令和４年度内閣府委託事業

令和４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５年３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４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 —

エグゼクティブ・サマリー vii
第 1 章　調査の概要 1
1.1 調査の目的 1
1.2 調査の内容、方法等 2
1.2.1 海外の取組の調査・整理・分析 2
1.2.2 日本の大学・研究機関等への説明会・意見交換会の企画・運営 2
1.3 調査の体制 3
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 5
2.1 米国 5
2.1.1 研究インテグリティの確保に関する要求と支援 8
(1) 2021 年度までの主な動き 8
(a) NSPM-33（2021 年 1 月 14 日） 8
(b) 米国の科学技術研究事業体のセキュリティとインテグリティを強化するための Recommended Practices（2021 年 1 月 19 日） 18
(c) 2021 年度国防権限法（National Defense Authorization Act: NDAA）（2021 年 1 月） 22
(d) NSPM-33 実施ガイダンス（2022 年 1 月 4 日） 24
(2) 2022 年度の動き 35
(a) The CHIPS and Science Act of 2022 (H.R. 4346)（2022 年 8 月 9 日） 35
(b) OSTP アップデート情報の発表（2022 年 8 月 31 日） 38
(c) 米国アカデミー報告書「米国の技術優位を保護する」（2022 年 9 月 29 日） 39
(d) “Safeguarding Science” Toolkit の発表（2022 年 11 月 15 日） 47
(e) 「研究セキュリティプログラム」のドラフト公表（2023 年 2 月 28 日） 49
2.1.2 資金配分機関における取組 52
(1) 米国科学財団（NSF） 55
(2) 国立衛生研究所（NIH） 61
(3) エネルギー省科学局 66
(4) DARPA 69
2.1.3 主要大学における取組 73
(1) マサチューセッツ工科大学（MIT） 74
(2) ハーバード大学 79
(3) スタンフォード大学 80
(4) カリフォルニア大学バークレー校 82
2.2 英国 84
2.2.1 研究インテグリティの確保に関する要求と支援 84

(1) 研究インテグリティについて英国政府が動き出した背景 84
(2) Trusted Research の目的と要求事項 85
2.2.2 資金配分機関等の取組 95
(1) Universities UK (UUK)の取組 95
(2) UKRI の取組 99
(3) UUK、UKRI 及び CPNI の 3 機関共同の取組 102
2.2.3 主な大学の取組 107
(1) マンチェスター大学の事例 108
(2) 参考情報 1：ストラスクライド大学の事例 109
(3) 参考情報 2：インペリアル・カレッジ・ロンドンの事例 109
2.2.4 研究インテグリティ確保のための支援 110
2.3 オーストラリア 112
2.3.1 概要 112
2.3.2 研究インテグリティの確保のための要求と支援 114
2.3.3 資金配分機関等における取組 115
2.3.4 豪州国立大学（ANU）における取組 117
2.3.5 最近の動向 119
2.4 カナダ 122
2.4.1 全般的状況 122
2.4.2 カナダ政府の取組み 124
2.4.3 カナダにおけるアクター 125
2.4.4 規制側・被規制側の主要アクターの研究セキュリティに関する認識 128
2.4.5 リスクアセスメント 131
2.4.6 地域ごとの懸念への対処 132
2.4.7 大学での取組み 133
(1) マギル大学 133
(2) トロント大学 135
2.5 欧州連合（EU） 137
2.5.1 研究インテグリティの確保に関する要求と支援 137
(1) 「研究・イノベーションにおける外国からの干渉に対応するためのスタッフ作業文書」（2022 年 1 月） 137
(2) Horizon Europe Program Guide Version 2（2022 年 4 月 11 日） 142
第 3 章　研究インテグリティについての説明会の実施 145
3.1 説明会開催の趣旨、目的 145
3.2 説明会の開催内容 145
3.3 説明会への参加状況 147
3.4 説明会への参加者からの感想・質問 147
第 4 章　調査のまとめと注目点 149

4.1 研究インテグリティの確保のための各国・地域の取組の注目点.....149
4.2 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.....153
4.3 研究インテグリティについての説明会の実施から得られた示唆等.....155
参考文献 157

― 図 目 次 ―

図 0-1：第 4 回説明会における事後アンケート結果..... xxviii
図 2-1：資金配分機関の長が開示を求める情報（12 か月以内に方針を作成）.....14
図 2-2：Subcommittee on Research Security（National Science and Technology Council の Joint Committee on the Research Environment に属する）のメンバー.....19
図 2-3：「Safeguarding Science」ポータルサイト.....48
図 2-4：ハーバード大学の研究コンプライアンス関係のポータルサイト.....80
図 2-5：英国における研究インテグリティに関連する政府機関／大学機関／R&D 資金提供機関、これらの機関が発行するガイドライン、関連する法規制、大学・研究機関等 との相互関係.....95
図 2-6：研究公正をめぐる豪州政府・研究機関の組織と仕組み.....121
図 2-7：外国干渉をめぐる豪州政府・研究機関の組織と仕組み.....121
図 2-8：カナダにおける研究セキュリティに関する主要なアクター.....128
図 3-1：第 4 回説明会における事後アンケート結果.....148

― 表 目 次 ―

表 0-1：The CHIPS and Science Act of 2022 の研究セキュリティ関連の規定の概要 xi
表 2-1：近年の研究インテグリティ関連文書（大統領府等）..... 7
表 2-2：近年の研究インテグリティ関連法（米国議会）..... 7
表 2-3：研究セキュリティ・インテグリティ確保のための連邦省庁への要求事項（NSPM-33，セクション 3）..... 9
表 2-4：研究セキュリティのリスクと保護に関する認識の向上に関する事項（NSPM-33，セクション 4 (a)）.....11
表 2-5：情報開示の要件とプロセスの強化に関する事項（NSPM-33, セクション 4 (b)）.....12
表 2-6：アクセス及び参加の制限に関する事項（NSPM-33，セクション 4 (c)）.....14
表 2-7：外国人留学生・研究者の審査に関する事項（NSPM-33，セクション 4 (d)）.....15
表 2-8：情報の共有に関する事項（NSPM-33，セクション 4 (e)）.....16
表 2-9：研究セキュリティ教育に関する事項（NSPM-33，セクション 4 (f)）.....16
表 2-10：リスクの同定と分析に関する事項（NSPM-33，セクション 4 (g)）.....17
表 2-11：国際研究開発協力の促進と保護に関する事項（NSPM-33, セクション 4 (h)）.....17
表 2-12：研究セキュリティとインテグリティを強化するために推奨される実践内容

.....21
表 2-13：2021 年度国防権限法第 223 条「連邦研究開発アワード（awards）への申請書における資金源の開示」 22
表 2-14：「情報開示の要件と標準化」についての実施ガイダンス項目.....26
表 2-15：Tier I と Tier II の参加者の情報開示要件 27
表 2-16：研究開発助成プロセスにおける個人情報・専門家情報の開示のガイダンス 28
表 2-17：プロジェクト情報の開示のガイダンス.....29
表 2-18：「デジタル永続的識別子」についての実施ガイダンス項目 30
表 2-19：「情報開示要件違反への対応」についての実施ガイダンス項目 31
表 2-20：開示要件不順守の研究機関に適用可能な、非強制的な行政措置・救済措置の例.....32
表 2-21：「情報共有」についての実施ガイダンス項目 33
表 2-22：「研究セキュリティプログラム」についての実施ガイダンス項目.....34
表 2-23：The CHIPS and Science Act of 2022 の研究セキュリティ関連の規定の概要 36
表 2-24：米国アカデミーズ報告書「米国の技術優位を保護する」の提言 41
表 2-25：全米アカデミーズ「科学技術安全保障円卓会議」の概要.....46
表 2-26：「経歴」（Biographical Sketch）の情報開示フォームの案.....53
表 2-27：「現在及び未決の（その他）支援」（Current and Pending (Other) Support）の情報開示フォームの案.....54
表 2-28：近年の研究インテグリティ関連文書（米国資金配分機関） 55
表 2-29：NSF における略歴、現在とペンディングの（その他）支援に関連する授与前及び授与後の開示要件 60
表 2-30：NIH におけるシニア/キーパーソンの略歴及びその他の支援に関連する授与前及び授与後の開示要件.....63
表 2-31：NIH Office of Extramural Research に報告された外国からの干渉事例....65
表 2-32：NIH の海外からの干渉事例のレビュー結果.....66
表 2-33：海外からの不当な影響による利益相反や責務相反の可能性を評価するためのリスクに応じた対策：シニア／キーパーソンの情報開示の評価要素（2021 年 12 月） 71
表 2-34：MIT 報告書（2022 年）の提言内容 76
表 2-35：Trusted Research Checklist for Academia、Trusted Research Guidance for Senior Leaders 及び Trusted Research Implementation Guide の 3 文書の概要 87
表 2-36：英国の政府機関、大学協会、資金提供機関等における研究インテグリティに関する取組とその流れ 92
表 2-37：研究セキュリティ、知的財産及び輸出管理に関するチェックリスト 98

表 2-38：「Managing risks in international research and innovation: An overview of higher education sector guidance」の包括的な目標、扱う脅威、大学へのリスク及びリスク緩和策 103
表 2-39：緩和策のチェックリスト 104
表 2-40：カナダ政府の研究セキュリティの強化に関する取組 124
表 2-41：ブリティッシュコロンビア州における外国脅威の例 132
表 2-42：「海外からの干渉」への対応策 139
表 3-1：研究インテグリティについての説明会の開催内容 146

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）が決定されたところである。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早期に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説明会を 4 回実施し、政府と大学・研究機関における研究インテグリティ確保のための取組等について、関係者の間での理解増進と情報共有を図った。

なお、「研究インテグリティ」は研究不正行為等への対応や産学連携による利益相反への対応等にも関わる大きな概念であるが、本調査では、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いることから、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] OECD. *Security in the Global Research Ecosystem*. OECD Science, Technology and Industry Policy Papers. June 2022 No. 130. p.12

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は、米国、英国、オーストラリア、カナダと欧州連合（EU）について調査した。調査の視点としては、特に、対象国・地域における研究インテグリティ確保のための取組（法令・ガイドライン等の制定、政府と大学・研究機関、資金配分機関等における具体的取組を含む）の全体像を俯瞰した際に、1）研究者、大学・研究機関、資金配分機関が研究インテグリティの確保のためにどこから何を要求されているか、2）1）の要求を研究者、大学・研究機関、資金配分機関が実施し、あるいはそれらの実施を確かなものとするためにどこからどのような支援が提供されているか、に注目した。この要求と支援に係るマクロな構図を把握した上で、注目すべき点を整理することを試みている。

なお、本委託調査は特に 2022 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 2021 年度までの動きについても適宜記述することとしている。

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 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ともに、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行われつつあることが大きな特色である。

研究インテグリティについての法令による規制、あるいはガイドライン等とその内容・特色

トランプ前政権は、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、この文書や、その後の米国における取組においては、「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)」という言葉が、「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」に相当する意味を有した用語として使用されてきている[2]。

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」は 2022 年 2 月に終了している。

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」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を含んでいる。

米国議会の動きとしては、2021 年 1 月に 2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）が制定され、その第 223 条で、すべての連邦政府の資金配分機関が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する研究者に対して求めることが義務付けられた。また、2022 年 8 月に CHIPS and Science Act が成立した。この法律（2 部構成）は半導体インセンティブに 5 年間で 527 億ドルを計上（appropriation)、そのうち、先端研究開発に 110 億ドル計上すること等とともに、研究セキュリティに関する規定を含んでおり、「外国人人材採用プログラム」（Foreign Talent Recruitment Programs）についてのガイドライン策定、米国科学財団（National Science Foundation: NSF）に Research Security and Policy Office の設置、研究開発助成の申請時にリスク評価を NSF が実施する権限の付与、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、独立したリスク評価センターを設立すること、等の規定を含んでいる（表 0-1 参照)。

NSPM-33 実施ガイダンスが発出されてから約 7 か月が経過した、2022 年 8 月 31 日に、OSTP は研究セキュリティに関する連邦政府の検討状況の最新情報を発表している。

- 連邦省庁が米国科学技術会議（National Science and Technology Council: NSTC）の研究セキュリティ小委員会（Subcommittee on Research Security: SRS）を通じて、助成金や協力協定を申請する研究者の潜在的な利益相反、責務相反を評価するための情報開示のための「標準データフィールド」と説明書（instruction）を作成する

[2] 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。

ことができたと説明している。これらの共通開示様式は、2022 年 10 月 31 日を期限としてパブリックコメントを募った。

- SRS は、2022 年春に「エンゲージメント・アワー」を訪れた約 40 の組織から意見を聞いた。これらの組織は、全米の公立・私立大学、様々な科学分野を代表する専門組織、研究セキュリティとインテグリティの強化に取り組む非営利組織、特にアジア系アメリカ人、太平洋諸島民、ハワイ先住民のコミュニティを代表する学術・擁護組織など、米国の研究エコシステムに貢献する多様な組織を代表するとのことである。SRS は 2022 年秋に、勧告と学んだ教訓をまとめた公的な報告書を発表する予定である（※2023 年 2 月時点で公表は確認できない）。
- 「デジタル永続的識別子」（Digital Persistent Identifiers: PID）関連の動きとしては、研究者が効果的な PID ポリシーを策定するために必要な法的、政策的、技術的、実施上の考慮事項に対処するため、SRS は最近、OSTP とエネルギー省が主導する省庁間討議を招集した。2022 年 3～5 月に、ほぼ全ての科学研究費助成機関からなるこの PID サブグループは、7 回の会合を開催した。研究者 PID ポリシーの策定と実施に関する情報、ベストプラクティス、教訓が共有され、また、より良い情報を提供するための内部ツールキットを開発している。
- 研究セキュリティプログラムを強化するために、SRS は NSPM-33 実施ガイダンスに詳述されている要件と、2022 年の「CHIPS and Science Act」の規定を検討して、さらに明確にするように努めた。NSPM-33 では、2 年連続で 5000 万ドル以上の連邦科学技術助成金を受ける研究機関に対し、NSPM-33 と関連する実施ガイダンスが定めた基準を満たす「研究セキュリティプログラム」を備えていることを証明するよう、連邦科学資金配分に要求することを指示している。これらの基準には、研究セキュリティプログラムの 4 つの特定分野、すなわち一般的な研究セキュリティ研修、海外渡航セキュリティ、サイバーセキュリティ、輸出セキュリティ（必要に応じて）が含まれる。CHIPS and Science Act は、研究セキュリティプログラム研修受講に関する要件を、高等教育機関又はその他の研究機関の職員として連邦科学技術資金の受給を申請するすべての対象者に拡大している。
- 研究セキュリティプログラムの要件が、研究機関のコスト及び管理負担への影響を最小限に抑えて満たされるようにするため、連邦政府は、2022 年 1 月公表の実施ガイダンスよりもさらに詳細に要件を規定する予定である。研究セキュリティプログラム基準の草案は、2022 年の秋に正式なパブリックコメント期間として利用できるようになると予定されている。（※その後、2023 年 2 月に”DRAFT Research Security Programs Standard Requirement”が公表されている[3]）

[3] https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf
その後、2023 年 3 月 7 日に、2023 年 6 月 5 日を期限に、パブリックコメントを募っているところである。（Request for Information; NSPM 33 Research Security Programs Standard Requirement. <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement >）

・ 連邦政府は、研究セキュリティプログラムに関する要求事項を遵守するための技術支援も提供する予定である。具体的には、NSF、国防省、エネルギー省、国立衛生研究所を含むいくつかの連邦機関が協力して、デジタルトレーニングコンテンツを開発し、他の研究機関が選択すればそれを使用できるようにする。

表 0-1：The CHIPS and Science Act of 2022 の研究セキュリティ関連の規定の概要

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

要求・支援の対象	内容
大統領府科学技術政策局（OSTP）	外国人人材採用プログラム（Foreign Talent Recruitment Programs）のガイドライン作成（Sec.10631） ・（FY2020 国防授権法 1746 条に基づき設立された）省庁間ワーキンググループと連携し、連邦研究機関に対し、外国人人材採用プログラムに関する統一したガイドラインを配布することを OSTP に要求。ガイドラインは、各連邦研究機関のすべての職員が外国人人材採用プログラムに参加することを禁止し、外国人人材採用プログラムの特徴を定義して説明する。2021 年度国防授権法 223 条に従い、研究助成申請書の主要研究者は、外国人人材採用プログラムの契約・協定・取決めの当事者である場合に情報開示しなければならず、また、悪意のある外国人人材採用プログラムに参加することはできない。
資金配分機関（一部は、資金配分機関→研究者・研究機関）	悪質な外国人人材採用プログラム（Malign Foreign Talent Recruitment Program）への参加の禁止（Sec.10632） ・各連邦機関に対し、研究助成金提案プロセスの一環として、提案書提出時又はその後毎年、助成期間中、対象個人が悪質な外国人人材採用プログラムに参加していないことを証明するよう求める方針を確立することを要求する。
	契約等をレビューするための資料を研究機関に要求する権限付与（Sec.10633） ・各連邦機関は、要請に応じて、研究開発助成の申請書に記載された全ての対象者について、外国人人材採用プログラムへの参加に特有の契約書、補助金、又は外国人任命、外国機関への雇用、その他の合意書の写しを含む、補足書類を提出するよう機関に求める権限を有している。研究機関と協議の上、契約、助成金、協定が、機関が支援する活動の能力を阻害する、又は機関が支援する活動との重複を生じさせると判断された場合、連邦研究機関と受領機関は、対象者の代替又は助成からの除外、助成額の削減、助成の停止/終了を開始することができる。各連邦機関は、最終的な行政措置が取られる前に、全ての対象者のプライバシーを保護し、措置の正当な理由を提供し、対象者にコメントや反論を提供し上訴する機会を与えるために必要な措置を講じるべきである。
	連邦政府研究資金を使う研究者：研究セキュリティ研修要件（Sec.10634） ・資金配分機関は、研究資金の公募申請の一部として申請書に記載された各対象者は研究セキュリティ訓練の修了（過去 1 年以内）を認証するという要件を設ける。 ・大学・研究機関は、雇用されている各対象者がそのような訓練を修了していることを証明する。 ・研究セキュリティ研修の内容は、サイバーセキュリティ、国際共同研究、海外渡航、海外からの介入、資金の適切な使用に関する規則、情報開示、責務相反、利益相反に焦点を当てる。
Comptroller General（GAO 長官）	研究資金の会計（Sec.10635） ・Comptroller General（※GAO の長官）に対し、研究のために懸念される外国組織が利用できる連邦資金に関する調査を実施することを要求する。この調査は、研究のために懸念される外国組織が利用できる連邦資金の量、種類、要件に関する評価を含むものとする。
NSF（一部は、NSF→研究者・研究機関）	Office of Research Security and Policy と Chief of Research Security の維持（Sec.10331-10332） ・NSF に、NSF 長官室内に少なくとも 4 名のフルタイムスタッフを擁する Research Security and Policy オフィスを維持することを要求。

要求・支援の対象	内容
NSF（一部は、NSF→研究者・研究機関）	Office of Research Security and Policy にリスクアセスメントの実施権限を付与（Sec.10336） ・NSF の監察官室（OIG）と連携して、NSF Office of Research Security and Policy が、研究開発助成の申請と NSF への情報開示について、オープンソースの分析・解析ツールの利用を含むリスク評価を実施する権限を付与する。
	オンラインリソースの開発（Sec.10334） ・NSF に対し、研究組織及び個人の研究者向けに、最新情報を含むオンラインリソースを開発するよう要請。
	研究不正等についての研究の公募継続（Sec.10335） ・NSF に対し、研究不正や研究インテグリティの侵害、有害な研究行為に関する研究を含む、研究行為や研究環境に関する研究を支援するための研究助成を継続することを要求。
	責任ある研究実践についての研修（Sec.10337） ・責任ある研究実践についての研修に関する 2007 年 America COMPETES Act の Sec.7009 を修正。ポスドク研究者、教員、上級職員を含めるよう要件を拡大。 ・プログラムは、メンター（研究指導者）の訓練、メンターシップ、潜在的な研究セキュリティの脅威に対する認識を高めるための訓練、連邦輸出管理・情報開示・報告要件に関する訓練を含むことを明記。
	研究セキュリティ・インテグリティ情報共有分析センター（Research Security and Integrity Information Sharing Analysis Organization）の外注（Sec.10338）
	Controlled information へのアクセスを持つ研究分野を同定する計画作成（Sec.10339） ・NSF に対して、国家情報長官室（ODNI）及び他の連邦機関と協議の上、主要技術重点分野を含む NSF が支援する研究分野で、controlled unclassified 情報（CUI）又は controlled classified 情報へのアクセスを伴う可能性のあるものを特定する計画を策定するとともに、研究助成に関して働く NSF 職員又は NSF 研究開発助成の対象者に CUI 又は controlled classified information へのアクセスを適宜付与するにあたりデューディリジェンスを行うことを要求。
	孔子学院を設置する研究機関への資金提供の原則禁止（Sec.10339A）
	研究倫理・社会的影響について公募提案書への記載を求める（Sec.10343） ・NSF に対し、利害関係者からの意見を踏まえ、助成金提案の指示書（instruction）を改訂し、研究開発費の支給に先立ち、倫理的・社会的配慮を提案の一部として含めることを義務付けることを要求する。利害関係者の意見を考慮し、NSF は何をもって「容易に予見可能又は定量化可能なリスク（readily foreseeable or quantifiable risk）」とするかについて明確なガイダンスを作成する。
エネルギー省長官	研究セキュリティに対処するツールの開発（Sec.10114） ・DOE 長官に対し、国家情報長官室（ODNI）が特定した脅威を反映した科学技術リスクマトリックスなど、研究セキュリティリスクを管理・軽減するためのツールやプロセスを開発・維持し、対象となる支援の下で実施される活動がもたらす米国の知的財産喪失のリスクや米国の国家安全保障への脅威を判断しやすくするよう要請。
GAO	GAO に対して NIST の研究セキュリティポリシー、プロトコル等についての調査研究を行うよう要求（Sec. 10247）
大学等研究機関	NSF に海外からの資金支援の有無を毎年報告（Sec.10339B） ・研究機関は、毎年 NSF に対し、贈与や契約を含め、当該機関が懸念される外国（foreign country of concern）に関連する外国資金源から直接又は間接的に受ける 5 万ドル以上の現在の資金援助について、要約文書の形で報告しなければならない。
研究者等	懸念される個人又は団体の禁止。（Sec.10636） ・新設の NSF Directorate for Technology, Innovation and Partnerships を含む、特定のプログラムに対する助成、アワード、プログラム、支援、その他の活動を受けること又は参加することを、懸念事項とされた人物又は団体（persons or entities identified as a concern）に禁止する。

出典：AAU. The CHIPS and Science Act of 2022 (H.R. 4346): Research Security Provisions. Last updated August 8, 2022. <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf> 等に基づき作成。

また、米国の全米アカデミーズ（National Academies）では DARPA と NSF からの依頼で、報告書「米国の技術優位を保護する」（*Protecting the U.S. Technological Advantages*）を作成し、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術をいかに保護するかを検討して公表した。この報告書は大統領府や連邦政府機関への提言を含む。また、全米アカデミーズには「科学技術安全保障円卓会議」が設置される[4]とともに、「オープンネス、国際的関与と連邦資金科学技術研究」についてのワークショップを 2022 年に 4 回開催し、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場となっている。

政府で研究インテグリティを担当する体制（主として対応する省庁）とその特色

米国政府において研究インテグリティは主として大統領府科学技術政策局（OSTP）が主導・取りまとめを担当しているが、研究開発に関連するすべての連邦省庁、資金配分機関が関係し、更に CIA、FBI 等の情報機関も含めて取り組むこととされていることに体制面の特色がある。

大統領から発出された NSPM-33（2021 年 1 月）の送付先は、大統領府レベルの 15 の連邦省庁（財務省、住宅都市開発省を除く）の長官に加え、行政管理予算局（OMB）の長、その他連邦政府独立省庁（環境保護庁、NASA、米国科学財団（NSF））の長、研究所等（NIH、スミソニアン協会）の長、さらに、情報機関の長（国家情報長官（Director of National Intelligence: DNI）、Director of CIA（中央情報局）、Director of FBI（連邦捜査局））、国家安全保障担当大統領補佐官（The Assistant to the President for National Security Affairs）、そして本件取りまとめを担当する大統領府科学技術政策局（Office of Science and Technology Policy: OSTP）の長が含まれていた。このように研究開発を行う連邦省庁とともに、情報機関に対する指示となっていることが特色と言える。

NSPM-33 実施ガイダンス（2022 年 1 月）は、米国科学技術会議（NSTC）の「研究環境に関する NSTC 合同委員会」（Joint Committee on the Research Environment）の「研究セキュリティ小委員会」（Subcommittee on Research Security）が策定している。研究セキュリティ小委員会の共同議長はエネルギー省、大統領府 OSTP、NSF、NIH の委員が務めており、大統領府の OSTP がこれらの委員会の事務局を務めており、委員には連邦省庁からのメンバーが連なっている。

また、連邦法である上記の The CHIPS and Science Act of 2022 は、上の表に示すように、議会から OSTP、連邦省庁、NSF 等資金配分機関、研究者に対して様々な要求がなされている。

研究インテグリティについての資金配分機関の対応とその特色

本調査では米国科学財団（NSF）、米国国立衛生研究所（National Institutes of Health:

[4] 2020 年度国防権限法の第 1746 条に基づき、米国科学財団、エネルギー省、国防省等の連邦省庁が全米アカデミーズと合意し設置されている。

NIH)、エネルギー省科学局、国防高等研究計画局（Defense Advanced Research Projects Agency: DARPA）について調査したが、いずれの資金配分機関でも NSPM-33 で要求されるように研究助成申請の主要な研究人員について経歴、現在・未決（pending）の支援（現物支給含む）についての情報開示を求めている。情報開示の項目、フォーマットについては以下のように現在共通開示フォーマットが開発中である。また、それぞれの資金配分機関で特徴的な取組が見られる。

- NSF は、米国科学技術会議（NSTC）の研究セキュリティ小委員会を代表して、研究申請書の経歴（Biographical Sketch）と現在・未決の（その他）支援（Current and Pending (Other) Support）の共通開示フォームについてパブリックコメントの募集を 2022 年 8 月 31 日に開始した。意見の募集は 2022 年 10 月 31 日までであり、それを踏まえ、最終的に決定される見込みである。NSPM-33（4(b)項）では研究者の負担軽減のために共通開示フォーマットの作成が要求されていた。
- NSF 職員等は研究セキュリティ関連のトレーニングの受講を義務付けられている。1 つ目のコースは、「科学とセキュリティのトレーニング」であり、NSF の情報開示方針と、外国政府の人材採用プログラムに関する NSF の新しい方針について学ぶ。このコース受講は、NSF の全スタッフとコントラクターに対して毎年義務付けられている。2 つ目のコース「科学とセキュリティのトレーニング: パート 2」は、プログラム担当者が助成等決定前に情報のリスク評価をどのように行うべきかというガイダンスとともに、助成等決定後の情報の取り扱いに関する内部プロセスの実施について概説する。このコースは、NSF のすべてのプログラムオフィサーとグラント管理者に受講が義務付けられている。
- NSF は、研究コミュニティ向けに研究セキュリティトレーニングを開発する取組を支援している。NSF は、国立衛生研究所、エネルギー省、国防省と共同で、連邦研究費の受給者に世界の研究エコシステムに対するリスクと脅威に関する情報、及びこれらのリスクから保護するために必要な知識とツールを提供するオンライントレーニングモジュールの開発に関する提案を求める公募を行い、現在、4 つのトレーニングモジュールが委託を受けた大学等で開発中である。
- NSF-77: Data Analytics Application Suite は、NSF の内部データの許容される利用を拡大し、NSF が支援する活動に参加する個人や組織から報告された情報を、研究事業に関連する公開情報とともに集約、連携、分析することを可能とする。このシステムで分析することで、情報開示内容に疑いのある申請書の発見につなげることが意図されている。
- DARPA の「海外からの影響対策プログラム」(Countering Foreign Influence Program: CFIP）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 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。高リスクと評価された提案は、リスク軽減計画を必要とする可能性があり、文書化された

リスク受容の決定が必要となる。非常に高いリスクと評価された提案は、リスク軽減計画及び文書化されたリスク受容の決定が必要となる。DARPA は 2021 年に CFIP を発表し、その後、2022 年 5 月に変更追加されているとのことである 。

研究インテグリティについての大学等の対応とその特色

本調査は、マサチューセッツ工科大学（MIT）、ハーバード大学、スタンフォード大学、カリフォルニア大学バークレー校（UC バークレー）について研究インテグリティ、研究セキュリティについての対応を調べた。以下のように、いずれの大学でも学長レベルのリーダーシップにより大学全体として対応が検討され具体的な取組が行われてきている。

- MIT China Strategy Group は、MIT の Richard Lester 教授（Associate Provost for International Activities; Japan Steel Industry Professor of Nuclear Science and Engineering）と Lily Tsai 教授（Chair of the Faculty; Ford Professor of Political Science; Director, MIT Gov/Lab）を共同議長とし、他に 5 人の教授、2 人の職員をメンバーとする。グループでは、政治指導者が基本的人権や価値観と相容れない政策を追求し、米国に安全保障上のリスクをもたらす国々の組織や個人と、MIT や他の米国の研究大学がどのように関わるべきか、について幅広い視点から検討し、2022 年 11 月に約 40 頁の報告書（*Engagement with China: An MIT Approach Final Report*）を公表した。
- 2019 年より MIT は格上げされたリスクマネジメントプロセスを導入している。2019 年、MIT は、国家安全保障、経済安全保障、市民・人権に関連する高度のリスクをもたらす可能性のある国際的な関与を伴う提案を審査する新しいプロセスを導入した。現在、この高リスク審査プロセス（elevated risk review process）では、中国、ロシア、サウジアラビアに関わるすべての関与案と、特別なリスクをもたらす可能性のあるその他の特定のプロジェクトが検討対象となっている。
- ハーバード大学の学芸科学学部（Faculty of Arts and Sciences: FAS）、工学・応用科学学部（School of Engineering and Applied Sciences: SEAS）と研究担当副学長室（Office of the Vice Provost for Research: OVPR）は、共有の「研究コンプライアンスプログラム」（Research Compliance Program: RCP）を設立した。このプログラムでは、OVPR のスタッフが 2023 年 2 月 15 日より、特定の研究コンプライアンス機能における運用的・管理的責任を担当する。移管される研究コンプライアンス機能は、教員・研究者の外部活動及び利益相反、輸出規制、国際的な共同研究及び活動の 3 つである。
- スタンフォード大学の「グローバル関与レビュープログラム」（Global Engagement Review Program: GERP）は、オープンかつ友好的なコミュニティを維持するために、潜在的な不当な海外影響力のリスクを評価するために作られた集中的な助言プロセスである。このプログラムは、不当な外国からの影響力、研究セキュリティ・研究インテグリティに関連するリスクを評価するために、外国への関与のさまざまな側面について助言する複数のオフィスからの情報を調整する。教員や管理者は、GERP ディレク

ターに連絡することで、GERP のレビューを推奨又は要求することができる。関与が高いリスクを示す場合、ディレクターは、専門家からなる GERP スタッフ委員会（GERP Staff Committee）と協力して、リスクを評価し、学術及び研究目標を支援する勧告を作成する。GERP スタッフ委員会が、ある契約に関連するリスクが特別に高いと判断する場合には、GERP スタッフ委員会は GERP 教員委員会（GERP Faculty Committee）にその問題を付託し、教員委員会は検討し、大学の指導者に助言と勧告を提供する。

- UC バークレーの「国際的な関与の原則」（Principles of International Engagement）声明は、2019 年に「国際的な関与の方針タスクフォース」（International Engagement Policy Task Force: IEPTF）によって作成され、2020 年に学長によって発表された。目的は、国際的な関与が UC バークレーの学術的な使命と地位にとって重要であることを伝えるとともに、国際的な関与を妨げる行為を非難することである。IEPTF は、キャンパス内外の国際的な関与に関する方針やガイダンスを策定することを目的とし、2019 年に UC バークレーの学長によって設置された。このタスクフォースは、学術計画担当副学長（Vice Provost for Academic Planning）と研究担当副学長（Vice Chancellor for Research）が担当し、学内の関係部署のメンバーが参加している。IEPTF は 2020 年 6 月に検討結果の報告書を発表した。報告書では、UC バークレーの国際的な関与に関する現状分析と提言をまとめた。幅広い項目についての提言を含んでいる。

米国における研究インテグリティの確保のための要求と支援：注目点

上記の連邦法や大統領覚書、ガイドライン等において、連邦省庁、資金配分機関、大学・研究機関、研究者等に対して、様々な要求事項が規定されており、それら要求を確実に実施してもらうための支援についても規定がある。それらは多項目にわたるものであるが、以下は特に注目される取組である。

- 研究セキュリティのトレーニングについて政府研究資金を受ける研究者に受講義務付け（CHIPS and Science Act）
- 研究セキュリティについて連邦法で規定されている（CHIPS and Science Act）
- 研究セキュリティについてのモデル教育プログラムの開発（NSF の公募で 4 大学に既に委託）
- 情報機関（CIA、FBI、ODNI）が政府の研究セキュリティ対応体制に入っている。当初の NSPM-33 から明示。
- 国土安全保障省による外国人留学生、外国人研究者への入国審査も研究セキュリティの対応策の中に位置づけられている。
- 外国人人材採用プログラムへの参加についての開示義務。政府研究機関の研究者は参加が禁止、大学等の政府資金受領研究者は、悪意のある外国人人材採用プログラムへの参加を禁止。
- 大統領府レベルの Subcommittee on Research Security（National Science and

Technology Council に属する）でほぼ全ての関係省庁（情報機関、安全保障担当大統領補佐官を含む）が集まって研究セキュリティ対応について対策する体制ができている。

- 同盟国、他の友好国に対しても研究セキュリティ対応について働きかけることをNSPM-33 に明記。
- 米国の全米アカデミーズ（National Academies）は、報告書「米国の技術優位を保護する」を作成し、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術をいかに保護するかについて、大統領府や連邦政府機関への政策提言をするとともに、「科学技術安全保障円卓会議」が設置される等、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場となっている。

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

研究インテグリティについての法令による規制、あるいはガイドライン等とその内容・特色

研究インテグリティそのものを規定する法規制はなく、「Trusted Research」が、英国における研究インテグリティを推進するイニシアティブという位置づけ。「Trusted Research」は、『研究者として、研究を保護し、法的義務（輸出管理、産学共同研究契約、武器禁輸、海外の司法コンプライアンス、一般データ保護規則（General Data Protection Regulation: GDPR）、特許法、National Security and Investment Act（NSI 法）等）をすべて果たしていることを確認すべし』という政府のキャンペーンである。

- 「Trusted Research」は、英国の研究セキュリティのプロトコルと言っても過言ではない。
- NSI 法は、「大学・研究機関が、他の当事者と協力して、適格な企業や資産を取得、売却、開発する際に遵守すべき事項」を示すために、「Trusted Research」キャンペーンに合わせて新たに制定された法律（2021 年 4 月 29 日制定、2022 年 1 月 4 日施行））である。「Trusted Research」そのものを規定するものではない。

国家インフラ保護センター（Centre for the Protection of National Infrastructure: CPNI）[5]により、「Trusted Research」に関して留意すべき事項を説明した、大学・研究機関研究者向けのガイダンス、大学・研究機関の研究及び職員のセキュリティ担当者向けの実践的ガイダンス、大学・研究機関の上級管理者向けのガイダンス、国際共同研究提案の際のチェックリストなどがある。

政府で研究インテグリティを担当する体制（主として対応する省庁）とその特色

CPNI と国家サイバーセキュリティセンター（National Cyber Security Centre: NCSC）

[5] CPNI は 2023 年 3 月に、「国家保護安全保障局」（National Protective Security Authority: NPSA）に名称変更するとともに、任務が拡大している。（”About NPSA” <https://www.npsa.gov.uk/about-npsa>）

のリーダーシップの下、「Trusted Research」キャンペーンを展開。

- ビジネス・エネルギー・産業戦略省（Department for Business, Energy & Industrial Strategy: BEIS）[6]が、英国の国際研究・イノベーションの保護という観点から支援。
  - 研究者を敵対行為から守り、輸出管理規制、サイバーセキュリティ及び知的財産の保護等のセキュリティ関連の課題についての政府の助言を提供するために、2021 年 5 月に、BEIS 内に Research Collaboration Advice Team (RCAT)を立ち上げ[7]。RCAT は、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（法的権限はない)。

研究インテグリティについての資金配分機関の対応とその特色

大学等研究のファンディング機関である UKRI が、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）を示した文書を発表。UKRI から資金提供を受けている組織は、この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及び対策を実施したことを証明できるようにする必要がある。

研究インテグリティについての大学等の対応とその特色

英国の大学連合である Universities UK (UUK)が、CPNI のガイダンスを補完する位置づけで、外国による敵対的な干渉から守り、学問の自由を促進するために教育機関が取るべき配慮や対策に関する詳細なガイドラインを公表。

UUK に加盟している 139 の大学や研究機関は、このガイドラインに基づき、各大学・機関の状況に合わせた運用を行うことが要請されている。

英国における研究インテグリティの確保のための要求と支援：注目点

以下は英国の研究インテグリティ確保のための取組のうち特に注目されるものを列挙している（政府・資金配分機関等からの要求、政府・資金配分機関等からの支援、大学等の取組など)。

- 英国の経済安全保障の一環として、経済的利益を享受している英国の国際研究・イノベーションの保護の観点から、ビジネス・エネルギー・産業戦略省 BEIS）が研究インテグリティに大きく関与。
- 国家安全保障機関のイニシアティブの下に研究インテグリティを推進。国家安全保障機関が、UUK 及び資金配分機関と手を握り、強力に研究インテグリティを推進。

[6] BEIS は、2023 年 2 月、スナク政権の下に、「Department for Energy Security and Net Zero（DESNZ)」、「Department for Science, Innovation and Technology（DSIT)」及び「Department for Business and Trade」の 3 つの省に分割された。

[7] BEIS の分割に伴い、現在 RCAT は「Department for Science, Innovation and Technology（DSIT)」に属するものと思われる（これに関する公式情報は無い)。

- 国家安全保障機関からベースとなる研究インテグリティに関するガイダンスを発行。
    - ✧ 大学・研究機関研究者向けのガイダンス
    - ✧ 大学・研究機関の研究及び職員のセキュリティ担当者向けの実践的ガイダンス
    - ✧ 大学・研究機関の上級管理者向けのガイダンス
    - ✧ 国際共同研究提案の際のチェックリスト　等
- 国家安全保障機関のガイダンスを補完する位置づけで、UUK から研究インテグリティに関するガイドラインを発行。
- 国家安全保障機関のガイダンスを踏まえて、資金配分機関から研究インテグリティに関する原則に関する文書を発行し、資金配分を受ける際の原則の遵守を要求（パートナーの適性評価、情報セキュリティ管理策の導入、知的資産を適切に管理するための共同研究契約の締結など）。
- 国家安全保障機関、UUK 及び資金配分機関の共同で、継続的に、研究インテグリティに関するガイダンスや関連資料の整備を実施。
- 政府・大学として、国際共同研究におけるリスク緩和策のチェックリストを作成・提示
- 政府・大学として、大学における研究インテグリティ活動の紹介

・ 法的権限はないが、政府として、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窓口機関（RCAT）を設立。

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

政府で研究インテグリティを担当する体制

豪州では、2017 年前後を境に豪州と中国との外交・経済関係が大きく変化したことによって、海外からの干渉にまつわる外国干渉セキュリティへの対応が本格化した。同年には、内務省直轄の防諜機関である豪州保安情報機構（Australian Security Intelligence Organisation: ASIO）のダンカン・ルイス長官（当時）が、中国を念頭に豪州の大学への干渉について、大学側が無防備であるとして警鐘を鳴らした。また 2020 年には、新型コロナウイルスの発生源について、モリソン首相（当時）が独立考査を求めたことに対し、中国が強く反発し、戦略的経済対話を停止するなどの事件もあった。豪中関係の悪化に伴い、同年 12 月に外国関係法が制定され、豪州の大学・研究機関が外国政府と取り決めを締結する際には、外務大臣への事前通知と承認取り付けが義務づけられるなどした。

こうした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）を設置することになる。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。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。

研究インテグリティについての法令による規制、あるいはガイドライン等とその内容・特色

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（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。２年後の 2021 年 11 月に改定された。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。それによると、外国干渉に対抗する上で政府が大学・研究機関の支援を提供するものは次の５項目とされる。

- 大学の上級管理者に対し、外国干渉の脅威と国家安全保障政策について説明する
- 外国干渉に対する大学職員の意識を向上させる
- 政府の保安情報機構（ASIO）や外国干渉対策調整センターを通じての大学への働きかけ
- 国益となる重要な技術に関する最新情報を提供する
- サイバーセキュリティ能力を強化し、インシデントに対処するためのガイダンスを提供する

一方、政府が大学・研究機関側に要求するものは次の４つのテーマに及ぶ。

（a）ガバナンスとリスクのフレームワーク
（b）コミュニケーション、教育及び知識共有
（c）デューディリジェンスやリスク評価、リスクマネジメント
（d）サイバーセキュリティ

ガイドラインの記述に沿って、主なものを拾っていくと要求事項は次のような形になっている。

(a)のガバナンス等については、リスク管理の責任者を置くことや、職員・学生が利用できる明確なリスク評価と報告の枠組みの設置などを求めている。

(b)のコミュニケーション等では、外国干渉を受ける危険性がある共同研究に従事する職員・学生に対し、コミュニケーション計画や教育プログラム、研修などの実施を求めている。この際、政府の保安情報機構（ASIO）や外国干渉対策調整センターが、大学・研究機関側を支援するための連絡窓口を提供することになっているのが大きな特徴といえる。

(c)のデューディリジェンス等では、１年に１回の割合で定期的な利害関係の申告を求めているほか、カウンターパートに対するデューディリジェンスの実施を求めている。また技術分野においては、豪州の防衛戦略物資リスト（DSGL）に含まれたり、国外への輸出や電子的な供給が規制されたりしていないかをチェックすることも義務づけている。

(d)のサイバーセキュリティでは、可能な限り脅威モデルなどの手法を用いることによってリスク軽減に努めたり、ベストプラクティスを徹底させたりすることなどを求めている。

研究インテグリティについての資金配分機関の対応とその特色

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。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 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。

研究インテグリティについての大学等の対応とその特色

その他のアクターの中でも、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。

豪州における研究インテグリティの確保のための要求と支援：注目点

外国干渉セキュリティにおける豪州の取組の特徴の 1 つは、内務省直轄の防諜機関である豪州保安情報機構（ASIO）に大きく依存していることにある。これまで見てきたように、ASIO は UFIT ガイドラインの運用に積極的に関わり、大学・研究機関側の連絡や相談の窓口としても機能しており、いわゆる公安情報に基づいてガイドラインが運用されている側面があるのではないかと思慮される。国内には表立った反発や反対論は見受けられないが、学問の自由との関係で問題提起する大学もある。

例えば、豪州国立大学（ANU）では、厳格な外国干渉セキュリティに対する措置を取る一方、学問の自由を守る立場から、そもそも「外国干渉とは何を意味するのか」という視点から、同大学は学内のインターネットサイトに「外国からの影響（influence）」と「外国からの干渉（interference）」の違いに注意喚起を促す同大研究者によるレポートを掲載している。

それによると、「豪州の対応は外国からの影響力のうち、最も悪質な形態である外国干渉を犯罪とみなし、その抑止に重点を置いてきた。しかし許容される外国からの影響と不法な外国からの干渉の間にはグレーゾーンが生まれつつある」として、行き過ぎた政府の外国干渉排除の動きにくぎを刺している。

特に注目される点としては、豪州の研究インテグリティに対する考え方は、あくまでも大学・研究機関による自主性や自己規制を重んじる形になっている点にあると言えそうである。

たとえ不正事案や外国干渉セキュリティにまつわる事案であっても、不正調査や認定を資金配分機関など外部の機関が行うことはなく、個別の大学あてに勧告を出すにとどまっているのが大きな特徴である。大学・研究機関は、あくまでも独自に通称・豪州規範（The

Australian Code for the Responsible Conduct of Research、「責任ある研究実施のための豪州規範」）や UFIT ガイドラインに沿って自主判断し、最終決定を下すとされている。

自主的なガイドラインや規範の運用にこだわる姿勢は、2021 年に UFIT ガイドラインが更新された際、過度な情報開示を求める政府草案に大学・研究機関側から強い反発が出て争点化し、政府側が修正を強いられた経緯にも現れている。政府草案では、「大学すべての研究者に、政党の所属と過去 10 年間の外国企業から受けた資金支援」を開示するよう求める踏み込んだ内容だったものが、反発を受け、このくだりは「大学側が利益相反開示の聴き取りをする対象の研究者を選べる」ように修正された。あくまでもガイドラインの運用は大学当局が自主的に行う、という原則が確認される結果となった。

また、その他の注目点としては、大学・研究機関側のアクターのうち豪州の上位８つの大学で組織するグループ８（Go8）が公表しているベストプラクティス（Measures taken by the Go8 to mitigate the threat of foreign interference in alignment with the UFIT Guidelines）がある。それによると、８大学がそれぞれ外国干渉を排除するためのオリジナルの方策を披露しあい、他の大学・研究機関の参考に供している[8]。例えば、豪州国立大学では AI を活用した先駆的な取組を行っている。貿易管理の対象になる可能性があるすべての研究を自動的に特定するため、AI を利用している、といった具合である。

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

研究インテグリティについての法令による規制、あるいはガイドライン等とその内容・特色

輸出管理関連法規の「規制品目プログラム（Controlled Goods Program）[9]」や医療倫理規制法令[10]などを除き、研究セキュリティ・研究インテグリティに関する包括的な法規制は存在しない。

イノベーション・科学・経済開発相、公共安全相、保健相による最新の声明では、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）における機密性の高い研究分野で研究を行うことを伴う助成金申請では、プロジェクトに携わる研究者のいずれかが、カナダの安全保障に危険をもたらす外国の国家主体の軍事、国防、国家安全保障団体に関係する大学、研究機関、研究所に所属している場合は、助成金を支給しないこととされた。

政府で研究インテグリティを担当する体制（主として対応する省庁）とその特色

連邦政府の 3 つの資金配分機関（CIHR、NSERC、SSHRC）に対しては、所管するイノベーション・科学・経済開発省、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

[8] Appendix-3-Go8-actions-against-the-Guidelines.pdf
[9] Defence Production Act の既製品目リスト掲載の物品・技術に関する規制
[10] Food and Drug Regulations (FDR) under the Food and Drugs Act (Canada)など

する。

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、オープンで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、Safeguarding Your Research ポータル[11]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結果を広めるための重要なチャネルとなっている。

外国影響やスパイからの研究コミュニティの保護は、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）が取り締まりを所管する。

研究インテグリティについての資金配分機関の対応とその特色

CIHR、NSERC、SSHRC は 2016 年に研究インテグリティに関する共通規範の「Tri-Agency Framework：Responsible Conduct of Research（RCR）」（RCR フレームワーク）を定めている。このフレームワークは FFP（捏造・改ざん・盗用）等の研究不正行為や利益相反行為への注意喚起を行い、発覚時の処理手順及び罰則等を定めている。フレームワークは 2021 年に改定されたが、現状では「研究セキュリティ」や「外国影響」に焦点を当てた規定は盛り込まれていない[12][13]。

カナダ政府とカナダ政府・大学共同ワーキンググループが作成した「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）」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影響についてのリスクアセスメントが要請されている。

研究インテグリティについての大学等の対応とその特色

マギル大学では 2020 年に外国干渉ワーキンググループ（McGill Foreign Interference Working Group）を設立し、同グループが大学全体の取組を指導的している。外国からの干渉を監視するため同グループは定期的に開催され、国家安全保障局との活発な連携が行われている。

トロント大学（University of Toronto）では 2021 年 8 月 30 日より、国際的なパートナーシップに携わる教員は、「研究パートナーシップ・セキュリティ情報文書（Research Partnership Security Information Document）」に必要事項を記入するよう求められている。

---

11 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>

12 カナダ政府ウェブサイト” Tri-Agency Framework: Responsible Conduct of Research (2016)”<https://rcr.ethics.gc.ca/eng/framework-cadre.html>

13 カナダ政府ウェブサイト” Tri-Agency Framework: Responsible Conduct of Research (2021)”https://rcr.ethics.gc.ca/eng/framework-cadre-2021.html

カナダにおける研究インテグリティの確保のための要求と支援：注目点

カナダにおける研究インテグリティの確保のための取組では、以下が注目される。

- 大学において国家安全保障当局との活発な連携が行われている。
- 外国影響やスパイからの研究コミュニティの保護は、公共安全省の一義的な責務であると宣明している。
- 地域別（州ごと）のリスク評価の参考資料を政府が用意している。

1.5 欧州連合における研究インテグリティ確保のための取組

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。本文書は、「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も可能である。「海外からの干渉」（foreign interference）への対応策について、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、説明している。

例えば、同作業文書では、学問の自由が一般的に尊重されている国では、リスクとなる価値観を詳細に評価する必要はないが、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り、「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。また、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説明している。

なお、欧州連合の研究資金プログラム（2021～2027 年）である Horizon Europe 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 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されている。追加されたのは以下の文章であり、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。

・ 「欧州委員会は、『研究・イノベーション（R&I）への海外からの干渉』に取り組むためのツールキットを発表した。この文書は、価値、ガバナンス、パートナーシップ、サイバーセキュリティに関する多くの勧告を提供しており、高等教育機関や研究実施機関が国際的な R&I に取り組む際の支援を提供することを目的としている。Horizon Europe に参加するすべての人は、この文書及び国レベルで存在する同等のアドバイスをよく理解し、提出予定のプロポーザルとの関連性を検討することが推奨される。」

1.6　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

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に対して、各国・地域の問題意識は共通しているものの、それへの対応策については、それぞれの国の科学技術行政体制や、科学コミュニティの特色あるいはそれらに関連する伝統や歴史的経緯を反映して、様々であり、どの国の取組がベストプラクティスと言える訳ではない。言い換えれば、ある国において有効な方法であっても、他の国においては科学者コミュニティや社会から反発を受けて取組が定着せず、有効に履行されないこともあり得る。

以上を考慮した上で、上記の各国・地域の調査結果で注目点として指摘された取組等において、1）要求に関連する取組等、2）支援に関連する取組等、さらに 3）それらを検討し、履行をフォローするための体制について、以下の取組等については、日本にとってレッスンを得ることが大きいのではないかと考えられる。

<u>研究インテグリティに関連する要求事項</u>

・　米国：研究セキュリティのトレーニングについて政府研究資金を受ける研究者に受講義務付け（CHIPS and Science Act）

<u>研究インテグリティに関する支援関連事項</u>

(a)　研究者への支援関連

・　英国：大学・研究機関研究者向けのガイダンスの策定

(b)　大学・研究機関等への支援関連

・　米国：研究セキュリティについてのモデル教育プログラムの開発

・　英国：助言の仕組み：Research Collaboration Advice Team (RCAT)。政府として、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窓口機関（RCAT）を設立。

・　英国：大学・研究機関の上級管理者向けのガイダンスの提供

・　豪州：大学の上級管理者に対し、外国干渉の脅威と国家安全保障政策について説明する（UFIT ガイドライン）

・　豪州：豪州の上位８つの大学で組織するグループ８（Go8）が外国干渉を排除するためのベストプラクティスを取りまとめ公表。

・　豪州：資金配分機関の ARC が競争的研究資金の申請時に、懸念のある機微技術が含まれていると判断した場合、ASIO など国家安全保障機関に審査と助言を依頼することがある。

・　カナダ：外国影響やスパイからの研究コミュニティの保護を責務とする公共安全省が地域別（州ごと）のリスク評価の参考資料を作成し、公表。

・ EU：「価値」（学問の自由へのコミットメントの強化、抑圧的な環境下にあるパートナーとの協力）を強調した「海外からの干渉」（foreign interference）への対応策の大学・研究機関への提示。

(c) 学協会等のアカデミアの取組

・ 米国：米国の全米アカデミーズ（National Academies）は、報告書「米国の技術優位を保護する」を作成し、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術を保護するかについて、大統領府や連邦政府機関への政策提言をするとともに、「科学技術安全保障円卓会議」が設置される等、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場となっている。

研究インテグリティの確保を検討・履行するための国の体制

・ 米国：大統領府レベルの Subcommittee on Research Security（National Science and Technology Council に属する）でほぼ全ての関係省庁（情報機関、安全保障担当大統領補佐官を含む）が集まって研究セキュリティ対応について対策する体制ができている。
・ 英国：国家安全保障機関が、UUK（大学協会）及び資金配分機関と手を握り、強力に研究インテグリティを推進。
・ 豪州：政府と大学・研究機関が共同してタスクフォース（UFIT: University Foreign Interference Taskforce）を設置。政府の保安情報機構（ASIO）や外国干渉対策調整センターを通じての大学への働きかけ。
・ カナダ：外国影響やスパイからの研究コミュニティの保護は、公共安全省の一義的な責務であると宣明している。

２．研究インテグリティについての説明会の実施

「研究インテグリティについての説明会」を、「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、大学等における取組についての講演を行うとともに、参加者との質疑応答を行うことで、研究インテグリティについての理解を深め、その確保のための具体的取組の情報交換を促進すること」を目的として開催した。研究インテグリティ関連の業務に関わっているあるいは関心を持つ、大学・研究機関の教員・研究者・職員を対象として、オンラインのウェビナー（第1～3回説明会：70分、第4回説明会：75分）を4回実施した。

各回の説明会の開催内容は以下のとおりである。第1～3回説明会では、政府からの説明を20分、大学事例についての説明を20分した後に、残りの時間（約20分間）を質疑応答に充てた。第4回説明会では約60分間のパネルディスカッションを行い、その中で適宜質疑応答を行った。

第1回説明会（2022年12月17日） 政府の取組：「研究インテグリティに係る対応方針とその取組状況」（内閣府、文部科学省） ※第2回、第3回説明会時も同様の説明。 大学の取組：「東北大学における研究インテグリティに関する取り組み」 東北大学　副理事（研究公正担当）　佐々木孝彦
第2回説明会（2023年1月17日） 大学の取組：「研究インテグリティの確保と大学法務～九州大学の取り組み」 九州大学　法務統括室 室長補佐・特任教授　佐藤弘基
第3回説明会（2023年1月27日） 大学の取組：「研究インテグリティ確保をリスクマネジメントにどう繋げるか？」 名古屋大学 学術研究・産学官連携推進本部 学術・連携リスクマネジメント部門 部門長　特任教授　宮林毅
第4回説明会（2023年3月9日） パネルディスカッション： 司会進行 東京大学 未来ビジョン研究センター 教授　渡部俊也 パネリスト 東北大学　副理事（研究公正担当）佐々木孝彦 九州大学　法務統括室 室長補佐・特任教授　佐藤弘基 名古屋大学 学術研究・産学官連携推進本部 学術・連携リスクマネジメント部門 部門長　特任教授　宮林毅 内閣府 科学技術・イノベーション推進事務局 上席政策調査員　田村朱麗 文部科学省 科学技術・学術政策局 参事官（国際戦略担当）付 参事官補佐　遠藤正紀　　係長　加藤拓巳

各説明会への参加者人数（主催者・事務局と講演者を除く）は、第1回説明会が約350人、第2回説明会が約250人、第3回説明会が約220人、第4回説明会が約280人であった。4回の説明会への参加者ののべ人数は約1,100人である。

説明会参加者へのアンケート結果によれば、参加者の所属は国立大学（48.9%）、公立大学（24.7%）、国立研究開発法人（18.9%）が多く、職種は大学職員（63.4%）、研究機関等の職員（18.9%）、大学教員（11.9%）が多かった（第1回説明会参加者227人の回答）。第2

～4 回説明会においても概ね同様の傾向が見られた。第 1～3 回説明会における政府側からの説明（内閣府・文部科学省）に対しては「とても参考になった」が 2 割程度、「参考になった」が 6～7 割程度であり、大学の事例についての説明については、「とても参考になった」が 4 割程度、「参考になった」が 5～6 割程度の回答だった。また、第 1～3 回の事例紹介者が全員参加し、パネルディスカッション形式で行った第 4 回説明会においては「とても参考になった」が 32.7%、「参考になった」が 64.2%であり、参加者の高い満足度が得られた。また、自由記入の質問（コメント、今後の要望等）に対しては、参加者に大学職員が多かったこともあり、研究インテグリティ確保のための具体的な事例（大学、国立研究開発法人等）をもっと知りたいとの声が多かった。また、今回の説明で取り上げた事例が規模の大きな研究大学であったことから、中小規模大学、地方大学における研究インテグリティ確保のための体制整備はどのように進めるべきかについて知りたいとの要望も多かった。

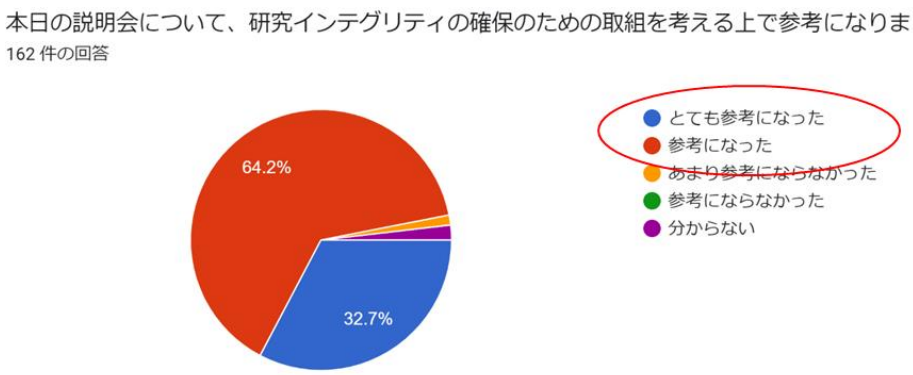


図 0-1：第 4 回説明会における事後アンケート結果

説明会では、上記のように、政府側からの説明、大学における取組の事例紹介の説明をするとともに、参加者との質疑応答等をすることで理解をより深めることが目的とされていたが、多くの質問が参加者から寄せられた。第 1 回説明会は 28 問（事前質問 22 問、当日 6 問）、第 2 回説明会は 23 問（事前 19 問、当日 4 問）、第 3 回説明会は 11 問（事前 5 問、当日 6 問）、第 4 回説明会は 22 問（事前 21 問、当日 1 問）の質問があった。主な質問内容は、研究インテグリティの概念や「新たなリスク」の具体的内容や判断についてのもの（「新たなリスク」とは何か。研究インテグリティで扱うリスクの具体的内容はどのようなもので、どのように判断を行うのか等）、研究インテグリティへ取り組むための組織についてのもの（安全保障輸出管理、利益相反等に関する既存の体制に、研究インテグリティ確保のための新たな組織等をどのように位置づけ、既存の体制をどのように拡充していけばいいのか等）が多かった。

第 4 回説明会では今後の政府の研究インテグリティ確保のための施策等への要望についてのコメントとしては、次年度以降も、同様の大学・研究機関における研究インテグリティ確保のための取組の先進的な事例についての情報共有をするための説明会等の実施を継続

することを希望する意見が多かった。また、今年度はオンライン会議で実施したが、「来年度以降は対面で直接意見交換ができる場を期待する」との意見もあった。

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）が決定されたところである。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早期に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説明会を 4 回実施し、政府と大学・研究機関における研究インテグリティ確保のための取組等について、関係者の間での理解増進と情報共有を図った。

なお、「研究インテグリティ」は研究不正行為等への対応や産学連携による利益相反への対応等にも関わる大きな概念であるが、本調査では、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[14]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

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

いうトピックとして議論されていることから、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諸外国・地域の政府、資金配分機関、大学・研究機関における研究インテグリティに対する認識・取組み状況について、調査・分析する。

① 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、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を次の観点で、文献調査及びインターネット調査する。調査対象国・地域は、米国、英国、オーストラリア、カナダ、EU とする。

(ア) 各国の研究者、大学・研究機関、研究資金配分機関のそれぞれが、どこから何を求められているかをリストアップし、その要求レベル（法令等による義務付け、ガイドライン等による自主規制、推奨事項等）が分かるように分類する。

(イ)(ア)で求められていることを各国の研究者、大学・研究機関、研究資金配分機関が実施するために、どこから、どのような支援が提供されているかをリストアップするとともに、特徴的な取組を含む支援の内容についてまとめる。

(ウ) 米国４大学（MIT、ハーバード大学、スタンフォード大学、カリフォルニア大学バークレー校)、英国１大学（マンチェスター大学)、オーストラリア１大学（オーストラリア国立大学)、カナダ２大学（マギル大学、トロント大学）について、それぞれどのような事項を実施しているのかをリストアップする。

(エ) 米国４研究資金配分機関（米国科学財団（NSF)、エネルギー省（DOE)、国立衛生研究所（NIH)、国防高等研究計画機関（DARPA))、英国１研究資金配分機関（研究・イノベーション機構（UKRI))、オーストラリア１研究資金配分機関（オーストラリア研究会議（ARC))、カナダ１研究資金配分機関（自然科学・工学研究会議（NSERC))、EU の研究資金配分の枠組みであるホライズンヨーロッパについて、それぞれどのような事項を実施しているのかをリストアップする。

調査分析結果は、日本が諸外国と調和した形で連携して研究活動をしていくのに必要な事項を特定するのに活用できるよう、体系的・構造的にまとめる。

1.2.2 日本の大学・研究機関等への説明会・意見交換会の企画・運営

研究インテグリティに対する意識を醸成するとともに、課題等を抽出・整理することを目的に、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・運営を行う。

実施形式：オンライン

実施回数：4回

参加者数：最大500人

時間：1－1.5時間／回

登壇者：各回政府関係者と外部等の有識者

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

谷田 邦一 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

山本 智史 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、説明会の企画・運営は依田が、各国・地域の調査は依田・多田・谷田・山本が主として担当した。報告書のとりまとめと米国・EU の調査は依田が、英国の調査は多田が、豪州の調査は谷田が、カナダの調査は山本が担当した。

本調査の実施に当たっては、説明会に参加いただいた有識者の方々、内閣府の調査担当者にご協力を頂いた。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

トランプ前政権は、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、この文書や、その後の米国における取組においては、「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）」という言葉が、「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」に相当する意味を有した用語として使用されてきている[15]。

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」は 2022 年 2 月に終了している。

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」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を含んでいる。

米国議会の動きとしては、2021 年 1 月に 2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）が制定され、その第 223 条で、すべての連邦政府の

[15] 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。

資金配分機関が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する研究者に対して求めることが義務付けられた。また、2022 年 8 月に CHIPS and Science Act が成立した。この法律（2 部構成）は半導体インセンティブに 5 年間で 527 億ドルを計上（appropriation）、そのうち、先端研究開発に 110 億ドル計上すること等とともに、研究セキュリティに関する規定を含んでおり、「外国人人材採用プログラム」（Foreign Talent Recruitment Programs）についてのガイドライン策定、米国科学財団（National Science Foundation: NSF）に Research Security and Policy Office の設置、研究開発助成の申請時にリスク評価を NSF が実施する権限の付与、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、独立したリスク評価センターを設立すること、等の規定を含んでいる。

表 2-1、表 2-2 は、それぞれ研究インテグリティ関連の大統領府等、米国議会における主な動きの年表である。主なものについては以下で、要求と支援（どこからどのどこへ（連邦政府、資金配分機関、大学等研究機関、研究者）、どのような内容）に注目して説明する。

表 2-1：近年の研究インテグリティ関連文書（大統領府等）

発行年	文書名	発行元
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

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。

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

2.1.1 研究インテグリティの確保に関する要求と支援

本セクションでは、2021 年度[16]までの動きとして、(a) NSPM-33（2021 年 1 月）、(b) Recommended Practices（2021 年 1 月）、(c) 2021 年度国防授権法（2021 年 1 月）の第 223 条、(d) NSPM-33 実施ガイダンス（2022 年 1 月）について説明する。次に、2022 年度の動きとして、(a) CHIPS and Science Act（2022 年 8 月）、(b) OSTP による検討状況公表（2022 年 8 月）、(c) 全米アカデミーズ報告書「米国の技術優位を保護する」(2022 年 9 月)、(d) "Safeguarding Science" Toolkit の発表（2022 年 11 月）、(e) 研究セキュリティプログラムのドラフト公表（2023 年 2 月）について説明する。

(1) 2021 年度までの主な動き

(a) NSPM-33（2021 年 1 月 14 日）

2021 年 1 月 14 日に発出された「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」（*Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*）[17]の宛先は、大統領府レベルの 15 の連邦省庁（財務省、住宅都市開発省を除く）の長官に加え、行政管理予算局（OMB）の長、その他連邦政府独立省庁（環境保護庁、NASA、米国科学財団）の長、研究所等（NIH、スミソニアン協会）の長、さらに、情報機関の長（Director of National Intelligence（国家情報長官（DNI））、Director of CIA（中央情報局）、Director of FBI（連邦捜査局））、The Assistant to the President for National Security Affairs、そして本件取りまとめを担当する Office of Science and Technology Policy（大統領府科学技術政策局）の長が含まれる。研究開発を行う連邦省庁とともに、情報機関に対する指示となっていることが特色と言える。

NSPM-33 の Section 1 ではこの大統領覚書の目的として、「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ものである」とし、「残念ながら、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。」と説明する[18]。

---

[16] 本委託調査は 2022 年度以降の動きを中心に調査することとされており、ここでの 2021 年度までと、2022 年度以降の区分は日本の会計年度に基づく。

[17] 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 <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>

[18] "This memorandum directs action to strengthen protections of United States Government-

Section 2 では、以下の 7 つの用語の定義をしている：「米国研究開発事業への参加者」（“participants in the United States R&D enterprise”）、「米国政府支援研究開発」（“United States Government supported R&D”）、「利益相反」（“conflict of interest(s)”）、「責務相反」（“conflict of commitment(s)”）、「海外政府支援人材採用プログラム」（“foreign government-sponsored talent recruitment program”）、「連邦政府職員」（“Federal personnel”）、「デジタル永続的識別子」（“digital persistent identifier”）。このうち、「米国研究開発事業への参加者」の定義は「研究者（学術研究機関、独立研究機関、医療センター・研究所、民間企業、又は連邦政府センター・研究所）と、連邦研究開発資金の配分及び授与のプロセスに参加する者」[19]である。

Section 3（Roles and Responsibilities）からは大統領覚書の具体的な内容であり、Section 3 では、研究資金を提供する連邦省庁の長等に対する要求事項が列記されている。要求事項は以下のとおりである。

表 2-3：研究セキュリティ・インテグリティ確保のための連邦省庁への要求事項（NSPM-33, セクション 3)

※青は要求事項（連邦省庁に対する要求）、赤は支援事項（連邦資金を受けとる組織への支援）に関連。太字・下線は筆者によるもの。

連邦政府が資金提供する研究の設計・実施・報告・審査、あるいは資金提供に大きな影響を与える、米国研究開発事業の参加者に対して、本大統領覚書の Section 4（b）に沿った適切な**情報の開示を要求**し、適用される連邦法及び規則に基づき、利益相反及び責務相反の有無、どこで起こっているかを確実に判断できるようにする。[20]
連邦資金を受け取る組織が、潜在的な利益相反や責務相反を含む研究セキュリティとインテグリティに対するリスクを特定し管理するための**方針とプロセスを確立し管理**することを確実にするために、その組織に協力する。[21]

supported Research and Development (R&D) against foreign government interference and exploitation.”

“Unfortunately, some foreign governments, including the People’s Republic of China, have not demonstrated a reciprocal dedication to open scientific exchange, and seek to exploit open United States and international research environments to circumvent the costs and risks of conducting research, thereby increasing their economic and military competitiveness at the expense of the United States, its allies, and its partners”

[19] “researchers at academic research institutions, independent research institutes, medical centers and institutes, private companies, and Federal Government research centers and laboratories, as well as those who participate in the process of allocating and awarding Federal R&D funding”

[20] “require that participants in the United States R&D enterprise who significantly influence the design, conduct, reporting, reviewing, or funding of Federally-funded research disclose appropriate information, consistent with Sec. 4(b) of this memorandum, that will enable reliable determinations of whether and where conflicts of interest and commitment exist, consistent with applicable Federal laws and regulations”

[21] “cooperate with organizations receiving Federal funds to ensure that the organizations have established and administer policies and processes to identify and manage risks to research security and integrity, including potential conflicts of interest and commitment”

研究資金、研究セキュリティ、インテグリティに悪影響を及ぼす可能性のある開示を、各機関の監察官（Inspector General）や法執行機関と協力し、適用される法律と整合するように特定する。[22]
開示要求を順守していない疑いのある事例の調査において、必要に応じて各機関の監察官及び法執行機関と協力する。[23]
開示方針への違反や、米国の研究開発事業のセキュリティとインテグリティを脅かすその他の活動への関与に対し、適切かつ効果的な帰結があるようにし、それを適用する。[24]
国土安全保障長官は、国土安全保障省（DHS）が国務省と連携し、米国の研究開発事業に参加・参画しようとする非移民学生及び交換訪問者の外国人個人を国家安全保障上のリスクについて確かに審査する責任がある。国土安全保障長官は、教育及び文化交流プログラムのために米国に来る外国人の合法的な入国と滞在を支援しながら、国家の安全を守るために、留学生及び研究者に関する情報を DHS が保持することを、適用法に沿って確実に行う責任がある。[25]
国家情報長官（DNI）は、米国の研究開発事業の安全保障に関連するような、外国アクターの能力、活動、意図を特定し評価するための情報コミュニティの取組を調整する。[26]
科学技術政策局（OSTP）長官は、米国科学技術会議（National Science and Technology Council: NSTC）を通じて、連邦政府資金による研究開発を外国政府の干渉から守るための活動と、研究セキュリティに対するリスクとこれらのリスクに対応する連邦政府の行動に対する認識を高めるための米国の科学界及び学術界への働きかけを調整する。[27]

[22] “identify, in cooperation with agency Inspectors General and law enforcement agencies as appropriate and as consistent with applicable law, disclosures that have the potential negatively to impact research funding, security, or integrity”
[23] “cooperate with agency Inspectors General and law enforcement, as appropriate, in investigation of suspected instances of failure to comply with disclosure requirements”
[24] “ensure the availability and application of appropriate and effective consequences for violations of disclosure policies and for engagement in other activities that threaten the security and integrity of the United States R&D enterprise.”
[25] “The Secretary of Homeland Security is responsible for ensuring that DHS, in conjunction with the Department of State, screens foreign individuals who are nonimmigrant students and exchange visitors seeking to participate or participating in the United States R&D enterprise for national security risks. The Secretary of Homeland Security is also responsible, consistent with applicable law, for ensuring that DHS maintains information regarding foreign students and researchers to protect national security while supporting lawful entry and stay of foreign individuals coming to the United States for educational and cultural exchange programs.”
[26] “The Director of National Intelligence (DNI) shall coordinate Intelligence Community efforts to identify and assess the capabilities, activities, and intentions of foreign actors as they relate to the security of the United States R&D enterprise.”
[27] “The Director of the Office of Science and Technology Policy (OSTP), through the National Science and Technology Council (NSTC), shall coordinate activities to protect Federally funded R&D from foreign government interference, and outreach to the United States scientific and academic communities to enhance awareness of risks to research security and Federal Government actions to address these risks.”

Section 4（Priorities）では、より具体的に、8 項目（「(a) 研究セキュリティリスクと保護への認識向上」、「(b) 情報開示の要件とプロセスの強化」、「(c) アクセス及び参加制限」「(d) 外国人留学生・研究者の審査」、「(e) 情報の共有」、「(f) 研究セキュリティ教育」、「(g) リスクの特定と分析」、「(h) 国際的な研究開発協力の推進と保護」）のそれぞれについて、連邦省庁・資金配分機関に対して求める事項が記載されている。具体的内容は、それぞれ以下のとおりである。

① 研究セキュリティのリスクと保護に関する認識の向上[28]

表 2-4：研究セキュリティのリスクと保護に関する認識の向上に関する事項（NSPM-33，セクション 4 (a)）

※赤は支援事項（連邦研究資金を受けとる組織等への支援）に関連。

要求相手機関	内容
大統領府科学技術政策局の長	DNI 及び必要に応じて他の連邦省庁の長と連携し、米国の研究開発事業に関与して、**研究セキュリティ及び研究インテグリティへのリスク、及びこれらのリスクを軽減するための政策や手段についての認識を高める**。[29]
国家情報長官（DNI）	他の連邦省庁の長と連携し、適用する法に従い、他の省庁、連邦・州・地方政府職員、研究機関、民間セクター、同盟国・パートナーへの普及に適した**研究セキュリティに関する情報・情報成果物を作成**する。[30]

[28] “Enhance Awareness of Research Security Risks and Protections”

[29] “in coordination with the DNI and heads of other agencies as appropriate, shall engage with the United States R&D enterprise to enhance awareness of risks to research security and integrity and policies and measures for mitigating these risks.”

[30] “develop, in coordination with the heads of other agencies, information and intelligence products related to research security that are suitable for dissemination, in accordance with applicable law, to other agencies; to Federal, State, local, and tribal officials; to research institutions; the private sector; and to allies and partners.”

② 情報開示の要件とプロセスの強化[31]

表 2-5：情報開示の要件とプロセスの強化に関する事項（NSPM-33，セクション 4 (b)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）、赤は支援事項（連邦研究資金を受けとる組織等への支援）に関連。

要求相手機関	内容
資金配分機関の長	連邦政府資金による研究開発事業の参加者に対して、潜在的な利益相反・責務相反に関連する**情報の開示を要求**する。[32]
連邦省庁	連邦政府資金による研究開発事業の以下の**関係者**からの情報開示を要求する。 ・連邦政府の研究開発資金を求める、あるいは受け取る主任研究者（PI）及びその他のシニア／キーパーソン。 ・連邦政府研究費の配分プロセスに参加する個人：プログラムオフィサー、査読者、諮問委員会・パネルのメンバー。 ・連邦機関の研究所及び施設の研究者（すなわち、連邦政府に雇用されているか否かを問わず、内部の研究者）（政府所有請負業者運営（GOCO）の研究所・施設を含む）。[33]
連邦省庁	**以下の開示を要求**する。 ・所属及び雇用 ・その他の支援及び資金源 ・海外のプログラム及び契約（「外国政府主催の人材採用プログラム」を含む） ・役職及び任命[34]
資金配分機関の長	【12 か月以内】に下表の情報の開示を求める方針を作成する。[35]（→図 2.1）

[31] “Strengthen Disclosure Requirements and Processes”

[32] “require the disclosure of information related to potential conflicts of interest and commitment from participants in the Federally funded R&D enterprise.”

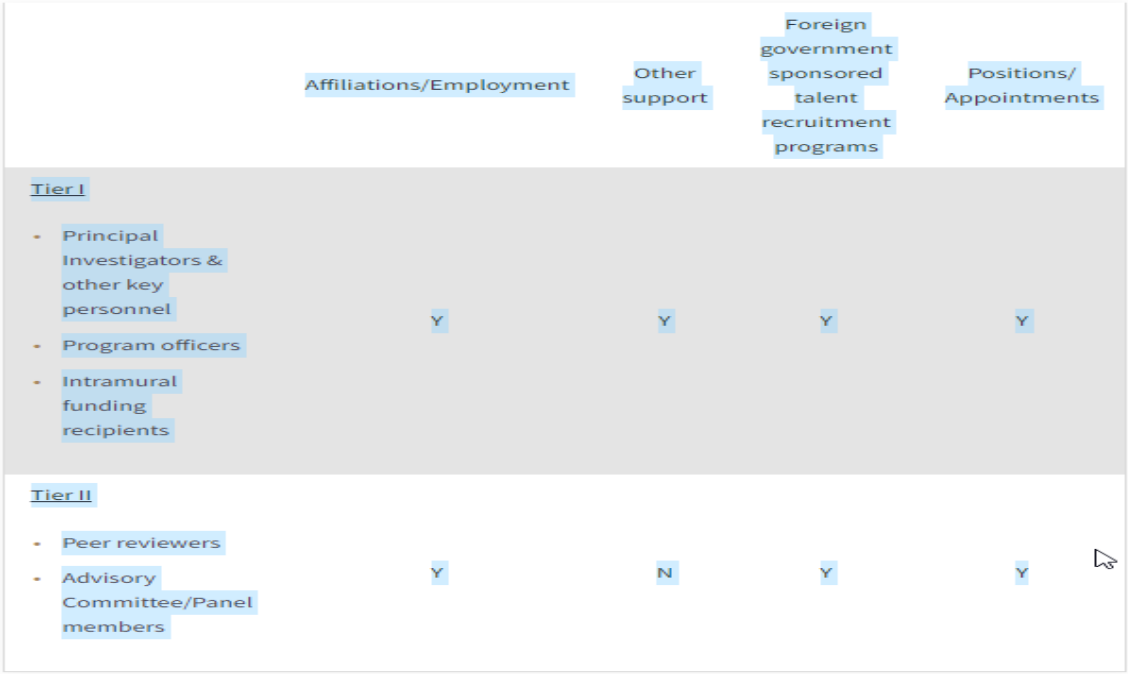
[33] “require disclosure from the following segments of the Federally funded R&D enterprise:
- Principal investigators (PIs) and other senior/key personnel seeking or receiving Federal R&D funding (i.e., extramural funding);
- Individuals participating in the process of allocating Federal funding: program officers, peer/merit reviewers, and members of advisory panels and committees; and
- Researchers at Federal agency laboratories and facilities (i.e., intramural researchers, whether or not Federally employed), including government owned, contractor-operated laboratories and facilities.”

[34] “require the following disclosures, : Affiliations and employment; Other support and funding sources; Foreign programs and contracts（including foreign government-sponsored talent recruitment programs）; and Positions and appointments”

[35] “establish policies requiring disclosure of the information reflected in the table below”

要求相手機関	内容
連邦省庁	初回の情報開示と、開示された**報告の更新**を求める。[36]
資金配分機関	【1 年以内】に連邦研究助成金の支援を受け、あるいはそれに従事する個々の研究者が、その個人の**永続的デジタル識別子**（digital persistent identifier）を提供するサービスに登録する要件に関する方針を作成する[37]。 **[Implementation Guideline (2022/1)で実施細目②を決定（後述）]**
資金配分機関	可能な限り、資金配分機関間で**開示プロセス、定義、書式を標準化**する。[38] **[Implementation Guideline (2022/1)で実施細目①を決定（後述）]**
行政管理予算局の長	OSTP、政府倫理局（Office of Government Ethics）、その他の機関と協力し、利益相反や責務相反の開示に関連する**方針と書式の標準化**を調整する。[39]
教育省長官	高等教育法第 117 条[40]の施行を通じて、**高等教育機関と海外との関係における財政的透明性**を促進することにより、学問の自由と国家安全保障との間のバランスを取ることを引き続き支援する。[41]
連邦省庁	開示要件に対する**潜在的な違反を特定し調査する仕組みと能力を強化**する（そのために、監察官、法律顧問、法執行機関、大学のプログラムオフィスやセキュリティ担当者、民間部門と協力する）。[42]
連邦省庁	**開示要件違反、及び研究セキュリティとインテグリティを脅かすその他活動への関与**に対して、**適切かつ効果的な帰結**を確かなものにする。[43] **[Implementation Guideline (2022/1)で実施細目③を決定（後述）]**

[36] “require initial disclosures and updates to disclosure reporting”
[37] “stablish policies regarding requirements for individual researchers supported by or working on any Federal research grant to be registered with a service that provides a digital persistent identifier for that individual.”
[38] “standardize disclosure processes, definitions, and forms across funding agencies to the extent practicable.”
[39] “work with OSTP, the Office of Government Ethics, and other agencies to coordinate the standardization of policies and forms related to disclosure of conflicts of interest and commitment.”
[40] 総額で 25 万ドル以上の贈与又は契約を海外から受け取っている高等教育機関は教育省に報告する必要がある。
[41] “continue to support the balance between academic freedom and national security by promoting financial transparency in the relationship between institutions of higher education (IHEs) and foreign sources through enforcement of section 117 of the Higher Education Act.”
[42] “strengthen mechanisms and capabilities to identify and investigate potential violations of agency disclosure requirements（そのために work with their Inspector General, General Counsel, law enforcement, university program offices and security officers, and the private sector）.”
[43] “ensure appropriate and effective consequences for violation of disclosure requirements and engagement in other activities that threaten research security and integrity”



	Affiliations/Employment	Other support	Foreign government sponsored talent recruitment programs	Positions/ Appointments
Tier I - Principal Investigators & other key personnel - Program officers - Intramural funding recipients	Y	Y	Y	Y
Tier II - Peer reviewers - Advisory Committee/Panel members	Y	N	Y	Y

図 2-1：資金配分機関の長が開示を求める情報（12 か月以内に方針を作成）

③ アクセス及び参加の制限

表 2-6：アクセス及び参加の制限に関する事項（NSPM-33，セクション 4 (c)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
連邦省庁の長	米国政府の研究施設へのアクセスと利用を管理・追跡する方針とプロセスを各機関が持つようにすること。[44]
連邦省庁の長	【12 か月以内】に、米国研究開発事業の参加者であり、それぞれの機関に現在雇用されている連邦職員が「外国政府主催の人材採用プログラム」に参加することを禁止する方針を定めるか、又は適用可能な既存の方針を明確化すること[45]、など。

[44] “ensure that their respective agencies have policies and processes to control and track access to and utilization of United States Government research facilities”

[45] “establish policies, or clarify existing policies where applicable, that prohibit Federal personnel currently employed by their respective agencies who are also participants in the United States R&D enterprise from participating in foreign government-sponsored talent recruitment programs.”

④ 外国人留学生・研究者の審査

表 2-7：外国人留学生・研究者の審査に関する事項（NSPM-33，セクション 4 (d)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
国務省長官 （国土安全保障省長官と調整）	留学生や研究者の審査プロセスが、米国の研究開発に対するリスクの性質の変化を反映するようにすること。[46]
国務省長官	米国での留学や研究活動を希望するビザ申請者の審査に、ビザ資格に適用されるすべての基準に基づき、リスクに基づくプロセス（risk-based process）を適用する。[47] 米国法に基づく関連基準に基づき、ビザ申請の審査に関連する場合において、領事がビザ申請者に関わる以下の情報を収集し考慮できるよう、必要な措置を講じる。 ・雇用及び職歴 ・経済的支援源 ・教育歴（教育機関、学位、研究指導教官を含む）。 ・現在及び過去の研究開発提携及びプロジェクト。 ・外国政府主催の人材採用プログラムへの現在及び申請中の参加状況。 ・学習・研究のプログラム ・予定されている業務の施設と場所。[48]
国土安全保障省長官	【3 か月以内】に、関連機関に対して以下を実施することを要求するために必要な規制と技術の更新を評価する。 ・留学生・交流訪問者情報システム（SEVIS）において、報告対象となる留学生及び研究者について、Section(d)(i)で規定された情報（※本表上記の情報）を報告すること。 ・SEVIS の更新を毎年、あるいは適切な場合にはより頻繁に行う。[49]

[46] “ensure that vetting processes for foreign students and researchers reflect the changing nature of the risks to United States R&D.”
[47] “apply a risk-based process to vet visa applicants seeking to study or conduct research activities in the United States, based on all applicable standards for visa eligibility.”
[48] “The Secretary shall take such steps as are necessary to ensure consular officers may collect and consider the following information pertaining to visa applicants, wherever relevant to the consular officer’s adjudication of a visa application based on relevant standards under United States law: Employment and employment history; Sources of financial support; Education history, including academic institutes, degree(s), and research advisor(s); Current and prior R&D affiliations and projects; Current and pending participation in foreign government-sponsored talent recruitment programs; Program of study and/or research; and Facility/facilities and location(s) of expected work.”
[49] “assess, within 3 months of the date of this memorandum, any regulatory and technical updates

要求相手機関	内容
	【上記の評価後、3 か月以内】に、国家安全保障担当大統領補佐官（APNSA）に対し、当該要件の実施に関する計画を提供する。[50]
国土安全保障省長官（国務省長官と調整）	【1 年以内】に、検索可能な中央データベースに Section 4 (d)(i)に規定された情報（※本表上記の情報）を含めることの実現可能性と有用性を評価する。[51]

⑤ 情報の共有（Information Sharing）

表 2-8：情報の共有に関する事項（NSPM-33，セクション 4 (e)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
連邦省庁の長	違反者に関する情報を、連邦資金配分機関全体、連邦法執行機関、国土安全保障省、州と共有する。 重大な懸念が生じたが最終決定がなされていない場合においては、他の連邦資金配分機関に通知することを検討する。[52] **[Implementation Guideline (2022/1)で実施細目④を決定（後述）]**

⑥ 研究セキュリティ教育

表 2-9：研究セキュリティ教育に関する事項（NSPM-33，セクション 4 (f)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	要求内容
資金配分機関の長	研究開発活動を行う、又は連邦研究開発資金の配分プロセスに参加する連邦機関の職員が、研究セキュリティのトレーニングを受けることを確実にする。[53]

necessary to require that relevant institutions:

- Report the same information specified above in section 4(d)(i) in the Student and Exchange Visitor Information System (SEVIS), for foreign students and researchers subject to reporting in that system; and,
- Provide updates in SEVIS annually, or more frequently where appropriate."

[50] "provide to the APNSA a plan regarding implementation of such requirements."

[51] "assess the feasibility and utility of including the information specified in section 4(d)(i) in a searchable centralized database."

[52] "share information about violators across Federal funding institutions and with Federal law enforcement agencies, the DHS, and State", "consider providing notice to other Federal funding institutions in cases where significant concerns have arisen but a final determination has not yet been made."

[53] "ensure that Federal agency personnel conducting R&D activities or participating in the process of allocating Federal R&D funding receive research security training."

⑦ リスクの同定と分析（Risk identification and analysis）

表 2-10：リスクの同定と分析に関する事項（NSPM-33，セクション 4 (g)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
資金配分機関の長	【12 か月以内】 年間 5,000 万ドルを超える連邦科学技術助成金を受ける研究機関は、「研究セキュリティプログラム」を確立し運営していることを資金配分機関に対して証明することを義務付ける。[54] 「研究セキュリティプログラム」には、サイバーセキュリティ、海外渡航セキュリティ、インサイダー脅威の認識と特定、及び必要に応じて輸出管理トレーニングの要素が含まれるべきである。[55] 米国の国家安全保障や経済安全保障に影響を与える重要な新興技術分野の研究開発で連邦資金を受ける機関には、研究セキュリティプログラムの追加要件が適切かどうか検討する。[56] **[Implementation Guideline (2022/1)で実施細目⑤を決定（後述）]**

⑧ 国際研究開発協力の促進と保護

Promote and Protect International R&D Cooperation

表 2-11：国際研究開発協力の促進と保護に関する事項（NSPM-33，セクション 4 (h)）

※青は要求事項（連邦省庁・資金配分機関に対する要求）に関連。

要求相手機関	内容
国務省長官（OSTP の長と他の連邦省庁の長と調整）	研究セキュリティに対するリスクに対する認識を高め、国際的な保護と対応努力に関する協力を改善する政策と実践を促進する目的で、外国の同盟国やパートナーと協力する。[57]

[54] “require that research institutions receiving Federal science and engineering support in excess of 50 million dollars per year certify to the funding agency that the institution has established and operates a research security program.”
[55] “Institutional research security programs should include elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training.”
[56] “consider whether additional research security program requirements are appropriate for institutions receiving Federal funding for R&D in critical and emerging technology areas with implications for United States national and economic security.”
[57] “engage with foreign allies and partners with the goal of promoting policies and practices that increase awareness of risks to research security and improve cooperation on international protection and response efforts.”

Section 5

国家安全保障担当大統領補佐官は、行政管理予算局長、OSTP の長と協力して、この大統領覚書の実施を調整し、毎年、この大統領覚書を実施するために資金配分機関がとった活動の詳細を記した報告書を作成し、大統領に提出しなければならない、としている。

（ただし、年次報告書の公表はこれまでのところ行われていない）

(b) 米国の科学技術研究事業体のセキュリティとインテグリティを強化するための Recommended Practices（2021 年 1 月 19 日）

上記の大統領覚書が出されたのとほぼ同じ時期に、「アメリカの科学技術研究事業のセキュリティとインテグリティを強化するために推奨される実践内容」（Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise）が、米国科学技術会議（NSTC）の「研究環境に関する NSTC 合同委員会」（Joint Committee on the Research Environment）の「研究セキュリティ小委員会」（Subcommittee on Research Security）から公表された。[58]

研究セキュリティ小委員会は、図 2-2 のメンバーであり、上記の大統領覚書の宛先となっていた大統領府レベルの省庁、研究開発に関係する省庁、さらに、情報コミュニティの機関も含む。Subcommittee on Research Security の目的は、「米国の科学技術研究事業のセキュリティとインテグリティを、米国の価値観やイノベーションエコシステムの開放性を損なうことなく強化するために、連邦政府の取組を調整すること」である。特に、「適切かつ効果的なリスク管理の調整、学術研究機関への効果的なコミュニケーションとアウトリーチの提供に関する連邦政府の取組の調整、連邦政府が出資する研究事業のセキュリティとインテグリティに関する研究機関向けのガイダンスの作成、学術研究機関向けの推奨事例の作成に焦点を当てている」と説明している。(p.i)

[58] 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.

SUBCOMMITTEE ON RESEARCH SECURITY

Co-Chairs

Steve Binkley, Department of Energy
Helena Fu, Office of Science and Technology Policy
Rebecca Keiser, National Science Foundation
Mike Lauer, National Institutes of Health
Aaron Miles, Office of Science and Technology Policy

Members

Departments
Department of Agriculture
Department of Defense
Department of Education
Department of Energy
Department of Homeland Security
Department of Justice
Department of State
Department of Transportation

Agencies
Federal Bureau of Investigation
Food and Drug Administration
National Aeronautics and Space Administration
National Institute of Standards and Technology
National Institutes of Health
National Oceanic and Atmospheric Administration
National Science Foundation
National Security Agency
Office of the Director of National Intelligence
United States Geological Survey
United States Patent and Trademark Office

Executive Office of The President
National Security Council
Office of Management and Budget
Office of Science and Technology Policy

出典：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. p.i.

図 2-2：Subcommittee on Research Security（National Science and Technology Council の Joint Committee on the Research Environment に属する）のメンバー

本文書の目的は、「研究機関（大学、研究機関、民間企業等）が米国の研究事業のセキュリティとインテグリティをより良く保護するために取るべき推奨事項を提示すること」であり、「NSPM-33 を補完するもの」であると説明している(p.1)。

本文書を参考にして、大学・研究機関は研究セキュリティとインテグリティの向上に取り組むことができるものであり、連邦政府から大学・研究機関への一つの支援とみることができる。

本文書では、まず、研究セキュリティとインテグリティを向上させるに当たっての「基本原則と価値」（Foundational principles and values）について説明する。以下がその内容である。これらのうちで、「開放性」、「透明性」、「説明責任」は、研究者個人から研究機関、政府まで、すべてに関係するものであり、「公平性」、「客観性」、「正直さ」、「尊重」は、個人や組織が研究の厳密性と再現性を確保するためにどのように研究を行うべきかの核心となるものであると説明する。「探求の自由」、「互恵主義」、「実力主義的な競争」は、すべての人に関係し、特に政府が保護し育成する責任があるものである、と説明する。

- 開放性（openness）と透明性（transparency）は、生産的な協力を可能にし、潜在的な利益相反・責務相反を適切に開示するのに役立つ。

- 説明責任（accountability）と正直さ（honesty）は、誤りを認め、進歩を妨げかねない行動を正すのに役立つ。
- 公平性（impartiality）と客観性（objectivity）は、不適切な影響や科学的知識の歪曲から守る。
- 尊敬の念（respect）は、全ての人の意見を聞き、貢献できる環境づくりに役立つ。
- 探求の自由（freedom of inquiry）は、個人の好奇心が科学的発見につながるようにする。
- 互恵主義（reciprocity）とは、科学者や研究機関が、全ての協力パートナーに利益をもたらす方法で、材料、知識、データ、施設や自然の場所へのアクセス、及びトレーニングを交換することを確実にするものである。
- 実力主義的な競争（merit-based competition）は、最高のアイデアやイノベーションが前進できるような公平な競争の場を確保するのに役立つ。(p.2)

なお、上の説明で「利益相反」「責務相反」については以下のように定義している（p.2）。

「利益相反」：個人、又は個人の配偶者や扶養家族が、研究の設計、実施、報告、又は資金調達に直接かつ重大な影響を与える可能性のある金銭的利害又は関係を持っている状況[59]。

「責務相反」：複数の雇用主又は他の事業体の間で、個人が矛盾する義務を受け入れたり、負ったりする状況。多くの組織の方針では、組織や資金提供機関の方針や約束を越えて時間を割く義務など、相反する時間の約束を「責務相反」と定義している。雇用主や研究助成機関と不適切に情報を共有したり、情報を隠したりする義務など、その他の種類の矛盾した義務も、研究のセキュリティとインテグリティを脅かす可能性があり、より広い意味での「責務相反」の一要素である。[60]

「これらの基本原則や価値観に反する行動は、研究事業のインテグリティを危うくする。研究事業のインテグリティを脅かす行為は、しばしば研究事業のセキュリティ（研究セキュリティ）に対するリスクももたらす」[61]と説明している。(p.3)

表 2-12 は、研究セキュリティとインテグリティを強化するために推奨される実践内容の 21 項目を示す。文書では各項目について、2～3 段落程度の説明が付されている。

---

[59] "a situation in which an individual, or the individual's spouse or dependent children, has a financial interest or relationship that could directly and significantly affect the design, conduct, reporting, or funding of research."

[60] "a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many organizational policies define conflicts of commitment as conflicting commitments of time, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to share information improperly with, or to withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment."

[61] "Behaviors that violate these foundational principles and values jeopardize the integrity of the research enterprise. Behaviors that threaten the integrity of the research enterprise often also pose risks to the security of the research enterprise, which we term research security." (p.3)"

表 2-12：研究セキュリティとインテグリティを強化するために推奨される実践内容

組織的なリーダーシップと監督機能の発揮
1. 研究のセキュリティとインテグリティの重要性を組織の指導層から伝える。
2. 研究セキュリティに対する組織的なアプローチを確保する。
3. 研究セキュリティとインテグリティのワーキンググループやタスクフォースを設置する。
4. 包括的な研究セキュリティプログラムを確立し、運用する。
開放性と透明性への期待を確立する。
5. 利益相反、責務相反、情報開示に関する組織方針を定め、運用する。
6. 潜在的な利益相反や責務相反を特定し、評価するために必要なすべての情報を組織に開示することを義務付ける。
7. 留学生や外国人研究者の情報を報告するための国土安全保障省の要求事項の遵守を徹底する。
8. 永続的デジタル識別子に関する方針を定める。
9. 外国からの贈与や契約を報告するための要件に確実に準拠する。
トレーニング、支援、情報の提供・共有
10. 研究事業の参加者に対して、責任ある研究の実施に関する研修を実施する。
11. 外国政府主催の人材採用プログラムへの参加を検討している者にガイダンスを提供する。
12. 研究セキュリティを強化するために、FBI 地方事務所と協力する。
13. 研究セキュリティとインテグリティに対するリスクを示す可能性のある状況や行動に対する認識を高め、それに対する保護策を講じる。
14. 情報開示に関するポリシーに違反する可能性がある場合、その情報を共有する。
組織の方針を遵守するための効果的なメカニズムを確保する。
15. 研究セキュリティとインテグリティを脅かす情報開示方針違反やその他の行為を発見するための効果的な手段を確立し、行使する。
16. 開示義務違反や研究セキュリティとインテグリティを脅かすその他の行為に対して、適切かつ効果的な帰結があることを保証する。
17. 雇用契約には、研究セキュリティとインテグリティを支援する条項を盛り込む。
共同研究及びデータに関連する潜在的なリスクの管理
18. 正式な研究パートナーシップを評価するための一元的な審査・承認プロセスを確立する。
19. 海外渡航の審査と指導のためのリスクベースのセキュリティプロセスを確立し、運用する。
20. 外国人訪問者及び客員研究者に関連する潜在的なリスクを管理する。
21. 効果的なデータセキュリティ対策を確立し、維持する。

出典：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. pp.6-15.

(c) 2021 年度国防権限法（National Defense Authorization Act: NDAA）（2021 年 1 月）

2021 年 1 月 1 日に 2021 年度国防権限法（FY 2021 National Defense Authorization Act (NDAA)）が制定され、その第 223 条（42 U.S.C. § 6605（Disclosure of funding sources in applications for Federal research and development awards）として法編纂）で、すべての連邦研究機関（資金配分機関）が申請プロセスの一環として現在及び未決（pending）の支援についての情報開示を申請する研究者から求めること等が義務付けられた。

申請者は、過去 3 年間に受けた、又は現在受けている、又は申請中（未決）の外国政府や外国組織からの資金提供や支援をすべて開示しなければならない。申請者は、自分自身や共同研究者が外国政府や外国組織から受けた、又は現在受けている、任命や称号、職位や役職をすべて開示しなければならない。開示された情報は、連邦政府のデータベースに保存される。開示義務違反が発覚した場合には、連邦政府は助成金の支払いを停止したり、返還を求めたりすることができる。

表 2-13：2021 年度国防権限法第 223 条「連邦研究開発アワード（awards）への申請書における資金源の開示」

※青は要求事項（連邦省庁・資金配分機関等に対する要求）。

(a)　開示要求（Disclosure requirement）

要求相手	要求内容
連邦研究機関	各連邦研究機関は、当該機関からの研究開発アワードの申請書の一部として、以下を要求するものとする。
研究者（提案者）	(1)申請書に記載された、研究に参加する個人が (A)開示時点において、個人が受けている、又は受けると予想される、現在及び未決のすべての研究支援の金額、種類、及び提供元を開示すること。 (B)開示が現在、正確かつ完全であることを証明すること。 (C)支援の授与前に機関の要請があった場合、及び授与期間中に機関が適切と判断した場合に、当該開示を更新することに同意すること。
研究者を雇用するエンティティ	(2)当該アワードを申請するエンティティは、当該エンティティに雇用され、申請書に記載された各対象者が、第(1)項に基づく要件を知らされていることを証明すること。

注）「連邦研究機関」（federal research agency）とは、年間の外部研究費が 1 億ドルを超える連邦機関（研究資金配分機関）をいう。アワードは助成金（grant）、契約（contracts）、研究協力（cooperative agreement）を含む。エンティティは大学や研究機関を通常は意味する。

(b) 一貫性（Consistency）

要求相手	要求内容
科学技術政策局長	科学技術政策局長（Director of the Office of Science and Technology Policy）は、国家科学技術会議（National Science and Technology Council）を通じて行動し、2020 会計年度国防権限法（公法 116-92 ; 42 U.S.C. 6601）1746 条(a)に基づく権限[62]に従い、(a)項に基づき連邦研究機関が発する要件に一貫性があることを確保する。

(c) 強制執行（Enforcement）

要求相手	要求内容
連邦研究機関	(1) 連邦研究機関は、第(a)項に基づき個人が開示した現在及び未決の研究支援が、連邦法又は機関の条件に違反する場合、研究開発アワードの申請を却下することができる。 (2) 研究開発賞に対する事業体の申請書に記載された対象個人が、(a)項に基づく情報の開示を故意に怠った場合、連邦研究機関は、以下の措置の 1 つ以上を講じることができる。 (A) 申請を却下する。 (B) 当該機関が当該個人又はエンティティに授与した研究開発アワードを一時停止又は終了させる。 (C) 当該個人又は団体に対する当該機関からの一切の資金提供を一時的又は永久的に中止する。 (D) 連邦規則集第 2 編第 180 部（part 180 of title 2, Code of Federal Regulations）、後継規則、又は他の適切な法律や規則に従って、個人又は団体を政府資金の受領から一時的又は永久に停止又は免除する。 (E) 第(a)項に基づく開示の不履行について、さらなる調査のために関係省庁の監察官に、又は刑事法もしくは民事法に違反したかどうかを調べるために連邦法執行当局に照会する。 (F) 他の機関に警告するために、個人又はエンティティをコンプライアンス違反として「連邦アワード受領者パフォーマンス・インテグリティ情報システム」（Federal Awardee Performance and Integrity Information System）に登録する。 (G) 個人又はエンティティに対して、適用される法律又は規則の下で許可されるその他の措置をとる。

[62] 2020 年度国防権限法（FY 2020 National Defense Authorization Act (NDAA)）第 1746 条で OSTP が主導し、NSTC に米国科学技術へ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の設置すること、OSTP は検討の調整をすること等とされている。

	(3) 第(2)項に記載された強制措置は、以下の場合にのみ、エンティティに対して講じることができる。 (A) エンティティが第(a)項(2)の要件を満たしていない。 (B) エンティティは、対象個人が第(a)(1)項に基づく情報の開示を怠ったことを知りながら、申請書が提出される前に当該非開示を是正するための措置を講じなかった。 (C) 当該連邦研究機関の長が以下のように決定する。 (i) そのエンティティは、対象となる個人によって所有、支配、又は実質的に影響を受けている、及び (ii) 当該個人が、故意に第(a)(1)項に基づく情報の開示を怠った。 (4) 通知 (1)又は(2)に基づく措置を講じようとする連邦研究機関は、可能な限り、連邦規則集 2 巻 180 部、後継規則、又はその他の適切な法律もしくは規則に従って、当該措置の対象となる各個人又はエンティティに、当該措置の具体的な理由を通知し、当該個人及び団体に、提案された措置に異議を申し立てる機会及び手続きを提供しなければならない。 (5) 証拠となる基準 第(2)項(D)に基づき資格停止又は剥奪を求める連邦研究機関は、連邦規則集第 2 編第 180 部、後継規則、又はその他の適切な法律又は規則に定められた手続き及び証拠基準に従うものとする。

注)「連邦規則集第 2 編第 180 部（part 180 of title 2, Code of Federal Regulations）」は、OMB Guidelines to Agencies on Governmentwide Debarment and Suspension (Nonprocurement)である。
出典）Cornell Law School. Legal Information Institute. 42 U.S. Code § 66–5 - Disclosure of funding sources in applications for Federal research and development awards <https://www.law.cornell.edu/uscode/text/42/6605>に基づき作成。

(d) NSPM-33 実施ガイダンス（2022 年 1 月 4 日）

2022 年 1 月 4 日、NSPM-33 を実施するためのガイダンスを発表した（*Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-Supported Research and Development*）。公表したのは、前術の文書と同じく、米国科学技術会議（NSTC）の「研究環境に関する NSTC 合同委員会」（Joint Committee on the Research Environment）の研究セキュリティ小委員会（Subcommittee on Research Security）である。[63]

[63] National Science and Technology Council. *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States*

本文書の目的は、「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(p.i)、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 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帰結、4. 情報の共有、5. 研究セキュリティプログラム）におけるより詳細なガイダンスを含む（p.ix)。

NSTC の議長であり、科学技術に関する大統領補佐官、かつ OSTP の長である Dr. Eric Lander は、前文で以下のように本文書の位置づけ、今後の課題について説明している（p.x～xi)。

- 我々が直面している研究セキュリティ上の課題は現実的かつ深刻であり、中国政府を含む一部の外国政府は、我々の最先端技術を不正に取得しようと懸命に努力している。これは容認できない。
- この実施指針は、私が 2021 年 8 月に打ち出した原則、すなわち、米国のセキュリティと開放性を守ること、善意の研究者が容易かつ適切に遵守できるよう明確にすること、政策が外国人嫌悪や偏見を助長しないようにすることを反映したものである。しかし、これらの重要な目標を達成するためには、まだまだやるべきことがある。
- 次の段階として、私は現在、連邦研究機関に対し、今後 120 日以内に、あらゆる連邦研究助成機関が使用できる（必要に応じて修正する）モデル助成金申請書と説明書（model grant application forms and instructions）を共同で開発するよう指示している。その目的は、政府が知るべきことを明確に記述し、研究者がどの資金配分機関に申請するかにかかわらず、可能な限り同じ情報を同じ方法で報告できるようにすることである。
- NSPM-33 に関する現在の取組は、研究者が連邦政府に情報を開示する方法を明確にし、簡素化しようとするものであるが、NSPM-33 の実施に関する他の重要な課題、すなわち、政府が研究資金や支援に関する決定を下す際にこの情報をどう利用するのかについては対処されていない。そのような課題も同様に重要であり、OSTP は将来的にそれらに対応するつもりである。

なお、このガイダンスでは、”research organization（研究組織）”、”federal research agency（あるいは research agency）（連邦研究省庁又は研究省庁）”について以下のように定義している。

”research organization”：「連邦研究機関に研究開発助成を申請した、又は助成を受けた事業体。この用語は、2021 年 NDAA（国防受権法）第 223 条に定義される「事業体」と同じ意味である。」[64]

Government-Supported Research and Development. A Report by the Subcommittee on Research Security, Joint Committee on the Research Environment. January 2022. <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>

[64] “An entity that has applied for or received an R&D award from a Federal research agency. This term has the same meaning as “entity” as defined in Section 223 of the NDAA for 2021.”

”federal research agency（research agency）”:「年間 1 億ドル以上の外部研究費を有する連邦省庁。この用語は、NSPM-33 の「資金配分機関」と同じ意味を持つ。」[65]

①情報開示の要件と標準化（Disclosure requirements and standardization）

・NSPM-33 の関連箇所は、Section 4(b)である。

・ガイダンスの目的は、「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、認証、裏付け文書の提供など）、及び省庁横断的な統一性の期待度について明確にする」ことである。

・以下の 15 項目の実施ガイダンスについて説明している[66]。なお、1.と 2.については標準化により、申請者の負担を軽減するという意味で「支援」とここでは分類している。

表 2-14：「情報開示の要件と標準化」についての実施ガイダンス項目

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

項目内容	要求元	要求先
1. 開示要求事項の標準化	―	連邦省庁
2. 開示様式・書式の標準化	―	連邦省庁
3. 査読者・諮問委員会委員の所属・役職の開示要件	連邦省庁	査読者等
4. 学生を含める開示要件の拡大の可能性	―	連邦省庁
5. 研究開発助成の申請プロセス（助成及び助成後の要素を含む）において要求される Tier I 開示要件に関連する情報収集	―	連邦省庁

[65] Any Federal department or agency with an annual extramural research expenditure of over $100,000,000. This term has the same meaning as “funding agency” in NSPM-33.

[66] 1. Standardization of disclosure requirements
2. Standardization of disclosure forms and formats
3. Requirements for peer reviewer and advisory committee member disclosure of affiliations and positions
4. Potential broadening of disclosure requirement to include students
5. Collection of information associated with the required Tier I disclosure requirements within R&D award application processes (including pre-award and post-award elements)
6. Collection of information related to financial conflicts of interest within R&D award application processes
7. Exclusions from disclosure requirements within R&D award application processes
8. Clarification regarding exclusion of gifts from disclosure requirements
9. Requirements for disclosing core facilities and shared equipment
10. Requirements for disclosing participation in foreign programs
11. Requirements for disclosure of foreign contracts to research agencies
12. Just-in-time submission of application information
13. Requirements for updating disclosures after an award has been made
14. Process(es) for individuals to correct inaccurate or incomplete submissions
15. Requirements and processes for research organizations applying for R&D awards to provide certification related to disclosure requirements

項目内容	要求元	要求先
6. 研究開発助成の申請手続きにおける利益相反に関連する情報収集	連邦省庁	研究組織
7. 研究開発助成申請プロセスにおける開示要求事項の適用除外	―	連邦省庁
8. 贈答（gifts）を開示対象外とすることについての明確化	―	連邦省庁
9. 中核施設及び共用設備の開示要件	連邦省庁	研究者
10. 海外プログラムへの参加に関する開示要件	連邦省庁	研究者
11. 資金配分機関に対する外国契約の開示要件	連邦省庁	研究者
12. 申請情報のジャストインタイム提出	―	連邦省庁
13. 助成後の開示内容の更新の必要性	連邦省庁	研究者
14. 不正確又は不完全な提出を個人が訂正するための手続き	―	連邦省庁
15. 研究開発助成を申請する研究機関が、開示要件に関連する証明書を提出するための要件と手続き	連邦省庁	研究組織

表 2-15：Tier I と Tier II の参加者の情報開示要件

Table 1. General NSPM-33 disclosure requirements for Tier I and Tier II participants.

Disclosures Required From:	Organizational Affiliations/ Employment	Positions/ Appointments	Foreign gov.-sponsored talent recruitment programs[3]	Current and pending support/ Other Support
Tier I • Principal investigators (PIs) and other senior/key personnel • Program officers • Intramural researchers[4]	Y	Y	Y	Y
Tier II • Peer reviewers • Advisory committee/Panel members	Y	Y	Y	N

出典：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. p.2.

表 2-16：研究開発助成プロセスにおける個人情報・専門家情報の開示のガイダンス

Table 2a. Guidance for disclosure of personal and professional information within R&D award application processes.

Type of Activity to be Disclosed	Biographical Sketch	Current & Pending/ Other Support	Annual Project Reports	Post-Award Information Terms & Conditions
PERSONAL INFORMATION				
Professional preparation (e.g., educational degrees)	✓			
Organizational Affiliations[#]	✓			
Academic, professional or institutional appointments, whether or not remuneration is received, and whether full-time, part-time, or voluntary	✓			
Paid consulting that falls outside of an individual's appointment; separate from institution's agreement		✓	✓	✓
RESEARCH FUNDING INFORMATION				
Current and pending support: All R&D projects currently under consideration from whatever source, and all ongoing projects, irrespective of whether support is provided through the proposing organization, another organization, or *directly* to the individual, and regardless of whether the support is direct monetary contribution or in-kind contribution (e.g., office/laboratory space, equipment, supplies, or employees)		✓	✓	✓
Current or pending participation in, or applications to, programs sponsored by foreign governments, instrumentalities, or entities, including foreign government-sponsored talent recruitment programs[6]	✓ (Appropriate placement may be contract-dependent)			
In-kind contributions not intended for use on the project/proposal being proposed		✓	✓	✓
Visiting scholars funded by an entity other than own institution		✓	✓	✓
Students and postdoctoral researchers funded by an entity other than own institution		✓	✓	✓
Travel supported/paid by an entity other than own institution to perform research activities with an associated time commitment		✓	✓	✓
Certification by the individual that the information disclosed is accurate, current, and complete		✓	✓	✓

[#]Some agencies may collect this information in Collaborators and Other Affiliations.

出典：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. p.4.

表 2-17：プロジェクト情報の開示のガイダンス

Table 2b. Guidance for disclosure of project information.

Type of Activity to be Disclosed	Facilities and Other Resources	Other
PROJECT INFORMATION		
In-kind contributions that support the research activity for use on the project/proposal being proposed	✓	
Private equity, Venture, or other capital financing*		✓
Supporting Documentation (e.g., contracts, grants, other agreements)^		✓

*See implementation guidance point 6 below.
^See implementation guidance point 11 below.

注：金銭的な利益相反がある場合には、株式等の情報開示が必要になる（第 2 項目）。また、海外政府との契約（外国人人材採用プログラムを含む）等がある場合にはその契約等の情報開示が必要になる（第 3 項目）。

出典：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. p.5.

②デジタル永続的識別子（Digital Persistent Identifiers）

・NSPM-33 の関連部分は、Section 4(b)(v)である。

・本項目のガイダンスの目的は、「研究機関が、管理負担を軽減しながら研究セキュリティとインテグリティを強化するために、デジタル永続的識別子（DPI）（あるいは永続的識別子（Persistent Identifiers: PID））を開示プロセスにどのように組み込むかを説明する」ことである。

・以下の 7 項目について説明している。[67] なお、申請者・申請機関の負担を軽減するという意味で「支援」とここでは分類している。

[67] "1. Incorporation of DPIs into grant and cooperative agreement application and disclosure processes
2. Requiring DPIs versus providing as an option for disclosures
3. Categories of individuals provided a DPI option for disclosures
4. Use of available DPI services
5. Common/core standards that a DPI service should meet to be included as an option for disclosure in Federal grant and cooperative agreement application processes
6. Ensuring interoperability across multiple options for DPI service
7. Potential for public disclosure of information provided to research agencies via a DPI service"

表 2-18：「デジタル永続的識別子」についての実施ガイダンス項目

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

項目内容	要求元	要求先
1. 助成金及び協力協定の申請及び開示手続きへの DPI の組み入れ	ー	連邦省庁
2. DPI を要求するか、あるいは情報開示のオプションとして提供するか。	ー	連邦省庁
3. DPI を情報開示の選択肢として提供する個人のカテゴリー	ー	連邦省庁
4. 利用可能な DPI サービスを利用する	ー	連邦省庁
5. 連邦補助金及び協力協定の申請手続きにおいて、DPI サービスが開示の選択肢として含まれるために満たすべき共通/中核的な基準	ー	連邦省庁
6. DPI サービスの複数のオプションにまたがる相互運用性の確保	ー	連邦省庁
7. DPI サービスを通じて連邦政府省庁に提供された情報の一般公開の可能性	ー	連邦省庁

③情報開示要件違反への対応（Consequences for Violation of Disclosure Requirements）

・関連する NSPM-33 の項目は Section 4(b)(ix) である。
・本項目の目的は、「連邦政府省庁及び研究機関のための適切なレベルの柔軟性を維持しながら、適用される法律及び規制と一致する、情報開示要件の違反に対する適切な対応を決定するためのガイドラインを提供する」ことである。
・実施ガイダンスは以下の 8 項目についてそれぞれ記述されている。[68]

[68] "1. Consequences for violation of disclosure requirements
2. Other potential administrative actions available to research agencies to address noncompliance with disclosure requirements
3. Factors for consideration in determining appropriate administrative actions and other consequences
4. Provision of more detailed information regarding administrative remedy and enforcement processes
5. Encouraging individuals to come forward and correct past omissions
6. Notice and due process in agency consideration and application of regulatory administrative action
7. Circumstances for potential imposition of consequences on research organizations
8. Circumstances for potential suspension or denial of Higher Education Act (HEA) Title IV funds"

表 2-19：「情報開示要件違反への対応」についての実施ガイダンス項目

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

項目内容	要求元	要求先
1. 開示要件違反への対応	―	連邦省庁
2. 開示要求の不遵守に対処するために連邦政府省庁が利用可能なその他の潜在的行政措置	―	連邦省庁
3. 適切な行政措置及びその他の対応を決定する際に考慮すべき要素	―	連邦省庁
4. 行政上の救済措置及び執行プロセスに関するより詳細な情報の提供	―	連邦省庁・NSTC 研究セキュリティ小委員会
5. 個人が名乗り出て過去の不作為を訂正することを奨励する。	―	連邦省庁
6. 規制当局の行政措置の検討・適用における通知と適正手続き	―	連邦省庁
7. 研究組織に対して対応する可能性のある状況	―	連邦省庁
8. 高等教育法（HEA）第 IV 章の資金が停止又は拒否される可能性がある状況	―	連邦省庁

注）高等教育法（HEA）第 IV 章は、連邦政府による学生への奨学金プログラム（federal student financial aid）についての規定である。

表 2-20：開示要件不順守の研究機関に適用可能な、非強制的な行政措置・救済措置の例

Table 3. Examples of non-enforcement administrative actions and remedies that may apply to research organizations for noncompliance with disclosure requirements.

Category	Examples	Citation
Monitoring/ administrative actions	• Financial and performance reports • Site visits • Video conferences, telephone calls, e-mails	2 CFR §200.329, Monitoring and reporting program performance
Remedies for noncompliance	• Specific award conditions • Require payments as reimbursements rather than in advance • Withhold authority to proceed to next phase pending evidence of acceptable performance within a given performance period • Require additional, more detailed financial reports • Require additional project monitoring • Require the organization to obtain technical or management assistance • Establish additional prior approvals	2 CFR §200.208, Specific conditions.
	• Withhold cash payments pending correction of the deficiency • Disallow all or part of the cost of the activity/action not in compliance • Wholly or partly suspend or terminate the Federal award • Withhold further Federal awards for the project or program	2 CFR §200.339, Remedies for noncompliance

出典：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. p.13.

④情報共有（Information Sharing）

・関連する NSPM-33 の項目は、Section(e)である。

・本ガイダンス項目の目的は、「違反及び違反の可能性に関する情報を連邦省庁が共有できる状況を明確にするとともに、そのような共有が、プライバシーやその他の法的・合理的な保護を尊重するためにどのように制限されるかについての保証を提供すること」[69]である。

・ガイダンス項目は、以下の 5 項目である。[70]

[69] "Provide clarity regarding circumstances when agencies may share information regarding violations and potential violations, and provide assurance regarding how such sharing will be limited to respect privacy and other legal and reasonable protections"

[70] "1. Circumstances for research agency sharing with other agencies information about violations of disclosure requirements
2. Circumstances for appropriate research agency sharing of information prior to final determination of a violation
3. Mechanisms for research agency sharing of information regarding violations with each other and with the public
4. Mechanisms for research agency sharing of information regarding potential violations
5. Proper sharing of information about violations and potential violations"

表 2-21：「情報共有」についての実施ガイダンス項目

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

項目内容	要求元	要求先
1. 連邦政府省庁が開示義務違反に関する情報を他連邦機関と共有する状況	―	連邦省庁
2. 違反の最終決定前に連邦政府省庁が情報を適切に共有する状況	―	連邦省庁
3. 連邦政府省庁が違反行為に関する情報を、連邦政府省庁相互及び一般市民と共有するための仕組み	―	連邦省庁
4. 連邦政府省庁が違反の可能性に関する情報を共有するための仕組み	―	監察官・連邦省庁
5. 違反行為及び違反の可能性に関する情報の適切な共有の仕組み	―	連邦省庁

⑤研究セキュリティプログラム（Research Security Programs）

・関連する NSPM-33 の項目は、Section 4(g) である。

・本ガイダンスの目的は、「研究セキュリティプログラムの要件、研究組織がどのように要件を満たすことが期待されるか、また、連邦政府省庁がどのようにプログラムの内容開発に貢献するかについて、明確にする」ことである。

・ガイダンスは以下の 9 項目について説明されている。[71]

[71] "1. Requirements for research security programs
2. Determination of which research organizations are subject to the requirement
3. Standardization of program requirements across organizations
4. Process for finalizing and implementing the requirement
5. Development of research security program content
6. Ensuring that cybersecurity elements of research security programs meet the objectives of the requirement
7. Certification of compliance with the requirement
8. Discretion of research organizations in structuring research security programs
9. Timeline for research organizations to establish compliance"

表 2-22：「研究セキュリティプログラム」についての実施ガイダンス項目

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

項目内容	要求元	要求先
1. 研究用セキュリティプログラムへの要求事項	連邦省庁	研究組織
2. どの研究組織が要求事項の対象となるかの決定	連邦省庁	研究組織
3. 組織横断的なプログラム要求事項の標準化	連邦省庁	研究組織
4. 要求事項の最終決定と実施のプロセス	ー	OSTP（NSTC 研究セキュリティ小委員会、OMB 等と調整）
5. 研究セキュリティプログラム内容の開発のための指導的な技術的支援の提供	ー	連邦省庁（特に、National Counterintelligence Task Force 、National Counterintelligence and Security Center）
6. 研究セキュリティプログラムのサイバーセキュリティ要素が、要求事項の目的に合致していることを確認する。	連邦省庁	研究組織
7. 要求事項への適合の証明	連邦省庁	研究組織
8. 研究セキュリティプログラムの構築における研究組織の裁量	連邦省庁	研究組織
9. 研究組織がコンプライアンスを確立するためのタイムライン	連邦省庁	研究組織

(2) 2022 年度の動き

(a) The CHIPS and Science Act of 2022 (H.R. 4346)（2022 年 8 月 9 日）

The CHIPS and Science Act of 2022 は 2022 年 8 月 9 日にバイデン大統領が署名し、成立した。米国で半導体を生産するインセンティブの創出に関する活動を行うため、CHIPS 基金（Creating Helpful Incentives to Produce Semiconductors for America Fund）を設立し、その資金を提供する等の内容を含む。

法律は、Division A（CHIPS Act of 2022）と、Division B（Research and Innovation）の 2 部構成である。Division A では、半導体インセンティブに 5 年間で 527 億ドルを計上（appropriation）、そのうち、先端研究開発に 110 億ドル計上すること、米国内の半導体製造施設に対する新たな投資税額控除などが含まれる。また、中国での半導体製造能力拡大が制限され、CHIPS 資金と投資税額控除の受給者は、レガシーチップの製造を除き、10 年間中国での半導体製造の拡大を禁止することが規定されている。Division B では、研究開発プログラムに対する 1700 億ドルの支出権限（authorization）がなされ、NSF（810 億ドル）、DOE（170 億ドル）、NIST、その他の DOC を含む複数の連邦機関の研究開発イニシアティブに対する 5 年間の資金の支出権限が認可された。[72]

また、この法律は、Division B に研究セキュリティに関する規定を含む (Division B : Title III−National Science Foundation for the Future, Subtitle D−NSF Research Security と、Title VI−Miscellaneous Science and Technology Provisions, Subtitle D−Research Security など)。具体的には、表 2-23 に示すように、以下のような NSF に対する要求規定を含んでいる。[73]

- Research Security and Policy Office を設置し、研究開発助成の申請及び NSF への情報開示に関するリスク評価を実施する権限を付与すること。
- 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、独立したリスク評価センターを設立すること。
- 研究セキュリティの責任者を設置し、研究者にガイダンスとリソースを提供する。

[72] Julia Jester, Toby Smith. Chips and Science Act. Association of American Universities. ARIS Office Hours, October 28, 2022; About the "CHIPS and Science Act" <https://beta.nsf.gov/chips>
[73] NSF. “About the "CHIPS and Science Act"” https://beta.nsf.gov/chips
https://www.whitehouse.gov/briefing-room/statements-releases/2022/08/09/fact-sheet-chips-and-science-act-will-lower-costs-create-jobs-strengthen-supply-chains-and-counter-china/
https://www.aau.edu/key-issues/chips-and-science-act-summary-research-security-provisions

表 2-23：The CHIPS and Science Act of 2022 の研究セキュリティ関連の規定の概要

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

要求・支援の対象	内容
大統領府科学技術政策局（OSTP）	外国人人材採用プログラム（Foreign Talent Recruitment Programs）のガイドライン作成（Sec.10631） ・（FY2020 国防授権法 1746 条に基づき設立された）省庁間ワーキンググループと連携し、連邦研究機関に対し、外国人人材採用プログラムに関する統一したガイドラインを配布することを OSTP に要求。ガイドラインは、各連邦研究機関のすべての職員が外国人人材採用プログラムに参加することを禁止し、外国人人材採用プログラムの特徴を定義して説明する。2021 年度国防授権法 223 条に従い、研究助成申請書の主要研究者は、外国人人材採用プログラムの契約・協定・取決めの当事者である場合に情報開示しなければならず、また、悪意のある外国人人材採用プログラムに参加することはできない。
資金配分機関（一部は、資金配分機関→研究者・研究機関）	悪質な外国人人材採用プログラム（Malign Foreign Talent Recruitment Program）への参加の禁止（Sec.10632） ・各連邦機関に対し、研究助成金提案プロセスの一環として、提案書提出時又はその後毎年、助成期間中、対象個人が悪質な外国人人材採用プログラムに参加していないことを証明するよう求める方針を確立することを要求する。
	契約等をレビューするための資料を研究機関に要求する権限付与（Sec.10633） ・各連邦機関は、要請に応じて、研究開発助成の申請書に記載された全ての対象者について、外国人人材採用プログラムへの参加に特有の契約書、補助金、又は外国人任命、外国機関への雇用、その他の合意書の写しを含む、補足書類を提出するよう機関に求める権限を有している。研究機関と協議の上、契約、助成金、協定が、機関が支援する活動の能力を阻害する、又は機関が支援する活動との重複を生じさせると判断された場合、連邦研究機関と受領機関は、対象者の代替又は助成からの除外、助成額の削減、助成の停止/終了を開始することができる。各連邦機関は、最終的な行政措置が取られる前に、全ての対象者のプライバシーを保護し、措置の正当な理由を提供し、対象者にコメントや反論を提供し上訴する機会を与えるために必要な措置を講じるべきである。
	連邦政府研究資金を使う研究者：研究セキュリティ研修要件（Sec.10634） ・資金配分機関は、研究資金の公募申請の一部として、申請書に記載された各対象者は研究セキュリティ訓練の修了（過去 1 年以内）を認証するという要件を設ける。 ・大学・研究機関は、雇用されている各対象者がそのような訓練を修了していることを証明する。 ・研究セキュリティ研修の内容は、サイバーセキュリティ、国際共同研究、海外渡航、海外からの介入、資金の適切な使用に関する規則、情報開示、責務相反、利益相反に焦点を当てる。
Comptroller General（GAO 長官）	研究資金の会計（Sec.10635） ・Comptroller General（※GAO の長官）に対し、研究のために懸念される外国組織が利用できる連邦資金に関する調査を実施することを要求する。この調査は、研究のために懸念される外国組織が利用できる連邦資金の量、種類、要件に関する評価を含むものとする。
NSF（一部は、NSF→研究者・研究機関）	Office of Research Security and Policy と Chief of Research Security の維持（Sec.10331-10332） ・NSF に、NSF 長官室内に少なくとも 4 名のフルタイムスタッフを擁する Research Security and Policy オフィスを維持することを要求。
	Office of Research Security and Policy にリスクアセスメントの実施権限を付与（Sec.10336） ・NSF の監察官室（OIG）と連携して、NSF Office of Research Security and Policy が、研究開発助成の申請と NSF への情報開示について、オープンソースの分析・解析ツールの利用を含むリスク評価を実施する権限を付与する。

要求・支援の対象	内容
NSF （一部は、NSF→研究者・研究機関）	オンラインリソースの開発（Sec.10334） ・NSF に対し、研究組織及び個人の研究者向けに、最新情報を含むオンラインリソースを開発するよう要請。
	研究不正等についての研究の公募継続（Sec.10335） ・NSF に対し、研究不正や研究インテグリティの侵害、有害な研究行為に関する研究を含む、研究行為や研究環境に関する研究を支援するための研究助成を継続することを要求。
	責任ある研究実践についての研修（Sec.10337） ・責任ある研究実践についての研修に関する 2007 年 America COMPETES Act の Sec.7009 を修正。ポスドク研究者、教員、上級職員を含めるよう要件を拡大。 ・プログラムは、メンター（研究指導者）の訓練、メンターシップ、潜在的な研究セキュリティの脅威に対する認識を高めるための訓練、連邦輸出管理・情報開示・報告要件に関する訓練を含むことを明記。
	研究セキュリティ・インテグリティ情報共有分析センター（Research Security and Integrity Information Sharing Analysis Organization）の外注（Sec.10338）
	Controlled information へのアクセスを持つ研究分野を同定する計画作成（Sec.10339） ・NSF に対して、国家情報長官室（ODNI）及び他の連邦機関と協議の上、主要技術重点分野を含む NSF が支援する研究分野で、controlled unclassified 情報（CUI）又は controlled classified 情報へのアクセスを伴う可能性のあるものを特定する計画を策定するとともに、研究助成に関して働く NSF 職員又は NSF 研究開発助成の対象者に CUI 又は controlled classified information へのアクセスを適宜付与するにあたりデューディリジェンスを行うことを要求。
	孔子学院を設置する研究機関への資金提供の原則禁止（Sec.10339A）
	研究倫理・社会的影響について公募提案書への記載を求める（Sec.10343） ・NSF に対し、利害関係者からの意見を踏まえ、助成金提案の指示書（instruction）を改訂し、研究開発費の支給に先立ち、倫理的・社会的配慮を提案の一部として含めることを義務付けることを要求する。利害関係者の意見を考慮し、NSF は何をもって「容易に予見可能又は定量化可能なリスク（readily foreseeable or quantifiable risk）」とするかについて明確なガイダンスを作成する。
エネルギー省長官	研究セキュリティに対処するツールの開発（Sec.10114） ・DOE 長官に対し、国家情報長官室（ODNI）が特定した脅威を反映した科学技術リスクマトリックスなど、研究セキュリティリスクを管理・軽減するためのツールやプロセスを開発・維持し、対象となる支援の下で実施される活動がもたらす米国の知的財産喪失のリスクや米国の国家安全保障への脅威を判断しやすくするよう要請。
GAO	GAO に対して NIST の研究セキュリティポリシー、プロトコル等についての調査研究を行うよう要求（Sec. 10247）
大学等研究機関	NSF に海外からの資金支援の有無を毎年報告（Sec.10339B） ・研究機関は、毎年 NSF に対し、贈与や契約を含め、当該機関が懸念される外国（foreign country of concern）に関連する外国資金源から直接又は間接的に受ける 5 万ドル以上の現在の資金援助について、要約文書の形で報告しなければならない。
研究者等	懸念される個人又は団体の禁止。（Sec.10636） ・新設の NSF Directorate for Technology, Innovation and Partnerships を含む、特定のプログラムに対する助成、アワード、プログラム、支援、その他の活動を受けること又は参加することを、懸念事項とされた人物又は団体（persons or entities identified as a concern）に禁止する。

出典：AAU. The CHIPS and Science Act of 2022 (H.R. 4346): Research Security Provisions. Last updated August 8, 2022. <https://www.aau.edu/sites/default/files/AAU-Files/Key-Issues/Science-Security/CHIPSandScienceFinalResearchSecurityProvisions.pdf> 等に基づき作成。

(b) OSTP アップデート情報の発表（2022 年 8 月 31 日）

2022 年 8 月 31 日に、大統領府科学技術政策局（OSTP）は研究セキュリティに関する検討の最新情報を発表した。米国科学技術会議（NSTC）の研究セキュリティ小委員会（SRS）は、連邦政府の研究省庁、研究セキュリティ活動を主導する省庁、研究コミュニティと数ヶ月にわたって討議し、連邦科学資金配分機関に助成金や共同研究契約を申請する研究者の潜在的な利益相反や責務違反を評価するための標準的なデータフィールドと情報開示の指示書の作成に成功した。全ての連邦科学資金配分機関は、標準化されたフォーマットの採用に向けて動き出すことに同意している。パブリックコメントとレビューのプロセスは 2022 年 8 月 31 日に Federal Register に掲示され、開始され、10 月 31 日まで意見が求められた。[74,75]

米国研究コミュニティとの関与

SRS は、2022 年春に「エンゲージメント・アワー」を訪れた約 40 の組織から意見を聞いた。これらの組織は、全米の公立・私立大学、様々な科学分野を代表する専門組織、研究セキュリティとインテグリティの強化に取り組む非営利組織、特にアジア系アメリカ人、太平洋諸島民、ハワイ先住民のコミュニティを代表する学術・擁護組織など、米国の研究エコシステムに貢献する多様な組織を代表するとのことである。これらの組織から提起されたアイデア、懸念や疑問点は、NSPM-33 方針の継続的な策定と実施に反映されるものであり、OSTP と SRS のメンバーが米国の研究コミュニティと協力することにコミットしていることを表す、としている。

SRS は 2022 年秋に、勧告と我々の学んだ教訓をまとめた公的な報告書を発表する予定である（※2023 年 2 月時点で公表は確認できない）。また、将来的にはエンゲージメント・アワーを追加する予定で、特に、地方の大学、歴史的に黒人の多い大学、ヒスパニック系の大学、トライバルカレッジ、その他の少数民族を支援する大学、地域の大学、コミュニティカレッジからの意見を聞くことに関心が高いとのことである。

---

[74] An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity (Morgan Dwyer, Principal Assistant Director for National Security, Office of Science and Technology Policy; Christina Ciocca Eller, Assistant Director of Evidence and Policy and Co-Chair of the National Science and Technology Council Subcommittee on Research Security, Office of Science and Technology Policy; and Ryan Donohue, AAAS Science and Technology Policy Fellow and Senior Policy Advisor, and Member of the National Science and Technology Council Subcommittee on Research Security, Office of Science and Technology Policy)
https://www.whitehouse.gov/ostp/news-updates/2022/08/31/an-update-on-research-securitystreamlining-disclosure-standards-to-enhance-clarity-transparency-and-equity/

[75] Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support. A Notice by the National Science Foundation on 08/31/2022
https://www.federalregister.gov/documents/2022/08/31/2022-18746/agency-information-collection-activities-request-for-comment-regarding-common-disclosure-forms-for

デジタル永続的識別子（Digital Persistent Identifiers）

研究者が効果的な PID ポリシーを策定するために必要な法的、政策的、技術的、実施上の考慮事項に対処するため、SRS は OSTP とエネルギー省が主導する省庁間討議を招集した。2022 年 3～5 月に、ほぼ全ての科学研究費助成機関からなるこの PID サブグループは、7 回の会合を開催した。研究者 PID ポリシーの策定と実施に関する情報、ベストプラクティス、教訓が共有された。同サブグループは、各機関が政策立案と実施にどのようにアプローチするかについて、より良い情報を提供するための内部ツールキットを開発している。

NSPM-33 の PID に関する規定を実施するための長期的なビジョンは、研究者が自分の PID を、履歴書と同じように、資金源、研究成果、所属などの重要情報を常に最新の状態に保つことができるようにすることである。研究者は自分の PID をあらゆる連邦助成申請システムに同期させることができ、負担低減と潜在的な善意のミスを減らすことができる。実装の鍵となるのか、情報開示データフィールドの標準化であり、統合を容易にするために何が必要かを省庁と PID 開発者の双方に明確にするとのことである。

研究セキュリティプログラム

研究セキュリティプログラムを強化するために、SRS は NSPM-33 実施ガイダンスに詳述されている要件と、2022 年の「CHIPS and Science Act」の規定を検討して、さらに明確にするように努めた。NSPM-33 では、2 年連続で 5000 万ドル以上の連邦科学技術助成金を受ける研究機関に対し、NSPM-33 と関連する実施ガイダンスが定めた基準を満たす「研究セキュリティプログラム」を備えていることを証明するよう、連邦科学資金配分機関が要求することを指示している。これらの基準には、研究セキュリティプログラムの 4 つの特定分野、すなわち一般的な研究セキュリティ研修、海外渡航セキュリティ、サイバーセキュリティ、輸出セキュリティ（必要に応じて）が含まれる。CHIPS and Science Act は、研究セキュリティ研修に関する要件を、高等教育機関又はその他の研究機関の職員として連邦科学技術資金の受給を申請するすべての者に拡大した。

研究セキュリティプログラムの要件が、研究機関のコスト及び管理負担への影響を最小限に抑えて満たされるようにするため、連邦政府は、実施ガイダンスよりもさらに詳細に要件を規定する予定である。研究セキュリティプログラム基準の草案は、2022 年の秋に正式なパブリックコメント期間として利用できるようになると予定されていた、その後、やや遅れて、2023 年 2 月後半に草案が公表されている（→49 頁を参照）。

(c) 米国アカデミー報告書「米国の技術優位を保護する」（2022 年 9 月 29 日）

米国の全米アカデミーズ（全米科学・工学・医学アカデミー）は、報告書「米国の技術優位を保護する」（*Protecting U.S. Technological Advantage*）を作成し、オープンネスと競

争の時代において、国家安全保障にとって戦略的に重要な技術をいかに保護するかについて、大統領府や連邦政府機関への政策提言をするとともに、「科学技術安全保障円卓会議」が設置される等、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場となっている。

まず、2022 年 9 月 29 日に公表された報告書「米国の技術優位を保護する」は、国防省の国防高等研究計画局（DARPA）と米国科学財団（NSF）の依頼を受け、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術の保護についてレビューするため、国家安全保障にとって重要な領域の研究の実施と商業化に関する政策と実践を検討する特別委員会を開催し、検討した結果に基づいている。[76]

全米アカデミーズが DARPA と NSF に検討を依頼されたのは以下の 3 つの質問である。[77]

1. 今日の競争的環境において、政府資金配分機関は、特定の技術を保護することと商業化のオプションの利点と欠点を考慮して、科学の開放性をどのように評価又は制限し、アイデアから商業化への移行を奨励すべきか。
2. 研究で発見された進歩、特に米国の国家安全保障に重大な影響を与える可能性のある進歩の生産と商業化に関する市場や制度の課題があるとすれば、どのような解決策が必要であろうか。
3. 研究、生産、商業化、技術保護に関連する適切な政策変更で、米国が資金提供する研究から生まれた進歩の米国内及び米国に利益をもたらすためのマーケティング/実用化を加速するのに役立つものは何か（特に国家安全保障上のリーダーシップにとって重要な技術について）

報告書の第 6 章は、開放と競争の時代に米国が技術を保護する方法について、委員会の結論と提言を書いている。(表 2-24)

[76] National Academies of Sciences, Engineering, and Medicine 2022. *Protecting U.S. Technological Advantage*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26647.
[77] 同上. p.11.

表 2-24：米国アカデミーズ報告書「米国の技術優位を保護する」の提言

提言 1 ・大統領は、大統領令（executive order）を通じて、基礎研究は可能な限り無制限のままであることが米国の方針であることを明確に再確認すべきである。さらに、大統領令は、連邦政府機関と連携して、科学技術政策局（Office of Science and Technology Policy）に、大統領令の発行から 120 日以内に、開かれた研究環境と制限された研究環境の基準を定めるように指示すべきである。 ・さらに、大統領令は、連邦政府機関に対し、助成金や契約の下での業務について、授与前に適切な環境を指定し、オープンな研究環境で実行できる支援業務の量を最大化するよう指示すべきである。この指定を行う際、いかなる制限や推奨される制限も、資金提供を受ける特定の研究助成金や契約にのみ適用され、資金提供を受ける機関全体に普遍的でないことを明確に表明すべきである。（p.79）
提言 2 ・米国科学財団（NSF）は、技術革新における米国のリーダーシップに必要な優秀な科学、研究、工学、革新的人材の開発、誘致、保持に不可欠な米国のイノベーションシステムの要素を定義する取組に出資し、調整する必要がある。NSF は、この取組に他の連邦科学機関、大学、研究機関、教育者、研究集約型企業を巻き込むべきである。NSF は、この取組開始から 180 日以内に、調査結果の詳細を記した報告書を作成する必要がある。 ・これらの調査結果に基づき、科学技術政策局は、連邦研究機関、国土安全保障省、国務省と連携し、国内の研究人材の育成、国際研究協力の機会の拡大、訓練や雇用のために優秀な人材を米国に引き付け維持することを目的とした政策やプログラムを通じて、科学技術におけるリーダーシップを促進する国家戦略を策定するべきである。（p.81）
提言 3 ・国家安全保障会議（National Security Council）、国家科学技術会議（National Science and Technology Council）、国家経済会議（National Economic Council）は、米国の技術リーダーシップやその他の国益にとって戦略的に重要な脅威や脆弱性を特定し評価するための省庁間プロセスを開発し主導するべきである。このプロセスには、各脅威について、連邦機関がリスクに対処する際に使用する関連リスク管理戦略及び評価基準の策定が含まれるべきである。これらのリスク管理戦略の実行は、「政府全体」のアプローチを確保するために、上記の省庁間プロセスによって調整され、監督される必要がある。 ・この省庁間リスク管理プロセスから得られる戦略は、以下のとおりとする。 ➢ 国家や経済の安全保障に影響を与える技術関連の脅威を、研究開発プロセスのできるだけ早い段階で定義するという意味で、プロアクティブなものである。 ➢ 敵対者の計画、行動、意図、能力を含むグローバルな現実と、保護すべき技術、保護できない技術に関する合理的なリスク受容の判断に基づく戦略的なものである。 ➢ 関連する脅威と脆弱性についての最新の理解に基づいており、必要に応じて調整され

るという点で、タイムリーである。 ➢ 輸出管理、情報分類、対米外国投資委員会（Committee on Foreign Investment in the United States）の決定など、技術保護のためのさまざまなメカニズムが、リスクを効果的に低減又は軽減するような方法で指示・調整される統合的なものである。 ➢ 適応性があり、特定された技術分野を科学、技術、国家安全保障の総合的な専門家による定期的なレビューの対象とするメカニズムがある。 ➢ 動的／反復的であり、脅威の状態の変更を正当化するような技術、環境、行為者に変化がないことを確認するための定期的な見直しがある。 ➢ 米国のイノベーション・リーダーシップに不必要かつ意図しない障壁をもたらすことがないよう、悪影響がないかどうかを評価する。（p.83）
提言 4 ・国家科学技術会議、国家安全保障会議、国家経済会議は、戦略的に重要なプラットフォームを特定し、その開発、管理、使用を対象とする協調的なリスク管理戦略を開発するための新しい政策枠組みを共同で開発すべきである。この新しい枠組みの要素は以下を含むべきである。 ➢ 米国の利益にとって不可欠な特定の技術プラットフォームを定義し、指定すること。 ➢ セキュリティ、インテグリティ、相互運用性、制御機能、ユーザー制御の性能基準など、プラットフォーム開発に含まれるべき技術的特徴や要件の特定に民間部門を関与させること。 ➢ 国際的なガバナンス機構、利用協定、規制アプローチ、貿易協定、コンテンツ要件、法執行協力協定など、プラットフォーム開発者又は利用者間の信頼関係を確立し管理するための首尾一貫した政府全体の戦略を開発すること ➢ 共有プラットフォームの使用に関連するセキュリティ又は信頼の問題に対するさまざまな対応を確立し、参加機関が適切な「インシデント対応」能力を計画・準備すること。

以下は同報告書の中で、本調査に関連を持つ部分の抜粋である。

<u>提言１と２について</u>

・ 現在のアプローチは、技術が開発され使用される状況について、時代遅れの仮定に基づいている。その第 1 の前提は、米国は新技術の開発において圧倒的な優位性を享受しており、この優位性は敵や競合相手を「アウトイノベート」（”outinnovating”）することによって守ることができる、というものである。第 2 の前提は、戦略的に重要な技術は、明確な目的を持った個別的なもの（discrete, with well-defined purposes）であるということである。第 3 の前提は、これらの技術は連邦政府の研究所や政府支援の学術研究から生まれ続け、その後、より広い用途のために商業化されるということである。第 4 の

前提は、技術関連のリスク管理は、主に特定の「重要技術」を不正な使用、所有、生産から保護することによって達成できるというものである。

- 今日の非常に競争の激しいグローバルな技術環境では、これらの仮定はもはや有効ではない。委員会の見解では、米国の技術的優位性を守るためには、「技術管理」（technology controls）を超えた根本的な発想の転換が必要であり、新しいアプローチの基礎を築くことが必要である。
- 競合国に対する米国の最大の優位性は、技術へのアクセスを制限する能力ではなく、同盟国と協力して新技術をいち早く開発し展開する能力に根ざしている。この優位性を最大化するために不可欠な戦略には、国内の研究・技術革新エコシステムの規模とスピードを促進すること、研究者やイノベーターを支援するためにリスクを取る環境を育成すること、世界で最も優秀な科学・工学・イノベーション人材を引き付け、維持し、支援することが含まれる。提言 1 及び 2 は、これらの戦略を支援するものである。

提言３について

- 技術に関連するリスクを管理するための現在の米国のアプローチは、これらの技術の所有、使用、製造に対する制限、又はそれらの開発に必要な知識や材料に対する制限に基づいている。技術革新のスピードと規模、民間発の技術の増加傾向を考えると、現在のリスク管理アプローチ（risk management approach）は有効性に限界があり、場合によっては逆効果になる可能性がある。その代わりに、米国政府は、米国が直面する技術関連の脅威と脆弱性を定義し、米国の技術リーダーシップに生じるリスクに対応するための効果的な戦略の実施を調整することに焦点を当てるべきである。これらの戦略を支える行動は、公共部門と民間部門、複数の連邦政府機関、そして必要であれば国際的なパートナーとの間で行われるかもしれない。提言 3 はこの問題に対処するものである。

提言４について

- 今日の技術システムは、その機能性、生産性、使用において、プラットフォームに依存し、多くの場合、プラットフォームの必要な構成要素となっている。プラットフォームは、プラットフォーム上のあらゆる技術を悪用することができる新しい共有の脆弱性をもたらしている。共有プラットフォームに固有の共依存性は、プラットフォームに対する制限や制御が、米国の国家安全保障や競争力を強化する有益な利用を含む、プラットフォームを利用するすべてのものを混乱させ、非常に大規模な意図しない結果を引き起こす可能性があることを意味する。プラットフォームを管理又は制御する分散化された、そしてしばしば国際的なガバナンスシステムは、基準、貿易、国際協定、規制、法執行を担当する複数の機関の間で、又は民間団体や国際パートナーとの間で、連邦政府の協調行動を必要とするかもしれない。提言 4 はこの問題に対処するものである。[78]

[78] 同上. pp.77-78.

全体的な結論としては、以下のように、同報告書は、①イノベーションと技術における戦略的優位性を高めるためには、開かれた研究環境と適切に制限された環境のバランスが重要である、②米国の政策は、リスクと創造性のバランスを適切に取りながら、研究活動に最適な環境を提供することを目指すべきである、③米国のイノベーションエコシステムを弱めず、新技術の開発と適用能力を保護・強化することが、特定の技術を保護することよりも重要である、としている。

- 米国の全体的な目標は、イノベーションと技術における戦略的優位性を最大限に高めることであるべきである。科学的発見とイノベーションは、広く開かれた参加が望ましいので、この目的を達成するための重要な要素は、開かれた研究環境で適切に実行できる仕事の量を最大化することであり、それによって科学と工学における米国のリーダーシップを促進し、優れた人材を引き付け、新技術につながる発見を強化することである。米国の利益を守るためにオープンな環境が適切でない特定のケースについては、連邦研究開発（R&D）資金提供者は、適切に制限された環境を必要とする特定のケースを明確に指定するリスク情報に基づく決定を行うべきである。
- 技術革新を行う上で、米国はオープンな研究開発環境と制限された研究開発環境の両方を持つことで利益を得ることができる。オープンな研究環境とは、参加、情報共有、出版に関する制限が比較的少ない環境であるが、研究プロセスのインテグリティを確保するための基本的な要件が含まれている。オープンな環境で行われる研究、トレーニング、教育は、研究者の才能を惹きつけ、発見のための創造的で革新的な条件を育成し、新しいアイデアや技術の開発を加速させるため、米国に利益をもたらす。オープンな環境でこの仕事を行うことは、情報や人の移動によって、知識やノウハウ、成果が敵に流れてしまうというリスクをもたらす。しかし、イノベーションリーダーにとっては、情報流出のリスクを軽減し、さらに新しい技術を革新することができるため、ほとんどの研究開発活動において、オープン化のメリットはリスクを上回る。イノベーションリーダー国よりも「速く走る」ことができる。
- すべての研究関連業務がオープン環境に適しているわけではないが、ほとんどの研究関連業務がオープン環境に適している。しかし、特定の用途においては、研究、開発、生産、及び関連する活動を、参加、協力、情報の共有、及び結果の普及を制限する制限付き環境に閉じ込める必要がある。これは、知識、ノウハウ、生産、及び技術の利用が、知識や情報を適切に使用するよう委託された人々に限定されることを確実にするためである。このような場合、敵対者に機密技術を広めるリスクを下げることは、そのような環境で行われる仕事の創造性と生産性に対する制限の悪影響を上回る。米国の政策は、ある研究活動に最も適したタイプの研究環境を指定することによって、これらのリスクの適切

なバランスを取るという目的を持つべきである。[79]

- 今日、米国は他国との人材獲得競争の激化に直面しており、これには外国人又は外国籍の科学者や技術者を米国から引き留めたり、引き離したりすることを目的とした特定のプログラムも含まれている。この競争に対する現在の米国の対応は、断片的で防衛的であり、外国人人材の採用を促進する代わりに、米国市民や機関による外国人人材プログラムへの参加を制限することに主眼を置いている。一貫した連邦政策は、米国市民のための国内 STEM 教育・訓練機会を強化する取組と、学生や労働者として海外の優秀な人材を惹きつける取組とを結びつけていない。現在の政策アプローチでは、人材誘致において長年の優位性を与えてきた米国のイノベーションシステムの特徴を強化・防衛する必要性を十分に考慮していない。[80]
- 今日の相互依存的でグローバルなイノベーションシステムにおいて、最大の脅威は、米国がそのイノベーションエコシステムを不注意に弱める一方で、他国が技術開発と商業化において米国が歴史的に優位に立ってきた行動を模倣し続けることである。この脅威に対抗するため、米国は新技術を開発し、その技術を軍事・商業の両分野の問題に適用する能力を保護し、拡大する必要がある。この能力を保護し強化することは、特定の技術を保護することよりも極めて重要である。[81]

「科学技術安全保障円卓会議」の設置とワークショップの開催

2019 年 12 月に成立した 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とともに、全米アカデミーズに「科学技術安全保障円卓会議」（National Science, Technology, and Security Roundtable）を設置することが規定された。円卓会議は、米国科学財団、エネルギー省、国防省等の連邦省庁が全米アカデミーズと合意し設置することとされている。

円卓会議の概要は、表 2-25 のとおりである。第 1 回円卓会議は 2020 年 11 月に開催され、2022 年 12 月の第 8 回円卓会議までこれまでに計 8 回の会議が開催されてきている。[82]

[79] 同上. p.79.
[80] 同上. p.81.
[81] 同上. p.85.
[82] National Academies website. “National Science, Technology, and Security Roundtable” <https://www.nationalacademies.org/our-work/national-science-technology-and-security-roundtable>

表 2-25：全米アカデミーズ「科学技術安全保障円卓会議」の概要

参加者	以下の機関等の代表者及び実務者を含める。 ・連邦科学省庁、情報機関、国家安全保障機関、法執行機関 ・高等教育機関、連邦政府研究所、産業界、非営利研究機関を含む米国科学事業の主要関係者
設置目的	A) 科学の進歩及び科学技術における米国のリーダーシップに必要な開かれた意見交換、及び国際的な才能を確保しつつ、米国の国家及び経済の安全を守ることに関連する重要な問題の探求。 B) 外国の干渉、サイバー攻撃、盗難又はスパイ行為を含む連邦政府が資金配分する研究開発におけるセキュリティ上の脅威及びリスクの特定及び考察を促進すること。 C) B)で特定された脅威及びリスクを、非機密データ及び関連事例の共有を含め、学術及び科学コミュニティに伝えるための効果的なアプローチの特定。 D) B)で特定された脅威及びリスクへの対処及び軽減するためのベストプラクティスの共有。 E) 外国の脅威に伴うリスクを軽減及び対処すべく政府及び学術・科学コミュニティによる短期及び長期にわたる潜在的対応についての検討。

出典：2020 年度国防権限法（FY 2020 National Defense Authorization Act (NDAA)）第 1746 条の規定に基づき作成。

さらに、同円卓会議の関連活動として、全米アカデミーズは、科学界と国家安全保障界の代表者、その他の連邦関連機関及び民間部門を集め、連邦政府が資金提供するオープンな科学研究システムを安全なものとし、強化するためのアプローチを検討するために 2022 年にワークショップを 4 回開催している（2022 年には 7 月 7 日・18 日・22 日、11 月 14~15 日）。

ワークショップでは、世界的に優秀な STEM 人材の獲得と維持、国際的な科学研究協力の促進、不正な海外からの干渉への対策などもテーマとして取り上げている。また、ワークショップでは、米国政府が支援する基礎研究の中で最も大きな割合を占め、多くの先端アプリケーション、新興技術、イノベーションを生み出している大学と連邦政府出資の研究開発センター（FFRDC）にも焦点を当てている。このワークショップでは、以下のようなトピックを取り上げた。(1) 重要な価値と資産としてのオープンサイエンスとテクノロジー研究、(2) グローバルな科学的関与と外国人人材の獲得、(3) 国際研究協力の利益とリスク評価、(4) オープンサイエンスの文脈における研究セキュリティ、(5) 科学研究コミュニティとセキュリティコミュニティの協力促進。

例えば、2022 年 11 月 14～15 日のワークショップでは、大学（インディアナ大学、カーネギーメロン大学、スタンフォード大学等）、連邦研究開発センター（ローレンスリバモア

国立研究所)、非営利機関、連邦政府機関（CIA）からの参加者の間で、以下のテーマについて、それぞれ約 1 時間ずつ討論した[83]。

- 国際的な STEM 人材と米国の研究競争力
- 国際共同研究：メリットと課題
- 代替アプローチの実用的な考察とリスク・ベネフィット
- コミュニティの自発的積極的関与（buy-in）とサイバーリスクの管理
- 科学研究、国家安全保障、法執行のコミュニティ間の協力関係の促進

(d) “Safeguarding Science” Toolkit の発表（2022 年 11 月 15 日）

2022 年 11 月 15 日に国家情報長官室（Office of the Director of National Intelligence）の米国防諜・セキュリティセンター（National Counterintelligence and Security Center: NCSC）が研究セキュリティ・インテグリティに対する広範なリスクに直面する研究者を支援するために、連邦政府機関、大学関係者と協力し、「Safeguarding Science ツールキット」（Safeguarding Science toolkit）を作成して公表した。このツールキットは、研究関係者が政府及び学術界のセキュリティのベストプラクティスにアクセスし、個々のニーズに合わせてツールを選択することを助けることが意図されている。[84]

このツールキットは、NSF、米国国立標準技術研究所（National Institute of Standards and Technology (NIST)）、運輸省及び連邦航空局（Federal Aviation Administration (FAA)）、保健福祉省、ホワイトハウス科学技術政策局、米国大学協会（American Association of Universities）と共同で NCSC によって開発され、インテグリティ、コラボレーション、開放性、セキュリティを重視する堅牢で弾力性のある米国の研究エコシステムを促進し、そのすべてがイノベーションを促進することを意図している。

NSPM-33 実施ガイダンスの「研究セキュリティプログラム」の第 5 項目（Development of research security content）では以下のように説明されていた。

> 連邦政府は、研究機関の裁量で研究セキュリティプログラムに組み込むことができるよう、研修内容やプログラム上のガイドライン、ツール、ベストプラクティスの開発を支援するための標準的な技術支援を提供する予定である。特に、国家防諜タスクフォース（National Counterintelligence Task Force）の代表機関が、米国防諜・セキュリティセンターと連携して、研究機関が研究セキュリティプログラム及びトレーニングの要件を満た

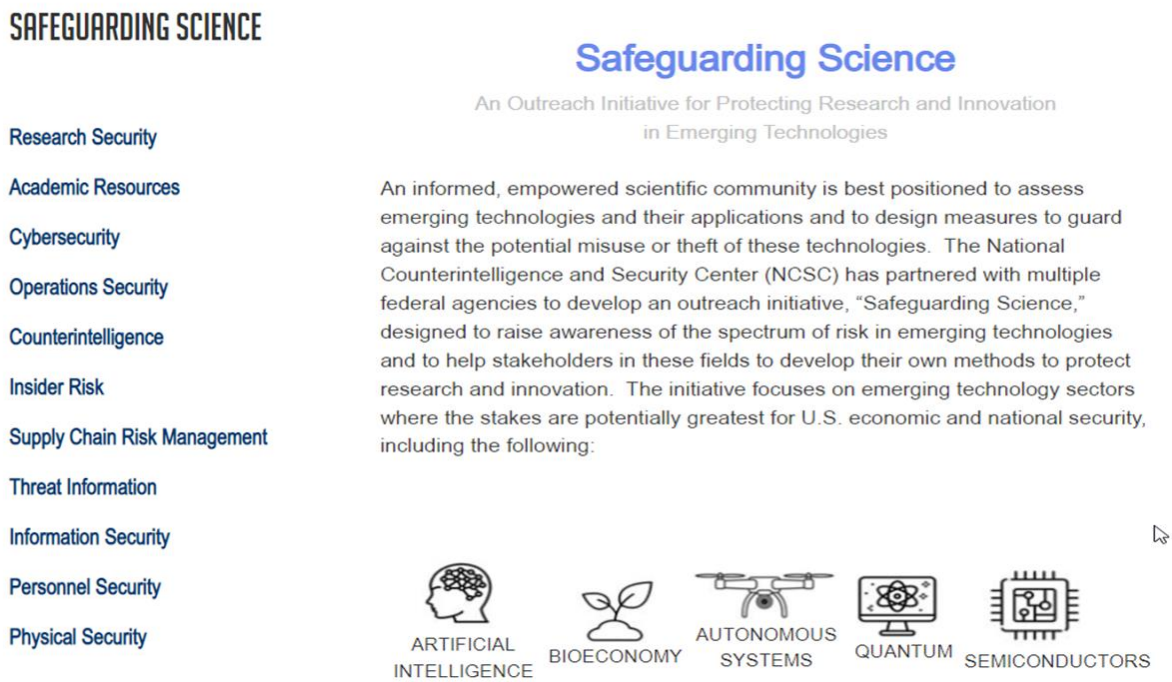
[83] Openness, International Engagement, and the Federally Funded Science and Technology Research Enterprise - A Workshop
<https://www.nationalacademies.org/event/08-29-2022/openness-international-engagement-and-the-federally-funded-science-and-technology-research-enterprise-a-workshop>

[84] “Safeguarding Science toolkit launched to help researchers defend scientific integrity.” NSF News. November 16, 2022
https://beta.nsf.gov/news/safeguarding-science-toolkit-launched-help

すために活用できるコンテンツを共同開発する。連邦政府は、研究機関向けの研究セキュリティプログラム情報及び実施リソースを開発・維持し、研究セキュリティプログラム内で使用するのに適したリソースを含むコミュニティコンソーシアムの形成を支援することを検討する必要がある。実務上可能な限り、プログラム内容の開発は、政府と組織との共同作業とすべきである。

このポータルサイトの作成について、NSF の研究セキュリティ戦略政策課長の Keiser 氏は「NSF は、連邦機関のパートナーと協力して、新しいオンラインの Safeguarding Science ツールキットの研究セキュリティセクションを提供できることを嬉しく思う」「このコンテンツを NSPM-33 実施ガイダンスの主要分野と合わせることで、現在進行中の研究セキュリティイニシアティブとそのガイダンスの意味を学界がより理解できるようにする。私たちは、研究コミュニティに役立つ情報とツールを提供し続けることを楽しみにしている」と述べている。

また、NSF 長官の Sethuraman Panchanathan 氏は「このツールキットは、研究者がオープンな共同研究を行うための枠組みを提供すると同時に、盗難や悪用などの脅威を寄せ付けないための保護を確立するもの」「このツールキットは、研究コミュニティや米国政府の科学・情報機関と連携し、リスクに対処するための情報、ベストプラクティス、ツールを共有し、研究エコシステムの繁栄を確保するために国際協力を推進する NSF の取組を示すものである」と述べている。



出典：Safeguarding Science: An Outreach Initiative for Protecting Research and Innovation in Emerging Technologies
<https://www.dni.gov/index.php/safeguarding-science>

図 2-3：「Safeguarding Science」ポータルサイト

(e) 「研究セキュリティプログラム」のドラフト公表（2023 年 2 月 28 日）

2023 年 2 月 28 日に大統領府科学技術政策局（OSTP）の研究セキュリティ小委員会が公表した「研究セキュリティプログラム標準要件案（DRAFT Research Security Programs Standard Requirement）」は、NSPM-33 実施ガイダンスの最後の条項である「研究セキュリティプログラム」に関するものである[85]。具体的には、NSPM-33 のセクション 4(g)は以下のとおりである。

> リスクの特定と分析：資金提供機関の長は、年間 5,000 万ドルを超える連邦科学技術支援を受ける研究機関に対し、その機関が「研究セキュリティプログラム」を確立し運営していることを資金提供機関に証明するよう求めるものとする。機関の「研究セキュリティプログラム」には、サイバーセキュリティ、海外渡航セキュリティ、内部脅威の認識と特定、及び必要に応じて輸出管理トレーニングの要素が含まれるべきである。資金提供機関の長は、米国の国家及び経済の安全保障に影響を与える重要かつ新興の技術分野における研究開発のために連邦政府の資金提供を受けている機関に対し、「研究セキュリティプログラム」の追加要件が適切であるかどうかを検討しなければならない。

対象研究機関は過去 2 年間の連続する各会計年度において、年間 5,000 万ドル以上の連邦科学技術支援を受けた研究組織である。連邦科学技術支援を受け、維持するための条件として、対象研究機関は、条件を満たす研究セキュリティプログラムを維持していることを証明しなければならない。自己認証は、対象となる研究機関に対し、年 1 回、SAM.gov（System for Award Management : U.S. General Services Administration が運営するウェブサイト）で集中的に行われる。

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それぞれ説明されている。このうち研究セキュリティのトレーニングについての説明は以下のとおり。

> 研究セキュリティのトレーニングは定期的に更新されなければならず、研究セキュリティの脅威の認識、識別、内部脅威などの構成要素を含む。研修は、教員、職員、学生など、適切な人員に合わせたものとする必要がある。対象となる研究機関は、毎年、そのトレーニングが要件を満たしていることを証明しなければならない。研修プログラムには、以下の分野での指導が含まれていなければならない。
>
> 1. 研究セキュリティが米国の研究開発にとって重要である理由と、何が海外からの干

[85] Subcommittee on Research Security. National Science and Technology Council. Office of Science and Technology Policy. DRAFT for Public Comment. DRAFT Research Security Programs Standard Requirement. Prepared by the Interagency Working Group on Research Security Programs, Subcommittee on Research Security, National Science and Technology Council. <https://www.whitehouse.gov/wp-content/uploads/2023/02/RS_Programs_Guidance_public_comment.pdf>

渉に当たるかを理解すること。

2. 米国の研究セキュリティの指針としての非差別の重要性。
3. 情報開示方針とそれがどのように使われるか。特に利益相反や責務相反について。
4. リスクの特定、管理、軽減（特に外国人人材採用プログラム、インサイダー脅威など）。
5. 資金の適切な使用。
6. 国際協力の価値と課題。
7. 責任ある海外渡航の実践。
8. サイバーセキュリティの基本的な衛生管理及びデータ保護の実践。ソーシャルエンジニアリングの脅威やサイバー侵害の認識と対応を含む。
9. 知的財産及びデータ保護の要件とベストプラクティス。

この「研究セキュリティプログラム標準要件」に対してのパブリックコメントの募集が2023年3月2日に開始された。2023年6月5日を期限として意見が求められている。[86]

OSTPは、関心のあるあらゆる利害関係者からのコメントを募集している。特に、OSTPは、研究セキュリティプログラムの要件の対象となる研究機関、研究者、研究機関を代表する専門組織、米国の研究エコシステム全体の多様な利益を代表する組織からの意見に関心をもっている。

特に以下の点についてのコメントが求められている。

1. 公平性（equity）：NSPM-33 の実施ガイダンスでは、研究セキュリティの方針と実践が公平かつ非差別的に実施されることを求めている。標準要件において、衡平性と非差別の基本的な約束が守られていないと思われる部分があるかどうか。
2. 明確性（clarity）：研究セキュリティプログラムの標準要件が明確であることが不可欠である。明確であることで、公平性、透明性、及びコンプライアンスが可能になる。特に、組織が標準要件の規定を理解し、遵守する能力に関連する、標準要件全体の明確さに関するコメントを求める。本基準の要求事項がどの程度明確であり、素直に採用できるのかどうか。
3. 実現可能性（feasibility）：研究セキュリティプログラム標準要件は、対象組織が採用を実現可能であると考える場合に、最も成功する。このことを念頭に置いて、標準要件には、実装の点で懸念される側面があるか。ある場合、その方法と理由は何か。
4. 負担（burden）：実現可能性と密接に関連するのは、負担である。研究コミュニティとの関わりから、金銭的な負担であれ、事務的な負担であれ、負担に対する懸念が高いことを理解することができた。標準要件の条項は、SAM.gov での認証の一元化や、

[86] 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 <https://www.federalregister.gov/documents/2023/03/07/2023-04660/request-for-information-nspm-33-research-security-programs-standard-requirement>

研究セキュリティトレーニングの開発に対する技術支援など、負担を軽減することを目的に設定されている。標準要件を実施する上で、研究コミュニティの負担を軽減するための他の方策はあるかどうか。

5. コンプライアンス：標準要求事項の草案では、要求事項への準拠の主要なモデルとして「自己認証」を提案しており、標準要求事項の発行から 1 年後に最初の認証が必要であるとしている。これらのアプローチについて、どのように考えるか。他に考慮すべき点はあるか。

2.1.2 資金配分機関における取組

2022 年には以下のように研究提案申請書の共通情報会議フォーム等のドラフト案が公表され、パブリックコメントが行われた。資金配分機関（NSF、NIH、DOE 科学局、DARPA）の取組について説明する前に、まず、この内容について説明する。

Common Disclosure Forms for the Biographical Sketch のパブリックコメント（2022 年 8 月 31 日）

米国科学財団（NSF）は、米国科学技術会議（NSTC）の研究セキュリティ小委員会を代表して、研究申請書の「経歴」（Biographical Sketch）と「現在及び未決の（その他）支援」（Current and Pending (Other) Support）のセクションの共通開示フォームについてパブリックコメントの募集を 2022 年 8 月 31 日に開始した。Biographical Sketch と Current and Pending (Other) Support の両方で収集されるすべてのデータ要素とその関連属性をまとめた Excel スプレッドシートをパブリックコメント用に添付している[87]。意見の募集は 2022 年 10 月 31 日までであり、それを踏まえ、最終的に決定される見込みである。

前述のように、NSPM-33 の 4(b)項では、「研究助成機関は、連邦政府が資金提供する研究開発事業への参加者から、潜在的な利益相反と責務に関連する情報の開示を求めるものとする」と指示されている。第 4(b)(vi)は、「各省庁は、最初の開示と毎年の更新のための書式を標準化し、これらの書式に付随して、関連する管理負担を最小限に抑えるための明確な指示を提供するべきである」と指示している。これを踏まえ、数ヶ月間、NSTC 研究セキュリティ小委員会は、シニアパーソン（上級研究員）からの一貫した開示要件を策定するとともに、連邦研究開発補助金又は協力協定の申請書の「経歴」「現在及び未決の（その他）支援」セクションの共通開示フォーム案を策定することに取り組んできたとのことである。

共通開示フォーム案は次表のとおりであるが、共通開示フォームの案について、以下の点について意見を求めていた。

(a) 提案された情報収集が、実用的な有用性を有するかどうかを含め、NSF の機能を適切に遂行するために必要であるかどうか。
(b) 提案された情報収集の負担に関する見積もりの正確さ（「経歴」と「現在及び未決の（その他）支援」の記入についてそれぞれ約 1 時間を要するとの見積もりについて）。
(c) 自動収集技術又は他の形態の情報技術の使用を含む、回答者に関する情報の質、有用性、及び明確性を高める方法。

[87] Federal Register/Vol. 87, No. 168/Wednesday, August 31, 2022/Notices
National Science Foundation. Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support <https://www.federalregister.gov/documents/2022/08/31/2022-18746/agency-information-collection-activities-request-for-comment-regarding-common-disclosure-forms-for>

(d) 適切な自動化、電子化、機械化、その他の技術的収集技術又はその他の形態の情報技術の利用を含め、回答すべき者の情報収集の負担を最小限にする方法。

表 2-26：「経歴」（Biographical Sketch）の情報開示フォームの案

	Section	*	Field	Format	More than one submission possible
1	Identifying Information	*	Name	Last, First(Middle, Suffix)	No
2			Persistent Identifier (PID) of the Senior/Key Person	URL, e.g.: https://orcid.org/NNNN-NNNN-NNNN-NNNN	No
3		*	Position Title	--	No
4	Organization and Location	*	Name	--	No
5		*	Location	City, (State/Province [XX],)Country	
6	Professional Preparation	*	Name of Organization	--	Yes
7		*	Location of Organziation	City, (State/Province [XX],)Country	
8		*	Degree Received (if applicable)	--	
9		*	Month and Year the Degree was Received (or expected receipt date)	MM/YYYY	
10		*	Field of Study	--	
11	Appointments and Positions	*	Start Date	YYYY	Yes
12		*	End Date	YYYY	
13		*	Appointment or Position Title	--	
14		*	Name of Organization	--	
15		*	Department (if applicable)		
16		*	Location of Organziation	City, (State/Province [XX],)Country	
17	Products	*	Names of Authors	Last, First Initial	Yes
18		*	Product Title	--	
19		*	Date of Publication or Release	DD/MM/YYYY	
20		*	Website URL	--	
21		*	Product Persistent Identifier	URL, e.g.: https://doi.org/10.NNNN/NXNXN	
22		*	Other Relevant Citation Information	--	
23	Certification	*	Signature	--	No
24		*	Date	DD/MM/YYYY	

出典：National Science Foundation. NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization
<https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp>

表 2-27：「現在及び未決の（その他）支援」（Current and Pending (Other) Support）の情報開示フォームの案

	Section	*	Field	Format	Character Limit	More than one submission possible
1	Identifying Information	*	Name	Last, First(Middle, suffix)		No
2			Persistent Identifier (PID) of the Senior/Key Person	URL (e.g.: https://orcid.org/NNNN-NNNN-NNNN-NNNN)		No
3		*	Position Title	--		No
4	Organization and Location	*	Name	--		No
5		*	Location	City, (State/Province [XX],)Country		
6	Project/Proposals	*	Project/Proposal Title	--	300	Yes
7		*	Status of Support	"Pending" or "Current"		
8			Proposal/Award Number (if available)	--		
9		*	Source of Support	--	60	
10		*	Primary Place of Performance	City, (State/Province [XX],)Country		
11		*	Project/Proposal Start Date	MM/YYYY		
12		*	Project/Proposal End Date	MM/YYYY		
13		*	Total Award Amount	$N,NNN,NNN,NNN,NNN	13 numerical	
14		*	Person-Month(s) (or Partial Person-Months) Per Year Committed to the Project	YYYY:NN.NN		
15		*	Overall Objectives	--	1500	
16		*	Statement of Potential Overlap	--		
17	In-Kind Contributions	*	Status of Support	"Pending" or "Current"		Yes
18		*	Source of Support	--	60	
19		*	In-Kind Contribution Start Date	MM/YYYY		
20		*	In-Kind Contribution End Date	MM/YYYY		
21		*	Summary of In-Kind Contribution	--	300	
22		*	Person-Month(s) (or Partial Person-Months) Per Year Associated with the In-kind Contribution	YYYY:NN.NN		
23		*	US Dollar Value of In-Kind Contribution	$N,NNN,NNN	13 numerical	
24		*	Overall Objectives	--	1500	
25		*	Statement of Potential Overlap	--		
26	Certification	*	Signature	--		No
27		*	Date	DD/MM/YYYY		

注：”Project/Proposals”のセクションでは、すべての現在あるプロジェクトと、現在資金提供を検討中のすべてのプロジェクトを開示する。”In-Kind Contributions”のセクションでは、現在及び未決の支援に関連するすべての現物支給を開示する。現物支給には、オフィスや研究室のスペース、設備、消耗品、従業員や学生のリソースが含まれるが、これらに限定されるものではない。

出典：National Science Foundation. NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization
<https://www.nsf.gov/bfa/dias/policy/nstc_disclosure.jsp>

表 2-28：近年の研究インテグリティ関連文書（米国資金配分機関）

発行年	文書名	発行元
2020.6	NIH Protecting U.S. Biomedical Intellectual Innovation	NIH
2021.7	NIH Foreign Interference Summary of Findings	NIH
2021	NIH Frequently Asked Questions (FAQs) Other Support and Foreign Components	NIH
2021.6.16	NSF Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support（その後、2021 年 8/24・9/1、2022 年 1/10、4/20、2023 年 1/30 に更新）<https://www.nsf.gov/bfa/dias/policy/disclosures_table/june2021.pdf>	NSF
2022.8.31	パブリックコメント(~2022/10/31) : Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support <https://www.federalregister.gov/documents/2022/08/31/2022-18746/agency-information-collection-activities-request-for-comment-regarding-common-disclosure-forms-for>	NSF
2022.9.1	NSPM-33 Implementation Guidance: Pre- and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support <https://www.nsf.gov/bfa/dias/policy/nspm_disclosuretable/nspm33_disclosuretable_sept2022.pdf>	NSF
2023.1.30	NSF Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending (Other) Support 更新版 <https://www.nsf.gov/bfa/dias/policy/disclosures_table.jsp>	NSF

出典：Stanford University website. “Academic Integrity and Undue Foreign Interference” <https://doresearch.stanford.edu/topics/academic-integrity-and-undue-foreign-interference#Policies_&_Resources>等に基づき作成。

近年の研究インテグリティ関連の資金配分機関からの公表文書等は表 2-27 のとおりである。以下、調査対象の資金配分機関における取組についてそれぞれ説明する。

(1) 米国科学財団（NSF）

NSF のウェブサイトの記載によれば、NSF は連邦政府が資金を提供する研究コミュニティと NSF スタッフのために、研究のセキュリティとインテグリティを強化する措置を講じることに熱心に取り組んできたとのことであり、措置には以下が含まれる。[88]

- NSF の職員と NSF が資金を提供する機関及び研究者の両方に対して、NSF の「提案及び採択方針と手順ガイド」（Proposal & Award Policies & Procedures Guide (PAPPG)）の開示規則の遵守を強調する。
- すべての NSF 職員が米国市民であること、又は市民権を取得する過程にあることを

[88] National Science Foundation. “Research Security” <https://beta.nsf.gov/research-security>

要求する。

- NSF 職員が外国人人材採用プログラムに参加することを禁止する。
- NSF の全職員に対して、毎年「科学とセキュリティのトレーニング」を義務付ける。

NSF 職員等向けのトレーニング

NSF 職員等には研究セキュリティ関連のトレーニングの受講を義務付けている。1 つ目のコースは、「科学とセキュリティのトレーニング」である。NSF の情報開示方針と、外国政府の人材採用プログラムに関する NSF の新しい方針について学ぶ。このコース受講は、NSF の全スタッフとコントラクターに対して毎年義務付けられている。

2 つ目のコース「科学とセキュリティのトレーニング：パート 2」は、プログラム担当者が助成決定前の情報のリスク評価をどのように行うべきかというガイダンスとともに、助成決定後の情報の取り扱いに関する内部プロセスの実施について概説する。このコースは、NSF のすべてのプログラムオフィサーとグラント管理者に受講が義務付けられており、NSF の全職員を対象としている。このコースは、特に PAPPG の改訂ガイダンスの説明に重点を置いている。

研究コミュニティ向けのトレーニングの開発

NSF は、研究コミュニティ向けに研究セキュリティトレーニングを開発する取組も支援している。NSF は、国立衛生研究所、エネルギー省、国防省と共同で、連邦研究費の受給者に世界の研究エコシステムに対するリスクと脅威に関する情報、及びこれらのリスクから保護するために必要な知識とツールを提供するオンライントレーニングモジュールの開発に関する提案を求める公募を行った。

現在、以下のトピックについて 4 つのトレーニングモジュールが開発中である。

1. なぜ研究セキュリティは重要な問題なのか？このトレーニングでは、研究セキュリティの問題点と、連邦政府が資金提供する研究の研究セキュリティが米国政府と国家安全保障にとって重要である理由について説明する。
2. 情報開示ポリシーとは何か、どのように使われるのか？このトレーニングでは、連邦資金提供機関の方針、なぜこの情報が重要なのか、そしてどのように使用されるのかについて説明する。
3. 連邦政府から資金提供を受けた受領者は、リスクを管理し軽減するためにどのような行動を取ることができるのか？本トレーニングでは、組織がどのようにして次世代の研究者の育成を含む研究のスチュワードとしての役割を果たすことができるのか、強固なリーダーシップと監督を示すこと、透明性を促進し、利益相反や責務相反から守るためのポリシーを確立し管理すること、研究セキュリティに関するトレーニング・支援・情報を提供すること、組織のポリシーを遵守するための効果的なメカニズムを確保すること、共同研究やデータに関する潜在リスクを評価・管理するプロセスを実施する

ことを説明する。

4. 国際共同研究は奨励されるのか？このトレーニングでは、原則的な国際協力は成功に不可欠であるが、外国の不適切な影響力は科学技術事業における国際協力の脅威であることを強調し、その重要な違いについて説明する。

NSF は「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）を選定した（NIH、DOE、DOD と共同で助成）。[89]

- 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）

NSF-77: Data Analytics Application Suite

2021 年 9 月の System of Records Notice (SORN)「NSF-77: Data Analytics Application Suite」は、NSF の内部データの許容利用を拡大するものである。NSF が支援する活動に参加する個人や組織から報告された情報を、研究事業に関連する公開情報とともに集約、連携、分析することが可能になる。これは、プライバシー法に基づくプロセスである。NSF-77 により、NSF は以下の事項に取り組むことができる。[90]

- 資金調達の成果と科学的事業に関する理解を結びつける。
- 多様性・公平性・包摂の活動やプログラムに対する NSF の理解を深める。
- 研究セキュリティの調整を改善し、正確性と公平性を保証する。
- 戦略的計画、共同研究、プログラム開発を強化する。

SORN は、PII 情報（personally identifiable information（個人を特定できる情報））を NSF の外部と共有することができる 3 つの状況（「日常的な使用」と呼ばれる）を規定して

---

[89] NSF 2022 Research Security Training for the United States Research Community awardees announced. December 9, 2022
<https://beta.nsf.gov/news/nsf-2022-research-security-training-united-states>
National Science Foundation. Research Security Training for the United States (U.S.) Research Community (PROGRAM SOLICITATION). May 23, 2022.
<https://www.nsf.gov/pubs/2022/nsf22576/nsf22576.htm>
関連記事は、Jeffrey Mervis. “NSF turns to big data to check if grantees have foreign ties” *Science*. 2022 Oct 7;378(6615):16. PMID: 36201572 DOI: 10.1126/science.adf1849

[90] Rebecca Keiser, Chief of Research Security, Strategy & Policy (CRSSP) Office of the Director. Research Security and Responsible Internationalization. Presentation to the NT-50 May 5, 2022
<https://researchservices.upenn.edu/wp-content/uploads/2022/04/Rebecca-Keiser-NSF-presentation.pdf>

いる。

1) NSF に報告された情報と他の情報源（例えば、発表された論文、特許など）との間の潜在的な矛盾を検証するために、NSF の資金提供を受けている機関と情報を共有することがある。

2) NSF の開示要件との矛盾が検証された情報は、国家及び研究の安全保障に関連する取組に情報を提供するために、連邦機関と共有されることがある。

3) ポートフォリオ管理の改善、イニシアティブの調整、及び科学的状況に対する政府の理解向上のため、連邦科学技術機関と情報を共有することがある。

SORN は 2021 年 11 月 9 日に公示され、12 月 9 日に効力を有するとしている。

なお、本システムは、以下のグループの個人に関する情報を含む。NSF にプロポーザルを提出する PI 及びシニアパーソン、NSF が資金提供する研究に参加した、又は NSF から資金提供を受けた大学院生、博士研究員、学部生、NSF から資金提供を受けたフェロー、学術論文又はその他の関連資料をパブリックドメインで発表した研究者、科学技術関連のメディアを発行する個人、科学技術関連部門（産業、NPO、教育、政府）の仕事とタイトルを公表している個人。[91]

Science and CHIPS Act of 2022 関連の措置

前述のように、以下は Science and CHIPS Act of 2022 により NSF が対応を要求されている事項である。

- NSF の研究セキュリティを強化する。この法律は、潜在的なセキュリティリスクを特定するために、NSF に Research Security and Policy Office を維持することを要求している。
- 研究者にベストプラクティスを教育し、連邦職員と大学研究者が悪意のある外国人人材採用プログラムに参加することを禁止する。この法律は、連邦研究機関から資金を得ようとする対象者に対し、研究セキュリティに関する年次研修を受けることを義務付ける。
- 研究セキュリティとインテグリティの情報共有組織を設立する。この法律は、研究機関や研究者が研究セキュリティを損なう不適切で違法な取組を特定するのに役立つ情報のクリアリングハウスとして機能する組織の設立を要求している。[92]
- 透明性を確保する。 この法律は、NSF の資金を申請する大学に対し、中国や「その他の懸念される外国」（foreign countries of concern）からの協定や贈与を情報開示するよう求めている。また、孔子学院を持つ大学に NSF の資金を提供することを禁止して

[91] Federal Register/Vol. 86, No. 214/Tuesday, November 9, 2021/Notices
National Science Foundation Privacy Act of 1974; System of Records
<https://www.govinfo.gov/content/pkg/FR-2021-11-09/pdf/2021-24487.pdf>

[92] 関連記事は、Richard L. Hudson. US science agency plans new centre for research security. *Science Business*. 17 Nov 2022. <https://sciencebusiness.net/news/us-science-agency-plans-new-centre-research-security>

いる。

情報開示の要求

Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 23-1, January 30, 2023) の第 II 章の B と D において、提案者による情報開示について説明されている[93]。

提案書の準備と提出プロセスの一環として、提案書に記載されたすべてのシニアパーソンは、審査員及びプログラム担当者が情報に基づいた推奨と資金調達の決定を行う際に役立つ情報を提出することが求められる。これらの情報開示は、以下の提案セクションで提供される。

・略歴（第 II 章 D.h(i)を参照のこと）。
・現在及び未決の支援（第 II.D.h(ii)章を参照）
・共同研究者及びその他の関係者（第Ⅱ章 D.h(iii)を参照）。

経歴書及び現在及び未決の支援文書では、提供された情報が正確、最新、かつ完全であることを個人が証明することが要求される。情報開示の要件に違反した場合、違反の特定の事実に基づいて適切とみなされる、刑事、民事、及び/又は行政上の結果につながる可能性がある。違反は、NSF の監察官室（OIG）によって徹底的に調査され、正当な理由がある場合には、司法省内の刑事・民事部門に照会される。

NSF は、違反を取り巻く事実に応じて、またデュープロセスの要件に合致するように、様々な措置を検討することができる。そのような措置には、以下が含まれるが、これらに限定されるものではない。

- NSF に提出された提案の不受理。
- これらの要件に違反した個人が、NSF のアワードの下で業務を遂行することを許可されないようにすること。
- NSF の審査員として参加する資格の喪失。
- アワードの一時停止又は終了
- SAM 又は FAPIIS（Federal Awardee Performance and Integrity Information System）に個人又は研究組織を登録し、他の機関に警告する。

[93] *Proposal & Award Policies & Procedures Guide* (PAPPG) (NSF 23-1). January 30, 2023. Chapter II: Proposal Preparation Instructions. B. NSF Disclosure Requirements

表 2-29：NSF における略歴、現在とペンディングの（その他）支援に関連する授与前及び授与後の開示要件

活用の種類	経歴	現在・未定（その他）の支援	施設、装置、その他資源	年次プロジェクト報告書	受賞後の情報	開示は必要ではない
専門的な準備（例：教育と訓練など）	X					
学術的、専門的、又は組織的なアポイントメント（報酬を受け取っているかどうか、フルタイム、パートタイム、又はボランタリーかどうかに関わらず）。	X					
提案団体、他団体、個人への直接支援の有無、金銭的価値の有無にかかわらず、現在検討中のすべてのプロジェクト（本プロジェクトを含む）、及び進行中のすべてのプロジェクト（例えば、受け取った支援がオフィス/研究室のスペース、機器、消耗品、従業員などの現物寄付であっても）。		X		X	X	
提案中のプロジェクト/提案に使用する、研究活動を支援する現物寄付			X			
提案されているプロジェクト/提案に使用することを目的とせず、関連する時間的制約がある現物寄付		X		X	X	
最近終了した支援又は終了した支援						X
外国政府が主催する人材採用プログラムを含む、外国政府、団体、又は事業体が主催するプログラムへの現在又は申請中の参加。		X（契約に依る）	X（契約に依る）	X	X	
外部団体から支援を受けている博士研究員、学生、客員研究員で、その研究活動が提案中のプロジェクト/提案に使用されることを目的としているもの。			X			
外部団体から支援を受けている博士研究員、学生、客員研究員で、その研究活動が提案中のプロジェクト/提案に使用することを目的とせず、関連する時間的制約がある場合。		X		X	X	
個人の所属組織との任命/契約の一部とみなされ、提案組織の「組織外活動」方針及び手順と一致するコンサルティング						X
個人の任命/合意の範囲外のコンサルティング、機関の契約とは別のもの		X		X	X	
会議又はワークショップに参加するために、外部団体から支援/支払われる旅費						X
時間的制約を伴う研究活動を行うために、外部団体から支援/支給される旅行		X		X	X	
研究の監督、監修、共著とは無関係に、名誉を与えるため、又は尊敬、尊重、賞賛を象徴する目的で贈られる謝礼やその他の金銭。						X
教育のコミットメント						X

活用の種類	経歴	現在・未定（その他）の支援	施設、装置、その他資源	年次プロジェクト報告書	受賞後の情報	開示は必要ではない
組織からライセンスされた知的財産（IP）に基づくスタートアップ企業						X
組織からライセンスされていない知的財産（IP）に基づくスタートアップ企業		X		X	X	
提案機関・出身機関から本人に提供されるスタートアップ・パッケージ						X
提案機関・母体機関以外からのスタートアップ・パッケージ		X		X	X	
制限のない贈答。						X
研修アワード、賞品						X
任命の一部としてのメンタリング、又は個人の研究活動に関与しないメンター/メンティーの取り決め						X
学年給、又は所属機関から本人に支給される給与						X
広く利用可能な基幹施設及び/又は共有機器						X
提案機関/母体機関に提供される F&A 償還金						X

出典：National Science Foundation, “NSF Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support,” January 30, 2023. <https://www.nsf.gov/bfa/dias/policy/disclosures_table.jsp>

(2) 国立衛生研究所（NIH）

NIH の Francis Collins 所長は、2018 年 8 月に「米国の生命医学研究のインテグリティを保護すること」について声明を公表した。そこで、懸念される 3 つの分野として、1）NIH 資金提供機関の一部の研究者が、外国政府を含む他の組織からの実質的な資源の提供を開示せず、NIH 資金の適切な使用に関する決定を歪める恐れがある、2）助成申請や、NIH が支援する生物医学研究から生まれた知的財産が他の国を含む組織に転用される、3）場合によっては査読者が機密情報を他者と共有（場合によっては外国組織を含む）、あるいは助成決定に影響しようとすることがあることを指摘した。[94]

NIH は、他の政府機関、NIH が資金提供する学術機関、米国の専門機関、及び NIH 所長諮問委員会のワーキンググループと協力して、以下について強固な方法を特定することを意図している。

1）すべての研究支援源、金銭的利益、所属の正確な報告を改善すること。

2）外国の科学者や機関とのものを含む NIH の長い伝統の共同研究を継続しながら、知的財産の安全性へのリスクを軽減すること。

3）査読のインテグリティを保護する追加のステップを取ること。

[94] Francis S. Collins, M.D., Ph.D. Director, National Institutes of Health. Statement on Protecting the Integrity of U.S. Biomedical Research. August 23, 2018.

研究申請書における情報開示

NIH のウェブサイトでは、情報開示について以下のように説明している。

- NIH の申請書及び NIH 助成金の期間を通じての完全な透明性は重要である。NIH は、研究申請書や助成金において、すべての研究支援源、海外からの資金提供、シニア／キーパーソンの金銭的利益相反の開示を要求している。NIH は、提案されている研究が重複する可能性のある他の資金源を受けていないか、必要な時間配分ができているか、金銭的利害が研究実施の客観性に影響を与える可能性がないかなどを判断するため、資金提供の決定を行う際にこの情報を使用する。[95]
- [申請者及び受領機関の責務】申請者及び受領機関は、以下を行わなければならない。
  - ✓ 申請書、進捗報告書（Research Performance Progress Reports）、及び「Just in Time」の提出書類には、すべての研究支援源、及びシニア／キーパーソンとして指名された個人の関連する所属について正確かつ完全に説明するよう、教員及びその他の職員と協力して確認する。
  - ✓ 助成金業務に携わるすべての上級／主要担当者が、規制及び組織の方針に従って、重要な財務的利害を開示することを確実にする。
  - ✓ NIH に提出するすべての報告書や連絡事項が完全かつ正確であることを確認する。
  - ✓ 連邦政府が資金提供した研究の適切な管理の一環として、専有情報（proprietary information）及び機密性の高いデータ（sensitive and confidential data）を保護する。
  - ✓ Sensitive な個人情報の不用意な開示、公開、又は紛失を防ぐために、合理的かつ適切なあらゆる措置を講じること。
  - ✓ NIH が支援する活動に重大な影響を与える開発については、直ちに NIH に通知する。
  - ✓ シニア／キーパーソンの経歴書やその他の支援の更新から、申請書の提出、進捗報告、最終報告書の提出まで、あるいは NIH の助成金に影響を与える重大な変更があった場合はいつでも、助成金のプロセス全体を通じて情報を開示すること。
  - ✓ NIH アワードに外国のコンポーネント（foreign components）を含める場合は、NIH の事前承認を得ること。
- NIH の責務は以下のとおりである。
  - ✓ 助成金授与の監視を維持する
  - ✓ 受賞前及び受賞後に、研究責任者を含む上級職／基幹職の「その他の支援」（Other Support）情報の更新を確認・承認する。
  - ✓ NIH プロジェクトに外国のコンポーネントを追加するためのリクエストを検討し、

[95] Requirements for Disclosure of Other Support, Foreign Components and Conflicts of Interest <https://grants.nih.gov/policy/foreign-interference/requirements-for-disclosure>

適切であれば承認する。

- ✓ 助成金授与の条件を確実に遵守するために、機関と協力する。
- ✓ ピアレビュープロセスの機密性・セキュリティを含むインテグリティを促進する。
- ✓ 補助金コンプライアンスに関連する潜在的な問題が発生した場合、機関に連絡する。
- ✓ 申請者と受給者に情報、ガイダンス、技術支援を提供する。

表 2-30：NIH におけるシニア/キーパーソンの略歴及びその他の支援に関連する授与前及び授与後の開示要件

活用の種類	経歴	その他の支援	年次プロジェクト報告書	受賞後の情報	開示は必要ではない
専門的な準備（例：教育、学位など）	X				
組織的な所属とアポイントメント	X				
学術的、専門的、又は組織的なアポイントメント（報酬を受け取っているかどうか、フルタイム、パートタイム、又はボランタリーかどうかに関わらず）。	X				
提案団体、他団体、個人への直接支援に関わらず、また金銭的価値の有無に関わらず（例えば、受けた支援がオフィス/研究室のスペース、設備、消耗品、従業員などの現物であっても）、現在あらゆるソースから検討中のすべてのプロジェクト、及びすべての進行中のプロジェクト。		X	X	X	
最近終了した支援又は終了した支援					X
外国政府が主催する人材採用プログラムを含む、外国政府、団体、又は事業体が主催するプログラムへの現在又は申請中の参加。	X（契約に依る）	X（契約に依る）			
提案されているプロジェクト/提案に使用することを意図していない現物寄付		X	X	X	
外部資金による研究室の客員研究員		X		X	
外部団体から資金提供を受けている学生及びポスドク研究者		X	X	X	
個人の任期の範囲外のコンサルティング、機関の契約とは別のもの		X	X	X	
個人が所属する機関への任命/契約の一部とみなされるコンサルティング（例：外国機関の PI が所属する機関内での保持契約など）。					X
時間的制約を伴う研究活動を行うために、外部団体から支援/支給される旅行		X	X	X	
会議又はワークショップに参加するために、外部団体から支援/支払われる旅費					X
研究の監督、監修、共著とは無関係に、名誉を与えるため、又は尊敬、尊重、賞賛を象徴する目的で贈られる謝礼やその他の金銭。					X

活用の種類	経歴	その他の支援	年次プロジェクト報告書	受賞後の情報	開示は必要ではない
教育のコミットメント					X
組織からライセンスされた知的財産（IP）に基づくスタートアップ企業					X
提案機関・出身機関から本人に提供されるスタートアップ・パッケージ					X
提案機関・母体機関以外からのスタートアップ・パッケージ		X	X	X	
研修アワード、賞品、贈答品。贈答品とは、見返りを期待せずに提供される資源（時間、サービス、特定の研究活動、金銭など）。					X
任命の一部としてのメンタリング、又は個人の研究活動に関与しないメンター/メンティーの取り決め					X
年収、又は所属機関から本人に支給される給与					X
広く利用可能な基幹施設及び/又は共有機器					X
提案機関/母体機関に提供される F&A 償還金					X
開示された情報が正確、最新、完全であることを本人が証明すること（例：研究者の署名など）		X	X		
裏付けとなる書類（契約書、助成金、その他の契約書など）		X			
重要な金銭的利害関係（「その他の支援」では必要ない開示）。※NIH FCOI ポリシー NIH GPS 4.1.10 を参照して記入。					X

出典：NIH. Pre-award and Post-award Disclosures Requirements Related to Biographical Sketch and Other Support for Sr./Key Personnel <https://grants.nih.gov/policy/foreign-interference/requirements-for-disc>

海外からの干渉のコンプライアンスレビュー結果

NIH では、海外からの干渉（foreign interference）についての調査を実施してきており、2022 年 12 月 9 日に公表された報告書（*Brief Summary of NIH Foreign Interference Cases*）は、2022 年 12 月 5 日時点の NIH における海外からの干渉についてのコンプライアンスレビューの特徴と結果をまとめたものである。NIH Office of Extramural Research のスタッフが大学・研究機関に連絡した 246 件のケースに焦点を当てている。[96]

表 2-31 は、懸念の元のソースに応じた海外からの干渉事例の特徴を示している。最も多いのは内部的なもので、NIH 機関職員が助成金文書と公表資料の不一致を発見したものである。過去 2 年間では、自己申告が増加し、司法省や FBI からの照会は減少している。これらの科学者の多くはアジア系であると自己申告している（市民権や国籍に関するデータは収集していない）。海外からの干渉の懸念の大部分を占めるのは中国関連であった。

[96] Michael Lauer, National Institutes of Health (NIH) Office of Extramural Research (OER) Patricia Valdez, NIH OER. Brief Summary of NIH Foreign Interference Cases. 2022-12-11. https://grants.nih.gov/sites/default/files/Foreign-Interference-12-9-22-report.pdf

表 2-32 は、これまでのコンプライアンス・レビューの結果である。ほとんどのレビューが未解決であるにもかかわらず、すでに 80%以上のケースで、少なくとも 1 つの重大なコンプライアンス違反があったと判断されている。10%未満は違反なしと判断された。半数以上の科学者が NIH グラントから外された。

表 2-31：NIH Office of Extramural Research に報告された外国からの干渉事例

特徴		内部	自己開示	司法省/FBI
合計		117)(47.6)	77 (31.3)	52 (21.1)
機関への連絡年	2018～2019 年	94 (80.3)	21 (27.3)	43 (82.7)
	2020～2022 年	23 (19.7)	56 (72.7)	9 (17.3)
性別	男性	96 (82.1)	65 (84.4)	38 (73.1)
	女性	17 (14.5)	9 (11.7)	10 (19.2)
人種	アジア人	93 (79.5)	49 (63.6)	40 (76.9)
	白人	18 (15.4)	21 (27.3)	3 (5.8)
国名	中国	107 (91.5)	66 (85.7)	52 (100.0)

注）数値は、NIH 職員が研究機関に連絡した事例数を示す。かっこ内の数値は%。
出典：Michael Lauer, National Institutes of Health (NIH) Office of Extramural Research (OER) and Patricia Valdez, NIH OER. *Brief Summary of NIH Foreign Interference Cases*. 2022-12-11. <https://grants.nih.gov/sites/default/files/Foreign-Interference-12-9-22-report.pdf>

表 2-32：NIH の海外からの干渉事例のレビュー結果

レビュー結果		数（%）
合計		246 (100.0)
違反内容	非開示の所属	208 (84.6)
	非開示のグラント支援	171 (69.5)
	非開示の人材採用アワード	130 (52.8)
	非開示の株式、特許、SFI	44 (17.9)
	重大な違反	208 (84.6)
	違反なし	14 (5.7)
措置	終了・辞任	103 (41.9)
	助成金からの機関の除外	53 (21.5)
	助成金からの除外	156 (63.4)
	ピアレビューからの除外	193 (78.5)
	コンプライアンスレビュー継続中	142 (57.7)

出典：Michael Lauer, National Institutes of Health (NIH) Office of Extramural Research (OER) and Patricia Valdez, NIH OER. *Brief Summary of NIH Foreign Interference Cases*. 2022-12-11. <https://grants.nih.gov/sites/default/files/Foreign-Interference-12-9-22-report.pdf>

(3) エネルギー省科学局

エネルギー省（Department of Energy: DOE）科学局のウェブサイトでは、「研究開発を加速させるためには国際協力が不可欠であるが、一部の政府は米国の科学技術の進歩や知的財産へのアクセスを積極的に追求し、経済的繁栄と安全保障を害している。DOE は、オープンで協力的な研究開発を維持しながら、研究セキュリティを確保するために、リスクを管理するための意図的かつ包括的な措置を講じてきた」と説明している[97]。その結果、DOE 命令 486.1A（DOE Order 486.1A）「外国政府の後援又は提携活動」（Foreign Government Sponsored or Affiliated Activities）など、DOE 及び研究所職員による潜在的な利益相反及び責務相反への対処を中心とした、多くの方針変更を行ってきたとのことである。

以下は、関連するすべての DOE 命令とポリシーである。

- DOE Order 486.1A, Foreign Government Sponsored or Affiliated Activities <https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder-a>
- DOE Policy 485.1A, Foreign Engagements with DOE National Laboratories <https://www.directives.doe.gov/directives-documents/400-series/0485.1-APolicy-a#:~:text=CURRENT%20DOE%20P%20485.1A%2C%20Foreign%20Engagements%20

[97] Office of Science. Department of Energy. "Office of Science Laboratory Policy: Science and Security" <https://www.energy.gov/science/office-science-laboratory-policy-science-and-security>

with%20DOE,bedrock%20for%20U.S.%20scientific%20research%20and%20technological%20development>

- DOE Order 483.1B Change 2, Cooperative Research and Development Agreements (CRADAS) <https://www.directives.doe.gov/directives-documents/400-series/0483.1-BOrder-b-chg2-ltdchg>
- DOE Order 481.1E Change 1, Strategic Partnership Projects (SPPs) Strategic Partnership Projects <https://www.directives.doe.gov/directives-documents/400-series/0481.1-BOrder-e-chg1-ltdchg>
- DOE Order 142.3B, Foreign National Access Program <https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b/@@images/file>
- DOE Order 550.1 Change 1 (LtdChg), Official Travel <https://www.directives.doe.gov/directives-documents/500-series/0550.1-BOrder-chg1-ltdchg>

研究提案時等における情報開示

2022 年 6 月 1 日に Financial Assistance Letter（FAL）がエネルギー省より出され、現在及び未決（pending）の支援についての開示要件の現状について以下の説明をしている。[98]

- エネルギー省と NNSA（National Nuclear Security Administration）の大半のプログラムオフィスは、現在及び未決の支援の開示を要求しているが、開示に含まれなければならない情報の種類については、ばらつきがある。開示要件の標準化は、NSPM-33 実施ガイダンスの中心テーマであり、連邦研究機関は、助成支援申請書と説明書のモデル作成を任されている。これらの取組が進行中である一方、DOE は、すべての DOE 及び NNSA プログラムオフィスに、一貫した現在及び未決の支援開示要件を組み込むことを義務付け、現在及び未決の支援開示の一部として省に提出される要求情報の種類を調和させるために、モデル書式を設定している。モデル書式が利用可能になった後の第 2 段階では、DOE は、現在及び未決の支援開示要件を更新し、エネルギー省内全体でより一貫性を持たせ、モデル書式との整合性を高めるための追加措置を講じる予定である。DOE と NNSA のプログラムオフィスは、2023 年度に、現在及び未決の支援を含む情報開示に関する更新を予定している。
- 現時点では、グラントオフィサーは、申請者が申請書パッケージのどこに現在及び未決の支援の開示を含めるべきか、また助成支援契約書にどのように要件を組み込むべきかを判断する裁量を持ち続けている。DOE は、第 2 段階でこの方法を再検討する予定

[98] Department of Energy No. FAL 2022-04. Financial Assistance Regulations Date June 1, 2022. Financial Assistance Letter. Subject: Department of Energy Current and Pending Support Disclosure Requirements for Financial Assistance

である。なお、改訂版 FAL（Financial Assistance Letter）が発行される前に、現在及び未決の支援を開示するための省庁間共通フォーマット及び指示が公布された場合、補助金担当者には、省庁間共通フォーマット及び指示を使用する権限が特に与えられている。

- なお、「現在及び未決の支援」の定義は、(a) 個人の研究開発努力を支援するために、(i)（支援の）源が外国か国内か、(ii)（支援の）資源がそれを申請するエンティティを通じて利用可能か、又は直接個人に利用可能か、(iii)（支援の）資源が金銭的価値を有するかどうか、にかかわらず、個人に利用可能となった、又は利用可能と見込まれるすべての資源、(b) オフィス又は実験室、機器、供給品、職員・学生の提供など時間の約束を必要とし、研究開発の努力に直接貢献できる物品の提供も含める。この用語は、NSPM-33 の研究者に適用される「その他の支援」（Other Support）という用語と同じ意味である。
- 「現在及び未決の支援」は、重複、過剰な責務、潜在的な利益・責務相反、及び他のすべての支援源の可能性を特定できるようにすることを目的としている。申請書の一部として、PI、プライム申請者及び提案された補助金レベルの各シニア／キーパーソンは、すべてのスポンサー支援された活動、アワード（awards）、アポイントメントのリストを提出しなければならない。（以下のいずれも含む：1. 有給か無給か、2. 条件付き贈与か条件なし贈与か、3. 常勤か非常勤か任意か、4. 教員か客員か非常勤か名誉か、5. 現金か現物か、6. 外国か国内か、7. 政府か民間か、8. 個人の研究を直接支援するか、学生・研究スタッフ・スペース・設備・その他の研究費を支援することによって個人を間接的に支援するか）。「外国政府主催の人材採用プログラム」への関与はすべて、「現在及び未決の支援」に特定しなければならない。
- 活動ごとに、以下の項目を記載することとする。
  - 活動のスポンサー又は資金の提供者
  - アワードの番号又はその他の識別番号
  - アワードや活動のタイトル。アワードや活動のタイトルが説明的でない場合、提案された研究との重複や相乗効果を明らかにするために、実施されている研究の簡単な説明を追加する。
  - 直接費、間接費、コストシェアを含む、アワード又は活動の総コスト又は価値。応募中の提案については、要求した資金の総額を提示する。
  - アワード期間（開始日～終了日）。
  - そのアワード又は活動に費やされる 1 年あたりの作業人月。

(4) DARPA

国防省の研究・技術担当国防次官（Under Secretary of Defense for Research and Engineering: USD(R&E)）の要請により、外国の不当な影響を特定し緩和するために、DARPA は、外国の影響を受けた潜在的な利益相反又は責務相反を特定する方針とプロセスを導入してきた。DARPA のポリシーの重要な信条は透明性であり、プロセスを公表した後、DARPA は一連のフィードバック・セッションを開催し、ポリシーの更新に反映させた。[99]

「海外から影響対策プログラム」（CFIP）

DARPA の「海外からの影響対策プログラム」（Countering Foreign Influence Program: CFIP）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。[100]

研究・技術担当国防次官の要請により、不当な外国からの影響を特定し緩和するために、ミッションサービスオフィス／セキュリティ・インテリジェンス本部（Mission Services Office/Security and Intelligence Directorate (MSO/SID)　CFIP チームは、基礎研究助成金又は協力協定アワード（fundamental research grant or cooperative agreement award）の交渉のために選ばれたすべてのシニア／キーパーソン（Senior/Key Personnel）のリスク査定を実施する。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、行政命令、連邦政策、及び一般に公開されている不当な外国影響力のあるエンティティ・リストとともに適用される。

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された情報に注目し、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」までとなる。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。

1. 低リスク又は中リスクと評価された提案には、リスク軽減計画又は文書化されたリスク受容の判断は必要ない。
2. 高リスクと評価された提案は、リスク軽減計画を必要とする可能性があり、文書化されたリスク受容の決定が必要となる。

---

[99] DARPA website “Universities” <https://www.darpa.mil/work-with-us/for-universities>
[100] Memorandum for DARPA Staff and Contractors. September 17, 2021. SUBJECT: DARPA Countering Foreign Influence Program (CFIP)
<https://www.darpa.mil/attachments/091721DARPACFIPPolicySigned.pdf>

3. 非常に高いリスクと評価された提案は、リスク軽減計画及び文書化されたリスク受容の決定が必要となる。

高リスク又は非常に高いリスクと評価された提案については、契約担当者は、選定後の活動の一環として、プログラムマネージャー（PM）、科学審査官（Scientific Review Official: SRO）、オフィスディレクター（OD、※OD が SRO でない場合）と調整し、提案者が交渉中にリスクに対処する機会（例：リスク軽減計画、代替のシニア/キーパーソンなど）を与える。提案者がリスクを低又は中程度に軽減する意思がない、又は軽減できない場合、PM、SRO、OD がそれにもかかわらず助成を進めるつもりであれば、DARPA 副局長（DARPA Deputy Director）はリスクを受け入れて助成を進めることに同意する必要がある。

DARPA は 2021 年に CFIP を発表し、その後、2022 年 5 月に変更追加されているとのことである[101]。DARPA は表 2-33 のようなレーティングで研究提案書を提出した研究者のリスクを評価する[102]。

[101] Countering Foreign Influence Program (CFIP) Frequently Asked Questions (FAQ) Incorporating Change 1, May 12, 2022 (changes are in italicized text)
<https://www.darpa.mil/attachments/CFIPFAQ.pdf>

[102] Ropes & Gray. Implementation of "Countering Foreign Influence Program" for Scientific Research Funded by DARPA. March 18, 2022.
https://www.ropesgray.com/en/newsroom/alerts/2022/march/implementation-of-darpas-countering-foreign-influence-program-for-funded-research
David Schwartz. "DARPA reveals how it will implement the Countering Foreign Influence Program, foreshadowing approaches of other federal funding agencies" March 22nd, 2022.
<https://techtransfercentral.com/2022/03/22/darpa-reveals-how-it-will-implement-the-countering-foreign-influence-program-foreshadowing-approaches-of-other-federal-funding-agencies/>

表 2-33：海外からの不当な影響による利益相反や責務相反の可能性を評価するためのリスクに応じた対策：シニア／キーパーソンの情報開示の評価要素（2021 年 12 月）

要因 1：外国人人材採用プログラム

レーティング	内　容
非常に高い	戦略的競合相手や、米国の技術を不正移転の対象としてきた国（country with a history of targeting US technologies for unauthorized transfer: CWHTUST）の政府が運営する外国人人材育成プログラムに現在（継続的に）参加していることを示す。
高い	戦略的競合相手又は CWHTUST の政府が運営する外国人人材プログラムに過去に参加したことがあり、そのプログラムとの職業上の関連が継続していることを示す。
中程度	CWHTUST と技術共有契約を結んでいる米国の同盟国政府が運営する外国人材プログラムに現在（継続的に）参加していることを示す。
低い	外国人人材プログラムへの参加がない。

要因 2：拒否されたエンティティ・リスト

レーティング	内　容
非常に高い	米国政府が特定した拒否したエンティティや人物リスト、大統領令 13959 号（EO13959）[103]又はその後の類似の発行物に記載されているエンティティと現在（継続的に）提携（affiliation）の関係を示す。
高い	米国政府が特定し拒否したエンティティや人物リスト、EO13959、又はその後の類似の発行物に記載されているエンティティと過去に又は最近複数回（過去 4 年以内）の関係（association）があること示す。
中程度	米国政府が拒否した企業リストや EO13959、又はそれに続く類似の発行物で特定されたエンティティと過去に複数の関係があることを示す。
低い	米国政府が特定した拒否されたエンティティや人物リスト、EO13959 又はその後の類似の発行物に記載されている企業との過去又は現在の連携、関係を示す指標がない。

[103] 中国の軍事関連企業等への株式投資等を禁じる大統領令（2020 年 11 月 12 日）。

要因 3：資金調達先

レーティング	内　容
非常に高い	戦略的競合相手又は CWHTUST の外国政府又は外国政府関連エンティティから現在（継続的に）直接資金提供を受けていることを示す。
高い	外国政府、又は戦略的競合相手や CWHTUST の外国政府関連エンティティからの直接資金提供の履歴/パターンを示す。
中程度	戦略的競合相手や CWHTUST の外国政府又は外国政府関連エンティティから、過去に継続的でない散発的な資金提供を受けていることを示す。
低い	戦略的競合相手又は CWHTUST の外国政府又は外国政府関連エンティティから過去に資金提供を受けたことを示さない。

要因 4：外国の機関又はエンティティ

レーティング	内　容
非常に高い	高リスクの外国政府、又は外国政府関連の機関やエンティティと現在（継続的に）に提携（affiliation）していることを示す。
高い	高リスクの外国政府、又は外国政府関連の機関やエンティティと複数の現在（継続的な）直接的関係があることを示す。
中程度	高リスクの外国政府又は外国政府関連の機関又はエンティティと過去に複数の直接的な関係があることを示す。
低い	リスクの高い外国政府、又は外国政府関連の機関やエンティティとの関連や提携がない。

出典：DARPA. *Risk-Based Measures to Assess Potential Undue Foreign Influence Conflicts of Interest or Conflicts of Commitment*. Incorporating Change 1, December 1, 2021.

2.1.3 主要大学における取組

海外からの不当な影響に対して対応するために、大学・研究機関等が実施できるベストプラクティスとしては、前述のように以下の報告書「アメリカの科学技術研究事業のセキュリティとインテグリティを強化するために推奨される実践内容」が、米国科学技術会議（NSTC）の「研究環境に関する NSTC 合同委員会」（Joint Committee on the Research Environment）の「研究セキュリティ小委員会」（Subcommittee on Research Security）から公表されている（→18 頁）。

- Subcommittee on Research Security. Joint Committee on the Research Environment of the National Science & Technology Council. *Recommended Practices for Strengthening the Security and Integrity of America's Science and Technology Research Enterprise*. January 2021.

また、米国の大学の協会、学術団体やグループも、以下のようなガイダンスを発表している[104]。

- American Council on Education (ACE). *Memorandum to ACE member Presidents and Chancellors*, May 10, 2018.
- The Association of American Universities (AAU) and the Association of Public & Land Grant Universities (APLU). University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus. Updated May 2020.
- Council on Government Relations (COGR). *Framework For Review of Individual Global Engagements in Academic Research*. Version 1.0, January 14, 2020
- Council on Government Relations (COGR). *Federal Focus on Inappropriate Foreign Influence on Research: Practical Considerations in Developing an Institutional Response*. August 18, 2021

以下は、マサチューセッツ工科大学（MIT）、ハーバード大学、スタンフォード大学、カリフォルニア大学バークレー校において注目される取組や動き等をまとめた。

[104] DARPA. Countering Foreign Influence Program (CFIP) Frequently Asked Questions (FAQ) Incorporating Change 1, May 12, 2022. <https://www.darpa.mil/attachments/CFIPFAQ.pdf>

(1) マサチューセッツ工科大学（MIT）

MIT China Strategy Group は、MIT の Richard Lester 教授（Associate Provost for International Activities; Japan Steel Industry Professor of Nuclear Science and Engineering）と Lily Tsai 教授（Chair of the Faculty; Ford Professor of Political Science; Director, MIT Gov/Lab）を共同議長とし、他に 5 人の教授、2 人の職員をメンバーとする。グループでは、政治指導者が基本的人権や価値観と相容れない政策を追求し、米国に安全保障上のリスクをもたらす国々の組織や個人と、MIT や他の米国の研究大学がどのように関わるべきか、について幅広い視点から検討し、2022 年 11 月に約 40 頁の報告書を公表した。以下はその骨子である。[105]

- アメリカの大学の自治とその教員の知的自治（intellectual autonomy）は、我々の教育システムにおける基本原則である。MIT や他の大学は、教育や研究の実践と原則について、より直接的で詳細な知識を活用し、独自のアプローチを開発する必要がある。中国との関わりにおいて独自の規制の枠組み、優先順位、目標を採用することで、大学は米国の教育、研究、イノベーションに害を及ぼすような外部からの規制を回避することもできる。
- 中国に関しては、これらの組織目標のうち最も重要なものは以下のとおりである。
  - ✓ MIT が研究、教育、イノベーションの分野で世界の最前線に立ち続けるために、最も才能のある中国人学生や学者を私たちのキャンパスに惹きつけることを継続する。
  - ✓ 中国系を含む MIT コミュニティのすべてのメンバーが、外部からの干渉、偏見、差別を恐れることなく、繁栄し、最高の仕事ができるようにする。
  - ✓ 私たちの教職員や学生が、中国の一流の研究者や機関と、両国にとって、また世界にとって重要な問題に取り組むことができるようにする。
  - ✓ 中国の科学、技術、イノベーション、ビジネス、歴史、文化、政治、経済について、学生を教育する。
  - ✓ 中国の科学者を含む MIT の中国人卒業生とのネットワークやコミュニケーションラインを維持・強化する。
- 同時に、教授陣と管理職によるこれらの目標の追求は、MIT コミュニティを結びつけ、国内外を問わず、MIT のすべての活動に適用される価値観に基づくものである。その価値とは、知的卓越性、開放性、発見と創造的な問題解決の奨励、独立性、すべての個人と集団に対する公平な扱い、表現、コミュニケーション、出版の自由などである。
- MIT のもう一つの重要な価値は、知的リスクに関するものである。新しい知識の追求に対するリスク回避的なアプローチは、MIT のような機関とは相容れないものであり、

[105] MIT China Strategy Group (Richard Lester and Lily Tsai (co-chairs), Suzanne Berger, Peter Fisher, M. Taylor Fravel, David Goldston, Yasheng Huang, Daniela Rus). *University Engagement with China: An MIT Approach Final Report*. November 2022. <https://global.mit.edu/about/report>

また、そうありたいと考えている。過度な、あるいは過剰な警戒心は、新しいアイデアの開発を阻害する。リスクは最小限に抑えるべきであるが、MIT はリスクを完全に排除することを求めも期待もしない。[106]

- 「越えてはいけないライン」として、以下を上げている。
  - ✓ MIT は、学術研究のインテグリティや客観性を損なう可能性のある共同活動を行うべきではない。例えば、研究者の知的独立に対する圧力や、研究結果のオープンな公表を制限しようとする試みなどが挙げられる。
  - ✓ MIT は、国内外を問わず、国籍、民族、人種、性別、その他の個人的特徴に基づき、特定の MIT 個人を共同研究への参加から排除しようとする共同研究先、スポンサー、寄付者の試みを受け入れてはならない。
  - ✓ MIT は、中国政府又は他の政府が米国の利益に反して先端技術を使用するのを助ける可能性のある研究協力に、公的又は民間のパートナーとの関係なく関与してはならない。
  - ✓ MIT は、中国政府（又は他の政府）による自国民に対する人権侵害やその他の行為に貢献する可能性のある研究協力に関与すべきではない。これには、出所や潜在的な用途が MIT の倫理基準やインフォームド・コンセント基準と矛盾するバイオメトリクス、遺伝子、その他のデータセットとの共同研究が含まれる可能性がある。
  - ✓ MIT は、中国（及びその他の国）での活動に関連するすべての連邦及び州の法律と規制を遵守しなければならず、MIT コミュニティのメンバーが MIT の従業員として仕事に従事する際には、その遵守の努力を支援する必要がある。また、MIT は、政府の規則や規制を遵守するための負担が、中国系（又はその他の民族や国籍）のコミュニティのメンバーに不釣り合いにならないように努めるべきである。
  - ✓ MIT は、MIT コミュニティの中核的価値観と相反する中国政府（又は他の政府）の行動を正当化したり、間接的に促進したりする可能性のある共同研究への関与に慎重であるべきである。そのような共同研究に関与するかどうかの最終決定は、そのリスクと期待される利益のバランスに依存し、PI と協議して行われるべきである。[107]

次表は報告書の提言内容をまとめたものである。

[106] 同上. p.17.
[107] 同上. p.17-18.

表 2-34：MIT 報告書（2022 年）の提言内容

MIT のリスク管理能力を強化する。 ・ PI が、中国の組織や個人が中国政府や中国共産党とどのような関係にあり、どのような義務を負っているのかを含め、中国における研究協力者の活動状況をより理解できるような情報リソースを開発する。 ・ PI が研究グループのメンバーに対して、情報、サンプル、機器をグループ外で共有する際の規範と期待について教育するのを助けるために、個々の研究科レベルで研修やその他のガイダンスを提供する。 ・ 利益相反、責務相反、現在及び未決の支援の開示のための内部報告システムの強化及び体系化、また重大なセキュリティリスクをもたらす中国やその他の国の同僚との非公式な協力関係を見直す。
MIT が企業と関係を持つことを不適格とすべき状況には、以下のようなものがある。 ・ 政府の諜報活動への直接的な関与、又は軍事用途のシステム、製品、サービスのプロバイダーとして中国軍との直接的な関係。 ・ 企業の活動が新疆ウイグル自治区又は中国の他の地域における人権の抑圧に寄与しているという信頼できる証拠。
MIT は、中国の国防大学、軍事研究機関、民間大学の国防重要研究所との研究協力に関与してはならない。
MIT のエグゼクティブ・専門家教育プログラムは、人権の抑圧に貢献している組織や、中国の軍事活動や諜報活動と直接関係のある組織を支援したり、力を与えたりしてはならない。
MIT の研究は PI が主導しており、リスク評価と管理における PI の役割は中心的なものである。MIT の PI への提言は以下のとおり。 ・ 中国との共同研究に着手する前に、PI は、MIT、研究コミュニティ、国に対するより広範な利益を含め、特に中国企業との共同研究から期待される利益について評価を行うべきである。独自の利益の期待は、共同研究が行われるための必要条件ではないが、リスクと利益の全体的な評価にとって重要である。 ・ PI は、研究グループの全メンバーが、グループ外との情報共有に関する規範と期待事項を理解し、これらの規範を継続的に強化する責任がある。 ・ 学生が研究グループや研究室のメンバーではない、あるいは大学院生が指導教官から独立して研究や学問を行うことが一般的な学科や分野では、指導教官は、国際共同研究及びその共同研究の内容を学科に報告する学生の責任について大学院生に指導を行うべきである。 ・ 教員は、外部活動に対していかなるレベルの報酬も受け取ることができるが、外国企業とのコンサルティングに対する高額な報酬は、教員が提供する特定のサービスをはるかに超えて、その企業の活動を承認しているとより広い社会からみなされる可能性があることを考慮する必要がある。教員は、中国政府や政府出資のプログラムから外部活動の

ための報酬を受け取る前に、細心の注意を払い、必要とされる利益相反や責務相反を含めて、現在及び未決の支援に関する開示において、そのような活動を完全に開示するよう助言される。教員が外部活動の一環として中国の団体と契約関係を結ぶことを検討する場合、その前に MIT の法律顧問室（Office of General Council）に助言を求めることが推奨される。 ・ 教員は、中国への技術移転を目的とした外国人人材採用プログラムに参加すべきではない。 ・ 教員は、MIT の学生やポスドク、あるいは知り合いの学生を中国での職に推薦することを躊躇すべきではない。しかし、推薦状を書くという見返りを得て教えることになったプログラムで、MIT 以外の学生の推薦状を書くことは避けなければならない。また、卒業生を中国での就職に導くことを目的としたプログラムにおいて、報酬の有無にかかわらず、組織的又は管理的な役割を果たすことも避けるべきである。
MIT は、中国の軍事・安全保障機関に現在雇用されていることが MIT によって知られている人物を、ポスドクや客員研究員に任命すべきではない。 ・ 米国の大学が海外からの学生を受け入れるかどうかを決定する責任は、連邦政府のビザ発給権限の行使を通じ、連邦政府と共有されている。中国からの留学生の受入れに関する連邦政府のビザ及び移民政策のさらなる明確化と安定化が緊急に必要である。我々は、学生ビザの資格を制限するような連邦政府の政策については、それが明確に規定され、制限の範囲が限定されることを強く求める。今日、私たちが最も懸念しているのは、連邦政府のビザ及び移民政策が不透明なままであるため、優秀な中国人学生や学者が MIT やその他の大学に出願したり、米国に滞在することを躊躇していることである。このような状況は、MIT だけでなく、より広く米国の科学、技術、イノベーション事業の強化にマイナスの影響を与える。
MIT は、学生が中国の歴史、社会、文化、言語、政治について知識を得る機会を拡大すべきである。経済発展、科学、そして中国のビジネス慣行とイノベーション能力に関する実践的で実践的な知識を身につけられるような、また、MIT の教員専門家とその学生が中国の科学技術能力と進歩についてより深く理解できるようなリソースも開発されるべきである。
MIT の教職員からなる委員会が、これらの提言の実施計画を立てること。

出典：MIT China Strategy Group (Richard Lester and Lily Tsai (co-chairs), Suzanne Berger, Peter Fisher, M. Taylor Fravel, David Goldston, Yasheng Huang, Daniela Rus). *University Engagement with China: An MIT Approach Final Report*. November 2022. <https://global.mit.edu/about/report>の executive summary の recommendations に基づき作成。

なお、報告書の記述によれば、2019 年より MIT は格上げされたリスクマネジメントプロセスを導入している。すなわち、2019 年、MIT は、国家安全保障、経済安全保障、市民・人権に関連する高度のリスクをもたらす可能性のある国際的な関与の提案を積極的に審査

する新しいプロセスを導入した。現在、この高リスク審査プロセス（elevated risk review process）では、中国、ロシア、サウジアラビアに関わるすべての関与案と、特別なリスクをもたらす可能性のあるその他の特定のプロジェクトが検討対象となっている。

高リスク審査プロセスでは、米国政府の政策と国益、さらにMITコミュニティ、コアバリュー、学術的使命への潜在的影響を考慮する。これらの審査は、MITのスポンサープログラム担当者が担当する、すべてのスポンサー活動の開発及び管理という通常の業務を補強するものである。リスクの高いレビューには、教員委員会と職員委員会の両方が関与し、それぞれがPIと協力する。これらの審査には、MITのワシントン事務所、MITやその他の国・地域の専門家、時には難しい問題の場合に教員委員会からも意見を求める。連邦法及び規制の遵守は、このような業務を進めるための必要条件であるが、進めるか否かを決定するための十分な根拠とはならないことが多々ある。さらに、通常、進めるかどうかの判断は、不完全又は部分的な情報に基づいて行わなければならない。複雑なトレードオフの関係にあるプロジェクトや、困難な政策課題を提起するプロジェクトは、3人の上級管理職からなる委員会であるシニアリスクグループ（Senior Risk Group）によって取り扱われる。

高リスク審査プロセスの重要な側面は、PIのリスクに対する認識を高め、PIと協力して、リスク管理に役立つ情報とアプローチを開発することである。これには、国家に対するリスク、MITに対するリスク、研究者個人に対するリスク、より大きな学術コミュニティに対するリスクなどが含まれる。常に問われるのは、「この共同研究を実施しない場合のリスクは何か」ということである。

このプロセスの結果、提案された共同研究のいくつかは却下され、多くは承認されたが、その他のものについては特定の条件が適用され、修正が求められている。[108]

[108] 同上. p.19.

(2) ハーバード大学

ハーバード大学では、研究インテグリティと研究セキュリティに関する方針の一環として、外国との関係や活動、資源を開示する方法についての情報やガイダンスをウェブサイトで提供している[109]。ハーバード大学の OVPR（Office of Vice Provost for Research）は、学内の 3 つのオフィス（OSP : Office for Sponsored Programs、ORA: Office of Research Administration、SPA: Sponsored Programs Administration）及び大学のその他教職員で協力し、開示要件の変更に対応した研究者や事務職員向けの内部ガイダンスやテンプレートを提供している。

「研究者のための教員情報公開・知的財産保護ガイダンス」（Faculty Disclosure & Intellectual Property Protection Guidance for Researchers）では、以下のトピックを扱っている：1. 基本原則、2. ピアレビュープロセスのインテグリティ、3. 資金援助、外部活動などに関する情報の透明性・公開性、4. 法規制の遵守、5. 知的財産（IP）の保護、6. 定義、7. よくあるご質問。また、研究者のためのポリシー、規則、ガイダンスは、「Research Policies & Compliance: Policies, rules and guidance for researchers and their projects」のウェブサイトにまとめられている。[110]

最近の動きとしては、「近年、研究コンプライアンス環境はかつてないペースで変化し、研究事業、その構造、及び新しい要件や規制に適応する能力が問われている。このため、ハーバード大学の文理学部（Faculty of Arts and Sciences: FAS）、工学・応用科学学部（School of Engineering and Applied Sciences: SEAS）と研究担当副学長室（Office of the Vice Provost for Research: OVPR）は、共有の「研究コンプライアンスプログラム」（Research Compliance Program: RCP）を設立した」とのことである。このプログラムでは、OVPR のスタッフが 2023 年 2 月 15 日より、特定の研究コンプライアンス機能における運用的・管理的責任を担当する。移管される研究コンプライアンス機能は、教員・研究者の外部活動及び利益相反、輸出規制、国際的な共同研究及び活動の 3 つであるとのことである。

[109] Harvard University website. “Faculty Disclosure: Policies, rules and guidance for researchers and their projects” <https://research.harvard.edu/faculty-disclosure-guidance/>
[110] Research Policies & Compliance: Policies, rules and guidance for researchers and their projects. <https://research.harvard.edu/research-policies-compliance/>

出典：Harvard University website. Research Policies & Compliance: Policies, rules and guidance for researchers and their projects
<https://research.harvard.edu/research-policies-compliance/#rcp>

図 2-4：ハーバード大学の研究コンプライアンス関係のポータルサイト

(3) スタンフォード大学

スタンフォード大学の学長とプロボストが 2023 年 2 月に公表した声明（「海外への関与と大学研究者への支援についての声明」）では、以下の内容について述べている。[111]

- 外国政府が米国の国家安全保障や研究環境のセキュリティとインテグリティを損なおうとする脅威をスタンフォード大学は真剣に受け止めている。研究大学にとって重要

[111] Marc Tessier-Lavigne, President and Persis Drell, Provost. Statement on Foreign Engagement and Support for University Researchers. February 8, 2023
<https://doresearch.stanford.edu/statement-foreign-engagement-and-support-university-researchers-0>

な問題を明らかにした報告書（MIT の 2022 年の報告書や米国科学技術アカデミーの 2022 年の報告書など）を参考にしている。

- すべての留学生、教員、スタッフ、ポスドク、卒業生は、スタンフォード・コミュニティの大切なメンバーであり、常に歓迎され、安全で、尊重され、大切にされていると感じるべきである。誰一人として、国籍や遺産に基づいて容疑者とみなされることがあってはならない。
- スタンフォード大学は、研究者に対してガイダンスと支援を提供することに取り組んでおり、政府の情報開示や報告の要件に従うことができるように資料や支援を用意している。適切な開示は、研究セキュリティと研究インテグリティを確保し、不適切な行為の疑いから自分自身を守るための最も重要なステップである。
- スタンフォード大学は、研究コミュニティに情報を共有することに取り組んでいる。連邦政府や他の信頼できる情報源から国家安全保障や人権問題に関する情報が提供されている。大学はこれらの情報をモニターし、関連する情報を伝えたり、研究活動に関連するリスクを特定したり軽減したりするための資料を作成したりしている。
- スタンフォード大学は、研究者の権利を保護し、正当な手続きを確保することに取り組んでいる。大学は、クロスボーダー活動に関連する場合、一部の研究者が政府機関の調査又は連邦法執行機関の対象になる可能性があることを理解している。大学の科学者に関する調査は、これらの調査の複雑さや機密性の必要性によって悪化し、研究コミュニティで恐怖と不確実性を引き起こしている。法執行機関から連絡を受けた学生や教員のためのガイダンスをウェブサイトに掲載している[112]。スタンフォード大学は、教員やスタッフがスタンフォードの職務の適法な遂行に起因して調査やその他の法的措置の対象となった場合、彼らを弁護し、補償する。

スタンフォード大学の「グローバル関与レビュープログラム」（Global Engagement Review Program: GERP）は、オープンかつウェルカムなコミュニティを維持するために、潜在的な不当な海外影響力のリスクを評価するために作られた集中的な助言プロセスである。このプログラムは、不当な外国からの影響力、研究セキュリティ・研究インテグリティへのリスクを評価するために、外国への関与のさまざまな側面について助言する複数のオフィスからの情報を調整する。教員や管理者は、GERP ディレクターに連絡することで、GERP のレビューを推奨又は要求することができる。関与が高いリスクを示す場合、ディレクターは、専門家からなる GERP スタッフ委員会（GERP Staff Committee）と協力して、リスクを評価し、学術及び研究目標達成を支援する勧告を作成する。GERP スタッフ委員会が、ある契約に関連するリスクが特別に高いと判断する場合には、GERP スタッフ委員会は GERP 教員委員会（GERP Faculty Committee）にその問題を付託し、教授委員会

[112] General Guidance: Contacts with Law Enforcement <https://doresearch.stanford.edu/sites/default/files/2023-02/Stanford%20General%20Guidance%20Contact%20with%20Law%20Enforcement_0.pdf>

は検討し、大学の指導者に助言と勧告を提供する。[113]

また、米国政府は、中国、ロシア、イラン、北朝鮮の政府がスポンサーとなっている「海外政府人材採用プログラム」（Foreign Government Talent Recruitment Programs: FGTRPs）について深刻な懸念を表明しており、中国、ロシア、イラン、及び北朝鮮が後援する FGTRP に参加すると、個人が特定の種類の連邦資金を受け取ることができなくなる場合がある。このため、スタンフォード大学では、これらのプログラムに参加するためには、必ず学部長の承認を得て、スタンフォード大学及び連邦資金提供機関に開示する必要があるとウェブサイトでは説明している。[114]

(4) カリフォルニア大学バークレー校

カリフォルニア大学バークレー校（UC バークレー）では、ウェブサイトで、国際的な共同研究に取り組む UC バークレーの研究者に情報やガイダンスを提供している。米国の高等教育における外国からの影響に対する連邦政府の懸念と、UC バークレーが研究のインテグリティ、輸出管理、開示要件、利益相反などの規制や方針に従ってそれらに対処している方法を説明している。また、研究者が自分たちのデータ、知的財産、学問の自由を保護するためのリソースやベストプラクティスも提供している。UC バークレーの長い伝統である強力な国際的な関与と教育・研究の卓越性を支援するとのことである。[115]

また、ウェブサイトは、UC バークレーの「国際的な関与の原則」（Principles of International Engagement）について説明している。この声明は、2019 年に「国際的な関与の方針タスクフォース」（International Engagement Policy Task Force）によって作成され、2020 年に学長によって発表された。目的は、国際的な関与が UC バークレーの学術的な使命と地位にとって重要であることを伝えるとともに、国際的な関与を妨げる行為を非難することである。声明では、以下の 5 つの原則を掲げている。[116]

---

[113] Stanford University website. “Academic Integrity and Undue Foreign Interference” <https://doresearch.stanford.edu/topics/academic-integrity-and-undue-foreign-interference#Policies_&_Resources>
Statement from President Marc Tessier-Lavigne and Provost Persis Drell on Foreign Engagement and Support for University Researchers. February 8, 2023 <https://doresearch.stanford.edu/topics/academic-integrity-and-undue-foreign-interference>

[114] Stanford University website. “Academic Integrity and Undue Foreign Interference” <https://doresearch.stanford.edu/topics/academic-integrity-and-undue-foreign-interference>
“While not prohibited if the participant complies with all applicable regulations, requirements and policies, participating in a FGTRP sponsored by China, Russia, Iran and North Korea can preclude an individual from receiving certain types of federal funding. Participation in these programs should always be approved by your School Dean, disclosed to Stanford and federal funding agencies.”

[115] University of California, Berkeley website. “International Collaboration, Research Integrity, & Foreign Influence” <https://globalengagement.berkeley.edu/research/international-collaboration-research-integrity-foreign-influence>

[116] University of California, Berkeley website. “UC Berkeley's Principles of International Engagement” <https://globalengagement.berkeley.edu/about/uc-berkeleys-principles-international-engagement>

- 国際的な関与はUCバークレーの教育・研究・公共奉仕の目標を達成するために不可欠である。
- 国際的な関与は多様性・包摂性・平等・正義を促進するために必要である。
- 国際的な関与は学問の自由・開放性・透明性・倫理性を尊重し保護するべきである。
- 国際的な関与は相互利益・相互尊重・相互責任を基礎として築かれるべきである。
- 国際的な関与は地域社会や世界社会に対する貢献や影響を考慮し評価されるべきである。

声明は、UCバークレーが国内外のパートナーやステークホルダーと協力して、グローバルな課題や機会に対応するための指針として機能する。

この「国際的な関与の方針タスクフォース」は、2019年にUCバークレーの学長によって設置されたもので、キャンパス内外の国際的な関与に関する方針やガイダンスを策定することを目的とした。このタスクフォースは、学術計画担当副学長（Vice Provost for Academic Planning）と研究担当副学長（Vice Chancellor for Research）が担当し、学内の関係部署のメンバーが参加し、以下の3つのサブチームで作業を行った。[117]

・国際協定・研究資金
・国際学生・訪問者・旅行者
・コミュニケーション

「国際的な関与の方針タスクフォース」は2020年6月に検討結果の報告書を発表した。報告書では、UCバークレーの国際的な関与に関する現状分析と提言をまとめた。以下の幅広い項目についての提言を含んでいる：国際的なパートナーシップの吟味、国際協定、国際的な贈答品、研究資金と情報開示、報告及びエスカレーションプロトコル、外国人留学生、客員研究員・ポスドク、非公式のビジター、アウトバウンド旅行者、輸出管理、インバウンド旅行者のためのサイバーセキュリティ・機密データ・知的財産の保護、コミュニケーションとバリュー、学問の自由の重視、教育する私たちのコミュニティ、コミュニケーションとトレーニングの展開とツール、今後の課題（プログラム開発と国際プログラムの一元的な支援）。[118]

[117] University of California, Berkeley website. “International Engagement Policy Task Force (IEPTF)” <https://globalengagement.berkeley.edu/initiatives/international-engagement-policy-task-force-ieptf>
[118] University of California, Berkeley. International Engagement Policy Task Force (IEPTF) report. June 6, 2020.
<https://globalengagement.berkeley.edu/sites/default/files/ieptf_executive_summary_public.pdf>

2.2 英国

2.2.1 研究インテグリティの確保に関する要求と支援

(1) 研究インテグリティについて英国政府が動き出した背景

英国は、国際協力による科学論文の発表数が世界で第 5 位であり[119]、このような海外との共同研究が英国の科学的発展に対して重要な役割を果たしている。英国政府のウェブサイトの一つによれば、英国は規則体系を守る国であり、これは外向きの国家として英国の利益に役立っており、非常に重要であり続けると考えられている。英国政府は、この規則体系により、人間の尊厳、人間の権利、自由、民主主義及び平等の尊重という共通の根源的な価値を防護するための国際的な協力関係を実現したとしている。[120]

英国の大学は世界中のパートナーと密接に連携している。英国の研究の半分以上は国際連携によるものである。例えば、2017 - 2018 年に英国の大学が得た研究による歳入額は 82 億ポンド（約 1.2 兆円）であったが、そのうち 13.9 億ポンド（約 2,100 億円）は海外からであった。このような国際連携は、研究へのファンディングや協力の枠を超えている。ポスドクの 42%、大学の職員の 31%が英国外の出身である。このような国際連携を発展・維持していくことは、英国の研究・イノベーションの成功の鍵を握っている[121]。

ビジネス・エネルギー・産業戦略省（Department for Business, Energy & Industrial Strategy: BEIS）[122]は、英国が長期的な国際研究・イノンベーションのパートナーとして選ばれるための目標を掲げた、「UK International Research and Innovation Strategy」[123]を 2019 年に発表した。近年、国際的な研究協力が盛んに展開する一方、アカデミアや産業界が行う研究活動を通じた技術流出により、国家安全保障に重大なリスクを与えることが英国政府の安全保障部門に認識されてきた。

こういった状況を踏まえて、2019 年 9 月に、英国政府の国家安全保障機関である国家インフラ保護センター（Centre for the Protection of National Infrastructure: CPNI）[124]と国家サイバーセキュリティセンター(National Cyber Security Centre: NCSC)が、「Trusted

---

[119] National Protective Security Authority (NPSA)ウェブサイト “Trusted Research” <https://www.npsa.gov.uk/trusted-research>

[120] 同上

[121] 同上

[122] 2023 年 2 月、スナク政権の下に、ビジネス・エネルギー・産業戦略省（Department for Business, Energy & Industrial Strategy（BEIS））は、Department for Energy Security and Net Zero（DESNZ）、Department for Science, Innovation and Technology（DSIT）及び Department for Business and Trade (DBT)の 3 つの省に分割された。

[123] GOV.UK ウェブサイト “Policy paper International Research and Innovation Strategy” <https://www.gov.uk/government/publications/uk-international-research-and-innovation-strategy/international-research-and-innovation-strategy-webpage>

[124] CPNI は 2023 年 3 月に、「国家保護安全保障局」（National Protective Security Authority: NPSA）に名称変更するとともに、任務が拡大している。(”About NPSA” <https://www.npsa.gov.uk/about-npsa>)

Research」というキャンペーンを全国展開し、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[125]を公表した。

(2) Trusted Research の目的と要求事項

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及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。

Trusted Research は、特に、STEM 科目、デュアルユース技術、新興技術、商業的に機密性のある研究分野等の研究者をターゲットとしており、英国の研究インテグリティを確保していくうえで、セキュリティの観点から、研究者が注意すべき事項や取るべき対策についてポイントを示している。

Trusted Research に関する助言は、研究・大学コミュニティとの協議により作成され、世界をリードする英国の研究・イノベーションセクターが、知的財産、機密性の高い研究及び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ように設計されている。

Trusted Research Guidance for Academia は、研究者に対して、セキュリティの観点から研究に係るリスクについて概説し、研究者として注意すべき事項について説明している。

- なぜあなたの研究を守ることが必要なのか？
- あなたは誰からのリスクを負っているのか？
- あなたの研究に対するリスクは何か？
- あなたはどの程度狙われているのか？
- あなたの研究を守る方法
  - ➢ 研究パートナーとのコラボレーションで注意すべきこと
    - ✧ デューディリジェンス
      - ● 新たな研究協力や研究助成を検討する際には、デューディリジェンス（適正評価）を行う。これには金銭面だけでなく、倫理的、法的及び国家安全保障的な考慮も必要である。そうすることで、その相手と共同研究を行うべきか否かについて、情報に基づくバランスの取れた決断を下すために必要なすべての情報を手に入れることができる。
    - ✧ 利益相反
      - ● 研究パートナーや研究資金提供者との間に潜在的な利害の対立があるこ

[125] CPNI Trusted Research ウェブサイト“Trusted Research Guidance for Academia”
< https://www.npsa.gov.uk/trusted-research-academia>

とを認識する。パートナーとはオープンに、あなたのセキュリティ対策とパートナーのセキュリティニーズについて定期的に話し合う。

- ✧ 隔離
  - 知的財産、研究及び個人情報の保護が必要な場合は、物理的にもオンライン上でも研究プログラム間で適切な隔離を行うようにする。研究へのアクセスは、正当な要件を満たす者にのみ許可する。

➢ 法的枠組みの活用

- ✧ 輸出管理
  - 自分の研究が輸出規制の対象かどうかを確実に把握する。研究活動は輸出管理法の対象であり、研究活動に輸出管理ライセンスが必要かどうかを確認するためのツールもある。
- ✧ 法律
  - 法制度
    - ➢ 海外の研究パートナーや資金提供者と共同研究を行う場合、その下で運営されるさまざまな法的枠組みを認識し、それが契約やパートナーシップにどのような影響を与える可能性があるかを確認しておく必要がある。
- ✧ GDPR（General Data Protection Regulation）
  - GDPR 法に基づいて取り扱うデータ及び情報を保護する責任を自覚する。
- ✧ National Security and Investment Act（NSI 法）
  - 英国政府は、企業や投資家を含む誰であれ、英国の国家安全保障に害を及ぼす可能性のある特定の買収を精査し、介入することができる。政府は買収に一定の条件を付けたり、必要であれば買収を取り消したり、阻止したりすることができるようになる。政府は、企業や投資家を含む誰であれ、英国の国家安全保障に害を及ぼす可能性のある特定の買収を精査し、介入することができるようになる。高等教育機関やその他の研究機関は、他の当事者と協力して適正企業や資産を取得・売却・開発する場合、NSI 法に留意する必要がある。

➢ 研究者の安全確保

- ✧ 注意喚起
  - 自身や同僚が、あなたとあなたの研究をオンラインで保護するために取ることができる対策を認識していることを確認する。良いサイバーセキュリティ対策を行うことにより、研究データの損失や侵害の可能性が低くなる。
- ✧ ビザ
  - 施設や IT ネットワークにアクセスする訪問研究者は、スタッフとして一

元管理され、適切なビザを取得していることを確認する。

✧ 出張時のアドバイス

- 会議や長期出張の際には、現地の法律や習慣、知的財産や機密データの保護について考慮する。IT に依存している場合は、それが海外で使用・アクセスできることを確認する。

Trusted Research では、大学・教育機関用として、「Trusted Research Guidance for Academia」の他、国際共同研究提案の際のチェックリスト「Trusted Research Checklist for Academia」[126]、海外で行う研究活動の注意事項「Countries and Conferences Guide」[127]、大学・研究機関の研究及び職員のセキュリティ担当者向けの実践的ガイダンス「Trusted Research Implementation Guide」[128]及び大学・研究機関の上級管理者向けのガイダンス「Trusted Research Guidance for Senior Leaders」[129]等の文書を発行している。

以下、Trusted Research の本質を理解するうえで極めて重要と考えられる、Trusted Research Checklist for Academia、Trusted Research Guidance for Senior Leaders 及び Trusted Research Implementation Guide の 3 文書の概要を示す。

表 2-35：Trusted Research Checklist for Academia、Trusted Research Guidance for Senior Leaders 及び Trusted Research Implementation Guide の 3 文書の概要
（未来工学研究所が 3 文書より一部和訳・編集）

文書名	概要
Trusted Research Checklist for Academia	研究インテグリティの観点から、研究者自身の国際共同研究提案に関する評価を支援するための質問事項として、以下を挙げている。 【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？ ・ 資金援助や関与の見返りに何を期待しているのか？ ・ その組織は、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

126 Trusted Research Checklist for Academia
<https://www.npsa.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academia.pdf>
127 TRUSTED RESEARCH Countries and Conferences
<https://www.npsa.gov.uk/system/files/Countries%20and%20Conferences%20Guide.pdf>
128 Trusted Research Implementation Guide
<https://www.npsa.gov.uk/system/files/Trusted%20Research%20Implementation%20Guide.pdf>
129 Trusted Research Guidance for Senior Leaders
<https://www.npsa.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Senior%20Leaders.pdf >

文書名	概要
	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、又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？ ・ この研究についての決定を、あなたの部署内でエスカレーションさせる（上位レベルでの処理事項とする？）必要性があるか？ 【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（IP）、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？

文書名	概要
	・ 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？
Trusted Research Guidance for Senior Leaders	研究インテグリティに関する大学の上級管理者向けのガイダンス。大学の上級管理者に対して、以下のような項目に関する確認を求めている。 ・ グッドガバナンス（研究協力の防護に責任を持つシニアリーダーシップレベルのリーダーを特定する等） ・ 最も機密性の高い研究の特定 ・ 脅威の特定 ・ デューディリジェンス（デューディリジェンスの過程で、風評被害、倫理的リスク、国家安全保障上のリスクなどを考慮するようにするなど） ・ リスクマネジメントアプローチの採用 ・ リスクの考慮（研究協力に伴うリスクを特定するための方針とプロセスが存在し、それらが周知されていることを確認するなど） ・ リスクの軽減 ・ 財務リスク ・ 適法性（国際協力の法的枠組みを明確に理解するなど） ・ 国際的な法的枠組み（国際的な研究協力者が活動する国の法的枠組みを考慮したプロセスと監視を行うようにするなど） ・ 職員の保護（外国人職員、客員研究員及び学生の採用と維持を支援するための適切なシステムがあることを確認するなど） ・ アクセス管理（職員、研究者、客員研究員及び産業界のパートナーが、研究に必要な建物、情報、ネットワークにのみアクセスできるようにし、研究上の機密事項についてはさらに保護するための適切な措置を検討するなど） ・ 研究と情報の保護（情報及びサイバーセキュリティポリシーが Trusted Research のアプローチをどのように支援しているかを理解するなど） ・ 信頼される研究文化の創造（模範を示して導くなど） ・ 信頼される関係の構築 上級管理者に対して、以下のような重要な問いかけをしている。 ・ 上級管理者レベルで、研究活動の確保に責任を持つのは誰か？

文書名	概要
	・ 自身の研究機関が財政的・評判的に依存しているパートナーや資金提供者を含め、自身の研究機関の最も重要なパートナーや資金提供者を把握しているか？ ・ リスクの高い共同研究を特定し、管理するためのプロセスを備えているか？ ・ 職員は、高リスクの共同研究について、いつ、誰に、対応すべき事項として上奏すべきか明確になっているか？ ・ 自身の研究機関が輸出管理、GDPR、その他の法的要件に準拠しているかということについて確信を持っているか？ ・ Trusted Research キャンペーンを組織内で推進する人物がいるか？
Trusted Research Implementation Guide	本ガイダンスは、大学・研究機関が、「Trusted Research Guidance for Academics」及び「Trusted Research Guidance for Senior Leaders」に概説されているアドバイスやガイダンスを実施することを支援するために作成されたものである。このガイダンスは、大学における研究及び職員のセキュリティを担当する者（又はチーム）を対象として、大学内でセキュリティに関する行動を定着させ、その行動を維持する環境を支援するための実践的な枠組みを提供する。 本ガイダンスでは、Trusted Research は、「セキュリティ行動の定着：5Es の活用（Embedding Security Behaviours: using the 5Es）」と呼ばれる枠組みに基づいて実施されるとしている。5Es は以下を意味する。 ・ Educate ➢ 職員に、自分、自分の研究及び機関に対するセキュリティ上の脅威について教育する。 ➢ セキュリティ上の行動を採用することによる利点及び採用しなかった場合の結果について教育する。 ➢ なぜその脅威がその機関にとって重要であるかについて、職員を教育する。 ・ Enable ➢ 簡単にアクセスできる研修や参考資料を提供することで、職員が自分自身とその機関にとって適切かつ妥当なセキュリティ対策を採用できるようにする。 ・ Environment ➢ 職員がセキュリティプロセスに従うことが容易な環境を作

文書名	概要
	り、これが日常的な業務慣行の一部として受け入れられることを目指す。 ・ Encourage ➢ フィードバックや、ソフト・ハード両面からのインセンティブを提供することで、優れたセキュリティ行動を奨励し、維持する。 ・ Evaluate ➢ 研究機関がセキュリティ向上の進捗状況を評価するための、成功の尺度となる重要業績評価指標を特定する。 本ガイダンスは、5Es の枠組みに基づいて Trusted Research を実施するためには、自身の研究機関が職員に求めるセキュリティ行動を理解することが極めて重要であるとし、機関及び職員（学術系及び非学術系）に適したプロセスを開発し、既存のセキュリティ体制を補完する必要があるとしている。また、研究機関の研究、職員及び評判を守るために大学が職員に求める役割と行動を決定すれば、5Es の枠組みを利用してセキュリティ行動を定着させ、持続させることができるとしている。

この意味で、Trusted Research は、国際共同研究に係っている全ての英国の研究者に対して、研究インテグリティの確保に必要とされる事項を示したプロトコルであり、英国の大学及び資金提供機関として研究インテグリティを確保し、あるいは保証するための土台を提供するものと言える。

表 2-36 に、Trusted Research を軸とした、英国における研究インテグリティに関する取組とその流れを示す。また、図 2-5 に、英国における研究インテグリティに関連する政府機関／大学機関／R&D 資金提供機関、これらの機関が発行するガイドライン、関連する法規制、大学・研究機関等との相互関係を示す。

表 2-36：英国の政府機関、大学協会、資金提供機関等における研究インテグリティに関する取組とその流れ

年月	イニシアチィブ、プログラム、法令等	策定機関	関連する発行文書（ガイドライン等）	発行文書等の目的、概要等
2019年9月	Trusted Research	Centre for the Protection of National Infrastructure (CPNI)（MI5 傘下）（英国政府の物理的・人的保護やセキュリティに関して権限を持つ国家機関）	Trusted Research Guidance for Academia	・ 大学・研究機関の研究者に Trusted Research について理解を深めさせる一環として、セキュリティの観点から研究に係るリスクや研究者として注意すべき事項について説明し、法的義務（輸出管理、産学共同研究契約、武器禁輸、海外の司法コンプライアンス、GDPR（General Data Protection Regulation）、Patents Act 2004 、National Security and Investment Act（NSI 法）（2021 年 4 月 29 日制定、2022 年 1 月 4 日施行）[130]等）もすべて果たしていることを確認することを要請したガイドライン。 ・ 高等教育機関やその他の研究機関は、他の当事者と協力して、適格な企業や資産を取得、売却、開発する場合、NSI 法に留意する必要がある。
2020 年 10 月	Managing risks in internationalization	Universities UK (UUK)	Managing risks in Internationalisation: Security related issues	・ 大学に対して、研究インテグリティについてしっかりと理解させるうえで、CPNI による既存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て発行されたガイドライン。 ・ 外国による不当な干渉から高等教育体制を保護するために、一連の対策・措置を整理し、UUK に加盟している 139 の大学や研究機構の状況に合わせた運用を要請。

[130] GOV.UK ウェブサイト “Policy paper International Research and Innovation Strategy” <https://www.gov.uk/government/collections/national-security-and-investment-act>

年月	イニシアチィブ、プログラム、法令等	策定機関	関連する発行文書（ガイドライン等）	発行文書等の目的、概要等
2021年3月	（輸出管理規制）	Export Control Joint Unit 、Department for International Trade[131]	Export controls applying to academic research	・ 「Trusted Research」に対応して、軍事目的に使用される危険性が高い分野の研究を行っている研究者やポスドク研究者を向けの輸出規制に関するガイドラインである。 ・ 科学技術研究に関する英国の輸出規制の適用有無を評価する方法及び国際研究協力に関するデューディリジェンス・プロセスの実施のあり方を説明し、研究者が輸出規制を正しく遵守することができるためのルールを示している。
2021年6月	National Security and Investment Act（NSI法）	Department for Business, Energy & Industrial Strategy (BEIS)[132]	National Security and Investment Act: guidance for the higher education and research-intensive sectors	・ NSI法は、「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もの。国家安全保障上重要な17の機微な分野を指定し、特定の買収について英国政府に届け出ることを義務付けている。 ・ 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左記ガイドラインを公表。
2021年5月25日	Research Collaboration Advice Team (RCAT)の設立	Department for Business, Energy & Industrial Strategy (BEIS)[133]	－	・ RCATは、「Trusted Research」に対応して、研究者を敵対行為から守り、輸出管理規制、サイバーセキュリティ、知的財産の保護等のセキュリティ関連の課題についての政府の助言を提供することを目的として設

[131] 2023年2月、スナク政権の下に、ビジネス・エネルギー・産業戦略省（Department for Business, Energy & Industrial Strategy（BEIS））は、Department for Energy Security and Net Zero（DESNZ）、Department for Science, Innovation and Technology（DSIT）及び Department for Business and Trade (DBT)の3つの省に分割された。これを受けて、現在、輸出管理は、Export Control Joint Unit、Department for International Trade 及び Department for Business and Trade の3つの組織により実施されている。

[132] BEISは3省に分割されたが、新たにNSI法を所管する省庁に関する情報は公表されていない。

[133] BEISの分割に伴い、RCATはDepartment for Science, Innovation and Technology（DSIT）に属するものと思われる（これに関する公式情報は無い）。

年月	イニシアチィブ、プログラム、法令等	策定機関	関連する発行文書 （ガイドライン等）	発行文書等の目的、概要等
				立された機関。 ・ 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（法的権限は無し）。
2021年8月	Trusted Research and Innovation (TR&I)	UKRI	Trusted Research and Innovation Principles	・ 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。 ・ UKRIから資金提供を受けている組織は、左記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及び対策を実施したことを証明できるようにする必要がある。
2022年6月	Managing risks in international research and innovation	UUK / UKRI / CPNI	Managing risks in international research and innovation: An overview of higher education sector guidance	・ CPNI 、UUK 及びUKRIの3機関が作成したガイドラインや主要原則（Trusted Research Guidance for Academia、Managing risks in internationalization: Security related issues 、Trusted Research and Innovation Principles）をハイレベルでまとめたガイダンス。 ・ 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、上記の既存ガイドラインをどのように導入すればよいかを概説。

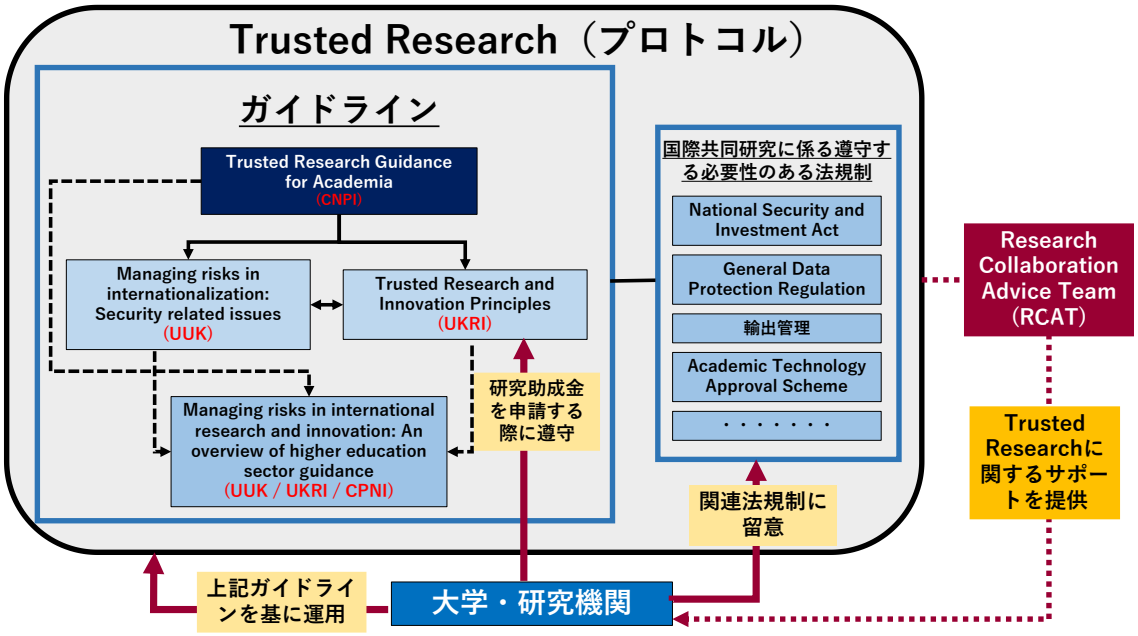


図 2-5：英国における研究インテグリティに関連する政府機関／大学機関／R&D 資金提供機関、これらの機関が発行するガイドライン、関連する法規制、大学・研究機関等との相互関係

2.2.2 資金配分機関等の取組

本項では、2.2.1 に示した英国における研究インテグリティに関する取組とその流れを踏まて、英国の大学協会である Universities UK (UUK)の取組、資金配分機関である UKRI の取組、並びに UUK 、UKRI 及び CPNI の 3 機関共同の取組を示す。

(1) Universities UK (UUK)の取組

UUK は、2020 年 10 月、外国による敵対的な干渉から守り、学問の自由を促進するために教育機関が取るべき配慮や対策について、詳細なガイドライン「Managing risks in internationalization: Security related issues」[134]を公表した（2021 年 8 月改訂版を発行）。

同ガイドラインは、大学として研究インテグリティを理解し、既存のガイドライン「Trusted Research Guidance for Academia」を補完するものであるとし、外国による不当な干渉から高等教育体制を保護するために、一連の対策・措置を整理し、UUK に加盟している 139 の大学や研究機構の状況に合わせた運用を要請している。

[134] UUK ウェブサイト “Managing risks in Internationalisation: Security related issues” <https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation>

(a) ガイドラインの位置付け

UUK は、本ガイドラインの位置づけとして、以下のように説明している。

- 本ガイドラインは、大学の統治機関及び執行責任者がこれらのリスクを管理するために必要なツールや支援を提供するものである。大学は必然的に学術的・専門的な専門知識を活用することになるが、アカウンタビリティは運営組織と執行責任者が負うことになる。
- このガイドラインは、外向的な高等教育セクターを抑制することを意図していない。むしろ UUK は、明確な見通しを持ち、リスクを管理しながら目標を追求するための手段を大学に提供することを目指している。本ガイドラインは、政府機関である CPNI が展開する Trusted Research キャンペーンなど、教育機関が利用できる既存の情報、助言及びガイダンスを補完することを意図している。
- 大学は英国の将来の繁栄と安全保障、そして共通の価値観を維持するために主導的な役割を担っている。このガイドラインは、国際的な共同研究を拡大し、その卓越性を守るための将来を保証するものである。
- このガイドラインは、国際教育戦略及び英国研究開発ロードマップという形で、国際教育と国際研究に対する野心的な戦略を発表している。このガイドラインはこのような活動の拡大が英国の大学の価値や国益を損なうことがないようにすることを意図した幅広い取組の一環として位置づけられている。

UUK は、安全保障上の問題が深刻化する中で、研究・イノベーション活動の成長、大学の自治、学問の自由、言論の自由を保護・促進するために、明確で協力的かつ建設的なアプローチをとることができるよう、政府と引き続き協力していくつもりであることを表明している。

(b) ガイドラインの目的

UUK は、高等教育におけるセキュリティ関連の問題について、3 つの長期目標を実現するための作業プログラムを確立している。

- 英国の大学が、国際的な安全保障上の脅威を管理・軽減するための首尾一貫した、積極的かつ戦略的・運用的なアプローチを有していることを証明することができる。
- 英国の大学は、持続可能で安全な国際的パートナーシップを追求する自信と能力を備えている。
- 英国の高等教育セクターと政府は、安全保障上の課題という背景のもと、研究・イノベーション（R&I）、 機関自治、学問の自由の保護・促進に向けて、明確かつ協力的で建設的なアプローチをとっている。

これらの目標を達成するために、UUK は以下の 3 つの中間成果を挙げている。

- セキュリティに関連する問題に関する個人の意識と理解の向上（教職員・学生を問わない）
- 組織のシステム、プロセス及び行動の強化
- 大学と政府との接点を含むエコシステムのより大きな変化とシステムの回復力

これらの中間成果は互いに重なり合い、相互に補強し合っている。このガイドラインの目的は、最初の 2 つの成果に向けて前進している教育機関を支援することである。

UUK は、このガイドラインの使用と配布を通じて、このガイドラインがカバーする問題への認識と理解が深まり、その結果、システム、プロセス、行動様式に変化が生じるとし、このような変化が、大学における国際的な協力関係や、大学のセキュリティ、繁栄、継続的な成功等に利益をもたらすとしている。

(c)　ガイドラインの構成

本ガイドラインは、以下の 4 つの章から構成される。

- 大学の評判と価値の防護
- 大学の人材の保護
- キャンパスの保護
- 大学のパートナーシップの保護

【大学の評判と価値の防護】

- セキュリティ関連の問題に対するレジリエンスの構築
- デューディリジェンスの再検討（風評リスク、倫理リスク、セキュリティリスクも考慮）
- 英国の高等教育の価値の促進。

【大学の人材の保護】

- 対内的・対外的ミュニケーションと知識の共有
- 渡航し海外で働くスタッフや学生の保護

【キャンパスの保護】

・サイバーセキュリティ、キャンパスの土地・建物及びビジター

【大学のパートナーシップの保護】

- 研究セキュリティ、知的財産及び輸出規制の遵守
- 国境を越えた教育のパートナーシップ

本ガイドラインには、研究セキュリティ、知的財産及び輸出規制に関するチェックリストが示されている。参考として、これを表 2-37 に示す。

表 2-37：研究セキュリティ、知的財産及び輸出管理に関するチェックリスト（「Managing risks in Internationalisation: Security related issues」[135]に基づき、未来工学研究所が一部和訳・編集）

チェック項目	内容
国際的な研究提携に関するデューディリジェンス	・ 国際的な研究協力が始まる前に、相応のリスク評価を行うという要件はどの程度明確か？ ・ 海外の研究プロジェクトのリスクアセスメントを実施する責任は誰にあるか？ ・ 研究の性質や提携の種類により、追加的な監視が必要な研究契約を特定するために、大学内にどのような方針が存在するのか？ ・ あなたの大学は、候補として考えている新しい研究パートナーが行っている研究業務の規模や種類をどのように調査しているか？ ・ あなたの大学では、個々の研究者や研究責任者が設立した小規模又は非公式な研究提携を監視するために、どのようなプロセスを取っているか？ ・ リスクの高い国際的な研究提携について、継続的なデューディリジェンスを行うために、どのような追加的な資源や支援があるか？ ・ 契約の合意事項の翻訳版には、同一の条件が含まれていることを確認するための措置をとったか？
知的財産を保護するための方針と契約書	・ あなたの機関は、知的財産を保護するためにどのような方針、ツール、枠組みを使用しているか？ ・ 研究協力に関する契約上の合意への署名と監視の責任は誰が負っているか? ・ 英国内の研究者間の一対一の共同研究など、資金提供のない研究プロジェクトで締結される契約や協定はどのようなプロセスで行われるのか？ ・ 契約上の研究協定の違反や変更に対処するプロセスはどのようなものか？ ・ 研究者は、英国に拠点を置く者も海外に拠点を置く者も、定期的

[135] 同上

チェック項目	内容
	に外部の業務義務や利益相反を開示するよう求められるか？ ・ 研究者がサイバーセキュリティ侵害や個人所有物の盗難を通じた知的財産の盗難等から保護するための対策を講じることを支援するために、どのようなトレーニングが利用できるか？
デュアルユーステクノロジーと輸出管理法	・ 研究者は「デュアルユース」という言葉を理解し、それが自分たちにどのような影響を与えるかを知っているか？ ・ 研究者は、自らの研究がデュアルユースとなる可能性を合理的にどのように考えるか？ ・ 研究者は、自分の研究が英国の経済・社会・安全保障上の利益を促進することと矛盾する目的に利用される可能性を、どのような形で考慮しうるか？ ・ 輸出管理法及びその他の関連する法的枠組みを確実に遵守するために、どのような戦略があるか？ ・ 研究者が学内外を問わず、どのような場合にさらなる助言を求めるべきかに関して、どのような指針があるか？ ・ 投資によって、英国の戦略的輸出規制や類似の措置が損なわれたり、回避されたりするリスクはないか？

なお、UUK は、大学管理機関及び上級管理者は、このガイドラインに示されたリスクを管理する責任を負う職員を特定し、明確なガバナンス構造を確立する必要があるとしている。UUK は、大学が国際化に伴うセキュリティ関連のリスクをどのように管理しているか、大学が直面するリスクとそのリスクをどのように軽減しているかに関する年次報告書を、大学の理事会に提出することを強く推奨するとしている。

(2) UKRI の取組

UKRI は、2021 年 8 月に、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を定めた「Trusted Research and Innovation Principles」[136]を公表した。

UKRI から資金提供を受けている組織は、「Trusted Research and Innovation Principles」に示された原則を採用し、これらの原則に合致する管理及び対策を実施したことを証明できるようにする必要がある。これは、新規の助成金と既存の助成金に適用される。

[136] UK Research and Innovation, "UK Research and Innovation Trusted Research and Innovation Principles," August 2021. <https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf>

以下は、Trusted Research and Innovation の原則の要点である。

(a) パートナーの適性評価

財政的及び非財務的な協力パートナーとなりうる組織や個人について、以下に概説する分野に関連して、適切なデューディリジェンス評価を実施すべきである。

リスクを特定する際に考慮される要因の例としては、プロジェクト活動の性質や想定される成果物、プロジェクト情報や成果物の非倫理的又はデュアルユースの可能性、詐欺、贈収賄及び汚職の可能性、並びに協力パートナーが挙げられる。

【法的枠組みと提携関係】

パートナー組織やその運営する国の法的枠組み及び憲法、所有者、他の企業、政府省庁、軍などとの正式な提携の有無について理解する必要がある。プロジェクト情報又はプロジェクトの成果物の取り扱いのインテグリティに潜在的なリスクをもたらす提携関係がある場合、組織のリスク選好度に沿って緩和策を講じるべきである。

また、組織は、「National Security and Investment Act（NSI 法）」の下で適用されるあらゆる義務についても認識しておく必要がある。

【価値観】

パートナー国がベースとしている民主的・倫理的価値観を理解し、それが英国の価値観と何が異なるかを理解することが重要。

【利益相反】

組織と関わりを持つ人々について、個人レベルでの意識を高めることはセキュリティに関連する潜在的なリスクを評価するために不可欠である。

組織のリスクへの選好度に合わせて適切なデューディリジェンスを行うことで、雇用、学習、共同研究、訪問及びデータへのアクセスなどを通して物理的あるいは仮想的に組織にアクセスする個人がもたらす既存又は潜在的な利益相反を特定することが可能である。

リスク指標としては、その人が軍関係者であるかどうか、他の収入源、他の雇用、研究インテグリティ又は倫理基準に対する違反の支持された申し立てなどを考慮することができる。

(b) 情報・知識共有管理

透明性と開放性は、研究とイノベーションの成功に不可欠ではあるが、この要件は、情報及び知識の共有を保護する必要性とのバランスをとる必要がある。したがって、組織は機密データや情報へのアクセスが適切に管理されるよう、強固な情報セキュリティ管理策を導入することが不可欠である。

【サイバーセキュリティ】
サイバー攻撃のリスクを軽減するには、スタッフと学生向けの広く公表されたガイダンスを含むセキュリティ意識向上及びトレーニングプログラムの一部として導入されたサイバーコントロールの開発を通じて達成される堅牢なサイバーセキュリティ文化が不可欠である。

【データの分離】
機密データは安全に保管する必要があり、共有プラットフォームが情報交換に使用される場合は、許可された個人のみがアクセスできるように、データを論理的に異なる場所に分離する必要がある。

【データへのアクセス】
機密データへのアクセスは、アクセスの明確な要件を持つ個人にのみ付与する必要がある。データの取り扱いと使用に関する根拠は、情報を共有する前に、すべての関係者によって明確に特定され、理解され、合意される必要がある。海外パートナーに適用される当該国の法律が、当局がすべての関係者の同意なしに機密情報にアクセスすることを許可する可能性があることに注意することが重要。

【研究プロジェクト活動と成果】
すべてのプロジェクト活動及びプロジェクトの成果の取り扱いは、適用される輸出管理法及びその他の法的要件に準拠していなければならない。さらに、プロジェクト活動の性質や想定される成果物について、デュアルユースや非倫理的な適用の可能性について、十分な配慮がなされなければならない。

(c) 商用への応用
特に、将来的に商業的な成果が実現し、英国を含む社会や経済に利益をもたらす可能性がある場合、プロジェクトから得られる機密データや知的財産権を含む知的資産が適切に管理されるよう、共同研究契約を締結する必要がある。

【知的資産と知的財産権】
プロジェクトから生まれた知的財産を含む知的資産は、専門的かつビジネス的な方法で管理されるべきである。これには、プロジェクトから生じる知的財産の保護を求めるのが最も適切な時期を決定することや、その影響を最大化するためにそれをどのように利用、譲渡、ライセンス供与、普及させるかを決定することが含まれる。

【プロジェクトの成果物の公開】

すべての研究パートナーは共同研究に先立ち、プロジェクトに由来する商業的な関連性や機密性の高いデータ、知見をいつ一般に公開するかについて正式に合意しておく必要がある。必要な場合には、出版前に知的財産を含む知識資産の保護を求めるか、代わりに、高レベルのバージョンを出版することが適切である。研究成果の公開を決定した場合、その成果は UKRI のオープンアクセス及びオープンデータに関する方針とガイダンスに従う必要がある。

【輸出管理】

英国の輸出規制は、機密性の高い技術、知識及び戦略的物資の輸出と伝達を制限するために設けられており、学術界にも他の輸出者と同様に適用される。UKRI から資金提供を受けているすべての組織は、資料の輸出から会議でのプレゼンテーションに至るまで、自分たちのプロジェクトや活動に適用される可能性のある輸出規制を確実に理解する必要がある。

(3) UUK、UKRI 及び CPNI の 3 機関共同の取組

UUK、UKRI 及び CPNI は、2022 年 6 月、これら 3 機関が共同で作成した主要原則とガイドラインをハイレベルでまとめた、「Managing risks in international research and innovation: An overview of higher education sector guidance」[137]を発表した。本ガイダンスは、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、既存のガイダンス（Trusted research guidance for academia（CPNI 作成）、Managing risks in internationalization: Security related issues （UKRI 作成）、Trusted Research and Innovation Principles（UKRI 作成）をどのように導入すればよいかを概説したものである。

本ガイダンスは、セキュリティ関連問題に関する他のガイダンスを補完するものであり、英国の大学が自信を持って、持続可能で安全な国際的パートナーシップを追求できるようにすることを目的としている。本ガイダンスは、UUK、UKRI、CPNI が作成したオリジナル文書の原則やガイドラインに代わるものではなく、オリジナル文書と併せ、全文を読むことを求めている。

表 2-38 に、本ガイダンスの包括的な目標、扱う脅威、大学へのリスク及びリスク緩和策を示す。

137 UUK/CPNI/UKRI, “Managing risks in international research and innovation: An overview of higher education sector guidance,” June 2022.
<https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf>

表 2-38：「Managing risks in international research and innovation: An overview of higher education sector guidance」の包括的な目標、扱う脅威、大学へのリスク及びリスク緩和策（「Managing risks in international research and innovation: An overview of higher education sector guidance」[138]に基づき、未来工学研究所が一部和訳・編集）

狙い	脅威	大学にとってのリスク	リスク緩和策
・ 大学や研究機関がセキュリティの脅威から組織・人材・研究を守ることができるようにすること。 ・ 学生・職員・学部の権利と機密情報を確実に保護すること。 ・ 英国の高等教育・研究セクターの評判とインテグリティを維持・強化すること。	このガイダンスが扱う最も深刻な国家安全保障上の脅威は、研究に対する国家の脅威である。 その他の脅威としては、サイバーアタック、不正な事業提案、テロ、海外の学生やスタッフの拉致や危害などがある。	これらの脅威を軽減できなければ、組織にとってより直接的なリスクも発生する。 これには、風評リスク、経済的損失、訴訟（輸出規制、NSI）、学生やスタッフの権利侵害などが含まれる。	・ 機密性の高い研究の特定 ・ パートナーに対するデューディリジェンス ・ 組織のトップによりリスクマネジメントが調整・承認されたグッドガバナンス ・ 教員の研修と意識向上 ・ 適切な情報管理・共有 ・ 適切な物理的・人的セキュリティ ・ 法令遵守

(a) 緩和策のチェックリスト

本ガイダンスでは、国家安全保障上の脅威として最も一般的なのは国家の脅威であり、組織は、以下のような国家や非国家主体から受ける様々なリスクに直面していると警告している。

・ サイバーアタックなどの積極的な敵対行為や違法行為、あるいは詐欺的又は法的に曖昧なビジネス提案や慣行を通じて、個人的に、金銭的又は社会的な利益を得ようとする。
・ 他国に対する自国の経済的、技術的及び軍事的優位性を高める機会を狙っている。
・ 自国民に対して技術的・軍事的優位性を行使しようとする、あるいは組織的な人権侵害、法的・財務的不正及び不利な評判を覆い隠すための PR の機会を得ようとする。

また、本ガイダンスでは、研究や専門知識は、学術機関、国家と連携した団体、民間企業や個人を通じてアクセスし、移転することができるとし、研究、データ及び職員の保護に失敗すると、組織や職員に金銭的損害や風評被害が生じ、研究インテグリティが損なわれる可能性、ひいては国家安全保障を損なう可能性もあるとしている。

大学は、これらの問題に真剣に取り組むことで、以下のことに貢献することができるとしている。

[138] 同上

・ 大学職員とキャンパスの保護
・ 大学の評判と価値の保護
・ 研究及びパートナーシップの保護
・ 英国の高等教育に対する信頼の保護

そのために、大学は以下のことを行う必要があるとしている。
・ 教育・研究パートナーを理解する。
・ 自身の義務を理解する。
・ 脅威、脅威緩和の方針及び脅威緩和のための役割について、職員と効果的にコミュニケーションをとる。
・ これらのリスクを緩和するために適切な行動をとる。

大学は、これらのリスクに対処し、リスクを軽減するための行動をとることにより、自らを守るだけでなく、英国の高等教育セクター及び信頼できるパートナーとしての共同的安全や評判の保護に貢献することができるとしている。

これらの脅威とガイドラインの意図する成果に関する詳細は、緩和策のチェックリストにまとめられている。

表 2-39：緩和策のチェックリスト
（「Managing risks in international research and innovation: An overview of higher education sector guidance」[139]に基づき、未来工学研究所が一部和訳・編集）

項目	緩和策の内容
1. 大学の評判と価値の保護	大学のガバナンス機構は個人に権限を与え、職員や学生が大学のリスク許容度に沿って国際的な協力関係を追求し、潜在的なリスクを軽減できるような文化を促進することを支援する必要がある。大学は、リスクを考慮する文化を醸成し、セキュリティ関連の問題を関連する政策に盛り込み、連帯責任の文化を構築すべきである。大学は次のような方法でこれを支援することができる。 ・ 安全保障関連のリスクマネジメントを重要かつ継続的な優先事項として確立する。 ・ 研究及び組織に対する国家安全保障上のリスクについて、理事会レベルのオーナーシップと可視性を確立する。 ・ 上位指導者チームの中から安全保障関連問題の責任者を任命する。 ・ パートナーを把握し、強固なデューディリジェンスに基づき、リスクアセスメントの結果を踏まえた意思決定（risk-informed decisions）を行う（例えば、財政的及び非財務的な協力パートナーとなり得る組織や個人のリスクアセスメントを通じて）。 ・ 主要なスタッフの責任を明確にする 。 ・ オープンで透明性のある議論を促進する。 ・ 行動規範や方針を策定し、懸念を表明するための仕組みを整備し、大学や部局

139 同上

項目	緩和策の内容
	に伝達する。 大学機関は、その自律性、言論の自由、学問の自由を引き続き推進しなければならない。
2. 研究の保護	財務的及び非財務的な研究パートナーと共同研究を行う場合、大学は知的財産の保護、情報に基づいた意思決定及びサイバーリスクの管理を行うことが重要である。大学は、次のような方法で研究を保護することができる。 ・ 法的枠組み、輸出規制及び GDPR の活用と理解 ・ 個人データや研究データの保護と厳重な保管 ・ データへのアクセスの制御と監視を含む、サイバーセキュリティ戦略の策定・実施・見直し ・ プロジェクトや研究活動の性質の考慮 研究者は、商業的な機密性、国家安全保障技術に関連する研究、将来的にデュアルユースや非倫理的な応用が可能な研究など、自分の研究のどの分野が最も機密性が高いかを把握する必要がある。
3. 大学の職員とキャンパスの保護	研究者は、自分自身と組織の研究を保護するために取られた措置について認識している。これには、海外で勤務する職員の保護や、海外からの研究者との協働の意味合いを理解することも含まれる。大学は、研究者が海外の学会に出席する際や海外の研究者と共同作業を行う際に、研究者の安全確保を支援し、プロセスと手順によって安全や福祉を促進する必要がある。大学は、以下のような形でこれを支援することができる。 ・ 内部及び外部とのコミュニケーションと知識共有のプロセスを開発する。 ・ 大学機関内の連絡窓口を明確にする。 ・ 適切な出張手配の計画を行う。 ・ 適切なデューディリジェンスとリスクアセスメントを実施する。 ・ 施設と訪問者の統合的な方針の策定（例：枠組み、訪問者のチェック、訪問者協定に関する戦略的監督、並びに、訪問者・職員に対するプロトコルに関する明確な情報、アドバイス及びガイダンス）
教育・研究パートナーシップを理解する	共同研究に際しては、自大学と研究パートナーにとってのセキュリティの意味を認識し、共同研究の適否を判断することが重要である。大学は、サプライチェーンやパートナーのセキュリティを理解するために適切なデューディリジェンスを行い、このプロセスが継続的かつ発展的であることを確認する必要がある。これは、大学が以下を行うのに資するはずである。 ・ 英国の法的枠組みと、パートナーやその活動する国の法的枠組みを理解する。 ・ パートナーの国の民主的・倫理的価値観と、それが英国とはどのように異なるかを理解する。 ・ 利害の衝突や状況の変化に対応する。 ・ 物理的な研究プログラムとオンライン研究プログラムを分離する。 ・ 競合する機関を保護し、その契約で期待されるものを理解する。 ・ 透明性のある研究コミットメントと活動を実証する。 ・ 国境を越えた教育パートナーシップを保護するための手段を検討し、出口戦略を策定する。

(b) ガイドラインの実施方法

本ガイドラインでは、リスクを効果的に管理するためには、大学は健全なガバナンスを有し、明確なリーダーシップと、リスクを特定し、評価し、軽減するための強固なプロセスを備えている必要があるとして、大学に対して以下の必要性を説いている。

- 大学にはすでにそのようなシステムやプロセスが存在しているはずであるが、セキュリティ関連リスクは斬新で進化し続ける性質があるため、特別な注意を払う必要がある。
- 大学は、国際的な協力関係やパートナーシップのセキュリティに関して、上位管理者レベルでの可視性と説明責任を確保することになる。また、リスクマネジメントアプローチを採用し、セキュリティを重視する文化を醸成する必要がある。大学はまた、セキュリティ意識の文化を促進し、個人と集団の責任を伝え、強化する必要がある。
- セキュリティ関連の課題への対応については、定期的に見直しを行い、大学の方針とプロセスを必要に応じて進化させ、現在の脅威に対応できるようにする必要がある。

上記を行うための最初のステップとして、本ガイダンスでは、以下を提案している。

- 上位管理職の中から、セキュリティ関連の事項を担当する者を任命する。
- 3 つの主要なガイダンスと、その他の関連するガイダンスに目を通す。
- 推奨される分野の専門知識を有する大学機関内の利害関係者からなるチームを結成する。
  - これには、「研究」、「国際」、「採用」、「運営・支援」、「募集・学生支援」等のチームが含まれるが、これに限定されない。また、IT、不動産、人事、財務、運営、教育、法律のような専門的なサービスも含まれる。
- 既存の関連プロセスを見直し、推奨されるアクションのリストを特定するとともに、指揮を取る者と時間軸を提案し、それをプロジェクト計画にして、理事や理事会に提示する。
- 上位責任者と報告を明確に定義した行動計画を策定する。大学が行ったアクションの例としては、以下が挙げられるが、これらに限定されるものではない。
  - 研究、財務、フィランソロピーなどの部門間でデューディリジェンス管理を統一する。
  - リスク登録簿（リスクレジスター）を拡充し、機関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を高度化する。
  - 大学機関の価値観、学問の自由及び言論の自由に関するポリシーを更新・改訂・作成する。
  - ポリシーやトレーニングプログラムの改善、セキュリティに関するスタッフトレーニング及び新しいワーキンググループや報告プロセスの構築を行う。
  - サイバーアタックや物理的な侵入テストを実施し、仮想及び物理的なセキュリティ・インフラストラクチャを更新する
  - フィッシングメールテスト、訪問者シミュレーション、危機管理手順のユースケー

スに対する使用など、セキュリティポリシーの「ストレステスト」を実施する。

- 大学機関の運営委員会がセキュリティ関連の事柄に関心を持ち、その進展が適切に伝達されるようにする（UUK のガイドラインでは、大学機関の運営委員会がセキュリティリスクに関する年次報告書を受け取ることを推奨)。
- 実務家、研究者及びより広範な学術サービススタッフが、ポリシーの更新や変更の理由を認識し、納得できるようにするための計画を立てる。これらの計画は、セキュリティの優先事項や脅威の変化を反映させるため、定期的にレビューする。

2.2.3 主な大学の取組

前述の、UUK 、UKRI 及び CPNI の共同の取組として作成された「Managing risks in international research and innovation: An overview of higher education sector guidance」では、英国の大学における「Trusted Research」への取組の事例として、ストラスクライド大学（University of Strathclyde)、インペリアル・カレッジ・ロンドン（Imperial College London）及びマンチェスター大学（University of Manchester）の事例が挙げられている。

ストラスクライド大学及びインペリアル・カレッジ・ロンドンの取組は、大学のトップレベルを巻き込んだワークショップ、学部や教授会とのセミナーやフォーラムなどによる研究セキュリティに関する意識の共有や認識の強化、研究セキュリティ体制の強化などが中心であり、両大学の「Trusted Research」の取組に関するサイトからは、特徴ある取組に関する情報が出てくるわけではない。

一方、マンチェスター大学では、研究者に、自身の研究に適用される可能性のある多種多様なプロセスについて、いつ、どのように関わるべきかを理解してもらううえで、大学としてどのように支援すれば良いのか、また、グローバルな課題に取り組もうとする研究者にとって、研究のプロセスの負担となる可能性があるという懸念が障壁とならないようにするうえで、大学としてどうすれば良いのか、といった問題に対処することを目的として、研究リスクプロファイラー（Research Risk Profiler）と呼ばれるオンラインツールを開発・運用している。これに関する情報は同大学のサイトでも公開されており、非常に参考になる。

ここでは、マンチェスター大学の取組を説明し、参考情報として、本ガイドラインに記載されている、ストラスクライド大学及びインペリアル・カレッジ・ロンドンの取組みを示す。

(1) マンチェスター大学の事例[140,141]

研究リスクプロファイラー（Research Risk Profiler）は、研究者が新しいプロジェクトを計画する際に、安全かつ確実にプロジェクトを進めることができるように、複雑なリスクやコンプライアンスに関する幅広いトピックをナビゲートすることを支援するものである。

このツールは、潜在的なリスクをプロファイリングし、関連する大学のアドバイスやセキュリティ関連の問題のリソースからのガイダンスを纏めた、研究プロジェクトに関する一連の質問で構成されている。

このツールは、研究者と、関連するリスクやコンプライアンス・プロセスのナビゲーションを支援することができる、専門サービス・スペシャリストの同僚・チームとを繋ぐものである。プロファイリングされるリスク領域には、パートナー評価、輸出規制、学術技術承認制度（Academic Technology Approval Scheme：ATAS）、情報セキュリティ、IP などの「Trusted Research」に関連するトピック及び研究倫理、旅行リスクが含まれる。

このツールは、研究者がプロジェクトに関する質問に答えることで、さらなる調査が必要な主要リスクを特定し、そのリスクプロファイルの概要に基づき、プロジェクトを支援するためのアドバイスやプロセスの案内を行う。研究者の回答が完了すると、プロジェクトの結果が提示される。

質問は、以下の 7 つの項目から構成されている。

- 国（資金提供国、研究パートナーの出身国、プロジェクト活動を行う国）
- 研究に関連する事項（外部研究資金源、研究パートナー、利益相反などに関する情報）
- 採用・ビジター（研究プロジェクトにおける外国人研究スタッフの採用の有無、外国からの訪問者の有無など）
- 規制されている研究分野（人間や動物実験などへの関連性の有無、輸出規制など）
- 情報・知識共有の管理（データ管理に関する事項）
- 商用利用（知的所有権に関する事項）
- 出張と安全防護対策

対象となるリスクは、CPNI Trusted Research キャンペーンで言及されている、主にプロジェクト外から発生するもの、及びリピュテーションや倫理的な考慮事項である。安全衛生リスクや技術リスクなど、個々のプロジェクトの実施に極めて特有なリスクは対象外である。

同大学のプロジェクトチームは、多くの研究者と協力してこのツールを開発し、フィード

140 マンチェスター大学ウェブサイト “Launch of the Research Risk Profiler tool” <https://www.staffnet.manchester.ac.uk/rbe/news/display/?id=27730>

141 UUK/CPNI/UKRI, “Managing risks in international research and innovation: An overview of higher education sector guidance,” June, 2022. <https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2022-06/managing-risks-in-international-research-and-innovation-uuk-cpni-ukri_1.pdf>

バックを受けて、若手研究者や経験豊富な研究者が異なる研究分野で新しいプロジェクトを計画する際に役立つガイダンスを全体に提供できることを確認したとされている。

(2) 参考情報１：ストラスクライド大学の事例[142]

ストラスクライド大学では、セキュリティに関する課題は多岐にわたり、大学組織や大学文化の多くの側面に及んでいる。

CPNI と UUK が最初のガイダンス文書を作成し、発表したとき、ストラスクライド大学では、多くの異なる専門職や学術団体の代表者、副学部長、大学倫理委員会の委員長を集めて、大学内でワークショップを開催することにした。

これにより、既存のさまざまな責任がどこにあるのか、また、既存の技術的・組織的発展がセキュリティ関連の問題とどの程度整合しているのかについて、十分な理解を得ることができた。最も重要なことは、文化的な課題という点で、機会（チャンス）と弱点の両方が浮き彫りになったことである。

この最初のレビューで得た理解は、セキュリティ関連の問題に関するその後の作業の多くに反映された。例えば、輸出管理に関する高等教育機関の取組や、高等教育輸出管理協会（Higher Education Export Control Association: HEECA）の設立を強力に支援し、関与することにつながった。

文化的な変化という点では、セキュリティの課題に対する理解不足が認められたが、同時に 2 つの重要な機会もあった。まず、ストラスクライド大学は産業界とのつながりが強く、長い間、学術的な目標を達成しながら、非学術的なパートナーとの協力に伴う責任について考えることに慣れている同僚が多くいたことである。第二に、研究インテグリティは、優れた学術的実践の主要原則を包含するものとして広く理解されていることから、セキュリティも包含されるべきであると判断された。その結果、ストラスクライド大学の研究インテグリティのポータルサイトを通じて、セキュリティ関連の問題に関する情報を取り入れることにした。

セキュリティは広範な性質を持っているため、ストラスクライド大学の様々な業務に組み込む必要がある。ストラスクライド大学は輸出管理に関する能力をさらに強化するための投資を行っている。最近、初のデータ・情報主任が任命されたことで、サイバーセキュリティに関する継続的な取組がさらに強化され、戦略策定の中心的な役割を担うようになった。また、ストラスクライド大学のセキュリティに関するマインドの継続的な発展を支援するため、役員レベルのチーフ・コンプライアンス・オフィサーを任命した。

(3) 参考情報２：インペリアル・カレッジ・ロンドンの事例[143]

インペリアル・カレッジ・ロンドンの現在のアプローチは、学問の厳密さとインテグリテ

142 同上
143 同上

ィという確立された原則を基礎とするものである。

インペリアル・カレッジ・ロンドンは、注意深く責任感のあるコミュニティを育成することによって、セキュリティに配慮する文化を実現することを目指している。インペリアル・カレッジ・ロンドンの研究コミュニティや意思決定者は、共同研究におけるリスクや特定の機会における不利益の可能性を認識できるよう、十分な情報を持っている必要がある。

インペリアル・カレッジ・ロンドンは、学部や教授会とのセミナーやフォーラムを継続的に開催し、セキュリティ関連の問題や法的背景に対する認識を積極的に高めている。これと並行して、インペリアル・カレッジ・ロンドンは法令遵守のための強固なプロセスを確立している。特に、輸出ライセンスの作成と管理、NSI 法の要件を満たすためのトリアージ手続きには、専門のリソースを配置している。

知識はこれらすべての基本であり、インペリアル・カレッジ・ロンドンは組織的に次のような重要な視点をもっている。

- Who : 我々は相手をどの程度知っているのか？法律上の立場はどうか？彼らは我々の価値観と一致しているか？
- What : 我々は何をしているのか？その活動には機微なものがあるのか？統制の対象となるものはあるのか？
- Where : その活動はどこで行なわれているのか？機微事項や禁輸措置の対象となる地域が関与しているのか？輸出が行われているのか？

インペリアル・カレッジ・ロンドンは、デューディリジェンスのプロセスを確立してきた。最近では、機密性が高いと判断される取引や活動に対する追加的な精査プロセスも含まれている。このプロセスでは、委員会が証拠を確認することができ、委員会は提案された活動の継続、停止、あるいは終了のための条件を助言することができる。

これは繰り返し行われる継続的なプロセスであり、適切なレベルの能力、特に管理された一貫したコンプライアンスを可能にするセクター特有のツールや情報へのアクセスに到達し、維持するためには十分な時間とリソースが重要である。

2.2.4 研究インテグリティ確保のための支援

2021 年 5 月 25 日に、英国ビジネス産業戦略省（BEIS）が、研究者を敵対行為から守り、輸出管理規制、サイバーセキュリティ及び知的財産の保護等のセキュリティ関連の課題についての政府の助言を提供するために、省内に Research Collaboration Advice Team (RCAT)を立ち上げた[144]。

RCAT は、英国政府と学術界の協力のもと、研究機関に対して、国際的な研究に関連する

[144] BEIS の分割に伴い、RCAT は Department for Science, Innovation and Technology（DSIT）に属するものと思われる（これに関する公式情報は無い）。

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ものである[145]。

英国政府は、英国の貴重な技術や機密技術にアクセスするために、容認できない手段を用いて国家安全保障を脅かす敵対的な行為者がおり、多くの場合、国際的な研究協力のパートナーの１人又は複数が、商業的、国家安全保障的、軍事的利益を求めて、不誠実さや脅しにより、データ、ノウハウ、機器にアクセスすることが原因となっていることを認識している。

RCAT は、研究者や大学のリーダーがこういったリスクを理解し、共同研究を支援するために適切かつ妥当な保護措置を講じることを支援し、英国のセキュリティ政策や規制について学術研究者の理解を深めるとともに、個々のニーズに合わせたリスク管理ガイダンスを提供することで、共同研究活動を支援するとしている。

RCAT は、研究者が国際的なプロジェクトを保護するために、次のような支援を行っている。なお、RCAT は法的権限を持つ機関ではない。研究者と研究機関の独立性を十分に尊重し、研究機関と自発的に連携している。

- 国際的な研究活動において遵守すべき法律や規制について、研究者の理解を深めること。
- 敵対者が用いる容認できない戦術、それが研究者とその研究をどのように危険にさらすか、そしてこれらのリスクを効果的かつ適切に管理する方法について、研究者の理解を深めること。
- 研究者がどのようにリスクに遭遇し、どのようにそれに対処しているか、また、政府と学術界がどのように協力して実践を改善できるかについて、政府の理解を深めること。
- 国家安全保障における英国の研究基盤の重要性を反映した政策や基準を学術機関が策定し、実施することを支援すること。

RCAT のアドバイザーは、研究提携、輸出規制、サイバーセキュリティ、特定の国際研究協力における知的財産の保護など、安全保障に関する機密事項や新たな話題について、大学がアドバイスを受けたり、内密に相談したりできるルートを提供している。

なお、RCAT のアドバイザーは、英国内の BEIS 事務所を拠点とする地域チームに配属されている。これらのアドバイザーは、各地域の研究機関と 1 対 1 の信頼できる関係を構築しており、大学・研究機関の上級研究リーダーに対する一貫した相談窓口となっている。

[145] GOV.UK ウェブサイト “Research Collaboration Advice Team (RCAT)” <https://www.gov.uk/government/groups/research-collaboration-advice-team-rcat>

2.3 オーストラリア

2.3.1 概要

豪州における研究インテグリティへの取組は、いわゆる研究倫理にまつわる「研究公正」と、学術研究の国際化に伴う海外からの干渉にまつわる「外国干渉セキュリティ」の２つに峻別できる。前者は大学・研究機関における研究の誠実さなどに焦点を当てたもので、不正行為を防ぐ目的で主として研究資金配分機関やそれぞれの大学・研究機関が個別に対応している。また後者は近年、研究活動の国際化が進む中で「新たな脅威」として注目を集めている分野で、外国政府や機関の干渉を排除する目的で、豪州の政府や大学機関などで構成される官学合同のタスクフォースが一体となって対応する仕組みになっている。それぞれ詳しく見ていく。

まずは研究公正について。豪州には大学・研究機関に競争的資金を配分する機関として、教育省が所管する豪州研究評議会（Australian Research Council: ARC）[146]と保健省が所管する国立保健医療研究協議会（National Health and Medical Research Council: NHMRC）[147]の２つがある。研究の不正に対しては、両機関が共同して組織・運営する豪州研究公正委員会（Australian Research Integrity Committee: ARIC）[148]が、資金配分機関や研究者個人などの求めに応じて不正対応プロセスの妥当性を審査する仕組みになっている。その際に準拠しているのが、通称・豪州規範（The Australian Code for the Responsible Conduct of Research、「責任ある研究実施のための豪州規範」）である[149]。同規範は 2007 年に両機関と豪州大学協会（UA）によって策定され、2018 年に改定されて今に至る。規範には法的拘束力はないものの、大学・研究機関が資金配分を受ける際に遵守することが求められている。

豪州の研究インテグリティに対する考え方は、あくまでも大学・研究機関による自主性や自己規制を重んじる形になっている。このためたとえ不正事案であっても、不正調査や認定を資金配分機関が行うことはなく、個別の大学あてに勧告を出すにとどまっているのが大きな特徴だ。同規範はそれを補完するガイドラインを普及することによって、豪州全体の研究不正を失くし研究活動の質的向上を図ることを目的としている。

次に外国干渉セキュリティについて説明する。豪州の政府や大学・研究機関が外国からの干渉に対応せざるをえなくなったのは、2017 年前後を境に豪州と中国との外交・経済関係が大きく変化したことが背景にあるとされる。それまで蜜月関係にあった豪中２国間関係

146 Home | Australian Research Council.< https://www.arc.gov.au/>
147 Home | NHMRC, <https://www.nhmrc.gov.au/>
148 Australian Research Integrity Committee (ARIC) | Australian Research Council, <https://www.arc.gov.au/about-arc/program-policies/research-security-and-integrity/research-integrity/australian-research-integrity-committee-aric>
149 The Australian Code for the Responsible Conduct of Research (nhmrc.gov.au), <https://www.nhmrc.gov.au/sites/default/files/documents/attachments/grant%20documents/The-australian-code-for-the-responsible-conduct-of-research-2018.pdf>

が急速に悪化したきっかけは、南シナ海の領有権問題や経済投資問題などにからんで中国との摩擦が増え、同国からの内政干渉が強まり始めたことにある。

○外国干渉セキュリティをめぐる主な流れ

2019 年 11 月　外国干渉タスクフォース（UFIT）ガイドラインを公表
　　豪州国立大がサイバー攻撃され 20 万人分の個人情報流出
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
2022 年 3 月　大学・研究機関の安全保障上のリスクに対し連邦議会が 27 の勧告

同年には、内務省直轄の防諜機関である豪州保安情報機構（ASIO）のダンカン・ルイス長官（当時）が、中国を念頭に豪州の大学への干渉について大学側が無防備であるとして警鐘を鳴らした。また 2020 年には、新型コロナウイルスの発生源について、モリソン首相（当時）が独立調査を求めたことに対し中国が大きく反発し、戦略的経済対話を停止するなどの事件もあった。こうした豪中関係の悪化に伴い、同年 12 月に外国関係法が制定され、豪州の大学・研究機関が外国政府と取り決めを締結する際には、外務大臣への事前通知と承認取り付けが義務づけられるなどした。

大学の現場では、最も規模が大きな中国人留学生をめぐり、学内で民主化を求める中国人留学生に対するハラスメントや告発が相次いだり、中国からの攻撃とみられる大学当局へのサイバー攻撃、研究成果や技術の海外流出などの事案が報告されたりする大きな変化が起きるようになった。

こうした豪中関係の悪化を背景に、豪州では 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[150]。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[151]。

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されているものもある。

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。

---

150 University Foreign Interference Taskforce - Department of Education, Australian Government, <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/university-foreign-interference-taskforce>

151 Guidelines to Counter Foreign Interference in the Australian University Sector - Department of Education, Australian Government, <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector>

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。大きな特徴は、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にある。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。

2.3.2 研究インテグリティの確保のための要求と支援

UFIT ガイドラインの内容を具体的に見ていこう。2021 年に改定された同ガイドラインは全文 24 ページ。大学・研究機関がリスク管理を実施する上で重要なテーマを次の 4 項目に分けて規定している。

（1）ガバナンスとリスクのフレームワーク
（2）コミュニケーション、教育及び知識共有
（3）デューディリジェンスやリスク評価、リスクマネジメント
（4）サイバーセキュリティ

それぞれの項目の中で、ガイドラインはアクター間の「支援」と「要求」を規定している。まず支援から見ていくと、ガイドラインは「外国干渉への高い耐性を構築することに寄与するため」として、外国干渉に対抗する上で政府が大学・研究機関に支援を提供するものとして次の 5 項目を提示している。

・大学の上級管理者に対し、外国干渉の脅威と国家安全保障政策について説明する
・外国干渉に対する大学職員の意識を向上させる
・政府の保安情報機構（ASIO）や外国干渉対策調整センターを通じての大学への働きかけ
・国益となる重要な技術に関する最新情報を提供する
・サイバーセキュリティ能力を強化し、インシデントに対処するためのガイダンスを提供する

続いて「要求」については、上記の 4 つのテーマごとに詳しく記述されている。主な要求事項は、次のとおり。

（1）のガバナンスにおいては、脅威のリスク管理の枠組みを構築した上で、リスク管理の責任者を置くことを求めている。このほか、職員や学生が利用できる明確なリスク評価と報告の枠組みなどを要求している。

（2）のコミュニケーションでは、外国干渉を受ける危険性がある共同研究などに従事する職員や学生に対し、コミュニケーション計画や教育プログラム、研修などの実施を求めている。このほか、信頼できる国際的なパートナーと外国からの干渉に対抗する先進取組事例を共有したり、共有研究や交流の場を設けたりすることを提案している。また政府に対しても、大学側が外国干渉の事例や試みを特定できるように支援することを求めている。具体的に

は、外国干渉対策調整センターが、大学を支援するための連絡窓口を提供することを挙げている。

（3）のデューディリジェンスやリスク評価の項目では、外国干渉を受ける恐れがある職員や学生に対し、１年に１回などの割合で定期的な利害関係の申告（外国の所属先や関係先、財務責任者の特定など）を求めると同時に、カウンターパートに対するデューディリジェンスの実施を求めている。なお同ガイドラインには、付録として外国機関や外国政府との関係にからんで利益開示のための想定質問も紹介されている。それによると、たとえば申告すべき資金援助の種類には、資金援助プログラム名や援助の期間、受けた援助の種類などの記載を求めている。

また技術分野においては、豪州の防衛戦略物資リスト（DSGL）に含まれたり、国外への輸出や電子的な供給が規制されたりしていないかどうかもチェックするとしている。

さらに大学側に、外国からの干渉リスクを評価し、管理する際に、研究者や教職員が助言や支援を求めることができる明確な連絡窓口を備えることも求めている。

（4）のサイバーセキュリティの項目では、可能な限り脅威モデルなどの手法を用いることによってリスク軽減に努めたり、ベストプラクティスを徹底させたりすることなどを求めている。またサイバーセキュリティを組織全体の人的問題としてとらえ、サイバーセキュリティ戦略を構築したり実施したりすることも求めている。

2.3.3 資金配分機関等における取組

○資金配分機関

豪州の資金配分機関は豪州研究評議会（ARC）と国立保健医療研究評議会（NHMRC）の２つである。両者と豪州の大学の連合体である豪州大学協議会（UA）の３者が、大学・研究機関の研究者に対し研究公正の原則を示す豪州規範を策定した。また ARC と NHMRC が共同で組織する研究公正委員会（ARIC）が、個別の大学などの求めに応じて不正事案の妥当性を審査する仕組みになっている。ただし ARIC による審査の対象はあくまでも同プロセスにとどまり、不正調査・認定の結果に立ち入ることはない。

長く研究公正の分野においてその審査や是正の中心になってきた ARC と NHMRC だが、豪中関係が悪化し始めた 2018 年７月以降は、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、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。その際、研究を支える利害関係について完全な透明性をもって研究助成金の申請が行われるよう、政府の外国干渉調整室と連携を取り合っているのが特徴である。これは 2019 年にできた UFIT ガイドラインを補完するための措置でもあった。

この措置に伴って、ARC は「利益相反・機密保持ポリシー（Conflict of Interest and Confidentiality Policy）」の改定を重ねており、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るようになっている[152]。なお、協力する国家安全保障機関の中には、内務省直轄の 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。

ARC はまた、安全保障管理が必要な機微技術の識別にもたずさわっている。豪州では 2021 年 11 月に「重要技術のための青写真と行動計画」が発表された[153]。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。この文書には、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。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。

○グループオブ８（Go8）

豪州の上位８つの大学で構成する組織である[154]。Go8 を構成する大学は、国家安全保障にからむリスクを検知し対処するための複数のプログラムを実施している。副学長がリーダーシップを発揮して調整にあたっている。準拠しているのは、UFIT ガイドラインである。Go8 は、UFIT において重要な役割を担っている。

Go8 の具体的な対応策は、利益相反や不正防止にあたり明確なガイダンスを提示することにある。研究パートナーの身元調査を定期的に行い、潜在的なリスクを認識できるようにする。また安全保障貿易管理チェックを行うとされる。外国からの干渉を緩和するためのベストプラクティスを、大学ごとにまとめて公表している[155]。

その手法は、例えば豪州国立大学ではＡＩを活用した先駆的な取組を行っている。貿易管理の対象になる可能性があるすべての研究を自動的に特定するため、ＡＩを利用している。また Go8 の大学は、政府の国家安全保障機関と定期的に連絡を取り合い、積極的に指導を

[152] Conflict of Interest and Confidentiality Policy | Australian Research Council, <https://www.arc.gov.au/about-arc/program-policies/conflict-interest-and-confidentiality-policy>
[153] Action Plan for Critical Technologies | Department of Industry, Science and Resources, <https://www.industry.gov.au/publications/action-plan-critical-technologies>
[154] Group of Eight (go8.edu.au), <https://go8.edu.au/>
[155] Go8 measures to safeguard Australia's sensitive research, <https://go8.edu.au/wp-content/uploads/2021/03/Go8-Measures-to-Safeguard-Australias-Research.pdf>

受けている。

このほか Go8 のメンバーは、豪州サイバーセキュリティセンターなどサイバー部門の専門機関とその脅威に関する情報共有を行なっている。大学職員への定期的なサイバーセキュリティ研修を行うなどしている。

○豪州大学連合（UA）

UA は 2007 年に設立された豪州国内の大学が加盟する連合体[156]。UA は豪州の大学部門の最高機関として、高等教育や研究が豪州や世界にとって社会的、経済的、文化的に大きな価値があることを主張している。加盟大学を代表し高等教育に関する政策提言や分析、統計データ、メディアの論評などを提供している。また豪州の大学を代表して海外の大学・研究機関と連携する場合に調整にあたっている。２つの資金配分機関や Go8 などとともに、国家安全保障にかかわるあらゆる事柄について、外国干渉を排除したり緩和したりする措置に加わっている。

2.3.4 豪州国立大学（ANU）における取組

豪州には合わせて 43 の大学があるが、ここでは外国からの干渉にゆかりが深く先進的な取組でも知られる豪州国立大学（ANU）を取り上げる[157]。研究インテグリティに関する同大学の取組は、研究公正についてはかなりの分量を割いて詳しく説明しているものの、外国干渉セキュリティに関する対応については閲覧許可がないと開くことができないサイトが多数あって断片的にしかうかがい知ることができない。インターネットによる大学のサイト検索を通じて、引き出すことができた事項について紹介する。

公開されているものでは、まず豪州国立大学では外国干渉に対処するために、学内に外国干渉諮問委員会（FIAC）を設けている[158]。その設立目的は「外国からの干渉リスクの管理について、大学コミュニティに監視、助言、保障を提供するため」としている。

構成メンバーは、研究・イノベーション担当の副学長を委員長とし、副学長２人、学部長２人、情報セキュリティ責任者１人からなっている。同委員会は、同大学と海外との共同研究についての管理内容について、学内で定期的に報告しているほか、問題が生じれば副学長に勧告を行う権限をもっている。

諮問委員会が行っている主な具体的措置の内容は次のとおり。

（1）外国干渉に関する外部からの問い合わせに対し同大学の窓口になる
（2）同大学の活動に対する外国干渉の可能性に関する事項について、政策的な助言を行う
（3）同大学のコミュニティに対し、外国干渉に関する最新のアドバイスを提供する

156 Home – Universities Australia, <https://www.universitiesaustralia.edu.au/>
157 ANU <https://www.anu.edu.au/>
158 Foreign Interference Advisory Committee - ANU, <https://www.anu.edu.au/about/governance/committees/foreign-interference-advisory-committee>

（4）国際的な研究・教育協力に関する検討や助言を行う
（5）政府からの外国干渉に関する要請に対し、同大学としての台頭を監督・承認する

外国干渉諮問委員会のもとで実務を担うのは、研究コンプライアンスチームと呼ばれる学内の組織である[159]。同チームは、国防輸出管理、外国干渉、海外斡旋、研究のインテグリティに関する問題で、広く同大学の研究者にアドバイスと支援を提供している。また同チームは国防省に登録されていて、大学を代表して国防輸出管理（DEC）の関するすべての許可証を申請することができる。DEC は、軍事用とデュアルユースの製品・技術の双方の輸出と供給を規制している。

同チームの役割は、諮問委員会が日常的に行っている業務（外国からの干渉リスクの管理に関する評価、監視、助言、大学コミュニティへの保証の提供など）を遂行するための事務作業を行うことである。同委員会は、海外との共同研究に関して判断を下し、適切な場合に副学長に勧告を行う。

同大では、外国企業との共同研究については、正式なもの（法的拘束力のある研究契約、賞や資金の獲得、スタッフ・学生の交換、名誉職など）、非公式なもの（学生の指導やパートナーとしての助成金申請など）を問わず、外国干渉諮問委員会に届け出る必要がある。提出は「e-フォーム」で行うとしている。

同大学はこうした厳格な外国干渉セキュリティに対する措置を取る一方、学問の自由を守る立場から、そもそも「外国干渉とは何を意味するのか」という視点から、重要な指摘をしている。

同大学は学内のインターネットサイトに「外国からの影響（influence）」と「外国からの干渉（interference）」の違いに注意喚起を促す同大研究者によるレポートを掲載している[160]。執筆は、ANU のキャサリン・マリンステッド国家安全保障カレッジ（National Security College: NSC）公共政策顧問によるもの。それによると、「豪州の対応は外国からの影響力のうち、最も悪質な形態である外国干渉を犯罪とみなし、その抑止に重点を置いてきた。しかし許容される外国からの影響と不法な外国からの干渉の間にはグレーゾーンが生まれつつある」として、行き過ぎた政府の外国干渉排除の動きにくぎを刺している。執筆者のマリンステッド NSC 公共政策顧問は「干渉とまではいかないが、豪主の価値や利益、主権と矛盾する外国からの影響に、豪州としてどのように対処すべきか」と問いかけている。

マンステッド氏は、行き過ぎた外国干渉の排除を防ぐ手立てとして、
（1）積極的な透明性の確保
（2）国にこだわらず発信国の政治的文脈に細心の注意を払う

159 Research Compliance - Staff Services - ANU, <https://services.anu.edu.au/business-units/research-services-office-of-research-and-innovation-services/research-compliance>
160 Navigating the Space Between Foreign Influence and Foreign Interference | National Security College (anu.edu.au) <https://nsc.crawford.anu.edu.au/department-news/18457/navigating-space-between-foreign-influence-and-foreign-interference>

（3）民主的な政治的権利と社会的結束を優先させる
（4）地方分権的な対応―強化する――の４つの原則を提示している。
さらにこれらの原則を運用するために必要な政策オプションとして、
（a）独立した主権コミッショナーの設置
（b）外国からの影響リスクに関する専用のオンラインポータルの作成
（c）外国干渉の前兆を補足するための立法措置
（d）強固で独立したメディアの支援―などを挙げている。

このほか同大学のサイトには、そもそも外国干渉とは何かという定義があいまいなため、メディア報道による中国共産党との関わりの指摘が先行している現在の風潮に対し、疑問を投げかけるような中国系オーストラリア人学生のエッセイが掲載されている[161]。それによると、単に中国共産党とのつながりがある人物に会ったり、中国関係団体が主催するイベントに参加したりしただけで外国干渉への関与と結び付けられてしまう危険を指摘している。

2.3.5 最近の動向

○連邦議会による国家安全保障リスク調査

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2022年３月、大学・研究機関に影響を与える国家安全保障リスクに関する調査（The Inquiry into national security risks affecting the Australian higher education and research sector、「豪州の高等教育及び研究部門に影響を与える国家安全保障上のリスクに関する調査」）を発表し、その中で豪州の大学・研究機関で起きた数々の国家安全保障上のリスク事例を紹介するとともに、外国干渉に対処するための27の勧告を行った[162]。

勧告の一部を紹介すると、例えば、UFITが職員や学生を対象とした国家安全保障問題に関する関連研修の導入、維持、発展を支援するよう勧告する（勧告３）、ASIOが議会への年次報告書において、オーストラリアの高等教育・研究部門に対する脅威について、より広範な脅威の評価の一環として定期的に情報を提供するよう勧告する（勧告10）といった具合である。

同調査は、2020年当時、内務大臣だったピーター・ダットン氏によって開始されたもので、高等教育及び研究部門に存在するすべての国家安全保障上のリスクについて調査が行われた。

---

161 foreign interference reporting - RegNet - ANU, <https://regnet.anu.edu.au/tags/foreign-interference-reporting>

162 Inquiry into national security risks affecting the Australian higher education and research sector – Parliament of Australia (aph.gov.au), <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Report>

その結果、民主化を支持する中国人や教職員が他の学生から本国に報告すると脅迫された事例や、スパイ活動、外国の機関との協力による知的財産の窃取などがあったことが判明した。2019～20 年に大学に対するサイバー攻撃が 100 件以上あり、新型コロナウイルスに絡むワクチンのデータを盗もうとする試みもあったという。生々しい事例では、2007 年以降、約 300 人の中国人科学者が人材派遣プログラムのもとで豪州に派遣され、レーダーやスーパーコンピュータ、暗号技術、ドローン群などの軍事関連技術を研究していた事例なども盛り込まれている。

その中で PJCIS は、豪州の大学・研究機関が UFIT を通じて国家安全保障上のリスクに関して、積極的に透明性の維持を行うことや、UFIT が一連の活動を監督し進捗状況について連邦政府に報告することを推奨している。また中国政府が資金を提供して運営されている孔子学院について、学問の自由と学生の福祉に関するリスクを認識し大学と外務大臣にリスク軽減のための措置を講ずるように求めている。

○中国の軍事関連大学をめぐる追跡調査（トラッカー）

連携するパートナーへのデューディリジェンス支援のため、豪州戦略政策研究所（ASPI）の国際サイバーポリシーセンターは 2019 年、中国の軍事関連の大学に関する追跡調査サイト（The China Defense Universities Tracker）を発表した[163]。中国の関係機関の危険度を４段階で示している。同サイトによると、中国では「軍民融合」を掲げ、民間の大学が軍隊や安全保障機関との連携を構築しているとともに、軍事力を向上させるために民間部門の研究を活用する政策が敷かれている。

同サイトには、全体で 174 の大学・研究機関が掲載されている。同サイトの分析によると、このうち危険度が「非常に高い」グループと「高い」グループ（人民解放軍の機関、安全保障・情報機関関連など）はそれぞれ 94 件、23 件あって、「中間」グループは 41 件、「低い」グループは 17 件となっている[164]。

同追跡サイトの調査では、「多くの中国の大学が軍事研究、軍事科学者の育成、軍民協力、軍事産業コングロマリットとの協力に従事し、機密研究に関与していることが判明した」と記述。「少なくとも 15 の民間大学が、サイバー攻撃や違法輸出、スパイ行為に関与していることが判明した」としている。このため「中国の大学との連携は、人民解放軍や治安当局によって監視、人権侵害、軍事目的のために利用される危険が高まっている」と指摘している。

こうした現状を踏まえた上で、大学に対する対応策としては、透明性を促進し、倫理、価値、安全保障上の利益の遵守を評価する独立した研究インテグリティ・オフィスを設置し、大学内から政治的影響を受けないよう管理上区別された組織として機能させることなどを推奨している。また政府に対する対応策としては、国立の「研究保全局」（仮称）を設置して、外国干渉に関する法令を整備・施行するとともに、中国防衛大学追跡調査を利用してビ

163 The China Defence Universities Tracker | Australian Strategic Policy Institute | ASPI, <https://www.aspi.org.au/report/china-defence-universities-tracker>
164 Home – Chinese Defence Universities Tracker — ASPI, <https://unitracker.aspi.org.au/>

ザ申請者の審査を改善したり、研究費支給の判断に役立てたりするべきだと推奨している。

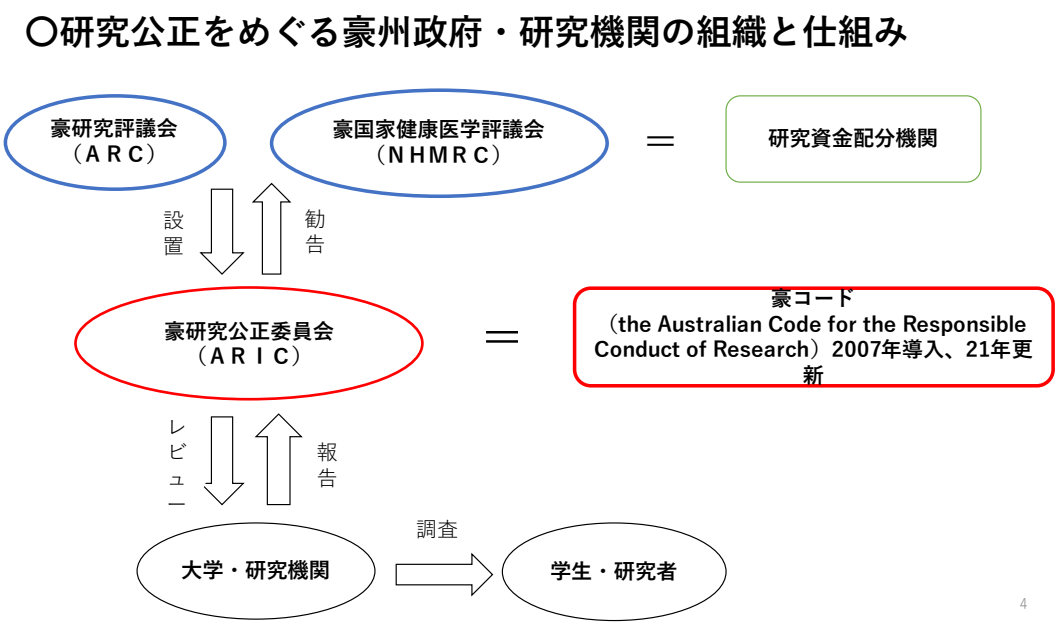


図 2-6：研究公正をめぐる豪州政府・研究機関の組織と仕組み

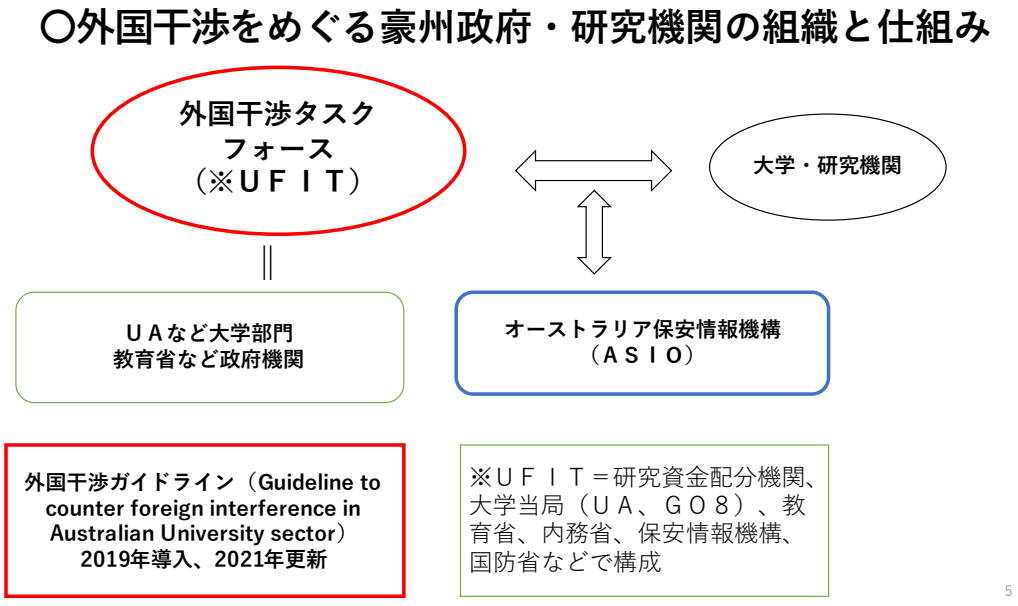


図 2-7：外国干渉をめぐる豪州政府・研究機関の組織と仕組み

2.4 カナダ

2.4.1 全般的状況

カナダの懸念国、特に中国への警戒感の背景には 2010 年代半ばに発覚した研究機関に対する中国政府が関与したサイバー攻撃事案があるとされる[165]。近年は COVID-19 パンデミックに乗じた研究セキュリティ上のリスクに焦点が当てられている[166]。

カナダの 3 つの主要な連邦研究資金配分機関（FA）は以下のとおり。

- カナダ保健研究機構（Canadian Institutes of Health Research：CIHR）
- カナダ自然科学・工学研究会議（Natural Sciences and Engineering Research Council of Canada：NSERC）
- 社会・人文科学研究会議（Social Sciences and Humanities Research Council of Canada：SSHRC）

上記 3 機関は 2016 年に研究インテグリティに関する共通規範の「Tri-Agency Framework：Responsible Conduct of Research（RCR）」（RCR フレームワーク）を定めている。このフレームワークは FFP（捏造・改ざん・盗用）等の研究不正行為や利益相反行為への注意喚起を行い、発覚時の処理手順及び罰則等を定めている。フレームワークは 2021 年に改定されたが、現状では「研究セキュリティ」や「外国影響」に焦点を当てた規定は盛り込まれていない[167][168]。

カナダ政府の研究セキュリティに関する情報提供サイトに、カナダ公共安全省の「研究セキュリティ情報の更新（Research Security Information Update）[169]」がある。

カナダ政府は研究セキュリティを「外国の脅威者に地政学的、経済的、安全保障上の利益をもたらす一方、カナダに不利益をもたらす可能性のある知識、技術、データを保護するための措置を指す。対象となる資産は、大量破壊兵器計画（化学、生物、放射線、核など）への応用可能な技術から、人工知能、量子コンピュータ、バイオ・ナノテクノロジーなどのデュアルユース技術（民生と軍事の両方に応用できる技術）、研究に用いられる知的財産や機密情報などである（Research security refers to the measures that protect knowledge, technologies, and data that could assist in the advancement of a foreign threat actor's

---

165 CRDS 報告書「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―」(2022).p3

166 カナダ政府ウェブサイト" Joint CSE and CSIS Statement – May 14, 2020"<https://www.canada.ca/en/security-intelligence-service/news/2020/05/joint-cse-and-csis-statement.html>

167 カナダ政府ウェブサイト" Tri-Agency Framework: Responsible Conduct of Research (2016)"<https://rcr.ethics.gc.ca/eng/framework-cadre.html>

168 カナダ政府ウェブサイト" Tri-Agency Framework: Responsible Conduct of Research (2021)"https://rcr.ethics.gc.ca/eng/framework-cadre-2021.html

169 カナダ公共安全省ウェブサイト" Research Security Information Update"< https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx >

geopolitical, economic, and security interests to the detriment of Canada's. The target assets can vary from applications in weapons of mass destruction programs (i.e., chemical, biological, radiological, and nuclear) to dual-use technologies (i.e., technologies with both civilian and military applications), such as artificial intelligence, quantum computing, and bio- and nanotechnology, to intellectual property and confidential information used for research)」と定義している。

研究セキュリティの内容を定義し、WMD や量子技術など具体的な分野を挙げる点が特徴的である。

研究セキュリティ上特に考慮が必要な機微分野については、後述のカナダ政府・大学共同ワーキンググループが作成した"National Security Guidelines for Research Partnerships"（国際研究協力に対する国家安全保障ガイドライン）に記述がある[170]。このガイドラインによると外国影響に対し脆弱な研究分野には以下のものが含まれるが、これらに限定されるものではない。

① 航空宇宙
② 人工知能
③ バイオテクノロジー
④ エネルギー生成、貯蔵、送電
⑤ ニューロテクノロジーとヒューマンマシンインテグレーション
⑥ 次世代コンピューティングとデジタルインフラ
⑦ 位置・ナビゲーション・タイミング
⑧ ロボティクスと自律システム
⑨ 重要鉱物及び重要鉱物サプライチェーンに関連する研究（詳しくは、カナダ政府の重要鉱物リストに掲載）
⑩ 重要インフラに焦点を当てた研究パートナーシップ
  - ✓ 重要インフラとは、カナダ人の健康、安全、セキュリティ、又は経済的福利、及び政府の効果的な機能にとって不可欠なプロセス、システム、施設、技術、ネットワーク、資産、サービスを指す。（重要インフラの詳細については、重要インフラに関する国家戦略及び重要インフラに関する行動計画に掲載）。
⑪ 利用することでカナダの国家安全保障に害を及ぼす可能性のある機密個人データへのアクセスの可能性を伴う研究パートナーシップ（以下に限定されない）
  - ✓ 個人を特定できる健康状態又は遺伝子に関するデータ（例：健康状態又は遺伝子検査結果）

[170] 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 >

- ✓ バイオメトリクス（例：指紋）
- ✓ 財務（例：支出や負債を含む機密口座情報）
- ✓ 通信（例：私的な通信）
- ✓ ジオロケーション
- ✓ 軍や情報機関のメンバーを含む政府関係者に関する個人データ

2.4.2 カナダ政府の取組み

カナダ政府は研究セキュリティの強化に関する取組について下表に見るような時系列で措置を講じてきた。

表 2-40：カナダ政府の研究セキュリティの強化に関する取組

日付	内容
2021 年 7 月 12 日	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。
2021 年 3 月 24 日	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。
2021 年 2 月 9 日	カナダ安全保障情報局（CSIS）長官が国際ガバナンス・イノベーションセンターで行った講演で、経済のほぼすべての部門において、カナダ企業が敵対的な外国人行為者の標的とされていることを概説した。また、「今日、我々の敵は、国内の小さな新興企業、企業の役員室、あるいは大学の研究室にあるコンピューターシステム上に保有される知的財産や先端研究に、より焦点を当てている」と指摘した。
2021 年 1 月 15 日	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。
2020 年 11 月 16 日	カナダ・サイバーセキュリティ・センターは、「2020 年の国家サイバー脅威評価（National Cyber Threat Assessment for 2020）」を発表した。
2020 年 9 月 17 日	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。研究機関は、研究環境とデータを保護する方法、一般的なサイバーセキュリティの脅威を組織

日付	内容
	がどのように理解すべきか、いくつかの基本的なセキュリティ対策を実施する方法に関する情報を得るために、この出版物を確認することが推奨される。
2020 年 9 月 14 日	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「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 14 日	イノベーション・科学・経済開発相、公安相、保健相が、カナダの研究コミュニティの全メンバーに対し、COVID-19 ワクチンと治療薬に関連するすべての研究、技術、開発を保護するために特別な予防措置を講じるよう促す声明を発表。
2020 年 5 月 14 日	カナダ通信保安局（CSE）と CSIS は、カナダの研究コミュニティに対し、パンデミック研究に関連するデータと技術が、国家的支援を受けた行為者にとって魅力的な標的になっていることを警告する共同声明を発表。
2020 年 4 月	COVID-19 ワクチン開発に関連して、CSIS がカナダの大学を含むバイオ製薬セクターへの脅威ブリーフィングを開始。
2019 年	公共安全省が「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（Building Security Awareness in the Academic Community）」文書を発表。

出典：カナダ公共安全省ウェブサイトから筆者作成

<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx>

2.4.3 カナダにおけるアクター

・省庁

カナダにおける研究セキュリティの取組に関する主要なアクターとして以下がある。なお、カナダでは教育は地方分権であり、中央政府は「カナダ政府・大学ワーキンググループ」に協力を要請し、参考となるガイドラインを作成するにとどまる[171]。

[171] カナダの教育は完全な地方自治で中央政府に教育省はなく、高等教育を含め州政府の教育省によって管轄されている。またほとんどの大学は州立である。カナダの 3 つの準州（ユーコン準州、ノースウエスト準州、ヌナブト準州）は、州ほどの憲法上の地位がなく、多くの分野で連邦政府による直接的な統制を受けている。しかし、教育に関しては、連邦政府はその責任を準州政府に委任しており、準州政府は州と協力して中等教育プログラムを提供している。（CICIC ウェブサイト" Ministries/departments responsible for education in Canada"<https://www.cicic.ca/1301/ministries_departments_responsible_for_education_in_canada.canada>）

連邦政府の 3 つの資金配分機関（CIHR、NSERC、SSHRC）に対しては、所管するイノベーション・科学・経済開発省、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。ただし輸出管理関連法規の「規制品目プログラム（Controlled Goods Program）[172]」や医療倫理規制法令[173]などを除き、研究セキュリティ・研究インテグリティに関する包括的な法規制は存在しない。

外国影響やスパイからの研究コミュニティの保護は、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）が取り締まりを所管する。

【機微な研究分野に関する法規制】

研究分野の中には、軍事力の向上と明らかに関連するものがあり（例えば、核、化学、生物、放射線、宇宙利用など）、カナダでは、これらの分野に関して研究の実施や得られた知識の輸出の際に従わなければならない以下の法令が存在する[174]。

- 通常兵器やデュアルユース品に関連する分野の研究は、輸出入許可法（Export and Import Permits Act：EIPA[175]）の対象となる可能性があり、カナダ国外の研究者への技術移転の前に許可が必要となる場合がある。
- ミサイル・ロケット技術、宇宙技術、化学・生物兵器・薬剤に関する研究も、EIPA の規制対象となる可能性がある。
- 原子力プログラムに関わる、又は原子力プログラムに適用される分野の研究については、EIPA 及び核不拡散輸出入管理規則（Nuclear Non-proliferation Import and Export Control Regulations[176]）の対象となる。
- 防衛生産法（Defence Production Act[177]）の別表（規制品目リスト）に記載されている商品・技術に関連する分野の研究は特に注意が必要であり、上記の規制品目プログラムの対象となる。
- 地域管理リスト（Area Control List[178]）（EIPA に基づく規制）に掲載されている国の研究機関との共同研究は、研究内容にかかわらず、カナダ総務省（GAC）の事前承認

[172] Defence Production Act の既製品目リスト掲載の物品・技術に関する規制
[173] Food and Drug Regulations (FDR) under the Food and Drugs Act (Canada)など
[174] カナダ政府ウェブサイト" Annex A- Sensitive research areas"< https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/national-security-guidelines-research-partnerships >
[175] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/acts/e-19/>
[176] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/regulations/sor-2000-210/index.html>
[177] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/acts/D-1/index.html>
[178] カナダ政府ウェブサイト"Justice Laws Website"<https://laws-lois.justice.gc.ca/eng/Regulations/SOR-81-543/index.html>

が必要となる。

- また、特別経済対策法（Special Economic Measures Act[179]）や国連法（UN Act[180]）に基づく制裁を受けた企業との共同研究についても、GAC の事前承認が必要となる場合がある。

ただし、潜在的な軍事、安全保障、諜報の用途が明確でなく周知されていない、あるいは国際的な武器・輸出規制体制がまだ合意に至っていないため、上記の規制が適用されないデュアルユース技術・新興技術についての扱いが問題であり続けている。

・カナダ政府・大学ワーキンググループ

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、オープンで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、Safeguarding Your Research ポータル[181]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結果を広めるための重要なチャネルとなっている。

ワーキンググループには、カナダ政府、資金配分機関・連邦研究機関、大学関係者、大学団体から、次のようなメンバーが参加している。

- カナダ国際関係省（外務省）（Global Affairs Canada）
- カナダイノベーション・科学・経済開発省（Innovation, Science and Economic Development Canada）
- カナダ公共安全省（Public Safety Canada: PS）
- カナダ安全保障情報局（Canadian Security Intelligence Service: CSIS）
- 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・イノベーション財団（Canada Foundation for Innovation: CFI）
- カナダ国家研究評議会（National Research Council Canada）
- 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）
- カナダ研究大学 U15 グループ（U15 Group of Canadian Research Universities）
- カナダ大学連盟（Universities Canada）

[179] カナダ政府ウェブサイト“Justice Laws Website” <https://laws-lois.justice.gc.ca/eng/acts/s-14.5/index.html>

[180] カナダ政府ウェブサイト“Justice Laws Website” <https://laws-lois.justice.gc.ca/eng/acts/u-2/index.html>

[181] 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>

➢ 各大学研究担当副学長

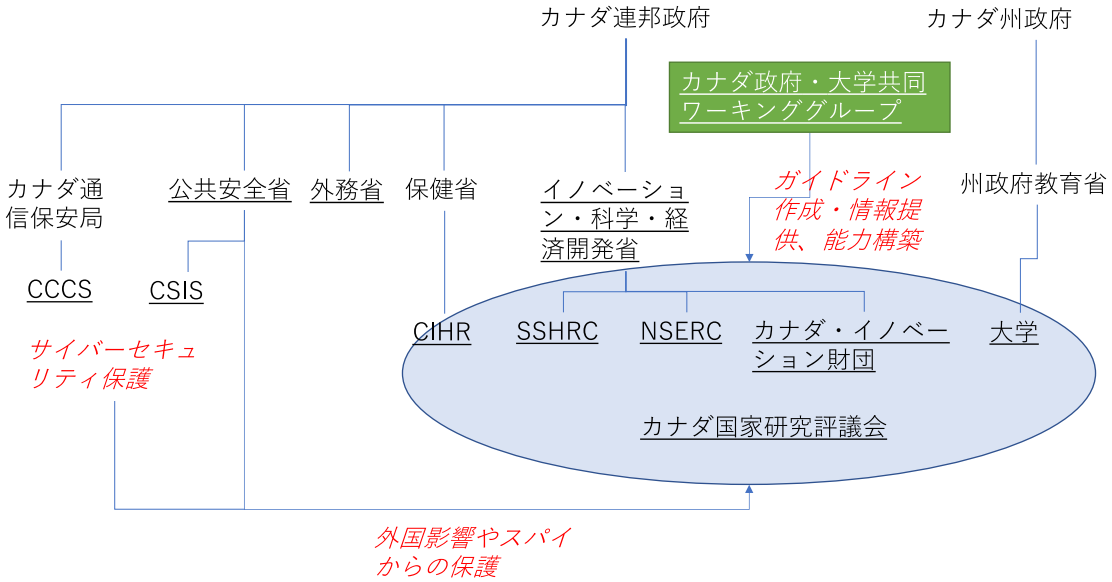


図 2-8：カナダにおける研究セキュリティに関する主要なアクター

2.4.4 規制側・被規制側の主要アクターの研究セキュリティに関する認識

・公共安全省による認識

カナダ公共安全省の年次報告書[182]によれば、同省は外国政府による敵対的な影響力の行使全般を注視している。同省は研究安全保障を脅かす外国による干渉活動を国家主体による敵対的活動（hostile activities by state actors：HASA）として捉え、経済安全保障及び国家安全保障に強く関連するテーマとして研究セキュリティ上の問題を認識し対応しようとしていることがうかがわれる。以下では同報告書中の関連する項目を引用する。

【国家主体による敵対的活動】

国家主体による敵対的活動（HASA）には、外国の国家又はその代理人がカナダの国益と価値を損なおうとするあらゆる行為が含まれる。敵対的活動は、多くの場合、あからさまな直接的軍事攻撃には至らないものの、欺瞞的、脅迫的、腐敗的、隠密的、又は違法な性質を持つ行動を伴う。HASA の脅威は、COVID-19 によって形成されたグローバル環境の結果として悪化し、外国の脅威行為者に彼らの目的を推進する機会を与えている。HASA は冷戦以来見られなかったレベルに達し、現在、カナダの国家安全保障にとって最大の戦略的脅

[182] カナダ公共安全省” Departmental Results Report 2021-22”
<https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-rslts-rprt-2021-22/index-en.aspx#s311>

威の一つとなっている。それは、カナダの政治システムのインテグリティ、民主的制度、社会的結束、学問の自由、経済、長期的繁栄を標的にしているからである[183]。

【国家安全保障に対する経済ベースの脅威】

カナダ人は、重要な新興技術分野の最先端に身を置き、それが経済成長と発展の重要な原動力となっている。これはカナダに新たな機会をもたらす一方で、国家安全保障上の新たな、そして潜在的に深刻な脆弱性をも生じさせた。特定の敵対勢力は、カナダ経済の重要な分野を利用して、自国の戦略的な軍事、情報、安全保障、経済的利益を高めようとしている。このような活動には、以下がある。

- カナダの国家安全保障にとって重要な部門や産業への外国投資
- カナダの国家安全保障にとって重要な商品、技術、ノウハウの輸出
- 機密性の高い技術や知的財産（IP）の開発のために、学術研究機関と、敵対的な外国人によって支配された、あるいはそれに関係する団体との間で結ばれるパートナーシップ

【研究セキュリティ】

カナダの国家安全保障コミュニティは、国家安全保障や経済的意義を持つ最先端の研究、企業秘密、知的財産のスパイ行為や盗難がもたらす脅威に取り組み続けている。公共安全省は、カナダの研究機関のセキュリティ態勢を強化するための多くのイニシアティブに関与した。2016 年以降、公共安全省はワークショップ、ツール、リソースを提供する Safeguarding Science イニシアティブを通じて、第一線の研究者や学術コミュニティと直接関わることで、研究セキュリティ上の脅威に対する意識を高めてきた。2021-22 年、Safeguarding Science チームは、関係者向けのオンラインワークショップの数を 33%増やし、カナダ全土で合計 1487 人が参加した。

・資金配分機関の認識

理工系の公的研究・資金配分機関であり、研究セキュリティ上のリスクにさらされやすい NSERC の研究セキュリティに関する現状認識は以下のとおりである（戦略文書"NSER 2030"[184]より）。

- 科学と工学のスピードと複雑さが増すにつれ、カナダの世界レベルの研究は、盗難、スパイ行為、知的財産の不正移転の標的になっている。NSERC は政策立案者や研究者とともに、世界の力学が変化する中で研究セキュリティを実践し、研究の中核

[183] Public Safety Canada. Public Safety Canada 2021 Transition Book - Issues Book: National Security.
<https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/trnstn-bndrs/20220223-2/006/index-en.aspx>
[184] NSERC ウェブサイト "NSERC 2030: Discovery. Innovation. Inclusion."
< https://www.nserc-crsng.gc.ca/NSERC-CRSNG/NSERC2030-CRSNG2030/report-rapport/index_eng.asp >

的価値であるインテグリティ、公平さ、信頼、説明責任、学問の自由を堅持しながら、研究のエコシステムを可能な限りオープンで必要な限り安全なものにするよう努めている。

- NSERC は、私たちの価値観に合致し、カナダの研究エコシステムに大きな付加価値をもたらす世界中の研究助成機関とパートナーシップを構築する。
- NSERC は、カナダの最も有望な研究者や研究機関が、国際的な同業者との強力なパートナーシップを構築することを支援する。
- NSERC は、カナダ研究調整委員会（Canada Research Coordinating Committee：CRCC）のリーダーシップのもと、他の機関や組織とともに、国際協力への「チーム・カナダ（３機関・CFI・連邦科学機関)」アプローチにおける熱意あるパートナーとなる。
- NSERC は、連邦政府のパートナー、学術機関、研究組織、個々の研究者とともに、カナダの知識、データ、知的財産を外国の脅威から守り、カナダの経済的繁栄、国家安全保障、研究事業の健全性を確保する。

NSERC が 2015 年に発表した前回の戦略プランの”NSERC 2020”では、グローバル化の方向性が強調されており(Go Global)、研究セキュリティに関する記述は見られず、むしろ国際共同研究の推進や留学生の受け入れ拡大が研究活動に関する国際社会でのカナダのプレゼンスを高めるために必須との認識が示されていた[185]。研究セキュリティや国家安全保障を強調する現在の戦略はこうした立場からの方向転換であると評価できる。

・カナダ政府・大学ワーキンググループの認識

同ワーキンググループのウェブサイト[186]によると、以下のように研究の国際化・オープン化のもたらす恩恵を強調しつつも、研究セキュリティ上のリスクの高まりを懸念している様子がうかがえる。

- 強い経済を築き、すべてのカナダ人の生活を向上させるためには、オープンで協力的な研究環境が必要である。カナダはオープンで協力的な研究と科学に取り組んでいる。教員、学生、知識の交流は、カナダが革新的な知識集約型社会・経済となるために必要な連携と能力の構築に寄与する。
- ただし、カナダ政府と大学は、カナダ国民が研究への多大な投資から引き続き利益を得られるようにすることは、共通の責任であると認識している。このため、大学、政府省庁、連邦助成審議会、国家安全保障機関は、継続的な関与活動の一環として定期的に連絡を取り合い、研究の安全性を確保するために協力している。

[185] NSERC ウェブサイト “NSERC 2020”< https://www.nserc-crsng.gc.ca/nserc-crsng/nserc2020-crsng2020/index_eng.asp>
[186] 同上

2.4.5 リスクアセスメント

「国際研究協力に対する国家安全保障ガイドライン」で説明されているように、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[187]。以下ではNSERCにおけるリスクアセスメントの流れを参考に具体的な運用を見ていきたい。

【基本的な判断枠組み】

研究者は、研究パートナーシップの申請書を NSERC のアライアンス助成金プログラムに提出する際に、リスクアセスメントを完了しなければならない。

NSERC が高リスクと判断したパートナーシップ助成金申請については、必要に応じて国家安全保障関連省庁・機関や研究者コミュニティのメンバーが関与し、国家安全保障審査を受けることになる。

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。

【プロセスの概要】

1.研究者

- 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。

2.研究機関

- 機関は、リスク質問票のレビューと検証を行う。
- 研究機関は、特定されたリスクに効果的に対処するために、研究者がリスク軽減計画を策定することを支援する。
- リスク調査票とリスク軽減計画（該当する場合）は、該当する助成金申請書に添付して提出する。

3.助成機関[188]

- 助成機関は、助成の評価基準に記載され、確立されたピアレビュープロセスに従って、受領したすべての研究パートナーシップ提案の科学的メリットの評価を実施する。
- 助成機関は、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

187 カナダ政府ウェブサイト” The National Security Guidelines for Research Partnerships' Risk Assessment Form” <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>

188 Science.gc.ca website. “Risk Assessment Review Process” <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/risk-assessment-review-process >

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、提案された研究プロジェクトの国家安全保障評価をどの安全保障機関が主導するのかを決定する（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)。主導する機関は、それぞれの権限と任務の下、評価を実施し、カナダ公共安全省に結果を知らせる。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。
- 助成機関は、科学的メリット評価の結果とともに、国家安全保障評価とカナダ公共安全省から受けた助言を考慮し、各申請に対する資金提供を最終決定する。

2.4.6 地域ごとの懸念への対処

カナダは広大な国土を有し、産業構造や天然資源の分布にも地域ごとに特徴がある。このような特性に鑑み、カナダで科学研究を行う際に直面する可能性のある外国干渉を含む特定のリスクについて詳しく知りたい場合、以下のように、カナダ安全保障情報局（CSIS）が作成した「Protect Your Research（研究を保護する)」から地域別（ブリティッシュコロンビア、アルバータ、サスカチュワン、マニトバ、オンタリオ、ケベック、ニューファンドランド・ラブラドール、プリンスエドワード島、ニューブランズウィック、ノバスコシア、ユーコン、ノースウェストテリトリーズ、ヌナブトの各州・準州）ファクトシートの概要を参照することができる[189]。

例えばブリティッシュコロンビア州では以下のような外国脅威（狙われやすい分野、具体的な標的、想定される手法）が挙げられている。

表 2-41：ブリティッシュコロンビア州における外国脅威の例

分野	• テクノロジー • バイオ医薬品 • 健康 • 輸送（航空宇宙、鉄道、環境対応車、海事機器、サプライチェーン） • アカデミア • エネルギー • マニュファクチャリング

[189] カナダ政府ウェブサイト” Protect your research”<https://science.gc.ca/site/science/en/safeguarding-your-research/general-information-research-security/who-are-you-risk/protect-your-research-regional-factsheets >

標的	• STEM 分野の先端研究・機器 • 知的財産権 • 重要インフラ資産 • 個人を特定できる情報（例：財務情報、健康情報など） • 政府情報 • 通信機能 より具体的な例としては、設計図、試験結果、製造又はマーケティング計画、独自の規格方式又はプロセス、従業員情報、ベンダー及び供給者情報、ソフトウェア、投資データ、企業戦略、アクセスプロトコル、及び特許などが挙げられる。
手法	• サイバー・エスピオネージ（スパイ） • ヒューマン・エスピオネージ • 技術・ノウハウの盗用と不正移転 • カナダの機密データの取得と活用 • 重要インフラへの外国からのアクセスとコントロール • インサイダー脅威 • 敵対的な海外投資 • リバースエンジニアリング • 破壊工作 • 搾取的ライセンス契約 • エリシテーション[190]

2.4.7 大学での取組み

(1) マギル大学[191]

マギル大学（McGill University）では、学術研究及び国際協力において、長年にわたりオープンな姿勢を貫いてきた。しかし、現在は研究セキュリティを確保し、外国からの干渉に対する保護を実施することは同様に重要な大学の責任であると認識されている[192]。留学生や客員教員、民間企業の協力者、外国政府の代表者、非営利団体、活動家、営利目的の競争相手など、自分たちの目的や利益のためにマギル大学の研究や研究者にアクセスしよう

[190] お世辞を言ったり、関心を示したり、誘導尋問をしたり、相互の利害を主張したり、無知を装ったりして、情報を引き出そうとすること。これらのテクニックは、業務とプライベートの両方の場面で使われることがある。

[191] マギル大学ウェブサイト”Foreign Interference” <https://www.mcgill.ca/research/about/foreign-interference >

[192] マギル大学では「外国からの干渉（Foreign Interference）」について「外国政府やその他の団体による、不当な影響力を行使しようとする、あるいは学術の中核的価値を侵害するような行為や活動を指す。このような干渉には、サイバーセキュリティ攻撃や、知的財産やアイデア財産に関連する情報収集活動が含まれる場合がある」と定義している。

とする人々が現れる可能性があり、コントラクター、職員、学生も含め、研究チームや研究機関の内部にいる人々は、研究やイノベーションに不適切にアクセスしたり、盗んだりするように、他者から支援や圧力を受ける可能性がある。

こうした問題意識から、マギル大学では 2020 年に外国干渉ワーキンググループ（McGill Foreign Interference Working Group）を設立し、同グループが大学全体の取組を指導している。同グループは研究イノベーション担当の副学長クラスなど 12 名のメンバーで構成されている。同グループの目的は、マギル大学の研究者が自らの研究、知的財産、知識開発を保護するために必要な教育・支援と、外国からの干渉に対する保護を実践することである。外国からの干渉を監視するため同グループは定期的に開催され、国家安全保障局との活発な連携が行われている。マギル大学は、さらなる調査が必要と思われる研究セキュリティ上の懸案事項が生じた場合、同グループに意見を求める。

マギル大学が整備する具体的な規定類としては、

- MOU の提案、キャンパス訪問、国際交流事業に関するガイドライン
- サイバーセキュリティに関するガイドライン
- 利益相反報告に関する規制
- 研究データ管理規定
- 研究提携、データ保護、海外からの訪問者に関するガイドライン（現在作成中）

がある。

カナダ公共安全省は、2021 年 5 月にマギル大学の科学者・学術者向けに開催される「Safeguarding Science Against Foreign Interference Workshop」を開催し外国干渉ワーキンググループもこれに協力した。ワークショップでは、円卓会議方式の質疑応答が行われ、兵器拡散リスク（化学、生物、放射線、核拡散、デュアルユース技術拡散のリスク）、サイバーセキュリティ、知的財産の盗難、その他のセキュリティに配慮した研究組織を維持するためのベストプラクティスに関する情報が提供された。また、カナダの機関、研究者、学術関係者が直面している特定のリスクを認識し緩和するのに役立つツールも提供された。

外国干渉ワーキンググループが推奨する、マギル大学関係者が参照すべき政府等のガイドラインや資料として以下が挙げられている。

- The Research Security Information Update (en anglais) <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-en.aspx>
- Le point sur la sécurité de la recherche (en français) <https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2021-rsi-psr-ma/index-fr.aspx>
- Mitigating economic and/or geopolitical risks in sensitive research projects (U15/Universities Canada) <https://science.gc.ca/site/science/en>

- Travel security guide for university researchers and staff (U15/Universities Canada) <https://science.gc.ca/site/science/en>
- Safeguarding Your Research, Government of Canada Portal <https://science.gc.ca/site/science/en/safeguarding-your-research>
- Actions Taken by Universities to Address Growing Concerns about Security Threats and Undue Foreign Influence on Campus (Association of American Universities/Association of Public and Land-grant Universities) <https://www.aau.edu/sites/default/files/Blind-Links/Effective-Science-Security-Practices.pdf>
- Guidelines to counter foreign interference in the Australian university sector released (Australian Government) <https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector>
- Canadian Security Intelligence Service (CSIS) Public Report 2020 <https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020-public-report.html>
- Foreign Interference and You (CSIS) <https://www.mcgill.ca/research/files/research/aose_foreigninterferencehandout_-_digital.pdf>
- L'ingérence étrangère et vous (SCRS) <https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210722/015/index-fr.aspx
- Guidelines on the National Security Review of Investments <https://ised-isde.canada.ca/site/investment-canada-act/en/guidelines/guidelines-national-security-review-investments>

(2) トロント大学[193]

トロント大学（University of Toronto）では 2021 年 8 月 30 日より、国際的なパートナーシップに携わる教員は、「研究パートナーシップ・セキュリティ情報文書（Research Partnership Security Information Document）」に必要事項を記入するよう求められている。これは、カナダ政府による研究セキュリティの重視政策に沿ったもので、カナダ政府・大学ワーキンググループによる提言に対応したものある。

トロント大学が外国干渉に関連して特に整備したガイドラインや規定としては以下がある。

193 トロント大学ウェブサイト"Safeguarding Your Research"< https://global.utoronto.ca/safeguarding-your-research/>

① 「国際的な研究パートナーシップの構築：原則とアプローチ（Engaging in International Research Partnerships: Principles and Approaches）[194]」：トロント大学では、教員や部局が国際的なパートナーシップを締結する際に考慮すべき一連の原則を策定した。教員が国際的なパートナーシップに関与する前にこれらを確認し、生産的で安全なパートナーシップを締結することが期待される、としている。

② 「国際的パートナーシップのための研究パートナーシップ・セキュリティ情報文書（Research Partnership Security Information Document for International Partnerships）[195]」：特定のプロジェクトを進める前に、PI（研究責任者）が「国際パートナー」と関わることの適切性と潜在的リスクを評価するためのツールである。国際パートナーとは、トロント大学と研究協力（大学院での研修や起業の機会も含む）を行っている、カナダ国外にある団体（学術団体、企業、政府、非営利団体など）と定義されている。法人の場合、カナダ国内に子会社やオフィスがあっても、本社がカナダ国外にある場合は、この書類に記入する必要がある。PI は大学の承認を得るために研究計画書・契約書を提出した後 2 週間以内に、本書類を提出する必要があり、提供された情報は一元的に審査され、2 週間以内に審査完了となる。必要に応じて、副学長室（国際担当）、副学長室（研究・イノベーション担当）、又は所属部門の担当者が、提案されたパートナーシップについて申請者と協議を行う。

[194] トロント大学ウェブサイト" ENGAGING IN INTERNATIONAL RESEARCH PARTNERSHIPS: PRINCIPLES AND APPROACHES"<https://global.utoronto.ca/wp-content/uploads/2015/08/Engaging-in-International-Partnerships.pdf>

[195] トロント大学ウェブサイト"Research Partnership Security Information Document for International Partnerships"<https://redcap.utoronto.ca/surveys/?s=PMF483RY8NMNNDJL >

2.5 欧州連合（EU）

2.5.1 研究インテグリティの確保に関する要求と支援

(1) 「研究・イノベーションにおける外国からの干渉に対応するためのスタッフ作業文書」（2022 年 1 月）

2022 年 1 月に、欧州委員会は「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）を発表した[196]。本文書は、「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。

前文では、文書の目的等について以下のように説明している。

- 「本書は可能な限り具体的であることを目指すが、(海外からの干渉に対処するための）万能のアプローチは存在せず、各組織が独自の対策を講じる必要がある。この文書は、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する。」
- 「本スタッフ用作業文書は、HEI（高等教育機関）及び RPO（研究実施機関）が、学問の自由、インテグリティ、機関の自治（academic freedom, integrity and institutional autonomy）などの基本的価値を守り、職員、学生、研究成果・資産を保護する努力を支援するために、海外からの干渉（foreign interference）を軽減するための実務に関する情報を提供することを目的として作成された。したがって、本規定は国際的な共同研究を制限するものではなく、むしろ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することを意図している（promote international collaboration that is as open as possible and as closed as necessary)。さらに、HEI や RPO に新たな事務処理の負担を強いるものではなく、可能な限り既存の仕組みの中に可能な措置を組み込むことを推奨する。」
- 「このスタッフ作業文書は、加盟国及び利害関係者と共同で作成され、ベストプラクティスの目録及び証拠の収集として意図されており、網羅的でも拘束力があるわけでもない。つまり、多くの問題について詳細な情報を提供しているが、この文書に含まれていない要素もあるかもしれない。さらに、インスピレーションの源として利用されるべきものである。加盟国や組織は、同じテーマについて他の手段を採用することを検討してもよい。抵抗

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

力の構築と海外からの干渉の事案への対応は、適切な場合には、地域及び国の当局と協議し、その支援を受けて行われるべきものである。」

ここで「海外からの干渉（foreign interference）」については、「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」[197]と冒頭の用語説明で定義している。

このような海外からの干渉の目的は、「海外の行為者の政治的、社会的、文化的、経済的、技術的利益を促進すること」であり、以下を含む。

- 海外の行為者の利益となる情報を不法に取得すること。
- 海外の行為者に有利となるように意思決定に影響を与えること
- 海外の行為者に反すると認識される価値観を弱体化する。」

また、海外の行為者は、目的を実現するために、以下のような海外からの干渉の戦術を展開可能であると説明している。

- 戦略的意思決定者に対する影響力のある代表者による政治的圧力
- 投資、寄付、資金提供、融資といった形での財政支援
- 戦略的地位にある人物を脅し、勧誘し、又は配置する
- 遠隔地又は現地でサイバーセキュリティを侵害するデジタル侵入
- 現地の利益に反する、又は海外の利益を促進する偽情報の流布

また、上述のように、海外からの干渉に対処すべきであるが、そのような対応は「国際的な共同研究を制限するものではなく、むしろ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することを意図」していることが強調されている（”*as open as possible and as closed as necessary*”）。「オープンサイエンス」（Open Science）が欧州では推進されており、それと「海外からの干渉」の防止とを、バランスを取って達成することが意図されているとみられる。第 1 章では、以下のように説明している。

- オープンサイエンスの実現は欧州委員会の政策的優先事項である。オープンサイエンスは、必ずしもオープンかクローズかという二項対立的なものではなく、むしろ研究の性質に応じて研究成果のさまざまな種類や側面をオープンにしたりしなかったりする、オープンさのスペクトラム（spectrum of openness）であることに注意することが重要である。このことは、「可能な限りオープンに、必要な限りクローズに」（as open as possible and closed as necessary）というモットーに反映されている。研究成果は、プライバシー、安全保障、政治、軍事、商業上の理由から、正当な理由によって公開されないことがある。

[197] “activities that are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU).”

また、海外からの干渉に対応するためには、「多次元的なアプローチ」を取るべきであると説明している。

- 高等教育機関と研究機関は、外国の研究者や組織との共同研究に対して恐怖心を抱くような文化ではなく、海外からの干渉に対抗するための自覚と連帯責任を持つ文化を醸成することが重要である。対応は共同研究のリスク、範囲、性格に比例させ、デューディリジェンスや複数の情報源から情報を得るべきである。本スタッフ作業文書に示された対策は、高等教育機関と研究機関における海外からの干渉に対する戦略的方針を策定するための初期導入として役立つものである。高等教育機関と研究機関は、これらの可能な対策を基に、それぞれのニーズや環境に応じて独自の内部対策を講じることが期待される。

既に述べたように、「海外からの干渉」（foreign interference）への対応策について、本報告書では、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、説明している。以下の表はこれらをまとめたものである。

表 2-42：「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. あなたの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、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）を特定し保護し、第三国からの潜在的な技術的、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).

(2) Horizon Europe Program Guide Version 2（2022 年 4 月 11 日）

欧州連合の研究資金プログラム（2021～2027 年）である Horizon Europe 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、その後、Version 1 は Version 1.1、1.2、1.3、1.4、1.5 とマイナー修正が加えられた。2022 年 4 月 11 日に公表された Version 2 では、上述の「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されている[198]。追加されたのは以下の文章である。

・ 「欧州委員会は、『研究・イノベーション（R&I）の海外からの干渉』に取り組むためのツールキットを発表した。この文書は、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に関する多くの勧告を提供しており、高等教育機関や研究実施機関

[198] 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

が国際的な R&I に取り組む際の支援を提供することを目的としている。Horizon Europe に参加するすべての人は、この文書及び国レベルで存在する同等のアドバイスをよく理解し、提出予定のプロポーザルとの関連性を検討することが推奨される。」

第3章　研究インテグリティについての説明会の実施

3.1 説明会開催の趣旨、目的

「研究インテグリティについての説明会」を、「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、大学等における取組についての講演を行うとともに、参加者との質疑応答を行うことで、研究インテグリティについての理解を深め、その確保のための具体的取組の情報交換を促進すること」を目的として開催した。研究インテグリティ関連の業務に関わっているあるいは関心を持つ、大学・研究機関の教員・研究者・職員を対象として、オンラインのウェビナー（第 1～3 回説明会：70 分、第 4 回説明会：75 分）を 4 回実施した。

<説明会の趣旨>
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いる。こうした中、我が国として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、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きており、2021 年 4 月には、研究インテグリティの確保に係る政府の対応方針が決定されたところである。このような背景のもとで、本説明会では、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、参加者との質疑応答を行う。
＜対象＞
研究インテグリティ確保のための政府施策や大学等における取組に関心のある者
（大学の教職員、研究機関・企業の研究者・事務担当者等）
＜開催方法＞
Zoom を用いたオンライン形式
＜参加費＞
無料
＜主催者・事務局＞
主催：内閣府
事務局：公益財団法人未来工学研究所

3.2 説明会の開催内容

各回の説明会の開催内容は以下のとおりである。第 1～3 回説明会では、政府からの説明を 20 分、大学事例についての説明を 20 分した後に、残りの時間（約 20 分間）を質疑応答に充てた。第 4 回説明会では約 60 分間のパネルディスカッションを行い、その中で適宜質疑応答を行った。

表 3-1：研究インテグリティについての説明会の開催内容

第 1 回説明会（2022 年 12 月 17 日） 政府の取組：「研究インテグリティに係る対応方針とその取組状況」（内閣府、文部科学省） ※第 2 回、第 3 回説明会時も同様の説明。 概要：近年、研究活動の国際化、オープン化に伴って、研究成果の帰属が不適切に取り扱われる等、外国からの不当な影響による利益相反・責務相反や技術流出等のリスクが顕在化している。このようなリスクへの対策の一環として、政府は、研究の健全性・公正性（研究インテグリティ）に係る対応方針を 2021 年 4 月に決定した。本発表では、政府の対応方針において、研究者、大学・研究機関、公的資金配分機関にどのようなことが求められているのかと、その実現を支援するための政府の取組について紹介する。 大学の取組：「東北大学における研究インテグリティに関する取り組み」 東北大学　副理事（研究公正担当）　佐々木孝彦 概要：最近の大学・研究機関を取り巻く研究環境の急速な変化の中で、特に国際化・オープン化が進む科学技術・イノベーションに関して、国際的にも研究活動の透明性や説明責任を研究者自らが果たし、大学・研究機関はそのマネジメントを行う「研究インテグリティ」の確保が求められている。東北大学では，約２年間の状況把握や対応制度検討を経て「研究インテグリティ」確保の体制整備を行ってきた。本取組の過程と現状について紹介する。
第 2 回説明会（2023 年 1 月 17 日） 大学の取組：「研究インテグリティの確保と大学法務～九州大学の取り組み」 九州大学　法務統括室 室長補佐・特任教授　佐藤弘基 概要：「研究インテグリティ」の確保を目指すためには、研究者自身による徹底を求めることに加えて、九州大学では大学全体のコンプライアンス体制の強化をすることも重要であると理解している。学内のコンプライアンス体制の強化のためには法務機能の充実が欠かせない。大学法務機能はどうあるべきか、九州大学での現状と目指す姿について紹介する。
第 3 回説明会（2023 年 1 月 27 日） 大学の取組：「研究インテグリティ確保をリスクマネジメントにどう繋げるか？」 名古屋大学 学術研究・産学官連携推進本部 学術・連携リスクマネジメント部門 部門長　特任教授　宮林毅 概要：名古屋大学では「研究インテグリティの確保について」全学的な観点から検討を進めている。留学生や外国人研究者への技術提供の事例では複合的なリスク案件が顕在化しており異なる切り口で全体を俯瞰して管理するようなトータルマネジメントの必要性が高まっている。研究インテグリティ確保の中核となるのは、透明化をキーワードにしてきた利益相反管理と考えており、従来の自己申告制度を拡充して人・物・金の流れを把握・確認し、研究者が遭遇する様々な複合リスクに対応できるマネジメント体制を構築できればと考えている。
第 4 回説明会（2023 年 3 月 9 日） パネルディスカッション： 司会進行 東京大学 未来ビジョン研究センター 教授　渡部俊也 パネリスト 東北大学　副理事（研究公正担当）佐々木孝彦 九州大学　法務統括室 室長補佐・特任教授　佐藤弘基 名古屋大学 学術研究・産学官連携推進本部 学術・連携リスクマネジメント部門 部門長　特任教授　宮林毅

内閣府 科学技術・イノベーション推進事務局 上席政策調査員　田村朱麗
文部科学省 科学技術・学術政策局 参事官（国際戦略担当）付
参事官補佐　遠藤正紀　　係長　加藤拓巳

3.3 説明会への参加状況

各説明会への参加者人数（主催者・事務局と講演者を除く）は、第 1 回説明会が約 350 人、第 2 回説明会が約 250 人、第 3 回説明会が約 220 人、第 4 回説明会が約 280 人であった。4 回の説明会への参加者ののべ人数は約 1,100 人であった。

3.4 説明会への参加者からの感想・質問

説明会参加者へのアンケート結果によれば、参加者の所属は国立大学（48.9%）、公立大学（24.7%）、国立研究開発法人（18.9%）が多く、職種は大学職員（63.4%）、研究機関等の職員（18.9%）、大学教員（11.9%）が多かった（第 1 回説明会参加者 227 人の回答）。第 2～4 回説明会においても概ね同様の傾向が見られた。第 1～3 回説明会における政府側からの説明（内閣府・文部科学省）に対しては「とても参考になった」が 2 割程度、「参考になった」が 6～7 割程度であり、大学の事例についての説明については、「とても参考になった」が 4 割程度、「参考になった」が 5～6 割程度の回答だった。

また、第 1～3 回の事例紹介者が全員参加し、パネルディスカッション形式で行った第 4 回説明会においては「とても参考になった」が 32.7%、「参考になった」が 64.2%であり、高い満足度が得られた（図 3-1）。

また、自由記入の質問（コメント、今後の要望等）に対しては、参加者に大学職員が多かったこともあり、研究インテグリティ確保のための具体的な事例（大学、国立研究開発法人等）をもっと知りたいとの声が多かった。また、今回の説明で取り上げた事例が規模の大きな研究大学であったことから、中小規模大学、地方大学における研究インテグリティ確保のための体制整備はどのように進めるべきかについて知りたいとの要望も多かった。

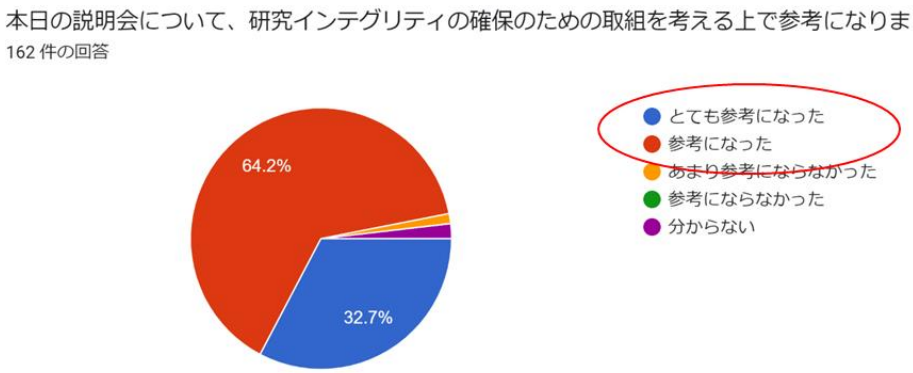


図 3-1：第 4 回説明会における事後アンケート結果

説明会では、上記のように、政府側からの説明、大学における取組の事例紹介の説明をするとともに、参加者との質疑応答等をすることで理解をより深めることが目的とされていたが、多くの質問が参加者から寄せられた。第 1 回説明会は 28 問（事前質問 22 問、当日 6 問）、第 2 回説明会は 23 問（事前 19 問、当日 4 問）、第 3 回説明会は 11 問（事前 5 問、当日 6 問）、第 4 回説明会は 22 問（事前 21 問、当日 1 問）の質問があった。主な質問内容は、研究インテグリティの概念や「新たなリスク」の具体的内容や判断についてのもの（「新たなリスク」とは何か。研究インテグリティで扱うリスクの具体的内容はどのようなもので、どのように判断を行うのか等）、研究インテグリティへ取り組むための組織についてのもの（安全保障輸出管理、利益相反等に関する既存の体制に、研究インテグリティ確保のための新たな組織等をどのように位置づけ、既存の体制をどのように拡充していけばいいのか等）が多かった。

第 4 回説明会では今後の政府の研究インテグリティ確保のための施策等への要望についてのコメントとしては、次年度以降も、同様の大学・研究機関における研究インテグリティ確保のための取組の先進的な事例についての情報共有をするための説明会等の実施を継続することを希望する意見が多かった。また、今年度はオンライン会議で実施したが、「来年度以降は対面で直接意見交換ができる場を期待する」との意見もあった。

第4章　調査のまとめと注目点

4.1 研究インテグリティの確保のための各国・地域の取組の注目点

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、カナダと欧州連合（EU）について調査した。調査の視点としては、特に、対象国・地域における研究インテグリティ確保のための取組（法令・ガイドライン等の制定、政府と大学・研究機関、資金配分機関等における具体的取組を含む）の全体像を俯瞰した際に、1）研究者、大学・研究機関、資金配分機関が研究インテグリティの確保のためにどこから何を要求されているか、2）1）の要求を研究者、大学・研究機関、資金配分機関が実施し、あるいはそれら実施を確かなものとするためにどこからどのような支援が提供されているか、に注目した。この要求と支援に係るマクロな構図を把握した上で、以下に注目点についてまとめた（*各国・地域の取組のまとめについては報告書冒頭の「エグゼクティブ・サマリー」（vii 頁）を参照すること*）。

4.1.1 米国

連邦法や大統領覚書、実施ガイダンス等において、連邦省庁、資金配分機関、大学・研究機関、研究者等に対して、研究インテグリティの確保のための様々な要求事項が規定されており、それら要求を確実に実施してもらうための支援についても規定がある。それらは多項目にわたるものであるが、以下は特に注目される取組である。

- 研究セキュリティのトレーニングについて政府研究資金を受ける研究者に受講義務付け（CHIPS and Science Act）
- 研究セキュリティについて連邦法で規定されている（CHIPS and Science Act）
- 研究セキュリティについてのモデル教育プログラムの開発（NSF の公募で 4 大学に既に委託）
- 情報機関（CIA、FBI、ODNI）が政府の研究セキュリティ対応体制に入っている。当初の NSPM-33 から明示。
- 国土安全保障省による外国人留学生、外国人研究者への入国審査も研究セキュリティの対応策の中に位置づけられている。
- 外国人人材採用プログラムへの参加を開示義務。政府研究機関の研究者は参加が禁止、大学等の政府資金受領研究者は、悪意のある外国人人材プログラムへの参加を禁止。
- 大統領府レベルの Subcommittee on Research Security（National Science and Technology Council に属する）でほぼ全ての関係省庁（情報機関、安全保障担当大統領補佐官を含む）が集まって研究セキュリティ対応について対策する体制ができている。
- 同盟国、他の友好国に対しても研究セキュリティ対応について働きかけることが

NSPM-33 に明記。

- 米国の全米アカデミーズ（National Academies）は、報告書「米国の技術優位を保護する」を作成し、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術をいかに保護するかについて、大統領府や連邦政府機関への政策提言をした。「科学技術安全保障円卓会議」が設置され、「オープンネス、国際的関与と連邦資金科学技術研究」についてのワークショップを開催し、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場を作っている。

4.1.2 英国

以下は英国の研究インテグリティの確保のための取組のなかで、特に注目されるものを列挙した。

- 英国の経済安全保障の一環として、経済的利益を享受している英国の国際研究・イノンベーションの保護の観点から、ビジネス・エネルギー・産業戦略省 BEIS）が研究インテグリティに大きく関与。
- 国家安全保障機関のイニシアティブの下に研究インテグリティを推進。国家安全保障機関が、大学協会及び資金配分機関と手を握り、強力に研究インテグリティを推進。
  - 国家安全保障機関からベースとなる研究インテグリティに関するガイダンスを発行。
    - 大学・研究機関研究者向けのガイダンス
    - 大学・研究機関の研究及び職員のセキュリティ担当者向けの実践的ガイダンス
    - 大学・研究機関の上級管理者向けのガイダンス
    - 国際共同研究提案の際のチェックリスト　等
  - 国家安全保障機関のガイダンスを補完する位置づけで、大学協会から研究インテグリティに関するガイダンスを発行。
  - 国家安全保障機関のガイダンスを踏まえて、ファンディング機関から研究インテグリティに関する原則に関する文書を発行し、ファンディングを受ける際の原則の遵守を要求（パートナーの適性評価、情報セキュリティ管理策の導入、知的資産を適切に管理するための共同研究契約の締結など）。
  - 国家安全保障機関、大学協会及びファンディング機関の共同で、継続的に、研究インテグリティに関するガイダンスや関連資料の整備を実施。
  - 政府・大学として、国際共同研究におけるリスク緩和策のチェックリストを作成・提示
  - 政府・大学として、大学における研究インテグリティ活動の紹介

・ 法的権限はないが、政府として、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窓口機関(RCAT)を設立。

4.1.3 豪州

以下は豪州における研究インテグリティの確保のための取組のなかで特に注目されるものである。

・ 外国干渉セキュリティにおける豪州の取組の特徴の１つは、内務省直轄の防諜機関である豪州保安情報機構（ASIO）に大きく依存していることにある。これまで見てきたように、ASIO は UFIT ガイドラインの運用に積極的に関わり、大学・研究機関側の連絡や相談の窓口としても機能しており、いわゆる公安情報に基づいてガイドラインが運用されている側面があるのではないかと思慮される。国内には表立った反発や反対論は見受けられないが、学問の自由との関係で問題提起する大学もある。
  - 例えば、豪州国立大学（ANU）では、厳格な外国干渉セキュリティに対する措置を取る一方、学問の自由を守る立場から、そもそも「外国干渉とは何を意味するのか」という視点から、同大学は学内のインターネットサイトに「外国からの影響（influence)」と「外国からの干渉（interference)」の違いに注意喚起を促す同大研究者によるレポートを掲載している。それによると、「豪州の対応は外国からの影響のうち、最も悪質な形態である外国干渉を犯罪とみなし、その抑止に重点を置いてきた。しかし許容される外国からの影響と不法な外国からの干渉の間にはグレーゾーンが生まれつつある」として、行き過ぎた政府の外国干渉排除の動きにくぎを刺している。

また、豪州の研究インテグリティに対する考え方は、あくまでも大学・研究機関による自主性や自己規制を重んじる形になっている点も注目される。たとえ不正事案や外国干渉セキュリティにまつわる事案であっても、不正調査や認定を資金配分機関など外部の機関が行うことはなく、個別の大学あてに勧告を出すにとどまっているのが大きな特徴だ。大学・研究機関は、あくまでも独自に通称・豪州規範（The Australian Code for the Responsible Conduct of Research、「責任ある研究実施のための豪州規範」）や通称・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」）に沿って自主判断し、最終決定を下すとされている。

自主的なガイドラインや規範の運用にこだわる姿勢は、2021 年に UFIT ガイドラインが更新された際、過度な情報開示を求める政府草案に大学・研究機関側から強い反発が出て争点化し、政府側が修正を強いられた経緯にも現れている。政府草案では、「大学すべての研

究者に、政党の所属と過去 10 年間の外国企業から受けた資金支援」を開示するよう求める踏み込んだ内容だったものが、反発を受け、このくだりは「大学側が利益相反開示の聴き取りをする対象の研究者を選べる」ように修正された。あくまでもガイドラインの運用は大学当局が自主的に行う、という原則が確認される結果となった。

4.1.4 カナダ

以下のカナダにおける取組は特徴的なものである。

- 大学における国家安全保障当局との活発な連携が行われている。
- 外国影響やスパイからの研究コミュニティの保護は、公共安全省の一義的な責務であると宣明している。
- 地域別（州ごと）のリスク評価の参考資料を政府が用意している。

4.1.5 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」（Tackling R&I foreign interference staff working document）を発表した。本文書は、「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。「海外からの干渉」（foreign interference）への対応策について、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、説明している。提案されている取組のなかで以下の「価値観」に関連するものについては、研究インテグリティの確保の観点からは、特徴的なものである。

〇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、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。

〇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。

この文書については、欧州連合の研究資金プログラム（2021～2027 年）である Horizon Europe のプログラムガイドの第 2 版（2022 年 4 月 11 日公表）で、「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された。追加された部分では「Horizon Europe に参加するすべての人は、この文書（※上記の「スタッフ作業文書」）及び国レベルで存在する同等のアドバイスをよく理解し、提出予定のプロポーザルとの関連性を検討することが推奨される」と説明している。

4.2 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

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に対して、各国・地域の問題意識は共通しているものの、それへの対応策については、それぞれの国の科学技術行政体制や、科学コミュニティの特色あるいはそれらに関連する伝統や歴史的経緯を反映して、様々であり、どの国の取組がベストプラクティスと言える訳ではない。言い換えれば、ある国において有効な方法であっても、他の国においては科学者コミュニティや社会から反発を受けて取組が定着せず、有効に履行されないこともあり得

る。

以上を考慮した上で、上記の各国・地域の調査結果で注目すべき点として指摘された取組等の中で、要求に関連する取組等、支援に関連する取組等、さらにそれらを検討し、履行をフォローするための体制について、以下については、日本にとってレッスンを得ることが大きいのではないかと考えられる。

研究インテグリティに関連する要求事項

・ 米国：研究セキュリティのトレーニングについて政府研究資金を受ける研究者に受講義務付け（CHIPS and Science Act）

研究インテグリティに関する支援関連事項

(a) 研究者への支援関連

・ 英国：大学・研究機関研究者向けのガイダンスの策定

(b) 大学・研究機関等への支援関連

・ 米国：研究セキュリティについてのモデル教育プログラムの開発

・ 英国：助言の仕組み：Research Collaboration Advice Team (RCAT)。政府として、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窓口機関（RCAT）を設立。

・ 英国：大学・研究機関の上級管理者向けのガイダンスの提供

・ 豪州：大学の上級管理者に対し、外国干渉の脅威と国家安全保障政策について説明する（UFIT ガイドライン）

・ 豪州：豪州の上位８つの大学で組織するグループ８（Go8）が外国干渉を排除するためのベストプラクティスを取りまとめ公表。

・ カナダ：外国影響やスパイからの研究コミュニティの保護を責務とする公共安全省が地域別（州ごと）のリスク評価の参考資料を作成し、公表。

・ EU：「価値観」（学問の自由へのコミットメントの強化、抑圧的な環境下にあるパートナーとの協力）に関連する、「海外からの干渉」（foreign interference）への対応策の大学・研究機関への提示。

(c) 学協会等のアカデミアの取組

・ 米国：米国の全米アカデミーズ（National Academies）は、報告書「米国の技術優位を保護する」を作成し、オープンネスと競争の時代において、国家安全保障にとって戦略的に重要な技術をいかに保護するかについて、大統領府や連邦政府機関への政策提言をした。全米アカデミーズに「科学技術安全保障円卓会議」が設置され、関係者（大学、連邦国立研究所、連邦政府機関、情報機関）の間での意見交換や共通理解の醸成のための場となっている。

研究インテグリティの確保を検討・履行するための国の体制

- 米国：大統領府レベルの Subcommittee on Research Security（National Science and Technology Council に属する）でほぼ全ての関係省庁（情報機関、安全保障担当大統領補佐官を含む）が集まって研究セキュリティ対応について対策する体制ができている。
- 英国 : 国家安全保障機関が、大学協会及び資金配分機関と手を握り、強力に研究インテグリティを推進。
- 豪州：政府と大学・研究機関が共同してタスクフォース（UFIT: University Foreign Interference Taskforce）を設置。政府の保安情報機構（ASIO）や外国干渉対策調整センターを通じての大学への働きかけ。
- カナダ : 外国影響やスパイからの研究コミュニティの保護は、公共安全省の一義的な責務であると宣明している。

4.3 研究インテグリティについての説明会の実施から得られた示唆等

「研究インテグリティについての説明会」はウェビナー形式で 4 回開催した。説明会では、政府側からの説明、大学における取組の事例紹介の説明をするとともに、参加者との質疑応答等をすることで理解をより深めることが目的とされていたが、多くの質問が参加者から寄せられた。主な質問内容は、研究インテグリティの概念や「新たなリスク」の具体的内容や判断についてのもの（「新たなリスク」とは何か。研究インテグリティで扱うリスクの具体的内容はどのようなもので、どのように判断を行うのか等）、研究インテグリティへ取り組むための組織についてのもの（安全保障輸出管理、利益相反等に関する既存の体制に、研究インテグリティ確保のための新たな組織等をどのように位置づけ、既存の体制をどのように拡充していけばいいのか等）が多かった。

本委託事業の最後の説明会の第 4 回説明会では、次年度以降も、同様の大学・研究機関における研究インテグリティ確保のための取組の先進的な事例についての情報共有をするための説明会等の実施を継続することを希望する意見が多かった。また、今年度はオンライン会議で実施したが、「来年度以降は対面で直接意見交換ができる場を期待する」との意見もあった。

参考文献

全般

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.

米国関係

Association of American Universities (AAU). The CHIPS and Science Act of 2022 (H.R. 4346): Research Security Provisions. Last updated August 8, 2022.

Collins, Francis S. M.D., Ph.D. Director, National Institutes of Health. Statement on Protecting the Integrity of U.S. Biomedical Research. August 23, 2018.

Dwyer, Morgan (Principal Assistant Director for National Security, Office of Science and Technology Policy); Christina Ciocca Eller, Assistant Director of Evidence and Policy and Co-Chair of the National Science and Technology Council Subcommittee on Research Security, Office of Science and Technology Policy; and Ryan Donohue, AAAS Science and Technology Policy Fellow and Senior Policy Advisor, and Member of the National Science and Technology Council Subcommittee on Research Security, Office of Science and Technology Policy. An Update on Research Security: Streamlining Disclosure Standards to Enhance Clarity, Transparency, and Equity.

Jester, Julia; Toby Smith. Chips and Science Act. Association of American Universities. ARIS Office Hours, October 28, 2022; About the "CHIPS and Science Act"

Lauer, Michael, National Institutes of Health (NIH) Office of Extramural Research (OER), Patricia Valdez, NIH OER. *Brief Summary of NIH Foreign Interference Cases*. 2022-12-11.

MIT China Strategy Group (Richard Lester and Lily Tsai (co-chairs), Suzanne Berger, Peter Fisher, M. Taylor Fravel, David Goldston, Yasheng Huang, Daniela Rus). *University Engagement with China: An MIT Approach Final Report*. November 2022.

National Academies of Sciences, Engineering, and Medicine. 2022. *Protecting U.S. Technological Advantage*. Washington, DC: The National Academies Press. https://doi.org/10.17226/26647.

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, "NSF Pre-award and Post-award Disclosures Relating to the Biographical Sketch and Current and Pending Support," January 30, 2023.

National Science Foundation. NSTC Research Security Subcommittee NSPM-33 Implementation Guidance Disclosure Requirements & Standardization

National Science Foundation. Proposal & Award Policies & Procedures Guide (PAPPG) (NSF 23-1). January 30, 2023. Chapter II: Proposal Preparation Instructions. B. NSF Disclosure Requirements

National Science Foundation. Privacy Act of 1974; System of Records. Federal Register/Vol. 86, No. 214/Tuesday, November 9, 2021/Notices.

National Science Foundation. Agency Information Collection Activities: Request for Comment Regarding Common Disclosure Forms for the Biographical Sketch and Current and Pending (Other) Support. Federal Register/Vol. 87, No. 168/Wednesday, August 31, 2022/Notices.

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

Department for Science, Innovation& Technology. Policy paper International Research and Innovation Strategy." 14 May 2019.

CPNI Trusted Research website. " Trusted Research Guidance for Academia " <https://www.npsa.gov.uk/trusted-research-academia>

CPNI. Trusted Research Checklist for Academia.

CPNI. TRUSTED RESEARCH Countries and Conferences.

CPNI. Trusted Research Implementation Guide.

CPNI. Trusted Research Guidance for Senior Leaders.

UK Research and Innovation, “UK Research and Innovation Trusted Research and Innovation Principles,” August 2021. < https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf>

UUK website. “ Managing risks in Internationalisation: Security related issues ” <https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation>

UUK/CPNI/UKRI, “Managing risks in international research and innovation: An overview of higher education sector guidance,” June 2022.

豪州関係

Department of Education, Australian Government *Guidelines to Counter Foreign Interference in the Australian University Sector*. October 2021.

Go8. *Go8 measures to safeguard Australia's sensitive research.*

National Health and Medical Research Council. *Australian Code for Responsible Conduct of Research*. 2018.

カナダ関係

Government of Canada ” National Security Guidelines for Research Partnerships”

Government of Canada.” The National Security Guidelines for Research Partnerships’ Risk Assessment Form”

Natural Sciences and Engineering Research Council of Canada. “NSERC 2030: Discovery. Innovation. Inclusion.”

Public Safety Canada. *Departmental Results Report 2021-22.*

EU 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.

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４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

2023 年 3 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）