2.2 英国

2.2.1 研究インテグリティの確保に関する要求と支援

(1) 研究インテグリティについて英国政府が動き出した背景

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

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

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

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

---

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

[120] 同上

[121] 同上

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

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

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

Research」 というキャンペーンを全国展開し、大学・教育機関向けに、研究インテグリティに関する理解を促すためのガイダンスとして、Trusted Research Guidance for Academics[125]を公表した。

(2) Trusted Research の目的と要求事項

Trusted Research は、英国が築いてきた研究・イノベーションセクターの成功を維持・向上させるため、英国の大学・研究機関が、国際共同研究に関して十分な情報を得た上で意思決定を行い、その際に自国の研究者及び学術的価値を保護できるよう支援することを目的としたイニシアチィブである。

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

Trusted Research に関する助言は、研究・大学コミュニティとの協議により作成され、世界をリードする英国の研究・イノベーションセクターが、知的財産、機密性の高い研究及び個人情報を保護しながら、国際的な科学協力を最大限に活用できるよう支援するように設計されている。

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

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

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

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

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

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

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

元管理され、適切なビザを取得していることを確認する。

✧ 出張時のアドバイス

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

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

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

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

文書名	概要
Trusted Research Checklist for Academia	研究インテグリティの観点から、研究者自身の国際共同研究提案に関する評価を支援するための質問事項として、以下を挙げている。 【新規パートナーについて】 ・ パートナーはなぜあなたと一緒に仕事をしたいと思うのか？ ・ 資金援助や関与の見返りに何を期待しているのか？ ・ その組織は、英国に敵対的と見なされる可能性のある国、あるいは英国とは異なる民主主義や倫理的価値観を持つ国と関係があるのか？ ・ パートナーに対するデューディリジェンスにより、敵対的な国家

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

文書名	概要
	とつながりのある軍や警察に代わって研究に関与していることが確認されたか？ ・ デューディリジェンスで得た情報の中で、あなたの研究が悪用されたり、意図しない応用でマイナスになる可能性はあるか？ ・ パートナーと研究を行うにあたり、法的、規制的、又は大学の方針的な制約があるか？ ・ 上記の質問に対する回答を考慮した上で、あなたや大学にとって、潜在的な風評リスクや倫理的リスクはないか？ ・ この研究についての決定を、あなたの部署内でエスカレーションさせる（上位レベルでの処理事項とする？）必要性があるか？ 【研究の関係性について】 ・ 提案されている覚書（MoU）の条件は、あなたの学部や大学の期待に沿うものか？ ・ 既存の知的財産（IP）、研究データ、機密情報、個人を特定できるデータなどをプロジェクトに提供しているか？提供している場合、その保護はどのように行われているのか？ ・ 生成された知的財産は誰が所有するのか？ ・ 生み出された知的財産を保護するための計画はあるか？ ・ あなたの学術機関の利益を保護するために、どのような契約上の要件を設けることができるのか？ ・ 研究パートナーは、あなたの機関の IT ネットワークにどのようにアクセスできるのか？彼らがアクセス権を持つ場合、それによってどのような広範な可視性がもたらされるのか？ ・ 類似した分野の研究の間で、物理的な分離や保護が必要なことが見られることはないのか？ 【既存のパートナーについて】 ・ 研究を進めることで、既存の研究パートナーとの間に利益相反の可能性が生じるか？ ・ 利益相反の潜在的可能性について、既存のパートナーと話をしたか？ ・ 秘密保持契約の条件を検討したか？これには、あなたが既存のパートナーに可視性を提供する必要があるとの期待が含まれているか？

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

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

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

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

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

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

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

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

年月	イニシアチィブ、プログラム、法令等	策定機関	関連する発行文書（ガイドライン等）	発行文書等の目的、概要等
2021 年 3 月	（輸出管理規制）	Export Control Joint Unit 、Department for International Trade[131]	Export controls applying to academic research	・ 「Trusted Research」に対応して、軍事目的に使用される危険性が高い分野の研究を行っている研究者やポスドク研究者を向けの輸出規制に関するガイドラインである。 ・ 科学技術研究に関する英国の輸出規制の適用有無を評価する方法及び国際研究協力に関するデューディリジェンス・プロセスの実施のあり方を説明し、研究者が輸出規制を正しく遵守することができるためのルールを示している。
2021 年 6 月	National Security and Investment Act（NSI 法）	Department for Business, Energy & Industrial Strategy (BEIS)[132]	National Security and Investment Act: guidance for the higher education and research-intensive sectors	・ NSI 法は、「Trusted Research」に対応して、英国の国家安全保障を脅かす可能性のある産業等に対する出資を規制するもの。国家安全保障上重要な 17 の機微な分野を指定し、特定の買収について英国政府に届け出ることを義務付けている。 ・ 2022 年 1 月に、大学等の研究機関における NSI 法の適用ルールを提示した左記ガイドラインを公表。
2021 年 5 月 25 日	Research Collaboration Advice Team (RCAT)の設立	Department for Business, Energy & Industrial Strategy (BEIS)[133]	―	・ RCAT は、「Trusted Research」に対応して、研究者を敵対行為から守り、輸出管理規制、サイバーセキュリティ、知的財産の保護等のセキュリティ関連の課題についての政府の助言を提供することを目的として設

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

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

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

年月	イニシアチィブ、プログラム、法令等	策定機関	関連する発行文書（ガイドライン等）	発行文書等の目的、概要等
				立された機関。 ・ 大学・研究機関に対して、国際的な研究に関連する国家安全保障上のリスクに関する公的なアドバイスを提供する最初の窓口となる（法的権限は無し）。
2021年8月	Trusted Research and Innovation (TR&I)	UKRI	Trusted Research and Innovation Principles	・ 国際共同研究のデューディリジェンスに関して、UKRIのファンディングを受ける機関への要求事項（原則）を定めた文書。 ・ UKRI から資金提供を受けている組織は､左記文書に示された原則を採用し、これらの原則に合致する管理及び対策を実施したことを証明できるようにする必要がある。
2022年6月	Managing risks in international research and innovation	UUK / UKRI / CPNI	Managing risks in international research and innovation: An overview of higher education sector guidance	・ CPNI 、UUK 及び UKRI の 3 機関が作成したガイドラインや主要原則（Trusted Research Guidance for Academia、Managing risks in internationalization: Security related issues 、Trusted Research and Innovation Principles）をハイレベルでまとめたガイダンス。 ・ 大学が国際的な研究・技術革新におけるセキュリティリスクを管理するために、上記の既存ガイドラインをどのように導入すればよいかを概説。

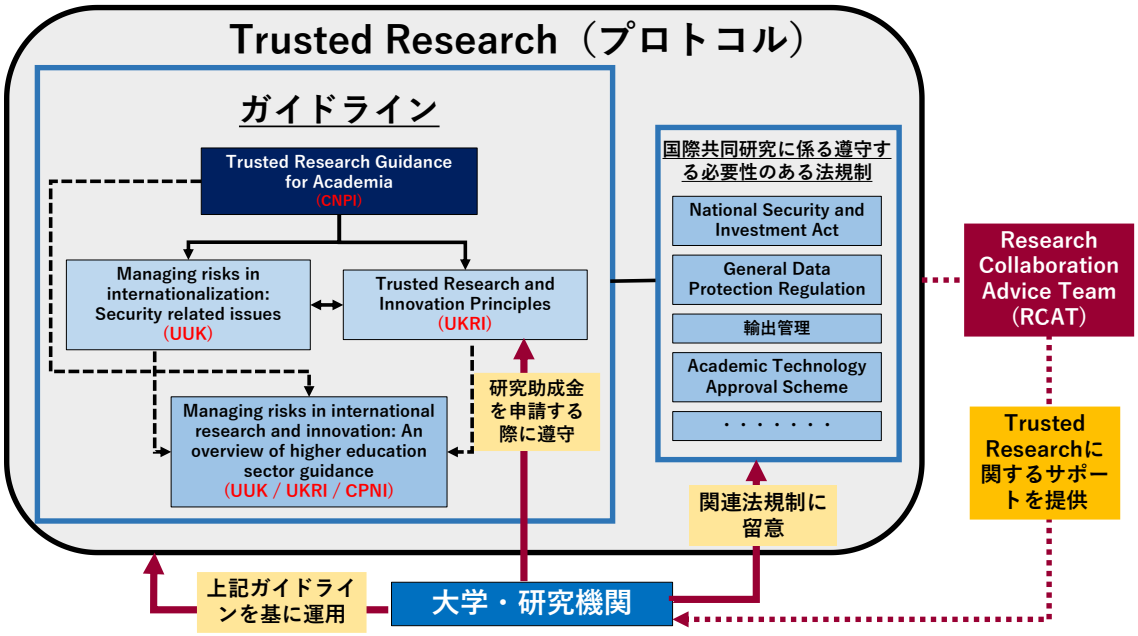

図 2-5：英国における研究インテグリティに関連する政府機関／大学機関／R&D 資金提供機関、これらの機関が発行するガイドライン、関連する法規制、大学・研究機関等との相互関係

2.2.2 資金配分機関等の取組

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

(1) Universities UK (UUK)の取組

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

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

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

(a) ガイドラインの位置付け

UUK は、本ガイドラインの位置づけとして、以下のように説明している。

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

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

(b) ガイドラインの目的

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

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

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

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

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

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

(c) ガイドラインの構成

本ガイドラインは、以下の 4 つの章から構成される。

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

【大学の評判と価値の防護】

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

【大学の人材の保護】

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

【キャンパスの保護】

・サイバーセキュリティ、キャンパスの土地・建物及びビジター

【大学のパートナーシップの保護】

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

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

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

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

135 同上

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

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

⑵ UKRI の取組

UKRI は、2021 年 8 月に、Trusted Research に基づき、国際共同研究のデューディリジェンスに関して、UKRI のファンディングを受ける機関への要求事項を定めた「Trusted Research and Innovation Principles」[136]を公表した。

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

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

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

(a) パートナーの適性評価

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

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

【法的枠組みと提携関係】

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

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

【価値観】

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

【利益相反】

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

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

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

(b) 情報・知識共有管理

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

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

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

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

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

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

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

【プロジェクトの成果物の公開】

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

【輸出管理】

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

(3) UUK、UKRI 及び CPNI の 3 機関共同の取組

UUK、UKRI 及び CPNI は、2022 年 6 月、これら 3 機関が共同で作成した主要原則とガイドラインをハイレベルでまとめた、「Managing risks in international research and innovation: An overview of higher education sector guidance」[137]を発表した。本ガイダンスは、大学が国際的な研究・技術革新におけるセキュリティリスクを管理するために、既存のガイダンス（Trusted research guidance for academia（CPNI 作成）、Managing risks in internationalization: Security related issues（UKRI 作成）、Trusted Research and Innovation Principles（UKRI 作成）をどのように導入すればよいかを概説したものである。

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

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

---

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

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

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

(a) 緩和策のチェックリスト

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

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

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

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

138 同上

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

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

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

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

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

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

139 同上

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

(b) ガイドラインの実施方法

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

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

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

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

スに対する使用など、セキュリティポリシーの「ストレステスト」を実施する。

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

2.2.3 主な大学の取組

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

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

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

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

(1) マンチェスター大学の事例[140,141]

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

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

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

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

質問は、以下の 7 つの項目から構成されている。

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

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

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

---

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

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

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

(2) 参考情報 1：ストラスクライド大学の事例[142]

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

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

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

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

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

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

(3) 参考情報 2：インペリアル・カレッジ・ロンドンの事例[143]

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

142 同上
143 同上

ィという確立された原則を基礎とするものである。

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

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

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

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

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

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

2.2.4 研究インテグリティ確保のための支援

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

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

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

国家安全保障上のリスクに関する公的なアドバイスを提供する最初の窓口となるものである[145]。

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

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

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

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

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

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

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

2.3 オーストラリア

2.3.1 概要

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

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

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

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

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

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

○外国干渉セキュリティをめぐる主な流れ

2019 年 11 月　　外国干渉タスクフォース（UFIT）ガイドラインを公表
　　豪州国立大がサイバー攻撃され 20 万人分の個人情報流出
2020 年 12 月　　外国関係法が成立
2021 年 11 月　　UFIT ガイドラインを改定
2022 年 3 月　　大学・研究機関の安全保障上のリスクに対し連邦議会が 27 の勧告

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

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

こうした豪中関係の悪化を背景に、豪州では 2019 年 8 月、政府（教育省、内務省、国防省など）と大学・研究機関が共同してタスクフォース（University Foreign Interference Taskforce: UFIT）を設置[150]。同 11 月には、外国干渉を排除するための通称・UFIT ガイドライン（Guideline to Counter Foreign Interference in the Australian University Sector、「大学セクターに対する外国の干渉に対抗するためのガイドライン」）を策定し発表した[151]。

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

UFIT は、外国からの干渉に対し大学への保護を強化するために設立された組織である。

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

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

2.3.2 研究インテグリティの確保のための要求と支援

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

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

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

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

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

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

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

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

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

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

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

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

2.3.3 資金配分機関等における取組

○資金配分機関

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

長く研究公正の分野においてその審査や是正の中心になってきた ARC と NHMRC だが、豪中関係が悪化し始めた 2018 年 7 月以降は、教育省の指示のもとで主要な国家安全保障機関と協力し、政府資金による研究の申請プロセスに対する監視を強化するようになった。その際、研究を支える利害関係について完全な透明性をもって研究助成金の申請が行われるよう、政府の外国干渉調整室と連携を取り合っているのが特徴である。これは 2019 年にできた UFIT ガイドラインを補完するための措置でもあった。

この措置に伴って、ARC は「利益相反・機密保持ポリシー（Conflict of Interest and Confidentiality Policy）」の改定を重ねており、外国機関との関係性を示す情報をより幅広

く開示するよう求めるようになっている[152]。なお、協力する国家安全保障機関の中には、内務省直轄の ASIO のほか連邦警察や豪州取引報告分析センター、豪州通信総局、豪州地理空間情報機構、国家情報局などのメンバーが含まれている。

ARC はまた、安全保障管理が必要な機微技術の識別にもたずさわっている。豪州では 2021 年 11 月に「重要技術のための青写真と行動計画」が発表された[153]。この計画によると、「重要技術」とは「国益を著しく向上させたり、リスクをもたらしたりする能力をもつ現在及び将来のテクノロジー」のこと。この文書には、国益のために重要技術を保護・促進するためのビジョンや戦略が規定されている。ARC は、競争的研究資金の申請にあたり、このリストに記載された技術が含まれている場合には、リスクがあるかどうかを検討することになっている。リスク要因には、次のような諸点が含まれるとしている。

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

こうしたリスクの存在が確認された場合、ARC は国家安全保障機関に報告し、懸念がある場合は助言するとされている。

○グループオブ８（Go8）

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

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

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

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

受けている。

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

○豪州大学連合（UA）

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

2.3.4 豪州国立大学（ANU）における取組

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

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

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

諮問委員会が行っている主な具体的措置の内容は次のとおり。

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

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

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

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

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

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

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

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

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

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

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

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

2.3.5 最近の動向

○連邦議会による国家安全保障リスク調査

豪州連邦議会のインテリジェンスとセキュリティに関する議会合同委員会（PJCIS）は 2022 年 3 月、大学・研究機関に影響を与える国家安全保障リスクに関する調査（The Inquiry into national security risks affecting the Australian higher education and research sector、「豪州の高等教育及び研究部門に影響を与える国家安全保障上のリスクに関する調査」）を発表し、その中で豪州の大学・研究機関で起きた数々の国家安全保障上のリスク事例を紹介するとともに、外国干渉に対処するための 27 の勧告を行った[162]。

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

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

---

161 foreign interference reporting - RegNet - ANU, <https://regnet.anu.edu.au/tags/foreign-interference-reporting>
162 Inquiry into national security risks affecting the Australian higher education and research sector – Parliament of Australia (aph.gov.au), <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Report>

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

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

○中国の軍事関連大学をめぐる追跡調査（トラッカー）

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

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

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

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

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

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

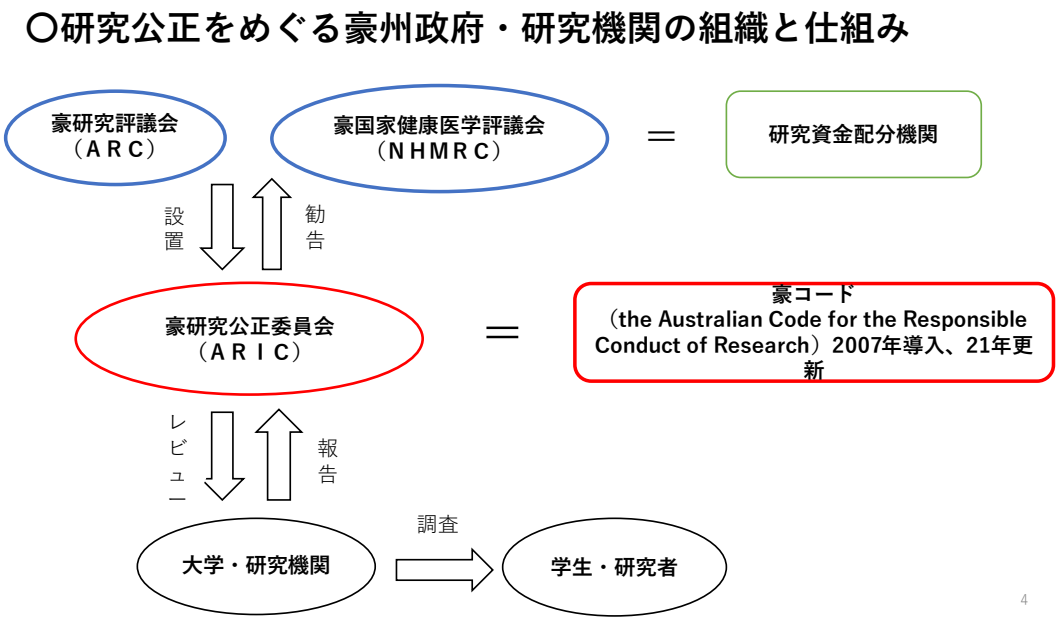

図 2-6：研究公正をめぐる豪州政府・研究機関の組織と仕組み

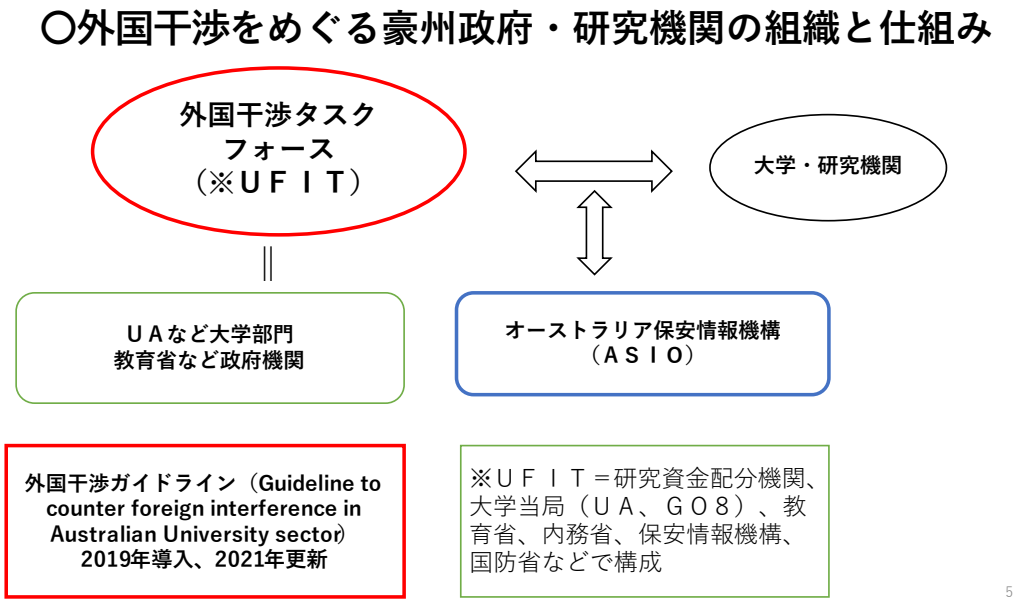

図 2-7：外国干渉をめぐる豪州政府・研究機関の組織と仕組み