究助成金申請プロセスの一環として、現在及び未決の支援についての情報開示を、申請研究者に対して求めることを義務付けた。
米国	Chips and Science 法【連邦法】	2022 年 8 月	連邦議会	「外国人人材採用プログラム」についてのガイドライン策定、米国科学財団（NSF）に Research Security and Policy Office を設置、研究開発助成の申請時にリスク評価を NSF が実施する権限付与、大学・研究機関や研究者がセキュリティリスクを理解し軽減できるように独立したリスク評価センターの設立などを連邦政府に義務付けた。
米国	NSF Guidelines for Research Security Analytics【NSF 規則】	2023 年 2 月更新	NSF	NSF の Office of the Chief of Research Security Strategy and Policy（OCRSSP）の責任とプロセス、NSF 職員によるモニタリング・報告、OCRSSP による許可・禁止行為、研究セキュリティ分析のためのデータ・サービス・分析手法、研究セキュリティ関連情報の共有原則について説明。
米国	「海外からの影響対策プログラム」（Countering Foreign Influence Program: CFIP）【国防省規則】	2022 年?	国防省 DARPA	DARPA の研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を目的とした適応型リスク管理セキュリティプログラム。リスク評価は、標準フォーム（SF）424「Senior/Key Person Profile (Expanded)」及びその付属文書等に基づいて行われる。
米国	高等教育機関における国防省資金配分による研究における望まない海外からの干渉への対抗【国防省規則】	2023 年 6 月	国防省	「基礎研究提案の利益相反緩和の判断材料となる決定マトリクス」を含む。「FY22 リスト」は、国防授権法 1286 条(c)(8)(A)に記載された問題のある活動に従事していることが確認された外国機関（外国の人材プログラムを含む）を特定。
英国	Trusted Research Guidance for Academics【NPSA 作成のガイダンス】	2019 年	国家防護安全保障局（National Protective Security Authority: NPSA）	大学・教育機関向けに、「Trusted research」に関する理解を促すためのガイダンスである。大学におけるセキュリティの脅威の管理とセキュリティガイダンスの実施に焦点を当てる。
英国	Managing risks in Internationalisation: Security related issues【UUK 作成文書】	2020 年 10 月	Universities UK (UUK)	NPSA の「Trusted Research」キャンペーンを踏まえ、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、英国の大学向けのガイドラインである。
英国	Managing risks in international research and innovation【ガイダンス】	2022 年 6 月	NPSA、UUK および UKRI	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、これまで作成したガイドラインや主要原則をまとめたガイダンスである。
英国	Security and risk: how universities can protect their research and people【ガイダンス】	2023 年 6 月更新	UUK	大学が直面する安全保障上の脅威、脅威に対処するための措置、大学で安全保障ガイダンスを実装する方法、大学全体で安全保障を重視する文化を根付かせる方法等について纏めたもの。

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
豪州	オーストラリアの大学分野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（UFIT ガイドライン）【政府・大学等共同策定文書】	2019 年 11 月（2021 年 11 月改定）	政府機関（教育省等）、豪州研究評議会（ARC）等の資金配分機関	外国からの干渉に共同で対処するために設置された「大学対外干渉タスクフォース(UFIT)」（政府機関、大学・研究機関が参加）」を通じて意見調整し、策定された。大学・研究機関における外国干渉セキュリティの一連の審査は、同ガイドラインに基づいて行われている。
豪州	重要技術のための青写真と行動計画【連邦政府規則】	2021 年 11 月	首相府 重要技術政策調整室(CTPCO)	豪州研究評議会（ARC）は、競争的研究資金の申請にあたり、このリストに記載された技術が含まれている場合には、リスクがあるかどうかを検討する。
豪州	トランスナショナル教育に関するデューディリジェンスについてのガイダンスノート【政府・大学等共同策定文書】	2023年6月	UFIT のトランスナショナル教育ワーキンググループ	トランスナショナル教育（Transnational education: TNE）、すなわち、学習者の所在地が教育機関の所在地とは異なる国である高等教育プログラムについての外国干渉リスクへの対応について記述。
カナダ	アカデミックなコミュニティにおけるセキュリティ意識の醸成【公共安全省規則】	2019 年	公共安全省	外国の国家や集団を含む潜在的脅威からカナダの学術機関における機密研究保護の重要性を強調。強力なサイバー衛生の実施、研究のデュアルユース用途の認識、法律や規制の下での責任の理解などを推奨
カナダ	Safeguarding Your Research Portal【政府・大学等共同策定文書】	2020年9月	カナダ政府・大学共同ワーキンググループ	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。ワーキンググループは定期的に会合を開き、本ポータルは研究セキュリティ強化の取組を広めるための重要なチャネルとなっている。
カナダ	国際研究協力に対する国家安全保障ガイドライン【連邦政府規則】	2021年7月	連邦政府	研究パートナーシップの開発、評価、資金提供におけるデューディリジェンス、リスク評価、緩和に焦点を当て、研究パートナーシップにおける国家安全保障への配慮を統合するためのガイドラインである。
カナダ	機微技術研究と、懸念される提携に関する政策【連邦政府規則】	2024年1月	連邦政府	機微技術研究分野のリストと、懸念される海外の大学・研究機関のリストを含む。機微技術研究分野研究の研究助成金等は、関与研究者が、海外の軍等の大学、研究機関等に所属又は資金等受領している時、今後は提供されない。
欧州連合	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【欧州委員会作成文書】	2022年1月	欧州委員会	EU 加盟国や大学・研究機関に対し法的拘束力を持つものではない。外国からの干渉の防止、対処のために大学・研究機関がどのような行動を取ることができるかを具体的に記述（価値観、ガバナンス、提携、サイバーセキュリティ）。
欧州連合	研究セキュリティ向上に関する理事会勧告の提案【欧州委員会作成文書】	2024年1月	欧州委員会	責任ある国際化のための原則について説明。リスクの特定と評価、セキュリティ方針と手順の策定、研究者等の意識改革の重要性を強調。さらに、国際協力と情報共有の必要性も強調。
フランス	デクレ 2011-1425：刑法 413 条 7 項への国の科学・技術可能性保護施策（PPST）の適用【デクレ（大統領・首相命令）】	2011 年 11 月	大統領府、首相府	PPST 実施のためのデクレ（大統領・首相命令） ※PPST：研究活動が行われている機関・施設において、国の優位性に貢献する戦略的知識、ノウハウ、機密性を有する技術を保護するために行われている政策。政策主管は仏防衛・国家安全総局（SGDSN：首相管轄）で政策実施監督は 6 つの省の防衛・安全保障上級高官（HFDS）。
フランス	科学・技術可能性保護施策（PPST）【アレテ（行政命令）】	2012年7月	政府	上記 PPST 実施のためのアレテ（行政命令）
フランス	国の科学・技術保護施策（PPST）について【省際間通達文書】	2012 年 11 月	政府	上記 PPST 実施のための省際間通達文書
フランス	国の科学・技術保護施策（PPST）【パンフレット】	現行版インターネット掲載：2018年8月	仏防衛・国家安全総局（SGDSN）	上記 PPST 実施のための普及パンフレット

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
フランス	我々の科学資産と学術の自由をより良く保護するために【調査報告書】	2021年9月	仏上院	研究活動を行っている機関、場所への外国からの脅威は無視できなくなっているという状況について、上院議員アンドレ・ガトランが主導する調査部会がまとめた報告書を発表した
ドイツ	大学の国際協力に関するガイドラインと基準【HRK 策定・発表文書】	2020年4月	ドイツ学長会議（HRK）	世界的な環境の大きな変化に伴い大学の国際協力についての対応を包括的に策定。
ドイツ	中国との大学の国際協力におけるガイドライン・クエスチョンズ【HRK 策定・発表文書】	2020年9月	ドイツ学長会議（HRK）	中国共産党（CCP）が研究機関に及ぼす影響などについて指摘。
ドイツ	マックス・プランク協会の国際協力の発展のためのガイドライン【マックス・プランク協会作成文書】	2021 年	マックス･プランク協会	研究の自由、ルールの遵守、個人の責任のバランスをとりながら、国際協力を成功させることができるように支援するために策定。 研究者らに国際協力における潜在的なリスクに対する認識を高めさせるなどの目的を有する。
スウェーデン	中国に係る問題へのアプローチ【政府通信】	2019年9月	スウェーデン外務省	影響力を高める中国との関係及び中国に対するスウェーデンの接近のあり方について概略を示し、中国との協力においては好機と困難の両面があるとの見解を示す。
スウェーデン	責任ある国際化：国際的学術交流のためのガイドライン【基金配分機関ガイドライン】	2020年2月	研究と高等教育機関の国際協力のためのスウェーデン財団	大学、研究機関とその教員及び職員、学界リーダー向けのガイドラインであり、国際共同研究や教育協力を行う際に考慮すべき点を挙げ、具体的なチェック項目を示し、このガイドラインに基づいて各大学等が責任ある国際化と学術協力のアプローチについて構造的かつ有用な議論を行うよう提案する。
スウェーデン	責任ある国際化によっていかに業務を遂行するかに関する高等教育機関への助言【資金配分機関文書】	2022年5月	研究と高等教育機関の国際協力のためのスウェーデン財団	規模や歴史、国際化の進展において異なる３大学と１研究機関の経験に基づいて、研究・教育の国際化によって生じる課題（challenges）を抽出し、対応策を検討することによって、４機関の異なる特性によって生じるアプローチをタイプ分けしてそれぞれのメリットと課題が整理されている。さらに、４機関の中の１つの大学を取上げ、その現状を詳細に分析し、参照ポイントの創設、知識の共有、成果の考察と接合の３点から構成される「責任ある国際化」モデルを提案する。
スウェーデン	世界に責任をもつ関与:チェックリスト【学術団体文書】	2023年4月	スウェーデン高等教育機関協会	国際協力活動の開始前にパートナー研究機関（者）について検討すべき 6 項目、すなわち ①民主主義と学問の自由が担保されているか、②パートナー研究者の評判と所属大学の評価、③データ使用、知的財産権、特許権に関する対立の可能性の有無、④研究の不正利用と意図しない悪意ある応用の可能性、⑤倫理ダンピング：ヒト及び生物のデータに関する安全性が確保されているか、⑥パートナー研究者の安全性は担保されているかを例示している。
ノルウェー	知識移転管理のためのガイドライン【政府ガイドライン】	2020 年 10 月	ノルウェー外務省	ノルウェーの輸出管理規則の枠内において特段の注意と考慮が求められる教育機関の外国人の入学許可や雇用等を支援することを目的に、これら教育機関に対し知識の「機微性の高さ」を評価し、外国の学生、研究員、雇用者への知識移転がノルウェーの輸出管理規則に違反しないかを査定することを求める。

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
ノルウェー	外国人研究者等受入れのための事前免許制【政府規則】	2022年3月	ノルウェー外務省	機微な知識の移転が外国人に行われる前に、外務省に事前許可のための免許を申請しなければならない。学術スタッフの募集、客員研究員の受け入れ、大学院の入学にはこの規則に基づく審査が求められる。免許＝事前許可は必ず入学許可や雇用契約がサインされる前に得ておかなければならない。なお、当該人物が免許の申請が必要な国の出身者か、否かについての固定的なリストはなく、ケースバイケースで査定しなければならない。
ノルウェー	責任ある国際知識協力のためのガイドラインとツール【政府ガイドライン】	2023年8月	ノルウェー教育研究省	国際学術協力におけるリスクを管理し、安全を強化するために、当該事業に対し考慮すべき点及び均衡の取れた協力関係を築く上で必要な情報を提示するとともに、機関がそれぞれの事情に応じて、独自の計画を立てることができるように実務的な手法を提供する。個々の大学がその関心の範囲、価値あるいは資産と弱点を特定し、リスクを認識することを要請する。
フィンランド	対中アクションプラン【政府行動計画】	2021年6月	フィンランド外務省	中国との協力、意義、将来の方向性について全体的な精査を行う一方､メンバー国としてEUと歩調を合わせるという観点に則って、中国との関係を協力、競合、制度的ライバルの3つの次元から捉える。人権に基づく外交と安全保障政策に従い、政策評価を人権への影響という観点から実施するため、中国の人権状況を注意深く監視しなければならないとする。
フィンランド	中国との学術協力のための勧告【政府勧告】	2022年3月	フィンランド教育文化省	フィンランドの高等教育機関および研究機関が自らの原則と価値によって中国のパートナーとの研究協力を推進すべきことを前提に、研究機関がその価値や関心に基づいて中国のパートナーとの協力を支援するとともに、対中協力において生じ得るリスクを周知し、注意を払うべき事項を例示する。
デンマーク	国際的な研究・イノベーション協力指針〈ガイドライン〉【政府ガイドライン】	2022年5月	デンマーク高等教育･科学省	2020年に高等教育･科学大臣が設置した「国際研究･イノベーション協力指針委員会（URIS）」で議論を行い、倫理的・財政的・安全保障上のリスクに対する組織的な意識向上、リスク管理のための組織的な枠組みと手順、全国的な共通アプローチと知識の共有の観点から提言を行った。本ガイドラインは、デンマークの教育・研究機関の経営陣を対象としたガイドラインである。
デンマーク	あなたの研究はリスクにさらされている？【ガイダンス】	2021年5月	デンマーク安全保障・情報局､デンマーク高等教育･科学省	安全保障・情報局と高等教育・科学省が、研究機関の職員が外国からの干渉やスパイ活動をどのように防止し、対応するかについて勧告したものである。
オランダ	Knowledge Security Framework	2021年7月	オランダ大学連盟	オランダの大学が知識セキュリティに対するコミットメントを表明し、知識セキュリティに関する意思決定や方針を策定する際の助けとなるように作成された。
オランダ	知識セキュリティに関する国家ガイドライン	2022年1月	オランダ大学連盟､オランダ王立芸術科学アカデミー等の研究セクターが共同で作成。	国際共同研究に対処し、機会と安全上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。
チェコ共和国	外国からの干渉対策マニュアル【内務省 ハイブリッド脅威対策センター作成文書】	2021年	内務省 ハイブリッド脅威対策センター	外国からの干渉に対抗するための個人の責任と組織の協力の重要性を強調。このガイドラインに従うことで、学術界は学問の自由を守り、透明性を維持し、外部からの脅威に対する強靭性を築くことができると説明。

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
ニュージーランド	信頼される研究－研究機関と研究者のためのガイダンス【ガイダンス】	2023年8月	Protective Security Requirements（特殊法人）、サイエンス･ニュージーランド､ニュージーランド大学協会	「Trusted research」の実施に向けて、ニュージーランドの研究・イノベーションにおける潜在的なリスクを理解し、研究者、大学、研究機関、産業界のパートナーが国際共同研究に自信をもって潜在的なリスクに対して決断できるよう支援するものである。
ニュージーランド	信頼される研究：セキュリティ保護要件－アオテアロア・ニュージーランドの大学執行部のための手引き【ガイダンス】	2022年9月	ニュージーランド大学協会	「Trusted Research」(信頼される研究) を進めるため、ニュージーランド国内大学の執行部（シニアリーダー）が、信頼される研究、セキュリティ保護要件を取りまとめた。本手引きでは、学において組織内部、教職員、学生等との対話を始める際の手引きとしてとりまとめられた。
韓国	「国家研究開発事業におけるセキュリティ対策」規則【8省庁共同規則】	2023 年 11 月	科学技術情報通信部等の 8 省庁	国家研究開発プロジェクトにおける機密技術や研究成果を外国のスパイ活動や不正アクセスから保護することを目的とし、国、大学・研究機関で実施すべきことを規定（委員会の設置、規則制定、責任者の任命、教育・研修等)。
韓国	研究セキュリティ管理及び研究成果保護の手引き	2022年3月	国家科学技術人材開発院	研究セキュリティ管理、研究進行段階別の研究者による研究セキュリティ管理、セキュリティ管理項目別の研究機関による研究セキュリティ管理についてそれぞれ説明している。
台湾	政府出資の国家基幹科学技術研究プログラム安全管理運営マニュアル【国家安全委員会作成文書】	2019年1月（2022 年改定）	国家安全委員会	政府出資の国家基幹科学技術研究プロジェクトが従うべき手順を規定。国家安全保障会議の科学技術チームによって運営される。
イスラエル	I2I イノベーション･トゥ・イノベーション: IDF イノベーション・パートナーシップ戦略【イスラエル国防軍作成文書】	2023年8月	イスラエル国防軍	軍事部門の関与により、新技術等から生じる新たな脅威への対応を図る枠組みや方向性の取りまとめ。安全保障状況の変化・変革に強い軍事人材の学術的・専門的・実践的育成や、研究機関・民間等との関係強化・情報共有等。

1.19　研究活動の国際化、オープン化に伴うリスクの管理（リスク判断を含む）のための主な取組のまとめ

米国、英国、豪州、カナダ、欧州連合においては、研究活動の国際化、オープン化に伴うリスクの管理（リスク判断を含む）のための主な取組としては以下のものがみられた。

<u>米国</u>

・国防省では、2023 年 6 月に「高等教育機関における国防省資金配分による研究における望まない海外からの干渉への対抗」（Department of Defense. Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education. June 29, 2023.）を策定、公表している。「基礎研究提案の利益相反緩和の判断材料となる決定マトリクス」は、プログラム管理者（program managers）と国防省構成機関（DOD Components）が基礎研究提案の潜在的な利益相反を審査する際に役立つ手引書である。
・国防省の研究機関である DARPA には、「海外からの影響対策プログラム」（Countering Foreign Influence Program: CFIP）がある。同プログラムは、不当な外国からの影響の

可能性を特定することにより、DARPA の研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を支援することを目的とした適応型リスク管理セキュリティプログラムである。CFIP のリスク評価は、標準フォーム（SF）424「Senior/Key Person Profile (Expanded)」及びその付属文書又は参照文書に記載されている情報に基づいて行われる。不当な外国影響力のリスク評価プロセスは、SF424 に記載されているすべての報告情報に注目し、過去 4 年間のシニア/キーパーソンの活動に最も重点を置いている。CFIP のリスク評価は、外国の影響を受けた利益相反又は責務相反を構成する可能性のある外国関連活動等の量、種類、時期に応じて、「低」から「非常に高い」までに分類されている。

・NSF は、2023 年 6 月に NSF Guidelines for Research Security Analytics を公表している[17]。同文書は、NSF 職員が研究助成金申請書等の情報や公開情報に基づいて実施するリスク判断やリスク分析の方法等についてのガイドラインである。定義（第 5 節）、Office of the Chief of Research Security Strategy and Policy（OCRSSP）の責任とプロセス（第 6 節）、NSF 職員によるモニタリング・報告（第 7 節）、OCRSSP による許可・禁止行為（第 8 節）、研究セキュリティ分析のためのデータ・サービス・分析手法（第 9 節）、研究セキュリティ関連情報の共有原則（第 10 節）について説明している。OCRSSP の活動は検証（verification）に関連するものであり、調査活動（investigation）は行わない。研究セキュリティ分析には、SCOPUS、Web of Science,米国特許商標局特許データベースが使用される。情報開示された研究資金、所属等とこれらの論文データ等の情報のミスマッチが調べられる。（9 節）

英国

・研究インテグリティに関するリスクの識別・分類、リスクの判断基準、リスク判断のフロー等について詳細に説明された文書ではないが、一般の大学研究者が国際共同研究の提案を行う際に、研究インテグリティに関するリスク発生の予防の観点から、わかりやすく、確認すべき事項を示したチェックリストである「Trusted Research Checklist for Academia」が、前述した「Trusted Research Guidance for Academics」に関連して NPSA から公開されている。項目は、新規パートナーについて、研究の関係性について、既存のパートナーについてのそれぞれについて確認事項を含む。

豪州

・豪州では 2019 年 11 月に、外国干渉を排除するための通称・UFIT ガイドライン（Guideline to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表した。同ガイドラインの 3 章「Due Diligence, Risk Assessments and Management」において、デューディリジェンスの方法、リスクマネジメントについて説明されている。また、以下のような関連文書が UFIT により作成され、教育省のウェブサイトで公表されている。

[17] https://new.nsf.gov/research-security/guidelines
https://nsf-gov-resources.nsf.gov/2023-05/NSF%20Research%20Security%20Guidelines-2023.pdf

-Due Diligence Assistance Framework (2021 年 11 月公表)

-Due diligence, risk assessments and management

・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）が発表された。豪州の資金配分機関である豪州研究評議会（ARC）は、競争的研究資金の申請にあたり、このリストに記載された技術が含まれている場合には、リスクがあるかどうかを検討することになっている。リスク要因には、次のような諸点が含まれるとしている。

-外国からの財政支援や教育又は研究関連活動

-外国の人材育成プログラムへの関与など

-外国の政府や軍隊、警察、諜報機関などへの直接の関与

-豪州が制裁措置をとっている体制、個人、組織への関与

<u>カナダ</u>

・NSERC におけるリスクアセスメントは、研究者が提出したリスク質問票を検討し、国家安全保障を考慮した評価が必要な場合には、カナダ公共安全省に照会され、カナダ公共安全省、カナダ安全保障情報局、又はカナダ通信保安局が主導して評価を実施するという特色を持つ。助成機関から照会された申請書を受け取ると、カナダ公共安全省は最初の審査を行い、結果を通知する。カナダ公共安全省は、評価結果及びアドバイスを助成機関に返却する。

・「Policy on Sensitive Technology Research and Affiliations of Concern」によるリスクアセスメントプロセスでは、大学または関連研究機関が、連邦資金配分機関およびカナダ・イノベーション財団（Canada Foundation for Innovation）に提出した、研究助成金および資金提供の申請書においては、1）機密技術研究分野を発展させる研究を含み、さらに、2）その助成金で支援される活動に関与する研究者のいずれかが、カナダの国家安全保障に危険をもたらす可能性のある軍、国防、または国家安全保障機関と関係のある海外の大学、研究機関、研究所に所属している場合、またはそこから資金や現物支援を受けている場合には、資金が提供されなくなる。このプロセスを支援するため、「機微技術研究分野（Sensitive Technology Research Areas）」のリスト、カナダの国家安全保障に危険を及ぼす可能性のある、軍、国防、国家安全保障機関と関係のある海外の大学・研究機関のリストが公表された。

<u>欧州連合</u>

・2022 年 1 月に欧州委員会は「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」を公表した。包括的な戦略を策定するためのツールキットとして作成されたもので、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た主要な注目分野をカバーしている。それぞれのカテゴリー別に、「海外からの干渉」への対応策を列挙している。

-価値観（1．学問の自由が危険にさらされている国やパートナー機関を特定する、2.

当該教育機関における学問の自由とインテグリティに対する外部からの圧力を理解するために、脆弱性評価（vulnerability assessment）を実施する、3. 機関及び個人レベルで学問の自由とインテグリティへのコミットメントを強化する、4. 抑圧的な環境下にあるパートナーとの協力を継続する）

-ガバナンス（1. 海外からの干渉に対する行動規範を公表する、2. 海外からの干渉委員会（Foreign Interference Committee）を設置する）

-パートナーシップ（1. リスクマネジメントシステムを導入するための一般的な前提条件を整備する、2. 強固なパートナーシップ合意を策定するための健全な手順を確立する）

-サイバーセキュリティ（1. サイバーセキュリティリスクの認知度向上、2. 海外からの干渉行為者によるサイバーセキュリティ攻撃を検知し、防止する、3. 海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う）

米国では、DARPA のような機関を含む国防省が、国防省が資金を提供する研究における好ましくない外国の影響に対抗するための方針を定めている。これらの方針は、標準的な書式や文書で提供された情報に基づき、研究者の経歴、所属、活動を詳細に精査することで、潜在的な利益相反や外国からの影響を特定することに重点を置いた、意思決定マトリクスや、外国影響対策プログラム（CFIP）のようなプログラムによって支えられている。また、NSF における提案された研究についてのリスク判断では、NSF 職員が研究助成金申請書に記載された情報や、書誌情報などの公開情報に基づいて実施するとしていることが特徴的である。

英国のアプローチは、国家保護安全保障局（NPSA）の「Trusted Research Checklist for Academia」に見られるように、国際的な共同研究における潜在的なリスクについて確認し、学者や研究者を導くことをより指向している。このチェックリストは、具体的なリスク評価プロセスを詳述するものではないが、研究者が研究インテグリティを維持することに焦点を当て、新規および既存のパートナーシップを評価するための枠組みを提供するものである。

オーストラリアは、UFIT ガイドラインに代表されるように、大学部門における外国からの干渉に対抗するための包括的なガイドラインと行動計画を策定している。これらのガイドラインは、デューディリジェンスの方法、リスク評価、管理戦略について詳述しており、特に重要な技術や、外国からの資金援助、外国人材プログラムへの関与、外国政府や制裁対象団体との提携がもたらす潜在的なリスクに焦点を当てている。

カナダのアプローチでは、研究助成機関と、カナダ公安庁、カナダ安全保障情報局、通信安全保障機構などの国家安全保障機関との間の共同作業が行われる。カナダにおけるリスク評価プロセスは、資金提供機関からの照会を受けて開始され、研究者の所属、特に外国の軍事・安全保障機関とのつながりなど、国家安全保障にリスクをもたらす可能性のあるものを徹底的に評価することが含まれる。

欧州連合（EU）の戦略は、価値観、ガバナンス、パートナーシップ、サイバーセキュリ

ティなど、多方面にわたる外国からの干渉に対処するための包括的なツールキットを包含している。EU は、組織レベルおよび個人レベルでの脆弱性評価の実施、海外干渉委員会の設置、攻撃を検知・防止するための強固なサイバーセキュリティ対策の実施に重点を置いている。

これらの国・地域は、研究インテグリティ、研究セキュリティを確保し、国家安全保障を守るという包括的な目標を共有しているが、リスク評価基準の具体性の度合い、学問の自由と安全保障上の懸念のバランス、学術機関と国家安全保障機関との協力の度合いなどの相違もみられる。

２．研究インテグリティについての国内ヒアリングの実施

国内の大学・研究機関における、研究インテグリティの確保、特に、研究の国際化やオープン化に伴う新たなリスクに対する対応のための取組等の現状や課題を把握し、今後の研究インテグリティの確保のための取組に役立てていくことを目的としてヒアリングを実施した。

ヒアリングは国内の大学・国立研究開発法人 10 機関（7 大学、3 国立研究開発法人）を対象として、2023 年 11～12 月に、約 1 時間半の時間でオンラインで実施した。大学・国立研究開発法人の研究インテグリティあるいは関連業務を担当する部署の職員等（担当部署の部課長等）からの対応を得た。ヒアリングは対象機関や担当者の名称は公開しないことを前提に実施し、ヒアリング対象機関は、ヒアリング結果についての報告書原稿内容の確認を、公開の適切性等の観点からお願いした。

大学については、機関種別（国立、公立、私立）、研究大学かどうか、規模（教員数、科研費獲得金額）、総合大学か単科大学か、の観点から選定した。

A 大学：大規模国立大学。研究大学。
B 大学：大規模国立大学。研究大学。
C 大学：中規模国立大学。
D 大学：公立の総合大学。
E 大学：私立の総合大学。
F 大学：私立の総合大学。
G 大学：私立の工業大学。

国立研究開発法人については、主要な機関から 3 法人を選定した。

質問内容は、1）研究インテグリティ確保のための規程整備、2）組織体制・運用方法（開示情報のリスク判断、リスクへの対応プロセス、既存の組織体制との関係）、3）運営トップレベルの関与、4）研修・教育、5）他機関との連携状況と、6）政府・資金配分機関への要望・提案の 6 項目について伺った。1)～5)の項目については取組等の現状と課題について伺った。

〇規程整備の内容及び運用方法について

ヒアリングした大学・国立研究開発法人では、利益相反管理、安全保障貿易管理に関する規程等を既に策定している。一部の大学・国立研究開発法人では、研究インテグリティについての規程についても 2022 年、2023 年に制定してきている。規程は基本的には文部科学省から示されたモデル規程を参考に策定されている。これらの枠組みは、政府からの方針に対応し、研究活動、特に国際的な研究活動の拡大に応じた新たなリスクを管理するための積極的な対策として策定されることが多い。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

- 大学間の比較：国立大学（A、B、C）では既に研究インテグリティについての規程を整備している。公立大学 D、私立大学（E、F、G）では、既に制定している利益相反規程、安全保障輸出管理規程の枠組みのもとで、必要な情報共有を図るなど運用面での対応をしており、研究インテグリティに関する規程の整備については他大学の動向等を注視しつつ検討しているのが現状である。
- 研究型大学とそれ以外の大学の比較：研究大学（A と B）は、研究活動のレベルの高さ、国際的研究活動の大きさを反映して、研究インテグリティとセキュリティに対して、より包括的で詳細なアプローチをとっている。それ以外の大学では、研究インテグリティに関連する対応に配分可能な資源への制限があり、各々の研究活動等を反映した合理的な対応について、他大学等の取組の情報を集めて、模索している段階と考えられる。
- 大学と国立研究開発法人の比較：国立研究開発法人(A、B、C)では、国立大学と同様に研究インテグリティについての規程の整備が既に行われており、政府とは緊密な調整が図られており、政府の方針への応答は早いとみられる。

規程整備の上での課題としては、規程に組織整備の内容（委員会の設置)、担当する事務局の部署を文言として書き込むことが必要となるため、それに関連する調整が必要とのことであった。また、後述の組織整備とも関連するが、規程を整備した後に、いかにその体制を運用するか、既存の委員会と新設の委員会との調整をいかに図るかといった課題が当然ある。

〇組織体制及び運用方法について

ヒアリングした大学・国立研究開発法人では、既に利益相反、安全保障輸出管理について検討する委員会、事務組織は設置されていた。一部の大学・国立研究開発法人ではそれに加えて、研究インテグリティに特化した問題を扱う委員会として、研究インテグリティ・マネジメント委員会（理事、部局長等をメンバーとする)、研究インテグリティ専門委員会（事務組織の担当課長等をメンバーとする）が新たに 2022 年、2023 年に設置された。研究インテグリティ担当室を設置した大学もあった。これらの委員会は、ポリシーの施行、助言的役割等のために、適宜開催され討議等が行われている。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

・国立大学で、特に大規模な研究大学（大学 A と大学 B）では、その広範な研究活動や複雑な問題にさらされる可能性が高いことを反映し、専門の「研究インテグリティ・マネジメント室」の設置、「研究インテグリティ・マネジメント委員会」の設置など、より専門特化した組織を持つ傾向がある。対照的に、中規模大学および私立大学（D、E、F、G 大学）は、研究インテグリティ業務を既存の組織体制（利益相反、安全保障輸出管理の委員会等）に組み込みし、担当部門間の調整を促進し、アドバイザーの役割の重要性を強調しながら、小規模に運営されている場合が多い。
・国立研究開発法人（A、B、C）では、研究インテグリティに包括的に取り組むために、さまざまな管理部門を統合することに強い重点を置いている。これらの国立研究開発法人は、大学が部局での対応の比重が大きいことと比較すると、より本部レベルで中央集権的なアプローチをとっているように見えるが、より機密性の高い研究を含んでいる可能性があるためとみられる。

全体として、どの大学・国立研究開発法人も研究インテグリティを確保するための取組をする必要性があるとの問題意識はあるものの、政府との距離、研究活動の国際化・オープン化の程度や大きさを反映して、新たなリスクへの対応のための取組の導入のスピードには差が出ている。

開示情報に基づくリスク判断の方法、関連する課題

ヒアリング対象の大学・国立研究開発法人においては、利益相反、機密技術の輸出管理、経済安全保障、研究の潜在的な軍事利用などに関連するリスクを積極的に管理している。そのアプローチは、研究者の厳格な自己開示プロセス、共同研究や提携の評価、特に外国企業との提携、外部からの影響から研究インテグリティを守ることなどが含まれる。情報の流れや技術的漏洩を包括的に管理する必要性が認識されており、多くの大学・国立研究開発法人が、開示された情報の正確性や適切性を検証する方法について模索している。

各機関とも、国際的な共同研究が増加し、機密性の高い技術が急速に開発されるなど、急速に進化する研究環境の中で、徹底的かつ効率的なリスク評価という課題に取り組んでいる。研究インテグリティの維持、セキュリティの確保、オープンで協力的な学術環境の育成のバランスは、共通のテーマである。

各機関で浮き彫りになっている課題には、研究者から詳細な個人情報や兼業等の情報を入手して確認することの難しさ、海外の複雑な資金提供や共同研究の構造を理解すること、開かれた学術的共同研究とセキュリティのバランスを維持することなどがある。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

・大規模で研究志向の国立大学（大学 A、大学 B）では、安全保障輸出管理や利益相反、研究インテグリティに焦点を当てた専門部署や委員会を設置するなど、リスク管理に対する体系的かつ包括的なアプローチを示している。中規模および小規模の機関、特に私立大学（C、E、F、G）は、個々の部局がリスク評価と管理において重要な役割を果た

している傾向があり、また、専門知識を有する外部アドバイザーからの助言も受けている。

・大学は、特にその教育的使命や、学問の自由と安全保障上の懸念とのバランスをとる必要性に照らして、利益相反等の管理を重視する傾向がある。国立研究開発法人（A、B、C）は、国家安全保障規制や輸出管理法の遵守に強い重点を置いているが、これは政府資金による研究や技術開発との関係がより緊密である可能性があることを反映しているとみられる。

<u>リスクが懸念される場合の対応プロセス</u>

ヒアリング対象とした大学・国立研究開発法人では、輸出規制の事前チェック、利益相反や安全保障輸出管理に関するアドバイザーとの協議、複雑なケースを審議・決定するための専門委員会の設置など、リスクを管理するためのさまざまな戦略を採用している。規程上の研究インテグリティとセキュリティに関する懸念やリスクに対処するための手順と体制を定めている。これには、様々な委員会、管理室、専門的な助言を行う外部組織やアドバイザーの関与が含まれる。ただし、多くの大学・研究機関では実際の対応プロセスについてはこれから学習している段階とみられる。

各機関は、新たなリスクに対応する態勢を整えており、リスクの定期的な監視・評価や、最新の規制・ガイドラインに基づくリスク管理戦略の更新を行う仕組みを持つ機関もある。多くの機関がアドバイザーとの協力関係を築いている。

<u>既存の組織体制との関係</u>

どの大学・国立研究開発法人も、安全保障輸出管理、利益相反への対応など、既存の組織構造（委員会や事務組織）の中での調整や、それら組織構造との調整を高めることが研究インテグリティの確保のためには重要であるとしている。それは、新たに研究インテグリティに関連する委員会や事務組織を設置している大学・国立研究開発法人でも、まだその途上にある大学においても同様とみられる。多くの大学・国立研究開発法人は、様々な部門間の緊密な連携の必要性を強調し、研究活動の国際化・オープン化の高まりに応じて発生する新たなリスクが、そのような緊密な連携を通じて見いだされ、対処することを目指している。

〇運営トップレベルの関与について

ヒアリングした大学・国立研究開発法人の多くは、トップレベルの管理職（理事長、学長、理事など）が、研究インテグリティ確保のための体制作り（規程整備や委員会等の体制整備）やその運営、取組の実施に関与することを重視している。

大学や国立研究開発法人では、研究インテグリティを担当する副学長や特定の管理職をガバナンスに組み込んでいる（担当理事の任命、委員会の委員長への任命など）。この体制は、内部の事務組織や、外部の専門家を含む様々な委員会によって支えられていることが多い。

また、多くの大学・国立研究開発法人では、研究インテグリティに関する懸念が発生した際に迅速に対処するため、担当事務組織から担当理事に相談するプロセスが決まっており、定期的なトップマネジメントとの協議も含まれる。

多くの大学・国立研究開発法人では、ガバナンス体制のさらなる強化に取り組んでおり、研究インテグリティとセキュリティ対策の強化に継続的に取り組んでいることがうかがえる。

ただし、一部の私立大学では、研究インテグリティに積極的に取り組んでいるものの、研究インテグリティの確保のための組織体制や業務プロセスはまだ初期段階にあり、模索しており、具体的な方針の決定や日常業務に対して経営トップの関与の度合いを決めていないところもある。

〇研修・教育、セミナーの実施について

研究インテグリティに関する教育・研修としては、e ラーニングプラットフォームの導入、情報資料の作成と配布、セミナーや研修会の開催などが挙げられる。大学や国立研究開発法人はこれまでも、利益相反、安全保障輸出管理や研究倫理に関する継続的な教育に積極的に取り組んできており、これら業務を効果的に実施するには、教員・研究者・事務職員の包括的な理解の必要性が強調されている。

研究インテグリティに関する複雑な概念を多忙な教職員や研究者に対して具体的に簡潔に伝えることの難しさ、多様で多忙な教職員が確実に理解することの難しさといった課題も認識されている。

どの大学・国立研究開発法人も研究インテグリティとセキュリティ対策の重要性を認識しているが、その教育・研修の戦略と実施規模は、利用可能な資源によっても大きく異なる。大規模な国立大学や研究大学（A、B）では、e ラーニングプラットフォームや詳細なケーススタディプレゼンテーションなど、幅広い教育ツールを取り入れ、より体系的かつ広範なプログラムを実施する傾向がある。これらの大学は、継続的な教育や、研究インテグリティを他のコンプライアンス分野と統合することに重点を置いている。

中規模および公立大学（C、D）も研究インテグリティを重視しているが、リソースが限られているため、セミナーや外部リソースへの依存度が高い。技術系大学を含む私立大学（E、F、G）は、安全保障輸出管理など特定の分野に重点を置く大学や、包括的な研究インテグリティ研修プログラムの計画段階にある大学など、多様なアプローチを示している。

〇他大学・研究機関との連携について

7 大学（A～G）、3 国立研究開発法人（A～C）へのインタビューから、研究のインテグリティ確保のための取組に関連した、他大学や研究機関との連携については、多様なアプローチや考え方があることが明らかになった。

A 大学は、国立研究大学のトップランナーとして、国内大学の中でリーダーシップを取ることを目指し、情報交換や取組に積極的である。B 大学は定期的な交流会を行っている

が、C 大学は研究インテグリティを学内の問題と考えており、外部との連携は限定的である。公立大学の D 大学は、アドバイザー的役割やコンソーシアムへの参加を通じて連携に力を入れているが、私立の E 大学と F 大学は、地域のネットワークに参加し、問題解決を共有している。

国立研究開発法人 A、B、C では、国立研究開発法人協議会（国研協）のタスクフォースでの情報共有や政府への要望の明確化などを図っており、同協議会を情報共有プラットフォームとして活用してきている。

〇政府・資金配分機関への要望・提案について

ヒアリングでは、大学と国立研究開発法人ともに、政府や資金配分機関への要望や提案があった。特に国立研究開発法人からは、研究インテグリティや情報セキュリティの確保に対する具体的な方針の設定、安定的な予算の確保、共通システムや研修構築への支援を求める声が多く聞かれた。大学からも似たような要望が出されているが、国立研究開発法人の方が具体的な要望が多かった。

研究インテグリティの確保のための取組の重要性についての理解は示されたものの、どの大学・国立研究開発法人においてもそのために要するリソースと熟練した人材の確保については、一貫した懸念が示された。特に、大規模な大学・国立研究開発法人であれば、専門部署や職員をこれらの問題に充てることができるが、小規模な大学では予算やマンパワーが限られているため、大きな苦戦を強いられているとの認識があった。研究インテグリティやセキュリティに関する業務が複雑化し、事務レベルでも法律や専門的な知識が必要になっていること、また、専門的な知識を持ったスタッフを配置する必要性について言及している。

政府や資金配分機関に対しては、より明確なガイドラインと、より実質的な支援を求めている。現在の政府からの説明会や意見交換会などの開催やガイドライン制定は評価されているが、より直接的な支援、行動のための明確な枠組み、政府各部門からの合理的なコミュニケーションの必要性を表明している。特に、私立大学からは、研究インテグリティ確保のための取組としては、最低限何をすることが必要なのかを示してもらった方が対応しやすいとの声があった。

国立研究開発法人からは、研究インテグリティとセキュリティの一体的な性質により重点を置き、強固なセキュリティインフラのための安定した資金と、政府や資金配分機関との協力のための明確なガイドラインの重要性を強調している。

３．研究インテグ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・国立研究所等で研究インテグリティに関連する業務に従事している者）を交えての意見交換会を 2023 年 10～11 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・仙台・大阪の 3 か所で開催した。

各回の説明会の開催内容は以下のとおりである。

＜プログラム＞

13:15-13:30　主催者挨拶・説明
13:30-14:30　講演と質疑応答（内閣府、警察、有識者）
・「研究インテグリティの確保に係る対応方針とその取組状況」（内閣府 科学技術・イノベーション推進事務局）
・「経済安全保障と警察の取組」（警察庁等）
・各意見交換会で以下有識者 1 名からの講演
第 1 回　「東京大学の研究インテグリティ確保に向けた取り組みと現場目線の研究インテグリティ対応」（東京大学 医学系研究科 利益相反アドバイザリー室 室長　明谷早映子）
第 2 回　「研究インテグリティの確保に向けた具体的取組の紹介－東北大学を例として－」（東北大学　金属材料研究所所長　副理事（研究公正担当）　佐々木孝彦）
第 3 回　「大学法務機能を活用した研究インテグリティ確保の実現」（九州大学 法務統括室 室長補佐・特任教授　佐藤弘基）
14:30-16:00　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を実施。
・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）を共有
・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、研究インテグリティに関するリスクへの備えに関して、所属する機関で取り組んでいることの共有
・対話 C：重要な取組を実施する上での課題等
研究インテグリティに関するリスクに備えて、所属する組織が追加で取り組むべきことと、取り組む上での課題について共有
・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に向けて、議論のポイントを検討
16:10-16:55　グループ討議結果に関する情報共有と全体討議
16:55-17:00　主催者挨拶

グループ討議は参加者が 6～8 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）、総合大学・単科大学（医科大学等）、研究大学かどうかなどを考慮し、可能な限り同種の機関が同一グループで討議できるように、事前に事務局が

行った。

各意見交換会への参加者人数（主催者・事務局と講演者を除く）は、第 1 回 43 人、第 2 回 21 人、第 3 回 42 人であった。第 1 回は国立研究開発法人からの参加者が 14 人いたが、第 2 回と第 3 回は大学関係者のみの参加となった。大学については国立大学、公立大学、私立大学のいずれの機関種からも 3 回ともに参加があった。

また、地域別に見ると、第 1 回（東京開催）は関東から、第 2 回（仙台開催）は東北から、第 3 回（大阪開催）は近畿からの参加者が多かった。ただし、今年度開催なかった北海道、中部、中国、四国、九州・沖縄地方からの参加者もみられ、ほぼ全国からの参加者があったと言えるだろう。

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、さまざまな機関からの参加があった。また、参加者の殆どは、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、担当の教員であった。

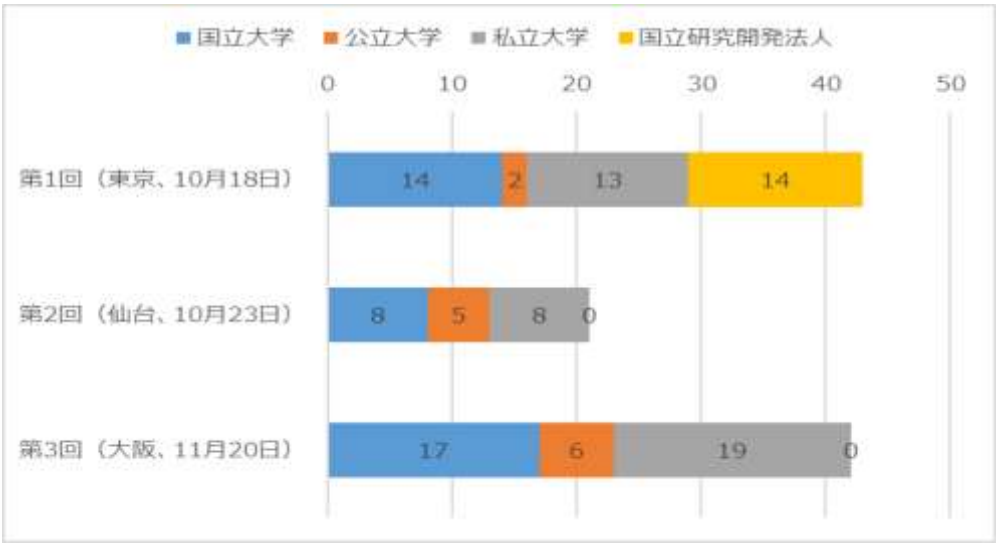


図 1 ：意見交換会への出席者人数：機関種別

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）内閣府からの説明について（参考になったかどうか（選択肢）、自由意見・コメント）、
2）警察からの説明について（参考になったかどうか（選択肢）、自由意見・コメント）、
3）有識者の講演について（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）

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図 2 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[18]、参加者

[18] 事後アンケートの回答率は、第 1 回 60%、第 2 回 76%、第 3 回 71%で、合計では 68%だった。

の意見は反映しているとみられる。3 カ所の平均を見ると、52.8%が「とても参考になった」と回答し、9 割以上の参加者が「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、全体的に満足度は高かったと考えられる。

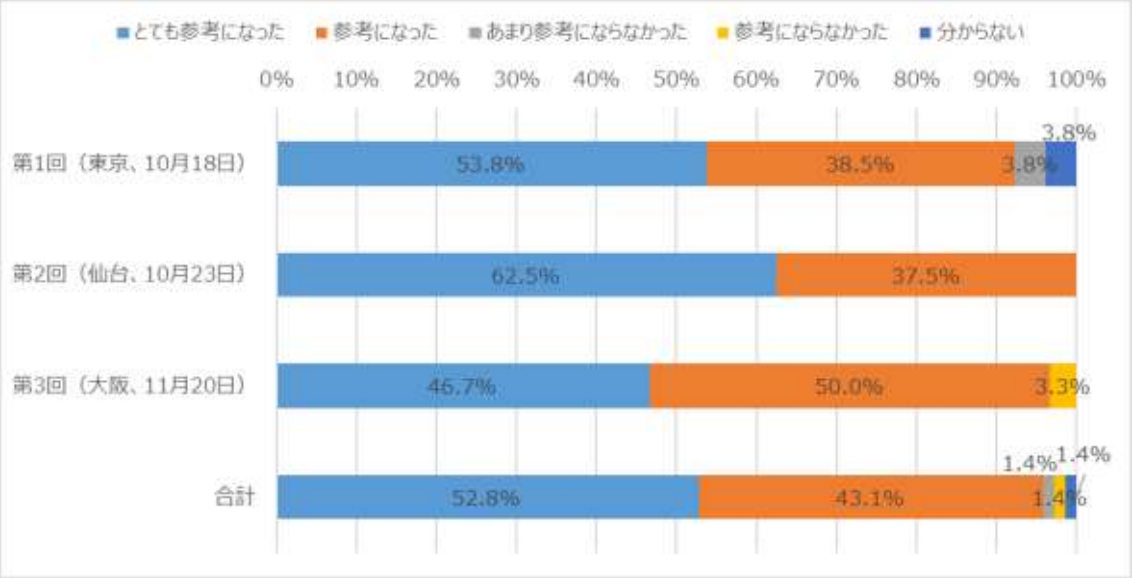


図２：意見交換会の事後アンケート結果：グループ討議について

また、内閣府からの説明、有識者の講演、グループ討議、意見交換会全体については、それぞれ自由記入により、以下のような意見があった。なお、ここでは参考になる意見等を紹介するが、自由記入で表明された意見等は必ずしも常に多数意見を反映しているとは言えないので、その点には留意が必要である。

内閣府からの講演について

政府の研究インテグリティ関連の政策についての理解が深まったとの回答があった一方で、研究インテグリティに関して、より明確なガイダンスと具体的な対策を求める声があった。研究インテグリティとセキュリティの重要性は認識されているものの、これらの基準を効果的に実施・維持するためには、より詳細で実践的なガイダンスやリソースが必要である、何が必須で、どのような対策をとるべきかについて、より明確なコミュニケーションが必要であると言った意見があった。具体的で実行可能なガイドラインがないため、大学・研究機関間の適用において一貫性が失われる可能性があるとの指摘もあった。

また、研究インテグリティの定義をより明確にし、経済的セキュリティと研究インテグリティの関係を概説するようなより包括的な資料を求める声があった。

大学職員からは、より明確な運営ガイドライン及び研究のインテグリティ維持における大学職員の役割の理解を深める必要性が強調された一方、研究インテグリティを効果的に管理するための具体的な情報やリソースの不足が共通の懸念事項として示された。また、職員や教員の意識と理解を深めることの重要性についても指摘された。

有識者の講演について

有識者からの講演は各回異なる大学教員からなされたが、参加者から共通して指摘された意見としては、第 1 に、リスク評価に関するケーススタディや方法論の共有・蓄積を強く要望している点あった。参加者は、研究インテグリティ確保に係る様々な懸念事項をそれぞれの大学・研究機関がどのように対処しているのか、具体的かつ実践的な事例に強い関心を示した。第 2 に、研究インテグリティ確保のための先進的な取組では、どのような組織構造や施策を採用しているのか、より詳細な情報の必要性が挙げられた。第 3 に、大規模大学で採用されたシステムをすべての大学・研究機関が見習うことができるのか、実施可能性への懸念が示す声があった。小規模でリソースに制限のある大学における体制構築についての意見もあった。

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は大きく 4 点にまとめることができる。第 1 に、時間的制約がある中でいかに有意義な情報交換を図るかという点である。グループ討論を高く評価しながらも、より深い議論を望んでいたとの指摘や、モデレータが主導する、より構造化された集中的なディスカッションへの要望が示された。ディスカッションの時間をもっと取りたい、他大学とは異なる視点や実践をもっと学びたい、といった声も聞かれた。第 2 は、グループ討議を通じて有効な情報共有が行われたとの指摘である。グループ討議では、さまざまな大学・研究機関の間で情報、課題、ベストプラクティスを共有する貴重な機会であった、大学や研究機関を超えた協力の重要性を強調するなどの意見があった。第 3 に、大学・研究機関のリソースの格差についての意見である。大学・研究機関によって資源や経営支援のレベルが異なるとの意見がある一方、潤沢な資金を持つ大学の参加者からは予算の制約や事務的支援に悩む他の大学と比べて、自分たちが有利な立場にあることを認識する声もあった。第 4 は、グループ討議で少人数で議論することを通じて、関係者の間でネットワーク作りができたという意見である。

意見交換会全体について

参加者は概して、意見交換会を啓発的で有益な会合であったと感じていた。参加者は、グループディスカッションや異なる機関から学ぶ機会を高く評価していた。今回の意見交換会のような対話と支援の継続的な実施が強く求められていた。ネットワーキングや継続的な議論の場の必要性を求める意見、このような議論を全国的に実施し、継続的な対話と支援のためのネットワークを構築することへの強い関心、ベストプラクティスや課題共有のための継続的なプラットフォームの必要性についての指摘などがあった。

グループ討議では、研究インテグリティについての理解度や実施レベルが多様で、機関ごとの異なることが浮き彫りになった。特に、小規模でリソースが限られている大学の参加者からは、より体系的なガイダンスや支援の必要性を指摘する声が多かった。小規模機関は研究インテグリティに取り組むための十分なスタッフやリソースを確保することが非常に困難であるため、特段の支援を求める声が多く聞かれた。多くの参加者、特に私立大学の参加

者からは、リソースの配分や具体的で実行可能なステップの必要性など、ガイドラインを実施するための実践的な側面についての強い関心が示された。

全体として、政府からのより明確なガイドラインや支援を求める傾向が見られた。研究インテグリティの定義をより明確にする必要があるとし、研究インテグリティに関連する問題の具体的取り扱いについて、より詳細なガイダンスを求める声があった。

第1章　調査の概要

1.1　調査の目的

近年、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おり、Ｇ７をはじめとする我が国と価値観を共有する国において、リスクへの対策は進展してきている。

こうした中、我が国としても研究環境の基盤となる価値を守りつつ国際的に信頼性のある研究環境を構築することが、必要な国際協力及び国際交流を進めていくために不可欠となっており、2021 年 4 月には「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティの確保に係る対応方針について」（統合イノベーション戦略推進会議）が決定された。同対応方針では、政府は、研究者及び大学・研究機関等における研究の健全性・公正性（研究インテグリティ）の自律的な確保を支援すべく、研究者、大学・研究機関等、研究資金配分機関等と連携しながら、研究者による適切な情報開示に関する取組、研究者の所属機関における対応に関する取組、研究資金配分機関等における対応に関する取組等について着手することとされており、さらに、その際には、諸外国の動向を踏まえ適時必要な検討を実施すること、大学・研究機関等と対話を継続的に行い情報提供を行う等に留意することとされている。

このような状況を背景として、本委託事業では、第１に、各国・地域における研究インテグリティに対する取組状況を調査・分析し、適宜我が国の取組と比較・分析するとともに、第 2 に、大学・研究機関の研究インテグリティの確保に係る取組の現状・課題・要望を把握することを目的に、7 大学と 3 国立研究開発法人に対してヒアリングを実施し、第 3 に、日本における研究インテグリティに対する意識醸成、課題等の抽出・整理、関係者のネットワーク形成をすることを目的に、大学・研究機関の教員・研究者・職員を対象に研究インテグリティについての意見交換会を 3 回実施した。

なお、政府では、研究インテグリティを、従来明示的に対応してきた不正行為や、産学連携における利益・責務相反に対する適切な対応や安全保障貿易管理等の法令順守などに加え、研究の国際化やオープン化に伴う新たなリスクに対して新たに求められる研究者や研究組織としての「規範」、すなわち新たに確保が求められる研究の健全性・公正性のこととしている。本調査では「研究インテグリティ」は、特に断りがない場合には、「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティ」を意味する用語として用いており、また、研究不正行為の防止・対応、産学連携活動に伴う利益相反、安全保障輸出管理に関連する取組等に関しては、調査の範囲とはしていない。

他方、「研究セキュリティ」、すなわち外国や非国家による研究への干渉を防ぐことは「研究インテグリティ」を強化することになり、また、透明性を高め、潜在的な利益相反や責務相反を開示し、リスクを管理することで「研究インテグリティ」を強化することは「研究セ

キュリティ」を守ることになるという相互関係にある[19]ことから、研究の国際化、オープン化に対するリスクへの対応について、国際的には研究セキュリティ・研究インテグリティというトピックとして議論されており、本報告書では「研究セキュリティ」の内容も調査の対象としている。

1.2　調査の内容、方法等

1.2.1　海外の取組の調査・整理・分析

次の要領で、研究活動の国際化、オープン化に伴う新たなリスクに関し、近年対応を積極的に進めているＧ７をはじめとする諸外国の政府、資金配分機関、学協会、大学・研究機関等における研究インテグリティに対する認識・取組状況について、文献調査を実施した。

① 主要国の政府、資金配分機関、学協会、大学・研究機関等の研究活動の国際化、オープン化に伴うリスクの管理に関して公表されている文書等（リスクの分類、リスクの判断基準、リスク判断のフロー、事例・想定事例等が記載されている文書等)を詳細に調査した。

調査対象国・地域は、米国、英国、カナダ、オーストラリア、EUである。

調査分析結果は、日本においてリスク判断を支援するための文書の作成を検討する際に活用できるよう、体系的・構造的にまとめた。

② 研究インテグリティに関する海外の取組の動向を把握する。

(ア) 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、各国の研究者、大学・研究機関、学協会、研究資金配分機関が、どのような枠組みで取組んでいるのか等に関する先行調査後に新たな動き（新たな文書の公表、既公表の文書のアップデート、記事等）があるかをインターネット上で継続的に調査した。

調査対象国・地域は、米国、英国、オーストラリア、カナダ、EU、フランス、ドイツである。

(イ) (ア)以外の10ヶ国程度について、研究インテグリティに関する取組状況を調査する。

なお、調査対象国については、研究インテグリティの確保のための取組に関して有益な情報が得られる国として選択した。

欧州：スウェーデン、ノルウェー、フィンランド、デンマーク、オランダ、チェコ共和国

アジア大洋州：ニュージーランド、韓国、台湾

中東：イスラエル

[19] OECD. *Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers. June 2022 No. 130. p.12

1.2.2　国内の取組の調査・整理・分析

大学・研究機関の研究インテグリティの確保に係る取組の現状・課題・要望を把握することを目的に、次の要領でヒアリングを実施した。

大学・研究機関数：10機関（7大学、3国立研究機関）

時間：1～1.5時間程度/機関

形式：オンライン（ただし、東京近郊の最大5機関については対面で実施する可能性あり）

① 事前準備

必要に応じて発注者と相談しながら、ヒアリングをする大学・研究機関の候補の選定、ヒアリング項目を検討・決定した。

② 実施

①で選定した大学・研究機関に対して、①で検討・決定したヒアリング項目に沿って、ヒアリングを実施した。

③ 実施のまとめ

ヒアリング結果を整理・分析し、現状・課題・要望、それらを踏まえ日本として今後取り組むべきこと等をまとめた。

1.2.3　日本の大学・研究機関等への意見交換会の実施

日本における研究インテグリティに対する意識醸成、課題等の抽出・整理、関係者のネットワーク形成をすることを目的に、日本の大学・研究機関等への研究インテグリティに関する説明会・意見交換会の企画・運営を主導した。なお、登壇者の候補の検討、議論のトピックなどの説明会・意見交換会の企画の検討は、必要に応じて発注者と相談しながら進めた。

対象者：研究インテグリティの実務に関わっている方々

実施形式：対面

実施回数：３回

開催地：国内主要都市（東京、仙台、大阪）

参加者数：50 名程度／回

会場形式：アイランド形式（島形式）（最大 6 グループ）

時間：約 4 時間／回

登壇者等：話題提供者として各回政府関係者や外部等の有識者２名程度、及び、グループ議論のモデレータ（最大 6 名）

その他：参加者等への飲み物の提供（茶・コーヒー等１杯／人程度）

1.3　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 主席研究員
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
浜田 志津子 公益財団法人未来工学研究所 政策調査分析センター 特別研究員
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

調査の全体取りまとめ、国内ヒアリング実施は依田が、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・浜田・多喜沢が担当した。報告書作成については、とりまとめ・海外取組（米国・カナダ・豪州・EU・チェコ共和国・韓国・台湾）・国内ヒアリング・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（スウェーデン・ノルウェー・フィンランド）について衛藤が、海外取組（デンマーク・ニュージーランド）について大竹が、海外取組（イスラエル）について多喜沢が担当した。

本調査の実施に当たっては、国内ヒアリングに協力いただいた大学・国立研究開発法人の方々、意見交換会に参加いただいた有識者と研究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、Tommy Shih 様（Associate Professor、Lund University（スウェーデン））、Tiina Vihma-Purovaara 様（Senior Ministerial Adviser、Ministry of Education, Science and Culture（フィンランド））、Holly McCracken 様（Director, Research Security; Innovation, Science and Economic Development Canada）、郭 育仁様（台湾 国立中山大学 社会科学部 日本研究センター教授）にヒアリングにご協力いただいた。謝意を表する。

なお、報告書の記述の責任は本委託業務の受託者である未来工学研究所にある。

第2章　各国・地域における研究インテグリティに対する取組状況

2.1　米国

2.1.1　2022 年度までの経緯

米国では、トランプ前政権が政権交代直前の 2021 年 1 月 14 日に「米国政府支援の研究開発に関する国家安全保障戦略についての国家安全保障大統領覚書 33 号」（*National Security Presidential Memorandum-33*（NSPM-33））を発出した。同大統領覚書では、「中華人民共和国を含む一部の外国政府は、開かれた科学的交流への相互献身を示しておらず、研究を行うためのコストとリスクを回避するために、米国及び国際的に開かれた研究環境を利用しようとし、それによって、米国、その同盟国、パートナーを犠牲にして、経済及び軍事競争力を向上させようとしている」と説明し、「米国政府が支援する研究開発（R&D）を、外国政府の干渉や搾取から守るための行動を指示する」としている。なお、この文書及びその後の米国における取組においては、「研究活動の国際化、オープン化に伴う新たなリスクに対する研究インテグリティ」に相当する用語として「研究セキュリティ（research security）」あるいは「研究セキュリティとインテグリティ（research security and integrity）」が用いられている[20]。

バイデン大統領は、2021 年 1 月の大統領就任後に NSPM-33 を追認する一方で、トランプ政権下の 2018 年に司法省で始まった、大学・研究機関で活動する中国のスパイ研究者の摘発キャンペーンである「China Initiative」については 2022 年 2 月に終了させている。

また、2022 年 1 月 4 日、大統領府 OSTP は、「NSPM-33 実施ガイダンス」（*Guidance for Implementing National Security Presidential Memorandum 33*（NSPM-33））を発表した。同文書の目的は、「連邦省庁に対し、NSPM-33 の実施に関する指針を提供すること」にある。各機関がその実施努力に適用すべき一般的なガイダンス（general guidance）が述べられ、さらに NSPM-33 において取り上げられた、研究セキュリティの確保に関連する 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の結果、4. 情報の共有、5. 研究セキュリティプログラム）に関する詳細なガイダンスを含む内容となっている。

このように、米国では研究セキュリティの確保のために大統領覚書（NSPM-33）が大統領から、その実施ガイダンスが大統領府 OSTP（Office of Science and Technology Policy（科学技術政策局））が事務局を務める委員会から発出されている。それらとともに、2020

[20] NSPM 33 implementation plan によれば、研究インテグリティは「研究開発活動の提案、実施、評価、報告において、客観性、正直さ、透明性、公平性、説明責任、スチュワードシップなどの専門的な価値観や原則を遵守すること」（Adherence to professional values and principles – including objectivity, honesty, transparency, fairness, accountability, and stewardship – in proposing, performing, evaluating, and reporting research and development activities）と、研究セキュリティ（research security）は「国家や経済の安全保障を損なう研究開発の不正利用を目的とした行為、関連する研究インテグリティの侵害、外国政府の干渉から研究事業を保護すること」（Safeguarding the research enterprise against behaviors aimed at misappropriating research and development to the detriment of national or economic security, related violations of research integrity, and foreign government interference）と説明されている。

年度国防権限法（2019 年 12 月）、2021 年度国防権限法（2021 年 1 月）、CHIPS and Science Act（2022 年 8 月）に関連する条項が規定されている。このように、法令面では「研究セキュリティ」の確保に係る法律が連邦政府大統領府レベルで規定され、他方体制面では CIA や FBI といった情報機関を含む関連する連邦省庁が一体となって、研究者、大学・研究機関、資金配分機関に対して、研究セキュリティ確保のための様々な要求を行うと同時に、研究セキュリティプログラム策定や支援センター設置などの支援の強化も図られつつある。このように、法令と組織体制を両輪とする制度整備が米国の大きな特色である。[21]

表 2-1：近年の研究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
2019.12.6	Fundamental Research Security（通称：JASON Report）<https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf>	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（トランプ前大統領時）
2021.1.19	Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise <https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/NSTC-Research-Security-Best-Practices-Jan2021.pdf>	Subcommittee on Research Security, Joint Committee on the Research Environment, National Science & Technology Council
2021.8.10	Clear Rules for Research Security and Researcher Responsibility <https://www.whitehouse.gov/ostp/news-updates/2021/08/10/clear-rules-for-research-security-and-researcher-responsibility/>	Dr. Eric Lander (President's Science Advisor and Director of the OSTP)
2022.1.4	Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33). <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>	ホワイトハウス
2022.8.31	An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity <https://www.whitehouse.gov/ostp/news-updates/2022/08/31/an-update-on-research-securitystreamlining-disclosure-standards-to-enhance-clarity-transparency-and-equity/>	Morgan Dwyer ら（OSTP）OSTP ブログ
2023.2	Draft Research Security Programs Standard Requirements	Subcommittee on Research

[21] 以上の説明については、「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）に基づく（pp.viii~xi）。

発行年	文書名	発行元
		Security, Joint Committee on the Research Environment, National Science & Technology Council

出典：スタンフォード大学ウェブサイト．”Academic Integrity and Undue Foreign Interference” <https://doresearch.stanford.edu/topics/academic-integrity-and-undue-foreign-interference#Policies_&_Resources>などに基づき作成。「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。

表 2-2：近年の研究インテグリティ関連法（米国議会）

発行年	法律名	発行元
2019.12	2020 年度国防権限法（FY 2020 National Defense Authorization Act (NDAA)）※第 1746 条に、大統領府科学技術政策局（OSTP）が主導し、国家科学技術会議（NSTC）に米国科学技術の海外からの干渉等からの保護等を検討するための省庁間ワーキンググループを設置すること、全米アカデミーズに科学技術安全保障円卓会議を設置すること等を規定。	米国議会
2021.1	2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）※第 223 条で研究提案時等の情報開示について規定	米国議会
2022.8	CHIPS and Science Act 2022	米国議会

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、2023 年3月、7頁）を更新.

2.1.2 最近の主な動き

以下は、本委託調査の実施時期である2023年4月以降の主な動きである。上記の大統領覚書（NSPM-33）の実施ガイダンスや、CHIPS and Science Act（2022年8月）の関連条項で政府に実施を求められていることなどが順次実施されてきている。

(1) 大統領府科学技術政策局における動き等

2023年2月28日に大統領府科学技術政策局（Office of Science and Technology Policy）の研究セキュリティ小委員会が「研究セキュリティプログラム」ドラフト（DRAFT Research Security Program Standard Requirement）を公表した。同文書では、海外渡航のセキュリティ、研究セキュリティのトレーニング、サイバーセキュリティについて説明をしている。[22]

同文書については、パブリックコメントが実施され（2023年3月2日～6月5日）、公平

[22] この内容については、「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、49～51 頁）を参照。

性、明確性、実現可能性、負担、コンプライアンスに関して意見が求められた。Association of American Universities (AAU)等から意見提出があった。

2024年2月の現時点において、パブリックコメントの終了後の本文書をめぐる動向は確認できない。

(2) 米国科学財団（NSF）における動き等

研究セキュリティ分析のNSFガイドラインの公表

NSFは2023年6月に「研究セキュリティ分析のためのNSFガイドライン」（NSF Guidelines for Research Security Analytics）を公表した。同ガイドラインでは、新たに設置された「研究セキュリティ戦略・政策課」（Office of the Chief of Research Security Strategy and Policy）の責任、分析プロセス、原則等について説明している。[23] 詳しい内容については2.1.3で説明する。

「研究セキュリティプログラムについての研究」の開始

NSFは2023年7月12日に、「研究セキュリティプログラムについての研究」（Research on Research Security Program）を開始することを公表した[24]。このプログラムでは特に、研究セキュリティ・リスクを特定する方法と、それを防止・軽減するための戦略を評価するプロジェクトに資金が提供される。

プログラムの開始を前に、NSFは意識向上のためのワークショップに資金を提供し、国内外の研究セキュリティの専門家を集め、新プログラムで研究すべきテーマやトピックを特定する。会議の成果は今後公開される予定である。同プログラムで想定される研究トピックの候補として以下のようなテーマが挙げられている。同ワークショップではこれら以外のトピックも含めて、重視すべきトピックについて議論が行われる予定である。

NSF「研究セキュリティプログラムについての研究」プログラムのテーマ候補

○研究セキュリティ上の脅威の性質と蔓延性（pervasiveness）

- 研究セキュリティ上の脅威や違反の種類、蔓延度、頻度、深刻度、潜在的な意味合いと影響、最も頻繁に標的とされる分野と技術。
- 研究セキュリティに関する規則や規制に違反する動機付けや強要の要因。
- 公開されている基礎／基盤研究の分類やその他の制限を正当化する要因。
- 研究セキュリティ問題への取組が過度に積極的であったり、不十分であったりすることによって生じうる、基礎／基盤研究のエコシステムへの脅威。

[23] NSF. *NSF Guidelines for Research Security Analytics*. June 2023.
<https://new.nsf.gov/research-security/guidelines>
<https://nsf-gov-resources.nsf.gov/2023-05/NSF%20Research%20Security%20Guidelines-2023.pdf>
[24] NSF website. “NSF announces Research on Research Security Program” July 12, 2023.
<https://new.nsf.gov/news/nsf-announces-research-research-security-program>

・ 研究セキュリティに関する規則や規制に起因する、学問の自由に対する現実的または認知された制約。
・ 利用を前提とした基礎研究と好奇心を重視した基礎研究（use-inspired and curiosity-driven foundational research）との間の研究セキュリティ・リスクの対比や、基礎研究から応用研究、トランスレーショナルリサーチに至るまでの研究セキュリティ・リスク。
・ 研究セキュリティ上の脅威や違反を予測する能力、そのような予測を行うために必要なデータ、予測に関連する不確実性の定量化。

〇研究セキュリティ上の脅威・違反の特定、緩和、予防

・ 研究者及び研究組織のリーダーが、研究セキュリティ上の脅威及びそれらに対処するための現在の取組についてどの程度理解しているか、また、それらの理解に役立つ情報源は何か。
・ 研究セキュリティに関する現在の教育・訓練活動の有効性と、その有効性を改善する方法。
・ 科学と研究に関する意見の相違や誤った情報が、研究セキュリティの脅威や違反の特定、緩和、防止に与える影響。
・ 研究セキュリティ上の脅威や違反について、個人や組織からの報告を妨げる要因と、報告を改善するために取り得る措置。
・ 研究セキュリティ上の脅威や違反の発見と予防のための、定量的なリスク測定・軽減機能の活用。
・ 研究セキュリティ上の脅威や違反の発見・軽減に役立つ人工知能（AI）の活用と、AIが意図せず、あるいは意図的に脅威や違反を助長する可能性のある方法。

〇研究セキュリティの国際的側面

・ 研究セキュリティにおける米国の取組と他国の取組の比較、研究セキュリティにおける国際協力の可能性と望ましいあり方、米国が研究セキュリティにおいて協力すべき相手国の選定を導くための基準。
・ 研究セキュリティ上の脅威と国内政策の決定が、外国人のSTEM人材の採用と維持に与える影響。
・ 研究セキュリティ上の脅威の特定と緩和に対する現実的・認知的なスティグマ（汚名）の影響と、それを克服するための戦略。

出典：NSF 23-126. Dear Colleague Letter: Workshop to Inform Development of the NSF Research on Research Security Program (RRSP). June 29, 2023 <https://www.nsf.gov/pubs/2023/nsf23126/nsf23126.jsp>

「研究セキュリティ・インテグリティ情報共有分析組織」の設置のための公募実施

2023年8月2日に、NSFは「研究セキュリティ・インテグリティ情報共有分析組織」（Research Security and Integrity Information Sharing Analysis Organization（RSI-ISAO））の設置のための公募を開始した。大学・非営利機関・民間企業が応募することが可能である。公募提案書の受付は10月30日に締め切られている。なお、同組織の設置は、「2022年CHIPSおよび科学法」の第10338条においてNSFに求められている。

NSFの担当部署は、研究セキュリティ戦略ポリシー課（Office of the Chief of Research

Security Strategy and Policy）である。独立した支援組織を政府との契約に基づき設立し、米国の研究コミュニティが外国政府の干渉に対処することを支援し、研究コミュニティの利害関係者同士や、NSFを通じてそれらの利害関係者と米国政府機関をつなぐパイプ役とすることを目指しているとのことである。

公募情報によれば「研究セキュリティ・インテグリティ情報共有分析組織」の概要は以下のとおりである。

「研究セキュリティ・インテグリティ情報共有分析組織」の概要

○RSI-ISAOの主な任務は以下のとおりである。これらの任務は、研究セキュリティにおける３つの機能領域、1）ツール・訓練、2）コミュニティ参加・問い合わせ、3）データ分析・報告のいずれかに分類することができる。

- 情報のクリアリングハウスとしての役割
- 標準的なリスク評価フレームワークとベストプラクティスの開発
- 研究セキュリティリスクに関するタイムリーな報告書の提供
- 研修と支援の提供
- 標準化された情報収集の実現
- リスクと識別のパターンの分析を支援する。
- 研究セキュリティ強化のためのその他の適切な措置

○利害関係者の関与と法的要件に基づき、RSI-ISAOは以下を行う。

- 研究コミュニティの全メンバーに均一な質のサービスを提供する
- 研究組織、および組織または関連団体を通じた研究者個人からの具体的な支援要請に対応する
- 一般に入手可能な情報および米国政府機関からの機密解除された情報を含む、unclassifiedの情報のみを取り扱う。
- 研究関係者のために、米国政府機関、研究機関、民間部門から提供された情報に基づいて分析を行い、報告書を発行する。

○授与情報

初年度の資金は最高950万ドルで、受賞と同時に確約される。その後の2年目から5年目までの助成金は、予算が確保されるまでの間、1年あたり少なくとも1,000万ドルとなる可能性があり、指定された目標に対する達成度について毎年十分なレビューが行われることが条件となる。

○賞の授与数

2023年度の資金を使用し、2024年度に1件の協力契約が締結される。

「略歴、現在および保留中の（その他の）支援に関する共通の開示書式」の公表

NSFは、2023年11月に「略歴、現在および保留中の（その他の）支援に関する共通の開示書式」（Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support）を公表した[25]。全米科学技術評議会（NSTC）の研究セキュリティ小委員会は、数か月間かけて、上級職員が使用するための一貫した開示要件の作成に取り組むとともに、連邦研究開発（R&D）補助金または協力協定の申請書の略歴および現在および保留中の（その他の）支援セクションの共通開示書式案の作成に取り組んできていたとのことである。

NSPM-33 実施ガイダンスの「開示要件と標準化」セクションでは、「開示要件（誰が何を開示するか、関連する制限と除外など）、開示プロセス（更新、訂正、証明、裏付け文書の提供など）、期待される省庁横断的な統一度について明確にする」こととしていた。

４つの研究セキュリティのオンライン教育モジュールの公表

NSFは2024年1月30日に、全米の研究者や研究機関が利用できる、以下の4つのインタラクティブなオンライン研究セキュリティ・トレーニング・モジュールの提供を開始した。[26]対象は米国の研究者や研究機関であるが、日本からもアクセス可能である。

・モジュール1：研究セキュリティ入門　https://rst.nsf.gov/introduction/story.html
・モジュール2：情報開示の重要性　https://rst.nsf.gov/disclosure/story.html
・モジュール3：リスクの管理と軽減　https://rst.nsf.gov/risk/story.html
・モジュール4：国際協力の重要性　https://rst.nsf.gov/internationalcollaboration/story.html

NSF は 2022 年 12 月に「Research Security Training for the United States Research Community program」の公募を実施し、上記の４つのトレーニング内容について、以下の４件の提案（期間と助成金額）が選定された（NIH、DOE、DOD と共同で助成）。[27]

- Research Security Training: The Importance of Research Security, The University of Alabama in Huntsville（１年間（2022/11～2023/10）、＄477K）
- Research Security Training: The Importance of Disclosure, Texas A&M University System（１年間、＄471K）
- Research Security Training: Risk Management and Mitigation, University of Pennsylvania（１年間、＄306K）
- Research Security Training: International Collaboration, Associated Universities, Inc., and AUI Labs（１年間、＄499K）

[25] NSF website. “NSTC Research Security Subcommittee: NSPM-33 Implementation Guidance Disclosure Requirements & Standardization” <https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp>
[26] NSF website. “NSF research security training modules now available”. January 30, 2024. <https://new.nsf.gov/news/nsf-research-security-training-modules>
[27] 「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、57 頁）

NSFの「研究提案・助成ポリシー手続きガイド」（PAPPG）の内容更新

NSFは2024年５月24日に効力開始となる、Proposal & Award Policies & Procedures Guide (PAPPG)の内容更新を行った[28]。2022年CHIPS及び科学法（CHIPS and Science Act）の要求等による変更を含む。研究セキュリティと外国人人材プログラムに関連した変更としては、悪質な外国人材採用プログラムの当事者である個人は、NSF提案の上級／キーパーソンを務める資格はないことを明記した新しいセクションの追加等（第I.E.3章(b)、第II.D.1.d(ix)章、第II.D.1.e(ii)章）であった。また、海外からの資金援助に関して、2022年CHIPS及び科学法で義務付けられた年次報告要件を取り入れるための修正が加えられた（第II.B章）。

(3) 国防省における動き等

基礎研究プロジェクト審査についての国防省方針

国防省は、2023年6月に「基礎研究プロジェクト審査についての国防省方針」を発表した（Department of Defense. Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education. June 29, 2023.）[29]。以下のような３部構成である。

第1部：基礎研究のリスクベース安全審査に関する方針の紹介
第2部：基礎研究提案の緩和決定に役立つ意思決定マトリックスの紹介
第3部：2019会計年度ジョン・S・マケイン国防修正授権法（公法115-232）第1286条を受けて公表されたFY22年度リストの紹介

同文書は「基礎研究提案の利益相反緩和の判断材料となる決定マトリクス」（Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions）を含む。プログラム管理者（program managers）と国防省構成機関（DOD Components）が基礎研究提案の潜在的な利益相反を審査する際に役立つ手引書になる。

孔子学院免除プログラム

2021会計年度の国防権限法（NDAA）第1062条では、孔子学院を設置（host）している米国の高等教育機関について、国防長官から免除を受けない限り、同省が資金を提供することを禁止しており、資金提供の禁止は2023年10月1日に発効した。

---

[28] NSF website. “Summary of Changes to the PAPPG (NSF 24-1)” <https://new.nsf.gov/policies/pappg/24-1/summary-changes>

[29] Department of Defense. Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education. June 29, 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?et_rid=900087807&et_cid=4802420>
DOD website “Academic Research Security” <https://basicresearch.defense.gov/Programs/Academic-Research-Security/>

国防省は、「孔子学院免除プログラム」（Confucius Institute Waiver Program (CIWP)、DoD Office of the Under Secretary of Defense for Research and Engineering）に基づいて、孔子学院を主催し、2021NDAA第1062条によって要求される資金提供の禁止からの免除を希望する米国の高等教育機関からの免除申請を検討し、承認または拒否する。

(4) その他

全米アカデミーズ報告書

全米アカデミーズ（National Academies）は2023年に報告書「米国高等教育機関における外国資本の言語・文化機関：リスク評価・緩和のための施策」（Foreign-Funded Language and Culture Institutes at U.S. Institutions of Higher Education: Practices to Assess and Mitigate Risk）を公表した[30]。同報告書は、以下を含めて８つの提言をしている。

提言1：米国の受入機関は、学内の外国資本の語学・文化教育機関に関連するリスクを特定し、対処し、軽減するための適切な方針、手順、プロセスを策定し、実施すべきである。

提言3：米国の受入機関は、パートナー国が懸念国と見なされる場合、当該パートナー国を考慮すべきである。この場合、米国の受入機関は、そのような国と関係のある語学・文化教育機関がもたらす可能性のあるリスクをよりよく理解し、軽減するために、追加的な審査を検討すべきである。

提言5：連邦研究費が5,000万ドル未満であり、NSPM-33の対象外である研究機関に対し、研究セキュリティに関する提言と実施可能な慣行の策定を支援するため、追加調査を実施すべきである。

議会特別委員会報告書の公表

2023年12月に、米国議会下院の特別委員会が、米中関係についての報告書を策定し、公表した[31]。「米国と中国共産党の戦略的競争に関する下院特別委員会」（House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party）は、中国の侵略と経済操作のパターンを研究し、中国との経済的・技術的競争についての戦略を提言している。戦略には3つの柱があり、このうち、第２の柱である「中国の軍事近代化と人権侵害を助長する米国の資本と技術の流れを止めること」という提言、および提言４の「米国の研究セキュリティを強化し、悪意のある人材リクル

[30] National Academies (2023). Foreign-Funded Language and Culture Institutes at U.S. Institutions of Higher Education: Practices to Assess and Mitigate Risk. <https://nap.nationalacademies.org/catalog/27065/foreign-funded-language-and-culture-institutes-at-us-institutions-of-higher-education>

[31] House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*. 2023.

ートを防御する」が研究インテグリティ、研究セキュリティに関係する内容となっている。提言 4 の具体的内容は以下の8点を含む。

1) NSPM-33ガイドラインを拡大し、連邦研究助成金申請者自身および主要なチームメンバーについて、外国団体との関係や利害関係の開示を義務付け、毎年更新する。
2) 防衛・軍事研究に関与する中国研究機関を追跡するデータベースを構築し、米国の大学や連邦機関が共同研究や助成金提案を評価する際に役立てる。
3) 国際貿易局の統合審査リスト（International Trade Administration's Consolidated Screening List）、国防省の中国軍事企業リスト（Department of Defense's Chinese Military Companies List）、米空軍の中国航空宇宙研究所の中国国防科学技術重点研究室リスト（U.S. Air Force's China Aerospace Studies Institute's list of PRC Defense Science and Technology Key Labs）に掲載されている企業を含め、米国企業が軍事・国防研究開発（R&D）に携わる中国企業との研究協力に関与することを禁止する法律を制定する。
4) 外国の敵対国との重要技術に関する共同研究において輸出規制品目を使用する場合、米国の研究機関に輸出管理ライセンスの取得を義務付ける。
5) 高等教育法第117条の施行を監督し、米国の大学に対し、外国からの贈与や契約を教育省に開示することを義務付ける。
6) 米国の大学に対し、海外からの贈与や契約の受益者を特定するための「顧客・寄付者把握（know-your-customer/donor）」ルールの適用を義務付けることにより、第117条を強化する。
7) 国務省に対し、中国との科学技術協定に「人権」と「軍事目的使用」のガードレールを設けることを義務付け、議会の委員会との協議を確保する。
8) 基礎研究のために連邦政府から補助金を受ける大学に対し、NSPM-33の実施を義務付け、リスクベースのセキュリティ審査を実施し、中国の悪意ある影響や技術移転のリスクに対抗する。

なお、特別委員会には立法権限がある訳ではないので、上記の提言を実現するためには、議会で法律として採択されることが必要となる。

2.1.3 研究活動の国際化、オープン化に伴うリスクの管理のための主な取組

米国では、National Security Presidential Memorandum 33（NSPM-33）に基づき、研究セキュリティ・インテグリティ政策について各省が分権的なアプローチを取っている。NSF、国防省がそれぞれの政府研究費に基づく研究プロジェクトについてのリスク判断の文書を策定し、いずれも 2023 年 6 月に公表している。

(1) 米国科学財団（NSF）における取組

NSF は、2023 年 6 月に NSF Guidelines for Research Security Analytics を公表している[32]。同文書では、定義（第 5 節）、Office of the Chief of Research Security Strategy and Policy（OCRSSP）の責任とプロセス（第 6 節）、NSF 職員によるモニタリング・報告（第 7 節）、OCRSSP による許可・禁止行為（第 8 節）、研究セキュリティ分析のためのデータ・サービス・分析手法（第 9 節）、研究セキュリティ関連情報の共有原則（第 10 節）について説明しており、研究セキュリティ関連の調査を要する事例も挙げられている。

- Office of the Chief of Research Security Strategy and Policy (OCRSSP)は、NSF 内で唯一、研究セキュリティに関連する高度な監視・検証活動を行うことを承認された部署である（NSF における研究セキュリティに関する調査部署の一元化の原則)。（第 6 節）
- 1）提案機関・受賞機関に対する研究セキュリティに関する連絡は、すべて OCRSSP のみが行う。 2）OCRSSP の活動は検証（verification）に関連するものであり、調査活動（investigation）は行わない。 3）プログラムスタッフが、PI と研究セキュリティ上の懸念について話し合うことは許されない。研究セキュリティ上の懸念をメリット審査プロセスに組み込むことも許されない。（メリットレビューと研究セキュリティの判断との分離の原則）（第 6 節）
- OCRSSP のスタッフは、特定の国籍や人種的アイデンティティを選択するような分析を行うことが禁じられている（国籍・人種による分析の禁止)。（第 8 節）
- 研究セキュリティ分析には、SCOPUS、Web of Science,米国特許商標局特許データベースが使用される。情報開示された研究資金、所属等とこれらの論文データ等の情報のミスマッチを調べる。（9 節）

(2) 国防省における取組

前述のように、国防省では、2023 年 6 月に「高等教育機関における国防省資金配分による研究における望まない海外からの干渉への対抗」（Department of Defense. Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education. June 29, 2023.）を策定し、公表している。国防省全体で一貫した透明性のある実施を確保し、国防省が資金提供する研究者や機関に現実的な期待を持たせ、法律や規則を遵守し、無差別であることであることが本文書の目標である。

この方針には、"Decision Matrix to Inform Fundamental Research Proposal Mitigation Decisions "（基礎研究提案の利益相反緩和の判断材料となる決定マトリクス）と "FY22 Lists Published in Response to Section 1286 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) as amended "

[32] https://new.nsf.gov/research-security/guidelines
https://nsf-gov-resources.nsf.gov/2023-05/NSF%20Research%20Security%20Guidelines-2023.pdf

（「2019 会計年度ジョン・S・マケイン国防授権法（公法 115-232）改正 1286 条に対応して公表された FY22 リスト」）という 2 つの文書が添付されている。

- 「基礎研究提案の利益相反緩和の判断材料となる決定マトリクス」は、プログラム管理者（program managers）と国防省構成機関（DOD Components）が基礎研究提案の潜在的な利益相反を審査する際に役立つ手引書である。この文書はまた、利益相反の種類とそれが発生する時間枠に応じて、緩和が必要または推奨される条件についても記述している。
- 「FY22 リスト」は、同法 1286 条(c)(8)(A)に記載された問題のある活動に従事していることが確認された外国機関を特定するもので、問題のある外国の人材プログラムも特定されている。

(3) DARPA における取組

特に、国防省の研究機関である DARPA には、「海外からの影響対策プログラム」（Countering Foreign Influence Program: CFIP）がある。同プログラムは、不当な外国からの影響の可能性を特定することにより、DARPA の研究プロジェクトに関連する重要な技術及び実施者の知的財産の保護を支援することを目的とした適応型リスク管理セキュリティプログラムである。（2022 年版報告書の 2.1.2 節(4)を参照（p.69））

CFIP のリスク評価は、標準フォーム（SF）424「Senior/Key Person Profile (Expanded)」及びその付属文書又は参照文書に記載されている情報に基づいて行われる。不当な外国による影響力のリスク評価プロセスは、SF424 に記載されているすべての報告情報に注目し、過去 4 年間のシニア/キーパーソンの活動に最も重点を置いている。CFIP のリスク評価は、外国の影響を受けた利益相反又は責務相反を構成する可能性のある外国関連活動等の量、種類、時期に応じて、「低い」から「非常に高い」までに区分されている。国籍や市民権は、このプロセスでは収集されず、リスク評価の要因にはならない。

CFIP リスク評価プロセスは、DARPA の科学的審査プロセスとは別に実施され、最終的な授与の前に裁定される。CFIP リスクアセスメントの結果、リスク評価と関連するリスク軽減又は受諾のガイダンスが提示される。

2.2 英国

2.2.1 2022 年度までの経緯

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。

「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、研究インテグ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 Academics」を公表した。

2020 年 10 月、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、研究インテグリティについて理解させるうえで、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」を発行した。

2021 年 6 月、英国政府は、「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）を制定し、2022 年 1 月に、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」を公表した。

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)を設立した。

一方、英国の R&D 資金配分機関である UKRI（UK Research and Innovation)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「Managing risks in international research and innovation」を、2022 年 6 月に共同で公表した。

このように、英国では、「Trusted Research」を柱として、政府機関、大学機関及び R&D 資金配分機関が一体となって、大学・研究機関における研究インテグリティの取組を支援してきたということができる。

2.2.2 最近の主な動き

2024 年 1 月時点の段階で、英国政府において、研究インテグリティに関して新しい展開は見られないが、2023 年 9 月に、前述した RCAT の活動状況に関するアップデート情報として、RCAT の 2022 年から 2023 年にかけての活動状況に関する情報（Research Collaboration Advice Team: progress made from 2022 to 2023）が公開[33]されていることが確認された。

また、UUK に関しては、UUK が 2020 年 10 月に公表した「Managing risks in internationalization: Security related issues」に関連して、大学が直面する安全保障上の脅威、安全保障の脅威に対処するために多くの大学が講じている措置、大学で安全保障ガイダンスを実装する方法、大学全体で安全保障を重視する文化を根付かせる方法等について纏めたものを、「Security and risk: how universities can protect their research and people」というタイトルでウェブサイト上に公開[34]されたことが確認された（2023 年 6 月更新）。

以下これらの情報について示す。

(1) RCAT に関するアップデート情報

以下、RCAT の 2022 年から 2023 年にかけての活動状況を中心とした主なアップデート情報を示す。

a. RCAT の目的

RCAT は、変化する研究安全保障の状況について政府からの明確な助言を求める学術界の需要に応えるため、2021 年に設立された。RCAT には、以下の 3 つの戦略的な優先事項がある。

- 国際的な研究協力における国家安全保障上の懸念、特に特定の活動やパートナーシップに適用される必要のある規制について、研究会に信頼される助言を提供する。
- 「Trusted Research」に関してより良い理解と適用を構築するために研究機関と協力し、段階的に研究文化を変えていくことを支援する。
- 研究機関が扱っている様々な問題についての情報を収集・共有することで、研究界や政府がより微妙な理解ができるように支援する。

[33] https://www.gov.uk/government/publications/research-collaboration-advice-team-progress-made-from-2022-to-2023/research-collaboration-advice-team-progress-made-from-2022-to-2023
[34] https://www.universitiesuk.ac.uk/topics/funding-finance-and-operations/security-and-risk-how-universities-can）

b. RCAT の進捗状況

- 2022 年 3 月以来、RCAT のアドバイザーは 130 以上の研究機関と関わってきた。RCAT のアドバイザーは、研究機関内の研究室と秘密厳守で継続的に対話を行っている。
- RCAT のメンバーは完全に採用され、訓練を受けている。RCAT は、バーミンガム、カーディフ、エディンバラ、ロンドン及びサルフォードに拠点を置く 12 人のアドバイザーと 15 人のスタッフで構成されている。
- RCAT は、政府の主要部署と強固な協力関係を築いている。こうした関係は、学界に対して政府横断的な助言を結びつけるという RCAT の目的にとって極めて重要である。
- RCAT は学界から概ね好評を得ており、今後さらに助言サービスを発展させる計画もある。最近行われた RCAT による学界へのアンケートには 90 名から回答が寄せられ、助言サービスの発展に影響を与えるために利用される予定である。

c. RCAT が学んでいること

RCAT のアドバイザーは、100 件以上の複雑な事例の管理を含め、研究機関や研究室が直面する問題について 350 件以上の助言を提供してきた。助言を行った中で最も多かったのは、以下の 5 つの問題であった。

- 輸出管理（32%）
- 特定の問い合わせ（23%）
- 国家安全保障・投資（NSI）法（18%）
- 機関のガバナンスと研究セキュリティ・ポリシー（15%）
- 学術技術承認スキーム（ATAS）（9%）

RCAT は、英国の研究が直面している具体的な脅威、敵対的なアプローチ及び存在する脆弱性について、より明確なイメージを構築している。

RCAT はまた、具体的かつ詳細な事例について、大学側と連携し、個別の助言が必要な場合には助言を提供してきた。これらの事例の大半は、研究界から提起されたものであり、研究界が RCAT との協力に積極的であることを示している。

リスクの高い共同研究において、RCAT が懸念を抱いている研究分野には以下が含まれる。

- 先端材料
- 人工知能
- 先端ロボット工学
- 合成生物学
- 量子技術
- 宇宙技術

RCAT は、研究機関がリスク情報を活用した意思決定ができるように、特定の共同研究についての問い合わせに合わせた助言と緩和策を提供している。

(2) Security and risk: how universities can protect their research and people

以下、「Security and risk: how universities can protect their research and people」の構成と概要を示す。

a. 大学が直面する安全保障上の脅威

大学が直面する最も顕著な安全保障上の問題は、敵対的な国家主体からの脅威であるとし、大学は、国家主体や非国家主体から、以下のような様々なリスクに直面しているとしている。

- サイバー攻撃などの積極的な敵対行為や違法行為、あるいは詐欺的な、あるいは法的に曖昧な事業提案や慣行を通じて、個人的、経済的及び社会的利益を追求する。
- 経済的及び軍事的利益のために、他国に対する科学技術の優位性を高めようとする。
- 彼ら自身の国民に対して、それらの優位性を利用することを追求する。
- 人権侵害の非難に対する広報手段として、英国との科学的・経済的関係を利用する。

b. 安全保障の脅威に対処するために多くの大学が講じている措置

- 研究、財務、慈善活動等の部門に跨って、デューディリジェンスに関する管理を統一する。
- リスク登録簿を見直し、大学内のチーム間で共有する。
- デューディリジェンスのプロセスとチェックの見直しを行う。
- 組織の価値観、学問の自由及び言論の自由に関する方針を更新・改訂・作成する。
- 必要に応じて、ポリシーや研修プログラムの見直しを行い、安全保障関連事項に関する職員研修の見直しを行い、新たなワーキンググループや報告プロセスを創設する。
- 仮想的・物理的な安全保障インフラを更新するために、サイバー攻撃や物理的な侵入テストを実施する。
- フィッシングメールのテスト、訪問者のシミュレーション、ユースケースに照らした危機発生時の手順など、ポリシーの「ストレステスト」を実施する。

c. 大学で安全保障ガイダンスを実装する方法

- 上級幹部チームメンバーの一人に、安全保障関連事項の責任者を任命する。
- 英国で発行されている 3 つの主要ガイダンス（「Trusted Research Guidance for Academics」、「Managing risks in internationalization: Security related issues」及び「Trusted Research and Innovation Principles」）と関連するガイダンスを確認する。
- 安全保障に関連する専門知識を有する、所属機関全体の利害関係者からなるチームを編

成する。

- 既存の関連プロセスをレビューし、プロジェクト計画として経営幹部や理事会に提示できるような、推奨されるアクションのリストを、提案された実施期間とタイムスケールとともに特定する。
- 上級責任者が明確に定義されたアクションプランを策定し、所属機関の運営組織に報告する。
- 安全保障関連事項が所属機関の理事会の関心事となり、その進展が適切に伝えられるようにする。UUK のガイドラインでは、所属機関の理事会が、安全保障リスクに関する年次報告書を受け取ることを推奨している。
- 実務担当者、学術関係者及びより広範な学術サービススタッフが、ポリシーの更新とその理由を認識し、更新や変更の理由を納得できるようにするための計画を策定する。これらの計画は、セキュリティ上の優先事項や脅威の変化を反映するために定期的に見直す。

d. 大学全体で安全保障を重視する文化を根付かせる方法

- 早い段階から、学識経験者や幅広い専門スタッフと双方向の対話を行うようにする。安全保障に関する事項が大学全体で理解されること、また、安全保障が妨げになるのではなく、むしろ有効なものとみなされることが重要である。
- 多くの大学では、異なるチームや部門に国際化または安全保障のチャンピオンを任命することが効果的であることを理解している。それは、人々は同僚からの情報を信頼する傾向があるからである。
- ウェブページなどの組織内のリソースが明確で、最新でアクセスしやすく、質問がある場合の連絡先が明記されていることが望ましい。
- 組織内の議論を支援するために、安全保障問題に関する連絡窓口を開設し、明確に伝達する。
- すべてのチームや部門を横断して話し合う。安全保障に対する意識は、研究部門や提携部門に限ったことではなく、教育、学生サービス、学生自身及びその他安全保障問題が自分たちに関係するとは考えていなかった利害関係者グループにも関係する。
- 安全保障問題に関するメッセージを聴衆に合わせて調整し、それが、実用的で、補足資料による裏付けがあり、複雑さが適切であることを確認する。複雑すぎるメッセージも単純すぎるメッセージも、いずれも役に立たない。
- 上級幹部から、安全保障問題がいかに優先的な事項であるかについて明確なメッセージを発信する。
- 安全保障に関する懸念が正当なものであることを認める。懸念を脇に追いやるのは逆効果である。安全保障に配慮することがいかに優れた研究・教育を可能にすることにつながるのか、また、職員が安全保障に配慮できるようにするために安全保障対策が存在することに焦点を当てる方が、懸念を打ち消すよりも生産的である。
- 信頼できる情報や優れた事例を共有するために、安全保障問題をめぐる部門全体の話し

合いに参加する機会を求める。

・ どのような研修が役に立つかを検討する。

2.2.3 研究活動の国際化、オープン化に伴うリスクの管理のための主な取組

前述したように、英国においては、「Trusted Research」という統一的な枠組みを規定して、政府機関、大学協会及び R&D 資金配分機関が一体となって、大学向けに、研究活動の国際化、オープン化に伴うリスクの管理のための各種ガイドラインを策定・公開してきた。

その中で、研究インテグリティに関するリスクの識別・分類、リスクの判断基準、リスク判断のフロー等について詳細に説明された文書ではないが、一般の大学研究者が国際共同研究の提案を行う際に、研究インテグリティに関するリスク発生の予防の観点から、わかりやすく、確認すべき事項を示したチェックリストである「Trusted Research Checklist for Academia」[35]が、前述した「Trusted Research Guidance for Academics」に関連して NPSA から公開されている。

表 2-3 に、同チェックリストの構成と内容を示す。

表 2-3：NPSA から公開されている国際共同研究の提案の際のチェックリストの内容
（出典：Trusted Research Checklist for Academia[36]）

項目	確認事項
新規パートナーについて	・ パートナーは、なぜあなたと一緒に仕事をしたいと思うのか？ ・ パートナーは、資金援助や関与の見返りに何を期待しているのか？ ・ パートナーの組織は、英国に敵対的と見なされる可能性のある国、あるいは英国とは異なる民主主義や倫理的価値観を持つ国と関係があるのか？ ・ パートナーに対するデューディリジェンスにより、敵対的な国家とつながりのある軍や警察に代わって研究に関与していることが確認されたか？ ・ デューディリジェンスで得た情報の中で、あなたの研究が悪用されたり、意図しない応用でマイナスになる可能性はあるか？ ・ パートナーと研究を行うにあたり、法的、規制的、または大学の方針的な制約があるか？ ・ 上記の質問に対する回答を考慮した上で、あなたや大学にとって、潜在的な風評リスクや倫理的リスクはないか？ ・ パートナーとの共同研究についての決定を、あなたの部署の上位の管理者の判断事項とする必要性はないか？

[35] https://www.npsa.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academia.pdf
[36] Ibid.

項目	確認事項
研究の関係性について	・ 提案されている覚書（MoU）の条件は、あなたの学部や大学の期待に沿うものか？ ・ 既存の知的財産、研究データ、機密情報、個人を特定できるデータなどをプロジェクトに提供しているか？提供している場合、その保護はどのように行われているのか？ ・ 生成された知的財産は誰が所有するのか？ ・ 生み出された知的財産を保護するための計画はあるか？ ・ あなたの学術機関の利益を保護するために、どのような契約上の要件を設けることができるのか？ ・ 研究パートナーは、あなたの機関の IT ネットワークにどのようにアクセスできるのか？彼らがアクセス権を持つ場合、それによってどのような広範な可視性がもたらされるのか？ ・ 類似した分野の研究の間で、物理的な分離や保護が必要なことが見られることはないのか？
既存のパートナーについて	・ 研究を進めることで、既存の研究パートナーとの間に利益相反の可能性が生じるか？ ・ 利益相反の潜在的可能性について、既存のパートナーと話をしたか？ ・ 秘密保持契約の条件を検討したか？これには、あなたが既存のパートナーに可視性を提供する必要があるとの期待が含まれているか？ ・ ・ この研究は、あなたやあなたの学部、大学が既に結んでいる既存の契約上の合意に違反しないか？

その一方、英国では、2022 年から、英国内閣府（Cabinet Office）より、国家防護安全保障局（NPSA）の「Trusted Research」キャンペーンの一環として、国際的な共同研究に携わる研究者や同僚が直面する可能性のある具体的なリスクシナリオを提示したケーススタディを説明した 3 つのビデオが、YouTube で公開されている。これを、表 2-4 に示す。

表 2-4：国際的な共同研究に携わる研究者や同僚が直面する可能性のある具体的なリスクシナリオを提示したケーススタディを説明した 3 つのビデオ

（出典：YouTube: Cabinet Office (Trusted Research for Academia Guidance - Risk Case Studies)）[37]

ケーススタディ	ケーススタディの概要	URL
リピュテーショナルリスク	あなたはリスク管理者である。 2019 年、ある大学の研究者が大企業の英国子会社から相談を受けた。その企業の本社は、経済的及び軍事的な目的を織り交ぜた非民主的な国にある。その研究者は、プラズマを操作する 2 年間のプロジェクトに資金を提供する企業との契約に合意した。半年後、企業は研究の方向転換を望んだ。研究者はプロジェクト終了後、米国のメーカーから専門装置を購入するよう求められた。プロジェクト終了後、研究者はその装置を企業の本社に送るように依頼された。研究者はその依頼に同意し、プロジェクト完了後、その装置を搬送した。しかし、その企業が米国の輸出規制の対象であることが判明した。研究者が誤ってその規制に違反して機器を譲渡したため、自分自身と大学の評判の両方が危険にさらされた。 このビデオは、このような状況になる前に、リスク管理者のあなたが、いかに対応すれば良かったのかを問うもの。	https://www.youtube.com/watch?v=WBsJvc6M3QM&list=PLVnRbAyuOGuqkW4hE0nnhya-SOcmq7V8T&index=1
国家安全保障・投資法違反	あなたはリスク管理者である。 数年来、英国のある大学がフォトニクスの研究に携わってきた。その研究は高い技術準備レベルに達していたが、現在は資金援助が打ち切られている。しかし、海外の大学が研究を継続することに興味を示しており、その大学関係者は彼らと一緒に研究を続けることができると約束している。英国の研究者は、この重要な分野での研究を続けたいという熱意から、研究データと研究成果を海外の研究機関に移したが、海外の研究機関への情報移転は NSI 法（国家安全保障・投資法）に違反していた。 このビデオは、このような状況になる前に、リスク管理者のあなたが、いかに対応すればよかったのかを問うもの。	https://www.youtube.com/watch?v=PqZVt197qpw&list=PLVnRbAyuOGuqkW4hE0nnhya-SOcmq7V8T&index=2

[37] https://www.youtube.com/playlist?list=PLVnRbAyuOGuqkW4hE0nnhya-SOcmq7V8T

ケーススタディ	ケーススタディの概要	URL
知的所有権	あなたはリスク管理者である。 英国の大学が海外の大学と顔認識技術の共同研究契約を締結し、IP へのアクセス権を共有することになった。海外の大学は大規模な資金提供と 2 名の研究員のスポンサーになることに同意した。英国の大学が綿密な財務デューディリジェンスを実施したところ、すべて問題はなかった。しかし 1 年後、その海外の大学が、監視と弾圧を支援する軍や警察と協力していることが明らかになったというニュースが流れた。英国の大学は大変な状況にさらされている。 このビデオは、このような状況になる前に、リスク管理者のあなたが、いかに対応すれば良かったのかを問うもの。	https://www.youtube.com/watch?v=FBGD_i-pBkE&list=PLVnRbAyuOGuqkW4hE0nnhya-SOcmq7V8T&index=3

2.3 オーストラリア

2.3.1 2022 年度までの経緯

豪中関係の悪化を背景に、豪州では 2019 年 8 月に、政府と大学・研究機関が共同してタスクフォース（University Foreign Interference Taskforce: UFIT）を設置した。政府側は教育省だけでなく内務省や国防省などを含むのが特徴である。また、大学・研究機関側には、競争的資金を配分する機関である豪州研究評議会（Australian Research Council: ARC）と国立保健医療研究協議会（National Health and Medical Research Council: NHMRC）のほか国内 43 の大学で組織する豪州大学連合（Universities Australia: UA）、上位 8 つの大学で構成するグループオブ 8（Go8）といった組織も加わっている。

UFIT は 2019 年 11 月、外国干渉を排除するための通称 UFIT ガイドライン（Guidelines to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表した。2 年後の 2021 年 11 月に改定されている。豪州の大学・研究機関における外国干渉セキュリティの一連の審査は、同ガイドラインに基づいて行われている。

UFIT を構成するアクターの中では、とりわけ ARC の役割が大きいが、ARC では 2018 年 7 月以降、教育省の指示のもとで主要な国家安全保障機関と協力し合い、政府資金による研究の申請プロセスに対する監視を強化するようになった。また「利益相反・機密保持ポリシー（Conflict of Interest and Confidentiality Policy）」を公表して改定を重ねており、外国機関との関係性を示す情報をより幅広く開示するよう求めている。なお、協力する国家安全保障機関の中には、内務省直轄の豪州保安情報機構（Australian Security Intelligence Organisation: ASIO）のほか連邦警察や豪州取引報告分析センター、豪州通信総局、豪州地理空間情報機構、国家情報局などのメンバーが含まれている。

大学の動向としては、例えばグループ 8 を構成する大学は、リスクを検知するための複数のプログラムを実施しているほか、利益相反や不正防止にあたり明確なガイダンス（Measures taken by the Go8 to mitigate the threat of foreign interference in alignment with the UFIT Guidelines）を提示している。また豪州大学連合も、2 つの資金配分機関やグループ 8 とともに、外国干渉を排除したり緩和したりするための措置に加わっている。[38]

また、2022 年 3 月には、豪州連邦議会のインテリジェンスとセキュリティに関する議会合同委員会（PJCIS）が大学・研究機関の安全保障上のリスクに対し 27 の勧告をした。

2.3.2 最近の主な動き

2021年11月にUFITガイドラインの改訂版が公表されて以降、豪州の研究インテグリティ関連の施策に大きな動きは見られないが、これまでのガイドラインや政府の取組に関連

[38] 以上の説明については、「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）に基づく（pp.xix~xxii）。

していくつかの動きが見られた。

まず、2023年3月には上記の豪州連邦議会のインテリジェンスとセキュリティに関する議会合同委員会（PJCIS）の27の勧告のそれぞれについての連邦政府からの反応の文書が公表された[39]。「政府は提言の大部分（majority）を歓迎し、大筋で支持（broadly supports）する」[40]とし、議会報告書で「高等教育・研究機関および連邦政府機関が、UFITやその他の主要な取組を通じて、外国干渉に対する意識を高め、レジリエンスを高めるために、実質的な取組を行っていると認めていることを歓迎する」と評価している。

2023年6月には、UFITのトランスナショナル教育ワーキンググループ（Transnational Education Working Group）からトランスナショナル教育に関するデューディリジェンスについてのガイダンスノートが公表された[41]。トランスナショナル教育（Transnational education: TNE）とは、学習者の所在地が教育機関の所在地とは異なる国である高等教育プログラムのことである。

2023年8月には、UFITガイドラインの制定後の大学における外国干渉リスクへの対応の取組状況についての報告書が公表された[42]。

以下、TNEについてのデューディリジェンス文書と、UFITガイドラインの履行状況の報告書について、それぞれ概要を説明しよう。

表 2-5：近年の豪州における研究インテグリティ関連の主な動き

時期	内容
2019年8月	政府（教育省、内務省、国防省など）と大学・研究機関が共同してタスクフォース（University Foreign Interference Taskforce: UFIT）を設置
2019年11月	外国干渉を排除するための通称・UFITガイドライン（Guidelines to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表
2020年12月	外国関係法が成立
2021年11月	UFITガイドラインを改定
2021年11月	豪州研究評議会（ARC）は「重要技術のための青写真と行動計

[39] Australian Government. *Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report: National security risks affecting the Australian higher education and research sector*. February 2023.

[40] 27 の勧告のうち、唯一不支持（unsupported）の政府回答は、勧告 10「ASIO の議会に対する年次報告書に大学・研究機関に対する脅威についてのアセスメントの情報を含めること」に対してであった。年次報告書は 1 つの部門についてのみ焦点を当てるものではなく、また、敵に対して対抗可能な情報を与えることとなるとの理由である。

[41] University Foreign Interference Taskforce Transnational Education Working Group. *Guidance Note on Due Diligence*. June 2023.
<https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/transnational-education-guidance-note-due-diligence>

[42] Department of Education. *Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector*. August 2023.

時期	内容
	画」を発表
2022年3月	豪州連邦議会のインテリジェンスとセキュリティに関する議会合同委員会（PJCIS）は大学・研究機関の安全保障上のリスクに対し27の勧告。
2023年2月	政府が豪州連邦議会のPJCISの勧告に対する反応を公表。
2023年6月	UFITのトランスナショナル教育ワーキンググループが「デューディリジェンスに関するガイダンスノート」を公表。
2023年8月	教育省がUFITガイドラインの履行状況についての報告書を公表。

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、2023年3月）112～121頁などから作成。

(1) トランスナショナル教育に関するデューディリジェンスについて

このガイダンスノート（Guidance Note）は、大学外国干渉タスクフォース（UFIT）のトランスナショナル教育ワーキンググループ （Transnational Education Working Group: TNEWG）によって作成されたものである。UFITガイドラインを補足するとの位置づけであり、トランスナショナルな教育環境に特化したデューディリジェンスに関する追加的な助言を大学に提供することを目的として作成された。

オーストラリアにおけるトランスナショナル教育（TNE）の拡大は、ダイナミックに変化するリスク状況をもたらし、外国干渉のリスクから保護するために、大学セクターは様々なアプローチを必要とするとの状況認識が示され、TNEセクターが直面するリスクには、以下のようなものがあるとする。

- 海外でのデータ保有と相互作用の増大によるサイバーセキュリティの脆弱性の増大
- 海外で維持されるインフラから生じる保護セキュリティリスク
- パートナーの利益における透明性の欠如
- オーストラリアの個人情報保護法を遵守するための海外の学生データの管理
- 学生および職員の安全と福利厚生
- オーストラリアと海外の法律、保護、自由の交錯。

これらのリスクを含め、TNEのリスクマネジメントの考慮事項を、法的義務、パートナー機関の所在地と管轄、パートナー機関の経歴と評判、成果物、リスク管理とコンフリクト、契約と商業的取り決めの各分野について列挙している。

(2) UFIT ガイドラインの大学・研究機関における履行状況報告書について

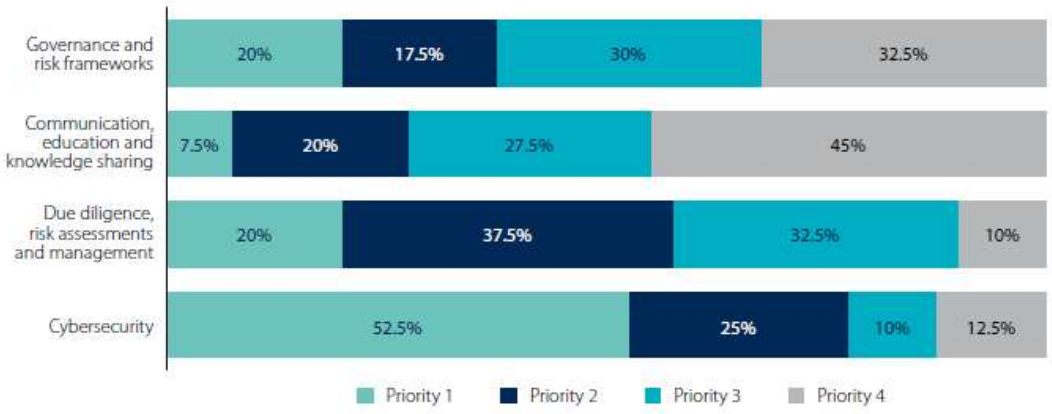
2022年9月に、Jason Clare教育大臣は、UFITガイドラインに大学がどのように対応しているかについて包括的なレビューをすることとした。2023年初めに、教育省は大学セク

ターとの協議のために2段階のアプローチを取ることとし、大学と対面およびヴァーチャルで協議を行うとともに、大学および関連団体を対象としてアンケート調査を実施した。このプロセスには、42のオーストラリアの大学、8つの関連団体、９政府機関が参加した。

その結果をまとめたものがこの報告書であるが、同書は「2021年にUFITガイドラインの改訂版が発表されて以来、豪州のすべての大学はガイドラインの実施に積極的に取り組んでいる」と総括している。

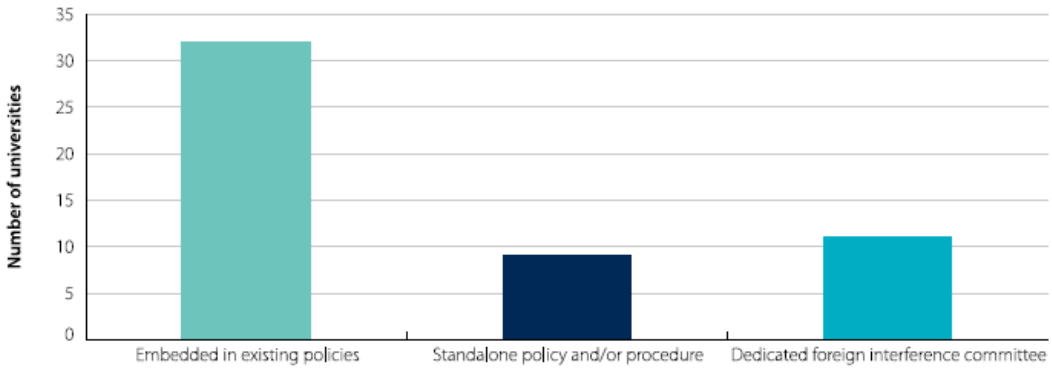
- 各大学のリスクレベルに比例して、実施の程度や成熟度は様々である。各大学には固有のリスクプロファイルがあり、外国干渉を管理するための万能の戦略は存在しない。UFITガイドラインが、各大学は自発的にリスクの大きさに比例して取り組むと規定している点について、大学セクターは支持をしている。
- ガイドラインの実施については、大学幹部レベルによる関与があり、このガイドラインを実務者レベル、研究ユニットや学生に定着させるための取組が進行中である。今後は、研修資料、ベストプラクティス事例、その他の事例などを共有し、特に学生へのリスク周知を強化することが有益である。
- 大学はサイバー攻撃のリスクを認識し、ガイドラインで言及されている以上のセーフガードを実施している。サイバー攻撃への脆弱性に対する大学の防御を向上させるための取組は、継続的に行われる必要がある。
- 大学はガイドラインの導入が一時的な取組ではないことを認識している。リスク環境は絶えず変化し続けており、外国の干渉への対抗は、適応性とアプローチの進化を必要とする継続的なプロセスである。政府からの頻繁で具体的な情報の共有が、ガイドラインの継続的な実施を支援することになる。
- 政府と大学セクターが協力する機会が引続き存在する。知識と情報共有の改善、より多くのトレーニング資源の提供、そして実施に関する大学セクターの進捗状況の年次報告は、すべて将来における協力の機会を提供するものである。

図 2-1は、UFITガイドラインにおける対策の4つの柱は、1. ガバナンスとリスクの枠組み（Governance and risk frameworks）、2. コミュニケーション、教育、知識の共有（Communication, education and knowledge sharing）、3. デューディリジェンス、リスク評価、管理（Due diligence, risk assessments and management）、そして4. サイバーセキュリティ（Cybersecurity）である。これら４つの優先順位は、「サイバーセキュリティ」が最も高く、次に「デューディリジェンス、リスク評価、管理」とする大学が多かった。また、図 2-2は、外国干渉リスクへの対応策に関して、既存の対策に内包して実施、単独・独立の取組を実施、単独・独立の委員会を設置のいずれであるのかを示している。図のように、既存の対策に内包して実施している大学が多いことが分かる。



出典：Department of Education. *Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector*. August 2023.

図 2-1：UFIT ガイドラインの実施状況調査の結果：４つの柱の優先順位



出典：Department of Education. *Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector*. August 2023.

図 2-2：UFIT ガイドラインの実施状況調査の結果：対応策の既存の施策との関係

最後に、報告書では、UFITをはじめとし、今後の大学セクターと政府の連携を通じ、外国干渉リスクに継続的に対応していくためには以下の取組が必要であるとしている。

○脅威の文脈

・ 政府と大学の間で具体的かつ頻繁に情報を共有し、大学が直面するリスクに関する最も適切な情報を確保する。

○サイバーセキュリティ

・ 脅威のモデル化技術、サイバーセキュリティへのアプローチ、得られた教訓を共有し、大学全体の能力構築の機会とするとともに、リスクの進展に応じた継続的な議論を行う。

○国家安全保障エコシステム

・ 大学への一貫した合理的な働きかけを確保するため、政府機関間で定期的な協力を行

う。

・　大学部門に適用されるすべての国家安全保障法制の概要をまとめたロードマップを作成し、大学に対する政府内の責任機関の連絡先を記載する。
・　大学によるガイドラインの継続的な実施に関する年次調査を完了し、政府によって提供される継続的な作業と支援が状況に適応していることを確認する。

〇ガバナンスとリスクの枠組み

・　学内での干渉が疑われる、または実際に発生した場合に大学が取るべき推奨される次のステップのフローチャートを作成する。職員と学生の双方に適用される内部報告および外部報告へのアプローチを示す。

〇コミュニケーション、教育、知識の共有

・　さまざまな層（例：学術・専門スタッフ、学部生・大学院生、HDR（Higher Degree Research）学生）に合わせた、さらなる研修資料とリスクコミュニケーション計画を開発する。
・　部門全体のリソースの共有を促進するため、実務家／役員レベルのメンバーで構成される、外国干渉に特化した部門全体の実践コミュニティを設立する。
・　小規模の地方大学向けにテーマを絞ったセッションを含む、定点ワークショップやセミナーを開催し、部門内の人材の継続的なスキルアップとトレーニングを確保する。
・　ベストプラクティス事例を含む追加的なケーススタディの開発・提供について、大学と政府が協力して、リスクとはどのようなものかをより効果的に大学に伝える。

〇デューディリジェンス、リスク評価および管理

・　大学間を移動する研究者の事務負担を軽減するため、研究者の利益申告の中央登録簿を作成する。
・　各大学で、基本的なデューディリジェンス・チェックを実施するためのツールの開発を行う。
・　大学間の透明性を高めるため、「利益相反」（conflict of interest）から「利益申告」（declaration of interest）に用語を変更するとともに、大学間の透明性を促進する。

2.3.3 研究活動の国際化、オープン化に伴うリスクの管理のための主な取組

オーストラリアにおける取組については、前述のように、国家安全保障機関の関与に特色がある。例えば、政府（教育省、内務省、国防省など）と大学・研究機関が共同して設置したタスクフォース（University Foreign Interference Taskforce: UFIT）では、豪州の防諜機関である内務省直轄の保安情報機構（ASIO）に主導されている。

(1) 「大学海外干渉タスクフォース」（UFIT）による取組

上記の豪州ではタスクフォースは 2019 年 8 月に設置された。同 11 月には、外国干渉を排除するための通称 UFIT ガイドライン（Guideline to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表した。

同ガイドラインは 2021 年 11 月に改定され、2019 年版と同じく大学当局が自主的に運用することが原則になっている。利益開示義務については、大学側が対象となる研究者などを選べるようになったほか、外国からの干渉のリスクが高いものについては、過去 5 年間の状況を報告しなければならないとするものもある。

UFIT は、外国からの干渉に対し大学への保護を強化するために設立された組織である。大学部門と政府機関を結集し、豪州の大学が世界レベルの研究を継続できるよう、信頼と回復力のある環境を支援・構築し、リスクに応じて大学が意思決定をできるように導く役割を担う。豪州の防諜機関である内務省直轄の保安情報機構（ASIO）が全体を主導していることが大きな特徴である。外国干渉については、この組織が中心になって調査や執行活動を行うとされる。

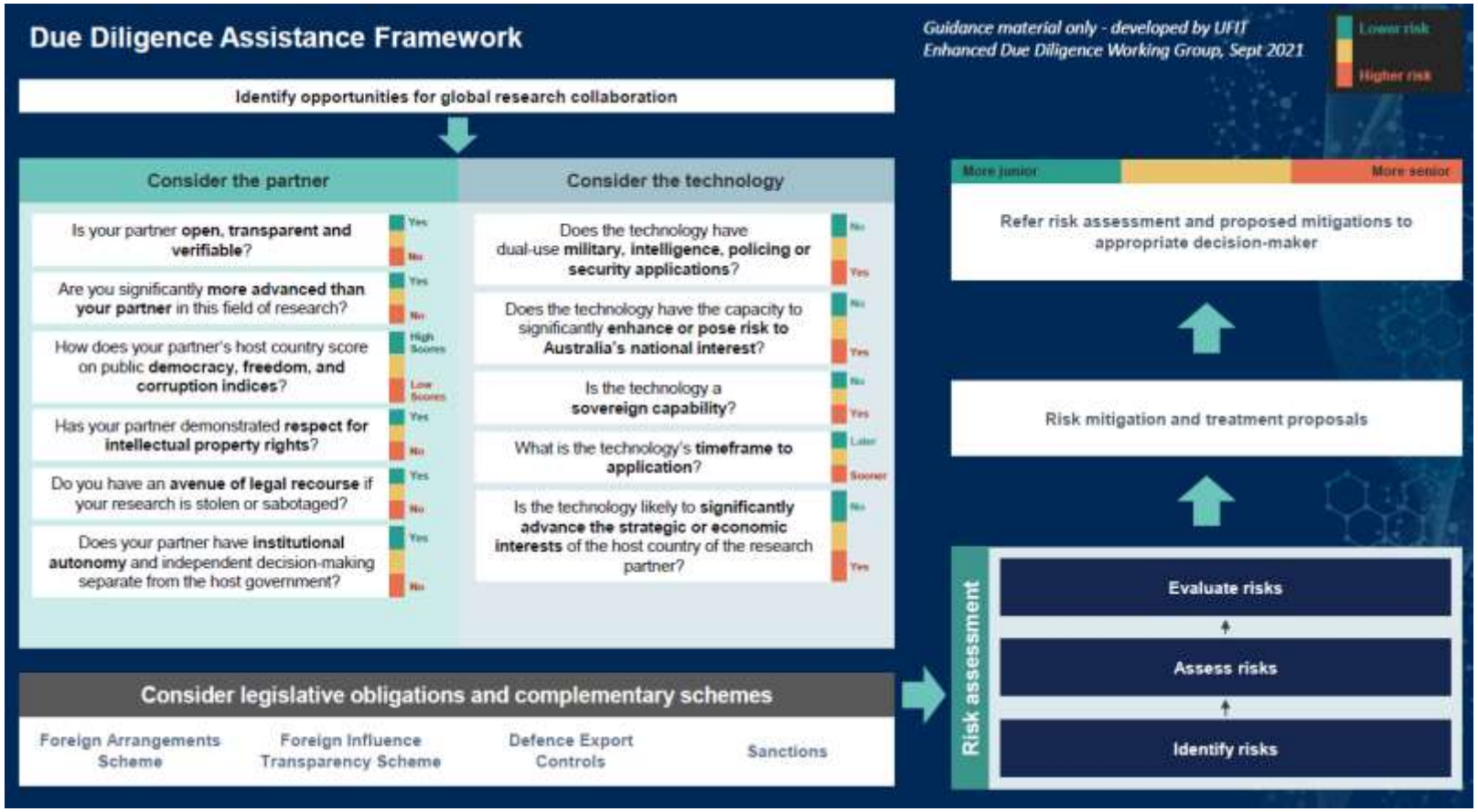
同ガイドラインの 3 章「Due Diligence, Risk Assessments and Management」では、デューディリジェンスの方法とリスクマネジメントについて説明がされている。また、以下のような関連文書が UFIT により作成され、教育省のウェブサイトで公表されている。

・Due Diligence Assistance Framework (2021 年 11 月公表)（図 2-3）
<https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/due-diligence-assistance-framework>

・Due diligence, risk assessments and management
<https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/due-diligence-risk-assessments-and-management>

・Using open source information for due diligence（2021 年 11 月公表）
<https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/factsheet-open-source-information>

・Case studies – Due diligence, risk assessments and management
<https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-due-diligence>



出典：Department of Education. *Due Diligence Assistance Framework.* 2021 <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/due-diligence-assistance-framework>

図 2-3：Due Diligence Assistance Framework

(2) 「重要技術のための青写真と行動計画」

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）が発表された。この計画によると、「重要技術」とは「国益を著しく向上させたり、リスクをもたらしたりする能力をもつ現在及び将来のテクノロジー」のことである。同文書には、国益のために重要技術を保護・促進するためのビジョンや戦略が規定されている。

豪州の資金配分機関である豪州研究評議会（ARC）は、競争的研究資金の申請にあたり、このリストに記載された技術が含まれている場合には、リスクがあるかどうかを検討することになっている。リスク要因には、次のような諸点が含まれるとしている。

・外国からの財政支援や教育又は研究関連活動
・外国の人材育成プログラムへの関与など
・外国の政府や軍隊、警察、諜報機関などへの直接の関与
・豪州が制裁措置をとっている体制、個人、組織への関与

こうしたリスクの存在が確認された場合、ARC は国家安全保障機関に報告し、懸念がある場合は助言するとされている。（2022 年版報告書（未来工学研究所）、2.3.3 節（p.115））[43]

[43] https://www.pmc.gov.au/news/launch-blueprint-and-action-plan-critical-technologies
https://www.industry.gov.au/publications/critical-technologies-statement"

2.4 カナダ

2.4.1 2022 年度までの経緯

2019年に公共安全省（Public Safety Canada）が「学術界における安全保障意識の醸成（Building Security Awareness in the Academic Community）」と命名された文書を発表した。[44] この文書は、外国の国家や集団を含む潜在的脅威からカナダの学術機関における機密研究を保護することの重要性及び国家安全保障や経済的利益に影響を与えかねない知的財産や研究成果の不正取得に関連するリスクを強調している。本文書では、学術機関がセキュリティ対策を強化し、脅威に対する脆弱性を軽減するための実践方法として、強力なサイバー衛生の実施、研究のデュアルユース用途の認識、法律や規制の下での責任の理解などを推奨している。また、潜在的なパートナーや共同研究者を評価し、機密データへのアクセスを管理し、研究の完全性と利益相反についてメンバーを教育するよう、教育機関に助言している。同時に、研究データや知的財産の悪用や窃盗から守りながら、オープンで協力的な研究環境を維持することの難しさを認めている。

2020年9月にカナダ政府は、カナダ政府・大学共同ワーキンググループ（Government of Canada-Universities Working Group）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）」[45]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。省庁と関係機関が参加するカナダ政府・大学ワーキンググループは、研究を保護し、カナダ国民に最大限の利益をもたらす方法であり、オープンな共同研究を推進するために設立された。グループは定期的に会合を開き、「ポータルサイト」はこのグループの研究セキュリティの強化に関する取組の成果を広めるための重要なチャネルとなっている。

2021年1月にカナダ政府は、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安相に義務づけた。外国の影響やスパイから研究コミュニティを保護することは、公共安全省の一義的な責務である。サイバーセキュリティ分野では、カナダ安全保障情報局（Canadian Security Intelligence Service（CSIS）：公共安全省傘下）及びカナダ・サイバー・セキュリティ・センター（Canadian Centre for Cyber Security (CCCS)：カナダ通信保安局傘下）が取締まりを所管する。連邦政府の3つの資金配分機関、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：NSERC）、社会・人文科学研究会議（Social Sciences and Humanities Research Council：SSHRC）に対しては、所

---

44 Public Safety Canada. “Building Security Awareness in the Academic Community” <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-prlfrtn/sfgrdng-scnc/sfgrdng-scnc-cdmc-cmmnty-en.aspx>

45 カナダ政府ウェブサイト” About the Government of Canada – Universities Working Group”<https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/about-government-canada-universities-working-group>

管のイノベーション・科学・経済開発省と保健省に加え公共安全省が研究セキュリティの取組を支援する。

2021年3月に、イノベーション・科学・経済開発相、公安相、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保護すると同時に、オープンで協力的な研究環境を支援する旨の声明を発表した。

2021年7月に、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、「国際研究協力に対する国家安全保障ガイドライン（National Security Guidelines for Research Partnerships）」を作成・公表した。同ガイドラインは、外国政府や関係者に関連する潜在的な国家安全保障上のリスクからカナダの研究エコシステムを守ることの重要性を強調している。研究パートナーシップの開発、評価、資金提供におけるデューディリジェンス、リスク評価、緩和に焦点を当て、研究パートナーシップにおける国家安全保障への配慮を統合するためのガイドラインを紹介している。これらのガイドラインは、カナダの安全保障を脅かしたり、経済や社会を混乱させたりする可能性のある、外国からの干渉、スパイ活動、望ましくない知識の移転からカナダの研究を護ることを目的としている。また、同ガイドラインでは、NSERCのような資金配分機関への助成金申請に際し、外国の影響についてのリスクアセスメントが要請されている。[46,47]

2023年2月14日の3大臣声明（イノベーション・科学・産業大臣、保健大臣、公安大臣）はガイドラインをさらに拡大し、「プロジェクトに携わる研究者の誰かが、（カナダの）国家安全保障に危険をもたらす外国の国家主体の軍事、国防、国家安全保障団体と関係のある大学、研究所、研究室に所属している」場合、機微な分野の研究に対する政府からの資金提供を禁止することを発表した。[48]

2.4.2 最近の主な動き

2024年1月16日の3大臣声明（イノベーション・科学・産業大臣、保健大臣、公安大臣）で、カナダの研究を外国の影響や国家安全保障上のリスクから守るための新たな措置を紹介している。これらの措置には、「機微技術研究と、懸念される提携に関する政策」（*Policy on Sensitive Technology Research and Affiliations of Concern*）、「研究セキュリティセンター」（Research Security Centre）の設立、「研究支援ファンド」（Research Support Fund）を通じた高等教育機関への5,000万ドルの投資が含まれてい

---

[46] カナダ政府ウェブサイト”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-partnership/national-security-guidelines-research-partnerships-risk-assessment-form>

[47] 以上の説明については、「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）に基づく（pp.xxii～xxiv）。

[48] Statement from Minister Champagne (Minister of Innovation, Science and Industry), Minister Duclos (Minister of Health) and Minister Mendicino (Minister of Public Safety) 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"

る。「機微技術研究と、懸念される提携に関する政策」は、研究助成金申請のガイドラインを定めるものであり、機微技術分野と、リスクをもたらす可能性のある軍事・国家安全保障に関係する組織との提携に重点を置いている。この方針は、カナダの研究を保護し、その協力的でオープンな性質を維持することを目的としている。[49]

このポリシーの策定は、関係省庁、連邦研究助成審議会（カナダ保健研究機構、カナダ自然科学・工学研究審議会、カナダ社会科学・人文科学研究審議会）、カナダ・イノベーション財団、カナダの安全保障・情報機関との緊密な協議のもとで行われた。研究コミュニティは「カナダ政府-大学ワーキンググループ」を通じて政策に意見を提供した。

表 2-6：近年のカナダにおける研究インテグリティ関連の主な動き

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安相に義務づけた。
2021年3月	・「研究安全保障政策声明（Research Security Policy Statement）」 イノベーション・科学・経済開発相、公安相、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。

[49] Statement from Minister Champagne, Minister Holland and Minister LeBlanc on new measures to protect Canadian research. From: Innovation, Science and Economic Development Canada. January 16, 2024 – Ottawa, Ontario.
<https://www.canada.ca/en/innovation-science-economic-development/news/2024/01/statement-from-minister-champagne-minister-holland-and-minister-leblanc-on-new-measures-to-protect-canadian-research.html>

時期	内容
2021年7月	・「国際研究協力に対する国家安全保障ガイドライン（National Security Guidelines for Research Partnerships）」 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・産業大臣、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・産業大臣、保健大臣、公安大臣） ・「機微技術研究と、懸念される提携に関する政策（Policy on Sensitive Technology Research and Affiliations of Concern）」の公表。

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、2023年3月）124～125頁などから作成。

(1) 「機微技術研究と、懸念される提携に関する政策（Policy on Sensitive Technology Research and Affiliations of Concern」）の概要

2024年初頭から、大学または関連研究機関が、連邦資金配分機関およびカナダ・イノベーション財団（Canada Foundation for Innovation）に提出した、機密技術研究分野を発展させる研究を含む研究助成金および資金提供の申請書は、その助成金で支援される活動に関与する研究者のいずれかが、カナダの国家安全保障に危険をもたらす可能性のある軍、国防、または国家安全保障機関と関係のある大学、研究機関、研究所に所属している場合、またはそこから資金や現物支援を受けている場合は、資金が提供されなくなる。

カナダ政府は、研究者がこれらの新しい要件が自分の研究に適用されるかどうかを迅速かつ効率的に判断できるよう、明確で定義された透明性の高いガイダンスを提供する２つのリストを公表して支援をする。

第一に、カナダ政府は、「機微技術研究分野（Sensitive Technology Research Areas）」のリストを公表する。これにより、研究者は自分の提案する研究がこの新しい要件の範囲内かどうかを自己評価できるようになる。既存の技術を利用するだけの研究は、このポリシーの対象外である。

第二に、カナダ政府は、カナダの国家安全保障に危険を及ぼす可能性のある、軍、国防、国家安全保障機関と関係のある指定研究機関のリストを公表する。このリストは、カナダ公共安全省と連邦政府全体の専門家がリスクベースのアプローチで作成したものである。

カナダの研究安全保障政策は、国を問わない（country-agnostic）。脅威は進化するものであり、世界のどこからでも起こりうることを認識し、研究の最新の進展に歩調を合わせ、複雑化する地政学的環境の中で進化するリスクに対処し続けることを確実にするため

に、両方のリストは定期的に見直される。連邦資金配分機関とカナダ・イノベーション財団は、この新方針を実施に移すための手続きとガイダンスを作成中である。書式や手続きなど、方針の実施に関するより詳細な情報は、方針の実施に先立ち、それぞれのウェブページで公表される予定である。

原則

この方針の策定および実施は、以下の原則に基づいて行われる。

- リスクを対象とする（risk-targeted）：この方針は、エビデンスに基づき、最も機微な技術研究分野と国家安全保障上の最も高い脅威に焦点を当てたものである。
- 科学的に適切であること（science appropriate）：可能な限りオープンかつ必要な限りの安全（as open as possible and as secure as necessary）を保証することにより、カナダの研究と研究資金のエコシステムへの影響を最小限に抑える。
- 透明性（transparent）：基準とガイダンスは明確であり、研究コミュニティがオープンにアクセスできる。
- 差別、ハラスメント、強制からの自由（free from discrimination, harassment and coercion）：この方針は、軍事、国防、国家安全保障に関わる特定の脅威に焦点を当てるものであり、いかなるグループや国を対象としたり、プロファイリングしたりするものではない。
- 研究コミュニティとの協力（collaboration with the research community）：継続的な対話と協議を通じて、研究セキュリティ対策を発展させる。

ステップ1：申請する助成金／資金が、機微技術研究分野の発展を目的としているかどうかを判断する。

NSERC、SSHRC、CIHRが提供する連邦研究助成金、またはカナダ・イノベーション財団が提供する研究助成金に応募する研究責任者（PI）は、機微研究分野のリストを確認し、提案する研究がリストに記載されている分野のいずれかの発展を目的としているかどうかを判断しなければならない。

ステップ2：研究者の所属の確認

機微技術の研究分野を推進する研究助成金による活動に関与するすべての研究者は、指定研究機関のリストを確認しなければならない。研究者が、指定研究機関のリストに掲載されている 1 つまたは複数の機関に所属している場合、またはそこから資金や現物支援を受けている場合、連邦補助金の申請プロセスを継続するためには、これらの関係を解消しなければならない。この方針で考慮されるのは、現在所属している機関のみであり、過去の所属は考慮されない。

研究助成金によって支援される活動に従事する、指名された役割を持つすべての研究者は、本方針を読み、理解し、同意し、遵守していることを証明する必要がある。研究者とその研究チームは、連邦助成金の支給期間中、本方針を遵守する必要がある。

機微技術研究分野について

機密技術研究分野（Sensitive Technology Research Areas）のリスト[50]は、カナダの研究開発にとって重要な先端技術や新興技術で構成されている。同時に、カナダの技術から不当に利益を得ようとする外国の国家、国家支援機関、非国家主体にとっても関心のある研究分野と考えられる。

リストは研究分野をカバーし、様々な開発段階にある技術を含む。特に懸念されるのは、研究段階の技術の進歩である。このリストは、すでにどこにでもあるような技術の使用をカバーすることを意図したものではない。

このリストは定期的に見直され、技術分野が発展・成熟し、カナダ政府、同盟諸国、学術研究界の科学技術専門家から新たな情報や見識が提供されるたびに更新される。

表 2-7：機微技術研究分野のリスト

1. 先進的デジタルインフラ技術（Advanced Digital Infrastructure Technology）
    - 先進的通信技術（Advanced communications technology）
    - 先進的コンピューティング技術（Advanced computing technology）
    - 暗号技術（Cryptography）
    - サイバーセキュリティ技術（Cyber security technology）
    - データストレージ技術（Data storage technology）
    - 分散型台帳技術（Distributed ledger technology）
    - マイクロエレクトロニクス（Microelectronics）
    - 次世代ネットワーク技術（Next-generation network technology）
2. 先進的エネルギー技術（Advanced Energy Technology）
    - 先進的エネルギー貯蔵技術（Advanced energy storage technology）
    - 先進的原子力発電技術（Advanced nuclear generation technology）
    - 無線電力伝送技術（Wireless power transfer technology）
3. 先進的素材と製造技術（Advanced Materials and Manufacturing）

○先進的素材（Advanced Materials）
- 強化された従来素材（Augmented conventional materials）
- オーキセティック素材（Auxetic materials）
- 高エントロピー素材（High-entropy materials）
- メタマテリアル（Metamaterials）
- 多機能・スマート素材（Multifunctional/smart materials）
- ナノ素材（Nanomaterials）
- 粉体素材（Powder materials for additive manufacturing）
- 超伝導素材（Superconducting materials）
- 二次元（2D）素材（Two-dimensional (2D) materials）

○先進的製造（Advanced Manufacturing）
- 付加製造（3Dプリンティング）（Additive manufacturing, 3D printing）
- 先進的半導体製造（Advanced semiconductor manufacturing）
- クリティカル素材製造（Critical materials manufacturing）
- 四次元（4D）印刷（Four-dimensional (4D) printing）
- ナノ製造（Nano-manufacturing）
- 二次元（2D）素材製造（Two-dimensional (2D) materials manufacturing）

[50] Innovation, Science and Economic Development Canada. *Sensitive Technology Research Areas*. January 2024. <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-areas>

4. 先進的センシングと監視（Advanced Sensing and Surveillance）
    - 先進的生体認証技術（Advanced biometric recognition technologies）
    - 先進的レーダー技術（Advanced radar technologies）
    - 原子干渉計センサー（Atomic interferometer sensors）
    - クロスキューイングセンサー（Cross-cueing sensors）
    - 電場センサー（Electric field sensors）
    - イメージングと光学デバイスとセンサー（Imaging and optical devices and sensors）
    - 磁場センサー（Magnetic field sensors, or magnetometers）
    - マイクロ（またはナノ）電気機械システム（Micro (or nano) electro-mechanical systems, M/NEMS）
    - 位置・航法・時間（PNT）技術（Position, navigation and timing technology）
    - サイドスキャンソナー（Side scan sonar）
    - 合成開口ソナー（Synthetic aperture sonar, SAS）
    - 水中（ワイヤレス）センサーネットワーク（Underwater (wireless) sensor network）
5. 先進的武器（Advanced Weapons）
6. 航空宇宙、宇宙および衛星技術（Aerospace, Space and Satellite Technology）
    - 先進的風洞（Advanced wind tunnels）
    - 軌道上サービス、組み立て、製造システム（On-orbit servicing, assembly and manufacturing systems）
    - ペイロード（Payloads）
    - 推進技術（Propulsion technologies）
    - 衛星（Satellites）
    - 宇宙ベースの位置・航法・時間技術（Space-based positioning, navigation and timing technology）
    - 宇宙ステーション（Space stations）
    - ゼロエミッション/燃料航空機（Zero-emission/fuel aircraft）
7. 人工知能とビッグデータ技術（Artificial Intelligence and Big Data Technology）
    - AIチップセット（AI chipsets）
    - コンピュータビジョン（Computer vision）
    - データサイエンスとビッグデータ技術（Data science and big data technology）
    - デジタルツイン技術（Digital twin technology）
    - 機械学習（Machine learning, ML）
    - 自然言語処理（Natural language processing）
8. 人間-機械統合（Human-Machine Integration）
    - ブレイン-コンピュータインターフェース（Brain-computer interfaces）
    - エクソスケルトン（Exoskeletons）
    - ニューロプロステティック/サイバネティックデバイス（Neuroprosthetic/cybernetic devices）
    - 仮想/拡張/混合現実（Virtual/augmented/mixed reality）
    - ウェアラブルニューロテクノロジー（Wearable neurotechnology）
9. 生命科学技術（Life Science Technology）

    ○バイオテクノロジー（Biotechnology）
    - バイオ製造（Biomanufacturing）
    - ゲノムシーケンシングと遺伝子工学（Genomic sequencing and genetic engineering）
    - プロテオミクス（Proteomics）
    - 合成生物学（Synthetic biology）

    ○医療・ヘルスケア技術（Medical and Healthcare Technology）
    - 化学、生物、放射線、核（CBRN）医療対策（Chemical, Biological, Radiological and Nuclear medical countermeasures）

- 遺伝子治療（Gene therapy）
- ナノ医療（Nanomedicine）
- 組織工学および再生医療（Tissue engineering and regenerative medicine）

10. 量子科学と技術（Quantum Science and Technology）
    - 量子通信（Quantum communications）
    - 量子コンピューティング（Quantum computing）
    - 量子素材（Quantum materials）
    - 量子センシング（Quantum sensing）
    - 量子ソフトウェア（Quantum software）
11. ロボット工学と自律システム（Robotics and Autonomous Systems）
    - 分子（またはナノ）ロボティクス（Molecular (or nano) robotics）
    - (半)自律/無人航空機/地上車両/海洋車両（(Semi-)autonomous/uncrewed aerial/ground/marine vehicles）

出典：Government of Canada. Innovation, Science and Economic Development Canada. *Sensitive Technology Research Areas*. January 2024.

懸念のある研究機関について

懸念のある研究機関のリスト[51]は、軍事・国防・国家安全保障機関と直接的または間接的に関係しているために、カナダの国家安全保障に最も高いリスクをもたらす研究組織・機関で構成されている。指定研究機関のリストは、世界のどの場所においも発生する可能性のある、カナダの国家安全保障に対する進化する脅威に対処するため、定期的に更新される。

現時点のリストには合計104機関が掲載されており、国別の内訳は中国85機関、ロシア7機関、イラン12機関である。

また、機関種別では、大学（university）が38機関、単科大学（college）が9機関、軍学校・アカデミー（academy）が25機関であり、それ以外は研究機関などである。

大学の例：「ハルビン工業大学（Harbin Engineering University、中国）」や「国立国防技術大学（National University of Defense Technology、中国）」など。

カレッジ：「空軍指揮大学（Airforce Command College、中国）」や「海軍指揮学校（Naval Command College、中国）」など。

研究機関：航空宇宙研究所（Aerospace Research Institute、イラン）」や「中国航空力学研究開発センター（China Aerodynamics Research and Development Center、中国）」など。

アカデミー：軍事科学アカデミー（Academy of Military Science、中国）」や「中国沿岸警備隊アカデミー（China Coast Guard Academy、中国）」など。

研究・技術分野では以下のものがみられる。

- 軍事科学と防衛：軍事的な分野に重点を置いているすべてのアカデミー、研究機関、大学が含まれる。リストにある組織のほとんどがこのカテゴリーに属し、特に中国の

[51] Innovation, Science and Economic Development Canada. *Named Research Organizations*. January 2024.

ものが多い。

- 航空宇宙および航空： 航空宇宙研究機関や各種飛行アカデミーのような機関。
- 情報通信技術： 情報伝達、コンピューティング技術、電子科学に重点を置く組織。
- 工学および技術研究： 一般的な工学系大学や技術研究所が含まれる。
- 生物・化学・医学研究： このカテゴリーには、医学系大学や生物・化学研究機関が含まれる。

これらの組織の大半は、軍事・防衛研究を志向しており、次いで航空宇宙・航空関連である。機関の多くは、航空宇宙、軍事科学、工学、情報技術などの分野を専門としている。これらの分野は防衛や技術の進歩に不可欠であり、軍事目的に利用される可能性がある。これらの組織のかなりの数は、それぞれの国の軍や政府と直接提携している。このことは、情報収集、サイバー戦争能力、高度な軍事技術の開発など、国家の優先事項に重点が置かれていることを意味する。

(2) 研究セキュリティセンター（Research Security Centre）の設置

研究セキュリティセンターは、政府の研究セキュリティ能力を強化する一環として、2022-23年度から5年間で3,460万ドル、継続的に840万ドルの投資を、2022年度予算において発表した。[52]

2022年度予算で、カナダ政府は研究を保護する能力を強化するための資源を発表した。この発表の一環として、カナダ公安庁（Public Safety Canada）は、研究コミュニティと学術機関に指導と助言を提供する研究セキュリティセンターを設立するために、5年間で1,260万ドル、継続的に290万ドルを割り当てた。[53]

研究セキュリティセンターは、全国の地域アドバイザーと、オタワにある中央ハブで構成されている。

現在、以下の地域に6人のアドバイザーがいる：

ビクトリア（ブリティッシュ・コロンビア、ユーコン、ノースウェスト準州をカバー）

エドモントン（アルバータ州、サスカチュワン州、マニトバ州をカバー）

グレーター・トロント・エリア（オンタリオ州とヌナブトをカバー）

ケベック・シティ（ケベック州をカバー）

ハリファックス（ニューブランズウィック、ノバスコシア、プリンス・エドワード島、ニューファンドランド・ラブラドールをカバー）

研究セキュリティセンターは、3つの分野を通じてカナダの研究事業の保護を支援する：

---

[52] 2024年1月16日 ・Statement from Minister Champagne, Minister Holland and Minister Leblanc on new measures to protect Canadian research

[53] “About the Research Security Centre”
https://www.canada.ca/en/services/defence/researchsecurity/about.html

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」の実施と、「機密技術研究および懸念される提携に関する方針（STRAC）」に関する助言の提供：同センターは、国家安全保障の審査プロセスを主導し、国家安全保障と技術的専門知識を結集して、助成金授与審議会の助成金決定に提供される助言が包括的で、脅威の進展に対応したものであることを保証する。

2. 地域アドバイザーのネットワーク

研究安全保障センターは、セーフガード・サイエンス・ワークショップ、関与、情報ツールの提供を通じて、学術機関や研究者に助言とガイダンスを提供する。

3. カナダ政府のサービスへのアクセス：

研究コミュニティがカナダ政府のサービスを利用する際の入り口となる。」

(3) 研究セキュリティの確保のための取組への助成金支給

2022年予算で発表された、研究支援基金（Research Support Fund）による研究セキュリティのための資金援助では、2022-23年から5年間で1億2500万ドル、継続的に2500万ドルが提供される。これは、「増加プロジェクト助成金」（Incremental Project Grants）を通じて利用可能であり、200万ドル以上の研究資金を受けている研究機関に拡大されている。[54]

2.4.3 研究活動の国際化、オープン化に伴うリスクの管理のための主な取組

NSERC におけるリスクアセスメントでは、研究者が提出したリスク質問票を検討し、国家安全保障を考慮した評価が必要な場合には、カナダ公共安全省に照会され、カナダ公共安全省、カナダ安全保障情報局、又はカナダ通信保安局が主導して評価を実施することが特色である。

(1) NSERC におけるリスクアセスメントプロセス

研究パートナーシップがカナダの国家安全保障にもたらす可能性のあるリスクを評価するために、連邦研究補助金申請に際しリスクアセスメント調査票を使用する義務がある。研究者は、リスク質問票を記入し、特定されたリスクの根拠を説明する。研究者は、機関とともにリスク軽減計画の作成に貢献する。

NSERC は、助成金申請書に添付されたリスク質問表とリスク軽減計画（該当する場合）を検討し、国家安全保障を考慮した評価が必要な申請については、関連する申請書類はカナダ公共安全省に照会される。この照会は、通常、科学的メリット評価が成功したと判断された後、助成機関によって資金調達の決定が下される前に行われる。

助成機関から照会された申請書を受け取ると、カナダ公共安全省は最初の審査を行い、結

[54] 2024 年 1 月 16 日　Statement from Minister Champagne, Minister Holland and Minister Leblanc on new measures to protect Canadian research

果を知らせる。カナダ公共安全省は、評価結果及びアドバイスを助成機関に返却する。

国家安全保障上のリスクが高いと評価されたプロポーザルには、資金が提供されない。[55]

(2) 「Policy on Sensitive Technology Research and Affiliations of Concern」によるリスクアセスメントプロセス

既に述べたように、2024 年初頭から、大学または関連研究機関が、連邦資金配分機関およびカナダ・イノベーション財団（Canada Foundation for Innovation）に提出した、研究助成金および資金提供の申請書は、1）機密技術研究分野を発展させる研究を含む、さらに、2）その助成金で支援される活動に関与する研究者のいずれかが、カナダの国家安全保障に危険をもたらす可能性のある軍、国防、または国家安全保障機関と関係のある大学、研究機関、研究所に所属している場合、またはそこから資金や現物支援を受けている場合には、資金が提供されなくなる。これを支援するため、「機微技術研究分野（Sensitive Technology Research Areas）」のリスト、カナダの国家安全保障に危険を及ぼす可能性のある、軍、国防、国家安全保障機関と関係のある指定研究機関のリストが公表された。

[55] NSERC におけるリスクアセスメントプロセス（2022 年版報告書（未来工学研究所）、2.4.5 節参照）

2.5 欧州連合（EU）

2.5.1 2022 年度までの経緯

2021年5月、欧州委員会は、国際的な研究・イノベーション政策のための新たな欧州戦略の概要を示した「研究・イノベーションへのグローバルなアプローチに関するコミュニケーション」を発表した[56]。これを受けて、欧州理事会は2021年9月、研究セキュリティに共同で取り組むことを政治的使命とする理事会結論を採択した。

続いて、2022年1月に欧州委員会は、「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」（Tackling R&I foreign interference staff working document）を発表した[57]。この文書は「スタッフ作業文書」というタイトルが示すように、欧州連合加盟国や大学・研究機関に対して法的拘束力を持つものではないが、外国からの干渉を防止し、対処するために大学・研究機関がどのような行動を取ることができるかを具体的に記述しており、チェックリストとして利用することが可能である。また、「海外からの干渉」（foreign interference）への対応策については、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つの類型に分けてリストアップし、それぞれ詳しく説明している。

例えば、当該作業文書では、学問の自由が脅かされている国の機関や個人との学術協力には、常にリスク分析と緩和策の策定が必要であり、第一段階として、懸念すべき国を特定することが重要であるとしている。その際、「学問の自由度指数」（Academic Freedom Index (AFi)）が最初の方向性を示していると説明している。さらに、教育機関における学問の自由とインテグリティに対する外的圧力を理解するために、脆弱性評価を実施することについても述べている。

欧州連合の研究資金プログラムであるHorizon Europe（2021～2027年）のプログラムガイドは2021年6月17日に初版（Version 1.0）が公表されたが、2022年4月11日に公表された第２版（Version 2）では、「研究・イノベーションにおける海外からの干渉（R&I Foreign Interference）」に関する段落が文書の第8章「8. International cooperation and association」に追加される等の修正がなされ[58]、上記の「スタッフ作業文書」への理解と検討を申請者等に求めている。[59]

---

[56] Commission communication on the Global approach to research and innovation: Europe's strategy for international cooperation in a changing world, COM(2021) 252 of 18.05.2021

[57] European Commission. Directorate-General for Research and Innovation. *Tackling R&I Foreign Interference. Staff Working Document* (2022/1)

[58] European Commission. *Horizon Europe Program Guide*. Version 2. 11 April 2022. <https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/programme-guide_horizon_en.pdf> 現在は Version 4（2023 年 10 月 15 日）まで更新されている。

[59] 以上の説明については、「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）に基づく（p.xxiv）。

2.5.2 最近の主な動き

欧州委員会は2023年6月に「欧州経済安全保障戦略」（European Economic Security Strategy）を公表した[60]。この戦略では、優先的に取り組むべき４つのリスクカテゴリを特定している。それらは、1）サプライチェーンの回復力に対するリスク、2）重要インフラの物理的およびサイバーセキュリティに対するリスク、2）技術セキュリティおよび技術流出のリスク、4）経済的依存関係の武器化または経済的強制のリスクである。同戦略はこれらのリスクに対処するための３つの柱（促進、保護、提携）で構成されている。すなわち、1）EUの競争力と成長を促進し、単一市場を強化し、強く弾力的な経済を支援して、EUの研究・技術・産業基盤を育成すること、2）必要な場合には的を絞った新たな手段を含め、さまざまな政策や手段を通じて経済安全保障を保護すること、3）世界各国との協力提携関係を構築し、さらに強化することである。同戦略では、研究セキュリティについては、２番目の柱の関連で触れており、先述の「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」はより広範に研究セキュリティを強化するために役立つものであることを述べ、また、既存のツールを体系的かつ厳格に実施し、残存するギャップを特定することにより、研究セキュリティを向上させる方策を今後提案すると述べている。

2023年6月29日には、「研究イノベーションのグローバルアプローチの実践についての第１回報告書」が公表された。その第３節「研究開発に対するEUのグローバルアプローチのバランス調整：公平な競争条件と相互主義に向けて」において「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」について言及している。欧州委員会はG7 SIGRE Working Groupにおいて各国で共有できる研究セキュリティの原則を開発していくとしている。[61]

そして2024年1月には、欧州委員会は「研究セキュリティ向上に関する理事会勧告の提案」（Proposal for a COUNCIL RECOMMENDATION on enhancing research security）を発表した[62]。文書の位置づけとしては、欧州理事会は「理事会勧告」を決定することができるが、欧州委員会はその理事会勧告についての提案を作成する権限を持つ。2024年の第１四半期中には欧州理事会において勧告を採択することを目指すとしている。

本文書は研究活動を安全保障上の脅威から守るための指針を示しており、「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」の内容に基づいて作成されている。リスクの特定と評価、セキュリティ方針と手順の策定、研究者やスタッフの意識改革の重要性を強調している。さらに、安全保障上の課題に対処するための国際協力と情報共有の必要性も強調されている。

---

[60] European Commission. “Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy.” Brussels, 20.6.2023. JOIN(2023) 20 final.
[61] European Commission. First biennial report on the implementation of the Global Approach to research and innovation. Brussels, 29.6.2023. COM(2023) 356 final. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52023DC0356"
[62] European Commission. “Proposal for a COUNCIL RECOMMENDATION on enhancing research security.” Brussels, 24.1.2024. COM(2024) 26 final.2024/0012 (NLE)

また、同じく 2024 年 1 月に公表された、経済安全保障強化に向けた政策パッケージ「経済安全保障の推進：５つの新たなイニシアティブの導入」では、5 つのイニシアティブの１つとして研究セキュリティ強化が位置付けられている[63]。

表 2-8：最近の EU における研究インテグリティ関連の主な動き

時期	内容
2021年5月	欧州委員会は、「研究・イノベーションへのグローバルなアプローチに関するコミュニケーション」を公表。
2021年9月	欧州理事会は、研究セキュリティに共同で取り組むことを政治的使命とする理事会結論を採択。
2021年11月	欧州理事会は、「欧州研究地域政策アジェンダ2022-2024」を採択。海外からの干渉への対処が優先分野の一つと位置付けられた。
2022年1月	欧州委員会は「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」を公表。
2022年4月	欧州議会は、2022年1月公表の「スタッフ作業文書」について歓迎する旨を決議（4月6日のグローバルアプローチについての決議）。
2023年5月	欧州理事会の競争理事会（Competitiveness Council）において、「知識セキュリティと責任ある国際化」について政策討議を実施（2024年1月公表の理事会勧告提案へのインプットとなる）。
2023年6月	欧州委員会は「欧州経済安全保障戦略」を公表。
2023年10月	欧州委員会は重要技術リストを公表[64]。
2024年1月24日	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」を公表。同日に、「経済安全保障の推進：５つの新たなイニシアティブの導入」を公表。

出典：European Commission. *Proposal for a COUNCIL RECOMMENDATION on enhancing research security*. Brussels, 24.1.2024. COM(2024) 26 final.2024/0012 (NLE)などから作成。

以下で、2024年1月に公表された「研究セキュリティ向上に関する理事会提言の提案」の内容について詳しく見ていこう。

(1) 「研究セキュリティに関する理事会勧告の提案」の内容

「研究セキュリティに関する理事会勧告の提案」は以下の内容で構成されている。

・はじめに

[63] European Commission. *Communication from the Commission to the European Parliament and the Council Advancing European Economic Security: An Introduction to Five New Initiatives*. Brussels, 24.1.2024. Com(2024) 22 Final.

[64] Commission recommendation on critical technology areas for the EU's economic security for further risk assessment with Member States, C(2023) 6689 of 03.10.2023

・範囲（スコープ）
・責任ある国際化のための原則
・提言
-資金配分機関の役割について
-高等教育機関とその他の研究実施機関への支援について
-国レベルでの行動支援について
・報告

まず、理事会勧告の問題意識とその策定の政治的背景を紹介した後、勧告が対象とする範囲について説明される。「研究セキュリティ」の定義が提案され、どのような組織や利害関係者が主な対象であるかが示される。

次に、責任ある国際化（responsible internationalisation）のための原則が提案される。この原則は、EU、加盟国、個々の研究実施機関といった様々なレベルにおいて、研究セキュリティに対する政策的対応を考える際に留意すべきと考えられている。

- 学問の自由と機関の自治を十分に尊重し、この分野による自治を重視する；
- 特にR&Iと安全保障の専門知識を結びつけることによって、このセクターを支援し、力を与えるための政府全体の枠組み（all-of-government framework）をとること
- 基礎研究、応用研究、高等教育を含むセクター全体へのアプローチ（all of sector approach）を支援すること
- リスクベースのアプローチに基づく保護措置の比例性
- 国家安全保障上のリスクだけでなく、倫理やインテグリティへの配慮にも焦点を当てる。
- 国を問わないアプローチ（country-agnostic approach）をとり、あらゆる形態の差別やスティグマ化を避ける

次のセクションは、加盟国に対する具体的な提言である。４つの小項目に分かれており、最初の小項目は、支援体制の構築とガイダンスの提供という観点から、公的機関が研究・イノベーション部門に対して行うべきことを提言している。第2の小項目は、研究セキュリティを強化する上で、国の資金配分機関が果たす重要な役割を取り上げている。第３の小項目は、加盟国が高等教育機関や研究実施機関を支援するために推奨されるべき点を詳述している。第４の小項目では、欧州委員会の支援行動やイニシアティブの概要を示す。

最後のセクションでは、勧告に対するフォローアップをどのように促進し、モニタリングするのかが明記される。

表 2-9：「研究セキュリティに関する理事会勧告の提案」の概要

○イントロダクション

1. 理事会は、質の高い研究とイノベーションに不可欠な要素として、開放性、国際協力、学問の自由の重要性を強調している。しかし、これらの価値は、国際的緊張の高まりや地政学的利益によって脅かされつつあり、悪意のある影響や悪用によって欧州の研究とイノベーションが損なわれる危険性がある。
2. オープンサイエンスと国際協力がグローバルな課題に取り組む上で極めて重要である。
3. その一方、欧州の研究・イノベーション部門を「ハイブリッドな脅威」（hybrid threats）にさらすことにもなる。
4. ハイブリッドな脅威は、秘密裏の方法から完全な窃盗に至るまで、安全保障のみならず欧州における学問の自由をも危うくするものである。
5. 高等教育機関や研究機関は、ますます複雑化する国際情勢に直面している。重要な知識や技術が軍事目的や基本的価値観に反して使用される可能性のある国への移転にはリスクを伴う。このような共同研究は、必ずしも違法ではないものの、安全保障上および倫理上重大な懸念をもたらす。
6. 国際協力の管理責任は、機関自治と学問の自由の原則の下、主として高等教育機関と研究機関にある。公的政府機関（public authorities）は、国際協力がオープンで安全な状態を維持できるよう、これらの機関が十分な情報を得た上で意思決定を行い、関連するリスクを管理できるよう支援すべきである。
7. 研究セキュリティを強化するために、EUレベルで議論や様々なイニシアティブが実施されてきた。
8. 欧州議会は、文化・学術・宗教分野における外国からの干渉に対抗するため、学問の自由と外国からの資金提供の透明性を強化する必要性を強調している。
9. EUの安全保障同盟戦略と安全保障と防衛に関する戦略的羅針盤は、ハイブリッド脅威を含む、より広範な安全保障と防衛に関する懸念に取り組んでいる。EUの輸出管理規則は、特にデュアルユース商品や技術に関する研究セキュリティにおいて重要な役割を果たしている。
10. 欧州委員会と上級代表は、経済安全保障に対するリスクを軽減するための促進、保護、パートナーシップに焦点を当てた欧州経済安全保障戦略を提案している。これには、先端半導体、人工知能、量子、バイオテクノロジーなどの重要技術分野への重点的な取組が含まれる。
11. この戦略を受けて、欧州委員会はリスク評価の対象となる重要技術分野を特定した。これらの評価は、研究とイノベーションのエコシステムの開放性を維持しつつ、研究セキュリティを強化するための方策に反映される。
12. 加盟国や利害関係者との議論では、研究セキュリティに関する問題や、それに見合った政策対応について、より明確にし、理解を共有する必要性が強調されている。
13. 研究セキュリティを強化するための加盟国による努力の進捗は、有益ではあるが、欧州研究領域を分断しかねない各国政策のパッチワークを生み出す危険性がある。公平な競争の場を確保し、欧州研究領域の完全性を維持するためには、EUレベルでの調整が必要である。

14. 効果的な研究安全保障措置には、EU、国、地域、個々の研究機関を含むすべてのレベルで一貫した適用が必要である。
15. 輸出管理規則や外国人研究者に対するビザ要件など、EUの法律や規則を遵守するための具体的なケースは、解釈上のガイダンスから利益を得ることができる。
16. 研究とイノベーションのエコシステムに影響を及ぼすハイブリッド脅威の構造的評価が不可欠である。これには、政策立案者間の状況認識の強化や、情報分析能力への依存が含まれる。
17. 民間部門、特に研究集約型の新興企業や中小企業における研究とイノベーションのリスクへの対応は極めて重要である。デュアルユース品目の輸出規制と外国投資の審査に関する既存の規則に注意を払うべきである。
18. 本勧告の作成にあたっては、加盟国およびEUのパートナーから得た二国間および多国間の経験を考慮した。策定されたアプローチは、様々な国際的な場におけるパートナーとのセーフガード措置の整合性を図る継続的な努力とともに、欧州独自の状況に適したものであるべきである。
19. 研究セキュリティは、ますます顕著な関心事となっており、さらなる啓発、相互学習、柔軟で機敏な学習アプローチが必要である。

まとめると、欧州連合理事会は、国際的な協力と競争の中で、研究とイノベーションの安全保障を守るための複雑で発展的な課題を認識している。EU理事会は、開放性と学問の自由という基本的価値を守りつつ、リスクから保護するバランスの取れた措置の必要性を強調している。安全で統合された欧州研究領域を維持するためには、機関や組織に対する支援とともに、EUレベルでの調整が不可欠である。

○範囲

1. 本勧告の目的上、「研究セキュリティ」とは、以下に関連するリスクを管理することを指す：

   (a) 重要な知識、ノウハウ、技術が、例えば第三国の軍事目的に転用された場合、EUとその加盟国の安全保障に影響を及ぼす可能性のある、望ましくない移転。

   (b) 研究への悪意ある影響。EUにおける学問の自由と研究の完全性を侵害するような、特定の物語を拡散させたり、学生や研究者の自己検閲を煽ったりしたために、第三国によって研究が利用される可能性がある；

   (c) EU内外を問わず、知識や技術が基本的価値を抑圧したり損なったりするために利用されるという倫理や誠実さの侵害。
2. 本勧告の目的上、「国際協力」とは、公的・私的な研究実施機関や高等教育機関が、EU域外に拠点を置く研究・イノベーション組織や企業と協力することと理解すべきである。EU域内に本拠を置き、EU域外から所有または管理されている研究・イノベーション組織や企業は、リスク評価に基づいて検討されるべきである。
3. 本勧告において、「リスク評価」とは、国際的な研究・イノベーション協力に関連して、主要なリスク要因の組み合わせを考慮するプロセスを指す。これらの要因の組み合わせがリスクレベルを決定する。評価すべき主要な要素は、以下の４つのカテゴリーに分類することができる：
   - 国際協力に参加するEUを拠点とする組織のリスクプロファイル：研究プロジェクトに関連

する、財政的依存を含む組織の強みと脆弱性を考慮する；

- 国際協力が実施される研究・イノベーション領域：プロジェクトが研究領域、例えば重要技術分野に焦点を当てているか、安全保障や倫理・人権の観点から特にセンシティブと考えられる方法論や研究インフラに関与しているかを検討する；
- 国際的パートナーが拠点を置く、あるいは所有・管理する第三国のリスクプロファイル（例：制裁対象国であるか、法治や人権保護の実績に欠陥があるか、積極的な民軍融合戦略をとっているか、学問の自由が制限されているか）
- 国際的なパートナー組織のリスクプロファイル：協力を想定している組織についてデューディリジェンスを実施し、政府や軍とのつながりがあるかどうかなど、関与している研究者やスタッフの所属、研究結果の最終的な使用や応用に関するパートナーの意図を調べる。

4. 本勧告の目的上、「研究・イノベーション部門」とは、公的・私的を問わず、EU全域のすべての研究実施機関および高等教育機関を対象とする。技術移転機関、国際化機関、商工会議所、研究集約型企業など、他の利害関係者の重要性に鑑みれば、本勧告は、EUの研究・イノベーション・エコシステムにおける他のすべての関係者にも同様に関連しうる。関連する場合には、教育関連の国際協力活動も考慮されうる。

○責任ある国際化のための原則

1. 国際的な研究・イノベーション協力の責任は、主として高等教育機関やその他の研究実施機関にあることを考慮し、学問の自由と機関の自治を推進し、擁護し続けることが必要である。
2. 「可能な限りオープンに、必要な限りクローズドに」という原則に則り、研究成果が検索可能、アクセス可能、相互運用可能、再利用可能（FAIR）であることを確保しつつ、セキュリティ上の懸念など適用される制約を十分に考慮した上で、オープンで安全な第三国のパートナーとの研究・イノベーションにおける国際協力を引き続き推進・奨励する必要がある。
3. 措置の比例性を確保することが求められる：セーフガードを導入する場合、問題となっているリスクを軽減し、不必要な管理負担を避けるために厳密に必要な範囲を超えないようにすることが重要である。目的はリスクを軽減することであり、連結を解除することではない。
4. 保護主義や研究・イノベーションの不当な政治的道具化を避けつつ、研究安全保障措置を、連邦や国家の安全保障を含む経済的安全保障の保護、学問の自由を含む共有価値の擁護に向けることが求められる。
5. 「学問の自由には学問的責任が伴う」という原則に基づき、高等教育機関やその他の研究実施機関の社会的責任を強調しつつ、研究者・革新者が十分な情報に基づいた意思決定を行えるよう、研究分野内の自治を促進することが重要である。
6. 政府全体のアプローチを採用し、関連する専門知識やスキルを結集し、研究セキュリティに対する包括的なアプローチを確保し、研究・イノベーション部門に対する政府の行動やメッセージの一貫性を促進する必要がある。
7. これは、研究・イノベーション協力における機会とリスクに対するバランスの取れたアプローチが維持され、新たな脅威主体の出現を含む脅威の状況における進展が見過ごされないことを保証

する最善の方法であると考えられる。

8. 保護措置の意図せざる副作用として起こりうる、直接的、間接的を問わず、あらゆる形態の差別や汚名を回避し、基本的権利や共有された価値観を完全に尊重するためのあらゆる努力が払われることを確保することが必要である。
9. 進化するリスク、新たな知見、地政学的文脈によって形成される研究安全保障のダイナミックな性質を認識し、研究安全保障政策が常に最新で、効果的かつ適切であることを確保するために、定期的なレビューを実施する学習的アプローチを必要とする。

○提言

加盟国に対し、以下のことを勧告する。教育機関の自治と学問の自由を十分に尊重し、各国の事情と国家の安全保障に対する責任に従って、以下のことを行うことを勧告する：

1. 前述の責任ある国際化のための原則を考慮しつつ、本項に列挙した要素を最大限に活用し、研究セキュリティを強化するための首尾一貫した一連の政策行動の策定と実施に取り組むこと。
2. 責任と役割を明確化し、国内行動計画を策定し、関連する場合には国内ガイドラインを策定し、研究セキュリティを強化するための関連措置やイニシアティブを、その実施スケジュールとともに列挙することを目的として、研究・イノベーション関係者との対話に参加する。
3. 研究・イノベーションにおける国際協力に関連するリスクに研究者やイノベーターが対処するのを支援するための支援体制、例えば研究安全保障アドバイザリー・ハブを構築する。分野横断的な専門知識とスキルを結集し、研究実施機関が十分な情報に基づいた意思決定を行うために利用できる情報やアドバイスを提供し、将来の国際協力の機会とリスクを比較検討する。
4. サイバーセキュリティの観点を含む脅威の状況の分析や、政策に関連する研究の実施や委託を通じて、研究セキュリティ政策立案のための証拠基盤を強化する。
5. EUの経済安全保障にとって重要な技術分野に関する欧州委員会勧告によって特定された重要技術については、加盟国とともにさらなるリスク評価を行うとともに、そのような集団的リスク評価の結果に特に注意を払う。
6. 特に、高等教育、研究・イノベーション、外交、情報・安全保障を担当する政策立案者を結集し、政府内の分野横断的協力を強化する。
7. 機密・非機密のブリーフィングや専任のリエゾンオフィサーなどを通じて、前述の分析・研究に関する公的・民間研究機関との情報交換を促進する。
8. 定期的なレジリエンス・テストやインシデント・シミュレーションを通じて、研究部門のレジリエンスや、適用される研究セキュリティ・ポリシーの有効性・比例性についての知見を得る。
9. デュアルユース品目に関する適用可能なEUの輸出管理規則及び第29条TEU及び第215条TFEUに従って採択された制裁措置の遵守を確保するため、特に無形技術移転（ITT）に関する国内措置を講じるとともに、特定の技術の移転を禁止する制裁措置など、研究及びイノベーションに関連する制裁措置の実施及び執行を強化する。
10. 公的資金を通じて開発されたツールやリソースを共有し、これらのツールやリソースの国境を越えた利用を促進し、使いやすくアクセスしやすい方法で提供することを目的として、研究開発へ

の外国からの干渉への取組に関するEUのワンストップ・ショップ・プラットフォームに積極的に貢献する。

11. 民間部門とともに、研究集約型の新興企業や中小企業を含む、民間研究・イノベーションに携わる企業向けの的を絞った情報やガイダンスを開発する。
12. 適切な場合には、リスク評価に基づき、本勧告に含まれる措置を、学生および職員の移動活動を含む高等教育における国際協力活動に適用することを検討する。

研究助成機関の役割について

13. 以下のことを確実にするために、研究助成機関と協力する：
    (a) 研究セキュリティは、プロジェクトのリスクプロファイルを規定する様々な要因を考慮した申請プロセスの不可欠な一部である。その目的は、研究協力が行われる背景や、どのような動機や（隠れた）意図がその役割を果たしうるかについて、受益者を刺激し、潜在的なリスクや脅威を前もって確認し、後の段階での問題を可能な限り回避することである。
    (b) 懸念事項（「レッドフラッグ」）がある研究プロジェクトは、そのリスクプロファイルに応じたリスク評価を受け、その結果、特定されたリスクに対処する適切なセーフガード措置に合意する。
    (c) 国の資金プログラムでセーフガード措置を適用する場合には、関連するEUの資金プログラムで適用されているものが考慮される。
    (d) 申請者は、リスクの高いプロジェクトのパートナー候補から、例えばパートナーシップ契約の合意を通じて、研究成果が人権の尊重を含む基本的価値を守る形で利用されるよう保証を求める。
    (e) 研究セキュリティ上の懸念に対処するための十分な専門知識とスキルが研究助成機関内にあり、また、インシデントの把握やコンプライアンス違反の場合の信頼できる措置を含む、様々な段階でのプロジェクトを監督するための適切な監視・評価手段が整備されていること。

高等教育機関およびその他の研究実施機関への支援について

14. 高等教育機関およびその他の研究実施機関に対し、以下を奨励・支援する。
    (a) 情報交換、相互学習、ツールやガイドラインの開発、事故報告を促進するため、関係者によるセクター全体のプラットフォームを構築する。希少で分散している資源や専門知識を最大限に活用するために、リソースのプーリングを検討する。
    (b) 不必要な事務的負担を避けつつ、リスク評価、パートナー候補のデューディリジェンス、懸念要素（「レッドフラッグ」）がある場合のより高いレベルの内部意思決定へのエスカレーションを含む、内部リスク管理手順を構造的に実施する。
    (c) 基本的価値観の尊重、学問の自由、互恵性、成果の普及と価値化、成果のライセンシングや移転、スピンオフの創出など知的財産管理に関する取り決めなど、重要な枠組み条件を盛り込むよう主張し、協定の条件が遵守されない場合の出口戦略を確保する。
    (d) 高等教育・研究における外国政府後援の人材育成プログラムに関するリスクを評価し、特にその受益者に課される望ましくない義務に焦点を当て、外国政府後援の学内コース・研修提供者が受入機関の使命と規則を遵守することを保証する。

(e) 専任の研究セキュリティの専門知識と技能に投資し、適切な組織レベルで研究セキュリティの責任を負わせ、サイバー衛生と、開放性とセキュリティが両立する文化の醸成に投資する。

(f) 実務担当者や新入職員に対する研修の一環として、オンラインコースを含む研修プログラムを開発し、次世代のセキュリティアドバイザーや政策立案者の育成を目的としたカリキュラムを開発する。構造的な審査プロセスの一環として、研究職、特に重要な研究領域の研究職の応募書類について、懸念を抱かせる要素（「レッドフラッグ」）をチェックし、発見できるよう採用担当者を訓練する。

(g) 科学出版物やその他のあらゆる形態の研究成果の普及において、資金源や研究スタッフの所属の完全な透明性を確保し、海外からの依存や利害の対立やコミットメントが研究の質や内容に影響を与えることを避ける。

(h) 物理的、仮想的な区分けを導入し、研究所や研究インフラ、データ、システムなど、特に機密性の高い分野については、厳密な必要性に基づいてアクセスが許可されることを保証し、オンラインシステムについては、強固なサイバーセキュリティの取り決めを行う；

(i) 直接的・間接的を問わず、あらゆる形態の差別や汚名が防止され、個人の安全が保証されるようにする。特に、出身国によるディアスポラへの強制や、その他の形態の悪意ある影響に注意を払う。

国レベルでの行動支援について

15. 本勧告の実施を支援するために欧州委員会が実施した、または実施する意向のある行動を促進する観点から、全面的に協力する。

(a) 意識の向上、相互学習の促進、政策の一貫性の促進を図るため、オープンな調整方法、特にERAの統治機構を最大限に活用する。

(b) 研究セキュリティに関する欧州専門家センター（European Centre of Expertise on Research Security）を中心的な拠点として設立し、欧州委員会の研究開発への外国からの干渉への取組に関するワンストップショップ・プラットフォームと連携させ、EU全体の実践共同体を形成し、関係機関との構造的な対話を維持するとともに、研究セキュリティに関する政策に関連した研究を行い、EU全体の傾向とパターンを分析することに貢献する。

(c) 上級代表と協力して、研究・イノベーションのエコシステムに影響を及ぼすハイブリッドな脅威を構造的に評価することにより、政策立案者の状況認識を高める。

(d) 高等教育機関や官民の研究実施機関が自主的に利用できる国レベルのレジリエンス・テスト手法を開発する。

(e) 加盟国とともに、また、利害関係者の参加を得て、重要技術のリスク評価に関する作業を継続し、同時にリスク評価と研究安全保障措置に関する情報共有とアプローチの一貫性を確保するための対話に関与する。

(f) 高等教育機関や官民の研究実施機関による、将来のパートナーについてデューディリジェンスの実施を支援するための、国にとらわれない、また国に特化したツールやリソースを開発する。

(g) 必要に応じて、リスク評価手順の開発および関連するEU法の適用に関する解釈ガイダンスを作成する。

(h) 研究・イノベーション部門と連携し、研究資金源や研究者の所属の透明性を高める最善の方法を評価する。

(i) 研究セキュリティに関する国際パートナーとの対話を強化するとともに、多国間の場において、このテーマに関するEUの共通の考えを伝えるためのイニシアティブをとる。

○報告

1. 加盟国には、本勧告を可能な限り速やかに実施することが推奨される。加盟国は、それぞれの出発点を考慮し、研究セキュリティを強化するためにとるべき対応策を定めた行動計画（加盟国への勧告のポイント2で言及されている）を、［理事会採択から9ヶ月後の日付を挿入］までに欧州委員会と共有するよう要請される。
2. 欧州委員会は、加盟国と協力し、関係する利害関係者と協議した上で、ERAガバナンスのモニタリングおよび報告の枠組みを用いて、本勧告の実施における進捗状況をモニタリングし、2年ごとに、研究・イノベーションのためのグローバルアプローチに関する報告の一環として、理事会に報告する。綿密な評価の後、また地政学的状況の今後の進展に照らして、さらなるステップや措置を提案する可能性がある。

2.5.3 研究活動の国際化、オープン化に伴うリスクの管理のための主な取組

「オープンサイエンス」（Open Science）が欧州では推進されており、オープンサイエンスと「海外からの干渉」の防止をバランス良く達成することが意図されている（「可能な限り開放的で、必要な限り閉鎖的な国際的共同研究を促進」）。欧州委員会が策定し、2022 年 1 月に公表された「研究・イノベーションにおける外国からの干渉に対処するためのスタッフ作業文書」（Tackling R&I foreign interference staff working document）は、「スタッフ作業文書」というタイトルであることからも分かるように、欧州連合加盟国や、大学・研究機関に対して法的拘束力を持つものではない性格を持つ。

「海外からの干渉（foreign interference）」とは「外国の国家レベルの行為者によって、あるいは外国の国家レベルの行為者のために行われる活動で、強制的、隠密的、欺瞞的、又は腐敗させるものであり、欧州連合（EU）の主権、価値、利益に反するものである」。

この文書は、欧州連合加盟国や、大学・研究機関に対して法的拘束力を持つものではないが、海外からの干渉を防止し、対処するために、大学・研究機関がどのような行動を取ることができるかを具体的に記述しており、チェックリストとして利用することも可能である。

包括的な戦略を策定するためのツールキットとして作成されたもので、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た主要な注目分野をカバーしている。それぞれのカテゴリー別に、「海外からの干渉」への対応策を列挙している（2022 年版報告書（未来工学研究所）の表 2-42（p.139）「「海外からの干渉」への対応策」を参照）。以下の表はこれらをまとめたものである。

表 2-10：「海外からの干渉」への対応策

価値観

1. 学問の自由が危険にさらされている国やパートナー機関を特定する。
・ 最初の方向付けとして、「世界の学問の自由度指数」（AFi）を参考にする。
・ 次に、その国や特定のパートナー機関の研究・教育・制度環境について、より詳細に評価する。
・ その後、学問の自由を損なう外部要因の動機を分析し、欧州の研究者や機関を制限したり道具化したりする外部要因の能力を監視する。
2. 当該教育機関における学問の自由とインテグリティに対する外部からの圧力を理解するために、脆弱性評価（vulnerability assessment）を実施する。
・ 機関及び/又はプロジェクト固有の脆弱性評価を実施する。
・ 外部のアクターとの既存の協力関係によって、何らかの依存関係が生じていないかどうかを確認する。
・ すべてのパートナーシップ協定が学問の自由を適切に保護していることを確認する。
・ 研究者に授与される名誉学位だけでなく、外部からの任命を監視する。
・ 学問の自由や普遍的な価値が危険にさらされている機関と交流するすべての人にトレーニングを提供する。
・ 学問の自由に対する脅威を機関内でマッピングするための報告メカニズムを構築する。
3. 機関及び個人レベルで学問の自由とインテグリティへのコミットメントを強化する。
・ 特定の脆弱性が特定されたら、それに対処する。
・ 学問の自由と普遍的価値が危険にさらされている機関と関わるすべての人にトレーニングを提供する。
・ 学問の自由とインテグリティを、あらゆる学術教育プログラムのコアカリキュラムに組み込む。
・ 学問の自由とインテグリティの重要性を、頻繁に、そして公に表明する。
・ 学問の基本的価値の重要性と保護についての学生、教員、事務職員の意識を向上させる。
・ 外部のアクターが抑圧しようとする研究テーマに取り組む学者を支援する。
・ 学問の自由が脅かされている国からの客員学者や新入生に対する専用の支援プログラムを立ち上げる。
・ 迫害されている学者や学生を保護するために、（一時的な）聖域を提供することを支援する。
・ 民主主義の誓約書への署名を検討する。
4. 抑圧的な環境下にあるパートナーとの協力を継続する。
・ 非自由主義的な制度環境にいる学生、学友、機関に汚名を着せたり、疎外したりしないようにする。
・ 抑圧的な環境が学問の自由にどのような影響を与えうるかについて、認識と理解を深める。
・ 抑圧的な環境での危険な研究が、関連する委員会によって自動的に拒否される（それによって抑圧される）ことがないように、標準的な倫理手順を見直す。
・ 抑圧的な環境における監視リスクの管理を支援するため、データとデジタルセキュリティに関するガイダンスと個別の技術支援を提供する。
・ ハラスメント、拘留、失踪のケースに対処するための緊急手順を設定する。
・ 抑圧的な環境との協力に対処するために調整された、透明性と審査メカニズムにコミットする。

ガバナンス

1. 海外からの干渉に対する行動規範を公表する。
・ 以下の保護を確保する。 ➢ 学問の自由 ➢ データのセキュリティと知的財産 ➢ 研究、教育、学習支援における卓越性と開放性。 ➢ 倫理、インテグリティ、信頼。
・ 以下の手順を含む。 ➢ 海外からの干渉の特定（データ漏洩や倫理的に問題のある研究を含む）。 ➢ 内部告発者の保護。 ➢ 内部利益相反への対処。
2. 海外からの干渉委員会（Foreign Interference Committee）を設置する。
・ 委員会は既存の組織構造と統合され、以下を担当する。 ➢ 教育・訓練による意識改革 ➢ 潜在的なリスクの監視 ➢ 国際協力における研究データ及び知的資産の管理。関係する研究グループへのアドバイスや支援の提供。 ➢ リスク管理及びリスク軽減 ➢ 海外からの干渉の調査

パートナーシップ

1. リスクマネジメントシステムを導入するための一般的な前提条件を整備する。
・ 海外からの干渉調査委員会（Foreign Interference Investigative Committee）は、手順を見直し、必要な場合はそれを拡大・強化することで、すべてのパートナーシップにおいて知識のセキュリティと学問のインテグリティが保護されるようにすべきである。
・ パートナーシップに関わる潜在的なリスクと、それを軽減するための機関の方法について、幅広い認識を高める。
・ リスク管理戦略への支持を高める。
・ 輸出管理法及び外国直接投資（FDI）審査に関する認識と知識を高める。
・ 機関の「クラウンジュエル」（※王冠を飾る宝石のような価値あるもの）を特定して保護し、第三国から見た潜在的な技術的、安全保障的、経済的利益を理解する。
・ パートナーシップに関する計画を「海外からの干渉委員会」に報告するための基準を定め、報告のフォローアップに責任を持つ者を決定する。
・ 様々なタイプのパートナーシップに対するデューディリジェンスの最低レベルを定義する。
・ 海外からの干渉委員会は、リスク管理小委員会又は作業部会を設置することができる。
2. 強固なパートナーシップ合意を策定するための健全な手順を確立する。
・ ポジティブなアジェンダの開発：国際協力のための安全又は低リスクの領域を特定する。
・ パートナーシップの準備：国際化の一環として、戦略的なビジョンに基づくことを確認する。
・ パートナー組織について、またその国の研究システムにおける位置づけについて、正しい知識を身につける。
・ デューディリジェンスの実施：セキュリティ、価値観、評判に関する潜在的なリスクをスタッフが評価できるように情報を収集する。
・ パートナーシップ協定を慎重に交渉する：金銭的な約束、知的財産権、データ管理、オープンサイエンスなど、責任の透明性を確保する。

・　合意の履行の監視：海外からの干渉の可能性に関する問題に焦点を当てる。
・　協力の成果を評価し、将来の関与のための教訓を得る。

サイバーセキュリティ

1. サイバーセキュリティリスクの認知度向上
・　機密コンピューティング（confidential computing）を含む、利用可能で実装されているすべてのデータ保護技術に関するトレーニングを開発し、セミナーを開催する。
・　研究者、学生、事務・支援スタッフに対し、サイバー衛生（cyber hygiene）に関する教育・訓練を行い、リスクを特定し、サイバー攻撃を回避・対処する方法を知ってもらう。
・　サイバー攻撃が疑われる場合に、わかりやすいエスカレーションプロセスを開発・伝達し、報告されたインシデントをトリアージするための単一の連絡窓口を周知する。
・　サイバーセキュリティリスクのトップ 10 リストの維持と伝達を行う。
・　サイバーセキュリティインシデントを説明するベストプラクティスを掲載したニュースレターを定期的に発行する。
2. 海外からの干渉行為者によるサイバーセキュリティ攻撃を検知し、防止する。
・　オープンソースインテリジェンス（OSINT）調査を定期的に設定・実行し、異常な行動にフラグを立てるアラート機能を作成する。
・　研究者、事務・支援スタッフの審査手順を策定する。
・　サイバーセキュリティ認証を受けた機器を調達し、機密コンピューティングを含むデータセットの機密保護ソリューション（confidentiality protection solutions）の開発に投資する。
・　必要なレベルに応じた物理的なアクセス制御を実施する。
・　オフィス・企業活動クラスターにおいて、オペレーティングシステムとインストールされたアプリケーションの集中管理アプローチを開発し、ローカル管理権（LAR）を無効化及び削除する。
・　重要なサービスやリポジトリにアクセスするための二要素認証（2FA）を有効にし、既知の悪意あるウェブサイトや侵害するウェブサイトへのアクセスを禁止するブロックリストを維持・実施する。
3. 海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う。
・　教訓を共有し、共有ブラックリスト、評価システム、データベースを更新することにより、状況認識能力を向上させる。
・　影響を受ける当事者と対応に必要な人物の双方が参加する明確なプロセスを含む、インシデント処理のための計画を策定する。SIM3 セキュリティインシデント管理成熟度モデル（SIM3 Security Incident Management Maturity Model）などのインシデント処理モデルから慣行や要素を採用する。
・　フォレンジック準備機能を導入し、対応にかかる時間を短縮する。
・　違反したスタッフの懲戒処分を行い、その際、デジタル調査の証拠も含める。
・　インシデントに対して、関連する法執行機関、国家情報・セキュリティ機関、知的財産局、データ保護当局を関与させる。

出典：European Commission. Directorate-General for Research and Innovation. *Tackling R&I Foreign Interference*. Staff Working Document (2022/1).
「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、139～142 頁）

2.6 フランス

2.6.1 研究活動の国際化、オープン化に伴うリスク管理の概要

研究活動の国際化、オープン化に伴うリスク管理について、フランスでは 2011 年から政府主導で「国の科学・技術可能性保護（PPST[65]）」という省際間プログラムの政策が採られてきた。これは主に軍事や経済の保護の視点でのアプローチで進められてきたものである。海外からの干渉、影響から自国の利益となる科学技術研究やその成果を守るための策が施され、法的裏付け、行政上での制度化が行われてきた。

一方、フランスにおける研究インテグリティ（フランスでは科学インテグリティ[66]の用語が使われている）とは、主に職業倫理のアプローチからくる概念とされてきており、研究活動の国際化、オープン化に伴うリスク管理とは別の案件となっている。例えば主要資金配分機関である仏国立研究機構（ANR[67]）の ANR 2024 年行動計画[68]に掲げられた 6 つの誓約で、研究活動の国際化、オープン化に伴うリスク管理である PPST と科学インテグリティはそれぞれ別項目として書かれている。

当報告書は、研究活動の国際化、オープン化に伴うリスクに関するフランスの状況・施策調査が目的であるため、フランスでの研究インテグリティ（フランスでは科学インテグリティ）の状況、施策でなく、PPST を中心とした研究活動の国際化、オープン化に伴うリスクに係ることがらを記述していく。

研究活動の国際化、オープン化に伴うリスク管理について、近年研究活動を行っている機関、場所への外国からの脅威は無視できなくなっているという状況について、2021 年、上院議員アンドレ・ガトランが主導する調査部会が「我々の科学資産と学術の自由をより良く保護[69]」と題される報告書を発表した。つまり「研究活動の国際化、オープン化に伴うリスク管理について」の状況調査である。ここでは調査内容とともに今後の進言も付されている。

現場である研究機関ではリスク管理のために PPST が制度化されているものの、適用対象となる分野の範囲が不十分であったり、制度自体がさらに進化していかなければならなかったり等の評価があり、また PPST 担当者以外の研究機関関係者はまだシステムについての認識が浅いために、PPST 担当者以外のスタッフ、研究実施者への、説明会やネットでの記事掲載による PPST の啓蒙活動から取り組んでいこうという動きが見られる。

---

65 PPST：Protection du Potentiel Scientifique et Technique de la nation
66 科学インテグリティ：intégrité scientifique
67 ANR：Agence Nationale de la Recherche
68 ANR Plan d'action 2024, 2023 年 7 月（2023 年 9 月にアップデート版発表）
69 Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021

2.6.2 政府・省庁の政策、ガイドライン

(1) 国の科学・技術可能性保護（PPST）

国の科学・技術可能性保護（PPST：Protection du Potentiel Scientifique et Technique de la nation）施策とは、公立、民間に関わらず研究活動が行われている機関・施設において、国の優位性に貢献する戦略的知識、ノウハウ、機密性を有する技術を保護するために行われている省際間プログラムである。2011 年より政府主導で進められてきたもので、リスクを伴う研究活動を行う場（ZRR：制限規定適用区域[70]）の設定とリスクの種類、遵守規則が定められている。この規則に違反した場合には刑法に基づいて罰せられることになっている。

a. PPST 主管機関・実行の責任者

PPST を取りまとめているのは首相管轄の仏防衛・国家安全総局（SGDSN[71]）である。SGDSN の役割は PPST の指揮管理と省庁間の調整である。また手順の遵守を保証する。そして以下の 6 つの省には防衛・安全保障上級高官（HFDS[72]）が任命されている。

防衛・安全保障上級高官（HFDS）が置かれている 6 つの省

1. 高等教育・研究省（国民教育・若者省[73]も管轄）
2. 軍事省
3. 農業・食料主権省
4. 経済・財務・産業及びデジタル主権省
5. 保健予防省
6. エコロジー移行・地域結束省

HFDS の役割は、研究活動が行われる機関と連携し、保護の必要性を決定する。また制限規定適用区域（ZRR）の設置と解除、ZRR へのアクセスについて意見を提示する。各省の HFDS は国家安全総局（SGDSN）と連携をとりながら PPST の実践を進めている。

一方、各研究活動機関の責任者はその機関における PPST について責任を負う。責任者は機関内に安全保障・防衛担当官（FSD[74]）、ZRR 管理者などを指名し彼らに PPST の実施を委任する。

---

[70] ZRR：Zone à régime restrictive
[71] Secrétariat général de la défense et de la sécurité nationale
[72] Haut Fonctionnaire de Défense et de Sécurité
[73] 2024 年 1 月の内閣改造により国民教育・若者省はスポーツ省を統合し、国民教育・若者・スポーツ・オリンピック競技大会・パラリンピック競技大会省に改称
[74] FDS：Fonctionnaire de sécurité et de défense

b. 制限規定対象区域（ZRR）とリスクの種類

制限規定対象区域（ZRR）とは、施設・機関・事業所で戦略的研究または生産活動が行われる場所であり、例えばこれらの活動が行われるオフィス、研究所、実験プラットフォームなどである。ZRR に出入りして作業（契約による請負作業、協力協定に基づく作業、下請け作業なども含む）が行われる場合は、いかなる作業者でもその研究機関を管轄する省庁にアクセス申請が必要である。担当省の防衛・安全保障上級高官（HFDS）はアクセス申請を審査し、最長 2 カ月以内に技術・安全分析に基づく意見を発表する[75]。この担当省の HFDS の意見がアクセスを認める場合でも、研究機関の責任者はそれに従う義務はなく、別の決定を下すこともできる。一方、HFDS の意見がアクセスに否定的な場合、研究機関の責任者はこの意見に従う義務があり、ZRR へのアクセス申請は拒否される[76]。

その技術・安全分析では、ZRR における研究活動・研究成果が流用、傍受されたりする場合に想定されるリスクを以下の 4 つの種類に分類している。

ZRR における 4 つのリスクのカテゴリー

1. フランスの経済的利益に損害が生じる
2. 外国の軍事力を高めフランスの防衛能力を弱める
3. 大量破壊兵器およびその飛翔体（ミサイル等）の拡散につながる
4. 国内あるいは国外におけるテロ目的に利用される

c. PPST の法源

2011 年より進められてきた国の科学・技術可能性保護（PPST）の政策を保障する行政上、刑法上の法源は以下のようになっている。

[75] 情報 https://www.sgdsn.gouv.fr/files/files/Nos_missions/a5-ppst-v5.pdf　2023 年 12 月 15 日取得
[76] 情報 https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation/foire-aux-questions　2023 年 12 月 15 日取得

表 2-11：PPST の法源に関する文書[77]

2011 年 11 月	デクレ 2011-1425：刑法 413 条 7 項への国の科学・技術可能性保護施策（PPST）の適用[78]
2012 年 7 月	アレテ（命令）：科学・技術可能性保護施策（PPST）命令[79]
2012 年 7 月	アレテ（命令）：テロリズム或いは大量破壊兵器・その飛翔体の拡散のために流用される可能性のあるノウハウのある専門性について（非公開文書、フランス特別機密文書に分類）[80]
2012 年 11 月	省際間通達文書：国の科学・技術保護施策（PPST について）[81]

出典：仏刑法 413 条、表作成：未来工学研究所

d. PPST の情報システム安全保障方針（PSSI）[82]

国の科学・技術可能性保護（PPST）では関係する研究機関に情報システム安全保障方針（PSSI）の策定を義務付けている。PSSI はその機関の内部文書であり、国家情報システムセキュリティ庁（ANSSI）[83]が奨励する対策やそれぞれの研究機関に特有の状況に対応する内容を取り入れたもので、情報システムの健全な利用と、セキュリティに関する事故・事件、およびそれらに関連する経費の削減を目的としている[84]。

(2) その他の主な政策

a. 国際協力契約・合意の審査

国の科学・技術可能性保護（PPST）に加え、高等教育・研究省とヨーロッパ・外務省による国際協力計画・合意の審査システムが存在する。これは教育法 D123-19[85]で定められており「外国または国際機関と契約を締結しようとする全ての教育機関は、学術的か非学術的かを問わず、高等教育担当大臣、監督当局および外務大臣に契約書の草案を提出しなければならない」とされている。このスクリーニングは、大学および研究機関が外国の大学および研究機関と契約を結ぶ自由の原則を定めた教育法に法的根拠がある。両省は共同研究契約を審査し、1 ヶ月以内に反対の意思を表明しなければならない。1 ヶ月を超えて反対意見が

[77] 情報 https://www.senat.fr/rap/r20-873/r20-87314.html, Sénat, 2023 年 12 月 15 日取得
[78] Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation
[79] Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation
[80] Arrêté du 3 juillet 2012 relatif aux spécialités dont les savoir-faire sont susceptibles d'être détournés à des fins de terrorisme ou de prolifération d'armes de destruction massive et de leurs vecteurs (document non publié, classifié « Confidentiel Défense - Spécial France »)
[81] Circulaire interministérielle du 7 novembre 2012 de mise en oeuvre du dispositif de protection du potentiel scientifique et technique de la nation
[82] PSSI : Politique de Sécurité des Systèmes d'Information
[83] ANSSI : Agence nationale de la sécurité des systèmes d'information
[84] SGDSN, https://www.sgdsn.gouv.fr/files/files/Nos_missions/a5-ppst-v5.pdf 2023 年 12 月 15 日取得
[85] Article D123-19, Version en vigueur depuis le 18 juin 2015, Modifié par DÉCRET n°2015-668 du 15 juin 2015 - art. 4

出されなければ合意審査はクリアしたとされる。

2019 年 1 月からの統計では毎月およそ 28 件の国際合意がこの審査にかけられており、反対の意思が表明されたものは全体の 6.5%となっている[86]。

b. 研究のための経済インテリジェンスガイド[87]

知識の創造と普及が経済発展に与える影響がますます重要になってきた 21 世紀、フランスでも研究分野は知識創造の主要な手段であり、それゆえ国の経済において重要な役割を果たしていることが強く認識されてきた。そして 2010 年、国の将来のために戦略的に有望あるいは不可欠な分野を成長させる目的で、研究・イノベーションのための国家の大型予算投入政策である「未来への投資プログラム（PIA[88]）」が開始された。それに呼応し、経済インテリジェンスの概念の、研究分野への導入を促進するため 2011 年、「研究のための経済インテリジェンスガイド」が発表された。策定と主管はフランスにおける経済インテリジェンスを指揮する省際経済インテリジェンス委員会（D2IE[89]）で、研究分野のための同インテリジェンスガイドの発表と指導を担当しているのは高等教育・研究省である。2011 年に発表されてから刷新されつつ、現在も研究分野を促進・監督するツールとして利用されている。

この施策の主な柱は、戦略的インテリジェンスと無形資産の保護、企業競争力の支援と公的研究機関の技術移転能力、そして経済安全保障であり、適用対象は大学、理工学校、研究関連の組織団体、研究関連の財団と、すべての研究活動を行う機関となっている。

同インテリジェンスガイドは以下のカテゴリーごとにまとめられている。

1) 戦略的監視
2) 無形資産の管理
3) 情報システムセキュリティ方針
4) 研究と社会経済の間のインターフェイスの発展
5) 国際政策

[86] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021
[87] Guide de l’intelligence économique pour la recherche
[88] PIA : Programme d'investissements d'avenir
[89] D2IE : Délégation interministérielle à l’intelligence économique

2.6.3　研究機関、資金配分機関の状況

これまで政府の政策・施策を見てきたが、これが現場ではどのように捉えられ実施されているのか、資金配分機関である仏国立研究機構（ANR[90]）、国立の最大研究機関である仏国立科学研究所（CNRS[91]）、大学としてソルボンヌ大学の状況を見てみる。

a. 資金配分機関の例：仏国立研究機構（ANR）

仏国立研究機構（ANR）は 2005 年、フランスの科学研究とイノベーション促進のために設立され、研究分野における複合領域間共同、官民協力の推進によりフランスの欧州・国際研究分野での地位の向上の実現を目指す機構である。主な役割は資金配分、研究促進・研究機関管理であり、主管は高等教育・研究省（MESR）となっている。2022 年年次報告によると 11 億ユーロの予算で 2,000 以上の研究プロジェクトへの資金配分を行っている。

ANR 2024 年行動計画[92] では以下の誓約が謳われており、その中で「科学インテグリティ」（1 つ目の項目）、知識・ノウハウの保護について（PPST : 6 つ目の項目）が挙げられている。

<ANR 2024 年行動計画での誓約>

1. 職業倫理と科学インテグリティ
2. 性別による差別の軽減
3. 開かれた科学：成果へのアクセスなど
4. 科学と社会：持続可能な社会のための科学
5. 遺伝資源へのアクセスとその公正な利益配分：名古屋議定書（2010 年）
6. 国の科学技術可能性保護(PPST)

6 番目の誓約である PPST、つまり当調査の焦点である「研究活動の国際化、オープン化に伴うリスク管理」について、ANR は ANR の資金配分を受ける者および ANR の資金配分への応募者に仏防衛・国家安全総局（SGDSN）の推奨に従った施策を講じることを促進すると掲げている。また高等教育・研究省の防衛・安全保障上級高官（HFDS）が指揮する防衛・安全保障上級高官課（SHFDS[93]）に従い、ANR は海外の組織との協力チームで資金配分に応募する者や海外共同プロジェクトを実施しようとする者は高等教育・研究省の SHFDS によってプロジェクト審査が行われることが記されている。

b. 研究機関の例：仏国立科学研究所（CNRS）

国立科学研究所（CNRS）はフランス最大の研究機関である。高等教育・研究省（MESR）が主管する国立研究所で、予算およそ 40 億€、スタッフ 33,000 人以上、うち研究者およそ

[90] ANR : Agence Nationale de la Recherche
[91] CNRS : Centre national de la recherche scientifique
[92] ANR Plan d’action 2024, 2023 年 7 月（2023 年 9 月にアップデート版発表）
[93] SHFDS : Service du haut fonctionnaire de défense et de sécurité

28,000 人、フランスおよび外国で合計 1,100 以上の研究所という規模を持つ組織となっている[94]。年間平均約 250 件の国外との協力合意が結ばれている[95]。

CNRS における研究活動の国際化、オープン化に伴うリスク管理について CNRS のウェブサイトで紹介されているリスク管理担当官の話や、実践項目には以下のものがある。

1. 海外からのリスク管理と研究インテグリティに関して
   CNRS において安全保障・防衛担当官（FSD）が話したこと[96]：アカデミック・インテグリティとは､科学インテグリティも含む｡科学インテグリティという意味が、外国が利益のために科学を悪用することを防ぐことも含むならば、このような脅威は、国家の基本的利益に対する脅威であり、PPST の下での FSD の職務対象となる。一方、職業倫理担当責任者は、尊厳、誠実さ、公平性、中立性、世俗性といった倫理的義務や原則を遵守するために必要なあらゆる助言を CNRS 職員に提供する任務を担っている。2012 年から 2018 年までの間にこれら職務の多さによって役割が希薄化する危険性がある。全体的な調整が不可欠であり、PPST、科学インテグリティ、職業倫理のメカニズムの間で、構造的かつ組織的な対話が確立されなければならない。
2. CNRS での実践[97]
   CNRS では、外国が関わる協力契約案件について安全保障・防衛担当官（FSD）が 18 の部局に対し 12 の基準を設定しており、案件の承認にはこれら基準のチェックが少なくとも CNRS の FSD、場合によっては署名前に主管省庁である高等教育・研究省の防衛・安全保障上級高官（HFDS）の意見が必要となる。そのチェックポイントの例は以下のようになっている。

   - 国外の CNRS 施設に設定された制限規定対象区域（ZRR）内でのすべての行為
   - 既に署名された協力関係の改訂
   - 科学研究を行うために中国の奨学金の資金を利用する外国人の、高等教育・研究省（MESR）のチェック
   - ロシアのメガグラント、千人計画を含む中国の奨学金を得ている者
   - 仏国立研究機構（ANR）が、フランス政府単体のプログラムあるいは EU の Horizon Europe 枠組プログラムで資金配分を行うプロジェクトにおいて、そのプロジェクト設計に欧州以外の国の組織との協力が含まれているもの。

[94] CNRS https://www.cnrs.fr/fr/carte-didentite, 2023 年 12 月 15 日取得
[95] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021
[96] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021
[97] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021

- アメリカ DARPA[98]など海外機関のプログラムへの参加

3. 制度の確立と拡充について：安全保障・防衛担当官（FSD）の人員数の不足

後述のガトラン・レポートでは、CNRS は大きな組織に関わらず安全保障・防衛担当官（FSD）をリーダーとした小さなチームで業務を担当している現状を挙げている。そして PPST 制度の確立と拡充のためには人員の増加とそれを可能にするための予算配分が必要だと書かれている[99]。

c. 大学の例：ソルボンヌ大学

ソルボンヌ大学では大学活動における外国の干渉と技術の横取り（傍受・流出等）のリスクを認識し、研究、研修の段階での保護についてグッドプラクティスを実施しているとし、2023 年 11 月、同大学の安全保障・防衛担当官（FSD）を務めている地政学者で文学部教授のフィリップ・ブランジェ氏の PPST の解説と必要性についてのインタビューを同大学のウェブサイトに掲載している[100]。インタビューのタイトルは「どのように私たちの科学的および技術的な可能性を保護するか[101]」というものである。インタビュー記事の内容は、外国からの干渉、情報流出の危険性についてと、国際交流を維持しながら、研究、研修活動を安全に行っていくための方法、その実施のためにソルボンヌ大学が焦点を充てているポイントなどである。

国際交流を維持しながら、研究、研修活動を安全に行っていくための方法について同教授は以下の点を挙げている。

1. PPST によって課される制約と、ソルボンヌ大学が利用できる手段との間の良好なバランスを定義すること
2. 研究コミュニティが PPST の対象になる研究活動の場で、国外からの干渉と技術の横取りに対するグッドプラクティスを遵守させること
3. それぞれの研究機関、研究室に適応したペースでこれらの保護措置を徐々に採用すること
4. これらの措置が十分に受け入れられ、うまく適用されるように、信頼の空間を作ること
5. 施設のセキュリティ、コンピュータ保護、管理ファイルの管理、研究管理、国際協力案件に関する専門性を、人材面、所内で使われる情報システムとその管理面でも強化する。そのためにはリスクに関する知識を深めることが必要である。

セキュリティ確保の実践のためにソルボンヌ大学が焦点を充てているポイントには以下の 3 点が挙げられている。

98 Defense Advanced Research Projects Agency
99 Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021
100 Université de Sorbonne, https://www.sorbonne-universite.fr/actualites/comment-proteger-notre-potentiel-scientifique-et-technique. 2023 年 12 月 15 日取得
101 Comment protéger notre potentiel scientifique et technique ?

1. 運営の面では、研究所長、FSD、ソルボンヌ大学の事務局の間で、行動と手順の完璧な一貫性が必要であること
2. データ共有、内部通信プラットフォームの作成、海外出張時の通信文での情報の保護、コンピュータセキュリティ技術、機密情報の識別などコンピュータ通信手段に関する保護手段の向上
3. 研究室、実験室など現場のセキュリティ強化

2.6.4 ガトラン・レポート

2021 年 9 月、上院議員アンドレ・ガトランが主導する調査部会がまとめた「我々の科学資産と学術の自由をより良く保護[102]」と題された報告書が発表された。ここでは便宜的に「ガトラン・レポート」とする。

a. ガトラン・レポート概要

「長い間保護されてきたと思われていたフランスの研究・高等教育界は、今や外国による影響力行使の試みとはもはや無縁ではなく、外国による影響力行使の試みを免れることはできない[103]」という認識から 2021 年 7 月、国会レベルでこの状況を調査分析するための委員会が結成された。報告担当者は上院議員のアンドレ・ガトランが務めた。

調査では 30 回以上の公聴会が行われ、高等教育機関および高等教育施設への質問が行われた。また、すでに影響を受けているいくつかの国にも調査を拡大した。このレポートの内容は、2022 年 11 月のライデン国際アジア研究所の報告書[104]でも取り上げられている。

ガトラン・レポートでは自国、すなわちフランスの科学技術に関する知識やノウハウの安全保障についての状況の調査分析、起こり得る危険への注意喚起、そして今後について 5 つの目標と 26 の勧告を提言している。

また、大学・研究機関への海外からの干渉による危険は高まっている点、今の PPST の適用対象となる分野の範囲が不十分な点、制度自体がさらに進化していかなければならない点などの評価がある。特に今の PPST の適用対象となる分野に含まれていない人文科学・社会科学分野での保護施策が必要であること、PPST のシステムにおいて情報が一つに集まらず分散し、集中できていない形であること、より効果的にシステムを動かすためには予算が必要であること、などが挙げられている。また、脅威となる特定の国についても分析がなされている。

---

[102] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021

[103] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021, Sénat

[104] How National Governments and Research Institutions Safeguard Knowledge Development in Science
and Technology

b. レポートの 5 つの目標と 26 の勧告[105]

同レポートで挙げられた 5 つの目標は以下のようになっている。

1. 国政レベルにおいて、外国からの干渉に対する対策を優先項目に挙げること。
2. 学術の自由、科学インテグリティ（研究インテグリティ）と研究の保護のための制約について折り合いをつけつつ保護施策をより発展させる。
3. 大学レベルでの国際協力について透明性を確保する。
4. 高等教育・研究機関の協力関係を管理する行政上のプロセスを強化
5. 国、欧州および国際レベルでの、規定およびガイドラインの採用の促進

それぞれの目標の中での勧告を下表に挙げる。

表 2-12：ガトラン・レポートが提案する 5 つの目標と 26 の勧告（抄訳）[106]

目標 1	現況の把握と大学界とともに適切な回答を得るため、外国からの干渉にかかる問題を政策の優先項目に引き上げる
勧告 1	警報の状況把握、発令数とその際の対応処置、高等教育・研究分野に関する外国からの影響のレベルの評価の実施
勧告 2	「高等教育・研究分野の外国からの影響・事件監視委員会」の発足
勧告 3	上記委員会はフランスにおける外国からの脅威に関する定期的な報告書を作成
勧告 4	上記報告書は国会に最新のものを報告する形にし、国会でこの件が議題として取り上げられるようにする
目標 2	大学の自律を尊重する中、学術の自由と科学インテグリティの価値を守るよう大学を支援する
勧告 5	PPST の対象分野を拡大する。特に現在は対象となっていない人文科学、社会科学にも適用させるようにする
勧告 6	高等教育・科学技術・イノベーション分野の機関の職業倫理担当部署に機関内の職業倫理と（違反の場合の）特定プロセスの強化を委ねる
勧告 7	上記職業倫理担当部署と高等教育研究省（MESR）の防衛・安全保障上級高官（HFDS）とで定期的に情報交換ができる形を作る。
勧告 8	上記職業倫理担当部署と連携し、防衛・安全保障上級高官（HFDS）の職務と専門性を強化させる。
勧告 9	安全保障・防衛担当官（FSD）のネットワークを作り、省庁の専門性を受け、実践とともに情報を中央に集める。
勧告 10	安全保障・防衛担当官（FSD）の権限を明確にする。職業倫理専門家と連携し、学術界に対し欧州圏以外からの影響によるリスクについて注意喚起を行えるようにする。注意喚起は特定の複数の地域、国に関して強化される。
勧告 11	（勧告 9 で言及した）安全保障・防衛担当官（FSD）ネットワークは、特定の複数の国との協力についてのガイドラインを作成し広く学術界に配布する。

[105] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021, Sénat

[106] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021, Sénat

勧告 12	高等教育機関の理事会の中での地域の公共団体の地位を鑑み、地域の公共団体への注意喚起を確実に行う。
勧告 13	公立の機関以外の学術関係機関にも科学資産と学術の自由の保護施策を拡げる。
勧告 14	国家情報システムセキュリティ庁（ANSSI[107]）による大学の情報システムに関する監査を一般化する。
勧告 15	大学界・学術界への外部からの干渉の検出と保護のための予算を強化する。これは大学及びヨーロッパ・外務省の予算に枠を設けて行う。
目標 3	全ての大学の国際協力について透明性、相互性を国レベルで作りあげる
勧告 16	博士論文、ポストドクターの研究、科学的発表物の中で欧州以外の国から直接または間接的に援助を受けた際に報告する義務を、教育法にのっとり、また研究法の考えのもと、研究者の義務をデクレ（政令）に明文化する。
勧告 17	高等教育・研究機関およびシンクタンクで行われるプロジェクトへの欧州外からの経済支援の源泉を透明化する制度を作る。
勧告 18	欧州外の国との大学交流において相互性の必要性を国レベルに伝える。
勧告 19	欧州外の研究機関や企業において交わされる合意書には学術の自由と科学インテグリティの尊重の条項を常に加える。
目標 4	高等教育・研究機関の協力関係を管理する行政上のプロセスを強化
勧告 20	高等教育・研究省、経済・財務・産業及びデジタル主権省、ヨーロッパ・外務省、軍事省等の関係省がプロジェクトの承認に関する提訴意見を行うために教育法の条文の改正を行う。
勧告 21	上記関連の条文について、承認プロジェクトの調査期間を 3 カ月与える。
勧告 22	フランス企業の欧州外の海外拠点で行われる研究の承認は例外なくチェックする。
目標 5	国、欧州および国際レベルでの、規定およびガイドラインの採用を促進する
勧告 23	フランス国内で学術の自由と科学インテグリティを損なう干渉、場合によっては刑罰規定も含め法的、行政的措置の採用を考える。
勧告 24	欧州レベルでは EU に科学外交の戦略を提案する。
勧告 25	欧州および国際レベルで学術の自由と科学インテグリティを指標とした大学のランキングを導入するよう働きかける
勧告 26	欧州、国際レベルでデューディリジェンスとコンプライアンスに基礎を置く大学交流のガイドラインを促進する。

[107] ANSSI：Agence nationale de la sécurité des systèmes d'information

c. 国際関係についての記述[108]

ガトラン・レポートでは脅威となる国、脅威を受ける国のことなど、この事案についての国際関係・世界の状況について言及している。

ここでは、まず総括として、今日中国は科学技術・研究分野において他国への影響、干渉、情報流出、傍受のための政策を長期的に実行できる能力があり、その政策はグローバルに展開され、システマティックであるため、最重要警戒国としている。また、既にこの種の政策を進めているロシア、トルコ、ペルシャ湾の特定の国などは、中国の戦略と同様に長期的、世界規模、システマティックに実行できる能力があるだろうから将来的に危険度が更に上昇する国になっていくことも予測される、と書かれている。

ただし例に挙げられたトルコの場合は中国の場合と異なる性質を持ち、科学技術や経済に関わる知識分野への干渉というより、トルコのナショナリズム、イスラム教主義をフランスにおいても拡充・強化するために高等教育機関システムを利用する政策であると分析されている。

また、脅威を受ける側の国の分析では、アングロサクソン諸国（オーストラリア、イギリス、カナダ、アメリカ）は、数年前[109]から自国の大学セクターの脆弱性を認識していたと書かれている。例えばオーストラリアとイギリスの大学部門は外国からの留学生の授業料収入に大きく依存している構図があり、この点がウィークポイントとなっていることなどが挙げられている。そのため、これらの国々は、高等教育制度を保護するための法的枠組みやガイドラインの導入を各国議会の後押しを受けて検討・導入を始めている、と書いている。

最重要警戒国の中国が展開する孔子学院については、以下のように記載・分析されている。孔子学院は 2005 年に 1 校目がフランスに設立された。それ以来フランス各地で開校され 2021 年には 17 校が数えられる。各校は主にフランスの中規模都市に開かれたが、これは偶然でなく恣意的な配置戦略である。開校地に選ばれているのは大学がある地方都市であり、フランス全土にネットを張る形である。またブレスト市のように海軍の拠点がある都市もおさえている。

しかし、その影響力の事例は網羅的に把握できていない。その原因は干渉事例の報告システムがないこと、あるいは、そのような影響力を正確に特定することが困難なためである。そのため実効的な報告や危険特定システムを稼働させることが必要である、と同レポートは進言している。

2.6.5　今後の動向の展望

フランスでは政策実施において大統領府はじめ国のトップの政策決定権者側からの要請のベクトルが強い傾向にある。研究分野において政府が国外からの脅威を防ぐことを目的

[108] Mieux protéger notre patrimoine scientifique et nos libertés académiques, Rapport d'information n° 873 (2020-2021), déposé le 29 septembre 2021, Sénat,
[109] ガトラン・レポートのための調査が行われた 2021 年の数年前

として制度化した PPST をさらに強化・拡充していかなければならないという意見が出ている。しかし学術界の自立性尊重との折合いで妥協点を見つけなければならないことや、制度の不完全さ、現段階で研究実施機関への落とし込みが不十分であることが挙げられている。今後、より現在の状況に合った確固たるシステムへ変えていくこと、そしてそれを担当者以外の研究活動従事者へ落とし込み、実践させていくことが課題だと専門家や関係者らは考えている。

2.7 ドイツ

2.7.1 ドイツにおける研究活動の国際化、オープン化に伴うリスク管理の概要

ドイツにおいて研究活動の国際化、オープン化に伴うリスク管理の議論は、2010 年代終盤、連邦情報局（BND[110]）が中国からのリスクについて警戒が必要であると報告したことをきっかけに連邦政府側からさらに大きく取り上げられることになり[111]、2020 年以降、それが学協会、研究機関にも拡がっていった。

ドイツ学長会議（HRK[112]）はガイドラインを作成し（2020-2021）、マックス・プランク（MPG）などドイツを代表するような大規模研究機関や、ドイツ学術機関アライアンス（またはドイツ科学団体連盟：JIPSTI-JST 表記）など学術界の組織もこの問題に対処すべく様々なガイドラインを策定・実施している。例えば、ドイツ学長会議 HRK の「大学の国際協力に関するガイドラインと基準[113]」や、マックス・プランクの「マックス・プランク協会の国際協力の発展のためのガイドライン（2021）[114]」などが挙げられる。

ドイツでの当案件についての対応は、連邦政府からの関連知識の開発と普及を促進・支援し、意識を向上させるための施策に加え、ドイツ学長会議（HRK）、やマックス・プランク（MPG）など大学以外の大規模研究機関を通じて、学術界が強力に関与していることが特徴的である。

今後は、研究の自立性と国際協力によって得る科学・経済的利益との折衝点について学術界がどう対応するか、連邦国家政府と学術界との調整この案件でのポイントとなり得る。

以下にドイツの STI システム、研究活動の国際化、オープン化に伴うリスク管理についての施策の変遷、策定・発表・実施されたガイドラインの例を紹介する。

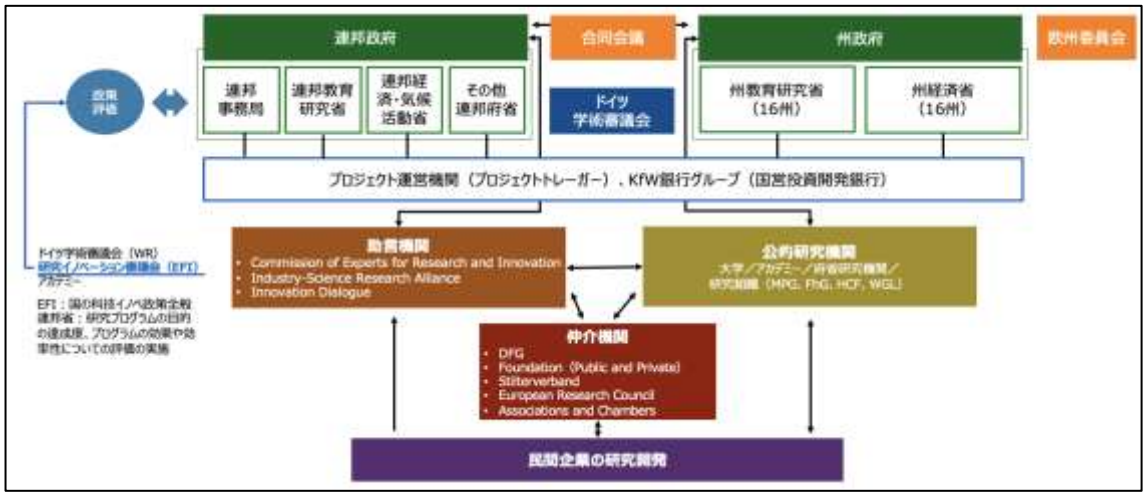
2.7.2 ドイツ STI システムと研究活動の国際化、オープン化に伴うリスク管理

ドイツは連邦制国家であり、STI 分野は連邦政府と 16 の州政府が政策を進める分権的科学技術研究開発システムとなっている。学術界の政策・方針は各州政府が責任を持っており、基本的に連邦政府には権限がない。しかし、連邦政府は、公的研究開発資金の配分や科学技術イノベーション政策の立案、大規模な科学プロジェクト（航空、宇宙、海洋、原子力等）の実施に主たる責任を有している。そして連邦政府と各州政府間の調整は「連邦政府・各州合同科学会議（GWK[115]）」によって行われている。

---

110 BND：Bundesnachrichtendienst
111 BfV. "BfV annual report 2020 - Brief summary 2020 Report on the Protection of the Constitution (Facts and Trends)". June 2021
112 HRK：Hochschulrektorenkonferenz
113 Guidelines and standards in international university cooperation, HRK, 2020 年
114 MPG. "GUIDELINES for the development of international collaborations of the Max-Planck-Gesellschaft". March 2021
115 GWK：Gemeinsame Wissenschaftskonferenz von Bund und Ländern

図 2-4：ドイツの STI システム



出典：Bundesbericht Forschung Und Innovation 2022 を元に未来工学研究所作成

(1) 連邦政府

研究活動の国際化、オープン化に伴うリスク管理について、2017 年にドイツ学術交流会（DAAD[116]）が中国の学術・研究界での脅威を報告[117]するなどの議論の種はあったが、2019 年、連邦情報局（BND）が中国からのリスクについて警戒が必要であると報告したことをきっかけに、連邦政府側からさらに大きく取り上げられることになり、それが学協会、研究機関にも拡がっていった[118]。

連邦政府側でナレッジ・セキュリティを担当している主要省庁には連邦教育研究省（BMBF）、外務省（AA）、連邦経済・エネルギー省（BMWK）および同省管轄の連邦経済・輸出管理庁（BAFA）が挙げられる。

(2) 研究機関

主要な研究実施機関には、4 大非営利研究機構・協会のマックス・プランク（MPG）、フラウンホーファ（FhG）、ヘルムホルツ（HGF）、ライプニッツ（WGL）があり、傘下の研究所がドイツ国内各所に研究拠点を有している。

116 DAAD：Deutscher Akademischer Austauschdienst
117 Daten & Analysen zum Hochschul- und Wissenschaftsstandort, DAAD-BILDUNGSSYSTEMANALYSE China, DAAD, 2017
118 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022

表 2-13：ドイツ 4 大非営利研究機構・協会

研究機関	特徴
マックス・プランク（MPG）	基礎研究に重点を置き、あらゆる分野にわたる 82 の研究所を運営
フラウンホーファ（FhG）	応用科学、工学、技術革新に焦点を当てた 105 の研究所とセンターを運営
ヘルムホルツ（HGF）	巨大科学、インフラに焦点を当てた 18 の中大規模の独立研究センターで構成
ライプニッツ（WGL）	主に人文科学、芸術、社会科学の分野で 93 の独立した研究所を構成

出典：未来工学研究所作成

このような研究機関でも、後述のように、研究活動の国際化、オープン化に伴うリスクのためのガイドラインが策定されており、特にマックス・プランク（MPG）とライプニッツ（WGL）に積極的な取組が見られている。

(3) 学協会・資金配分機関

以下に、ドイツの STI における学協会、資金配分機関を表に示す。順序は規模や上位・下位の順でなく、当報告書で挙げる主な研究活動の国際化、オープン化に伴うリスク施策に関する機関を上に示す。

表 2-14：ドイツ STI システムにおける学協会、資金配分機関

機関名	活動
ドイツ学長会議（HRK）	当案件の研究インテグリティ及びリスクに関して、国際協力研究におけるガイドラインを作成している。また、連邦教育研究省（BMBF）、下記のドイツ学術機関アライアンスとともに、当案件についてウェブセミナーを開催するなど、大学側の代表として中心的役割を担っている。
ドイツ学術機関アライアンス（またはドイツ科学団体連盟：JIPSTI-JST 表記）	ドイツの学術・研究・助成機関の総意として、学術政策、研究支援、および学術システムの発展について定期的に意見を表明している。連邦教育研究省（BMBF）、ドイツ学長会議（HRK）とともに当案件についてウェブセミナーを開催している。
ドイツ学術交流会（DAAD）	学生・研究者の交流のための助成機関。大学機関と協力し、ガイドラインを作成している。
研究イノベーション審議会（EFI[119]）	ドイツの STI 政策の評価、年次レポート作成

[119] EFI：Expertenkommission Forschung und Innovation

機関名	活動
レオポルディーナ国立科学アカデミー	ドイツの科学分野における国立アカデミー。当案件についても積極的に基準作成などを行なっている。 研究インテグリティからのアプローチでドイツ研究振興協会（DFG[120]）とともに研究の悪用リスクを最小限に抑え、個々の研究者・ 研究機関・大学による自主規制を支援するためのガイドラインを作成している（2014 年）[121]。
ドイツ研究振興協会（DFG）	公的基礎研究費配分などを担当。研究インテグリティからのアプローチでドイツ国立科学アカデミーとともに、研究の悪用リスクを最小限に抑え、個々の研究者・ 研究機関・大学による自主規制を支援するためのガイドラインを作成している（2014 年）[122]。また、このガイドラインに加え、研究プロジェクトのセキュリティ面の取り扱いを募集要項に取り込んでいる。
ドイツ中国学会（DVCS[123]）	ドイツにおける中国に関する事柄に取り組む学会。 2018 年「ドイツの学術機関と中国との交流に関するドイツ中国学会のガイダンス[124]」を出している。
連邦政府・各州合同科学会議（GWK）	連邦政府と州政府との調整を行い、公的研究機関への資金配分、高等教育協定の意思決定、などを行なっている。

出典：未来工学研究所作成

2.7.3 リスク管理施策の背景・経緯

(1) 研究の国際化の発展期

ドイツは東西統合後、従来の国内科学技術保護政策が終わり、国際化、国際競争力強化の推進が始められた。高等教育・研究分野では機関の活動の質の管理、能力基盤作成、競争力と多様性マネジメントを進める政策に転換し、高等教育の国際化、国際協力の促進による競

120 DFG：Deutsche Forschungsgemeinschaft
121 German Research Foundation(DFG)and German National Academy of Sciences Leopoldina,2014。Scientific Freedom and Scientific Responsibility, OECD, INTEGRITY AND SECURITY IN THE GLOBAL RESEARCH ECOSYSTEM, 2022 の情報より
122 German Research Foundation(DFG)and German National Academy of Sciences Leopoldina,2014。Scientific Freedom and Scientific Responsibility, OECD, INTEGRITY AND SECURITY IN THE GLOBAL RESEARCH ECOSYSTEM, 2022 の情報より
123 DVCS：Deutsche Vereinigung für Chinastudien e. V. （英：German Association of Chinese Studies）
124 Handlungsempfehlungen der Deutschen Vereinigung für Chinastudien e.V. zum Umgang deutscher akademischer Institutionen mit der Volksrepublik China（英：Guidance by the German Association for Chinese Studies on the Interaction of German Academic Institutions with the People's Republic of China）, DVCS, 2018

争力強化、世界トップレベルまでの向上への努力の段階に移った[125]。

それ以降、国外からの学生・研究者は増加し、非英語圏では最も多くの国外留学生を受け入れる国となった。これには留学生の学費優遇措置の効果もあるとも見られているが、一方、マックス・プランク（MPG）、フラウンホーファ（FhG）、ヘルムホルツ（HGF）、ライプニッツ（WGL）のドイツ 4 大研究機関で研究活動をしたいというドイツ国外の研究者の希望の影響が強いと考察できる。実際、同 4 大研究機関では、外国からの研究者数の割合は 25%となっている[126]。

一方、レオポルディーナ国立科学アカデミーとドイツ研究振興協会（DFG）は、2014 年、日本政府（内閣府）が研究インテグリティの構成について「従来、明示的に対応を進めてきた部分」と同種の目的で研究の悪用リスクを最小限に抑え、個々の研究者・ 研究機関・大学による自主規制を支援するためのガイドラインを作成している。そこでは研究機関や大学には、法的規制の遵守に加え、安全保障に関連する研究を取り扱う際の倫理的ルールの策定が推奨されている[127]。

(2) 中国からのリスクによる方針の転換期

高等教育・研究分野での国際化が進む中、2017 年、ドイツ学術交流会（DAAD）は「高等教育・科学ロケーションに関するデータ＆分析[128]」で中国の学術・研究の脅威について言及するレポートを発表した。この報告が中国からの脅威が喚起される契機となり、実際に国としてさらに動き始めたのは 2019-2020 年であった。

2020 年、連邦憲法擁護庁（BfV[129]）は連邦情報局（BND）が中国からのリスクへの警戒に対処する必要性を報告したことから、その年次レポートで、孔子学院をはじめ中国の科学技術研究・教育の脅威について著している[130]。

これらから、教育研究省（BMBF）やドイツ学長会議（HRK）が主だって、研究活動の国際化、オープン化に伴うリスクのためのガイドラインやその他施策の策定のための取組が活発になっていく。

(3) ガイドライン作成期

既に個々の組織ベースでは、ドイツ連邦経済・輸出管理庁（BAFA[131]）の「学術界におけ

---

125 Mehmet Evrim Altin, "Internationalization of the German Higher Education System New Player in the Market", Athens Journal of Education - Volume 6, Issue 3 – Pages 237-256, 08/2019

126 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022

127 German Research Foundation(DFG)and German National Academy of Sciences Leopoldina,2014。Scientific Freedom and Scientific Responsibility, OECD, INTEGRITY AND SECURITY IN THE GLOBAL RESEARCH ECOSYSTEM, 2022 の情報より

128 Daten & Analysen zum Hochschul- und Wissenschaftsstandort, DAAD-BILDUNGSSYSTEMANALYSE China, DAAD, 2017

129 BfV：Bundesamt für Verfassungsschutz

130 BfV annual report 2020

131 BAFA：Bundesamt für Wirtschaft und Ausfuhrkontrolle,（英：Federal Office for Economic Affairs and Export Control）

る輸出入管理マニュアル：2019 年[132]」やドイツ中国学会（DVCS）の「ドイツの学術機関と中国との交流に関するドイツ中国学会のガイダンス：2018 年」で、中国との学術交流に関して留意すべき点について指針が示されていた。そして教育研究省（BMBF）は経済・産業スパイに関する調査研究プロジェクト WISKOS[133]を進めていた。WISKOS プロジェクトは 2015 年～2018 年に、連邦政府資金を投入した経済・産業スパイに関する調査研究であり、教育研究省（BMBF）、連邦刑事警察庁（BKA[134]）が発注した調査研究プロジェクトである。フラウンホーファ（FhG）、マックス・プランク（MPG）を主な受託機関として行われる。

これらの動きに加え、前述の連邦憲法擁護庁（BfV）の報告などを受け、連邦政府、ドイツ学長会議（HRK）など大学組織側、そしてマックス・プランク（MPG）、ライプニッツ（WGL）など研究機関によって複数のガイドライン、留意点を示し対策を取るよう推奨する文書が策定されていく。

ドイツ学長会議（HRK）では 2020 年の年次報告書及びそれに次ぐ中国との大学協力に関する文書が作成され、研究機関側ではマックス・プランク（MPG）、ライプニッツ（WGL）など研究機関がガイドラインを作成した。また、レオポルディーナ国立科学アカデミーは安全保障に関連する研究を継続している。

2.7.4 主要ガイドライン、施策、レポートの例

前項に記述したよう、ドイツでは 2020 年以降、国全般でのガイドライン作成期に入り、複数の組織機関がガイドラインを策定している。ライデン・アジアセンターの分析[135]によると、これらガイドラインのそれぞれは焦点を当てるポイントが少しずつ異なっており、同センターは大きく総合的ガイドライン、スパイ行為に関するガイドライン、研究機関側からのガイドラインに分類して報告している。

(1) 総合的ガイドライン

2020 年 4 月、ドイツ学長会議 HRK は「大学の国際協力に関するガイドラインと基準[136]」を発表した。その前文において HRK は「世界的な環境の大きな変化に伴い、高等教育制度においても、批判的な評価と方向づけの必要性が高まっている」としており、この文書は「戦略とガバナンス」、「共同教育と学習」、「共同研究」、「トランスナショナルな場としての大学」という包括的な側面を中心に策定されている[137]。

---

132 Export Control in Academia Manual, BAFA, 2019
133 WISKOS：Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa,ドイツ及び欧州における経済スパイ及び競合者探知プロジェクト。参考「WISKOS ドイツの経済・産業スパイ研究プロジェクト」2021 年 6 月,久保田隆
134 BKA：Bundeskriminalamt
135 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022
136 Guidelines and standards in international university cooperation, HRK, 2020 年
137 HRK, ガイドラインの紹介 https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guidelines-and-standards-in-international-university-

また同年 9 月、HRK は上記「大学の国際協力に関するガイドラインと基準」を補完する形で「中国との大学の国際協力におけるガイドライン・クエスチョンズ[138]」を発表している。その目的は「ドイツの大学関係者（大学全体および個々の大学関係者）が中国との学術協力の重要な側面について認識を高め、中国の大学や学術機関との弾力的なパートナーシップを確立し、さらに発展させるための刺激、支援、方向性を提供し、実りある発展の道筋を明らかにすること」と書かれており[139]、中国共産党（CCP）が研究機関に及ぼす影響や、中国における学問の自由の限界について懸念が高まっていることを指摘している[140]。

またドイツ学術交流会（DAAD）は 2020 年、「レッドラインはない - 複雑な枠組み条件の下での科学協力：No red lines - science cooperation under complex framework conditions[141]」と題したガイドラインを策定している。これは DAAD 国際科学協力コンピテンスセンター（KIWi[142]）が中心となり作られたもので、ここでは、焦点を以下の 6 項目に分類し問題点、対応などが書かれている[143]。

1. 安全保障状況
2. 一般的な政治的要請
3. 法の支配と政治的枠組み
4. それぞれの科学システムの機会とリスク
5. 科学的パートナー機関の実績と正確さ
6. それぞれの機関の戦略への組込み

⑵ スパイ行為に関するガイドライン

教育研究省（BMBF）が進めていた経済・産業スパイに関する調査研究プロジェクト WISKOS は「ドイツの研究拠点にとってのリスク - 科学的スパイ行為や競合他社へのスパイ行為に対処するためのガイドライン[144]」を発表している。これは当 WISKOS プロジェクトの 2015 年～2018 年の間の調査研究業務の成果をもとに策定されたものである。ライデン・アジアセンターは「このガイドラインは、ドイツの大学や研究機関にスパイ活動に関す

cooperation/, 2024 年 1 月 15 日取得

138 Guiding Questions on University Cooperation with the People's Republic of China, HRK, 2020 年

139 HRK, https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guiding-questions-on-university-cooperation-with-the-peoples-republic-of-china/, 2024 年 1 月 15 日取得

140 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022

141 原題：Keine roten Linien – Wissenschaftskooperationen unter komplexen Rahmenbedingungen

142 KIWi：Gründung des Kompetenzzentrums Internationale Wissenschaftskooperationen (英：Competence Centre for International Academic Collaborations)

143 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022

144 Risiken für den deutschen Forschungsstandort - Leitfaden zum Umgang mit Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext （英：Risks for the German research location - Guidelines for dealing with scientific espionage and spying on competitors in the scientific context）
https://www.mpg.de/12584445/Handlungsleitfaden_Wissenschaftsorganisationen_final.pdf, MPG, 2024 年 1 月 15 日取得

る情報を提供するものである。さらに、推奨事項や追加リソースを提供しており、大学内のリスク分析やガバナンス構造といった共通のテーマを扱うだけでなく、研究者が研究機関を去った後の職業活動を追跡するといった具体的な提案も行っている」と分析している[145]。

(3) 研究機関、研究関連組織側からのガイドライン、分析レポート等

2021 年には、マックス・プランク（MPG）やライプニッツ（WGL）といった大きな研究機関が、ガイドラインや報告書を積極的に発表するようになった。

MPG の主要なガイドラインには以下の 2 つが挙げられる。

1. 責任ある行動のためのガイドライン（2021）[146]
   Guidelines For Responsible Conduct
   ここでは、マックス・プランク協会のような研究組織にとって、責任を持って規則に従って行動することは不可欠であること、科学の分野でも、科学を支援する分野でも、すべての人が法律や内部規則を遵守することが不可欠であることとし、研究所の全てのスタッフに対して、特にリスクの高い分野において、正しい行動をとるためのガイダンスを提供することを目的として策定された[147]。
   独語、英語の両方が併記されて作られている。
   ライデン・アジアセンターは同ガイドラインについて「技術移転、IT リスク、倫理的研究慣行、研究の倫理的利用、輸出管理、利益相反、学問の自由など、知識の安全保障のあらゆる分野を網羅している」と評している[148]。

2. マックス・プランク協会の国際協力の発展のためのガイドライン（2021）[149]
   Guidelines for the Development of International Cooperations of the Max Planck Society
   この文書はマックス・プランク協会の科学者が、研究の自由、ルールの遵守、個人の責任のバランスをとりながら、不確実で困難な条件の下でも国際協力を成功させることができるように支援するために策定された[150]。
   独語文、英語文の 2 セットが 1 つの文書ファイルに納められている。
   ライデン・アジアセンターは同ガイドラインについて「潜在的なリスクに対する認識を高め、適用される法的規則や要件、助言を得るための選択肢について研究者に

---

145 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022
146 独語タイトル：LEITPLANCKEN- Hinweise fu¨r verantwortliches Handeln, MPG, 2021 年 https://www.mpg.de/18156413/leitplancken.pdf, 2024 年 1 月 15 日取得
147 MPG, https://www.mpg.de/about_us/procedures, 2024 年 1 月 15 日取得
148 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022
149 独語タイトル：LEITLINIEN zur Ausgestaltung internationaler Kooperationen der Max-Planck-Gesellschaft, MPG, 2021 年 https://www.mpg.de/16784189/mpg-guidelines-for-international-cooperations-2021.pdf, 2024 年 1 月 15 日取得
150 MPG, https://www.mpg.de/about_us/procedures, 2024 年 1 月 15 日取得

知ってもらうことを目的としている」と評している。

ライプニッツ協会のガイドラインでは 2021 年の「国際科学協力におけるリスク管理-考えるべき点：Risk management in international scientific cooperation –points to consider[151]」が挙げられる。OECD の「グローバルな研究エコシステムにおけるインテグリティとセキュリティ：2022 年[152]」では同ガイドラインについて「マックス・プランク協会と同様に、傘下の研究機関や研究者に対して、パートナー国の政治状況やそれに伴う研究パートナーのモチベーションを評価することを求めている」と評されている。

その他、国際公共政策研究所（GPPi[153]）は 2020 年「危険なビジネス - 非民主主義国との研究協力再考。財団・大学・市民社会組織・シンクタンクのための戦略：Risky Business: Rethinking Research Cooperation with Non-Democracies. Strategies for Foundations, Universities, Civil Society Organizations, and Think Tanks[154]」という報告書を発表しており、また、レオポルディーナ国立科学アカデミーは 2022 年「情報パンフレット - ドイツにおける安全保障関連研究の取り扱いについて：Information Brochure - The Handling of Security-Relevant Research in Germany[155]」という啓蒙のための紹介文書を作るなど、2020 年以降研究機関や研究関連組織側からの、研究活動の国際化、オープン化に伴うリスク管理のためのガイドラインや分析報告書の作成が活発となっている。

また、ドイツ航空宇宙センター（DLR）は「安全で成功する国際研究開発協力のためのガイダンス集：Annotated collection of guidance for secure and successful international R&I cooperation[156]」という、各国・国際機関におけるこの案件について著された文書目録をまとめている。2022 年にアップデートされた版では、オーストラリア、ベルギー、カナダ、デンマーク、EU、フィンランド、ドイツ、日本、オランダ、ニュージーランド、OECD、スウェーデン、イギリス、アメリカの文書情報が挙げられている。

日本に関しては、2019 年の「大学・国立研究開発法人の外国企業との連携に係るガイドライン」が挙げられている。

(4) ウェブセミナーの実施

連邦教育研究省（BMBF）はドイツ学長会議（HRK）、ドイツ航空宇宙センター（DLR）、ドイツ学術機関アライアンス[157]とともに毎月学術界向けにナレッジ・セキュリ

151 https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/Über_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf, 2024 年 1 月 15 日取得
152 Scientific Freedom and Scientific Responsibility, OECD, INTEGRITY AND SECURITY IN THE GLOBAL RESEARCH ECOSYSTEM, 2022
153 GPPi：Global Public Policy Institute
154 GPPi, https://gppi.net/2020/10/22/rethinking-research-cooperation-and-exchange-with-non-democracies, 2024 年 1 月 15 日取得
155https://www.leopoldina.org/fileadmin/redaktion/Ueber_uns/Kooperationen/Information_The_Handling_of_Security-Relevant_Research_in_Germany_-_An_Overview_web.pdf, 2024 年 1 月 15 日取得
156 https://www.kooperation-international.de/fileadmin/user_upload/annotated-collection-2022.pdf, 2024 年 1 月 15 日取得
157 JIPSTI-JST 表記ではドイツ科学団体連盟

ティに関するセミナーを毎月開催している。HRK やアライアンスとの緊密な連携により、セミナーには学術関連機関から多くの参加者がある。これには連邦外務省（AA）や連邦経済・輸出管理庁（BAFA）も協力し、国際協力と知識の安全保障に関連する問題についての情報提供やデュアルユース、技術移転、輸出管理規制の実施のための施策の推進が行われている[158]。

2.7.5 総括

ドイツのアプローチは非常に包括的で、連邦政府からの関連知識の開発と普及を促進・支援し、意識を向上させるための施策に加え、ドイツ学長会議（HRK）、ドイツ学術機関アライアンス[159]、レオポルディーナ国立科学アカデミー、マックス・プランク（MPG）やライプニッツ（WGL）など大学以外の大規模研究機関を通じて、学術界が強力に関与していることが特徴的である。そのため、アプローチはボトムアップ的ともいえる[160]。これはドイツが連邦制国家であり連邦政府のほか州政府が大学組織について運営責任がある性質を持つ点に加え、学術の自由・自律を尊重する STI 分野の研究関連組織、研究機関の意向が大きく表されていると見られる。

158 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022
159 JIPSTI-JST 表記ではドイツ科学団体連盟
160 How national governments and research institutions safeguard knowledge development in science and technology, Leiden Asia Centre, 2022

2.8 スウェーデン

2.8.1 スウェーデンにおける「研究インテグリティ」に係る取組の特徴

スウェーデンの「研究のオープン化、国際化に伴う新たなリスクへの対応（以下、新たなリスクへの対応）」策は「責任ある国際化（responsible internationalization）」と呼ばれている。「インテグリティ」は研究不正等を防止する研究倫理をめぐる事柄を指す用語として使われている（Vie 2022）。もっとも、研究倫理に関する規定でも「良好な研究実践の責任と研究上の不正行為の調査に関する法（Act on Responsibility for Good Research Practice and Examination of Research Misconduct）」のように「responsibility」がその名称に用いられており、「責任ある（responsible）」もしくは「責任（responsibility）」は、スウェーデンの学界、研究者の研究及び教育活動上の理念の一つだということができる。

一連の「新たなリスクへの対応」において、中国は対応策のタイトル等で名指しこそされていないが、中国との協力活動がその前提になっている。後述するように、スウェーデンは 2010 年前後より研究及び教育分野において対中協力を積極的に進めてきた（STINT 2018）。そのため、地政学上のリスクに伴う 2019 年 3 月の欧州連合（EU）の対中政策転換[161]に伴う対応策の構築が急がれ、中国を意識した対応策の構築が取り組まれた。

しかしながら、「新たなリスクへの対応」策では、中国を敵視したり、脅威とみなしたりする言葉を避け、中国との研究/教育協力を引き続き重視する姿勢も示す[162]。2020 年に始まる一連の対応策には必ず「好機と挑戦（opportunities and challenges）」というフレーズが登場し、対中研究協力はスウェーデンの研究者に挑戦的なリスクだけでなく、チャンスやメリットももたらすことを強調している。

スウェーデンの取組はガイドライン、助言、チェックリストから構成されるが、資金配分機関と学界の共同作業によって進められてきた。ガイドラインと助言は「研究と高等教育機関の国際協力のためのスウェーデン財団（The Swedish Foundation for International Cooperation in Research and Higher Education、通称、STINT）」[163]、チェックリストは「スウェーデン高等教育機関（大学）連合（The Association of Swedish Higher Education Institutions、通称 SUHF）」が発刊したものである。しかしながら、これらの文書の起草を担ったのはルンド大学、カロリンスカ研究所、スウェーデン王立工科大学の教授たちであった。なかでも、ルンド大学の Tommy Shih 准教授は策定の中心人物で、2018 年の政府報告書以来、スウェーデンにおける研究の国際化、オープン化への対応に深く関与してきた。こ

---

161 2019 年 3 月欧州委員会は中国を経済的競争相手であり、ヨーロッパ的価値とは相容れない統治体制の「体制的ライバル a systemic rival」と位置づけ、中国への警戒を表明した（European Commission 2019.）

162 対応策の作成を中心的に担ったルンド大学の Tommy Shih 准教授は、2023 年 10 月 4 日、18:30-19:30 に実施したオンライン・インタビューの中で、この点について証言した。

163 1994 年に研究と高等教育機関（大学）の国際化を推進することを目的に政府によって設立された資金配分機関である。①国際協力プロジェクトへの「戦略的助成」、②ポスドクの「海外研究助成」、③教育サバティカル、④国際共同研究に際しての相手国側も含めて移動・滞在に要する資金を提供する「移動助成」を実施している。

うした学界主導の取組もスウェーデンの特徴の一つに挙げることができる。

ガイドライン、助言、チェックリストに一貫してみられるスタンスは、研究者あるいは大学・研究機関のリスクへの自覚を促し、かれら自身がリスクの防止と発見に主体的に取り組むことを促す自律性の推奨である。こうした考え方は、研究における不正等の防止と倫理に関する「インテグリティ」にみられる特徴であり、その点で「新たなリスクへの対応」の取組は既存の「インテグリティ」規制体系の部分と位置付けることができる。

さらに、中国との研究協力及び教育交流においてどのようなリスク、課題が生じるのか、実態調査も実施された。2 つの調査のうち、一つはスウェーデン国内のみならず中国でもワークショップ形式の聞き取りを行うなどバランスに配慮した調査である。また、米国など主要国が直面する深刻な問題とは異なる身近で、どの大学でも国際協力の過程において日常的に起こり得るような問題例が列挙されている。

2.8.2　スウェーデンにおける取組の背景と経緯

経済成長はもとより、科学技術の研究開発とイノベーションの分野（以下、STI）において急成長を遂げる中国との協力関係の構築は、スウェーデンに大きなメリットをもたらすと考えられてきた。上記のように 2010 年前後より、STI の対中研究協力が推進されてきた。たとえば、2019 年時点で同国と中国の研究者による共同論文は 20,000 件以上に及び、中国との研究協力はスウェーデンの科学研究における国際的プレゼンスの向上に貢献してきた（Tardell 2021）。また。2019 年におけるスウェーデン–中国の 2 国間共同研究の成果論文はスウェーデンの研究者が発表した全論文の 7.1%を占めていた（Tommy Shih and Erik Forsberg 2023）。

スウェーデン政府はルンド大学の教授及び准教授から構成されたタスクフォースチームに対中研究協力のあり方について諮問した。この諮問の背景には、スウェーデンの研究、イノベーション及び高等教育における対中協力は他の欧米諸国に比べて遅れを取り、この分野において急速に力をつけている中国と協力関係を発展させる必要があるとの認識があった（STINT 2018a）[164]。

ところが、2017 年ごろから新疆ウイグル自治区での人権侵害が明らかになり、中国への過度な接近が危惧されるようになった。スウェーデンは人権、民主主義、法の支配を重視し、外交においてもそれらの価値を全面に押し出してきた（Government Communication 2016）。人権侵害問題は中国との研究協力のあり方を見直す契機になった。2018 年 9 月には両国関係を悪化させる出来事が相次いだ。まず、中国の反対を押し切ってスウェーデン政府がダライ・ラマ 14 世の入国を許可し、9 月 12 日南部の都市マルメで法話が開催された。9 月上旬には、中国人観光客がストックホルムのホステルで起こしたトラブルが中国政府を巻き込んだ騒動となり、外交問題にまで発展し、スウェーデン国民の対中感情も冷え込んだ

164 スウェーデン語の報告書は、政府ホームページ、https://www.regeringen.se/artiklar/2018/10/sverige-och-kina--starkt-samverkan-for-en-hallbar-framtid/より閲覧可能である。

[165]。

このような中、2018 年 10 月に上梓された報告書「スウェーデンは中国といかに協力すべきか（Report to the government on how Sweden should cooperate with China）」は、中国との研究/教育協力は多方面で利益ももたらすが、法制度や規範の違いに注意する必要があり、同国に対する深い理解と研究協力における体系的アプローチが求められると提言した（STINT 2018b）。

翌 2019 年には、外務省が政府通信「中国に係る問題へのアプローチ（Approach to matters relating to China）」を発行し、中国の発展が及ぼす影響が大きく、適切なアプローチを要する 9 つの政策領域のうちの一つとして「研究と教育」に言及した。この領域で特段の注意を要する課題として、倫理、学問の自由、知的財産権の保護、研究成果が軍事目的に使われる可能性が懸念されるような軍事部門との繋がりを挙げ、STINT と関連機関に対し中国と関係するスウェーデンの大学・研究機関の戦略、行動及びネットワークづくりの強化に貢献すべきことを求めた（Government Communication 2019）。

政府通信は、問題への対処には中国についての知識を蓄積するための投資が必要だと結論づけ、近いうちに政府が中国に関する知識センターを設立する予定だとした。そして、2020 年以降、中国と研究協力において起こり得る問題を洗い出し、リスク回避のためのガイドライン（2020 年「責任ある国際化：国際的学術交流のためのガイドライン Responsible internationalisation: Guidelines for reflection on international academic collaboration」STINT）、助言（2022 年「責任ある国際化によっていかに業務を遂行するかに関する高等教育機関への助言 Recommendation to Higher Education Institutes on How to work with responsible internationalisation」STINT））、チェックリスト（「世界に責任を持つ関与：チェックリスト Global Responsible Engagement: Checklist」SUHF[166]）が順次公表された。

また、2021 年、政府とスウェーデン国際問題研究所の協定に基づいて、同研究所の 1 ユニットとして「スウェーデン国立中国センター （Swedish National China Centre）」[167]が設立された。スウェーデンの中国政策の調査研究、中国研究に関する最新の知見や情報を公開し、中国に関係する政府機関/関係者のほか大学/研究機関、研究者、企業、個人に提供することを目的にしているが、監視的役割（watch dog）も担っている。2021 年に中国との研究協力における問題点をスウェーデン国内 6 大学と 3 資金提供組織に所属する 12 人の研究者に実施したインタビュー調査に基づく研究論文を本センターのホームページ上で公開している（Tardell 2021）。

2023 年には、中国との研究協力における研究者及び教育担当者が直面した問題やリスク等の現状を調査した研究論文が発表された（Shih and Forsberg 2023）。本論文では、中国とスウェーデンの研究協力 20 事業を対象に、ワークショップや討論会、面接によりスウ

165 一連の騒動の詳細は北村（2018）に詳しい。
166 SUHF（スウェーデン高等教育機関協会 The Association of Swedish Higher Education）は 1995 年に設立されたスウェーデン国内の大学の連合組織である。38 の大学（16）及び大学附属の高等専門学校（22）から構成される。
167詳細は https://kinacentrum.se/en/about/を参照のこと。

ェーデンと中国の双方 51 人の事業参加者から聞き取りを行い、互恵主義の欠落、倫理上の問題、透明性の欠如などの課題を特定した。

2022 年の「助言」の中では、具体的な取組が進められている王立工科大学のリスク対処が検証されていた。その他の大学でもホームページにリスクへの注意喚起が掲載されているが、実際にどのような取組が実施されているのかは現時点では明らかではない。

2.8.3　スウェーデンにおける取組の詳細

すでに述べたように、スウェーデンにおける「新たなリスクへの対応」の取組はガイドライン、助言、チェックリストから構成されるが、その中心に位置するのはガイドラインである。助言とチェックリストはガイドラインを基礎に、前者は大学における実践事例を通して、実際の運用を示すのに対し、後者はガイドラインの内容に基づいて、個々の研究者が国際協力に入る前に検討すべき項目を平易に整理した内容となっている。また、こうした取組に並行して、対中協力に従事する研究者が実際にどのような挑戦的課題に直面したのか、その具体的内容を検証する実態調査も行われた。

(1)　「責任ある国際化：国際的学術交流のためのガイドライン」（Shih, Gaunt, & Östlund 2020）

本ガイドラインは、大学等に何らかの行為を命じる指示書や問題の具体的な解決策を示す処方箋ではなく、大学等が自らリスクを発見し、解決の方向性を見出すための提案もしくは指針であり、責任ある国際化を担保する上で注意を要する領域に焦点を当て、研究機関（者）が考慮すべき事柄を示すものだと位置付けられている。その意図するところは、それぞれの大学と研究機関（以下、大学等）が国際化と国際的学術協力へのアプローチに関して構造的かつ有用な議論を行う助けになることである。

内容は、総論と各論から構成される。

a. 総論

総論は、まず「国際共同研究は好機と同時に挑戦的な課題を伴い、なかでも研究体制が未だ発展途上にあったり、過去に汚職や人権侵害が見られたり、民主的な統治が行われていなかったりする国の研究者との協力においては、このような課題が生じやすい」ので、「国際共同研究の好機とリスクを特定し、評価し、取り扱い、監視するための構造的な手続きとそれを可能にする資源が求められる」と指摘する。その上で、大学等に以下のような４項目からなる注意を促す。

①　リスクを認識し、それを取り扱う人あるいは組織の責任の所在を明確にすること。もっとも、その事業において生じる結果や起こり得る事件を予測するのは難しいので、事業実

施過程において、起こるかもしれない悪い結果に気づくことが肝要である。

②　個々の大学等は責任ある研究の国際化を担保するための手続きを自ら決定しなければならない。この手続きの対象者は、研究と教育における国際協力を主導し、発展させる研究及び教育のスタッフ、管理部門の職員、より戦略的な協力関係を企画する各領域の学会長、大学連合の長などの学界リーダーである。

③　責任ある国際化の評価にあたっては、パートナー機関もしくは事業パートナーの地政学的、歴史的、社会的、政治的文脈について理解しておくことが望ましい。

④　スウェーデンではヒトや動物に関する研究については倫理的な認証を獲得しなければならないが、それが法規あるいは規範のいずれによるのかについては、国によって異なるので、パートナーとなる国の倫理規程について事前に入念な下調べが必要な場合がある。機関レベルでの協定の場合には、一般的には当該機関の法律スタッフが精査する。知的財産の場合も同様の措置が必要と考えられる。その他の事業では、非開示の協定、国家安全保障問題、国際機関による制裁措置に関して熟慮しなければならない。パートナー国の報道機関、SNSなど情報媒体のリスク評価、財政リスク評価なども事前に実施すべき場合がある。

以上のように、ガイドラインは、共同事業を行う前の「事前審査」の実施を推奨する。事前審査には「スウェーデンの文脈に基づいて、パートナーと協力を発展させる際の異なるステージで生じる多くの疑問に注目し、それらを体系化することによって、各大学等が自らの手続きを生み出すこと」が期待される。総論は、各大学等が自ら手続きを定め、個々の研究プロジェクトやそれに従事する教員はその責任に加え、この手続きを学習し、問題に遭遇したときに対処する能力を身につけることが望ましい」と締めくくる。

b.　各論

各論では、国際協力を評価する際に考慮すべき事柄が以下の６つの観点から説明されている。

①　なぜ、どのように当該協力が行われるのか？

計画の段階において、協力の便益と期待される効果を評価する。具体的には、協力の狙いは明確か、相互の関係は資源の面でバランスが取れているか、研究は教育に統合されるのか、若手とシニアの両方の研究者が参加するのか、協力関係は弾力的かつ持続可能なものか、協力関係は透明性が担保されているか、について確認すること。具体的なチェック項目

・当該協力はなぜ実施され、短期的かつ長期的な効用は何か。
・資金の利用と学識においてバランスはとれているのか。
・協力関係の発展のための計画や目標はあるのか。

・事業の財源がどのように調達され、何を持って事業完成とするのか。
・財源の独立性、インテグリティ、倫理、学問の自由等におけるリスクはないのか。
・当該事業がもたらす好機と挑戦的課題を議論し、当事者間で共有されているか。
・当該事業の規模に相応しいレベルの責任者（学部長、学科長、学科研究部長など）が協議に参加しているか。

② どのレベルのどのような行為者が協力しているのか

大学の国際協力研究における最終責任は当該大学の管理下に置かれ、大学当局は当該事業に関して事前に以下のような事項を検討しなければならない。

・当該事業はどの機関のどのレベルの担当者の間で行われるのか。
・当該協力は大学で正式に承認され、認証されているのか。
・同様の協力をした経験はあるのか、ある場合それはどのように管理されたのか。
・公式の協定に署名してよいか。

③ パートナー国の政治的、社会的、文化的文脈

協力パートナーの出身国の政治的、社会的、文化的な文脈から生じ得る課題を考慮しなければならない。たとえば、研究対象、聞き取り対象者、あるいは研究者自身が迫害を受けている民族や少数派、あるいはその他の社会的弱者グループである場合には、事業計画を慎重に立てる必要があり、次のような点を考慮しなければならない。

・研究者とその所属大学等はパートナー国の政治的、社会的、文化的条件についての知識を一般的、あるいは当該事業との関連で持っているか。
・パートナー国の政治的、社会的、文化的文脈を全般的に理解するために、大学は組織的にどのような支援が提供できるか。

④ 法的文脈

デュアルユース（軍事と民事両方に利用できる）に関し、大量破壊兵器の不拡散に関する協定に基づき、特定の国家のグループや人物とは協力できないことがある。具体的には、次のような事項を考慮しなければならない。

・当該研究の結果が直ちにデュアルユースになるリスクはないか。
・事業の科学的内容が国際的制裁によって制約を受ける可能性はないか。
・知的財産権の保護を考慮する必要はないか。
・パートナー国のデータの保護と安全性の状況はどのようになっているのか。
・教育協力の場合、学生の管理と学位授与において現行のスウェーデンの法的枠組みと齟齬はないのか。

⑤ 組織の独立性

当該協力が及ぼす大学の学問の自由や評判への影響を評価する必要がある。この場合には専門家の分析を仰ぐのが望ましい。この問題に関しては、次のような項目を考慮しなけれ

ばならない。

・パートナー国の政府関係者が、当該分野で許容とみなされる範囲を超えて研究が取り上げる話題や内容、データ集積について介入してくることはないか。

・当該パートナーとの協力が研究者とその部署や大学の評判を貶めるリスクはないか。

・協力が当該大学自体の財政、組織及び学問の独立性に影響するようなことはないか。

⑥　倫理的観点

「倫理放棄（ethics dumping、強力な倫理規制のある国の研究者が規制のより弱い国の倫理規制によって実験や検査を実施すること）」に対する注意喚起(本題との関連性が希薄につき詳細は省略)。

(2)　「責任ある国際化によっていかに業務を遂行するかに関する高等教育機関への助言」（STINT 2022）

この助言は、カロリンスカ研究所、スウェーデン王立工科大学（KTH）及びルンド大学の協力の下、STINT によって発行された大学/研究機関に向けた文書である。２部構成となっており、第１部では、タイプの異なる３つの大学（KTH は理工系の単科大学、ルンドはスウェーデンではウプサラ大学に次いで歴史のある総合大学、エルブルー大学は 1977 年に創設された国内では新しい大学）と研究機関（カロリンスカ研究所）の４事例に基づいて、研究と教育の国際化によって生じる挑戦的な課題を抽出し、対応策を検討し、提示している。第２部は、国際的な共同研究や理工系留学生の多い KTH の事例に基づいて国際化によって直面する課題とそのアプローチを論じている。

a. 国際化に対する４タイプのアプローチ

本文書によると、国際化の度合いによって、大学のアプローチは大きく４つに分けることができるという。以下、その内容を簡単にみておこう。

タイプ A

まず、国際化が相対的に遅れ、挑戦的な課題に個人ベースで、アドホックに対応するタイプである。このタイプでは、国際化に伴う課題がリーダーに見え辛く、組織的なアプローチが難しい。したがって、他の大学の経験をケーススタディし、そこから学ぶのが現実的なアプローチである。

タイプ B

次に、高いレベルで国際化が進展し、それに伴って様々な問題にも直面している一方、責任ある国際化に向けた戦略的努力が不十分なタイプである。問題の発覚や経験が常に下部組織から立ち上がり、リーダーはそうした上がってくる問題に反応するだけの分散的アプローチ（decentralized approaches）に終始する。この分散型モデルは問題が起こった時に柔軟な対応が可能というメリットがある反面、デメリットは組織的な調整ができない点で

ある。そのため、責任ある国際化に関する議論がバラバラでまとまらない。個々の経験や最も深刻な問題の共有と理解を深め、また「優れた取組」を組織全体に広める必要がある。

タイプ C

３つ目が、経験が薄く、かつ国際化への注目が狭く、既存の国際協力に対する一定の洞察力はあるものの、それがより小さな一群に集中し、広がりを持たないタイプである。こうした経験の共有が狭いサークルに留まるタイプでは、リーダーが他の大学が遭遇した問題に影響される傾向にある。組織としてこうした問題を認識し、学内で共有することがなく、戦略と実践の間にギャップが生じやすい。したがって、このタイプでは、組織内外のスタッフ間の幅広い経験の交流を意識的に推進することが求められる。

タイプ D

幅広い経験があり、具体的な事例から効果的な対応を得ているタイプである。問題の全体像を把握し、責任ある国際化のための一体的な方向を導き出す指導力がある。しかし、トップダウンな手法ゆえに、リーダーと研究・教育スタッフの間の意識の乖離が生じ易い。また、膨大な経験ゆえに対応のルーティン化が進行する一方、ガイドライン通りに進めるなど官僚的、あるいは硬直的すぎるなどのデメリットも少なくない。

この中央集権型アプローチは、素早い対応能力を減退させ、さらに学問の自由の侵害の可能性も生じる。しかし、最も複雑な事例/問題は、こうしたより中央集権的な仕組みによって確定され、取り扱われるべきである。他方、グレーゾーンを取り扱うには、異なるレベルのスタッフがこの新しい課題について責任を持って対処できるような「責任ある国際化」の文化を醸成するようなアプローチを取るなど、このタイプでは事例ごとにケースバイケースの柔軟な対応が望まれる。

b. 責任ある国際化モデル

以上の事例研究を踏まえて、本文書は次のような 3 つのポイントからなる「将来を見据えたアプローチ」を提案する。

まず、参照拠点の創設である。国際化の問題について議論するグループを結成し、議論を深める。国際化が進む大学ではミックスグループで経験を議論し、共有する。国際化が遅れている大学は、他の大学の事例を使って、この問題の理解に努める。次に、知識の共有のためにスタッフを集め、それぞれの関連テーマ毎にプロジェクトを結成する。そして、３つ目がプロジェクトの成果を考察し、それらを接合する統合である。最後に、2020 年以来、スウェーデンの大学では責任ある国際化が考慮されるようになったが、組織的なアプローチはまだ十分ではないと、締め括られている。

(3) 「世界に責任を持つ関与：チェックリスト」(SUHF 2023)

「世界に責任ある関与：チェックリスト（以下、チェックリスト）」は、スウェーデン高等教育機関協会（The Association of Swedish Higher Education Institutions, SUHF)が、

国内の大学/研究機関向けに発行したものである。国際協力活動の開始前にパートナー研究機関（者）に関して検討すべき 6 項目を挙げ、事前の検討によってリスクを防ぐことを推奨している。以下、項目毎にチェックすべき事項を簡単にみておこう。

a. 民主主義の原則と厳格な学問の自由が守られているか

パートナー機関及び研究者の出身国は、人権侵害、学問の自由の侵害によって国連や EU による制裁の対象になっていないか。また、当該国の国家当局が研究内容や研究領域、あるいはデータ収集に関して影響力を行使しようとするリスクはないか。

b. パートナー機関（研究者）の評判と外部からの評価

パートナーになる研究者及び研究機関の倫理的基準もしくは外部評価が協力関係を持つことになったスウェーデンの研究者とその所属機関に倫理的ダメージを与えたり、評判（reputations）を損傷したりするリスクはないか。パートナー研究者はその帰属国家の政府や政党とどのような関係を持っているのか。当該プロジェクトやその活動が当該機関の最も重要な価値、理念と対立することはないか。

c. データの使用、知的財産権（IPR）、パテント権に関する対立

当該研究者とパートナー研究者は、使用前のデータへのアクセス、機密保持、研究成果の所有権、研究成果のパテントと商業化のための私的利用を含む IPR に関する理解を共有しているか。どのように適正なデータ保護を図るのか。

d. 研究の不正利用と意図的ではない悪意ある応用

大学や研究機関の相互訪問、共同プロジェクト、研究と教育協力が、直接的な誤解、不正利用、明らかに意図しないにもかかわらず悪用になるような成果応用などに巻き込まれることはないか。共同研究に軍事や防衛産業と深く関わるような人物、あるいは人権侵害をするような共同研究者を含んでいないか。

e. 倫理ダンピングと個人及び生物学的なデータに関する安全性

共同プロジェクトや研究協力が動物、ヒト、ヒトの組織、もしくは個人のデータの使用に関して重大な倫理的懸念が生じることはないか。必要に応じで、パートナー国及びスウエーデンの倫理審査当局による倫理的許可を獲得しているか。共同プロジェクトや研究協力には個人データあるいは個人データに基づく大規模な生物学的データを倫理的許可と適正なデータ移転に関する合意なしに使用する内容を含んでいないか。

f.　研究者個人の安全

共同研究や共同研究機関の代表者が法的であれ実際においてであれ、かれらの出身国において差別されたり、抑圧されたりするリスクはないか。訪問、プロジェクト参加、協力活動が、スタッフや博士院生、パートナーになっている同僚や学生を伝染病、テロの脅威、犯罪、汚職、諜報活動、情報の窃盗等のリスクに晒すことはないか。

2.8.4　スウェーデンの取組をめぐる考察

スカンジナビア諸国（スウェーデン、ノルウェー、デンマーク）の研究インテグリティと倫理における規制のあり方を比較した Knut Jørgen Vie (2022)は、規制の一般的アプローチを 3 つに区分して説明した。すなわち、研究者個人もしくは各研究機関の裁量に委ねられる自由放任、不正行為を犯罪と規定し、いかなる行動が違反に当たるのかを細かく定める法的取締り、そして自己規制を強力に要請する高次規制（meta-regulation）である。

高次規制は、当該行為者が自らの責任を理解し、それを果たすことによって、規制に取組むアプローチである。当局は行為者が自ら規範に従い得る手段を提供し、自己決定の権限を付与する。このアプローチは自由放任と法的取締りの間に位置付けられ、自己規制の領域と構造の理解と支持を高めるための訓練を通して、研究者への普及が促進される。

Vie (2022)によると、元来研究は複雑でダイナミックなため、規制が難しいとの認識の下、スウェーデンはこれら 3 つが混在するアプローチを採用している[168]。まず規制法によって、捏造、改竄、剽窃に関する最も深刻な違反を特定して、これらの違反が重大だと認定されると同法の規定に基づいて対処する。調査と認定は「国立研究不正行為評価委員会（Swedish National Board for Assessment of Research Misconduct）」が行う。委員会は、研究不正行為として告発されている事案を捜査し、捜査完了後は事案を当該研究機関に差し戻す。当該研究機関は、処分の決定とともに、事案に関係する学術誌や出資財団に報告を行わなければならない。委員会の関与は不正行為の有無の判断に限定されており、不正行為者の処分については関与できない。また、評価委員会の決定に不服がある場合には行政裁判所に上訴することができる。

一方、重大性の低い事案の処遇についての定めはなく、それは重大性の低い事案を法によって規制するのは限界があることが認識され、研究コミュニティの自主規制に委ねるのが最善だと考えられているからである。従って、大学・研究機関には、不正防止のための啓発の推進、研究倫理に関する議論の活発化、適正な研究のあり方の文書化とアーカイブ化、違反の速やかな発見と違反処理のためのシステムの構築（内部告発者保護を含む）、法に定められた不正行為に関する速やかな評価委員会への報告、法規違反以外の不正行為の処遇等に関する適正な体制と手続きの構築といった責務が生じる（Vie 2022）。

[168] Vie (2022)は、他の 2 カ国（ノルウエーとデンマーク）も同じく、3 つの混合アプローチだとしている。

研究者は業務上の自由度が著しく大きいので、個々人の道徳的判断に委ねざるを得ない面も少なくない。そのため、法に従うだけでは、責任を果たすに十分ではなく、研究遂行に関連する法律はもとより、行動規範についての知識を獲得し、所属研究機関が提供するトレーニングに参加する責務を負う（Vie 2022）。

「新たなリスク」への対応策は、近年の研究の国際化とオープン・サイエンスの潮流の中で、研究の開放性と透明性を担保すると同時に、研究者及び研究機関とその成果を保護するための管理が求められて登場するに至った（Vie 2022）。したがって、スウェーデンにおける一連の取組は、既存のインテグリティ・倫理に対する規制アプローチの延長線上に新たに付け加えられたものであり、その性質も既存のアプローチを継承し、研究者や大学・研究機関が責任を自覚するのを促し、自らリスクの防止と発見に努めるための知識と情報を提供することに主眼が置かれている。

事実、スウェーデンの取組をリードしてきたルンド大学の Shih 准教授は、ガイドライン、助言、チェックリストを通して、研究機関や研究者に国際協力において生じ得る挑戦的課題やリスクを周知し、認識を深めてもらうことが重要だと指摘している[169]。では、問題やリスクが認知された際に、誰がそれらを処理し、解決を図るのか。同じく Shih 准教授によると、リスクマネジメントはケースバイケースで、大学・研究機関もしくは資金配分機関が対応可能な問題についてはそれらが対応し、輸出管理や安全保障に関わる問題は所管の省庁に回され、担当省庁が法令に基づいて処理し、さらに不正や倫理に係る問題の場合には研究不正行為評価委員会に付託される[170]。

換言すれば、スウェーデンにおける「新たなリスクへの対応」策の鍵となる行為者は、大学・研究機関とそこに所属する研究者である。しかしながら、ガイドラインや助言、チェックリストへの対応は、個々の大学・研究機関に一任されており、カロリンスカ研究所や王立工科大学のように積極的な対応をとる組織がある一方、全く対応が図られていない大学も少なくない[171]。このように、取組にばらつきが生じてしまうのが、「ソフトな規制」（Vie 2022）の欠点の一つといえよう。

[169] 10 月 4 日（18:30～19:30）に筆者が Shih 准教授に行ったインタビューにおける動詞の発言に基づく。
[170] 出典は Tommy Shih 准教授のインタビュー中の発言による。
[171] 出典は Tommy Shih 准教授のインタビュー中の発言による。

2.9 ノルウェー

2.9.1 ノルウェーにおける「研究インテグリティ」に係る取組の特徴

ノルウェーにおける「研究のオープン化、国際化に伴う新たなリスクへの対応策（以下、新たなリスクへの対応策）」には、スウェーデン、フィンランドと同様「責任」という用語が用いられ、「責任ある国際協力（responsible international cooperation）」と呼ばれている。従来の研究不正等への対応は、研究倫理（research ethics）[172]である。

ノルウェーの取組は、外務省が「知識移転管理」のために大学・研究機関への規制を強化する「研究セキュリティ」を打ち出し、教育研究省がそれを踏まえて本課題についてのガイドラインを作成するという手順で進められてきた。つまり、大学・研究機関のための「新たなリスクへの対応策」は、外務省管轄の「安全保障輸出管理」の部分と位置付けられていると捉えることができる。

外務省の規制は、大学・研究機関が外国人について雇用、客員研究員身分での滞在許可、大学院への入学許可を行う場合には、事前に許可申請を行い、免許を得なければならない「事前免許制」を内容とし、免許を必要とする対象者の出身国は国連や EU など国際機関の被制裁国はもとより、ケースバイケースで判断される。

学問の自由に抵触することが懸念される事前免許制に、当然学界は反対した。しかしながら、学界自体の取組は積極性に欠け、教育研究省の委託によりノルウェー研究評議会（Norwegian Council of Universities, UHR）[173]と担当部局（Directorate for Higher Education and Skills, NH-dir）が策定したガイドラインは、外務省の「知識移転管理」規制と一体化した内容であった。同じ北欧諸国のスウェーデン、フィンランドに比べると、リスクの査定と管理を全面に打ち出した対応策だと言うことができる。

2.9.2 ノルウェーにおける取組の背景と経緯

ロシアと国境を接するノルウェーは伝統的にロシアの諜報・工作活動に注意を払ってきた。特に 2014 年のロシアによるクリミア併合後は、ロシアを対諜報活動の最前線に置いてきた。2022 年 2 月 24 日に始まったウクライナ侵攻後は、EU と歩調を合わせて、ロシア制裁を行っている。一方、中国については、2017 年頃までは他の北欧諸国と同様、良好な関係を築き、学術交流も活発であった。しかし、安全保障への懸念と人権問題がより重視されるようになり、中国も警戒対象国になった。2019 年 3 月に EU が中国を「体制的ライバル（a systemic rival）」と定義したのを受けて、ノルウェーは EU 非加盟国ではあるが、追随した（Forsby 2022）。

たとえば、2023 年版の「国家脅威査定」（ノルウェー治安サービス部、PST）は、注意す

[172] たとえば、National Committee for Research Ethics in the Social Sciences and the Humanities (NESH) (2021)を参照。
[173] UHR は、国内 32 の大学、大学内カレッジ、私立大学を代表する組織である。

べき国家について以下のように指摘する（Norwegian Ministry of Foreign Affairs 2021）。

「2023 年、ノルウェーは、大量破壊兵器とその他の軍事的開発のための外国の国家プログラムに関与する者が秘密裏に試みる設備と技術の入手行為を白日の下に晒す事業を開始した。ノルウェーの研究/教育機関は知識の不正な移転の餌食になることが予想される。ロシア、中国、イランおよびパキスタンには特別な注意が必要である。特にロシアと中国の行為者がノルウェーの国家利益に脅威を与えるか、否かについてさらなる査定を要す。

デジタル分野における最大の脅威になる行為者はロシアと中国であるが、イランと北朝鮮もノルウェーのコンピューター・ネットワークシステムに侵入しようとしている。しかし、ロシアや中国は、自前のネットワークを開発する能力を持ち始め、脅威が一段と増している。

研究分野における中国による常習的な諜報の脅威の古典的な手法の一つは、該当する個人と研究上の親密な関係を築くことである。まず、当該研究者を中国のシンクタンクの雑誌に高額な原稿料の論文を書いてほしいと誘うことから始まる。続いて、この研究者は中国で開催されるカンファレンスに全額中国持ちで招待される。関係構築は様ざまな機会を通じて続き、その最終的な目的は当該研究者の機微情報を共有することである。

新興テクノロジーを探求している大学や学部は諜報を行う国にとって魅力的なターゲットである。なかでも、中国はこの点における活発なアクターである。中国当局は、急速な軍隊の近代化を図るために私人の行為者を利用するという露骨な手法を用いる。民用技術を軍事部門に応用する、すなわち軍事にデュアルユースの価値を持ち込むことが中国諜報活動の最も重要な目的である。」

ノルウェーの主要な大学には 70 を超える国から 700 人以上の院生やポスドク、訪問研究員が滞在している（Norwegian Ministry of Foreign Affairs 2021）。ノルウェーの主要 4 大学の研究レベルは、QS 世界大学ランキング（2023 年）によると、世界 1500 大学中、オスロ大学 101 位、ベルゲン大学 207 位、ノルウェー科学工科大学 352 位、トロムソ北極大学 454 位と、トップレベルとは言えないまでも、高い水準を維持している[174]。しかし、ノルウェーの学術にとって重要なのは、大学の研究が軍事産業と深く結びついている点である。

200 年余りの歴史を持つノルウェーの軍事産業は、軍隊及びその関連事業者、軍事産業、そして学界の 3 者の協働によって発展を遂げてきた。その生産量の 80%がアメリカ合衆国を含む 50 カ国以上に輸出され、ノルウェーの基幹産業の一翼を担っている[175]。輸出先は

[174] 出典は、Rankings: The 8 best universities in Norway for 1024/1925https://www.study.eu/best-universities/norway, available at https://www.study.eu/best-universities/norway. QS 世界大学ランキングは、104 地点の 1500 大学について何千人もの学識者の評判に基づいて評価し、順位をつけたもので、世界で最も利用されている（https://www.topuniversities.com/qs-world-university-rankings 参照のこと）。

[175] 2022 年の武器輸出国別ランキング（Global Ecomomy.Com: Arms Exports, Country Ranking）によ

90%が NATO 加盟国や EU 諸国である。しかし、より重要な事業は、アメリカ合衆国が主導する「F-35 統合打撃戦闘機計画（F-35 Joint Strike Fighter Program）」[176]に参加し、先端複合部品、電気系統や機械部品の製造等に従事していることである（Svensgård 2022）。

軍事産業はノルウェーの国家プロジェクトの一つであり、またアメリカ合衆国との生産連携は研究の安全保障強化を動機づける。ノルウェーの「新たなリスクへの対応策」がより「研究セキュリティ」に傾き、知識移転を厳しく規制するのは、まさしくこのためだと考えられる。

2020 年 6 月、外務省は大学・研究機関における知識移転の規制強化を目的に、外国人の雇用と入学、研究滞在に対し「事前免許制」を導入すると発表し、10 月にはノルウェーの輸出管理規則の枠内において高等教育機関（大学）の外国人の入学許可や雇用を支援することを目的にした「知識移転管理のためのガイドライン Retningslinjer for kontroll med kunnskapsoverføring (Guidelines for control of knowledge transfer)」[177]を打ち出した。

2021 年 6 月 11 日、外務省は知識移転に関する輸出管理規則を内閣に提出し、承認を得た。2022 年 3 月、外務省は、事前免許制を盛り込んだ「知識移転管理規則」案を公表するとともに、同 28 日から 2022 年 6 月 22 日までを目処に大学・研究機関など学界に対し、本案に対する意見（public comments）を求めた。2022 年 12 月 20 日、学界からの意見を受けて、外務省は「知識移転管理 Kontroll av kunnskapsoverføring」規制の更新版を発表した。

一方、学界側は 2022 年 10 月 21 日に大学におけるガイドライン策定に向けたワークショップ「公平な研究協力関係の観点による責任ある国際協力のためのガイドラインの開発 (Developing Guidelines for Responsible International Cooperation Through the Lens of Equitable Research Partnerships)」[178]を開催した。この中で、ノルウェー研究評議会と研究・技能局が教育研究省の依頼を受けて、大学・研究機関の国際協力における機会、課題、葛藤をめぐる知識と注意の向上に資することを目的に「責任ある国際協力のためのガイドライン」を作成中であることを明らかにした。

そして、翌 2023 年夏に「責任ある国際知識協力のためのガイドラインとツール (Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid)」が完成し、同年 8 月 14 日に公開された。その数ヶ月後には英語版[179]がアップロードされた。

ると、ノルウェーは 19 位である。ちなみにスウェーデン 20 位、フィンランド 32 位である。出典：https://www.theglobaleconomy.com/rankings/arms_exports/.

176 本事業については Congressional Research Service 発刊の「F-35 Joint Strike Fighter (JSF) Program, May 2, 2022」（https://sgp.fas.org/crs/weapons/RL30563.pdf）を参照のこと。

177 Available at https://www.regjeringen.no/no/tema/utenrikssaker/Eksportkontroll/om-eksportkontroll/kunnskap/id2500543/

178 Available at https://www.forskningsradet.no/en/events/2022/guidelines-for-responsible-international-cooperation-equitable-research-partnerships/

179 ノルウェー語版は https://hkdir.no/retningslinjer-og-verktoy-for-ansvarlig-internasjonalt-kunnskapssamarbeid、英語版は https://hkdir.no/en/guidelines-and-tools-for-responsible-international-knowledge-cooperation よりアクセス可能。

2.9.3 ノルウェーにおける取組の詳細

上述のように、ノルウェーの取組は外務省が規制する「知識移転管理」が先行し、教育研究省のガイドラインはその枠組みを研究現場でどのように適用して、研究における国際協力で生じ得るリスクに対応するのか、その具体的な手法を提案する内容となっている。

(1) 外務省の「知識移転管理」の方針

a. 知識移転管理のための外務省ガイドライン

2020 年 10 月、外務省は 2015 年刊行のガイドラインを更新し、新たに「知識移転管理のためのガイドライン（Retningslinjer for kontroll med kunnskapsoverføring）、以下外務省ガイドライン」として発表した。以下では、外交白書英語概要版の中に「機微な知識移転の管理（Control of the transfer of sensitive knowledge）」[180]というタイトルで再掲されている文書に基づいて、この「知識移転管理」ガイドラインの概要を述べる。

① 目的

外務省ガイドラインによると、輸出管理の対象は機材、サービス、テクノロジー・技術であり、このテクノロジーには知識といった無形技術が含まれる。そのため、無形技術である知識を扱う大学等の教育機関が外国人の入学許可や雇用を行う場合、それらは輸出管理の対象になる。本ガイドラインは、「ノルウェーの輸出管理規則の枠内において教育機関が実施する外国人の入学許可や雇用を支援すること」を目的にしている。

大学が取り扱う知識の中でも特段の注意と配慮が必要なのは、「機微な sensitive」分野における外国人の入学や雇用である。機微な分野とは、大量破壊兵器やその運搬の開発、製造あるいは使用が可能なテクノロジーに関する知見を与えるようなより高度なレベルの研究、教育あるいは業務を指す。輸出管理規則は、あらゆるタイプの大量破壊兵器とその輸送手段、通常兵器に使用可能な設備や技術に関する知識を管理する権能を有する。従って、大学は、その研究・教育分野における「機微性の高さ」を査定し、それらが外国の学生、研究員、雇用者に移転されることがノルウェーの輸出管理規則に違反しないか、否かについて査定しなければならない。

さらに、輸出管理規則は、外国機関との共同研究、研究情報や成果の共有にも適用されるので、研究情報の発信や大学院課程のコース、学会なども査定の対象になる。

② 適用

本規則は、主に輸出制限下にある国及び大量破壊兵器やその輸送手段の開発の恐れが確実視される、もしくは疑われる国出身の学生の入学許可、ポスドク研究生や客員研究員の受入れ及び雇用の申請を処理する過程において適用される。

---

[180] Available at https://www.regjeringen.no/contentassets/570f97ec452d42b5913e690052413ac6/en-gb/pdfs/stm202020210035000engpdfs.pdf.

バイオテクノロジーを含む生命科学、生化学、化学生成技術を含む化学、核物理学を含む物理学、航空及び航空技術、機械工学、材料工学、サイバネティクス、医学・獣医学、数学の分野における博士候補生の受入れには特段の査定が必要である。

上記のリスト以外でも、外務省の項目リスト II で扱われ、よって大量破壊兵器とその輸送手段の拡大の恐れのあるテクノロジー領域については、博士及び修士課程の学生を受け入れるに当たって、大学は注意を怠ってはならない。

b.　外務省外国人研究者等受入れのための事前免許制

2022 年 3 月に、知識移転管理のためのガイドラインに学生の入学許可、ポスドク研究生や客員研究員の受入れ及び雇用における「事前免許制」が追加された。以下の説明は、ノルウェー科学工科大学のウェブサイトに掲載された英語版[181]による。

まず、輸出管理規則の対象になるのは、軍事目的の技術を含む防衛関連機材と民用を目的にしているが軍事に転用可能なデュアルユース機材の 2 つのカテゴリーで、学術分野での技術と知識は後者のデュアルユースに該当する場合が多いと述べ、本規則の目的、規制の方法である免許制、免許を必要とする対象者について順次説明されている。

① 目的

輸出管理規制の目的は、国際法とノルウェーの安全保障/防衛政策に違反する戦略的な機材、サービス及び技術の輸出禁止を確実に履行するとともに、ノルウェーの機材、サービス及び技術が大量破壊兵器拡散に寄与する可能性を阻止することにある。

「技術」には、知識のような無形技術が含まれるので、大学・研究機関（以下、大学等）の学術活動はこの規制が網羅する専門分野において機密性のある知識や技術を保有する。従って、大学等はその知識と技術の取り扱いに責任を持ち、外国人の雇用、特殊なコースへの外国人学生の入学、その他外国人の受入れや雇用による知識移転に関して輸出管理規則を遵守しなければならない。

② 事前許可（免許）制

機密性のある知識や技術に関する規則を遵守するために、大学は知識が外国人に移転される前に、外務省に事前の許可を得るための「免許」を申請しなければならない。特に、学術スタッフの募集、ポスドクや客員研究員の受入れ、大学院の入学にはこの規則に基づく審査が求められる。事前許可（免許）は必ず入学あるいは受入れ許可や雇用契約がサインされる前に得ておかなければならない。

③ 事前許可を要する対象者

当該人物が輸出管理規則に違反もしくは免許の申請が必要な国の出身者か否かについて、定められた固定的リストはない。被制裁国家はもとより、ケースバイケースで査定していく

181 Control of Knowledge Transfer, available at https://i.ntnu.no/wiki/-/wiki/English/Control+of+knowledge+transfer

必要がある。従って、候補者が所謂問題となる国の出身である場合、入学、受入れ、人事の手続きを遅滞させないためには、外務省の輸出管理担当者にできる限り早く連絡を取らなければならない。

(2) 教育研究省のガイドラインとツール

2023 年 8 月教育研究省は「責任ある国際知識協力のためのガイドラインとツール(Retningslinjer og verktøy for ansvarlig internasjonalt kunnskapssamarbeid)[182]以下教育研究省ガイドライン」を発表した。このガイドラインは、ノルウェーの研究・教育機関が遵守すべき法規の概説とともに、大学組織の指導部及び事務方が考慮すべき要点と手続きに焦点を当て、国際的学術協力におけるリスクを管理し、安全を強化するための手段を提示している。ここでは、その英語版「Guidelines and Tools for Responsible International Knowledge Cooperation」(Offerdal et al. 2023)を使用する。文書は、序、学術の価値と責任、大学等研究機関における安全保障管理、被用者と学生、研究と大学教育における協力関係と協定、国の責任と調整の６つの章から構成される。それぞれの課題の背景、関連法やガイドラインなどを説明した上で、考慮すべき事項を提起する。本稿では、「新たなリスクへの対応策」に特に関連した部分に的を絞って、その概要を記す。従って、最終章の「国の責任と調整」は関連する国の機関を紹介する内容であるため省略し、序から５章までを取り上げる。

a. 序

① 目的

教育研究省ガイドラインの目的は、国際的な知識協力に関する事業に対して考慮すべき点及び均衡の取れた協力関係を築くために必要な情報を提供するとともに、機関がそれぞれの事情に応じて、独自の計画を立てることができるように実務的な手法を提供することにある。しかし、ガイドラインが提示する事項は一般的な助言であり、各機関はその関心の範囲、価値あるいは資産、そして弱点を特定し、国際協力の協定の際には、リスクを認識し、注意を払わなければならない。

② ノルウェーの大学の現況

ノルウェーの大学が直面するであろう挑戦的課題（challenges）は他の多くの国とは異なっている。ノルウェーの大学は相対的に規模が小さい上、アメリカ合衆国、イギリスあるいはオーストラリアのように多数の外国人スタッフや学生の誘致を大々的に行なってはいない。他方、他の国に比べて自律性がより高く、広範な自由を享受するが、その反面責任も大きい。

---

[182] Available at https://hkdir.no/retningslinjer-og-verktoy-for-ansvarlig-internasjonalt-kunnskapssamarbeid.

大学の研究・教育の国際化においては、挑戦的課題に関するより多くの知識が必要である。

b.　学術の価値と責任

① 学問の自由の保護と侵害

ノルウェーの大学の学問の自由と責任は、大学及び大学カレッジ法の 1-5 項（Section 1-5 of the Act relating Universities and University Colleges）によって規制されている。同法は、大学等が学問の自由を推進し、保護するとともに、研究開発の結果の透明性の確保に努める旨を規定する。ノルウェーでは学問の自由が法律によって強力に保護されているが、それは絶対的なものではなく、医療研究法、生命工学法、政府職員法など複数の法律による制約はある。

学問の自由は国際的にも保護されなければならない。国際協力においては、たとえばジェンダーやセクシュアリティ、民族的少数派、国境や地政学的定義をめぐる問題などで自由が侵害される事例がみられる。

② 大学等が学問の自由の侵害を取扱い、管理するための査定項目

・戦略、計画や規則を通して学問の自由の保護と推進を組織的に行っているか。
・スタッフや学生、訪問研究員の間に、また課程やセミナーにおいて学問の自由に関する知識と自覚を高めるための責任を果たしているか。
・学問の自由の侵害や脅威を見つけ出すためのシステムを構築しているか。
・国際協力の協定を結ぶ際に考慮すべき項目
  * 研究資金が望ましくない関係を導くリスクはないか。
  * 他国の非学術的行為者が許容範囲を超えるような影響力を研究や教育に行使するリスクはないか。
  * 学問の自由が協定文書の中に明示されているか。
  * 協定文書に学問の自由を保障する条件が明示されているか。
  * 学問の自由の侵害が確認された際に、いつ、どのように協力関係を終了するかについて具体的な手続きが準備されているか。

③ 国際協力の学術環境に関して考慮すべき事項

・当該プロジェクトにおける学問の自由の意味を協力パートナーと議論しなさい。
・協力パートナーの母国における学問の自由の枠組み条件についてよく知っているか、確認しなさい。
・パートナー側の学問の自由への制約が協力関係に与える影響を考慮しなさい。
・学問の自由の枠組み条件を協定文書の出発点に置いているか、確認しなさい。
・資金等に関する事柄が学問の自由に影響する可能性を考慮に入れなさい。
・研究の枠組みに影響する資金等についての透明性を担保しなさい。

④ 研究倫理法

ノルウェーの大学の研究倫理は「研究倫理組織法（Act on the Organisation of Research Ethics, or Research Ethics Act）」によって統制され、大学等に以下の事項の実施を要請している。

・当該組織の研究は、承認された研究倫理に従って実施されているか、確認すること。
・学位候補者と被用者に研究倫理について訓練を実施すること。
・全ての研究従事者が研究倫理の規範を習熟していること。
・研究倫理規範に違反する可能性のあるあらゆるケースを考慮すること。
・こうした違反ケースに対処するためのガイドラインを有していること。
・不正行為について検討する委員会を任命すること。
・深刻な違反の可能性がある場合は「国立研究不正調査委員会(National Commission for the Investigation of Research Misconduct)」に報告しなさい。

⑤ 国立研究倫理委員会（the National Research Ethics Committee）ガイドライン

当ガイドラインは、以下のような基本項目からなる。

・研究参加者は、情報提供者等と同様に尊厳を持って扱われなければならない。
・研究者は自らの行為が良い結果を生むように、また悪い結果であっても、それが受容可能な範囲に止まるように行動しなければならない。
・全ての研究プロジェクトは公正に設計され、実施されなければならない。
・研究者は認証された規範に従い、かれらの同僚や公衆に対して責任を持ち、開かれ、真摯に行動しなければならない。

⑥ 大学組織の管理と運営のための査定事項

・研究インテグリティと倫理のためのガイドライン、システム、そして手続きは当該組織のウェブサイトで容易に閲覧できるか。
・学期中および組織内部において研究倫理ガイドラインに関するより多くの訓練機会を提供できているか。
・疑われる研究倫理規範違反を処理するための有効な装置を組織内部に確立しているか。
・研究の遂行、資金、専門家の査読、評価、協力に関する利害上の不公平及び対立を明らかにできるような手続きが確立されているか。
・研究の公表と普及のための手続きが明記されているか。

⑦ 研究環境にける査定事項

・研究プロジェクトの倫理的査定は関連するガイドラインや規則に従っているか。
・協力当事国間の認識や立法の相違を避けるために、研究倫理の問題について事前協議を行なっているか。
・研究実施者やプロジェクト参加者全員が認証された研究倫理規範に習熟しているか。
・当該研究に付随もしくはそれによって引き起こされる被用者の健康と安全、そして社会と

環境に対する影響を考えなさい。
・研究から生じる可能性のある潜在的損害とリスクを考えなさい。

⑧ 研究のオープン化と共有

研究のオープン化においては、研究過程は開放と知識の共有によって特徴づけられ、以下のような項目への考慮が求められる。
・データ管理に関するガイダンスと訓練が必要か、また実施においては規則や適用可能な行動規範に従うべきか、さらに可能なシステムやインフラがあるのか、考えなさい。
・大学は、オープンアクセスの出版とデータ管理に関する業務のための学術環境をどのように支援できるのかを考えなさい。
・開放性には異なる観点が含まれる。国家の安全保障利益、データ保護、法的課題、あるいは競争のような比較衡量すべき状況において、規則に関する枠組みに従って、いかに可能な限りベストな方法で対応できるのかを考えなさい。

c.　大学等研究機関における安全保障管理

責任ある国際知識協力の業務は大学の安全保障管理構造に連結され、そのリスクマネジメント全体の一部を構成する。従って、教育研究省所管の大学には、国家安全保障法(Security Act)、関連事業者安全保障規則（Security of Undertakings Regulations）、市民保護と緊急対応に関する省業務のための指示書（Instructions for the Ministries' work on civil protection and emergency preparedness）等の関連法が適用され、これらが規定する安全保障管理対策を遵守しなければならない。

① 安全保障管理において大学が査定すべき事項
・国際的な接触と活動においてリスクに晒される可能性がある、あるいは保護されるべき資産やインフラを特定できているか。
・国際的接触と活動に関連する異なるタイプのリスクを特定し、対処するシステムと手続きを構築しているか。
・特定されたリスクを軽減するための安全保障対処法について考慮しているか。
・リスクと脆弱性分析（Risk and Vulnerability Analyses, RVA）が適用される国際協力並びに被用者と学生の移動は存在しないか。
・当該機関の緊急対応計画が適用される国際的活動ではないのか。
・当該機関において、海外との協力関係、合意、資金流入、共同事業、データの安全性、外国人の雇用者や学生の入学、訪問研究員の受入れなどの経験はないか。
・国際的業務のリスクマネジメントに関する責任と役割を定義できているか。
・上記事項を実施するためのガイドラインもしくはその他の資源があるか。
・学生、教員、事務職員が問題を共有しているか。

② 情報の安全保障

大学は、教育研究省が定める「高等教育機関における情報の安全保障とデータ保護」の方針に従って、情報の安全保障に努めなければならない。

③ 知識移転の輸出管理における推奨事項

・どの知識分野が輸出管理規則によって網羅されるのか概要を把握しなさい。
・どのような国際協力活動、教育課程やポストに輸出管理規則が適用されるのか概要を把握しなさい。
・どの機材、実験施設、情報が輸出管理において追加的保護の対象になり、またこれらの資産を保護するための安全システムを開発するための対象になるのかを確定しなさい。
・機微な対象領域に関する知識移転管理を確実に行うための内部手続きを開発しなさい。

④ 知識移転管理に組織的に対応するための査定事項

・輸出管理を当該機関のリスクマネジメントの一部として取り入れ、これに責任を持つ専門的な人材を任命しなさい。ただし、当該機関の安全保障業務は管理者が担保するものでなければならない。
・研究分野の（リスク）評価は、規則を遵守するための安全保障手続きに基づいて作られるが、輸出管理規則が適用される研究機関の価値と資産の範囲は当該分野の行政的支援と管理システムと調和したものでなければならない。
・知識を扱う機関（大学等）は、国際的知識協力に制約が課される被制裁国の概要を把握しなければならない。なお、イラン国籍の者、対イラン制裁及び制限措置に関する規則（regulations on sanctions and restrictive measures against Iran)に列挙されているイラン製の機材・技術・知識に関係する人物については「事前許可」が適用されなければならない。
・輸出管理規則が対象とする分野の雇用では、標準化された経歴審査の導入を考えなさい。
・より広範な権限、権利、アクセス権を持つポストについては定期的な経歴審査による認証を行うべきか、考えなさい。
・違法な知識移転あるいはその可能性のある行為を感知した場合には、ノルウェー治安サービス部（PST）に連絡しなさい。

⑤ 学術環境に関する査定事項

・当該研究分野は輸出管理規則が網羅する知識領域に列記されてはいないか。
・研究、教育あるいは国際的プロジェクト協力が輸出管理規則のリスト II すなわちデュアルユース可能な実験、技術及び機材を使って行われていないか。
・国際協力によって開発される知識が軍事に適用される可能性はないか。
・計画中の知識協力への参加国は制裁リストに列挙されている国ではないか。協力がもたらす（負の）含意を考慮しなさい。

d. 被用者と学生

法に基づく外国人の雇用における経歴審査は雇用者の責任である。機関あるいは雇用責任者が当該人物に関してどのような情報を収集すべきかについては、資格要件とその他の法的もしくは契約上の要件を含む当該ポストの性質による。

経歴審査は、身分証の審査、学歴と職歴の照合、信用審査、商取引についての関心から構成される。経歴審査に際しては、被審査者に事前に説明を行い、書面にて了解を得ておく必要がある。

① 雇用と任命における査定事項

・いずれのポストや分野が経歴審査を必要とするのかを考えなさい。
・関連する法規に従った手続きを標準化するための経歴審査手続きシステムを整備しなさい。
・満足できる経歴審査を行うための情報が不足している場合には、志願者と学術課題について深く議論をするのが助けになる。書誌情報を使って経歴の虚偽の確認もできる。
・雇用に先立ち、志願者には輸出管理規則がかれらの専門性の向上と仕事に影響する旨を伝えるのが望ましい。知識移転のための輸出管理規則が網羅する専門分野には特にこれが当てはまる。雇用契約の中に独立条項としてこの留保条件を加えることを考えても良い。

② 被用者保護

新しく雇用した被用者には、輸出管理規則、研究倫理、学問の自由についての理解を促す特別な措置を取ることなど、かれらを保護するための手続きを整備しなさい。

③ 雇用者の責任の査定事項

・生じ得る利害の対立と脆弱性に気づくように、異なる機関や部門で業務を行う被用者を登録し、誰が外部のどこで、どのような仕事をしているかが一目でわかるような地図を作成しておくことを考えなさい。
・研究と教育の国際協力における兼業の潜在的な影響を協力事業の計画と実施において査定するための手続きを確立しなさい。

④ 兼業、外部機関との緊密な関係、資金関係が当該研究や教育活動に悪影響を及ぼしたり、雇用関係の忠誠心に関わる対立を生み出したりしないかを考えなさい。

・学術的業務が耐え難い圧力にさらされた時には、直接の上司、安全保障担当者、あるいは機関のインテグリティ委員会に連絡しなさい。
・部外者と共有しても良いかどうか確証のない情報を共有して欲しいと外部の行為者に頼まれた場合には、当該機関の安全保障管理者か、可能であれば PST の担当管に連絡しなさい。
・外国旅行やその他の状況で圧力を感じるような経験をした場合には、直接の上司や安全保

障担当者に連絡をして助言や支援を受けなさい。
・研究パートナーや訪問研究員、研究協力者が非倫理的な行為をしていると疑いを持ったら、直接の上司、安全保障担当者あるいはインテグリティ委員会に連絡しなさい。

⑤ 研究者の招聘と保護措置に関する査定事項
・当該機関の訪問研究員について概要を把握する必要性を考慮しなさい。
・訪問研究員の物理的かつ電子的アクセスに関するアクセス規則を考えなさい。

⑥ 被用者の渡航
被用者の海外渡航について雇用者は責任を負う。そのために、当該機関は内部手続きを整備して、被用者が常にどこにいるのか、その大まかな所在を把握する手続きを確立し、必要時には支援できるようにすべきである。ノルウェーが安全政策協力関係を結んでいない国を旅行する被用者は持参する電子機器に注意が必要である。たとえば予備の携帯電話を持参するのも良い。

⑦ 学生の渡航
・ジェンダー、肌の色、性的指向性、脆弱な少数派などの属性に関連する安全上の挑戦的課題を懸念したことはないか、確認しなさい。
・個人情報を第三国に渡す時にはその情報の保護に万全を期しなさい。
・渡航国に関する十分な情報を獲得し、滞在先で必要な安全策を確実に理解し、学びなさい。同行者がいる場合にはかれらの安全についても万全を期しなさい。
・個人的安全と情報の安全が脅かされたり、学術的価値に敵対したりするような事件に遭遇した場合の報告手続きを確立しなさい。
・海外の受入れ機関における連絡先を明確にしなさい。
・外務省の旅行アプリ「Reiseklar」に登録することを学生に推奨しなさい。
・学生に保険の持参、「ノルウェー在外学生協会 Association of Norwegian Student Abroad」への加入及び会員証の持参を推奨しなさい。

⑧ 学生の保護
・学生に自らの意見を表明する自由のための必要条件、研究倫理原則を教えなさい。
・学生が圧力や監視に晒された場合に、助けや支援を求めることのできる機関の明示的な連絡先を構築しなさい。

e.　研究と大学教育における協力関係と協定

① 研究協力における査定事項
・協定書には当該協力が長期か、短期かを明記されているか。
・学術スタッフが当該事業において同等な協力関係を発展させるような組織的支援が構築

されているか。
・財源、会計手続き、報告、雇用、そして規則について相互理解ができるようにパートナー機関の事務スタッフと協力しなさい。
・協力パートナーとその国家、諜報機関そして軍隊との連携と結びつきの可能性を調べなさい。
・協力パートナーのリスク調査（たとえば、行動、その所属組織が運営する事業セクター、業務を所有する会社の分類など）を実行しなさい。
・自らの価値、資産、安全そして評判へのリスクを査定するに足りる情報を確実に収集しなさい。この情報には共有的情報、個人情報、知的財産権に関するパートナー国の法規が含まれる。
・パートナーのノルウェーの機関への滞在は、当該機関の研究者や学生に対して、自然環境、社会あるいは政治に関わる何らかの特別なリスクを含んではいないか、考えなさい。
・パートナー国への研究滞在では、居住許可証、ビザなど滞在許可が必要か。
・当該プロジェクトに潜在するリスクの広がりを考えなさい。リスクは単に責任ある国際協力に止まらず、すべての学術的かつ事務的なリスクへと拡張するのか、考慮する必要がある。
・学問の自由のような価値が協定合意に含まれるのかを考えなさい。

② 研究者と学術環境における査定事項
・協力方法の発展に可能な限り時間を費やせるように、できるだけ早く計画立案を始めなさい。研究資金とそれぞれの機関が負担する費用を公平に分担すること。資金準備の際にはパートナー側組織の費用見積りとその算出方法について尋ねなさい。
・合意（書）の文言に不正確さを招くような文化的違いはないか。
・デュアルユースの可能性を考えなさい。
・成果物の商業利用の機会を確認しなさい。
・知的財産権に関連する戦略が必要とされていないかを判断しなさい。他国ではパテントの開発が明確な政治的目標になる。パテントは具体的なアイデアについて有限の保護を必要とし、アイデアの複製が簡単なほどパテント権が侵害されやすくなる。パテントを申請する際には、パートナーによる権利侵害に備えて裁判で自らのパテント権を守る準備をしたほうが良い。

③ 高等教育分野における協力関係
・協力の目的を定義しなさい。
  * なぜ協力パートナーにこの国を選んだのか。
  * なぜパートナーはこの人物でなければならなかったのか。
・パートナーは認定された高等教育機関で学位を授与されているか。
・当該教育協力はノルウェーの単位認定枠組みと互換性があるか。学年歴はどのようになっているかなど、パートナー国と機関の教育システムを確認しなさい。

④ 合意における査定事項

・特別な事情がない限り、合意は公開されなければならない。
・合意に含まれるべき事項には、パートナーの定義、協力の目的とゴール、財源、スケジュール、設備・インフラ・ソフトウエア・IT へのアクセス権、フォローアップ体制、予定される知的財産権の定義と合意、非公開事項、論文等の発行ルールなどが含まれる。

f. 国の責任と調整

関連する国の機関の列挙と説明（省略）

(3) 教育研究省「研究と高等教育長期計画 2023-2032 Long-Term Plan for Research and Higher Education: 2023-2032」[183]

本計画の中では「安全」という項目が設けられ、ロシアの対ウクライナ戦争、台頭する中国が引き起こす地政学的課題など研究・教育においてもさまざまなレベルにおいて安全について検討しなければならないと注意喚起されている。

2.9.4 ノルウェーの取組に関する考察

大学の人事に介入する外務省「事前免許制」は、学問の自由の侵害が懸念されるアプローチである。外務省が 2022 年 3 月事前免許制を導入するための「知識移転管理規則」改正案を提起した際には、ノルウェーの学界からは当然批判の声が上がった。2022 年 7 月 18 日付けの「大学世界ニュース」の Jan Petter Myklebust (2022)によると、外務省が学界に対し本改正案へのパブリックコメントを求めたのに対し、ノルウェー大学評議会（UHR）に加え、個別大学、研究機関、その他の利害関係者など 34 の組織と個人から意見が出された。学界からは、「輸出管理規制の必要性は認めるが、改正案は国家安全保障に比重がかかりすぎており、学問の自由が犠牲にされ、既存の大学法とも対立する」、「ノルウェーの研究水準を後退させ、大学教育と研究における国際化に負の影響をもたらす」などの意見が出された。

外務省に提出した意見書の中で、UHR は「提案は、学問の自由の侵害に加え、国際協力と開かれた研究への挑戦である。ノルウェーのような研究集中型の国にとって、国際協力は決定的に重要で、イノベーションと競争力の向上にとって目指すべきゴールである。研究の国際協力は、ノルウェーの研究を改善し、事業、ネットワーク、インフラ、そして市場への接近力向上に貢献する」と述べ、規制が他の国に比べて強すぎると重要かつ幅広い研究領域において競争力が弱まるとの懸念を表明した（Myklebust 2022）。さらに、

183 https://www.regjeringen.no/contentassets/9531df97616e4d8eabd7a820ba5380a9/en-gb/pdfs/stm202220230005000engpdfs.pdf.

「政府にはノルウェーを含む欧州の方が他の国よりも進んでいるという誤った偏見があり、非民主主義国家の中には研究と競争力において欧州よりも進んだ国もある」と述べ、闇雲にこうした国家との研究協力を遮断する姿勢を暗に批判した（Myklebust 2022）。

オスロ大学学長の Svein Stølen 教授も、「外務省は科学者のアイデアを管理し、その提案はノルウェーの研究を他国と共有するのを阻止するものだ」と指摘し、「ノルウェーの研究はやがて孤立し、場外に出されてしまう」と研究の後退を危惧する（Myklebust 2022）。

ノルウェーでは、2021 年 9 月の総選挙で右派連合が敗れ、8 年ぶりに政権交代があった。同年 10 月に労働党のヨナス＝ガール・ストーレを首相とする労働党と中央党の連立政権が発足した。すなわち、2020 年に外務省が知識移転管理の規制強化と「事前免許制」の導入を提案した当時は保守党を中心とする右派が政権を担っていたが、提案が議論の俎上に載ったのは左派中道政権になってからである。従って、この知識移転管理規制が政治的イデオロギーと連動したものではないことは明らかであろう。野党のうち、右派の進歩党は賛成、リベラル左派の自由党と緑の党は「重要な問題なので議会で議論すべき」との見解であり、必ずしも反対を表明しているわけではなかった（Myklebust 2022）。

一方、知識移転管理に対する学界の取組への批判もある。2022 年 11 月 19 日付けの「サイエンスノルウェー」において当誌記者の Siw Ellen Jakobsen は、「諜報の専門家がノルウェーの学界はスパイ活動にもっと警戒すべきであり」、「大学は訪問研究員の経歴調査を改善しなければならない」旨の記事を寄稿した(Jakobsen 2022)。Jakobsen によると、同年 10 月、北極大学で市民防衛とハイブリッド戦争を研究していた訪問研究員がスパイ行為により PST に告訴された。当該研究員はロシアのスパイで、ノルウェー北部地域政策に関するネットワークと情報を盗んだとみられている（Jakobsen 2022）。

Jakobsen は、ノルウェーの大学にはこうした訪問研究員の経歴を常時審査する仕組みがなく、経歴審査の改善を速やかに行うべきだとの専門家の意見を紹介している。この専門家の見解では「安全保障審査 security assessment」は広範で複雑なプロセスから構成される「機密取扱者適格性審査 security clearance」とは異なり、前者は当該人物の専門性や所属先を丁寧に審査するといった事項で足りるという。事実、この告訴された訪問研究員は修士号すら取得していなかった（Jakobsen 2022）。経歴調査をきちんと行なっていれば、事件は未然に防ぐことができたかもしれないのである。

外務省がパブリックコメントを募集したのは 2022 年 3 月～6 月であったので、このスパイ事件はその後に発覚したことになる。事件がどの程度学界に衝撃を与えたかは定かではない。しかし、事件の翌年の 8 月に発刊された教育研究省のガイドラインは、知識移転管理規則の方針と歩調を揃えた研究における安全保障の脅威への備えを打ち出した内容であった。スパイ活動を目の当たりにしたことが学界の考え方に影響していないとは言えない。また、すでに指摘したように、軍事産業に大学の研究が深く関与し、産学連携が確立していることも、学問の自由よりも研究の安全保障を優先せざるを得ない要因の一つと考えられる。

とはいえ、教育研究省のガイドラインは第 1 章の「学術の価値と責任」において学問の

自由を取り上げ、その価値を保護し、かつ推進することの重要性を詳細に議論し、ガイドラインが安全保障のために学問の自由を侵害するものでは必ずしもないという観点を強調する。この点は、学界の懸念やガイドライン作成に関与した学界関係者に配慮した結果でもあろう。

同じく北欧のスウェーデンとフィンランドの「新たなリスクへの対応策」には、「好機 opportunities と挑戦 challenges」という鍵となる言葉が用いられ、国際協力はリスクもあるが国内の研究を発展させるチャンスだという考え方をとっていた。教育研究省のガイドラインでは「好機」という用語は文中で 8 回使われてはいたが、スウェーデンとフィンランドのように、キーワードあるいは対策の方針ではない。この点にも、融和よりも「安全保障」を優先するノルウェーの取組の志向性が示されていよう。

2.10　フィンランド

2.10.1　フィンランドにおける「研究インテグリティ」に係る取組の特徴

フィンランドの科学技術の発展に中国は不可欠との認識のもと、同国は中国との学術交流を積極的に進めてきた。しかしながら、2019 年以降の EU の対政策の新方針（「a systemic rival」）により、その見直しを迫られた。とはいえ、ライデン大学アジアセンターの Ingrid d'Hoogle と Jonas Lammertink は、知識移転保護措置など厳格なリスク対応策が構築されていないことから、「リスク認識の欠如がいまだフィンランドの国としての対応を形作る主要なファクターである」（D'Hoogle and Lammertink 2022）と指摘している。

フィンランドの「研究のオープン化、国際化に伴う新たなリスクへの対応（以下、新たなリスクへの対応）」は、同国にとって最も重要な国際研究協力のカウンターパートである中国に的を絞った対中研究協力対策として進められてきた。同じ北欧諸国であるスウェーデン、ノルウェーと同様「責任ある responsible」がキーワードであるが、その取組は後塵を拝する。スウェーデンのような体系的な対応が構築されていない一方、安全保障輸出管理と一体化した厳格な知識移転規制を敷くノルウェーに比べるとかなり温和な対策に留まる。

しかしながら、対中研究協力について議論するインフォーマルかつボトムアップな「中国ラウンドテーブル」と称される官民一体となった問題解決組織が制度を補い、フィンランドの取組を特徴づけている（ D'Hoogle and Lammertink 2022）。ラウンドテーブルは、元々はフィンランド科学評議員中国担当（Finish Science Councilor for China）の傘下に組織され、教育文化省と外務省が主催し、中国担当評議員が推進を主導してきた。ところが、次第に大学の国際部門の代表や中国研究者から構成されるインフォーマルで開放的な組織に形を変え、ボトムアップに機能するようになった。テーマ別に ５つのワーキンググループに分かれて議論を積み上げ、政府（教育文化省）の対策づくりに現場の中国研究や関連事業の関係者（研究者や研究機関、企業関係者、法律家）が意見や考えを反映したり、かれらの疑問や問題を政府が受け取り、解答や解決策を示したりする場に発展した。

警戒しつつも、中国がもたらすメリットを考慮して良好な関係も維持するバランス志向がフィンランドの対中関係の基本姿勢である。

2.10.2　フィンランドにおける取組の背景と経緯

フィンランドは 19 世紀初頭から 1917 年の独立までロシアの支配下にあり、しかもロシアとは 1,340 キロに渡って国境を接する。したがって、ロシアを潜在的な脅威とみなし、警戒を維持する一方、過度に刺激することなく、慎重な対ロ外交に努め、そのため NATO にも加盟してこなかった。しかし、ロシアのウクライナ侵攻によって状況は一変、2023 年に NATO 加盟を果たした（Pillai 2022）。

複雑なロシア関係とは異なり、中国は友好国として経済的結びつきを強めてきた。学術交流も盛んになり、中国はフィンランドの科学技術分野の発展に極めて重要な位置を占める

ようになった。2017 年には習近平がフィンランドを訪問し、両国は「未来志向の新しい形の両国協力関係 future-oriented new-type cooperative partnership」に調印した。国内では、メディアや世論の間から中国の人権問題や抑圧的政治を批判する動きが高まったが、政府は経済と政治を切り離し、友好関係を維持した（Karppanen 2022)。ところが、2019 年欧州委員会が中国戦略文書（China Strategy Paper）において中国を「体制的ライバル a systemic rival」、すなわち経済的競争相手であり、ヨーロッパ的価値とは相容れない統治体制の国家だと定義して対中警戒を表明した（European Commission 2019)。そのため、加盟国であるフィンランドも方向転換を迫られることになった。

2021 年、フィンランド外務省は「政府対中アクションプラン Governmental Action Plan on China」発表し、翌 2022 年 3 月、教育文化省が「中国との学術協力のための勧告 Recommendations for academic cooperation with China, Ministry of Education and Culture」を発表した。

2022 年、フィンランド国内唯一の孔子学院が中国政府のプロパガンダに使われているとして閉鎖された（D'Hoogle and Lammertink 2022)。

しかし、他方で、大学教育における中国への依存は高く、たとえばヘルシンキから約 200 メートル東に位置するラッペーンランタ市にあるラッペーンランタ大学（LUT）のラハティキャンパスは、その学部学生の大部分と教員の約半数を中国出身者が占め、中国抜きでは教育活動が危ぶまれる状況にある(YLE NEWS 2021)。中国との研究・教育における協力関係の悪化は、フィンランドの大学の存続さえも揺るがす重大な問題を内包している。

2.10.3　フィンランドにおける取組の詳細

(1)　外務省の方針：「政府対中アクションプラン（以下プラン）」2021 年（Ministry of Foreign Affairs, 2021）

a. 概要

本プランは、「最善の場合のシナリオでは、中国の発展がフィンランドの競争力を高める」ことを前提に、中国との協力、意義、将来の方向性について精査することを目的にしている。しかしながら、フィンランドは EU メンバー国として EU の対中基本理念と歩調を合わせなければならないため、フィンランドの対中国関係は協力のみならず、競合と体制的ライバル（systemic rivalry）の次元からのアプローチの必要性も強調する。なかでも、フィンランドの中国に対する懸念事項は人権問題であり、「フィンランドの外交と安全保障政策は人権に基礎づけられ、その意味するところは、外交・安全保障政策の評価を人権への影響という観点から行うことであり、中国の人権状況の進展を注意深く監視しなければならない」と記す。

まず全般的な対中関係の検証ののち、環境・気候、食糧・天然資源、教育・研究・イノベーション、福祉・健康、司法・安全保障、文化・メディア・スポーツの個別分野について検

討するという構成になっている。ここでは、本報告書のテーマである「教育・研究・イノベーション」に絞って概要を紹介しよう。

b. 各論：教育・研究・イノベーション

教育・研究・イノベーション分野の対中協力については次のような大きく３つの観点を打ち出す。

① 対中協力の可能性

・フィンランドは、中国における教育、研究、技術革新の発展を注視し、協力関係を築き、中国が先導する技術的専門知識のフィンランドへの移転を推進する。
・科学技術に関する２カ国間協力では、国力と国益に基づく部門間の協力を推進する一方、フィンランド企業の知財とイノベーションを保護するためサイバーセキュリティの向上も重視する。
・高等教育と研究における対中協力のレベルを一層引き上げる。特に、大学の応用科学分野における協力と教員の訓練は将来的に有用な機会をもたらす可能性が高く、その研究及び教育協力を支援する。

② 対中協力における注意点

・対中協力は次のような制約を伴う。オープンサイエンス原則の制約、中国の工作活動による研究遂行上の制約、知的財産権（IPR）に関するデータ利用への制約、情報ネットワークへの制約などである。
・対中関係では、諜報のリスクとテクノロジーのスーパーパワー間の競争に備えることが肝要であり、学術とヨーロッパ的価値についての原則及び実践を堅持した上で、協力する必要がある。
・研究開発とイノベーションの協力においては両者が恩恵を共有し合う互恵主義と公平性を担保しなければならない。
・中国のテクノロジーにおける先進性や研究協力への資金力、そしてその商業市場としての重要性は、協力の活発化を推進させる一方、研究協力の成果と技術移転が世界における中国の立ち位置を有利にすることを認識しなければならない。
・最先端の機微な分野における協力は、他の国との協力機会を制約する可能性がある。

③ 対中協力のスタンス

・フィンランドの対中基本姿勢は、フィンランドの利益、目標、価値に基づいて、引き続き協力関係を維持することである。
・チームフィンランド−中国ネットワーク（Team Finland China network）[184]を通してフ

[184] チームフィンランドとは政府が同国企業などの海外活動を支援するために創設した関係機関（者）のネットワークで、特に中国ネットワークは、特に中国で活動するフィンランドの企業や団体の支援にあた

ィンランドの対中ノウハウを高める。
・中国の重要性が高まるにつれ、様々な部門における中国関連の知見を強化する必要性も増す。したがって、中国語や中国社会に関する専門家の育成のための長期的投資が求められる。

以上のように、外務省の「政府対中アクションプラン」は中国をフィンランドの研究開発にとって重要なパートナーと位置づけ、協力関係を今後も発展させていくという方針を確認するものである。対中協力によって生じ得るリスクへの警戒は示されてはいるが、協力への希求性が上回る。

(2) 教育文化省の方針:「中国との学術協力のための勧告、以下勧告」2022 年 3 月（Ministry of Education and Culture 2022）

a. 総論

教育文化省の「勧告」は、上記の外務省「プラン」の基本方針に沿って作成されている。したがって、ここでも「システムや文化が異なるものの、中国との協力は学術組織にとっても、また一般社会にも利益がある」ので、中国を重要な国際的パートナーと位置付ける。すなわち、「勧告」は、フィンランドの高等教育機関及び研究機関がかれら自身の原則と価値に基づいて中国のパートナーとの研究協力に邁進することを前提に、フィンランドの学界における最も重要な観点である学問の自由と科学的査読における誠実さ（integrity）、科学におけるグッドプラクティスに加え、国家間の競合と安全保障に対する注意を促すという内容である。

その目的は、「高等教育機関および研究機関が彼らの価値や関心に基づいて中国のパートナーと仕事を続けることを支援すること」にある。そのために、大学/研究機関が潜在化する挑戦的な課題（challenges）を知らされ、それに一層の注意を払うとともに、フィンランドの大学/研究機関と科学にとって重要な原則を推進できるような支援を行うことを目指すとしている。以下、内容を概観しておこう。

b. 対中協力における注意事項

中国との研究と教育の協力において配慮すべき注意事項として以下の 3 点が挙げられている。

① 学問の自由と科学における学界の査読に対する信頼性を尊重し、科学のグッドプラクティスを遵守すること。

る（詳細は、https://finlandabroad.fi/chn/contacts-and-networking 参照のこと）

フィンランドの研究者が遭遇する可能性のある問題やリスクには、倫理基準違反、政治的影響力、研究成果のデュアルユース、該当する法律や合意規程に対する違反、透明性、平等性、合意遵守等の互恵主義に反する行為などがある。

②国家の安全保障と技術のデュアルユースに注意を払い、安全/安心の研究環境を確保すること。

③ 競争力の維持に努めること。

研究開発競争の中で、研究者が遭遇する可能性のあるリスクには、学術協力における政府の影響力行使、安全保障貿易管理違反、調査データの不正移転、サイバー攻撃、スパイ活動などのほか、文化的価値の対立、地政学的次元の課題、競争の一層の激化などがある。

c. 提案

以上のような問題認識に立ち、『勧告』は「全ての安全かつ効果的な国際学術交流は、自律的な大学/研究機関の一般的な責任から始まる」と指摘し、相互に同意された実践と戦略的アプローチの必要性を述べ、次の 3 点について提案する。

① 当該機関自身の行動規範と立ち位置に基づく安全な協力とパートナー関係
・良い統治と十分な勤勉さが当該大学/研究機関の国際的な実践に組み込まれていること。
・リスク管理の仕組み、例えば協力に先立つリスク分析、パートナー関係を評価するための仕組みを国際協力の手続きに組込むこと。
・リスク認識を協力関係継続の前提条件にすること。
・問題や危機的状況への介入と通報手段を整備すること。

② 倫理的かつ価値的な選択
・学術的インテグリティに合致し、学問の自由を保障する国際協力であること。
・学問の自由と自律の原則及び価値は内部と外部のコミュニケーションの一部であり、それを国際協力と協定に反映すること。
・国際協力における倫理的挑戦を研究室内と野外調査の両方で理解すること。
・協定の文言においては文化的政治的かつイデオロギー的な含意を考慮に入れること。

③ リスク認識
・大量破壊兵器、デュアルユース、あるいは人権に反する利用といった研究の選択肢を狭める政治的経済的ファクターを認識し、研究成果の適用可能性を理解すること。
・貿易管理規則遵守と要請される貿易ライセンス申請への責任。国連及び EU の制裁を遵守すること。
・ハラスメント、過剰な影響力の行使の試み、研究結果の複製や誤用などの安全保障リスク

など、協力において生じ得る問題を理解すること。
・当該研究者とパートナーが政治的に機微な問題に遭遇するリスクを予測すること。
・研究協力や研究成果の共有におけるデータ保護義務、データの取扱いやその拡散における政治的リスクを認識すること。
・外国の資金提供の場合には、その背景と信頼性を確認すること。
・全面協力関係（二重学位プログラムのようなものを含む）で生じ得る評判上のリスクと経済的インパクト（商業的利益や経済的依存を含む）を評価すること。
・海外において、また必要な場合には国内でも、コンピュータ、SNS、その他の電子機器の使用に関して注意を払うこと。

本文書（英語版）はわずか８ページ、しかも各項目を箇条書きによって列挙した、簡素なものである。外務省の『プラン』と同じく、中国との研究協力を是としている。その上で、『プラン』よりも詳細に対中協力におけるリスクと注意事項を列挙する。しかし、こうしたリスクの査定方法やリスク遭遇時の対応などの詳細は示されていない。

(3) 中国ラウンドテーブル

「勧告」がフィンランドの公表された唯一の「新たなリスクへの対応」策である。リスクに関する具体的な指針や指標を示すガイドライン、確認すべき事項を列挙して行動管理を促すチェックリストの類は今のところ作成されていない。しかも、その内容は、上記のように具体性の乏しい提言に留まっている。だが、フィンランドでは、この公表された文書を補う「中国ラウンドテーブル China Roundtable」[185]と称される非公式の取組が存在する。

本組織の発端は、2011 年に中国との研究協力がスタートし、教育文化省の科学評議員が対中研究協力をどのように進めるか、協力を推進する上での自らの役割はなにかなどを明らかにするために、大学・研究機関の関係者を集め、議論の場を設けたことにある。2019 年に地政学上の問題が騒がれるようになり、中国との関係についてさらなる論議が求められ、研究協力によるメリットやチャンスだけでなく、リスクについても議論するようになった。もっとも、議論の話題は参加者からの自発的な提案によって決められた。

教育文化省の「勧告」が俎上に上るようになると、議論にはさらに様々なアクターが加わるようになり、参加者が 100 名に達することもあった。なお、自由な議論を維持するため、議論の中身や結果の公表は行われていない。

教育文化省（科学顧問）が立ち上げを主導し、その後も会を主催しているが、外務省、雇用経済省などとも密接に連携している。参加者から要請のあった話題に関連する省が随時参加する。参加者には、中国研究者、中国関連業務関係者のほか、弁護士も含まれ、バラエティに富む。特別な入会資格はなく、自由に参加と退出が可能なオープンフォーラム方式が

185 このラウンドテーブルに関する記述は、教育文化省の科学担当上級顧問（Senior Ministerial Adviser）の Tiina Vihma-Purovaara 氏への聞取り調査に基づく。聞取りは 2023 年 11 月 3 日 15:00～16:00 に未来工学研究所がオンラインによって実施した。

採用されている。

テーマ毎にワーキンググループが設置され、現在「パートナーシップ評価」、「情報の安全保障」、「情報・通信技術協力」、「法的課題」、「大学スタッフと学生に対する具体的な支援」の 5 グループが活動している。ラウンドテーブルの下にワーキンググループが組織され、ワーキンググループの参加者は平均 15～20 人くらいである。年に 2 回、各大学の学長、学術委員会の委員長、教育文化省など関係省トップが参加する会合を開催し、意見交換を行なっている。

2.10.4　フィンランドの取組に関する考察

(1)　フィンランドの取組の評価

対決的言質を避け、リスクを認識しながらも良好な関係の維持に努める姿勢は、フィンランドにおける外務省の「アクションプラン」を貫く方針であり、それに続く教育文化省の「勧告」の基調を成す。

北京のフィンランド大使館上級教育科学専門官（senior specialist in education and science at Finland's embassy in Beijing）の Mari-Anna Suurmunne は、2021 年フィンランド公共放送（YEL）において、フィンランドの「勧告」の目的を「中国との協力に関して生じ得る挑戦的課題（challenges）への注意喚起」だとし、「フィンランドの大学・研究機関はヨーロッパとは異なる中国の社会システムや価値観を理解する必要があり、より多くの情報提供を受けて協力関係を築くのが望ましい」と語った（Myklebust 2022）。続けて、「科学の世界で頂点をめざす競争が異なるルールのもとで起こっており、中国は今世紀の半ばまでに科学における世界のリーダーになることを目指し、この分野の研究と教育に莫大な投資をしている」（Myklebust 2022）と述べ、中国との研究協力には大きな好機があるとの見解を暗に示した。

こうしたフィンランドの姿勢について、その取組を分析した D'Hoogle と Lammertink（D'Hoogle and Lammertink 2022）の評価は厳しい。D'Hoogle と Lammertink は、フィンランドの取組は、政府レベルのアプローチが小規模な点に加え、知識移転の保護措置が軽視されていると指摘する。かれら自身の調査によると、「勧告」策定の初期段階では知識移転とテクノロジーの倫理的利用が議論の焦点になっていたが、焦点は次第に学問の自由に移っていった。その結果、知識移転の問題は、具体性を欠いた包括的な記述に終始し、知識移転の安全性が担保された国際協力とは何かを特定化する作業は大学・研究機関に委ねられることになった。

フィンランドの「小規模かつ曖昧な」アプローチの要因として、かれらは次の 2 点を挙げる。まず、取組の日が浅く、緒に就いたばかりである点である。次に、フィンランドの外交政策自体が宥和的な姿勢を取っており、教育文化省もその方針を共有している点である（D'Hoogle and Lammertink 2022）。2 点目の外交方針の共有については賛同可能である。既述のように、外務省の「アクションプラン」は対決や警戒よりも友好や協力が色濃かった

が、政策の一貫性に鑑みれば、教育文化省が従うのは当然のことであろう。もっとも、1 点目の取組の浅さに関しては必ずしも同意はできない。と言うのも、2023 年 11 月の段階で政府レベルの新しい取組はなく、2022 年 3 月に発行された「勧告」が現時点における政府の公式の見解として用いられているからである。すなわち、フィンランドの取組の「小規模かつ曖昧さ」は、取組期間の問題ではなく、中国への配慮という同国の立場を示すものだと考えられる[186]。

加えて、D'Hoogle と Lammertink（D'Hoogle and Lammertink 2022）は、「勧告」における知識移転保護措置の希薄さに批判的であったが、この点を以てフィンランドがリスクに対して無防備だと言い切ることはできない。というのも、「勧告」は同国の安全保障・諜報サービス(Security and Intelligence Service, SUPO ）の助言の下に策定されたとの指摘がある（Myklebust 2022）。SUPO の担当者は、大学世界ニュース（University World News）の記者に次のような認識を語っている。

「教育文化省の『勧告』は歓迎である。フィンランドには中国が関心を持つ多くの専門技能と知識があり、中国には諜報活動を含む様ざまな手段を用いてこうしたノウハウを獲得する用意がある。多くの中国の大学は同国の軍事産業、軍隊、安全保障当局と密接な関係の下に研究をしているので、科学協力においてはフィンランドの大学が知らないうちに、研究が中国での軍事目的に使われたり、研究成果が中国における人権侵害の助長に利用されたりすることがある。また、研究倫理の問題、学問の自由の侵害、軍事部門との財政的結合、検閲などのリスクもある。中国では、研究の自由はなく、中国共産党が膨大な国家資金を用いて中国研究者の国際研究協力を操作する。それが（中国人）研究者の自由度を制約している。また、海外での交流プログラム終了後に中国への帰国を義務付ける問題もある。研究の国際協力は絶対的に重要であるが、潜在的なリスクは特定されなければならない」（Myklebust 2022）。

SUPO のこのようなリスク認識が、その支援を受けた教育文化省に共有されていなかったとは考えられない。教育文化省には対中協力における警戒感やリスク認識があったはずである。ただ、それが「勧告」に明瞭かつ強く示されなかっただけではないかと推測される。

既述のように、ラウンドテーブルに関する情報は非公開であった。公開文書である勧告は当然中国にも認知されるので、その内容、文言には注意を払わざるを得ない。友好と警戒の二面性を追求するフィンランドの取組において、後者の側面は慎重にならざるを得ず、具体的なリスク対応の部分は非公開、あるいは敢えて文章化しないと言うこともあり得る。ラウンドテーブルは、まさにこの非公開、非文章化によるリスク対応と言うことができるのではないだろうか。フィンランド教育文化省の担当者は、オープン化、国際化に伴う新たなリスクへのフィンランドの対応を「学問の自由と民主主義、学問の信頼に対する責任」と言う理念的な文言によって表現した[187]。この理念を担保するためのリスク対応を怠っているとは考えられない。

---

186 この点については、2023 年 11 月 3 日に実施した Tiina Vihma-Purovaara 氏への聞取り調査でも確認済みである。

187 聞き取り調査における Tiina Vihma-Purovaara 氏の発言に基づく。

しかも、ラウンドテーブルは問題共有だけでなく、その解決を即時に図ることができる実践型の仕組みである。D'Hoogle と Lammertink は政府と大学・研究機関が同じテーブルに着き、情報を共有するのは政策に首尾一貫性をもたらし、お互いの要請・要望が円滑に伝わって容易に問題解決に結び付くため、双方にとってメリットがあると評価した（D'Hoogle and D'Hoogle 2022）。しかし、非公開と非文書化の原則による限界もある。情報共有は出席者の間に限られ、一般化されてより広範な研究者や大学等の関係者に共有されることがない。また、情報の透明性、公開性という民主主義の原則にも合致しない。

(2) 大学側の反応

対中協力におけるリスクの査定と特定化は大学・研究機関の手に委ねられている。では、大学側は、「勧告」や「ラウンドテーブル」にみられるボトムアップな取組をどのように受止めているのだろう。

ラウンドテーブル関係者に聞取り調査をした D'Hoogle と Lammertink は「一般的に言えば、フィンランドの学界は、政治的に動機づけられて現場では扱い辛い立法措置には批判的なので、こうしたボトムアップなアプローチを歓迎している」と肯定的に評価する（D'Hoogle and Lammertink 2022）。設立から 10 年余り活動を続け、「勧告」をめぐる議論では 100 人もの参加者があったことは、ラウンドテーブルが中国に関わる研究者や大学関係者に支持されていることの証左の一つである。

「勧告」に関しては大学による自発的な取組がみられる。たとえば、大学世界ニュース（University World News）の記者のインタビューに対し、ヘルシンキ大学運営部門のトップ、Esa Hämäläinen は、「『勧告』を踏まえて、大学は新しいパートナーとの協力を統制するリスク査定手続きを導入し」、「大学トップに勧告する高いレベルの勧告委員会をすでに任命した」と述べ、大学が自ら積極的に取組んでいることを明らかにした。しかし、「この手続きは、中国に特化したものでは全くない」と付け加え、中国への配慮も忘れていない。また、「個々の研究プロジェクトはユニークであり、大学当局としては注意深い評価なしに価値ある重要な研究を阻止したくはない」と学問の自由優先の姿勢を示し、リスク査定の目的は「学部長や研究主査が、政治的、経済的、社会的、法的あるいは評判といった学術研究には直接関係しないリスクに早期に気づき、リスク発見時にはその緩和策を見出すのを支援すること」だと述べている（Myklebust 2022）。

一方、「勧告」を各大学で実践する上では、いくつかの課題が挙げられている。D'Hoogle と Lammertink が情報提供者から得た情報として指摘するのが、まず「勧告」が提起した観点を大学内で議論し、具体策に発展させるための資源と能力が不足している点である（D'Hoogle and Lammertink 2022）。また、現場が直面する課題と解決は自然科学と社会科学の間では大きく異なり、単一のアプローチでは対応できない点、学内の中国に関係する全てのスタッフに周知することの困難さなどが提起されたという。

フィンランドの取組は、対中研究協力における好機とリスクのバランスをいかに上手く保つかという点に集約でき、それは政府に限らず大学・研究機関にも共有されている観点だと言うことができる。

2.11　デンマーク

2.11.1　デンマークにおける「研究インテグリティ」に係る取組の特徴

デンマークの高等教育・科学省（Uddannelses- og Forskningsministeriet）では、2014 年 11 月に「Danish Code of Conduct for Research Integrity（研究インテグリティに関する行動規範）」[188]を策定した。デンマークの研究インテグリティの行動規範の基本原則は、誠実さ（Honesty）、透明性（Transparency）、説明責任（Accountability）に基づくものとした[189]。本行動規範は、日本における「研究公正」に関わる内容が中心であるが、研究セキュリティに直接明示していないものの、「データ管理」や「共同研究」の項目で、研究データに関する研究機関の管理的側面や、研究文化、研究インテグリティに対する認識が学問分野、機関、国によって異なる可能性があるため、共同研究パートナーと合意を確立し、責任ある研究を実施できるようにすることを明示した。

2020 年代に入ると、国防情報局、国防情報局サイバーセキュリティセンター、警察情報局から、中国、ロシア等との国際研究・イノベーション協力上の懸念事項が指摘され、デンマーク高等教育・科学省は、2020 年に「Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde（以下、URIS：国際研究・イノベーション協力指針委員会）」を設置し、2022 年 5 月に『Afrapportering: Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde』（国際的な研究・イノベーション協力指針〈ガイドライン〉）を公表した[190]。また、ガイドラインの公表前年には、デンマーク安全保障情報局（Danish Security and Intelligence Service：以下 PET）は、高等教育・科学省とともに、「Is your research at risk?」を公表し、研究機関の職員がどのように外国からの干渉やスパイ活動を防止し、対応するかの勧告を行っている。2 つのガイドラインは、公表時期が異なるものの、URIS のガイドラインは、教育・研究機関の経営陣を対象としたもので、PET が策定したガイドラインは、研究者を対象としたものである。

2.11.2　デンマークにおける取組の背景と経緯

研究・イノベーションにおける国際協力は、デンマークのような規模が小さく、開放的な

---

188 デンマーク高等教育・科学省「Danish Code of Conduct for Research Integrity（研究インテグリティに関する行動規範）」, 2014 年 11 月.

189 「Danish Code of Conduct for Research Integrity」では、研究インテグリティの誠実さ、透明性、説明責任の 3 つの基本原則について、誠実さは、研究の信頼性を確保するため、研究者は目的、方法、データ、分析、結果、結論の報告に誠実であるべきとした。透明性では、科学的推論の信頼性を確保し学術的考察が関連分野の研究慣行と一致していることを保証するため研究のすべての段階は透明であるべきで、報告はオープンであることが必要であるとした。説明責任では、研究の信頼性を確保するため、全ての関係者が実施された研究に対する説明責任を負う。具体的には、研究結果の正確性と信頼性、すべての関連規制の遵守、教育・研修・監督を通じた研究インテグリティの文化を醸成し維持すること、責任ある研究実施に対する違反に適切な処置で対処することを掲げた。また、責任ある研究実施のための 6 つの基準は、①研究計画と実施、②データ管理、③出版とコミュニケーション、④オーサーシップ、⑤共同研究、⑥利益相反からなる。研究機関レベルでは、追加的に仕様や方針、手順を策定することが推奨されている。

190 https://ufm.dk/publikationer/2022/filer/uris-afrapportering-2022.pdf

経済にとり重要であると認識されている[191]。研究・イノベーションにおける強力でオープンな国際協力は、高度に専門化された海外の研究施設や知識へのアクセスの提供機会を得るとともに、デンマークへの人材誘致を支援するものとなる。

一方で、デンマークの教育・研究機関は、研究・イノベーションにおける国際協力は、過去 10 年間でより複雑化し、高度な倫理的、財政的、安全保障上のリスクを伴うことを認識している。例えば、倫理的、財政的なリスクでは、EU の Horizon 2020 や海外の資金配分機関（米国・国立科学財団等）からの要求に対応するため、デンマーク高等教育・科学省は、2014 年 11 月に「研究インテグリティに関する行動規範」を策定した。デンマークの研究インテグリティの行動規範の基本原則は、前述のとおり、誠実さ、透明性、説明責任に基づき、研究インテグリティについて研究者の日常業務における実用的なツールとして、分野横断的な基準を定めた。この中で「責任ある研究実施」では、研究プロセスに関わる全ての人が、研究を実施するための高い基準（データの適切な収集・管理から研究結果の普及に至るまで）に従うことが必要とした。また、研究セキュリティにも係る部分としては、「データ管理」項目の「責任分担」では、研究者は一次資料およびデータ保管の責任を有しているが、研究機関は守秘義務要件や規制、ガイドラインに合致した安全なデータ保管施設を提供する責任があることを定めるとともに、保管される資料、データへのアクセスが認められるとした[192]。「共同研究」項目では、研究文化や研究インテグリティに対する認識が学問分野、機関、国によって異なる可能性があるため、共同研究パートナーと合意を確立し責任ある研究を実施できるようにすべきとした。他方、本規範が作成された時点では、共同研究パートナーに対して、2009 年に作成された OECD グローバル・サイエンス・フォーラム「Investigating Research Misconduct Allegations in International Collaborative Research Projects – A Practical Guide（国際共同研究プロジェクトにおける研究不正行為疑惑の調査－実践ガイド）」[193]を参考にする等、研究インテグリティの中でも、研究不正に関するガイドが中心であると考えられる。

一方で、デンマークの各機関（国防情報局、サイバーセキュリティセンター、警察情報局）[194]においても、外国の国家がデンマークの競争力にとり、安全保障政策に悪影響を及ぼす可能性のある知識、技術、製品を違法に獲得しようとする傾向が高まっていることを報告して

---

191 デンマーク高等教育・科学省「Afrapportering - Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde（国際研究・イノベーション協力指針委員会報告書）」, 2022 年 5 月 25 日.

192 研究機関の研究者の資料、データへのアクセスは、契約上の法的義務や倫理・機密保持・プライバシー問題、知的財産権等が現行規制に抵触する場合を除いた場合である。

193 2007 年に OECD グローバル・サイエンス・フォーラムが 2007 年に国際的な専門家からなる委員会を設置し、研究機関が不正行為を調査し、よくある“落とし穴”を回避するための実践的な勧告として作成された。国際共同研究の合意書に挿入できる「定型文」や国際的な研究不正行為の調査を実施するための基本原則、ガイドイラン、手順案が含まれている。(https://web-archive.oecd.org/2012-06-14/118158-42770261.pdf)

194 各機関の報告として、デンマーク国防情報局（Forsvarets Efterretningstjenestes）の「Udsyn 2021」報告書（デンマークの安全保障と戦略的利益における海外の最も重要な脅威とその他の状況の全体像を取りまとめたもの）、国防情報局サイバーセキュリティセンター（Forsvarets Efterretningstjenestes Center）の「Cybertruslen mod Danmark 2021」（サイバーセキュリティの年次評価報告書）、デンマーク警察情報局（Politiets Efterretningstjenestes）の「Vurdering af spionagetruslen mod Danmark 2022」（デンマークに対するスパイの脅威の評価報告書）がある。

いる。これまで国際的な研究・イノベーション協力においては、北朝鮮やイラン等の国際的な制裁を受けている国に留意する必要があったが、近年ではロシア、中国が留意する国として浮上してきた。背景には、ロシアは、政治、経済、軍事に関する情報収集や新技術開発においてロシアの立場を強化するような事項に重点を置くとともに、ロシアによるウクライナ侵攻も研究・イノベーション協力の停止に至った。また、中国については、2017 年に制定された国家情報法があり、中国の国家機関、民間機関は、要請があれば、安全保障当局に協力することが義務付けられた。中国の研究機関（個々の研究者を含む）は、国家機関から独立していないため、学問の自由だけでなく、研究倫理や誠実さに関わる問題が生じる可能性が懸念される。また、ロシア、中国の両国とも、学問の自由を制限し、政治的に敏感なテーマについて検閲を行い、軍民一体化により人権侵害を含む知識、技術の軍事利用や非倫理的な利用リスクがある。中でも、世界トップクラスの研究環境を有する中国との共同研究は、デンマーク、EU、同志国の研究機関や企業にとって非常に重要で有益であるが、デリケートな技術分野における中国の研究能力の強化に貢献することに基本的なジレンマを抱えている。

これらから、デンマークでは、高等教育・科学省が、2020 年秋に URIS を設置し、2022 年 3 月まで議論を行い、同年 5 月には、委員会報告書（「国際的な研究・イノベーション協力指針」）として公表し、高等教育・科学大臣に報告した。URIS での検討では、国内外の専門家も議論に参加し、EU や同志国の取組やガイドラインも参考にした。イェスパー・ペーターセン（Jesper Petersen）高等教育・科学大臣は、大学は中国のような国々と協力する際には、危機感を持つ必要があること、これらの国との国際的な研究・イノベーション協力により、デンマークの研究者が軍事能力の構築や人権侵害に加担する危険性の高い可能性を懸念し、国全体としてパラダイムシフトを実施することを示した。

2.11.3　デンマークにおける取組の詳細

(1)　URIS「国際的な研究・イノベーション協力指針」

前述のとおり、URIS（国際研究・イノベーション協力指針委員会）[195]は、2022 年 5 月に『Afrapportering Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde』（国際的な研究・イノベーション協力指針〈ガイドライン〉）を公表した。

URIS では、国際的な研究・イノベーション協力の新たなアプローチとして、リスク管理に重点を置き、ⅰ）倫理的、財政的、安全保障上のリスクに対する組織的な意識向上、ⅱ）リスク管理のための組織的な枠組みと手順、ⅲ）関係当局やデンマークの教育・研究環境にまたがる全国的な共通アプローチと知識共有の強化の必要性の観点から提言し、デンマークの教育・研究機関の経営陣に向けたガイドラインを作成した[196]。なお、本報告（ガイドラ

[195] 2020 年に高等教育・科学大臣が設置した委員会。委員会は、デンマークの大学（8 つの大学）、専門職大学、政府研究助成機関のリーダー等の 11 人のメンバーから構成される。
[196] 高等教育・科学省プレスリリース“Ny rapport: Behov for skærpet tilgang til forskningssamarbejde

イン）は、高等教育・科学大臣に報告した。

URIS では、国際的な研究・イノベーション協力について、以下の点をリスクとして、検討を行った。

【URIS の論点：国際研究・イノベーション協力上のリスク】

- 研究データの責任ある管理および著作権保護を含む、研究インテグリティおよび責任ある研究実施の原則の違反
- 人権侵害を含む、軍事的または非倫理的な技術の利用
- デンマークの教育・研究機関における外国人学生／職員による、外国からの干渉およびセキュリティ違反
- 研究協力による、独裁的な国家におけるセンシティブな分野の研究・イノベーション能力の強化、構築への貢献可能性

本ガイドラインは、イントロダクション、要旨、委員会の主な結論と提言、新ガイドライン、フォローアップで構成される。

【ガイドラインの構成】
第 1 章　イントロダクション
第 2 章　要旨
第 3 章　委員会の主な結論と提言
第 4 章　新ガイドライン
　　4.1　重要な研究の特定と保護
　　4.2　ビジネスパートナーの把握
　　4.3　教育機関・職員・学生の保護
第 5 章　フォローアップ

【ガイドライン】

本ガイドラインは、デンマークの大学は、他国（例えば、中国）と協力する際に、デンマークの研究者が軍事力の強化や人権侵害に加担する危険性が生じないか、より危機感を持つことを求めている。具体的には、デンマークの教育・研究機関は、特定分野について特定の国との研究協力で、米国の教育・研究機関や企業との協力の可能性を減少させる可能性があることを認識すべきであるとした。国際的な共同研究において、リスク管理が十分に重視されない場合、デンマークの企業を含む欧州企業は、デンマークの教育・研究機関に対する信頼を失う可能性がある。このため、ガイドラインは、デンマークの安全保障と競争力、そ

med blandt andre Kina”（New report: Need for a tougher approach to research collaboration with, among others, China）, 2022 年 5 月 25 日. (https://ufm.dk/aktuelt/pressemeddelelser/2022/ny-rapport-behov-for-skaerpet-tilgang-til-forskningssamarbejde-med-blandt-andre-kina)（2024 年 1 月アクセス）

して、デンマークの研究の基本的価値と推進において必要なものと位置付けている[197]。

URIS の議論では、重要な研究・イノベーションを特定、保護するのは教育・研究機関の責任であることを強調している。一方で、ガイドラインを完全に実施するには、教育・研究機関の経営陣と職員の両方がオーサーシップを持つ必要があることを指摘した。中でも、職員や学生がリスクを管理し、共同研究の潜在的な利益を促進するための仕組みや手順を構築することは、研究機関の管理職の責任であるとした。このため、本ガイドラインの読み手は、教育・研究機関の管理職を対象に作成された。以下、ガイドラインの概要を示す。

URIS のガイドラインは、①重要な研究の特定・保護、②共同研究パートナーの認識、③教育機関・職員・学生の保護の 3 つのカテゴリーからなり、9 つの具体的な行動を提案している。

重要な研究の特定・保護について、URIS の議論にて、外国の研究者がデンマークの利益を損なうような独自のデータ、企業機密、軍事的ノウハウに不法にアクセスしようとする例が浮上しているとともに、情報機関の評価では、外国の国家主体が知識を得たり、技術移転を図る傾向が強まっていることが示された（例えば、中国の千人プログラム等）。商業的・軍事的ノウハウが失われるリスクが最も高いのは自然科学、健康科学、技術科学分野であるが、社会科学や人文科学にも学問の自由の喪失や検閲、研究影響を書き換える（社会的に是とする方向に分析づける）等のリスクが明らかになっている。このため、ほとんど全ての研究分野で外国からの干渉を受けるリスクがあり得ること、EU や同志国で特定国の特定分野の協力を排除する一般的な決定はされていないものの、Horizon Europe や Digital Europe Program では、中国、ロシア等の国の機関、企業は共同プロジェクトに参加できないことになっていることを示した。

ビジネスパートナーの把握について、外国からの干渉を実際に認識するのは非常に複雑で、研究者が特定の研究テーマに取り組むことに同意しても、海外のパートナーは研究者がこれまでに実施してきた研究データにアクセスすること等を考えているケースがある。デンマーク工科大学（Technical University of Denmark：DTU）の事例でも、中国の国立国防技術大学の中国人研究者との共著論文を執筆するケースや、DTU に留学していた中国人の博士課程学生が帰国後、軍用大学とのつながりがあったことが分かるケースもある。URIS では、中国との共同研究は、中国で優秀な研究者が政府機関に近いことも多い事実により複雑になっており、多くの利害のもつれが懸念された。

教育・研究機関、職員、学生の保護では、近年、デンマークの教育・研究機関が巻き込まれた事例からも、国際的な共同研究に伴う脅威が現実的に複雑であることが浮き彫りになっている。一方で、全ての職員、学生が研究の倫理的、金銭的、セキュリティのリスクを経験しているわけではなく、研究者自身が外国からの干渉の標的になると認識するのが難しい状況である。外国からの干渉は、人的、経済的な方法からデジタル的な方法まで多様であり複合的であることを認識する必要があるとした。

以下、ガイドラインのカテゴリー、項目、URIS の提言事項を示す。

197 https://www.universityworldnews.com/post.php?story=20220531144822860

表 2-15：ガイドラインのカテゴリーと項目

カテゴリー	項目および提言事項（箇条書き箇所）
1．重要な研究の特定・保護	研究の価値と可能性を把握する • 公的研究助成財団は二国間協力について教育・研究機関、高等教育・科学省と緊密に対話すること • 高等教育・科学省は、教育・研究機関の協力を得て、個々の研究分野における特定国との協力程度（従業員数、学生数、プロジェクト協力、特定国からの資金の流れ）の共通概要を作成すること
	知識と成果を保護する • 公的研究助成機関は、デンマークのプロジェクト参加者に対し、知的財産権、知識共有の範囲、所有権を明確に規定した国際パートナー・コンソーシアム契約書の作成を求めること
	輸出管理規制と投資審査法に精通する • デンマーク企業局は、研究・イノベーション分野における輸出管理体制および投資審査法について、規則の適用機関向けのガイド等、カウンセリングを実施すること
2．ビジネスパートナーの把握	取引先を調査する • 高等教育・科学省は、外国の大学、企業と軍・政党とのつながりに関する欧州や国際的な関連データベースにアクセスする可能性を探り、教育・研究機関の身元調査を支援できるようにすること
	なぜ、協力するかを自問する • 高等教育・科学省は、教育・研究政策外交官をデンマーク大使館に派遣する等をして、教育・研究分野における特定国の行動に関する能力と知識を向上させること
	協力する対象を限定する • 特定の技術、データ、設備、結果を共有または利用するかは、国際協力協定や国際協力関係を標準としてポジティブリストに含めること（何を共有し、共有したくないかの明確なシグナルを国際的なパートナーに送ることができる）
3．教育・研究機関、職員、学生の保護	脅威があることを認識する • 高等教育・科学省、外務省、国防省、情報機関は、各教育・研究機関に対し、現在の脅威に関する最新情報を提供し、各機関の取組に積極的に貢献すること
	安全手順とシステムを重視する • 〔研究機関に対し〕組織内の指揮命令系統の明確化、コミュニケーションチャンネルとセキュリティの取り扱い手順を確立すること • 〔研究機関に対し〕非同盟諸国への渡航、滞在の際の行動、注意、不審な問合せを経営陣に報告する方法を徹底させること
	従業員と学生を守る • 〔研究機関に対し〕副次的雇用に関する内部規則の見直し • 〔研究機関に対し〕新入職員の手順、外国人職員の管理、干渉の報告

出典：URIS「Afrapportering Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde」（国際的な研究・イノベーション協力指針〈ガイドライン〉）より未来工学研究所作成.

(2) PET「あなたの研究リスクとは?」

デンマークでは、2021 年 5 月に、デンマーク安全保障・情報局（PET）とデンマーク高等教育・科学省（Ministry of Higher Education and Science）において、『Is your research

at risk?』を公表した。同レポートは、研究機関の職員が外国からの干渉やスパイ活動をどのように防止し、対応するかについて勧告したものである。

【報告書の構成】
1. より良い準備の必要性
2. 脅威の現実
3. 重大な研究
4. 曝露された研究分野
5. あなたがさらされている脅威の度合い
6. 研究の収集方法
7. セキュリティを向上させる 8 つのヒント

外国からの干渉、スパイ活動、影響活動は、デンマーク刑法第 12 編の第 107 条から第 109 条に定義されており、スパイ行為は、国家のために秘密にしておかなければならない事項に関する情報を収集し、または伝達する行為であり、スパイ活動は、デンマークの国家または公共の利益のために秘密にされるべき事項に関する情報を収集または伝達する活動であるとしている。スパイ行為の中には、デンマークの公共利益やデンマークに居住する個人の安全等を危険にさらす、または国家安全保障を危うくするようなデータの開示も含まれる。

リスクにさらされる研究分野は絶えず変化し、外国の諜報機関がハイテクや防衛関連分野を恒常的に注目している。このため、自然科学、社会科学、人文科学に関連する多くの研究プログラムを含め、全ての大学は、潜在的に外国からの干渉を受ける危険性があることを明確にした。外国の干渉やスパイ行為にさらされる可能性があるものとして、商業的または特許可能な結果につながる可能性がある成果、遺伝子情報や商業的な検査データ等の機微なデータや個人を特定できる情報が含まれているもの、外国で軍事目的に使用される可能性またはデュアルユースの両方に応用可能性がある成果、国際的な戦略的政治交渉の基礎となる可能性を有するものが挙げられる。

上記を踏まえ、研究の安全確保のためのヒントとして、①脅威を認識する、②研究の価値を評価する、③外国人訪問者の枠組みを設定する、④海外出張上の注意、⑤IT セキュリティに集中する、⑥物理的セキュリティに重点を置く、⑦用心（無防備への備え）、⑧報告を挙げた。

表 2-16：研究の安全確保のための 8 つのヒント

ヒント	主な内容
1）脅威を認識する	• 脅威と、スパイ活動や外国からの干渉に使用される方法を認識すること • 妨害やスパイ行為による脅威を周知させ、共同の取組に関するコンセンサスを形成すること
2）研究の価値を評価する	• 責任ある研究者は、研究結果が商業的に興味深いか、安全保障や防衛技術に関連しているか、デュアルユース用途があるか等を検討すべきである • 誰が何にアクセスすべきかを決めるべき
3）外国人訪問者の枠組みを設定する	• 訪問に先立ち、どの情報を訪問者と共有するか、特にどの情報を共有しないかを決めておく • 参加者リストの直前の変更に注意する • 訪問中、ゲストがいつもと違う行動をとっていないか観察する。国家安全保障上の利害がある訪問を事前に PET に知らせること（推奨）
4）海外出張上の注意	• 海外への旅行、会議、滞在に関連して、セキュリティに重点を置くこと（持参する書類やデータのリストを作成することを含む） • 海外の Wi-fi は監視されている可能性があるため、機密性の高い情報にはアクセスしないこと（VPN サービスの利用） • すべての機器の Bluetooth をオフ
5）IT セキュリティに集中する	• ウイルス対策プログラム、スパムフィルター、VPN 接続によるアクセスなど、効果的なセキュリティ・パッケージのインストール • 仕事とプライベートの使い分け（電子メールアドレス、携帯機器） • ソーシャルメディアのプライバシー設定を確認し、どの個人情報を表示するか検討すること • 情報源が信頼できるかどうかわからない場合、アクセスしない（添付ファイル、リンク、USB メモリ）
6）物理的セキュリティに重点を置く	• アクセス・コードを使用する場合は、権限のない者に読み取られないよう保護すること • 侵入を試みた形跡はないかの確認 • 施設内への部外者の視界を遮ること • 暗証番号付きキャビネットの番号管理　他
7）用心（無防備への備え）	• 他人を信頼しようとするのは自然であり、誰でも確認や承認を求めるが、逆に利用されることを留意
8）報告	• 外国からの干渉やスパイ行為など、懸念を抱かせるような経験は報告するべき

出典：Danish Security and Intelligence Service (PET)（2021）「IS YOUR RESEARCH AT RISK? - Tips on foreign interference and espionage for researchers and other staff」より未来工学研究所作成.

2.12 オランダ

2.12.1 オランダにおける「研究インテグリティ」に係る取組の特徴

オランダにおいては、「研究インテグリティ」に関する用語として、「知識セキュリティ（Knowledge Security）」が使用されている。これは、何よりもまず、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ものである。オランダ政府としては、「知識セキュリティ」に関して、以下のような見解を持っている[198]。

- 知識の移転が、国の安全保障を損なうようなものであれば、それは望ましいものではない。
- 「知識セキュリティ」は、他国による教育や研究への隠然たる影響も伴う。このような他国からの干渉は、学問の自由と社会の安全を危うくする。
- 「知識セキュリティ」は、基本的人権を尊重しない国との協力において起こりうる倫理的問題を含む。
- 世界レベルの高等教育や科学は、国際的な協力や世界中から集まる科学者の才能なしには成り立たない。国家レベルの知識セキュリティに関するガイドラインは、国際協力が安全に行われることを保証するのに役立つ。
- 知識安全保障に対するいかなる措置を導入するにしても、バランスが不可欠である。基本原則は常に「可能な限りオープンに、必要な場合は保護する」である。

知識とイノベーションは、スパイ活動などの伝統的な手段と並行して、あるいは組み合わせて使用される可能性のある戦略的な権力の道具と見なされるようになってきている。このような動きは、オランダの知識セクターに携わるすべての人に影響を及ぼすものであり、知識の安全を確保するために最大限の努力をすることは、オランダ政府が共同して取り組むべき課題であるという認識を持っている。

このような認識を踏まえて、オランダ政府は、2022 年 1 月に、National knowledge security guidelines（知識セキュリティに関する国家ガイドライン）[199] を作成・公開した。

2.12.2 オランダにおける取組の背景と経緯

表 2-17 に、オランダにおける「知識セキュリティ」の取組の流れを示す。

オランダ政府は、大学・研究機関が国家主体による様々な脅威に直面していることに留意し、2020 年後半から、中国のオランダ中央政府とオランダのほぼ全てのアカデミックな機関との間で、「知識セキュリティ対話」が開始された。この中で、教育・文化・科学省（Ministry of Education, Culture and Science: OCW（オランダ語略名））はオランダ司法・安全省テロ対策調整官（National Coordinator for Security and Counterterrorism: NCTV（オラン

198 Government of the Netherlands (Contact Point for Knowledge Security) (https://english.loketkennisveiligheid.nl/knowledge-security)
199 “National knowledge security guidelines: Secure international collaboration,” January 2022.

ダ語略名））および国家情報安全保障局（General Intelligence and Security Service: AIVD（オランダ語略名））と協力して、オランダ大学連盟（Universities of The Netherland: UNL（オランダ語略名））及びその 14 の提携大学、オランダ王立芸術科学アカデミー（Royal Netherlands Academy of Arts and Sciences: KNAW（オランダ語略名））、オランダ科学研究機構（Netherlands Organization for Scientific Research: NWO（オランダ語略名））及びその 19 の提携研究機関、オランダ大学医療センター連盟（Dutch Federation of University Medical Centers: NFU（オランダ語略名））及びその 7 つの提携大学医療センターとの対話等が行われた。この「知識セキュリティ対話」は、大学・研究機関内の事務レベルでのセキュリティ意識向上に貢献した。同時に、一連の対話は、大学・研究機関が何を必要としているのか、どこにまだ打つ手があるのかについての洞察をオランダ政府に提供した[200]。

2020 年 11 月、オランダ政府は、「教育・文化・科学大臣、法務・治安大臣及び経済・気候担当国務大臣から下院議長への書簡 : 高等教育・科学における知識セキュリティに関する議会書簡」で、オランダにおいて、知識セキュリティに関するガイドラインの作成、脅威評価の実施、知識セキュリティに関する相談窓口の設置等、知識セキュリティを構造的に強化するための対策を、オランダ議会に提示した[201]。

2021 年 2 月、国家情報安全保障局（AIVD）、軍事情報安全保障局（Military Intelligence and Security Service: MIVD（オランダ語略名））及びオランダ司法・安全省テロ対策調整官（NCTV）により、国家アクター脅威評価（State Actors Threat Assessment: DBSA（オランダ語略名））が実施され、その内容がオランダ議会下院に提出された。この中で、経済スパイ活動は、特にオランダのトップの産業セクターや大学等の知識機関を標的としていることが言及された[202]。

2021 年 7 月、オランダ大学連盟（UNL）が当時の教育・文化・科学大臣に、「Knowledge Security Framework」を提出した。このフレームワークは、オランダの大学が知識セキュリティに対するコミットメントを表明し、知識セキュリティに関する意思決定や方針を策定する際の助けとなるように作成されたものである。同フレームワークは、大学の管理職、研究者、大学セクター全体及び関係省庁を対象としている[203]。

2022 年 1 月 31 日、オランダ大学連盟（UNL）、オランダ王立芸術科学アカデミー（KNAW）、応用研究組織連盟（Dutch Applied Research Organizations: TO2（オランダ語略名））、オランダ大学医療センター連盟（NFU）、オランダ科学研究機構（NWO）等の研究セクター

[200] Letter from the Ministers of Education, Culture and Science, of Economic Affairs and Climate and of Justice and Security to the Chairman of the House of Representatives of the States General (31 January 2022) (https://zoek.officielebekendmakingen.nl/kst-31288-948.html)
[201] Letter to Parliament on measures to ensure knowledge safety in higher education and science (27-11-2020) (https://open.overheid.nl/documenten/ronl-2d5d6a09-f681-4edc-90a6-fbefe84f6da2/pdf)
[202] Letter from the Minister of Justice and Security to the President of the House of Representatives of the States General, February 2021. (https://zoek.officielebekendmakingen.nl/kst-30821-125.html)
[203] Association of Cooperating Universities in the Netherland, "Framework Knowledge Security Dutch Universities（英語翻訳版）," 2021. (https://www.universiteitenvannederland.nl/files/documenten/Domeinen/Integrale%20veiligheid/VSNU%20Framework%20Knowledge%20Security%20Dutch%20Universities.pdf)

が共同で、「National knowledge security guidelines」（知識の安全保障に関する国家ガイドライン）[204]を作成・公開した。このガイドラインは、国際共同研究に対処し、機会と安全上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、オランダ政府は、省庁間の共同により、「National Contact Point for Knowledge Security」を設置し、「Knowledge Security Desk」を立上げた。これは、大学等が、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[205]。

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。今後、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。知識セキュリティに関するリスクの検討と同ガイドラインの遵守に関する全責任は申請者である大学・研究機関にある。申請者は申請時に、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[206]。

申請書または授与されたプロジェクトにおいて、知識セキュリティ上のリスクが明らかに示唆される場合、オランダ科学研究機構（NWO）は申請者またはプロジェクトリーダーに対し、申請書または研究プロジェクトがガイドラインにどのように準拠しているかを示すよう求めることができる。状況によっては、NWO はプロジェクトリーダーおよび担当の大学・研究機関と協議することがある。この要請に応えられない場合、あるいは申請書やプロジェクトがガイドラインに準拠していないことが判明した場合、資金提供に影響を及ぼす可能性がある[207]。

[204] “National knowledge security guidelines: Secure international collaboration,” January 2022.
[205] https://www.loketkennisveiligheid.nl/
[206] https://www.nwo.nl/en/knowledge-security
[207] Ibid.

表 2-17：オランダにおける知識セキュリティの取組の流れ

期日	概要
2020 年後半	オランダ中央政府とオランダのほぼ全てのアカデミックな機関との間で、「知識セキュリティ対話」が始まった[208]。
2020 年 11 月	オランダ政府は、「教育・文化・科学大臣、法務・治安大臣及び経済・気候担当国務大臣から下院議長への書簡：高等教育・科学における知識の安全性に関する議会書簡」で、オランダにおいて知識セキュリティを構造的に強化するための対策を、オランダ議会に提示した[209]。
2021 年 2 月	国家情報安全保障局（AIVD）、軍事情報安全保障局（MIVD）及びオランダ司法・安全省テロ対策調整官（NCTV）により、国家アクター脅威評価（DBSA）が実施され、その内容がオランダ議会下院に提出された[210]。
2021 年 7 月	オランダ大学連盟（UNL）が、当時の教育・文化・科学大臣に対して、オランダの大学が知識セキュリティに対するコミットメントを表明し、知識セキュリティに関する意思決定や方針を策定する際の助けとなるものとして「Knowledge Security Framework」[211]を提出した。
2022 年 1 月 31 日	オランダ大学連盟（UNL）、オランダ王立芸術科学アカデミー（KNAW）、応用研究組織連盟（TO2）、オランダ大学医療センター連盟（NFU）、オランダ科学研究機構（NWO）等の研究セクターが共同で、国際共同研究に対処し、機会と安全上のリスクを検討することが求められる大学・研究機関の管理者向け指針として「National knowledge security guidelines」[212]を作成・公開。
2022 年 1 月 31 日	オランダ政府省庁の共同で、大学等が気軽に国際共同研究に関する機会とリスクや実務的な事項に関連する質問をすることができる中央窓口として「National Contact Point for Knowledge Security」を設置し、「Knowledge Security Desk」を立上げた[213]。
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。今後、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になった[214]。

[208] Letter from the Ministers of Education, Culture and Science, of Economic Affairs and Climate and of Justice and Security to the Chairman of the House of Representatives of the States General (31 January 2022) (https://zoek.officielebekendmakingen.nl/kst-31288-948.html)
[209] Letter to Parliament on measures to ensure knowledge safety in higher education and science (27-11-2020) (https://open.overheid.nl/documenten/ronl-2d5d6a09-f681-4edc-90a6-fbefe84f6da2/pdf)
[210] Letter from the Minister of Justice and Security to the President of the House of Representatives of the States General, February 2021. (https://zoek.officielebekendmakingen.nl/kst-30821-125.html)
[211] Association of Cooperating Universities in the Netherland, "Framework Knowledge Security Dutch Universities（英語翻訳版）," 2021.
[212] "National knowledge security guidelines: Secure international collaboration," January 2022.
[213] https://www.loketkennisveiligheid.nl/
[214] https://www.nwo.nl/en/knowledge-security

2.12.3 オランダにおける取組の詳細

オランダにおいては、大学・研究機関が「知識セキュリティ」を担保していくうえで、「Knowledge Security Framework」及び「National knowledge security guidelines」の 2 つが重要な役割を持つと考えられる。この 2 つの文書は、知識セキュリィを担保するうえで、特に、リスクマネジメントとそのプロセスを重要視している。

以下、これを踏まえて、「Knowledge Security Framework」及び「National knowledge security guidelines」における、リスクマネジメントの考え方を中心に詳説する。

(1) Knowledge Security Framework

このフレームワークの目的は、国際協力の機会と知識セキュリティのリスクを評価するための基盤を提供することである。同フレームワークは、知識セキュリティに関する政策や意思決定を行うための、国にとらわれない評価フレームワークを大学管理者に提供するものである。このフレームワークは、研究内容、規模、専門性にかかわらず、すべての大学に適用できるように設計されている。この枠組みは、大学の職員個人、理事会、大学セクター全体、オランダの関連省庁にも適用されるとされる。

本フレームワークは、知識セキュリィリスクを評価するための基盤を提供するにあたり、リスクマネジメントについて詳しく説明している。以下にこの概要を示す。

(a) リスクマネジメントのプロセス

知識セキュリティは、既存のリスクマネジメントプロセスの中に組み込む必要がある。そうすることで、既存のプロセスの成熟度を高めることができる。知識セキュリティは学際的なリスク領域であるため、セキュリティのリスクマネジメントを包括的に行うための組織化が、このフレームワークの実施を成功させるための重要な条件となる。これには、例えば、以下のようなものが含まれる。

- 機密技術のある物理的エリアへのアクセス
- リスクの高いテーマ／トピックに関する職員の採用前スクリーニング
- リスクの高い国からの高度なコンピューターシステムの調達
- 外部資金調達の評価
- 職員による内部脅威リスクへの対応
- 内部告発ポリシーに従った報告への対応

リスクマネジメントには、継続的なリスク管理プロセスとリスク分析という 2 つの方向性がある。いずれのプロセスにおいても、リスクの識別、リスク評価、リスク対応及びリスクの監視という 4 つのプロセスがある。通常、これらのプロセスには、以下が含まれる。

- リスクマネジメントに関する役割と責任を含む、リスクマネジメントプロセス及びステップの説明

- リスクカテゴリとそれに対応するリスクの許容度
- 様々なリスクに関する職員の意識向上プロセスとの関連付け
- リスクを識別するための標準化されたアプローチ及びテンプレート
- リスクの影響の大きさ及び起こりやすさに基づき、リスクを評価するための標準化されたアプローチ及びテンプレート
- リスク対応を選択するための標準化されたアプローチ
- 残存リスクと対策を追跡・監視するためのリスク登録簿
- リスクマネジメントプロセス全体の有効性を評価し、改善点を特定するための評価システム

(b) デューディリジェンス／予備調査

リスクマネジメントの一環としてのアドホックなプロセスの一つに、デューディリジェンス（共同研究のパートナーシップに関する入念な事前調査）がある。このようなプロセスを開始するタイミングは、新規提携の前と、提携の延長・更新時の 2 回が自然である。

継続的な提携に対してこのリスクマネジメントプロセスを適用するには、特に大規模大学では多額の投資が必要となる。したがって、知識セキュリティのリスクが高い場合にのみ、既存の提携関係を検討するのが賢明である。

(c) リスクの識別

知識セキュリティは、定期的なリスク識別プロセスの一部に含めるべきである。これらのリスクは複雑であるため、通常のリスク管理者に加えて、知識セキュリティの専門家が明確に関与する必要がある。リスクの識別は、知識セキュリティの側面に関するいわゆる「トリガーリスト」[215]を使用することで、効果的に実施することができる。これらのリストは、プロセスに関与する個人に対して、発生しつつある進展や重要であると思われる事例を想起させるために使用することができる。トリガーリストの例としては、以下が挙げられる。

- 高リスクの国家またはその他自由の無い国家
- 機密性が高い、または輸出規制リストに掲載されている研究・教育テーマ
- 大学自体で発生した事件、インテリジェンス・安全保障サービス、メディアなどの情報源から得た広範囲の情報
- 大学に関連する最近の地政学的・技術的動向

リスク識別のための入力として、以下を含めることもできる。

- 内部告発ポリシーからの報告書
- 国の情報サービスデスク、知識セキュリティ諮問チームその他の関連報告書
- 知識セキュリティに関連する過去の事件

[215] リスクの引き金となるもの。

・　新しいパートナーシップ
・　パートナーシップの全リスト

(d) リスク評価

リスクの起こりやすさとリスクの影響の大きさに関する概念を用いてリスクを評価することにより、当該機関にとってどの程度大きなリスクであるかを判断することができる[216]。評価が困難なリスクが識別された場合には、シナリオに基づくアプローチをとることができる。以下は、知識セキュリティのリスクにより影響を受ける事項として考慮に値するものである。

・　学問の自由（自分の研究について発表したり話したりすることが許されること）
・　職員の価値観（性別、セクシュアリティ、個人的信条にかかわらず平等に扱われること
・　職員の身体的・知的自由
・　国家のイノベーション能力

(e) リスク対応

標準的なリスクマネジメントプロセスに従って、評価されたリスクへの対応を検討する。リスク対応は、通常、大学のリスク許容度に基づいて行われる。

標準的なリスク対応には、以下が含まれる。

・　リスクの受容：リスク登録簿に、リスク所有者の氏名、リスクを受容した終了日などの詳細を記録する。
・　リスク対策：リスク登録簿に、講じられた対策と、その対策により、どのようにして内在リスクから残存リスクへ移行させるかを含めて記載する。
・　リスクの回避：リスクを回避するという決定は、将来のリスクの管理に影響を与える可能性があることから、その詳細を記録することは有用である。
・　リスクの共有：大学は他の教育・研究機関、政府、あるいは保険会社とリスクを共有することができる。

(f) リスクの監視

識別・評価されたリスクへの対応後に、残存リスクの変化を監視する。残存リスクの変化は、基礎となるリスクの変化（起こりやすさと影響の変化）、またはリスク対応の有効性の変化（例えば、対策が有効でないことが判明した、またはリスク受容期間が満了したなど）により生じる。このプロセスにおいては、リスク登録簿を利用する。リスク登録簿には、少なくとも、固有のリスク、リスク対応、残存リスク及びリスク所有者の詳細が記載されている。定期的にリスクの見直しを行い、PDCA サイクルで、リスクの識別・評価・対応・監視

[216] オランダの多くの大学は、リスクに関する用語やリスクの影響分類の標準化に関して取り組んでおり、リスク評価を容易に行うことができるようである。

を繰り返す。

(2) National knowledge security guidelines

2023 年 4 月より、研究機関がファンディングに関する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。これにより、オランダにおいては「National knowledge security guidelines」が、知識セキュリティを確保するための国家的なガイドラインとして位置づけられたと考えられる。

本ガイドラインでは、国際共同研究を行う研究者が、知識セキュリティを確保するための検討事項、評価・分析の考え方、留意事項等について説明しており、これには、「脅威評価」、「リスク評価」及び「リスクマネジメント」の考え方が含まれる。

以下、「National knowledge security guidelines」で説明されている、「脅威評価」、「リスク評価」及び「リスクマネジメント」の考え方を示す。

(a) 脅威評価

国家権力者は、軍事目的や基本的価値観に反する目的のために利用できる知識や技術を獲得するために、さまざまな方法を用いている。例えば、中央管理下の人材プログラム、移住した同胞（または元同胞）への圧力、デジタル・スパイ活動、戦略的地位にある個人のリクルートなどがある。

大学間提携もまた、その手段として利用される。このような場合、学術パートナーは政府の延長として機能する。これによって、表向きは学術的なパートナーシップであるにもかかわらず、二重の意図が付与されることになる。国家主体が影響や干渉を目的とした活動を行うこともある。例えば、（その国に関する）意見に影響を与えようとしたり、好ましくないテーマに関する研究を妨げようとしたりする。

このような国々は、自国民に対する統制を維持しようとする。出身国から監視されているという知識は、関係する研究者や学生に不安をもたらす。そのような不安は、自己検閲や、学問的価値観の根幹を損なうことにつながりかねない。

(b) リスク評価

機関内の機微な知識領域を正確に特定することが重要である。例えば、軍事的応用のために特別に開発された知識や、デュアルユース技術などが挙げられる。デュアルユース技術のリストは有用な示唆を与えるが、網羅的なものではない。輸出規制の範囲外の知識分野も、機密性が高い可能性がある。例えば、AI、先端ロボット工学、量子技術などの領域である。

このような分野では、例えば大規模な監視プログラムに関連するなど、研究成果が非倫理的に利用されるリスクが高まる可能性がある。このようなリスクは、国独自に先端的な地位を占める技術領域や、国の重要なプロセスの継続に影響を与える技術及び実行可能な代替手段がないために国が依存している技術については、さらに大きくなる。

また、その機関が、研究面で国際的なリーダーである場合、その研究成果の知識移転に関連するリスクをもたらす領域を示すことも重要である。機密性の高い知識領域ごとに、以下

のような方法で簡単なリスク評価を行うべきである。

- 国家安全保障・テロ対策調整官（NCTV）、国家情報安全保障局（AIVD）、軍事情報安全保障局（MIVD）が公表している「国家アクター脅威アセスメント」（国家や国家に支援された行為者によって、どのような国家安全保障上の利益が害されるのか、あるいは害される可能性があるのか、また、どのような形で害される可能性があるのかについての洞察を提供するもの）[217]などの公的な脅威情報を利用して、その国のリスクプロファイルを推定することができる。国際的なランキングを参考にすることもできる。例えば、学問の自由や法の支配の尊重に関するランキングのスコアが低ければ、赤信号を出すべきである。スコアが悪いからといって、必ずしも当該国の機関との協力の可能性が否定されるわけではないが、適切な予防措置を講じることが重要である。
- デューディリジェンスの一環として、海外のパートナーやクライアントの背景を調べることが重要である。これには、インターネット上の情報不足や、その機関が誰にも知られていないという事実のようなシグナルに細心の注意を払うことが含まれる。
- クライアントや研究資金提供者がどのような動機で、特定の成果にどのような関心を持っているかも考慮する。徐々に金銭的（または他の形）依存の状況に持ち込まれる可能性に注意することが重要である。
- 安全保障上のリスクがある場合は、安全保障コーディネーターを関与させ、パートナーとの関与に関する決定が、組織の理事会によるパートナー受け入れ方針に含まれていることを確認することが重要である。

(c) リスクマネジメント

大学・研究機関の中央レベルで、リスクマネジメントのプロセスを規制することが望ましい。リスクのレベルによっては、より厳格なリスク分析が必要な場合もあり、意思決定はより高い中央レベルで行うべきである。

リスクマネジメントは、理事会レベルで、知識セキュリティ責任者を指名し、知識セキュリティ責任者を支援する関連専門知識を有する専門家で構成される知識セキュリティ諮問チームを設置することから始まる。オープンなセキュリティ文化の一環として、大学等職員は、セキュリティリスクの兆候を報告できるチームの相談員にアクセスできるようにするべきである。これらの相談員は、知識セキュリティに関するリスクに精通しているべきである。

理事会レベルに対して、セキュリティの影響を受けやすい研究の提携、資金提供、外国人博士課程学生や客員研究員に関する最新の情報を提供することが必要になるが、これは、機関内の効果的なリスクマネジメントの基盤を形成することになる。また、単独では問題がないと思われるような進展の累積的影響についても洞察することができる。

研究機関内にオープンなセキュリティ文化を作ることが不可欠である。このために、セキ

[217] AIVD, MIVD and NCTV, “Threat Assessment State-sponsored Actors 2,” November 2022.

ュリティに関する啓発キャンペーンが有効である。このようなキャンペーンは、可能な限り、研修、チームセッション、シミュレーションなどを通じて、対象のグループの経験とリンクさせるべきである。

2.13　チェコ共和国

2.13.1　チェコ共和国における「研究インテグリティ」に係る取組の特徴

チェコ共和国は旧東欧国であり、OECD（1995 年）・NATO（1999 年）・EU（2004 年）の加盟国である。2014 年のクリミア併合以後では、チェコにおけるロシアの干渉に対する懸念が高まり、様々な対抗措置が取られてきている。特に、ロシアからの脅威（偽情報、ハイブリッド脅威等）への対抗のため、また、2010 年代後半から「外国からの干渉」に対抗するための措置（ハイブリッド脅威対策の政府機関の設置、大学・研究機関への外国からの干渉を防ぐためのマニュアル文書の策定）が実施されてきている。

2.13.2　チェコ共和国における取組の背景と経緯

2017 年 1 月に、「テロ・ハイブリッド脅威対策センター（Centre Against Terrorism and Hybrid Threats）」）が、2017 年末の総選挙を妨害するロシアの偽情報キャンペーンを防ぐために内務省によって設立された。2022 年 8 月に同センターは、「ハイブリッド脅威対策センター（Centre Against Hybrid Threats）」と改称している。

2019 年、プラハ・カレル大学（Univerzita Karlova v Praze）にあるチェコ・中国センターは、大学が中国大使館から秘密裏に支払いを受けていたことが発覚し、閉鎖された。[218] この事件を受けて、カレル大学は、ハイブリッド脅威対策センターに、大学が外国からの干渉に対抗するためのマニュアルの策定を求めた。これを受け、2021 年にハイブリッド脅威対策センターは、チェコの学術セクターのための「外国からの干渉対策マニュアル」（Counter Foreign Interference Manual for the Czech Academic Sector）を策定した。[219]

また、同じく 2021 年には、国防省がロシアからのハイブリッドの脅威、ハイブリッド干渉に対抗するための国家戦略「ハイブリッド干渉に対抗するための国家戦略」（National Strategy for Countering Hybrid Interference）を策定した。ただし、この文書は研究セキュリティの問題には特に触れていない。[220]

2.13.3　チェコ共和国における取組の詳細

上記の「外国からの干渉対策マニュアル」は、プラハ・カレル大学（Charles University in Prague）の要請により作成された。このマニュアルの目的は、高等教育機関の学問の自

---

[218] Ingrid d'Hooghe, and Jonas Lammertink (2022). *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology.* Leiden Asia Centre. pp.14-17.

[219] Ministry of the Interior of the Czech Republic, Security Policy Department, and Centre Against Terrorism and Hybrid Threats. Counter Foreign Interference Manual for the Czech Academic Sector. 2022. <https://cuni.cz/UK-11805-version1-cfi_manual_for_the_czech_academic_sector.pdf>

[220] National Strategy for Countering Hybrid Interference <https://www.army.cz/assets/en/ministry-of-defence/basic-documents/national-strategy---aj-final.pdf>

由、権利、透明な資金調達を守ることである。このマニュアルに従うことで、学術界は学問の自由を守り、透明性を維持し、外部からの脅威に対する強靭性を築くことができると説明している。内務省のテロやハイブリッド脅威対策を担当する部署が作成しているため、外国から教員や研究者の持つ情報に不法にアクセスするためにどのような働きかけがあるのか、それにどのように対抗するべきか、など具体的な内容である。

なお、Ingrid d'Hooghe, and Jonas Lammertink (2022)によれば、このマニュアルは、内務省のハイブリッド脅威対策センターが単独で策定しているものであり、他の省庁や政府全体の取組の一環として策定されているものでも、また政府の方針という訳でもないとのことである。

本文書で説明されている主な項目は以下のとおりである。

・体系的な組織のレジリエンス構築

- 本マニュアルは、外国からの干渉に対するレジリエンス（回復力、対抗力）を強化するシステムの確立に重点を置いている。
- 教員の個人的責任と、大学による標準化された組織的対策の両方を奨励している。
- 外国からの干渉からの保護は、学問の自由と権利を維持するために極めて重要である。

・どのように外国からの干渉に対抗するためのシステムを作るか

- 外国からの干渉によるリスクを軽減するためには、リスク管理、デューディリジェンス、コミュニケーションと研修、ノウハウの共有、サイバーセキュリティへの取組が必要である。（表 2-18 参照）

・研究者個人に焦点を当てた外国からの干渉手法（表 2-19 参照）

このマニュアルでは、外国勢力が個人の研究者を標的にするために使用する様々な手法とそれへの対抗策を紹介している。このセクションの内容については、軍等の情報業務従事者を対象とする教本を参考に作成されているため、他国の同様の文書には見られない内容となっている[221]。

- ✓ 勧誘：秘密目的のために学識経験者をリクルートする。
- ✓ 聞き出し：会話を通じて機密情報を収集する。
- ✓ 個人情報の悪用：公開されているデータを悪用する。
- ✓ 危険な申し出：招待、贈り物、有料の研修、旅行などの便宜を提供する。
- ✓ 海外旅行中のリスク：海外旅行中の脆弱性。
- ✓ 脅迫と強要：個人を危険にさらす脅迫。

・個人の備え

- この文書は、外国勢力の影響力が自分にどのような影響を及ぼし得るかを個人が理解するのに役立つ。
- 自己防衛と認識に関する指針を提供する。

[221] このため、Ingrid d'Hooghe, and Jonas Lammertink (2022)では、インタビューでの関係者の声として、大学教員や研究者を対象とするマニュアルの内容としては必ずしも適切ではないとの意見が紹介されている。

このマニュアルの策定に当たっては、欧州連合、英国、米国、豪州などの他国の、研究インテグリティ・研究セキュリティに関するマニュアル、ガイドライン、規則等を参考にしたとのことである。以下のような文書が参考文献として掲載されている。

European Commission. Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organisations. DRAFT 20 February 2020.

European Commission. Press Release. A Europe that protects: good progress on tackling hybrid threats. 29 May 2019.Brussels.

Center for Development of Security Excellence. Defense Counterintelligence and Security Agency のウェブサイト（https://www.cdse.edu/）

University of Kentucky. Guidance Regarding Foreign Influence in University Research. <https://www.research.uky.edu/office-sponsored-projects-administration/guidance-regarding-foreign-influence-university-research>

University of California. Office of the President. Ethics, Compliance and Audit Services <https://www.ucop.edu/ethics-compliance-audit-services/compliance/research-compliance/foreign-influence.html>

Cornell University. Disclose Foreign Collaborations and Support. <https://researchservices.cornell.edu/proposal/disclose-foreign-collaborations-and-support>

UK Parliament. A cautious embrace: defending democracy in an age of autocracies. 2019.

Universities UK. Managing risks in Internationalisation: Security related issues. 2020.

HRK. Leitfragen zur Hochschulkooperation mit der Volksrepublik China（「中華人民共和国との大学間協力に関する主な質問」）. 2020.

表 2-18：どのように外国からの干渉に対抗するためのシステムを作るか：まとめ

- 高等教育機関とその職員に対する干渉のリスクは現実に存在することを認識してください。
- 貴機関において、干渉のリスクを軽減する責任者を特定してください。
- リスク分析に干渉のリスクを含め、各レベル（トップマネージャー、干渉のリスクが高まると特定された職員、その他の職員や学生）、組織単位、プロジェクト（これらは、その活動内容によって異なるレベルのリスクに直面する）ごとに評価してください。
- 既存の安全規則と推奨事項を分析してください。
- 外国干渉を減らすための戦略を立ててください。
- 「相手を知る」原則を日常業務に組み込んでください。
- 職員と学生のためのトレーニングシステムを準備してください。
- 干渉のリスクは時間とともに変化する可能性があるため、リスク分析を繰り返し行ってください。
- 国または教育当局の規制要件に従い、干渉に対する内部規則を適宜調整してください。
- 外国勢力からの教育機関の収入に関する登録簿を作成してください。
- 干渉に関する情報を定期的に評価してください。得られた知見や教訓を活用して、リスク軽減システムをさらに改善してください。
- 干渉を含むインシデントが発生した場合のコミュニケーション計画を作成してください。

● あなたの経験を他の機関と共有してください。 ● 安全な海外渡航、贈答品の受領、外国勢力と接する際の行動、および学生・職員の政治活動に関する明確な規則を定めてください。

出典：Ministry of the Interior of the Czech Republic, Security Policy Department, and Centre Against Terrorism and Hybrid Threats. *Counter Foreign Interference Manual for the Czech Academic Sector*. 2022. p.33.

表 2-19：個人に焦点を当てた干渉手法のまとめ

外国勢力の関心の的になっていませんか？考えられる警告のサインは以下を含む。 ● 知人が現れ、あなたの仕事や趣味、生活について標準以上の質問をし、あなたの仕事や生活について並外れた知識を示す。あなたの長年の知人や友人が、外国勢力のためにあなたの情報を得るために利用される可能性があることに注意してください。外国勢力と協力し始めた場合、外国勢力のためにあなたの情報を得るために利用される可能性があるので注意してください。 ● 外国の機関や会社から、思いがけない有利な仕事の依頼を受ける。 ● 他で入手できる書類を要求される。 ● 旅行先で、あなたの所持品、荷物、電子機器などが改ざんされた形跡を見つける。 ● 突然、持ち物や携帯電話、ノートパソコンなどから引き離そうとされる。 ● 突然、地位の高い人物に会わないかと誘われる。 ● 海外で働き始めた元同僚に突然会う。 ● あなたの職場の情報が外国勢力によって入手されている可能性がある兆候は、あなたの仕事上のパートナーがその主題について必要以上に知識を示すときです。
外国からの影響に対する防衛の基本原則を意識しよう： ● 誰もが外国勢力にとって興味深い存在になりうる。 ● どんな情報でも、外国勢力にとっては非常に興味深いものになりうる。一見些細な情報であっても、悪用される可能性がある。 ● 信頼できる友人や同僚の輪の外で出会う誰もが、外国勢力の利益のために働く可能性がある。たとえ長い付き合いの人であっても、その可能性は決して否定できない。この場合、言動やトピックの目立った変化に注意してください。 ● ネット上や他の場所で入手できるあなたに関する情報が、上記で定義したカテゴリーに該当することを確認し、コミュニケーション（E メール、電話、手紙など）においてこのルールに従うこと。 ● 異常な状況に陥ったり、勧誘の標的になったりしたと思ったら、慌てずに関連する連絡先に知らせること。外国の勢力に協力すればするほど、事態は悪化する可能性があります。

出典：Ministry of the Interior of the Czech Republic, Security Policy Department, and Centre Against Terrorism and Hybrid Threats. *Counter Foreign Interference Manual for the Czech Academic Sector*. 2022. p.53.

2.14　ニュージーランド

2.14.1　ニュージーランドにおける「研究インテグリティ」に係る取組の特徴

ニュージーランドでは、英国と同様に「Trusted research（信頼される研究）」として、研究インテグリティ（研究セキュリティ）の取組を実施している。

「Trusted research」の目的は、世界をリードするニュージーランドの研究・イノベーション部門が、知的財産、機密性の高い研究、個人情報を保護しながら、国際的な科学協力が最大限実施できるよう支援するためのものである。

「Trusted research」に係るガイドラインは、国のセキュリティ・クリアランスを管理する政府の特殊法人である Protective Security Requirements（以下、PSR）[222,223]が、サイエンス・ニュージーランド[224]やニュージーランド大学協会ともに協力し作成した。「Trusted research」に関連するガイドラインは、下記となる。

ⅰ）Trusted Research - Guidance for Institutions and Researchers（信頼される研究－研究機関と研究者のためのガイダンス）(2023 年 8 月)

ⅱ）TRUSTED RESEARCH - Protective Security Requirements – Guide for Senior University Leaders in Aotearoa New Zealand（信頼される研究：セキュリティ保護要件－アオテアロア・ニュージーランドの大学執行部のための手引き）(2022 年 9 月)

2.14.2　ニュージーランドにおける取組の背景と経緯

ニュージーランドの安全保障を所掌する政府機関に「ニュージーランド安全保障情報局（The New Zealand Security Intelligence Service：以下、NZSIS)」がある。NZSIS は、ニュージーランドとニュージーランド人の安全を守ることを使命に、政府の優先事項に沿って情報を収集および分析し、意思決定者に国家安全保障に関する助言、セキュリティサービスを行っている[225]。NZSIS は、優先的な政策課題として、①スパイ活動および外国から

---

[222] PSR は、2014 年に設立された特殊法人（Crown Entities）であり、政府のセキュリティ・ポリシーの枠組みの中で、国のセキュリティ・クリアランスのプロセスを管理している。PSR の取組により、ニュージーランド政府組織は、信頼と信用に支えられた環境を得ることを目的としている。

[223] PSR は、特殊法人（Crown Entities）の一つである。特殊法人は、広範な公共部門に対して政府に代わってサービスを提供する。各法人は、閣僚から独立した理事会により統治され、設立法令に定められた特定目的、機能を実現させることが求められている。PSR の所管は、ニュージーランド安全保障情報局（NZSIS）であり、人的、情報、物理的セキュリティの管理に関する政府の要求事項に取り組む。（https://www.publicservice.govt.nz/system/crown-entities/all-of-government-requirements-and-expectations-on-statutory-crown-entities/security2/）

[224] サイエンス・ニュージーランドは、クラウンリサーチ研究所とキャラハン・イノベーション（Callaghan Innovation）〈クラウン企業〉により運営される社団法人である。クラウンリサーチ研究所（CRIs：Crown Research Institutes）は、1992 年に政府が設立した国有企業法人〈1992 年 CRIs 法〉で 7 つの研究所を傘下に持つ研究機関（研究会社）である。研究機関の予算は公的セクター、民間セクターの両方から負担されるほか、ニュージーランドの競争的研究資金制度を通じて資金を得ている（出典：JST/CRDS「ニュージーランドの研究開発システムの概要」、2018 年 12 月 24 日）。キャラハン・イノベーションは、2012 年にキャラハン・イノベーション法に基づき設立されたエージェント（Agent）である。取締役会は研究・科学・イノベーション大臣に任命され、CRI の取締役会よりも王室の管理下に置かれている。（https://sciencenewzealand.org/）

[225] ニュージーランド安全保障情報局（NZSIS）は、ニュージーランドとニュージーランド人の安全・安心を守ることをミッションとし、ニュージーランドの国家安全保障の保護、国際関係と福祉、経済的福祉

の干渉への対処（Countering espionage and foreign interference）、②暴力的過激主義とテロリズムへの対処（Countering violent extremism and terrorism）、③国家安全保障の評価（National security assessments）、④安全保障（Protective Security）からなる[226]。

NZSIS の「安全保障」の取組は、ニュージーランドの人、情報、資産を守るため、政府へのセキュリティ・クリアランス・サービスの提供、ニュージーランドの諜報機関である New Zealand Intelligence Community（NZIC）[227]や他の政府機関に対するセキュリティ防護サービスを提供するとともに、政府のセキュリティ防護要件のフレームワークを管理している[228]。これらセキュリティ・クリアランス等のプロセスは、NZSIS が管理している PSR が関わる。

「研究セキュリティ」に関する取組は、政府機関では PSR が中心的に関わり、「Trusted Research」を推進した。2023 年 8 月には、「Trusted Research: Guidance for Institutions and Researchers」を、サイエンス・ニュージーランド、ニュージーランド大学協会とともに作成し公表した。

ニュージーランドの「研究セキュリティ」、「Trusted research」の取組は、ニュージーランド大学協会で先行して行われた。2021 年 12 月には、英国国際大学協会（Universities UK International : UKKi）の「Joint statement from convening higher education associations（高等教育協会の会合からの共同声明）」に共同声明発表者に名を連ね、安全、安心、そして持続的な国際化を支える取組を連携して実施することについて、共同で宣言した[229]。また、2022 年 9 月には、信頼される研究（Trusted Research）を進めるため、シニアリーダー（大学執行部）向けと、研究者向けのガイドブック「TRUSTED RESEARCH - Protective Security Requirements – Guide for Senior University Leaders in Aotearoa New Zealand」を策定し公表した。

2.14.3　ニュージーランドにおける取組の詳細

(1)　PSR、サイエンス・ニュージーランド、ニュージーランド大学協会「Trusted Research: Guidance for Institutions and Researchers」

本ガイドは、政府機関である PSR が、サイエンス・ニュージーランド、ニュージーランド大学協会との協力により作成し公表した。

等に係る任務を実施している。具体的には、情報収集・分析・評価、安全保障に係るサービス・助言・支援、他の公的機関の機能を促進するための協力、差し迫った脅威に対応するための他機関との協力を実施している。ニュージーランドの国家安全保障情報に係る戦略（「National Security Intelligence Priorities - Whakaarotau Marumaru Aotearoa (NSIPs)」）は 2 年毎に見直される。（https://www.nzsis.govt.nz/about-us/）

[226] NZSIS の優先課題は、本文に挙げた 4 つのほか、2019 年 3 月に発生したクラストチャーチ・モスクのテロ攻撃に関する王立調査委員会の勧告にも関わる。

[227] NZIC は、自由で開かれた民主的社会を守るため、国家情報、評価、安全保障の中核機能を有し、インテリジェンスに基づく洞察と助言を行っている。（https://www.nzic.govt.nz/）

[228] NZSIS における「安全保障」の取組（https://www.nzsis.govt.nz/our-work/protective-security/）

[229] PwC あらた有限責任監査法人（2022）「研究インテグリティ（Research Integrity）に係る調査・分析報告書」, 2022 年 3 月.

信頼される研究（Trusted Research）を進める背景には、世界をリードするニュージーランドの研究・イノベーション部門が、知的財産、機密性の高い研究、個人情報を保護しながら、国際的な科学協力を最大限に活用できるよう支援することを目的としている。

ニュージーランドの国際共同研究システムのインテグリティを確保することは、研究・イノベーション部門の継続的な成功に不可欠である。

このガイダンスは、特に STEM（科学、技術、工学、数学)、イノベーション、デュアルユース技術、新興技術、商業的にセンシティブな研究分野の研究者に関連するものである。

本ガイドは、「Trusted research」の実施に向けて、ニュージーランドの研究・イノベーションにおける潜在的なリスクを理解し、研究者、大学、研究機関、産業界のパートナーが国際共同研究に自信をもって潜在的なリスクに対して決断できるよう支援することにある。ガイドは、1）研究の保護、2）ニュージーランドの研究に対するアプローチ、3）なぜ研究を保護するか、4）あなたの研究を守る方法からなる。

【本ガイドの構成】
1）研究の保護
2）ニュージーランドの研究に対するアプローチ
3）なぜ、研究を守るのか
　○　誰からリスクを受けるのか？
　○　どのように狙われているか？
　○　研究に対するリスクとは？
　○　あなたの研究はどの程度、狙われているか？
4）あなたの研究を守る方法
　○　研究パートナーとの協力
　○　法的枠組みを利用する
　○　研究者の安全確保を支援する

【ニュージーランドの研究に対するアプローチ】

ニュージーランドの研究・イノベーション部門は、国際的な研究パートナーシップ等を踏まえ、世界中から研究資金と研究投資を集めている。一方で、国際的なパートナーシップには、リスクがあり、国際的な研究・イノベーション活動の取組にあたっては、評判の低下、知的財産（IP）の損失、ニュージーランドの国益を損なうことを防ぐ必要がある。

【なぜ、研究を守るのか】

すべての研究がリスクにさらされる可能性があるが、共同研究や応用研究は脆弱である。共同研究は、ニュージーランドとは利害の異なる国の組織・機関に悪用される可能性があり、敵対的な意図を持つ人々が専門知識や IT ネットワーク、研究にアクセスする機会がある。また、応用研究は、商業的な応用を開発する場合に悪用され、知的財産を失う可能性がある。研究者個人では、研究に対する妨害（または損失)、知的財産を制限する可能性があり、研

究者としての評判や研究の実証能力に影響を与える。このことから、ガイドでは、どのようなリスクがあるかを示した。

表 2-20：研究・イノベーション上のリスク

項目	リスクの内容
誰からのリスクにさらされているか？	外国の国家主体は… ● 他国に対する経済的、軍事的、技術的優位性を高める研究・イノベーション基盤を開発する機会を求めている。 ● 政権の安定を優先し、国内の反体制、政治的反対、メディアの抑圧に重点を置く。 ● 政権の安定を維持するため、技術的・安全保障的な優位性を確保する。
どのように狙われているか？	● 外国の国家が、軍事的、商業的、技術的な利益の追求のため、ニュージーランドの大学や組織を標的に、個人情報、研究データ、知的財産を盗用しようとする。 ● 国際共同研究は、外国の国家行為者に、従来のスパイ活動やサイバーによる侵害活動を行うことなく、研究から利益を得る機会を提供する。 ● 外国の国家主体は、人、IT ネットワークへのアクセス、研究（機密性の高いアプリケーションを有する可能性のある研究）への参加機会を共同研究で得ることができる。 ● 外国の諜報機関にとり、学会等のイベントや研究派遣はニュージーランドの研究者にアクセスするための容易な経路となる。 ● フィッシングメールのようなサイバー攻撃によって標的にされることもある。
研究に対するリスクとは？	● 信頼の喪失（研究データの盗用や不適切な保護、悪用等により、公的機関、民間企業の信頼の喪失） ● 完全性と法令遵守の低下（ニュージーランドの輸出規制〈Customs and Excise Act 2018〉に従わない等） ● 単一の研究資金源への過度な依存 ● 資金提供機会の損失と経済的損失（外国がニュージーランドの研究者の成果を盗用したことが発覚した場合、盗用された研究者自身や研究者が所属する研究機関は将来の研究資金を集めることが難しくなる可能性がある。また、研究者の研究成果を非倫理的な目的で悪用したり、競合他社が研究者のスポンサーの研究データや情報にアクセスした場合、研究者自身が経済的損失に直面する可能性がある）

項目	リスクの内容
	● 評判の低下（外国が研究者自身の成果を軍事的または権威主義的な目的で利用したことが明らかになることで、評判が損なわれる可能性がある〈国を含めて〉）
あなたの研究はどの程度、狙われているか？	あなたの研究が… ● 商業的な機密性があるか。 ● 特許の可能性があるか。 ● 機密性の高い防衛技術や国家安全保障技術に関連しているか。 ● 将来的にデュアルユースや非倫理的な用途に使われる可能性があるか。

出典：PSR、サイエンス・ニュージーランド、ニュージーランド大学協会「Trusted Research: Guidance for Institutions and Researchers」より未来工学研究所作成.

【あなたの研究を守る方法】

研究者は、自身の研究を保護し、法的義務を果たしていることを確認し、 研究協力について十分な情報を得た上で意思決定できる。そのためには、研究パートナーとの共同研究に係る情報管理（知的財産の保護、国際共同研究に係る情報取得、サイバーリスクの管理）、法的枠組みの利用（契約、輸出規制、プライバシー要件の理解）、研究者の安全確保（個人情報および研究データの保護、海外の研究者との協力〈適切なビザの取得等〉、海外の学会参加）等が必要であるとした。

(2) ニュージーランド大学協会「TRUSTED RESEARCH - Protective Security Requirements - GUIDE FOR Senior University Leaders in Aotearoa New Zealand」

ニュージーランド国内の 8 大学では、「Trusted Research」（信頼される研究）を進めるため、ニュージーランド国内大学の執行部（シニアリーダー）が、信頼される研究、セキュリティ保護要件について、前述の「TRUSTED RESEARCH - Protective Security Requirements (GUIDE FOR Senior University Leaders in Aotearoa New Zealand)」をとりまとめた。本ガイドは、大学において組織内部、教職員、学生等との対話を始める際に役立つものとして作成された。

ニュージーランドを取り巻く研究・イノベーション環境は、開かれた共同研究、学問の自由、個人や組織が独自に設計・実施する研究に価値を置いている。ニュージーランドの研究・イノベーションセクターは、グローバルな知識創造と交換のエコシステムの一部として、数多くの国際的な共同研究を行っている。その結果、経済的、技術的、社会的、健康的、文化的国益をもたらしている。

本ガイドは、地政学的環境の複雑さが増す中で、主権国家が国民、知識、国益を守るため、国際的パートナーシップに伴う研究活動のリスクをどのように管理するかを示したものである。本ガイドは、ニュージーランドの大学機関は、国益、法令遵守、国際条約の遵守、ニュージーランドの安全保障の維持に係る責任を有することを認識するとともに、大学機関

が有する学問的価値（教職員や学生の学問の自由、言論の自由、マオリの権利、利益、文化的価値の保護）をどのように守り、外国からの干渉、軍事利用のための研究の流用・悪用リスクにどのように対処するかを明確にした。

ニュージーランドでは、国際的な研究協力に対して、制限的なアプローチではなく、豊かな研究環境を実現するために研究協力を実施可能とするためのアプローチとして、「Trusted Research - Protective Security Requirements（TR-PSR)」（信頼される研究ーセキュリティ保護要件）と名付けた。

本ガイドでは、大学の学術的価値とニュージーランドの国益（タンガタ・ワヌアを含むアオテアロア・ニュージーランド[230]）の保護、研究の不正流用・盗用、国際的な研究パートナーシップの潜在的リスクの管理と外国からの干渉影響を最小限に抑えること、輸出規制や政府の保護セキュリティ要件等への対応を目的にガイドラインを策定した。

【ガイドの構成】
1）アオテアロア・ニュージーランドの文脈を踏まえた「信頼される研究（TR-PSR)」実施のための価値観と原則
2）何を考慮するか
3）大学におけるツール

本ガイドは、ニュージーランドの大学の執行部が「信頼される研究」をどのように考えるかを対象としたもので、「信頼される研究」を実施するための価値観・原則を理解し、下記に示す項目を執行部向けの検討事項とした。

［ガイドの助言項目：ワイタンギ条約の理解・認識／良い統治形態／政策・計画・リスク評価／法規制の遵守／人材・資産・評判の保護（教職員と学生、キャンパスの資産、パートナーシップ）／コミュニケーションと研修］

次いで、「信頼される研究」を適切に実施するための大学向け支援ツール（研究契約のリスクアセスメント、リスクマネジメント・フレームワーク）を示した。

【信頼される研究の価値観・原則】

本ガイドでは、「信頼される研究（TR-PSR)」の価値観と原則として、下記を挙げている。

●ワイダンギ条約（Te Tiritio Waitangi）[231]の原則と、“土地の人々”（Tangata whenua）

[230] アオテアロア：ニュージーランドのテレオマオリ（マオリ語）の国名のこと。〈https://www.newzealand.com/jp/maori-culture/〉

[231] ワイダンギ条約は、1840 年 2 月 6 日にニュージーランド北島のワイダンギにて、先住民のマオリと英国王権との間で締結された条約。条約の内容は、全てのマオリは英国女王の臣民となり、ニュージーランドの主権を王権に譲ること、マオリの土地保有権は保障されるがそれらの土地は全て英国政府へのみ売却されること、マオリは英国国民としての権利が認められることである。2023 年 10 月の総選挙後の国民等との連立交渉で ACT 党の先住民政策の一部実現に合意し、現政権の連立合意にワイダンギ条約の再解釈が盛り込まれている。（https://ja.wikipedia.org/wiki/%E3%83%AF%E3%82%A4%E3%82%BF%E3%83%B3%E3%82%AE%E

とワイダンギ条約の教育プログラム（Tangata Tiriti）[232]の関係の認識
●共同研究、連携研究、国内研究、国際研究を可能にするガイダンスの提供（研究インテグリティを含む）
●アオテアロア・ニュージーランドの法令遵守：機密技術および知的財産の輸出管理
●アオテアロア・ニュージーランドの安全の維持・良き地球市民の義務の認識（国益の保護と、関連する国際条約・協定の支持）
●開かれた共同研究、学問の自由、個人・地域・組織が独自に構想・実施する研究の推進
●リスク管理、オープンな共同研究、機会の追求のバランス
●信頼される共同研究の推進と、責任ある研究、行動規範、倫理、インテグリティの認識
●マタウランガ・マオリ（マオリ族の伝統的知識）[233]を含め、マオリ語に対する認識の深化
●太平洋におけるアオテアロア・ニュージーランドの背景の認識
●全ての研究分野と先住民研究を包含すること
●研究者、研究に関わる人々、研究コミュニティに影響を与える人々を守る（知的財産、マタウランガ・マオリ（マオリ族の伝統的知識）、研究データ、個人情報、教職員・学生の福利厚生を保護）
●教育と情報共有を通じて教職員・学生の意識と知識を深める
●ガイダンスの継続的な見直し・更新の必要性の認識（地域、国、国際的な法的環境のダイナミックな進化に対応）
●国にとらわれない、コンテクストを意識した地政学的観点を取り入れる

【信頼される研究が適用されるケース】

「信頼される研究（TR-PSR）」が適用されるケースは、機密性の高い共同研究や応用研究である。これらの研究活動は、国内および国際的な法的・文化的なコンプライアンス要件を満たすために、リスク評価と継続的なモニタリングとレビューが必要とされる。「信頼される研究」として研究活動を考慮して進めることは、国や組織の評判、先住民の権利（知的財産、マタウランガ・マオリ（マオリ族の伝統的知識）、先住民のノウハウ、先住民の権利・利益・文化的価値）、国益や安全保障等を損ねることや、国際条約への違反を防ぐためのものである（研究が利用されることによる損失を防ぐ）。共同研究や応用研究は、ニュージーランドの研究者、研究コミュニティとは異なる利益や動機を持つ外国の個人・組織、また政治的、文化的、政策的に異なる国の人々により不正利用や悪用されやすい。このため、機密性の高い研究が必要である。

6%9D%A1%E7%B4%84）　（2024 年 1 月 26 日調べ）
[232] ワイダンギ条約に関する教育プログラムのこと。教育プログラムは、ワイダンギ条約に関する簡単で正確な情報を提供するもので、非マオリとマオリの関係を構築するために、新規移住者や年配の移住者に教育（条約、憲法）を促すためのものである。（http://www.treatypeople.org/about/）
[233] mātauranga Māori（マタウランガ）は、マオリ族の伝統的な知識を表し、知識は学際的、総合的なものである。（https://en.wikipedia.org/wiki/M%C4%81tauranga_M%C4%81ori）　（2024 年 1 月 26 日調べ）

【信頼される研究を行う上で考慮すべきこと】

「信頼される研究（TR-PSR）」に関する教育は、現在および将来の教職員や学生にとり、研究システムの法的、文化的、コンプライアンス的な枠組みの理解や外国からの干渉に関するリスクを管理する上で最善の方法である。政策においても、デュアルユース、政治的リスク、文化的センシティブなテクノロジー研究等、より広範な研究に影響を与える新たな法律や規制を考慮したハイレベルな政策ガイダンスの開発も必要である。

表 2-21：「信頼される研究」のために考慮すべきこと

評価項目	サブ項目	大学（執行部）が考慮すべきこと
良い統治形態	—	● 既存組織のガバナンス構造を検討する。TR-PSR のためのハイレベルの監督、意思決定を特定する ● ガバナンスグループの設置 ● 執行部から TR-PSR 要件の監督者と執行チームメンバーを特定 ● 執行部が国際共同研究、パートナーシップの安全確保 ● 共同研究に関連する風評、倫理、国益のリスクに関する議論 ● ラインマネジメントの確保
政策、計画、リスクアセスメント	—	● 既存組織のポリシーの枠組みの見直し ● 方針の新規作成／修正：研究方針、人事、財務、サイバーセキュリティ、知的財産、倫理、研究データ管理、入学方針、実務等 ● リスク評価・管理（執行部のリスク許容度、コスト/便益評価） ● 監督の実施、より高い保護が必要な研究の特定 ● 潜在的な脅威の特定
法的、規制、コンプライアンス	—	● 輸出管理制度の変更の影響評価 ● 輸出管理モデルの作成 ● キャッチオール規制の実施やコミュニケーションチャンネルに関して外務貿易省と継続的な関わりを確保 ● 研究協力に影響を及ぼす国際的な協力枠組みに対する理解とリソース開発（組織のプロセスと監視がこれらを考慮） ● リスク管理の実践（2005 年の公文書法に沿って）
人材、資産、評判の保護	人材	● TR-PSR に関連するリスク管理上の問題を特定し、人事部に報告（インサイダーの脅威、利益相反/外部利害の開示、外部利益、複数の所属・仕事・資金源に関するリスクの考慮） ● 海外に出張する教職員・学生に関連する TR-PSR プロトコール、輸出管理（キャッチオール規制を含む）の説明と訓練の実施（国外への情報・データの持ち出し、国外でのアクセス制限） ● 海外渡航リスク、機密情報やデータのセキュリティの助言

評価項目	サブ項目	大学（執行部）が考慮すべきこと
		● リソースやトレーニングの開発（採用、配属、導入プログラム） ● 海外から客員研究員を招聘する際のデューディリジェンスの実施方針とプロセスの策定
	資産	● マオリ族のデータや個人情報の保護（TR-PSR や輸出規制が研究データ管理の方針や実務に与える影響を検討 ● 機密性の高い研究に必要なサイバーセキュリティのリスク管理とインフラの検討・実施 ● アクセスレベルの制限・管理の検討
	評判	● 効果的なデューディリジェンスの方法を検討 ● リスクに応じた政府関係機関への相談
コミュニケーションと研修	―	● 大学内外の戦略とリソースの検討 ● 内部コミュニケーションと関連組織 ● コミュニケーションチャンネルの確立・維持 ● 海外の大学・研究機関との連絡網の確立・維持・共有 ● TR-PSR メカニズムの定着

出典：ニュージーランド大学協会「Trusted Research：Protective Security Requirements」より未来工学研究所作成.

【大学機関向けツール】

本ガイドでは、「信頼される研究」に係るリスクマネジメント・フレームワークを提供している。リスク評価にあたっては、「信頼される研究リスクマトリクス」[234]、リスク対応計画のガイダンスツール（「信頼される研究リスク登録簿」[235]）を作成している。

例えば、リスクマトリクスの例を表 2-22 に示す。リスクマトリクスは、「信頼される研究」に最も関連するリスク区分に対して 4 つの段階のガイダンスを反映したものである。区分は、学問の自由、先住民および文化的プロトコール（マウリ、太平洋文化を含む）、財政、自然環境、情報損失（知的財産、個人情報を含む）、IT・インフラ、機関の評判、運営上の混乱、政治的／国家的アイデンティティ、研究戦略、セキュリティとウェルビーイング（学生）、セキュリティとウェルビーイング（職員）、信頼される研究の法規制等からなる。なお、この区分自体は、例示であり、区分間の相互依存関係を考慮する必要がある。

各区分に対するリスク評価の段階は、軽微（Minor）、中程度（Moderate）、重大（Major）、深刻（Severe）の 4 つの段階を設定している。例えば、学問の自由に対しては、軽微（わずかな影響：先住民族の文化的尊重に対する軽度の懸念）、中程度（いくつかの影響：学問の

234 TR-PSR Risk Matrix (https://www.universitiesnz.ac.nz/sites/default/files/uni-nz/TR-PSR%20Risk%20Matrix.pdf)
235 TR-PSR Risk Register (https://www.universitiesnz.ac.nz/sites/default/files/uni-nz/TR-PSR%20Risk%20Register.pdf)

自由に対する懸念)、重大（かなりの影響：学問の自由に対する深刻な懸念)、深刻（重大な影響：学問の自由に対する深刻な懸念）等と評価定義を設けている。そして、これら区分のリスクの発生可能性について、「非常に高い－高い－可能性あり－可能性が低い」の 4 つの状況で評価する。リスクマトリクスは、リスク区分に 2 つの段階で評価するツールと言える。

表 2-22：「信頼される研究（TR-PSR)」リスクマトリクス

	軽微	中程度	重大	深刻
学問の自由				
先住民および文化的プロトコール				
財政				
自然環境				
情報損失（知的財産、個人情報を含む）				
IT・インフラ				
機関の評判				
運営上の混乱				
政治的／国家的アイデンティティ				
研究戦略				
セキュリティとウェルビーイング（学生）				
セキュリティとウェルビーイング（職員）				
信頼される研究の法規制				

出典：Universities New Zealand「TR-PSR Risk Matrix」より未来工学研究所作成。
（https://www.universitiesnz.ac.nz/sites/default/files/uni-nz/TR-PSR%20Risk%20Matrix.pdf）

2.15　韓国

2.15.1　韓国における「研究インテグリティ」に係る取組の特徴

韓国における、研究成果等の海外への遺漏防止のための取組は、研究活動の国際化の進展に応じて、主として産業部門を対象に実施されてきた。しかし、近年では、韓国の大学や研究機関に対して、海外からの共同研究の申し出が増加してきており、セキュリティ上の懸念の声が挙がっていること、また諸外国において研究インテグリティへの対策が進んできていることから、大学・研究機関における対策が取り組まれるようになってきた。

韓国は、半導体など高度の科学技術力を持ち、中国の隣国であると同時に、米国の同盟国として、科学技術セキュリティを確保するための政策に取り組んでいる。2023 年 6 月には「国家研究開発事業におけるセキュリティ対策規則」（국가연구개발사업 보안대책）を科学技術情報通信部など 8 省庁の共同告示基準として定めた。また、諸外国の研究インテグリティの取組についての事例調査等も実施されるようになっている。

2.15.2　韓国における取組の背景と経緯

韓国は、技術の進歩と国際協力の増加に伴い、研究セキュリティの重要性を認識し始めた。初期の対策ではサイバーセキュリティと知的財産権の保護に重点が置かれていた。韓国は、研究セキュリティを強化し、研究活動への外国からの干渉を防ぐために、いくつかの措置を講じてきた[236]。これらの措置は、機密技術や知的財産を保護し、韓国国内で行われる研究が国家安全保障上の利益に合致させることを目的としている。

OECD の研究インテグリティ・セキュリティについての報告書（2022 年）によれば、これまで、韓国では、「研究インテグリティ」あるいは「研究公正」（research integrity）については大学・研究機関の周知の概念であるのに対して、研究セキュリティ（research security）は、産業部門と関連した用語として理解され、対応されてきたという[237]。

産業技術については「対外貿易法」（대외무역법）、「産業技術の流出防止及び保護に関する法律」（산업기술의 유출방지 및 보호에 관한 법률）などで技術流出が管理されている。

- 対外貿易法：戦略物資に指定された技術の輸出時、産業部または関係部署の許可が必要。
- 産業技術流出防止法 ： 国家核心技術（국가핵심기술）等と指定され、新技術等と公示・認証される技術の場合、保護対策を樹立し、国家核心技術の場合には輸出統制・買収・合併などの統制を行う。[238]

---

[236] 研究事業セキュリティ管理規定[施行 2009. 2. 20.] [国立環境科学院例規第 453 号、2009. 2. 20.、一部改正] <https://www.law.go.kr/LSW/admRulInfoP.do?admRulSeq=2000000073597>
Ministry of Science, ICT, and Future Planning
「国家研究開発事業セキュリティ管理標準マニュアル」（국가연구개발사업 보안관리 표준 매뉴얼）
Manual of security management on national research development project. 2014 年 4 月

[237] OECD. *Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers. June 2022 No. 130. p.65.

[238] 科学技術情報通信部 研究制度革新課、KISTEP（韓国科学技術企画評価院）制度革新センター「国際

他方、近年、韓国の大学や研究機関に対して、中国からの共同研究の申し出が増加してきており、セキュリティ上の懸念の声が指摘されるようになっている。2024 年 2 月 6 日の中央日報の記事[239]によれば、先端技術関連学科を運営する韓国内主要大学 10 校を確認した結果、相当数の大学がここ数年、中国の大学から研究協力の提案を受けたことが分かった。正式に中国と韓国の大学間の共同研究や業務協約（MOU）の締結を提案したり、学会の人脈などを利用して教授陣に直接接触が行われたりしている。記事は、このように、「半導体・ディスプレイ・二次電池など先端技術関連の国内大学研究陣が中国の大学から破格の共同研究提案を受けるケースが増えている。海外大学との協力は一般的だが、国内の研究・開発段階でのセキュリティ基準とガイドラインが曖昧で、核心技術の流出に対する懸念が高まっている」と指摘する。

また、本報告書の他のセクションで説明しているように、米国、欧州連合、豪州など、あるいは日本において研究インテグリティについての対策も進んでいる。

このような背景の中で、韓国においても、大学や研究機関における規程策定や研修実施等を義務付けるなど、必要な対策が取られるようになってきている。

2022 年 10 月に、韓国政府は、経済安全保障と国家安全保障などの観点から戦略的に技術主導権を確保すべき「国家必須戦略技術」（국가 필수전략기술）を指定し、「国家戦略技術育成方案」（국가전략기술 육성 방안）を発表した（国家科学技術諮問会議全員会議）。その際には、「韓国は主要国間で共有される中核的研究資産の非合法的な情報漏洩を避けるため、研究セキュリティ（연구보안）のシステムを強化」し、「特に、戦略技術国際協力の過程で生じる研究セキュリティ事項など、海外事例分析を通じて研究者ガイドライン（연구자 가이드라인）を策定・提示する計画である」と発表した[240]。

また、2023 年 3 月には、「国家戦略技術育成に関する特別法」（국가전략기술 육성에 관한 특별법）を制定した。国家戦略技術を迅速に開発するための研究開発支援政策と国家戦略技術の研究開発事業に対する特例の根拠を設け、戦略技術育成基盤の造成、人材育成、国内外の協力強化などを推進する体系を構築している[241]。

続いて、2023 年 11 月に、「国家研究開発事業におけるセキュリティ対策規則」（科学 ICT 省告示第 2023-39 号等（施行日：2023 年 11 月 20 日））を、科学技術情報通信部など 8 省庁の共同告示基準として定めた。この規則は、後述のように、国家研究開発事業について、

研究協力時の研究資産流出防止のための主要国の政策事例集」（국제연구협력 시 연구자산+유출 방지를 위한 주요국+정책사례집）2023 年 6 月

[239] 中央日報記事「50 억 줄테니 같이 연구하자" 中대학 수상한 파격 제안」중앙일보. 2024 年 2 月 6 日（50 億ウォン出すから一緒に研究しよう：中国大学からの破格のオファー）
<https://www.joongang.co.kr/article/25227144#home>

[240] Ministry of Science and ICT. Press release “Korea to announce national strategy to become a technology hegemon” 2022/10/28.
<https://www.msit.go.kr/eng/bbs/view.do?sCode=eng&mId=4&mPid=2&pageIndex=&bbsSeqNo=42&nttSeqNo=746&searchOpt=ALL&searchTxt=>

[241] 科学技術情報通信部 研究制度革新課、KISTEP（韓国科学技術企画評価院）制度革新センター「国際研究協力時の研究資産流出防止のための主要国の政策事例集」（국제연구협력 시 연구자산+유출 방지를 위한 주요국+정책사례집）2023 年 6 月

機密技術や研究成果を外国のスパイ活動や不正アクセスから保護することを目的とし、中央省庁は委員会を設置し、事業についてのセキュリティリスクを判断し、高いものについてはセキュリティ課題として指定する。研究機関においては、セキュリティ対策を策定して、セキュリティ総括担当者を任命し、研究者に研修を受けさせるなどの必要なセキュリティ対策を行うことが求められている。

2.15.3 韓国における取組の詳細

OECD の STI Compass の STI policies for research security in Korea（韓国の研究セキュリティのための STI 政策）には、韓国特許保護庁における取組と、上記の「国家研究開発事業におけるセキュリティ対策規則」の 2 つが挙げられている。[242]

また、前述のように、政府の科学技術政策の研究所が研究インテグリティについての海外事例調査を開始している。

(1) 「国家研究開発事業におけるセキュリティ対策規則」の制定（2023 年）

このうち、「国家研究開発事業におけるセキュリティ対策規則」（국가연구개발사업 보안대책）[243]は、2023 年に定められた。担当省庁は、科学技術情報通信部（Ministry of Science and ICT (MSIT;과학기술정보통신부)等である(科技部など 8 省庁の共同告示基準)。

国家研究開発革新法（국가연구개발혁신법）上のセキュリティ対策を講じ、政府研究助成金による研究プロジェクトに関する重要情報を保護するための規則と位置付けられる。

大学・研究機関は、セキュリティ対策を設ける必要があり（第 4 条)、セキュリティ対策総括担当者を指定するとともに（第 5 条)、セキュリティ対策を審議するために研究セキュリティ審議会を設置・運営することが求められる（第 6 条)。また、セキュリティ教育を教職員に対して実施することも必要である（第 7 条)。

また、未来核心技術（미래핵심기술）などのセキュリティ課題を遂行しているか、遂行より 3 年を経過していない研究者が、①セキュリティ課題に関して外国機関と接触する場合には報告が、②外国との共同研究遂行の場合には事前承認が求められる（第 8 条)。報告や事前承認は所属機関の長が実施し、その後に、所属機関から政府省庁等に対して報告が行われる。

外国研究者等のセキュリティ課題への参加については、韓国人だけでは目的達成が難しい場合、補足的に認めることを原則とすること等が規定されている（第 9 条)。

---

[242] OECD. STPI Compass (portal on research security). Korea. <https://stip.oecd.org/stip/research-security-portal/policy-initiatives?conceptUris=http:%2F%2Fkim.oecd.org%2FTaxonomy%2FGeographicalAreas%23SouthKorea>

[243] 韓国法令情報サイト（「研究セキュリティ」（연구 보안）で検索）<https://www.law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=연구%20보안>

（抜粋）

第 1 条（目的）この指針は、「国家研究開発革新法」第 21 条第 1 項及び同法施行令第 44 条による中央行政機関の長が樹立する所管国家研究開発事業及び研究開発課題（以下「研究開発課題等」）に関するセキュリティ対策として、法第 21 条第 1 項による重要情報が流出しないようにすることを目的とする。

第 2 条（適用範囲）この指針は、中央行政機関所管国家研究開発事業に適用する。ただし、中央行政機関の長が当該国家研究開発事業に対してその特性により別途のセキュリティ規定を設けた場合、当該指針を優先して適用することができる。

第 3 条(研究開発課題 セキュリティ課題分類) ①中央行政機関の長は、法第 21 条第 2 項により所管研究開発課題をセキュリティ課題に指定・解除するなど、分類が必要なときは、検討のために当該研究開発分野及びセキュリティ業務専門家等で構成されたセキュリティ課題分類委員会を設置して運営しなければならない。（略）

第 4 条（研究開発機関のセキュリティ対策の樹立等）研究開発機関の長は、法第 21 条第 1 項及び令第 44 条によるセキュリティ対策（以下「研究機関セキュリティ対策」という。）として別表 1[244]による事項を含む独自の規定を設けなければならない。ただし、共同研究開発機関が独自のセキュリティ対策を設けることが困難な場合、又は主管研究機関と共同研究開発機関のセキュリティ対策を統一的に運営する必要がある場合には、主管研究開発機関のセキュリティ対策に共同研究開発機関が従うようにする。

第 5 条(セキュリティ対策総括担当者指定等) ①研究開発機関の長は、所属役職員の中から第 4 条による研究機関セキュリティ対策による業務を総括するセキュリティ対策総括担当者を指定しなければならない。

②その他、セキュリティ対策総括担当者の指定手続・業務等に関する事項は、第 4 条による研究機関セキュリティ対策で定める。

第 6 条(研究セキュリティ審議会の構成及び運営) ①研究開発機関の長は、次の各号の事項を審議するために、研究開発機関内に研究セキュリティ審議会を構成・運営しなければならない。

1. 研究機関セキュリティ対策の樹立・変更（研究セキュリティに関する自己規定の制・改正をいう）に関する事項

2.法第 21 条第 3 項によるセキュリティ管理措置のための計画に関する事項

3.法第 21 条第 3 項によるセキュリティ管理措置に関する自己点検結果及び自己点検結果による措置案に関する事項

4.第 8 条による外国政府等との接触管理に関する事項

5.第 9 条による外国研究者等の参加に関する事項

6. セキュリティ事故に対する措置計画及び再発防止対策に関する事項

7. 研究機関セキュリティ対策に違反した研究者に対する懲戒に関する事項

[244] 1. セキュリティ管理体系、2.セキュリティ課題に参加する研究者(研究責任者及び外国人を含む)管理、3. 研究開発内容及び研究開発成果の報告、4. 研究施設の管理、5.情報通信網の管理の各項目について規定されている。
<https://www.law.go.kr/flDownload.do?flSeq=134883203&flNm=%5B 별표%5D+연구기관보안대책에+포함되어야+하는+사항%28 제 4 조+관련%29>

8. セキュリティ課題参加研究者に対するセキュリティ手当の支給に関する事項

9. その他、研究開発機関の長がセキュリティに関して審議が必要であると認める事項

②その他、研究セキュリティ審議会の構成・運営に関する事項は、研究機関セキュリティ対策で定める。

第 7 条(セキュリティ教育及びセキュリティ誓約) ① 研究開発機関の長は、セキュリティ課題を遂行する予定である又は遂行している研究者に対し、次の各号の事項を含むセキュリティ教育を実施しなければならない。

1. 本指針による研究者の義務

2. 研究機関セキュリティ対策による研究者の義務事項

3. セキュリティ課題の遂行による優遇措置に関する事項

4. 義務事項に違反する場合に法、「産業技術の流出防止及び保護に関する法律」、「対外貿易法」により受けることができる不利益に関する事項

5. その他セキュリティ事故の予防に必要な事項

②第 1 項による教育を受けた研究者は、研究開発機関の長にセキュリティ誓約書を提出しなければならない。

③第 2 項によるセキュリティ誓約書の書式は、別紙第 1 号書式に従い、必要な場合、研究開発機関の長がその内容を準用して定めることができる。

④研究開発機関の長は、必要な場合、セキュリティ課題を遂行しない所属研究者及びその他所属職員に対してもセキュリティ教育を行うことができ、特にセキュリティ上必要な場合、誓約書を提出させることができる。

第 8 条(外国政府等との接触管理等) ① セキュリティ課題を遂行しているか遂行してから 3 年が経過しない研究者が外国に所在する政府・機関・団体又は外国人等（本社と支社の所在が異なるときは、本社位置を基準とすることを原則とする）とセキュリティ課題と関連して接触（研究者が相互作用する場合又は特定して有意な程度に接触が繰り返される場合をいう。）する場合には、当該接触日から 10 日以内に接触日時・場所・方法・内容等に関する事項を現在所属している研究開発機関の長（退職で所属機関がないか、又は法第 2 条第 3 号による研究開発機関でない機関に移職する場合には、最後に所属していた研究開発機関の長）に報告しなければならない。

② セキュリティ課題を遂行しているか遂行してから 3 年が経過しない研究者が外国政府・機関・団体等の支援を受けて研究開発を行う場合、事前に研究セキュリティ審議会の審議を経て現在の研究者が所属する研究開発機関の長（退職で所属機関がないか、法第 2 条第 3 号による研究開発機関でない機関に引っ越す場合には、最後に所属していた研究開発機関の長）の事前承認を受けなければならない。

③研究開発機関の長は、第 1 項により報告された事項、第 2 項により事前承認した事項を報告及び承認後 1 月以内に中央行政機関の長に報告し、国家情報院長に通知する。

第 9 条(外国研究者等のセキュリティ課題参加等) ①セキュリティ課題への大韓民国国籍を持たない外国人の参加は、内国人を通じた目的達成が難しい場合、補足的に認めることを原則とする。

②研究開発機関の長は、セキュリティ課題に関して外国政府・機関・団体等と共同研究を遂行しようとしたり、これらに研究の一部を遂行させようとする場合、中央行政機関の長の事前承認を得なければならない。

③研究開発機関の長は、セキュリティ課題に対する外国人の参加を承認しようとする場合、第 6 条による研究セキュリティ審議会の審議を経なければならない。このとき、研究セキュリティ審議会は、外国人のセキュリティ課題への寄与の可能性、技術格差などを考慮する際、今後外国に技術流出する可能性などを総合的に検討しなければならない。

④研究開発機関の長は、第 2 項により中央行政機関の長の事前承認を得た、又は第 3 項によりセキュリティ課題に外国人を参加させた場合、該当事項が発生し、1 月以内に当該セキュリティ課題において外国研究開発機関等と共同研究等のための条約事項又はこれに準ずる事項、また参加外国人の身上及び課題参加範囲、課題関連情報アクセス権の範囲等の情報を中央行政機関の長に報告し、国家情報院長に通知しなければならない。

第 10 条(セキュリティ等級表記) 略

第 11 条（セキュリティ課題遂行による優遇措置）略

第 12 条(セキュリティ管理実態点検) 略

第 13 条(セキュリティ事故に対する措置) 略

第 14 条(研究開発結果によるセキュリティ課題分類) 略

第 15 条(セキュリティ課題研究開発成果の帰属及び実施) 略

第 16 条(非公開研究開発成果への準用) 略

第 17 条(権限の代行) 略

第 18 条（見直し期限）中央行政機関の長は、この告示について「訓令・例規等の発令及び管理に関する規定」により、2022 年 1 月 1 日基準で 3 年ごとになる時点（3 年目ごとの 12 月 31 日までをいう）ごとにその妥当性を検討して改善等の措置をしなければならない。

(2) 諸外国の研究インテグリティ・セキュリティ対策の事例調査

韓国政府では、科学技術政策の政府研究所において、研究インテグリティ、研究セキュリティについての事例研究調査などが近年実施されており、諸外国の先進的な取組等を韓国の大学・研究機関に対して紹介している。

まず、2023 年 6 月に、科学技術情報通信部の研究制度革新課と KISTEP（韓国科学技術企画評価院）制度革新センターは、調査報告書「国際研究協力時の研究資産流出防止のための主要国の政策事例集」（국제연구협력 시 연구자산+유출 방지를 위한 주요국+정책사례집）を公表している。[245]

本事例集は、「国家研究開発革新法」第 21 条に基づき、研究機関がセキュリティ対策を樹立する上で、主要国の事例を通じ、重要な研究資産の流出を防止し主要国の事例を通じて核心研究資産の流出を防止し、国外の脅威から所属研究者と研究機関を保護することを支援する目的で発行された」と位置づけられた調査研究である。調査対象国は、米国、日本、英国、豪州の 4 か国であり、報告書の付録には、「国際研究協力時のリスク診断のためのチェ

[245]科学技術情報通信部 研究制度革新課、KISTEP（韓国科学技術企画評価院）制度革新センター「国際研究協力時の研究資産流出防止のための主要国の政策事例集」（국제연구협력 시 연구자산+유출 방지를 위한 주요국+정책사례집）. 2023 年 6 月.

ックリスト」として、これら 4 か国においてこれまでに策定されたチェックリストを掲載している。

次に、2022 年 3 月に KIRD（국가과학기술인력개발원（国家科学技術人材開発院））は、「研究セキュリティ管理及び研究成果保護の手引き：研究セキュリティの理解」（연구보안 관리 및 연구성과보호의 길라잡이 : 연구보안의 이해）を作成した[246]。同手引きは、本文約 80 頁、付録が 20 頁のマニュアルで、構成は以下のとおりである。

Part 1.研究セキュリティ管理を理解する
Part 2. (研究進行段階別) 研究者の研究セキュリティ管理
Part 3. (セキュリティ管理項目別) 研究機関の研究セキュリティ管理
よくある質問
付録(研究セキュリティ管理別添様式)

また、STEPI（Science and Technology Policy Institute（科学技術政策研究所））の情報ブリーフ文書が、2023 年 6 月の G 7 サミットにおける研究インテグリティ、研究セキュリティ関連の動向について報告している。韓国政府や韓国の科学技術研究への示唆として、以下の 3 点を挙げている（以下、引用）。[247]

- 示唆点 1 : 研究セキュリティ・研究インテグリティのリスク低減の観点から長期的な研究リスク管理体系を構築すること。
  - 国際社会の研究セキュリティの議論を研究革新全般にわたる常時的なリスク管理体系の導入のきっかけとし、変化する研究環境とリスク要因を持続的にモニタリングする。
  - 変化する研究環境とリスク要因を持続的にモニタリングし、リスク低減の観点から研究セキュリティ管理戦略の樹立と履行体系の点検方案を策定する。
  - 事後対応ではなく予防措置、違反に対する処罰より遵守に対するインセンティブ提供方式のアプローチが望ましい。
- 示唆点 2 : 韓国研究エコシステムの研究セキュリティ・研究インテグリティ環境の診断及びリスク管理基盤の造成。
  - 韓国的な文脈に基づく研究セキュリティと研究インテグリティのリスクレベルの診断及び必要措置の策定。その過程で、研究エコシステム構成員間の十分なコミュニケーションと持続的な合意形成の努力が前提となり、現場密着型の施策の策定が可能になる。
  - 最新の研究インテグリティ指針の案内、研究セキュリティのリスク認識の向上、

[246] KIRD（국가과학기술인력개발원（国家科学技術人材開発院））「연구보안 관리 및 연구성과보호의 길라잡이 : 연구보안의 이해」（「研究セキュリティ管理及び研究成果保護の手引き：研究セキュリティの理解」）2022 年 3 月
[247] 선인경(2023), G7, '디리스킹(de-risking)' 강조한 연구안보 위험관리방안 제시. STEPI 보고서. 과학기술정책 Brief. 2023.6.16
（ソンインギョン(2023)、G7、「脱リスク(de-risking)」を強調した研究安全保障リスク管理方案を提示。STEPI「科学技術政策 Brief」）

模範事例の発掘・拡散、そのためのリスク管理基盤の造成に焦点を当てる。

- 示唆点 3: リスク管理を通じた信頼できる研究エコシステムの健全性と安定性の増進に貢献する。
  - 研究セキュリティリスク管理は、研究エコシステム全構成員の努力が必要な共同の宿題である。研究セキュリティ脅威事件の発生を個人研究者の逸脱的な行動として認識するのではなく、健全で安全な研究環境の醸成への努力が優先されるべきである。

2.16　台湾

2.16.1　台湾における「研究インテグリティ」に係る取組の特徴

台湾は半導体、エレクトロニクスなど高度の科学技術力を持つ。台湾にとって、知識の安全保障と経済の安全保障の確保は極めて重要であり、科学技術を保護し、中国の干渉のリスクを軽減するための措置は、台湾の政策、法律、社会的イニシアティブの自明な要素となってきた。結果として、研究インテグリティや研究セキュリティ[248]は自明の取組であるため、台湾では概念としてはあまり知られてこなかった。唯一の公式ガイダンス文書は、政府出資の「国家基幹科学技術研究プログラム安全管理運用マニュアル」（国家安全委員会、2019 年、更新 2022 年）である。

その代わりに、経済安全保障や外国からの干渉、特に偽情報への対処を目的とした、より広範な政策の一環として措置が取られている。台湾は中国からの強力かつ広範な干渉に苦しんでいるため、ほとんどの法律や措置は、中国によってもたらされるリスクの軽減に焦点を当てている。[249] 国家安全法（National Security Act、1987 年制定、最終改正 2022 年）、台湾地区及び大陸地区人民関係条例（The Act Governing Relations between the People of the Taiwan Area and Mainland Area、1992 年制定、最終改正 2022 年）という 2 つの法律が国家中核的重要技術やハイテク産業の保護について規定している。

さらに、上記のように、2019 年 1 月に、政府出資の国家基幹科学技術研究プロジェクトの従うべき手順（政府出資の国家基幹科学技術研究プログラム安全管理運営マニュアル）が策定され、国家安全保障会議の科学技術チームによって運営されるなど、近年は法令遵守が特に、厳しくなってきている。[250]

2.16.2　台湾における取組の背景と経緯

中国との対立・緊張関係にも関わらず、中国からの留学生はこれまでも多かった。中国と台湾の学生交流は 2011 年から 2019 年にかけて盛んになった。ピークは 2015 年と 2016 年で、41,000 人以上の中国人留学生が台湾の短期留学や学位留学プログラムに参加した。このように中学から台湾への留学生は多かったものの、2017 年以降は、中国側のビザ管理強化が原因とされ、その数は減少した。2020 年 4 月、中国政府は台湾の大学への中国人留学生の申請をすべて停止した。この措置は現在も続いており、COVID-19 のパンデミックを背景に取られた停止措置であったが、より恒久的なものになると予想する者もいるとのことである。[251]

---

[248] 言葉としては「學術倫理與安全」（「学術の倫理と安全」）が該当する。
[249] Ingrid d'Hooghe, and Jonas Lammertink (2022). *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden Asia Centre. pp.37-40.
[250] Ingrid d'Hooghe, and Jonas Lammertink (2022).
[251] Ingrid d'Hooghe, and Jonas Lammertink (2022).

また、2022 年 7 月には、2 人の台湾人教授が、中国の長江奨学生人材招聘プログラムのもとで、対艦ミサイルと半導体技術という安全保障上重要な技術についての情報、すなわち国家機密を漏らしたとして捜査された（台湾地区及び大陸地区人民関係条例の違反）。1 人の教授は、以前に対艦ミサイル研究開発プログラム「興風 2 号」のメンバーであったが、2013 年以降、中国のアモイ大学でミサイル迎撃や自動離着陸システムなどの講義を行ったとして告発された。もう一人の元教授は、半導体研究に携わっていたが、2016 年 4 月から西安大学で教鞭をとっていたとされている。[252]

最近でも、2023 年 12 月に、台湾国防大学の有力教授が中国と技術協力する会社を 2014 年に設立し、10 年間にわたって何度も中国と行き来していることが検察の捜査で明らかになったとの報道があった。[253]

2.16.3 台湾における取組の詳細

(1) 「国家安全法」、「台湾地区及び大陸地区人民関係条例」等

上記の２つの法律のうち、「国家安全法」は、外国、中国本土、香港、マカオ、または敵対的な外国勢力が設立等した組織や団体等や、それらが派遣する者のために、国家核心重要技術についての営業秘密を取得し、漏洩すること等を禁じている（第 3 条）。国家核心重要技術とは、外国、大陸地区、香港、マカオ、国外の敵対勢力に流出すれば、国の安全、産業競争力、経済発展を大きく損なうものと規定されており、特別に指定されている[254]。

次に、「台湾地区及び大陸地区人民関係条例」は、台湾のハイテク産業を保護し、台湾の大学や研究機関への中国大陸人の関与を含む台湾と大陸の人々の取引を規制することによって、重要技術の流出を防止するものである。中国（大陸）の国民でも、台湾に戸籍があれば、台湾の学術研究機関の教員や研究員になることができる。ただし、台湾で 20 年以上戸籍を有していなければ、国家安全保障に関わる業務や科学技術機密の研究に従事することはできない、とされている（第 21 条）[255]。

また、「大陸地区出身者の台湾地区への入域許可弁法」は両岸協力などの問題を扱っており、例えば台湾の大学と中国の政党、政府、軍事機関との協力を禁じている（第 33 条）。[256]

ここ数年、法律の遵守に関する監視の目が特に厳しくなっており、「国家安全法」、「台湾

---

252 “New probe of ex-Yuan Ze professors to be opened” LEAKS TO CHINA? The education minister said that an initial investigation of two professors had not achieved anything because of obstruction by Chinese officials Lee Hsin-fang and Jonathan Chin. Taipei Times. 2022/7/29 <https://www.taipeitimes.com/News/taiwan/archives/2022/07/29/2003782614>

253 <https://www.rfa.org/mandarin/yataibaodao/gangtai/hcm2-12122023085352.html> <https://www.epochtimes.com/gb/23/12/11/n14134114.htm>

254 国家科学技術委員会「公布國家核心關鍵技術加強保護營業秘密」2023 年 12 月 5 日」 <https://www.nstc.gov.tw/folksonomy/detail/ab71317e-c22e-467a-b3a0-7515aa2bfe6e?l=CH&utm_source=rss>

255 全国法規資料庫. “Act Governing Relations between the People of the Taiwan Area and the Mainland Area” <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=Q0010001>

256 Ingrid d’Hooghe, and Jonas Lammertink (2022).

地区及び大陸地区人民関係条例」は 2022 年に改正された[257]。

(2) 政府出資の国家基幹科学技術研究プログラム安全管理運営マニュアル

2019 年 1 月に策定された「政府出資の国家基幹科学技術研究プログラム安全管理運営マニュアル（「政府資助國家核心科技研究計畫安全管制作業手冊」）」（「国家安全委員会（國家科學及技術委員會（NSTC））、2019 年、更新 2022 年）は、政府出資の「国家基幹科学技術研究プロジェクト」が従うべき手順を規定している。マニュアルの構成は以下のとおりである。[258]

1. 用語の定義
2. 序文
3. 科学技術グループの組織と運営
4. 国家基幹科学技術プロジェクトの承認
5. 国家基幹科学技術研究プロジェクトの安全管理
6. 科学技術研究開発成果の保護に関する規則

マニュアルでは、国家基幹科学技術として以下の 6 分野が挙げられている。すなわち、(1)農業科学技術（農業委員会の責任）、(2)製造キーテクノロジー（経済部の責任）、(3)航空宇宙・衛星技術（国家科学委員会の責任）、(4)海洋科学技術（海洋委員会の責任）、(5)先進集積回路設計・プロセス技術（国家科学委員会担当）、(6)ネットワーク・セキュリティのための重要技術（行政院の責任）である。これらは政府助成研究プロジェクトに関するものであり、政府助成以外の民間企業での研究、技術開発も含む前述の国家核心重要技術とは異なる。

マニュアルでは、政府の安全管理措置が説明され、規制と審査メカニズムの概要、開示書式や質問票のモデルが掲載されている。[259]

マニュアルの 5 章「国家基幹科学技術研究プロジェクトの安全管理」の概要は以下のとおりである。

- 「政府資金による科学技術研究プロジェクトが国家基幹科学技術研究プロジェクトと認定された場合、政府資金提供機関は資金提供契約に当該プロジェクトが国家基幹科学技術研究プロジェクトであることを明記する。
- 関連機関は規則に従って国家基幹科学技術研究プロジェクトの参加者、研究成果、データを管理しなければならず、プロジェクト実施機関は政府資金提供機関の検査に協力する義務を負う。
- プロジェクトの実施機関は、「A クラス」国家基幹科学技術研究プロジェクトのコア技術、設備、データにアクセスする可能性のある関係者を面接調査し、「政府補助国家基

257 湯野基生「台湾：国家安全法の改正」『外国の立法』296（2023. 6）. 国立国会図書館調査及び立法考査局.
258 國家科學及技術委員會 112 年 1 月「政府資助國家核心科技研究計畫安全管制作業手冊」<https://data.gov.tw/dataset/107413>
259 Ingrid d'Hooghe, and Jonas Lammertink (2022).

幹科学技術研究プロジェクト関係者調査書」（表 2）に記入する。

- 外国人、大陸人、香港人、マカオ人が国家基幹科学技術研究プロジェクトに参加する場合、資金提供機関の同意を得なければならない。

上記の「政府補助国家基幹科学技術研究プロジェクト関係者調査書」（表 2）のうち、面接時のインタビューの質問は以下を含んでおり、特に中国本土との関係（居住、就労、財産等の利害関係）については親族を含めて情報を開示することが求められている。

「表 2：政府出資の国家基幹科学技術研究計画スタッフに関する調査」：インタビュー質問

- 回答者と回答者の配偶者の二親等[260]以内の血族または義理の親族で、外国に居住または就労したことのある人について、氏名、調査対象者との関係、居住したことのある国・地域、就労したことのある国を記入。
- 以下の 3 つのいずれかに該当する場合は、発生時期、政府・企業名、状況を記入。
  (1) 外国、中国本土、香港、マカオに財産、商取引、または金融上の利害関係がある。
  (2) 現在または過去に外国、中国本土、香港、マカオで勤務していた者。
  (3) 外国、中国本土、香港、マカオの大使館または駐在員事務所と取引がある。
- 過去 7 年以内に海外、中国本土、香港に出張または教育目的で渡航したことがある者。海外出張（メーカー主催の海外出張を含み、中華民国政府機関から指定された公式出張を除く）の期間、場所、国、理由を記入。
- 以下の退職事由に該当する場合は、退職事由コード、退職期間、退職組織、退職理由を記入。(1)解雇 (2)解雇を告げられての退職 (3)不祥事による退職 (4)業績不振による退職 (5)その他不本意な退職。
- 過去 7 年間に破産宣告を受けた、または自ら破産宣告をした場合は、その期間、理由、金額、内容を記入。

[260] 2 親等は、自分と配偶者の兄弟姉妹・祖父母・孫までを含む。

2.17　イスラエル

2.17.1　イスラエルにおける「研究インテグリティ」に係る取組の特徴

イスラエル[261]の研究のオープン化、国際化に伴う新たなリスクへの対応に関して、「研究倫理（research ethics）」「研究セキュリティ（research security）」「アカデミック・インテグリティ（academic integrity）」「責任ある―（responsible -）」等の語がみられる。新たなリスクの相手国として懸念される中国等については、その存在を念頭におきながら、取組の運用を通じて柔軟な対応を図っている。また、国家施策としての研究奨励・オープンイノベーションと、それらに対する規制・倫理とを、相反ではなく相乗と捉える姿勢が特徴的である。以下、取組の背景と経緯、詳細について述べる。

2.17.2　イスラエルにおける取組の背景と経緯

イスラエルは GDP に占める研究開発費の割合が約 5.6%（2021 年）と世界で最も高く[262]、地政学的背景もあって軍事や先端エレクトロニクス等の分野で重点的に投資し、国家政策としてオープンサイエンス・オープンイノベーションを奨励している。2010 年代のネタニヤフ政権下で積極的に進めてきた中国との研究開発協力の強化により、デュアルユースを含むテクノロジー部門に対する中国の投資が大幅に増加し[263]、中国は技術分野の買収を進めていった[264]。

このような中国の影響を懸念する米国の方針を受け、2019 年、対外投資の国家安全保障面を評価する諮問委員会（The Advisory Committee for Evaluating National Security Aspects of Foreign Investments）を財務省（Ministry of Finance）に設立した[265,266]。2022 年、米国との間で技術戦略ハイレベル対話を行い、インフラやテクノロジー分野等の中国との主要取引についての情報共有、研究セキュリティ、輸出管理、投資審査などを含む両国の

---

261 本章中、ヘブライ語資料に基づく部分は、機械翻訳を参考に概要を記述した。イスラエル科学人文アカデミーに関する部分は、2024 年 1 月現在、同アカデミーの公式サイトへのアクセスが切断される状態が続いているため、Internet Archive Wayback Machine: https://archive.org/ にて可能な範囲で確認した。イスラエル立法府（Knesset）や教育省（Ministry of Education）の公式サイトも同様にアクセスエラーとなり、かつ、上記アーカイブでも参照できないため、本報告書では触れていない。

262 OECD. “Gross domestic spending on R&D”. https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

263 Yosshi Melman. "China Is Spying On Israel to Steal U.S. Secrets" Foreign Policy. March 24, 2019. https://foreignpolicy.com/2019/03/24/china-and-russia-are-spying-on-israel-to-steal-u-s-secrets-putin-netanyahu-xi-haifa-ashdod-iai-elbit/

264 Arbell, Dan et al. "What do Israel’s China ties mean for its relationship with the US?" *International Institute for Strategic Studies website*. May 8, 2019. https://www.iiss.org/online-analysis/online-analysis//2019/05/israel-china

265 Ministry of Finance. “The Advisory Committee for Evaluating National Security Aspects of Foreign Investments“ https://www.gov.il/en/departments/policies/foreign-investment-board

266 Babb, Casey. “Proceed with Caution: Israeli Research Collaboration with China” *INSS website.* No. 1645, September 20, 2022. https://www.inss.org.il/publication/academic-relations-china/

技術エコシステムに対するリスクの管理に焦点を当てた[267,268]。この時期、国内のインフラ構築に中国関連の技術や組織を避ける動きもあり [266]、中国の輸出については経済産業省（Ministry of Economy and Industry）のデュアルユース規制の下で抑制的な運用となっている[269,270]。また、上記諮問委員会は 2022 年、主に中国やロシアの案件を念頭に同委員会への付託を義務付ける際の基準の策定や、外務省の地位を正委員に格上げする等の強化がなされた[271]。

また、研究に関する従来からの主な法令として、研究奨励については「高等教育審議会法（The Council for Higher Education Law）（1958 年）」「イスラエル科学人文アカデミー法（Israel Academy of Sciences and Humanities Law）（1961 年）」「産業研究開発奨励法（The Encouragement of Industrial Research and Development Law）（1984 年）」「国家民間研究開発評議会法（National Council for Civilian Research and Development Law）（2002 年）」等があり、研究倫理については生物医学や知的財産等の各分野の法令で定められている[272]。これらの法令に基づき、大学や研究機関・学協会・資金配分機関・各研究分野等で、様々な規範や仕組みを設けている。

ヘブライ大学（Hebrew University of Jerusalem）では、同大学研究開発局（The Authority for Research and Development）の研究倫理のウェブサイトに、上記の研究に関する法令・規則等が一覧でまとめられている [272]。学内規程として「研究における行動規範（Code of Conduct in Research）」「利益相反規程（Conflict of Interest Code）」等が定められている。研究者やスタッフはこれらの規程の遵守を約し「適切な行動と利益相反に関する声明」に署名する必要があり、利益相反に関して大学利益相反委員会のアドバイスを求めることができる。大学倫理委員会には、全学部の代表者を中心とする最高倫理委員会および各学術専門分野の代表者を中心とする教員倫理委員会とがある（一部の委員会は 2023 年 6 月現在まだ設立過程にある）。

ワイツマン科学研究所（Weizmann Institute of Science）では、ウェブサイトの「倫理行動規範（Code of Ethical Conduct）」のページに、その主となる倫理規範（Ethical Code）および倫理の一般原則や倫理的課題として「研究所の方針、倫理基準、法律の遵守」「金融取引」「利益相反」「平等と無差別」「ジェンダーバイアスの回避」「セクシャルハラスメントの防止」「安全と健康」「環境」「助成金の要件と条件の遵守」「知的財産と情報へのアクセス」

---

[267] The White House, “Fact Sheet: U.S.-Israel Strategic High-Level Dialogue on Technology,” September 30, 2022.
[268] Harkov, Lahav. "Israel agrees to update US about China trade to avoid tension" *Jerusalem Post.* January 3, 2022. https://www.jpost.com/international/article-691425
[269] Ministry of Economy and Industry. “Export Control Agency, Ministry of Economy and Industry” https://www.gov.il/en/Departments/General/duexportcontrol-info
[270] Granot, Ofer. "Tightened Global Enforcement of US Export Controls: The Significance for Israel" *INSS website.* No. 1738. June 14, 2023. https://www.inss.org.il/publication/bis/
[271] Schanzer, Jonathan, et al. "Wary of China, Israel Toughens Screening of Foreign Investments" *Foundation for Defense of Democracies website*. November 17, 2022. https://www.fdd.org/analysis/2022/11/17/israel-toughens-screening/
[272] The Authority for Research and Development, The Hebrew University of Jerusalem. “Research Ethics” https://research.huji.ac.il/התשתית-החוקית

「規範違反と内部告発」が挙げられている[273]。同所の「学術的誠実さと責任ある研究行為の方針および手順（Academic Integrity and Responsible Conduct of Research (RCR) Policy &Procedures）」では、RCR 逸脱が疑われるケースは、同研究所の研究公正責任者を兼ねる副所長等へ連絡することとなっており、調査結果は所長に報告される。研究に関する契約に法的な懸念点がある場合は、 研究助成金およびプロジェクト事務局の責任者を通じて法的審査を受けるよう指示される。

イスラエル科学人文アカデミー（Israel Academy of Sciences and Humanities）では、倫理的な科学研究を実施することの重要性に鑑み、1996～2010 年に運営されていた生命倫理委員会[274]を 2017 年に再設置した[275]。国内外の生命倫理分野の活動や生物学的問題に関わる倫理的、法的、社会的側面について、同アカデミーに報告・助言を行っている。同委員会のウェブサイトにおいて、生命倫理の議論を促進するためのアンケートフォームを設置しており、匿名での回答が可能となっている[276]。

イスラエルイノベーション庁（Israel Innovation Authority: IIA）では、研究資金申請を評価する過程で、検査チームが申請者の事業所訪問・研究室施設見学やデモンストレーションのリクエストを行うことがあり、この検査チームの意見を受けて、同庁所属者に経済産業省や財務省のメンバーも加わる研究委員会にて検討・評価を行う[277]。2018 年に「国外での知的財産の使用許可を与える手順」[278]を定め、国内の多国籍企業における同庁の支援を受けての知的財産の開発・共有を、一定要件と研究委員会の承認を経ることにより可能にした。2023 年 10 月には「機密保持の手順[279]」にて、資金受給者の法令遵守状況や資金使用状況等を確認するに際しての、政府機関や権限を有する諸機関との情報共有について定めを設けた。

分野別では、以下の取組が研究セキュリティに資するとの評価がある[280,281]。バイオセキュリティ分野では、「生物学的病原体研究規制法（the Regulation of Research into Biological Disease Agents Law）(2008 年)」に基づき、危険な病原体を用いた研究について承認の申請が義務付けられ、有識者や政府関係機関の委員で構成する審議会が評価を行う。法律違反には罰則が定められている。サイバーセキュリティ分野では、政府はイランを

---

273 Weizmann Institute of Science. “Code of Ethical Conduct”.
https://www.weizmann.ac.il/pages/about-institute/code-ethical-conduct
274 Israel Academy of Sciences and Humanities. http://bioethics.webcare.org.il/
275 Israel Academy of Sciences and Humanities.
https://www.academy.ac.il/RichText/GeneralPage.aspx?nodeId=1219
276 Israel Academy of Sciences and Humanities.
https://www.academy.ac.il/RichText/GeneralPage.aspx?nodeId=1423
277 Israel Innovation Authority.
https://innovationisrael.org.il/בדיקה-והערכת-הבקשה/
278 Israel Innovation Authority.
https://innovationisrael.org.il/rules/2-הוראות-למתן-הרשאה-לשימוש-בידע-מחוץ-לישי/
279 Israel Innovation Authority.
https://innovationisrael.org.il/rules/נוהל-שמירת-סודיות-ופעילות-רשות-החדשנו
280 Wilner, Alex et al. "Research at risk: Global challenges, international perspectives, and Canadian solutions" *International Journal*. 2022, Vol.77 (1) 26-50.
281 Lev, Ori. "Regulating dual-use research: Lessons from Israel and the United States" *Journal of Biosafety and Biosecurity* 2019, Vol.1 (2) 80-85.
https://www.sciencedirect.com/science/article/pii/S2588933819300287

中東における主要なサイバー脅威と明示しており[282]、科学技術省による教育カリキュラムの導入や大学内の専門の研究センターの設置、イスラエル国家サイバー総局（Israel National Cyber Directorate: INCD）による政策策定・報告書公表、内部のサイバー緊急対応チーム（CERT）による対応支援、民間企業・学術機関・他政府機関との連携が行われている。

2.17.3 イスラエルにおける取組の詳細

以上の主要な機関や分野の取組とは区別して、政府はこれまで研究セキュリティに関して研究部門への規制に消極的であったとされており（Wilner 2022）[280]、今後も国家安全保障の観点から規制を加える場合に中国やロシア等の特定国の明示はしないとみられている（Melman 2019）[263]。国家安全保障研究所（Institute for National Security Studies: INSS）から、中国による研究上の損失について公表されずオープンソース情報も少ないことや、広く民間の学術・研究団体も含めると新たなリスクへの対応態勢が整っていないことが指摘され、研究セキュリティのガイドラインや研究協力協定の確立、外国人留学生の審査メカニズム、新たなリスクへの対応のための官民連携等の必要性が唱えられてきた[266,283]。研究奨励と規制のバランス、そして研究開発面を含めた米中のバランスという政治的課題の調整は国外からも注目されてきた[264,280,284,285]。

そのような中、2023 年 8 月に IDF から「I2I イノベーション・トゥ・イノベーション: IDF イノベーション・パートナーシップ戦略（I2I Innovation to Innovation: IDF's Innovation Partnership Strategy）[286]」が示された。オープンイノベーションと軍組織間のコラボレーションにより、新技術等から生じる可能性のある安全保障上の脅威や機会を特定し対応を図る枠組みや方向性が取りまとめられている。

I2I の指導原則の一つ「非伝統的なイノベーション力強化プロセスの推進」は、「伝統的」な軍事部門が、国内の「非伝統的」団体、即ち民間企業や研究機関等との直接的・無媒介の接触を確立することで、イノベーション力強化と共に、常に最新動向を把握し新たなリスクの特定・対応を目指す。その実施例である「イノフェンス（iNNOFENSE）」は、IDF・DDR&D（国防省研究開発局）の協力により 2019 年に創設された、民間部門と安全保障部門のデュ

[282] Israel National Cyber Directorate. " Iran is a main cyber threat on the Middle East" June 26, 2019. https://www.gov.il/en/departments/news/unna_cyber_week_2019
[283] INSS ISRAEL. "Research Security Amidst Great Power Competition." YouTube. https://www.youtube.com/watch?v=B9N8b495_fc
[284] Egozi, Arie. "White House pressuring Israel to cut research ties with China over dual-use concerns" *Breaking Defense*. September 29, 2022. https://breakingdefense.com/2022/09/white-house-pressuring-israel-to-cut-research-ties-with-china-over-dual-use-concerns/
[285] Schanzer, Jonathan et al. "Aligning U.S.-Israeli Cooperation on Technology Issues and China" *Center for a New American Security website*. March 9, 2022. https://www.cnas.org/publications/reports/aligning-u-s-israeli-cooperation-on-technology-issues-and-china
[286] Combat Methods & Innovation Division (CMI), IDF. "I2I Innovation to Innovation: IDF's Innovation Partnership Strategy" LinkedIn. August 2023. https://www.linkedin.com/posts/nir-weingold-ıl-2b6730a0_partnerships-and-innovation-empower-each-activity-7093781126212653056-ZI5r?trk=public_profile_like_view

アルユース技術プロジェクトのためのイノベーション・プログラムである。運営を行う iHLS（企業）・SOSA（企業）等は、IDF を含むイスラエルの安全保障エコシステム内の運用上および組織上のニーズに対応し、法的助言を含めビジネス面を広く支援する。

同じく指導原則の一つ「経験やプロセスの共有による共通の知識・技術の開発」のための研修・教育システムの一例に、2021 年 10 月に開設された「イノベーション、イントラプレナーシップ、トランスフォーメーションのための防衛大学（the Defense College for Innovation, Intrapreneurship and Transformation）」がある。「敵が変わり、社会が変わる。我々も変わり一緒に変わらなければならない」[287]という意識の下、オープンユニバーシティの協力により、訓練や実験、様々な分野の研究や規範に関する学術教育を行う。IDF の起業家やイノベーターに加え、防衛コミュニティのパートナーも利用可能である。また、IDF は革新的な技術や取組に関する知識を共有するために、会議やサミットの開催、業界団体への加入、大学や研究所との関係構築等を通じ、最新技術開発の情報を入手し、新技術や新たな脅威を含むトピックやテーマを取り扱う。

2023 年 12 月には、イノベーション科学技術省の主導と法務省（Ministry of Justice）の協働による「責任あるイノベーション - 人工知能（AI）の規制と倫理に関するイスラエルの方針（Responsible Innovation - Israel's Policy on Artificial Intelligence Regulation and Ethics）[288]」が示された。AI 分野の規制や倫理に関する国内初の包括的な方針であり、上記 2 省と IIA・プライバシー保護庁（the Privacy Protection Authority）等の政府機関や国内主要 AI 企業・学界等と協働し、基本的権利と公共の利益を守りつつ、民間部門の開発と責任ある利用を促進する枠組みを確立する（公共部門の AI 分野に関する政府の方針は別途策定中である）。OECD の AI 原則を前提とし、「責任ある」の概念に重きをおき、イノベーションと倫理・規制を相反的ではなく相乗的・相互補完的と捉えている。同方針は、「差別」「人間の監視」「説明可能性」「AI との相互作用の開示」「信頼性、堅牢性、セキュリティ、安全性」「説明責任と法的責任」「プライバシー」の 7 項目を主要な倫理・規制の課題とし、課題への対処のための提言を示している。

提言の一つ「AI 規制のための政策枠組みの確立」では、各分野の規制当局の権限強化、フレームワークの国際的相互運用性、リスクベースのアプローチの採用、漸進的な開発と規制の実験、ソフトな手法による規制、マルチステークホルダーによる協力等が掲げられている。ソフトな手法の例として、拘束力のない倫理原則、基準、監督のない自主規制等が挙げられている。また、提言「AI 政策調整センターの設立」では、専門家ベースの省庁間組織として、各分野の規制当局への助言や組織間調整、AI の規制や基準に関する国際フォーラムでの国家代表としての関与、責任あるイノベーションに関する情報やツールの公開、産業界・学界・市民組織・政府との継続的な議論と知識の共有を促進するための協議の場の設置等が挙げられている。同センターの主導によるリスク管理ツールの開発、例えば規制機関と民間事業者の間で共通の用語集を作成するリスク管理フレームワーク等も提唱されている。

---

[287] The Defense College for Innovation, Intrapreneurship and Transformation, IDF. https://www.idf.il/41563

[288] Ministry of Innovation, Science and Technology. December 17, 2023. "Israel's Policy on Artificial Intelligence Regulation and Ethics" https://www.gov.il/en/Departments/policies/ai_2023

2024 年 1 月、「外国からの影響と干渉の定義（Defining Foreign Influence and Interference)」[289]が示された。この文書は、外国の影響と介入の戦略的課題に関する近刊の覚書の一部である。同覚書は、INSS とイスラエル情報遺産・記念センター（Israel Intelligence Heritage & Commemoration Center: IICC）が、諜報省（Ministry of Intelligence）の協力を得て共同で作成されたもので、敵対国としてのロシア・イラン・中国等の視点からこの課題を検証する記事や、経済界・学術界を含めての影響の性質を扱う記事が含まれる。

同文書は、過去 10 年間の欧米民主主義諸国間における外国影響・干渉に関する研究・政策関連のイニシアティブや法的措置について、概念的・規範的隔たりがあることに着目する。影響と介入の区別について、既存の定義やアプローチで多用されてきた「意図」「透明性」「正当性」といった視点の限界に言及する。また、2010 年代以降の大国間競争・武力行使を伴わない政治主体間の敵対的な国際関係を背景とした「ハイブリッド活動」「グレーゾーン」の概念を前提に、区別の主観性や相対性を指摘する。そして、対外的な影響力は国際関係において常に基本的な手段であり、したがって新しい概念的な戦略的な枠組みは必要なく、外国の様々な国力の源泉（外交・情報・軍事・経済・金融・宗教等）が自国の価値観・規範・法令と矛盾していると認識される場合に外国の影響が干渉とされる、と結論付けている。

同月、INSS およびイスラエル・中国政策センター（Israel-China Policy Center）から覚書「イスラエルの国家技術戦略（National Technology Plan in Israel)」[290]が示された。大国間の技術競争とグローバリゼーションの後退の影響に対するイスラエルの議論・戦略・国家計画が確立していないことを改めて指摘し、現状の短期的視点に基づく投資戦略や研究開発の中国依存が高い状況等に対して警告する。技術先進国たる米国・欧州連合・日本・韓国が研究開発能力と生産能力の両方を強化していることや、オランダ・ドイツ・アイルランドが学術界を強化し研究・開発・生産への投資を奨励していることを参考として挙げる。これらの国のように利益や価値観の共通する国との研究開発・産業面でのパートナーシップを強めることが安全保障の確保や持続的な発展、世界の主導的地位の維持にも資するとして、この観点からの国家技術戦略の確立を強く求めている。

2.17.4 イスラエルの取組に関する考察

イスラエルは他国の取組状況を参考にしながら自国の技術戦略それ自体やいわゆる外国干渉等の課題に対するあり方について議論・検討が続く中、新たなリスクに既存の枠組みを活かした対応を行っていくことが考えられる。また、2022 年末に返り咲いたネタニヤフ政権下、国の右傾化、司法の弱体化や今般の戦争等を背景に、新たなリスクへの対応にも IDF 等の影響力が強まっていく可能性がある。

---

289 Fridman, Ofer. “Defining Foreign Influence and Interference” *INSS website.* January, 2024. https://www.inss.org.il/publication/influence-and-interference/

290 Sobelman, Ariel et al. “National Technology Plan in Israel” *INSS website.* January 2024. https://www.inss.org.il/publication/technology-memorandum/

本書で触れた取組のうち、I2I のように実力機構の直接的な関与という点については、日本においては安全保障の実効性確保の観点からどのように連携を図っていくべきかといった形で一定程度慎重な検討を要することになろう。とはいえ、実力機構が会議やサミットの場を通じて学術機関や民間企業等と情報共有を行うことや、実力機構関係者への研究の規範を含む学術的教育等を通じて安全保障状況の変化・変革に強い人材を専門的・実践的に育成するといった取組は、新たなリスクへの対応力を高めるものとして参考となる。

また、AI 方針のように産官学民の連携、マルチステークホルダーの協力体制を進めることは、従来的なリスク対応の文脈に限らず、研究活動の透明性を確保し説明責任を果たすといった研究者や研究組織の規範にも役立つ。加えて、AI のように先端分野や国家的重点分野から先行的に新たなリスクを見据えた体制を整備していくことは、後々他分野へも普及・応用し得る点で有用であろう。民間部門を含め共通用語を採用するためのリスク管理フレームワークや国際協定の確立等もまた、分野を問わず新たなリスクに速やかに対応するために必要である。

最後に、研究の国際化やオープン化に伴う新たなリスクについての倫理・規制を前向きに捉え積極的に取り組むことの重要性は、日本や世界の研究・イノベーションにおいても共通するものと考えられる。

2.18 研究活動の国際化、オープン化に伴うリスクの管理のための主な取組のまとめ

米国、英国、豪州、カナダ、欧州連合においては、研究活動の国際化、オープン化に伴うリスクの管理（リスク判断を含む）のための主な取組としては以下のものがみられた。

米国

・国防省では、2023 年 6 月に「高等教育機関における国防省資金配分による研究における望まない海外からの干渉への対抗」（Department of Defense. Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education. June 29, 2023.）を策定、公表している。「基礎研究提案の利益相反緩和の判断材料となる決定マトリクス」は、プログラム管理者（program managers）と国防省構成機関（DOD Components）が基礎研究提案の潜在的な利益相反を審査する際に役立つ手引書である。

・国防省の研究機関である DARPA には、「海外からの影響対策プログラム」（Countering Foreign Influence Program: CFIP）がある。同プログラムは、不当な外国からの影響の可能性を特定することにより、DARPA の研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を支援することを目的とした適応型リスク管理セキュリティプログラムである。CFIP のリスク評価は、標準フォーム（SF）424「Senior/Key Person Profile (Expanded)」及びその付属文書又は参照文書に記載されている情報に基づいて行われる。不当な外国影響力のリスク評価プロセスは、SF424 に記載されているすべての報告情報に注目し、過去 4 年間のシニア/キーパーソンの活動に最も重点を置いている。CFIP のリスク評価は、外国の影響を受けた利益相反又は責務相反を構成する可能性のある外国関連活動等の量、種類、時期に応じて、「低」から「非常に高い」までに分類されている。

・NSF は、2023 年 6 月に NSF Guidelines for Research Security Analytics を公表している[291]。同文書は、NSF 職員が研究助成金申請書等の情報や公開情報に基づいて実施するリスク判断やリスク分析の方法等についてのガイドラインである。定義（第 5 節）、Office of the Chief of Research Security Strategy and Policy（OCRSSP）の責任とプロセス（第 6 節）、NSF 職員によるモニタリング・報告（第 7 節）、OCRSSP による許可・禁止行為（第 8 節）、研究セキュリティ分析のためのデータ・サービス・分析手法（第 9 節）、研究セキュリティ関連情報の共有原則（第 10 節）について説明している。OCRSSP の活動は検証（verification）に関連するものであり、調査活動（investigation）は行わない。研究セキュリティ分析には、SCOPUS、Web of Science,米国特許商標局特許データベースが使用される。情報開示された研究資金、所属等とこれらの論文データ等の情報のミスマッチが調べられる。（9 節）

[291] https://new.nsf.gov/research-security/guidelines
https://nsf-gov-resources.nsf.gov/2023-05/NSF%20Research%20Security%20Guidelines-2023.pdf

英国

・研究インテグリティに関するリスクの識別・分類、リスクの判断基準、リスク判断のフロー等について詳細に説明された文書ではないが、一般の大学研究者が国際共同研究の提案を行う際に、研究インテグリティに関するリスク発生の予防の観点から、わかりやすく、確認すべき事項を示したチェックリストである「Trusted Research Checklist for Academia」が、前述した「Trusted Research Guidance for Academics」に関連して NPSA から公開されている。項目は、新規パートナーについて、研究の関係性について、既存のパートナーについてのそれぞれについて確認事項を含む。

豪州

・豪州では 2019 年 11 月に、外国干渉を排除するための通称・UFIT ガイドライン（Guideline to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表した。同ガイドラインの 3 章「Due Diligence, Risk Assessments and Management」において、デューディリジェンスの方法、リスクマネジメントについて説明されている。また、以下のような関連文書が UFIT により作成され、教育省のウェブサイトで公表されている。

-Due Diligence Assistance Framework (2021 年 11 月公表)

-Due diligence, risk assessments and management

・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）が発表された。豪州の資金配分機関である豪州研究評議会（ARC）は、競争的研究資金の申請にあたり、このリストに記載された技術が含まれている場合には、リスクがあるかどうかを検討することになっている。リスク要因には、次のような諸点が含まれるとしている。

-外国からの財政支援や教育又は研究関連活動

-外国の人材育成プログラムへの関与など

-外国の政府や軍隊、警察、諜報機関などへの直接の関与

-豪州が制裁措置をとっている体制、個人、組織への関与

カナダ

・NSERC におけるリスクアセスメントは、研究者が提出したリスク質問票を検討し、国家安全保障を考慮した評価が必要な場合には、カナダ公共安全省に照会され、カナダ公共安全省、カナダ安全保障情報局、又はカナダ通信保安局が主導して評価を実施するという特色を持つ。助成機関から照会された申請書を受け取ると、カナダ公共安全省は最初の審査を行い、結果を通知する。カナダ公共安全省は、評価結果及びアドバイスを助成機関に返却する。

・「Policy on Sensitive Technology Research and Affiliations of Concern」によるリスクアセスメントプロセスでは、大学または関連研究機関が、連邦資金配分機関およびカナダ・イノベーション財団（Canada Foundation for Innovation）に提出した、研究助成金およ

び資金提供の申請書においては、1）機密技術研究分野を発展させる研究を含み、さらに、2）その助成金で支援される活動に関与する研究者のいずれかが、カナダの国家安全保障に危険をもたらす可能性のある軍、国防、または国家安全保障機関と関係のある海外の大学、研究機関、研究所に所属している場合、またはそこから資金や現物支援を受けている場合には、資金が提供されなくなる。このプロセスを支援するため、「機微技術研究分野（Sensitive Technology Research Areas）」のリスト、カナダの国家安全保障に危険を及ぼす可能性のある、軍、国防、国家安全保障機関と関係のある海外の大学・研究機関のリストが公表された。

欧州連合

・2022 年 1 月に欧州委員会は「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」を公表した。包括的な戦略を策定するためのツールキットとして作成されたもので、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た主要な注目分野をカバーしている。それぞれのカテゴリー別に、「海外からの干渉」への対応策を列挙している。

-価値観（1. 学問の自由が危険にさらされている国やパートナー機関を特定する、2. 当該教育機関における学問の自由とインテグリティに対する外部からの圧力を理解するために、脆弱性評価（vulnerability assessment）を実施する、3. 機関及び個人レベルで学問の自由とインテグリティへのコミットメントを強化する、4. 抑圧的な環境下にあるパートナーとの協力を継続する）

-ガバナンス（1. 海外からの干渉に対する行動規範を公表する、2. 海外からの干渉委員会（Foreign Interference Committee）を設置する）

-パートナーシップ（1. リスクマネジメントシステムを導入するための一般的な前提条件を整備する、2. 強固なパートナーシップ合意を策定するための健全な手順を確立する）

-サイバーセキュリティ（1. サイバーセキュリティリスクの認知度向上、2. 海外からの干渉行為者によるサイバーセキュリティ攻撃を検知し、防止する、3. 海外からの干渉によるサイバーセキュリティ攻撃への対応と復旧を行う）

米国では、DARPA のような機関を含む国防省が、国防省が資金を提供する研究における好ましくない外国の影響に対抗するための方針を定めている。これらの方針は、標準的な書式や文書で提供された情報に基づき、研究者の経歴、所属、活動を詳細に精査することで、潜在的な利益相反や外国からの影響を特定することに重点を置いた、意思決定マトリクスや、外国影響対策プログラム（CFIP）のようなプログラムによって支えられている。また、NSF における提案された研究についてのリスク判断では、NSF 職員が研究助成金申請書に記載された情報や、書誌情報などの公開情報に基づいて実施するとしていることが特徴的である。

英国のアプローチは、国家保護安全保障局（NPSA）の「Trusted Research Checklist for

Academia」に見られるように、国際的な共同研究における潜在的なリスクについて確認し、学者や研究者を導くことをより指向している。このチェックリストは、具体的なリスク評価プロセスを詳述するものではないが、研究者が研究インテグリティを維持することに焦点を当て、新規および既存のパートナーシップを評価するための枠組みを提供するものである。

オーストラリアは、UFIT ガイドラインに代表されるように、大学部門における外国からの干渉に対抗するための包括的なガイドラインと行動計画を策定している。これらのガイドラインは、デューディリジェンスの方法、リスク評価、管理戦略について詳述しており、特に重要な技術や、外国からの資金援助、外国人材プログラムへの関与、外国政府や制裁対象団体との提携がもたらす潜在的なリスクに焦点を当てている。

カナダのアプローチでは、研究助成機関と、カナダ公安庁、カナダ安全保障情報局、通信安全保障機構などの国家安全保障機関との間の共同作業が行われる。カナダにおけるリスク評価プロセスは、資金提供機関からの照会を受けて開始され、研究者の所属、特に外国の軍事・安全保障機関とのつながりなど、国家安全保障にリスクをもたらす可能性のあるものを徹底的に評価することが含まれる。

欧州連合（EU）の戦略は、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など、多方面にわたる外国からの干渉に対処するための包括的なツールキットを包含している。EU は、組織レベルおよび個人レベルでの脆弱性評価の実施、海外干渉委員会の設置、攻撃を検知・防止するための強固なサイバーセキュリティ対策の実施に重点を置いている。

これらの国・地域は、研究インテグリティ、研究セキュリティを確保し、国家安全保障を守るという包括的な目標を共有しているが、リスク評価基準の具体性の度合い、学問の自由と安全保障上の懸念のバランス、学術機関と国家安全保障機関との協力の度合いなどの相違もみられる。

第3章　国内の取組の調査・整理・分析（ヒアリング調査）

3.1　ヒアリングの実施概要

国内の大学と国立研究開発法人における、研究インテグリティの確保、特に、研究の国際化やオープン化に伴う新たなリスクに対する対応のための取組等の現状や課題を把握し、今後の研究インテグリティの確保のための取組に役立てていくことを目的としてヒアリングを実施した。

ヒアリングは国内の大学・国立研究開発法人 10 機関（7 大学、3 国立研究開発法人）を対象として、2023 年 11～12 月に、約 1 時間半の時間でオンラインで実施した。ただし、1 大学については質問項目への書面での回答を得た。大学・国立研究開発法人の研究インテグリティあるいは関連業務を担当する部署の職員等（担当部署の部課長等）からの対応を得た。ヒアリングは未来工学研究所の担当者が実施し、内閣府と文部科学省から調査関係者がオブザーバーとして参加した。

質問項目は後述のとおりであり、ヒアリング実施前に質問リストを送付し、ヒアリングでは適宜補足の質問をした。また、ヒアリングは対象機関や担当者の名称は公開しないことを前提に実施し、ヒアリング対象機関は、ヒアリング結果についての報告書原稿内容の確認を、公開の適切性等の観点からお願いした。

3.1.1　対象機関の選定

7 大学、3 国立研究開発法人にヒアリングを実施した。大学については、「令和 3 年度　大学等における産学連携等実施状況」（文部科学省）、国立研究開発法人については「（令和 4 年度）研究インテグリティフォローアップ調査結果」で、1）回答時点までに利益相反・責務相反に関する規程を既に整備し、2）研究インテグリティの確保のためリスクマネジメントをする組織体制を既に整備し、かつ、3）関係者に適切な理解を促す取組を実施している大学・国立研究開発法人の中から、選定した。これらの条件を付したのは、既にある程度の取組をしている大学・国立研究開発法人からの取組の現状や課題について回答を得るためである。

また、さらに、大学については、機関種別（国立、公立、私立）、研究大学かどうか、規模（教員数、科研費獲得金額）、総合大学か単科大学か、の観点から選定した。以下の大学を選定した。選定した大学に対して、内閣府からヒアリング実施について打診し、承諾を得た上で実施した。

A 大学：大規模国立大学。研究大学。
B 大学：大規模国立大学。研究大学。
C 大学：中規模国立大学。
D 大学：公立の総合大学。
E 大学：私立の総合大学。

F 大学：私立の総合大学。

G 大学：私立の工業大学。

国立研究開発法人については、主要な機関から 3 法人を選定した。同様に、選定した法人に対して、内閣府からヒアリング実施について打診し、承諾を得た上で実施した。

3.1.2 ヒアリング質問項目

質問内容は以下の囲み内のとおりである。1）研究インテグリティ確保のための規程整備、2）組織体制・運用方法（開示情報のリスク判断、リスクへの対応プロセス、既存の組織体制との関係）、3）運営トップレベルの関与、4）研修・教育、5）他機関との連携状況と、6）政府・資金配分機関への要望・提案の 6 項目について伺った。1)～5)の項目については取組等の現状と課題について伺った。

質問項目 1)と 2)は、研究インテグリティへの対応のためには大学・国立研究開発法人の規程策定と組織体制の整備がまず求められると考えられるため含めたものである。また、質問項目 3)についてはそれら体制整備を進め、効果的に運用していくためには理事長、学長等のトップレベルの関与が重要だろうと考えて含め、質問項目 4)については、研究インテグリティの確保のためには体制整備に加え、教職員の知識や意識の向上が求められると考えられるために含めた。質問項目 5)については、大学・国立研究開発法人が研究インテグリティの確保のための取組等を進める上では他大学・他国立研究開発法人における先進的な取組についての知識獲得や、同様の課題を持つ大学・国立研究開発法人間での情報共有が重要だろうと考えて含めた。最後の質問項目は、今後の政府における施策等を考えるための情報を得るためである。

- 貴機関における研究インテグリティの確保のための規程整備（利益相反・責務相反に関するもの等）の内容と運用方法を教えてください。また、それら規程整備に関連する課題はありますか。
- 貴機関では、研究インテグリティの確保のためのマネジメントを行う組織体制と運用方法を教えてください。また、その体制・運用に関連する課題はありますか。
  - 研究者が開示した情報（職歴・研究経歴、所属機関・役職（兼業や、外国の人材登用プログラムへの参加、雇用契約のない名誉教授等を含む）、外部機関から受けている各種の支援）についてどのようにリスク判断をしていますか。また、開示された情報内容の適切さ、正しさはどのように確認していますか。これらの点について、どのような課題がありますか。
  - リスクが懸念される場合の対応プロセスはどのようなものですか。
  - 既存の組織体制（安全保障輸出管理、産学連携、研究不正対応等）との関係はどうなっていますか。
- 貴機関の運営トップレベルは、研究インテグリティの確保に向けての検討体制や運営体制にどのように関与していますか？具体的な取組や意思決定プロセスを教えてくださ

い。

- 貴機関では、研究インテグリティの確保に向けて、関係者（教員、研究者、職員、学生）の理解を促すための研修・教育やセミナーの実施内容と頻度、効果を教えてください。また、その研修やセミナーに関連する課題はありますか。
- 貴機関は研究インテグリティの確保のための取組（規制整備整備、体制整備、研究実施等）に関して、他大学・研究機関との連携をどのように進めていますか。具体的な連携内容や取組を教えてください。また、その連携に関連する課題はありますか。
- 政府には、研究者及び大学・研究機関等における研究インテグリティの自律的な確保を支援する役割がありますが、貴機関において研究インテグリティの確保を進めるに際して、政府や資金配分機関に対しての要望はありますか。具体的な要望あるいは提案があれば教えてください。

3.2　ヒアリング結果

3.2.1　大学へのヒアリング結果

(1)　A大学

A 大学は国立大学であり、研究大学である。

a.　規程整備の内容・運用方法とその課題

研究インテグリティに関連する利益相反に関しては研究推進部研究推進課が担当しており、利益相反等に関する規程が以前から設けられ、運用されている。特に現存する利益相反の規程等を新たに改定するという形での運用は行われていない。研究インテグリティに関しては、「研究インテグリティの確保に関する規程」を新設し、必要な事項をまとめた。本規程で対象とするのは、研究活動の国際化やオープン化に伴い生じる新たなリスクへの対応である。既存の規程でカバーされている領域に関しては、新たな対応を行うものではない。

2022 年から検討を重ね、2023 年 3 月に該当規程を施行した。規程に関する検討の際に、「研究インテグリティ管理に関する基本方針」という文書も併せて作成した。方針を初めに策定し、その方針に基づいて関連する他部署との意見交換を行い、細部を調整した。「研究インテグリティの確保に関する規程」の内容に関しては、東北大学の同様の規程を一定程度参考にしながら作成した。しかし、本学としては「研究インテグリティ・マネジメント室」を新規に設立しており、この部分においては他の大学と異なると考えられる。

規程整備の段階において、特に課題となったのは、利益相反の管理、特に研究インテグリティに関連する利益相反の担当部署をどこにするかであり、かなりの協議を要した。産学連携における利益相反と研究インテグリティに関連する利益相反は、概念や管理すべき事項において大きく異なると理解している。このため、従来の利益相反の管理枠組みでは対応が困難であるとの判断のもと、研究インテグリティに関連する利益相反については、研究インテグリティの担当部署が管理することとなった。

b.　組織体制と運用方法と、関連する課題

本学では、上記のように、新たに「研究インテグリティ・マネジメント室」を設置した。研究インテグリティ・マネジメント室は、横並びの部署よりも上位に位置し、様々な側面からの判断を行った上で、各担当部署に対して情報収集の要請や問題対応の指示を出すコントロールセンターの役割を果たしている。他大学では、委員会を立ち上げ、従来の部局による対応と委員会による判断を行っていると考えられるが、本学ではこの新室の設立により、従来の本部の他部署とは異なる形で、研究インテグリティのみを専門的に管理している。利益相反や安全保障輸出管理については、各部局から本部に案件が上がり、情報が流れる体制

が整っており、既存の委員会等が各案件について判断を下している。しかし、研究インテグリティに関しては、その案件の複雑さから、本部の他の組織とは別に「研究インテグリティ・マネジメント室」を設立し、従来の本部の部署と情報共有を行いながら、研究インテグリティに関する管理を行っている。この体制では、研究者から直接「研究インテグリティ・マネジメント室」への相談や問い合わせ、自己申告が行われる。

同時に設置した「研究インテグリティ・マネジメント委員会」のメンバーには、研究担当理事及び本部の連携部署の課長級職員が参加している。

本学では研究インテグリティに関しては早期対処とリスク管理が重要であると考えている。そのため、重大でない案件については、まず研究インテグリティ・マネジメント室が基本的に処理を行う。重大な事案に関しては、研究担当理事に直接、報告と相談を行う。インテグリティ・マネジメント室では、研究担当理事や執行部からの判断を求める形で管理を行っている。また、自己申告に関しては、研究者から直接オンライン等を通じて情報を提供いただき、研究インテグリティ・マネジメント室にて情報の分析を行っている。

研究担当理事に直接かつ迅速に相談を行うような運用方法を採っており、研究インテグリティに関連する件で少なくとも 2 週間に 1 回程度の頻度で相談が行われている。

研究インテグリティに関しては、各部局による判断ではなく、すべて研究インテグリティ・マネジメント室に集約する体制を取ることにした。これは、研究インテグリティ・マネジメントに関しては、大学の経営方針に基づいた経営判断に関わる事項が多いため、各部局の担当者に判断を任せるのではなく、直接本部にて管理を行うという趣旨に基づく。

研究インテグリティ・マネジメント室では、研究インテグリティ担当の専任教員としてのポストを設け、同教員が室長を務めている。本学では安全保障輸出管理と研究インテグリティ・マネジメントが一体化しており、室長は安全保障と研究インテグリティの両方を担当している。その他の職員は講師 1 名、専門職員 1 名、事務補佐員 1 名の計 4 名で運営している。事務職員は研究推進部に所属し、研究インテグリティと安全保障輸出管理を担当している。なお、研究インテグリティ・マネジメント室の教職員数は 4 名であるが、ここで勤務する教職員は、安全保障や国際的なリスク判断に関する特別なバックグラウンドを有するわけではない。

開示情報に基づくリスク判断の方法、関連する課題

リスクの判断については、主に四つの観点（利益相反・責務相反、安全保障輸出管理、経済安全保障・研究インテグリティ、軍事研究）から管理を行っている。各案件については、これらの観点から個別に評価し、問題の有無や特に問題のある部分を判断している。

研究インテグリティに関する利益相反・責務相反リスクに関しては、主に責務相反リスクが重要であると考えており、従来の利益相反管理では十分にカバーされていなかったが、今後は責務相反リスクの管理が必要であると認識している。情報流出や技術流出リスクに関しては、安全保障の観点からの管理を行ってきたが、安全保障リスク管理以外の部分で、経済安全保障の観点からの管理が必要と考えられる技術についても検討を進めている。研究

妨害リスクとしては、外部からの影響による研究内容の妨害や、その可能性についても検討している。最後に、信頼低下リスク、レピュテーション・リスクとして、外国政府からの影響を受けた中で教育現場で学生に与える影響やその可能性の管理も、研究インテグリティの観点から新たに判断が必要であると考えている。

情報の適切さや正確さに関しては、インターネットを用いた確認等、可能な範囲で裏付け調査を行っているが、詳細な内容や連携の経緯等については、研究者個人に尋ねる他ないため、個々に情報のフォローアップ調査を行っている。本学では、教員が正確な情報を提供しているという前提で運用しており、客観的な調査結果に基づいて裏付情報の確認を行うが、追加調査や正確性の判断に多くの時間を費やすことは行っていない。

課題に関しては、研究者本人のみが把握している情報や、本人からの申告がなければ得られない情報の取得が困難である点が挙げられる。これらの情報をどのように確保するかが課題である。さらに、本年度初めて研究者から自己申告を受けた際には、外国からの資金提供や無償の便宜供与等に関して、教員が正確に理解するのが難しいという問題が生じた。また、人材登用プログラムに関しては、本人が十分に認識していない場合もあり、現在の国際情勢を鑑みると、このようなプログラムを明確に識別し、情報を導き出すことが特に困難であると認識している。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合の対応プロセスについては、研究インテグリティ・マネジメント室が相談内容の詳細を聞き、分析を行った上で必要な対応策を検討し、研究担当理事に相談する。その後、対応策に関しては、我々から直接教員に対し、管理方法の提案や注意点の指示などを行う形で対応をお願いしている。

既存の組織体制との関係

既存の組織体制との関係に関しては、研究インテグリティ・マネジメント室を設置し、業務を一体化させているため、特に問題はないと認識している。人事、産学連携や研究不正に関しても、体制構築時に複数の打ち合わせを重ね、良好な関係を築いているため、必要な情報提供が協力的に行われている。部局との関係に関しても同様である。リスク判断に際しては、必要な情報を提供いただき、我々が判断した内容は情報提供として共有し、関連部署にも通知する形で運用している。ただし、各部署が取得した情報は、それぞれの部署で管理すべきものであり、関連部署のみで確認する形で情報を取得しているため、我々が勝手に他部署のデータにアクセスすることはない。

c. 運営トップレベルの関与（取組、意思決定プロセス）

本学においては、研究インテグリティについて、役員会、部局長会議の両方で先に説明を

行い、その理解を得た上で、全学的に情報を広めている。役員は、特に意識が高く、早期対応の重要性や経済安全保障における問題点について積極的に意見を述べており、それに対応することが課題となっている。このように、運営トップレベルでの理解と敏感さが高まっていると認識している。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

教員に対して簡潔な説明で研究インテグリティの内容を伝えることの難しさを認識しており、まずは継続的な説明を行うことに重点を置いている。安全保障輸出管理の説明会では、研究インテグリティに関する情報も併せて提供している。加えて、部局長会議で研究担当理事から話をして、部局長レベルでの理解促進を図っている。

特に人文社会科学系については、従来、安全保障輸出管理に関しては対象外との認識があったが、本学では研究インテグリティが分野を問わないことを強調しており、自己申告についても適切に対応してもらっている状況である。

2023 年 4 月からは、本学独自の e ラーニング教材を開発し、学内で利用可能にした。また、各部局に対して、研究インテグリティに関する説明会の開催を周知し、部局の依頼に基づき実施している。説明会の内容としては、想定される事例と本学で実際にあった相談事例を脚色して紹介し、理解を深める取組を進めている。また、本学の手続きや研究インテグリティに関する基本的な情報を提供しており、教員の多忙を考慮し、重要なポイントを先に伝えるなどの工夫もしている。最終的には説明会に参加した研究者が、自己申告の必要性について理解し、実際に発生した事例を参照に教員が類似の事態に遭遇していないかを自ら確認することを目標としている。2024 年にはブラッシュアップを行い、具体的な事例を紹介することで、より理解しやすい内容に改善することを目指している。

加えて、研究安全保障と研究インテグリティを統合した講演を今後実施する予定である。実際に講演を行うと、多くの相談が寄せられる効果が見られる。教員からは、特定の案件に関する質問や、これまで気づかなかった事項についての申告などが寄せられている。このため、e ラーニングも重要だが、直接対面での説明の重要性も認識している。ただ、教員も多忙であるため、時間的な制約が大きい。そのため、教授会等での短時間の説明をお願いしており、10 分から 15 分の短い時間でも理解できるような内容を準備することを優先している。

e. 他大学・研究機関との連携、関連する課題

他大学からの依頼により、本学の取組について紹介をするということが、2023 年に入ってから増えてきた。おそらく、本学の研究インテグリティのホームページに情報を掲載していることから、多くの方がそれを見て、本学の体制を知りたいと考えているのであろう。基本的には名刺交換を行ったことで、多くの方から連絡を受けるという状況である。内容は様々で、まだ体制が整っていないため、どうするべきかという問いかけがある一方、ある程

度体制ができており、e ラーニングなどの細かい部分の対応についての意見交換を行うこともある。

本学は国内の大学をリードする役割を担っており、イニシアティブを取ることが一つの目標である。安全保障のみならず、研究インテグリティの面においても、他の大学を引っ張っていく立場を目指している。そのため、本学の体制が他の大学に役立つのであれば、意見交換を通じて、その知識を広めていくことに力を注ぎたいと考えている。

課題としては、名刺交換などをして知り合いにならなければ、他の大学の体制について情報交換を行うことは難しいということである。安全保障の分野では経済産業省がアドバイザー事業を実施しており、先進的な大学の教員を派遣し、情報交換やアドバイスを提供するようなことをしている。このようなサービスを利用することは、知り合いではない大学からもアドバイスを受ける手段として、より容易であると考えられる。

f. 政府・資金配分機関への要望・提案

本学では、既に 1 年間をかけて研究インテグリティについて解釈を深め、研究インテグリティ・マネジメントについての方針を確立してきた。現時点で特に政府への要望はないが、将来的には、この分野を適切に管理できる人材が必要であると考えている。今後、どのようにこれらの人材を育成していくかについての検討が求められる。

また、本学としては、将来的には、研究全体をマネジメントする体制を目指しており、研究インテグリティはその一部になるが、このような体制構築に必要な資金やサポートがあると望ましい。さらに、安全保障の分野と同様に、研究インテグリティに関する理解を深めるための研究も必要であると考えている。

(2) B大学

B 大学は関東地方の国立大学であり、研究大学である。

a. 規程整備の内容・運用方法とその課題

研究インテグリティの確保を目的として、2022 年 4 月 1 日に本学の利益相反規則を改正した。改正の概要は以下の通りである。

ア. 随時報告の追加：これまで年 1 回の報告のみであったが、事案に応じて随時報告を求めるように変更した（修正報告も含む）。

イ. 企業等の範囲の拡大：報告対象を、本学と契約関係にある企業等に限定していたものから、全ての企業等に拡大した（株式等の保有を除く）。

ウ. 個人的な利益の範囲の改定：兼業報酬、実施料等の収入、給与、株式等の保有に加えて、企業等からの本学の管理下にない資金、施設・設備・機器等の物品、役務等の受け入れで、職務に関連するもの、又は職務の信頼性を損なう恐れのあるものを金額に関わらず全て対象とする。

次に、経済産業省によるみなし輸出管理の明確化に伴う関連省令・通達の改正に対応し、輸出管理を強化するため、2022 年 5 月 1 日に本学の安全保障輸出管理規則を改正した。改正の概要は以下の通りである。

ア. 学生・教職員の受け入れ時に「特定類型該当性」の確認を新たに規定し、技術提供に関する事前確認時の帳票類を追加（「特定類型自己申告書」「誓約書」）および改訂（「確認シート」「取引審査票」）した。

イ. 輸出管理統括責任者（特定類型該当者の把握）および部局輸出管理責任者の規定を見直し、規則違反に対する罰則規定を明記（追加）した。

研究インテグリティの確保に関する課題としては、大学教員は、教育・研究活動以外の研究資金獲得のための活動や大学運営に関わる活動に忙殺され、研究活動のための時間がますます少なくなっていることがある。また、研究インテグリティの確保で問題とされる行動に関わっている、あるいは関わる可能性のある教員は限られているという実態もある。したがって、研究インテグリティの確保を目的とした規則・規程整備においても、教員の負担をできる限り低減することに配慮しながら、技術流出やレピュテーション・リスクに対応できる体制を整備していくことが必要である。本学の利益相反規則の改正は、このような意図の下に行われた。

また、経済産業省によるみなし輸出管理の明確化に伴う関連省令・通達の改正に関連する課題は、輸出管理を以前よりも厳格に実施した結果、大学本部及び部局における事務負担が大幅に増大したことである。

b. 組織体制と運用方法と、関連する課題

研究インテグリティの確保のための組織体制の整備

2023 年 3 月に、研究インテグリティの確保のための基本方針を策定し（2023 年 3 月 23 日学長決定)、研究インテグリティの確保に関する規則（2023 年法人規則第 30 号）を制定した。続いて 2023 年 5 月には、研究インテグリティの確保のための具体的な対応策を定め（2023 年 5 月 29 日研究担当副学長決定)、これらを学内の各部局に周知した。

研究担当副学長を研究インテグリティ・マネジメントの統括責任者とし、学長の下で統括責任者を議長にした「研究インテグリティ・マネジメント会議」（7 人の副学長等で構成）を設置した。この会議は産学連携、学生、国際、財務、人事を担当する副学長、利益相反・輸出管理マネジメント室長などを構成員として、研究インテグリティに関する基本方針、戦略及び重要事項の審議を行うものである。さらに、統括責任者を委員長とする「研究インテグリティ・マネジメント実務委員会」（8 人の各課長・室長等で構成）を設置した。この委員会には国際室、組織・職員課、財務企画課、学生交流課、研究企画課、産学連携企画課、利益相反・輸出管理マネジメント室の各課長・室長が委員として参加し、関係法人規則等の制定及び改廃の立案、要請、調査、教育研修等の審議を行う。

また、研究インテグリティに関する相談窓口（大学本部研究推進部研究企画課総務係）を設置した。

研究インテグリティの確保のための組織体制の運用方法

本学では、研究者からの情報開示だけでなく、問題が発生する前の段階での大学本部への相談を重視している。各部局の教員や事務担当者には、「研究インテグリティの確保のための具体的な対応について（研究担当副学長決定)」に示された想定されるリスク事例が発生した場合、直ちに本部の相談窓口に相談するように周知している。

相談があった場合、相談窓口は当事者から詳細な情報を収集し、利益相反・輸出管理マネジメント室に連絡し、そこで可能な限りの情報を収集してリスク評価を行う。その結果は研究企画課に伝えられ、研究企画課と研究担当副学長が協議し、必要に応じて研究インテグリティ・マネジメント会議や研究インテグリティ・マネジメント実務委員会の開催の必要性を判断する。特に重要な案件については学長と協議して対応案を検討し、その結果に従い担当教員等と面談して最終的な措置を決定する。これらの経緯や最終的な措置については、研究インテグリティ・マネジメント実務委員会等のメンバーと情報共有している。

課題としては、本学の研究インテグリティの確保のための組織体制は、2023 年 7 月に運用を開始して以降、成果を挙げつつあるが、学内の各部局の教員・事務担当者と本部との間で、研究インテグリティの確保の重要性についての危機感を共有することであり、それが運用を軌道に乗せる上での鍵となると認識している。

開示情報に基づくリスク判断の方法、関連する課題

研究の健全性・公正性に関連するリスクが生じる可能性がある事例が発生した場合、まずは当該事例が「ア 先端的な重要技術等の提供であるかどうか」を判断する。

該当する可能性がある場合には、次に「イ 相手国・地域・機関の懸念度が大きいかどうか」および「ウ 世界情勢等からのレピュテーション・リスクがあるかどうか」を判断する。

特に、「イ 相手国・地域・機関の懸念度が大きいかどうか」に関しては、主に利益相反・輸出管理マネジメント室が判断を行う。判断の基準としては、「輸出管理対象国のグループ D」や経済産業省の「外国ユーザーリスト」に掲載されている国・地域・機関であるか、米国商務省産業安全保障局（BIS）のウェブサイト掲載の Entity List に記載されているか、オーストラリアの独立系シンクタンク（ASPI）が作成したリストに掲載されている中国の大学・研究機関であって懸念度が高い場合であるかどうかなどを評価基準とする。また、安全保障貿易情報センター（CISTEC）が提供する情報（CHASER）なども参照し、リスクを総合的に判断している。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合の対応プロセスについては、上記のとおりである。

既存の組織体制との関係

研究インテグリティの管理については、研究企画課が所管しているが、研究企画課は、研究不正に関する事項も所管している。さらに、研究企画課は安全保障輸出管理を担当する利益相反・輸出管理マネジメント室と密接に連携し、研究インテグリティに対応している。また、産学連携を担当する産学連携企画課も研究インテグリティ・マネジメント実務委員会のメンバーとして、情報を共有している。

この研究インテグリティ・マネジメント実務委員会は、研究インテグリティの統括責任者を含む、国際局国際室の担当課長、総務部組織・職員課長、財務部財務企画課長、学生部学生交流課長、研究推進部研究企画課長、産学連携部産学連携企画課長、利益相反・輸出管理マネジメント室長で構成されている。これらのメンバーは、研究インテグリティに関連するあらゆる情報を共有しており、組織間の緊密な連携を通じて、研究の健全性と公正性を保つための体制を強化している。このような構造は、異なる部門間の連携を促進し、研究活動における様々な側面で発生するリスクを管理するために重要である。

c. 運営トップレベルの関与（取組、意思決定プロセス）

本学では、研究インテグリティの確保のための取組として、学長が体制整備の責務を負い、研究担当副学長を研究インテグリティ・マネジメントの統括責任者に任命している。この統括責任者の下に、産学連携、学生、国際、財務、人事を担当する副学長および利益相反・輸出管理マネジメント室長をメンバーとする「研究インテグリティ・マネジメント会議」を設置している。この会議では、研究インテグリティの確保に関する基本方針、戦略及び重要事項を審議し、研究の公正性と透明性を保つための重要な決定を行っている。

加えて、学長自身もこの問題に積極的に取り組んでおり、統括責任者である研究担当副学長は、問題の重要性に応じて、随時、学長と協議しながら問題の取り扱いを進めている。これにより、研究インテグリティに関する問題に迅速かつ適切に対応するための柔軟な体制が確立されている。

d.　研修・教育、セミナーの実施内容・頻度・効果、関連する課題

本学では、研究インテグリティの確保を目的とした様々な研修・教育活動を実施している。具体的な活動内容は以下の通りである。

研究インテグリティへの対応に関するチラシの作成・配付

研究インテグリティに関わる利益相反規則の改正に伴い、A4 版表裏のチラシ（日本語及び英語）を作成し、2022 年 3 月に全学に配付し周知を図った。また、利益相反・輸出管理マネジメント室のウェブサイトにも公開し、誰でも閲覧可能にした。

研究インテグリティ確保のための動画の作成と配信

「利益相反自己申告制度の変更についてー研究インテグリティへの対応ー」と題する解説動画を作成し、2022 年 3 月に利益相反・輸出管理マネジメント室のウェブサイト及び学内 e-learning サイト「manaba」で公開し、常時学習可能にした。この動画については学外者も閲覧できるため、学外からの相談も複数寄せられている。

コンプライアンス専門委員会セミナー

2022 年 7 月 26 日に全教職員対象のセミナー（オンライン）で、「研究インテグリティと利益相反事例」と題した講演を実施した。

2022 年度研究倫理 FD 研修会

2023 年 3 月 10 日に、研究推進部主催の研修会で、研究者や研究に関する業務を行う事務職員を対象に、「研究インテグリティの自律的な確保を目指してー利益相反マネジメントと輸出管理を中心としてー」と題した講演（オンライン）を実施した。

コンプライアンスセミナー

2023 年 9 月 7 日に「研究インテグリティの自律的な確保のために」と題した講演（オンライン）を実施した。この動画は学内 e-learning サイト「manaba」に掲載され、学内構成員が常時視聴できるようになっている。また、英訳して英語での視聴も可能にした。

これらの取組により、研究インテグリティに関する意識が高まり、学外からの相談も複数寄せられている。

e.　他大学・研究機関との連携、関連する課題

研究インテグリティへの対応について、国立大学法人等研究協力部課長会議等において情報交換及び意見交換が行われている。また、大学が所在する地区等における輸出管理業務関係の部署の会合においても、情報交換が行われている。

f.　政府・資金配分機関への要望・提案

大学は諜報機関や調査機関ではないため、国際交流の相手機関のリスク評価に係る情報収集には困難が伴う。この点において、JST や NEDO などから懸念情報の提供があれば有益であると考えられる。

また、外為法が対象とする機微技術については、条約や国際的な枠組みに基づいて、大量破壊兵器の開発などへの利用・転用の可能性があるものが管理対象である。技術等の提供の

許可・不許可は最終的に経済産業大臣が判断する。このような明確な目的と判断者の存在は、管理の理解を容易にする。しかし、研究インテグリティの確保に向けた対応においては、教職員から利害関係の情報開示を求めたとしても、その情報の扱い方や判断基準、対策の方法が明確でなく、外為法に基づく技術流出管理とは異なる管理方法を示す必要がある。これがなされない場合、輸出管理との二重管理に陥る可能性がある。

(3) C大学

C 大学は中規模の国立大学である。

a. 規程整備の内容・運用方法とその課題

「研究インテグリティの確保に関する規程」を 2022 年 7 月に制定した。文部科学省や内閣府からの通知等を受け、作成されたものである。内容については、文部科学省からモデル例として示された内容を活用するなどしており、特別な規程を制定しているわけではない。中心的な内容としては、「研究インテグリティ・マネジメント委員会」を立ち上げること、およびこれを担当するのが研究推進課であることである。具体的な研究インテグリティ上の課題が発生した際の対応プロセスについては、委員会で議論されるが、規程上での具体的な運営方法については明記されていない。

利益相反に関しては、「利益相反マネジメント規程」が別途存在し、こちらで取り扱われている。

b. 組織体制と運用方法と、関連する課題

本学においては、多くの大学でも見られるように、研究インテグリティ・マネジメント委員会および研究インテグリティ・マネジメント専門委員会を設置している。担当理事は、研究担当理事である。研究インテグリティ・マネジメント委員会には、研究担当理事の他、人事担当理事、総務担当理事、そして 1 名の教員が含まれている。専門委員会には、この教員がトップとして参加し、各種案件に応じて人事、利益相反、安全保障輸出管理などを担当する職員が加わっている。

委員会の開催頻度に関しては特に決められたものはない。研究インテグリティ・マネジメント委員会は初回に一度開催され、その際に研究インテグリティ・マネジメント専門委員会の体制等が決定されたが、その後は特定の案件がないため、開催されていない。なお、委員会の招集については担当理事が決定する。

研究インテグリティ・マネジメント委員会の事務局に対して、研究者が直接相談することも可能となっている。窓口に連絡が入った後は、必要に応じて研究インテグリティ・マネジメント専門委員会や研究インテグリティ・マネジメント委員会へ案件が回される運用になっている。

実際の運用としては、安全保障輸出管理、利益相反、共同研究、寄附など関連事項については、通常の学内ルールに従って手続きを進める。個々の案件を判断しているのは、部局の担当部署である。例えば安全保障輸出管理の場合、事前に相談シートが提出されると、それを基に担当する複数名の教員が内容を確認する。確認において、リスクが存在すると判断され、安全保障輸出管理のみでは決定が困難な場合、研究インテグリティの窓口に連絡が来るような体制になっている。相談事項については、まず部局に提出され、部局において対応さ

れる。専門家もいないため、基本的には部局の教職員が関連業務を担当している。

研究インテグリティの委員会を設置する理由として、各委員会の境界に位置するような問題が多い場合や、複数の委員会が関わる案件が存在する場合に、この委員会の存在意義が顕在化すると考えられる。しかし、現時点で、本学において、そのような案件は特に発生していない。国の観点からは、他の委員会を総括する形で研究インテグリティ委員会が機能することが期待されているかもしれないが、実際は並列的に設置されている感がある。現在の仕組みの構築にあたっては、大規模な大学の仕組みを参考にしているが、特に人的リソースの面で大きな違いがあるため、100%同様の仕組みを取り入れることはできない。

研究インテグリティの事務担当は現状 1 名である。関連する案件として 2023 年度に相談があったのは 1 件のみである。大規模な大学や国際交流に特に注力している大学と比較すると、研究インテグリティの案件となりうる海外との案件自体が少ないというのが現状である。

課題として、実際に検討が必要となる案件が発生した場合、どのように対応するかという点があるが、必要に応じて学内で適切な知識を持つ人間を加え、委員会において検討を行うことになると思われる。

また、本学では部局ごとに研究インテグリティ関連の取組に若干の温度差が見られる。特に、理系学部は、研究内容の関係上リスクが高いため、積極的に関与している。一方、文系学部は、関連性が低く、研究インテグリティに関してはそれほど積極的ではないと感じている。

開示情報に基づくリスク判断の方法、関連する課題

安全保障輸出管理の場合、相手方の情報はインターネットで検索するなどして、十分に調査を行っている。共同研究時には、受け入れる人物や相手方についても同様に調査を行う。ただし、職員採用時の過去の経歴チェック、兼業先の役職確認等は、大きなリスクが懸念される場合以外は履歴書や書類、本人の申告ベースでの確認となり、実施可能な範囲でのみ確認をしているのが現状である。

研究インテグリティの観点から、懸念される組織・人物を考慮する際、具体的な相手方情報の判断は、主に外国ユーザーリストや米国のリスト（ENTITY LIST、Denied Persons List）に基づいて行われている。日本の法律に則った場合は、外国ユーザーリストが主な基準となり、それに基づいて相手先を判断している。他の情報源から得られる情報は限られており、大部分の場合、これ以上の情報は入手できていない。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合の対応プロセスには、先に述べた委員会が関与することになる。リスクが懸念される際には、まず全学の窓口に連絡をしてもらうように指示している。その後、内容を確認し、前述の委員会で判断を下すことが一般的な流れである。教員からの相談

や、各部署においてリスクが懸念される何らかの事項が生じた場合は、必要に応じて担当理事と相談することになるが、先にも触れたように、2023 年についてはこれまでに 1 件しか発生していない。

既存の組織体制との関係

既存の組織体制（安全保障輸出管理、産学連携、研究不正対応等）との関係については、利益相反など他の委員会が担当する領域との横連携は十分に取れていると思われる。研究インテグリティの委員会はほとんど開催されていないが、安全保障輸出管理に関する委員会は概ね毎月開催されており、委員会では研究インテグリティに関連する問題にも踏み込んだ検討がされている。

研究インテグリティ・マネジメント委員会には、利益相反の委員会に参加している総務課副課長、職員の採用業務に関連する人事課長、兼業関連の業務に関連する労務課長、さらに、産学連携や安全保障輸出管理の委員会に参加している研究推進課長等がメンバーとなっている。したがって、委員間での関連事項に関する連携はかなり幅広く、それぞれの委員会にはこのような複数の役割を持つメンバーが参加している状況である。

大学職員としては、研究推進課のほか、人事課、労務課、総務課の職員が関与しているが、職員レベルで日常的に情報共有や連携を行っている。本学は規模がそれほど大きくなく、関連事項の担当者が同じ建物内にいることもあり情報共有は容易である。

c.　運営トップレベルの関与（取組、意思決定プロセス）

運営トップレベルの関与や具体的な取組、意思決定プロセスについては、研究インテグリティの委員会には理事 3 名が参加している。この委員会は事実上学長直轄とも言える形で運営されており、トップマネジメントによる検討が行われている。意思決定のプロセスに関しては、基本的には委員会で検討することとなるが、重要な案件については、最終的に学長が決定することとなる。研究インテグリティに対する取組は、トップレベルの理解がかなり進んでいると感じられる。

d.　研修・教育、セミナーの実施内容・頻度・効果、関連する課題

研究インテグリティについては、2022 年度においては研修という形で行われておらず、外部講師を招きセミナーの形式で 1 回実施された。今年度は、コンプライアンス関係として、安全輸出管理、研究インテグリティ、利益相反、ハラスメント、内部統制など、多岐にわたり実施している。研究インテグリティ研修の実施頻度は基本的に年 1 回である。

研修そのものでどの程度効果が出ているのかは不明であるが、理解を深めるための取組として継続されている。教職員にどの程度の理解が求められるかについては、具体的な評価が難しい。案件が比較的少ないため、直接的な緊急性を感じていないことから、個々の認識

としては重要視されつつも、最も緊急性の高い課題とは捉えられていないことがある。逆に、安全保障輸出については、日常の研究活動や出張と密接に関連しており、その点に意識が向けられている。

従来対応してきた利益相反や研究不正等とは異なり、研究インテグリティについての学内での理解についてはスムーズに受け入れられているとは言えない。実際、現場の教員からは研究インテグリティについての基本的な疑問を受ける事もあり、そもそもの概念の理解から始めることが最も重要であると考えられる。

その他に課題としては、学内研修の実施が挙げられる。研究インテグリティのそもそもの概念を理解してもらうためにも学内研修は不可欠であるが、そのための研修資料の内製には、手間がかかると感じられる。今年度は動画を作成したが、内閣府の説明会の資料や、本学の組織体制等を用い、資料に AI の音声でナレーションを行い作成した。学内研修実施にあたって、活用できそうな動画を検索したが、外部で見当たらず、自前で作成する必要があった。経済産業省から提供されている安全保障輸出管理の説明動画のような、政府提供の動画があればそのまま活用することもできて非常に有用である。

e. 他大学・研究機関との連携、関連する課題

研究インテグリティについては学内の事項として捉えており、他大学・研究機関等の学外との連携は特に実施していない。周辺地域の大学と課題に関して協議する場は現時点では存在しない。経済産業省による安全保障輸出管理のネットワークがある程度である。研修を実施する際に、周辺大学の先生にお願いするようなことはある。

f. 政府・資金配分機関への要望・提案

大学では予算・人員が減少している状況であるため、研究インテグリティ等の管理的な仕事の増加は負担となっている。大きな規模の大学ではリスク管理を一元化した部署を設置し、そこに専門職を配置するなど効率的な運営も可能であろうが、本学のような多くの大学では、研究関連部署や総務関連部署など、様々な部署で通常業務に加えて研究インテグリティ等に関する業務が行われることとなり、体制を検討すること自体も負担となっているのではと考えている。

研究インテグリティについての体制整備を進める上で、最低限必要な条件について、共通的なガイダンスが政府から示される方がやりやすい。具体的な体制や運用に関しては、各大学に判断が求められているが、このようにヒアリングや追加のフォローアップ調査が継続的に行われるため、結局は、政府が考えている一定の形式で整備することを各大学は求められることになる。規模による違いはあるかもしれないが、最低限必要な条件が当初から明確であれば、より効率的に体制整備を進めることができると考えている。

(4) D大学

D 大学は関東地方の公立大学である。

a. 規程整備の内容・運用方法とその課題

研究インテグリティに関連して、利益相反・責務相反の規程及び安全保障輸出管理に関する規程を定めている。研究インテグリティ単独の規程は作成していないが、今後の課題として認識している。現時点での方向性としては、当面の間、既存の利益相反規程及び利益相反マネジメント委員会にて対応を継続することとなる。

利益相反に関しては、利益相反のポリシー、マネジメント規程、利益相反委員会の要綱、委員会の運用手順書を定めている。責務相反については、兼業規程が制定されている。利益相反マネジメント委員会は 2007 年に設置され、ポリシーは 2005 年に制定された。利益相反マネジメント委員会の下には、臨床研究の利益相反委員会と臨床研究以外に関する利益相反委員会を設置している。審議はこれらの 2 つの委員会にてそれぞれ行われ、年 1 回、親委員会である利益相反マネジメント委員会に報告を行う。利益相反マネジメント委員会は、外部有識者と契約し、委員会の運用手順書で定められた範囲外の相談を提供している。

利益相反委員会では、自己申告書の提出を教職員から受け、必要に応じて助言や審査の通知を行っている。自己申告書の提出が求められるのは、産学連携活動の開始時、共同研究開始時、倫理委員会の申請時、ベンチャー企業認定時である。責務相反に関しては、兼業が発生する場合に教職員から人事課へ申請書を提出し、それを基に確認を行っている。現時点では、利益相反、責務相反ともに基本的にエクセルの自己申告書を担当部署に提出している。

情報の開示者に関しては、利益相反は本学の教職員及び非常勤教職員で委員会が指定する者を対象としている。通常の利益相反・責務相反は学生を対象外としているが、倫理審査の際には学生を含む。責務相反に関しては、教職員全員に開示を求めている。開示する情報については、利益相反では情報開示者とその家族が学外団体から受ける一定以上の金銭的な利益や、研究に関与している企業に在籍しているかどうか、家族が関与しているかについて開示を求めている。責務相反については、どのような内容でどこと兼業しているか、報酬、契約期間について開示を求めている。

次に、安全保障輸出管理に関して、管理規程を策定し運用している。運用については、学生と教員で分けて行っており、医系・理系を中心に対応している。外国籍の教員は、特定類型に該当するか否かについて事前確認シートで確認を行い、入学・採用後は契約書を提出する。大学院生以上の留学生には、受入前に教員からの事前確認シートを取得し確認をするとともに、誓約書の提出を求めている。教員については採用時に特定類型に該当するか否かの自己申告書の提出を求めている。

安全保障輸出管理についての全体的な運用に関しては、経済産業省のアドバイザーに助言を受けながら体制を構築している。安全保障貿易センター(CISTEC)に加入し、該非判定に迷う場合は相談を行っている。また、地区の安全保障輸出管理担当者の勉強会や担当者ネットワークにも参加し、情報収集を行っている。学生に関しては、現時点で大学院生の医系・

理系大学院生、研究生を対象としている。

b. 組織体制・運営方法と、関連する課題

研究インテグリティに関連しては、利益相反の状況を学内理事で構成される利益相反マネジメント委員会で検討し、意思決定を行っている。委員会では、審査状況の把握、関連規程の策定、フローの設定等が理事長以下で判断されている。

研究推進部の研究支援担当課では、本学の研究リスクマネジメントの統括を行い、安全保障輸出管理と利益相反の業務に関しては同部の産学連携担当課が所管している。安全保障輸出管理に関しては、留学生を扱う部署や人事課などと連携し、連絡会を設置して情報共有を進め、セミナーの共同開催などで学内啓発活動を行っている。本学の規模に適した第一歩であると考えている。

各部署において利益相反、安全保障輸出管理、研究インテグリティを担当する職員は、利益相反と安全保障輸出管理に限定すると、職員は 2 名である。これら 2 名は業務の一環として、それぞれの対応を行っている。利益相反と安全保障輸出管理の業務量は、安全保障輸出管理が約 30%、利益相反が約 40%である。これらを担当する職員のバックグラウンドは、長年のリスク判断経験者という訳ではなく、一般職員である。そのため、利益相反や安全保障輸出管理においては外部の専門家をアドバイザーとして委嘱するなどして適宜助言を受ける体制を構築している。

URA（大学研究管理者）は配置しているが、研究インテグリティに精通した URA の配置に至っていない。専門家の URA を配置することは一つの手段であるが、本学の予算的な問題により実現に至っていない。

申告は研究者からの発生ベースで行われており、内容についても学内の兼業情報との結合は行われていない。そのため、大学全体としてのリスクマネジメント系の情報が集約されていない部分があり、データベースの構築や情報共有の部分の構築が必要である。

研究インテグリティ確保のためのマネジメント体制としては、文部科学省が示す東北大学の事例をモデルケースとして考えている。複数の部署と連携して進める必要があり、現在も連携はしているが組織体系的に一つのまとまりになっていない。理想的には研究インテグリティ専門の室を設置することであるが、本学の規模や予算的な問題により、現状では実現が困難である。

開示情報に基づくリスク判断の方法、関連する課題

情報の開示は、人事課や医学部など、各関連部署で行われている。必ずしも産学連携担当課が全て受けとる訳ではない。兼業関係の情報は人事課が、安全保障輸出管理関係は研究推進部が最終的な審査を行っている。

安全保障輸出管理に関しては、採用時、受入時に事前確認シートを用いて該非判定、リスト規制及びキャッチオール規制の判定を行っている。判断に迷う場合は、アドバイザーに相談してリスク判断を行っている。

情報の適切性、正確性の確認に関しては、基本的に手順書に沿ってコメントを出している。

手順書による判断が困難な場合、利益相反のアドバイザーに相談しリスク判断を行っている。ただし、提示された情報内容についての確認は一般に困難であり、今後の課題として認識している。

リスク判断の一元化に関しては、利益相反に関しては、利益相反委員会が最終的に確認を行い、責任を持っている。安全保障輸出管理の責任者を研究推進部長が兼務し、基本的にはその部署が確認を行っている。リスクが懸念される場合は、他の担当部署にも情報が共有される。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合、利益相反のアドバイザーや安全保障輸出管理の担当者に相談し、適切なマネジメントを行うようにしている。安全保障輸出管理の場合、該非判定を行い、判断が困難な場合は経済産業省のアドバイザーに相談を行う。

リスク判断については内閣府からのチェックリスト改定の通知があったが、現時点ではそれに対応した整備は行っていない。チェックリストに出ていることは承知しており対応については検討している。現時点ではリスク判断の見直しが必要になった場合には、適宜、アドバイザーに相談をすることとなる。

既存の組織体制との関係

組織体制については、利益相反、安全保障輸出管理、産学連携は産学連携担当課で行われており、研究不正に対する対応は研究支援担当課で行われている。兼業等に関しては人事課が担当している。このように情報については様々な場所に存在するが、特に安全保障輸出管理等に関しては、他部署と連携を取りながら必要な情報共有が行われている。

c.　運営トップレベルの関与（取組、意思決定プロセス）

公立大学のガバナンス構造として、学長は教育・研究を、理事長は経営全般および地方自治体との関係を担当している。利益相反や研究インテグリティに関する学内の責任者は、理事長である。トップレベルの運営体制に関しては、理事長をトップとするコンプライアンス推進委員会が設置されている。理事長以下のレベルでは、学内理事で構成される経営方針会議において、適宜意思決定が行われている。

現在、大学におけるガバナンスの強化は、本学としても重要な課題と捉えられており、理事長は度々ガバナンス体制の整備に努めている。2022 年のコンプライアンス担当の設立に続き、2024 年度 4 月に向けてさらなる体制整備が学内で検討されている。これは理事長のトップダウンによる動きである。

d.　研修・教育、セミナーの実施内容・頻度・効果、関連する課題

本学では定期的にセミナーを開催しており、利益相反に関しては 2021 年度、2022 年度にそれぞれ 2 回セミナーを実施した。安全保障輸出管理に関しては、2022 年度に経済産業

省のアドバイザーを招いてセミナーを開催した。

研修への学生の参加は可能であるが、セミナーは主に教員、研究者、職員を対象としている。学生に対する研修は必ずしも義務化されていないが、留学生に対しては入学時に注意喚起を行い、義務付けられている内容に関する資料を配布し、対象となる学生には誓約書の提出を求めている。理系、医系の学生については、現時点では日本人学生が多く、留学生については、特に中国からの学生が多い。英語の資料も提供されている。

課題として、本学では個別の利益相反や安全保障輸出管理の体制は整備されているが、全学的な理解を促進するための啓発活動が十分ではない。人員が限られている中で、啓発活動に十分に取り組むことが困難であることが課題となっている。

e. 他大学・研究機関との連携、関連する課題

本学では他大学の専門人材をアドバイザーとして招いており、連携につながっている。連携の実績として、3 公立大学において、研究支援部署の会議を年に 1 回開催し、その中で研究インテグリティやリスクマネジメントに関する状況について情報交換を行っている。会議以外の場でも適宜相談を行う状況である。

また、コンソーシアムへの参加も行っており、リスクマネジメント全般に関しては、様々な大学の集まる連絡会議に参加し、利益相反の勉強会にも参加している。安全保障輸出管理に関しては、アドバイザーから紹介された勉強会にも参加し、他大学との情報交換を行っている。

他の大学や研究機関との連携によるメリットは、学びや取組に関する情報共有である。具体的な事案に関する相談も行っているが、本学は工学部がないため、安全保障輸出管理に関する事案が直接的には多くない。国立大学は持っている情報量が多く、取組や対応が早い傾向にあり、国立大学からの情報提供を受けているが、本学の組織体制を考える上で役立っている。

f. 政府・資金配分機関への要望・提案

政府や資金配分機関に対する要望に関しては、本学はノウハウが少なく、人的リソースの配分が困難であることから、研究インテグリティの拡大を図る中で、資金面で支援が得られれば非常に助かる。人員については、具体的には 1 名の専門的知識を持つ職員を配置する必要がある。専門的な知識を持った人材を派遣してもらうか、または本学で雇用することが可能とするように支援が望ましい。アドバイザーとしての参加ではなく、組織に入り体制を構築し、全体をまとめるような役割を担う人材が必要であると考えられる。

政府からの情報提供や説明会は最近頻繁に行われており、多くの場に参加している。これらの情報提供は非常に参考になっており、進んでいる他の大学の事例から全体像を把握し、本学の体制において実施可能な部分を常に検討している。このような機会に参加できることを非常にありがたく思っている。

(5) E 大学

E 大学は関西地方の私立の総合大学である。

a. 規程整備の内容・運用方法とその課題

研究インテグリティの確保に関連する規程としては、まず研究倫理指針がある。研究倫理に関わる事項について、教員に対して本学での研究の倫理について定めている。また、利益相反規程と安全保障輸出管理規程を策定している。これらの３つの規程に基づき、研究倫理委員会、利益相反委員会、安全保障輸出管理委員会という３つの委員会を設置しており、各課題に対応している。

これらの委員会の事務局は研究部が担当しており、部内において連携が取れていると考えている。研究倫理と安全保障輸出管理は、研究環境を担当する課が担当し、利益相反に関しては研究企画課および人事課が関与している。利益相反・責務相反に関する懸念が生じた場合、利益相反アドバイザーに相談している。また、安全保障輸出管理に関しては、輸出管理アドバイザーに相談し、進めている。

本学では、研究インテグリティに特化した委員会は設けていないが、研究倫理委員会がその機能を担う方向で現在考えている。研究インテグリティの確保に向けて、研究者・職員から報告された情報を基に、組織としてリスクマネジメントを行うための規程等の整備については、既存の規程で対応することとなる。

政府から研究インテグリティに関する対応が求められるようになって以降、提供されたガイドラインの各項目について、内容を確認し、対応する部署と対応者を特定した。チェック体制に不足がある項目については新たにチェックフローを追加するなどの対応を取り、組織体制内での対応が可能であることが確認できたため、現行の体制で対応を進めている。新たな規程の必要性については、現在の規程で対応可能であると考えており、不測の事態についても、想定範囲内で対応できていると考えている。研究インテグリティ全般については、研究部が担当している。

国立大学法人では研究インテグリティの確保のための取組が進行中であり、私立大学もその追随を図っている段階と認識している。本学では、現在のところ既存の規程で対応可能であると考えているが、他大学の動向を注視し、その動きを踏まえ対応を考えている。海外との共同研究件数は多くないが、懸念がある話を近年よく聞くようになってきた。オープンサイエンスについては、G7 声明などに基づいて国として推進していく方向であり、大学としてもそのリスクを含めて検討している。大学全体として、オープンサイエンスや国際化についての議論を進めていく方針である。

b. 組織体制・運営方法と、関連する課題

上記の三つの規程に基づき運用されている。委員会の委員長は、利益相反委員会および安

全保障輸出管理委員会については研究担当の副学長が務め、研究倫理委員会においては学長が委員長を務める。委員会のメンバーは基本的に教員が中心で、利益相反委員会には研究担当の副学長をトップに、研究部長・副部長（教員ポスト）、利益相反アドバイザー兼研究部の事務部長、人事部長が参加している。

利益相反委員会は案件ごとに開催され、不定期ではあるが、実績としては月に 1 回程度のペースで開催されている。研究倫理委員会は年 2 回定期的に開催されるが、問題が発生した場合は随時開催される。安全保障輸出管理委員会については、年 1 回が基本だが、問題が発生した場合は随時開催される。

利益相反委員会には事務職員 2 名が、安全保障輸出管理には 1 名の職員が担当している。委員会には直接関与していないが、三つの委員会に関連する課題に多くの職員が関わっており、委員会のみを担当する職員はおらず、多くの職員が複数の業務の一部として取り組んでいる。輸出管理アドバイザーは非常勤の教員ポストを担っており、週に 2 回大学に出勤し、それ以外の時間はメールで相談に応じている。利益相反アドバイザーは常勤の産学官連携戦略本部の副本部長兼事務部長が務めている。

担当の大学職員は定期的に入れ替わり、その度に業務について学習する必要がある。ただし、職員は入れ替わるものの、アドバイザーは同じ方が続いており、それに頼りにしている。また、国立大学に比べると職員の入れ替わりは少なく、部署異動は 5 年から 8 年程度に 1 回であるため、一定期間は一つのポストに留まることが多い。また、対応した事例についてはリストで残し、引き継ぎの際にどのような対応をしたかの蓄積が行われている。

研究インテグリティに関連する業務を列挙すると以下のとおりである。

- 安全保障輸出管理に関しては、学長を最高責任者とする委員会が設置され、海外の大学機関等との共同研究における安全保障リスク管理が実施されている。この管理の範囲には、貨物の輸出、技術の輸出、人材の受け入れ等が含まれている。技術流出や情報流出につながるリスクは、安全保障輸出管理の観点から対応されており、共同研究や産学連携活動は契約締結段階で対応される。国際共同研究に関しては、出張ベースでの活動や協定書の締結などが行われており、これらは必ず事務部門を通じて行われるため、安全保障管理の確認が可能である。
- 利益相反及び責務相反の懸念が生じた場合には、規程に基づき、委員会および利益相反アドバイザーが対応している。利益相反委員会は、兼業申請関連での審議も行われる。窓口は所属の学部等であり、学部等で承認された内容を元に人事課が確認し、その後利益相反委員会として研究部が受け取る形となっている。兼業先の大学が安全保障輸出管理上問題があるかどうかも、利益相反委員会でチェックされ、懸念がある場合は研究環境担当課に連絡し、輸出管理アドバイザーに相談する。
- 留学生受け入れに際しては、研究部ではなく学部や国際部が書類チェックを行っている。教員採用に関しては、採用決定後に経歴の確認や必要な書類の聴取を行い、チェックしている。

- 教員採用に関しては、採用時の兼業情報は学部事務室、リサーチオフィスでチェックしている。採用後には、本務教員の兼業規程に基づき、兼業する際にチェックが行われる。
- 研究活動における不正行為については、研究倫理委員会が管理している。通報窓口は公開され、情報収集が行われている。
- 監査担当の部署として、業務監査室が設置されており、学内の業務や研究執行に関して監査を行っている。安全保障輸出管理に関しては、4 年前に業務監査室の監査を受けた。

開示情報に基づくリスク判断の方法、関連する課題

具体的な問題が発生した際には、まずアドバイザーに相談し、現場で対応可能であればそこで処理する。重大な問題であれば、随時上位の部門へ報告し、研究部事務部長、研究部長、研究担当副学長へと報告を上げる。さらに重大な場合は学長まで相談する。最終的にはすべて学長に報告されるため、知らないところでの判断は行われない。研究担当副学長まで相談するケースは年に 2 回から 3 回程度ある。海外のデュアルユース研究の研究費に関する議題などで研究担当副学長が議論に参加し、結論を出したケースが記憶にある。学長に相談するケースは記憶にない。

人事部における判断と研究部における判断は存在するが、全体で総合的に判断する必要が生じた際、あるいは何らかの懸念が発生した際には、研究環境担当課に相談が持ち込まれ、輸出管理アドバイザーによる判断が求められる。教員から開示された情報には、職歴に関するもののみならず、「このような人材を雇用したい」とか、「海外との共同研究を計画している」といった相談もある。このような人材の雇用や共同研究に関して、安全保障輸出管理上の懸念がある場合には研究部の研究環境担当課への相談が行われる体制となっている。

課題としては、対応すべき事項のボリュームは多くはないが、場当たり的に対応しているような状況もあることが指摘されている。

リスクが懸念される場合の対応プロセス

主に、安全保障輸出管理および利益相反に関わる問題があるため、これらは研究部で対応が行われている。多様なリスクが存在するが、関連する教員、所属学部長との相談を経て、研究部で対応する。

既存の組織体制との関係

各受付事務部門は安全保障輸出管理のチェック項目を認識した上で確認を行い、課題が生じた場合には研究環境担当課で一元的に把握されるようになっている。ただし、兼業に関する全てのデータを研究環境担当課が確認する訳ではなく、各受付部署は自身が受け付け

た教員の情報のみを把握することが適切であるとされている。

情報の一元化に関しては、現在、一元的なデータベースへのアクセスが可能な体制にはなっていない。情報が一元化されることによるアクセス制限の問題も考慮されている。兼業の観点からは、教員職員の個人情報保護が重要であり、基本的には人事部門で情報が管理されている。

三つの委員会の相互連携については、研究部の職員が担当している。

c. 運営トップレベルの関与（取組、意思決定プロセス）

先に述べた研究倫理委員会が、学長の指示の下、研究インテグリティの確保を目的として他大学の状況などの調査を行い、今後の研究インテグリティ委員会の設立や規程の制定などを検討している。意思決定プロセスに関しては、研究倫理委員会に諮られる案件については、学長の判断によって決定がなされる。規程の策定や委員会の仕組みについては、当面は現行のやり方で対応することとしているが、この判断は学長レベルで行われ、研究倫理委員会で議論された結果である。

また、各委員会は学長の下に設置されており、安全保障輸出管理体制においては、最高責任者として学長が設定されている。これは規程にも定められている。実務を担う委員会については、委員長として研究担当の副学長が配置されており、この体制で対応している。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

研究インテグリティよりも安全保障に特化した説明会を、年 1 回開催している。対象は自然科学系の学部と、人文社会系の実験系学部である。教授会で 30 分の時間を確保し、直近の事件などを例に挙げて注意喚起を行っている。内容としては、基本的な知識に加え、具体的な事例に基づいた説明を行っている。使用している教材は、輸出管理アドバイザーがその都度作成しており、経済産業省や文部科学省の資料を参照しているが、特定の教材は作成していない。学生向けの研修は行っていない。ただし、研究倫理に関しては各学部で取組を行っている。

事務局向けの説明会も年 1 回開催しており、対象は留学生受入れ部門の国際部や研究支援部門と、各学部の事務室の職員である。内容は 1 時間にわたり詳細なものとなっている。

研究インテグリティについては、それ単独で研修を実施しておらず、安全保障輸出管理などの話の中に一部含まれている程度である。

教職員の間で研究インテグリティについての意識は高まっているものの、情報漏洩の懸念や意識の浸透度には不安がある。海外での発表時に技術輸出の意識がないなどの課題が存在している。研究インテグリティという概念自体がまだ十分に理解されておらず、質問もあまり寄せられていない。教員だけでなく職員も、研究インテグリティを完全に理解するのは難しいと感じている。概念の明確化が必要とは思うが、その難しさも認識している。

e. 他大学・研究機関との連携、関連する課題

安全保障輸出管理に関連し、本学の周辺地区において大学輸出管理担当者ネットワークが設けられている。このネットワークでは、国公立および私立大学の関係者が集まり、研究インテグリティに関する議論も頻繁に行われている。意見交換や情報交換を通じて、様々な課題に対する対応策を随時検討し、進めている状況である。

f. 政府・資金配分機関への要望・提案

政府や資金配分機関に対する具体的な要望や提案は特にないが、研究インテグリティに関する理解の難しさについては、学内でいくつかの声が挙がっている。特に、文部科学省や内閣府など、研究インテグリティに関わる部署が多岐にわたり、異なる部署から様々な通知が来るため、大学側がどの部署に対応すべきか困惑する場合がある。研究インテグリティに関する事項を一本化し、一つの部局で担当してもらえるとわかりやすくなると思う職員もいる。

内閣府や文部科学省が東北大学の事例をモデルとして示したり、大学向けのチェックリストを作成したりする取組は非常に参考になると感じている。

(6) F 大学

F 大学は私立総合大学である。

a. 規程整備の内容・運用方法とその課題

研究インテグリティの確保を目的とし、規程の整備が本学において行われている。具体的には、利益相反管理規程および安全保障管理輸出管理に関する規程が制定されている。利益相反管理に関しては、規程により各学部において運用されており、重大な事案が発生した場合には、全学的な委員会を開催することとなる。しかし、現状では重大な事案はなく、全学的な委員会は開催せずに各学部において利益相反管理の運用が行われている状態である。

また、安全保障輸出管理に関しては、全学的な取組として位置付けられており、本部の研究支援担当部署が所管している。懸念事項が発生した場合、ワークフローによる申請が行われ、各学部において確認・承認された後、研究支援担当部署および輸出管理アドバイザーによる最終確認と規程に基づく承認が行われている。

課題に関しては、利益相反管理については既に長期にわたり規程が設けられ、各学部において取り組まれているが、それら取組についての課題の全学的管理に至っていない状態であることである。他方、安全保障リスク管理については、全学的に一元化が図られており、最近制定された安全保障輸出管理に関する規程により、全学的な運用が実現している。研究インテグリティに関しては、大学横断的な取組が必要であると考えられており、既存の研究推進委員会や安全保障関連輸出管理委員会との連携を図りながら、今後の対策を検討する必要があると考えている。

このように、利益相反管理および安全保障輸出管理に関する規程については、それぞれ設けられているところであるが、研究インテグリティに関する規程の作成については、他大学の事例を参考にしながら、次年度以降の検討が進められる予定である。

政府による研究インテグリティに関する動向については、詳細な把握まで至っていないものの、大まかな内容については理解している状況である。研究インテグリティの範囲については広範と感じており、ある程度の区切りがあるのか、あるいはもっと幅広く考慮していく必要があるのかについて、理解が曖昧な状況である。研究インテグリティに関しては、主に安全保障輸出管理に関連するところからのつながりがあるというイメージを持っているが、その理解が正しいかどうかなどが議論になるところである。

b. 組織体制と運用方法と、関連する課題

利益相反および安全保障輸出のリスク管理については、それぞれ専門の委員会が設けられている。全学的な協議が必要な場合には、各学部の委員会だけでなく、全学的な委員会に上げて検討する体制が整っている。日常的な取組は、各学部ごとの利益相反委員会にて対応しており、必要に応じて全学的な委員会を開催する体制が取られている。安全保障輸出管理

についても同様で、必要に応じて全学的な委員会において協議を行う体制が設けられている。利益相反に関する事項で全学的な議論が必要な場合、研究推進委員会において議論される。安全保障輸出管理に関しては、安全保障輸出管理委員会が存在する。

研究不正対応や研究公正の担当部署としては、受付窓口と研究支援担当部署が対応しており、告発があった場合には受付窓口が対応し、必要に応じて学部での検討（予備調査・予備調査委員会）を経て、全学的な委員会（研究公正委員会）の開催が行われる。

研究インテグリティについては、研究推進委員会が、研究推進、研究環境の整備、および研究倫理、研究不正を含む研究公正の管理を担当しており、研究インテグリティに関連する事項を扱う役割もこの委員会にあると想定している。研究推進委員会の委員長は副学長が担当しており、研究推進委員会には、副学長、各学部長、各学部の事務部長、および財務部など関連する法人部局の事務部長が参加している。副学長は 7 人いるが、全員が同委員会に参加している。ただし、現状では、研究インテグリティそのものに関する明確な定めはなく、経営層のマネジメントの関与や、部局横断的な取組を考慮し、適切な体制について現在検討が進められている段階である。

研究インテグリティを担当する大学事務組織としては、調査やヒアリングの依頼があった場合には、研究支援担当部署にて対応している。

組織体制の課題に関しては、研究インテグリティについては部局横断的な取組が必要とされており、コントロールの実施が研究支援担当部署のみでは難しい部分があると認識している。このため、経営層のマネジメントを含めた体制の運営についても検討が必要と考えているところである。

開示情報に基づくリスク判断の方法、関連する課題

教員からの開示情報に関しては、研究支援担当部署が共同研究に関する事項を扱っている一方で、学外兼職に関する事項は別の部署が担当している。現時点において研究者からの情報開示やそれに基づくリスク判断に関しては、研究支援担当部署では特に行っていない。

教員採用に関しては、各学部と人事部が担当している。採用プロセスにおいては、研究者の過去の経歴やリスクに関する判断は、学部レベルで行われている。学部での判断の後、人事部による別の視点からの判断が加わる場合もある。それらの判断には、研究支援担当部署は直接関与していない。

現段階では、これらの情報は常に部門間で共有されているわけではない。ただし、研究支援担当部署と学外兼職を担当する部署との間で必要に応じて連携が行われている。このような状況を踏まえ、リスク判断をどうするのかについては今後さらに検討を進める必要があると考えている。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合、基本的な対応としては委員会を開催し、その場で審議を行った

上で必要な手続きを講じることとされている。具体的な事例がまだ発生していないのが現状であるが、現段階では委員会を通じた適切な手続きを学内で行うことを想定している。

研究推進委員会に関しては、委員会自体は年に 1 回開催されるが、それに付随する小さな部会や運営委員会は数ヶ月に一度の頻度で開催されている。これにより、継続的な審議と意思決定の場が提供されている。

既存の組織体制との関係

現時点で研究インテグリティに関する専門の取りまとめ部署は設置されていないので、問題が発生した場合には研究支援担当部署が部署間の調整を行うことになる。

体制整備に関しては、緊急性がまだ高くないと認識されているものの、様々な指摘を受けており、他大学の状況を参考にしながら体制の整備について検討を進める必要があると考えている。

c. 運営トップレベルの関与（取組、意思決定プロセス）

大学の運営トップレベルが、研究インテグリティ確保に向けた検討体制および運営体制へどのように関与するかについては、現時点では具体的な方針が定まっていない。このため、今後も学内関連部署での引き続きの検討が必要であると考えられている。

研究推進委員会に副学長の 7 名が参加しており、過去、同委員会において研究インテグリティに関する議論が行われた事例はない。ただし、研究インテグリティは、順次取り組んでいく必要があると認識している。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

研究インテグリティについての研修・教育については、これから学内で関連部署とも相談しながら実施を検討していく段階である。

なお、研究倫理教育の研修は、受付窓口にて 2014 年から APRIN e ラーニングプログラム（当時は CITI Japan）のカリキュラムを実施しており、1 年に 1 課題ずつ全教員および研究費に関係する事務職員全てに対し受講を促す啓発活動を継続的に行っている。利益相反や安全保障リスク管理に関連する講習も、これに含まれる形で行われる。年に 1 回は、全学を対象にオンラインで実施され、毎年受講を啓発している。

APRIN e ラーニングプログラムには研究インテグリティのモジュールが加わっているが、研究インテグリティの課題を受けることを要求したことはこれまでなく、今後において実施する可能性がある段階である。

また、年 2 回、受付窓口及び研究支援担当部署にて、研究倫理に関する講演会をオンデマンド形式で実施している。

e.　他大学・研究機関との連携、関連する課題

研究インテグリティのみを取り扱うものではないが、周辺地区の私立大学の間で、知的財産の勉強会を開催している。この会には 11 大学が参加しており、産学連携に関する事例の紹介や困りごと、進め方について、年に 1 回から 2 回、会合を開催し、参加者同士で質問を交わしながら情報共有し、参考にしている。各校とも、多岐にわたる共同取組が行われており、事例を参照しながら、必ずしも一致した足並みで進むわけではないが、先行事例を基に取組を進めることが多い。本学も多数の研修会にも参加し、今後の取組方針を検討していく所存である。

f.　政府・資金配分機関への要望・提案

最近では、内閣府、文部科学省、大学協会などにより、研究インテグリティに関するセミナーや説明会が開催されている。参加する必要性は感じているが、大学行事などが重なり最近は参加できていない状況である。今後は研修会などに積極的に参加しようと考えている。研修会では具体的に、研究インテグリティの組織を構築する過程で生じた課題やうまくいかなかった事例について、それらを乗り越える方法があれば教えていただければ、参考になると考えている。

(7) G 大学

G 大学は私立の工業大学である。

a. 規程整備の内容・運用方法とその課題

利益相反規程を制定しており、目的、利益相反の定義、利益相反の対象者の範囲、及び利益相反の対象となる事項について定めている。具体的な規程の運用においては、大学では共同研究や受託研究を行う際、その研究が 200 万円以上の場合等に、研究者本人が自己申告することで、利益相反の関係の有無を確認する措置を講じている。また、物品の無償提供を受ける場合には、無償提供相手先から提供される物品について、利益相反の関係がないかどうかの確認を行っている。また、責務相反についても定義を明確にしている。また、不正行為の防止等に関する規程も設けられている。研究者倫理に関する規程は、インテグリティに関する議論が始まる前から存在しており、大きな変更は行われていない。安全保障に関する規程や委員会体制は、2020 年から導入された比較的新しいものである。

政府からの研究インテグリティについての通知等は、2022 年頃から始まったと認識しているが、それに応じた規程の修正や内容の改正はこれまでのところ特に行っていない。研究インテグリティの確保のために今後必要な修正や調整があるかどうかは、まだ検討の途上である。利益相反規程は 2017 年に制定されたものであり、その後組織変更を行った際に若干の修正を加えたが、条文の大きな変更は行っていない。

規程整備に関連する課題については特にないが、全般的なインテグリティに関連する問題では、法律に関する知識が関与してくることがある。現状、事務局の大多数の職員は事務職員であり、法律に関する専門的な知識が必要とされる場合、判断に迷う事例が時折生じているというのが、課題と言える。

なお、本学では科研費を受け取っている教員が海外出張し、海外の研究者と意見交換や打ち合わせをすることはあるものの、国際共同研究に関しては、事例は少なく、海外機関からの研究費の受入れは確認されていない。

b. 組織体制と運用方法と、関連する課題

研究インテグリティに関しては、主に安全保障輸出管理及び大学における利益相反や研究者倫理に関連する部分が該当すると考えられる。組織体制としては、安全保障輸出管理委員会と研究者倫理委員会が設置されている。これらの委員会の事務は、大学事務局の研究支援部署が担当している。

安全保障輸出管理体制における最高責任者は理事長が務めており、その下に統括責任者として学長がいる。輸出管理における管理責任者は、教育職員と一般職員および大学院生は副学長が務め、研究職員が行う業務に関する管理責任者は各研究所の所長としている。なお、副学長は安全保障輸出管理委員会の委員長を務め、委員会では輸出管理に関する重要事項

を審議する。

研究活動における不正行為の防止に関する体制についても同様に、最高管理責任者を理事長、統括管理責任者を学長としている。統括管理責任者を補佐し、不正防止計画の実質的な権限を持つ研究倫理教育責任者がおり、コンプライアンス担当の学長補佐が担当している。研究倫理教育責任者の役割として、研究者倫理教育の実施及び受講の管理があり、実施状況を定期的に統括管理責任者へ報告している。

教員が採用された後、他の大学で講義する、あるいは会社の顧問になる、委員を務める、コンサルタントを引き受けるなどの場合は、教員は学長へ兼職届を提出し、許可を受ける必要がある。する。その行為が教員の職務に抵触しない範囲であれば、兼職が認められる。

研究者倫理、産学連携、安全保障輸出管理のうち、貨物の輸出と技術の提供に関しては研究支援部署が事務を管轄しており、安全保障輸出管理のうち、人の受入に関しては、国際交流担当部署が事務を管轄している。

さらに、監査室は、年間を通じて研究費の使用状況を確認する活動を行い、公益通報があった場合の学内窓口を務める。また、監査法人と連携し、会計関連の不正の有無を確認する役割を担っている。

研究支援部署では、パート及び嘱託職員を含め 7 名の体制を取っており、実質的な体制は 5 名である。しかし、研究者倫理や安全保障のみを専業で担当するスタッフはおらず、これらは職員の業務の一部となっている。研究費の管理が業務の大部分を占めており、インテグリティ関連の業務は全体の 2 割から 3 割程度である。

開示情報に基づくリスク判断の方法、関連する課題

開示された情報に関して、職歴、研究経歴、所属役職等の部分については、雇用時に提出される履歴書や外部機関の公開情報（eRAD 等）により確認される。しかし、これらの情報の真実性に関しては、研究支援部署の側で積極的に検証しているわけではない。外部機関からの各種支援に関しても、教員の自己申告に基づき管理されており、追跡調査などは行っていない。

ただし、海外出張に伴う貨物の輸出や海外の研究者・機関への情報・技術の提供については、安全保障輸出管理規程に基づき事前確認を実施している。確認の結果によっては、輸出管理統括責任者や経済産業省への許可申請を行うなど、ガイドラインに沿った確認が行われる。学会発表等に関する問い合わせに対しては、教員からの情報提供とインターネットを通じた情報収集を行い、その正確性を確認している。

リスクが懸念される場合の対応プロセス

安全保障輸出管理面における運用に関しては、出張などによる技術提供や貨物輸出について、事前確認を実施している。この事前確認は、共同研究や、教員が海外の企業や機関と協力を希望する場合にも行う。事前確認について、輸出管理責任者は、内容を精査し、詳細

な調査が必要であると判断した場合、学内のガイドラインに従って、追加の書類提出を求める。最終的に輸出管理統括責任者が、経済産業省への許可申請が必要であると判断した場合には、そのための手続きを適宜進める流れとなる。

研究不正行為の告発に関しては、学内であれば監査室が担当し、学外であれば法律事務所に委託している。大学のホームページに設置された公益通報窓口を通じて、不正行為の疑いがある場合には連絡がなされるようになっている。不正行為の疑いがある場合には、予備調査委員会を設置し、調査を行い、その結果に基づいて、本格的な調査を行うべきであると最高責任者が判断した場合には、本調査委員会を設置し、本格的な調査を行う。

既存の組織体制との関係

研究インテグリティの体制整備についての政府資料を見ると、全組織的なリスクマネジメントの体制図が描かれており、安全保障、産学連携、研究不正対応といった各領域が一元管理されることが望ましいとされている。しかし、本学では、これらは委員会として独立した形で運用されている。事務組織においては、研究支援部署がこれらの事務局を合わせて担当しており、その体制が現時点の本学の現状である。

今後については、大型の研究費の申請や分野横断的な研究費への応募、さらには海外の大学との連携を加速化しようとする動きが学内に存在する。そのため、安全保障輸出管理などは今まで以上に注意を払う必要があると考えている。ただし、現時点ではリスクマネジメントに関して、大幅な組織体制の変更や規程の改正は予定されていない。もちろん、法改正などで何らかの対応が必須となる事項については、適切に対応する方針である。

c. 運営トップレベルの関与（取組、意思決定プロセス）

理事長は大学経営全般を司り、学長は教学、教育、研究に関する日々の方針を決定し、運営する責任者である。研究インテグリティに関しても、日常的な責任は学長が担っている。委員会においては、コンプライアンスを担当する学長補佐が委員長を務めている。ただし、共同研究や受託研究など、大学と外部との契約に関わる最終決裁者は、理事長である。そのため、産学連携や研究関連契約の代表者について問われた際には、理事長であると回答している。

他方、理事長が運用面や規程面に関して具体的に介入することは、実際にはほとんどないのが現状である。問題が生じた際には、委員会を設置し、報告を受け、判断を求める体制となっているため、運営体制や検討体制への常時の関与は少ないと言える。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

新任教員に対して、人事部主催の着任時オリエンテーションにおいて、研究支援担当者から研究者倫理や安全保障輸出管理に関する規程についての説明を行っている。大学に所属

する教員や研究者として守るべきルールの概要を伝えるという形を取っている。また、新任教員は「APRIN e ラーニングプログラム（eAPRIN）」を必ず受講することが求められている。

研究者倫理に関しては、4 年に 1 回、教職員に対して、該当する e ラーニングプログラムによる研修を実施している。学部生には、1 年次の教育の一環として研究者倫理の教育を受けさせ、大学院生に対しても、研究者としてのキャリアの入口に立つ彼らに対して、e ラーニング教材を用いた研修を行っている。

安全保障輸出管理に関しては、年 1 回、外部の専門家や CISTEC に講師を依頼し、基本的な講習会を開催している。特に、海外へ技術や物質を提供する際の事前確認の重要性を強調しており、その内容については、安全保障に関わる可能性がある点に留意するよう指導している。

課題としては、e ラーニングは新任教員が必ず受講する体制が整っているが、安全保障輸出管理については、特に人文系の教員から、自分の研究分野が軍事に関連しないとの見解に基づく疑問や、事前確認の必要性に対する疑問が提出されている。このような疑問に対して十分に説明を行い、これらの教員にも理解してもらう必要があることが、主にスタッフレベルでの課題である。

e.　他大学・研究機関との連携、関連する課題

研究インテグリティに関しては、個別の研修会で知り合った機関との情報交換を行う程度であり、具体的に連携を図りながら取り組む段階には至ってはいないのが現状である。

f.　政府・資金配分機関への要望・提案

大学の事務職員にも複雑な判断を求める事例が増加しているが、関係法令など専門知識を持つことが対応を容易にすると考えられる。特に、安全保障輸出管理関係の事前確認は、現在最も日常的に発生する業務であり、教員の海外出張に関連する事前確認業務が、担当者の負担となっている。簡単な質問から難しい質問まで、どこに相談すれば解決の糸口を得られるかを知ることができる相談窓口があれば、事務レベルでも大変助かると考える。このような支援は、資金的な支援よりも価値が高いだろう。そうした支援が提供されれば、本学だけでなく、他の大学にとっても大いに助かるのではないか。

3.2.2　国立研究開発法人へのヒアリング結果

(1)　国立研究開発法人 A

a.　規程整備の内容・運用方法とその課題

研究インテグリティ確保に関連する規程として、まず、「利益相反マネジメント規程」は、公益性、公平性、中立性、透明性を担保し、社会的信頼を獲得するために重要な利益相反について規定している。利益相反マネジメント委員会は、利益相反マネジメントの企画運用等を審議する場であり、毎年 3 月に役職員から自己申告書を提出させ、その内容に基づき利益相反による弊害の有無を確認し、必要に応じてヒアリングを実施する。弊害が生じている、または生じる可能性がある場合には、産学連携活動等の改善または中止といった勧告を行う。利益相反の自己申告書では、兼業情報、寄付金の受領、物品供与の受領、共同研究の実施状況などが開示される。利益相反の監査にはコンプライアンス担当課が関わる。

第 2 に、「研究活動の不正行為の防止及び対応に関する規程」については、研究活動の不正行為の防止と対応、研究活動の不正行為が起こりにくい環境の整備と強化を内容としている。役職員は、研究活動の不正行為を行わない旨の誓約書を提出し、研究活動に関わるデータや研究ノートは適切に管理されるよう、管理監督者が指導する。誓約書では、不正行為の未然防止や発見時の報告、誠実な勤務などが誓約される。不正に関する通報には、内部ではコンプライアンス担当課が担当し、外部では法律事務所が通報窓口として設置されている。研究活動の不正行為の疑いが生じた場合、予備調査委員会や研究不正調査委員会を設置して対応する。

第 3 に、「安全保障輸出管理規程」には、基本方針、輸出管理体制、該非判定の手続き、用途確認及び需要者等の確認を行う手続き、監査の実施、研修の実施などが定められており、組織として安全保障輸出管理上の確認を行っている。また、安全保障輸出管理に関する誓約書では、無断での物品の提供や持ち出し、兵器転用の防止、手続きの遵守などが誓約される。

最後に、研究インテグリティの確保に関する規程は、2024 年 1 月に制定し、施行する。その内容は、研究インテグリティの定義、役職員の責務、研究者の責務、問題発生時の会議体設置、相談窓口の設置などが含まれる。現段階では、研究インテグリティに関する業務は総務担当課が中心となって運用しているが、組織規程においても、研究インテグリティに関する業務を総務担当課に追加し、窓口として明示することで、組織的に対応する位置づけとなっている。安全保障輸出管理は国際担当課、利益相反はコンプライアンス担当課が担当するが、研究インテグリティ全般にわたる窓口として総務担当課が機能する。

新規程における研究インテグリティの定義は、研究活動の国際化やオープン化に伴う新たなリスクに対応するといった意味合いを持つ。規程策定時の主な議論としては、研究インテグリティの定義の明確化と、研究所内での規程の浸透が挙げられる。策定時のハードルとしては、研究インテグリティの定義に関する様々な見解やニュアンスの違いが存在する点が挙げられる。

規程整備に関する課題としては、「利益相反マネジメント規程」に関しては、研究インテグリティに関する社会的な議論の高まりに伴い、自己申告書の提出頻度や内容が十分であるか検証することが難しい点が考えられる。また、「研究活動の不正行為の防止及び対応に関する規程」においては、研究ノートの保存期間（現状は 10 年間）と通報のタイミングの兼ね合いが課題として考えられる。

b. 組織体制と運用方法と、関連する課題

安全保障輸出管理は国際担当課が、研究インテグリティは総務担当課が、利益相反と研究不正対応はコンプライアンス担当課が担当している。国際担当課は、安全保障輸出管理と国際協力関係に関する業務に分かれており、総務担当課は現在、研究インテグリティに対応する職員が 1 人いる。プロパーの職員は通常、3 年程度の期間で異動し、外部専門家も安全保障輸出管理に関する知見の底上げのために任期を限定して雇用されている。これにより、組織に蓄積された知見が継承される体制が構築されている。

また、2024 年 4 月にはインテグリティ担当課を新設し、コンプライアンス担当課や国際担当課などの業務をインテグリティの観点から引き継ぐことになる。国際担当課の安全保障輸出管理グループなどが移行することになる。コンプライアンス担当課の業務は一部吸収されるが、内部監査の機能は引き続きコンプライアンス担当課に残る。この組織再編により情報共有が進むことが期待されている。

現在のところ、研究インテグリティに関する専門の委員会の設置は想定されていないが、必要に応じてマネジメント会議が開催される。

今後の組織再編では、研究インテグリティの確保に資するためにどのような人員を配置するかが検討されることになり、関連する部署の人員も例えば併任の形で関与することが考えられている。人事や情報セキュリティの観点からの対応が要検討である。

また、機関全体として総合リスクマネジメントを行う枠組みとして、各部署の関連するリスクを審議し検討するリスク管理会議が設置されている。この会議は年に 1 回開催され、各部署からのリスク事例の報告を受け、既存の対策に加えて追加すべき防止策を検討する。これにより、組織として PDCA サイクルを用いた総合的なリスクの管理を図っている。リスク管理会議は、年 1 回、理事長をヘッドとして開催されることが規定されている。

リスク管理会議自体では研究インテグリティについて直接審議するわけではないが、各部署の取組が研究インテグリティの確保や向上に資することから、実質的に研究インテグリティを支える会議体となっていると考えられる。総合リスク管理会議の事務は総務担当課が担当し、メンバーは理事長、理事、部門長、所長、本部の部長などが含まれる。関連する規程として、「総合リスクマネジメント規程」があり、様々な規模のリスクを幅広く想定し、対応方法についてマトリックス図を用いた議論が行われる。「総合リスクマネジメント規程」では、会議体としての「リスク管理会議規程」が定められており、理事長や指名された理事、本部の部長、研究所の所長などが参加している。

課題として考えられることは、各部署間の情報共有と連携強化が挙げられる。研究インテ

グリティの総括的な部署として機能していた課については、2024 年 1 月の組織規程の改正により、その役割が明確になり、今後の取組の強化が予定されている。具体的には、2024 年 4 月に組織再編が予定されており、インテグリティ担当課の設置が計画されている。この新組織には、これまで行ってきた横断的な取組と、新たに強化される研究インテグリティ関連の業務が集約され、研究インテグリティの確保に向けた取組が行われる予定である。

開示情報に基づくリスク判断の方法、関連する課題

リスク判断は、人事、研究費、利益相反、総務、国際、監査コンプライアンスなど、各部門でも行われているが、リスク判断に迷う場合には本部で検討される。組織内での情報はスムーズに流れており、問題が生じた場合には迅速に連絡が行われる体制が整っている。担当理事に速やかに報告し、その後の処理や防止策は組織内で水平展開できるように、会議で決定された事項は全職員が閲覧可能なイントラを通じて共有される。また、外部の専門家との意見交換やリスク管理会議への参加も行われており、安全保障輸出管理に関しては CISTEC 講師による講習会が行われ、リスク管理会議には外部の専門家が委員として参画している。

課題としては、履歴書等に記載された経歴に関する証明書の提出要求や、自己申告書の内容の真実性についての検証が挙げられる。特に海外の情報に関しては言語の問題や情報量の差異により、オープンソースでの確認には限界があると考えられる。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合の対応プロセスについては、先ほど述べた各種規程に従う。研究不正の懸念が生じた場合、研究不正防止規程に基づいて研究不正調査委員会を設置し、不正の事実関係を調査する。不正が認定された場合には、論文の取り下げやその他必要な対応を行う。利益相反が生じた（る）場合には、先ほど述べた利益相反マネジメント規程に基づき、利益相反マネジメント委員会を通じて審議が行われる。研究不正調査委員会で調査実施中は、当該者に対して研究費の一時的な支出停止等の措置を取る。また、利益相反に懸念が生じた場合には、当該者に産学連携活動の是正、改善等の勧告に関する報告を求めることになる。

いずれにせよ、これらの場合は、委員会内でしっかりと審議を行うことになる。

既存の組織体制との関係

2024 年 1 月以降は組織規程に総務担当課が研究インテグリティの総括的な部署であることを明示する。また、2024 年 4 月には新たな組織として、現在個別の各部署が対応している研究インテグリティ関連の業務を総合的に、組織的に対応する部署設置を計画している。

研究インテグリティに関する新たなリスクに対処するため、各研究現場と、研究者本人か

らの情報は総務担当課で集約され、窓口となる。現在総務担当課の担当は 1 人で業務を行っており、2024 年 1 月に研究インテグリティ規程が施行されると、業務の進め方を再検討する必要があると考えている。相談件数などが不明瞭なため、人員が限られている中で、体制を再構築する必要がある。

c. 運営トップレベルの関与（取組、意思決定プロセス）

利益相反マネジメントについては、総務担当理事が委員長を務める利益相反マネジメント委員会が設置されており、外部有識者も含めて審議する体制が取られている。また、研究インテグリティに関する担当は総務担当理事としており、2024 年 1 月の規程制定後、4 月の組織再編を通じて体制強化を図る。

さらに、理事長を最高責任者とするリスク管理会議が存在し、総務担当理事等が総括責任者として理事長を補佐する体制が取られている。

経営層や関係部署には適宜情報を伝達し、定期的に開催される会議で審議を行っている。情報共有はイントラを通じても行われ、各部署の長が参加する会議を通じても行われている。

これらの体制において PDCA サイクルを回しており、研究不正に関する体制として、年に 1 回研究倫理教育の方針の策定を行い、研究不正が発生した際の対応責任者として総務担当理事が中心となって対応している。研究不正が発生した場合は、外部専門機関に委託解析を行うことも検討されている。また、コンプライアンス担当課が内部監査を行い、その結果を理事会議に報告し、PDCA サイクルに活用している。研究ノートに関しては、産学連携担当課において年に 1 回チェックを行う体制が取られている。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

本機関では、研究インテグリティを含めたコンプライアンスと倫理教育に対して、体系的なアプローチを採用している。安全保障輸出管理やコンプライアンスに関する e ラーニング研修を年に一回行い、研究倫理教育や初任者研修、管理職昇任者講座においても年 1 回実施している。さらに、利益相反マネジメント講演会をビデオ配信で年 1 回開催し、利益相反に関する理解を促進している。機関内のイントラには関連資料を常時掲載し、専門家によるオンライン研修も実施して理解の推進を図っている。

全役職員への研修は毎年行われており、特別な事情がない限り、期日内に受講することとされている。

研究インテグリティに関する専門のセミナーや教育はこれまで実施されていないが、新たな研究インテグリティ規程の作成に伴い、職員向けに研究インテグリティについて説明する必要があると考えられており、その実施について検討中である。

課題としては、研究インテグリティに関する基準や定義について、全役職員の知識レベルを統一するのが困難であること、外部委託するにしても第三者機関や教育機関の選定基準

や必要要件が明確でないことなどが挙げられる。また、研究者によっては、研究インテグリティの取組が研究活動の足かせと認識され、研究活動に支障を与える可能性があるとの懸念もある。研究インテグリティの確保の度合いと研究活動への支障のバランスについての難しさもあると考えられる。

e. 他大学・研究機関との連携、関連する課題

政府と連携し、国研全体で研究インテグリティの確保と徹底を目指している。この一環として、国立研究開発法人協議会（国研協）内に研究インテグリティタスクフォースが設置されている。このタスクフォースでは、研究インテグリティに関する取組の共有や法人関係の共通課題の検討、政府への要望提出などが行われており、これまで 3 回の会合が開催された。

また、他の法人と連携し、情報共有を深めている。各法人の進捗状況や先行する法人の取組を参考にしながら、研究インテグリティの確保に関する規程の制定を行った。

課題としては、法人によって予算や人員の規模が異なるため、他法人の良好な実践事例をそのまま取り入れることが難しい場合がある。法人の体力、すなわち経済的、人的リソースが課題と考えられる。

f. 政府・資金配分機関への要望・提案

研究インテグリティと研究セキュリティは一体不可分な概念であり、補完し合うものであるとの認識である。研究セキュリティには、情報セキュリティが非常に重要な対策となり、ネットワークの監視装置や情報セキュリティシステムの整備が必要であると考えている。これらのシステム整備には、導入初期費用だけでなく、毎年多額の予算が必要になり、対応するための人員も必要であるため、研究インテグリティの確保に資する取組に対して、安定的な予算の確保が不可欠であると考えている。特に規模の小さい法人にとっては、この問題はさらに切実であると感じている。

研究インテグリティや情報セキュリティの確保には様々な取組があるが、政府に対しては、取組事例を複数提示していただき、法人が対応可能な内容を選択できるように、情報提供を続けていただくことを望んでいる。法人としても努力を続ける必要があるが、政府と協力して取り組むことができれば、さらにありがたい。

資金配分機関に対しては、研究インテグリティが確保されていない法人には資金配分をためらうことになるため、具体的にどのような取組を行っていれば資金配分の申請ができるかを明示していただくこと、資金配分機関と政府が連携し、具体的な要件を定めることが、国全体の研究セキュリティや研究インテグリティの確保と強化に繋がると考えられる。

(2) 国立研究開発法人B

a. 規程整備の内容・運用方法とその課題

研究インテグリティの確保を目的とし、研究インテグリティに関する規程が制定され、2023 年に施行された。本規程では、研究者等は、研究機関に対して必要な情報の開示を行うよう定めた。内閣府及び政府からの要請に応じて作成されたものである。本規程の策定に合わせて、文部科学省の方針や大学での既存規程を参考にしつつ、研究インテグリティの強化に向けた体制の検討が行われた。利益相反や兼業等に関しても開示を求める規程等が定められているが、新たに定められた本規程では、包括的に改めて必要な情報の開示を行うよう明確にすることで、研究インテグリティの確保に資するような取組を行うことを目指している。

その他には、利益相反及び責務相反に関しては、理事会決定に基づき、利益相反委員会の設置規程および利益相反問題に関する方針が制定されている。これらに基づき、研究者等に対する必要な情報開示の要求及びリスク評価リスク対応が行われている。

b. 組織体制と運用方法と、関連する課題

組織体制については、上記規定の施行と同時に、研究インテグリティを統括する本部（以下「本部」）が設置され、相談窓口を設ける形で機能している。本部は、関連部署と共に情報共有及びリスク評価を行い、必要に応じて提携している法律事務所等の助言も得て、懸念がある場合への対応が可能な体制を構築している。

これまで本部事務部門で実施していた安全保障輸出管理及び利益相反関連業務の人員が本部に移管されている。また、関係部署の職員は兼務という形で、本部に参加している。本部では、安全保障輸出管理に関する情報や、インテグリティの観点で必要な確認事項について、関係部署に照会をかけ、開示を求める形で対応を行っている。

本部は、研究の国際化及びオープン化に伴う新たなリスクに対応することを基本理念としており、安全保障輸出管理業務、利益相反業務を中核に、様々な情報を繋ぎながら対応している。

2023 年に新たな組織が設立されてから業務は非常に忙しく、特に力を入れているのは実際に研究を実施している研究現場に対する説明である。限られたリソースであがってくる相談に迅速かつ効果的に業務を進める必要がある。研究現場との信頼関係を築くことで情報開示などのコミュケーションが円滑に行われると考えており、手続きの複雑さが研究者の負担にならないように注意しながら、必要な情報を適切に判断し、その合理性について説明責任が果たせる枠組みを構築することが重要である。

新たな組織立ち上げの課題としては、情報共有の仕方と人材育成が挙げられる。特に、適正な人材の確保と育成に時間をかける必要があると認識されている。

開示情報に基づくリスク判断の方法、関連する課題
リスクが懸念される場合の対応プロセス
既存の組織体制との関係

従来より研究者に情報開示を含む各種申請手続きを求め、申請は関係部署において処理される。例えば、採用時には審査票を用いて安全保障輸出管理の点からのチェックを行い、より懸念される場合やより慎重な対応が求められる場合は相談を受けながら業務を実施する体制を構築している。

それらの業務の中で研究インテグリティに関わる関連情報を必要に応じて取得・管理する流れとなっている。各部署での手続きを進めるフローの中で、必要な範囲で連携を図り、関連部署とともにリスク評価を行い、懸念がある場合は連携して対処する体制を構築している。また、外部機関のリスクレベルが変化した場合には、安全保障輸出管理審査を再度実施するなど、必要に応じてリスク評価をし直している。

IT、通商関係、サイバーセキュリティ、知的財産について、各国法制に関して高い専門性と実務経験を有する弁護士で構成される外部専門機関である法律事務所と、研究インテグリティの確保に関するマネジメントの強化と法令遵守を含む法律事務の処理の委任契約を締結し、必要に応じて専門的な立場から助言を受ける体制としている。

研究インテグリティについての新しい本部を設立することにより、これまでにはなかったリスク判断が可能となり、研究インテグリティに関する判断については、外為法のリスト規制だけでなく、様々な検討を行い、リスクを承知した上で進めるプロセスをとっている。

研究活動は卓越した研究者らの国際的な頭脳循環により水準が上がるものであるが、緊張感とリスクの高まりも認識し、研究者が予期せぬトラブルに巻き込まれないようにするのが機関のマネジメントの責任である。しかし、研究活動が無用に萎縮することがないよう、バランスを取りながら進めることが必要であると考えている。

本機関におけるインテグリティの判断にあたり必要に応じて、提携している法律事務所に相談することや経産省に外為法の整理を再照会するなどを実施しており、判断に時間がかかることもある。

c. 運営トップレベルの関与（取組、意思決定プロセス）

研究インテグリティの確保に関わるマネジメントについて、その業務を統括するため総括責任者を設置している。緊張感を持って適切にリスクマネジメントを行うとともに、研究活動が萎縮しないようにバランスをとりながら進めていくことが大きな方針である。

本部の本機関内での周知に関しては、研究現場との共有が重要である。これまでに研修会の開催や、幹部会議での方向性の共有、研究リーダーが集まるリーダー会議での本部の活動やチェックリストの使用などの説明が行われてきた。

人材の獲得についても課題として残っている。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

研修を介して、研究インテグリティとして安全保障輸出管理や利益相反に関する研修が提供されている。加えて、外部有識者による講演を交えた研究機関内向けの全体説明会や、各研究センターの研究リーダーが集まるリーダー会議において、周知及び理解の増進のための説明会が実施されている。研究インテグリティ等の研修の際の、研究現場からの反応については、受け止めに対して、温度差が存在していると感じられている。教育・研修に当たっては、多国籍の研究者が数多く在籍していることから、誤解のないよう丁寧かつ慎重な説明が必要であると認識されている。

研修の教材に関しては、現在、本機関で作成した安全保障輸出管理や利益相反に関する教材が使用されており、定期的な更新が行われている。新規採用者には、これらの研修を受講することが義務付けられている。

研究インテグリティ専用の教材の開発及び特化した研修の実施については、今後検討される予定である。現状では、安全保障輸出管理や利益相反に焦点を当てた研修が主に行われ、最近の動向に基づいて研究インテグリティに関する説明会が開催されている。研修が多過ぎると研究者に負担を与える可能性があるため、最適な研修計画の策定は今後の検討課題である。

e. 他大学・研究機関との連携、関連する課題

他機関との連携に関して現状は、国立研究開発法人協議会（国研協）にて連絡や情報共有の仕組みが設けられている。国研協では、研究インテグリティのタスクフォースが設けられ、各法人間で取組の状況や情報が共有されている。多くの法人が課題に直面しているが、有益な情報の共有が行われていると認識されている。

加えて、必要に応じたヒアリングや意見交換を各法人に対して 2023 年夏頃に実施し、取組を進めてきた。今後も、他の大学や研究機関との連携を進め、グッドプラクティスの共有を促進する考えである。他法人へのヒアリングや、有用な情報を HP で発信されている大学等の取組を参考にしている。

連携に関連する課題としては、国研協のタスクフォースを通じた情報共有が行われており、研究インテグリティについてのどの程度、何を行うべきかというラインについて法人間での共通認識の明確化が求められており、これが明確になればさらに進展が期待されると考えられている。

f. 政府・資金配分機関への要望・提案

現在、本機関において実施されている研究は、成果の公開を基本としており、研究者はその認識のもと研究活動を進めている。適切な管理の下、公開を原則とする研究を推進することが重要であると認識されている。ただし、同時に、厳しい安全保障環境の認識を共有し、

リスクへの意識を様々な階層で高める必要があると認識されている。情報漏洩のリスクに対して厳格に対応することが求められており、これらを踏まえた対応が必要とされている。

国際競争力を持つ研究活動においては、日本国内のみならず、世界中から卓越した研究者が集まり、繋がることが重要である。次世代の研究者や技術者の育成と発展を促進することが重要であり、研究活動が不必要に萎縮するような規制は避けるべきであるとの認識がある。

このような基本的な認識を踏まえ、政府への要望としては、研究インテグリティや研究セキュリティに関する議論が進んでいるが、実務上、実効性のあるガイドラインやリソース配分など、ある一定の枠組みが整備されることが望ましいと考えている。

(3) 国立研究開発法人C

a. 規程整備の内容・運用方法とその課題

研究の健全性・公正性の対応に関しては、2023 年 4 月に研究インテグリティについての規程を施行した。研究インテグリティの規程の内容には、研究インテグリティの定義及び委員会の設置に関する組織体制が含まれている。研究インテグリティの定義は、研究の国際化・オープン化に伴う新たなリスクに対応し、新たに確保が求められる研究の健全性・公正性を指すとされている。

同規程に基づき、研究インテグリティに関する新たな組織体制が確立されている。具体的には、「研究インテグリティ・マネジメント委員会」が設置され、情報の集約や検討を行い、「研究インテグリティ・マネジメント専門委員会」が専門的事項の検討を担当している。

また、利益相反マネジメントについては、利益相反に関する調査審議を実施する委員会が設置され、対応する規程が整備されている。

規程整備の課題としては、利益相反マネジメントに関しては、利益相反マネジメント委員会への自己申告を義務付ける個人的な利益の基準が明文化されており、利害関係を有する組織への兼業や株式保有状況などが含まれる。しかし、研究インテグリティに関しては、対象となる事項が多岐にわたり、懸念される国に関する情勢が変化するため、利益相反マネジメントと同様の基準の整備は現時点では完全には行われていない状況であることである。

b. 組織体制と運用方法と、関連する課題

研究インテグリティの確保のためのマネジメント組織体制については、上記のように、規程に定められた「研究インテグリティ・マネジメント委員会」と「研究インテグリティ・マネジメント専門委員会」を設置している。研究インテグリティ・マネジメント委員会については、研究インテグリティ・マネジメント専門委員会より上位の組織であり、構成員としては機関の理事等の役員、各関係部署の長、部門長などが含まれている。マネジメント委員会の長は担当の理事である。研究インテグリティ・マネジメント専門委員会に関しては、専門的な内容の検討を行うための委員会であり、各担当部署レベルの室長などが参加している。専門委員会の委員長はインテグリティ・マネジメント委員会の副委員長が務めている。

これらの委員会において、必要に応じて検討を行う。現状においては、研究インテグリティの確保に関するマネジメントの対象となるケースについての前例が乏しく、個別案件ごとにリスクが懸念されるか否かの判断を行っている。その都度、対象となるケースのマネジメント方法を模索しており、直近では研究者が参加する国際的なイベントの参加について審議する機会があり、その際に対処フローを整理した。

2023 年 4 月に体制が確立してから、本年中に委員会と専門委員会はそれぞれ 1 回ずつ開催されている。特に明確な開催回数は定めておらず、必要な事項が発生した場合に適宜開催される体制を取っている。企画系部署が研究インテグリティの主担当であり、今後の組織体

制の検討も念頭に置いている。基本的に当該企画系部署において 1 名が担当者として窓口を務め、適宜他の事務局メンバーや委員会の委員長、副委員長に相談内容を共有している。

研究インテグリティの規程が制定される前は、研究インテグリティのマネジメントは本機関内で行われていなかった。2023 年 4 月 1 日以降、研究インテグリティのマネジメントという観点で検討が加わり、様々なリスクマネジメント体制と連携しながら、様々な新たなリスクに対処する体制を取っている。既存のマネジメント体制で行われている部分については、その体制と連携しながら対応し、新たに発生するリスクについては、既存の体制と議論をしながら進めていっている。

研究インテグリティに関連する部署として、他には、総務系部署が研究不正や利益相反に関連する話に関わっており、安全管理・安全保障の管理については国際関連部署が、人事については人事系部署が担当している。

今後は、前例が増えていけば、案件ごとの対処フローも明確になり、マネジメントの負担の軽減が期待されるが、しばらくの間は案件ごとにマネジメント方法を模索する状況が続くと考えられる。他法人の前例や参考になる情報があれば、それを共有していただければ幸いである。

開示情報に基づくリスク判断の方法、関連する課題

研究者が開示した情報に関するリスク判断については、現在研究者に自己点検を実施していただき、その報告を求める手続きを行っている。報告された内容に基づき、リスクのレベルに応じて研究インテグリティ・マネジメント委員会やマネジメント専門委員会にて必要な対応を検討する体制を整備している。

リスク判断のために特別なツールを使用しているわけではないが、研究者による自己点検を実施し、その内容を集約している。具体的には、兼業内容等に関する質問に対する回答を収集し、その回答と実際に提出された申請内容を比較して、その正確性を確認する体制が確立されている。

課題としては、兼業申請などの既存の申請との照合を行う作業において、その内容の確認作業に負荷が大きくなっている点が挙げられる。

リスクが懸念される場合の対応プロセス

リスクが懸念される場合の対応プロセスについては、研究者本人からの相談や、事務局が入手した情報に基づき、懸念があると判断された場合に対処される。リスクが存在すると判断された内容に関しては、直接是正を求める措置が取られ、あるいは担当部署の担当者による改善対応が実施される形になる。

既存の組織体制との関係

安全保障輸出管理、産学連携、研究不正対応等については、それぞれの担当部署が既存の組織体制に基づき対応しており、各部署では既存の審査体制を通じて業務を実施している。また、各担当部署の担当者が研究インテグリティ・マネジメント委員会や研究インテグリティ・マネジメント専門委員会のメンバーとしても参加していることにより、必要に応じて情報共有が可能な体制を現状整備している。

c. 運営トップレベルの関与（取組、意思決定プロセス）

研究インテグリティ・マネジメント委員会には本機関の役員が配属されている形態をとっており、当該委員会においては、本機関としての検討・意思決定等に必要な体制が構築されている。

研究インテグリティの重要性は役員レベルでも認識されており、担当理事及びマネジメント委員会の委員長、副委員長と共に、近時、ほぼ日常的に研究インテグリティ・マネジメントの取り組み方について討議を行っている状況である。

d. 研修・教育、セミナーの実施内容・頻度・効果、関連する課題

関係部署の担当者を対象に、研究インテグリティに関する説明会を開催したほか、外部講師を招聘して研究インテグリティに関する研修会を実施した。さらに、研究インテグリティに関連する e-learning の導入に向けた検討も進めている状況である。

課題としては、研究インテグリティに関する教育やセミナーを実施可能な専門家や専門機関が限られており、依頼先の選定に困難を伴っている点が挙げられる。

e. 他大学・研究機関との連携、関連する課題

他大学との連携に関しては、国研協において最近設立された研究インテグリティのタスクフォースにおける活動の一環として、各法人の研究インテグリティについての取組状況に関する情報共有をしている。また、2023 年 10 月に開催された内閣府主催の実務者向けの研究インテグリティについての意見交換会においても、各研究機関の実務担当者との意見交換を行った。

この件に関する課題としては、先日の意見交換会で他の法人の担当者も述べていたように、現在、多くの大学や研究機関が研究インテグリティについての対応方法を模索している段階にあり、具体的な他法人との連携を実施する体制や段階には至っていないことである。

f. 政府・資金配分機関への要望・提案

政府や資金配分機関に対する要望は、以下の点である。これらは他の法人からも国研協などで以前から提起されている内容である。

まず、第三者機関や外部専門家によるレビューに関する要望がある。これまでの調査やヒアリングでの第三者機関からのレビューに関する質問に基づき、内閣府が想定するレビュー機関や専門家についての情報提供を求めている。さらに、各法人が別々に第三者機関や外部専門家に依頼することで生じる判断の差異を回避するため、具体的な第三者機関や外部専門家のリストの提示、もしくは内閣府が第三者機関として各法人の対応を見る体制の構築を検討するよう要望している。また、各法人が同じ機関や専門家のレビューを受ける体制についても検討を求めており、具体例として内閣サイバーセキュリティセンター（NISC）が情報セキュリティに関してこのような役割を果たしている状況を引き合いに出している。

次に、e ラーニングや申請システムの構築に関する費用面の懸念と、各法人で研修資料を英語化する際に表現や説明内容が異なる可能性があることから、政府主導で共通システムや共通の研修構築を実施することを求めている。

3.3　ヒアリング結果のまとめ・分析

7 つの大学（大学 A～大学 G）と 3 つの国立研究開発法人（国立研究開発法人 A～C）へのヒアリング結果から、研究インテグリティの確保のための取組の現状や課題に関して、以下、各質問項目についてまとめる。

3.3.1　規程整備の内容及び運用方法について

ヒアリングした大学・国立研究開発法人では、利益相反管理、安全保障貿易管理に関する規程等を既に策定している。一部の大学・国立研究開発法人では、研究インテグリティについての規程についても 2022 年、2023 年に制定してきている（表 3-1)。規程は基本的には文部科学省から示されたモデル規程を参考に策定されている。これらの枠組みは、政府からの方針に対応し、研究活動、特に国際的な研究活動の拡大に応じた新たなリスクを管理するための積極的な対策として策定されることが多い。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

- 大学間の比較：国立大学（A、B、C）では既に研究インテグリティについての規程を整備している。公立大学 D、私立大学（E、F、G）では、既に制定している利益相反規程、安全保障輸出管理規程の枠組みのもとで、必要な情報共有を図るなど運用面での対応をしており、研究インテグリティに関する規程の整備については他大学の動向等を注視しつつ検討しているのが現状である。
- 研究型大学とそれ以外の大学の比較：研究大学（A と B）は、研究活動のレベルの高さ、国際的研究活動の大きさを反映して、研究インテグリティとセキュリティに対して、より包括的で詳細なアプローチをとっている。それ以外の大学では、研究インテグリティに関連する対応に配分可能な資源への制限があり、各々の研究活動等を反映した合理的な対応について、他大学等の取組の情報を集めて、模索している段階と考えられる。
- 大学と国立研究開発法人の比較：国立研究開発法人(A、B、C)では、国立大学と同様に研究インテグリティについての規程の整備が既に行われており、政府とは緊密な調整が図られており、政府の方針への応答は早いとみられる。

規程整備の上での課題としては、規程に組織整備の内容（委員会の設置)、担当する事務局の部署を文言として書き込むことが必要となるため、それに関連する調整が必要とのことであった。また、後述の組織整備とも関連するが、規程を整備した後に、いかにその体制を運用するか、既存の委員会と新設の委員会との調整をいかに図るかといった課題が当然ある。

表 3-1：研究インテグリティの確保に関連する規定の整備状況・課題

ヒアリング先	内　　容
大学 A：国立研究大学	・利益相反規程等が既に制定されていた。「研究インテグリティの確保のための規程」等を 2023 年に新設。 ・「研究インテグリティの確保のための規程」等の際に課題となったのは研究インテグリティの利益相反の担当部署をどこにするか。
大学 B：国立研究大学	・2022 年に利益相反規則（随時報告の追加、個人的利益の範囲の改正等）と安全保障輸出管理規則（学生・教職員の受入れ時に「特定類型該当性」確認の追加等）を改正。 ・研究インテグリティの確保に関する規則等を 2023 年に制定。 ・課題は教員負担をいかに低減しつつ、研究インテグリティの確保を図るか。
大学 C：中規模国立大学	・利益相反規程は既に策定されていた。2022 年に「研究インテグリティの確保に関する規程」を制定。
大学 D：公立大学	・利益相反・責務相反規程、安全保障輸出管理の規程は既に制定。研究インテグリティ単独の規程はまだ策定していない。
大学 E：私立大学	・研究倫理指針、利益相反規程、安全保障輸出規程を既に策定。 ・現在は既存の規程で対応可能と考えているが、他大学の動向を注視して、対応を考えている。
大学 F：私立大学	・利益相反規程および安全保障輸出管理に関する規程が制定されている。 ・課題は研究インテグリティに関して大学横断的な取組が必要であり、既存の委員会との連携を図り、今後の対策を検討する必要がある。
大学 G：私立工業大学	・利益相反規程と安全保障輸出管理に関する規程を制定。研究インテグリティについての規程はまだ作成していない。
国立研究開発法人 A	・利益相反マネジメント規程、安全保障輸出管理規定を制定。研究インテグリティの確保に関する規定を 2024 年 1 月から施行。
国立研究開発法人 B	・利益相反委員会の設置規程等は既に制定。研究インテグリティの確保に関する規程を 2023 年に施行。
国立研究開発法人 C	・2023 年 4 月に研究インテグリティについての規程を施行。

3.3.2　組織体制及び運用方法について

ヒアリングした大学・国立研究開発法人では、既に利益相反、安全保障輸出管理について検討する委員会、事務組織は設置されていた。一部の大学・国立研究開発法人ではそれ

に加えて、研究インテグリティに特化した問題を扱う委員会として、研究インテグリティ・マネジメント委員会（理事、部局長等をメンバーとする）、研究インテグリティ専門委員会（事務組織の担当課長等をメンバーとする）が新たに 2022 年、2023 年に設置された。研究インテグリティ担当室を設置した大学もあった。これらの委員会は、ポリシーの施行、助言的役割等のために、適宜開催され討議等が行われている。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

・国立大学で、特に大規模な研究大学（大学 A と大学 B）では、その広範な研究活動や複雑な問題にさらされる可能性が高いことを反映し、専門の「研究インテグリティ・マネジメント室」の設置、「研究インテグリティ・マネジメント委員会」の設置など、より専門特化した組織を持つ傾向がある。対照的に、中規模大学および私立大学（D、E、F、G 大学）は、研究インテグリティ業務を既存の組織体制（利益相反、安全保障輸出管理の委員会等）に組み込みし、担当部門間の調整を促進し、アドバイザーの役割の重要性を強調しながら、小規模に運営されている場合が多い。

・国立研究開発法人（A、B、C）では、研究インテグリティに包括的に取り組むために、さまざまな管理部門を統合することに強い重点を置いている。これらの国立研究開発法人は、大学が部局での対応の比重が大きいことと比較すると、より本部レベルで中央集権的なアプローチをとっているように見えるが、より機密性の高い研究を含んでいる可能性があるためとみられる。

全体として、どの大学・国立研究開発法人も研究インテグリティを確保するための取組をする必要性があるとの問題意識はあるものの、政府との距離、研究活動の国際化・オープン化の程度や大きさを反映して、新たなリスクへの対応のための取組の導入のスピードには差が出ている。

表 3-2：研究インテグリティの確保に関連する組織体制の整備状況・課題

ヒアリング先	内　　容
大学 A：国立研究大学	・利益相反、安全保障輸出管理についての部署は既にあった。「研究インテグリティ・マネジメント室」と「研究インテグリティ・マネジメント委員会」を 2023 年に新たに設置。
大学 B：国立研究大学	・2023 年に「研究インテグリティ・マネジメント会議」「研究インテグリティ・マネジメント実務委員会」を設置。 ・課題は、各部局の教員・事務担当者と本部の間で研究インテグリティ確保の重要性についての危機感を共有すること。
大学 C：中規模国立大学	・2022 年に「研究インテグリティ・マネジメント委員会」「研究インテグリティ専門委員会」を新設。 ・課題は、実際に検討を要する事案が発生した時にどう対応するのかと、部局ごとに研究インテグリティ関連の取組に差異が見られること。

ヒアリング先	内　　容
大学 D：公立大学	・利益相反マネジメント委員会（その下に利益相反委員会を設置）を設置。安全保障輸出管理はアドバイザーの助言を受けて、採用時の自己申告書の提出、外国籍教員の事前確認シートによる確認等を実施。
大学 E：私立総合大学	・研究倫理委員会、利益相反委員会、安全保障リスク管理委員会を設置。事務局はいずれも研究部。利益相反アドバイザー、安全保障輸出管理アドバイザーに相談。研究インテグリティに特化した委員会は設けていない。
大学 F：私立総合大学	・利益相反および安全保障リスク管理については、それぞれ委員会を設置。研究インテグリティについては、研究推進委員会が、研究推進、研究環境の整備、および研究倫理、研究不正を含む研究の心構えの管理を担当。 ・組織体制の課題に関しては、研究インテグリティについては部局横断的な取組が必要。
大学 G：私立工業大学	・安全保障輸出管理委員会と研究者倫理委員会を設置。委員会の事務は、主に大学事務局内の研究支援部署が担当。
国立研究開発法人 A	・2024 年 4 月にはインテグリティ担当課を新設。研究インテグリティに関する専門の委員会は設置しない。課題は、情報共有と各部署間の連携強化。
国立研究開発法人 B	・2023 年に研究インテグリティを統括する本部を設置。新たな組織立ち上げの課題としては、情報共有の仕方と人材育成。
国立研究開発法人 C	・2023 年 4 月に、「研究インテグリティ・マネジメント委員会」「研究インテグリティ・マネジメント専門委員会」を設置。

(1)　開示情報に基づくリスク判断の方法、関連する課題

ヒアリング対象の大学・国立研究開発法人においては、利益相反、機密技術の輸出管理、経済安全保障、研究の潜在的な軍事利用などに関連するリスクを積極的に管理している。そのアプローチは、研究者の厳格な自己開示プロセス、共同研究や提携の評価、特に外国企業との提携、外部からの影響から研究インテグリティを守ることなどが含まれる。情報の流れや技術的漏洩を包括的に管理する必要性が認識されており、多くの大学・国立研究開発法人が、開示された情報の正確性や適切性を検証する方法について模索している。

各機関とも、国際的な共同研究が増加し、機密性の高い技術が急速に開発されるなど、急速に進化する研究環境の中で、徹底的かつ効率的なリスク評価という課題に取り組んで

いる。研究インテグリティの維持、セキュリティの確保、オープンで協力的な学術環境の育成のバランスは、共通のテーマである。

各機関で浮き彫りになっている課題には、研究者から詳細な個人情報や兼業等の情報を入手して確認することの難しさ、海外の複雑な資金提供や共同研究の構造を理解すること、開かれた学術的共同研究とセキュリティのバランスを維持することなどがある。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

- 大規模で研究志向の国立大学（大学 A、大学 B）では、安全保障輸出管理や利益相反、研究インテグリティに焦点を当てた専門部署や委員会を設置するなど、リスク管理に対する体系的かつ包括的なアプローチを示している。中規模および小規模の機関、特に私立大学（C、E、F、G）は、個々の部局がリスク評価と管理において重要な役割を果たしている傾向があり、また、専門知識を有する外部アドバイザーからの助言も受けている。
- 大学は、特にその教育的使命や、学問の自由と安全保障上の懸念とのバランスをとる必要性に照らして、利益相反等の管理を重視する傾向がある。国立研究開発法人（A、B、C）は、国家安全保障規制や輸出管理法の遵守に強い重点を置いているが、これは政府資金による研究や技術開発との関係がより緊密である可能性があることを反映しているとみられる。

(2) リスクが懸念される場合の対応プロセス

ヒアリング対象とした大学・国立研究開発法人では、輸出規制の事前チェック、利益相反や安全保障輸出管理に関するアドバイザーとの協議、複雑なケースを審議・決定するための専門委員会の設置など、リスクを管理するためのさまざまな戦略を採用している。規程上の研究インテグリティとセキュリティに関する懸念やリスクに対処するための手順と体制を定めている。これには、様々な委員会、管理室、専門的な助言を行う外部組織やアドバイザーの関与が含まれる。ただし、多くの大学・研究機関では実際の対応プロセスについてはこれから学習している段階とみられる。

各機関は、新たなリスクに対応する態勢を整えており、リスクの定期的な監視・評価や、最新の規制・ガイドラインに基づくリスク管理戦略の更新を行う仕組みを持つ機関もある。多くの機関がアドバイザーとの協力関係を築いている。

(3) 既存の組織体制との関係

どの大学・国立研究開発法人も、安全保障輸出管理、利益相反への対応など、既存の組織構造（委員会や事務組織）の中での調整や、それら組織構造との調整を高めることが研究インテグリティの確保のためには重要であるとしている。それは、新たに研究インテグリティに関連する委員会や事務組織を設置している大学・国立研究開発法人でも、まだその途上にある大学においても同様とみられる。多くの大学・国立研究開発法人は、様々な

部門間の緊密な連携の必要性を強調し、研究活動の国際化・オープン化の高まりに応じて発生する新たなリスクが、そのような緊密な連携を通じて見いだされ、対処することを目指している。

3.3.3　運営トップレベルの関与について

ヒアリングした大学・国立研究開発法人の多くは、トップレベルの管理職（理事長、学長、理事など）が、研究インテグリティ確保のための体制作り（規程整備や委員会等の体制整備）やその運営、取組の実施に関与することを重視している。

大学や国立研究開発法人では、研究インテグリティを担当する副学長や特定の管理職をガバナンスに組み込んでいる（担当理事の任命、委員会の委員長への任命など）。この体制は、内部の事務組織や、外部の専門家を含む様々な委員会によって支えられていることが多い。

また、多くの大学・国立研究開発法人では、研究インテグリティに関する懸念が発生した際に迅速に対処するため、担当事務組織から担当理事に相談するプロセスが決まっており、定期的なトップマネジメントとの協議も含まれる。

多くの大学・国立研究開発法人では、ガバナンス体制のさらなる強化に取り組んでおり、研究インテグリティとセキュリティ対策の強化に継続的に取り組んでいることがうかがえる。

ただし、一部の私立大学では、研究インテグリティに積極的に取り組んでいるものの、研究インテグリティの確保のための組織体制や業務プロセスはまだ初期段階にあり、模索しており、具体的な方針の決定や日常業務に対して経営トップの関与の度合いを決めていないところもある。

3.3.4　研修・教育、セミナーの実施について

研究インテグリティに関する教育・研修としては、e ラーニングプラットフォームの導入、情報資料の作成と配布、セミナーや研修会の開催などが挙げられる。大学や国立研究開発法人はこれまでも、利益相反、安全保障輸出管理や研究倫理に関する継続的な教育に積極的に取り組んできており、これら業務を効果的に実施するには、教員・研究者・事務職員の包括的な理解の必要性が強調されている。

研究インテグリティに関する複雑な概念を多忙な教職員や研究者に対して具体的に簡潔に伝えることの難しさ、多様で多忙な教職員が確実に理解することの難しさといった課題も認識されている。

どの大学・国立研究開発法人も研究インテグリティとセキュリティ対策の重要性を認識しているが、その教育・研修の戦略と実施規模は、利用可能な資源によっても大きく異なる。大規模な国立大学や研究大学（A、B）では、e ラーニングプラットフォームや詳細なケーススタディプレゼンテーションなど、幅広い教育ツールを取り入れ、より体系的かつ

広範なプログラムを実施する傾向がある。これらの大学は、継続的な教育や、研究インテグリティを他のコンプライアンス分野と統合することに重点を置いている。

中規模および公立大学（C、D）も研究インテグリティを重視しているが、リソースが限られているため、セミナーや外部リソースへの依存度が高い。技術系大学を含む私立大学（E、F、G）は、安全保障輸出管理など特定の分野に重点を置く大学や、包括的な研究インテグリティ研修プログラムの計画段階にある大学など、多様なアプローチを示している。

3.3.5 他大学・研究機関との連携について

7 大学（A～G）、3 国立研究開発法人（A～C）へのインタビューから、研究のインテグリティ確保のための取組に関連した、他大学や研究機関との連携については、多様なアプローチや考え方があることが明らかになった。

A 大学は、国立研究大学のトップランナーとして、国内大学の中でリーダーシップを取ることを目指し、情報交換や取組に積極的である。B 大学は定期的な交流会を行っているが、C 大学は研究インテグリティを学内の問題と考えており、外部との連携は限定的である。公立大学の D 大学は、アドバイザー的役割やコンソーシアムへの参加を通じて連携に力を入れているが、私立の E 大学と F 大学は、地域のネットワークに参加し、問題解決を共有している。

国立研究開発法人 A、B、C では、国立研究開発法人協議会（国研協）のタスクフォースでの情報共有や政府への要望の明確化などを図っており、同協議会を情報共有プラットフォームとして活用してきている。

3.3.6 政府・資金配分機関への要望・提案について

ヒアリングでは、大学と国立研究開発法人ともに、政府や資金配分機関への要望や提案があった。特に国立研究開発法人からは、研究インテグリティや情報セキュリティの確保に対する具体的な方針の設定、安定的な予算の確保、共通システムや研修構築への支援を求める声が多く聞かれた。大学からも似たような要望が出されているが、国立研究開発法人の方が具体的な要望が多かった。

研究インテグリティの確保のための取組の重要性についての理解は示されたものの、どの大学・国立研究開発法人においてもそのために要するリソースと熟練した人材の確保については、一貫した懸念が示された。特に、大規模な大学・国立研究開発法人であれば、専門部署や職員をこれらの問題に充てることができるが、小規模な大学では予算やマンパワーが限られているため、大きな苦戦を強いられているとの認識があった。研究インテグリティやセキュリティに関する業務が複雑化し、事務レベルでも法律や専門的な知識が必要になっていること、また、専門的な知識を持ったスタッフを配置する必要性について言及している。

政府や資金配分機関に対しては、より明確なガイドラインと、より実質的な支援を求めている。現在の政府からの説明会や意見交換会などの開催やガイドライン制定は評価されているが、より直接的な支援、行動のための明確な枠組み、政府各部門からの合理的なコミュニケーションの必要性を表明している。特に、私立大学からは、研究インテグリティ確保のための取組としては、最低限何をすることが必要なのかを示してもらった方が対応しやすいとの声があった。

国立研究開発法人からは、研究インテグリティとセキュリティの一体的な性質により重点を置き、強固なセキュリティインフラのための安定した資金と、政府や資金配分機関との協力のための明確なガイドラインの重要性を強調している。

表 3-3：政府・資金配分機関への研究インテグリティの確保に関連する要望・提案

ヒアリング先	内　　容
大学 A：国立研究大学	・今後、どのように人材を育成していくかについての検討が求められる。 ・体制構築に必要な資金やサポートがあると望ましい。 ・研究インテグリティに関する理解を深めるための研究も必要。
大学 B：国立研究大学	・JST や NEDO などから懸念情報の提供があれば有益。 ・外為法への対応と異なり、研究インテグリティ関連の対応では、教職員から開示された情報の扱い方や判断基準、対策の方法が明確ではない。
大学 C：中規模国立大学	・研究インテグリティについての体制整備を進める上では、最低限必要な条件等について共通的なガイダンスが政府から示される方がやりやすい。
大学 D：公立大学	・人的リソースの配分が困難なため、研究インテグリティ対応について資金面での支援があれば助かる。 ・政府からの情報提供や説明会等開催はとても参考になっている。
大学 E：私立大学	・研究インテグリティに関する政府通知は政府の一つの部局で担当してもらえるとわかりやすくなるのではないか。 ・政府からの情報提供は参考になる。
大学 F：私立大学	・研究インテグリティの組織を構築する過程で生じた課題やうまくいかなかった事例についての情報提供は参考になる。
大学 G：私立工業大学	・どこに相談すれば解決の糸口を得られるかを知ることができる相談窓口が政府等にあれば、事務レベルで大変助かる。

ヒアリング先	内　　容
国立研究開発法人 A	・研究インテグリティと研究セキュリティは一体不可分な概念。情報セキュリティシステム整備が必要であり、その安定予算確保が不可欠。 ・研究インテグリティ確保の事例提供の継続。 ・資金配分機関は、具体的に研究インテグリティ確保のためにどんな取組をすることが必要かの要件を明示すること。
国立研究開発法人 B	・ガイドラインやリソース配分など、ある一定の枠組みが整備されることが望ましい（その際、研究の公開原則、研究活動を不必要に委縮させないことが重要）。
国立研究開発法人 C	・内閣府が想定するレビュー機関や専門家についての情報提供。 ・e ラーニングや申請システム構築の費用面の懸念。各法人で研修資料を英語化する際に表現や説明内容が異なる可能性がある。このため、政府主導で共通システムや共通の研修構築を実施する。

第4章　研究インテグリティについての意見交換会の実施

4.1　意見交換会の趣旨、目的

研究インテグ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・国立研究所等で研究インテグリティに関連する業務に従事している者）を交えて意見交換会を 2023 年 10～11 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・仙台・大阪の 3 か所で開催した。

＜対象＞

・大学、国立研究所等において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に従事している者（大学の教職員、研究機関の研究者・事務担当者等）

＜定員＞

35 名程度を予定として募集

＜開催日時・場所＞

第 1 回　2023 年 10 月 18 日（水）13:15～17:00　東京開催

第 2 回　2023 年 10 月 23 日（月）13:15～17:00　仙台開催

第 3 回　2023 年 11 月 20 日（月）13:15～17:00　大阪開催

＜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

4.2　意見交換会の開催内容

上記のように、3 回の意見交換会はいずれも 13 時 15 分から 17 時までの開催であり、開催プログラムは以下の形式とした。

＜プログラム＞

13:15-13:30　主催者挨拶・説明

13:30-14:30　講演と質疑応答（内閣府、警察、有識者）

・「研究インテグリティの確保に係る対応方針とその取組状況」（内閣府 科学技術・イノベーション推進事務局）

・「経済安全保障と警察の取組」（警察庁等）

・各意見交換会で以下有識者 1 名からの講演

第 1 回　「東京大学の研究インテグリティ確保に向けた取り組みと現場目線の研究インテグリティ対応」（東京大学 医学系研究科 利益相反アドバイザリー室 室長　明谷早映子）

第 2 回　「研究インテグリティの確保に向けた具体的取り組みの紹介－東北大学を例として－」（東北大学　金属材料研究所所長，副理事（研究公正担当）佐々木孝彦）

第 3 回　「大学法務機能を活用した研究インテグリティ確保の実現」（九州大学 法務統括室 室長補佐・特任教授　佐藤弘基）

14:30-16:00　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：重要な取組を実施する上での課題等
　研究インテグリティに関するリスクに備えて、所属する組織で追加で取り組むべきことと、取り組む上での課題について共有

・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

16:55-17:00　主催者挨拶

グループ討議は参加者が 6～8 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）、総合大学・単科大学（医科大学等）、研究大学かどうかなどを考慮し、なるべき同種の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）。

4.3　意見交換会への参加状況

上記のように、意見交換会の参加者対象者は、「大学、国立研究所等において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に従事している者」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り、会場定員を超える場合には一部 2 名参加希望の大学・研究機関からの参加人数を 1 名に減らしてもらうよう調整した。

3 回の意見交換会のそれぞれへの参加状況は表 4-1・図 4-1（機関種別）、表 4-2・図 4-2（地域別）に示すとおりである。第 1 回は 43 人、第 2 回は 21 人、第 3 回は 42 人が参加

した。第 1 回は国立研究開発法人からの参加者が 14 人いたが、第 2 回と第 3 回は大学関係者のみの参加となった。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（東京開催）は関東から、第 2 回（仙台開催）は東北から、第 3 回（大阪開催）は近畿からの参加者が多かった。ただし、今年度開催なかった北海道、中部、中国、四国、九州・沖縄地方からの参加者もみられ、ほぼ全国からの参加者があったと言えるだろう。

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、担当の教員が殆どであった。

表 4-1：意見交換会への出席者人数：機関種別

	国立大学	公立大学	私立大学	国立研究開発法人	合計
第1回（東京、10月18日）	14	2	13	14	43
第2回（仙台、10月23日）	8	5	8	0	21
第3回（大阪、11月20日）	17	6	19	0	42
合計	39	13	40	14	106

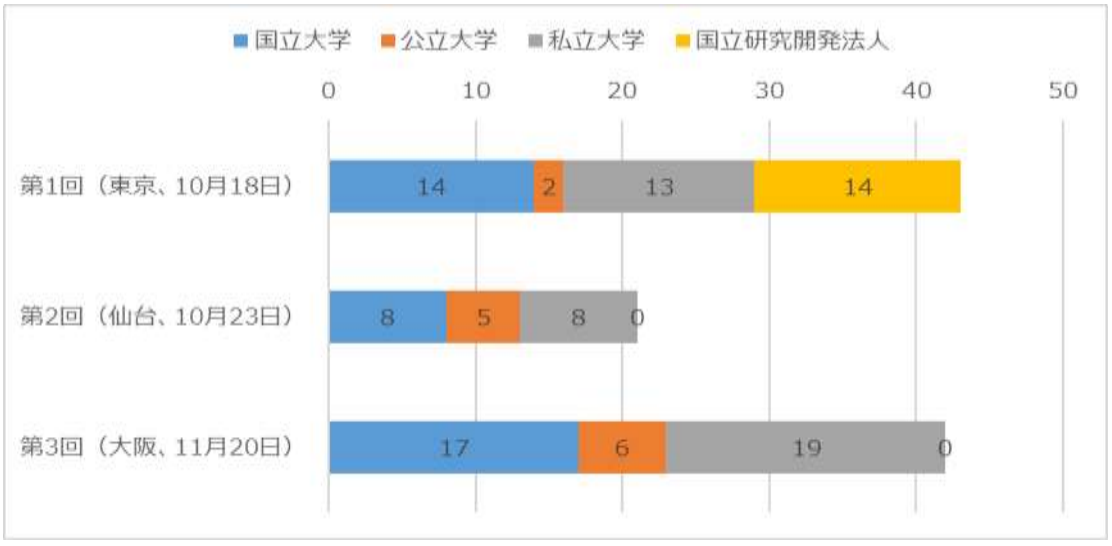


図 4-1：意見交換会への出席者人数：機関種別

表 4-2：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、10月18日）	1	2	31	3		1	3	2	43
第2回（仙台、10月23日）	1	11	4	2	1			2	21
第3回（大阪、11月20日）	2		2	4	22	3	2	7	42
合計	4	13	37	9	23	4	5	11	106

図 4-2：意見交換会への出席者人数：地域別

4.4 意見交換会参加者からの感想・質問等

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）内閣府からの説明について（参考になったかどうか（選択肢）、自由意見・コメント）、
2）警察からの説明について（参考になったかどうか（選択肢）、自由意見・コメント）、
3）有識者の講演について（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）

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 4-3、図 4-3 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[292]、参加者の意見は反映しているとみられる。5～6 割の参加者は「とても参考になった」、約 4～5 割は「参考になった」と考えていることが分かった。9 割以上の参加者は「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。

[292] 事後アンケートの回答率は、第 1 回 60%、第 2 回 76%、第 3 回 71%で、合計では 68%だった。

表 4-3：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、10月18日）	14	10	1	0	1	26
第2回（仙台、10月23日）	10	6	0	0	0	16
第3回（大阪、11月20日）	14	15	0	1	0	30
合計	38	31	1	1	1	72

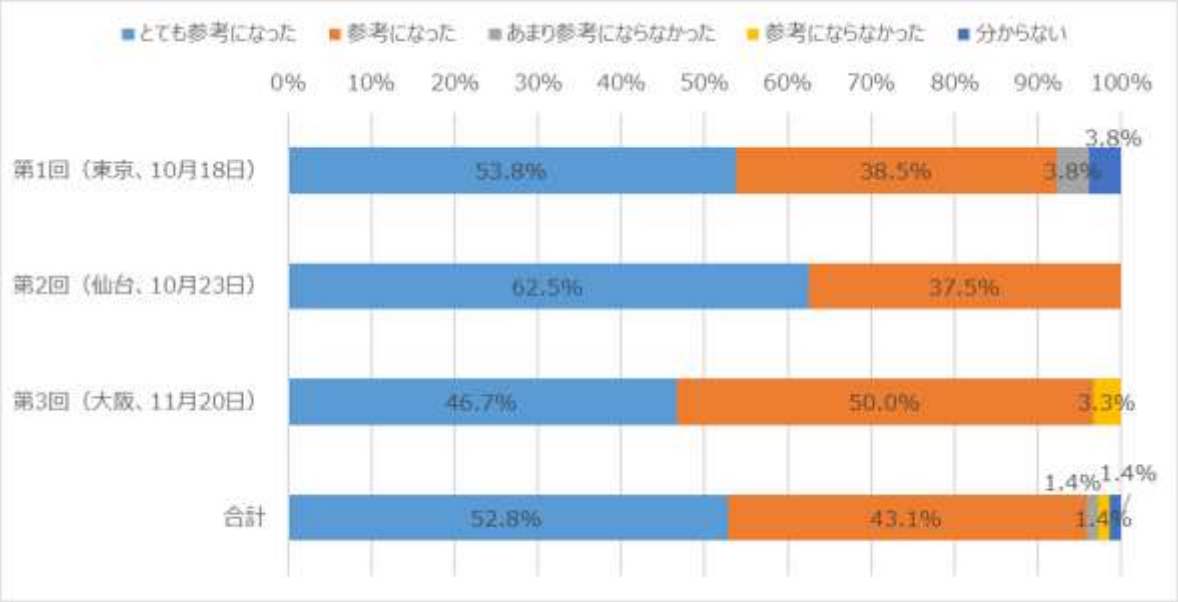


図 4-3：意見交換会の事後アンケート結果：グループ討議について

また、内閣府からの説明、有識者の講演、グループ討議については、それぞれ概要以下の自由記入の意見があった。なお、以下は参考になる意見等を紹介しているが、自由記入で表明された意見等は必ずしも常に多数意見を反映しているとは言えないことには留意が必要である。

<u>内閣府からの講演について</u>

政府の研究インテグリティ関連の政策についての理解が深まったとの回答があった一方で、研究インテグリティに関して、より明確なガイダンスと具体的な対策を求める声があった。研究インテグリティとセキュリティの重要性は認識されているものの、これらの基準を効果的に実施・維持するためには、より詳細で実践的なガイダンスやリソースが必要であることとの意見や、何が必須で、どのような対策をとるべきかについて、より明確なコミュニケーションが必要であるとの回答があった。具体的で実行可能なガイドラインがないため、大学・研究機関間で一貫性のない適用がなされる可能性があるとの指摘もあった。

また、研究インテグリティの定義をより明確にし、経済的セキュリティと研究インテグリティの関係を概説する、より包括的な資料を求める声があった。

大学職員からは、より明確な運営ガイドラインの必要性と、研究のインテグリティ維持における大学職員の役割の理解を深める必要性を強調し、研究インテグリティを効果的に管理するための具体的な情報やリソースの不足は、共通の懸念事項として示された。また、職員や教員の意識と理解を深めることの重要性が指摘された。

以下が意見の例である。

・改めて、国の方針について、確認できた。(私立大学、大学職員)
・研究インテグリティをめぐる現在の状況についての理解が深まった。研究者の先生方及び研究を守るために必要な取組であることについて、理解が深まった。(国立大学、大学職員)
・研究インテグリティの方針および重要性は理解できたが、やはり大学規模や分野別の落とし込みについてはそれぞれ対応しなければいけないのだと分かった。(公立大学、大学職員)
・担当部署に相談する体制の整備との文言が何度か出たが、そもそもどういう部署が担当になり、どんな案件ならば相談すべきかを内閣府の側から示してくれないと、現場の職員は困ると思う。(国立大学、大学教員)
・今の取組に加えて、機関が何をしなければならないのか示されるとよかった。(公立大学、大学職員)
・チェックリストの提供など大学への配慮に感謝する。しかし、安全保障輸出管理や利益相反、研究不正ガイドラインのように、業務として具体的に何を行うのか（申請書、業務手順書など）が明らかにされていない。今後、何をすべきなのかが理解しにくい状況である。（私立大学、大学職員）
・研究インテグリティの定義が不明確なため、政府が求める内容が見えにくかった。(国立研究開発法人、研究機関の職員)
・幹部をはじめとした教職員の意識醸成が大切だと思う。(私立大学、大学職員)

<u>有識者の講演について</u>

有識者からの講演は 3 回異なる大学教員からなされたが、参加者から共通して指摘された意見としては、第 1 に、リスク評価に関するケーススタディや方法論の共有・蓄積を強く望んでいるということがあった。参加者は、研究インテグリティ確保のための様々な懸念事項が様々な大学・研究機関でどのように対処されているか、具体的かつ実践的な事例に強い関心を示した。第 2 に、参加者からは、研究インテグリティ確保のための先進的な取組において、どのような組織構造や施策を採用しているのかについてより詳細な情報の必要性が示された。第 3 に、すべての大学・研究機関で大規模大学で採用されたシステムを見習うことの現実性について懸念が示す声があった。小規模でリソースに制限のある大学においてどのように体制構築を図るかについての意見があった。

以下が意見の例である。

・実際の取組事例を聞くことができて参考になった（特に体制について）(公立大学、大学職員)
・実際にご担当されている先生のお話は、実際の対応方法や問題点など伺えてとても参考になった。（私立大学、大学職員)
・各大学・機関ともに、手探りで対応を進めていること、共通の悩みがあることがわかった。(私立大学、大学職員)
・規模がかなり異なるので参考になる部分とそうでない部分があった。自施設に適した取組を、という話しだったが、かけられる人員、コストに大きな差異があると感じた。(公立大学、大学職員)
・本学にも当てはまるような課題も持ちながら、研究インテグリティ確保の実現に向けて取り組まれた内容を聞くことで、本学では、どこまで、何ができるか、少しイメージが沸いた。(私立大学、大学職員)
・組織執行部による理解の重要性など、参考となる点が多く得られた。(私立大学、大学職員)
・対象者、対象としているリスク、判断方法など、リスク管理業務の一端を伺うことができ、大変参考になった。(私立大学、大学職員)
・自身の組織と比べた結果、とても真似できない。(国立大学、大学教員)
・必ずしも追随出来るものではないが、他を知ることは自身の取組を振り返る良い機会となった。(国立大学、大学教員)
・理解を深めてもらうにはまずこちらがきちんと理解しなくてはならない、そのうえでどう共感を得ていくか、大きな課題ながらヒントの糸口が見えた気がした。(国立大学、大学教員)
・本学はまだスタートラインにさえ立てていないので、大変刺激を受けた。(私立大学、大学職員)
・中小規模の大学でも体制整備ができるとのことだったが、具体例を知りたい。(公立大学、大学職員)

<u>グループ討議について</u>

グループ討議についての自由記入の意見では、まず、第 1 に、時間的制約がある中でいかに有意義な情報交換を図るかという点についての指摘があった。参加者からは、グループ討論を高く評価しながらも、より深い議論を望んでいたとの指摘や、モデレータが主導する、より構造化された集中的なディスカッションへの要望も示された。参加者からは、ディスカッションの時間をもっと取りたい、他大学とは異なる視点や実践をもっと学びたい、といった声も聞かれた。第 2 に、グループ討議を通じて有効な情報共有が行われたとの指摘があった。グループ討議では、さまざまな大学・研究機関の間で情報、課題、ベストプラクティスを共有する貴重な機会であったとの意見や、大学や研究機関を超えた協力の重要性を強調する意見があった。第 3 に、大学・研究機関のリソースの格差についての指摘である。大学・研究機関によって資源や経営支援のレベルが異なることが指摘され、また、潤沢な資金

を持つ大学の参加者は、予算の制約や事務的支援に悩む他の大学と比べて、自分たちが有利な立場にあることを認識する意見があった。第 4 に、グループ討議で少人数で議論することを通じて、関係者の間でネットワーク作りに役だったとの指摘があった。

以下は意見の例である。

・研究者への周知の問題など、各大学等の取組や現状の疑問点・問題点、運用に向けた体制構築での検討など、様々な状況を知ることができて、大変有意義な会だった。（私立大学、大学職員）
・他大学の取組の現状、問題点、今後の課題がわかり、持ち帰って検討する際の非常に重要な情報を得られることができた。（私立大学、大学職員）
・講演を聞く機会は多いが、このように他大学と討議や対話といったかたちで研究インテグリティで課題や知見を深めることができたのは貴重な機会だった。（私立大学、大学職員）
・悩みも共有できる場で、もっと時間が欲しいくらいだった。（国立大学、大学職員）
・各大学・機関ともに、手探りで対応を進めていること、共通の悩みがあることがわかった。（私立大学、大学職員）
・研究インテグリティに関する他大学の取組状況が参考になる。（私立大学、大学職員）
・課題設定がグループごとに行われ、参加機関の機関内の検討度合いに合わせた議論がなされたように思うが、今一つ議論が深堀されなかった。（国立大学、大学教員）
・もう少し深くディスカッションしたかった。情報や課題など共有できることが多く，大変有意義だった。（私立大学、大学職員）
・実際に各法人がどういった取組をしていて、どういったことが課題になっているのかを詳細に共有でき、自身の所属機関において必要な点などについて気づきを得ることができた。（国立研究開発法人、研究機関の職員）
・他の国研の考え方や、問題意識が共有され、今後の研究インテグリティの取組の参考となった。（国立研究開発法人、研究機関の研究者）
・同じ悩みを共有していることが分かり、安心するとともに、今後も相談できる関係性が築けた。（国立研究開発法人、研究機関の職員）
・他大学の取組状況、課題が共有できたことは、参考になったとともにネットワークを構築できたことは大変ありがたい取組でした。（私立大学、大学職員）
・体制整備の必要性がまだ大規模大学と中規模大学では特に差があると感じた。（公立大学、大学職員）
・他大学の取組状況を知ることができた。国立大学は、規模も人材も公立大学に比べると充実していることがよくわかった。（公立大学、大学職員）
・国立大学と私立大学における状況の違いをヒシヒシと感じた。（私立大学、大学職員）
・グループ内の規模感なり取組状況に差があったが参考になった。（国立大学、大学職員）

意見交換会全体について

図 4-3 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。参加者は、グループディスカッションや異なる機関から学ぶ機会を高く評価した。今後も今年度実施した意見交換会のような継続的な対話と支援が強く求められた。ネットワーキングや継続的な議論の場の必要性についての指摘があった。全国で、このような議論を継続し、継続的な対話と支援のためのネットワークを構築することに強い関心が示され、ベストプラクティスや課題を共有するための継続的なプラットフォームの必要性の指摘があった。

また、会議では、研究インテグリティについての理解度や実施レベルが様々であることが浮き彫りになり、特に小規模でリソースが限られている大学からの参加者からは、より体系的なガイダンスや支援が必要であるとの指摘が多かった。研究インテグリティに取り組むための十分なスタッフやリソースを確保することの難しさを強調し、小規模な機関への支援を求める声が目立った。多くの参加者、特に私立大学の参加者からは、リソースの配分や具体的で実行可能なステップの必要性など、ガイドラインを実施するための実際的な側面についての関心の声があがった。

全体として、政府からのより明確なガイドラインや支援を求める声があった。研究インテグリティの定義をより明確にする必要性を強調し、研究インテグリティに関連する問題の具体的取り扱いについて、詳細なガイダンスを求める声があった。

以下は意見の例である。

・大学等の関係者での意見交換はとても面白く役立った。（国立大学、大学職員）
・グループディスカッションについては、同じような状況の大学と意見交換ができて参考になった。（私立大学、大学職員）
・やはりグループディスカッションの効果は大きいと感じた(国立大学、大学教員）
・他大学のご担当から生の声をきけて非常に参考になった。（国立大学、大学教員）
・グループ討議の時間は有意義で、気づかない点をご教示いただけた。（国立大学、大学職員）
・講演を聞いてディスカッションすることで、少しではあるがまず本学がやらなければいけないことが何かをイメージできた。（私立大学、大学職員）
・研究インテグリティについて、情報が少なく、今回の会議は非常に役に立った。（国立研究開発法人、研究機関の研究者）
・各機関の取組状況や課題も共有でき、有意義な意見交換会だった。（国立研究開発法人、研究機関の職員）
・研究インテグリティについて各法人手探りで対応されている中、数少ない専門家のお話を聞けたことや、各法人の担当者と知り合うことができた点が一番の収穫だった。今後もこのような機会を設けていただけると大変有難い。（国立研究開発法人、研究機関の職員）
・他機関との担当者同士の交流の場として、大変有意義と感じた。（国立研究開発法人、研究機関の職員）
・このような意見交換会を継続して行っていただくと、色々な情報が入手できて有意義と思う。（国立大学、大学職員）

・ぜひこのような交流、意見交換の場をこれからも設けていただきたい。行き詰った時に相談できるネットワークができたらと願う。(国立大学、大学教員)
・このような会を定期的に開催してもらえれば助かる。(公立大学、大学職員)
・またこのように意見交換や対話ができる機会を設けていただけると、非常にありがたい。（私立大学、大学職員)
・今後も定期的に開催いただけるとありがたい。(私立大学、大学職員)
・話を聞いていると、研究機関個々での解決がなかなか難しいことが分かった。国のサポートを望みたい。(国立大学、大学職員)
・特に小さな大学は研究インテグリティに対応する人員をしっかり確保できているわけではなく、小規模大学でも対応していけるような方策を検討いただきたい。(国立大学、大学職員)
・対応したいが対応方法が理解できていない。現場レベルで具体的な対応方法を説明していただきたい。(私立大学、大学職員)
・皆さんが悩むところは似たようなところと分かったが、どのようにすれば良いかという明確な答えは得られなかった。（国立研究開発法人、研究機関の職員)
・大学によって取組や対応が異なっても構わないことが分かった。(私立大学、大学職員)
・危険な相手(企業・機関)について調べるツール(リストと検索機能含む)の提供をお願いしたい。（私立大学、大学職員)
・人員、コストをかけずに体制を整備し、有効に機能している施設があれば紹介いただきたいと思う。(公立大学、大学職員)
・予算が削られ、入学生確保や学務が優先される状況下、研究インテグリティ問題はどうしても後回しなる、という意見は切実である。相談窓口を設置したり、HP で Q&A や事例を公開したりといった国のサポートが不可欠だと思った。(私立大学、大学職員)
・大学・法人として、どこまで本気で取り組むかが非常にポイントであることが共有できてよかった。また、人脈形成ができたので、今後、活用していきたい。(私立大学、大学職員)

第5章　調査のまとめ・分析と注目点

5.1　各国・地域における研究インテグリティに対する取組状況の調査における注目点のまとめ

以上、17 カ国・地域の研究インテグリティ政策は、オープンかつ倫理的な研究環境を育成すると同時に、国際的な共同研究、スパイ活動、外国からの干渉に関連するリスクから学術的・科学的活動を保護することの重要性への共通した認識を反映している。以下は、これらの多様な地政学的背景の中で共通して観察されたポイントである。

- 共通の目標：どの国・地域も、自国の安全保障上の利益、知的財産、技術的進歩を、特に経済的・軍事的安全保障に不可欠とみなされる分野において、潜在的な外国の脅威から守ることに力を注いでおり、特に近年取組は強化されてきている。
- ガイドラインと枠組み：英国やニュージーランドの「Trusted Research」やカナダの「Safeguarding Your Research Portal」、また北欧の「responsible research」など、国際共同研究におけるリスク管理について、大学・研究機関や研究者に明確な指針を示すことを目的とした具体的なガイドラインや枠組みを策定している国が大半である。
- 政府と大学・研究機関の協力：政府機関、大学・研究機関間の連携を促進し、研究インテグリティ、研究セキュリティの総合的な強化を図る傾向が顕著である。例えば、オーストラリアの UFIT や英国の Universities UK、カナダのカナダ政府-大学ワーキンググループは、マルチステークホルダーアプローチを強調している。
- リスクの高いパートナーシップや技術への焦点（risk-based なアプローチ）：スウェーデン、ノルウェー、フィンランド、デンマークなどは、国際協力、特に中国やロシアなど急速に進展する研究協力や地理的隣接に伴う脅威のためにリスク管理を重視している。カナダの新方針では、機微技術とリスクの高い海外大学・研究機関をリストで指定している。他方で、EU では「国を問わないアプローチ」（country-agnostic approach）をとり、特定国をターゲットと明示せずに、特定国や地域の出身者への差別を防止するための配慮も見られる。
- 法律および規制措置：一部の地域では、研究セキュリティ確保の取組について法的強制力を与えるために法律が制定され、また、近年の国際情勢の緊迫を背景として議会における法律制定の動きが見られる。例えば、米国の国防授権法や Chips および科学法、フランスの PPST プログラムがその例である。
- サイバーセキュリティとデジタル保護措置：サイバーセキュリティ対策は、研究セキュリティ戦略の重要な要素であり、機密データや研究成果をサイバー脅威や不正アクセスから保護する必要性に対処するものである。研究インテグリティ、研究セキュリティの確保のための取組においては、大学・研究機関におけるサイバーセキュリティ対策が含まれていることが多い。例えば、欧州委員会の「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」である。

- 教育と意識向上：研究インテグリティとセキュリティの重要性に関する研究者や研究機関のスタッフの認識を高め、ベストプラクティスに関するトレーニングを提供することは、共通のテーマである。これは、研究コミュニティ内に責任と警戒の文化を醸成することを目的としている。政府資金でオンライン研修教材を開発したり（米国）、大学・研究機関間で共有するなどの動きがみられる。
- モニタリングとコンプライアンス：各国は、研究活動を監視し、セキュリティプロトコルの遵守を確保するための仕組みを導入または強化している（カナダの新ポリシーなど）。これには、国際的なパートナーシップや資金源を吟味する際のリスク評価やデューディリジェンスが含まれる。
- 国際研究協力の重要性：安全保障が重視される一方で、国際的な研究協力の利点も認識されている。政策では、リスクの軽減と国際的な科学協力の利点の活用のバランスをとることを目指している（EU のオープンサイエンス重視など）。
- 各国独自の事情：各国のアプローチは、その国特有の地政学的背景、技術的強み、戦略的優先事項の影響を受けている。例えば、イスラエルが国防と民生研究部門の統合に重点を置いていることや、台湾が機密技術の知識移転の防止に重点を置いていること、さらに軍事産業が学界との協働で発展し、基幹産業の一つをなすノルウェーでは軍事先端技術の移転防止を図っていることは、国家安全保障上の独自の懸念を反映している。

また、調査対象とした国・地域の中では以下のような進んだ取組も見られた。カナダの政策は明確で先進的であり、カナダ固有のニーズに効果的に対応しているが、米国と EU は、その政策、インフラ、世界的影響力が、世界の研究インテグリティ・セキュリティ基準に広範な影響を与えるベンチマークと実践を設定しているという意味で、主導的である。

・カナダは、特に "Safeguarding Your Research Portal "と "National Security Guidelines for Research Partnerships"、「機微技術研究と、懸念される提携に関する政策」の開発・策定により、研究インテグリティ・研究セキュリティの確保のための積極的かつ体系的なアプローチを示している。これらの措置は、「研究セキュリティセンター」の設立や機密技術研究に焦点を当てた政策の導入と相まって、特に研究コミュニティに実用的なガイドラインやリソースを提供するという点で、カナダのアプローチが先進的であることを示唆している。研究セキュリティ対策をより広範な国家安全保障の枠組みの中に統合する一方、国際的な協力を促進する環境を整備している。
・米国と欧州連合（EU）は、いくつかの理由から、研究インテグリティ・研究セキュリティ政策の分野でリードしていると考えられる。米国は、NSPM-33 のようなイニシアティブと、それに続く科学技術政策局（OSTP）のガイダンスを通じて、研究インテグリティと研究セキュリティを守るための強固な枠組みを築き、国際的なリーダーシップも取ってきた。このような努力は、法的・規制的手段（Chips and Science 法、国防授権法）によって補完されている。米国の指導的地位は、その広範な連邦研究インフラと研究機関の

世界的影響力によってさらに強固なものとなっている。

・EU もまた、「研究とイノベーションへのグローバルなアプローチに関するコミュニケーション」や、「研究セキュリティ向上に関する理事会勧告の提案」に見られるように、外国からの干渉に対処するための包括的なアプローチにより、研究セキュリティにおけるリーダーとしての地位を確立している。EU の戦略は、加盟国間の集団行動を重視し、EU 圏の規制的枠組みを活用して、研究セキュリティとインテグリティに関する課題に取り組む一方、オープンサイエンスや研究協力といった価値観を推進している点で注目に値する。

表 5-1 において、調査対象国・地域における研究インテグリティに関する主な規則・ガイドライン等（名称、制定年月、担当機関、内容・特徴）をまとめた。

表 5-1：調査対象国・地域における研究インテグリティに関する主な規則・ガイドライン等

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
米国	国家安全保障大統領覚書-33(NSPM-33)【大統領令】	2021年1月	大統領府科学技術政策局（OSTP）	米国政府が支援する研究開発（R&D）を、外国政府の干渉や搾取から守るための行動を指示。研究セキュリティの確保に関連する 5 分野（1. 情報開示の要件と標準化、2. デジタル永続的識別子、3. 開示義務に違反した場合の結果、4. 情報の共有、5. 研究セキュリティプログラム）。
米国	NSPM-33 実施ガイダンス【連邦政府規則】	2022年1月	大統領府科学技術政策局（OSTP）	連邦省庁に対し、NSPM-33 の実施（上記の 5 分野）に関する詳細な指針を提供。
米国	FY2020 国防授権法【連邦法】、FY2021 国防授権法【連邦法】	2019 年 12 月、2021 年 1 月	連邦議会	すべての連邦政府の資金配分機関に対して、研究助成金申請プロセスの一環として、現在及び未決の支援についての情報開示を、申請研究者に対して求めることを義務付けた。
米国	Chips and Science 法【連邦法】	2022年8月	連邦議会	「外国人人材採用プログラム」についてのガイドライン策定、米国科学財団（NSF）に Research Security and Policy Office を設置、研究開発助成の申請時にリスク評価を NSF が実施する権限付与、大学・研究機関や研究者がセキュリティリスクを理解し軽減できるように独立したリスク評価センターの設立などを連邦政府に義務付けた。
米国	NSF Guidelines for Research Security Analytics【NSF 規則】	2023年2月更新	NSF	NSF の Office of the Chief of Research Security Strategy and Policy（OCRSSP）の責任とプロセス、NSF 職員によるモニタリング・報告、OCRSSP による許可・禁止行為、研究セキュリティ分析のためのデータ・サービス・分析手法、研究セキュリティ関連情報の共有原則について説明。
米国	「海外からの影響対策プログラム」（Countering Foreign Influence Program: CFIP）【国防省規則】	2022 年?	国防省 DARPA	DARPA の研究プロジェクトに関連する重要な技術及び実行者の知的財産の保護を目的とした適応型リスク管理セキュリティプログラム。リスク評価は、標準フォーム（SF）424「Senior/Key Person Profile (Expanded)」及びその付属文書等に基づいて行われる。
米国	高等教育機関における国防省資金配分による研究における望まない海外からの干渉への対抗【国防省規則】	2023年6月	国防省	「基礎研究提案の利益相反緩和の判断材料となる決定マトリクス」を含む。「FY22 リスト」は、国防授権法 1286 条(c)(8)(A)に記載された問題のある活動に従事していることが確認された外国機関（外国の人材プログラムを含む）を特定。
英国	Trusted Research Guidance for Academics【NPSA 作成のガイダンス】	2019 年	国家防護安全保障局（National Protective Security Authority: NPSA）	大学・教育機関向けに、「Trusted research」に関する理解を促すためのガイダンスである。大学におけるセキュリティの脅威の管理とセキュリティガイダンスの実施に焦点を当てる。
英国	Managing risks in Internationalisation: Security related issues【UUK 作成文書】	2020 年 10 月	Universities UK (UUK)	NPSA の「Trusted Research」キャンペーンを踏まえ、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、英国の大学向けのガイドラインである。
英国	Managing risks in international research and innovation【ガイダンス】	2022年6月	NPSA、UUK および UKRI	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、これまで作成したガイドラインや主要原則をまとめたガイダンスである。
英国	Security and risk: how universities can protect their research and people【ガイダンス】	2023年6月更新	UUK	大学が直面する安全保障上の脅威、脅威に対処するための措置、大学で安全保障ガイダンスを実装する方法、大学全体で安全保障を重視する文化を根付かせる方法等について纏めたもの。

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
豪州	オーストラリアの大学分野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（UFIT ガイドライン）【政府・大学等共同策定文書】	2019 年 11 月（2021 年 11 月改定）	政府機関（教育省等）、豪州研究評議会（ARC）等の資金配分機関	外国からの干渉に共同で対処するために設置された「大学対外干渉タスクフォース(UFIT)」（政府機関、大学・研究機関が参加）」を通じて意見調整し、策定された。大学・研究機関における外国干渉セキュリティの一連の審査は、同ガイドラインに基づいて行われている。
豪州	重要技術のための青写真と行動計画【連邦政府規則】	2021 年 11 月	首相府 重要技術政策調整室(CTPCO)	豪州研究評議会（ARC）は、競争的研究資金の申請にあたり、このリストに記載された技術が含まれている場合には、リスクがあるかどうかを検討する。
豪州	トランスナショナル教育に関するデューディリジェンスについてのガイダンスノート【政府・大学等共同策定文書】	2023年6月	UFIT のトランスナショナル教育ワーキンググループ	トランスナショナル教育（Transnational education: TNE）、すなわち、学習者の所在地が教育機関の所在地とは異なる国である高等教育プログラムについての外国干渉リスクへの対応について記述。
カナダ	アカデミックなコミュニティにおけるセキュリティ意識の醸成【公共安全省規則】	2019 年	公共安全省	外国の国家や集団を含む潜在的脅威からカナダの学術機関における機密研究保護の重要性を強調。強力なサイバー衛生の実施、研究のデュアルユース用途の認識、法律や規制の下での責任の理解などを推奨
カナダ	Safeguarding Your Research Portal【政府・大学等共同策定文書】	2020年9月	カナダ政府・大学共同ワーキンググループ	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。ワーキンググループは定期的に会合を開き、本ポータルは研究セキュリティ強化の取組を広めるための重要なチャネルとなっている。
カナダ	国際研究協力に対する国家安全保障ガイドライン【連邦政府規則】	2021年7月	連邦政府	研究パートナーシップの開発、評価、資金提供におけるデューディリジェンス、リスク評価、緩和に焦点を当て、研究パートナーシップにおける国家安全保障への配慮を統合するためのガイドラインである。
カナダ	機微技術研究と、懸念される提携に関する政策【連邦政府規則】	2024年1月	連邦政府	機微技術研究分野のリストと、懸念される海外の大学・研究機関のリストを含む。機微技術研究分野研究の研究助成金等は、関与研究者が、海外の軍等の大学、研究機関等に所属又は資金等受領している時、今後は提供されない。
欧州連合	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【欧州委員会作成文書】	2022年1月	欧州委員会	EU 加盟国や大学・研究機関に対し法的拘束力を持つものではない。外国からの干渉の防止、対処のために大学・研究機関がどのような行動を取ることができるかを具体的に記述（価値観、ガバナンス、提携、サイバーセキュリティ）。
欧州連合	研究セキュリティ向上に関する理事会勧告の提案【欧州委員会作成文書】	2024年1月	欧州委員会	責任ある国際化のための原則について説明。リスクの特定と評価、セキュリティ方針と手順の策定、研究者等の意識改革の重要性を強調。さらに、国際協力と情報共有の必要性も強調。
フランス	デクレ 2011-1425:刑法 413 条 7 項への国の科学・技術可能性保護施策（PPST）の適用【デクレ（大統領・首相命令）】	2011 年 11 月	大統領府、首相府	PPST 実施のためのデクレ（大統領・首相命令） ※PPST : 研究活動が行われている機関・施設において、国の優位性に貢献する戦略的知識、ノウハウ、機密性を有する技術を保護するために行われている政策。政策主管は仏防衛・国家安全総局（SGDSN : 首相管轄）で政策実施監督は 6 つの省の防衛・安全保障上級高官（HFDS）。
フランス	科学・技術可能性保護施策（PPST）【アレテ（行政命令）】	2012年7月	政府	上記 PPST 実施のためのアレテ（行政命令）
フランス	国の科学・技術保護施策（PPST）について【省際間通達文書】	2012 年 11 月	政府	上記 PPST 実施のための省際間通達文書
フランス	国の科学・技術保護施策（PPST）【パンフレット】	現行版インターネット掲載：2018年8月	仏防衛・国家安全総局（SGDSN）	上記 PPST 実施のための普及パンフレット

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
フランス	我々の科学資産と学術の自由をより良く保護するために【調査報告書】	2021年9月	仏上院	研究活動を行っている機関、場所への外国からの脅威は無視できなくなっているという状況について、上院議員アンドレ・ガトランが主導する調査部会がまとめた報告書を発表した
ドイツ	大学の国際協力に関するガイドラインと基準【HRK 策定・発表文書】	2020年4月	ドイツ学長会議（HRK）	世界的な環境の大きな変化に伴い大学の国際協力についての対応を包括的に策定。
ドイツ	中国との大学の国際協力におけるガイドライン・クエスチョンズ【HRK 策定・発表文書】	2020年9月	ドイツ学長会議（HRK）	中国共産党（CCP）が研究機関に及ぼす影響などについて指摘。
ドイツ	マックス・プランク協会の国際協力の発展のためのガイドライン【マックス・プランク協会作成文書】	2021 年	マックス･プランク協会	研究の自由、ルールの遵守、個人の責任のバランスをとりながら、国際協力を成功させることができるように支援するために策定。 研究者らに国際協力における潜在的なリスクに対する認識を高めさせるなどの目的を有する。
スウェーデン	中国に係る問題へのアプローチ【政府通信】	2019年9月	スウェーデン外務省	影響力を高める中国との関係及び中国に対するスウェーデンの接近のあり方について概略を示し、中国との協力においては好機と困難の両面があるとの見解を示す。
スウェーデン	責任ある国際化：国際的学術交流のためのガイドライン【基金配分機関ガイドライン】	2020年2月	研究と高等教育機関の国際協力のためのスウェーデン財団	大学、研究機関とその教員及び職員、学界リーダー向けのガイドラインであり、国際共同研究や教育協力を行う際に考慮すべき点を挙げ、具体的なチェック項目を示し、このガイドラインに基づいて各大学等が責任ある国際化と学術協力のアプローチについて構造的かつ有用な議論を行うよう提案する。
スウェーデン	責任ある国際化によっていかに業務を遂行するかに関する高等教育機関への助言【資金配分機関文書】	2022年5月	研究と高等教育機関の国際協力のためのスウェーデン財団	規模や歴史、国際化の進展において異なる３大学と１研究機関の経験に基づいて、研究・教育の国際化によって生じる課題（challenges）を抽出し、対応策を検討することによって、４機関の異なる特性によって生じるアプローチをタイプ分けしてそれぞれのメリットと課題が整理されている。さらに、４機関の中の１つの大学を取上げ、その現状を詳細に分析し、参照ポイントの創設、知識の共有、成果の考察と接合の３点から構成される「責任ある国際化」モデルを提案する。
スウェーデン	世界に責任をもつ関与:チェックリスト【学術団体文書】	2023年4月	スウェーデン高等教育機関協会	国際協力活動の開始前にパートナー研究機関（者）について検討すべき 6 項目、すなわち ①民主主義と学問の自由が担保されているか、②パートナー研究者の評判と所属大学の評価、③データ使用、知的財産権、特許権に関する対立の可能性の有無、④研究の不正利用と意図しない悪意ある応用の可能性、⑤倫理ダンピング：ヒト及び生物のデータに関する安全性が確保されているか、⑥パートナー研究者の安全性は担保されているかを例示している。
ノルウェー	知識移転管理のためのガイドライン【政府ガイドライン】	2020 年 10 月	ノルウェー外務省	ノルウェーの輸出管理規則の枠内において特段の注意と考慮が求められる教育機関の外国人の入学許可や雇用等を支援することを目的に、これら教育機関に対し知識の「機微性の高さ」を評価し、外国の学生、研究員、雇用者への知識移転がノルウェーの輸出管理規則に違反しないかを査定することを求める。

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
ノルウェー	外国人研究者等受入れのための事前免許制【政府規則】	2022年3月	ノルウェー外務省	機微な知識の移転が外国人に行われる前に、外務省に事前許可のための免許を申請しなければならない。学術スタッフの募集、客員研究員の受け入れ、大学院の入学にはこの規則に基づく審査が求められる。免許＝事前許可は必ず入学許可や雇用契約がサインされる前に得ておかなければならない。なお、当該人物が免許の申請が必要な国の出身者か、否かについての固定的なリストはなく、ケースバイケースで査定しなければならない。
ノルウェー	責任ある国際知識協力のためのガイドラインとツール【政府ガイドライン】	2023年8月	ノルウェー教育研究省	国際学術協力におけるリスクを管理し、安全を強化するために、当該事業に対し考慮すべき点及び均衡の取れた協力関係を築く上で必要な情報を提示するとともに、機関がそれぞれの事情に応じて、独自の計画を立てることができるように実務的な手法を提供する。個々の大学がその関心の範囲、価値あるいは資産と弱点を特定し、リスクを認識することを要請する。
フィンランド	対中アクションプラン【政府行動計画】	2021年6月	フィンランド外務省	中国との協力、意義、将来の方向性について全体的な精査を行う一方､メンバー国としてEUと歩調を合わせるという観点に則って、中国との関係を協力、競合、制度的ライバルの3つの次元から捉える。人権に基づく外交と安全保障政策に従い、政策評価を人権への影響という観点から実施するため、中国の人権状況を注意深く監視しなければならないとする。
フィンランド	中国との学術協力のための勧告【政府勧告】	2022年3月	フィンランド教育文化省	フィンランドの高等教育機関および研究機関が自らの原則と価値によって中国のパートナーとの研究協力を推進すべきことを前提に、研究機関がその価値や関心に基づいて中国のパートナーとの協力を支援するとともに、対中協力において生じ得るリスクを周知し、注意を払うべき事項を例示する。
デンマーク	国際的な研究・イノベーション協力指針〈ガイドライン〉【政府ガイドライン】	2022年5月	デンマーク高等教育･科学省	2020年に高等教育･科学大臣が設置した「国際研究･イノベーション協力指針委員会（URIS）」で議論を行い、倫理的・財政的・安全保障上のリスクに対する組織的な意識向上、リスク管理のための組織的な枠組みと手順、全国的な共通アプローチと知識の共有の観点から提言を行った。本ガイドラインは、デンマークの教育・研究機関の経営陣を対象としたガイドラインである。
デンマーク	あなたの研究はリスクにさらされている？【ガイダンス】	2021年5月	デンマーク安全保障・情報局､デンマーク高等教育･科学省	安全保障・情報局と高等教育・科学省が、研究機関の職員が外国からの干渉やスパイ活動をどのように防止し、対応するかについて勧告したものである。
オランダ	Knowledge Security Framework	2021年7月	オランダ大学連盟	オランダの大学が知識セキュリティに対するコミットメントを表明し、知識セキュリティに関する意思決定や方針を策定する際の助けとなるように作成された。
オランダ	知識セキュリティに関する国家ガイドライン	2022年1月	オランダ大学連盟､オランダ王立芸術科学アカデミー等の研究セクターが共同で作成。	国際共同研究に対処し、機会と安全上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。
チェコ共和国	外国からの干渉対策マニュアル【内務省 ハイブリッド脅威対策センター作成文書】	2021年	内務省 ハイブリッド脅威対策センター	外国からの干渉に対抗するための個人の責任と組織の協力の重要性を強調。このガイドラインに従うことで、学術界は学問の自由を守り、透明性を維持し、外部からの脅威に対する強靭性を築くことができると説明。

国・地域	ガイドライン・規制等名称【種類】	制定年月	担当政府機関等	内容・特徴
ニュージーランド	信頼される研究－研究機関と研究者のためのガイダンス【ガイダンス】	2023年8月	Protective Security Requirements（特殊法人）、サイエンス・ニュージーランド、ニュージーランド大学協会	「Trusted research」の実施に向けて、ニュージーランドの研究・イノベーションにおける潜在的なリスクを理解し、研究者、大学、研究機関、産業界のパートナーが国際共同研究に自信をもって潜在的なリスクに対して決断できるよう支援するものである。
ニュージーランド	信頼される研究：セキュリティ保護要件－アオテアロア・ニュージーランドの大学執行部のための手引き【ガイダンス】	2022年9月	ニュージーランド大学協会	「Trusted Research」（信頼される研究）を進めるため、ニュージーランド国内大学の執行部（シニアリーダー）が、信頼される研究、セキュリティ保護要件を取りまとめた。本手引きでは、学において組織内部、教職員、学生等との対話を始める際の手引きとしてとりまとめられた。
韓国	「国家研究開発事業におけるセキュリティ対策」規則【8省庁共同規則】	2023 年 11 月	科学技術情報通信部等の 8 省庁	国家研究開発プロジェクトにおける機密技術や研究成果を外国のスパイ活動や不正アクセスから保護することを目的とし、国、大学・研究機関で実施すべきことを規定（委員会の設置、規則制定、責任者の任命、教育・研修等）。
韓国	研究セキュリティ管理及び研究成果保護の手引き	2022年3月	国家科学技術人材開発院	研究セキュリティ管理、研究進行段階別の研究者による研究セキュリティ管理、セキュリティ管理項目別の研究機関による研究セキュリティ管理についてそれぞれ説明している。
台湾	政府出資の国家基幹科学技術研究プログラム安全管理運営マニュアル【国家安全委員会作成文書】	2019年1月（2022 年改定）	国家安全委員会	政府出資の国家基幹科学技術研究プロジェクトが従うべき手順を規定。国家安全保障会議の科学技術チームによって運営される。
イスラエル	I2I イノベーション・トゥ・イノベーション：IDF イノベーション・パートナーシップ戦略【イスラエル国防軍作成文書】	2023年8月	イスラエル国防軍	軍事部門の関与により、新技術等から生じる新たな脅威への対応を図る枠組みや方向性の取りまとめ。安全保障状況の変化・変革に強い軍事人材の学術的・専門的・実践的育成や、研究機関・民間等との関係強化・情報共有等。

5.2 研究インテグリティについての国内ヒアリングの実施

国内の大学・研究機関における、研究インテグリティの確保、特に、研究の国際化やオープン化に伴う新たなリスクに対する対応のための取組等の現状や課題を把握し、今後の研究インテグリティの確保のための取組に役立てていくことを目的としてヒアリングを実施した。

ヒアリングは国内の大学・国立研究開発法人 10 機関（7 大学、3 国立研究開発法人）を対象として、2023 年 11～12 月に、約 1 時間半の時間でオンラインで実施した。大学・国立研究開発法人の研究インテグリティあるいは関連業務を担当する部署の職員等（担当部署の部課長等）からの対応を得た。ヒアリングは対象機関や担当者の名称は公開しないことを前提に実施し、ヒアリング対象機関は、ヒアリング結果についての報告書原稿内容の確認を、公開の適切性等の観点からお願いした。

大学については、機関種別（国立、公立、私立）、研究大学かどうか、規模（教員数、科研費獲得金額）、総合大学か単科大学か、の観点から選定した。

A 大学：大規模国立大学。研究大学。
B 大学：大規模国立大学。研究大学。
C 大学：中規模国立大学。
D 大学：公立の総合大学。
E 大学：私立の総合大学。
F 大学：私立の総合大学。
G 大学：私立の工業大学。

国立研究開発法人については、主要な機関から 3 法人を選定した。

質問内容は、1）研究インテグリティ確保のための規程整備、2）組織体制・運用方法（開示情報のリスク判断、リスクへの対応プロセス、既存の組織体制との関係）、3）運営トップレベルの関与、4）研修・教育、5）他機関との連携状況と、6）政府・資金配分機関への要望・提案の 6 項目について伺った。1)～5)の項目については取組等の現状と課題について伺った。

〇規程整備の内容及び運用方法について

ヒアリングした大学・国立研究開発法人では、利益相反管理、安全保障貿易管理に関する規程等を既に策定している。一部の大学・国立研究開発法人では、研究インテグリティについての規程についても 2022 年、2023 年に制定してきている。規程は基本的には文部科学省から示されたモデル規程を参考に策定されている。これらの枠組みは、政府からの方針に対応し、研究活動、特に国際的な研究活動の拡大に応じた新たなリスクを管理するための積極的な対策として策定されることが多い。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

- 大学間の比較：国立大学（A、B、C）では既に研究インテグリティについての規程を整備している。公立大学 D、私立大学（E、F、G）では、既に制定している利益相反規程、安全保障輸出管理規程の枠組みのもとで、必要な情報共有を図るなど運用面での対応をしており、研究インテグリティに関する規程の整備については他大学の動向等を注視しつつ検討しているのが現状である。
- 研究型大学とそれ以外の大学の比較：研究大学（A と B）は、研究活動のレベルの高さ、国際的研究活動の大きさを反映して、研究インテグリティとセキュリティに対して、より包括的で詳細なアプローチをとっている。それ以外の大学では、研究インテグリティに関連する対応に配分可能な資源への制限があり、各々の研究活動等を反映した合理的な対応について、他大学等の取組の情報を集めて、模索している段階と考えられる。
- 大学と国立研究開発法人の比較：国立研究開発法人(A、B、C)では、国立大学と同様に研究インテグリティについての規程の整備が既に行われており、政府とは緊密な調整が図られており、政府の方針への応答は早いとみられる。

規程整備の上での課題としては、規程に組織整備の内容（委員会の設置）、担当する事務局の部署を文言として書き込むことが必要となるため、それに関連する調整が必要との

ことであった。また、後述の組織整備とも関連するが、規程を整備した後に、いかにその体制を運用するか、既存の委員会と新設の委員会との調整をいかに図るかといった課題が当然ある。

〇組織体制及び運用方法について

ヒアリングした大学・国立研究開発法人では、既に利益相反、安全保障輸出管理について検討する委員会、事務組織は設置されていた。一部の大学・国立研究開発法人ではそれに加えて、研究インテグリティに特化した問題を扱う委員会として、研究インテグリティ・マネジメント委員会（理事、部局長等をメンバーとする）、研究インテグリティ専門委員会（事務組織の担当課長等をメンバーとする）が新たに 2022 年、2023 年に設置された。研究インテグリティ担当室を設置した大学もあった。これらの委員会は、ポリシーの施行、助言的役割等のために、適宜開催され討議等が行われている。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

・国立大学で、特に大規模な研究大学（大学 A と大学 B）では、その広範な研究活動や複雑な問題にさらされる可能性が高いことを反映し、専門の「研究インテグリティ・マネジメント室」の設置、「研究インテグリティ・マネジメント委員会」の設置など、より専門特化した組織を持つ傾向がある。対照的に、中規模大学および私立大学（D、E、F、G 大学）は、研究インテグリティ業務を既存の組織体制（利益相反、安全保障輸出管理の委員会等）に組み込みし、担当部門間の調整を促進し、アドバイザーの役割の重要性を強調しながら、小規模に運営されている場合が多い。

・国立研究開発法人（A、B、C）では、研究インテグリティに包括的に取り組むために、さまざまな管理部門を統合することに強い重点を置いている。これらの国立研究開発法人は、大学が部局での対応の比重が大きいことと比較すると、より本部レベルで中央集権的なアプローチをとっているように見えるが、より機密性の高い研究を含んでいる可能性があるためとみられる。

全体として、どの大学・国立研究開発法人も研究インテグリティを確保するための取組をする必要性があるとの問題意識はあるものの、政府との距離、研究活動の国際化・オープン化の程度や大きさを反映して、新たなリスクへの対応のための取組の導入のスピードには差が出ている。

<u>開示情報に基づくリスク判断の方法、関連する課題</u>

ヒアリング対象の大学・国立研究開発法人においては、利益相反、機密技術の輸出管理、経済安全保障、研究の潜在的な軍事利用などに関連するリスクを積極的に管理している。そのアプローチは、研究者の厳格な自己開示プロセス、共同研究や提携の評価、特に外国企業との提携、外部からの影響から研究インテグリティを守ることなどが含まれる。情報の流れや技術的漏洩を包括的に管理する必要性が認識されており、多くの大学・国立研究開発法人が、開示された情報の正確性や適切性を検証する方法について模索している。

各機関とも、国際的な共同研究が増加し、機密性の高い技術が急速に開発されるなど、急速に進化する研究環境の中で、徹底的かつ効率的なリスク評価という課題に取り組んでいる。研究インテグリティの維持、セキュリティの確保、オープンで協力的な学術環境の育成のバランスは、共通のテーマである。

各機関で浮き彫りになっている課題には、研究者から詳細な個人情報や兼業等の情報を入手して確認することの難しさ、海外の複雑な資金提供や共同研究の構造を理解すること、開かれた学術的共同研究とセキュリティのバランスを維持することなどがある。

大学・国立研究開発法人の類型別には以下のような違いがみられた。

・大規模で研究志向の国立大学（大学 A、大学 B）では、安全保障輸出管理や利益相反、研究インテグリティに焦点を当てた専門部署や委員会を設置するなど、リスク管理に対する体系的かつ包括的なアプローチを示している。中規模および小規模の機関、特に私立大学（C、E、F、G）は、個々の部局がリスク評価と管理において重要な役割を果たしている傾向があり、また、専門知識を有する外部アドバイザーからの助言も受けている。
・大学は、特にその教育的使命や、学問の自由と安全保障上の懸念とのバランスをとる必要性に照らして、利益相反等の管理を重視する傾向がある。国立研究開発法人（A、B、C）は、国家安全保障規制や輸出管理法の遵守に強い重点を置いているが、これは政府資金による研究や技術開発との関係がより緊密である可能性があることを反映しているとみられる。

<u>リスクが懸念される場合の対応プロセス</u>

ヒアリング対象とした大学・国立研究開発法人では、輸出規制の事前チェック、利益相反や安全保障輸出管理に関するアドバイザーとの協議、複雑なケースを審議・決定するための専門委員会の設置など、リスクを管理するためのさまざまな戦略を採用している。規程上の研究インテグリティとセキュリティに関する懸念やリスクに対処するための手順と体制を定めている。これには、様々な委員会、管理室、専門的な助言を行う外部組織やアドバイザーの関与が含まれる。ただし、多くの大学・研究機関では実際の対応プロセスについてはこれから学習している段階とみられる。

各機関は、新たなリスクに対応する態勢を整えており、リスクの定期的な監視・評価や、最新の規制・ガイドラインに基づくリスク管理戦略の更新を行う仕組みを持つ機関もある。多くの機関がアドバイザーとの協力関係を築いている。

<u>既存の組織体制との関係</u>

どの大学・国立研究開発法人も、安全保障輸出管理、利益相反への対応など、既存の組織構造（委員会や事務組織）の中での調整や、それら組織構造との調整を高めることが研究インテグリティの確保のためには重要であるとしている。それは、新たに研究インテグリティに関連する委員会や事務組織を設置している大学・国立研究開発法人でも、まだその途上にある大学においても同様とみられる。多くの大学・国立研究開発法人は、様々な

部門間の緊密な連携の必要性を強調し、研究活動の国際化・オープン化の高まりに応じて発生する新たなリスクが、そのような緊密な連携を通じて見いだされ、対処することを目指している。

〇運営トップレベルの関与について

ヒアリングした大学・国立研究開発法人の多くは、トップレベルの管理職（理事長、学長、理事など）が、研究インテグリティ確保のための体制作り（規程整備や委員会等の体制整備）やその運営、取組の実施に関与することを重視している。

大学や国立研究開発法人では、研究インテグリティを担当する副学長や特定の管理職をガバナンスに組み込んでいる（担当理事の任命、委員会の委員長への任命など)。この体制は、内部の事務組織や、外部の専門家を含む様々な委員会によって支えられていることが多い。

また、多くの大学・国立研究開発法人では、研究インテグリティに関する懸念が発生した際に迅速に対処するため、担当事務組織から担当理事に相談するプロセスが決まっており、定期的なトップマネジメントとの協議も含まれる。

多くの大学・国立研究開発法人では、ガバナンス体制のさらなる強化に取り組んでおり、研究インテグリティとセキュリティ対策の強化に継続的に取り組んでいることがうかがえる。

ただし、一部の私立大学では、研究インテグリティに積極的に取り組んでいるものの、研究インテグリティの確保のための組織体制や業務プロセスはまだ初期段階にあり、模索しており、具体的な方針の決定や日常業務に対して経営トップの関与の度合いを決めていないところもある。

〇研修・教育、セミナーの実施について

研究インテグリティに関する教育・研修としては、e ラーニングプラットフォームの導入、情報資料の作成と配布、セミナーや研修会の開催などが挙げられる。大学や国立研究開発法人はこれまでも、利益相反、安全保障輸出管理や研究倫理に関する継続的な教育に積極的に取り組んできており、これら業務を効果的に実施するには、教員・研究者・事務職員の包括的な理解の必要性が強調されている。

研究インテグリティに関する複雑な概念を多忙な教職員や研究者に対して具体的に簡潔に伝えることの難しさ、多様で多忙な教職員が確実に理解することの難しさといった課題も認識されている。

どの大学・国立研究開発法人も研究インテグリティとセキュリティ対策の重要性を認識しているが、その教育・研修の戦略と実施規模は、利用可能な資源によっても大きく異なる。大規模な国立大学や研究大学（A、B）では、e ラーニングプラットフォームや詳細なケーススタディプレゼンテーションなど、幅広い教育ツールを取り入れ、より体系的かつ広範なプログラムを実施する傾向がある。これらの大学は、継続的な教育や、研究インテグリティを他のコンプライアンス分野と統合することに重点を置いている。

中規模および公立大学（C、D）も研究インテグリティを重視しているが、リソースが限られているため、セミナーや外部リソースへの依存度が高い。技術系大学を含む私立大学（E、F、G）は、安全保障輸出管理など特定の分野に重点を置く大学や、包括的な研究インテグリティ研修プログラムの計画段階にある大学など、多様なアプローチを示している。

〇他大学・研究機関との連携について

7 大学（A～G）、3 国立研究開発法人（A～C）へのインタビューから、研究のインテグリティ確保のための取組に関連した、他大学や研究機関との連携については、多様なアプローチや考え方があることが明らかになった。

A 大学は、国立研究大学のトップランナーとして、国内大学の中でリーダーシップを取ることを目指し、情報交換や取組に積極的である。B 大学は定期的な交流会を行っているが、C 大学は研究インテグリティを学内の問題と考えており、外部との連携は限定的である。公立大学の D 大学は、アドバイザー的役割やコンソーシアムへの参加を通じて連携に力を入れているが、私立の E 大学と F 大学は、地域のネットワークに参加し、問題解決を共有している。

国立研究開発法人 A、B、C では、国立研究開発法人協議会（国研協）のタスクフォースでの情報共有や政府への要望の明確化などを図っており、同協議会を情報共有プラットフォームとして活用してきている。

〇政府・資金配分機関への要望・提案について

ヒアリングでは、大学と国立研究開発法人ともに、政府や資金配分機関への要望や提案があった。特に国立研究開発法人からは、研究インテグリティや情報セキュリティの確保に対する具体的な方針の設定、安定的な予算の確保、共通システムや研修構築への支援を求める声が多く聞かれた。大学からも似たような要望が出されているが、国立研究開発法人の方が具体的な要望が多かった。

研究インテグリティの確保のための取組の重要性についての理解は示されたものの、どの大学・国立研究開発法人においてもそのために要するリソースと熟練した人材の確保については、一貫した懸念が示された。特に、大規模な大学・国立研究開発法人であれば、専門部署や職員をこれらの問題に充てることができるが、小規模な大学では予算やマンパワーが限られているため、大きな苦戦を強いられているとの認識があった。研究インテグリティやセキュリティに関する業務が複雑化し、事務レベルでも法律や専門的な知識が必要になっていること、また、専門的な知識を持ったスタッフを配置する必要性について言及している。

政府や資金配分機関に対しては、より明確なガイドラインと、より実質的な支援を求めている。現在の政府からの説明会や意見交換会などの開催やガイドライン制定は評価されているが、より直接的な支援、行動のための明確な枠組み、政府各部門からの合理的なコミュニケーションの必要性を表明している。特に、私立大学からは、研究インテグリティ

確保のための取組としては、最低限何をすることが必要なのかを示してもらった方が対応しやすいとの声があった。
国立研究開発法人からは、研究インテグリティとセキュリティの一体的な性質により重点を置き、強固なセキュリティインフラのための安定した資金と、政府や資金配分機関との協力のための明確なガイドラインの重要性を強調している。

5.3　研究インテグ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・国立研究所等で研究インテグリティに関連する業務に従事している者）を交えて意見交換会を 2023 年 10～11 月に 3 回開催した。

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・仙台・大阪の 3 か所で開催した。

グループ討議は参加者が 6～8 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。

各意見交換会への参加者人数（主催者・事務局と講演者を除く）は、第 1 回は 43 人、第 2 回は 21 人、第 3 回は 42 人が参加した。第 1 回は国立研究開発法人からの参加者が 14 人いたが、第 2 回と第 3 回は大学関係者のみの参加となった。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（東京開催）は関東から、第 2 回（仙台開催）は東北から、第 3 回（大阪開催）は近畿からの参加者が多かった。ただし、今年度開催なかった北海道、中部、中国、四国、九州・沖縄地方からの参加者もみられ、ほぼ全国からの参加者があったと言えるだろう。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、担当の教員が殆どであった。

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）内閣府からの説明について（参考になったかどうか（選択肢）、自由意見・コメント）、
2）警察からの説明について（参考になったかどうか（選択肢）、自由意見・コメント）、
3）有識者の講演について（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）

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では、5～6 割の参加者は「とても参考になった」、約 4～5 割は「参考になった」と考えていることが分かった。9 割以上の参加者は「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。

また、内閣府からの説明、有識者の講演、グループ討議、意見交換会全体については、それぞれ概要以下の自由記入の意見があった。なお、以下は参考になる意見等を紹介している

が、自由記入で表明された意見等は必ずしも常に多数意見を反映しているとは言えないことには留意が必要である。

内閣府からの講演について

政府の研究インテグリティ関連の政策についての理解が深まったとの回答があった一方で、研究インテグリティに関して、より明確なガイダンスと具体的な対策を求める声があった。研究インテグリティとセキュリティの重要性は認識されているものの、これらの基準を効果的に実施・維持するためには、より詳細で実践的なガイダンスやリソースが必要であることとの意見や、何が必須で、どのような対策をとるべきかについて、より明確なコミュニケーションが必要であるとの回答があった。具体的で実行可能なガイドラインがないため、大学・研究機関間で一貫性のない適用がなされる可能性があるとの指摘もあった。

また、研究インテグリティの定義をより明確にし、経済的セキュリティと研究インテグリティの関係を概説する、より包括的な資料を求める声があった。

大学職員からは、より明確な運営ガイドラインの必要性と、研究のインテグリティ維持における大学職員の役割の理解を深める必要性を強調し、研究インテグリティを効果的に管理するための具体的な情報やリソースの不足は、共通の懸念事項として示された。また、職員や教員の意識と理解を深めることの重要性が指摘された。

有識者の講演について

有識者からの講演は 3 回異なる大学教員からなされたが、参加者から共通して指摘された意見としては、第 1 に、リスク評価に関するケーススタディや方法論の共有・蓄積を強く望んでいるということがあった。参加者は、研究インテグリティ確保のための様々な懸念事項が様々な大学・研究機関でどのように対処されているか、具体的かつ実践的な事例に強い関心を示した。第 2 に、参加者からは、研究インテグリティ確保のための先進的な取組において、どのような組織構造や施策を採用しているのかについてより詳細な情報の必要性が示された。第 3 に、すべての大学・研究機関で大規模大学で採用されたシステムを見習うことの現実性について懸念が示す声があった。小規模でリソースに制限のある大学においてどのように体制構築を図るかについての意見があった。

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、まず、第 1 に、時間的制約がある中でいかに有意義な情報交換を図るかという点についての指摘があった。参加者からは、グループ討論を高く評価しながらも、より深い議論を望んでいたとの指摘や、モデレータが主導する、より構造化された集中的なディスカッションへの要望も示された。参加者からは、ディスカッションの時間をもっと取りたい、他大学とは異なる視点や実践をもっと学びたい、といった声も聞かれた。第 2 に、グループ討議を通じて有効な情報共有が行われたとの指摘があった。グループ討議では、さまざまな大学・研究機関の間で情報、課題、ベストプラクティスを共有する貴重な機会であったとの意見や、大学や研究機関を超えた協力の重要性を強

調する意見があった。第 3 に、大学・研究機関のリソースの格差についての指摘である。大学・研究機関によって資源や経営支援のレベルが異なることが指摘され、また、潤沢な資金を持つ大学の参加者は、予算の制約や事務的支援に悩む他の大学と比べて、自分たちが有利な立場にあることを認識する意見があった。第 4 に、グループ討議で少人数で議論することを通じて、関係者の間でネットワーク作りに役だったとの指摘があった。

意見交換会全体について

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。参加者は、グループディスカッションや異なる機関から学ぶ機会を高く評価した。今後も今年度実施した意見交換会のような継続的な対話と支援が強く求められた。ネットワーキングや継続的な議論の場の必要性についての指摘があった。全国で、このような議論を継続し、継続的な対話と支援のためのネットワークを構築することに強い関心が示され、ベストプラクティスや課題を共有するための継続的なプラットフォームの必要性の指摘があった。

また、会議では、研究インテグリティについての理解度や実施レベルが様々であることが浮き彫りになり、特に小規模でリソースが限られている大学からの参加者からは、より体系的なガイダンスや支援が必要であるとの指摘が多かった。研究インテグリティに取り組むための十分なスタッフやリソースを確保することの難しさを強調し、小規模な機関への支援を求める声が目立った。多くの参加者、特に私立大学の参加者からは、リソースの配分や具体的で実行可能なステップの必要性など、ガイドラインを実施するための実際的な側面についての関心の声があがった。

全体として、政府からのより明確なガイドラインや支援を求める声があった。研究インテグリティの定義をより明確にする必要性を強調し、研究インテグリティに関連する問題の具体的取り扱いについて、詳細なガイダンスを求める声があった。

参考文献

全般

D'Hoogle, Ingrid and Lammertink, Jonas (2022). *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden Asia Centre. 2022.

OECD. *Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers. June 2022 No. 130.

国立研究開発法人科学技術振興機構　研究開発戦略センター「オープン化、国際化する研究におけるインテグリティ 2022 ―我が国研究コミュニティにおける取組の充実に向けて―」CRDS-FY2022-RR-01. 2022 年 5 月.

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」内閣府委託調査. 2023 年 3 月.

米国関係

Department of Defense. *Countering Unwanted Foreign Influence in Department-funded Research at Institutions of Higher Education*. June 29, 2023.

House Select Committee on the Strategic Competition between the United States and the Chinese Communist Party. *Reset, Prevent, Build: A Strategy to Win America's Economic Competition with the Chinese Communist Party*. 2023.

National Academies. *Foreign-Funded Language and Culture Institutes at U.S. Institutions of Higher Education: Practices to Assess and Mitigate Risk*. 2023.

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 and Technology Council. Joint Committee on the Research Environment. Subcommittee on Research Security. *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*. January 2021.

National Science Foundation. NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization

National Science Foundation. *NSF Guidelines for Research Security Analytics*. June 2023.

Office of Science and Technology Policy. Request for Information; NSPM 33 Research Security Programs Standard Requirement. Federal Register / Vol. 88, No. 44 / Tuesday, March 7, 2023 / Notices.

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

英国関係

GOV.UK website, “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>

GOV.UK website, “Research Collaboration Advice Team: progress made from 2022 to 2023” <https://www.gov.uk/government/publications/research-collaboration-advice-team-progress-made-from-2022-to-2023/research-collaboration-advice-team-progress-made-from-2022-to-2023>

NPSA Trusted Research website, “Trusted Research Guidance for Academia” <https://www.npsa.gov.uk/trusted-research-academia>

UKRI, “Trusted Research and Innovation Principles,” August 2021.

UUK, “Managing risks in Internationalisation: Security related issues,” October 2020.

UUK website, “Security and risk: how universities can protect their research and people” <https://www.universitiesuk.ac.uk/topics/funding-finance-and-operations/security-and-risk-how-universities-can>

YouTube: Cabinet Office (Trusted Research for Academia Guidance - Risk Case Studies) <https://www.youtube.com/playlist?list=PLVnRbAyuOGuqkW4hE0nnhya-SOcmq7V8T>

豪州関係

Australian Government. *Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report: National security risks affecting the Australian higher education and research sector*. February 2023.

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.

National Health and Medical Research Council. *Australian Code for Responsible Conduct of Research*. 2018.

University Foreign Interference Taskforce Transnational Education Working Group. *Guidance Note on Due Diligence*. June 2023.

カナダ関係

Government of Canada. *National Security Guidelines for Research Partnerships*. 2021.

Government of Canada.” The National Security Guidelines for Research Partnerships’ Risk Assessment Form”

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.

Natural Sciences and Engineering Research Council of Canada. “NSERC 2030: Discovery. Innovation. Inclusion.”

Public Safety Canada. *Departmental Results Report 2021-22.*

欧州連合関係

European Commission. Directorate-General for Research and Innovation. *Tackling R&I Foreign Interference. Staff Working Document* (2022/1)

European Commission. *Horizon Europe Program Guide*. Version 2. 11 April 2022.

European Commission. “Joint Communication to the European Parliament, the European Council and the Council on European Economic Security Strategy.” Brussels, 20.6.2023. JOIN(2023) 20 final.

European Commission. “Proposal for a COUNCIL RECOMMENDATION on enhancing research security.” Brussels, 24.1.2024. COM(2024) 26 final.2024/0012 (NLE).

European Commission. *Communication from the Commission to the European Parliament and the Council Advancing European Economic Security: An Introduction to Five New Initiatives*. Brussels, 24.1.2024. Com(2024) 22 Final.

フランス関係

ANR. "ANR Plan d’action 2024". juillet 2023, mise à jour septembre 2024

D21E, MESR. "Guide de l’intelligence économique pour la recherche". 2011

Gouvernement français - Légifrance. "Décret n° 2011-1425 du 2 novembre 2011 portant application de l'article 413-7 du code pénal et relatif à la protection du potentiel scientifique et technique de la nation". novembre 2011

Gouvernement français - Légifrance. "Arrêté du 3 juillet 2012 relatif à la protection du potentiel scientifique et technique de la nation". juillet 2012

Gouvernement français - Légifrance. "Circulaire interministérielle du 7 novembre 2012 de mise en oeuvre du dispositif de protection du potentiel scientifique et technique de la

nation". novembre 2012

Gouvernement français - Légifrance. "Article D123-19, Version en vigueur depuis le 18 juin 2015, Modifié par DÉCRET n°2015-668 du 15 juin 2015 - art. 4". juin 2015

Leiden Asia Centre. "How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology". November 2022

Sénat. "Mieux protéger notre patrimoine scientifique et nos libertés académiques - Rapport d'information n° 873 (2020-2021)". septembre 2021

SGDSN. "Dispositif de protection du potentiel scientifique et technique de la nation (présentation)". Publié sur le web - août 2018

Université de Sorbonne. "Comment protéger notre potentiel scientifique et technique ?". Publié sur le web - novembre 2023

ドイツ関係

BAFA. "Export Control in Academia Manual". 2019

BfV. "BfV annual report 2020 - Brief summary 2020 Report on the Protection of the Constitution (Facts and Trends)". June 2021

BMBF - WISKOS, MPG. "Risiken für den deutschen Forschungsstandort". Published on the Web：2018

DAAD. "Daten & Analysen zum Hochschul- und Wissenschaftsstandort, DAAD-BILDUNGSSYSTEMANALYSE China". 2017

DAAD - KIWi. "No red lines - science cooperation under complex framework conditions". 2020

DFG, Deutsche Akademie der Naturforscher Leopoldina e.V. "Scientific Freedom and Scientific Responsibility：Recommendations for Handling Security-Relevant Research". 2014

DLR. "Annotated collection of guidance for secure and successful international R&I cooperation". updated：2022

DVCS. "Handlungsempfehlungen der Deutschen Vereinigung für Chinastudien e.V. zum Umgang deutscher akademischer Institutionen mit der Volksrepublik China（英：Guidance by the German Association for Chinese Studies on the Interaction of German Academic Institutions with the People's Republic of China）". 2018

HRK. "Guidelines and standards in international university cooperation". April 2020

HRK. "Guiding Questions on University Cooperation with the People's Republic of China". 2020

Leiden Asia Centre. "How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology". November 2022

Mehmet Evrim Altin. "Internationalization of the German Higher Education System New Player in the Market - Athens Journal of Education - Volume 6, Issue 3 – Pages 237-256". August 2019

MPG. "GUIDELINES for the development of international collaborations of the Max-Planck-Gesellschaft". March 2021

久保田隆. "WISKOS - ドイツの経済・産業スパイ研究プロジェクト". 2021 年 6 月

スウェーデン関係

European Commission. *Commission Reviews Relations with China, Proposes 10 Actions*. 12 March 2019.

Government Communication. *Human Rights, Democracy and the Principles of Rule of Law in Swedish Foreign Policy*. 2016

Government Communication. *Approach to Matters Relating to China*. 2019.

Shih, T., Gaunt, A. & Östlund, S. *Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration*. Stockholm: STINT, 2020.

Shih, Tommy and Forsberg, Erik. "Origins, motives, and challenges in Western–Chinese research collaborations amid recent geopolitical tensions: Findings from Swedish–Chinese research collaborations." *Higher Education*, 85, pp. 651–667. 2023.

STINT (a). *Academic Collaboration Sweden-China*. May 2018.

STINT (b). *Report to the Government on How Sweden Should Cooperate with China*. 2018.

STINT. *Recommendation to Higher Education Institutes on How to Work with Responsible Internationalisation*. May 2022.

SUHF (2023). *Global Responsible Engagement: Checklist*. 11 April 2023.

Tardell, Miriam. "Swedish experiences of research collaboration with China: Challenges and the way forward: A report from the Swedish National China Centre." *Swedish National China Centre*. 2021.

Vie, Knut Jørgen. "Empowering the research community to investigate misconduct and promote research integrity and ethics: New regulation in Scandinavia." *Science and Engineering Ethics*, 28: 59. 2022.

北村豊.「宿泊騒動が中国とスウェーデンの外交問題に」『日経ビジネス』. 2018 年 9 月 28 日.

ノルウェー関係

Forsby, Andreas. "Falling out of favor: How China lost the Nordic countries." *The Diplomat*. June 24, 2022.

Jakobsen, Siw Ellen. "Norwegian academics must be more vigilant against espionage, says intelligence expert: Universities need to improve their background checks on visiting researchers in Norway." *Sciencenorway no*. 19 Nov. 2022.

Myklebust, Jan Petter. "Universities say new rules will hurt international research." *University World News*. 18 July 2022.

National Committee for Research Ethics in the Social Sciences and the Humanities (NESH). *Guidelines for Research Ethics in the Social Sciences and the Humanities, 5th*

edition. 2021.

Norwegian Ministry of Foreign Affairs. *Recommendation for Norwegian Exports of Defence-Related Products in 2020, Export Control and International Non-Proliferation Cooperation*. 2021.

Norwegian Police Security Service (PST). *National Threat Assessment 202*3. 2023.

Offerdal, Kristine et al. *Guidelines and Tools for Responsible International: Knowledge Cooperation*. Norwegian Directorate for Higher Education and Skills. 2023.

Svensgård, Torbjørn. "Capabilities made in Norway: Norwegian defence industry delivers world-class defence equipment to the world." *European Security & Defence*. 14 October 2022.

フィンランド関係

D'Hoogle, Ingrid and Lammertink, Jonas (2022). *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Leiden Asia Centre. 2022.

European Commission. *Commission Reviews Relations with China, Proposes 10 Actions*. 12 March 2019.

Karppanen, Anton. "How Will Finland-China Relations Change in a New Security. Environment?". *CHOICE (China Observers in Central and Eastern Europe)*. August 9, 2022.

Ministry of Education and Culture. *Recommendations for Academic Cooperation with. China*. 2022.

Ministry of Foreign Affairs. *Governmental Action Plan on China*. 2021.

Myklebust, Jan Petter. "Is university autonomy at risk?" *University World News*. 06 June 2022.

Pillai, Helmi. "A new era of Finnish foreign policy begins." *Centre for European Reform*. 19 December 2022.

YLE NEWS. *Intelligence Service Concerned about Espionage at Finnish Universities*. 5.11.2021.

デンマーク関係

Danish Security and Intelligence Service. (2021) "Is your research at risk?", May 2021.

Uddannelses- og Forskningsministeriet. (2014) "Danish Code of Conduct for Research Integrity", November 2014.

Uddannelses- og Forskningsministeriet. (2022) "Afrapportering: Udvalg om retningslinjer for internationalt forsknings- og innovationssamarbejde", May 2022.

オランダ関係

AIVD, MIVD and NCTV, “Threat Assessment State-sponsored Actors 2,” November 2022.

Association of Cooperating Universities in the Netherland, “Framework Knowledge Security Dutch Universities,” 2021.

Government of the Netherland website, “Contact Point for Knowledge Security” <https://english.loketkennisveiligheid.nl/>

NOW website, “Knowledge security” < https://www.nwo.nl/en/knowledge-security>

Letter from the Ministers of Education, Culture and Science, of Economic Affairs and Climate and of Justice and Security to the Chairman of the House of Representatives of the States General (31 January 2022)< https://zoek.officielebekendmakingen.nl/kst-31288-948.html>

Letter to Parliament on measures to ensure knowledge safety in higher education and science (27-11-2020) <https://open.overheid.nl/documenten/ronl-2d5d6a09-f681-4edc-90a6-fbefe84f6da2/pdf>

Letter from the Minister of Justice and Security to the President of the House of Representatives of the States General, February 2021. <https://zoek.officielebekendmakingen.nl/kst-30821-125.html>

チェコ共和国関係

Ministry of Defence of the Czech Republic. *National Strategy for Countering Hybrid Interference*. 2021.

Ministry of the Interior of the Czech Republic, Security Policy Department, and Centre Against Terrorism and Hybrid Threats. *Counter Foreign Interference Manual for the Czech Academic Sector*. 2022.

ニュージーランド関係

Protective Security Requirements. (2023) “Trusted Research - Guidance for Institutions and Researchers”, August 2023.

Universities New Zealand. (2022) “TRUSTED RESEARCH - Protective Security Requirements – Guide for Senior University Leaders in Aotearoa New Zealand”, September 2022.

JST/CRDS. (2018) “ニュージーランドの研究開発システムの概要”, 2018 年 12 月 24 日.

斉藤徹史・森 直子. (2016) “ニュージーランドの法と政策研究序説－民営化と中小企業政策研究を中心に－”, 東北公益文科大学総合研究論集第 31 号, 2016 年 12 月 20 日.

PwC あらた有限責任監査法人. (2022) “研究インテグリティ（Research Integrity）に係る調査・分析報告書”, 2022 年 3 月.

韓国関係

科学技術情報通信部（Ministry of Science and ICT (MSIT;과학기술정보통신부)等「국가연구개발사업 보안대책」（国家研究開発事業におけるセキュリティ対策規則」）2023.

科学技術情報通信部 研究制度革新課、KISTEP（韓国科学技術企画評価院）制度革新センター.「국제연구협력 시 연구자산+유출 방지를 위한 주요국+정책사례집」（国際研究協力時の研究資産流出防止のための主要国の政策事例集））2023 年 6 月.

선인경(2023), G7, '디리스킹(de-risking)' 강조한 연구안보 위험관리방안 제시. STEPI 보고서. 과학기술정책 Brief. 2023.6.16（ソンインギョン(2023)、G7、「脱リスク(de-risking)」を強調した研究安全保障リスク管理方案を提示。STEPI「科学技術政策 Brief」）

KIRD（국가과학기술인력개발원（国家科学技術人材開発院））「연구보안 관리 및 연구성과보호의 길라잡이 : 연구보안의 이해」（「研究セキュリティ管理及び研究成果保護の手引き：研究セキュリティの理解」）2022 年 3 月

台湾関係

國家科學及技術委員會 112 年 1 月「政府資助國家核心科技研究計畫安全管制作業手冊」（「国家基幹科学技術研究プログラム安全管理運用マニュアル」（国家安全委員会、2019 年、更新 2022 年））

国家科学技術委員会「公布國家核心關鍵技術加強保護營業秘密」2023 年 12 月 5 日」

湯野基生「台湾：国家安全法の改正」『外国の立法』296（2023. 6）. 国立国会図書館調査及び立法考査局.

イスラエル関係

Arbell, Dan et al. "What do Israel's China ties mean for its relationship with the US?" *International Institute for Strategic Studies website*. May 8, 2019.

Babb, Casey. "Proceed with Caution: Israeli Research Collaboration with China" *INSS website.* No. 1645, September 20, 2022.

Combat Methods & Innovation Division (CMI), IDF. "I2I Innovation to Innovation: IDF's Innovation Partnership Strategy" LinkedIn. August 2023.

Egozi, Arie. "White House pressuring Israel to cut research ties with China over dual-use concerns" *Breaking Defense*. September 29, 2022.

Fridman, Ofer. "Defining Foreign Influence and Interference" *INSS website*. January, 2024.

Granot, Ofer. "Tightened Global Enforcement of US Export Controls: The Significance for Israel" *INSS website.* No. 1738. June 14, 2023.

Harkov, Lahav. "Israel agrees to update US about China trade to avoid tension" *Jerusalem Post*. January 3, 2022.

INSS ISRAEL. "Research Security Amidst Great Power Competition." *YouTube*.

Israel National Cyber Directorate. "The Israel National Cyber Directorate: Iran is a main

cyber threat on the Middle East" June 26, 2019.

Lev, Ori. "Regulating dual-use research: Lessons from Israel and the United States" *Journal of Biosafety and Biosecurity* 2019 Vol.1 (2) 80-85.

Melman, Yosshi. "China Is Spying On Israel to Steal U.S. Secrets" *Foreign Policy*. March 24, 2019.

Ministry of Economy and Industry. "Export Control Agency, Ministry of Economy and Industry"

Ministry of Finance. "The Advisory Committee for Evaluating National Security Aspects of Foreign Investments"

Ministry of Innovation, Science and Technology. "Israel's Policy on Artificial Intelligence Regulation and Ethics" December 17, 2023.

""Schanzer, Jonathan et al. "Wary of China, Israel Toughens Screening of Foreign Investments" *Foundation for Defense of Democracies website*. November 17, 2022.

Schanzer, Jonathan et al. "Aligning U.S.-Israeli Cooperation on Technology Issues and China" *Center for a New American Security website*. March 9, 2022.

Sobelman, Ariel et al. "National Technology Plan in Israel" *INSS website.* January 2024.

The Authority for Research and Development, The Hebrew University of Jerusalem. "Research Ethics"

The White House, "Fact Sheet: U.S.-Israel Strategic High-Level Dialogue on Technology," September 30, 2022.

Weizmann Institute of Science. "Code of Ethical Conduct"

Wilner, Alex et al. "Research at risk: Global challenges, international perspectives, and Canadian solutions" *International Journal*. 2022, Vol.77 (1) 26-50.

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

2024 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）