

○研究インテグリティ・研究セキュリティの確保のための具体的な対応について

令和5年5月29日
研究担当副学長決定

改正 令和 8年 5月28日

研究インテグリティ・研究セキュリティの確保のための具体的な対応について

1 国立大学法人筑波大学及び部局において今後取り組むべき事項

- (1) 国立大学法人筑波大学は、研究者等、事務職員、技術職員等に対し、以下の事項について啓発に努める。
 - ア 研究活動の国際化、オープン化に伴う新たなリスクを認識すること。
 - イ 研究者等は、自らの研究活動の透明性を確保し、かつ、説明責任の必要性を理解すること。
 - ウ 利益相反・責務相反及び技術・情報流出の危険性並びに防止の重要性を認識すること。
- (2) 各部局は、研究者等とともに以下の情報についてその把握に努める。
 - ア 兼業を含む全ての所属組織と役職（海外の人材登用プログラムへの参加、名誉教授等を含む。）
 - イ 海外を含む外部機関から供与された全ての資金や資金以外の支援
 - ウ 研究者等が関与する全ての共同研究等の相手方や参画者の情報
- (3) 研究推進部研究企画課は、研究インテグリティ・研究セキュリティの相談窓口を通して各部局と研究インテグリティ・研究セキュリティの確保のための情報の共有及び連携の強化に努める。

2 部局における対応の基本的な考え方

各部局においては、当該部局に所属する大学教員等の研究者又は当該部局を担当する支援室の職員等が、研究活動の国際化、オープン化に伴う新たなリスクに対応して、輸出管理事案及び利益相反事案としてそれぞれ定められた手続を取るものを除いて、次の場合にそれぞれの手続を進める前に、以下の連絡部署に速やかに連絡するものとし、連絡後は研究インテグリティ及び研究セキュリティの確保のために必要な取組に主体的に協力するものとする。懸念度の高い事案については、対応等の決定までに数か月以上を要することに留意すること。

- (1) 研究の健全性・公正性に係るリスクを生じ得る事案が生じたとき
- (2) 当該部局に所属する大学教員等の研究者が、内閣府「研究セキュリティの確保に関する取組のための手順書」に定める特定研究開発プログラム（府省が資金配分機関と相談の上で指定する研究開発プログラム）に応募又は参加するとき
- (3) 共同研究先の企業等から研究セキュリティ確保のための取組を求められたとき

・連絡部署（相談窓口）：研究推進部研究企画課研究公正係

E-mail：research_integrity-security@un.tsukuba.ac.jp

内線：2922

3 研究の健全性・公正性に係るリスクを生じ得る事案についての判断

以下の(1)のような事案（これらはあくまで例示であり、これらに限定されるわけではない。）のうち、(2)に掲載している判断基準のアとイ、アとウ、イとウあるいはアとイとウの

ように重複して該当する場合や、イヤウに単独で該当する場合には、連絡部署（相談窓口）に連絡するものとする。また、当初は該当しない場合であっても、事後に該当することになった場合も同様とする。

(1) リスクが生じる可能性のある事例

- ・ 国際交流協定
- ・ 海外出張
- ・ 海外から／への研究員・留学生の受入れ／派遣
- ・ 海外機関とのクロスアポイントメント／兼業
- ・ 海外機関からの荣誉称号付与
- ・ 海外機関との共同研究／共同研究契約
- ・ 海外からの寄附の申入れ
- ・ 海外ファンドへの申請・受入れ
- ・ 懸念機関である国内法人との協力関係
- ・ 外国政府・機関等から強い影響を受けている居住者への技術提供

(2) 連絡するかどうかの判断基準

ア 先端的な重要技術等の提供であるかどうか

提供される技術が、輸出管理のリスト規制に該当するか、あるいは、そのおそれがあるときは、輸出管理手続をとらなければならない。それにあてはまらない場合であって、重要技術でありながら公知となっていない場合が該当する。政府が策定する重要技術領域リストに掲載される技術を重要技術とすることとするが、これが策定されるまでの間は、経済安全保障の強化に向けた基本指針で示された20の技術領域をもって、これに替えることとする（「特定重要技術の研究開発の促進及びその成果の適切な活用に関する基本指針」（令和4年9月30日閣議決定）p. 7（バイオ技術、医療・公衆衛生技術（ゲノム学含む）、人工知能・機械学習技術、先端コンピューティング技術、マイクロプロセッサ・半導体技術、データ科学・分析・蓄積・運用技術、先端エンジニアリング・製造技術、ロボット工学、量子情報科学、先端監視・測位・センサー技術、脳コンピュータ・インターフェース技術、先端エネルギー・蓄エネルギー技術、高度情報通信・ネットワーク技術、サイバーセキュリティ技術、宇宙関連技術、海洋関連技術、輸送技術、極超音速、化学・生物・放射性物質及び核（CBRN）、先端材料科学）。

イ 相手国・地域・機関の懸念度が大きいかどうか

- ・ 相手国・地域として懸念度が大きいのは、以下の場合などである。
 - (a) 輸出管理対象国のグループDが該当する。すなわち、輸出貿易管理令別表第3の2（国連武器禁輸国・地域）、輸出貿易管理令別表第4（懸念国）の国・地域である（アジア：アフガニスタン、イラン、イラク、レバノン、北朝鮮、アフリカ：コンゴ民主共和国、スーダン、ソマリア、中央アフリカ、南スーダン、リビア）。
 - (b) 経済産業省で提供している、大量破壊兵器等の開発等の懸念が払拭されない外国所在団体の情報である「外国ユーザーリスト」に掲載されている国・地域の場合
<https://www.meti.go.jp/policy/anpo/law00.html>
- ・ 相手機関として懸念度が大きいのは、以下の場合などである。
 - (a) 経済産業省で提供している、大量破壊兵器等の開発等の懸念が払拭されない外国所在団体の情報である「外国ユーザーリスト」に掲載されている場合
<https://www.meti.go.jp/policy/anpo/law00.html>
 - (b) 米国のBIS（商務省産業安全保障局）のウェブサイトに掲載されている米国の商

務省、国務省、財務省の制裁リストを統合したスクリーニングリスト(Consolidated Screening List; CSL) に記載されている場合

<https://www.trade.gov/consolidated-screening-list>

<https://www.trade.gov/data-visualization/csl-search>(リストの検索エンジン)

ウ 世界情勢等からのレピュテーションリスクがあるかどうか

特定の企業との関係で、当該企業が、外国での著しい人権侵害に関わっている場合など(例えば、2022年8月31日に、国連人権高等弁務官事務所(OHCHR)が発表した報告書(OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China)において、監視システムが、虹彩スキャンや顔画像などの生体認証データ収集の形での対面及び電子監視など、必要な技術を提供する民間のセキュリティ及び技術企業と提携して開発されたことが報告されている。)に、それらの企業と協力関係を持つことは、本学にとって大きなレピュテーションリスクとなり得る。

附 記

この決定は、令和5年7月20日から実施する。

附 記(令8.5.28)

この決定は、令和8年5月28日から実施し、この決定による改正後の研究インテグリティの確保のための具体的な対応についての規定は、同年4月1日から適用する。