

日本語仮訳:

グローバルな研究エコシステムに おけるインテグリティとセキュリティ

経済協力開発機構 (OECD)

科学技術産業ポリシーペーパー (130号)

Original:

INTEGRITY AND SECURITY IN THE GLOBAL RESEARCH ECOSYSTEM

OECD

SCIENCE, TECHNOLOGY AND INDUSTRY
POLICY PAPERS

June 2022 No. 130

原著は、OECDにより、OECD科学技術産業ポリシーペーパー第130号として、“Integrity and security in the global research ecosystem”と題して英語で発表されたものである。

©OECD 2022, <https://doi.org/10.1787/1c416f43-en>

本翻訳はOECDが作成したものではなく、OECDの公式翻訳ではない。翻訳の品質及び著作物の原文との整合性は、翻訳の著者に責任がある。原著と翻訳との間に齟齬がある場合は、原著の本文のみを有効とする。

© 2022 国立研究開発法人科学技術振興機構（JST）による翻訳

Originally published by the OECD in English under the title: “Integrity and security in the global research ecosystem”, OECD Science, Technology and Industry Policy Papers, No. 130

© OECD 2022, <https://doi.org/10.1787/1c416f43-en>

This translation was not created by the OECD and should not be considered an official OECD translation. The quality of the translation and its coherence with the original language text of the work are the sole responsibility of the author or authors of the translation. In the event of any discrepancy between the original work and the translation, only the text of original work shall be considered valid.

© 2022 Japan Science and Technology Agency (JST), for this translation

日本語仮訳版「グローバルな研究エコシステムにおけるインテグリティとセキュリティ」の公表にあたって

経済協力開発機構（OECD）のグローバル・サイエンス・フォーラム（GSF）は、OECDの科学技術政策委員会（CSTP）の下に設置された作業部会の一つであり、研究開発ファンディング・システム、科学的助言、研究基盤の在り方等について、加盟国間の科学技術協力を推進し、各国の取組の情報交換や科学政策策定に活用可能な国際的な枠組みの構築に向けた提言等を行うことを目的としている。

本報告書は、GSFにおけるプロジェクト“Integrity and security in the global research ecosystem”（グローバルな研究エコシステムにおけるインテグリティとセキュリティ）の成果を取りまとめた報告書について、国立研究開発法人科学技術振興機構（JST）研究開発戦略センター（CRDS）が、OECDの許諾を受けて翻訳し、公表するものである。

科学研究における自由と国際協力は科学の進歩の基礎となるものである。また、パンデミック、気候変動等のグローバルな課題に取り組むには国際的な研究協力が不可欠である。しかし、このオープンな研究環境を自らの利益のために不当に利用しようとする動きが一部の政府や非国家主体の間で広がっており、多くの国は、公的研究に対する外国の干渉は、国家安全保障と経済安全保障に対する重大なリスクと捉えるようになってきている。

このような認識を受けて、GSFは、研究の自由・開放性・無差別性を確保しつつ、国家安全保障と経済安全保障上のリスクを低減するための実用的な情報と推奨事項を各国に提示することを目的として、2020年10月から「グローバルな研究エコシステムにおけるインテグリティとセキュリティ」に関するプロジェクトを開始し、我が国を含む13か国の専門家が参画した定期的な専門家会合、2回の国際ワークショップでの検討を踏まえ、2022年6月にその成果を取りまとめた報告書を公表した。

本報告書では、研究インテグリティとセキュリティの確保について、各国政府・研究資金配分機関・研究機関・大学・学協会・政府間組織の優れた実践例と、それらを踏まえた各国政府等への政策提言が示されている。

我が国においても、2021年4月に「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」を政府が決定し、大学・研究機関等において具体的な取組が進んでいる段階である。

また、CRDSでは、我が国の政府や大学・研究機関等の取組の具体化に資することなどを目的として、以下の活動を実施してきた。

○調査報告書の作成

①「オープン化、国際化する研究におけるインテグリティ」（2020年10月公表）

- ・国内外の動向や課題について調査を行い、利益相反に重点を置いた研究インテグリティの強化が研究セキュリティの強化に資すること、まずは研究者から所属機関への情報開示を徹底することにより、研究に関する透明性を高めることなどを提言

②「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年5月公表）

- ・米、豪、英、加、EUの政府等の取組を俯瞰するとともに、我が国の研究コミュニティが、研究インテグリティの確保に向けた取組を進めていく上で参考になると考えられる海外の大学の情報を提供

○文部科学省の依頼に基づき、上席フェローの岩瀬公一がGSF専門家会合のメンバーとして、本報告書のプロジェクトに参画（2020年10月から2022年6月まで）

○OECDと合同で我が国の研究コミュニティに向けたワークショップを開催（2022年6月）

このような中で、本報告書で紹介されている各国政府等の実践例や政策提言は、今後我が国において、研究インテグリティとセキュリティに関する取組を推進していくうえで、有益な示唆と知見を提供するものと考えられる。

このため、我が国の関係者に本報告書の内容を広く周知すべく、仮訳版を作成し公表することとした。

本報告書の内容が、今後の我が国における研究インテグリティとセキュリティに関する取組の推進の一助となることを願っている。

2022年11月
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

この序文は、日本語版の作成者である国立研究開発法人科学技術振興機構（JST）が執筆したものであり、原著である英語版には含まれない。この序文に記載されている意見や論拠は、全て日本語版の作成者のものであり、いかなる形であれ OECD やその加盟国に帰属するものではない。

グローバルな研究エコシステムにおける インテグリティとセキュリティ

経済協力開発機構（OECD）

科学技術産業ポリシーペーパー（130号）

本論文は、2022年5月15日に科学技術政策委員会（Committee for Scientific and Technological Policy）によって書面により承認・機密解除され、経済協力開発機構（OECD）事務局によって公表のために準備されたものである。

代表団への留意事項

本文書は、O.N.Eでも参照コードで入手可能である。DSTI/STP/GSF(2021)11/FINAL

本文書及びここに含まれるあらゆるデータと地図は、いかなる領土に係わる状態又は主権、国際的境界線又は国境の確定、並びに領土、都市又は地域の名称に影響を与えるものではない。

イスラエルの統計データは、イスラエルの関係当局が提供し、これに責任を負うものである。OECDによるこのようなデータの使用は、ゴラン高原・東エルサレム・ヨルダン川西岸におけるイスラエルの入植地の国際法上の地位に影響を与えるものではない。

トルコ共和国による注：

本文書中の「キプロス」に関する情報はキプロス島南部に関するものである。同島には、トルコ系とギリシャ系のキプロス人の双方を代表する単一の当局は存在しない。トルコは北キプロス・トルコ共和国（TRNC）を承認している。国連の枠組みにおいて永続的かつ公平な解決策が見いだされるまで、「キプロス問題」に関するトルコの見解に変更はない。

すべてのOECDに加盟する欧州連合加盟国及び欧州連合による注：

キプロス共和国はトルコを除くすべての国連加盟国によって承認されている。本文書に記載されている情報は、キプロス共和国政府の実効支配下にある地域に関するものである。

出版物の正誤表は、www.oecd.org/about/publishing/corrigenda.htm からオンラインで見ることができる。

© OECD 2022

本著作物の使用については、デジタル・印刷を問わず、<http://www.oecd.org/termsandconditions> に記載されている規約が適用される。

グローバルな研究エコシステムにおける インテグリティとセキュリティ

研究インテグリティとセキュリティに関する責任は、国際的な研究エコシステムの中で複数の主体に分散している。これらの主体には各国政府・研究資金配分機関・研究機関・大学・学協会・政府間組織が含まれる。本報告書では、研究の自由を守り、国際研究協力を推進し、開放性と無差別性を確保しつつ、国家と経済の安全保障を確保するための様々な主体の政策と行動について説明している。また、本報告書では、外国の干渉を防ぎ、リスクを管理し、将来にわたって科学に対する信頼を確保するために行われている行動の具体例を紹介するとともに、各国がより幅広い研究インテグリティの枠組みの一部として、研究セキュリティを強化するための効果的な政策を策定するのを支援するための提言を示している。

序文

科学的発見は、世界中の知性・ノウハウ・才能・資金・インフラを合わせて活用する相互に関連した国際的なエコシステムの中で起こる。科学研究における自由と国際協力は科学の進歩の基礎となるものである。科学的な情報とデータのオープンで透明性の高いコミュニケーションと普及、研究資料の共有は、グローバルな科学エコシステムが効果的に機能する上で不可欠である。COVID-19のパンデミック、気候変動、その他の複雑な社会経済問題等のグローバルな課題に取り組むには国際的な研究協力が不可欠である。

しかし、オープンな研究環境を自らの利益のために不当に利用し、歪めようとする動きを一部の政府や非国家主体が強めており、新たな課題と脅威が生まれつつある。現在では多くの国が、公的研究における不正な情報伝達や外国の干渉を、国家と経済に対する重大な安全保障上のリスク、科学研究の自由に対する脅威と捉えるようになっている。

2020年の早い時期にCOVID-19のパンデミックが宣言されると、この世界的な危機に対処するためには、国際的な研究協力とデータと情報の共有が不可欠であることがすぐに明らかとなった。しかし、パンデミックの真の規模が明らかになるにつれ、科学的知識や技術へのアクセスをめぐる問題は、地政学的要素にますます影響されるようになった。各国が自国の利益を守り、ワクチンやその他の治療法の開発へのアクセスをコントロールしようと努力する中、研究セキュリティは研究・政策コミュニティにとって切実な問題となった。多くの国で国民の重要な分野における科学に対する信頼が低下し、グローバルな研究エコシステムのインテグリティが脅かされたのである。

パンデミックの進行に伴い科学が注目される中、OECDグローバル・サイエンス・フォーラムは2020年10月に「グローバルな研究エコシステムにおけるインテグリティとセキュリティ」に関するプロジェクトを立ち上げた（付託事項については付属書Bを参照）。このタイトルに示されているように、研究インテグリティとセキュリティは相関しているため、これらを併せて考える必要があることは当初から認識されていた。同様に、公的研究が本来持っている国際的な性質も、このプロジェクトに組み込まれている。従って、本プロジェクトの目的は、国家と経済の安全保障を担保する一方で、研究の自由を守り、国際研究協力を促進し、開放性と無差別性を確保するための優れた実践例を特定することにある。

本プロジェクトが完了した2022年の初めの数カ月、ウクライナはロシアによる大規模な軍事侵攻を受けた。OECD諸国の大学や公的研究機関は、両国との関係を再検討することを迫られた。その多くは、ロシアの研究機関との協力を中止し、あるいはウクライナからの難民科学者の受け入れる措置を講じている。これらの措置が一時的なものであることを願っているが、地政学的要素が研究に及ぼす影響と、安全保障上の懸念が非常に動的であることが改めて明らかとなった。今日の同盟国や友好国は、すぐに明日の脅威となりうる。この複雑で急速に変化する世界において、グローバルな研究エコシステムのインテグリティとセキュリティを確保することの妥当性は、おそらく以前よりも高まっている。これは必ずしも議論しやすいテーマではなく、強固な主張やしばしば分裂した見解もあるが、無視できない問題である。

本報告書では、研究の自由を守り、国際研究協力を推進し、開放性と無差別性を確保しつつ、国家と経済の安全保障を確保するための優れた実践例を特定・分析している。研究インテグリティとセキュリティに関する責任は、国際的な研究エコシステムの中で複数の主体に分散している。こうした主体には、各国政府・研究資金配分機関・研究機関・大学・学協会・政府間組織が含まれる。本報告書はこれらの主体それぞれに実用的な情報とガイダンスを提供するものである。本報告書で紹介されている優れた実践例は、研究セキュリティに関する各国政府のSTI政策のオンラインモニタリングツールでも公開されている（<https://stip.oecd.org/stip/>）。

謝辞

本プロジェクトの監督・実施に当たり、GSF 代表団の推薦により選ばれた専門家で構成される国際専門家グループ（EG、付属書 C を参照）が組織された。本最終政策報告書はこのグループが作成したものである。本報告書は、OECD-GSF 事務局の田村嘉章と Carthage Smith が、EG の全メンバーからの情報提供を受けて起草したものである。このほかにも多くの人々が重要な貢献をした。その中には、本プロジェクトのために開催され、優れた実践例や課題の特定に焦点を当てた 2 回のワークショップにプレゼンターやパネリストとして参加した 30 人以上の専門家が含まれている。これらのイベントには、30 カ国以上から、各国政府・研究資金配分機関・研究機関・大学・学協会・国際機関の代表者約 150 人が参加した。

目次

グローバルな研究エコシステムにおけるインテグリティとセキュリティ	3
序文	4
1 エグゼクティブサマリー	9
2 政策提言と行動オプション	11
3 イントロダクション	16
4 国際協力－グローバルな研究エコシステムの重要な要素	19
5 研究プロセスへの外国の干渉	23
6 政策と行動	29
7 まとめ	48
参考文献	49
付属書 A 主要な概念と多様な視点	57
付属書 B グローバルな科学エコシステムにおける 研究インテグリティに関する付託事項	61
付属書 C GSF 専門家会合のメンバー	64
表	
表 4.1 国際的な科学交流と協力のための多国間枠組み	21
表 6.1 機微技術・情報分野	31
表 6.2 研究資金配分機関に開示する活動の種類	37
図	
図 2.1 研究インテグリティと研究セキュリティ	12
図 2.2 リスク管理のサイクル	13
図 4.1 国際共著による科学論文の割合 (OECD、2006年及び2020年)	19
図 4.2 COVID-19の生物医学研究に関する国際科学協力 (2020年1月～11月30日)	20

図 4.3 医学研究論文の総数（分数カウント）から選定した
主要経済圏とそれらの上位 5 つのパートナー経済圏
（2020 年 1 月 1 日～11 月 30 日） 20

図 6.1 助成金申請のリスク評価プロセス 35

図 6.2 研究活動機微性評価ツール
（REST:Research Engagements Sensitivities Tool） 40

図 6.3 英国大学協会の安全保障関連問題への取組における中間成果 42

別欄

別欄 2.1 研究インテグリティとセキュリティに関わる政策分野 14

別欄 3.1 用語集 17

別欄 5.1 事例研究 - 研究における窃盗 25

別欄 5.2 事例研究 - 欺瞞的行為 26

別欄 5.3 事例研究 - 強制的行為 27

別欄 5.4 事例研究 - 研究評価における課題 27

別欄 5.5 研事例研究 - サイバーセキュリティ 28

別欄 6.1 英国 CPNI による研究提案の評価用チェックリスト 33

別欄 6.2 リスク評価質問票 39

別欄 6.3 デューデリジェンスプロセスの実施 43

別欄 6.4 学問の自由の保護 43

OECD の出版物をフォローする：

 <https://twitter.com/OECD>

 <https://www.facebook.com/theOECD>

 <https://www.linkedin.com/company/organisation-eco-cooperation-development-organisation-cooperation-developpement-eco/>

 <https://www.youtube.com/user/OECDLibrary>

 <https://www.oecd.org/newletters/>

本報告書には StarLinks がある **StatLinks** 
...service that delivers Excel® files from the printed page!

本書の表又はグラフの下に StatLinks  がある。対応する Excel® スプレッドシートをダウンロードするには、ブラウザの入力欄にリンクを入力するか、デジタル版のリンクをクリックする。

1 | エグゼクティブサマリー

科学的発見は、世界中の知性・ノウハウ・才能・資金・インフラを合わせて活用する相互に関連した学際的で国際的なエコシステムの中で起こる。科学研究における自由と国際協力は科学の進歩の基礎となるものである。科学的な情報とデータのオープンで透明性の高いコミュニケーションと普及、研究資料の共有は、グローバルな科学エコシステムが効果的に機能する上で不可欠である。

しかし、オープンな研究環境を自らの利益のために不当に利用し、歪めようとする動きを一部の政府や非国家主体が強めており、新たな課題と脅威が生まれつつある。現在、一部のOECD加盟国は、公的研究における不正な情報伝達や外国の干渉を、国家と経済に対する重大な安全保障上のリスク、科学研究の自由に対する脅威と捉えるようになってきている。このことは、国際協力、研究者養成、人材採用、助成金申請のピアレビューなど、研究の中核となるいくつかの面において重要な意味を持つ。安全保障上のリスクは、慎重に管理されなければ、国際的な研究エコシステムの健全性と有効性を著しく損ない、研究成果に対する信頼性を低下させかねない。

本報告書は、公開文書と、作成を監督した専門家グループに参加しているOECD加盟13カ国から収集した追加情報の分析に基づいている（付属書Cを参照）。また、本プロジェクトのために開催された2回の国際ワークショップの成果も含まれている。本報告書では、研究の自由を守り、国際研究協力を推進し、開放性と無差別性を確保しつつ、国家と経済の安全保障を確保するための優れた実践例を特定・分析している。

研究インテグリティとセキュリティに関する責任は、国際的な研究エコシステムの中で様々な規模で行動する複数の主体に分散している。こうした主体には、各国政府・研究資金配分機関・研究機関・大学・学協会・政府間組織が含まれる。分野や国を超えた相互学習には大きな可能性があるものの、これらの主体の多くはすでに将来の政策展開に向け、健全な基盤となる対策を講じている。

国家政府レベルでは、機密情報を管理するための規制がすでにいくつかの国で存在している。これらを守るため、研究機関・大学・研究者は、利益相反（COI）や責務相反（COC）の開示を法的に求められる場合がある。各国政府は、研究セキュリティとインテグリティに対するリスクについての認識を高めるべく、ガイドラインやチェックリストを作成しており、これらの多くにはリスク軽減のための政策や対策が付随している。一部の国では、研究者がリスクを特定・管理し、国際協力におけるセキュリティを強化できるよう、情報機関・法執行機関・研究機関・大学が協力や情報交換を強化している。

研究資金配分機関レベルでは、ガイドラインが、助成金申請者・ピアレビューアー・研究機関職員のCOIとCOCの定義・管理に役立つことがある。一部の研究資金配分機関では、研究資金の申請及び審査プロセスにリスクの評価・管理を組み込んでいる。申請者はリスク評価質問票に回答し、国家・経済の安全保障上のリスクが確認された場合は、研究資金配分機関や所属機関と協力し、リスク軽減計画を策定することが求められる。

公的研究機関（PRI）は、外国からの干渉のリスクを体系的に評価し、新たな研究機会に関する意思決定を支援するツールを開発している。一部のPRIでは、研究者と受託業者が、高リスクと評価された場合には、一部の人材採用プログラムなど、外国政府が主催し、または関係する特定の活動や提携活動に従事することが禁止されている。

大学は、研究セキュリティに対するリスクを軽減し、科学研究のインテグリティと自由を守るための規則やガイドラインを策定している。研究セキュリティに対するリスクを管理するため、専門の委員会や組織を設置し、研究者や事務職員の意識を高める研究セキュリティ教育を行っている大学もある。大学協会は、研究セキュリティの確保に向けて大学が実施している様々な実践例を特定し、それらに関する意識を高めるための調査を実施している。

学協会は、その会員やより広い研究コミュニティ向けに、合意に基づくガイドラインを策定している。一部の学教会は、研究者の意識を高め、経験を共有するためのワークショップを開催している。また、研究機関や大学に助言を行うローカル委員会を設置しているところもある。研究セキュリティと科学的自由のバランスを考慮した適切な政策的措置について各国政府に助言することもある。

政府間レベルでは、G7 諸国が研究エコシステムのセキュリティとインテグリティに関するワーキンググループを設立し、オープンで相互的な研究協力に対するリスクから、研究とイノベーションのエコシステムを保護するために有効な共通原則の策定が計画されている。欧州委員会は2022年初頭、研究とイノベーションに対する外国の干渉を軽減する方法を示したツールキットを発表した。

本報告書では、現在進行中の行動をもとに7つの包括的な提言を行っており、それぞれが様々な主体による行動を必要としている：

1. グローバルな研究エコシステムの重要な要素として、科学研究の自由と国際協力の重要性を強調する
2. 研究セキュリティへの配慮を、研究インテグリティに関する国家的・組織的枠組みに組み込む
3. 研究におけるリスク管理に向けた相応で体系的なアプローチを推進する
4. 利益相反又は責務相反に関する開放性と透明性を促進する
5. 明確なガイドラインを作成し、手続きを合理化し、不要な事務手続きを抑制する
6. より統合された効果的な政策を展開するために、部門や機関を越えて協力する
7. 研究インテグリティとセキュリティに関する国際的な情報交換を強化する

これらの提言については、具体的な行動の提案も含め、次章で詳細に説明している。

2 | 政策提言と行動オプション

本プロジェクトで実施された各国についての調査や2回の国際ワークショップでの議論から、以下の提言が生まれた。研究インテグリティとセキュリティはOECD加盟国に共通する懸念事項であるが、その背景はかなり異なる。従って、各政策提言や関連する行動オプションの優先順位は国によって異なる可能性がある。これらの提言に対応して各国が実施している行動の具体的な情報と事例は、本報告書の第6章で取り上げている。

2.1 グローバルな研究エコシステムの重要な要素として、科学研究の自由と国際協力の重要性を強調する

研究の自由と国際協力は、科学研究に不可欠な要素であり、国際的組織の公式・非公式な提言や宣言の多くに明記されている。地政学的な緊張や政府の行動は、科学の自由や国際協力を損ない、実際の又は認識上の外国人嫌悪や偏見の原因となる可能性がある。

- ・各国政府は、安全保障上の問題に対し、相応なリスク管理を行いつつ、国際協力を促進すべきである。この観点では、国際的な移動と外国人研究者の採用は、国際協力の根幹として認識されるべきである。
- ・研究機関や大学は、科学研究と科学コミュニケーションの自由を尊重した上で、人種や国籍に関わらず、すべての人が平等に扱われるような包摂的かつ包摂的な環境を維持すべきである。

2.2 研究セキュリティへの配慮を、研究インテグリティに関する国家的・組織的枠組みに組み込む

国際協力が普及し科学的生産における地理的分布が変化中、研究インテグリティと科学的責任の一環として、不正な情報伝達や外国からの干渉の軽減を考慮する必要がある（図2.1 研究インテグリティと研究セキュリティ及び付属書Aを参照）。

- ・セキュリティとリスク管理は、研究インテグリティの本質的な側面として、研究機関の文化やプロセスに組み込まれるべきである。この達成を支援するため、政府・研究資金配分機関・研究機関・大学・学協会は、例えば、専用のワークショップを開催、又は教育・研修プログラムを開発することができる（6.1.2、6.5.3、6.7の例を参照）。
- ・各国は、すでに国の研究インテグリティ事務局がある場合は、その権限を拡張することができる。また、政府内に研究セキュリティの専門窓口や専門センターを設置し、研究エコシステム全般にわたってカウンターパートと連携することもできる（6.1.2の例を参照）。

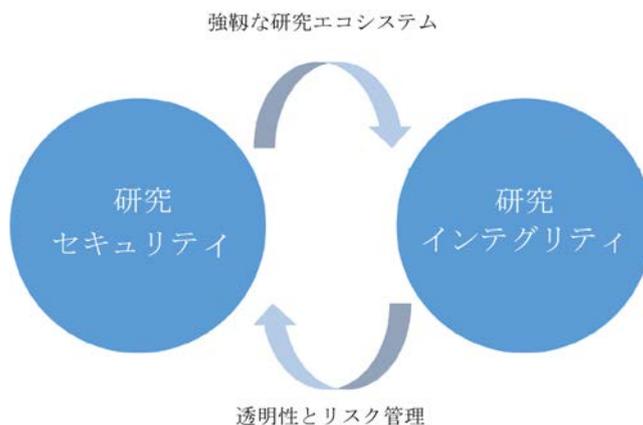


図2.1 研究インテグリティと研究セキュリティ

透明性を高め、潜在的な利益相反（COI）や責務相反（COC）を開示し、リスクを管理することによって研究インテグリティを強化することにより、研究セキュリティは保護される。研究セキュリティ、すなわち外国の国家や非国家による研究への干渉を防止することは研究インテグリティの強化につながる。

2.3 研究におけるリスク管理に向けた相応で体系的なアプローチを推進する

リスク管理においては、科学研究における自由を認める一方、セキュリティも考慮する必要がある。研究インテグリティとセキュリティに向けた方針と行動は、健全なリスクの特定と評価に基づき、定期的に見直し、必要に応じて、改訂する必要がある。すべての研究機関や研究プロジェクトが同じレベル又は種類のリスクに直面しているわけではない。リスク管理と意思決定において、研究機関の自律性を維持することは、リスクを効果的に特定するだけでなく、研究部門全体の同意を得る上でも極めて重要である。

- ・ 科学と安全保障に関わる機関は、定期的に情報を交換し、国際協力の利益とリスクに関する相互理解を深めるべく、信頼されるプロセスを開発する必要がある（6.1.3の例を参照）。
- ・ 政府は、大学や専門家集団による責任ある自己管理（Self-policing）を奨励し、潜在的なリスクをより良く理解・特定・軽減するための能力開発を支援すべきである（6.1.2の例を参照）。
- ・ 政府・研究資金配分機関・研究機関・大学は、セキュリティ戦略の成熟度を定期的に評価し、方針や行動を修正し、その効果を確保する必要がある（図2.2リスク管理のサイクルを参照）。特定の集団に対する差別や人種プロファイリング、研究協力の縮小など、意図しない結果を招かないように監視することが重要である。

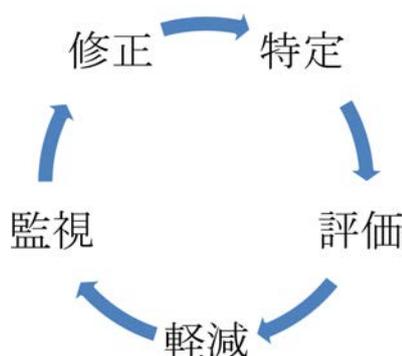


図2.2 リスク管理のサイクル

リスク管理にはリスクの特定・評価・軽減が含まれる。リスク軽減策は、リスクの可能性と潜在的な影響に相応のものでなければならない。リスク軽減策を実施した後、そのプラスとマイナスの効果を監視する必要がある、それに応じ、軽減策を修正しなければならない場合がある。

2.4 利益相反又は責務相反に関する開放性と透明性を促進する

国際的な共同研究において、潜在的なCOIやCOCを認識し、回避することは必ずしも容易ではない。潜在的なCOIやCOCの開示要件を明確にし、透明性の確保とリスク管理の支援に向けたプロセスを確立することが重要である。

- ・ 政府は、大学を含む研究提供者と協力し、研究セキュリティの問題についての認識を高め、研究提供者や研究者に対して、どのような情報を提供することが要求・期待されているかを明確に伝えるべきである（6.1.2、6.1.3、6.2.2、6.5.3の例を参照）。
- ・ 研究資金配分機関・研究機関・大学は、研究者がCOIやCOC、潜在的な研究セキュリティリスクに関する情報を申告することを確保するよう、明確で透明性のあるシステムを構築する必要がある。チェックリストやツールキットはリスクの特定と軽減のプロセスを導く有効な情報源となりうる（6.2の例を参照）。
- ・ 大学・研究機関・個々の研究者は、研究パートナーシップの構築に際し、デューデリジェンスを確保するための透明性のあるプロセスを実施すべきである。新規プロジェクトのリスク評価に加え、進行中のプロジェクトを監視する必要もある（6.3、6.5.1、6.5.2の例を参照）。

2.5 明確なガイドラインを作成し、手続きを合理化し、不要な事務手続きを抑制する

政府・研究資金配分機関・研究機関・大学は、研究者に不要な負担をかけないよう、特定のリスクに的を絞った単純明快で曖昧さのないガイドラインを作成する必要がある。

各国政府と研究資金配分機関は、可能であれば既存のプロセスを活用し、セキュリティ対策に伴う追加的な事務負担を抑制しなければならない。難解・複雑で負担の大きい規則には効果は期待できず、研究の進展に悪影響を与える可能性もある。

- ・ 研究セキュリティを確保するために新たな手続きが必要となる場合があるが、可能な限り、既存の手続き及び／又は仕組みと整合させるべきである（6.1.1、6.2.3、6.3、6.5.2の例を参照）。

- ・大学や研究機関は、研究者が方針の動向を把握し、新たな規制やガイダンスに伴う負担を最小限に抑えるための透明性の高いプロセスを確立しなければならない。研究者を方針の策定に参加させることは、政策の有効性を高める上で有効である（6.3 及び6.5.2 の例を参照）。

2.6 より統合された効果的な政策を展開するために、部門や機関を越えて協力する

異なるステークホルダーの行動は、相互の利益のために効果的に調整される必要がある。研究インテグリティとセキュリティは、多くの政策分野と関連している（別欄2.1 研究インテグリティとセキュリティに関わる政策分野を参照）。同時に、研究インテグリティとセキュリティは、研究資金配分機関・研究機関・大学・科学者個人など、省庁以外の複数のステークホルダーが関与している。こうした複雑さは、研究インテグリティとセキュリティの保護に伴う責任と行動について合意することを困難にする場合がある。

- ・政府は、研究セキュリティに関心を持つ省庁や部署をまとめる調整機構を設けることができる。このような機構は、協議とコミュニケーションにおいて重要な役割を果たすとともに、関連の政策に助言を与え、監視することができる（6.1.1 と6.1.3 の例を参照）。
- ・教育・科学・イノベーションを担当する省庁は、研究エコシステムの様々な主体（研究資金配分機関・研究機関・大学・学術研究コミュニティ）間の協力と情報交換を奨励すると同時に、他の政府機関と緊密に連携する必要がある（6.1.3の例を参照）。
- ・研究機関や大学は、研究セキュリティの問題と自らが直面している事例に関する情報を、自らの機関内にとどまらず、他の研究機関や研究エコシステムのステークホルダーと共有すべきである。（6.4と6.7の例を参照）。

別欄2.1 研究インテグリティとセキュリティに関わる政策分野

国民保護
サイバーセキュリティ
防衛・情報
教育
海外投資
出入国管理
イノベーションと知的財産権（IPR）
法執行
プライバシーとデータガバナンス
科学
貿易・輸出管理

2.7 研究インテグリティとセキュリティに関する国際的な情報交換を強化する

科学の進歩は、国際協力とデータや情報の開かれた共有に依存している。研究インテグリティとセキュリティに関する相互理解の構築と集団的アプローチの強化に向けた協力は、すべての国に最善の利益をもたらす。

- ・ 政府・研究資金配分機関・研究機関・大学は、研究インテグリティとセキュリティにおける課題と優れた実践例について情報を交換すべく、国際的な対話の場を設ける必要がある（6.8の例を参照）。
- ・ 各国政府・研究資金配分機関・研究機関・大学間で科学協力協定を策定する際は、研究インテグリティとセキュリティの問題を明示的に検討すべきである。
- ・ OECDや科学技術・イノベーション（STI）政策における権限を持つその他の国際機関は、各国と協力し、研究インテグリティとセキュリティ、国際協力に関する情報交換と政策立案を促進すべきである（6.8の例を参照）。

3 | イントロダクション

科学的発見は、世界中の知性・ノウハウ・才能・資金・インフラを合わせて活用する相互に関連した学際的で国際的なエコシステムの中で起こる。科学研究における自由と国際協力は科学の進歩の基礎となるものである。科学的な情報とデータのオープンで透明性の高いコミュニケーションと普及、研究資料の共有は、グローバルな科学エコシステムが効果的に機能する上で不可欠である。

しかし、オープンな研究環境を自らの利益のために不当に利用し、歪めようとする動きを一部の政府や非国家主体が強めており、新たな課題と脅威が生まれつつある。現在、多くのOECD加盟国は、公的研究における不正な情報伝達や外国の干渉を、国家と経済に対する重大な安全保障上のリスク、科学研究の自由に対する脅威と捉えるようになってきている（JASON, 2019^[1]; D’Hooghe and Lammertink, 2020^[2]; Australian Security Intelligence Organisation, 2020^[3]）。このことは、国際協力、研究者養成、人材採用、助成金申請のピアレビューなど、研究の中核となる幅広い活動において重要な意味を持つ。安全保障上のリスクは、慎重に管理されなければ、国際的な研究エコシステムの健全性と有効性を著しく損ない、研究成果に対する信頼性を低下させかねない。

こうした懸念を受け、OECDグローバル・サイエンス・フォーラム（GSF）は、2020年に「グローバルな研究エコシステムにおけるインテグリティとセキュリティ」に関するプロジェクトを立ち上げることに合意した。このプロジェクトは、研究の自由を守り、国際研究協力を推進し、開放性と無差別性を確保しつつ、国家と経済の安全保障を確保するための優れた実践例の特定を目的としていた（付託事項全文については付属書Bを参照）。国際専門家グループは、プロジェクトを監督し、情報や事例の収集に協力した。国別情報については、一般に入手可能な文書の机上分析に加え、各国政府・研究資金配分機関・研究機関・大学・国際研究プロジェクト・国際協力インフラ・学協会における優れた実践例に焦点を当てた2回の専用国際ワークショップがこれを補完している。

研究インテグリティは優れた研究実践や科学者個人の行動と同義であるため、倫理や個人の不正行為（捏造・改ざん・盗用等）の防止といった様々な問題を包含することができる。しかし、本プロジェクトでは研究エコシステムのインテグリティの強化に注目し、特に国家と経済の安全保障上の脅威と科学研究の自由に対する外国の干渉を軽減することに重点を置いている。また、インテグリティとセキュリティへのリスクに対するグローバルな研究エコシステムの強靱性を高めるに当たり、政府（研究担当省庁等）と公的研究提供者（研究機関や大学等）の役割と責任にも焦点が当てられている。その際、本プロジェクトは国を問わないことを旨としており、国家安全保障上のリスクに対する見識は経時的に変化する地政学的要素の影響を受けることが認識されている。

本報告書は、エグゼクティブサマリーに続き、前章（第2章）が政策提言という構成になっている。また、簡単なイントロダクションと用語解説に続き、本報告書の残りの部分では、これらの提言の背景と根拠について説明している。第4章では、国際研究協力がどのように増加し、科学と社会に貢献しているかを探り、国際研究協力の既存の枠組みについて簡単について要約している。第5章では、本報告書の3つの重要な相互作用テーマである研究インテグリティ・研究セキュリティ・国際協力と、各国が懸念している安全保障と外国の干渉との関係を検討している。第6章では、研究インテグリティとセキュリティの懸念に対して各国が実施している政策や行動を紹介している。

別欄 3.1 用語集

研究インテグリティ、研究セキュリティ及び関連の概念について議論する際の課題の一つは、国やコミュニティによってそれらの定義が異なることである。共通の理解を築き、誤解を避けるためには、重要な用語の定義を共有することが重要である。本報告書で使用している「作業上の定義」を以下に要約する。これらの重要な用語のニュアンスや多様な視点からの考察は付属書 A に示している。

利益相反（COI）と責務相反（COC）

利益相反とは、一次的利益に関する専門的な判断や行動が、二次的利益によって不当に影響を受ける危険性がある一連の状況である（American Association of University Professors, 2014^[4]; UK Research and Innovation, n.d.^[5]）。責務相反とは、個人が複数の雇用主から過剰な量の仕事や相反する職務を引き受ける状況である（Office of Science and Technology Policy, 2020^[6]）。

有害な研究慣行

有害な研究慣行とは、研究事業の伝統的な価値観に違反し、研究プロセスに有害な影響を及ぼす可能性のある行為である（Committee on Responsible Science et al., 2017^[7]）。有害な研究慣行には、虚偽表示、注意義務違反、不正行為の申し立てへの不適切な対応等が含まれる（Purdue University, n.d.^[8]）。窃盗・欺瞞・強制は、研究セキュリティとの関連でより直接的に懸念される有害な研究慣行である（第5章を参照）。

懸念されるデュアルユース研究

懸念されるデュアルユース研究とは、研究自体は有益な目的のために行われていても、意図的に害を与え、公衆衛生や国家安全保障を脅かすために利用され得る知識や技術が生まれることが（現在の理解に基づき）合理的に予想される研究である（Public Safety Canada, 2020^[9]; BBSRC, MRC and Wellcome Trust, 2015^[10]）。

デューデリジェンス

デューデリジェンスとは、ある組織との取引に備えて行われる、当該組織の分析のことである（Merriam-Webster, n.d.^[11]）。国際研究協力の場合、デューデリジェンスではパートナーの過去の活動とその事業分野、その運営組織の商業的・倫理的地位、そして法的環境と規制環境が調査される（Universities UK, 2020^[12]）。

科学研究の自由

科学研究の自由には、研究課題を自由に定め、理論を選択・開発し、実証的資料を集め、健全な学術研究方法を考案・採用し、従来の考え方の正誤を問い、新しい考え方を提案する権利が含まれる。これには、研修や教育による場合も含め、研究成果を広く共有し、普及させ、発表する権利も含まれる。研究者が自身の仕事環境や政府・機関の検閲・差別による不利益を被ることなく、自分の意見を発表する自由でもある。専門的又は代表的な学術団体や関連の学術会議に参加する自由もある（Ministerial Conference on the European Research Area, 2020^[13]）。

外国の干渉 vs 外国の影響

外国の干渉は、外国の主体によって、又は外国の主体に代わって行われ、対象となる国家の主権・価値・利益に反する行為である。それは、強制的、非公然、欺瞞的又は腐敗的でもある。通常的外交関係の一環として、オープンで透明な方法で行われる外国の影響とは対照的である（University Foreign Interference Taskforce, 2021^[14]）。干渉と影響を区別することは状況によっては有益であるが、両者の境界線は必ずしも明確ではない。

知識のセキュリティ

知識のセキュリティとは、知識や技術の不正な移転を防止すること意味する。また、科学研究の自由を直接的又は自主規制によって損なうような、高等教育と研究への国家主体による非公然の影響を防ぐことも含まれている。

オープンサイエンス

オープンサイエンスとは、研究者・政府・研究資金配分機関・科学コミュニティが、研究を加速させる手段として、公的資金による研究の成果の主要なアウトプットである出版物と研究データを、デジタル形式により、無制限又は最小限の制限で一般公開する取組と定義できる（OECD, 2015^[15]）。広義では、オープンサイエンスの一環として、科学と社会とのより密接な関係が強調される。

互恵性

互恵性とは、すべての共同研究パートナーに利益をもたらす方法により、研究材料・成果物・知識を共有することである。互恵性は、協力を報いる能力やその利益を活用する能力において研究パートナー間に非対称性がある場合でも、協力が相互に有益であることを保証するものであり、効果的な協力には必須である。

研究エコシステム

研究システムには、研究資金提供者、各種の研究機関や大学、個々の研究者など、様々な主体が関与している。これらの主体は相互依存の関係にあり、ダイナミックなエコシステムの中で共に行動している。政策的枠組み、公式又は非公式な規則、規範、基準はすべて、ローカルからグローバルに至る様々な規模で運営される研究エコシステムのガバナンスにおいて重要な要素である。グローバルな研究エコシステムは、異なる国益を持つ異なる国の主体間の相互作用によって特徴づけられる。

研究インテグリティ

研究インテグリティは、研究の倫理を意味する包括的な用語である (Sutrop, Parder and Juurik, 2020^[16])。インテグリティは研究者個人のみならず、研究機関や研究エコシステム全体についても考えられる。本プロジェクトでは、「研究インテグリティ」とは、優れた科学的実践（科学研究の自由、開放性、誠実性、説明責任等）を構成し、国際研究協力を規制する特定の価値・規範・原則（互惠性、公平性、無差別等）を特に意味する。これらは、個々の研究者、研究機関、社会システムとしての科学、そして研究プロセスの各段階に適用される（図2.1 研究インテグリティと研究セキュリティを参照）。

研究不正

研究不正とは、狭義には、研究の提案、実施、審査又は研究結果の報告における捏造・改ざん・盗用（FFP）と定義することができる。捏造とは、虚偽のデータや結果を作り出し、それを記録・報告することである。改ざんとは、研究材料・機器・プロセスを操作したり、データや結果を変更・省略したりして、研究内容を正確に記録しないことである。盗用とは、適切なクレジットを与えることなく、他人のアイデア、プロセス、結果又は言葉を流用することである（Office of Science and Technology Policy, 2000^[17]）。

研究セキュリティ

グローバル化した研究エコシステムにおいて、研究セキュリティの確保とは、望ましくない外国の国家や非国家による研究への干渉を防ぐことを意味する。研究セキュリティの主な目的は、研究エコシステムを保護し、それにより、正当な国益と経済的利益を保護することにある（図2.1 研究インテグリティと研究セキュリティを参照）。

科学外交

科学外交は、科学と外交の接点に位置する一連の行動と広く理解されている。科学外交は次の3つの事象に分類されてきた。「外交のための科学」：外交目的を推進するための科学の利用、「科学のための外交」：科学技術の進歩を促進するための外交の利用、「外交の中の科学」：外交プロセスへの科学又は科学的主体の直接的関与（European Union Science Diplomacy Alliance, n.d.^[18]）。

4 | 国際協力—グローバルな研究エコシステムの重要な要素

国際協力は、科学が機能する上で不可欠な要素である。OECD 諸国では、国際協力が関わる科学論文の割合は、2006年の20%から2020年に28%に増加しており、これはすべての科学分野で同様である（図4.1 国際共著による科学論文の割合（OECD、2006年及び2020年）を参照）（OECD, 2021^[19]; n.d.^[20]）。

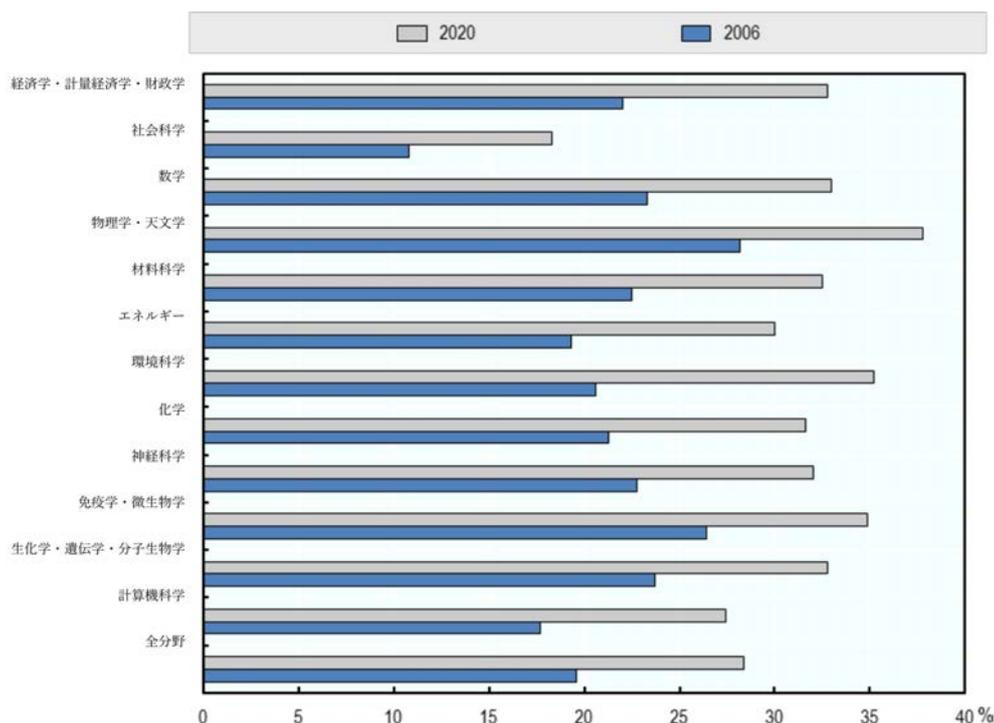


図4.1 国際共著による科学論文の割合（OECD、2006年及び2020年）

備考：この図は異なる国の研究機関の間で共著された科学論文の割合を示している。

出典：Scopus Custom Data, Elsevier, Version 5.2021, September 2021 をもとに OECD が算出（OECD, 2021^[19]; n.d.^[20]）。

COVID-19のパンデミック、気候変動、その他の社会経済的課題のようなグローバルな問題は、国際研究協力なしには取り組むことはできない。COVID-19のパンデミックに対する世界的な対応は、国際協力の重要性を実証している。このことは、図4.2 COVID-19の生物医学研究に関する国際科学協力（2020年1月～11月30日）と図4.3 医学研究論文の総数（分数カウント）から選定した主要経済圏とそれらの上位5つのパートナー経済圏（2020年1月1日～11月30日）（OECD, 2021^[21]）に示されている。また、これらの図は、政府の地政学的・イデオロギー的立場に関わらず、異なる国の研究者が共同で研究に参加しており、科学協力が一般的には非政治的な活動であることを示している。オープンサイエンスと国境を越えた研究データや情報の共有は、科学的にパンデミックに対処する上で必須となっている（OECD, 2020^[22]）。

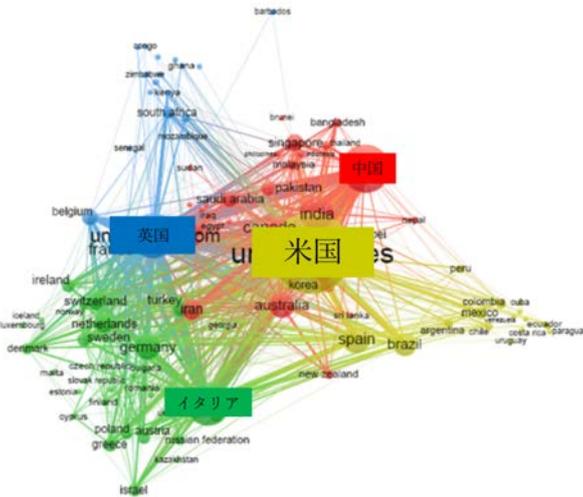


図4.2 COVID-19の生物医学研究に関する国際科学協力（2020年1月～11月30日）

備考：項目間の線は経済圏間の協力関係を表す。2つの経済圏の距離は、共著の実績から見た両経済圏の関連性を示している。一般的に、2つの経済圏の位置が近いほど、両者の関連性は強くなる。詳細な方法論については、<https://doi.org/10.1787/888934223099>を参照。PubMedにおけるCOVID-19の論文投稿で大勢を占めているのは米国と中華人民共和国（以下、中国）である。両国は互いに主要な共同研究のパートナーでもある。COVID-19に関する国際研究協力が大きく関わっている他の経済圏には、英国、ドイツ、フランス、イタリア、オーストラリア、カナダ、インドが含まれる。

トルコ共和国による注:本文中の「キプロス」に関する情報はキプロス島南部に関するものである。同島には、トルコ系とギリシャ系のキプロス人の双方を代表する単一の当局は存在しない。トルコは北キプロス・トルコ共和国（TRNC）を承認している。国連の枠組みにおいて永続的かつ公平な解決策が見いだされるまで、「キプロス問題」に関するトルコの見解に変更はない。

すべてのOECDに加盟する欧州連合加盟国及び欧州連合による注：キプロス共和国はトルコを除くすべての国連加盟国によって承認されている。当文書に記載されている情報は、キプロス共和国政府の実効支配下にある地域に関するものである。

出典：OECD Science, Technology and Innovation Outlook 2021、米国国立衛生研究所PubMedデータ<https://pubmed.ncbi.nlm.nih.gov/>（2020年11月30日にアクセス）をもとに作成。（OECD, 2021^[21]）

StatLink <https://doi.org/10.1787/888934223099>

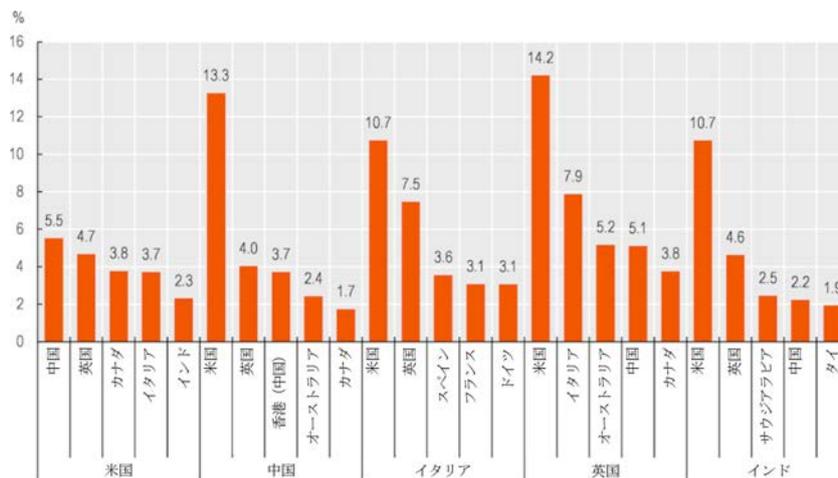


図4.3 医学研究論文の総数（分数カウント）から選定した主要経済圏とそれらの上位5つのパートナー経済圏（2020年1月1日～11月30日）

備考:2020年1月1日から11月30日までの対象期間中に74,155件の論文が登録されている。米国の共著による論文は16,964件。そのうちの84%は国内での共著、残りは国際協力によるものである。米国の共著相手国のトップは中華人民共和国（以下、中国）であり、米国と中国の共同研究による論文は、米国におけるCOVID-19関連の医学研究論文の5.5%を占めている。

出典：OECD Science, Technology and Innovation Outlook 2021、米国国立衛生研究所（NIH）PubMedデータ<https://pubmed.ncbi.nlm.nih.gov/>（2020年11月30日にアクセス）をもとに作成（OECD, 2021^[21]）

StatLink <https://doi.org/10.1787/888934223479>

4.1 国際的な科学交流と協力のための多国間枠組み

国際協力は科学研究の本質的な部分を構成しており、その旨が国際的組織の公式・非公式な提言や宣言の多くに明記され、これを推進すべき理由とその方法の基礎を提供している（表4.1 国際的な科学交流と協力のための多国間枠組みを参照）。これらの国際的な原則や規範は世界的（国連、ユネスコ、OECD）に又は地域的（EU）に、大多数の国によって承認されている。

表4.1 国際的な科学交流と協力のための多国間枠組み

提言／宣言	主な重点項目
経済的、社会的及び文化的権利に関する国際規約（United Nations Human Rights Office of the High Commissioner, 1966 ^[23] ）	締約国は「科学と文化の保存・発展・普及を確保する」ために行動しなければならない。また、締約国は「科学的研究及び創造的活動に不可欠な自由」を尊重することに合意するとともに、「科学的及び文化的分野における国際的な接触及び協力の奨励及び発展から得られる利益」を認識する。
科学と科学者に対する提言（UNESCO, 2017 ^[24] ）	各国に対し、「他の権利を尊重した上で協力的なオープンサイエンスのメカニズムを確立・推進し、科学的知識の共有を図る」ことが推奨されている。
オープンサイエンスに関する国連教育科学文化機関（ユネスコ）提言（UNESCO, 2021 ^[25] ）	各国は、機関・国家の効果的なオープンサイエンス政策と、既存の国際法及び地域法と整合性のある法的枠組みを策定することが奨励されている。
科学技術国際協力に関する理事会勧告（OECD, 2021 ^[26] ）	勧告では、加盟国は、相互の利益となる科学技術の移転を図り、経済・社会の進歩を阻む障壁を排除することの重要性を強調すべきとされている。また、署名国は、協力的なプロジェクトを推し進め、加盟国間で学生や科学者の交流を奨励し、海外の科学者や技術者による基礎研究施設の利用に便宜を図り、基礎研究の成果の普及を推進することに合意している。 勧告の中で各国は、「科学技術における国際協力に当たり、科学的価値や規範（研究インテグリティ、科学的調査や表現の自由等）について調和のとれた理解を確立すること」が求められている。また、「科学技術の国際協力に伴うリスクを軽減し、それに対処することにより、相互利益を念頭に協力の有効性と効率性を高める」ことも強調されている。
対企業及び企業間の国際技術協力の促進に関する理事会勧告（OECD, 2022 ^[27] ）	データの漏洩や窃盗、技術移転の強制、研究資源の搾取、デュアルユース技術の悪用など、国際技術協力に伴うリスクを防止・軽減するための適切な措置を講じつつ、効果的かつ効率的な技術協力を阻む障壁を最小化することが推奨されている。また、効果的なリスク管理と適切な規制環境を考慮しつつ、新規及び新興技術の利用と応用のための国際的なガバナンスの枠組みを開発するに当たり、企業・大学・公的研究・市民社会間の協力を支援することが加盟各国に奨励されている。
公的資金による研究データへのアクセスに関する理事会勧告（OECD, 2021 ^[28] ）	データ及びその他の研究関連デジタルオブジェクト（メタデータ・アルゴリズム・ワークフロー・モデル・コード等のソフトウェア）を広く共有することが提唱されている。
ニューロテクノロジーにおける責任あるイノベーションに関する理事会勧告（OECD, 2019 ^[29] ）	ニューロテクノロジーに関するデータの共有に向けた共同インフラと環境を構築することにより、科学的な協力を促進し、オープンサイエンスの国際文化を支援することが各国に求められている。
人工知能に関する委員会の提言（OECD, 2019 ^[30] ）	AIに関する知識を共有し、国際的な取り組みを推進することが望ましいとされている。
規約・手続規則（International Science Council（ISC）, 2018 ^[31] ）	国際学術会議（ISC）は「科学とその恩恵にアクセスする公平な機会を推進するとともに、民族的出自・宗教・国籍・言語、政治的又はその他の意見、性別・性自認・性的指向・障害・年齢等に由来する差別に反対する」ことを宣言している。180カ国の国立アカデミーとあらゆる研究分野を代表する科学連盟で構成されるISCの全メンバーは、科学の普遍性を維持することを宣言しており、その一例として、政治的禁輸に直面している国家間での科学者の移動を支援してきた。

科学研究の自由に関するボン宣言 (Ministerial Conference on the European Research Area, 2020 ^[13])	欧州連合（EU）の研究担当大臣とイノベーション・研究・文化・教育・青年担当の欧州委員会委員は <i>科学研究の自由に関するボン宣言</i> （Ministerial Conference on the European Research Area, 2020 ^[13] ）を採択した。宣言は表現の自由、結社の自由、移動の自由、教育を受ける権利など、科学研究の自由を保護することを署名者に約束させている。
研究・イノベーション（R&I）分野における国際協力に関するマルセイユ宣言（French Presidency of the Council of the European Union, 2022 ^[32] ）	EUの高等教育・研究・イノベーション担当大臣は、国際的な研究・イノベーション・高等教育の協力において、科学研究と学問の自由を促進・保護するとともに、国際協力の伴う安全保障上のリスクに対処し、これを管理するための措置を講じることに同意している。
研究インテグリティに関するシンガポール声明（World Conference on Research Integrity, 2010 ^[33] ）	この声明は、異なる国や文化的背景における研究インテグリティを検討し、詳細なガイドラインと実践を展開するための規範的な基礎を提供している。また、研究インテグリティの主要な原則と、それに伴う研究者の責任を定義している。4つの原則とは、誠実性、説明責任、専門家としての礼儀と公平性、そして優れた管理である（詳細は付属書Aを参照）。これらの原則又はそのバリエーションは、研究インテグリティに関する他の多くの国際的又は国内的な宣言・規約・ガイドラインで取り上げられている（The All European Academies（2017 ^[34] ）、Science Europe（2016 ^[35] ）、the InterAcademy Partnership（IAP）（2016 ^[36] ）等）。

最近改訂された*科学技術国際協力に関する理事会勧告*（OECD, 2021^[26]）と*マルセイユ宣言*（French Presidency of the Council of the European Union, 2022^[32]）が、国際協内に在するリスクに対処する必要性を具体的に述べている点は注目に値する。しかしながら、これらの勧告は全体として、科学研究の自主性と自由を尊重しつつ、研究におけるオープンで包摂的な国際協力の価値と、そのような協力を支援する政府の役割を強調している。こうした様々な国際的合意に記載されている価値観や規範、活動は、国や機関レベルのガイドラインや規約の多くに反映されており、グローバルな研究エコシステムの運営を主に支配している。

5 | 研究プロセスへの外国の干渉

国際的な科学協力や交流における、国家や経済の安全保障への脅威を懸念する国が増えている。これらの脅威は、不正な情報伝達や技術移転、知的財産の窃盗にとどまらない可能性がある。特に、大学キャンパス内で研究者が脅迫され、その結果、弱い立場の人間が窃盗やスパイ活動を強要されることが懸念されている。人文・社会科学（SSH）の研究者が、国家主体から特定のテーマに関する研究の回避や通信の検閲を強要されることがある。特に研究者が無力で支援されていないと感じる環境におかれている場合、国家の干渉に対する恐怖が自己検閲の原因となることがある。こうした干渉は研究の実施と管理に影響を与えるが、同様に、脅威とそれに対する過度な対応の両方が、研究インテグリティと研究の基本原則・規範を損なう可能性も懸念されている。

一般に、国家安全保障の担保又は核不拡散義務の履行を目的とした軍備と原子力技術等に適用される輸出管理制度は各国で十分に整備されている。従来の輸出管理制度は、主に機微技術を対象としており、この点から、化学・生物・放射線・核・爆発物技術に関する研究をデュアルユースと定義することが各国政府で常態化している。関連のデュアルユース技術を含む軍備の開発は、多くの国際的な法的合意の対象となっている（United Nations, 2013^[37]; 1968^[38]; 1972^[39]）。

データ・情報・ノウハウといった無体物の移転や、特定の実用的な目的なしに行われる科学研究を規制することは容易でない。基盤的研究は、伝統的に輸出管理の対象外とされてきた（Government of the United Kingdom, 2021^[40]）。同時に、基礎研究の多くの分野から得る知識が、潜在的にデュアルユースと考えられることも認識されている。例えば、人工知能（AI）や量子コンピュータは、民生・軍事の双方に利用される可能性があると同時に、企業・国家・地域間の激しい経済競争の対象にもなっている。伝統的な法律では知的財産権が保護されている。しかし、インターネット時代にデータ・情報・ノウハウを保護することは容易でない。また、アクセス制限は研究インテグリティの原則とオープンサイエンスに相反する可能性がある。

オープンで信頼に基づく科学的協力と、保護的であっても潜在的に制限的な規制との間のバランスを保つことは各国にとって大きな課題となっている。また、過剰規制や過度の干渉は科学研究・交流の自由に影響を与える一方、国際的な規制や規範が共有・尊重されていないと、研究が不正利用されるだけでなく、法的・倫理的制約のない国において特定の研究が選択的に実施される可能性がある。政府による干渉を受けずに、信頼できる国際協力と開かれた意見交換を促進すべく、世界共通の取組に向けた政策が求められている。

5.1 研究インテグリティ・研究セキュリティ・国際研究協力の関連性

研究インテグリティは、優れた科学的実践を構成するとともに国際研究協力を規制する価値観・規範・原則（前者については、学問の自由、開放性・誠実性・説明責任等、後者については、互惠性・公平性・無差別性等）の上に築かれるものである。研究セキュリティは、研究エコシステムと国家安全保障及び経済的利益を、外国の国家や非国家等の外部の干渉から保護することを目的としている。研究インテグリティと研究セキュリティは、いずれも研究エコシステムを保護する上で不可欠である（前出図2.1 研究インテグリティと研究セキュリティ参照）。COIとCOCの特定と管理は、研究セキュリティにとって重要であり、研究インテグリティの向上にもつながる。

オープンな国際協力、研究インテグリティ、研究セキュリティの間でバランスをとることは、政府・研究資

金配分機関・研究機関・大学・学協会、個々の研究者など、研究エコシステムに関わるすべてのステークホルダーにとっての課題となっている。

5.2 有害な研究慣行

個人の研究不正は、一般的に改ざん・捏造・盗用（FFP）や様々な「疑わしい」研究行為と関連しているが、研究セキュリティとの関連でより直接的に懸念される「有害な慣行」は他にも数多くある（Australian Security Intelligence Organisation, 2020^[3]）。これらは、個人又は組織の行動のレベルでしばしば発生するが、外国の国家又は非国家主体の利益によって動機づけ及び／又は支援されることが典型的である。また、研究機関や大学間での国際協力やパートナーシップが直接関わる場合もある。

OECD加盟国の多くで懸念されている有害な慣行について以下で説明する。

5.2.1 データ・サンプル・ノウハウの窃盗又は悪用

国際協力や交流における窃盗を各国が懸念している。窃盗とは、主任研究者や受入機関の許可なく、データ・サンプル・ノウハウ等を取得することである。窃盗は、物理的又はサイバー的な様々な方法で行われ、利益相反や責務相反にも関連する可能性がある。

共同研究は外国の組織や機関によって悪用される可能性がある。外国のパートナーは、研究パートナーシップや共同活動への参加を悪用して知識・成果・技術にアクセスし、不当な経済的利益を得るために利用したり、悪意のある用途に悪用したり、損害を与えるために悪用されることがある（BBSRC, MRC and Wellcome Trust, 2015^[10]）。外国のパートナーによる不正利用は、評判を損なうのみならず、機関・国家の経済的損失の原因となる可能性がある。

別欄 5.1 事例研究 — 研究における窃盗

日常的な研究活動で発生し得る研究インテグリティとセキュリティのリスクを説明すべく、いくつかの国では事例研究が実施されている。これらの事例は、匿名又は架空のもので、研修や意識向上に利用できる身近なシナリオを取り上げている。

研究における窃盗

ある研究者が、複数の医学研究所に勤務し、企業秘密を盗み、外国政府からの報酬を受けた後に外国に譲渡した。また、その研究者は、盗んだ企業秘密をもとに医療キットを製造・販売する会社を立ち上げた。彼女は起訴され、30カ月の実刑判決を受け、300万ユーロの賠償金を支払い、さらに資産を没収されることになった（Department of Justice, 2021^[41]）。

内部の脅威

ある大学の研究者は、勤務する大学で3人の博士課程学生を指導する責任を負っている。彼女は、学生たちの作業スケジュールを助けるため、研究棟や実験室への24時間365日の出入りを許可している。ある夜、彼女が研究室に戻ると、ひとりの学生が、その学生とは無関係の研究データやメモに目を通していた。その情報は、他のチームメンバーによって保護されずに保管されていた。もしそれが機微または秘密の情報であれば、彼女と彼女の研究チームは、研究から得られる可能性のある個人的・職業的又は経済的・商業的利益を失う危険性があった。彼女のチームの評判やキャリアにも悪影響を及ぼす可能性がある（Government of Canada, 2021^[42]）。

犯罪的ハッカーによる悪用の可能性

提案されている研究プロジェクトは、コンピュータープログラム、特に無線ルーター・スマートフォン・ノートパソコンのOSの脆弱性をAIによって体系的に特定し、自動防御対策を開発することを目的としている。この研究プロジェクトの成果は、これらのコンピュータープログラムを定期的に監視・更新する必要があるあらゆる場所で役立つものと思われる。同時に、この成果は、定期的に監視・更新されない多数の機器に存在する脆弱性を特定し、悪用することも可能にするであろう（German National Academy of Sciences Leopoldina, n.d.^[43]）。このプロジェクトに内在するリスクを効果的に管理するにはどうすればよいか？

出典：病院の研究者が企業秘密を盗んで中国に売ることを共謀して実刑判決（Department of Justice, 2021^[41]）；シナリオ3 - インサイダーの脅威と研究の窃盗（Government of Canada, 2021^[42]）；セキュリティ関連の研究テーマと事例研究に関する情報（German National Academy of Sciences Leopoldina, n.d.^[43]）

5.2.2 欺瞞的行為

欺瞞的行為には、意図的な情報の隠蔽や省略が含まれる。外国からの又は商業的な報酬や提携の隠蔽は、しばしば利益責務や責務相反に関わる欺瞞的行為と認識されている。例えば、雇用を求める外国人学者は、母国の機関との関係やビザ当局が関連があると考えた情報を申告しないようにしたくなる可能性がある（JASON, 2019^[1]）。

研究者の主たる雇用主に申告することなく、他の機関及び／又は外国でサテライトラボやグループを運営することも欺瞞的行為とみなされる可能性がある。また、主な所属機関の規則や指導に反し、同機関の資料をサテライトラボに提供する行為は、関係者が直ちにそう判断するとは限らないが、窃盗である（JASON, 2019^[1]）。

二重取りは欺瞞的行為の特殊な形態である。研究者は、既に完了している、または他の団体、場合によっては他国によって資金提供されている研究を実施するとして、受入機関に対する資金提供を申請することにより、「二重取り」をすることがある（Office of Science and Technology Policy, 2020^[6]）。この場合も、二重取りと、密接に関連した研究を支援する複数の資金提供者が存在することがある通常の研究資金調達プロセスとの境界線を定義することは必ずしも容易でない。

外国人留学生は、外国の治安部隊や企業との関係など、責務相反を隠しながら大学に入学することができる。このような場合、大学は、国家や経済の安全保障を損なう可能性があることに気づかずに、そのような人材を教育することがある（Parliamentary Joint Committee on Intelligence and Security, 2021^[44]）。同様に、研究機関や大学は、利益相反や責務相反を申告していない海外人材を採用する可能性がある。このようなことから、移動の奨励や海外人材の採用を目的とした特別なプログラムが多くの国で提供されており、その中には強制的行為につながるような条件を含むものがあることに注意が必要である（次節参照）。

また、科学的なアイデアや研究成果に対する正当な謝辞を述べないことも欺瞞的行為である。これは、伝

統的に科学論文の著者権に関連して、研究インテグリティの重要な側面として認識されてきた。しかし、研究セキュリティの観点からは、このような行為は窃盗に等しいような広範な意味を帯びてくる。

別欄 5.2 事例研究 – 欺瞞的行為

日常的な研究活動で起こりうる研究インテグリティとセキュリティに対するリスクを説明するために、いくつかの国で事例研究が実施された。これらの事例は、匿名又は架空のもので、研修や意識向上に利用できる身近なシナリオを取り上げている。

海外からの資金提供及び海外の所属先の不開示

国の研究資金配分機関から資金提供を受けている研究者が、その機関の申請・授与方針に基づいて申告することが求められていたにもかかわらず、資金提供の申請書の中で、海外からの資金と海外の所属先に関する情報を一切申告していなかった。そこで、研究資金配分機関が召喚状を発行し、その研究者は、外国の人材採用プログラム申請書の一部を含むいくつかの文書を提出したが、十分な情報が得られなかった。研究資金配分機関は、研究者が召喚に応じなかったことを考慮し、研究者が所属する大学への授与を停止するとともに、研究者に政府全体の資格停止処分（評価者・アドバイザー・コンサルタントとしての活動の禁止を含む）を一定期間課した（National Science Foundation, n.d.^[45]）。

外国の軍事大学での雇用

ある工学・情報技術分野の教授は、主な所属機関で農業応用を目的とした群集システムの公的資金プロジェクトに取り組んでいた。その彼が、海外の軍事大学に教授として所属していることがメディアで報じられた。彼は、海外の大学での自分の役職を主な所属機関に申告していなかった（Department of Education, Skills and Employment, 2021^[46]）。

出典：研究セキュリティ（National Science Foundation, n.d.^[45]）；シナリオ2 - 外国の人材採用プログラムへの参加（Government of Canada, 2021^[47]）；事例研究 - デューデリジェンス、リスク評価と管理（Department of Education, Skills and Employment, 2021^[46]）

5.2.3 強制的行為

海外で研究している奨学生が、研究活動の内容を報告しなかったり、母国のために情報を収集しなかったりした場合、奨学金や研究助成金の打ち切り、母国の家族への脅迫といった形で強制されることがある。外国人研究者は、研究資源・名声・特権の剥奪といった脅迫により、受入国又は受入機関から強制されることもある。研究者が他国で活動している期間中に、ある国の情報機関や安全保障機関への協力を求める規則は、法的措置の脅威を伴う強制の一形態である（JASON, 2019^[1]）。このような規則は、一部の人材採用プログラムに適用されている。強制的行為は、利益相反や責務相反を生み出し、個人がこれらの相反を申告することを非常に困難にする可能性がある。

強制的行為は、科学研究の自由を侵害する可能性がある。ある国は、既存のパートナーシップの制限又は解消といった脅迫を行うことにより、外国研究者がその国にとって機微な研究を行うことを抑制するかもしれない（Bekkers, Oosterveld and Verhagen, 2019^[48]）。また、その国は、人権状況に関する情報など、現地の情報へのアクセスを制限することもあり、人文・社会科学（SSH）の研究分野によっては特に課題となる場合がある（Tardell, 2021^[49]；Human Rights Watch, 2021^[50]；Gattolin, 2021^[51]）。一部の外国人研究者の中には、自己検閲、特定の企業との協力、人材採用プログラムへの参加等について、母国政府から圧力を受ける人もいる。一方、一部の外国人研究者は、母国政府や外国の組織と協力していないにもかかわらず、受入国で排除や差別を受けていると感じている。

個人に加え、「独立した」研究組織や機関も同様に、国家の強い統制や影響下に置かれることがあり、法律や要件を根拠に、又は国内外での活動に対する国家支援の見返りとして、情報の共有を強制又は要求されることがある。OECD 諸国の大学には、研修や研究のために海外の機関と提携を結んでいるが、こうした機関が政治的及び／又は軍事的に強い影響力を受けている事実を見逃している例がある。同様に、このような組織的なパートナーシップは、文化の重要な違いに対応する必要が往々にしてあり、優れた倫理的慣行や科学研究の自由が十分に配慮されるとは限らない。このようなパートナーシップは、機関やその職員、学生にとって、問題となる利益相反や責務相反を生み出す可能性がある。

別欄 5.3 事例研究 — 強制的行為

日常的な研究活動で起こりうる研究インテグリティとセキュリティに対するリスクを説明するために、いくつかの国で事例研究が実施された。これらの事例は、匿名又は架空のもので、研修や意識向上に利用できる身近なシナリオを取り上げている。

外国からの出版妨害

ある教授が、COVID-19に対する外国の対応について論文を発表し、将来の悲惨な状況を予測した。すると、その国の領事館は、その論文が外国の政府を批判し、威信が傷ついたと主張し、論文の撤回と公式な謝罪を彼女の大学に要求してきた。その大学は、この論文の撤回と謝罪の要求を拒否した。その大学は、言論の自由と学問の自由に強くコミットしており、その研究と論文は徹底したピアレビューを受けているものと判断した (Department of Education, Skills and Employment, 2021^[52])。

外国の人材採用プログラムへの参加

ある教授が、海外の大学から、彼の専門分野の非常勤教授にならないかと打診された。外国の大学は、旅費は全額負担し、1年のうちの夏学期の3カ月間のみ、講義を行い、研究プロジェクトに参加すれば報酬を支払うと申し出た。もし、その教授がこの職に就いていたら、契約の条件として、あるいは外国の機関での勤務期間中に、秘密情報や商業情報の開示義務を負っていたか、又はそのように強制されていたかもしれない。彼の母国の政府は、外国の機関への任命は、主な所属機関にその旨報告することを推奨している (Government of Canada, 2021^[47])。

出典：事例研究 - ガバナンスとリスクフレームワーク (Department of Education, Skills and Employment, 2021^[52])

5.3 研究評価における課題

5.3.1 守秘義務違反

ピアレビューアーは、論文発表や助成金の支給前に秘密情報にアクセスし、外国政府を含む他の主体に、その情報を移転することができる (JASON, 2019^[1])。専有情報やデータの流用は、研究体制に関わる主体間の信頼関係のみならず、科学に対する国民の信頼をも損ねる可能性がある (Office of Science and Technology Policy, 2020^[6])。

5.3.2 ねじ曲げられた意思決定

一般的に、外国人査読者を含むピアレビューアーは、未発表の秘密情報に特権的にアクセスできる。これが個人的な利益のために利用される可能性があり、それは確立された研究インテグリティの原則に反する不正行為とみなされる。研究セキュリティの観点から、利益相反又は責務相反を有するピアレビューアーは、外国政府を含む外部の主体の利益のためにピアレビュープロセスにおける意思決定をねじ曲げる可能性がある。

別欄 5.4 事例研究 — 研究評価における課題

日常的な研究活動で起こりうる研究インテグリティとセキュリティに対するリスクを説明するために、いくつかの国で事例研究が実施された。これらの事例は、匿名又は架空のもので、研修や意識向上に利用できる身近なシナリオを取り上げている。

守秘義務違反

ある国立研究機関の著名な上級研究者は、COIとCOCに関連した守秘義務違反により、総額で100万ドルを超える4つの助成金を打ち切られた。国立研究資金配分機関による徹底的な調査の結果、その研究者が、同機関の方針に反して、複数の開示されていない海外の所属先を有していることが判明した。また、同調査の結果、その研究者は、査読者の氏名や査読スコアを海外の研究機関と度々共有し、ピアレビュープロセスの規定に違反していることも判明した。その研究者は、外国の人材採用プログラムに参加しており、それ自体は許容されることであった。しかし、人材採用プログラムへの参加は研究資金配分機関に開示されておらず、同プログラムの契約には非開示と問題行動の双方に関連する条項が含まれていた (National Science Foundation, n.d.^[45])。

5.4 サイバーセキュリティ

研究に関わるサイバーセキュリティは多くの国で大きな関心となりつつある。デジタル化が進む世界では、多くの公共機関や民間機関がサイバーセキュリティに関心を持っており、サイバーセキュリティに関する問題の多くは研究に限ったものではない（OECD, 2015^[53]）。この点を考えると、研究機関や大学は、厳格なリスク管理プロセスを採用するなど、公共インフラで受け入れられている最善の実践を展開し、ITインフラ・データ資産・関連活動のセキュリティを確保する必要がある（National Cyber Security Centre, 2019^[54]）。さらに、本来、国際的かつオープンな研究でありながら、しばしば機微で高価値のデータや情報を生成・利用する研究に関連する特定の関心領域がある。

サイバー攻撃は、大学や研究機関のデータやITシステムに被害を与え、研究データの消失や研究活動の停止につながる可能性がある（Canadian Centre for Cyber Security, 2020^[55]）。また、サイバー脅威の主体は、大学や研究機関の情報システムを利用して、他の組織を攻撃することもできる。COVID-19のパンデミックで激増したバーチャルミーティングはこうした攻撃に極めて脆弱である。

特に個人の研究者は、インターネットを使ってオープンでインフォーマルな交流を行い、セキュリティに十分な注意を払わないまま国際的なコミュニケーションを行うことが多いため、脆弱性は高いと言える。フィッシング攻撃は、個人情報などを盗んだり、コンピューティングシステムにランサムウェアを仕込んだりする最も一般的な攻撃のひとつである。フィッシングメールは、研究者を誘導し、秘密情報の送信、悪意のあるウェブサイトへのアクセス、感染した添付ファイルのダウンロード等を促すものである（Centre for the Protection of National Infrastructure (CPNI), n.d.^[56]）。

研究データや知識の物理的な窃盗は、研究者が主たる所属機関にいる場合でも起こりうるが、海外渡航時の方がリスクは高くなる可能性がある。国際的な移動が研究の重要な側面であることを考えると、これは特に懸念すべき問題である。渡航中、ホテル・会議室・交通機関等でデータや書類を盗まれることがある（U15 Group of Canadian Research Universities and Universities Canada, 2019^[57]）。会議中にUSBメモリーを使ってファイルを移転したり、メモリー経由で研究者のパソコンがコンピューターウイルスに感染したりすることもある（Centre for the Protection of National Infrastructure (CPNI), n.d.^[56]）。このように、IT機器に対する物理的な窃盗や妨害は、その後のサイバー攻撃の前兆ともなりえる。

別欄 5.5 事例研究 — サイバーセキュリティ

日常的な研究活動で起こりうる研究インテグリティとセキュリティに対するリスクを説明するために、いくつかの国で事例研究が実施された。これらの事例は、匿名又は架空のもので、研修や意識向上に利用できる身近なシナリオを取り上げている。

リモートアクセス情報

ある学術研究所の博士課程学生が、専門分野の海外学会に招待された。その学生は、農業ビジネス用ドローンの新しい機能に関する現在の研究について発表するよう依頼された。会期中、リモートアクセスのための情報が外国の主体に捕捉され、大学のシステムと学生の研究内容への恒久的なアクセスリンクが確立された。その結果、帰国後1カ月もしないうちに、この学生の研究が模倣され、試作品が市販されてしまった。また、そのドローン技術は、外国で軍事作戦にも利用されている（Department of Education, Skills and Employment, 2021^[58]）。

渡航中のデータの物理的窃盗

ある研究者が海外の国際会議に渡航し、研究内容を発表・議論した。その研究者は、自分のパソコンと研究関連の情報が入ったUSBキーを会場に持ち込んだ。会議中、彼は複数の海外パートナーと連絡を取り、彼のUSBキーを同僚のデバイスに接続することで情報やデータを交換した。もし、彼のデータや研究成果が不正使用された場合、その研究成果に対する評価は容易に他人のものとなっていた可能性がある（Government of Canada, 2021^[59]）。

出典：事例研究 - サイバーセキュリティ（Department of Education, Skills and Employment, 2021^[58]）；シナリオ5 - セキュリティと渡航（Government of Canada, 2021^[59]）

6 | 政策と行動

研究インテグリティとセキュリティに対する責任は、国際的な研究エコシステムに関わる多くの主体間で分担されている。これらの主体には、各国政府・研究資金配分機関・研究機関・大学・大学協会・学教会等が含まれる。研究インテグリティとセキュリティを保護すべく、これらの主体が現在実施している活動について以下で説明する。

ここで説明する事例の多くは、米国・オーストラリア・英国・カナダのものであるが、これらの国は研究セキュリティを監視し、その懸念を公にするという点で最も積極的に活動してきたと言える。しかし最近、COVID-19のパンデミックに関連した技術的主権をめぐる議論が、国家の資金による公的研究を誰が利用し、誰がそこから利益を得るかというより幅広い問題に波及するにつれ、他の国々も関与を深めている。

6.1 各国政府

6.1.1 政策と規制

国家と経済の安全保障上のリスクに対する懸念の高まりと、研究インテグリティと科学研究の自由を保護する必要性から、一部の政府は数年前から対策に乗り出している。例えば、2018年、米国司法省は、学術分野への脅威を含め、国家安全保障上の特定の脅威に焦点を当てた新しいイニシアチブの創設を発表した。米国で活動する個々の科学者や学者が起訴（必ずしも成功したわけではない）された事例はいくつかある（Department of Justice, n.d.^[60]; 2020^[61]; 2018^[62]; 2021^[63]）。米国連邦議会では、連邦研究助成金の申請時に、研究資金源の開示を認め、義務づける法案が可決されている（116th Congress, 2021^[64]）。また、米国政府は法執行機関と研究資金配分機関との間の協力の強化を求める大統領覚書を発表し、米国政府が支援する研究をさらに保護することをこれらの機関に指示している（The White House, 2021^[65]）。この覚書には実施ガイダンスが付属しており、次のようなことが述べられている：開示方針（潜在的な利益相反・責務相反に影響を与える可能性のある外部関与に関し、連邦政府から資金提供を受けた研究者が適切な情報を資金配分機関や研究組織に提供する）、監督と執行（開示要件違反の結果及び同違反に関する情報の機関間共有について、連邦政府機関が明確かつ適切な方針を設ける）、コンプライアンスを容易にする機関間標準開示要件とデジタル報告ツール、及び多額の連邦研究開発資金を得た研究組織が適切な研究セキュリティプログラムを維持できるような措置（The White House, 2021^[66]; National Science and Technology Council, 2022^[67]）。最新のガイダンスでは、政府全体の政策とプロセスを明確に統一すること、そして外国人嫌悪や偏見の助長を防ぐことが強調されている。

英国では、国家安全保障・投資（NSI）法により、英国の国家安全保障を損なう可能性のある特定の買収に国の政府が介入することが認められている（Department for Business, Energy & Industrial Strategy, 2021^[68]）。大学や公的研究機関が保有するものを含め、17の機微領域に属する英国の資産を市場に出す場合、売り手は政府に通知することが法律で義務づけられている。これらの機微領域（表6.1 機微技術・情報分野を参照）のほとんどは研究集約型であり、様々な官民研究パートナーシップが存在することが特徴的である。また、英国にはアカデミック・テクノロジー承認スキーム（ATAS）があり、特定の機微領域で大学院進学を目指す留学生にこれが適用される（Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office, 2013^[69]）。特定の国からの留学生は、英国でこれらの領域を

学ぶ前に ATAS の証明書を申請しなければならない。

英国の NSI 法が特定する機微領域は、他の国や地域の機関で特定されている安全保障上の機微領域とかなり重複している。一方、カナダでは、国際共同プロジェクトにおける潜在的な国家安全保障上のリスクを評価することが個々の研究者に求められており、*国際研究協力に対する国家安全保障ガイドライン*（Government of Canada, 2021^[70]）では、機微又はデュアルユースとみなされ、特に注意が必要な研究領域を特定している（表 6.1 機微技術・情報分野を参照）。また、この機微技術リストを補完する形で、ガイドラインでは、従来の規制品目規定の対象となる機微データが研究内容に含まれているか否かを評価することが研究者に求められている。

日本では従来、国内居住者への技術移転は輸出とみなされてこなかったが、外国の政府や企業の影響を受ける可能性のある国内居住者への機微技術の移転を、国が管理するようになっている。外国の政府や企業から多額の金銭的利益を得ているか、又はこれらと契約関係（雇用契約等）にある国内居住者は外国の政府や企業の影響を受ける可能性があることとみなされることになる。

一部の国には、外国の干渉を起こしやすと考えられる「要注意」国を特定している政策があるが、多くの国では、国にとらわれないアプローチをとっている。国別アプローチは、公的研究機関や大学のリスクマネジメントの主な取組の対象を、少数の国に絞れるという利点がある。しかし、特定の人々に対する偏見や文化的偏見、差別のリスクがこのアプローチには内在している。国にとらわれないアプローチでは、ある時点で要注意とされる国のリストが将来的に変わる可能性があること、また、通常は政治的同盟国とみなされる国同士のパートナーシップや協力にもリスクが伴うことが認識されている。

表 6.1 機微技術・情報分野

	機微領域・技術
国家安全保障・投資法（英国）	先端材料 先端ロボティクス 人工知能 民生原子力 通信 演算処理装置 政府への重要なサプライヤー 暗号化認証 データインフラ 防衛 エネルギー 軍事・デュアルユース 量子技術 人工衛星・宇宙技術 非常事態対応サプライヤー 合成生物学 輸送
研究パートナーシップのための国家安全保障ガイドライン（カナダ）	先端材料と製造技術 先端海洋技術 先端センシングと監視技術 先端兵器 航空宇宙 人工知能 バイオテクノロジー エネルギーの生産・貯蔵・伝送 医療技術 ニューロテクノロジー、人間と機械の融合 次世代コンピューティングとデジタルインフラ 位置・ナビゲーション・タイミング 量子科学 ロボティクスと自律システム 宇宙技術
ホライズンヨーロッパプロジェクトにおける情報の分類（欧州委員会）	研究テーマ — 爆発物 — 化学、生物、放射性物質、核 — 重要インフラとユーティリティ — 国境警備 — 知的な監視システム — テロリズム — 組織犯罪 — デジタルセキュリティ — 宇宙 研究／成果の種類 — 脅威の評価 — 脆弱性評価 — 仕様 — 能力評価 — インシデント／シナリオ

出典：国家安全保障・投資法（Department for Business, Energy & Industrial Strategy, 2021^[68]）；研究パートナーシップのための国家安全保障ガイドライン（Government of Canada, 2021^[70]）；ホライズンヨーロッパプロジェクトにおける情報の分類（European Commission, 2021^[71]）

6.1.2 ガイダンス

政府と政府機関は、研究部門に対し、インテグリティとセキュリティの強化に向けたガイドラインを策定している。これらは主に大学や研究資金配分機関を対象としているが、個々の研究者にも適用されることがある。

米国政府は、*米国の科学技術研究体制のセキュリティとインテグリティの強化に向けた推奨取組*（National Science & Technology Council, 2021^[72]）を発表しており、セキュリティとインテグリティをより強力に保護するための研究機関への提言が含まれている。この提言には、COI 及び COC に関する組織方針の確立、情報開示要件の標準化、責任ある研究活動についての研究者向け研修の提供、開示要件違反に対する適切かつ効果的な罰則の設定等が明示されている。

一方、英国の国家インフラ保護センター（CPNI）（n.d.^[56]）は、国際研究協力におけるインテグリティを促進すべく、*アカデミア向けトラステッドリサーチのガイダンス*を発表している。特に、英国の研究とイノベーションにおいて重要とされる分野の研究者が対象となっている（STEM 分野、新興技術やデュアルユースの可能性のある技術、商業的に機微な研究分野等）。このガイダンスは研究コミュニティや大学コミュニティとの協議をもとに作成されたものである。CPNI は、国際協力に伴うリスクと、英国の研究者が同リスクにどのように晒されるかを概説している。ガイドラインには、大学レベル及び個人向けのアドバイスが含まれている。研究者はCPNIのウェブページからガイドラインにアクセスできる。また、主要な質問に答えることで、研究プロポーザルを自己評価できるチェックリストも提供されている（別欄6.1英国CPNIによる研究提案の評価用チェックリストを参照）（Centre for the Protection of National Infrastructure（CPNI）, 2020^[73]；n.d.^[74]）。一方、*アカデミア向けトラステッドリサーチのガイダンス*に加え、*英国輸出管理合同ユニット*（2021^[40]）は、学術研究に適用される輸出管理を主眼とするガイダンスを発表している。

英国政府（2021^[75]）は、研究者を敵対行為から保護し、国際協力の安全な実施に向けてアドバイスを提供する研究協力アドバイスチーム（Research Collaboration Advice Team：RCAT）を新たに設立した。具体的には、輸出管理、サイバーセキュリティ、知的財産の保護等についてアドバイスを提供している。RCATは、政府の窓口として機能しており、現在のプロジェクトや提案の中に潜在的なリスクがあると判断した国内の大学の要請に応じている。また、アドバイザーは研究機関や大学に積極的に働きかけ、アドバイスやガイダンスを実践するためのサポートをしている。

別欄 6.1 英国 CPNI による研究提案の評価用チェックリスト

英国 CPNI は、共同研究提案の評価に向け、以下の質問を含むチェックリストを開発している。

新規パートナーについて

なぜ、パートナーはあなたと一緒に仕事をしたいと思うのか？
 財政的な支援や関与の見返りとして、彼らは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、又は英国とは異なる民主的・倫理的価値観を持つ国と関わっているか？
 パートナーに対するデューデリジェンスの結果、敵対的な国家と関わる軍や警察に資するような研究への関与は特定されているか？
 デューデリジェンスで得た情報から判断し、あなたの研究が、悪用又は意図しないネガティブな用途に使用される可能性はあるか？
 このパートナーと研究を行うに当たり、法律、規制又は大学の方針による制約はあるか？
 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評判や倫理に関わる潜在的なリスクは存在するか？
 この研究に関する決定を、あなたの部署内で、より重要な問題として扱う必要があるか？

研究提携について

提案されている覚書（MoU）の条件は、あなたの学部と大学の期待に沿ったものであるか？
 既存の知的財産（IP）・研究データ・機微情報・個人を特定できるようなデータをプロジェクトに提供するか？提供する場合、それらはどのように保護されるか？
 発生した IP は誰が所有することになるか？
 得られた IP 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の保護に向けて、どのような契約要件を設けることができるか？
 研究パートナーは、あなたの IT ネットワークにどのようにアクセスできるようになるか？アクセスできるのであれば、それによってどの程度広い範囲の情報が入手可能となるか？
 類似分野の研究を物理的に分離又は保護する必要はあるか？

既存のパートナーについて

研究を進めることにより、既存の研究パートナーとの間に利益相反が生じる可能性はあるか？
 既存のパートナーと利益相反の可能性について話したか？
 秘密保持契約の条件を検討したか？既存のパートナーに、あなたが情報提供する必要があることを想定しているか？
 この研究は、あなた自身、あなたの学部又は大学が既に契約で合意している事項に違反しないか？

出典：チェックリスト：研究提案評価（Centre for the Protection of National Infrastructure（CPNI）, n.d.^[74]）

ニュージーランド政府は、研究機関・大学・研究者向けにトラステッドリサーチ・ガイダンスを作成している（2021^[76]）。このガイダンスでは、教育・研究・科学技術・税関・プライバシー・出入国・情報セキュリティ・海外投資に関する既存の法律のうち、研究セキュリティに関わる問題が分析されている。

オーストラリアの教育大臣は、2019年、大学外国干渉タスクフォース（UFIT）を設立し、UFITはオーストラリアの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作成した（2021^[14]）。このタスクフォースでは、外国の干渉に対処すべく、大学と政府機関が協力し合っている。UFITのガイドラインは、ガバナンスの枠組み、デューデリジェンス、コミュニケーション、リスクとサイバーセキュリティに関する教育等を対象としている。このガイドラインは、事例研究、ツールキット、最善の実践ガイドを含むガイダンス資料で補完されている。ガイドラインは、最初のガイドラインの発表以降に外国の干渉の脅威が増大してきた経緯をより詳しく取り上げ、大学側がそのような干渉を特定し、これに対処できるよう2021年に改訂された。改訂されたガイドラインは、より具体化かつ明確化され、新たに生じる外国の干渉リスクにも対応する一方、大学が自らのリスクに相応の方法で実践できるようになっている。

カナダ政府は、2020年、*研究セキュリティとCOVID-19に関する政策声明*を公表した（Government of Canada, 2020^[77]）。この声明では、研究エコシステムのメンバーに対し、自身の仕事における潜在的なリスクを認識し、オープンサイエンスへの強いコミットメントとCOVID-19のパンデミックへのグローバルな研究対応を支援しながら、自身の知識創造とイノベーションを守るべく、適切な手段を講じるよう要請している。

カナダ政府は、最近、*国際研究協力に対する国家安全保障ガイドライン*を発表し、カナダに脅威を与える国家やグループの軍事・安全保障・情報能力の向上、あるいはカナダの経済・社会・重要インフラの崩壊に

つながるような外国の干渉・スパイ活動・望ましくない知識移転を防止しようとしている（Government of Canada, 2021^[70]）。このガイドラインでは、デュアルユースの可能性がある、あるいは外国政府、軍隊、その他の主体から狙われている機微研究分野が特定されている（表6.1 機密技術・情報分野を参照）。このガイドラインは、連邦政府の研究パートナーシップ資金に適用されるが、これを利用し、潜在的な研究パートナーシップに伴うリスクを評価・軽減することにより、研究を保護することがすべての研究者に推奨されている。各研究者は、連邦研究パートナーシップ助成プログラムに申請書を提出する際、リスク評価フォームに必要事項を記入しなければならない（Government of Canada, 2021^[78]）。

また、カナダ政府は、学术界や国家安全保障コミュニティのパートナーと密接に連携し、自分のペースで進められる2つのオンラインコースを開発した。その目的は、研究者やその他の大学職員を教育・訓練することにある。「研究セキュリティ入門」及び「研究者のためのサイバーセキュリティ」と題されたこれら40分のコースは、重要情報の概要をハイレベルで提供し、様々な教育的手法を駆使して利用者の関心を集めている。両コースとも任意かつ無料で提供されており、「あなたの研究を守るポータル」（Government of Canada, 2021^[79]）からアクセスできる。また、参加者には修了証が発行される。カナダでは現在、新コースの作成とトレーナーの育成に向け、さらなる手段が検討されている。

日本では、研究の国際化・オープン化に伴う新たなリスクに対応すべく、研究インテグリティを確保するための一連の政策方針を政府が策定している（付属書Aを参照）（Integrated Innovation Strategy Promotion Council, 2021^[80]）。これにともない、研究者は、所属先の研究機関と研究資金配分機関の双方に対し、海外の資金援助や所属先に関する情報を報告することが求められるようになった。政府は、2021年、公的研究費に関するガイドラインを改定し、報告すべき情報を府省共通研究開発管理システム（e-Rad）に保存できるようにし、研究者の事務負担を軽減した。報告を怠った場合の罰則として、今後5年間の研究費の申請を禁止している。また、政府は、研究機関や大学向けに新しい政策方針に関するセミナーを実施し、研究機関・大学や研究者向けにチェックリストのひな形が提供されている。

オランダ政府も、研究機関や大学向けにガイドライン・チェックリスト・自己評価ツールを開発し、国際協力において知識のセキュリティを保護するにはどのような要素を考慮すべきかを明示している（Ministry of Education, Culture and Science, 2020^[81]; 2021^[82]）。ここでいう知識のセキュリティとは、知識や技術の無断移転や、自己検閲につながったり学問の自由を損なったりしかねない国家主体による高等教育・研究への非公然的影響を防止することと定義されている。政府は、研究機関や大学からの問い合わせに対応し、その意思決定を支援すべく、一元的窓口となる知識セキュリティセンターの設置も予定している。

6.1.3 研究機関・大学・情報機関・法執行機関の間での情報の共有

情報機関・法執行機関・研究機関・大学の間でより効果的に協力し、情報を交換することは、多くのOECD加盟国の政府と研究機関の双方が必須と考えている。このような協力が効果を発揮するには、政府が科学研究の自由と自律性を尊重することが重要な前提条件となる。

米国政府が支援する研究開発の国家安全保障政策に関する大統領覚書（The White House, 2021^[65]）は、科学技術政策局（OSTP）局長に対し、国家情報長官（DNI）及び必要に応じて他の機関の長と連携し、米国の研究開発体制に働きかけることにより、研究セキュリティとインテグリティに対するリスクに関する意識と、リスクを軽減するための政策と対策を強化することを求めている。米国では、研究資金配分機関にCOIやCOCを適切に開示しなかった科学者が起訴されており（Cho, Kingdollar and Soshi, 2021^[63]）、こうした起訴に対し、学术界に大きな懸念と抗議が広がってきている。これを受け、米国政府は、研究機関が地元の連邦捜査局（FBI）事務所と連携することにより、双方の間で懸念を正しく伝え合い、これを把握するよう提言した。

同様に、諸外国でも研究機関・大学・政府機関の間の連携強化を促進している。オーストラリアでは、教

育・技能・雇用省と内務省が共同で、大学外国干渉タスクフォースを設置している。同タスクフォースのオーストラリアの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（2021^[14]）は、運営グループと4つのワーキンググループ（研究と知的財産、外国との協力、サイバーセキュリティ、コミュニケーションと文化）によって作成され、大学と情報機関を含む政府機関から約40名が参加した。

英国では、国家インフラ保護センター（CPNI）が学術分野のパートナーとの共同ワークショップに参加し、研究に対する国家安全保障上のリスクの管理に向けて大学を支援している。このワークショップの目的は、国際研究協力におけるリスクとセキュリティの特定・管理において学者を支援することにある。また、安全な研究協力に関する相互に有益な情報を秘密裏に共有するために、2021年にCPNI STEM大学フォーラムが設立された。CPNI STEP大学フォーラムの構成メンバーは、英国のSTEM研究集約型の大学と組織、CPNI、そして国家サイバーセキュリティセンターである。このフォーラムには必要に応じ、政府機関や独立行政法人の代表者も招聘されている。

カナダでは、カナダ政府-大学ワーキンググループ（Government of Canada, n.d.^[83]）が設立されており、大学・政府省庁・連邦助成評議会・国家安全保障機関が参加している。設立文書には「研究を保護し、カナダ人の利益を最大化する方法により、オープンで協同的な研究を進めるために設立された」とある。運営面を見ると、自然科学・工学研究会議（NSERC）の提携助成事業では、リスクが特定された場合、助成金申請書を国家安全保障機関又は関連政府省庁に照会するリスク評価プロセスが実施されている（図6.1助成金申請のリスク評価プロセスを参照）（Government of Canada, 2021^[78]）。

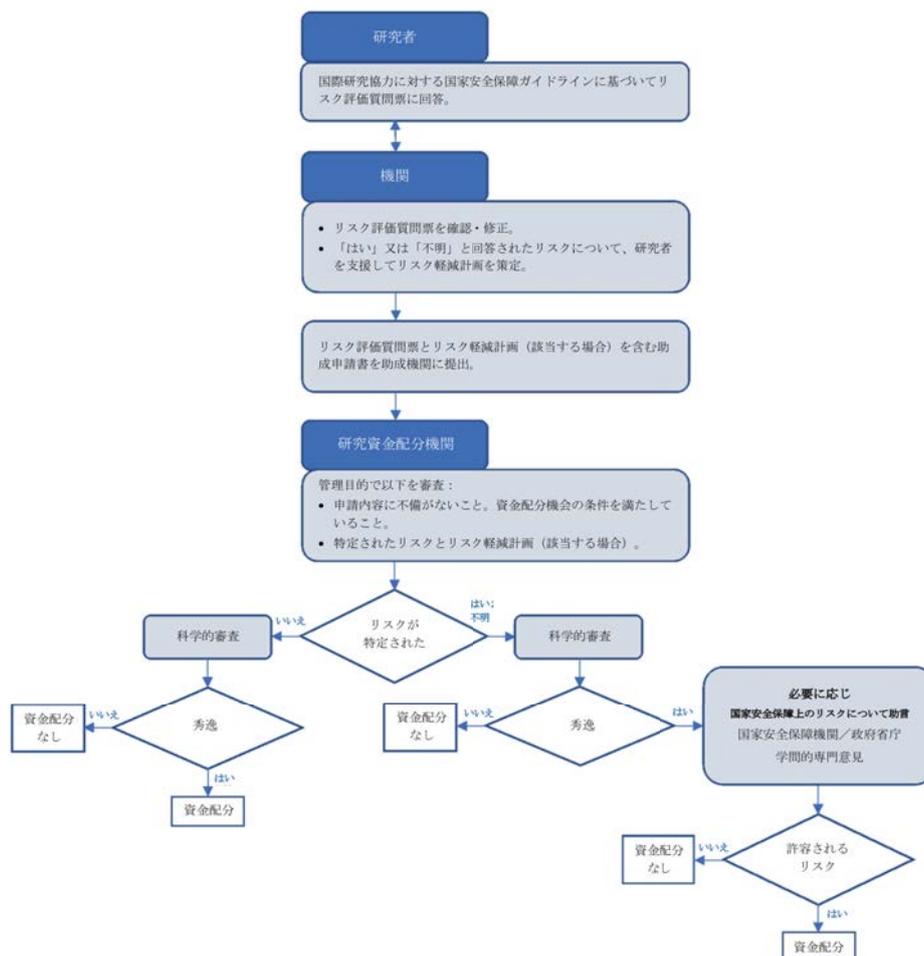


図6.1 助成金申請のリスク評価プロセス

NSERCの提携助成事業（カナダ）では、リスク質問票（別欄6.2 リスク評価質問票参照）とリスク軽減計画が要求され、審査される。特定の申請については、必要に応じて国家安全保障機関や関係省庁に照会される。

出典：リスク評価フォーム、国際研究協力に対する国家安全保障ガイドライン（Government of Canada, 2021^[78]）

6.2 研究資金配分機関

6.2.1 ガイドラインと規則

インテグリティと開放性を促進する様々な対策に加え、一部の研究資金配分機関は、研究に対する外国の望ましくない干渉に対処すべく、具体的な措置を講じている。これには研究費の申請者や受給者、研究提案の審査員、各機関の職員を対象とした措置が含まれる。

英国研究・イノベーション機構（UKRI）は、ガイダンスと積極的な助成保証・監査プログラムに裏づけられた一連の資金配分方針に基づき、支援対象の研究が実施される環境と方法に対して同機関が期待することを明示している。UKRI（2021^[84]）はまた、国際協力のためのデューデリジェンスに関し、資金配分する組織への期待を示した原則も発表している。しかし、各研究機関の自律性に配慮し、ガイドラインの遵守を積極的には監視していない。

米国国立科学財団（NSF）は、職員が外国政府の人材採用プログラムに参加することを禁止している。一方、研究セキュリティ戦略・政策担当責任者という役職を設け、研究セキュリティの向上に向けた戦略の策定と実施、及び他の連邦機関との調整を担当させている（National Science Foundation, 2020^[85]）。

ノルウェーでは、国立研究会議の資金配分を受けたプロジェクトは契約で管理されている。この契約によると、適用される法律・規制、倫理的ガイドライン及び優れた研究実践における認定品質基準・規範を遵守することがプロジェクトマネージャーに求められる。ポルトガルでは、行政法により、助成金の審査に関わる者はすべてそのCOIを申告しなければならない。

6.2.2 利益相反又は責務相反の管理

COI及び／又はCOCの申告に関する規則やガイドラインは、研究資金の申請者、研究資金配分機関の支援を受けているプロジェクトに参加する研究者、ピアレビューアー、研究機関の職員を対象とすることができる。各国の研究資金配分機関は、概ね同じ規則を設けているが、開示要件は特定の状況に適合させている（表6.2 研究資金配分機関に開示する活動の種類を参照）。

表 6.2 研究資金配分機関に開示する活動の種類

	対象	申告すべき利益の内容
オーストラリア研究評議会 (ARC)	資金配分の申請者、ピアレビューアー、機関職員	<ul style="list-style-type: none"> — 専門的な職 — 他組織の委員会のメンバー — コンサルタント業務 — 研究関連活動に対する海外からの経済的支援（現金又は現物支給） — 外国が主催する人材採用プログラムとの現在・過去の関連又は所属（過去10年間） — 外国政府、外国政党、外国国有企業、外国軍隊及び／又は外国警察組織との現在の関連又は所属 — 取締役会 — 顧問団 — 専門家としての関わり — 家族・個人的な関係 — 研究活動を支援するために、外部から現金・サービス・設備等の形で報酬を受領することを含む金銭的利益
カナダ・イノベーション財団 (CFI)、カナダ保健研究機構 (CIHR)、カナダ自然科学・工学研究会議 (NSERC)、カナダ社会科学・人文学研究会議 (SSHRC)	資金配分の申請者とピアレビューアー	<ul style="list-style-type: none"> — 助成の機会または審査中の申請に起因する業務上又は個人的な利益 — 申請者又は申請者の所属機関との業務上又は個人的な関係 — 助成の機会または審査中の申請における直接的又は間接的な金銭的利益
ドイツ研究振興協会 (DFG)	ピアレビューアー	<p>原則として以下の場合には除外される：</p> <ol style="list-style-type: none"> 1. 第一親等、婚姻関係、生涯の伴侶関係、同棲関係 2. 提案の成功に伴う個人的な金銭的利益又は第1項に記載された人物による経済的利益 3. 現在又は今後の緊密な科学的協力関係 4. 大学からの提案の場合：研究団体の代表者は、自身の提案と同じ会議で審議される提案のピアレビューには参加不可 5. 従属的な雇用関係又は監督関係（例：ポスドク段階までの師弟関係等）であり、その関係が終了してから6年までのもの 6. a) 法人からの提案の場合：当機関又は参加機関への所属又は異動の承認待ち b) 個人からの提案の場合：同じ学部又は大学以外の同じ研究所への所属又は異動の承認待ち 7. 大学からの提案の場合：申請を行った大学の評議会や同様の監督的委員会等で活動している研究者は、当該大学が提出する提案の審査や決定には参加不可 <p>原則として以下の場合には個別案件ごとの対応となる：</p> <ol style="list-style-type: none"> 8. 第1項に該当しない関係、その他の個人的な関係や相反 9. 第8項に記載された人物の金銭的利益 10. 個人からの提案の場合：同じ大学又は大学以外の同じ研究機関への所属又は異動の承認待ち 11. 第7項に記載されていない大学組織への参加（より大きな研究環境にある科学諮問委員会等） 12. 過去3年以内の研究協力（共同出版等） 13. 密接に関連した研究テーマを持つプロジェクトの提案又は実施（競合） 14. 現在進行中の選考プロセス、又は過去12ヶ月以内に完了した選考プロセスへの申請者又は選考委員としての参加 15. 過去12ヶ月以内の相互に対するピアレビュープロセスへの参加

英国研究・イノベーション機構（UKRI）	資金配分の申請者	<ul style="list-style-type: none"> — 提案された研究に関与する、組織又はプロジェクトパートナー（指定された雇用組織以外）からの個人的な報酬 — 研究に関与又は研究から利益を得る可能性のある組織の、大量の株式保有又はその他の金銭的利益 — 助成金に関わる又は申請書に記載されていないが研究成果から利益を得る可能性のある営利団体からの研究支援（現金又は現物支給） — 申請書に記載されている又は研究やその成果から利益を得る可能性のある組織との無報酬での関与 — 政治・圧力団体との関与 — 家族及び同じ世帯に暮らす人間の関連する既知の利益
米国連邦研究機関	資金配分の申請者	<ul style="list-style-type: none"> — 専門的準備（学位等） — 組織への所属 — 学術的、専門的又は機関による任命 — 直接の金銭的貢献又は現物支給かを問わず、すべての研究開発プロジェクトに対する現在受給中及び申請中の支援 — 外国の政府、機関又は団体によるプログラム（外国政府による人材採用プログラムを含む）への参加、参加に関する承認待ち又は参加申請中 — 外部団体から資金提供を受けている客員研究員 — 外部団体から資金提供を受けている学生とポスドク研究者 — 個人の任命の範囲外である有償コンサルタント業務（研究機関の契約とは別） — 時間的拘束を伴う研究活動のために、外部団体から支援又は支払いを受けた渡航 — 開示された情報が正確、最新かつ完全であることを本人自らが証明すること

出典：ARC 利益相反及び秘密保持方針（Australian Research Council, 2020^[86]）；利益相反及び秘密保持（Government of Canada, 2016^[87]）；利益相反を回避するためのガイドライン（German Research Foundation（DFG）, n.d.^[88]）；利益の申告：申請者（UK Research and Innovation（UKRI）, n.d.^[89]）；米国政府が支援する研究開発のための国家安全保障戦略に関する国家安全保障大統領覚書33（NSPM-33）の履行のためのガイダンス（National Science and Technology Council, 2022^[67]）

米国政府説明責任局（GAO）（2020^[90]）は、規則やガイドラインに加え、海外の所属先等の必要な情報の開示を怠った場合の措置を文書化することを研究資金配分機関に推奨している。その際、役割と責任を含む調査のプロセスの概要を示し、申し立てが立証された場合に講じ得る行政措置又は強制措置をこれに含めなければならない。研究資金配分機関が講じ得る行政措置や強制措置には、研究者の所属大学への調査の依頼、助成金の停止、訴訟が含まれる。

6.2.3 リスクの評価と管理

いくつかの研究資金配分機関は、研究資金の申請と審査のプロセスにリスク評価を取り入れている。

カナダの場合、連邦政府の研究資金パートナーシップである自然科学・工学研究会議（NSERC）の提携助成事業への申請者は、リスク評価質問票に回答しなければならない（別欄6.2 リスク評価質問票を参照）。申請者がリスクを特定した場合は、リスク軽減計画を策定する必要がある。研究資金配分機関は、資金配分の決定前にリスク評価質問票とリスク軽減計画を審査する（図6.1 助成金申請のリスク評価プロセスを参照）。

米国エネルギー省（DOE）は、科学技術リスクマトリクスを開発し、規制管理制度はないものの、国家又は経済安全保障上の影響を考慮する場合に追加的な保護措置が必要と思われる重要な新興研究の分野を特定している（United States Department of Energy, 2021^[91]）。DOE は、このリスクマトリクスにより、国際業務に関連する省内の決定を指揮・管理している。

別欄 6.2 リスク評価質問票

カナダでは、国際研究協力に対する国家安全保障ガイドラインに基づき、研究者は以下のような「はい」「いいえ」形式の質問を含む質問票に回答しなければならない。

自身の研究の把握

その研究から得た知識や知的財産（IP）に、外国政府、軍又はその代理人が関心を持つ可能性がある。
研究者が意図していない用途であっても、その研究分野は軍事、警察又は情報機関に应用される可能性がある。
機密とされる分野の研究に該当する。
「カナダ輸出管理リストガイド」及び「核不拡散輸出入管理規定」の対象分野に関与している。
防衛生産法第35条に規定され、規制対象とされる商品／技術に関連する分野に関与している。
随時改訂される輸出管理リスト・輸入管理リスト・地域規制リストの対象分野に関与している。
重要鉱物とそのサプライチェーンに関連する研究分野に関与している。
機微な個人データ又は全体として機微である可能性のある大量のデータを扱っている。
重要インフラに焦点を当てた研究分野に関与している。
提案されたプロジェクトに使用される研究施設又はインフラに機微なデータが収容される、及び／又は当該のパートナーシップとは無関係のインフラへのアクセスが提供される。

パートナーの把握

あなたのパートナー組織、その親組織及び／又は子会社・関連会社が、カナダの国家安全保障に悪影響を及ぼす可能性がある第三者である政府、軍又は組織への研究の移転につながる可能性のある提携又はパートナーシップを有している。
あなたのパートナー組織、その親組織及び／又は子会社・関連会社が、外国政府の影響や支配を受ける可能性がある（例：その国への知識移転を強制する政策及び／又は法律があるなど）。
最終的な資金源及び／又は資金提供者にとっての価値が不明確な資金提供の申し出がある。
研究者が外国に転勤するか、外国で研究を再現すること（例：ミラーラボの設立）を条件とした資金提供の申し出がある。
あなたのパートナー組織が、詐欺、賄賂、スパイ、汚職又はその他の透明性や倫理的行動の欠如を表す犯罪行為で告発されたり、その罪を認めていたり、有罪判決を受けたことがある。
政府、軍又はその他の第三者機関への研究の移転につながり得る利益相反や所属先が研究チームメンバーに存在することを示唆する情報がある。
あなたのパートナー組織が、当該パートナーシップとは無関係な研究を実施するため、カナダの施設、ネットワーク又は資産を利用することができる。
あなたのパートナー組織が、地域規制リストに掲載されている国にある。

出典：リスク評価フォーム（Government of Canada, 2021^[78]）

英国のいくつかの研究評議会とウェルカム・トラスト（2021^[92]）は、助成金申請書に、申請者の提案に関連する短期・中期的な悪用リスクの検討を求める質問を盛り込んでいる。また、助成金申請のピアレビューを行う外部の専門家に対し、悪用リスクに関するガイダンスを提供している。深刻な悪用リスクが懸念され、受入機関と合意した管理戦略によってこれを払拭できない場合、当該の申請に対して資金は配分されない。プロジェクト中に新たに発生し、申請段階で特定されていなかったかもしれない懸念のあるデュアルユース研究に関連する新たなリスクについて、研究者は、研究資金配分機関と受入機関に通知することが期待されている。

ドイツ研究振興協会（DFG）とドイツ国立科学アカデミーは、悪用リスクを最小限に抑え、個々の研究者・研究機関・大学による自主規制を支援するためのガイドラインを作成している（German Research Foundation（DFG）and German National Academy of Sciences Leopoldina, 2014^[93]）。このガイドラインは、個々の研究者に対して、リスクを分析し、これを最小限に抑え、責任を持って機微な研究結果を公表し、悪用される可能性の高い研究を回避することを推奨している。また、研究機関や大学には、法的規制の遵守に加え、安全保障に関連する研究を取り扱う際の倫理的ルール策定が推奨されている。DFGではこのガイドラインに加え、研究プロジェクトのセキュリティ面の取り扱いを募集要項に取り込んでいる。申請者は、提案されたプロジェクトに差し迫ったデュアルユースのリスクが存在するか否かを評価しなければならない。そのようなリスクがある場合は、リスク便益分析を提示し、リスクを最小化する手段について説明しなければならない。申請者が所属する研究機関や大学に研究倫理委員会がある場合は、事前に委員会に相談し、委員会の意見書を研究提案に添付する必要がある（German Research Foundation（DFG）, n.d.^[94]）。

6.3 公的研究機関

公的研究機関（PRI）の中には、政府省庁の一部であって、国家経済の特定分野で研究とイノベーションの推進を担当する機関がある。この場合、研究者はこれらのPRIで公務員として雇用され、公務員に広く適用される関連規則とガイダンスが適用されることになる。また、PRIは政府から独立し、多くの国における大学運営と同様の方法で独自の雇用条件を設定できる場合もある。ただし、国によっては大学職員が公務員の地位を持つこともある。

米国エネルギー省（DOE）は、DOE職員と受託業者に対し、外国政府が支援する特定の人材採用プログラム、外国政府が支援又は関連する活動への参加と同時にDOEの施設内で働くことを禁止している。

2020年から2021年にかけて、オーストラリア連邦科学産業研究機構（CSIRO）は、外国の干渉リスクを評価し、新たな研究機会について体系的に意思決定を行うために研究活動機微性評価ツール（REST: Research Engagements Sensitivities Tool）を開発した。プロジェクトの承認における最終決裁者のランクは、プロジェクトのリスク評価レベルに対応している。評価者が高いリスクを指摘した場合、CEOが新しいパートナーとの協力を承認しなければならない（図6.2 研究活動機微性評価ツール（REST:Research Engagements Sensitivities Tool）を参照）。CSIROはリスク評価のツールやノウハウをオーストラリアの大学と共有し始めている。

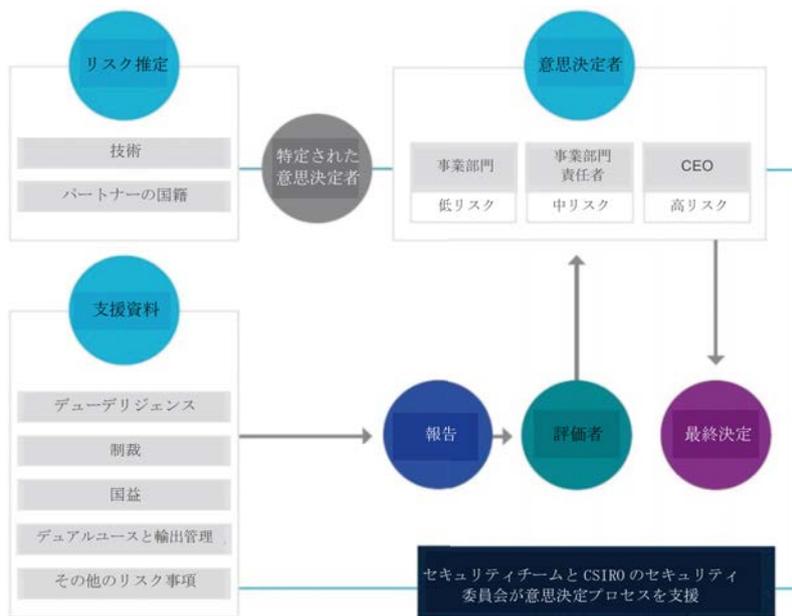


図6.2 研究活動機微性評価ツール（REST:Research Engagements Sensitivities Tool）

オーストラリアのCSIROは、外国の干渉リスクを評価し、新たな研究機会について体系的に意思決定を行うために、研究活動機微性評価ツール（REST: Research Engagements Sensitivities Tool）を開発した。

ドイツでは最近、マックスプランク協会が所属研究者向けの新しいガイドラインを作成している（Max Planck Society, 2021^[95]）。このガイドラインでは、国際協力を始める前に、人権、学問の自由、科学スパイに関するリスクを特定し、最小化することを研究者に推奨している。また、研究者が第三者から資金を受け入れる場合には、運営本部による事前承認が必要となる（Max Planck Society, 2021^[96]）。さらに、研究者が規則について疑問を持った場合は、オンブズパーソンが内密に助言することができる（Max Planck

Society, n.d.^[97])。ライプニッツ協会では、マックスプランク協会と同様に、傘下の研究機関や研究者に対して、パートナー国の政治状況やそれに伴う研究パートナーのモチベーションを評価することを求めている (Leibniz Association, 2021^[98])。

6.4 大学協会

大学協会は、大学へのガイダンスの提供において重要な役割を果たすことができる。カナダで最も研究活動が盛んな大学の集まりであるU15カナダ研究大学連盟は、*機微研究における経済的・地政学的なリスクの軽減 (Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects (2019^[99]))* という指針を発表している。この指針は、研究者や研究支援部門が、経済的・地政学的なリスク評価を実施し、重要なリスクを軽減するための、実践的なアドバイスと最善の実践例を提供するものである。この指針には、経済的・地政学的なリスク評価のための実践的なチェックリストとマトリクスも含まれている。チェックリストでは、強力なプロジェクトチームの構築、非学術パートナーの評価、サイバーセキュリティとデータ管理、研究成果の活用への検討、海外渡航などのテーマが取り上げられている。

米国では、公立・ランドグラント大学協会 (APLU) と米国大学協会 (AAU) (2020^[100]) が、キャンパスにおける国家安全保障上の脅威と外国政府の不当な影響に関する懸念に対処するための大学の行動を発表している。具体的には、研究セキュリティの確保、知的財産の窃盗や学術スパイからの保護、外国政府の不当な影響力の行使や学術の中核的価値の侵害を企む外国政府及び／又はその他の団体による行動や活動の防止に向けた大学側の対策が調査された。また、AAUとAPLU (2021^[101]) は、国家安全保障上の懸念に対して維持すべき基本原則と価値観も明らかにしている。その価値観には、潜在的な利益相反の申告や知的財産の尊重に加え、学問の自由、表現の自由、包摂性、多様性、透明性、協力が含まれる。また、外国人研究者との非公式な研究提携や正式な協定の締結に対する行政上の障壁を最小限にすることを政府に求めている。

ドイツ大学学長会議は、ドイツの大学の国際的なパートナーシップに向けたガイドラインと基準を策定している (2020^[102])。共同研究のガイドラインは、研究の自由、共同研究の付加価値、科学的・倫理的・法的基準の遵守、対等なパートナーシップ、研究者の移動の促進を原則としている。倫理的・法的基準には、安全保障関連の研究の取り扱いに関する規則に加え、知的財産の保護に関する法律が含まれている。また、ドイツ学術交流会も、ガイドラインを公表するとともに、大学が国際的なパートナーシップを評価する際にアドバイスを提供する窓口を設けている。

英国の大学を代表する組織である英国大学協会 (UUK) (2020^[12]) は、大学・職員・学生を保護し、国際化に伴うリスクを管理することができるよう、大学を支援するためのガイドラインを発表している。このガイドラインには、大学の運営組織とエグゼクティブリーダー向けの重要な行動や事例研究が含まれている。UUKは、持続可能で安全な国際パートナーシップを維持した上で国際安全保障上の脅威を軽減するには、個人の意識と理解、機関のシステム・プロセス・行動、そして部門横断的なシステム・プロセスの変革が不可欠だと主張している (図6.3 英国大学協会の安全保障関連問題への取組における中間成果を参照)。UUKは、大学のシニアリーダーがリスクを認識する文化を醸成することにより、セキュリティ関連の問題に対する機関の強靱性が高まると主張している。

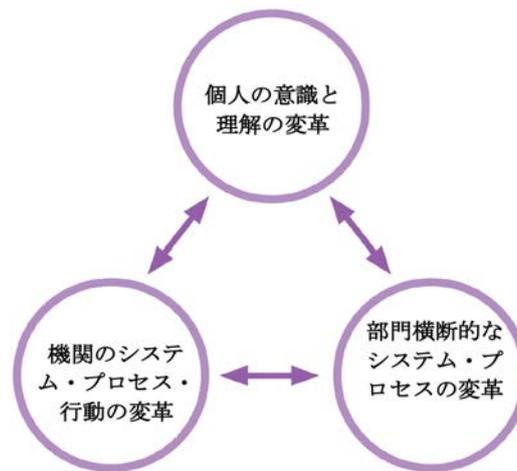


図 6.3 英国大学協会の安全保障関連問題への取組における中間成果

英国大学協会（UUK）は、安全保障関連問題について3つの長期的な目標を設定している：1）英国の大学は、国際的な安全保障上の脅威を管理・軽減するために、首尾一貫した戦略的・運用的な前向きのアプローチをとっていることを証明できる。2）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、自信を持って追求できる。3）英国の高等教育部門と政府は、安全保障上の課題の中で、研究・イノベーション（R&I）の成長、組織の自律性、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。UUKは、これらの長期的な目標の達成に向け、次の3つの中間成果を設定している：a）職員や学生の間で、安全保障関連の問題に対する意識や理解を深める。b）組織のシステム・プロセス・行動の強化。c）大学と政府の接点、システムの強韌性を含むエコシステムのより広い変化。これらの中間成果は互いに重複しており、補完し合う関係にある。

出典：国際化の下でのリスク管理：セキュリティ関連問題（Universities UK, 2020^[12]）

英国大学協会（UUK）は、財務上のリスクに加え、評判上のリスク・倫理上のリスク・安全保障上のリスクも考慮するよう大学に推奨している（Universities UK, 2020^[12]）。UUKは、大学が取るべき行動として、パートナーを知ること、リスクに応じた意思決定を行うこと、強固な契約を締結・維持すること、職員の役割と責任を明確にすることなどを挙げている。これらは、安全保障関連のリスクを評価し、大学への潜在的な損害を軽減する包括的デューデリジェンスプロセスの一環とされている（別欄 6.3 デューデリジェンスプロセスの実施を参照）。デューデリジェンスは、海外に渡航あるいはそこで勤務する職員や学生を保護する上でも重要と考えられている。

別欄 6.3 デューデリジェンスプロセスの実施

デューデリジェンスを徹底するための英国大学協会（UUK）の行動リスト

自分のパートナーを知る

- ・ パートナーシップや共同研究を可能な限り開示することを職員に義務づけるなど、十分な情報に基づく意思決定を支援する。

リスク情報に基づいた意思決定を行う

- ・ パートナー団体に質問票への回答や書類・証拠の提出を依頼する。
- ・ 所属機関の学術的専門家、ウェブ検索、購読サービス、専門会社を活用する。

強固な協定を締結し、維持する

- ・ 安全保障関連のリスクを管理するため、最善の実践の契約締結の仕組みとポリシーを使用する。
- ・ 契約書や覚書の条件には、学術活動のインテグリティを保護する条項を含める。
- ・ 国際的なパートナーシップやプロジェクトに加え、投資・寄付・慈善活動・商業化・設備投資・授業料収入、職員の名誉職やコンサルタント職等の収入源について定期的に見直す。
- ・ 継続的なデューデリジェンスにより、海外の組織や研究者がもはや適切なパートナーではないことが明らかとなった場合、いかなる責任も負わずに契約を解消できるよう、適切な出口戦略を策定する。

職員の明確な役割と責任を確立する

- ・ 安全保障関連のリスクを特定し、それに対して行動できるように職員を支援する。

出典：国際化の下でのリスク管理：セキュリティ関連問題（Universities UK, 2020^[12]）

スウェーデンの研究・高等教育国際協力財団（STINT）は、責任ある国際化：国際的な学術共同研究についての考察のためのガイドライン（Shih, Gaunt and Östlund, 2020^[103]）を策定しており、共同研究の様々な段階で問うべき重要な質問が掲載されている。これらの質問の中には、学問の自由の制限につながるリスクを評価するものもある（別欄 6.4 学問の自由の保護を参照）。このガイドラインは、スウェーデンの大学間及び大学内での対話の基礎となっている。

別欄 6.4 学問の自由の保護

責任ある国際化：国際的な学術共同研究についての考察のためのガイドラインでは、学問の自由を制限、又はスウェーデンの法律や国際条約に抵触する可能性があるリスクを評価するため、以下のような質問を設けている。

学問の自由

- ・ プロジェクトの資金調達方法は、独立性、インテグリティ、倫理性又は学問の自由に関するリスクを伴わないか？
- ・ 研究者や高等教育機関は、相手国の政治的・社会的・文化的状況について総合的かつ適切な知識を有しているか？
- ・ 研究機関において、研究者が相手国の状況を理解し行動するために、どのようなサポートが提供されているか？
- ・ 共同研究は、他の当事者との関係において、自身の高等教育機関の独立性に影響を与える可能性はあるか？
- ・ 学問の自由が制限される場合、どのように対処すべきであるか？どこに境界線を引くべきか？この研究は、プロジェクトパートナーにどのような影響を与えるか？

法的観点

- ・ 研究成果のデュアルユースに伴う直接的リスクはあるか？
- ・ 戦略物資とみなされるような研究成果はあるか？
- ・ プロジェクトの科学的内容が国際的な制裁によって制限される可能性はあるか？

出典：責任ある国際化：国際的な学術共同研究についての考察のためのガイドライン（Shih, Gaunt and Östlund, 2020^[103]）

6.5 大学

6.5.1 方針とガイドライン

研究セキュリティに伴うリスクを軽減し、研究インテグリティと科学研究の自由を促進・確保するために、各国の多くの大学が独自の規則やガイドラインを設定し始めている。これらの方針は、個々の懸念事項が表面化した後、又は国家安全保障機関との協議を受けて策定されたものであることが多い。関連するすべての活動を網羅的に調査することは本報告書の範囲を超えるが、ここでは大学が実践しているいくつかの事例を紹介する。

テキサス大学オースティン校（n.d.^[104]）は、「利益相反や責務相反が懸念されるような職員の学外活動について、開示・承認・文書化するための透明性あるシステムを提供すること」を目指している。同大学の方針として、研究者に金銭的利益の開示の提出と、必修研修の受講が義務づけられている。ミシガン大学（米国）・ロチェスター大学（米国）・トロント大学（カナダ）・マギル大学（カナダ）も同様の方針を策定し、国内法の遵守に加え、科学研究の自由を外国の違法な干渉から保護することを目指している。

ロチェスター大学の暫定ガイドライン（Committee on Science and Security, 2019^[105]）は、学内又は海外を問わず、研究協力のあらゆる側面を対象としている。具体的には、あらゆる種類の国際的な協力や支援（人材採用プログラム・助成金・贈与等）の開示が求められており、現在、米国の多くの大学においてもこれは同様である。また、ロチェスター大学は、同校の方針が遵守されていることを確認すべく、学生・教員・研究者又は短期滞在者（研究室や施設の見学者・ゲスト講師・講演者）を含む訪問者の監視を徹底している。

トロント大学は、*国際的な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チェックリスト*（University of Toronto, 2021^[106]）を作成している。このチェックリストは、主任研究者が特定のプロジェクトを進める前に、海外のパートナーと関わることの適切性とそれに伴うリスクを評価することを支援するものである。主任研究者は、研究提案の提出後2週間以内、又は国際的な研究パートナーシップの開始前にこのチェックリストに記入しなければならない。

6.5.2 管理・監督

一部の大学では、専門の委員会や機構が研究セキュリティリスクの管理責任を負っている。

例えば、ミシガン大学では、研究COI委員会（University of Michigan, n.d.^[107]）が設置されている。同委員会は、研究提案に資金を提供される研究者が開示した外部活動を審査し、それが研究の設計・実施・報告に直接かつ重大な影響を与える可能性があるかどうかを決定する。研究COI委員会による審査の目的は、各個人の私的利益が科学・研究スポンサー・大学・同僚・学生に対する当人の主たる義務に不当に影響しないことを確認する点にある。そこでCOIが特定された場合、通常、COIを適切に管理できるような戦略が策定される。

オランダの各大学には、知識セキュリティアドバイザリーチームがある（Association of Universities in the Netherlands (VSNU), 2021^[82]）。これは、安全リスク管理・情報セキュリティ・国際協力の専門家構成されるバーチャルチームで、特定の研究テーマや国、人材問題等の専門家も後から選出できるようになっている。また、このチームは、大学の執行部が知識セキュリティの問題について意思決定をすることを支援している。小規模の大学が知識セキュリティリスクの評価に必要な専門知識をすべて備えていない場合、他の大学の知識セキュリティアドバイザリーチームから専門知識を「借りる」ことができます。

ほとんどの国の大多数の大学は、研究セキュリティや利益相反を管理する専門委員会を設けていないが、

これらの問題を担当すると思われる組織は一般的に存在する。適切に構成され、資源を付与された機関内審査委員会・倫理委員会・研究インテグリティ委員会は、それぞれ異なる状況においてその役割を果たすことができる。

6.5.3 研究セキュリティ研修

一部の大学では、研修プログラムを通じて、研究セキュリティ問題に関する職員の意識向上に取り組んでいる。

ミシガン大学では、研究倫理とコンプライアンスに関連した研修オプションが用意されている。責任ある研究・奨学金に関する教育と評価のためのプログラムは、大学教職員と学生にオンライン研修モジュールを提供している（University of Michigan, n.d.^[108]）。扱うテーマは、研究インテグリティ・利益相反・輸出管理・研究情報セキュリティ等である。当初、このトレーニングは連邦政府の資金によるプロジェクトの関係者へのみ義務づけられていたが、現在では奨学金や研究に関わるすべての教職員と学生に受講が推奨されている。

スウェーデンのルンド大学では、すべての博士課程の学生に研究倫理コースの受講が義務づけられている。このコースの目的は、新しい技術の開発と実施における倫理的な課題を含め、研究インテグリティの基礎と研究倫理の知識を提供することにある（Lund University, 2020^[109]）。ノルウェーでは、研究の倫理とインテグリティに関する法律により、すべての研究機関と大学に対し、新技術の悪用を含めた研究倫理に関する教育をすべての職員と研究者に提供することが義務づけられている（Langtvedt, 2020^[110]）。これらのイニシアチブは、研究インテグリティと新技術の悪用に関する問題を明確に取り上げているため、研究セキュリティに関するより広範な問題に対応し、必要に応じて拡張できることは想像に難くない。同様に、研究セキュリティに容易に対応できる教育・訓練活動が世界中の大学に数多く存在することは間違いない。

6.6 国際的な研究プロジェクトと研究インフラ

国際的な研究プロジェクトや研究インフラで行われている研究の中には核物理学やバイオディフェンス等の分野における研究など、一般に知られたデュアルユース技術に関連するものがある。こうした場合、当該の技術に適用される国内外の規制や条約の現行枠組みの中で研究が行われる。しかし、国際的な研究プロジェクトやインフラの大半は、国際条約が適用されず、多くの国で機微だと見なされないテーマを扱っている。大規模な国際プロジェクトやインフラは、しばしば独自のガバナンス構造を持っており、その中には自律的な国際法的地位を持っているものも少数ながら存在する。資金助成や所有権は多くの国で共有されている可能性があり、このような状況では国家や経済の安全保障に向けられる懸念や外国の干渉に対する視点が異なってくる。

その一例が、欧州連合（EU）が資金を提供するヒューマン・ブレイン・プロジェクト（HBP）である。この大規模な国際プロジェクトでは、責任ある研究とイノベーションのための専用フレームワークが開発されており、その活動のすべてが既存の倫理原則及び異なる管轄区域に適用される法的規制に準じて行われるようになっている。これには人権やデータ保護への具体的な配慮も含まれている。また、このプロジェクトでは、科学的・技術的成果の政治・安全保障・情報・軍事面での利用と悪用が監視されるとともに、研究の進展の過程で生じる倫理的・社会的問題についても対策が講じられている（Human Brain Project, n.d.^[111]）。

6.7 学協会

学協会は、学会員や研究コミュニティ全体にガイドラインを提供する重要な役割を担っている。米国科学・工学・医学アカデミーは、全米科学技術安全保障円卓会議（National Academies of Sciences, Engineering and Medicine, 2020^[112]）を立ち上げている。この会議には、研究関係省庁・国家情報機関・法執行機関・学術研究機関・ビジネス界の関係者が参加している。具体的には、連邦政府資金による研究開発に伴う安全保障上のリスクの特定と検討、学術・科学コミュニティにリスクを伝えるための効果的なアプローチの特定、そしてリスク軽減に向けた最善の実践の共有が計られている。

英国王立協会（2021^[113]）は、英国政府が外国影響登録制度（FIRS: Foreign Influence Registration Scheme）を検討した際にコメントを提供している。同協会は、内務省宛ての書簡の中で、研究の窃盗・悪用・搾取及び個人情報の紛失など、敵対行為による脅威が存在することを認めている。これらの脅威に対処しなければ、個人又は組織の評判が損なわれ、社会全体に対する大きな脅威となりかねない。同時に、過度な規制が、学術研究コミュニティを萎縮させ、国際研究協力の阻害要因となるリスクも強調されている。このような公的な意見は、適切な政策的措置を策定する上で考慮され、バランスをとる必要のある重要な諸要素を決定することにも貢献している。

ドイツ科学アカデミーは、安全保障に関連する研究の取り扱いに関する会議やワークショップを定期的開催し、これらに様々な分野の専門家を招いている（German National Academy of Sciences Leopoldina, n.d.^[114]）。このイベントの目的は、研究の安全保障上の側面について研究者自身の認識を高め、経験を共有することにある。参加者は、安全保障関連の具体的な研究プロジェクトについて討議し、悪意ある利用による破滅的なシナリオを防ぐ手段として、研究者の自主規制が十分か否かを議論する。ドイツ科学アカデミーは、ドイツの研究機関や大学が安全保障関連の研究の倫理面を担当する地域の委員会を設立することを支援している。現在、130の地域の委員会又は窓口担当者が安全保障関連の研究プロジェクトの倫理的評価について研究コミュニティを積極的に支援している（German National Academy of Sciences Leopoldina and German Research Foundation (DFG), 2020^[115]; German National Academy of Science Leopoldina, n.d.^[116]）。

米国の科学者で構成される独立助言グループJASONは、外国の研究機関と関わる前に主任研究者が考慮すべき一連の有益な質問を提案しており、それらはツールキットやチェックリストとして米国の研究者によって活用されている（JASON, 2019^[1]）。

6.8 多国間活動

G7諸国は2021年半ばに、研究エコシステムのセキュリティとインテグリティ（SIGRE）に関するワーキンググループを設立し、オープンで相互的な研究協力に対するリスクからG7全体の研究とイノベーションのエコシステムを保護すべく、共通原則を策定しようとしている（G7, 2021^[117]）。このワーキンググループは、研究インテグリティとセキュリティに関する理解を共有すべく、研究者・イノベーター・ビジネスリーダー・政策立案者のスキルや経験を結集し、バーチャルアカデミーとツールキットに向けた提案を作成する予定である。これは、国際研究開発体制のインテグリティの促進・保護に向け、ファイブアイズ諸国（オーストラリア、カナダ、ニュージーランド、英国、米国）間で確立されている対話を発展させるものである。

欧州委員会は、最近、研究とイノベーションに対する外国の干渉を軽減するツールキットを発表している（European Commission, 2022^[118]）。このツールキットは、職員・学生・研究成果・資産の保護に加え、

学問の自由、インテグリティ、研究機関の自治など、研究機関と大学の基本的価値の保護に向け、その支援を目的とした最善の実践を概説している。このツールキットに加え、ホライズンヨーロッパプロジェクトにおける情報分類では、潜在的に機微で、特定のリスク評価・管理の対象となる研究対象や情報の種類を特定している（表 6.1 機密技術・情報分野を参照）（European Commission, 2021^[71]）。

アジア太平洋経済協力会議（APEC）フォーラムは、*研究インテグリティに関する APEC 指導原則*を定め、研究の実施・管理責任を明確化している（APEC Human Resources Development Working Group, 2022^[119]）。透明性を高めるべく、この原則では、利益相反と考えられるもの、その可能性があるもの、及び実際の利益相反につながりうる金銭的・家族的・学術的・職業的、その他の利益を開示することを研究者に推奨している。同時に、研究者の利益の開示と管理を支援する枠組みを提供することが研究機関に推奨されている。

研究資金配分機関レベルでは、研究資金配分機関のネットワークであるサイエンスヨーロッパとグローバルリサーチカウンシル（GRC）が2021年、COVID-19への科学的対応の経験に触発され、研究の倫理・インテグリティ・文化について討議を始めている。一方、GRCは、2022年5月の総会で、*直ちに結果の出る研究の倫理・インテグリティ・文化に関する原則と実践についての声明*（Global Research Council, 2022^[120]）を承認している。これには研究セキュリティ関連の問題への配慮も含まれている。

7 | まとめ

予測不能で急速に変化する世界において、科学は、グローバルな社会的課題に対処するために必要な政策決定と技術開発に情報を提供するために不可欠な新しい知識を提供している。科学の発展には国際協力と科学的な自由が不可欠である。しかし、多くの国で、科学の不正流用や非難、研究への外国の干渉に対する懸念が高まっている。これらはグローバルな研究エコシステムのインテグリティに対する深刻な脅威であり、研究セキュリティとインテグリティの双方を強化し、社会的信頼を高める方向で、こうした脅威を認識・管理する政策的措置が必要とされている。

本報告書では、研究の自由を守り、国際研究協力を推進し、開放性と無差別性を確保しながら、国家と経済の安全保障を守るための政策と行動について述べている。研究インテグリティとセキュリティに対する責任は、国際的な研究エコシステムに関わる複数の主体に分散している。これらの主体には、各国政府・研究資金配分機関・研究機関・大学・学協会・大学協会等が含まれる。これらの主体は、国内外で協力し、科学への信頼を将来にわたって確保するための効果的な政策を立案・実施しなければならない。

本報告書の冒頭でまとめた7つの包括的な提言（第2章を参照）は、研究インテグリティのより広い枠組みの一環として、各国が研究セキュリティに取り組む際に役に立つものと思われる。それぞれの提言について、第6章で紹介した優れた実践例をもとに、数多くの政策オプションが提案されている。

研究インテグリティとセキュリティは、OECD加盟国共通の懸念事項であるが、その背景はかなり異なる。従って、各政策提言の優先順位や行動に関連したオプションは国によって異なるものと思われる。政府・研究資金配分機関・研究機関・大学は、意図しない結果を監視する一方で、定期的にセキュリティ戦略の成熟度を評価し、政策や行動を修正することにより、それらの効果を保証する必要がある。

参照文献

- 116th Congress (2021), William M. (Mac) *Thornberry National Defense Authorization Act for Fiscal Year 2021*, <https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf>. [64]
- All European Academies (2017), *The European Code of Conduct for Research Integrity*, <https://www.allea.org/wp-content/uploads/2017/05/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017.pdf>. [34]
- American Association of University Professors (2014), *Recommended Principles to Guide Academy-Industry Relationships*, The AAUP Foundation, https://www.aaup.org/file/Academy-Industry%20Relationships_0.pdf. [4]
- APEC Human Resources Development Working Group (2022), *APEC Guiding Principles for Research Integrity*, <https://www.apec.org/apecapi/publication/getfile?publicationId=1a7ab7d8-6d0c-4d94-be4b-2342cd08cdfa>. [119]
- Association of American Universities (AAU) and Association of Public Land-grant Universities (APLU) (2021), *Principles and Values to Guide Actions Relevant to Foreign Government Interference in University Research*, <https://www.aau.edu/key-issues/principles-and-values-guide-actions-relevant-foreign-government-interference-university>. [101]
- Association of Universities in the Netherlands (VSNU) (2021), *Framework Knowledge Security Dutch Universities*, <https://www.universiteitenvannederland.nl/files/documenten/Domeinen/Integrale%20veiligheid/VSNU%20Framework%20Knowledge%20Security%20Dutch%20Universities.pdf>. [82]
- Association Public Land-grant Universities (APLU); Association of American Universities (AAU); (2020), *University Actions to Address Concerns about Security Threats and Undue Foreign Government Influence on Campus*, <https://www.aplu.org/members/councils/governmental-affairs/CGA-library/effective-science-and-security-practices---what-campuses-are-doing/file>. [100]
- Australian Research Council (2020), *ARC Conflict of Interest and Confidentiality Policy*, <https://www.arc.gov.au/about-arc/program-policies/conflict-interest-and-confidentiality-policy>. [86]
- Australian Security Intelligence Organisation (2020), *ASIO Submission to the Parliamentary Joint Committee on Intelligence and Security*, <https://www.aph.gov.au/DocumentStore.ashx?id=9f0851be-082b-4b56-ac25-873163fb73c4&subId=699731>. [3]
- BBSRC, MRC and Wellcome Trust (2015), *BBSRC, MRC and Wellcome Trust Position Statement on Dual Use Research of Concern and Research Misuse*, <https://cms.wellcome.org/sites/default/files/wtp059491.pdf>. [10]
- Bekkers, F., W. Oosterveld and P. Verhagen (2019), *Checklist for Collaboration with Chinese Universities and Other Research Institutions*, <https://hcss.nl/report/checklist-for-collaboration-with-chinese-universities-and-other-research-institutions/>. [48]
- Bladwin, D. (1997), "The concept of security", *Review of International Studies*, Vol. 23/1, pp. 5-26, <https://doi.org/10.1017/s0260210597000053>. [129]
- Canadian Centre for Cyber Security (2020), *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats to the Health Sector*, <https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threats-health-sector>. [55]
- Centre for the Protection of National Infrastructure (CPNI) (2020), *Trusted Research Guidance for Academia*, <https://www.cpni.gov.uk/trusted-research-guidance-academia>. [73]
- Centre for the Protection of National Infrastructure (CPNI) (n.d.), *Checklist: Evaluating research proposals*, <https://www.cpni.gov.uk/system/files/Trusted%20Research%20Checklist%20for%20Academia.pdf>. [74]
- Centre for the Protection of National Infrastructure (CPNI) (n.d.), *Trusted Research Guidance for Academics*, <https://www.cpni.gov.uk/system/files/Trusted%20Research%20Guidance%20for%20Academia.pdf>. [56]

- Cho, I., B. Kingdollar and M. Soshi (2021), *Harvard professor Charles Lieber found guilty of lying about China ties*, The Harvard Crimson, https://www.thecrimson.com/article/2021/12/22/lieber-verdict-day6/?utm_source=Nature+Briefing&utm_campaign=f22b5a5686-briefing-dy-20220104&utm_medium=email&utm_term=0_c9dfd39373-f22b5a5686-45800330#.YeJY0h5Mxws.link (accessed on 15 January 2022) . [63]
- Committee on Economic, Social and Cultural Rights (2020), *General Comment No. 25 (2020) on Science and Economic, Social and Cultural Rights (Article 15 (1)(b) , (2) , (3) and (4) of the International Covenant on Economic, Social and Cultural Rights)* , <https://undocs.org/E/C.12/GC/25>. [136]
- Committee on Responsible Science et al. (2017), *Fostering Integrity in Research*, National Academies Press, Washington, D.C., <https://doi.org/10.17226/21896>. [7]
- Committee on Science and Security (2019), *International Research & Global Collaboration*, <http://www.rochester.edu/research/pdfs/international-research-guidelines.pdf>. [105]
- Department for Business, Energy & Industrial Strategy (2021), *National security and investment act: guidance for the higher education and research-intensive sectors*, <https://www.gov.uk/government/publications/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors/national-security-and-investment-act-guidance-for-the-higher-education-and-research-intensive-sectors> (accessed on 5 August 2021) . [68]
- Department of Education, Skills and Employment (2021), *Case studies – cybersecurity*, <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-cybersecurity> (accessed on 13 January 2022) . [58]
- Department of Education, Skills and Employment (2021), *Case studies – due diligence, risk assessments and management*, <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-due-diligence#toc-case-study-1-safeguarding-national-security> (accessed on 13 January 2022) . [46]
- Department of Education, Skills and Employment (2021), *Case studies – governance and risk frameworks*, <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/case-studies/case-studies-governance-and-risk-frameworks#toc-case-study-3-protecting-academic-freedom> (accessed on 13 January 2022) . [52]
- Department of Justice (2021), *Hospital researcher sentenced to prison for conspiring to steal trade secrets and sell to China*, <https://www.justice.gov/opa/pr/hospital-researcher-sentenced-prison-conspiring-steal-trade-secrets-and-sell-china> (accessed on 24 March 2022) . [41]
- Department of Justice (2020), *The China Initiative: year-in-review (2019-20)* , <https://www.justice.gov/opa/pr/china-initiative-year-review-2019-20> (accessed on 13 May 2022) . [61]
- Department of Justice (2018), *Attorney general Jeff Session's China Initiative fact sheet*, <https://www.justice.gov/opa/speech/file/1107256/download> (accessed on 18 June 2020) . [62]
- Department of Justice (n.d.), *Information about the Department of Justice's China Initiative and a compilation of China-related prosecutions since 2018*, <https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related> (accessed on 8 May 2021) . [60]
- D'Hooghe, I. and J. Lammertink (2020), *Towards Sustainable Europe-China Collaboration in Higher Education in Research*, <https://leidenasiacentre.nl/wp-content/uploads/2020/10/Towards-Sustainable-Europe-China-Collaboration-in-Higher-Education-and-Research.pdf>. [2]
- European Commission (2022), *Tackling R&I Foreign Interference*, <https://doi.org/10.2777/513746>. [118]
- European Commission (2021), *Classification of Information in Horizon Europe Projects*, https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/horizon/guidance/classification-of-information-in-he-projects_he_en.pdf. [71]
- European Commission (2020), *Concept Note on Tackling Foreign Interference in Higher Education Institutions and Research Organisations*, <https://s3.eu-central-1.amazonaws.com/euobs-media/3ef6dc3d60ee27a2df16f62d47e93fdc.pdf>. [132]
- European Union Science Diplomacy Alliance (n.d.), *www.science-diplomacy.eu*, <https://www.science-diplomacy.eu/> (accessed on 22 January 2022) . [18]
- Fedasiuk, R. and E. Weinstein (2020), *Universities and the Chinese Defense Technology Workforce*, Center for Security and Emerging Technology, <https://doi.org/10.51593/20200043>. [131]

- Flagg, M. and Z. Arnold (2021), *New Research Security Institutions Short Policy Brief*, Center for Security and Emerging Technology, <https://doi.org/10.51593/20200051>. [130]
- Foreign & Commonwealth Office and Foreign, Commonwealth & Development Office (2013), *Academic Technology Approval Scheme (ATAS)*, <https://www.gov.uk/guidance/academic-technology-approval-scheme> (accessed on 5 August 2021) . [69]
- French Presidency of the Council of the European Union (2022), *Marseille Declaration on International Cooperation in Research and Innovation (R&I)*, <https://presidence-francaise.consilium.europa.eu/media/xi1kxzg/marseille-declaration.pdf>. [32]
- G7 (2021), *G7 Research Compact*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1001133/G7_2021_Research_Compact_PDF_356KB_2_pages.pdf [117]
- Gattolin, A. (2021), *Rapport D'information*, <http://www.senat.fr/rap/r20-873/r20-8731.pdf>. [51]
- German National Academy of Science Leopoldina (n.d.), *Contact persons and commissions in Germany responsible for ethics of security-relevant research*, https://www.leopoldina.org/ueber-uns/kooperationen/gemeinsamer-ausschuss-dual-use/kommissionsliste/?tx_leoinstitutions_institutionslist%5Baction%5D=list&tx_leoinstitutions_institutionslist%5Bcontroller%5D=List&cHash=8e12faffd7dcfa05a6ef95703d72a04a (accessed on 23 February 2022) . [116]
- German National Academy of Sciences Leopoldina (n.d.), *Conferences and workshops of the Joint Committee on the Handling of Security-Relevant Research*, <https://www.leopoldina.org/en/about-us/cooperations/joint-committee-on-dual-use/dual-use-conferences-and-workshops/>. [114]
- German National Academy of Sciences Leopoldina (n.d.), *Information on selected security-relevant research topics and case studies*, <https://www.leopoldina.org/en/about-us/cooperations/joint-committee-on-dual-use/research-topics-and-case-studies/#c8500> (accessed on 16 January 2022) . [43]
- German National Academy of Sciences Leopoldina and German Research Foundation (DFG) (2020), *Joint Committee of the DFG and Leopoldina on the Handling of Security-Relevant Research - Third Progress Report*, https://www.leopoldina.org/uploads/tx_leopublication/2020_Progress_Report_Joint_Committee_Dual_Use.pdf. [115]
- German Rectors' Conference (2020), *Guidelines and Standards in International University Cooperation*, <https://www.hrk.de/resolutions-publications/resolutions/beschluss/detail/guidelines-and-standards-in-international-university-cooperation/>. [102]
- German Research Foundation (DFG) (n.d.), *Guidelines for Avoiding Conflicts of Interest*, https://www.dfg.de/formulare/10_201/10_201_en.pdf. [88]
- German Research Foundation (DFG) (n.d.), *Proposal Preparation Instructions*, https://www.dfg.de/formulare/54_01/54_01_en.pdf. [94]
- German Research Foundation (DFG) and German National Academy of Sciences Leopoldina (2014), *Scientific Freedom and Scientific Responsibility*, https://www.dfg.de/download/pdf/dfg_im_profil/geschaefsstelle/publikationen/stellungnahmen_papiere/2014/dfg-leopoldina_forschungsrisiken_de_en.pdf. [93]
- Global Research Council (2022), *Statement of Principles and Practices for Research Ethics, Integrity, and Culture in the Context of Rapid-Results Research*, https://globalresearchcouncil.org/fileadmin/documents/GRC_Publications/SoP_Research_Ethics_May_2022.pdf. [120]
- Global Research Council (n.d.), *Statement of Principles for Research Integrity*, https://www.globalresearchcouncil.org/fileadmin/documents/GRC_Publications/grc_statement_principles_research_integrity_FINAL.pdf. [121]
- Government Accountability Office (2020), *Agencies Need to Enhance Policies to Address Foreign Influence*, <https://www.gao.gov/assets/gao-21-130.pdf>. [90]
- Government of Canada (2021), *Executive summary of national security guidelines for research partnerships*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98256.html (accessed on 5 August 2021) . [70]
- Government of Canada (2021), *Risk assessment form*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98257.html (accessed on 5 August 2021) . [78]
- Government of Canada (2021), *Safeguarding your research*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html (accessed on 13 May 2022) . [79]
- Government of Canada (2021), *Scenario 2 - participation in foreign talent and recruitment programs*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98278.html (accessed on 13 January 2022) . [47]

- Government of Canada (2021), *Scenario 3 - insider threats and research theft*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98279.html (accessed on 13 January 2022) . [42]
- Government of Canada (2021), *Scenario 5 - security and travel*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98281.html (accessed on 13 January 2021) . [59]
- Government of Canada (2020), *Policy statement on research security and covid-19*, <https://www.canada.ca/en/innovation-science-economic-development/news/2020/09/policy-statement-on-research-security-and-covid-19.html> (accessed on 8 May 2021) . [77]
- Government of Canada (2016), *Conflict of interest and confidentiality*, http://www.science.gc.ca/eic/site/063.nsf/eng/h_90108244.html?OpenDocument (accessed on 9 May 2021) . [87]
- Government of Canada (n.d.), *About us*, https://www.ic.gc.ca/eic/site/063.nsf/eng/h_98090.html (accessed on 8 May 2021) . [83]
- Government of the United Kingdom (2021), *Dedicated government team to protect researchers' work from hostile activity*, <https://www.gov.uk/government/news/dedicated-government-team-to-protect-researchers-work-from-hostile-activity> (accessed on 4 October 2021) . [75]
- Government of the United Kingdom (2021), *Export controls applying to academic research*, <https://www.gov.uk/guidance/export-controls-applying-to-academic-research> (accessed on 23 September 2021) . [40]
- Human Brain Project (n.d.), *Responsible research and innovation*, <https://www.humanbrainproject.eu/en/about/project-structure/work-packages/work-package-9/> (accessed on 22 January 2022) . [111]
- Human Rights Watch (2021), *They Don't Understand the Fear We Have*, <https://www.hrw.org/report/2021/06/30/they-dont-understand-fear-we-have/how-chinas-long-reach-repression-undermines>. [50]
- Integrated Innovation Strategy Promotion Council (2021), *Regarding the Response Policy for Securing Research Integrity Against New Risks Associated with the Internationalization and Openness of Research Activities*, <https://www8.cao.go.jp/cstp/tougosenryaku/9kai/siryoy1-2.pdf>. [80]
- InterAcademy Partnership (IAP) (2016), *Doing Global Science: A Guide to Responsible Conduct in the Global Research Enterprise*, <https://www.interacademies.org/publication/doing-global-science-guide-responsible-conduct-global-research-enterprise>. [36]
- International Science Council (ISC) (2018), *Statutes and Rules of Procedure*, <https://council.science/wp-content/uploads/2018/06/ISC-Statutes-approved-May-2018.pdf>. [31]
- JASON (2019), *Fundamental Research Security*, https://nsf.gov/news/special_reports/jasonsecurity/JJSR-19-21FundamentalResearchSecurity_12062019FINAL.pdf. [1]
- Kivimaa, P. (2022), "Transforming innovation policy in the context of global security", *Environmental Innovation and Societal Transitions*, Vol. 43, pp. 55-61, <https://doi.org/10.1016/j.eist.2022.03.005>. [128]
- Langtvedt, N. (2020), *The act on ethics and integrity in research*, <https://www.forskningsetikk.no/en/resources/the-research-ethics-library/legal-statutes-and-guidelines/the-act-on-ethics-and-integrity-in-research/> (accessed on 22 February 2022) . [110]
- Leibniz Association (2021), *Risk Management in International Scientific Cooperation – points to consider*, https://www.leibniz-gemeinschaft.de/fileadmin/user_upload/Bilder_und_Downloads/%C3%9Cber_uns/Internationales/Risk_management_in_international_scientific_cooperation.pdf. [98]
- Lund University (2020), *Research Ethics*, https://www.student.lth.se/fileadmin/lth/genombrottet/Course_Plan_Research_Ethics_2021_GEM090F_ENG_.pdf. [109]
- Max Planck Society (2021), *Guidelines for Responsible Conduct*, <https://www.mpg.de/18156413/leitplancken.pdf>. [96]
- Max Planck Society (2021), *Guidelines for the Development of International Collaborations of the Max-Planck-Gesellschaft*, <https://www.mpg.de/16784189/mpg-guidelines-for-international-cooperations-2021.pdf>. [95]
- Max Planck Society (n.d.), *Ombudspersons*, <https://www.mpg.de/about-us/organisation/ombudspersons> (accessed on 22 February 2022) . [97]
- McGill University (n.d.), *Foreign interference*, <https://www.mcgill.ca/research/about/foreign-interference> (accessed on 7 May 2021) . [133]

- Medical Research Council (MRC), Biotechnology and Biological Sciences Research Council (BBSRC), and Wellcome Trust (2021), *Managing Risks of Research Misuse: joint policy statement*, <https://www.ukri.org/publications/managing-risks-of-research-misuse-joint-policy-statement/>. [92]
- Merriam-Webster (n.d.), *Due diligence*, <https://www.merriam-webster.com/dictionary/due%20diligence> (accessed on 28 September 2021) . [11]
- Merton, R. (1973), *The Normative Structure of Science*, University of Chicago Press, <https://press.uchicago.edu/ucp/books/book/chicago/S/bo28451565.html>. [141]
- Ministerial Conference on the European Research Area (2020), *Bonn Declaration on Freedom of Scientific Research*, https://www.bmbf.de/files/10_2_2_Bonn_Declaration_en_final.pdf. [13]
- Ministry of Education, Culture and Science (2020), *Knowledge Security in Higher Education and Research*, <https://www.government.nl/documents/letters/2020/11/27/knowledge-security-in-higher-education-and-research>. [81]
- National Academies of Sciences, Engineering and Medicine (2020), *Co-chairs appointed to lead new national science, technology, and security roundtable*, <https://www.nationalacademies.org/news/2020/10/co-chairs-appointed-to-lead-new-national-science-technology-and-security-roundtable#:~:text=Roundtable%20%7C%20National%20Academies-,Co%2DChairs%20Appointed%20to%20Lead%20New,Science%2C%20Technology%2C%20and%20> (accessed on 31 August 2021) . [112]
- National Cyber Security Centre (2019), *The Cyber Threat to Universities*, <https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities>. [54]
- National Institutes of Health (n.d.), *What is research integrity*, https://grants.nih.gov/policy/research_integrity/what-is.htm. [124]
- National Science & Technology Council (2021), *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>. [72]
- National Science and Technology Council (2022), *Guidance for Implementing National Security Presidential Memorandum 33 (NSPM-33) on National Security Strategy for United States Government-supported Research and Development*, <https://www.whitehouse.gov/wp-content/uploads/2022/01/010422-NSPM-33-Implementation-Guidance.pdf>. [67]
- National Science Foundation (2020), *NSF creates new research security chief position*, https://www.nsf.gov/news/news_summ.jsp?cntn_id=300086 (accessed on 8 May 2021) . [85]
- National Science Foundation (n.d.), *Research security*, <https://beta.nsf.gov/research-security> (accessed on 24 February 2022) . [45]
- New Zealand Government (2021), *Trusted Research*, <https://protectivesecurity.govt.nz/assets/Campaigns/PSR-ResearchGuidancespreads-17Mar21.pdf>. [76]
- OECD (2022), *Recommendation of the Council for Facilitating International Technology Co-operation with and among Businesses*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0282>. [27]
- OECD (2021), *OECD Calculations Based on Scopus Custom Data, Elsevier, Version 5.2021, September 2021*, https://stip.oecd.org/stats/SB-StatTrends.html?i=INTL_20_X&v=3&t=2006,2020&s=OECD (accessed on 2 September 2021) . [19]
- OECD (2021), *OECD Science, Technology and Innovation Outlook 2021: Times of Crisis and Opportunity*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/75f79015-en>. [21]
- OECD (2021), *Recommendation of the Council Concerning Access to Research Data from Public Funding*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0347>. [28]
- OECD (2021), *Recommendation of the Council on International Co-operation in Science and Technology*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0237>. [26]
- OECD (2020), *Why Open Science Is Critical to Combatting COVID-19*, https://read.oecd-ilibrary.org/view/?ref=129_129916-31pgjnl6cb&title=Why-open-science-is-critical-to-combatting-COVID-19. [22]
- OECD (2019), *Recommendation of the Council on Artificial Intelligence*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>. [30]
- OECD (2019), *Recommendation of the Council on Responsible Innovation in Neurotechnology*, <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0457#mainTex>. [29]

- OECD (2015), *Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document*, OECD Publishing, Paris, <https://dx.doi.org/10.1787/9789264245471-en>. [53]
- OECD (2015), “Making Open Science a Reality”, *OECD Science, Technology and Industry Policy Papers*, No. 25, OECD Publishing, Paris, <https://dx.doi.org/10.1787/5jrs2f963zs1-en>. [15]
- OECD (2009), *Co-ordinating Committee for Facilitating International Research Misconduct Investigations*, <http://www.oecd.org/sti/inno/42713295.pdf>. [127]
- OECD (2009), *Investigating Research Misconduct Allegations in International Collaborative Research Projects*, <http://www.oecd.org/sti/inno/42770261.pdf>. [140]
- OECD (2007), *Report from the Workshop on Best Practices for Ensuring Scientific Integrity and Preventing Misconduct*, <http://www.oecd.org/science/inno/40188303.pdf>. [139]
- OECD (n.d.), *Scientometrics*, <https://www.oecd.org/sti/inno/scientometrics.htm> (accessed on 25 February 2022) . [20]
- Office of Science and Technology Policy (2020), *Enhancing the Security and Integrity of America's Research Enterprise*, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/07/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise.pdf>. [6]
- Office of Science and Technology Policy (2000), “Federal policy on research misconduct”, *Federal Register*, Vol. 65/235, pp. 76260-76264, <https://www.govinfo.gov/content/pkg/FR-2000-12-06/html/00-30852.htm>. [17]
- Parliamentary Joint Committee on Intelligence and Security (2021), *Official Committee Hansard: National security risks affecting the Australian higher education and research*, https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt/3ca6fe4f-b221-48f6-812e-ccfd3cd59d55/toc_pdf/Parliamentary%20Joint%20Committee%20on%20Intelligence%20and%20Security_2021_03_19_8604_Official.pdf;fileType=application%2Fpdf#search=%22committe. [44]
- PricewaterhouseCoopers Aarata LLC (2021), *Research Integrity Investigation and Analysis Report*, https://www8.cao.go.jp/cstp/english/doc/report_en.pdf. [125]
- Public Safety Canada (2020), *Building Security Awareness in the Academic Community*, https://www.publicsafety.gc.ca/cnt/ntnl-scrnt/cntr-trrrsm/cntr-prlfrtn/sfgrdng-scnc/_fls/sfgrdng-scnc-cdm-cmmnty-en.pdf. [9]
- Purdue University (n.d.), *Detrimental research practices (DRPs)*, <https://www.purdue.edu/gradschool/academics/detrimental-research-practices.html> (accessed on 26 September 2021) . [8]
- Royal Society (2021), *Royal Society Submission to Home Office Consultation on Legislation to Counter State Threats*, <https://royalsociety.org/topics-policy/publications/2021/royal-society-submission-to-home-office-consultation-on-legislation-to-counter-state-threats/>. [113]
- Science Europe (2016), *Research Integrity Practices in Science Europe Member Organisations*, <https://doi.org/10.5281/zenodo.5060196>. [35]
- Shih, T., A. Gaunt and S. Östlund (2020), *Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration*, https://www.stint.se/wp-content/uploads/2020/02/STINT_Responsibile_Internationalisation.pdf. [103]
- Sutrop, M., M. Parder and M. Juurik (2020), “Research ethics codes and guidelines”, in *Handbook of Research Ethics and Scientific Integrity*, Springer International Publishing, Cham, https://doi.org/10.1007/978-3-030-16759-2_2. [16]
- Tardell, M. (2021), *Swedish Experiences of Research Collaboration with China: Challenges and the Way Forward*, <https://www.ui.se/globalassets/ui.se-eng/publications/other-publications/swedish-experiences-of-research-collaboration-with-china.pdf>. [49]
- The Norwegian National Research Ethics Committees (2016), *Guidelines for Research Ethics in Science and Technology*, https://www.forskningsetikk.no/globalassets/dokumenter/4-publikasjoner-som-pdf/60126_fek_guidelines_nent_digital.pdf. [122]
- The University of Texas at Austin (n.d.), *Conflict of interest, conflict of commitment, & outside activities*, <https://provost.utexas.edu/policies-and-compliance/conflict-of-interest> (accessed on 9 July 2020) . [104]
- The White House (2021), *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/> (accessed on 14 January 2022) . [66]

- The White House (2021), *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/?utm_source=link. [65]
- U15 Group of Canadian Research Universities (2019), *Mitigating Economic and/or Geopolitical Risks in Sensitive Research Projects*, <https://telfer.uottawa.ca/assets/research/documents/docs/Mitigating-economic-and-or-geopolitical-risks-in-sensitive-research-projects-dec-2019.pdf>. [99]
- U15 Group of Canadian Research Universities and Universities Canada (2019), *Travel Security Guide for University Researchers and Staff*, <https://www.univcan.ca/tools-for-navigating-changing-geopolitical-realities/>. [57]
- UK Research and Innovation (2021), *UK Research and Innovation Trusted Research and Innovation Principles*, <https://www.ukri.org/wp-content/uploads/2021/08/UKRI-170821-TrustedResearchandInnovationPrinciples.pdf>. [84]
- UK Research and Innovation (n.d.), *UK Research and Innovation Conflicts of Interest Policy*, <https://www.ukri.org/wp-content/uploads/2020/11/UKRI-171120-ConflictsOfInterestPolicy-Dec19.pdf>. [5]
- UK Research and Innovation (UKRI) (n.d.), *Declaration of Interests: Applicants*, <https://www.ukri.org/wp-content/uploads/2020/11/UKRI-261120-Declaration-of-Interests-for-applicants-v2.pdf>. [89]
- UNESCO (2021), *UNESCO Recommendation on Open Science*, <https://unesdoc.unesco.org/ark:/48223/pf0000379949.locale=en>. [25]
- UNESCO (2017), *Recommendation on Science and Scientific Researchers*, The United Nations Educational, Scientific and Cultural Organization, <https://unesdoc.unesco.org/ark:/48223/pf0000263618>. [24]
- UNESCO (2005), *Universal Declaration on Bioethics and Human Rights*, http://portal.unesco.org/en/ev.php-URL_ID=31058&URL_DO=DO_TOPIC&URL_SECTION=201.html. [137]
- UNESCO (1997), *Recommendation Concerning the Status of Higher-Education Teaching Personnel*, http://portal.unesco.org/en/ev.php-URL_ID=13144&URL_DO=DO_TOPIC&URL_SECTION=201.html. [138]
- United Nations (2013), *The Arms Trade Treaty*, https://thearmstradetreaty.org/hyper-images/file/ATT_English/ATT_English.pdf?templateId=137253. [37]
- United Nations (1972), *Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, <https://treaties.unoda.org/t/bwc> (accessed on 13 May 2022) . [39]
- United Nations (1968), *Treaty on the Non-proliferation of Nuclear Weapons (NPT)* , <https://www.un.org/disarmament/wmd/nuclear/npt/text> (accessed on 13 May 2022) . [38]
- United Nations Human Rights Office of the High Commissioner (1966), *International Covenant on Economic, Social and Cultural Rights*, <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx>. [23]
- United States Department of Energy (2021), *Unclassified Foreign National Access Program*, <https://www.directives.doe.gov/directives-documents/100-series/0142.3-BOrder-b-chg1-ltdchg>. [91]
- Universities UK (2020), *Managing Risks in Internationalisation: Security Related Issues*, <https://www.universitiesuk.ac.uk/policy-and-analysis/reports/Documents/2020/managing-risks-in-internationalisation.pdf>. [12]
- Universities UK (2019), *The Concordat to Support Research Integrity*, <https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-08/Updated%20FINAL-the-concordat-to-support-research-integrity.pdf>. [123]
- University Foreign Interference Taskforce (2021), *Guidelines to Counter Foreign Interference in the Australian University Sector*, <https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector/resources/guidelines-counter-foreign-interference-australian-university-sector>. [14]
- University of Michigan (n.d.), *Conflict of Interest (COI)* , <https://research-compliance.umich.edu/conflict-interest-coi> (accessed on 9 May 2021) . [107]
- University of Michigan (n.d.), *Welcome to PEERRS*, <http://my.research.umich.edu/peerrs/> (accessed on 9 May 2021) . [108]

- University of Toronto (2021), *Research Partnership Security Checklist for International Partnerships*, [106]
<https://www.utsc.utoronto.ca/research/sites/utsc.utoronto.ca.research/files/docs/Research-Partnership-Security-Checklist-for-International-Partnerships.pdf>.
- World Conference on Research Integrity (2013), *Montreal Statement on Research Integrity in Cross-Boundary Research Collaborations*, [126]
<https://wcrif.org/montreal-statement/file>.
- World Conference on Research Integrity (2010), *Singapore Statement on Research Integrity*, [33]
<https://wcrif.org/documents/327-singapore-statement-a4size/file>.
- World Intellectual Property Organization (1996), *WIPO Copyright Treaty (WCT)*, [135]
<https://wipolex.wipo.int/en/text/295157>.
- World Intellectual Property Organization (1979), *Paris Convention for the Protection of Industrial Property*, [134]
<https://wipolex.wipo.int/en/text/287556>.

付属書A 主要な概念と多様な視点

本報告書で使用する主な用語については、用語集（別欄3.1 用語集）で簡単な作業上の定義を示しているが、一部の用語は国やコミュニティによって使い方や捉え方が異なる。グローバルなエコシステムの中で共通認識を持つためには、この違いを理解することが重要である。そこで、この付属書では少数の国際的組織や国の例を挙げ、これらの重要な用語のいくつかをより詳しく再検討している。

研究インテグリティ

研究インテグリティに関するシンガポール声明（*The Singapore Statement on Research Integrity*）（World Conference on Research Integrity, 2010^[33]）は、広く認められた研究インテグリティの原則と、それに関連する研究者の責任について述べている。ここでは異なる国や文化を背景に研究インテグリティを検討し、詳細なガイドラインと活動を定めるための規範的基礎が提示されている。また、研究インテグリティの主要な原則と、それに伴う研究者の責任も定義されている。4つの原則とは、誠実性、説明責任、専門家としての礼儀と公平性、そして優れた管理責任である。研究インテグリティとは、研究開発活動の提案・実施・評価・報告において、これらの原則を遵守することである。4つの原則から、研究不正（「FFP」捏造、改ざん、盗用）、著者資格、ピアレビュー、利益相反の開示、研究倫理等に関する14の責任を導き出すことができる（シンガポール声明の焦点は個々の研究者にあることに留意）。

グローバルリサーチカウンシルの*研究インテグリティのための原則声明*（n.d.^[121]）は、研究インテグリティに根ざした国際環境づくりにおける研究資金配分機関の責任に焦点を当てている。その中で、研究資金配分機関についての原則は、リーダーシップ、推進、教育、透明なプロセス、不正行為に関する申し立てへの対応、研究支援条件、国際協力と定義されている。

欧州40カ国以上の50を超えるアカデミーで構成される全欧州アカデミー（2017^[34]）は、研究インテグリティの基本原則を信頼性・誠実性・尊重・説明責任と定義している。

ノルウェーの場合、科学的インテグリティは基本的な研究倫理にすでに取り込まれているものとされている。科学的インテグリティとは、真理を追究するという共通の目的のもと、優れた科学的実践を維持し、これを遵守することである。不正行為は優れた科学的実践に対する重大な違反である。また、科学的インテグリティの規範は、研究の種類を問わず、研究プロセスのあらゆる段階に適用される（The Norwegian National Research Ethics Committees, 2016^[122]）。

英国では、誠実性、厳密性、透明性、オープンなコミュニケーション、すべての人に対する配慮と尊重、説明責任が英国の研究インテグリティを支援するコンコルダート（Universities UK, 2019^[123]）の重要な要素とされている。

米国国立衛生研究所（NIH）によると、研究インテグリティとは、研究を提案・実施・評価する際に誠実かつ検証可能な方法を用いること、規則・規制・ガイドラインの遵守に特に注意して研究結果を報告すること、そして一般に認められている専門的な規範に従うこととされている（National Institutes of Health, n.d.^[124]）。

日本政府は、研究インテグリティを、「研究成果の共有と互惠性の維持、研究活動における説明責任と透明性の確保に向けて、日本の研究者及び研究機関が遵守すべきもの」と考えている。研究インテグリティには、「研究の国際化とオープン化の進展に伴い、個々の研究者が直面する新たなリスクに対応すること」も含まれると考えられている（図 A.1 研究インテグリティの様々な側面を参照）。（PricewaterhouseCoopers Aarata LLC, 2021^[125]）

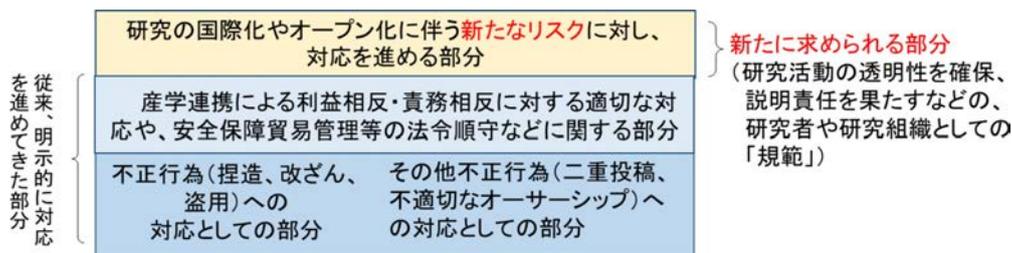


図 A.1 研究インテグリティの様々な側面

出典：内閣府 研究インテグリティに係る調査・分析報告書（PricewaterhouseCoopers Aarata LLC, 2021^[125]）

研究インテグリティの解釈には違いがあるものの、優れた研究の実施に向け、個々の研究者を対象とした一連の原則とガイドラインが必要であることはほとんどの国が認めている。また、国際協力において、研究インテグリティ、すなわち優れた研究実践に一定の注意が払われており（モンリオール声明を参照（World Conference on Research Integrity, 2013^[126]））、OECD-GSFは2009年に国際研究不正調査の推進に関する報告書と実践ガイドを作成している（OECD, 2009^[127]）。しかし、この国内及び国際的なガイダンスはいずれも、個々の研究者の行動と国際的な研究エコシステムのインテグリティに影響を与えるような研究セキュリティ関連のより広範な問題を考慮していない。

研究セキュリティ

一般に、セキュリティとは社会的価値の面で脅威が不在又はリスクが低いこと、あるいは脅威から十分に保護されていることを意味する。それは国民国家のみならず、個人・社会構造・技術システム・人類全体の保護も意味する（Kivimaa, 2022^[128]; Bladwin, 1997^[129]）。

研究インテグリティとは、研究の真実性と質のことであり、研究セキュリティとは、科学や研究におけるインプット・プロセス・アウトプットをリスク（不正アクセス・窃盗・スパイ行為）から保護し、さらに、これを特定及び／又は軽減する措置を意味する傾向にある。

一般的に研究セキュリティは、固有の規制や慣行を伴う技術及び／又は軍事的な問題と関連しているため、しばしば研究インテグリティとは区別される。例えば、韓国の場合、研究インテグリティは学術分野では一般的な概念であるのに対し、研究セキュリティは産業分野と関連づけられている。

米国の安全保障・新興技術研究センター（CSET）（Flagg and Arnold, 2021^[130]）は、研究セキュリティを「報酬・欺瞞・強制・窃盗など、違法又は一般的な規範に反する手段で外国の主体が科学研究を取得することを防ぐ措置」と定義している。

このように、グローバル化した研究エコシステムにおける研究セキュリティとは、研究に対する不当な政治的影響、研究成果の望ましくないデュアルユースへの応用、利益相反と責務相反、サイバー攻撃等を防ぐことを意味する。研究セキュリティの主な目的は、知的財産・知的知識・ノウハウを保護し、望ましくない国家や非国家主体によるこれらの資産の不当な搾取を防ぐことにより、国内外の研究システムのインテグリティと健全性に加え、国の経済的利益も保護することにある。

利益相反・責務相反

一般的に研究者とその所属機関は、しばしば複数の主体から資金援助を受けており、国際協力や官民パートナーシップにおいて複数の所属先や役職を持っている。このこと自体は必ずしも問題とはならない。しかし、利益相反や責務相反は行動をねじ曲げ、科学に対する国民の信頼を損なう可能性がある。利益相反と責務相反は重複しており、置き換えられて使われることもあるが、両者は以下のように区別することができる。

利益相反：利益相反とは、一次的利益に関する専門的な判断や行動が二次的利益によって不当に影響される

危険性がある一連の状況をいう（American Association of University Professors, 2014^[4]; UK Research and Innovation, n.d.^[5]）。利益相反には個人又は組織のレベルで金銭の授受を伴うことが多々ある。

責務相反：責務相反は、個人が複数の雇用主から過剰量の仕事や相反する職務を引き受ける状況で発生する可能性がある（Office of Science and Technology Policy, 2020^[6]）。複数の責務を負い、遂行能力に限界がある場合、これは個人から研究室や研究所に至る主体で起こり得る。

互恵性

公的資金による研究の成果の大半は研究者間で、また社会と共有されており、そのプロセスはますますオープンになりつつある。同時に、研究活動に伴う利益・不利益・負担も共有されている（The Norwegian National Research Ethics Committees, 2016^[122]）。互恵性とは、すべての協力パートナーが利益を享受し、負担を分担するようなやり方で、材料・知識・データ・施設と自然環境へのアクセス、トレーニングや人材の交流を交換することをいう。互恵性は、協力し合う研究パートナー間で能力に非対称性があったとしても、相互に有益な協力となるようにするものであるため、効果的な協力に必要なものである。従って、協力における互恵性とは、透明性、研究及び施設への平等なアクセス、データの共有、契約の遵守を意味する（D'Hooghe and Lammertink, 2020^[2]）。

互恵性が普遍的に受け入れられるためには、公平性と併せて考慮される必要がある。科学から得られる利益への公平なアクセスは、国際的な科学の包括的な規範枠組みに取り入れられている（第4章を参照）。近年、オープンサイエンスが強調されることで、公平なアクセスの確保が重視されるようになった。もし互恵性が、貢献した分しか得られない、あるいは誰もが等しく貢献する必要があるという意味であるなら、資源や能力の乏しい国や機関、個人に対する偏見が生まれ、現時点での力量の差がさらに広がる可能性がある。これは互恵性の本来の姿ではない。従って、互恵性と公平性を同時に考えることが重要である。

デュアルユース研究・技術

デュアルユース研究・技術は、他の有益な目的のために実施されているにもかかわらず、意図的に危害を加えたり、公衆衛生や国家安全保障を脅かすために利用されたりする可能性がある（Public Safety Canada, 2020^[9]; D'Hooghe and Lammertink, 2020^[2]）（別欄 3.1 用語集を参照）。

デュアルユース技術やその他の機微技術は、輸出管理規制によって管理されているが、民生技術とデュアルユース技術が明確に区別されていない場合が多々ある。JASON（2019^[1]）は、人工知能・ロボット工学・電池技術など、明らかにデュアルユースの可能性がある基盤的研究分野を管理することは事実上不可能であり、望ましいことでもない結論づけている。

ジョージタウン大学ウォルシュ外交学院の安全保障・新興技術研究センター（2020^[131]）の報告書は、軍事部門に関連する外国の機関（軍事大学、防衛関連企業等）と直接又は間接的に協力することのリスクを強調している。このような協力は、民間の技術や知識が外国で軍事目的に利用されるリスクを高めることになる。

外国の干渉 vs 外国の影響

一部の国では、外国の干渉と外国の影響が区別されている。この2つの用語の意味は重複しており、同義で使われることもある。しかし、両者が区別される場合、外国の干渉は、意図的に隠された望ましくない活動に適用されるのに対し、外国の影響は、透明で正常な外交関係を意味する。

外国の干渉：外国の主体によって、又は外国の主体のために行われる干渉で、強制的、非公然的、欺瞞的又は腐敗的で、国家の主権・価値・利益に反する行為（University Foreign Interference Taskforce, 2021^[14]; European Commission, 2020^[132]）。この範囲に含まれる行為としては、研究者が軍に所属していることの隠蔽、外国政府や企業との提携の非公開、サイバー攻撃等がある。（McGill University, n.d.^[133]）

外国の影響：外国の影響は、オープンで透明性のある方法で行使される（University Foreign

Interference Taskforce, 2021^[14]）。どの国も、様々な方法で他国に影響を与えている。例えば、文化交流の促進は一般的な活動であり、多くの国の政府が海外で文化イベントや語学教育を支援している。

付属書B グローバルな科学¹エコシステムにおける研究インテグリティに関する付託事項

この付託事項（ToR）は、OECDグローバル・サイエンス・フォーラム（GSF）の第42回会合において研究規範・基準・インテグリティに関するプロジェクトの開始が決定されたことを受け、スコーピンググループが作成したものである。

プロジェクト

課題

基礎科学の発見は、世界中の知性・ノウハウ・才能・資金・インフラを合わせて活用する、相互に関連した学際的で国際的なエコシステムのなかで起こることが多くなっている。研究の自由と国際協力は、科学の進歩の基礎となるものである。科学的情報やデータのオープンで透明性のあるコミュニケーションと普及及び資料の共有は、グローバルな科学エコシステムが効果的に機能する上で不可欠とされており、一般的にこのオープン性は無差別・公平・説明責任等の価値観と関連づけられている。また、研究協力では、すべてのパートナーの利益となるように資料や知識を交換する互惠主義と、最高のアイデアやイノベーションの実現のために公平な競争環境を確保する能力主義という概念が考慮されている。エコシステムが効果的に機能する上で、これらの慣行と規範²の尊重は必須であると科学界では一般に受け止められている。

基本的な科学知識はグローバルな公共財とみなすことができるが、各国及び／又は主体によるこの知識の利用は、各国のイノベーションシステムの有効性に依存しており、一部は知的財産に関する国際規制体制下に置かれている（World Intellectual Property Organization, 1979^[134]; 1996^[135]）。しかし、研究とイノベーションは連続しており、競争前研究（グローバルな公共財）と競争的研究（知的財産権保護の対象）の境界は曖昧な場合が多々ある。その結果、科学のグローバルな機能と経済的な見返りに対する様々な期待との間に緊張関係が生まれる。政府やその他の主体は、自身のアジェンダには整合するものの、確立された研究協力の規範・原則とは矛盾する活動に関わることにより、グローバルな科学エコシステムのインテグリティを損なう可能性がある。

一方、地球温暖化、生物多様性の損失、自然災害、経済的移民、健康パンデミックなど、社会が国境を問わない一層複雑な課題に直面する中、公共部門のみならず、民間部門の主体も含む幅広い関係者が協力して、これらの課題に取り組む必要がある。これはすべての国にとってグローバルな公共財であり、経済発展のために必要でもある。COVID-19パンデミックにより、危機時における国際的かつ部門横断的な科学協力の重要性とその課題の両方が明らかとなった。国や部門を超えて科学的データ・資料・結果を共有したことにより、科学界は当面の危機に対応するための政策の立案と実施を支援することができた。新しい診断法と治療法の開発には、今後も国際協力と開放性が不可欠であることは明らかである。ワクチンの開発競争に勝利するのは誰か、また、それに伴う公益と潜在的な経済的利益がどのように分けられるのか、これらははるかに曖昧な問題であるが、地政学や経済的利益が主な決定要因ではないと考えるのは賢明ではないだろう。厳しいプレッシャーと世間の監視の中で、倫理基準を守り、研究の厳密性とインテグリティを確保することは、国

- 1 このプロジェクトはSTEMや人文・社会科学（SSH）を含むすべての科学分野を対象としている。
- 2 マートンのCUDOS規範（1973^[141]） - 普遍主義、共同主義、公平無私、組織的な懐疑主義
 普遍主義：科学的妥当性はその参加者の社会的・政治的地位及び個人的属性とは無関係。
 共同主義：すべての科学者が科学的財産を共同で所有し、集団で共同作業を推進。
 公平無私：科学機関はそれを構成する各個人の利益よりも共通の科学事業の利益のために行動。
 組織的な懐疑主義：科学的主張を受け入れる前にこれを批判的に精査すべき。

際的な科学エコシステムが COVID-19 のパンデミックに対応する上で大きな課題となっている。

このような緊張感はあるものの、これまで国際的な科学エコシステムはかなりよく機能する傾向にあった。一方、国際的に認められた規範的な合意や法的規制は、民主的なプロセスが必要なチェックとバランスを提供することで、広く尊重される枠組みの条件を作り出した（International Science Council (ISC), 2018^[31]; World Intellectual Property Organization, 1979^[134]; 1996^[135]; United Nations Human Rights Office of the High Commissioner, 1966^[23]; 2020^[136]）（UNESCO, 2017^[24]; 2005^[137]; 1997^[138]）。異常事態が発生することも時にはあったが、長い時間にわたって科学の普遍性はほぼ維持されてきた。しかし、一部の政府や非国家主体が、確立された規範や慣行をくつがえし、オープンな研究環境を自らの利益のために利用する動きがますます巧妙化しており、これにともない、新たな課題や脅威が生まれつつある。不正な情報伝達は、現在、OECD加盟国の多くで国家及び経済の安全保障上の重大なリスクと見なされている。これは、助成金提案のピアレビュー、研究者養成、人材採用、共同研究など、様々な研究活動のインテグリティに大きく影響する。これらの問題に対処し、グローバルな科学エコシステムのインテグリティを確保しなければ、国際協力や科学への信頼が著しく損なわれることになる。

研究インテグリティと研究エコシステムを強化するための体系的なアプローチ

この活動の2つの目的は、研究エコシステムのインテグリティに焦点を当てた加盟各国の事例研究・政策・適用される法律・規制・手続きを特定し、つきあわせること、そして研究インテグリティと研究の自由を確保する上で各国が採用し得る優れた実践を特定することである。

このプロジェクトの目的は、利益相反や責務相反³に対処し、研究インテグリティを促進するための実践的な情報と提言を各国に提供することにある。また、国際ワークショップを開催し、国を超えてステークホルダー間で相互学習と議論を促進することを意図している。

政策提言やオプションを含め、最終結果は報告書にまとめられる。とりあげる主な問いは以下の通りである。

1. 政府や管轄の科学当局は、どのような原則や規範をもとに研究や国際協力を支援しているか？どのような規制・政策・慣行をもとにそれらの原則を運用し、ひいては国内及びグローバルな研究エコシステムのインテグリティを高めるのか。
2. 政府や管轄の科学当局は、研究エコシステムにおける利益相反と責務相反の開示をどのように奨励し、防止・軽減・管理しているか。
3. 管轄の科学当局は、国家と経済の安全保障と科学協力の推進及び学問の自由・開放性・無差別性の保護のバランスをどのようにとっているか。
4. 政府は、抑圧的な影響、敵対的な主体、外国の干渉など、研究体制のインテグリティに対するリスクについて、大学・研究機関・研究者の認識をどのようにして高められるか。大学等の研究実施機関や研究資金配分機関は、研究システムのインテグリティを脅かす行為に対し、そのリスクをどのように軽減し、あるいはこれに対処することができるのか。
5. 研究機関は、研究エコシステムのインテグリティを維持すべく、既存の規範や基準をどのように実践しているか、又は新たな対策を検討しているか。既存のルールを破壊、一般に認められた学問的規範を破棄、又は学問の自由や民主主義・人権規範を無視する主体など、新規の又は発生しつつある課題や対立に研究機関はどのように対処しているか。

3 利益相反は、一次的利益に関する専門的な判断や行動が二次的利益によって不当に影響される危険性がある一連の状況である（American Association of University Professors, 2014^[4]; UK Research and Innovation, n.d.^[5]）。責務相反は、個人が複数の雇用主から過剰量の仕事や相反する職務を請け負う状況で発生する可能性がある（Ministerial Conference on the European Research Area, 2020^[13]）。利益相反と責務相反は重複しており、置き換えられて使われることがある。研究インテグリティに適用される定義は他にまとめられている（JASON, 2019^[11]）。

6. 研究者と研究機関は、学生・チームメンバー・研究パートナーを選ぶ際、又は資金援助を受けるとき、無差別と研究の自由の原則を堅持した上で、研究インテグリティに対するリスクを考慮しつつ、十分な情報を得た上で、バランスのとれた決定をどのように行うのか。
7. 国際的研究パートナーシップの可能性の評価に当たり、どのような便益リスク分析が行われているか。特に、海外のパートナーとの協力において、どのように相互の利益共有を確保しているか。
8. 研究資金配分機関は、ピアレビュープロセスを含む研究の評価が安全かつ公正に行われていること、また、それがアイデアや知的資本の不正流用につながらないことをどのように保証できるか。研究資金配分機関にとって、潜在的な利益相反と責務相反を検知・監視・管理する最善の方法はなんであるか？
9. 政府や研究資金配分機関は、研究機関に研究インテグリティを強化させるために、ガイダンスやインセンティブをどのように提供すればよいか。

研究規範・基準・インテグリティに関するGSFのこれまでの活動

本プロジェクトは、捏造・改ざん・盗用等の個人の不正行為に焦点を当てた、*科学的インテグリティの確保と不正行為の防止に向けた最善の実践に関するワークショップの報告*（OECD, 2007^[139]）と、*国際共同研究プロジェクトにおける研究不正行為の申し立てについての調査*（OECD, 2009^[140]）といった以前のOECD-GSFの作業と関連している。

GSFプロジェクト

このプロジェクトでは以下を行う：

1. 各国で認識されている課題と、それらが、関連する国際的な枠組み、国の政策、規制、施策・プログラム、組織的な慣行によってどの程度対応されているかに関する情報を収集する。
2. 収集した情報を各政治的イニシアティブレベルで水平的に分析する。必要に応じ、各国の情報の垂直方向の分析も実施する。
3. 国際的な専門家や関連のステークホルダーのコミュニティの代表者による国際ワークショップを開催し、追加の情報や事例研究を収集し、参加者間の相互学習を促進する。
4. 上記活動で得られた知見に基づき、優れた実践例、ステークホルダーへの政策提言・オプションを提供する最終報告書を作成する。

このプロジェクトは野心的であり、その意図は様々な国や機関における課題・懸念・行動を概観することにある。これにより、その後の詳細なフォローアッププロジェクト（研究インテグリティにおける特定の脅威に向けたツールキットやガイドラインの開発等）の基礎となり得る優れた実践の特定につながるであろう。

参加者案

このプロジェクトは、GSFの支援のもとで実施される予定である。プロジェクトの活動と成果を監督する専門家会合（EG）は、GSFへの各国代表団からの指名により設立される。

付属書C GSF 専門家会合のメンバー

国名	氏名	所属	組織
オーストラリア	Rachael Mitchell / Michelle Traynor-Brack / Freya Kaine	Director, National Security Engagement	Department of Education, Skills and Employment
カナダ	Sinead Tuite	Senior Director, Digital Research Infrastructure	Innovation, Science and Economic Development Canada / Government of Canada
カナダ	Martha Crago	Vice-Principal (Research and Innovation)	McGill University
フランス	Fabien Laurençon		Ministry of Economy and Finance, the Department of Economic Security
ドイツ	Andra-Maria Popa	Scientific Researcher	DLR project management agency
ドイツ	Claudia Heffftler ¹	Scientific Researcher	DLR project management agency
日本	岩瀬 公一	上席フェロー	科学技術振興機構（JST）研究開発戦略センター（CRDS）
日本	山崎 恵理子	参事官補佐（国際担当）	内閣府科学技術・イノベーション推進事務局
韓国	Inkyoung Sun	Head of Office of Development Cooperation Research	Science and Technology Policy Institute (STEPI)
韓国	Sun Kun Oh	Emeritus Professor of Physics	Konkuk University
オランダ	Peter-Paul Verbeek ²	Professor of Philosophy of Technology	University of Twente
ノルウェー	Helene Ingjerd	General Director	The Norwegian National Research Ethics Committees
ポルトガル	Bruno Béu		Foundation for Science and Technology
南アフリカ	Liapeng Matsau	Deputy Director	Research, South African Qualifications Authority
南アフリカ	Pradish Rampersadh	Chief Executive Officer	South African Council for Natural Scientific Professions (SACNASP)
スイス	Edwin Charles Constable	Professor	University of Basel
英国	Ben Sharman	Senior Global Policy Manager	UK Research and Innovation
英国	Sion Griffiths		International Research and Innovation Team BEIS
米国	Michael Imperiale	Associate Vice President for Research - Policy and Compliance	University of Michigan
米国	Bridget M. Turaga	Programme Director	Office of International Science and Engineering, National Science Foundation

1 2021年11月まで

2 2021年1月27日の第1回EG会議のみ出席。

岩瀬 公一 上席フェロー (科学技術イノベーション政策ユニット／海外動向ユニット)
村松 哲行 フェロー (科学技術イノベーション政策ユニット)

CRDS-FY2022-XR-01

日本語仮訳：
グローバルな研究エコシステムにおける
インテグリティとセキュリティ

経済協力開発機構 (OECD)
科学技術産業ポリシーペーパー (130号)

Original:

**INTEGRITY AND SECURITY IN THE GLOBAL
RESEARCH ECOSYSTEM**

OECD
SCIENCE, TECHNOLOGY AND INDUSTRY POLICY PAPERS
June 2022 No. 130

令和 4 年 11 月 November 2022
ISBN 978-4-88890-819-1

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
Center for Research and Development Strategy, Japan Science and Technology Agency

〒102-0076 東京都千代田区五番町7 K's 五番町
電話 03-5214-7481
E-mail crds@jst.go.jp
<https://www.jst.go.jp/crds/>

本書は著作権法等によって著作権が保護された著作物です。
著作権法で認められた場合を除き、本書の全部又は一部を許可無く複写・複製することを禁じます。
引用を行う際は、必ず出典を記述願います。

This publication is protected by copyright law and international treaties.
No part of this publication may be copied or reproduced in any form or by any means without permission of JST,
except to the extent permitted by applicable law.
Any quotations must be appropriately acknowledged.
If you wish to copy, reproduce, display or otherwise use this publication, please contact crds@jst.go.jp.

FOR THE FUTURE OF
SCIENCE AND
SOCIETY



CRDS

<https://www.jst.go.jp/crds/>

